Behobene Probleme

Feb 24, 2017

Die folgenden Probleme wurden in XenMobile 10.4 behoben Behobene Upgrade Tool-Probleme werden unter der Überschrift "XenMobile Upgrade Tool 10.4" am Ende dieses Artikels aufgeführt.

Hinweis: Ab Version 10.4 heißen die mobilen Worx-Apps "XenMobile-Apps". Die meisten Einzel-Apps wurden ebenfalls umbenannt. Weitere Informationen finden Sie unter Info über XenMobile Apps.

Wenn Sie zum Hinzufügen einer App aus dem öffentlichen App-Store für Windows Phone eine URL aus dem Microsoft-Store eingeben, schlägt der Upload fehl. [CXM-13468]

Nach einem Upgrade von XenMobile 9 auf 10.3.6 ist es in manchen Konfigurationen auf zuvor in XenMobile 9 registrierten Geräten nicht möglich, installierte Apps aufzurufen oder neue Apps aus dem WorxStore herunterzuladen. Außerdem verschwinden Apps aus Worx Home und Benutzer können nicht auf den WorxStore zugreifen. [CXM-13708]

Wenn Sie eine WiFi-Geräterichtlinie mit einem festgelegten WiFi-Kennwort einrichten, das Sonderzeichen (z. B. <, > oder &) enthält, werden die Benutzer aufgefordert, ihr WiFi-Kennwort einzugeben. [CXM-13717]

Beim Hochladen einer iOS-Unternehmensapp, deren Symbol eine Größe über 1000 KB hat, wird der Fehler "Symbol nicht gefunden" angezeigt. [CXM-13729]

Wird bei aktiviertem Clustering ein Befehl zum Löschen aller Daten an ein getrenntes Gerät gesendet, erfolgt die Löschung wie erwartet, sobald das Gerät eine Verbindung herstellt. Wird das Gerät allerdings neu registriert oder mit einem anderen Knoten im Cluster verbunden, erfolgt die Löschung erneut. [CXM-13793]

Die Berechtigung "Registrierung für gemeinsam genutzte Geräte" ist für die RBAC-Rolle in XenMobile Service-Bereitstellungen (Cloud) standardmäßig aktiviert. Dies führt dazu, dass alle Geräte von Benutzern mit dieser Administratorrolle als gemeinsam genutzte Geräte registriert werden. [CXM-15203]

Wenn Sie die Clientzertifikatauthentifizierung konfigurieren und auf dem Zertifizierungsstellenserver die Option zum Erfordern der Servernamensanzeige aktiviert ist, schlägt die Registrierung fehl. [CXM-15312]

Bei der Suche nach Apps in Google Play über die XenMobile-Konsole werden je nach Android-Betriebssystem des registrierten Geräts manche Apps nicht angezeigt. Beispielsweise werden Apps, die mindestens Betriebssystemversion 4.4 erfordern, nicht im Ergebnis angezeigt. [CXM-15653]

Wenn Sie einen lokalen Benutzer in einer lokalen Gruppe erstellen und dieser versucht, ein Windows 10-Gerät zu registrieren, schlägt die Registrierung fehl. [CXM-16895]

Wenn Sie eine Citrix Launcher-Richtlinie erstellen, können die Benutzer Android-Geräte registrieren. Wenn Sie jedoch eine Richtlinieneinstellung ändern, können die Benutzer Citrix nicht mit dem in der Richtlinie festgelegten Kennwort verlassen. Fügen Sie das Kennwort als Workaround neu in die Richtlinieneinstellungen ein und aktualisieren Sie die Richtlinie. [CXM-17157]

Wenn Sie die Option "ShareFile aktivieren" in XenMobile deaktivieren, können Benutzer in Secure Mail für Android auf Anlagen, unabhängig von deren Typ, nicht zugreifen. [CXM-17887]

Bei einem Update von XenMobile 10.3.6 mit Rolling Patch 1 auf XenMobile 10.4 laufen permanente Lizenzen unter Anzeige einer Fehlermeldung ab. [CXM-17900]

Bei einem Update von XenMobile 10.3.6 auf XenMobile 10.4 bleiben permanente Lizenzen zwar gültig, es wird jedoch gemeldet, dass sie abgelaufen seien. [CXM-17987]

Wenn Sie eine Nicht-US-URL einer öffentlichen Windows-Store-App eingeben, wird in der XenMobile-Konsole ein Fehler angezeigt. Bei Verwendung der URL der US-Store-App ist der Upload erfolgreich. [CXM-18013]

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]

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 bei der XenMobile-Konsole zu **Analysieren > Berichterstellung** navigieren und dann auf **Inaktive Geräte** klicken, wird eine leere Seite angezeigt statt eine Datei herunterzuladen. [#609649]

Über den XenMobile NetScaler Connector werden bei einer Synchronisierung mit ActiveSync keine Samsung 5.x-Geräte abgerufen. [#613522]

Wenn Sie für Android eine WiFi-Geräterichtlinie mit dem Authentifizierungstyp 802.1xEAP erstellen, ist das Kennwortfeld keinPflichtfeld mehr. [#614932]

Dieser Fix behebt ein Sicherheitsrisiko. Weitere Informationen finden Sie im Sicherheitsbulletin http://support.citrix.com/article/CTX207824.
Hinweis: Dieser Sicherheitsfix wird erst nach einem zweiten Neustart des XenMobile-Servers angewendet. [#624347]

Zurzeit können Sie Ihre Android-ID nicht wie unter **Einstellungen > Google Play-Anmeldeinformationen** in der XenMobile-Konsole beschrieben abrufen, indem Sie *#*#8255#*#* auf Ihrem Telefon eingeben. Verwenden Sie eine Geräte-ID-App aus dem Google Play Store, um die ID Ihres Geräts anzuzeigen. [#633854]

Bei der Windows Phone-Registrierung wird Worx Home manchmal nicht gestartet. [#633884]

Deaktivierte HDX-Apps werden im Worx Store nicht aufgezählt.[#634110]

Der XenMobile-Server zeigt falsche Benutzerdaten in der Protokolldatei an. [#636754]

Nach dem Update von XenMobile 10.3.1 auf 10.3.6 werden Dateityp und Zielordner in den Eigenschaften der Dateirichtlinie auf der XenMobile-Konsole nicht ordnungsgemäß angezeigt.[#640334]

Das Textfeld für das VPP-Token hat eine maximale Länge von 256 Zeichen. [#640692]

Windows Phone-Geräte können nicht mit sAMAccount-Attributen registriert werden. [#640847]

Nach dem Entfernen registrierter Benutzern aus dem ShareFile-Steuerungssubsystem werden diese Benutzer möglicherweise in der Benutzerauditprotokolldatei der XenMobile-Konsole angezeigt. [#641342]

Nach dem Upgrade von XenMobile Server 10.1 auf 10.3.x wird mit einem Klick auf "https:///zdm/enrollmdm.html" iOS nicht als Plattformauswahl aufgeführt. [#641771]

Bei der Registrierung eines Geräts mit Worx Home für iOS ist die MDM-Registrierung ggf. erfolgreich, die MAM-Registrierung schlägt jedoch fehl. [#644892]

Das Löschen verschachtelter Gruppen wird nicht in der Anzeige berücksichtigt. [#647557]

Wenn **Verwalten > Registrierung** mehr als 2000 Einträge hat und Sie auf **Exportieren** klicken, wird die Seite leer angezeigt und kein Bericht generiert. [#647855]

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. [#647987]

Das Hochladen von iOS-Apps schlägt fehl. Es wird folgende Fehlermeldung angezeigt: Hochgeladene mobile App ist ungültig. Anwendungssymbol wurde nicht gefunden.[#649574]

Der XenMobile-Server kann aufhören zu reagieren und es wird Arbeitsspeichermangel gemeldet. [#650490]

Probleme mit der Datenlöschung auf Geräten aufgrund von Cluster-Meldungen. [#650555]

Beim Konfigurieren einer VPN-Geräterichtlinie können Sie keine Portnummer angeben. [#650972]

Nach dem Upgrade des XenMobile-Servers bei aktiviertem Clustering können mehrere Deadlocks auftreten. Der Server kann aufhören, zu reagieren. [#651122]

Auf der XenMobile-Konsole wird zusammen mit der Aufforderung zum Bestätigen eines Gerätelöschvorgangs keine Seriennummer angezeigt. [#651185]

Die SSO-Richtlinie unter XenMobile Server 10.3.6 funktioniert nicht wie erwartet. Die Benutzer werden weiterhin zur Kennworteingabe aufgefordert. [#651860]

Das Deaktivieren der iPad-App-Zuordnung für VPP-Apps ist in XenMobile 10.3.6 nicht möglich.[#652280]

Wird eine Bereitstellungsgruppe aus einer Geräterichtlinie gelöscht, wird die Änderung in XenMobile nicht gespeichert und die Bereitstellungsgruppe bleibt der Richtlinie zugewiesen. [#652321]

Das Speichern eines kurzen FQDN ist für ein SSO-Konto nicht möglich. [#652704]

Wenn ein Benutzer die Berechtigung zur Geräteverwaltung von seinem Android-Gerät entfernt, wird der Gerätezustand sowohl für MDX- als auch für MAM-Geräte auf "Orange/nicht verwaltet" geändert und der Benutzer hat keinen Zugriff auf MDX-Apps. Der MAM-Zustand müsste weiterhin "Grün/verwaltet" sein. [#655180]

Wenn die Geräteeinstellung in XenMobile 9.0 für die mindestens oder maximal erforderliche Betriebssystemversion auf 10 oder höher festgelegt ist und für MDX und Enterprise Apps ausgeschlossene Geräte festgelegt sind, wird diese Regel nach dem Upgrade nicht richtig migriert. Apps, die angezeigt werden sollten, werden nicht angezeigt, und Apps, die nicht angezeigt werden sollten, werden angezeigt. [#603412]

Wenn Microsoft SQL Server so konfiguriert ist, dass die Groß-/Kleinschreibung beachtet werden muss, schlägt ein Upgrade fehl, wenn die Tabelle "Id_Generator" in Form von "Id_generator" angegeben wird. [#623300]

Nach dem Upgrade von XenMobile 9 auf XenMobile 10 ist der Typ des Werts für die Richtlinie "Persönlicher Hotspot"

"Boolesch" statt "Zeichenfolge". [#633337]

Wenn der Name einer Active Directory-Gruppe das @-Zeichen enthält, schlagen Upgrades fehl. [#633718]

Wenn der Device Manager 9.0-Server für die Verwendung einer lokalen PostgreSQL-Instanz konfiguriert ist und Sie localhost als Verweis für den Datenbankserver verwenden, schlägt das Upgrade fehl. Ersetzen Sie als Workaround in der Datei ew-config.properties auf dem Device Manager 9.0-Server alle localhost-Verweise durch die IP-Adresse des Device Manager-Datenbankservers und fahren Sie dann mit den Upgradevoraussetzungen fort. [#635023]

Wenn Sie in XenMobile 9.0 für die LDAP-Verbindung den Parameter **Users organizational unit** festgelegt haben, wird nach dem Upgrade auf XenMobile 10 der vollständige Stammkontext nicht an die Organisationseinheit der Benutzer angehängt. Beispiel: OU=MDMUsers, OU=SALES müsste OU=MDMUsers, OU=SALES, DC=citrite, DC=com entsprechen. Sie müssen das entsprechende Update daher in XenMobile 10 manuell vornehmen. [#635981]

Wenn bei einem Upgrade das Supportpaket hochgeladen wird, wird der Fehler gemeldet, dass das Setup von MAM fehlgeschlagen ist und Einzelheiten in den Protokollen zu finden sind. Im Upgrade Tool werden beschädigte MAM-Daten beibehalten. [#638062]

Wenn der Name einer Active Directory-Gruppe einen Punkt (.) enthält, verlieren als Bereitstellungsgruppe migrierte Rollen die Gruppenzuweisung. [#647590]

Wenn die Webproxy-Einstellung in App Controller das Zeichen "\" enthält, kann der XenMobile 10.1-Server nicht gestartet werden. Es wird gemeldet, dass die Haupt-App gestartet wird, während der Server mit dem Neustart fortfährt. [#647919]

Nach dem Upgrade von XenMobile 9 auf XenMobile 10 werden kostenpflichtige VPP-Apps aus dem XenMobile-Store (Worx-Store) nicht installiert, es sei denn, die App-Konfiguration erzwingt die Installation. [#668102]

Nach einem Upgrade auf XenMobile 10.3.6 ist es in Konfigurationen mit domänenübergreifender Authentifizierung auf zuvor in XenMobile 9 registrierten Geräten nicht möglich, installierte Apps aufzurufen oder neue Apps aus dem Worx-Store (XenMobile-Store) herunterzuladen. [CXM-13708]

Nach einem Upgrade von XenMobile 9 auf XenMobile 10 werden installierte Apps aus öffentlichen Stores im XenMobile-Store (Worx-Store) als nicht abonniert angezeigt. [CXM-17936]

Wenn die Datenbankverbindungs-URL "localhost" ist, muss die Datei ew-config.properties nicht mehr bearbeitet werden.

Wenn Sie RBAC-Rollen mit auf Active Directory oder LDAP und Active Directory oder eine untergeordnete Ebene beschränktem Zugriff konfiguriert haben, werden diese Einstellungen nach dem Upgrade nicht ausgewählt, wenn Sie sich bei der XenMobile-Konsole als Administrator anmelden.

Bekannte Probleme

Feb 24, 2017

Nachfolgend sind bekannte Probleme in XenMobile 10.4 aufgeführt.

Beim Konfigurieren von Citrix Launcher funktioniert die Option **Just Once** nicht. Sie müssen auf **Always** klicken. [CXM-13413]

Bei der erneuten Registrierung von Android-Geräten erfolgt in manchen Fällen unerwartet eine selektive Löschung. [CXM-13716]

Wenn Sie in der XenMobile-Konsole öffentliche Apps konfiguriert haben und nach dem Update auf XenMobile 10.4 Secure Hub auf Windows 10-Tablets bereitstellen, werden die öffentlichen Apps nicht angezeigt. [CXM-16516]

Wenn Benutzer mit Citrix Launcher im MDM-Modus den XenMobile Store öffnen, wird dieser in einem Standardbrowser geöffnet, selbst wenn Sie einen anderen Browser auf einer Positivliste aufgelistet haben. [CXM-17097]

Citrix Launcher kann Logo- und Hintergrundbilder nicht von Servern mit selbstsigniertem Zertifikat herunterladen. [CXM-17159]

Bei Verwendung der XenMobile-Konsole mit Internet Explorer 11 können Sie keine neue LDAP-Konfiguration hinzufügen. [CXM-18324]

Probleme bei Daten und Richtlinien

Beim Upgrade werden Syslog-Serverkonfigurationsdaten nicht zum XenMobile-Server migriert. [#558539]

Einige Einschränkungsrichtlinienkonfigurationen waren ab Version 10.1 veraltet. Daher kann bei einem Upgrade von XenMobile 9 auf XenMobile 10.4 nicht die vollständige Einschränkungsrichtlinie auf Windows Phone 10-Geräten bereitgestellt werden. Wenn Sie die Richtlinieneinstellungen in XenMobile 10.4 anzeigen und speichern, wird die Richtlinie jedoch erfolgreich bereitgestellt. [#608541]

Wenn Ihre XenMobile 9-Bereitstellung die Unternehmensapp gpsstats.apk enthält, kann das Upgrade auf XenMobile 10.4 fehlschlagen. [CXM-17992]

Nach dem Upgrade von XenMobile 9 auf XenMobile 10.4 sind Windows-Geräte im MDM-Modus statt im MAM+MDM-Modus, außerdem wird der XenMobile Store nicht geöffnet. Als Workaround können die Benutzer ein migriertes Gerät erneut registrieren. [CXM-18532]

Google Play-Apps

Wenn Sie eine öffentliche Google Play-App für Android-Geräte mit einem Standardsymbol migrieren, wird das Standardsymbol nach der Migration nicht in der XenMobile-Konsole angezeigt. Sie müssen die App entweder bearbeiten und speichern oder auf Check for Updates klicken, damit das Symbol angezeigt wird. [#557996]

SQL Server

Wenn Sie eine PostgreSQL-Datenbank verwenden, können MAM-Geräte nach einem Upgrade nicht neu registriert werden. Löschen Sie als Workaround die Geräteeinträge aus XenMobile und senden Sie Registrierungsbenachrichtigungen an die

Benutzer. [#632831]

RBAC

Nach dem Upgrade treten Probleme mit RBAC-Einstellungen auf:

- Wenn Sie eine Super Admin-Rolle konfiguriert haben, werden standardmäßig alle Berechtigungen ausgewählt. Nach dem Upgrade sind nur drei Berechtigungen ausgewählt: RBAC, Enrollment und Release Management.
- Wenn Sie eine benutzerdefinierte Super Admin-Rolle erstellt haben, sollten standardmäßig alle Support-Berechtigungen ausgewählt sein. Nach dem Upgrade ist keine Support-Berechtigungseinstellung ausgewählt. Um dieses Problem zu lösen, erstellen Sie die Support-Berechtigung nach dem Upgrade. [#569350, #569395, #569423]

Citrix Secure Hub und Citrix Store

Wenn Ihr WorxStore einen benutzerdefinierten Namen hat, treten nach dem Upgrade von XenMobile 9 auf XenMobile 10.4 Probleme beim Registrieren sowie beim Zugreifen auf Worx Home und den WorxStore auf. Als Workaround setzen Sie vor dem Upgrade den Namen des Stores auf die Standardeinstellung **Store** zurück. Informationen zu dem erforderlichen Workaround finden Sie unter Voraussetzungen für das Upgrade Tool. [#619458]

Wenn Sie nach einem Upgrade von XenMobile 9.0 auf XenMobile 10.4 die LDAP-Option **Benutzersuche nach** auf **sAMAccountName** festlegen, können sich Benutzer mit Geräten im Nur-MAM-Modus nicht bei Citrix Secure Hub authentifizieren. [#628233]

Android for Work

Nach einem Upgrade schlägt die SAML-Anmeldung für Android for Work fehl, weil das SAML-Zertifikat die Erweiterung ".pem" hat und diese vom XenMobile-Server nicht importiert wird. [#631795]

Stellen Sie als Workaround folgendermaßen sicher, dass XenMobile das richtige SAML-Zertifikat hat:

1. Exportieren Sie das SAML-Zertifikat aus XenMobile 9 App Controller mit einem privaten Schlüssel (AppController.example.com). Das Zertifikat hat das PEM-Format und die Erweiterung ".pem".

2. Erstellen Sie aus der PEM-Datei mit dem Befehl "openssl" eine PFX-Datei:

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

3. Importieren Sie die PFX-Datei in XenMobile 10.3 als SAML-Schlüsselspeicher.

4. Exportieren Sie das SAML-Zertifikat ohne privaten Schlüssel aus XenMobile 10.4 und laden Sie es in die Android for Work-Domäne hoch.

Architektur

Feb 24, 2017

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 Secure Hub 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 mobile Apps, die in und außerhalb des Unternehmens erstellt wurden (z. B. XenMobile-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 Clustering.

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. Architekturdiagramme finden Sie in den Artikeln Reference Architecture for On-Premises Deployments und Reference Architecture for Cloud Deployments des XenMobile-Bereitstellungshandbuchs. Eine vollständige Liste der Ports finden Sie unter Portanforderungen.

Mobilgeräteverwaltungsmodus (MDM-Modus)

XenMobile MDM Edition bietet Mobilgeräteverwaltung für iOS, Android, Amazon und Windows Phone (siehe Unterstützte Geräteplattformen in XenMobile). Sie stellen XenMobile im MDM-Modus bereit, wenn Sie nur die MDM-Funktionen 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, aber keine Windows Phone-Geräte (weitere Informationen finden Sie unter Unterstützte Geräteplattformen in XenMobile). Sie stellen XenMobile im MAM-Modus bereit ("Nur-MAM-Modus"), wenn Sie nur die MAM-Features von XenMobile ohne Geräteregistrierung 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

Die Verwendung von MDM und MAM zusammen ermöglicht die Verwaltung mobiler Apps und Daten sowie von Mobilgeräten für iOS, Android und Windows Phone (weitere Informationen finden Sie unter Unterstützte Geräteplattformen in XenMobile). Sie stellen XenMobile im ENT-Modus bereit (Enterprise), 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.

Systemanforderungen und -kompatibilität

Apr 24, 2017

Weitere Informationen zu Anforderungen und Kompatibilität finden Sie in den folgenden Artikeln:

- XenMobile-Kompatibilität
- Unterstützte Geräteplattformen
- Portanforderungen
- Skalierbarkeit
- Lizenzierung
- FIPS 140-2-Konformität
- Sprachunterstützung

Für die Ausführung von XenMobile 10.4 gelten die folgenden Mindestanforderungen:

- Eines der Folgenden:
  - XenServer (unterstützte Versionen: 6.5.x oder 7.0); weitere Details finden Sie unter XenServer
  - VMware (unterstützte Versionen: ESXi 5.5 oder ESXi 6.0); weitere Informationen finden Sie unter VMware.
  - Hyper-V (unterstützte Versionen: Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2); weitere Informationen finden Sie unter Hyper-V.
- Dual-Core-Prozessor
- 4 virtuelle CPUs
- 8 GB RAM
- 50 GB Speicherplatz

XenMobile-Version 10.4.x erfordert Citrix Lizenzserver 11.12.1 oder höher.

Für die Ausführung von NetScaler Gateway mit XenMobile 10.4 gelten die folgenden Mindestanforderungen:

- Eines der Folgenden:
  - XenServer (unterstützte Versionen: 6.5 oder 7.0)
  - 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

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

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 unterstützt SQL AlwaysOn Availability Groups und SQL-Clustering für hohe Datenbankverfügbarkeit.

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 9.5.2 und 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 3.6
StoreFront 3.5
StoreFront 3.0
StoreFront 2.6
Web Interface 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 10.4 unterstützt die folgenden E-Mail-Server:

- Exchange 2016

- Exchange 2013
- Exchange 2010

Portanforderungen

Feb 24, 2017

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 Citrix Secure Hub, 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 zu NetScaler Gateway finden Sie unter Configuration Settings for your XenMobile Environment in der NetScaler Gateway-Dokumentation. Informationen über NetScaler-eigene IP-Adressen, wie z. B. die NetScaler-IP-Adresse (NSIP), die IP-Adresse des virtuellen Servers (VIP) und die 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 (TCP und UDP)	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	NetScaler Gateway	NTP-Server

(TCP und UDP)	(NTP) verwendet.	XenMobile	
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 dem 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 Callback-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-	NetScaler Gateway	XenApp oder XenDesktop

	basierten Anwendungen im internen Netzwerk verwendet. Citrix empfiehlt, diesen Port geöffnet zu lassen.		
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

	Wird für den Download von Protokollen und Supportpaketen für alle XenMobile-Clusterknoten von einem Knoten verwendet.	XenMobile	XenMobile
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

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, Secure Hub für Android oder Secure Hub 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	XenMobile	LDAP-

	verwendet.		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

Diese Portkonfiguration gewährleistet, dass auf Android-Geräten mit Secure Hub 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 Secure Hub über die aktuellen Sicherheitsinformationen für die Umgebung verfügt, in der das Gerät registriert wird. Kann ein Gerät ADS nicht erreichen, lässt wird es von Secure Hub 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 Secure Hub 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

Skalierbarkeit und Leistung

Feb 24, 2017

Die Kenntnis der Größe der XenMobile-Infrastruktur ist ein wichtiger Faktor bei der Entscheidung darüber, wie Sie XenMobile bereitstellen und konfigurieren. Dieser Artikel enthält Daten aus Skalierbarkeitstests und Informationen zur Bestimmung der Infrastrukturanforderungen im Hinblick auf Leistung und Skalierbarkeit für kleine bis große lokale XenMobile 10.4-Bereitstellungen.

"Skalierbarkeit" bedeutet in diesem Zusammenhang die Fähigkeit vorhandener Geräte, also derer, die bereits registriert sind, zeitgleich eine Wiederverbindung mit der Bereitstellung herzustellen.

- *Skalierbarkeit* ist die maximale Anzahl registrierter Geräte in der Bereitstellung.
- *Anmelderate* ist die maximal mögliche Wiederverbindungsrate vorhandener Geräte.

Die Daten in diesem Artikel sind aus Tests von Bereitstellungen einer Größenordnung von 10.000 bis 60.000 Geräten abgeleitet. Bei den Tests wurden mobile Geräte mit bekannten Arbeitslasten verwendet.

Alle Tests wurden mit XenMobile Enterprise Edition durchgeführt.

Für die Tests wurde NetScaler Gateway 7500 für Bereitstellungen von bis zu 10.000 Geräten und NetScaler Gateway 5550 für Bereitstellungen mit mehr als 10.000 Geräten verwendet. Ein NetScaler Gateway-Gerät mit einer ähnlichen oder mehr Kapazität sollte ein ähnliches oder höheres Maß an Skalierbarkeit und Leistung erzielen.

Die folgende Tabelle enthält das Ergebnis der Skalierbarkeitstests:

Skalierbarkeit	**Maximal 60.000 Geräte**	
Anmelderate	Wiederverbindungsrate vorhandene Geräte	Maximal 7.500 Geräte pro Stunde
Konfiguration	NetScaler Gateway	MPX 7500, MPX 5550
	XenMobile Enterprise Edition	XenMobile-Servercluster mit 5 Knoten
	Datenbank	Externe Microsoft SQL Server-Datenbank

Testergebnis nach Gerätezahl und Hardwarekonfiguration

Die folgende Tabelle enthält das Testergebnis für die getesteten Gerätezahlen und Hardwarekonfigurationen.

Anzahl der Geräte	10.000	30.000	45.000	60.000

Wiederverbindungsrate vorhandener Geräte pro Stunde	833	3.750	5.625	7.500
XenMobile-Server – Modus	Eigenständig	Cluster	Cluster	Cluster
XenMobile-Server – Cluster	nicht zutreffend	3	4	5
XenMobile-Server – virtuelles Gerät	Speicher = 12 GB RAM vCPUs: 4	Speicher = 16 GB RAM vCPUs: 6	Speicher = 24 GB RAM vCPUs: 8	Speicher = 24 GB RAM vCPUs: 8
Active Directory	Speicher = 8 GB RAM vCPUs: 4	Speicher = 16 GB RAM vCPUs: 4	Speicher = 16 GB RAM vCPUs: 4	Speicher = 16 GB RAM vCPUs: 4
Externe Microsoft SQL Server-Datenbank	Speicher = 32 GB RAM vCPUs: 16	Speicher = 32 GB RAM vCPUs: 12	Speicher = 48 GB RAM vCPUs = 4 mit je 4 Kernen	Speicher = 48 GB RAM vCPUs = 4 mit je 4 Kernen

Bei Bereitstellungen mit 45.000 Geräten wurde SQL Server zur Erhöhung der Arbeitsthreads auf 2.000 konfiguriert. Bei Bereitstellungen mit 60.000 Geräten wurde SQL Server zur Erhöhung der Arbeitsthreads auf 3.000 konfiguriert. (Informationen zum Festlegen der Anzahl der Arbeitsthreads in SQL Server finden Sie in dem Microsoft-Artikel Konfigurieren der Serverkonfigurationsoption "Maximale Anzahl von Arbeitsthreads".)

Skalierbarkeitsprofil

Die folgende Tabelle enthält eine Übersicht über das zur Ermittlung der Daten in diesem Artikel verwendete Testprofil:

Active Directory - Konfiguration	Verwendetes Profil
Benutzer	100.000
Gruppen	200.000
Schachtelungsebenen	5

XenMobile Server-Konfiguration	Gesamt	Pro Benutzer
Richtlinien	20	20
Apps	270	50
Öffentliche App	200	0
MDX	50	30
Web & SaaS	20	20
Aktionen	50	
Bereitstellungsgruppen	20	
Active Directory-Gruppen pro Bereitstellungsgruppe	10	

SQL	
Anzahl der Datenbanken	1

Bei den Skalierbarkeitstests wurden Daten zur Wiederverbindungsfähigkeit von bei einer Bereitstellung registrierten Geräten über einen Zeitraum von 8 Stunden gesammelt.

In den Tests wurde ein Wiederverbindungsintervall simuliert, in dem die XenMobile-Serverknoten einer höheren Last als normal ausgesetzt waren, da die Geräte bei der Wiederverbindung alle geltenden Sicherheitsrichtlinien abrufen. Bei nachfolgenden Wiederverbindungen werden nur geänderte oder neue Richtlinien per Push auf iOS-Geräten bereitgestellt, sodass die Last auf den XenMobile-Serverknoten verringert wird.

Bei den Tests wurden 50 % iOS- und 50 % Android-Geräte verwendet.

Es wurde davon ausgegangen, dass die wiederverbindenden Android-Geräte zuvor eine GCM-Benachrichtigung erhalten haben.

Während des 8-stündigen Testintervalls erfolgten folgende App-bezogene Aktivitäten:

- Secure Hub wurde einmal zum Auflisten von Apps geöffnet.
- 2 SAML-Web-Apps wurden geöffnet.
- 4 MAM-Apps wurden heruntergeladen.
- 1 STA wurde zur Verwendung durch Secure Mail generiert.

- 240 STA-Ticketvalidierungen, 1 für jedes Secure Mail-Verbindungsereignis über ein Micro-VPN wurden ausgeführt.

Referenzarchitektur

Informationen zu der für die Bereitstellungen in den Skalierbarkeitstests verwendeten Referenzarchitektur finden Sie unter "Core MAM+MDM Reference Architecture" in Reference Architecture for On-Premises Deployments.

Hinweise und Einschränkungen

Bei der Interpretation der Ergebnisse der Skalierbarkeitstests in diesem Artikel ist Folgendes zu beachten:

- Die Windows-Plattform wurde nicht getestet.
- Die Push-Bereitstellung von Richtlinien wurde für iOS- und Android-Geräte getestet.
- Jeder XenMobile Server-Knoten unterstützt maximal 10.000 Geräte gleichzeitig.

Lizenzierung

Feb 24, 2017

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

Weitere Informationen zur Lizenzierung von NetScaler Gateway finden Sie in der Dokumentation zu NetScaler Gateway. Bei XenMobile wird die Citrix Lizenzierung zum Verwalten von Lizenzen verwendet. Informationen über die Citrix Lizenzierung finden Sie auf der Website zum Citrix Lizenzprogramm.

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

Sie müssen vor dem Herunterladen der XenMobile-Lizenzen die Citrix Lizenzierung installieren. Der Name des Servers, auf dem Sie die Citrix Lizenzierung installiert haben, ist zum Generieren der Lizenzdatei erforderlich. Wenn Sie XenMobile installieren, wird die Citrix Lizenzierung standardmäßig auf dem Server installiert. Alternativ können Sie eine vorhandene Bereitstellung der Citrix Lizenzierung zum Verwalten der XenMobile-Lizenzen verwenden. Weitere Informationen zur Installation, Bereitstellung und Verwaltung der Citrix Lizenzierung finden Sie unter Lizenzieren des Produkts.

Hinweis

XenMobile 10.4.x erfordert den Citrix Lizenzserver 11.12.1 oder höher, ältere Versionen funktionieren nicht mit XenMobile 10.4.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.

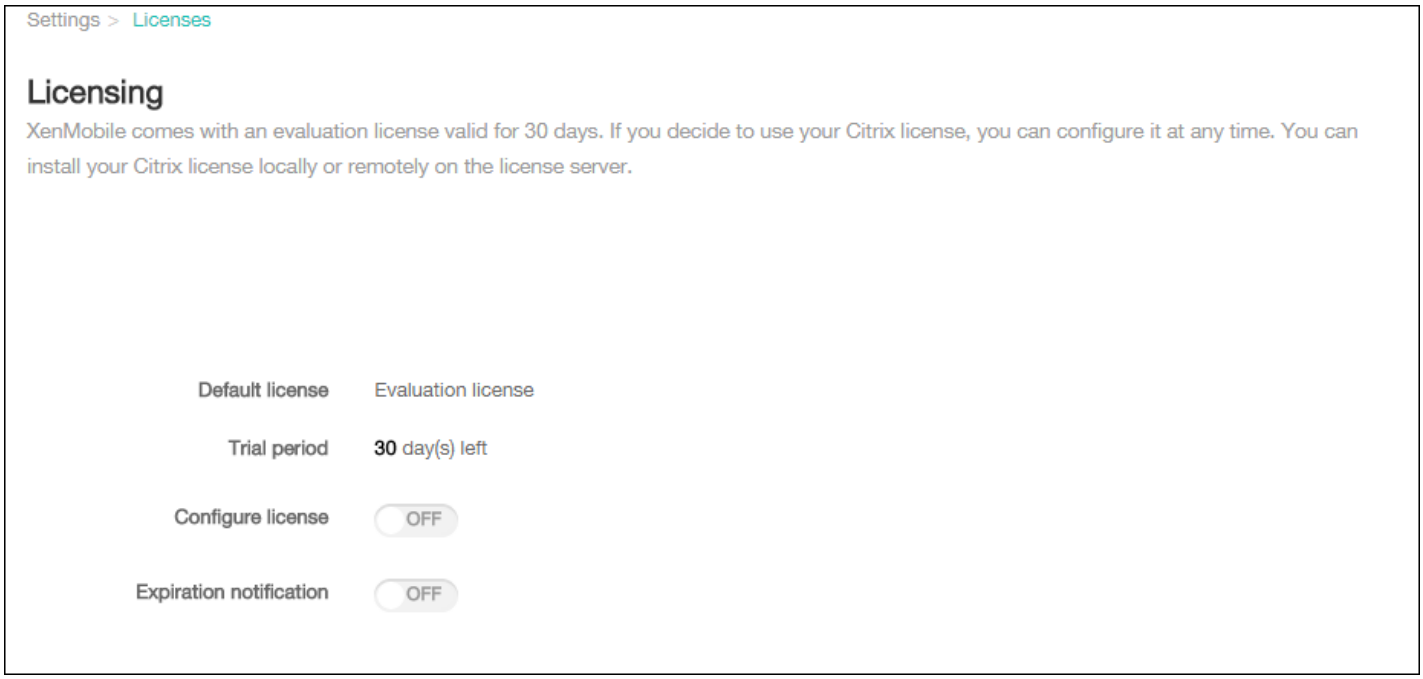
Ohne Lizenz kann XenMobile zu Evaluierungszwecken voll funktionsfähig für einen Zeitraum von 30 Tagen ausgeführt werden. Der Testmodus ist nur einmal möglich, der 30-tägige Kulanzzeitraum beginnt mit der Installation von XenMobile. Der Zugriff auf die XenMobile-Webkonsole ist nie gesperrt, unabhängig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

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.

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.

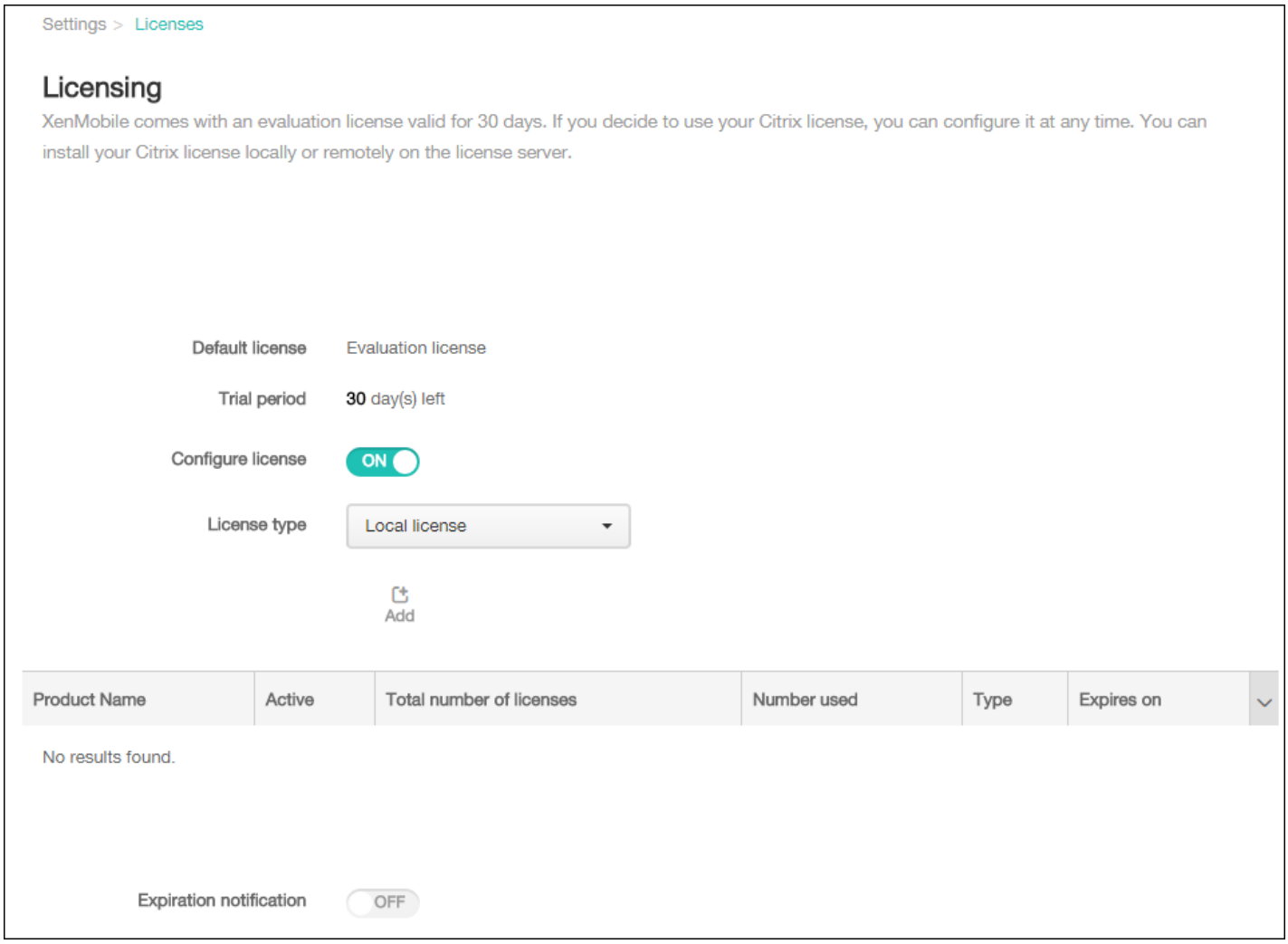
Sie können alle lokalen Lizenzen über die XenMobile-Konsole verwalten.

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.

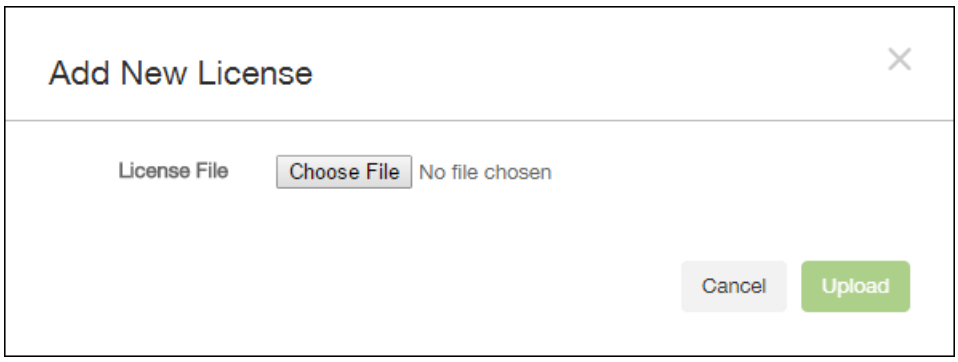
2. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

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.

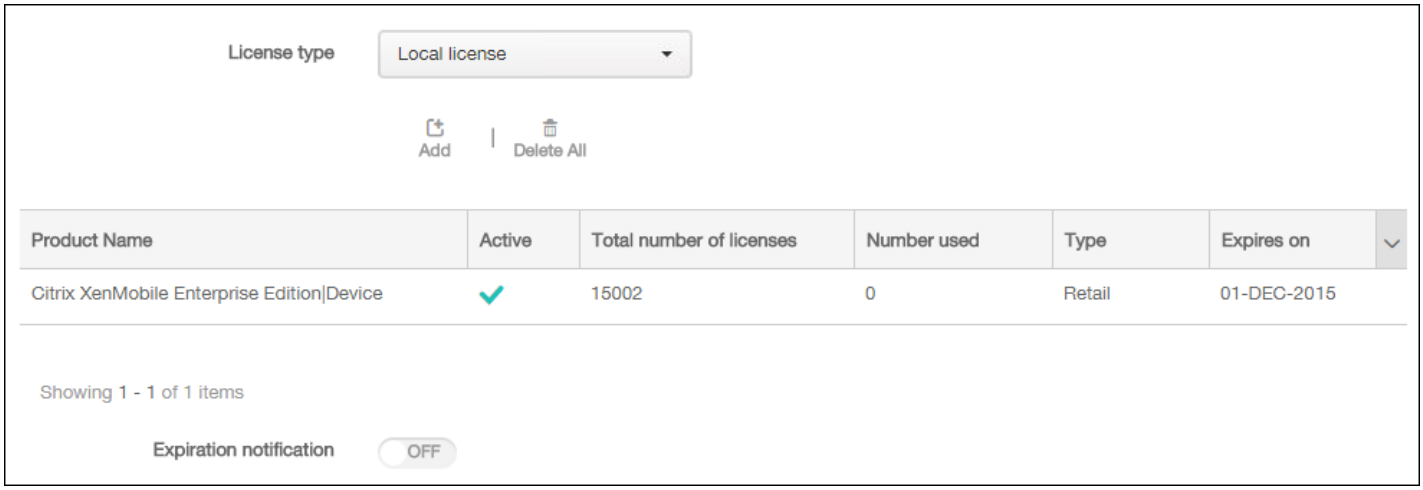


5. Stellen Sie sicher, dass **Lizenztyp** auf **Lokale Lizenz** festgelegt ist, und klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Lizenz hinzufügen** wird angezeigt.



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.

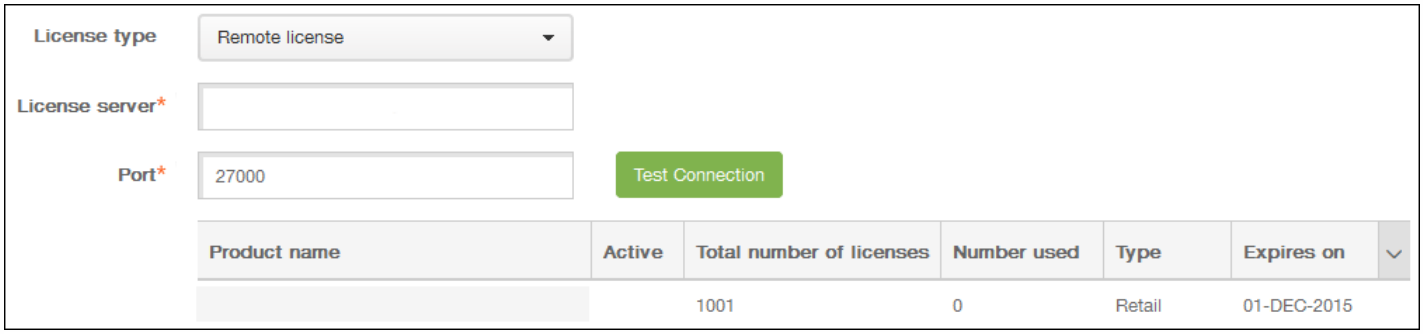


8. Wenn die Lizenz in der Tabelle auf der Seite **Lizenzierung** angezeigt wird, aktivieren Sie sie. Wenn dies die erste Lizenz in der Tabelle ist, wird sie automatisch aktiviert.

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:

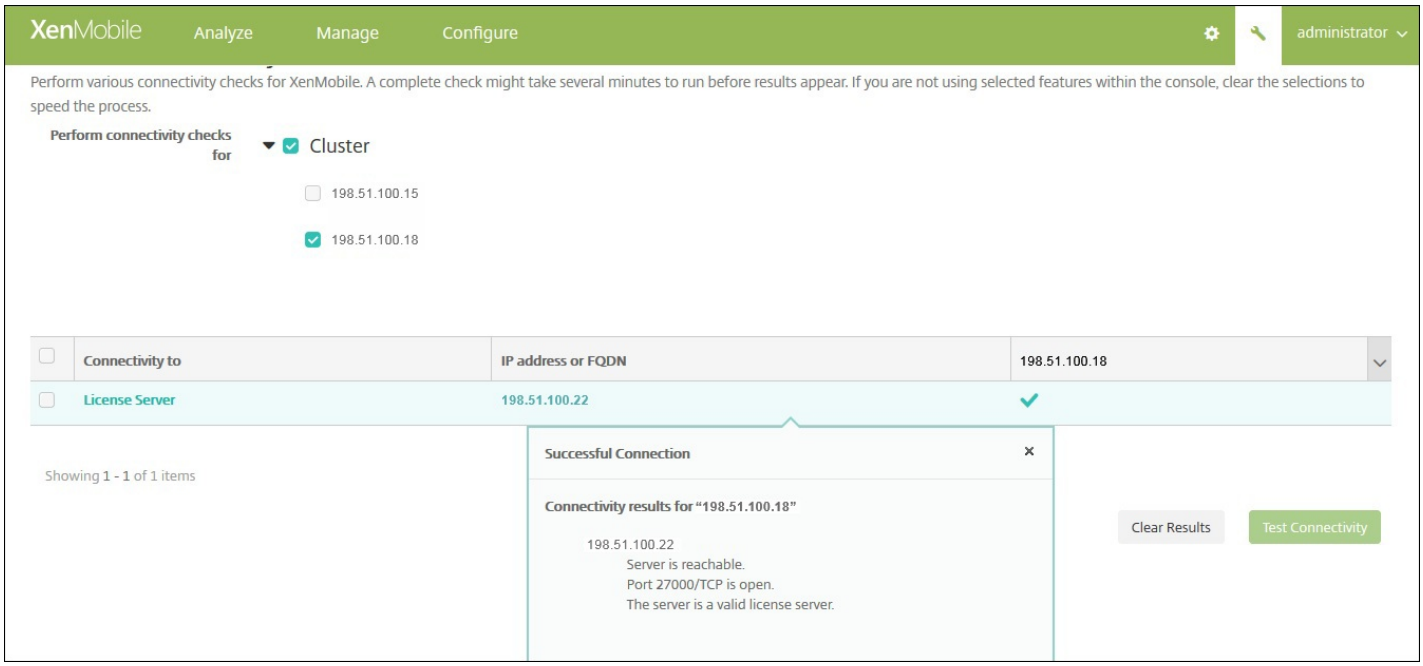
- **Lizenzserver**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Remoteservers für die Lizenzierung ein.
- **Port**: Übernehmen Sie den Standardport oder geben Sie die Portnummer für die Kommunikation mit dem Lizenzserver ein.

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:

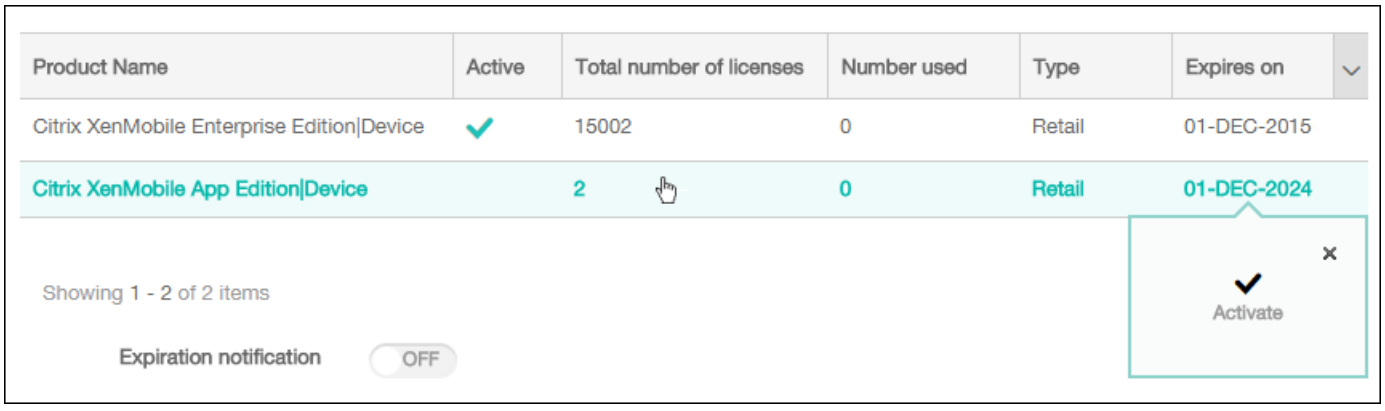
- XenMobile kann mit dem Lizenzserver kommunizieren.
- Die Lizenzen auf dem Lizenzserver sind gültig.
- Der Lizenzserver ist mit XenMobile kompatibel.

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



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.



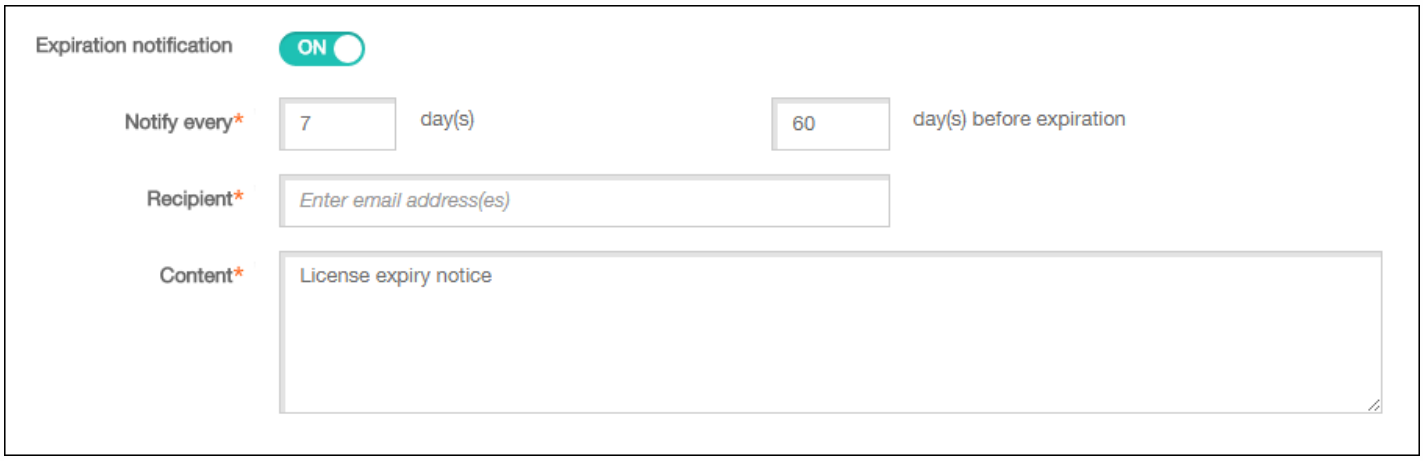
2. Klicken Sie auf **Aktivieren**. Das Dialogfeld **Aktivieren** wird angezeigt.

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

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

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.

FIPS 140-2-Konformität

Apr 24, 2017

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: FIPS-Unterstützung steht nur für lokale Installationen von XenMobile-Server zur Verfügung. 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

Apr 24, 2017

XenMobile-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 unter http://support.citrix.com/article/CTX119253.

Dieser Artikel enthält eine Liste der in XenMobile 10.4 unterstützten Sprachen.

- Französisch
- Deutsch
- Koreanisch
- Portugiesisch
- Vereinfachtes Chinesisch

Ein X bedeutet, dass die App in der jeweiligen Sprache zur Verfügung steht. Secure Forms ist derzeit nur auf Englisch verfügbar.

Hinweis: Ab Version 10.4 heißen die mobilen Worx-Apps "XenMobile-Apps". Die meisten Einzel-Apps wurden ebenfalls umbenannt. Weitere Informationen finden Sie unter Info über XenMobile Apps.

iOS und Android

	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	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	Nur iOS
Arabisch	X	X	X	X	X	Nur iOS
Russisch	X	X	X	X	X	X

Windows

	Secure Hub	Secure Mail	Secure Web
Französisch	X	X	X
Deutsch	X	X	X
Spanisch	X	X	X
Italienisch	X	X	X
Dänisch	X	X	X
Schwedisch	X	X	X

In der folgenden Tabelle wird für jede App aufgeführt, welche Sprachen des Nahen Ostens unterstützt werden. Ein X gibt an, dass die Funktion für die betreffende Plattform verfügbar ist. Windows-Geräte unterstützen keine Sprachen mit

Schreibrichtung von rechts nach links.

	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
Secure Tasks	X	X
Secure Notes	X	X
QuickEdit	X	X

Installation und Konfiguration

Apr 24, 2017

Vorbereitungen:

Die nachfolgende Prüfliste 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.

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

Installationsanweisungen finden Sie unter Installieren von XenMobile weiter unten in diesem Artikel.

Prüfliste zur Installationsvorbereitung

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. Reservieren Sie eine IP-Adresse, wenn Sie eine Instanz von XenMobile installieren. Wenn Sie einen Cluster konfigurieren, notieren Sie alle benötigten IP-Adressen.	XenMobile	
	• 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	NetScaler Gateway	

	Geben Sie alle internen Netzwerke und Netzwerksegmente an, auf die Benutzer zugreifen müssen, wenn sie eine Verbindung mit Secure Hub oder dem NetScaler Gateway-Plug-In herstellen und Split-Tunneling auf "Ein" gesetzt ist.		
	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 unter Das Citrix Lizenzierungssystem.

•	Voraussetzung	Komponente	Speicherort notieren
	Universelle Lizenzen erhalten Sie auf der Citrix Website. Weitere Informationen finden Sie unter Lizenzierung in der NetScaler Gateway-Dokumentation.	NetScaler Gateway XenMobile Citrix Lizenzserver	

Zertifikate

XenMobile und NetScaler Gateway erfordern Zertifikate für Verbindungen mit anderen Citrix Produkten und Anwendungen auf Benutzergeräten. Weitere Informationen finden Sie unter Zertifikate und Authentifizierung in der Dokumentation zu 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.

✓	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. Das in XenMobile verwendete SQL Server-Dienstkonto muss die Rollenberechtigung "DBcreator" haben.	XenMobile	

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	
	Notieren Sie die Callback-URL.	XenMobile	

Benutzerverbindungen: Zugriff auf XenDesktop, XenApp und Citrix Secure Hub

Citrix empfiehlt, dass Sie Einstellungen für Verbindungen zwischen XenMobile und NetScaler Gateway und zwischen XenMobile und Secure Hub mit dem Konfigurationsassistenten in NetScaler konfigurieren. Sie erstellen einen zweiten virtuellen Server, damit Benutzerverbindungen von Citrix Receiver und Webbrowsern mit Windows-basierten Anwendungen und virtuellen Desktops in XenApp und XenDesktop ermöglicht werden. 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 Secure Hub.	NetScaler Gateway	

Installieren von XenMobile

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.

> ## 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.

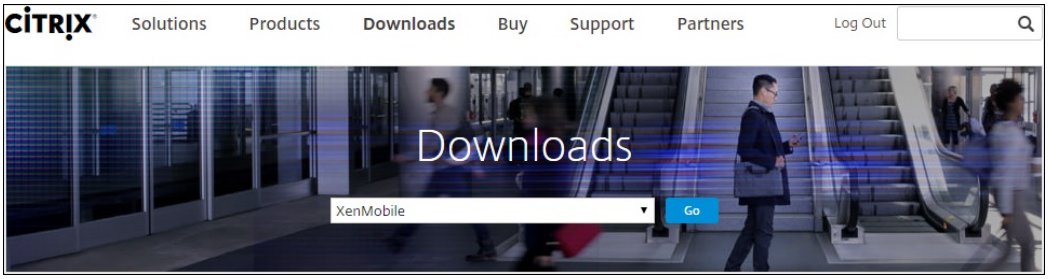
Windows Server 2012 R2 erfordert die zusätzlichen Schritte nicht.

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

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 Anmelden und melden Sie sich an 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 auf Download neben dem entsprechenden virtuellen Image, das zum Installieren von XenMobile unter XenServer, VMware oder Hyper-V verwendet werden soll.
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 an 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.

Die anfängliche Konfiguration von XenMobile ist ein zweiteiliger Prozess.

1. Konfigurieren Sie IP-Adresse, Subnetzmaske, Standardgateway, DNS-Server usw. für XenMobile über die XenCenter-

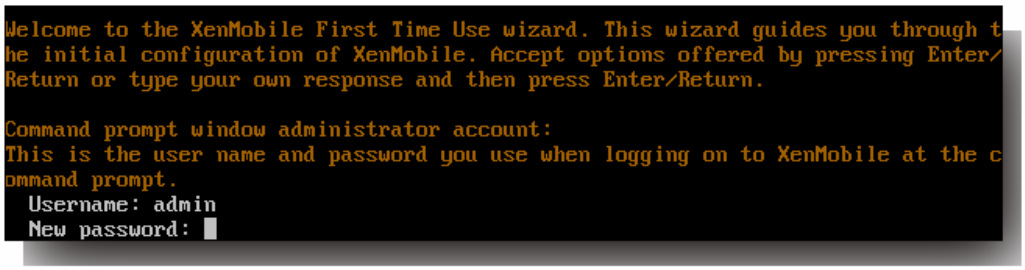
oder vSphere-Befehlszeilenkonsole.

2. Melden Sie sich bei der XenMobile-Verwaltungskonsole an und folgen Sie den Anweisungen der Bildschirme für die Erstanmeldung.

> **Hinweis**
>
> Bei Verwendung eines vSphere-Webclients wird empfohlen, die Netzwerkeigenschaften nicht bei der Bereitstellung der OVF-Vorlage über die Seite **Customize template** 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 Benutzernamen und das Kennwort des Administrators 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 (wie z. B. Sternchen) angezeigt. Es wird nichts angezeigt.

4. Stellen Sie die folgenden Netzwerkinformationen bereit und geben Sie dann y ein, um die Einstellungen zu speichern:
   1. IP-Adresse des XenMobile-Servers
   2. Netzwerkmaske
   3. Standardgateway (IP-Adresse des Standardgateways in der DMZ)
   4. Primärer DNS-Server (IP-Adresse des DNS-Servers)
   5. Sekundärer DNS-Server (optional)

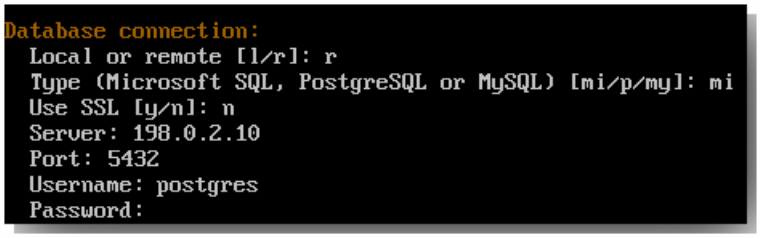
Hinweis: Die hier und in folgenden Abbildungen angezeigten Adressen sind nicht funktionsfähig und dienen nur als Beispiel.

5. Geben Sie y ein, um die Sicherheit zu erhöhen, indem Sie eine zufällige Passphrase zur Verschlüsselung erzeugen, oder n, um Ihre eigene Passphrase anzugeben. Citrix empfiehlt die Eingabe von y 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). Einzelheiten zu FIPS finden Sie unter FIPS. Stellen Sie auch sicher, dass die unter Konfigurieren von FIPS erläuterten Voraussetzungen erfüllt sind.

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

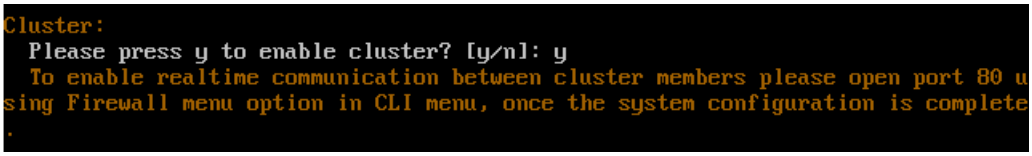


1. Sie können eine lokale oder remote Datenbank verwenden. Geben Sie l für lokal oder r für remote ein.
2. Wählen Sie den Datenbanktyp. Geben Sie mi für Microsoft SQL oder p für PostgreSQL ein.
   Wichtig:
   - Citrix empfiehlt die Remote-Verwendung von Microsoft SQL. PostgreSQL ist Teil von XenMobile 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 Sie y 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 Sie y eingeben, um das Clustering von XenMobile-Knoten oder -Instanzen zu aktivieren.



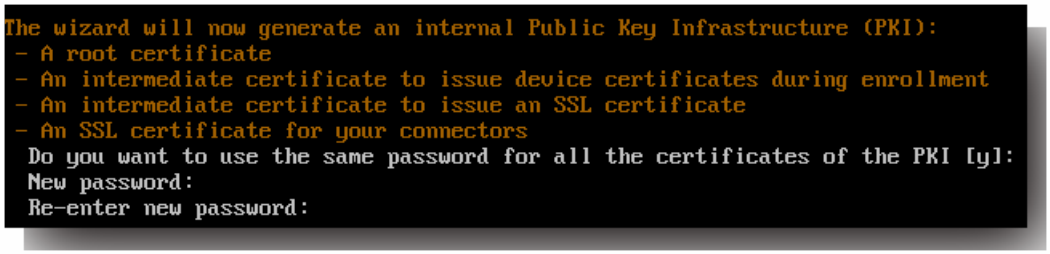
Wichtig: Wenn Sie einen XenMobile-Cluster aktivieren, öffnen Sie nach der Systemkonfiguration Port 80, um die Echtzeitkommunikation zwischen Clustermitgliedern zu aktivieren. Dieser Vorgang muss auf allen Clusterknoten ausgeführt werden.

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.

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. Drücken Sie y, wenn Sie dasselbe Kennwort für alle Public Key-Infrastruktur-Zertifikate verwenden möchten. Informationen zum XenMobile-PKI-Feature finden Sie unter Hochladen von Zertifikaten.



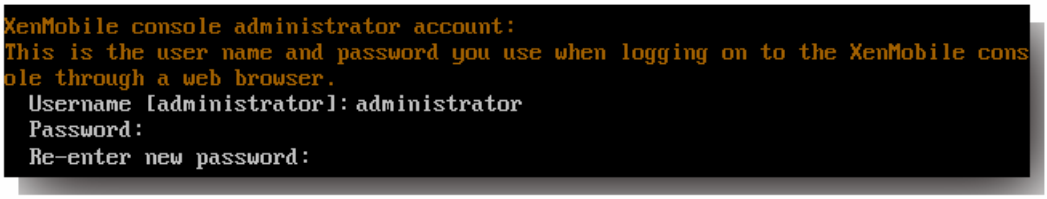
Wichtig: Wenn Sie Knoten oder Instanzen von XenMobile in Clustern verwenden möchten, müssen Sie identische Kennwörter für die nachfolgenden Knoten angeben.

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.

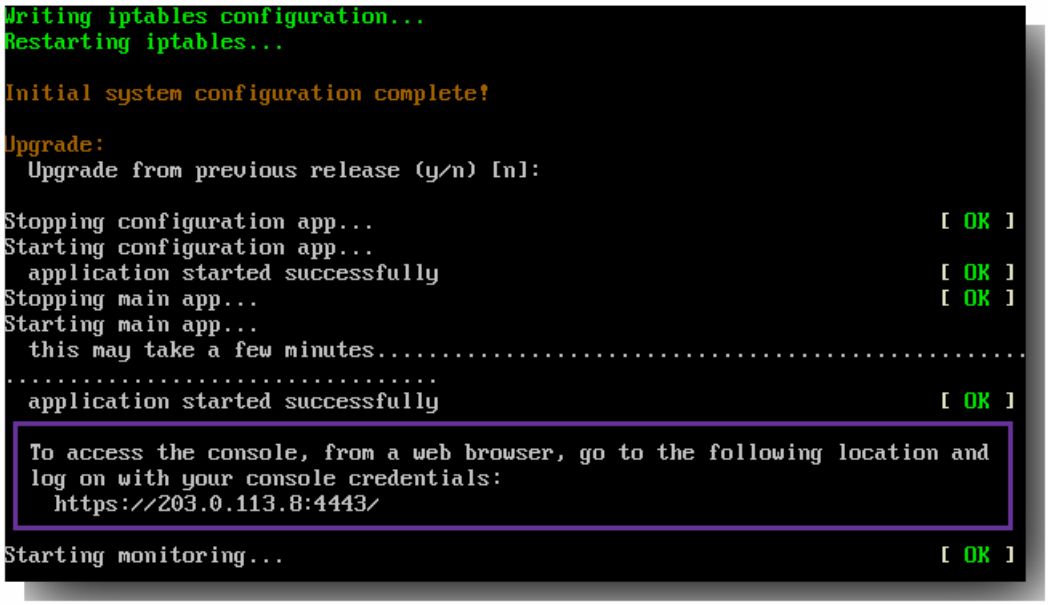


Hinweis: Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt. Es wird nichts angezeigt.

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.

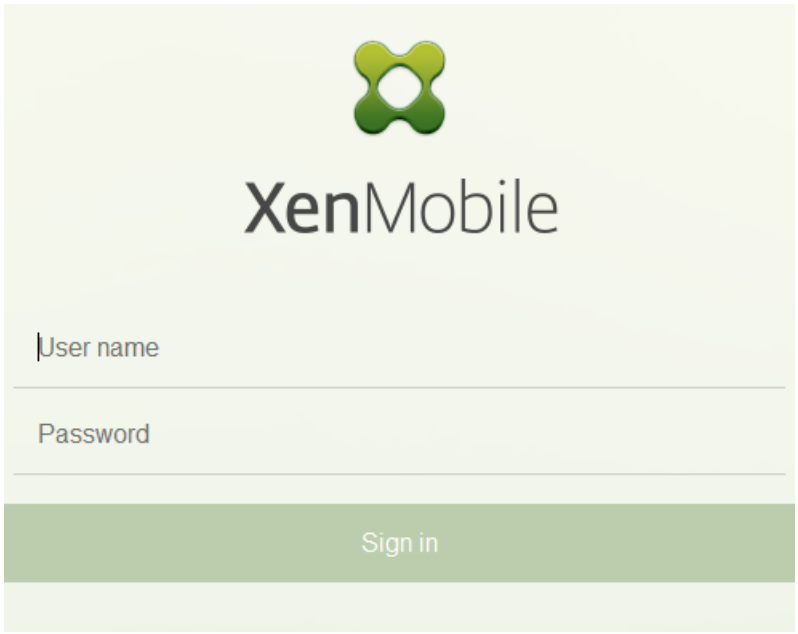
19. Kopieren Sie die vollständige nun angezeigte URL und setzen Sie die Erstkonfiguration von XenMobile in Ihrem Webbrowser fort.



Nach Abschließen des erstens Teils 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 "Erste Schritte" auf Starten. Die Seite "Licensing" wird angezeigt.
4. Konfigurieren Sie die Lizenz.Wenn Sie keine Lizenz hochladen, verwenden Sie eine Evaluierungslizenz für 30 Tage. Informationen zum Hinzufügen und Konfigurieren von Lizenzen und zum Konfigurieren von Ablaufbenachrichtigungen finden Sie unter Lizenzierung.

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 Zertifikat auf Importieren. Das Dialogfeld Importieren wird angezeigt.

6. Importieren Sie das APNs- und SSL Listener-Zertifikat. Wenn Sie iOS-Geräte verwalten, benötigen Sie ein APNs-Zertifikat. Informationen zur Arbeit mit Zertifikaten finden Sie unter Zertifikate.

Hinweis: Dieser Schritt erfordert den Neustart des Servers.
7. Konfigurieren Sie NetScaler Gateway, wenn die Umgebung dies erfordert. Informationen zum Konfigurieren von NetScaler Gateway finden Sie unter NetScaler Gateway und XenMobile und Konfigurieren von Einstellungen für die XenMobile-Umgebung.

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.

Nachbereitung: Starten Sie den XenMobile-Server neu, um die Zertifikate zu aktivieren.

Konfigurieren von FIPS in XenMobile

Feb 24, 2017

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.

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.

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.

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.

Konfigurieren von Clustering

Apr 24, 2017

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.

Der vollqualifizierte Domänenname (FQDN) der virtuellen IP-Adresse des MDM Load Balancers und der virtuellen IP-Adresse des MAM Load Balancers entspricht dem Registrierungs-FQDN, d. h. dem FQDN des XenMobile-Servers.
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

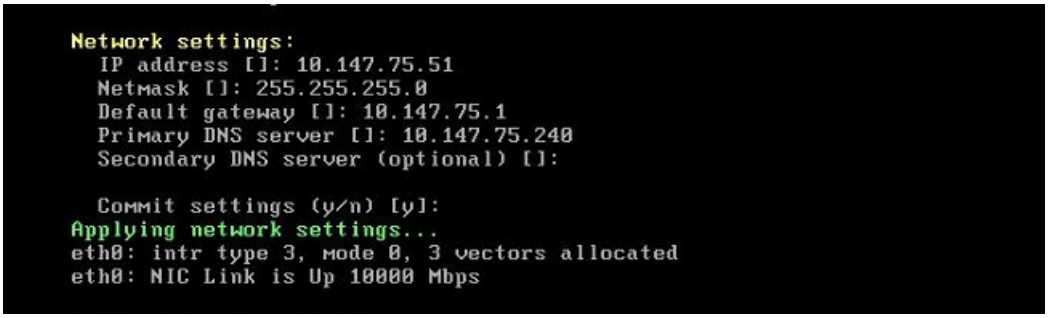
- Sie haben den erforderlichen XenMobile-Knoten vollständig konfiguriert.
- Eine öffentliche IP-Adresse für den MDM Load Balancer.
- Eine private IP-Adresse in einem von RFC 1918 definierten Bereich für den MAM Load Balancer.
- Serverzertifikate
- Sie haben eine freie IP für die virtuelle IP-Adresse von NetScaler.

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

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

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

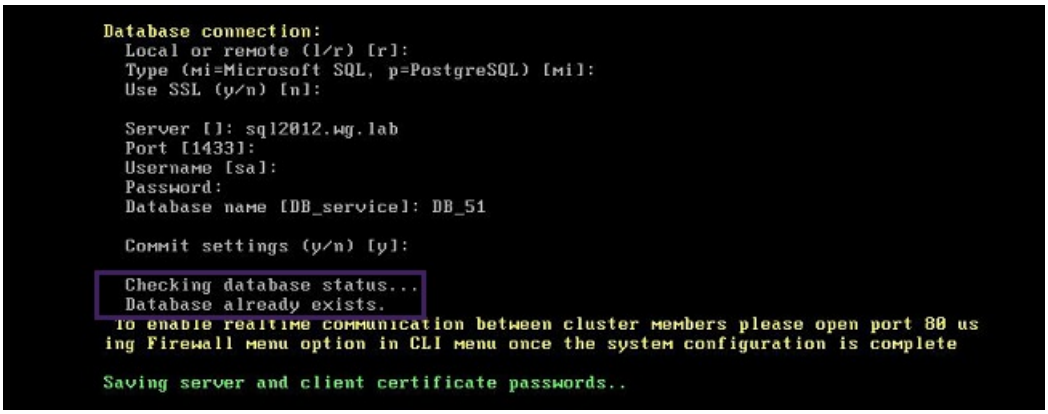
2. Geben Sie die Details der Netzwerkkonfiguration wie in der folgenden Abbildung dargestellt an.



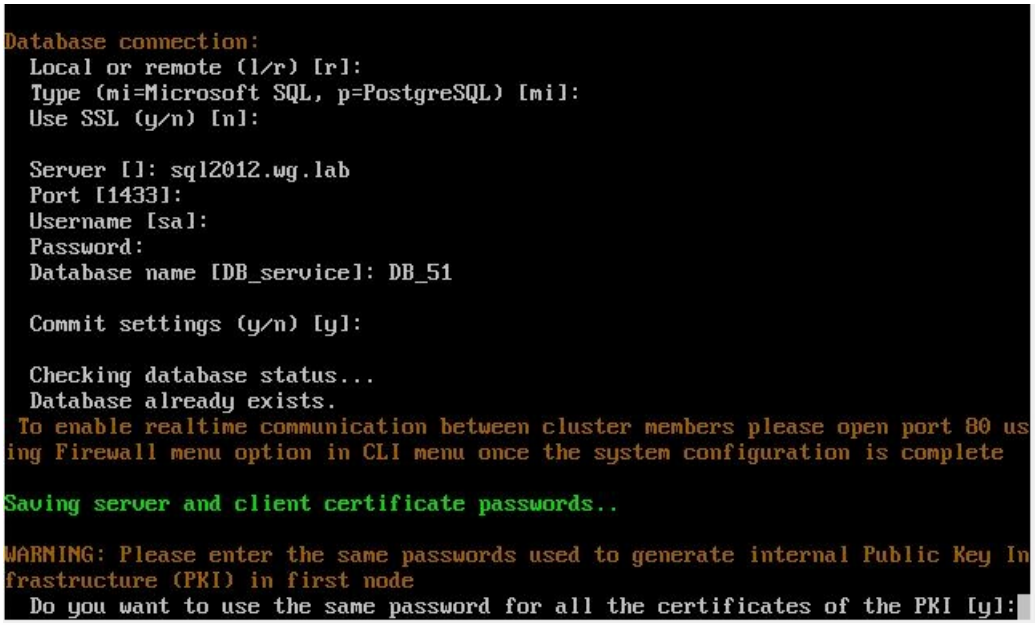
3. Wenn Sie das Standardkennwort für den Schutz von Daten verwenden möchten, geben Sie y ein. Geben Sie andernfalls n und anschließend ein neues Kennwort ein.

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

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.

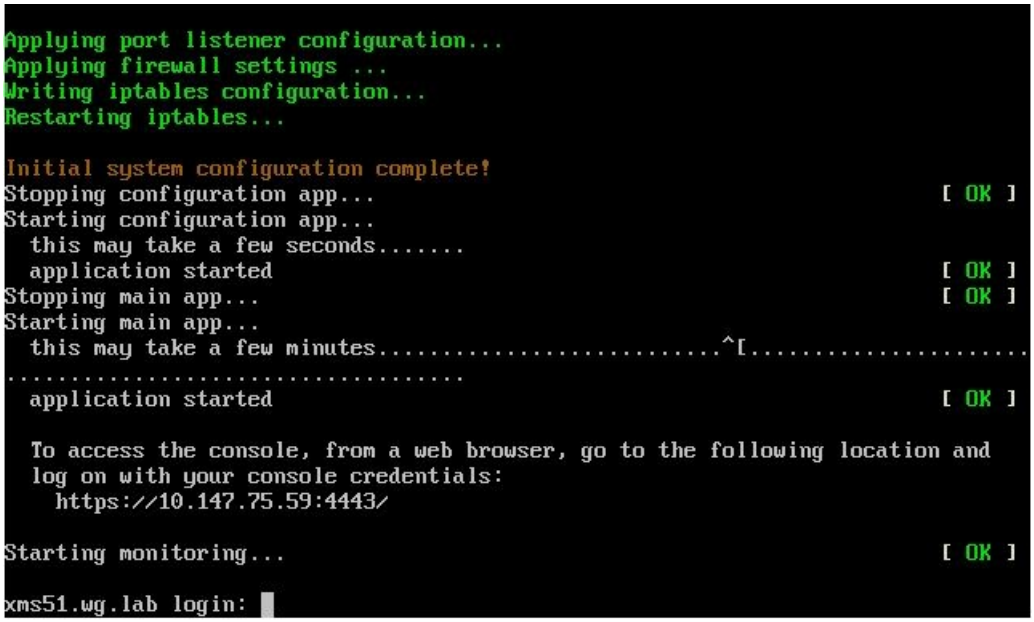


6. Geben Sie die gleichen Kennwörter für die Zertifikate an, wie für die erste VM.



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.



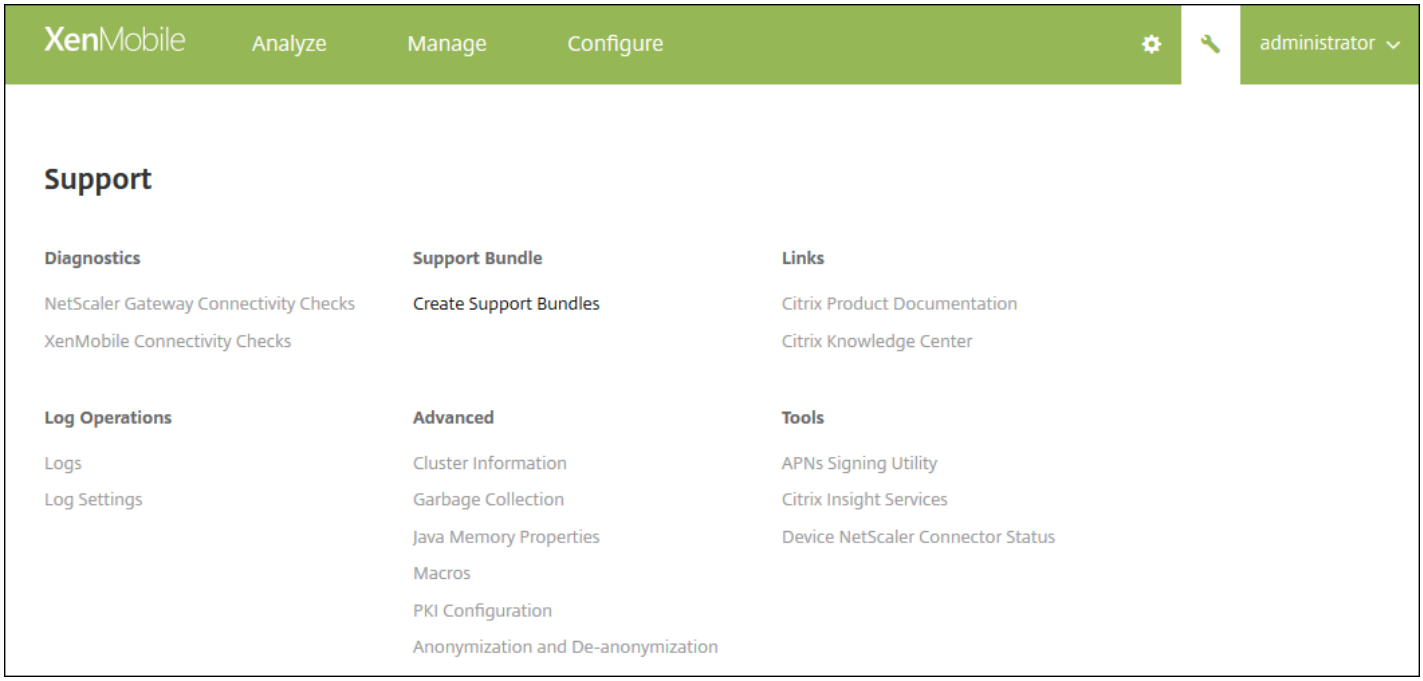
Hinweis: Das Anmeldedialogfeld ist das gleiche wie für die erste VM. Die Übereinstimmung zeigt Ihnen, dass beide VMs den gleichen Datenbankserver verwenden.

8. Verwenden Sie den vollqualifizierten Domänennamen (FQDN) von XenMobile, um die XenMobile-Konsole in einem Webbrowser zu öffnen.

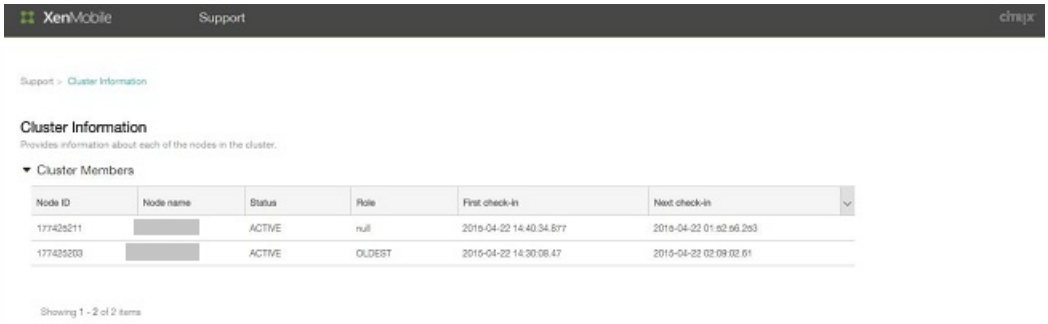
9.Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben.

Die Seite **Support** wird geöffnet.

10. Klicken sie unter **Erweitert** auf **Clusterinformationen**.



Alle Informationen über den Cluster werden angezeigt, einschließlich Informationen zu Clustermitgliedern, Geräteverbindungen, Aufgaben usw. Der neue Knoten gehört nun zu dem Cluster.

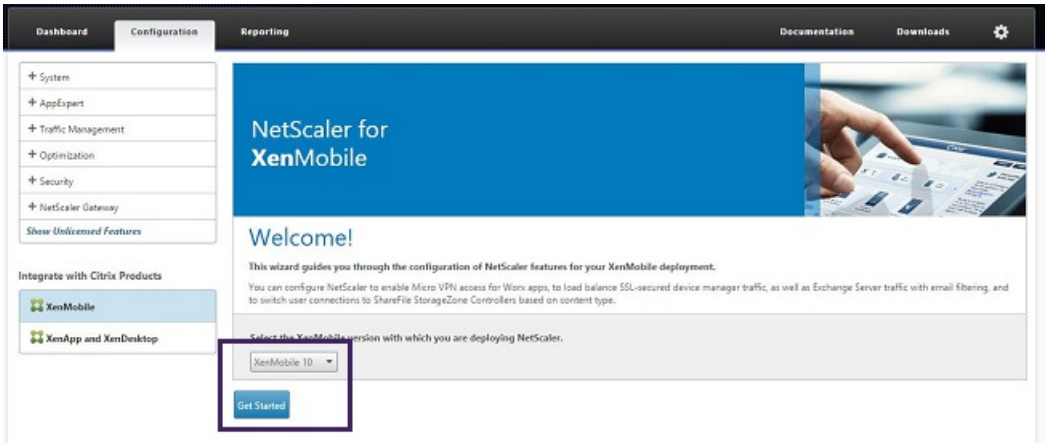


Sie können auf die gleiche Weise noch weitere Knoten hinzufügen. Der erste dem Knoten hinzugefügte Cluster hat die Rolle **OLDEST**. Anschließend hinzugefügte Cluster haben die Rolle **NONE** oder **null**.

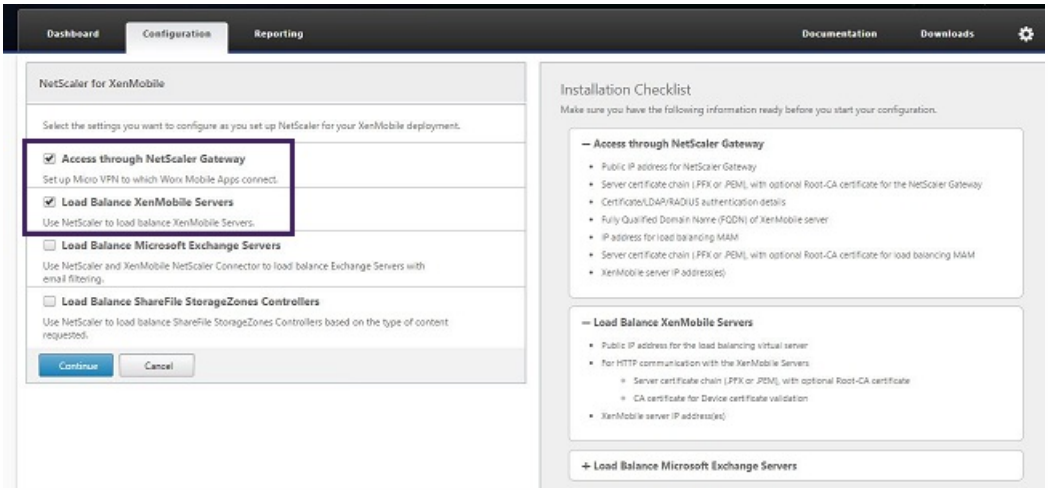
Nachdem Sie die erforderlichen Knoten als Mitglieder des XenMobile-Clusters hinzugefügt haben, müssen Sie für die Knoten den Lastausgleich durchführen, um auf die Cluster zuzugreifen. Der Lastausgleich geschieht, indem Sie den XenMobile-Assistent in NetScaler 10.5.x ausführen. Folgen Sie diesen Schritten,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

1. Melden Sie sich an NetScaler an.

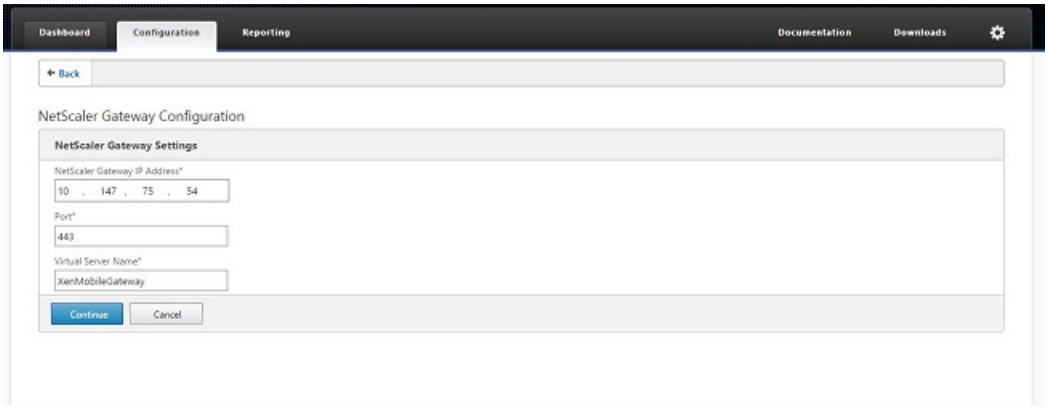
2. Klicken Sie auf der Registerkarte Configuration auf XenMobile und dann auf Get Started.



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

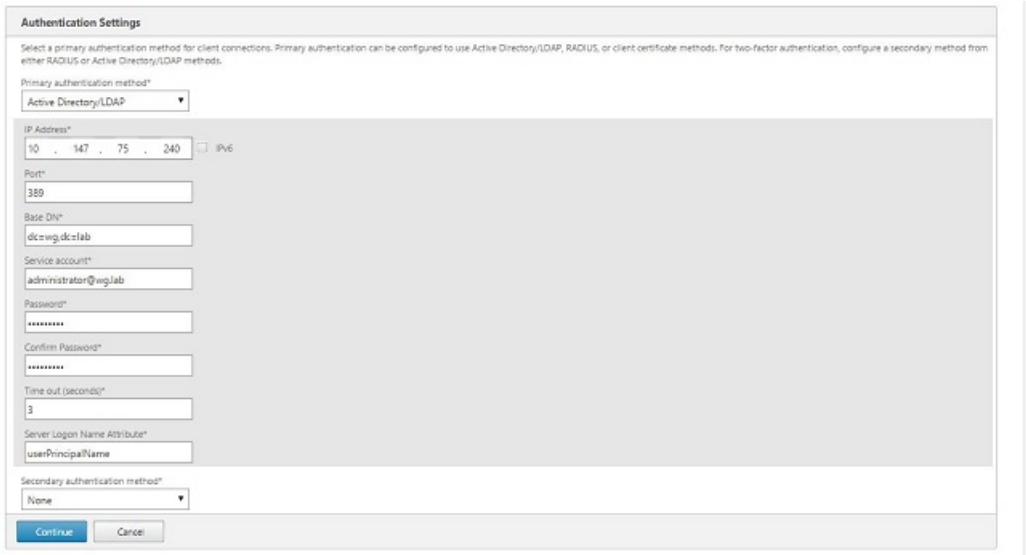


4. Geben Sie die IP-Adresse für NetScaler Gateway ein und klicken Sie auf Continue.



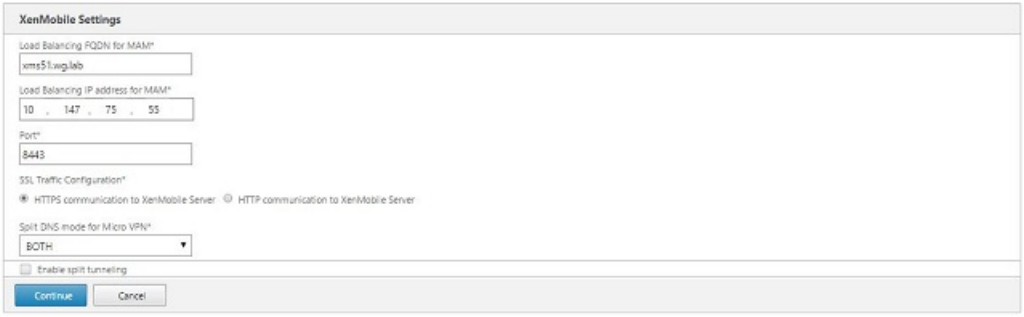
5. Binden Sie mit einer der folgenden Methoden das Serverzertifikat an die virtuelle IP-Adresse von NetScaler Gateway und klicken Sie dann auf Continue.
   - Wählen Sie unter Use existing certificate das Serverzertifikat aus der Liste aus.
   - Klicken Sie auf die Registerkarte Install Certificate, um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

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



   Hinweis: Stellen 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.

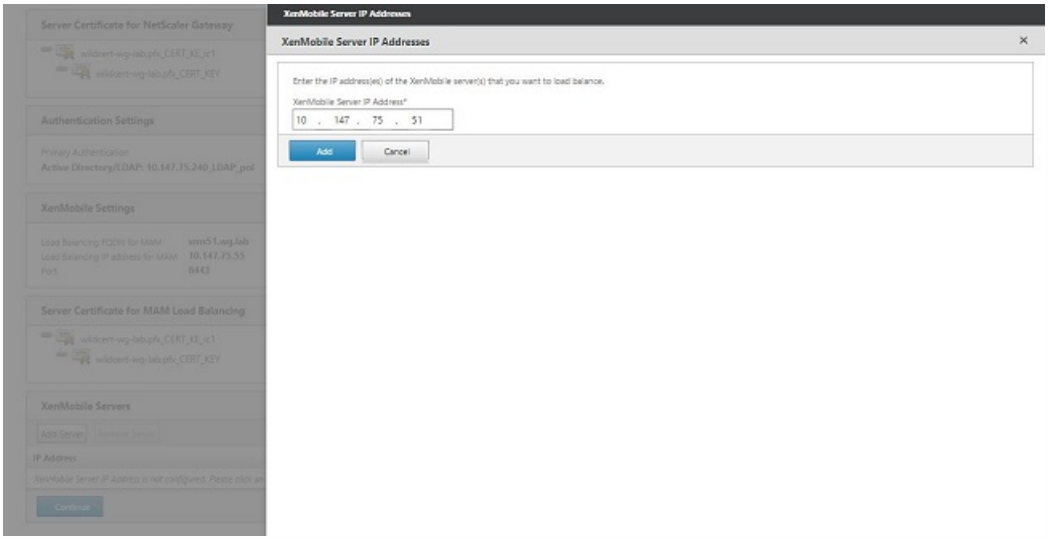


Hinweis: Stellen Sie sicher, dass der vollqualifizierte Domänenname (FQDN) der virtuellen IP-Adresse für den MAM-Lastausgleich und der FQDN von XenMobile gleich sind.

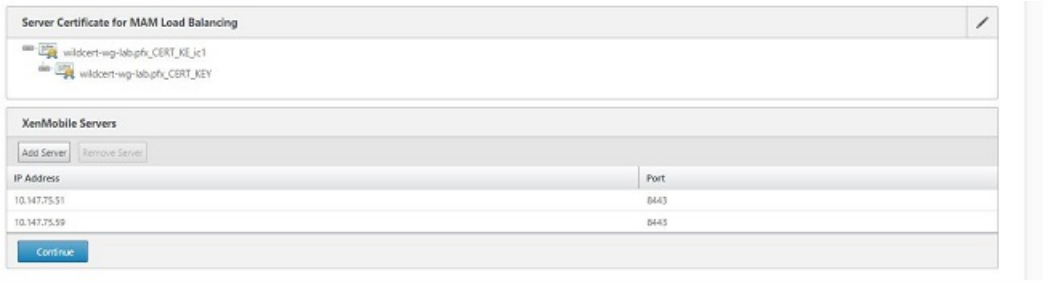
8. Wenn Sie den SSL-Brückenmodus (HTTPS) verwenden möchten, wählen Sie HTTPS communication to XenMobile Server aus. Wenn Sie aber SSL-Offload verwenden möchten, wählen Sie HTTP communication to XenMobile Server aus, wie in der voranstehenden Abbildung dargestellt. Für die Zwecke dieses Artikels nehmen wir SSL-Brückenmodus (HTTPS).
9. Binden Sie das Serverzertifikat für die virtuelle IP-Adresse des MAM-Lastausgleichs und klicken Sie auf Continue.

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

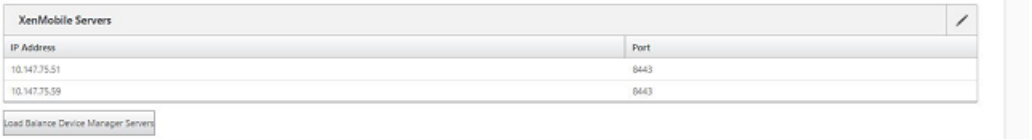
11. Geben Sie die IP-Adresse des XenMobile-Knotens ein und klicken Sie auf Add.



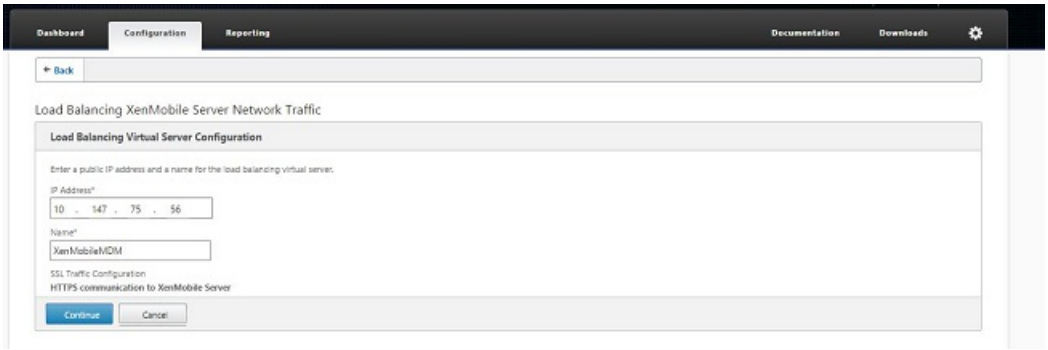
12. Wiederholen Sie die Schritte 10 und 11 , um weitere XenMobile-Knoten hinzuzufügen, die Teil des XenMobile-Clusters sind. Sie sehen dann alle XenMobile-Knoten, die Sie hinzugefügt haben. Klicken Sie auf Continue.



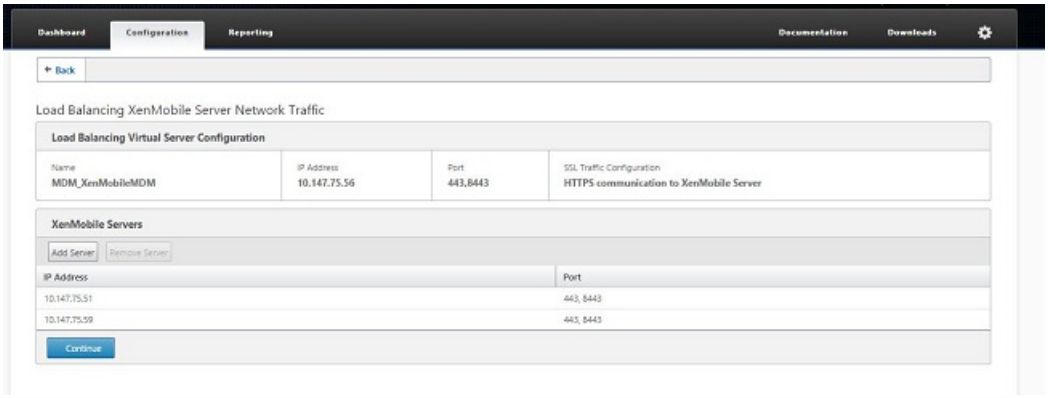
13. Klicken Sie auf Load Balance Device Manager Servers, um mit der Konfiguration des MDM-Lastausgleichs fortzufahren.



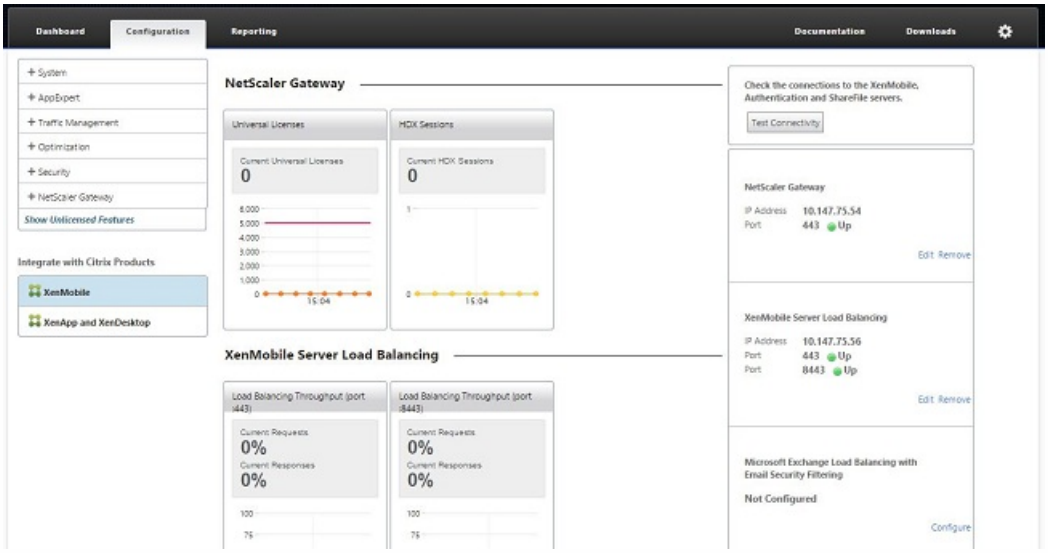
14. Geben Sie die IP-Adresse ein, die für den MDM-Lastausgleich verwendet werden soll und klicken Sie auf Continue.



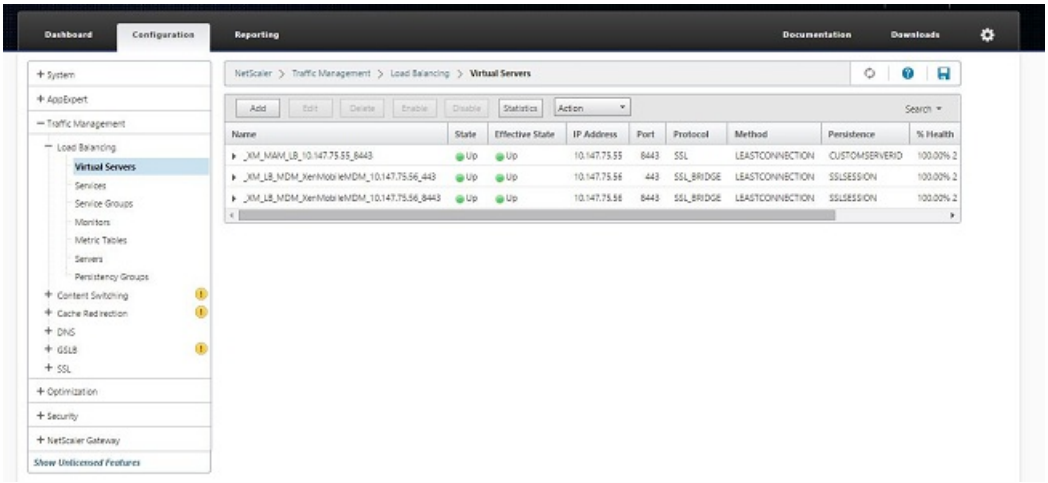
15. Sobald Sie die XenMobile-Knoten in der Liste sehen, klicken Sie auf Continue und dann auf Done, um den Vorgang abzuschließen.



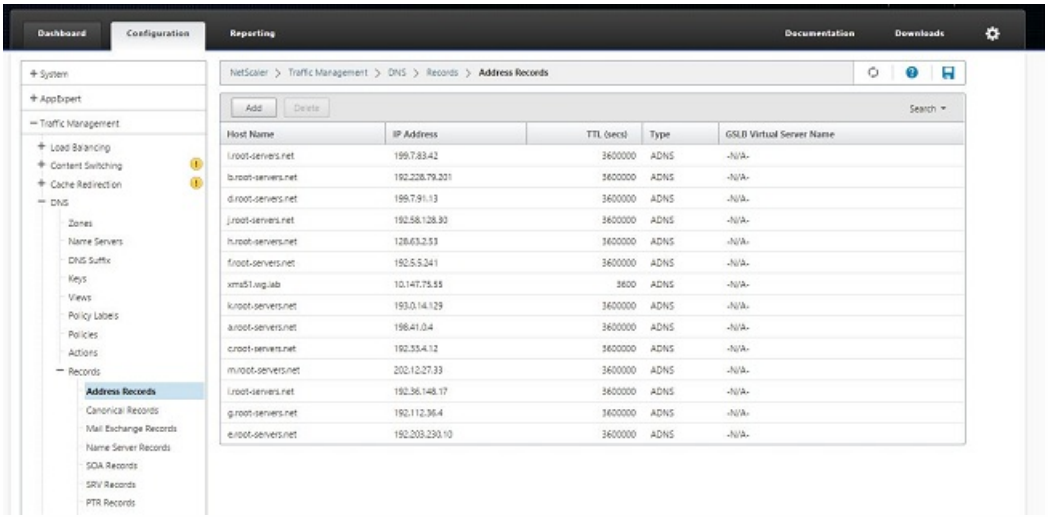
Der Status der virtuellen IP-Adresse wird auf der Seite XenMobile angezeigt.



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.



Leitfaden zur Notfallwiederherstellung

Feb 24, 2017

Sie können XenMobile-Bereitstellungen mit mehreren Sites für die Notfallwiederherstellung und einer Aktiv-Passive-Failoverstrategie einrichten. Weitere Informationen finden Sie im XenMobile-Bereitstellungshandbuch im Artikel Notfallwiederherstellung.

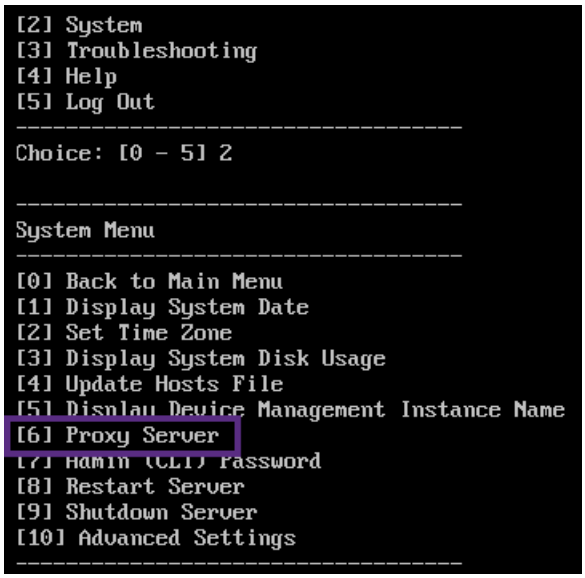
Aktivieren von Proxyservern

Feb 24, 2017

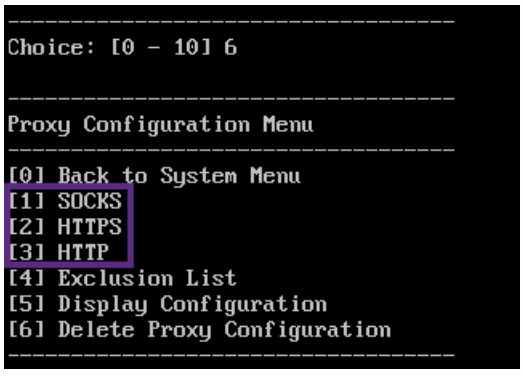
Zum Steuern von ausgehendem Internetverkehr können Sie in XenMobile einen Proxyserver für den Verkehr einrichten. Dazu müssen Sie den Proxyserver über die Befehlszeilenschnittstelle (CLI) einrichten. Zum Einrichten des Proxyservers müssen Sie das System neu starten.

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.



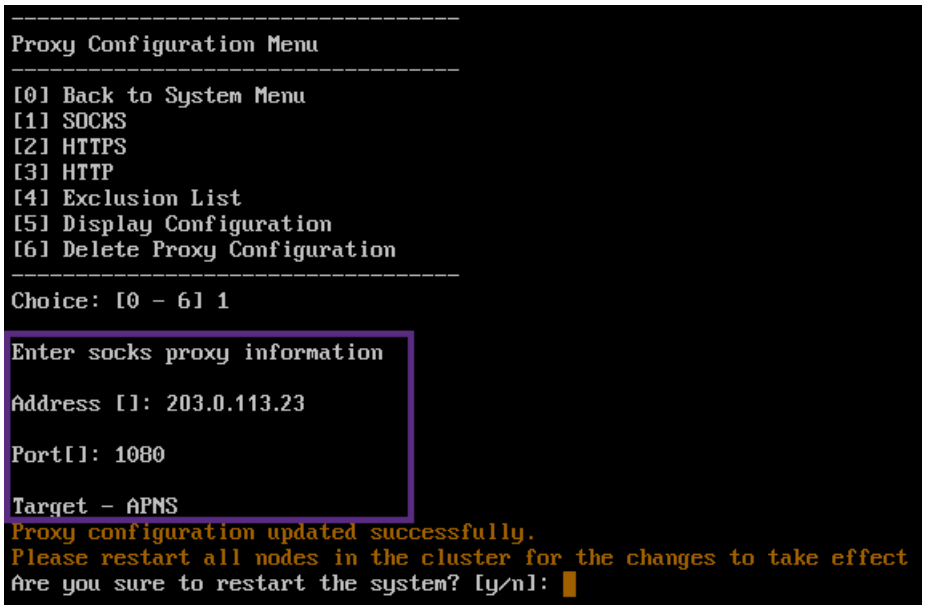
3. Geben Sie im Menü für die Proxykonfiguration **1** für die Auswahl von SOCKS ein, **2** für die Auswahl von HTTPS oder **3** für die Auswahl von HTTP.



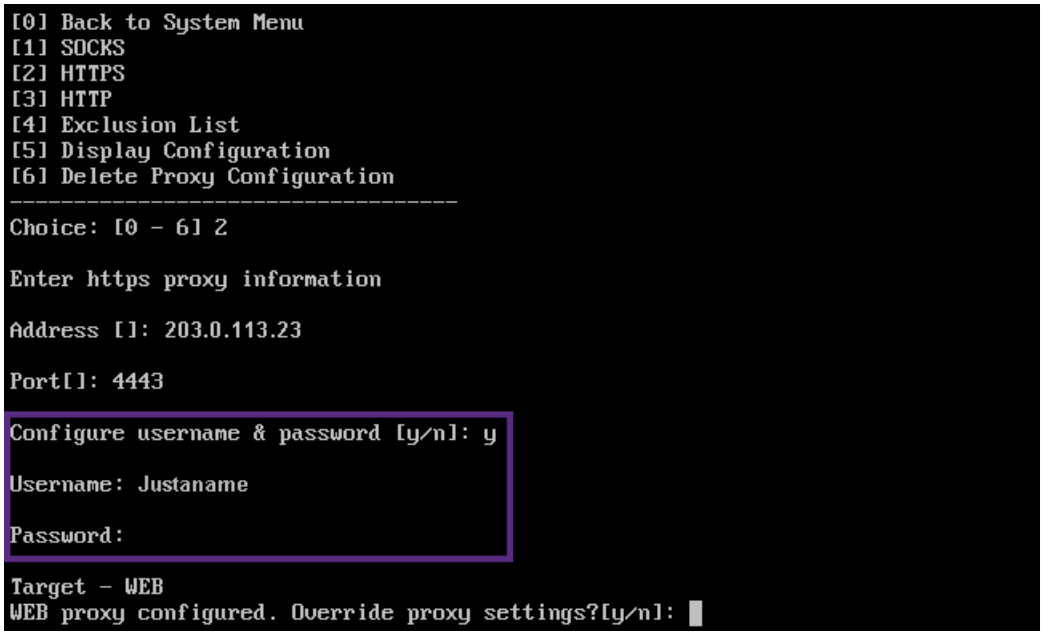
4. Geben Sie IP-Adresse, Portnummer und Ziel des Proxyservers ein. In der folgenden Tabelle sind die für die Proxyservertypen unterstützten Zieltypen aufgeführt.

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.

Servereigenschaften

Apr 24, 2017

XenMobile bietet viele Eigenschaften für serverweite Vorgänge. In diesem Abschnitt werden viele Servereigenschaften und Informationen zum Hinzufügen, Bearbeiten und Löschen von Servereigenschaften erläutert.

Informationen zu den normalerweise konfigurierten Eigenschaften finden Sie unter Servereigenschaften im virtuellen XenMobile-Handbuch.

Servereigenschaften – Definitionen

Add Device Always

Bei Festlegung auf **Wahr** fügt XenMobile der XenMobile-Konsole ein Gerät hinzu, selbst die Registrierung fehlschlägt, sodass Sie sehen können, welche Geräte eine Registrierung versucht haben. Der Standardwert ist **Falsch**.

Audit Log Cleanup Execution Time

Die Startzeit der Auditprotokollbereinigung im Format HH:MM AM/PM. Beispiel: 04:00 AM. Der Standardwert ist **02:00 AM**.

Audit Log Cleanup Interval (in Days)

Die Anzahl der Tage, die der XenMobile-Server das Auditprotokoll aufbewahrt. Der Standardwert ist: **1**.

Audit Logger

Bei Einstellung von **Falsch** werden Benutzeroberflächenereignisse nicht erfasst. Der Standardwert ist **Falsch**.

Audit Log Retention (in Days)

Die Anzahl der Tage, die der XenMobile-Server das Auditprotokoll aufbewahrt. Der Standardwert ist **7**.

Certificate Renewal in Seconds

Der Zeitpunkt in Sekunden vor Ablauf eines Zertifikats, zu dem XenMobile die Verlängerung beginnt. Wenn ein Zertifikat beispielsweise am 30. Dezember abläuft und diese Eigenschaft auf 30 Tage festgelegt ist, versucht XenMobile, das Zertifikat zu verlängern, wenn das Gerät zwischen dem 1. und dem 30. Dezember eine Verbindung herstellt. Der Standardwert ist**2592000** Sekunden (30 Tage).

Connection Timeout to Microsoft Certification Server

Die Zeitdauer in Sekunden, die XenMobile auf eine Antwort vom Zertifikatserver wartet. Wenn der Zertifikatserver langsam ist und einen hohen Netzwerkdatenverkehr erfährt, können Sie dies auf 60 Sekunden oder mehr erhöhen. Ein Zertifikatsserver, der nach 120 Sekunden reagiert, erfordert Wartungsmaßnahmen. Der Standardwert ist **15000** Millisekunden (15 Sekunden).

Deploy Log Cleanup (in Days)

Die Anzahl der Tage, die der XenMobile-Server das Bereitstellungsprotokoll aufbewahrt. Der Standardwert ist **7**.

Disable SSL Server Verification

Bei Einstellung von **Wahr** wird die SSL-Serverzertifikatüberprüfung deaktiviert, wenn die folgenden Bedingungen alle 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 als nicht vertrauenswürdig ansieht. Der Standardwert ist **Wahr**.

Enable Console

Wenn **Wahr** festgelegt ist, wird der Benutzerzugriff auf die Konsole des Selbsthilfeportals aktiviert. Der Standardwert ist **Wahr**.

Enable/Disable Hibernate statistics logging for diagnostics

Bei Einstellung von **Wahr** wird die Protokollierung der Ruhezustandsstatistik zur Unterstützung bei der Behandlung von Anwendungsleistungsproblemen aktiviert. Ruhezustand ist eine Komponente, die für Verbindungen zwischen XenMobile und Microsoft SQL Server verwendet wird. 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. Der Standardwert ist **Falsch**.

Enable Notification Trigger

Aktiviert oder deaktiviert Secure Hub-Clientbenachrichtigungen. Mit **Wahr** werden Benachrichtigungen aktiviert. Der Standardwert ist **Wahr**.

Full Pull of ActiveSync Allowed and Denied Users

Die Zeitdauer in Sekunden, die XenMobile auf eine Antwort von der Domäne wartet, wenn ein PowerShell-Befehl zum Abruf der Basislinie der ActiveSync-Geräte durchgeführt wird. Der Standardwert ist **28800** Sekunden.

Identifies if telemetry is enabled or not

Gibt an, ob Telemetrie (Programm zur Verbesserung der Benutzerfreundlichkeit, CEIP) aktiviert ist. Sie können beim Installieren oder Aktualisieren von XenMobile festlegen, ob Sie am CEIP teilnehmen möchten. Wenn in XenMobile nacheinander 15 Uploads fehlgeschlagen sind, wird die Telemetrie deaktiviert. Der Standardwert ist **Falsch**.

Inactivity Timeout in Minutes

Wenn die Servereigenschaft **Webdienste-Timeouttyp** auf **INACTIVITY_TIMEOUT** festgelegt ist, definiert diese Eigenschaft die Zeitdauer in Minuten, nach welcher XenMobile einen inaktiven Administrator abmeldet, der auf die XenMobile-Konsole über die öffentliche API des XenMobile-Servers oder eine Drittanbieter-App zugegriffen hat. Ein Timeout von **0** bedeutet, dass inaktive Benutzer angemeldet bleiben. Der Standardwert ist **5**.

iOS Device Management Enrollment Auto-Install Enabled

Bei Einstellung auf "Wahr" wird durch diese Eigenschaft die Zahl der Benutzereingriffe bei der Geräteregistrierung gesenkt. Die Benutzer müssen auf die Option zum Installieren der Stammzertifizierungsstelle (falls erforderlich) und auf die Option zum Installieren des MDM-Profils klicken.

iOS Device Management Enrollment First Step Delayed

Diese Eigenschaft gibt an, wie lange bei der Geräteregistrierung nach der Eingabe der Anmeldeinformationen durch den Benutzer gewartet wird, bis die Aufforderung zum Installieren des Stammzertifikats der Zertifizierungsstelle angezeigt wird. Citrix empfiehlt, dass Sie diese Eigenschaft nur bearbeiten, wenn Probleme mit der Netzwerklatenz oder Geschwindigkeit auftreten. Legen Sie in diesem Fall den Wert nicht auf mehr als 5000 Millisekunde (5 Sekunden) fest. Der Standardwert ist **1000** Millisekunden (1 Sekunde).

iOS Device Management Enrollment Last Step Delayed

Diese Eigenschaft gibt an, wie lange bei der Geräteregistrierung nach der Installation des MDM-Profils gewartet wird, bis der Agent auf dem Gerät gestartet wird. Citrix empfiehlt, dass Sie diese Eigenschaft nur bearbeiten, wenn Probleme mit der Netzwerklatenz oder Geschwindigkeit auftreten. Legen Sie in diesem Fall den Wert nicht auf mehr als 5000 Millisekunde (5 Sekunden) fest. Der Standardwert ist **1000** Millisekunden (1 Sekunde).

iOS Device Management Identity Delivery Mode

Gibt an, ob XenMobile das MDM-Zertifikat auf Geräten mit **SCEP** (aus Sicherheitsgründen empfohlen) oder **PKCS12** verteilt. Im PKCS12-Modus wird das Schlüsselpaar auf dem Server generiert und es erfolgt keine Aushandlung. Der Standardwert ist **SCEP**.

iOS Device Management Identity Key Size

Definiert die Länge der privaten Schlüssel für MDM-Identität, iOS-Profildienst und XeMobile-iOS-Agent-Identitäten. Der Standardwert ist **1024**.

iOS Device Management Identity Renewal Days

Der Zeitpunkt in Tagen vor Ablauf des Zertifikats, zu dem XenMobile die Verlängerung beginnt. Beispiel: Wenn ein Zertifikat in 10 Tagen abläuft und diese Eigenschaft auf **10** festgelegt wurde, wird ein neues Zertifikat ausgestellt, wenn ein Gerät eine Verbindung 9 Tage vor dem Ablauf herstellt. Der Standardwert ist **30** Tage.

iOS MDM APNS Private Key Password

Diese Eigenschaft enthält das APNs-Kennwort, das XenMobile zur Übertragung von Pushbenachrichtigungen an den Apple-Server erfordert.

iOS MDM APNS Private Key Password

Diese Eigenschaft enthält das APNs-Kennwort, das XenMobile zur Übertragung von Pushbenachrichtigungen an den Apple-Server erfordert.

MAM_MACRO_SUPPORT

Konfiguriert den XenMobile-Server für Nur-MAM-Bereitstellungen, damit Benutzer, die sich mit einem iOS- oder Android-Gerät bei Secure Hub mit E-Mail-Anmeldeinformationen registrieren, automatisch bei Secure Mail registriert werden. Die Benutzer müssen dann für die Registrierung bei Secure Mail keine weiteren Informationen eingeben und keine zusätzlichen Schritte ausführen. Fügen Sie diesen benutzerdefinierten Schlüssel hinzu und verwenden Sie den Standardwert **Wahr**, um die automatische E-Mail-Registrierung zu aktivieren. Die Clienteigenschaften ENABLE_CREDENTIAL_STORE und SEND_LDAP_ATTRIBUTES sind ebenfalls erforderlich.

Bei der ersten Verwendung von Secure Mail werden die E-Mail-Adresse des Benutzers, die Domäne und die Benutzer-ID von Secure Hub abgerufen. Secure Mail verwendet die E-Mail-Adresse für die Autodiscovery. XenMobile sucht den Exchange Server anhand von Domäne und Benutzer-ID, sodass eine automatische Authentifizierung des Benutzers in

Secure Mail ermöglicht wird. Der Benutzer wird von XenMobile zur Eingabe des Kennworts aufgefordert, wenn die Richtlinie nicht auf Kennwort-Passthrough festgelegt ist, er muss jedoch keine weiteren Informationen eingeben.

NetScaler Single Sign-On

Bei Einstellung von **Falsch** ist das Rückruffeature von XenMobile beim Single Sign-On von NetScaler zum XenMobile-Server deaktiviert. Mit dem Rückruffeature wird von XenMobile die NetScaler Gateway-Sitzungs-ID überprüft, wenn die NetScaler Gateway-Konfiguration eine Rückruf-URL enthält. Der Standardwert ist **Falsch**.

Number of consecutive failed uploads

Zeigt die Anzahl der aufeinander folgenden Fehler beim Upload zum Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) an. XenMobile erhöht den Wert, wenn ein Upload fehlschlägt. Nach 15 Upload-Fehlern deaktiviert XenMobile das CEIP (auch als Telemetrie bezeichnet). Weitere Informationen finden Sie unter der Servereigenschaft **Identifies if telemetry is enabled or not**. XenMobile setzt den Wert auf **0** zurück, wenn ein Upload erfolgreich ist.

Number of Users Per Device

Die maximale Anzahl der Benutzer, die das gleiche Gerät in MDM registrieren können. Der Wert **0** bedeutet, dass eine unbegrenzte Anzahl von Benutzern dasselbe Gerät registrieren kann. Der Standardwert ist **0**.

Pull of Incremental Change of Allowed and Denied Users

Die Zeitdauer in Sekunden, die XenMobile auf eine Antwort von der Domäne wartet, wenn ein PowerShell-Befehl zum Abruf des Deltas der ActiveSync-Geräte durchgeführt wird. Der Standardwert ist **60** Sekunden.

Read Timeout to Microsoft Certification Server

Die Zeitdauer in Sekunden, die XenMobile beim Lesen auf eine Antwort vom Zertifikatserver wartet. Wenn der Zertifikatserver langsam ist und einen hohen Netzwerkdatenverkehr erfährt, können Sie dies auf 60 Sekunden oder mehr erhöhen. Ein Zertifikatsserver, der nach 120 Sekunden reagiert, erfordert Wartungsmaßnahmen. Der Standardwert ist **15000** Millisekunden (15 Sekunden).

REST Web Services

Aktiviert oder deaktiviert den REST-Webdienst. Der Standardwert ist **Wahr**.

Session Log Cleanup (in Days)

Die Anzahl der Tage, die der XenMobile-Server das Sitzungsprotokoll aufbewahrt. Der Standardwert ist **7**.

Server Mode

Legt fest, ob XenMobile im MAM-Modus (App-Verwaltung), MDM-Modus (Geräteverwaltung) oder ENT(Enterprise)-Modus (Verwaltung von Apps und Geräten) ausgeführt 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.

Wenn Sie eine Lizenz für die XenMobile MDM Edition haben, ist der effektive Servermodus immer auf MDM festgelegt, unabhängig von der Einstellung für den Servermodus unter "Server Properties". Wenn Sie eine Lizenz für die MDM Edition haben, wird durch Festlegen des Servermodus auf MAM oder ENT die Anwendungsverwaltung nicht

aktiviert.

Ihre Lizenzen sind für Edition	Geräte in diesem Modus registrieren	Servermodus festlegen auf
Enterprise / Advanced	MDM-Modus	MDM
Enterprise / Advanced	MDM+MAM-Modus	ENT
MDM	MDM-Modus	MDM

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. Bei Enterprise- und Advanced-Lizenzen entspricht der effektive Servermodus dem eingestellten Servermodus (**ENT** oder **MDM**). Wenn der Servermodus **MAM** ist, ist der effektive Servermodus "ENT".

Der Servermodus wird dem Serverprotokoll jedes Mal hinzugefügt, wenn eine Lizenz aktiviert oder gelöscht wird und wenn Sie den Servermodus unter "Servereigenschaften" ändern. Informationen zum Erstellen und Anzeigen von Protokolldateien finden Sie unter Protokolle und Anzeigen und Analysieren von Protokolldateien in XenMobile.

Static Timeout in Minutes

Wenn die Servereigenschaft **Webdienste-Timeouttyp** auf **STATIC_TIMEOUT** festgelegt ist, definiert diese Eigenschaft die Zeitdauer in Minuten, nach welcher XenMobile einen Administrator abmeldet, der auf die XenMobile-Konsole über die öffentliche API des XenMobile-Servers oder eine Drittanbieter-App zugegriffen hat. Der Standardwert ist **60**.

Trigger Agent Message Suppression

Aktiviert oder deaktiviert Secure Hub-Clientmeldungen. Der Wert **Falsch** aktiviert die Meldungen. Der Standardwert ist **Wahr**.

Trigger Agent Sound Suppression

Aktiviert oder deaktiviert Secure Hub-Clienttöne. Der Wert **Falsch** aktiviert die Töne. Der Standardwert ist **Wahr**.

Unauthenticated App Download for Android Devices

Bei Einstellung 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 das Authentifizierungstoken enthält. Der Standardwert ist **Falsch**.

Unauthenticated App Download for Windows Devices

Wird nur für ältere Versionen von Secure Hub verwendet, die Einmaltickets nicht validieren. Bei Einstellung von **Falsch** können Sie nicht authentifizierte Apps von XenMobile auf Windows-Geräte herunterladen. Der Standardwert ist **Falsch**.

Use ActiveSync ID to Conduct an ActiveSync Wipe Device

Bei Einstellung von **Wahr** verwendet XenMobile Mail Manager die ActiveSync-ID als Argument für die asWipeDevice-Methode. Der Standardwert ist **Falsch**.

Users only from Exchange

Wenn **Wahr** festgelegt ist, wird die Benutzerauthentifizierung für ActiveSync Exchange-Benutzer deaktiviert. Der Standardwert ist **Falsch**.

WebServices Timeout Type

Gibt an, wie ein von der öffentlichen API abgerufenes Authentifizierungstoken abläuft. Bei Einstellung auf **STATIC_TIMEOUT** behandelt XenMobile ein Authentifizierungstoken als abgelaufen, wenn der über die Servereigenschaft **Statisches Timeout in Minuten** festgelegte Zeitraum verstrichen ist.

Bei Einstellung auf **INACTIVITY_TIMEOUT** behandelt XenMobile ein Authentifizierungstoken als abgelaufen, wenn der über die Servereigenschaft **Inaktivitätstimeout in Minuten** festgelegte Zeitraum verstrichen ist. Der Standardwert ist **STATIC_TIMEOUT**.

XAM One-Time Ticket

Gültigkeitsdauer eines Tokens für die einmalige Authentifizierung (OTT) zum Download einer App in Millisekunden. 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. Der Standardwert ist **3600000**.

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

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. Der Standardwert ist **30**.

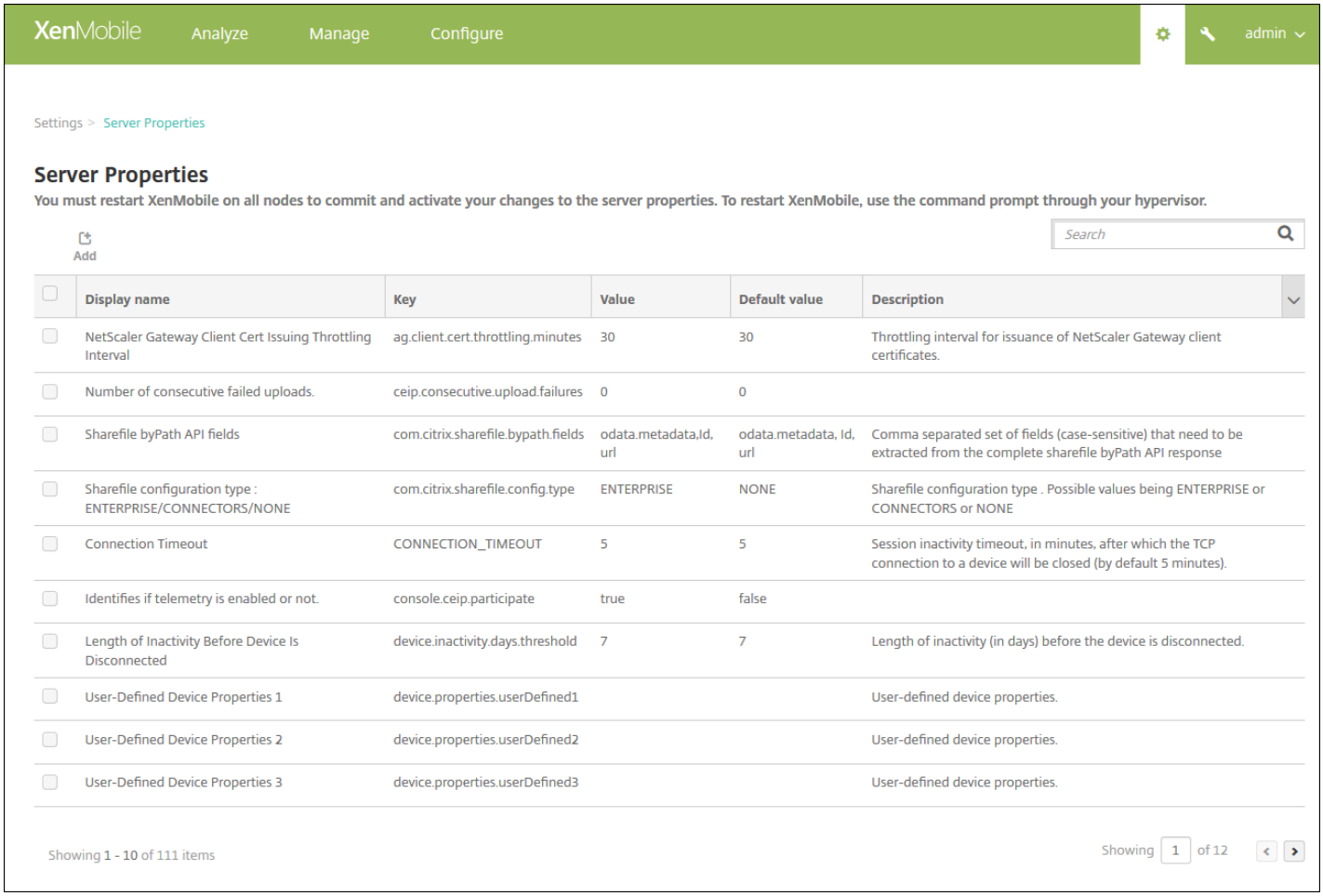
Hinzufügen, Bearbeiten oder Löschen von Servereigenschaften

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.

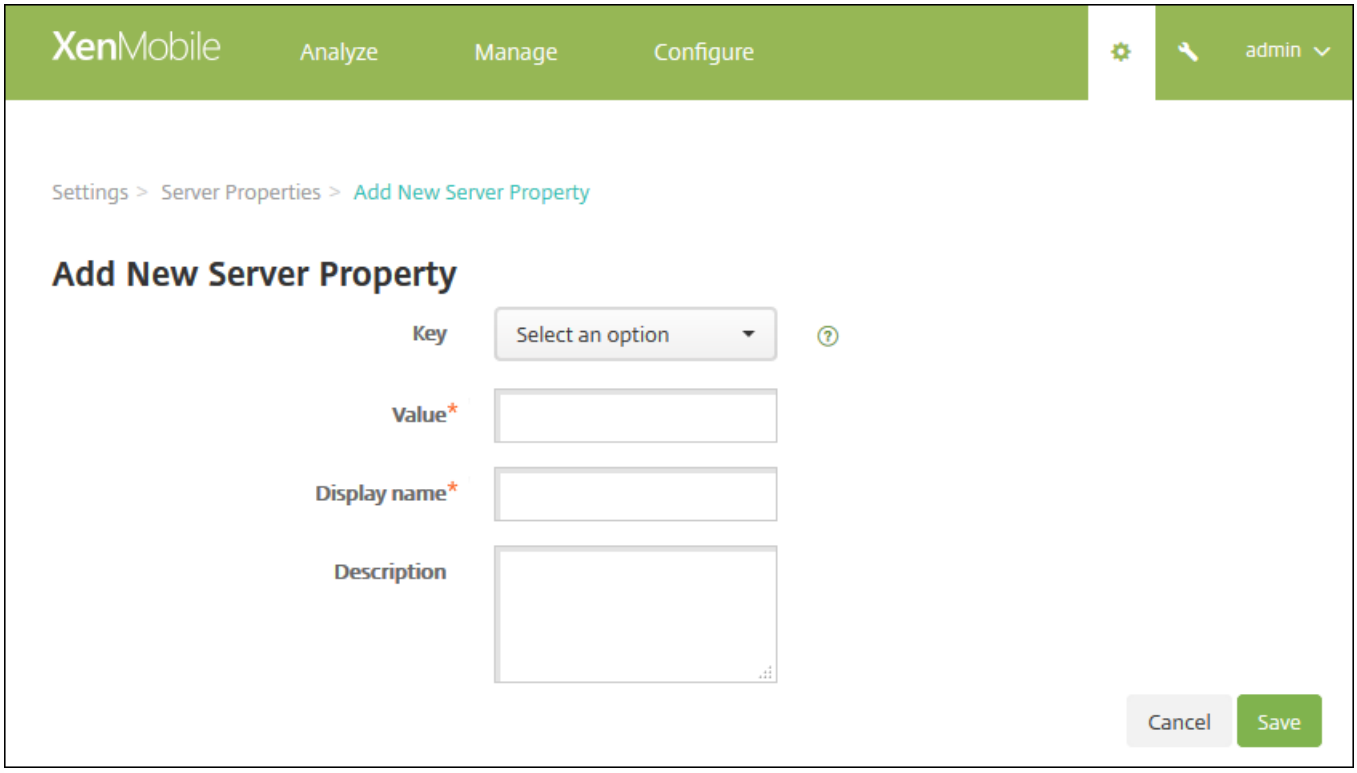
> **Hinweis**
>
> Zum Neustarten von XenMobile verwenden Sie die Eingabeaufforderung durch den Hypervisor.

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.



1. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Servereigenschaft hinzufügen** wird angezeigt.



2. Konfigurieren Sie folgende Einstellungen:

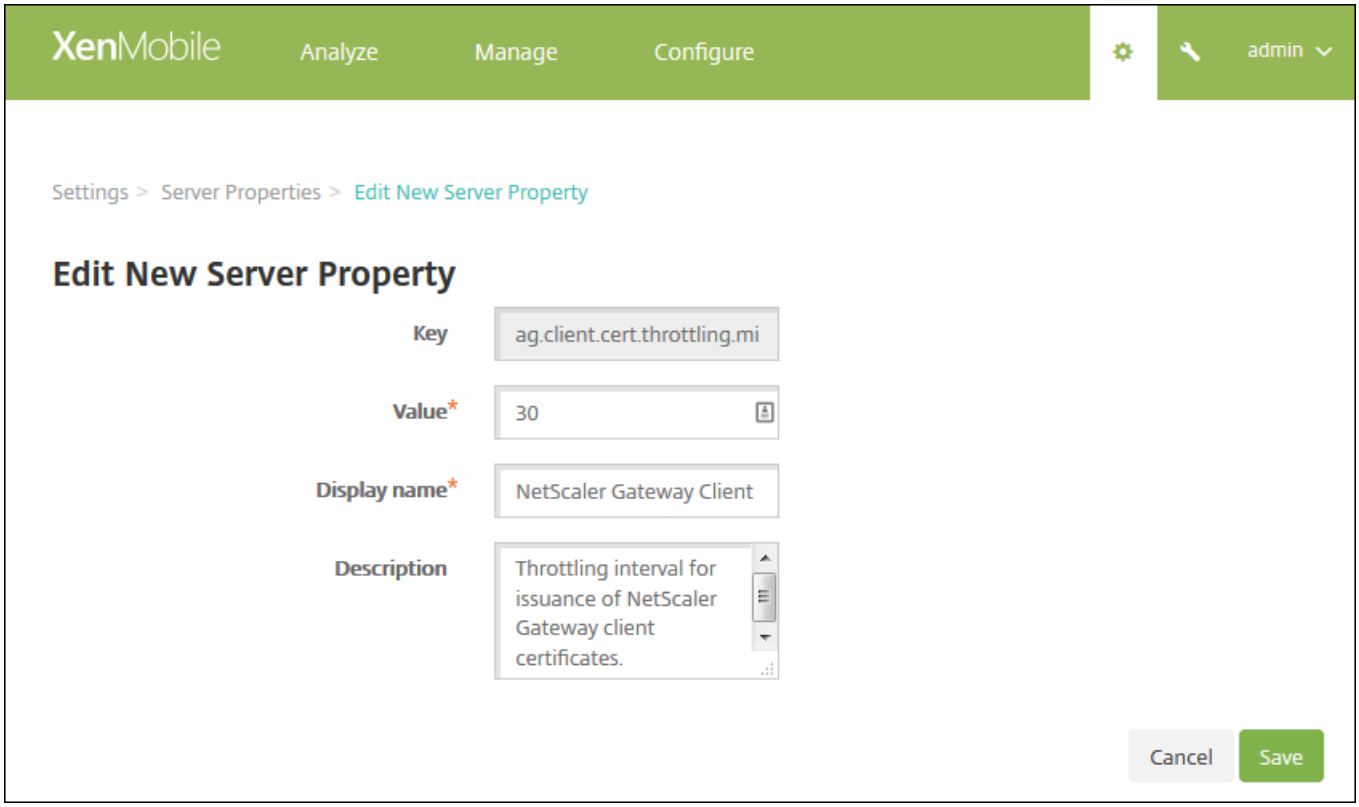
- **Schlüssel**: Wählen Sie in der Liste den geeigneten Schlüssel aus. Bei Schlüsseln wird Groß- und Kleinschreibung unterschieden. Bevor Sie Änderungen vornehmen, müssen Sie sich an den Citrix Support wenden oder einen speziellen Schlüssel anfordern.
- **Wert**: Geben Sie je nach ausgewähltem Schlüssel einen Wert ein.
- **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**.

1. Wählen Sie in der Tabelle **Servereigenschaften** die zu bearbeitende Servereigenschaft 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 einen anderen Eintrag in der Liste klicken, wird das Menü 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**: Der Wert der Eigenschaft.
- **Anzeigename**: Der Name der Eigenschaft.
- **Beschreibung**: Die Beschreibung der Eigenschaft.

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

1. Wählen Sie in der Tabelle **Servereigenschaften** die zu löschende Servereigenschaft aus.

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

2. Klicken Sie auf **Löschen**.Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie erneut auf **Löschen**.

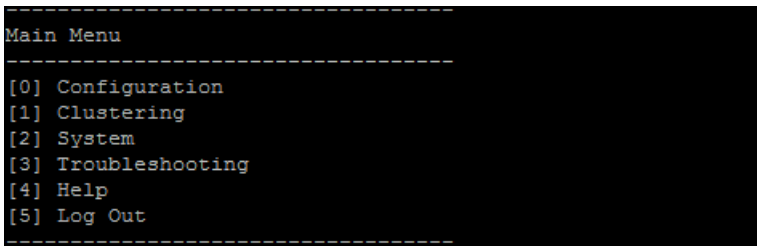
Optionen für die Befehlszeilenschnittstelle

Feb 24, 2017

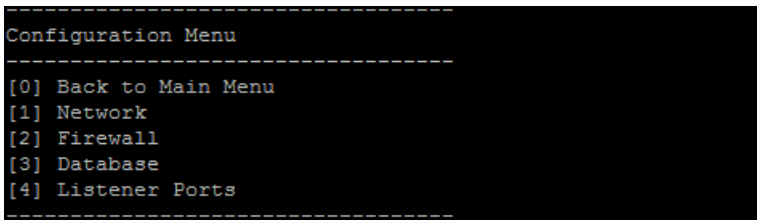
Sie können jederzeit wie folgt auf die Optionen der Befehlszeilenschnittstelle (CLI) zugreifen:

- Auf dem Hypervisor, auf dem Sie XenMobile installiert haben (Citrix XenServer, Microsoft Hyper-V oder VMware ESXi). Wählen Sie im Hypervisor die importierte XenMobile-VM, rufen Sie das Eingabeaufforderungsfenster auf und melden Sie sich mit Ihrem Administratorkonto für XenMobile an. Informationen hierzu finden Sie in der Dokumentation zum Hypervisor.
- Mit SSH, falls SSH in der Firewall aktiviert ist. Melden Sie sich bei Ihrem XenMobile-Administratorkonto an.

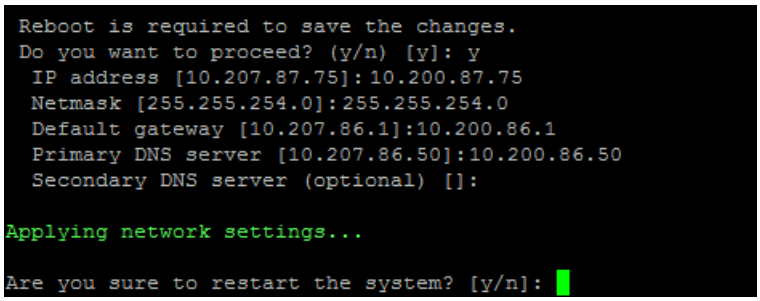
Mit der CLI können Sie eine Reihe von Aufgaben zur Konfiguration und Problembehandlung durchführen. Nachfolgend sehen Sie das Hauptmenü der CLI.



Nachfolgend werden Beispiele für das Menü **Configuration** und die Einstellungen der Optionen aufgeführt.



[1] Network



[2] Firewall

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction
 - enter c as value to clear list

  HTTP service
    Port: 80
    Enable access (y/n) [y]: y
    Access white list []:

  Management HTTPS service
    Port: 4443
    Enable access (y/n) [y]:
    Access white list []:

  SSH service
    Port [22]:
    Enable access (y/n) [y]:
    Access white list []:

  Management API (for initial staging) HTTPS service
    Port [30001]:
    Enable access (y/n) [n]:

  Remote support tunnel
    Port [8081]:
    Enable access (y/n) [n]:

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

[3] Database

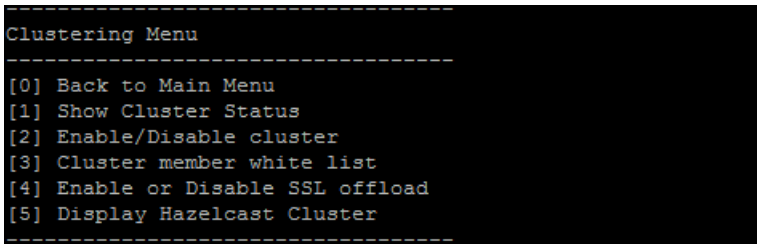
```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```

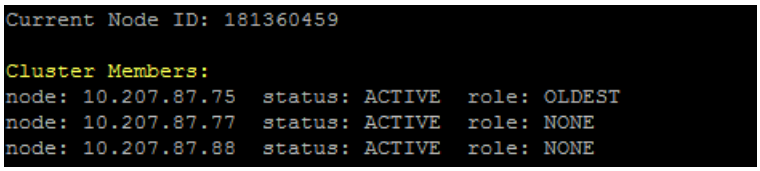
[4] Listener Ports

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]:
```

Nachfolgend werden Beispiele für das Menü **Clustering** und die Einstellungen der Optionen aufgeführt.



[1] Show Cluster Status



[2] Enable/Disable cluster

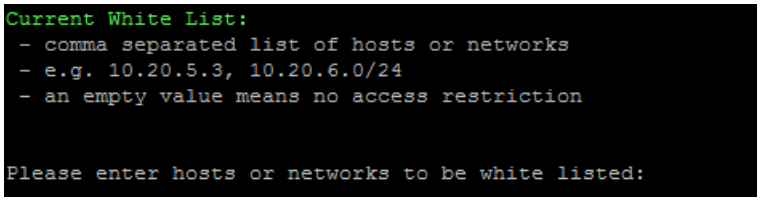
Wenn Sie das Clustering aktivieren, wird die folgende Meldung angezeigt:

> 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.

[3] Cluster member white list



[4] Enable or disable SSL offload

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.

[5] Display Hazelcast Cluster

Wenn Sie Option [5] zum Anzeigen der Hazelcast-Cluster auswählen, werden die folgenden Optionen angezeigt:

> Hazlecast Cluster Members:
>
> [IP addresses listed]
>
> NOTE: If a configured node is not part of the cluster, please reboot that node.

Über das Menü **System** können Sie verschiedene Informationen auf Systemebene anzeigen, den Server neu starten oder herunterfahren und auf erweiterte Einstellungen zugreifen.

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

[12] Advanced Settings

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

****************************************************

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

Unter **Server Tuning** können Sie das Serververbindungstimeout, maximale Verbindungen pro Port und maximale Threads pro Port festlegen.

Nachfolgend werden Beispiele für das Menü **Troubleshooting** und die Einstellungen der Optionen aufgeführt.

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

[1] Network Utilities

```
----------------------------------
Network Menu
----------------------------------
[0] Back to Troubleshooting Menu
[1] Network Information
[2] Show Routing Table
[3] Show Address Resolution Protocol (ARP) Table
[4] PING
[5] Traceroute
[6] DNS Lookup
[7] Network Trace
----------------------------------
```

[2] Logs

```
----------------------------------
Logs Menu
----------------------------------
[0] Back to Troubleshooting Menu
[1] Display Log File
----------------------------------
```

[3] Support Bundle

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

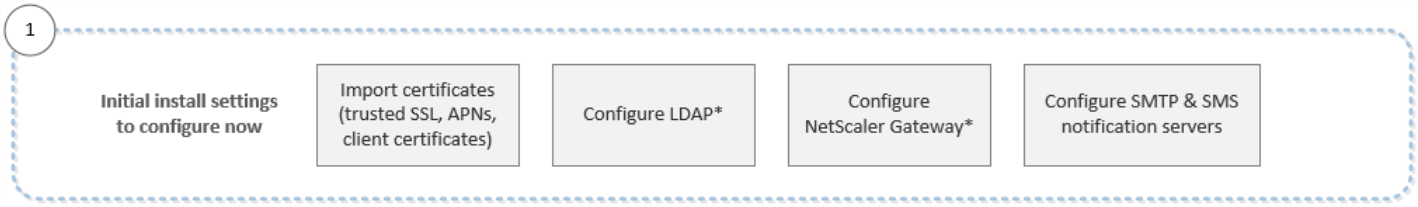
Workflows für erste Schritte mit der XenMobile-Konsole

Feb 24, 2017

Die XenMobile-Konsole ist das zentrale Verwaltungstool in XenMobile. In diesem Artikel wird vorausgesetzt, dass Sie XenMobile installiert haben und für die Arbeit mit der Konsole bereit sind. Informationen zur Installation von XenMobile finden Sie unter Installieren von XenMobile. Einzelheiten zur Browserunterstützung der XenMobile-Konsole finden Sie unter Browserunterstützung im Artikel zur XenMobile-Kompatibilität.

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.

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:

- Authentifizierung
- NetScaler Gateway und XenMobile
- Benachrichtigungen

Zur Unterstützung von Android-, iOS- und Windows-Plattformen müssen Sie die folgenden kontospezifischen Einstellungen haben.

Android

- Erstellen Sie Google Play-Anmeldeinformationen. Informationen finden Sie unter Get Started with Publishing.
- Erstellen Sie ein Android for Work-Konto. Weitere Informationen finden Sie unter Android for Work.
- 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. Weitere Informationen finden Sie in der Hilfe für Android for Work.

iOS

- Erstellen Sie eine Apple-ID und ein Developer-Konto. Informationen finden Sie unter Apple Developer Program.
- Erstellen Sie ein APNs-Zertifikat. Sie benötigen ein Apple APNs-Zertifikats, wenn Sie iOS-Geräte mit der XenMobile

Service (Cloud)-Bereitstellung verwalten und Push-Benachrichtigungen für die WorxMail-Bereitstellung verwenden möchten. Informationen zur Beschaffung von APNs-Zertifikaten finden Sie im Apple Push Certificates Portal. Weitere Informationen zu XenMobile und APNs finden Sie unter APNs-Zertifikate und Pushbenachrichtigungen für WorxMail für iOS.

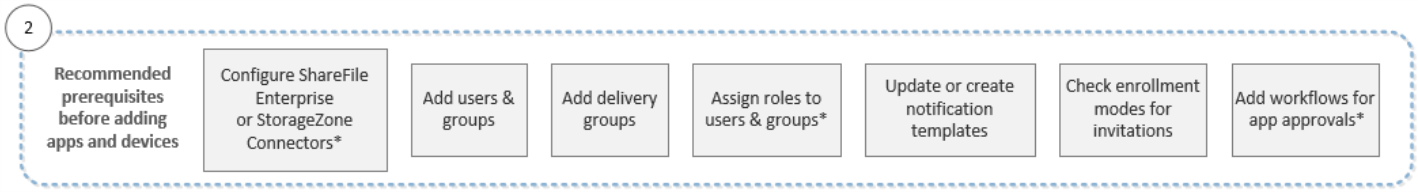
- Erstellen Sie ein Unternehmenstoken für das Programm für Volumenlizenzen. Informationen finden Sie unter Apple Volume Purchasing Program.

Windows

- Erstellen Sie ein Entwicklerkonto für den Microsoft Windows-Store. Informationen finden Sie im Microsoft Dev Center.
- Beschaffen Sie eine Herausgeber-ID für den Microsoft Windows-Store. Informationen finden Sie im Microsoft Dev Center.
- Beschaffen Sie ein Unternehmenszertifikat von Symantec. Informationen finden Sie im Microsoft Dev Center.
- Stellen Sie sicher, dass Sie ein öffentliches SSL-Zertifikat zur Verfügung haben, wenn Sie XenMobile-Autodiscovery für die Registrierung von Windows Phone-Geräten verwenden möchten. Weitere Informationen finden Sie unter XenMobile Autodiscovery-Dienst.
- Erstellen Sie ein Anwendungsregistrierungstoken (AET). Informationen finden Sie im Microsoft Dev Center.

Der Workflow zeigt Voraussetzungen, deren Konfiguration vor dem Hinzufügen von Apps und Geräten empfohlen wird.

Hinweis: Die mit einem Sternchen gekennzeichneten Elemente sind optional.

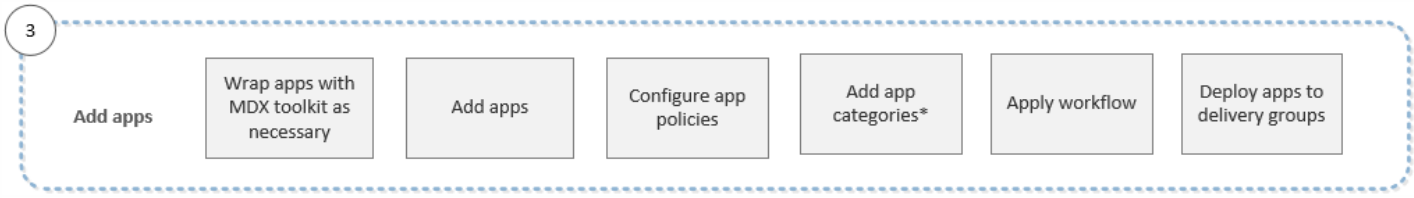


Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden Artikeln der Citrix Produktdokumentation:

- Benutzerkonten, Rollen und Registrierung
- Bereitstellen von Ressourcen
- Konfigurieren von Rollen mit RBAC
- Benachrichtigungen
- Erstellen und Verwalten von Workflows

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
- MDX-Richtlinien
- Erstellen und Verwalten von Workflows
- Bereitstellen von Ressourcen

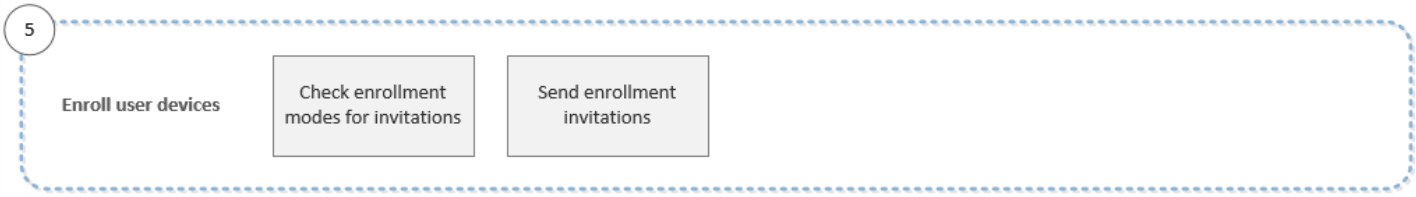
Der Workflow zeigt die beim Hinzufügen und Registrieren von Geräten in XenMobile empfohlene Reihenfolge.

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:

- Geräte
- Unterstützte Geräteplattformen
- Bereitstellen von Ressourcen
- Überwachen und Support
- Automatisierte Aktionen

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

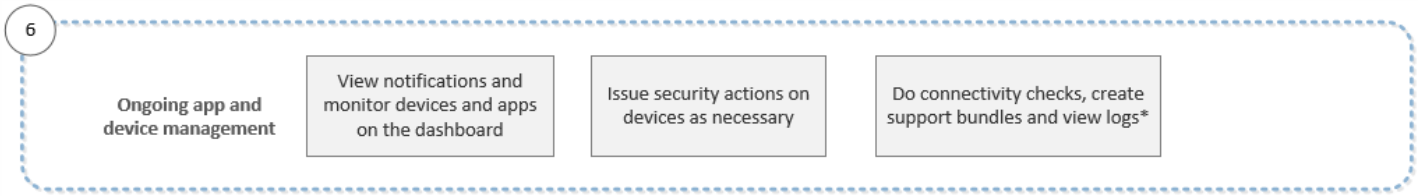


Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden Artikeln der Citrix Produktdokumentation:

- Benutzerkonten, Rollen und Registrierung
- Benachrichtigungen

Dieser 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 Sieunter Überwachen und Support.

Authentifizierung

Apr 24, 2017

Mehrere Komponenten spielen bei der Authentifizierung in XenMobile eine Rolle:

- **XenMobile-Server**: Auf dem XenMobile-Server legen Sie die Sicherheit für die Registrierung und die Registrierungserfahrung fest. Über die Optionen für das Onboarding von Benutzern können Sie vorgeben, ob die Registrierung für alle oder nur auf Einladung möglich sein soll und ob eine zweistufige oder eine dreistufige Authentifizierung verwendet werden soll.Über die Clienteigenschaften können Sie die Citrix PIN-Authentifizierung aktivieren und die PIN-Komplexität und -Ablaufzeit konfigurieren.
- **NetScaler**: NetScaler bietet Endpunkte für Micro VPN-SSL-Sitzungen sowie Sicherheit bei der Datenübertragung im Netzwerk und ermöglicht das Definieren der Authentifizierungserfahrung beim Zugriff auf Apps durch Benutzer.
- **Secure Hub**: Secure Hub wirkt mit dem XenMobile-Server bei der Registrierung zusammen. Secure Hub ist die Entität auf Geräten, die mit NetScaler kommuniziert: Wenn eine Sitzung abläuft, erhält Secure Hub ein Authentifizierungsticket von NetScaler und übergibt es an die MDX-Apps. Citrix empfiehlt die Verwendung von Zertifikatpinning zum Schutz vor Man-in-the-Middle-Angriffen. Weitere Informationen finden Sie im Abschnitt über das Zertifikatpinning des Artikels Secure Hub.

  Secure Hub moderiert zudem den MDX-Sicherheitscontainer durch Übertragen von Richtlinien, Erstellen einer neuen Sitzung mit NetScaler bei einem App-Timeout und durch Festlegen des MDX-Timeouts und der Benutzererfahrung. Außerdem ist Secure Hub für die Erkennung von Jailbreaks, Geolocation-Prüfungen und alle von Ihnen angewendeten Richtlinien verantwortlich.

- **MDX-Richtlinien**: MDX-Richtlinien erstellen den Datentresor auf Geräten. MDX-Richtlinien leiten Micro VPN-Verbindungen zurück zu NetScaler und erzwingen Einschränkungen für den Offlinemodus sowie die Einhaltung von Clientrichtlinien (z. B. Timeouts).

Weitere Informationen zu Überlegungen bei der Konfiguration der Authentifizierung und eine Übersicht über ein- und zweistufige Authentifizierung finden Sie im Bereitstellungshandbuch unter Authentifizierung .

Mit Zertifikaten erstellen Sie in XenMobile sichere Verbindungen und authentifizieren Benutzer. Im Rest dieses Artikels werden Zertifikate behandelt. Informationen zu weiteren Konfigurationsdetails finden Sie in den folgenden Artikeln:

- Authentifizierung mit Domäne oder mit Domäne und Sicherheitstoken
- Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne
- PKI-Entitäten
- Anmeldeinformationsanbieter
- APNs-Zertifikate
- SAML für Single Sign-On bei ShareFile
- Einstellungen des Microsoft Azure Active Directory-Servers

Zertifikate

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 Citrix PIN für den Single Sign-On-Zugriff auf XenMobile-aktivierte Apps ein. Citrix PIN vereinfacht zudem die Benutzerauthentifizierung. Mit Citrix 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. Anweisungen finden Sie unter APNs-Zertifikate.

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	.p12 (.pfx auf Windows-basierten Computern)	SSL, SAML, APNs XenMobile generiert außerdem eine vollständige PKI während der Installation.
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.

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. Informationen zum Erstellen, Hochladen und Konfigurieren von Clientzertifikaten finden Sie unter Authentifizierung mit Clientzertifikat oder mit Clientzertifikat und Domäne.

Anforderungen an private Schlüssel

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

Hochladen von Zertifikaten in die Konsole

Beim Hochladen von Zertifikaten in die Konsole haben Sie zwei Hauptoptionen:

- Sie können per Klick den Import eines Schlüsselspeichers veranlassen und den Eintrag im Schlüsselspeicherrepository angeben, den Sie installieren möchten (es sei denn, Sie laden ein PKCS#12-Zertifikat hoch).
- Sie können ein Zertifikat per Klick importieren.

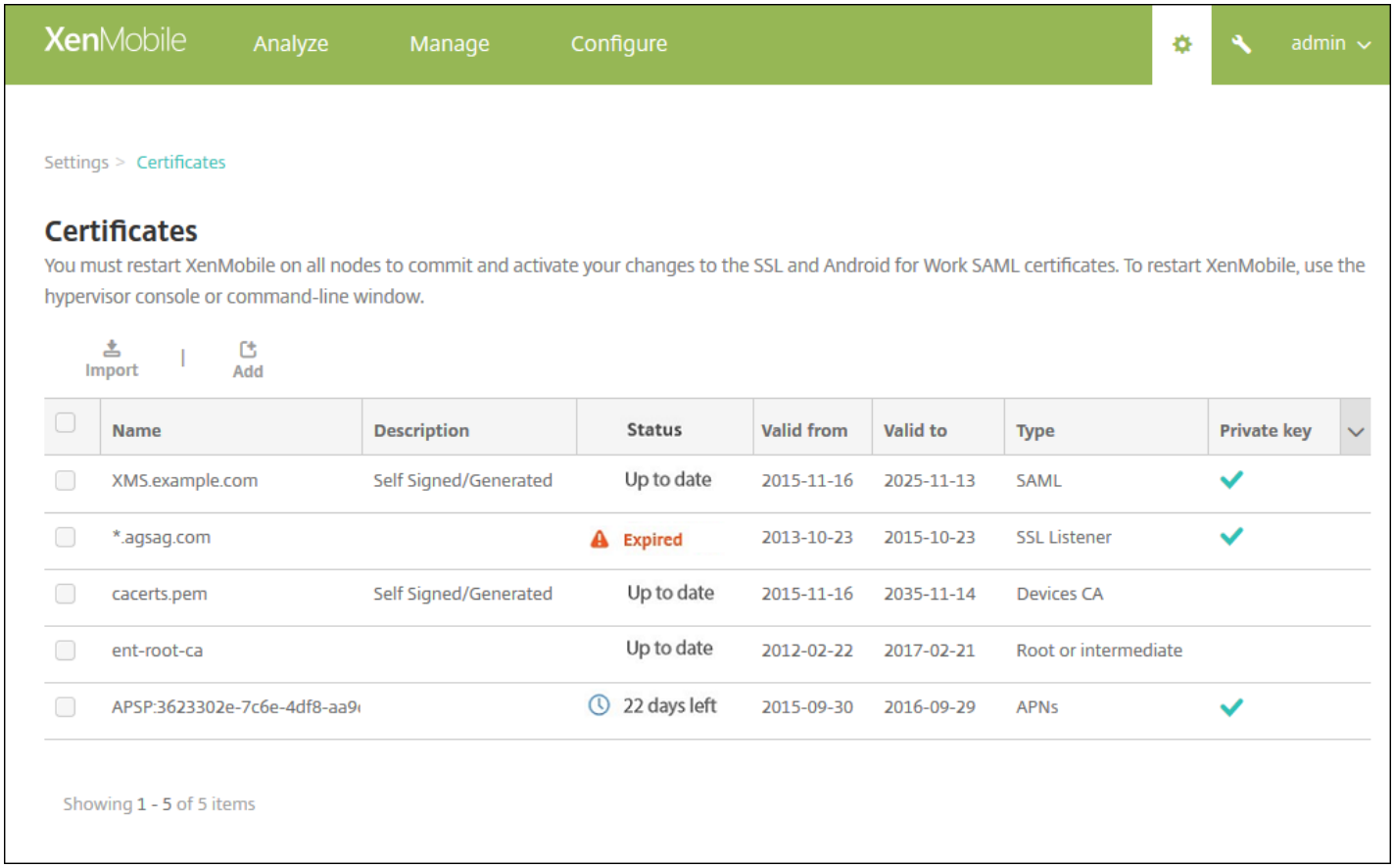
Sie können das ZS-Zertifikat ohne privaten Schlüssel hochladen, das die Zertifizierungsstelle zum Signieren von Anforderungen verwenden soll, und ein SSL-Clientzertifikat mit privatem Schlüssel für die Clientauthentifizierung. Wenn Sie die Entität der Microsoft-Zertifizierungsstelle konfigurieren, müssen 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.

Importieren eines Schlüsselspeichers

Schlüsselspeicher sind Repositorys mit Sicherheitszertifikaten und können als solche 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.

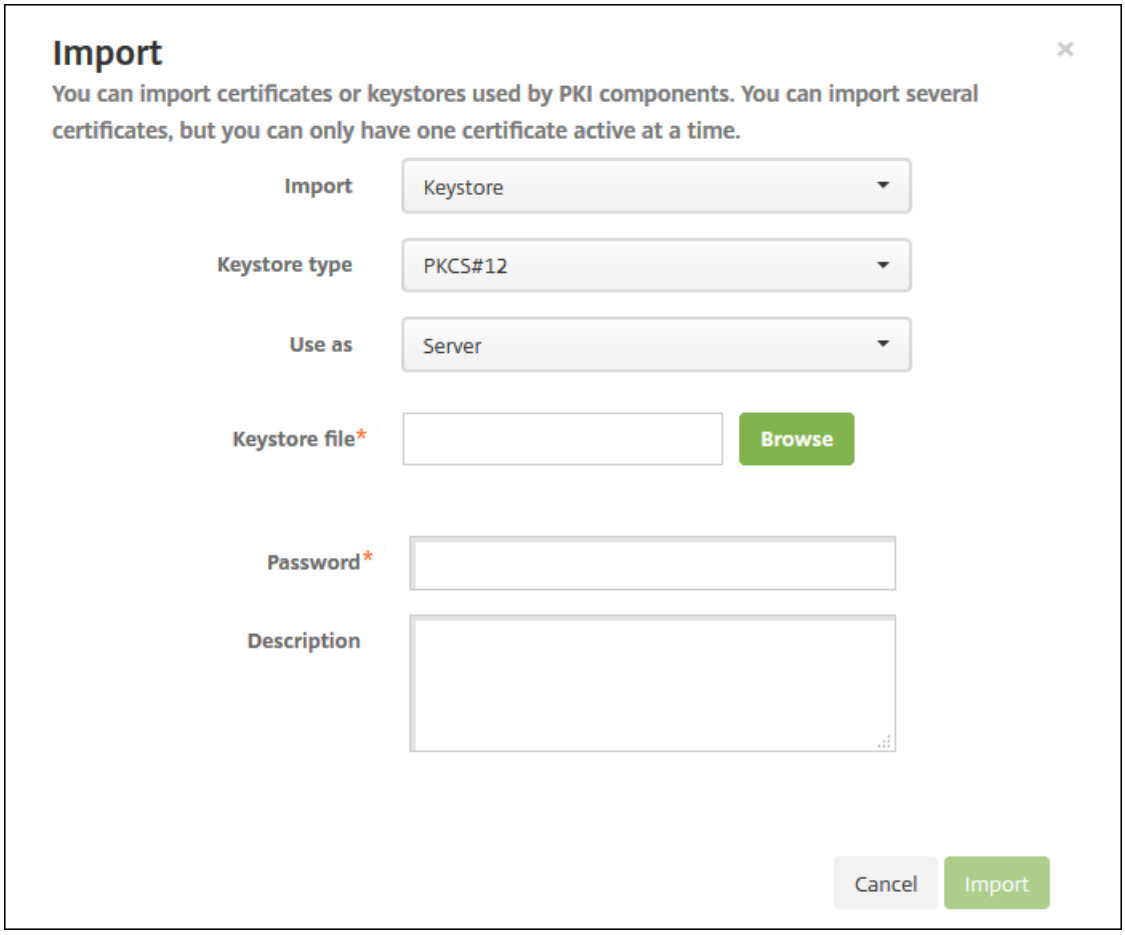
2. Klicken Sie auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.



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

4. Konfigurieren Sie folgende 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**.
- **Verwenden als**: Wählen Sie in der Liste aus, wie das Zertifikat verwendet werden soll. 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**: Navigieren Sie zu dem Schlüsselspeicher, den Sie importieren möchten. Der Dateityp ist "P12" (auf Windows-Computern "PFX").
- **Kennwort**: Geben Sie das dem Zertifikat zugewiesene Kennwort 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.

So importieren Sie ein Zertifikat

Beim Importieren eines Zertifikats aus einer Datei oder einem Schlüsselspeichereintrag versucht XenMobile die Erstellung einer Zertifikatkette und importiert alle Zertifikate in der Kette (wobei für jedes ein Serverzertifikateintrag erstellt wird). Dies funktioniert nur, wenn die Zertifikate in der Datei oder dem Schlüsselspeichereintrag tatsächlich eine Kette bilden, z. B. wenn jedes folgende Zertifikat in der Kette Aussteller des vorherigen Zertifikats ist.

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

1. Klicken Sie in der XenMobile-Konsole auf 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 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.
- **SSL-Listener**. Der Secure Sockets Layer-Listener benachrichtigt XenMobile über SSL-Kryptografieaktivitäten.

5. Navigieren Sie zu dem Schlüsselspeicher, den Sie importieren möchten. Der Dateityp ist "P12" (auf Windows-Computern "PFX").

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.

Aktualisieren eines Zertifikats

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

Klicken Sie zur optimalen Aktualisierung des Zertifikats in der XenMobile-Konsole auf das Zahnradsymbol oben rechts, um die Seite **Einstellungen** zu öffnen. Klicken Sie anschließend auf **Zertifikate**. Importieren Sie das neue Zertifikat im 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.

Verwalten der XenMobile-Zertifikate

Es empfiehlt sich, die in einer XenMobile-Bereitstellung verwendeten Zertifikate, insbesondere das Ablaufdatum und verknüpfte Kennwörter, nachzuverfolgen. Die Informationen in diesem Abschnitt sollen Ihnen die Zertifikatverwaltung in XenMobile erleichtern.

Ihre Umgebung kann einige oder alle der folgenden Zertifikate enthalten:

XenMobile Server
SSL-Zertifikat für MDM-FQDN
SAML-Zertifikat (für ShareFile)
Stamm- und Zwischenzertifikate der Zertifizierungsstelle für die vorangehenden Zertifikate und andere interne Ressourcen (StoreFront/Proxy usw.)
APNs-Zertifikat für iOS-Geräteverwaltung
Internes APNs-Zertifikat für Secure Hub-Benachrichtigungen des XenMobile-Servers
PKI-Benutzerzertifikat für PKI-Verbindungen

MDX Toolkit
Apple Developer-Zertifikat
Apple-Provisioningprofil (pro Anwendung)
Apple APNS-Zertifikat (zur Verwendung mit Citrix Secure Mail)
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 (Offload-Konfiguration)
SSL-Zertifikat für StoreFront-Lastausgleich
Stamm- und Zwischenzertifikate der Zertifizierungsstelle für die vorangehenden Zertifikate

Wenn ein Zertifikat abläuft, wird es ungültig. Sie können dann keine weiteren sicheren Transaktionen in Ihrer Umgebung ausführen und haben keinen Zugriff mehr auf XenMobile-Ressourcen.

> **Hinweis**
>
> Die Zertifizierungsstelle (CA) fordert Sie vor dem Ablaufdatum zur Verlängerung Ihres SSL-Zertifikats auf.

Zertifikate des Apple Diensts für Push-Benachrichtigungen (APNs) laufen jedes Jahr ab. Vergessen Sie nicht, vor Zertifikatablauf ein neues APNs-SSL-Zertifikat zu erstellen und vor Ablauf des Zertifikats zu aktualisieren.Läuft das Zertifikat ab, verursacht dies für Benutzer Inkonsistenzen bei Secure Mail-Pushbenachrichtigungen.Außerdem können Sie

keine weiteren Pushbenachrichtigungen für Ihre Apps senden.

Zum Registrieren und Verwalten von iOS-Geräten bei bzw. mit XenMobile müssen Sie ein APNS-Zertifikat erstellen und einrichten.Wenn das Zertifikat abläuft, können die Benutzer keine Registrierung bei XenMobile durchführen und Sie können keine iOS-Geräte verwalten. Informationen finden Sie unter APNs-Zertifikate.

Sie können den APNs-Zertifikatstatus und das Ablaufdatum anzeigen, indem Sie sich beim Apple Push Certificate Portal anmelden. Sie müssen sich mit demselben Benutzerkonto anmelden, das bei der Erstellung des Zertifikats verwendet wurde.

Sie erhalten außerdem 30 und 10 Tage vor dem Ablaufdatum eine E-Mail-Benachrichtigung von Apple mit folgendem Text:

"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.

Um sich zu vergewissern, dass Sie ein gültiges iOS-Verteilungszertifikat haben, führen Sie die folgenden Schritte aus:

1. Erstellen Sie über das Apple Enterprise Developer-Portal eine explizite App-ID für jede App, die Sie mit dem MDX Toolkit umschließen möchten. Beispiel einer zulässigen App-ID: com.Firmenname.Produktname.
2. Wechseln Sie im Apple Enterprise Developer-Portal zu **Provisioningprofile** > **Distribution** und erstellen Sie ein internes Provisioningprofil. 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.

Um sich zu vergewissern, dass alle XenMobile-Serverzertifikate gültig sind, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der XenMobile-Konsole auf **Einstellungen** und dann auf **Zertifikate**.
2. Vergewissern Sie sich, dass alle Zertifikate (APNS-, SSL- Listener-, Stamm- und Zwischenzertifikate) gültig sind.

Der Schlüsselspeicher ist eine Datei mit den Zertifikaten, mit denen Sie Android-Apps signieren. Wenn die Gültigkeit der Schlüssel abläuft, können Benutzer kein nahtloses Upgrade auf neue App-Versionen mehr ausführen.

Symantec ist exklusiver Anbieter von Codesignaturzertifikaten für den Microsoft App Hub-Dienst. Entwickler und Softwareherausgeber verwenden App Hub zum Verteilen von Apps für Windows Phone und Xbox 360 zum Download über den Microsoft Store bzw. Windows Marketplace. Weitere Informationen finden Sie unter Symantec Code Signing Certificates for Windows Phone in der Symantec-Dokumentation.

Wenn das Zertifikat abläuft, können Windows Phone-Benutzer sich nicht registrieren, keine vom Unternehmen veröffentlichte und signierte Apps installieren und keine auf dem Gerät installierte Unternehmensapp starten.

Weitere Informationen zur Handhabung des Zertifikatablaufs bei NetScaler finden Sie unter Handhabung des Zertifikatablaufs in NetScaler im Knowledge Center des Citrix Supports.

Ein abgelaufenes NetScaler-Zertifikat hindert Benutzer daran, Geräte zu registrieren, auf den Store zuzugreifen, bei der Verwendung von Secure Mail eine Verbindung mit Exchange Server herzustellen und HDX-Apps anzuzeigen und zu öffnen (je nachdem, welches Zertifikat abgelaufen ist).

Expiry Monitor und Command Center ermöglichen Ihnen, Ihre NetScaler-Zertifikate zu überwachen und benachrichtigt Sie, wenn ein Zertifikatablauf ansteht. Die beiden Tools helfen bei der Überwachung der folgenden NetScaler-Zertifikate:

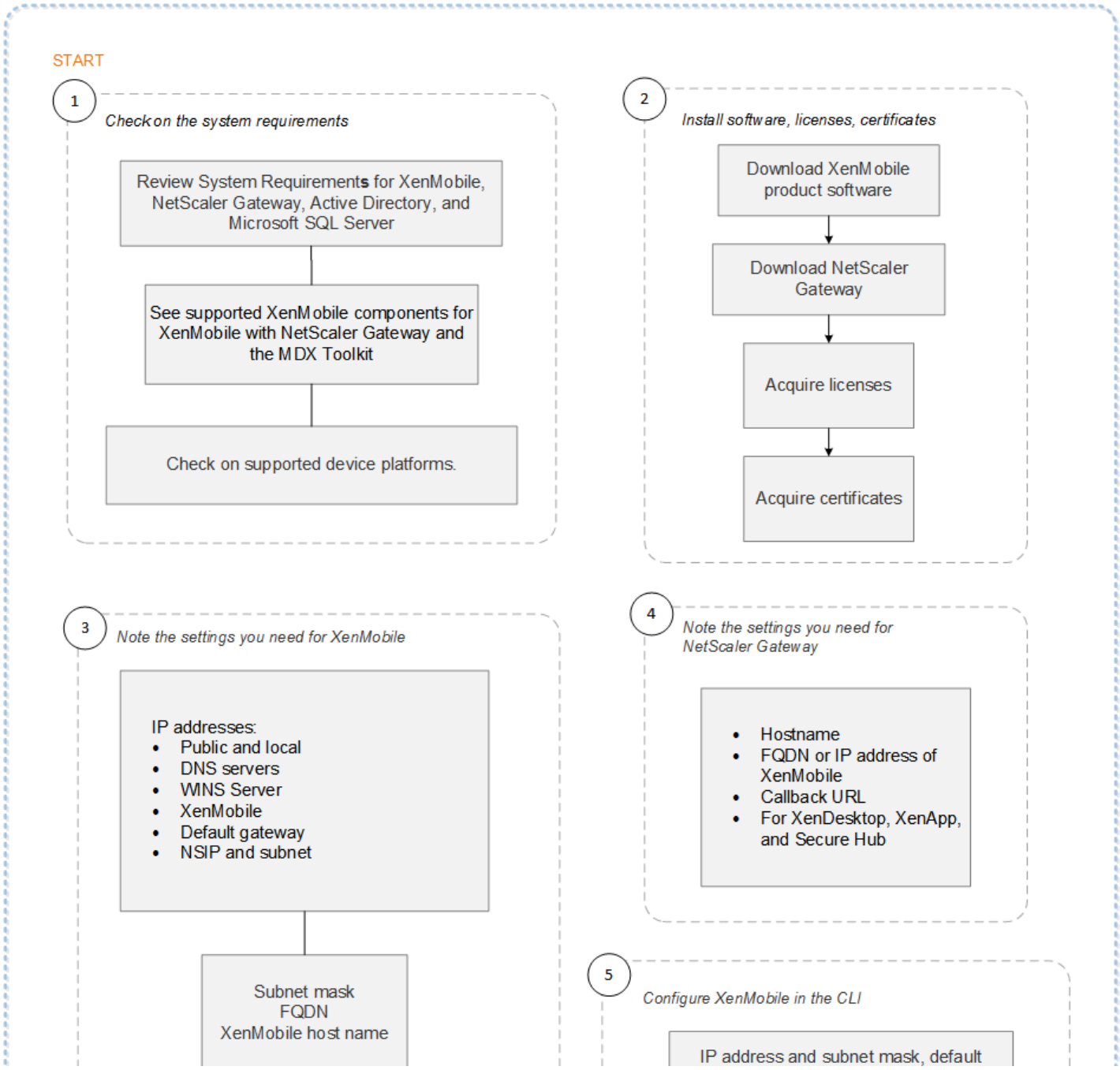
SSL-Zertifikat für MDM-FQDN
SSL-Zertifikat für Gateway-FQDN
SSL-Zertifikat für ShareFile SZC-FQDN
SSL-Zertifikat für Exchange-Lastausgleich (Offload-Konfiguration)
SSL-Zertifikat für StoreFront-Lastausgleich
Stamm- und Zwischenzertifikate der Zertifizierungsstelle für die vorangehenden Zertifikate

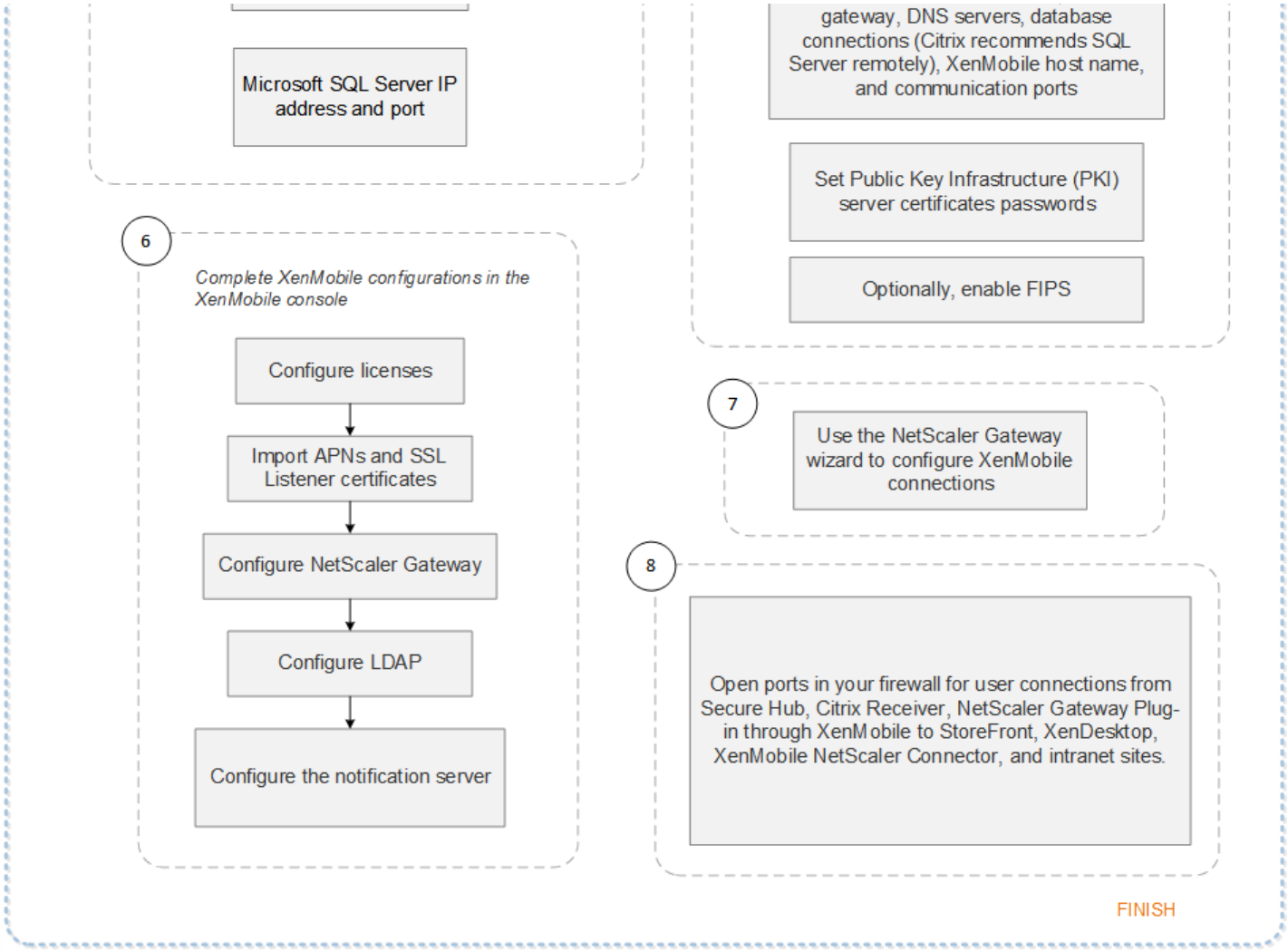
NetScaler Gateway und XenMobile

Feb 24, 2017

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. Konfigurieren Sie NetScaler Gateway in der XenMobile-Konsole wie in diesem Artikel beschrieben.

Dieses Flussdiagramm zeigt die Hauptschritte der Bereitstellung von XenMobile mit NetScaler Gateway. Im Anschluss an die Abbildung folgen Links zu Abschnitten zu jedem Schritt.





1

- Systemanforderungen und -kompatibilität

2

- Installation und Konfiguration

3

- Prüfliste zur Installationsvorbereitung

4

- Prüfliste zur Installationsvorbereitung

5

- Konfigurieren von XenMobile im Eingabeaufforderungsfenster

6

- Konfigurieren von XenMobile in einem Webbrowser

7

- Konfigurieren von Einstellungen für die XenMobile-Umgebung

8

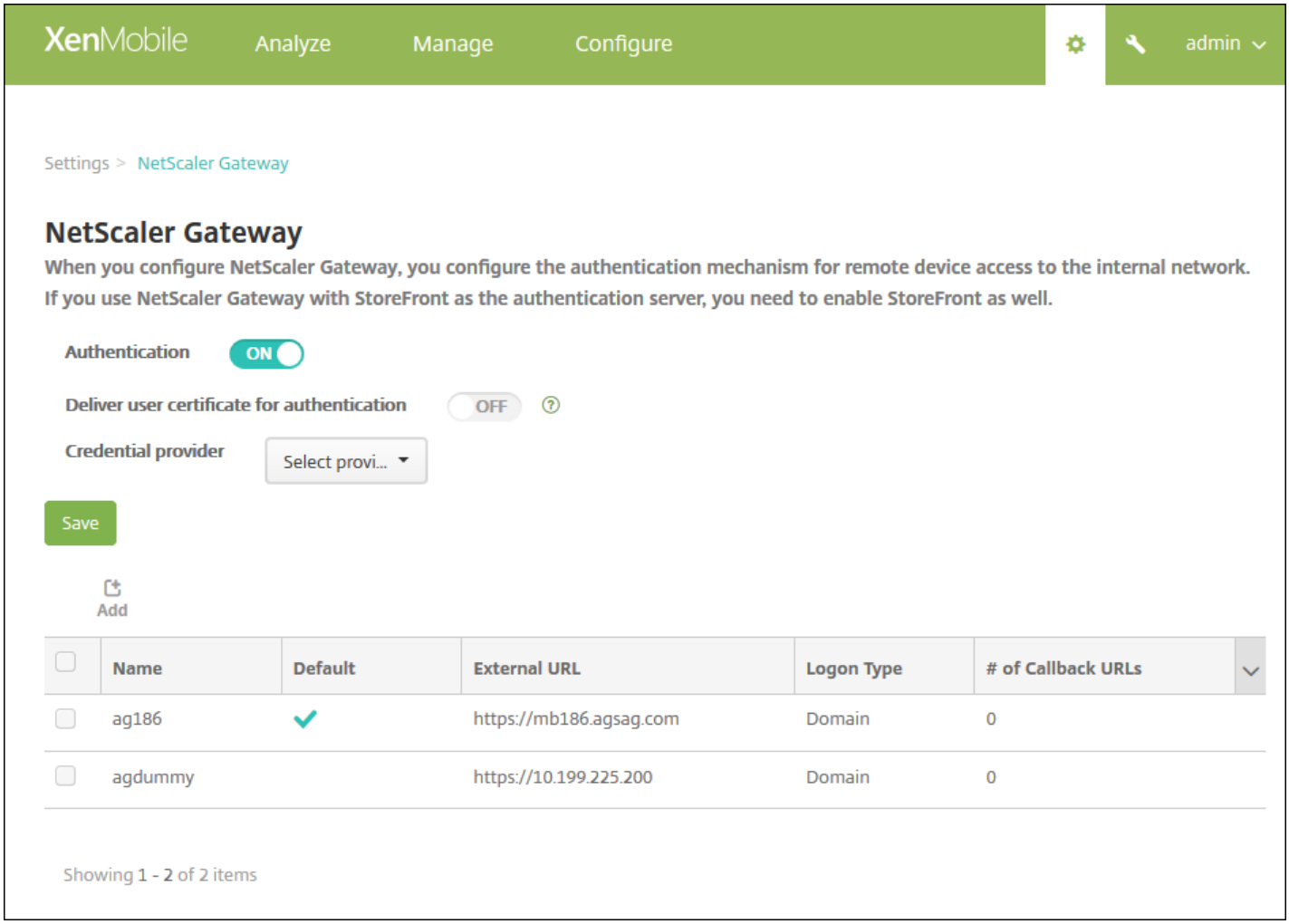
- Ports

Das Flussdiagramm ist auch im PDF-Format verfügbar.

Flussdiagramm für die Bereitstellung von XenMobile

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:

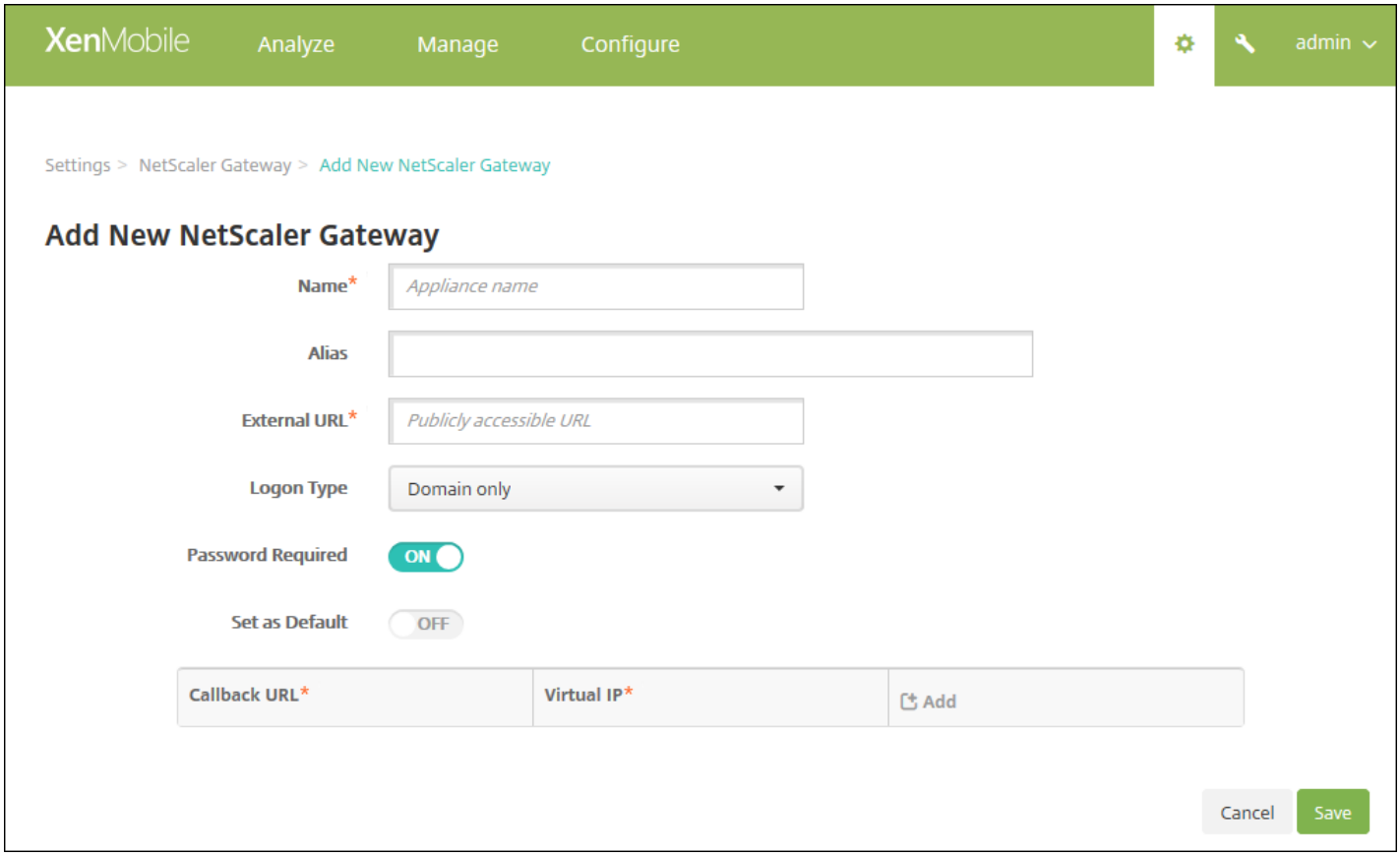
- **Authentifizierung**: Wählen Sie aus, ob die Authentifizierung aktiviert werden soll. Der Standardwert ist **EIN**.
- **Benutzerzertifikat für Authentifizierung bereitstellen**: Wählen Sie aus, ob XenMobile das Authentifizierungszertifikat zusammen mit Secure Hub verwenden soll, sodass NetScaler Gateway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

6. 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, ist eine zusätzliche Konfiguration in NetScaler Gateway erforderlich, damit Secure Hub unterstützt wird. 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. Die Callback-URL muss in eine IP-Adresse aufgelöst werden, die der XenMobile-Server erreichen kann. Es muss jedoch keine externe NetScaler Gateway-URL sein.

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

Authentifizierung mit Domäne oder mit Domäne und Sicherheitstoken

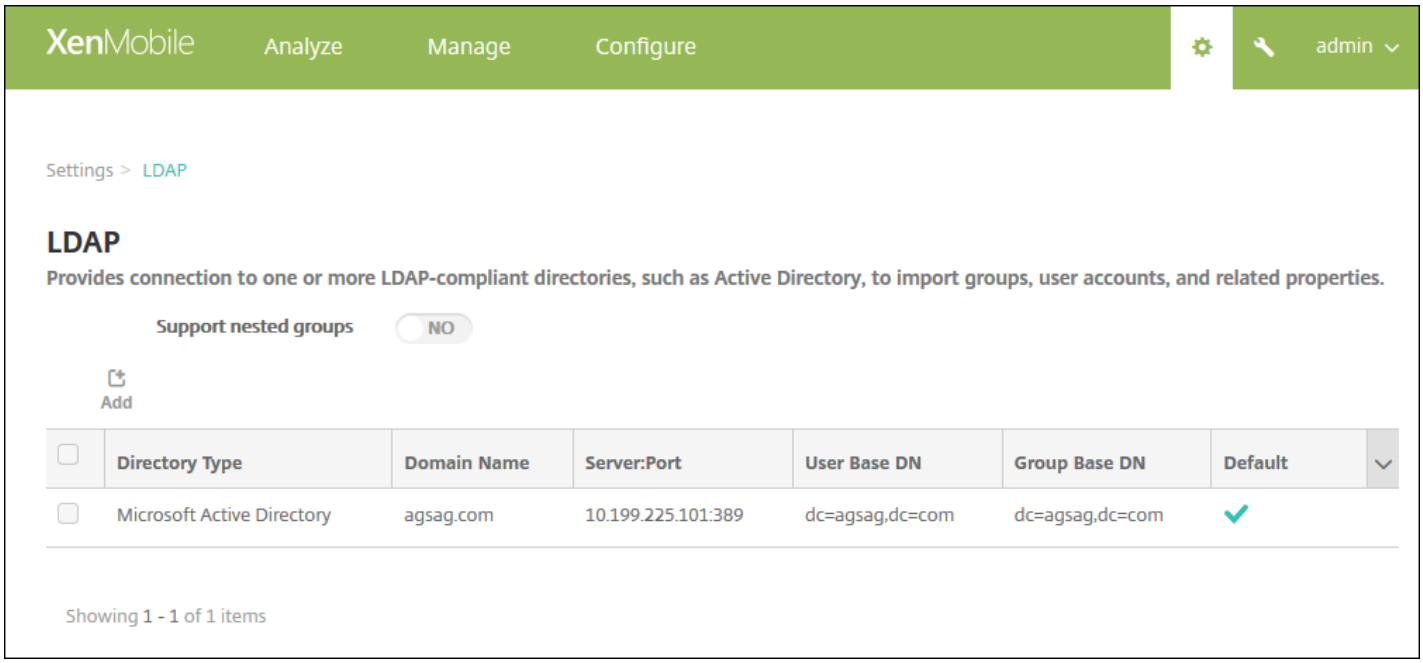
Feb 24, 2017

XenMobile unterstützt die domänenbasierte Authentifizierung unter Verwendung eines oder mehrerer Lightweight Directory Access Protocol-konformer Verzeichnisse (z. B. Active Directory). Sie können in XenMobile eine Verbindung mit einem oder mehreren Verzeichnissen konfigurieren und dann unter Verwendung der LDAP-Konfiguration Gruppen, Benutzerkonten und zugehörige Eigenschaften importieren.

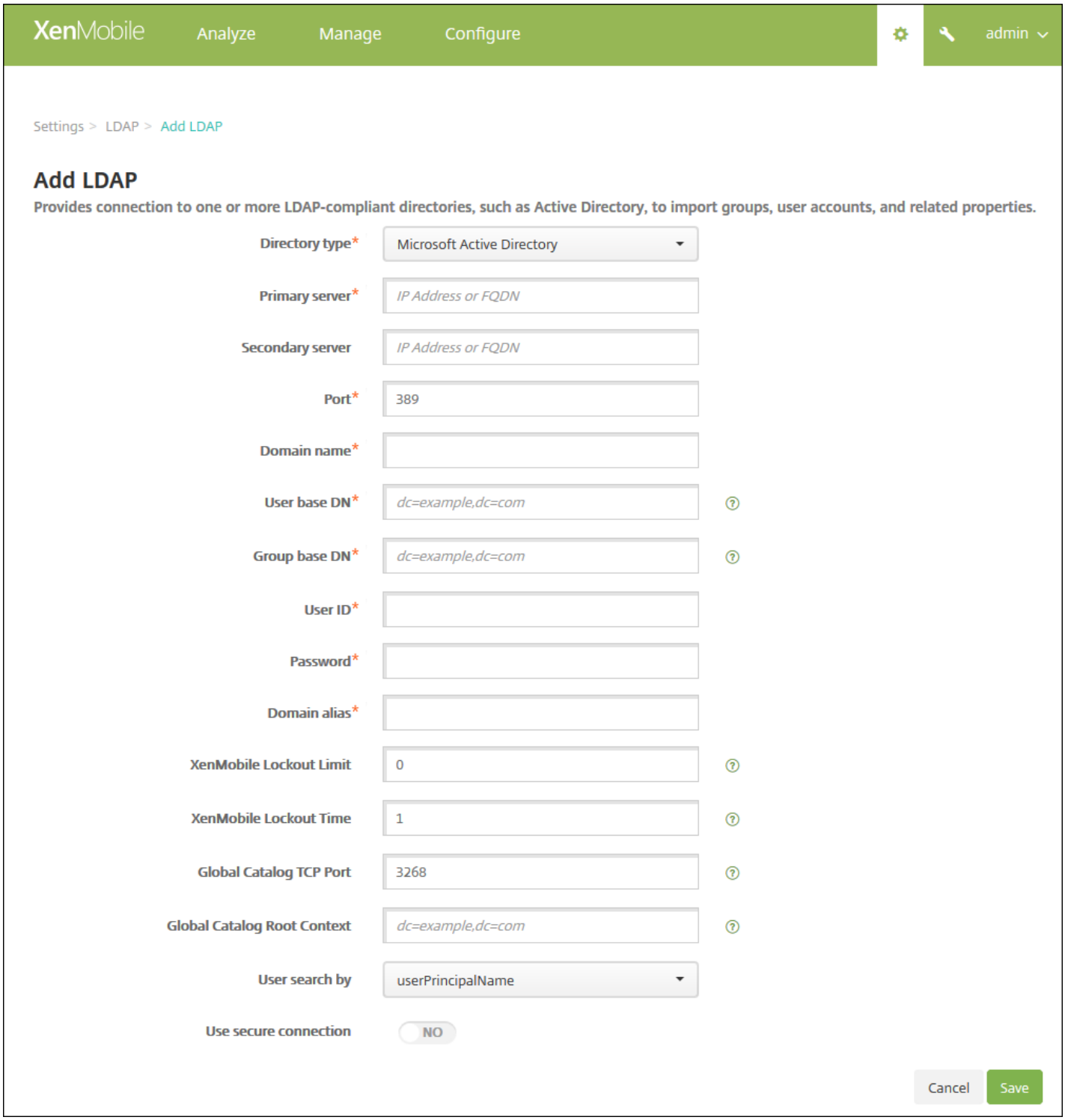
LDAP ist ein herstellerneutrales Open-Source-Anwendungsprotokoll zur Verwaltung eines verteilten Verzeichnisinformationsdiensts über ein Internet Protocol-Netzwerk. Verzeichnisinformationsdienste werden verwendet, um Informationen zu Benutzern, Systemen, Netzwerken, Diensten und Anwendungen über das 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.

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.

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 folgende Einstellungen:

- **Directory Type**: Klicken Sie in der Liste auf den Verzeichnistyp. Der Standardwert ist **Microsoft Active Directory**.
- **Primary server**: Geben Sie den für LDAP verwendeten primären Server an. Sie können die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) eingeben.
- **Secondary server**: Geben Sie optional die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) für den sekundären Server (sofern konfiguriert) ein. Dieser Server ist ein Failoverserver und wird verwendet, wenn der primäre Server nicht erreichbar ist.

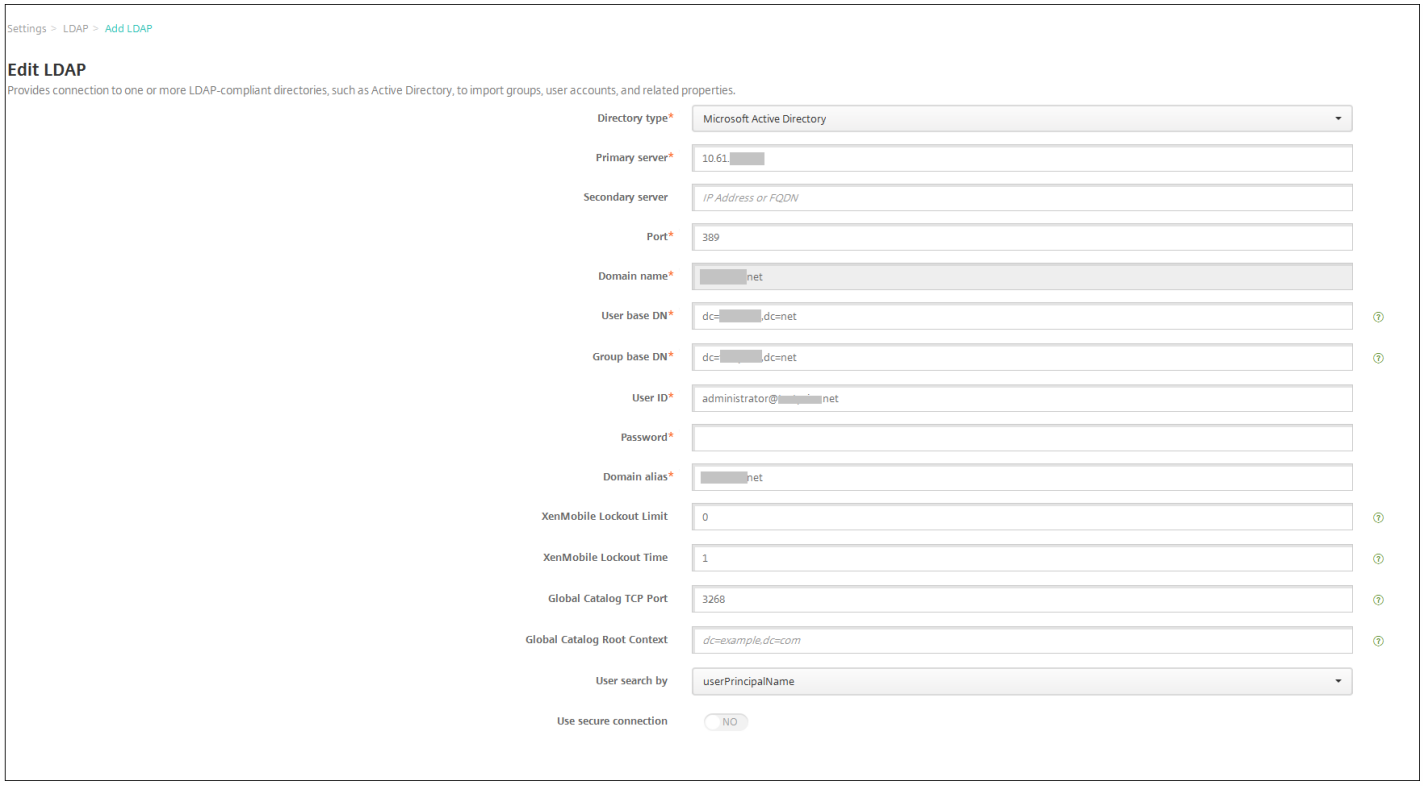
- **Port**: Geben Sie die Portnummer des LDAP-Servers ein. Die Standardeinstellung für unsichere LDAP-Verbindungen ist 389. Verwenden Sie Port 636 für sichere LDAP-Verbindungen, 3268 für unsichere Microsoft-LDAP-Verbindungen oder 3269 für sichere Microsoft-LDAP-Verbindungen.
- **Domain name**: Geben Sie den Domänennamen ein.
- **User base DN**: Geben Sie den Speicherort von Benutzern in Active Directory über einen eindeutigen Bezeichner ein. Syntaxbeispiele: ou=users, dc=example oder dc=com.
- **Group base DN**: Geben Sie den Speicherort von Gruppen in Active Directory ein. Beispiel: cn=users, dc=domain, dc=net, wobei "cn=users" für den Containernamen der Gruppen und "dc" für die Domänenkomponente von Active Directory steht.
- **User ID**: Geben Sie die dem Active Directory-Konto zugeordnete Benutzer-ID ein.
- **Password**: Geben Sie das dem Benutzer zugeordnete Kennwort ein.
- **Domain alias**: Geben Sie ein Alias für den Domänennamen ein.
- **XenMobile Lockout Limit**: Geben Sie eine Zahl zwischen 0 und 999 für die Anzahl zulässiger fehlgeschlagener Anmeldeversuche ein. Wenn Sie 0 festlegen, wird der Benutzer nie aufgrund fehlgeschlagener Anmeldeversuche aus XenMobile ausgesperrt.
- **XenMobile Lockout Time**: Geben Sie eine Zahl zwischen 0 und 99999 für den Zeitraum in Minuten ein, den ein Benutzer nach einer Überschreitung des Sperrlimits abwarten muss. Wenn Sie 0 festlegen, muss der Benutzer nach einer Sperrung nicht warten.
- **Global Catalog TCP Port**: Geben Sie die TCP-Portnummer des Servers für den globalen Katalog ein. Die Standard-TCP-Portnummer ist 3268. Verwenden Sie für SSL-Verbindungen die Portnummer 3269.
- **Global Catalog Root Context**: Geben Sie optional den Stammkontext für den globalen Katalog ein, der eine Suche im globalen Katalog von Active Directory ermöglicht. Diese Suchfunktion existiert zusätzlich zu der Standard-LDAP-Suche und ermöglicht die Suche in jeder Domäne ohne Angabe des Domänennamens.
- **User search by**: Klicken Sie in der Liste auf **userPrincipalName** oder **sAMAccountName**. Der Standardwert ist **userprincipalname**.
- **Use secure connection**: Wählen Sie aus, ob sichere Verbindungen verwendet werden sollen. Der Standardwert ist **NO**.

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 **Edit**.Die Seite **LDAP** 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 der Authentifizierung mit Domäne und Sicherheitstoken

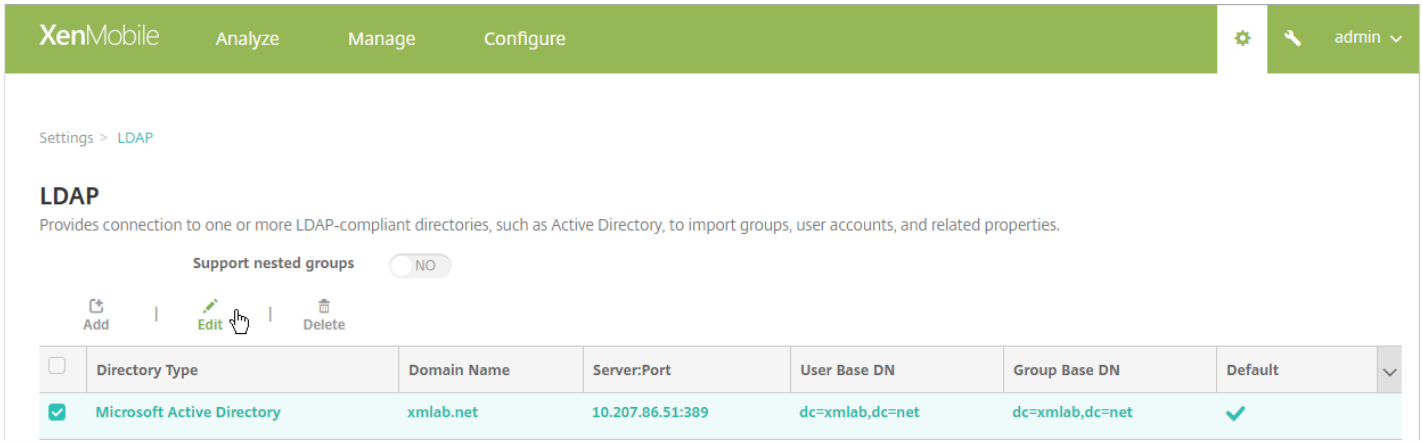
Sie können XenMobile konfigurieren, sodass Benutzer sich mit ihren LDAP-Anmeldeinformationen und einem Einmalkennwort authentifizieren müssen. Dabei wird das RADIUS-Protokoll verwendet.

Sie können diese Konfiguration mit der Citrix 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.

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.

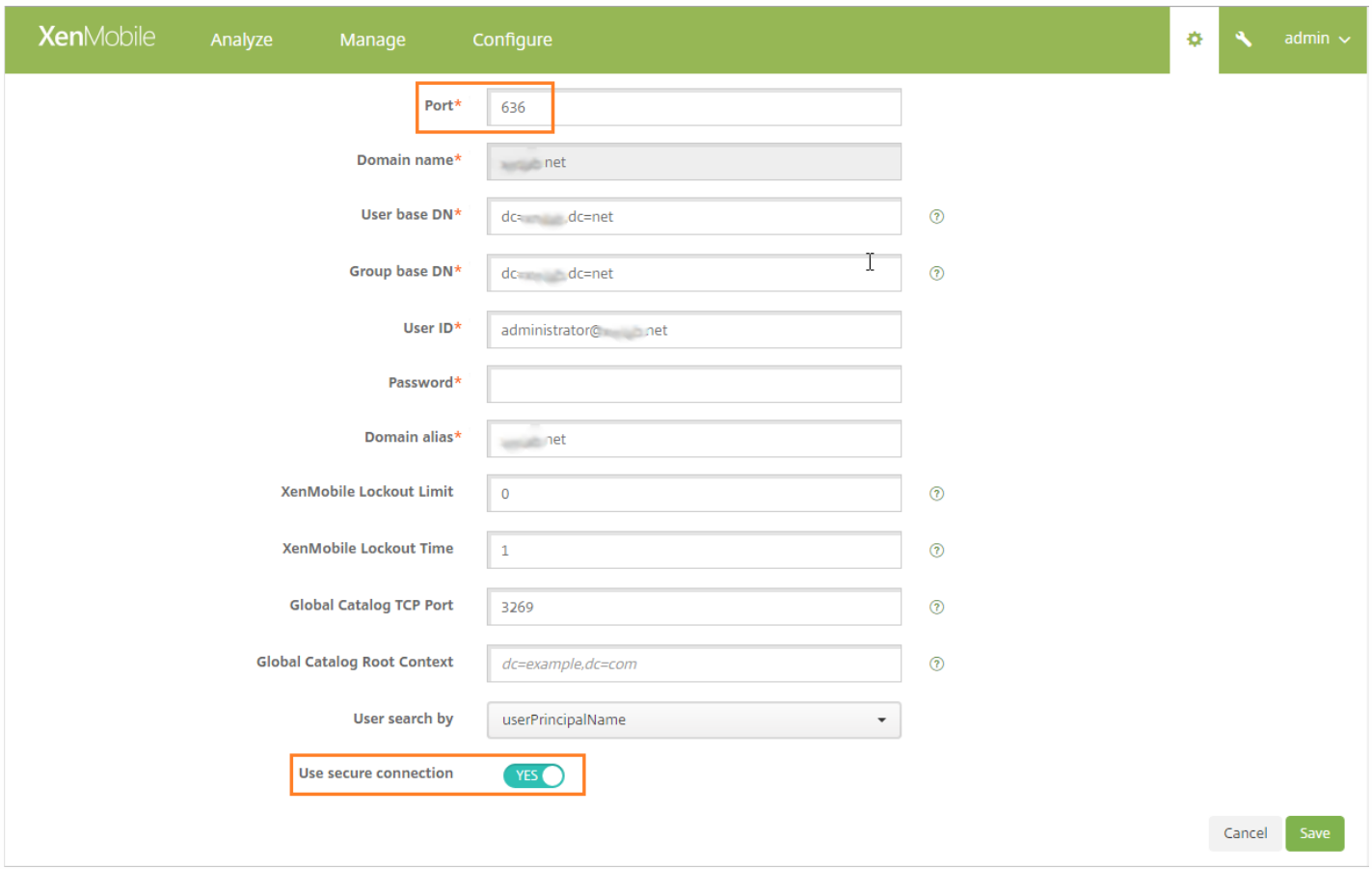
1. Klicken Sie in **Einstellungen** auf **LDAP**.

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.

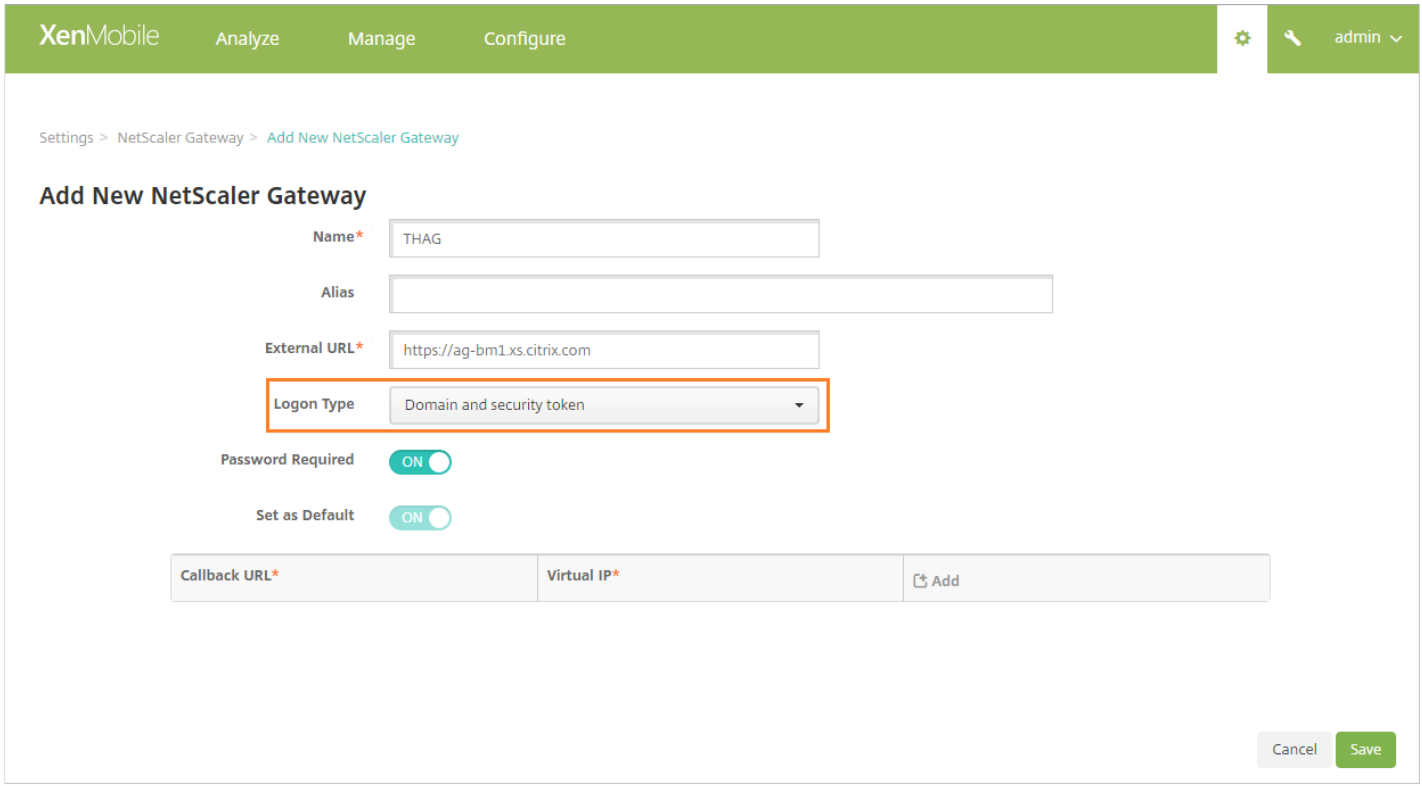


Für die folgenden Schritte wird angenommen, dass Sie XenMobile bereits eine NetScaler Gateway-Instanz hinzugefügt haben. Anweisungen zum Hinzufügen einer Instanz von NetScaler Gateway finden Sie unter Hinzufügen einer neuen NetScaler Gateway-Instanz.

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

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

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



Um die Worx-PIN und die Zwischenspeicherung von Benutzerkennwörtern 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 Clienteigenschaften.

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.

Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne

Apr 24, 2017

Standardmäßig ist XenMobile für die Authentifizierung per Benutzernamen und Kennwort konfiguriert. Als zusätzliche Sicherheitsstufe für die Registrierung bei und den Zugriff auf die XenMobile-Umgebung ist die zertifikatbasierte Authentifizierung in Betracht zu ziehen. In der XenMobile-Umgebung bietet diese Konfiguration die beste Kombination aus Sicherheit und Benutzererfahrung, denn sie verbindet die besten SSO-Möglichkeiten mit der Sicherheit der zweistufigen Authentifizierung über NetScaler.

Wenn Sie LDAP nicht zulassen und Smartcards oder ähnliche Methoden verwenden, können Sie durch Konfigurieren von Zertifikaten XenMobile eine Smartcard präsentieren. Die Benutzer registrieren sich in diesem Fall mit einer eindeutigen PIN, die von XenMobile generiert wird. Sobald ein Benutzer Zugriff hat, erstellt XenMobile das Zertifikat, das ab dann für die Authentifizierung bei der XenMobile-Umgebung verwendet wird, und stellt dieses bereit.

Sie können die in XenMobile erforderliche Konfiguration mit dem NetScaler für XenMobile-Assistenten durchführen, wenn Sie die NetScaler-Authentifizierung per Zertifikat oder per Zertifikat und Domäne verwenden. Sie können den NetScaler für XenMobile-Assistenten nur einmal ausführen.

In Hochsicherheitsumgebungen, in denen die Verwendung von LDAP-Anmeldeinformationen außerhalb der Organisation in öffentlichen oder unsicheren Netzwerken eine große Sicherheitsbedrohung darstellt, kann die zweistufige Authentifizierung mit Clientzertifikat und Sicherheitstoken verwendet werden. Weitere Informationen finden Sie unter Configuring XenMobile for Certificate and Security Token Authentication.

Die Clientzertifikatauthentifizierung steht im XenMobile-MAM-Modus (Nur-MAM-Modus) und im ENT-Modus (wenn Benutzer sich bei MDM registrieren) zur Verfügung. Die Clientzertifikatauthentifizierung steht im XenMobile-ENT-Modus nicht zur Verfügung, wenn Benutzer sich im Legacy-MAM-Modus registrieren. Zum Verwenden von Clientzertifikatauthentifizierung im Enterprise- oder MAM-Modus müssen Sie den Microsoft-Server, den XenMobile-Server und dann NetScaler Gateway konfigurieren. Folgen Sie den in diesem Artikel beschriebenen allgemeinen Schritten.

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.

Führen Sie in NetScaler Gateway die in der NetScaler Gateway-Dokumentation unter Configuring Client Certificate or Client Certificate and Domain Authentication beschriebene Konfiguration durch.

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.

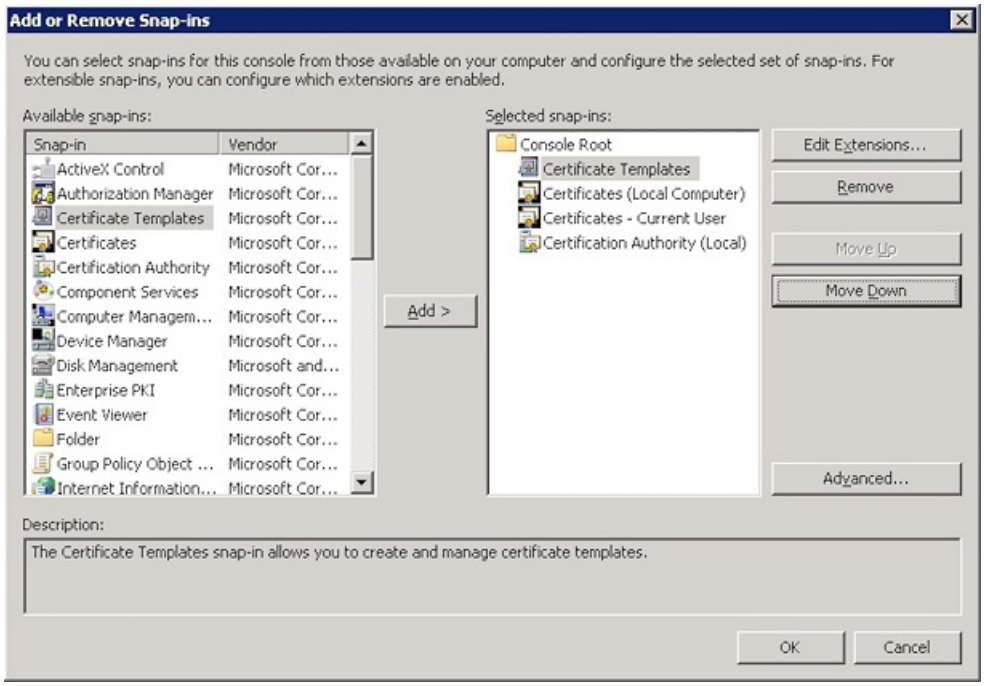
- Informationen zum Konfigurieren der zertifikatbasierten Authentifizierung für Exchange ActiveSync finden Sie in diesem Microsoft-Blog.
- Wenn Sie private Serverzertifikate zum Schützen des ActiveSync-Datenverkehrs an Exchange Server verwenden, müssen die mobilen Geräte alle Stamm- und Zwischenzertifikate haben. Ansonsten schlägt die zertifikatbasierte Authentifizierung beim Einrichten des Postfachs in Secure Mail 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 Secure Mail für iOS, Android und Windows Phone mit der aktuellen MDX Toolkit-Version umschlossen wird.

Hinzufügen eines Zertifikat-Snap-Ins zu Microsoft Management Console

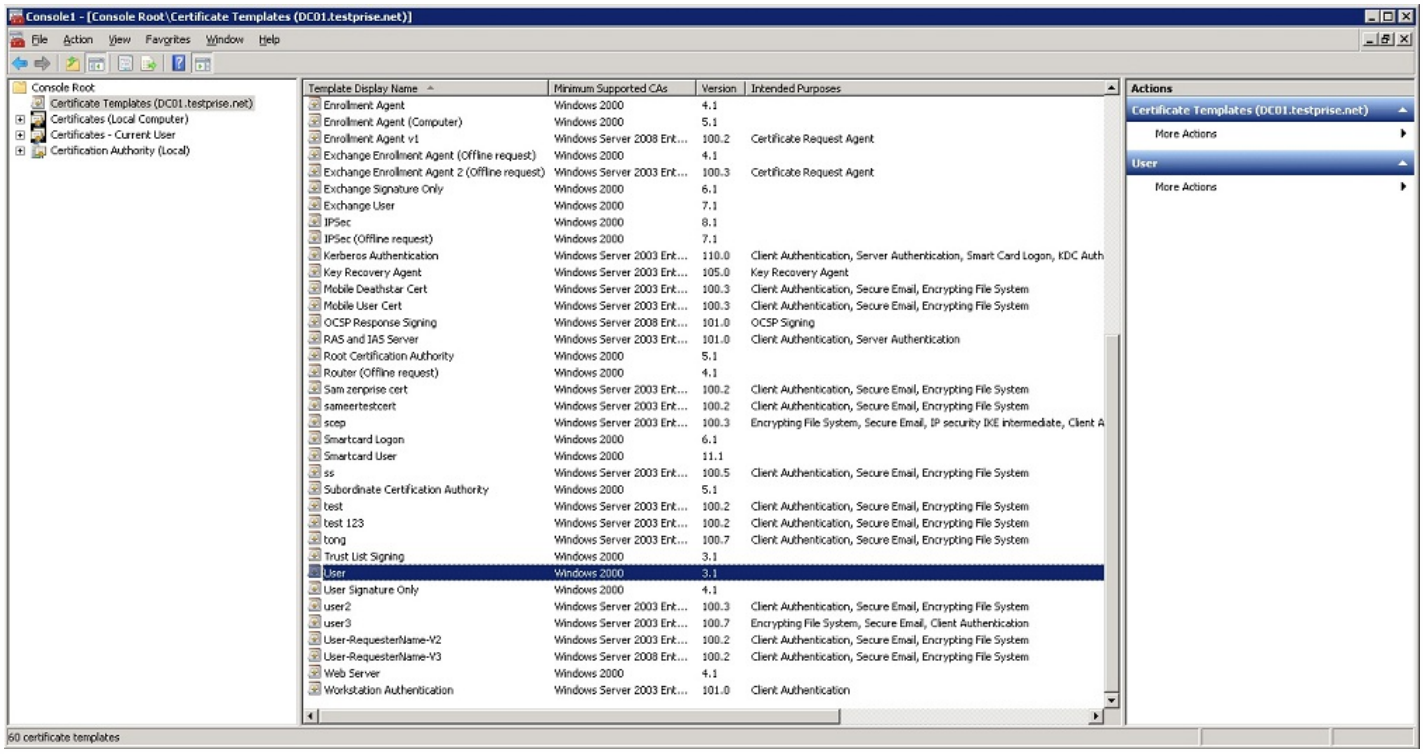
1. Öffnen Sie die Konsole und klicken Sie auf **Snap-In hinzufügen/entfernen**.

2. Fügen Sie die folgenden Snap-Ins hinzu:

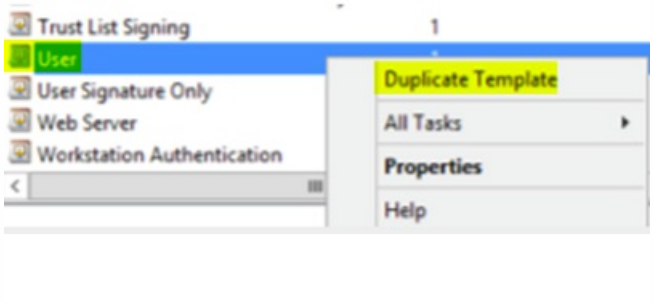
   Zertifikatvorlagen
   Zertifikate (lokaler Computer)
   Zertifikate – aktueller Benutzer
   Zertifizierungsstelle (lokal)



3. Erweitern Sie **Zertifikatvorlagen**.



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

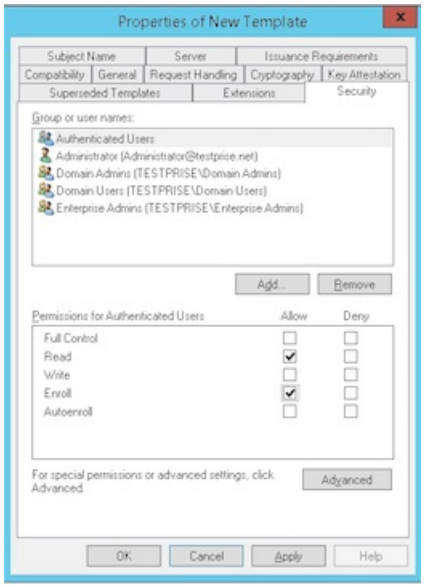


5. Geben Sie den Anzeigenamen der Vorlage an.

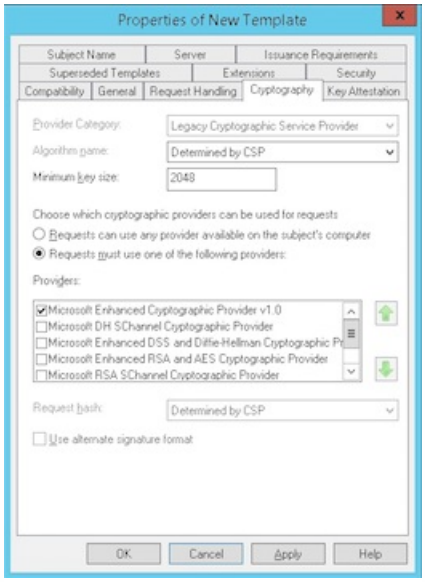
> **Wichtig:** Aktivieren Sie das Kontrollkästchen **Zertifikat in Active Directory veröffentlichen** nur bei Bedarf. Wenn diese Option aktiviert ist, werden alle Benutzer-Clientzertifikate in Active Directory erstellt/bereitgestellt, wodurch Ihre Active Directory-Datenbank überladen werden kann.

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

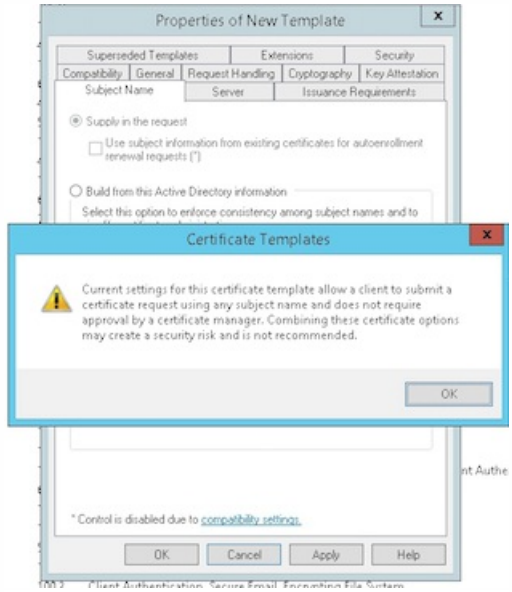
7. Wählen Sie unter **Sicherheit** in der Spalte **Zulassen** die Option **Registrieren** für die authentifizierten Benutzer aus.



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



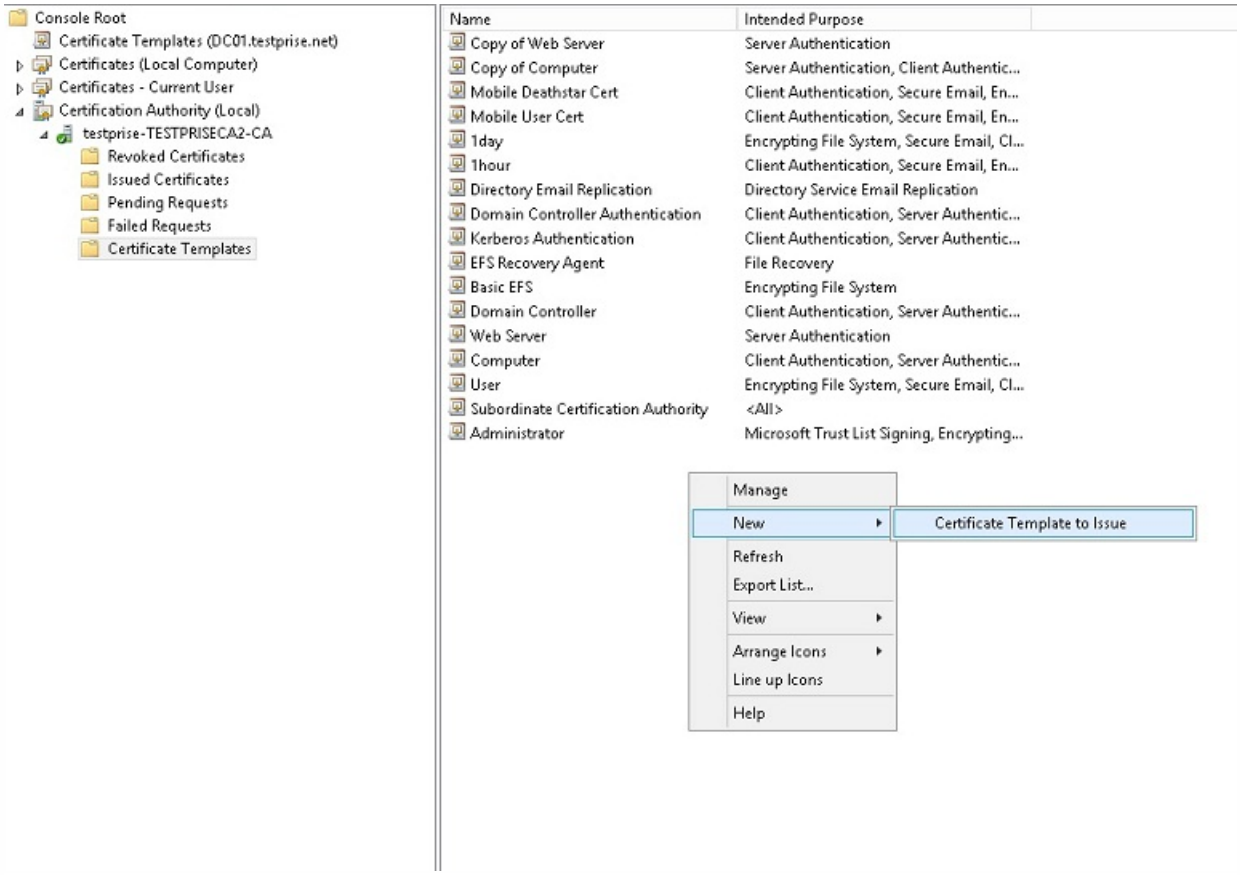
9. Wählen Sie unter **Antragstellername** die Option **Informationen werden in der Anforderung angegeben** aus. Wenden Sie die Änderungen an und speichern Sie.



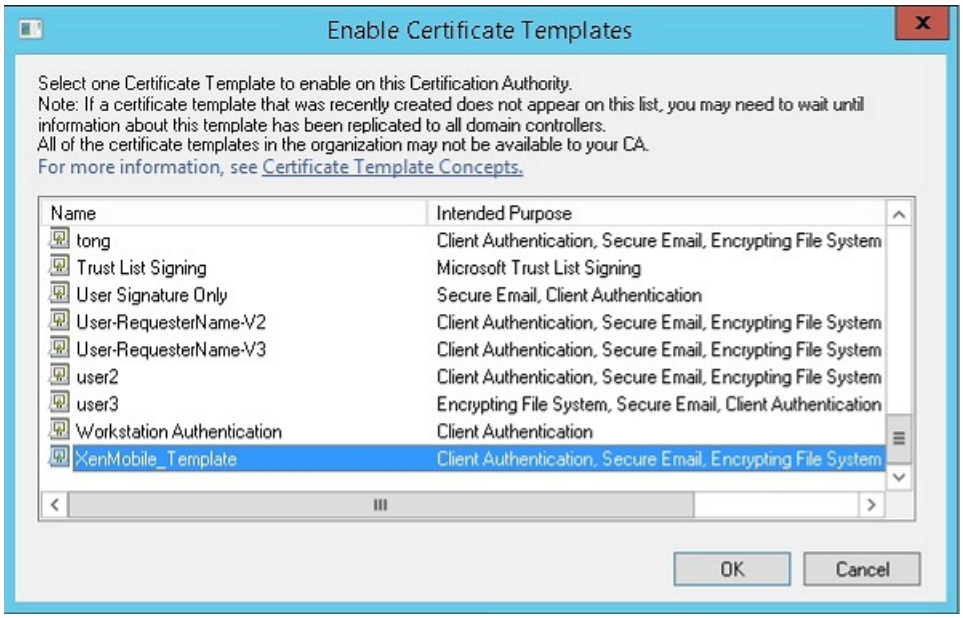
Hinzufügen der Vorlage zur Zertifizierungsstelle

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.

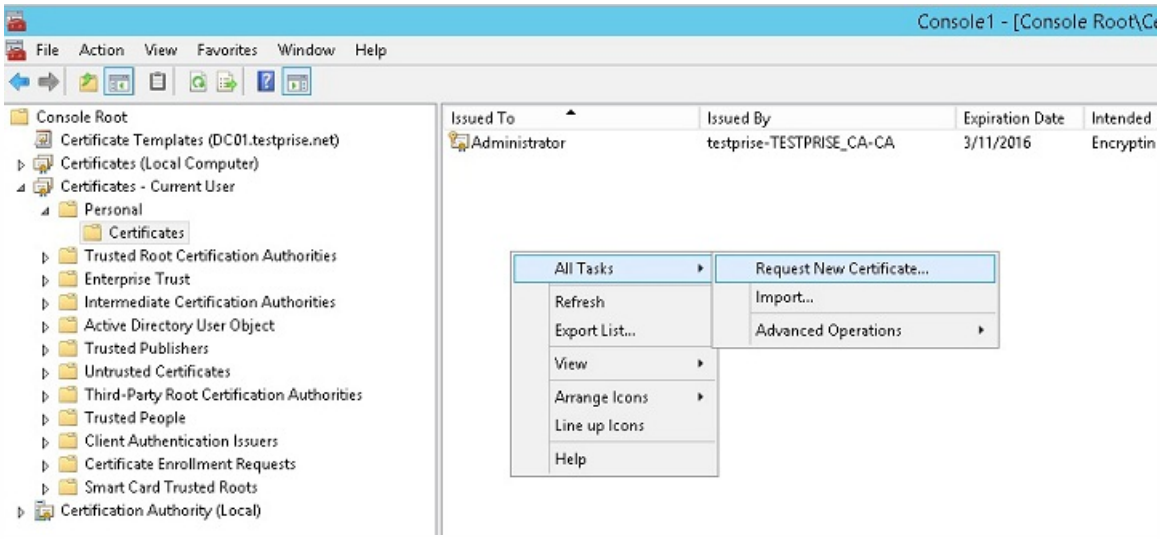


Erstellen eines PFX-Zertifikats vom ZS-Server

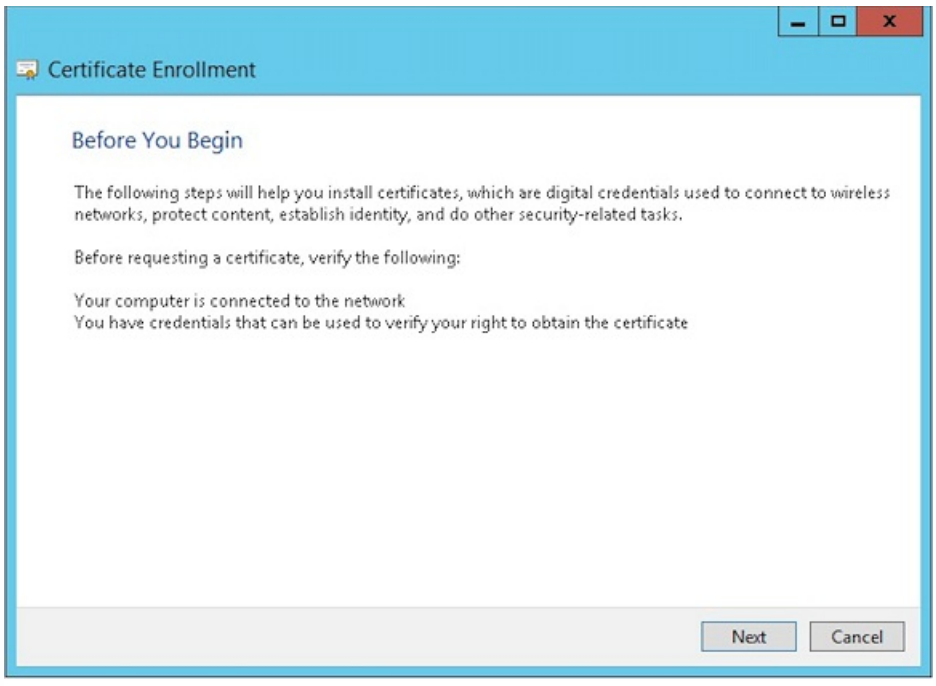
1. Erstellen Sie mit dem Dienstkonto, mit dem Sie sich angemeldet haben, ein PFX-Benutzerzertifikat. Diese PFX-Datei wird in XenMobile hochgeladen, um ein Benutzerzertifikat im Namen der Benutzer anzufordern, die ihre Geräte registrieren.

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

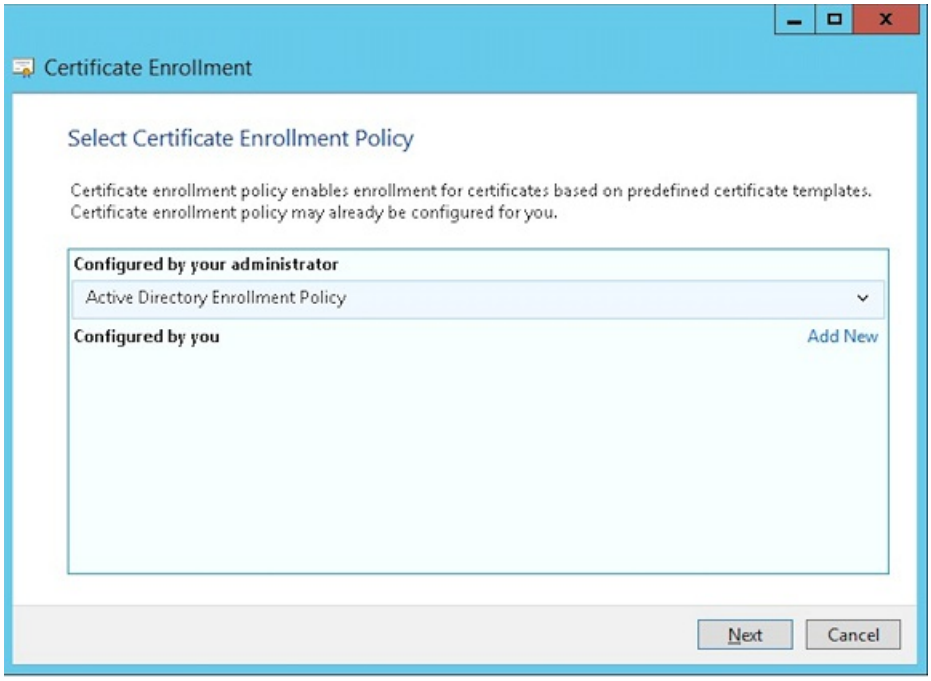
3. Klicken Sie mit der rechten Maustaste in den rechten Bereich und klicken Sie auf **Neues Zertifikat anfordern**.



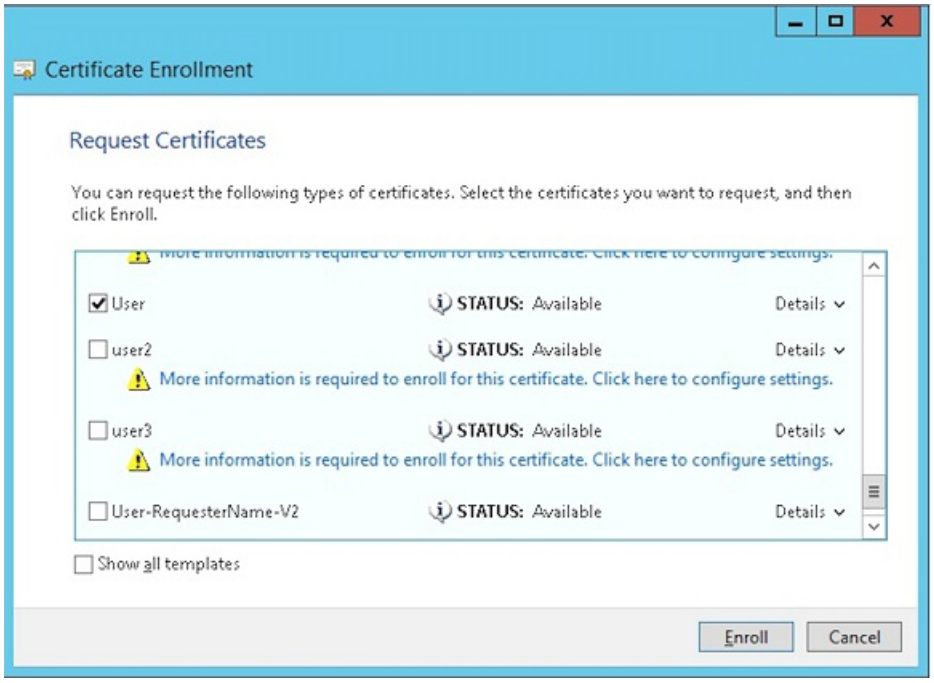
4. Der Bildschirm **Zertifikatregistrierung** wird angezeigt. Klicken Sie auf **Weiter**.



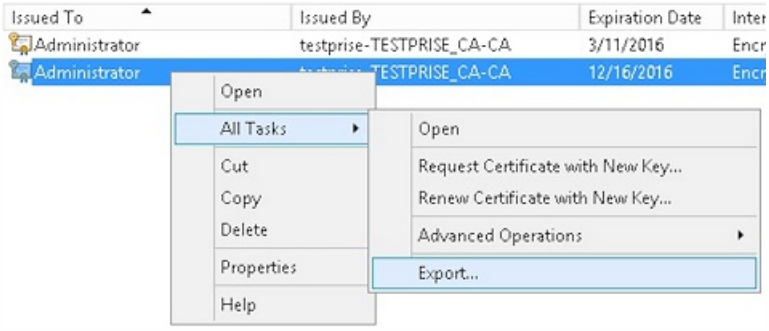
5. Wählen Sie **Active Directory-Registrierungsrichtlinie** und klicken Sie auf **Weiter**.



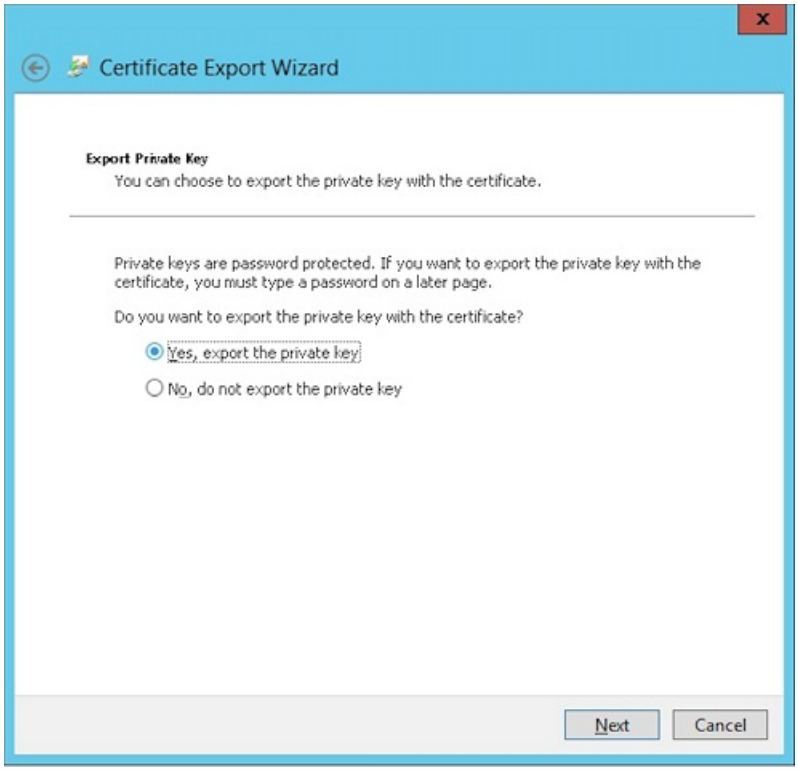
6. Wählen Sie die Vorlage **Benutzer** und klicken Sie auf **Registrieren**.



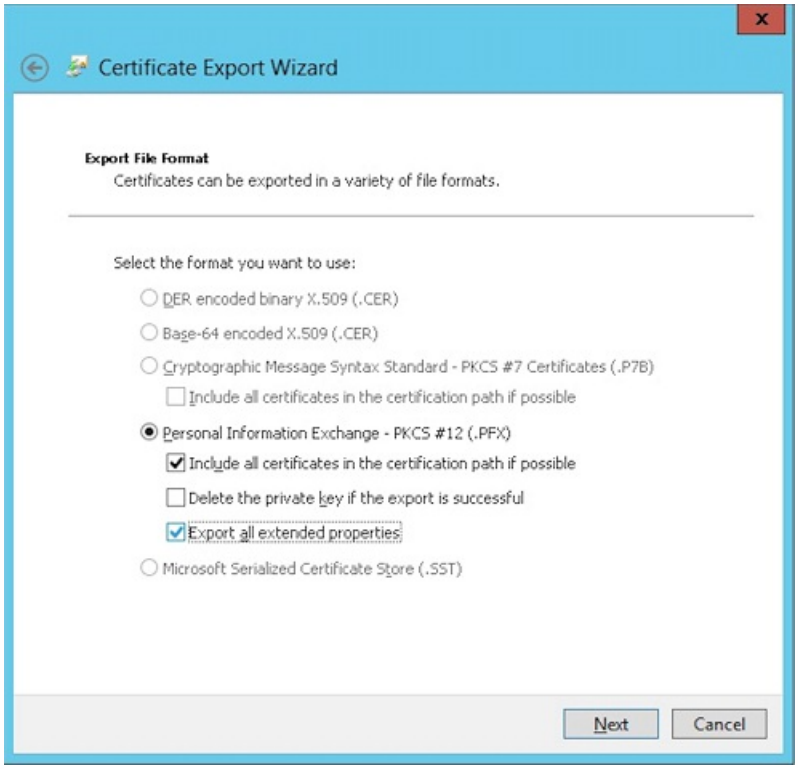
7. Exportieren Sie die PFX-Datei, die Sie im vorherigen Schritt erstellt haben.



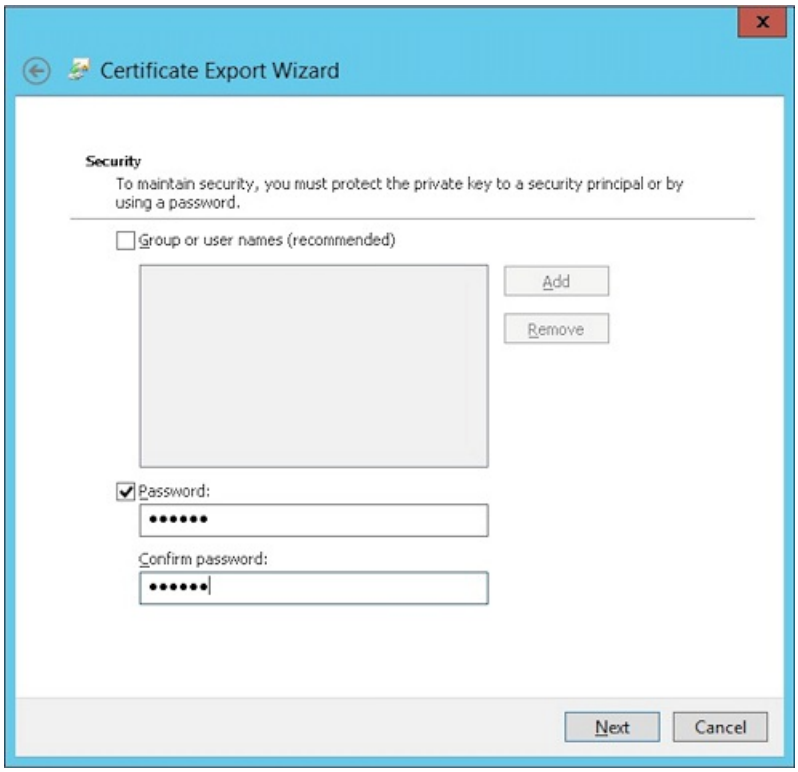
8. Klicken Sie auf **Ja, privaten Schlüssel exportieren**.



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.

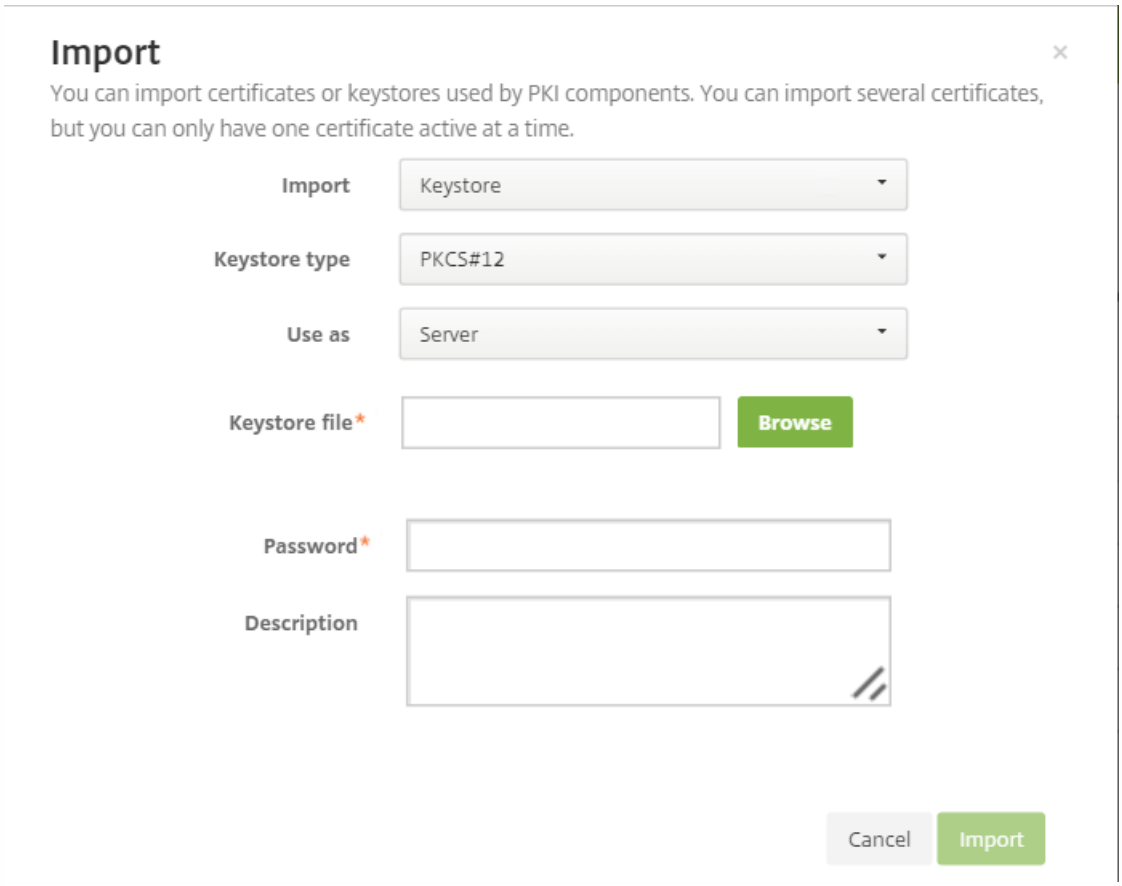
Hochladen des Zertifikats in XenMobile

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.



4. Klicken Sie auf **Importieren**.

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

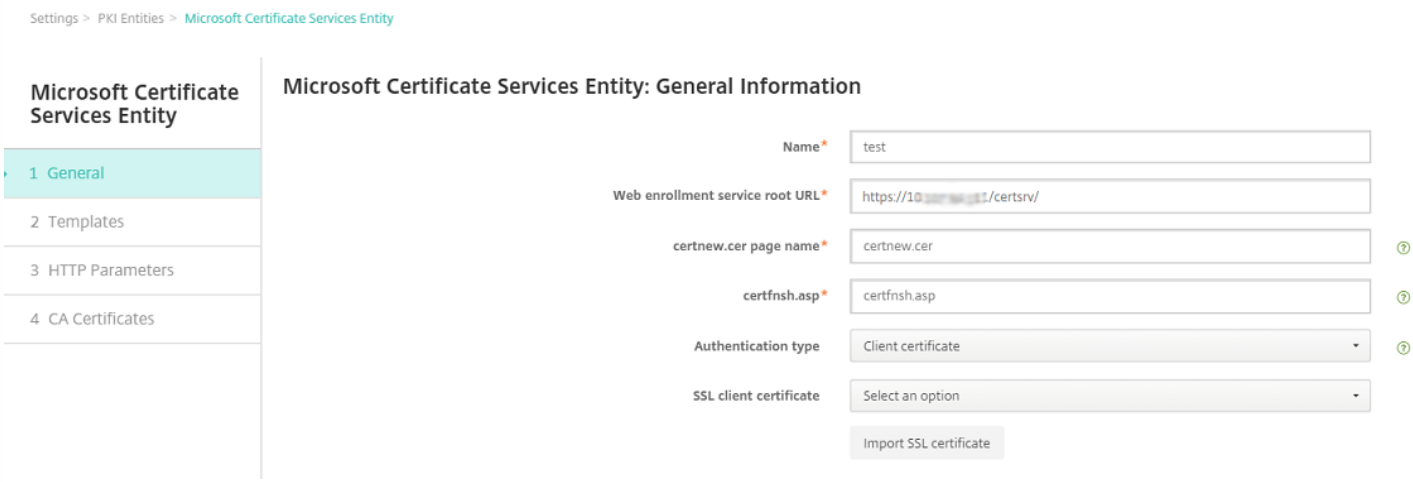
Erstellen der PKI-Entität für die zertifikatbasierte Authentifizierung

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

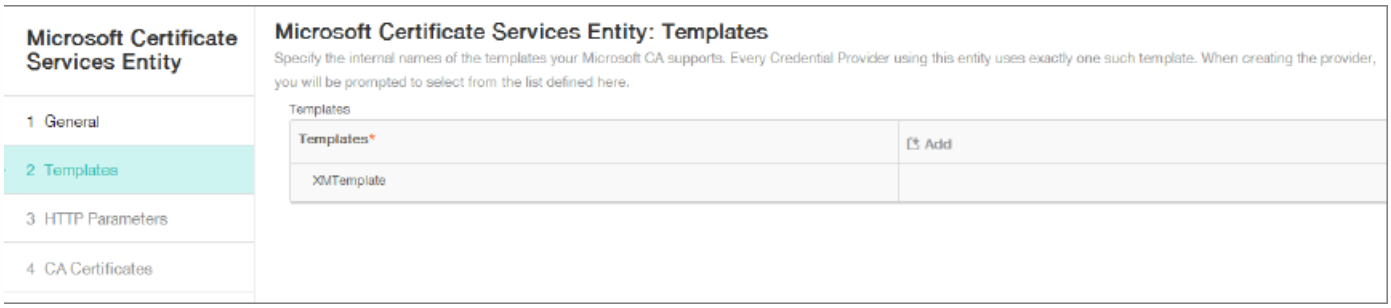
2. Klicken Sie auf **Hinzufügen** und dann auf **Microsoft Zertifikatdiensteentität**. Der Bildschirm **Microsoft Zertifikatdiensteentität: Allgemeine Informationen** wird angezeigt.

3. Geben Sie die folgenden Parameter ein:

- **Name**: Geben Sie einen Namen ein.
- **Stamm-URL des Webregistrierungsdiensts**: https://RootCA-URL/certsrv/
  Achten Sie darauf, den letzten Schrägstrich (/) im URL-Pfad hinzuzufügen.
- **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.

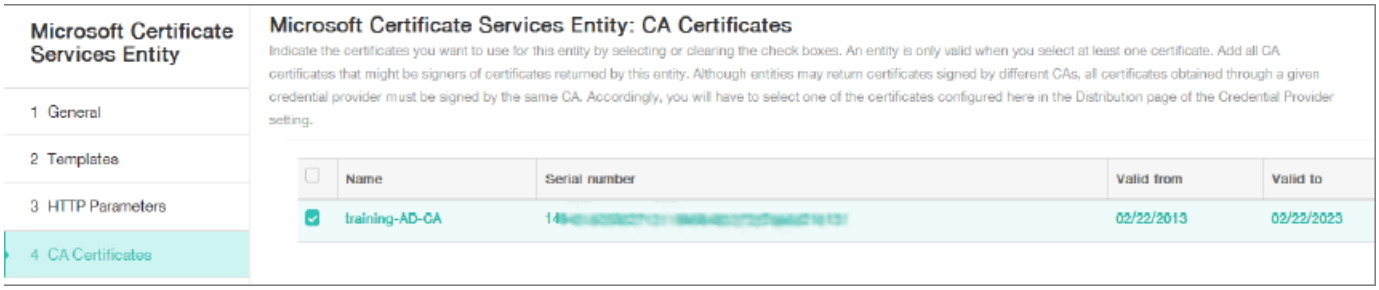


4. Fügen Sie unter **Vorlagen** die Vorlage hinzu, die Sie beim Konfigurieren des Microsoft-Zertifikats erstellt haben. Leerstellen sind nicht zulässig.



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**.

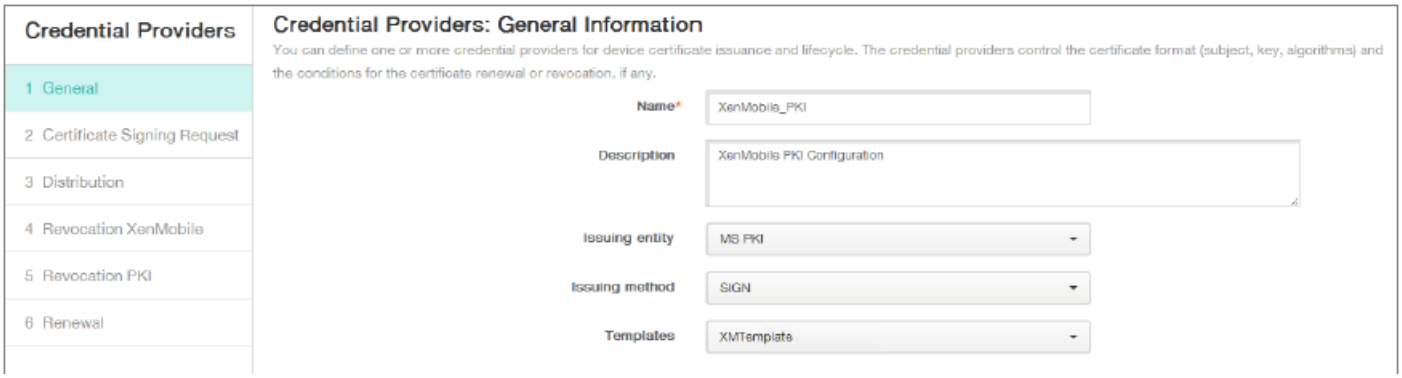
Konfigurieren der Anmeldeinformationsanbieter

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.

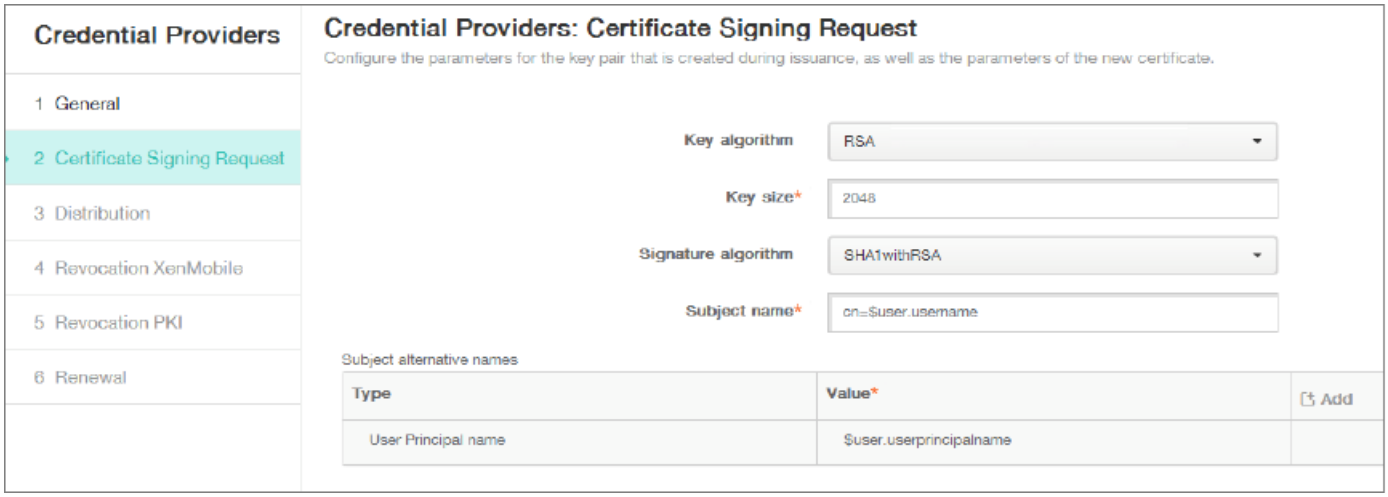


4. Klicken Sie auf **Zertifikatsignieranforderung** und geben Sie die folgenden Parameter ein:

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

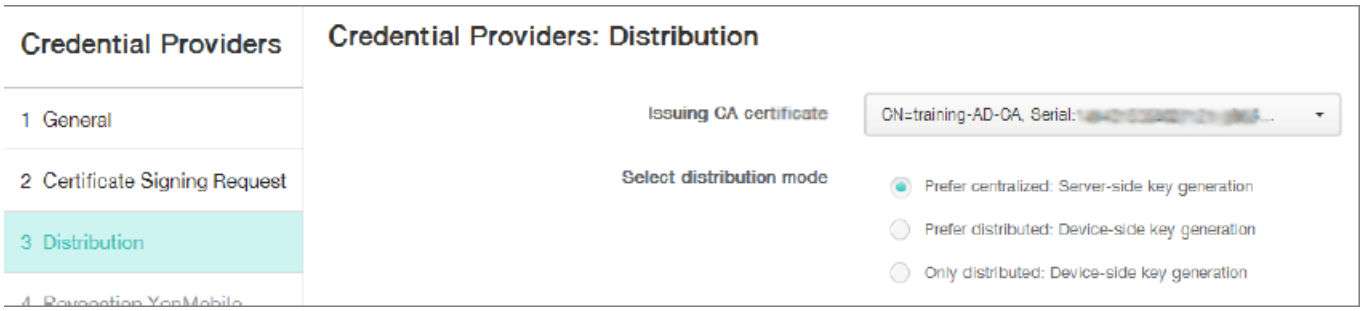
Klicken Sie für **Alternative Antragstellernamen** auf **Hinzufügen** und geben Sie die folgenden Parameter ein:

- **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**.

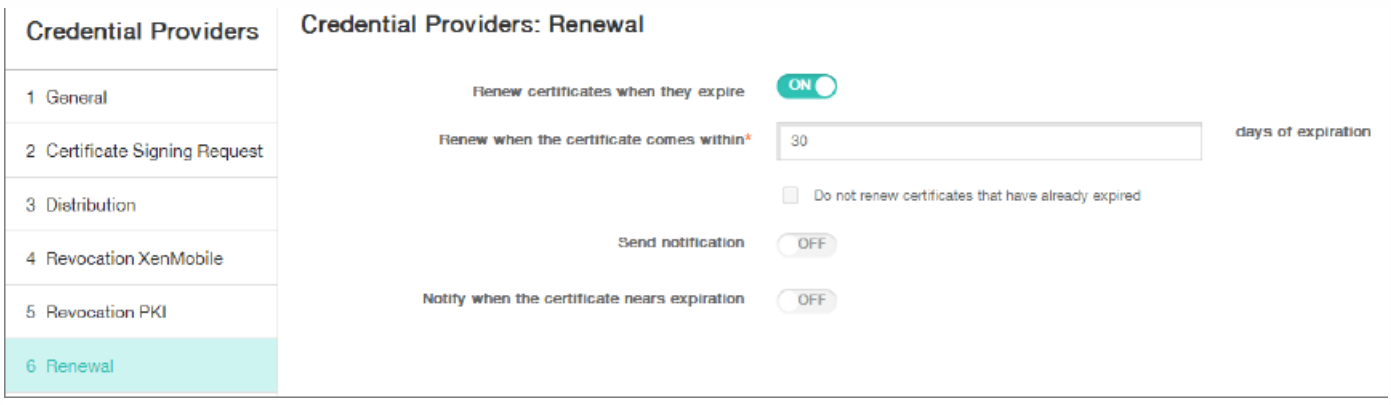


6. Legen Sie für die zwei folgenden Abschnitte **XenMobile-Sperrung** und **PKI-Sperrung** die Parameter nach Bedarf fest. Die beiden Optionen werden in diesem Artikel übersprungen.

7. Klicken Sie auf **Verlängerung**.

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

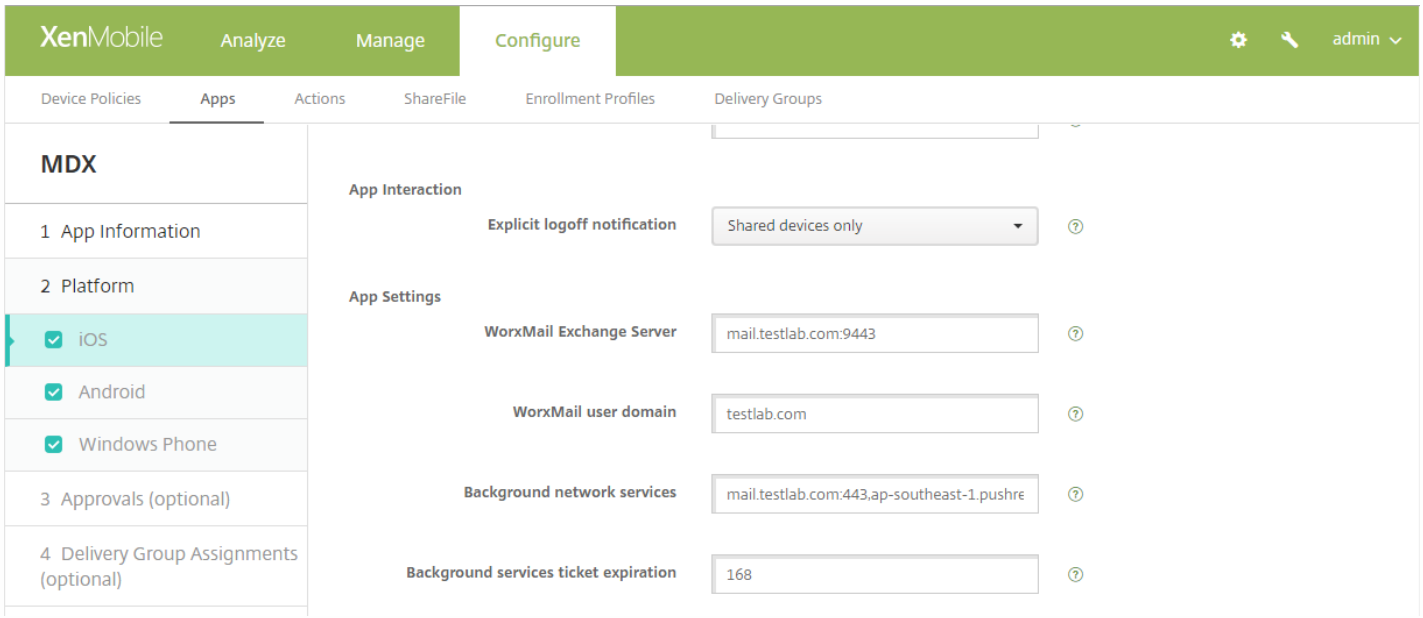
9. Behalten Sie für alle anderen Einstellungen die Standardwerte bei oder ändern Sie sie nach Bedarf.



10. Klicken Sie auf **Speichern**.

Konfigurieren von Secure Mail für die zertifikatbasierte Authentifizierung

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



Konfigurieren der NetScaler-Zertifikatbereitstellung in XenMobile

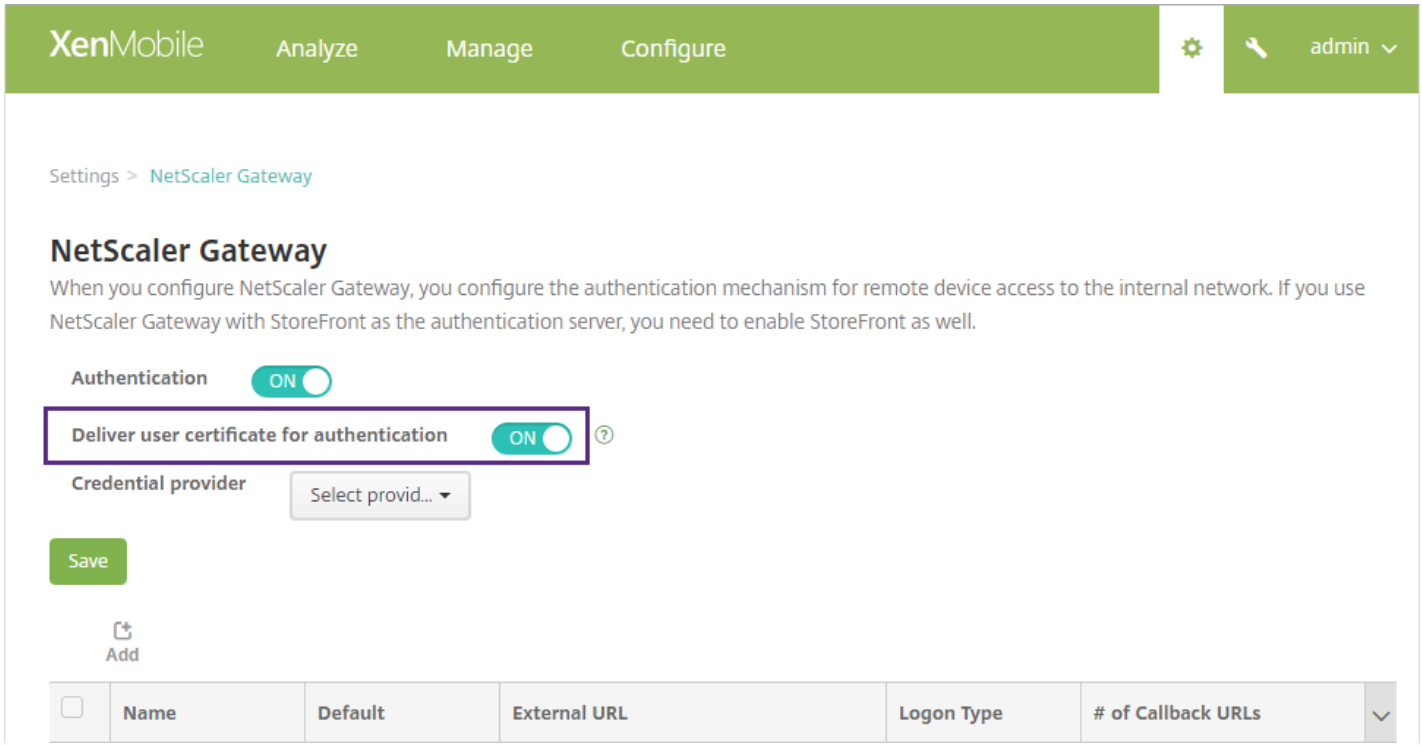
1. Melden Sie sich bei der XenMobile-Konsole an und klicken Sie auf das Zahnradsymbol rechts oben. Der Bildschirm **Einstellungen** wird angezeigt.

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:

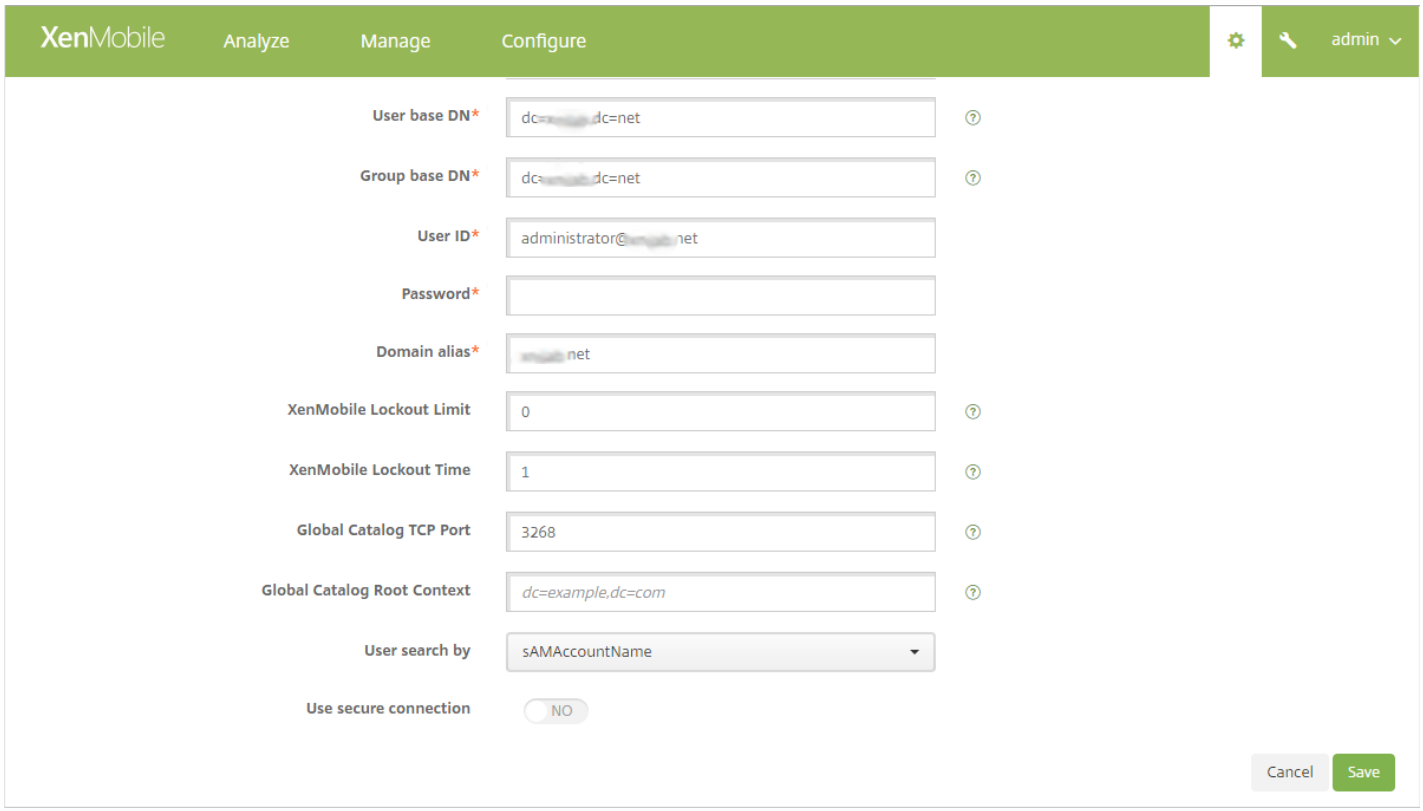
- Externe URL: **https://URLIhresNetScalerGateways**
- **Anmeldetyp**: Zertifikat
- **Kennwort erforderlich**: AUS
- **Als Standard setzen**: EIN

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 und 10

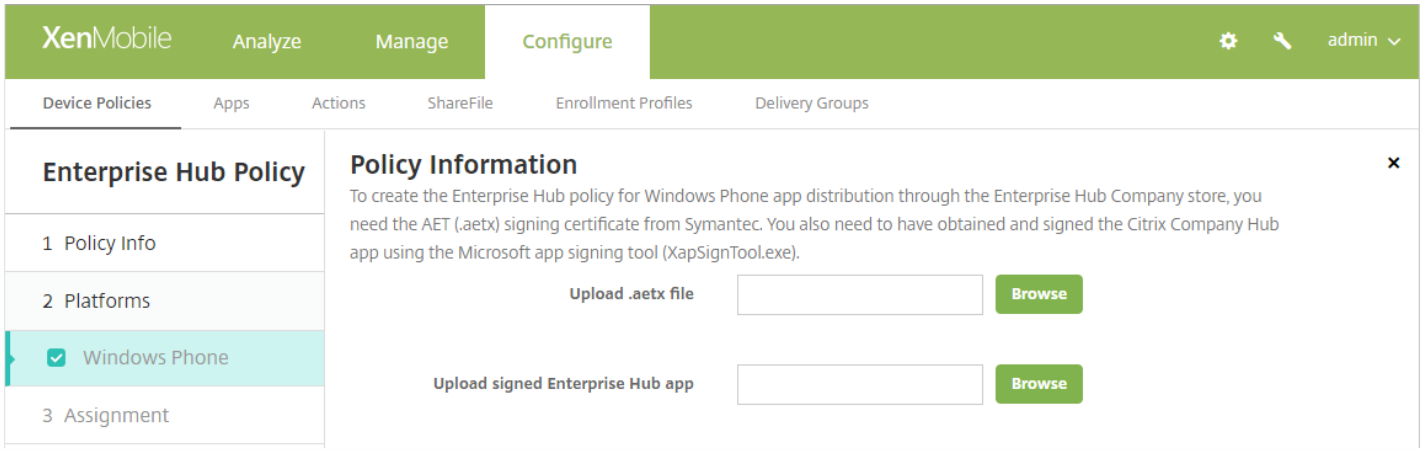
Für Windows Phone-Geräte müssen Sie eine Enterprise Hub-Richtlinie zum Bereitstellen der AETX-Datei und des Secure Hub-Clients erstellen.

> **Hinweis**
>
> Vergewissern Sie sich, dass für die AETX- und die Secure Hub-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 > Gerätерichtlinien**.

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 Secure Hub-App für den Enterprise Hub aus.



4. Weisen Sie die Richtlinie Bereitstellungsgruppen zu und speichern Sie sie.

Problembehandlung bei der Clientzertifikatkonfiguration

Wenn die Konfiguration wie oben beschrieben erfolgt ist und auch NetScaler Gateway konfiguriert wurde, sieht der Workflow für Benutzer folgendermaßen aus:

1. Der Benutzer registriert sein mobiles Gerät.

2. XenMobile fordert den Benutzer auf, eine Citrix PIN zu erstellen.

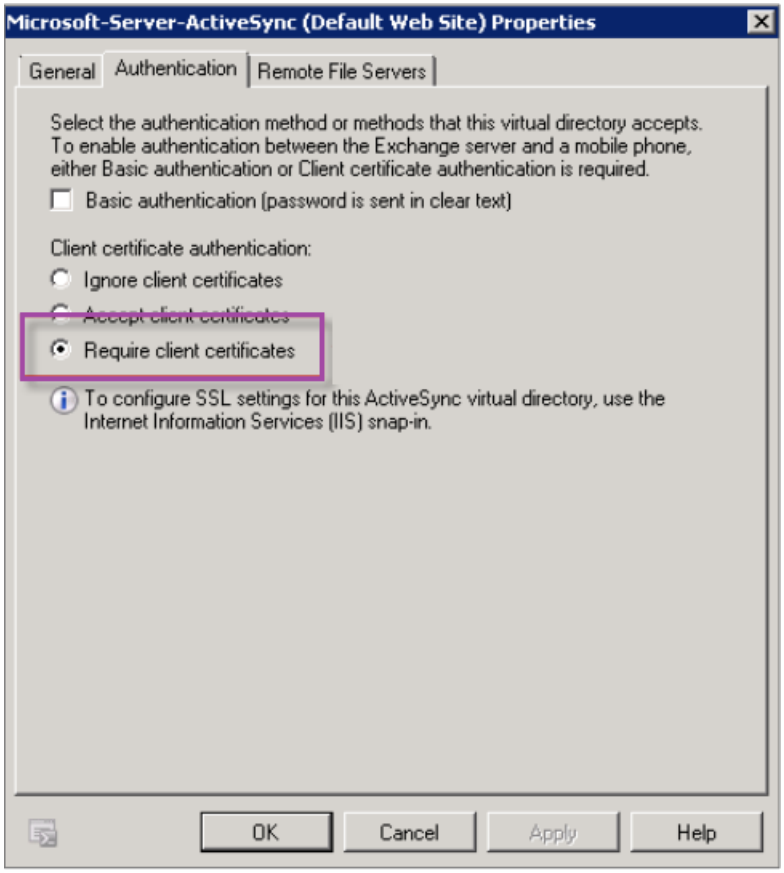
3. Der Benutzer wird an den XenMobile Store weitergeleitet.

4. Wenn der Benutzer Secure Mail für iOS, Android oder Windows Phone 8.1 startet, wird er nicht zur Eingabe von Anmeldeinformationen zum Konfigurieren des Postfachs aufgefordert. Stattdessen fordert Secure Mail das Clientzertifikat aus Secure Hub an und sendet es zur Authentifizierung an Microsoft Exchange Server. Wenn XenMobile beim Starten von Secure Mail durch die Benutzer die Eingabe von Anmeldeinformationen anfordert, prüfen Sie die Konfiguration.

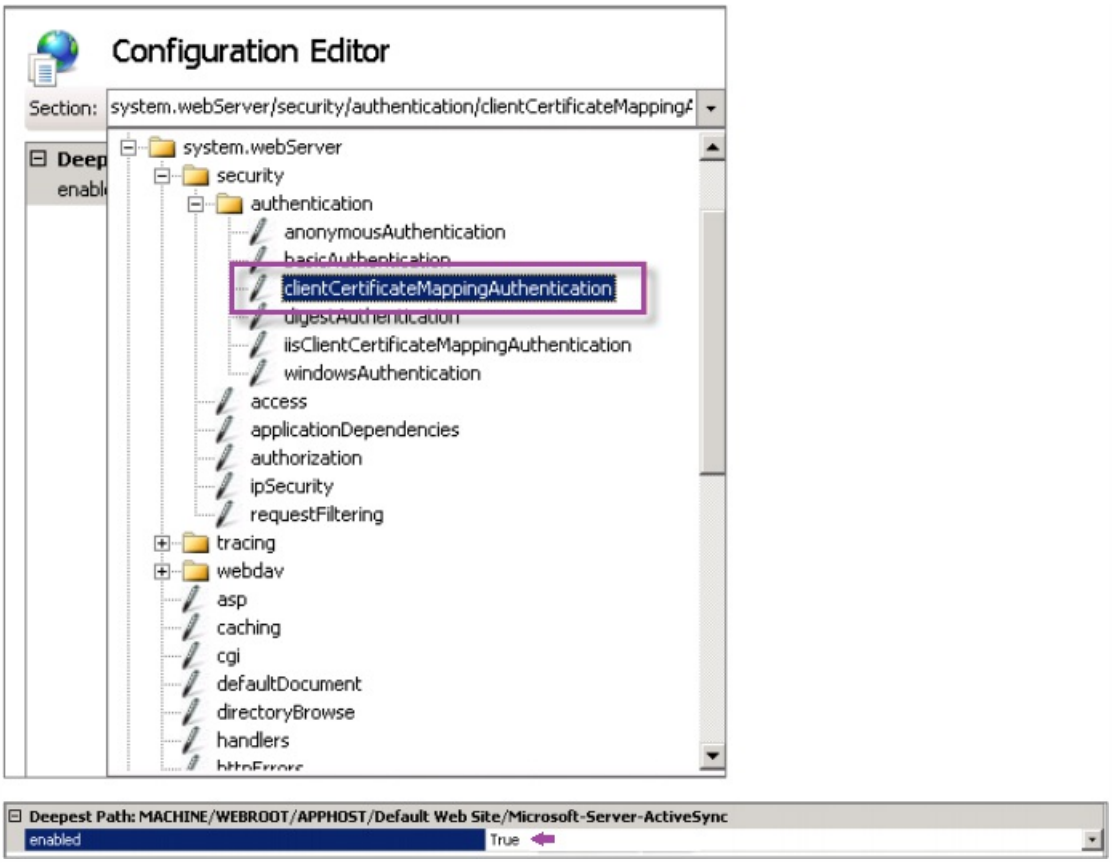
Wenn die Benutzer Secure Mail herunterladen und installieren können, die Postfachkonfiguration jedoch nicht abgeschlossen werden kann, führen Sie folgende Schritte aus:

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 finden Sie 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 Secure Mail 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 Secure Hub-Apps verwendet wird.
- Vergewissern Sie sich, dass zum Signieren und Umschließen von Secure Hub, Secure Mail und Anwendungsregistrierungstoken die gleiche Aussteller-ID verwendet wird.

PKI-Entitäten

Feb 24, 2017

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

XenMobile unterstützt folgende Arten von PKI-Entitäten:

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

XenMobile unterstützt die folgenden Zertifizierungsstellenserver:

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

Allgemeine PKI-Konzepte

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

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

Informationen über Zertifizierungsstellenzertifikate

Beim Konfigurieren einer PKI-Entität müssen Sie in XenMobile angeben, welches 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.

Generic PKI

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

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

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

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

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

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

Hinzufügen einer GPKI

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.
- **Keine**
- **HTTP Basic**: Geben Sie den Benutzernamen und das 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.

Microsoft Zertifikatdienste

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

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

Hinzufügen einer Microsoft-Zertifikatdienste-Entität

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 den Anforderungen für Microsoft Zertifikatdienste-Vorlagen finden Sie in der Microsoft-Dokumentation zu Ihrer Windows Server-Version. In XenMobile gelten außer den unter "Zertifikate" aufgeführten Regeln für Zertifikatformate keine weiteren Anforderungen für die von XenMobile verteilten 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.

NetScaler-Zertifikatsperrliste

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.

Eigenverwaltete Zertifizierungsstellen

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

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

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

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

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

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

Hinzufügen von eigenverwalteten Zertifizierungsstellen

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

Feb 24, 2017

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

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

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

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

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

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

Methoden der Zertifikatausstellung

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

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

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

Zertifikatbereitstellung

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

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

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

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

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

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

Die folgende Tabelle zeigt die SCEP-Verteilung in XenMobile:

Kontext	**SCEP unterstützt**	**SCEP erforderlich**
iOS-Profildienst	Ja	Ja
Registrierung für die iOS-Mobilgeräteverwaltung	Ja	Nein
iOS-Konfigurationsprofile	Ja	Nein
SHTP-Registrierung	Nein	Nein
Konfigurieren von SHTP	Nein	Nein
Windows Phone/-Tablet-Registrierung	Nein	Nein
Windows Phone/-Tablet-Konfiguration	Nein, außer für die WiFi-Geräterichtlinie, die für Windows Phone 8.1 unterstützt wird, und die neueste Version von Windows 10	Nein

Kontext	SCEP unterstützt	SCEP erforderlich

Zertifikatsperre

Es gibt drei Arten der Sperre.

- **Interne Sperre**: Die interne Sperre wirkt sich auf den von XenMobile gepflegten Zertifikatstatus aus. Dieser Status wird berücksichtigt, wenn XenMobile ein eingehendes Zertifikat auswertet oder OCSP-Statusinformationen für ein Zertifikat bereitstellen muss. Die Konfiguration des Anmeldeinformationsanbieters bestimmt, wie sich diverse Bedingungen auf diesen Status auswirken. Beispielsweise kann durch den Anmeldeinformationsanbieter festgelegt sein, dass über den Zertifikatanbieter abgerufene Zertifikate als gesperrt gekennzeichnet werden, wenn sie vom Gerät gelöscht wurden.
- **Extern weitergegebene Sperre**: Eine Sperrung dieser Art (auch "Revocation XenMobile") gilt für von einer externen PKI bezogene Zertifikate. Das Zertifikat wird in der PKI gesperrt, wenn es intern von XenMobile gesperrt wird, unter den in der Anmeldeinformationsanbieter-Konfiguration festgelegten Bedingungen. Der Aufruf zum Ausführen der Sperre erfordert eine Generic PKI-Entität (GPKI) mit Sperrfunktion.
- **Extern durchgeführte Sperre**: Eine Sperrung dieser Art (auch "Revocation PKI") gilt ebenfalls nur für von einer externen PKI bezogene Zertifikate. Beim Auswerten des Status von Zertifikaten fragt XenMobile diesen bei der PKI ab. Ist das Zertifikat gesperrt, wird es von XenMobile intern ebenfalls gesperrt. Bei diesen Methoden wird das OCSP-Protokoll verwendet.

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

Zertifikatverlängerung

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

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

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

Erstellen eines Anmeldeinformationsanbieters

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 "Zertifikat signieren", d. h. bei jeder Ausstellung wird von XenMobile ein neues Schlüsselpaar mit dem für die Entität ausgewählten CA-Zertifikat signiert. Ob das Schlüsselpaar auf dem Gerät oder auf dem Server generiert wird, hängt von der ausgewählten Verteilungsmethode ab.

1. Klicken Sie in der XenMobile-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 Clientzertifikatauthentifizierung **Zertifikat 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 **Ausstellendes ZS-Zertifikat** 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 aus:
  - **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 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 Zertifikatantragstellers. **Hinweis:** Sie können XenMobile-Makros für Werte im DN-Feld verwenden. Beispiel: CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation
- 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. Wenn Zertifikate bei Ablauf verlängert werden sollen, legen Sie auf der Seite **Anbieter für Anmeldeinformationen: Verlängerung** für **Zertifikate erneuern, wenn sie ablaufen** die Option **Ein** fest.

Zusätzliche Felder werden eingeblendet.

- Geben Sie im Feld **Zertifikat erneuern, wenn es 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.

APNs-Zertifikate

Apr 24, 2017

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 diesem Abschnitt enthalten in der Reihenfolge ihrer Auflistung grundlegende Informationen zu den Verfahren :

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

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

Informationen zur Apple MDM-Pushzertifikatmigration

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

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

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

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

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

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

Erstellen einer Zertifikatsignieranforderung mit Microsoft IIS

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

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

Erstellen einer Zertifikatsignieranforderung auf einem Macintosh-Computer

1. Starten Sie auf einem Computer mit Mac OS X unter **Anwendungen** > **Dienstprogramme** die Anwendung Keychain Access.
2. Öffnen Sie das Menü **Keychain Access** und klicken Sie auf **Preferences**.
3. Ändern Sie auf der Registerkarte **Certificates** die Einstellung für **OCSP** und **CRL** in **Off** und schließen Sie das Fenster "Preferences".
4. Klicken Sie im Menü **Keychain Access** 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-E-Mail-Adresse**: 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 Zertifikatassistenten abgeschlossen ist.

Erstellen einer Zertifikatsignieranforderung mit Open SSL

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

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

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

2. Die folgende Meldung bezüglich der Informationen für die Zertifikatbenennung wird angezeigt. Geben Sie die Informationen wie angefordert ein.
   Sie werden zur Eingabe von Informationen aufgefordert, die in Ihre
   Zertifikatanforderung aufgenommen werden.
   Bei der angeforderten Information handelt es sich um einen Distinguished Name (DN).
   Nicht alle angezeigten Felder müssen ausgefüllt werden.
   Bestimmte Felder enthalten einen Standardwert.
   Wenn Sie '.' eingeben, bleibt das Feld leer.

   Ländername (Code aus 2 Buchstaben) [AU]:US
   Staat oder Provinz (vollständiger Name) [Some-State]:CA
   Ortsname (z. B. Stadt) []:RWC
   Organisationsname (z. B. Unternehmen) [Internet Widgits Pty Ltd]:Kunde
   Organisationseinheitsbezeichnung (z. B. Abteilung) []:Marketing
   Allgemeiner Name (z. B IHR Name) []:John Doe
   E-Mail-Adresse []:john.doe@customer.com

3. Geben Sie bei der nächsten Meldung ein Kennwort für den privaten CSR-Schlüssel ein.
   Geben Sie die folgenden zusätzlichen Attribute
   ein, die mit der Zertifikatanforderung gesendet werden.
   Ein Anfragekennwort []:
   Ein optionaler Unternehmensname []:

4. Senden Sie die CSR an Citrix.

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

Signieren der Zertifikatsignieranforderung (CSR)

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

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

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

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

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

Hinweis: Es gibt Berichte über Probleme mit der Anmeldung beim Apple Push 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 **Abbrechen** und führen Sie den Download über das nächste Fenster aus.

Erstellen eines PFX-Zertifikats für APNs mit Microsoft IIS

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

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

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

4. Navigieren Sie zu der Datei Certificate.pem von Apple. Geben Sie dann 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 **Schlüsselspeicher**.
13. Wählen Sie unter **Verwenden als** die Option **APNs** aus.
14. Wählen Sie unter **Schlüsselspeicher** die zu importierende Schlüsselspeicherdatei aus, indem Sie auf **Durchsuchen** klicken und zum Speicherort der Datei navigieren.
15. Geben Sie unter **Kennwort** das Kennwort für das Zertifikat ein.
16. Klicken Sie auf **Importieren**.

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

1. Suchen Sie auf dem Macintosh-Computer mit Mac OS X, auf dem Sie die Zertifikatsignieranforderung erstellt haben, das von Apple erhaltene PEM-Zertifikat.
2. Doppelklicken Sie auf die Zertifikatdatei, um sie in die Schlüsselsammlung zu importieren.
3. Wenn Sie aufgefordert werden, das Zertifikat einer bestimmten Schlüsselsammlung hinzuzufügen, behalten Sie die standardmäßig angezeigte Anmeldeschlüsselsammlung bei und klicken Sie dann auf **OK**. Das neu hinzugefügte Zertifikat wird nun in der Liste der Zertifikate angezeigt.
4. Klicken Sie auf das Zertifikat und dann im Menü **Datei** auf **Exportieren**, um das Zertifikat 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 das PFX-Dateiformat 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, die Sie zum Generieren der Zertifikatsignieranforderung und Exportieren des Zertifikats verwendet haben, nicht beibehalten möchten, empfiehlt Citrix, den privaten und öffentlichen Schlüssel zu speichern und aus dem lokalen System zu exportieren. Ansonsten wird der Zugriff auf APNs-Zertifikate zur Wiederverwendung ungültig und Sie müssen das gesamte Verfahren zum Erstellen von Zertifikatsignieranforderung und APNs-Zertifikat wiederholen.

Erstellen eines PFX-Zertifikats für APNs mit OpenSSL

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

1. Führen Sie an einer Eingabeaufforderung oder Shell folgenden Befehl aus:
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12

2. Geben Sie ein Kennwort für die PFX-Datei ein. Merken Sie sich das Kennwort, denn Sie benötigen es erneut, wenn Sie das Zertifikat in XenMobile hochladen.
3. Notieren Sie den Speicherort der PFX-Zertifikatdatei und kopieren Sie die Datei auf den XenMobile-Server, damit Sie sie mit der XenMobile-Konsole hochladen können.

Importieren eines APNs-Zertifikats in XenMobile

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

1. 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 **Schlüsselspeicher**.
5. Wählen Sie unter **Verwenden als** die Option **APNs** aus.
6. Navigieren Sie zu der P12-Datei auf Ihrem Computer.
7. Geben Sie ein Kennwort ein und klicken Sie auf **Importieren**.

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

Erneuern eines APNs-Zertifikats

Zum Erneuern eines APNs-Zertifikats führen Sie dieselben Schritte aus wie beim Erstellen eines Zertifikats. Anschließend laden Sie das neue Zertifikat über das 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 Verlängern 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. Stellen Sie beim Verlängern des Zertifikats sicher, dass Sie denselben Unternehmensnamen und dieselbe Apple-ID verwenden.

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

1. Generieren Sie eine Zertifikatsignieranforderung mit Microsoft Internetinformationsdienste (IIS).
2. Laden Sie die neue CSR auf die Website XenMobile APNs CSR Signing hoch und klicken Sie dann auf **Sign**.
3. Senden Sie die signierte Zertifikatsignieranforderung über das 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 auf das Zahnradsymbol rechts oben in der Konsole. 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 **Schlüsselspeicher**.
10. Wählen Sie unter **Verwenden als** die Option **APNs** aus.
11. Navigieren Sie zu der P12-Datei auf Ihrem Computer.
12. Geben Sie ein Kennwort ein und klicken Sie auf **Importieren**.

SAML für Single Sign-On bei ShareFile

Feb 24, 2017

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 Secure Hub 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 Secure Mail-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" des XenMobile-Bereitstellungshandbuchs.

Voraussetzungen

Damit Sie Single Sign-On für XenMobile und ShareFile-Apps konfigurieren können, müssen die folgenden Voraussetzungen erfüllt sein:

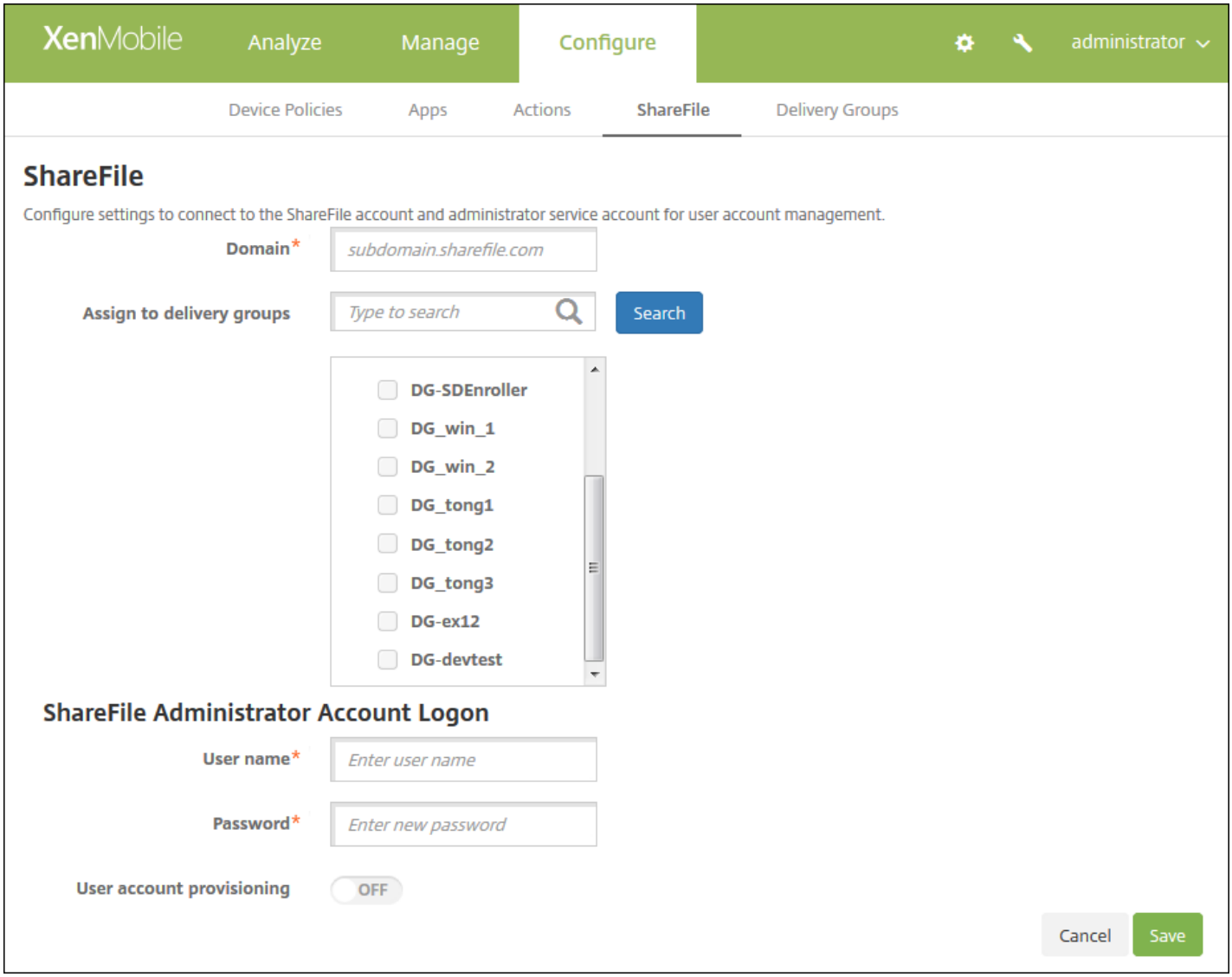
- MDX Toolkit Version 9.0.4 oder höher (für mobile ShareFile-Apps)
- Erforderliche mobile ShareFile-Apps:
  - ShareFile für iPhone Version 3.0.x
  - ShareFile für iPad Version 2.2.x
  - ShareFile für Android Version 3.2.x
- Secure Hub 9.0 (für ShareFile Mobile-Apps): Installieren Sie nach Bedarf die Version für iOS bzw. Android.
- ShareFile-Administratorkonto

Stellen Sie sicher, dass XenMobile und ShareFile eine Verbindung herstellen können.

Konfigurieren des ShareFile-Zugriffs

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**.

Einrichten von SAML für umschlossene ShareFile MDX-Apps

Die folgenden Schritte gelten für iOS- und Android-Apps und -Geräte.

1. Umschließen Sie die mobile ShareFile-App mit dem MDX Toolkit. Informationen 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 in dem o. a. Arbeitsgang konfiguriert 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 Secure Hub auf dem Benutzergerät.

2. Laden Sie die mobile ShareFile-App aus dem XenMobile Store herunter und installieren Sie sie.

3. Starten Sie die mobile ShareFile-App. ShareFile wird ohne Anforderung von Benutzernamen und Kennwort gestartet.

Überprüfung mit Secure Mail

1. Falls noch nicht geschehen, installieren und konfigurieren Sie Secure Hub auf dem Benutzergerät.

2. Laden Sie Secure Mail aus dem XenMobile Store herunter, installieren und konfigurieren Sie es.

3. Öffnen Sie ein neues E-Mail-Formular und tippen Sie auf **Von ShareFile anfügen**. Die zum Anfügen verfügbaren Dateien werden ohne Anforderung von Benutzernamen und Kennwort angezeigt.

Konfigurieren von NetScaler Gateway für andere ShareFile-Clients

Wenn Sie den Zugriff für nicht umschlossene ShareFile-Clients (z. B. Website, Outlook-Plug-In oder Synchronisierungsclients) konfigurieren möchten, müssen Sie NetScaler Gateway folgendermaßen konfigurieren, damit es die Verwendung von XenMobile als SAML-Identitätsanbieter unterstützt:

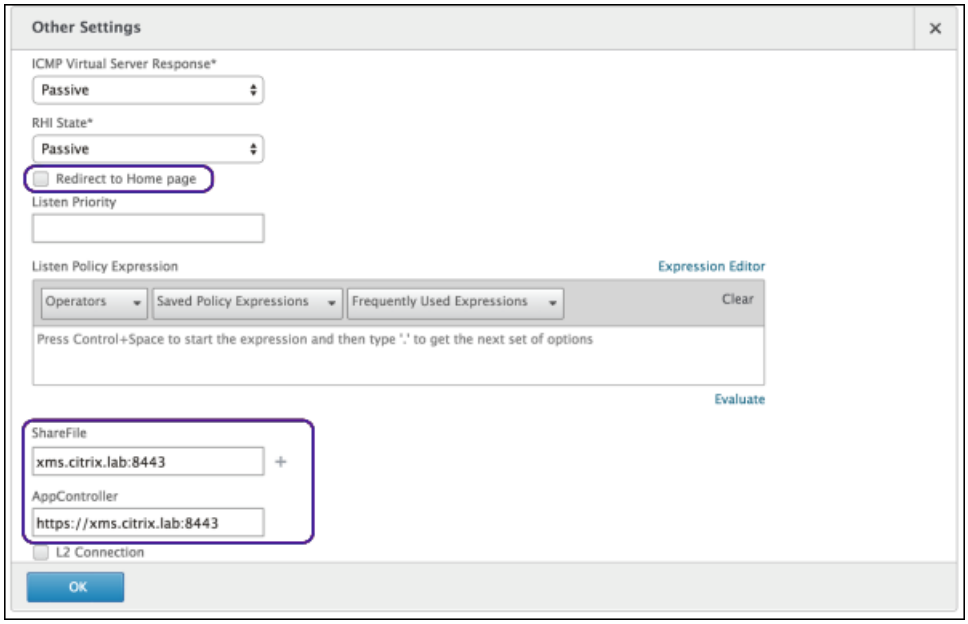
- Deaktivieren Sie die Homepageumleitung.
- Erstellen Sie eine ShareFile-Sitzungsrichtlinie und ein Profil.
- Konfigurieren Sie Richtlinien auf dem virtuellen NetScaler Gateway-Server.

Deaktivieren der Homepageumleitung

Sie müssen die Standardverarbeitung von Anforderungen, die über den /cginfra-Pfad eingehen, deaktivieren, damit den Benutzern die ursprüngliche angeforderte interne URL anstelle der konfigurierten Homepage angezeigt wird.

1. Bearbeiten Sie die Einstellungen für den virtuellen NetScaler Gateway-Server, der für XenMobile-Anmeldungen verwendet

wird. Navigieren Sie in NetScaler 10.5 zu **Other Settings** und deaktivieren Sie das Kontrollkästchen **Redirect to Home Page**.



2. Geben Sie unter **ShareFile** den internen Namen des XenMobile-Servers und die Portnummer ein.

3. Geben Sie unter **AppController** die XenMobile-URL ein.

Mit dieser Konfiguration werden Anforderungen an die über den /cginfra-Pfad eingegebene URL genehmigt.

Erstellen einer ShareFile-Sitzungsrichtlinie und eines Anforderungsprofils

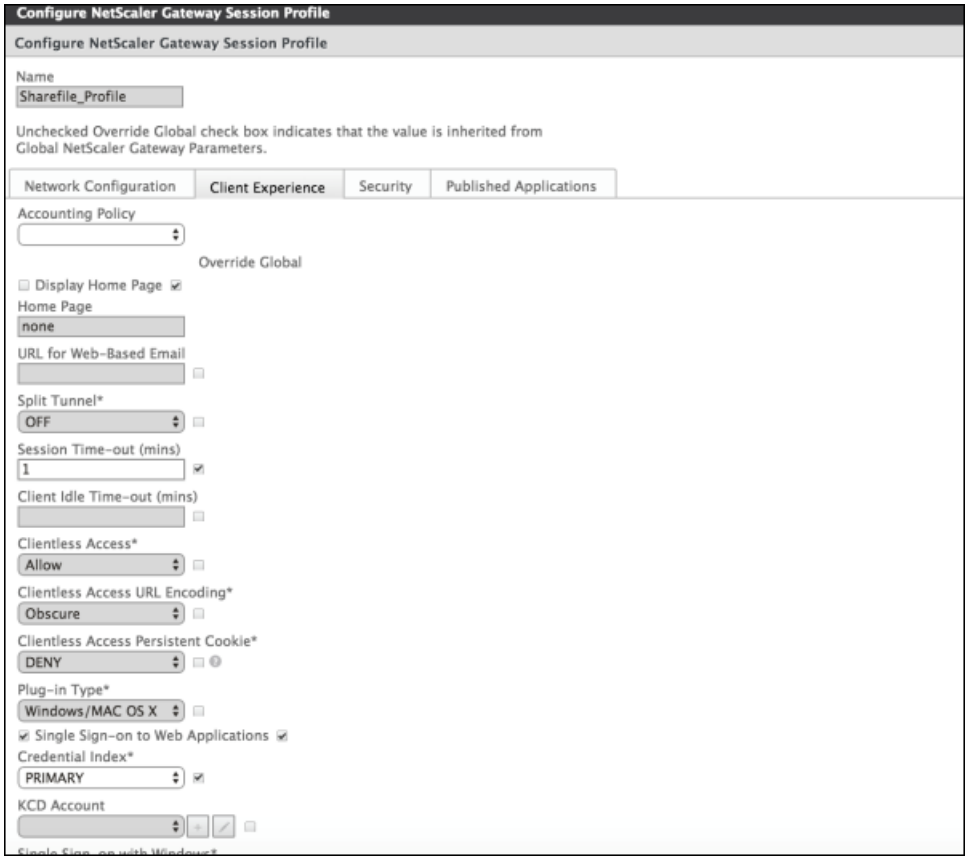
Konfigurieren Sie die folgenden Einstellungen zum Erstellen einer ShareFile-Sitzungsrichtlinie und eines Anforderungsprofils:

1. Klicken Sie im Konfigurationsprogramm für NetScaler Gateway im linken Navigationsbereich auf **NetScaler Gateway > Policies > Session**.

2. Erstellen Sie eine neue Sitzungsrichtlinie. Klicken Sie auf der Registerkarte **Policies** auf **Add**.

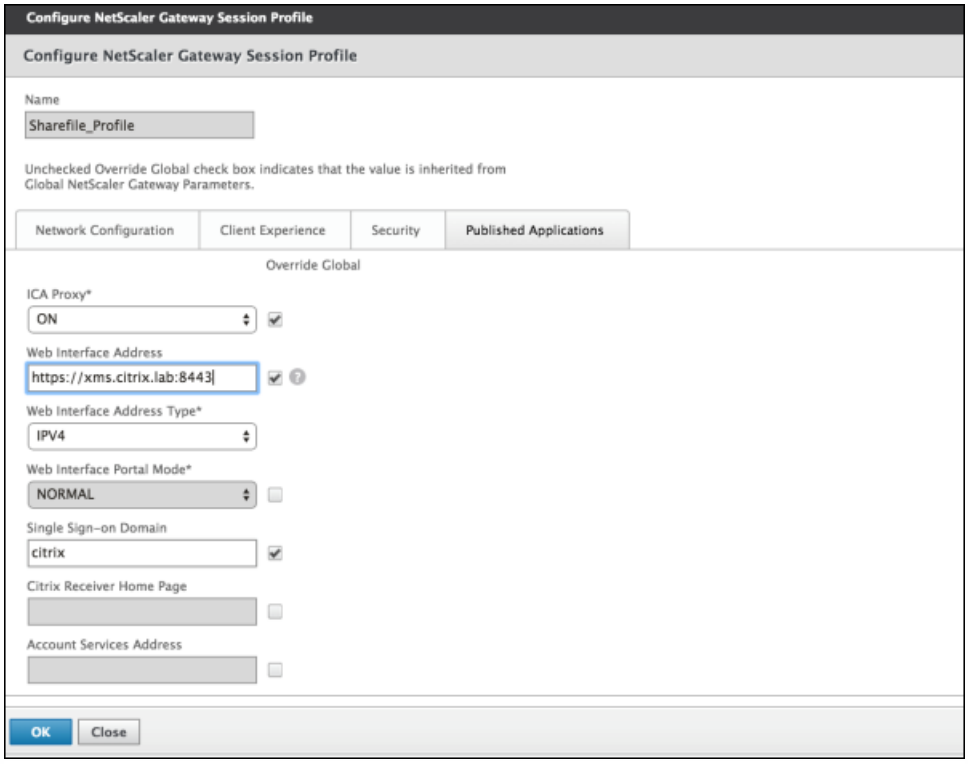
3. Geben Sie im Feld **Name** den Ausdruck **ShareFile_Policy** ein.

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**.



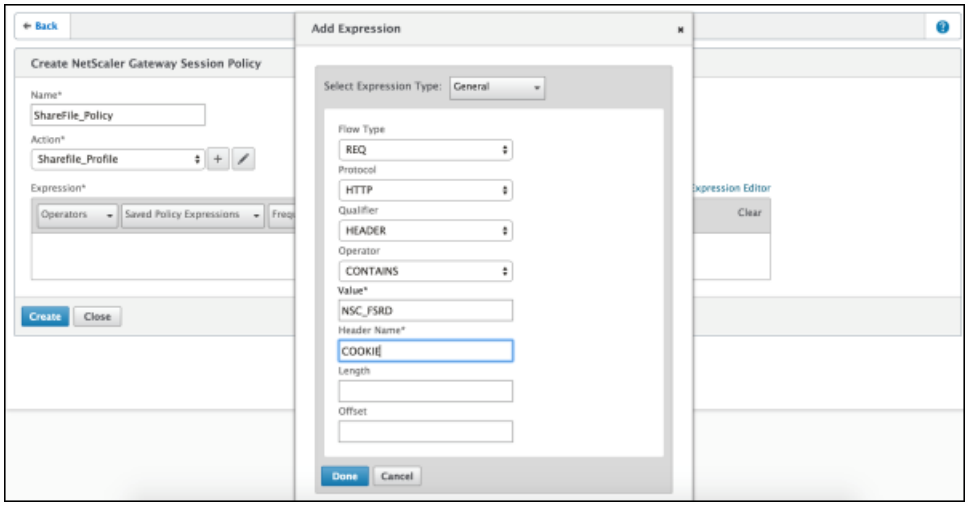
Konfigurieren Sie folgende Einstellungen:

- **ICA Proxy**: Klicken Sie in der Liste auf **ON**.
- **Web Interface Address**: Geben Sie die URL des XenMobile-Servers ein.
- **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**.

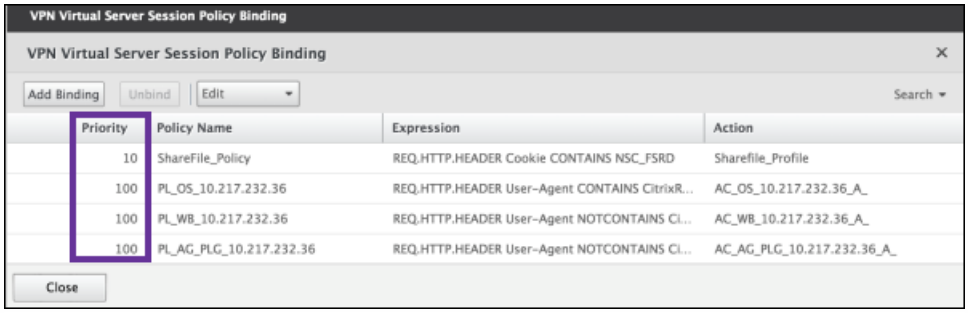
2. Klicken Sie im Bereich **Details** auf den virtuellen NetScaler Gateway-Server.

3. Klicken Sie auf **Bearbeiten**.

4. Klicken Sie auf **Configured policies > Session policies** und dann auf **Add binding**.

5. Wählen Sie **ShareFile_Policy** aus.

6. Bearbeiten Sie die automatisch generierte Prioritätszahl unter **Priority** für die ausgewählte Richtlinie so, dass sie die höchste Priorität (die niedrigste Zahl) vor allen anderen aufgeführten Richtlinien hat (siehe folgende Abbildung).



7. Klicken Sie auf **Done** und speichern Sie die ausgeführte NetScaler-Konfiguration.

Konfigurieren von SAML für ShareFile-Apps ohne MDX

Ermitteln Sie anhand der folgenden Schritte den internen App-Namen für die ShareFile-Konfiguration.

1. Melden Sie sich bei dem Verwaltungstool für XenMobile unter Verwendung der URL **https://:4443/OCA/admin/** an. Geben Sie dabei "OCA" unbedingt in Großbuchstaben ein.

2. Klicken Sie in der Liste **View** auf **Configuration**.

3. Klicken Sie auf **Applications > Applications** und notieren Sie den unter **Application Name** für die App angezeigten Namen mit dem unter **Display Name** angezeigten Anzeigenamen "ShareFile".

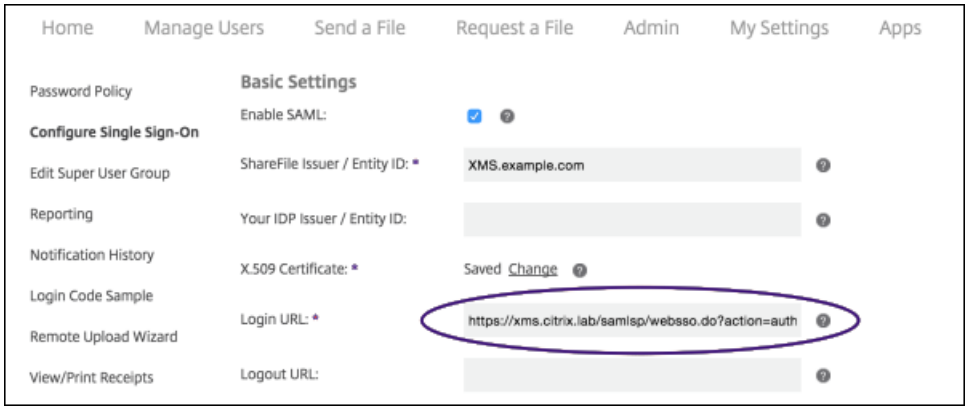
Ändern der SSO-Einstellungen für ShareFile.com

1. Melden Sie sich bei Ihrem ShareFile-Konto (https://<Unterdomäne>.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 des Verfahrens SAML für Single Sign-On bei ShareFile 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.).

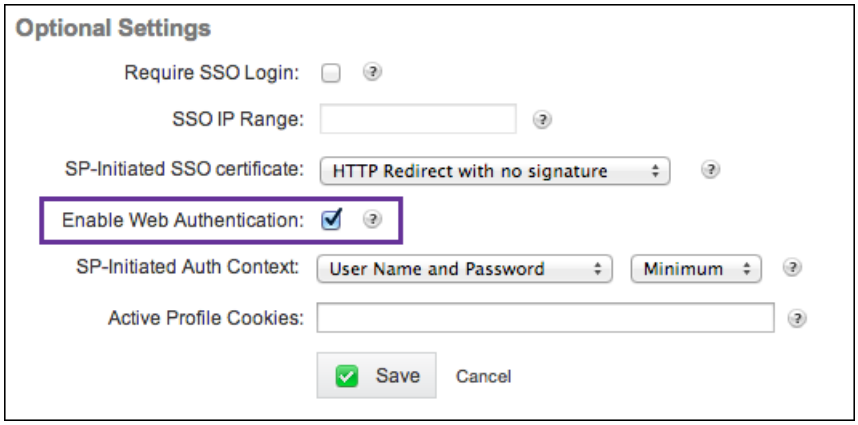
  Die URL sollte nun in etwa so aussehen:
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?
  action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

- 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 der Konfiguration

Überprüfen Sie die Konfiguration wie nachfolgend beschrieben.

1. Rufen Sie im Browser https://<subdomain>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 <Unterdomäne>.sharefile.com werden angezeigt. Wenn keine ShareFile-Ordner angezeigt werden, prüfen Sie, ob Sie die richtigen Anmeldeinformationen eingegeben haben.

Einstellungen des Microsoft Azure Active Directory-Servers

Apr 24, 2017

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 Dieses Feature ist nicht auf Windows 10-Telefonen verfügbar.
- Registrieren Sie sich bei MDM als Teil von Azure AD. Treten Sie als Teil des addinga-Arbeitskontos auf einem persönlichen Gerät bei.

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.

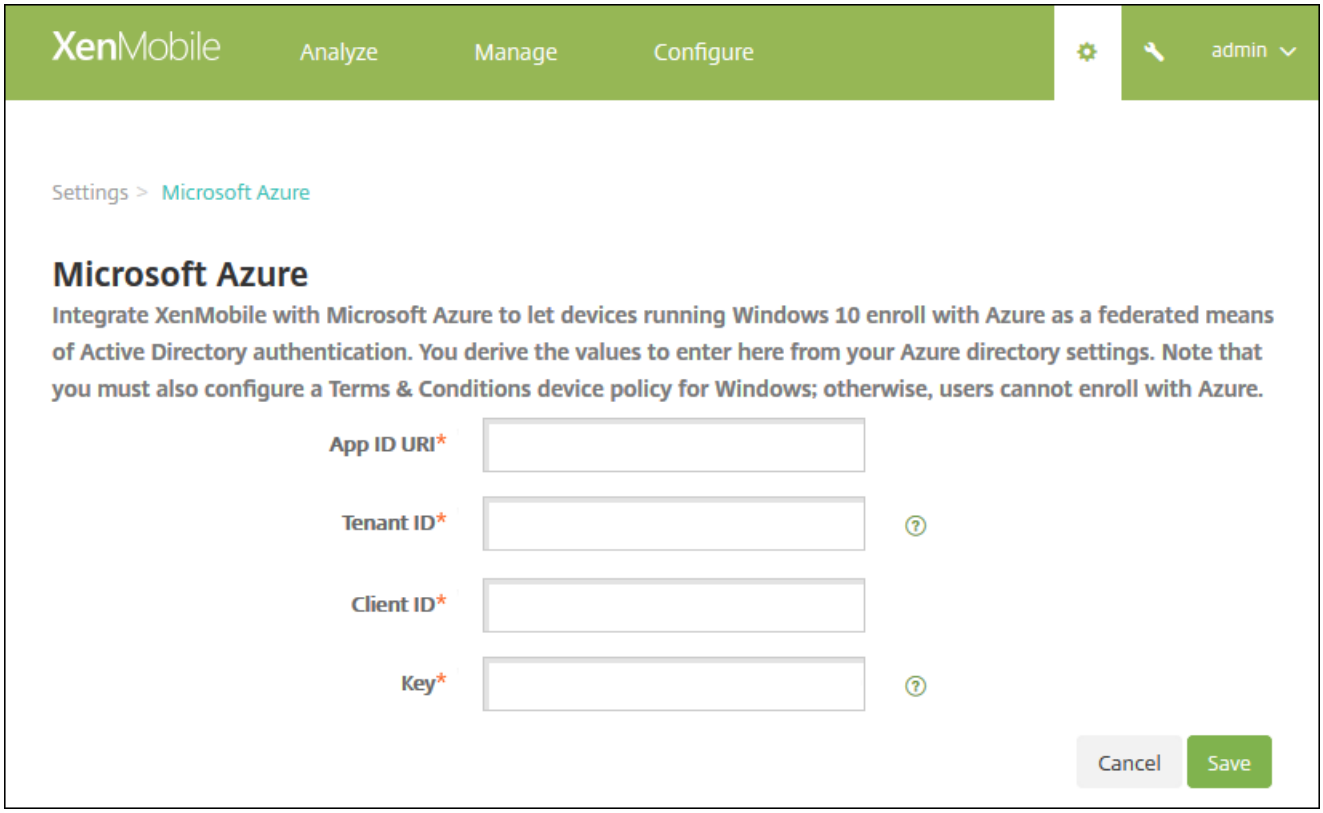
Sie benötigen die folgenden Informationen von Ihrem Microsoft Azure-Konto zum Konfigurieren der Einstellungen in der XenMobile-Konsole:

- 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 **Plattformen** auf **Microsoft Azure**. Die Seite **Microsoft Azure** wird angezeigt.



3. Konfigurieren Sie folgende 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 XenMobile Store 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.

Upgrades

Apr 24, 2017

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.

Für das Upgrade von XenMobile haben Sie die folgenden Optionen:

- **Upgrade von XenMobile 9.0 auf XenMobile 10.4**
  Verwendung des in XenMobile 10.4 integrierten XenMobile Upgradetools. Weitere Informationen finden Sie in den Artikeln in diesem Abschnitt.
  Das Upgrade Tool unterstützt alle Editionen von XenMobile 9: MDM, App und Enterprise.
  Informationen zu behobenen und bekannten Probleme finden Sie unter Behobene Probleme und Bekannte Probleme.
  Das ältere Upgrade Tool ist nicht mehr auf Citrix.com verfügbar.
- **Upgrade von XenMobile 10.3.x auf XenMobile 10.4**
  Verwenden Sie die Seite **Releasemanagement** der XenMobile-Konsole. Weitere Informationen finden Sie im vorliegenden Artikel.
  Das Upgrade Tool wird zum Installieren von XenMobile 10.3.x nicht verwendet.
- **Upgrade von XenMobile 10 oder 10.1 auf XenMobile 10.4**
  Verwenden Sie zunächst die Seite **Releasemanagement** der XenMobile-Konsole für das Upgrade von XenMobile 10 oder 10.1 auf XenMobile 10.3.Verwenden Sie dann die Seite **Releasemanagement** für das Upgrade von XenMobile 10.3 auf 10.4. Weitere Informationen finden Sie im vorliegenden Artikel.Das Upgrade Tool wird für diese Installationen nicht verwendet.

Überblick über den Upgradepfad

XenMobile Server-Version	Releasenummer	Upgrade auf	Releasenummer	Upgradepfad	Releaseupdatespeicherort
XenMobile Server 9 mit installiertem Rolling Patch 9	9.0.0_97106	XenMobile Server 10.4	10.4.0.116	XenMobile Server 9 auf 10.4	Laden Sie das erforderliche Rolling Patch herunter. Das Upgrade Tool für XenMobile 10.4 ist in XenMobile Server integriert.
XenMobile Server 10 oder 10.1	10.1.0.63030	XenMobile Server 10.3	10.3.0.824	XenMobile 10 oder 10.1 auf XenMobile 10.3	Download
XenMobile Server 10.3.x	10.3.x	XenMobile Server 10.4	10.4.0.116	XenMobile 10.3.x auf XenMobile 10.4	Download

10.4.0.?

10.4.0.?

Upgrade von XenMobile 10 oder 10.1 auf Version 10.3 bzw. von XenMobile 10.3 auf Version 10.4

Voraussetzungen:

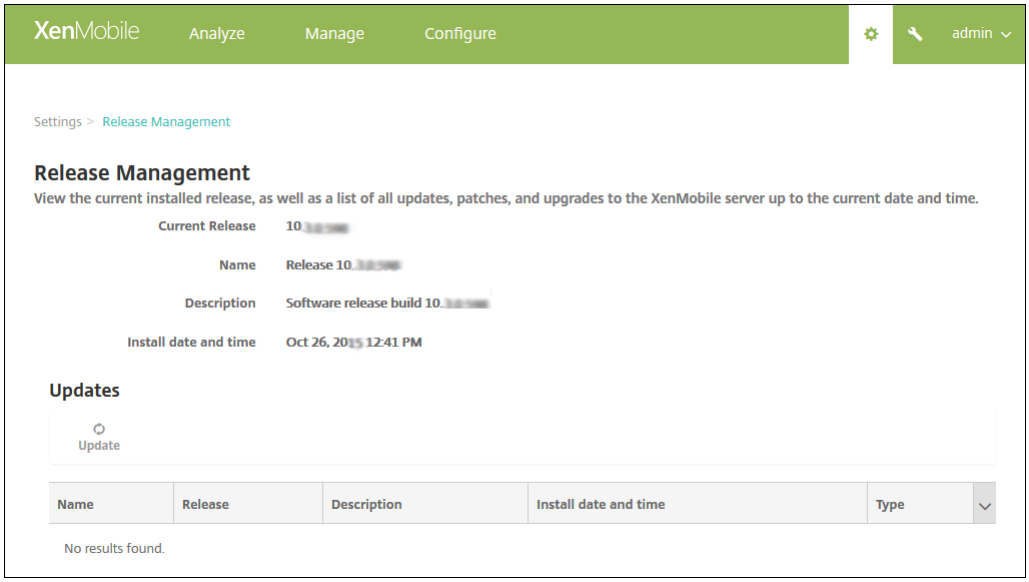
- Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine (VM) zum Erstellen eines Systemsnapshots.
- Sichern Sie die Konfigurationsdatenbank des Systems.
- Überprüfen Sie die Systemanforderungen für die Version, auf die Sie aktualisieren. Informationen für XenMobile 10.4 finden Sie unter Systemanforderungen.

Wenn Sie eine Clusterbereitstellung haben, lesen Sie die Anweisungen am Ende dieses Artikels.

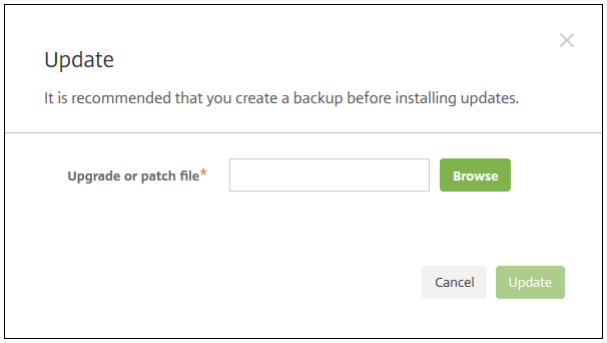
1. Melden Sie sich mit Ihrem Konto auf der Citrix Website an und laden Sie die XenMobile-Upgradedatei (.bin) an einen geeigneten Speicherort herunter.

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.



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



5. Klicken Sie auf **Durchsuchen**, navigieren Sie zum Speicherort der von Citrix.com heruntergeladen XenMobile-Upgradedatei und wählen Sie sie aus.

6. Klicken Sie auf **Update** und starten Sie XenMobile neu, wenn Sie dazu aufgefordert werden.

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.

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.

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.

Upgrade von XenMobile-Clusterbereitstellungen

Wenn das System im Clustermodus konfiguriert ist, führen Sie die folgenden Schritte aus, um jeden Knoten mit XenMobile 10 zu aktualisieren:

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

2. Fahren Sie alle Knoten, mit Ausnahme dessen, den Sie zuerst aktualisieren, herunter.Zum Herunterfahren von Knoten verwenden Sie das **Systemmenü** in der Befehlszeilenschnittstelle.

3.Führen Sie ein Upgrade des Knotens durch, den Sie nicht heruntergefahren haben.

3. Überprüfen Sie, ob der Dienst auf dem aktualisierten Knoten ausgeführt wird.

4. Starten Sie die anderen Knoten nacheinander.

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

Voraussetzungen für das Upgrade Tool

Feb 24, 2017

Für das Upgrade von XenMobile 9.0 auf XenMobile 10.4 verwenden Sie das in XenMobile 10.4 integrierte Upgrade Tool.

Das Upgrade Tool unterstützt Folgendes:

- In sämtlichen XenMobile-Servermodi (ENT, MAM, MDM) registrierte iOS- und Android-Geräte
- Im MDM-Modus registrierte Windows Phones und -Tablets
- Im Enterprise-Modus registrierte Windows Phones
- Im MDM-Modus registrierte Windows CE-Geräte

Wenn die Multi-Tenant Console (MTC) unter XenMobile 9.0 aktiviert ist, können Sie sie in eine eigenständige XenMobile 10.4-Bereitstellung migrieren. XenMobile 10 unterstützt die Multi-Tenant Console nicht, daher müssen Sie die aktualisierten Instanzen individuell verwalten. Lesen Sie nach der Schaffung der in diesem Artikel aufgeführten Voraussetzungen den Artikel Aktualisieren des MTC-Mandantenservers auf XenMobile 10.4.

XenMobile 10.4 unterstützt die NetScaler Gateway-Versionen 11.1.x, 11.0.x und 10.5.x.

Das in XenMobile 10.4 integrierte Upgrade Tool unterstützt außerdem NetScaler Gateway 10.1.x. Citrix bietet keine Unterstützung für die Verwendung von NetScaler Gateway 10.1 in Verbindung mit XenMobile 10.4. Sie können jedoch NetScaler Gateway 10.1-Bereitstellungen mit dem Upgrade Tool von XenMobile 10.4 aktualisieren. Danach empfiehlt sich ein Upgrade von NetScaler Gateway auf die neueste unterstützte Version.

> **Important**
>
> Das Upgrade ist ein komplexer Prozess. Lesen Sie vor dem Upgrade die Informationen zu bekannten Problemen, planen Sie das Upgrade, und schaffen Sie alle in diesem Artikel beschriebenen Voraussetzungen. Zusätzliche Hilfe beim Upgrade bieten die Installationschecklisten in diesem Blog.
>
> Nach Ausführung des Upgrade Tool müssen sich alle Nachbereitungsschritte ausführen.
>
> Werden nicht alle Voraussetzungen erfüllt, kann das Upgrade fehlschlagen. In diesem Fall müssen Sie über die Befehlszeilenkonsole eine neue XenMobile 10.4-Instanz konfigurieren und das Upgrade Tool erneut starten.

Planen des Upgrades

Citrix empfiehlt, dass Sie das Upgrade in den folgenden Etappen ausführen.

1. Führen Sie einen Upgradetest in einer Testumgebung aus, wobei Sie alle Schritte zur Vorbereitung und zum Ausführen des Upgrade Tools ausführen. Citrix empfiehlt, ein Testupgrade durchzuführen, um den Upgradevorgang auszuprobieren und einen Eindruck von dem Ergebnis zu bekommen, das nach dem vollständigen Produktionsupgrade zu erwarten ist. Bei einem solchen Test wird das Upgrade der Konfigurationsdaten, nicht jedoch das der Benutzerdaten getestet.

Für NetScaler Gateway 11.1 (bzw. die Mindestversion 10.5) empfiehlt Citrix, mit dem NetScaler für XenMobile-Assistenten eine neue NetScaler-Bereitstellung mit NetScaler Gateway und virtuellen Servern für den Lastausgleich einzurichten.

2. Prüfen Sie, ob bei dem Testupgrade die Konfigurationsdaten (z. B. LDAP, Richtlinien und Apps) einwandfrei aktualisiert

wurden. Prüfen Sie Testgeräte.

3. Führen Sie das Produktionsupgrade in der Produktionsumgebung durch und aktivieren Sie die Produktionsumgebung. Planen Sie Ausfallzeiten für das Upgrade ein.

Informationen zu Test- und Produktionsupgrade

Führen Sie mit dem XenMobile 10.4 Upgrade Tool zunächst ein Testupgrade durch und dann das vollständige Produktionsupgrade.

Option "Test Drive"
Bei Auswahl von "Test Drive" erfolgt ein Upgradetest mit den Produktionskonfigurationsdaten für den Vergleich zwischen XenMobile 9.0 und XenMobile 10.4 ohne Auswirkungen auf die Produktionsumgebung. Der Upgradetest erfolgt nur an Konfigurationsdaten, Gerätedaten (XenMobile Enterprise Edition-Bereitstellungen) oder Benutzerdaten werden nicht getestet.

Das Ergebnis des Upgradetests ist ausschließlich zur Verwendung für Testzwecke vorgesehen. Für eine Testbereitstellung können Sie kein Upgrade durchführen. Für ein Produktionsupgrade müssen Sie den Prozess von Anfang an erneut durchführen. Upgradetests sind bei allen XenMobile 9.0-Editionen möglich.

Option "Upgrade"
Bei Auswahl der Option "Upgrade" werden zunächst sämtliche Konfigurations-, Geräte- und Benutzerdaten aus XenMobile 9.0 in eine neue Instanz von XenMobile 10.4 mit demselben vollqualifizierten Domänennamen (FQDN) kopiert. Alle Daten bleiben in XenMobile 9.0 bestehen, bis Sie den XenMobile 10,4-Server in die Produktion übernehmen.

Wenn Sie sich nach dem Upgrade bei der XenMobile 10.4-Konsole anmelden, sehen Sie alle Benutzer- und Gerätedaten, die von XenMobile 9.0 übertragen wurden.

Nicht per Upgrade Tool migrierte Elemente

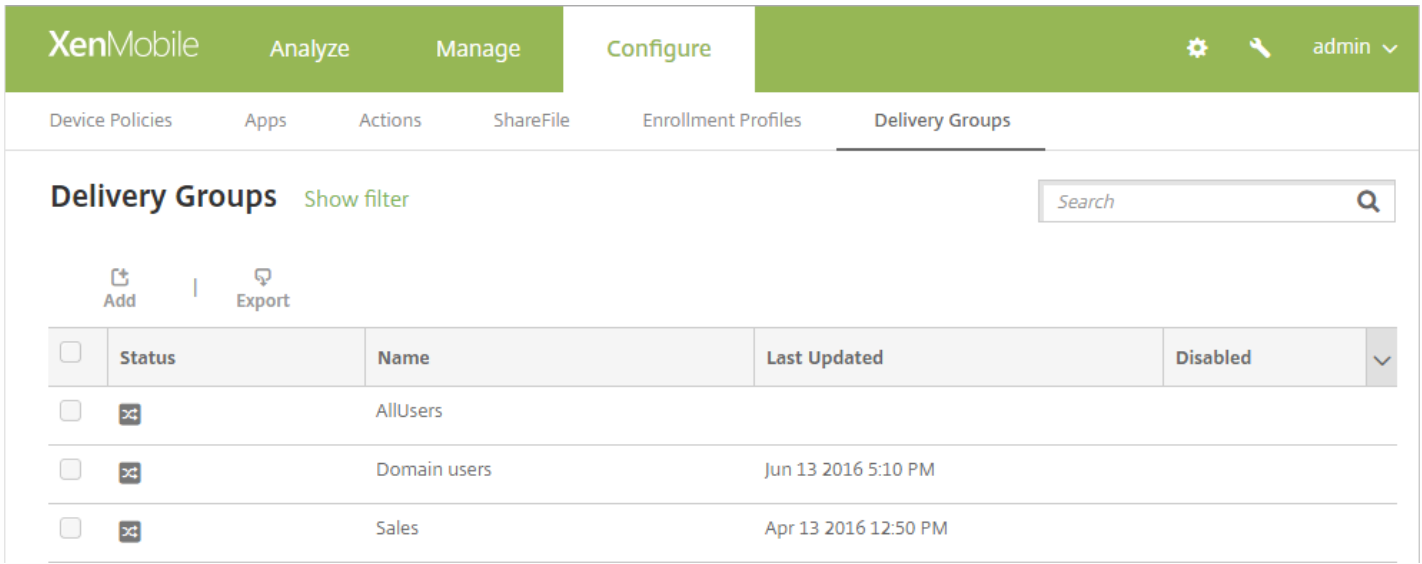
Die folgenden Informationen werden mit dem Upgrade Tool nicht nach XenMobile 10.4 migriert:

- Lizenzinformationen
- Berichtdaten
- Servergruppenrichtlinien und zugeordnete Bereitstellungen (in XenMobile 10.4 nicht unterstützt)
- Managed Service Provider (MSP)-Gruppe
- Richtlinien und Pakete für Windows 8.0
- Bereitstellungspakete, die nicht in Gebrauch sind, z. B., wenn ihnen keine Benutzer oder Gruppen zugewiesen sind
- Alle anderen Konfigurations- oder Benutzerdaten (siehe Upgradeprotokoll)
- CXM Web (durch Citrix Secure Web ersetzt)
- DLP-Richtlinien (durch Citrix ShareFile ersetzt)
- Benutzerdefinierte Active Directory-Attribute
- Wenn Sie mehrere Branding-Richtlinien konfiguriert haben, werden diese nicht migriert. XenMobile 10.4 unterstützt nur eine Branding-Richtlinie. Es darf daher nur eine Branding-Richtlinie in XenMobile 9.0 verbleiben, damit sie erfolgreich nach XenMobile 10.4 migriert werden kann.
- Alle Einstellungen in der Datei auth.jsp in XenMobile 9.0, die den Zugriff auf die Konsole einschränken Zugriffseinschränkungen auf die Konsole in XenMobile 10.4 sind Firewalleinstellungen, die Sie in der Befehlszeilenschnittstelle konfigurieren können.
- Syslog-Serverkonfigurationen

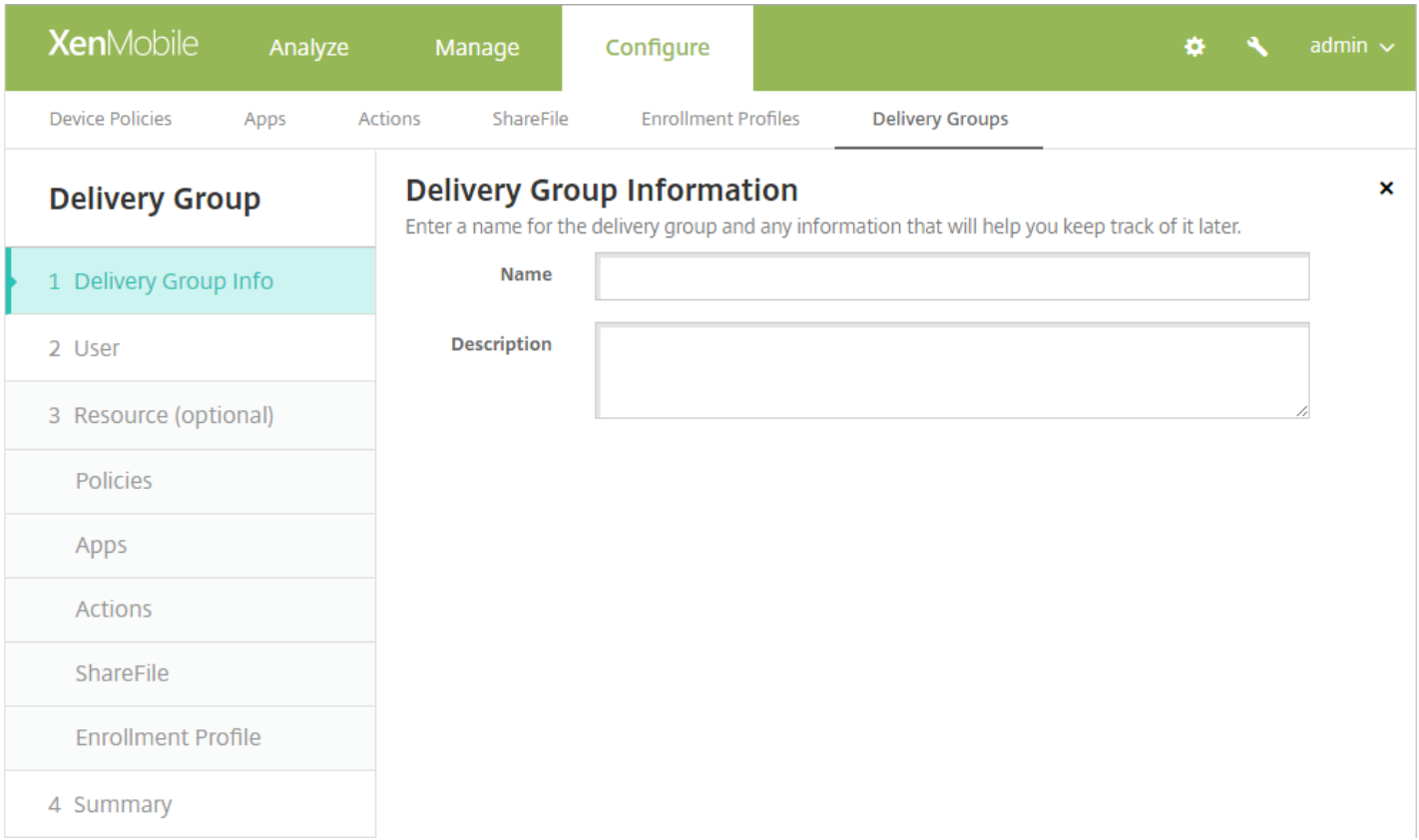
- Formfill-Connectors, die in XenMobile 9.0 konfiguriert wurden (in XenMobile 10.4 nicht unterstützt)

Änderungen in XenMobile

- Mit dem Upgrade Tool erfolgt kein Upgrade von Active Directory-Benutzern, die lokalen Gruppen zugewiesen sind.Sie können Active Directory-Benutzer später lokalen Gruppen zuweisen.
- XenMobile 10 unterstützt keine verschachtelten, lokalen Gruppen. Bei einem Upgrade von XenMobile 9 wird die Hierarchie der lokalen Gruppen entfernt.
- Device Manager-Bereitstellungspakete werden in XenMobile als Bereitstellungsgruppen bezeichnet (s. folgende Abbildung). Weitere Informationen finden Sie unter Bereitstellen von Ressourcen.

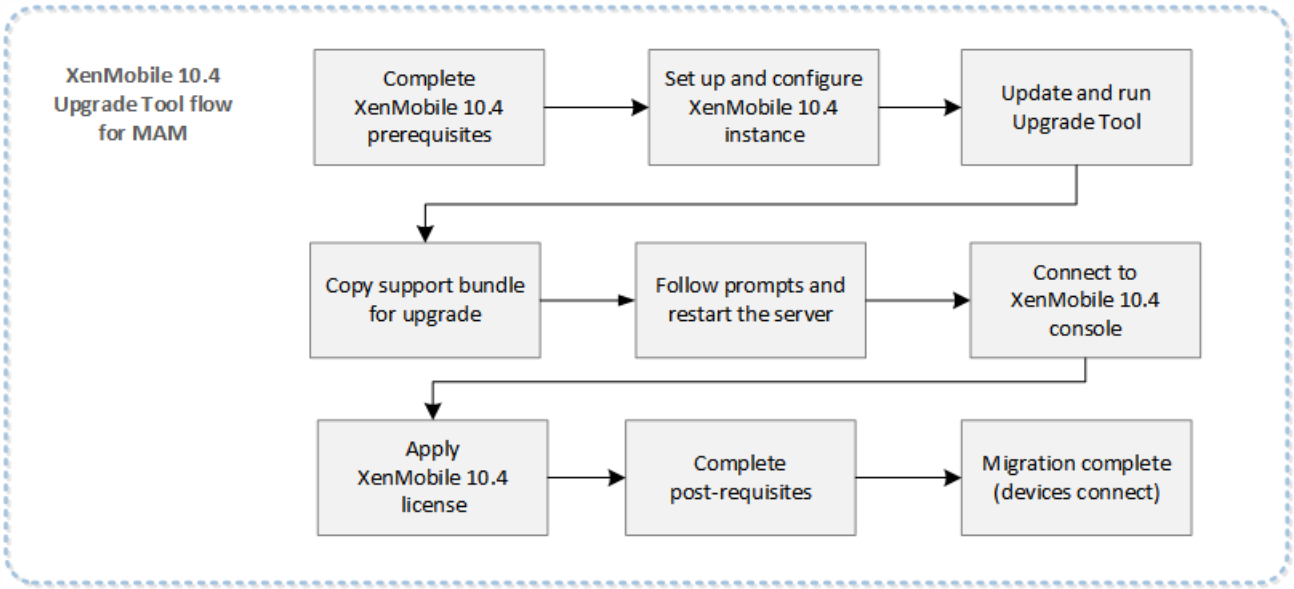


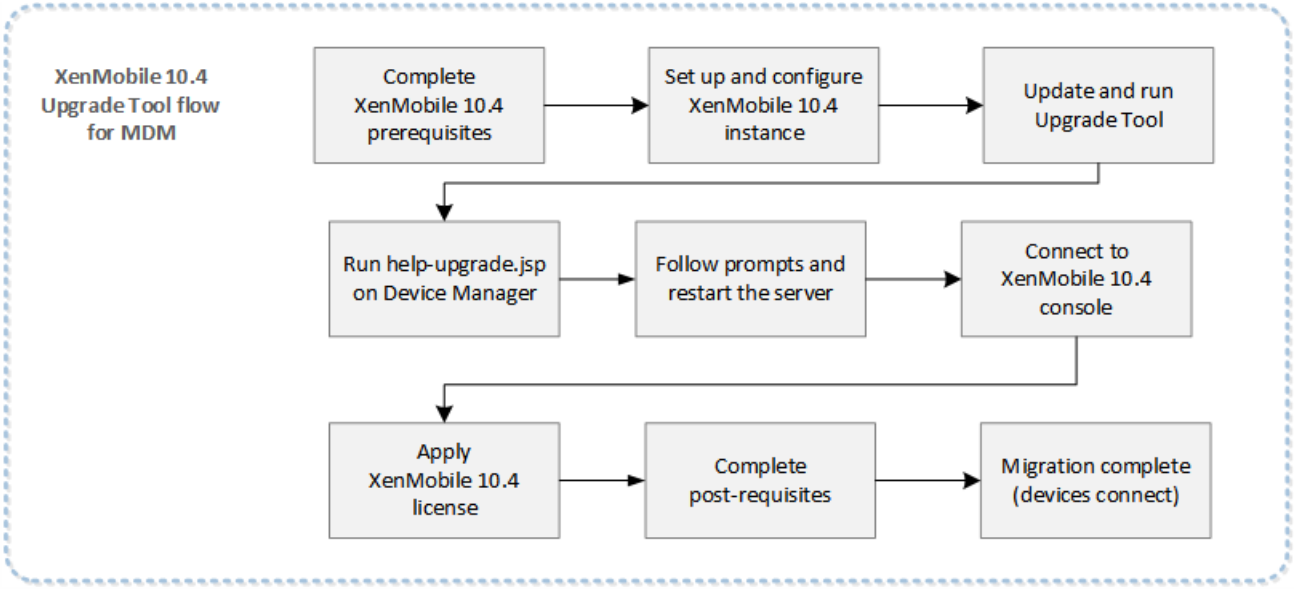
Innerhalb der Bereitstellungsgruppe können Sie die Richtlinien, Aktionen und Apps für die Benutzergruppen anzeigen, die Ressourcen benötigen.

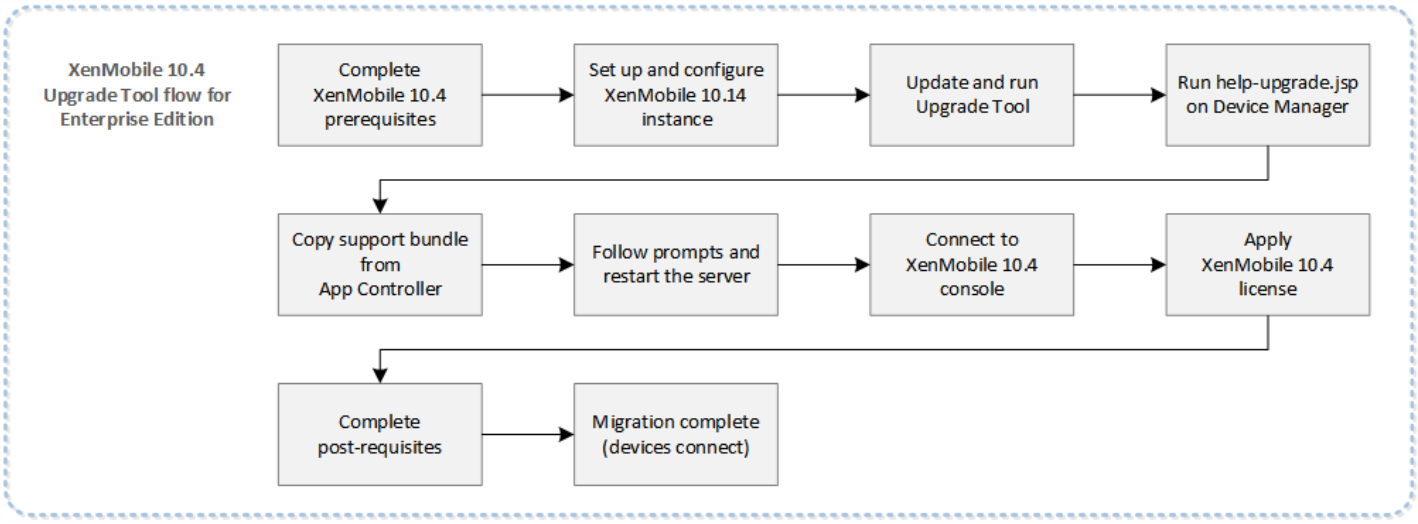


Workflow des Upgrades von XenMobile 9.0 auf XenMobile 10.4

Die folgenden Abbildungen zeigen die grundlegenden Schritte beim Upgrade von XenMobile 9.0 auf XenMobile 10.4.







Voraussetzungen für Windows Phone-Geräte im Enterprise-Modus

Citrix empfiehlt die nachfolgenden Schritte für das Upgrade einer XenMobile 9.0 Enterprise-Umgebung auf XenMobile 10.4, wenn diese im Enterprise-Modus registrierte Windows Phones enthält und Worx Home 9.x verwendet wird.

1. Führen Sie ein Upgrade von Worx Home auf Device Manager auf die Version 10.2 durch und stellen Sie Worx Home 10.2 dann bereit.

2. Deinstallieren Sie Worx Home 9.x manuell von den Geräten.

3. Weisen Sie die Benutzer an, über den Download Hub auf ihrem Telefon die von Ihnen über Device Manager bereitgestellte Version 10.2 von Worx Home zu installieren.

4. Führen Sie nach der Schaffung der in diesem Artikel aufgeführten Voraussetzungen ein Upgrade auf XenMobile 10.4 durch. Entsprechende Anweisungen finden Sie unter Aktivieren und Ausführen des XenMobile Upgrade Tools.

5. Führen Sie die unter Nachbereitung eines Upgrades beschriebenen Änderungen an NetScaler durch, damit die Geräte

wieder eine Verbindung herstellen können.

Erforderliches App Controller-Patch

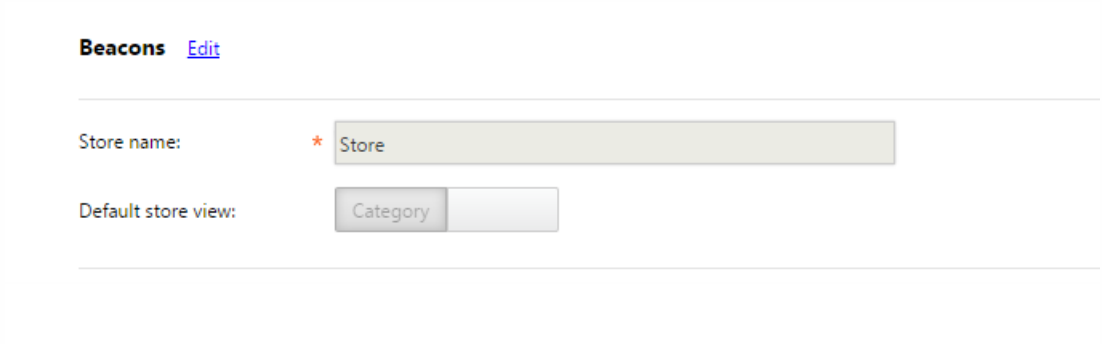
Laden Sie Rolling Patch 9 für XenMobile 9.0 App Controller von https://support.citrix.com/article/CTX218552 herunter.

Klicken Sie in der App Controller Management Console auf **Settings > Release Management**. Klicken Sie auf **Update** und wählen Sie dann die Patchdatei aus, die Sie heruntergeladen haben. Klicken Sie auf **Upload** und starten Sie App Controller neu.

Benutzerdefinierter Storenamen in XenMobile 9

Vor dem Upgrade von XenMobile 9 auf XenMobile 10.4 müssen Sie benutzerdefinierte Storenamen in die jeweiligen Standardnamen ändern, damit registrierte Windows-Geräte nach dem Upgrade weiterhin funktionieren. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX214553.

Wenn der Storename in App Controller geändert wurde und nicht mehr "Store" lautet, müssen Sie bei einem Upgrade im MAM- oder Enterprise-Modus den Namen auf die Standardeinstellung **Store** zurücksetzen, bevor Sie ein Supportpaket für das Upgrade erstellen.



System- und Portanforderungen

Informationen zu den erforderlichen Versionen verwandter Komponenten (z. B. Citrix Lizenzserver) finden Sie im Artikel Systemanforderungen.

- **NetScaler**: Speichern Sie vor dem Upgrade von NetScaler eine Kopie der NetScaler-Konfigurationsdatei (ns.conf). Aktuelle NetScaler-Versionen enthalten den NetScaler für XenMobile-Assistenten, mit dem Sie die Integration von NetScaler und XenMobile mühelos durchführen können. Weitere Informationen finden Sie unter Konfigurieren von Einstellungen für die XenMobile-Umgebung und FAQ: XenMobile 10 and NetScaler 10.5 Integration.
- **Firewall und Ports**: Öffnen Sie ähnliche Firewallports für die neue XenMobile 10.4 Server-IP-Adresse wie für die XenMobile 9.0 Server-IP-Adresse. Informationen zu den Portanforderungen für XenMobile 10.4 finden Sie unter Portanforderungen.
- **LDAP-Server**: Stellen Sie sicher, dass der neue XenMobile 10.4-Server eine Verbindung mit mindestens einem LDAP-Server herstellen kann. Wenn Sie den Server nach dem Upgrade neu starten, muss eine aktive Verbindung mit LDAP-Servern bestehen.

Datenbankmigration

In der folgenden Tabelle werden die möglichen Datenbankmigrationsoptionen aufgeführt. Informationen zu den Systemanforderungen finden Sie unter XenMobile 10.4 – Datenbankanforderungen.

Von XenMobile 9.0	Auf XenMobile 10.4

Enterprise Edition

App Controller	MDM	
Lokale PostgreSQL	Lokale PostgreSQL	Lokale PostgreSQL
Lokale PostgreSQL	MS SQL	MS SQL
Lokale PostgreSQL	Remote PostgreSQL	Remote PostgreSQL

App Edition

Lokale PostgreSQL	Lokale PostgreSQL
Lokale PostgreSQL	Remote PostgreSQL
Lokale PostgreSQL	MS SQL

MDM Edition

Lokale PostgreSQL	Lokale PostgreSQL
MS SQL	MS SQL
Remote PostgreSQL	Remote PostgreSQL

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

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

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

1. Öffnen Sie die Datei pg_hba.conf und suchen Sie die folgende Zeile:

    host all all 127.0.0.1/32 md5

2. Zum Zulassen aller IP-Adressen ändern Sie die Zeile in:

host all all 0.0.0.0/0 md5

Fügen Sie alternativ einen weiteren Hosteintrag hinzu, um Verbindungen mit der IP-Adresse des XenMobile-Servers zuzulassen:

host all all 10.x.x.x/32 md5

3. Speichern Sie die Datei.

4. Beenden und starten Sie den Dienst.

5. Öffnen Sie die Datei postgresqlconf und suchen Sie die folgende Zeile:

#listen_addresses = 'localhost'

6. Ändern Sie die Zeile in:

listen_addresses = '*'

7. Beenden Sie den PostgreSQL-Dienst und starten Sie ihn erneut, um die Änderungen zu anzuwenden.

Wenn der Datenbanklösung ein benutzerdefinierter Port zugewiesen ist, müssen Sie sicherstellen, dass der Port in der Firewall für XenMobile 9.0 Device Manager zugelassen und geöffnet ist. Dadurch kann XenMobile 10.4 eine Verbindung mit der Datenbank herstellen und die erforderlichen Informationen migrieren.

Bereitstellungspaketnamen mit Sonderzeichen

XenMobile 9.0-Bereitstellungspakete, deren Namen Sonderzeichen enthalten (!, $, (), #, % , +, *, ~, ?, |, {} und []) werden zwar aktualisiert, doch die entsprechenden Bereitstellungsgruppen in XenMobile 10.4 können nach dem Upgrade nicht bearbeitet werden. Außerdem verursachen lokale Benutzer und lokale Gruppen, die in XenMobile 9.0 erstellt wurden und deren Name eine eckige Klammer links ([) enthält, Probleme in XenMobile 10. 4 beim Erstellen von Registrierungseinladungen. Entfernen Sie vor dem Upgrade alle Sonderzeichen aus Bereitstellungspaketnamen und alle linken eckigen Klammern aus den Namen lokaler Benutzer und Gruppen.

Externes SSL-Zertifikat

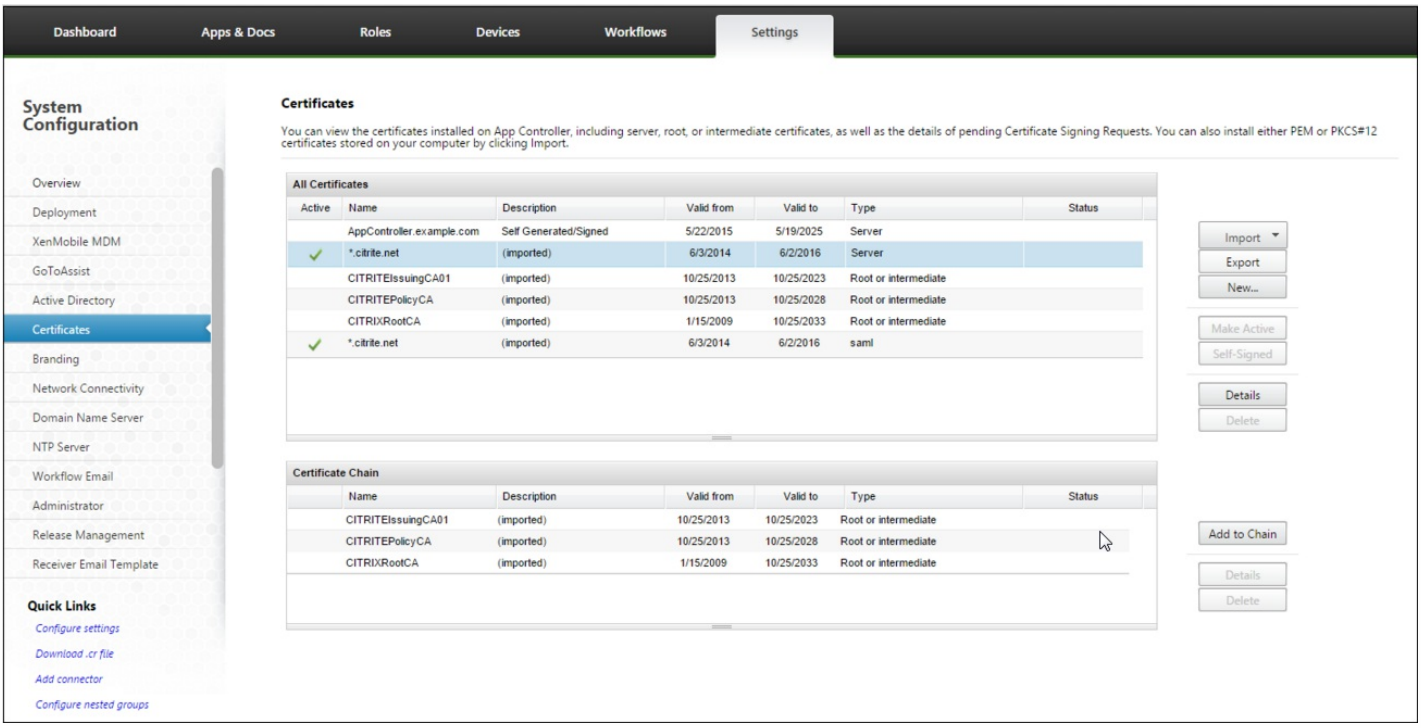
Externe SSL-Zertifikate müssen die im Citrix Supportartikel How to Configure an External SSL Certificate aufgeführten Bedingungen erfüllen. Überprüfen Sie die Datei pki.xml vor dem Upgrade, um sicherzustellen, dass das SSL-Zertifikat diese Bedingungen erfüllt.

Exportieren des XenMobile 9.0-Serverzertifikats

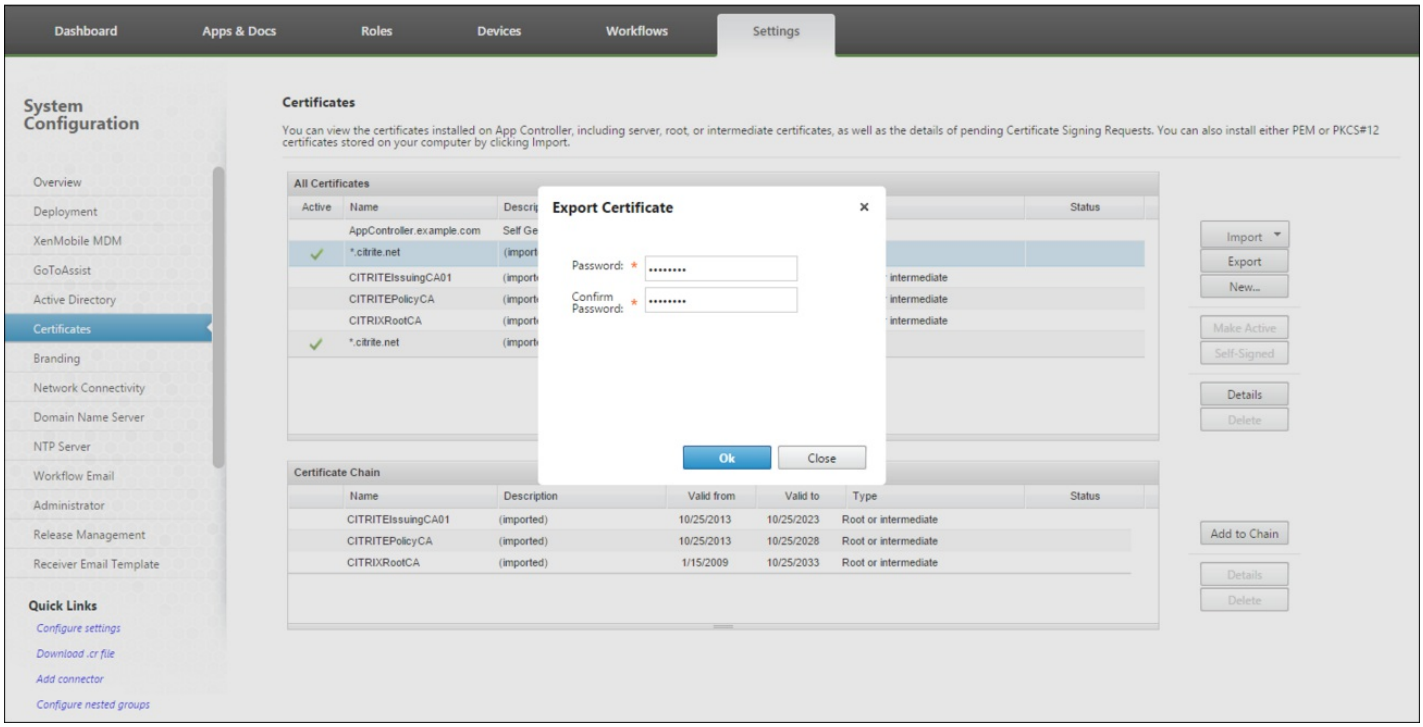
Wenn Sie ein Upgrade einer XenMobile 9.0 Enterprise Edition-Bereitstellung durchführen, müssen Sie das App Controller-Serverzertifikat exportieren. Bei der Nachbereitung müssen Sie das Serverzertifikat dann in NetScaler Gateway importieren. Mit den folgenden Schritten exportieren Sie das Serverzertifikat:

1. Melden Sie sich bei XenMobile 9.0 App Controller an und klicken Sie auf **Certificates**.

2. Klicken Sie in der Zertifikatliste auf das Serverzertifikat, das Sie exportieren möchten, und klicken Sie dann auf **Export**.



3. Geben Sie im Dialogfeld **Export Certificate** in beide Felder das Zertifikatkennwort ein und klicken Sie auf **OK**.



Server für den Upload des verschlüsselten Supportpakets

Stellen Sie einen Server bereit, auf den Sie das verschlüsselte Supportpaket über die XenMobile-Befehlszeilenschnittstelle mit File Transfer Protocol oder Secure Copy Protocol hochladen können.

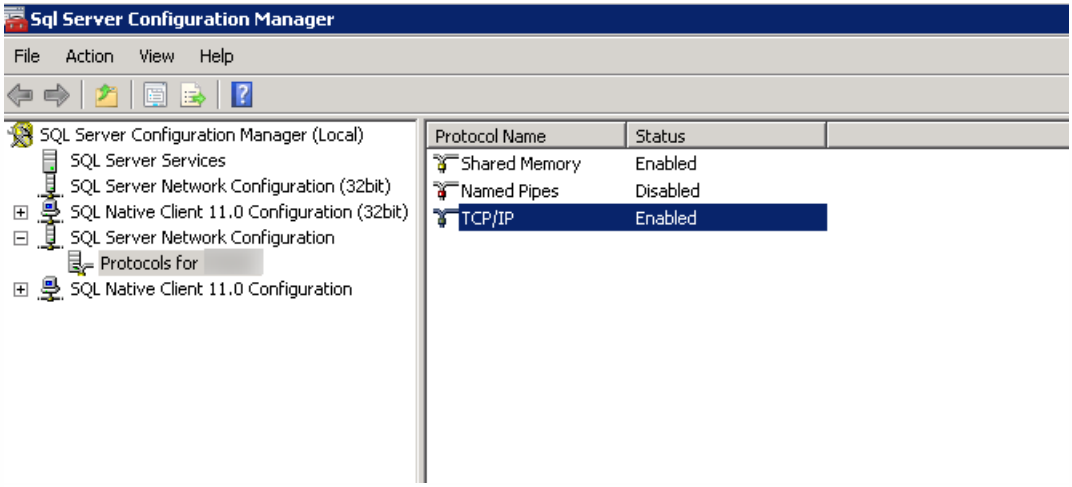
Aktivieren und Ausführen des XenMobile Upgrade Tools

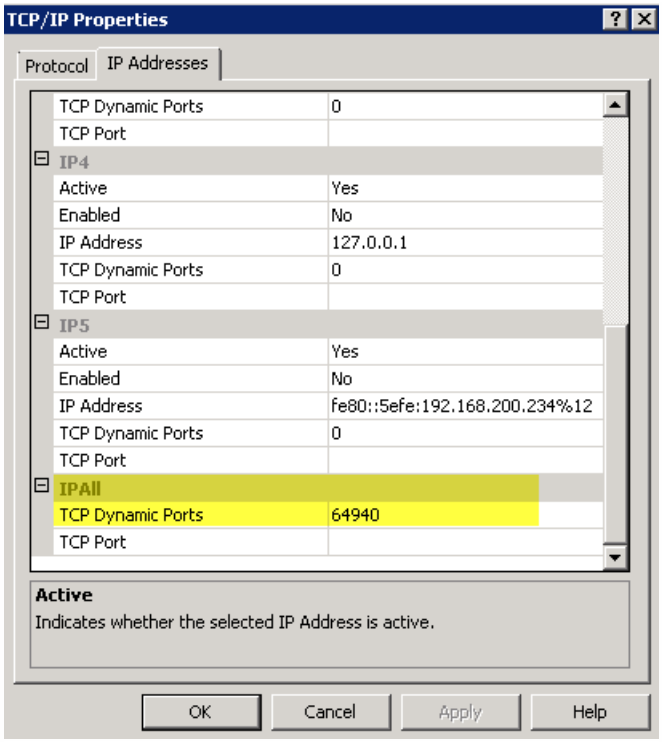
Feb 24, 2017

Wenn Ihre XenMobile 9-Umgebung die folgenden Voraussetzungen erfüllt, folgen Sie den Anleitungen in diesem Abschnitt, bevor Sie mit dem Upgrade fortfahren.

- XenMobile 9 MDM Edition oder Enterprise Edition hat eine externe 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).

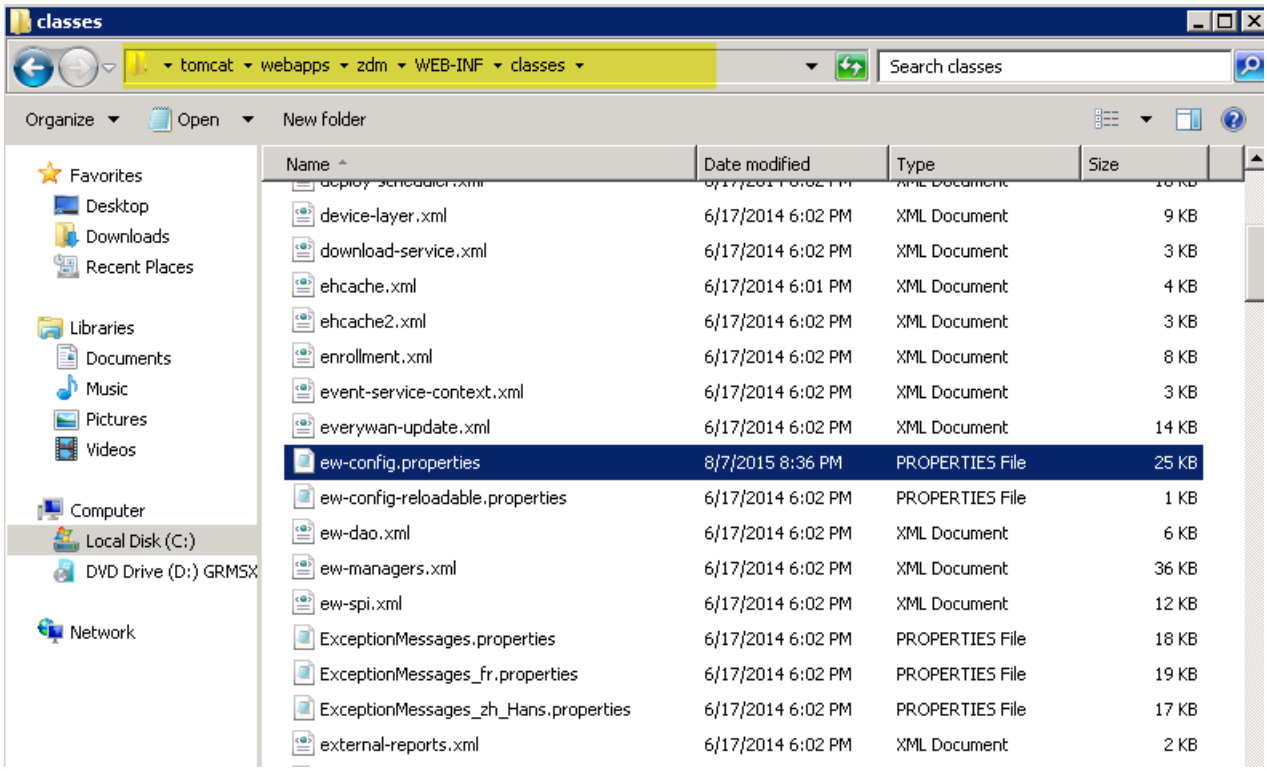
> ## Hinweis
>
> Citrix empfiehlt, die SQL Server-Datenbankinstanz immer auf einem statischen Port auszuführen, weil der XenMobile-Server kontinuierlichen Zugriff auf die Datenbank benötigt. Diese Verbindung erfolgt im Allgemeinen durch eine Firewall. Sie müssen daher den entsprechenden Port in der Firewall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





Schritte zur Upgradevorbereitung

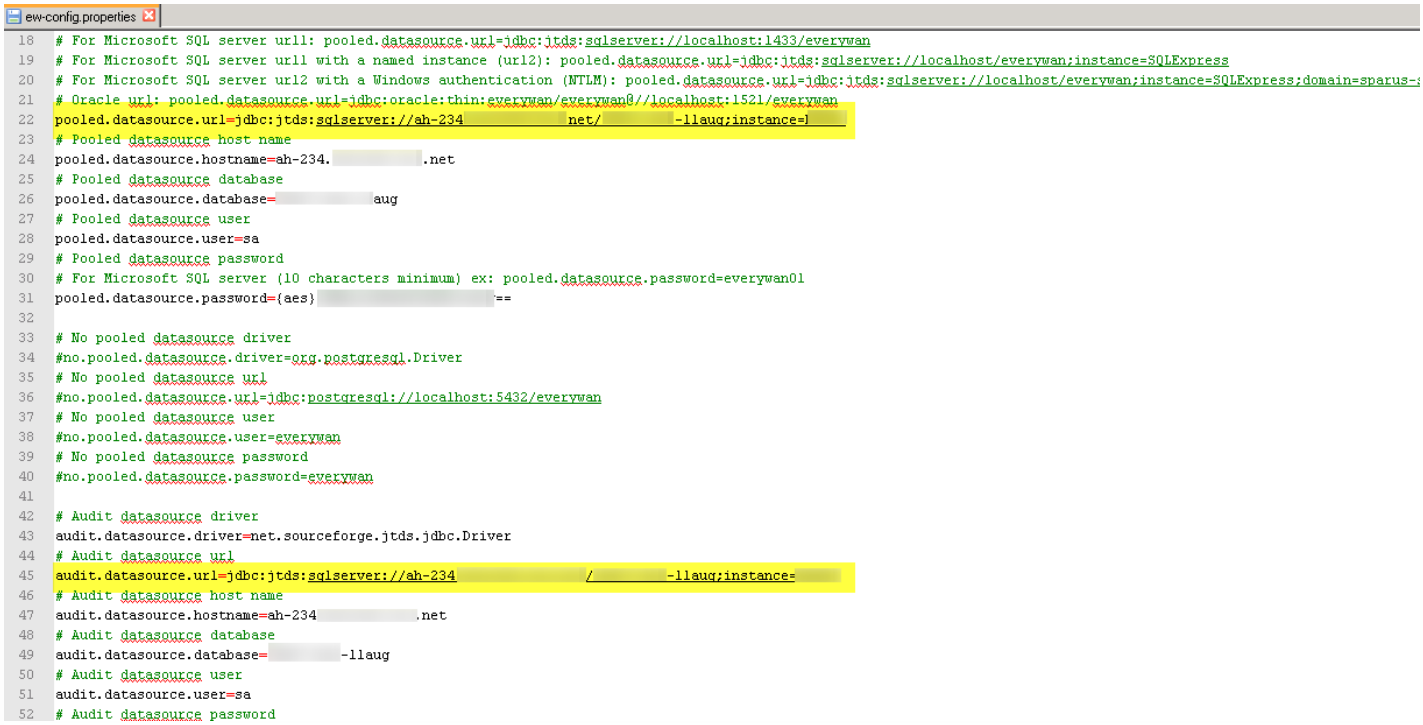
1. Navigieren Sie zum Device Manager-Installationsverzeichnis und öffnen Sie die Datei ew-config.properties. Diese Datei ist in tomcat/webapps/zdm/WEB-INF/classes.



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

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

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

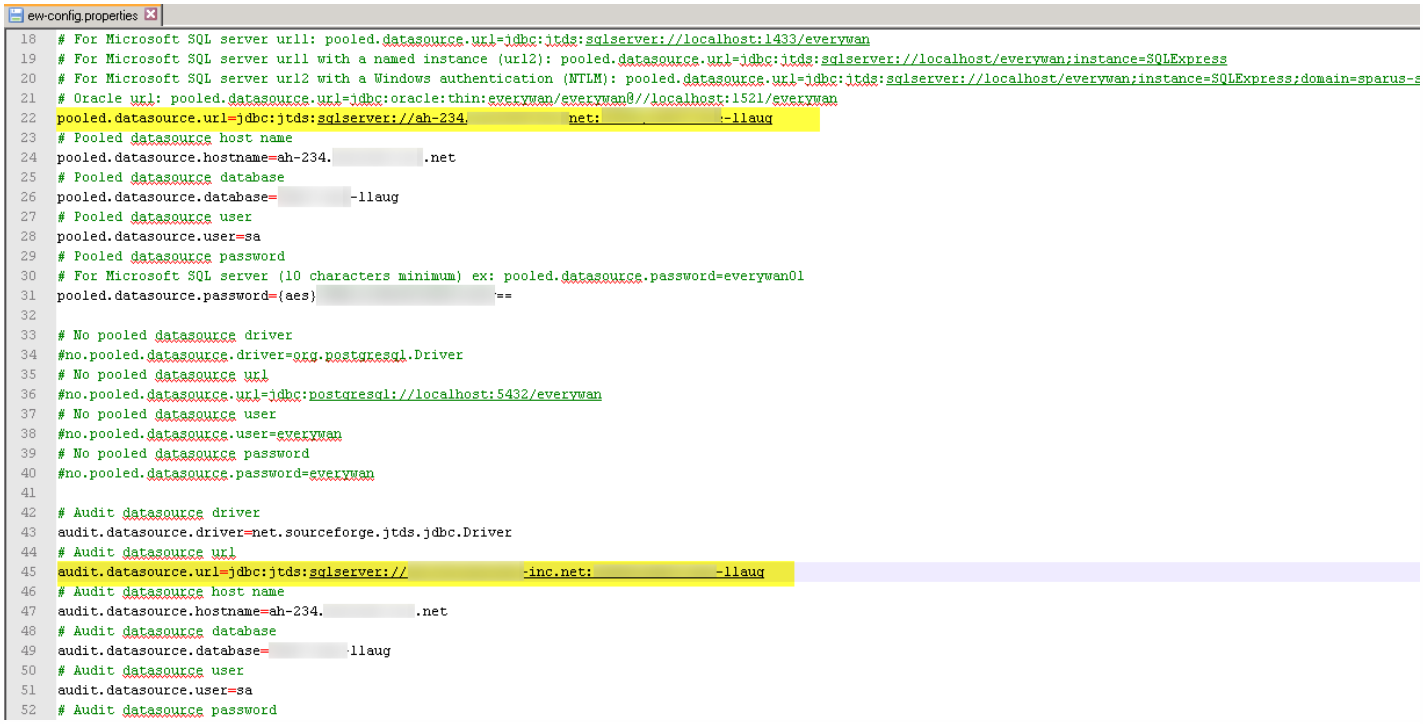


3. Entfernen Sie den Instanznamen aus den aufgeführten URLs und fügen Sie den Port sowie den FQDN des SQL Servers hinzu. In diesem Fall ist 64940 der erforderliche Port.

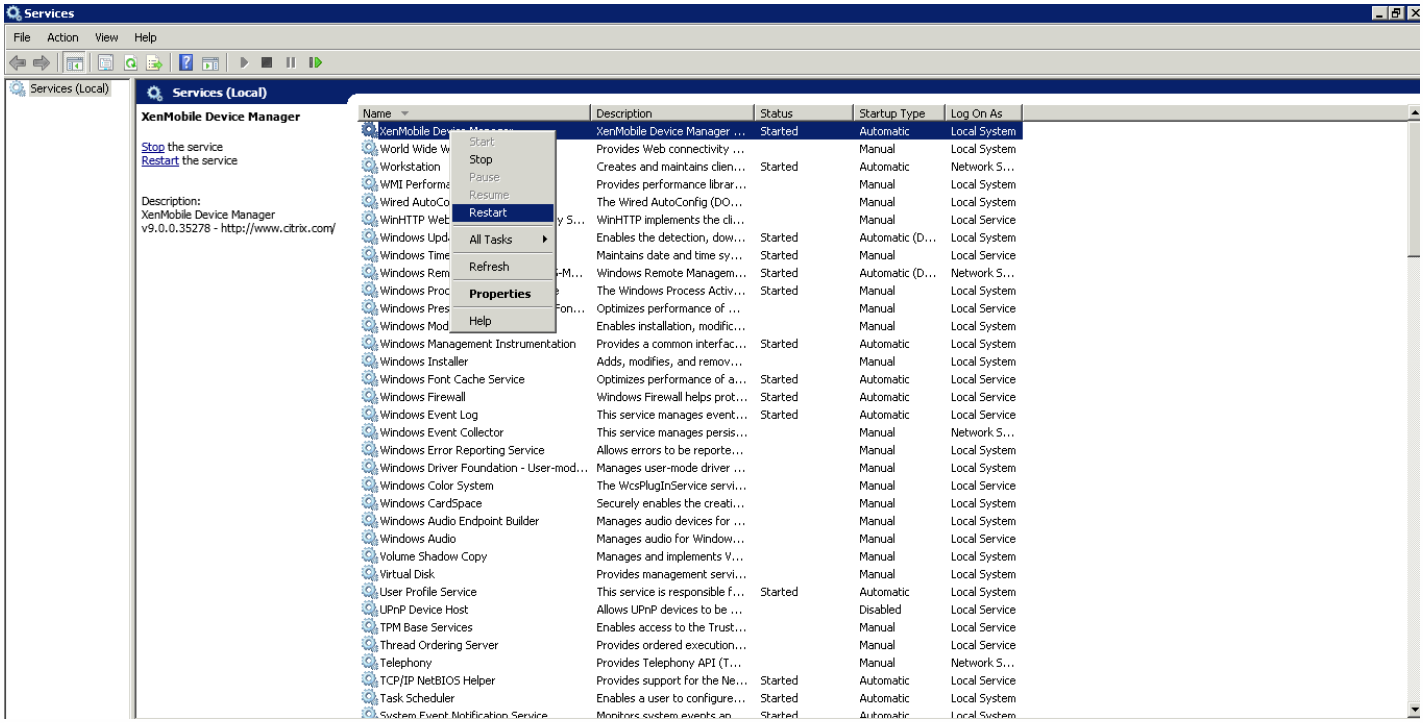
pooled.datasource.url=jdbc:jtds:sqlserver:// :64940/

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

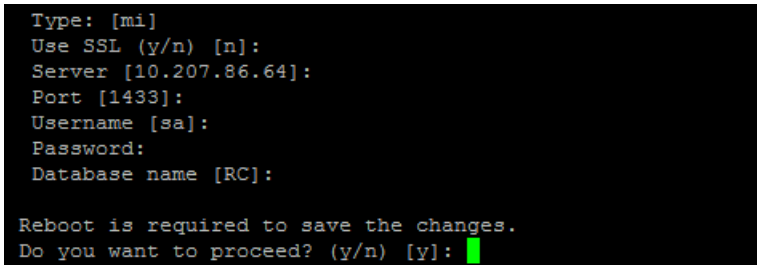
> ## Hinweis
>
> Citrix empfiehlt, eine Sicherung oder Kopie zu erstellen oder genau aufzuschreiben, welche Änderungen Sie in der Datei ew-config.properties vornehmen. Diese Informationen sind nützlich, falls ein Fehler beim Upgrade auftritt.



4. Starten Sie den Device Manager-Dienst neu. Aktualisieren Sie die Geräteverbindungen, wenn die Device Manager-Instanz neu gestartet wurde.



5. Ermitteln Sie, ob der XenMobile 10.x-Server ebenfalls benannte SQL-Instanzen verwendet. Wenn dies der Fall ist, identifizieren Sie den Port, auf dem die benannte Instanz ausgeführt wird. Wenn der Port ein dynamischer Port ist, empfiehlt Citrix, dass Sie ihn in einen statischen Port konvertieren. Wenn Sie später während des Upgrades den folgenden Teil des Datenbank-Setups erreichen, konfigurieren Sie den statischen Port auf dem neuen XenMobile-Server.



Jetzt können Sie das Upgrade fortzusetzen.

Upgrade von XenMobile-Clusterbereitstellungen

Wenn Ihr System im Clustermodus konfiguriert ist:

1. Fahren Sie alle Knoten, mit Ausnahme dessen, den Sie zuerst aktualisieren, herunter. Zum Herunterfahren von Knoten verwenden Sie die Einstellungen in der Befehlszeilenschnittstelle.

2. Führen Sie ein Upgrade des Knotens durch, den Sie nicht heruntergefahren haben, indem Sie die Schritte im nächsten Abschnitt "Aktivieren und Ausführen des Upgrade Tools" befolgen.

3. Nach Sie geprüft haben, ob das erste Upgrade einwandfrei erfolgte, fügen Sie die übrigen Knoten nacheinander ein. Zum Wiedereinfügen gehen Sie folgendermaßen vor:

    a. Starten Sie den Knoten.

    b. Führen Sie, wenn Sie dazu aufgefordert werden, kein Upgrade des Knotens durch.

    c. Fügen Sie den Knoten in die Clusterdatenbank ein.

    Anschließend wird der Knoten automatisch aktualisiert.

4. Führen Sie alle Aufgaben der Nachbereitung auf jedem Knoten durch, nachdem Sie ihn wieder in das Cluster eingefügt haben.

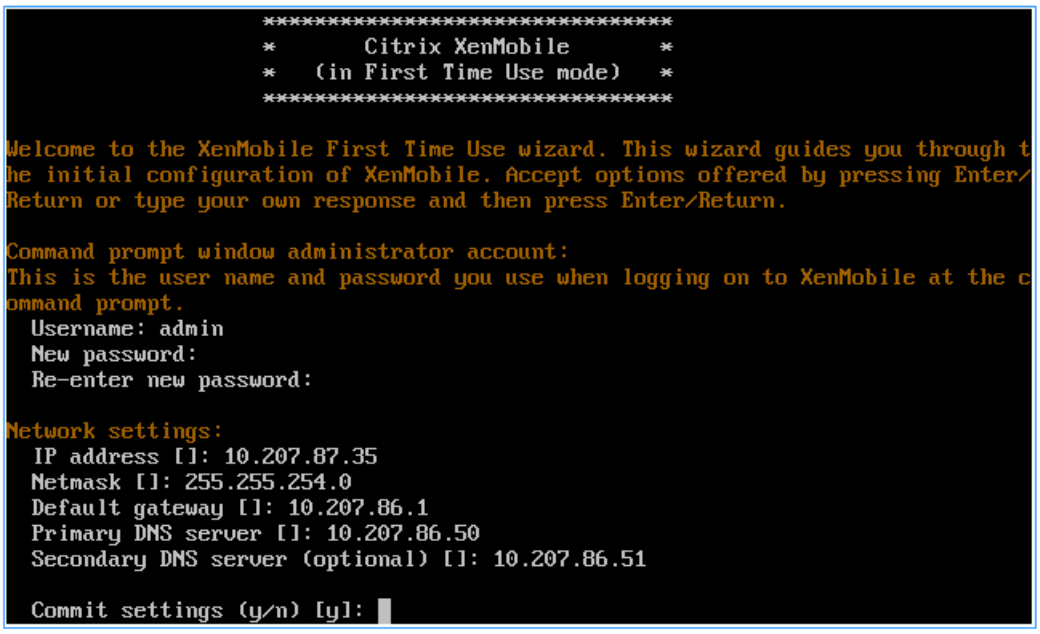
Aktivieren und Ausführen des Upgrade Tools

Aktivieren Sie das Upgrade Tool über die Befehlszeilenschnittstelle (CLI) bei der Erstinstallation von XenMobile 10.4.

> **Important**
>
> Wenn Sie einen Snapshot des Systems erstellen möchten, tun Sie dies nach der anfänglichen XenMobile 10.4-Konfiguration und vor dem Zugriff auf das Upgrade Tool.

1. Geben Sie in der CLI Ihren Administratorbenutzernamen, das zugehörige Kennwort und Ihre Netzwerkeinstellungen ein.

2. Geben Sie **y** ein, um die Einstellungen zu übergeben.

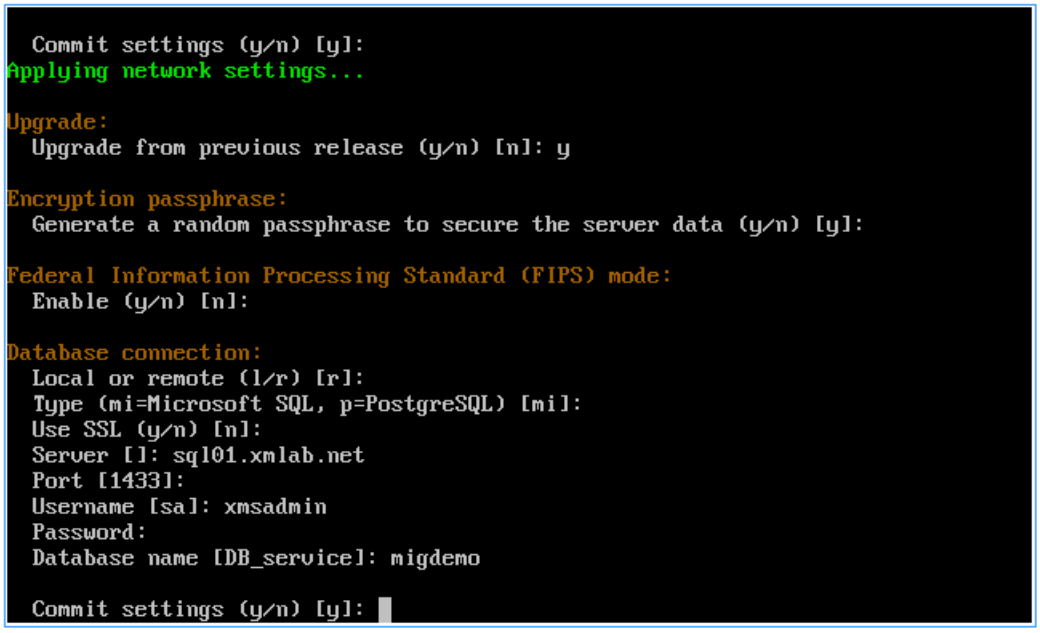


3. Geben Sie **y** ein, um das Upgrade durchzuführen.

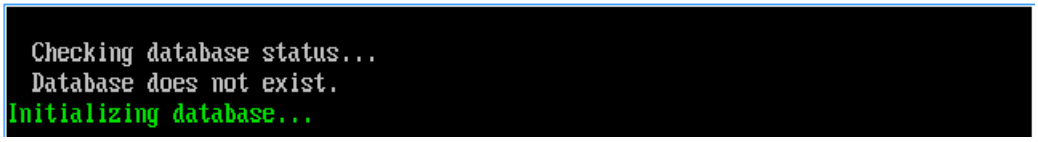
> ## Hinweis
>
> Wenn Sie hier nicht "y" eingeben, müssen Sie eine neue XenMobile 10.4-Instanz in der Befehlszeilenkonsole konfigurieren und das Upgrade Tool erneut starten.

4. Wählen Sie die Erstellung einer zufälligen Passphrase aus und aktivieren Sie optional FIPS. Geben Sie die Datenbankverbindungsinformationen ein.

5. Geben Sie **y** ein, um die Einstellungen zu übergeben.



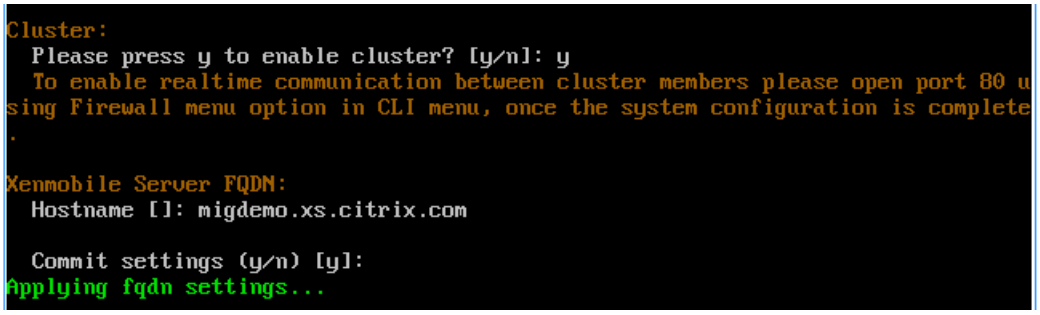
XenMobile initialisiert die Datenbank.



6. Wählen Sie aus, ob geclusterte Server aktiviert werden sollen. Geben Sie den vollqualifizierten Domänennamen (FQDN) von XenMobile ein. Beachten Sie Folgendes:

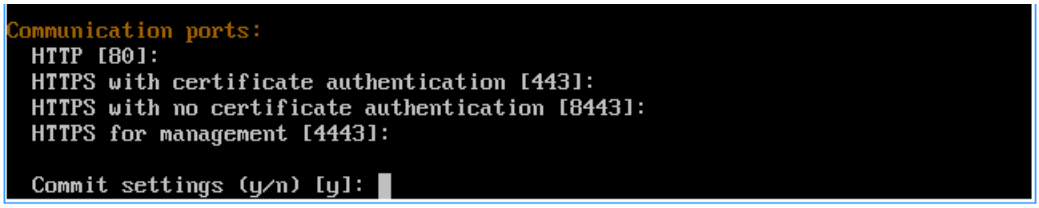
- Bei Bereitstellungen von XenMobile Enterprise Edition ist der FQDN derselbe wie der FQDN von XenMobile 9.0 MDM.
- Bei MAM-Bereitstellungen ist der FQDN derselbe wie der FQDN von XenMobile 9.0 App Controller.
- Bei MDM-Bereitstellungen ist der FQDN derselbe wie der FQDN von XenMobile 9.0 Device Manager.

> **Important**
>
> Der FQDN der 9.0-Umgebung muss mit dem der 10.4-Umgebung übereinstimmen.



7. Geben Sie **y** ein, um die Einstellungen zu übergeben.

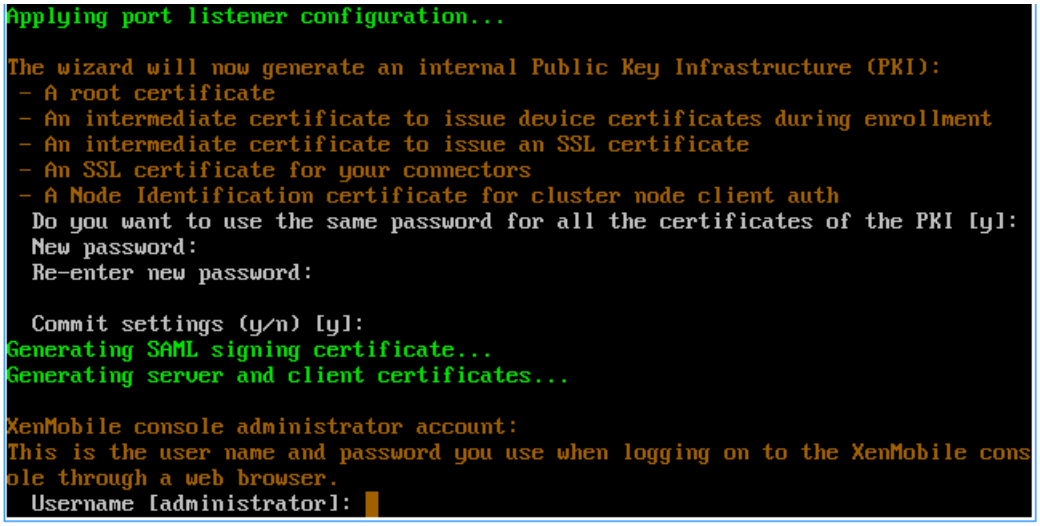
8. Legen Sie die Kommunikationsports fest.



9. Geben Sie **y** ein, um die Einstellungen zu übergeben.

10. Wählen Sie aus, ob das gleiche Kennwort für alle Zertifikate verwendet werden soll, und geben Sie das Kennwort ein.

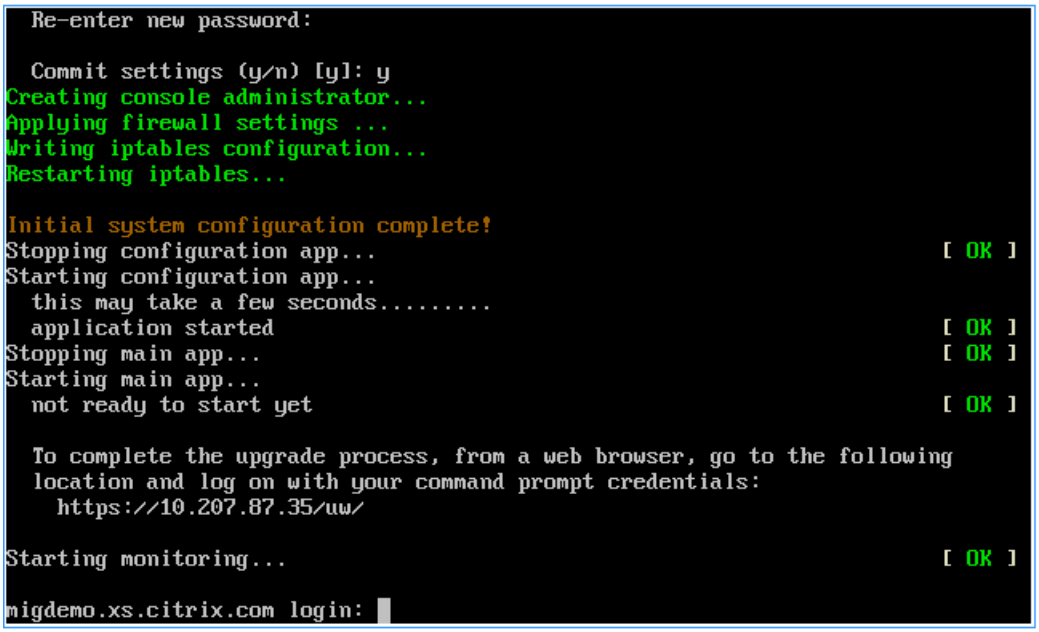
11. Geben Sie **y** ein, um die Einstellungen zu übergeben.



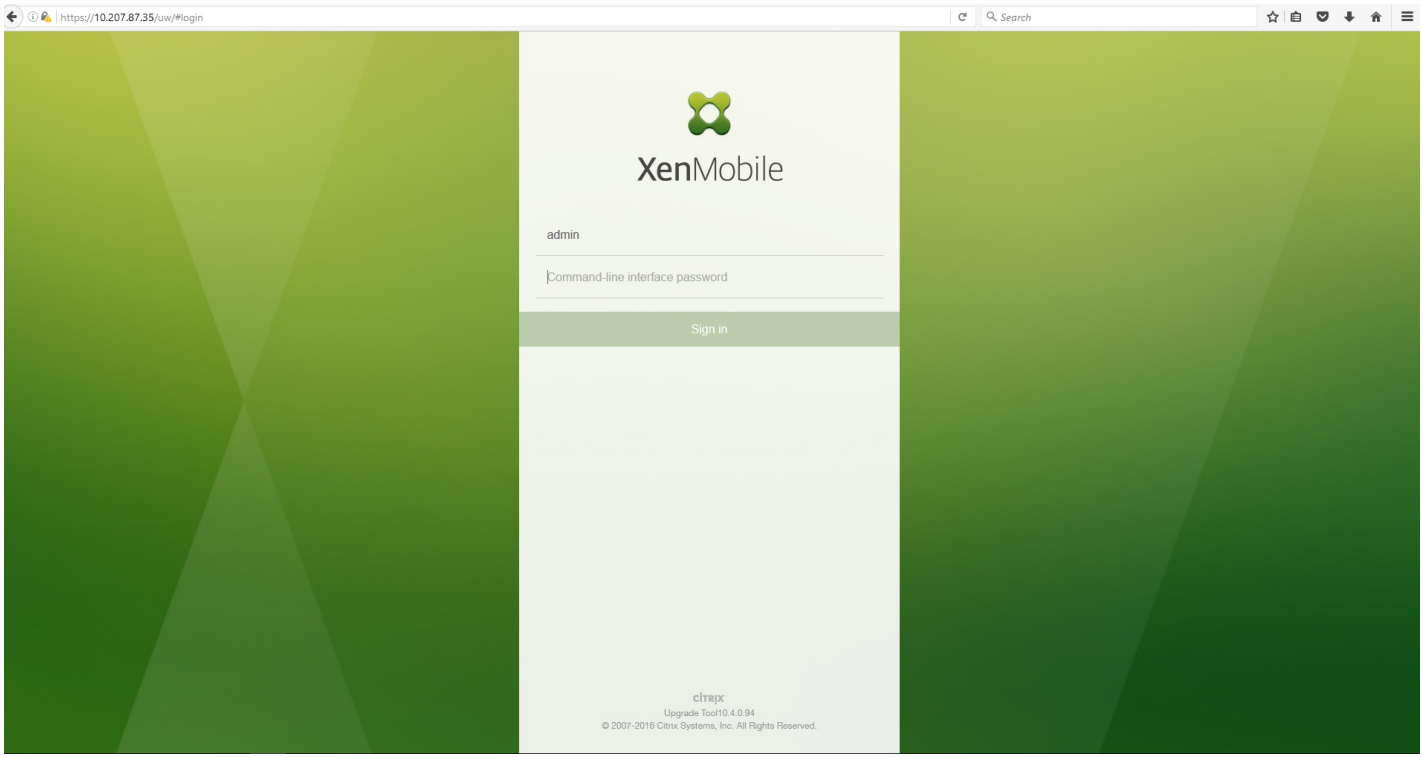
12. Geben Sie den Benutzernamen und das Kennwort für den XenMobile-Konsolenadministrator ein.

13. Geben Sie **y** ein, um die Einstellungen zu übergeben.

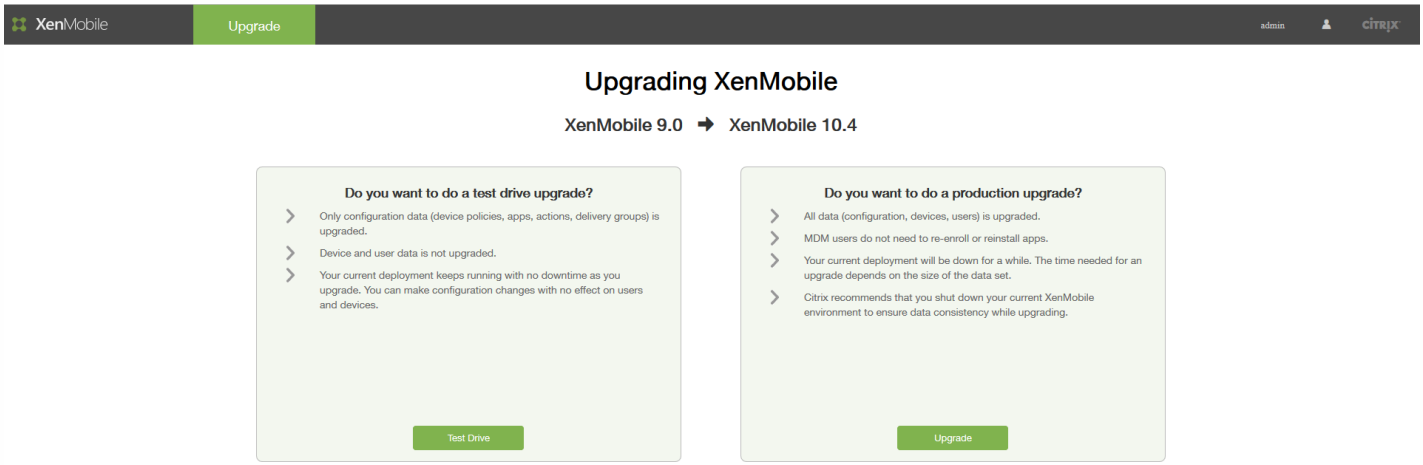
Von XenMobile 10.4 wird das Upgrade Tool zur einmaligen Verwendung aktiviert.



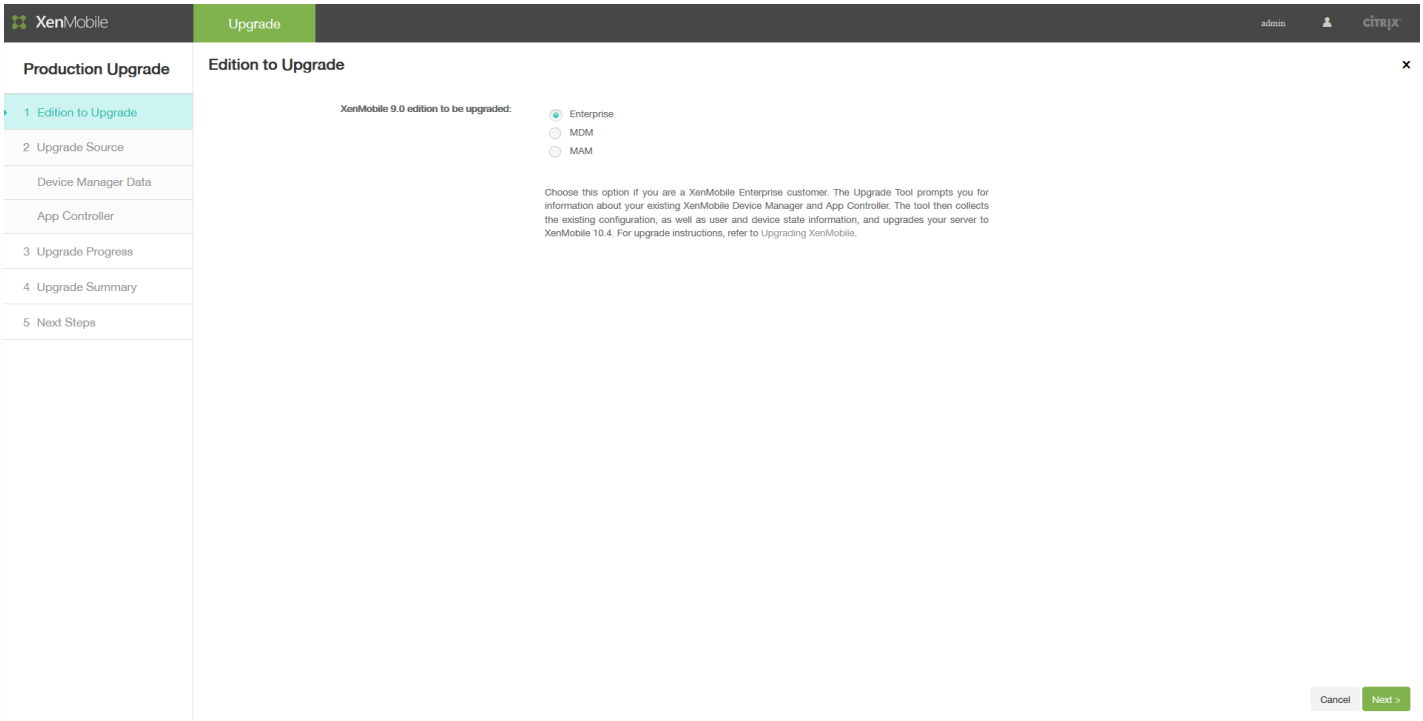
14. Greifen Sie auf das Upgrade Tool mit einem Browser unter der Adresse https://<IP-Adresse des XenMobile-Servers>/uw/ zu und melden Sie sich mit den Anmeldeinformationen an, die Sie in der CLI festgelegt haben.



15. Sie können nun auswählen, ob Sie das Upgrade testen oder ein vollständiges Produktionsupgrade durchführen möchten. Die nachfolgenden Anweisungen gelten für ein Produktionsupgrade. Klicken Sie auf der Seite **Upgrading XenMobile** auf **Next**.



16. Wählen Sie auf der Seite **Edition to Upgrade** Ihre Edition. Die Abbildung unten zeigt die Enterprise Edition als ausgewählt.



17. Klicken Sie auf **Weiter**.

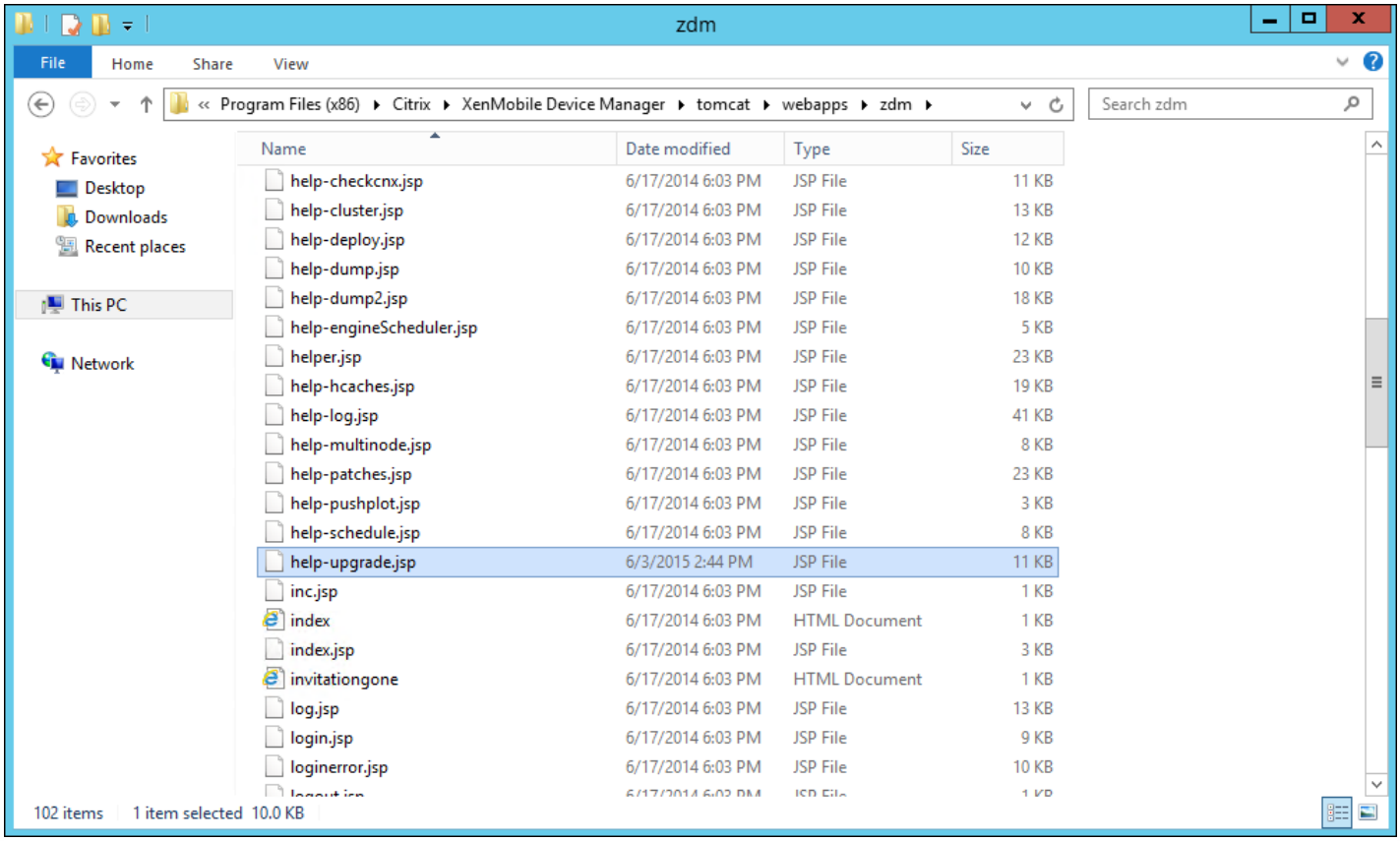
Wenn Sie eine Enterprise- oder MDM-Edition aktualisieren, wird die Seite **Device Manager** angezeigt. Führen Sie die Schritte 18 bis 22 für diese Seite aus.

Wenn Sie eine MAM-Edition aktualisieren, fahren Sie mit Schritt 23 zum Ausfüllen der Seite **App Controller** fort.

18. Sammeln Sie die für die Migration der vorhandenen XenMobile 9.0 Device Manager-Daten erforderlichen Dateien. Sie erhalten ebenfalls Zugriff auf die Datenbank-URL und den Benutzernamen, den Sie in die Seite **Device Manager** kopieren müssen.

a. Klicken Sie auf den Link in Schritt 1 auf der Seite **Device Manager** und speichern Sie die heruntergeladene Datei help-upgrade.zip.

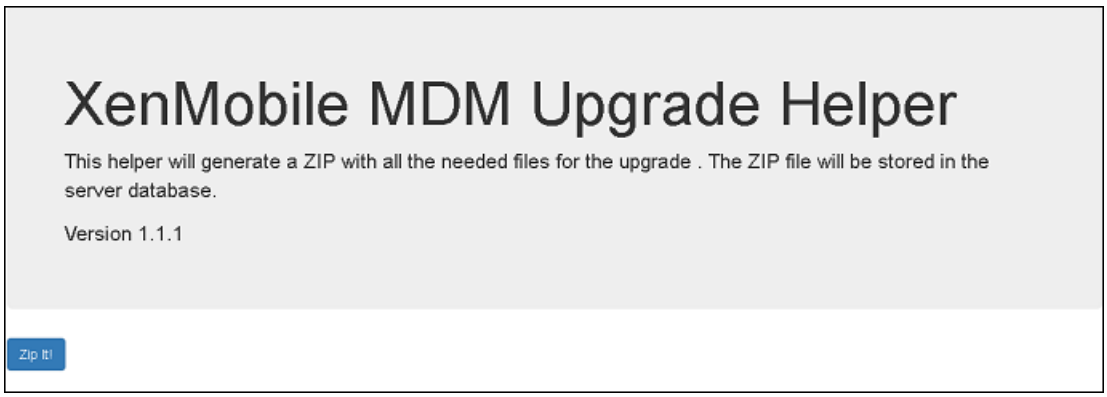
b. Extrahieren Sie die Datei help-upgrade.jsp auf dem Computer mit XenMobile 9.0 Device Manager in das Verzeichnis <MDM-Installationspfad>\tomcat\webapps\zdm.



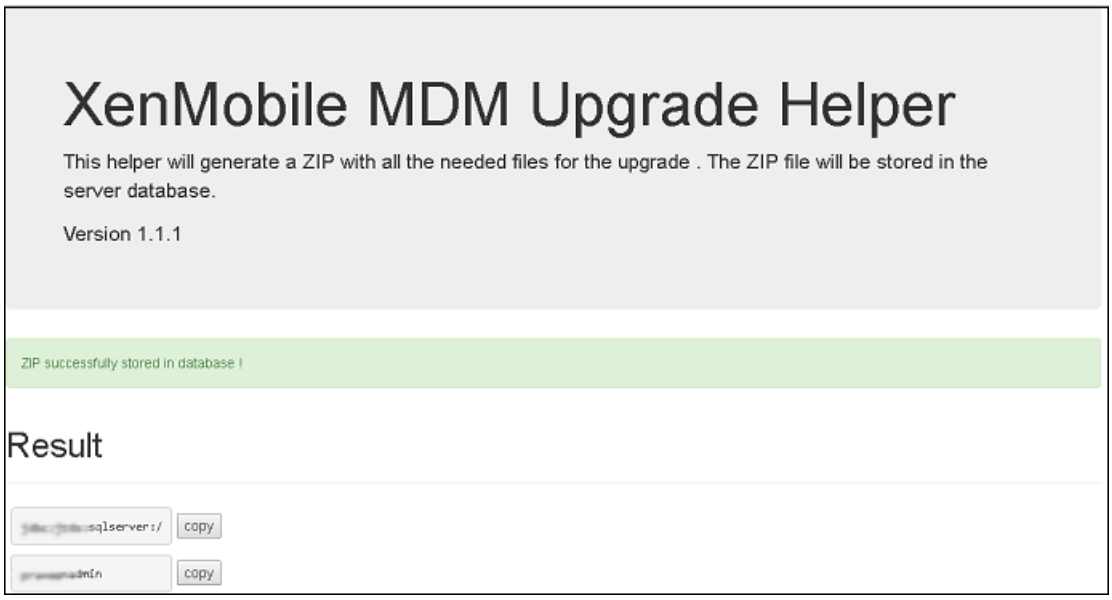
c. Melden Sie sich in einem Browserfenster beim XenMobile 9.0-Server an.

d. Geben Sie in einer separaten Browserregisterkarte die URL https://localhost/zdm/help-upgrade.jsp ein. Damit wird die Seite **XenMobile MDM Upgrade Helper** geöffnet, über die alle XenMobile 9.0-Dateien, die für das Upgrade auf XenMobile 10.4 erforderlich sind, gesammelt und komprimiert werden. Die ZIP-Datei wird dann in der Serverdatenbank gespeichert und von dort aus extrahiert.

e. Klicken Sie auf **Zip it** und befolgen Sie die angezeigten Schritte zum Sammeln der für das Upgrade erforderlichen Dateien.



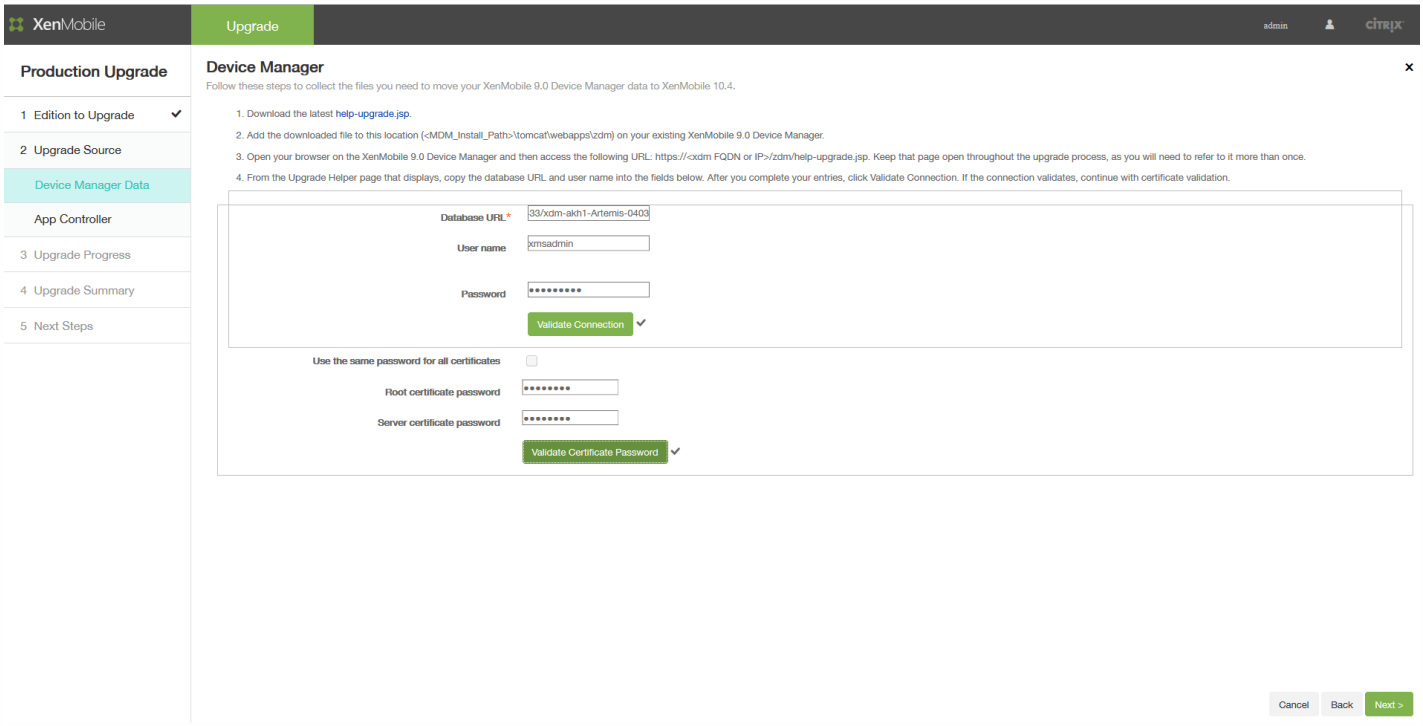
19. Kopieren Sie die unter **Result** angezeigte URL und fügen Sie sie in das Feld **Database URL** auf der Seite **Device Manager** des Upgrade Tools ein. Kopieren Sie anschließend den Benutzernamen und fügen Sie ihn auf der Seite **Device Manager** ein.



20. Führen Sie im Upgrade Tool folgende Schritte aus:

    a. Geben Sie das Kennwort ein und klicken Sie dann auf **Validate Connection**.

    b. Geben Sie das Kennwort für jedes Zertifikat ein und klicken Sie dann auf **Validate Password**.

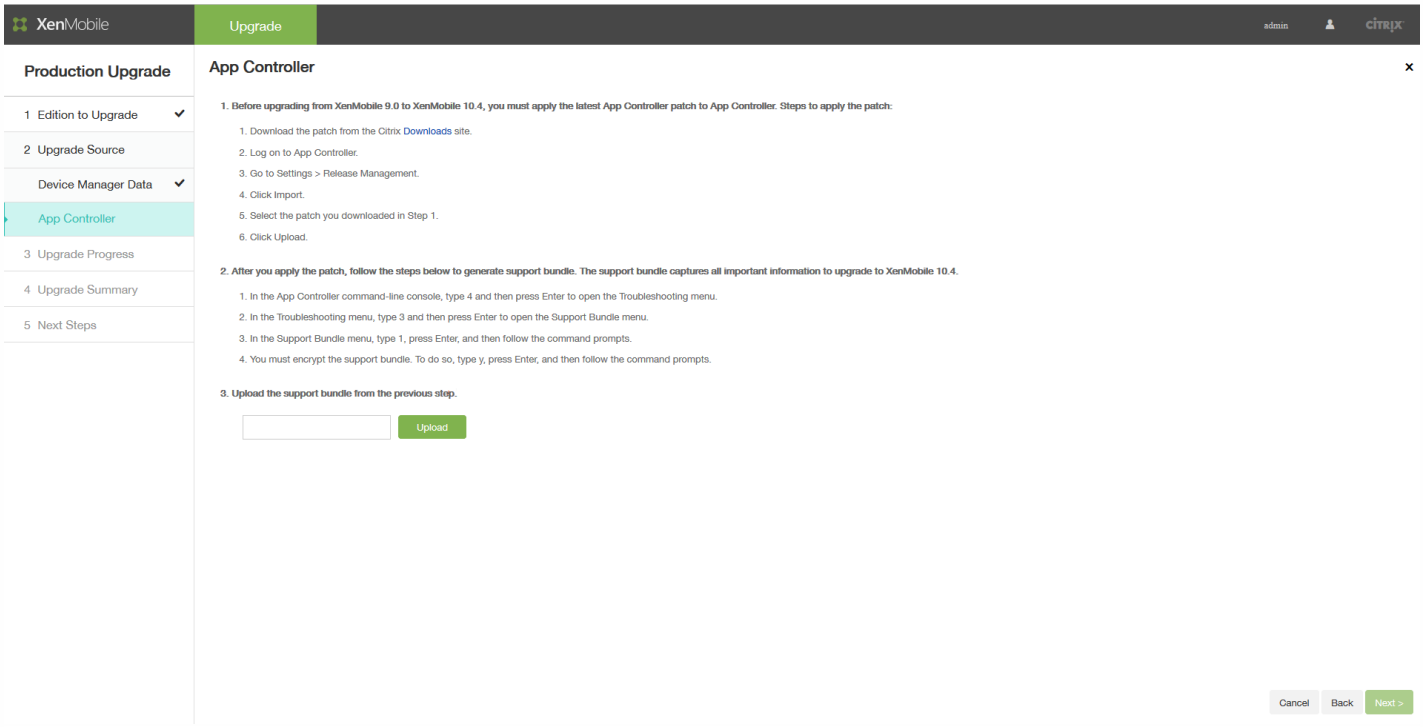


21. Klicken Sie auf **Weiter**.

22. Wenn Sie die Datei ew-config.properties geändert haben, starten Sie den XDM-Dienst unter XenMobile 9 MDM neu und rufen Sie https://localhost/zdm/help-upgrade.jsp auf, um die ZIP-Komprimierung zu wiederholen. Auf diese Weise wird die Datei ew-config.properties neu gelesen und in der XenMobile MDM 9-Datenbank zur Vorbereitung auf die Migration

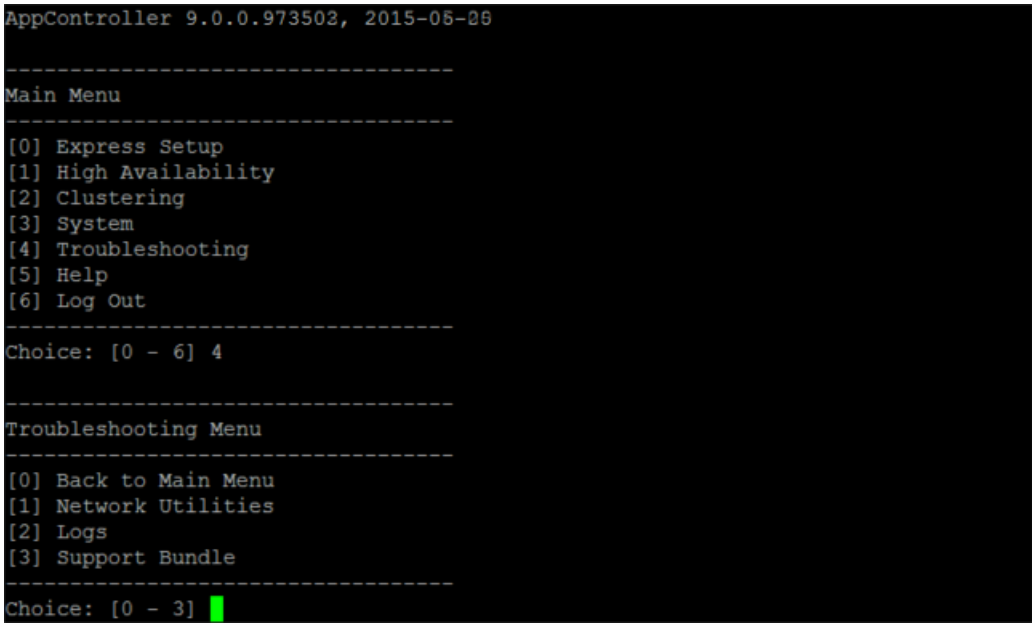
gespeichert.

23. Als Nächstes wenden Sie auf App Controller ein Upgrade-Patch an, generieren ein Supportpaket und laden dieses hoch. Führen Sie zunächst ein App Controller-Upgrade gemäß den Anweisungen in Abschnitt 1 der Seite **App Controller** durch.

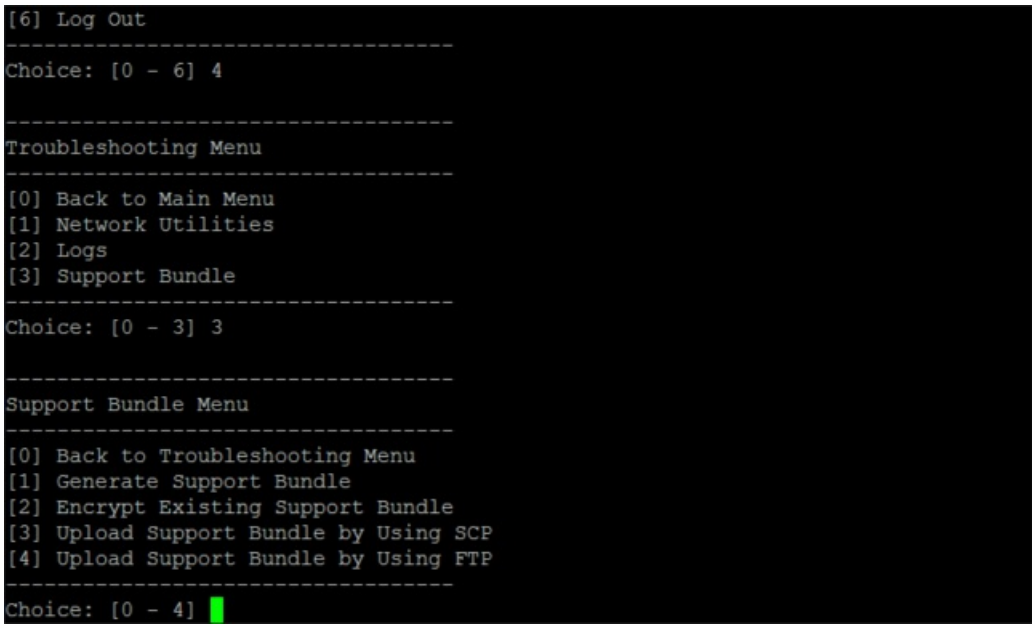


25. Fahren Sie mit den Anweisungen in Abschnitt 2 der Seite **App Controller** fort:

a. Geben Sie in der App Controller-Befehlszeilenkonsole den Wert **4** ein und drücken Sie die EINGABETASTE, um das Menü "Troubleshooting" zu öffnen.

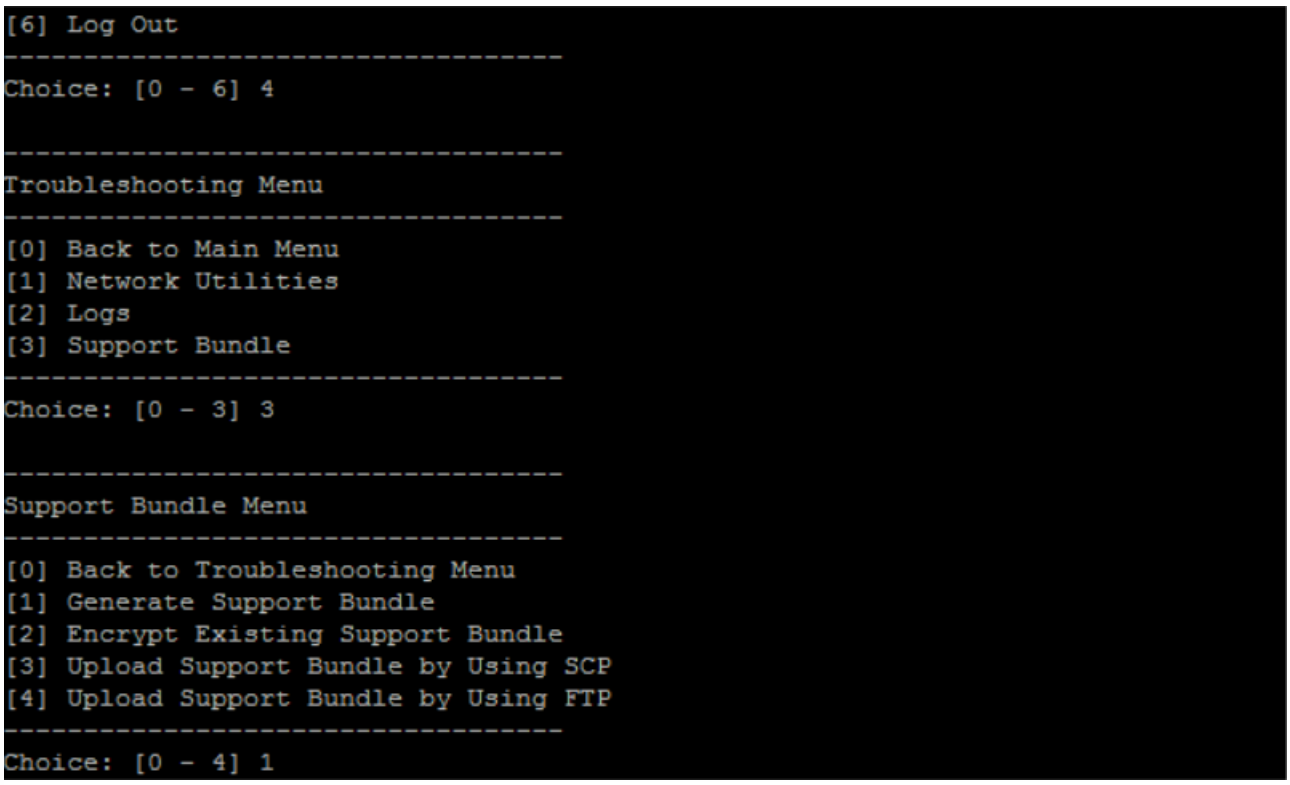


b. Im Menü "Troubleshooting" geben Sie **3** ein und drücken die EINGABETASTE, um das Menü "Support Bundle" zu öffnen.



c. Im Menü "Support Bundle" geben Sie **1** ein und drücken Sie die EINGABETASTE. Folgen Sie dann den Eingabeaufforderungen.

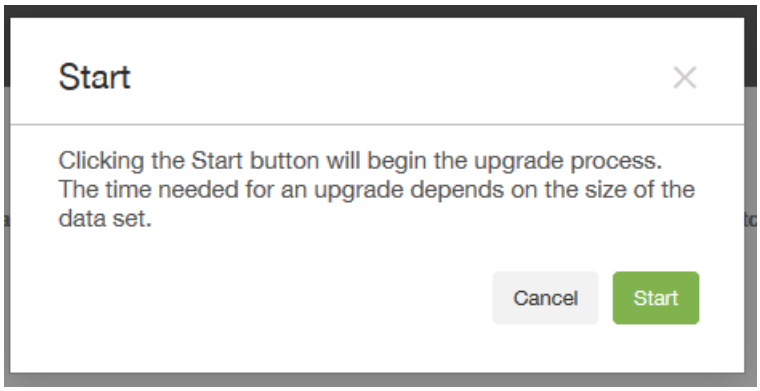
Hinweis: Sie müssen das Supportpaket verschlüsseln.



26. Geben Sie in Abschnitt 3 auf der Seite **App Controller** das Supportpaket an und klicken Sie auf **Upload**.

Das Upgrade Tool verarbeitet die gesammelten Dateien (XenMobile Enterprise Edition und MAM-Edition) und das Supportpaket. Dieser Vorgang kann länger als 15 Minuten dauern, wenn zahlreiche Benutzer migriert werden.

27. Klicken Sie auf **Weiter**. Das Bestätigungsdialogfeld zum Starten wird angezeigt.



28. Klicken Sie auf **Start**. Die nun angezeigte Seite **Upgrade Progress** enthält Fortschrittsanzeigen, anhand derer Sie das Datenupgrade von XenMobile 9.0 beobachten können. Wenn das Upgrade abgeschlossen ist, stehen die Fortschrittsanzeigen auf 100 % und die Schaltfläche **Next** wird verfügbar.

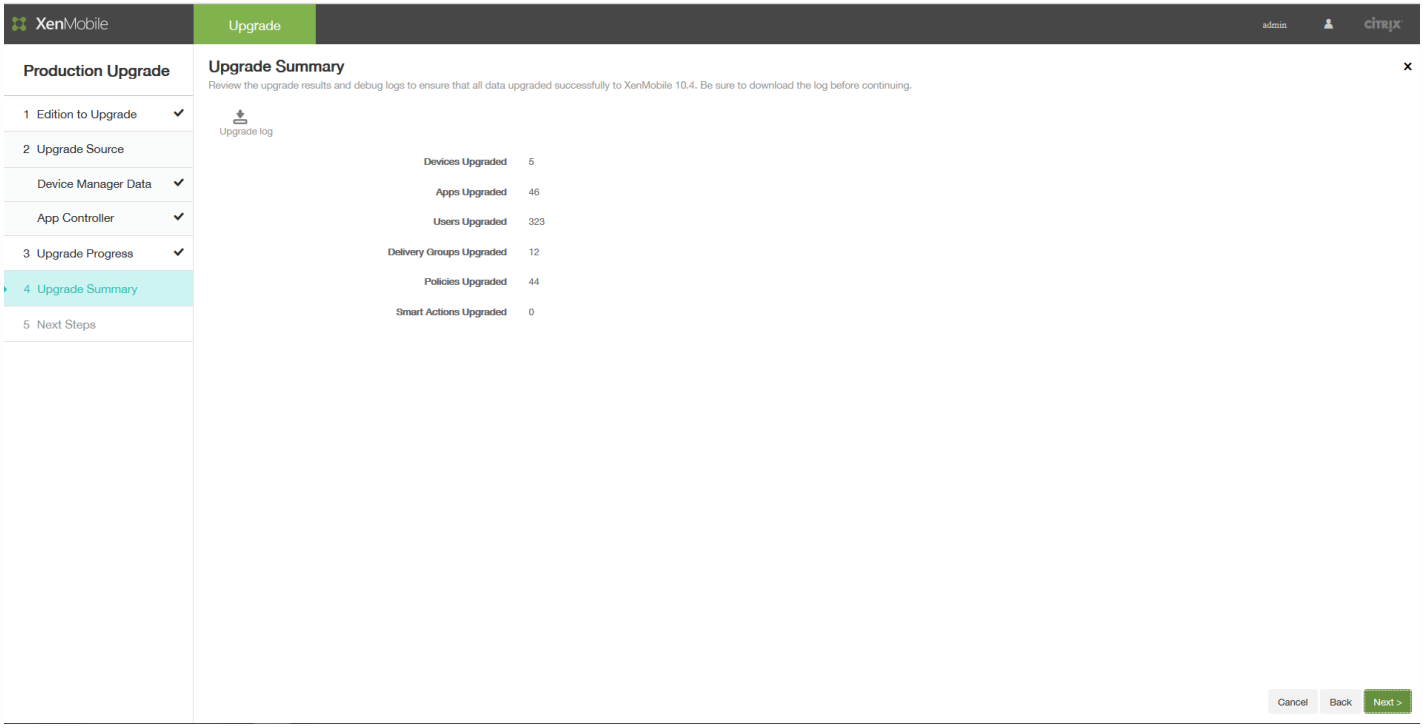
Hinweis

Wenn das Upgrade fehlschlägt, können Sie die Protokolle anzeigen, um die Ursache des Problems zu ermitteln. Sie müssen dann eine neue XenMobile 10.4-Instanz importieren und das Upgrade neu starten. Sie können nicht mit der Schaltfläche "Zurück" des Browsers zu vorherigen Seiten zurückkehren und Informationen korrigieren.

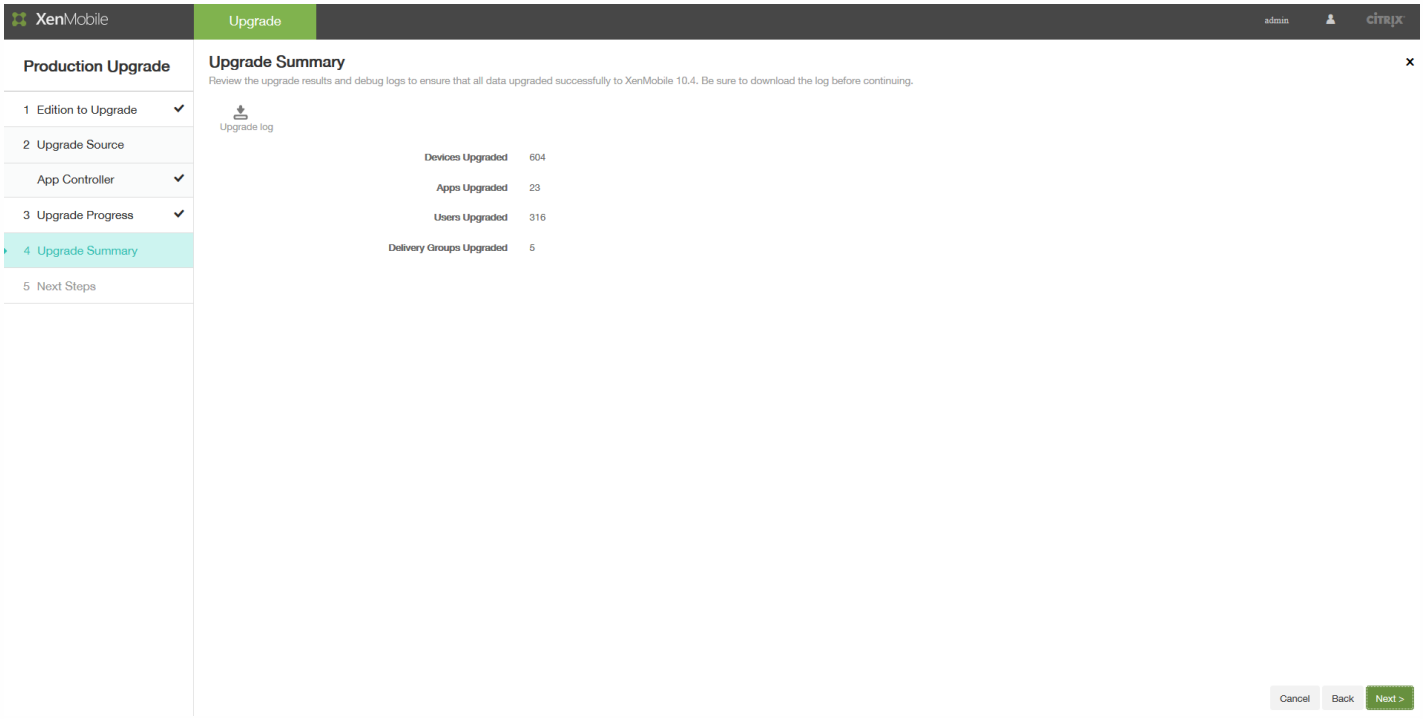
Auf der Seite "Upgrade Progress" wird gemeldet, wenn das Upgrade erfolgreich durchgeführt wurde.

29. Klicken Sie auf **Weiter**. Die Seite **Upgrade Summary** wird angezeigt.

Wenn Sie ein Upgrade einer Enterprise Edition oder MAM-Edition durchführen, sieht die Seite **Upgrade Summary** ungefähr so aus:



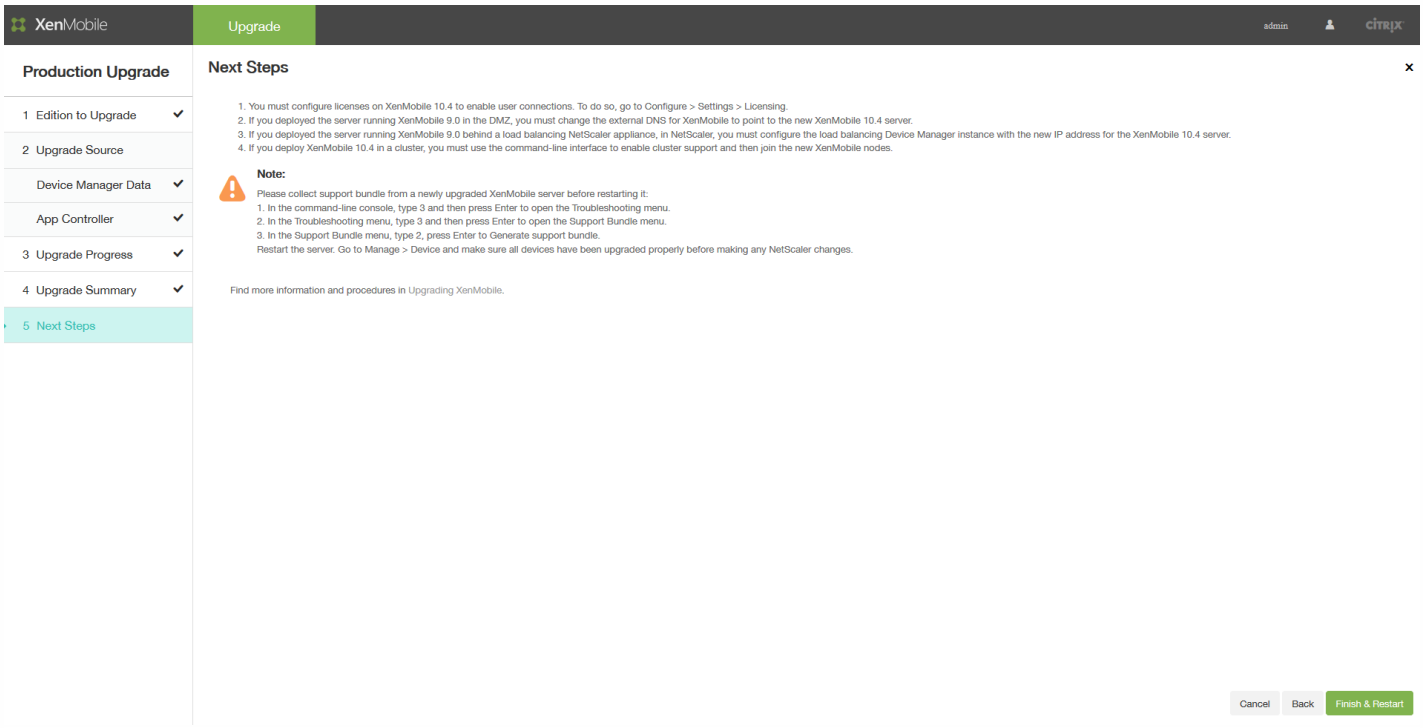
Wenn Sie ein Upgrade einer MDM-Edition durchführen, sieht die Seite **Upgrade Summary** ungefähr so aus:



30. Klicken Sie auf das Symbol für das Upgradeprotokoll, um das Protokoll herunterzuladen. Laden Sie das Protokoll herunter, bevor Sie die Seite verlassen.

Citrix empfiehlt, dass Sie anhand des Protokolls prüfen, ob Richtlinien, Einstellungen, Benutzerdaten usw. einwandfrei auf XenMobile 10.4 aktualisiert wurden.

31. Nach dem Herunterladen des Upgradeprotokolls klicken Sie auf **Next**. Die Seite **Next Steps** wird angezeigt.



Anweisungen zu diesen Schritten finden Sie unter Nachbereitung eines Upgrades.

Nachbereitung eines Upgrades

Feb 24, 2017

Wenn das Upgrade mit dem Upgrade Tool abgeschlossen ist, liefert dieses eine Übersicht über die nächsten Schritte. Welche Art der Nachbereitung erforderlich ist, hängt von der installierten NetScaler-Version ab, davon, ob Sie den NetScaler für XenMobile-Assistenten zum Konfigurieren von NetScaler verwendet haben, und von Ihrer XenMobile Edition.

Lesen Sie die nachfolgende Liste der Nachbereitungsaufgaben durch und führen Sie alle für Ihre Umgebung erforderlichen aus.

1. Konfigurieren von Lizenzen in XenMobile zur Ermöglichung von Benutzerverbindungen Weitere Informationen finden Sie in diesem Verfahren.

2. Wenn Sie den Server mit XenMobile 9.0 in der DMZ bereitgestellt haben, ändern Sie das externe DNS für XenMobile dahingehend, dass es auf den neuen XenMobile 10.4-Server verweist.

3. Wenn Sie den Server mit XenMobile 9.0 hinter einem NetScaler Gateway-Gerät mit Lastausgleich bereitgestellt haben, nehmen Sie die folgenden Änderungen bei NetScaler durch:

   a. Konfigurieren eines neuen virtuellen Lastausgleichservers für das Upgrade Weitere Informationen finden Sie in diesem Verfahren.

   b. Konfigurieren eines Adresseintrags zum Verweisen des FQDN des App Controller-Servers auf den neuen Lastenausgleichsserver für das Upgrade Weitere Informationen finden Sie in diesem Verfahren.

   c. Ändern des virtuellen Lastausgleichsservers für Device Manager, sodass er auf die neue IP-Adresse des XenMobile-Servers verweist Weitere Informationen finden Sie in diesem Verfahren.

   d. Ändern von NetScaler Gateway, sodass es auf den neuen FQDN des XenMobile-Servers verweist Weitere Informationen finden Sie in diesem Verfahren.

   e. Die folgenden Aufgaben gelten nur für folgende Fälle:

      – Sie haben den NetScaler für XenMobile 9-Assistenten in NetScaler 11.1, 11.0 oder 10.5 verwendet.

      – Sie verwenden NetScaler Gateway 10.1 (nicht empfohlen).

      – Sie haben zum Konfigurieren von NetScaler 10.5 oder einer höheren Version für XenMobile nicht den NetScaler für XenMobile-Assistenten verwendet.

   Die Verfahren für die oben aufgeführten Fälle finden Sie in den folgenden Artikeln der Dokumentation für das XenMobile Upgrade Tool 10.1:

      Erstellen eines virtuellen MAM-Lastausgleichsservers auf der Grundlage einer SSL-Brücke
      Erstellen eines virtuellen MAM-Lastausgleichsservers auf der Grundlage einer SSL-Offload-MDM-Konfiguration

4. Wenn Sie XenMobile 10.4 in einem Cluster bereitstellen, müssen die Clusterunterstützung mit der XenMobile 10.4-Befehlszeilenoberfläche (CLI) aktivieren und die neuen XenMobile-Knoten anfügen. Informationen zur Verwendung der XenMobile-CLI finden Sie unter Optionen des Menüs "Clustering".

5. Führen Sie die restlichen, für Ihre Umgebung erforderlichen Nachbereitungsschritte aus.

In diesem Abschnitt werden auch Nachbereitungsschritte für die Secure Ticket Authority, den Network Time Protocol-Server (NTP), den Hostnamen des XenMobile-Servers, die Aktualisierung nicht im Upgrade eingeschlossener Informationen, benutzerdefinierte Storenamen und die XenMobile-Geräteregistrierung nach dem Upgrade behandelt.

Konfigurieren von Lizenzen in XenMobile zur Ermöglichung von Benutzerverbindungen

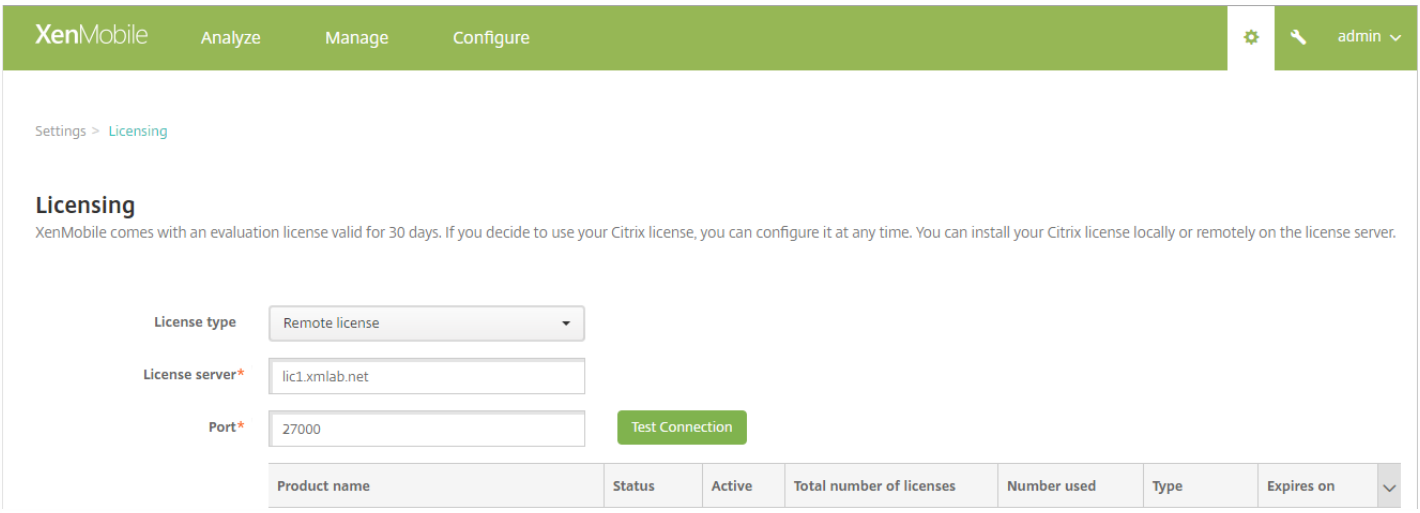
XenMobile 10.4 unterstützt nur die Citrix V6-Lizenzierung. Damit Benutzer Verbindungen herstellen können, müssen Sie die lokale bzw. Remote-Lizenzkonfiguration in der XenMobile 10.4-Konsole wie nachfolgend beschrieben festlegen.

1. Laden Sie die neue Lizenzdatei herunter. Anweisungen hierzu finden Sie unter Citrix Lizenzierung.

2. Melden Sie sich bei der aktualisierten XenMobile 10.4-Konsole an: Gehen Sie zu https://:4443.

- Bei einem MDM- oder ENT-Upgrade melden Sie sich mit Ihren Administratoranmeldeinformationen für XenMobile 9.0 Device Manager an.
- Bei einem MAM-Upgrade melden Sie sich mit Ihren Administratoranmeldeinformationen für XenMobile 9.0 App Controller an.

3. Gehen Sie zu **Einstellungen > Lizenzierung**.



Weitere Informationen zu lokalen und Remotelizenzen finden Sie unter Lizenzierung.

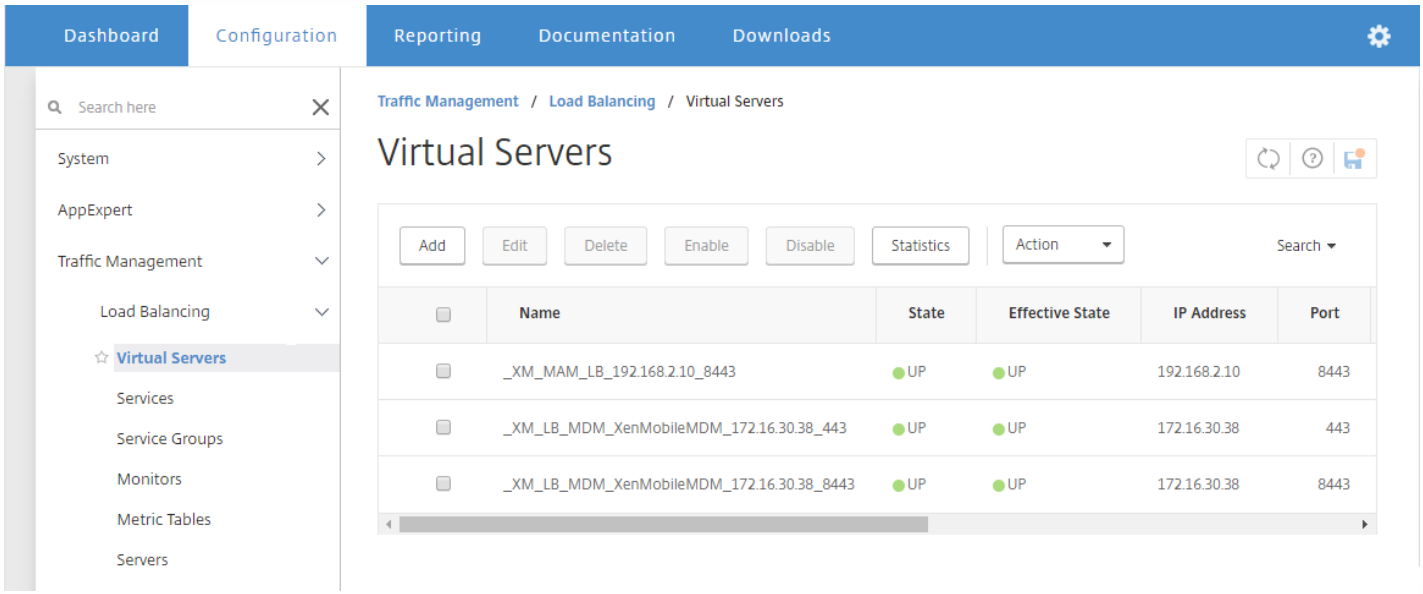
Konfigurieren eines neuen virtuellen Lastausgleichservers für das Upgrade

> **Important**
>
> Diese Nachbereitung ist nur für Produktionsupgrades von XenMobile Enterprise Edition erforderlich, nicht für MAM- oder MDM-Upgrades.

Nach einem Produktionsupgrade von XenMobile Enterprise Edition auf XenMobile 10.4 müssen Sie einen neuen virtuellen Lastausgleichserver für den XenMobile 9.0 App Controller-FQDN konfigurieren. Dafür verwenden Sie das NetScaler Gateway-Konfigurationstool.

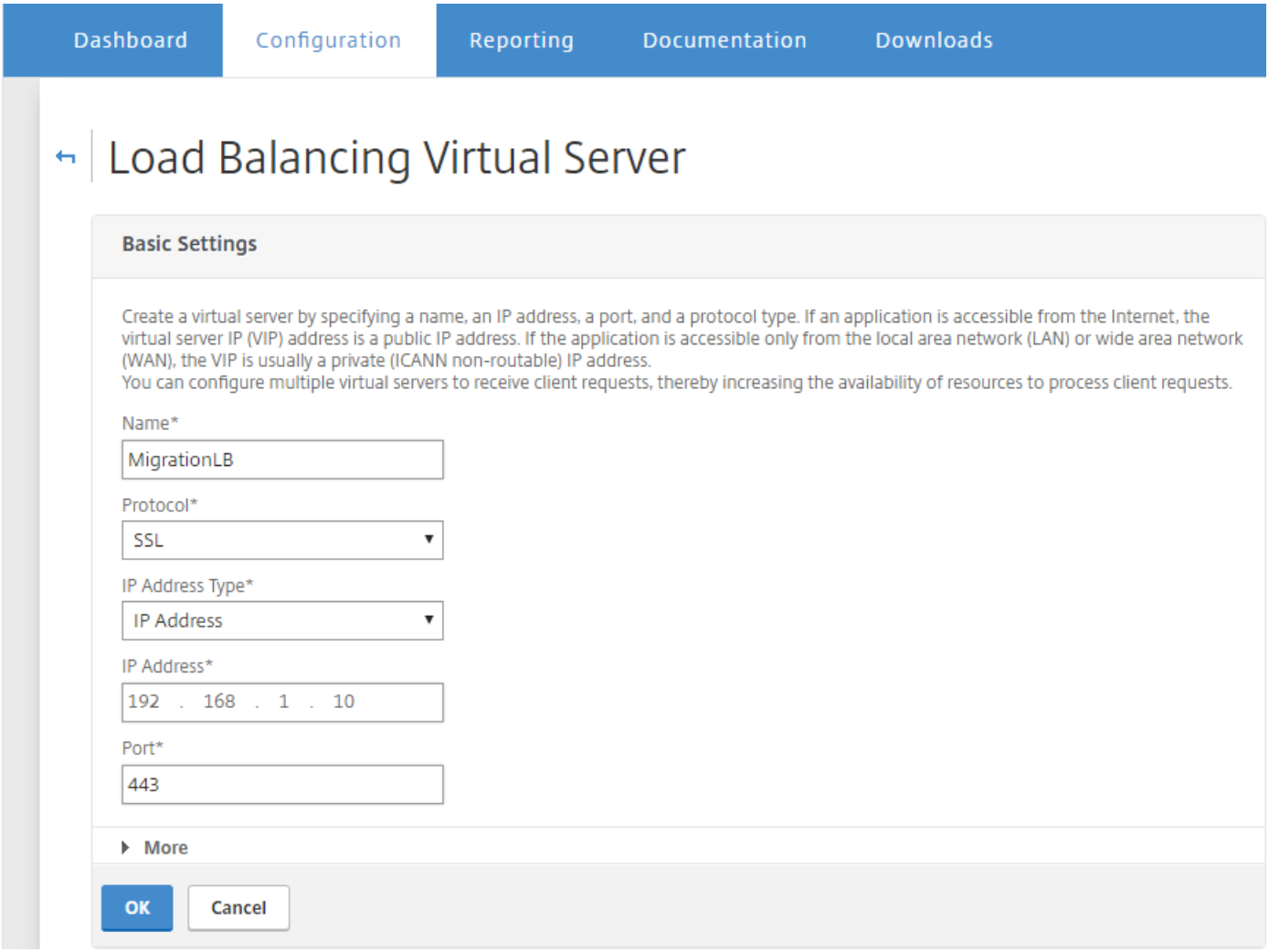
Die Screenshots in diesem Abschnitt zeigen NetScaler Gateway 11.1. Sie sind bei NetScaler Gateway 11.0 und 10.5 ähnlich.

1. Klicken Sie auf **Traffic Management > Load Balancing > Virtual Servers**.



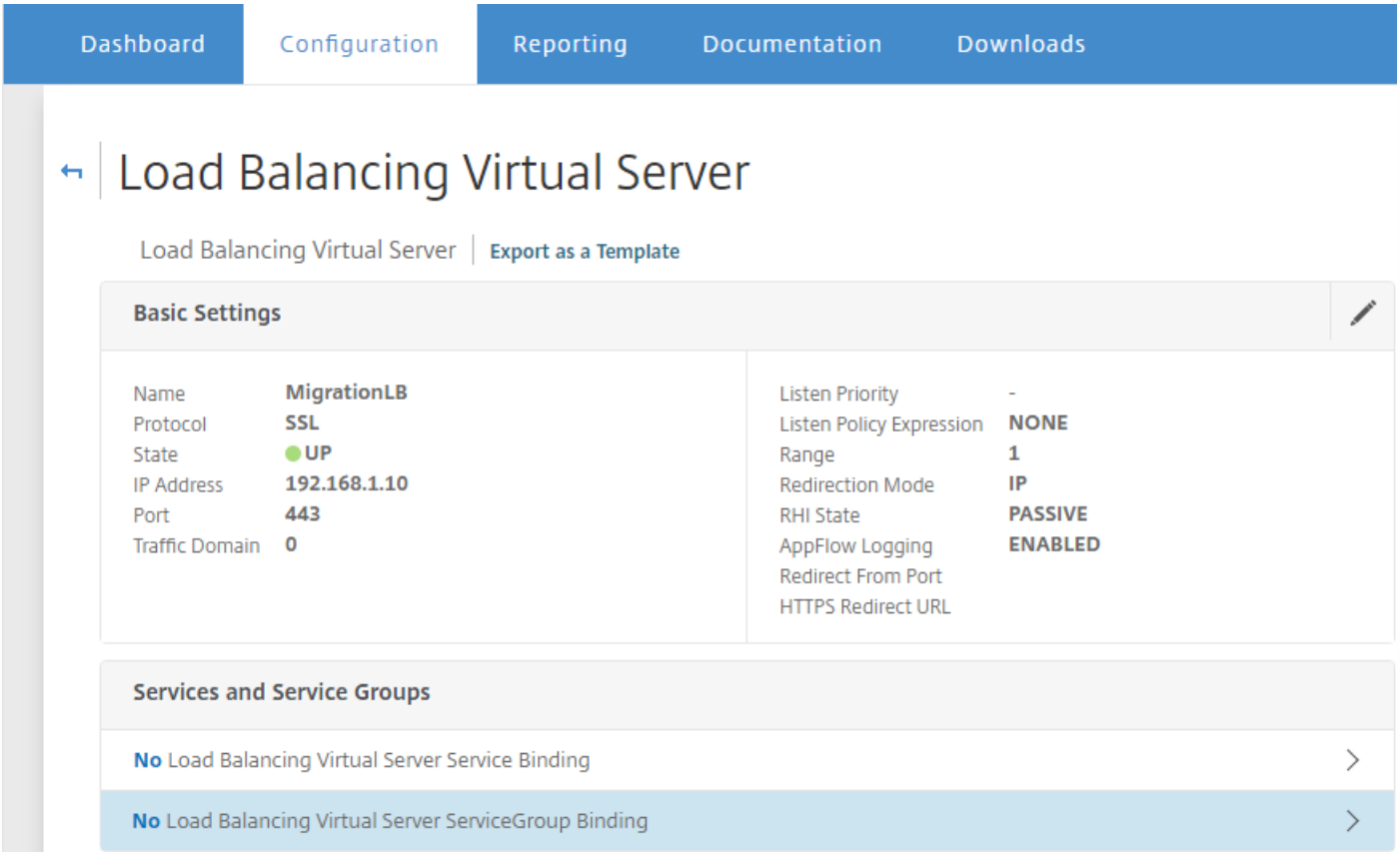
2. Klicken Sie auf **Hinzufügen**.

3. Konfigurieren Sie auf der Seite **Load Balancing Virtual Server** die folgenden Einstellungen und klicken Sie auf **OK**.

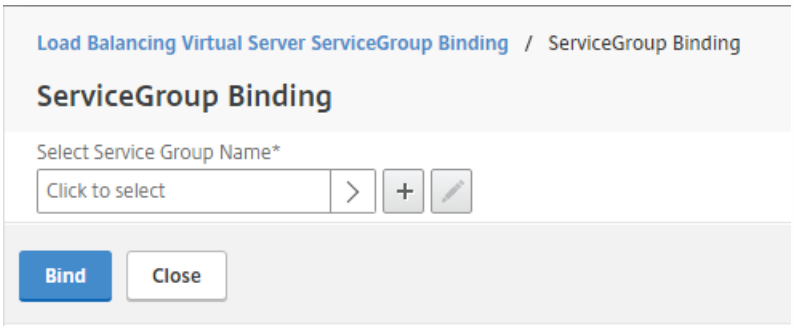


- **Name**: Geben Sie einen Namen für den neuen Load Balancer ein.
- **Protocol**: Wählen Sie **SSL**. Der Standardwert ist **HTTP**.
- **IP Address**: Geben Sie eine IP-Adresse für den neuen Load Balancer gemäß RFC 1918 ein, z. B. 192.168.1.10.
- **Port**: Legen Sie **443** fest.

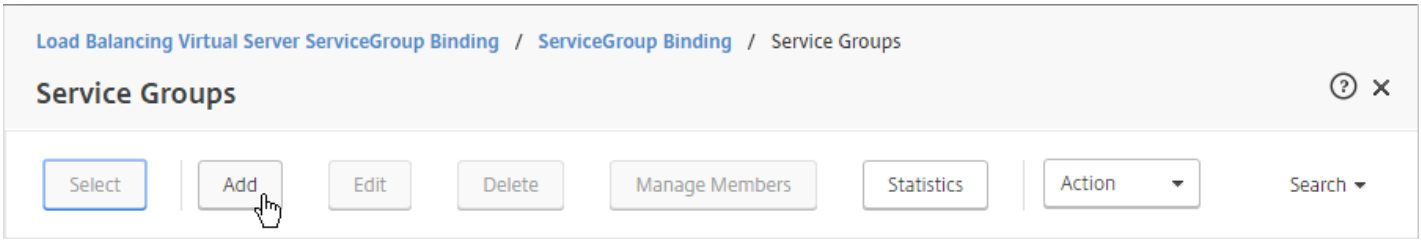
4. Klicken Sie unter **Services and Service Groups** auf **No Load Balancing Virtual Server Service Group Binding**.



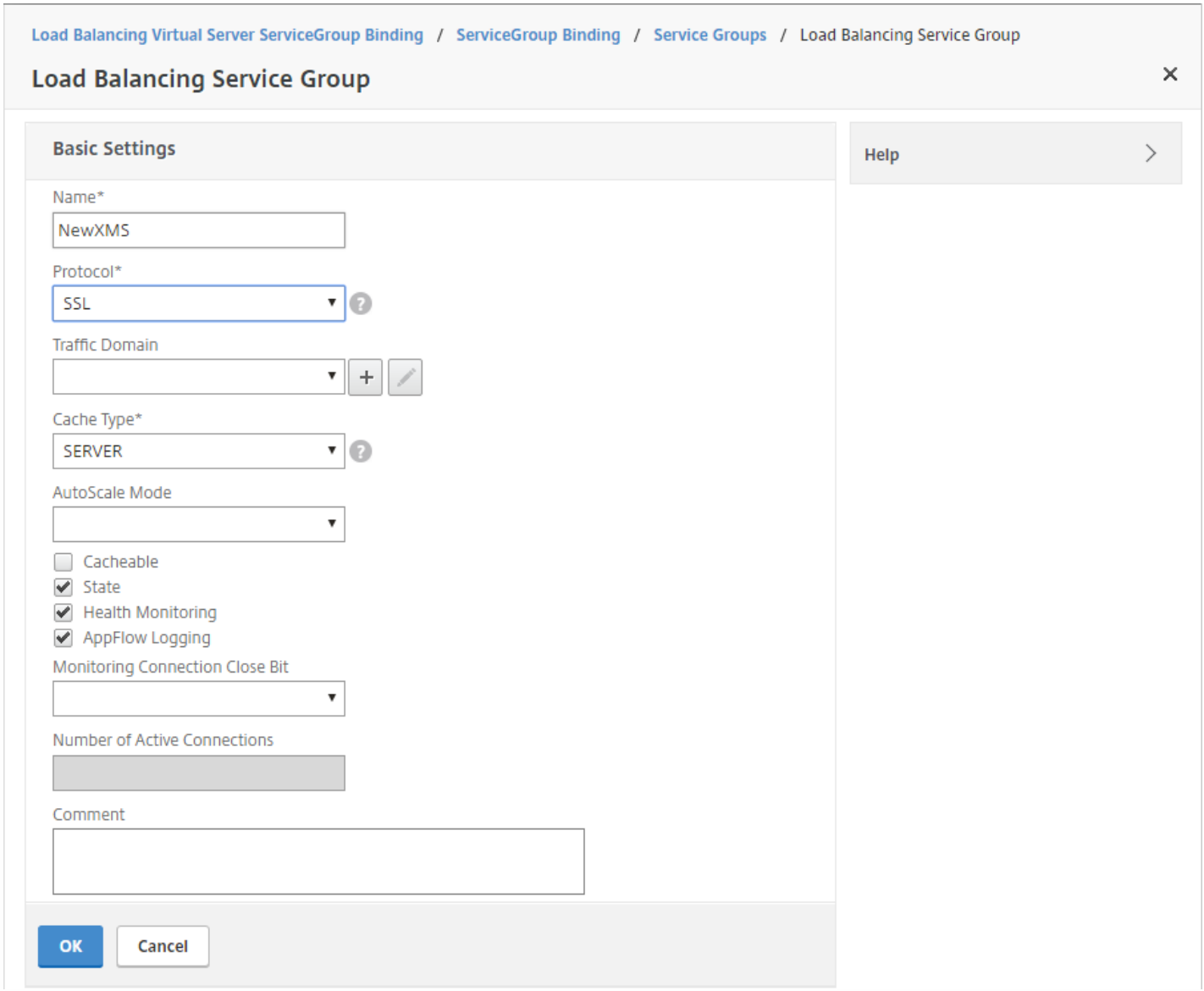
5. Klicken Sie unter **Select Service Group Name** auf **Click to Select**.



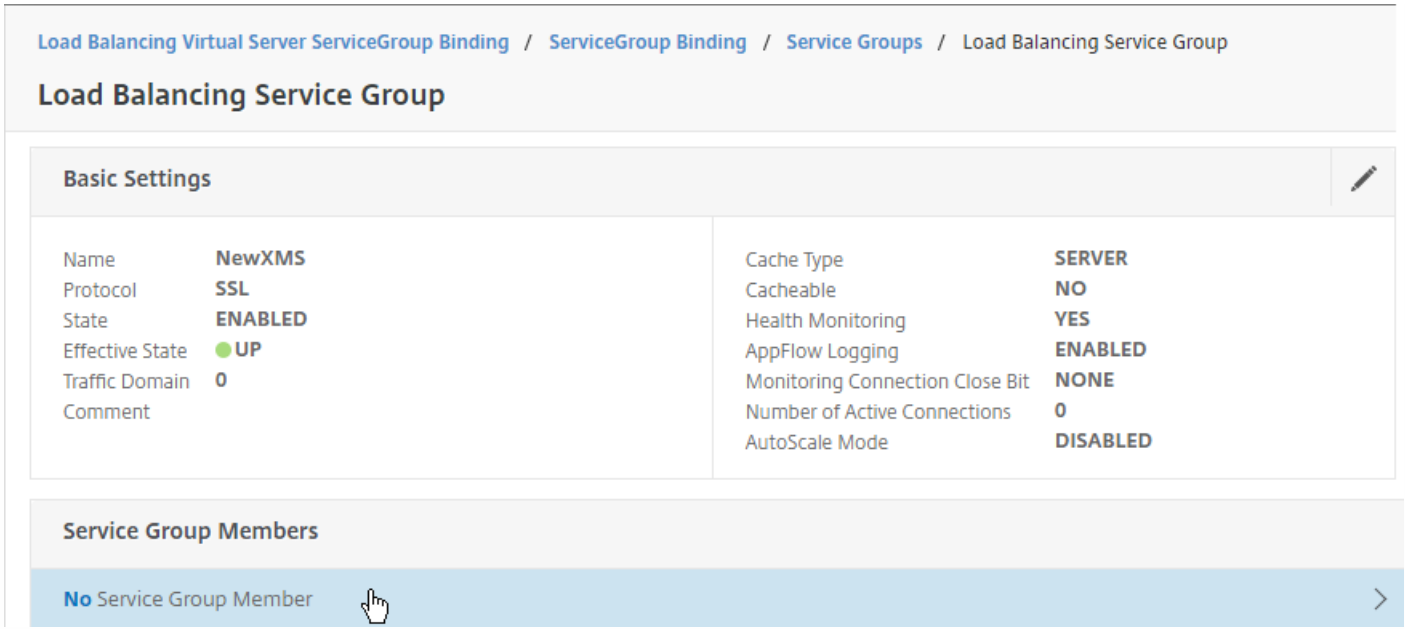
6. Klicken Sie auf **Add**, um eine neue Dienstgruppe zu erstellen.



7. Geben Sie auf der Seite **Load Balancing Service Group** einen Namen für die neue Dienstgruppe ein, legen Sie als Protokoll **SSL** fest und klicken Sie dann auf **OK**.

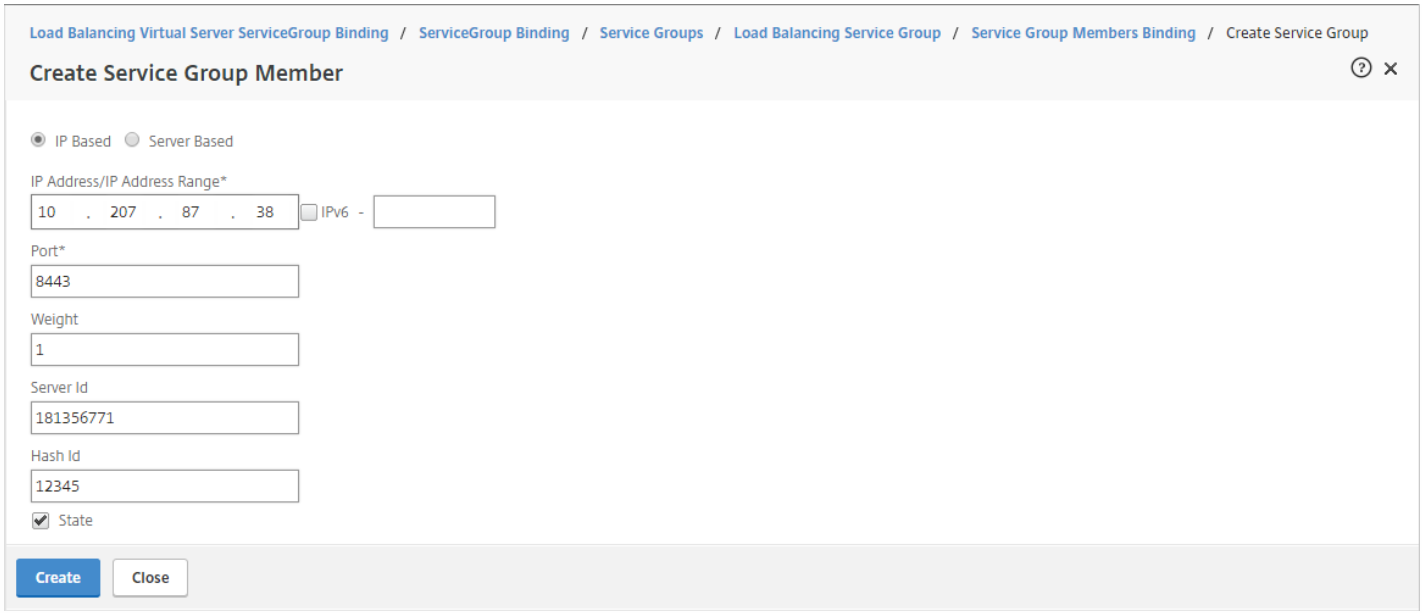


8. Klicken Sie auf **No Service Group Member**.

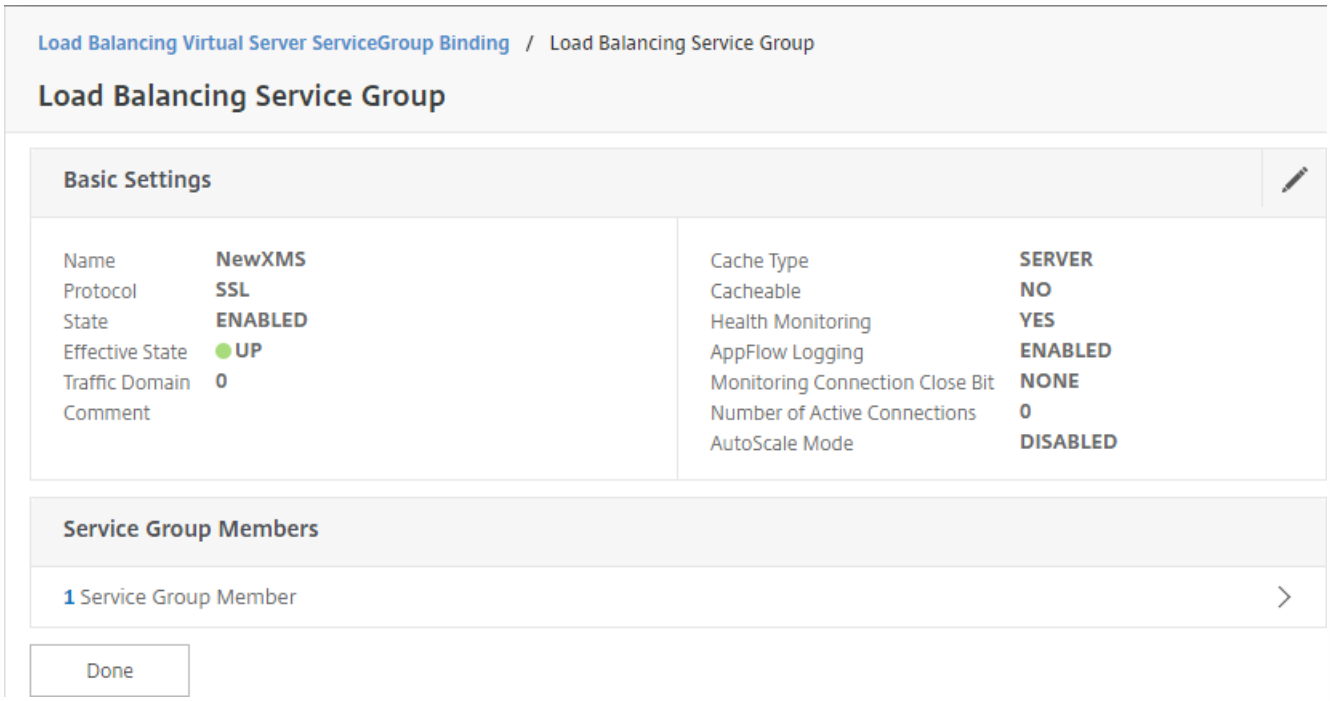


9. Konfigurieren Sie auf der Seite **Create Service Group Member** die folgenden Einstellungen:

- **IP Address/IP-Address Range**: Geben Sie die IP-Adresse des XenMobile 10.4-Servers ein.
- **Port**: Legen Sie **8443** fest.
- **Server ID**: Wenn Sie eine Migration aus einer geclusterten XenMobile 9.0-Umgebung in eine geclusterte XenMobile 10.4-Umgebung durchführen, geben Sie die Serverknoten-ID des aktuellen XenMobile-Servers ein. Zum Nachsehen der Serverknoten-ID melden Sie sich bei der Befehlszeilenschnittstelle (CLI) des XenMobile 10.4-Servers an und geben Sie **1** ein, um das Menü **Clustering** aufzurufen. Die Serverknoten-ID wird als **Current Node ID** aufgeführt.

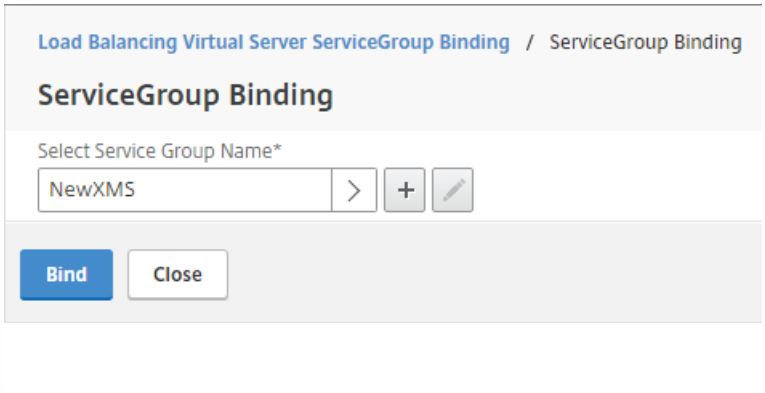


10. Klicken Sie auf **Create** und dann auf **Done**.

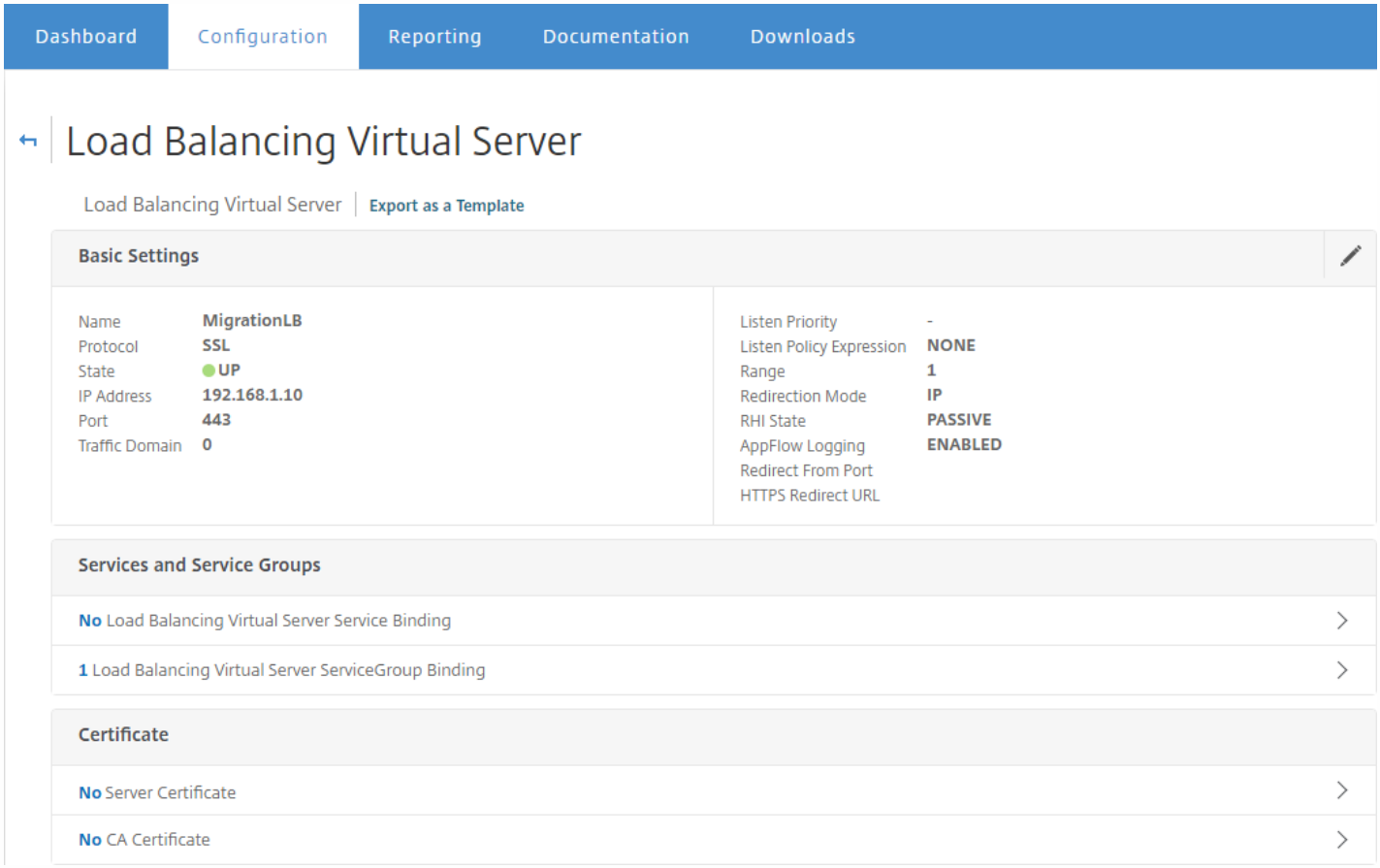


11. Klicken Sie auf **Done** und anschließend auf **OK**.

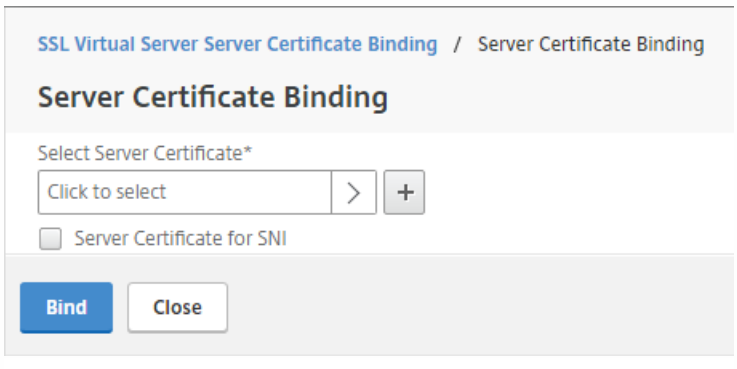
12. Klicken Sie auf **Bind** und im nächsten Bildschirm auf **Done**.



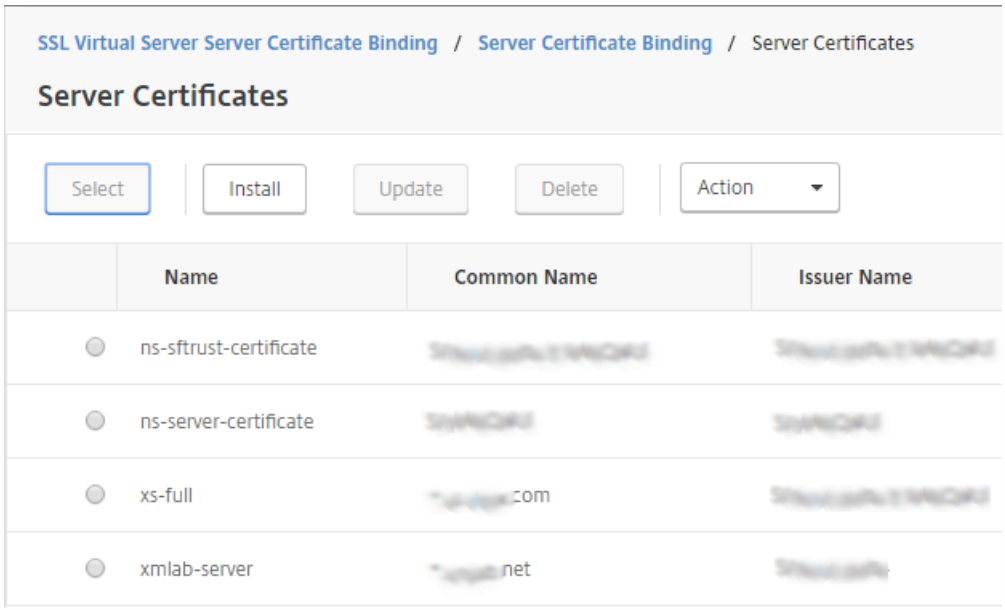
13. Klicken Sie unter **Certificates** auf **No Server Certificate**.



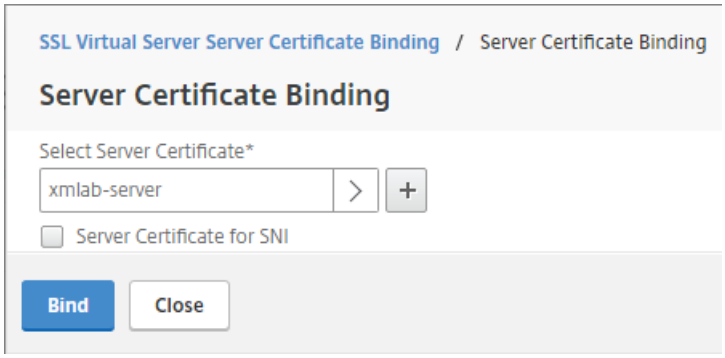
14. Klicken Sie unter **Server Certificate Binding** auf **Click to Select**.

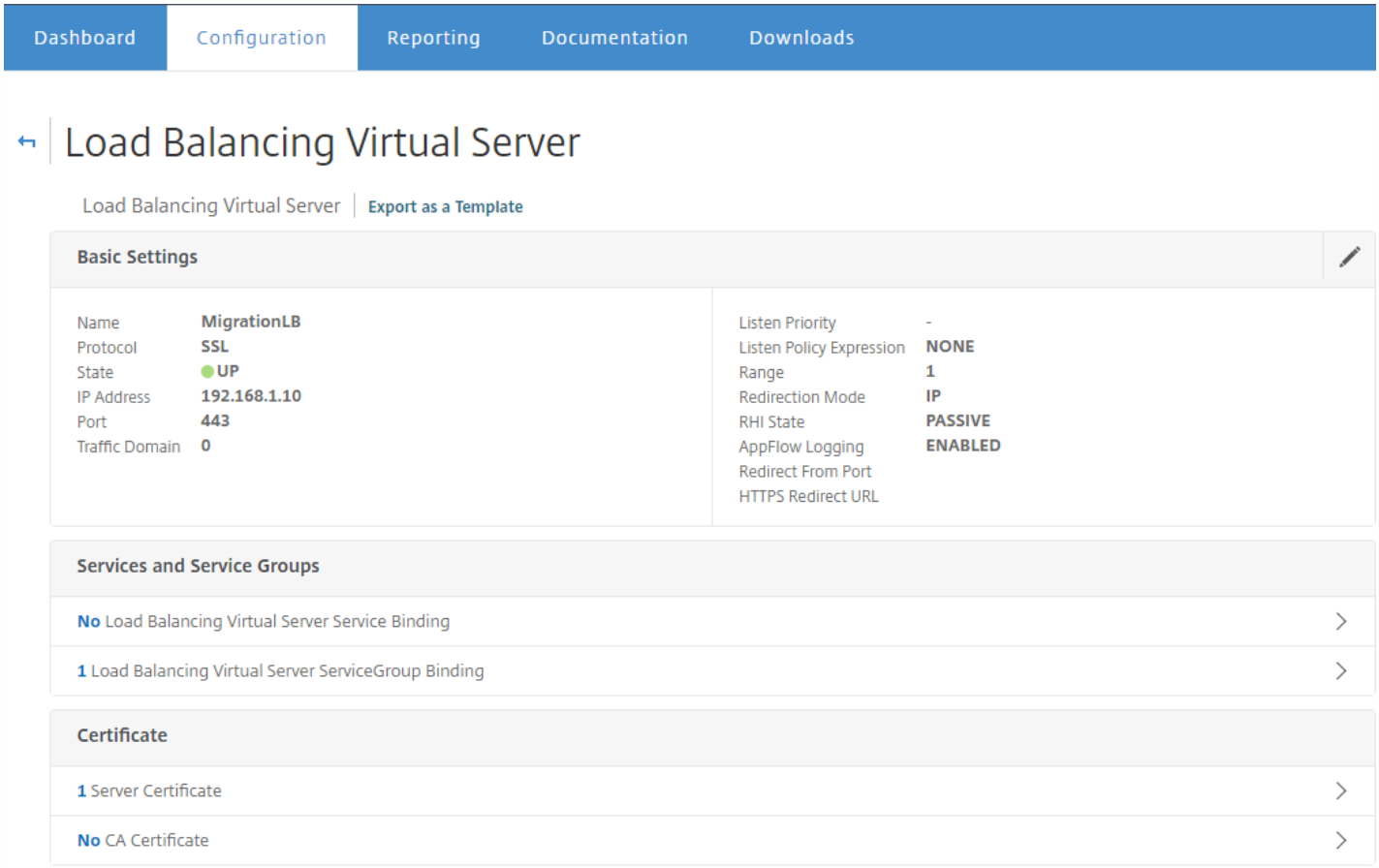


15. Klicken Sie unter **Certificates** auf das XenMobile 9.0-Serverzertifikat, das Sie wie unter Voraussetzungen für das Upgrade Tool beschrieben exportiert haben, und klicken Sie dann auf **OK**.

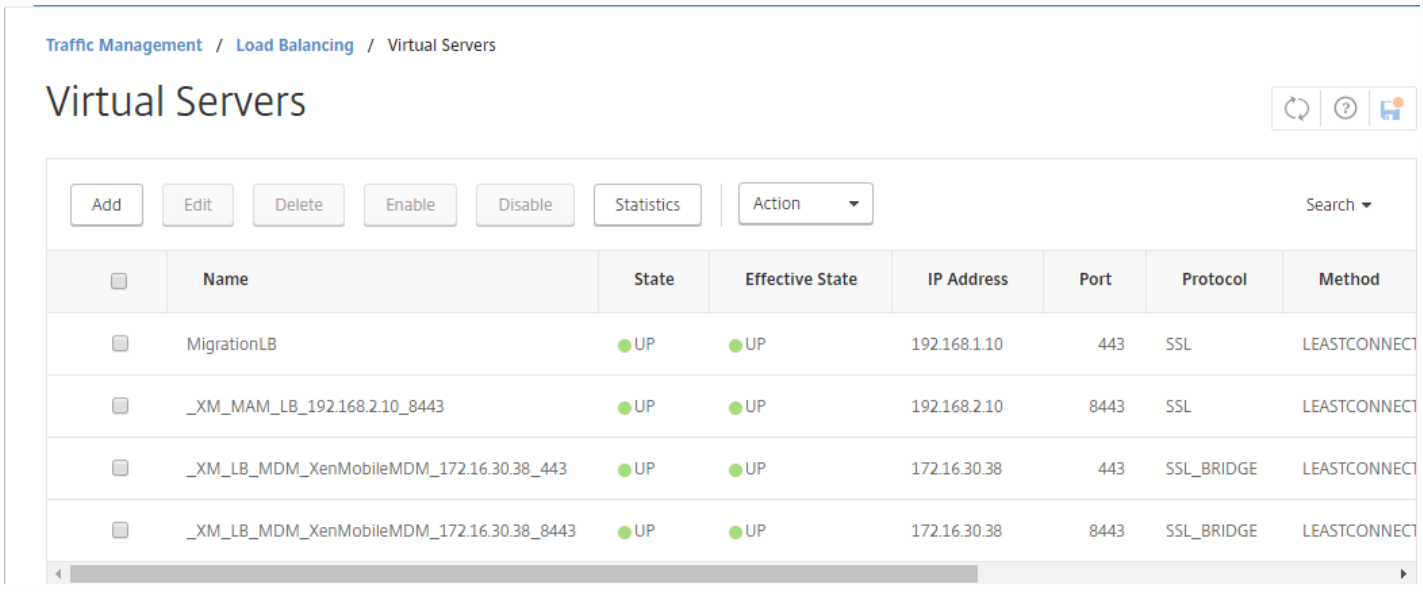


16. Klicken Sie auf **Bind** und im nächsten Bildschirm auf **Done**.





17. Klicken Sie auf die Schaltfläche "Refresh", um sich zu vergewissern, dass der Server ausgeführt wird.

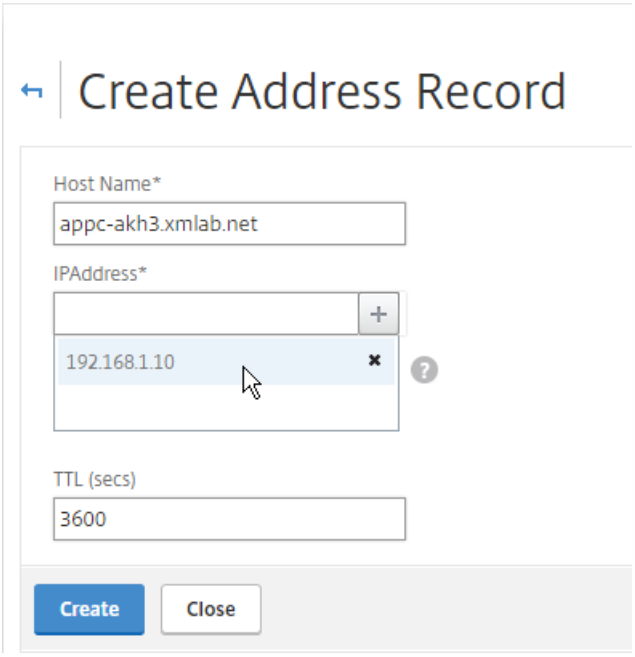


Konfigurieren eines Adresseintrags zum Verweisen des FQDN des App Controller-Servers auf den neuen Lastenausgleichsserver für das Upgrade

1. Melden Sie sich bei NetScaler an, klicken Sie auf **Traffic Management > DNS > Records > Address Records** und anschließend auf **Add**.

Hinweis

Wenn Sie eine Global Server Load Balancing-Konfiguration haben, führt das Hinzufügen eines Adresseintrags dazu, dass das Global Server Load Balancing-System für den Server autoritativ mit der lokalen IP-Adresse antwortet.



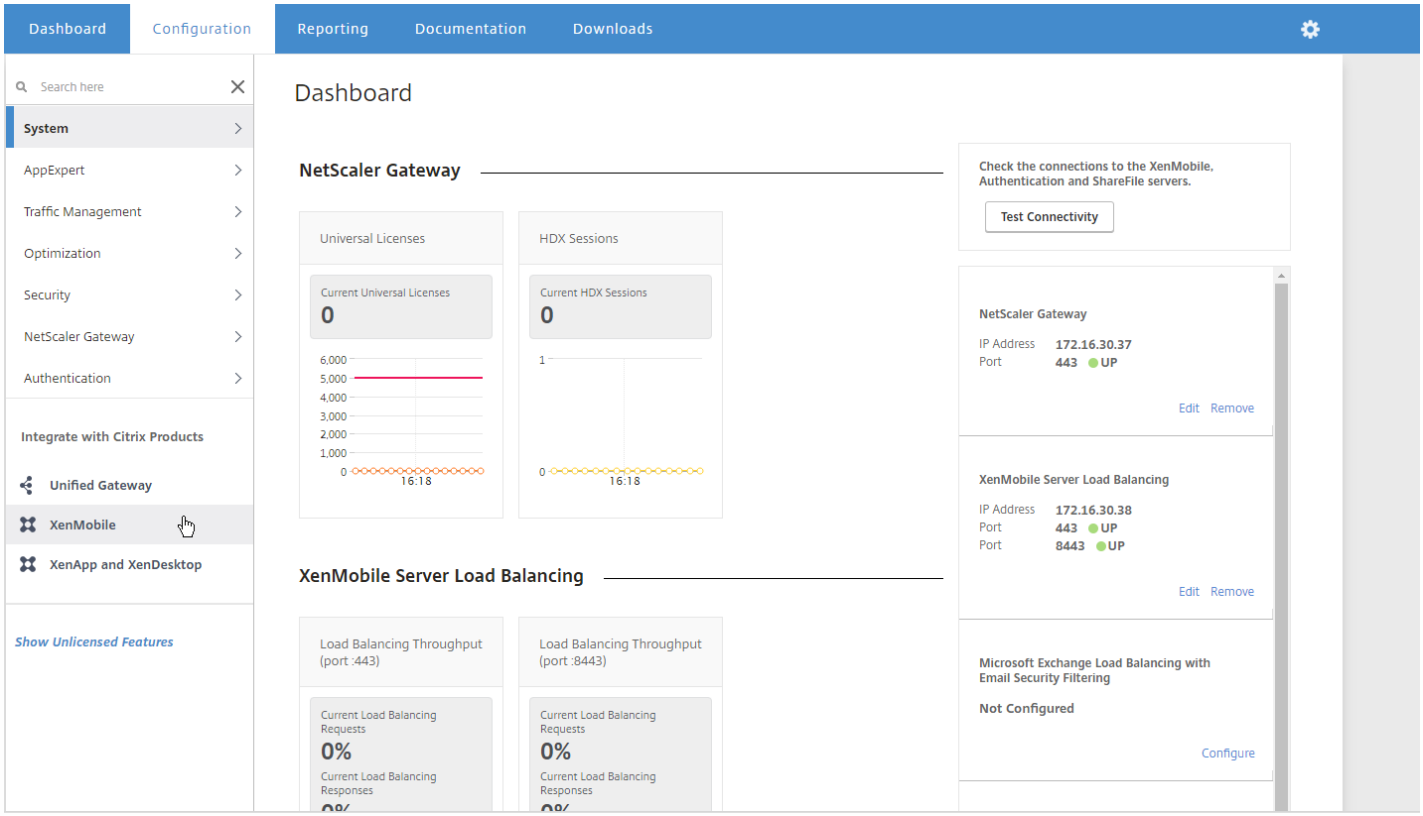
Ändern des virtuellen Lastausgleichsservers für Device Manager, sodass er auf die neue IP-Adresse des XenMobile-Servers verweist

Wenn Sie den Server mit XenMobile 9.0 hinter einem NetScaler-Gerät für den Lastausgleich bereitgestellt haben, müssen Sie die Lastausgleichinstanz von XenMobile 9.0 Device Manager in NetScaler mit der neuen IP-Adresse des XenMobile 10.4-Servers konfigurieren.

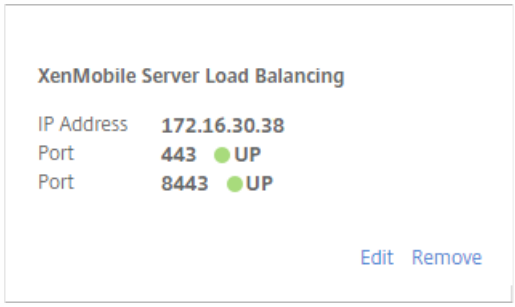
Das Verfahren unterscheidet sich, je nachdem, ob Sie NetScaler 11.1, 11.0 oder 10.5 verwenden.

NetScaler 11.1

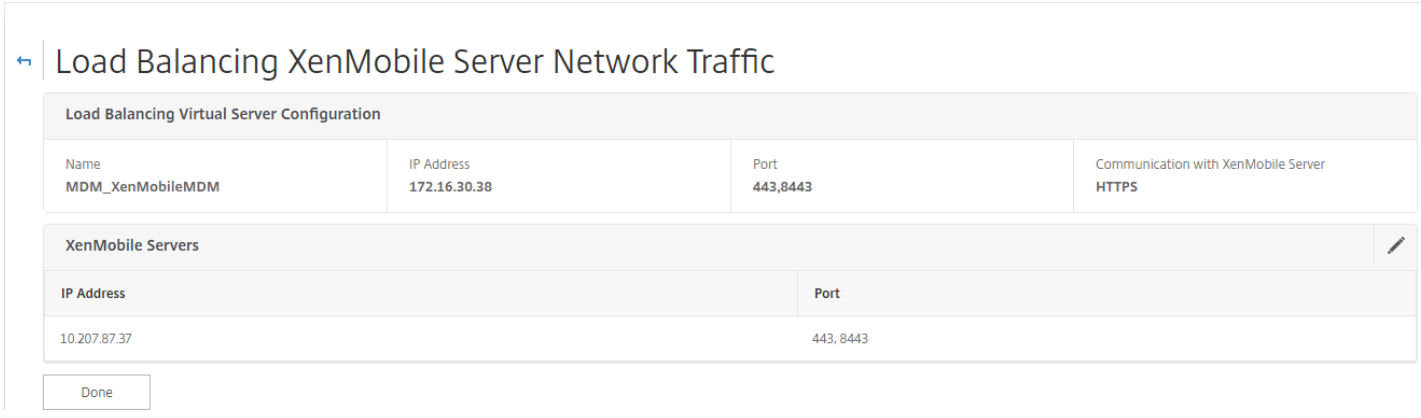
1. Klicken Sie unter **Integrate with Citrix Products** auf **XenMobile**.



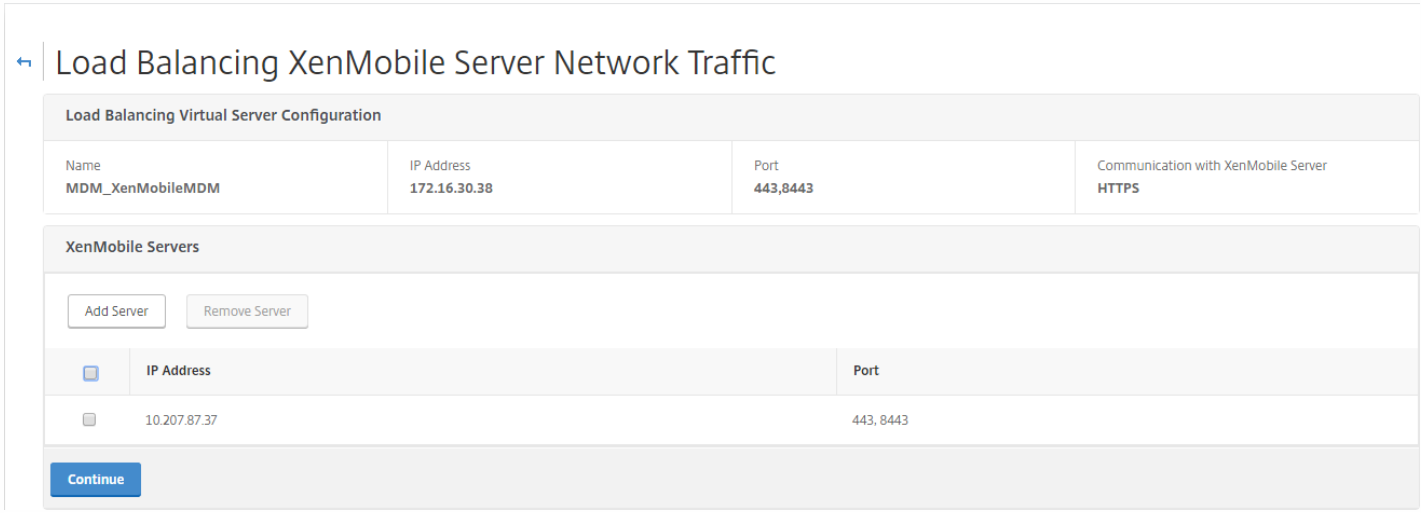
2. Klicken Sie rechts unter **XenMobile Server Load Balancing** auf **Edit**.



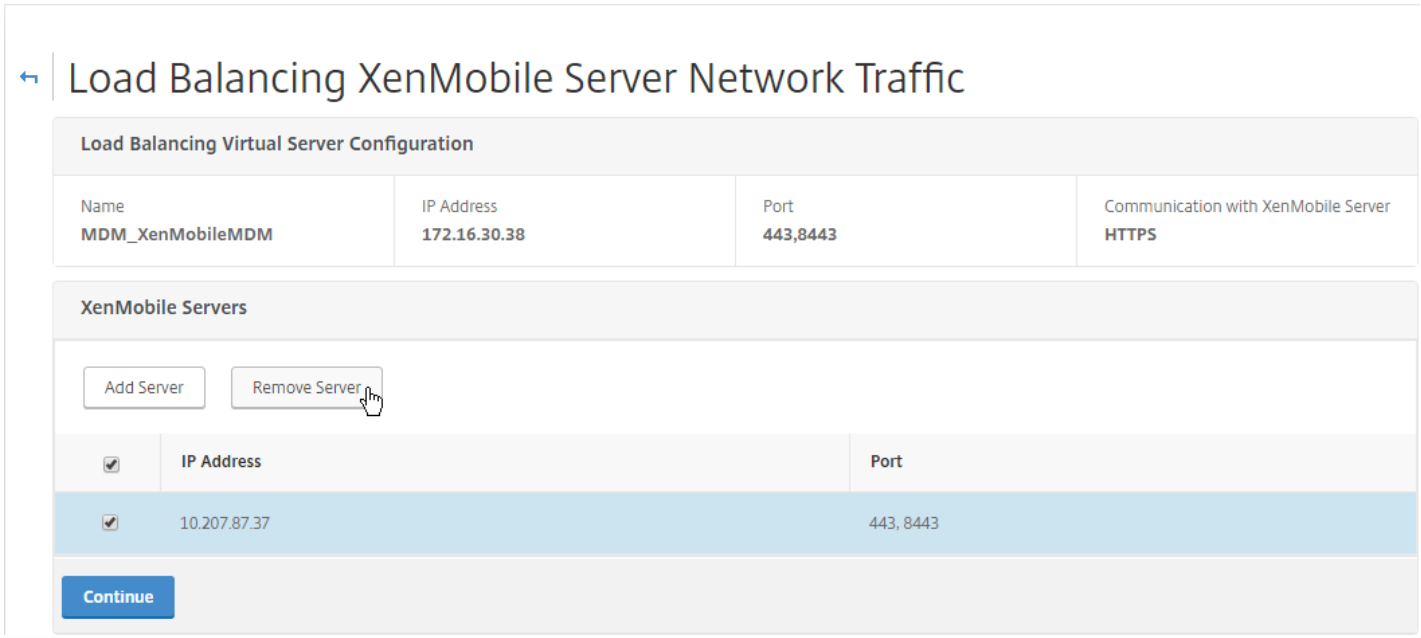
Die Seite **Load Balancing XenMobile Server Network Traffic** wird angezeigt.



3. Klicken Sie auf das Stiftsymbol für "XenMobile Servers", um die zugehörigen Einstellungen zu öffnen.



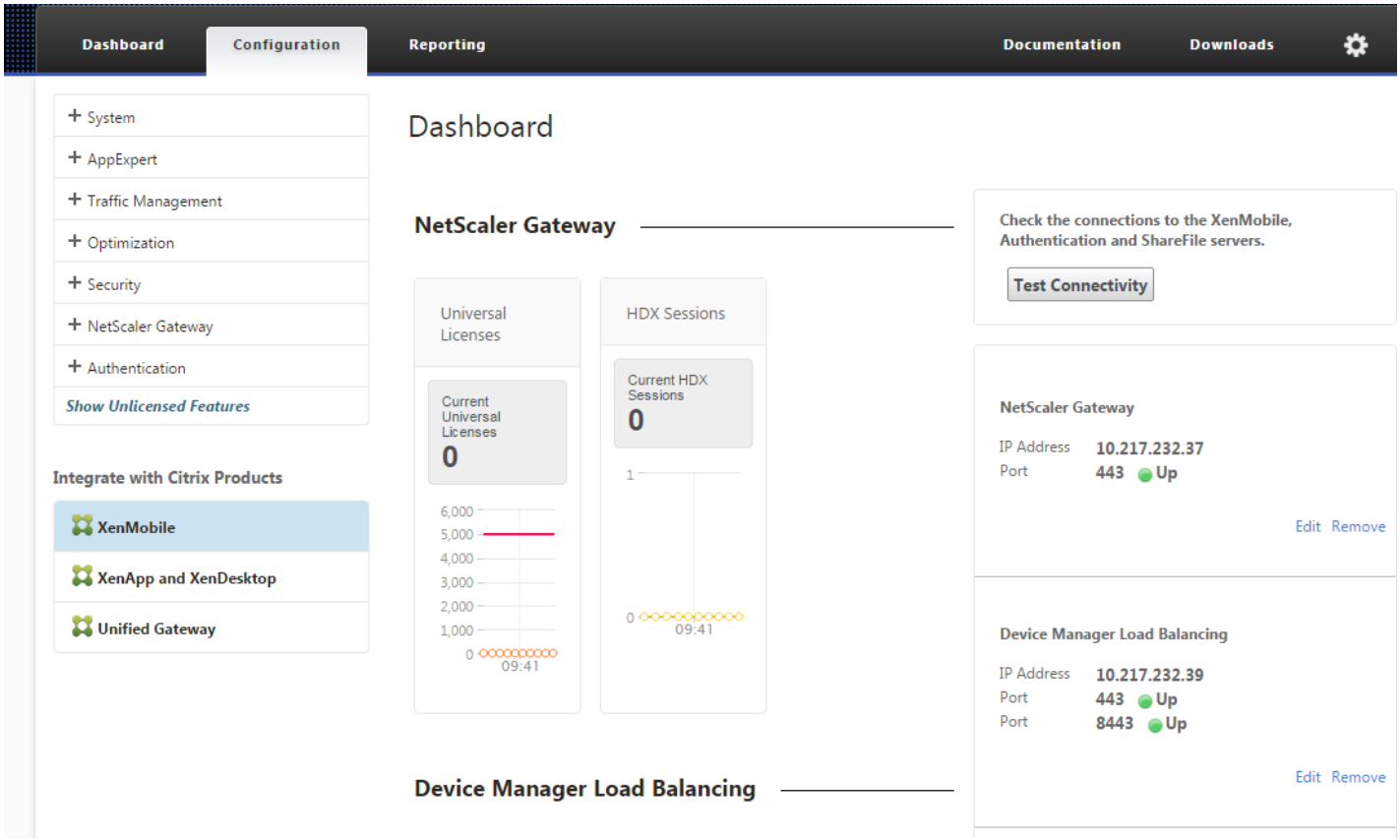
4. Wählen Sie die IP-Adresse des 9.0 Device Manager-Servers aus und klicken Sie auf **Remove Server**.



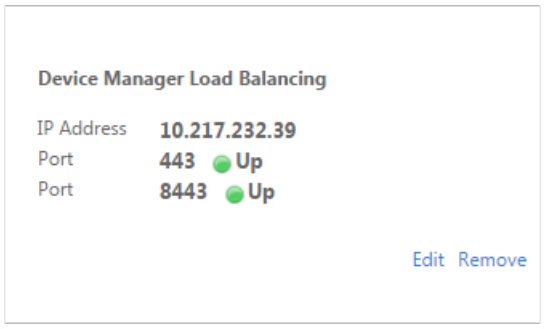
5. Klicken Sie auf **Add Server** und fügen Sie die IP-Adresse des neuen XenMobile 10.4-Servers hinzu.

NetScaler Version 11.0 oder 10.5

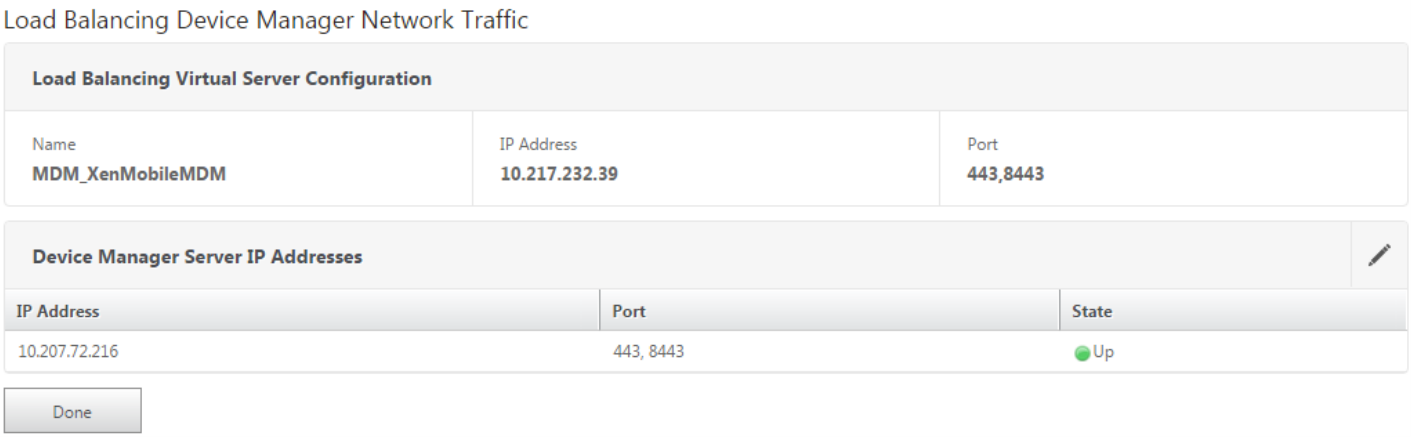
1. Klicken Sie unter **Integrate with Citrix Products** auf **XenMobile**.



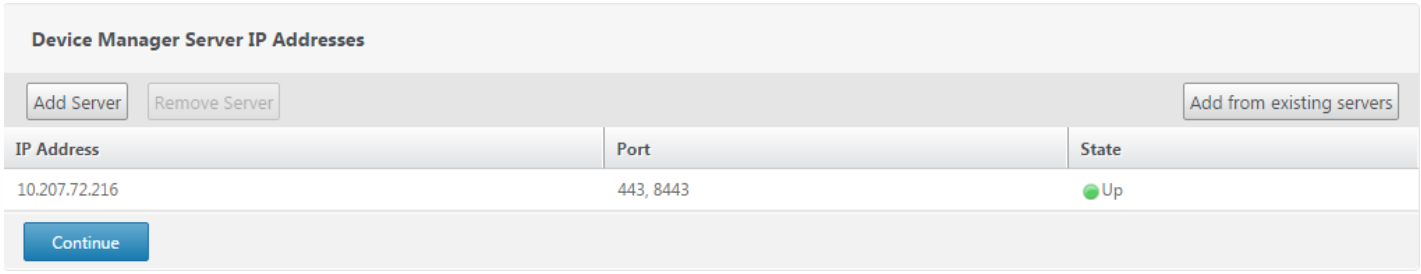
2. Klicken Sie rechts unter **Device Manager Load Balancing** auf **Edit**.



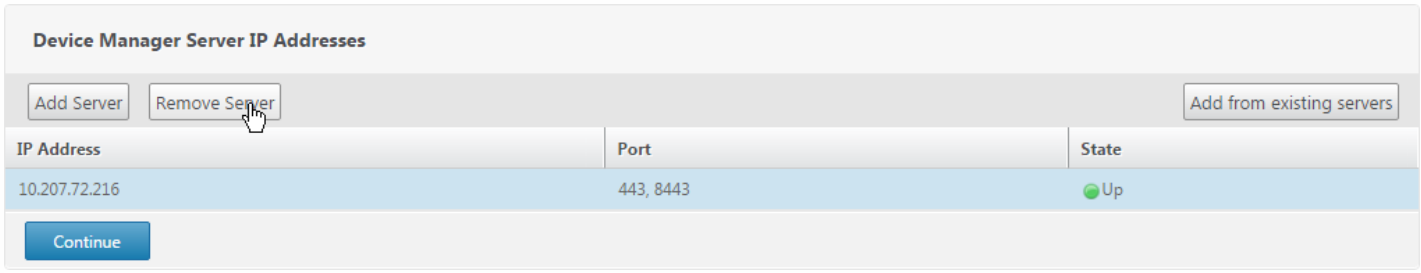
Die Seite **Load Balancing Device Manager Network Traffic** wird angezeigt.



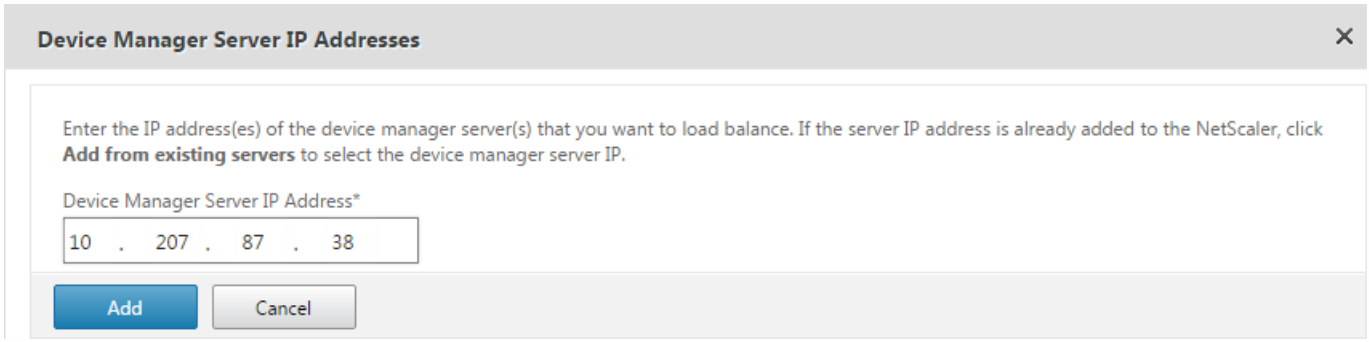
3. Klicken Sie auf das Stiftsymbol für **Device Manager Server IP Addresses**, um die zugehörigen Einstellungen zu öffnen.



4. Wählen Sie die IP-Adresse des 9.0 Device Manager-Servers aus und klicken Sie auf **Remove Server**.



5. Klicken Sie auf **Add Server** und fügen Sie die IP-Adresse des neuen XenMobile 10.4-Servers hinzu.



Ändern von NetScaler Gateway, sodass es auf den neuen FQDN des XenMobile-Servers verweist

NetScaler Gateway verweist in dieser Phase auf den App Controller-FQDN. Sie müssen NetScaler so ändern, dass es auf den neuen XenMobile 10.4-FQDN verweist XenMobile 10.4 überwacht Port 8443 anstelle von Port 443. Wenn Sie NetScaler mit dem NetScaler für XenMobile 9-Assistenten eingerichtet haben, müssen Sie die Portnummer im FQDN verwenden (s. Beispiele in den Tabellen unten).

XenMobile Enterprise Edition

Ändern Sie den FQDN von App Controller so, dass er auf den neuen XenMobile 10.4-FQDN verweist, d. h. den XenMobile 9.0 Device Manager-FQDN gefolgt von Port 8443. Die folgende Tabelle zeigt ein Beispiel.

XenMobile 9,0 Komponente	FQDN der Komponente	XenMobile 10.4 Enterprise Edition-FQDN
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	nicht zutreffend
NetScaler Gateway	access.example.com	nicht zutreffend

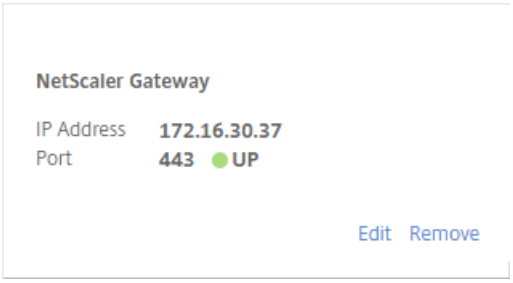
XenMobile App Edition

Ändern Sie den FQDN von App Controller so, dass er auf den neuen XenMobile 10.4-FQDN verweist, d. h. den XenMobile 9.0 App Controller-FQDN gefolgt von Port 8443. Die folgende Tabelle zeigt ein Beispiel.

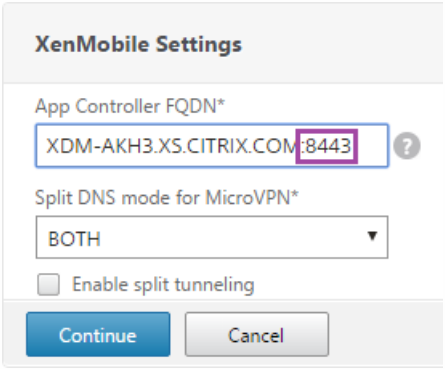
XenMobile 9,0 Komponente	FQDN der Komponente	XenMobile 10.4 Enterprise Edition-FQDN
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	nicht zutreffend

1. Klicken Sie unter **Integrate with Citrix Products** auf **XenMobile**.

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



3. Klicken Sie auf das Stiftsymbol neben **XenMobile Settings**, ändern Sie den App Controller-FQDN in den XenMobile-Server-FQDN und hängen Sie an den FQDN **:8443** an. Beispiel: ***SAMPLE-XENMOBILE.FQDN*.COM:8443**.



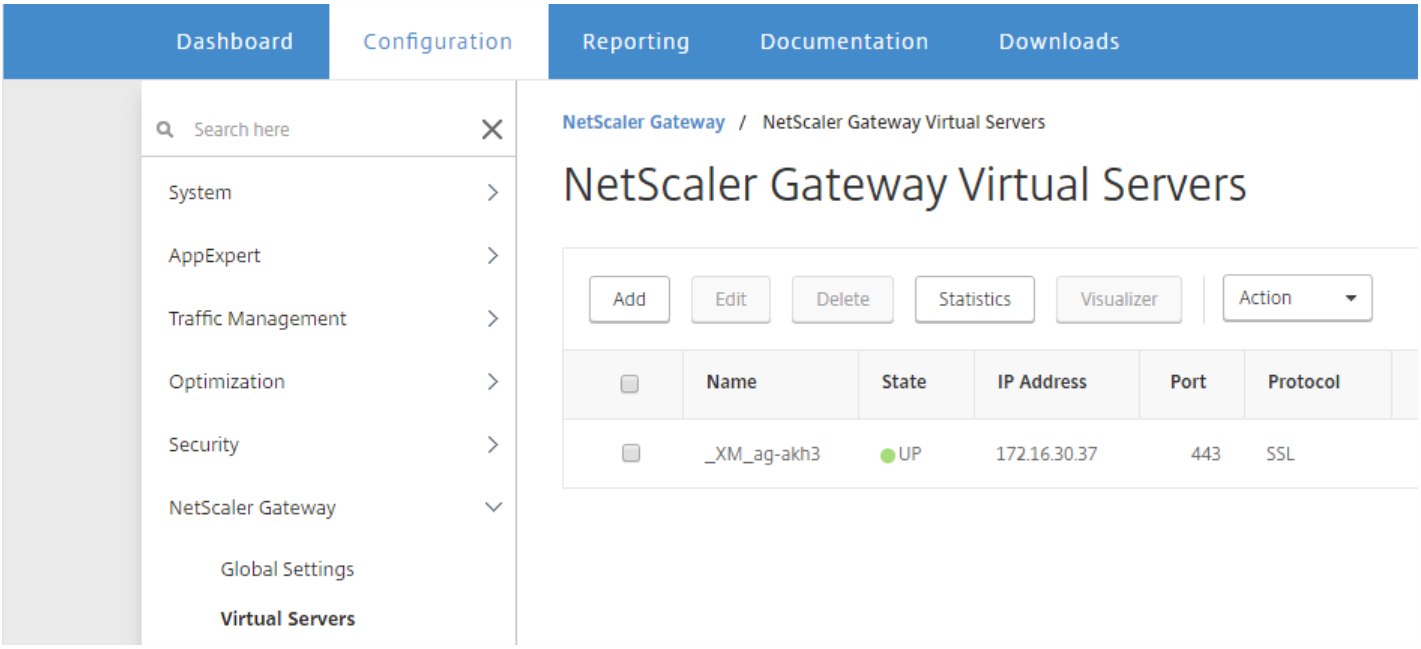
4. Klicken Sie auf **Continue** und dann auf **Finish**.

Hinzufügen der IP-Adresse oder des FQDN des Servers mit der Secure Ticket Authority

Als Nächstes müssen Sie das DNS aktualisieren, damit der FQDN des Servers, auf dem die STA ausgeführt wird, in die IP-Adresse des XenMobile 10.4-Servers aufgelöst wird. In Einzelfällen ist der STA-Server nach der Nachbereitung nicht in NetScaler gebunden, obwohl er in der Liste **VPN Virtual Server STA Server Binding** steht.

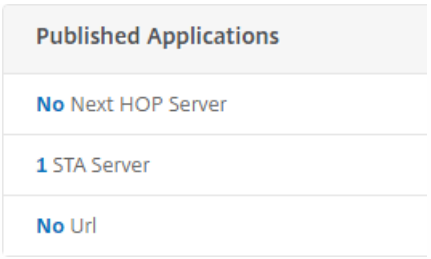
Fügen Sie in NetScaler Gateway die IP-Adresse oder den FQDN des STA-Servers wie folgt hinzu:

1. Klicken Sie auf **Netscaler Gateway > Virtual Servers**.

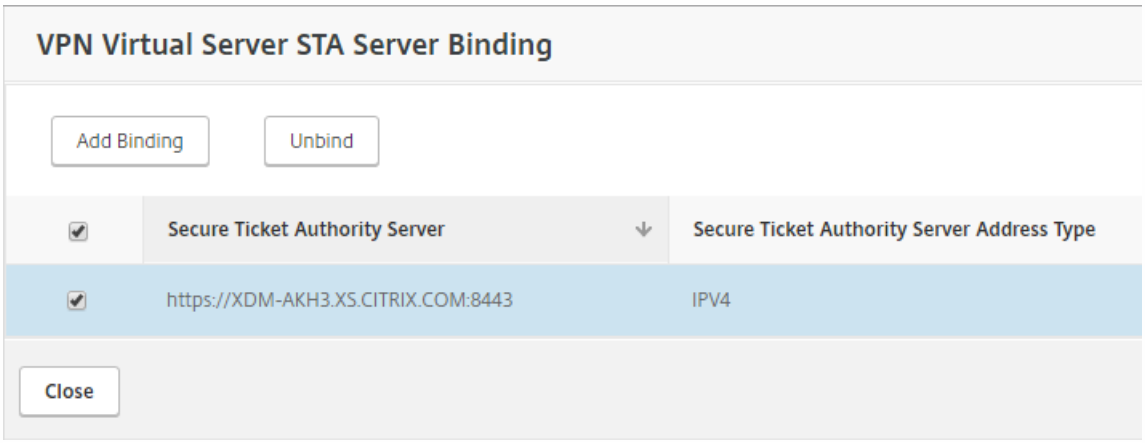


2. Vergewissern Sie sich, dass für den virtuellen NetScaler Gateway-Server der Zustand **Up** angezeigt wird. Wählen Sie den konfigurierten virtuellen NetScaler Gateway-Server aus und klicken Sie auf **Edit**.

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



4. Notieren Sie die für **Secure Ticket Authority Server** angegebene URL für Schritt 6. Wählen Sie den Secure Ticket Authority-Server in der Liste aus.



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

6. Geben Sie im Feld **Secure Ticket Authority Server** die in Schritt 4 notierte URL ein.

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

NTP-Einstellungen

Synchronisieren Sie die Zeit auf NetScaler und dem XenMobile-Server. Verweisen Sie NetScaler und den XenMobile-Server auf denselben öffentlichen NTP-Server (Network Time Protocol).

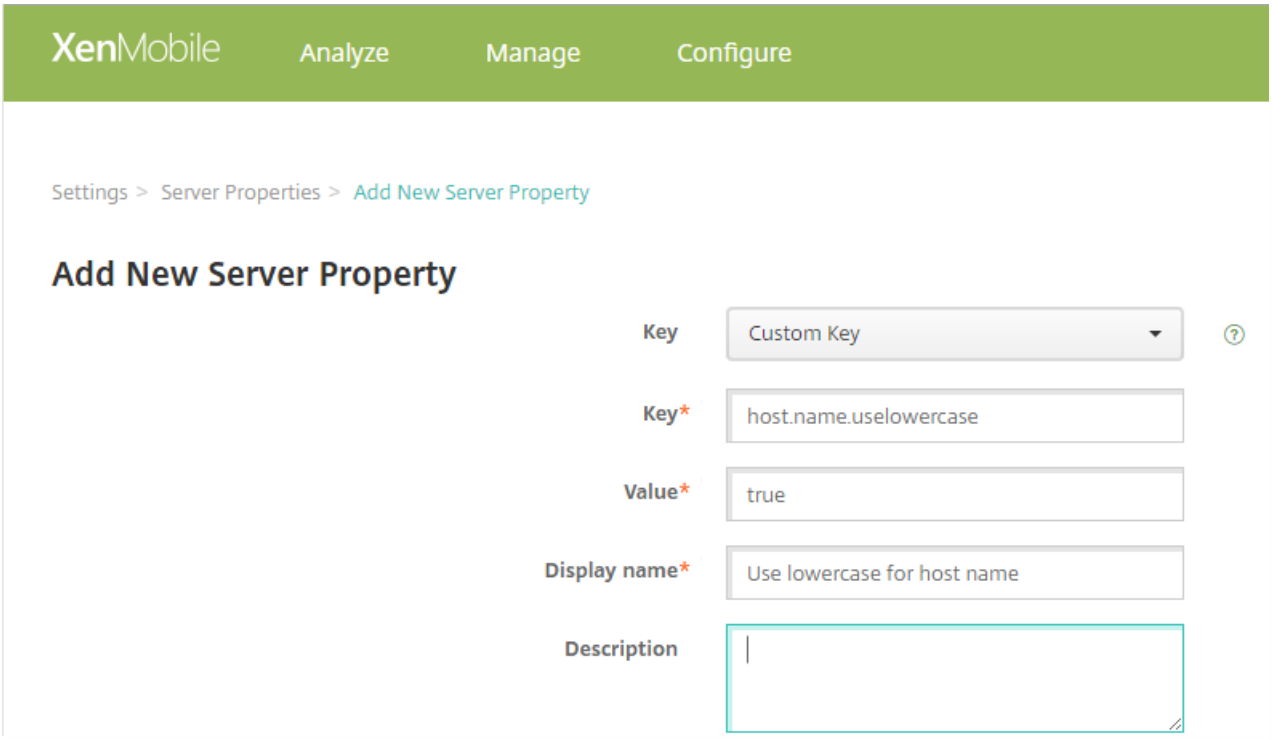
Servereigenschaft für XenMobile 9.0-Hosts mit Großbuchstaben im Namen

Wenn der Name Ihres XenMobile 9.0-Hosts Großbuchstaben enthält, führen Sie die folgenden Schritte durch, damit mobile Geräte auf den Citrix Store zugreifen können:

1. Gehen Sie in der XenMobile 10.4-Konsole zu **Einstellungen > Servereigenschaften**.

2. Klicken Sie auf **Hinzufügen** und füllen Sie die Felder wie folgt aus:

- **Schlüssel**: Wählen Sie **Benutzerdefinierter Schlüssel**.
- **Schlüssel**: Geben Sie **host.name.uselowercase** ein.
- **Wert**: Geben Sie **true** ein.
- **Anzeigename**: Geben Sie eine Beschreibung für den Schlüssel ein.



3. Starten Sie den XenMobile-Server neu.

Aktualisieren nicht im Upgrade eingeschlossener Informationen

Aktualisieren Sie die folgenden Elemente nach Bedarf:

- Managed Service Provider (MSP)-Gruppe
- Benutzerdefinierte Active Directory-Attribute
- RBAC-Rollen
  Bei einem Upgrade einer lokalen Umgebung treten bei den RBAC-Einstellungen Probleme auf. Weitere Informationen finden Sie unter Bekannte Probleme.
- Protokolleinstellungen
- Jegliche in der Datei migration.log aufgeführten Konfigurations- oder Benutzerdaten
- Syslog-Serverkonfiguration

Benutzerdefinierter Storename

Zur Vorbereitung des Upgrades gehört das Ändern eines benutzerdefinierten Citrix Store-Namens auf den Standardwert. Wenn Sie diesen Vorbereitungsschritt nicht durchgeführt haben, müssen Sie einen der folgenden Nachbereitungsschritte ausführen, bevor Sie den XenMobile-Server 10.4 verwenden:

- Wenn Sie viele Windows-Geräte betreuen, ändern Sie den Namen des Stores auf die Standardeinstellung. Anschließend müssen sich Benutzer mit iOS- und Android-Geräten von Citrix Secure Hub (zuvor Worx Home) ab- und wieder anmelden.
- Wenn Sie weniger Windows-Geräte als iOS- und Android-Geräte betreuen, wird empfohlen, dass die Benutzer der Windows-Geräte ihre Geräte neu registrieren.

Weitere Informationen finden hierzu Sie unter http://support.citrix.com/article/CTX214553.

XenMobile-Geräteregistrierung nach dem Upgrade

Benutzer müssen ihre Geräte nach dem Produktionsupgrade auf XenMobile 10.4 nicht erneut registrieren. Die Geräte sollten basierend auf dem Taktintervall automatisch eine Verbindung mit dem XenMobile 10,4-Server herstellen. Benutzer werden möglicherweise jedoch aufgefordert, sich neu zu authentifizieren, damit das Gerät die Verbindung wiederherstellen kann.

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

Aktualisieren des MTC-Mandantenservers auf XenMobile 10.4

Feb 24, 2017

Wenn unter XenMobile 9.0 MDM oder Enterprise Edition die Multi-Tenant Console (MTC) aktiviert ist, können Sie mit der MTC verwaltete XenMobile 9-Instanzen zu eigenständigen XenMobile 10.4-Instanzen migrieren. XenMobile 10 unterstützt die Multi-Tenant Console nicht, daher müssen Sie die aktualisierten Instanzen individuell verwalten.

1. Vor allen MTC-Clients muss Netzwerkadressübersetzung (NAT) konfiguriert sein.

2. Installieren Sie eine XenMobile 10,4-Instanz.

3. Wenn auf dem MTC-Mandanten keine Portzuordnung aktiviert ist, führen Sie die folgenden Schritte aus:

    a. Stellen Sie sicher, dass die XenMobile 10,4-Serverports, die HTTPS-Kommunikation mit Zertifikaten (normalerweise Port 443) und HTTPS-Kommunikation ohne Zertifikate (8443) zulassen, mit den Ports für die XenMobile-Instanz übereinstimmen.

    b. Konfigurieren Sie einen neuen Port für die Verwaltung.

    c. Wenn Portzuordnung aktiviert ist, verwenden Sie den Port, der dem XenMobile-Server zugeordnet ist, und nicht den Port, auf dem der XenMobile-Server abhört.

4. Verwenden Sie beim XenMobile-Serverstart den Instanznamen **zdm**.

5. Wenn Sie das Upgrade Tool über die XenMobile-Befehlszeilenschnittstelle aktivieren, müssen Sie auf die Upgradeaufforderung mit **Yes** antworten.

6. Kopieren Sie auf dem für das Upgrade vorgesehenen Server die folgenden Dateien aus dem Ordner C:\Programme (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\webapps\tenant-name\WEB-INF\classes

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

7. Kopieren Sie die folgenden Dateien aus C:\Programme (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name:

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

8. Kopieren Sie die Datei C:\Programme (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xml und bearbeiten Sie sie wie nachfolgend beschrieben.

9. Entfernen Sie mit Ausnahme von Port 80 alle Portconnectors, die vom anderen Mandanten verwendet werden, aus server.xml.

10. Entfernen Sie auf dem verwendeten Portconnector den Instanznamen aus allen Dateipfaden im folgenden Bereich:

keystoreFile="C:\Programme (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\https.p12"

in

keystoreFile="C:\Programme (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\https.p1"

11. Wiederholen Sie Schritt 10 für folgende Dateipfade:

truststoreFile="C:\Programme (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\cacerts.pem.jks"

in

truststoreFile="C:\Programme (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\cacerts.pem.jks"

12. Erstellen Sie eine ZIP-Datei mit den Dateien, die Sie in den Schritten 6 bis 8 kopiert haben.

13. Öffnen Sie die IP-Adresse des XenMobile 10.4-Servers mit https://*IP-Adresse:Port*/uw/?cloudMode, wobei *Port* die HTTPS- Verbindung mit einem Zertifikat ist. Der Upgradeassistent wird geöffnet.

14. Wählen Sie gemäß den Anweisungen im Upgradeassistenten **MDM** oder **Enterprise**.

Für MDM-Upgrades werden Sie zum Hochladen der ZIP-Datei aufgefordert. Sie müssen außerdem die Datenbank auf Richtigkeit überprüfen und das Kennwort für das Zertifizierungsstellenzertifikat eingeben.

Für Enterprise-Upgrades werden Sie zum Hochladen des Supportpakets für App Controller aufgefordert.

15. Melden Sie sich nach dem Neustart des XenMobile-Servers bei der XenMobile-Konsole an. Verwenden Sie dabei die IP-Adresse des XenMobile-Servers gefolgt von der Verwaltungsportnummer.

16. Verweisen Sie die NAT auf einen neuen Server.

17. Führen Sie die erforderlichen Änderungen an der Firewall aus, um die vom XenMobile-Server verwendeten Ports zuzulassen.

Benutzerkonten, Rollen und Registrierung

Apr 24, 2017

In XenMobile konfigurieren Sie Benutzerkonten und Gruppen sowie Rollen für Benutzerkonten und Gruppen. Sie konfigurieren auch den Registrierungsmodus und Einladungen. Sie konfigurieren diese Einstellungen in der XenMobile-Konsole auf der Registerkarte **Verwalten** und der Seite **Einstellungen**.

Auf der Registerkarte **Verwalten** können Sie die folgenden Schritte ausführen:

- Klicken Sie auf **Benutzer**, 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 und Löschen lokaler Benutzerkonten
  - Importieren von Benutzerkonten über eine CSV-Provisioningdatei und Provisioningdateiformate
  - Hinzufügen oder Entfernen von Gruppen in XenMobile

  Sie können mit Workflows auch die Erstellung und Entfernung von Benutzerkonten verwalten (siehe weiter unten unter Erstellen und Verwalten von Workflows).

- Klicken Sie auf **Registrierung**, um bis zu sieben Registrierungsmodi zu konfigurieren. Jeder Modus hat eine eigene Sicherheitsstufe und eigene Verfahren zum Registrieren von Geräten 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

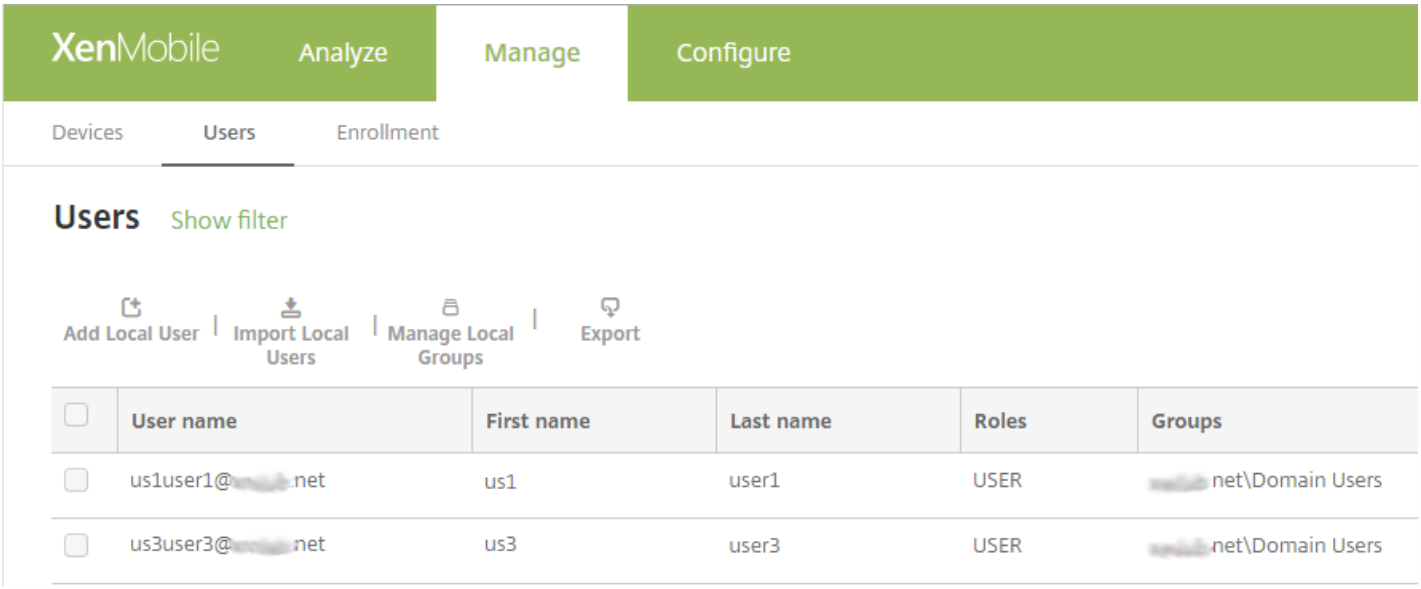
Auf der Seite **Einstellungen** können Sie folgende Einstellungen ändern:

- 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
- 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: Secure Hub, SMTP oder SMS. Einzelheiten finden Sie in den folgenden Abschnitten:
  - Erstellen und Aktualisieren von Benachrichtigungsvorlagen

Erstellen, Bearbeiten und Löschen lokaler Benutzerkonten

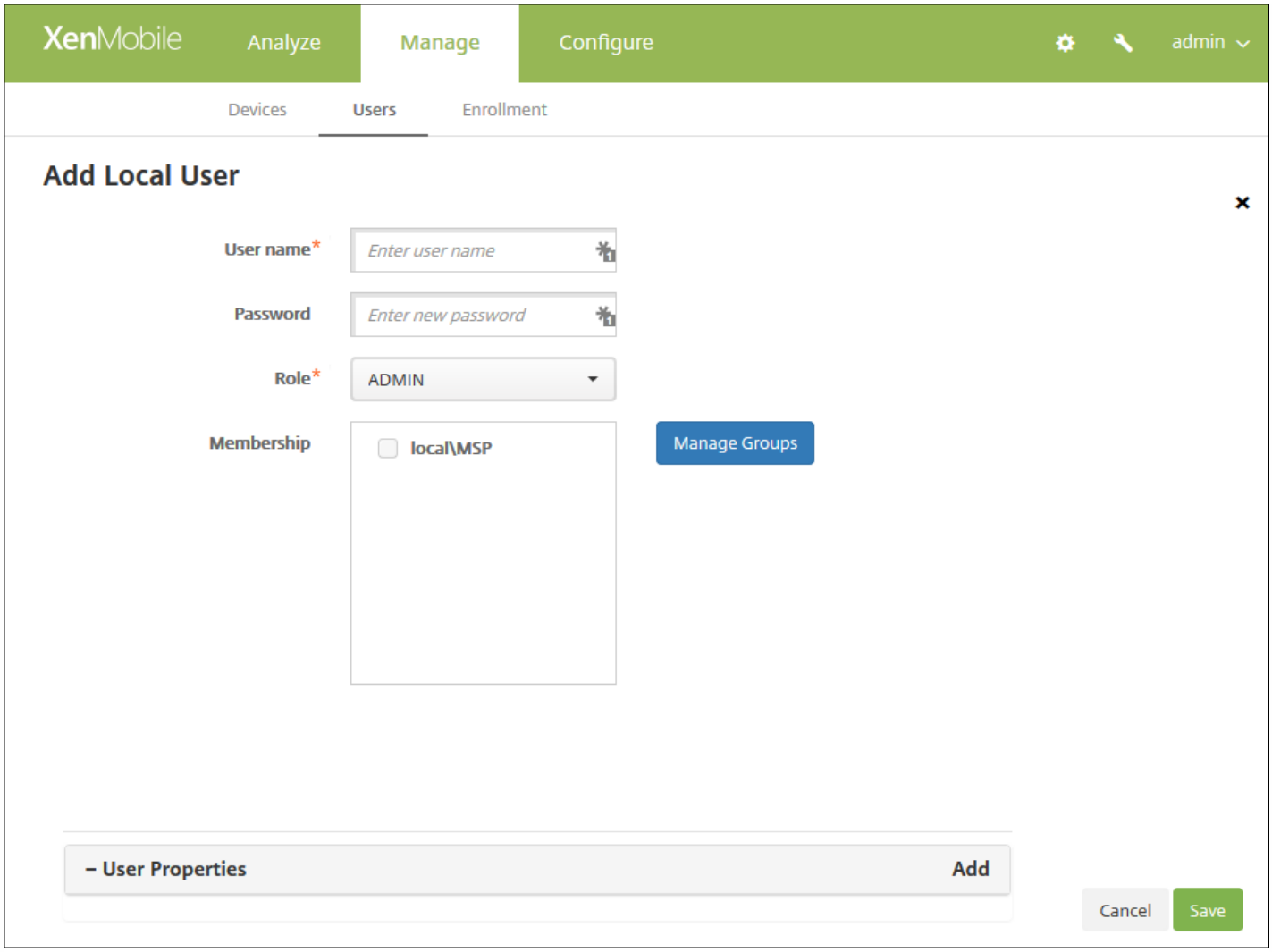
Sie können lokale Benutzerkonten in XenMobile manuell hinzufügen oder mit einer Provisioningdatei importieren. Eine Anleitung zum Importieren von Benutzerkonten aus einer Provisioningdatei finden Sie unter Importieren von Benutzerkonten über eine CSV-Provisioningdatei.

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



Hinzufügen eines lokalen Benutzerkontos

1. Klicken Sie auf der Seite **Benutzer** auf **Lokalen Benutzer hinzufügen**. Die Seite **Lokalen Benutzer hinzufügen** wird angezeigt.



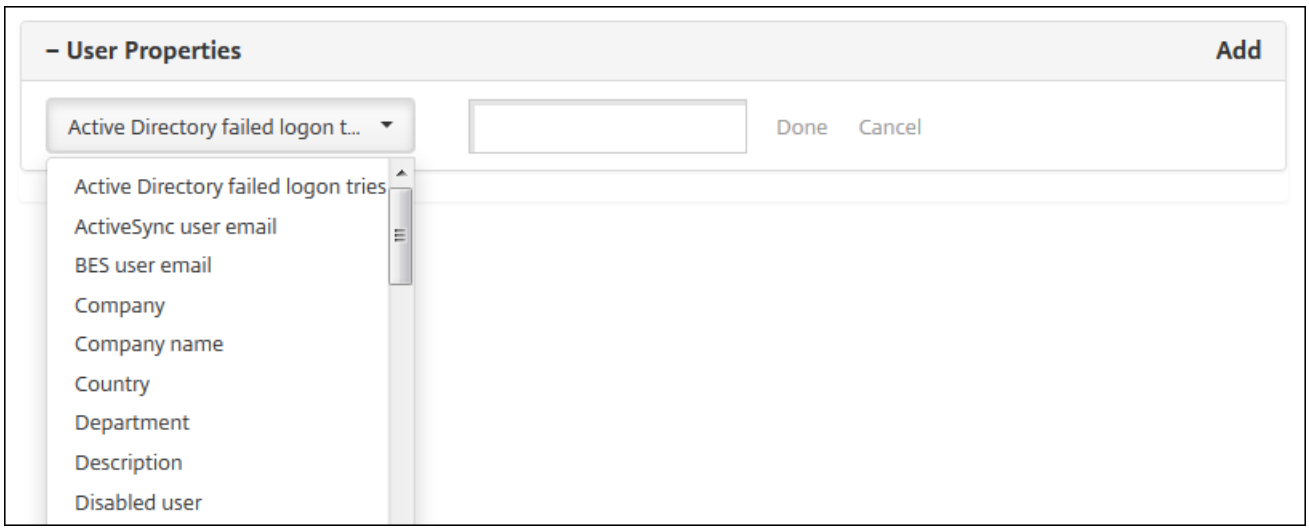
2. Konfigurieren Sie folgende Einstellungen:

- **Benutzername**: Geben Sie den Benutzernamen ein. Diese Angabe ist erforderlich. Namen dürfen Leerzeichen sowie Groß- und Kleinbuchstaben enthalten.
- **Kennwort**: Geben Sie ein optionales Benutzerkennwort ein.
- **Rolle**: Klicken Sie in der Liste auf die Rolle des Benutzers. Weitere Informationen über Rollen finden Sie unter Konfigurieren von Rollen mit RBAC. 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.

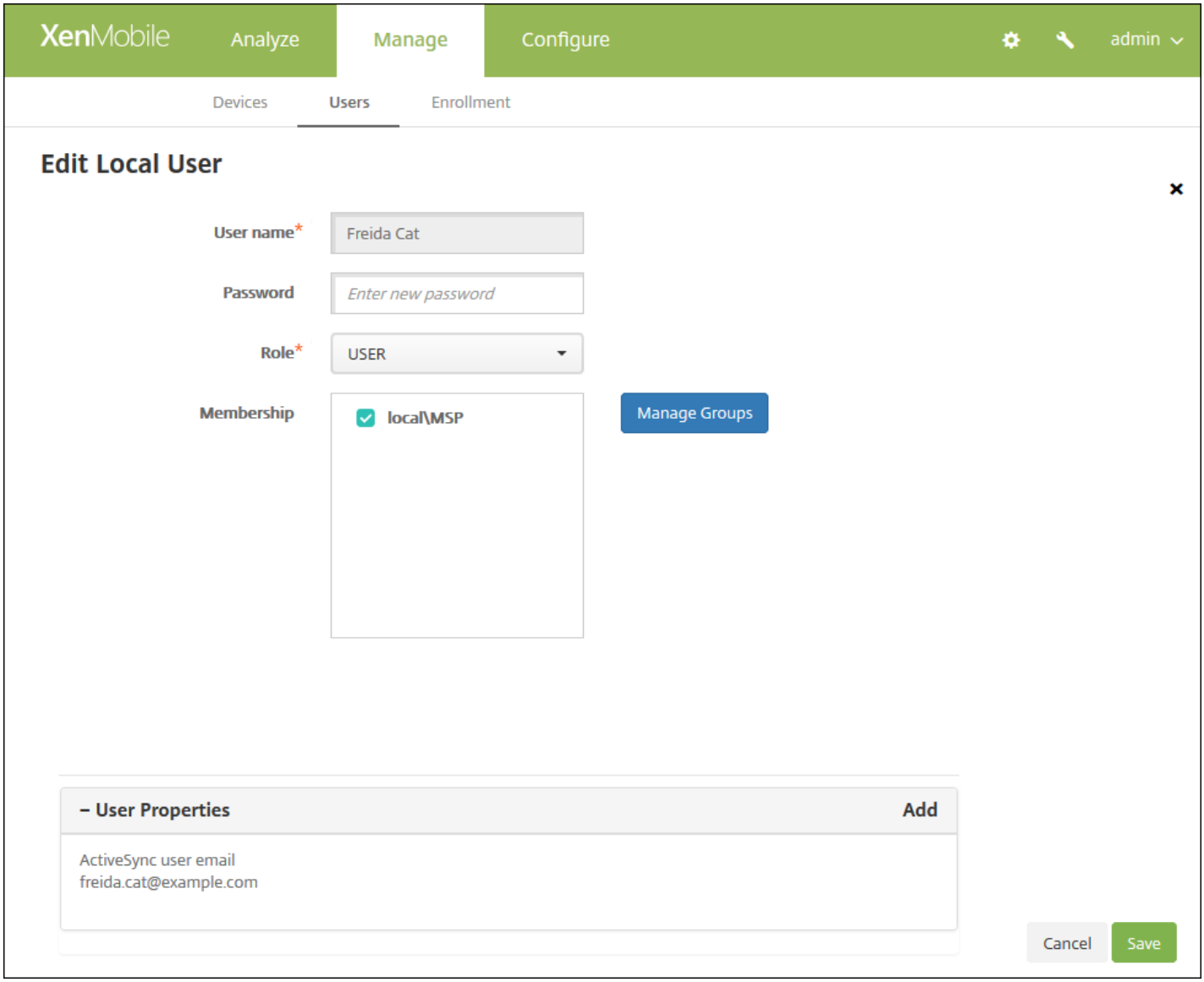
Zum Bearbeiten einer Benutzereigenschaft klicken darauf und nehmen Sie die Änderungen vor. Klicken Sie auf **Fertig**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Eintrag unverändert zu lassen.



3. Klicken Sie auf **Speichern**.

Bearbeiten eines lokalen Benutzerkontos

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.



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 in der Liste auf die Rolle des Benutzers.
- **Mitgliedschaft**: Klicken Sie in der Liste auf die Gruppen, zu denen das Benutzerkonto gehören soll. Zum Entfernen eines Benutzerkontos 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.

Löschen eines lokalen Benutzerkontos

1. Wählen Sie auf der Seite **Benutzer** in der Liste das Benutzerkonto aus.

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

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

3. Klicken Sie auf **Löschen** zum Löschen des Benutzerkontos oder auf **Abbrechen**, um es beizubehalten.

Importieren von Benutzerkonten

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

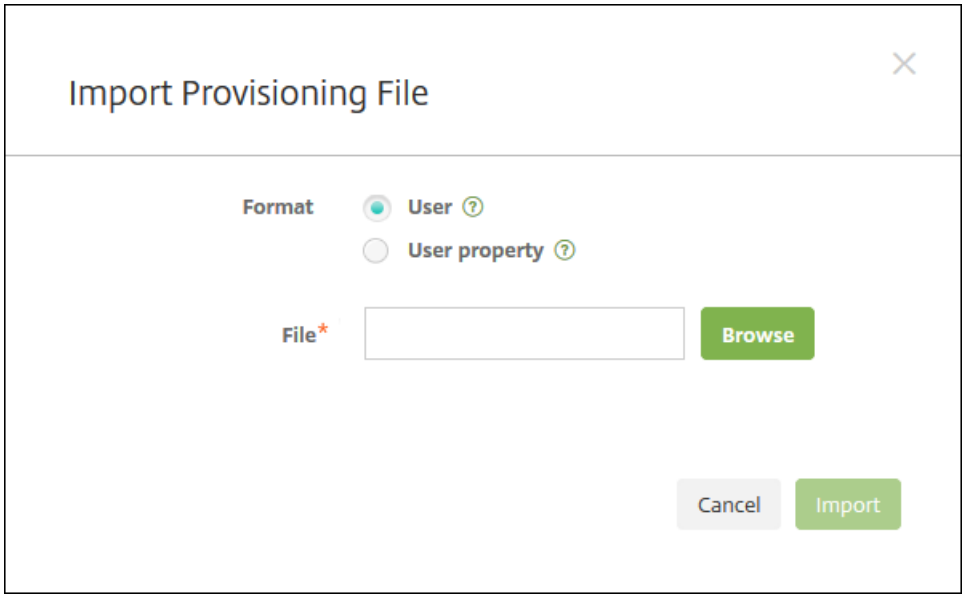
Hinweis:

- Verwenden Sie für lokale Benutzer den Domänennamen zusammen mit dem Benutzernamen in der Importdatei. Beispiel: Geben Sie username@domain an. Wenn der lokale Benutzer, den Sie in diesem Format erstellen oder importieren, für eine verwaltete Domäne in XenMobile vorgesehen ist, beachten Sie folgende Punkte. Der Benutzer kann sich nicht mit den entsprechenden LDAP-Anmeldeinformationen registrieren.
- Beim Importieren von Benutzerkonten in das interne Benutzerverzeichnis von XenMobile deaktivieren Sie die Standarddomäne, um den Importvorgang zu beschleunigen. Beachten Sie, dass die Deaktivierung der Domäne sich auf Registrierungen auswirkt. Daher müssen Sie die Standarddomäne nach dem Import wieder aktivieren.
- Lokale Benutzer können im UPN-Format (Benutzerprinzipalname) angegeben werden. Allerdings wird empfohlen, nicht die verwaltete Domäne zu verwenden. Wird 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. 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

Eine manuell erstellte Provisioningdatei zum Importieren von Benutzerkonten und -eigenschaften in XenMobile muss eines der folgenden Formate haben:

- **Felder der Provisioningdatei für Benutzer**: user;password;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. Die Eigenschaft "propertyV;test;1;2" müsste beispielsweise in der Provisioningdatei in folgender Form eingegeben werden: propertyV\;test\;1\;2.
- Gültige Werte für **Rolle** sind die vordefinierten Rollen USER, ADMIN, SUPPORT und DEVICE_PROVISIONING sowie alle von Ihnen definierten Rollen.
- Der Punkt (.) wird als Trennzeichen zum Erstellen von Gruppenhierarchien verwendet und kann daher nicht in Gruppennamen verwendet werden.
- Eigenschaftsattribute in Attributprovisioningdateien müssen in Kleinbuchstaben geschrieben werden. Bei der Datenbank wird zwischen Groß- und Kleinschreibung unterschieden.

Beispiel für Benutzerprovisioninginhalt

Der Eintrag "user01;pwd\;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

In einem anderen Beispiel bedeutet der Eintrag "AUser0;1.password;USER;ActiveDirectory.test.net" Folgendes:

- **Benutzer**: AUser0
- **Kennwort**: 1.password
- **Rolle**: USER
- **Gruppe**: Active Directory.test.net

Beispiel für Benutzerattribut-Provisioninginhalt

Der Eintrag user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value, bedeutet:

- **Benutzer**: user01
- **Eigenschaft 1**
  - **Name**: propertyN
  - **Wert**: propertyV;test;1;2
- **Eigenschaft 2**:
  - **Name**: prop 2
  - **Wert**: prop2 value

Konfigurieren von Registrierungsmodi und Aktivieren des Selbsthilfeportals

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. Im Selbsthilfeportal generieren Benutzer nach der Anmeldung Registrierungslinks, mit denen sie ihre Geräte registrieren können, oder wählen die Option, eine Registrierungseinladung an das eigene E-Mail-Konto zu senden. Zum Konfigurieren von Registrierungsmodi verwenden Sie in der XenMobile-Konsole die Seite **Einstellungen** > **Registrierung**.

Zum Senden von Registrierungseinladungen verwenden Sie die Seite **Verwalten** > **Registrierung**. Weitere Informationen finden Sie unter Senden von Registrierungseinladungen.

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.

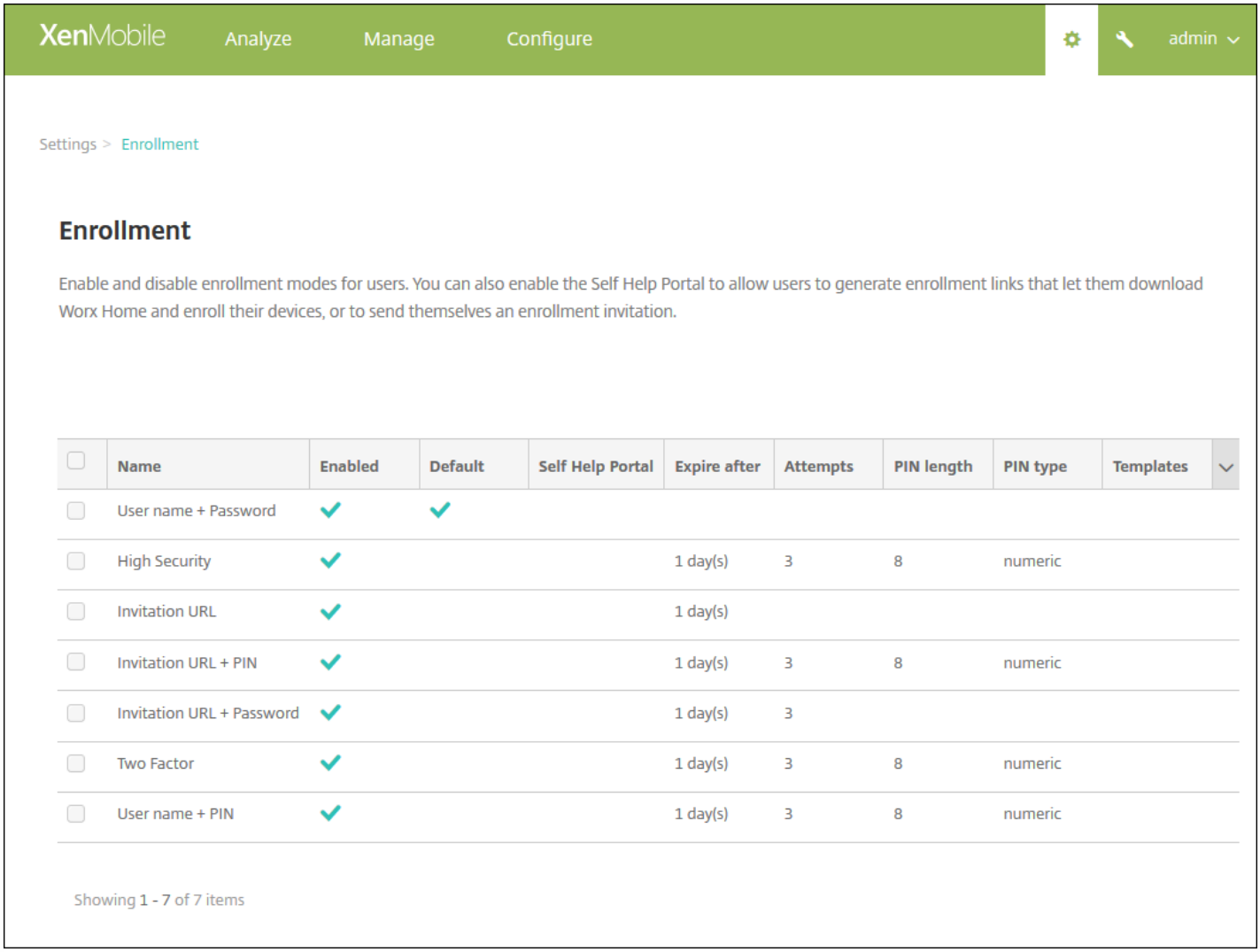
1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

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, deaktivieren Sie ihn oder erteilen Sie Benutzern Zugriff darauf über das Selbsthilfeportal.

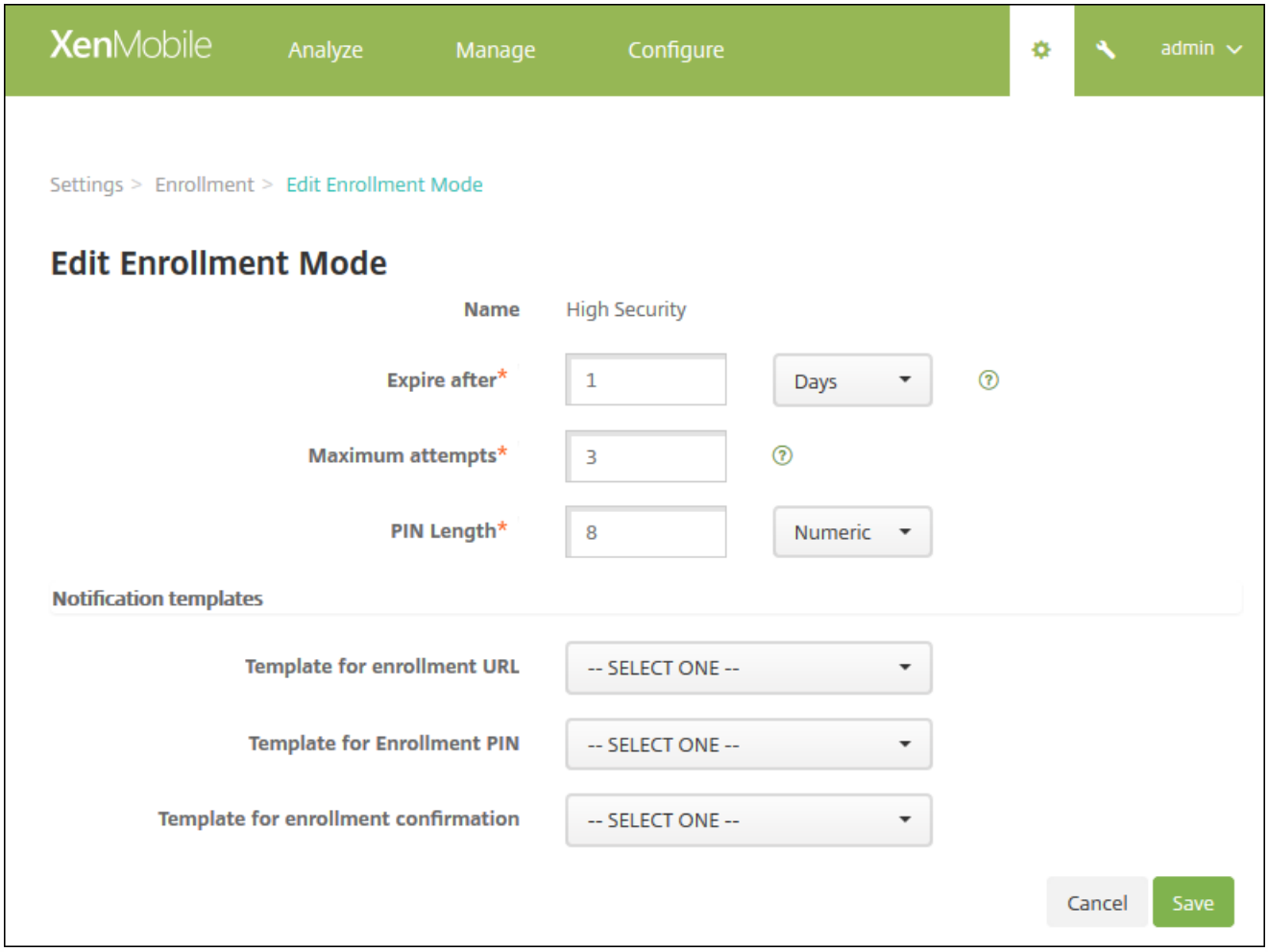
Hinweis: Wenn Sie das Kontrollkästchen neben einem Registrierungsmodus auswählen, wird das Menü mit den Optionen

oberhalb der Liste der Registrierungsmodi angezeigt. Wenn Sie an eine andere Stelle in der Liste klicken, wird das Menü mit den Optionen rechts daneben angezeigt.



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 Standardwert

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: Sie können **Nur Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** als Standardregistrierungsmodus festlegen.

1. Wählen Sie **Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** zum Festlegen 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.

Hinzufügen oder Entfernen von Gruppen

Gruppen werden im Dialogfeld **Gruppen verwalten** in der XenMobile-Konsole verwaltet. Dieses kann über die Seite

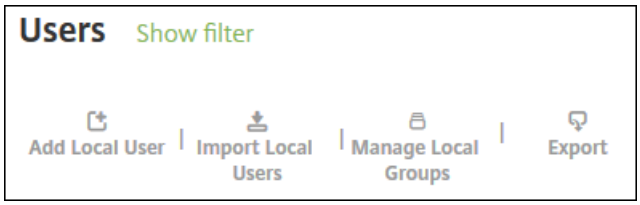
Benutzer, **Lokalen Benutzer hinzufügen** oder **Lokalen Benutzer bearbeiten** aufgerufen werden. Es gibt keinen spezifischen Befehl zum Bearbeiten von Gruppen.

Das Entfernen einer Gruppe hat keine Auswirkungen auf die Benutzerkonten. Beim Entfernen einer Gruppe wird lediglich die Zuordnung des Benutzers 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.

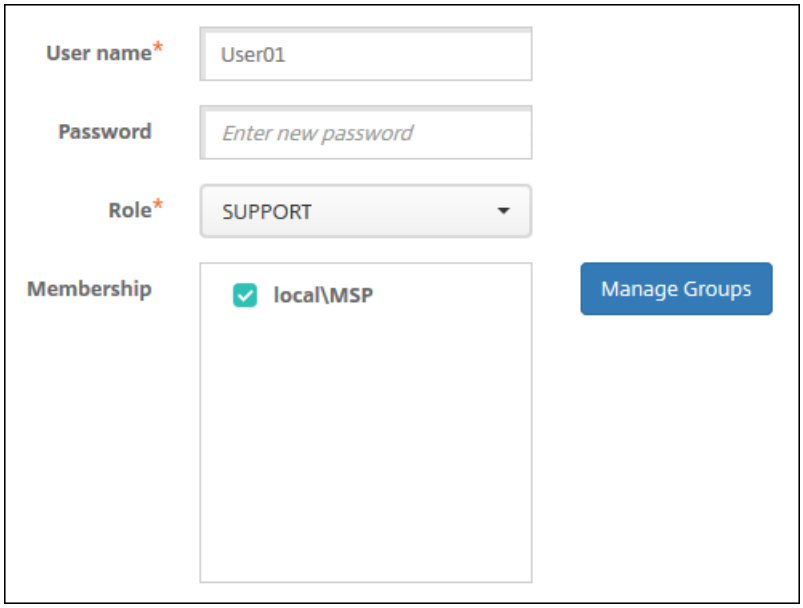
Hinzufügen einer lokalen Gruppe

1. Führen Sie einen der folgenden Schritte aus:

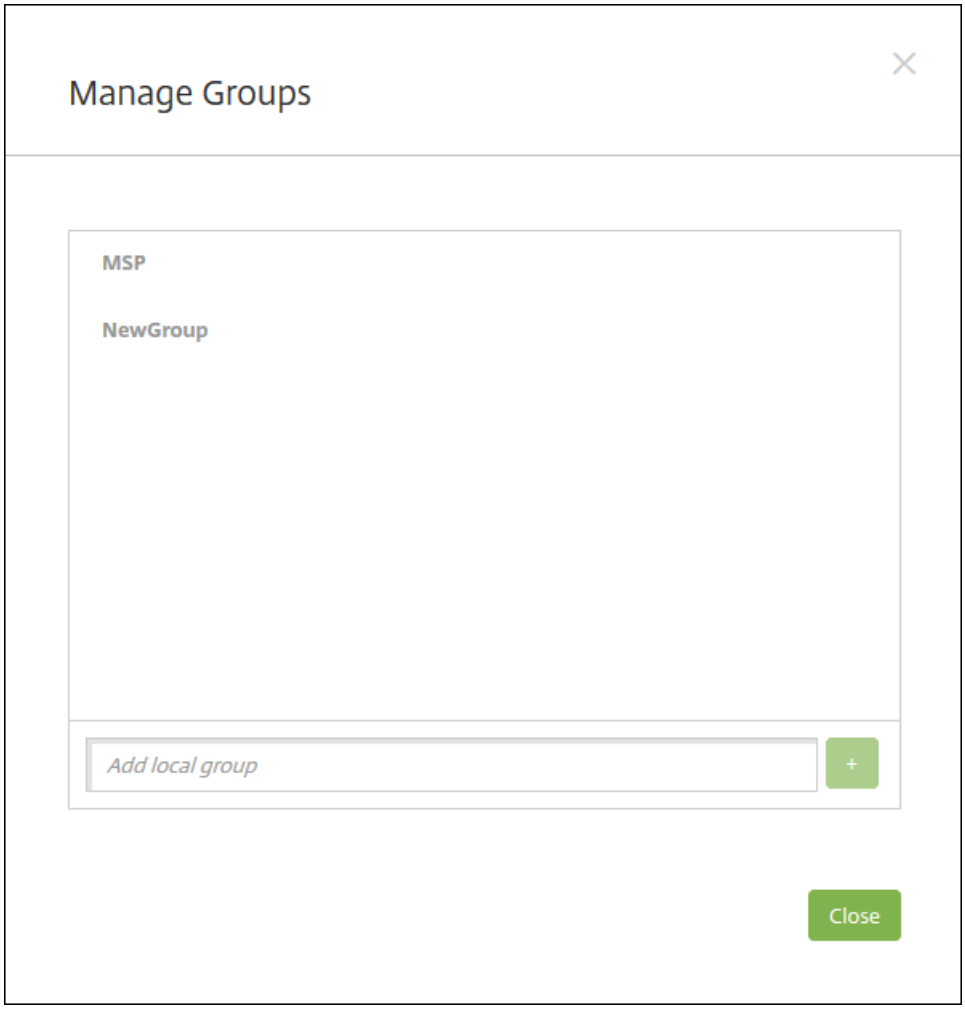
- Klicken Sie auf der Seite **Benutzer** auf **Lokale Gruppen verwalten**.



- 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**.

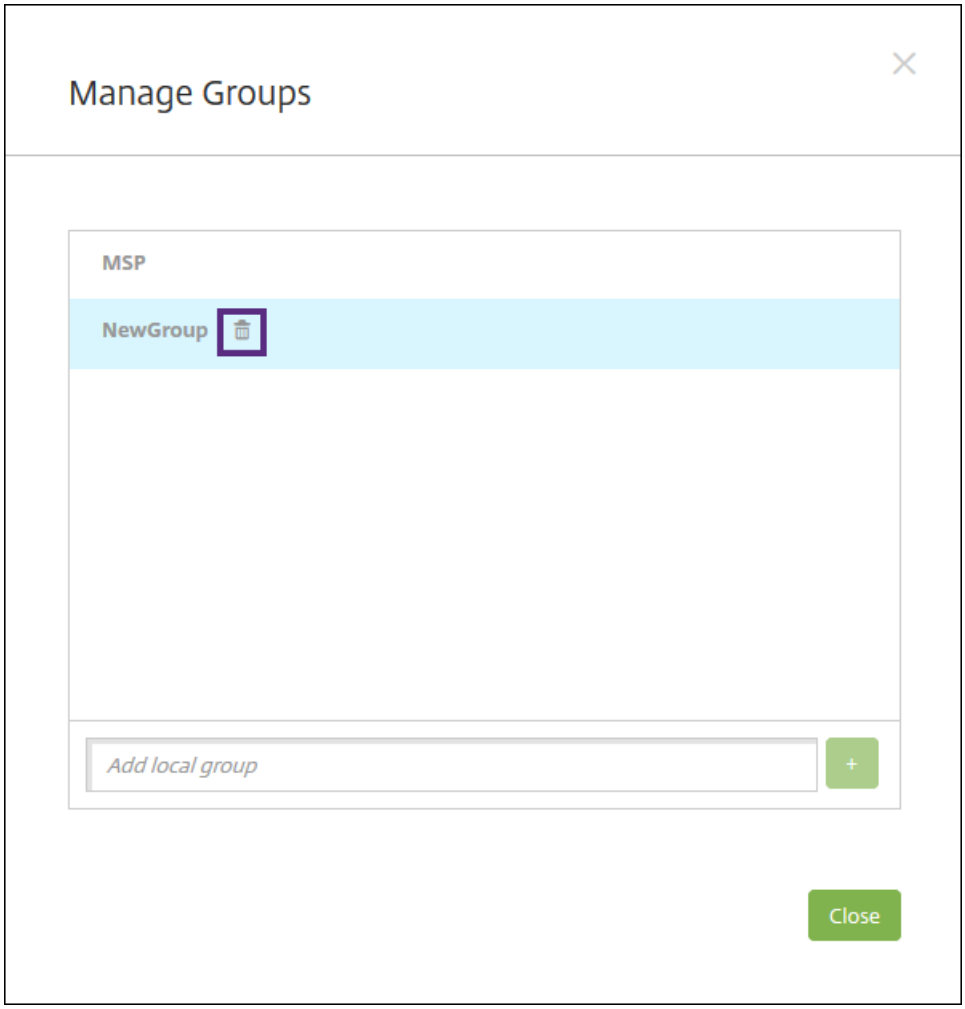
Entfernen einer Gruppe

Hinweis: Das Entfernen einer Gruppe hat keine Auswirkungen auf die Benutzerkonten. Beim Entfernen einer Gruppe wird lediglich die Zuordnung des Benutzers 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**.

Erstellen und Verwalten von Workflows

Sie können das Erstellen und Entfernen von Benutzerkonten mit Workflows verwalten. Damit ein Workflow verwendet werden kann, ermitteln Sie die Personen in Ihrer Organisation, die zum Genehmigen von Benutzerkontenanforderungen berechtigt sind. Anschließend können Sie mit der Workflowvorlage Benutzerkontenanforderungen erstellen und genehmigen.

Beim ersten Einrichten von XenMobile konfigurieren Sie Einstellungen für Workflow-E-Mails. Diese müssen festgelegt werden, bevor Sie Workflows verwenden können. Sie können die Einstellungen für Workflow-E-Mails jederzeit ändern. Diese Einstellungen umfassen E-Mail-Server, Port, E-Mail-Adresse und Angaben dazu, ob die Anforderung zum Erstellen des Benutzerkontos genehmigt werden muss.

Workflows können in XenMobile an zwei Stellen konfiguriert werden:

- Auf der Seite **Workflows** in der XenMobile-Konsole. Auf der Seite **Workflows** können Sie mehrere Workflows zur Verwendung mit App-Konfigurationen konfigurieren. Wenn Sie Workflows auf der Seite Workflows konfigurieren, können Sie den Workflow während des Konfigurierens der App auswählen.
- Wenn Sie einen Anwendungsconnector konfigurieren, geben Sie in der App einen Workflow-Namen an und konfigurieren anschließend die Personen, die die Benutzerkontoanforderung genehmigen können. Siehe Hinzufügen von Apps in XenMobile.

Sie können bis zu drei Ebenen für die Genehmigung von Benutzerkonten durch leitende Mitarbeiter zuweisen. Wenn noch weitere Personen zum Genehmigen eines Benutzerkontos berechtigt sein sollen, können Sie anhand des Namens oder der E-Mail-Adresse nach den Freigabeberechtigten suchen und sie auswählen. Wenn XenMobile die Person gefunden hat, können Sie sie zum Workflow hinzufügen. Alle Personen im Workflow erhalten E-Mails zum Genehmigen oder Ablehnen des neuen Benutzerkontos.

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

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

3. Klicken Sie auf **Hinzufügen**. Die Seite **Workflow hinzufügen** wird angezeigt.

4. Konfigurieren Sie folgende 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. Sie erstellen E-Mail-Vorlagen im Bereich **Benachrichtigungsvorlagen** der XenMobile-Konsole unter **Einstellungen**. Wenn Sie auf das Augensymbol rechts neben dem Feld klicken, wird eine Vorschau der Vorlage angezeigt, die Sie konfigurieren.
- **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 Person in das Suchfeld ein und klicken Sie dann auf **Suchen**. Für die Namen wird Active Directory verwendet.
- Wenn der Name 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 Selected additional required approvers 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.

5. Klicken Sie auf **Speichern**. Der erstellte Workflow wird auf der Seite **Workflows** angezeigt.

Nach dem Erstellen des Workflows können Sie dessen Details und die mit ihm verbundenen Apps anzeigen oder den Workflow löschen. Ein einmal erstellter Workflow kann nicht mehr geändert werden. Wenn ein Workflow mit anderen Genehmigungsebenen oder Freigabeberechtigten benötigt wird, müssen Sie einen weiteren Workflow erstellen.

Anzeigen von Details und Löschen eines Workflows

1. Auf der Seite **Workflows** wählen Sie in der Liste der vorhandenen Workflows einen bestimmten Workflow aus. Klicken Sie dafür auf die Zeile in der Tabelle oder aktivieren Sie das Kontrollkästchen neben dem Workflow.

2. Klicken Sie zum Löschen des Workflows auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie erneut auf **Löschen**.

Wichtig: Sie können diesen Vorgang nicht rückgängig machen.

Konfigurieren von Rollen mit RBAC

Feb 24, 2017

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.

Wenn Sie *Berechtigungen anwenden*, definieren Sie die Benutzergruppen, die mit der RBAC-Rolle verwaltet werden dürfen. Der Standardadministrator kann die angewendeten Berechtigungseinstellungen nicht ändern. Die angewendeten Berechtigungen gelten standardmäßig für alle Benutzergruppen.

Wenn Sie eine *Zuweisung* durchführen, weisen Sie die RBAC-Rolle einer Gruppe zu, sodass diese Benutzergruppe die RBAC-Administratorrechte erhält.

Konfigurieren von Rollen mit RBAC

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.

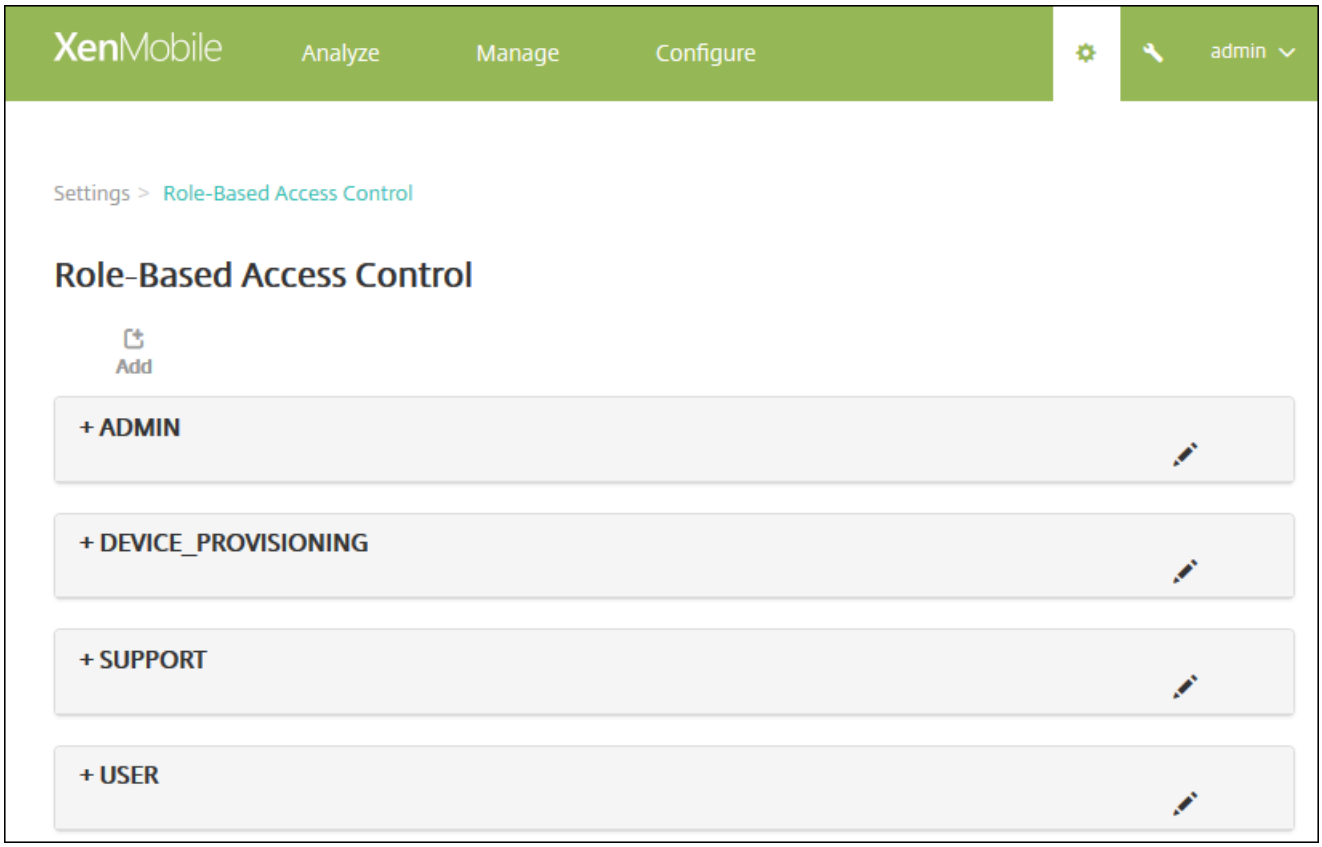
Hinweis: Lokalen Benutzern kann bei Bedarf nur eine Rolle zugewiesen werden.

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

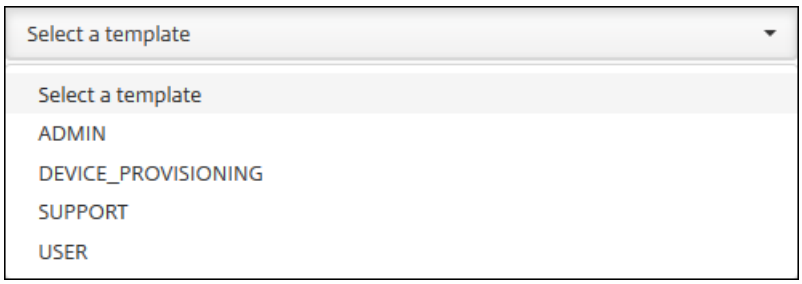
vorhandenen Rolle, um diese zu bearbeiten, oder klicken Sie auf das Papierkorbsymbol rechts neben einer von Ihnen hinzugefügten Rolle, um sie zu löschen. Sie können die Standardbenutzerrollen nicht löschen.

- 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.

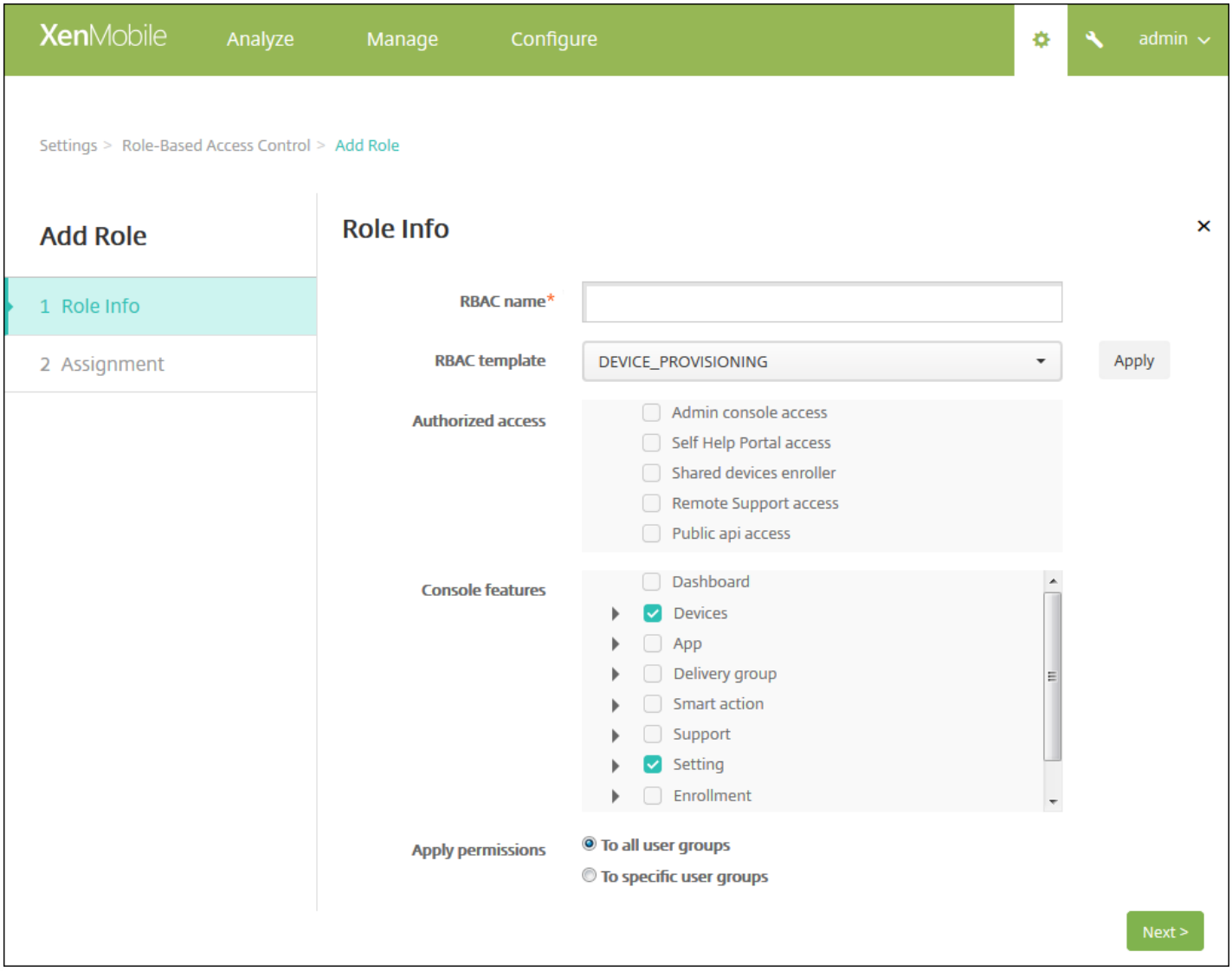
4. Geben Sie die folgenden Informationen zum Erstellen einer neuen Benutzerrolle bzw. zum Bearbeiten einer vorhandenen Benutzerrolle ein:

- **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.

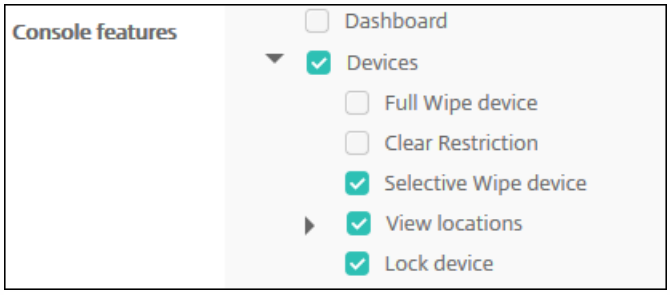


5. Klicken Sie auf rechts neben dem Feld **RBAC-Vorlage** auf **Anwenden**, um die Kontrollkästchen für **Autorisierter Zugriff** und **Konsolenfeatures** gemäß den Berechtigungen der ausgewählten Vorlage einzustellen.

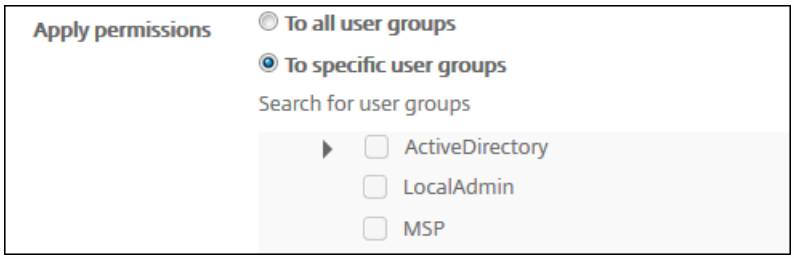


6. Aktivieren bzw. deaktivieren Sie die Kontrollkästchen für **Autorisierter Zugriff** und **Konsolenfeatures**, um die Rolle anzupassen.

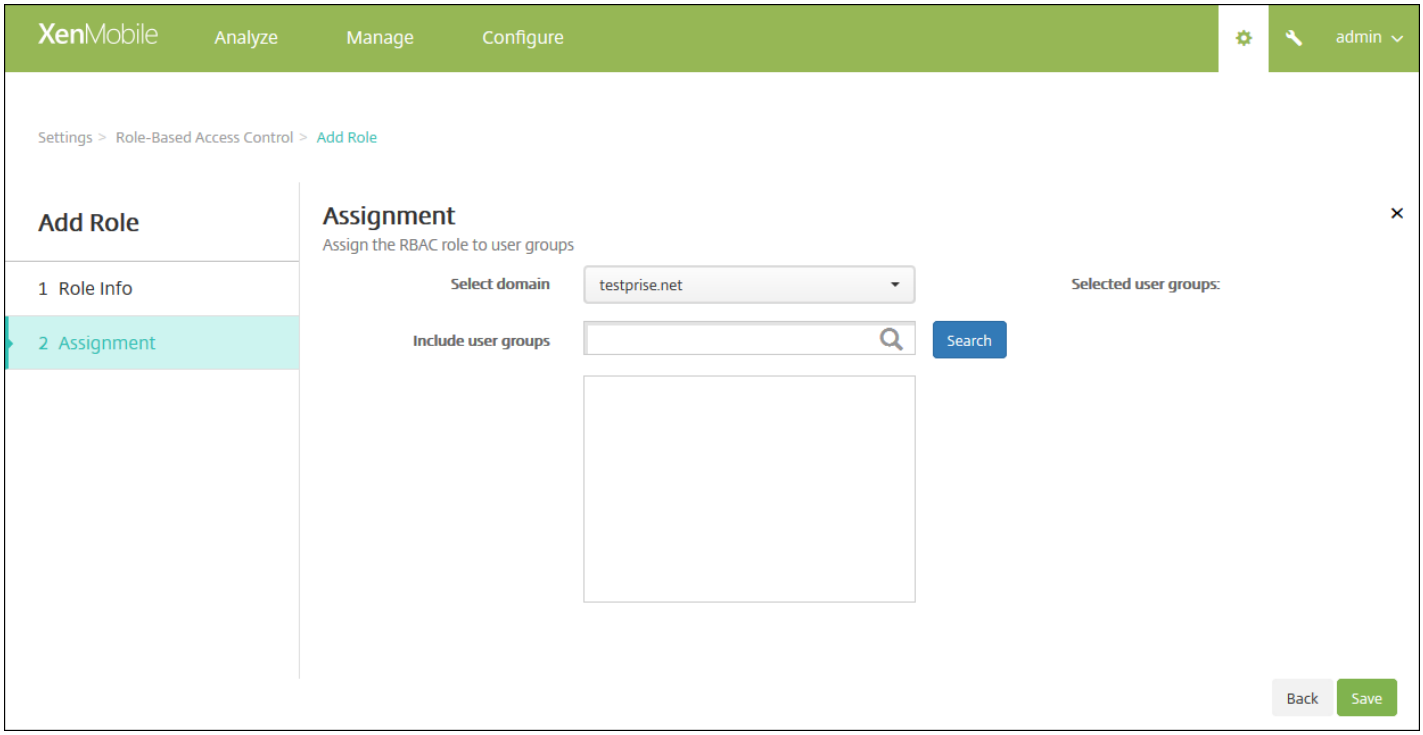
Wenn Sie auf das Dreieck neben einem Konsolenfeature klicken, werden featurespezifische Berechtigungen angezeigt, die Sie aktivieren und deaktivieren können. Wenn Sie auf das oberste Kontrollkästchen eines Konsolenbereichs klicken, wird der Zugriff auf den Konsolenbereich verweigert. Zum Aktivieren des Zugriffs auf spezifische Optionen müssen Sie jeweils das zugehörige Kontrollkästchen aktivieren. In dem Beispiel unten werden beispielsweise die Optionen **Gerät vollständig löschen** und **Einschränkungen deaktivieren** für die der Rolle zugewiesenen Benutzer nicht in der Konsole angezeigt und die mit einem Häkchen versehenen Optionen werden angezeigt.



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.

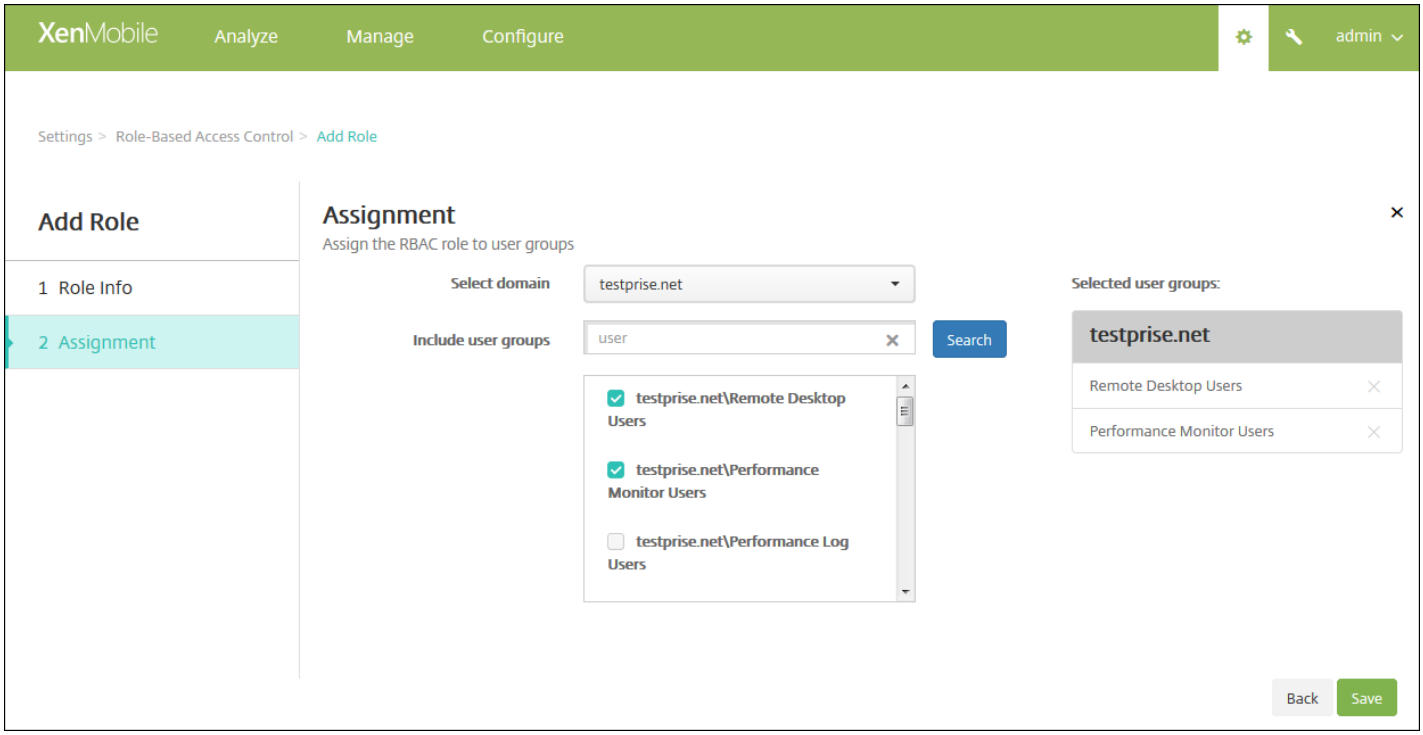


8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** wird angezeigt.



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**.

Benachrichtigungen

Feb 24, 2017

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 Kommunikationssystemen für Textnachrichten. SMS 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.

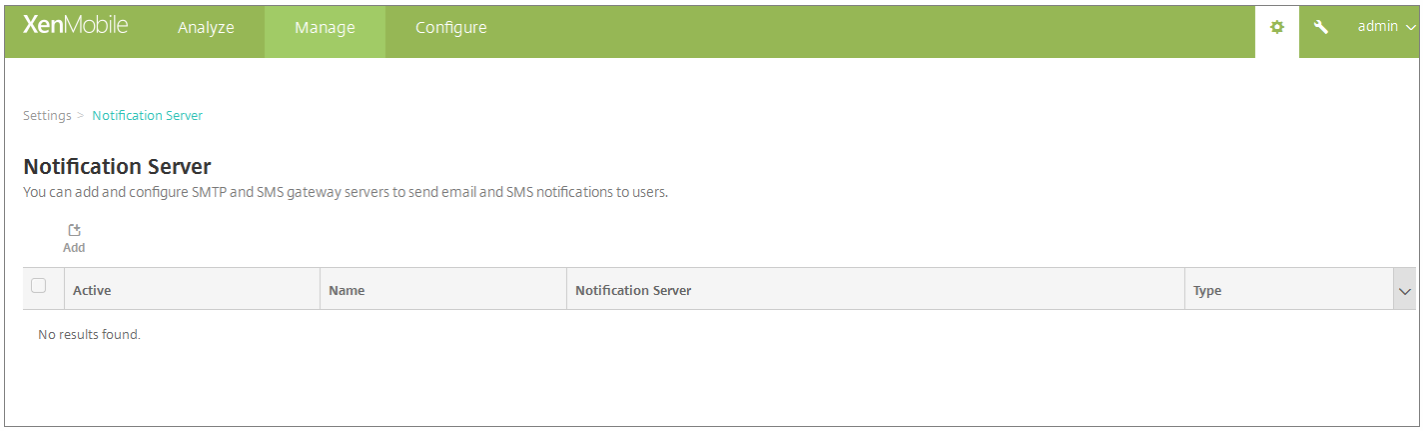
Voraussetzungen

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

Konfigurieren eines SMTP-Servers und eines SMS-Gateways

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

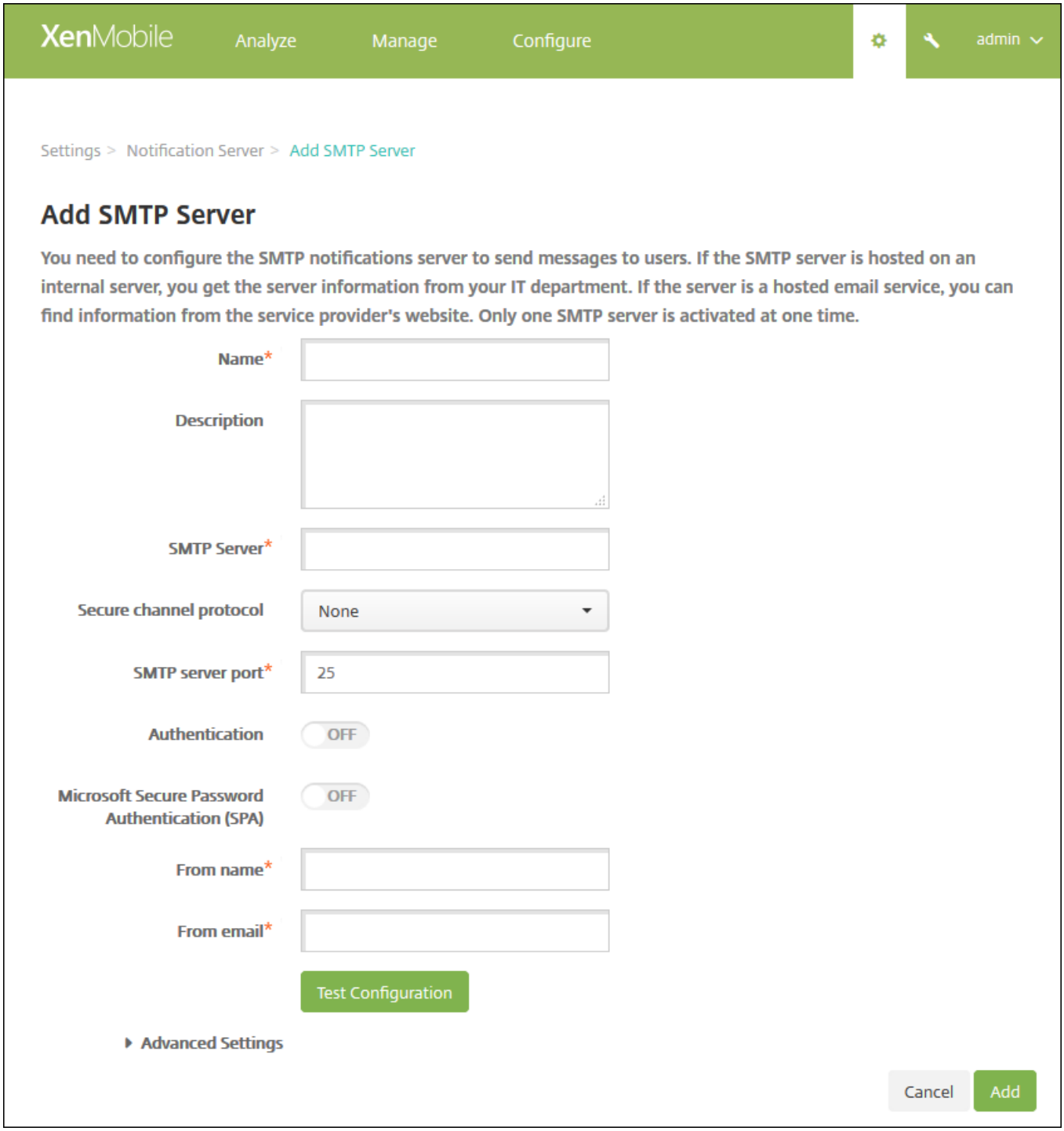
2. Klicken Sie unter **Benachrichtigungen** auf **Benachrichtigungsserver**. Die Seite **Benachrichtigungsserver** wird angezeigt.



2. Klicken Sie auf **Hinzufügen**. Ein Menü mit Optionen zum Konfigurieren eines SMTP-Servers oder 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.

Hinzufügen eines SMTP-Servers



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.

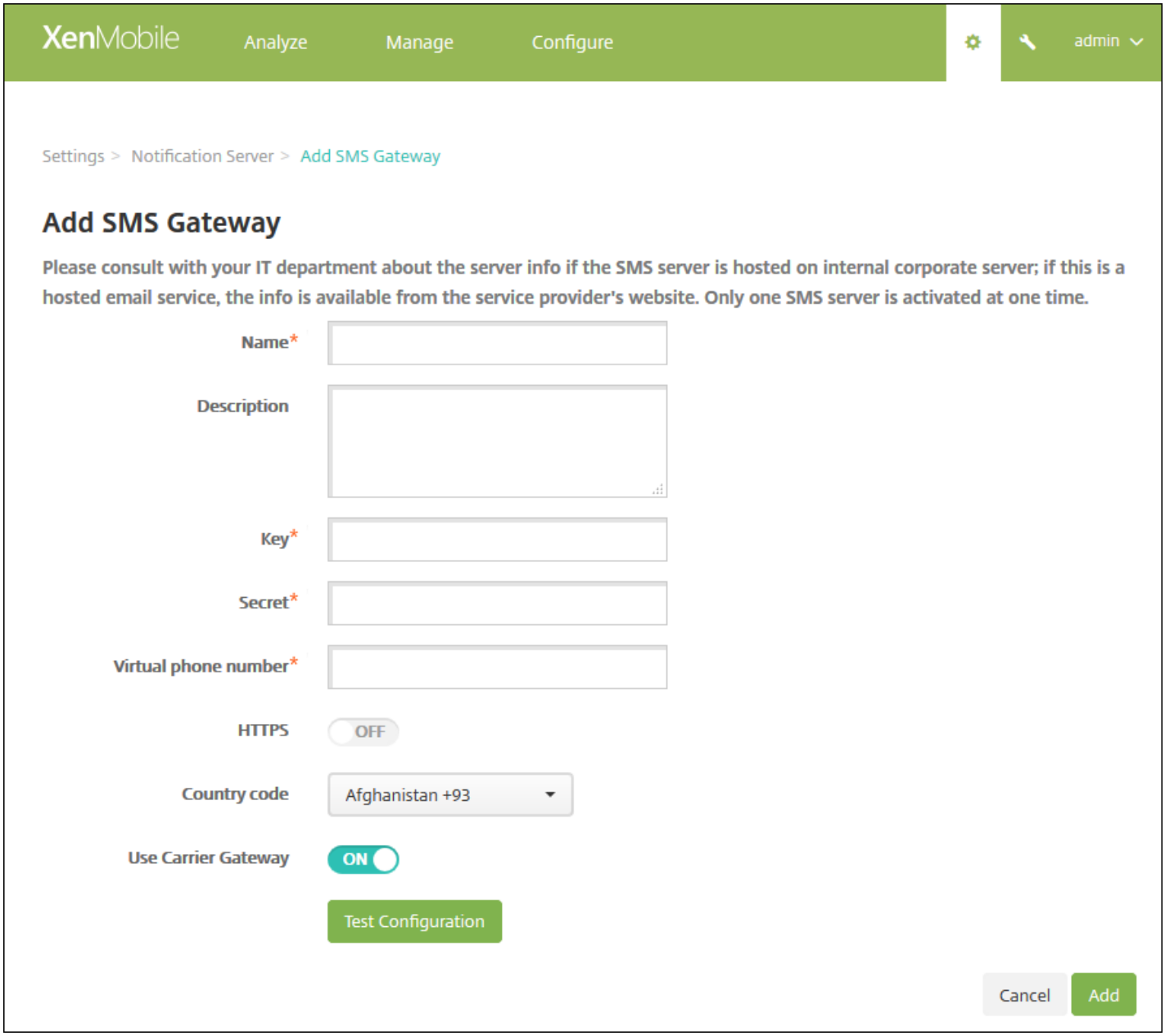
2. Klicken Sie auf **Konfiguration testen**, um eine Test-E-Mail zu senden.

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**.

Hinzufügen eines Netzbetreiber-SMS-Gateways



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 eingeben und dürfen in diesem Feld nur Zahlen verwenden. 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**.

  Wichtig: Übernehmen Sie die Einstellung **EIN** für "HTTPS", es sei denn, Sie werden vom Citrix Support dazu aufgefordert, sie zu deaktivieren.

- **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.

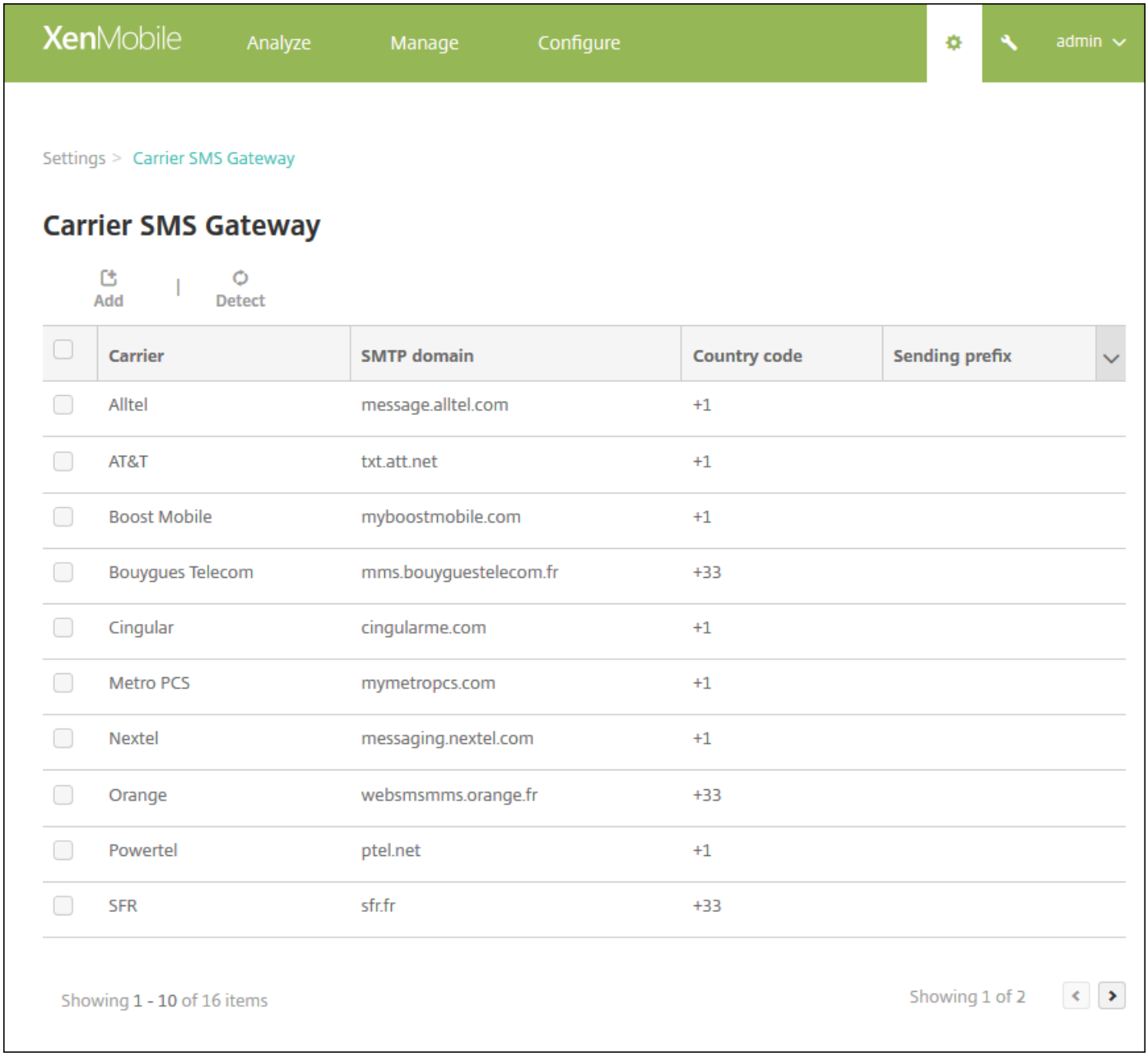
2. Klicken Sie auf **Hinzufügen**.

Hinzufügen eines Netzbetreiber-SMS-Gateways

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.

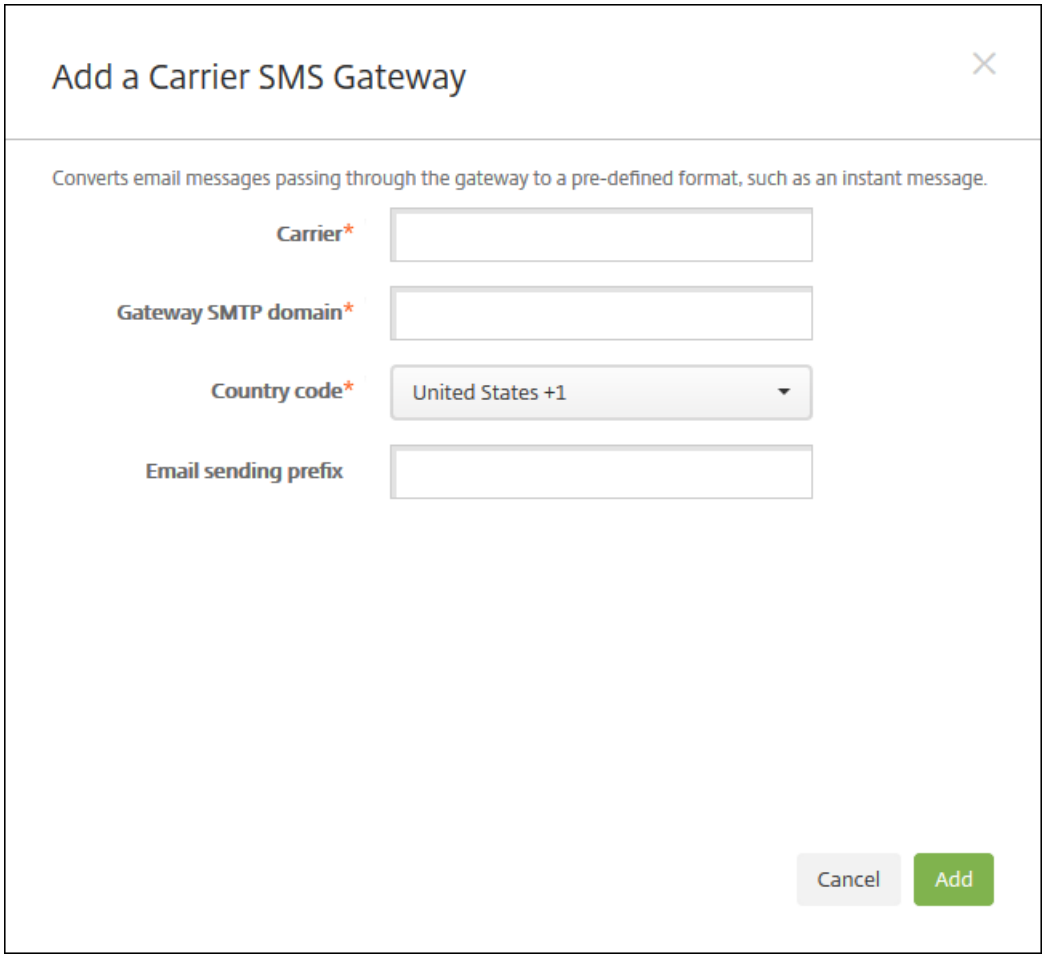
1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

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.

Erstellen und Aktualisieren von Benachrichtigungsvorlagen

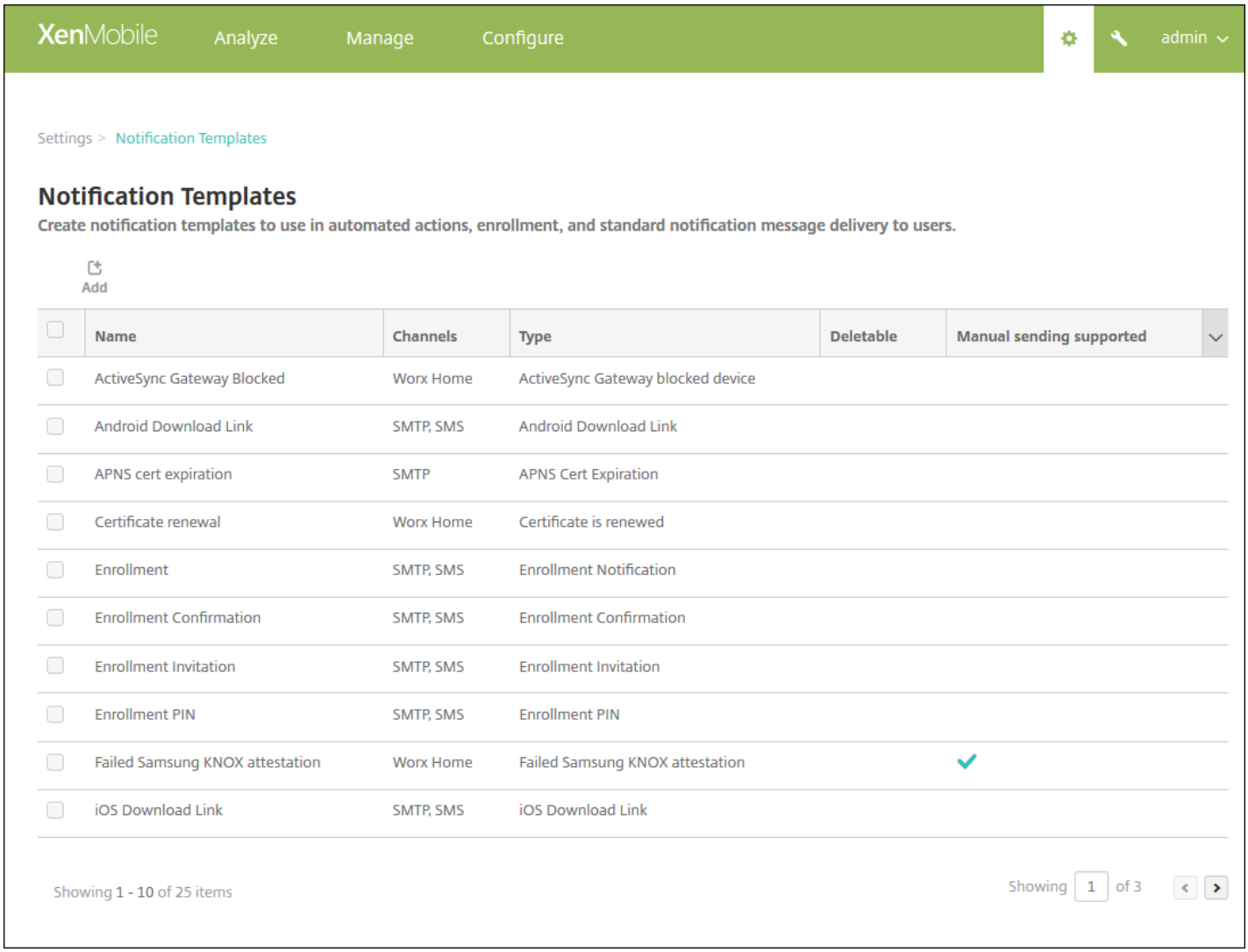
Sie können Benachrichtigungsvorlagen zur Verwendung in automatisierten Aktionen, bei der Registrierung und für Standardbenachrichtigungen an Benutzer erstellen und aktualisieren. Sie können Benachrichtigungsvorlagen zum Senden von Nachrichten über drei verschiedene Kanäle konfigurieren: Secure Hub, SMTP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

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.

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 folgende 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 **Secure Hub** 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.

Secure Hub:

- **Aktivieren**: Klicken Sie hier zum Aktivieren dieses Benachrichtigungskanals.
- **Nachricht**: Geben Sie die Nachricht ein, die an Benutzer gesendet werden soll. Dieses Feld ist erforderlich, wenn Sie Secure Hub 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 Geräte.

- **Betreff**: Geben Sie einen aussagekräftigen Betreff für die Benachrichtigung ein. Diese Angabe ist erforderlich.
- **Nachricht**: Geben Sie die Nachricht ein, die an 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 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 Secure Hub. 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.

2. Klicken Sie auf **Löschen** zum Löschen der Benachrichtigungsvorlage oder auf **Abbrechen**, um den Vorgang abzubrechen.

Geräte

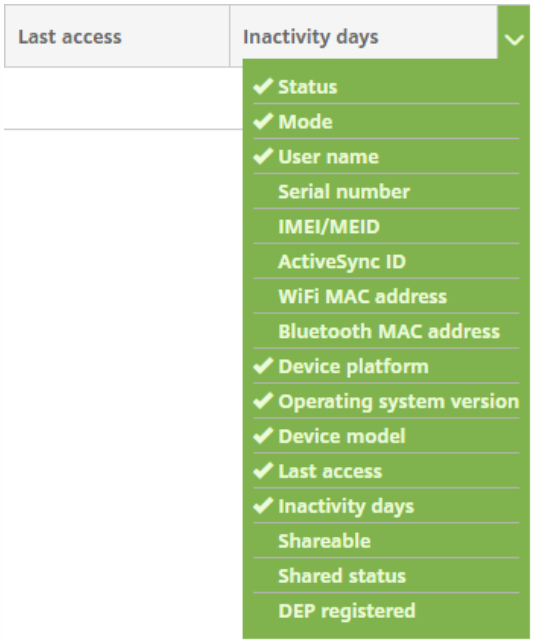
Apr 24, 2017

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 Geräteprovisioning finden Sie unter Geräteprovisioningdateiformate.

Auf der Seite **Geräte** der XenMobile-Konsole werden alle Geräte mit folgenden Informationen aufgelistet:

- **Status** (Symbole, die angeben, ob ein Jailbreak vorliegt, ob das Gerät verwaltet wird, ob ActiveSync Gateway verfügbar ist und welchen Bereitstellungszustand das Gerät aufweist)
- **Modus** (ob das Gerät im MDM- oder MAM-Modus oder beidem verwaltet wird)
- Weitere Informationen, z. B. **Benutzername**, **Gräteplattform**, **Betriebssystemversion**, **Gerätemodell**, **Letzter Zugriff** und **Inaktivität (in Tagen)**. Dies sind die standardmäßig angezeigten Tabellenspalten.

Zum Anpassen der Tabelle **Geräte** klicken Sie auf den Pfeil nach unten in der letzten Spaltenüberschrift und aktivieren die Spaltenüberschriften, die in der Tabelle angezeigt werden sollen, bzw. deaktivieren diejenigen, die nicht angezeigt werden sollen.



Sie können Geräte manuell hinzufügen, Geräte aus einer Geräteprovisioningdatei importieren, Gerätedetails bearbeiten, Sicherheitsaktionen durchführen, Benachrichtigungen an Geräte senden und Geräte löschen. Sie können auch alle Gerätedaten aus der Tabelle in eine CSV-Datei exportieren, um einen benutzerdefinierten Bericht zu generieren. Der Server exportiert alle Geräteattribute und wenn Sie Filter anwenden, werden diese beim Erstellen der CSV-Datei berücksichtigt.

Weitere Informationen zum Verwalten von Geräten finden Sie in den folgenden Abschnitten:

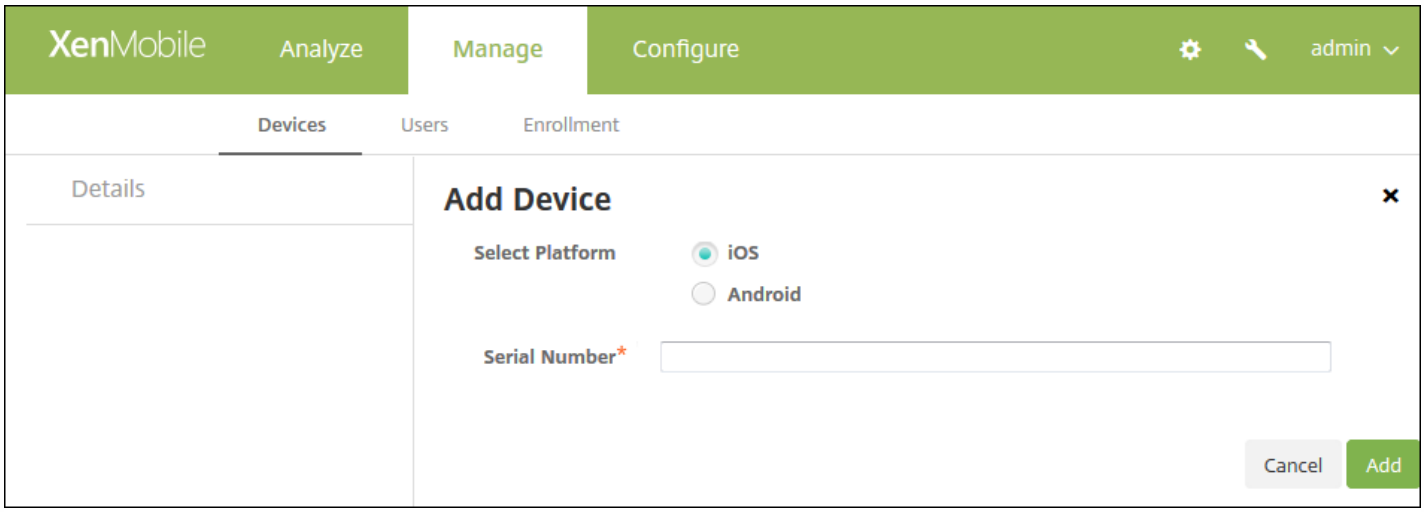
- Gerät manuell hinzufügen
- Geräte aus einer Provisioningdatei importieren
- Sicherheitsaktionen durchführen
- Benachrichtigung an Geräte senden

- Geräte löschen
- Gerätetabelle exportieren
- Geräte manuell per Tag kennzeichnen
- Geräteprovisioningdateiformate
- Namen und Werte von Geräteeigenschaften

Gerät manuell hinzufügen

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.

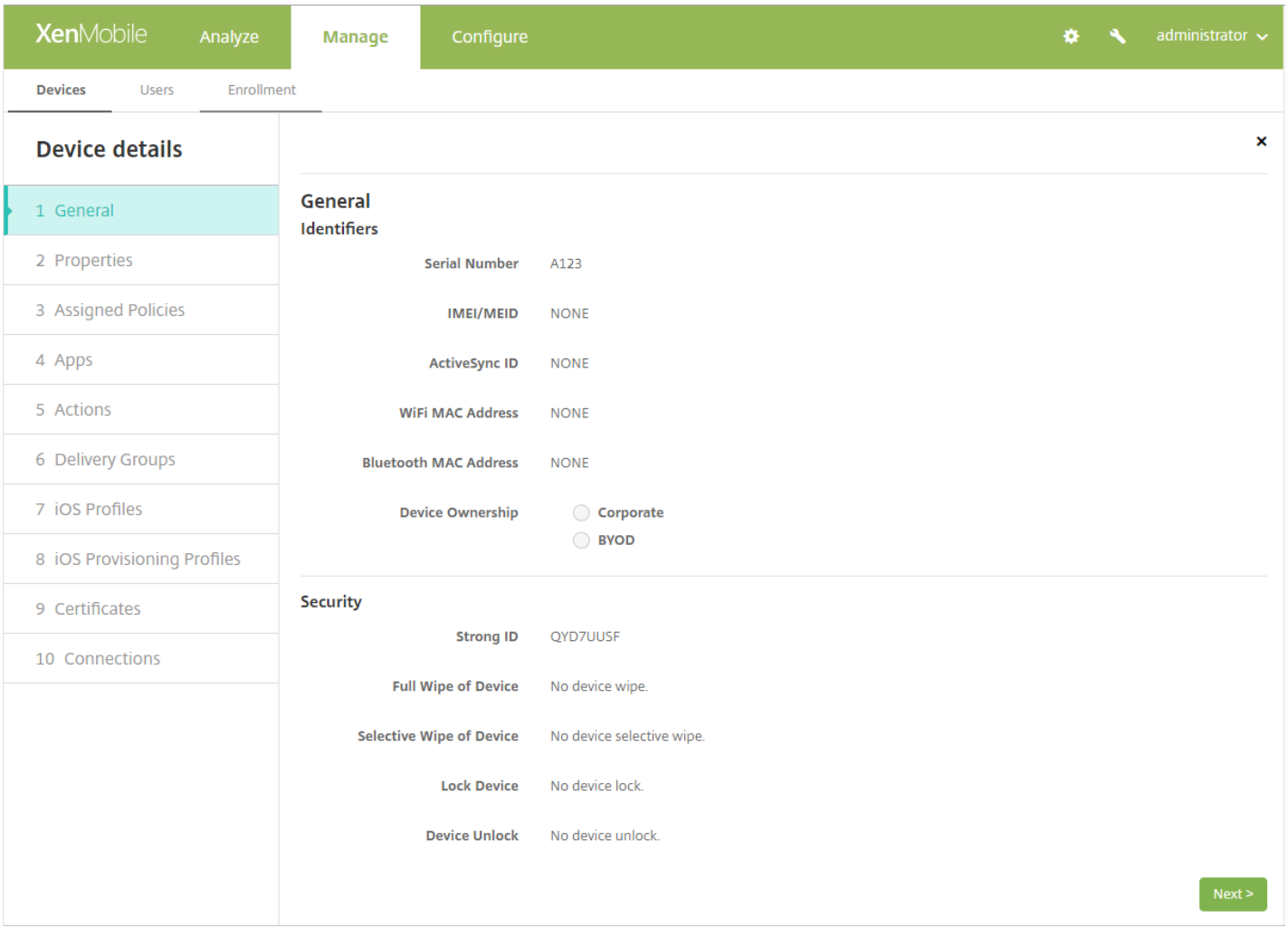


3. Konfigurieren Sie folgende Einstellungen:

- **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. Auf der Seite **Allgemein** werden Gerätekennungen aufgeführt, z. B. die Seriennummer, ActiveSync-ID und weitere plattformspezifische Informationen. Wählen Sie für **Gerätebesitz** die Option **Unternehmen** oder **BYOD**.

Auf der Seite **Allgemein** werden außerdem Sicherheitseigenschaften aufgeführt, z. B. starke ID, Gerätesperrung, Umgehen der Aktivierungssperre und weitere plattformspezifische Informationen.

6. Auf der Seite **Eigenschaften** werden die von XenMobile bereitgestellten Geräteeigenschaften aufgeführt. Diese Liste enthält alle in der beim Hinzufügen des Geräts verwendeten Provisioningdatei enthaltenen Geräteeigenschaften. Wenn Sie eine Eigenschaft hinzufügen möchten, klicken Sie auf **Hinzufügen** und wählen Sie eine Eigenschaft in der Liste. Gültige Werte für jede Eigenschaft finden Sie unter Namen und Werte von Geräteeigenschaften in diesem Artikel.

Wenn Sie eine Eigenschaft hinzufügen, wird sie zunächst in der Kategorie angezeigt, in der Sie sie hinzufügen. Wenn Sie anschließend auf **Weiter** klicken und dann zu der Seite **Eigenschaften** zurückkehren, wird die Eigenschaft in der richtigen Liste angezeigt.

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. Die verbleibenden Abschnitte mit Gerätedetails enthalten zusammenfassende Informationen zu dem Gerät.

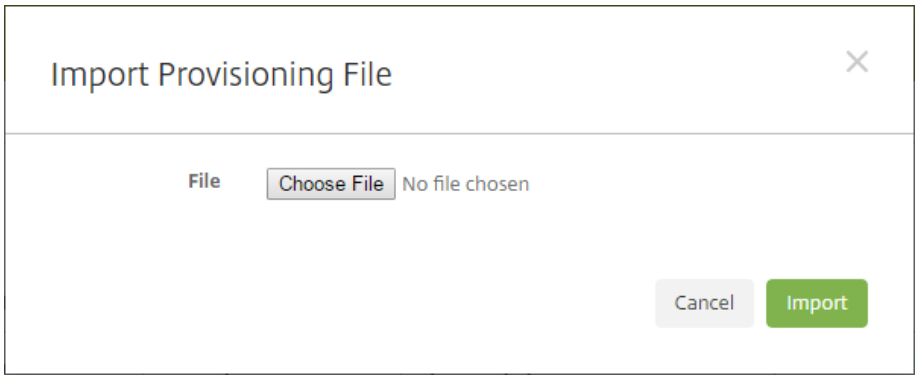
- **Zugewiesene Richtlinien**: zeigt die Anzahl der zugewiesenen bereitgestellten, ausstehenden und fehlgeschlagenen Richtlinien an. Für die einzelnen Richtlinien werden Name, Typ und letzte Bereitstellung angezeigt.

- **Apps**: zeigt die Anzahl der installierten, ausstehenden und fehlerhaften Apps der letzten Bestandsaufnahme an. Es werden App-Name, ID, Typ und weitere Informationen angezeigt.
- **Aktionen**: zeigt die Anzahl der bereitgestellten, ausstehenden und fehlgeschlagenen Aktionen an. Es werden Aktionsname und Uhrzeit der letzten Bereitstellung angezeigt.
- **Bereitstellungsgruppen**: zeigt die Anzahl der erfolgreichen, ausstehenden und fehlerhaften Bereitstellungsgruppen an. Für jede Bereitstellung werden der Name der Bereitstellungsgruppe und die Uhrzeit der Bereitstellung angezeigt. Wählen Sie eine Bereitstellungsgruppe, um weitere Informationen (Status, Aktion und Kanal oder Benutzer) anzuzeigen.
- **iOS-Profile**: zeigt den aktuellen iOS-Profilbestand mit Namen, Typ, Unternehmen und Beschreibung an.
- **iOS-Provisioningprofil**: zeigt Informationen zum Provisioningprofil für die Verteilung im Unternehmen an, z. B. UUID, Ablaufdatum und verwaltet oder nicht.
- **Zertifikate**: zeigt Informationen für gültige, abgelaufene und gesperrte Zertifikate an, z. B. Typ, Anbieter, Herausgeber, Seriennummer und Zeit in Tagen bis zum Ablauf.
- **Verbindungen**: zeigt den ersten und letzten Verbindungsstatus an. Für jede Verbindung werden zudem der Benutzername und der Zeitpunkt der vorletzten und letzten Authentifizierung angezeigt.
- **TouchDown** (nur Android-Geräte): zeigt die letzte Geräteauthentifizierung und die letzte Benutzerauthentifizierung an. Es werden Name und Wert jeder angewendeten Richtlinie angezeigt.

Importieren von Geräten aus einer Provisioningdatei

Sie können die Datei eines Mobilfunkanbieters oder Geräteherstellers oder Ihre eigene Provisioningdatei importieren. Weitere Informationen finden Sie unter Geräteprovisioningdateiformate in diesem Artikel.

1. Gehen Sie zu **Verwalten > Geräte** und klicken Sie auf **Importieren**. Das Dialogfeld **Provisioningdatei importieren** wird angezeigt.



2. Klicken Sie auf **Datei wählen** und navigieren Sie zu der Datei, die Sie importieren möchten.

3. Klicken Sie auf **Importieren**. In der Tabelle **Geräte** wird die importierte Datei angezeigt.

4. Zum Bearbeiten der Geräteinformationen wählen Sie die Datei und klicken Sie auf **Bearbeiten**. Informationen über die Seiten mit den Gerätedetails finden Sie unter Manuelles Hinzufügen von Geräten.

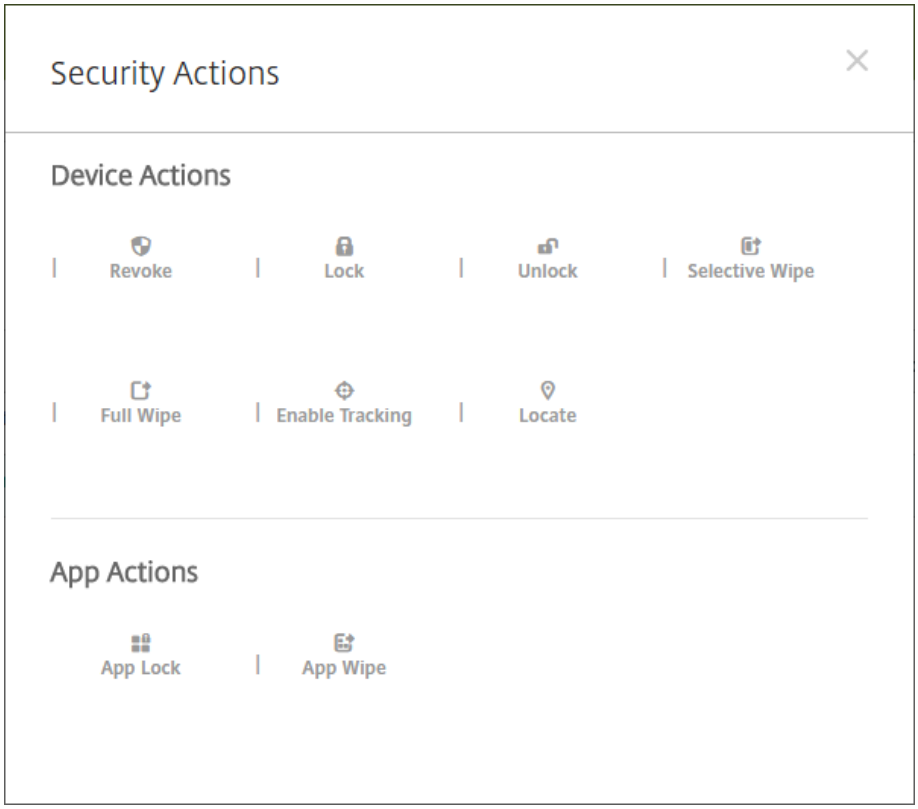
Durchführen von Sicherheitsaktionen

Auf der Seite **Geräte** können Sie Sicherheitsaktionen für Geräte und Apps durchführen. Zu den Geräteaktionen gehören Widerrufen, Sperren, Entsperren und Löschen. Zu den App-Sicherheitsaktionen gehören Sperren und Löschen.

1. Wählen Sie auf der Seite **Verwalten > Geräte** ein verwaltetes Gerät aus und klicken Sie auf **Sicherheit**.

2. Klicken Sie unter **Sicherheitsaktionen** auf eine Aktion und folgen Sie sämtlichen Aufforderungen.

Details über die Aktionen finden Sie unter Automatisierte Aktionen.



Manuelles Sperren, Entsperren, Löschen und Rückgängigmachen des Löschvorgangs

1. Gehen Sie zu **Verwalten** > **Geräte**, wählen Sie ein verwaltetes 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 der Benutzer momentan gesperrt oder gelöscht.

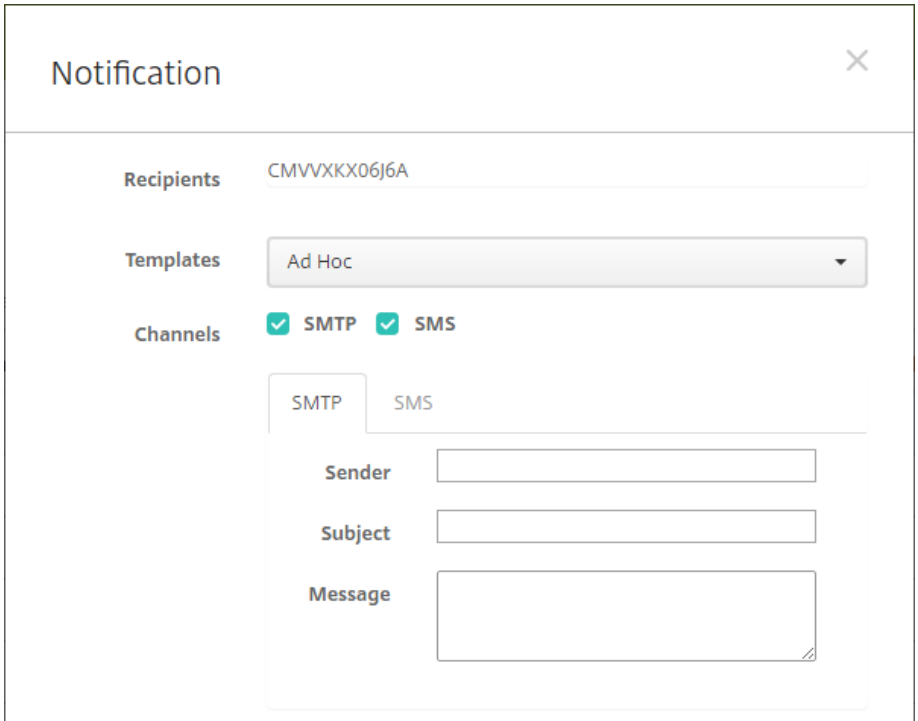
3. Bestätigen Sie die Aktion.

Senden einer Benachrichtigung an Geräte

Sie können Benachrichtigungen an Geräte über die Seite Geräte senden. Weitere Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen.

1. Wählen Sie auf der Seite **Verwalten > Geräte** das oder die Geräte aus, an die Sie die 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 folgende 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. Standardwert ist **SMTP** und **SMS**. Klicken Sie auf die Registerkarten zum Anzeigen des Nachrichtenformats für die einzelnen Kanäle.
- **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**.

Geräte löschen

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**. Sie können diesen Vorgang nicht rückgängig machen.

Exportieren der Gerätetabelle

1. Filtern Sie die Tabelle **Geräte** nach den Informationen, die in der Exportdatei angezeigt werden sollen.

2. Klicken Sie auf die Schaltfläche **Exportieren** oberhalb der Tabelle **Geräte**. Die Informationen in der Tabelle **Geräte** werden extrahiert und in eine CSV-Datei konvertiert.

3. Bei Erscheinen der entsprechenden Aufforderung öffnen oder speichern Sie die CSV-Datei. Ihre Vorgehensweise hängt von dem verwendeten Browser ab. Sie können den Vorgang auch abbrechen.

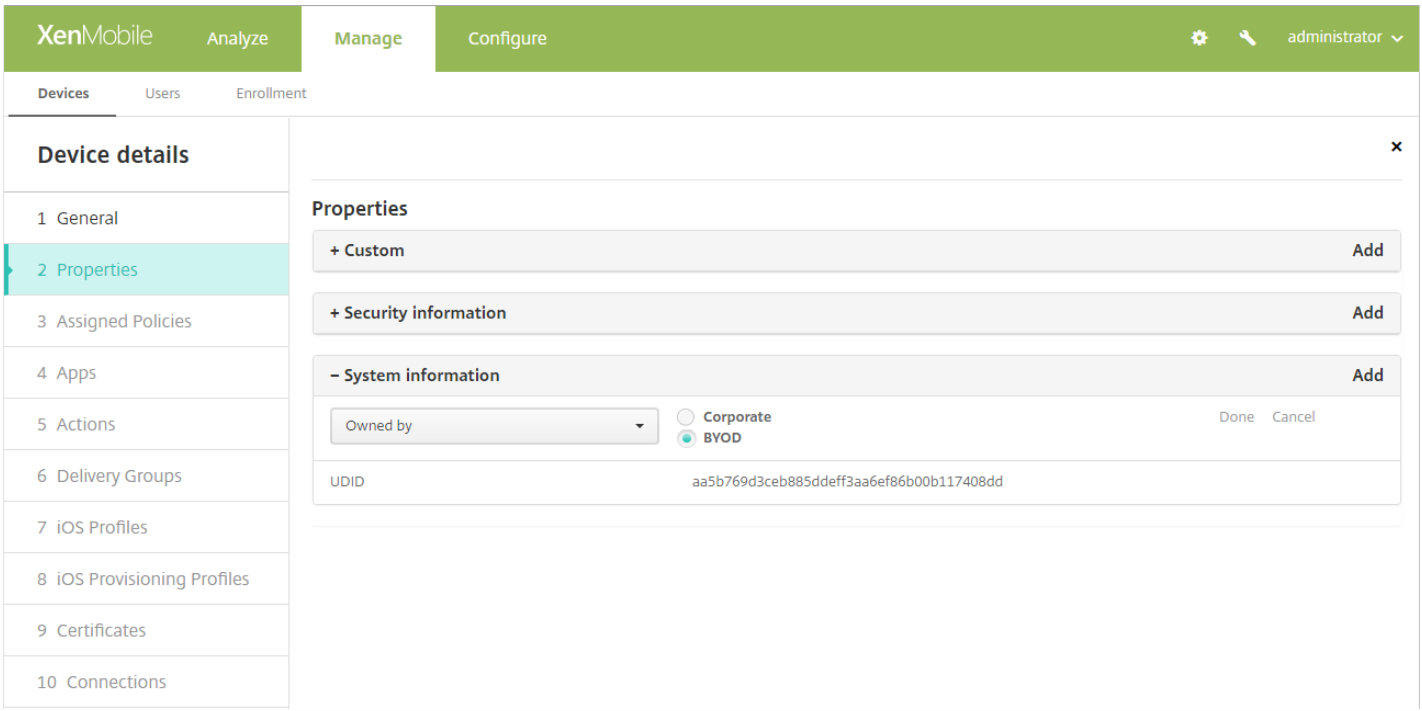
Geräte manuell per Tag kennzeichnen

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

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

Hinweise:

- Namen und Werte von Eigenschaften finden Sie unter "Namen und Werte von Geräteeigenschaften" im nächsten Abschnitt.
- Verwenden Sie den UTF-8-Standardzeichensatz.
- Trennen Sie die Felder in der Provisioningdatei durch Semikola (;). Wenn ein Feld ein Semikolon enthält, schützen Sie es mit einem umgekehrten Schrägstrich (\).

  Beispiel: Schützen Sie das Semikolon der Eigenschaft propertyV;test;1;2

so:
propertyV\;test\;1\;2

- Die Seriennummer ist für iOS-Geräte erforderlich, da sie bei iOS als Geräte-ID verwendet wird.
- Für andere Geräteplattformen müssen Sie entweder die Seriennummer oder die IMEI verwenden.
- Gültige Werte für **OperatingSystemFamily** sind **WINDOWS**, **ANDROID** oder **iOS**.

Beispiel einer Geräteprovisioningdatei KOPIEREN

```
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;
```

Jede Zeile der Datei enthält ein Gerät. Der erste Eintrag in dem Beispiel oben bedeutet Folgendes:

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

Namen und Werte von Geräteeigenschaften

Name der Eigenschaft auf der Seite "Verwalten > Geräte"	**Namen und Werte in der Geräteprovisioningdatei**	**Werttyp**
Windows HAS AIK Present?	WINDOWS_HAS_AIK_PRESENT	Zeichenfolge
Konto vorübergehend gesperrt?	GOOGLE_AW_DIRECTORY_SUSPENDED	Zeichenfolge
Code zum Umgehen der Aktivierungssperre	ACTIVATION_LOCK_BYPASS_CODE	Zeichenfolge
Aktivierungssperre aktiviert	ACTIVATION_LOCK_ENABLED Werte (Bedeutung):	Boolesch

	1 (Ja) 0 (Nein)	
Aktives iTunes-Konto	ACTIVE_ITUNES Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
ActiveSync-ID	EXCHANGE_ACTIVESYNC_ID	Zeichenfolge
ActiveSync-Gerät ist MSP bekannt	AS_DEVICE_KNOWN_BY_ZMSP Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Administrator deaktiviert	ADMIN_DISABLED Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
Amazon MDM API verfügbar	AMAZON_MDM Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Android for Work - Geräte-ID	GOOGLE_AW_DEVICE_ID	Zeichenfolge
Android for Work-aktiviertes Gerät?	GOOGLE_AW_ENABLED_DEVICE	Zeichenfolge
Android for Work - Installationstyp	GOOGLE_AW_INSTALL_TYPE Werte: DeviceAdministrator (Gerätebesitzer) AvengerManagedProfile (verwaltetes Work-Gerät) ManagedProfile (Work-Profil)	Zeichenfolge
Bestandskennzeichen	ASSET_TAG	Zeichenfolge
Status für automatische Updates	AUTOUPDATE_STATUS	Zeichenfolge
Verfügbarer RAM	MEMORY_AVAILABLE	Ganzzahl

Verfügbarer Speicherplatz	TOTAL_DISK_SPACE	Ganzzahl
BIOS-Info	BIOS_INFO	Zeichenfolge
Backupakku	BACKUP_BATTERY_PERCENT	Ganzzahl
Firmwareversion für Basisband	MODEM_FIRMWARE_VERSION	Zeichenfolge
Akkustatus	BATTERY_STATUS	Zeichenfolge
Akku wird geladen	BATTERY_CHARGING Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
BES-Gerät ist MSP bekannt	BES_DEVICE_KNOWN_BY_ZMSP Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
BES-PIN	BES_PIN	Zeichenfolge
Agent-ID für BES-Server	ENROLLMENT_AGENT_ID	Zeichenfolge
BES-Servername	BES_SERVER	Zeichenfolge
BES-Serverversion	BES_VERSION	Zeichenfolge
BitLocker-Status	WINDOWS_HAS_BIT_LOCKER_STATUS	Zeichenfolge
Bluetooth MAC-Adresse	BLUETOOTH_MAC	Zeichenfolge
Boot Debugging Enabled?	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED	Zeichenfolge
Boot Manager Rev List Version	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION	Zeichenfolge
CPU-Taktfrequenz	CPU_CLOCK_SPEED	Ganzzahl
CPU-Typ	CPU_TYPE	Zeichenfolge

Version der Netzbetreibereinstellungen	CARRIER_SETTINGS_VERSION	Zeichenfolge
Mobilnetzbreitengrad	GPS_LATITUDE_FROM_CELLULAR	Zeichenfolge
Mobilnetzlängengrad	GPS_LONGITUDE_FROM_CELLULAR	Zeichenfolge
Cellular-Technologie	CELLULAR_TECHNOLOGY	Ganzzahl
Mobilnetzzeitstempel	GPS_TIMESTAMP_FROM_CELLULAR	Datum
Kennwort bei nächster Anmeldung ändern?	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN	Zeichenfolge
Clienteräte-ID	CLIENT_DEVICE_ID	Zeichenfolge
Cloudbackup aktiviert	CLOUD_BACKUP_ENABLED Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
Code Integrity Enabled?	WINDOWS_HAS_CODE_INTEGRITY_ENABLED	Zeichenfolge
Code Integrity Rev List Version	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION	Zeichenfolge
Farbe	COLOR	Zeichenfolge
Erstellungszeit	GOOGLE_AW_DIRECTORY_CREATION_TIME	Zeichenfolge
Aktuelles Betreibernetzwerk	CURRENT_CARRIER_NETWORK	Zeichenfolge
Aktueller Ländercode für mobiles Gerät	CURRENT_MCC	Ganzzahl
Code für aktuelles mobiles Netzwerk	CURRENT_MNC	Zeichenfolge
DEP Policy	WINDOWS_HAS_DEP_POLICY	Zeichenfolge
Datenroaming zugelassen	DATA_ROAMING_ENABLED Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch

Datum des letzten iCloud-Backups	LAST_CLOUD_BACKUP_DATE	Datum
Beschreibung	DESCRIPTION	Zeichenfolge
Device Enrollment Program-Profil zugewiesen	PROFILE_ASSIGN_TIME	Datum
Pushbereitstellung von Device Enrollment Program-Profil	PROFILE_PUSH_TIME	Datum
Device Enrollment Program-Profil entfernt	PROFILE_REMOVE_TIME	Datum
Device Enrollment Program-Registrierung durch	DEVICE_ASSIGNED_BY	Zeichenfolge
Device Enrollment Program-Registrierungsdatum	DEVICE_ASSIGNED_DATE	Datum
Gerätetyp	DEVICE_TYPE	Zeichenfolge
Gerätemodell	MODEL_ID	Zeichenfolge
Gerätename	DEVICE_NAME	Zeichenfolge
'Nicht stören' aktiviert	DO_NOT_DISTURB Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
ELAM Driver Loaded?	WINDOWS_HAS_ELAM_DRIVER_LOADED	Zeichenfolge
ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE	Datum
Unternehmens-ID	ENTERPRISE_ID	Zeichenfolge
Externer Speicher 1: Verfügbarer Speicherplatz	EXTERNAL_STORAGE1_FREE_SPACE	Ganzzahl
Externer Speicher 1: Name	EXTERNAL_STORAGE1_NAME	Zeichenfolge

Externer Speicher 1: Gesamtspeicherplatz	EXTERNAL_STORAGE1_TOTAL_SPACE	Ganzzahl
Externer Speicher 2: Verfügbarer Speicherplatz	EXTERNAL_STORAGE2_FREE_SPACE	Ganzzahl
Externer Speicher 2: Name	EXTERNAL_STORAGE2_NAME	Zeichenfolge
Externer Speicher 2: Gesamtspeicherplatz	EXTERNAL_STORAGE2_TOTAL_SPACE	Ganzzahl
Externer Speicher verschlüsselt	EXTERNAL_ENCRYPTION Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
Firewallstatus	FIREWALL_STATUS	Zeichenfolge
Firmwareversion	FIRMWARE_VERSION	Zeichenfolge
Erste Synchronisierung	ZMSP_FIRST_SYNC	Datum
GPS-Höhe	GPS_ALTITUDE_FROM_GPS	Zeichenfolge
GPS-Breitengrad	GPS_LATITUDE_FROM_GPS	Zeichenfolge
GPS-Längengrad	GPS_LONGITUDE_FROM_GPS	Zeichenfolge
GPS-Zeitstempel	GPS_TIMESTAMP_FROM_GPS	Datum
Google Directory - Alias	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS	Zeichenfolge
Google Directory - Familienname	GOOGLE_AW_DIRECTORY_FAMILY_NAME	Zeichenfolge
Google Directory - Name	GOOGLE_AW_DIRECTORY_NAME	Zeichenfolge
Google Directory - primäre E-Mail	GOOGLE_AW_DIRECTORY_PRIMARY	Zeichenfolge
Google Directory - Benutzer-ID	GOOGLE_AW_DIRECTORY_USER_ID	Zeichenfolge
HAS_CONTAINER	HAS_CONTAINER Werte (Bedeutung):	Boolesch

	1 (Ja) 0 (Nein)	
HTC API-Version	HTC_MDM_VERSION	Zeichenfolge
HTC MDM API verfügbar	HTC_MDM Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
Hardwareverschlüsselung	HARDWARE_ENCRYPTION_CAPS	Ganzzahl
Hash des aktuell angemeldeten iTunes-Storekontos	ITUNES_STORE_ACCOUNT_HASH	Zeichenfolge
Netzbetreiber für Heimnetzwerk	SIM_CARRIER_NETWORK	Zeichenfolge
Heimatländercode für mobiles Gerät	SIM_MCC	Ganzzahl
Code für mobiles Heimnetzwerk	SIM_MNC	Zeichenfolge
ICCID	ICCID	Zeichenfolge
IMEI/MEID-Nummer	IMEI	Zeichenfolge
IMSI	IMSI	Zeichenfolge
IP-Standort	IP_LOCATION	Zeichenfolge
Identität	AS_DEVICE_IDENTITY	Zeichenfolge
Interner Speicher verschlüsselt	LOCAL_ENCRYPTION Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Issued At	WINDOWS_HAS_ISSUED_AT	Zeichenfolge
Jailbreak/Rooting	ROOT_ACCESS Werte (Bedeutung):	Boolesch

	1 (Ja) 0 (Nein)	
Kernel Debugging Enabled?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED	Zeichenfolge
KIOSK-Modus	IS_KIOSK Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Letzte bekannte IP-Adresse	LAST_IP_ADDR	Zeichenfolge
Zeit der letzten Richtlinienaktualisierung	LAST_POLICY_UPDATE_TIME	Datum
Letzte Synchronisierung	ZMSP_LAST_SYNC	Datum
Ortungsdienst aktiviert	DEVICE_LOCATOR Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY	Zeichenfolge
MEID	MEID	Zeichenfolge
Postfachsetup	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP	Zeichenfolge
Hauptakku	MAIN_BATTERY_PERCENT	Ganzzahl
Mobiltelefonnummer	TEL_NUMBER	Zeichenfolge
Modell-ID	SYSTEM_OEM	Zeichenfolge
Netzwerkadaptertyp	NETWORK_ADAPTER_TYPE	Zeichenfolge
NitroDesk TouchDown installiert	TOUCHDOWN_FIND Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
NitroDesk TouchDown über MDM	TOUCHDOWN_LICENSED_VIA_MDM	Boolesch

lizenziert	Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	
Betriebssystembuild	SYSTEM_OS_BUILD	Zeichenfolge
Betriebssystemsprache (Gebietsschema)	SYSTEM_LANGUAGE	Zeichenfolge
Betriebssystemversion	SYSTEM_OS_VERSION	Zeichenfolge
Adresse der Organisation	ORGANIZATION_ADDRESS	Zeichenfolge
Geschäftliche E-Mail-Adresse	ORGANIZATION_EMAIL	Zeichenfolge
Organization Magic	ORGANIZATION_MAGIC	Zeichenfolge
Name der Organisation	ORGANIZATION_NAME	Zeichenfolge
Telefonnummer der Organisation	ORGANIZATION_PHONE	Zeichenfolge
Andere Version	OTHER	Zeichenfolge
Nicht richtlinientreu	OUT_OF_COMPLIANCE Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Besitz von	CORPORATE_OWNED Werte (Bedeutung): 1 (Unternehmen) 0 (BYOD)	Boolesch
PCR0	WINDOWS_HAS_PCR0	Zeichenfolge
PIN-Code für Geofence	PIN_CODE_FOR_GEO_FENCE	Zeichenfolge
Passcode richtlinientreu	PASSCODE_IS_COMPLIANT Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch

Passcode richtlinientreu gemäß Konfiguration	PASSCODE_IS_COMPLIANT_WITH_CFG Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
Passcode vorhanden	PASSCODE_PRESENT Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
Umkreisverletzung	GPS_PERIMETER_BREACH Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
Persönlicher Hotspot aktiviert	PERSONAL_HOTSPOT_ENABLED Werte (Bedeutung): 1 (Ja) 0 (Nein)	Boolesch
Plattform	SYSTEM_PLATFORM	Zeichenfolge
API-Level der Plattform	API_LEVEL	Ganzzahl
Richtlinienname	POLICY_NAME	Zeichenfolge
Primäre Telefonnummer	IDENTITY1_PHONENUMBER	Zeichenfolge
Primäre SIM, IMEI	IDENTITY1_IMEI	Zeichenfolge
Primäre SIM, IMSI	IDENTITY1_IMSI	Zeichenfolge
Primäre SIM, Roaming	IDENTITY1_ROAMING Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Produktname	PRODUCT_NAME	Zeichenfolge

Geräte-ID des Herausgebers	PUBLISHER_DEVICE_ID	Zeichenfolge
Reset Count	WINDOWS_HAS_RESET_COUNT	Zeichenfolge
Restart Count	WINDOWS_HAS_RESTART_COUNT	Zeichenfolge
SBCP Hash	WINDOWS_HAS_SBCP_HASH	Zeichenfolge
SMS-fähig	IS_SMS_CAPABLE Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Safe Mode aktiviert?	WINDOWS_HAS_SAFE_MODE	Zeichenfolge
Samsung KNOX API verfügbar	SAMSUNG_KNOX Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Samsung KNOX API-Version	SAMSUNG_KNOX_VERSION	Zeichenfolge
Samsung KNOX-Nachweis	SAMSUNG_KNOX_ATTESTED Werte (Bedeutung): 1 (bestanden) 0 (nicht bestanden)	Boolesch
Aktualisierungsdatum für Samsung KNOX-Nachweis	SAMSUNG_KNOX_ATT_UPDATED_TIME	Datum
Samsung SAFE API verfügbar	SAMSUNG_MDM Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Samsung SAFE API-Version	SAMSUNG_MDM_VERSION	Zeichenfolge
Bildschirm: Auflösung X-Achse	SCREEN_XDPI	Ganzzahl (ppi)

Bildschirm: Auflösung Y-Achse	SCREEN_YDPI	Ganzzahl (ppi)
Bildschirm: Höhe	SCREEN_HEIGHT	Ganzzahl (Pixel)
Bildschirm: Anzahl der Farben	SCREEN_NB_COLORS	Ganzzahl
Bildschirm: Größe	SCREEN_SIZE	Dezimal (Zoll)
Bildschirm: Breite	SCREEN_WIDTH	Ganzzahl (Pixel)
Sekundäre Telefonnummer	IDENTITY2_PHONENUMBER	Zeichenfolge
Sekundäre SIM, IMEI	IDENTITY2_IMEI	Zeichenfolge
Sekundäre SIM, IMSI	IDENTITY2_IMSI	Zeichenfolge
Sekundäre SIM, Roaming	IDENTITY2_ROAMING Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Secure Boot aktiviert?	WINDOWS_HAS_SECURE_BOOT_ENABLED	Zeichenfolge
SecureContainer aktiviert	WINDOWS_HAS_BIT_LOCKER_STATUS	Zeichenfolge
Seriennummer	SERIAL_NUMBER	Zeichenfolge
Sony Enterprise API verfügbar	SONY_MDM Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Sony Enterprise API-Version	SONY_MDM_VERSION	Zeichenfolge
betreuten	betreuten Werte (Bedeutung): 1 (Ja)	Boolesch

	0 (Nein)	
Grund für vorübergehende Sperrung	GOOGLE_AW_DIRECTORY_SUSPENTION_REASON	Zeichenfolge
Manipulierter Status	TAMPERED_STATUS	Zeichenfolge
AGB	TERMS_AND_CONDITIONS	Zeichenfolge
Nutzungsbedingungen und Vereinbarung angenommen?	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS	Zeichenfolge
Testsignierung aktiviert?	WINDOWS_HAS_TEST_SIGNING_ENABLED	Zeichenfolge
Gesamt-RAM	MEMORY	Ganzzahl
Speicherplatz gesamt	FREEDISK	Ganzzahl
UDID	UDID	Zeichenfolge
Benutzeragent	USER_AGENT	Zeichenfolge
Benutzerdefiniert 1	USER_DEFINED_1	Zeichenfolge
Benutzerdefiniert 2	USER_DEFINED_2	Zeichenfolge
Benutzerdefiniert 3	USER_DEFINED_3	Zeichenfolge
Benutzersprache (Gebietsschema)	USER_LANGUAGE	Zeichenfolge
VSM aktiviert?	WINDOWS_HAS_VSM_ENABLED	Zeichenfolge
Anbieter	VENDOR	Zeichenfolge
Sprachfähig	IS_VOICE_CAPABLE Werte (Bedeutung): 1 (Wahr) 0 (Falsch)	Boolesch
Sprachroaming zugelassen	VOICE_ROAMING_ENABLED Werte (Bedeutung): 1 (Ja)	Boolesch

	0 (Nein)	
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY	Zeichenfolge
WNS-Benachrichtigungsstatus	WNS_PUSH_STATUS	Zeichenfolge
URL für WNS-Benachrichtigung	PROPERTY_WNS_PUSH_URL	Zeichenfolge
Ablaufdatum der URL für WNS-Benachrichtigung	PROPERTY_WNS_PUSH_URL_EXPIRY	Zeichenfolge
WiFi MAC-Adresse	WIFI_MAC	Zeichenfolge
WinPE Enabled?	WINDOWS_HAS_WINPE	Zeichenfolge
XenMobile-Agent-ID	AGENT_ID	Zeichenfolge
XenMobile-Agentrevision	EW_REVISION	Zeichenfolge
XenMobile-Agentversion	EW_VERSION	Zeichenfolge

Sperren von iOS-Geräten

Apr 24, 2017

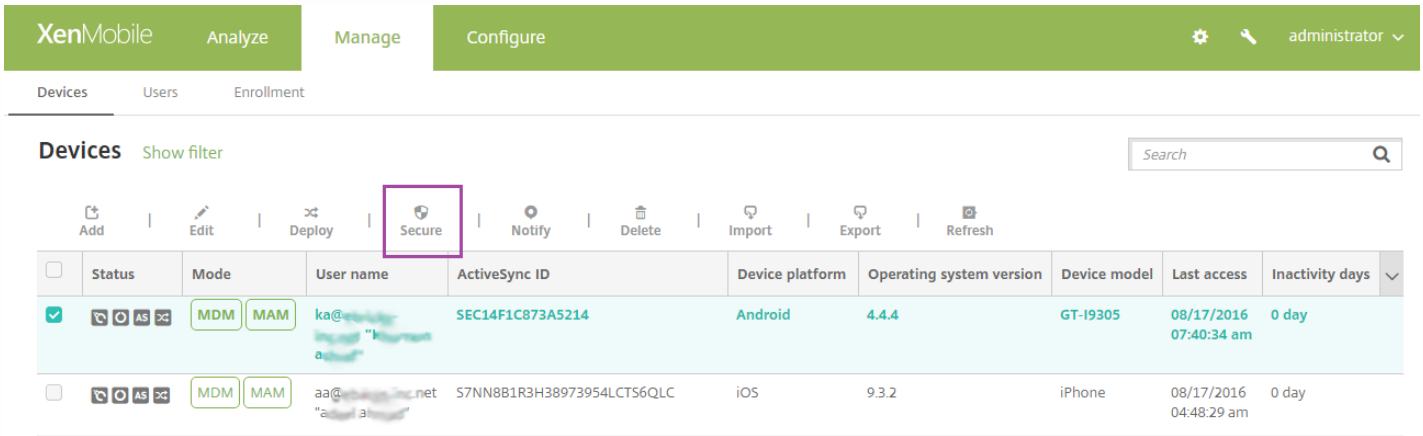
Sie können ein verlorenes iOS-Gerät sperren und eine entsprechende Nachricht und Telefonnummer auf dem Sperrbildschirm anzeigen lassen. Dieses Feature wird für iOS 7-Geräte und höher unterstützt.

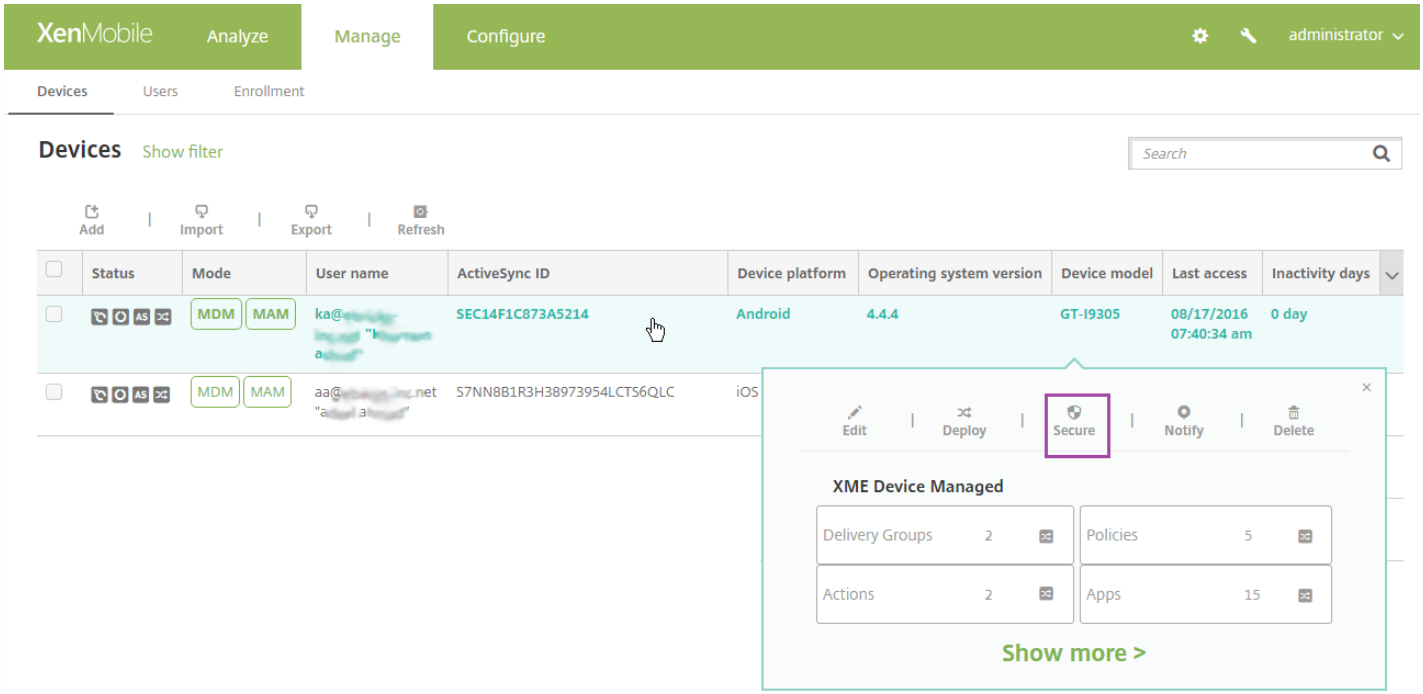
Damit eine Nachricht und Telefonnummer auf einem gesperrten Gerät angezeigt wird, muss die Richtlinie Passcode in der XenMobile-Konsole auf "true" festgelegt werden. Alternativ können Benutzer den Passcode auf dem Gerät auch manuell aktivieren.

1. Klicken Sie in der XenMobile-Konsole auf **Verwalten > Geräte**. Die Seite **Gerätename** wird angezeigt.

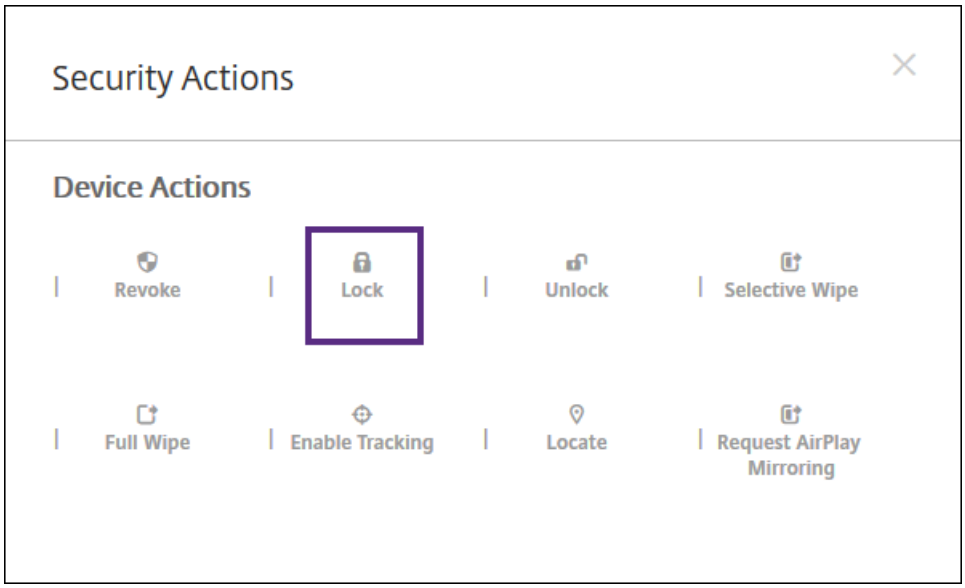
2. Wählen Sie das iOS-Gerät aus, das Sie sperren möchten.

Wenn Sie das Kontrollkästchen neben einem Gerät aktivieren, wird das Menü mit den Optionen oberhalb der Liste angezeigt. Wenn Sie auf ein Element in der Liste klicken, wird das Menü mit den Optionen rechts daneben angezeigt.

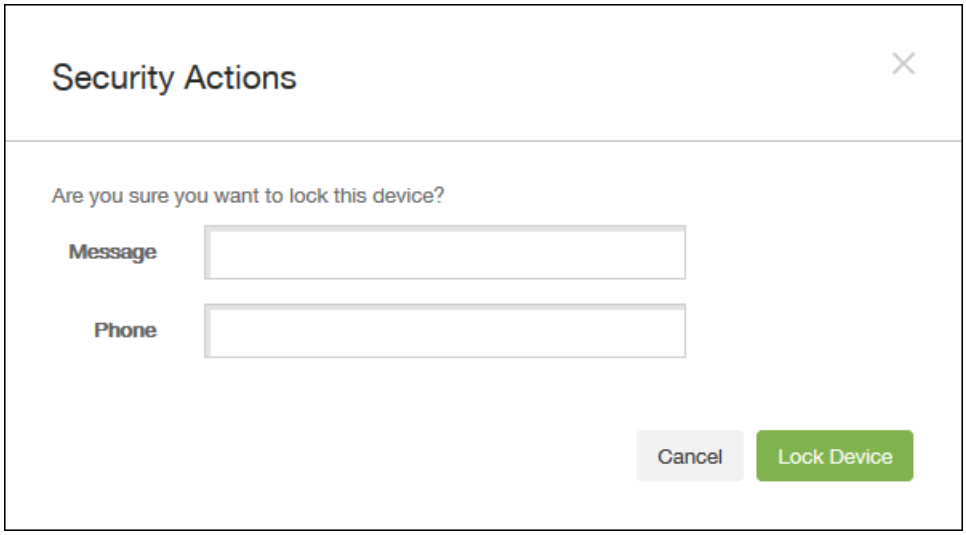




3. Wählen Sie im Menü "Optionen" die Option **Sicherung**. Das Dialogfeld **Sicherheitsaktionen** wird angezeigt.



4. Klicken Sie auf **Sperren**. Das Bestätigungsdialogfeld **Sicherheitsaktionen** wird angezeigt.



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

iPads ab iOS 7: iOS hängt die Wörter "Lost iPad" an alles an, was Sie im Feld **Nachricht** eingeben. iPhones ab iOS 7: Wenn Sie das Feld **Nachricht** leer lassen und eine Telefonnummer angeben, wird die Meldung "Besitzer anrufen" auf dem Sperrbildschirm des Geräts angezeigt.

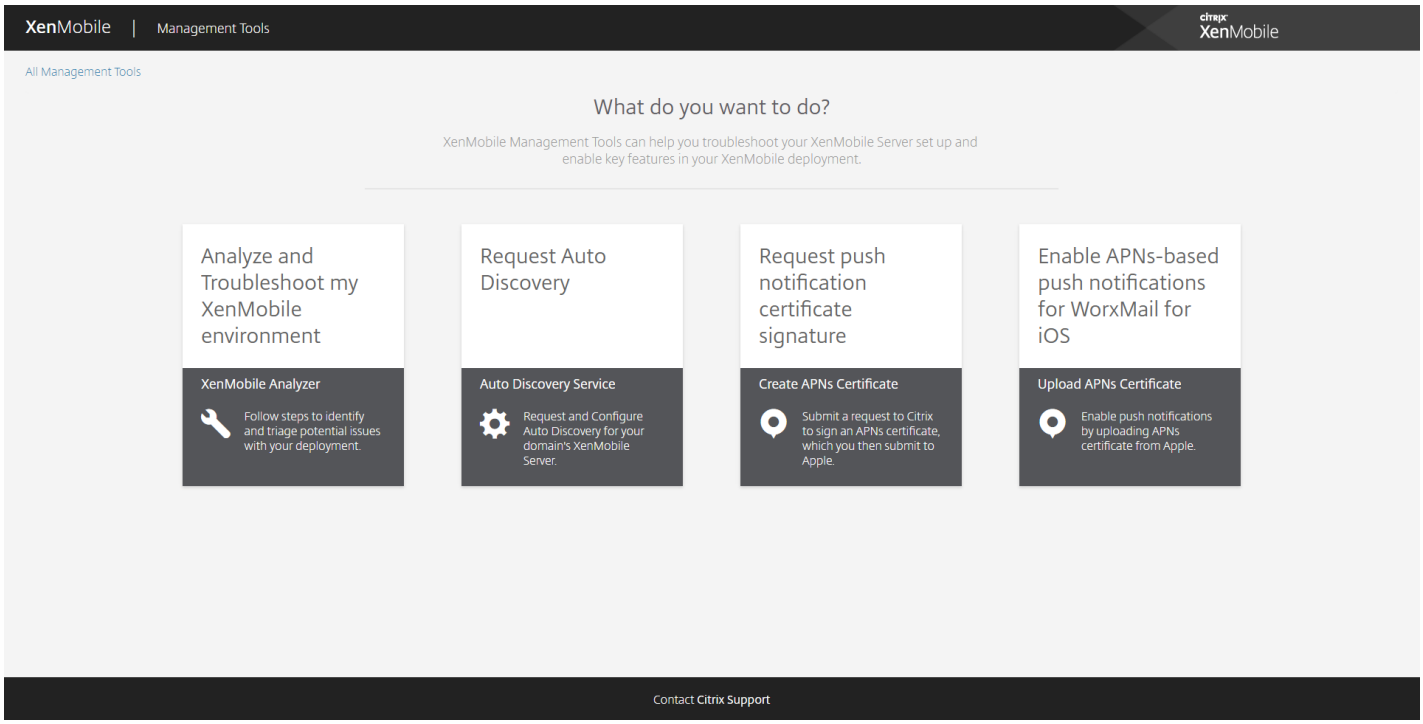
6. Klicken Sie auf **Gerät sperren**.

XenMobile Autodiscovery-Dienst

Feb 24, 2017

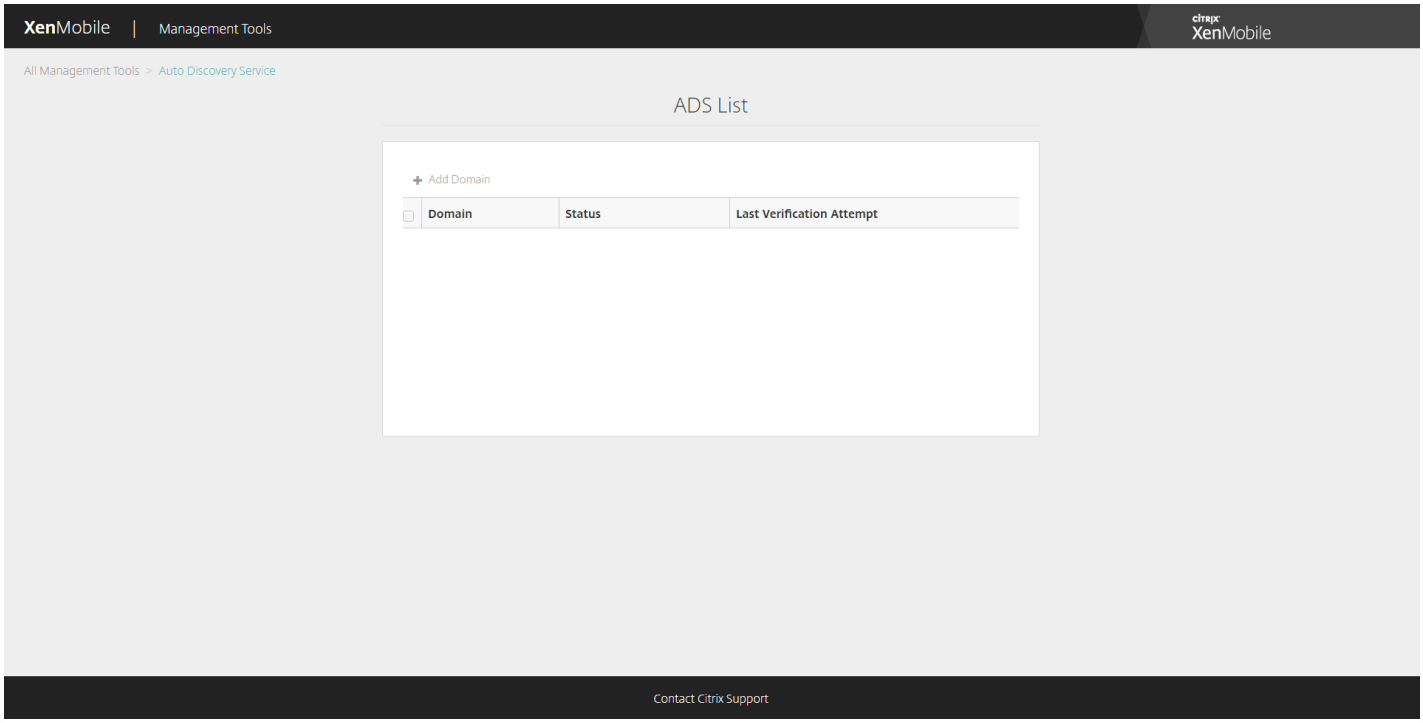
Autodiscovery ist ein wichtiger Teil vieler XenMobile-Bereitstellungen. Autodiscovery vereinfacht den Registrierungsvorgang für Benutzer. Diese können bei der Geräteregistrierung dann ihren Netzwerkbenutzernamen und ihr Active Directory-Kennwort verwenden, statt Angaben zum XenMobile-Server eingeben 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**.

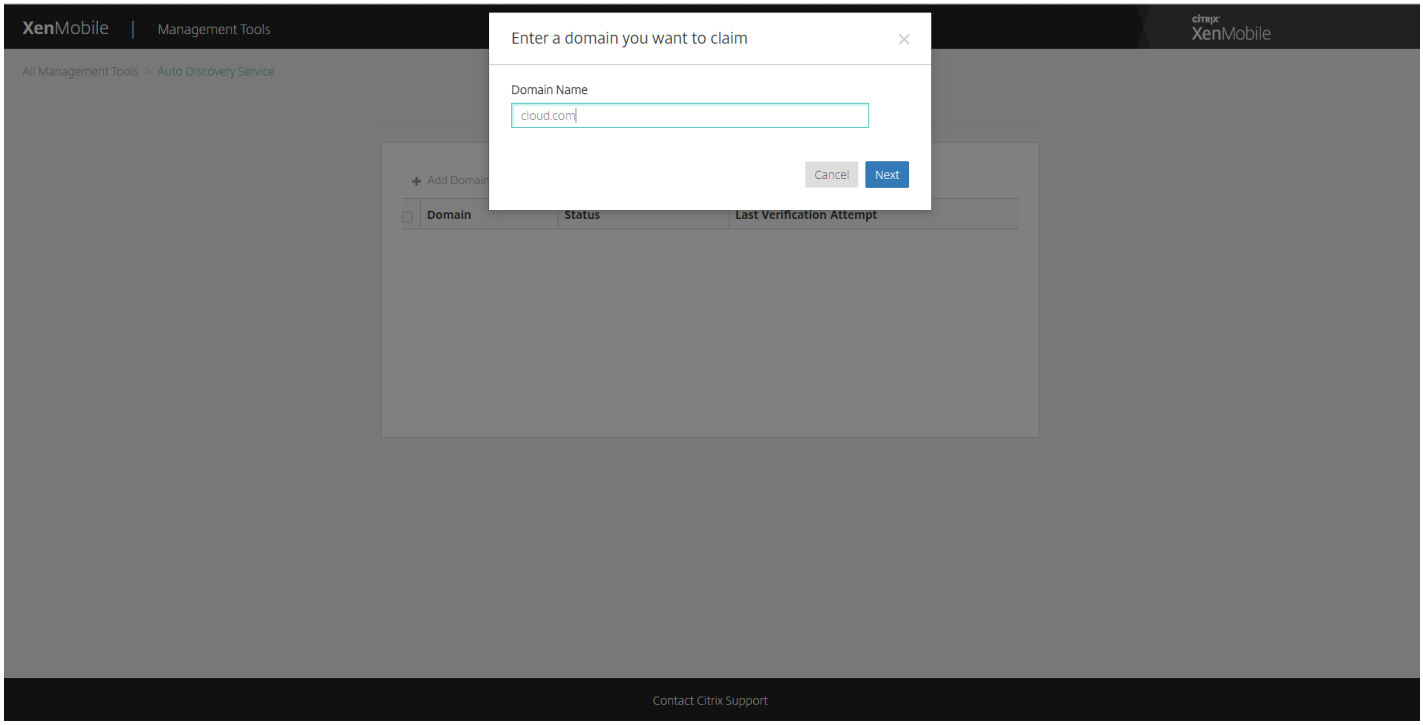


Anfordern von Autodiscovery

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.

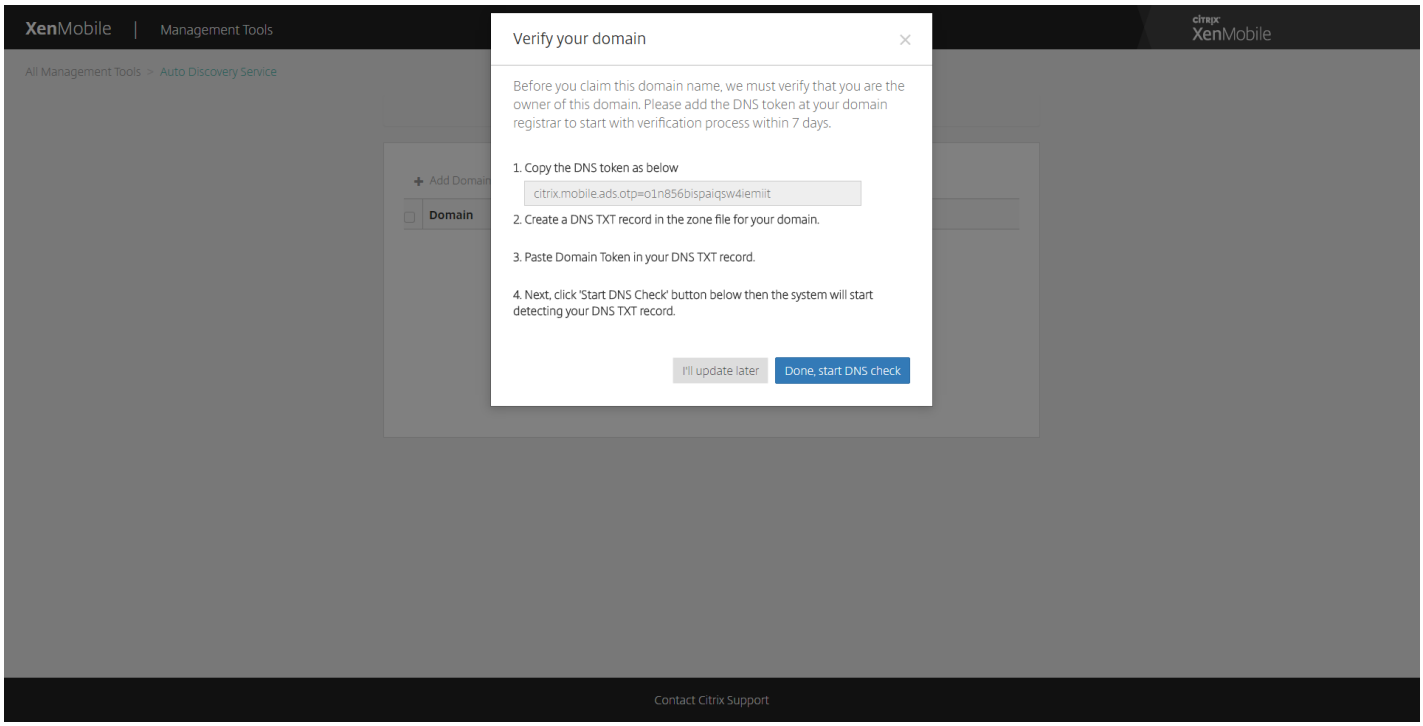
Zum Erstellen eines DNS-TXT-Datensatzes müssen Sie sich bei dem Portal des Hosting-Anbieters der Domäne anmelden, die Sie in Schritt 2 oben hinzugefügt haben. Über das Domänenhostingportal können Sie die Domänennamenserver-Datensätze bearbeiten und einen benutzerdefinierten TXT-Datensatz hinzufügen. 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".

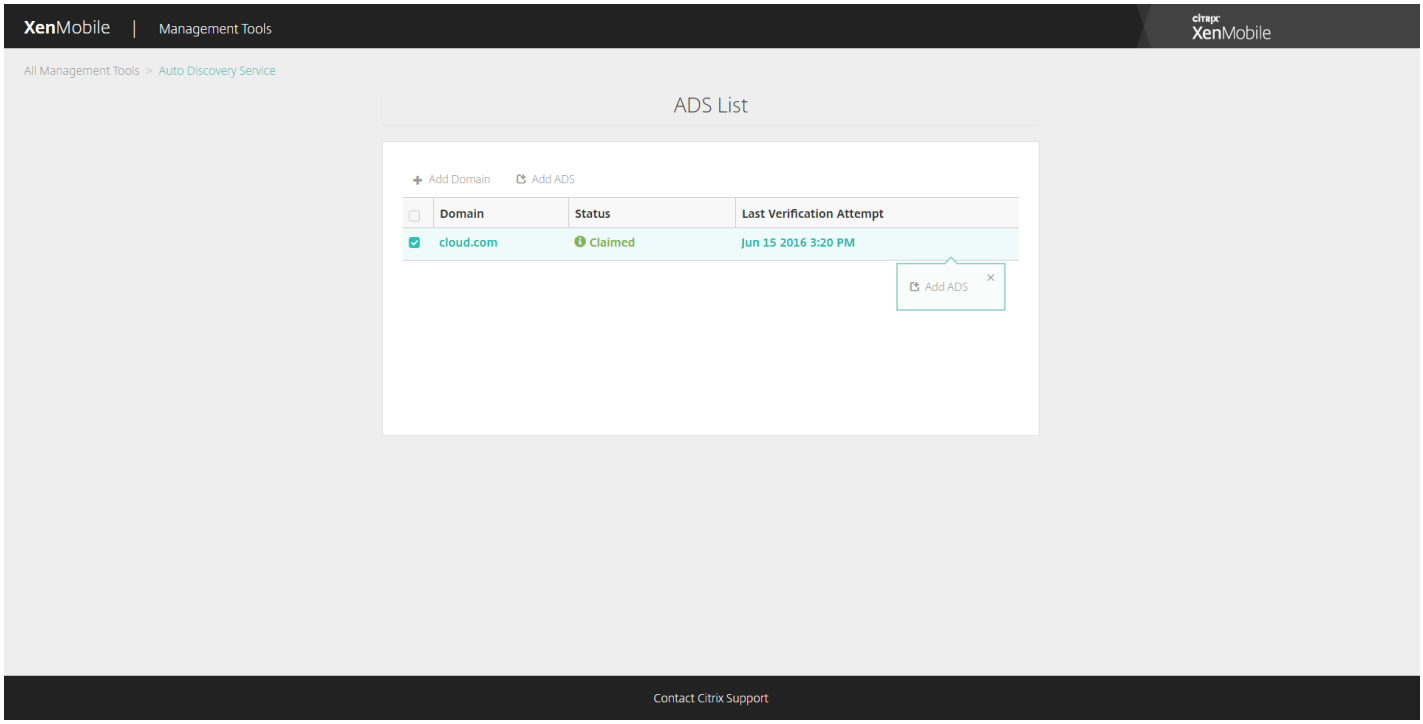
Das System erkennt den DNS-TXT-Datensatz. Alternativ können Sie auf "I'll update later" klicken. Die Aufzeichnung wird dann gespeichert. Die DNS-Prüfung wird erst gestartet, wenn Sie auf den Datensatz mit dem Status "Waiting" und dann auf "DNS Check" klicken.

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.

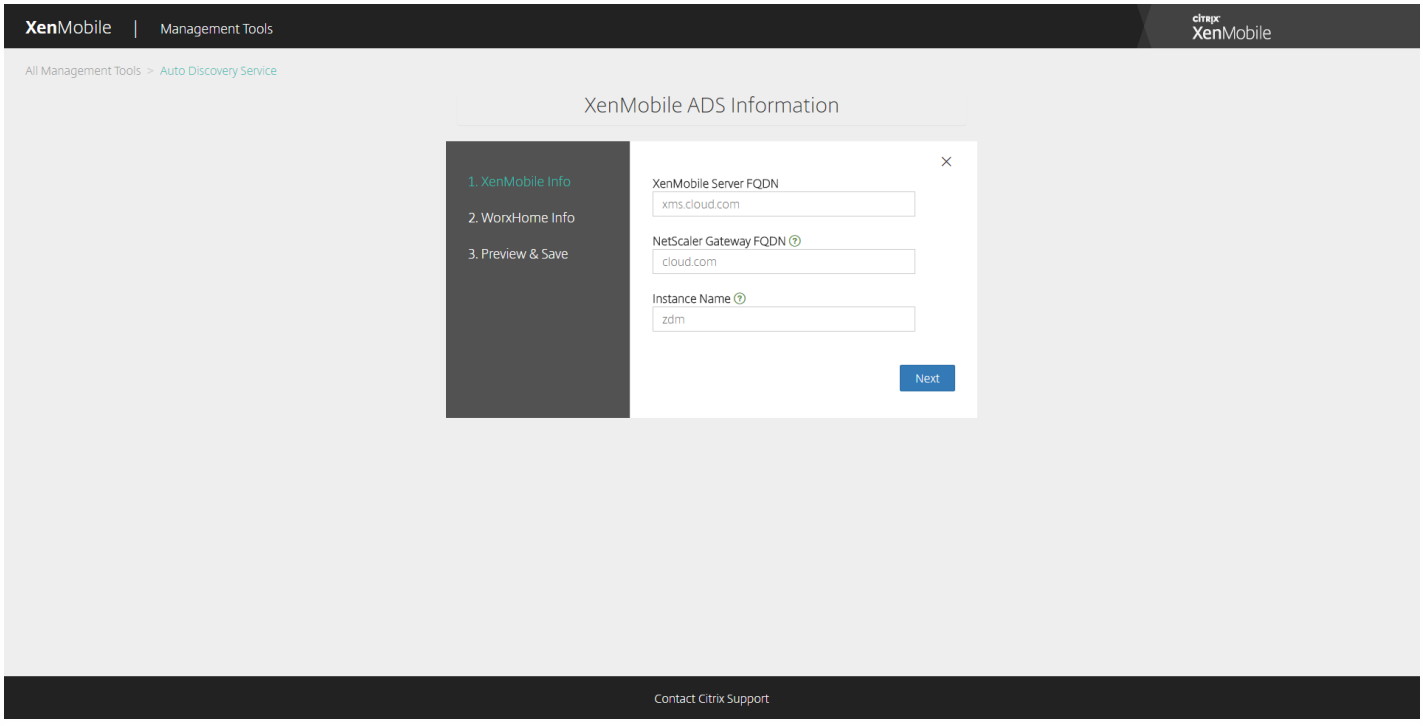


4. Nachdem Sie Ihre Domäne beansprucht haben, geben Sie Autodiscovery-Dienstinformationen ein. Klicken Sie mit der rechten Maustaste auf den Domänendatensatz, für den Sie Autodiscovery anfordern, und klicken Sie auf **Add ADS**.

Wenn Ihre Domäne bereits einen Autodiscovery-Datensatz hat, öffnen Sie einen Fall beim Citrix Support, um diesen nach Bedarf zu ändern.



5. Machen Sie Eingaben für **XenMobile Server FQDN**, **NetScaler Gateway FQDN** und **Instance Name** und klicken Sie auf **Next**. Wenn Sie nicht sicher sind, fügen Sie eine Standardinstanz "zdm" hinzu.



Zu dem Screenshot oben muss erwähnt werden, dass Worx Home jetzt Secure Hub heißt.

6. Geben Sie die folgenden Informationen für Secure Hub ein und klicken Sie dann auf **Next**.

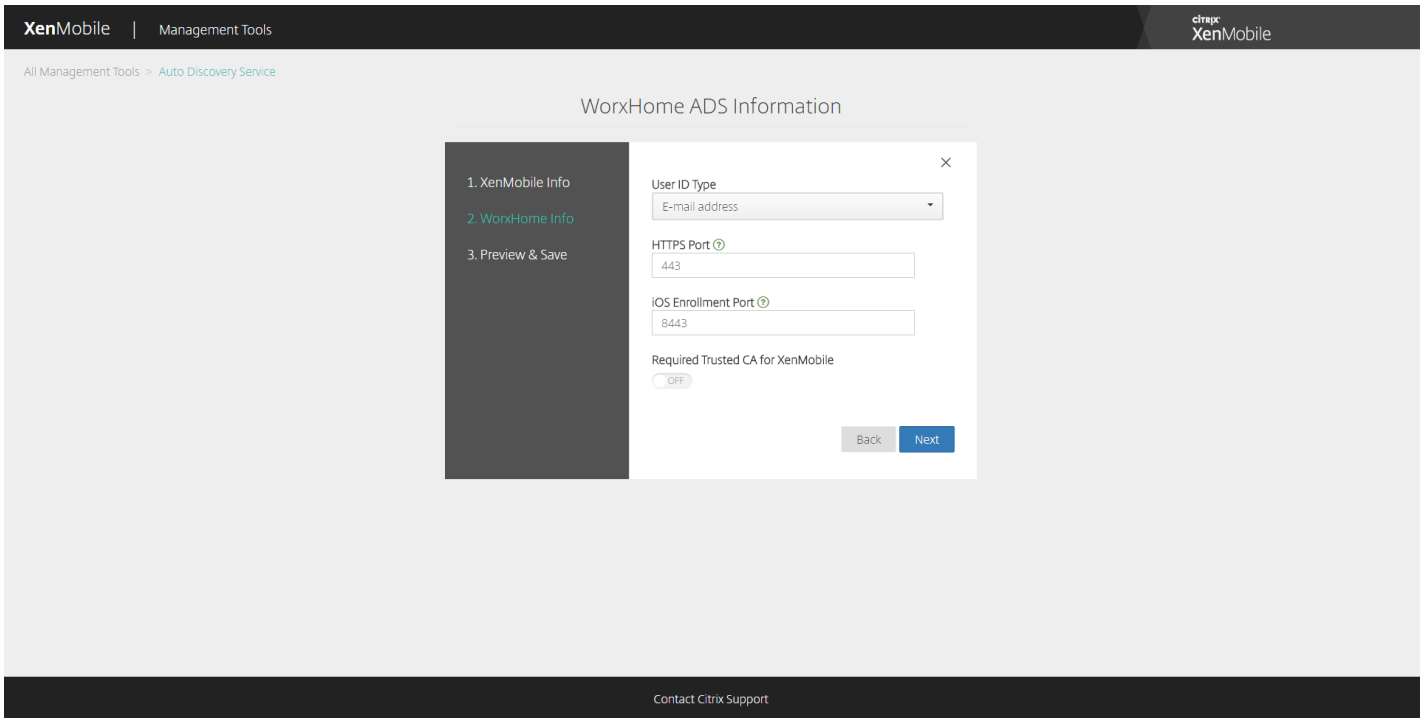
a. **User ID Type**: Wählen Sie für den ID-Typ, mit dem Benutzer sich anmelden, **E-mail address** oder **UPN** aus.

UPN wird verwendet, wenn der UPN (Benutzerprinzipalname) 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 address** 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 Secure Hub über HTTPS zugegriffen werden soll. Normalerweise ist dies Port 443.

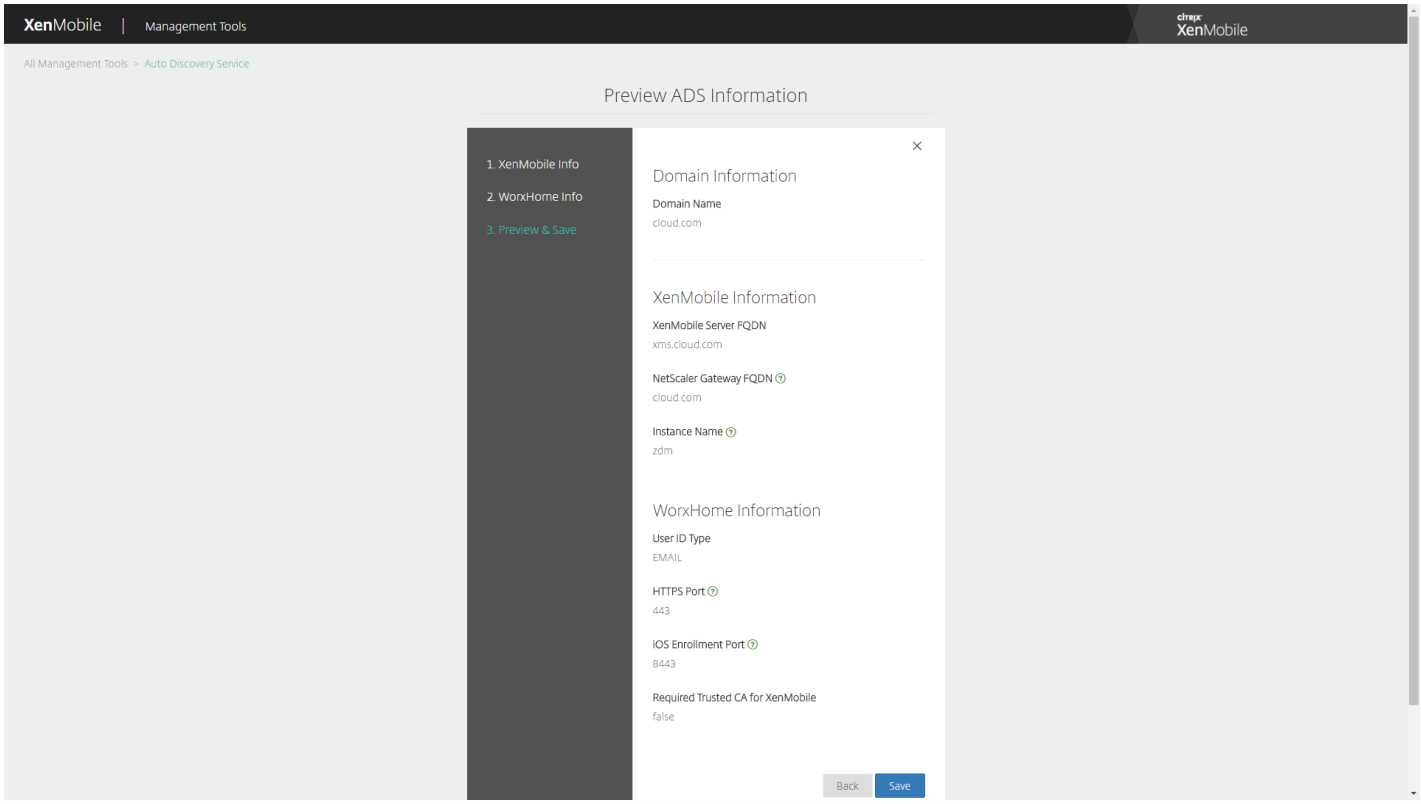
c. **iOS Enrollment Port**: Geben Sie den Port an, über den auf Secure Hub für die iOS-Registrierung zugegriffen werden soll. Normalerweise ist dies Port 8443.

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 im zugehörigen Abschnitt des Artikels Secure Hub der Dokumentation zu den XenMobile-Apps. Informationen zu den für das Zertifikatpinning erforderlichen Ports finden Sie im Support-Artikel XenMobile Port Requirements for ADS Connectivity.



Zu dem Screenshot oben muss erwähnt werden, dass Worx Home jetzt Secure Hub heißt.

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**.



Zu dem Screenshot oben muss erwähnt werden, dass Worx Home jetzt Secure Hub heißt.

Aktivieren von Autodiscovery

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.

Zum Aktivieren von Autodiscovery können Sie das Autodiscovery-Dienstportal unter https://xenmobiletools.citrix.com aufrufen.

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.)

Registrieren von Geräten

Apr 24, 2017

Für die sichere Remoteverwaltung von Benutzergeräten werden diese bei XenMobile registriert. Die XenMobile-Clientsoftware wird auf dem Benutzergerät installiert und die Identität des Benutzers wird authentifiziert. Anschließend werden XenMobile und das Benutzerprofil installiert. In der XenMobile-Konsole können Sie dann Geräteverwaltungsaufgaben durchführen. Sie können Richtlinien anwenden, Apps bereitstellen, Daten per Push auf das Gerät verschieben und verlorene oder gestohlene Geräte sperren, löschen und suchen.

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

Zum Aktualisieren der Konfigurationsoptionen für Benutzer und Geräte verwenden Sie die Seite **Verwalten > Registrierung**. Weitere Informationen finden Sie unter Senden einer Registrierungseinladung in diesem Artikel.

Android-Geräte

1. Rufen Sie auf dem Android-Gerät Google Play auf, laden Sie die Citrix Secure Hub-App herunter und tippen Sie dann auf die App.
2. Wenn Sie zum Installieren der App aufgefordert werden, klicken Sie auf **Weiter** und dann auf **Installieren**.
3. Wenn Secure Hub installiert ist, 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 Citrix PIN zur Anmeldung bei Secure Hub und anderen XenMobile-aktivierten Apps (Secure Mail, Secure Web, ShareFile usw.) einrichten. Sie müssen die Citrix PIN zweimal eingeben. Geben Sie im Bildschirm **Citrix PIN erstellen** eine PIN ein.
8. Geben Sie die PIN erneut ein. Secure Hub wird geöffnet. Sie können nun auf den XenMobile 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. Darüber hinaus werden Richtlinien, die Sie in XenMobile konfigurieren, auf dem Gerät bereitgestellt. Tippen Sie auf **Installieren**, um die Apps zu installieren.

Aufheben der Registrierung eines Android-Geräts auf und erneute Registrierung

Benutzer können über Secure Hub die Registrierung aufheben. Wenn Benutzer die Registrierung mit dem folgenden Verfahren aufheben, wird das Gerät weiterhin im Gerätebestand der XenMobile-Konsole angezeigt. Sie können auf dem Gerät jedoch keine Aktionen ausführen. Sie können das Gerät nicht verfolgen und Sie können die Gerätekonformität nicht überwachen.

1. Öffnen Sie die Secure Hub-App.

2. Abhängig davon, ob Sie ein Smartphone oder ein Tablet haben, führen Sie folgende Schritte aus:

Auf einem Smartphone:

a. Streichen Sie von der linken Seite des Bildschirms, um den Bereich "Einstellungen" zu öffnen.

b. Tippen Sie auf **Einstellungen**, **Konten** und dann auf **Konto löschen**.

Auf einem Tablet:

a. Tippen Sie auf den Pfeil neben Ihrer E-Mail-Adresse in der oberen rechten Ecke.

b. Tippen Sie auf **Einstellungen**, **Konten** und dann auf **Konto löschen**.

3. Tippen Sie auf **Erneut registrieren**. Eine Meldung wird angezeigt, um zu bestätigen, dass Sie das Gerät erneut registrieren möchten.

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.

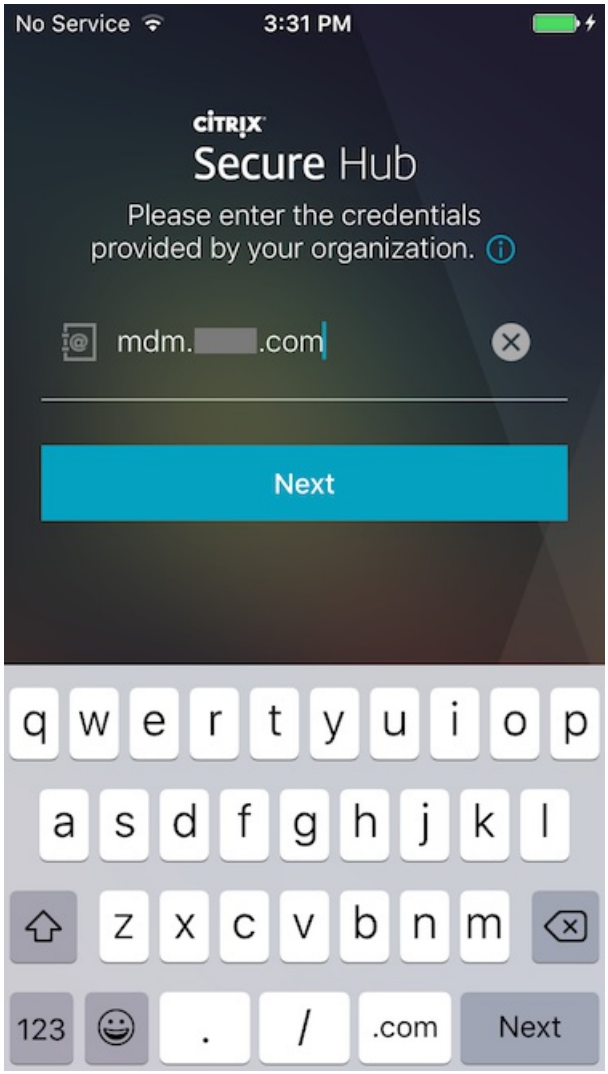
iOS-Geräte

1. Laden Sie die Secure Hub-App aus dem Apple iTunes-App Store auf das Gerät herunter und installieren Sie sie auf dem Gerät.

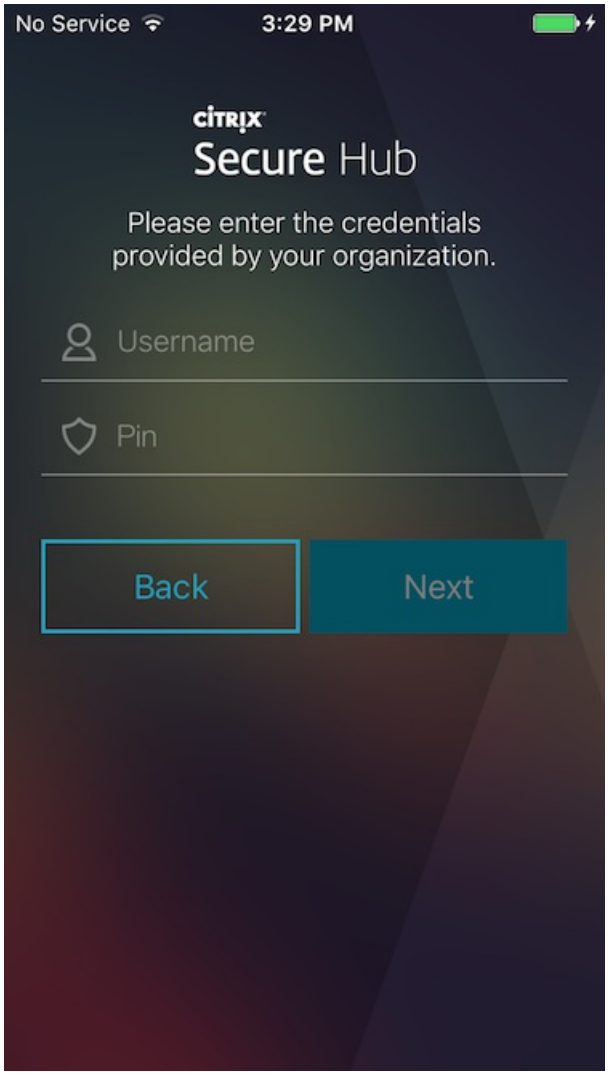
2. Tippen Sie auf dem Homebildschirm des iOS-Geräts auf die Secure Hub-App.

3. Wenn die Secure Hub-App geöffnet wird, geben Sie die vom Helpdesk erhaltene Serveradresse ein.

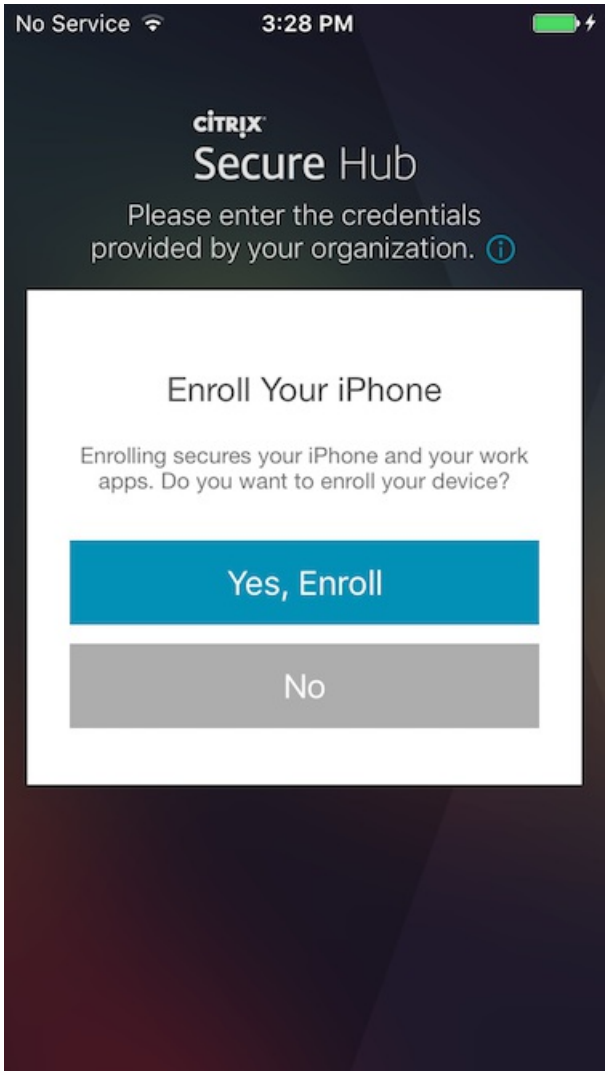
(Die angezeigten Seiten unterscheiden sich je nach XenMobile-Konfiguration u. U. von den folgenden Beispielen.)

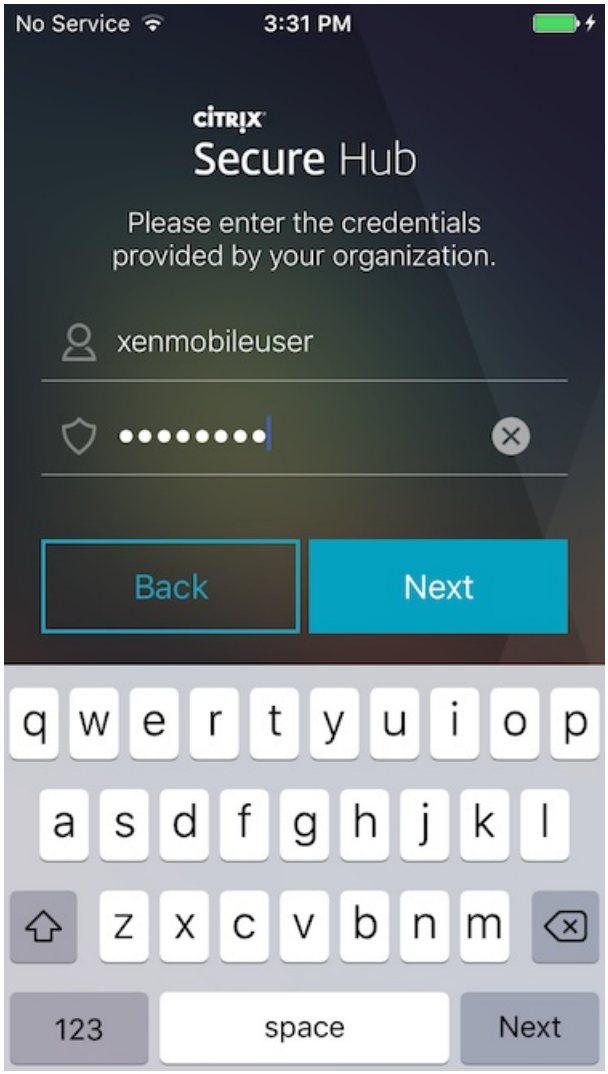


4. Geben Sie Ihren Benutzernamen und das Kennwort oder die PIN ein, wenn Sie dazu aufgefordert werden. Klicken Sie auf **Weiter**.



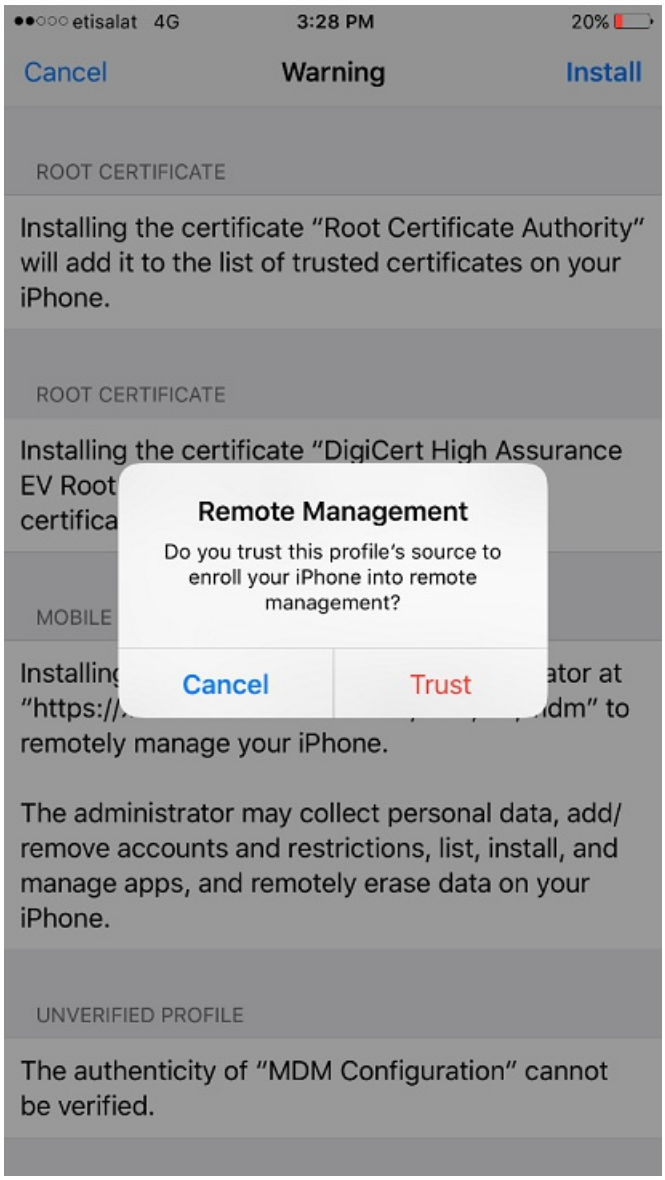
5. Wenn Sie zur Registrierung aufgefordert werden, klicken Sie auf **Ja, registrieren** und geben Sie Ihre Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden.



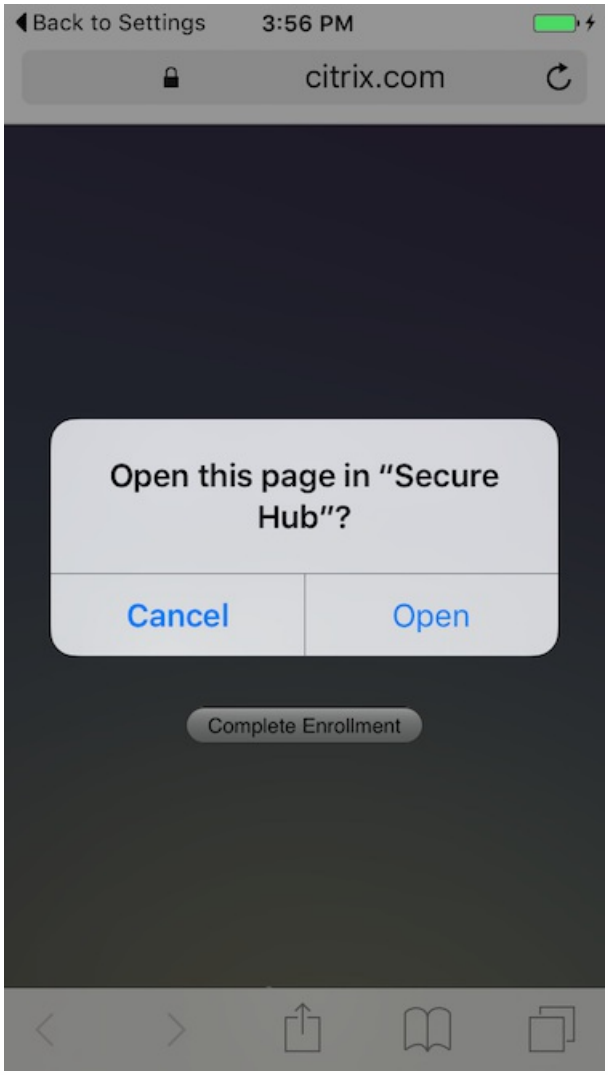


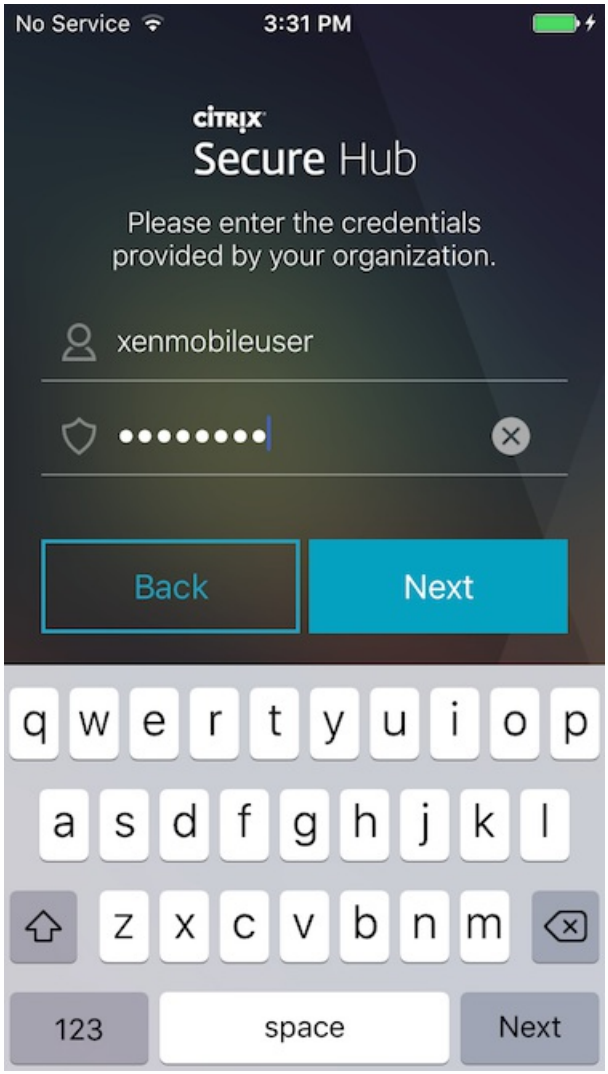
6. Tippen Sie auf **Installieren**, um den Citrix Profildienst zu installieren.

7. Tippen Sie auf **Vertrauensstellung**.



8. Tippen Sie auf **Öffnen** und geben Sie Ihre Anmeldeinformationen ein.





Mac OS X- und macOS-Geräte

Sie können Mac-Geräte, auf denen OS X oder macOS ausgeführt wird, nur in XenMobile für MDM registrieren. Mac-Benutzer führen die Registrierung per Funk direkt über das Gerät aus.

Für die Registrierung von Mac-Geräten gehen XenMobile-Administratoren wie folgt vor:

1. Richten Sie optional Mac-Geräterichtlinien in der XenMobile-Konsole ein. Weitere Informationen zu Geräterichtlinien finden Sie unter Geräterichtlinien. Der Abschnitt XenMobile-Geräterichtlinien nach Plattform enthält Informationen dazu, welche Geräterichtlinien Sie für Mac-Geräte konfigurieren können.

2. Senden Sie den Registrierungslink https://:8443/zdm/macos/otae an den Benutzer.

- serverFQDN der vollqualifizierte Domänenname (FQDN) des Servers, auf dem XenMobile ausgeführt wird.
- Port 8443 ist der sichere Standardport. Wenn Sie einen anderen Port konfiguriert haben, verwenden Sie diesen anstelle von 8443.
- "zdm" ist der Instanzname, der bei der Serverinstallation verwendet wird. Wenn Sie einen anderen Instanznamen konfiguriert haben, verwenden Sie stattdessen diesen Instanznamen.

Sie können den Link auch in einer E-Mail-Einladung senden. Weitere Einzelheiten finden Sie unter Senden von Registrierungseinladungen.

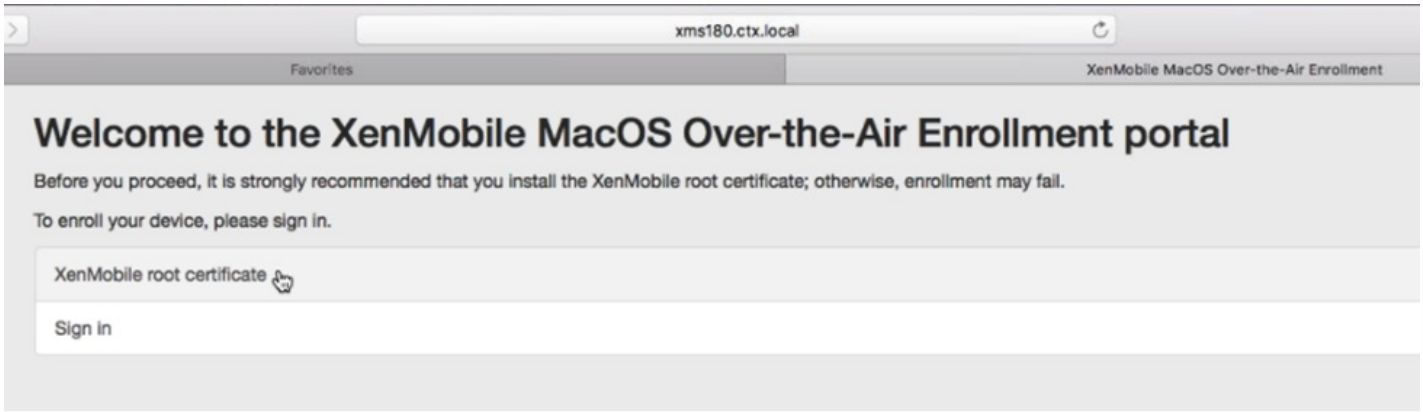
3. Die Benutzer installieren die benötigten Zertifikate. Wenn Sie ein öffentlich vertrauenswürdiges SSL-Zertifikat und ein öffentlich vertrauenswürdiges digitales Signaturzertifikat für iOS und macOS konfiguriert haben, wird den Benutzern die Aufforderung zum Installieren von Zertifikaten angezeigt. Weitere Informationen über Zertifikate finden Sie unter Zertifikate.

4. Für die Registrierung greifen Benutzer auf dem Mac-Gerät über Safari auf den Registrierungslink zu.

> **Hinweis:** Wenn Benutzer nicht auf den Link zugreifen können, sollten sie den Browserverlauf und den Cache löschen oder einen anderen Browser verwenden.

5. Benutzern werden diese Eingabeaufforderungen zur Installation von Zertifikaten standardmäßig angezeigt.

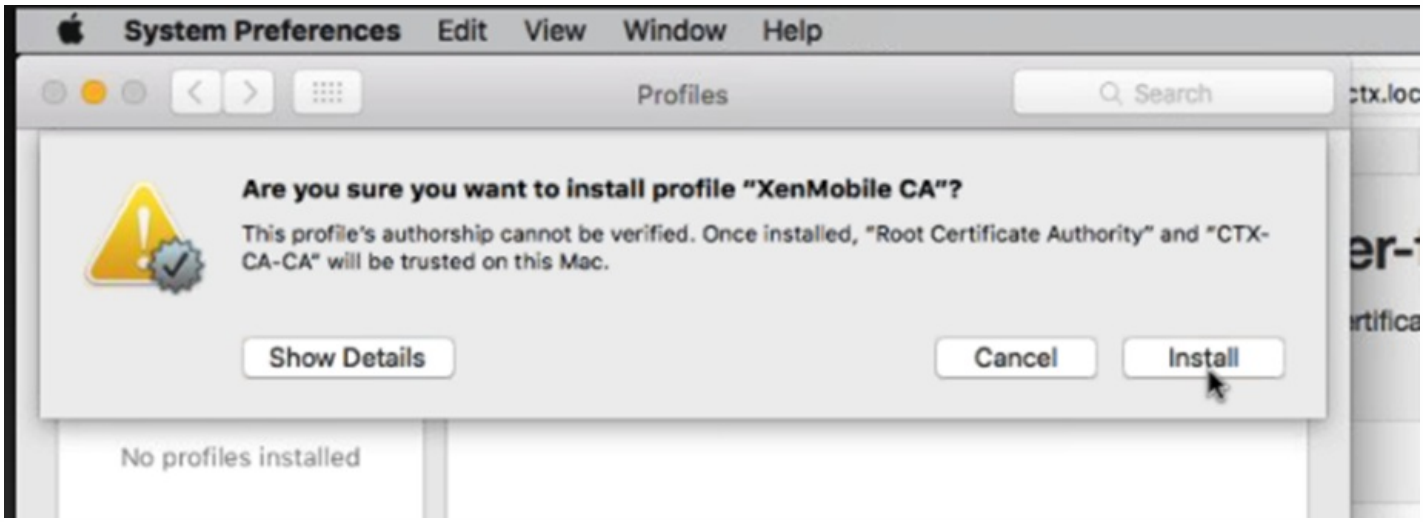
a. Benutzer klicken auf **XenMobile-Stammzertifikat**.



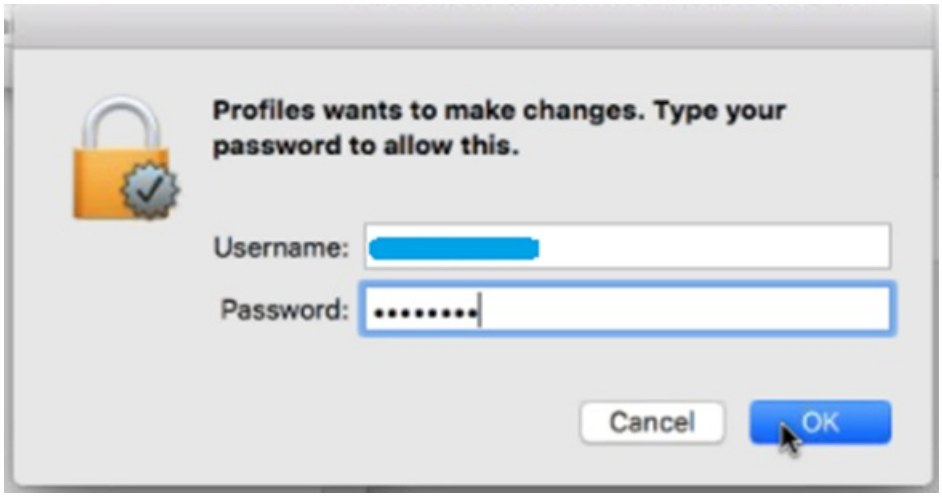
b. Benutzer klicken auf **Weiter**, um die Zertifikate zu installieren.

> **Hinweis:** Durch die Installation des Stammzertifikats der Zertifizierungsstelle des XenMobile-Servers wird ein vertrauenswürdiger Kommunikationskanal zwischen dem Gerät und XenMobile eingerichtet.

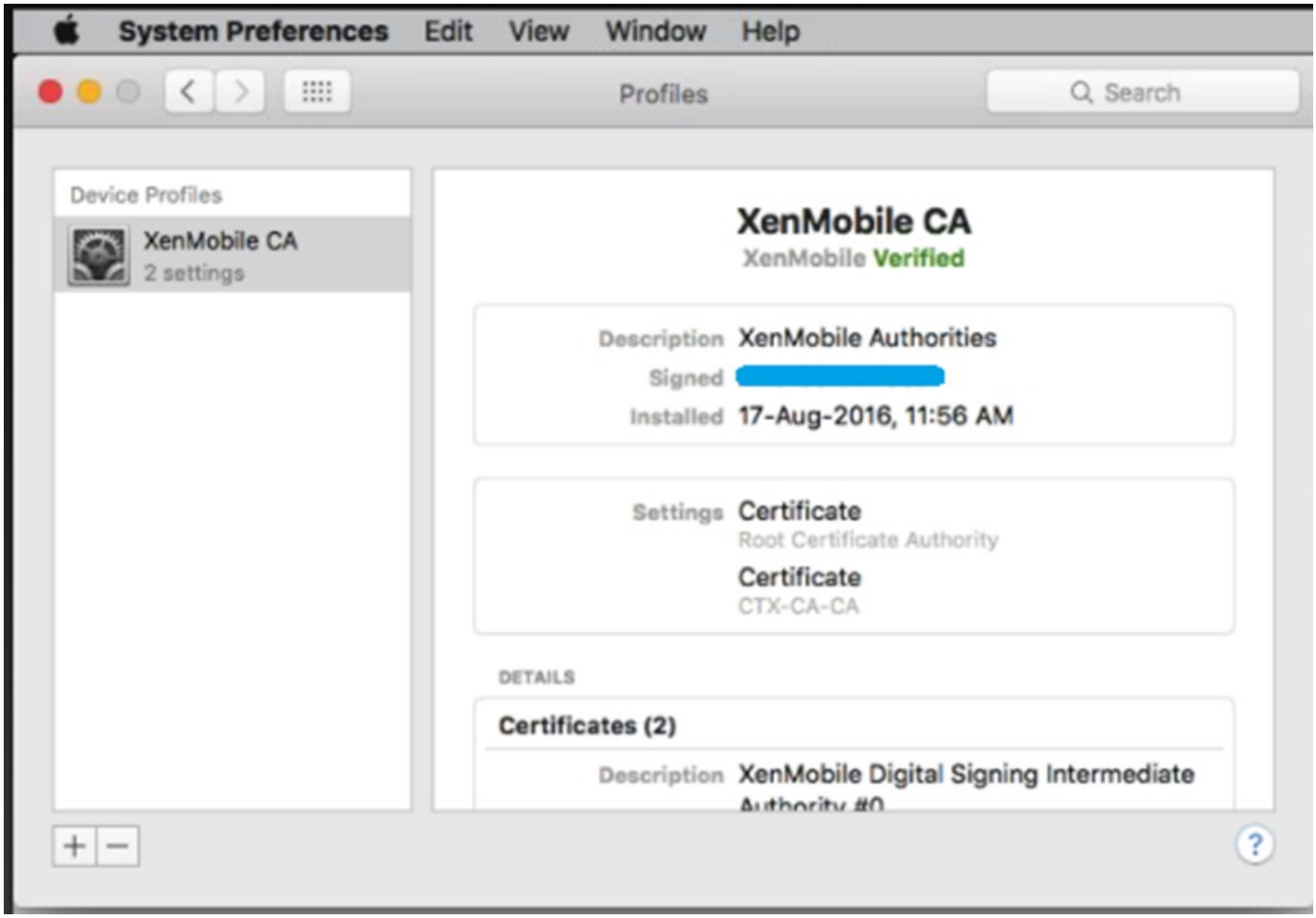
c. Benutzer klicken auf **Installieren**, um das XenMobile-Profil zu installieren.



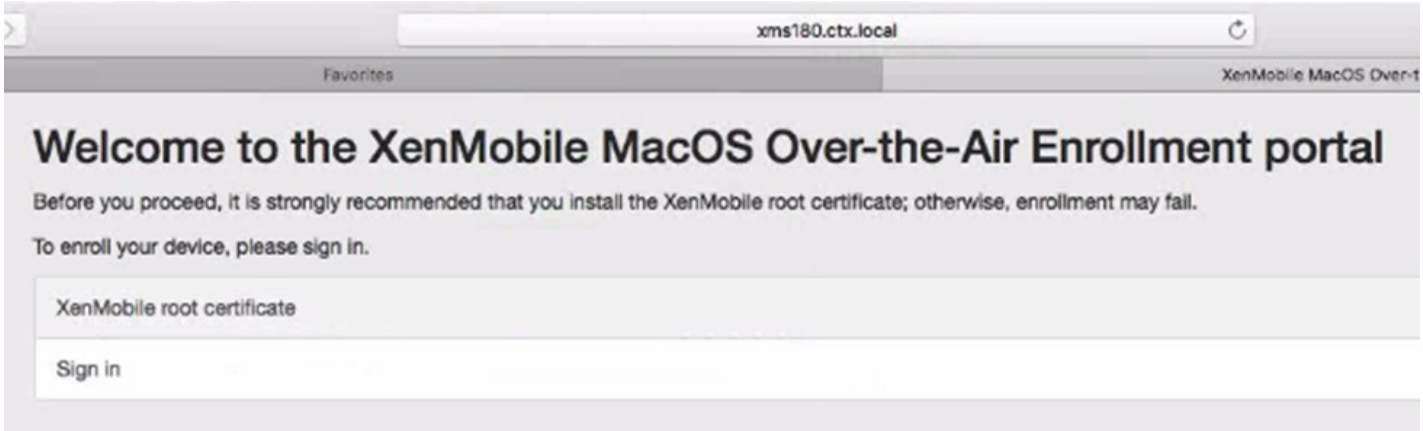
d. Benutzer geben bei Aufforderung die Anmeldeinformationen des Geräts ein.



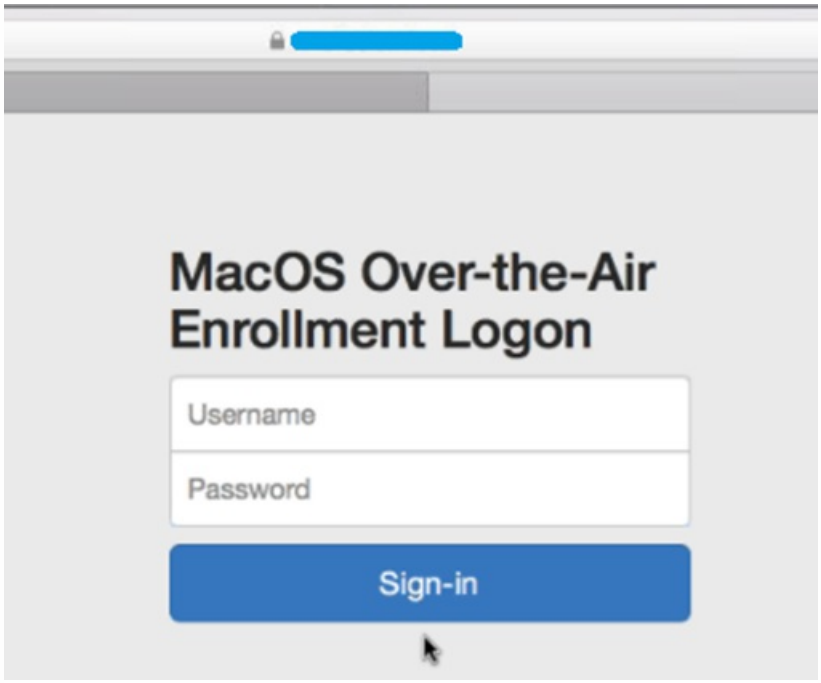
e. Dieser Bildschirm wird nach einer erfolgreichen Installation der XenMobile-Zertifikate unter **Profile** angezeigt. Benutzer schließen diesen Bildschirm, um die Geräteregistrierung fortzusetzen.



6. Im macOS-Portal für drahtlose Registrierung klicken Benutzer auf **Anmelden**.

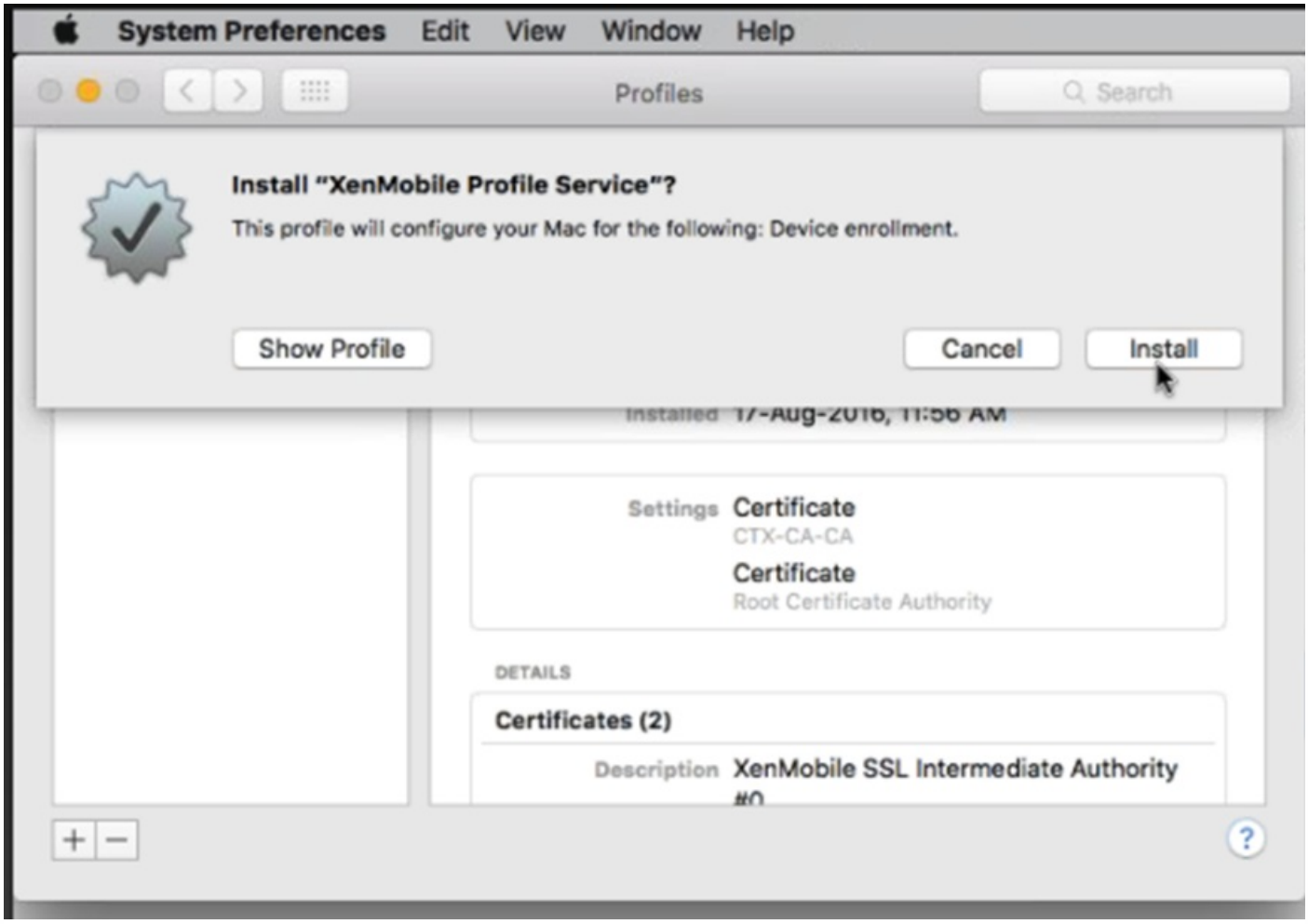


7. Benutzer geben die Anmeldeinformationen im UPN- oder sAMAccountName-Format ein, je nachdem, wie sie vom XenMobile-Administrator konfiguriert wurden, und klicken dann auf **Anmelden**.



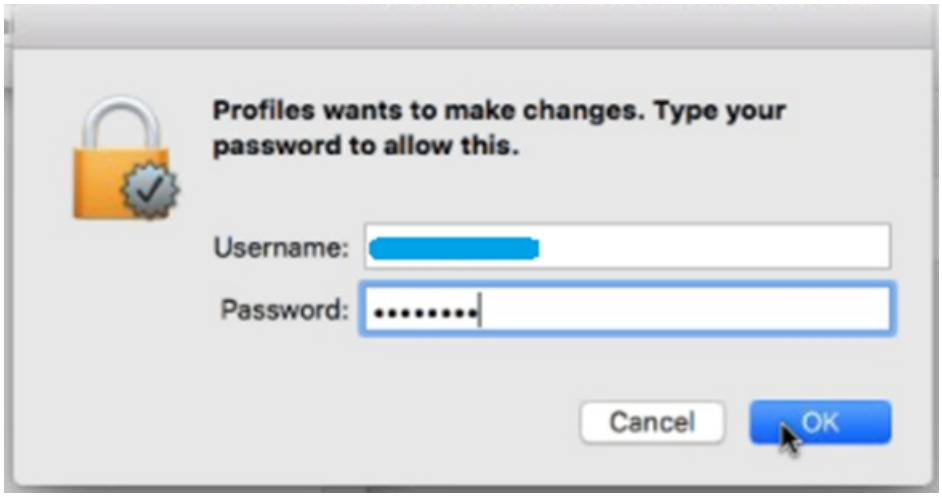
Hinweis: XenMobile prüft die Benutzeranforderung und überprüft die Anmeldeinformationen anhand von Active Directory. Die Anmeldeinformationen werden mit Active Directory überprüft.

8. Wenn die Anmeldung erfolgreich ist, wird das Fenster "XenMobile-Profildienst" angezeigt. Benutzer klicken auf **Installieren**, um den XenMobile-Profildienst zu installieren. Durch die Installation des XenMobile-Profildiensts kann der XenMobile-Administrator die Mac-Geräte remote verwalten.

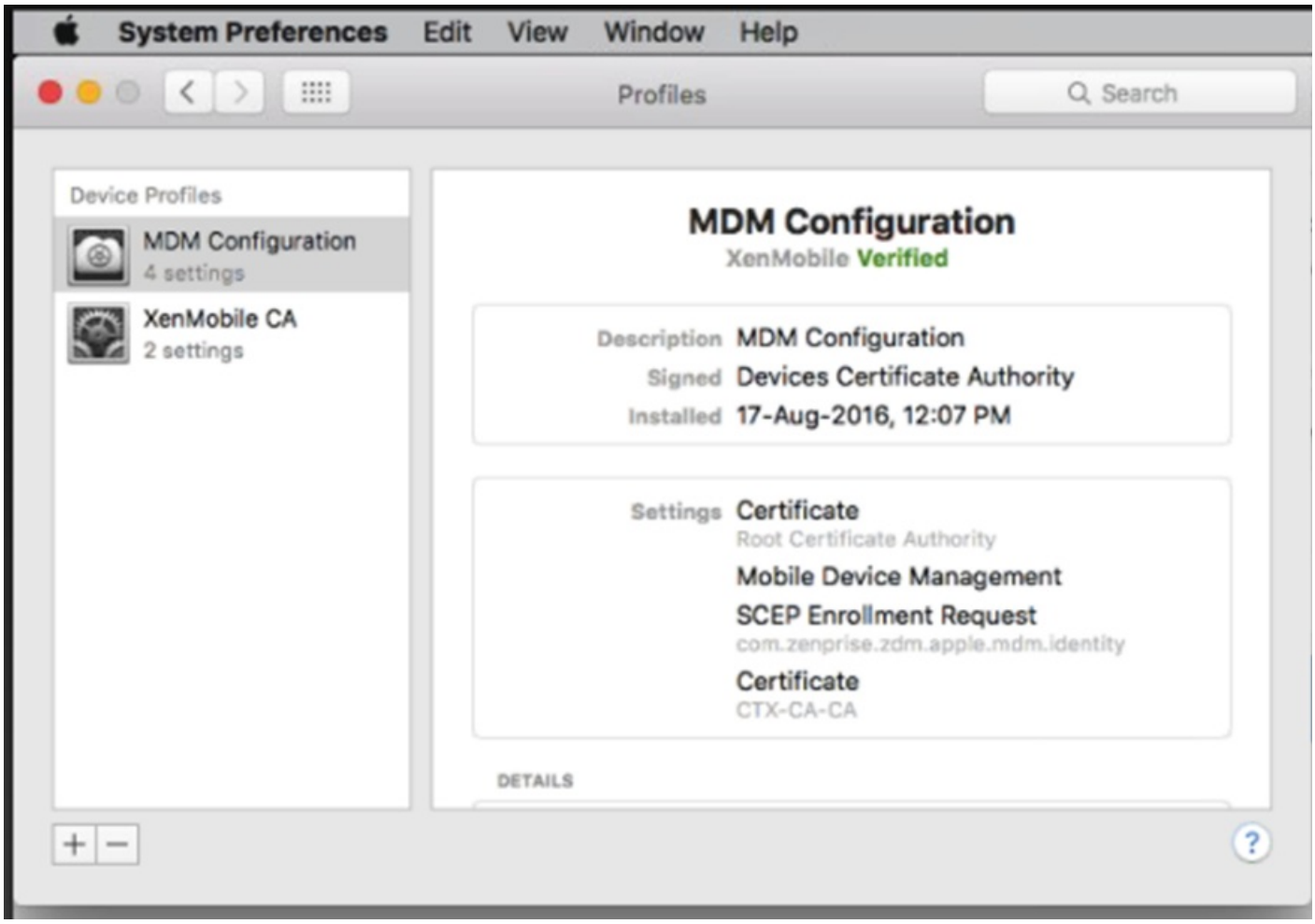


9. Zum Installieren des MDM-Profils klicken Benutzer auf **Weiter** und dann auf **Installieren**.

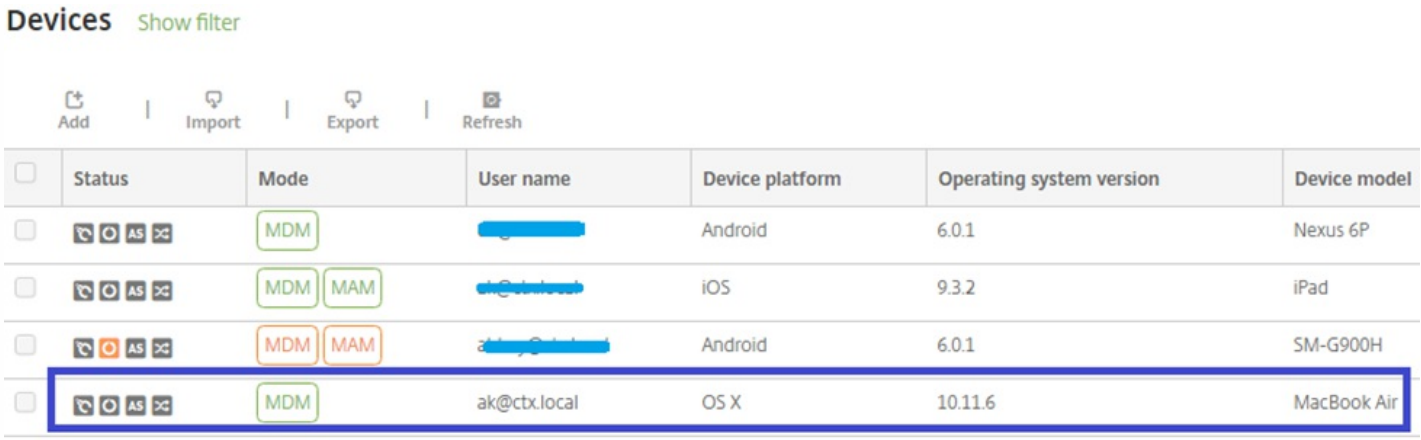
10. Benutzer geben bei Aufforderung die Anmeldeinformationen des Geräts ein.



11. Wenn das MDM-Konfiguration-Profil erfolgreich installiert wurde, wird der MDM-Konfigurationsbildschirm angezeigt.



12. Das Mac-Gerät wird jetzt auf der Registerkarte "Gerät" der XenMobile-Konsole angezeigt. Sie können Mac-Geräte nun mit XenMobile genauso verwalten wie Mobilgeräte.



Windows-Geräte

Sie können in XenMobile Geräte mit folgenden Windows-Betriebssystemen registrieren:

- Windows 8.1 und Windows 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 wichtig beim Upgrade von Windows 8 auf Windows 8.1, da die Benutzer möglicherweise nicht automatisch über alle verfügbaren Updates benachrichtigt werden.

2. Tippen Sie im Charms-Menü auf "Einstellungen" und dann auf Folgendes:

- Für Windows 8.1 tippen Sie auf "PC-Einstellungen > Netzwerk > Arbeitsbereich".
- Für Windows 10 tippen Sie auf "Konten > Arbeitsplatz oder Schule > Mit Arbeitsplatz oder Schule verbinden">.

3. Geben Sie Ihre geschäftliche E-Mail-Adresse ein und tippen Sie dann auf **Geräteverwaltung einschalten** (Windows 8.1)

bzw. **Weiter** (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. Geben Sie unter Windows 8.1 im Dialogfeld **Apps und Dienste des IT-Administrators zulassen** an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie auf **Einschalten**. Geben Sie unter Windows 10 im Dialogfeld **Nutzungsbedingungen** an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie dann auf **Annehmen**.

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 wichtig beim Upgrade von Windows 8 auf Windows 8.1, da die Benutzer möglicherweise nicht automatisch über alle verfügbaren Updates benachrichtigt werden.

2. Tippen Sie im Charms-Menü auf **Einstellungen** und dann auf Folgendes:

- Für Windows 8.1 tippen Sie auf **PC-Einstellungen > Netzwerk > Arbeitsbereich**.
- Für Windows 10 tippen Sie auf **Konten > Arbeitsplatz oder Schule > Mit Arbeitsplatz oder Schule verbinden**.

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 (siehe 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/serverInstance/Discovery.svc Wenn für SSL-Verbindungen ohne Authentifizierung eine andere Portnummer als 8443 verwendet wird, geben Sie die verwendete Portnummer mit der Adresse ein.
- 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. Geben Sie unter Windows 8.1 im Dialogfeld **Apps und Dienste des IT-Administrators zulassen** an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie auf **Einschalten**. Geben Sie unter Windows 10 im Dialogfeld **Nutzungsbedingungen** an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie dann auf **Annehmen**.

Registrieren von Windows Phone-Geräten

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-Unternehmensstore vor der Registrierung der Benutzer bereitstellen möchten, müssen Sie vorher eine Enterprise Hub-Richtlinie erstellen (mit einer signierten Windows Phone-App für Secure Hub für jede unterstützte Plattform).

1. Tippen Sie auf der Hauptseite des Windows Phone-Geräts auf das Symbol **Einstellungen**.

- Tippen Sie je nach Windows 10 Phone-Version auf **Konten > Arbeitsplatz oder Schule > Mit Arbeitsplatz oder Schule verbinden** oder auf **Konten > Arbeitsplatzzugriff > Für MDM-Verwaltungsdienst registrieren**.
- Tippen Sie unter Windows Phone 8.1 auf **PC-Einstellungen > Netzwerk > Arbeitsplatz** und dann auf **Konto hinzufügen**.

2. 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.

3. 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.

4. Geben Sie den Benutzernamen und die Domäne ein, sofern die Authentifizierung über einen Benutzernamen und eine Domäne erfolgt und tippen Sie auf **Anmelden**.

5. 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**.

6. 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.

7. Tippen Sie unter Windows Phone 8.1 im Bildschirm **Konto hinzugefügt** auf **Fertig**.

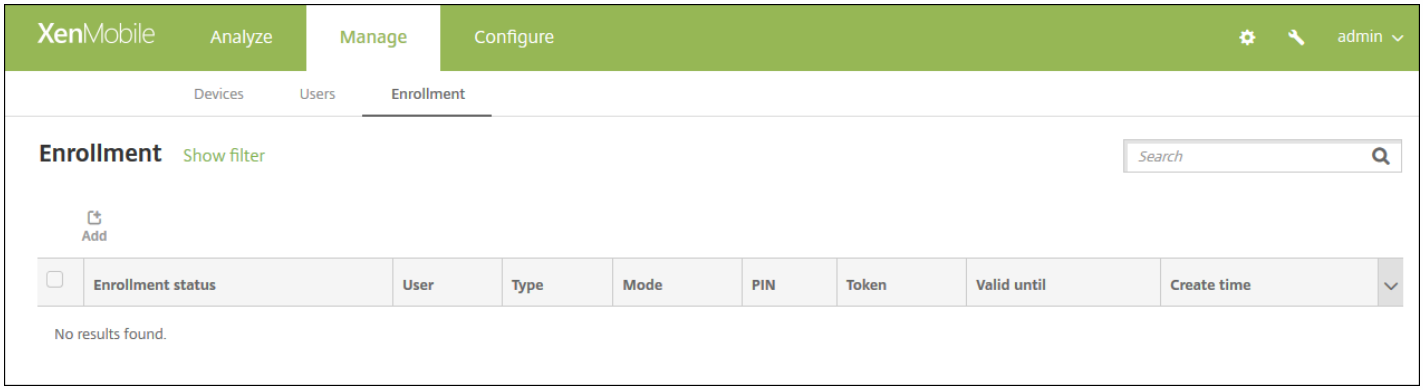
8. Zum Erzwingen einer Verbindung mit dem Server tippen Sie auf das Symbol zum Aktualisieren. Wenn das Gerät nicht manuell eine Verbindung mit Server herstellt, versucht XenMobile, die Verbindung wiederherzustellen. XenMobile versucht 5 Mal alle 3 Minuten eine Verbindung herzustellen, anschließend alle 2 Stunden. Sie können diese Verbindungsrate unter **Servereigenschaften** über die Option **Windows WNS-Taktintervall** ändern. Nachdem die Registrierung abgeschlossen ist, wird Secure Hub im Hintergrund registriert. Der Abschluss der Installation wird nicht angezeigt. Tippen Sie auf dem Bildschirm **Alle Apps** auf "Secure Hub".

Senden von Registrierungseinladungen

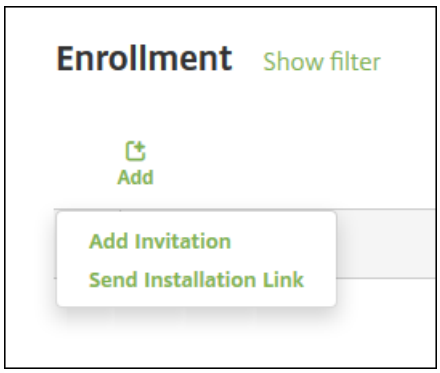
In der XenMobile-Konsole können Sie Registrierungseinladungen an Benutzer mit iOS- oder Android-Geräten senden. Sie

können auch einen Installationslink an Benutzer mit iOS-, Android- oder Windows-Geräten senden.

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



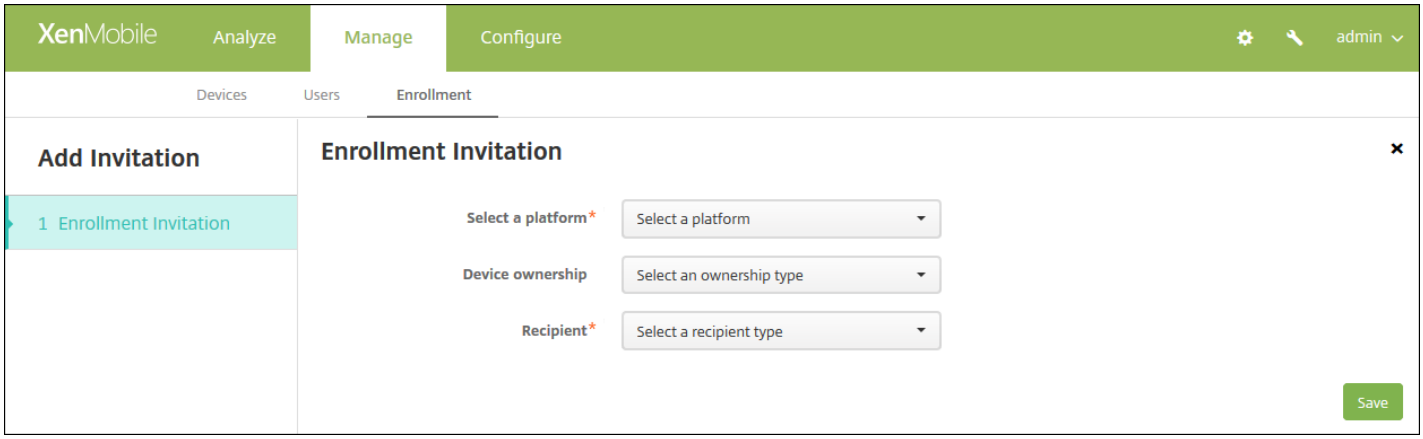
2. Klicken Sie auf **Hinzufügen**. Ein Menü mit den Registrierungsoptionen wird eingeblendet.



- 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.

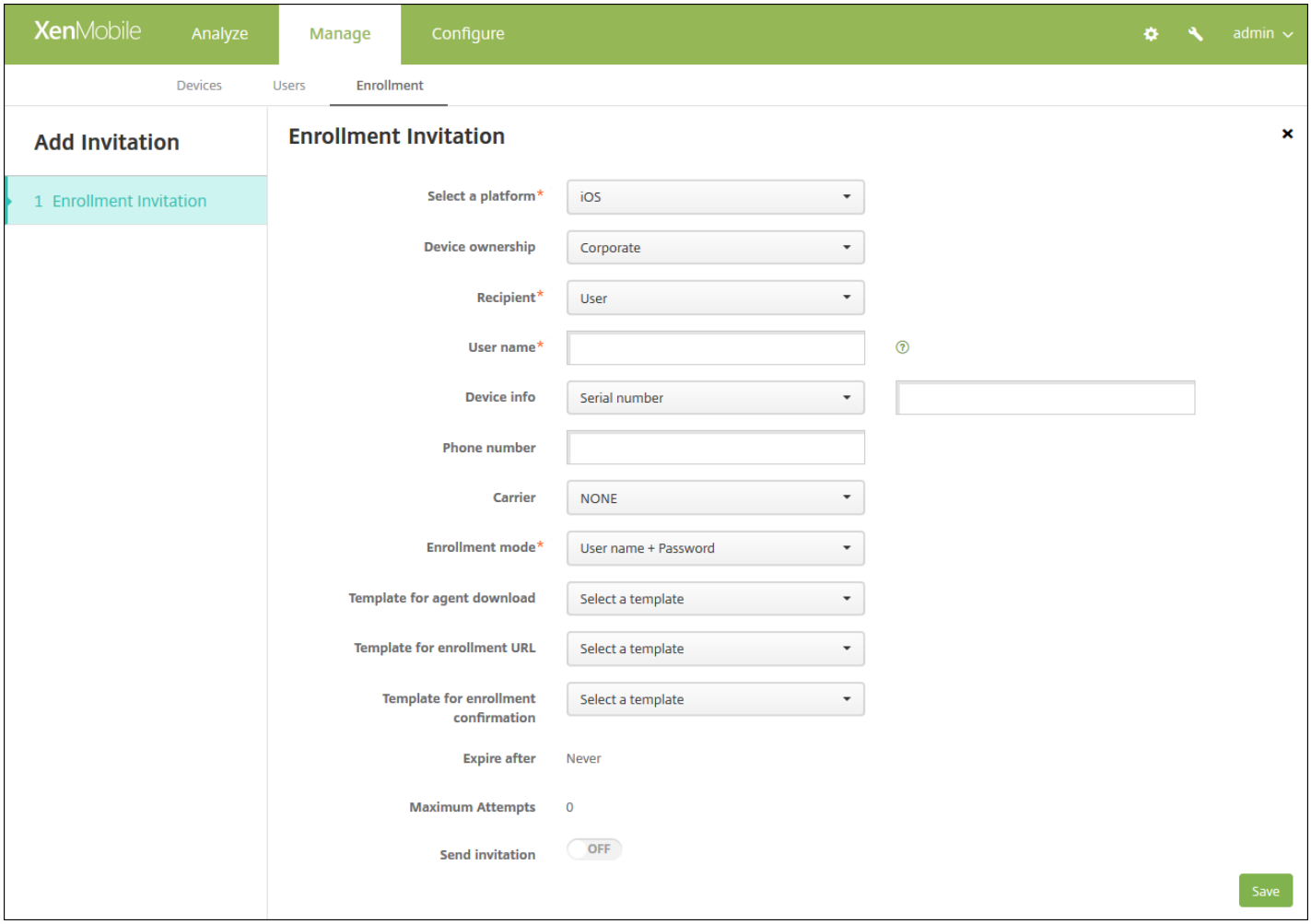


2. Konfigurieren Sie folgende Einstellungen:

- **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 **Gruppe** 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 dieser 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. Die Standardeinstellung ist **Benutzername + Kennwort**. Mögliche Optionen:
  - Hohe Sicherheit
  - Einladungs-URL
  - Einladungs-URL + PIN
  - Einladungs-URL + Kennwort
  - Zweistufig
  - Benutzername + PIN

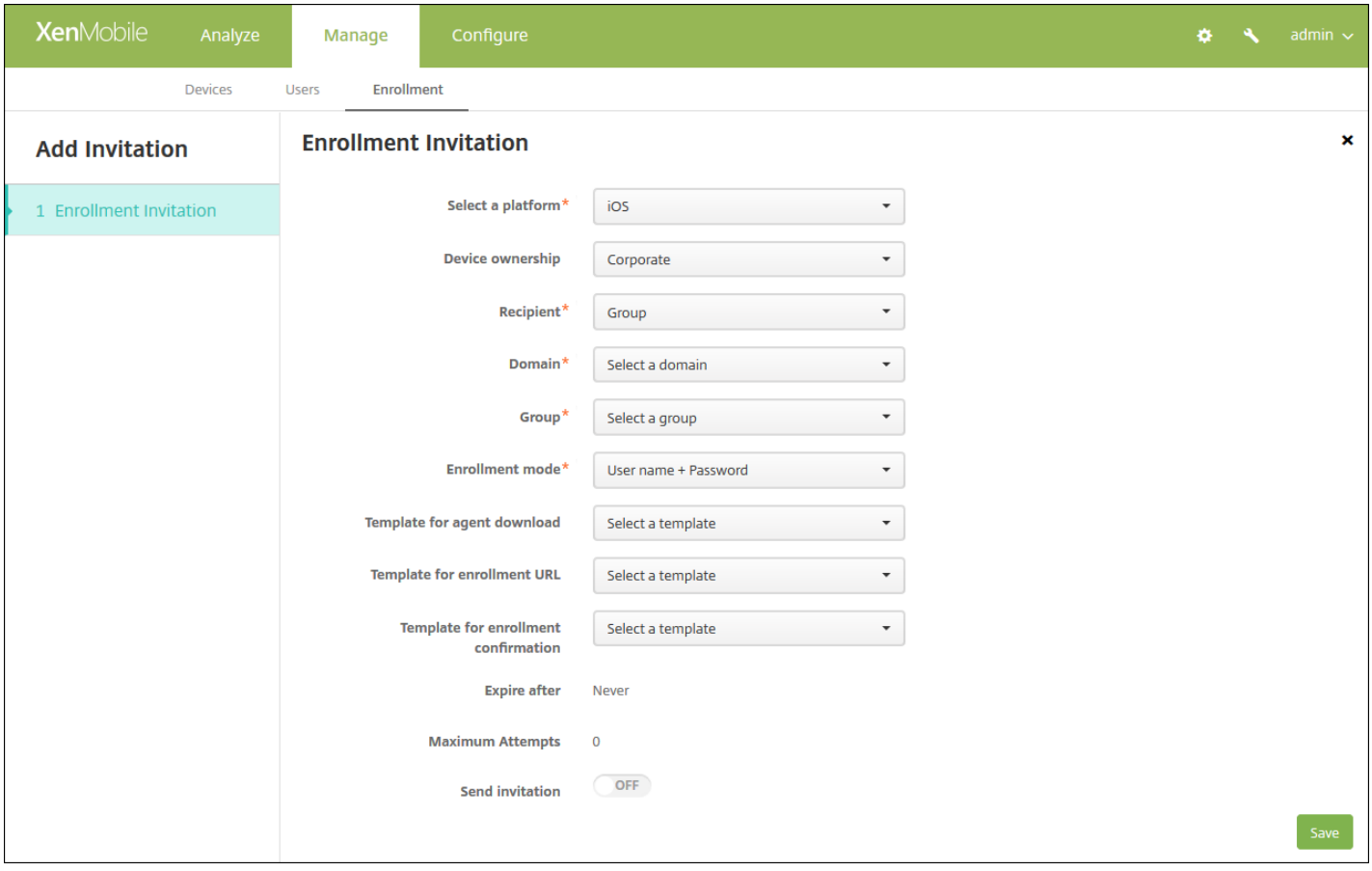
  Hinweis: Wenn Sie einen Registrierungsmodus mit PIN auswählen, wird das Feld **Vorlage für Registrierungs-PIN**

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 die Einladung lediglich in die Tabelle auf der Seite **Registrierung** eingefügt werden soll.

2. Klicken Sie auf **Speichern und senden**, wenn Sie **Einladung senden** ausgewählt haben. Klicken Sie andernfalls auf **Speichern**. Die Einladung wird in der Tabelle auf der Seite **Registrierung** aufgeführt.

Senden einer Registrierungseinladung an eine Gruppe



1. Konfigurieren Sie folgende Einstellungen:

- **Domäne**: Klicken Sie in der Liste auf die Domäne, in der Sie die Gruppe auswählen möchten.

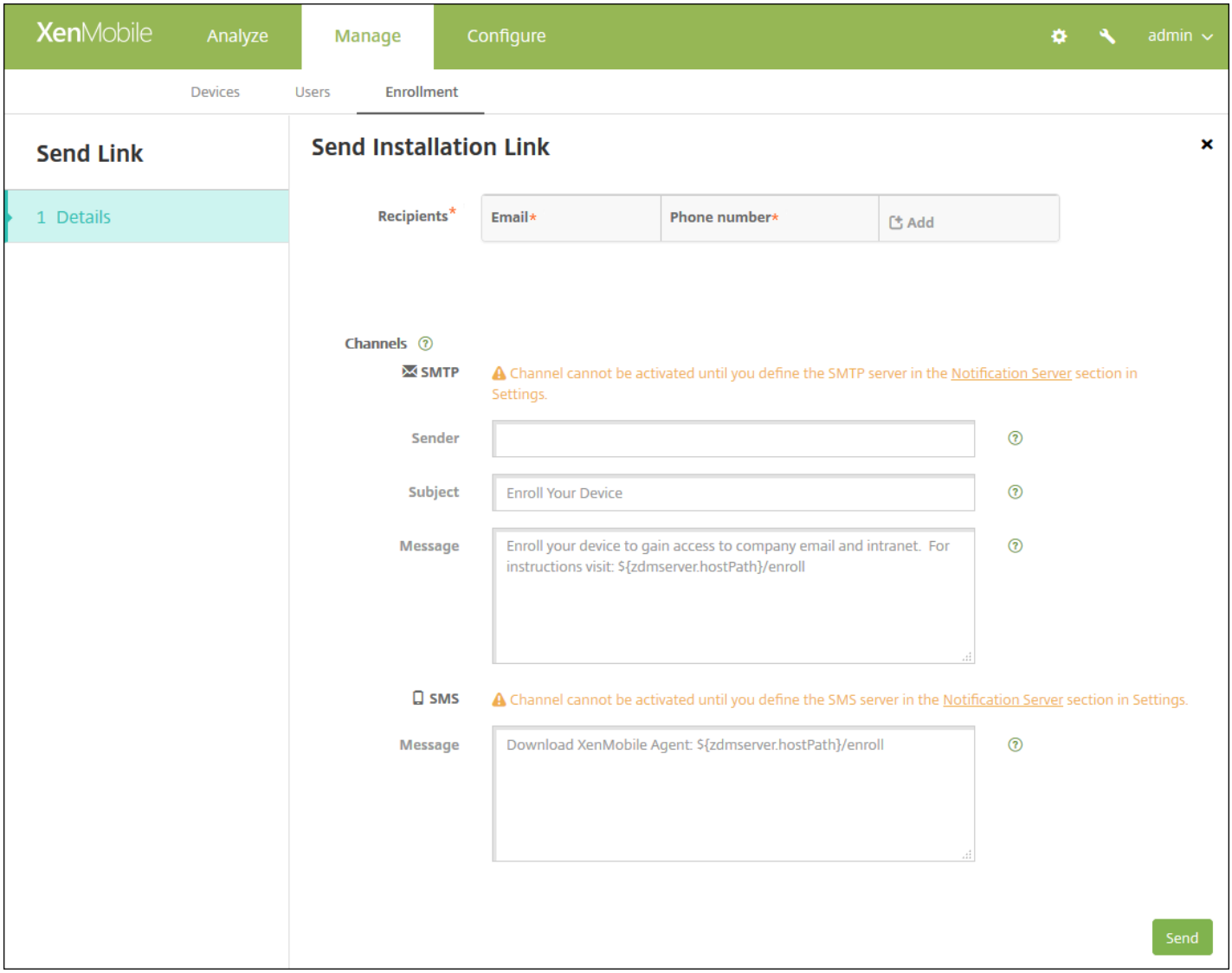
- **Gruppe**: Klicken Sie in der Liste auf die Gruppe, die die Einladung erhalten soll.
- **Registrierungsmodus**: Klicken Sie in der Liste auf die gewünschte Registrierungsmethode für Benutzer. Die Standardeinstellung ist **Benutzername + Kennwort**. Mögliche Optionen:
  - Hohe Sicherheit
  - Einladungs-URL
  - Einladungs-URL + PIN
  - Einladungs-URL + Kennwort
  - Zweistufig
  - 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 die Einladung lediglich in die Tabelle auf der Seite **Registrierung** eingefügt werden soll.

2. Klicken Sie auf **Speichern und senden**, wenn Sie **Einladung senden** ausgewählt haben. Klicken Sie andernfalls 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. Einzelheiten finden Sie unter Benachrichtigungen.

1. Konfigurieren Sie folgende 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 am 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. Einzelheiten finden Sie unter Benachrichtigungen.
  - **SMTP**: Konfigurieren Sie die folgenden 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 den 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 die 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.

Geräteregistrierungslimit

Feb 24, 2017

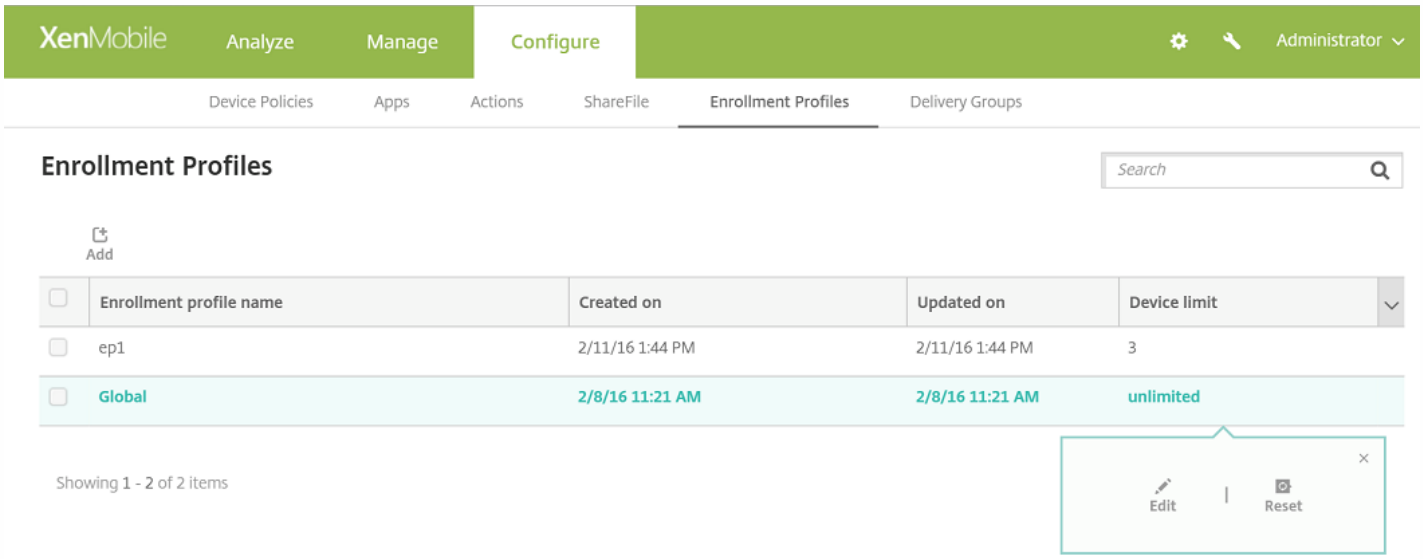
In den ENT-, MDM- und MAM-Servermodi können Sie die Anzahl von Geräten, die ein Benutzer registrieren kann, in der XenMobile-Konsole unter **Konfigurieren > Registrierungsprofile** einschränken. Einschränkungen können global oder pro Bereitstellungsgruppe gelten. Sie können mehrere Registrierungsprofile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

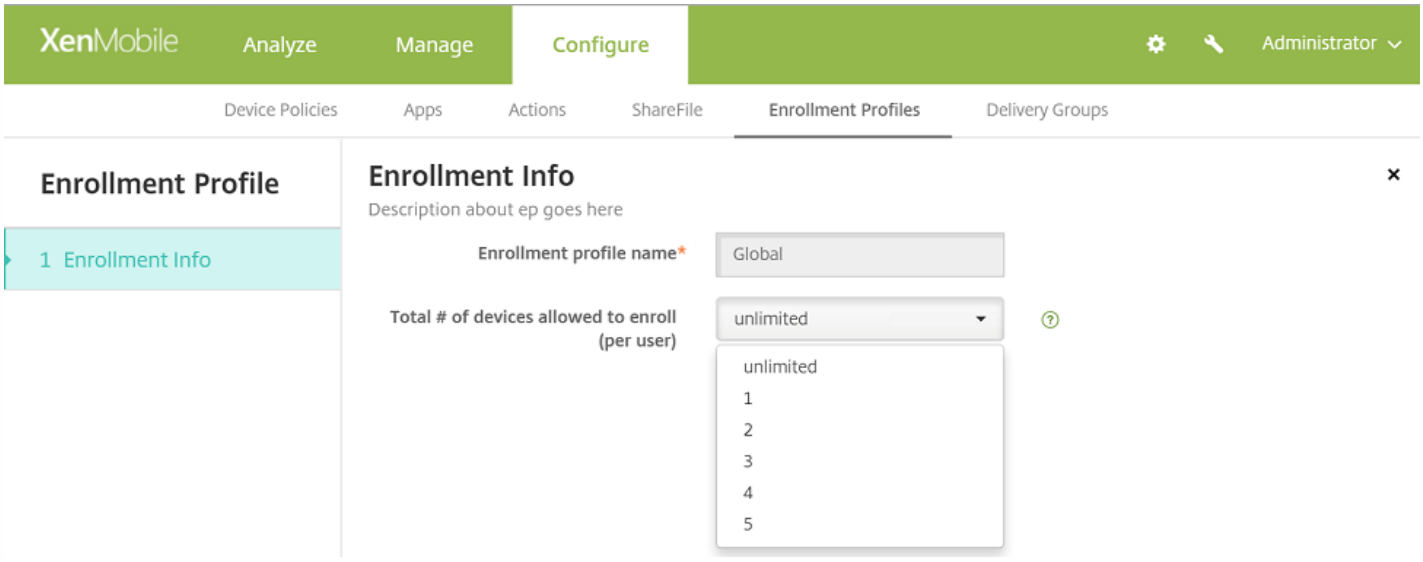
Konfigurieren eines globalen Geräteregistrierungslimits

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.

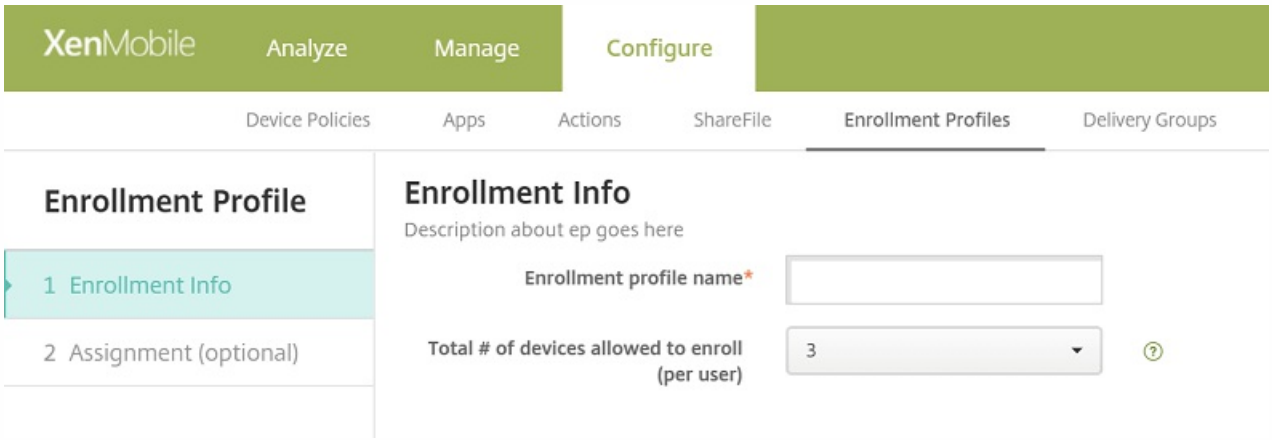


Konfigurieren eines Geräteregistrierungslimits für Bereitstellungsgruppen

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

   Die Seite **Registrierungsinfo** wird angezeigt.

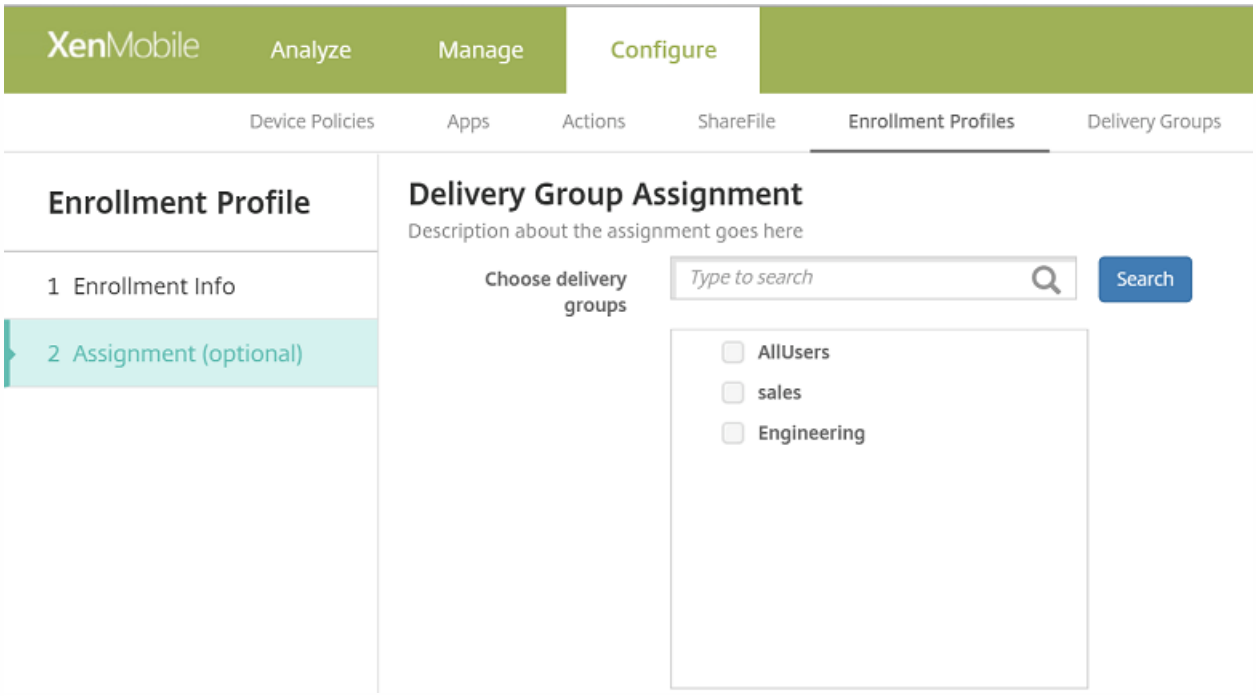
2. Geben Sie einen Namen für das neue Registrierungsprofil an und wählen Sie dann die Anzahl der Geräte aus, die Mitglieder mit diesem Profil registrieren können.



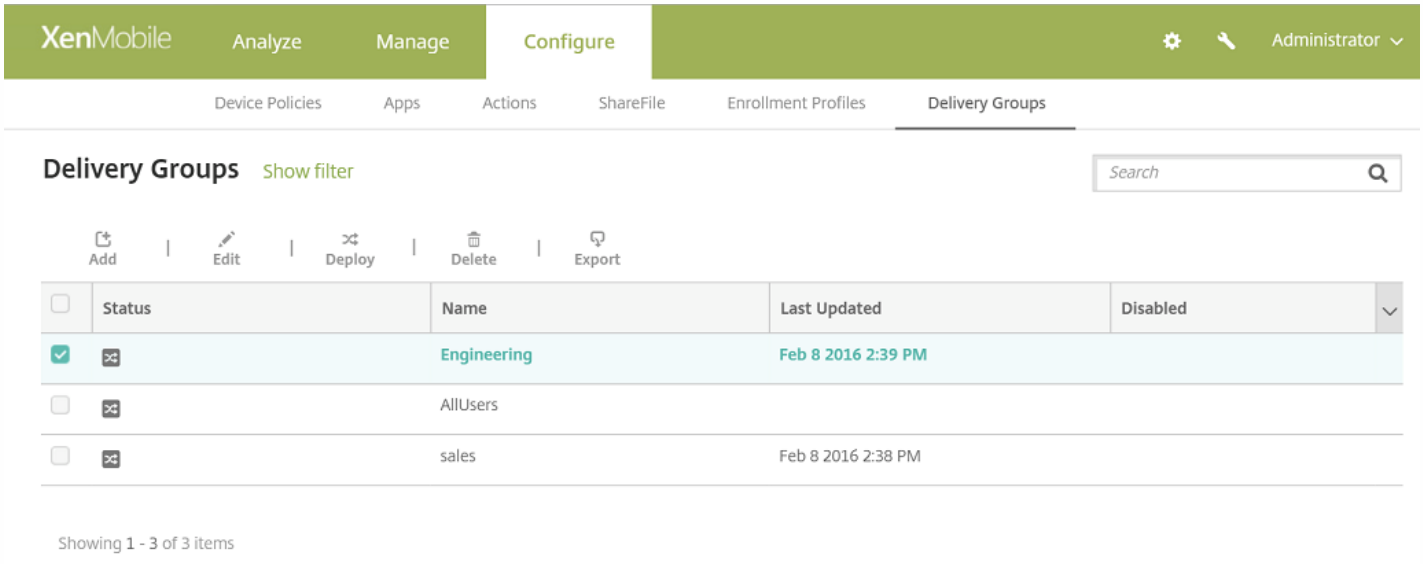
3. Klicken Sie auf **Weiter**.

   Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.

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

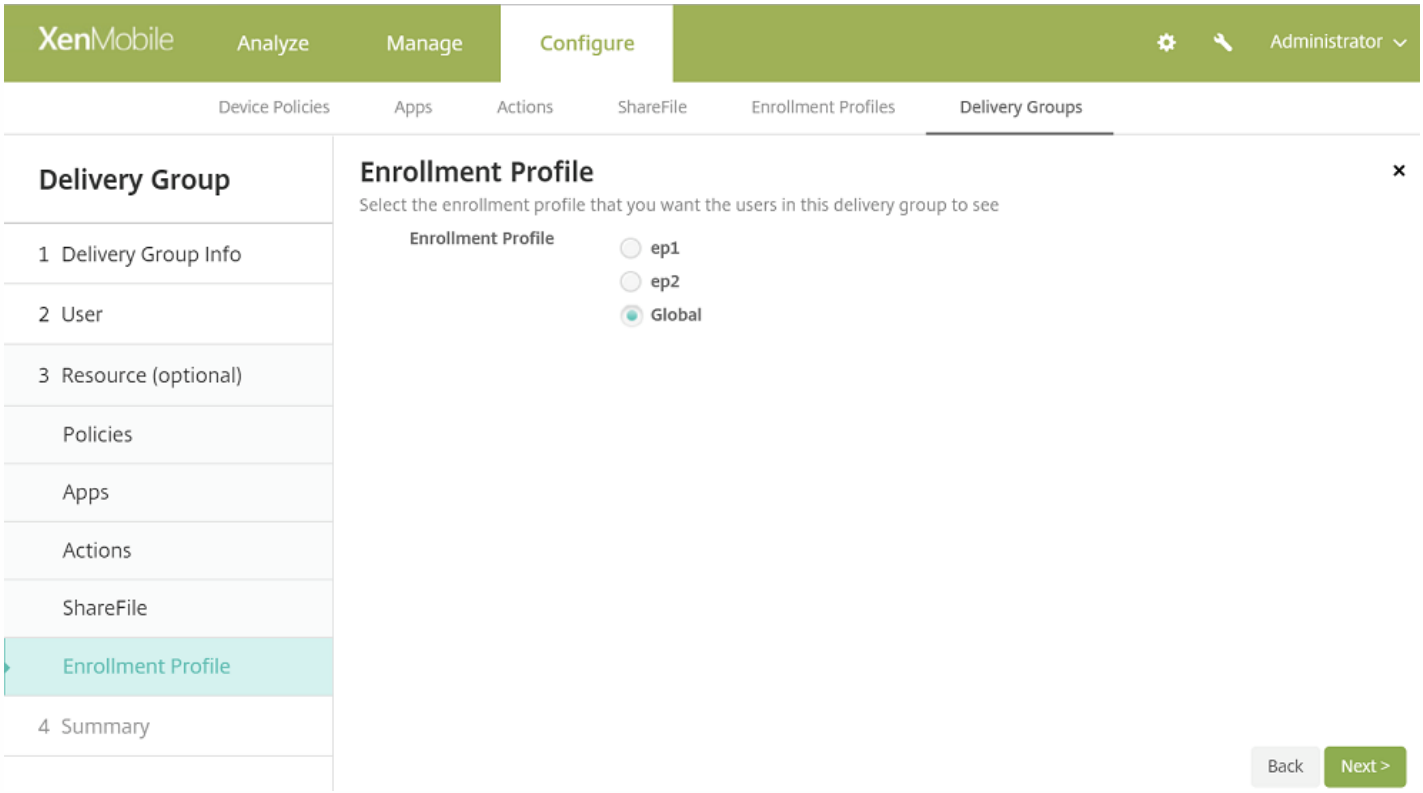


Wenn Sie später das Registrierungsprofil einer Bereitstellungsgruppe ändern möchten, wählen Sie **Konfigurieren > Bereitstellungsgruppen**. Wählen Sie die gewünschte Gruppe und klicken Sie auf **Bearbeiten**.



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

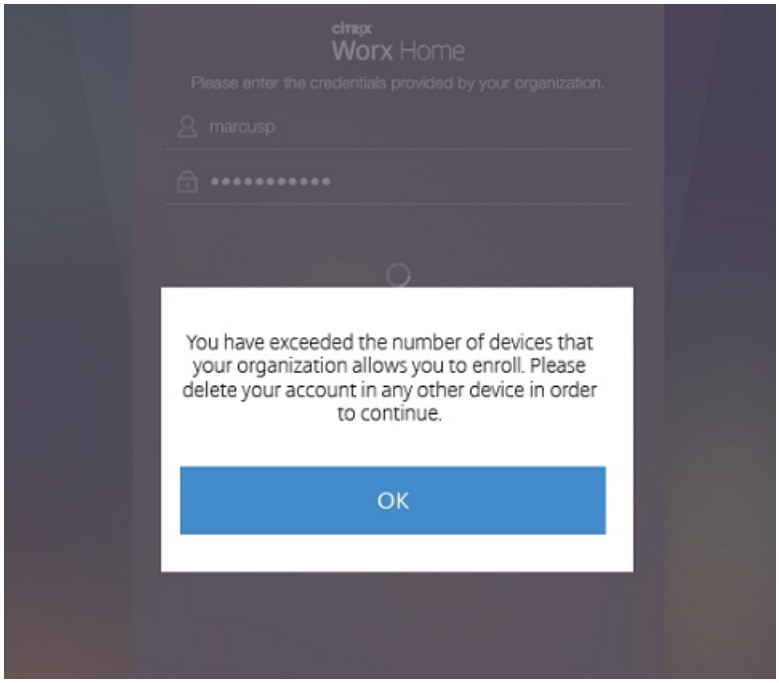
Wenn Sie das Geräteregistrierungslimit festlegen, können Benutzer ein neues Gerät mit den folgenden Schritten registrieren:

1. Melden Sie sich bei Secure Hub 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 Bildschirm zur Registrierung bei Secure Hub wird erneut angezeigt.

Gemeinsam genutzte Geräte

Feb 24, 2017

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, Citrix PIN, Touch ID, Benutzerentropie und zweistufige Authentifizierung werden nicht unterstützt.

MDM+MAM-Modus

- Nur auf iOS- und Android-Tablets verfügbar.
- Wird von XenMobile 10.3.x und höher unterstützt.
- Nur die Authentifizierung mit Active Directory-Benutzernamen und Kennwort wird unterstützt.
- Clientzertifikatauthentifizierung, Worx-PIN, Touch ID, Benutzerentropie und zweistufige Authentifizierung werden nicht unterstützt.
- Der MAM-Only-Modus wird nicht unterstützt. Die Geräte müssen in MDM registriert werden.
- Nur Secure Mail, Secure Web und die mobile ShareFile-App 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 XenMobile-Apps und mit MDX umschlossene Apps gemeinsam nutzen. Native Apps können nicht gemeinsam genutzt werden.
- Nach dem Download während der Erstregistrierung werden XenMobile-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:

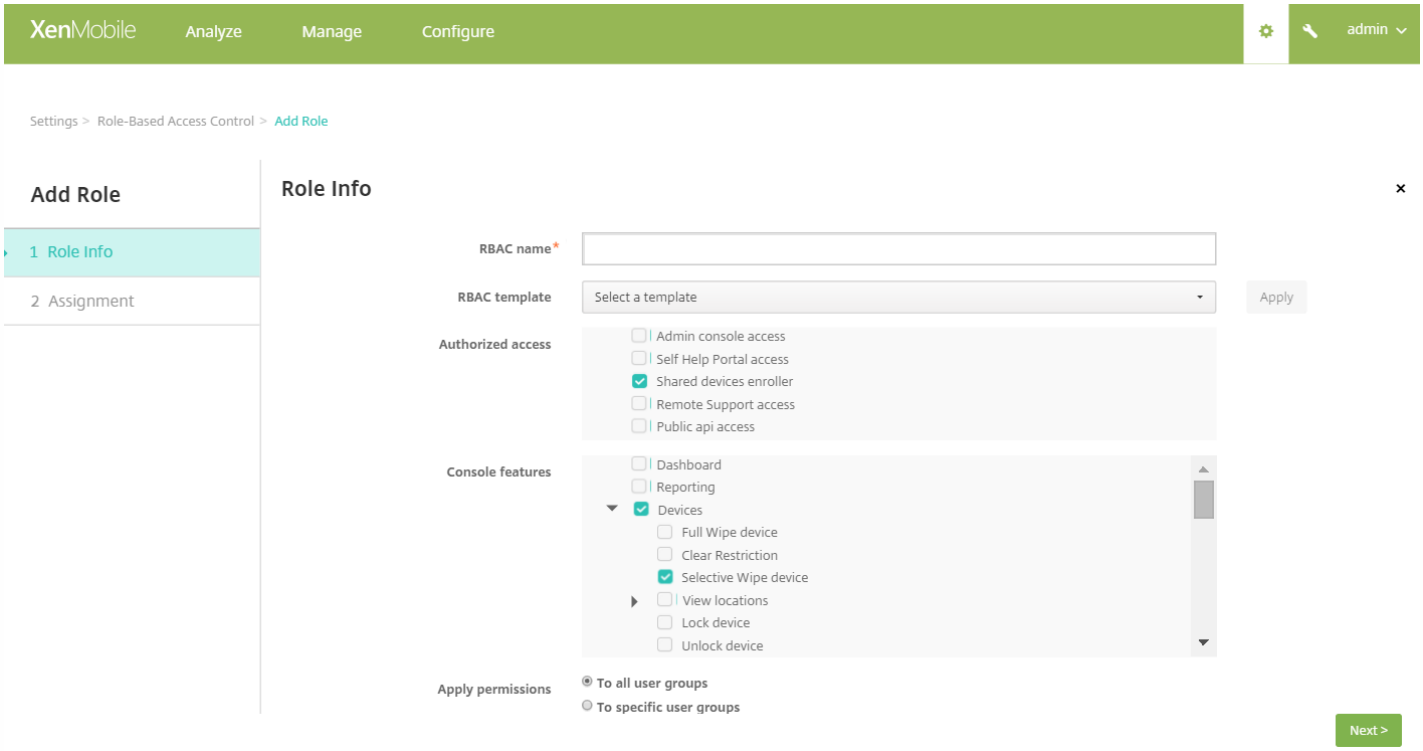
- iOS 9 und 10
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x (Nur-MDM-Modus)

Konfigurieren eines gemeinsam genutzten Geräts

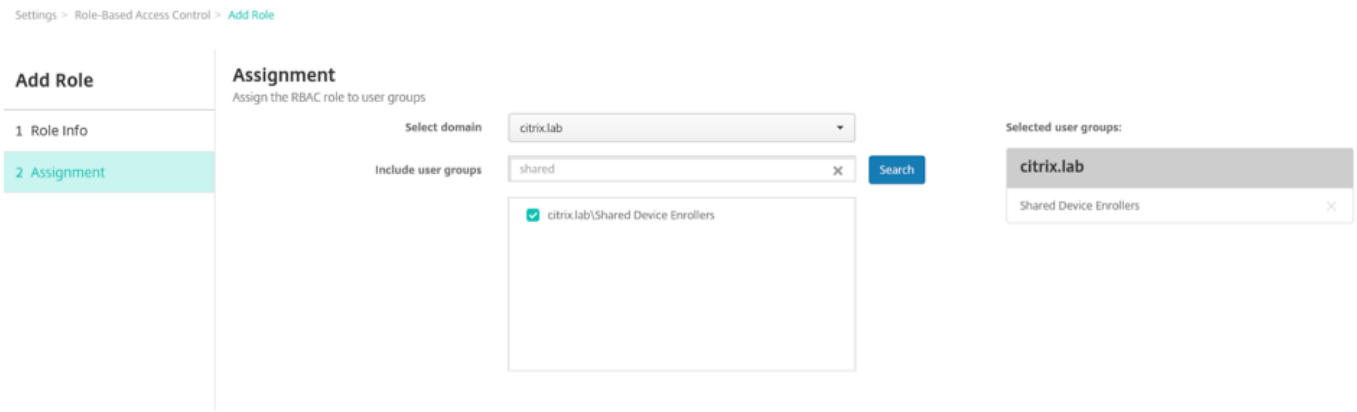
Mit den folgenden Schritten konfigurieren Sie ein gemeinsam genutztes Gerät.

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 Secure Hub gelöscht werden, wenn die Registrierung des Geräts aufgehoben wird.

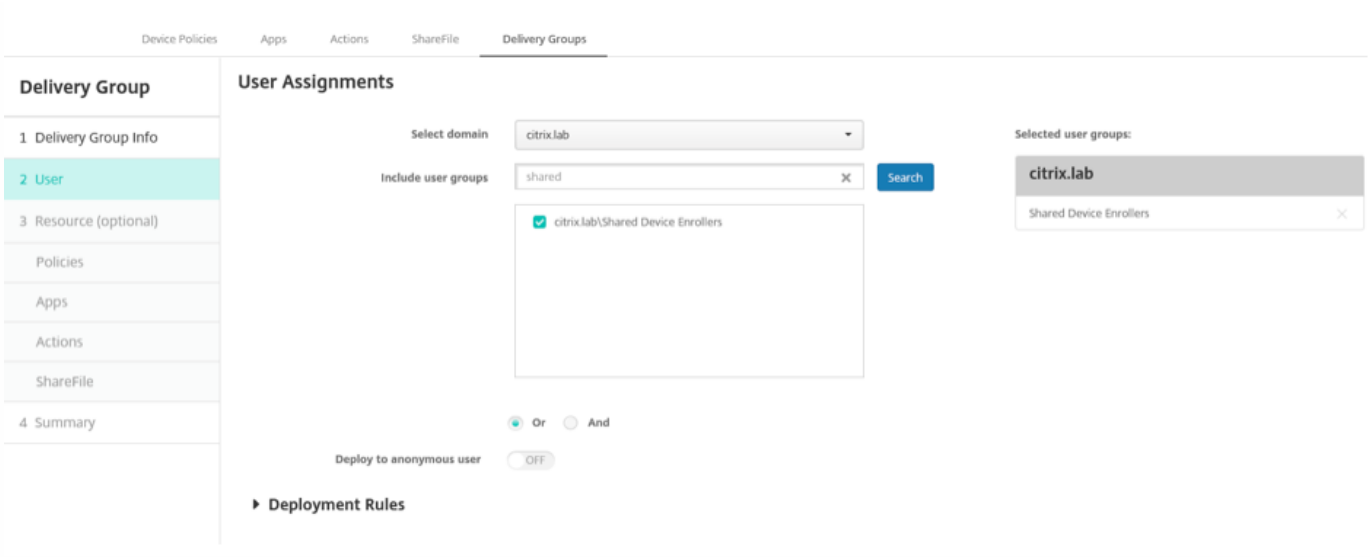
   Behalten Sie die Standardeinstellung **Auf alle Benutzergruppen** für **Berechtigungen anwenden** bei oder weisen Sie bestimmten Active Directory-Benutzergruppen Berechtigungen mit der Option **Auf bestimmte Benutzergruppen** zu.



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 Secure Hub 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 bei Secure Hub anmeldet, werden die Richtlinien und Apps des Benutzers 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

Secure Mail und Secure Web werden auf dem Gerät bereitgestellt, wenn die Registrierung von dem Benutzer für gemeinsam genutzte Geräte durchgeführt wird. Die Benutzerdaten werden sicher auf dem Gerät gespeichert. Die Daten werden anderen Benutzern nicht angezeigt, wenn sie sich bei Secure Mail oder Secure Web anmelden.

Es kann sich nur jeweils ein Benutzer bei Secure Hub anmelden. Der vorherige Benutzer muss sich abmelden, bevor der

nächste Benutzer sich anmelden kann. Aus Sicherheitsgründen speichert Secure Hub 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 Secure Hub nicht zu, dass neue Benutzer sich während des Entfernens der 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 Richtlinien für Secure Mail

- Für die optimale Leistung von Secure Mail legen Sie den maximalen 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
21–25	1 Woche oder weniger
6–20	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

Android for Work

Apr 24, 2017

Android at Work (früher "Android for Work") ist ein sicherer Arbeitsbereich auf Geräten mit Android 5.0 und höher. Der Arbeitsbereich isoliert geschäftliche Konten, Apps und Daten von persönlichen Konten, Apps und Daten. In XenMobile können Sie persönliche Geräte (BYOD) und dem Unternehmen gehörende Android-Geräte verwalten, indem Sie Benutzer anweisen, ein separates Arbeitsprofil auf ihren Geräten zu erstellen. Durch die Kombination der Hardwareverschlüsselung und der Richtlinien, die Sie bereitstellen, werden Unternehmens- und persönlicher Bereich auf Geräten zuverlässig getrennt. Sie können alle Unternehmensrichtlinien, Unternehmens-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 Android-Enterprise-Seite von Google.

Sie verwenden Google Play zum Hinzufügen, Erwerben und Genehmigen von Apps für die Bereitstellung in dem Android at Work-Arbeitsbereich von Geräten. Über Google Play können Sie private Android-Apps, öffentliche Apps und solche von Drittanbietern bereitstellen. Wenn Sie XenMobile einen kostenpflichtigen öffentlichen App-Store für Android at Work hinzufügen, können Sie den Lizenzierungsstatus für Massenkäufe überprüfen. Die Statusangabe enthält die Gesamtzahl der verfügbaren Lizenzen, die Zahl der aktuell verwendeten Lizenzen und die E-Mail-Adresse aller Benutzer, die Lizenzen verbrauchen. Einzelheiten finden Sie unter Hinzufügen einer App aus einem öffentlichen App-Store zu XenMobile.

Anforderungen für Android at Work:

- Öffentlich zugängliche Domäne
- Google-Administratorkonto
- Geräte mit Unterstützung für verwaltete Profile, auf denen Android 5.0+ Lollipop ausgeführt wird
- Ein Google-Konto, für das Google Play installiert wurde
- Geschäftliches Profil auf den Geräten eingerichtet

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

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

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

- Google-Verwaltungskonsole: https://admin.google.com/AdminHome
- Google Play-Verwaltungskonsole: https://play.google.com/work/apps
- Google Play Publish für Apps aus privaten Kanälen und selbstgehostete Apps: https://play.google.com/apps/publish
- Google Developer-Konsole zur Erstellung des Dienstkontos: https://console.developers.google.com

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

- Erstellen eines Android at Work-Kontos
- Einrichten eines Dienstkontos
- Herunterladen eines Android at 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-Einstellungen konfigurieren und Android-Apps in XenMobile verwalten. Weitere Informationen über das Erstellen von Anmeldeinformationen finden Sie unter Google Play-Anmeldeinformationen.

Erstellen eines Android at Work-Kontos

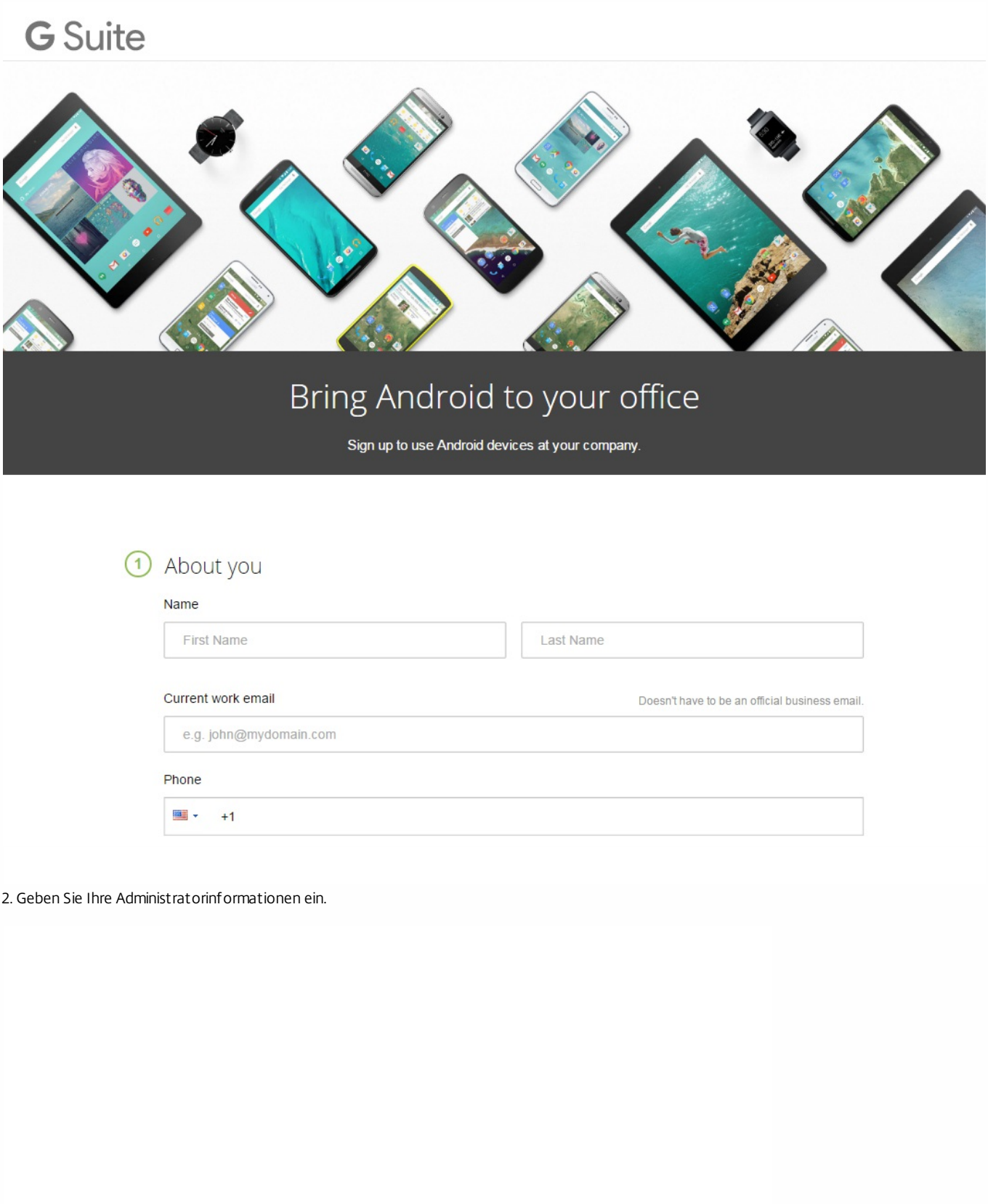
Die folgenden Voraussetzungen müssen erfüllt sein, damit Sie ein Android at Work-Konto erstellen können:

- Sie müssen eine Domäne haben (z. B. example.com).
- Google muss Ihre Eigentümerschaft der Domäne verifizieren.
- Aktivieren und Verwalten Sie Android at Work über einen Enterprise Mobility Management (EMM)-Anbieter (XenMobile 10.1 oder höher).

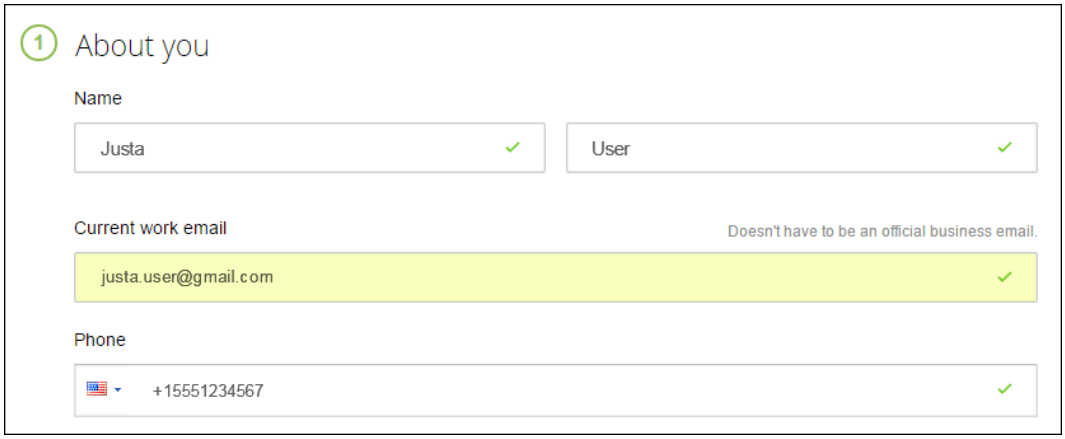
Wenn Ihr Domänenname bei Google bereits verifiziert wurde, können Sie mit dem Schritt Einrichten eines Android at Work-Dienstkontos und Download eines Android at Work-Zertifikats fortfahren.

1. Navigieren Sie zu https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

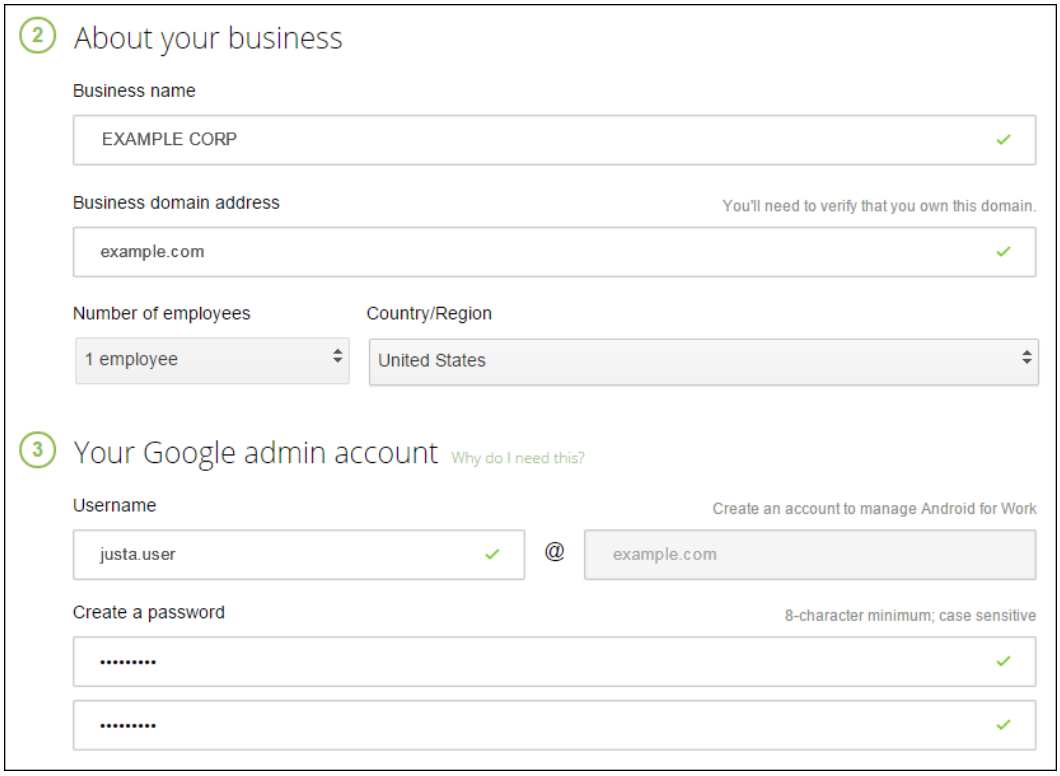
Auf der nachfolgend gezeigten Seite geben Sie die Administrator- und Unternehmensinformationen ein.



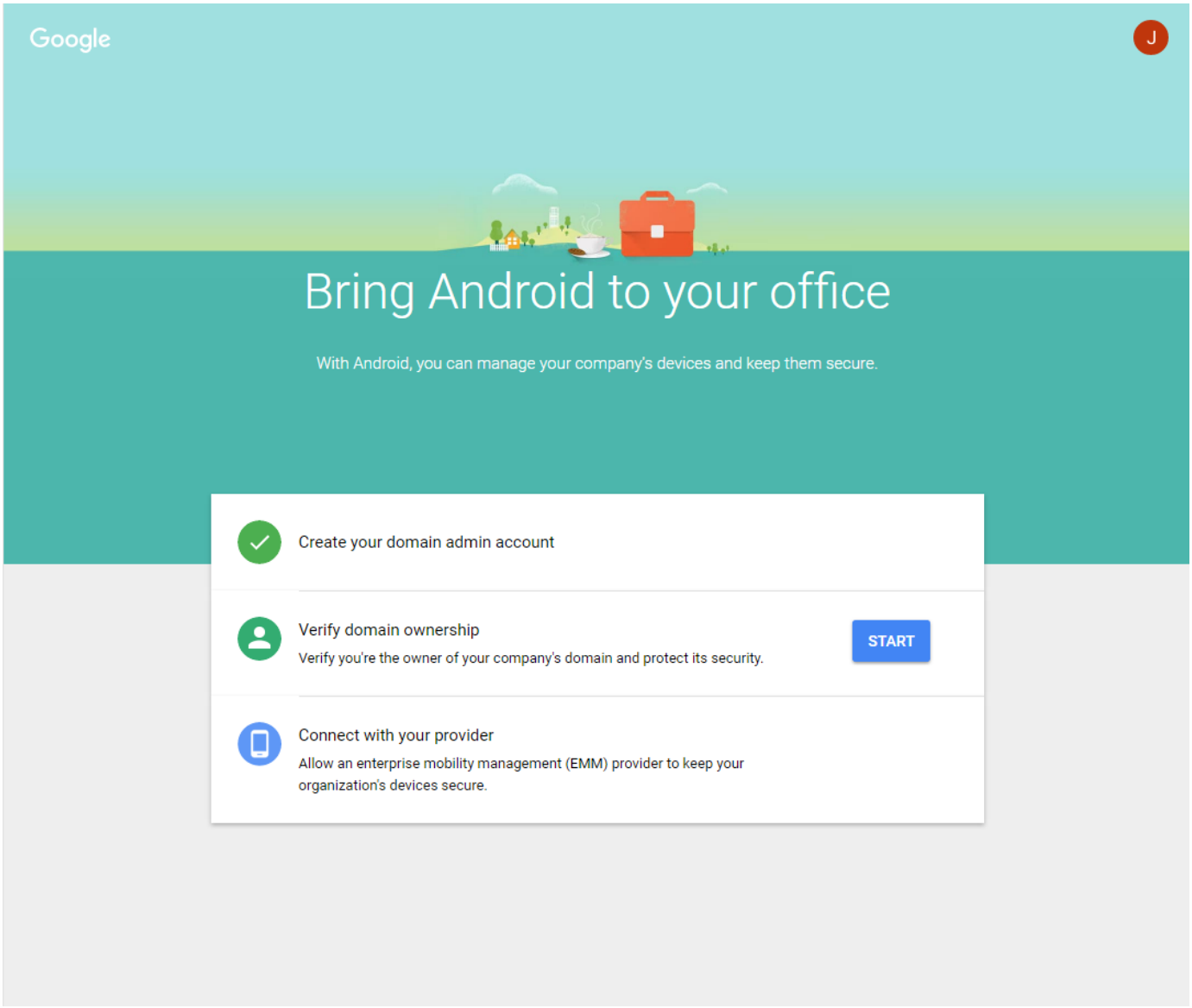
2. Geben Sie Ihre Administratorinformationen ein.



2. Geben Sie zusätzlich zu den Administratorinformationen Informationen zu Ihrem Unternehmen ein.



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



Überprüfen der Domäneneigentümerschaft

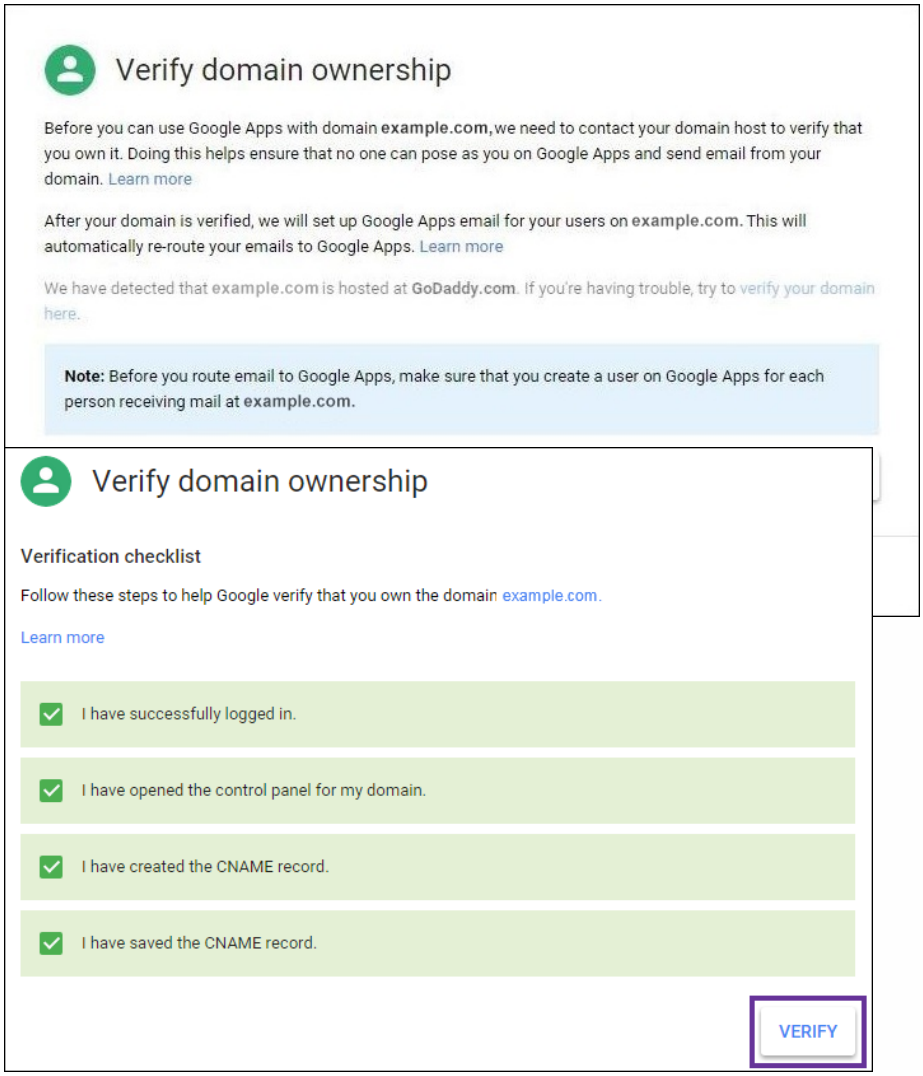
Zur Verifizierung Ihrer Domäne durch Google gibt es folgende Methoden:

- Hinzufügen eines TXT- oder CNAME-Datensatzes zu der Website Ihres Domänenhosts.
- Hochladen einer HTML-Datei auf den Webserver Ihrer Domäne.
- 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/.

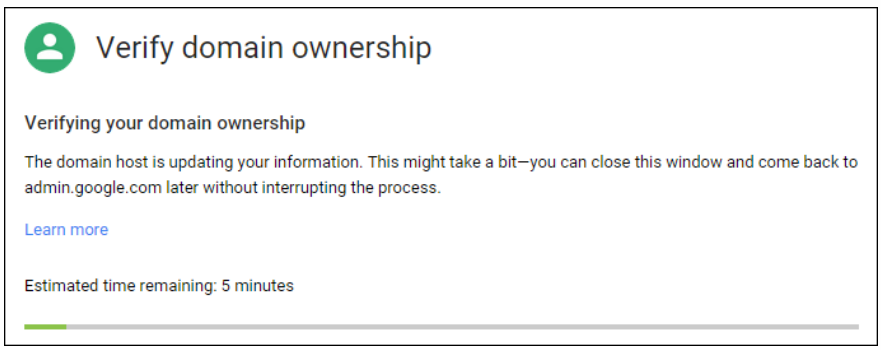
1. Klicken Sie auf **Start**, um die Domänenüberprüfung zu beginnen.

Die Seite **Verify domain ownership** wird angezeigt. Folgen Sie den angezeigten Anweisungen zum Überprüfen Ihrer Domäne.

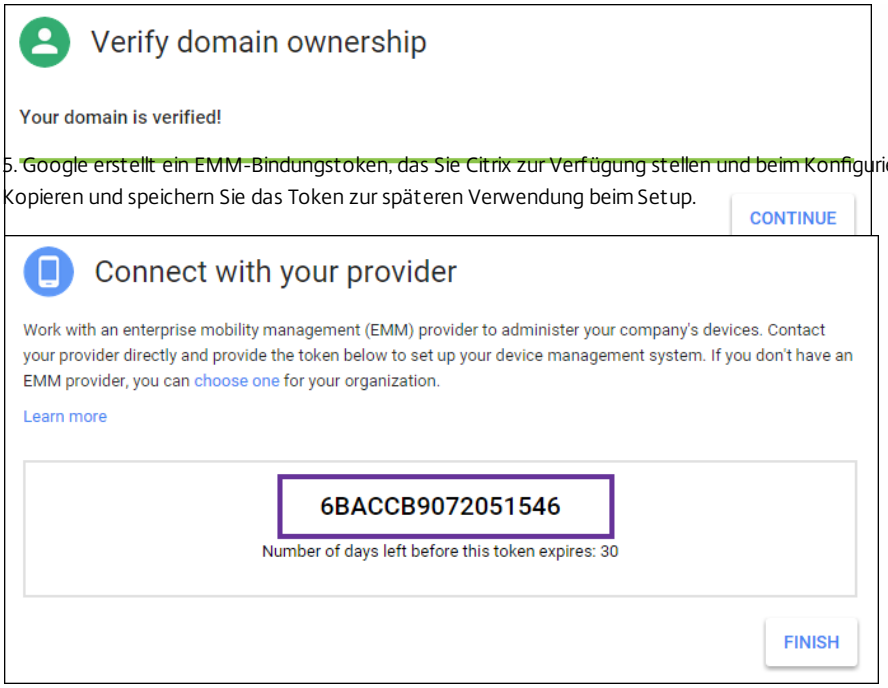
2. Klicken Sie auf **Verify**.



3. Google überprüft die Eigentümerschaft der Domäne.



4. Bei 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 at Work-Einstellungen verwenden. Kopieren und speichern Sie das Token zur späteren Verwendung beim Setup.

6. Klicken Sie auf **Finish**, um die Einrichtung von Android at Work abzuschließen. Es wird eine Seite mit der Meldung angezeigt, dass Ihre Domäne erfolgreich verifiziert wurde.

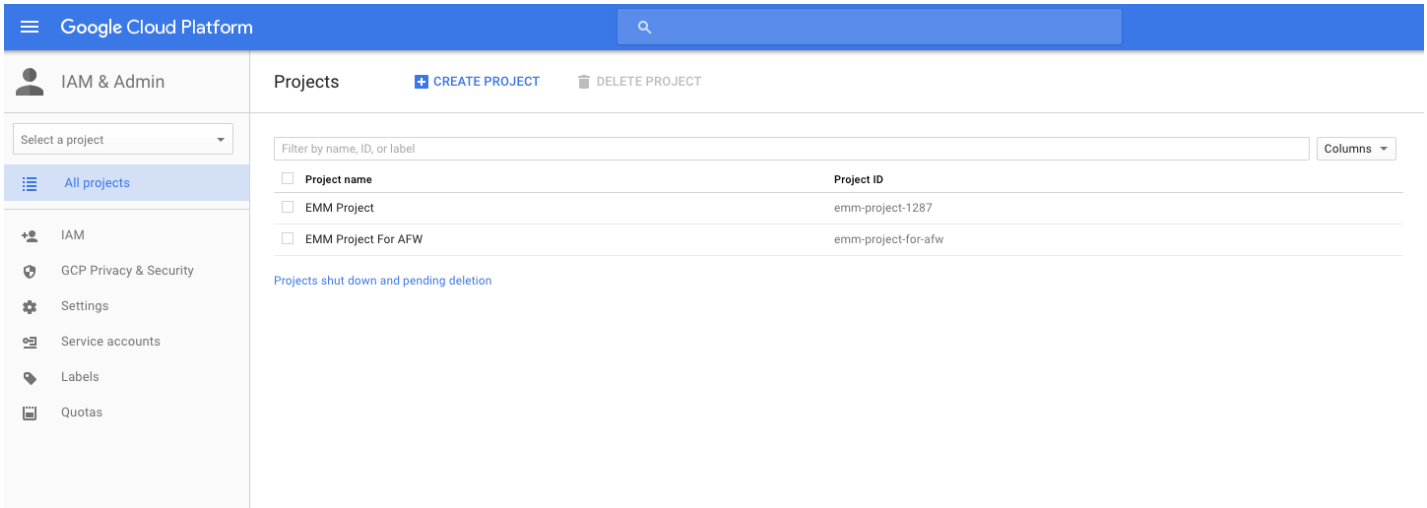
Nach dem Erstellen eines Android at Work-Dienstkontos können Sie sich bei der Google Admin Console anmelden und die Einstellungen Ihrer Mobilitätsverwaltung festlegen.

Einrichten eines Android at Work-Dienstkontos und Herunterladen eines Android at Work-Zertifikats

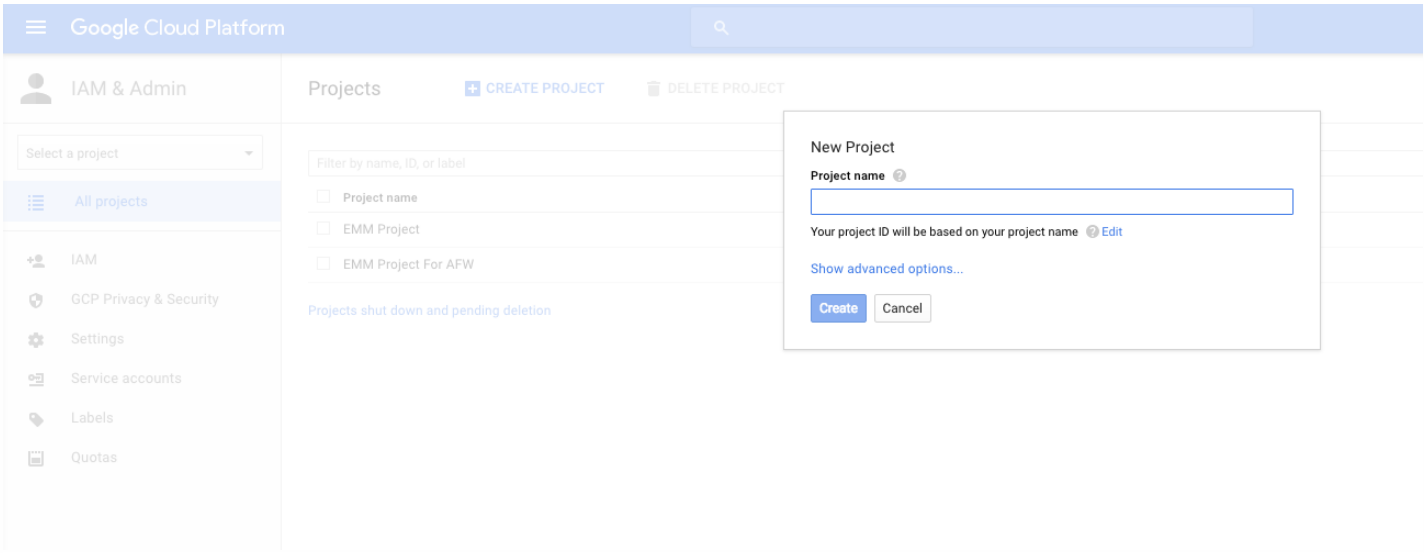
Damit XenMobile Google Play und Verzeichnisdienste kontaktieren kann, müssen Sie ein Dienstkonto mit dem Projektportal für Entwickler von Google erstellen. Das Dienstkonto wird für die Server-Kommunikation zwischen XenMobile und den Google-Diensten für Android verwendet. Weitere Informationen zum verwendeten 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.

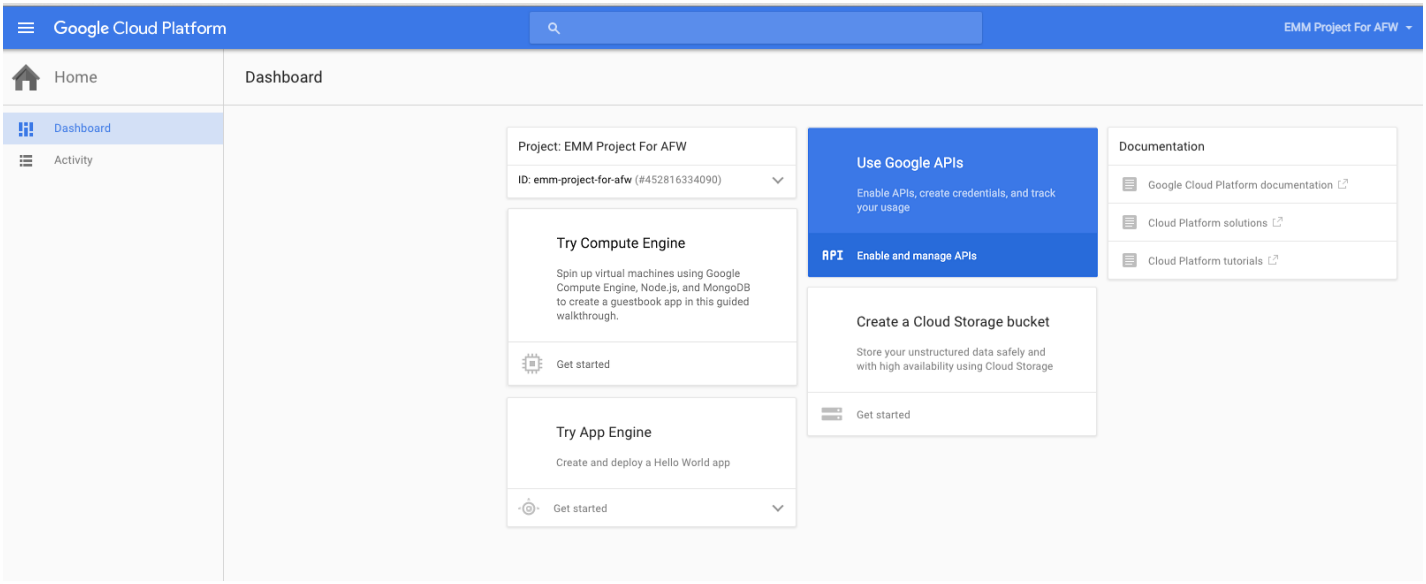
2. 2. Klicken Sie in der Liste **Projects** auf **Create project**.



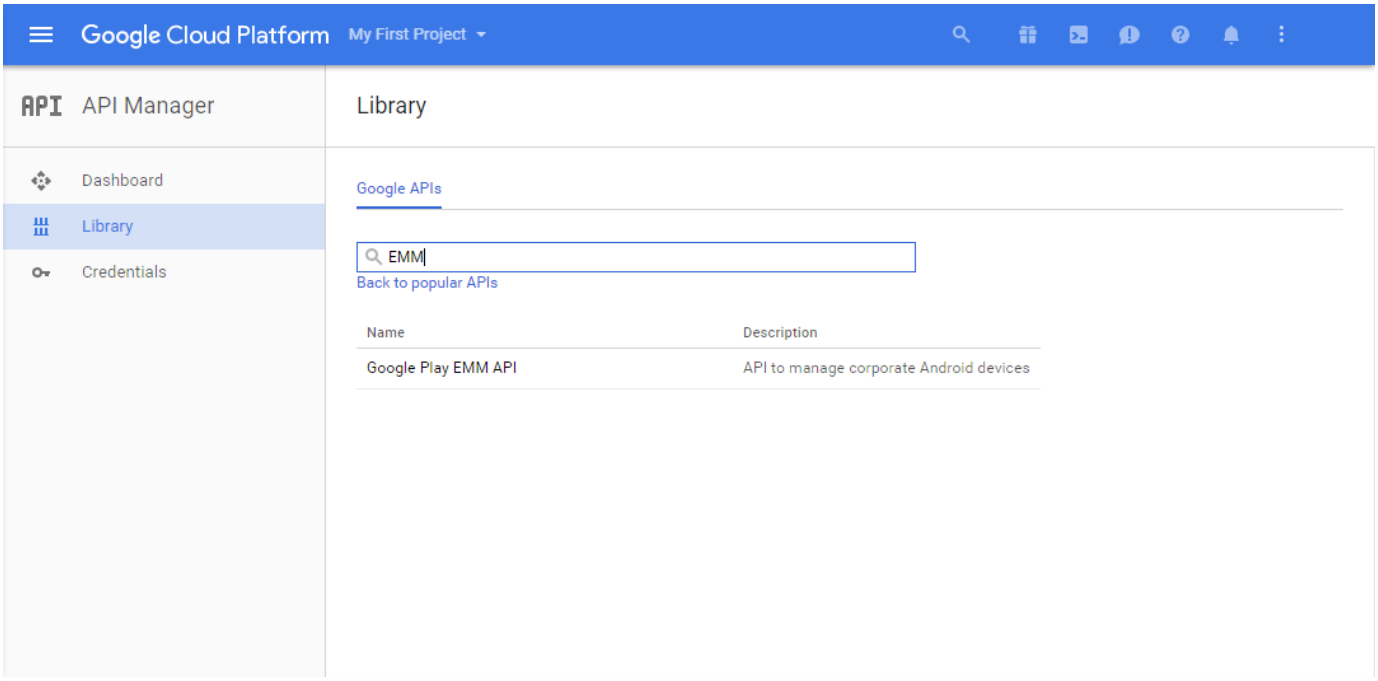
3. 3. Geben Sie unter **Project name** einen Namen für das Projekt ein.



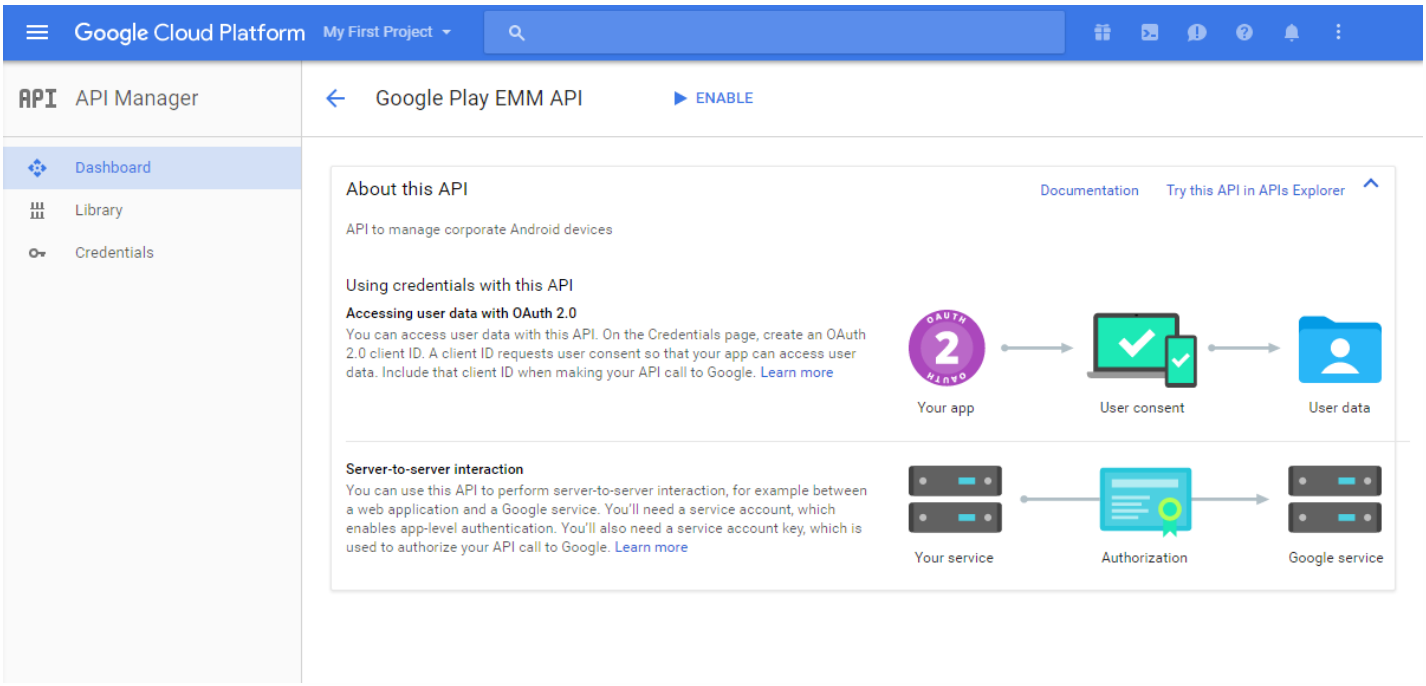
4. Klicken Sie im Dashboard auf **Use Google APIs**.



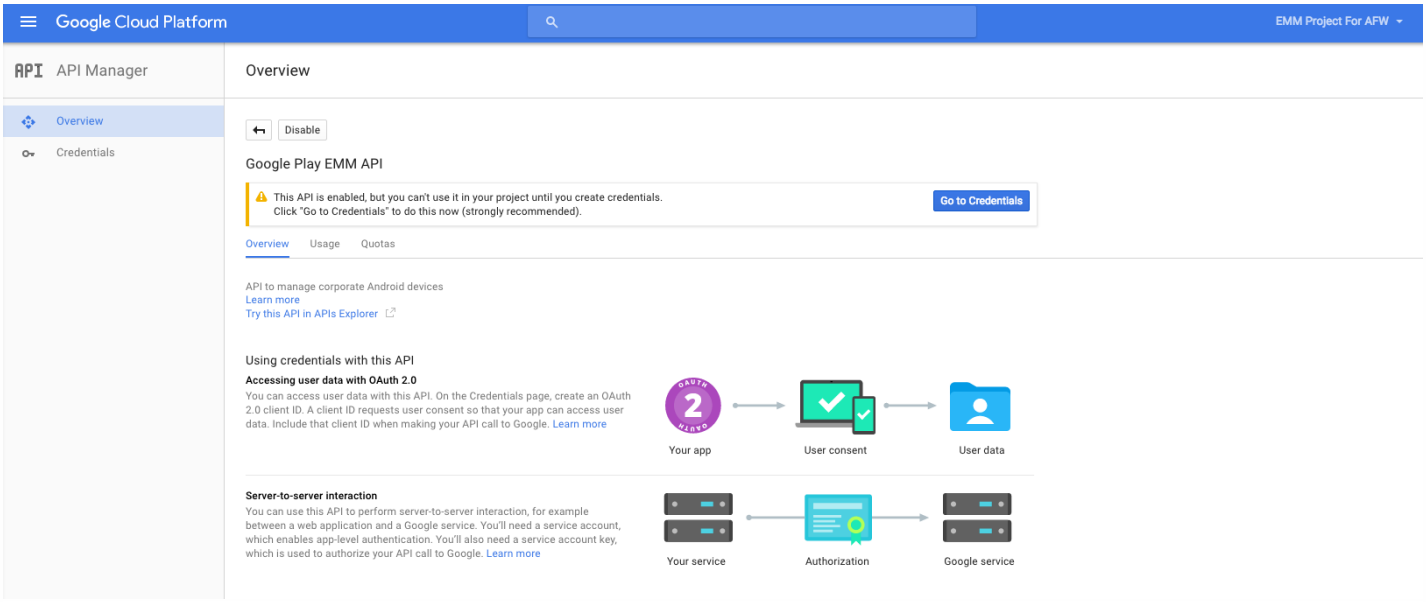
5. Klicken Sie auf **Library** geben Sie für **Search EMM** ein und klicken Sie auf das Suchergebnis.



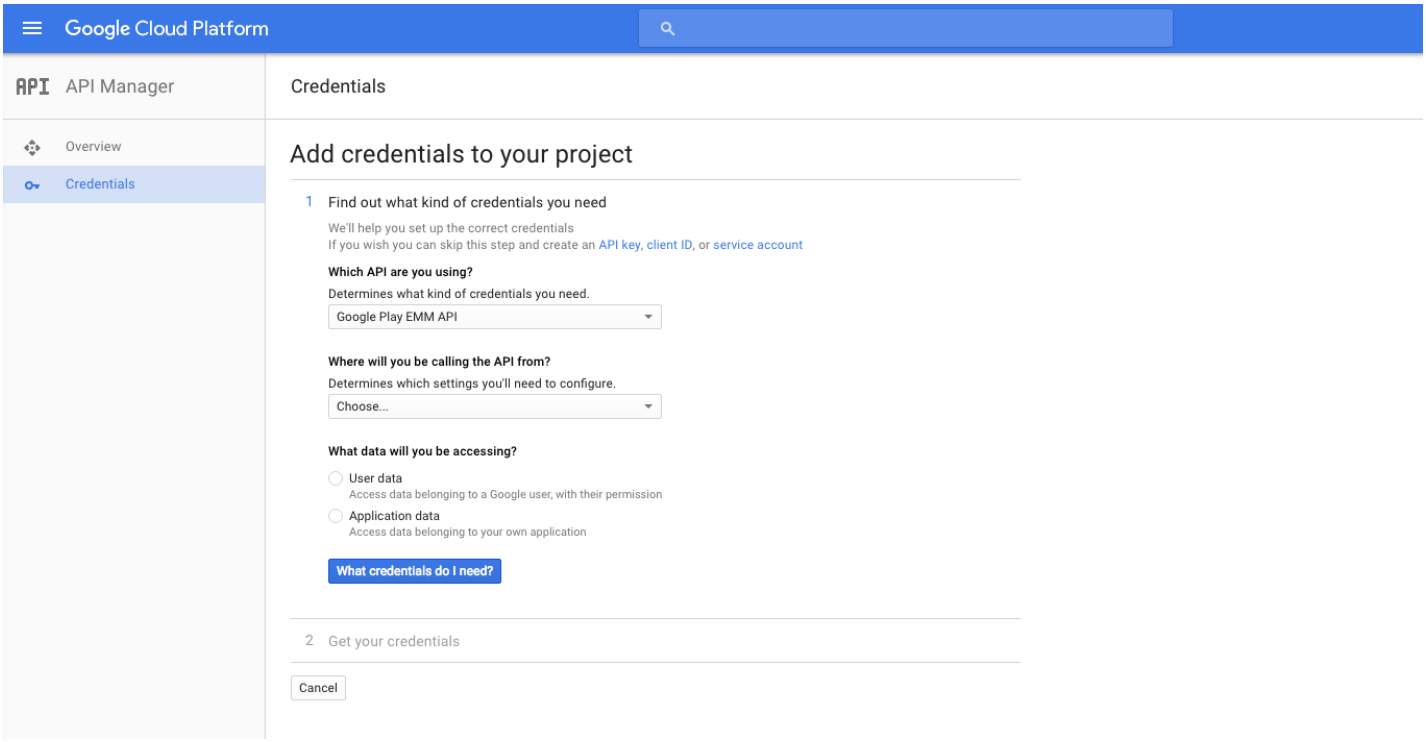
6. Klicken Sie auf der Seite **Overview** auf **Enable**.



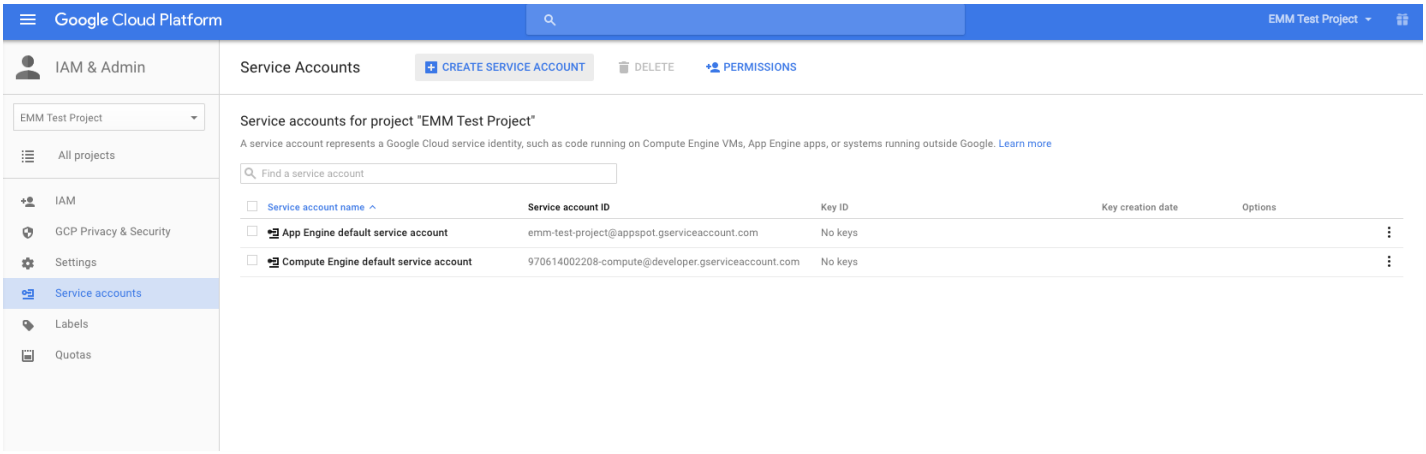
7. Klicken Sie neben **Google Play EMM API** auf **Go to Credentials**.



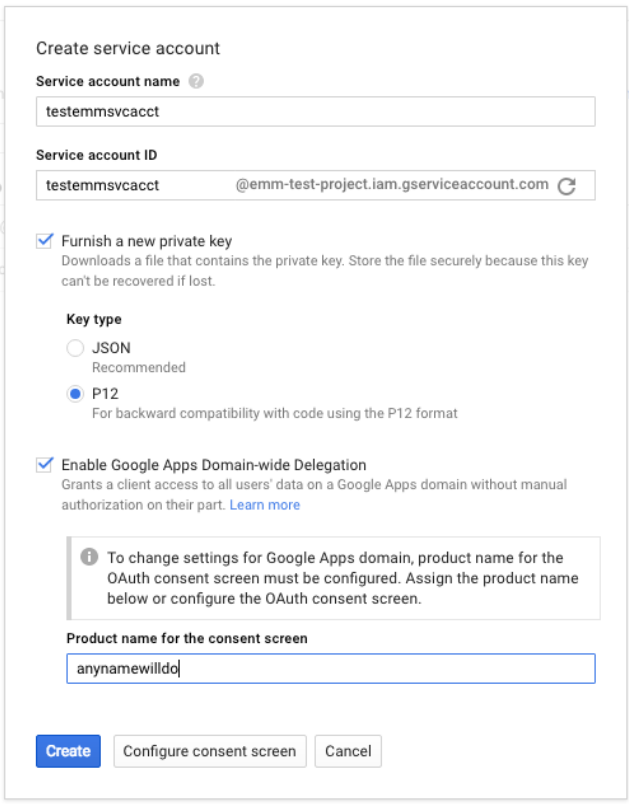
8. Klicken Sie in der Liste **Add credentials to our project** unter Schritt 1 auf **service account**.



9. Klicken Sie auf der Seite **Service Accounts** auf **Create Service Account**.

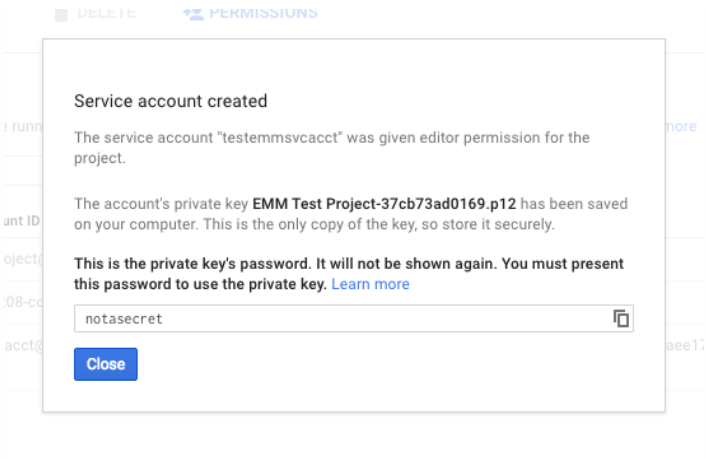


10. Geben Sie unter **Create service account** einen Namen für das Konto ein und aktivieren Sie das Kontrollkästchen **Furnish a new private key**. Klicken Sie auf **P12**, aktivieren Sie das Kontrollkästchen **Enable Google Apps Domain-wide Delegation** und klicken Sie auf **Create**.

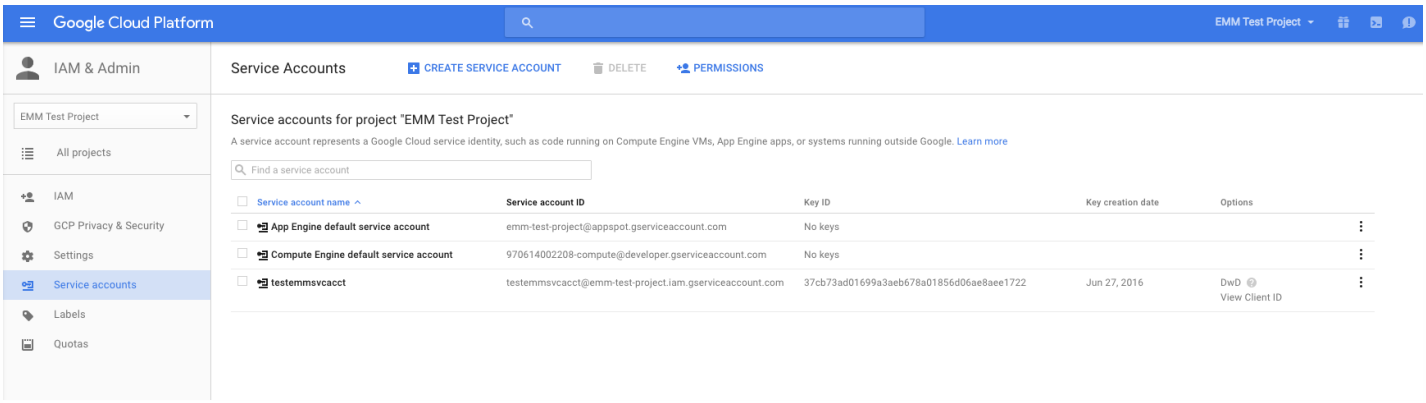


Die Zertifikatdatei (P12-Datei) wird auf Ihren Computer heruntergeladen. Speichern Sie das Zertifikat an einem sicheren Ort.

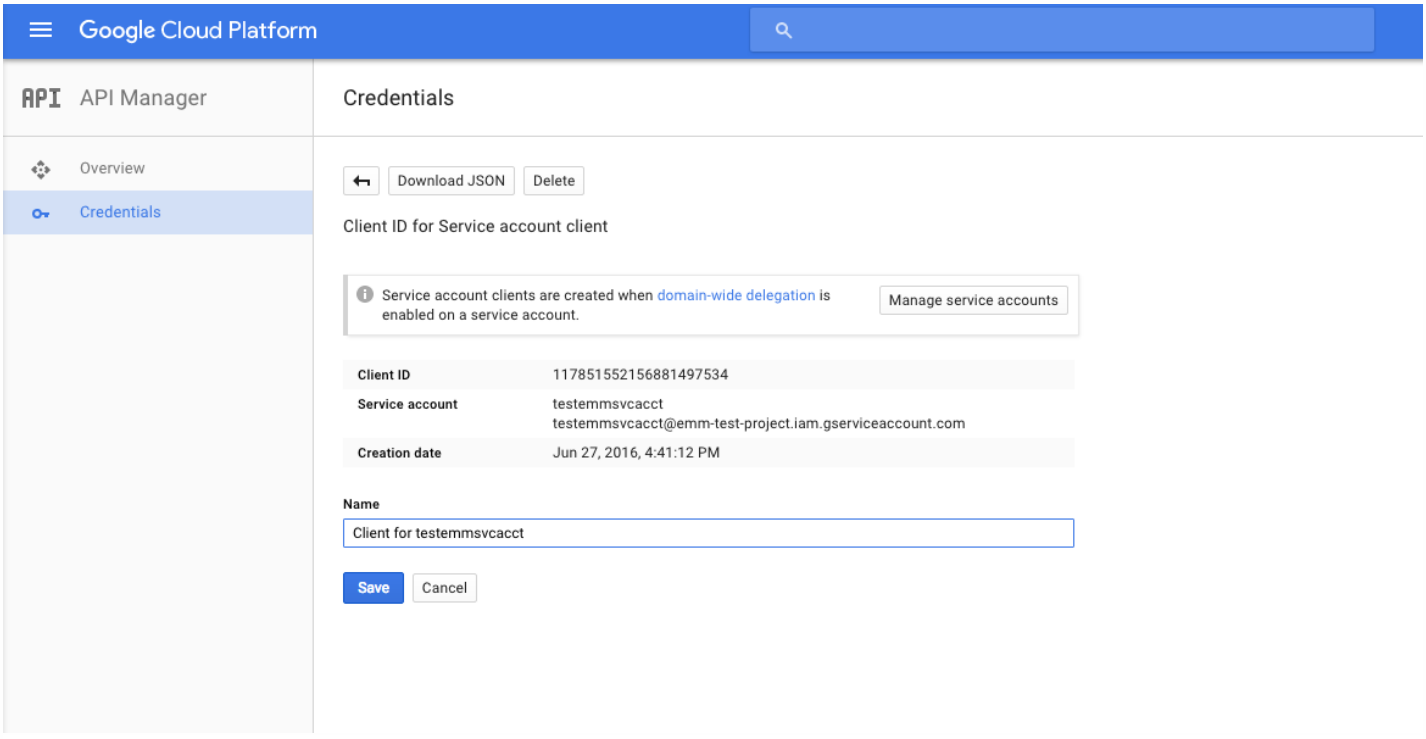
11. Klicken Sie auf der Seite **Service account created** auf **Close**.



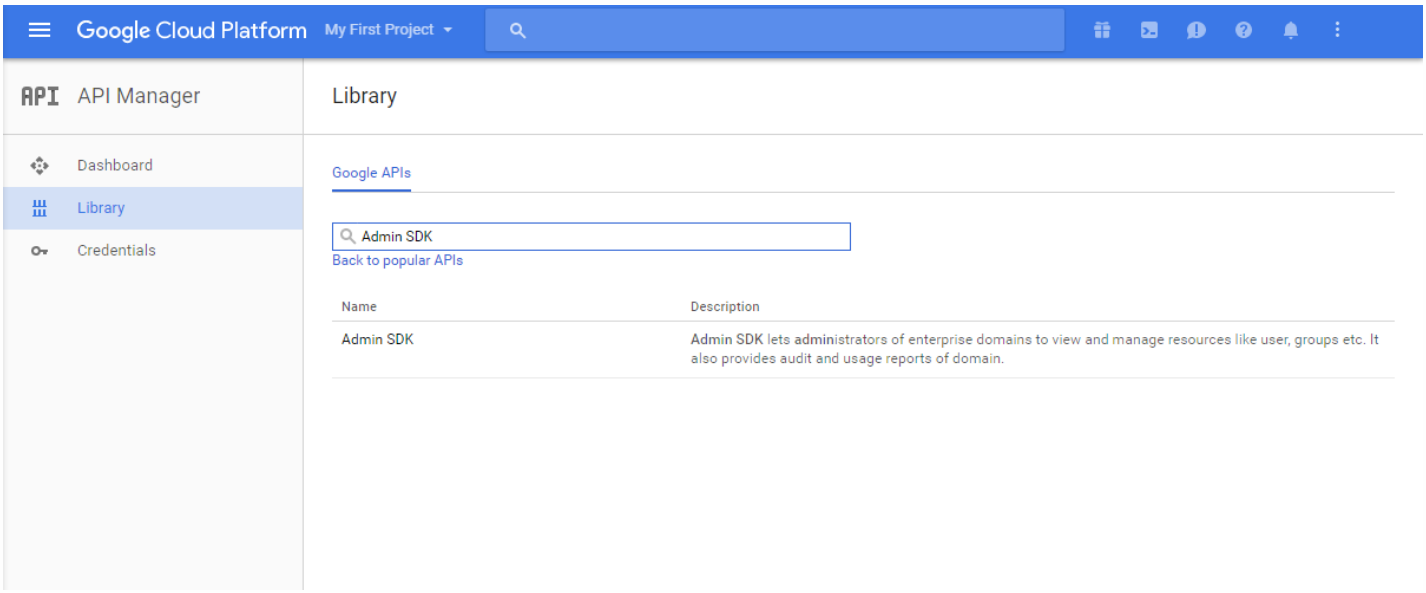
12. Klicken Sie unter **Permissions** auf **Service accounts** und dann unter **Options** für Ihr Dienstkonto auf **View Client ID**.



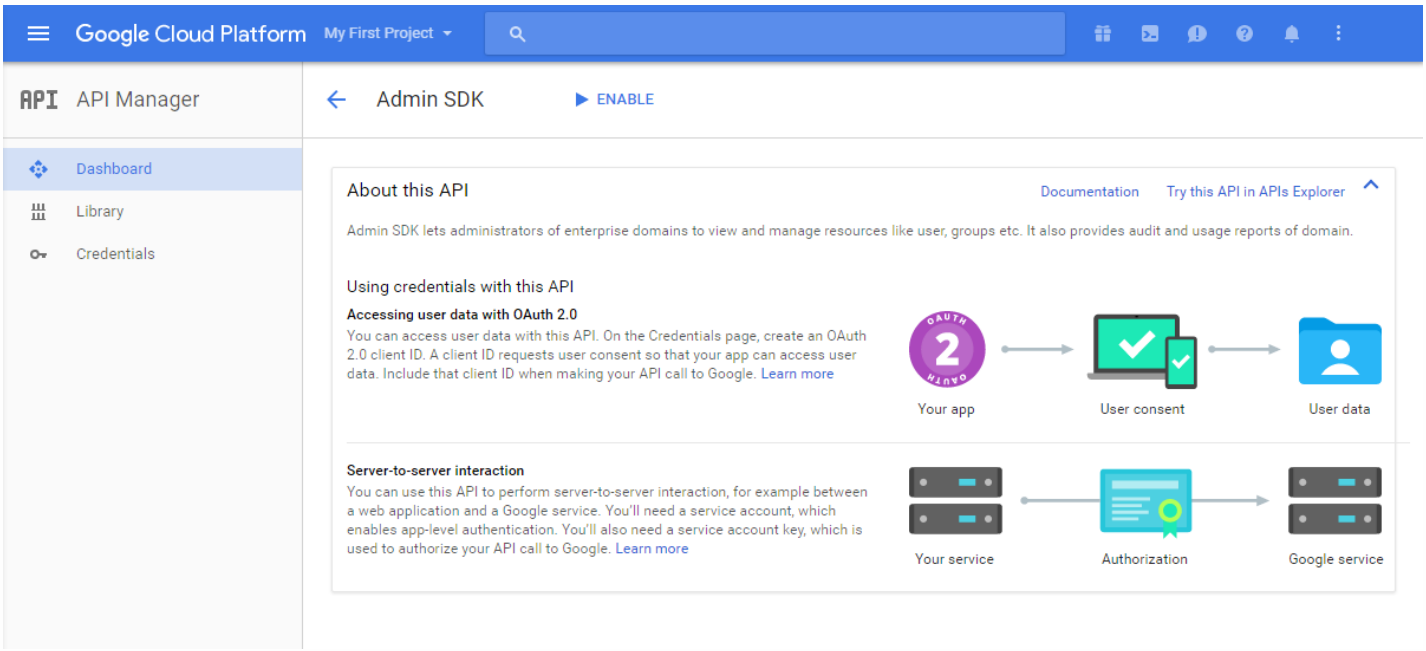
13. Die für die Kontoautorisierung auf der Google Admin Console erforderlichen Informationen werden angezeigt. Kopieren Sie die Client ID und Service account ID in einen Speicherort, um sie später von dort abzurufen. Sie müssen diese Informationen mit dem Domänennamen an den Citrix Support senden, damit sie auf eine Positivliste gesetzt werden.



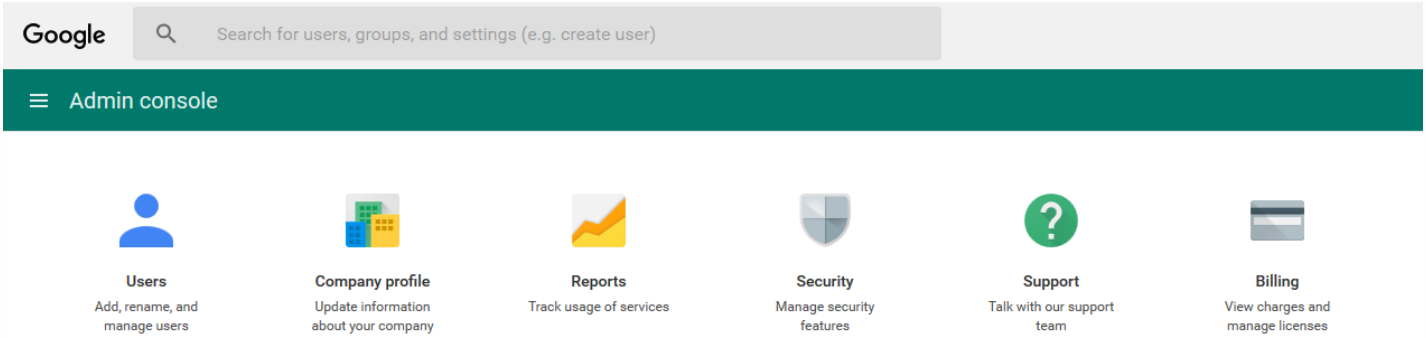
14. Suchen Sie auf der Seite **Library** den Eintrag **Admin SDK** und klicken Sie auf das Suchergebnis.



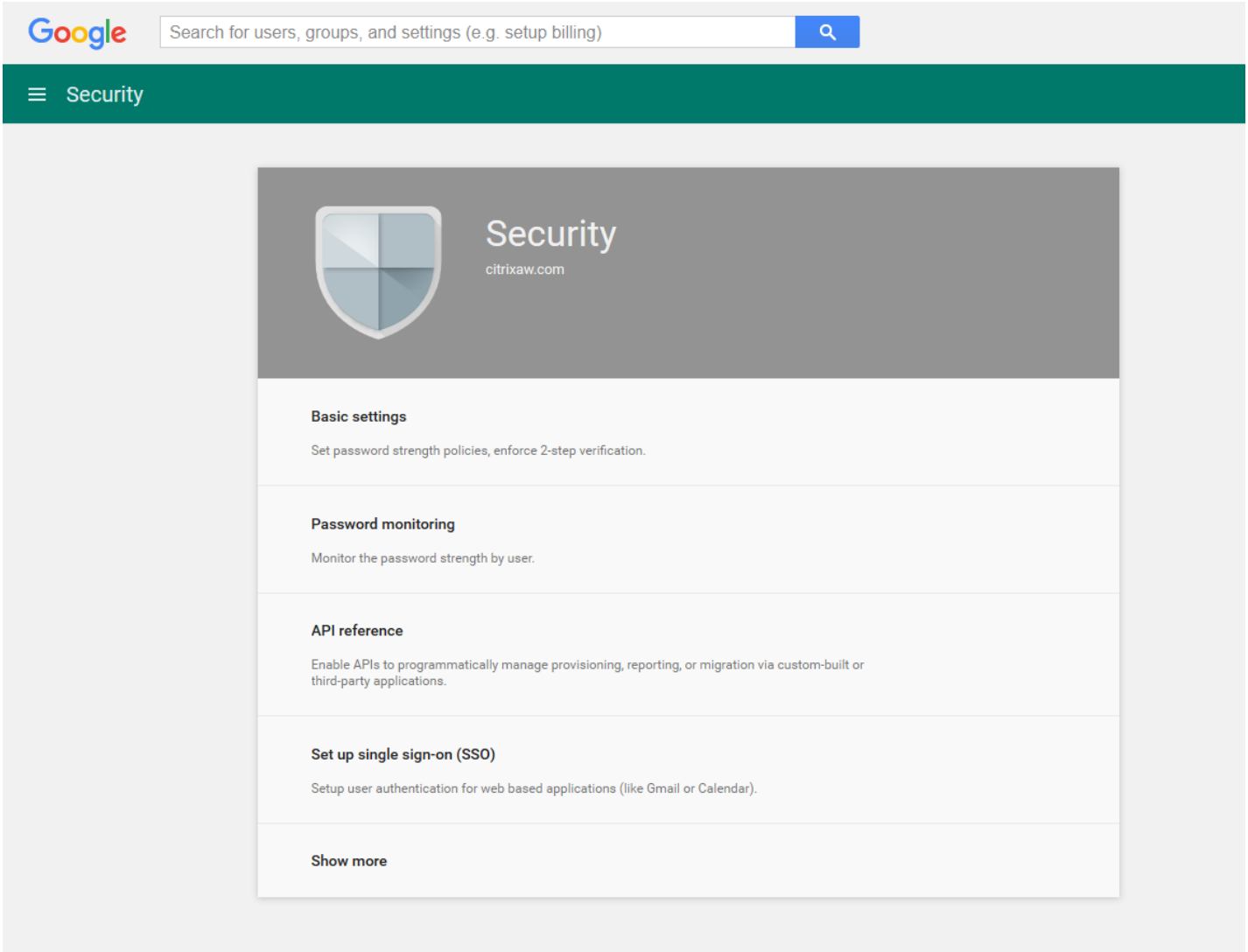
15. Klicken Sie auf der Seite **Overview** auf **Enable**.

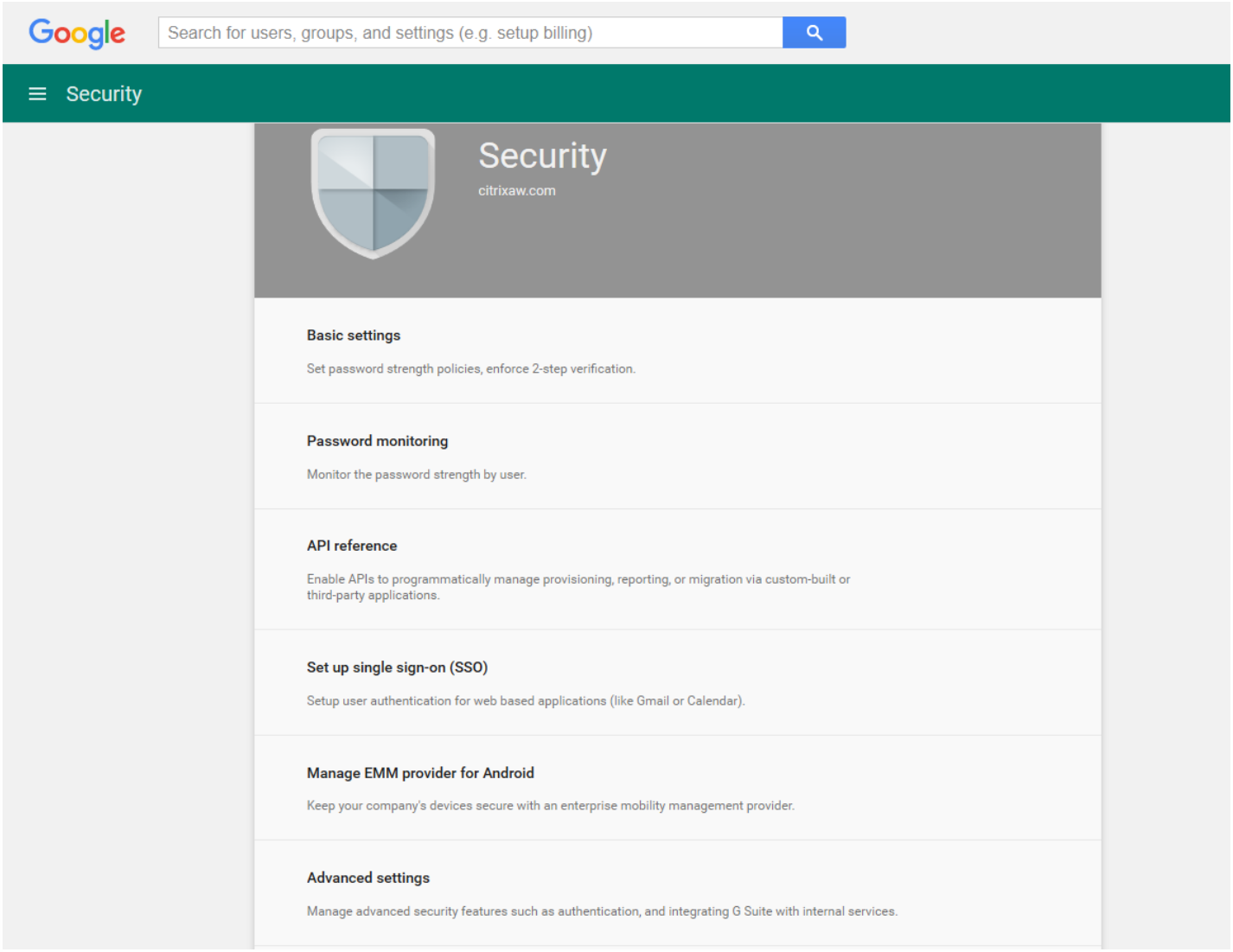


16. Öffnen Sie die Google Admin Console für Ihre Domäne und klicken Sie auf **Security**.

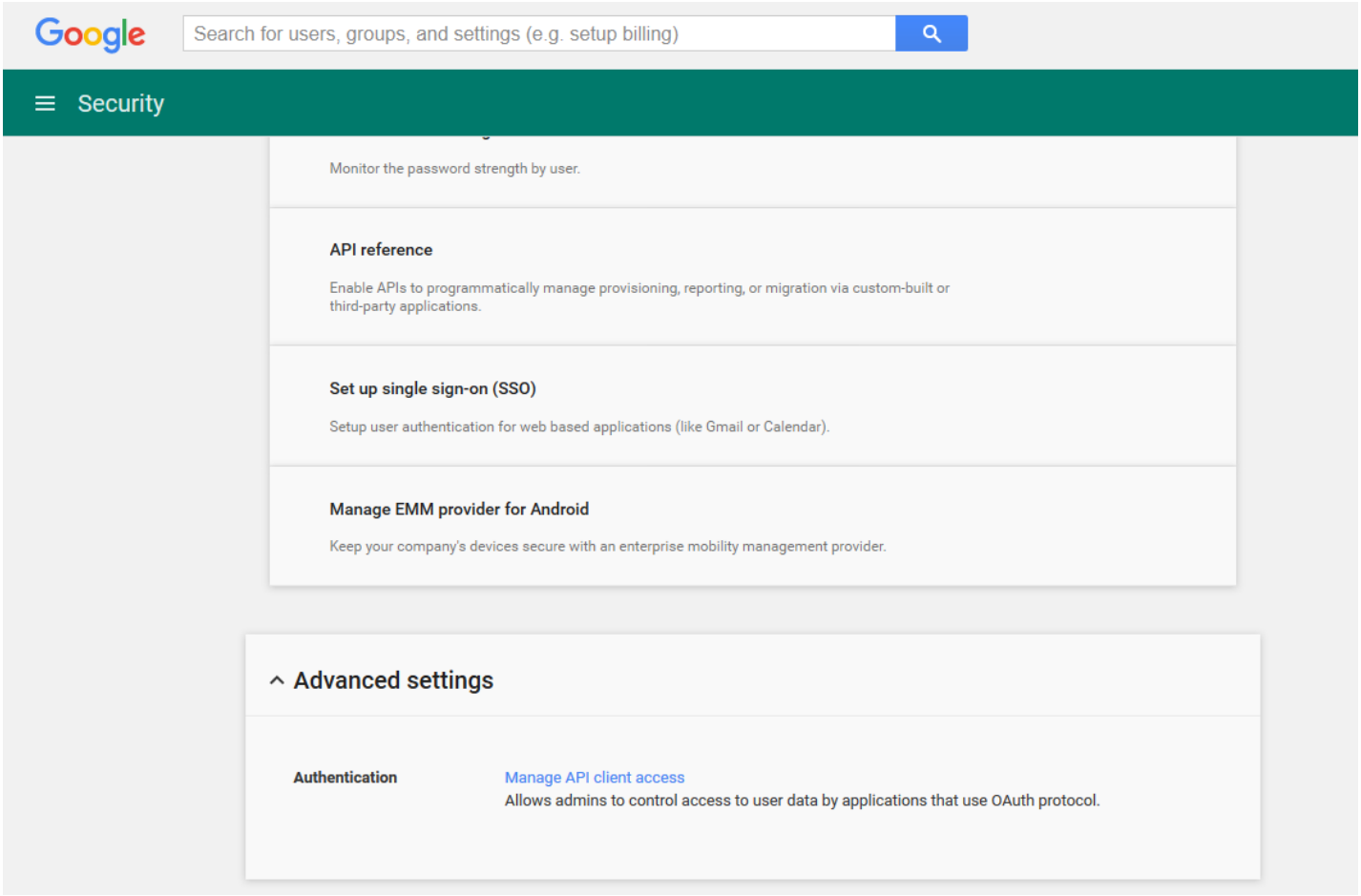


17. Klicken Sie auf der Seite **Settings** auf **Show more** und dann auf **Advanced settings**.

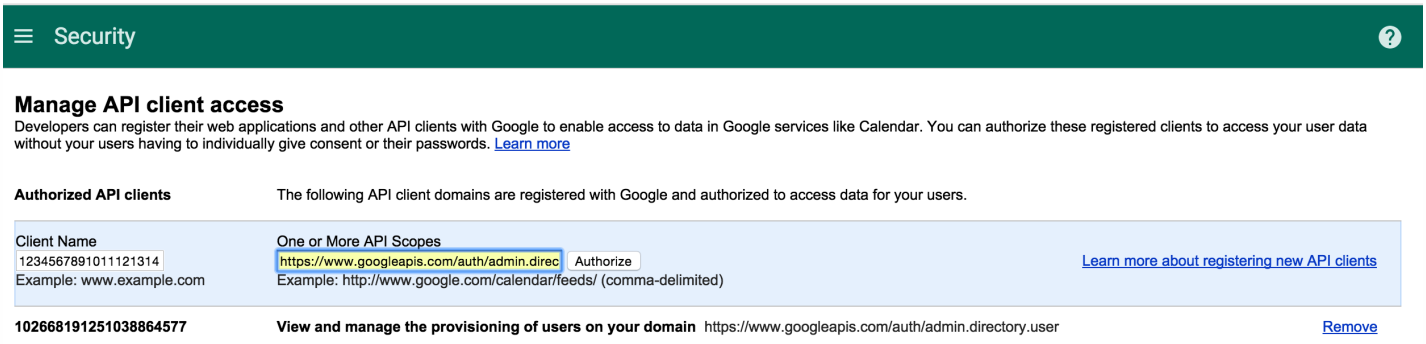




18. 4. Klicken Sie auf **Manage API client access**.



19. 17. 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**.



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). Kontaktinformationen für den technischen Support von Citrix finden Sie unter Technischer Support von Citrix.

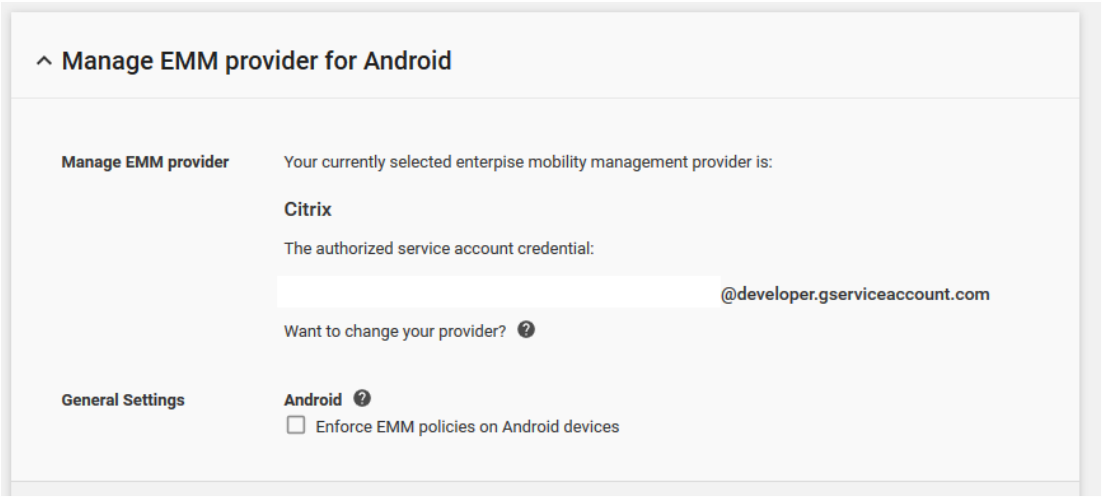
1. Zum Überprüfen der Bindung melden Sie sich beim Google-Verwaltungsportal an und klicken Sie auf **Security**.

2. Klicken Sie auf **Manage EMM provider for Android**.

Sie sehen dann, dass Ihr Android at Work-Konto bei Google nun an Citrix als EMM-Anbieter gebunden ist.

Nach der Prüfung der Tokenbindung können Sie XenMobile zum Verwalten der Android-Geräte verwenden. Importieren Sie das P12-Zertifikat, das Sie in

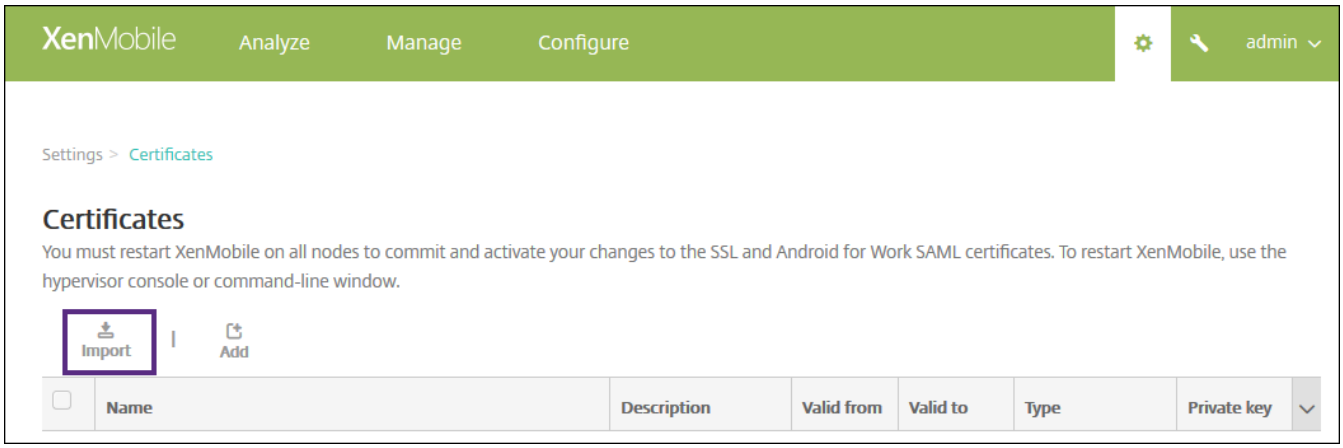
Schritt 14 erstellt haben. Richten Sie den Android at Work-Server ein, aktivieren Sie das SAML-basierte Single Sign-On und definieren Sie mindestens eine Android at Work-Richtlinie.



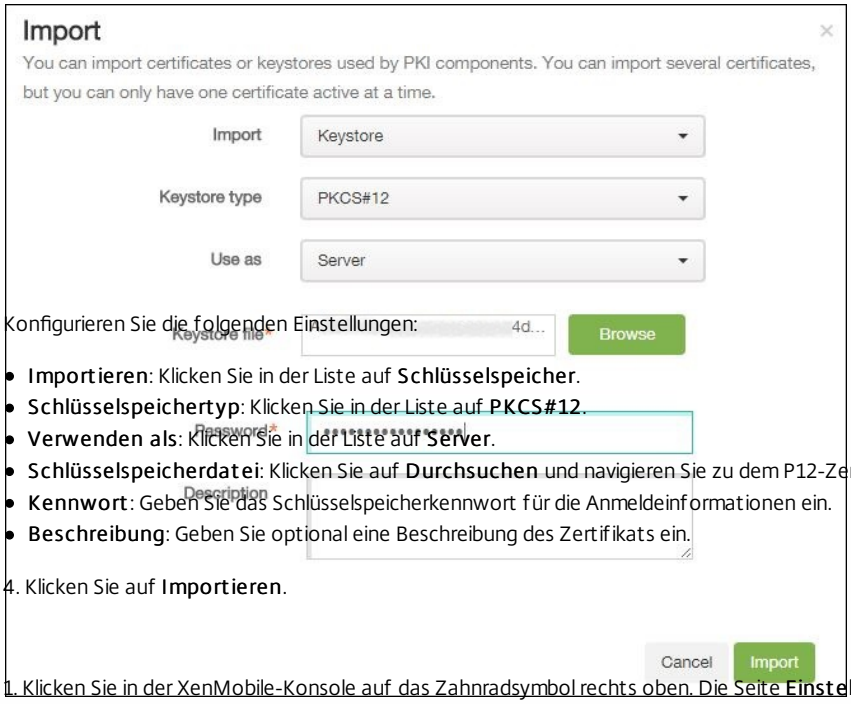
Führen Sie die folgenden Schritte zum Importieren des Android at Work-P12-Zertifikats aus:

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 **Importieren** wird angezeigt.



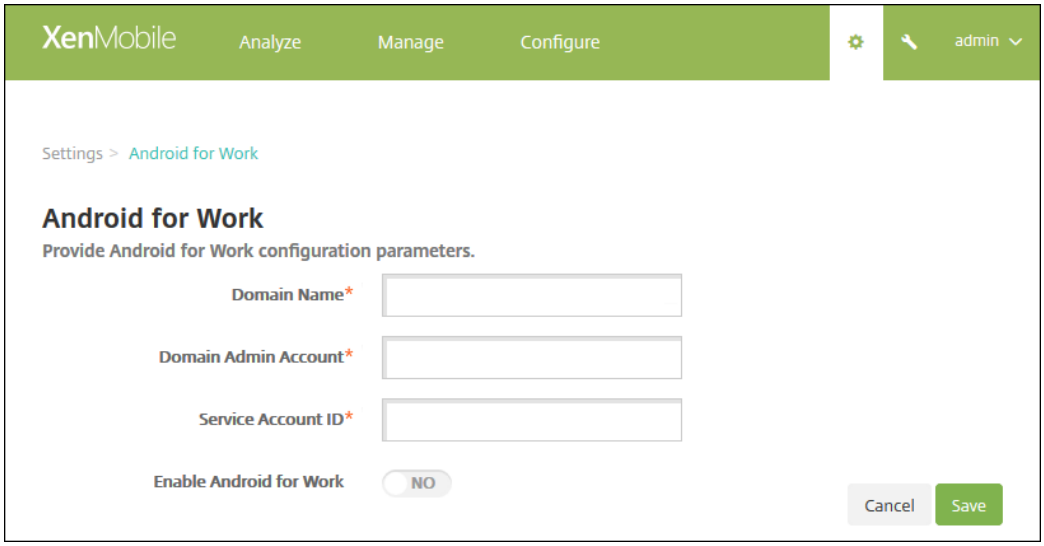
Konfigurieren Sie die folgenden Einstellungen:

- **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**.

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 at 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 (dienstkontoemail@xxxxxxxxx.iam.gserviceaccount.com).

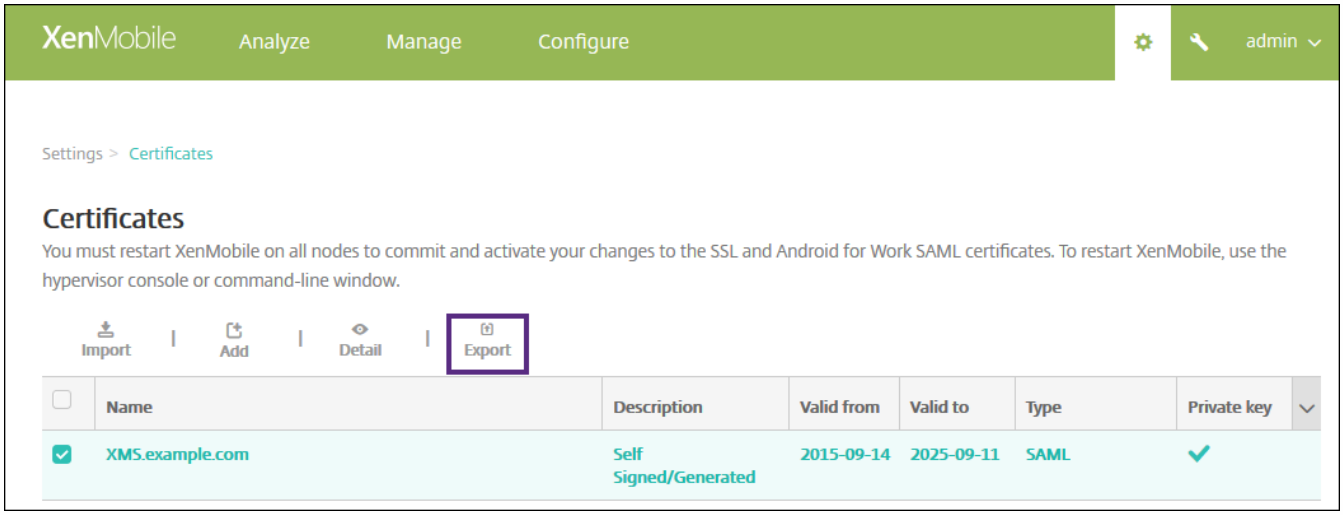
- **Android for Work aktivieren**: Klicken Sie zum Aktivieren oder Deaktivieren auf diese Option.

3. Klicken Sie auf **Speichern**.

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

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

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

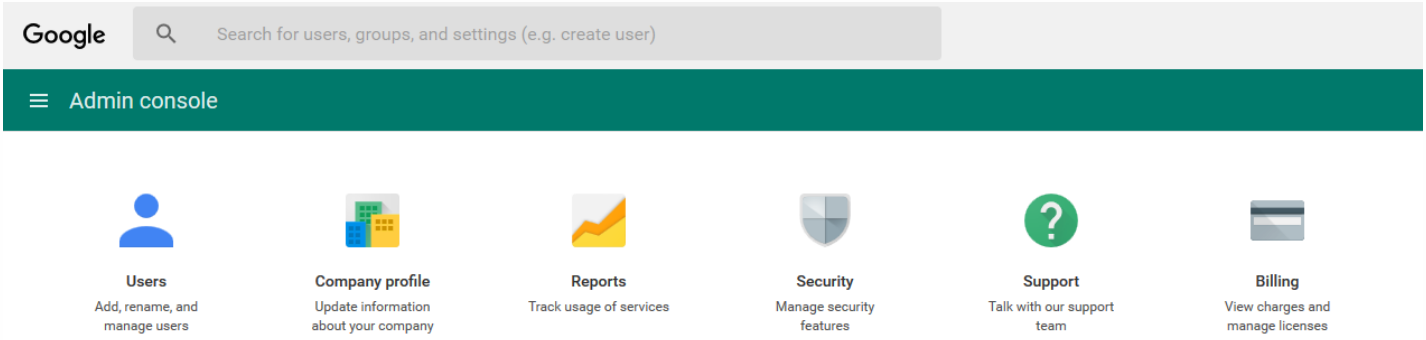


3. Klicken Sie in der Liste der Zertifikate auf das SAML-Zertifikat.

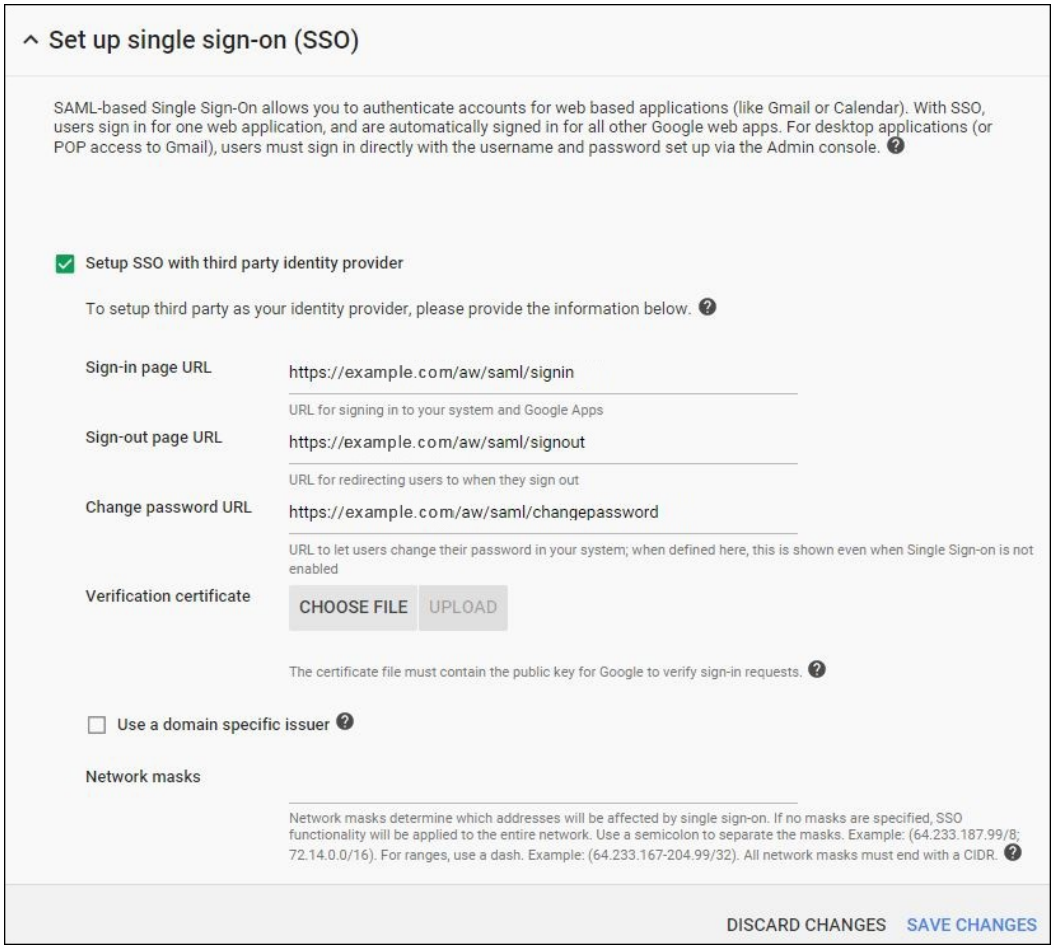
4. Klicken Sie auf **Exportieren** und speichern Sie das Zertifikat auf Ihrem Computer.

5. Melden Sie sich beim Google-Verwaltungsportal mit Ihren Android at Work-Administratoranmeldeinformationen an. Informationen zum Zugriff auf das Portal finden Sie unter Google-Verwaltungsportal.

6. Klicken Sie auf **Security**.



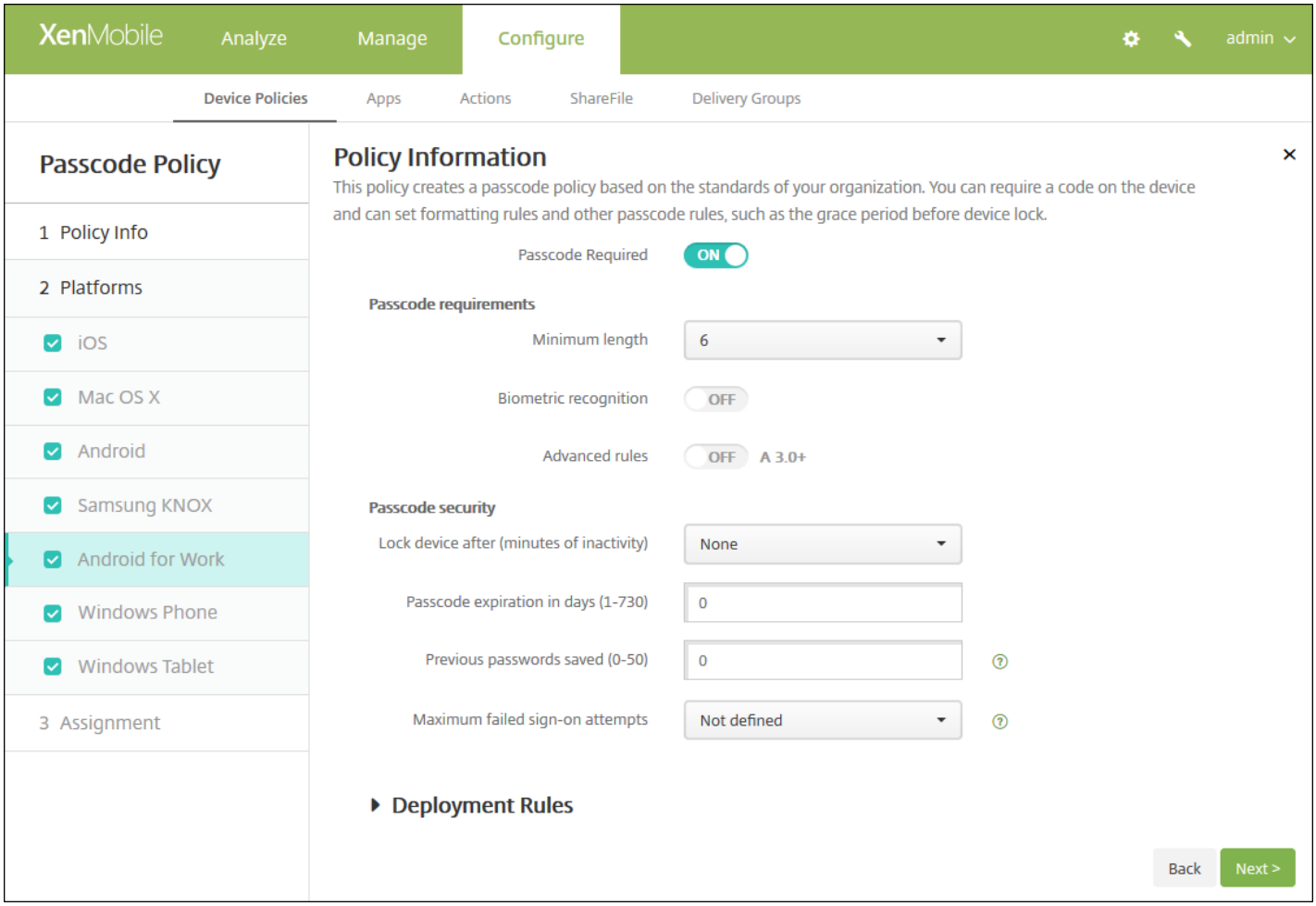
7. Klicken Sie unter **Security** auf **Set up single sign-on (SSO)** und konfigurieren Sie die folgenden Einstellungen:



- **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 dieses Feld definiert wird, wird diese Aufforderung für Benutzer angezeigt, 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**, um die Änderungen zu speichern.

Es empfiehlt sich die Einrichtung einer Passcode-Richtlinie, sodass Benutzer bei der ersten Registrierung einen Passcode auf ihrem Gerät festlegen müssen.



Grundlegende Schritte zum Einrichten einer Geräterichtlinie:

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

2. Klicken Sie auf **Konfigurieren** und dann auf **Geräterichtlinien**.

3. Klicken Sie auf **Hinzufügen** und wählen Sie dann im Dialogfeld **Neue Richtlinie hinzufügen** die Richtlinie aus, die Sie hinzufügen möchten. Klicken Sie 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.

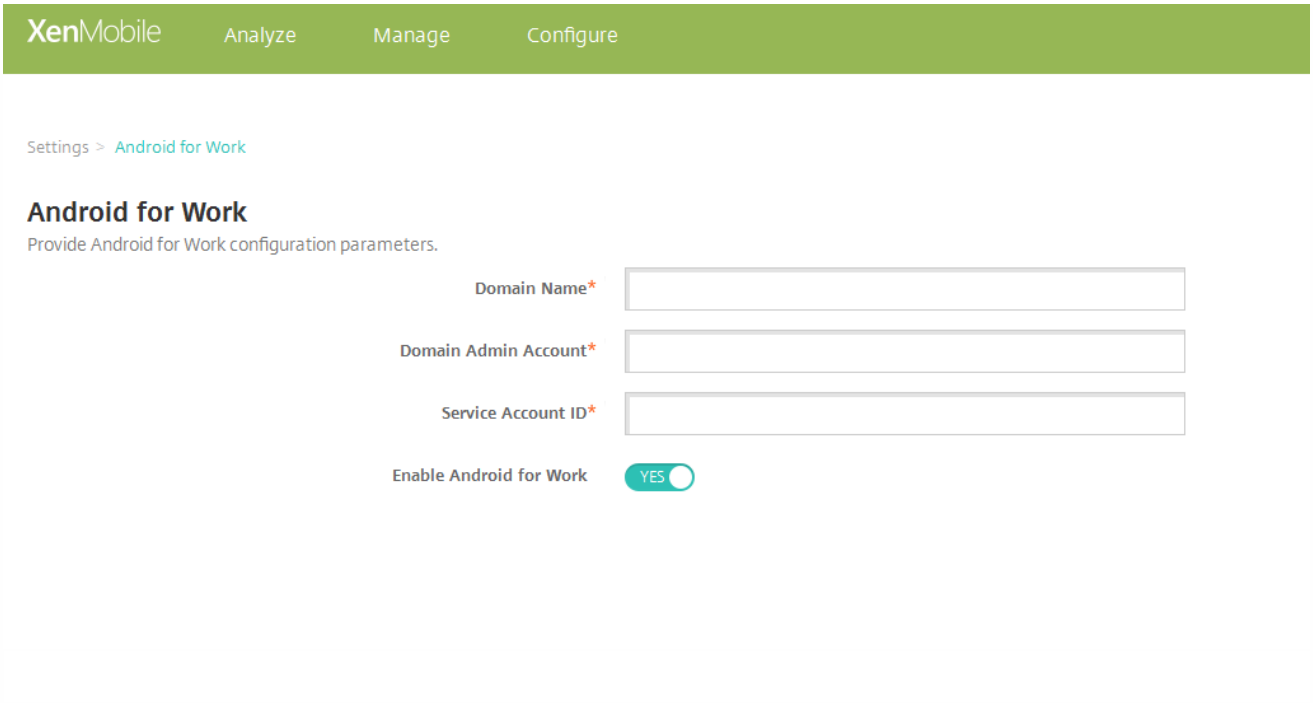
Weitere Informationen zum Einrichten von anderen Geräterichtlinien für Android for Work finden Sie unter XenMobile-Geräterichtlinien nach Plattform.

Konfigurieren von Android at Work-Kontoeinstellungen

Bevor Sie Android-Apps und Richtlinien auf Benutzergeräten verwalten können, müssen Sie eine Domäne und Kontoinformationen für Android at Work in XenMobile einrichten. Zunächst müssen Sie Android at Work-Einrichtungsaufgaben auf Google zum Einrichten eines Domänenadministrators erledigen und eine Dienstkonten-ID sowie ein Bindungstoken anfordern.

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 Konfigurationsseite **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 im Gerätebesitzermodus bei Android at Work

Wenn Sie Android at Work im Gerätebesitzermodus bereitstellen möchten, müssen Sie Daten per NFC (Near Field Communication) zwischen zwei Geräten übertragen. Auf dem einen Gerät muss das XenMobile Provisioning Tool ausgeführt werden, das andere muss auf die Werkseinstellungen zurückgesetzt werden. Der Gerätebesitzermodus ist nur für Unternehmensgeräte verfügbar.

Gründe für den Einsatz von NFC Bluetooth, WiFi und andere Kommunikationsmodi sind auf einem Gerät mit Werkseinstellungen deaktiviert. NFC ist das einzige Kommunikationsprotokoll, das das Gerät in diesem Zustand verwenden kann.

Voraussetzungen

- Eine XenMobile Server-Version 10.4, die für Android at Work aktiviert ist.
- Ein auf die Werkseinstellungen zurückgesetztes Gerät, das für Android at Work im Gerätebesitzermodus bereitgestellt wurde. Das Verfahren hierfür finden Sie weiter unten in diesem Artikel.
- Ein Gerät mit NFC-Funktion, auf dem das konfigurierte Provisioning Tool ausgeführt wird. Das Provisioning Tool ist in Secure Hub 10.3 und auf der Citrix Downloadseite verfügbar.

Jedes Gerät kann nur ein Android at Work-Profil haben, das von einer Enterprise Mobility Management-App (EMM) verwaltet wird. In XenMobile ist Secure Hub die EMM-App. Nur ein Profil ist pro Gerät zulässig. Wenn Sie versuchen, eine zweite EMM-App hinzuzufügen, wird die erste entfernt.

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 at Work initialisiert wird:

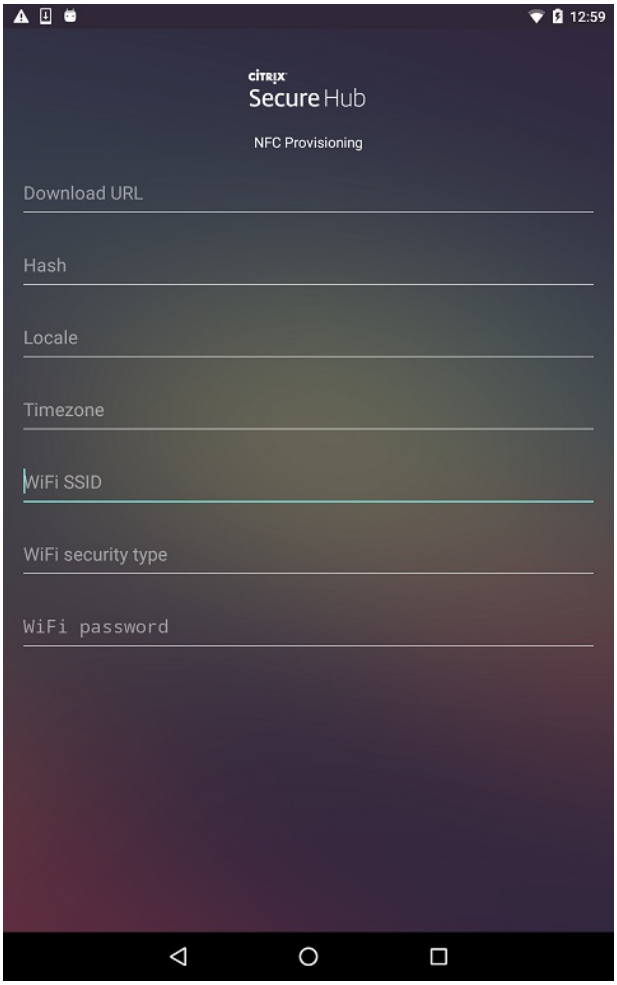
- Paketname der EMM-Anbieter-App, die als Gerätebesitzer (in diesem Fall Secure Hub) fungiert.
- Intranet-/Internetspeicherort, von dem das Gerät die EMM-Anbieter-App herunterlädt.

- SHA-1-Hash der EMM-Anbieter-App, um zu überprüfen, ob der Download erfolgreich ist.
- WiFi-Verbindungsdetails, sodass ein auf Werkseinstellungen zurückgesetztes Gerät eine Verbindung herstellen und die EMM-Anbieter-App herunterladen kann. Hinweis: Android unterstützt für diesen Schritt nicht 802.1x.
- Zeitzone für das Gerät (optional).
- Geografischer Standort des Geräts (optional).

Wenn die beiden Geräte eine Verbindung herstellen, werden die Daten vom Provisioning Tool an das Gerät mit den Werkseinstellungen gesendet. Diese Daten werden dann zum Download von Secure Hub mit Administratoreinstellungen verwendet. Wenn Sie keine Werte für Zeitzone und Speicherort eingeben, konfiguriert Android sie automatisch auf dem neuen Gerät.

Konfigurieren des XenMobile Provisioning Tools

Bevor Sie Daten per NFC übertragen können, müssen Sie das 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. Nachfolgend wird beschrieben, wie Sie die Textdatei konfigurieren und welche Felder diese enthält. Die App speichert die eingegebenen Informationen nicht. Erstellen Sie daher eine Textdatei zur Aufbewahrung der Informationen.

Konfigurieren des Provisioning Tools mit einer Textdatei

Nennen Sie die Datei nfcprovisioning.txt und speichern Sie sie auf der SD-Karte des Geräts im Ordner /sdcard/. 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 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. Sie wird verwendet, um zu prüfen, ob der Download erfolgreich ist. Das Verfahren zum Abrufen der Prüfsumme wird weiter unten in diesem Artikel beschrieben.

android.app.extra.PROVISIONING_WIFI_SSID=
Dies ist die WiFi-SSID des Geräts, auf dem das 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 den Sprach- und den Ländercode 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 keinen Länder- und Sprachcode eingeben, werden diese Felder automatisch ausgefüllt.

android.app.extra.PROVISIONING_TIME_ZONE=
Die Zeitzone, in dem 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 "Secure Hub" hartcodiert ist. Er wird hier nur der Vollständigkeit halber angegeben.

Bei einem mit WPA2 geschützten WiFi könnte die Datei nfcprovisioning.txt wie folgt aussehen:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u003d
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
android.app.extra.PROVISIONING_LOCALE=en_US
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Bei einem ungeschützten WiFi könnte die Datei nfcprovisioning.txt wie folgt aussehen:

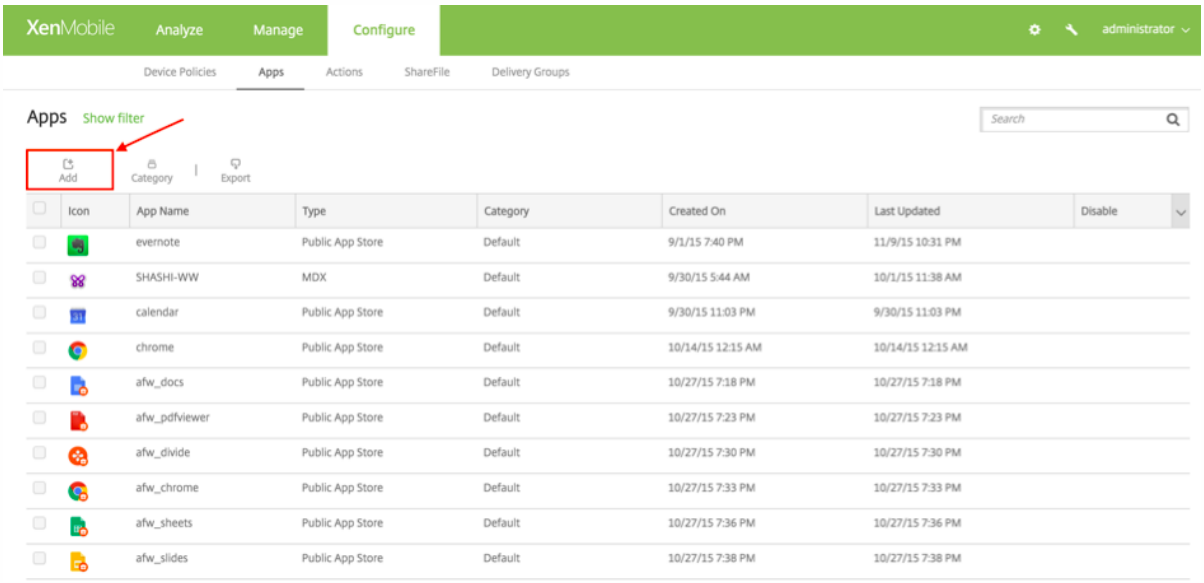
```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u003d
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
android.app.extra.PROVISIONING_LOCALE=en_US
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Abrufen der Secure Hub-Prüfsumme

Wenn Sie die Prüfsumme einer App abrufen möchten, fügen Sie die App als Unternehmensapp hinzu.

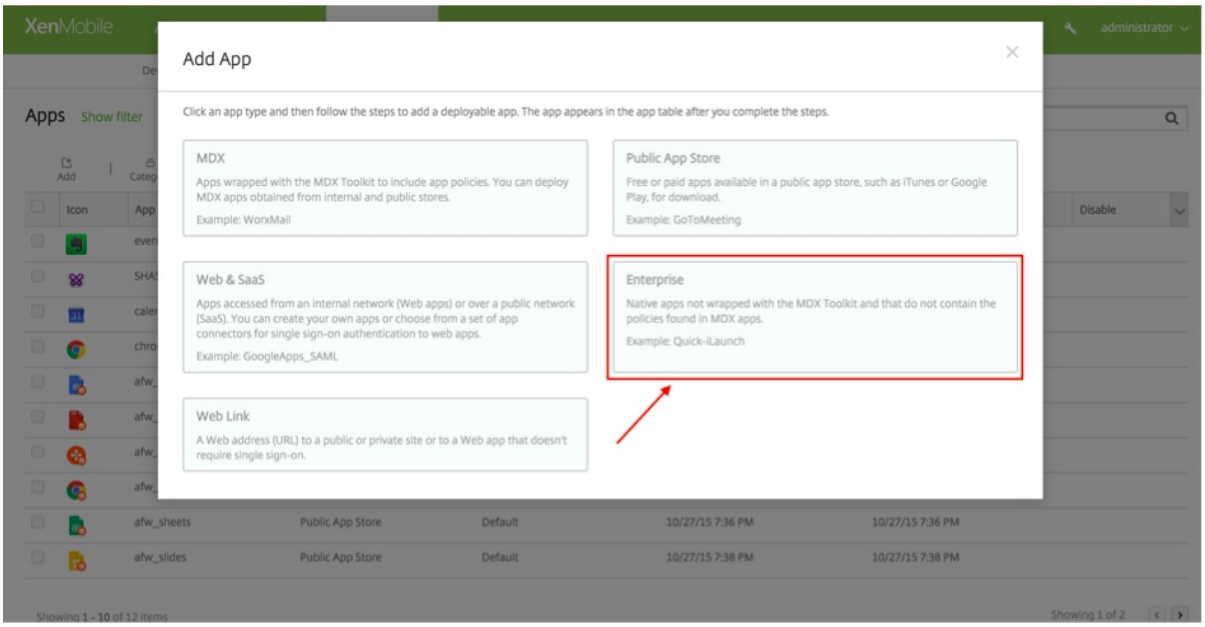
1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren** > **Apps** > **Hinzufügen**.

Das Fenster **App hinzufügen** wird angezeigt.



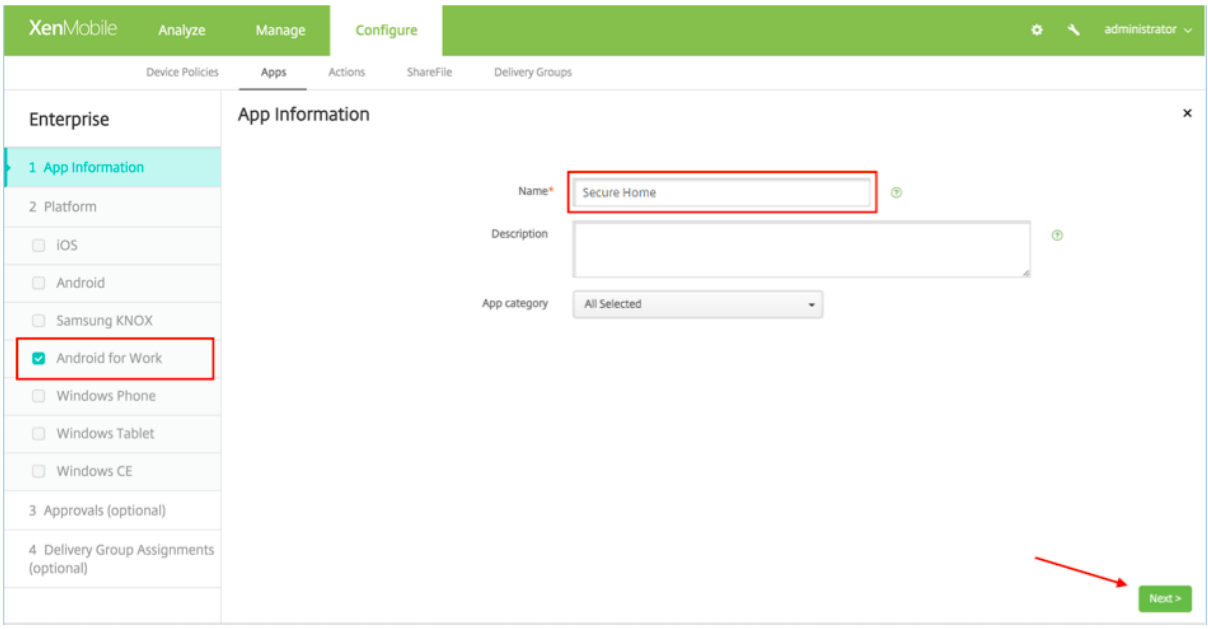
2. Klicken Sie auf **Enterprise**.

Die Seite **App-Informationen** wird angezeigt.

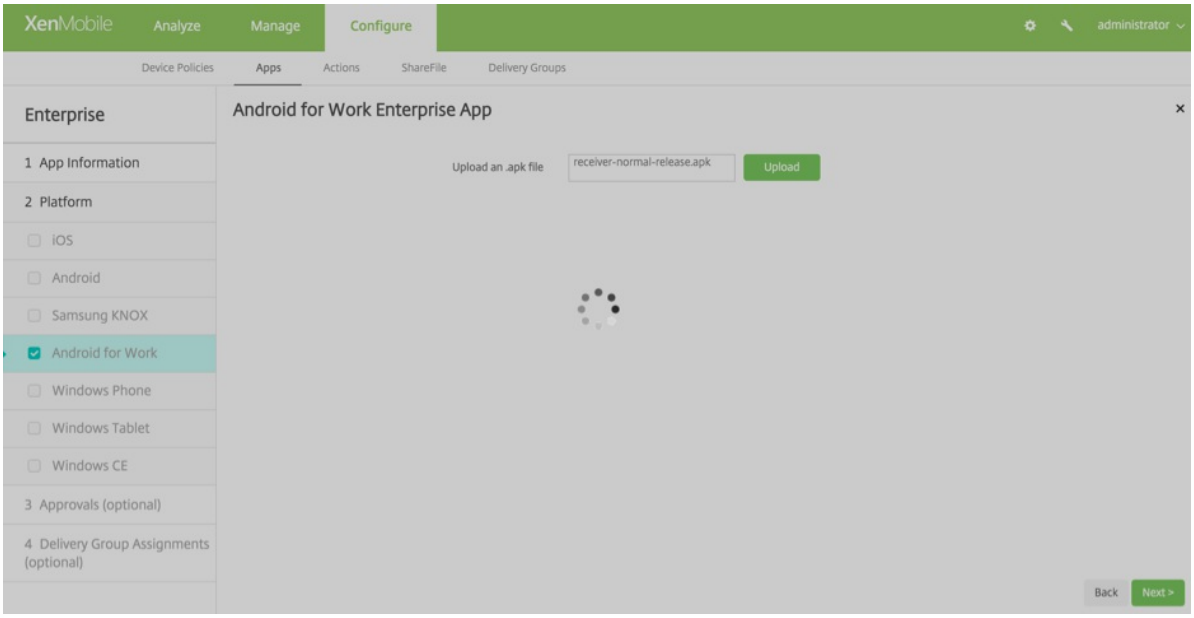


3. Wählen Sie die folgende Konfiguration und klicken Sie auf **Weiter**.

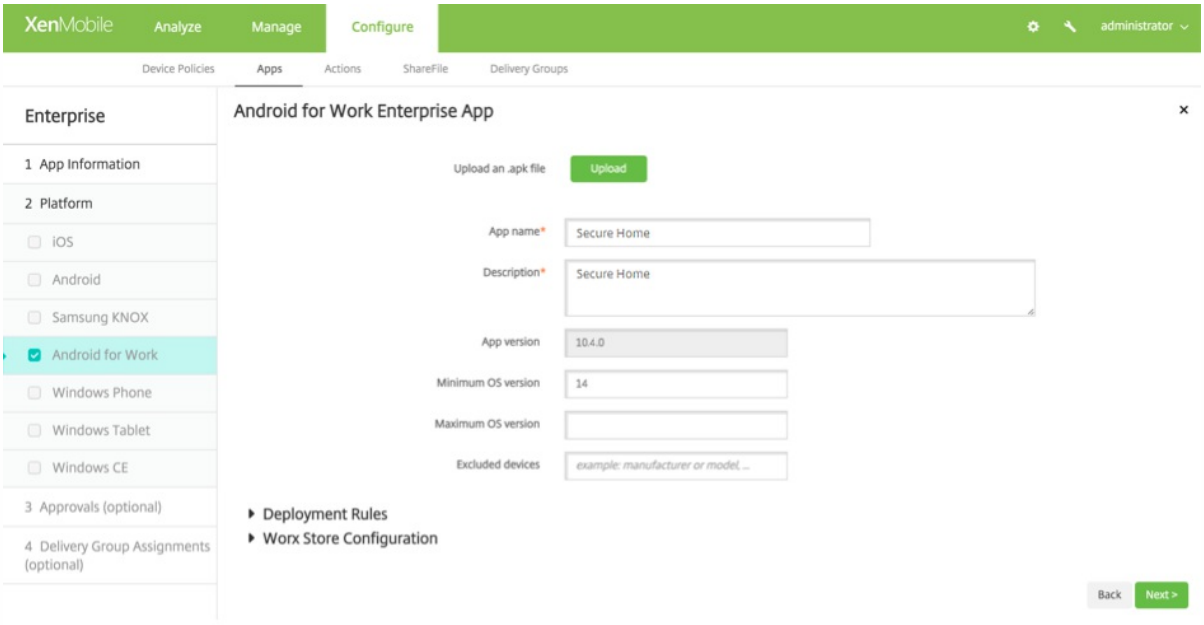
Die Seite **Android for Work-Unternehmensapp** wird angezeigt.



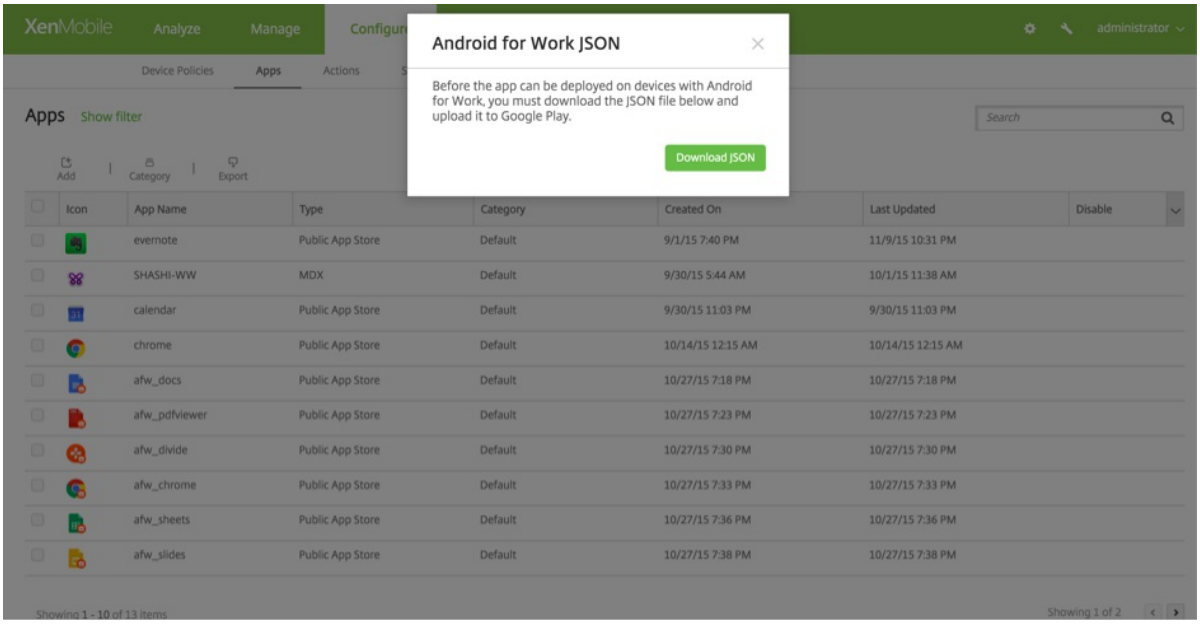
4. Geben Sie den Pfad für die APK-Datei an und klicken Sie auf **Weiter**, um die Datei hochzuladen.



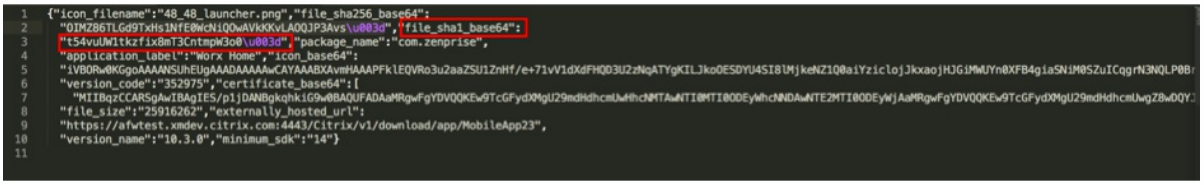
Wenn der Upload abgeschlossen ist, werden die Details des hochgeladenen Pakets angezeigt.



5. Klicken Sie auf **Weiter**, damit ein Bildschirm zum Herunterladen der JSON-Datei angezeigt wird, die Sie für den Upload in Google Play verwenden. Für Secure Hub ist kein Upload in Google Play erforderlich, aber Sie benötigen die JSON-Datei, um den SHA-1-Wert auszulesen.



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 Provisioning Tool ein. **Hinweis**: Der Hash-Wert muss URL-sicher sein.

- Konvertieren Sie alle **+** Zeichen in **-**.
- Konvertieren Sie alle **/** Zeichen in **_**.

- Ersetzen Sie die abschließenden 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 er URL-sicher ist.

Verwendete Bibliotheken

Das 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

Massenregistrierung von iOS-Geräten

Apr 24, 2017

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 zu kaufen.
- Sie können Apple Configurator zum Registrieren von Geräten verwenden, unabhängig davon, ob Sie diese direkt bei Apple erworben haben oder nicht.

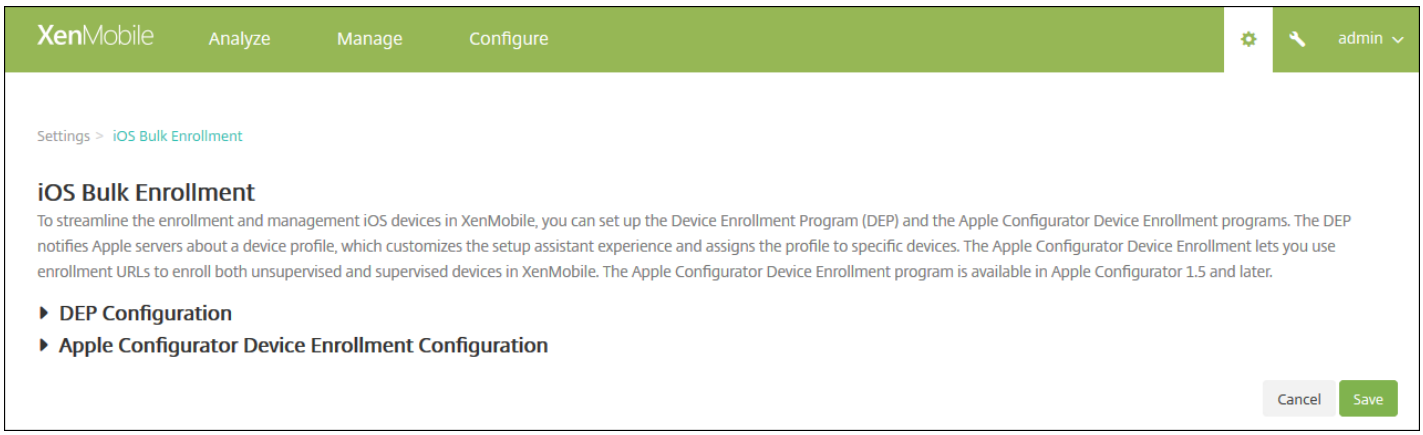
XenMobile 10.x unterstützt Apple Configurator v2.

Bei Verwendung des DEP brauchen Sie die Geräte nicht vorzubereiten. Sie senden Geräteseriennummern oder Bestellnummern über DEP. Dann können Sie die Geräte in XenMobile konfigurieren und registrieren. Nachdem die Geräte registriert haben, können Sie sie Benutzern aushändigen, die sie ohne weitere Konfiguration verwenden können. Darüber hinaus können Sie beim Einrichten von Geräten mit DEP einige Schritte des Setupassistenten eliminieren. Dadurch entfallen Aufgaben, die Benutzer andernfalls ausführen müssten, wenn sie ihre Geräte zum ersten Mal starten. 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. Nach dem Bereitstellen der Geräte mit den erforderlichen Richtlinien werden die Richtlinien beim 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. 2. Klicken Sie unter **Server** auf **iOS-Massenregistrierung**. Die Seite **iOS-Massenregistrierung** wird angezeigt.



Informationen zum Konfigurieren von DEP-Einstellungen finden Sie weiter unten. Wenn Sie Apple Configurator-Einstellungen konfigurieren, lesen Sie den Abschnitt Konfigurieren von Apple Configurator-Einstellungen.

Voraussetzung: 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.

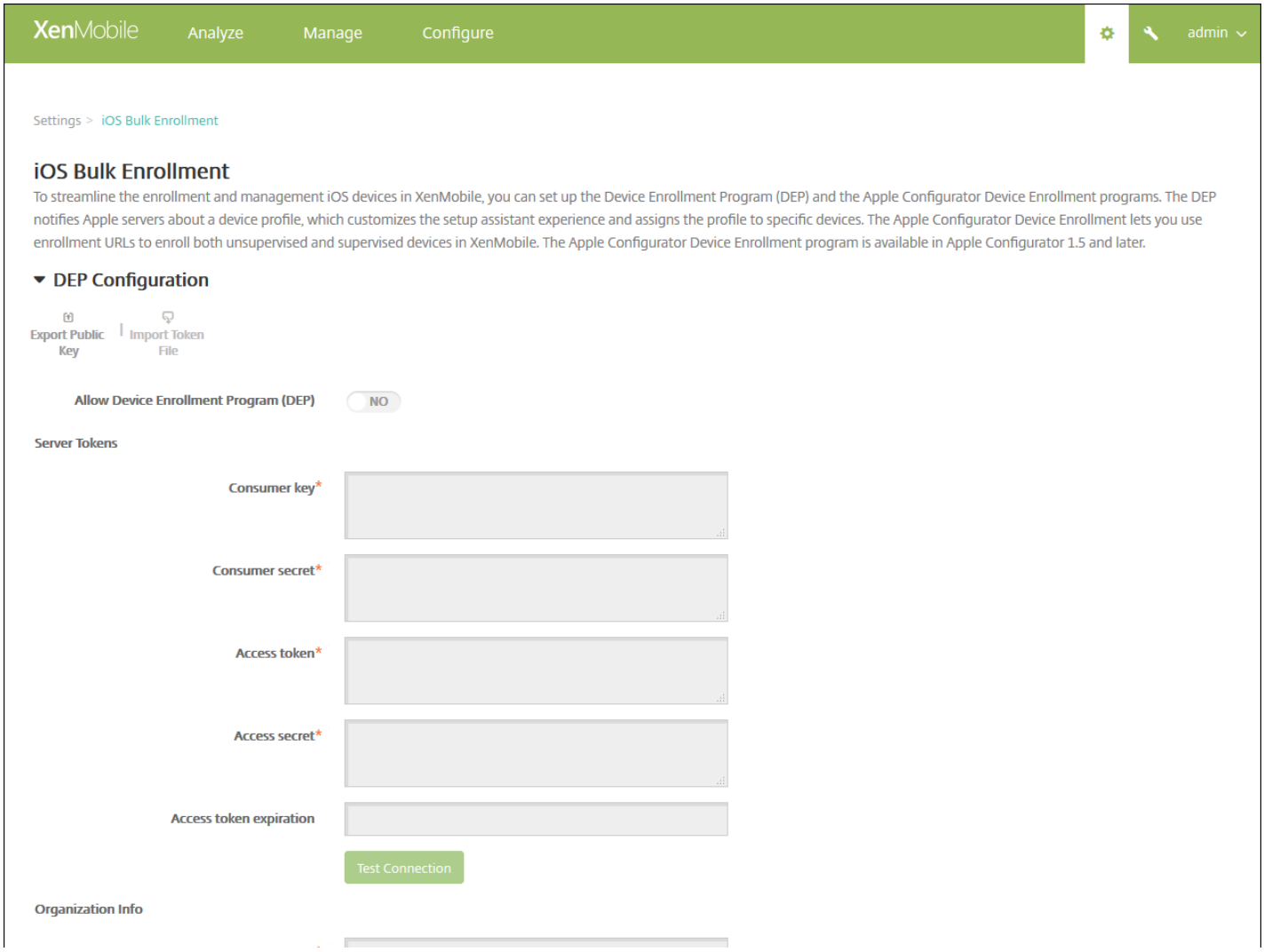
2. Navigieren Sie zu deploy.apple.com, melden Sie sich bei Ihrem DEP-Konto an und folgen Sie den Anweisungen zum Einrichten eines MDM-Servers. Im Rahmen dieses Prozesses stellt Apple ein Servertoken bereit.

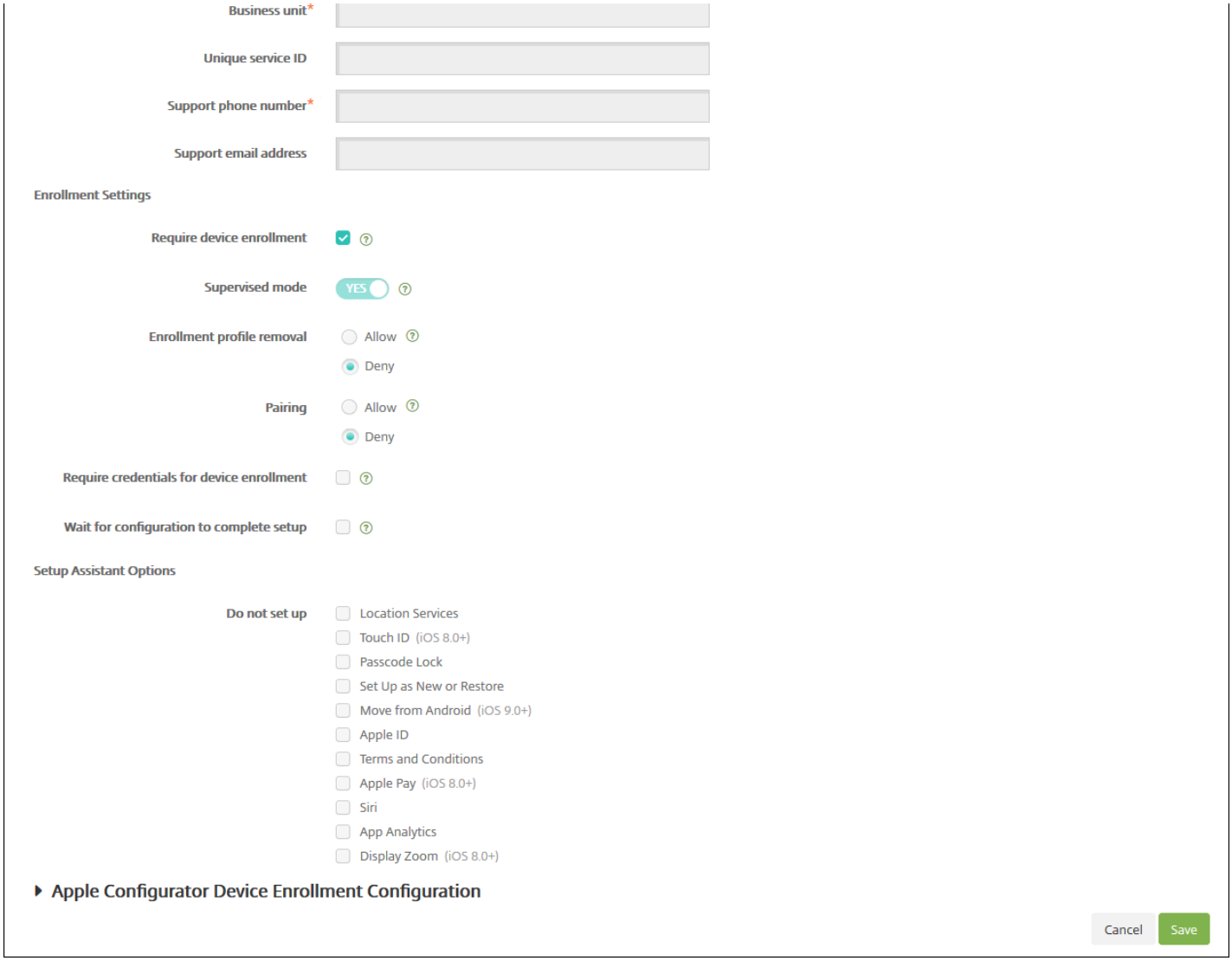
3. Klicken Sie auf der Seite **iOS-Massenregistrierung** auf **Tokendatei importieren** und fügen Sie das Apple-Servertoken in XenMobile hinzu.

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 dazu, wie Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie weiter unten in diesem Artikel

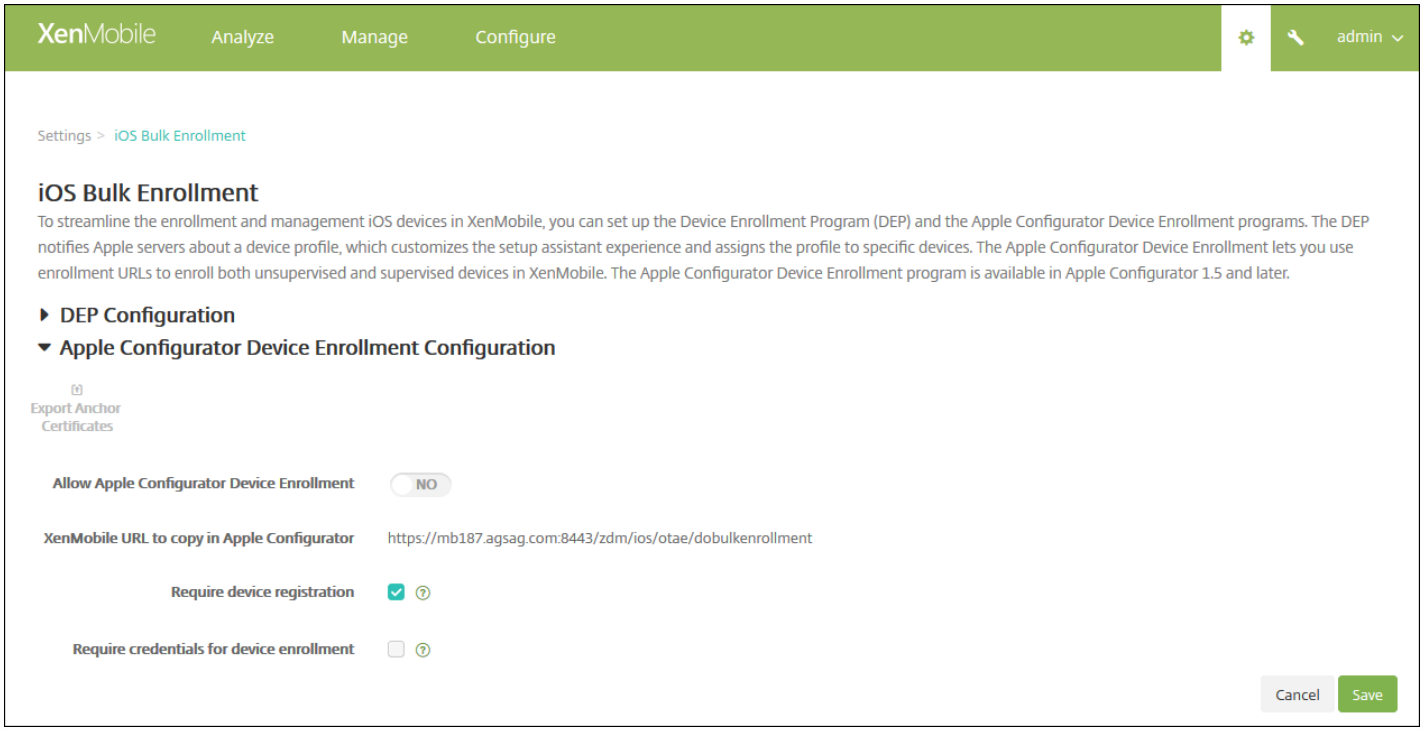
unter Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus.

- **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 ab Version 7.1 verfügbar.**Hinweis**: Wenn Sie DEP erstmalig einrichten und diese Option nicht aktivieren, werden die DEP-Komponenten (DEP-Benutzer, Secure Hub, Softwarebestand und DEP-Bereitstellungsgruppe) von Grund auf 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 ab Version 9.0 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
- **App-Analyse**: 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 **Export Anchor Certs** 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. 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 " href="https://help.apple.com/configurator/mac/1.0/#cad96c7acd6">Prepare devices der Apple Configurator-Hilfe.

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 10.4.

> ## Important
>
> Beim Versetzen eines Geräts in den betreuten Modus wird die ausgewählte iOS-Version auf dem Gerät installiert und sämtliche zuvor gespeicherten Benutzerdaten und Apps werden von dem Gerät gelöscht.

1. Installieren Sie Apple Configurator aus iTunes.

2. Schließen Sie das iOS-Gerät an den Apple-Computer an.

3. Starten Sie Apple Configurator. Der Configurator zeigt an, dass ein Gerät zur Vorbereitung für die Betreuung vorhanden ist.

4. Vorbereiten des Geräts für die Betreuung:

    a. Legen Sie für "Supervision" die Option **On** fest. Citrix empfiehlt, diese Einstellung zu aktivieren, wenn Sie ein Gerät kontinuierlich durch regelmäßige Neuanwendung einer Konfiguration steuern möchten.

    b. Geben Sie optional einen Namen für das Gerät ein.

    c. Klicken Sie in **iOS** auf **Latest** für die neueste iOS-Version, die Sie installieren möchten.

5. Wenn das Gerät zur Betreuung vorbereitet werden kann, klicken Sie auf **Prepare**.

Bereitstellung von iOS-Geräten über das Apple DEP

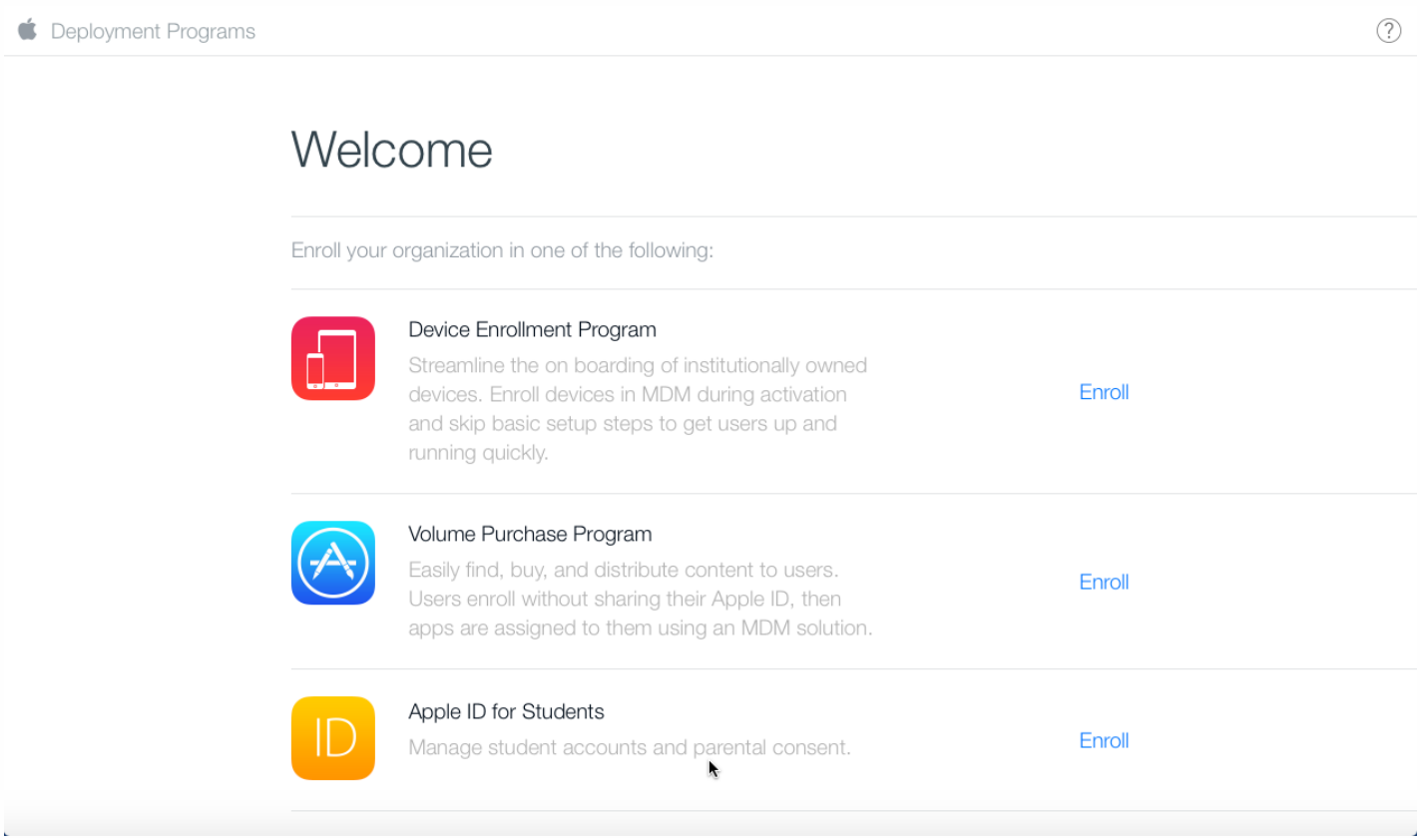
Feb 24, 2017

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.

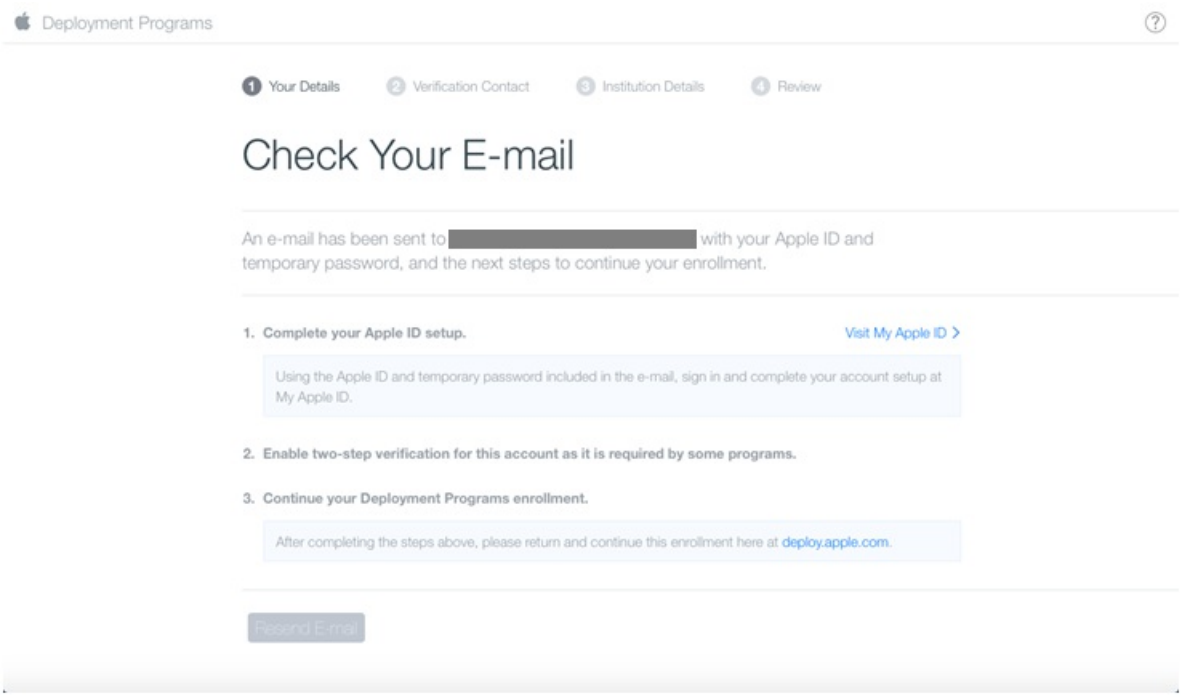
- Telefonnummer und E-Mail-Adresse der Firma oder der Organisation
- Verifizierungskontakt
- Unternehmens- oder Organisationsinformationen (D-U-N-S-Nummer/Steuernummer)
- Apple Kundennummer

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.

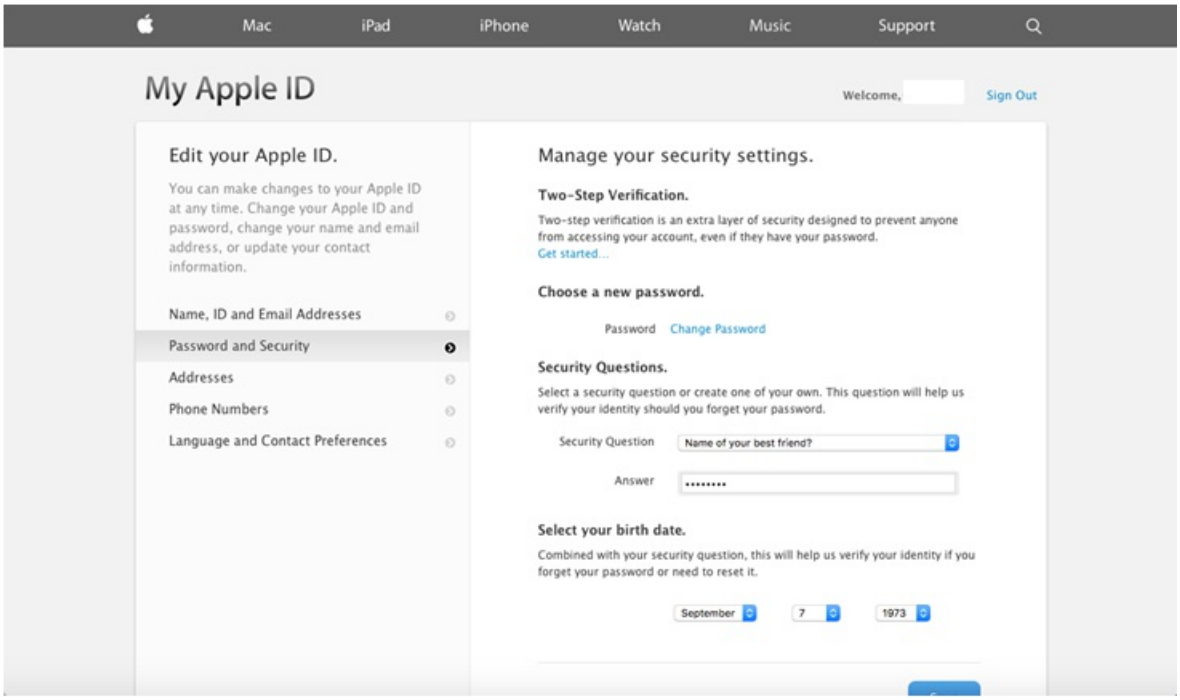
Beim Beantragen eines DEP-Kontos verwenden Sie am besten eine E-Mail-Adresse, die mit der Organisation verbunden ist, z. B. dep@company.com.



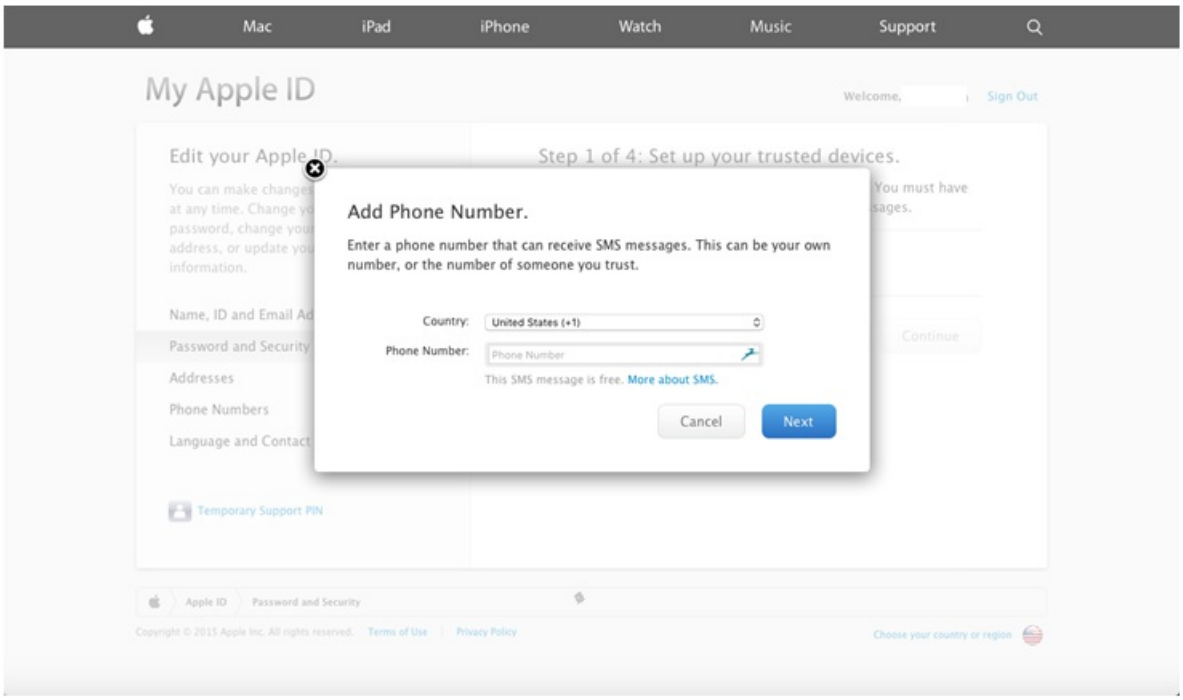
1. Wenn Sie die Organisationsinformationen angegeben haben, erhalten Sie per E-Mail ein temporäres Kennwort für die neue Apple-ID.



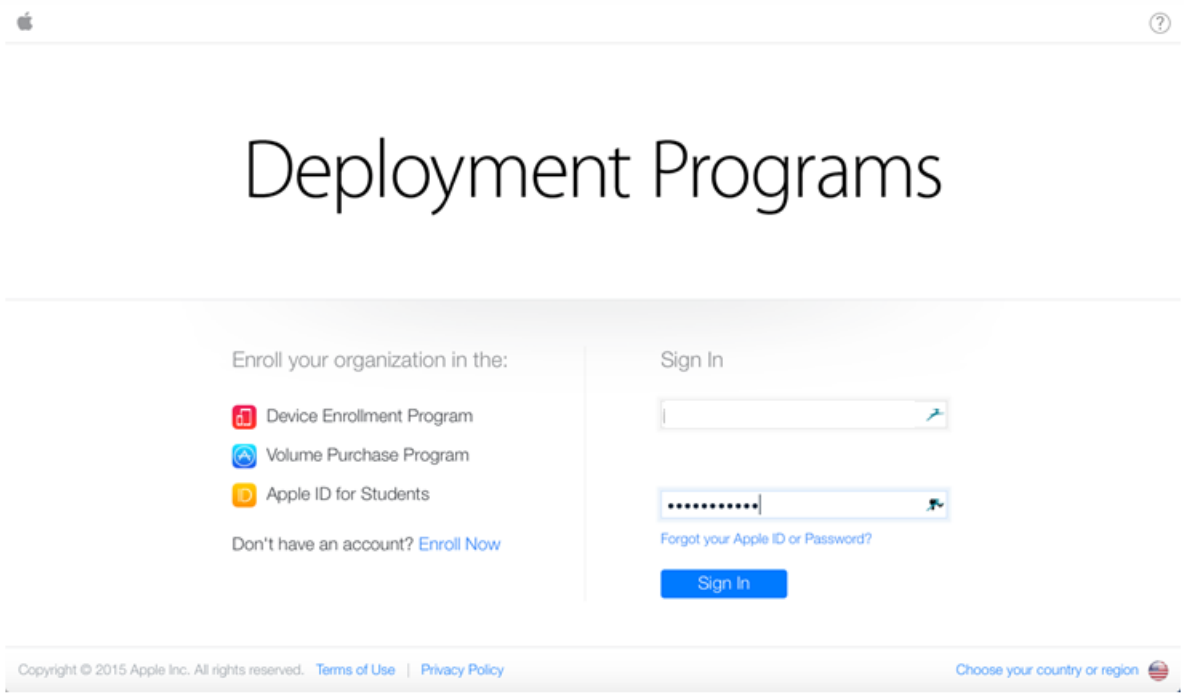
2. Melden Sie sich mit der Apple-ID an und legen Sie die Sicherheitseinstellungen für das Konto fest.



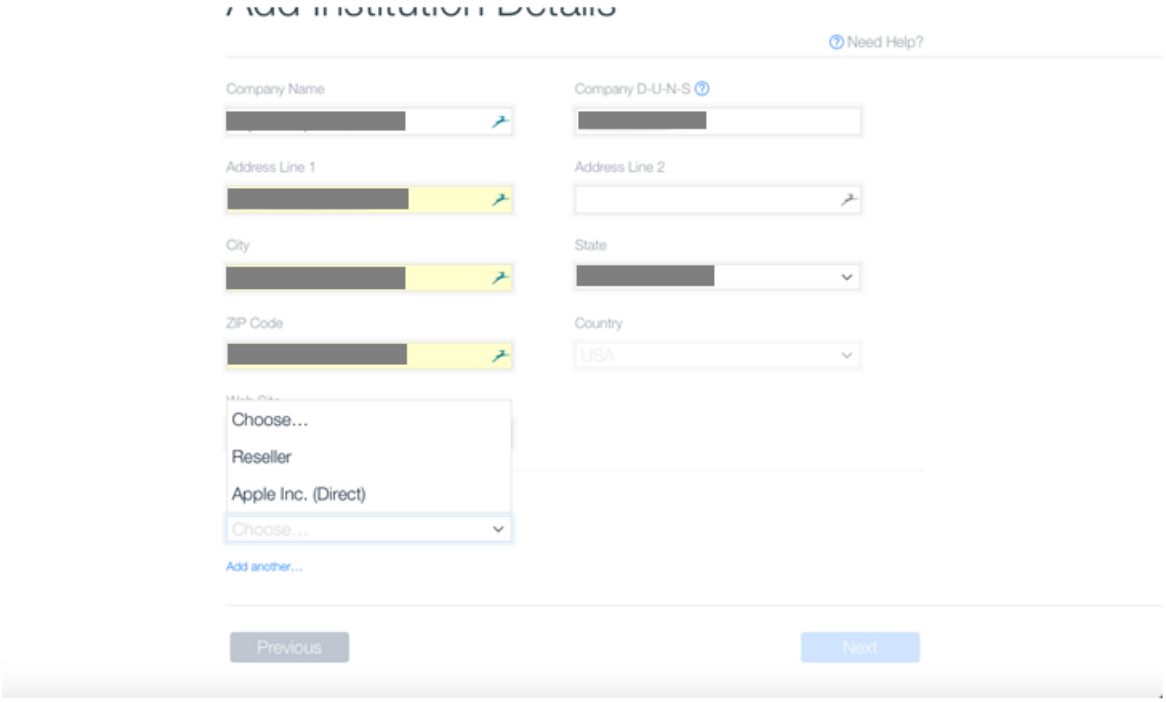
3. Konfigurieren und aktivieren Sie die Überprüfung in zwei Schritten, die für das DEP-Portal erforderlich ist. Bei diesen Schritten fügen Sie eine Telefonnummer hinzu, über die Sie die 4-stellige PIN für die Überprüfung in zwei Schritten erhalten.



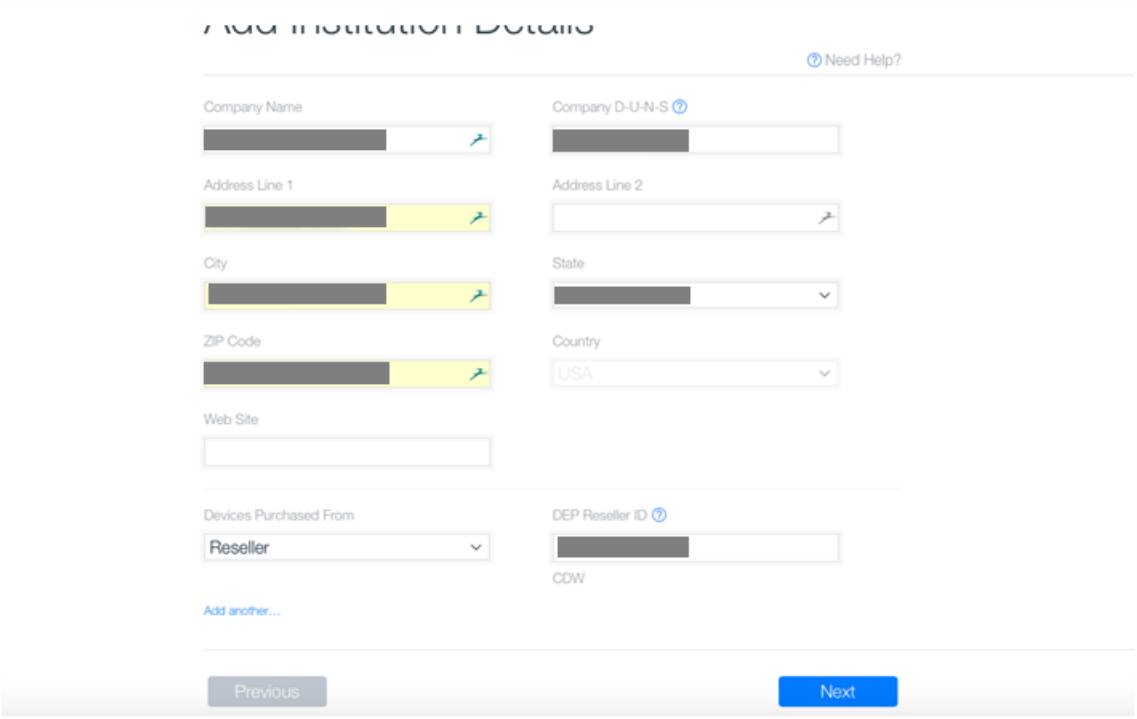
4. Melden Sie sich mit der Überprüfung in zwei Schritten beim DEP-Portal an und schließen Sie die Kontokonfiguration ab.

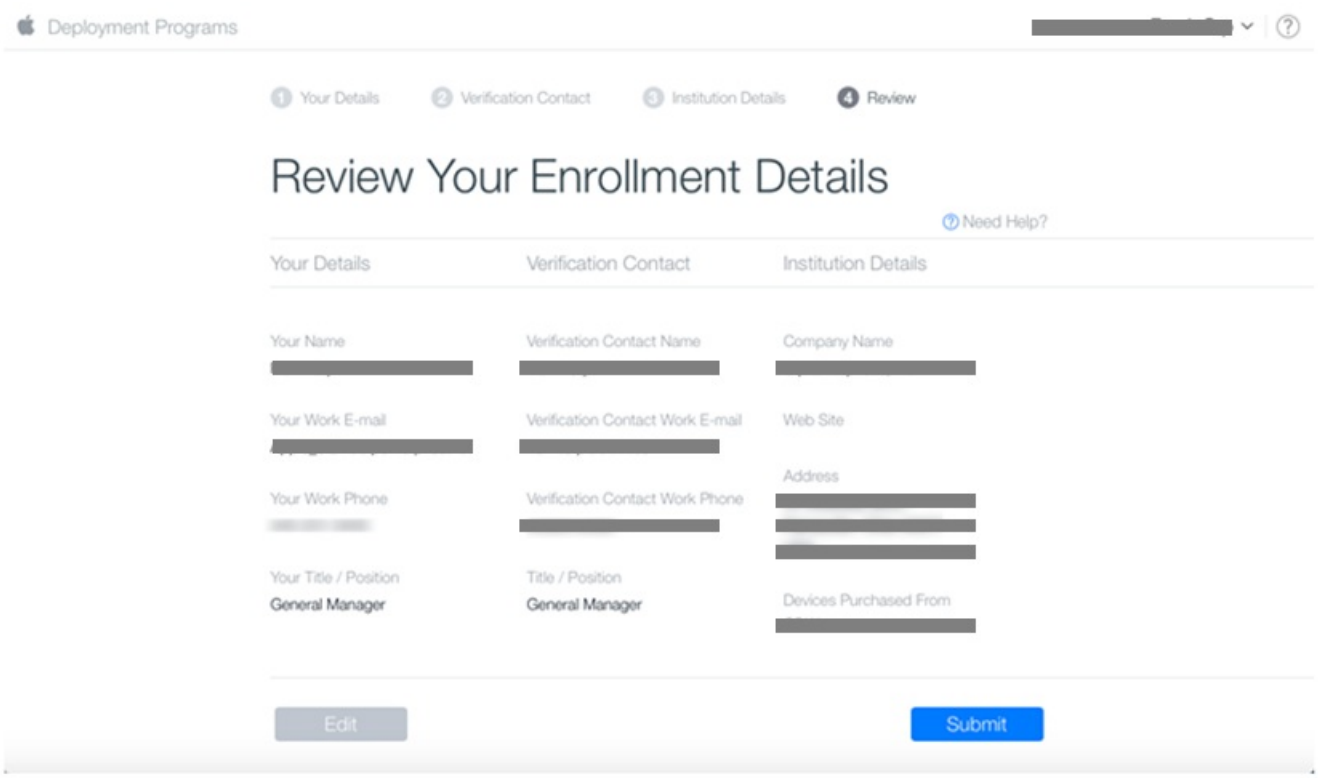


5. Fügen Sie die Details Ihres Unternehmens hinzu und wählen Sie aus, wo Sie Ihre Geräte erwerben. Details zu Erwerbsoptionen finden Sie im nächsten Abschnitt unter Bestellen von DEP-aktivierten Geräten.

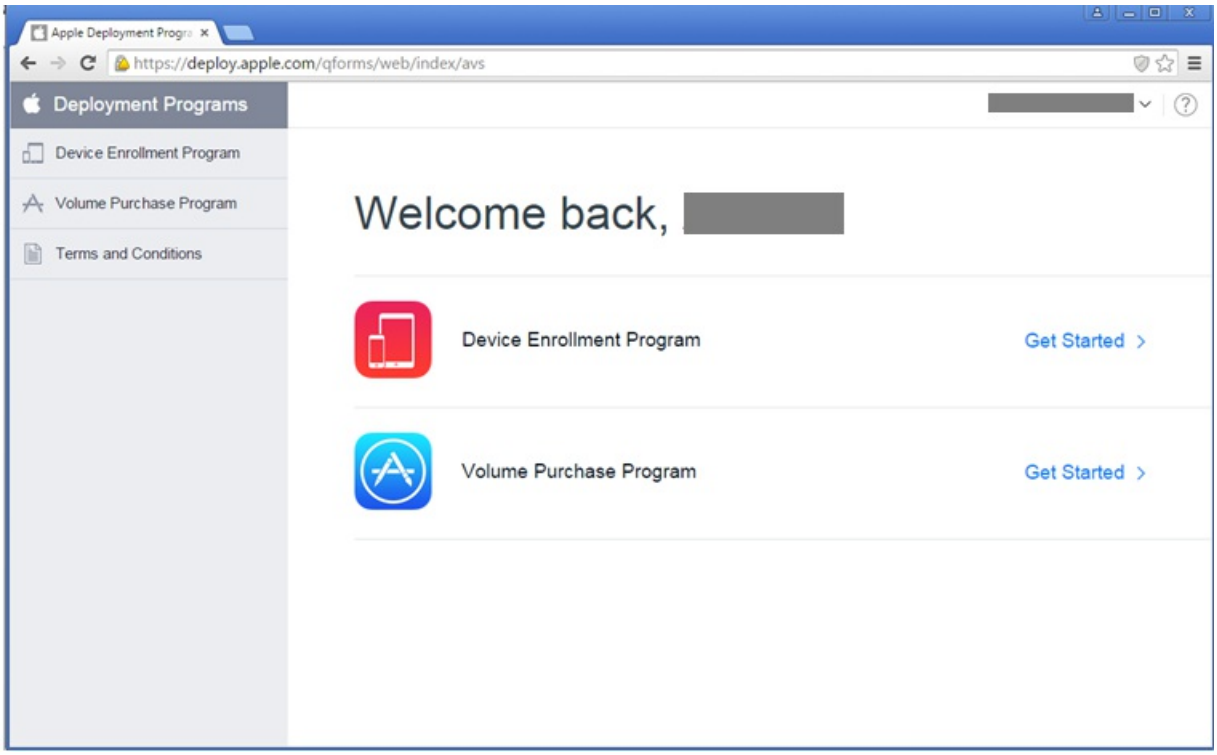


6. Fügen Sie die Apple-Kundennummer oder die DEP-Wiederverkäufer-ID hinzu und überprüfen Sie Ihre Registrierungsdetails. Warten Sie dann darauf, dass Apple Ihr Konto genehmigt.



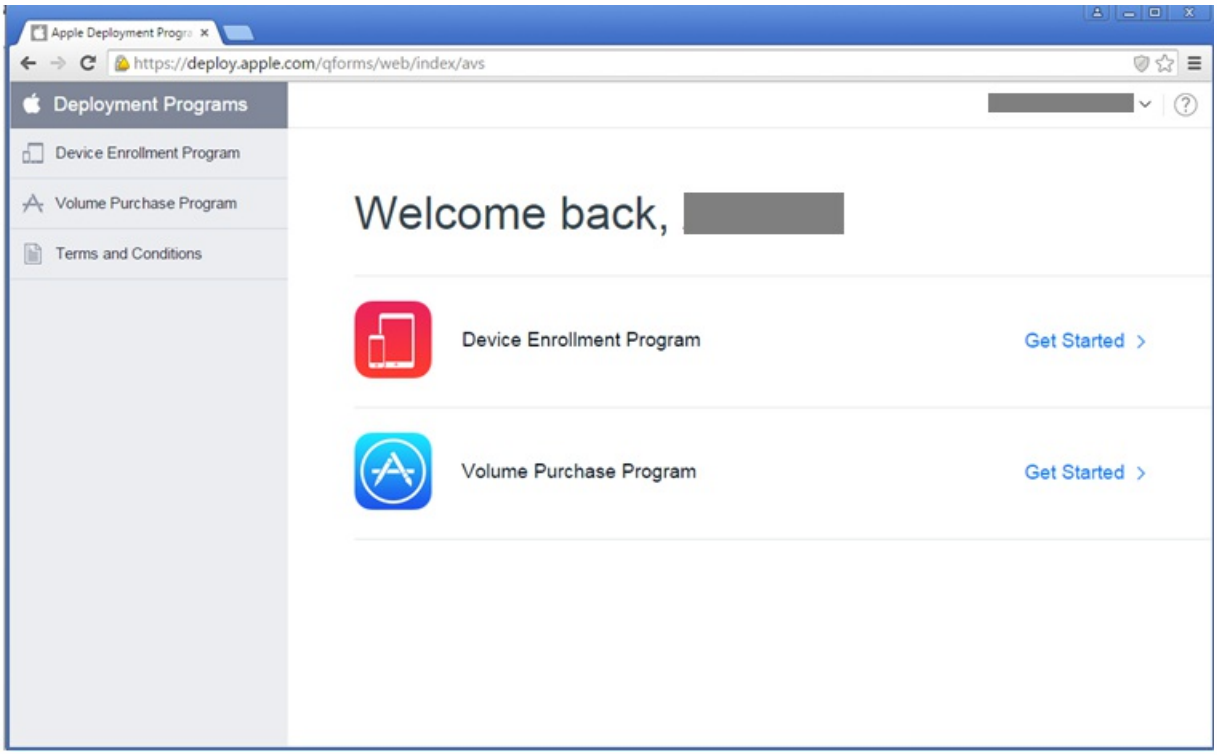


7. Wenn Sie Ihre Anmeldeinformationen von Apple erhalten haben, melden Sie sich beim Apple DEP-Portal an. Führen Sie dann die Schritte im nächsten Abschnitt aus, um Ihre Konto mit XenMobile zu verbinden.

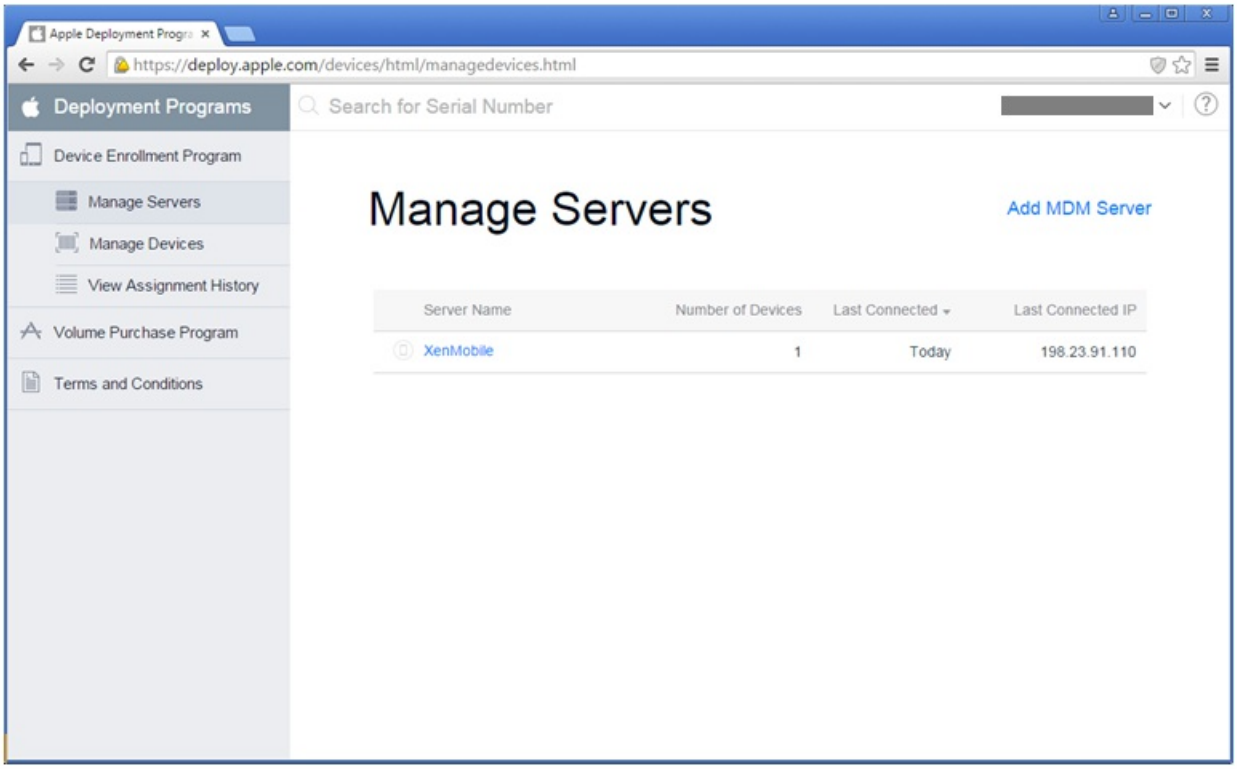


Befolgen Sie die Anleitungen in diesem Abschnitt, um Ihr Apple DEP-Konto mit Ihrer XenMobile-Serverbereitstellung zu verbinden.

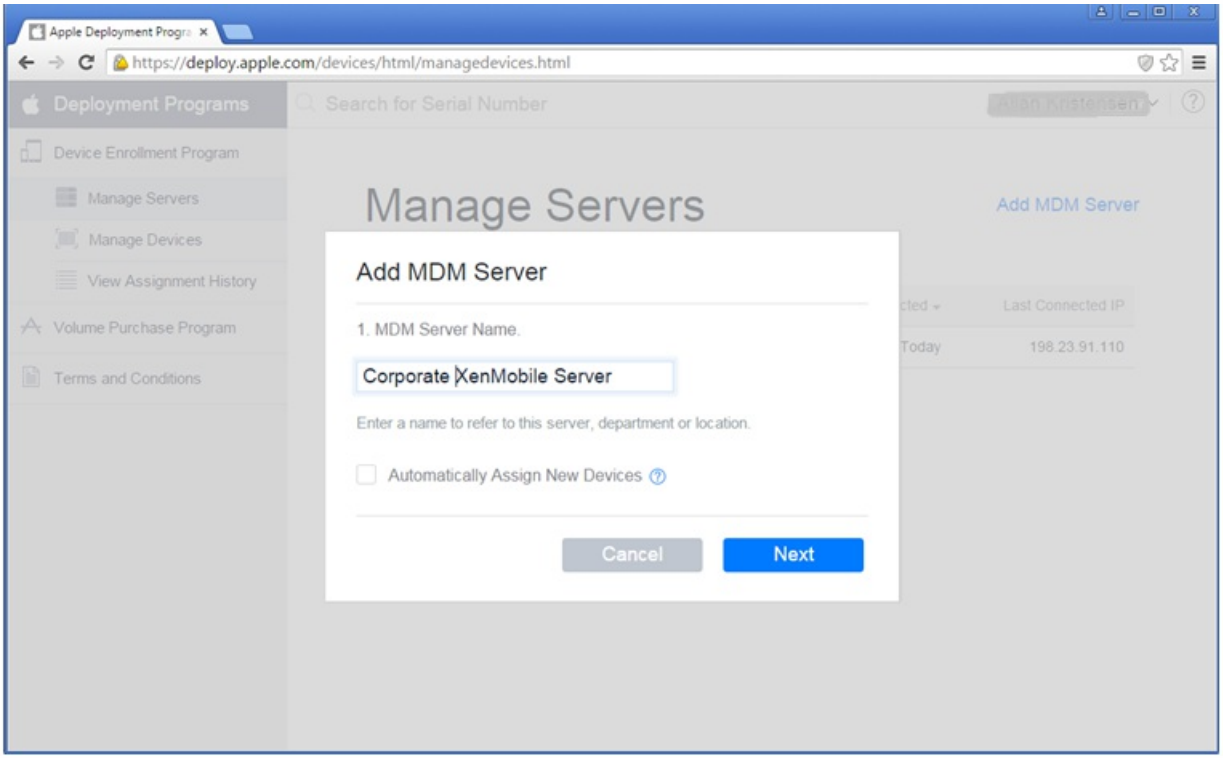
1. Klicken Sie links im Apple DEP-Portal auf **Device Enrollment Program**.



2. Klicken Sie auf **Manage Servers** und dann rechts auf **Add MDM Server**.



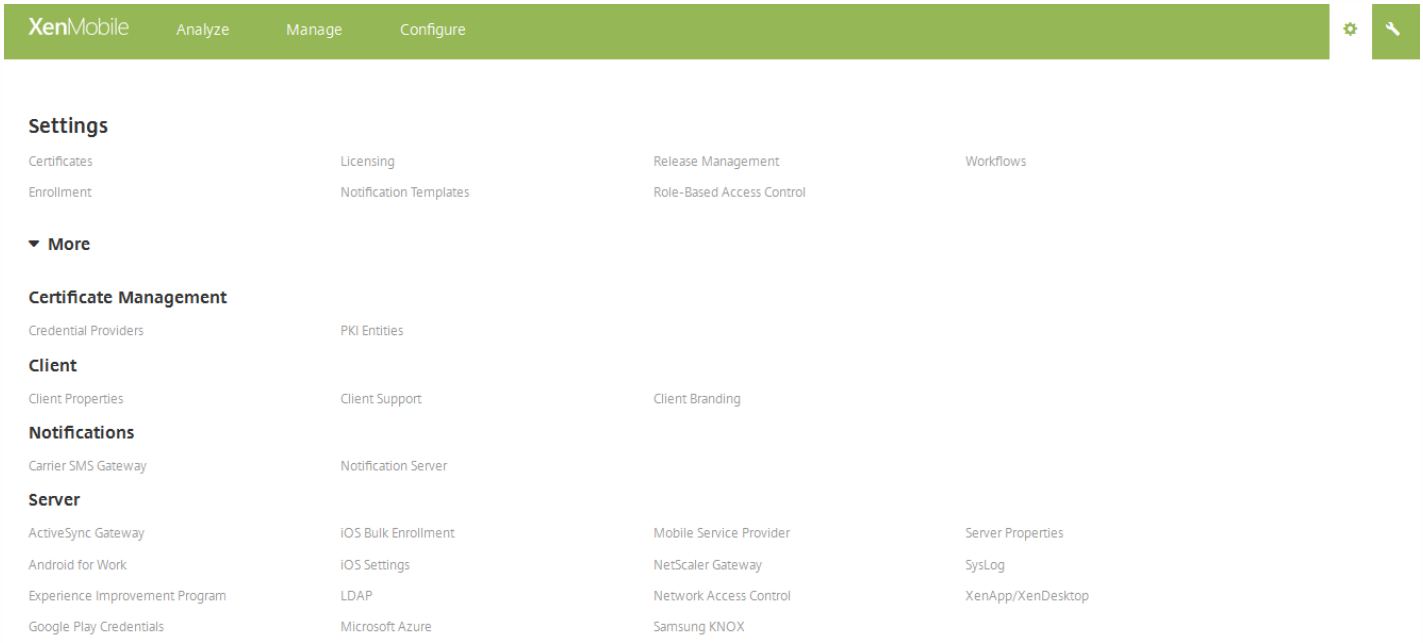
3. Geben Sie im Fenster **Add MDM Server** einen Namen für Ihren XenMobile-Server ein und klicken Sie auf **Next**.



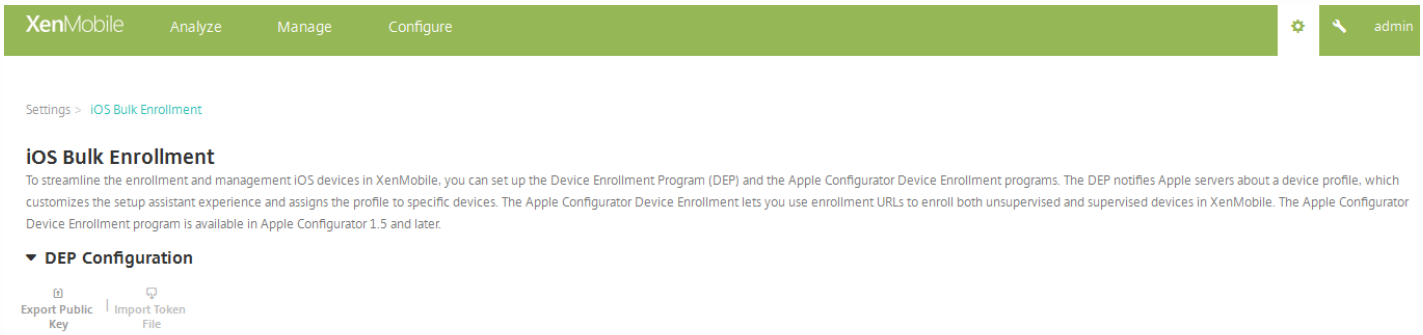
4. Laden Sie einen öffentlichen Schlüssel vom XenMobile-Server hoch. Generieren des Schlüssels in XenMobile:

   a. Melden Sie sich an der XenMobile-Konsole an und klicken Sie auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

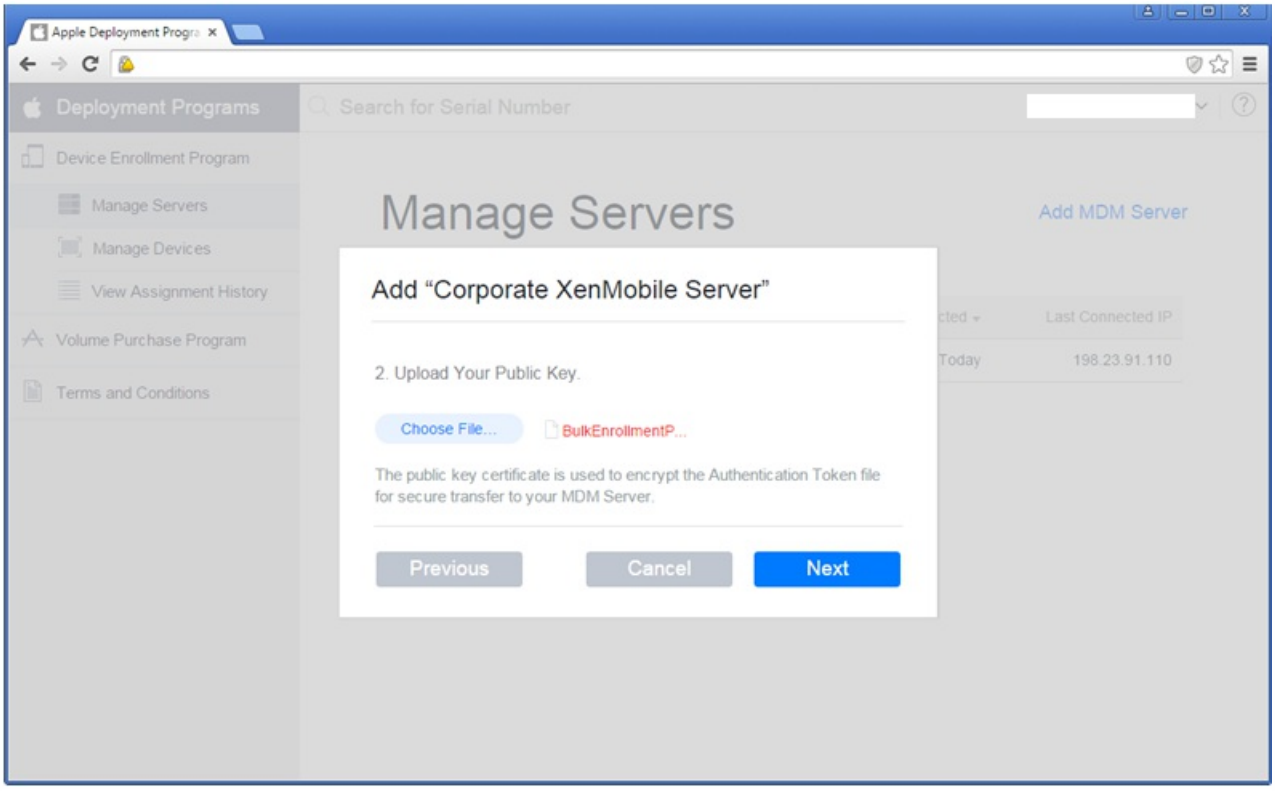
   b. Klicken Sie unter **Mehr** auf **iOS-Massenregistrierung**.



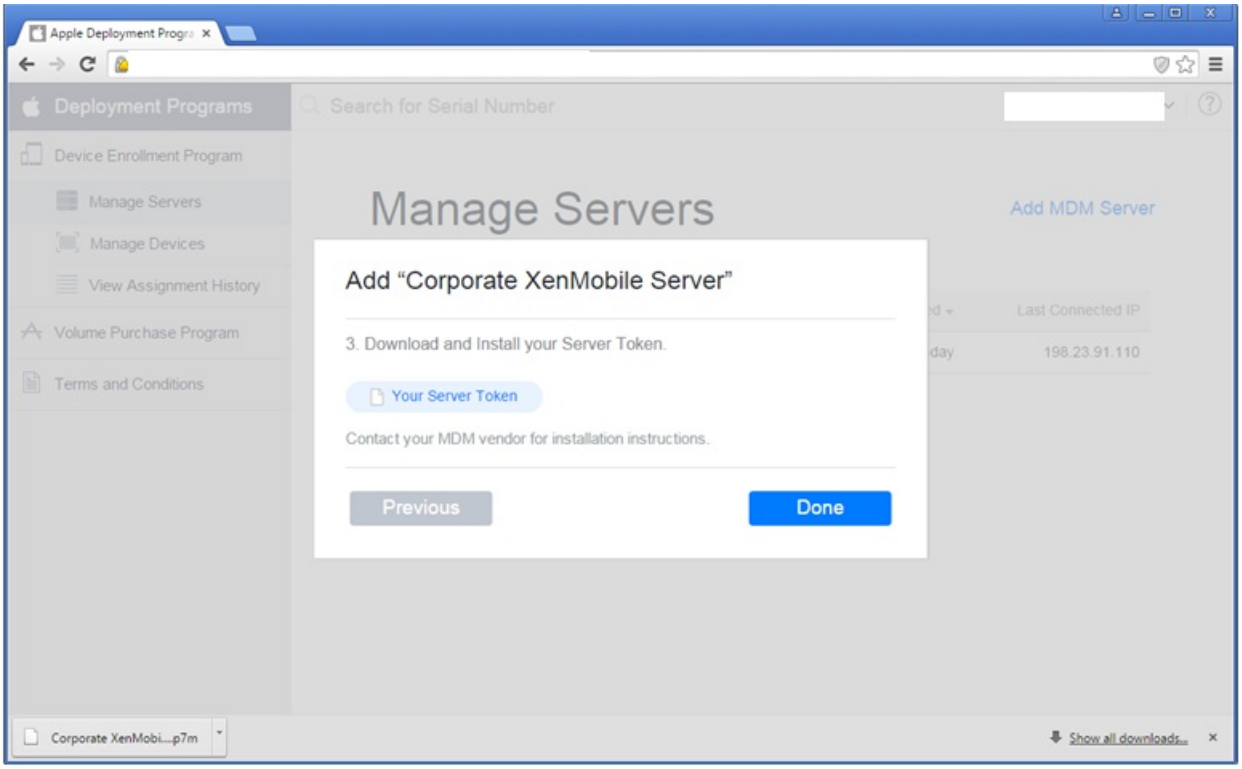
b. Erweitern Sie **DEP-Konfiguration** auf der Seite **iOS-Massenregistrierung** und klicken Sie auf **Öffentlichen Schlüssel exportieren**. Der öffentliche Schlüssel wird heruntergeladen.



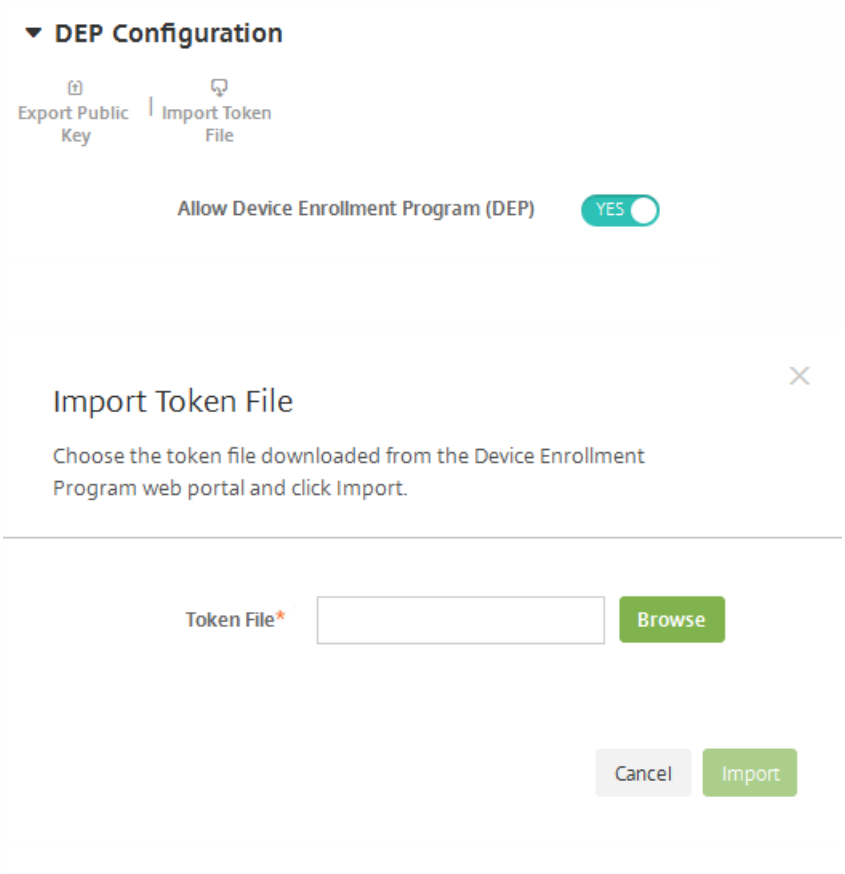
5. Klicken Sie im Apple DEP-Portal auf **Choose file**, wählen Sie den öffentlichen Schlüssel, den Sie heruntergeladen haben, und klicken Sie dann auf **Next**.



6. Klicken Sie auf **Your Server Token**, um einen Servertoken zu generieren, der vom Browser heruntergeladen wird, und klicken Sie dann auf **Done**.

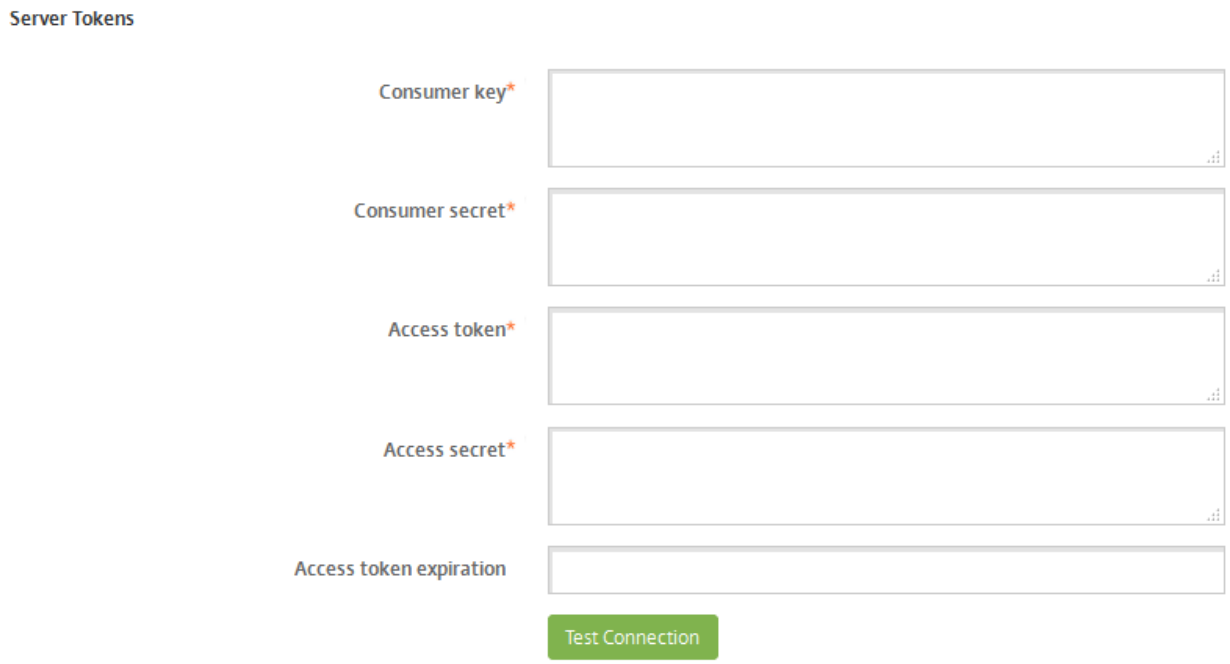


7. Klicken Sie in der XenMobile-Konsole auf der Seite **iOS-Massenregistrierung** neben **Device Enrollment Program (DEP) zulassen** auf "Ja", klicken Sie dann auf **Tokendatei importieren** und laden Sie die Tokendatei hoch, die Sie im vorherigen Schritt heruntergeladen haben.



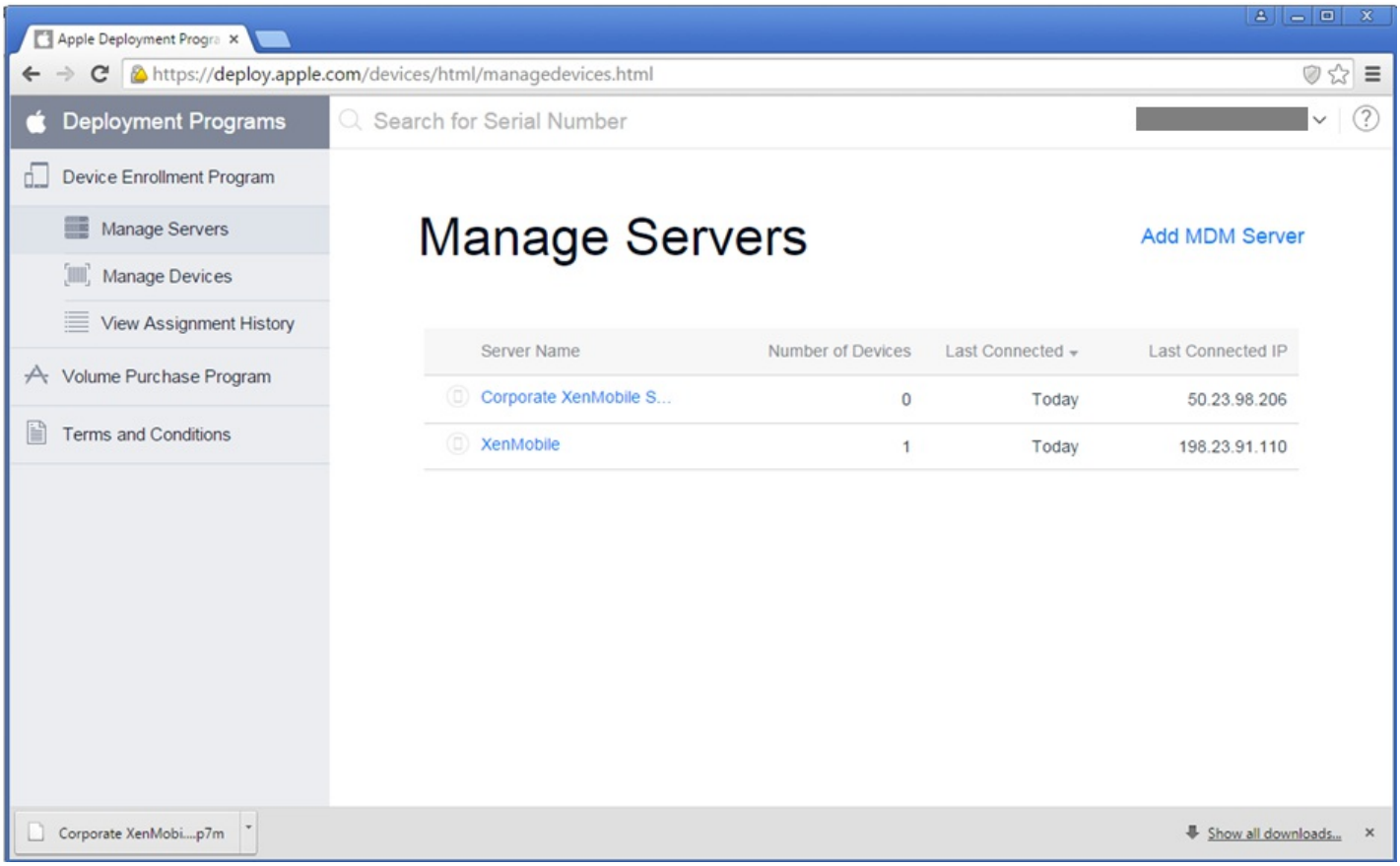
Nach dem Import der Tokendatei werden Ihre Apple DEP-Tokeninformationen in der XenMobile-Konsole angezeigt.

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.



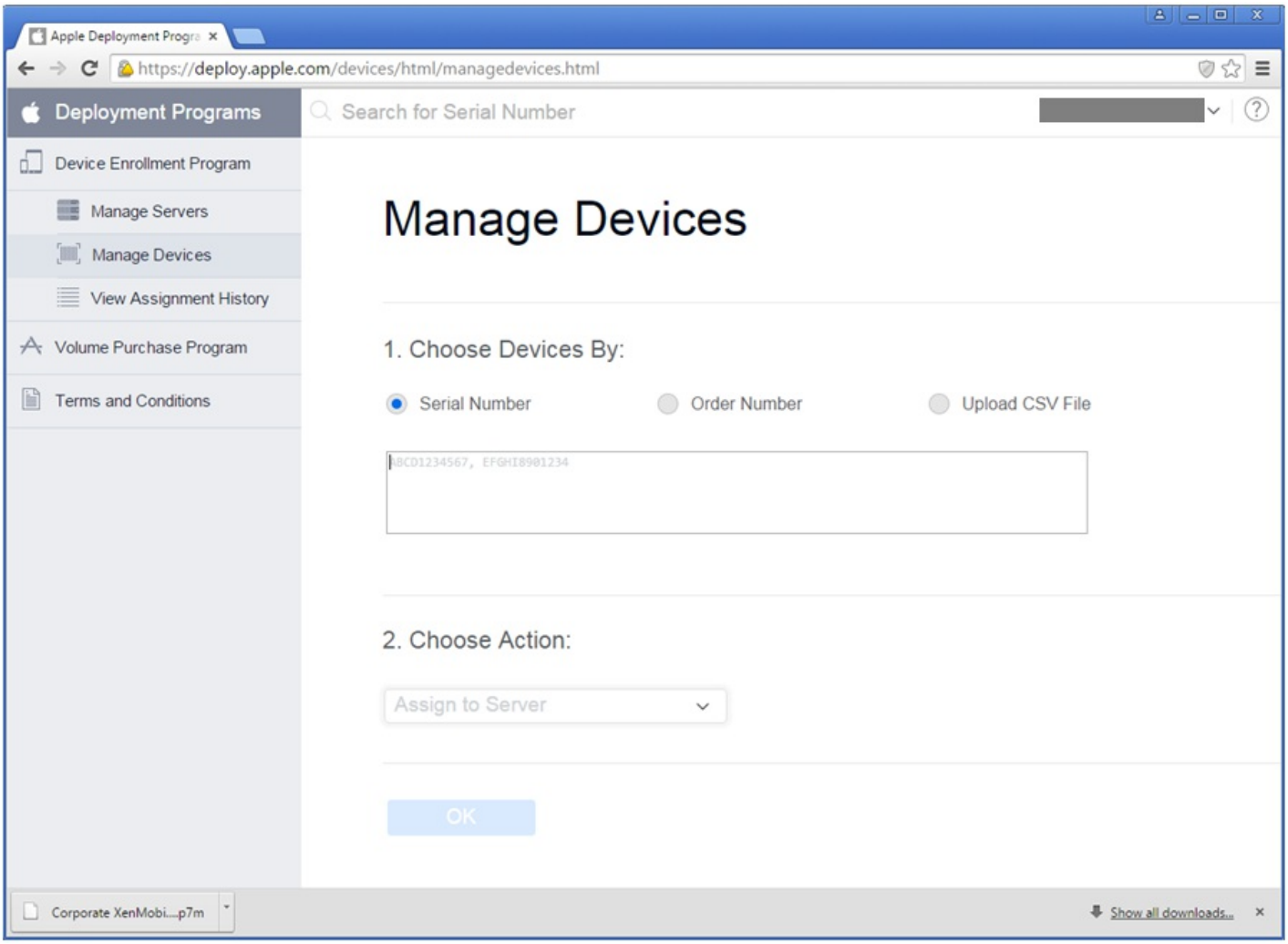
Sie können DEP-aktivierte Geräte direkt bei Apple oder für DEP autorisierten Wiederverkäufern und Netzbetreibern bestellen. Wenn Sie bei Apple bestellen, müssen Sie Ihre Apple Kunden-ID im Apple DEP-Portal angeben, damit Apple das gekaufte Gerät Ihrem Apple DEP-Konto zuordnen kann.

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.

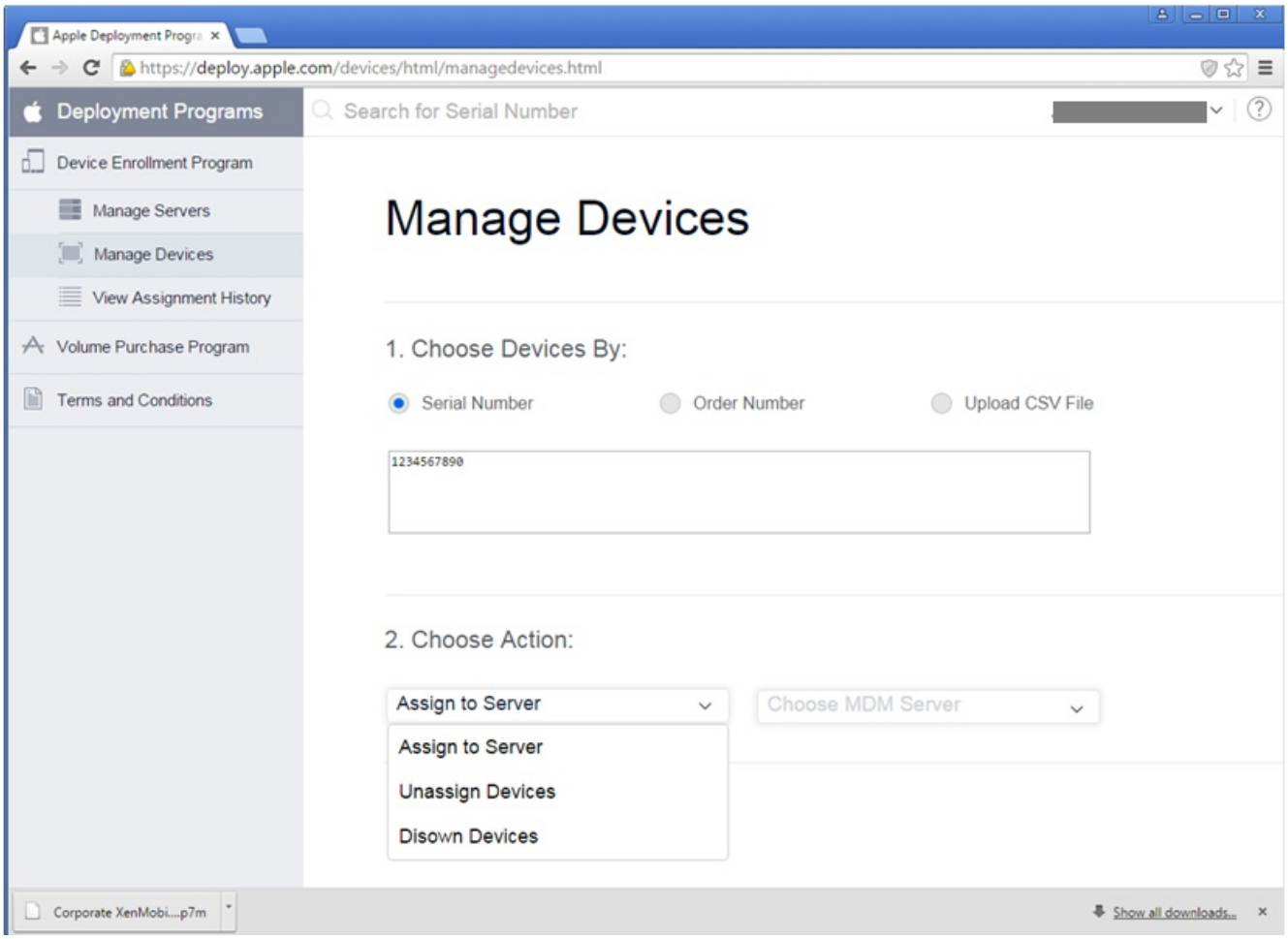
Mit den folgenden Schritten ordnen Sie Geräte in Ihrem Apple DEP-Konto über das DEP-Portal Ihrem XenMobile-Server zu.

1. Melden Sie sich beim Apple DEP-Portal an.

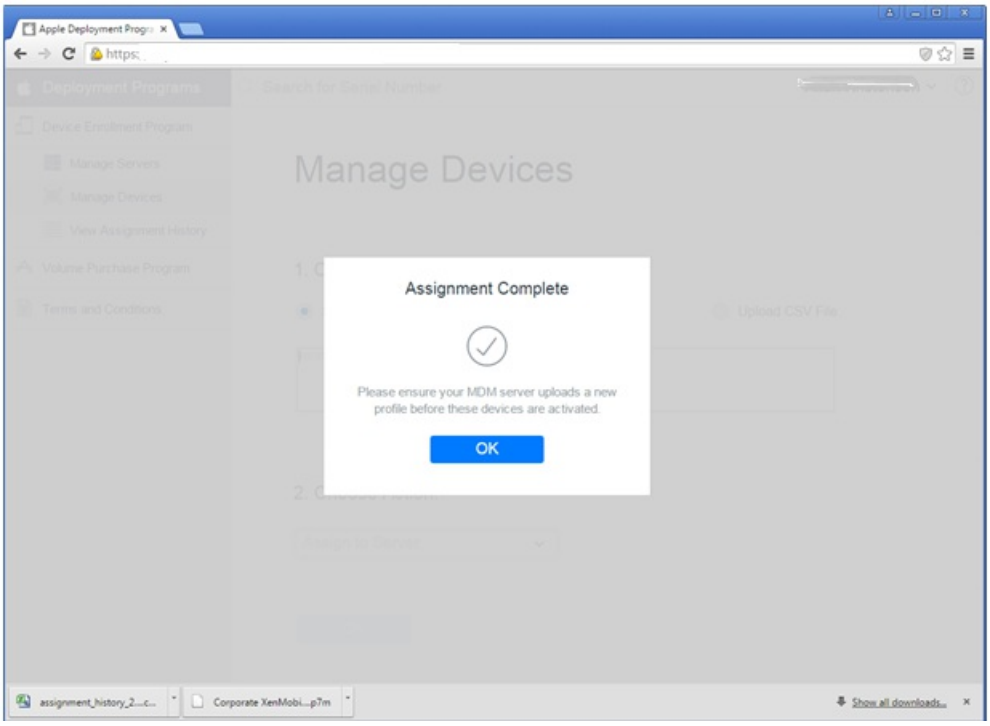
2. Klicken Sie auf **Device Enrollment Program**, klicken Sie auf **Manage Devices** und wählen Sie dann in **Choose Devices By** die Option aus, für die Sie Ihre Apple DEP-aktivierten Geräte hochladen und definieren möchten: **Serial Number**, **Order Number** oder **Upload CSV File**.



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.

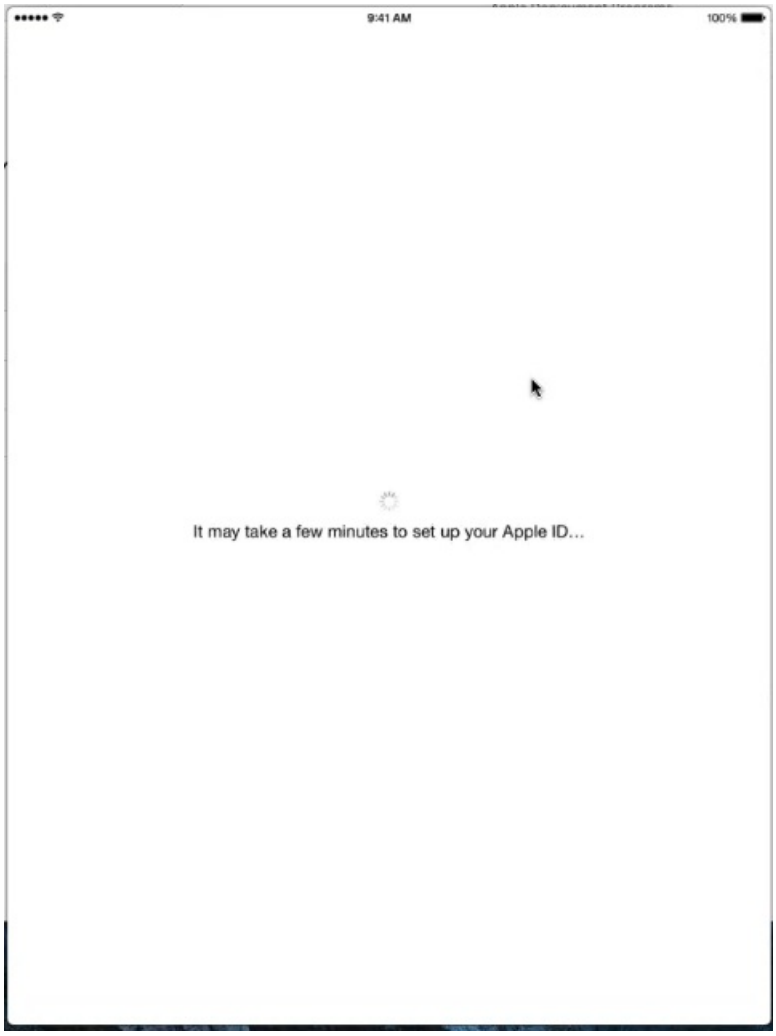
1. Benutzer starten ihr Apple DEP-aktiviertes Gerät.

2. Mit dem Konfigurationsassistenten konfigurieren Benutzer die Anfangseinstellungen auf ihrem iOS-Gerät.

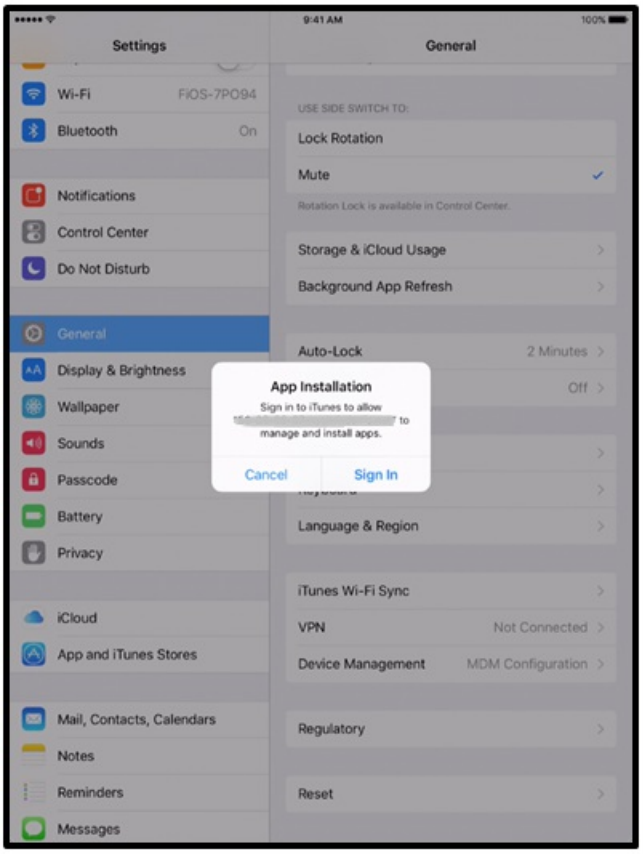
3. Das Gerät startet automatisch die XenMobile-Geräteregistrierung. Der Assistent führt Benutzer durch die Registrierung des Geräts beim XenMobile-Server, der dem Apple DEP-aktivierten Gerät zugeordnet ist.

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 Secure Hub heruntergeladen werden kann.



6. Die Benutzer öffnen Secure Hub und geben ihre Anmeldeinformationen ein. Entsprechend der Richtlinie müssen die Benutzer u. U. eine Citrix PIN erstellen und verifizieren.

Die übrigen erforderlichen Apps werden per Push auf dem Gerät bereitgestellt.

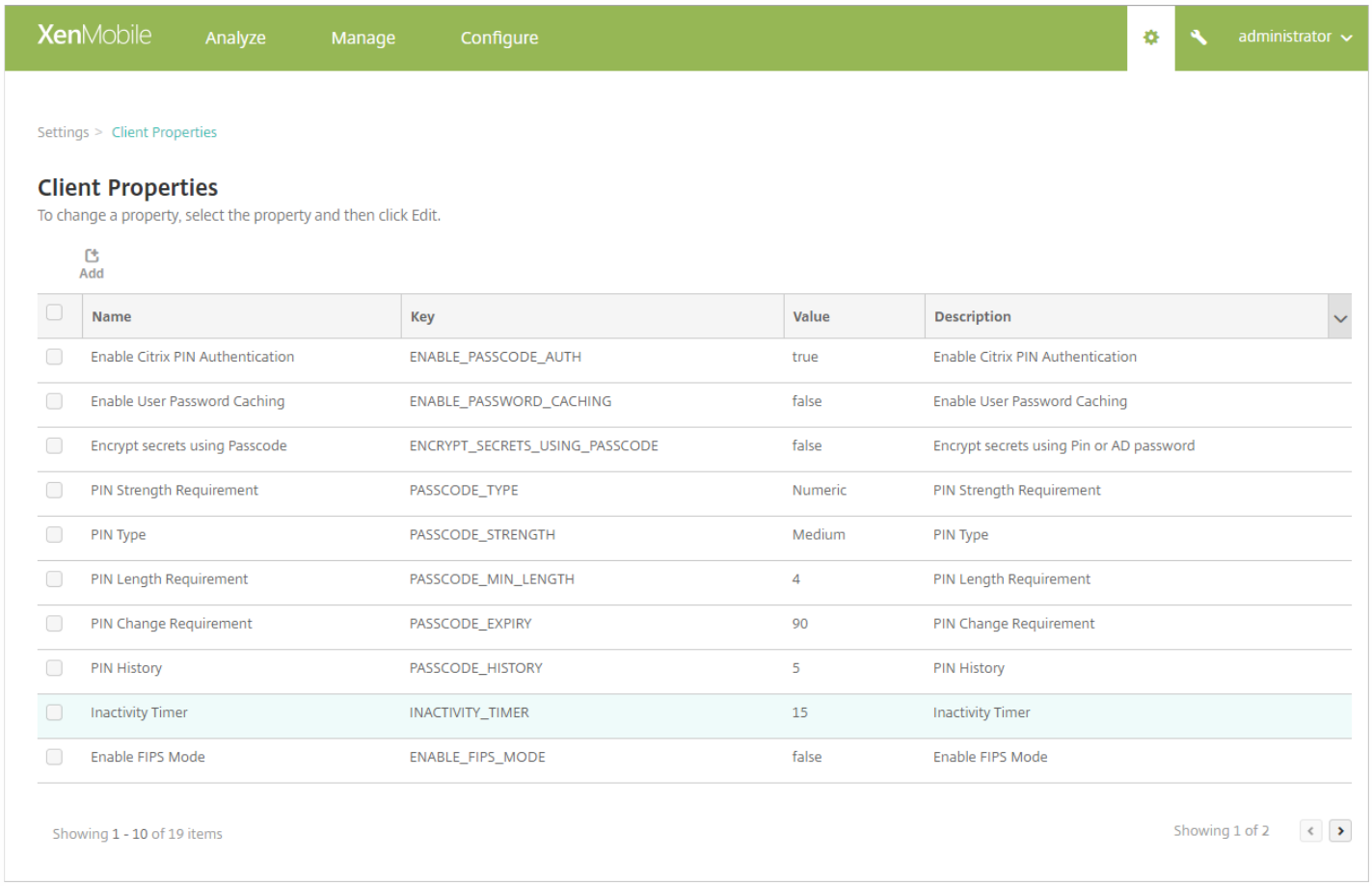
Clienteigenschaften

Apr 24, 2017

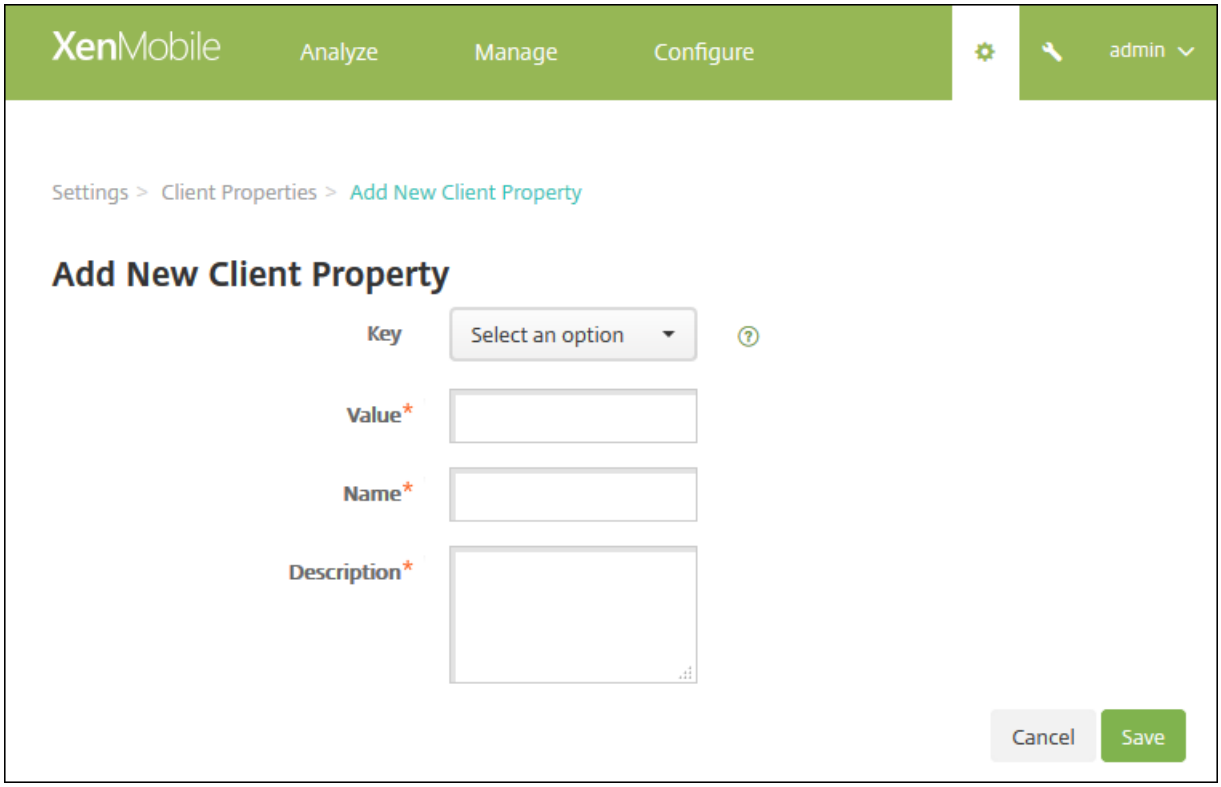
Clienteigenschaften enthalten Informationen, die direkt in Secure Hub auf den Geräten der Benutzer bereitgestellt werden.Mit diesen Eigenschaften können Sie erweiterte Einstellungen, z. B. die Citrix PIN, konfigurieren. Clienteigenschaften sind beim Citrix Support erhältlich.

Clienteigenschaften können sich bei jedem neuen Release von Client-Apps, insbesondere von Secure Hub, ändern. Informationen zu den häufig konfigurierten Clienteigenschaften finden Sie unter Referenz der Clienteigenschaften weiter unten in diesem Artikel.

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 **Neue Clienteigenschaft hinzufügen** wird angezeigt.



2. Konfigurieren Sie folgende 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 zu bearbeitende Clienteigenschaft aus.

Hinweis: Wenn Sie das Kontrollkästchen neben einer Clienteigenschaft aktivieren, 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 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 beizubehalten.

1. Wählen Sie in der Tabelle **Clienteigenschaften** die zu löschende Clienteigenschaft aus.

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

2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie erneut auf **Löschen** .

Referenz der Clienteigenschaften

Die vordefinierten XenMobile-Clienteigenschaften und deren Standardeinstellungen sind wie folgt:

CONTAINER_SELF_DESTRUCT_PERIOD

Anzeigename: MDX Container Self Destruct Period

Self-Destruct verhindert den Zugriff auf Secure Hub 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 Benutzergeräts 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 Secure Hub 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 den benutzerdefinierten Schlüssel **CONTAINER_SELF_DESTRUCT_PERIOD** hinzu.

Wert: Anzahl der Tage

DEVICE_LOGS_TO_IT_HELP_DESK

Anzeigename: Geräteprotokolle an IT-Helpdesk senden

Mit dieser Eigenschaft aktivieren bzw. deaktivieren Sie die Möglichkeit zum Senden von Protokollen an den IT-Helpdesk.

Mögliche Werte: **true** oder **false**

Standardwert: **false**

DISABLE_LOGGING

Anzeigename: Disable logging

Über diese Eigenschaft können Sie verhindern, dass Benutzer auf ihren Geräten Protokolle erstellen und hochladen. Die Protokollierung wird für Secure Hub 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 Secure Hub und MDX-Apps, die Auswirkungen auf die Benutzergeräte haben, nicht in der XenMobile-Konsole ändern.

Wenn Sie diese Eigenschaft auf **true** festlegen, wird in Secure Hub **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 dieser Eigenschaft wird die Absturzberichterstellung durch Crashlytics für XenMobile-Apps aktiviert bzw. deaktiviert.

Mögliche Werte: **true** oder **false**

Standardwert: **true**

ENABLE_FIPS_MODE

Anzeigename: Enable FIPS Mode

Mit dieser Eigenschaft wird der FIPS-Modus auf mobilen Geräten aktiviert oder deaktiviert. Wenn Sie den Wert ändern, übergibt Secure Hub bei der nächsten Onlineauthentifizierung den neuen Wert an das Gerät.

Mögliche Werte: **true** oder **false**

Standardwert: **false**

ENABLE_NETWORK_EXTENSION

Anzeigename: ENABLE_NETWORK_EXTENSION

Standardmäßig wird in XenMobile das Apple Network Extension-Framework aktiviert, wenn Secure Hub installiert wird. Zum Deaktivieren von Network Extension gehen Sie zu **Einstellungen > Clienteigenschaften**, fügen Sie den benutzerdefinierten Schlüssel **ENABLE_NETWORK_EXTENSION** hinzu und legen Sie den Wert auf **false** fest.

Standardwert: **true**

ENABLE_PASSCODE_AUTH

Anzeigename: Enable Worx PIN Authentication

Über diese Eigenschaft können Sie die Citrix PIN-Funktion aktivieren. Ist die Citrix PIN oder der Citrix 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 Citrix PIN lokal validiert und die Benutzer können auf die gewünschte App bzw. den gewünschten Inhalt zugreifen. Wenn Benutzer eine Onlineauthentifizierung durchführen, wird mit der Citrix PIN oder dem Citrix 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 diese Eigenschaft können Sie die lokale Zwischenspeicherung des Active Directory-Kennworts auf dem Mobilgerät zulassen. Wenn Sie diese Eigenschaft auf **true** setzen, müssen Sie auch die Eigenschaft ENABLE_PASSCODE_AUTH auf **true** setzen. Wenn "Benutzerkennwortcaching" aktiviert ist, werden die Benutzer von XenMobile aufgefordert, eine Citrix PIN oder einen Passcode festzulegen.

Mögliche Werte: **true** oder **false**

Standardwert: **false**

ENABLE_TOUCH_ID_AUTH

Anzeigename: Enable Touch ID Authentication

Für Geräte, die Touch ID-Authentifizierung unterstützen, wird mit dieser Eigenschaft Touch ID-Authentifizierung auf dem Gerät aktiviert oder deaktiviert. Anforderungen:

Auf Benutzergeräten muss Citrix PIN oder LDAP aktiviert sein. Wenn die LDAP-Authentifizierung deaktiviert ist (weil beispielsweise nur zertifikatbasierte Authentifizierung verwendet wird), müssen Benutzer eine Citrix PIN festlegen. In diesem Fall fordert XenMobile die Citrix PIN an, selbst wenn **ENABLE_PASSCODE_AUTH** auf

false festgelegt ist.

Setzen Sie **ENABLE_PASSCODE_AUTH** auf **false**, damit Benutzer beim Starten einer App auf eine Aufforderung zur Verwendung von Touch ID reagieren müssen.

Mögliche Werte: **true** oder **false**

Standardwert: **false**

ENABLE_WORXHOME_CEIP

Anzeigename: Enable Worx Home CEIP

Diese Eigenschaft 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_WORXHOME_GA

Anzeigename: Enable Google Analytics in Worx Home

Mit dieser Eigenschaft 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 Secure Hub (Worx Home) anmeldet.

Mögliche Werte: **true** oder **false**

Standardwert: **true**

ENCRYPT_SECRETS_USING_PASSCODE

Anzeigename: Encrypt secrets using Passcode

Mit dieser Eigenschaft können vertrauliche Daten auf Mobilgeräten in einem Geheimtresor statt in einem plattformbasierten systemeigenen Speicher (z. B. iOS-Schlüsselbund) gespeichert werden. Die Eigenschaft 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 diese Eigenschaft aktivieren, um eine höhere Sicherheit auf den Benutzergeräten zu erzielen. Die Benutzer werden im Ergebnis häufiger zur Authentifizierung mit der Citrix PIN aufgefordert.

Mögliche Werte: **true** oder **false**

Standardwert: **false**

INACTIVITY_TIMER

Anzeigename: Inactivity Timer

Diese Eigenschaft definiert die Zeitdauer (in Minuten), die ein Gerät inaktiv sein darf, bevor Benutzer zur Eingabe von

Citrix 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 der App-Passcode auf "Aus" festgelegt ist, werden die Benutzer für eine vollständige Authentifizierung an Secure Hub 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 Secure Hub für MDX- und Nicht-MDX-Apps.

Mögliche Werte: beliebige Ganzzahl

Standardwert: **15**

ON_FAILURE_USE_EMAIL

Anzeigename: On failure use Email to send device logs to IT help desk.

Mit dieser Eigenschaft 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_EXPIRY

Anzeigename: PIN Change Requirement

Diese Eigenschaft definiert, wie lange (in Tagen) die Citrix PIN bzw. der Citrix Passcode gültig ist. Nach diesem Zeitraum müssen die Benutzer die PIN bzw. den Passcode ändern. Wenn Sie diese Einstellung ändern, tritt der neue Wert erst in Kraft, wenn die aktuelle Citrix PIN bzw. der aktuelle Citrix Passcode eines Benutzers abläuft.

Mögliche Werte: **1** oder höher, **99** wird empfohlen 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.

Standardwert: **90**

PASSCODE_HISTORY

Anzeigename: PIN History

Diese Eigenschaft definiert die Zahl der bereits verwendeten Citrix 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.

Zulässige Werte: **1–99**

Standardwert: **5**

PASSCODE_MAX_ATTEMPTS

Anzeigename: PIN Attempts

Diese Eigenschaft legt fest, wie viele Falscheingaben der Citrix PIN bzw. des Worx-Passcodes zulässig sind, bevor die Benutzer zu einer vollständigen Authentifizierung aufgefordert werden. Nach einer vollständigen Authentifizierung werden die Benutzer aufgefordert, eine neue Citrix PIN bzw. einen neuen Passcode zu erstellen.

Mögliche Werte: beliebige Ganzzahl

Standardwert: **15**

PASSCODE_MIN_LENGTH

Anzeigename: PIN Length Requirement

Diese Eigenschaft definiert die Mindestlänge der Citrix PIN.

Zulässige Werte: **1–99**

Standardwert: **6**

PASSCODE_STRENGTH

Anzeigename: PIN Strength Requirement

Diese Eigenschaft definiert die Sicherheit der Citrix PIN bzw. des Citrix Passcodes. Wenn Sie diese Einstellung ändern, werden die Benutzer zum Festlegen einer neuen Citrix PIN bzw. eines neuen Citrix Passcodes aufgefordert, wenn sie sich das nächste Mal authentifizieren.

Mögliche Werte: **Low**, **Medium** und **Strong**

Standardwert: **Medium**

In der folgenden Tabelle werden die Kennwortregeln für die einzelnen Sicherheitseinstellungen gemäß PASSCODE_TYPE-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 Zahlen dürfen nicht alle gleich sein. Beispiel: 444444 ist nicht zulässig. 2. Alle Zahlen dürfen nicht aufeinanderfolgend sein. Beispiel: 123456 oder 654321 ist nicht zulässig.	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:

	Zulässig: 444333, 124567, 136790, 555556, 788888	abcd12, bcd123, 123abc, xy1234, xyz345 oder cba123 sind nicht zulässig. Zulässig: aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~
Hoch	Wie Einstellung "Medium" für Citrix PIN	Der Passcode muss mindestens einen Großbuchstaben und einen Kleinbuchstaben enthalten. Nicht zulässig: abcd12, DFGH2 Zulässig: Abcd12, jkrtA2, 23Bc#, AbCd
Strong	Wie Einstellung "Medium" für Citrix 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_TYPE

Anzeigename: PIN Type

Diese Eigenschaft definiert, ob Benutzer eine numerische Citrix PIN oder einen alphanumerischen Passcode festlegen können. Wenn Sie **Numeric** auswählen, können Benutzer nur eine numerische Citrix PIN festlegen. Wenn Sie **Alphanumeric** auswählen, können Benutzer eine Kombination aus Buchstaben und Ziffern (Passcode) festlegen.

Wenn Sie diese Einstellung ändern, müssen die Benutzer eine neue Citrix PIN bzw. einen neuen Passcode festlegen, wenn sie das nächste Mal zur Authentifizierung aufgefordert werden.

Mögliche Werte: **Numeric** oder **Alphanumeric**

Standardwert: **Numeric**

REFRESHINTERVAL

Anzeigename: REFRESHINTERVAL

In der Standardeinstellung sendet XenMobile dem Auto Discovery Server (ADS) alle 3 Tage einen Ping-Befehl für gepinnte Zertifikate. Zum Ändern des Aktualisierungsintervalls gehen Sie zu **Einstellungen > Clienteigenschaften**, fügen Sie den benutzerdefinierten Schlüssel **REFRESHINTERVAL** hinzu und legen Sie den **Wert** auf die Anzahl der

Stunden fest.

Der Standardwert ist 72 Stunden (3 Tage).

SEND_LDAP_ATTRIBUTES

Für Nur-MAM-Bereitstellungen können Sie XenMobile so konfigurieren, dass Benutzer, die sich mit einem iOS- oder Android-Gerät bei Secure Hub mit E-Mail-Anmeldeinformationen registrieren, automatisch bei Secure Mail registriert werden. Die Benutzer müssen dann für die Registrierung bei Secure Mail keine weiteren Informationen eingeben und keine zusätzlichen Schritte ausführen. Sie müssen die Servereigenschaft MAM_MACRO_SUPPORT festlegen.

Zum Konfigurieren dieser globalen Clientrichtlinie gehen Sie zu **Einstellungen > Clienteigenschaften**, fügen den benutzerdefinierten Schlüssel **SEND_LDAP_ATTRIBUTES** hinzu und legen den **Wert** wie folgt fest.

Wert: userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}

Die Attributwerte werden ähnlich wie bei MDM-Richtlinien in Form von Makros angegeben.

Beispiel einer Kontodienstantwort für diese Eigenschaft:

Hinweis: Bei dieser Eigenschaft behandelt XenMobile Kommas als Abschlusszeichen. Daher muss vor Kommas innerhalb von Attributwerten ein umgekehrter Schrägstrich gesetzt werden, damit sie vom Client nicht als Ende des Attributwerts interpretiert werden. Schreiben Sie den umgekehrten Schrägstrich "\\".

ActiveSync Gateway

Feb 24, 2017

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. Für jede Regel können Sie **Zulassen** oder **Verweigern** auswählen. Die Standardeinstellung ist **Zulassen**.

Weitere Informationen zur App-Zugriffsrichtlinie finden Sie unter App-Zugriffsrichtlinien für Geräte.

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 "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 Rooting

bzw. Jailbreak vorliegt.

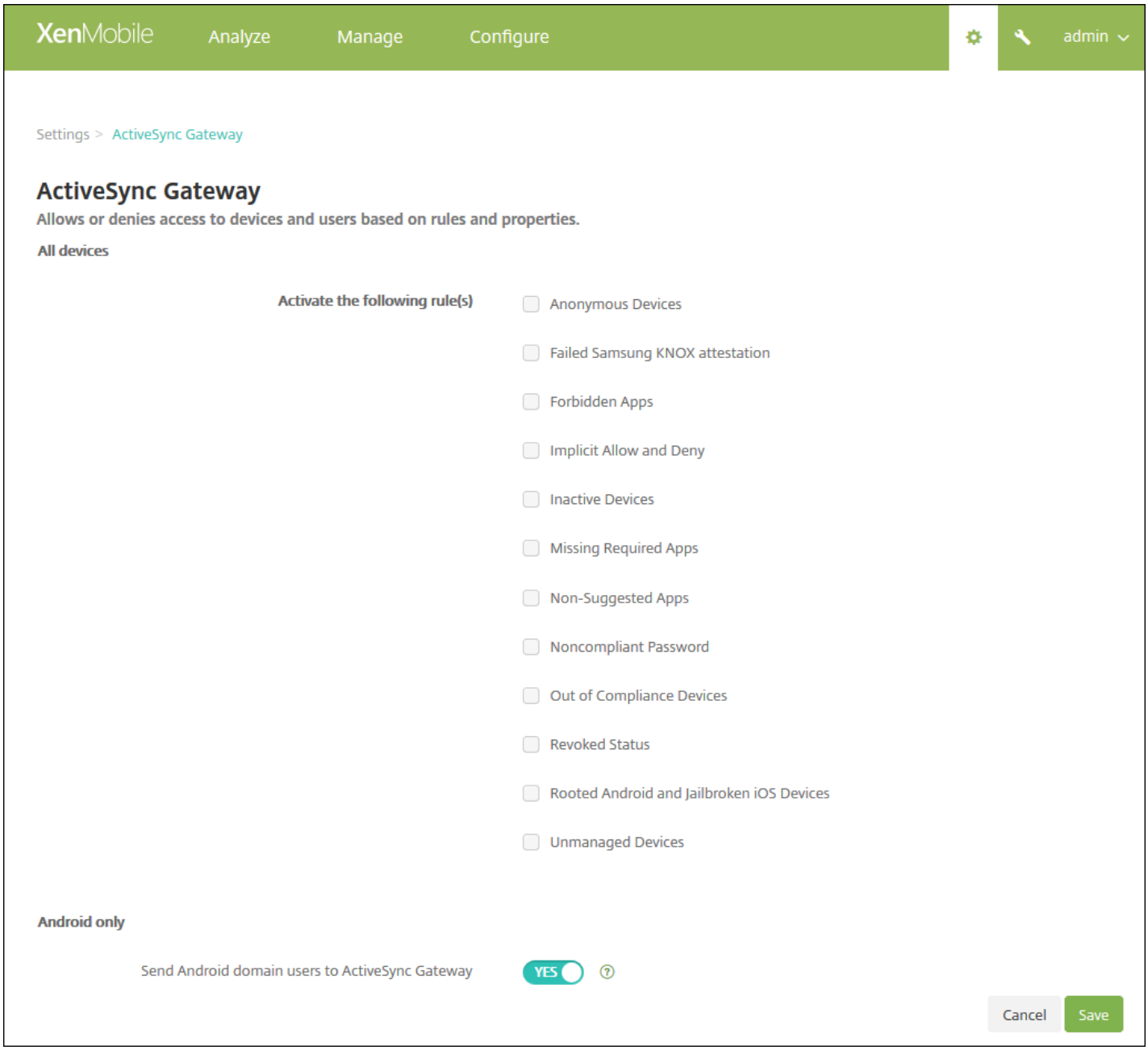
Nicht verwaltete Geräte: prüft, ob ein Gerät verwaltet, d. h. von XenMobile kontrolliert wird. Beispielsweise ist ein Gerät im MAM-Modus oder ein nicht registriertes Gerät nicht verwaltet.

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**.

Netzwerkzugriffssteuerung (NAC)

Feb 24, 2017

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. Weitere Informationen zur App-Zugriffsrichtlinie finden Sie unter App-Zugriffsrichtlinien für Geräte.

Inaktive Geräte: prüft, ob ein Gerät entsprechend dem unter "Schwellenwert für Tage inaktiv" in den Servereigenschaften festgelegten Wert inaktiv ist. Einzelheiten finden Sie unter Servereigenschaften.

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 Rooting bzw. Jailbreak vorliegt.

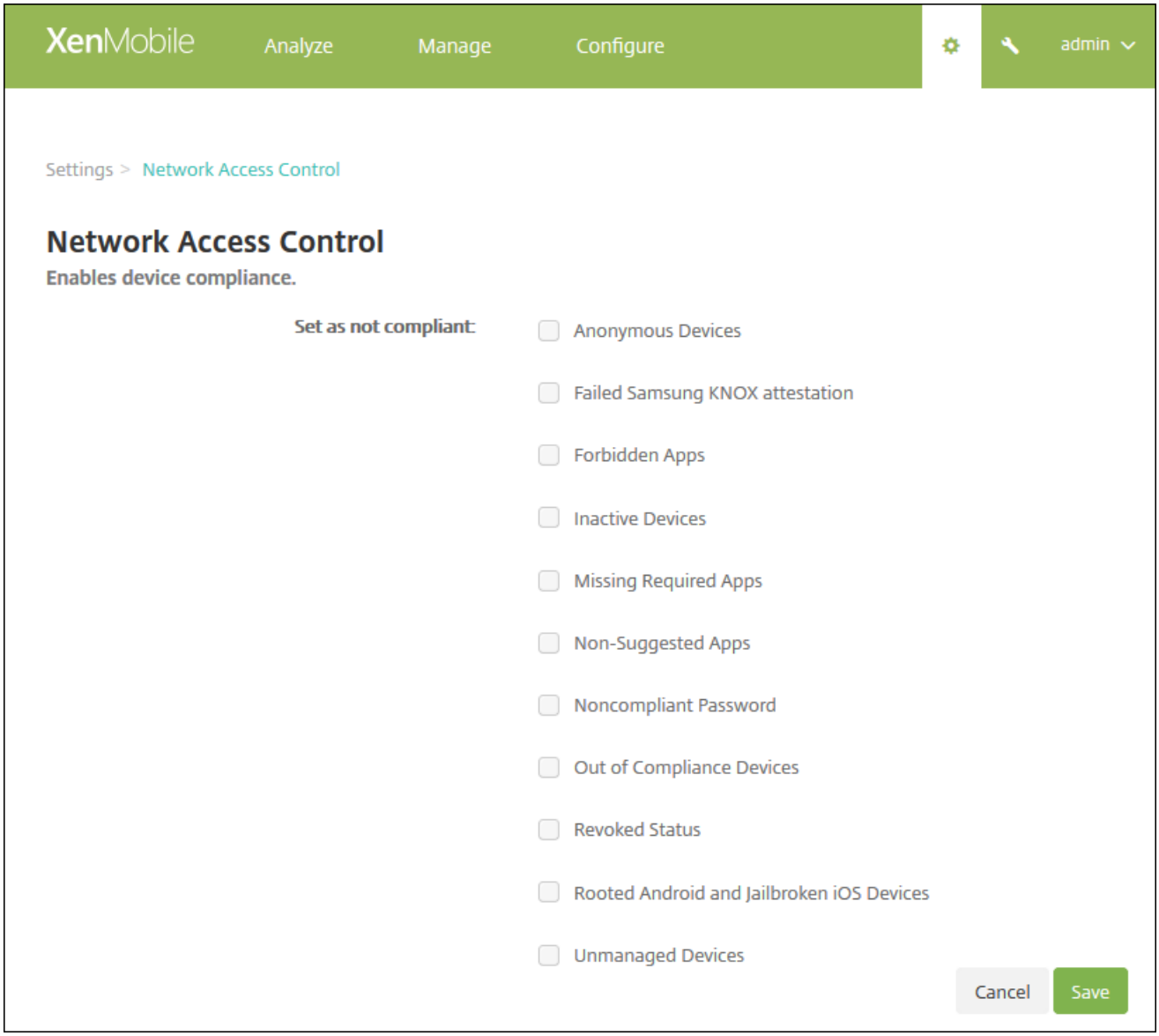
Nicht verwaltete Geräte: prüft, ob ein Gerät verwaltet, d. h. von XenMobile kontrolliert wird. Beispielsweise ist ein Gerät im MAM-Modus oder ein nicht registriertes Gerät nicht verwaltet.

> **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

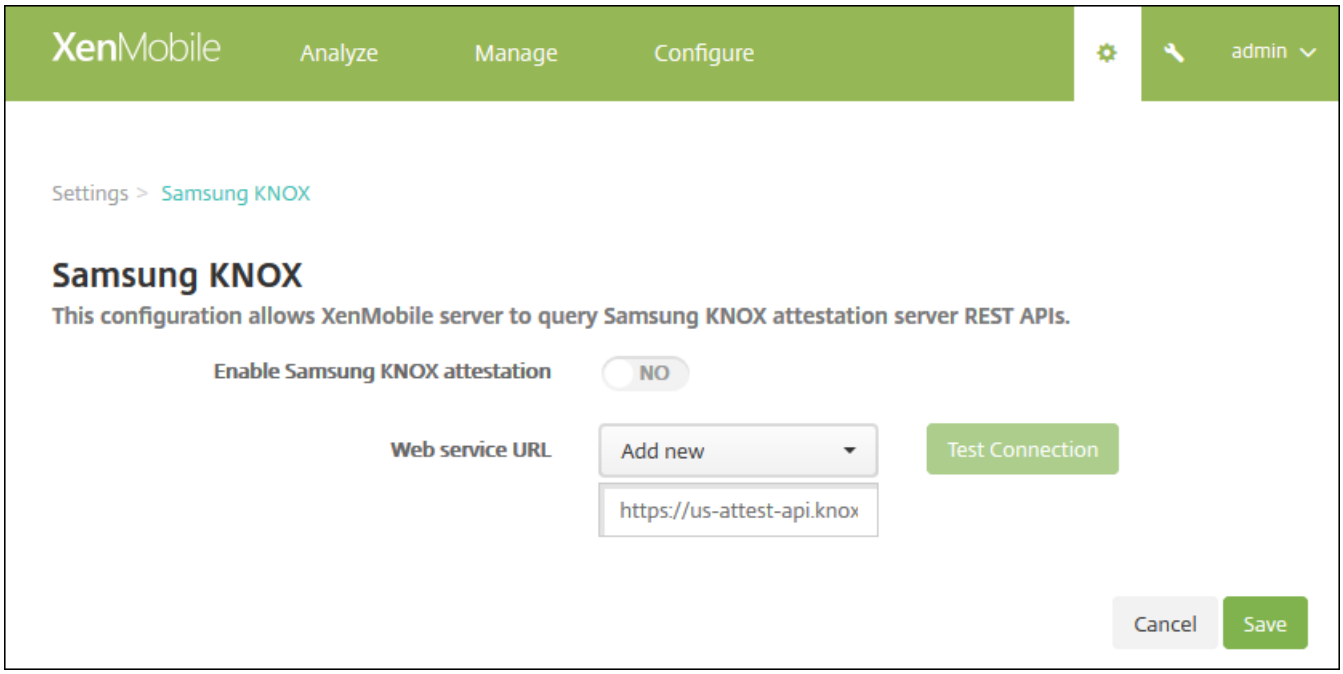
Feb 24, 2017

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 **Plattformen** auf **Samsung KNOX**. Die Seite **Samsung KNOX** wird angezeigt.



3. Wählen Sie für **Samsung KNOX-Nachweis aktivieren** aus, ob der Samsung KNOX-Nachweis aktiviert werden soll. Der Standardwert ist **NEIN**.

4 . Wenn Sie **Samsung KNOX-Nachweis aktivieren** auf **JA**festlegen, wird die Option **Webdienst-URL** aktiviert. Führen Sie einen der folgenden Schritte aus:

a. Klicken Sie auf den geeigneten Nachweisserver.

b. Klicken Sie auf **Neu hinzufügen** und geben Sie dann die Webdienste-URL ein.

5. Klicken Sie auf **Verbindung testen**, um die Verbindung zu prüfen. Es wird dann ein Erfolg oder Fehler gemeldet.

6. Klicken Sie auf **Speichern**.

Hinweis

Verwenden Sie Samsung KNOX Mobile Enrollment, um mehrere Samsung KNOX-Geräte bei XenMobile (oder einem beliebigen Manager für mobile Geräte) zu registrieren, ohne Geräte einzeln manuell zu konfigurieren. Weitere Informationen finden Sie unter Samsung KNOX Massenregistrierung.

Google Cloud Messaging

Apr 24, 2017

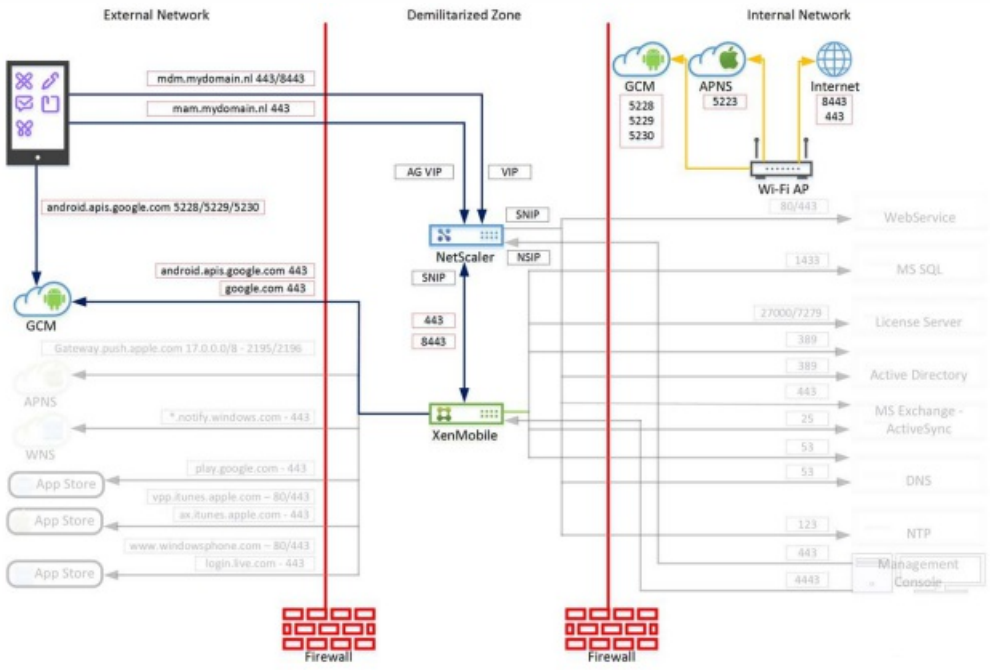
Alternativ zur Richtlinie **Aktives Abfrageintervall** können Sie mit Firebase Cloud Messaging (FCM) steuern, wie und wann Android-Geräte eine Verbindung mit XenMobile herstellen. Bei Verwendung der folgenden Konfiguration lösen Sicherheitsaktionen oder Bereitstellungsbefehle eine Pushbenachrichtigung aus, mit der der Benutzer aufgefordert wird, erneut eine Verbindung zum XenMobile-Server herzustellen.

Voraussetzungen

- XenMobile 10.3.x
- Neuester Secure Hub-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 FCM im externen und internen Netzwerk dargestellt.

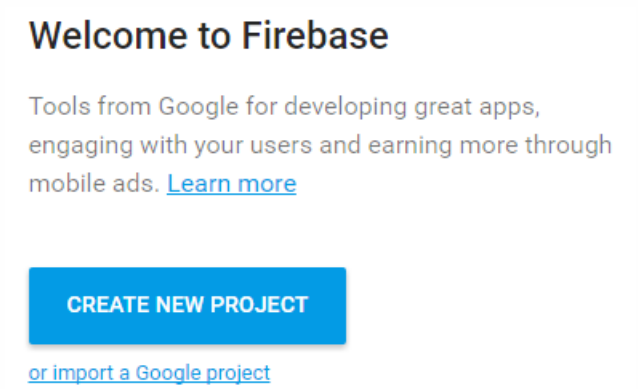


Konfigurieren Ihres Google-Kontos für FCM

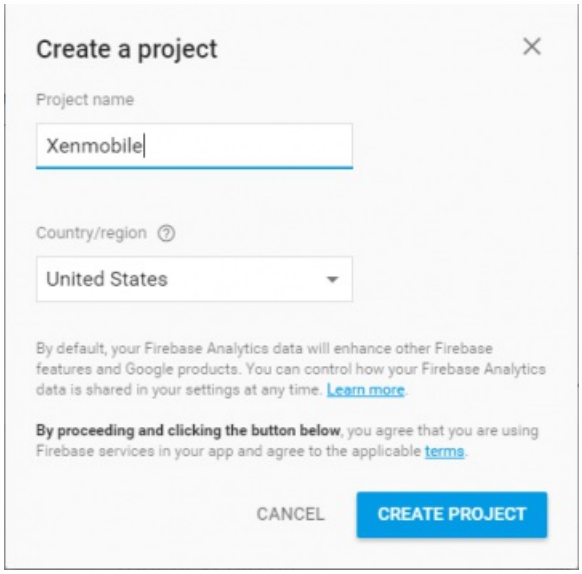
1. Melden Sie sich bei der folgenden URL mit den Anmeldeinformationen für Ihr Google Developer-Konto an:

   https://console.firebase.google.com/?pli=1

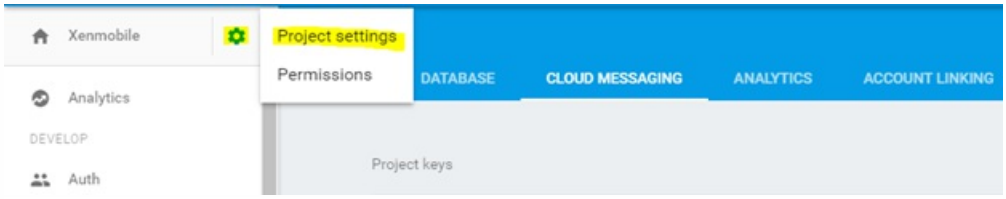
2. Klicken Sie auf **Create a project**.



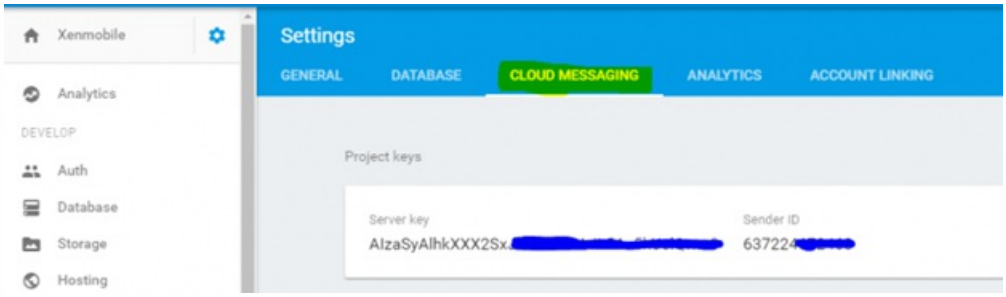
3. Geben Sie unter **Project name** einen Namen ein und klicken Sie auf **Create Project**.



4. Klicken Sie auf das Zahnradsymbol neben dem Projektnamen oben links und dann auf **Project Settings**.



5. Wählen Sie die Registerkarte **Cloud Messaging** aus. Auf dieser Seite finden Sie die Absender-ID und den Serverschlüssel. Kopieren Sie diese Werte, da sie auf dem XenMobile-Server bereitgestellt werden müssen. Es muss darauf hingewiesen werden, dass nach September 2016 alle Serverschlüssel in der Firebase-Konsole erstellt werden müssen.

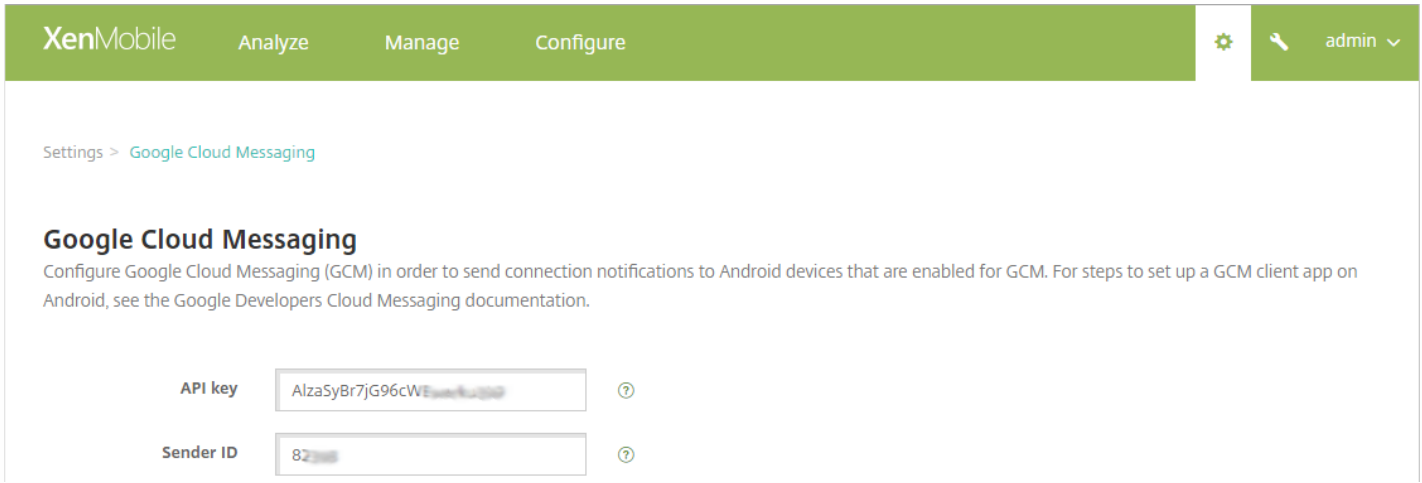


Konfigurieren von XenMobile für GCM

1. Melden Sie sich bei der XenMobile-Konsole an und klicken Sie auf **Einstellungen > Servereigenschaften**. Geben Sie in der Suchleiste **GCM** ein und klicken Sie auf "Suchen".

    a. Bearbeiten Sie den **GCM API-Schlüssel** und geben Sie den Firebase Cloud Messaging API-Schlüssel ein, den Sie im letzten Schritt der Konfiguration von Firebase Cloud Messaging kopiert haben.

    b. Bearbeiten Sie die **GCM Absender-ID** und geben Sie den Wert der Absender-ID ein, die Sie im vorherigen Vorgang notiert haben.



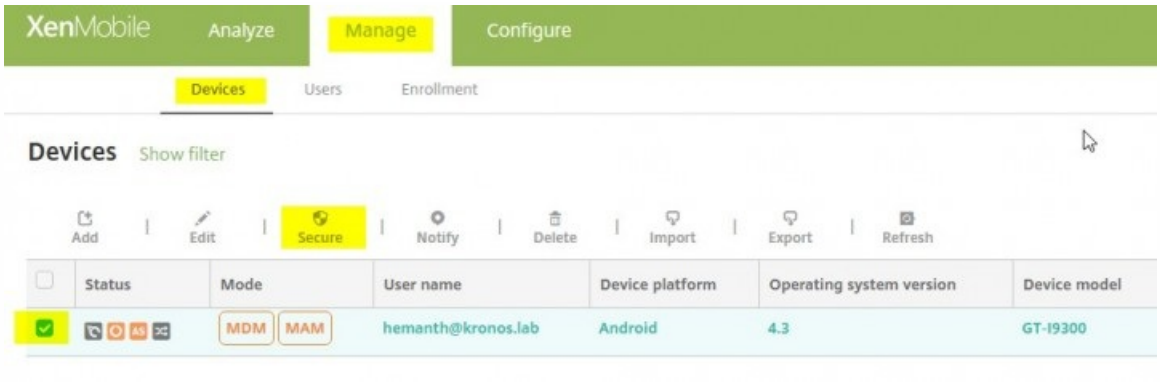
Testen der Konfiguration

Voraussetzung für das Testen der FCM-Konfiguration ist, dass keine **Planungsrichtlinie** konfiguriert ist. Legen Sie alternativ dazu die Richtlinie nicht auf **Immer** fest. Weitere Informationen zum Konfigurieren der **Planungsrichtlinie** finden Sie unter der Geräterichtlinie Planung.

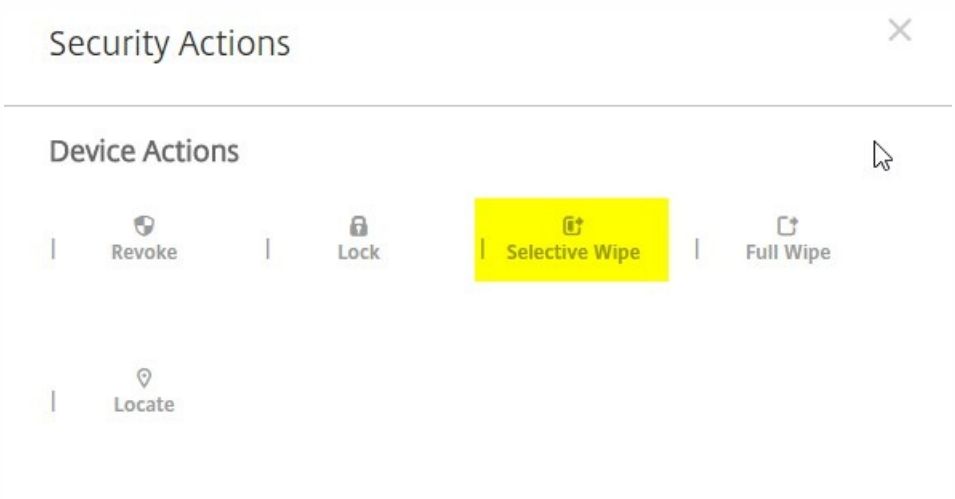
1. Registrieren Sie ein Android-Gerät.

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-Konsole 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.

Google Play-Anmeldeinformationen

Feb 24, 2017

XenMobile verwendet Google Play-Anmeldeinformationen zum Extrahieren von App-Informationen für Geräte.

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.

Hinweis

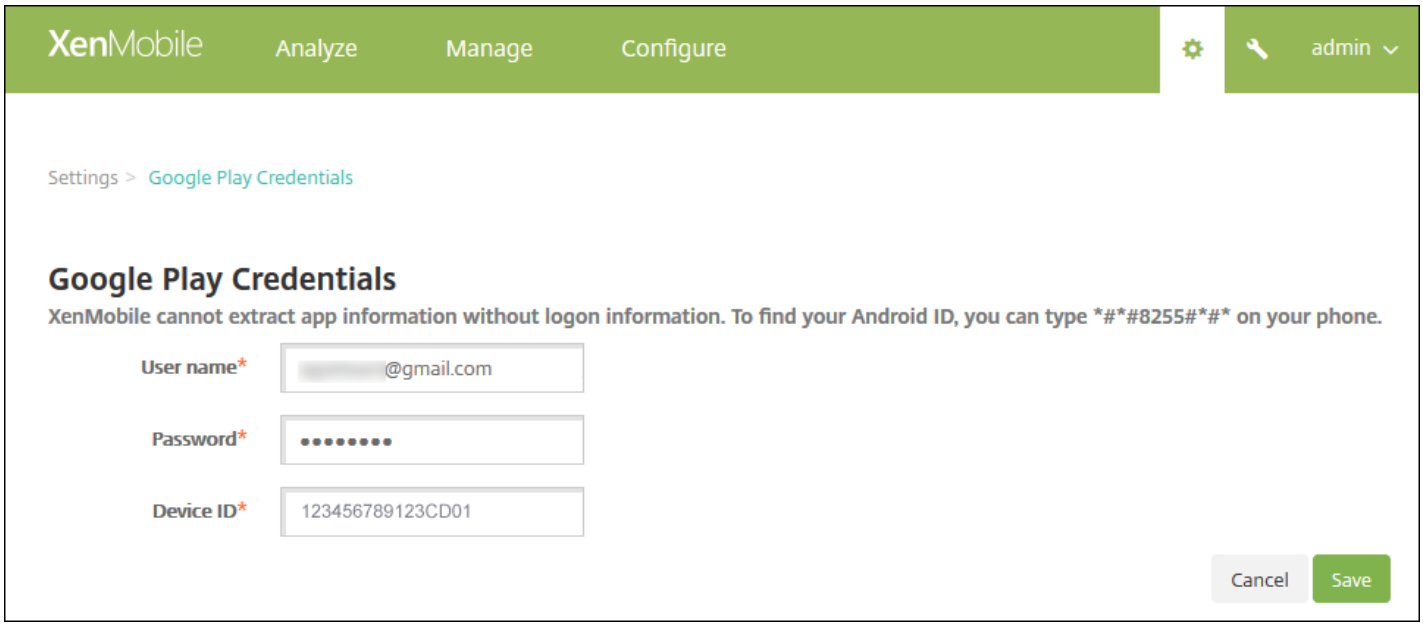
Bei der Suche nach Google Play-Apps in der XenMobile-Konsole werden Apps basierend auf dem Android-Betriebssystem des registrierten Geräts angezeigt. Auf einem Samsung S6 Edge-Gerät wird z. B. die Betriebssystemversion 6.0.1 ausgeführt. Wenn Sie nach Apps suchen, werden nur diejenigen im Suchergebnis angezeigt, die mit Android 6.0.1 kompatibel sind.

Important

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 **Plattformen** 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.
  Informationen zum Ermitteln der Android-ID finden Sie weiter oben in diesem Artikel.

3. Klicken Sie auf **Speichern**.

Geräterichtlinien

Apr 24, 2017

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 Plattformen und sogar zwischen Android-Geräten verschiedener Hersteller. Eine Matrix mit Richtlinien nach Plattform finden Sie in der PDF-Datei 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-Synchronisierung	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 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	Mit der Geräterichtlinie für App-Attribute können Sie für iOS-Geräte Attribute angeben (z. B. eine Paket-ID für die verwaltete App oder die ID für den VPN-Zugriff pro App).
App-Konfiguration	Mit dieser Richtlinie können Sie diverse Einstellungen und Verhalten von Apps, die eine verwaltete Konfiguration unterstützen, remote konfigurieren indem Sie eine XML-Konfigurationsdatei ("Eigenschaftenliste" bzw. "plist") auf iOS-Geräten oder Schlüssel/Wert-Paare für Windows Phones und Windows 10-Tablets/-PCs bereitstellen.
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 die 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. Das bedeutet, dass Benutzer ihr Gerät nur zum Ausführen einer einzigen App verwenden 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 über Browsergeräterichtlinien festlegen, ob auf den Benutzergeräten der Browser verwendet werden kann und welche Browserfunktionen verwendet werden können. Auf Samsung-Geräten können Sie den Browser vollständig deaktivieren oder Popupfenster, JavaScript, Cookies, automatisches Ausfüllen und Betrugswarnungen aktivieren oder deaktivieren.
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.
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.
Kopieren von Apps in den Samsung-Container	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 dort 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.
Kopieren von Apps in den Samsung-Container	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 dort 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.
Löschen von Dateien und Ordnern	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 • BitLocker-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 Gerätnamensrichtlinie können Sie Namen für iOS- und Mac OS X-Geräte festlegen, 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-Secure Hub. Zum Hochladen von Secure Hub für Windows Phone für XenMobile Enterprise Edition dürfen Sie beispielsweise nicht mehrere Unternehmenshubrichtlinien mit mehreren Versionen von Secure Hub 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 Secure Mail-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.
Launcher-Konfiguration	Mit dieser Richtlinie für Android-Geräte können Sie festlegen, welche Apps von Citrix Launcher zugelassen werden, ein benutzerdefiniertes Logo für das Citrix Launcher-Symbol und ein benutzerdefiniertes Hintergrundbild für Citrix Launcher auswählen und Kennwortanforderungen zum Beenden von Citrix Launcher festlegen.
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 Secure Hub 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.
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 im Versand von Provisioningprofilen an Benutzer per E-Mail und in der Bereitstellung der Profile auf einem Webportal zum Herunterladen und Installieren. 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 beim Antippen normal geöffnet und verwendet werden können.
Entfernen des Provisioningprofils	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 und 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.
Remotesupport	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	Über die Einschränkungsrichtlinie können Administratoren Features und Funktionalität auf verwalteten Geräten sperren und 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" (nicht zugelassen) 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 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.
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 Secure Hub 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".
Planung	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 FCM 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.
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

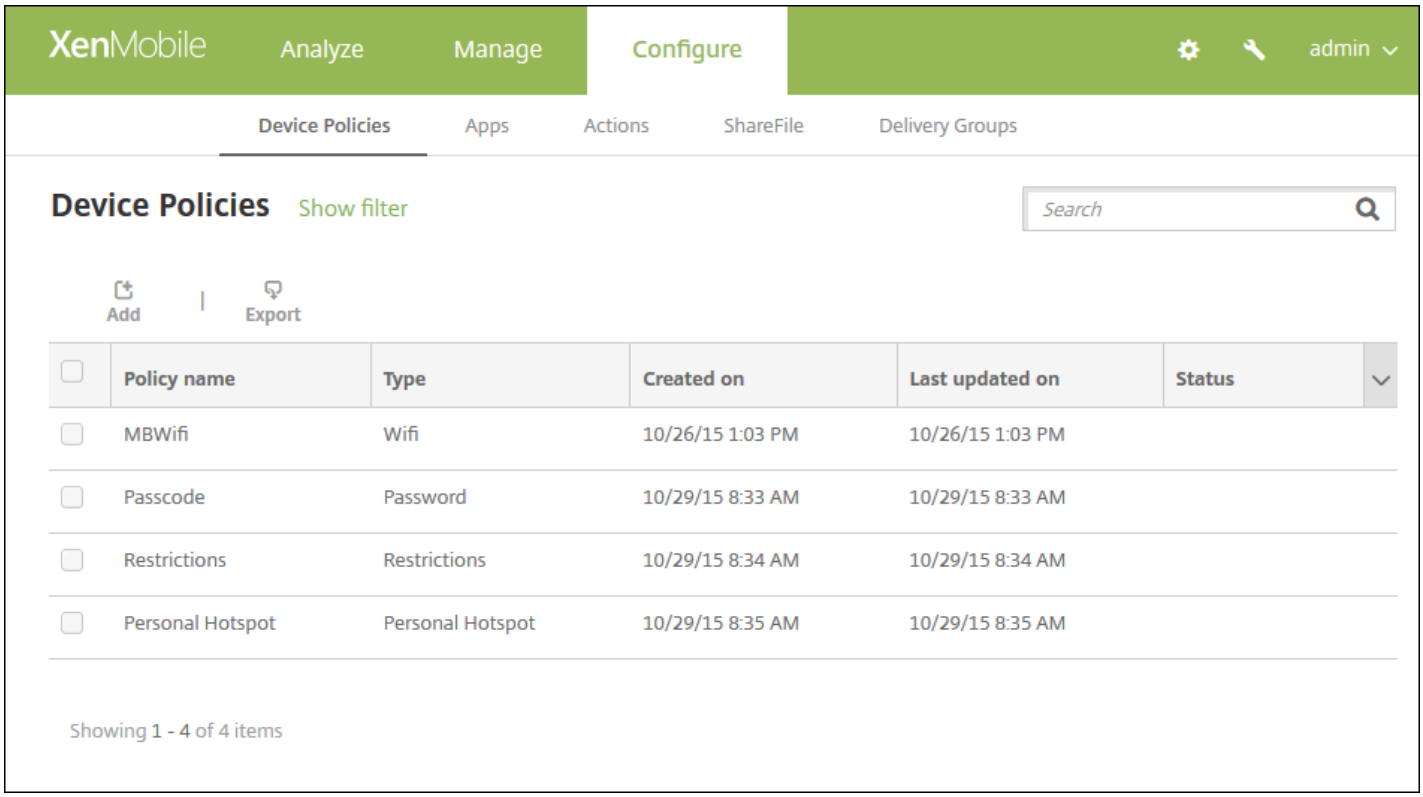
	installieren können.
Single Sign-On-Konto	Sie erstellen Single Sign-On-Konten (SSO) in XenMobile, damit Benutzer nach einmaliger Anmeldung auf XenMobile und interne Unternehmensressourcen von unterschiedlichen Apps aus zugreifen können. Sie müssen keine Anmeldeinformationen auf dem Gerät speichern. Die 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.
Store	Sie können in XenMobile eine Richtlinie erstellen, mit der Sie angeben, ob auf dem Homebildschirm von iOS-, Android- und Windows Tablet-Geräten ein XenMobile Store-Webclip angezeigt wird.
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 abonniert werden können, 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 ("Webclips") zu 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; bei Windows-Tablets sind nur eine Beschriftung und eine URL erforderlich.
WiFi	Mit der WiFi-Richtlinie können Administratoren bequem WiFi-Routerdetails, SSID, Authentifizierungs- und Konfigurationsdaten per Push auf verwalteten Geräten bereitstellen. Mit WiFi-Richtlinien legen Sie fest, wie Benutzer 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 Geräteplattformen vorgeben.
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.
XenMobile-Optionen	Sie fügen eine XenMobile-Optionsrichtlinie hinzu, um das Secure Hub-Verhalten für Verbindungen zwischen XenMobile und Android- bzw. Windows Mobile/CE-Geräten zu konfigurieren.

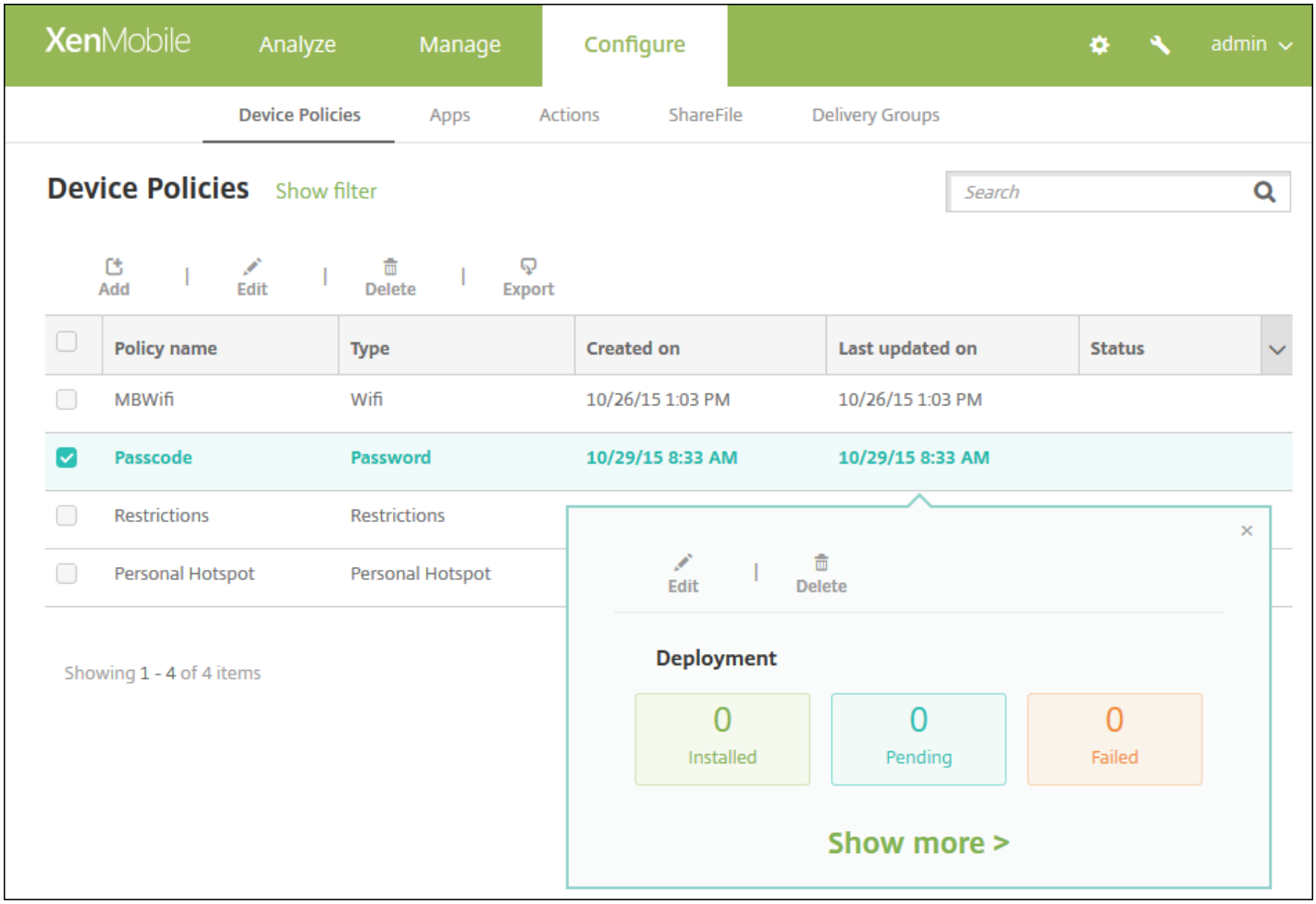
XenMobile-Deinstallation	Sie können in XenMobile diese Geräterichtlinie hinzufügen, um XenMobile von Android- und Windows Mobile-/CE-Geräten zu deinstallieren. Wenn diese Richtlinie bereitgestellt wird, entfernt sie XenMobile von allen Geräten in der Bereitstellungsgruppe.

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.

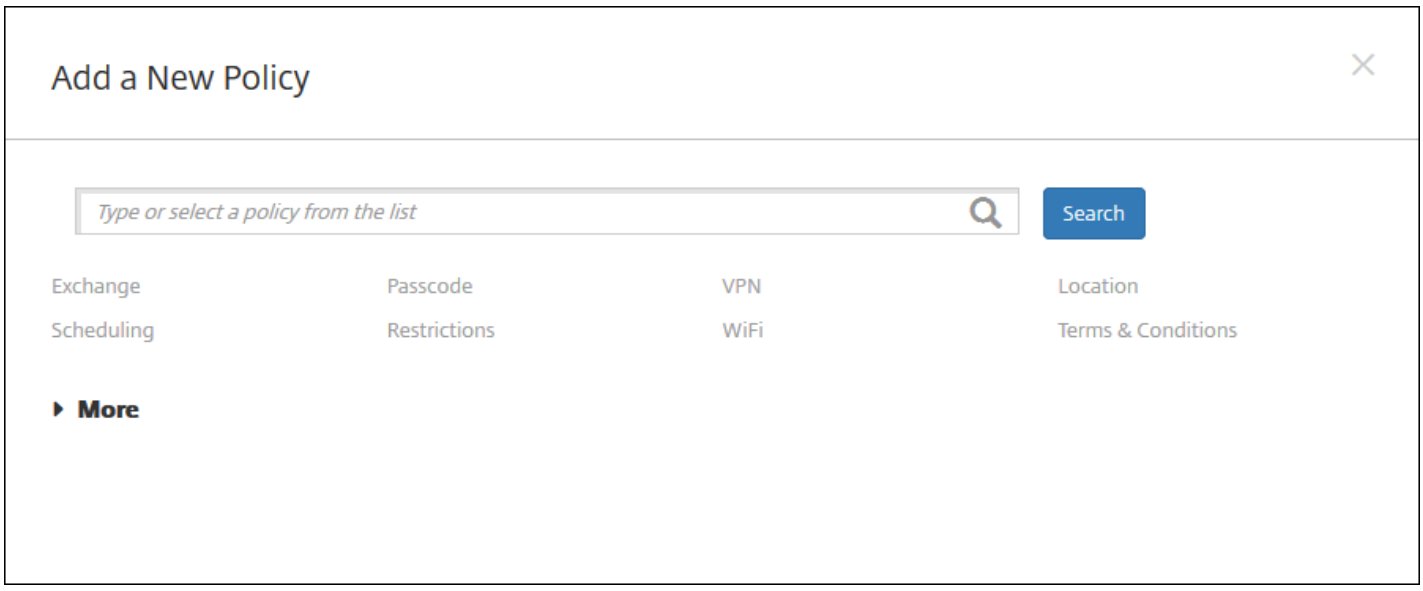


Zum Bearbeiten oder Löschen einer Richtlinie auf der Seite **Geräterichtlinien** können Sie das Kontrollkästchen neben der Richtlinie auswählen, um das Menü mit den Optionen oberhalb der Liste einzublenden, oder auf eine Richtlinie in der Liste klicken, um das Menü rechts neben dem Eintrag einzublenden.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



1.Klicken Sie auf der Seite **Gerätерichtlinien** auf **Hinzufügen**.

Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt. Mit **Mehr** können Sie weitere Richtlinien einblenden.

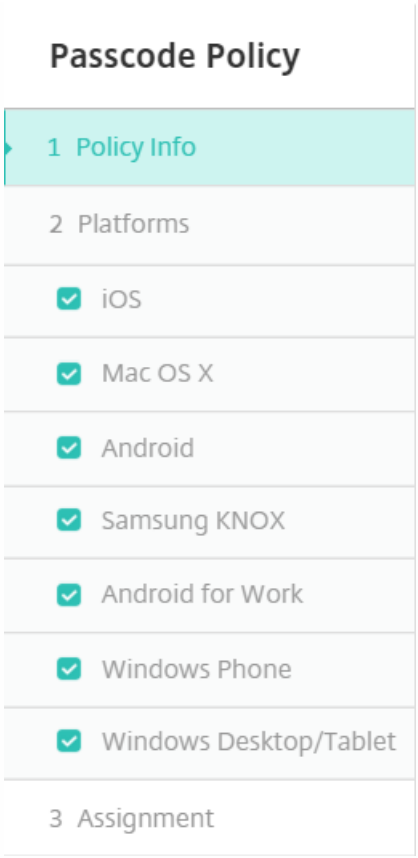


2. Zur Auswahl der gewünschten Richtlinie haben Sie folgende Möglichkeiten:

- 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.

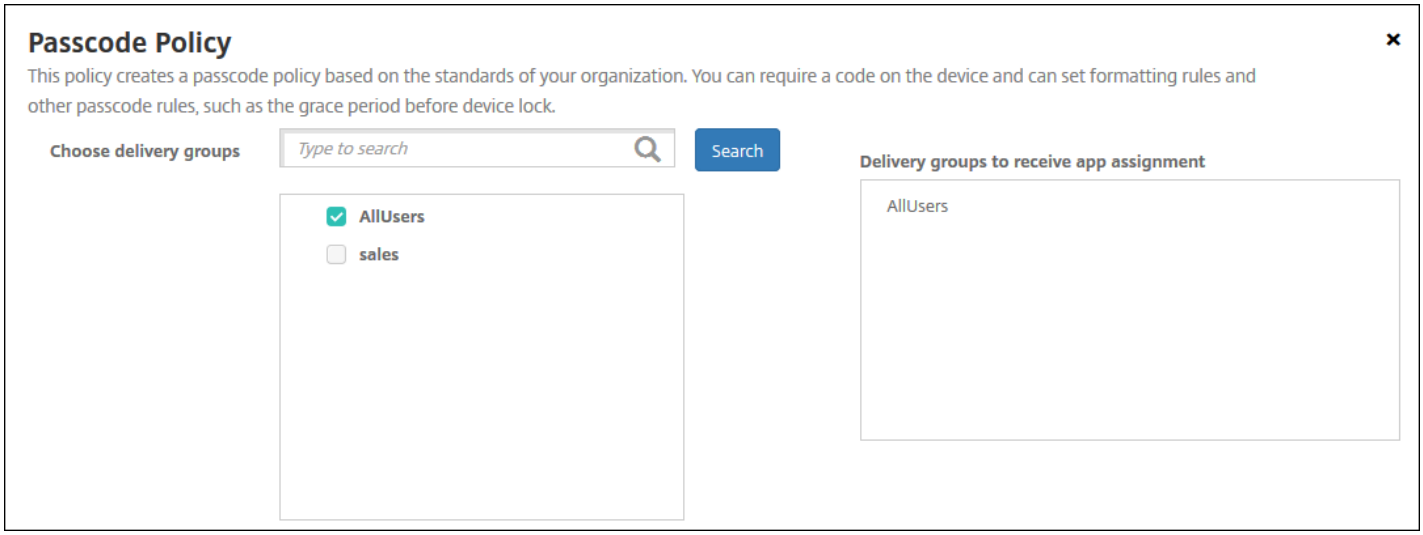


4. Geben Sie die erforderlichen Informationen auf der Seite **Richtlinieninformationen** ein und klicken Sie dann auf **Weiter**. Die Seite **Richtlinieninformationen** enthält Informationen zum Identifizieren und Verfolgen von Richtlinien (z. B. Richtlinienname). Diese Seite ist bei allen Richtlinien 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 **Geräterichtlinien** hinzugefügt.

1. Aktivieren Sie in der Tabelle **Geräterichtlinien** 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

Apr 24, 2017

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 10.4 unterstützt Geräterichtlinien für folgende Plattformen:

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Android
- Samsung SAFE
- Samsung SEAMS
- Windows Mobile/CE
- Windows Phone 8/Windows 10 Mobile
- Windows 8 und Windows 10 Desktop/Tablet (.86)

Informationen zu den in XenMobile 10.x unterstützten Geräten finden Sie unter Unterstützte Geräteplattformen.

Hinweis

- Unterstützung für Symbian-Geräte gibt es in XenMobile 10.3 nicht mehr.
- Wenn die Umgebung mit Gruppenrichtlinienobjekten (GPOs) konfiguriert ist, müssen Sie beim Konfigurieren der XenMobile-Geräterichtlinien für Windows 10 die folgende Regel berücksichtigen. Wenn eine Richtlinie auf einem oder mehreren registrierten Windows 10-Geräten Konflikte verursacht, hat die an das GPO angepasste Richtlinie Vorrang.

Geräterichtlinie für die AirPlay-Synchronisierung

Feb 24, 2017

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.

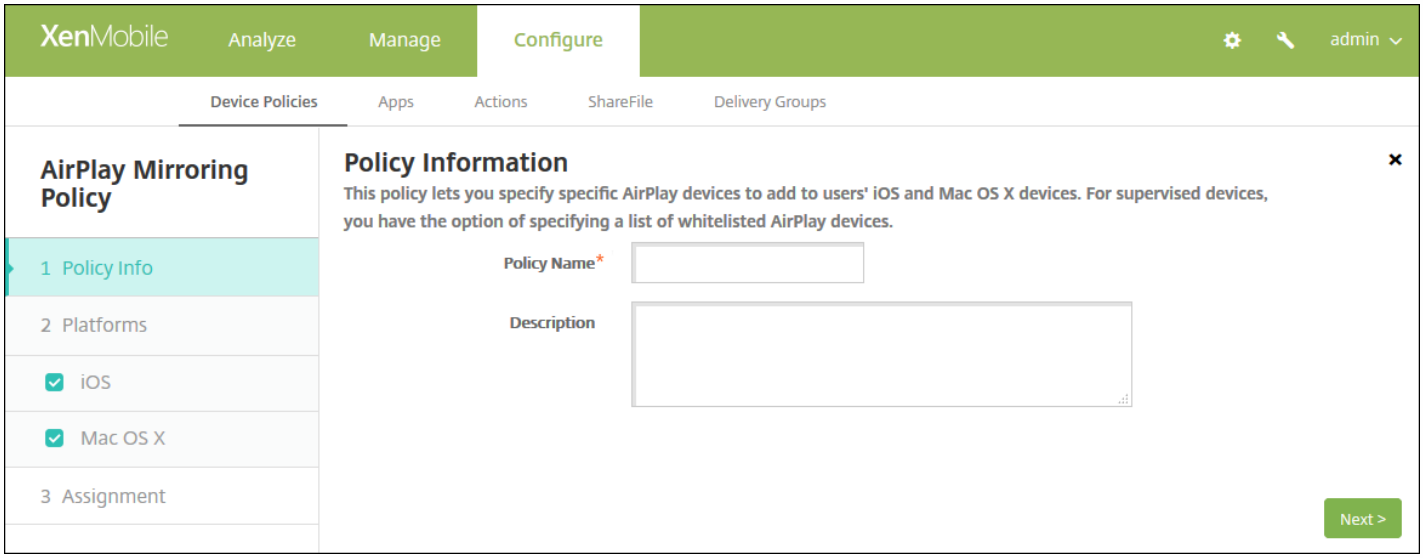
Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen spezifischer AirPlay-Geräte (z. B. Apple TV oder einen anderen Mac-Computer) einrichten und iOS-Geräten hinzufügen. Zudem können Sie Geräte zu einer Positivliste überwachter Geräte hinzufügen, sodass Benutzer nur die AirPlay-Geräte auf der 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.



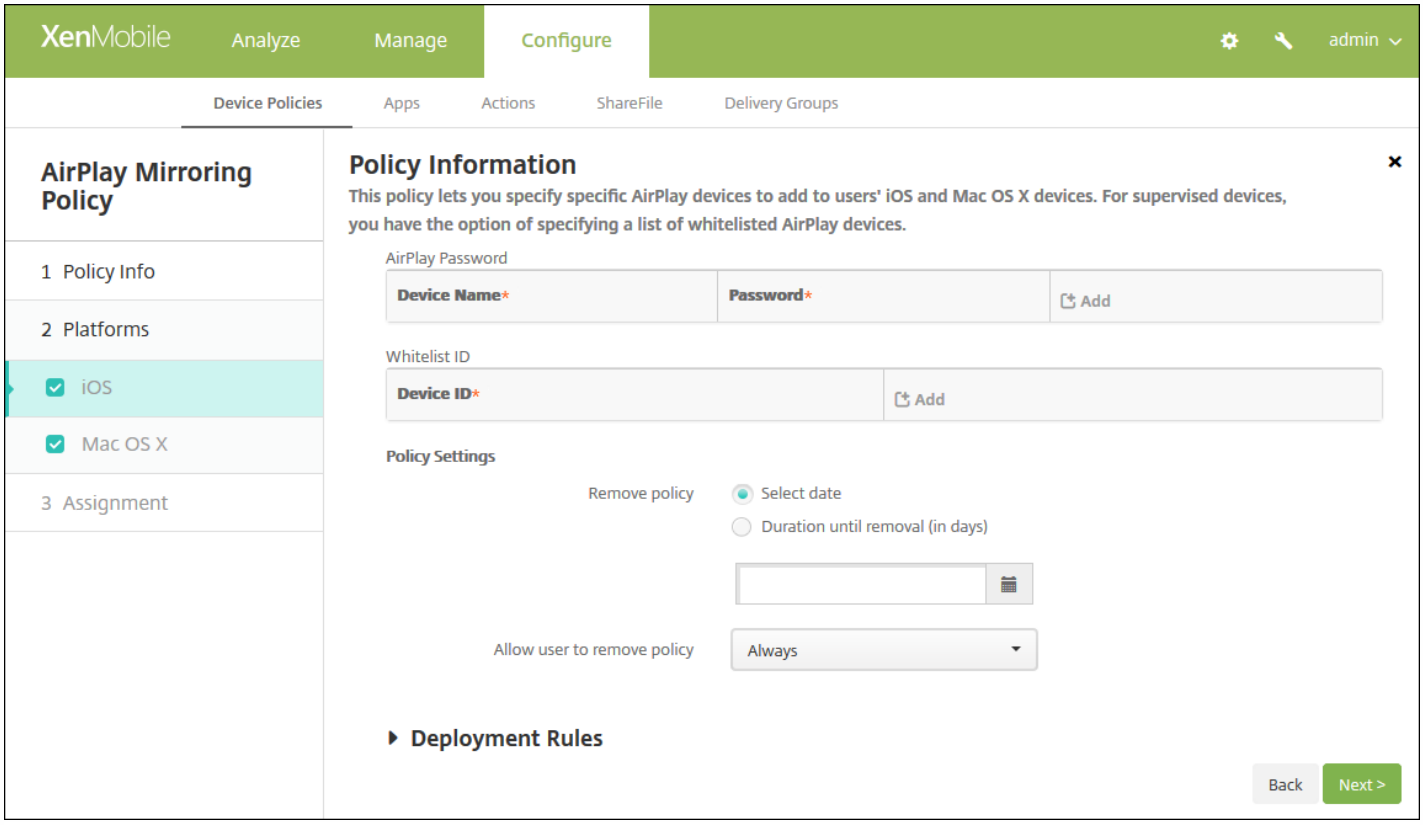
4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

- **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.



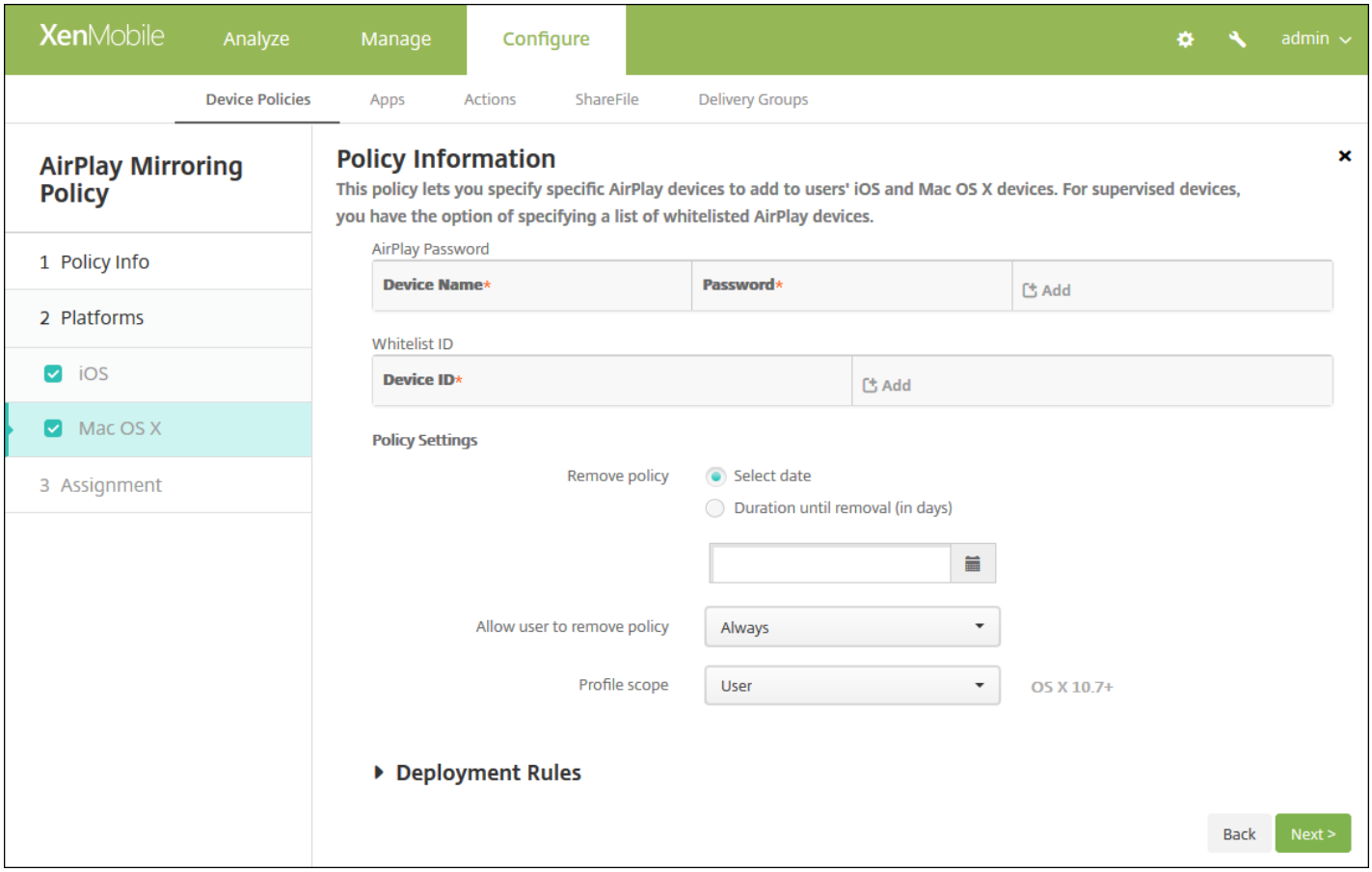
Konfigurieren Sie folgende Einstellungen:

- **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 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 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.

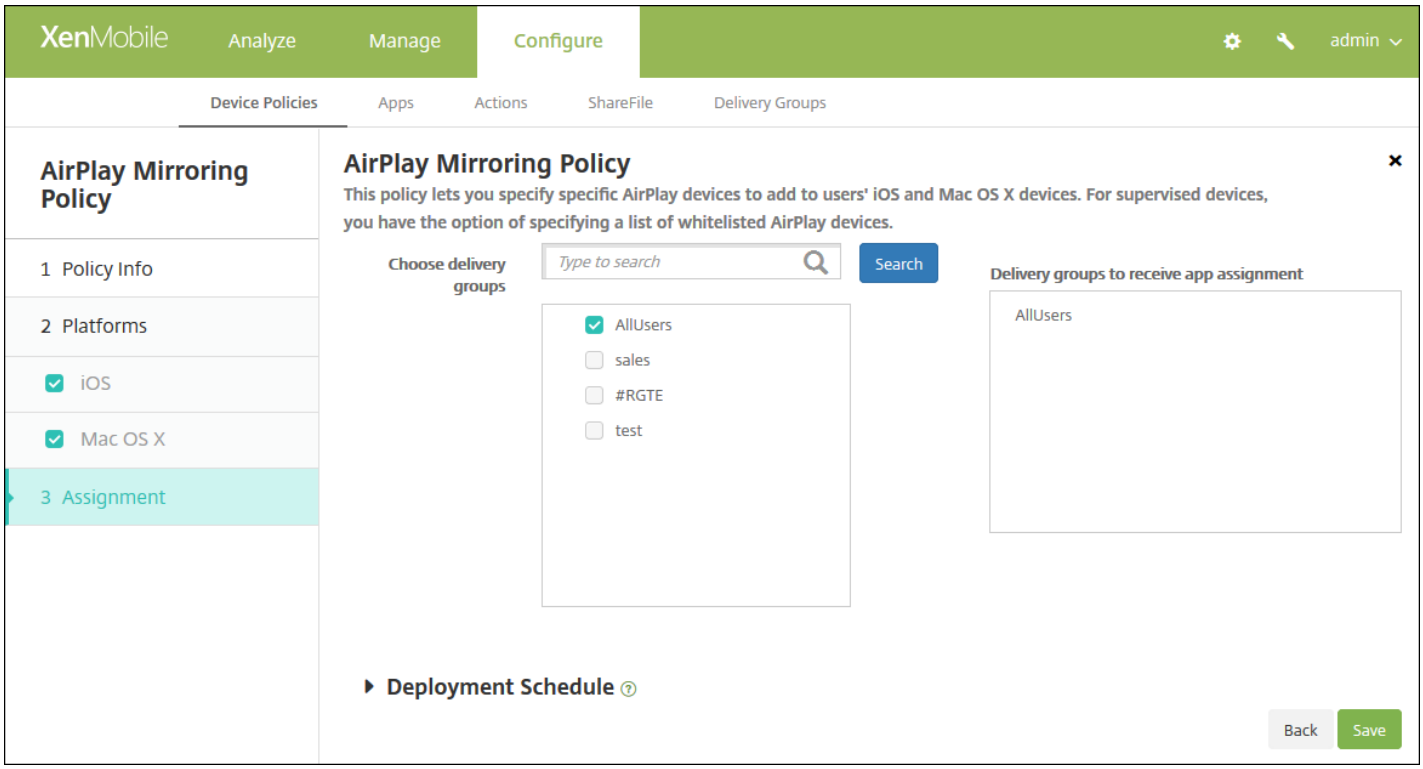
  Hinweis: Zum Löschen eines vorhandenen Geräts zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum

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 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 **Passcode erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
  - Klicken Sie neben **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**.

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

AirPrint-Geräterichtlinie

Feb 24, 2017

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.

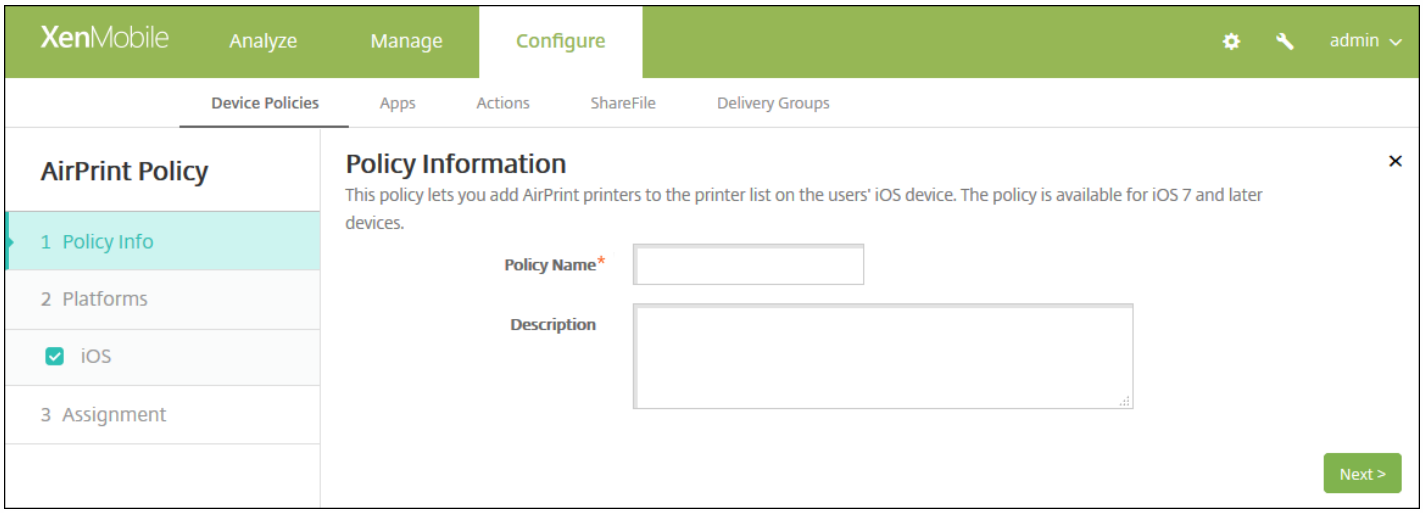
Hinweis:

- 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.

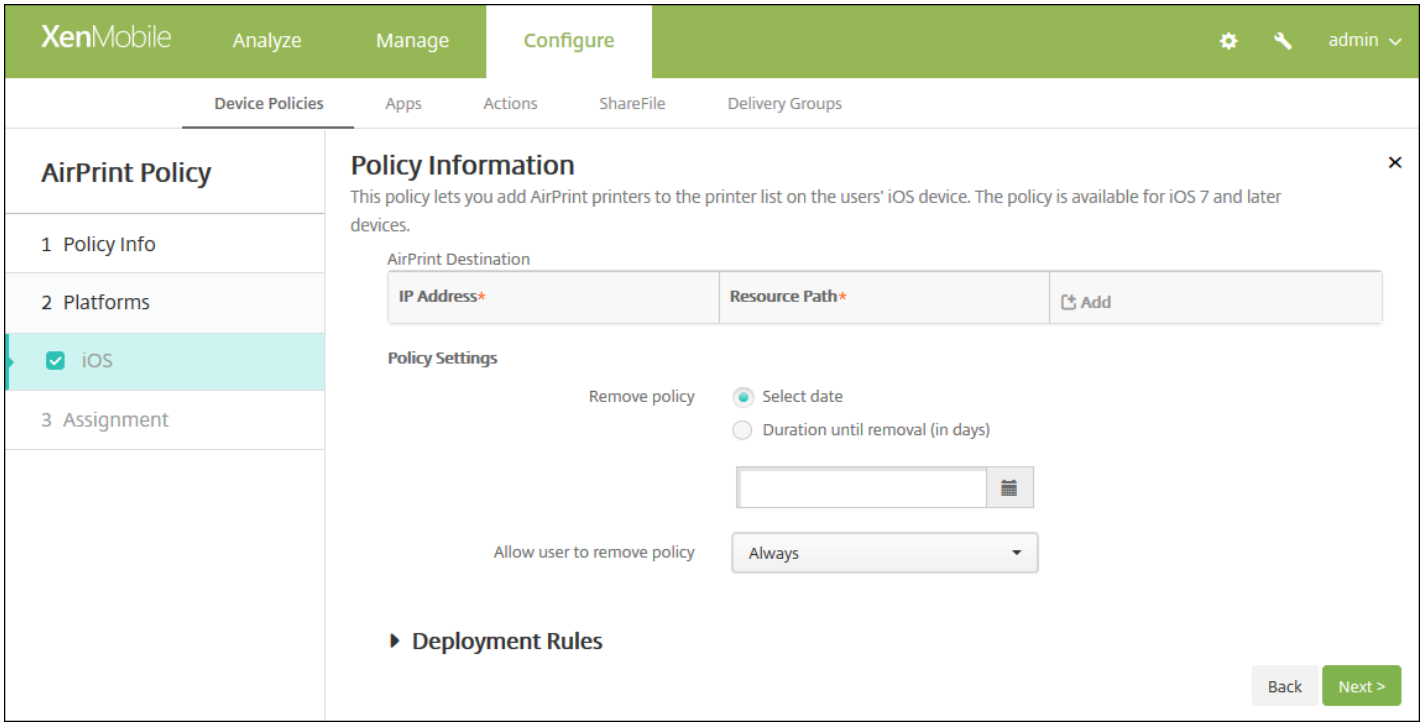
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **AirPrint**. Die Seite für die Richtlinieninformationen der Richtlinie **AirPrint** wird angezeigt.



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:

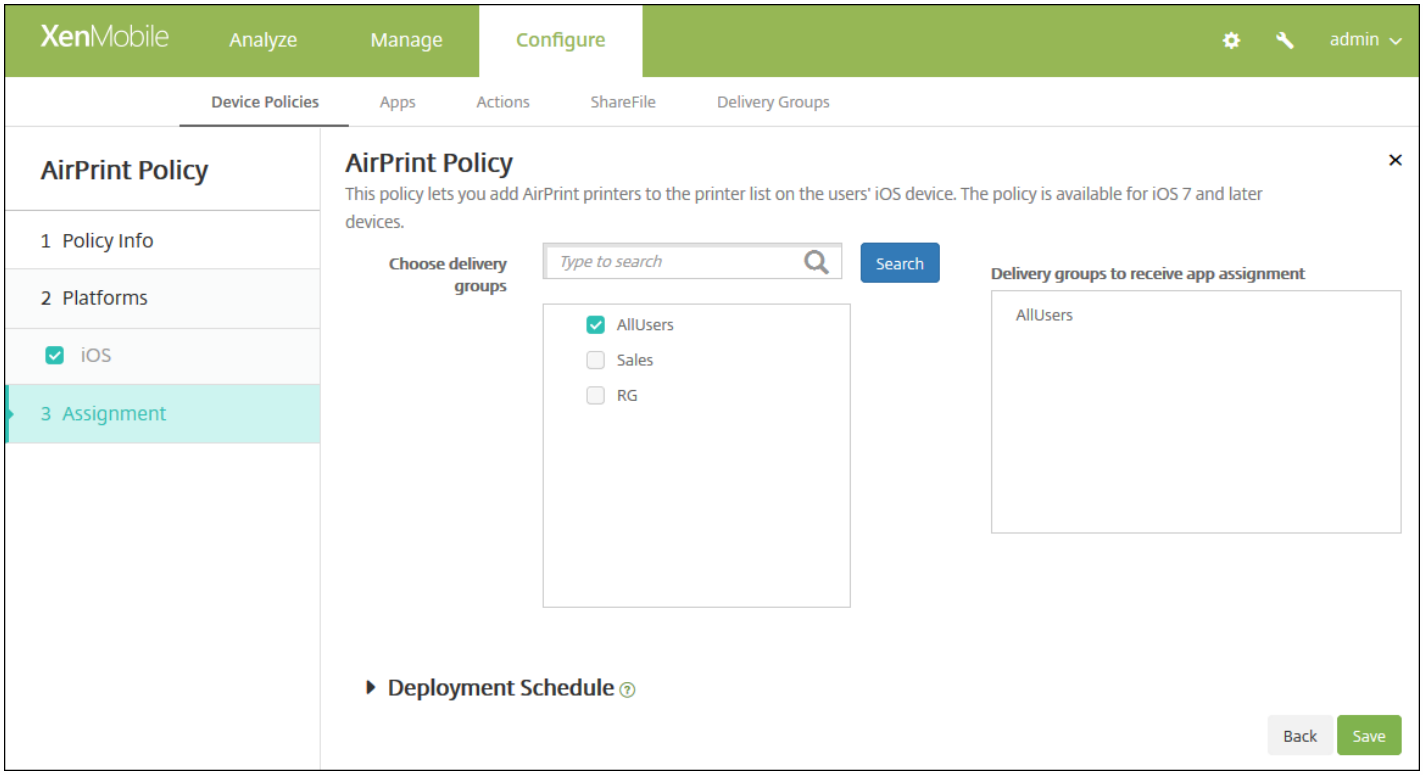
- **AirPrint-Ziel**: Für jedes AirPrint-Ziel, das Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **IP-Adresse**: Geben Sie die IP-Adresse des AirPrint-Druckers ein.
  - **Ressourcenpfad**: Geben Sie den Ressourcenpfad des Druckers ein. Dieser entspricht dem Parameter des Bonjour-Datensatzes in _ipps.tcp. 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** 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.

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Einschränkungsrichtlinie für Android for Work-Apps

Feb 24, 2017

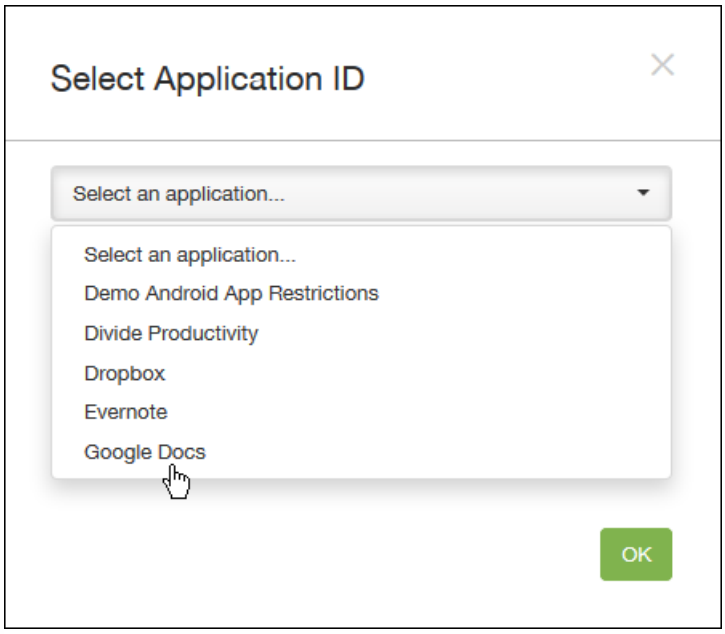
Sie können Einschränkungen für Android for Work-Apps ändern. Hierfür müssen jedoch die folgenden Vorbereitungen getroffen werden:

- Einrichtung von Android for Work auf Google Weitere Informationen finden Sie unter Verwalten von Geräten mit Android for Work.
- Erstellen 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.

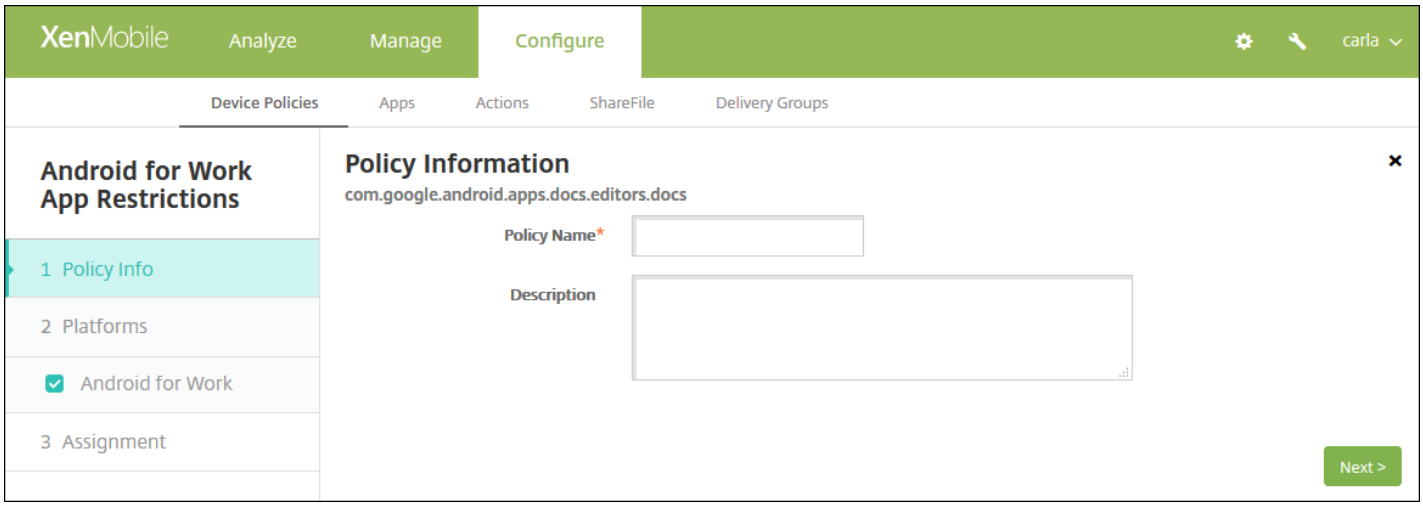
2. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

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**.

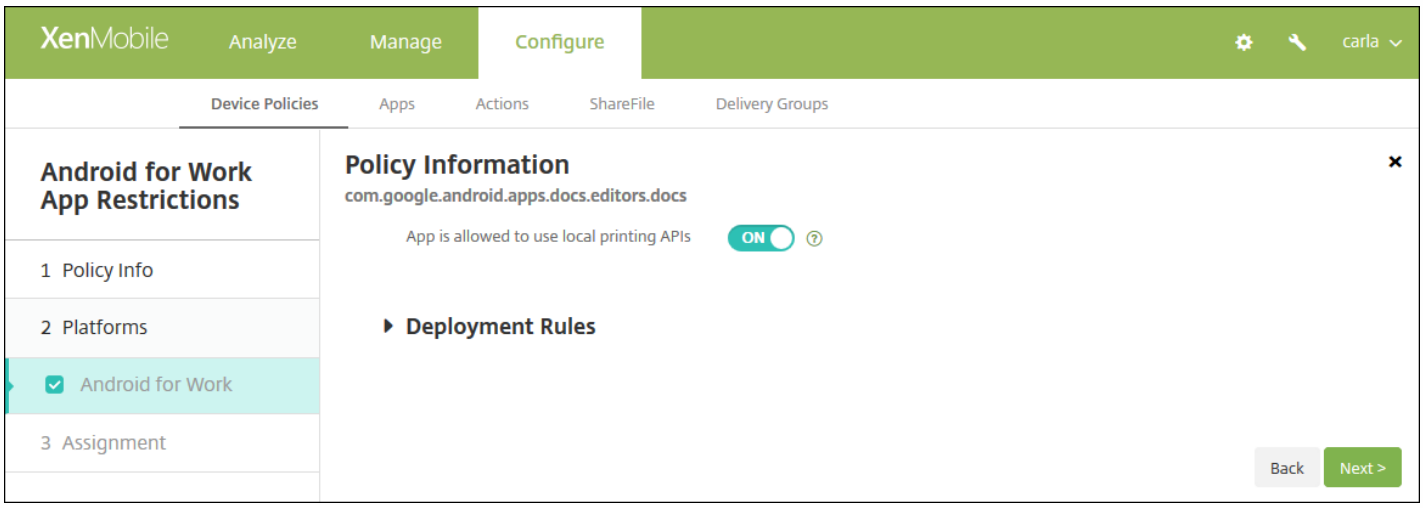
- Wenn XenMobile keine Android for Work-Apps hinzugefügt wurden, können Sie nicht fortfahren. Weitere Informationen zum Hinzufügen von Apps in XenMobile finden Sie unter Hinzufügen von Apps in XenMobile.
- Wenn der App keine Einschränkungen zugeordnet sind, wird eine entsprechende Benachrichtigung angezeigt. 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:

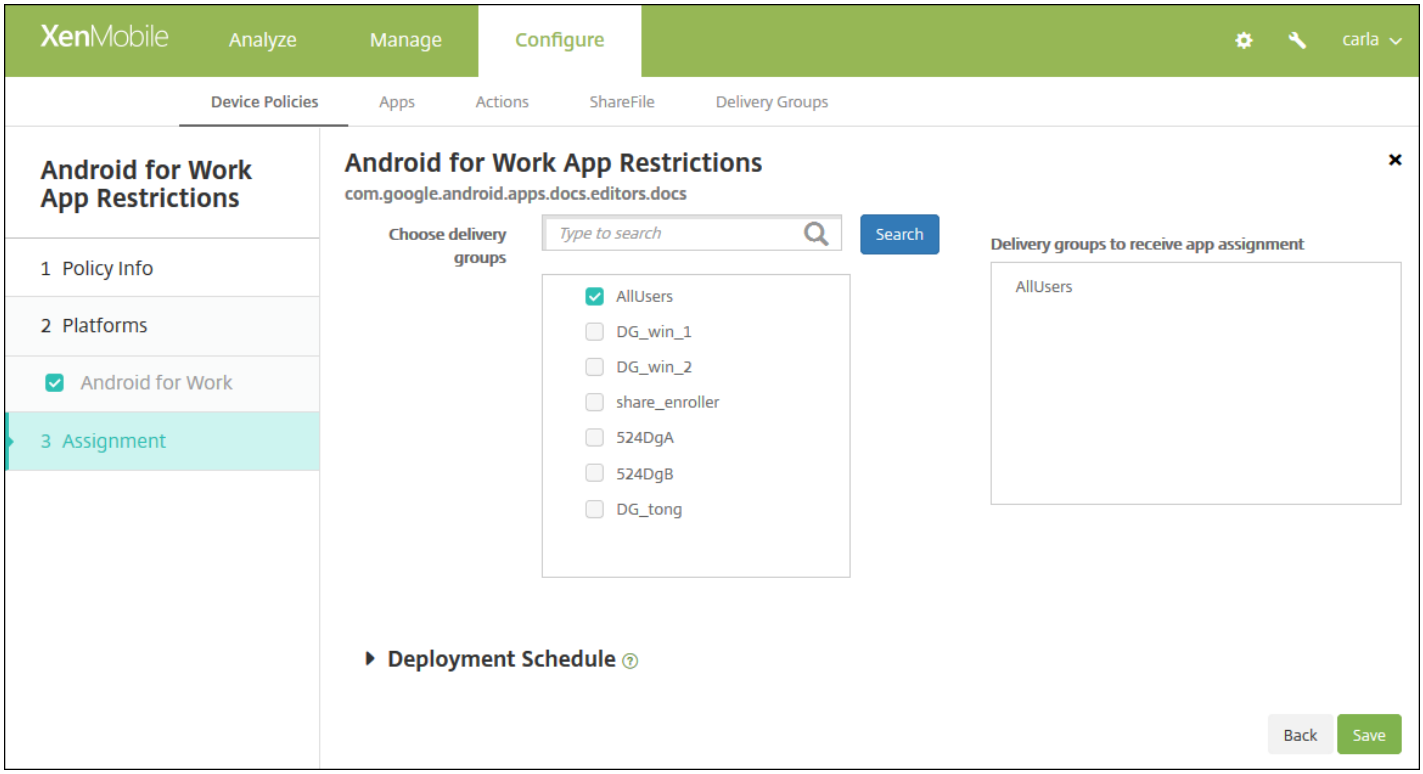
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

12. Klicken Sie auf **Speichern**.

APN-Geräterichtlinien

Feb 24, 2017

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

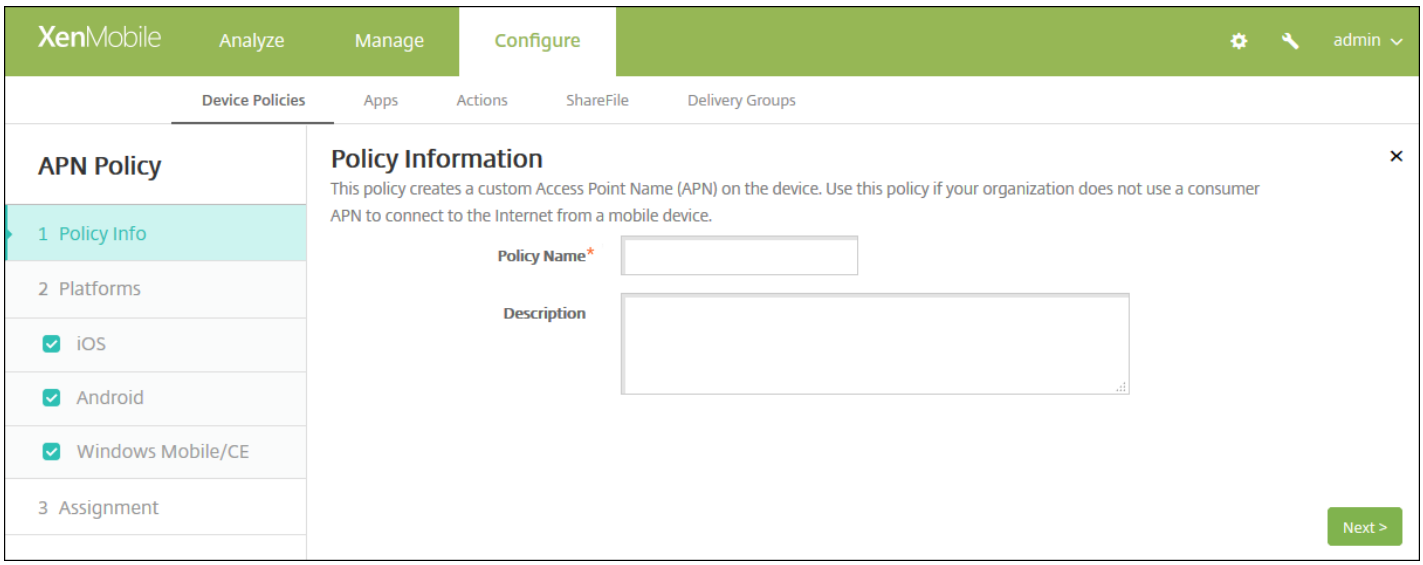
Android-Einstellungen

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:

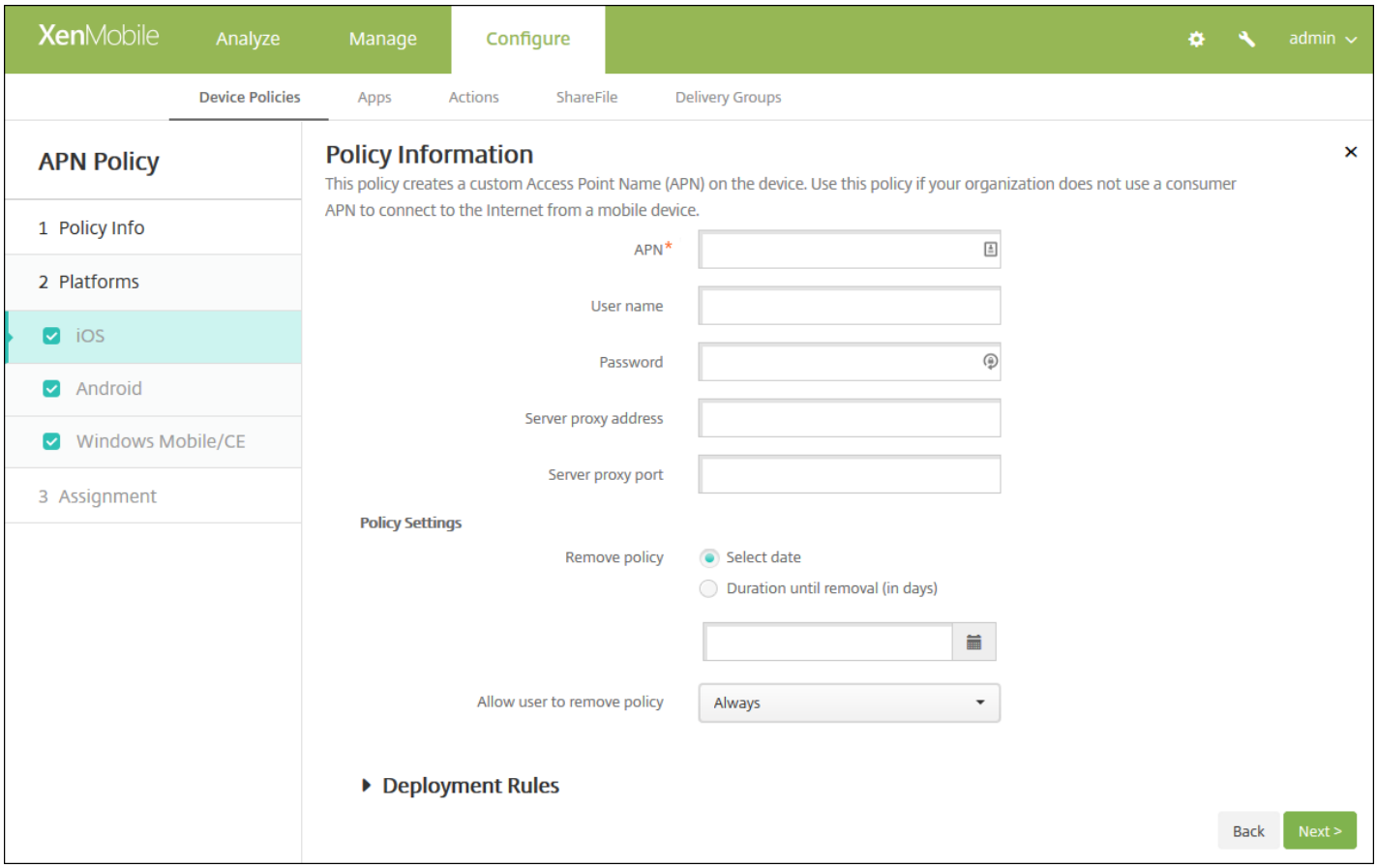
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

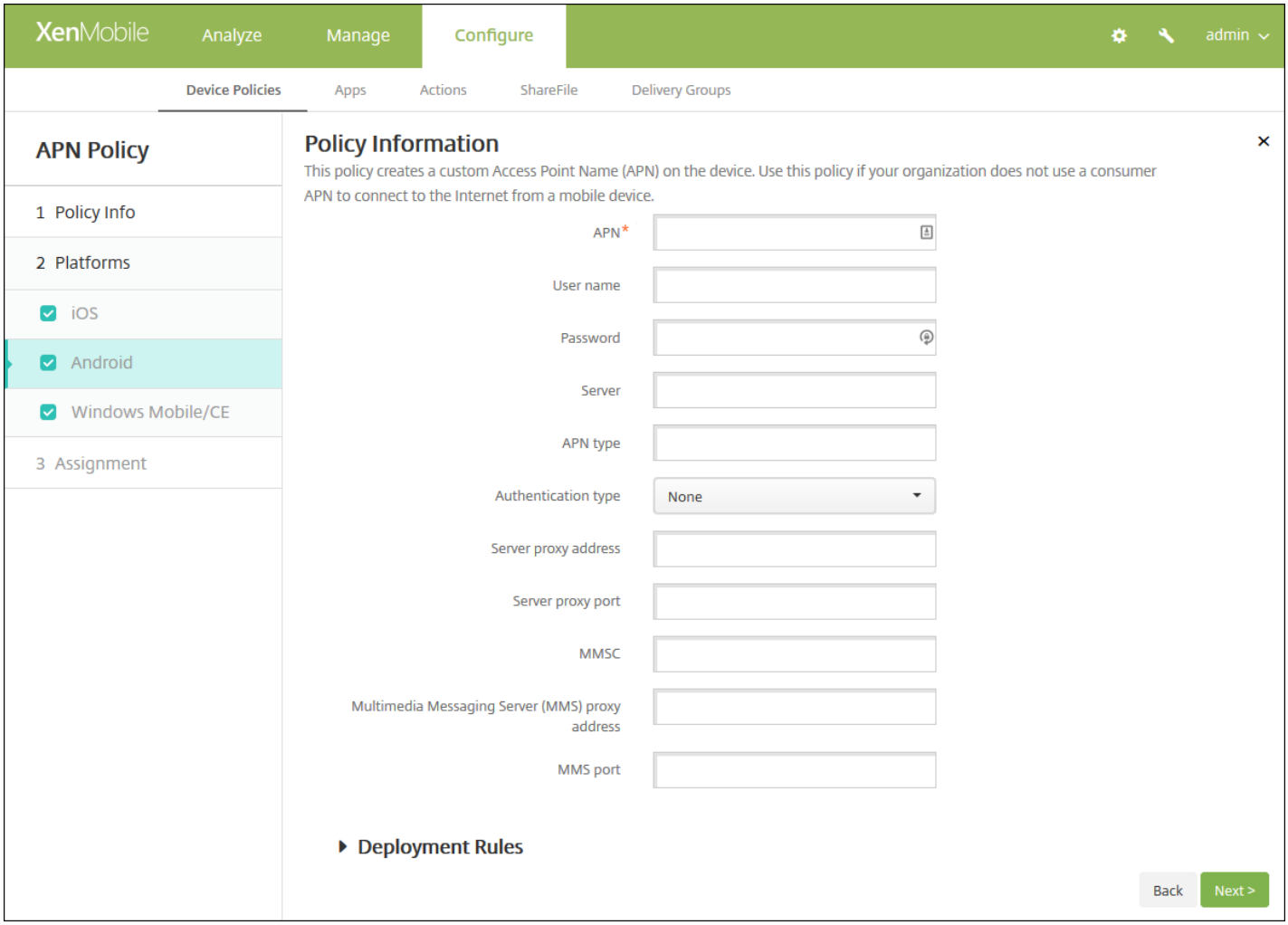
6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus.

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 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** 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.

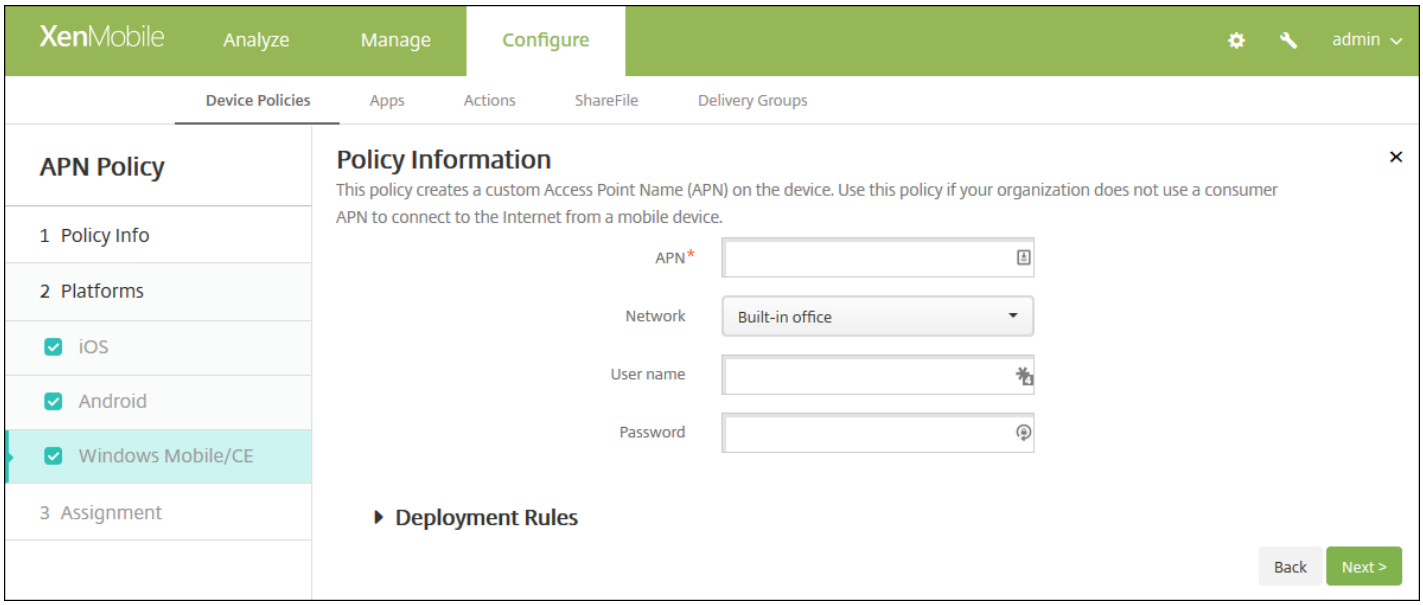


Konfigurieren Sie folgende Einstellungen:

- **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 Smartphones und ist in der Regel leer. Sie verweist auf einen WAP-Gateway-Server (Wireless Application-Protokoll) für Telefone, bei denen der Zugriff auf oder das Rendern von Standardwebsites nicht möglich war.
- **APN-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.

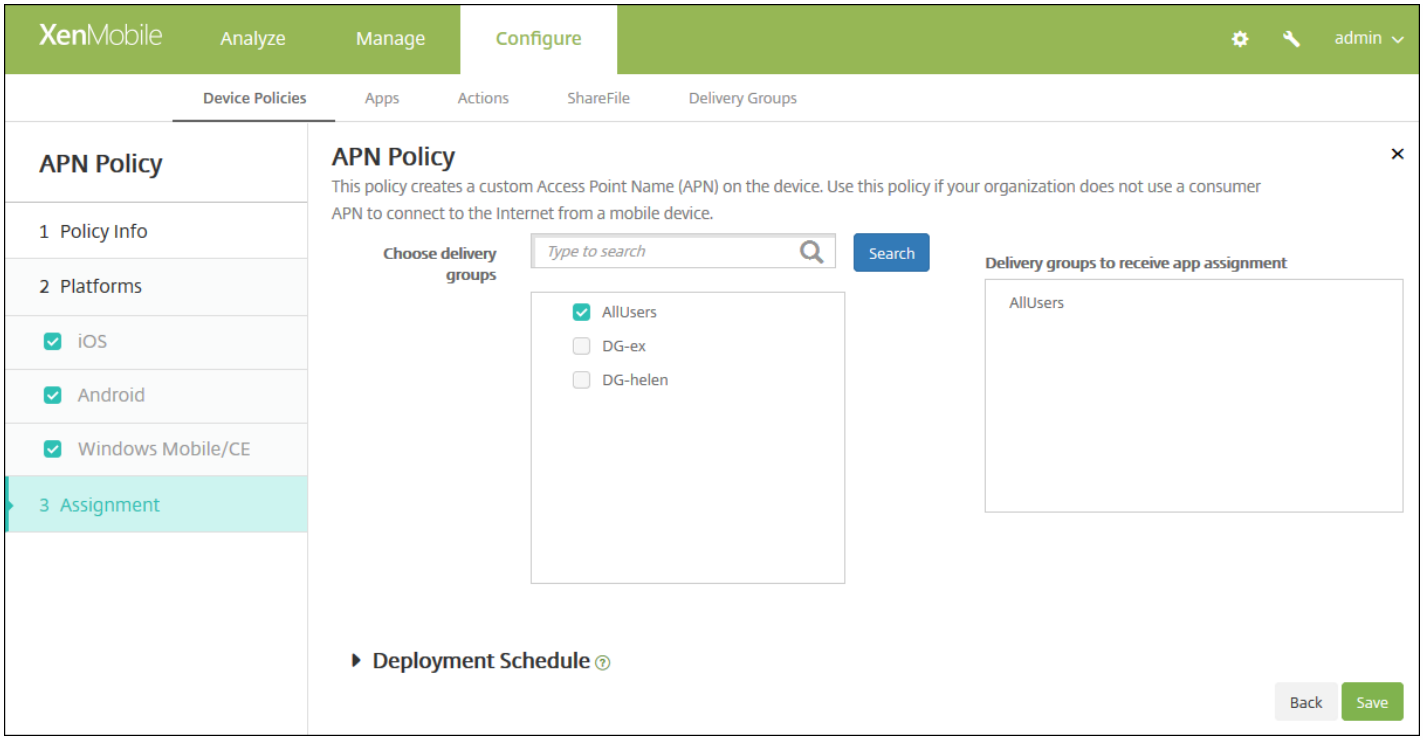
- **Authentifizierungstyp**: Klicken Sie in der Liste auf den gewünschten Authentifizierungstyp. Standardwert ist "Ohne".
- **Serverproxyadresse**: IP-Adresse oder URL des APN-HTTP-Proxys des Netzbetreibers.
- **Serverproxyport**: Portnummer des APN-Proxys. Sie ist erforderlich, wenn Sie eine Serverproxyadresse 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 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. 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.

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:

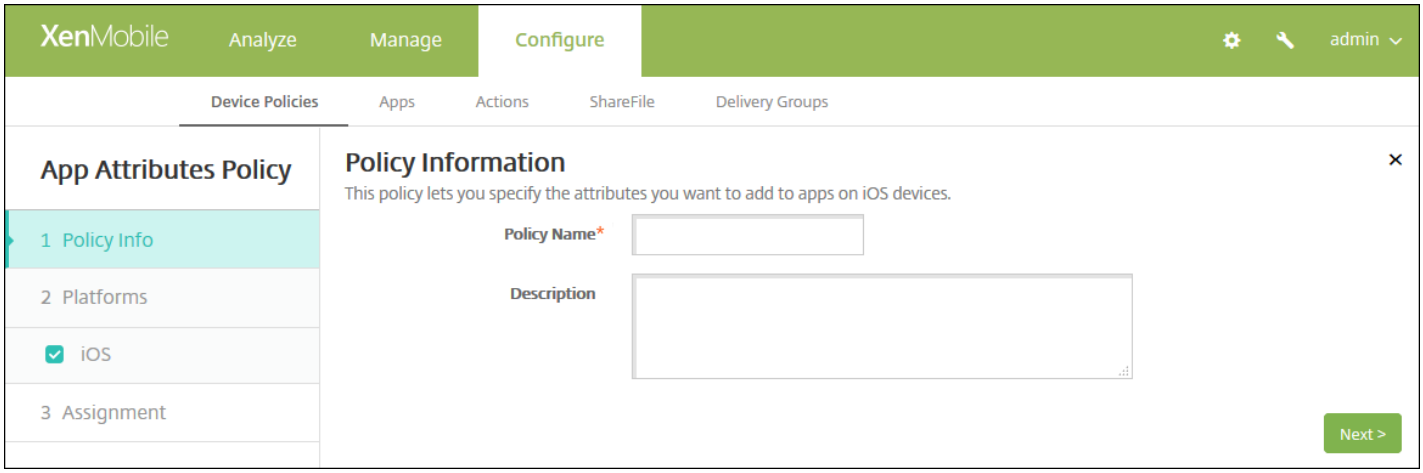
- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **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

Feb 24, 2017

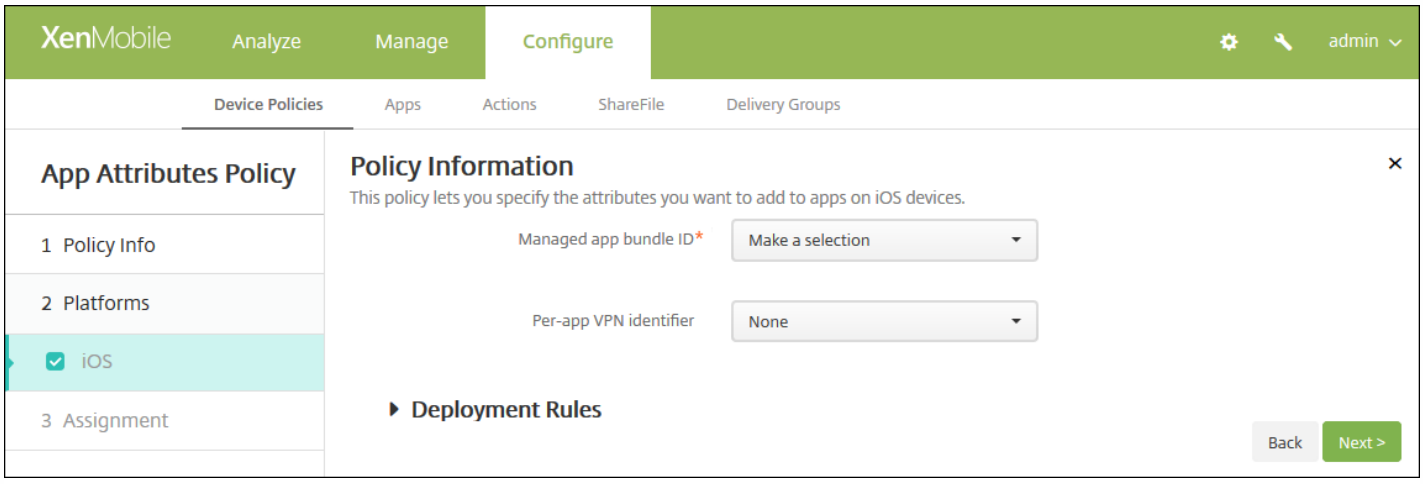
Mit der Geräterichtlinie für App-Attribute können Sie für iOS-Geräte Attribute angeben (z. B. eine Paket-ID für die verwaltete App oder die ID für den VPN-Zugriff pro App).



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.

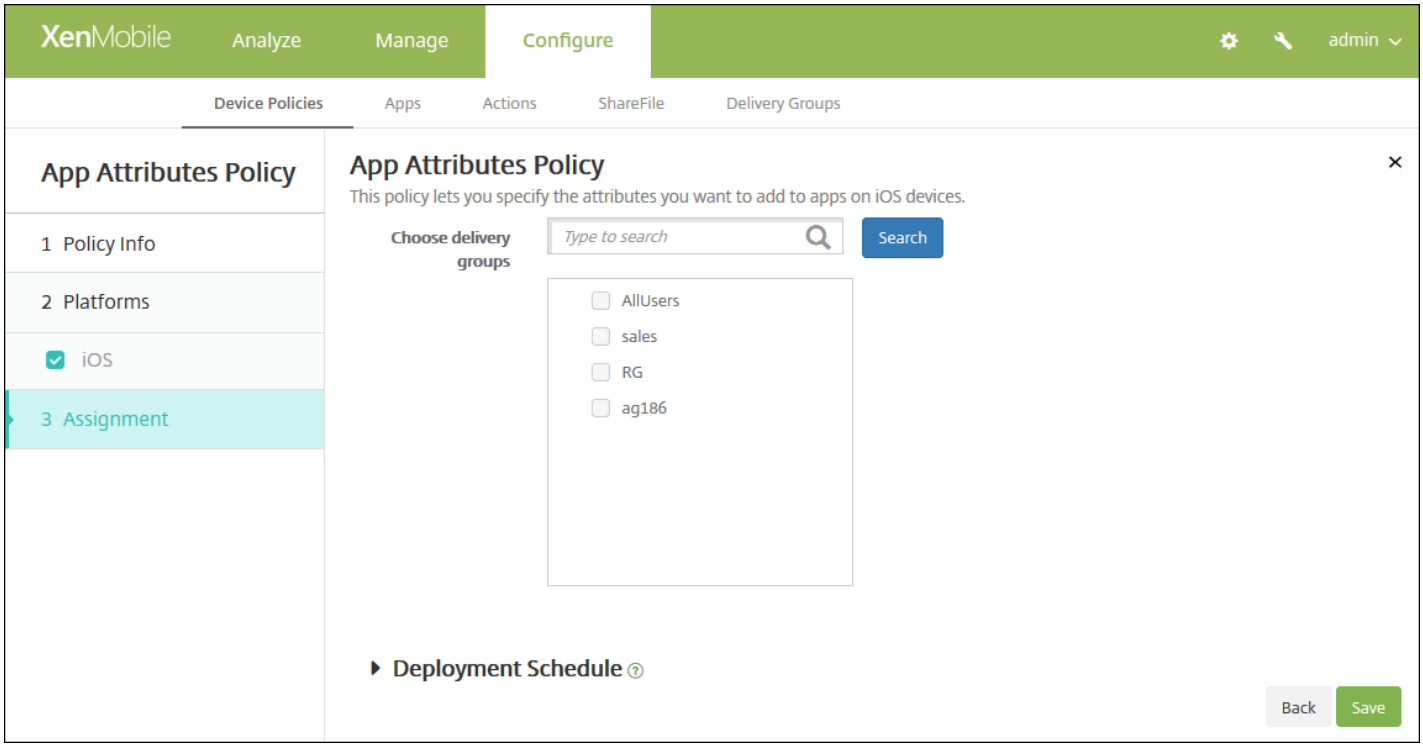
5. Klicken Sie auf **Weiter**. Die Plattformseite wird angezeigt.



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.

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 **Später** 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 "Einstellungen" > "Servereigenschaften" den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von "Bereitstellen für immer aktive Verbindungen", denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

App-Zugriffsrichtlinien für Geräte

Feb 24, 2017

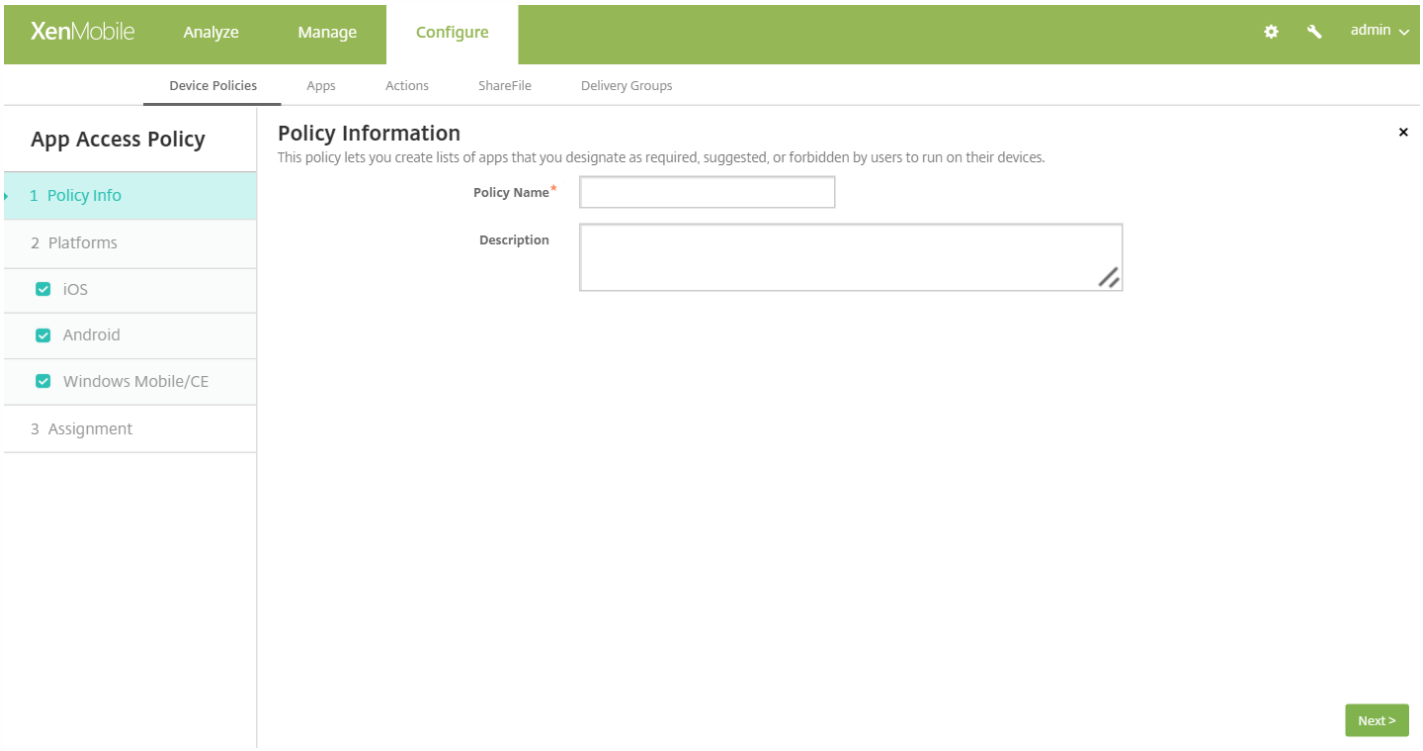
Über eine App-Zugriffsrichtlinie für Geräte können Sie in XenMobile eine Liste der Apps definieren, die auf Geräten installiert werden müssen, nach Wahl installiert werden können oder nicht installiert werden dürfen. Sie können dann eine automatisierte Aktion erstellen, mit der die Reaktion auf die Richtlinientreue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

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

App-Konfigurationsrichtlinie für Geräte

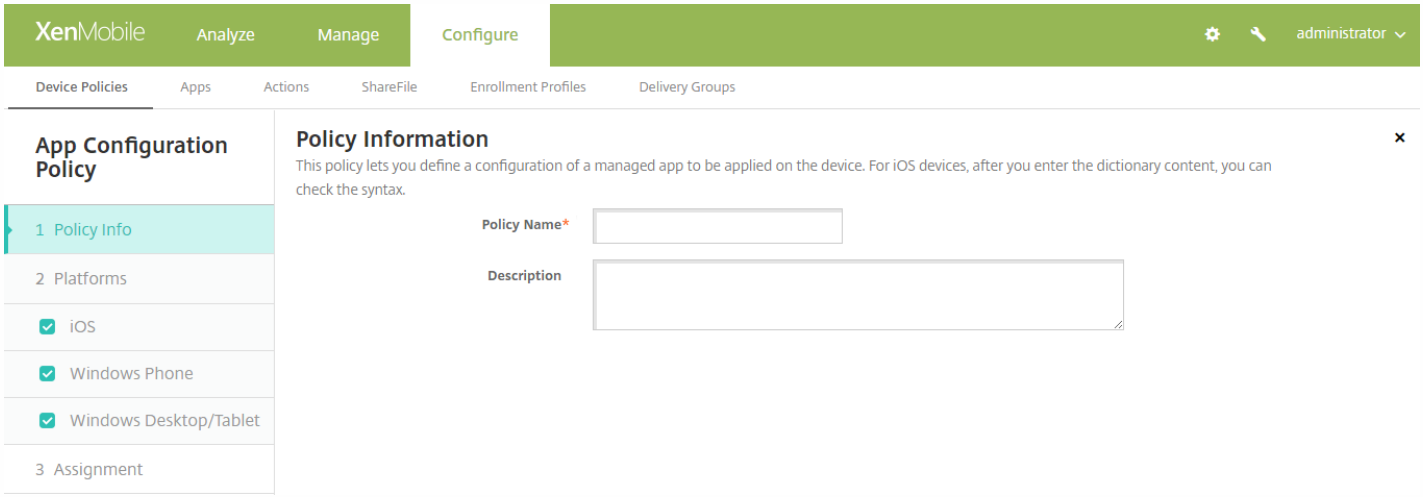
Feb 24, 2017

Sie können Apps, die eine verwaltete Konfiguration unterstützen, remote konfigurieren, indem Sie eine XML-Konfigurationsdatei ("Eigenschaftenliste" bzw. "plist") auf iOS-Geräten und Schlüssel/Wert-Paare für Telefone, Tablets und Desktop-Geräte, auf denen Windows 10 ausgeführt wird, bereitstellen. Die Konfiguration bestimmt verschiedene Einstellungen und Verhalten der Apps. XenMobile überträgt die Konfiguration per Push auf die Geräte, wenn die Benutzer die App installieren. 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 > 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-Konfiguration**. Die Seite **App-Konfiguration** wird angezeigt.



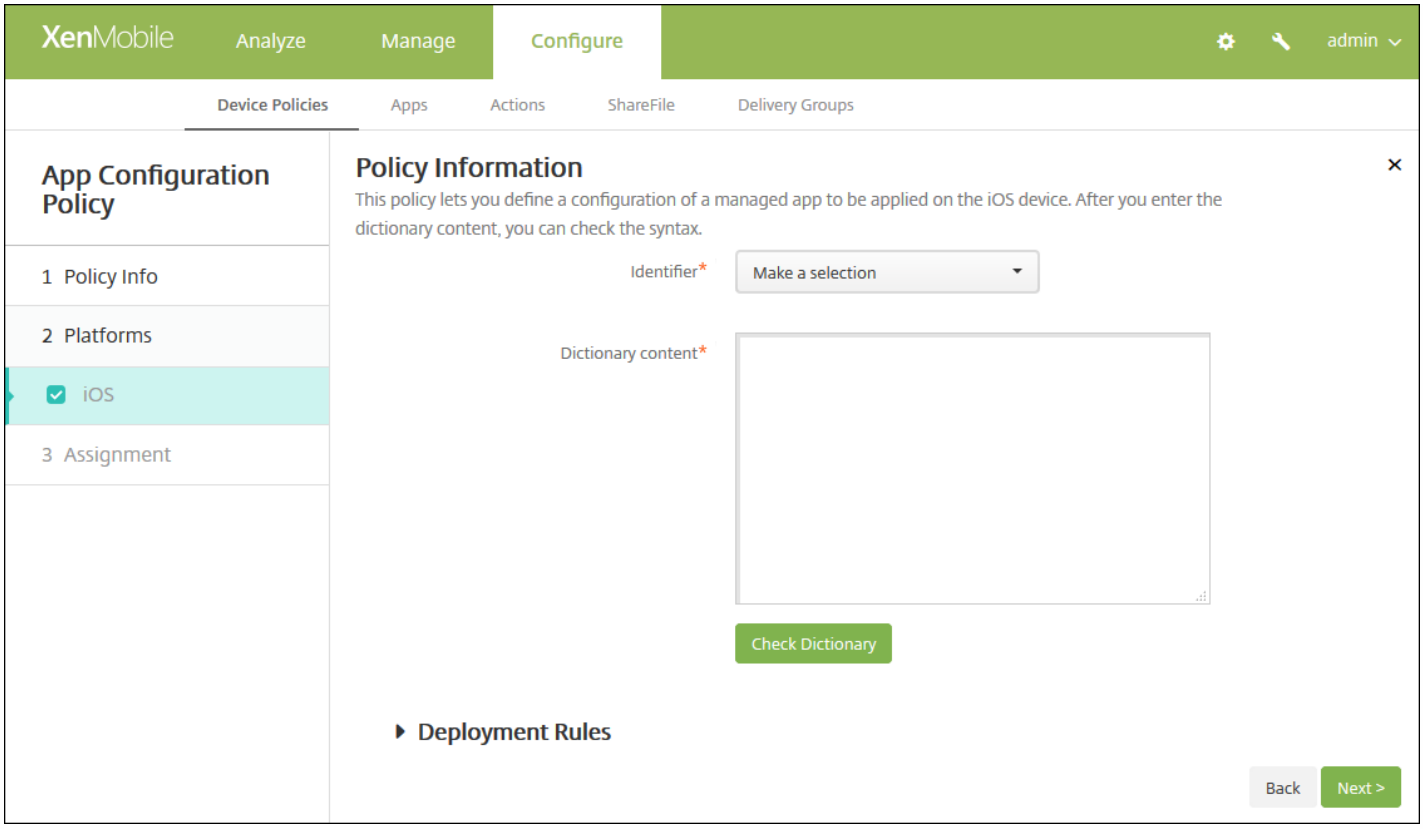
4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

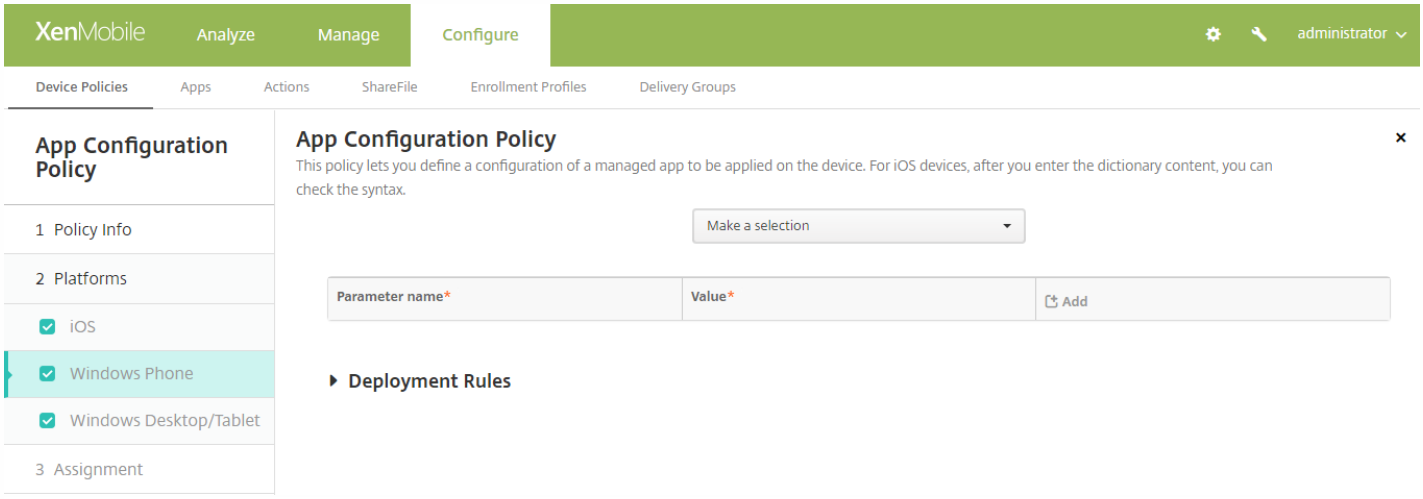
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

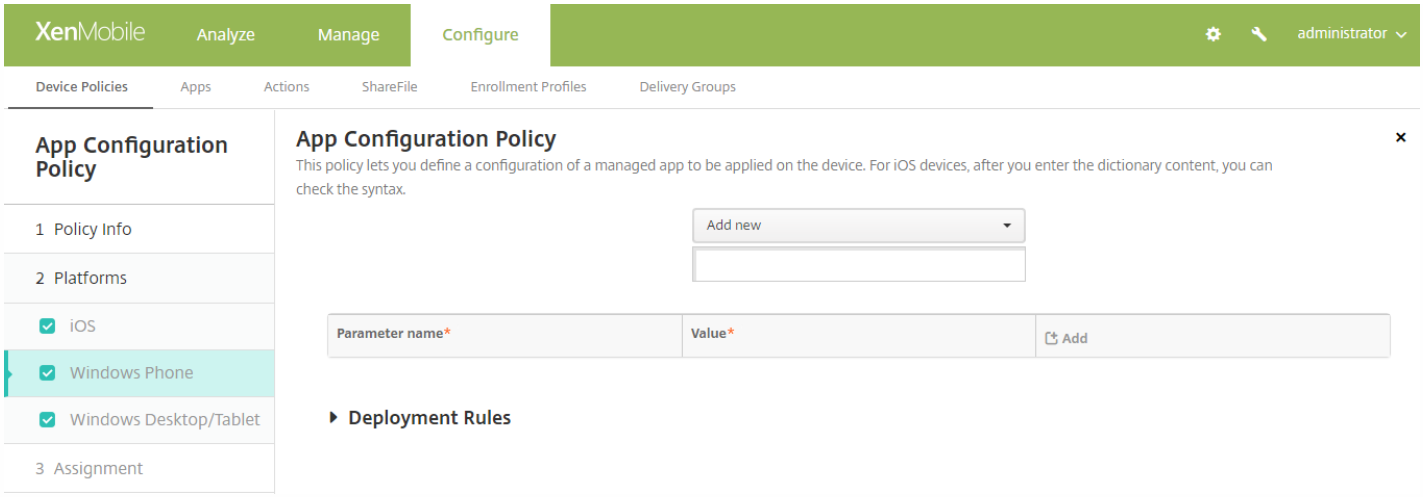
5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

   Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

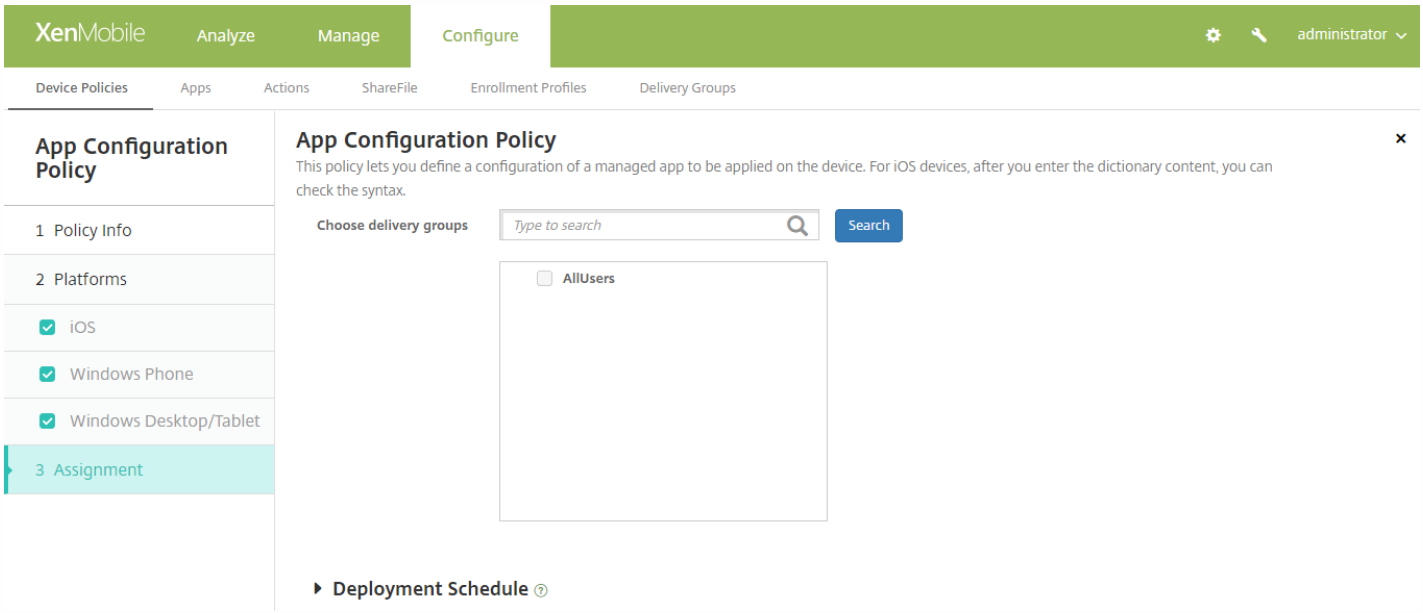
   Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 6.







7. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die App-Konfigurationsrichtlinie wird angezeigt.



8. 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.

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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

10. Klicken Sie auf **Speichern**.

App-Bestandsgeräterichtlinien

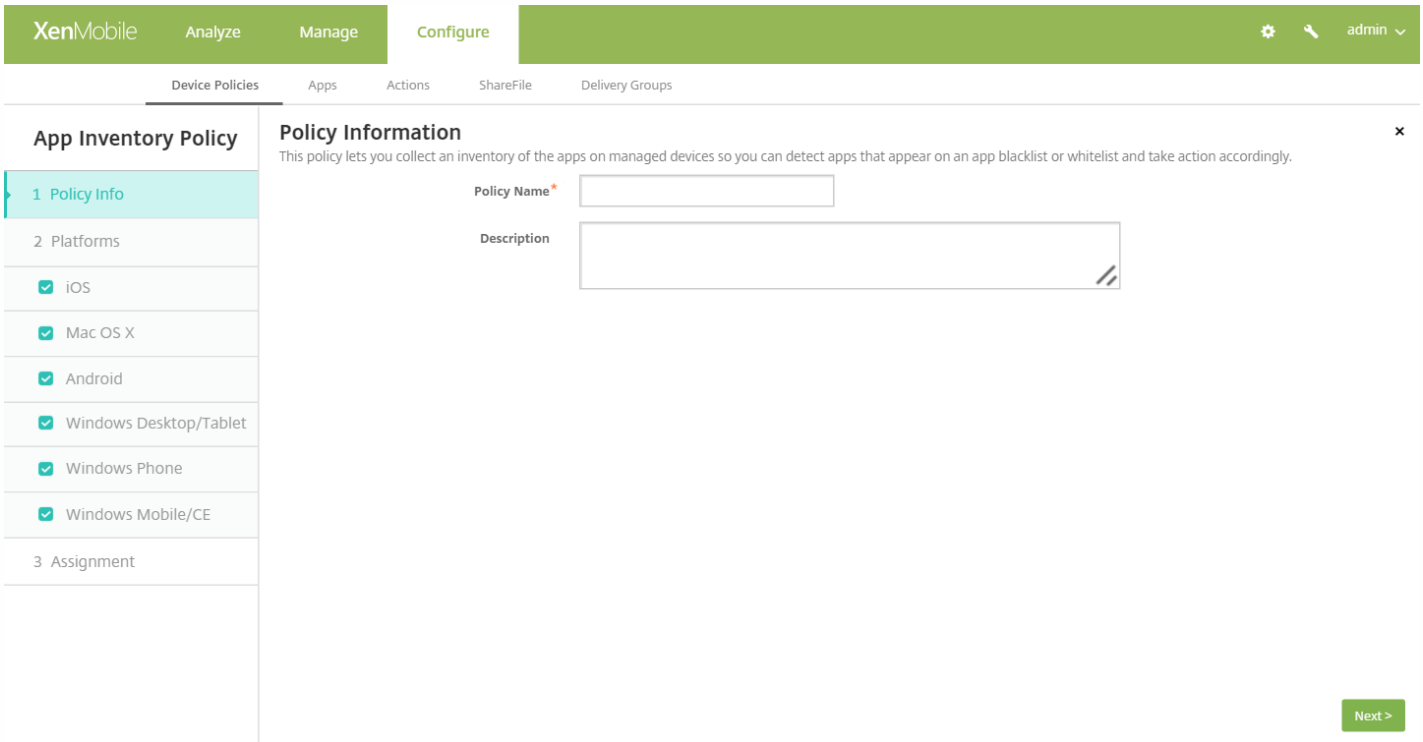
Feb 24, 2017

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.

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.

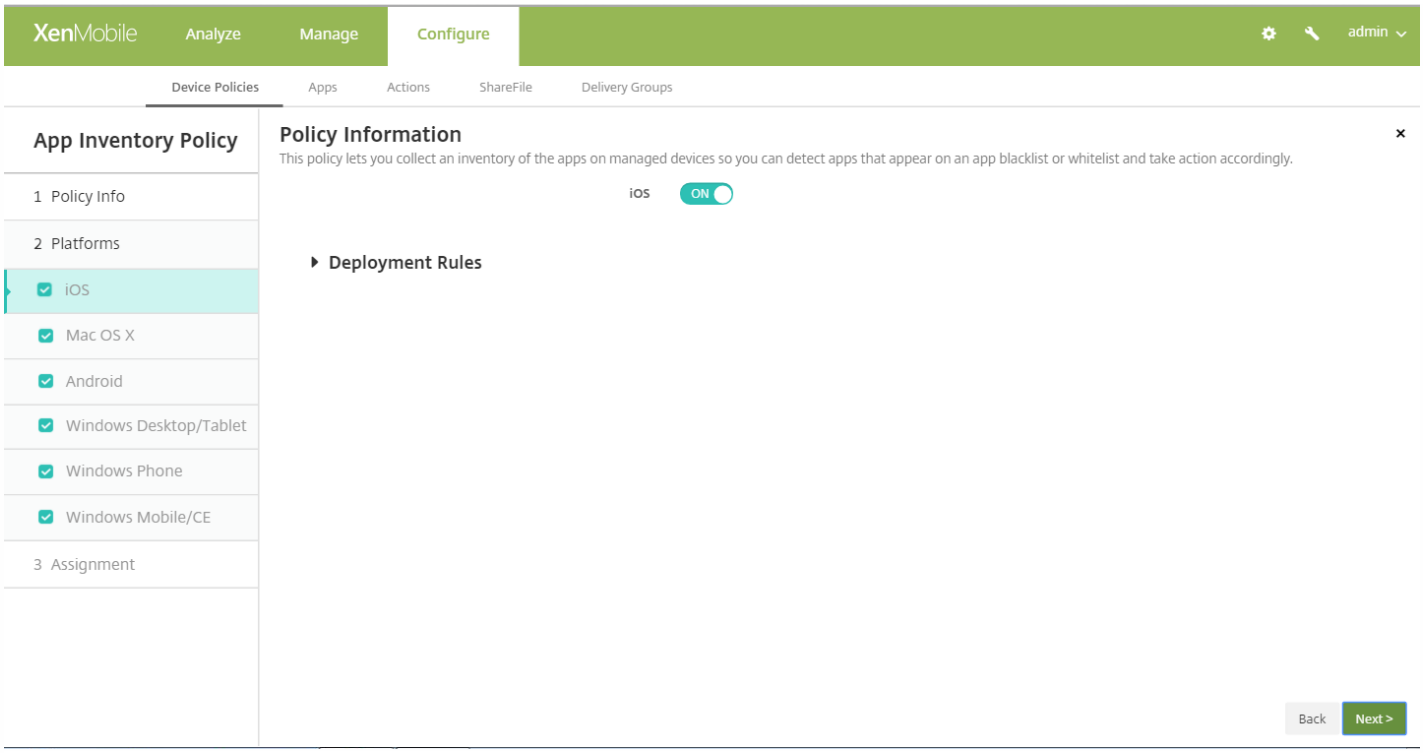
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **App-Bestand**. Die Seite **App-Bestand** wird angezeigt.



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.

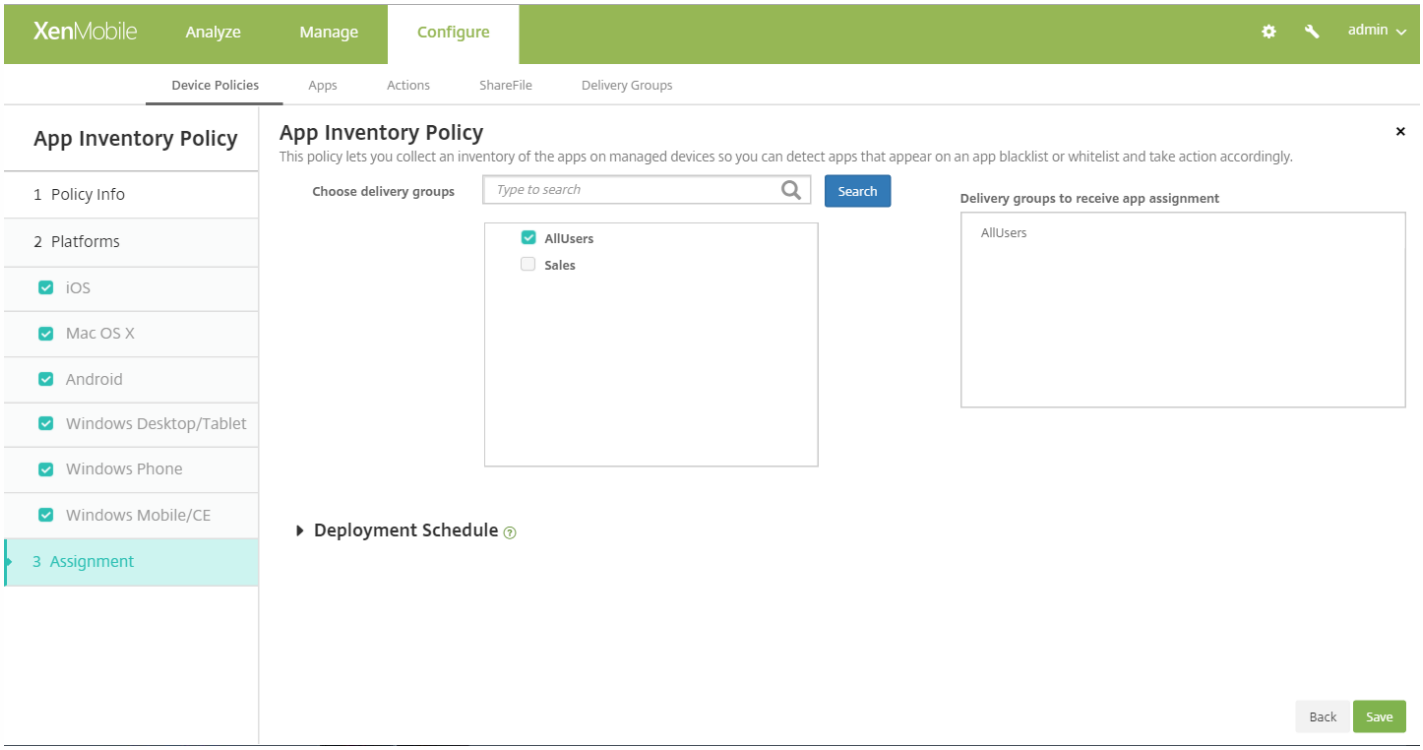


Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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**. Der Standardwert ist **EIN**.

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 Delivery groups to receive app assignment 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 Später 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie zum Sperren von Apps

Feb 24, 2017

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.

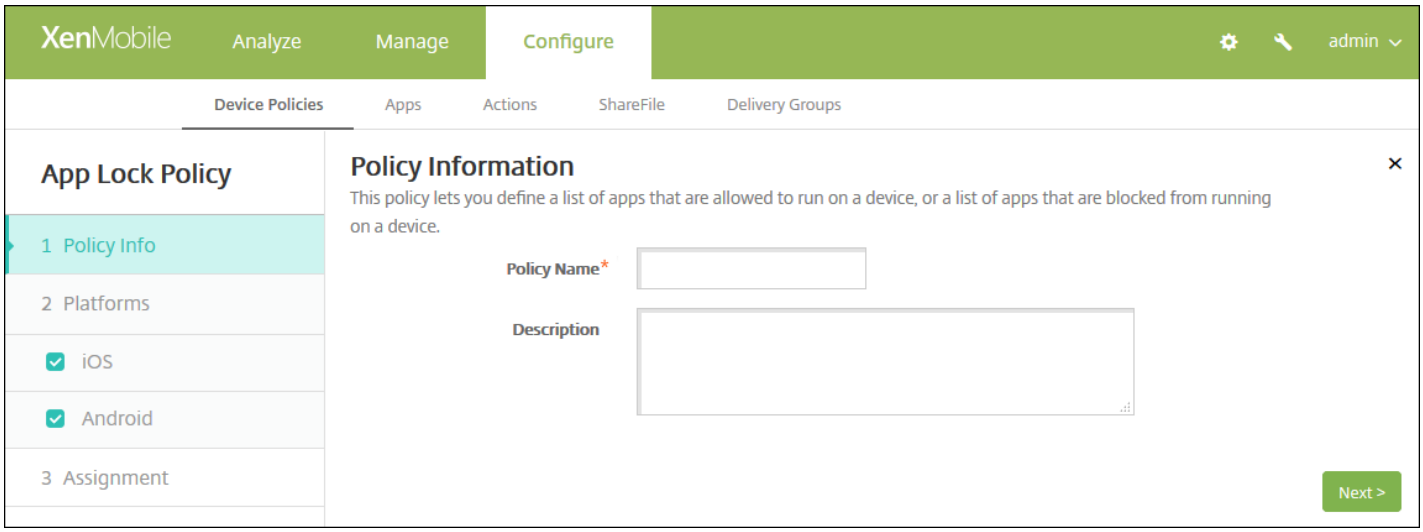
iOS-Einstellungen

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.



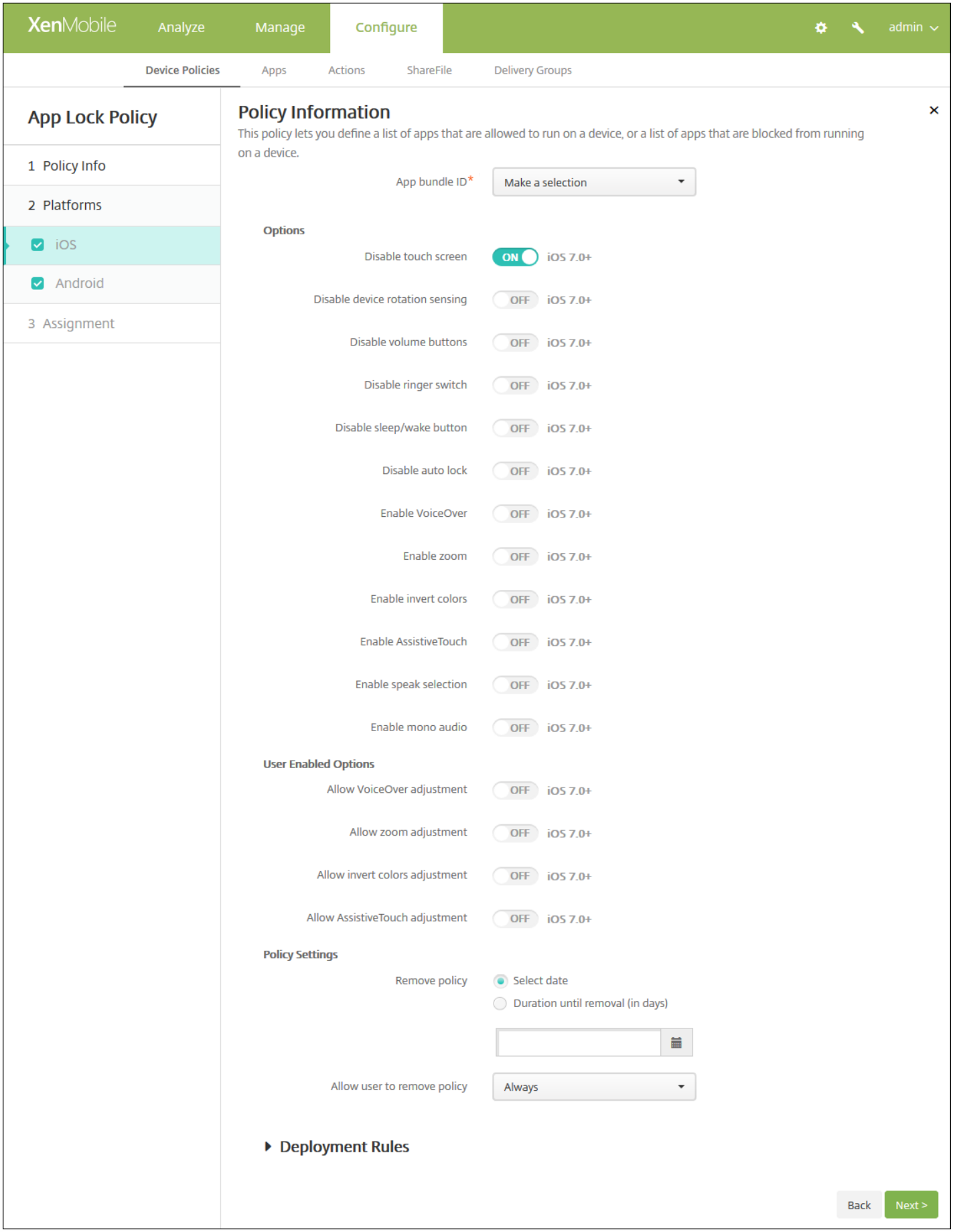
4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

- **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.

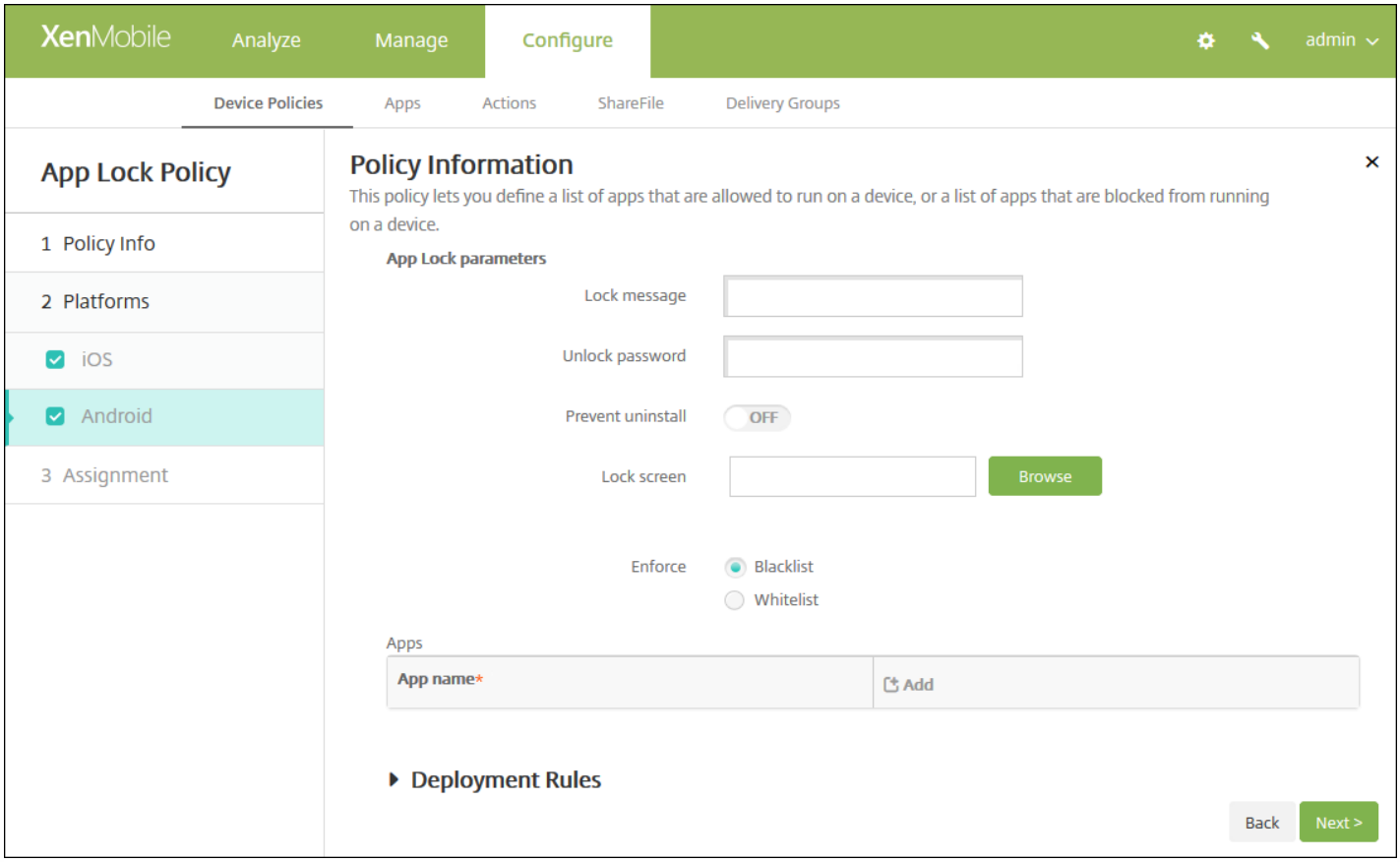
6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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 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 Sie folgende Einstellungen:

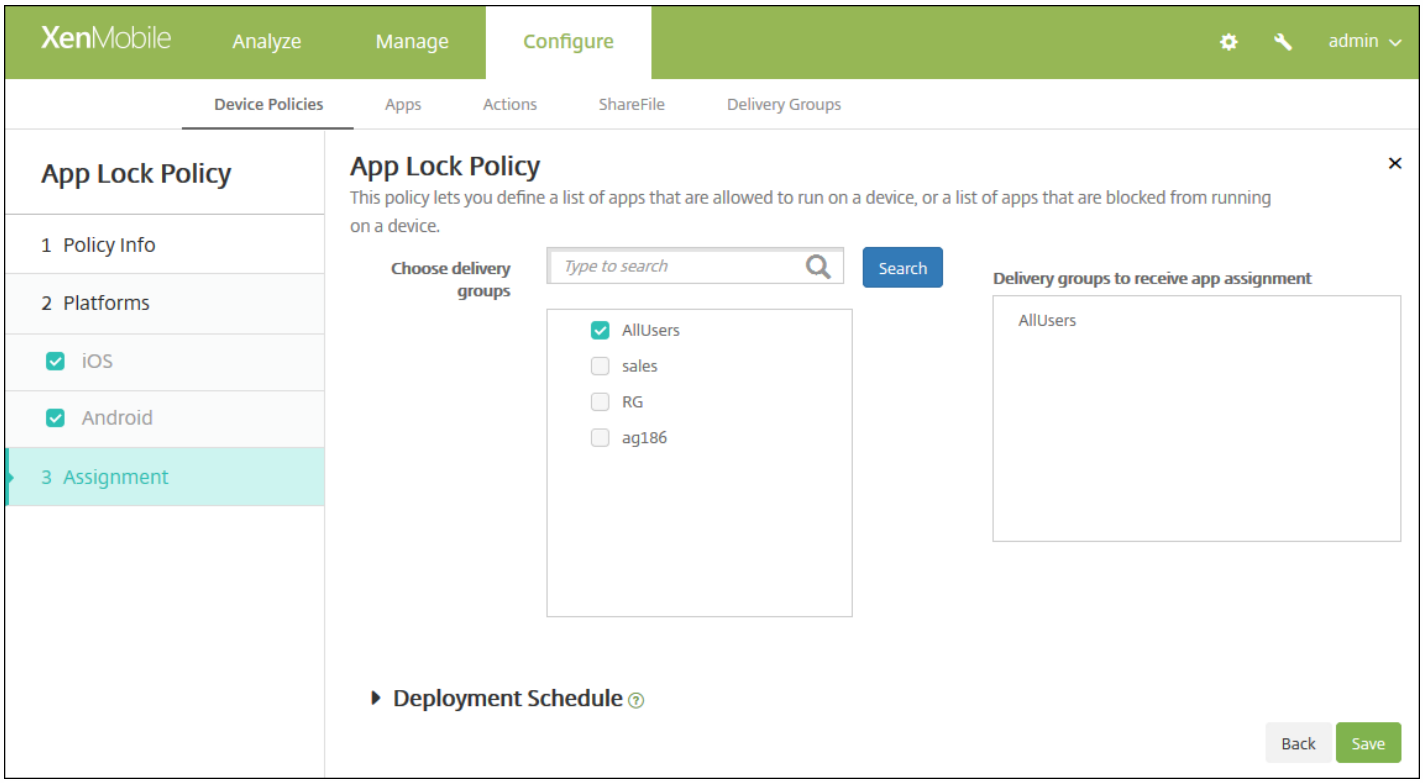
- **Parameter für App-Sperre**
  - **Sperrmeldung**: Geben Sie eine Meldung ein, die angezeigt wird, wenn ein Benutzer versucht, eine gesperrte App zu öffnen.
  - **Entsperrkennwort**: Geben Sie das Kennwort zum Entsperren der App ein.
  - **Deinstallation verhindern**: Wählen Sie aus, ob eine Deinstallation 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.

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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Richtlinie für die App-Netzwerkauslastung

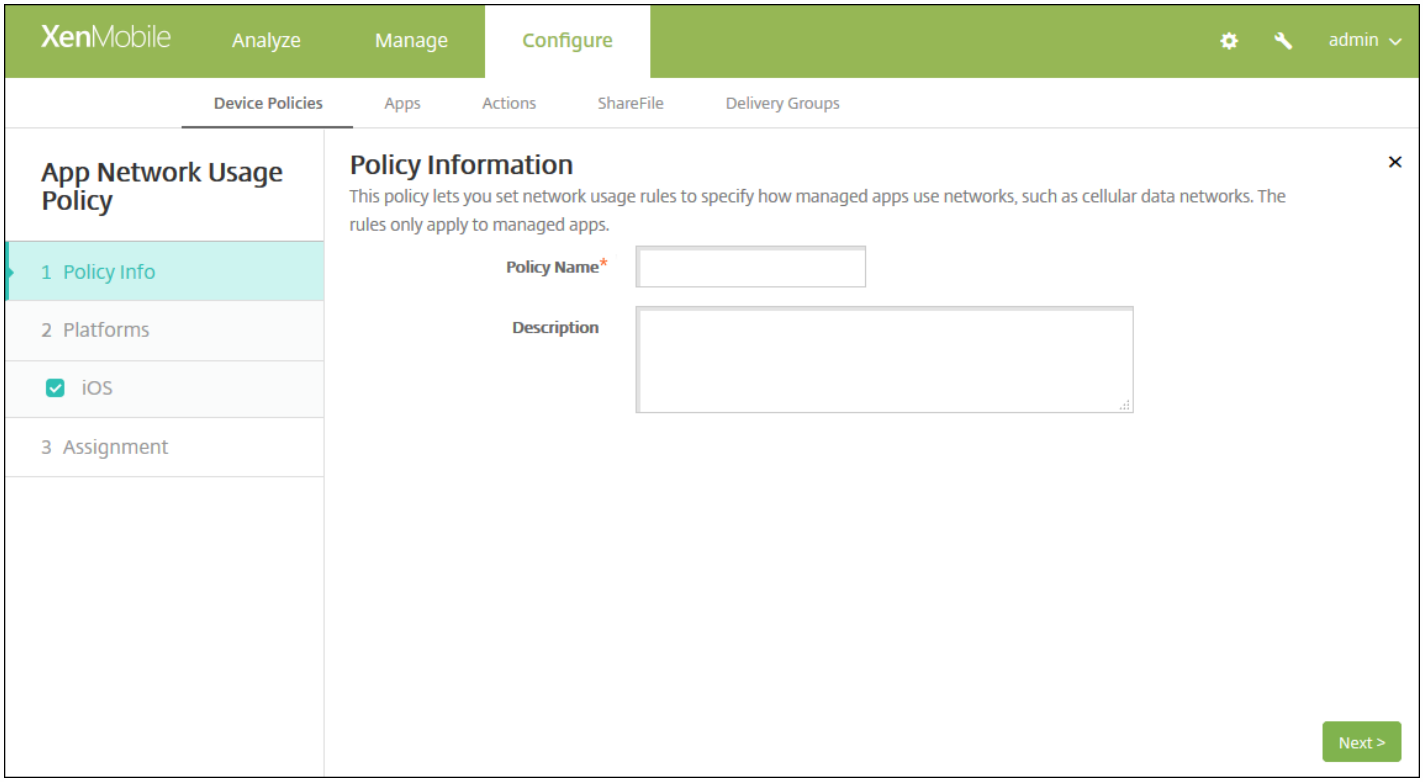
Feb 24, 2017

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.

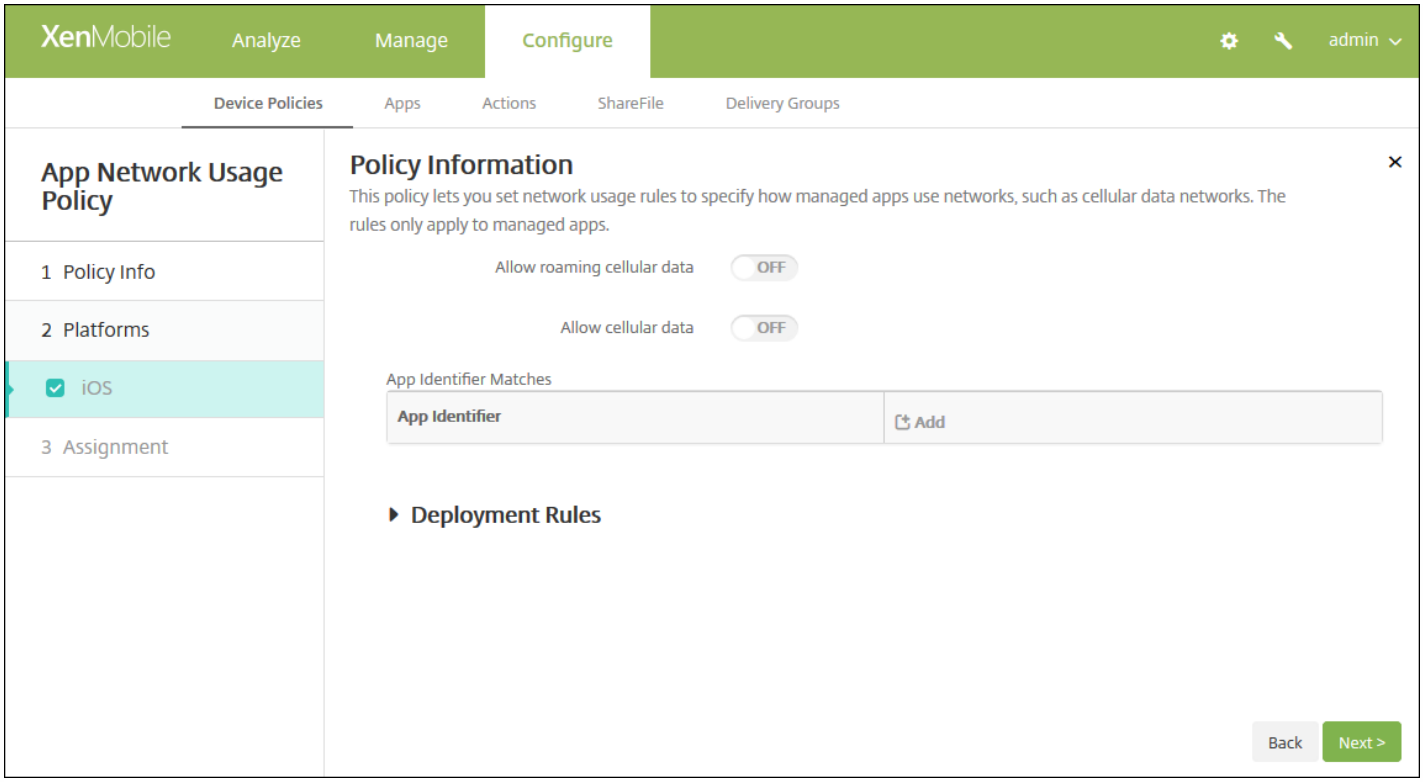
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **App-Netzwerkauslastung**. Die Seite **App-Netzwerkauslastung** wird angezeigt.



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.

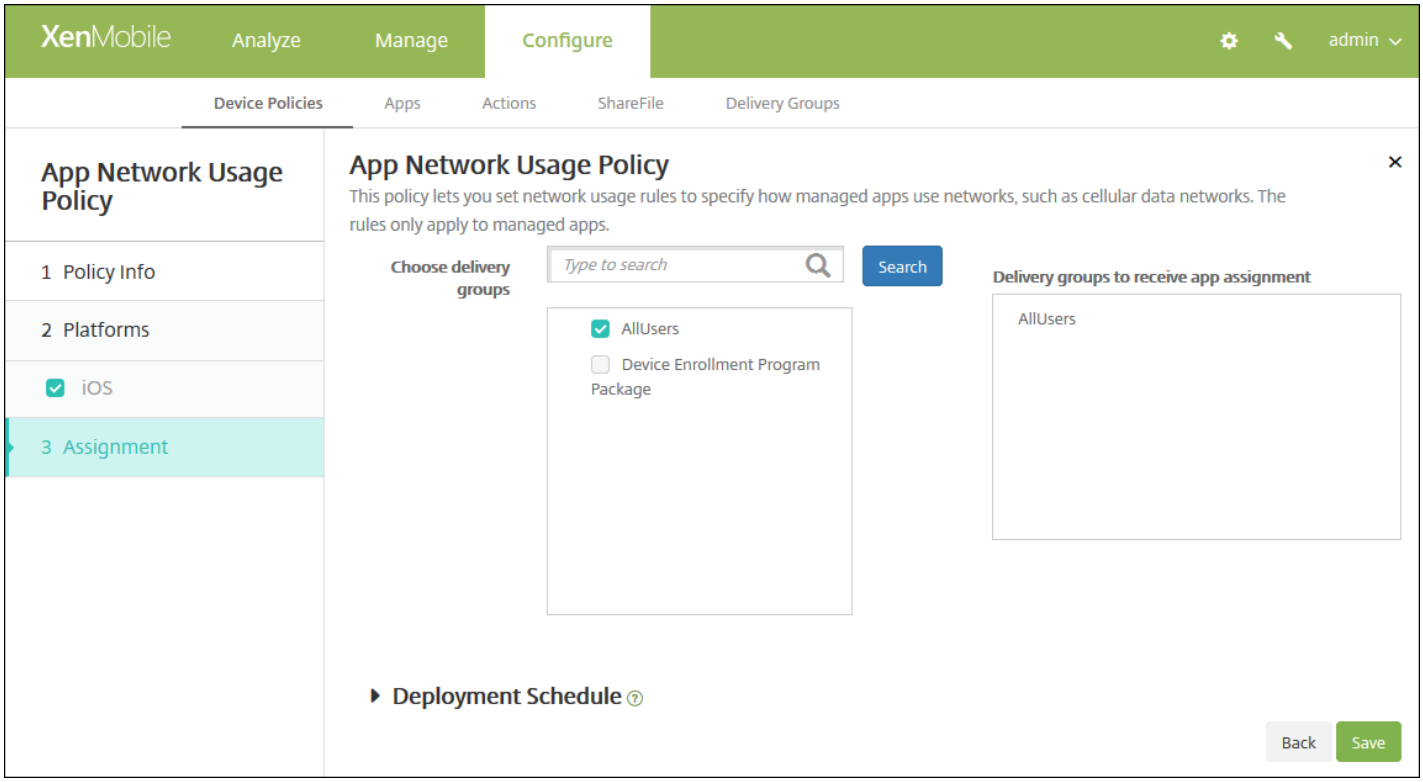
- **Roaming für mobile Daten zulassen**: Wählen Sie aus, ob die angegebenen Apps beim Roaming eine Mobilfunkdatenverbindung herstellen dürfen. Der Standardwert ist **AUS**.
- **Mobile Daten zulassen**: Wählen Sie aus, ob die angegebenen Apps eine Mobilfunkdatenverbindung verwenden dürfen. Der Standardwert 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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

App-Einschränkungsrichtlinien

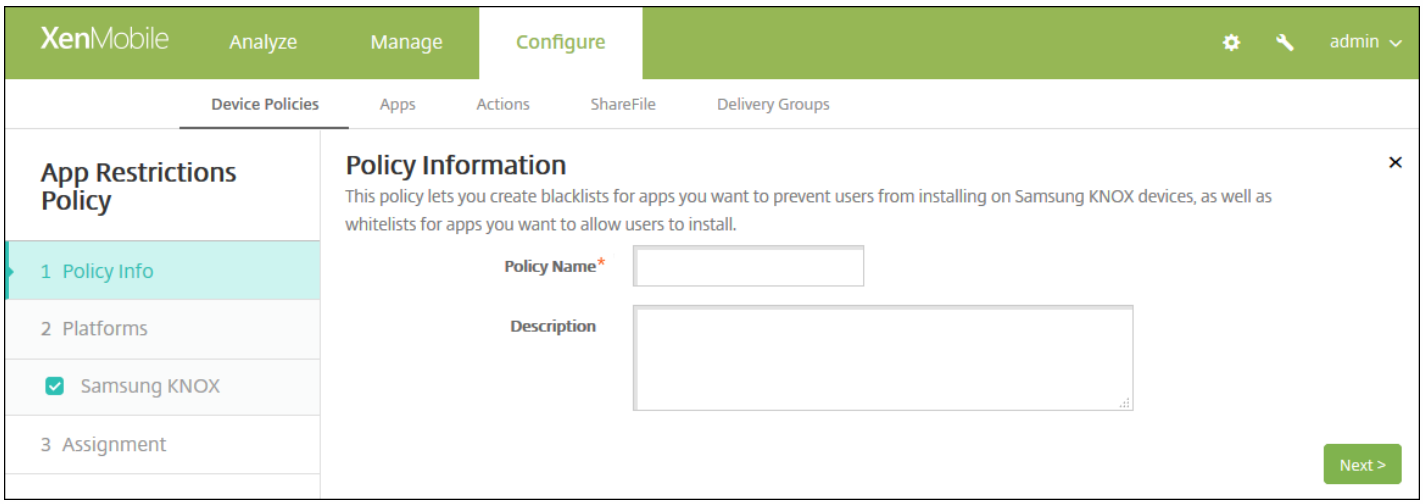
Feb 24, 2017

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 > Gerätерichtlinien**. Die Seite **Gerätерichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

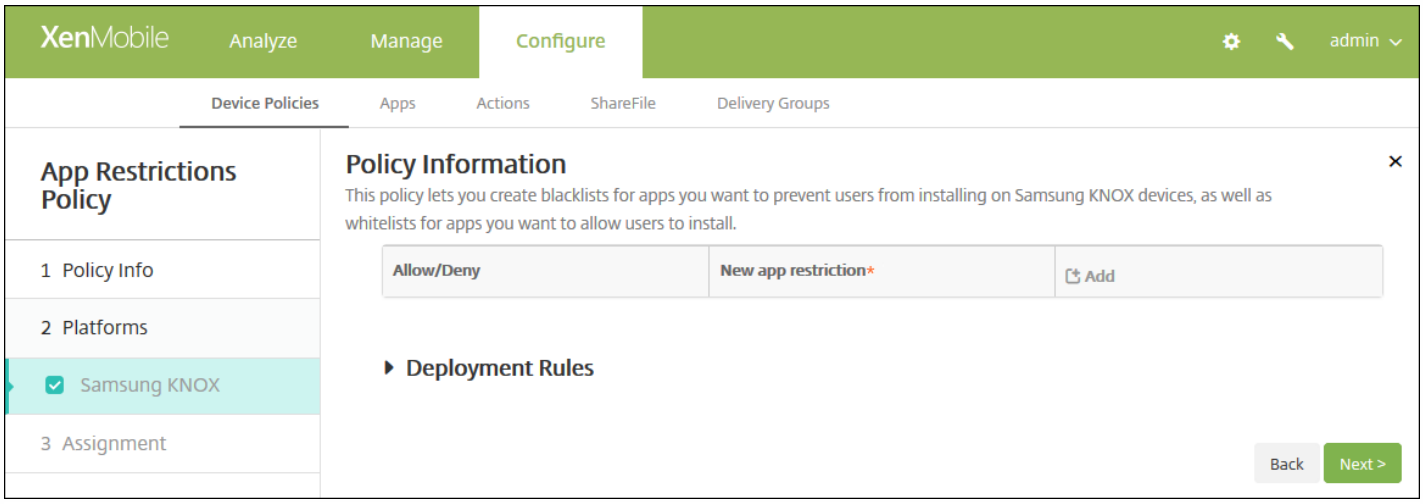
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **App-Einschränkungen**. Die Seite **App-Einschränkungen** wird angezeigt.



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:

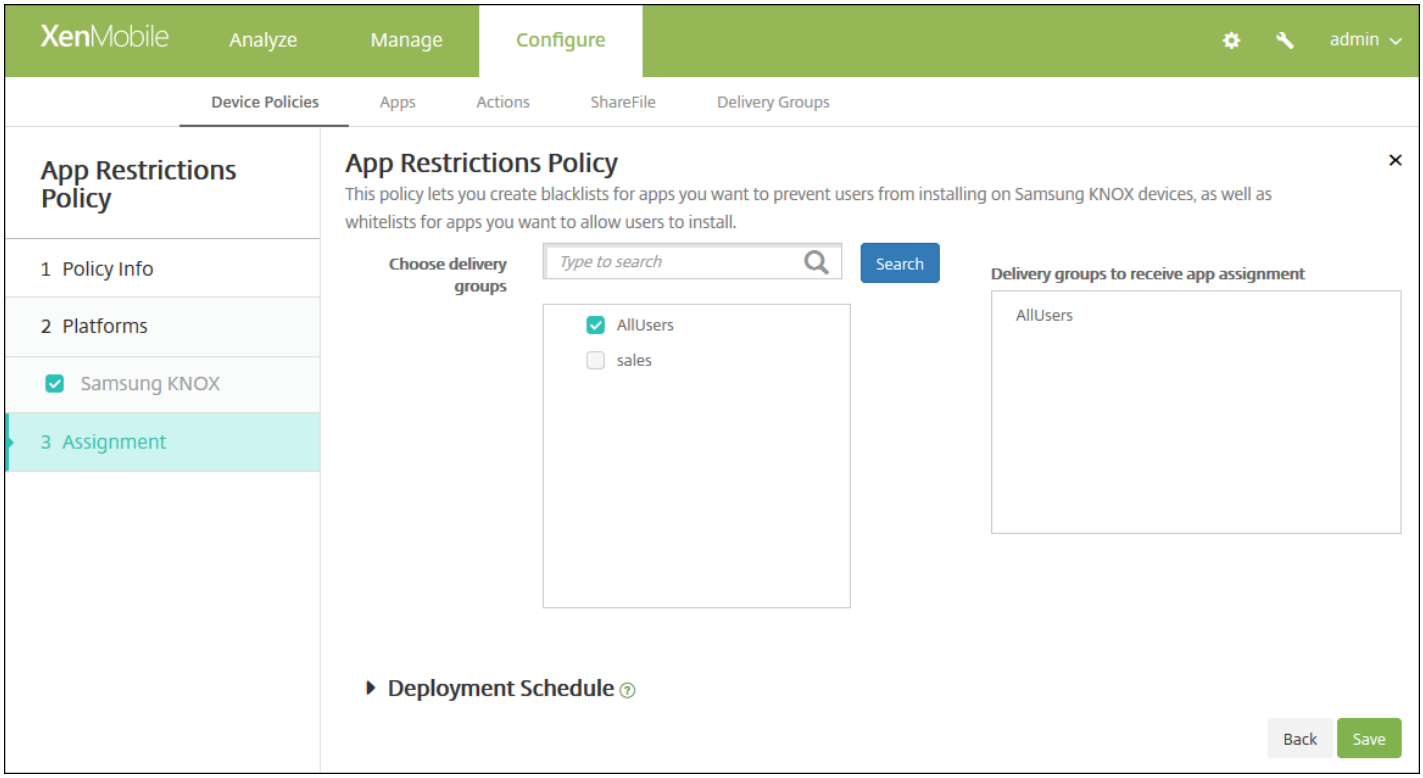
- **Zulassen/Verweigern**: Wählen Sie aus, ob Benutzern die Installation der App gestattet werden soll.
- **Neue App-Einschränkung**: Geben Sie die App-Paket-ID ein, z. B. "com.kmdm.af.crackle".
- Klicken Sie auf **Speichern**, um die App der Zulassen/Verweigern-Liste hinzuzufügen, oder auf **Abbrechen**, 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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

App-Tunnelrichtlinien für Geräte

Apr 24, 2017

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.

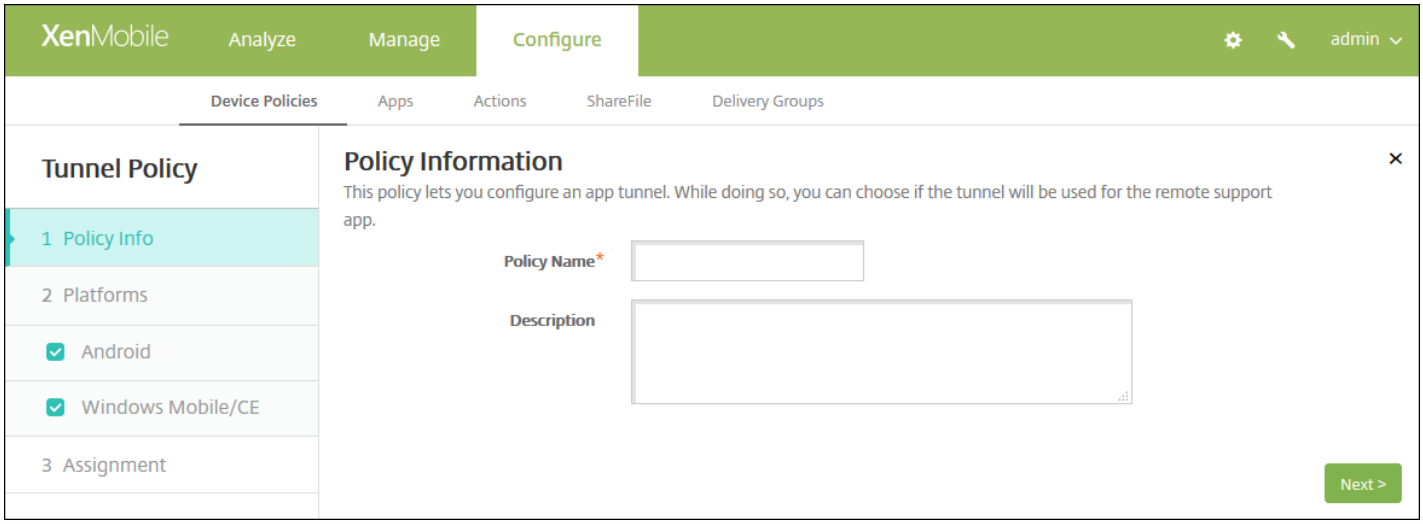
Android-Einstellungen

Windows Mobile-/CE-Einstellungen

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



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

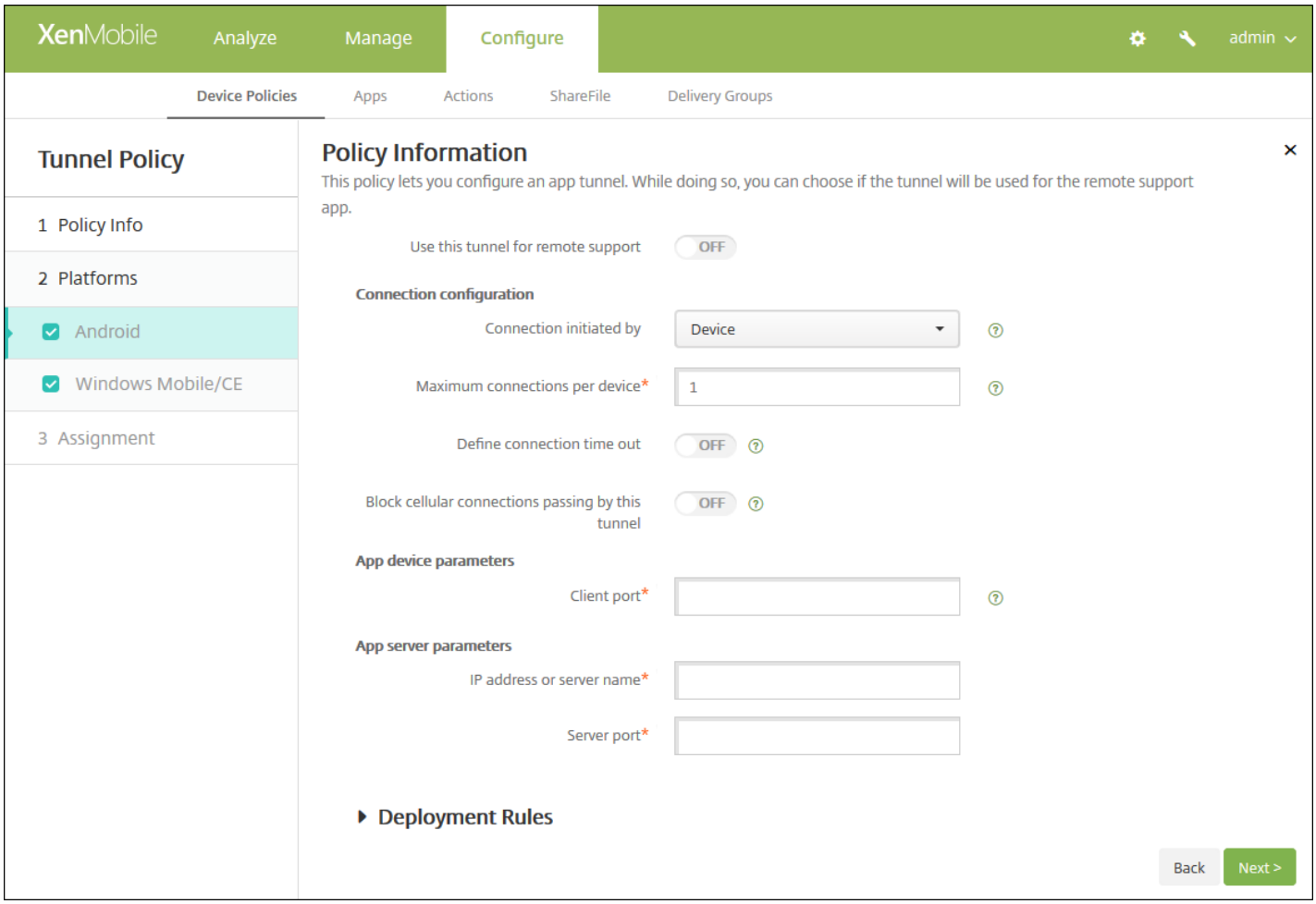
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Richtlinienplattform** 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.

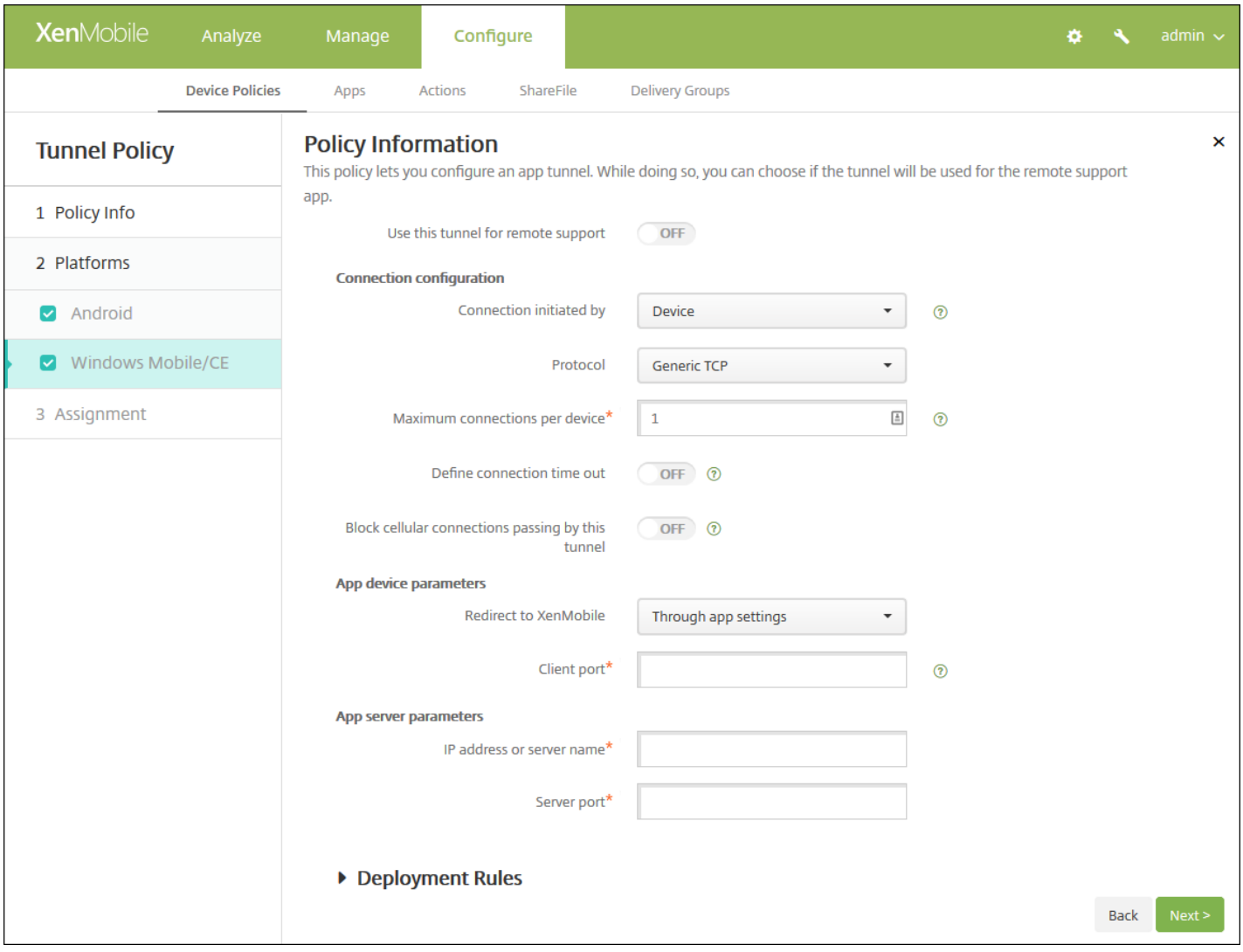
  Hinweis: Die Konfigurationsschritte unterscheiden sich je nachdem, ob Sie hier Remotesupport auswählen.

- 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:

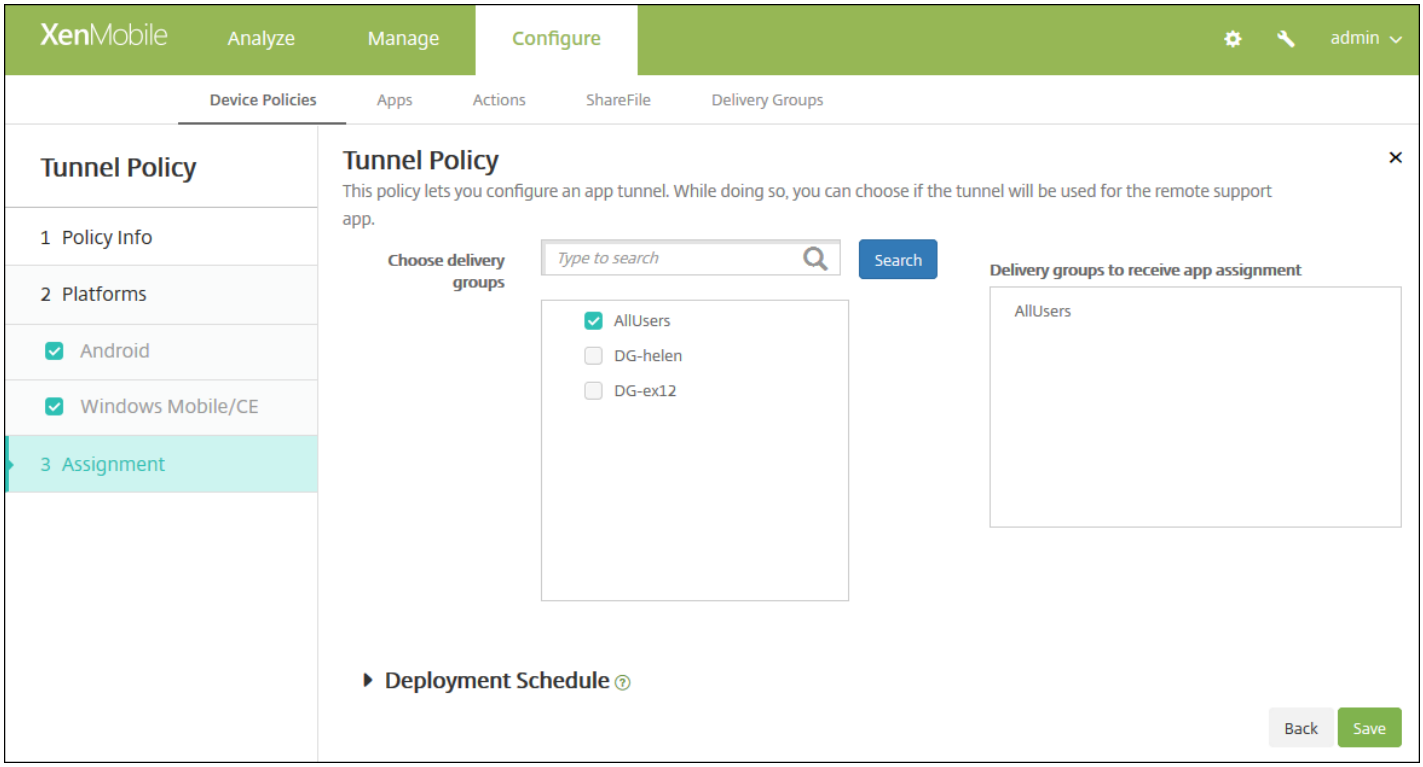
- **Tunnel für Remotesupport verwenden**: Geben Sie an, ob der Tunnel für Remotesupport verwendet werden soll.

Hinweis: Die Konfigurationsschritte unterscheiden sich je nachdem, ob Sie hier Remotesupport auswählen.

- Wenn Sie Remotesupport nicht auswählen, führen Sie folgende Schritte aus:
  - V**erbindung 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 das Alias unter **Lokales 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 Sie die Bereitstellungsregeln.

8. Klicken Sie auf **Weiter**. Die Seite **Tunnelrichtlinie** zum Zuweisen der Tunnelrichtlinie wird angezeigt.



9. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, 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. Der Standardwert ist **EIN**.Wenn Sie **AUS** wählen, müssen keine anderen Optionen konfiguriert werden.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Der Standardwert 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**. Der Standardwert ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Der Standardwert ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**. Diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

App-Deinstallationsrichtlinien für Geräte

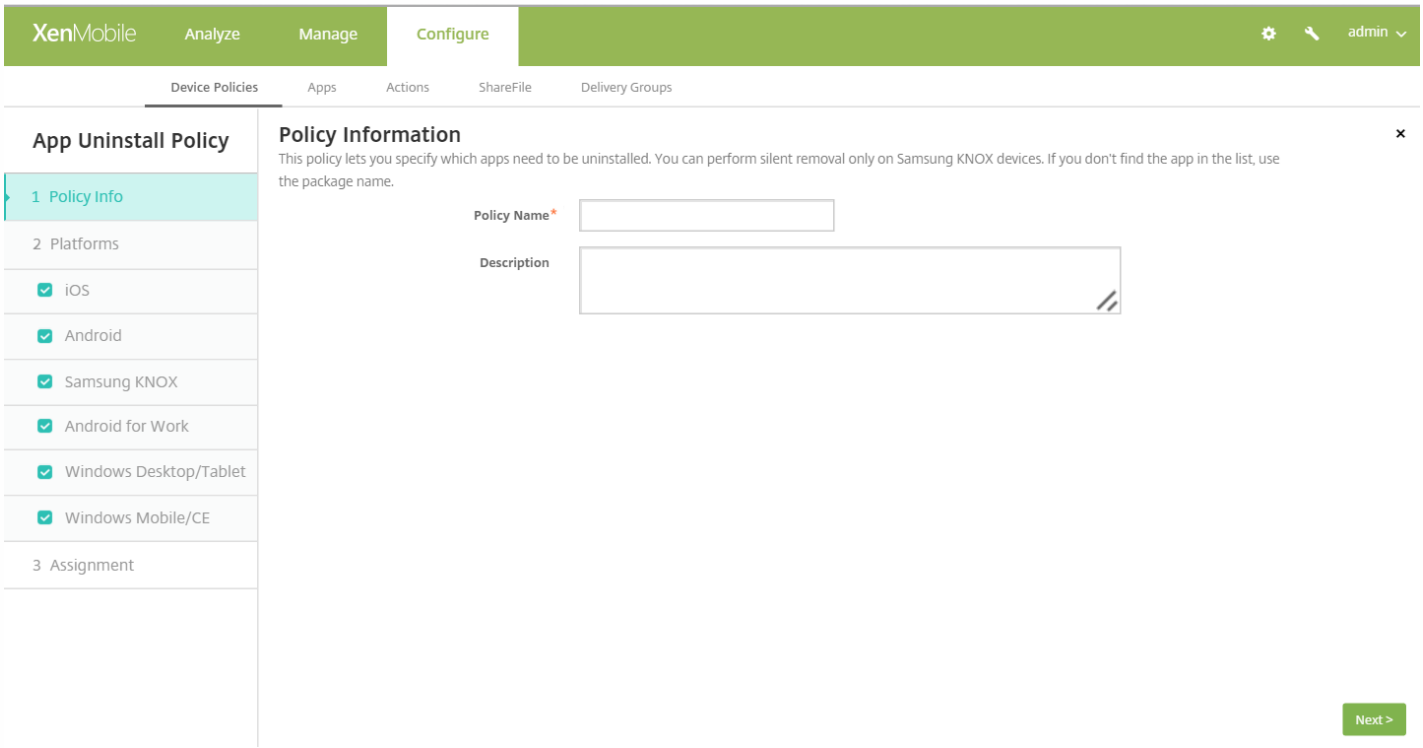
Feb 24, 2017

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. 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.

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.

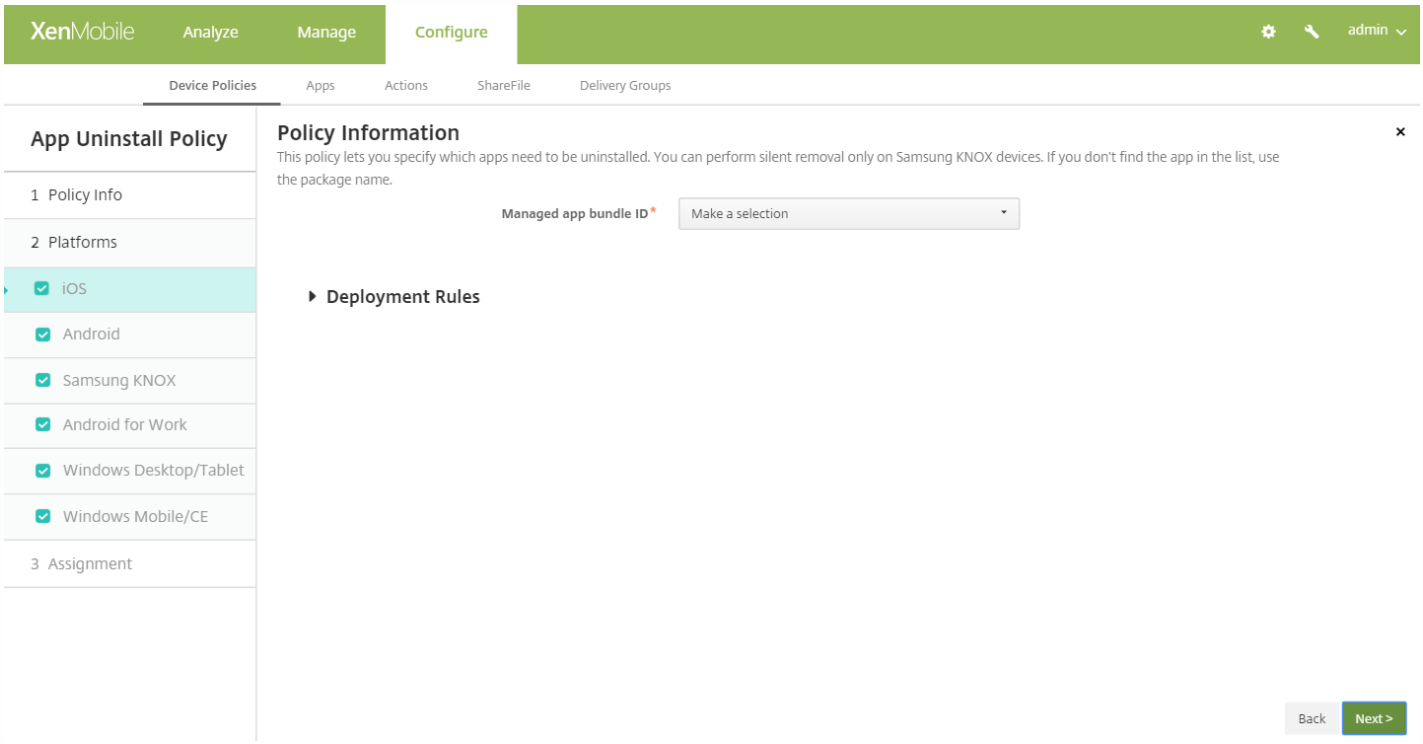
5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

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.

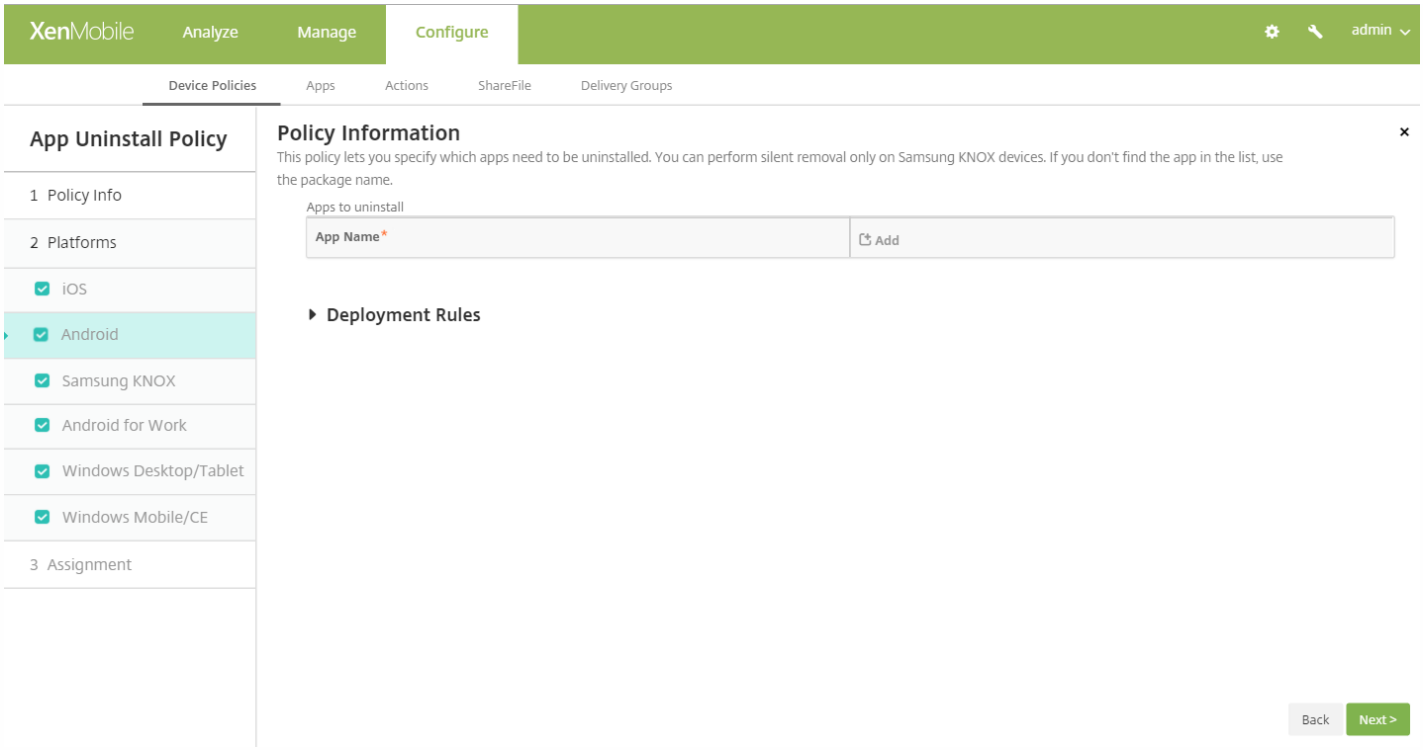
Konfigurieren von iOS-Einstellungen



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:

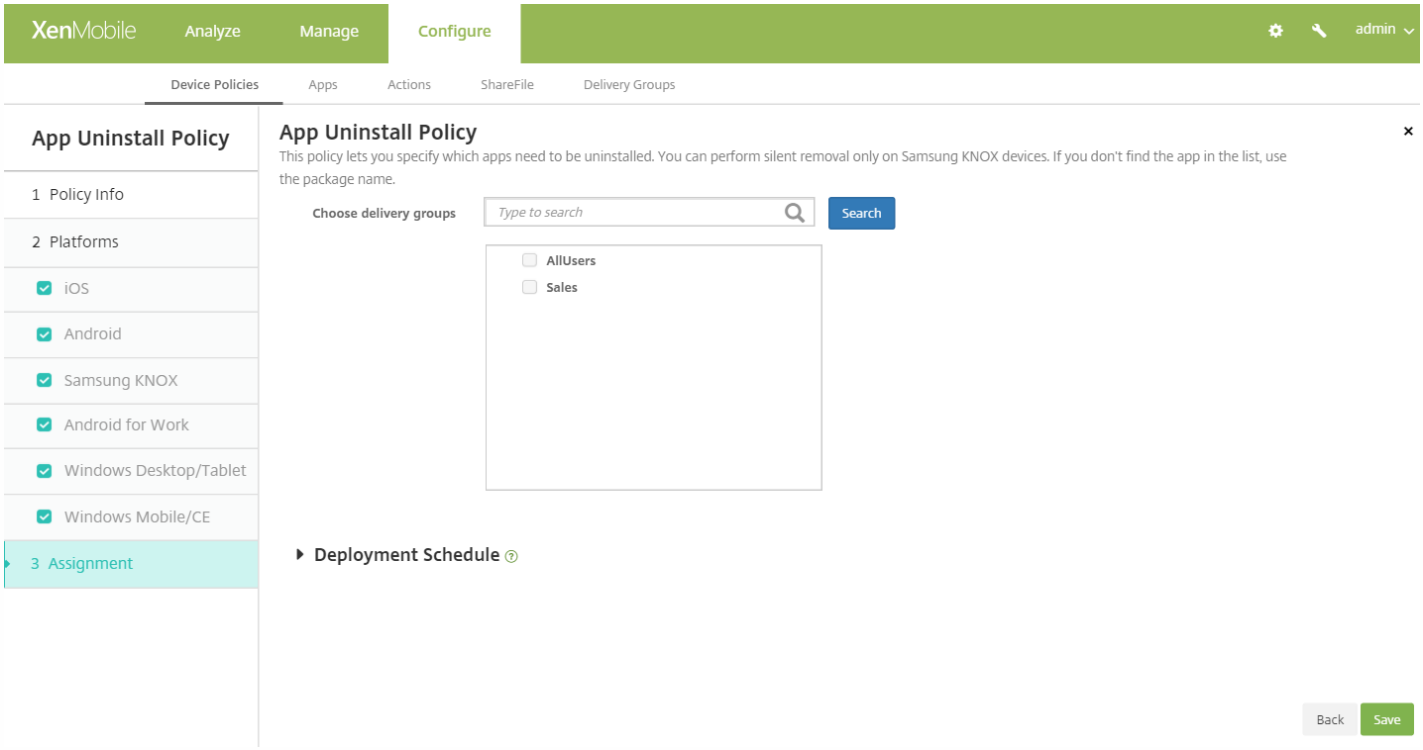
- **Apps zum Deinstallieren**: Klicken Sie für jede App, die Sie hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name**: Klicken Sie in der Liste auf eine vorhandene App oder klicken Sie auf **Add**, um einen neuen App-Namen einzugeben. Wenn keine Apps für 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Einschränkungsrichtlinien für die App-Deinstallation

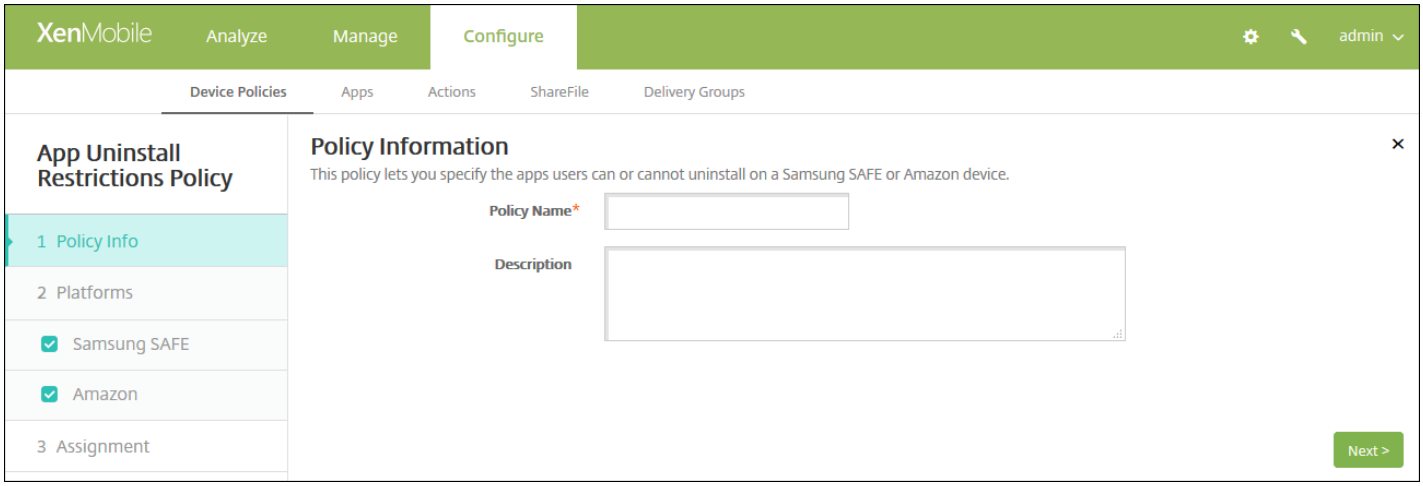
Feb 24, 2017

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.

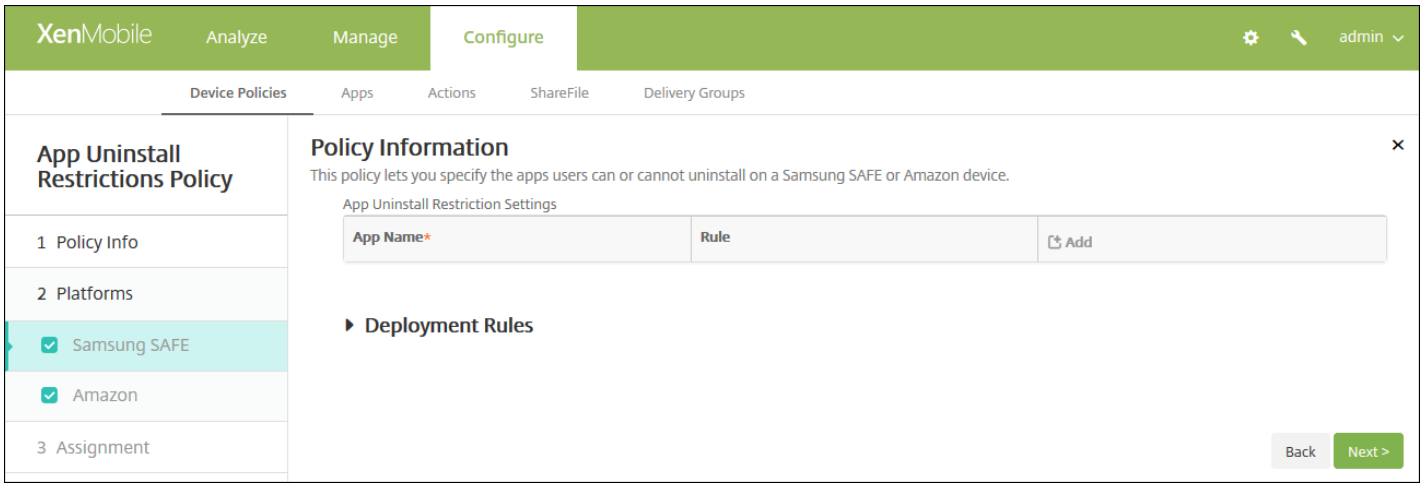
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Einschränkungen der App-Deinstallation**. Die Seite **Einschränkungen der App-Deinstallation** wird angezeigt.



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:

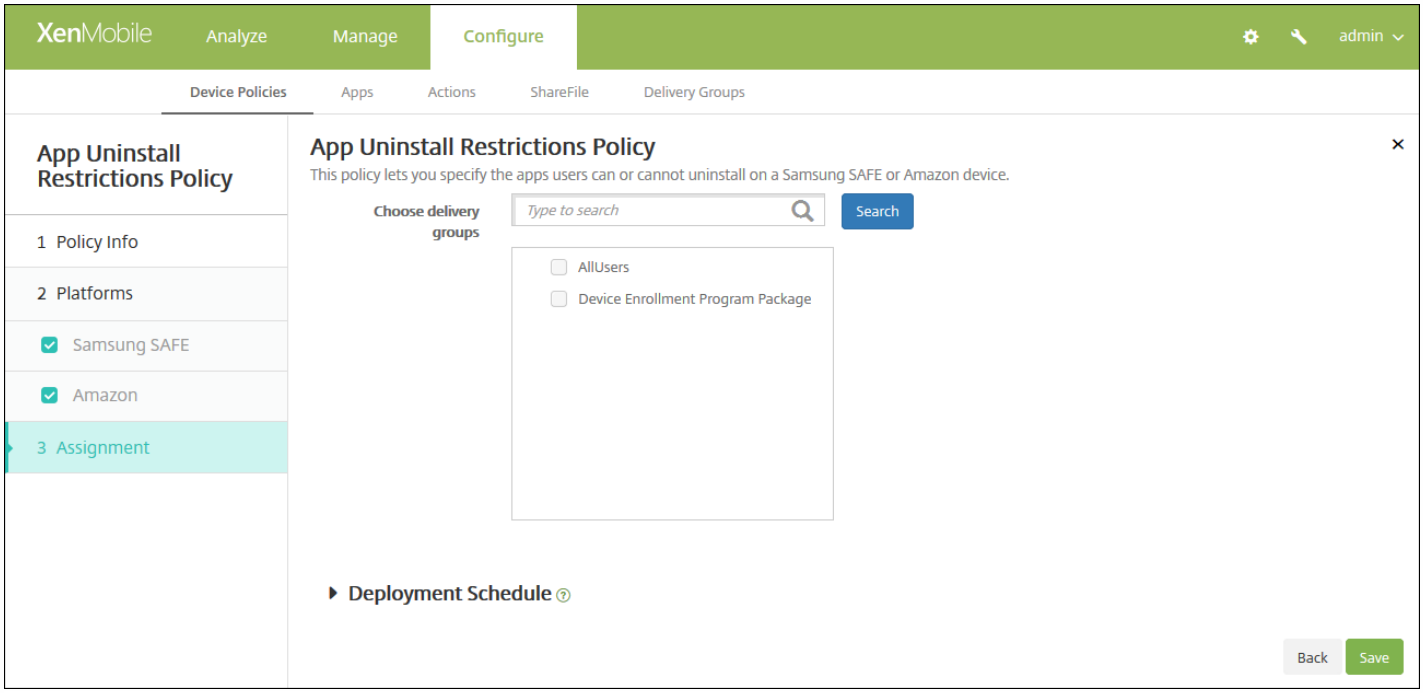
- **Einstellungen zum Einschränken der App-Deinstallation**: Klicken Sie für jede Regel, die Sie hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name**: Klicken Sie in der Liste auf eine vorhandene App oder klicken Sie auf **Hinzufügen**, um eine neue App hinzuzufügen.
  - **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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

12. Klicken Sie auf **Speichern**.

Browserrichtlinien für Geräte

Feb 24, 2017

Sie können Browserrichtlinien für Samsung SAFE- oder Samsung KNOX-Geräte erstellen, um festzulegen, ob die Benutzer den Browser verwenden können, oder um die Browserfunktionen einzuschränken, die auf den Geräten verwendet werden können.

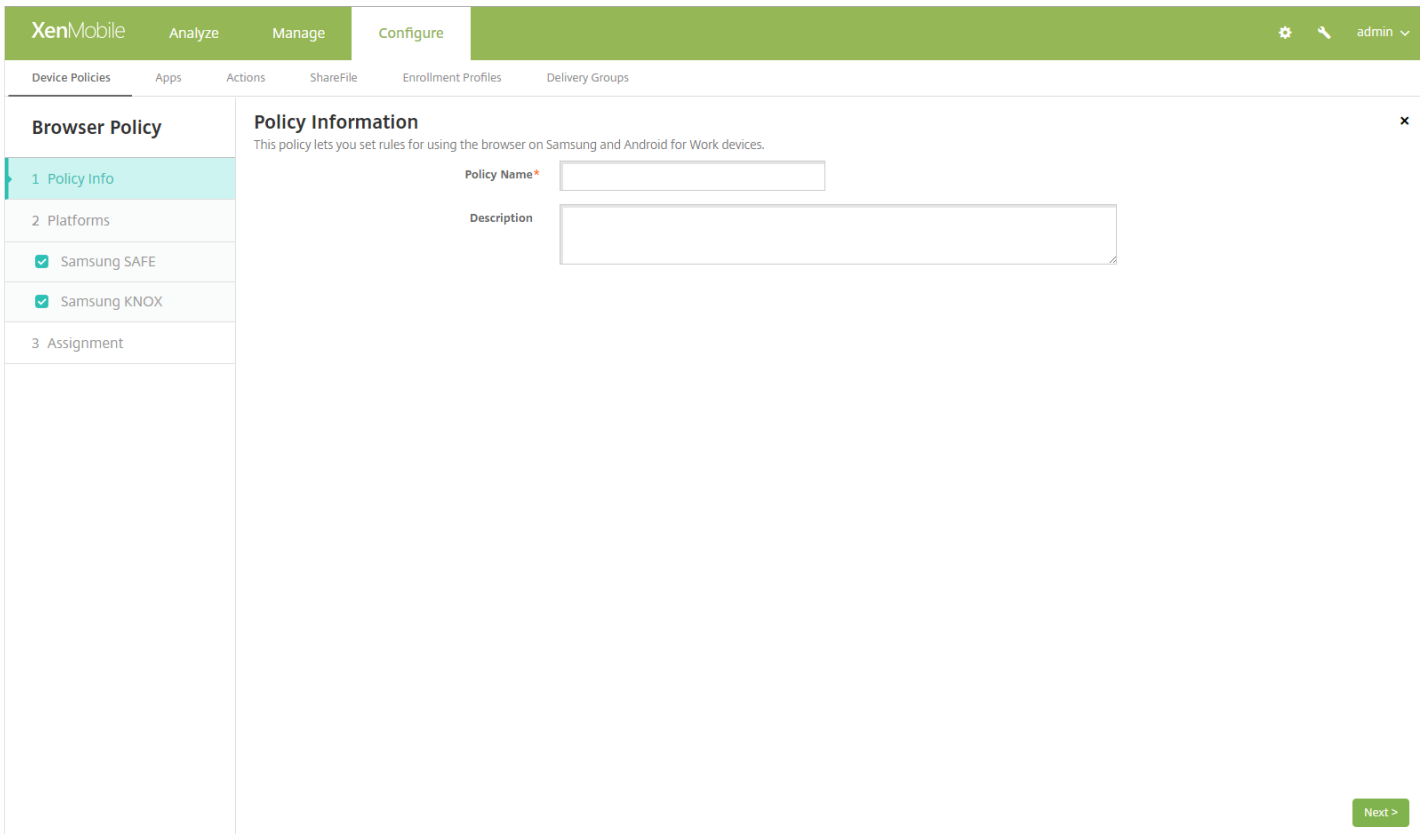
Auf Samsung-Geräten können Sie den Browser vollständig deaktivieren oder Popupfenster, JavaScript, Cookies, automatisches Ausfüllen und Betrugswarnungen aktivieren oder deaktivieren.

Samsung SAFE- und Samsung KNOX-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:

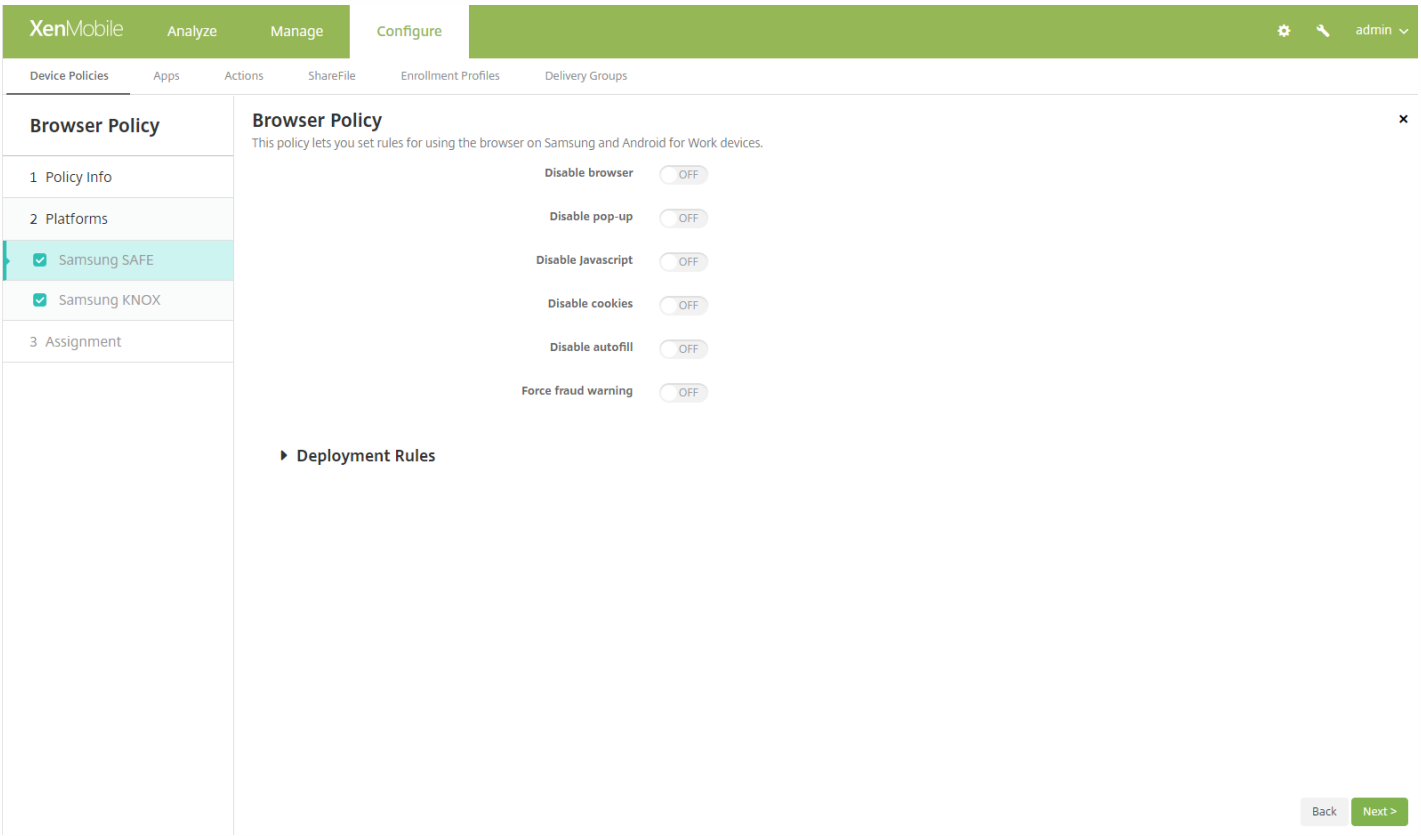
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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

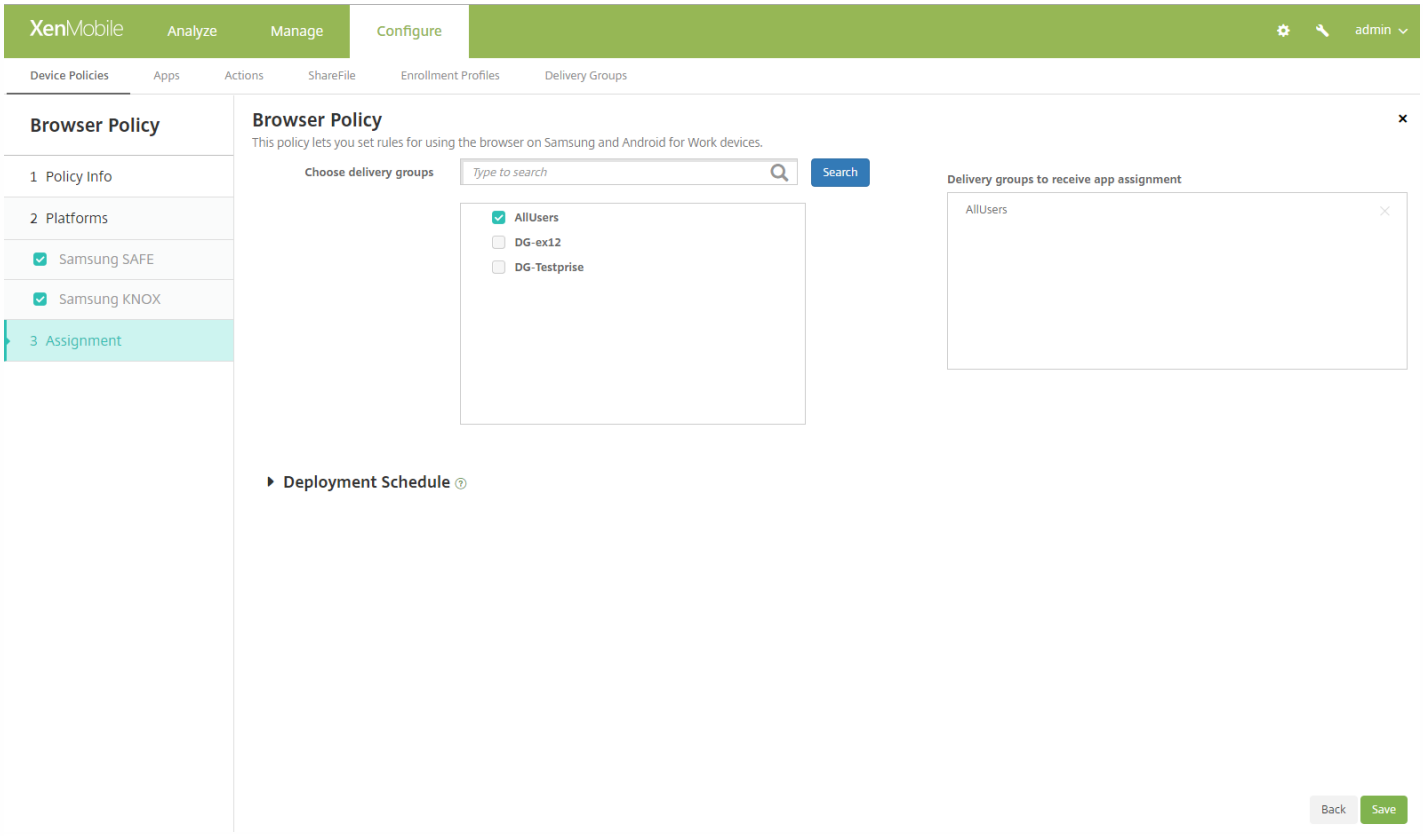


Konfigurieren Sie folgende Einstellungen:

- **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.

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Kalenderrichtlinien

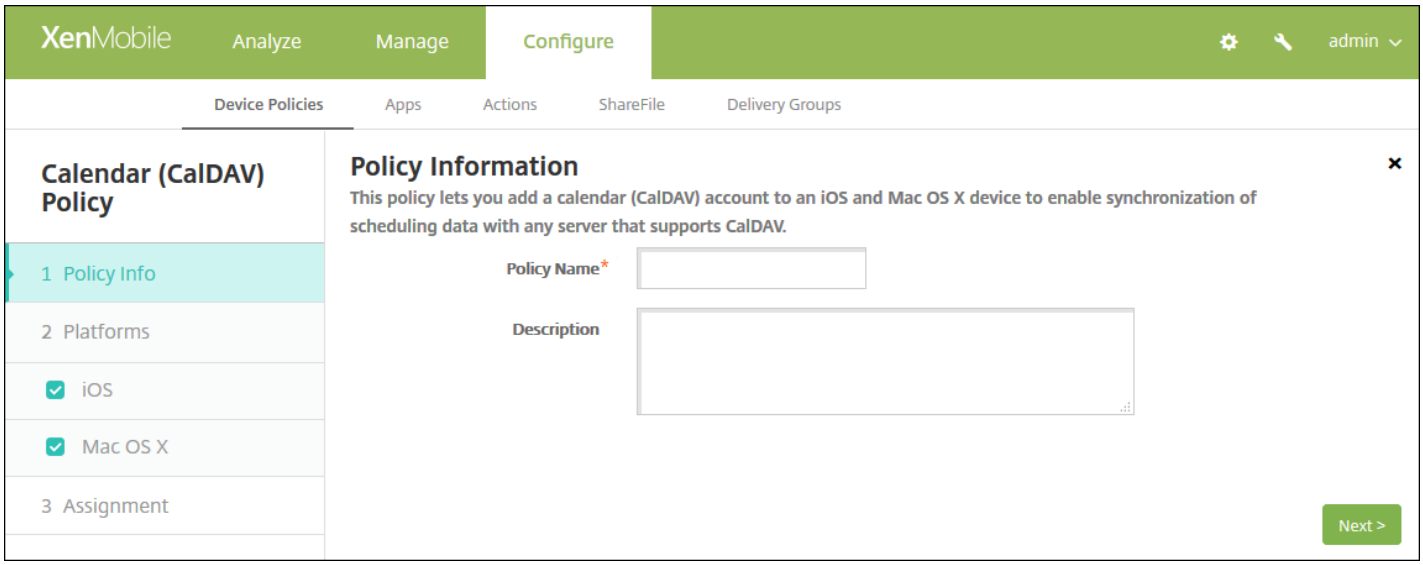
Feb 24, 2017

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:

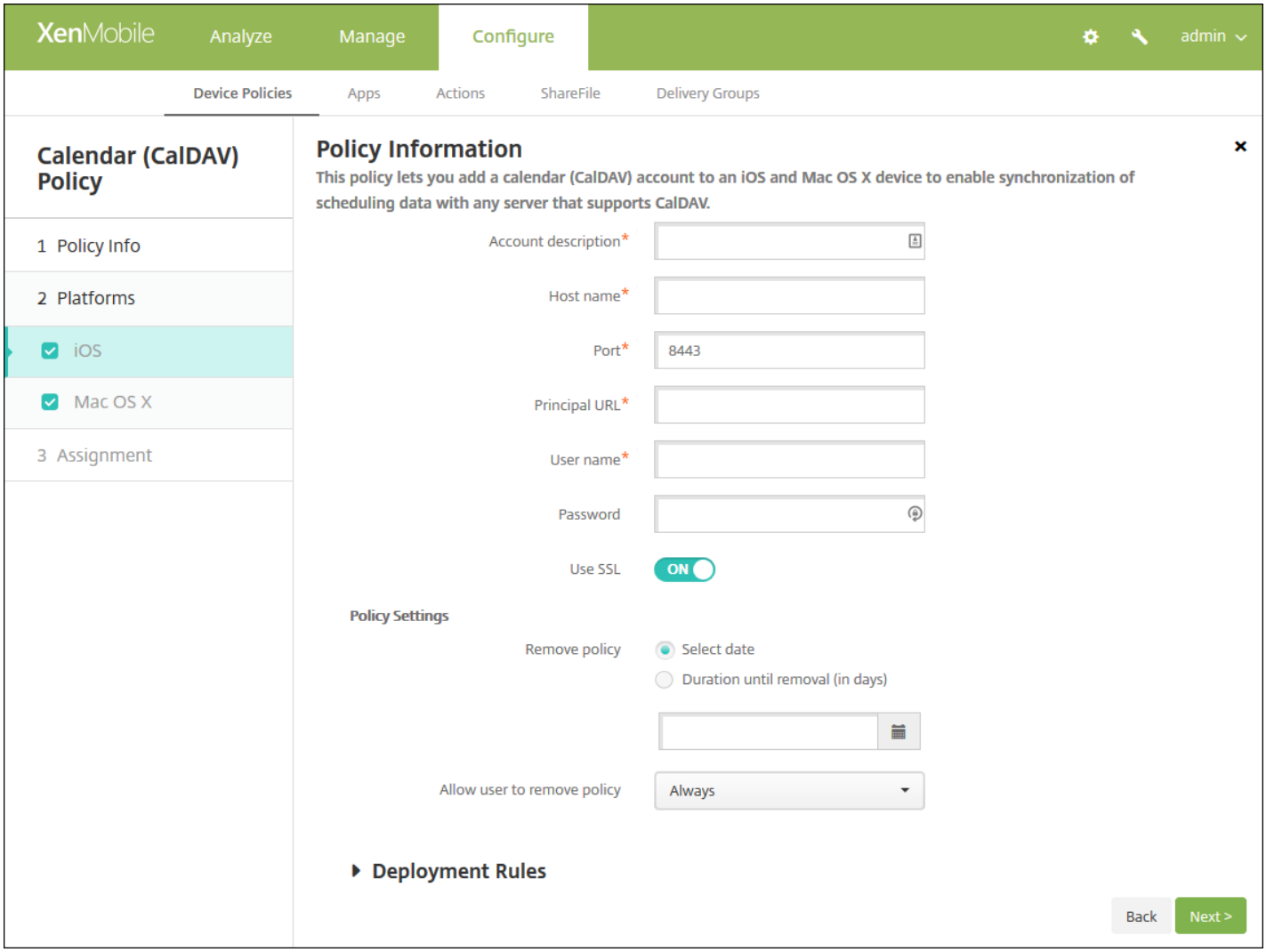
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

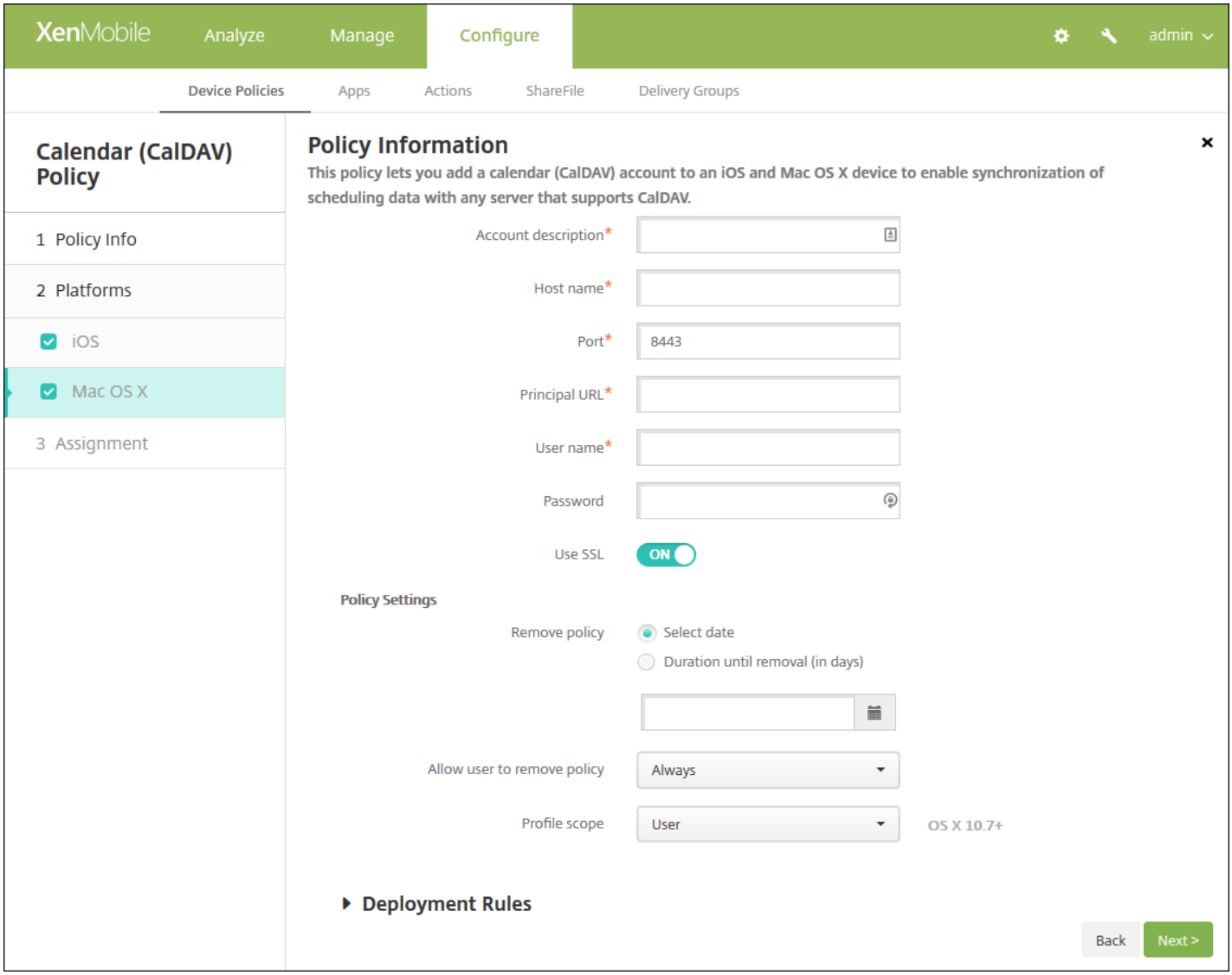
Konfigurieren von iOS-Einstellungen



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. Der Standardwert 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



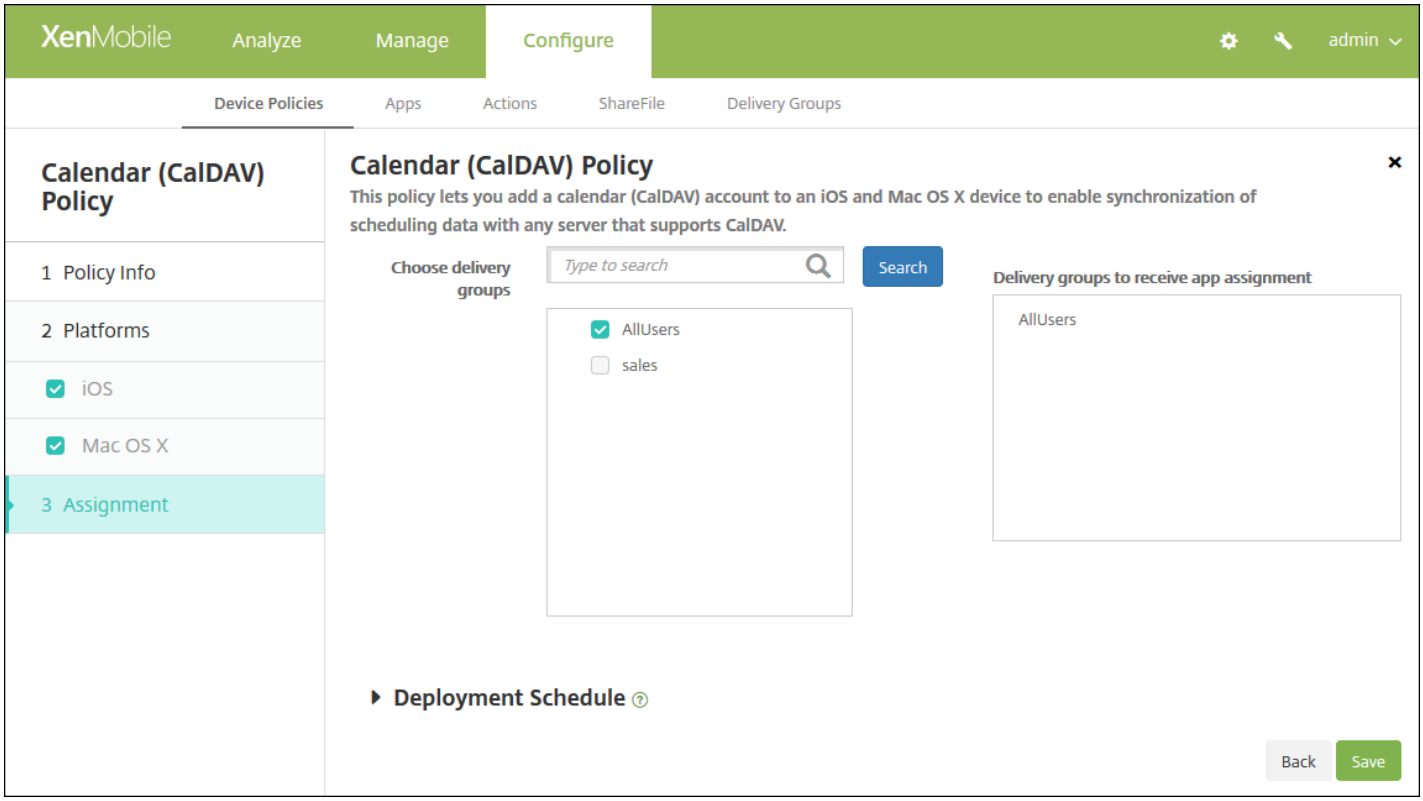
Konfigurieren Sie die folgenden Einstellungen:

- **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. Der Standardwert 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 **Passcode 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen,

mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Mobilfunkgeräterichtlinie

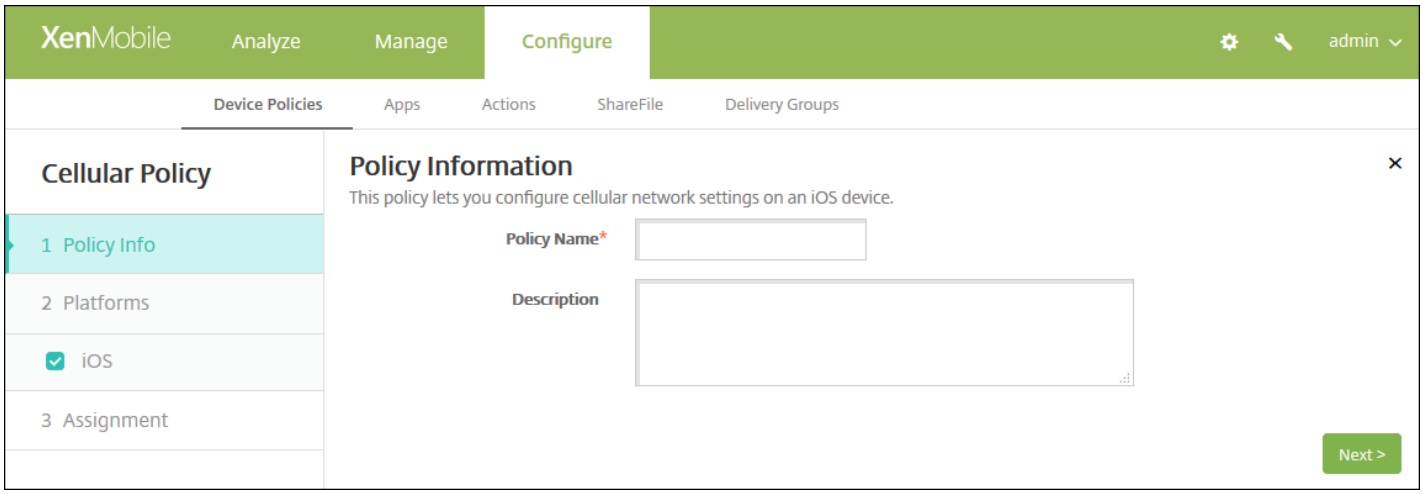
Feb 24, 2017

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.

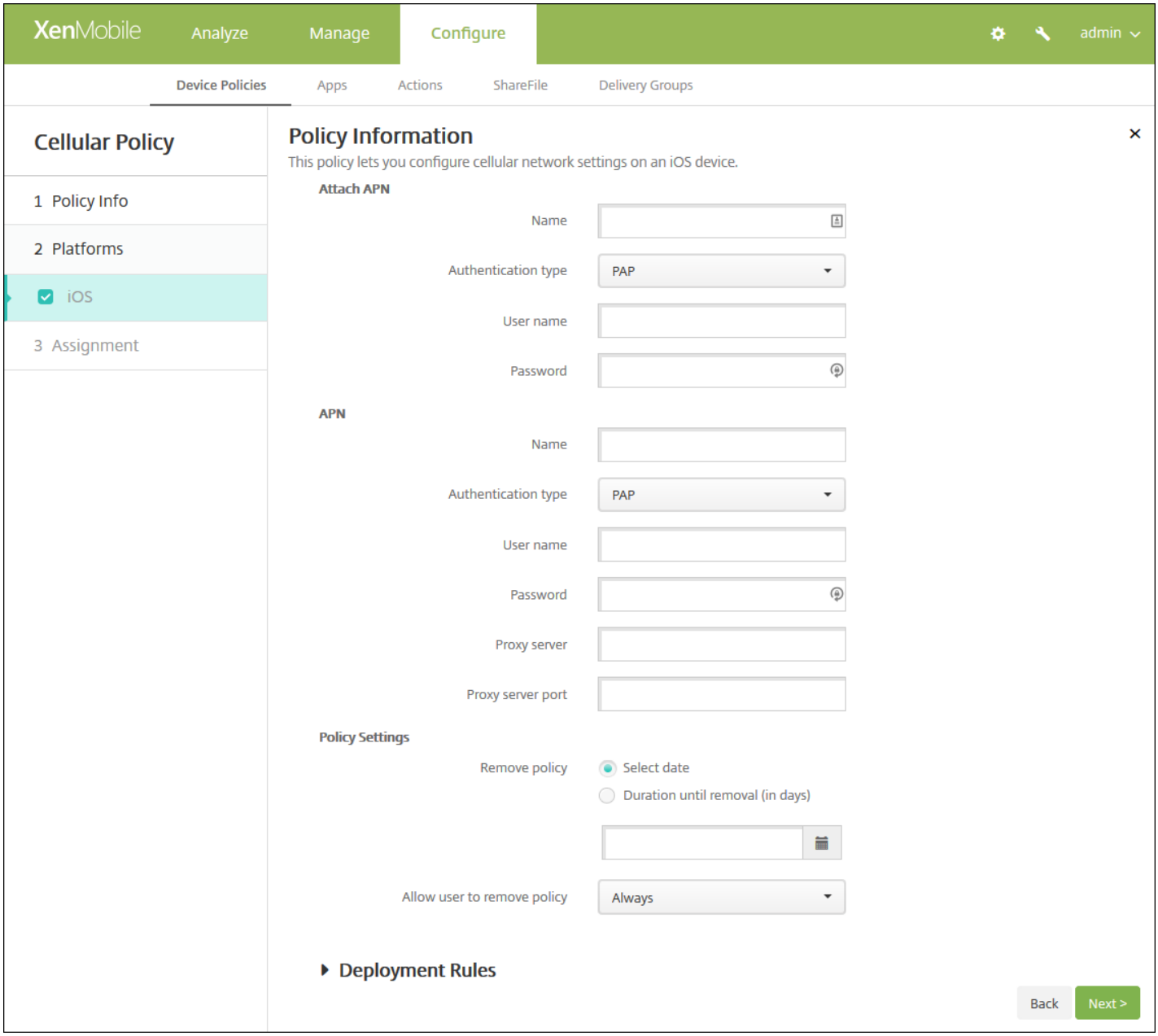
3. Erweitern Sie **Mehr** und klicken Sie unter **Netzwerkzugriff** auf **Mobilnetz**. Die Seite **Mobilnetz** wird angezeigt.



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.



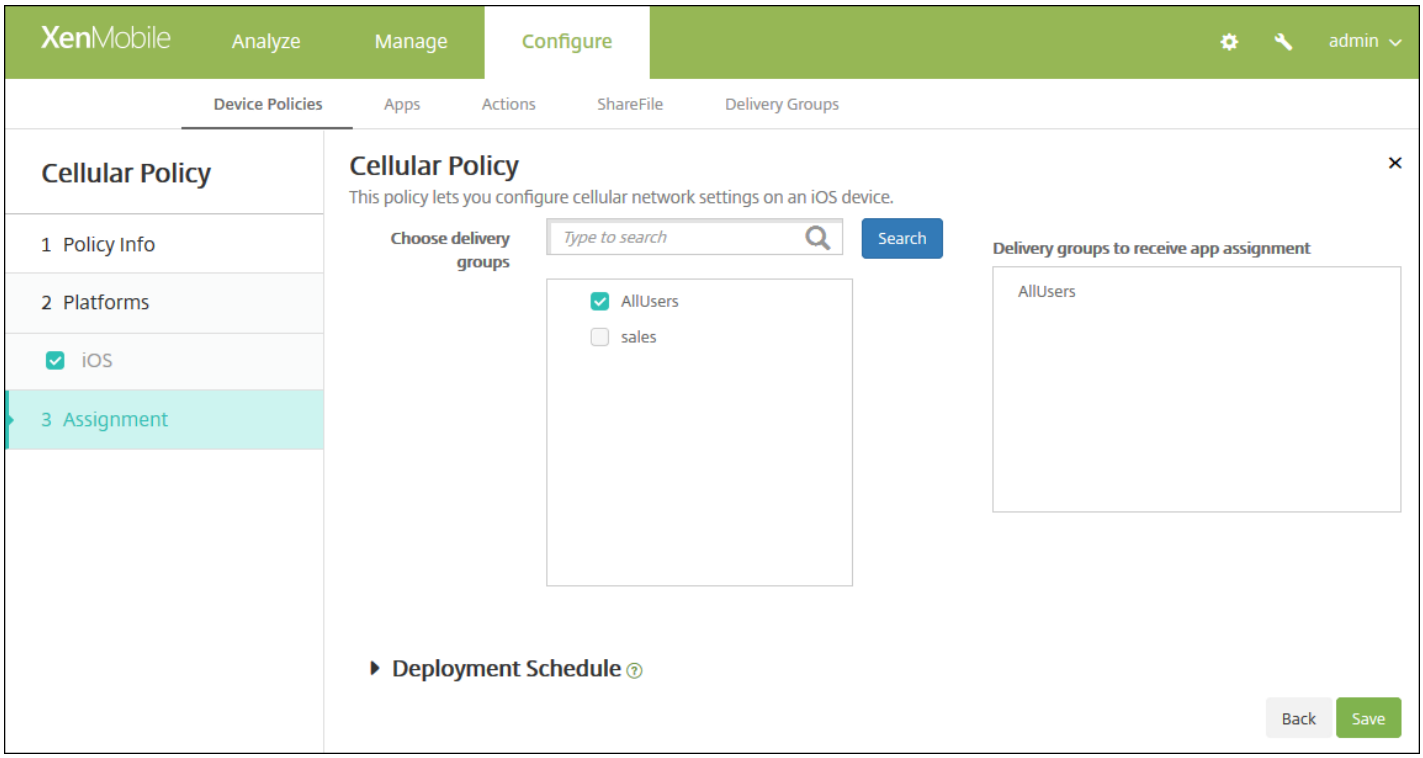
6. Konfigurieren Sie die folgenden Einstellungen:

- **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 einen 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 einen 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 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.

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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Verbindungsmanagerrichtlinie

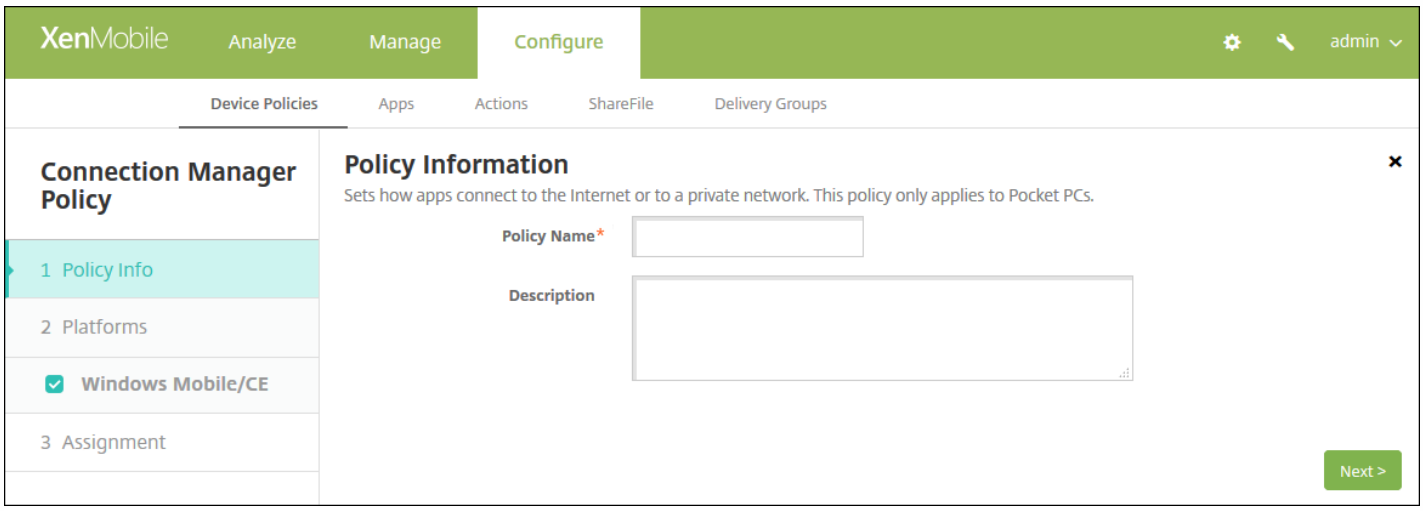
Feb 24, 2017

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.

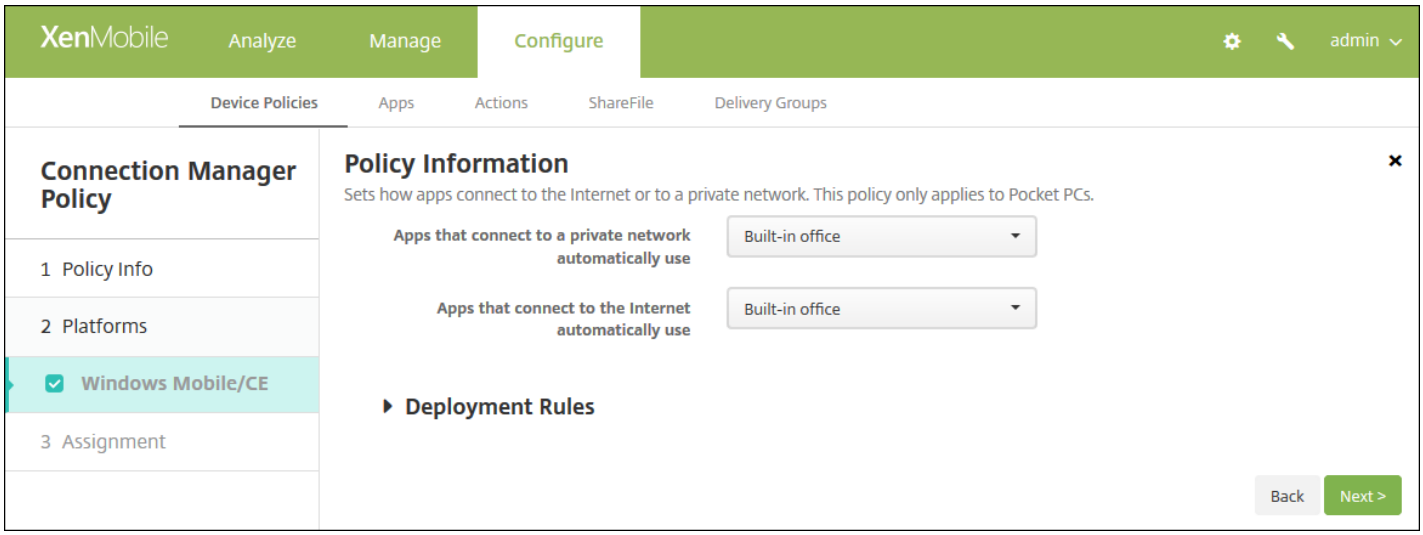
3. Klicken Sie auf **Mehr** und dann unter **Netzwerkzugriff** auf **Verbindungsmanager**. Die Seite **Richtlinieninfo** wird angezeigt.



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.



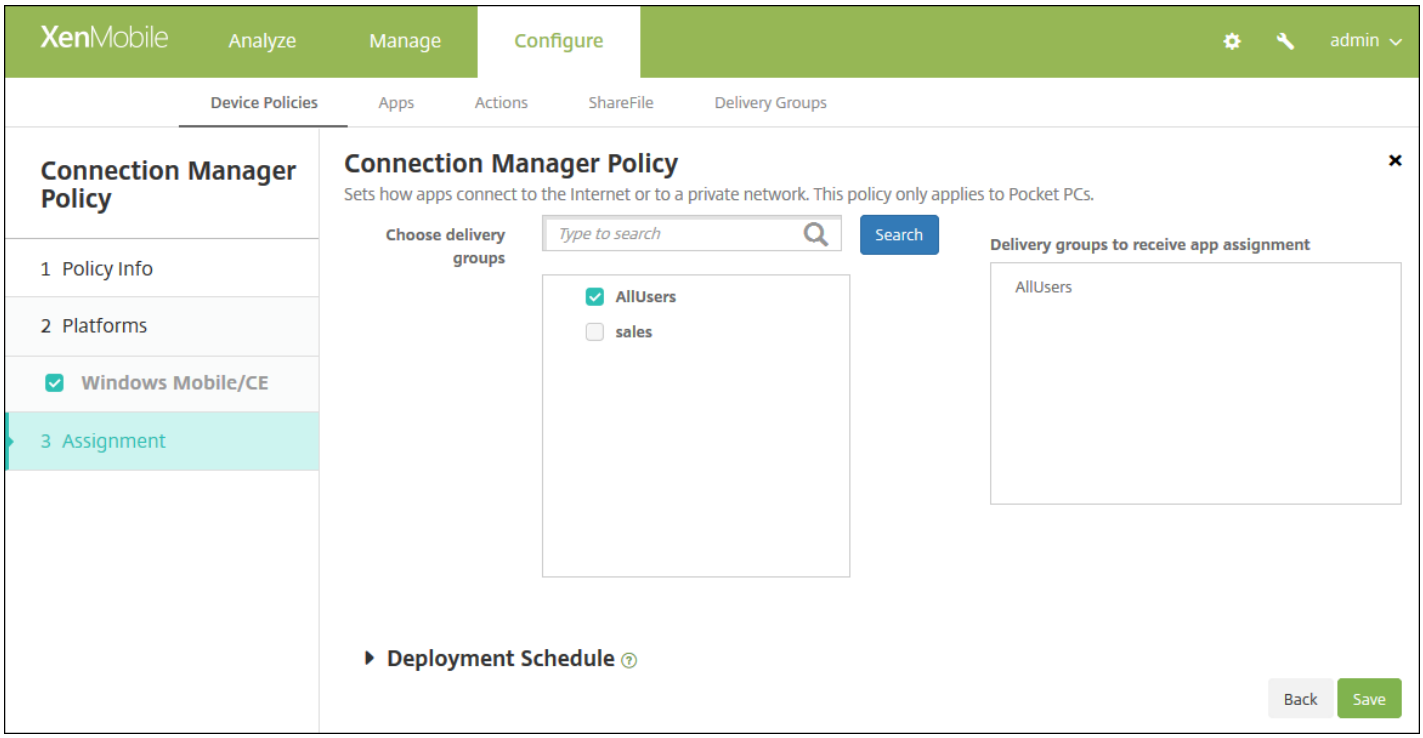
6. Konfigurieren Sie diese Einstellungen.

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 **Später** 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 **OFF**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Verbindungszeitplanrichtlinien für Geräte

Feb 24, 2017

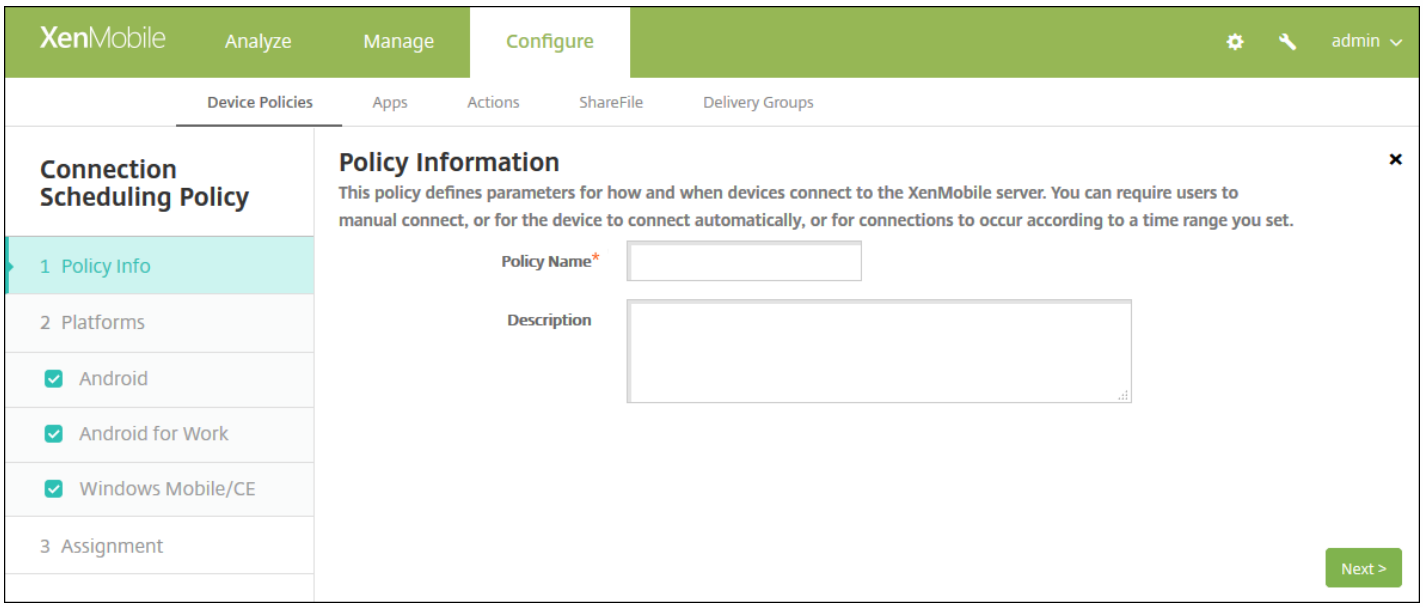
Sie erstellen Verbindungszeitplanrichtlinien, um vorzugeben, wie und wann Geräte eine Verbindung mit XenMobile herstellen sollen. Sie können diese Richtlinie auch für Geräte konfigurieren, die für Android for Work aktiviert sind.

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.

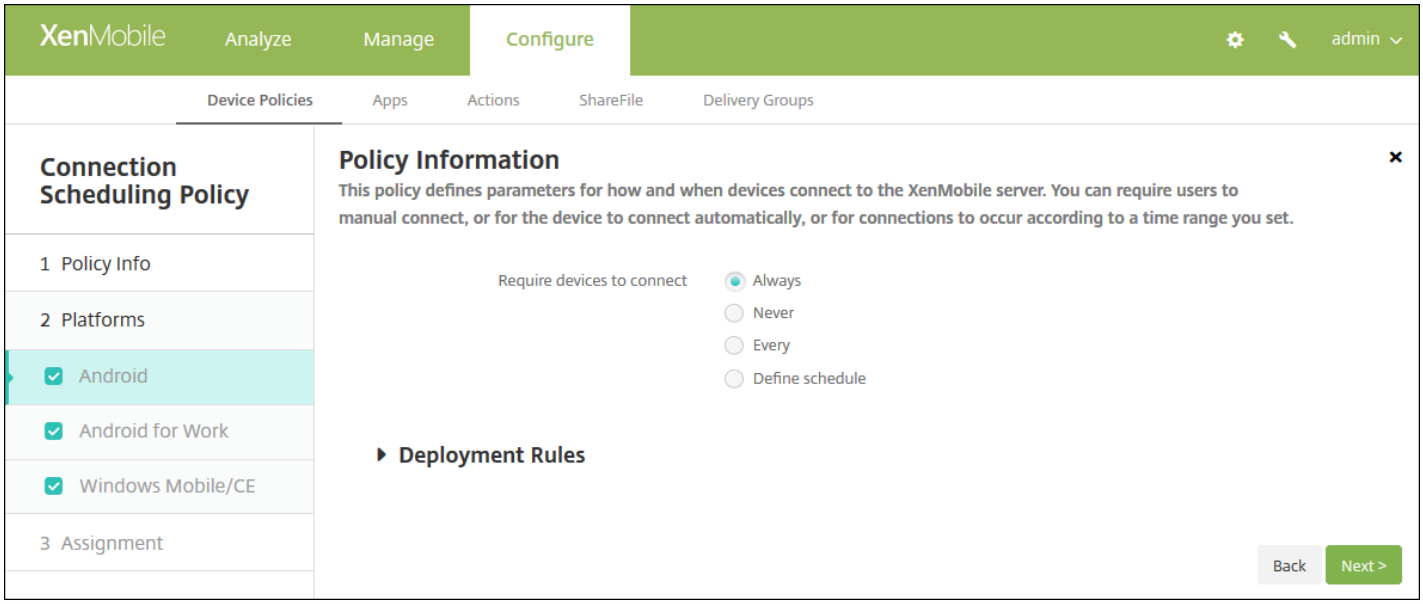
3. Klicken Sie auf **Planung**. Die Seite **Verbindungszeitplan** wird angezeigt.



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:

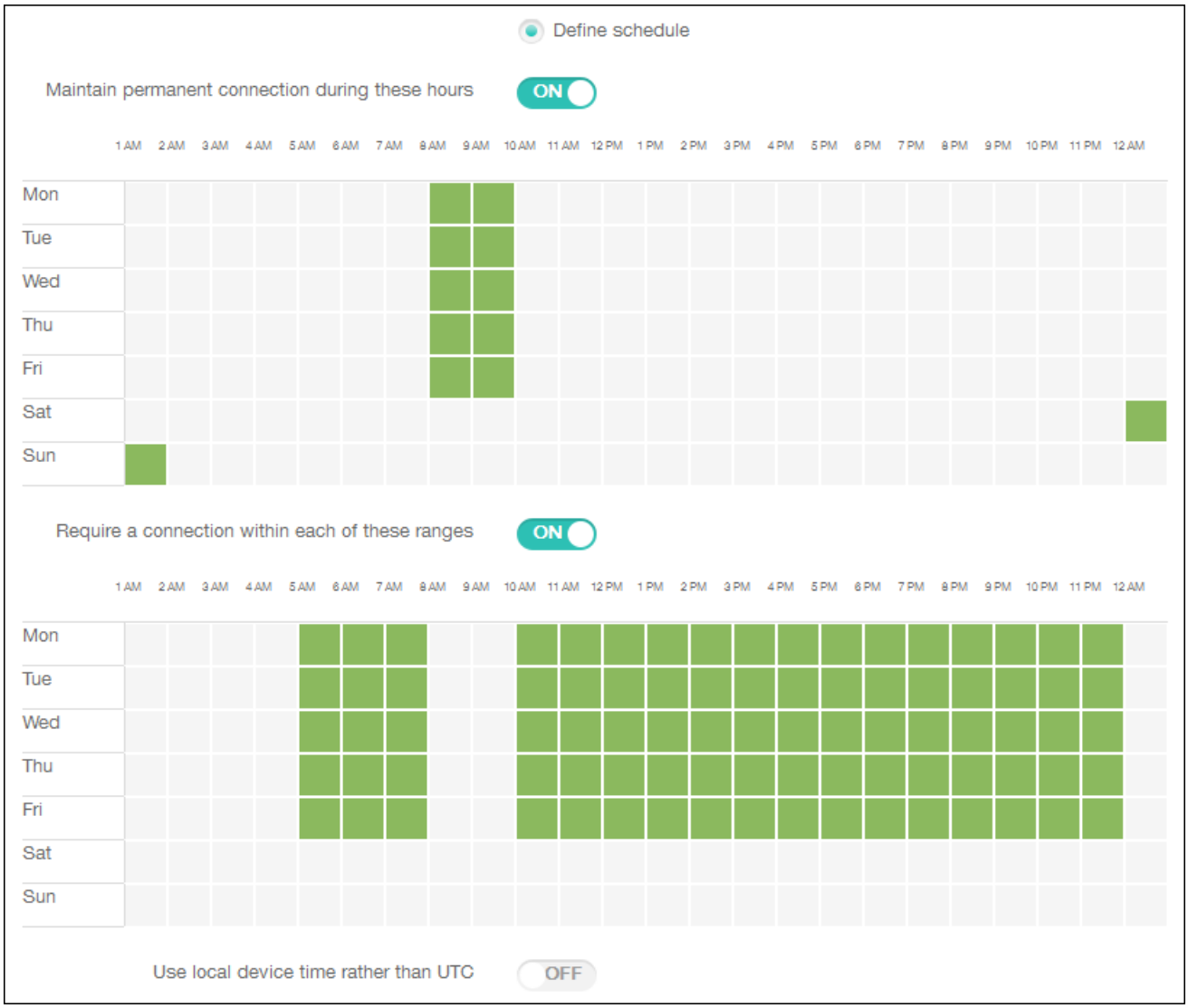
- **Geräte müssen Verbindung herstellen**: Klicken Sie auf die Option, die Sie für diesen Zeitplan festlegen möchten.
  - **Immer**: Die Verbindung bleibt jederzeit bestehen. XenMobile auf dem Benutzergerät versucht nach einer Netzwerkverbindungsunterbrechung eine Wiederherstellung der Verbindung mit dem XenMobile-Server und überwacht die Verbindung durch regelmäßige Übertragung von Steuerpaketen. Citrix empfiehlt diese Option zur Gewährleistung der optimalen 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 Produktionsumgebungen zu verwenden, da sie die Bereitstellung von Sicherheitsrichtlinien auf Geräten verhindert, sodass Benutzer nie neue Apps und Richtlinien erhalten.
  - **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.

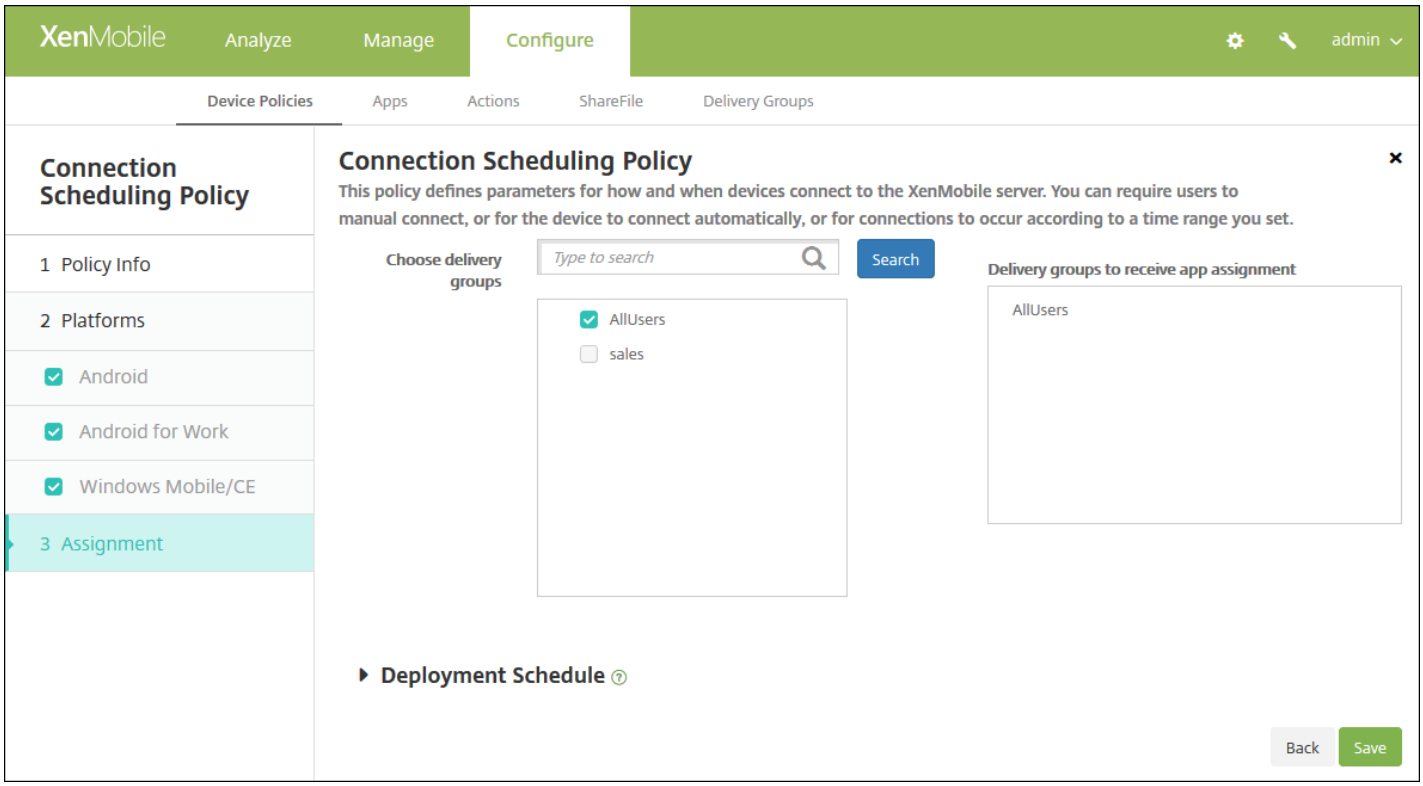
Definieren eines Verbindungszeitrahmens

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.



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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

12. Klicken Sie auf **Speichern**.

Geräterichtlinie für Kontakte (CardDAV)

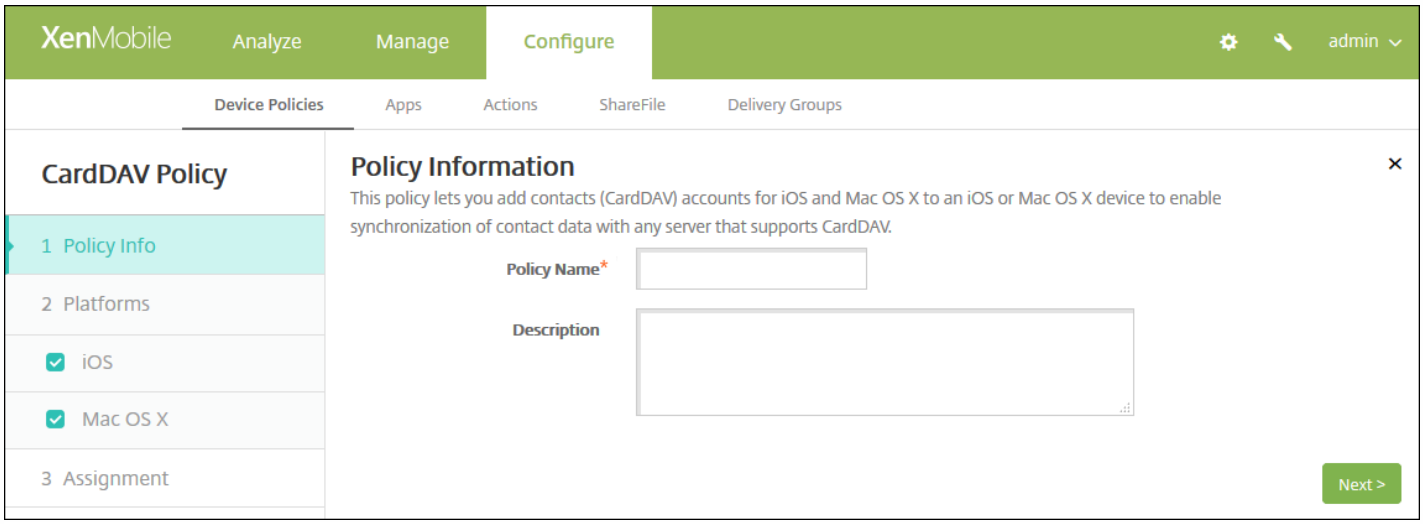
Feb 24, 2017

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:

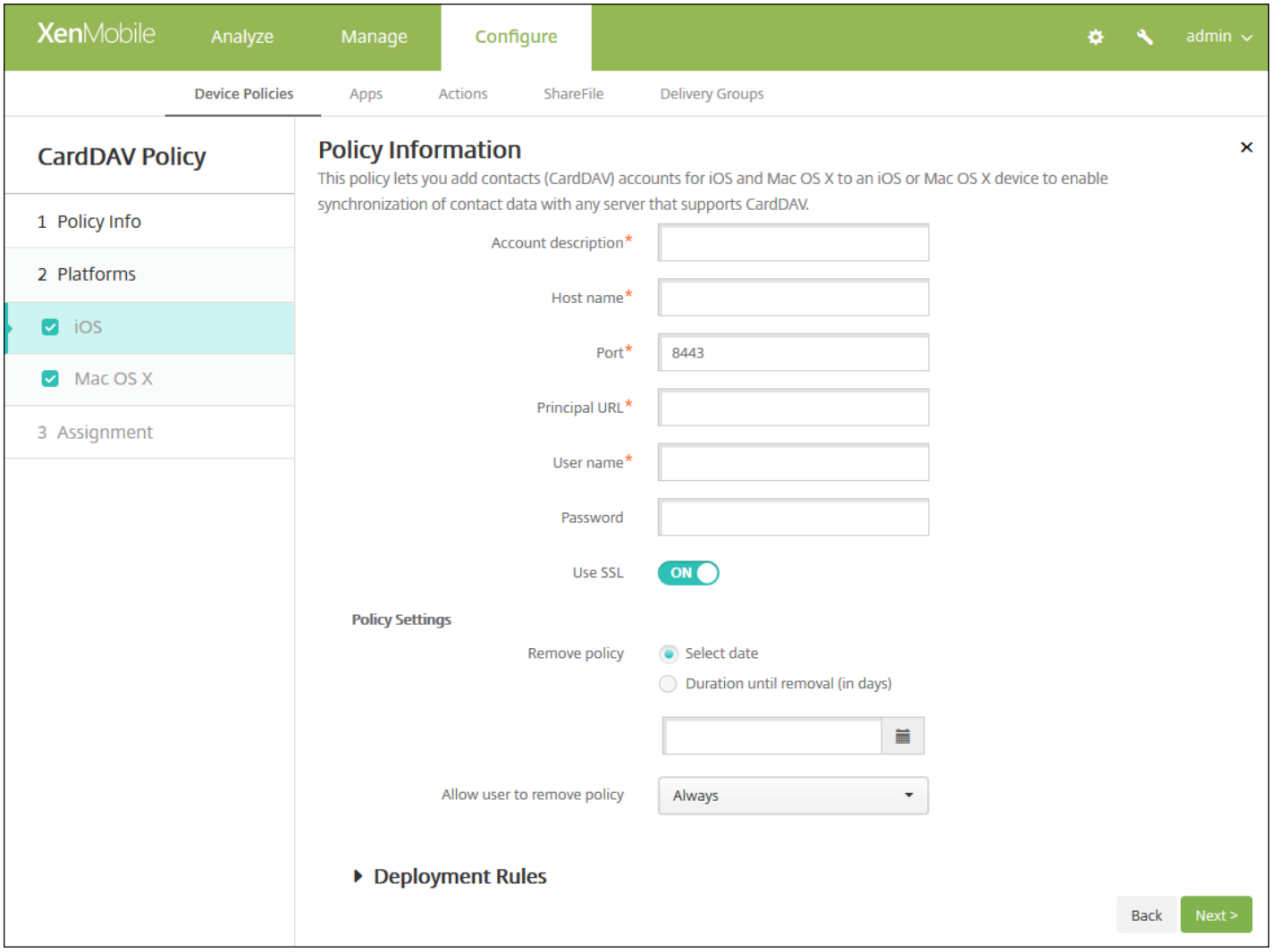
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

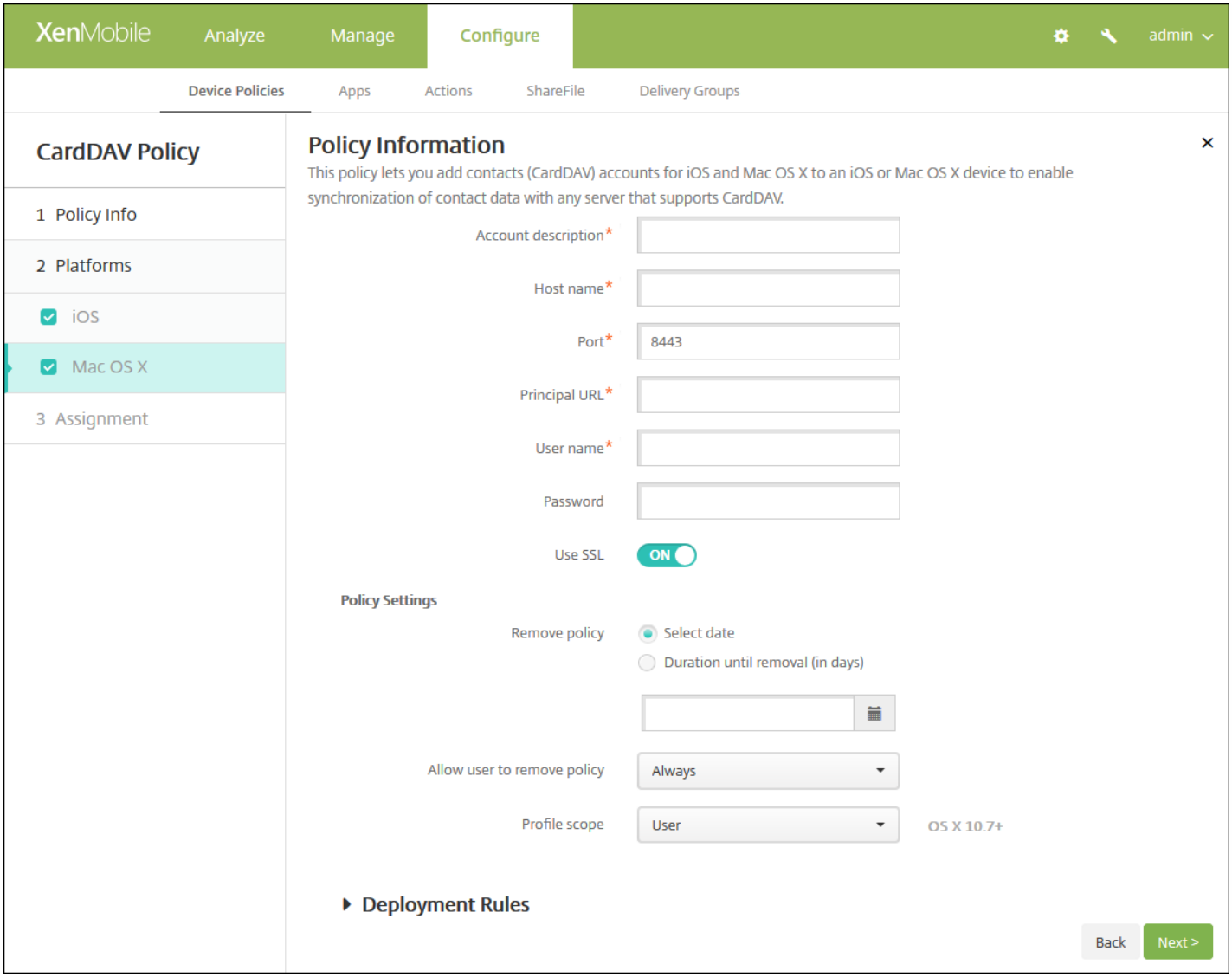
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Kontobeschreibung**: Geben Sie eine 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. Der Standardwert 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



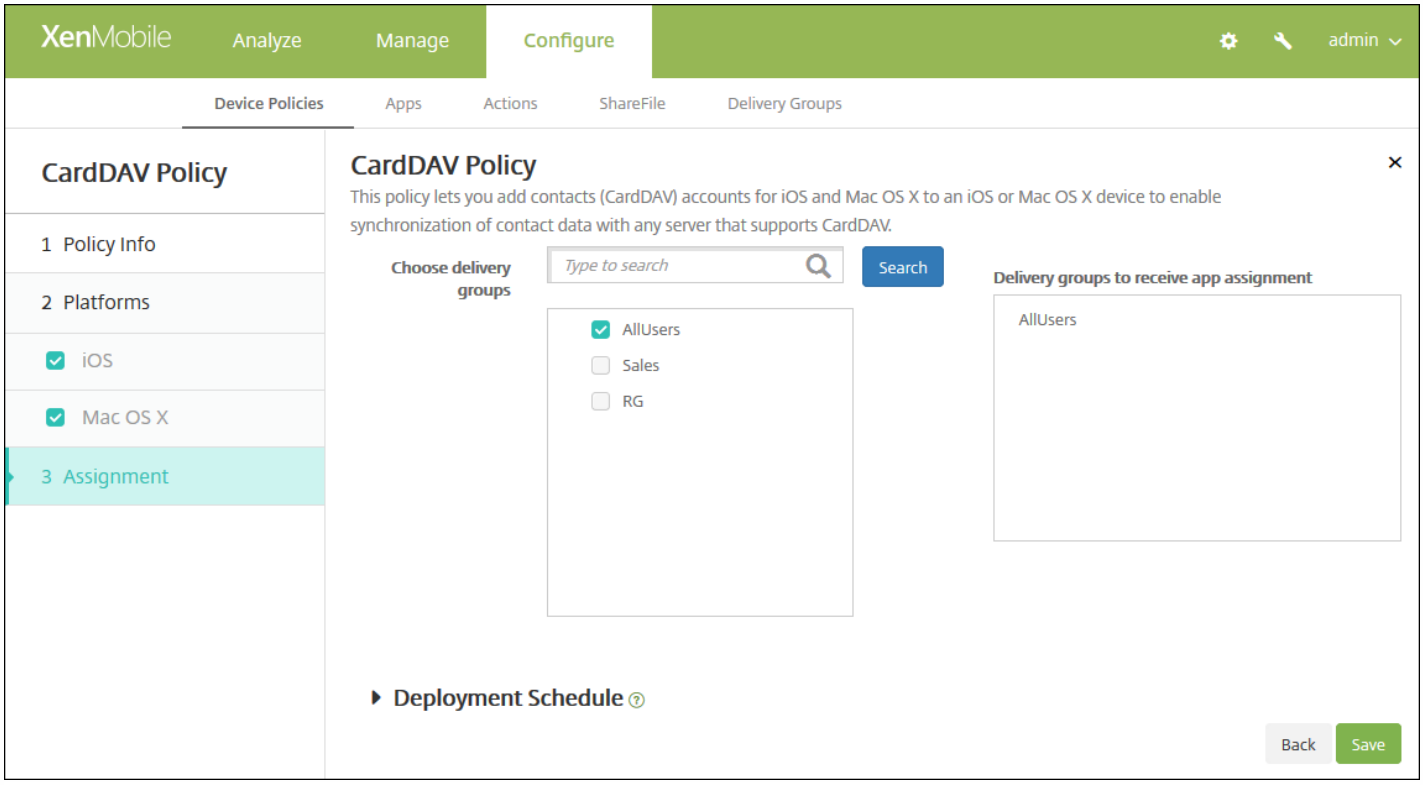
Konfigurieren Sie folgende Einstellungen:

- **Kontobeschreibung**: Geben Sie eine 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. Der Standardwert 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.
  - 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen,

mit Ausnahme von **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

Feb 24, 2017

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 KNOX-Container anmelden.

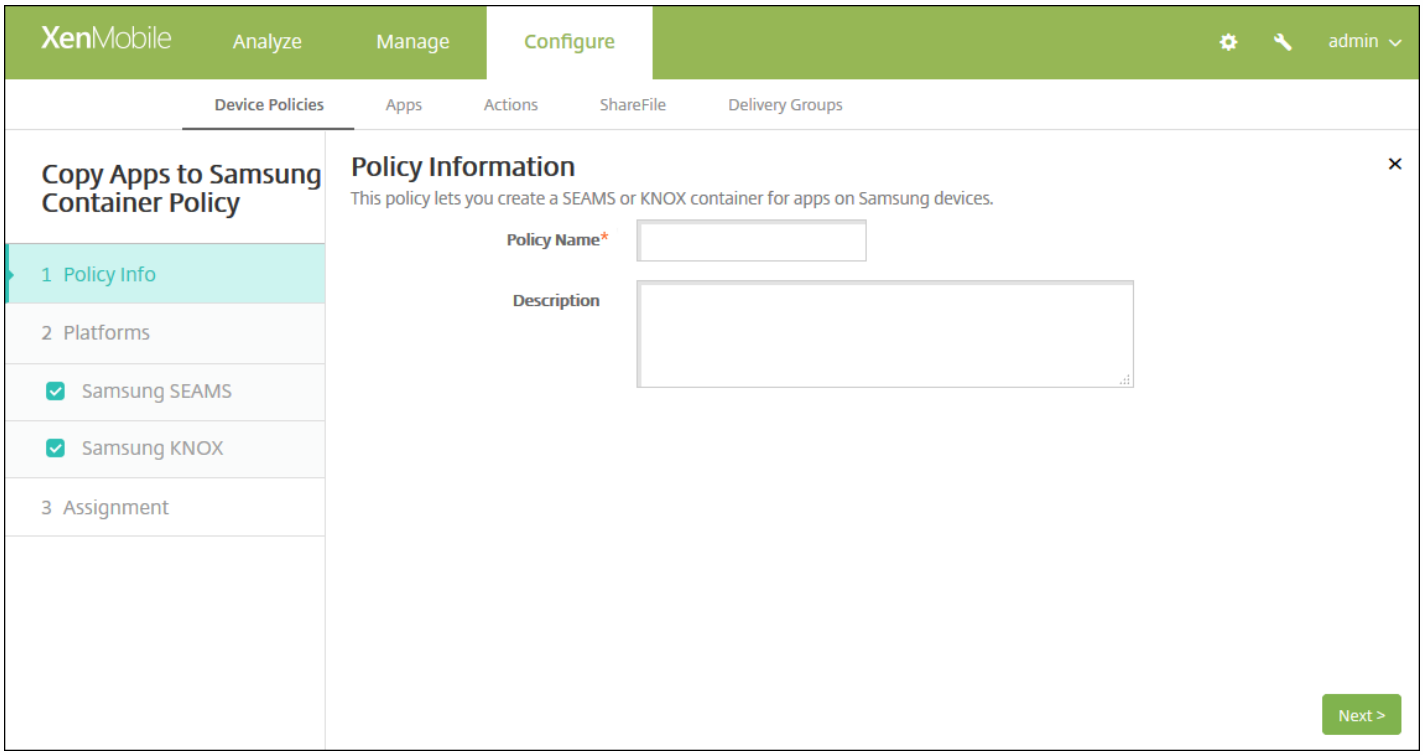
Voraussetzungen:

- 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.

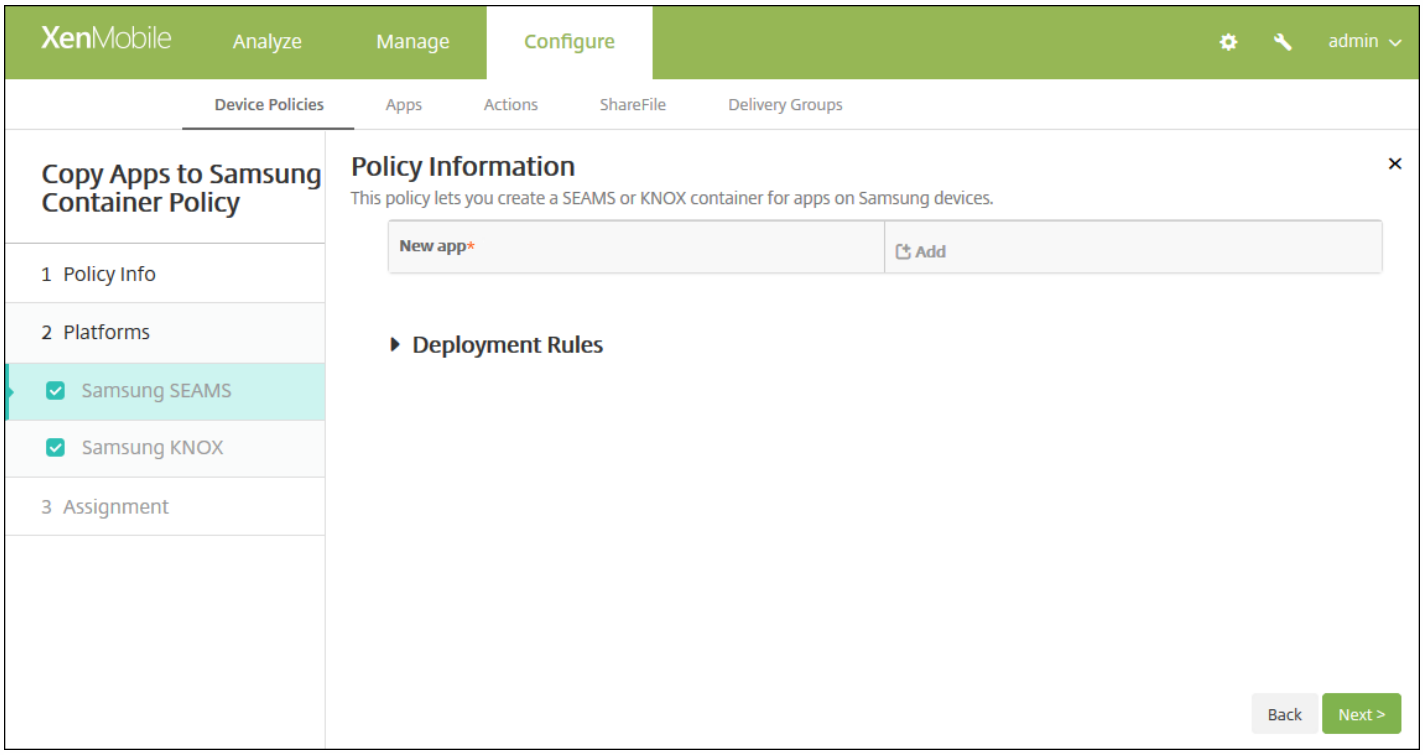
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Apps in Samsung Container kopieren**. Die Seite **Apps in Samsung Container kopieren** wird angezeigt.



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, z. B. "com.mobiwolf.lacingart" für die LacingArt-App.
  - Klicken Sie auf **Speichern** oder **Abbrechen**.

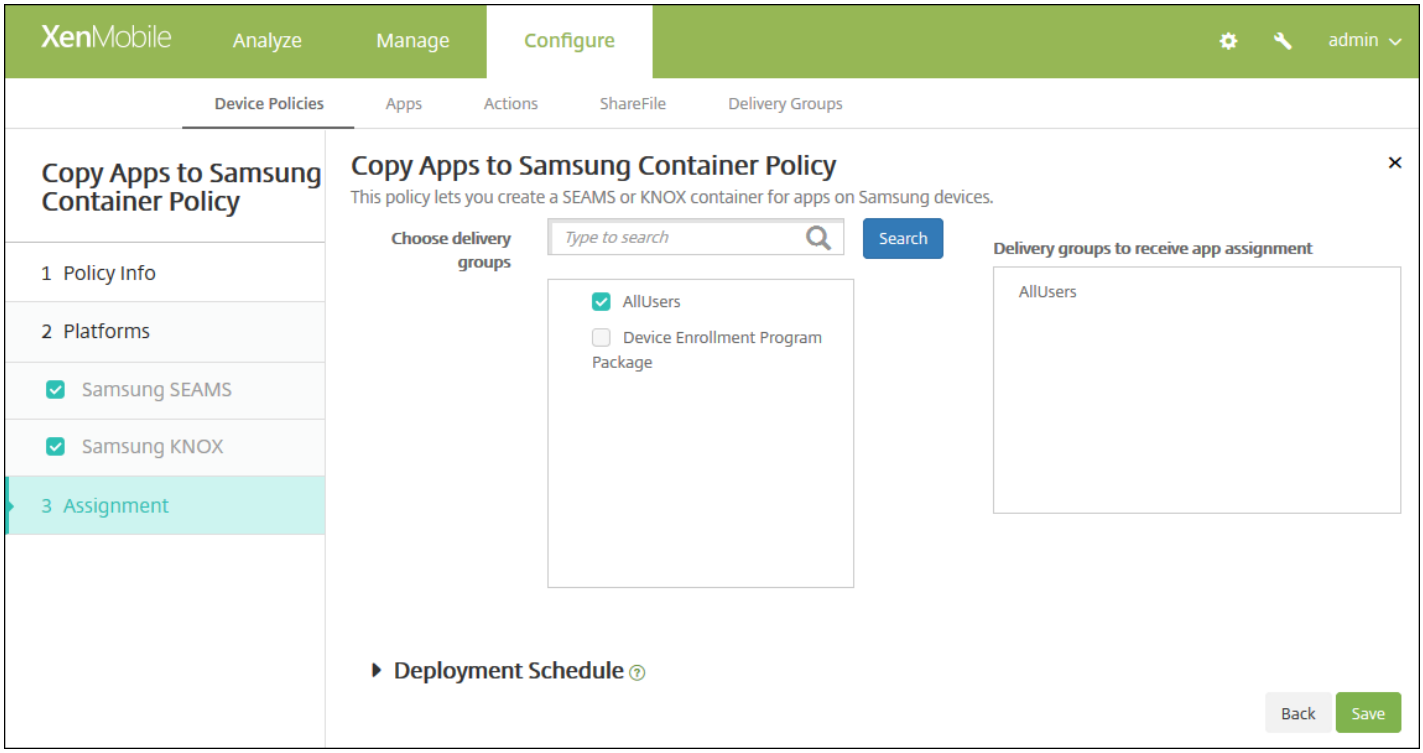
  Hinweis: Zum Löschen einer vorhandenen App zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, um ihn beizubehalten.

  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

9. Klicken Sie auf **Weiter**. Die nächste Plattformseite oder die Zuweisungsseite für **Apps in Samsung Container kopieren**

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 Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von "Bereitstellen für immer aktive Verbindungen", denn diese Option gilt nicht für iOS.

12. 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

Feb 24, 2017

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

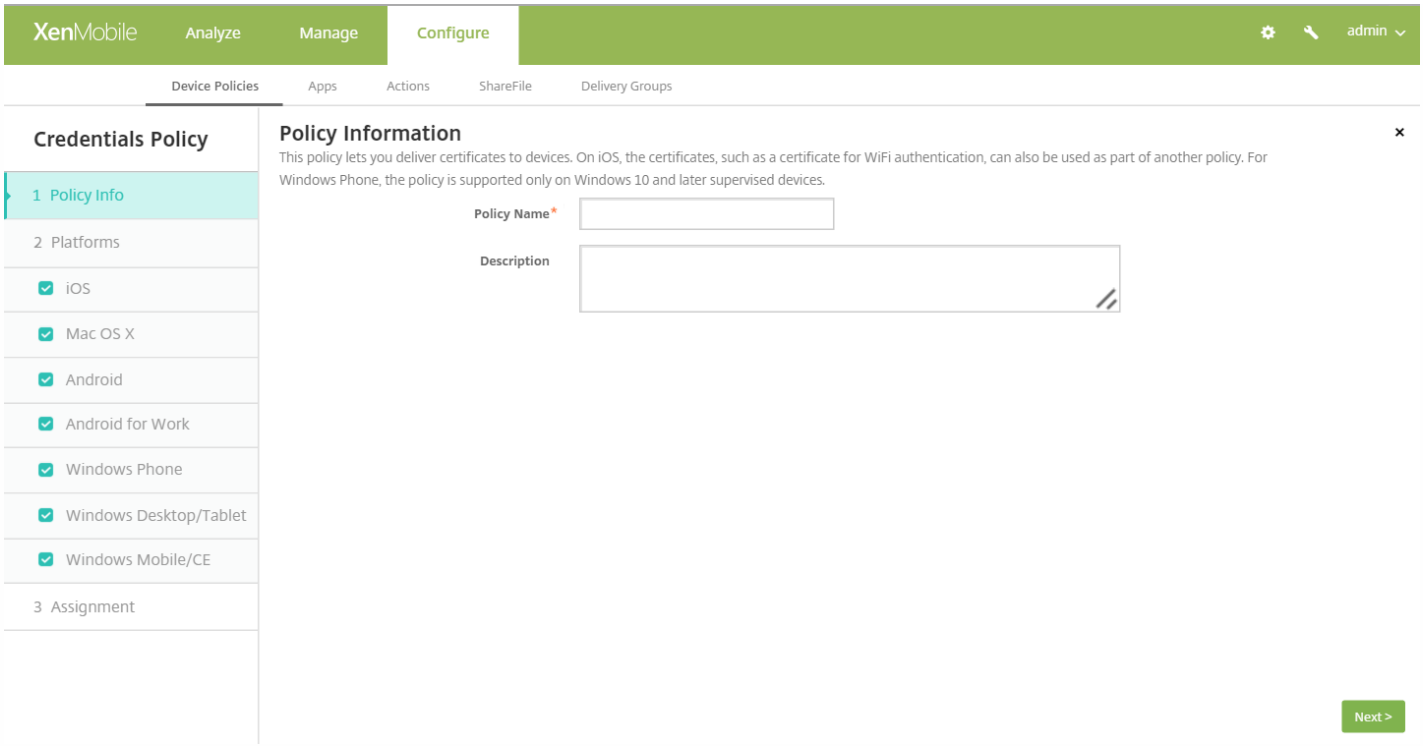
Windows Phone-Einstellungen

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:

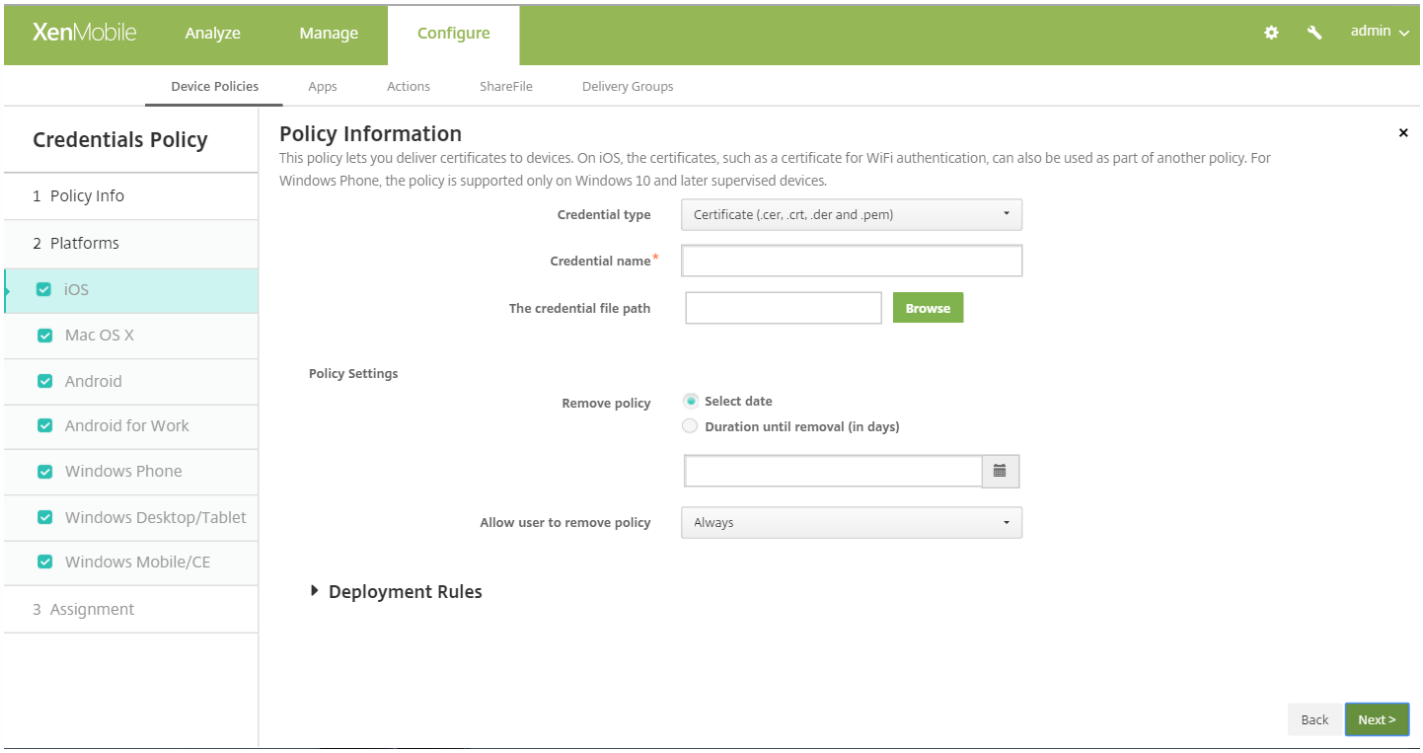
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

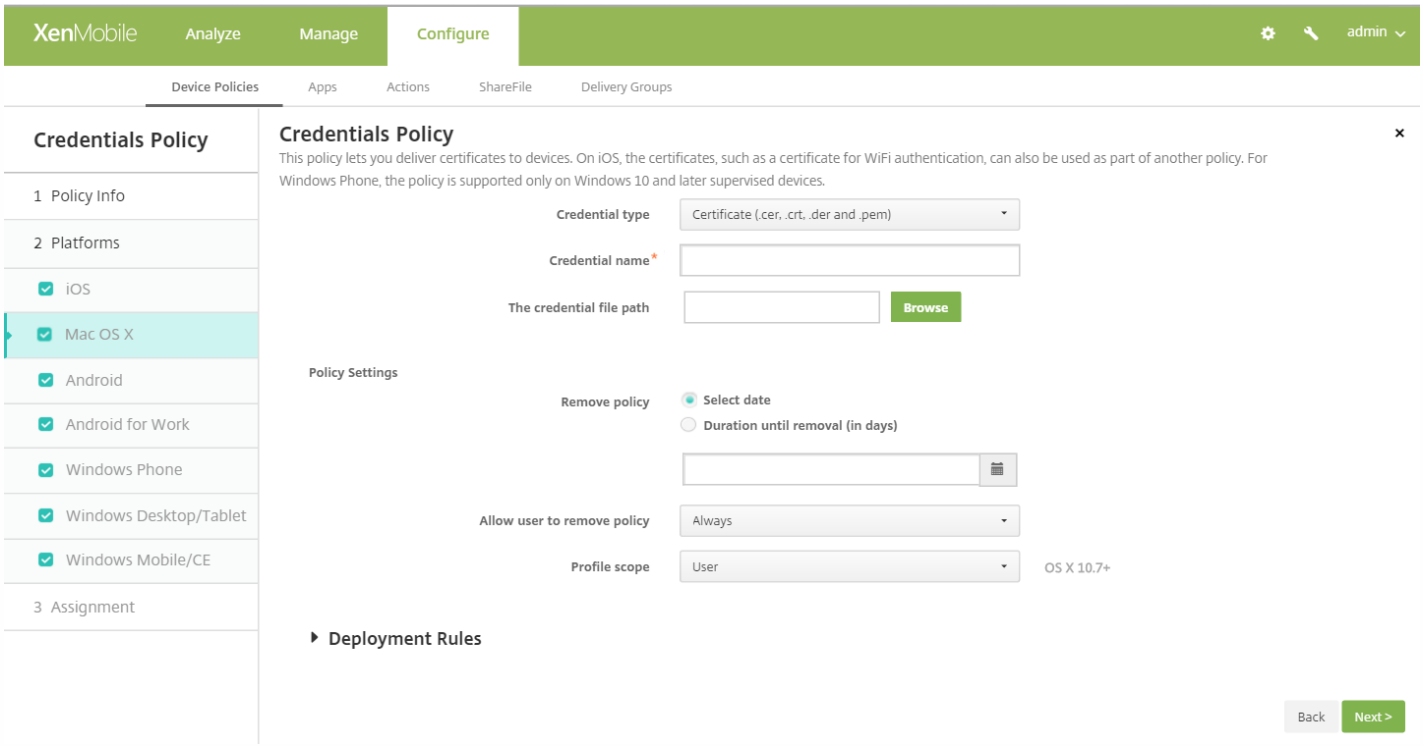
Konfigurieren von iOS-Einstellungen



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 eindeutigen 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 eindeutigen 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**, **Kennwort erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcode erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

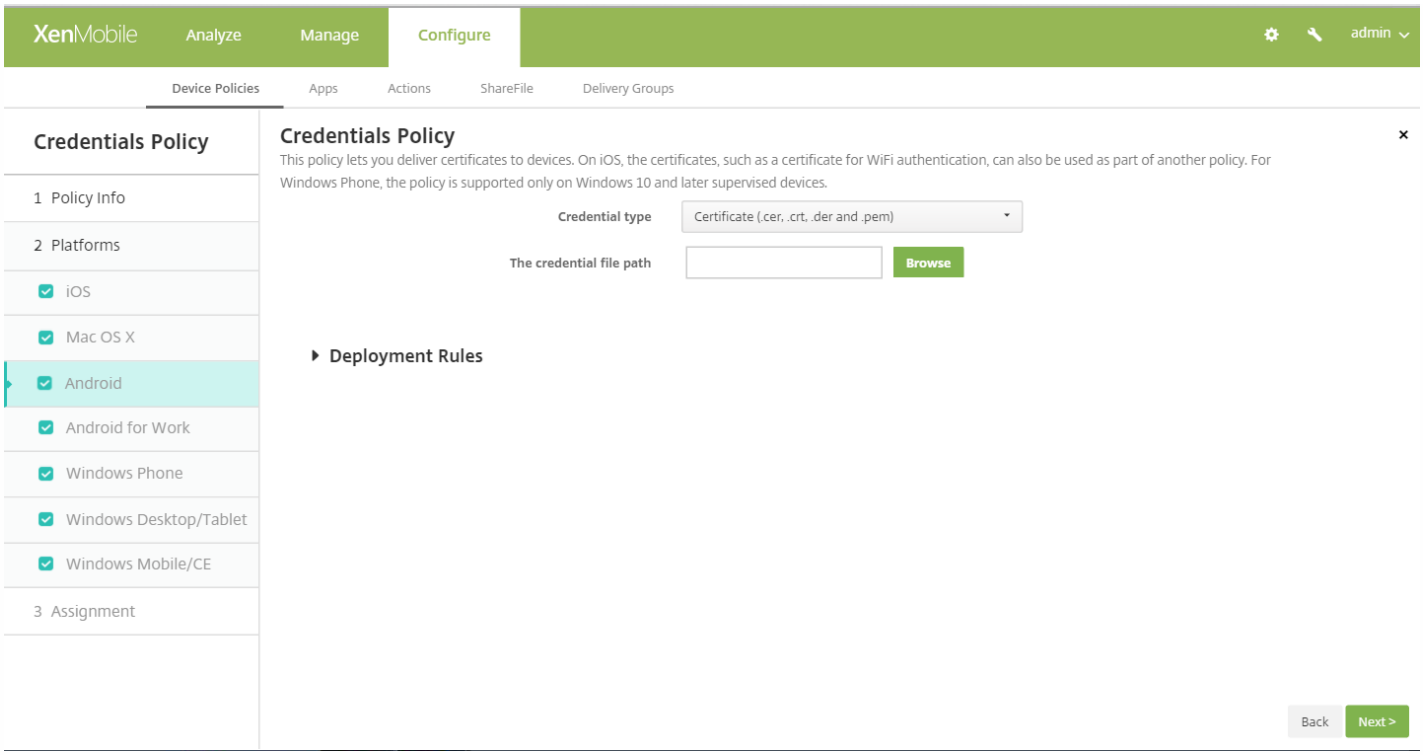
Konfigurieren von Mac OS X-Einstellungen



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 eindeutigen 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 eindeutigen 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**, **Kennwort erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcode 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.

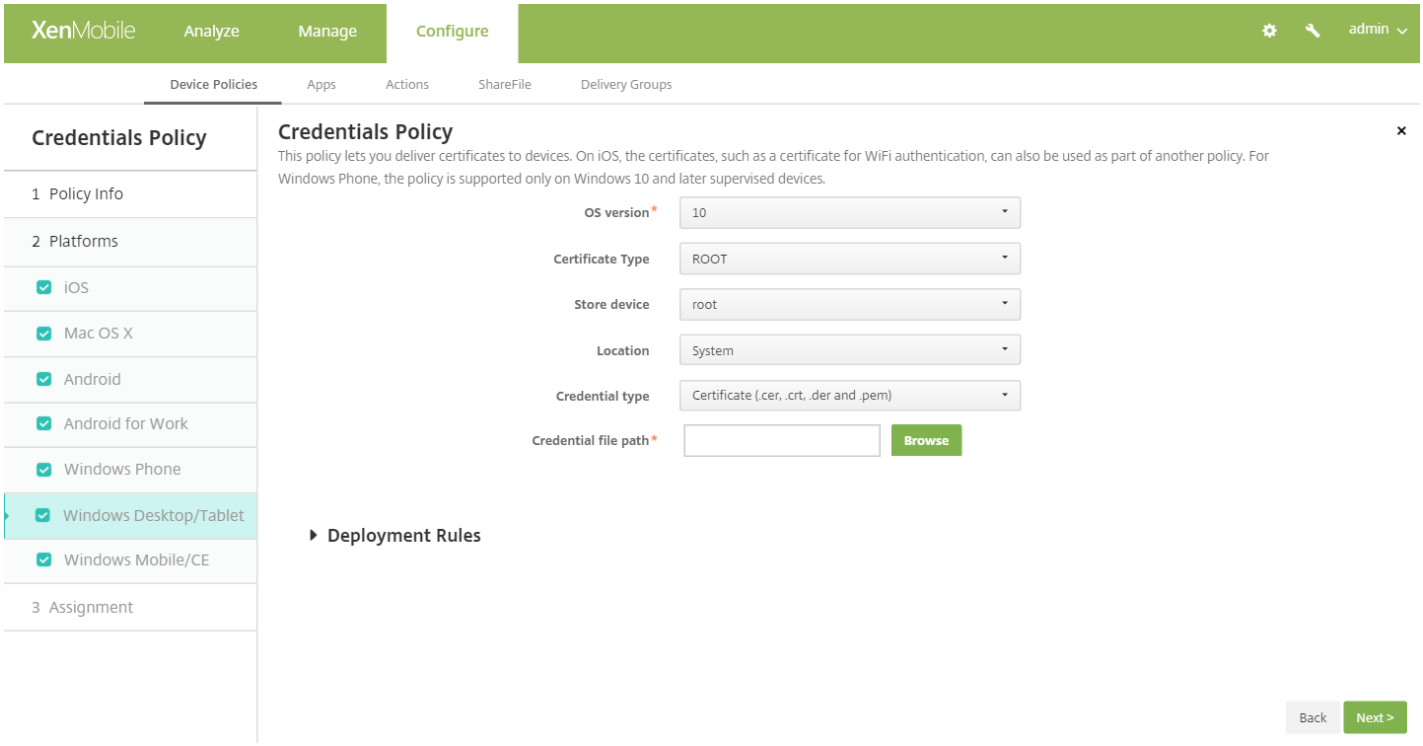
Konfigurieren von Android- und Android for Work-Einstellungen



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



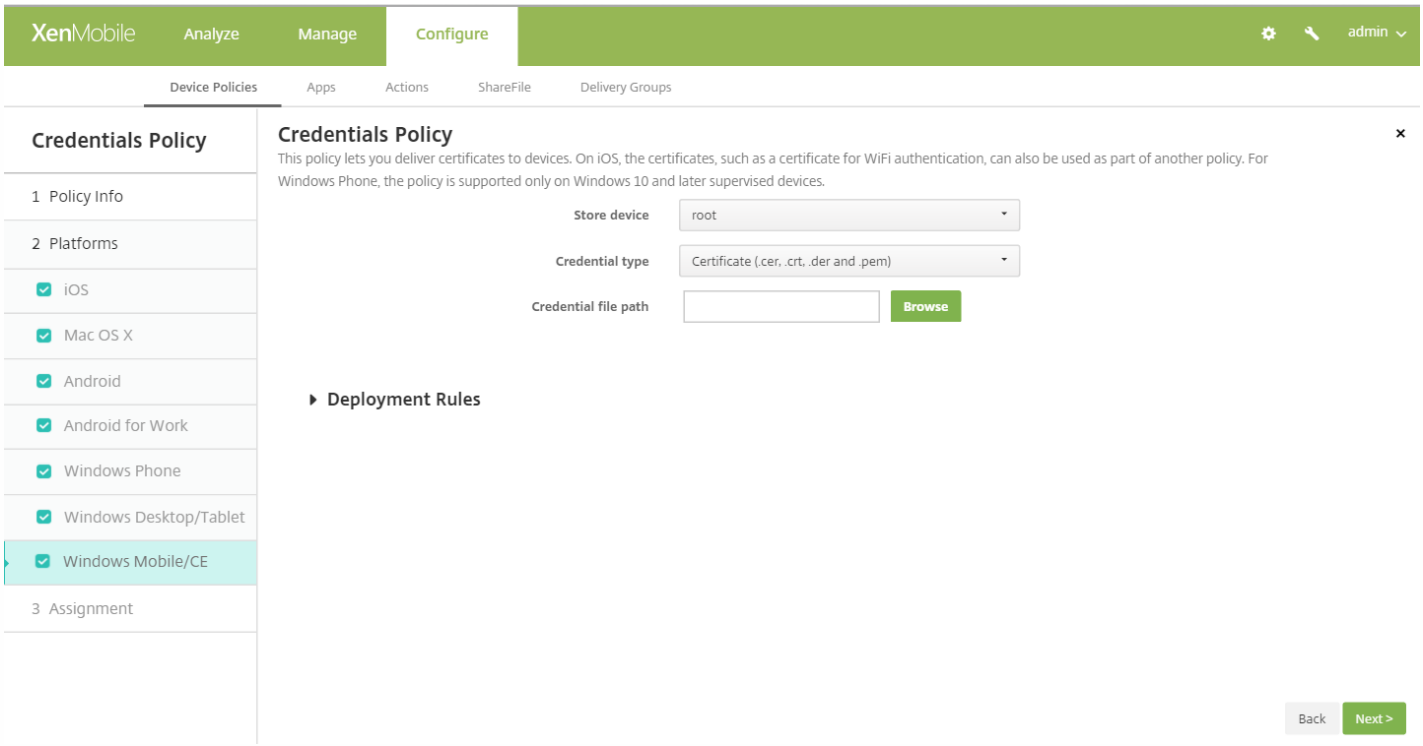
Konfigurieren Sie die folgenden Einstellungen:

- **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

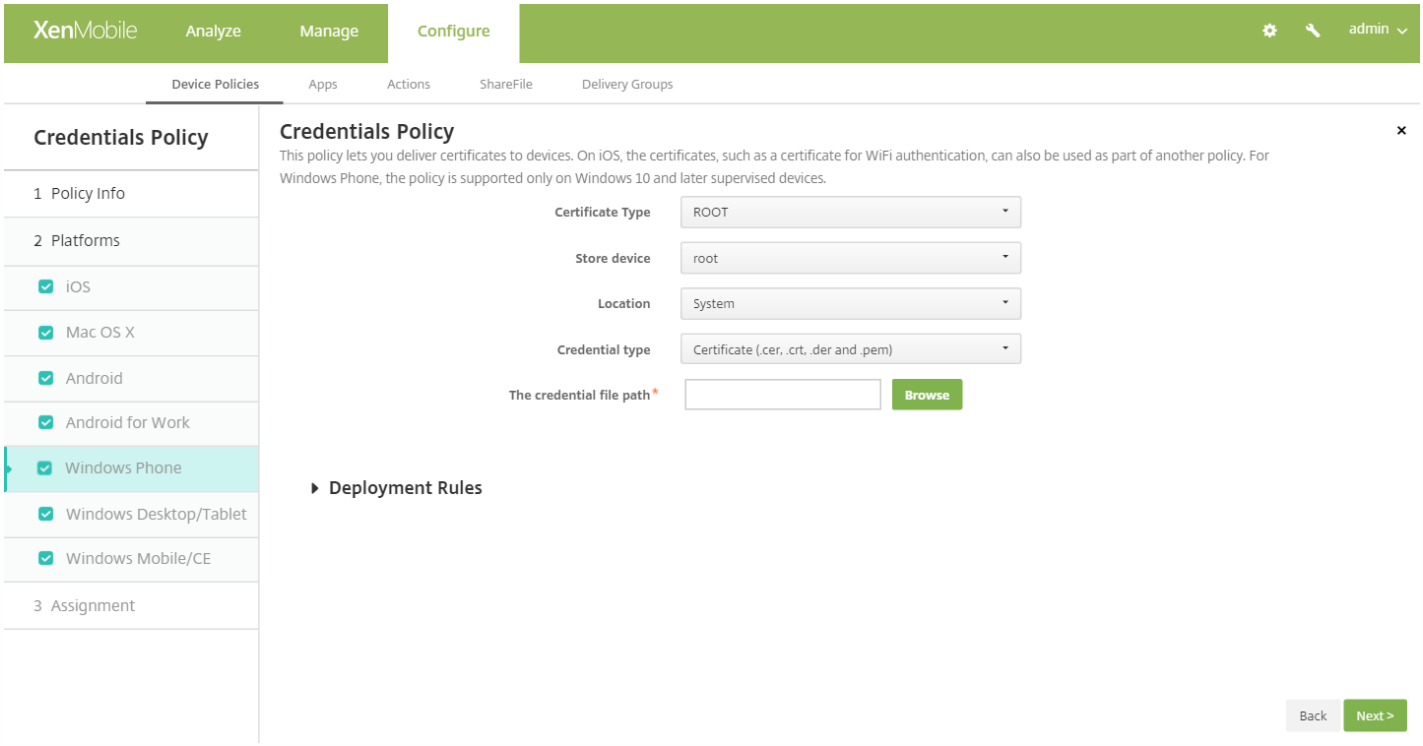
Konfigurieren von Windows Mobile-/CE-Einstellungen



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 mit Stamm- oder selbstsignierten Zertifikaten.
  - **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

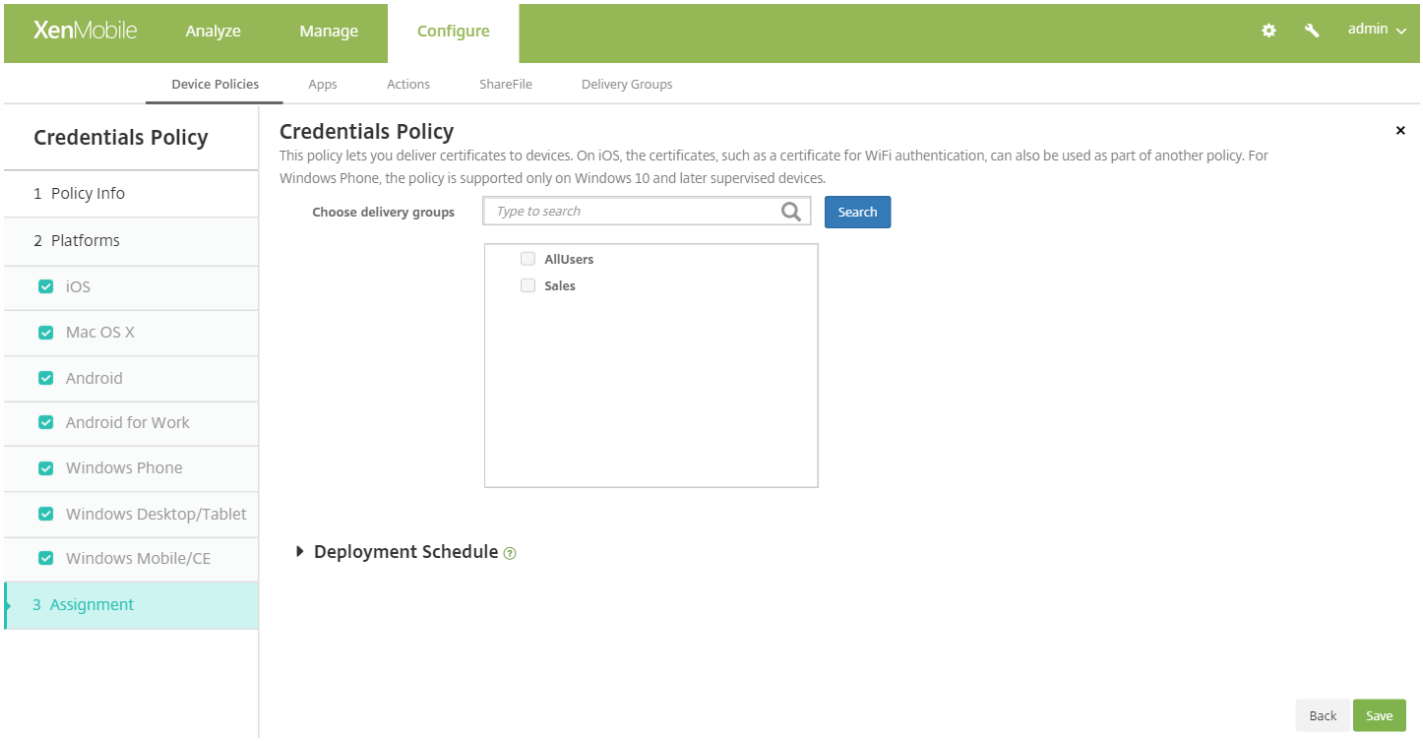


Konfigurieren Sie die folgenden Einstellungen:

- **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 Zertifikatdatei, 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 Zertifikatdatei, 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Benutzerdefinierte XML-Richtlinien für Geräte

Feb 24, 2017

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:

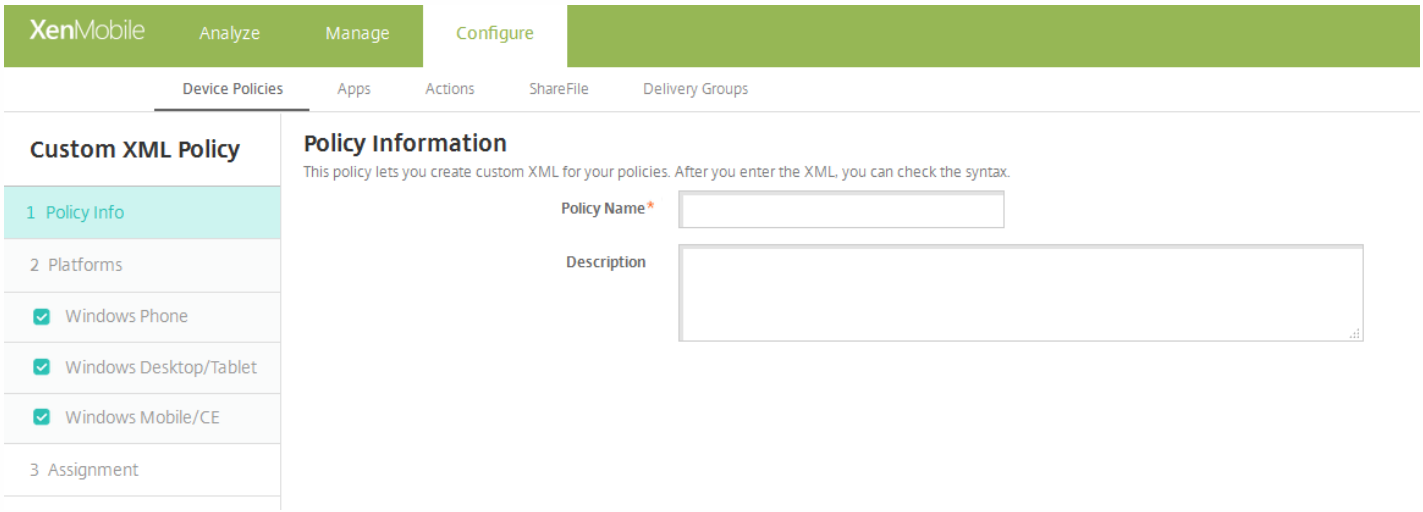
- Provisioning, d. h. Konfiguration des Geräts und Aktivieren bzw. Deaktivieren von Features
- Gerätekonfiguration, einschließlich des Zulassens der Änderung von Einstellungen und Geräteparametern durch die Benutzer
- Softwareupgrades, d. h. Bereitstellung neuer Software oder von Fehlerbehebungen für 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. Weitere Informationen zur Verwendung der OMA DM-API finden Sie auf Microsoft Developer Network unter OMA Device Management.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

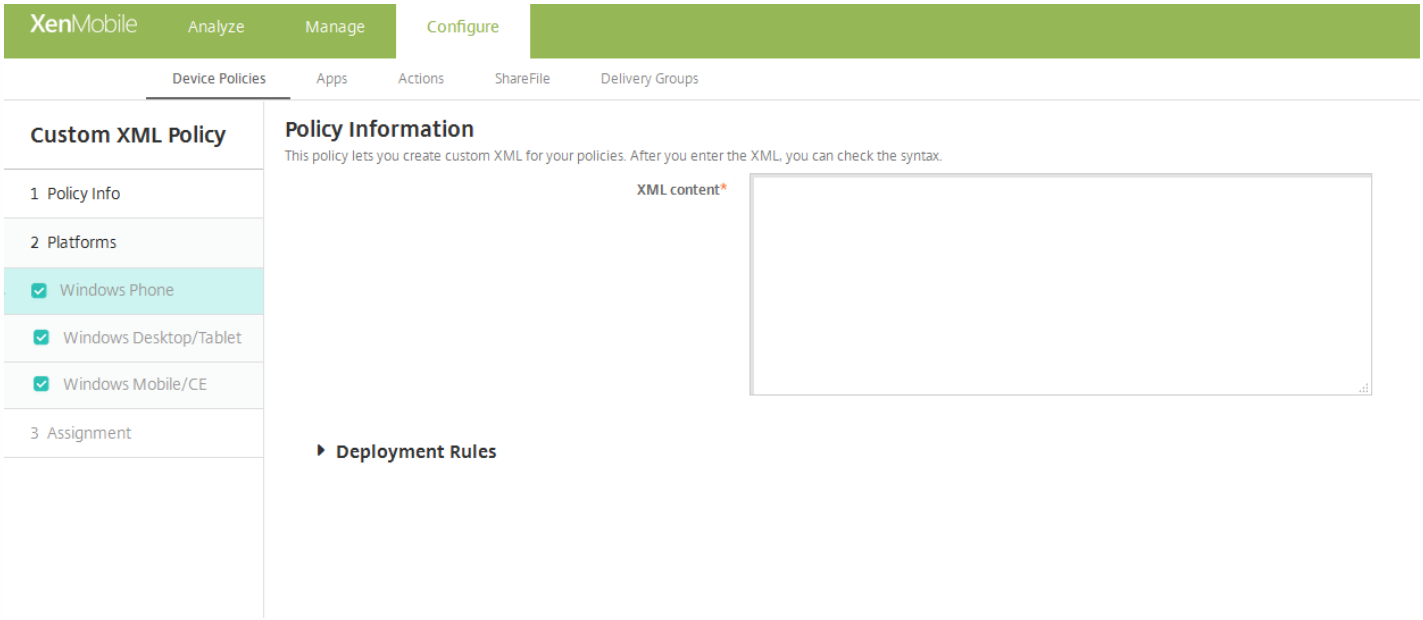
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Benutzerdefiniert** auf **Benutzerdefiniertes XML**. Die Seite für die Richtlinieninformationen der Richtlinie **Benutzerdefiniertes XML** wird angezeigt.



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

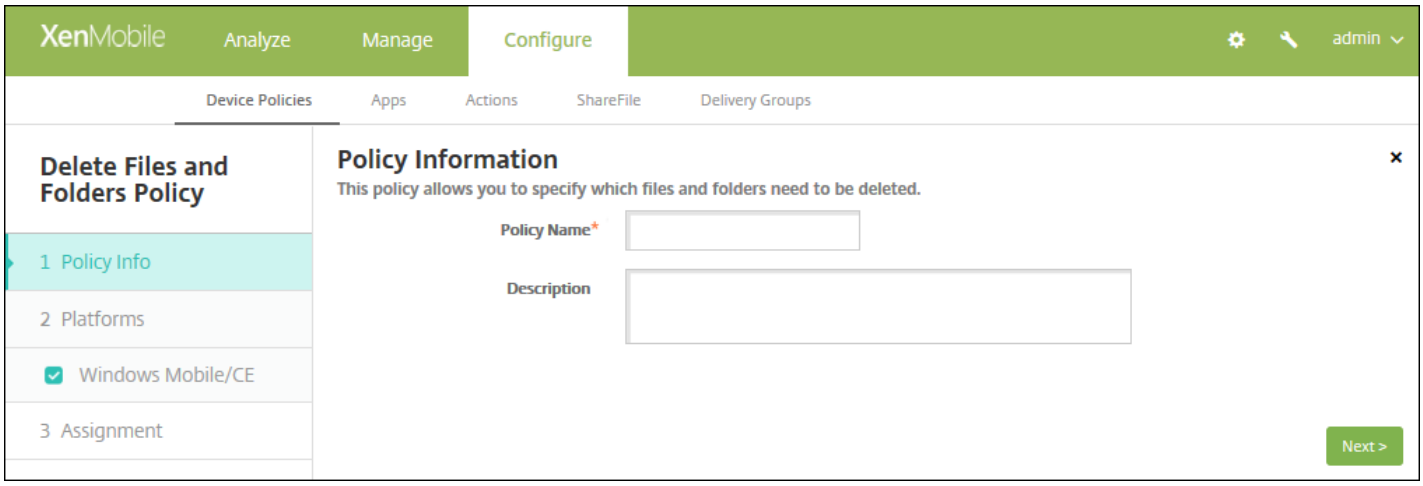
Feb 24, 2017

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.

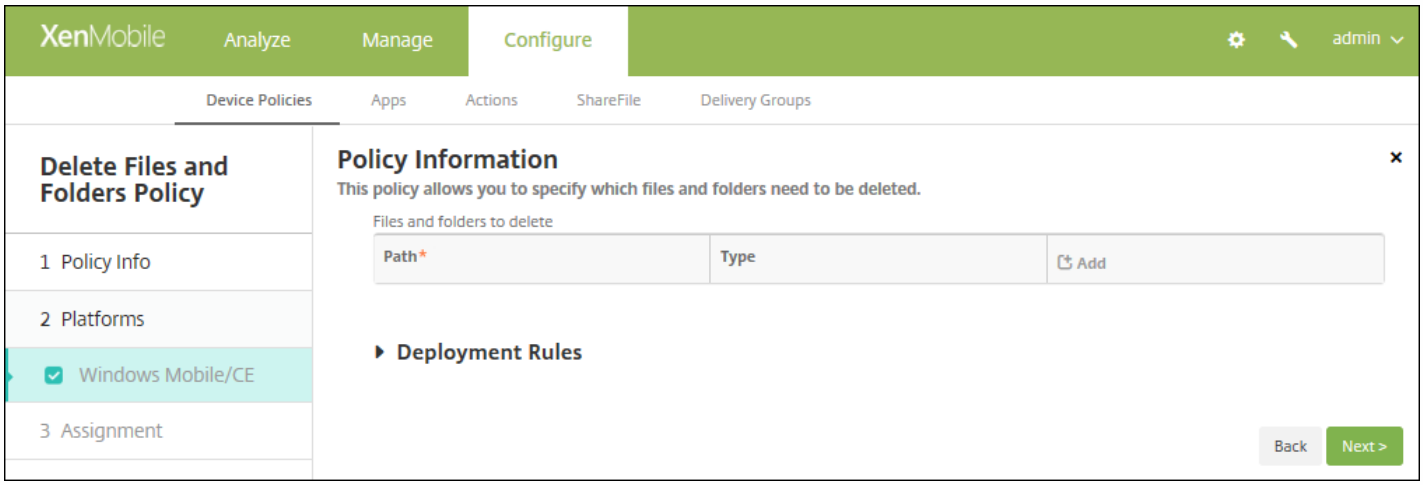
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Dateien und Ordner löschen**. Die Informationsseite für die Richtlinie wird angezeigt.



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:

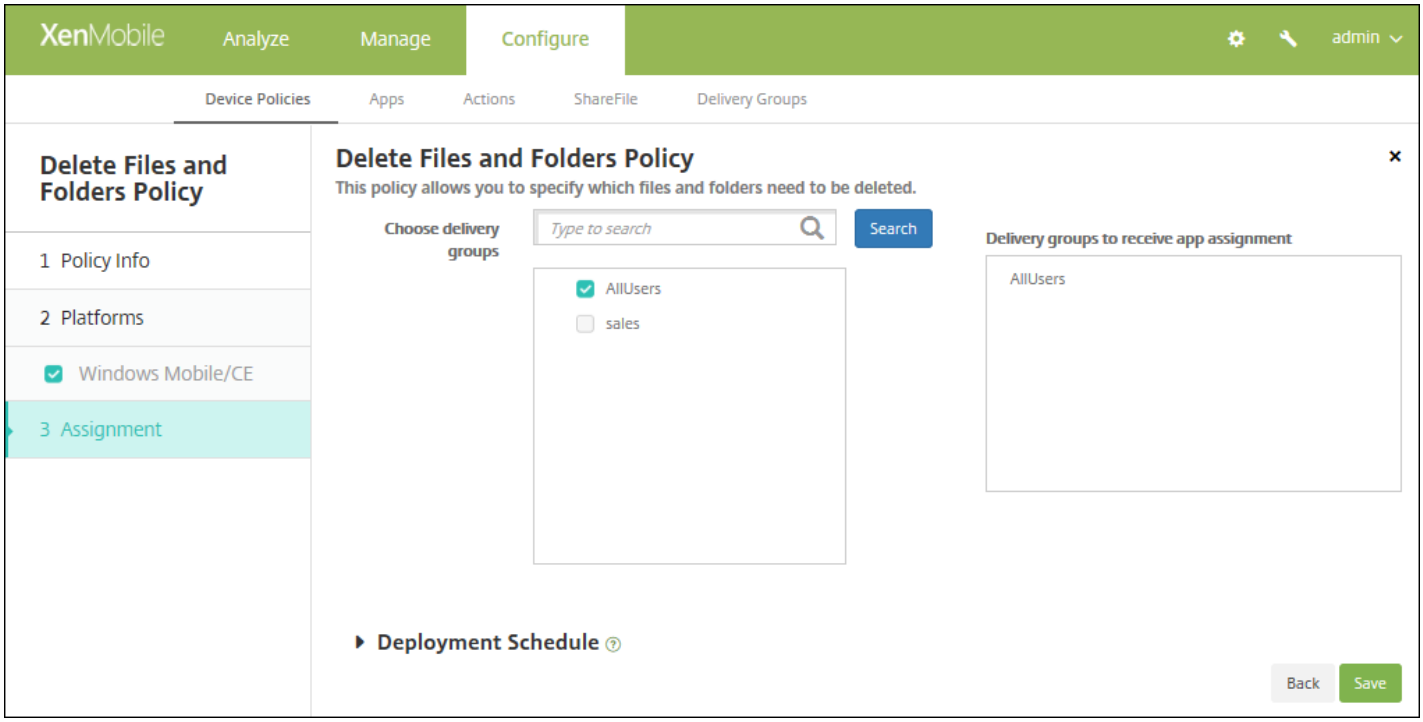
- **Folgende Dateien und Ordner löschen**: Klicken Sie für jedes Element, das gelöscht werden soll, auf "Hinzufügen" und führen Sie folgende Schritte aus:
  - **Pfad**: Geben Sie den Pfad zu der Datei bzw. dem Ordner ein.
  - **Typ**: Klicken Sie in der Liste auf "Datei" oder "Ordner". Die Standardeinstellung 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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie zum Löschen von Registrierungsschlüssel und -werten

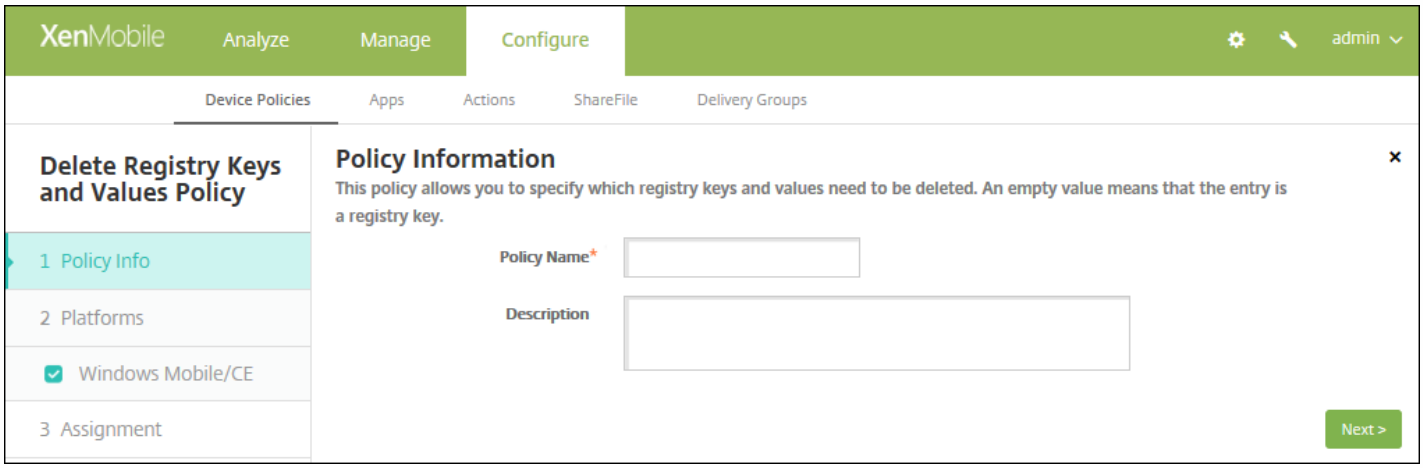
Feb 24, 2017

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.

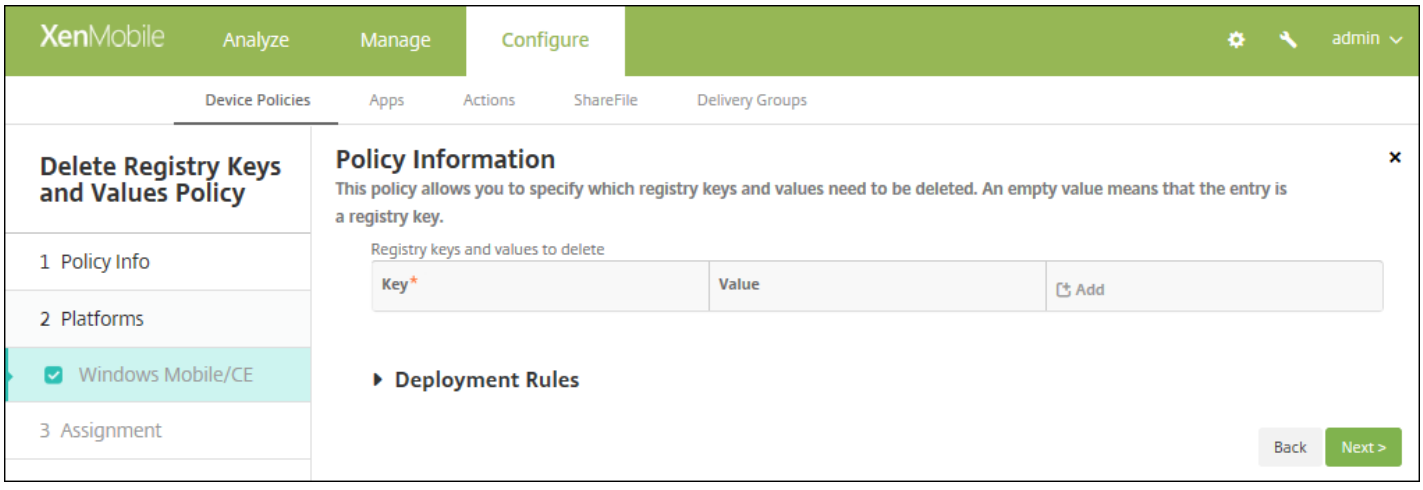
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Registrierungsschlüssel und -werte löschen**. Die Seite **Registrierungsschlüssel und -werte löschen** wird angezeigt.



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:

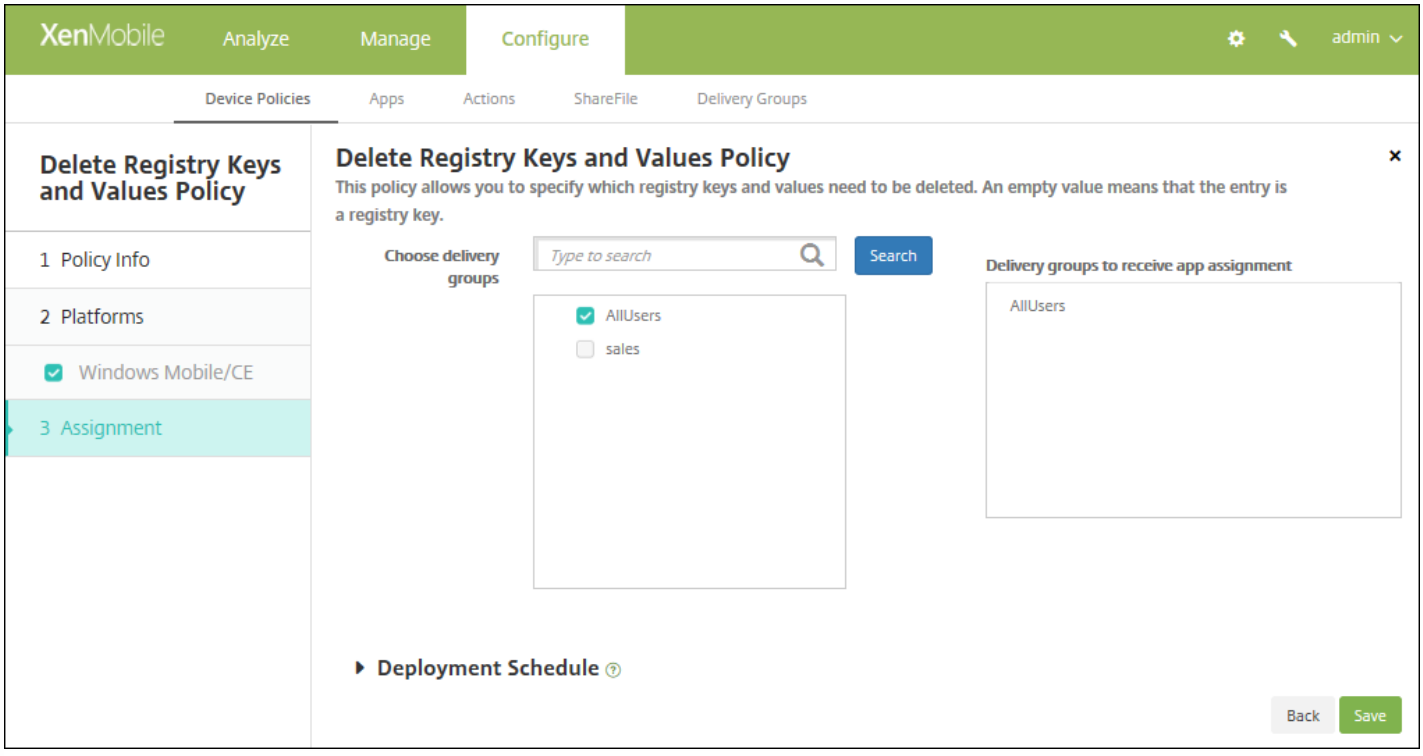
- **Folgende Registrierungsschlüssel und -werte löschen**: Klicken Sie für jeden Registrierungsschlüssel/-wert, der gelöscht werden soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Schlüssel**: Geben Sie den Pfad des Registrierungsschlüssels ein. Diese Angabe ist obligatorisch. Der 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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Integritätsnachweisrichtlinie für Geräte

Feb 24, 2017

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:

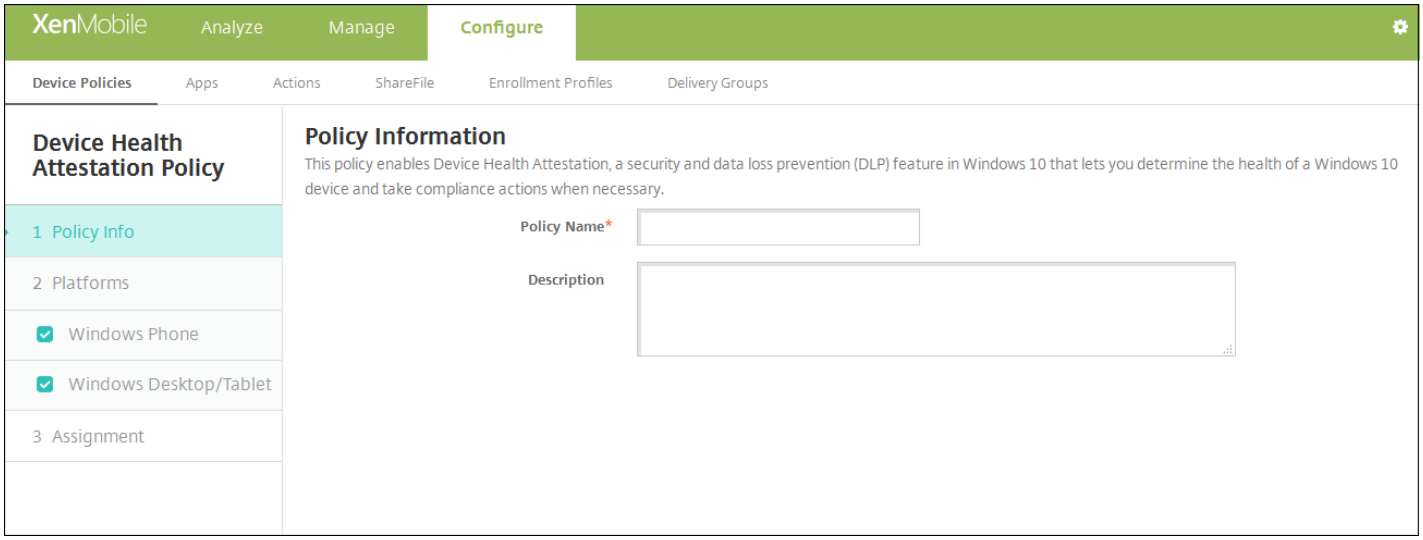
- AIK Present?
- Bit Locker Status
- Boot Debugging Enabled?
- Boot Manager Rev List Version
- Code Integrity Enabled?
- Code Integrity Rev List Version
- DEP Policy
- ELAM Driver Loaded?
- Issued At
- Kernel Debugging Enabled?
- PCR
- Reset Count
- Restart Count
- Safe Mode Enabled?
- SBCP Hash
- Secure 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.



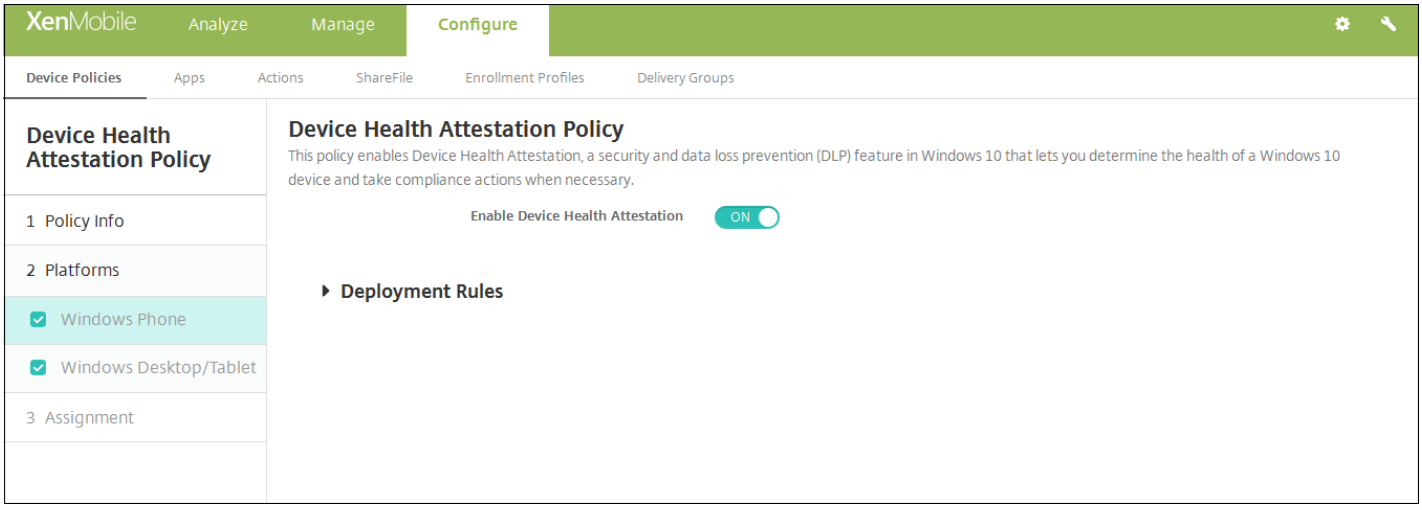
4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

- **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.

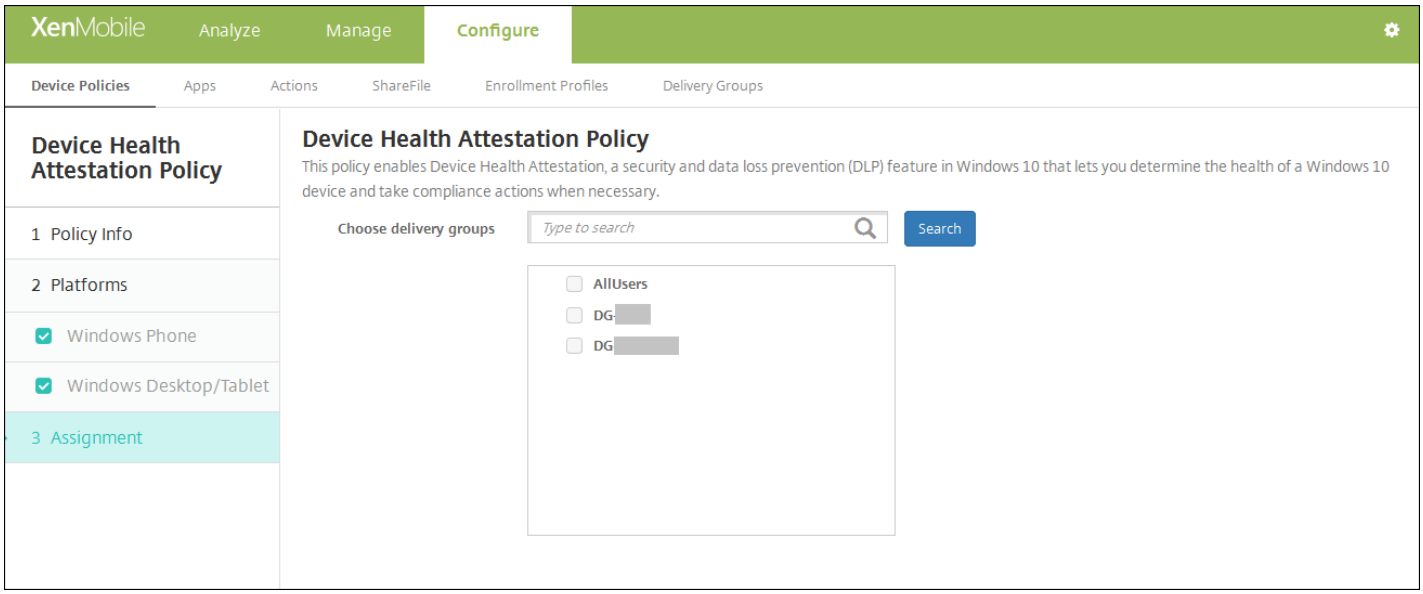


Konfigurieren Sie diese Einstellung für jede ausgewählte Plattform:

- **Integritätsnachweisrichtlinie für Windows-Geräte**: 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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Richtlinien für Gerätenamen

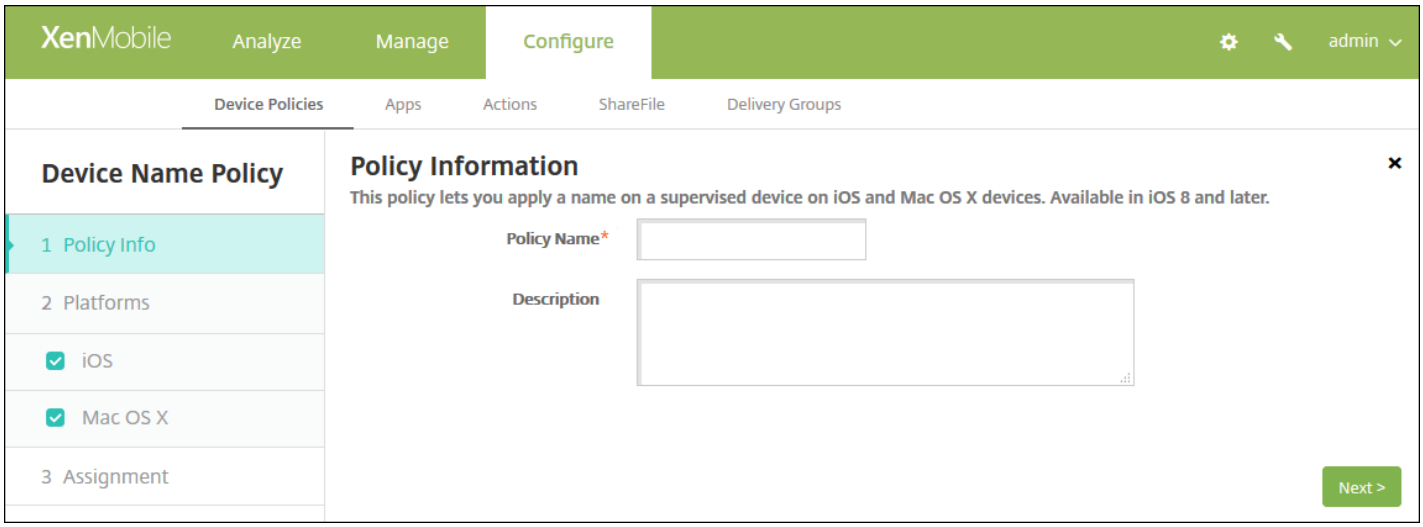
Feb 24, 2017

Sie können 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. 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:

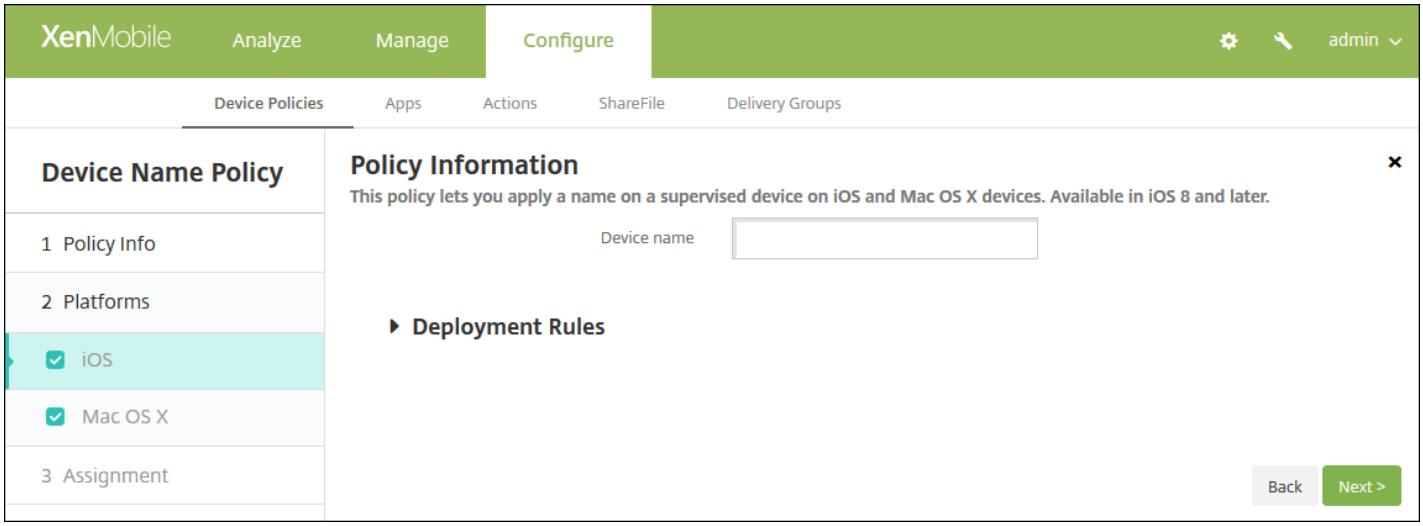
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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

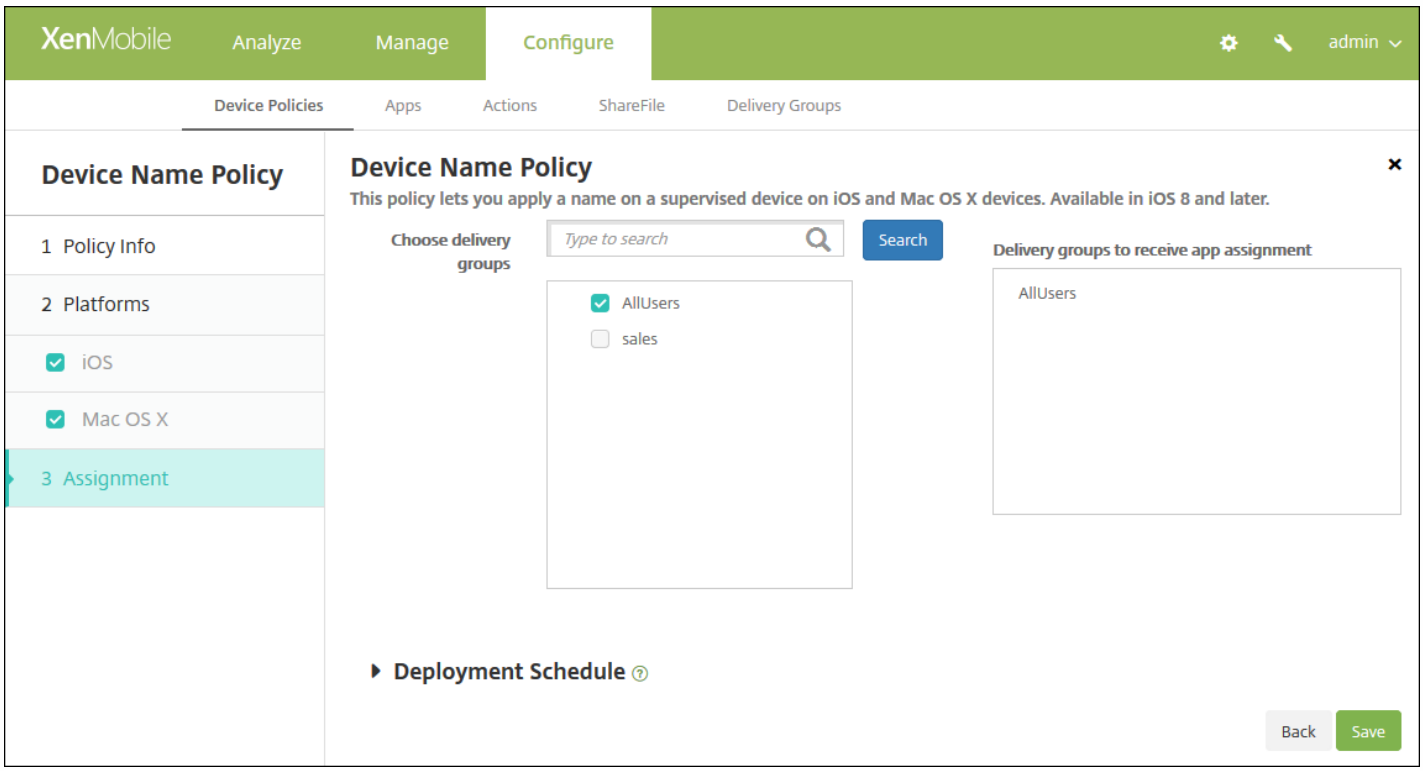


Konfigurieren Sie folgende Einstellung für die ausgewählten Plattformen:

- **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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Unternehmenshub

Feb 24, 2017

Mit einer Unternehmenshub-Geräterichtlinie für Windows Phone können Sie Apps über den Unternehmenshub-Unternehmensstore an Geräte verteilen.

Zum Erstellen der Richtlinie benötigen Sie Folgendes:

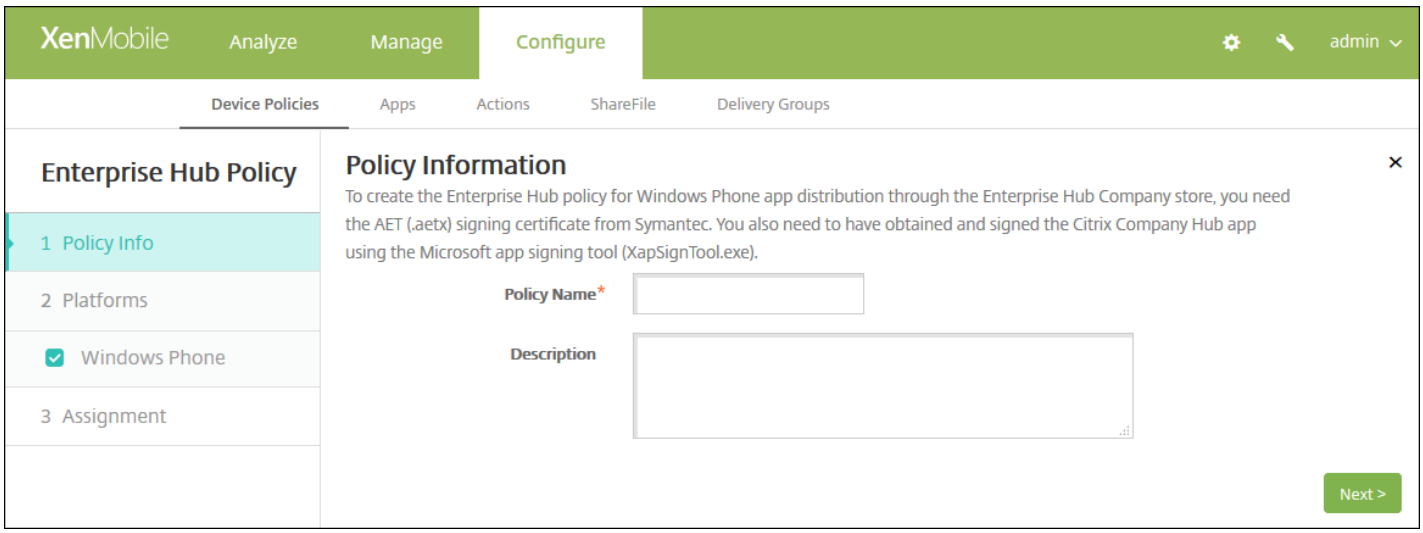
- Ein AET-Signaturzertifikat (.aetx) von Symantec
- Die mit dem Microsoft App-Signierungstool (XapSignTool.exe) signierte Citrix Company Hub-App

Hinweis: XenMobile unterstützt nur eine Unternehmenshubrichtlinie für einen Modus von Windows Phone-Secure Hub. Zum Hochladen von Secure Hub für Windows Phone für XenMobile Enterprise Edition dürfen Sie beispielsweise nicht mehrere Unternehmenshubrichtlinien mit mehreren Versionen von Secure Hub für XenMobile Enterprise Edition erstellen. Sie können nur die erste Unternehmenshubrichtlinie 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.

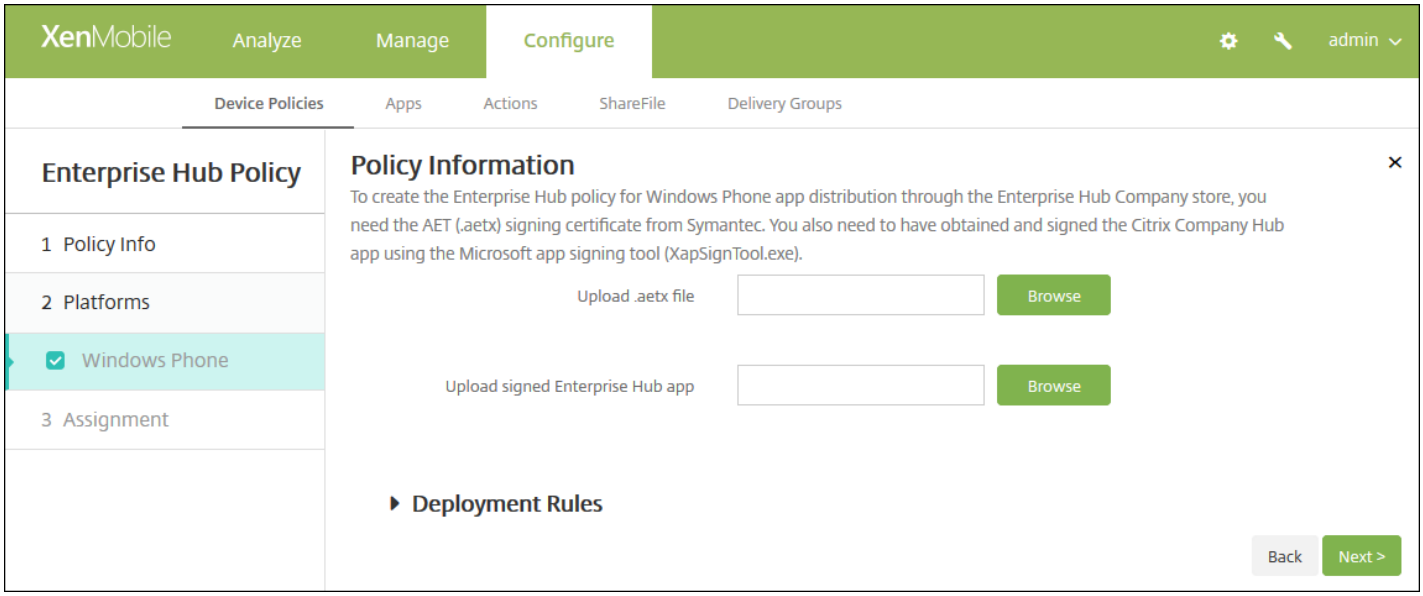
3. Erweitern Sie **Mehr** und klicken Sie dann unter **XenMobile-Agent** auf **Unternehmenshub**. Die Seite **Unternehmenshub** wird angezeigt.



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.

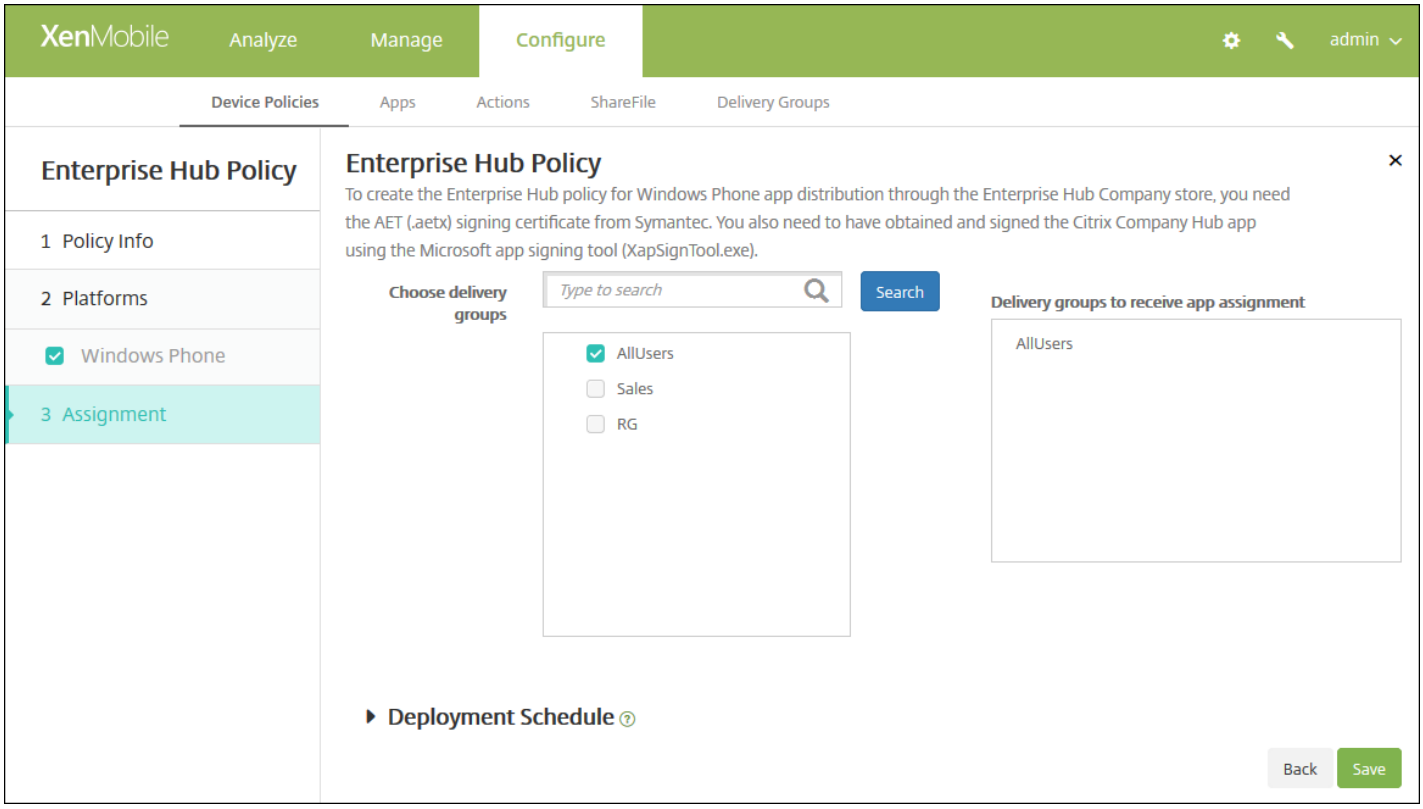


6. Konfigurieren Sie die folgenden Einstellungen:

- **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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Dateirichtlinien

Feb 24, 2017

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.

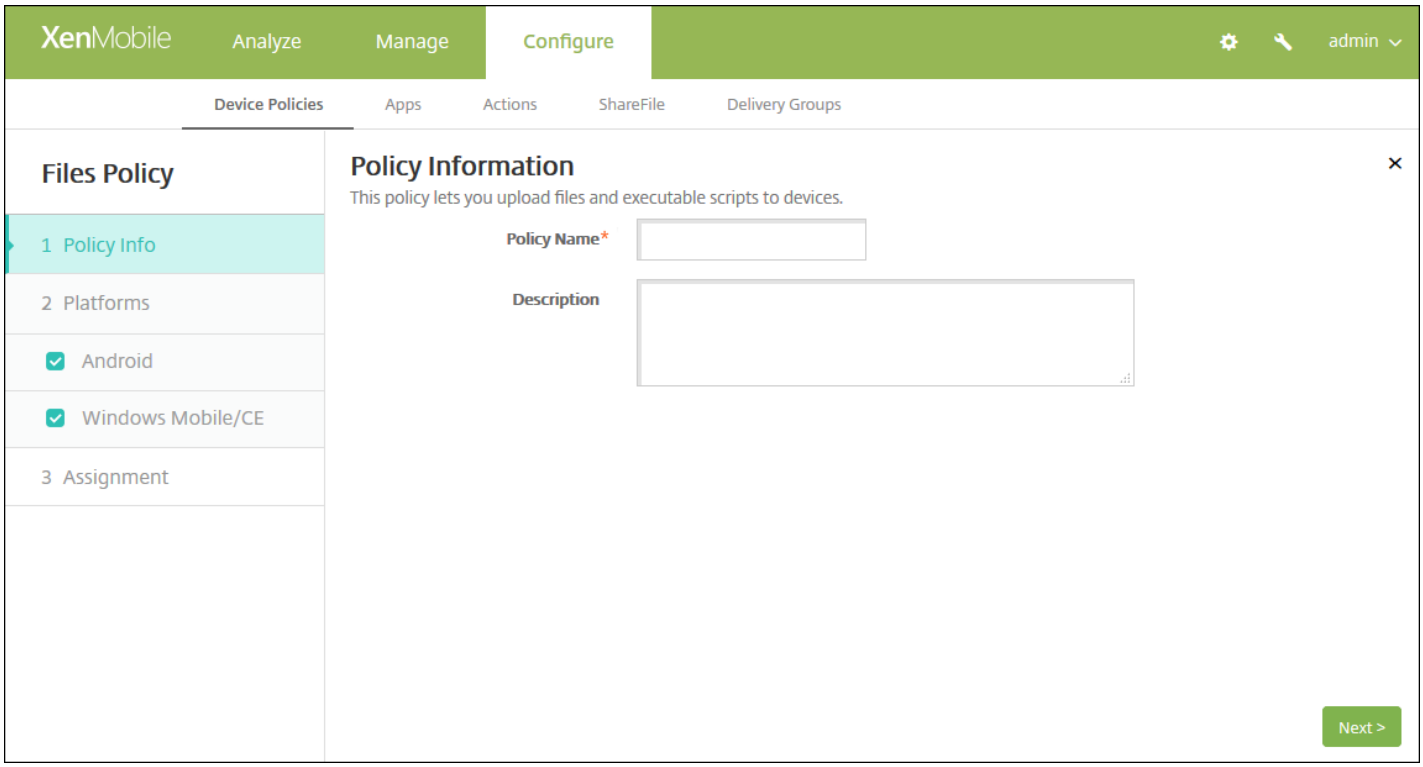
Sie können mit dieser Richtlinie die folgenden Dateitypen hinzufügen:

- 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.

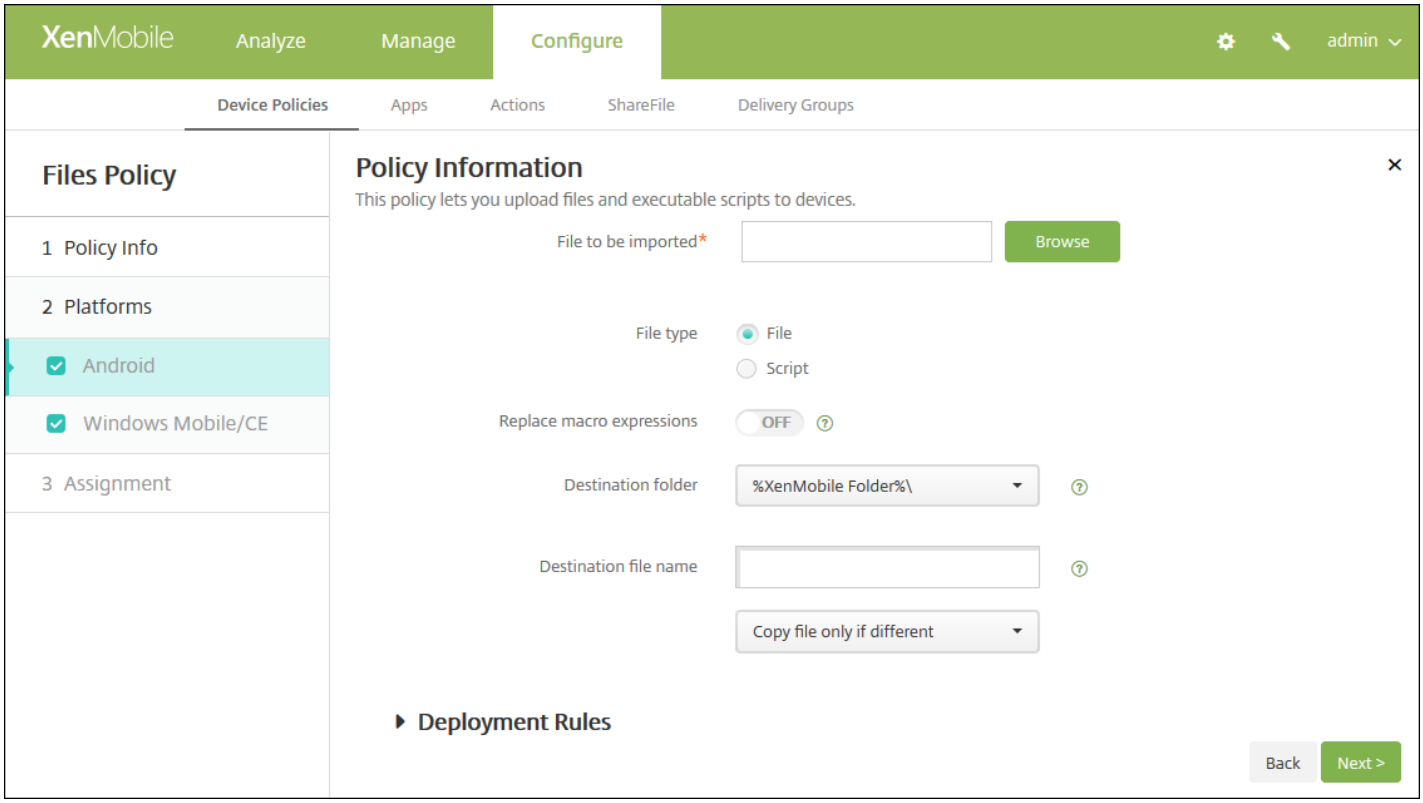
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Dateien**. Die Informationsseite **Dateien** wird angezeigt.



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.

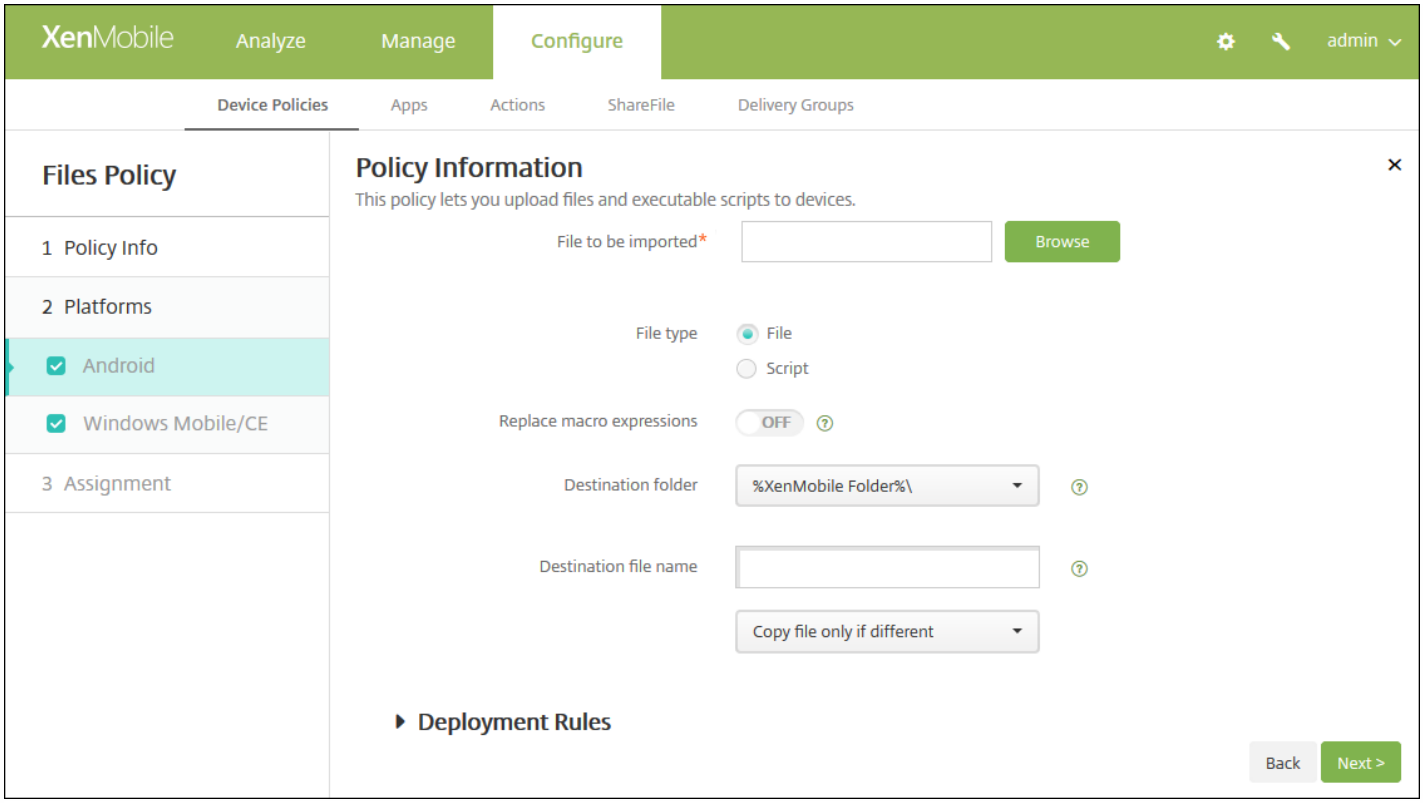
5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



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.

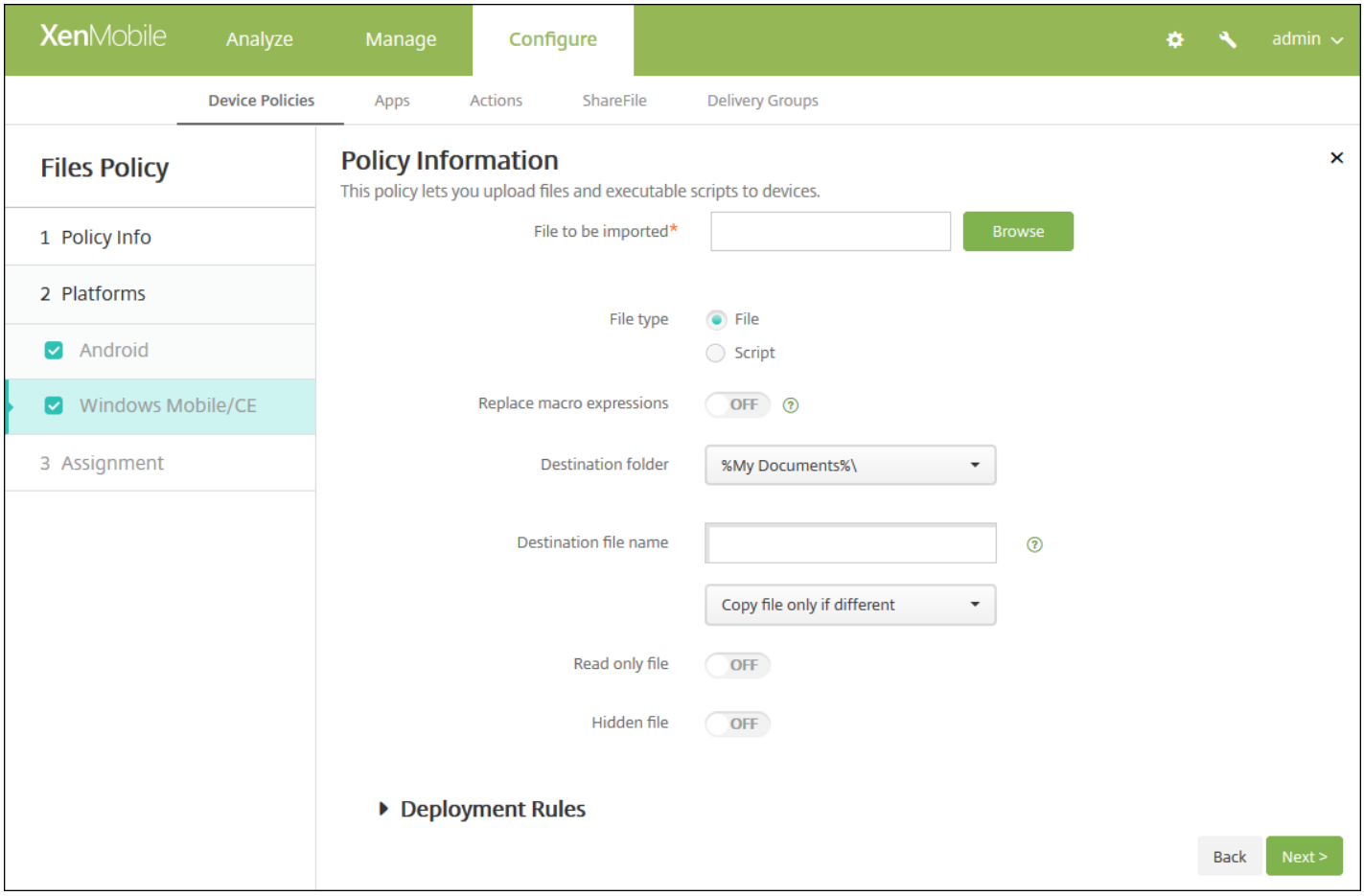
Konfigurieren von Android-Einstellungen



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.

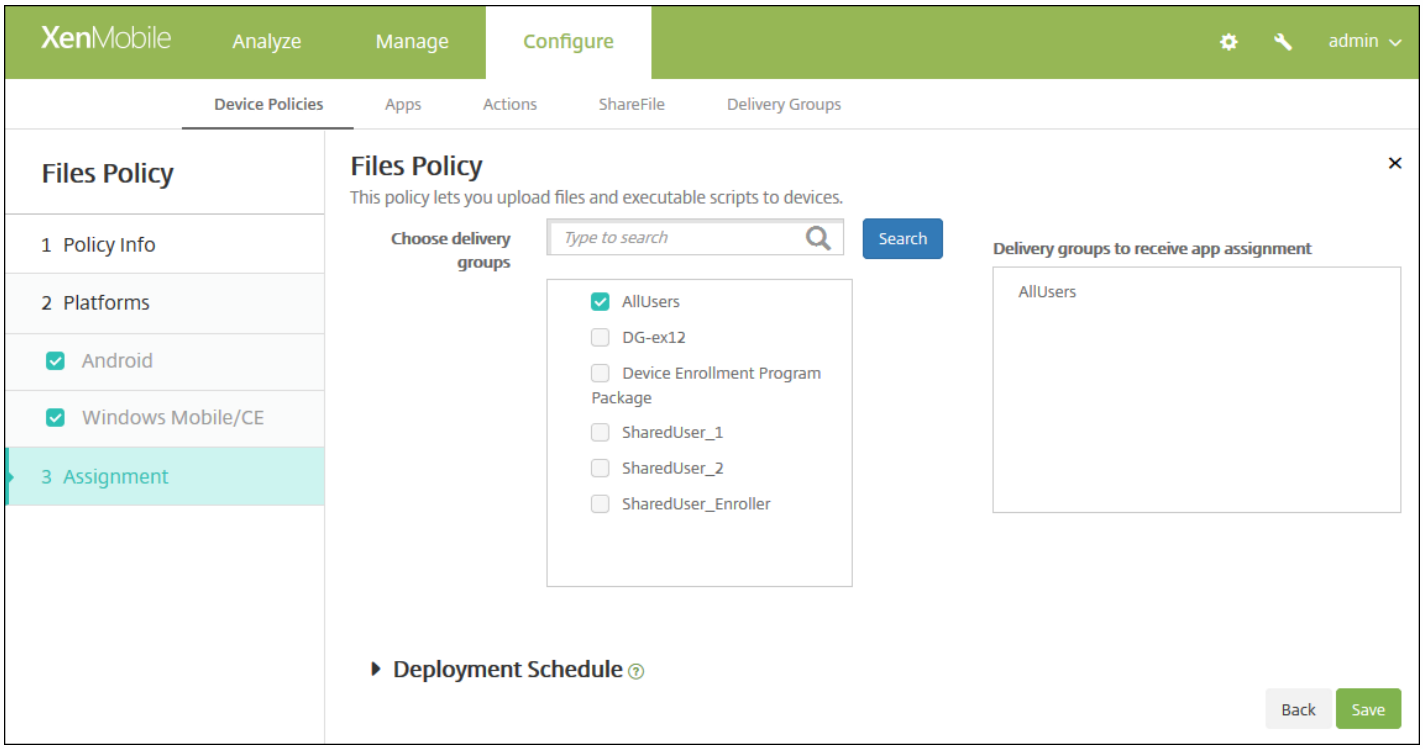
Konfigurieren von Windows Mobile-/CE-Einstellungen



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**.

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **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

Feb 24, 2017

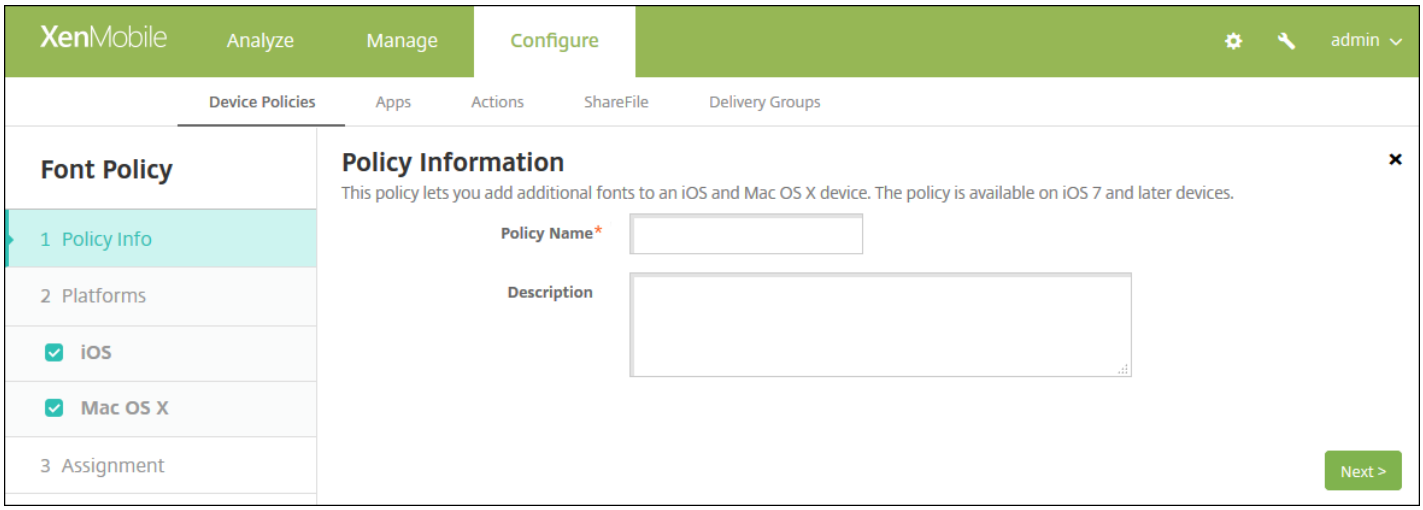
Sie können in XenMobile eine Geräterichtlinie einrichten, mit der zusätzliche Schriftarten auf iOS- und Mac OS X-Geräten hinzugefügt werden. Schriftarten müssen im Format TrueType (.ttf) oder OpenType (.oft) vorliegen. Schriftsammlungen (.ttc oder .otc) werden nicht unterstützt.

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:

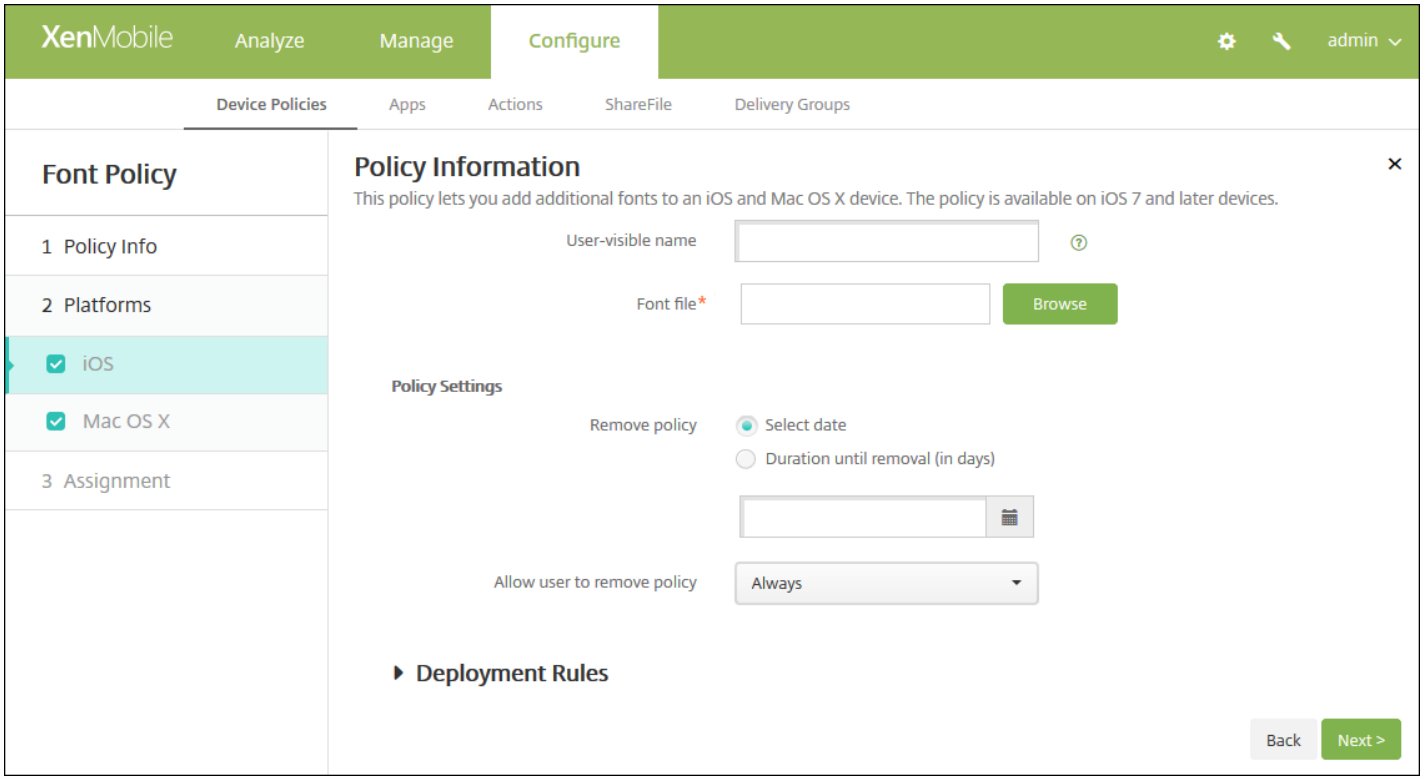
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

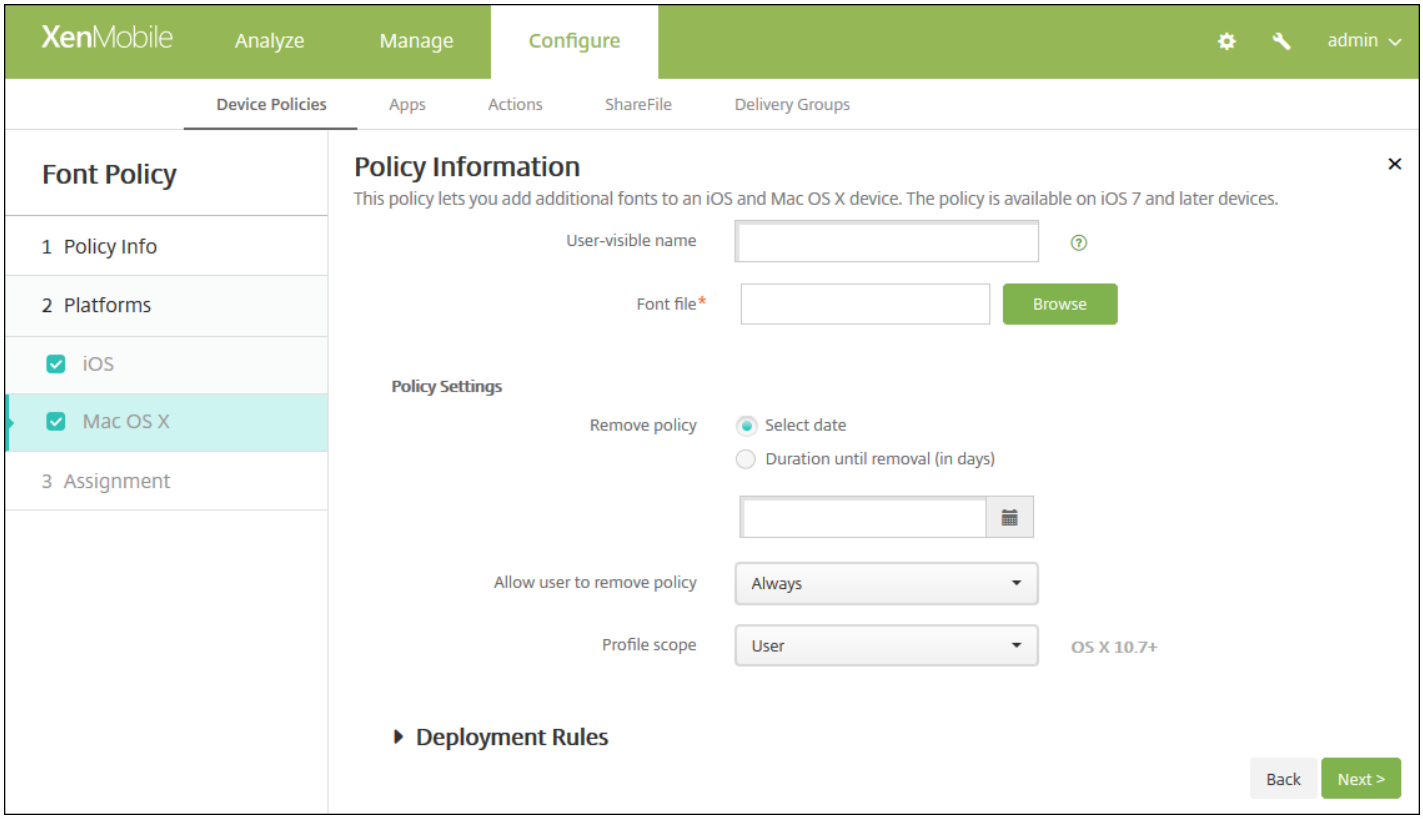
Konfigurieren der iOS-Einstellung



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 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

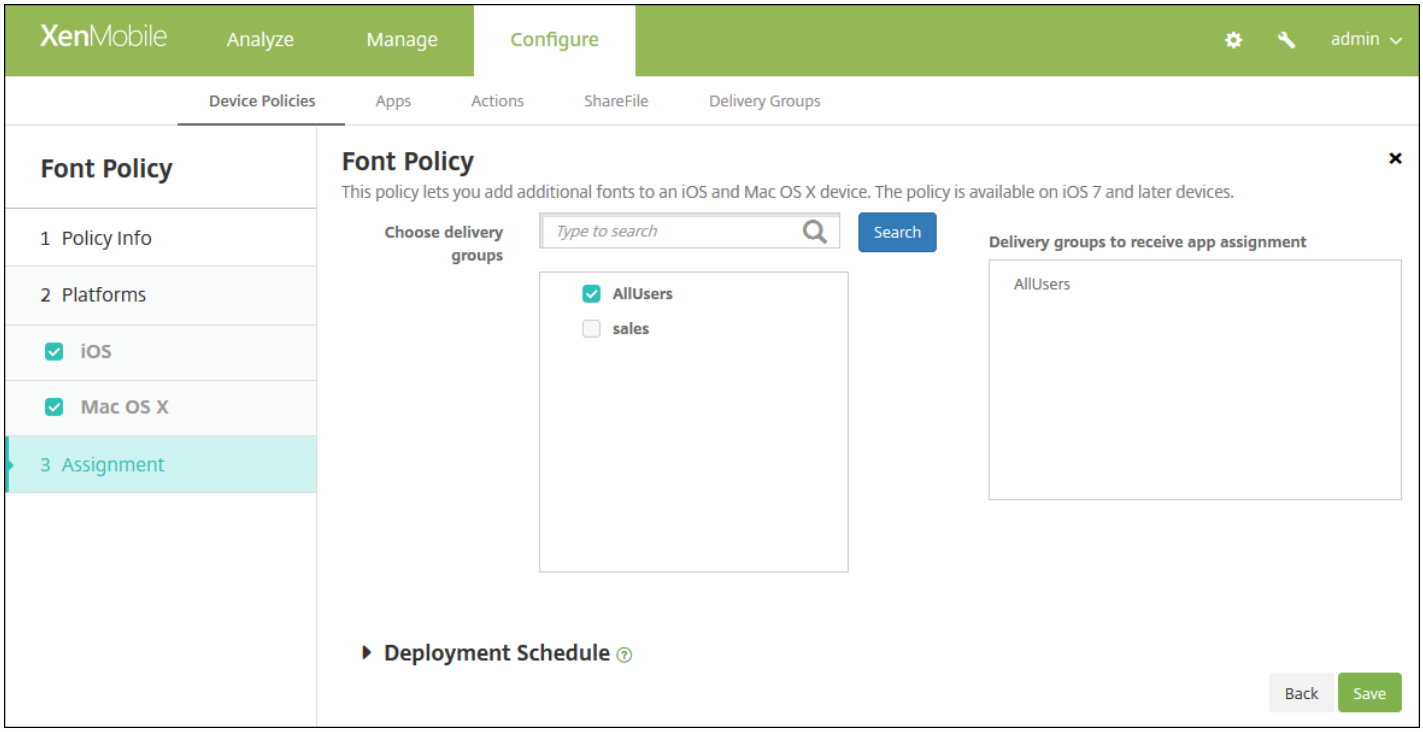


Konfigurieren Sie die folgenden Einstellungen:

- **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 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 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **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

Feb 24, 2017

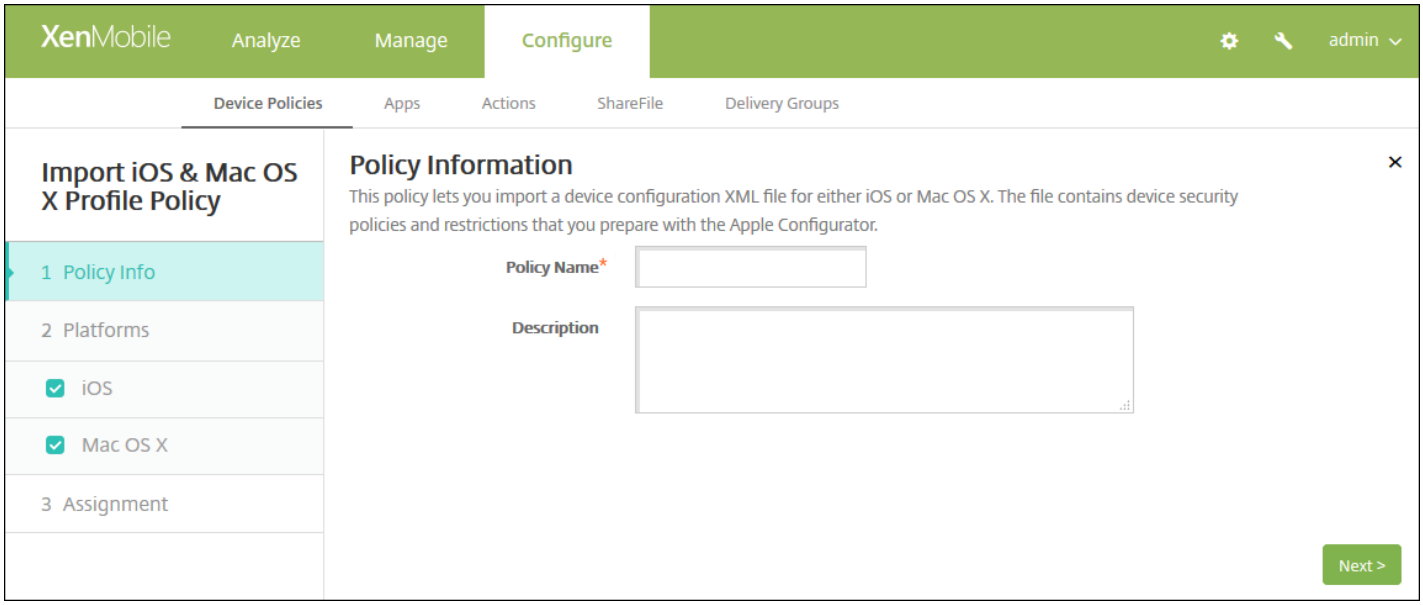
Sie können XML-Dateien für die Konfiguration von iOS- und OS X-Geräten in XenMobile importieren. Die Datei enthält Gerätesicherheitsrichtlinien und -einschränkungen, die Sie mit Apple Configurator vorbereitet haben.

Sie können iOS-Geräte mit Apple Configurator gemäß den Anweisungen im vorliegenden Artikel in den betreuten Modus versetzen. Weitere Informationen über das Erstellen von Konfigurationsdateien mit Apple Configurator finden Sie auf der Apple-Website in der Apple Configurator-Hilfe.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

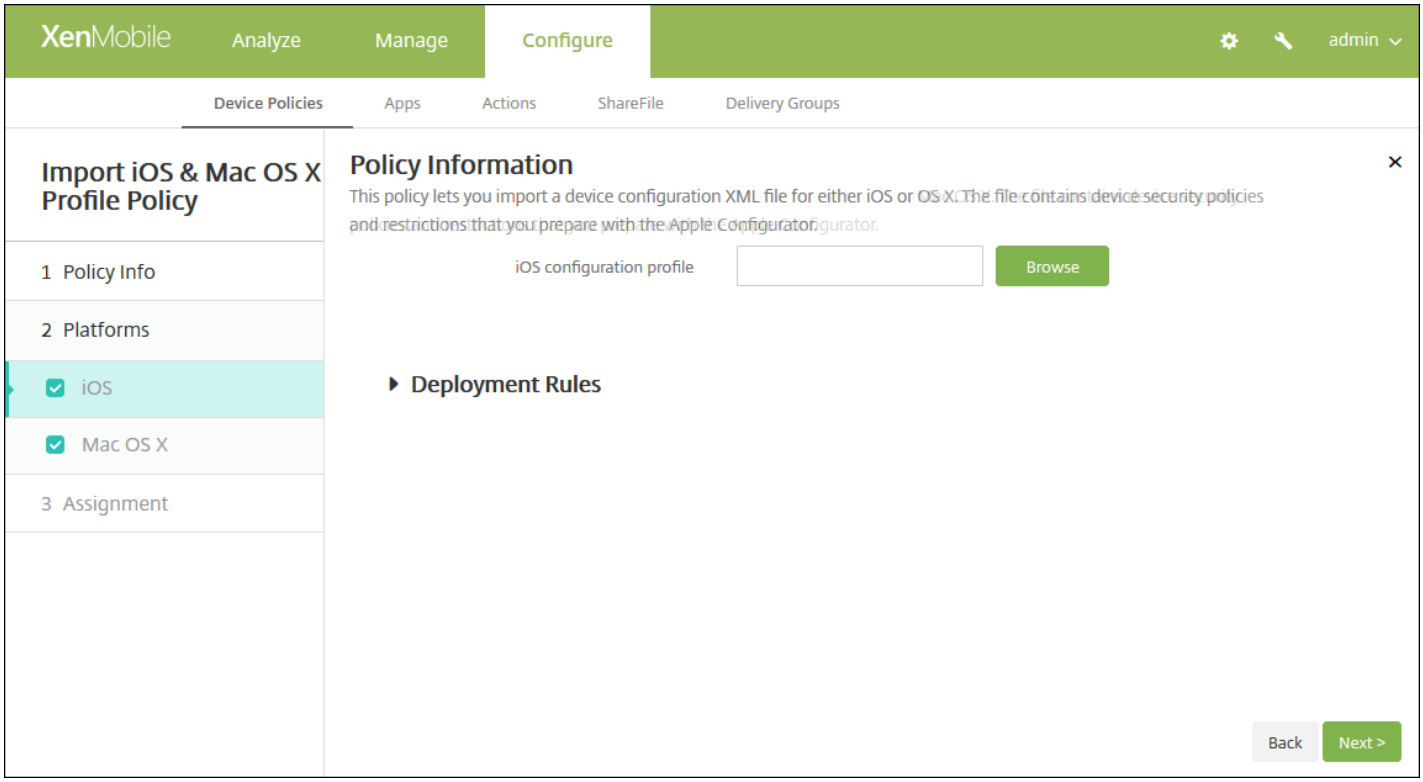
3. Erweitern Sie **Mehr** und klicken Sie unter **Benutzerdefiniert** auf **iOS- und Mac OS X-Profilimport**. Die Seite **iOS- und Mac OS X-Profilimport** wird angezeigt.



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.

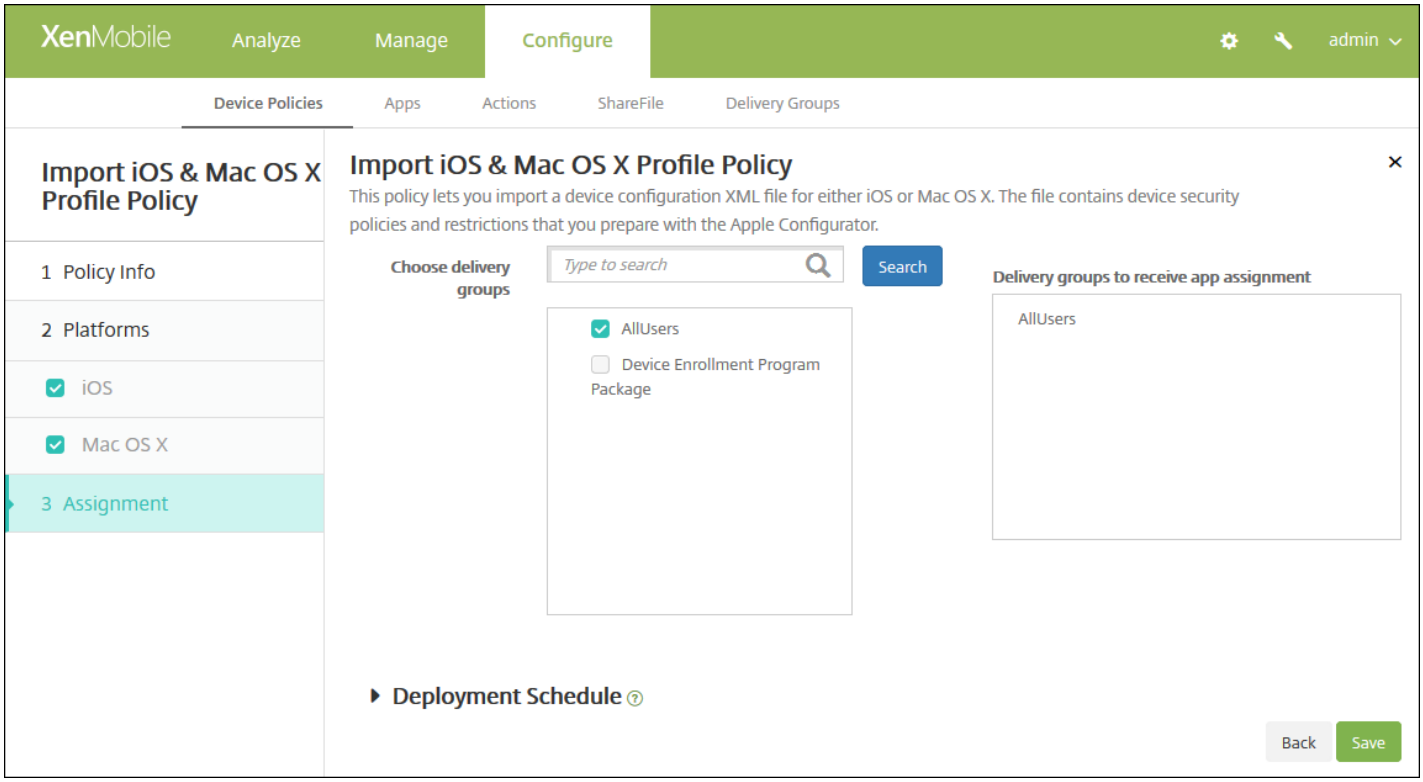
Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 8. .

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

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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

12. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Versetzen eines iOS-Geräts mit Apple Configurator in den betreuten Modus

Zur Verwendung des Apple Configurators brauchen Sie einen Apple-Computer mit OS X 10.7.2 oder höher.

Important

Beim Versetzen eines Geräts in den betreuten Modus wird die ausgewählte iOS-Version auf dem Gerät installiert und sämtliche zuvor gespeicherten Benutzerdaten und Apps werden von dem Gerät gelöscht.

1. Installieren Sie Apple Configurator aus iTunes.

2. Schließen Sie das iOS-Gerät an den Apple-Computer an.

3. Starten Sie Apple Configurator. Configurator zeigt an, dass ein Gerät zur Vorbereitung für die Betreuung vorhanden ist.

4. Bereiten Sie das Gerät für die Betreuung vor:

a. Legen Sie für **Supervision** die Option **On** fest. Citrix empfiehlt, diese Einstellung zu aktivieren, wenn Sie ein Gerät kontinuierlich durch regelmäßige Neuanwendung einer Konfiguration steuern möchten.

c. Geben Sie optional einen Namen für das Gerät ein.

c. Klicken Sie für "iOS" auf **Latest** für die neueste iOS-Version, die Sie installieren möchten.

5. Wenn das Gerät zur Betreuung vorbereitet werden kann, klicken Sie auf **Prepare**.

Kioskrichtlinie für Samsung SAFE

Feb 24, 2017

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

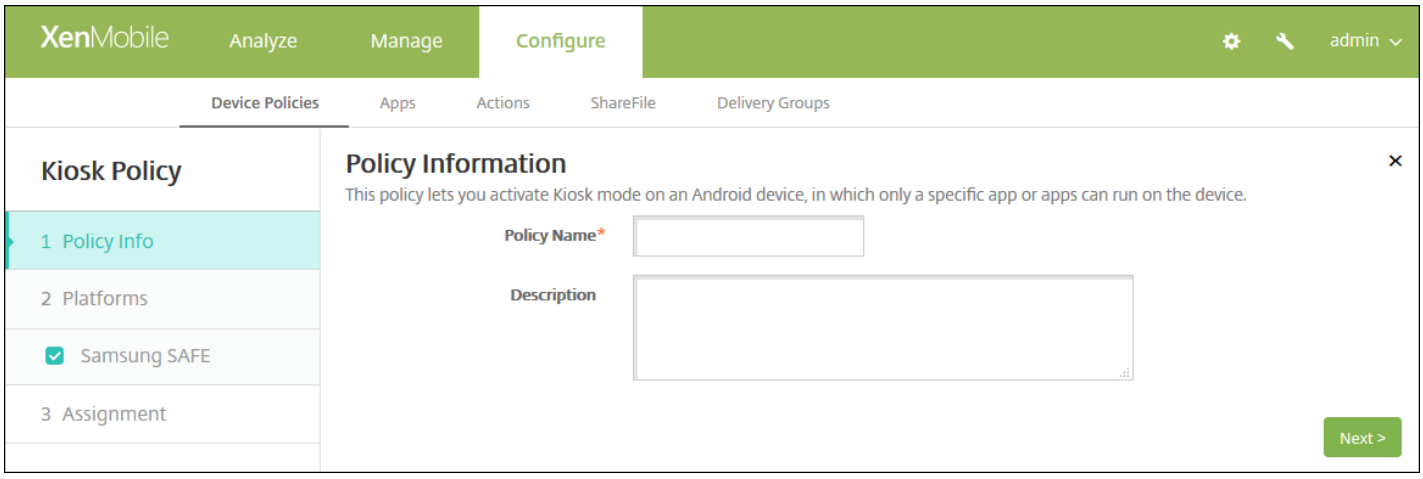
Hinweis:

- 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.

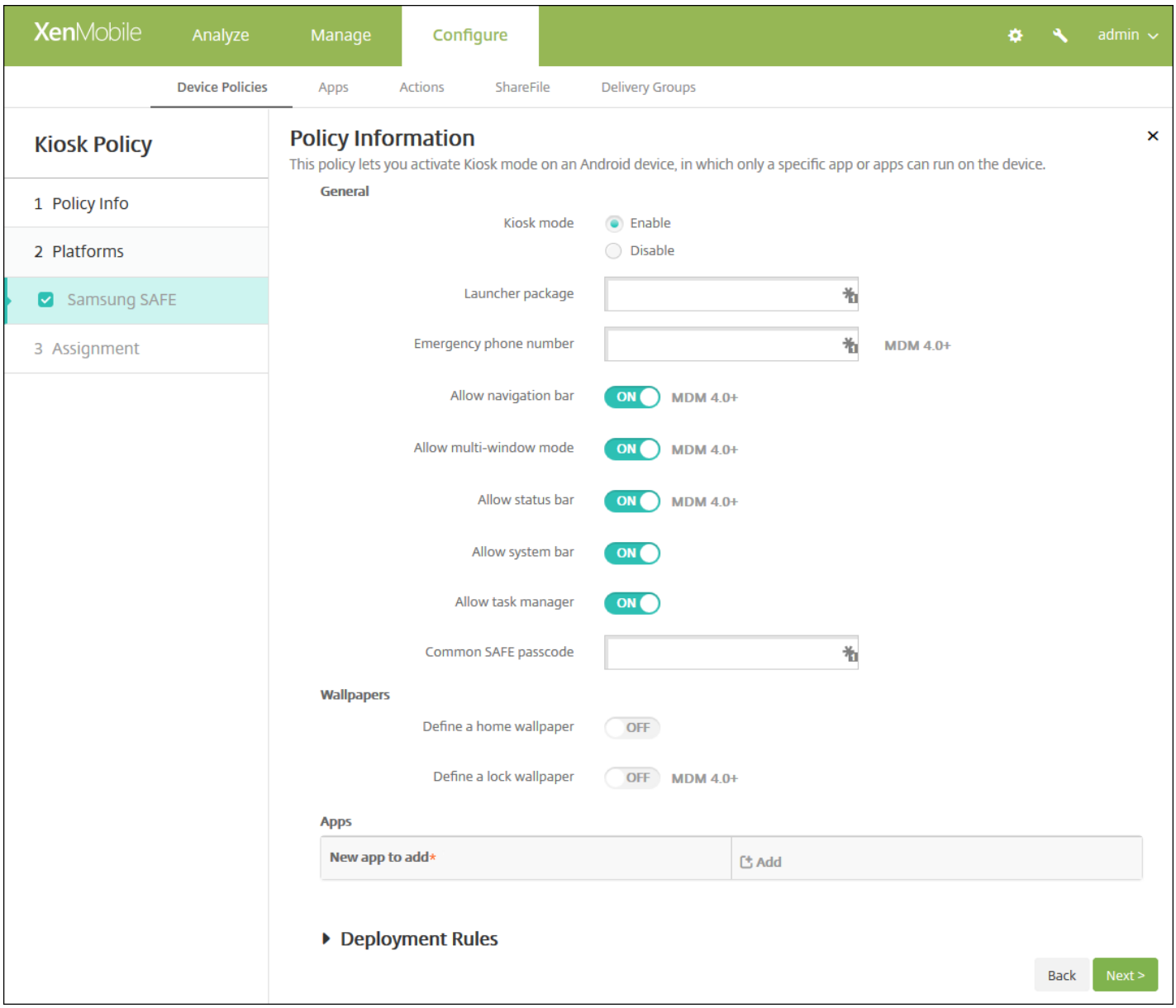
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Kiosk**. Die Seite **Kiosk** wird angezeigt.



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.

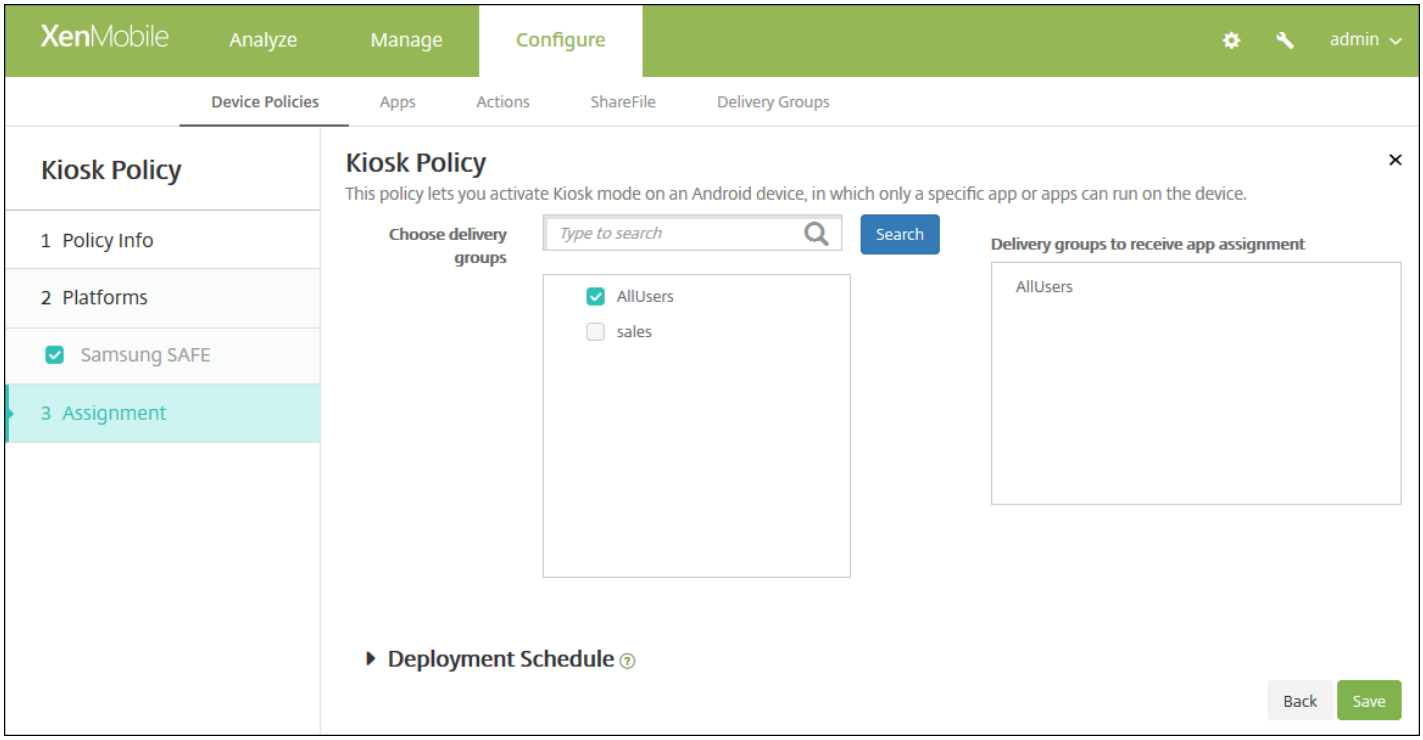
- **Notrufnummer**: Geben Sie optional eine Telefonnummer ein. Über diese Nummer kann der etwaige Finder eines verlorenen Geräts sich an Ihr Unternehmen wenden. Gilt nur für MDM 4.0 und höher.
- **Navigationsleiste zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus die Navigationsleiste anzeigen und verwenden können sollen. Gilt nur für MDM 4.0 und höher. Der Standardwert ist **EIN**.
- **Mehrfenstermodus zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus mehrere Fenster verwenden können sollen. Gilt nur für MDM 4.0 und höher. Der Standardwert ist **EIN**.
- **Statusleiste zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus die Statusleiste anzeigen können sollen. Gilt nur für MDM 4.0 und höher. Der Standardwert ist **EIN**.
- **Systemleiste zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus die Systemleiste anzeigen können sollen. Der Standardwert ist **EIN**.
- **Task-Manager zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus den Task-Manager anzeigen und verwenden können sollen. Der Standardwert 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Launcher-Konfigurationsrichtlinie für Android-Geräte

Feb 24, 2017

Mit Citrix Launcher können Sie die Benutzererfahrung für Android-Geräte in XenMobile anpassen. Mit einer Launcher-Konfigurationsrichtlinie können Sie folgende Citrix Launcher-Features steuern:

- Verwalten von Android-Geräten, sodass Benutzer nur auf von Ihnen festgelegte Apps Zugriff haben
- Optionale Angabe eines benutzerdefinierten Logos als Citrix Launcher-Symbol sowie eines benutzerdefinierten Hintergrundbilds für Citrix Launcher
- Festlegen eines Kennworts, das die Benutzer zum Beenden von Launcher eingeben müssen

Mit Citrix Launcher können Sie diese Einschränkungen auf Geräteebene festlegen, gleichzeitig bietet Launcher den Benutzern die benötigte Flexibilität durch integrierten Zugriff auf Geräteinstellungen, etwa für WiFi, Bluetooth und Gerätepasscode. Citrix Launcher ist nicht als zusätzliche Sicherheitsstufe gedacht.

Nach der Bereitstellung von Citrix Launcher wird es von XenMobile anstelle des Android-Standardstartprogramms installiert.

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

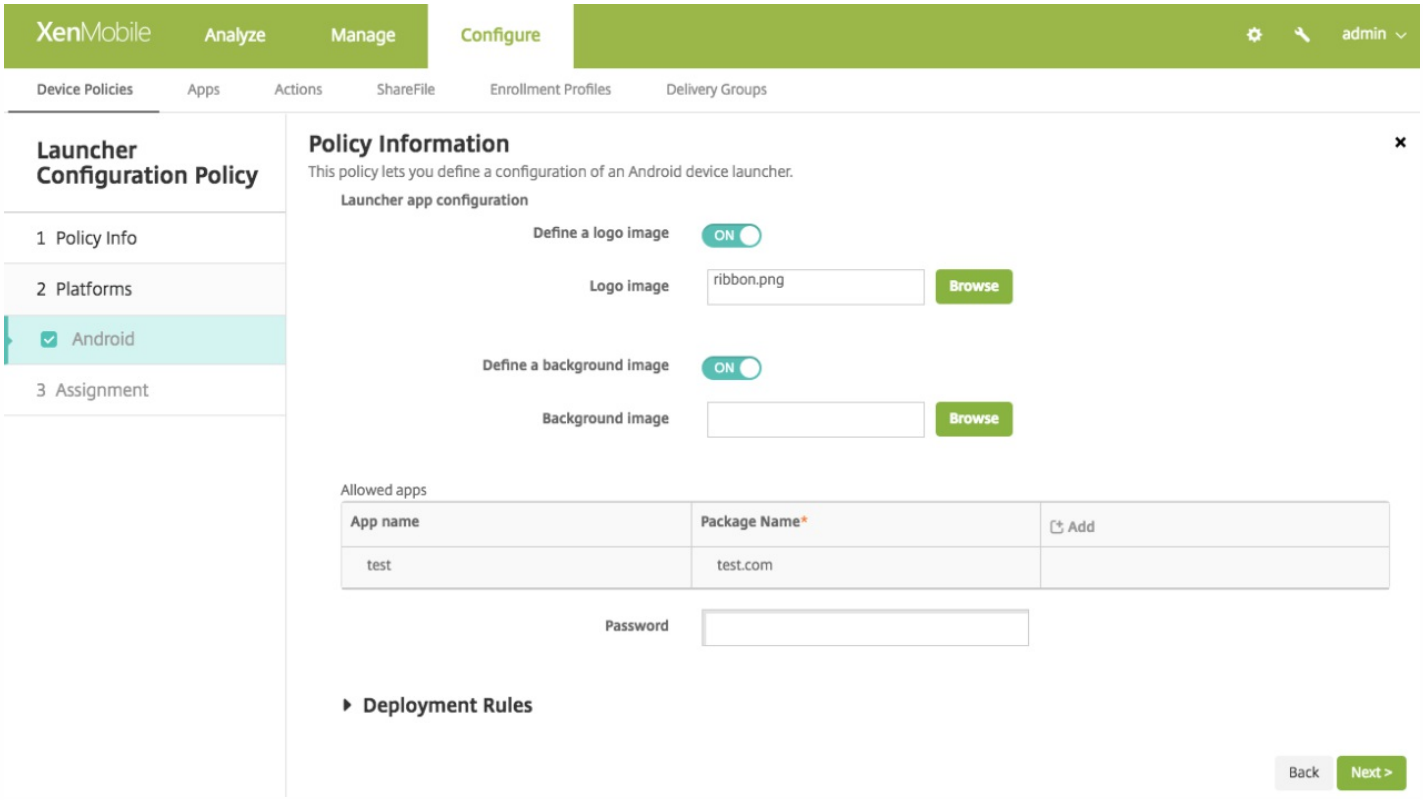
2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Beginnen Sie mit der Eingabe von **Launcher** und wählen Sie in der Liste **Launcher-Konfiguration** aus. Die Seite **Launcher-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 Informationsseite **Android Platform** wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

- **Logobild definieren**: Wählen Sie aus, ob ein benutzerdefiniertes Logobild als Citrix Launcher-Symbol verwendet werden soll. Der Standardwert ist **AUS**.
- **Logobild**: Wenn Sie **Logobild definieren** aktivieren, klicken Sie auf **Durchsuchen**, navigieren Sie zu der Datei mit dem gewünschten Bild und wählen Sie diese aus. Es können Dateien des Typs PNG, JPG, JPEG und GIF verwendet werden.
- **Hintergrundbild definieren**: Wählen Sie aus, ob ein benutzerdefiniertes Bild für den Citrix Launcher-Hintergrund verwendet werden soll. Der Standardwert ist **AUS**.
- **Hintergrundbild**: Wenn Sie **Hintergrundbild definieren** aktivieren, klicken Sie auf **Durchsuchen** und navigieren Sie zu der Datei mit dem gewünschten Bild. Es können Dateien des Typs PNG, JPG, JPEG und GIF verwendet werden.
- **Zugelassene Apps**: Klicken Sie für jede App, die Sie in Citrix Launcher zulassen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Neue App zum Hinzufügen**: Geben Sie den vollständigen Namen der App ein. Beispiel: "com.android.calendar" für die Android-Kalender-App.
  - 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 **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.
- **Kennwort**: Kennwort, das die Benutzer zum Beenden von Citrix Launcher eingeben müssen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Launcher-Konfigurationsrichtlinie wird angezeigt.

9. Konfigurieren der Bereitstellungsregeln

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 **Später** 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**.

12. Klicken Sie auf **Speichern**.

LDAP-Geräterichtlinien

Feb 24, 2017

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.

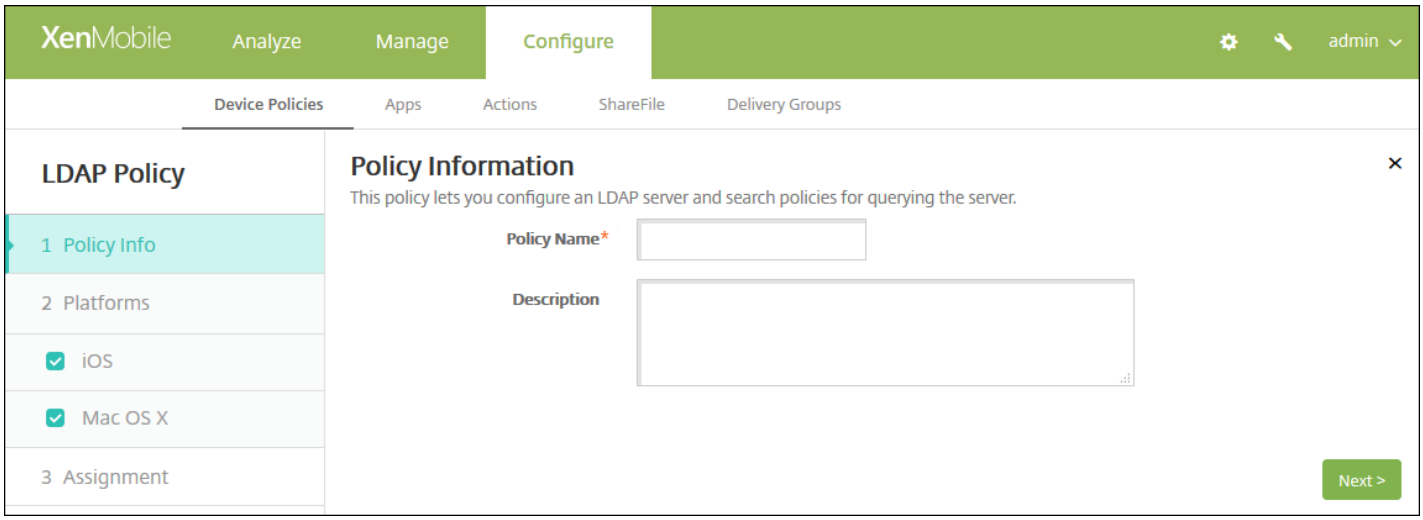
iOS-Einstellungen

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:

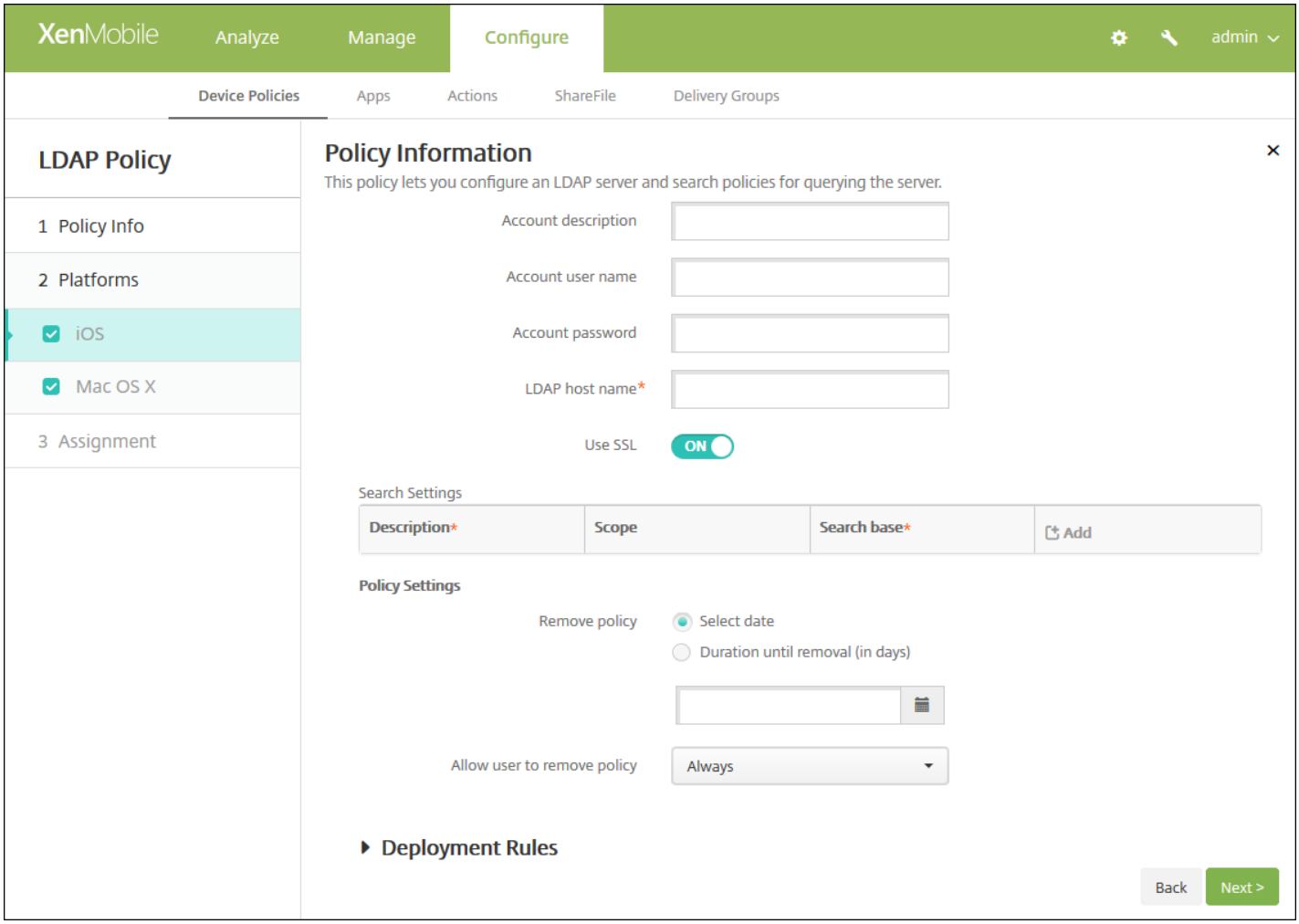
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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. Der Standardwert 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.

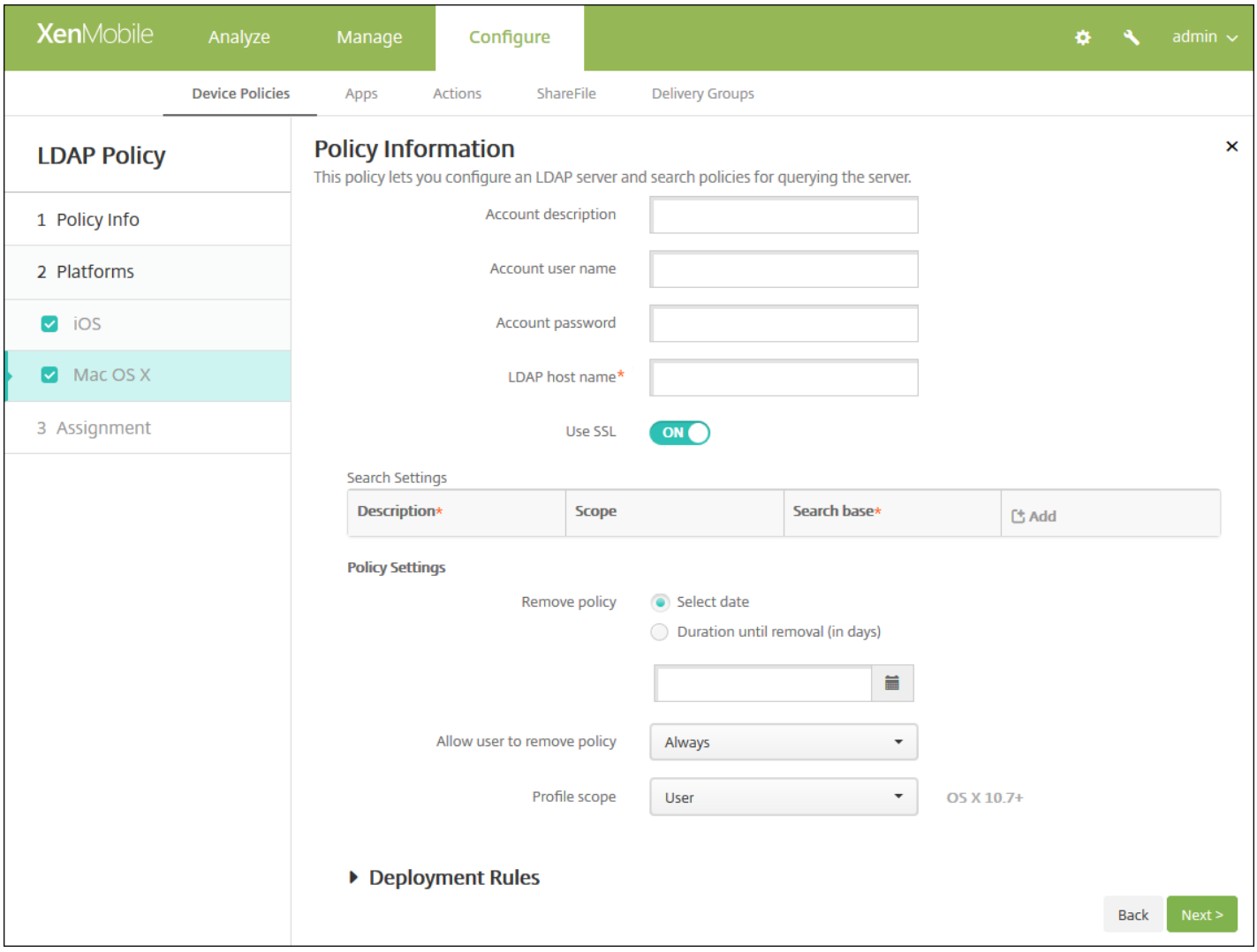
- Wiederholen Sie diese Schritte für jede Sucheinstellung, die Sie hinzufügen möchten.

  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.
- **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. Der Standardwert 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.

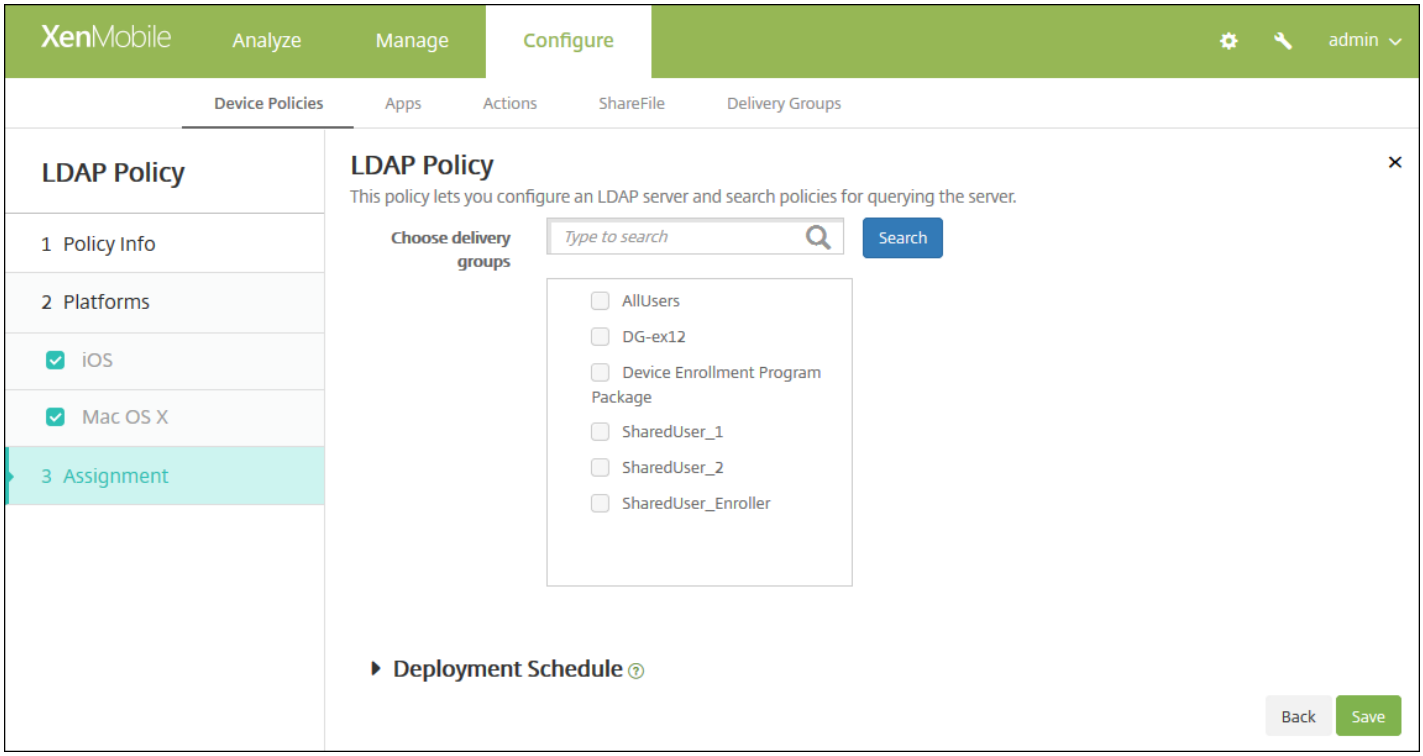
    Hinweis: Zum Löschen einer vorhandenen Sucheinstellung zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf "Löschen" zum Löschen des Eintrags oder auf "Bearbeiten", um ihn beizubehalten.

    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.
- 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **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

Feb 24, 2017

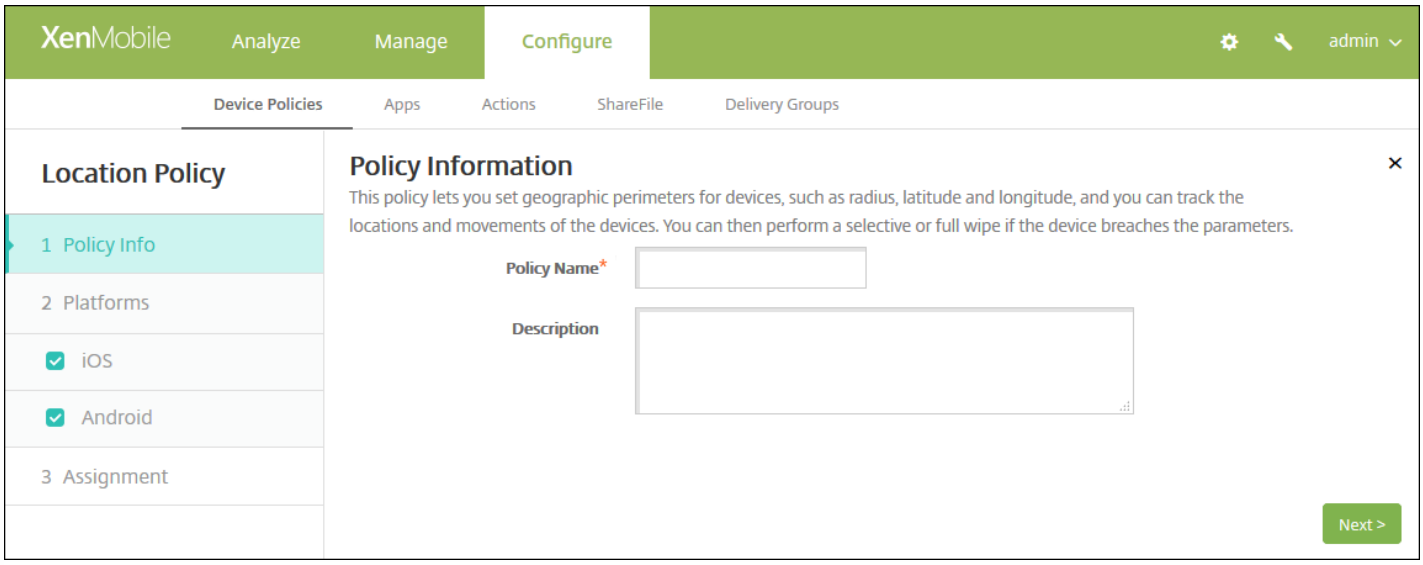
Mit einer Standortrichtlinie legen Sie in XenMobile geografische Grenzen fest und verfolgen den Standort und die Bewegung der Geräte der Benutzer. Wenn ein Benutzer den festgelegten Bereich (*Geofence*) verlässt, kann XenMobile eine selektive oder vollständige Löschung der Daten auf seinem Gerät durchführen. 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:

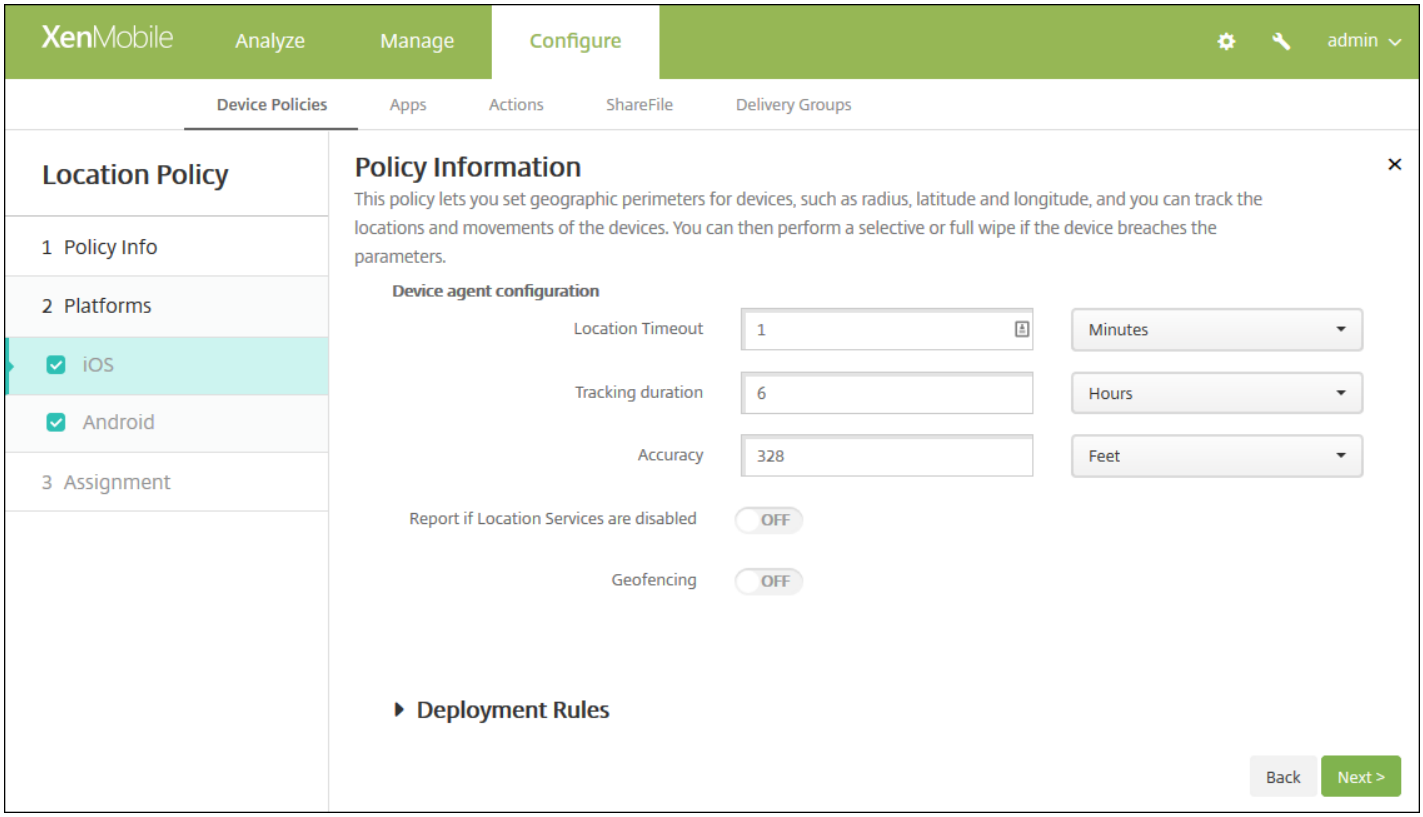
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

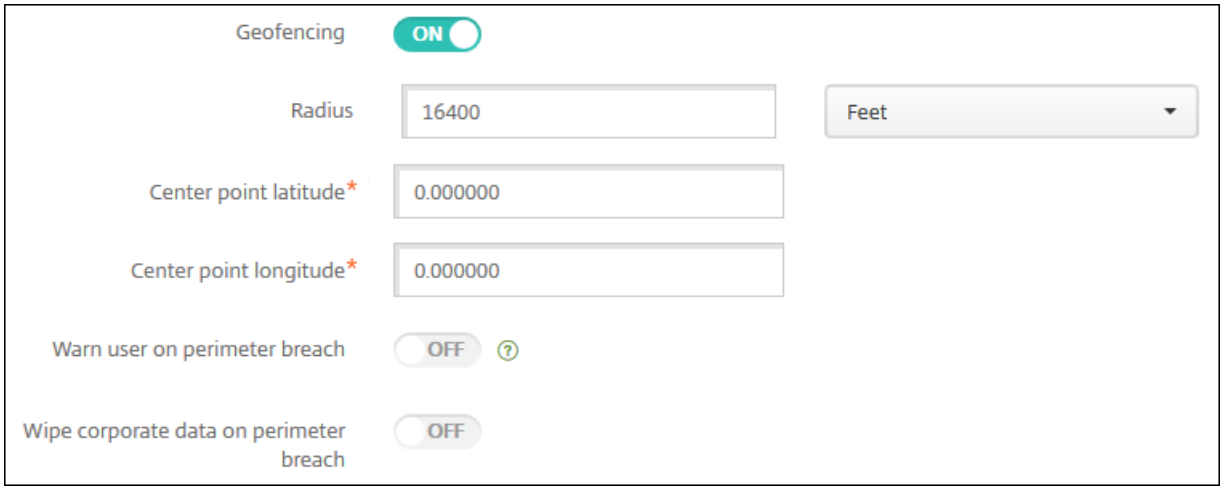
Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 7.

Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

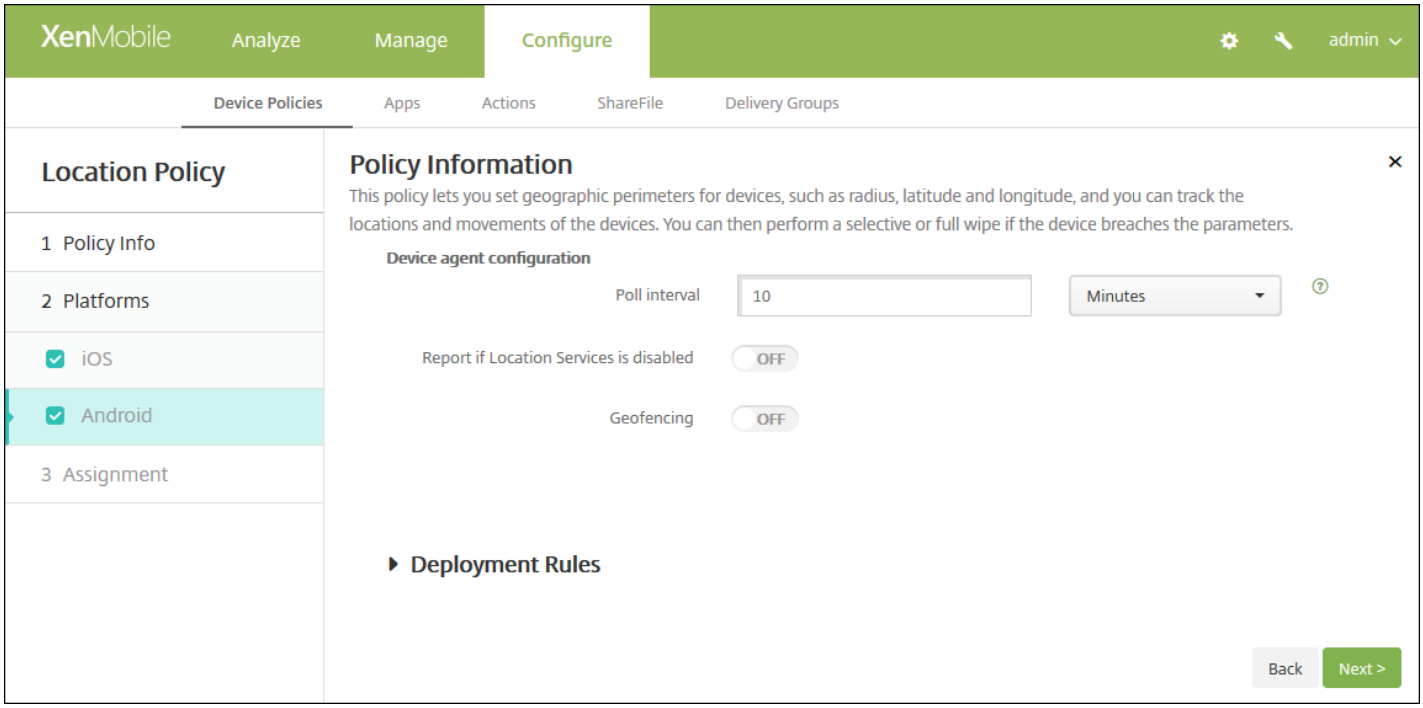
- **Standorttimeout**: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf **Sekunden** oder **Minuten**, um festzulegen, wie häufig XenMobile den Gerätestandort abrufen soll. Gültige Werte sind 60-900 Sekunden oder 1-15 Minuten. Der Standardwert ist 1 Minute.
- **Trackingdauer**: Geben Sie eine 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**



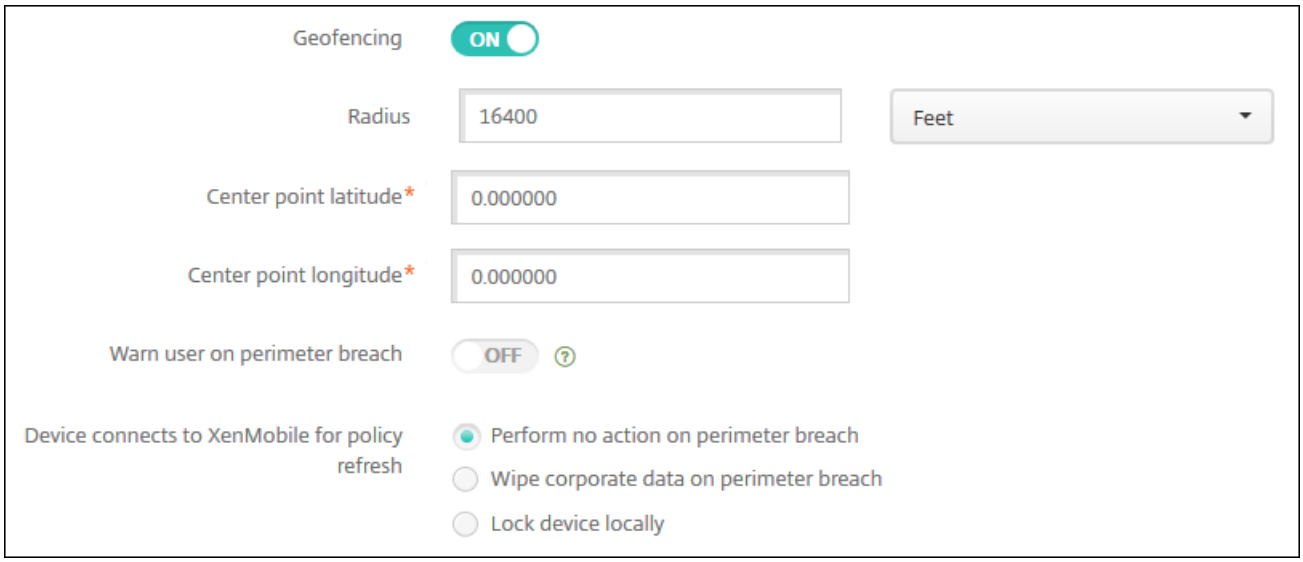
Bei Auswahl von "Geofencing" konfigurieren Sie die folgenden Einstellungen:

- **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:

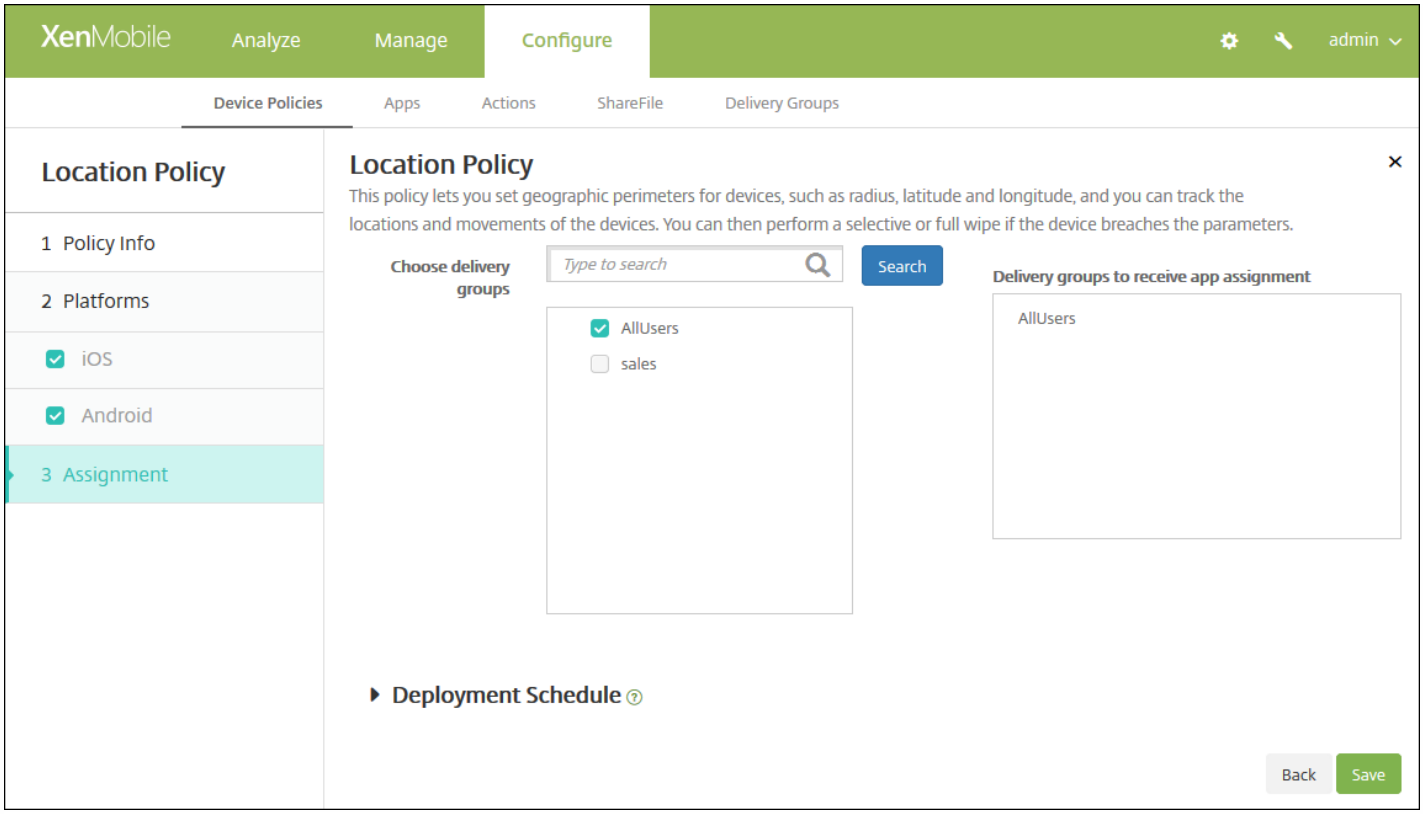
- **Radius**: Geben Sie zur Messung des Radius eine Ziffer ein und klicken Sie in Liste auf die Einheit. Der Standardwert ist 16.400 Fuß. Gültige Werte für den Radius:

- 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

E-Mail-Geräterichtlinien

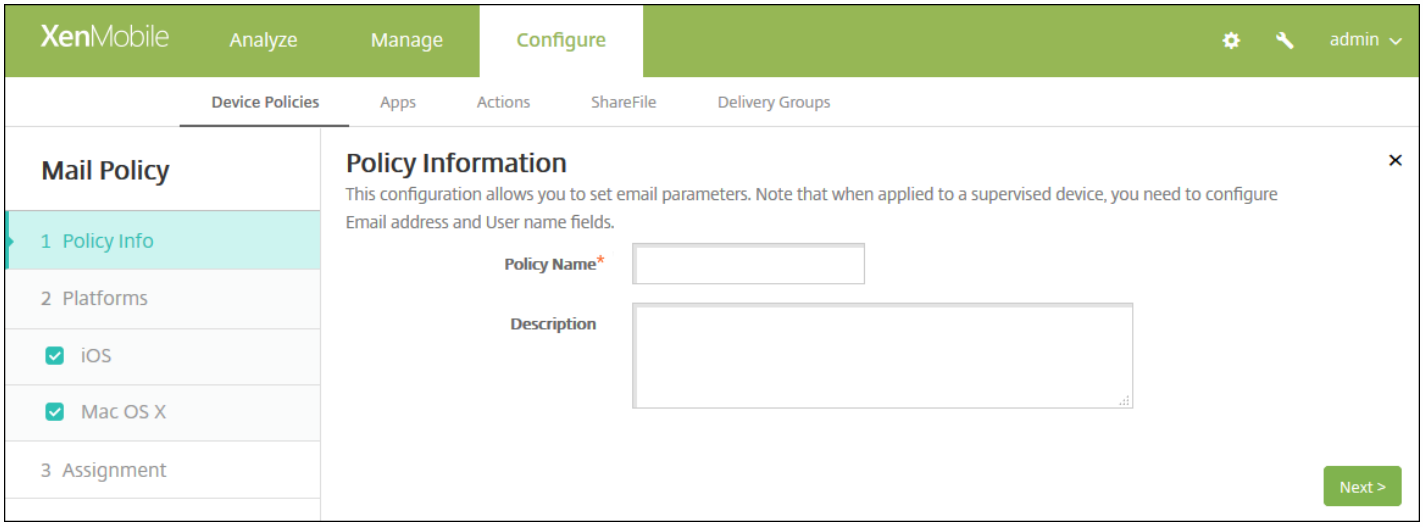
Feb 24, 2017

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.

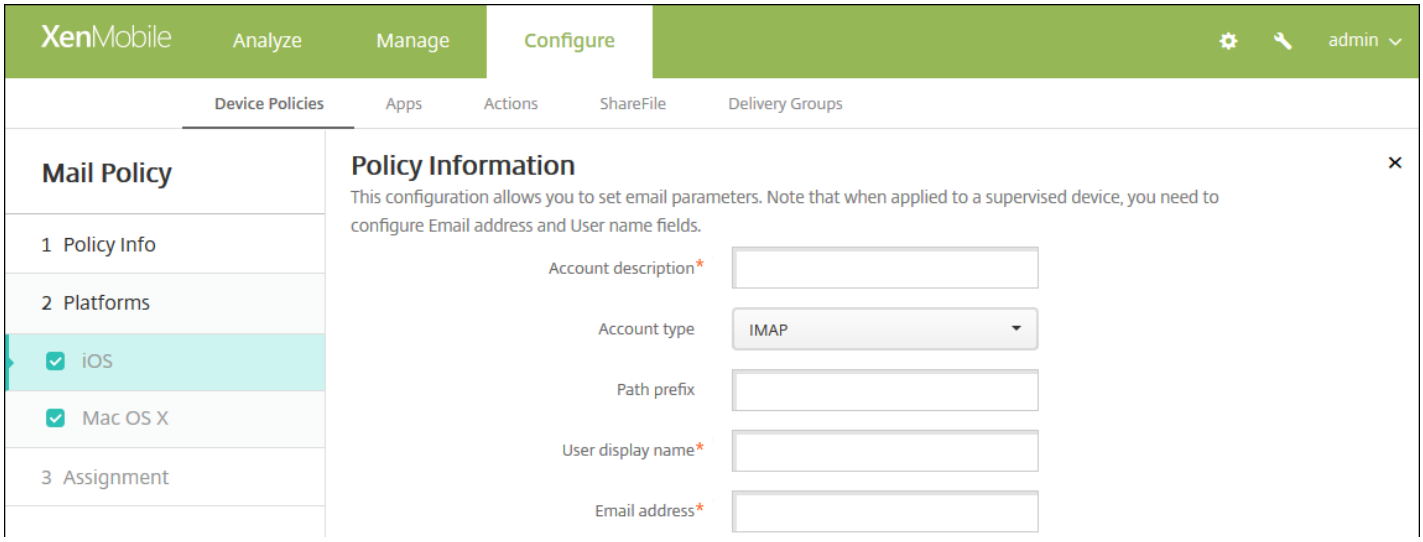
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **E-Mail**. Die Seite **E-Mail** wird angezeigt.

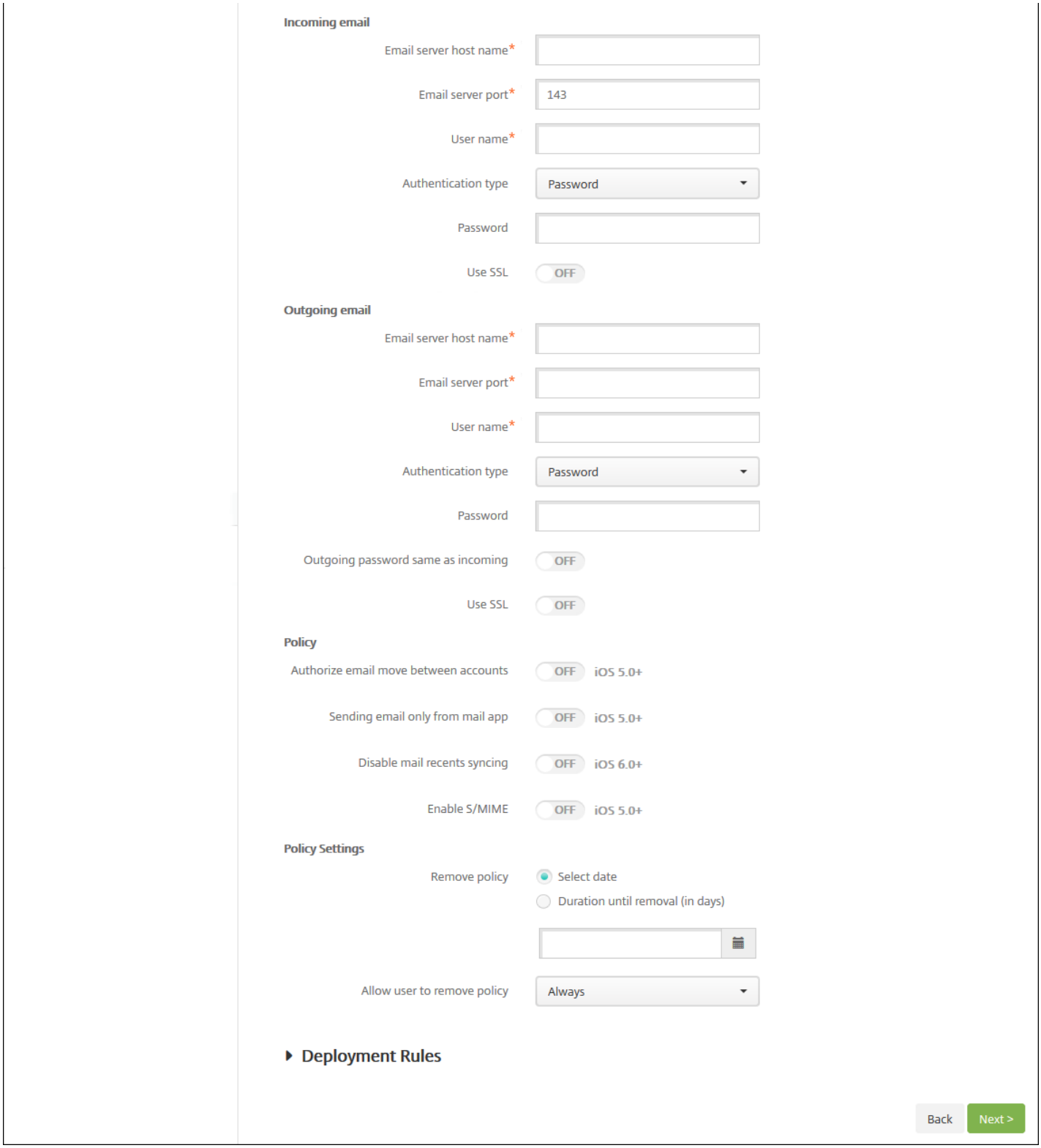


4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

- **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 zur Anzeige in Nachrichten usw. an. 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 vor, 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.
  - **Synchronisierung aktueller E-Mails deaktivieren**: Wählen Sie aus, ob eine Synchronisierung zuletzt verwendeter

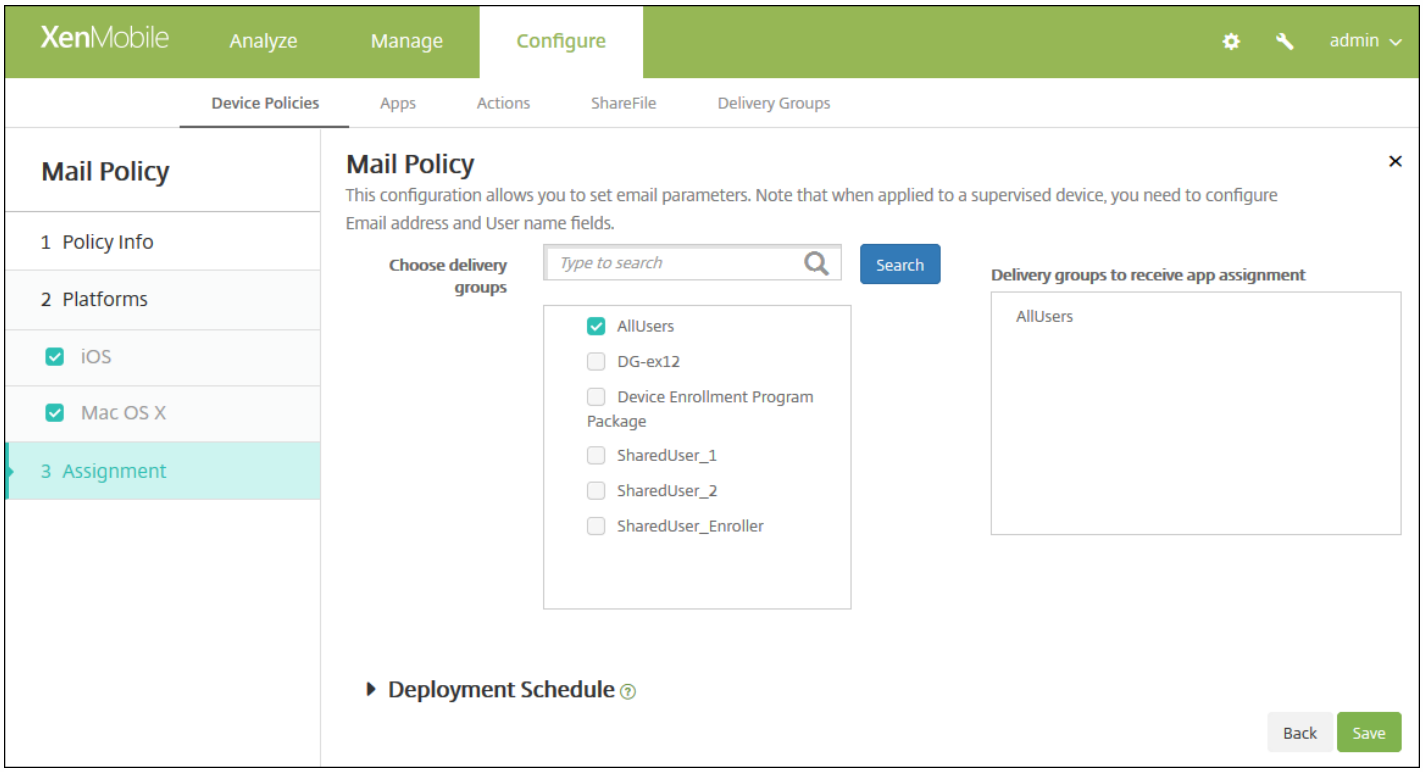
Adressen durch die Benutzer verhindert werden soll. Der Standardwert ist **AUS**. Diese Option gilt nur für iOS 6.0 und höher.

- **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 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.
  - 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **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

Feb 24, 2017

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.

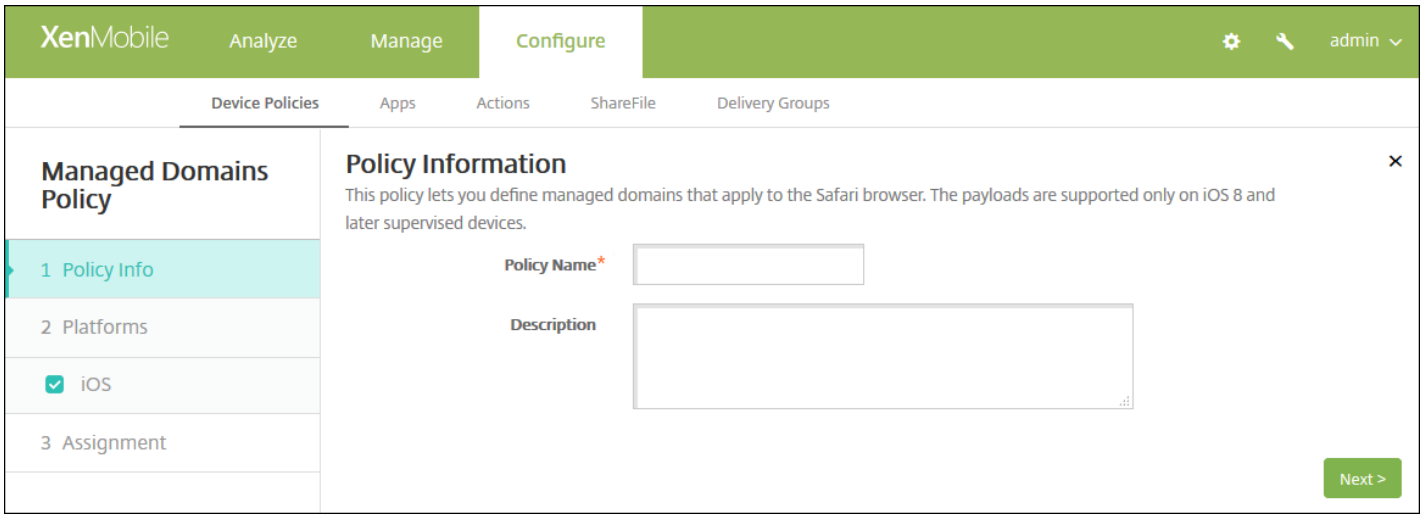
Wenn ein Benutzer eine E-Mail an einen Empfänger sendet, dessen Domäne nicht auf der Liste der verwalteten E-Mail-Domänen steht, wird auf seinem Gerät eine Warnung angezeigt, dass die E-Mail an eine Person außerhalb der Domäne des Unternehmens gesendet wird.

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.

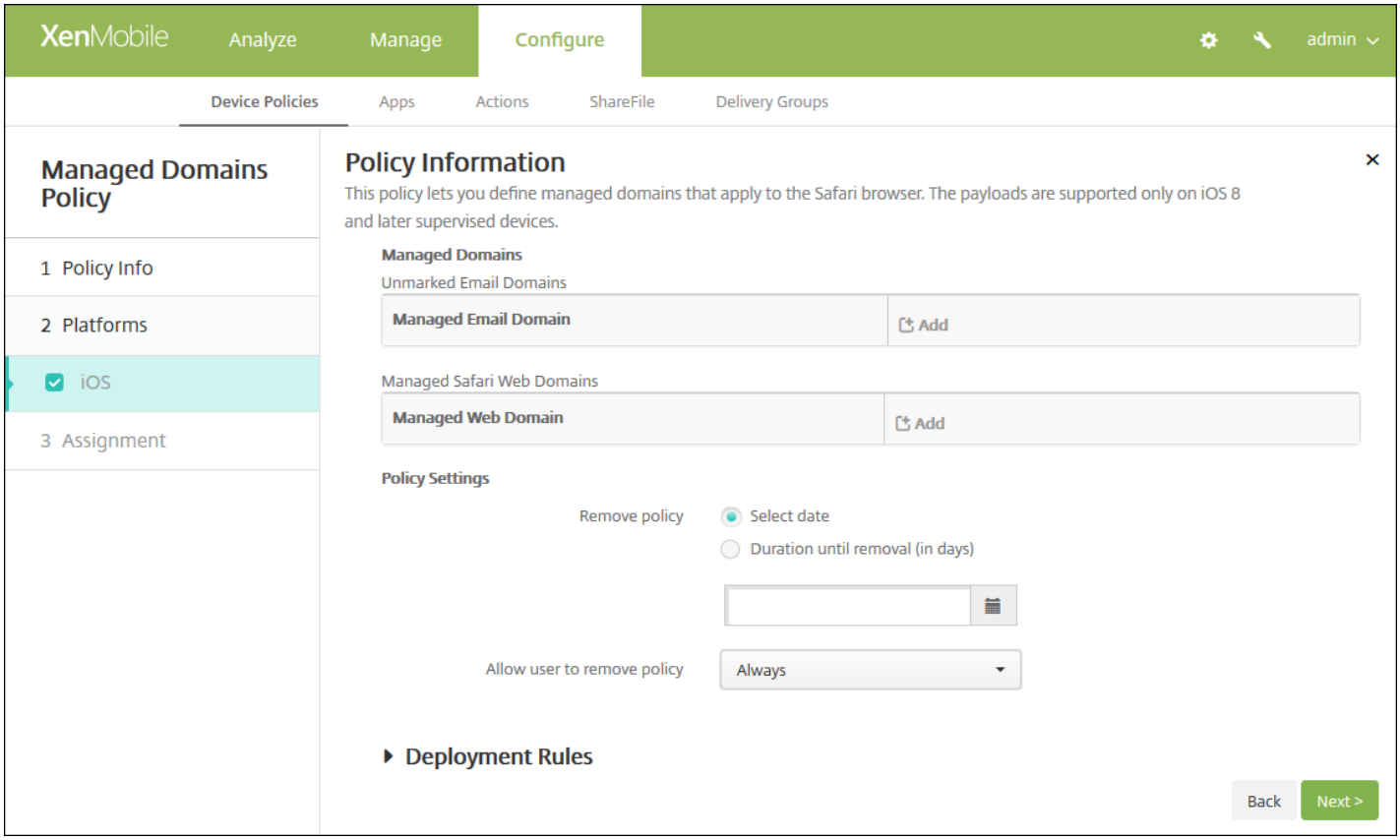
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Verwaltete Domänen**. Die Seite **Verwaltete Domänen** wird angezeigt.



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.

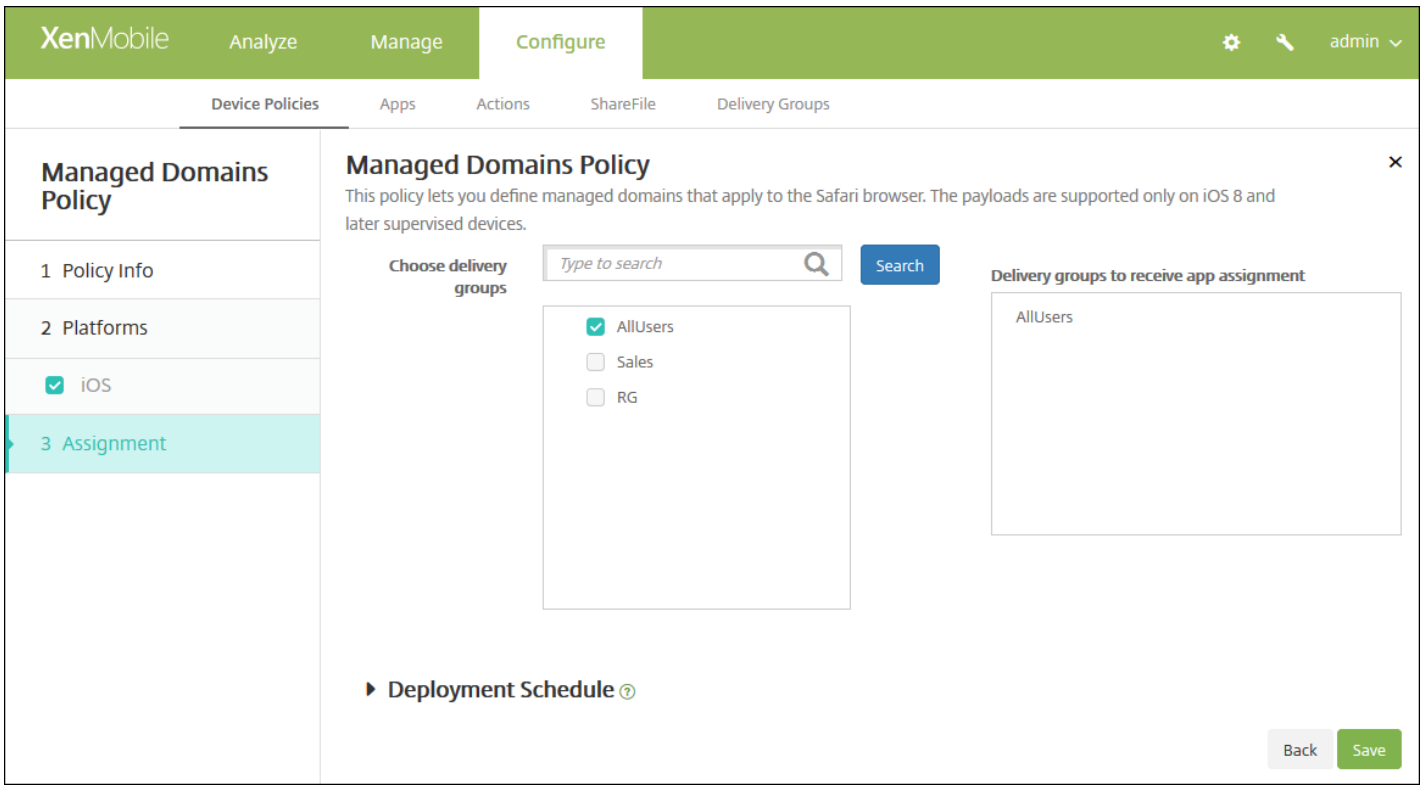
      Hinweis: Zum Löschen einer vorhandenen Domäne zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, um ihn beizubehalten.

      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** 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.

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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im

Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

MDM-Optionsrichtlinien für Geräte

Feb 24, 2017

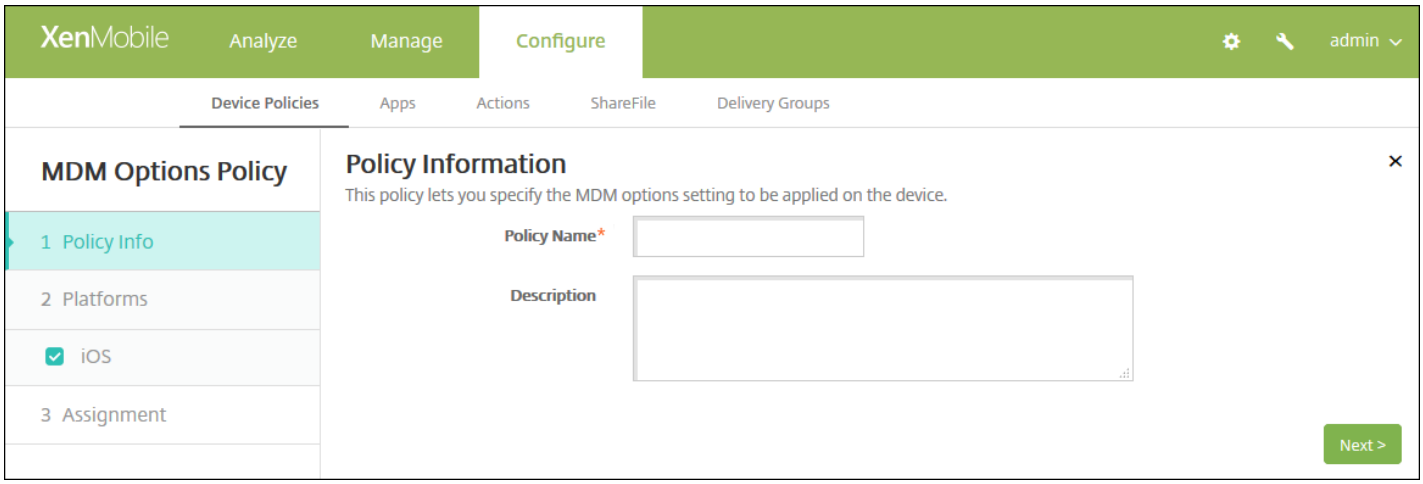
Sie können in XenMobile eine Geräterichtlinie zum Verwalten der Aktivierungssperre des Features "Mein iPhone/iPad suchen" auf betreuten Geräten mit iOS 7.0 und höher erstellen. Anweisungen zum Versetzen von iOS-Geräten in den betreuten Modus finden Sie unter Versetzen von iOS-Geräten mit dem Apple Configurator 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.

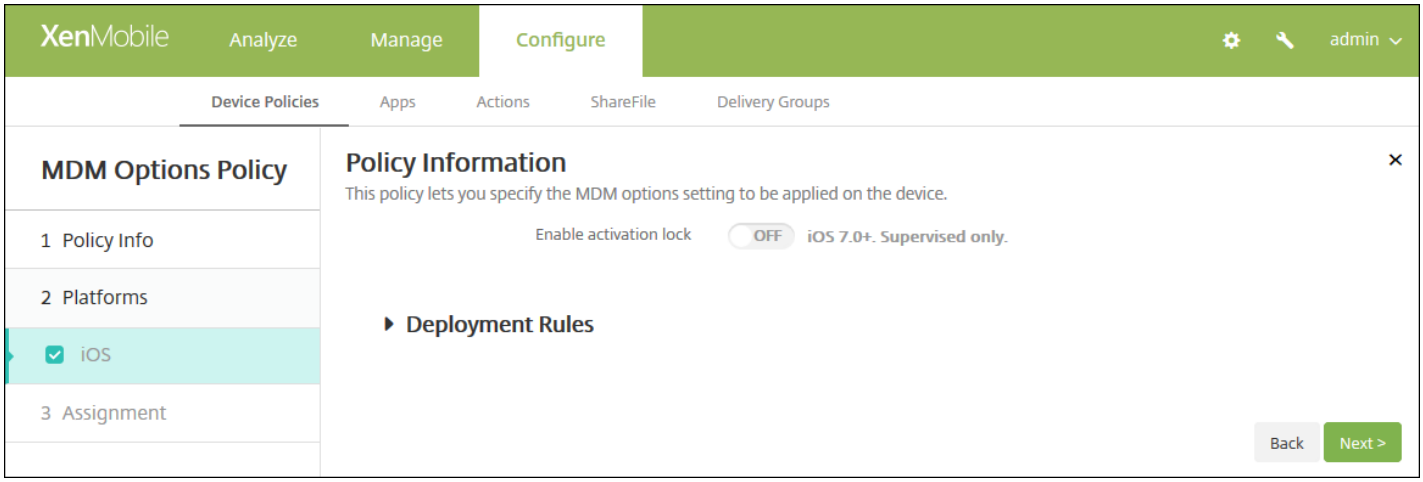
3. Erweitern Sie **Mehr** und klicken Sie unter **Endbenutzer** auf **MDM-Konto**. Die Seite **MDM-Optionen** wird angezeigt.



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.

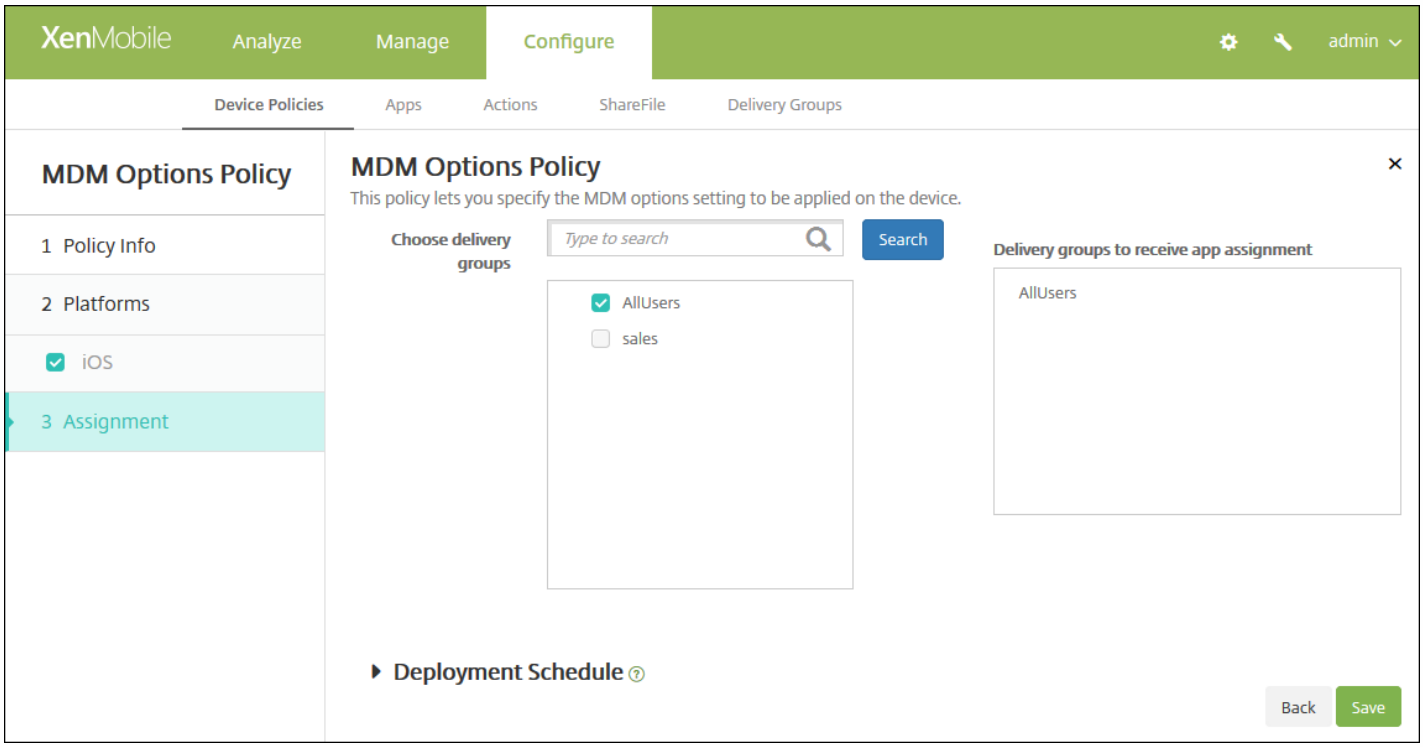


6. Konfigurieren Sie folgende Einstellung:

- **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 **ON**. Wenn Sie **AUS** auswählen, müssen keine anderen Optionen konfiguriert werden.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Microsoft Exchange ActiveSync-Geräterichtlinien

Feb 24, 2017

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

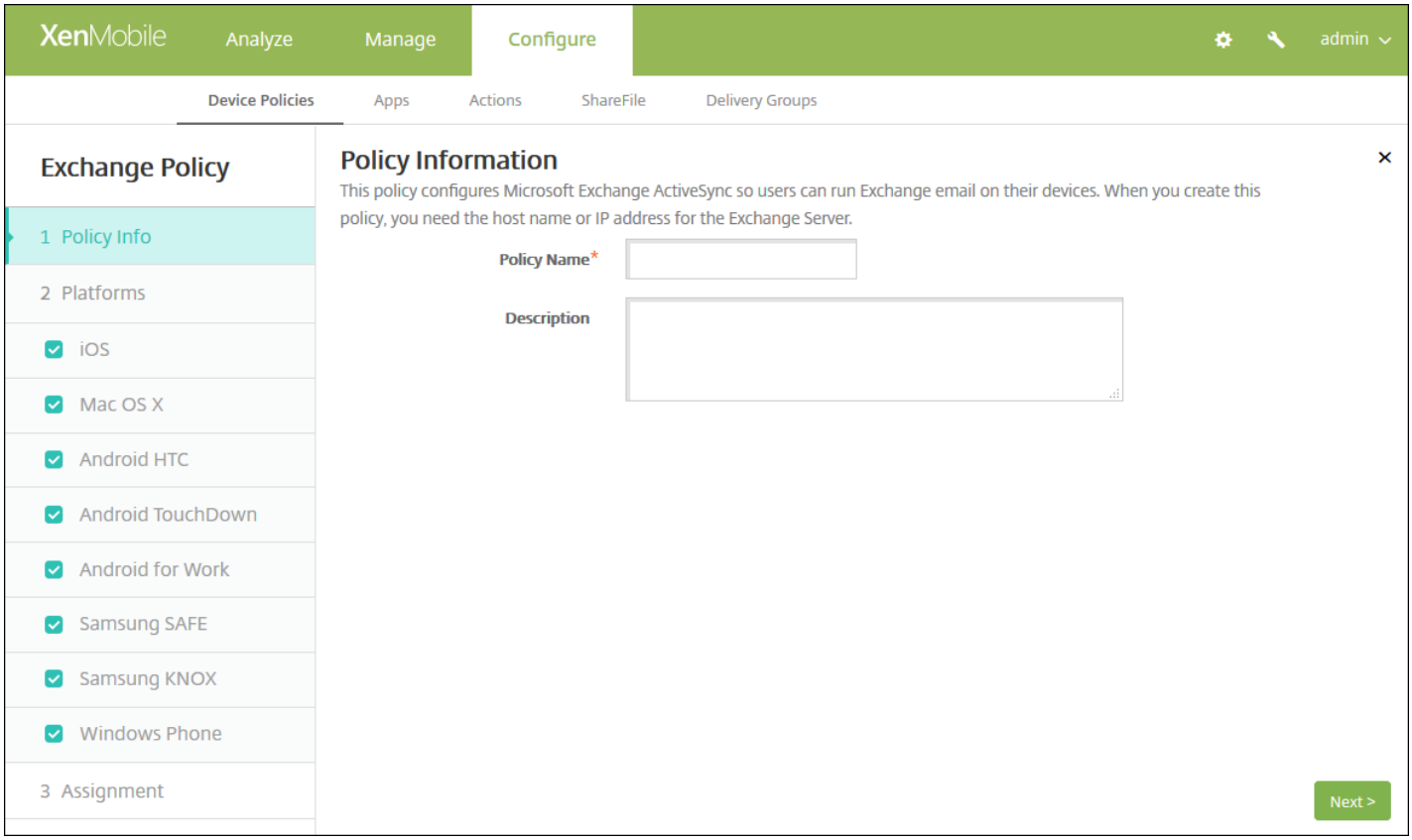
Windows Phone-Einstellungen

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.



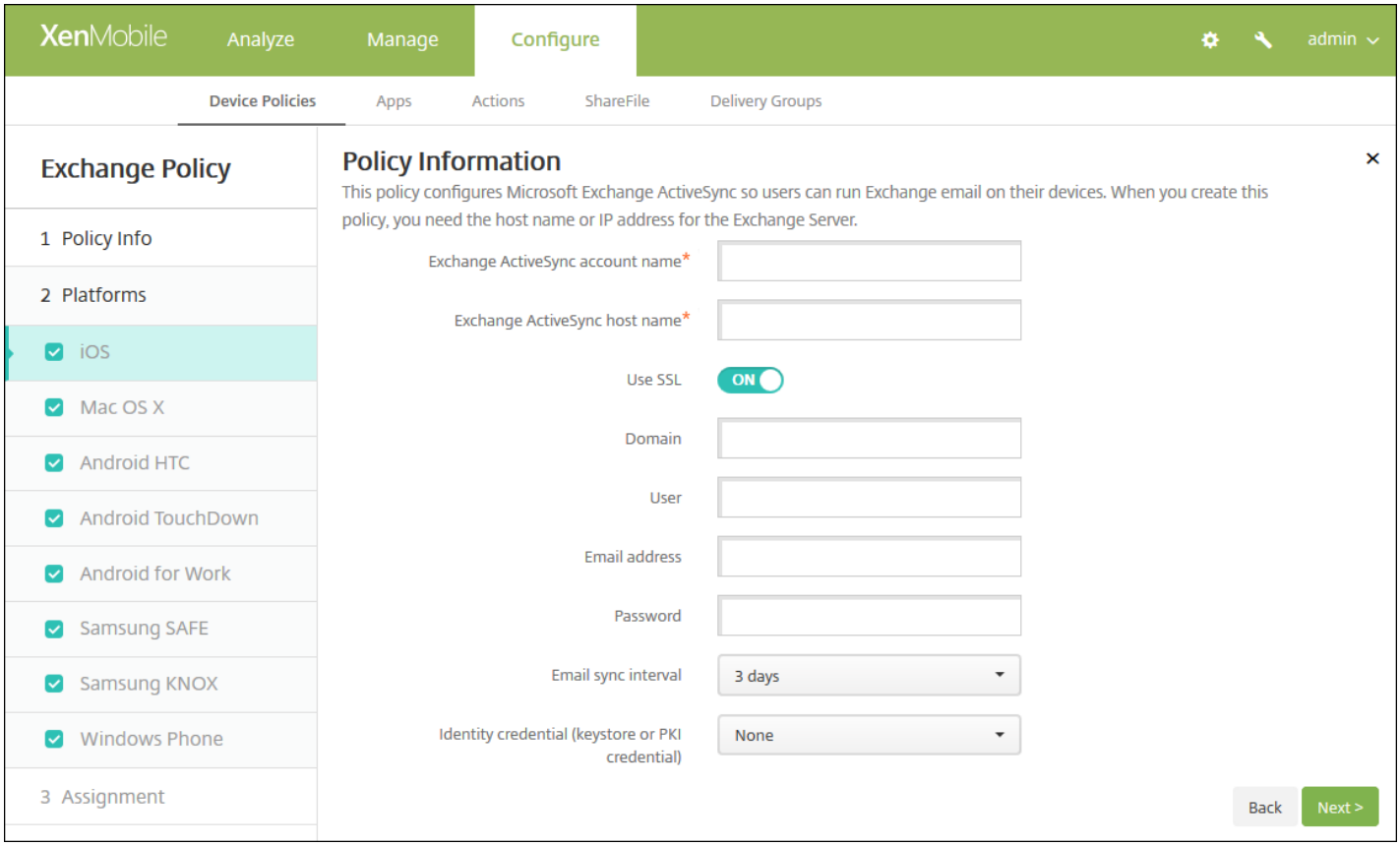
4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

- **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



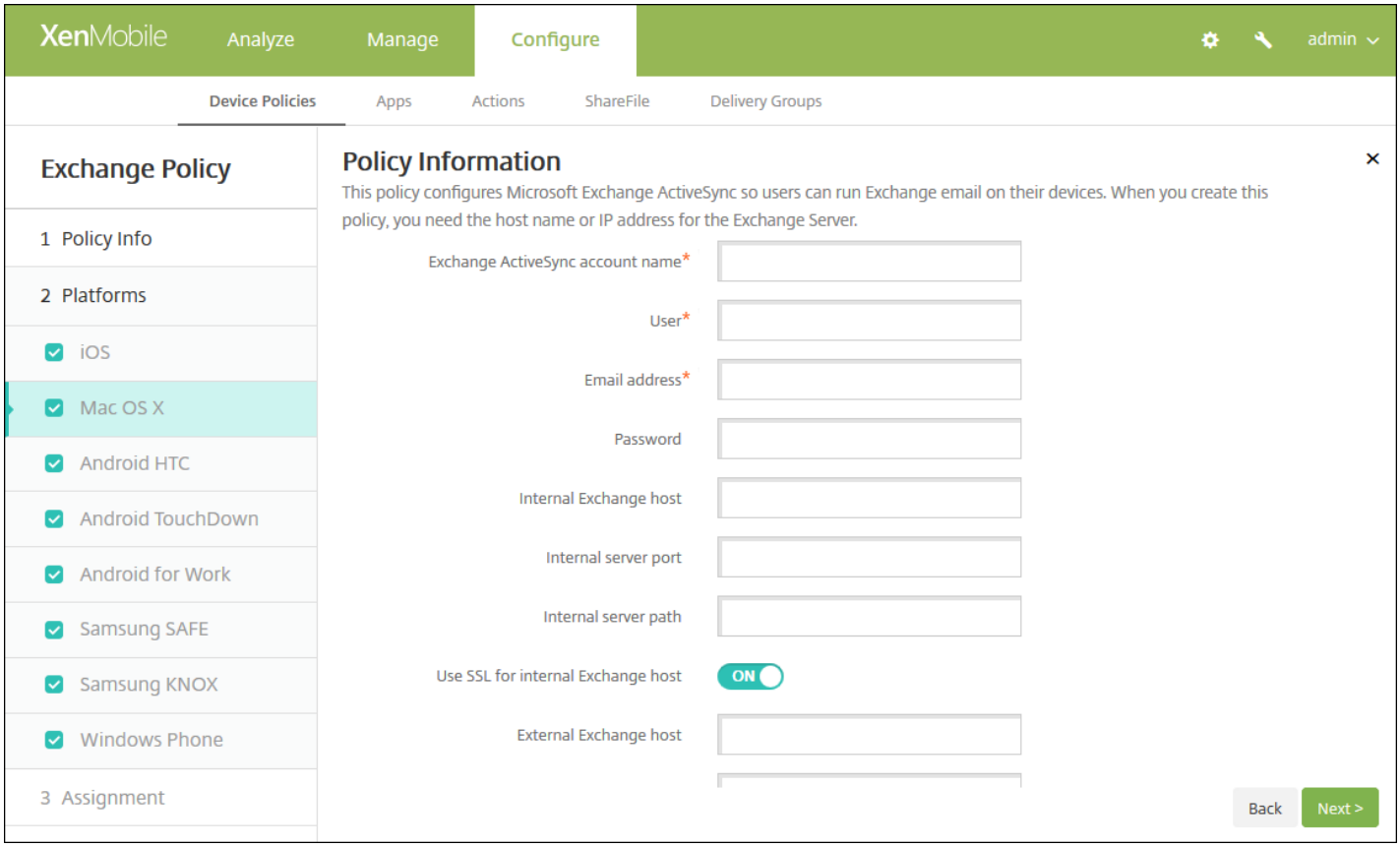
Konfigurieren Sie folgende Einstellungen:

- **Exchange ActiveSync-Kontoname**: Geben Sie die Beschreibung des E-Mail-Kontos ein, die auf den Geräten angezeigt werden soll.
- **Exchange ActiveSync-Hostname**: Geben Sie die Adresse 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 dieser Liste optional auf Identitätsanmeldeinformationen, sofern 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 vor, 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

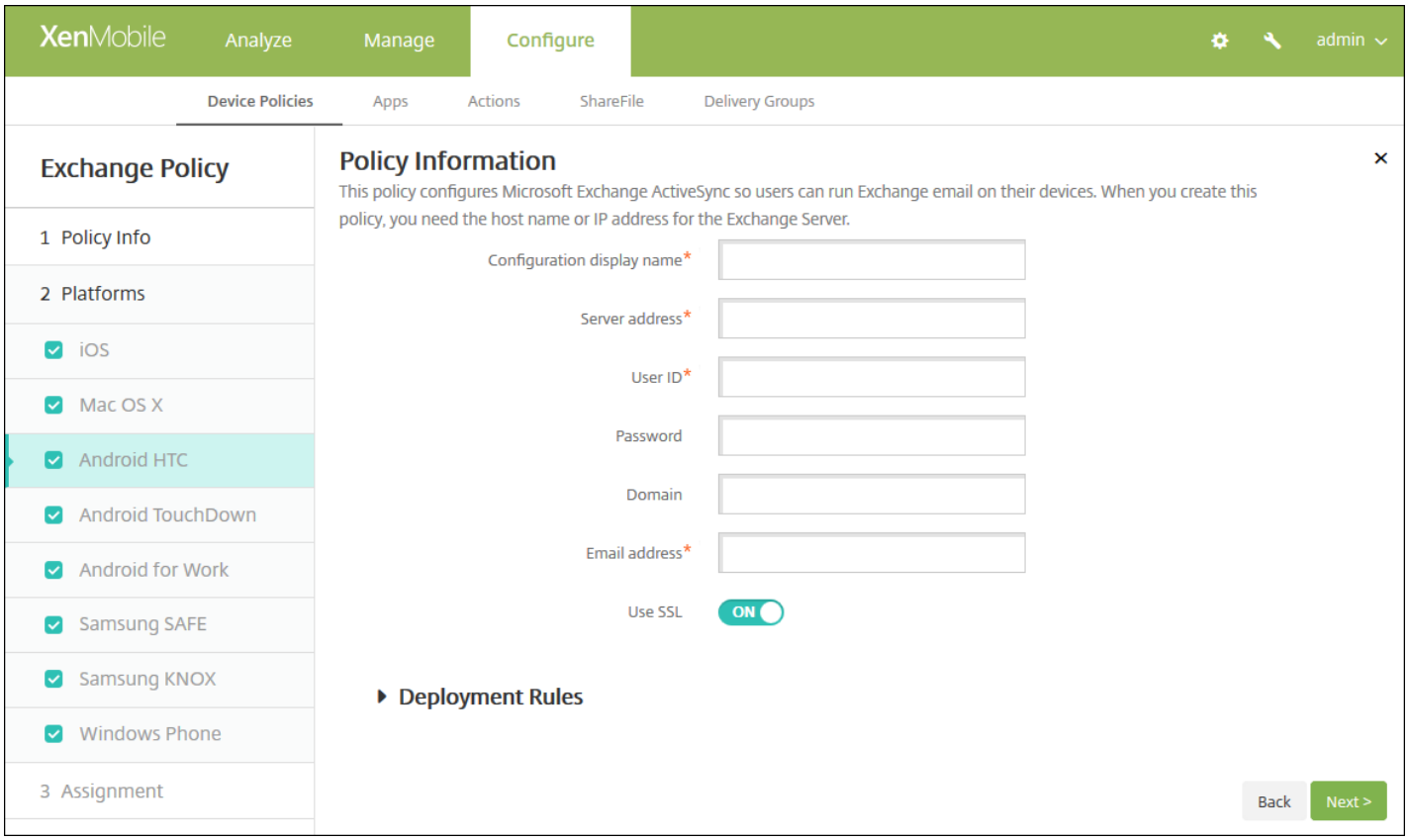


Konfigurieren Sie folgende Einstellungen:

- **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



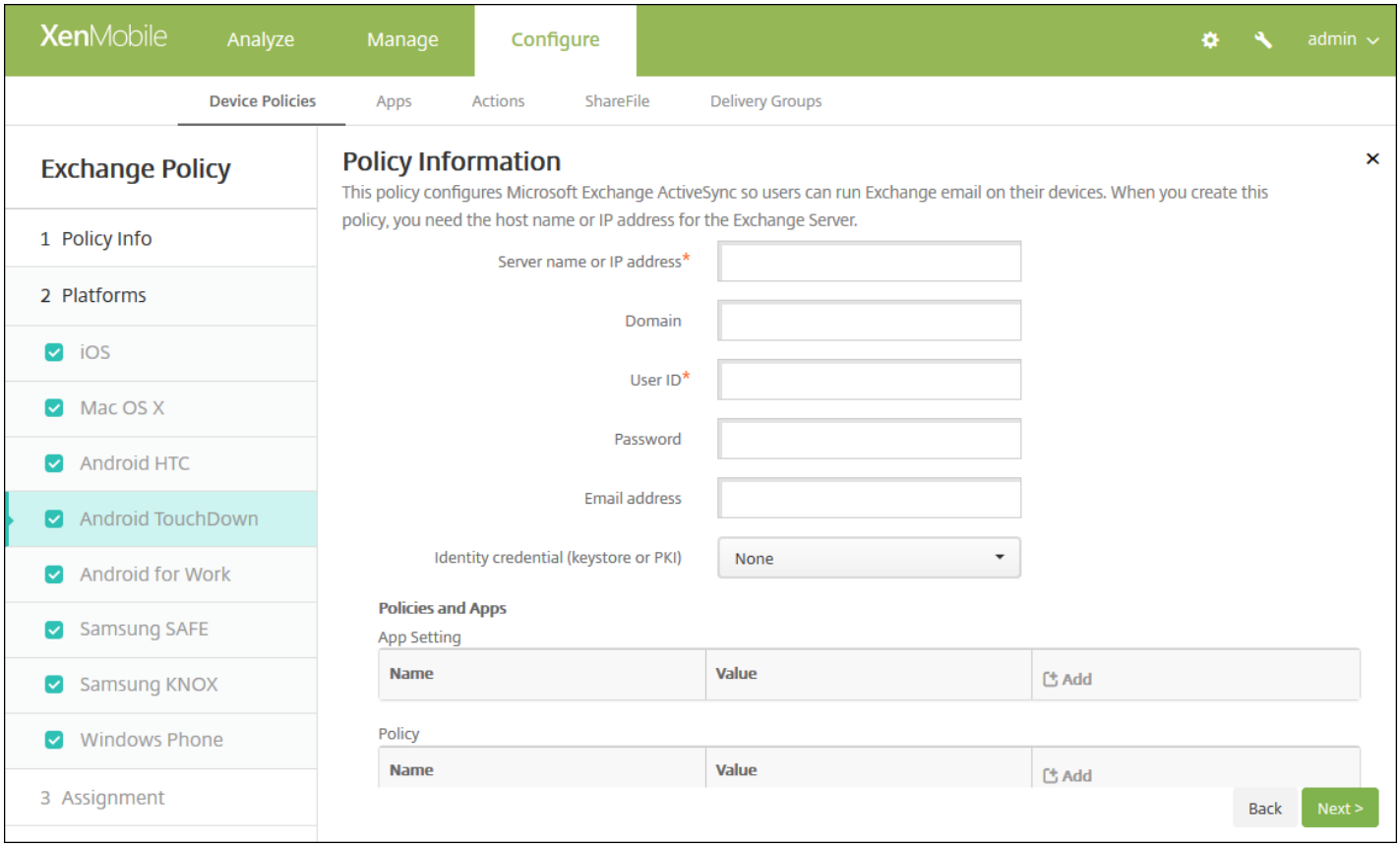
Konfigurieren Sie folgende Einstellungen:

- **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-Servers 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



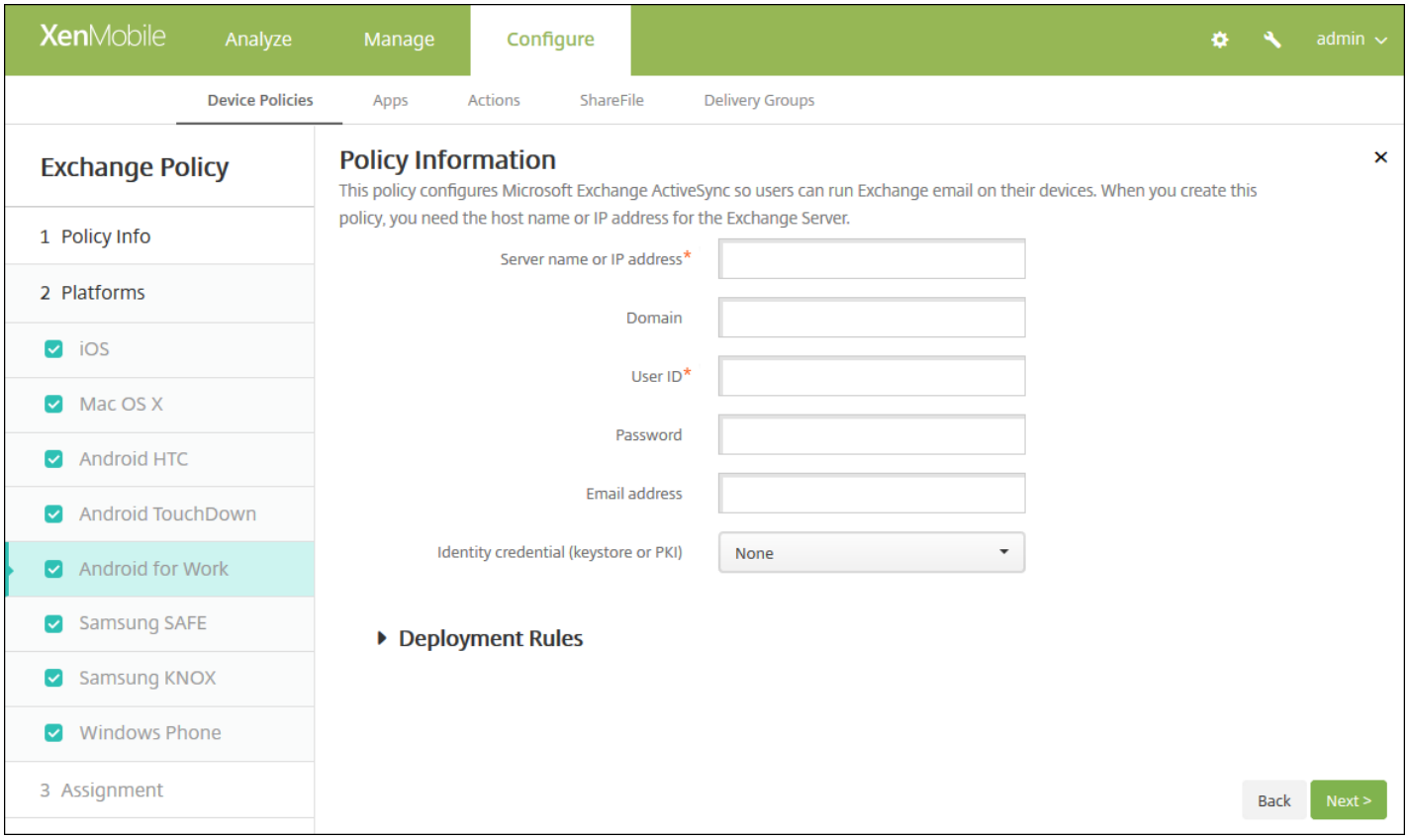
Konfigurieren Sie folgende Einstellungen:

- **Servername oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **Benutzer-ID**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${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 dieser Liste optional auf Identitätsanmeldeinformationen, sofern 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.

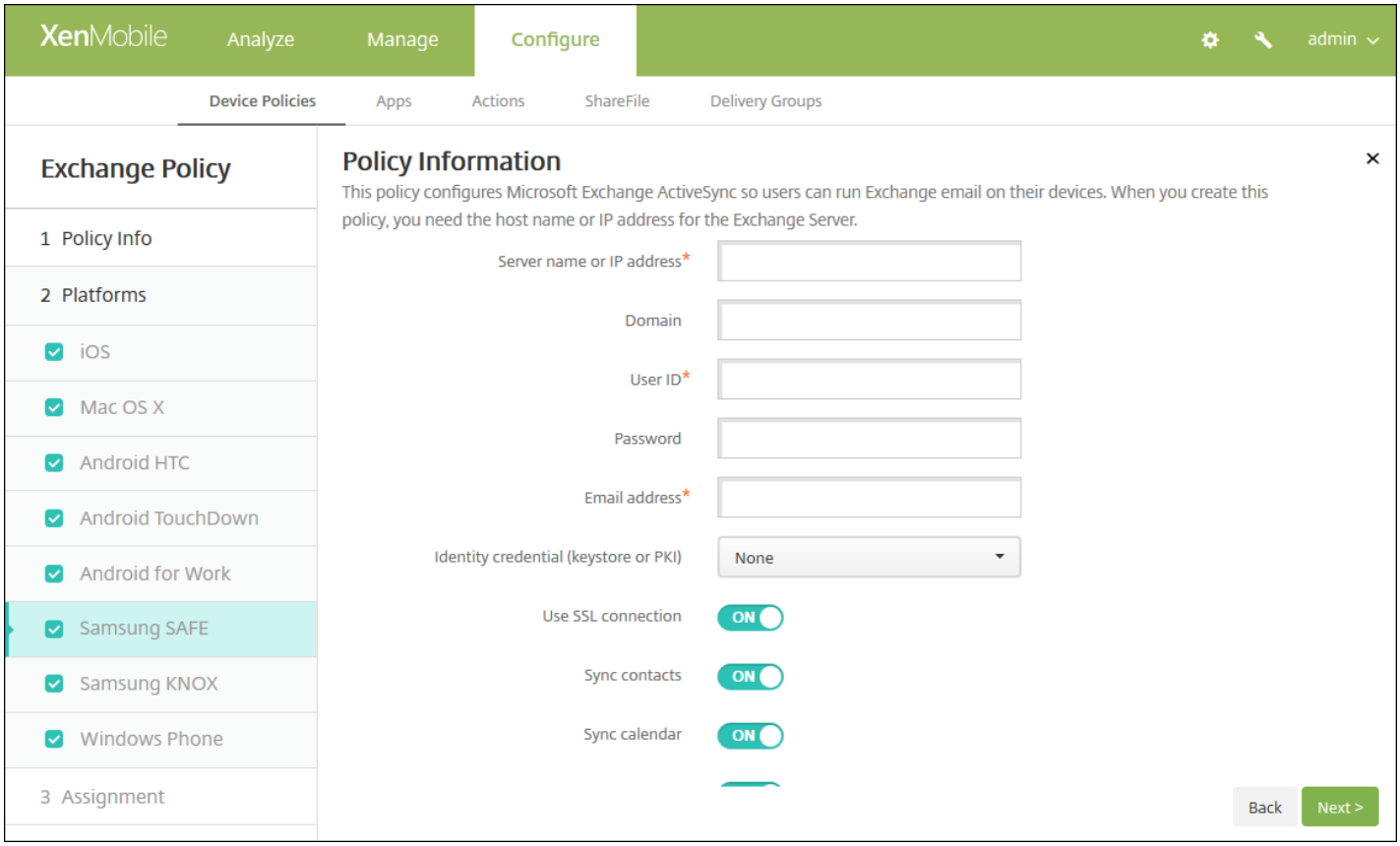
Konfigurieren von Android for Work



Konfigurieren Sie folgende Einstellungen:

- **Servername oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **Benutzer-ID**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${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 dieser Liste optional auf Identitätsanmeldeinformationen, sofern Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert. Der Standardwert ist **Ohne**.

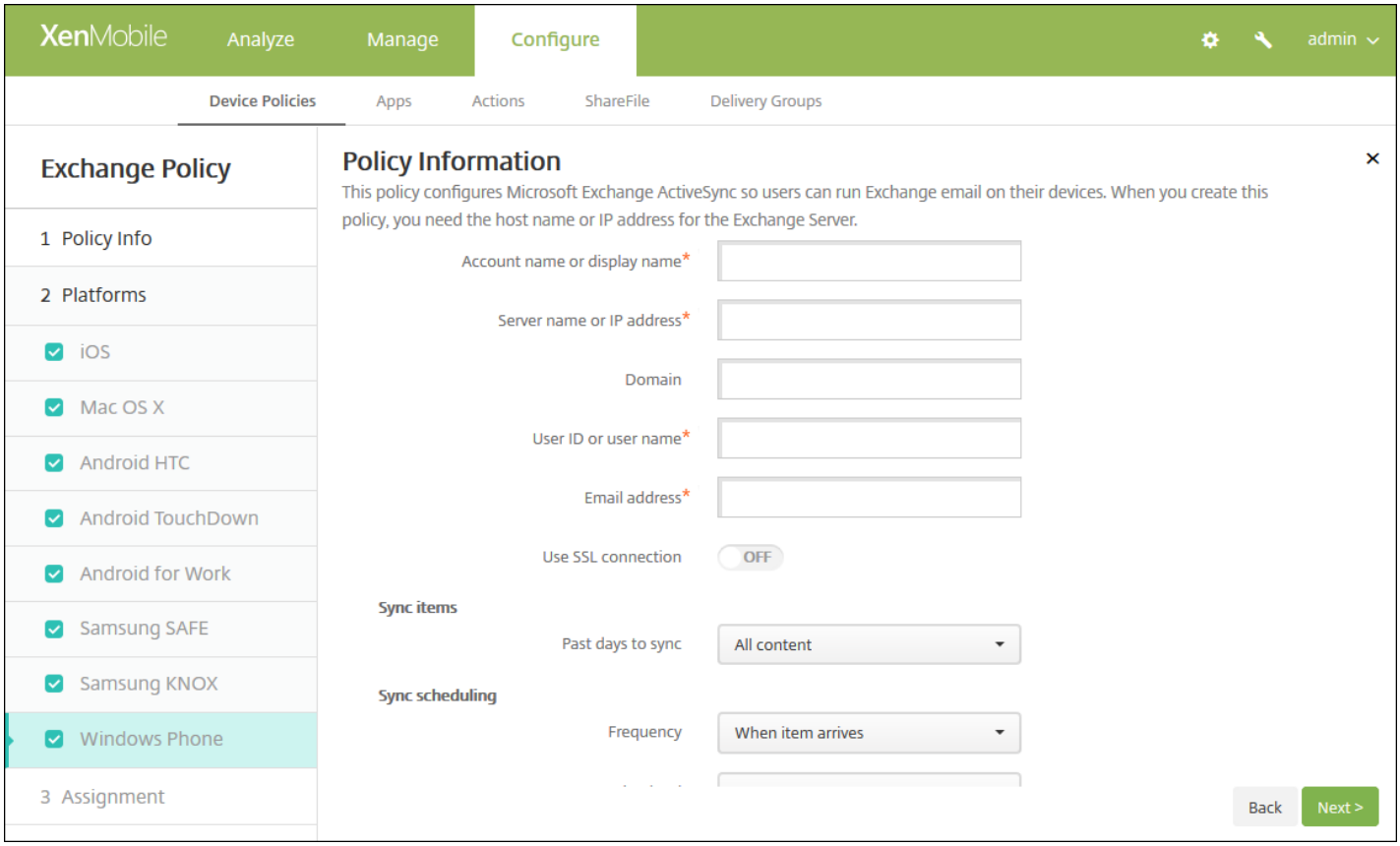
Konfigurieren von Samsung SAFE- und Samsung KNOX-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Servername oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **Benutzer-ID**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${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 dieser Liste optional auf Identitätsanmeldeinformationen, sofern 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**.
- **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



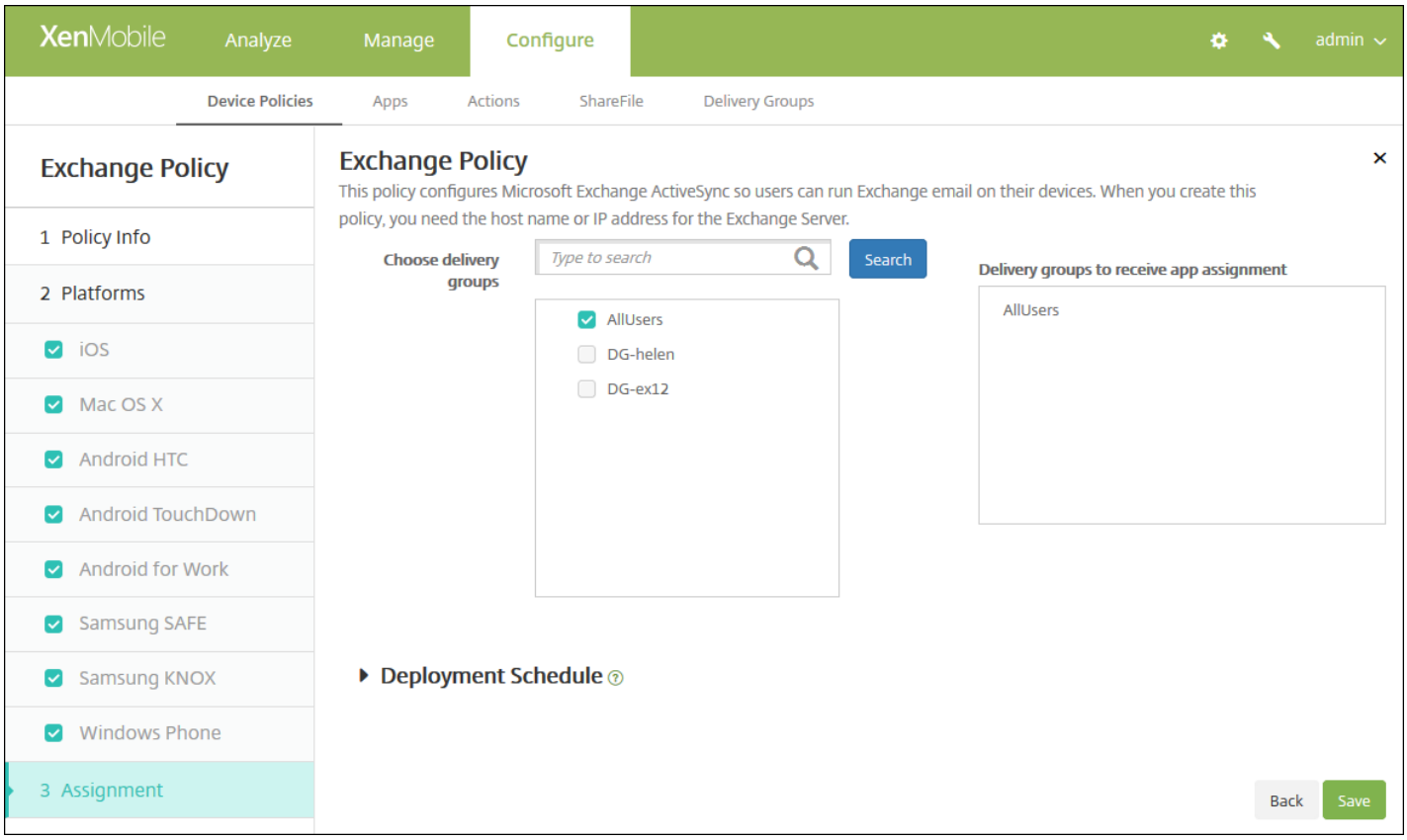
Konfigurieren Sie folgende Einstellungen:

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie für Unternehmensinformationen

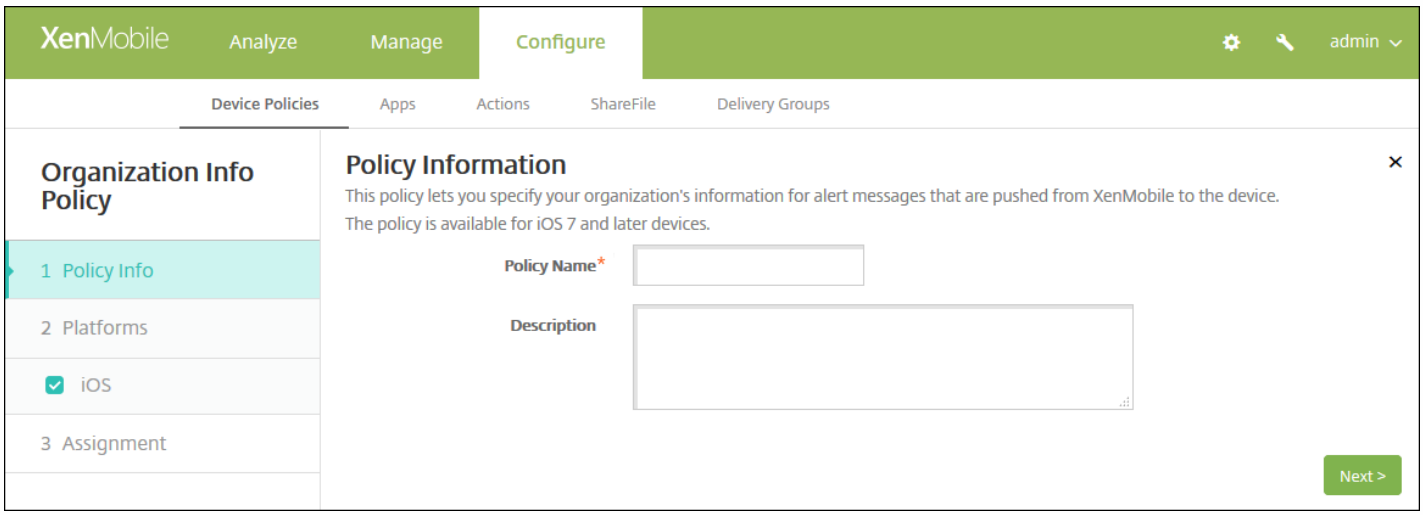
Feb 24, 2017

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.

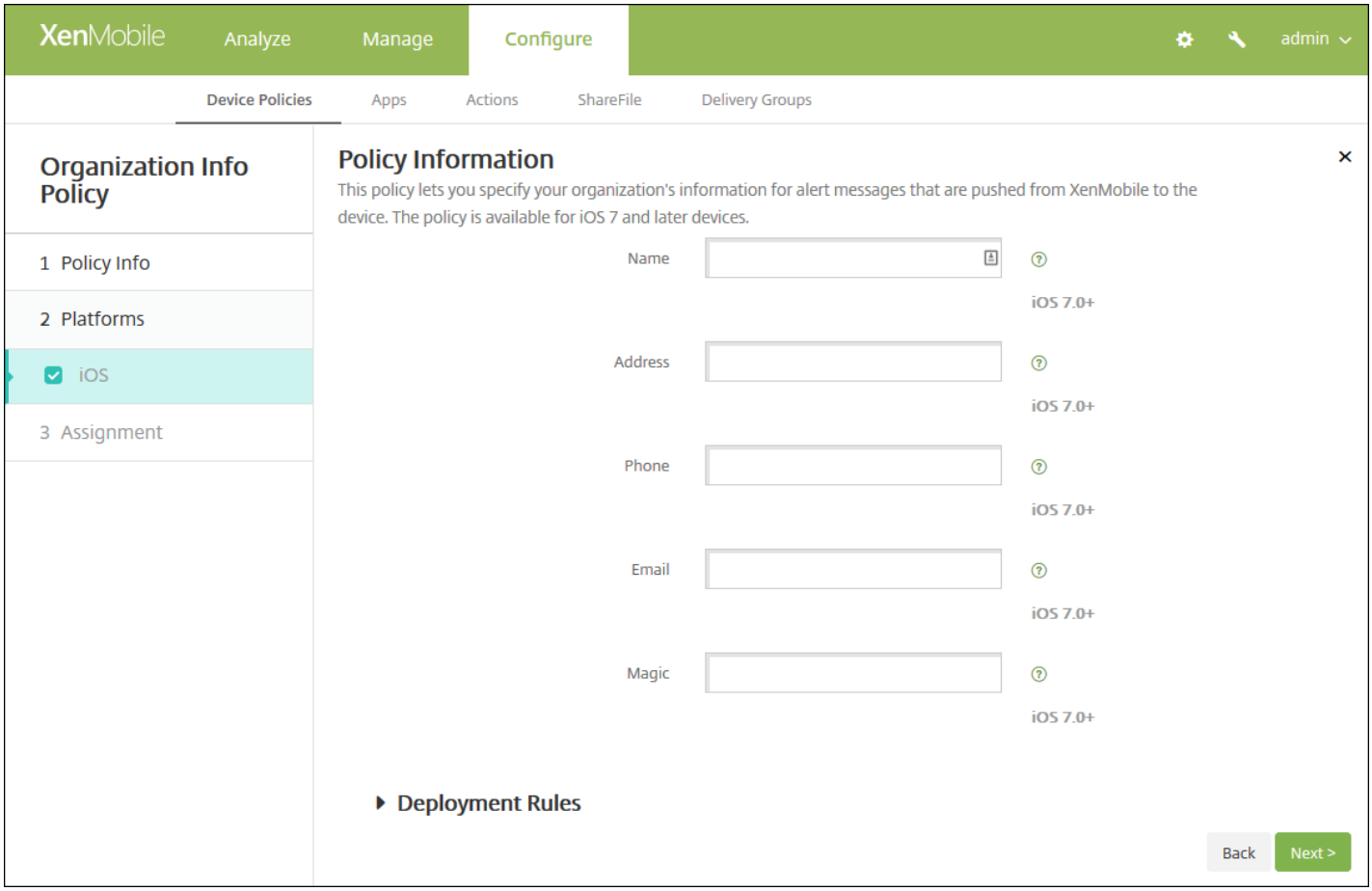
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **Informationen zum Unternehmen**. Die Seite für die Richtlinieninformationen der Richtlinie **Unternehmensinformationen** wird angezeigt.



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.

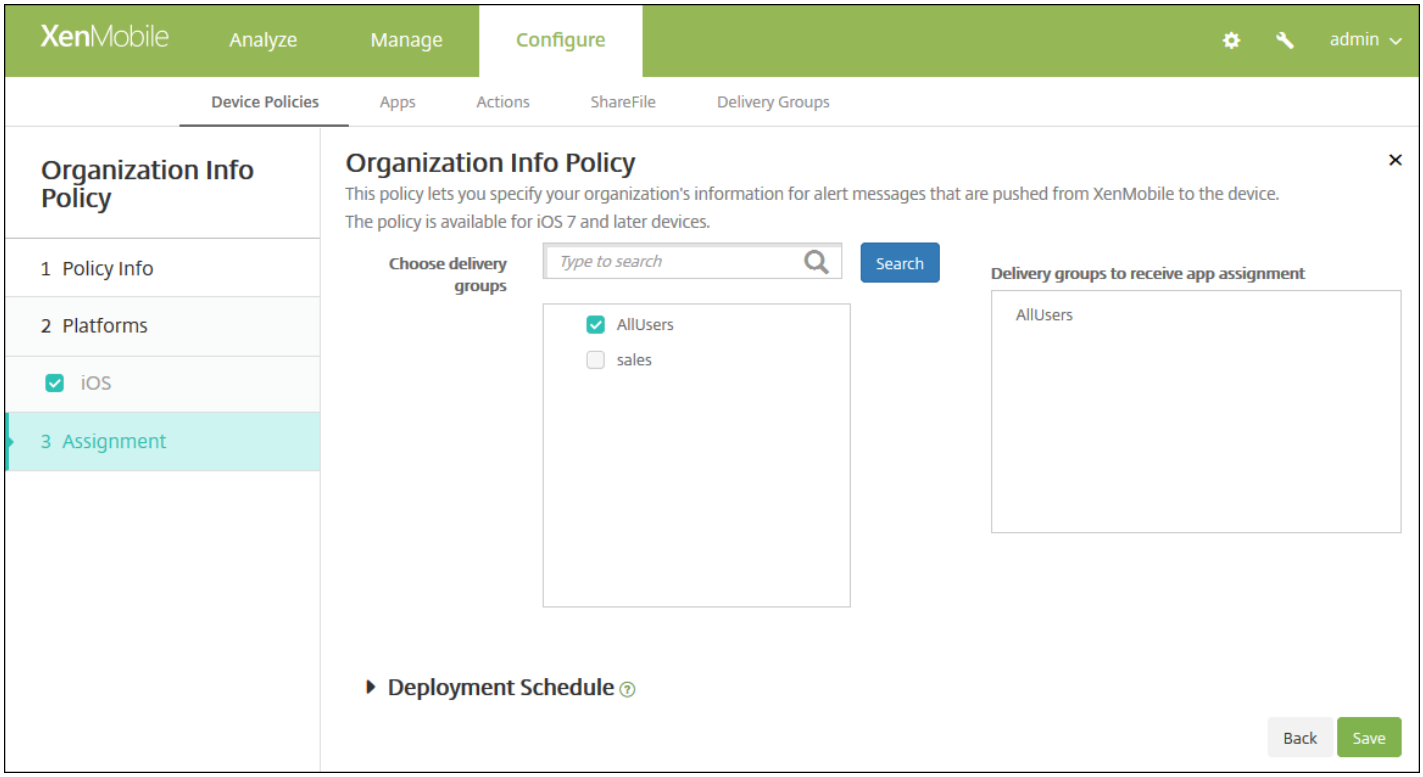


Konfigurieren Sie folgende Einstellungen:

- **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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Passcoderichtlinien für Geräte

Feb 24, 2017

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

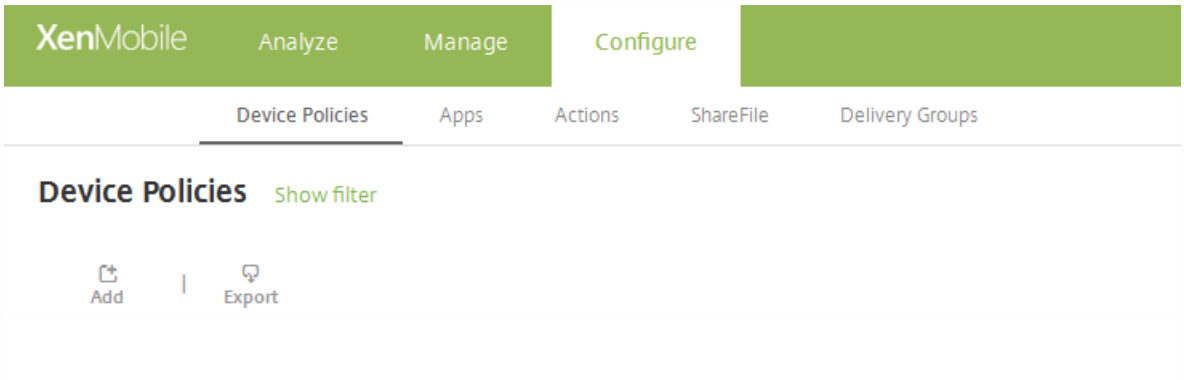
Samsung KNOX-Einstellungen

Android for Work-Einstellungen

Windows Phone-Einstellungen

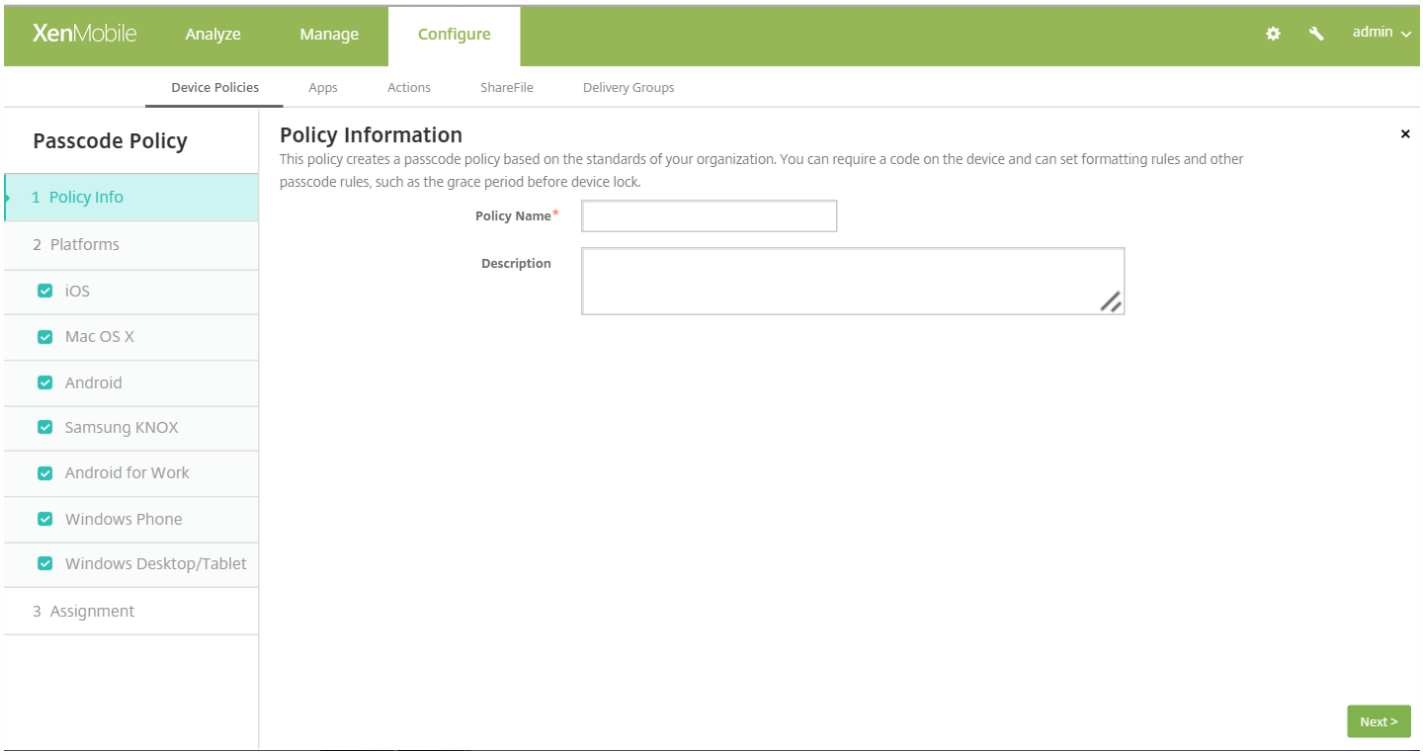
Windows Desktop/Tablet-Einstellungen

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:

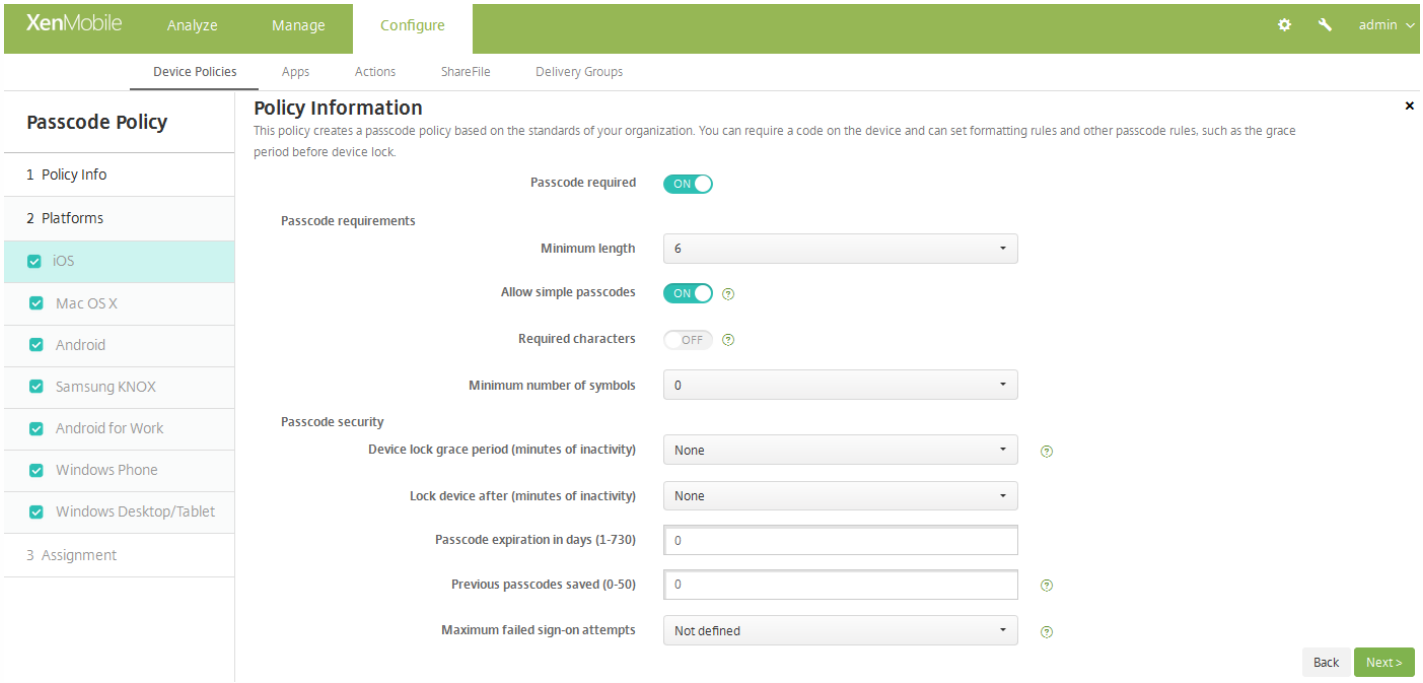
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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

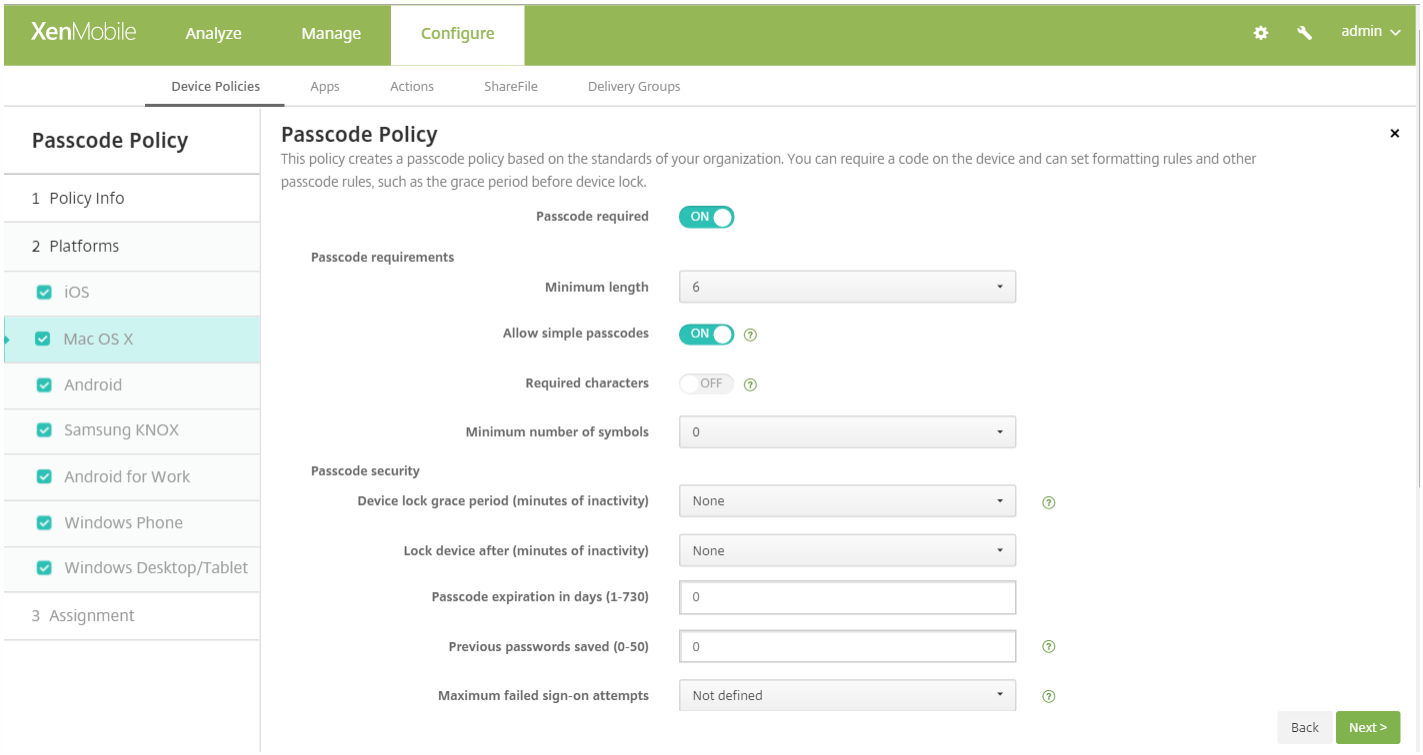


Konfigurieren Sie die folgenden Einstellungen:

- **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



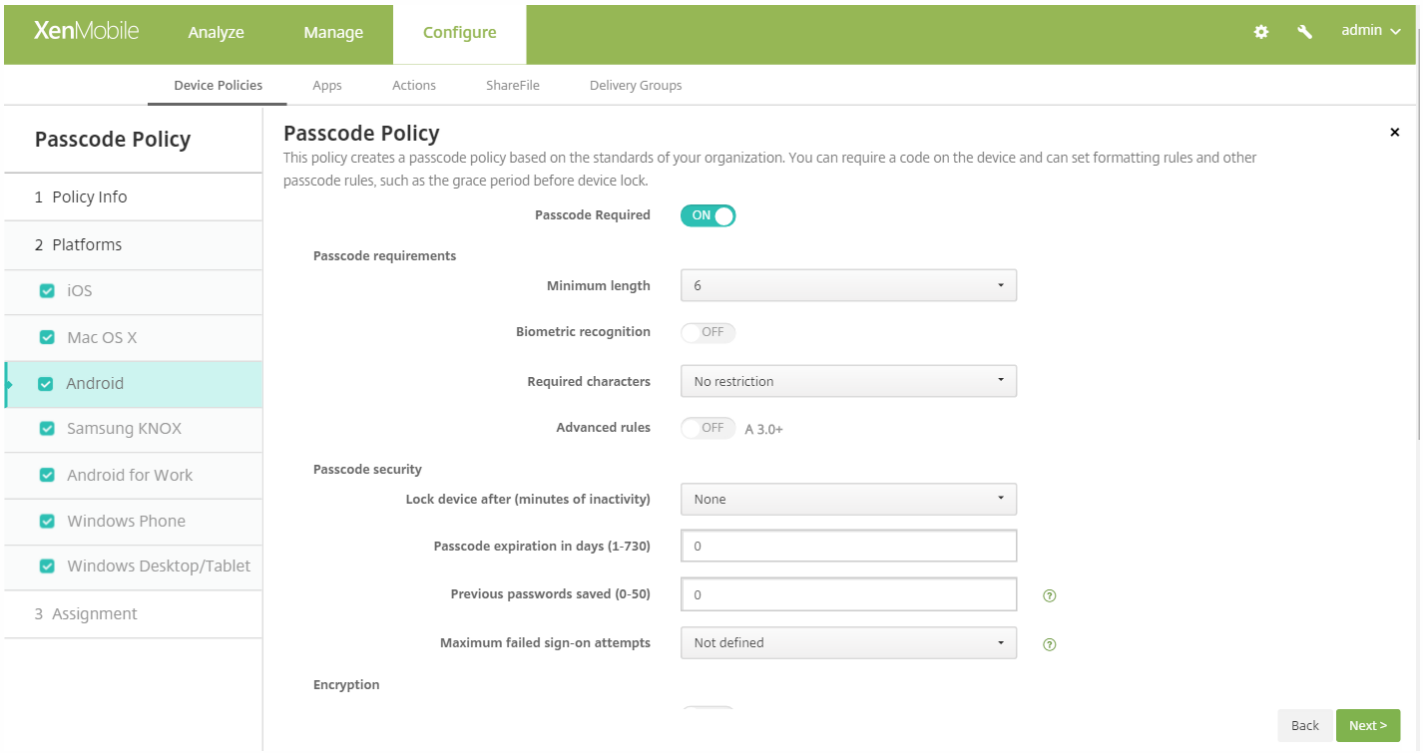
Konfigurieren Sie folgende Einstellungen:

- **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. 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 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.

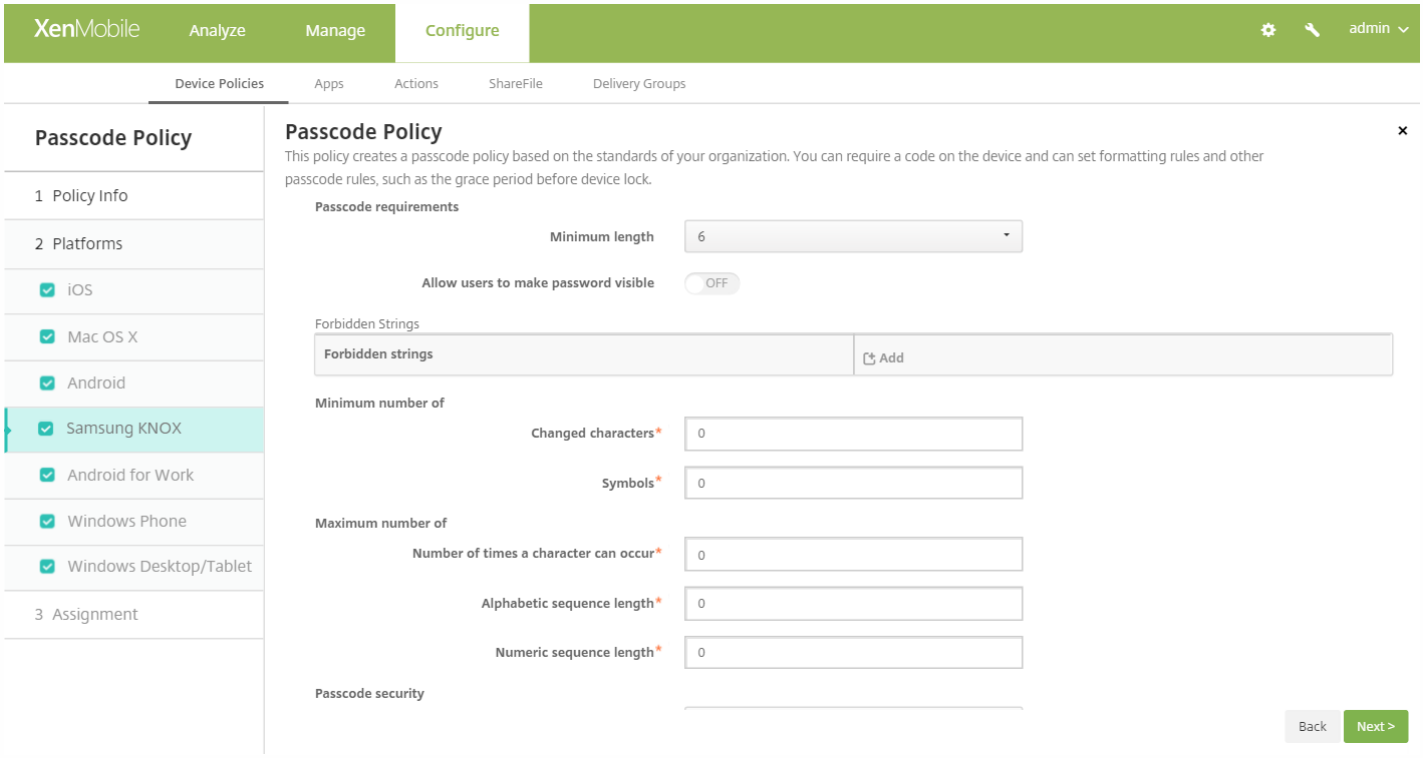
- **Samsung SAFE**
  - **Gleichen Passcode für alle Benutzer verwenden**: Wählen Sie aus, ob der gleiche Passcode für alle Benutzer verwendet werden soll. Der Standardwert ist **AUS**. Diese Einstellung gilt nur für Samsung SAFE-Geräte und ist unabhängig von der Einstellung für **Passcode erforderlich** 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. Der Standardwert 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. 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.

Konfigurieren der Samsung KNOX-Einstellungen



Konfigurieren Sie folgende Einstellungen:

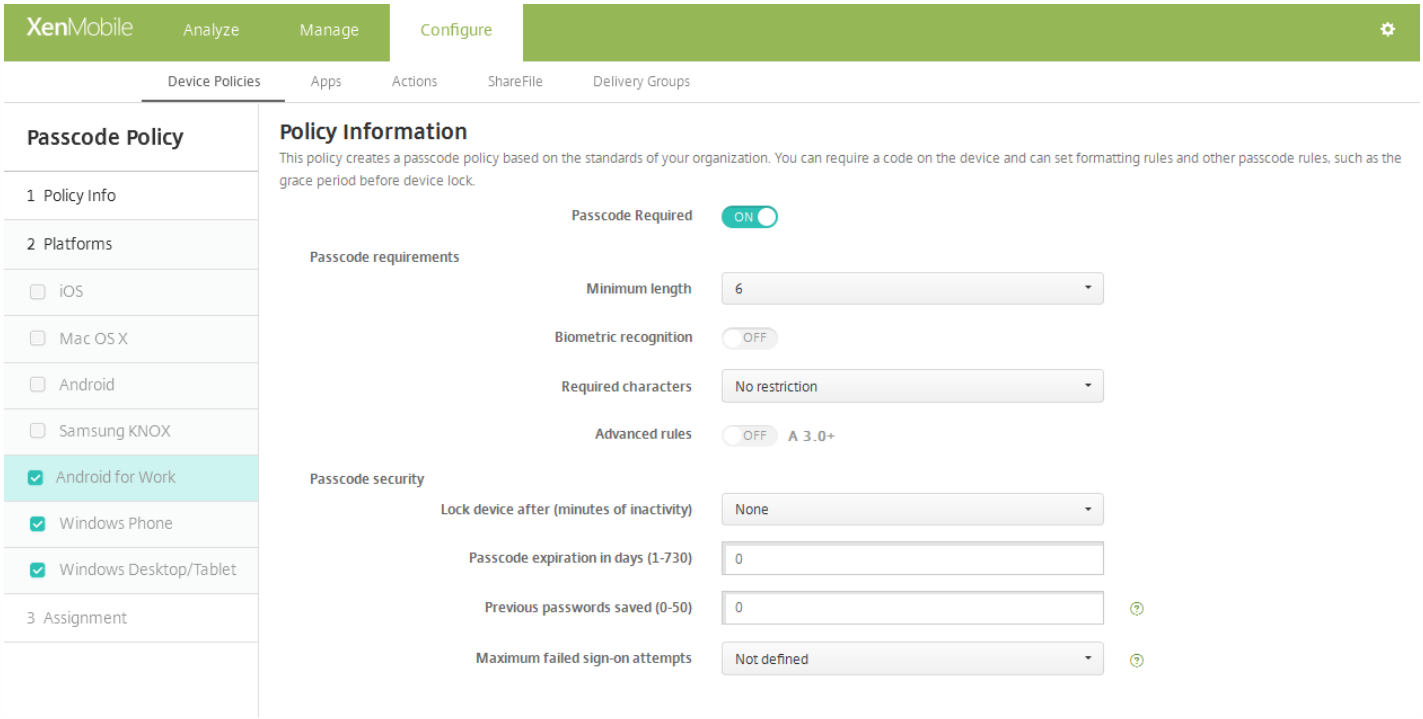
- **Passcodeanforderungen**
  - **Mindestlänge**: Klicken Sie in der Liste auf die Mindestlänge für den Passcode. Der Standardwert ist **6**.
  - **Benutzer dürfen Kennwort anzeigen**: Wählen Sie aus, ob Benutzern das Anzeigen des Kennworts ermöglicht werden soll.
  - **Verbotene Zeichenfolgen**: Durch 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

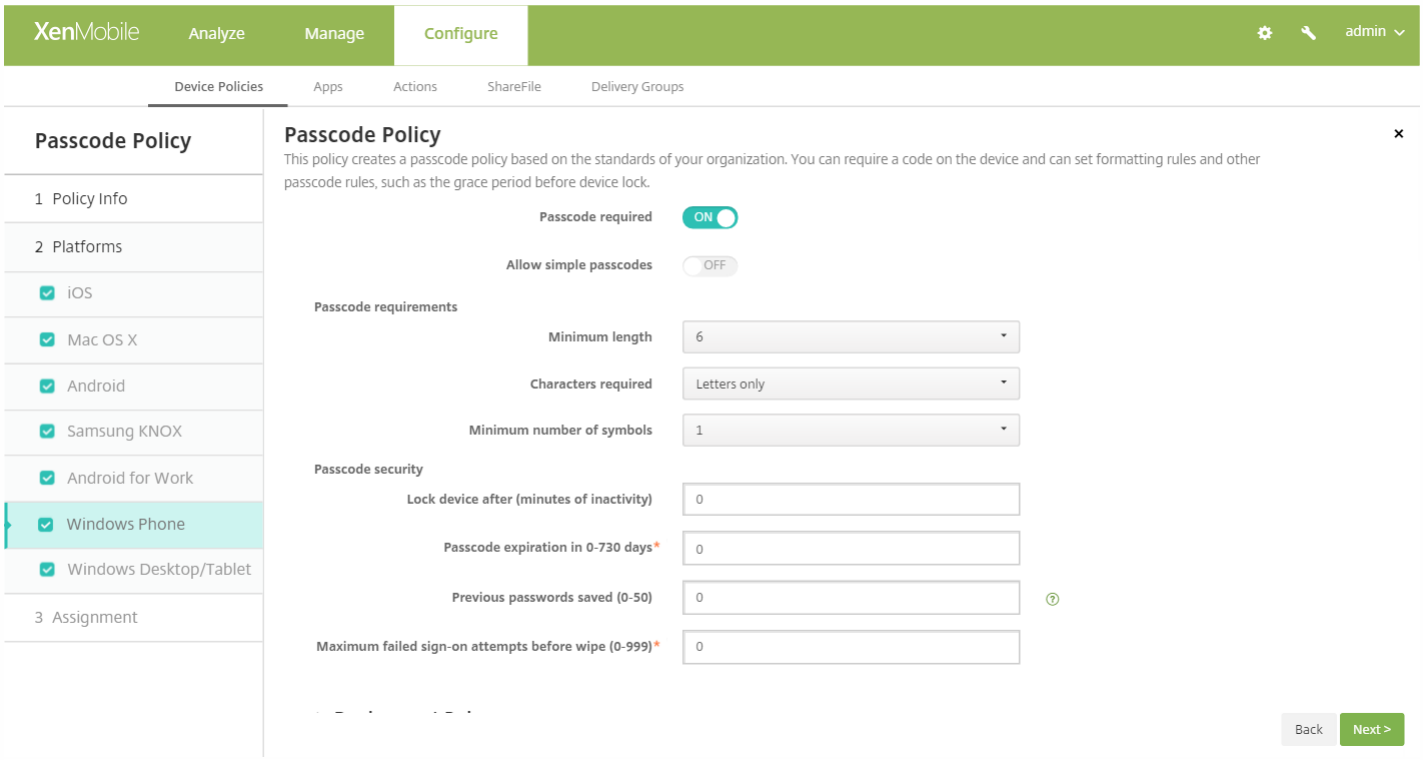


Konfigurieren Sie folgende Einstellungen:

- **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

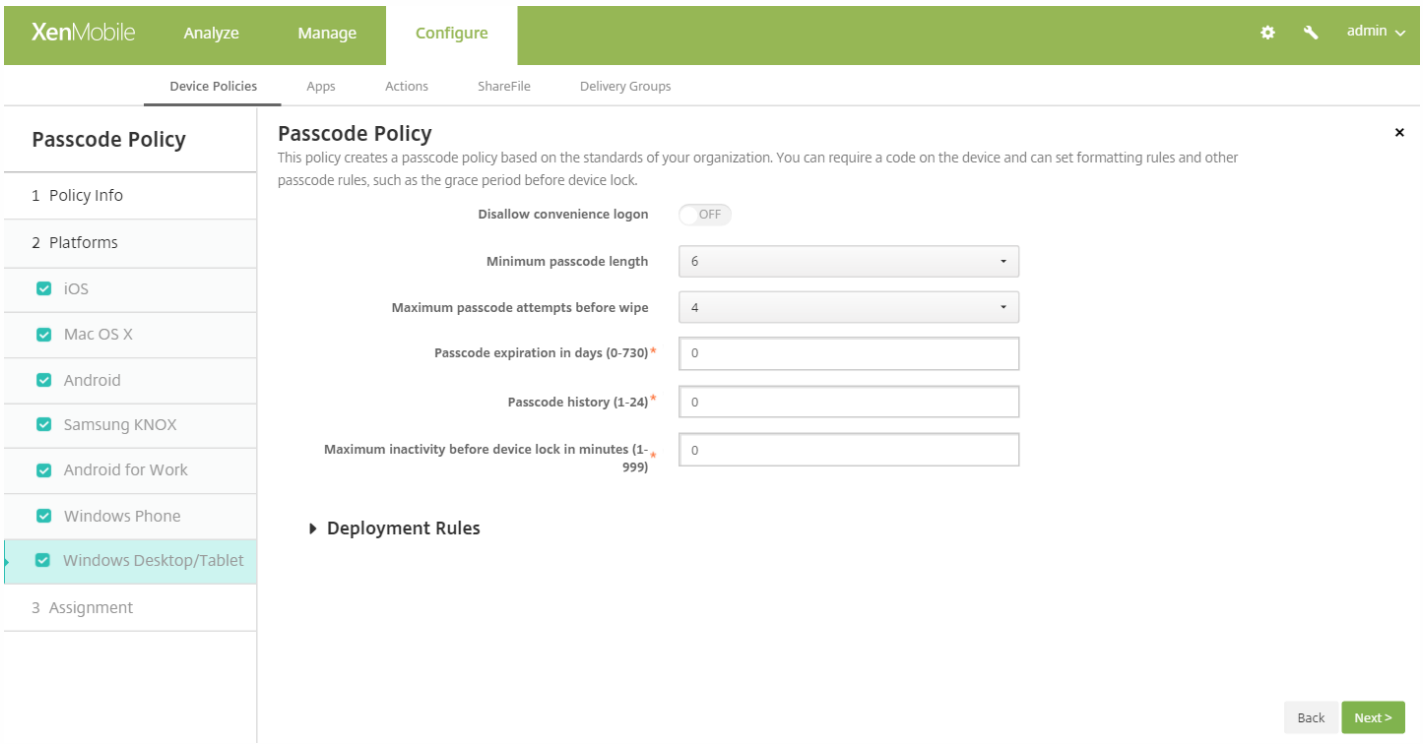


Konfigurieren Sie folgende Einstellungen:

- **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

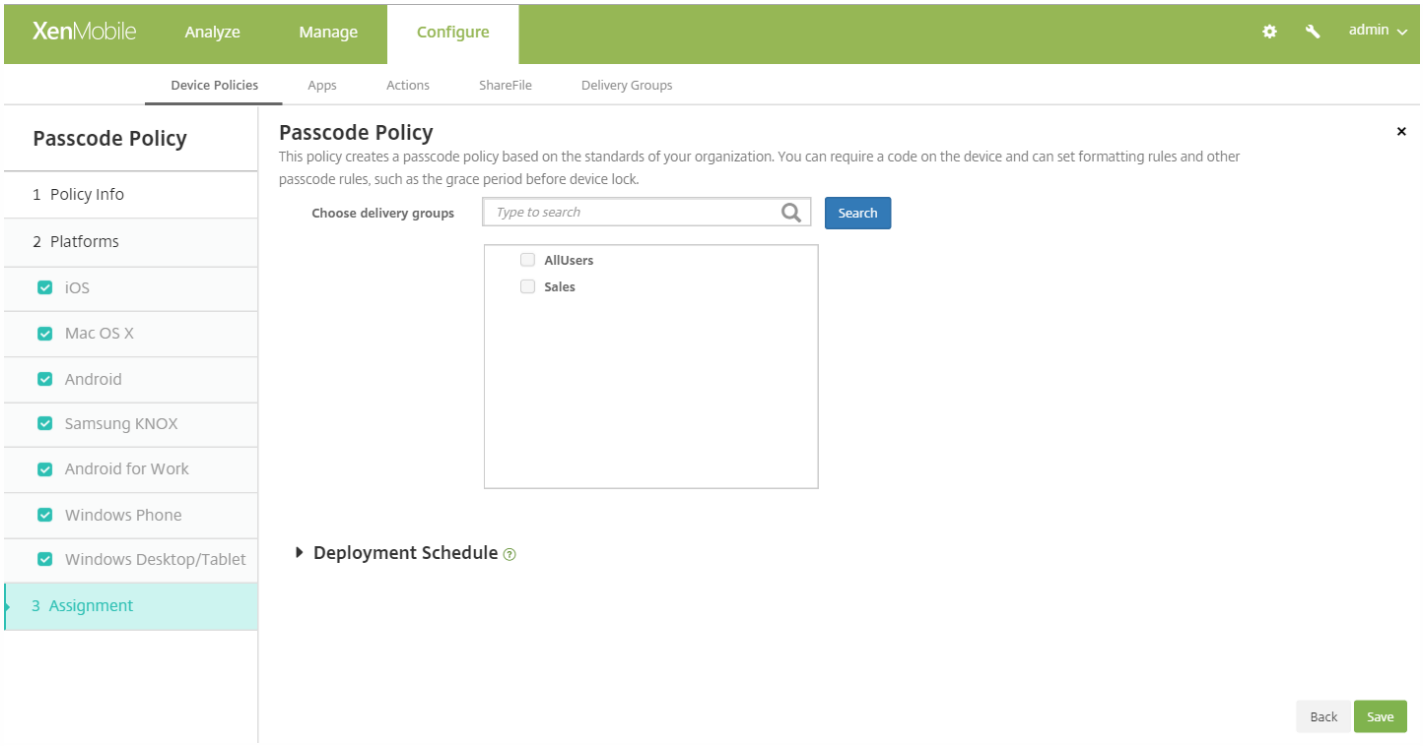


Konfigurieren Sie folgende Einstellungen:

- **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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Richtlinien für persönliche Hotspots

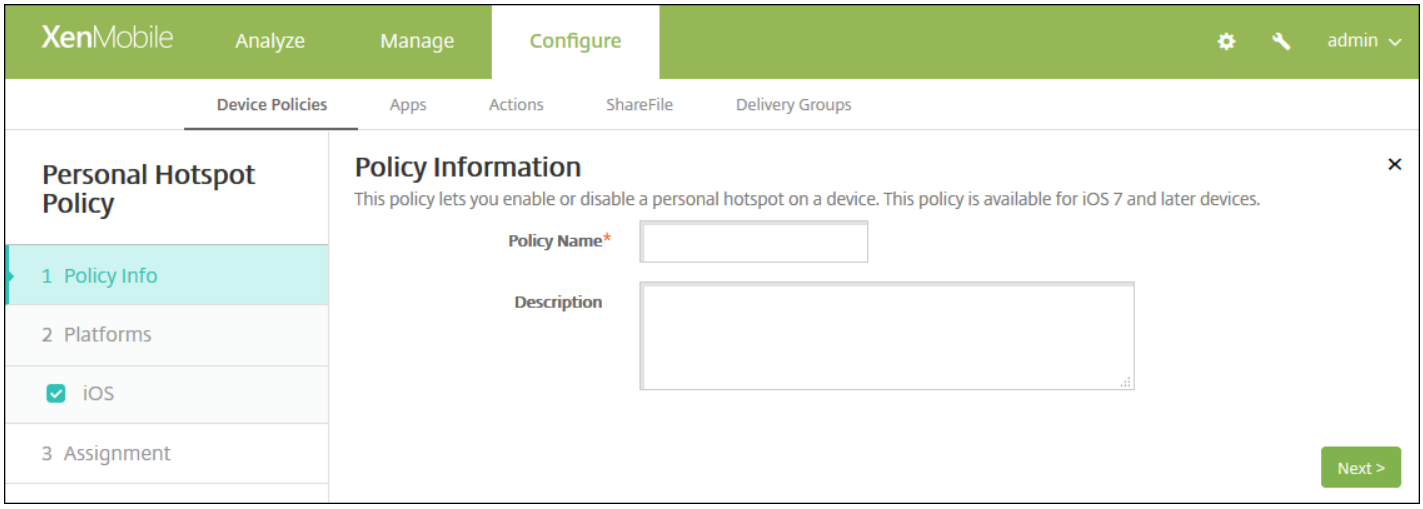
Feb 24, 2017

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.

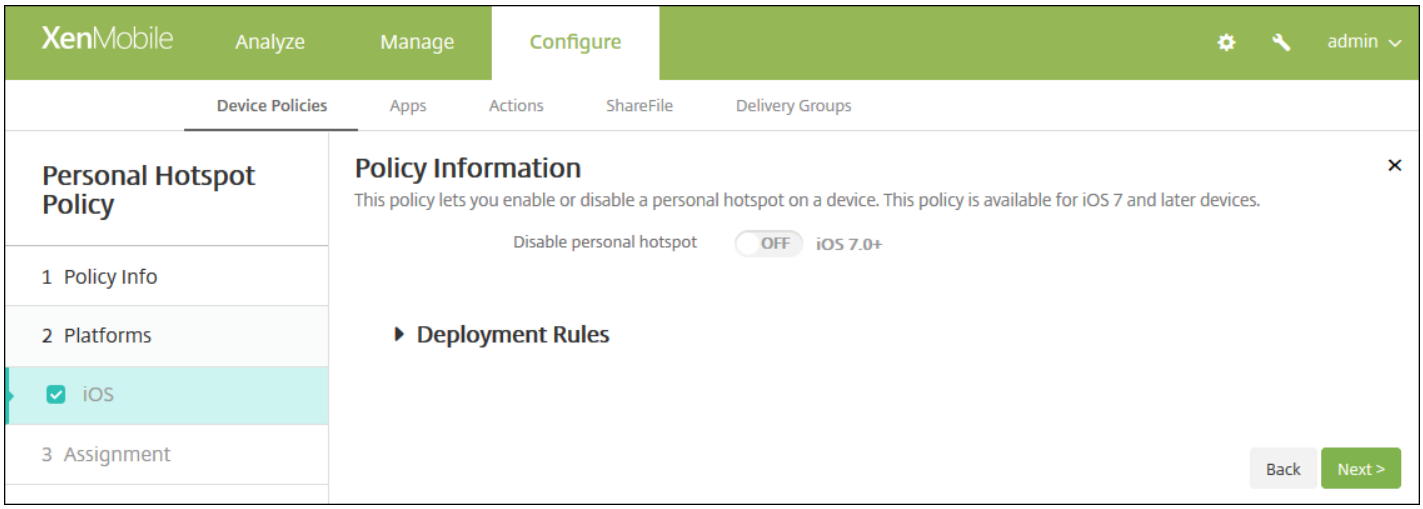
3. Erweitern Sie **Mehr** und klicken Sie unter **Netzwerkzugriff** auf **Persönlicher Hotspot**. Die Seite **Persönlicher Hotspot** wird angezeigt.



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.

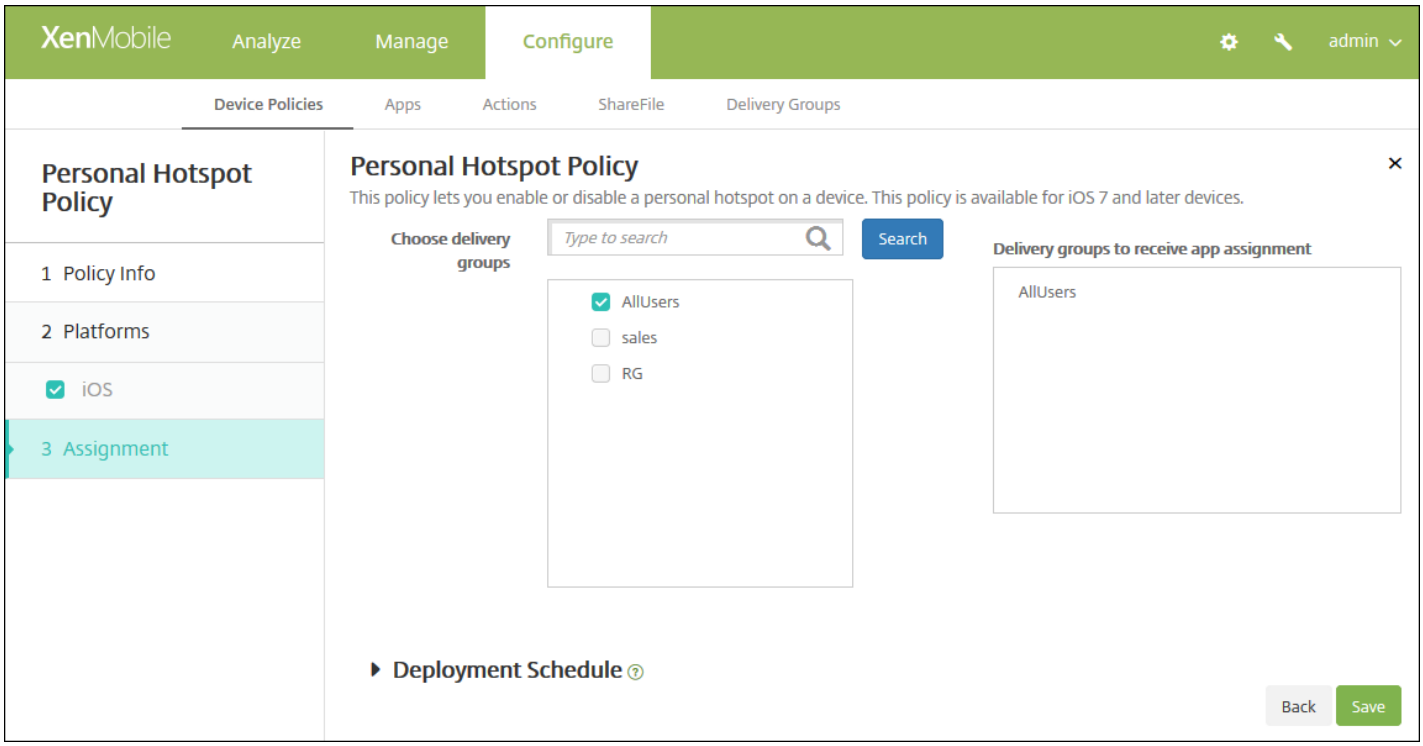


6. Konfigurieren Sie folgende Einstellung:

- **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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Richtlinien zum Entfernen von Profilen

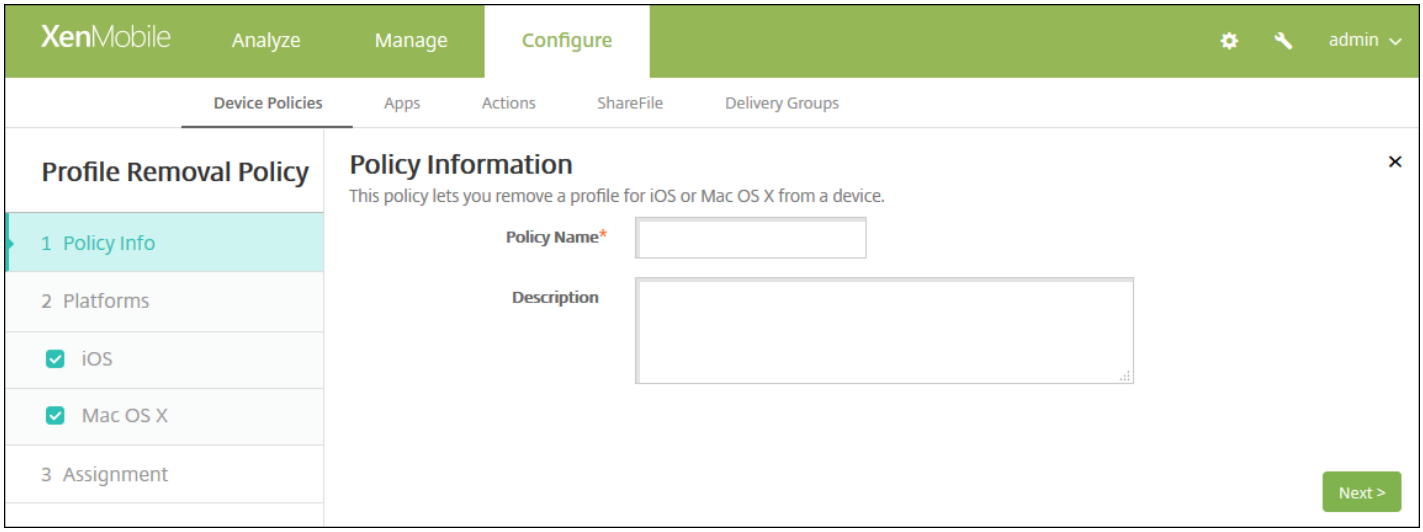
Feb 24, 2017

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:

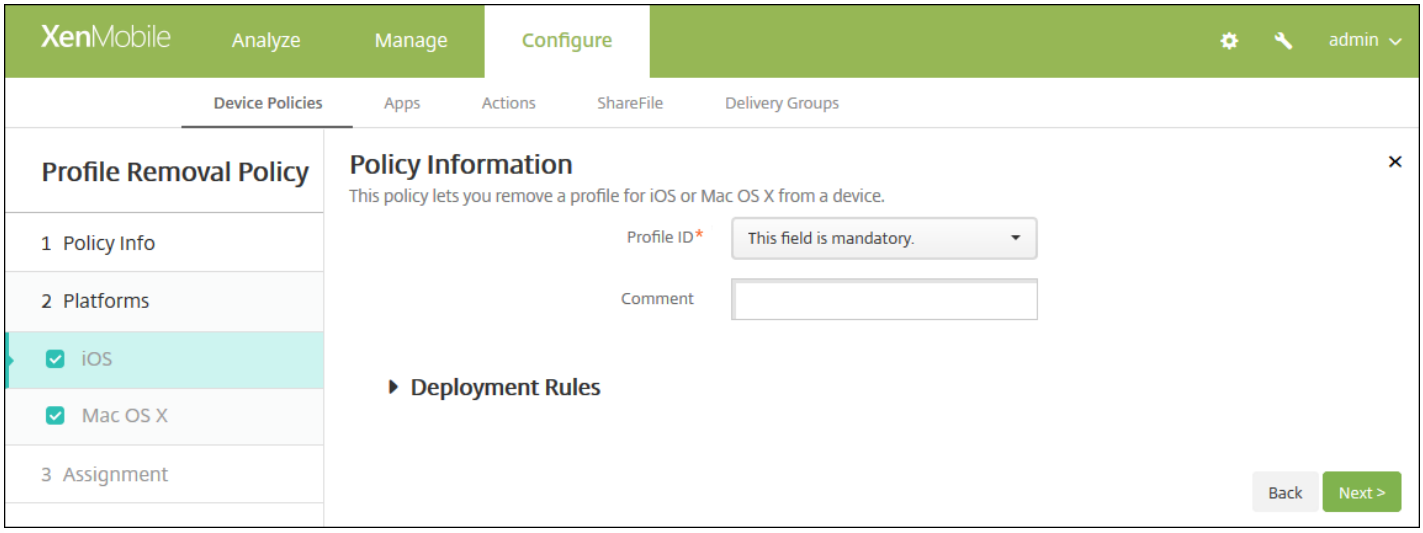
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

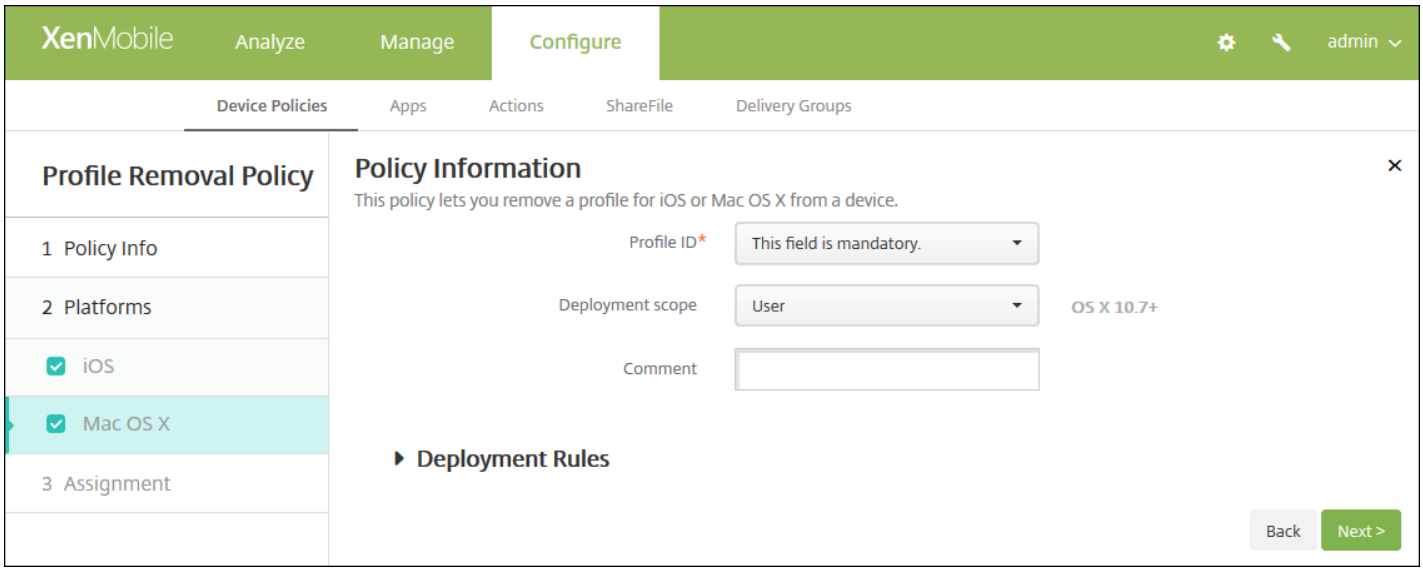
Konfigurieren der iOS-Einstellung



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

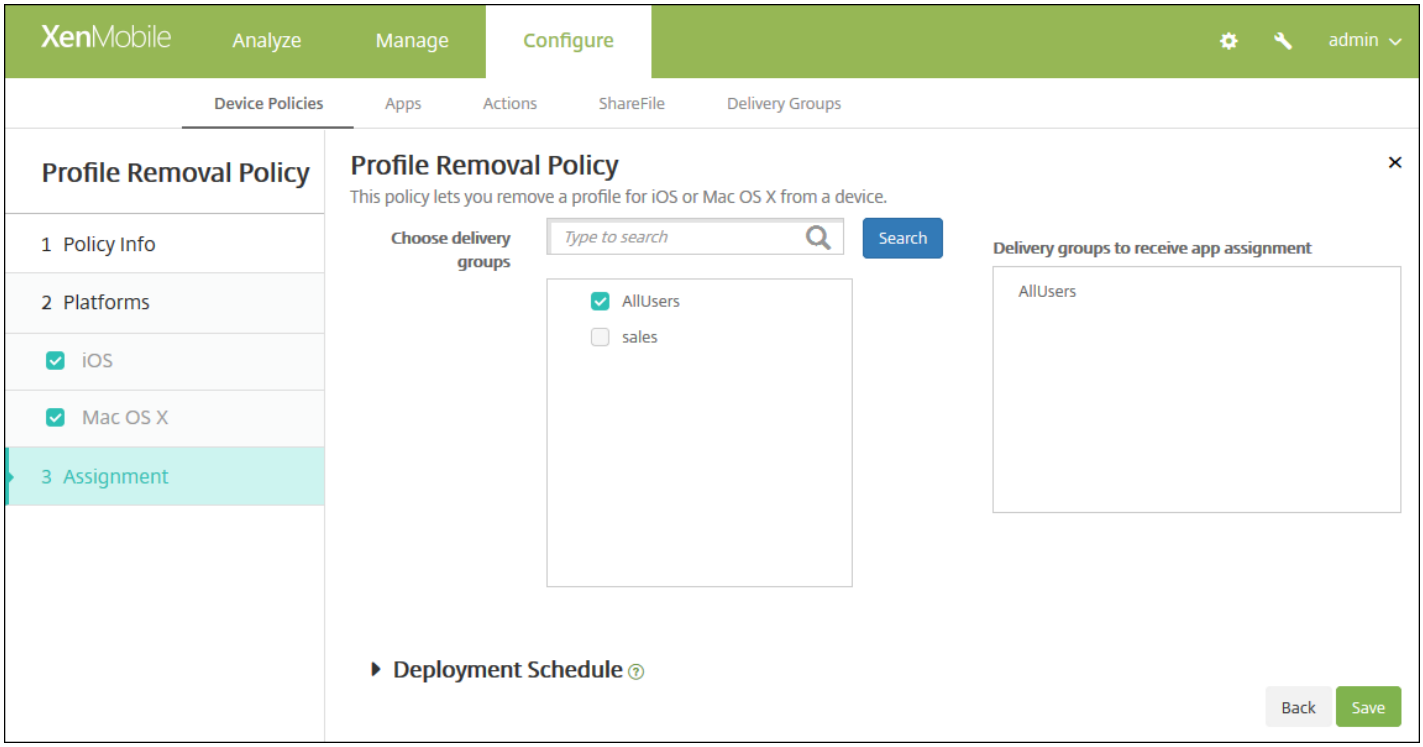


Konfigurieren Sie folgende Einstellungen:

- **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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Provisioningprofilrichtlinie

Feb 24, 2017

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.

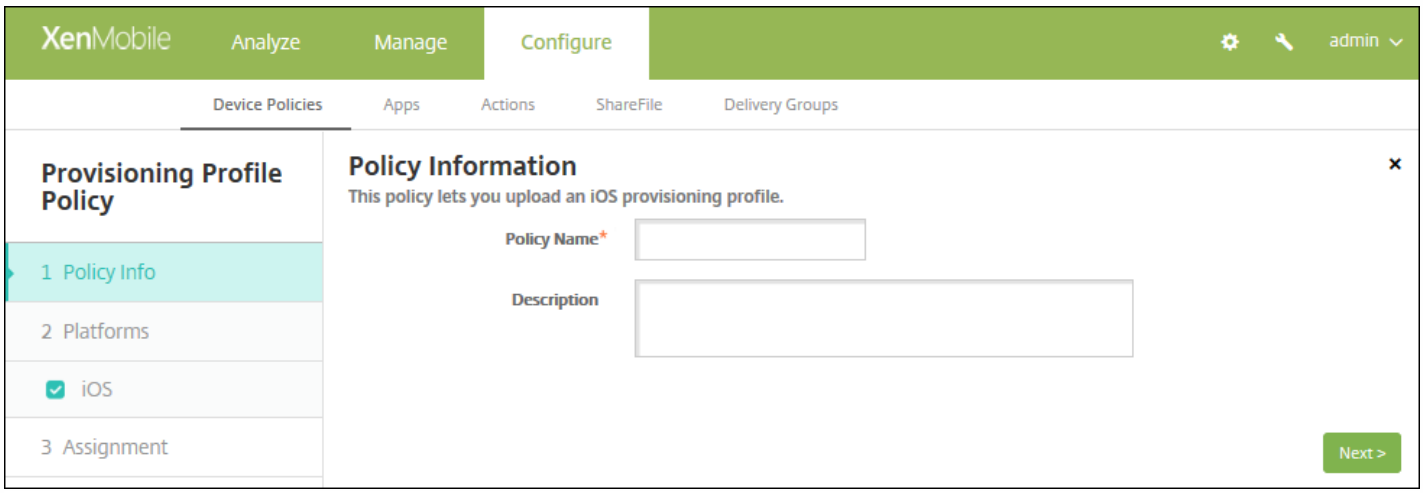
Um die Benutzer mit diesem Vorgang nicht zu behelligen, können Sie in XenMobile Provisioningprofile über Geräterichtlinien installieren und entfernen. Fehlende oder abgelaufene Profile werden nach Bedarf entfernt und aktuelle Profile auf den Geräten installiert, sodass Apps beim Antippen normal geöffnet 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.

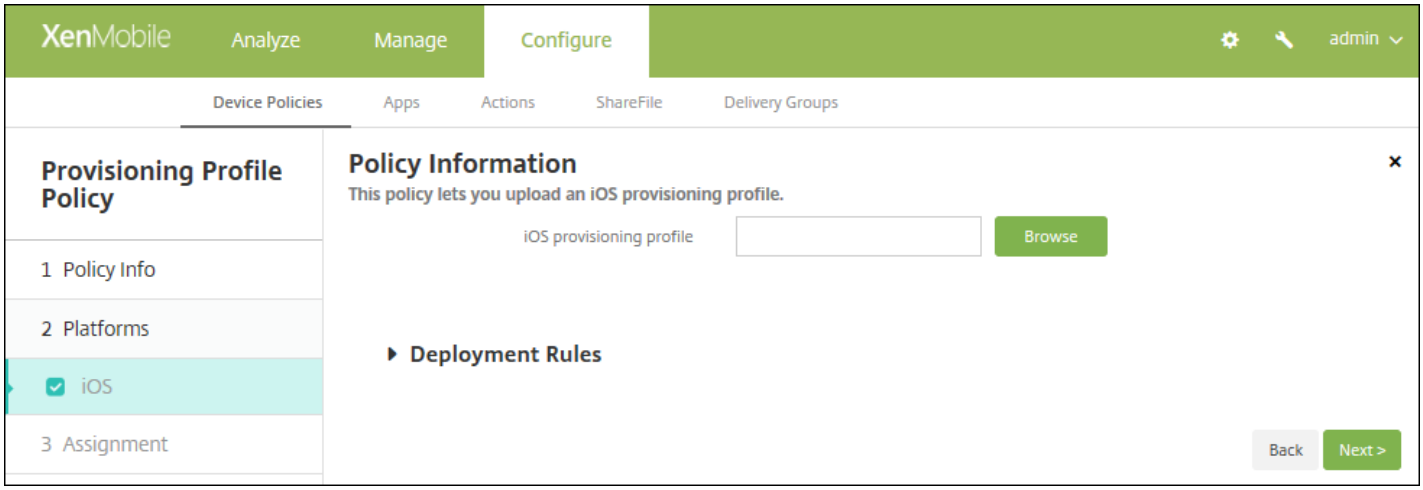
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Provisioningprofil**. Die Seite **Provisioningprofil** wird angezeigt.



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.

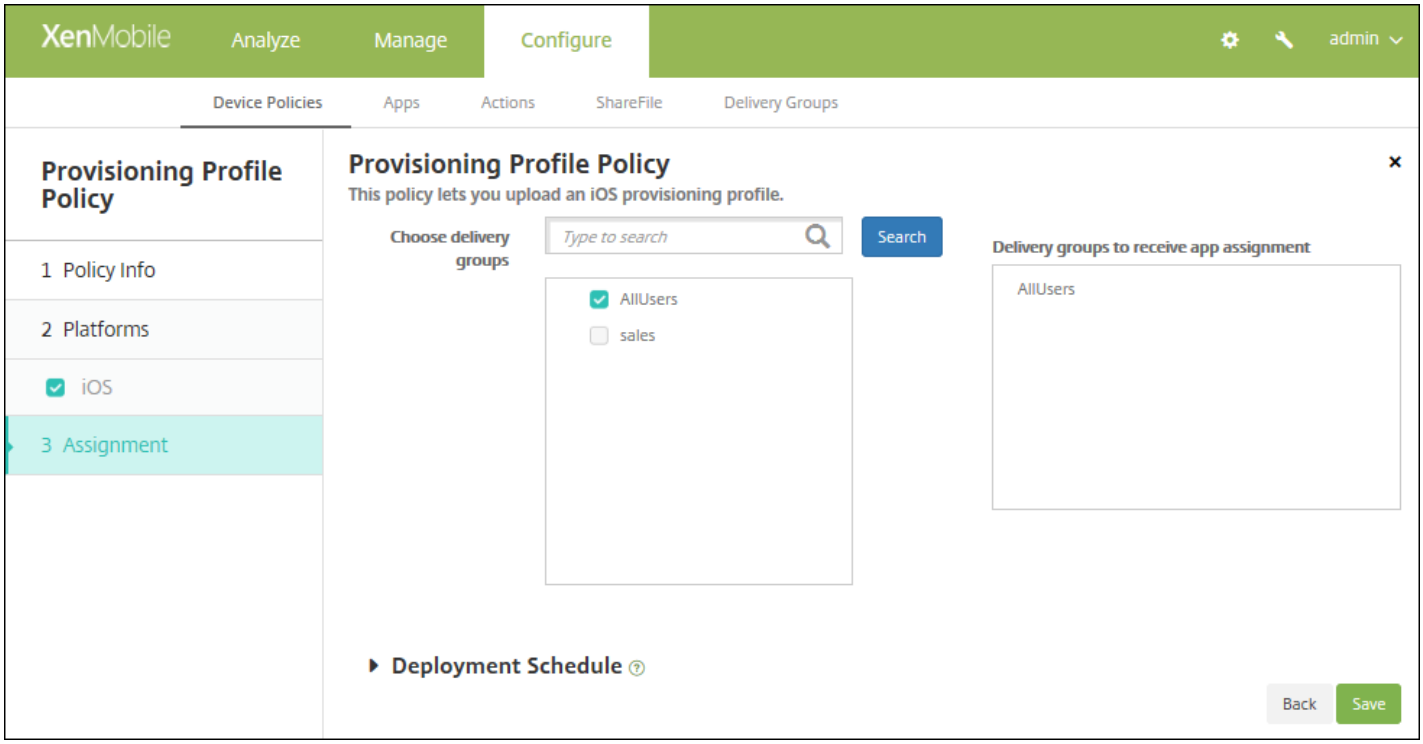


6. Konfigurieren Sie folgende Einstellung:

- **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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Richtlinie zum Entfernen von Provisioningprofilen

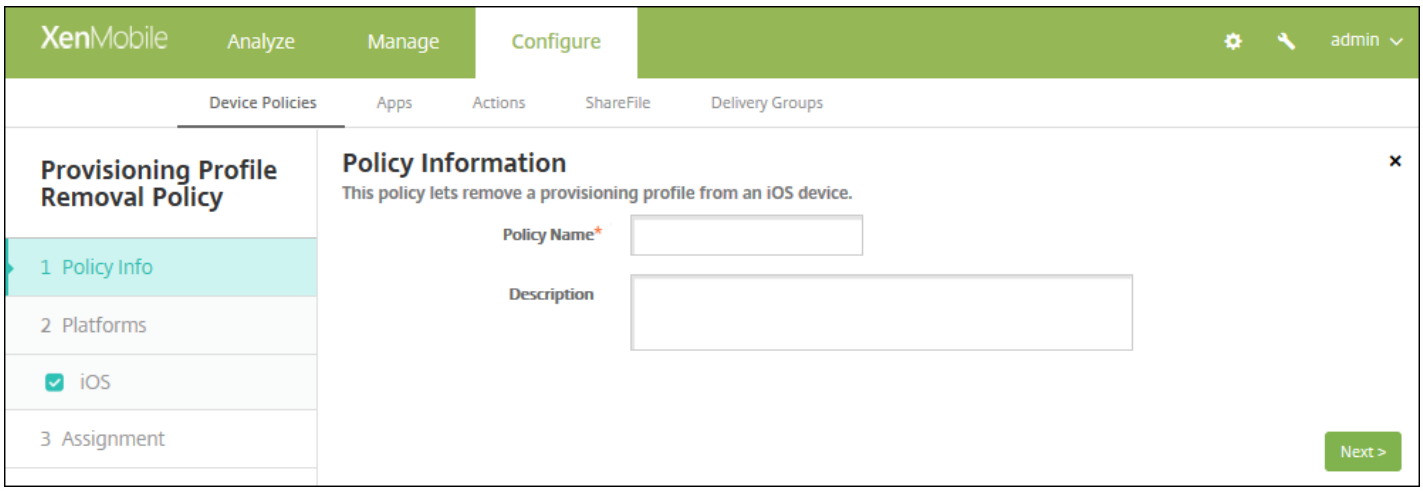
Feb 24, 2017

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.

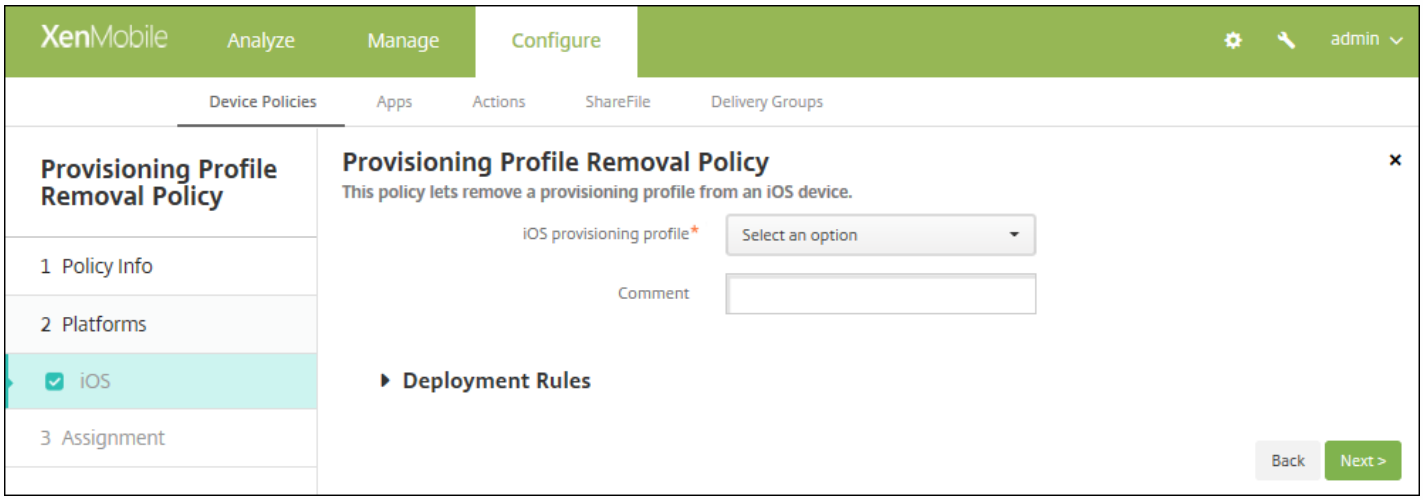
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Entfernen** auf **Entfernen des Provisioningprofils**. Die Seite **Richtlinieninformationen** wird angezeigt.



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.

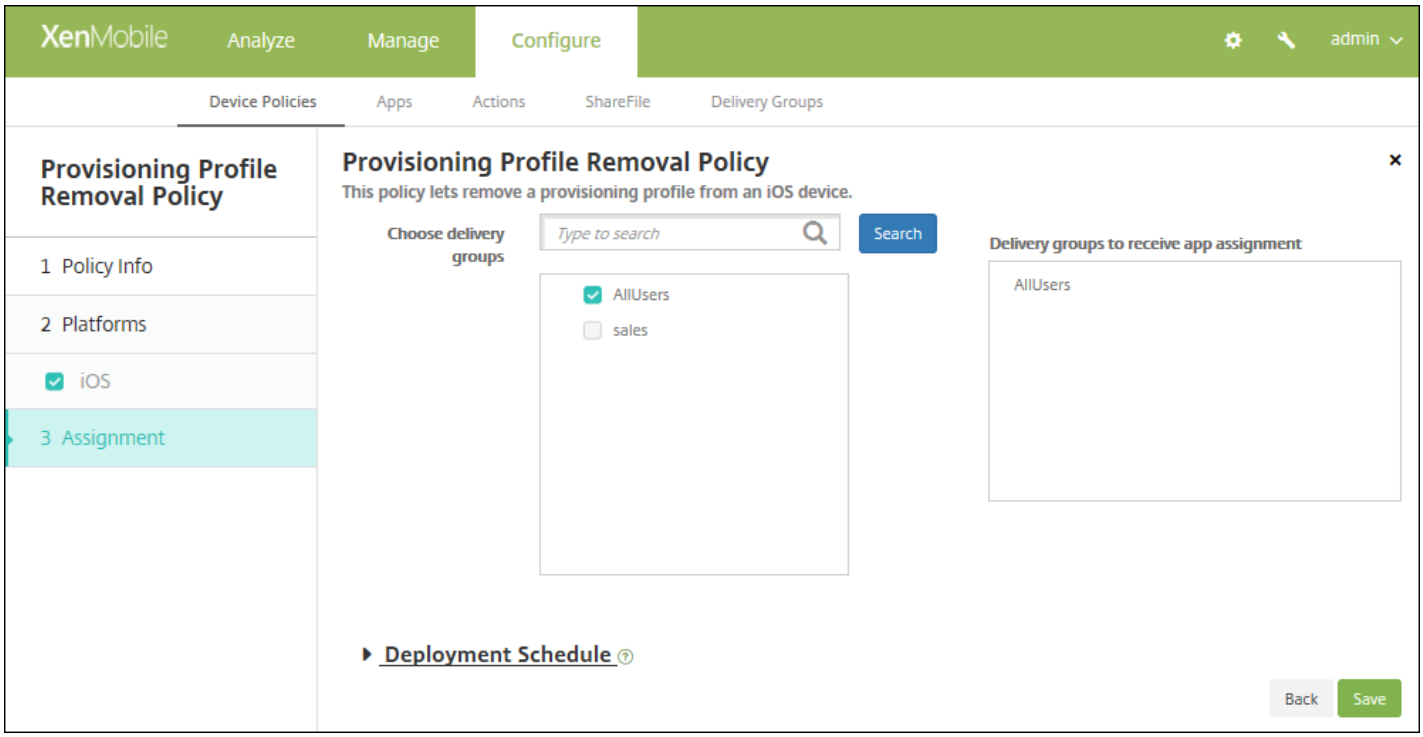


6. Konfigurieren Sie die folgenden Einstellungen:

- **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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Proxy-Geräterichtlinien

Feb 24, 2017

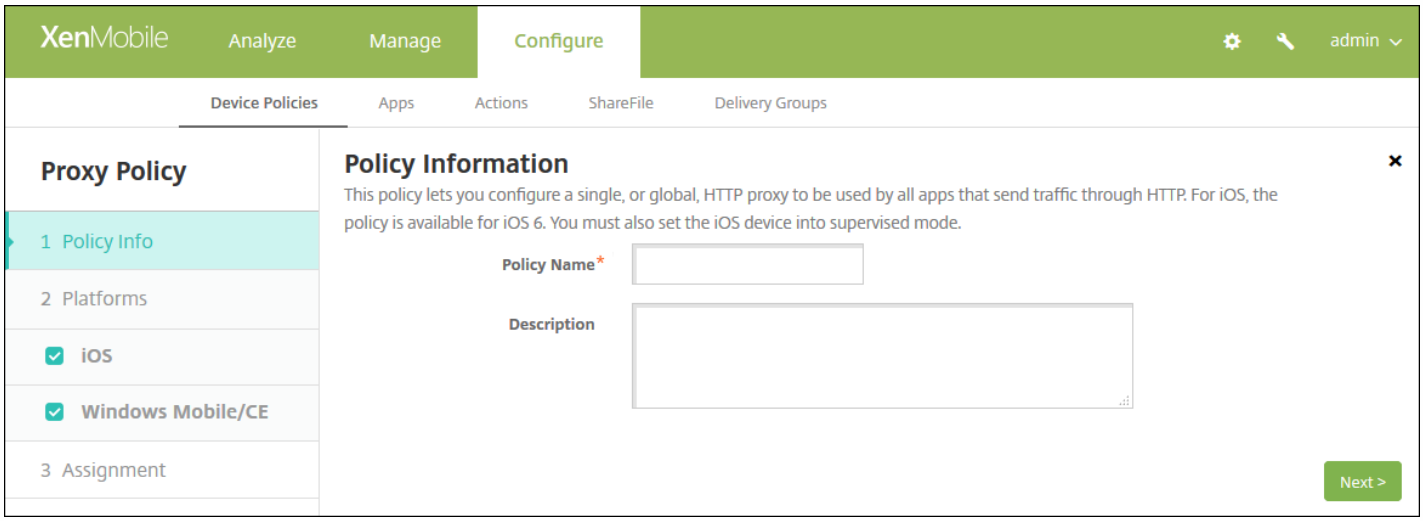
Sie können in XenMobile eine Richtlinie zum Festlegen globaler HTTP-Proxy-Einstellungen für Geräte mit Windows Mobile/CE oder iOS 6.0 oder höher hinzufügen. Sie können nur eine globale HTTP-Proxyrichtlinie pro Gerät bereitstellen.

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:

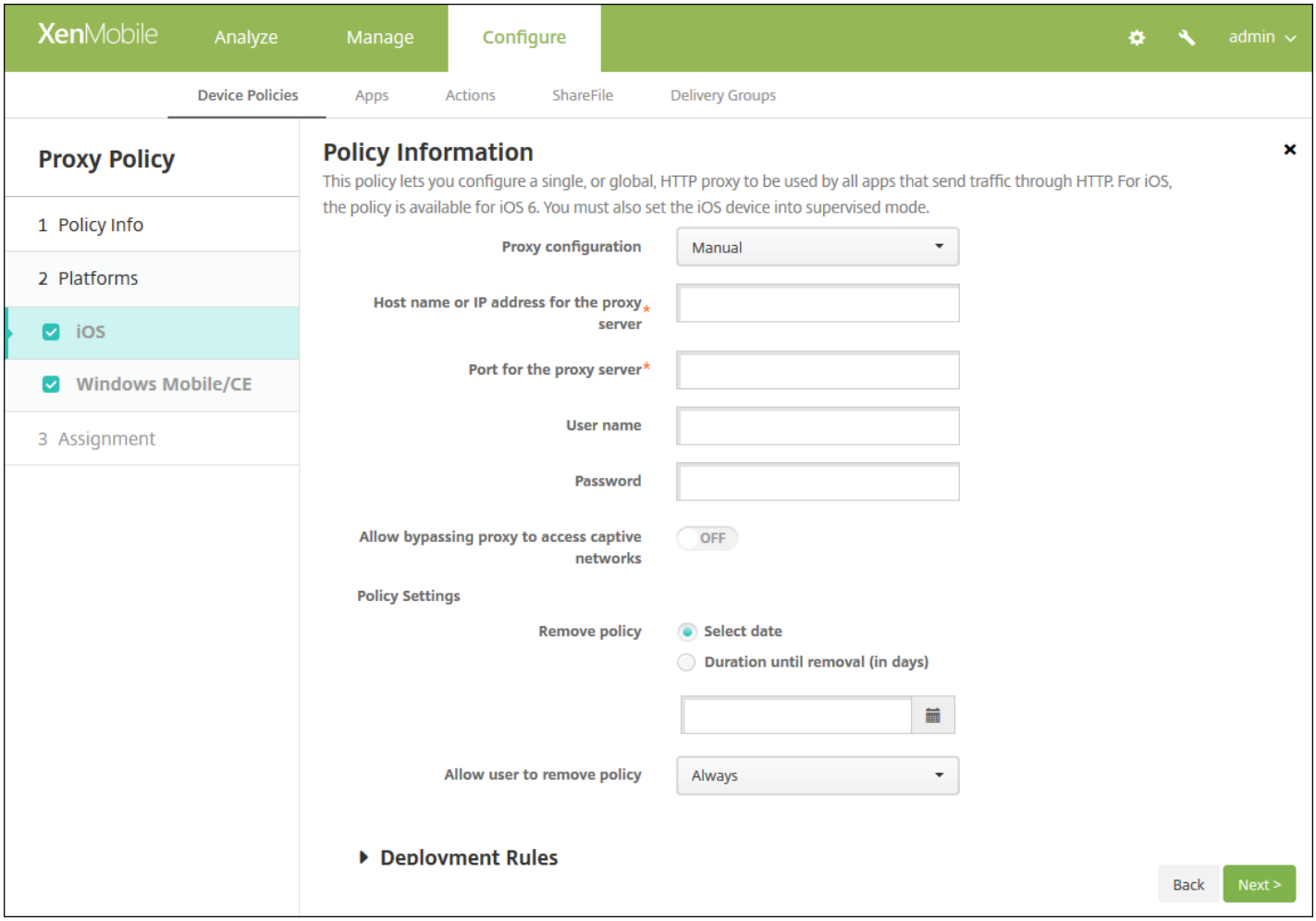
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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

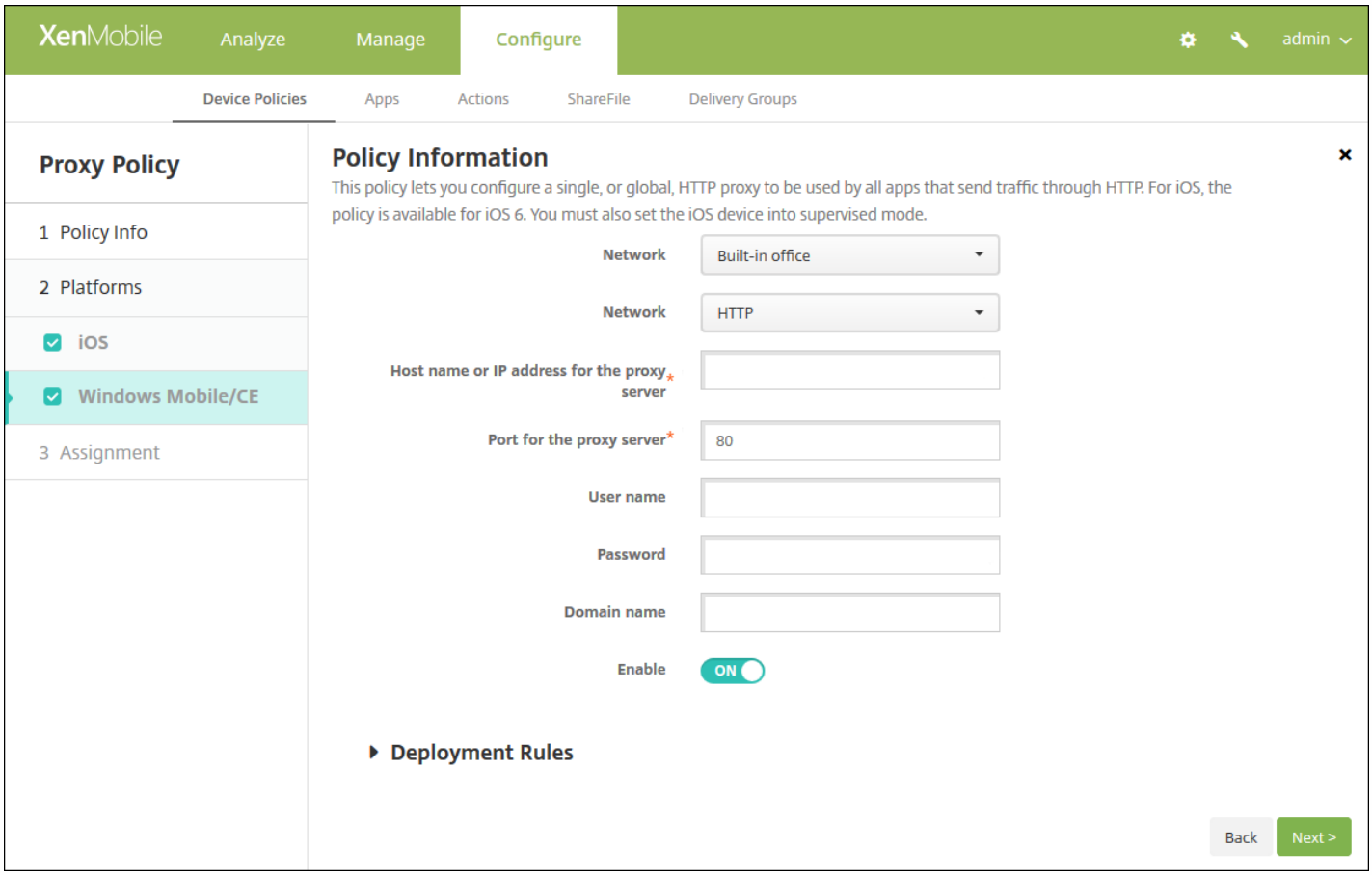


Konfigurieren Sie folgende Einstellungen:

- **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. Der Standardwert 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



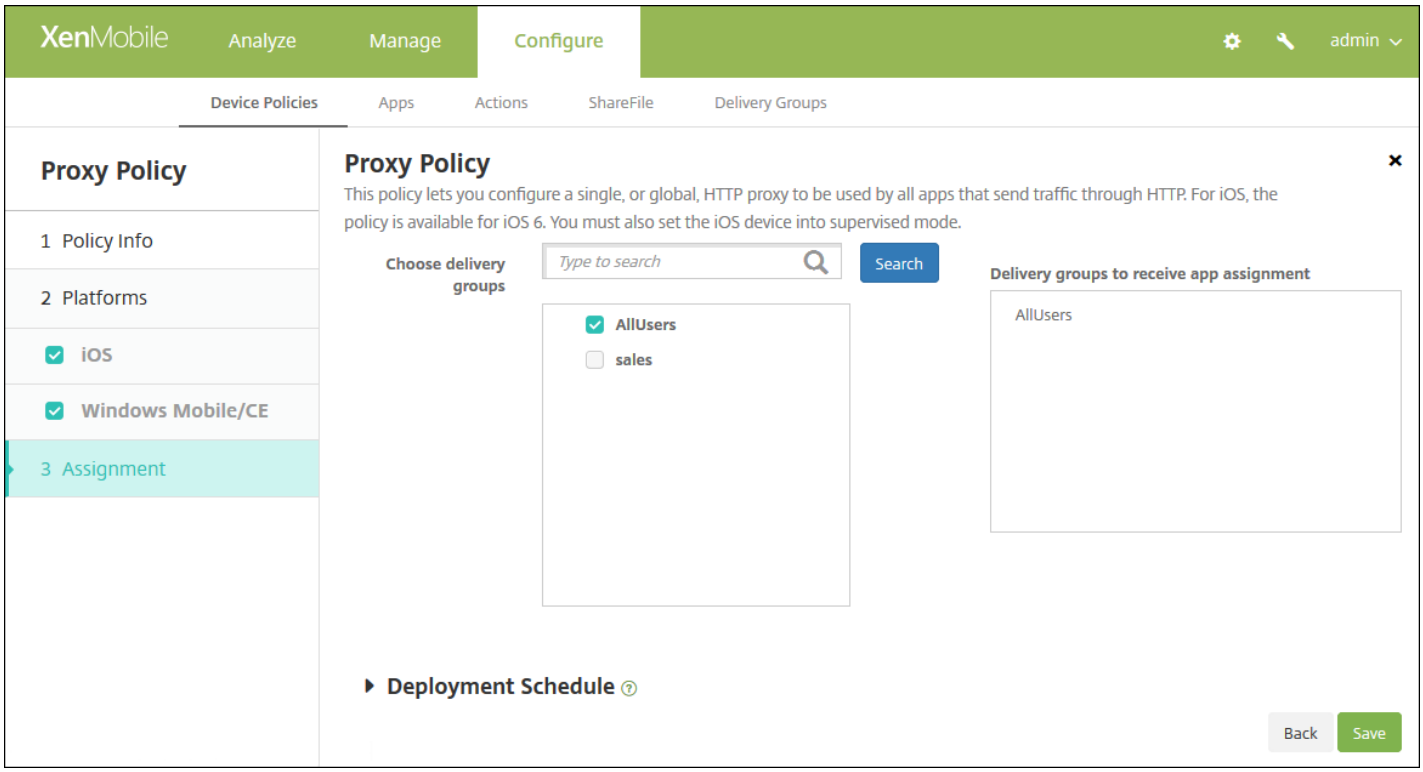
Konfigurieren Sie folgende Einstellungen:

- **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. Der Standardwert 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 "always-on" ist für iOS-Geräte nicht verfügbar.

- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Registrierungsrichtlinie

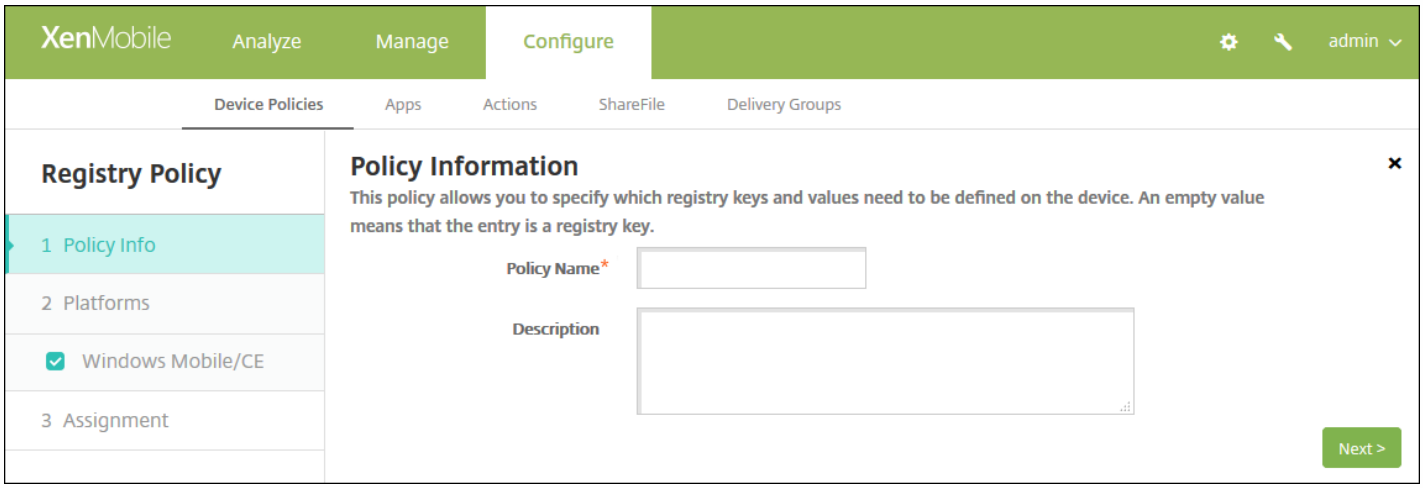
Feb 24, 2017

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.

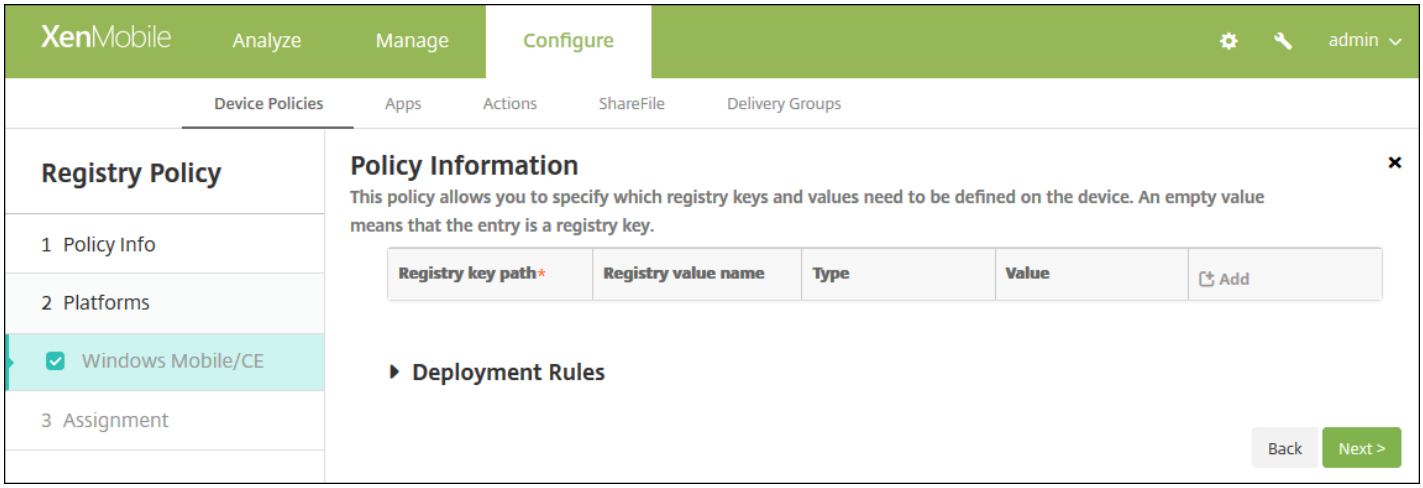
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Benutzerdefiniert** auf **Registrierung**. Die Seite **Registrierung** wird angezeigt.



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:

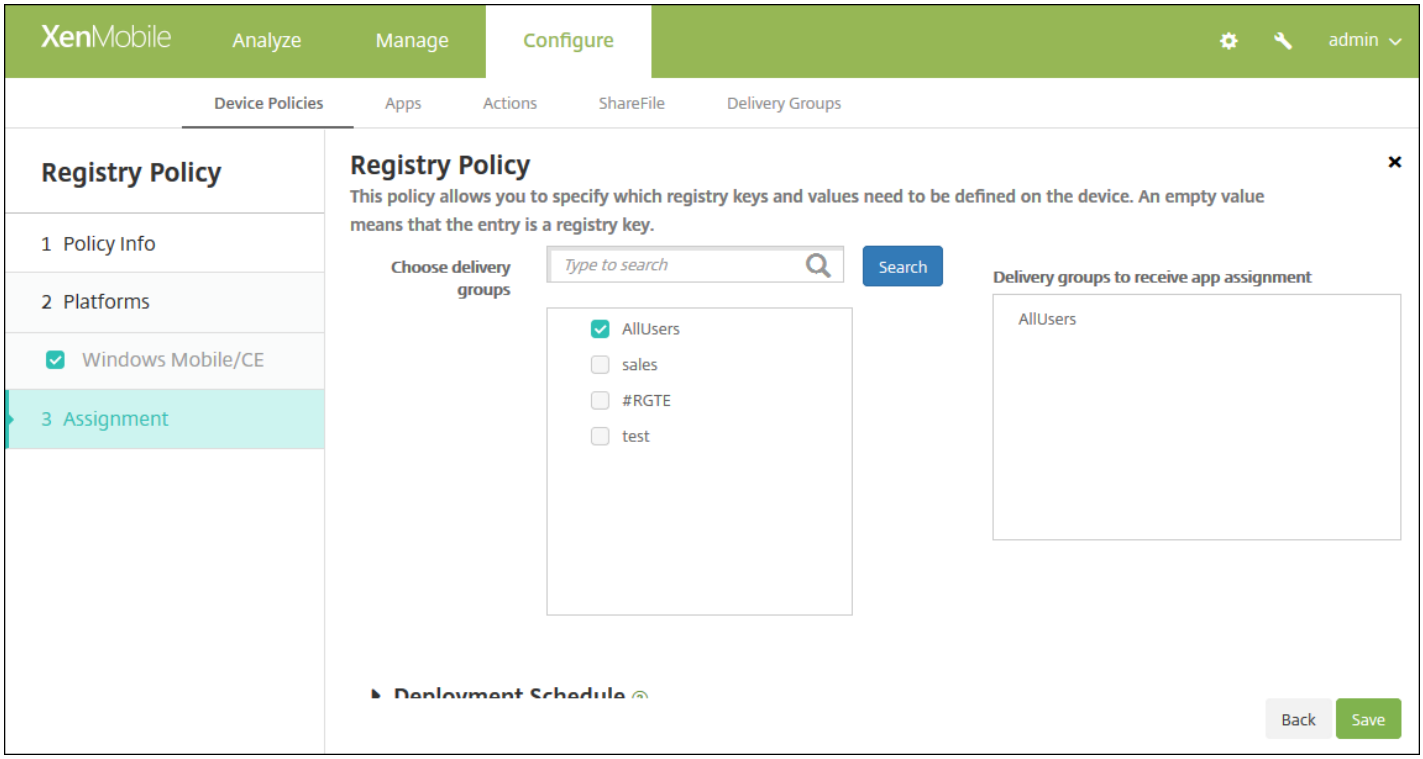
- Klicken Sie für jeden Registrierungsschlüssel bzw. jedes Schlüssel/Wert-Paar, das Sie hinzufügen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
- **Registrierungsschlüsselpfad**: Geben Sie den vollständigen Pfad des Registrierungsschlüssels ein. Geben Sie beispielsweise *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows* 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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie für Remotesupport

Feb 24, 2017

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.

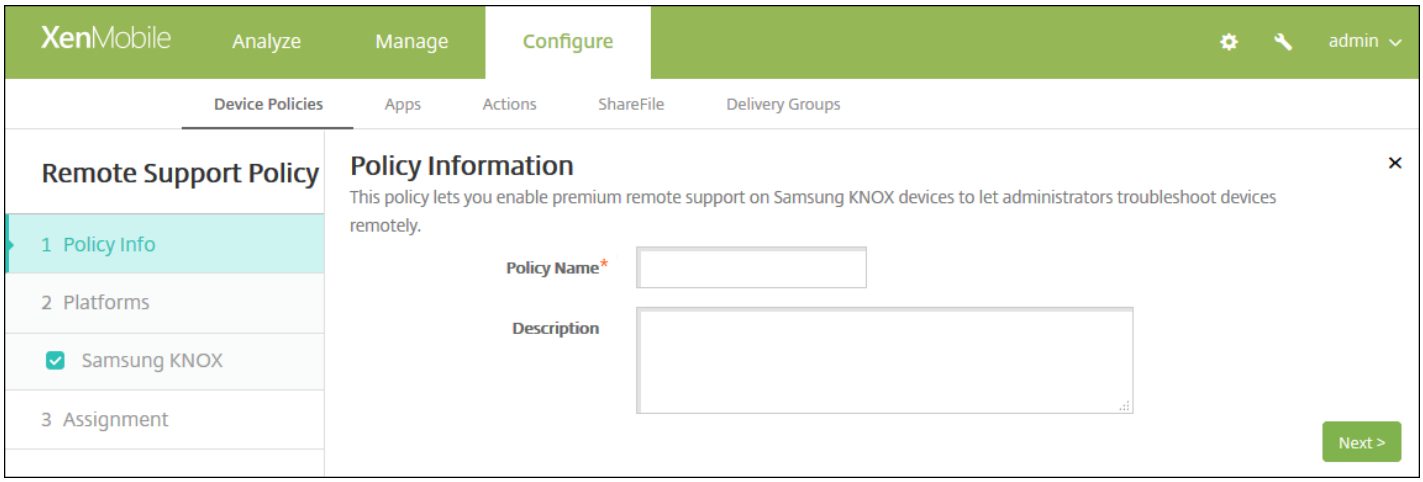
Hinweis: Zum Implementieren der Richtlinie müssen Sie die folgenden Schritte ausführen:

- 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.

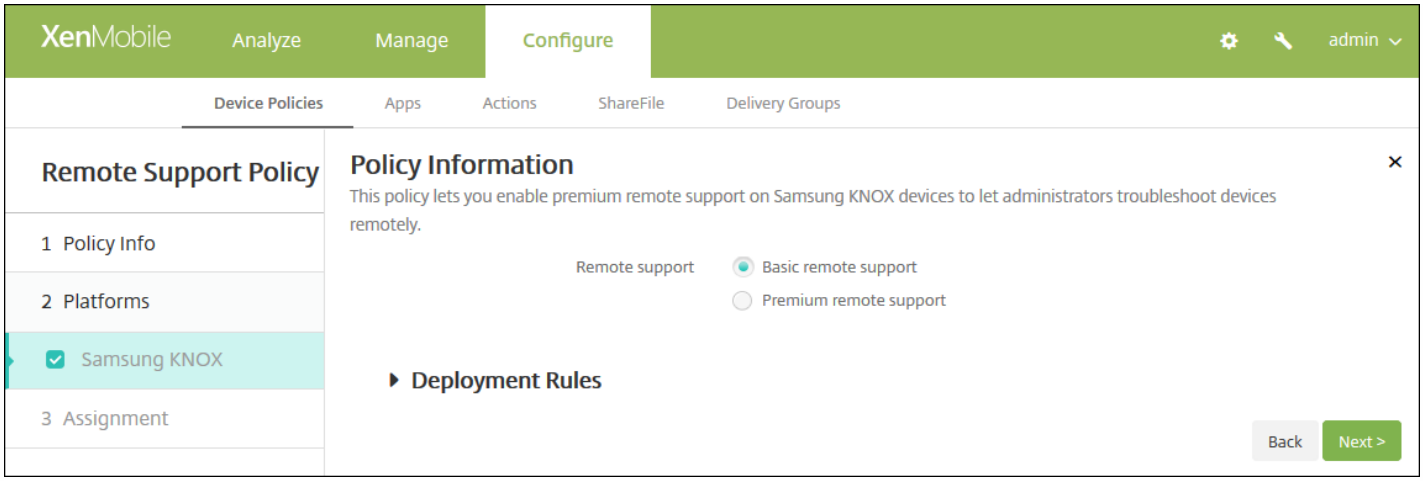
3. Erweitern Sie **Mehr** und klicken Sie unter **Netzwerkzugriff** auf **Remotesupport**. Die Seite **Remotesupport** wird angezeigt.



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.

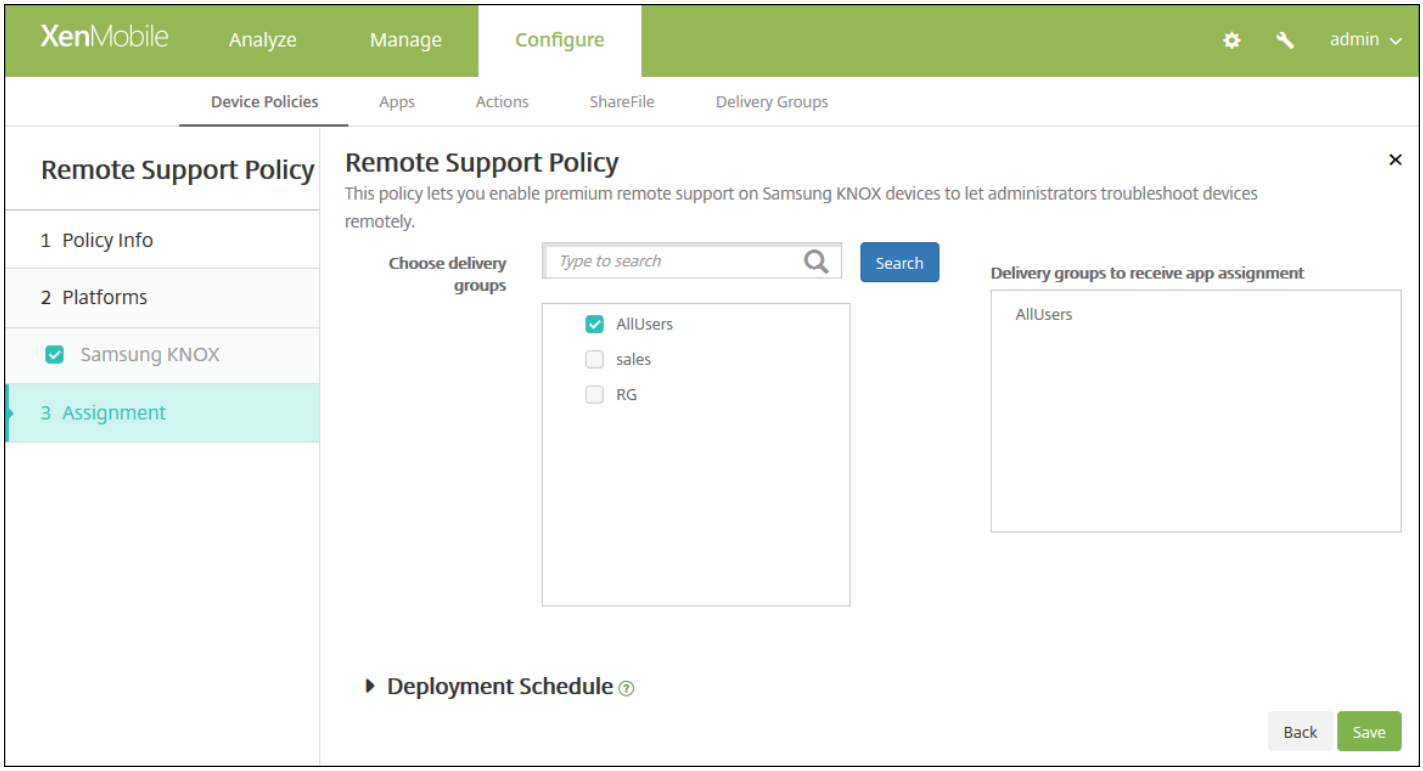


6. Konfigurieren Sie folgende Einstellung:

- **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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Beschränkungsrichtlinien für Geräte

Feb 24, 2017

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.

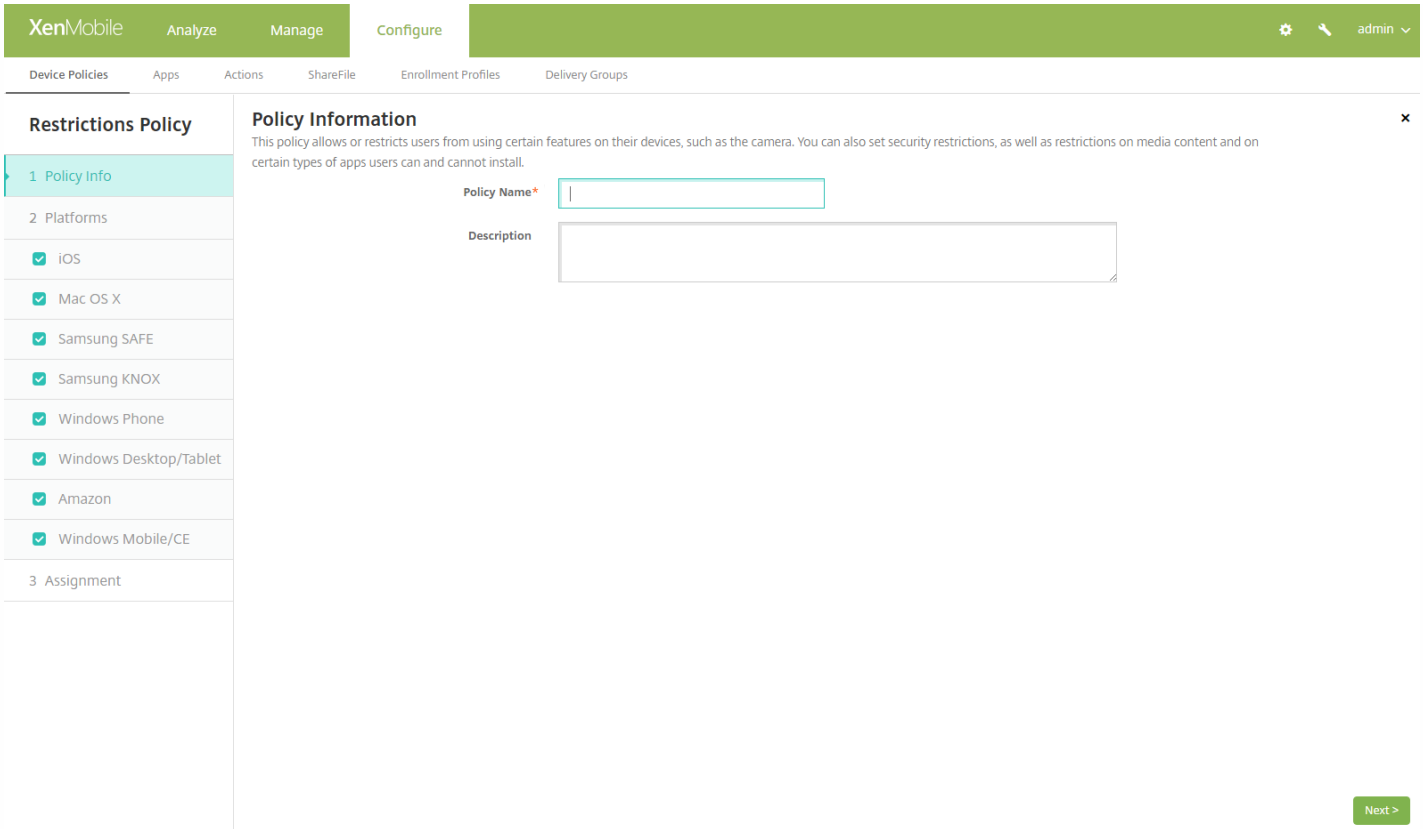
Diese Geräterichtlinie ermöglicht oder verhindert, dass Benutzer auf bestimmte Features auf Geräten, z. B. die Kamera, zugreifen. Sie können außerdem Einschränkungen für Sicherheit und Medieninhalte festlegen und vorgeben, welche App-Typen Benutzer installieren können. Die meisten Einschränkungen sind standardmäßig auf **EIN** (zugelassen) festgelegt. Die wichtigsten Ausnahmen bilden das Feature "iOS-Sicherheit - Erzwingen" sowie alle Windows-Tablet-Features, die standardmäßig auf **AUS** (nicht zugelassen) 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 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 **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.

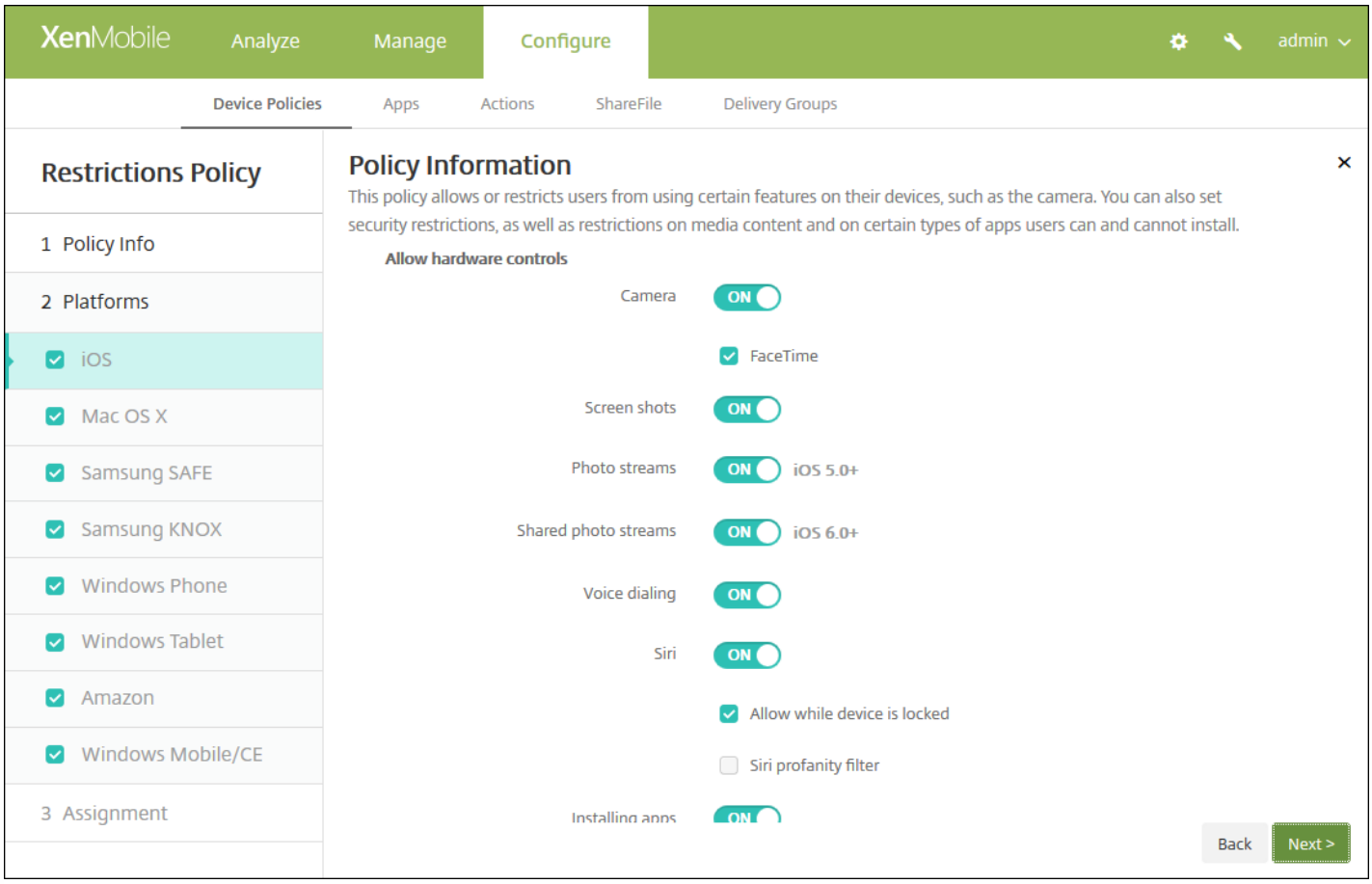
4. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

5. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Sie können anschließend die Richtlinieninformationen für jede ausgewählte Plattform ändern. Klicken Sie zum Einschränken auf die gewünschten Features (siehe nachfolgende Abschnitte), wodurch deren Einstellung in **OFF** geändert wird. Wenn nicht anders angegeben, sind Features in der Standardeinstellung aktiviert.

Bei Auswahl von:
iOS konfigurieren Sie 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

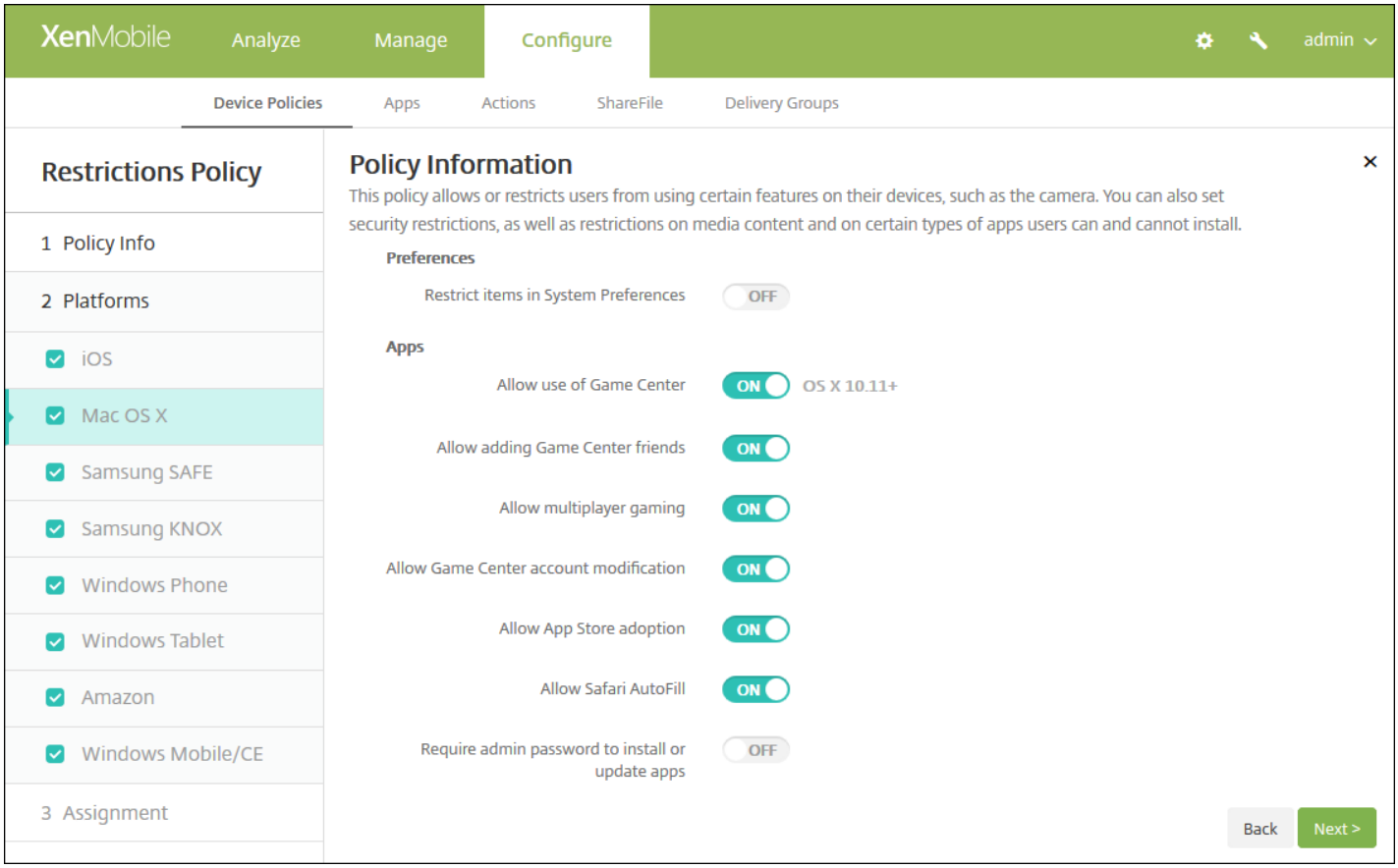
Nachdem Sie die Einschränkungen für eine Plattform festgelegt haben, stellen Sie wie in Schritt 7 in diesem Artikel beschrieben die Bereitstellungsregeln für die Plattform ein.

Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:



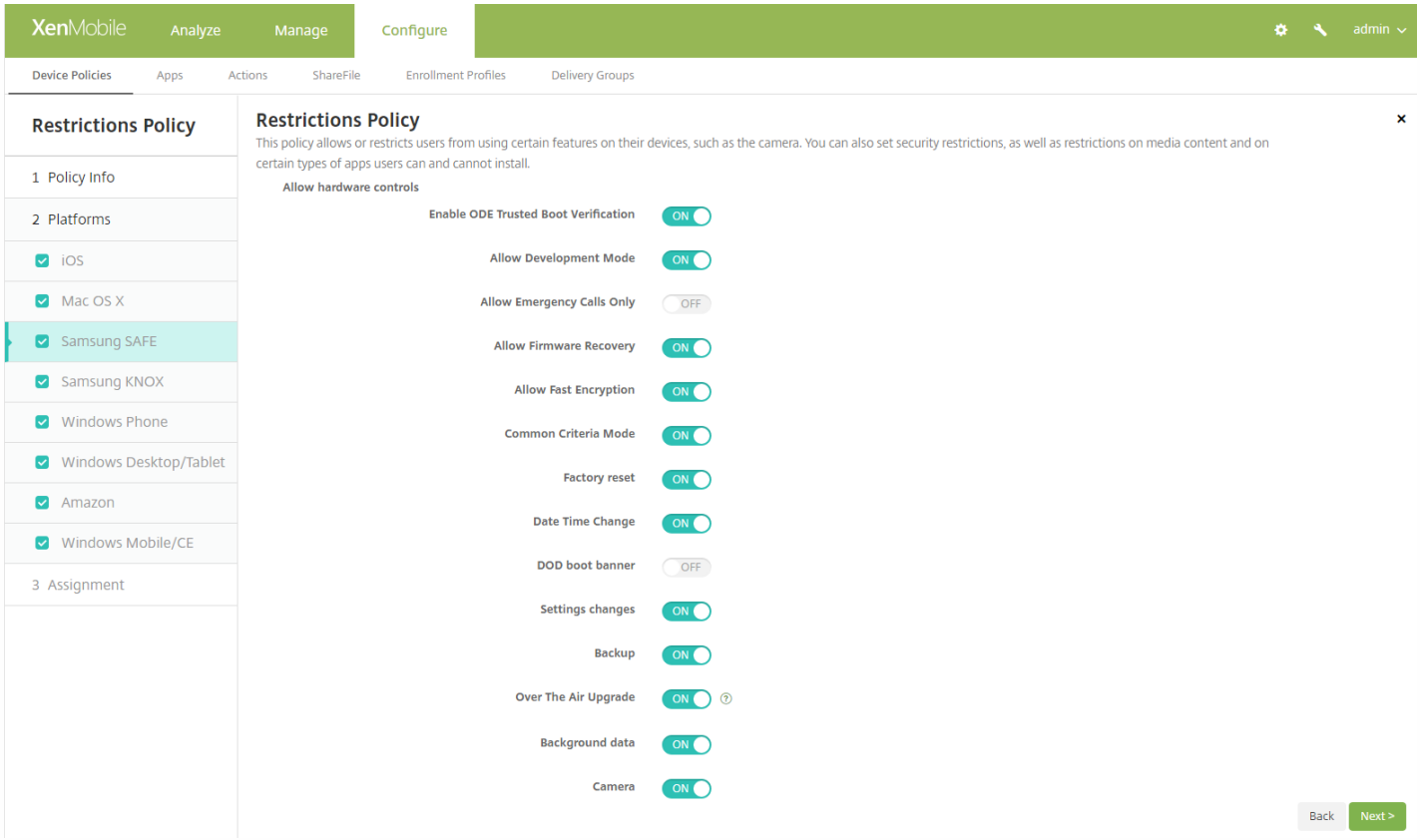
iOS-Einstellungen

Konfigurieren von Mac OS X-Einstellungen



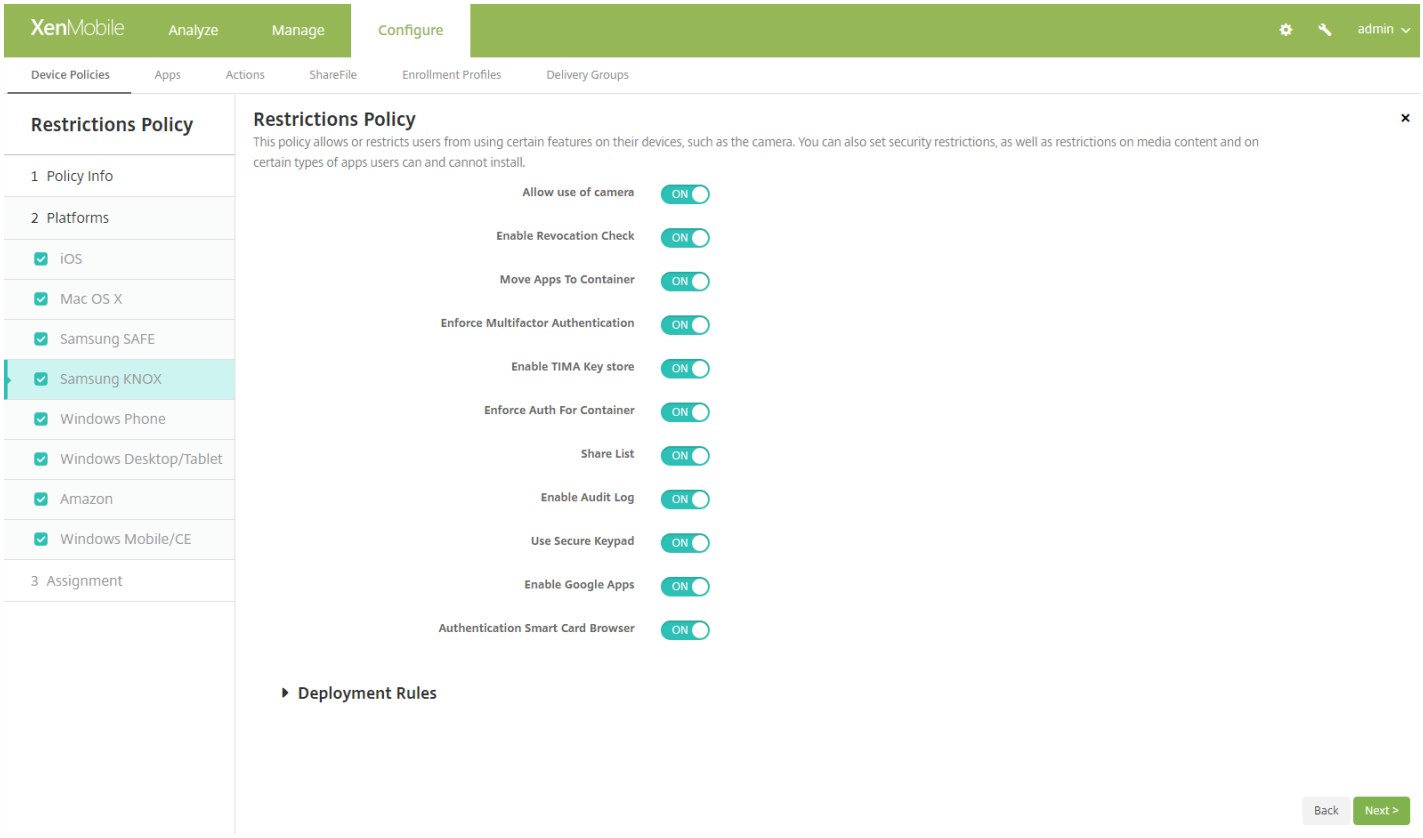
Mac OS X-Einstellungen

Konfigurieren der Samsung SAFE-Einstellungen



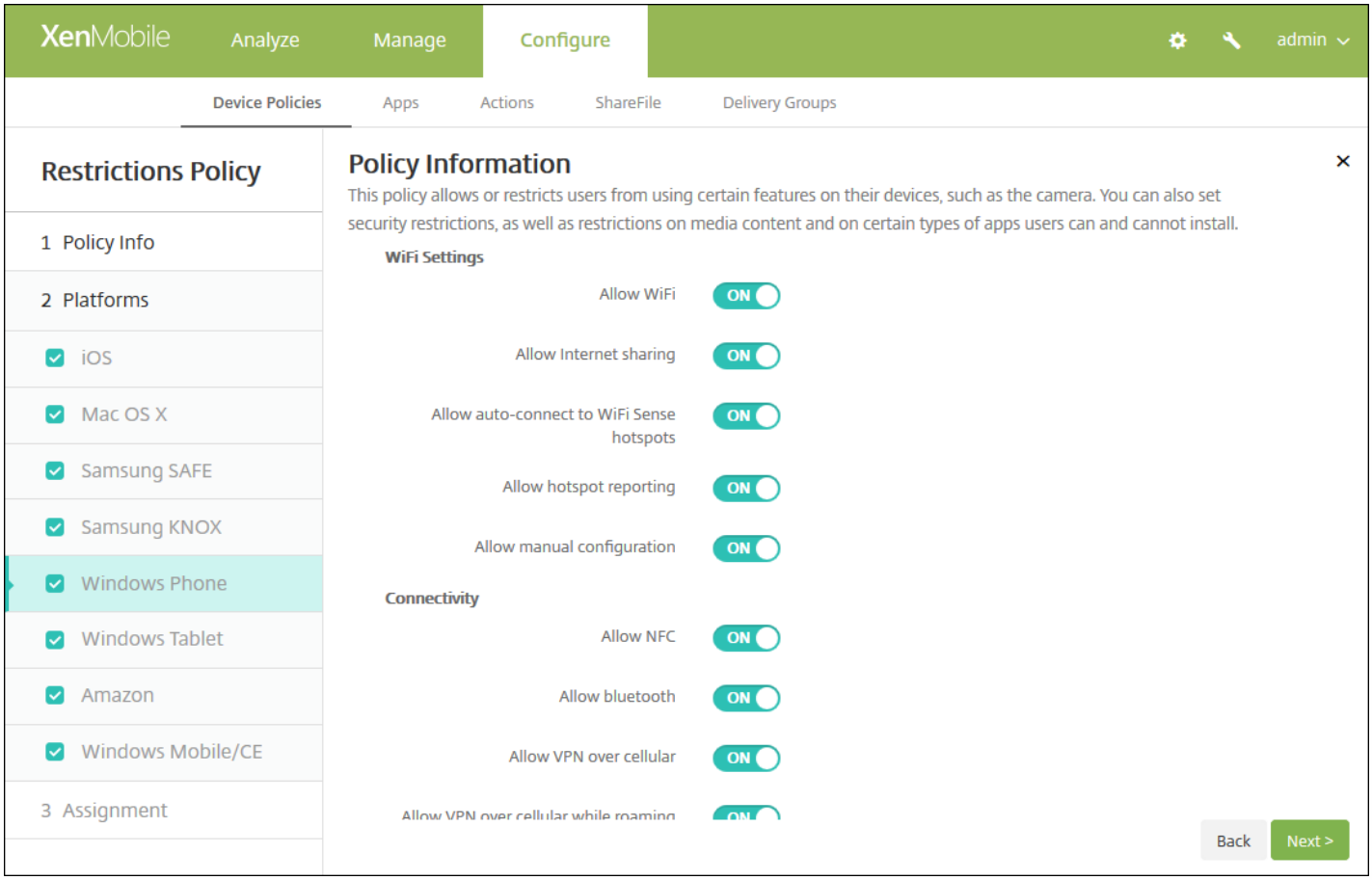
Samsung SAFE-Einstellungen

Konfigurieren der Samsung KNOX-Einstellungen



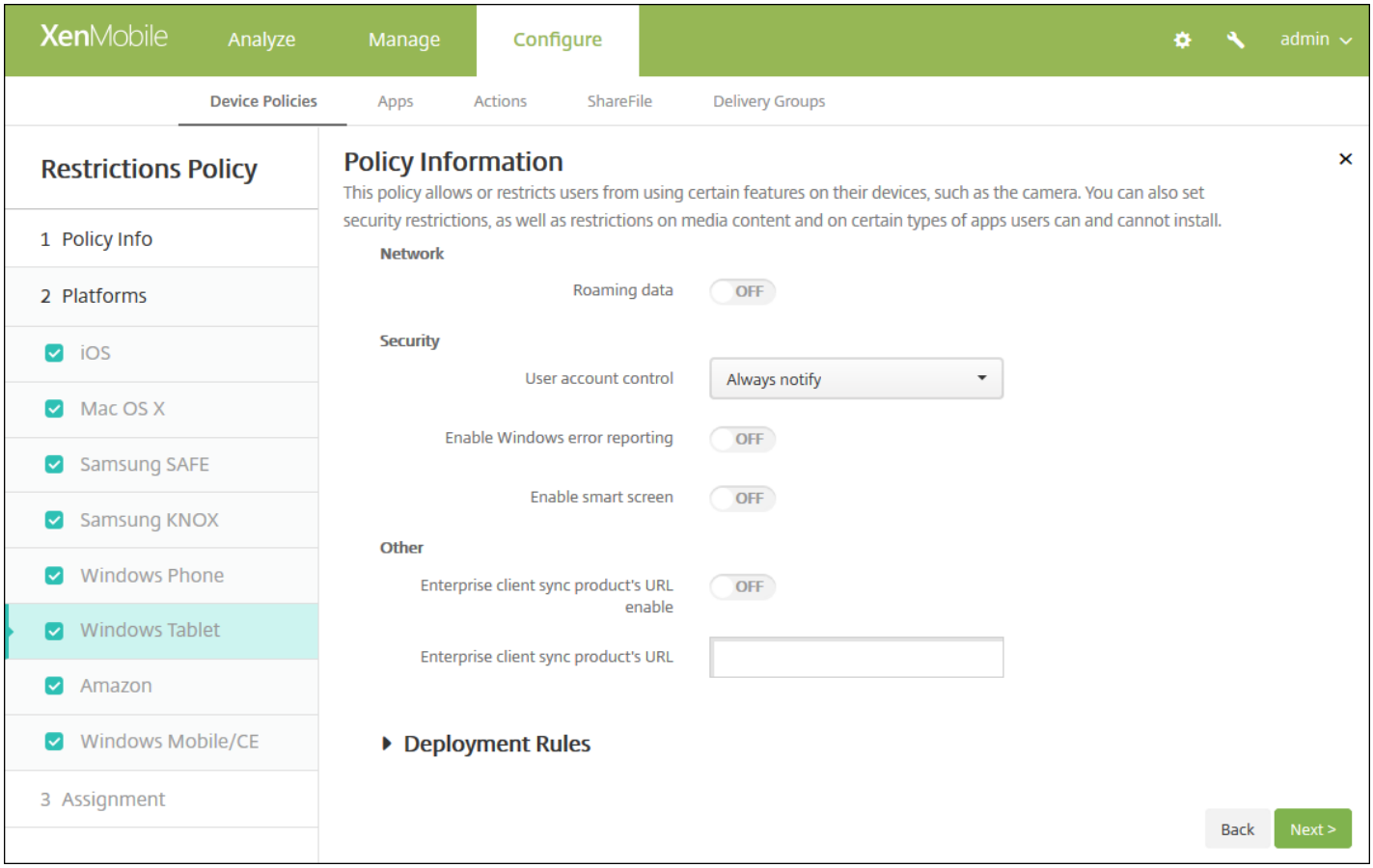
Samsung KNOX-Einstellungen

Konfigurieren von Windows Phone-Einstellungen



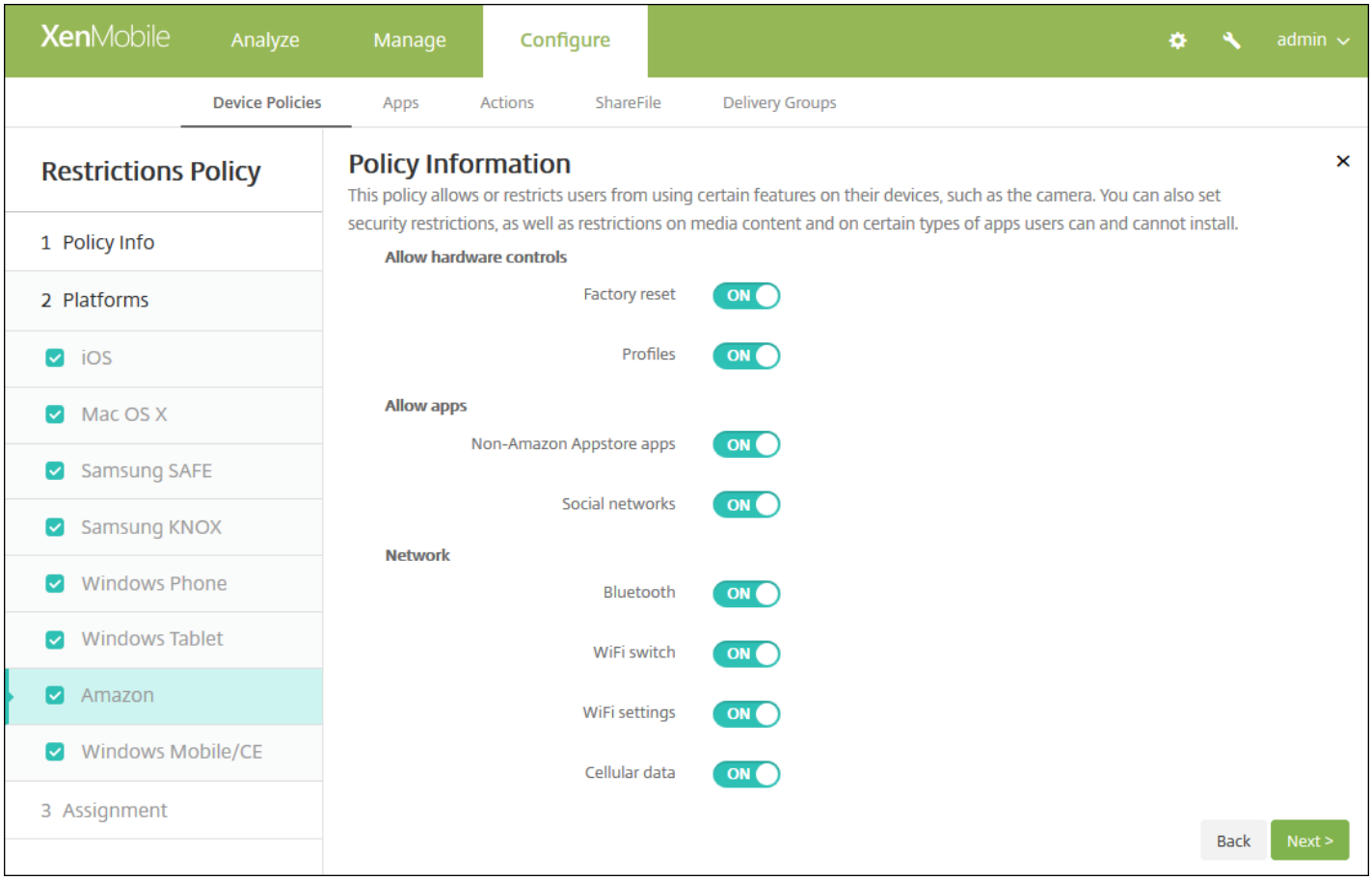
Windows Phone-Einstellungen

Konfigurieren von Windows Desktop-/Tablet-Einstellungen



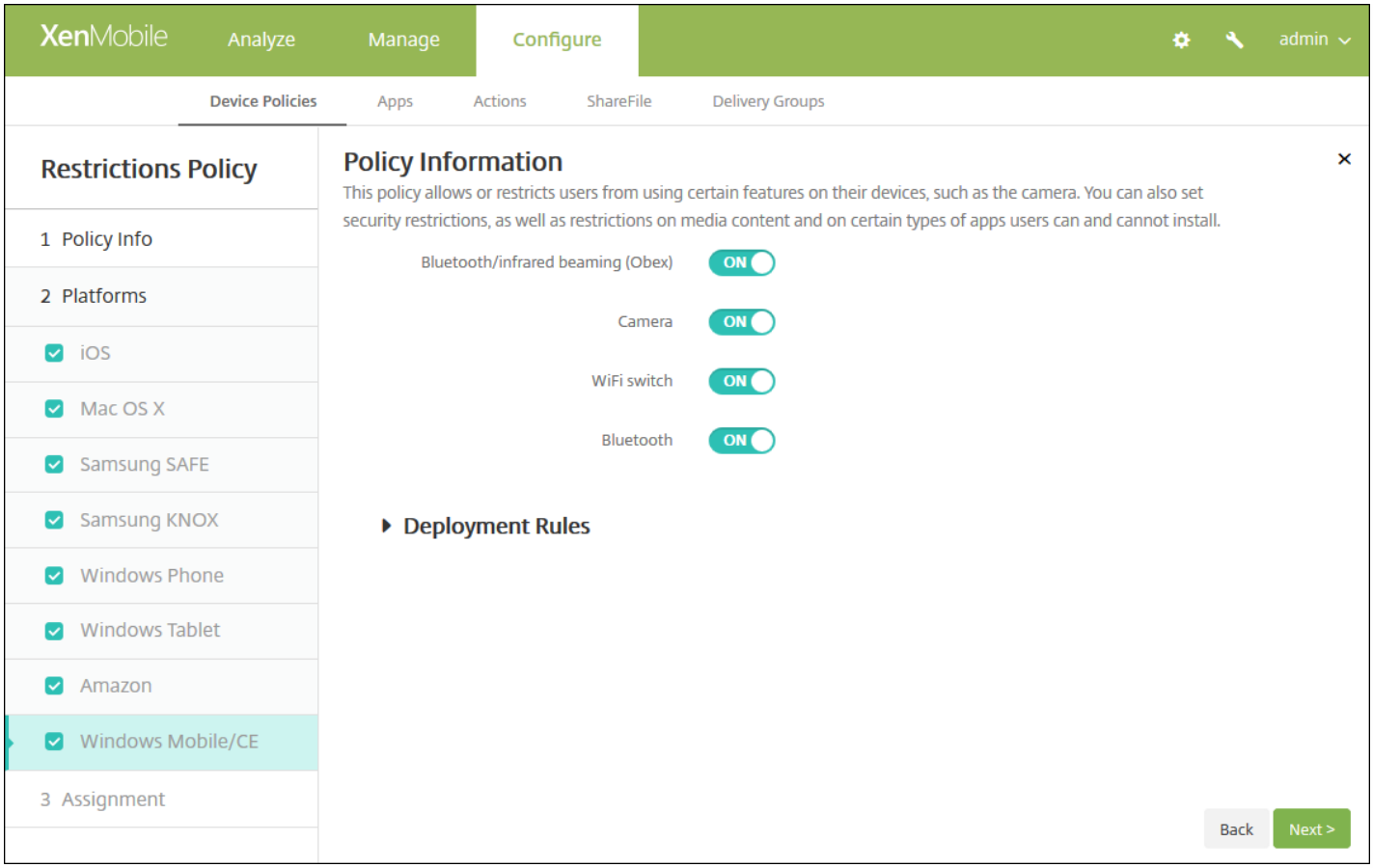
Windows Desktop/Tablet-Einstellungen

Konfigurieren von Amazon-Einstellungen



Amazon-Einstellungen

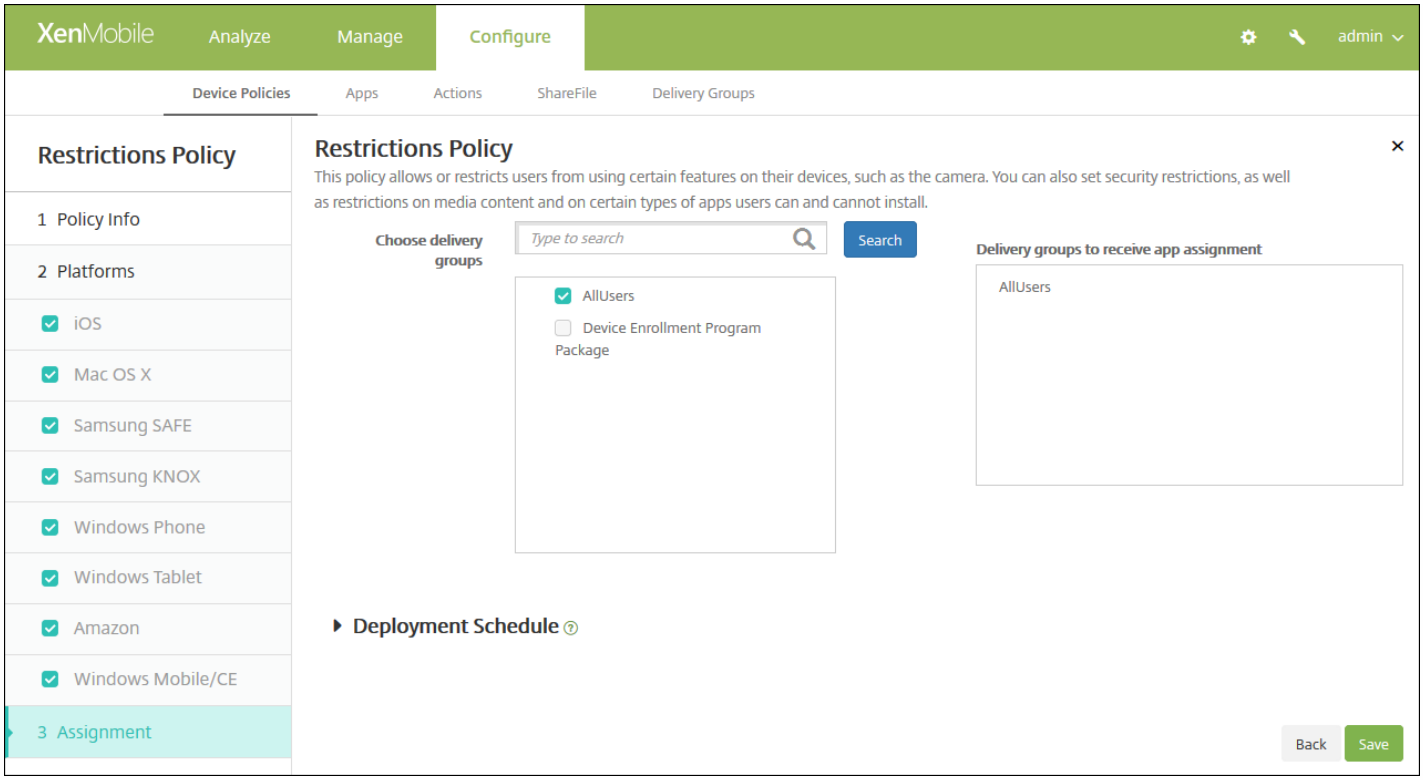
Konfigurieren von Windows Mobile-/CE-Einstellungen



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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

10. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Roamingrichtlinien

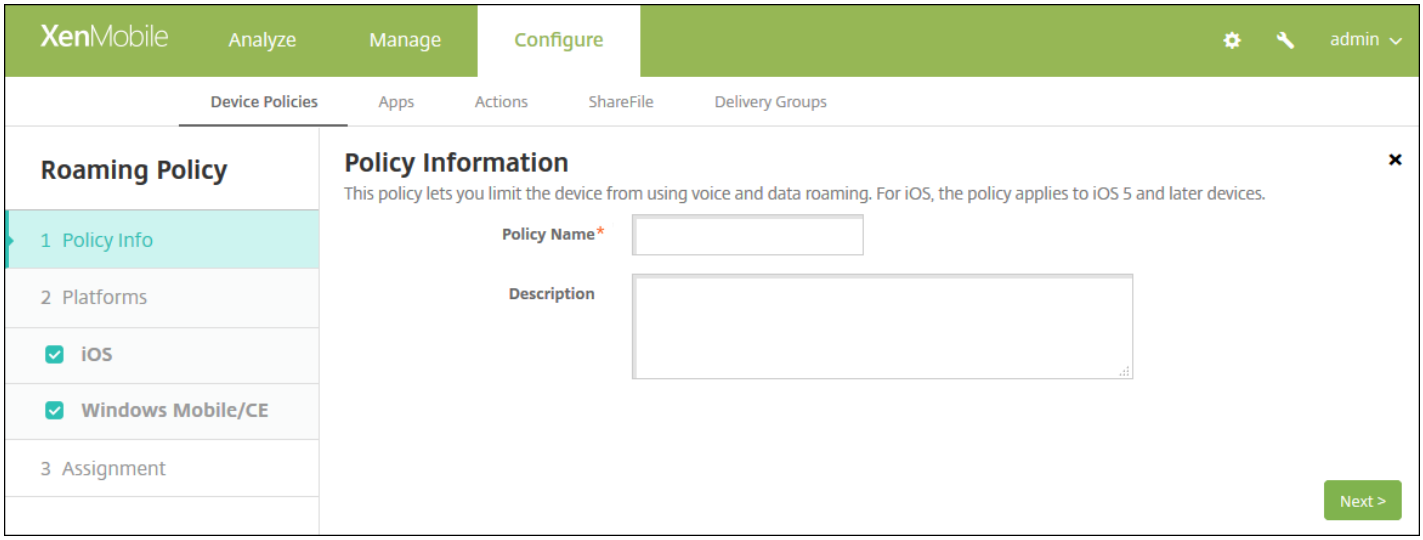
Feb 24, 2017

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:

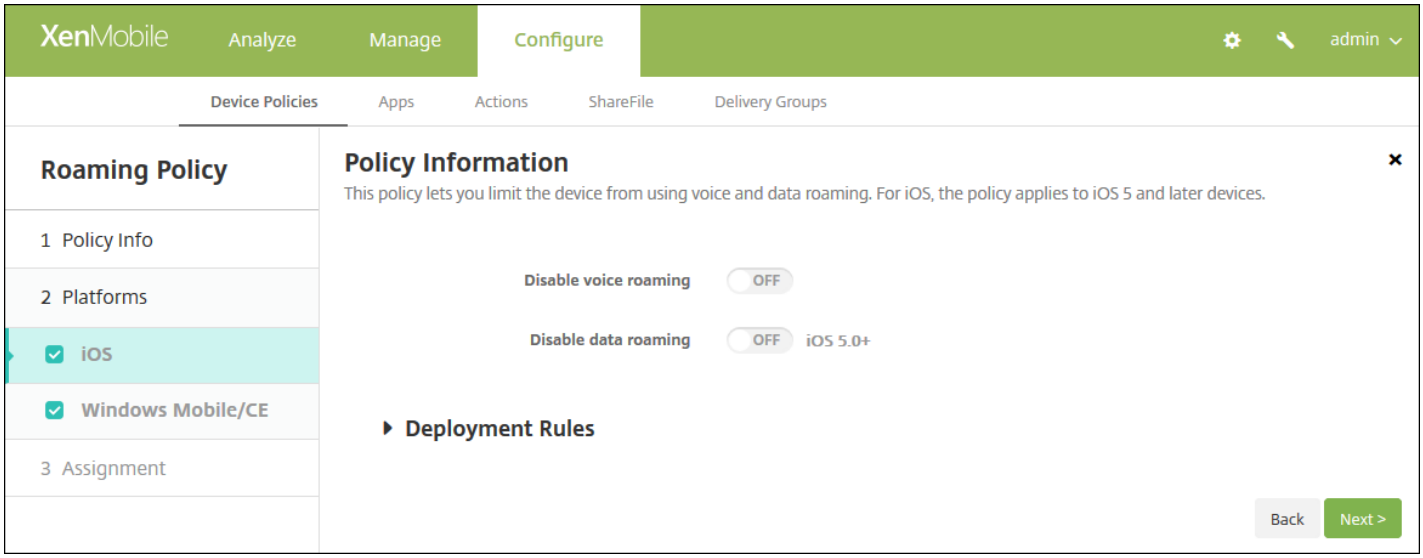
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

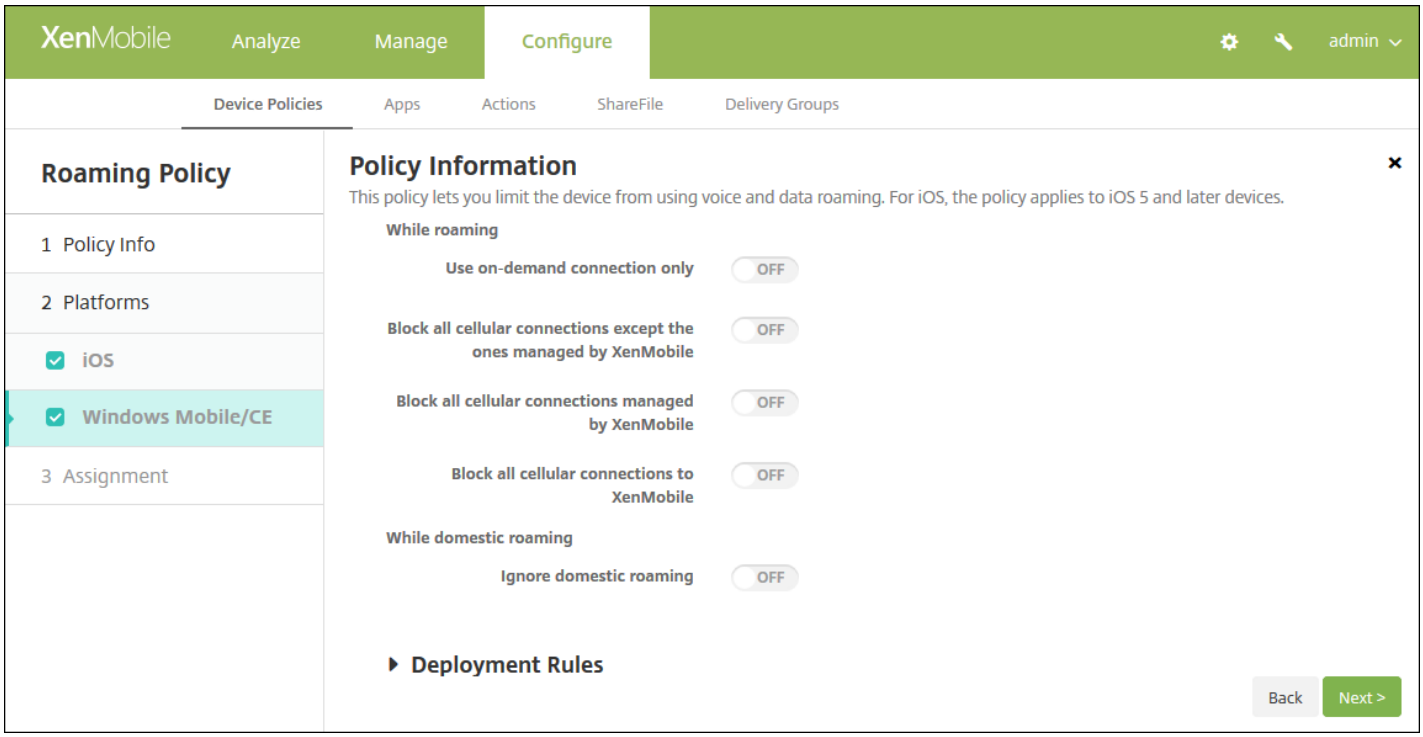
Konfigurieren von iOS-Einstellungen



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

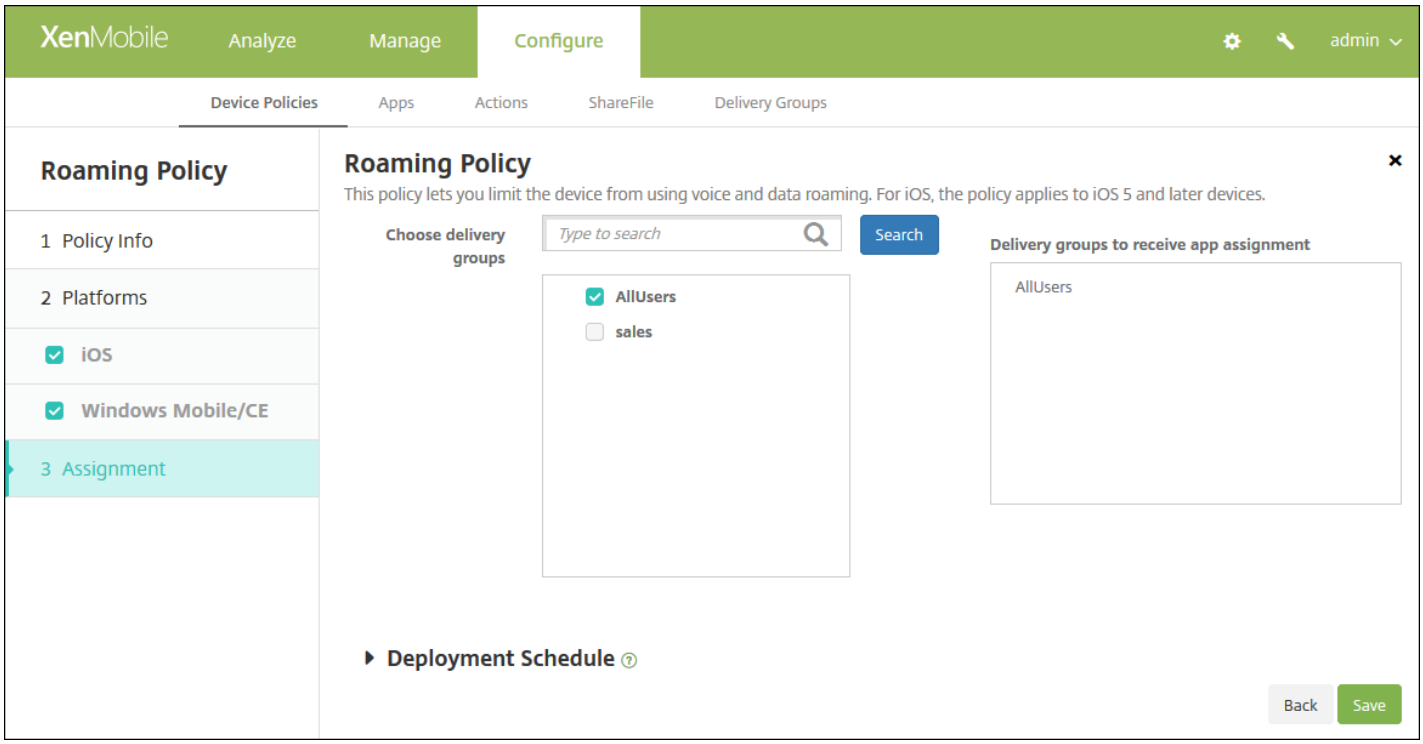


Konfigurieren Sie folgende Einstellungen:

- **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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Samsung MDM-Richtlinien für Geräte

Feb 24, 2017

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.

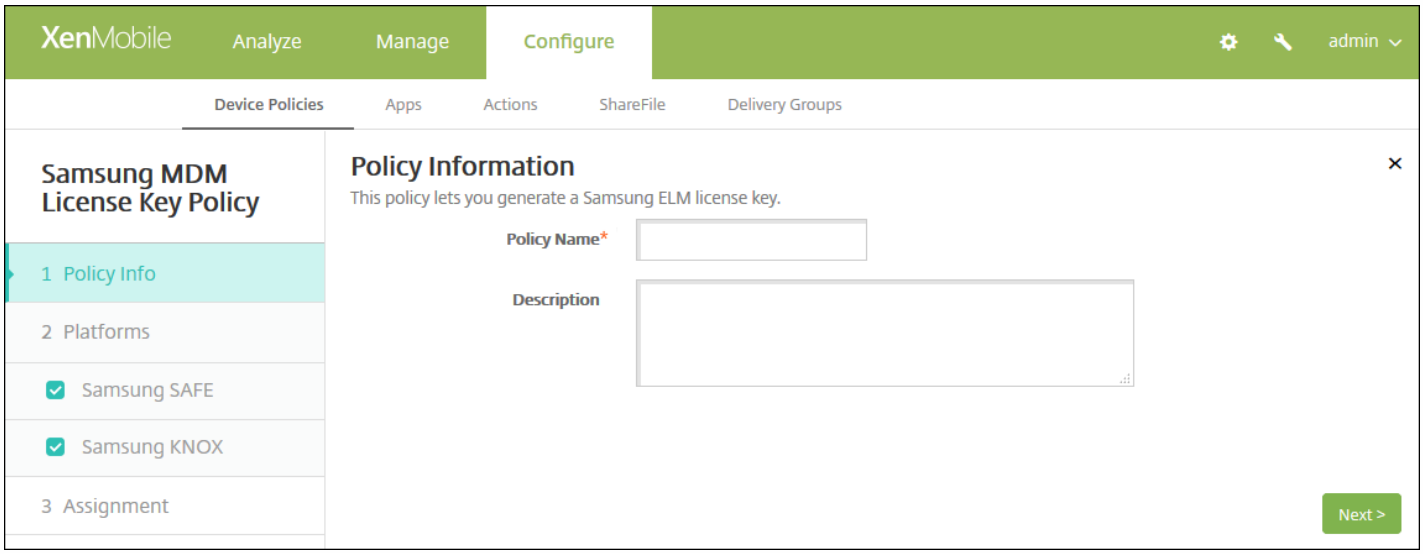
Bevor Sie SAFE-Richtlinien und -Einschränkungen bereitstellen können, müssen Sie die SAFE-APIs durch Bereitstellen des integrierten Samsung Enterprise License Management-Schlüssels (ELM) auf Geräten aktivieren. Zum Aktivieren der Samsung KNOX-API müssen Sie zusätzlich zur Bereitstellung des ELM-Schlüssels 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 Secure Hub 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. 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:

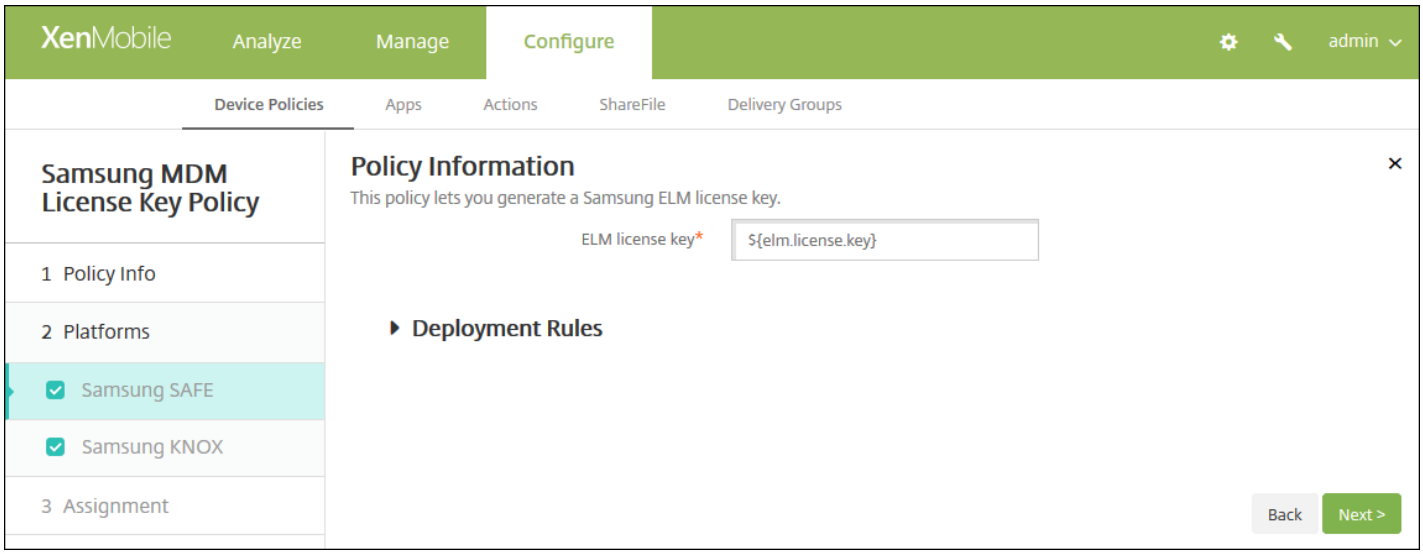
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

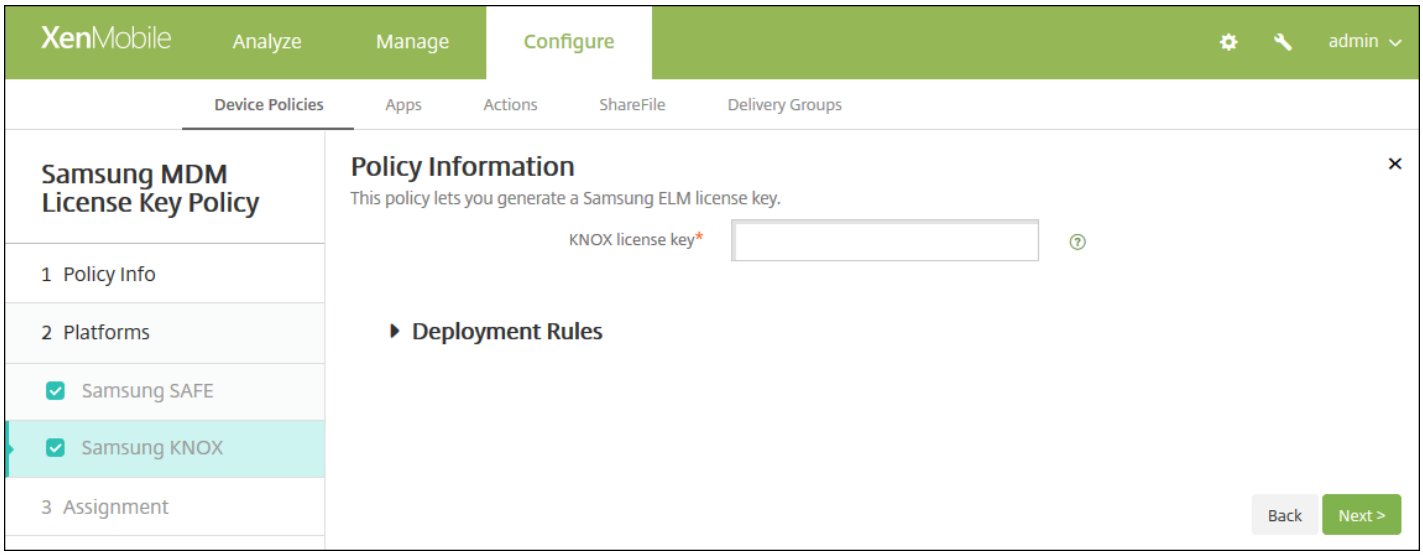
Konfigurieren der Samsung SAFE-Einstellungen



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.

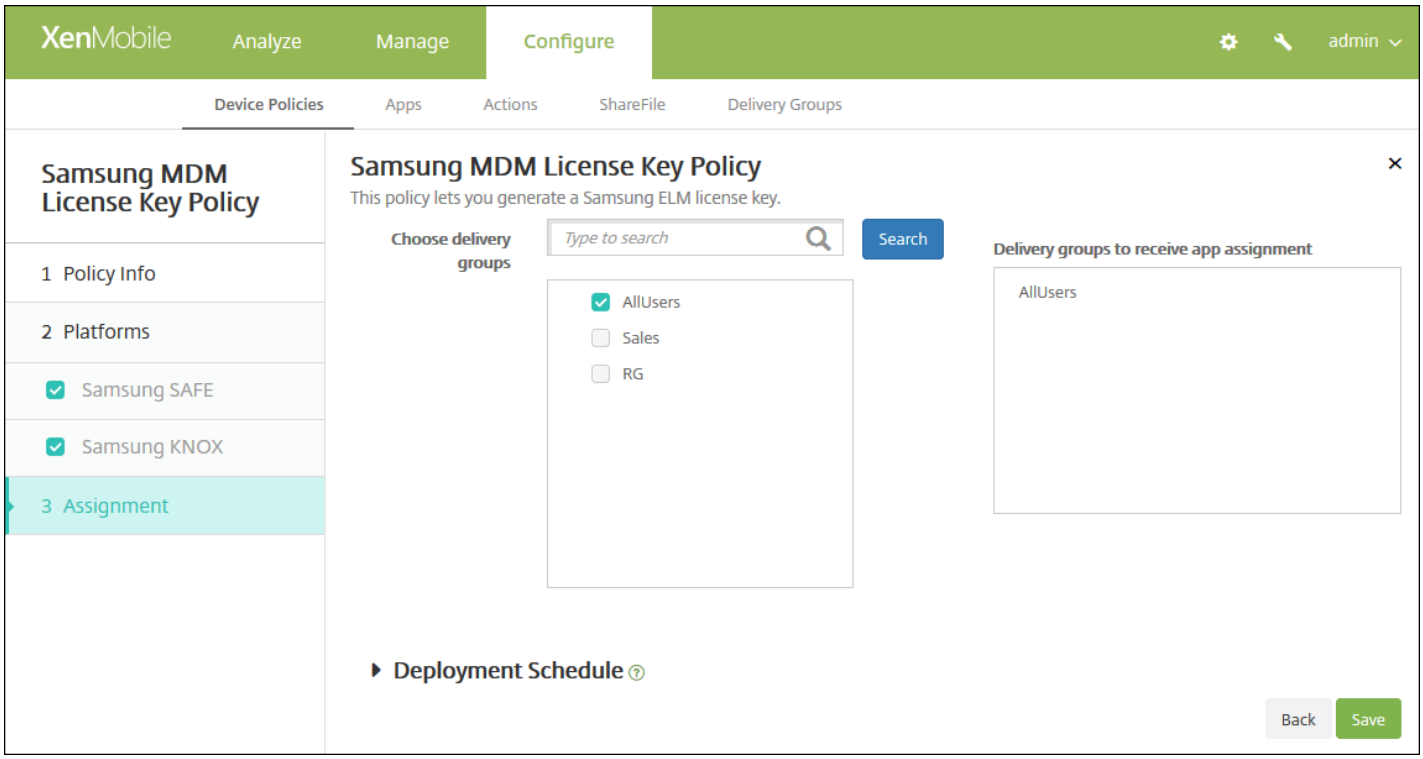
Konfigurieren der Samsung KNOX-Einstellungen



Konfigurieren Sie folgende Einstellung:

- **KNOX-Lizenzschlüssel**: Geben Sie den 25-stelligen KNOX-Lizenzschlüssel ein, den Sie von Samsung erhalten haben.

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Samsung SAFE-Firewallrichtlinie

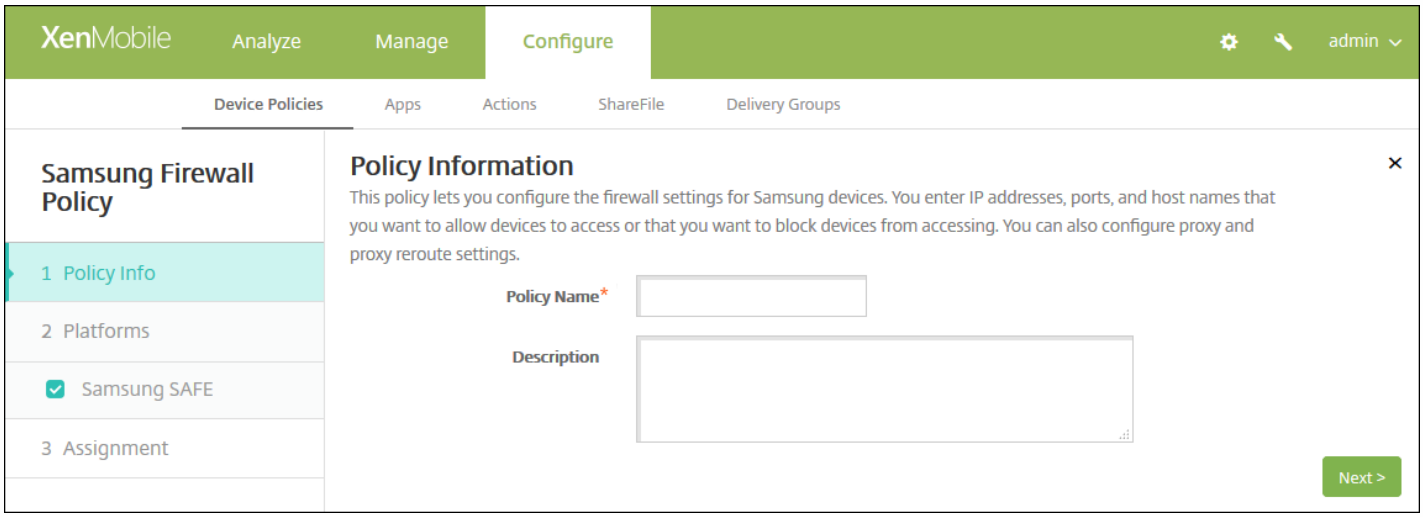
Feb 24, 2017

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.

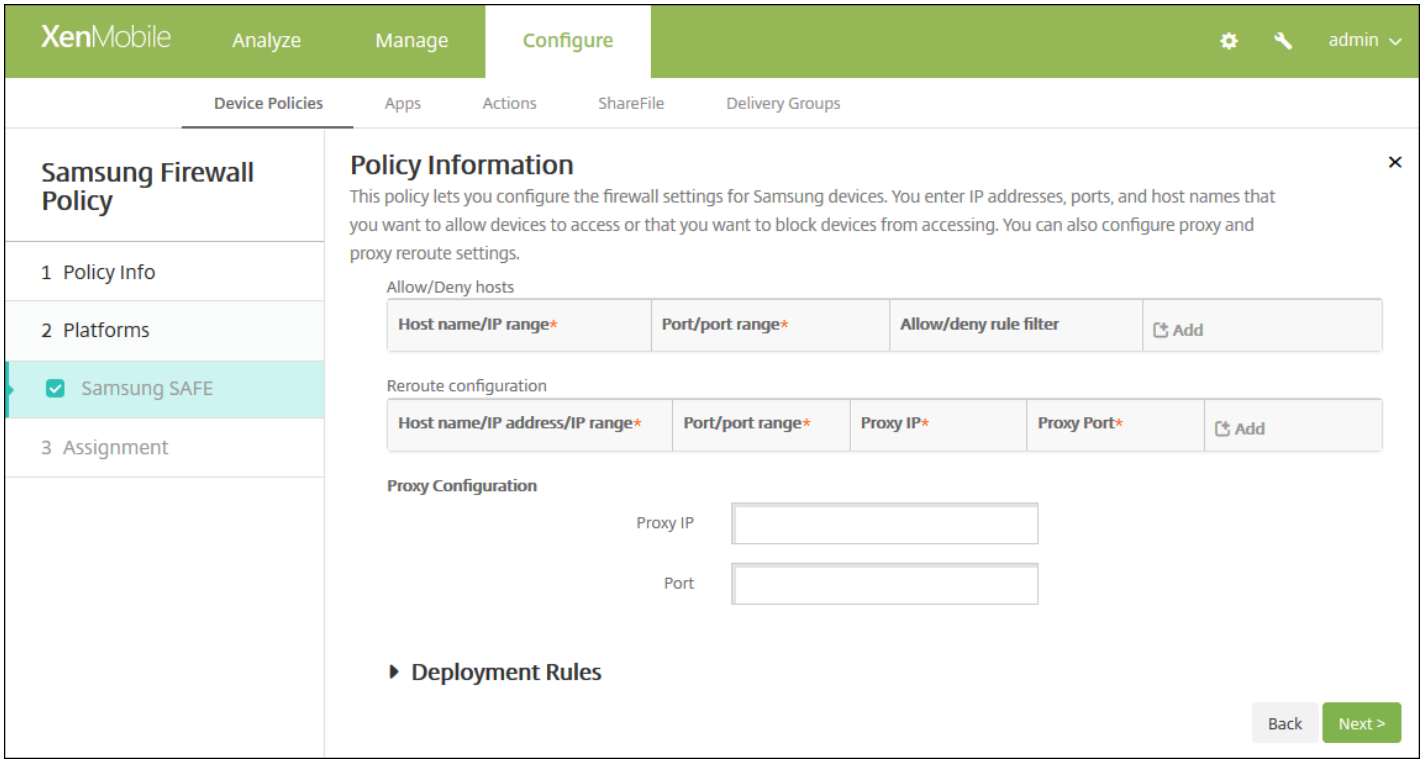
3. Erweitern Sie **Mehr** und klicken Sie unter **Netzwerkzugriff** auf **Samsung-Firewall**. Die Seite **Samsung-Firewall** wird angezeigt.



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.

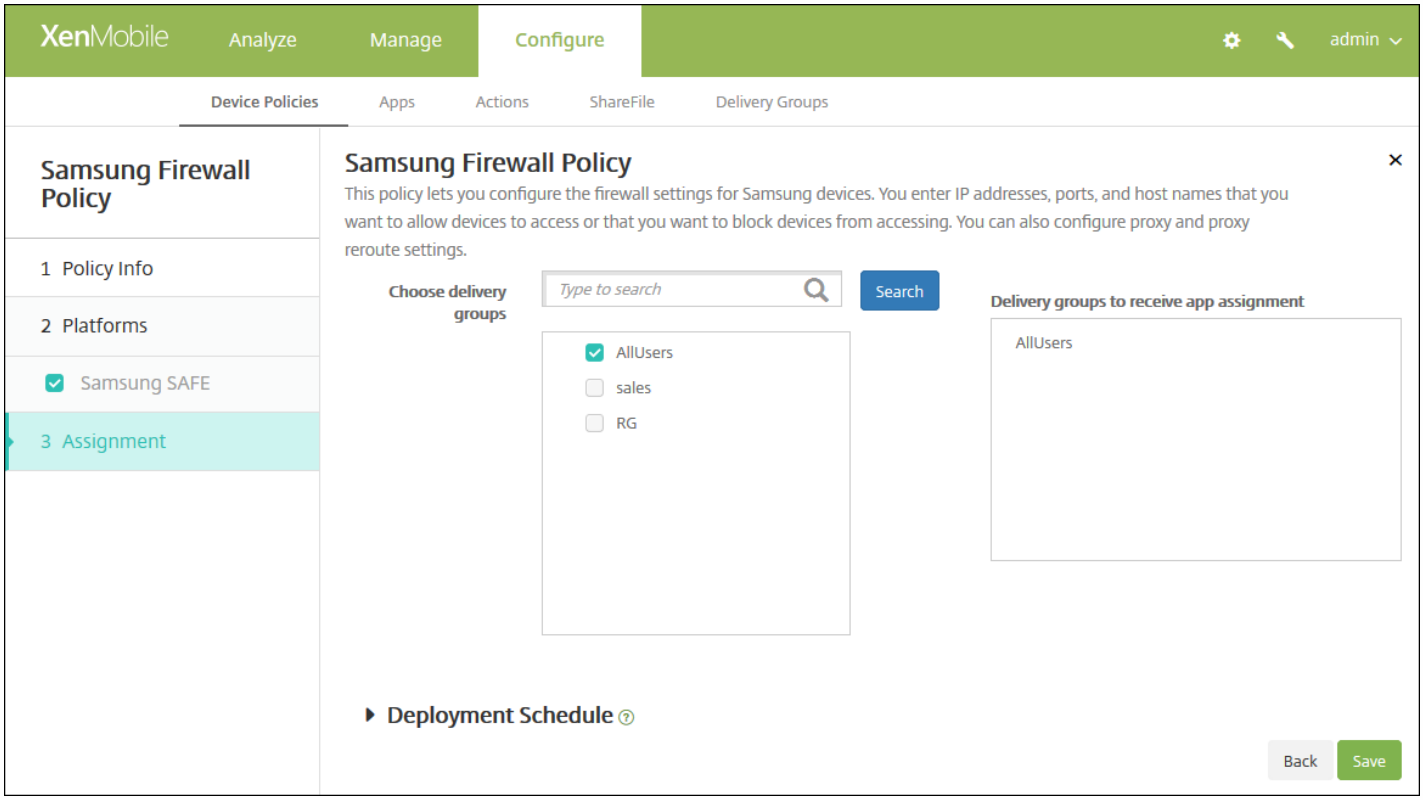
    Zum Bearbeiten eines Elements zeigen Sie auf dessen Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

SCEP-Geräterichtlinien

Feb 24, 2017

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.

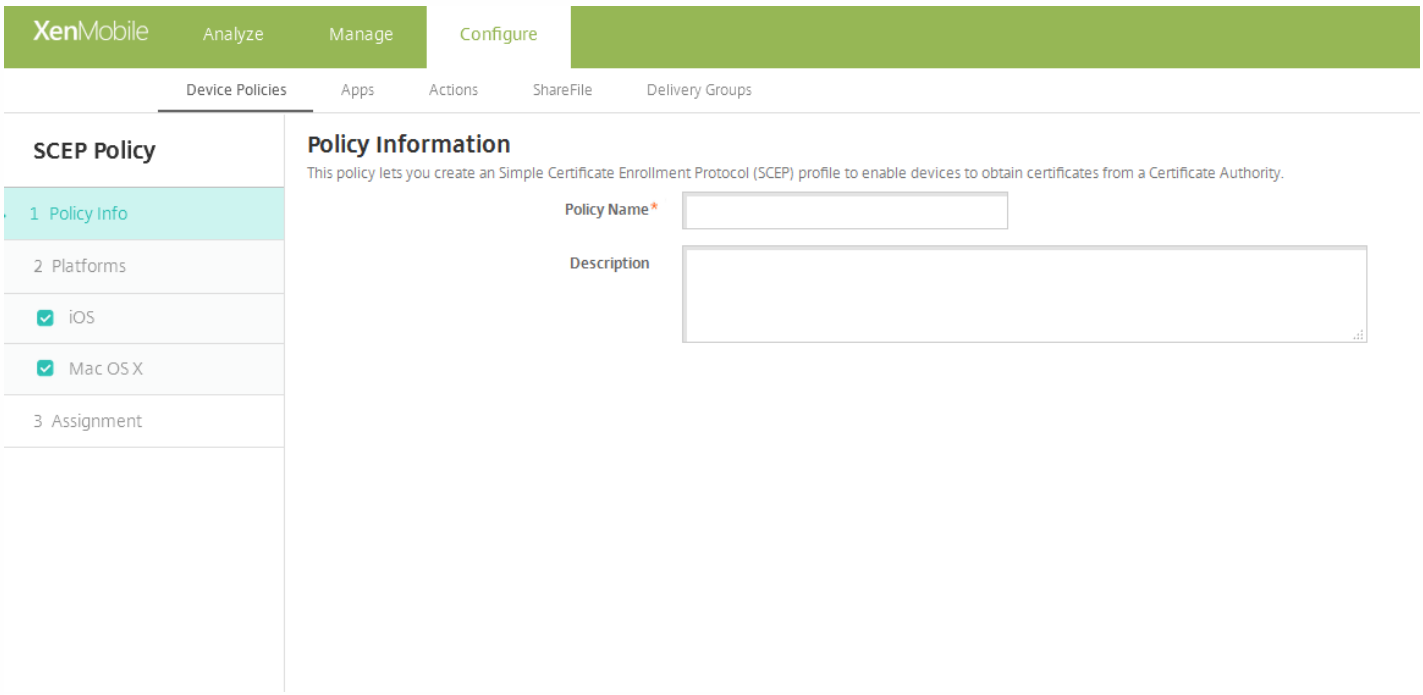
iOS-Einstellungen

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.

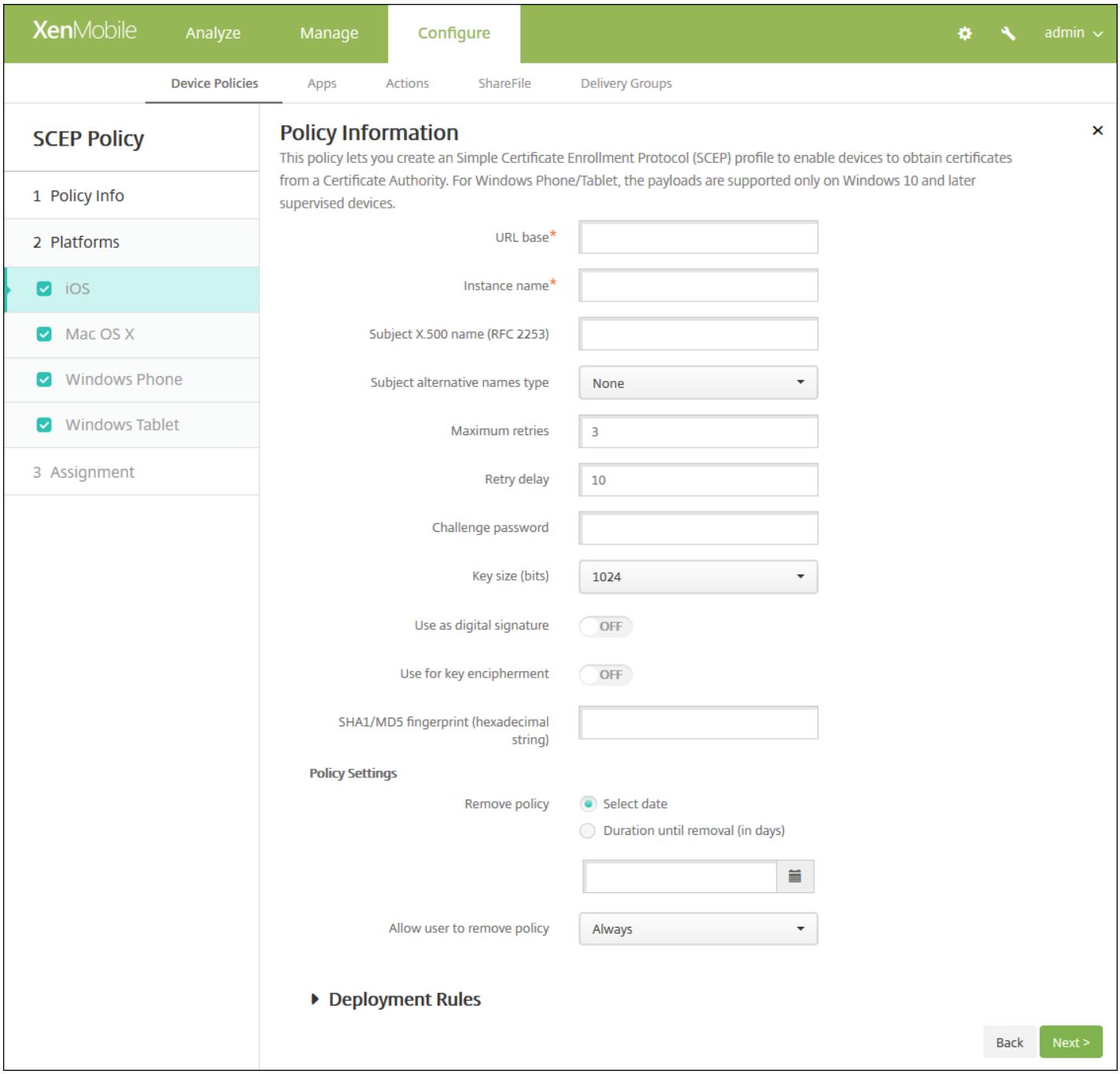
5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

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



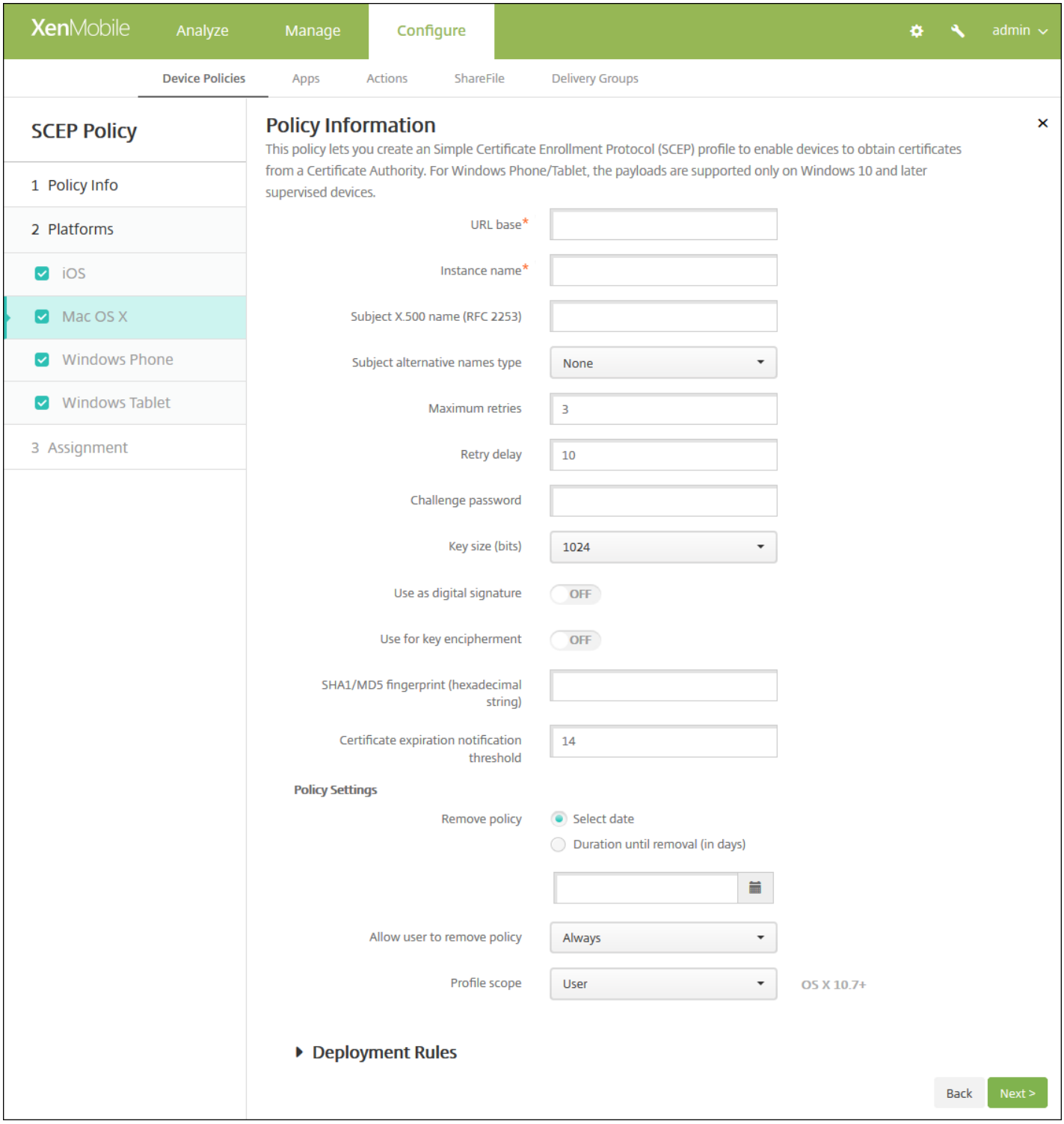
Konfigurieren Sie folgende Einstellungen:

- **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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **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

Feb 24, 2017

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.

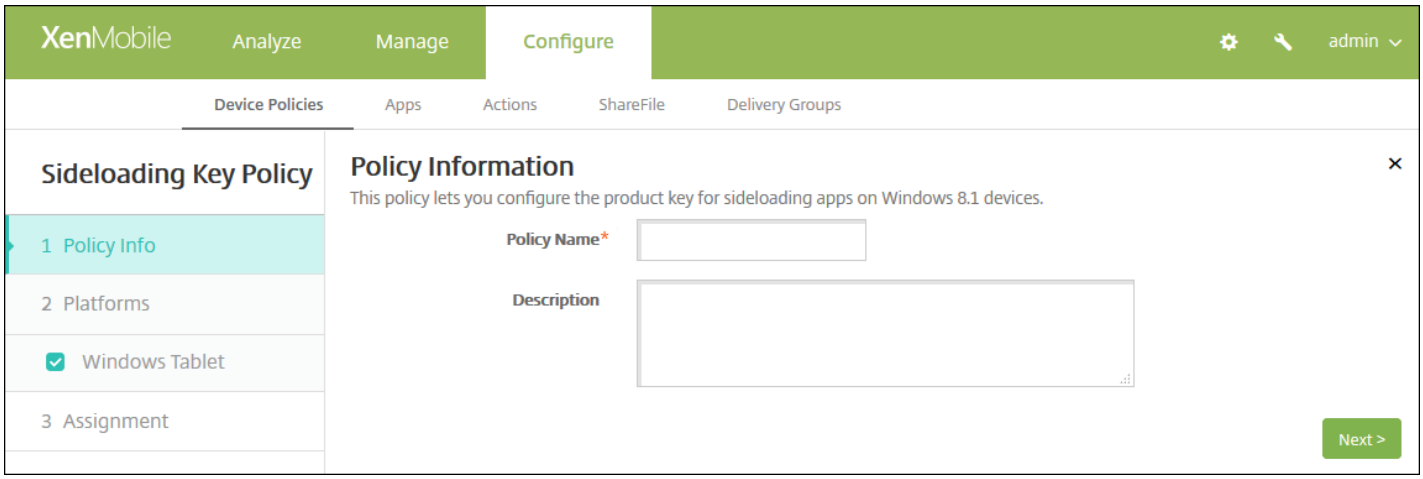
Sie benötigen zum Erstellen der Richtlinie die folgenden Informationen:

- 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.

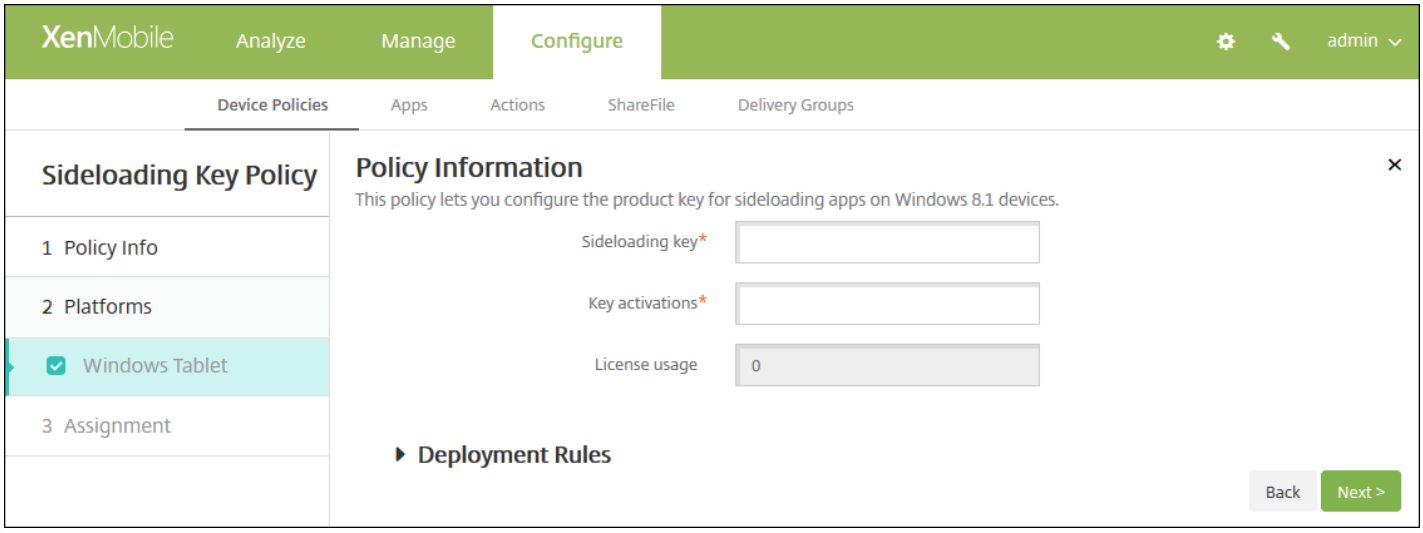
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Sideloadingschlüssel**. Die Seite **Sideloadingschlüssel** wird angezeigt.



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.

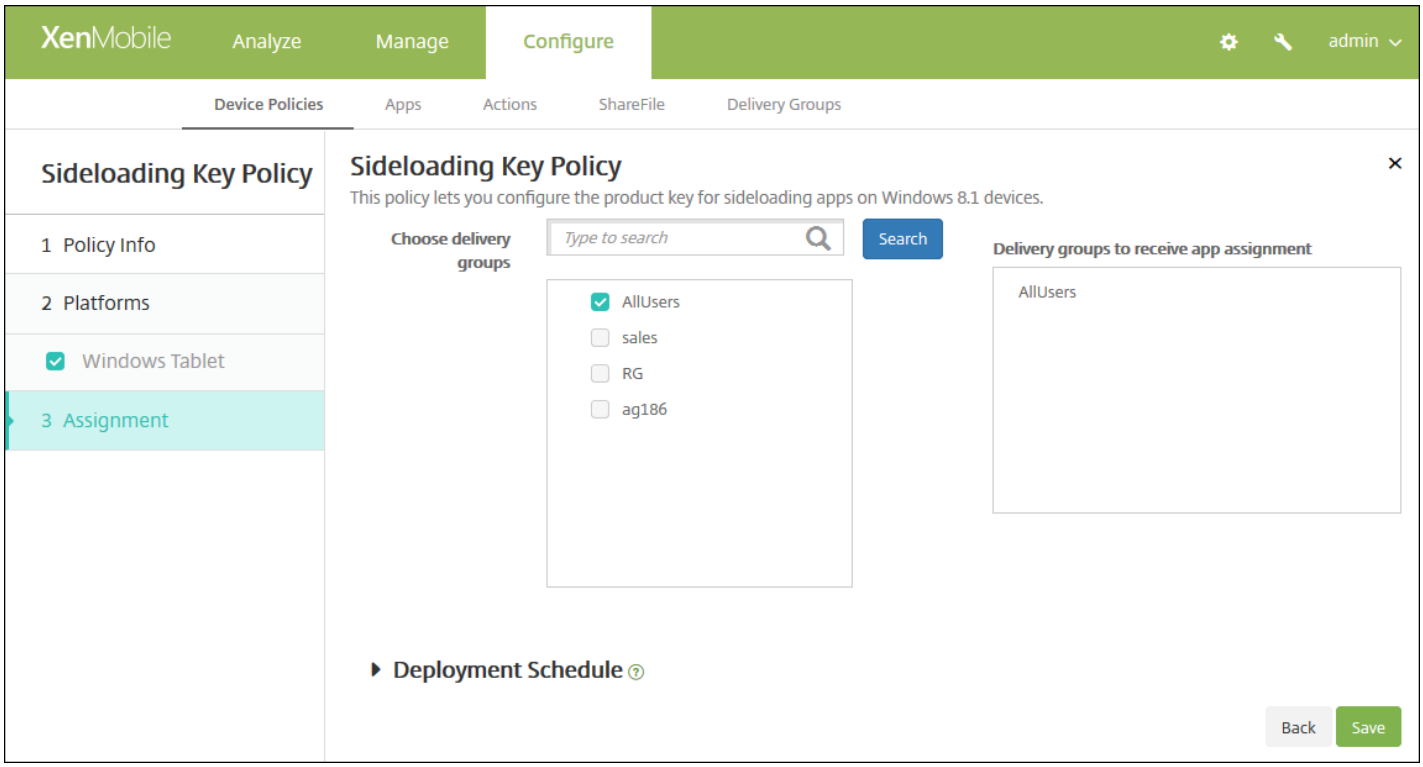


6. Konfigurieren Sie die folgenden Einstellungen:

- **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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie für Signaturzertifikate

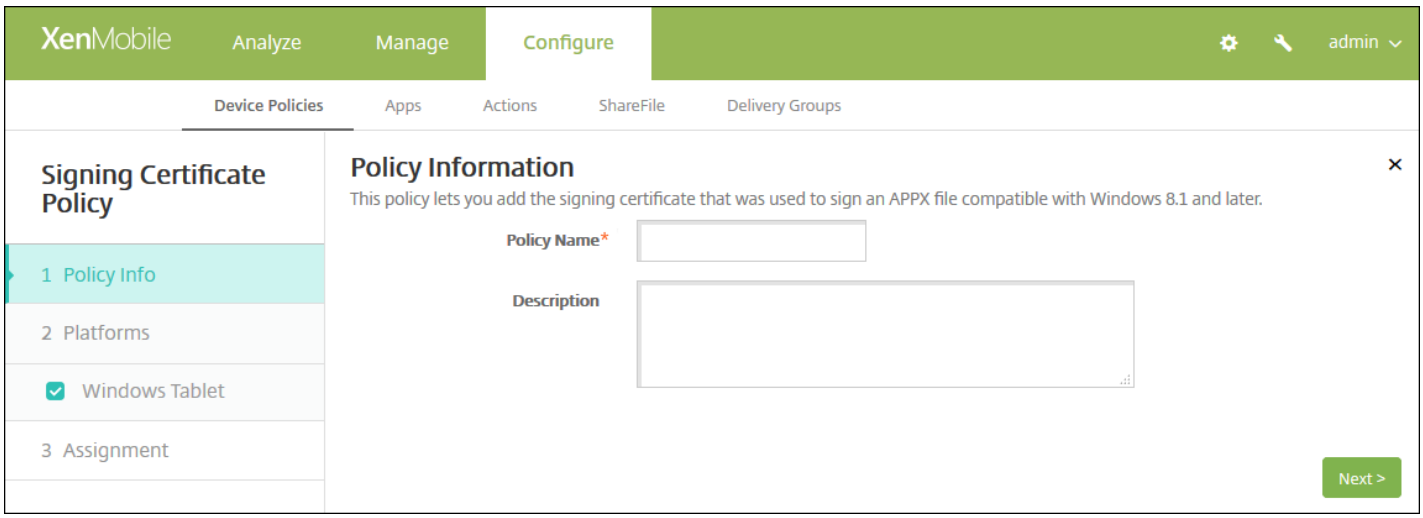
Feb 24, 2017

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.

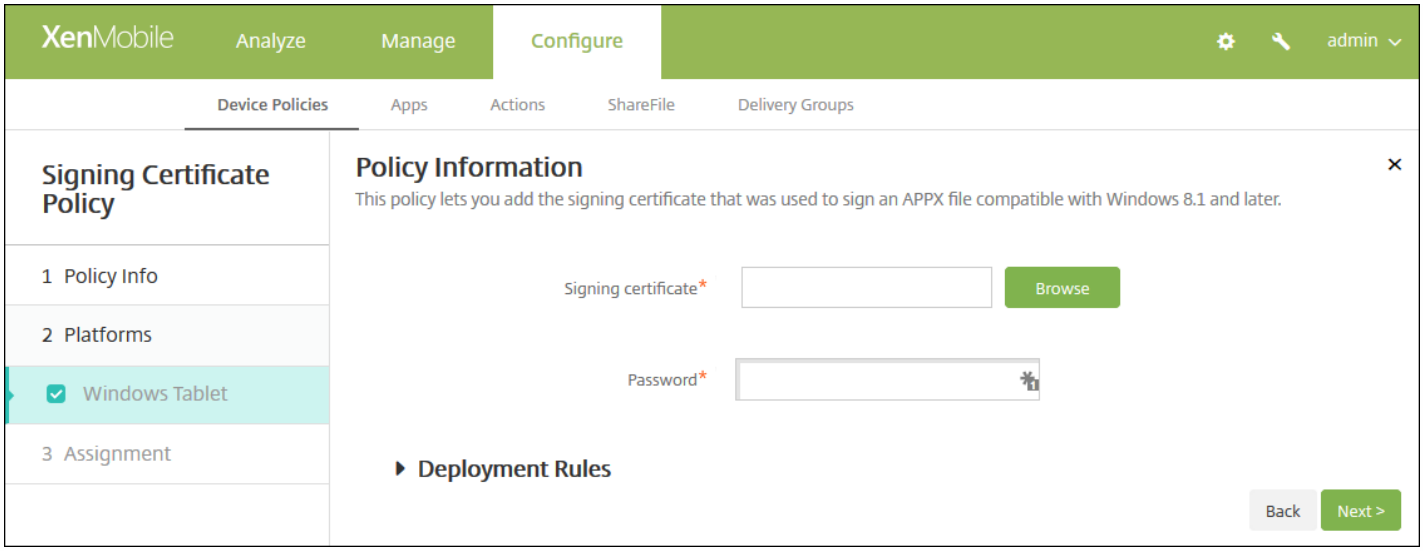
3. Klicken Sie auf **Mehr** und dann unter **Apps** auf **Signaturzertifikat**. Die Seite **Signaturzertifikat** wird angezeigt.



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.

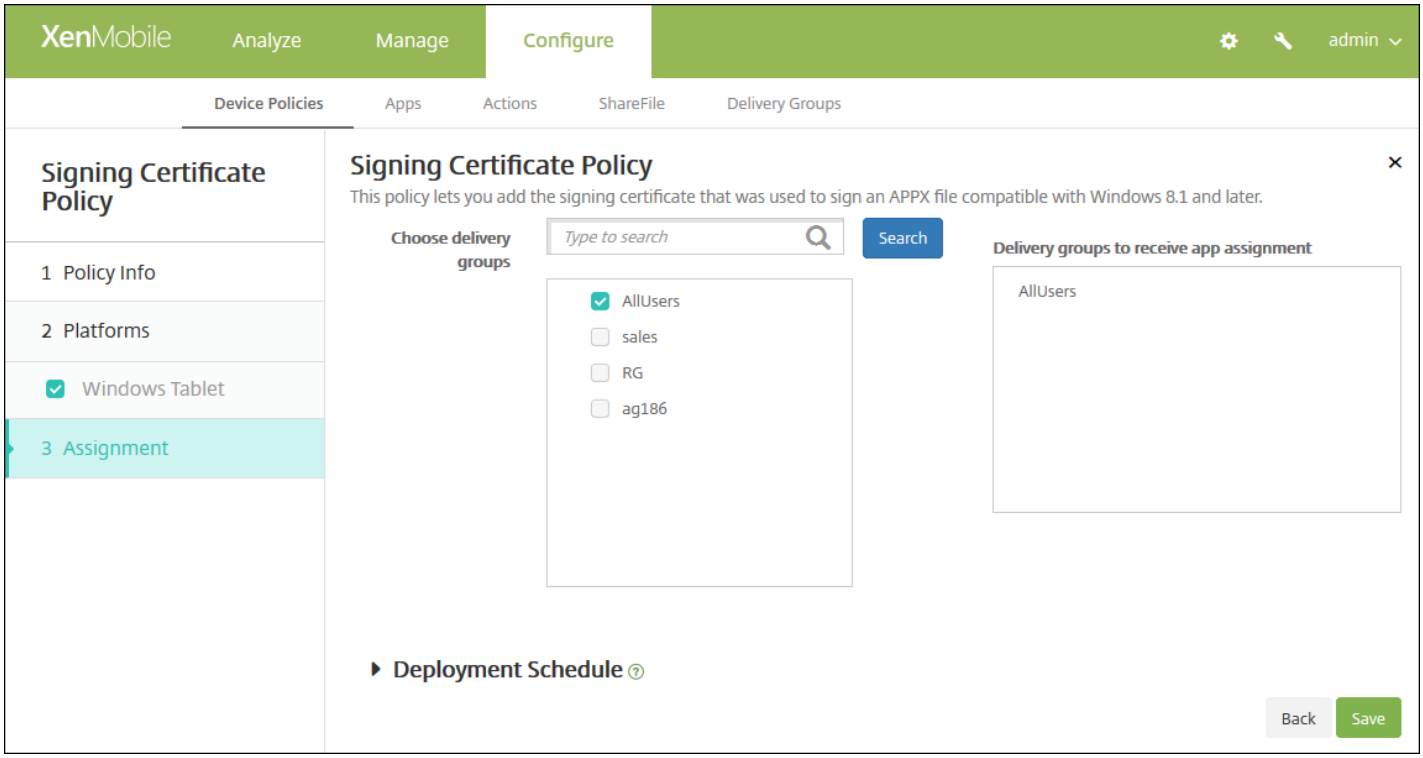


6. Konfigurieren Sie die folgenden Einstellungen:

- **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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Single Sign-On-Kontorichtlinien

Feb 24, 2017

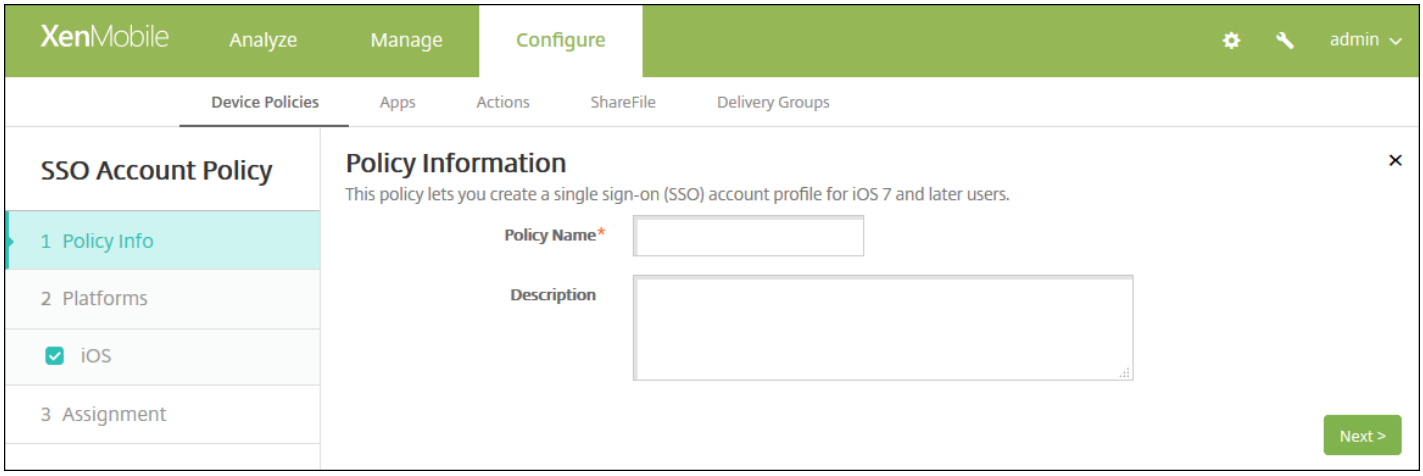
Sie erstellen Single Sign-On-Konten (SSO) in XenMobile, damit Benutzer nach einmaliger Anmeldung auf XenMobile und interne Unternehmensressourcen von unterschiedlichen Apps aus zugreifen können. Sie müssen keine Anmeldeinformationen auf dem Gerät speichern. Die Unternehmensanmeldeinformationen des SSO-Kontos 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.

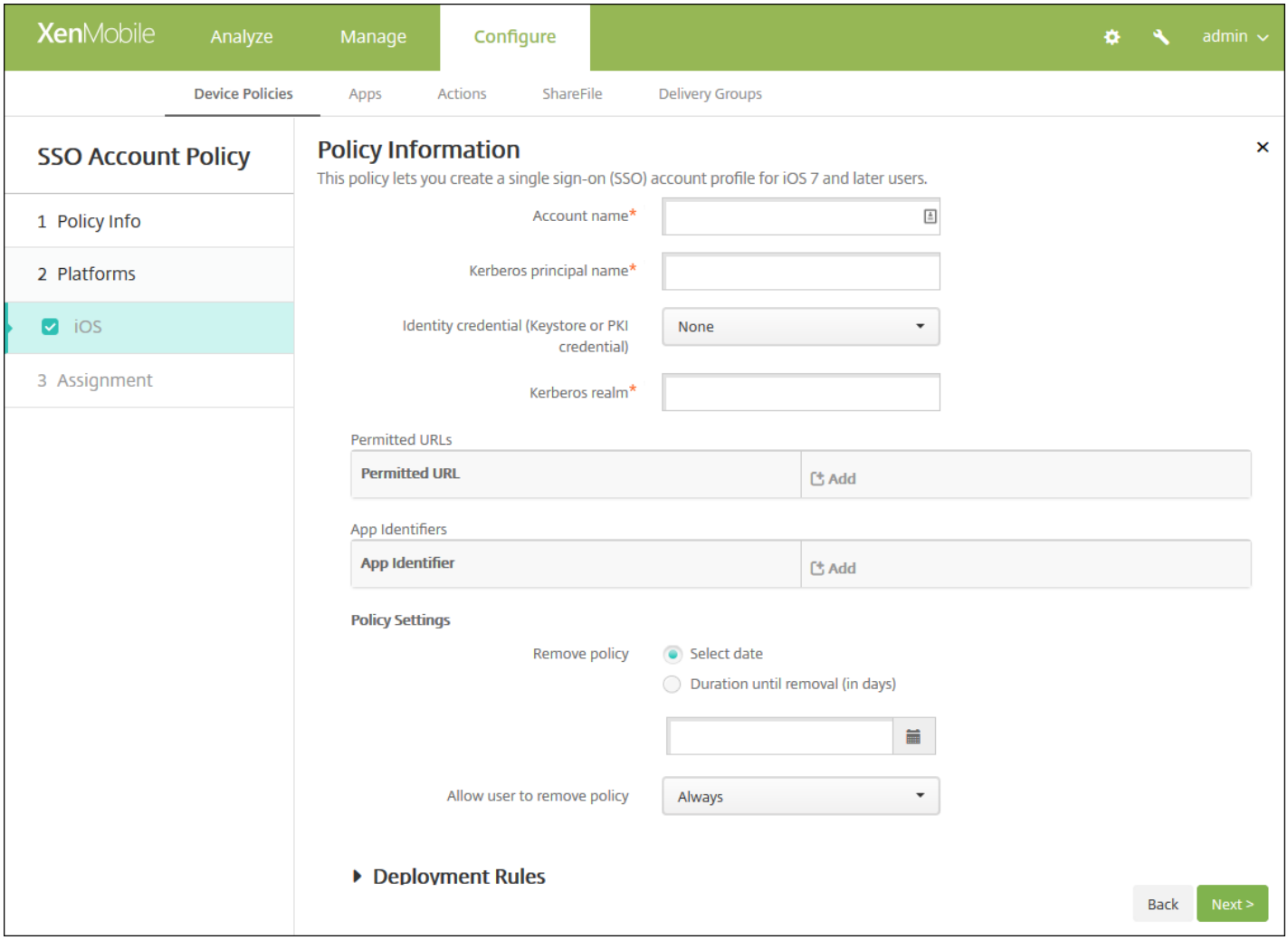
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **SSO-Konto**. Die Seite für die Richtlinieninformationen der Richtlinie **SSO-Konto** wird angezeigt.



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 Kerberos-Anmeldung zwischengespeicherten Tokens. 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.

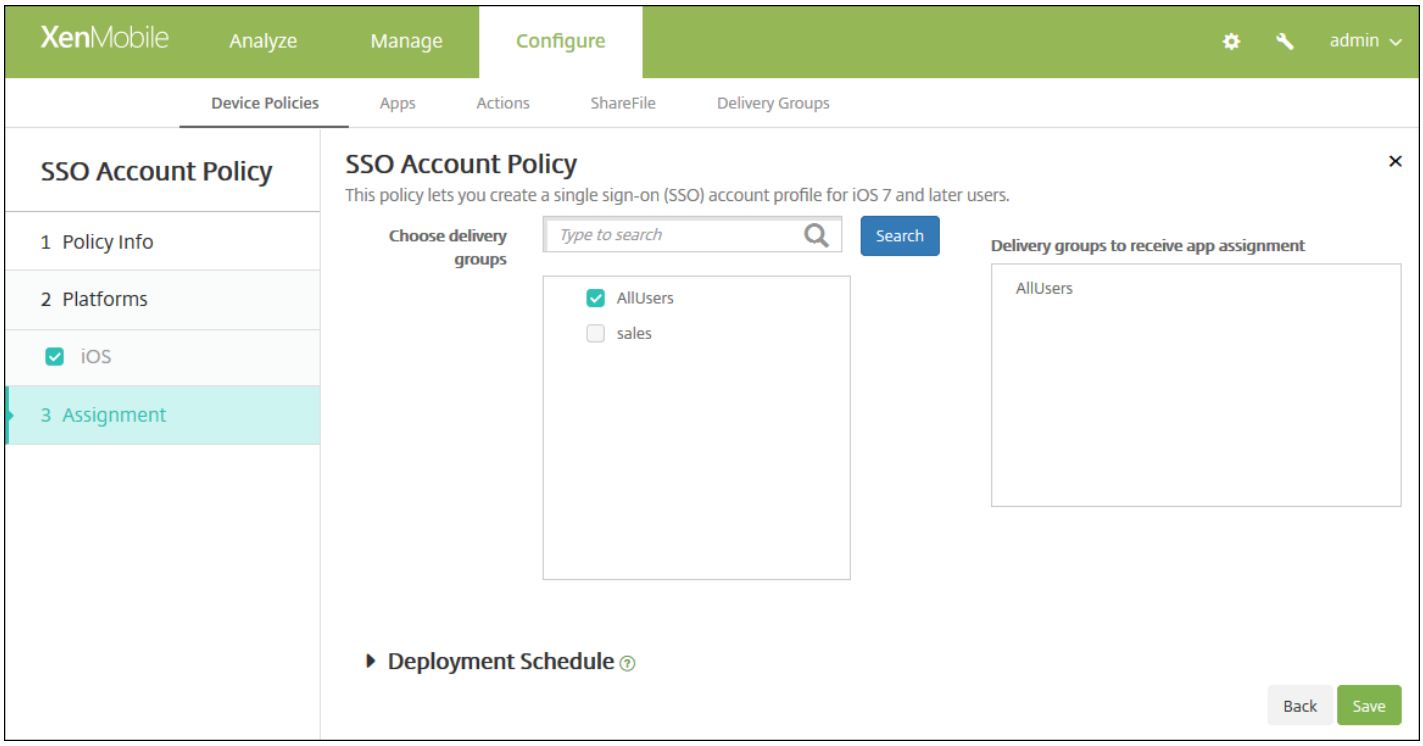
    Hinweis: Zum Löschen vorhandener URLs oder App-IDs zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf "Löschen" zum Löschen des Eintrags oder auf "Bearbeiten", um ihn beizubehalten.

    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 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.

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

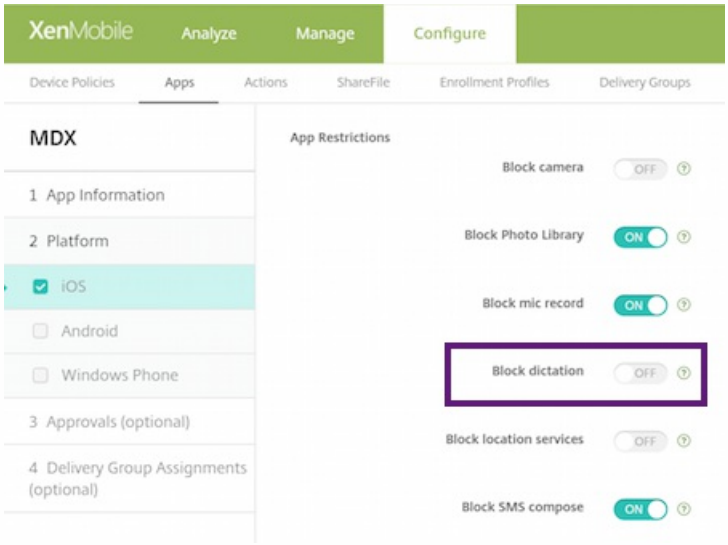
Richtlinien für Siri und die Diktierfunktion

Feb 24, 2017

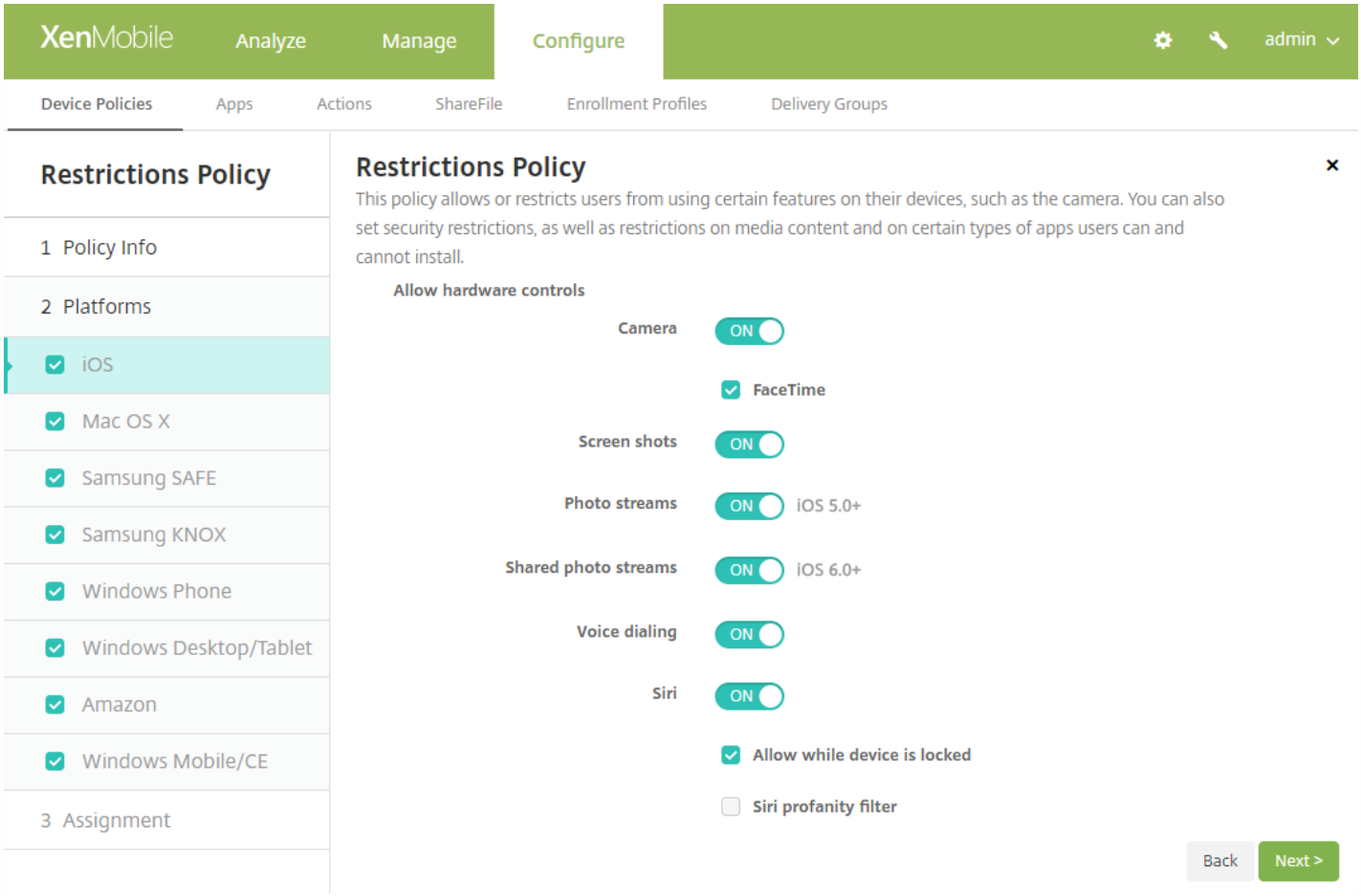
Wenn Benutzer auf einem iOS-Gerät Siri eine Frage stellen oder Text diktieren, werden die Sprachdaten von Apple zur Verbesserung von Siri gesammelt. Die Sprachdaten werden über die cloudbasierten Dienste von Apple gesendet und verlassen somit den sicheren XenMobile-Container. Diktierter Text verbleibt 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

Feb 24, 2017

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

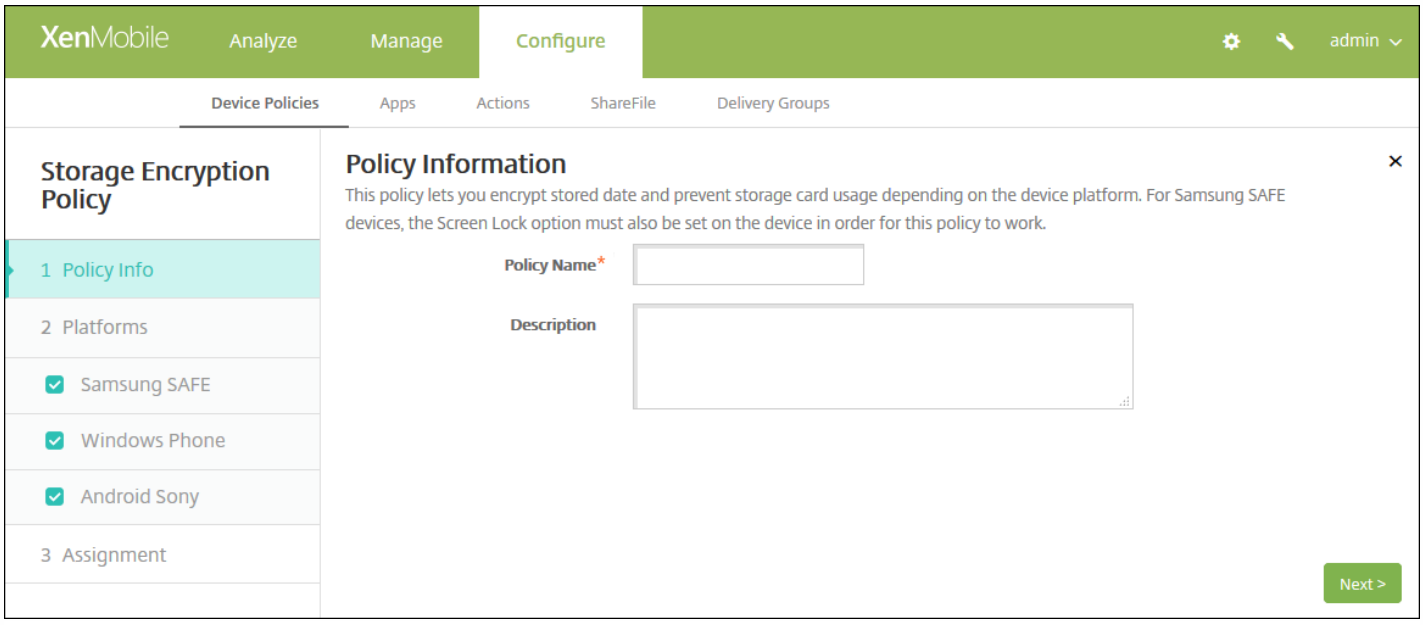
Hinweis: Vergewissern Sie sich vor der Konfiguration dieser Richtlinie, dass bei Samsung SAFE-Geräten die folgenden Anforderungen erfüllt sind:

- 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.

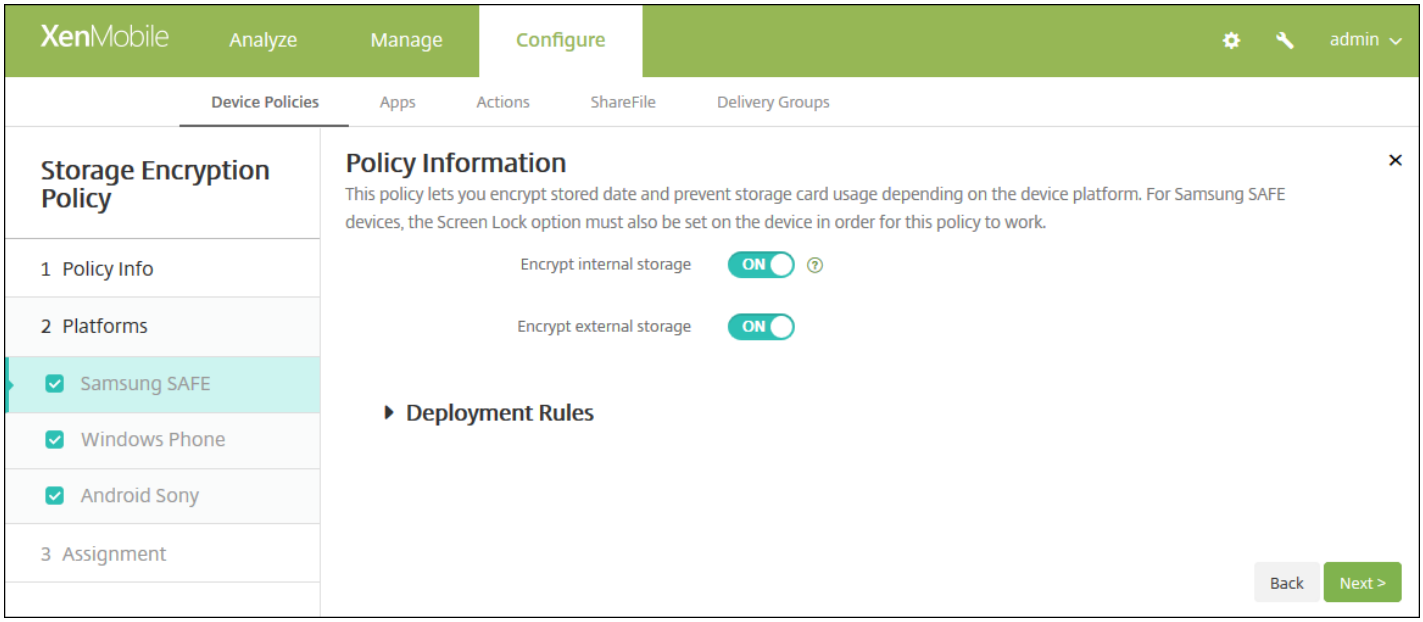
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

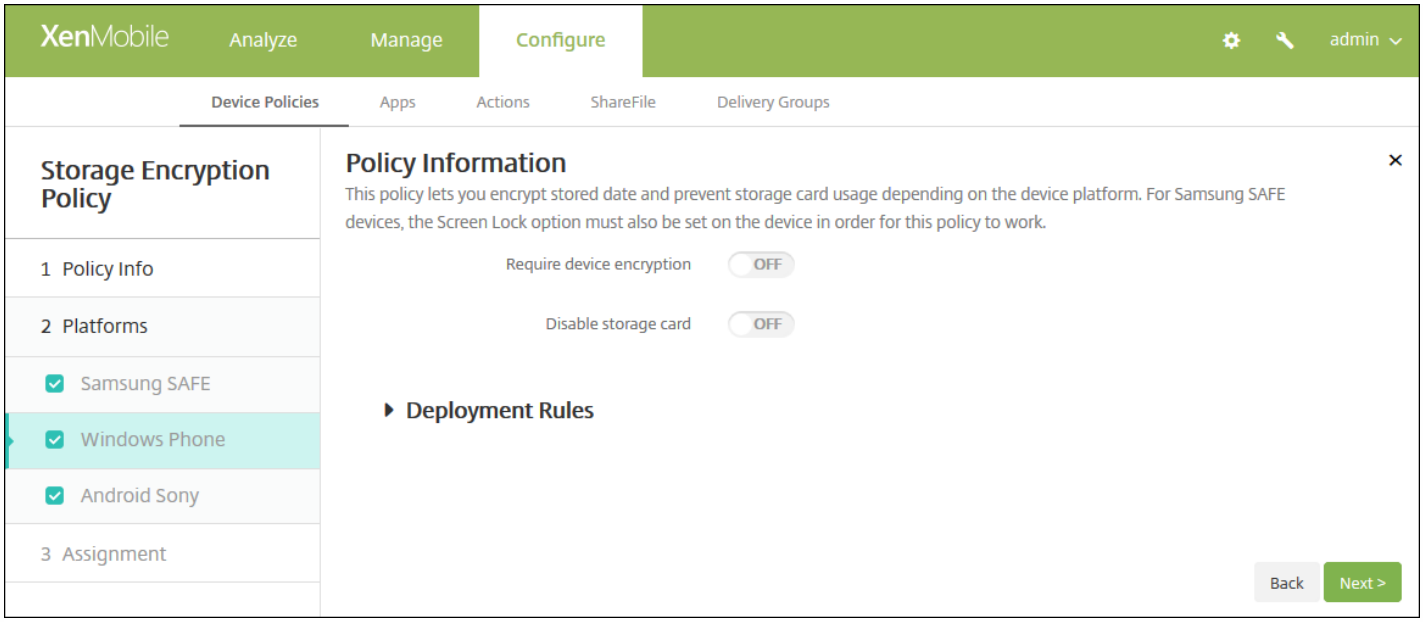
Konfigurieren der Samsung SAFE-Einstellungen



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. Der Standardwert ist **EIN**.
- **Externen Speicher verschlüsseln**: Wählen Sie aus, ob der externe Speicher auf Geräten verschlüsselt werden soll. Der Standardwert ist **EIN**.

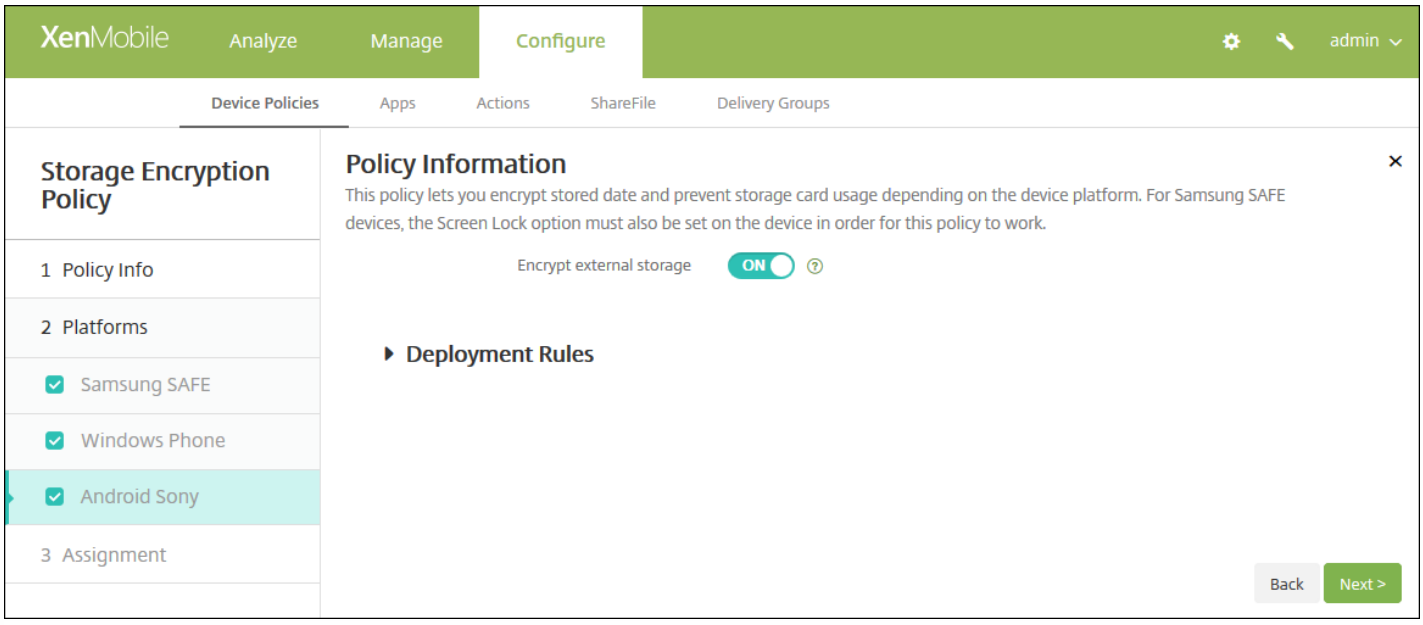
Konfigurieren von Windows Phone-Einstellungen



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**.

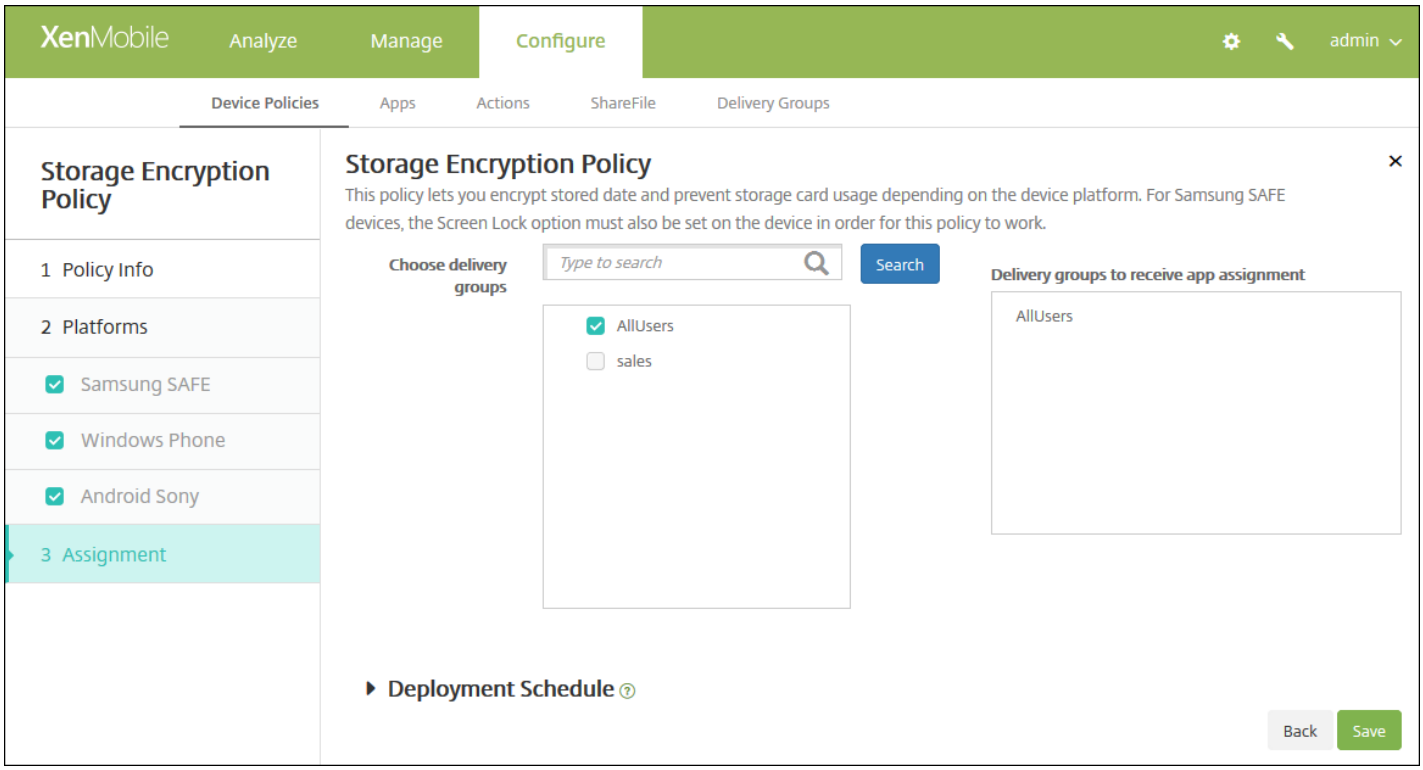
Konfigurieren von Android Sony-Einstellungen



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. Der Standardwert ist **EIN**.

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Richtlinie für abonnierte Kalender

Feb 24, 2017

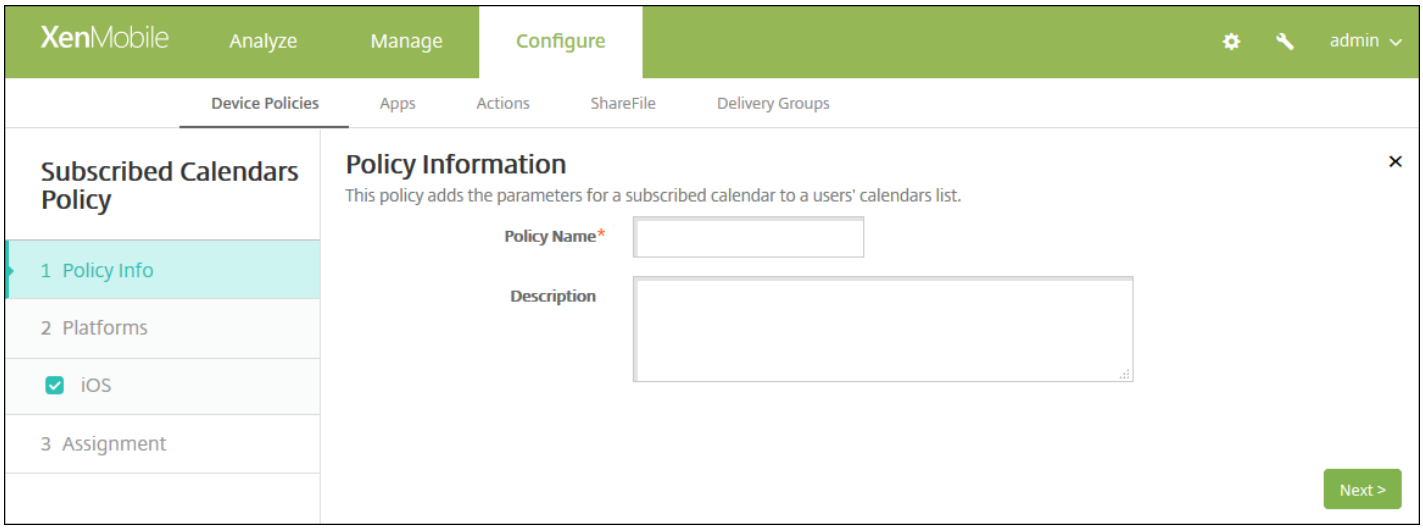
Sie können in XenMobile eine Richtlinie einrichten, mit der ein abonnierter Kalender der Liste der Kalender auf iOS-Geräten hinzugefügt wird. Die Liste der öffentlichen Kalender, die zum Abonnieren verfügbar sind, finden Sie unter www.apple.com/downloads/macosx/calendars.

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 > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

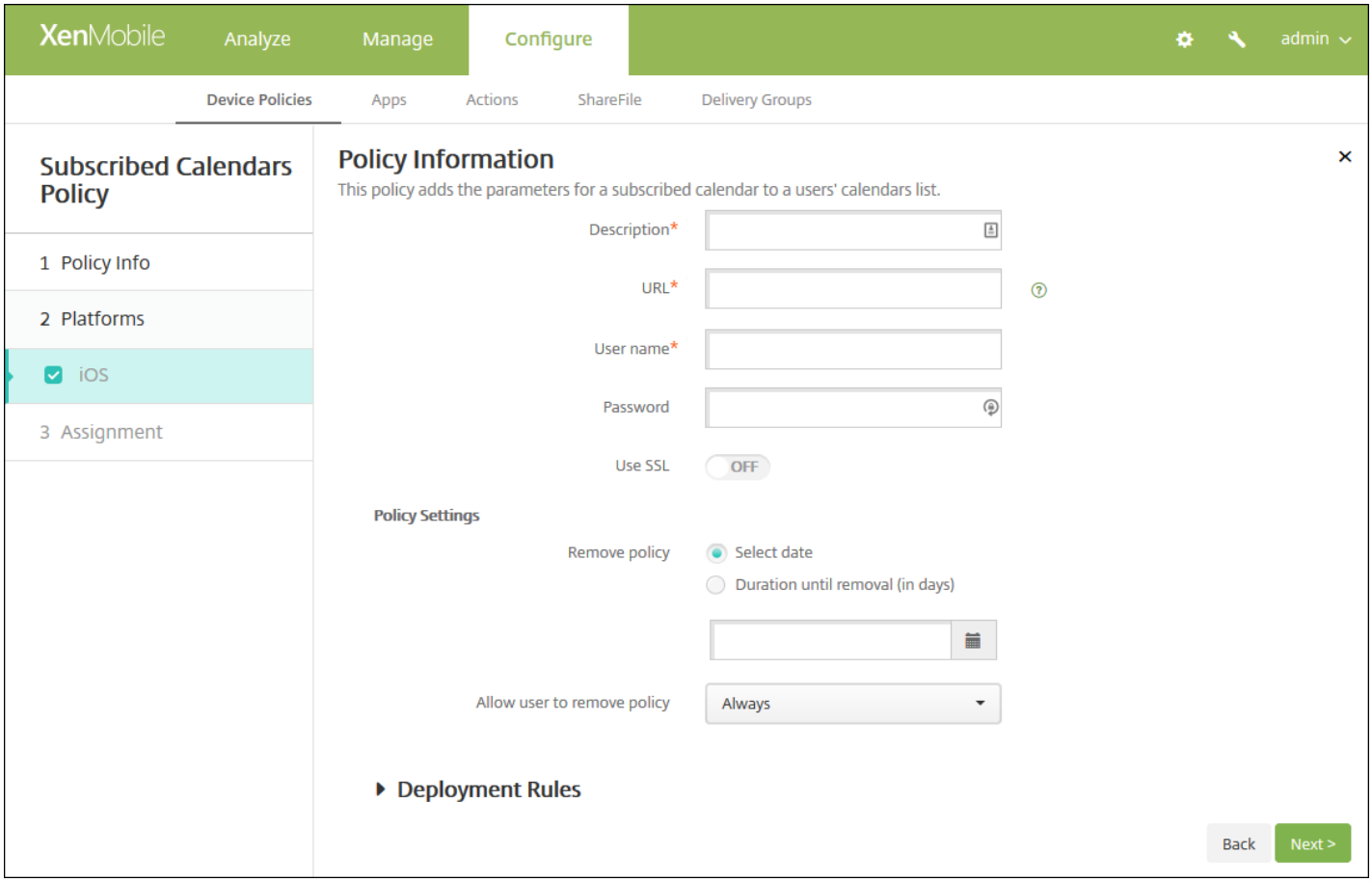
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **Abonnierte Kalender**. Die Seite für die Richtlinieninformationen der Richtlinie **Abonnierte Kalender** wird angezeigt.



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.

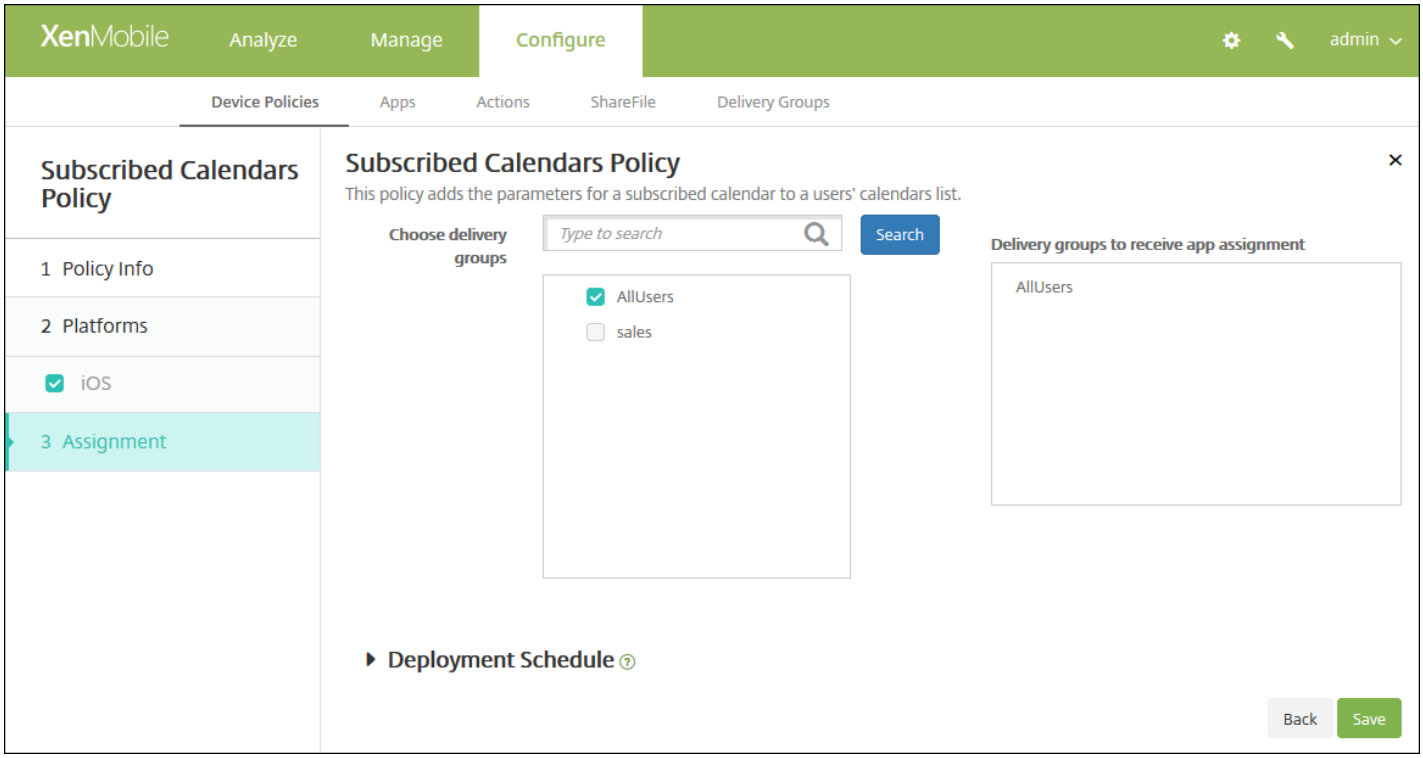


6. Konfigurieren Sie die folgenden Einstellungen:

- **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 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.

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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

AGB-Geräterichtlinien

Feb 24, 2017

Sie erstellen Geräterichtlinien für Nutzungsbestimmungen in XenMobile, wenn Sie möchten, dass die Benutzer die unternehmensspezifischen Richtlinien für Verbindungen mit dem Unternehmensnetzwerk akzeptieren. Wenn Benutzer ihr Gerät bei XenMobile registrieren, werden ihnen die Nutzungsbestimmungen angezeigt. Sie müssen diese akzeptieren, damit sie ihr Gerät registrieren können. Lehnen sie die Nutzungsbedingungen ab, wird die Registrierung abgebrochen.

Sie können mehrere Richtlinien für Nutzungsbestimmungen in unterschiedlichen Sprachen erstellen, wenn Ihr Unternehmen internationale Benutzer hat und Sie möchten, dass diese die Nutzungsbestimmungen in ihrer Muttersprache annehmen. 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.

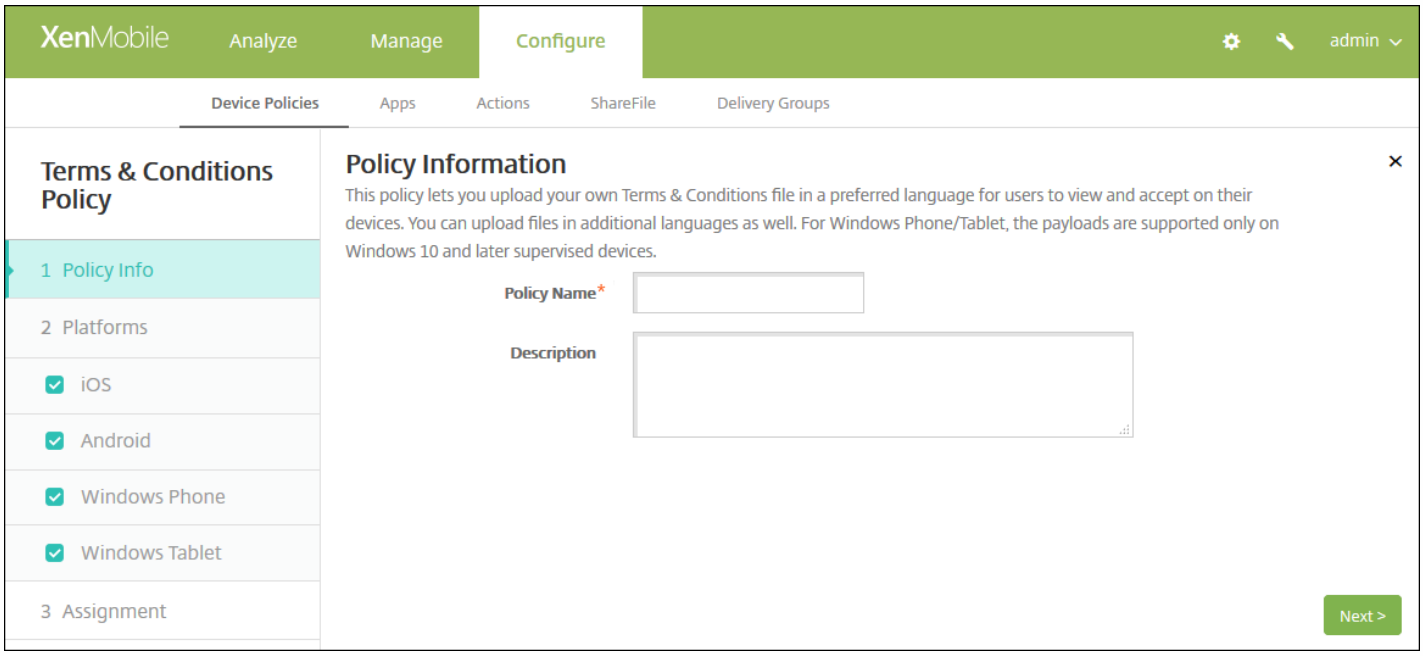
iOS- und Android-Einstellungen

Windows Phone- und Windows Tablet-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.

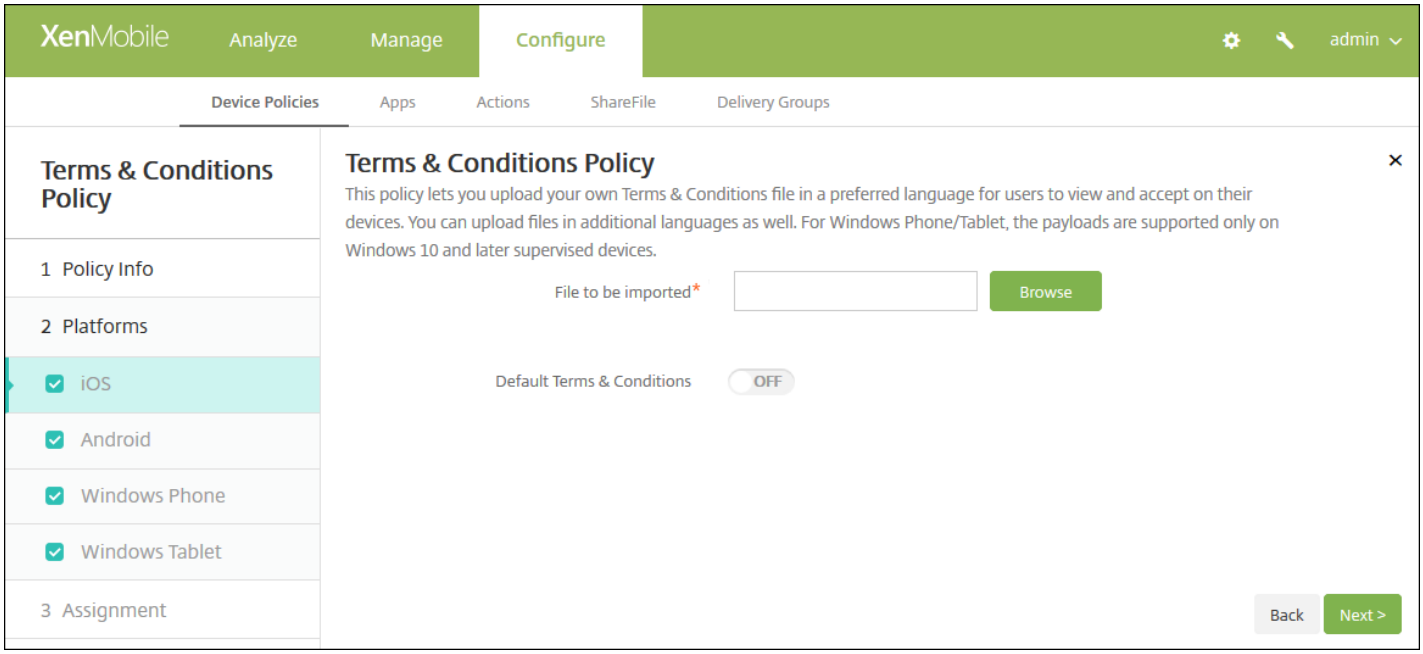
3. Klicken Sie auf **AGB**. Die Seite **Richtlinie für AGB** wird angezeigt.



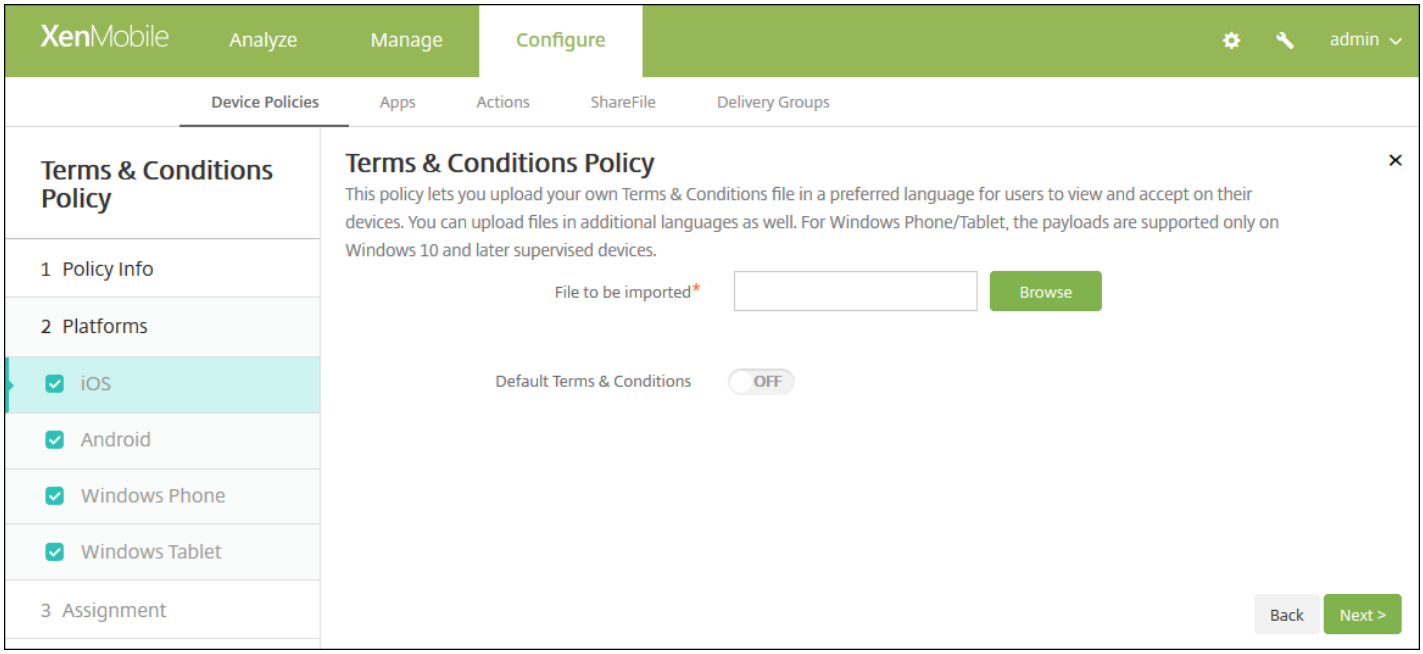
4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

- **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 AGB-Richtlinieninformationen wird angezeigt.



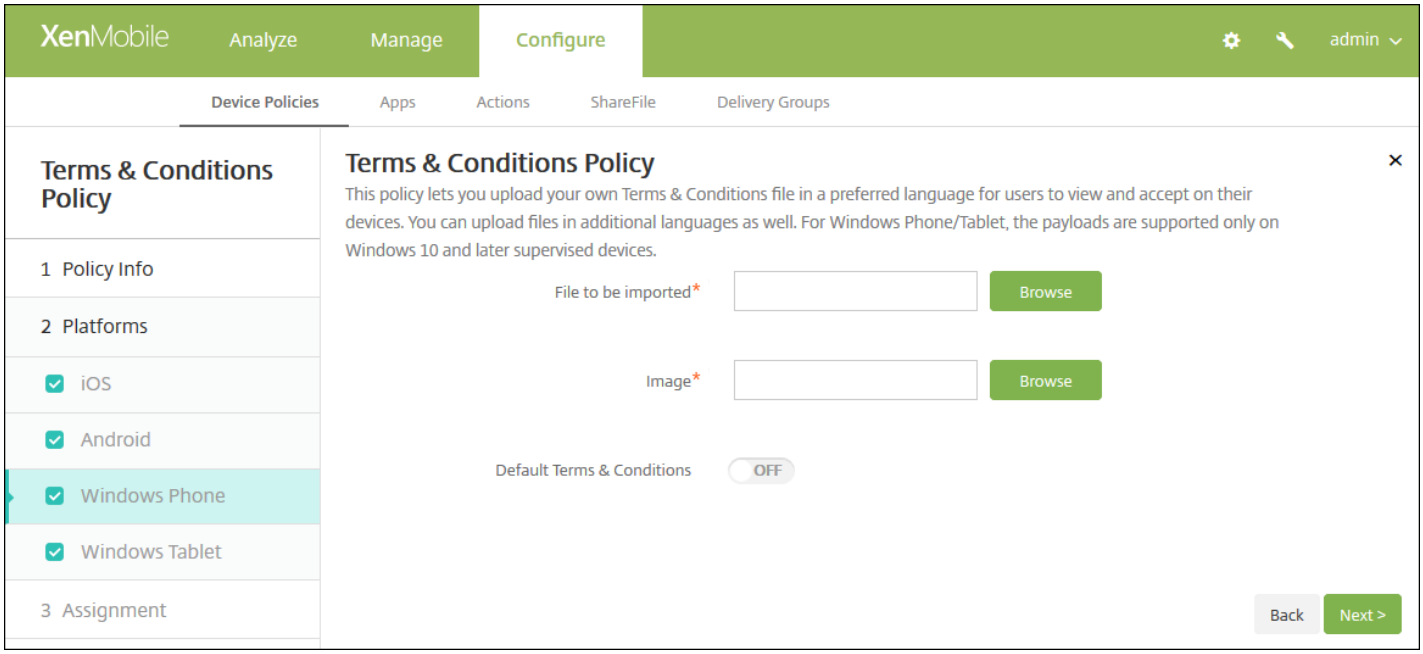
iOS- und Android-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Zu importierende Datei**: Klicken Sie zur Auswahl der zu importierenden Datei mit den Nutzungsbestimmungen auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.
- **AGB (Standard)**: Wählen Sie aus, ob die importierte Datei als Standarddokument für Benutzer verwendet werden soll, die Mitglied mehrerer Gruppen mit unterschiedlichen AGB sind. Der Standardwert ist **AUS**.

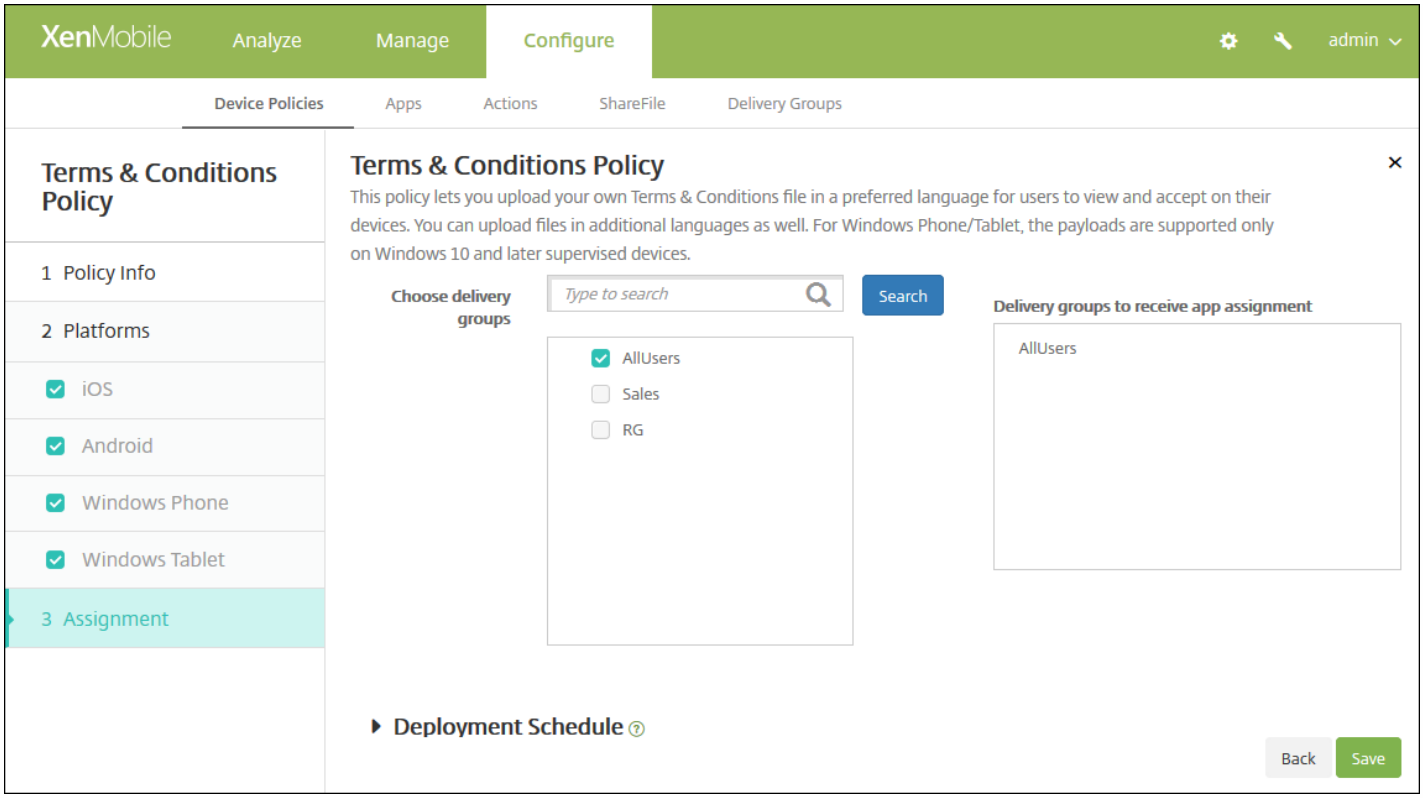
Windows Phone- und Windows Tablet-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Zu importierende Datei**: Klicken Sie zur Auswahl der zu importierenden Datei mit den Nutzungsbestimmungen auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.
- **Bild:** Klicken Sie zur Auswahl der zu importierenden Bilddatei auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.
- **AGB (Standard)**: Wählen Sie aus, ob die importierte Datei als Standarddokument für Benutzer verwendet werden soll, die Mitglied mehrerer Gruppen mit unterschiedlichen AGB sind. Der Standardwert ist **AUS**.

6. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die AGB-Richtlinie wird angezeigt.



7. 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.

8. Klicken Sie auf **Speichern**.

Versetzen eines iOS-Geräts mit dem Apple Configurator in den betreuten Modus

Feb 24, 2017

Mit Apple Configurator fügen Sie Geräte einem Apple-Computer an, auf dem die Apple Configurator-App ausgeführt wird. 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. Informationen zu Apple Configurator einschließlich Systemanforderungen finden Sie unter Informationen zu Apple Configurator.

> **Important**
>
> Beim Versetzen eines Geräts in den Überwachungsmodus wird die ausgewählte iOS-Version auf dem Gerät installiert und sämtliche zuvor gespeicherten Benutzerdaten und Apps werden von dem Gerät gelöscht.

1. Installieren Sie den Apple Configurator aus iTunes.
2. Schließen Sie das iOS-Gerät an den Apple-Computer an.
3. Starten Sie den Apple Configurator. Der Configurator zeigt an, dass ein Gerät zur Vorbereitung für die Betreuung vorhanden ist.
4. Vorbereiten des Geräts für die Betreuung:
    1. Legen Sie für die Überwachung die Option Ein fest. Citrix empfiehlt, diese Einstellung zu aktivieren, wenn Sie ein Gerät kontinuierlich durch regelmäßige Neuanwendung einer Konfiguration steuern möchten.
    2. Geben Sie optional einen Namen für das Gerät ein.
    3. Klicken Sie in iOS auf Latest für die neueste iOS-Version, die Sie installieren möchten.
5. Wenn das Gerät zur Überwachung vorbereitet werden kann, klicken Sie auf Prepare.

VPN-Geräterichtlinien

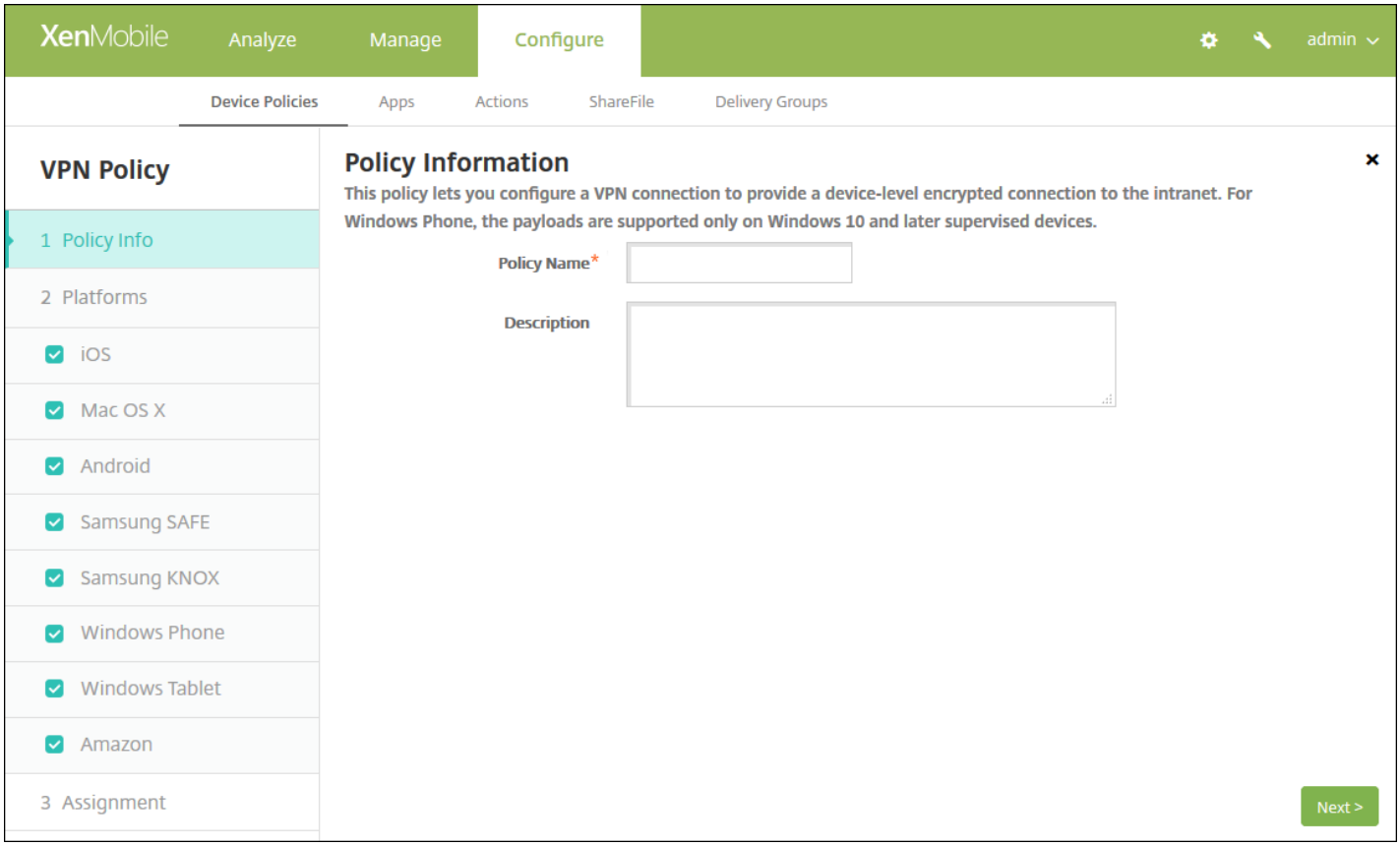
Feb 24, 2017

Sie können in XenMobile eine Geräterichtlinie hinzufügen, um die Einstellungen für ein VPN (virtuelles privates Netzwerk) für eine sichere Verbindung zwischen Geräten und Unternehmensressourcen zu konfigurieren. VPN-Richtlinien können für folgende Plattformen konfiguriert werden: iOS, Android (einschl. für Android for Work aktivierte Geräte), Samsung SAFE, Samsung KNOX, Windows Tablet, Windows Phone und Amazon. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Artikel detailliert 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 **VPN**. Die Seite **VPN** wird angezeigt.



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

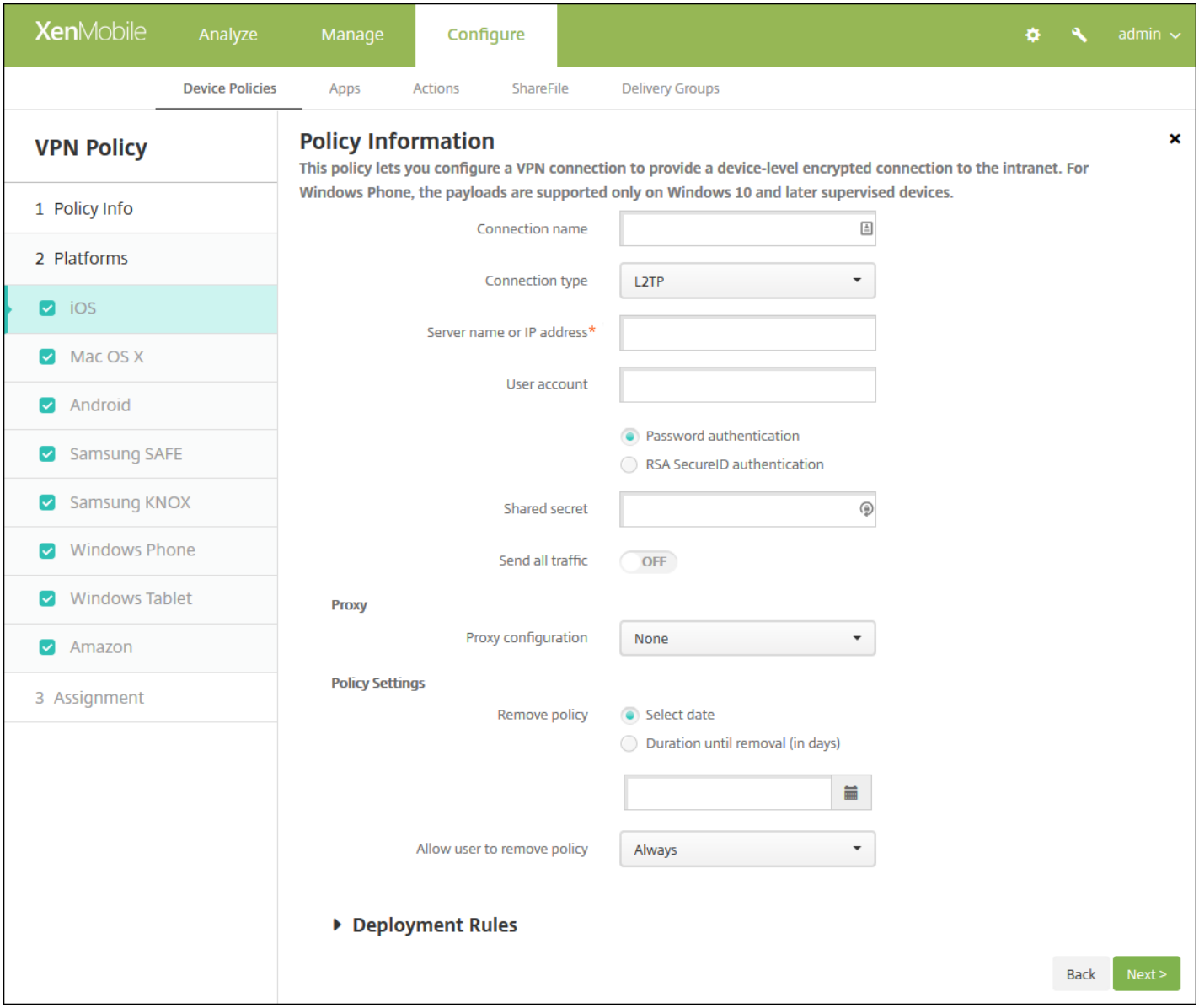
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt. Auf der Plattformseite sind alle Plattformen ausgewählt, die iOS-Plattform wird als erste angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Deaktivieren Sie die Plattformen, die Sie nicht konfigurieren möchten.

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 dieser Einstellungen

- **Verbindungsname**: Geben Sie einen Namen für die Verbindung ein.
- **Verbindungstyp**: Wählen Sie in der Liste das Protokoll aus, das für die Verbindung verwendet werden soll. Die Standardeinstellung ist **L2TP**.
  - **L2TP**: Layer-2-Tunnelingprotokoll mit Authentifizierung mit vorinstalliertem Schlüssel
  - **PPTP**: Point-to-Point Tunneling.
  - **IPSec**: Ihre Unternehmens-VPN-Verbindung
  - **Cisco AnyConnect**: Cisco AnyConnect VPN-Client
  - **Juniper SSL**: Juniper Networks SSL VPN-Client
  - **F5 SSL**: F5 Networks SSL VPN-Client
  - **SonicWALL Mobile Connect**: einheitlicher Dell VPN-Client für iOS
  - **Ariba VIA**: Ariba Networks Virtual Internet Access-Client
  - **IKEv2 (nur iOS)**: Internet Key Exchange Version 2 für iOS
  - **Citrix VPN**: Citrix VPN-Client für iOS

- **Benutzerdefiniertes SSL**: benutzerdefiniertes Secure Socket Layer

In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt.

Konfigurieren von L2TP

Konfigurieren von PPTP

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

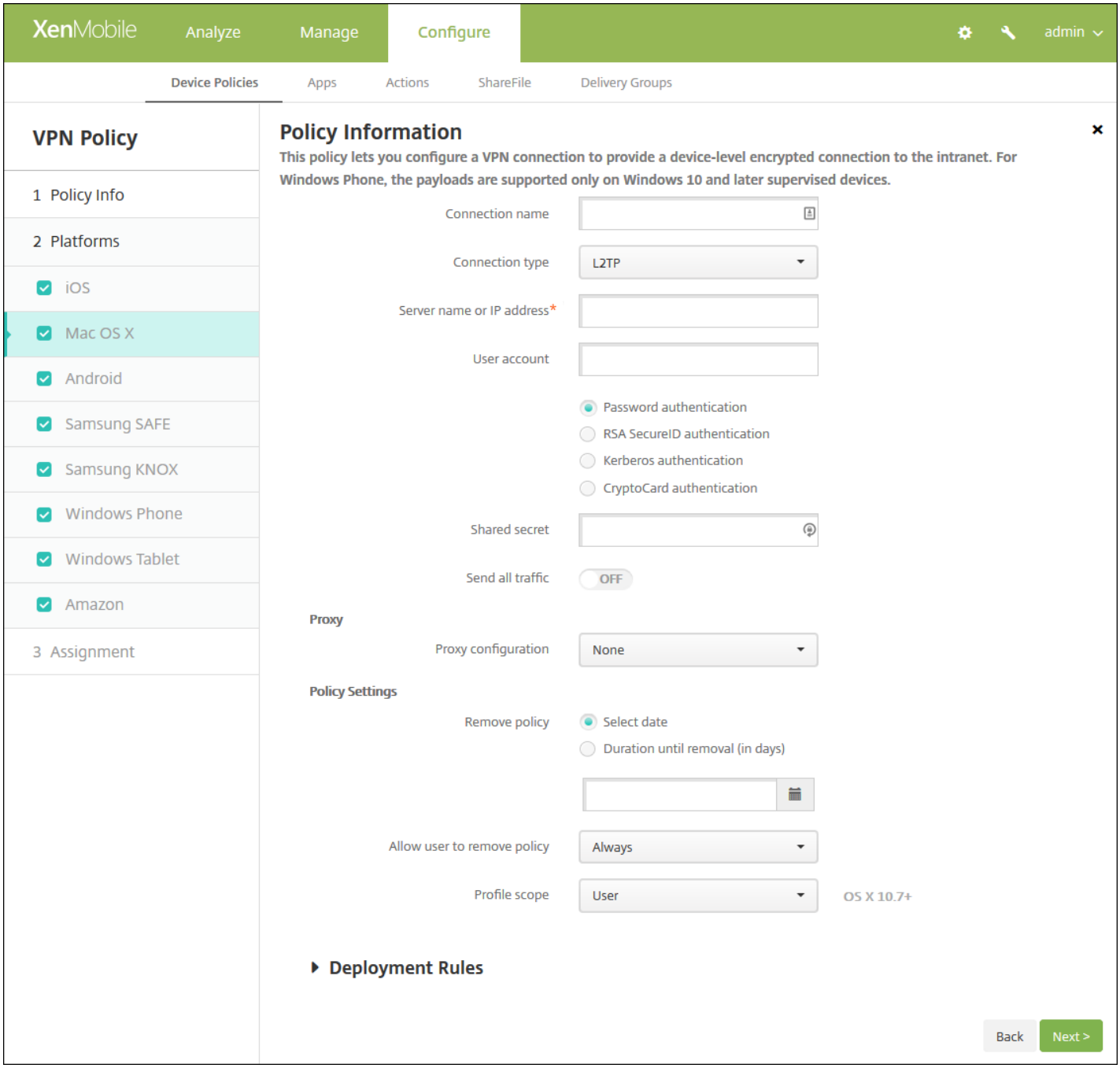
Konfigurieren von Citrix VPN-Protokoll

Konfigurieren des benutzerdefinierten SSL-Protokolls

Konfigurieren der Einstellungen für VPN bei Bedarf

- **Proxy**
  - **Proxykonfiguration**: Wählen Sie in der Liste nach Bedarf das Routing der VPN-Verbindung über einen Proxyserver aus. Der Standardwert ist **Ohne**.
    - 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 einen optionalen Benutzernamen für den Proxyserver ein.
      - **Kennwort**: Geben Sie ein optionales Kennwort für den Proxyserver ein.
    - Bei Auswahl von **Automatisch** konfigurieren Sie die folgende Einstellung:
      - **Proxyserver-URL**: Geben Sie die URL des Proxyservers ein. Diese Angabe ist erforderlich.
- **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**, **Kennwort 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:

- **Verbindungsname**: Geben Sie einen Namen für die Verbindung ein.
- **Verbindungstyp**: Wählen Sie in der Liste das Protokoll aus, das für die Verbindung verwendet werden soll. Der Standardwert ist "L2TP".
  - **L2TP**: Layer-2-Tunnelingprotokoll mit Authentifizierung mit vorinstalliertem Schlüssel
  - **PPTP**: Point-to-Point Tunneling.
  - **IPSec**: Ihre Unternehmens-VPN-Verbindung
  - **Cisco AnyConnect**: Cisco AnyConnect VPN-Client
  - **Juniper SSL**: Juniper Networks SSL VPN-Client
  - **F5 SSL**: F5 Networks SSL VPN-Client

- **SonicWALL Mobile Connect**: einheitlicher Dell VPN-Client für iOS
- **Ariba VIA**: Ariba Networks Virtual Internet Access-Client
- **Citrix VPN**: Citrix VPN-Client
- **Benutzerdefiniertes SSL**: benutzerdefiniertes Secure Socket Layer

In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt.

Konfigurieren von L2TP

Konfigurieren von PPTP

Konfigurieren von IPSec

Konfigurieren von Cisco AnyConnect

Konfigurieren von Juniper SSL

Konfigurieren von F5 SSL

Konfigurieren von SonicWALL

Konfigurieren von Ariba VIA

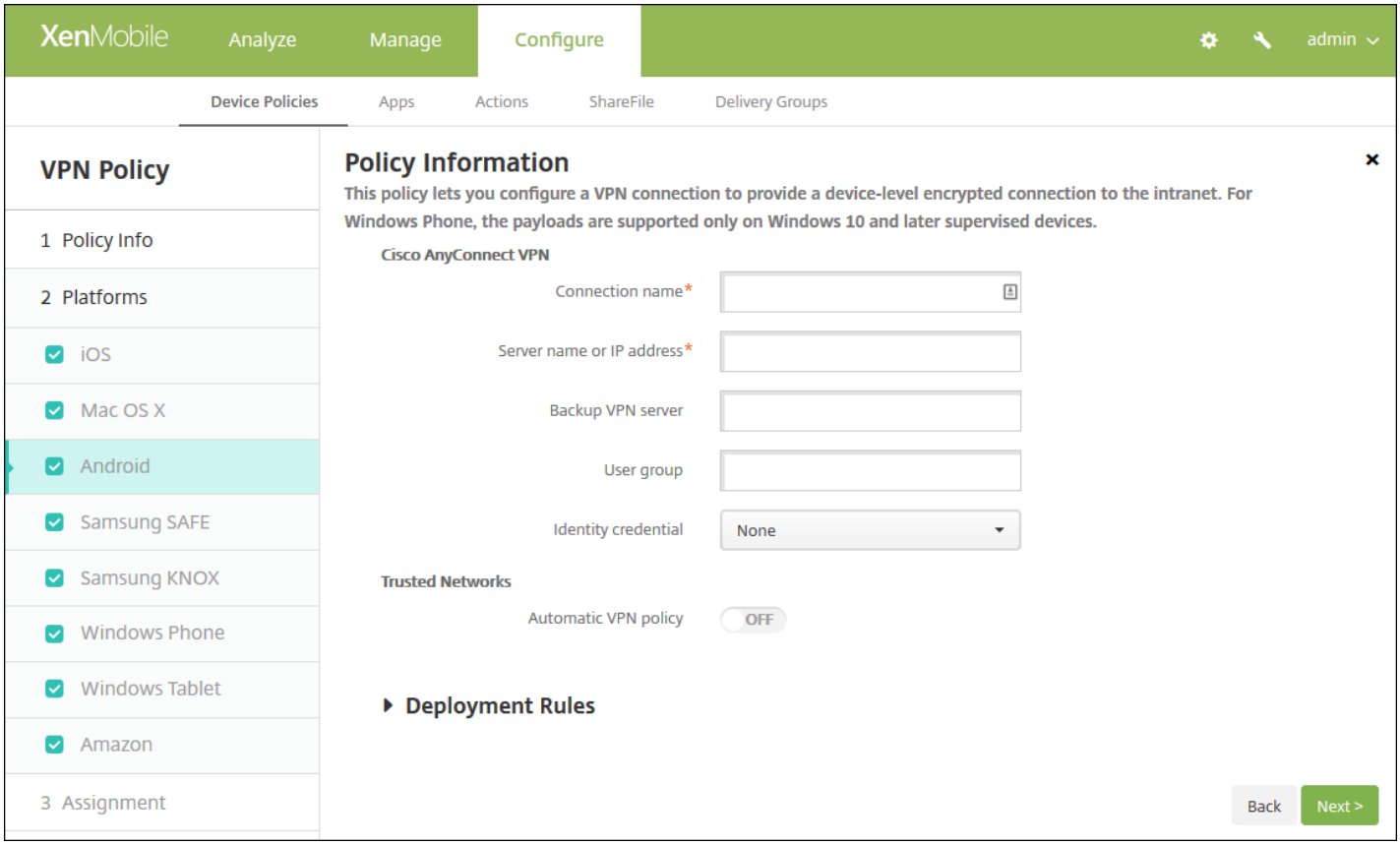
Konfigurieren von Citrix VPN-Protokoll

Konfigurieren des benutzerdefinierten SSL-Protokolls

Konfigurieren der Einstellungen für VPN bei Bedarf

- **Proxy**
  - **Proxykonfiguration**: Wählen Sie in der Liste nach Bedarf das Routing der VPN-Verbindung über einen Proxyserver aus. Der Standardwert ist **Ohne**.
    - 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 einen optionalen Benutzernamen für den Proxyserver ein.
      - **Kennwort**: Geben Sie ein optionales Kennwort für den Proxyserver ein.
    - Bei Auswahl von **Automatisch** konfigurieren Sie die folgende Einstellung:
      - **Proxyserver-URL**: Geben Sie die URL des Proxyservers ein. Diese Angabe ist erforderlich.
- **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.

Konfigurieren von Android-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Cisco AnyConnect VPN**
  - **Verbindungsname**: Geben Sie einen Namen für die Cisco AnyConnect VPN-Verbindung ein. Diese Angabe ist erforderlich.
  - **Servername oder IP-Adresse**: Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein. Diese Angabe ist erforderlich.
  - **Backup-VPN-Server**: Geben Sie die Informationen des sekundären VPN-Servers ein.
  - **Benutzergruppe**: Geben Sie die Informationen zur Benutzergruppe ein.
  - **Identitätsanmeldeinformationen**: Wählen Sie in der Liste Anmeldeinformationen aus.
- **Vertrauenswürdige Netzwerke**
  - **Richtlinie für automatisches VPN**: Aktivieren oder deaktivieren Sie diese Option, um festzulegen, wie das VPN auf vertrauenswürdige und nicht vertrauenswürdige Netzwerke reagiert. Wenn Sie diese Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
    - **Richtlinie für vertrauenswürdiges Netzwerk**: Klicken Sie in der Liste auf die gewünschte Richtlinie. Der Standardwert ist **Trennen**. Mögliche Optionen:
      - **Trennen**: Der Client trennt die VPN-Verbindung im vertrauenswürdigen Netzwerk. Dies ist die Standardeinstellung.
      - **Verbinden**: Der Client initiiert die VPN-Verbindung im vertrauenswürdigen Netzwerk.
      - **Nichts tun**: Der Client unternimmt keine Aktion.
      - **Anhalten**: Setzt die VPN-Sitzung aus (anstatt sie zu trennen), wenn ein Benutzer nach dem Herstellen einer VPN-Sitzung außerhalb eines vertrauenswürdigen Netzwerks ein als vertrauenswürdig konfiguriertes Netzwerk

betritt. Verlässt der Benutzer das vertrauenswürdige Netzwerk wieder, wird die Sitzung fortgesetzt. Auf diese Weise muss beim Verlassen eines vertrauenswürdigen Netzwerks keine neue VPN-Sitzung erstellt werden.

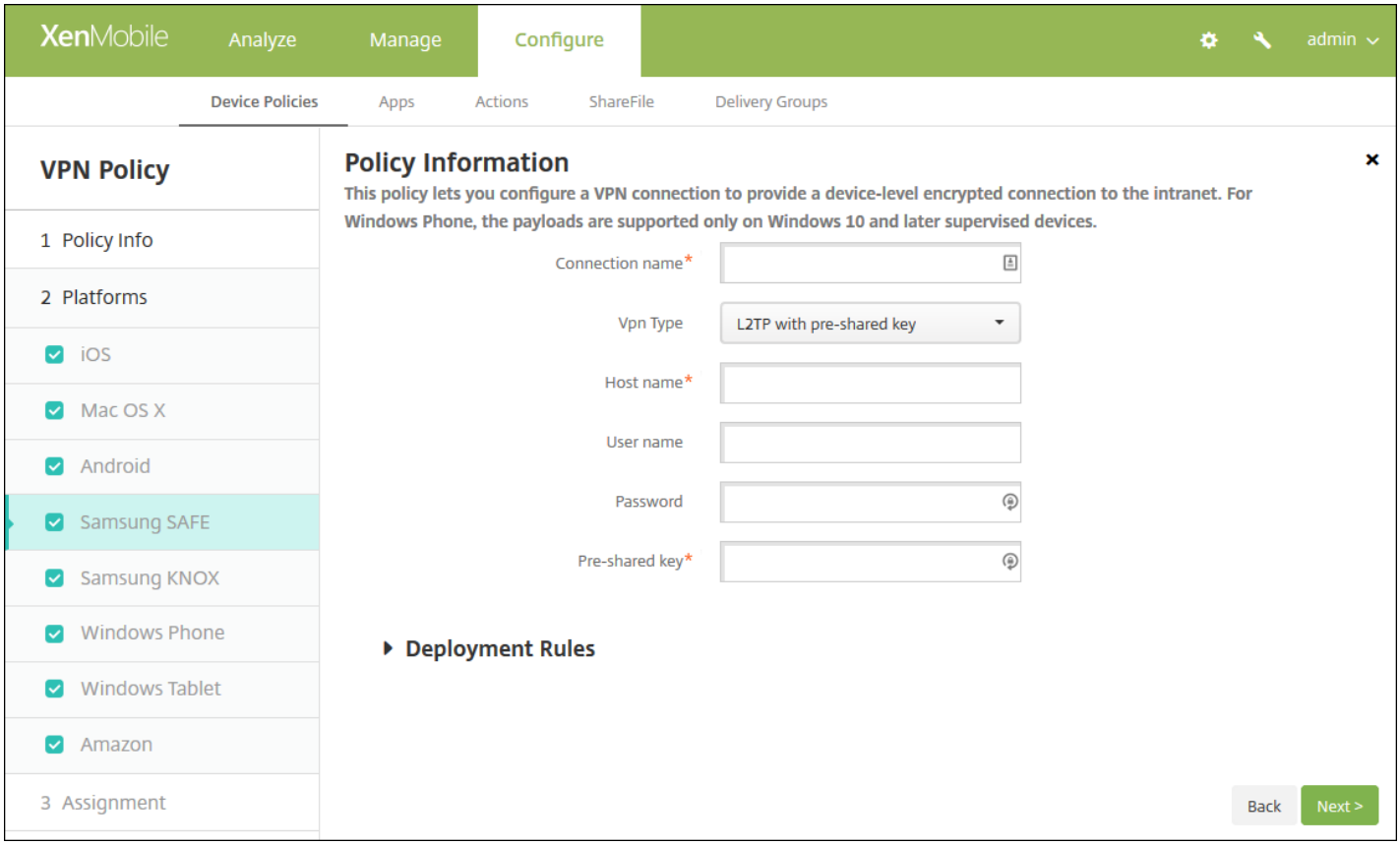
- **Richtlinie für nicht vertrauenswürdiges Netzwerk**: Klicken Sie in der Liste auf die gewünschte Richtlinie. Der Standardwert ist **Verbinden**. Mögliche Optionen:
  - **Verbinden**: Der Client initiiert die VPN-Verbindung im nicht vertrauenswürdigen Netzwerk.
  - **Nichts tun**: Der Client initiiert die VPN-Verbindung im nicht vertrauenswürdigen Netzwerk. Mit dieser Option wird Always-On-VPN deaktiviert.

- **Vertrauenswürdige Domänen**: Klicken Sie für jedes Domänensuffix, das die Netzwerkschnittstelle haben darf, wenn der Client sich im vertrauenswürdigen Netzwerk befindet, auf **Hinzufügen**, und führen Sie die folgenden Schritte aus:
  - **Domäne**: Geben Sie den Namen der gewünschten Domäne ein.
  - Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Vertrauenswürdige Server**: Klicken Sie für jede Serveradresse, die die Netzwerkschnittstelle haben darf, wenn der Client sich im vertrauenswürdigen Netzwerk befindet, auf **Hinzufügen**, und führen Sie die folgenden Schritte aus:
  - **Server**: Geben Sie den Namen des gewünschten Servers ein.
  - Klicken Sie auf **Speichern**, um den Server zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

    Hinweis: Zum Löschen eines vorhandenen Servers 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 Servers 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 der Samsung SAFE-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Verbindungsname**: Geben Sie einen Namen für die Verbindung ein.
- **VPN-Typ**: Wählen Sie in der Liste das Protokoll aus, das für die Verbindung verwendet werden soll. Der Standardwert ist **L2TP mit vorinstalliertem Schlüssel**. Mögliche Optionen:
  - **L2TP mit vorinstalliertem Schlüssel**: Layer-2-Tunnelingprotokoll mit Authentifizierung mit vorinstalliertem Schlüssel Dies ist die Standardeinstellung.
  - **L2TP mit Zertifikat**: Layer-2-Tunnelingprotokoll mit Zertifikat
  - **PPTP**: Point-to-Point Tunneling
  - **Unternehmen**: Ihre Unternehmens-VPN-Verbindung Gilt für SAFE-Versionen vor 2.0.
  - **Generisch**: generische VPN-Verbindung Gilt für SAFE-Versionen ab 2.0.

In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen VPN-Typen aufgeführt.

Konfigurieren von L2TP mit vorinstalliertem Schlüssel

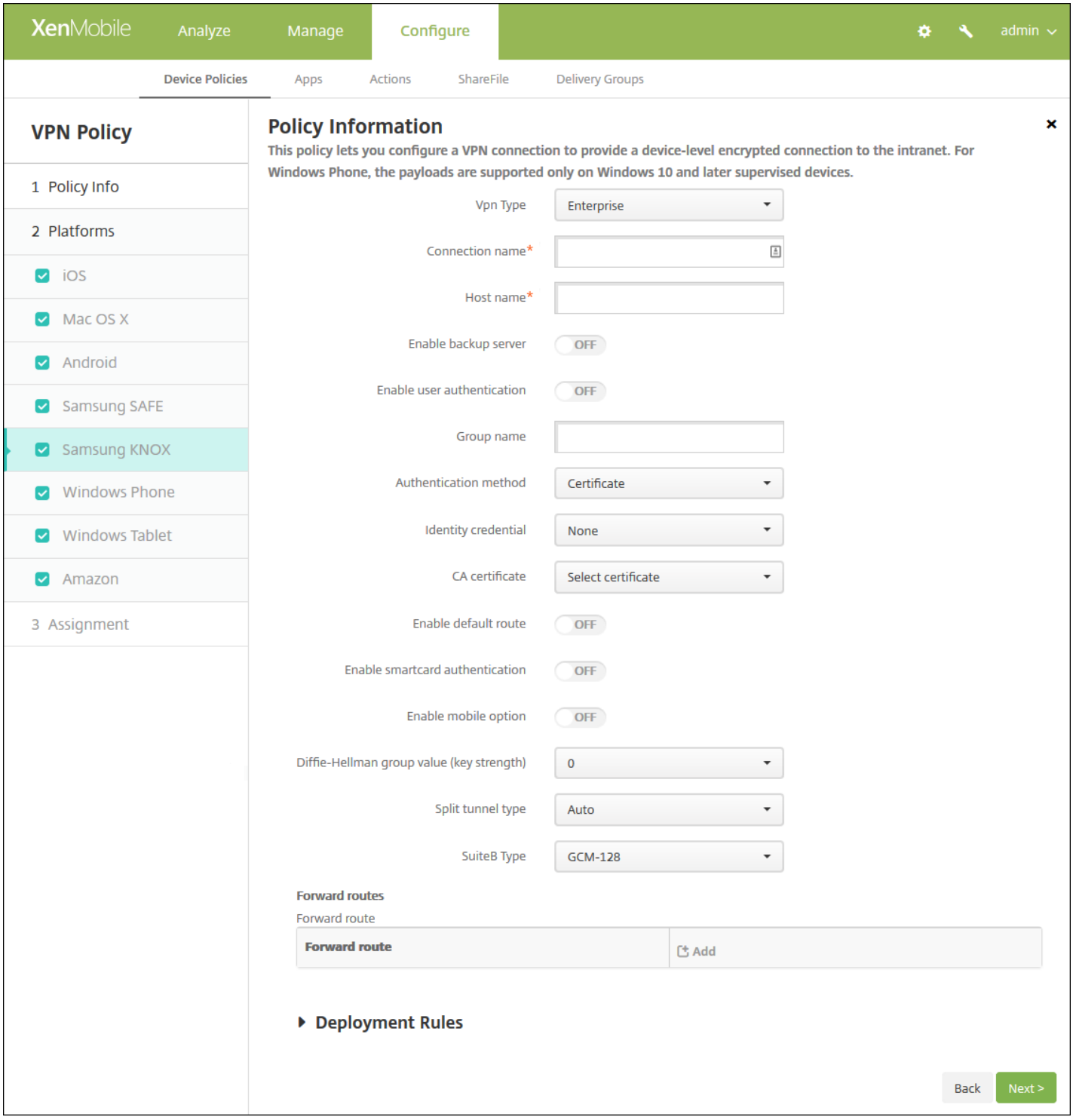
Konfigurieren von L2TP mit Zertifikat

Konfigurieren von PPTP

Konfigurieren des Enterprise-Protokolls

Konfigurieren des generischen Protokolls

Konfigurieren der Samsung KNOX-Einstellungen



Hinweis: Alle Samsung KNOX-Richtlinien gelten ausschließlich innerhalb des Samsung KNOX-Containers.

Konfigurieren Sie folgende Einstellungen:

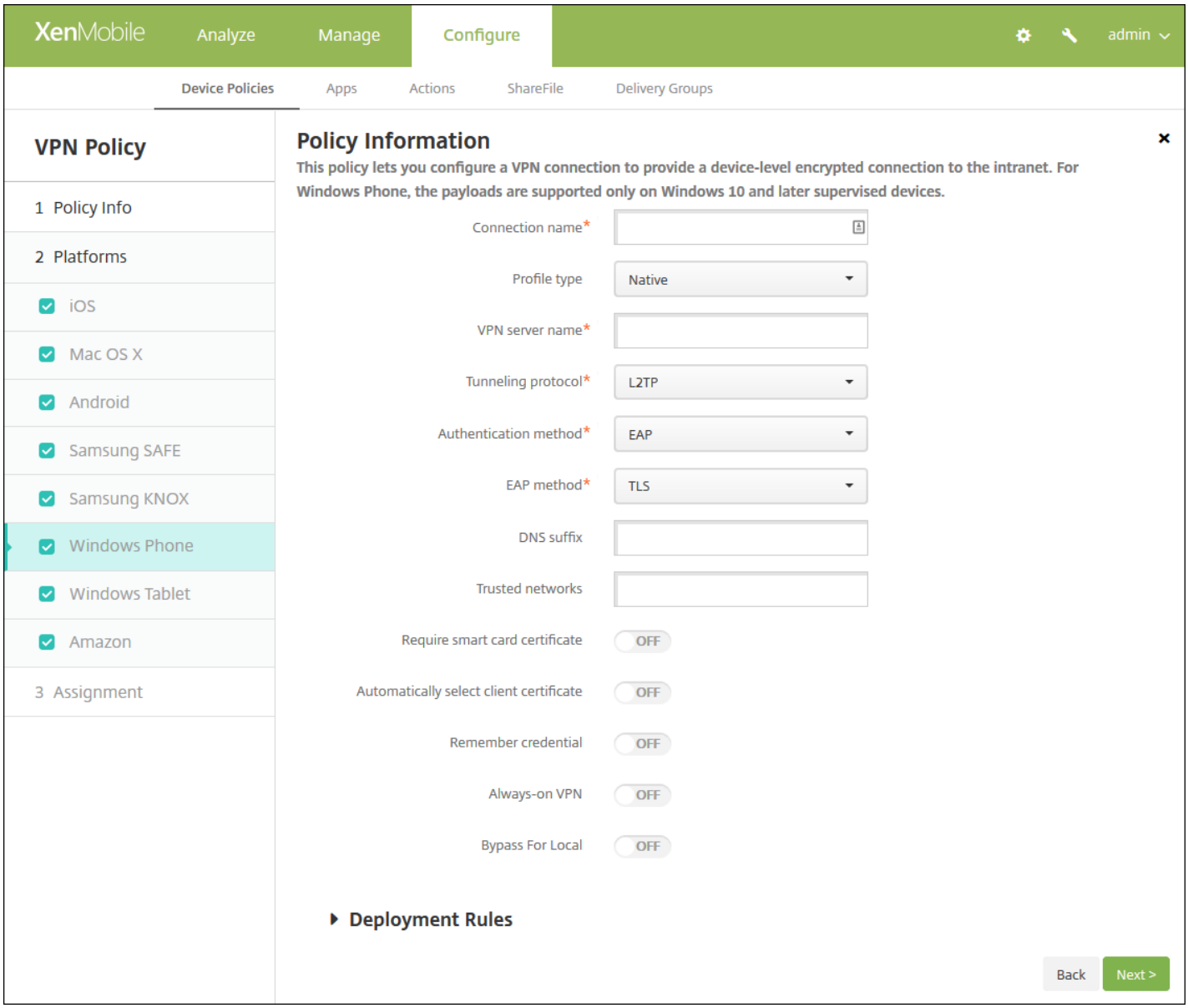
- **VPN-Typ**: Klicken Sie in der Liste auf den Typ der VPN-Verbindung. Zur Auswahl stehen **Enterprise** (für KNOX-Versionen vor 2.0) und **Generisch** (für KNOX-Versionen ab 2.0). Der Standardwert ist **Unternehmen**.

In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt.

Konfigurieren des Enterprise-Protokolls

Konfigurieren des generischen Protokolls

Konfigurieren von Windows Phone-Einstellungen



Hinweis: Die Einstellungen werden nur für betreute Geräte unter Windows 10 und höher unterstützt.

Konfigurieren Sie folgende Einstellungen:

- **Verbindungsname**: Geben Sie einen Namen für die Verbindung ein. Diese Angabe ist erforderlich.
- **Profiltyp**: Klicken Sie in der Liste auf **Nativ** oder **Plug-In**. Der Standardwert ist **Nativ**. In den folgenden Abschnitten werden die Einstellungen der Optionen erläutert.
- **Einstellungen für Profiltyp "Nativ"**: Diese Einstellungen gelten für in Windows Phone-Geräte integrierte VPNs.
  - **VPN-Servername**: Geben Sie den FQDN oder die IP-Adresse des VPN-Servers ein. Diese Angabe ist erforderlich.
  - **Tunnelingprotokoll**: Klicken Sie in der Liste auf den gewünschten VPN-Tunneltyp. Die Standardeinstellung ist **L2TP**.

Mögliche Optionen:

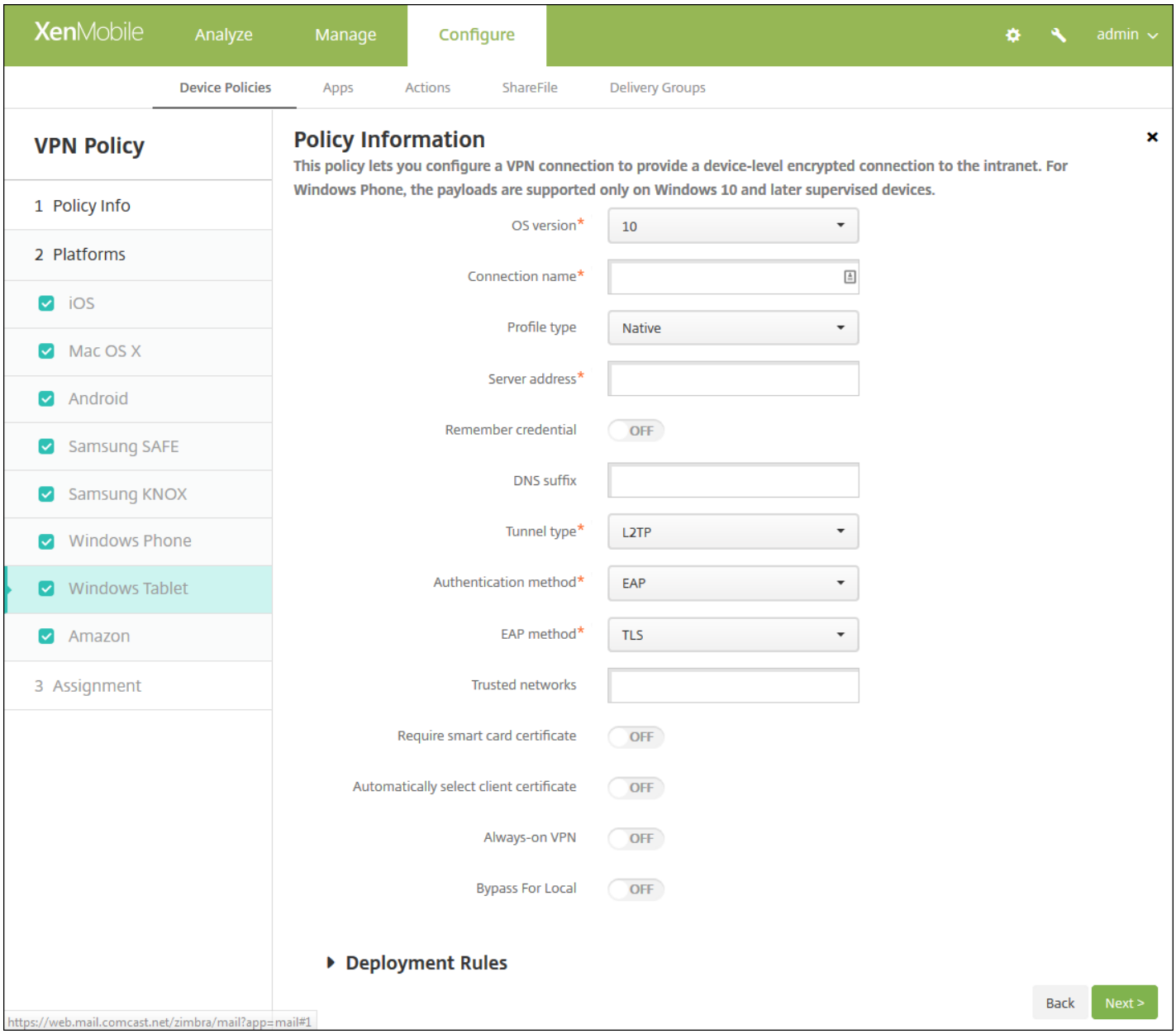
- **L2TP**: Layer-2-Tunnelingprotokoll mit Authentifizierung mit vorinstalliertem Schlüssel
- **PPTP**: Point-to-Point Tunneling.
- **IKEv2**: Internet Key Exchange Version 2

- **Authentifizierungsmethode**: Klicken Sie in der Liste auf die gewünschte Authentifizierungsmethode. Die Standardeinstellung ist **EAP**. Mögliche Optionen:
  - **EAP**: Protokoll der erweiterten Authentifizierung
  - **MSChapV2**: Challenge Handshake Authentication von Microsoft für die gegenseitige Authentifizierung. Diese Option ist nicht verfügbar, wenn Sie "IKEv2" als Tunnel auswählen. Bei Auswahl von MSChapV2 wird die Option **Automatisch Windows-Anmeldeinformationen verwenden** angezeigt. Der Standardwert ist **AUS**.
- **EAP-Methode**: Klicken Sie in der Liste auf die gewünschte EAP-Methode. Der Standardwert ist **TLS**. Dieses Feld ist nicht verfügbar, wenn Sie MSChapV2 aktiviert haben. Mögliche Optionen:
  - **TLS**: Transport Layer Security
  - **PEAP**: Protected Extensible Authentication Protocol
- **DNS Suffix**: Gebe Sie das DNS-Suffix ein.
- **Vertrauenswürdige Netzwerke**: Geben Sie die Netzwerke durch Kommas getrennt ein, für die keine VPN-Verbindung erforderlich ist. Benutzer im Drahtlosnetzwerk des Unternehmens haben beispielsweise direkten Zugriff auf geschützte Ressourcen.
- **Smartcardzertifikat erforderlich**: Wählen Sie aus, ob ein Smartcardzertifikat erforderlich sein soll. Der Standardwert ist AUS.
- **Automatisch Clientzertifikat auswählen**: Wählen Sie aus, ob das Clientzertifikat für die Authentifizierung automatisch gewählt werden soll. Der Standardwert ist AUS. Diese Option ist nicht verfügbar, wenn "Smartcardzertifikat erforderlich" aktiviert ist.
- **Anmeldeinformationen speichern**: Wählen Sie aus, ob die Anmeldeinformationen im Cache gespeichert werden sollen. Der Standardwert ist AUS. Wenn diese Option aktiviert ist, werden die Anmeldeinformationen, sofern möglich, gespeichert.
- **Always-on VPN**: Wählen Sie aus, ob die VPN-Verbindung immer aktiv sein soll. Der Standardwert ist AUS. Wenn diese Option aktiviert ist, bleibt die VPN-Verbindung bestehen, bis der Benutzer sie manuell trennt.
- **Bei lokalen Adressen umgehen**: Geben Sie die Adresse und die Portnummer ein, damit lokale Ressourcen den Proxyserver umgehen können.

- **Konfigurieren des Plug-In-Protokolls:** Die nachfolgenden Einstellungen gelten für VPN-Plug-Ins aus dem Windows-Store, die auf Geräten installiert sind.
  - **Servername oder IP-Adresse**: Geben Sie die URL, den Hostnamen oder die IP-Adresse des VPN-Servers ein.
  - **Client-App-ID**: Geben Sie den Paketfamiliennamen des VPN-Plug-Ins ein.
  - **XML für Plug-In-Profil**: Klicken Sie auf "Durchsuchen", navigieren Sie zum Speicherort der Datei des gewünschten benutzerdefinierten VPN-Plug-In-Profils und wählen Sie diese aus. Informationen zu Format und anderen Details erhalten Sie bei dem Anbieter des Plug-Ins.
  - **DNS Suffix**: Gebe Sie das DNS-Suffix ein.
  - **Vertrauenswürdige Netzwerke**: Geben Sie die Netzwerke durch Kommas getrennt ein, für die keine VPN-Verbindung erforderlich ist. Benutzer im Drahtlosnetzwerk des Unternehmens haben beispielsweise direkten Zugriff auf geschützte Ressourcen.
  - **Anmeldeinformationen speichern**: Wählen Sie aus, ob die Anmeldeinformationen im Cache gespeichert werden sollen. Der Standardwert ist AUS. Wenn diese Option aktiviert ist, werden die Anmeldeinformationen, sofern möglich, gespeichert.
  - **Always-on VPN**: Wählen Sie aus, ob die VPN-Verbindung immer aktiv sein soll. Der Standardwert ist AUS. Wenn diese Option aktiviert ist, bleibt die VPN-Verbindung bestehen, bis der Benutzer sie manuell trennt.

- **Bei lokalen Adressen umgehen**: Geben Sie die Adresse und die Portnummer ein, damit lokale Ressourcen den Proxyserver umgehen können.

Konfigurieren von Windows Tablet-Einstellungen



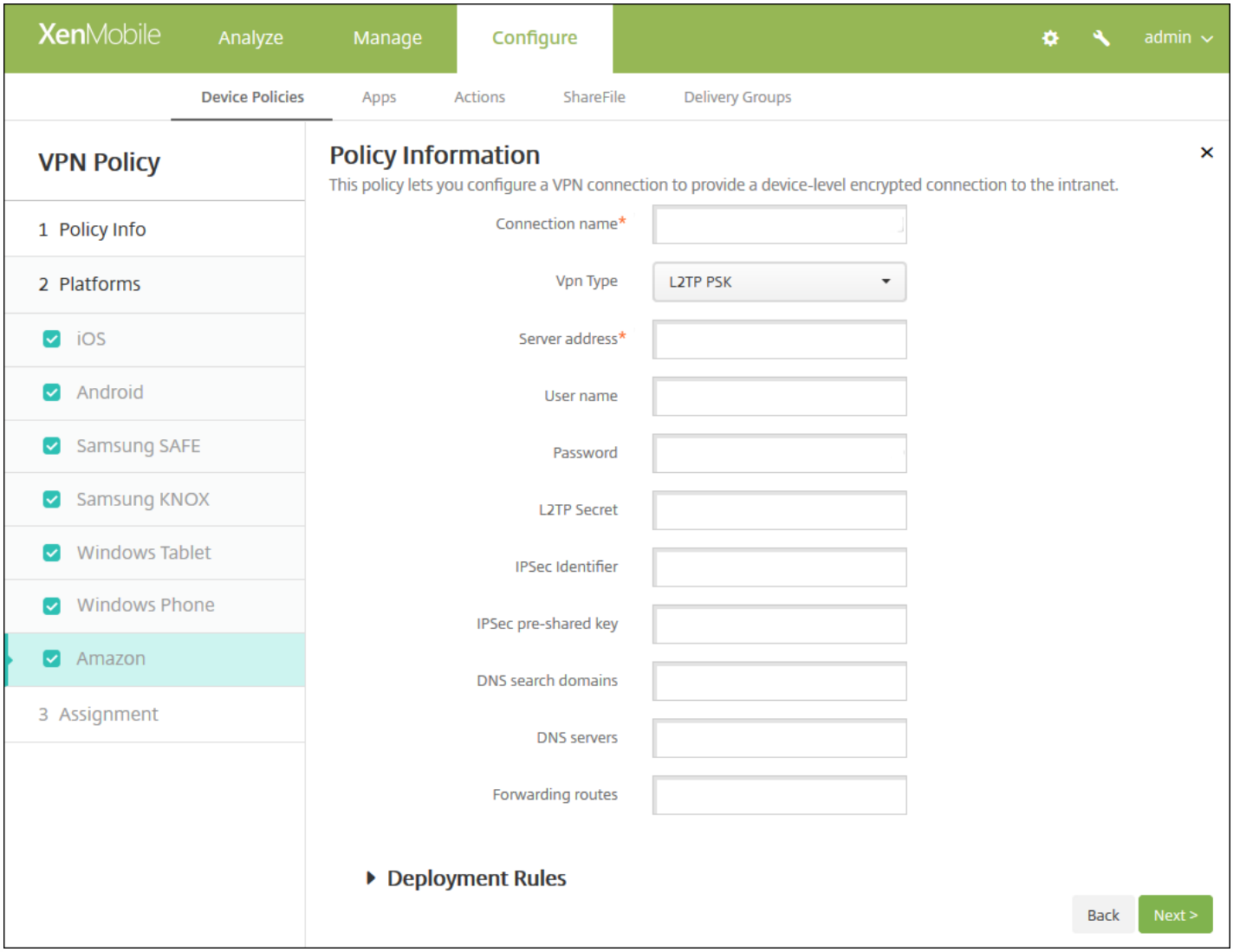
Konfigurieren Sie folgende Einstellungen:

- **OS-Version**: Klicken Sie in der Liste auf **8.1** für Windows 8.1 oder auf **10** für Windows 10. Der Standardwert ist **10**.

Konfigurieren von Windows 10-Einstellungen

Konfigurieren von Windows 8.1-Einstellungen

Konfigurieren von Amazon-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Verbindungsname**: Geben Sie einen Namen für die Verbindung ein.
- **Verbindungstyp**: Klicken Sie auf den Verbindungstyp. Mögliche Optionen:
  - **L2TP PSK**: Layer-2-Tunnelingprotokoll mit Authentifizierung mit vorinstalliertem Schlüssel. Dies ist die Standardeinstellung.
  - **L2TP RSA** : Layer-2-Tunnelingprotokoll mit RSA-Authentifizierung.
  - **IPSEC XAUTH PSK**: Internet Protocol Security mit vorinstalliertem Schlüssel und erweiterter Authentifizierung.
  - **IPSEC HYBRID RSA**: Internet Protocol Security mit Hybrid-RSA-Authentifizierung.
  - **PPTP**: Point-to-Point Tunneling.

In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt.

Konfigurieren der L2TP PSK-Einstellungen

Konfigurieren der L2TP RSA-Einstellungen

Konfigurieren der IPSEC XAUTH PSK-Einstellungen

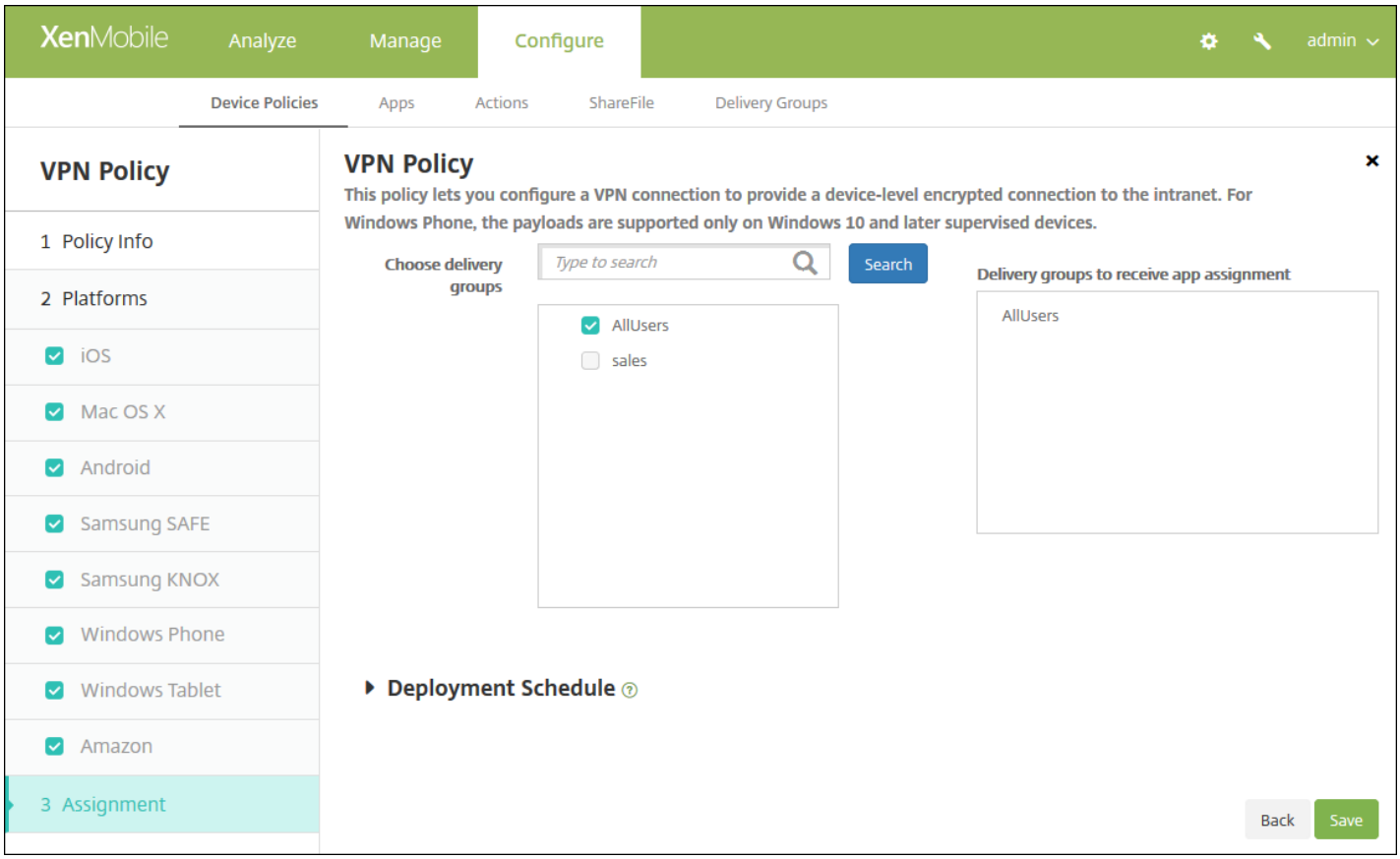
Konfigurieren der IPSEC AUTH RSA-Einstellungen

Konfigurieren der IPSEC HYBRID RSA-Einstellungen

Konfigurieren der PPTP-Einstellungen

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die VPN-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 **Später** 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**. Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Hintergrundbild-Geräterichtlinie

Feb 24, 2017

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.

In der folgenden Tabelle werden die von Apple empfohlenen Bildgrößen für iOS-Geräte aufgeführt.

Gerät		**Bildgröße in Pixeln**
iPhone	**iPad**	
4, 4s		640 x 960
5, 5c, 5s		640 x 1136
6, 6s		750 x 1334
6 Plus		1080 x 1920
	Air, 2	1536 x 2048
	4, 3	1536 x 2048
	Mini 2, 3	1536 x 2048
	Mini	768 x 1024

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

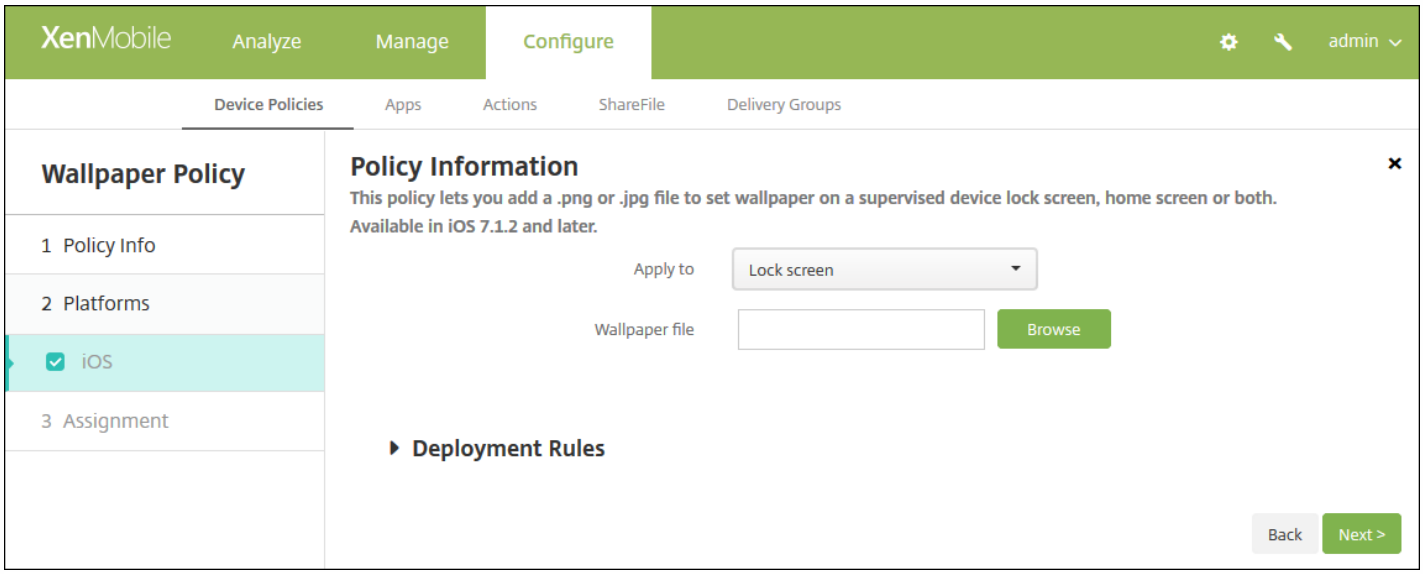
2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie unter **Endbenutzer** auf **Hintergrundbild**. Die Seite **Hintergrundbild** 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.

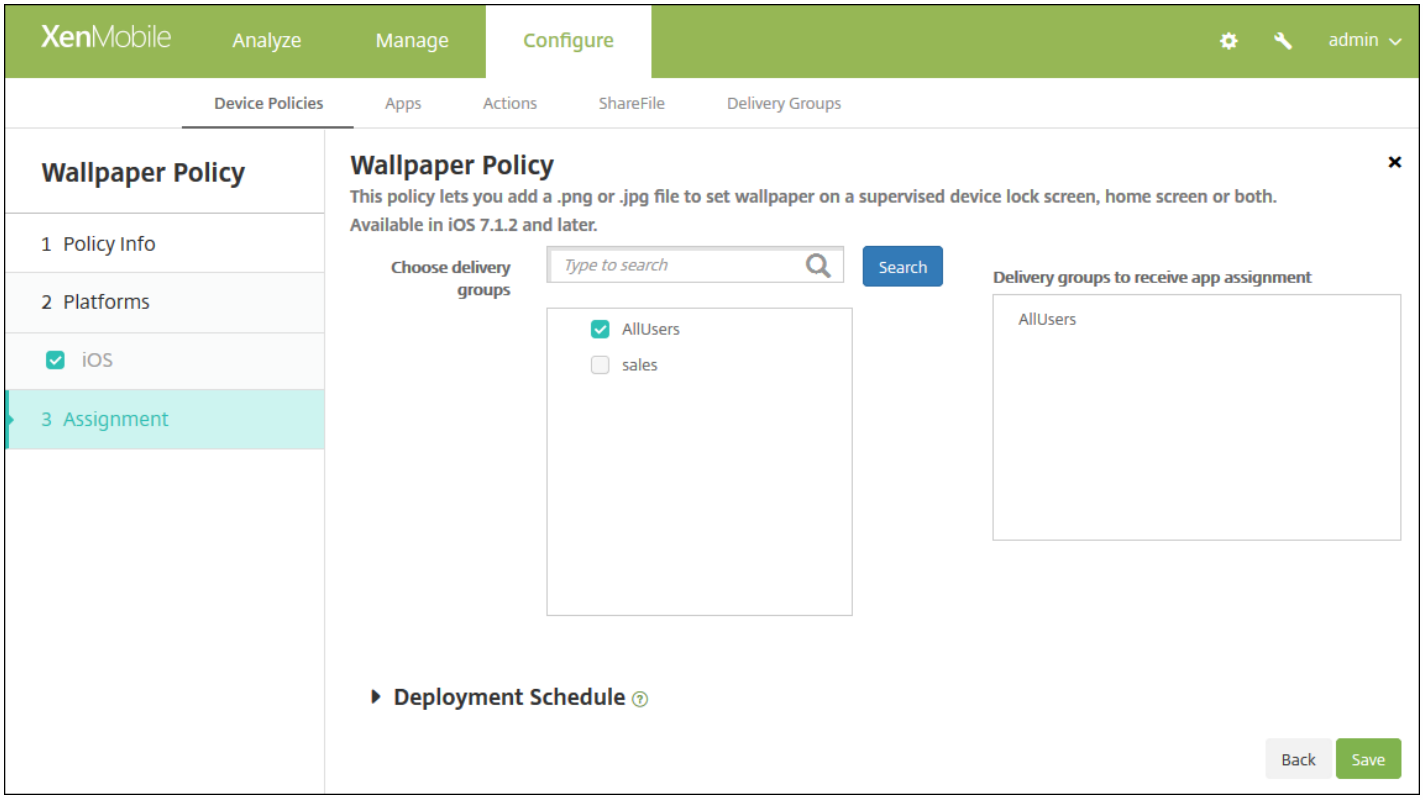


Konfigurieren Sie folgende Einstellungen:

- **Anwenden auf**: Wählen Sie in der Liste **Sperrbildschirm**, **Homebildschirm (Symbolliste)** oder **Sperr- und Homebildschirm** aus, um festzulegen, wo das Hintergrundbild angezeigt werden soll.
- **Hintergrundbilddatei**: Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der Hintergrundbilddatei, um diese auszuwählen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Hintergrundbildrichtlinie 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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie für Webinhalt

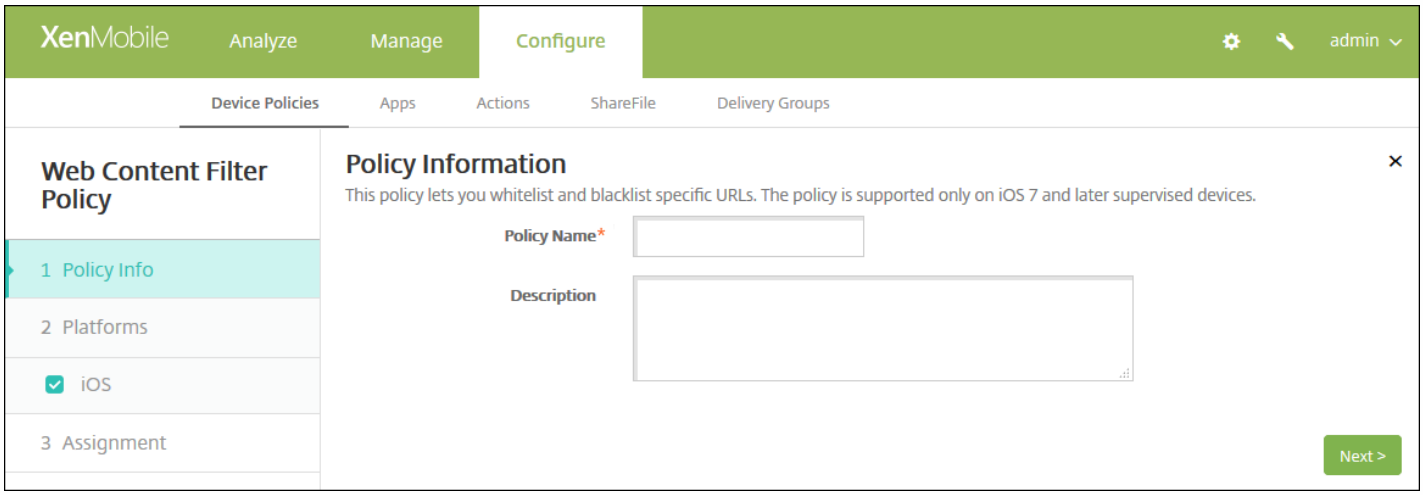
Feb 24, 2017

Sie können in XenMobile eine Geräterichtlinie zum Filtern von Webinhalt auf iOS-Geräten mit der automatischen Filterfunktion von Apple in Verbindung mit Ihren Website-Positivlisten und -Sperrlisten hinzufügen. Diese Richtlinie gilt nur für iOS 7.0 und höher im betreuten Modus. Informationen, wie Sie Geräte in den betreuten Modus versetzen finden Sie unter 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.

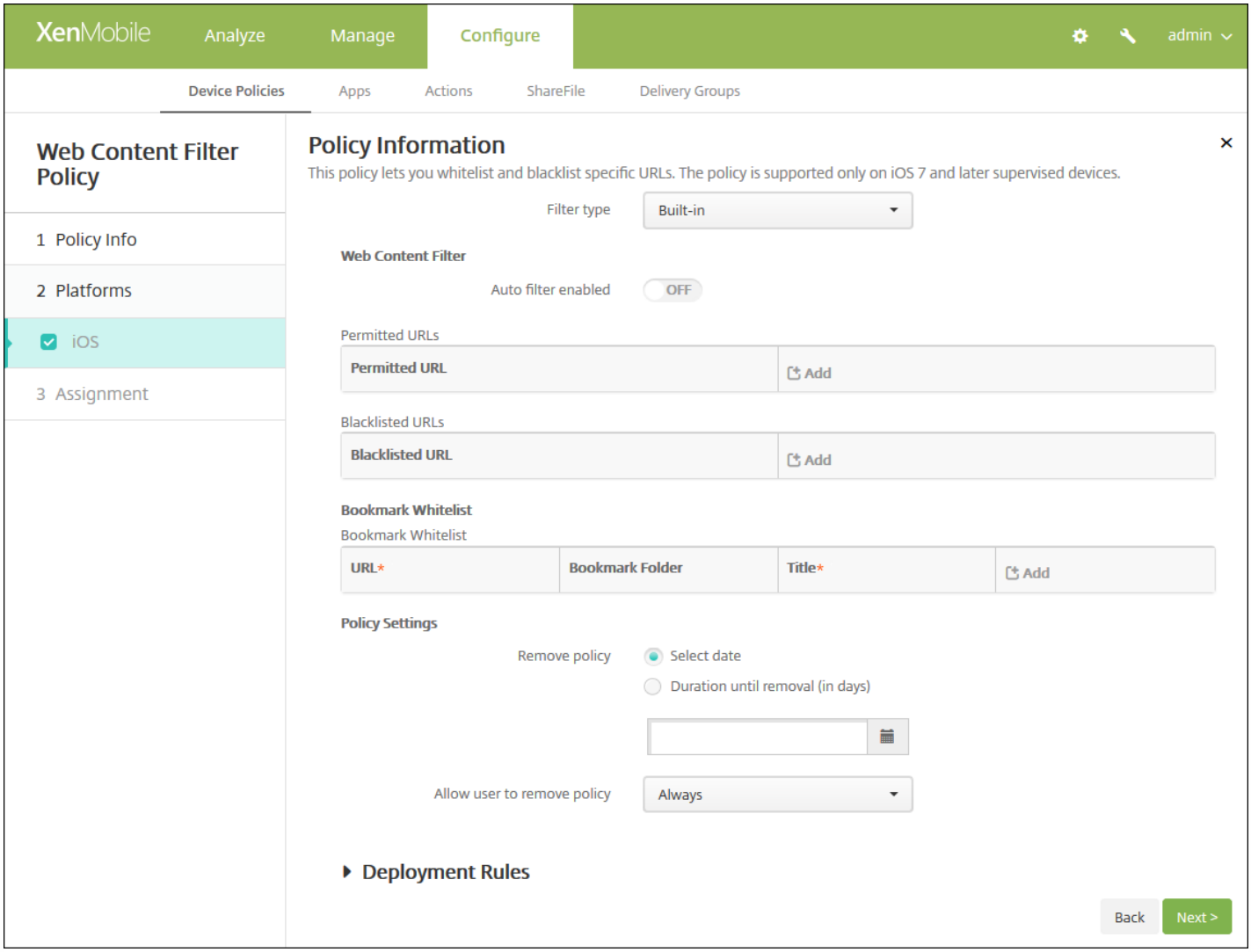
3. Klicken Sie auf **Mehr** und dann unter **Sicherheit** auf **Webinhaltsfilter**. Die Seite **Webinhaltsfilter** wird angezeigt.



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 für die iOS-Plattform wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

- **Filtertyp**: Klicken Sie in der Liste auf eine **Integriert** oder **Plug-In** und führen Sie der Auswahl entsprechenden Schritte durch. Der Standardwert ist **Integriert**.

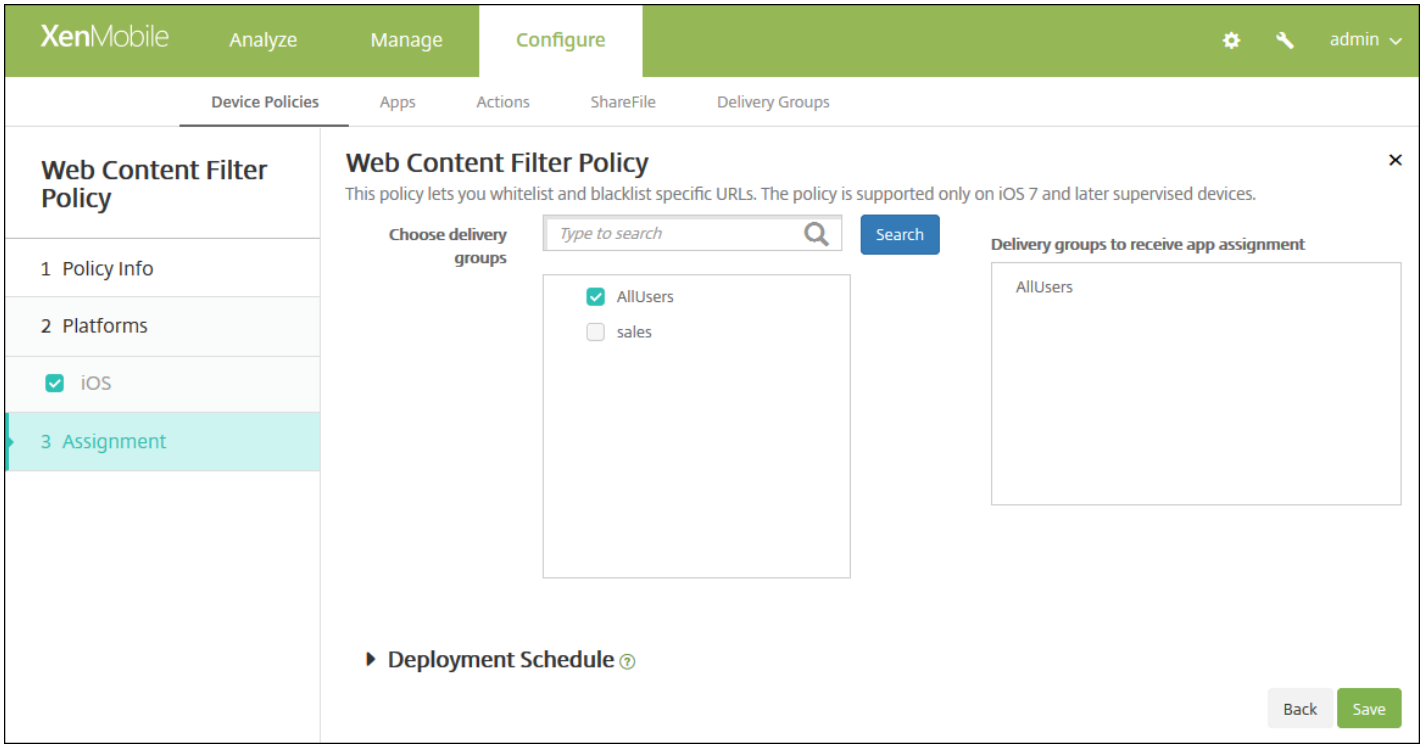
Einstellungen für integrierte Filter

Einstellungen für Plug-In-Filter

- **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.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Webinhaltsfilterrichtlinie 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Webclip-Geräterichtlinien

Feb 24, 2017

Sie können Verknüpfungen, bzw. Webclips, für 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 sind nur eine Beschriftung und eine URL erforderlich.

iOS-Einstellungen

Mac OS X-Einstellungen

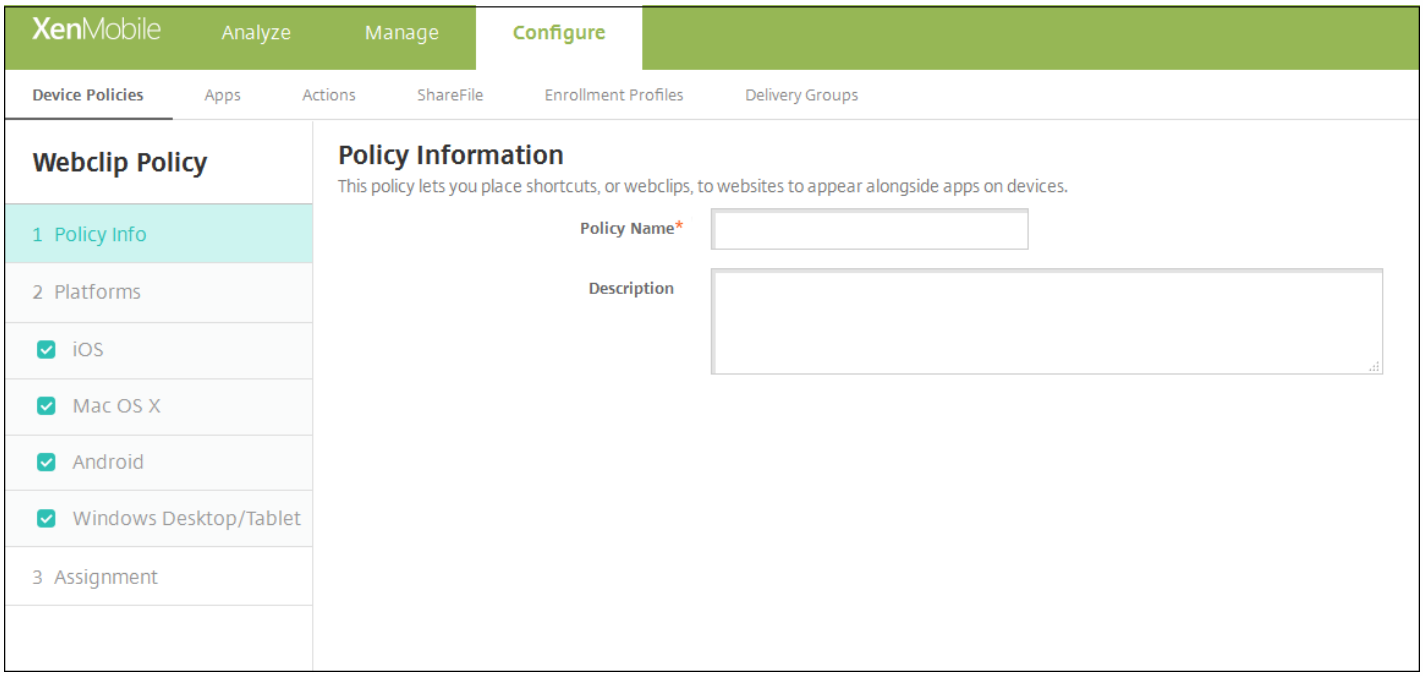
Android-Einstellungen

Windows Desktop/Tablet-Einstellungen

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Webclip**. Die Seite **Webclip** wird angezeigt.



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

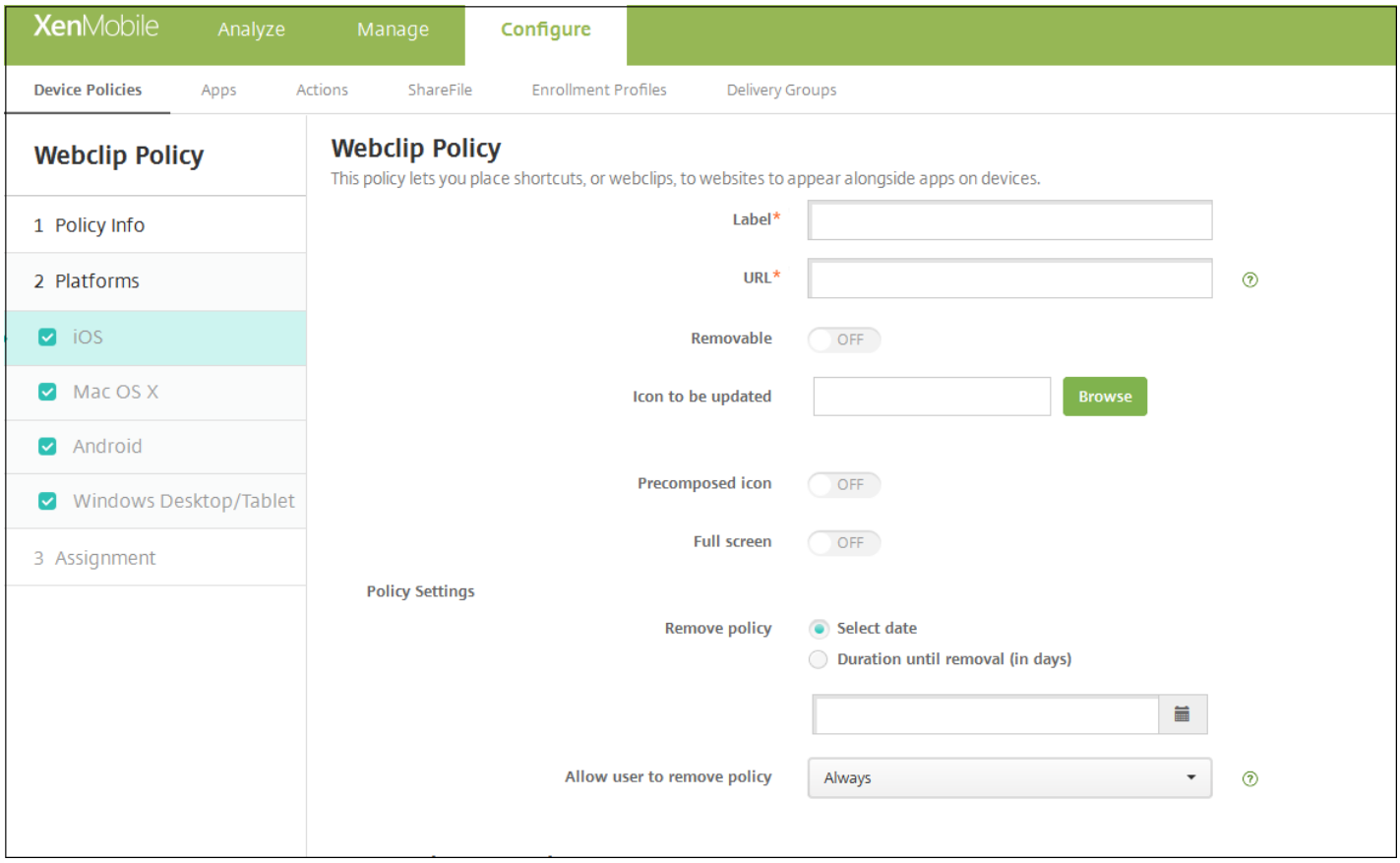
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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.

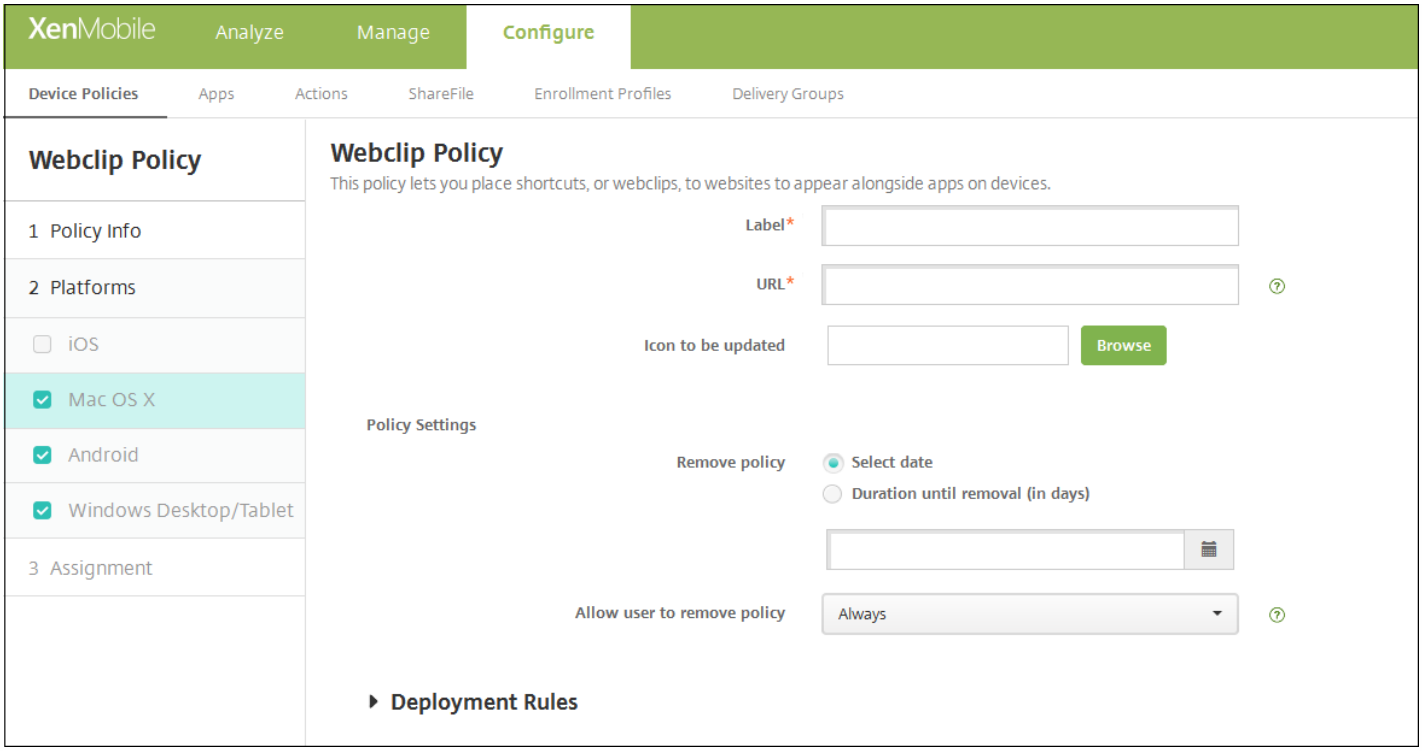
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Beschriftung**: Geben Sie die Beschriftung für den Webclip ein.
- **URL**: Geben Sie die URL des Webclips ein. Die URL muss mit einem Protokoll beginnen, z. B. "http://server".
- **Entfernbar**: Wählen Sie aus, ob Benutzer den Webclip entfernen können sollen. Der Standardwert ist **AUS**.
- **Zu aktualisierendes Symbol**: Klicken Sie zur Auswahl des zu aktualisierenden Symbols auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.
- **Vorverfasstes Symbol**: Wählen Sie nach Bedarf Effekte (runde Ecken, Schlagschatten, Widerschein) für das Symbol aus. Die Standardeinstellung ist **Aus**, d. h. die Effekte werden angewendet.
- **Vollbild**: Wählen Sie aus, ob die verknüpfte Webseite im Vollbildmodus geöffnet werden 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**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

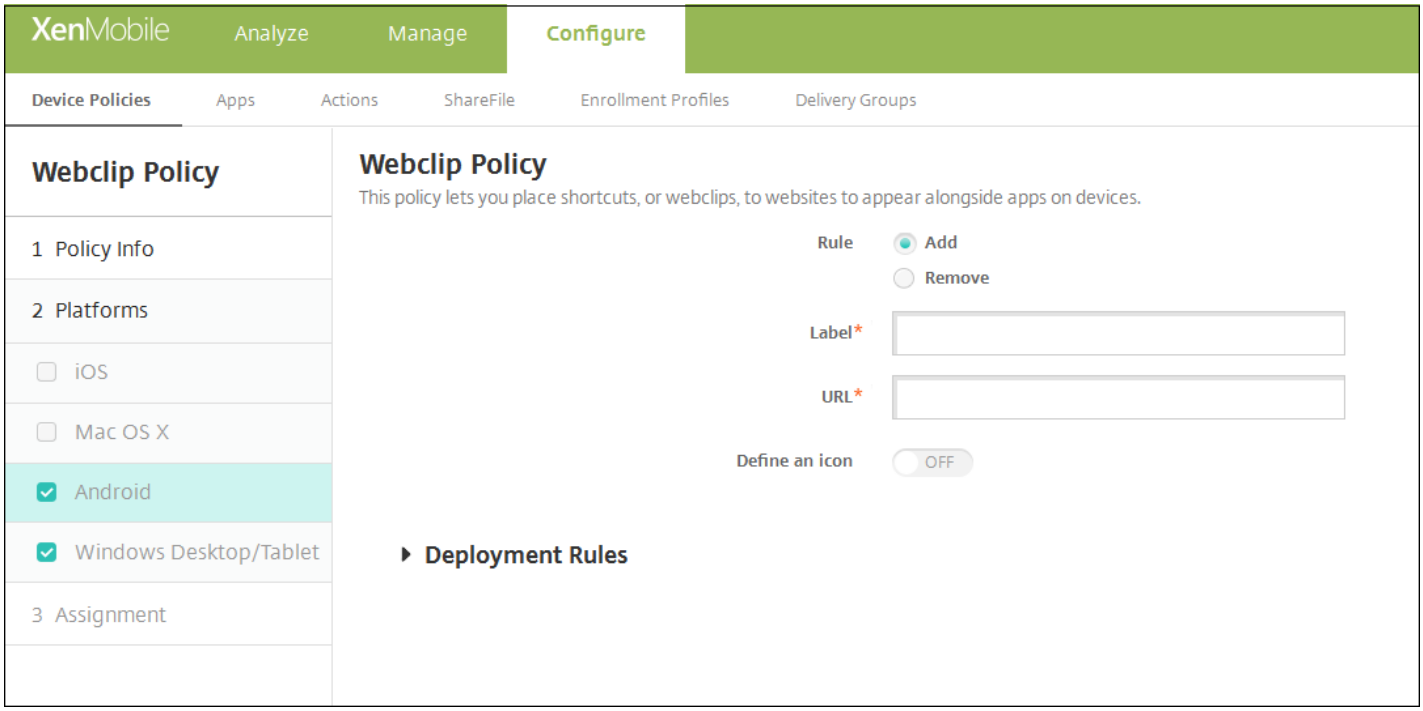
Konfigurieren von Mac OS X-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Beschriftung**: Geben Sie die Beschriftung für den Webclip ein.
- **URL**: Geben Sie die URL des Webclips ein. Die URL muss mit einem Protokoll beginnen, z. B. "http://server".
- **Zu aktualisierendes Symbol**: Klicken Sie zur Auswahl des zu aktualisierenden Symbols auf "Durchsuchen" und navigieren Sie zum Speicherort der Datei.
- **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 in der Liste **Gültigkeitsbereich für Profil** auf **Benutzer**oder **System**. Diese Option ist für OS X 10.7 und höher verfügbar.

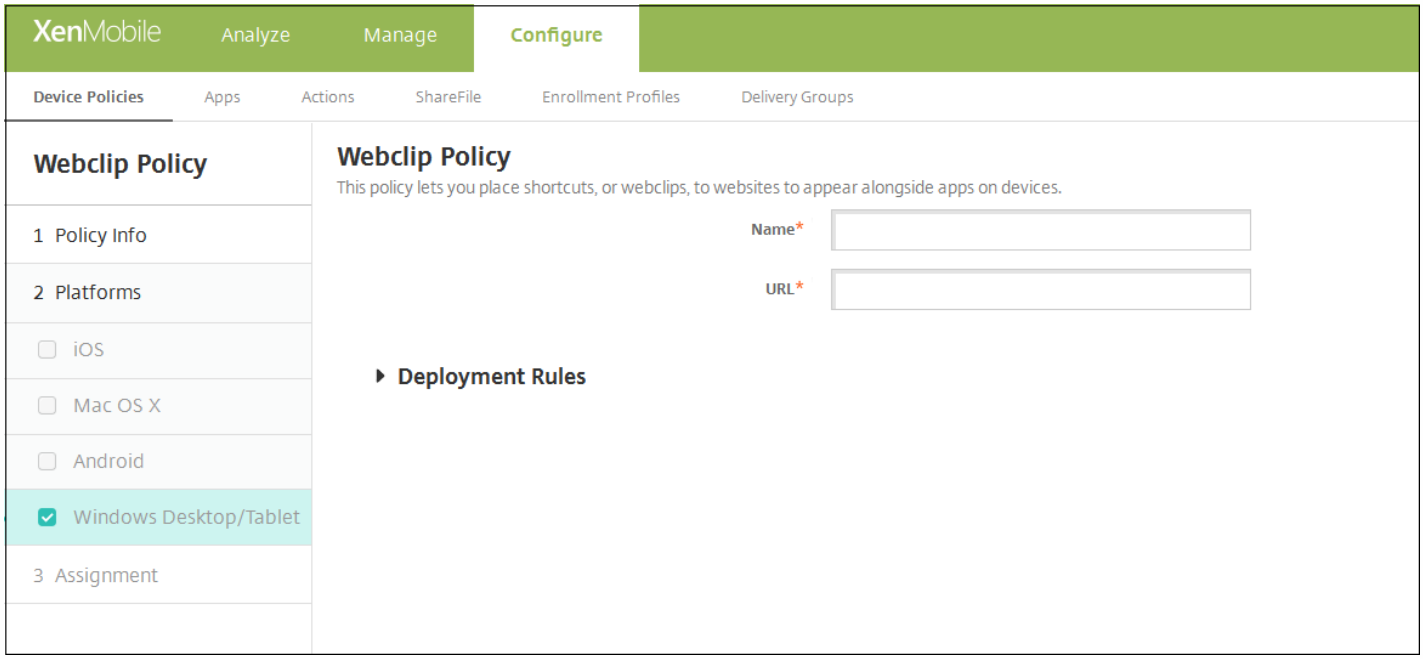
Konfigurieren von Android-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Regel**: Wählen Sie aus, ob durch die Richtlinie ein Webclip hinzugefügt oder entfernt werden soll. Der Standardwert ist **Hinzufügen**.
- **Beschriftung**: Geben Sie die Beschriftung für den Webclip ein.
- **URL**: Geben Sie die URL des Webclips ein.
- **Symbol definieren**: Wählen Sie aus, ob eine Symboldatei verwendet werden soll. Der Standardwert ist **AUS**.
- **Symboldatei**: Wenn Sie für **Symbol definieren** die Einstellung **Ein** festgelegt haben, klicken Sie zum Auswählen der Symboldatei auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.

Konfigurieren von Windows Desktop-/Tablet-Einstellungen

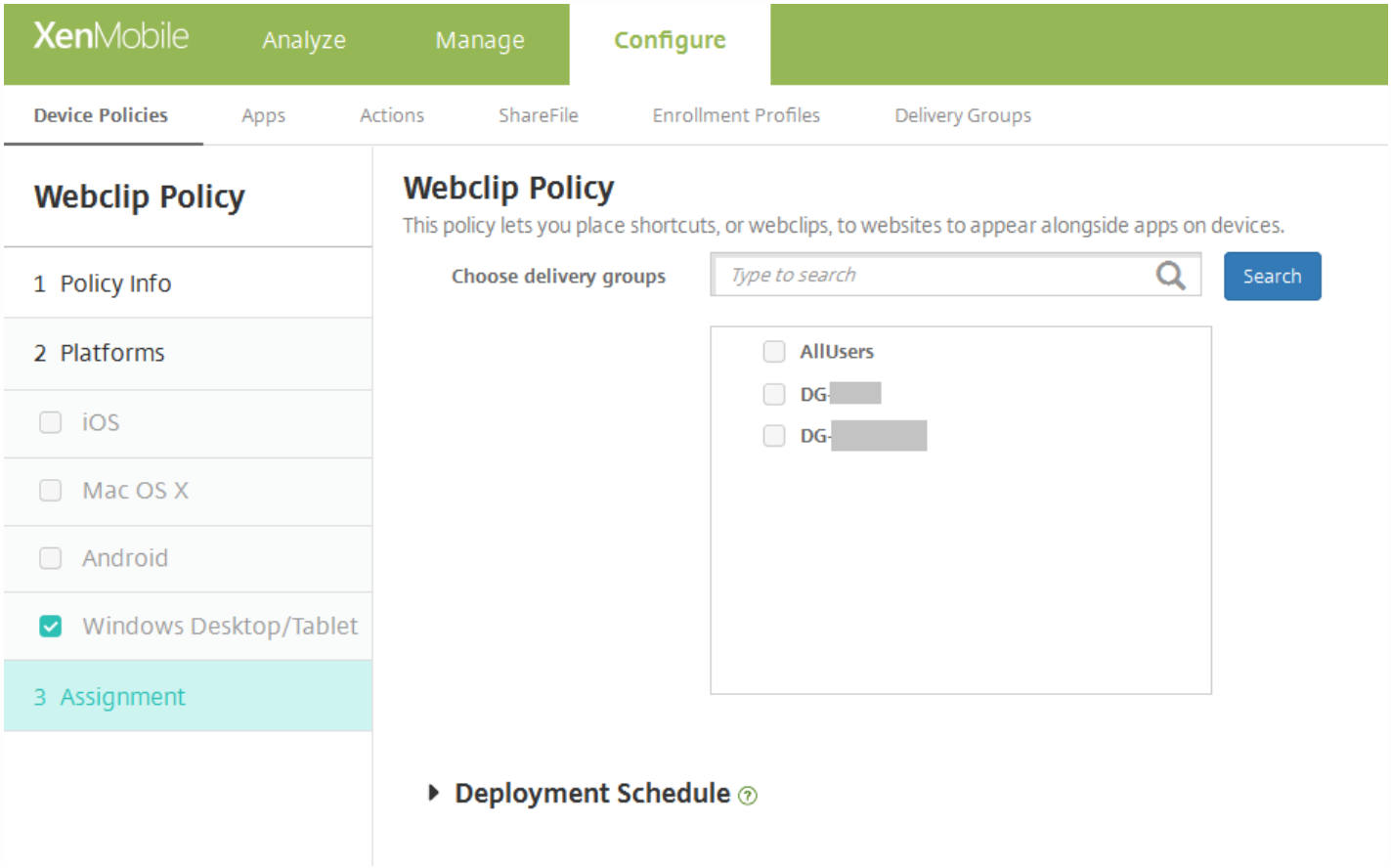


Konfigurieren Sie folgende Einstellungen:

- **Name**: Geben Sie die Beschriftung ein, die mit dem Webclip angezeigt werden soll.
- **URL**: Geben Sie die URL des Webclips ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Webclip-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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

WiFi-Richtlinien für Geräte

Feb 24, 2017

WiFi-Geräterichtlinien werden in XenMobile über die Seite **Konfigurieren > Gerätерichtlinien** der XenMobile-Konsole erstellt und bearbeitet. Mit WiFi-Richtlinien legen Sie fest, wie Benutzer eine Verbindung mit WiFi-Netzwerken aufbauen, indem Sie Netzwerknamen und -typen, Authentifizierungs- und Sicherheitsrichtlinien sowie die Verwendung von Proxyservern definieren und weitere WiFi-bezogene Informationen für alle Benutzer der von Ihnen ausgewählten Geräteplattformen vorgeben.

WiFi-Einstellungen können für folgende Plattformen konfiguriert werden: iOS, Mac OS X, Android (einschl. Geräte mit Android for Work-Aktivierung), Windows Phone und Windows-PCs/Tablets. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Artikel detailliert beschrieben.

iOS-Einstellungen

Mac OS X-Einstellungen

Android-Einstellungen

Windows Phone-Einstellungen

Windows Desktop/Tablet-Einstellungen

Important

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

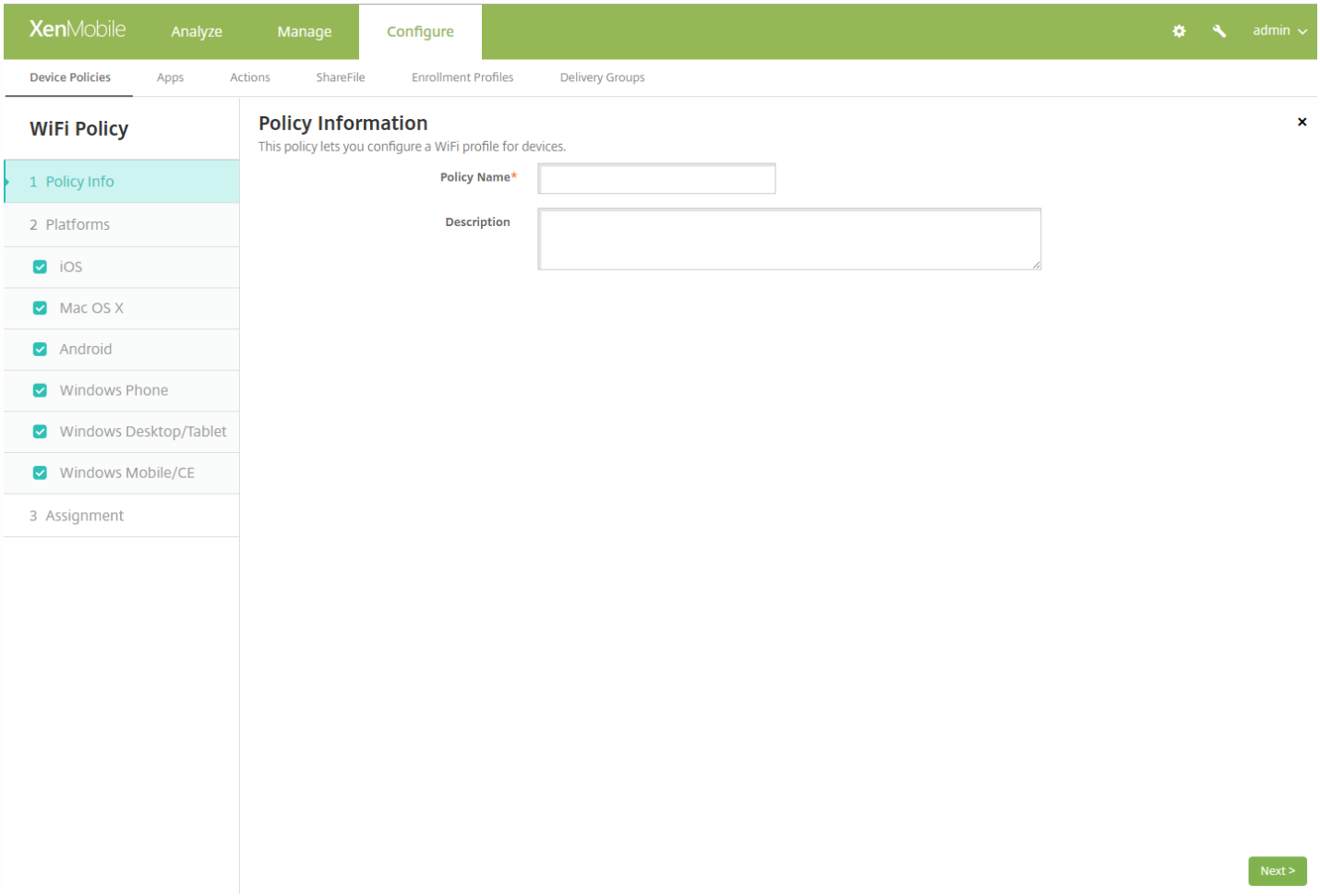
- Erstellen Sie alle Bereitstellungsgruppen, die Sie verwenden möchten.
- Halten Sie Namen und Typ des Netzwerks bereit.
- Planen Sie die zu verwendenden Authentifizierungs-/Sicherheitstypen.
- Halten alle ggf. erforderlichen Proxyserverinformationen bereit.
- Installieren Sie alle erforderlichen Zertifizierungsstellenzertifikate.
- Halten Sie alle erforderlichen gemeinsamen Schlüssel bereit.
- Erstellen Sie die PKI-Entität für zertifikatbasierte Authentifizierung.
- Konfigurieren Sie Anmeldeinformationsanbieter.

Weitere Informationen finden Sie im Artikel Authentifizierung.

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 **WiFi**. Die Seite **WiFi** wird angezeigt.



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

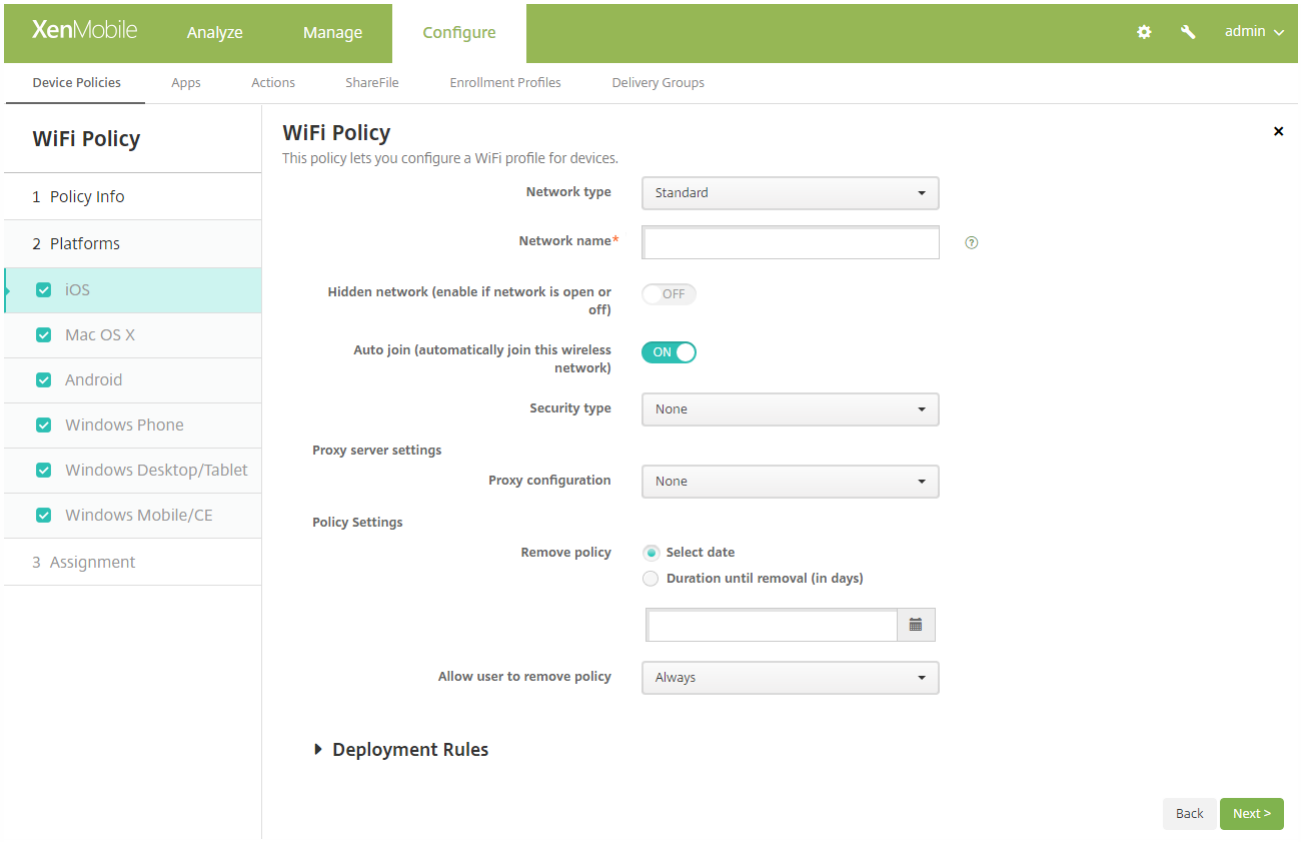
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

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:

- **Netzwerktyp**: Klicken Sie in der Liste auf **Standard**, **Legacyhotspot** oder **Hotspot 2.0**, um den Netzwerktyp festzulegen, den Sie verwenden möchten.
- **Netzwerkname**: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke angezeigt wird. Gilt nicht für **Hotspot 2.0**.
- **Ausgeblendetes Netzwerk (aktivieren, wenn Netzwerk offen oder ausgeschaltet ist)**: Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **Automatisch verbinden (automatisch mit diesem Drahtlosnetzwerk verbinden)**: Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll. Der Standardwert ist **EIN**.
- **Sicherheitstyp**: Klicken Sie in der Liste auf den Sicherheitstyp, den Sie verwenden möchten. Gilt nicht für **Hotspot 2.0**.
  - Ohne: Es ist keine weitere Konfiguration erforderlich.
  - WEP
  - WPA/WPA2 (Persönlich)
  - Beliebig (Persönlich)
  - WEP (Unternehmen)
  - WPA/WPA2 (Unternehmen)
  - Beliebig (Unternehmen)

  In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

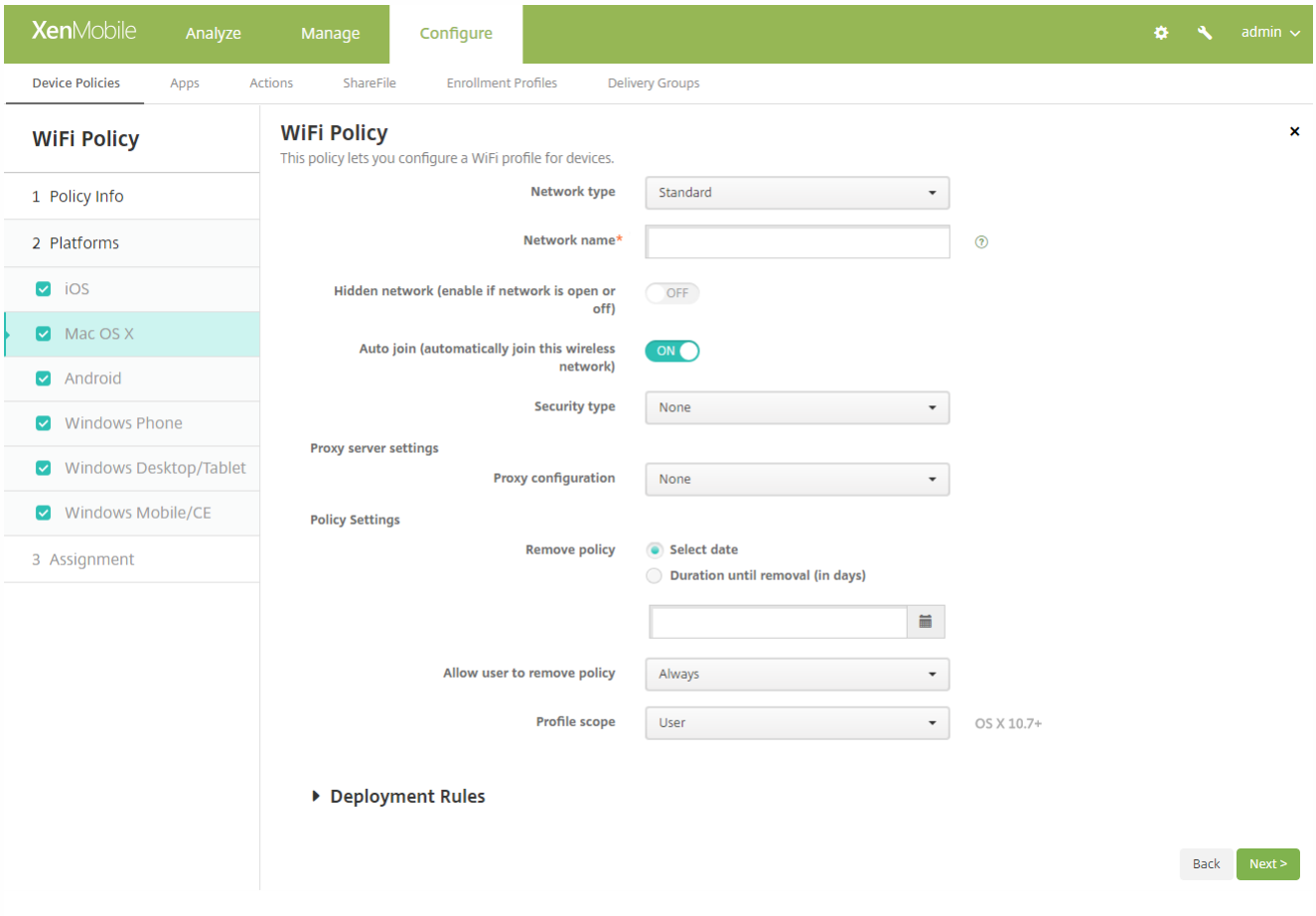
WPA, WPA Persönlich, Beliebig (Persönlich)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Beliebig (Unternehmen)

- **Proxyservereinstellungen**
  - **Proxykonfiguration**: Wählen Sie in der Liste "Ohne", "Manuell" oder "Automatisch" aus, um das Routing der VPN-Verbindung über einen Proxyserver zu konfigurieren, und konfigurieren Sie ggf. zusätzliche Optionen. Der Standardwert ist "Ohne" und erfordert keine weitere Konfiguration.
  - Bei Auswahl von **Manuell** konfigurieren Sie die folgenden Einstellungen:
    - **Hostname oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein.
    - **Serverport**: Geben Sie die Nummer des Proxyserverports ein.
    - **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:
    - **Server-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. Der Standardwert ist **EIN**. Diese Option ist nur für iOS 7.0 und höher verfügbar.

- **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:

- **Netzwerktyp**: Klicken Sie in der Liste auf **Standard**, **Legacyhotspot** oder **Hotspot 2.0**, um den Netzwerktyp festzulegen, den Sie verwenden möchten.
- **Netzwerkname**: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke angezeigt wird. Gilt nicht für **Hotspot 2.0**.
- **Ausgeblendetes Netzwerk (aktivieren, wenn Netzwerk offen oder ausgeschaltet ist)**: Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **Automatisch verbinden (automatisch mit diesem Drahtlosnetzwerk verbinden)**: Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll. Der Standardwert ist **EIN**.
- **Sicherheitstyp**: Klicken Sie in der Liste auf den Sicherheitstyp, den Sie verwenden möchten. Gilt nicht für **Hotspot 2.0**.
  - Ohne: Es ist keine weitere Konfiguration erforderlich.
  - WEP
  - WPA/WPA2 (Persönlich)
  - Beliebig (Persönlich)
  - WEP (Unternehmen)
  - WPA/WPA2 (Unternehmen)
  - Beliebig (Unternehmen)

  In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

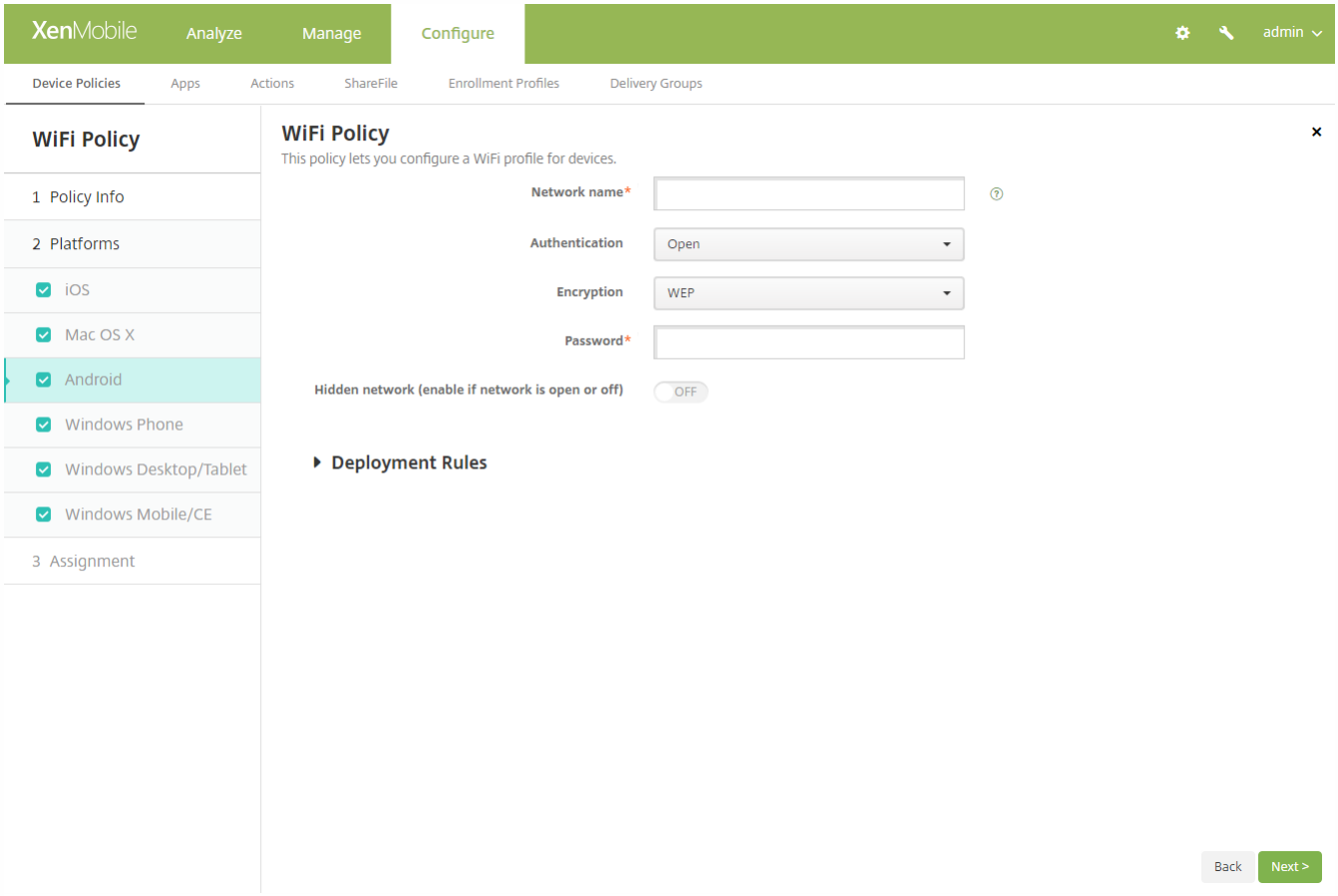
WPA, WPA Persönlich, WPA 2 Persönlich, Beliebig (Persönlich)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Beliebig (Unternehmen)

- **Als Konfiguration für Anmeldefenster verwenden**: Wählen Sie aus, ob die gleichen Anmeldeinformationen für die Benutzeranmeldung verwendet werden sollen.
- **Proxyservereinstellungen**
  - **Proxykonfiguration**: Wählen Sie in der Liste "Ohne", "Manuell" oder "Automatisch" aus, um das Routing der VPN-Verbindung über einen Proxyserver zu konfigurieren, und konfigurieren Sie ggf. zusätzliche Optionen. Der Standardwert ist "Ohne" und erfordert keine weitere Konfiguration.
  - Bei Auswahl von **Manuell** konfigurieren Sie die folgenden Einstellungen:
    - **Hostname oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein.
    - **Serverport**: Geben Sie die Nummer des Proxyserverports ein.
    - **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:
    - **Server-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. Der Standardwert ist **EIN**. Diese Option ist nur für iOS 7.0 und höher verfügbar.
- **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:

- **Netzwerkname**: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke auf den Geräten der Benutzer angezeigt wird.
- **Authentifizierung**: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden soll.
  - Offen
  - Freigegeben
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

  In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

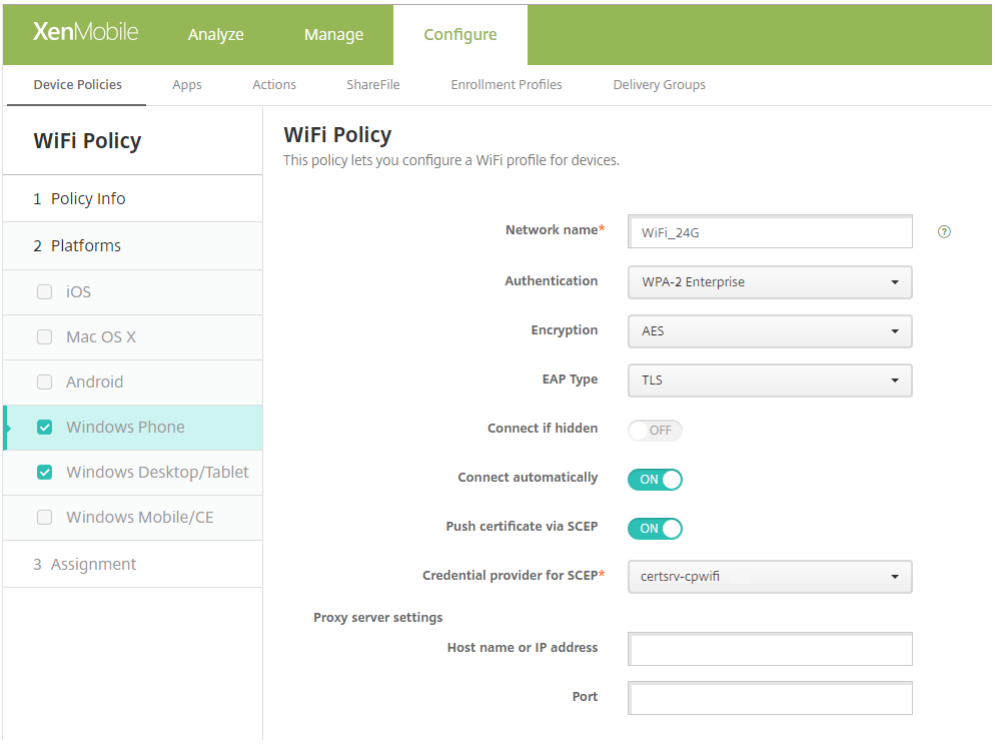
Offen, freigegeben

WPA, WPA-PSK, WPA2, WPA2-PSK

802.1x

- **Ausgeblendetes Netzwerk (aktivieren, wenn Netzwerk offen oder ausgeschaltet ist)**: Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

Konfigurieren von Windows Phone-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Netzwerkname**: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke auf den Geräten der Benutzer angezeigt wird.
- **Authentifizierung**: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden soll.
  - Offen
  - WPA (Persönlich)
  - WPA-2 (Persönlich)
  - WPA-2 Enterprise: Bei der neuesten Version von Windows 10 erfordert die Verwendung von WPA-2 Enterprise die Einrichtung von SCEP, sodass XenMobile das Zertifikat für die Authentifizierung beim WiFi-Server an die Geräte senden kann. Zum Konfigurieren von SCEP rufen Sie die Seite **Verteilung** von **Einstellungen > Anmeldeinformationsanbieter** auf. Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.

    In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

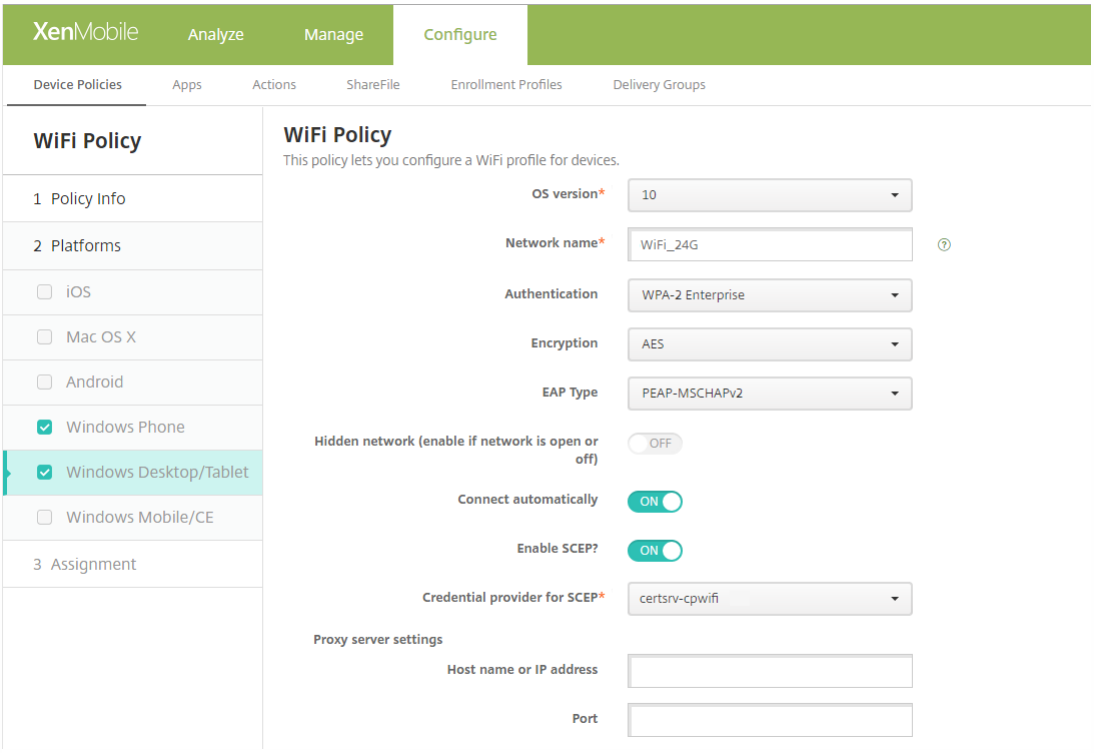
Offen

WPA (Persönlich), WPA-2 (Persönlich)

WPA-2 (Unternehmen)

- **Proxyservereinstellungen**
  - **Hostname oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein.
  - **Port**: Geben Sie die Portnummer des Proxyservers ein.

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

- **Authentifizierung**: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden soll.
  - Offen
  - WPA (Persönlich)
  - WPA-2 (Persönlich)
  - WPA (Unternehmen)
  - WPA-2 Enterprise: Bei der neuesten Version von Windows 10 erfordert die Verwendung von WPA-2 Enterprise die Einrichtung von SCEP, sodass XenMobile das Zertifikat für die Authentifizierung beim WiFi-Server an die Geräte senden kann. Zum Konfigurieren von SCEP rufen Sie die Seite **Verteilung** von **Einstellungen > Anmeldeinformationsanbieter** auf. Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.

    In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

Offen

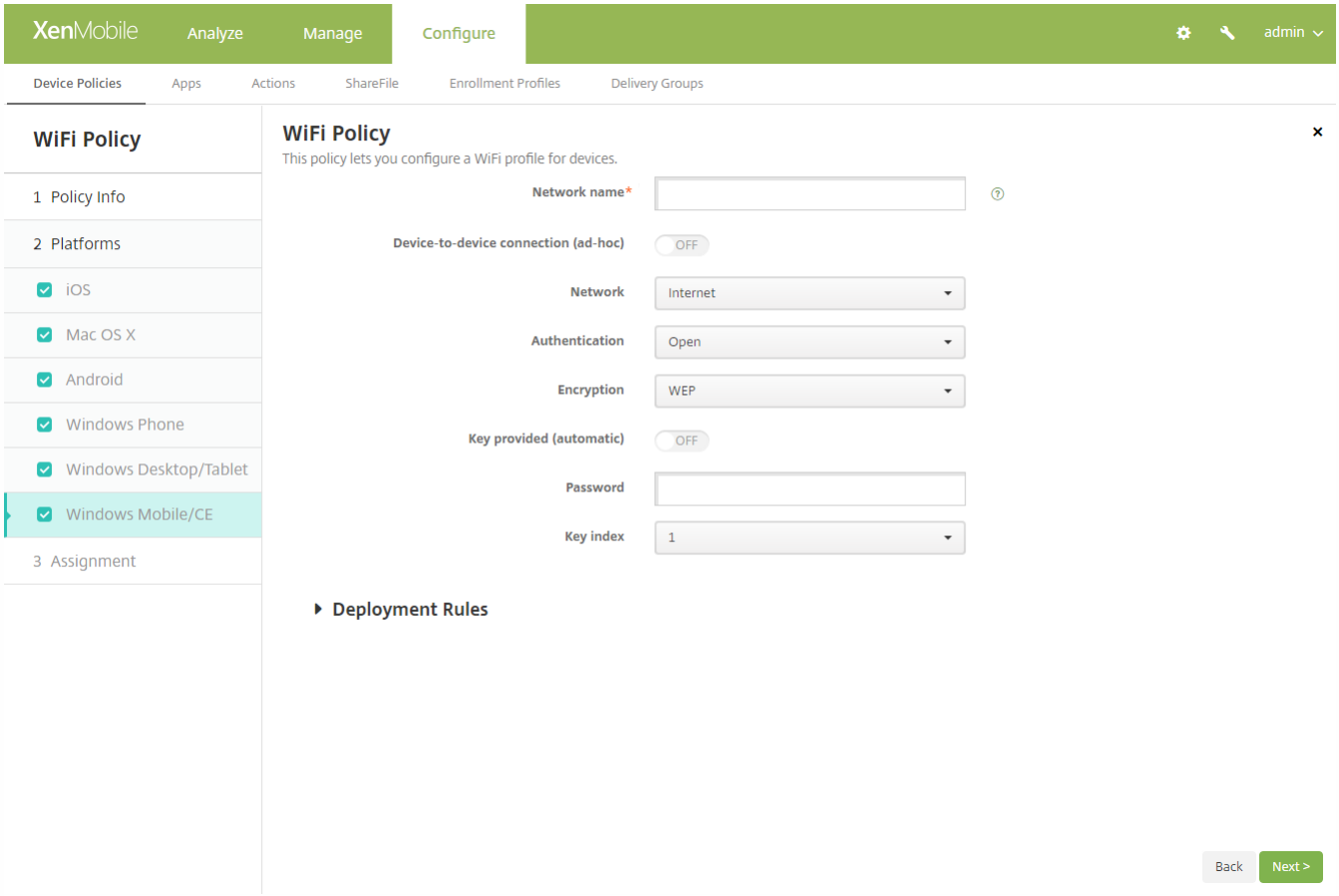
WPA (Persönlich), WPA-2 (Persönlich)

WPA-2 (Unternehmen)

Windows 8.1-Einstellungen

- **Netzwerkname**: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke auf den Geräten der Benutzer angezeigt wird.
- **Authentifizierung**: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden soll.
  - Offen
  - WPA (Persönlich)
  - WPA-2 (Persönlich)
  - WPA (Unternehmen)
  - WPA-2 (Unternehmen)
- **Ausgeblendetes Netzwerk (aktivieren, wenn Netzwerk offen oder ausgeschaltet ist)**: Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **Automatisch verbinden**: Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

Konfigurieren von Windows Mobile/CE



Konfigurieren Sie folgende Einstellungen:

- **Netzwerkname**: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke auf den Geräten der Benutzer angezeigt wird.
- **Gerät-zu-Gerät-Verbindung (ad hoc)**: ermöglicht eine direkte Verbindung zweier Geräte. Die Standardeinstellung ist **Aus**.
- **Netzwerk**: Wählen Sie aus, ob das Gerät mit einer externen Internet-Quelle oder einem Intranet verbunden ist.
- **Authentifizierung**: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden soll.
  - Offen
  - WPA (Persönlich)
  - WPA-2 (Persönlich)
  - WPA-2 (Unternehmen)

  In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

Offen

WPA (Persönlich), WPA-2 (Persönlich)

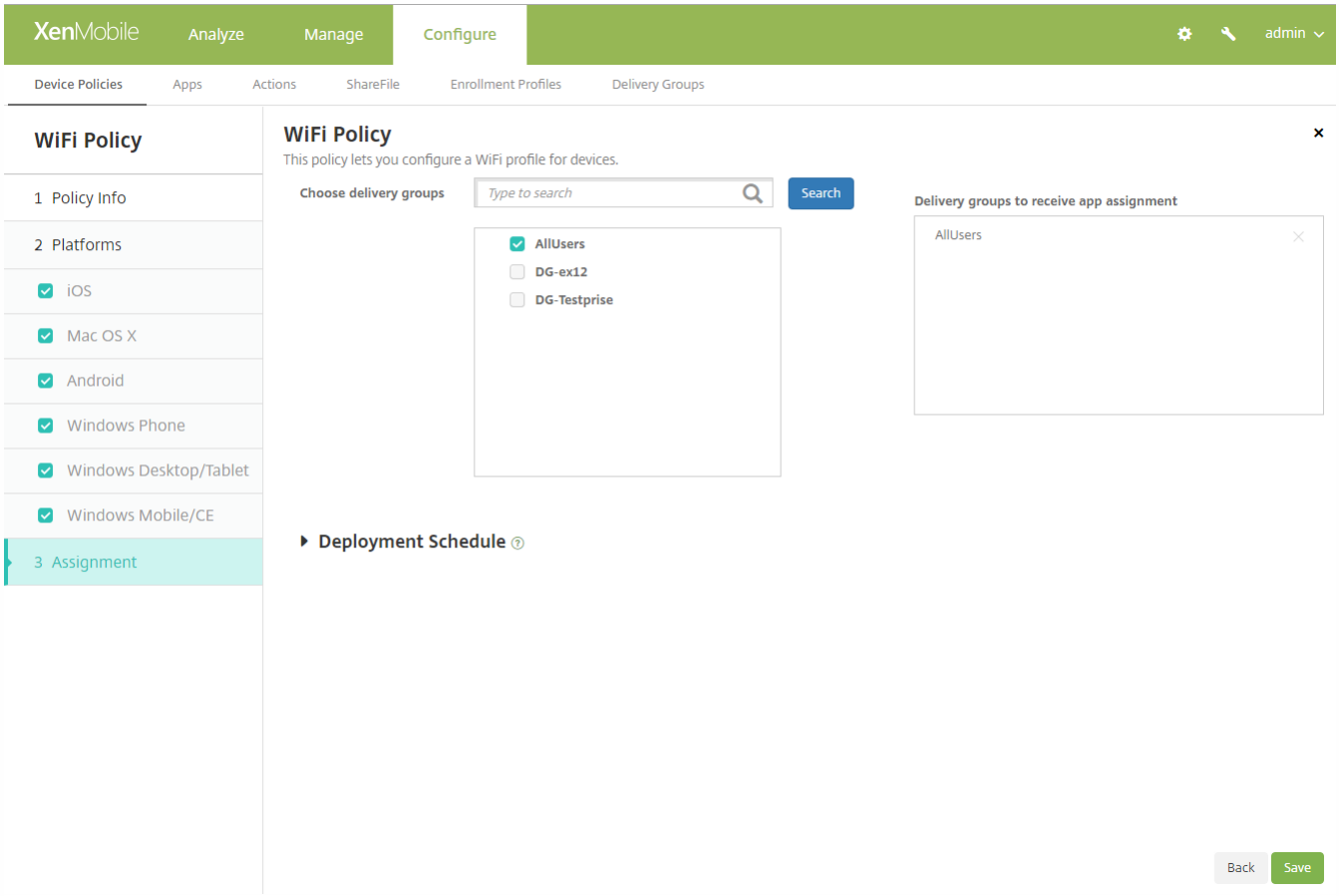
WPA-2 (Unternehmen)

- **Schlüssel (automatisch)**: Wählen Sie aus, ob der Schlüssel automatisch bereitgestellt wird. Die Standardeinstellung ist **Aus**.
- **Kennwort**: Geben Sie das Kennwort in dieses Feld ein.
- **Schlüsselindex**:Geben Sie den Schlüsselindex an. Verfügbare Optionen sind 1, 2, 3 und 4.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die WiFi-Richtlinie wird angezeigt.

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die WiFi-Richtlinie wird angezeigt.
8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die WiFi-Richtlinie wird angezeigt.
8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die WiFi-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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Windows CE-Geräterichtlinie für Zertifikate

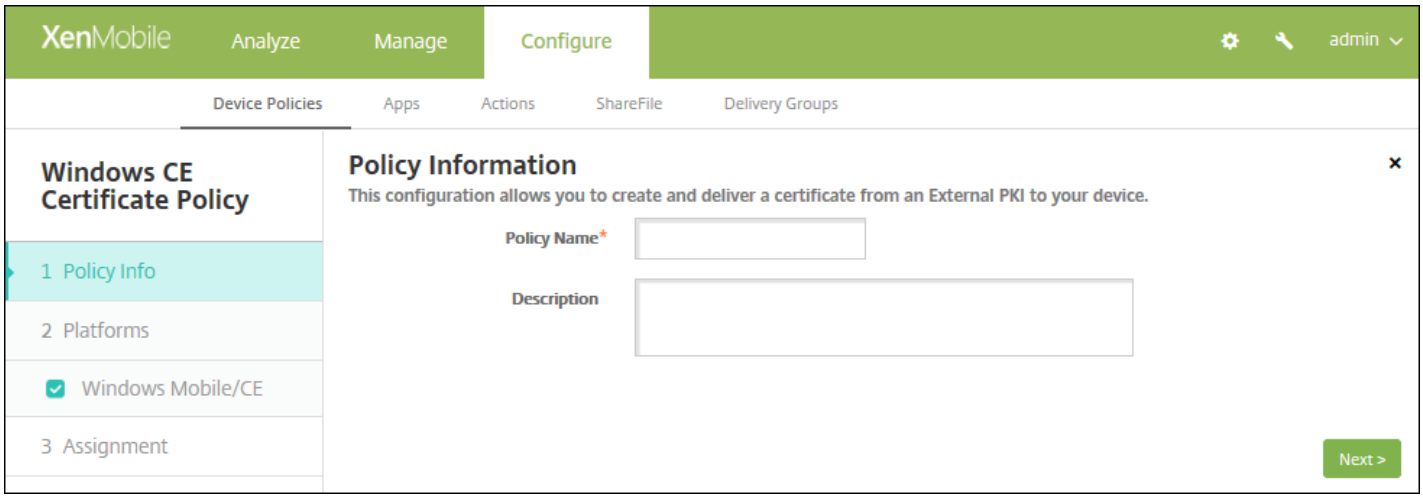
Feb 24, 2017

Sie können in XenMobile eine Geräterichtlinie zum Erstellen und Bereitstellen von Windows Mobile-/CE-Zertifikaten von einer externen PKI auf den Geräten der Benutzer erstellen. Informationen zu Zertifikaten und PKI-Entitäten finden Sie unter Zertifikate.

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.

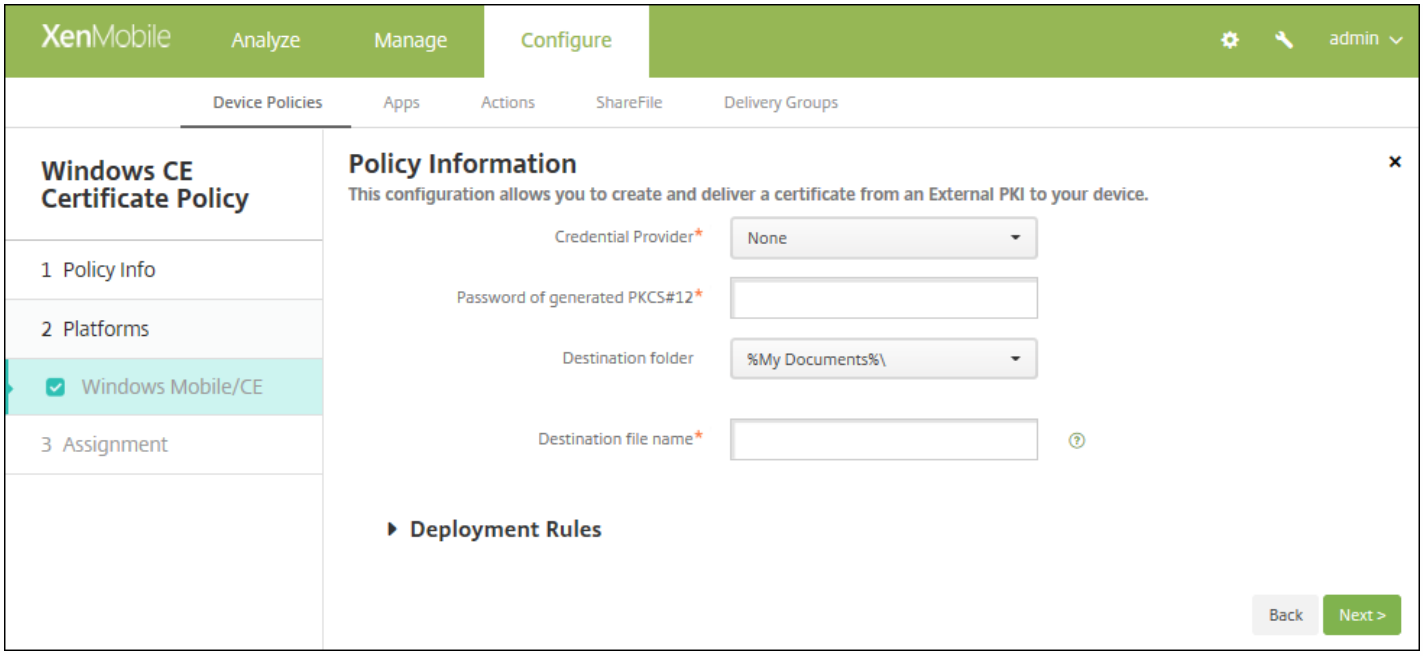
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Windows CE-Zertifikat**. Die Seite **Windows CE-Zertifikat** wird angezeigt.



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.

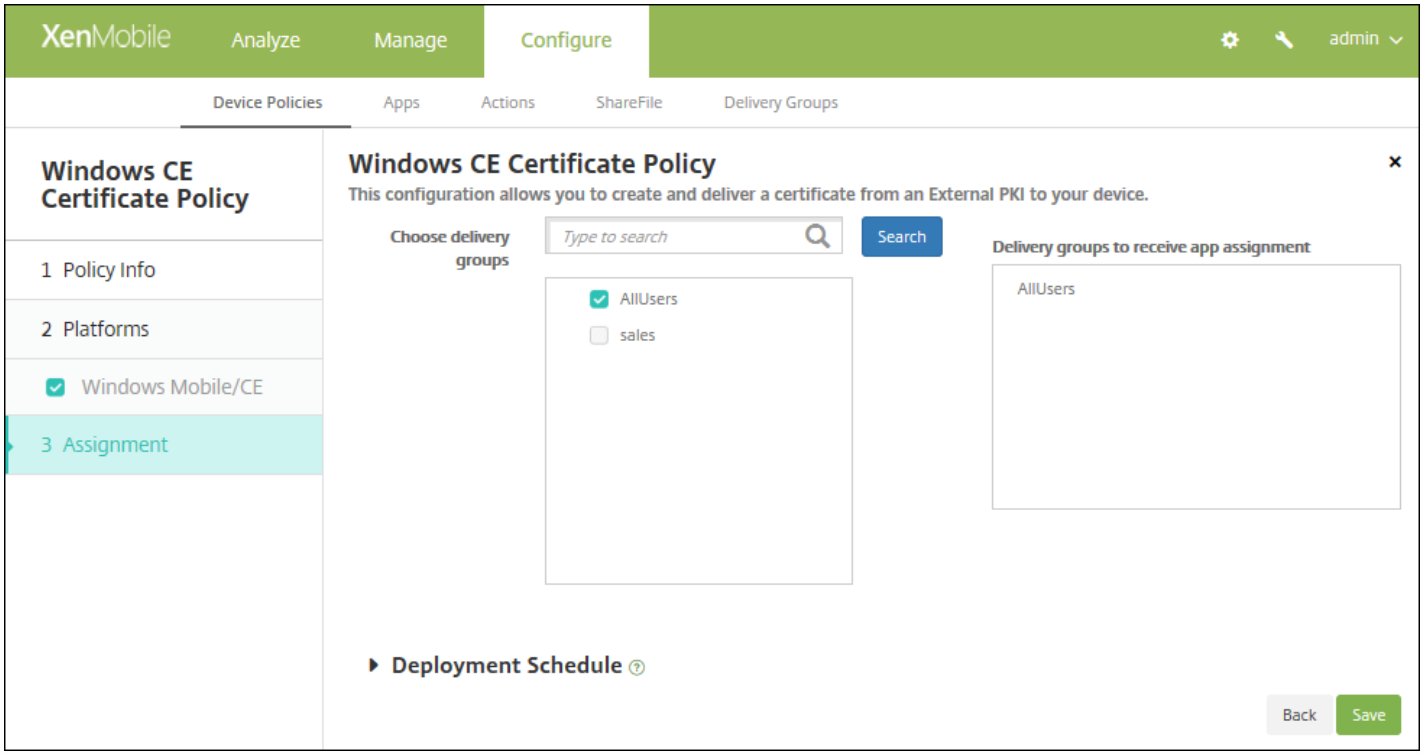


6. Konfigurieren Sie die folgenden Einstellungen:

- **Anmeldeinformationsanbieter**: Klicken Sie in der Liste auf den Anmeldeinformationsanbieter. Der Standardwert ist **Ohne**.
- **Kennwort des generierten PKCS #12**: Geben Sie das Kennwort für die Verschlüsselung der Anmeldeinformationen ein.
- **Zielordner**: Klicken Sie in der Liste auf den Zielordner für die Anmeldeinformationen oder auf **Hinzufügen**, um einen Ordner hinzuzufügen, der noch nicht in der Liste enthalten ist. Es gibt folgende Voreinstellungen:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %Eigene Dokumente%\\
  - %Windows%\
- **Name der Zieldatei**: Geben Sie den Namen der Datei mit den Anmeldeinformationen ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuordnung** für die Windows CE-Zertifikatrichtlinie 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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

XenMobile Store-Geräterichtlinie

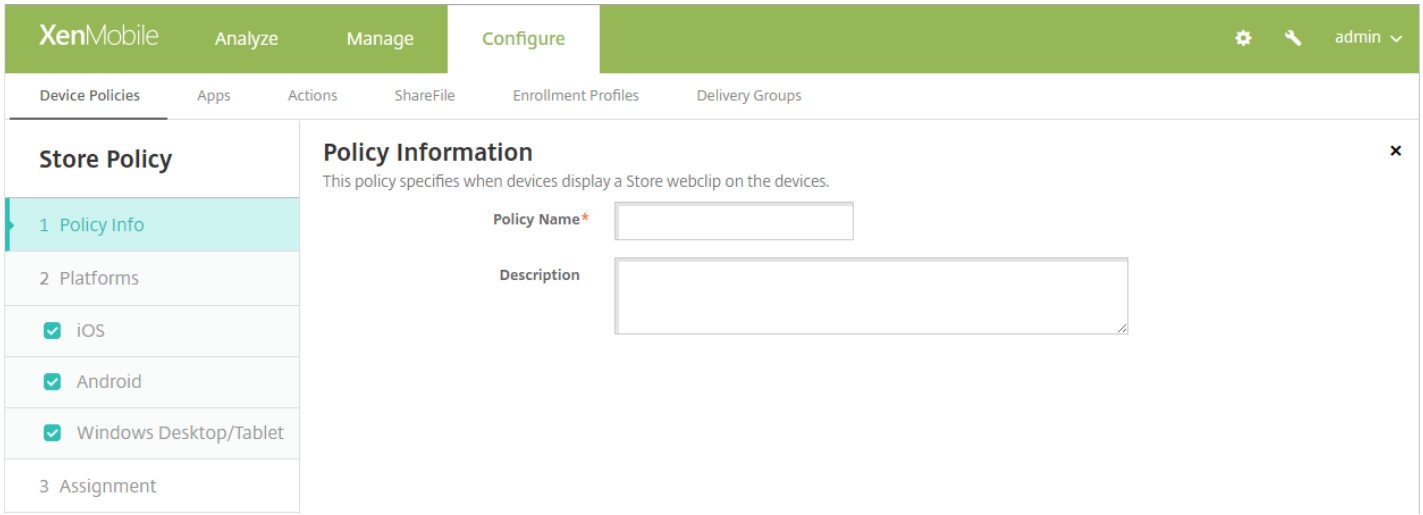
Apr 24, 2017

Sie können in XenMobile eine Richtlinie erstellen, mit der Sie angeben, ob auf dem Homebildschirm von iOS-, Android- und Windows Tablet-Geräten ein XenMobile Store-Webclip angezeigt wird.

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.

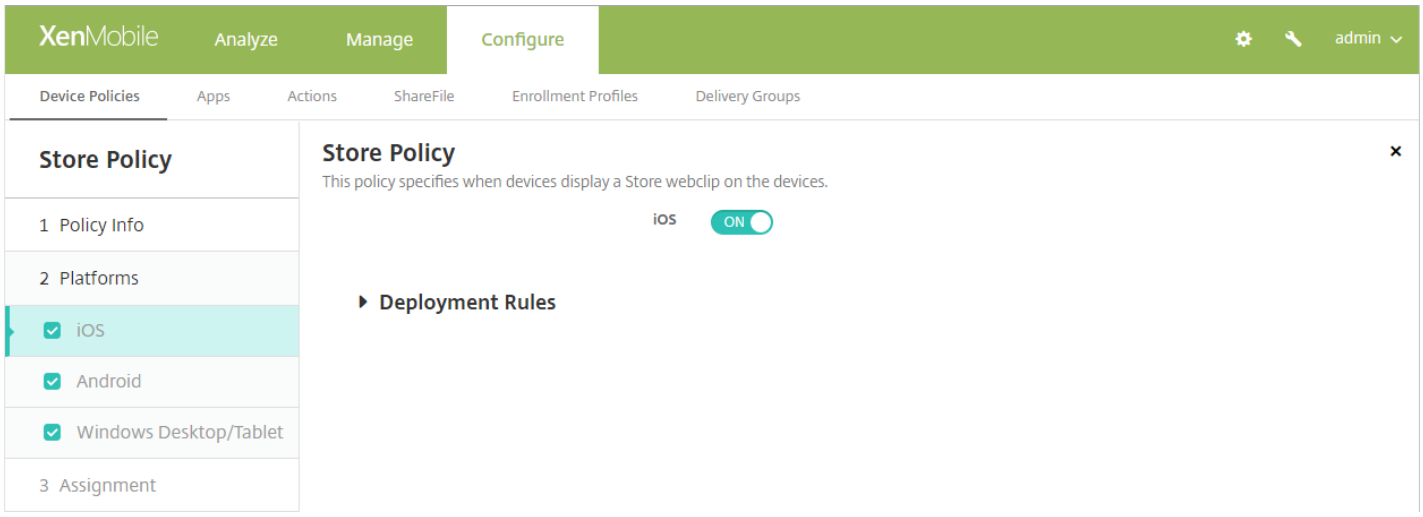
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Store**. Die Seite **Store-Richtlinie** wird angezeigt.



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 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.

7. Legen Sie für jede Plattform, die Sie konfigurieren, fest, ob ein XenMobile Store-Webclip auf den Geräten angezeigt werden soll. Der Standardwert ist **EIN**.

Wenn Sie mit dem Konfigurieren jeweiligen Plattform fertig sind, konsultieren Sie die Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 8.

8. Konfigurieren Sie die Bereitstellungsregeln.

9. Klicken Sie auf **Weiter**. Die Seite "Zuordnung" für die **XenMobile Store-Richtlinie** wird angezeigt.

10. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, 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. Der Standardwert ist **EIN**.Wenn Sie **AUS** wählen, müssen keine anderen Optionen konfiguriert werden.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Der Standardwert 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**. Der Standardwert ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Der Standardwert ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**. Diese Option gilt nicht für iOS.

12. Klicken Sie auf **Speichern**.

XenMobile-Optionsrichtlinien für Geräte

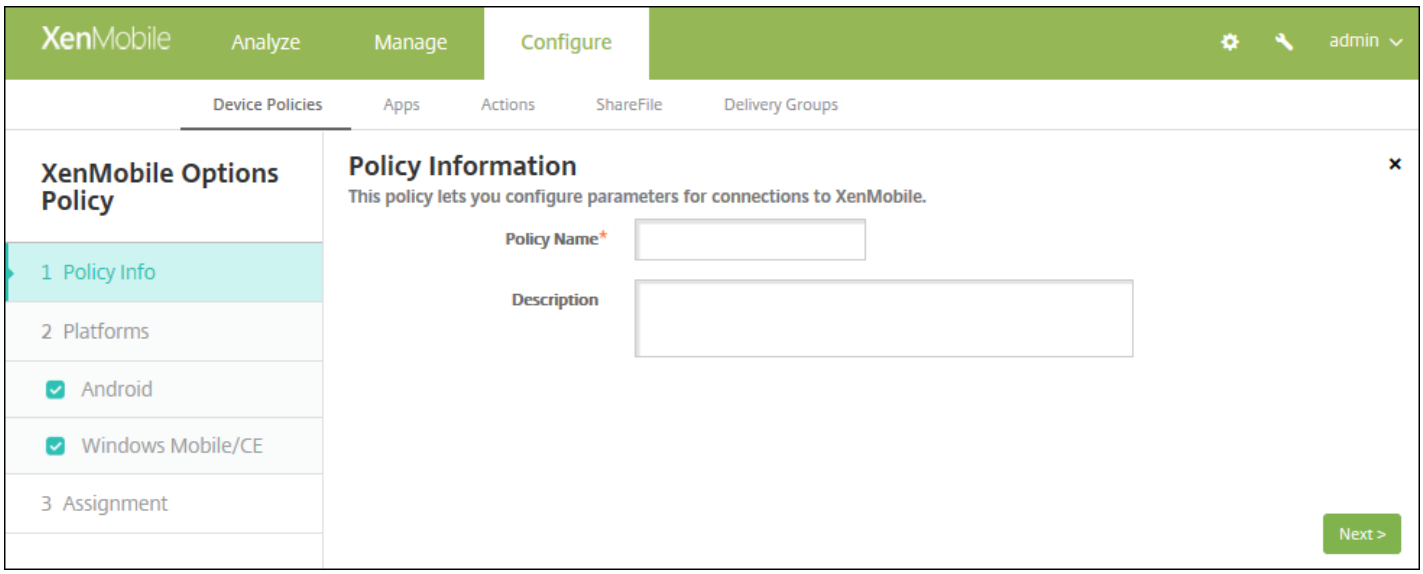
Feb 24, 2017

Sie fügen eine XenMobile-Optionsrichtlinie hinzu, um das Secure Hub-Verhalten für Verbindungen zwischen XenMobile und Android- bzw. Windows Mobile/CE-Geräten zu 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 dann unter **XenMobile-Agent** auf **XenMobile-Optionen**. Die Seite für die Richtlinieninformationen der Richtlinie **XenMobile-Optionen** wird angezeigt.



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

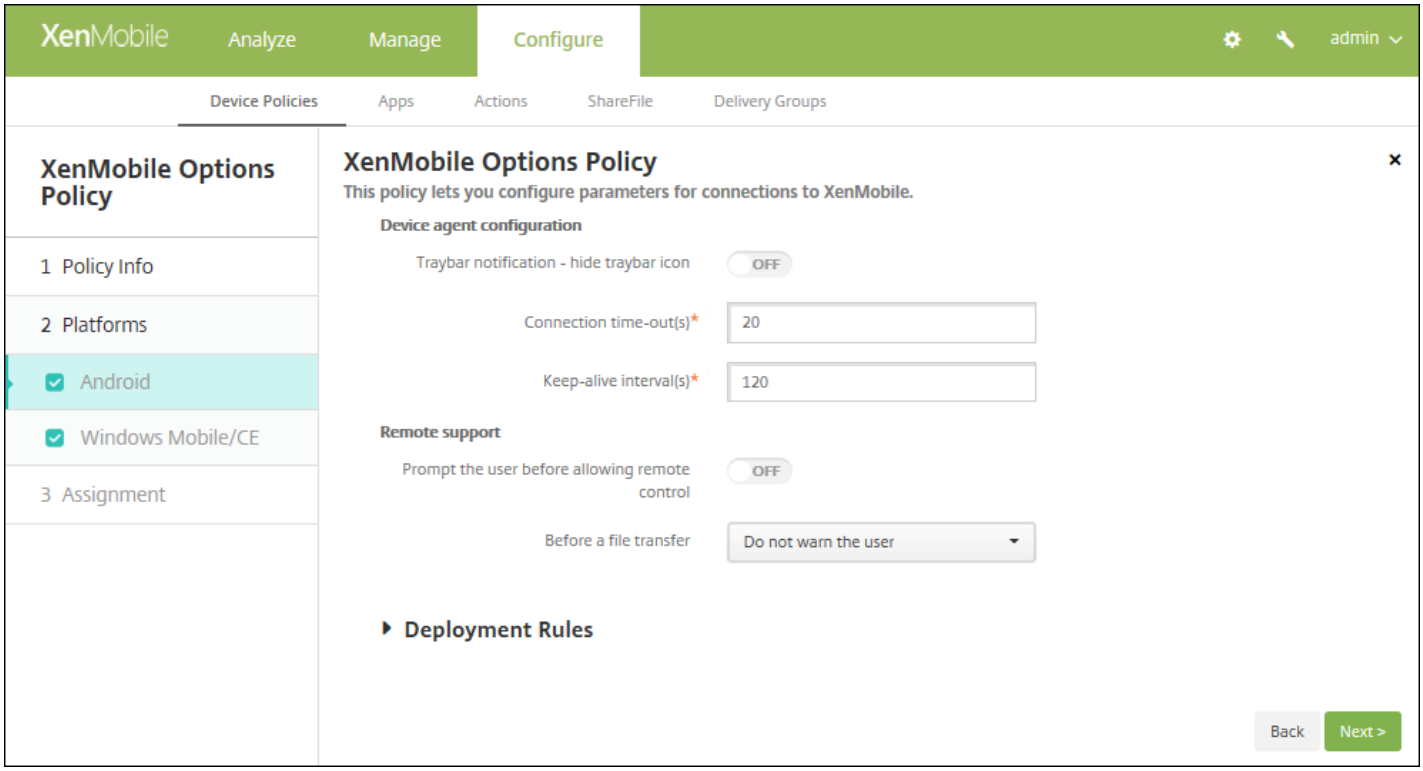
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **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.

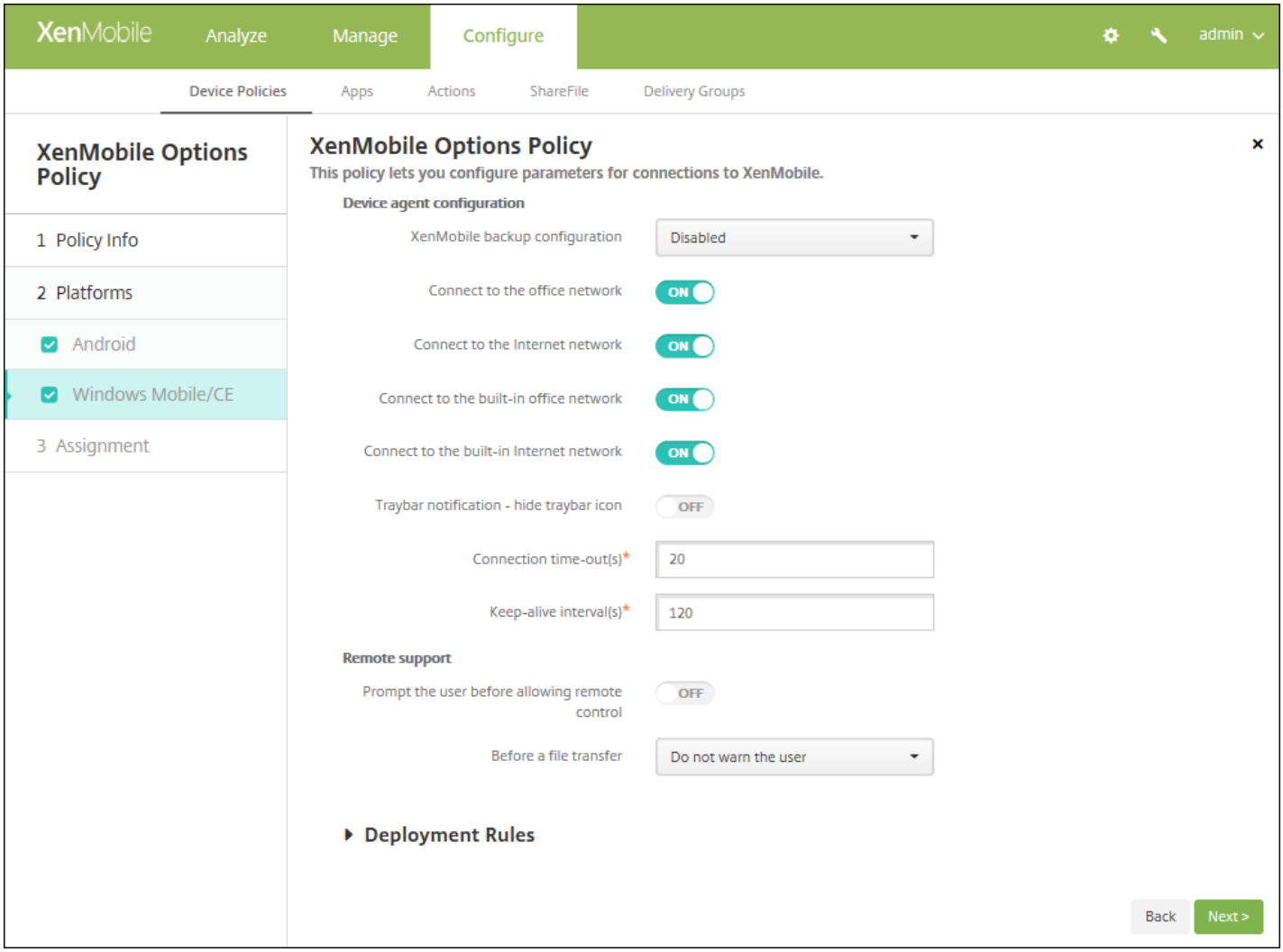
Konfigurieren von Android-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Benachrichtigung im Infobereich - Infobereichsymbol ausblenden**: Wählen Sie aus, ob das Taskleistensymbol angezeigt oder verborgen werden soll. Der Standardwert ist **AUS**.
- **Verbindungstimeout(s)**: Geben Sie an, wie lange (in Sekunden) Verbindungen im Leerlauf sein dürfen, bevor eine Zeitüberschreitung eintritt. Der Standardwert ist 20 Sekunden.
- **Keep-Alive-Intervall(e)**: Geben Sie an wie lange (in Sekunden) Verbindungen aufrechterhalten bleiben sollen. Der Standardwert ist 120 Sekunden.
- **Benutzer fragen, bevor Remotesteuerung zugelassen wird**: Wählen Sie aus, ob vor dem Zulassen des Remotesupports eine Aufforderung an den Benutzer erfolgen soll. Der Standardwert ist **AUS**.
- **Vor einer Dateiübertragung**: Wählen Sie in der Liste aus, ob Benutzer bei einer Dateiübertragung gewarnt oder um Erlaubnis gebeten werden sollen. Verfügbare Werte: **Benutzer nicht warnen**, **Benutzer warnen**, und **Erlaubnis einholen**. Der Standardwert ist **Benutzer nicht warnen**.

Konfigurieren von Windows Mobile-/CE-Einstellungen



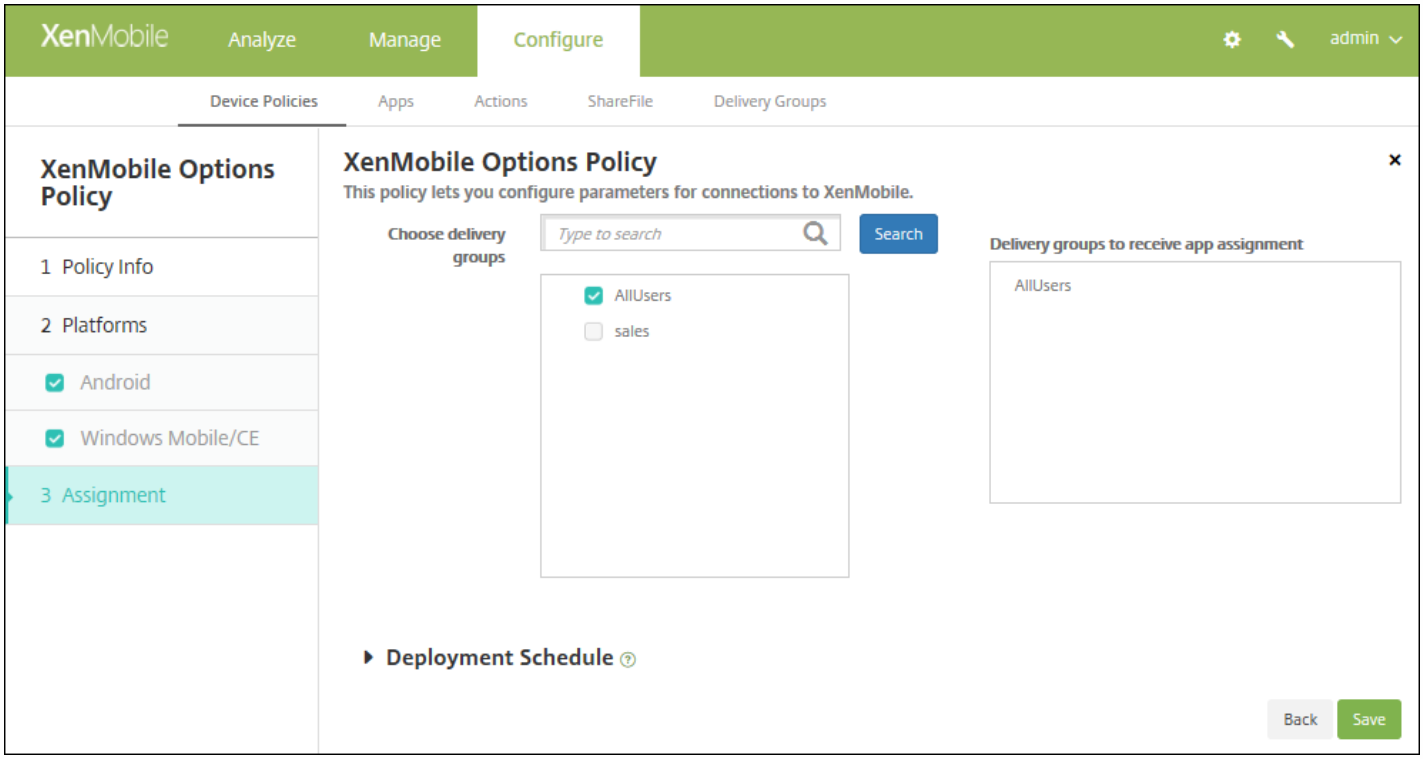
Konfigurieren Sie folgende Einstellungen:

- **Geräteagentkonfiguration**
  - **XenMobile-Backupkonfiguration**: Klicken Sie in der Liste auf eine Option für das Backup der XenMobile-Konfiguration auf den Geräten. Die Standardeinstellung ist **Deaktiviert**. Verfügbare Optionen:
    - Deaktiviert
    - Bei erster Verbindung nach XenMobile-Installation
    - Bei erster Verbindung nach jedem Geräteneustart
  - **Mit Büronetzwerk verbinden**
  - **Mit Internet-Netzwerk verbinden**
  - **Mit integriertem Büronetzwerk verbinden**: Bei Einstellung auf **EIN** erkennt XenMobile das Netzwerk automatisch.
  - **Mit integriertem Internet-Netzwerk verbinden**: Bei Einstellung auf **EIN** erkennt XenMobile das Netzwerk automatisch.
  - **Benachrichtigung im Infobereich - Infobereichsymbol ausblenden**: Wählen Sie aus, ob das Taskleistensymbol angezeigt oder verborgen werden soll. Der Standardwert ist **AUS**.
  - **Verbindungstimeout(s)**: Geben Sie an, wie lange (in Sekunden) Verbindungen im Leerlauf sein dürfen, bevor eine Zeitüberschreitung eintritt. Der Standardwert ist 20 Sekunden.
  - **Keep-Alive-Intervall(e)**: Geben Sie an wie lange (in Sekunden) Verbindungen aufrechterhalten bleiben sollen. Der Standardwert ist 120 Sekunden.

- **Remotesupport**
  - **Benutzer fragen, bevor Remotesteuerung zugelassen wird**: Wählen Sie aus, ob vor dem Zulassen des Remotesupports eine Aufforderung an den Benutzer erfolgen soll. Der Standardwert ist **AUS**.
  - **Vor einer Dateiübertragung**: Wählen Sie in der Liste aus, ob Benutzer bei einer Dateiübertragung gewarnt oder um Erlaubnis gebeten werden sollen. Verfügbare Werte: **Benutzer nicht warnen**, **Benutzer warnen**, und **Erlaubnis einholen**. Der Standardwert ist **Benutzer nicht warnen**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die XenMobile-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 **Später** 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 **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

XenMobile-Deinstallationsrichtlinie

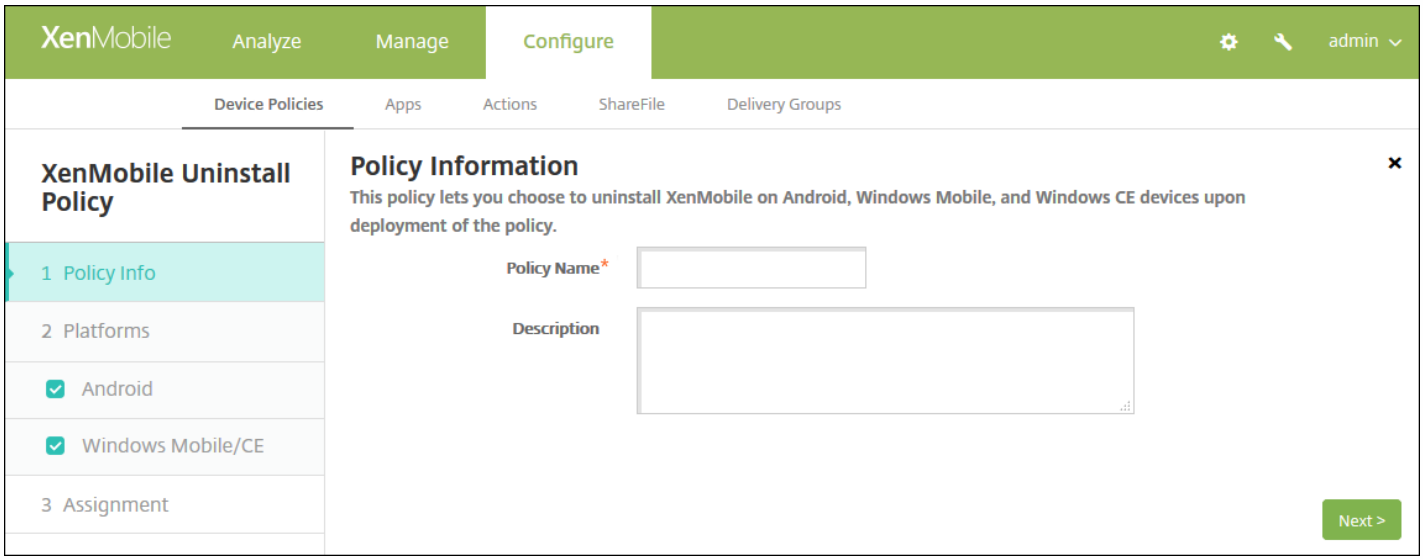
Feb 24, 2017

Sie können in XenMobile eine Geräterichtlinie einrichten, mit der XenMobile von Android- und Windows Mobile-/CE-Geräten deinstalliert wird. Wenn diese Richtlinie bereitgestellt wird, entfernt sie XenMobile von allen Geräten in der Bereitstellungsgruppe.

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 **XenMobile-Deinstallation**. Die Seite für die Richtlinieninformationen der Richtlinie **XenMobile-Deinstallation** wird angezeigt.



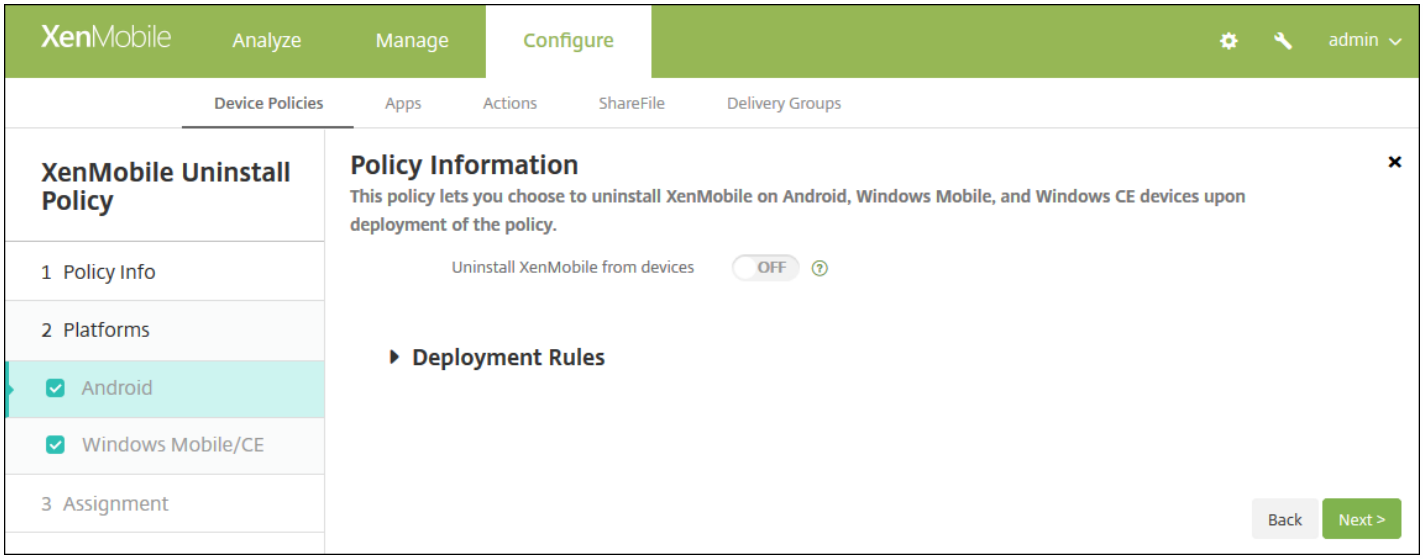
4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

- **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.

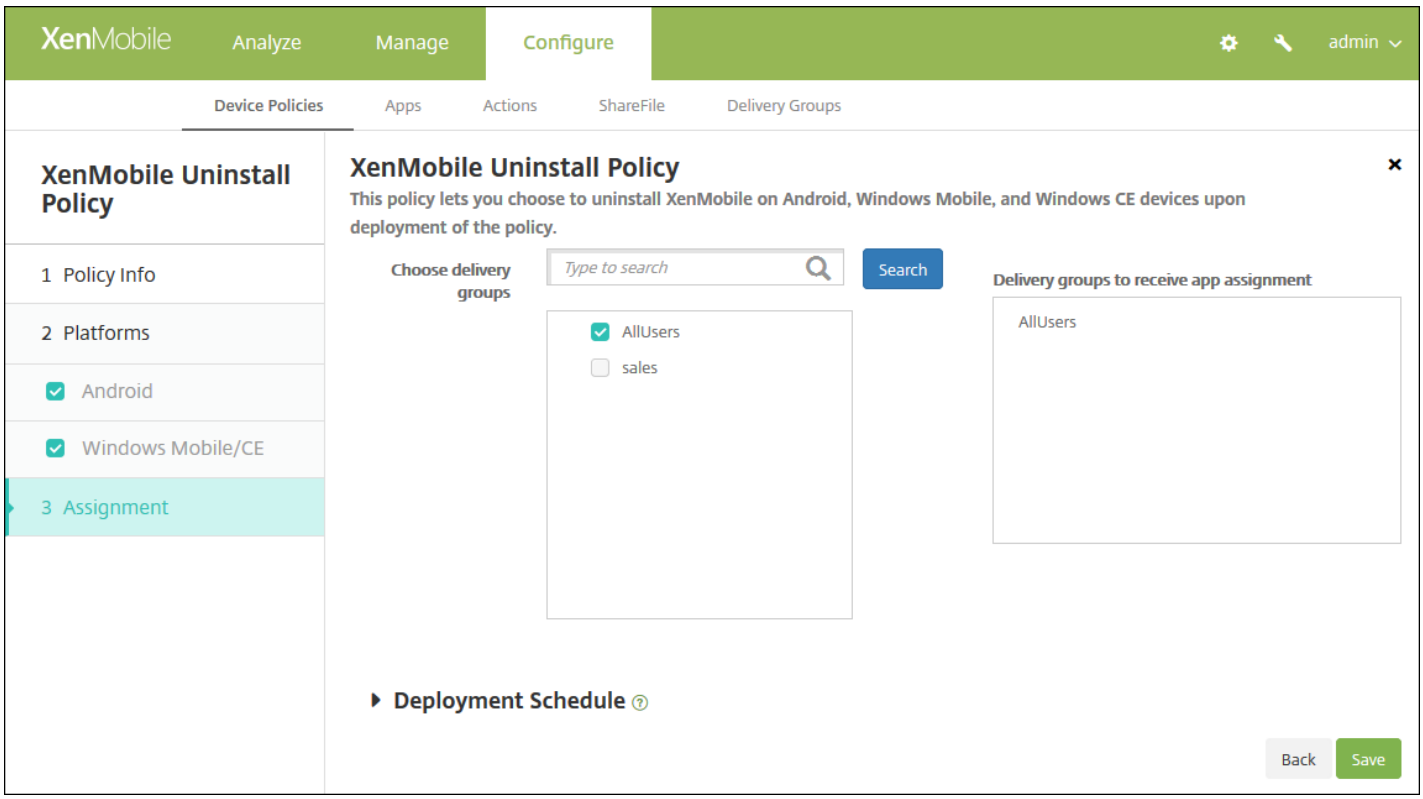


Konfigurieren Sie diese Einstellung für jede ausgewählte Plattform:

- **XenMobile von Geräten deinstallieren**: Wählen Sie aus, ob XenMobile von allen Geräten deinstalliert werden soll, für die Sie die Richtlinie bereitstellen. Der Standardwert ist **AUS**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die XenMobile-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 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Hinzufügen von Apps

Feb 24, 2017

Sie können Apps in XenMobile verwalten. Wenn Sie Apps in der XenMobile-Konsole hinzufügen, können Sie sie in Kategorien einteilen und für Benutzer bereitstellen.

Sie können in XenMobile folgende App-Arten hinzufügen:

- **MDX**: Das sind Apps, die mit dem MDX Toolkit umschlossen wurden (und die zugehörigen Richtlinien). Sie stellen MDX-Apps von internen und öffentlichen Stores bereit.
- **Öffentlicher App-Store**: kostenlose oder kostenpflichtige Apps in einem öffentlichen App-Store, z. B. iTunes oder Google Play. Beispiel: GoToMeeting.
- **Web und SaaS**: Apps, auf die über ein internes Netzwerk (Web-Apps) oder öffentliches Netzwerk (SaaS) zugegriffen wird. Sie können eigene Apps erstellen oder einen der verfügbaren App-Connectors für die Single Sign-On-Authentifizierung bei vorhandenen Web-Apps verwenden. Beispiel: GoogleApps_SAML.
- **Enterprise**: native Apps, die nicht mit dem MDX Toolkit umschlossen wurden und nicht die Richtlinien für MDX-Apps enthalten.
- **Weblinks**: Webadressen (URLs) für eine öffentliche oder private Website oder eine Web-App, die kein Single Sign-On erfordert.

Hinweis

Citrix unterstützt die automatische Installation von iOS- und Samsung Android-Apps. Bei einer automatischen Installation werden Benutzer nicht aufgefordert, Apps zu installieren, die Sie für das Gerät bereitstellen. Stattdessen werden die Apps automatisch im Hintergrund installiert. Sie müssen die folgenden Voraussetzungen erfüllen, damit die Installation automatisch erfolgen kann:

- Für iOS-Apps muss das verwaltete iOS-Gerät im betreuten Modus sein. Einzelheiten finden Sie unter Importieren von Richtlinien für iOS- und Mac OS X-Profile.
- Für Android-Apps müssen Samsung for Enterprise- (SAFE) oder KNOX-Richtlinien auf dem Gerät aktiviert sein. Hierfür müssen Sie über die Geräterichtlinie "Samsung MDM-Lizenzschlüssel" Samsung ELM- und KNOX-Lizenzschlüssel generieren. Weitere Informationen finden Sie unter Samsung MDM-Richtlinien für Geräte.

XenMobile unterstützt Apps für iOS, Mac OS X, Android und Windows, einschließlich XenMobile-Apps (z. B. Secure Hub, Secure Mail, Secure Web), und die Verwendung von MDX-Richtlinien. Mit der XenMobile-Konsole können Sie Apps hochladen und dann auf Benutzergeräten bereitstellen. Neben XenMobile-Apps können Sie die folgenden Arten von Apps hinzufügen:

- Apps, die Sie für Ihre Benutzer entwickeln.
- Apps, in denen Sie Gerätefeatures mit MDX-Richtlinien zulassen oder beschränken möchten.

Zum Verteilen von XenMobile-Apps für iOS und Android laden Sie die MDX-Datei für den öffentlichen Store von Citrix herunter, laden die Dateien in die XenMobile-Konsole hoch (**Konfigurieren > Apps**), aktualisieren die MDX-Richtlinien nach Bedarf und laden dann die MDX-Dateien in die öffentlichen App-Stores hoch.Weitere Informationen finden Sie unter Hinzufügen einer MDX-App in diesem Artikel.

Zum Verteilen von XenMobile-Apps für Windows laden Sie die App-Dateien von Citrix herunter, umschließen sie mit dem MDX Toolkit, laden sie in die XenMobile-Konsole hoch, ändern die MDX-Richtlinien nach Bedarf und stellen die Apps auf den Benutzergeräten über Bereitstellungsgruppen bereit. Weitere Informationen finden Sie unter Bereitstellung von XenMobile-Apps im öffentlichen App-Store in der Dokumentation zu den XenMobile-Apps.

Mit dem MDX Toolkit von Citrix können Apps für iOS-, Mac OS X-, Android- und Windows-Geräte mit Citrix Logik und Richtlinien umschlossen werden. Mit dem Tool können Sie eine Anwendung, die in Ihrer Organisation erstellt wurde, oder eine App, die außerhalb des Unternehmens erstellt wurde, sicher umschließen.

XenMobile enthält eine Reihe von Anwendungsconnectors. Diese Vorlagen können Sie für Single Sign-On (SSO) bei Web- und SaaS-Anwendungen (Software as a Service) und in einigen Fällen auch zum Erstellen und Verwalten von Benutzerkonten konfigurieren. XenMobile umfasst SAML-Connectors (Security Assertion Markup Language). SAML-Connectors werden für Webanwendungen verwendet, die das SAML-Protokoll für SSO und zur Benutzerkontenverwaltung unterstützen. XenMobile unterstützt SAML 1.1 und SAML 2.0.

Sie können auch eigene SAML-Connectors erstellen.

Weitere Informationen finden Sie unter Hinzufügen von Web- und SaaS-Apps in diesem Artikel.

Unternehmensapps residieren üblicherweise im internen Netzwerk. Die Benutzer können eine Verbindung mit Apps über Secure Hub herstellen. Beim Hinzufügen einer Unternehmensapp wird der erforderliche App-Connector von XenMobile erstellt. Weitere Informationen finden Sie unter Hinzufügen von Unternehmensapps in diesem Artikel.

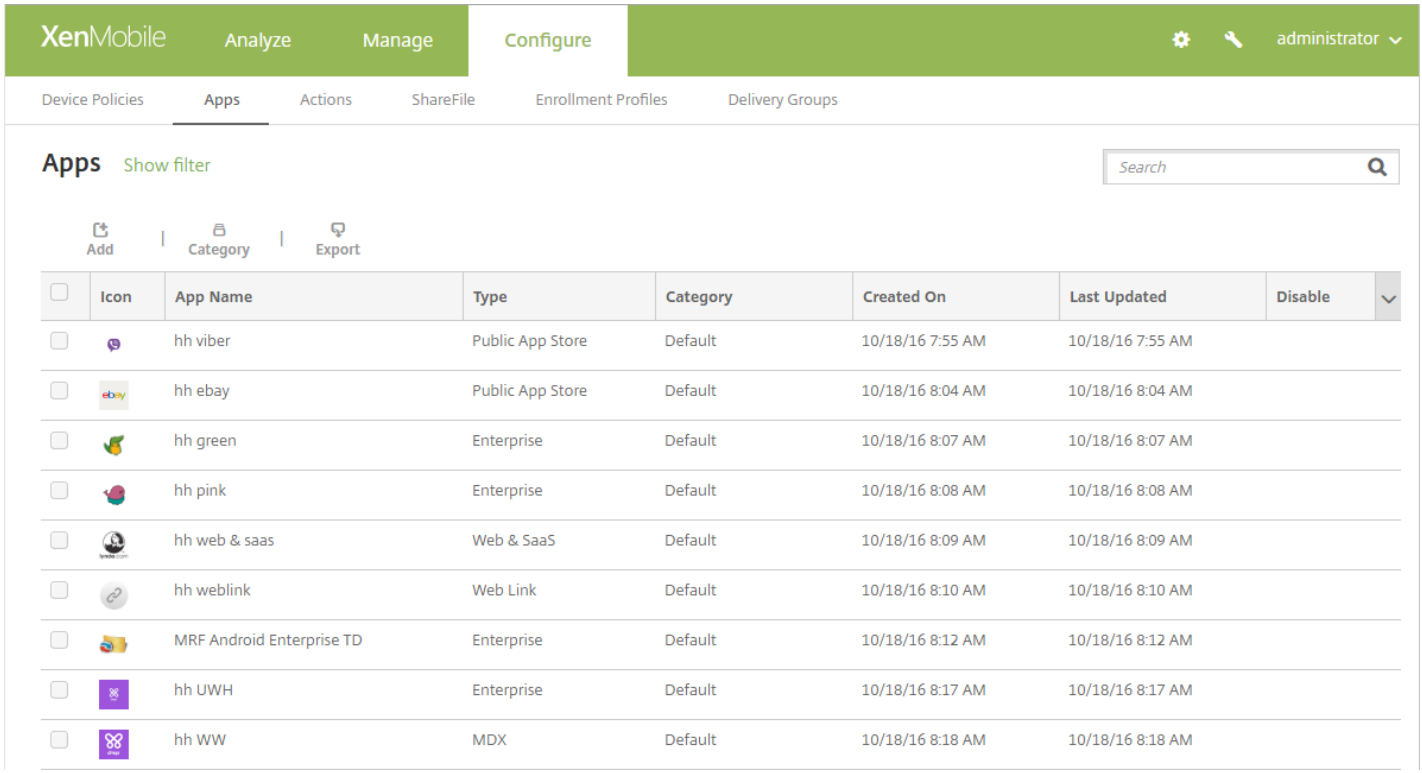
Sie können Einstellungen zum Abrufen der Namen und Beschreibungen von Apps aus dem Apple App Store, Google Play und dem Windows Store konfigurieren. Bei Abrufen der App-Informationen aus dem Store werden der vorhandene Name und die vorhandene Beschreibung in XenMobile überschrieben. Weitere Informationen finden Sie unter Hinzufügen von Apps aus einem öffentlichen App-Store in diesem Artikel.

Ein Weblink ist die Webadresse einer Internet- oder Intranetsite. Er kann auch auf eine Web-App zeigen, für die kein SSO erforderlich ist. Wenn Sie die Konfiguration eines Weblinks abgeschlossen haben, wird dieser als Symbol im XenMobile Store angezeigt. Der Link wird mit der Liste der verfügbaren Anwendungen und Desktops angezeigt, wenn Benutzer sich bei Secure Hub anmelden. Weitere Informationen finden Sie unter Hinzufügen von Weblink-Apps in diesem Artikel.

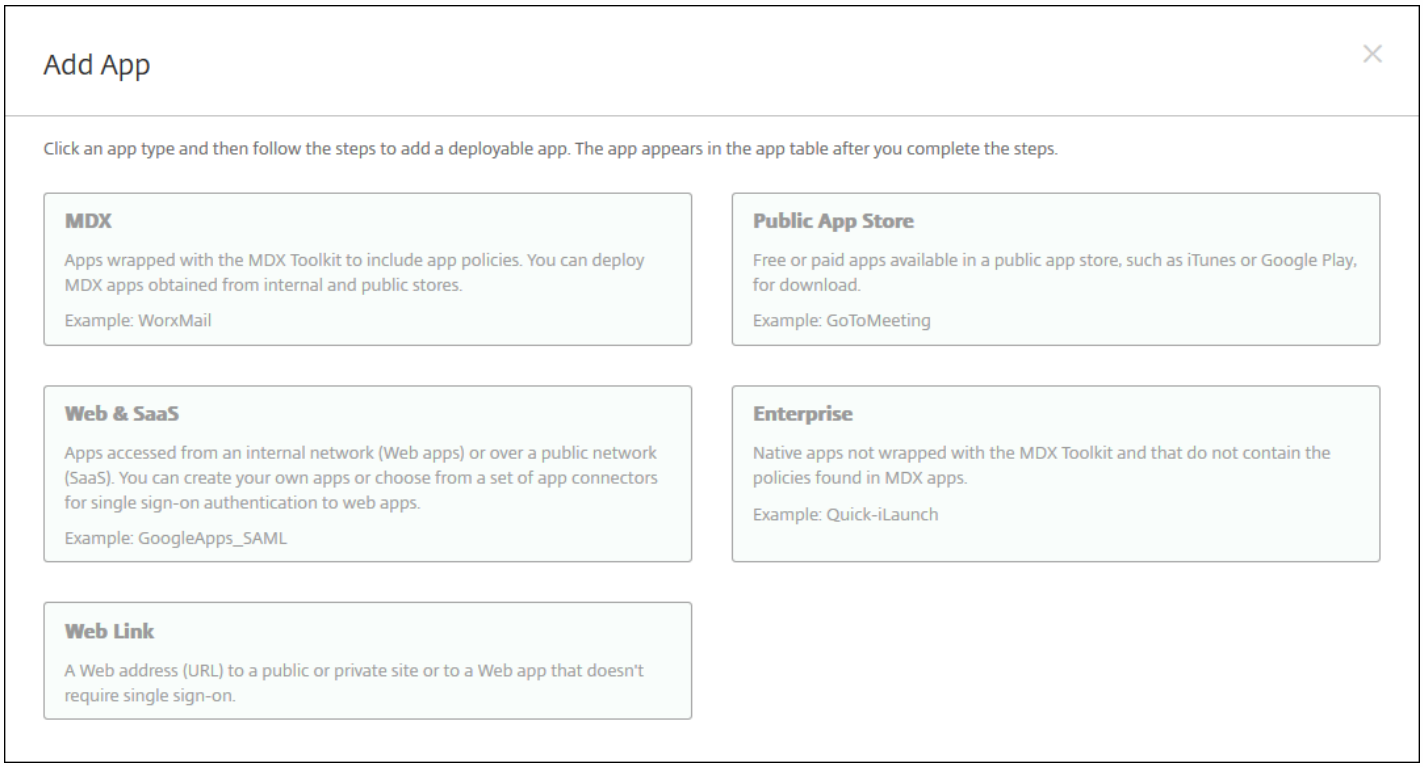
Hinzufügen von MDX-Apps

Wenn Sie eine umschlossene mobile MDX-App für iOS-, Android- oder Windows Phone-Geräte erhalten, können Sie diese in XenMobile hochladen. Nach dem Hochladen der App können Sie die App- und Richtlinieneinstellungen konfigurieren. Informationen über die für die einzelnen Geräteplattformen verfügbaren App-Richtlinien finden Sie unter .MDX-Richtlinien In dem Abschnitt finden Sie ebenfalls detaillierte Richtlinieninformationen.

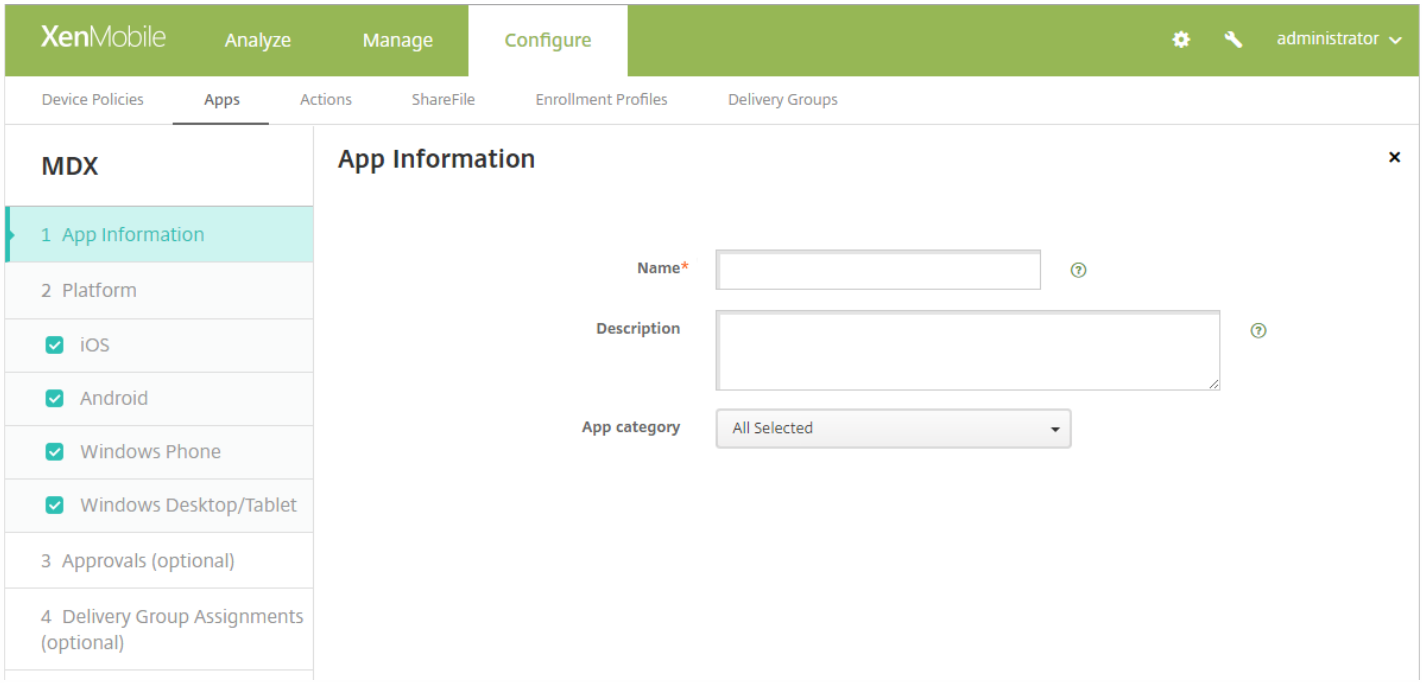
1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren** > **Apps**. Die Seite **Apps** wird angezeigt.



2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



3. Klicken Sie auf **MDX**. Die Seite **App-Informationen** wird angezeigt.



4. Geben Sie auf der Seite **App-Informationenen** die folgenden Informationen ein:

- **Name**: Geben Sie einen aussagekräftigen Namen für die App ein. Dieser Name wird in der Tabelle der Apps unter **App-Name** angezeigt.
- **Beschreibung**: Geben Sie optional eine Beschreibung der App ein.
- **App-Kategorie**: Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen möchten. Weitere Informationen über App-Kategorien finden Sie unter Erstellen von App-Kategorien.

5. Klicken Sie auf **Weiter**. Die Seite **Plattform** 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 11.

7. Klicken Sie auf **Upload** und navigieren Sie zum Speicherort der gewünschten MDX-Datei.

- Wenn Sie eine iOS-B2B-App aus dem Programm für Volumenlizenzen hinzufügen, klicken Sie auf **Ist Ihre Anwendung eine VSS-B2B-Anwendung?** und klicken Sie in der Liste auf das B2B-VPP-Konto, das Sie verwenden möchten.

8. Klicken Sie auf **Weiter**. Die Seite mit den App-Details wird angezeigt.

9. Konfigurieren Sie die folgenden Einstellungen:

- **Dateiname**: Geben Sie den Dateinamen der App ein.
- **App-Beschreibung**: Geben Sie eine Beschreibung für die App ein.
- **App-Version**: Geben Sie optional die Nummer der App-Version ein.
- **OS-Version (Minimum)**: Geben Sie die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
- **OS-Version (Maximum)**: Geben Sie die neueste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
- **Ausgeschlossene Geräte**: Geben Sie optional Hersteller oder Gerätemodelle an, auf denen die App nicht ausgeführt

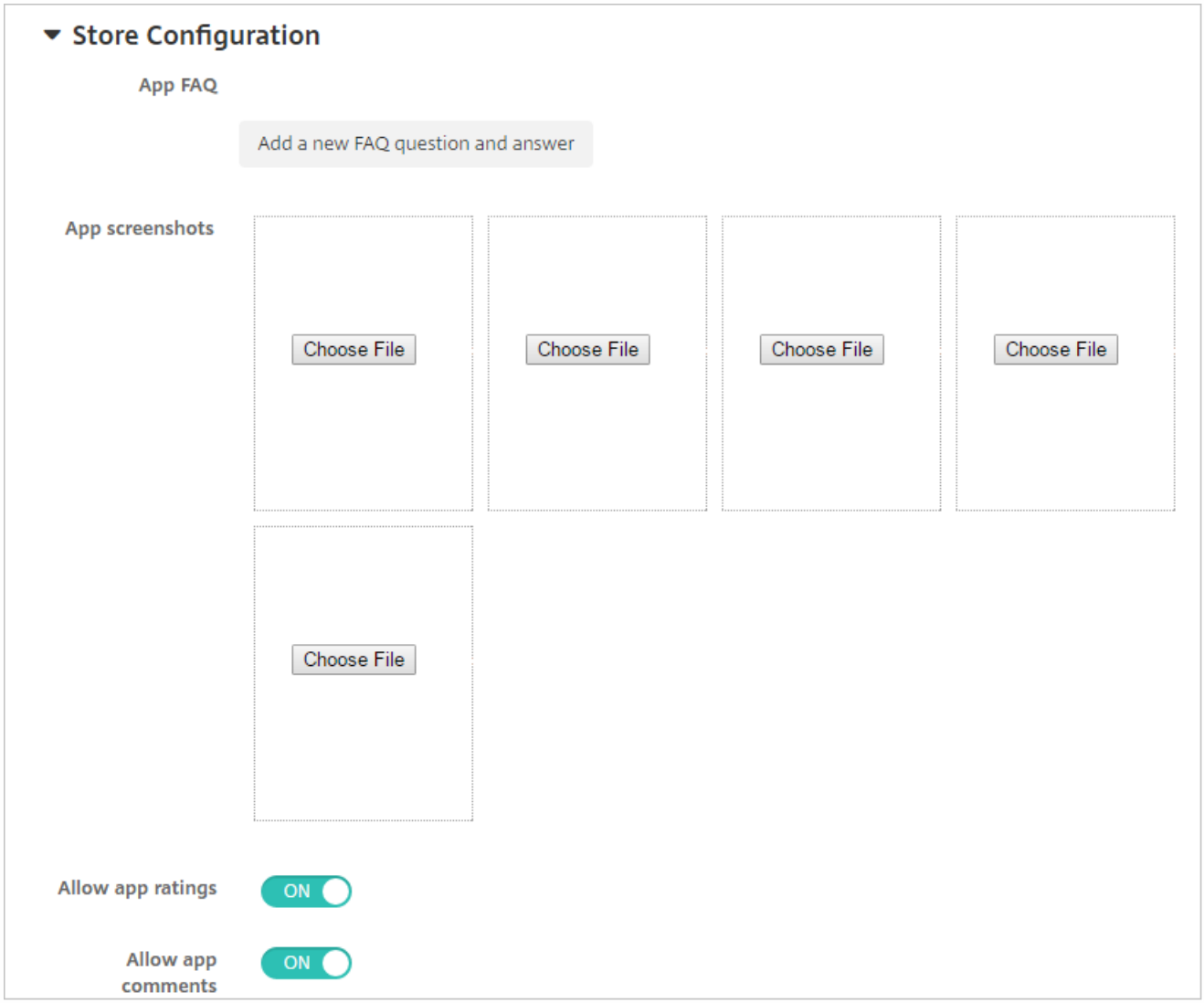
werden kann.

- **App entfernen, wenn MDM-Profil entfernt wird**: Wählen Sie aus, ob die App von Geräten entfernt werden soll, wenn das MDM-Profil entfernt wird. Der Standardwert ist **EIN**.
- **App-Datenbackup verhindern**: Wählen Sie aus, ob Benutzer die App-Daten sichern können sollen. Der Standardwert ist **EIN**.
- **Verwaltung der App erzwingen**: Wählen Sie aus, ob Benutzer bei Installation der App als nicht verwaltet aufgefordert werden, die Verwaltung der App auf nicht betreuten Geräten zuzulassen. Der Standardwert ist **EIN**. Verfügbar in iOS 9.0 und höher.

10. Konfigurieren Sie die **MDX-Richtlinien**. MDX-Richtlinien variieren je nach Plattform und bieten Optionen für Richtlinienbereiche wie Authentifizierung, Gerätesicherheit, Netzwerkanforderungen, Sonstiger Zugriff, Verschlüsselung, App-Interaktion, App-Einschränkungen, App-Netzwerkzugriff, App-Protokolle und App-Geofence. In der Konsole kann eine QuickInfo mit einer Beschreibung der Richtlinien angezeigt werden. Weitere Informationen über App-Richtlinien für MDX-Apps, z. B. eine Tabelle mit Informationen dazu, welche Richtlinien für welche Plattformen gelten, finden Sie unter MDX-Richtlinien.

11. Konfigurieren Sie die Bereitstellungsregeln.

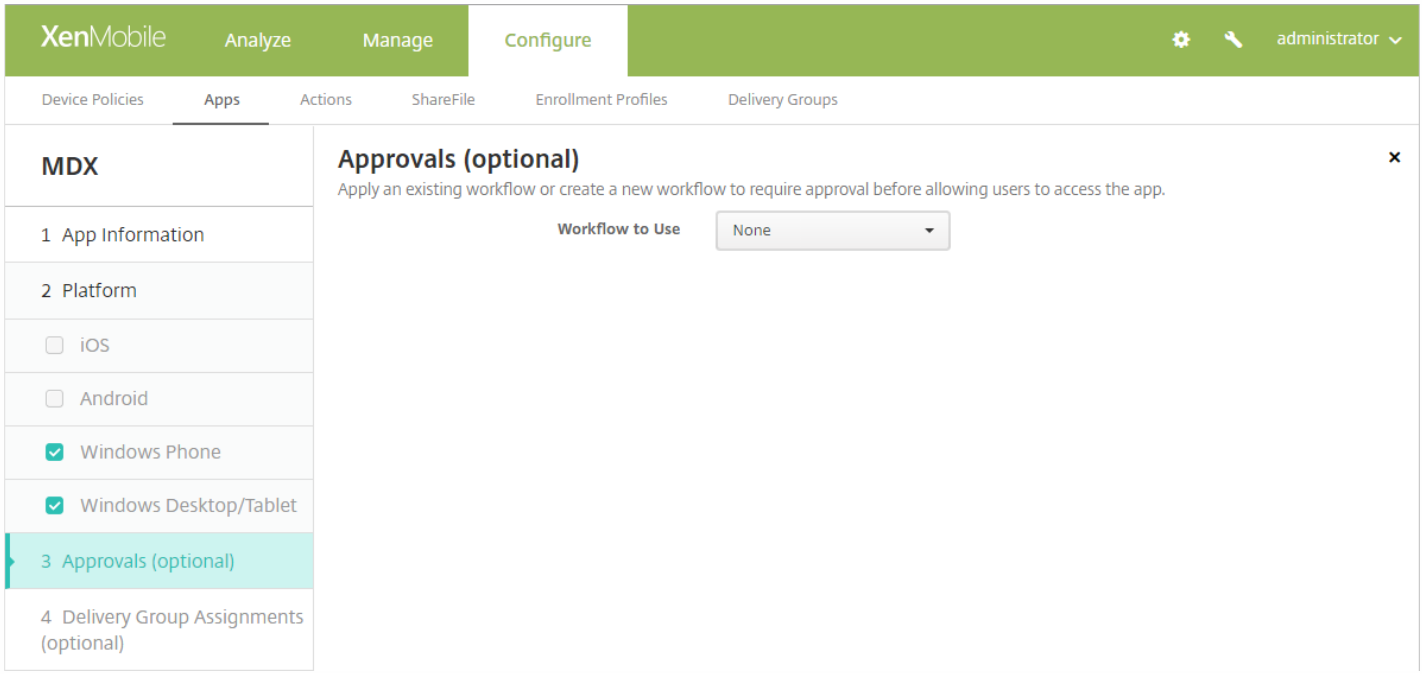
12. Erweitern Sie **XenMobile Store-Konfiguration**.



Sie können optional FAQ oder Screenshots für die App zur Anzeige im XenMobile 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 XenMobile 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. Der Standardwert ist **EIN**.
  - **App-Kommentare zulassen**: Wählen Sie aus, ob eine Kommentierung der App durch die Benutzer zugelassen werden soll. Der Standardwert ist **EIN**.

13. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.



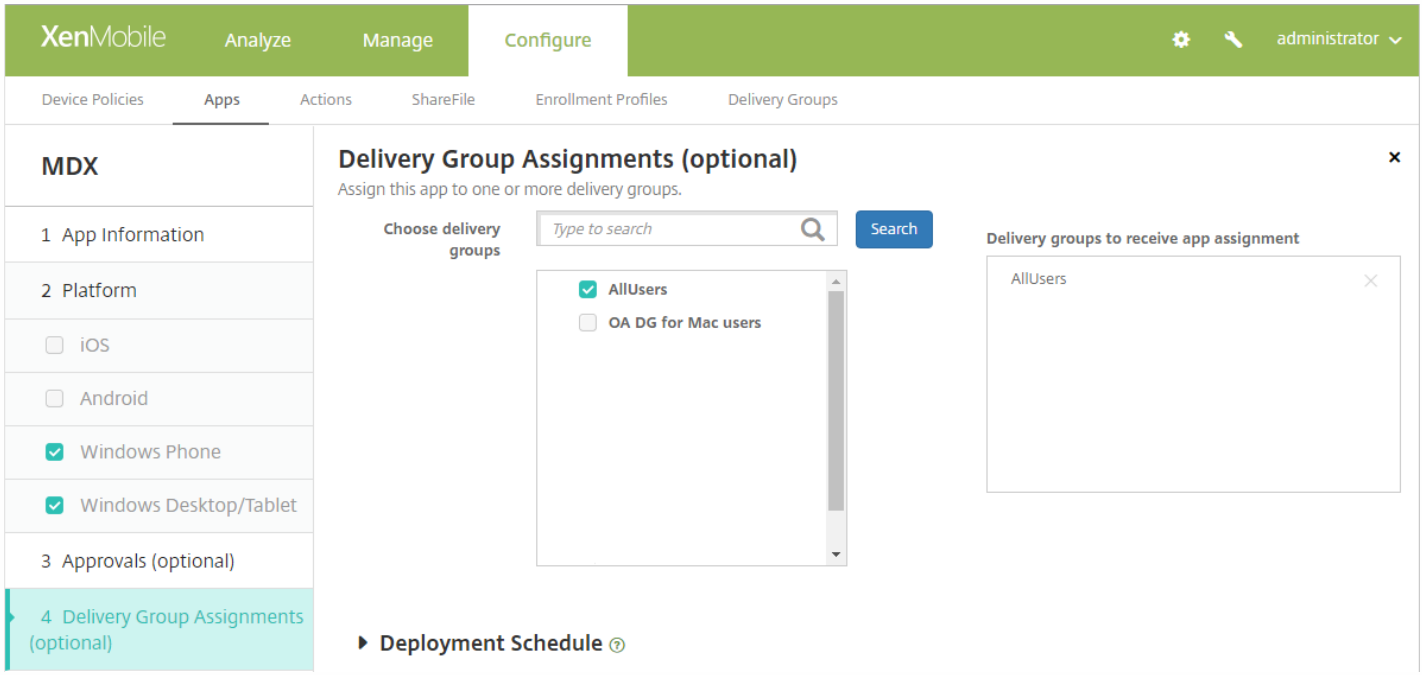
Wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist, verwenden Sie Workflows. Wenn Sie keine Genehmigungsworkflows einrichten müssen, fahren Sie mit Schritt 15 fort.

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. 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.

14. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.



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 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

17. Klicken Sie auf **Speichern**.

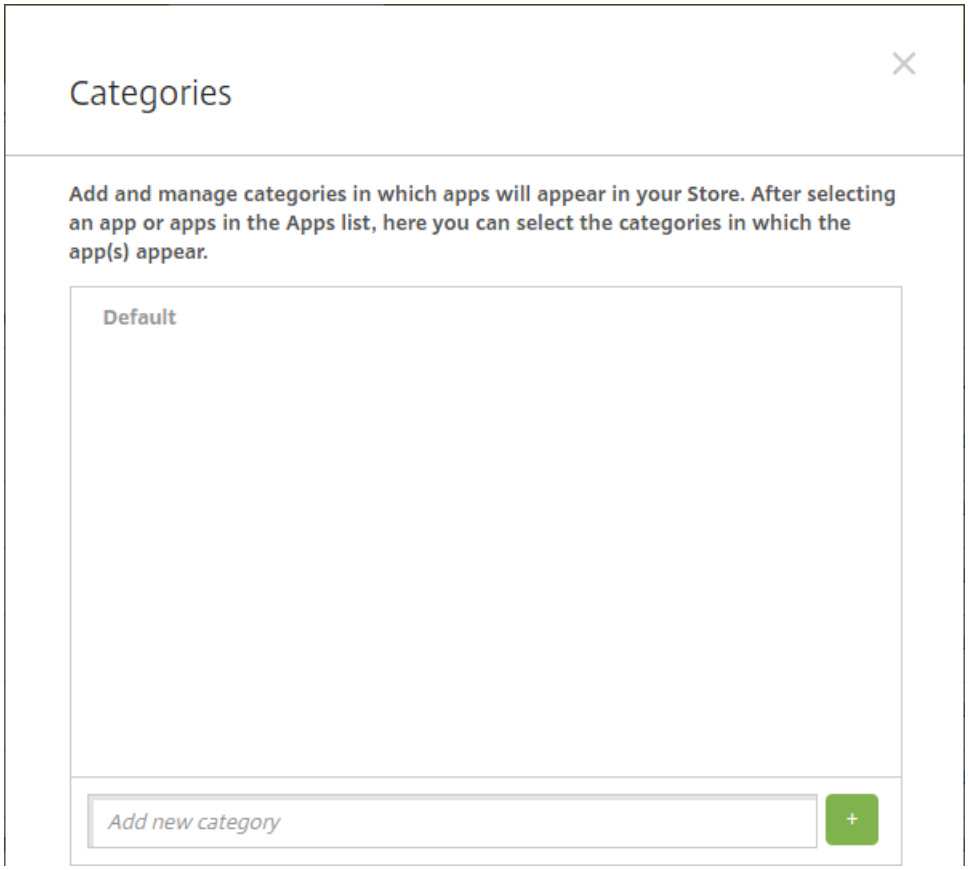
Erstellen von App-Kategorien

Wenn Benutzer sich bei Secure Hub anmelden, erhalten sie eine Liste der Apps, Weblinks und Stores, die Sie in XenMobile hinzugefügt und konfiguriert haben. Mit App-Kategorien können Sie dafür sorgen, dass Benutzer nur auf die von Ihnen vorgesehenen Apps, Weblinks oder Stores zugreifen können. Sie können beispielsweise eine Kategorie "Finanzen" erstellen und dann nur Apps hinzufügen, die für den Bereich Finanzen relevant sind. Ebenso können Sie eine Kategorie "Vertrieb" konfigurieren, der nur Apps für den Vertrieb zugewiesen werden.

Kategorien werden in XenMobile auf der Seite **Apps** konfiguriert. Wenn Sie eine App, einen Weblink oder einen Store hinzugefügt bzw. bearbeitet haben, können Sie diese(n) einer oder mehreren Kategorien zuweisen.

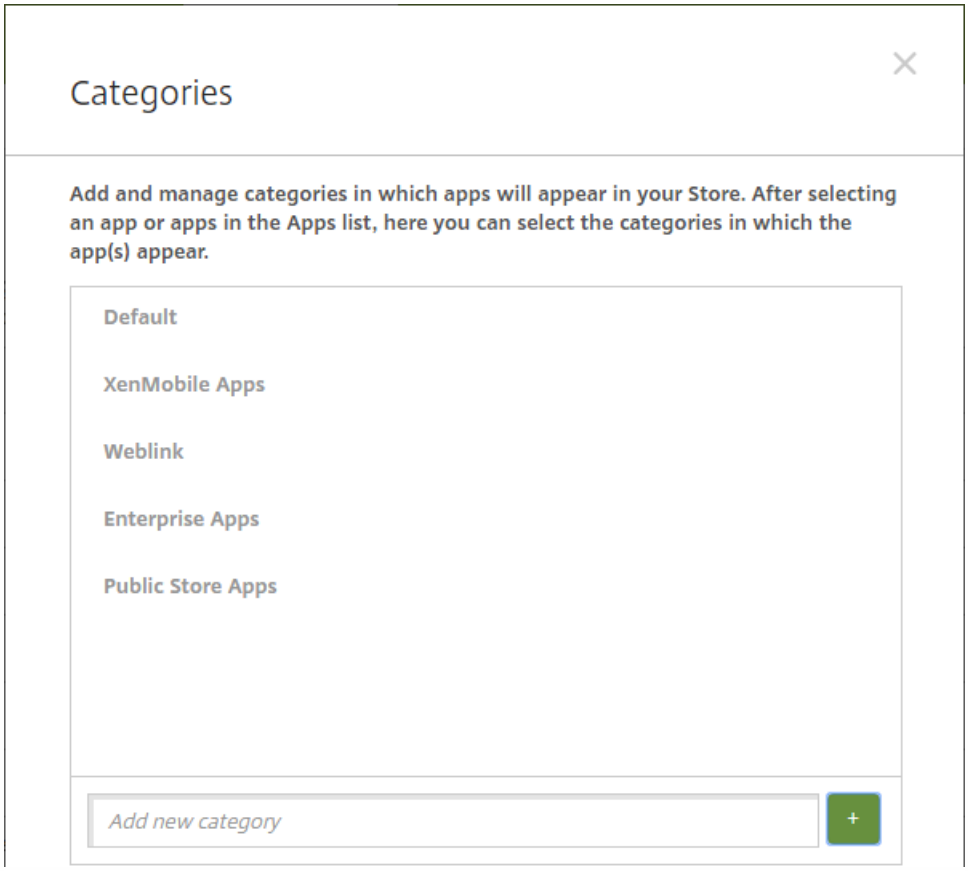
1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren** > **Apps**. Die Seite **Apps** wird angezeigt.

2. Klicken Sie auf **Kategorie**. Das Dialogfeld **Kategorien** wird angezeigt.



3. Führen Sie für jede Kategorie, die Sie hinzufügen möchten, folgende Schritte aus:

- Geben Sie einen Namen für die Kategorie, die Sie hinzufügen möchten, im Feld **Neue Kategorie hinzufügen** unten im Dialogfeld ein. Sie können beispielsweise Unternehmensapps eingeben, wenn Sie eine Kategorie für Unternehmensapps erstellen.
- Klicken Sie auf das Pluszeichen (+), um die Kategorie hinzuzufügen. Die neu erstellte Kategorie wird hinzugefügt und wird im Dialogfeld **Kategorien** angezeigt.



4. Wenn Sie alle Kategorien hinzugefügt haben, schließen Sie das Dialogfeld **Kategorien**.

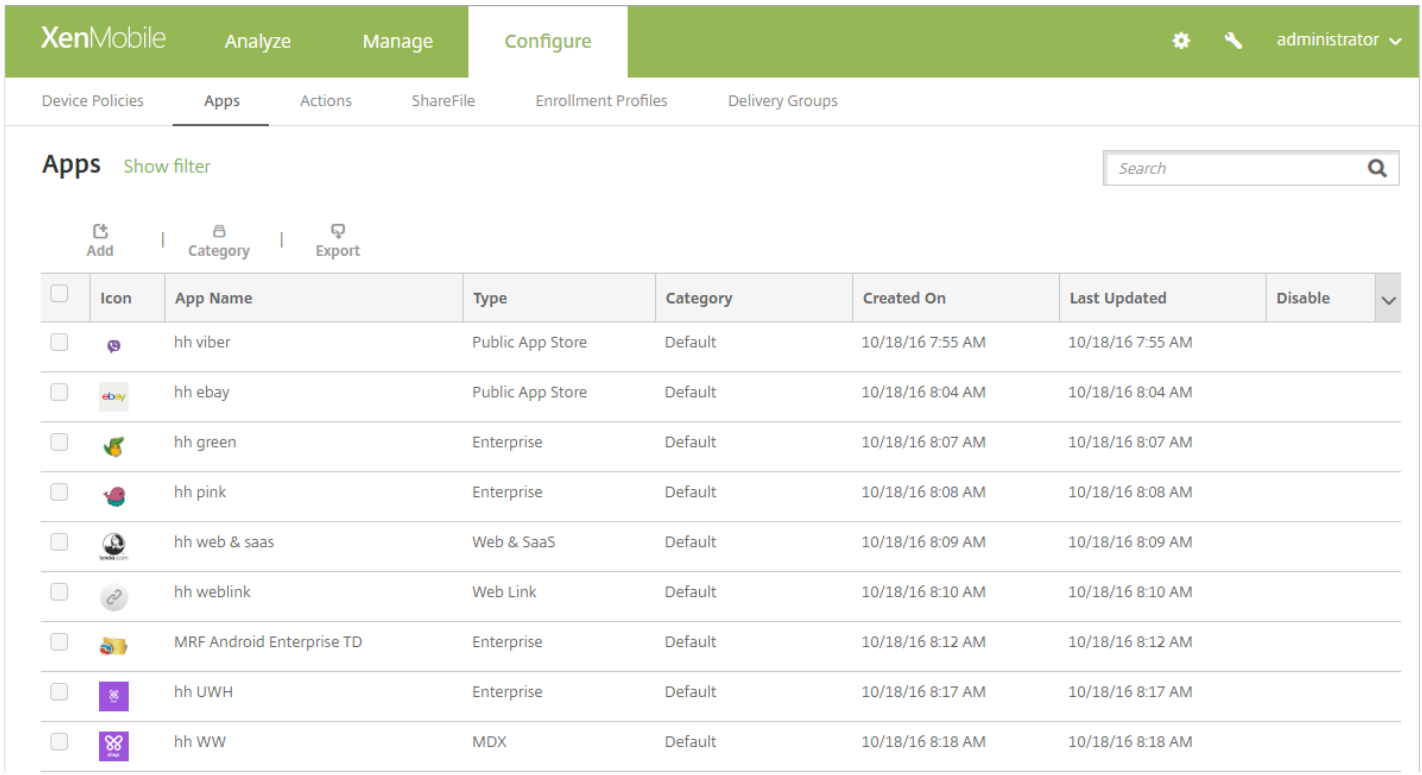
5. Auf der Seite **Apps** können Sie vorhandene Apps einer neuen Kategorie zuweisen.

- Wählen Sie die App aus, die Sie kategorisieren möchten.
- Klicken Sie auf **Bearbeiten**. Die Seite **App-Informationen** wird angezeigt.
- Wenden Sie die neue Kategorie an, indem Sie das zugehörige Kontrollkästchen in der Liste **App-Kategorie** aktivieren. Deaktivieren Sie die Kontrollkästchen aller Kategorien, die Sie der App nicht zuweisen möchten.
- Klicken Sie auf die Registerkarte **Zuweisungen für Bereitstellungsgruppen** oder auf allen folgenden Seiten auf **Weiter**, um durch die verbleibenden Seiten zur App-Einrichtung zu gehen.
- Klicken Sie auf der Seite **Zuweisungen für Bereitstellungsgruppen** auf **Speichern**, um die Kategorie anzuwenden. Die neue Kategorie wird auf die App angewendet und in der Tabelle **Apps** angezeigt.

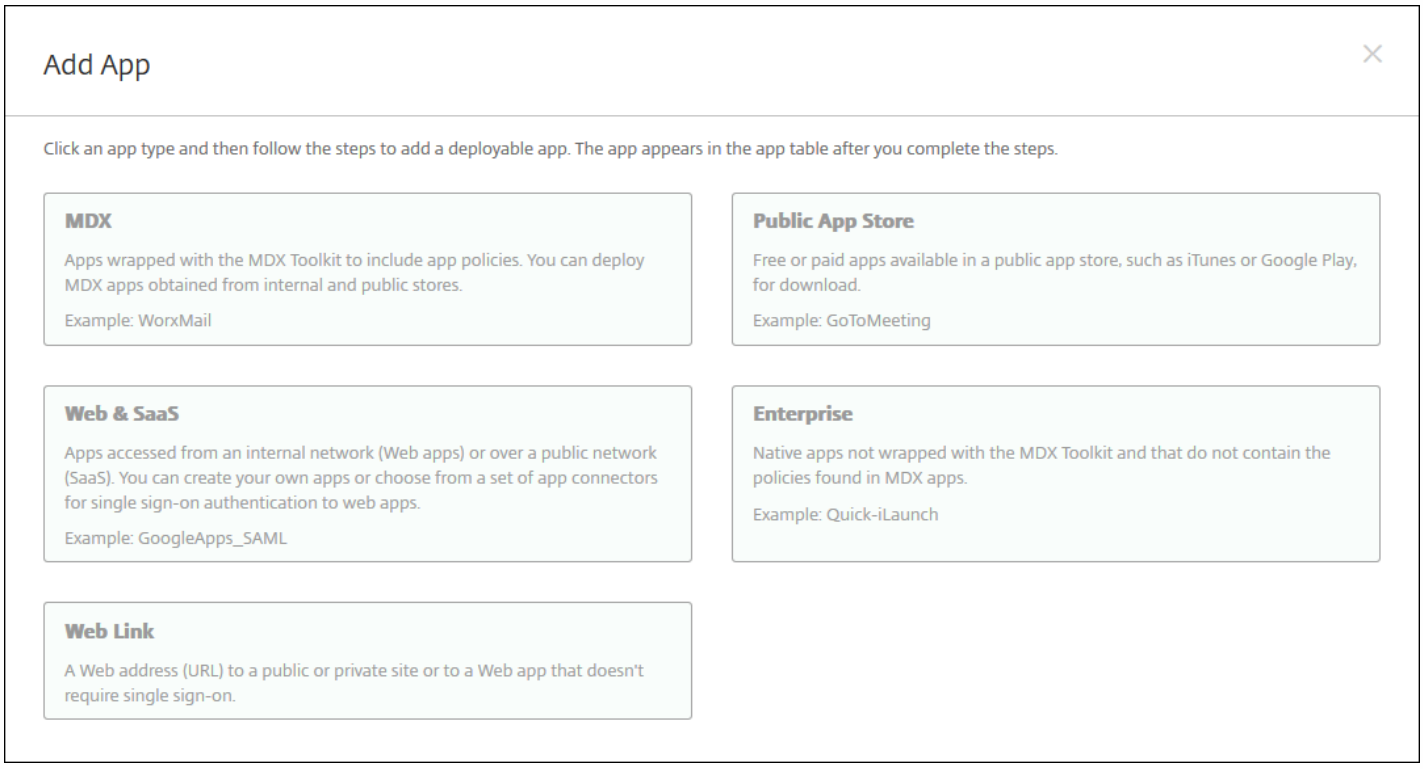
Hinzufügen von Apps aus einem öffentlichen App-Store

Sie können XenMobile kostenlose oder kostenpflichtige Apps, die in einem öffentlichen App Store (z. B. iTunes oder Google Play) verfügbar sind, hinzufügen. Beispiel: GoToMeeting. Wenn Sie 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. Das Massenkaufabonnement für Android for Work vereinfacht für eine Organisation das Finden, Kaufen und Bereitstellen von Apps und anderer Daten in großer Zahl.

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



2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



3. Klicken Sie auf **Öffentlicher App-Store**. Die Seite **App-Informationen** wird angezeigt.

4. Geben Sie auf der Seite **App-Informationenen** die folgenden Informationen ein:

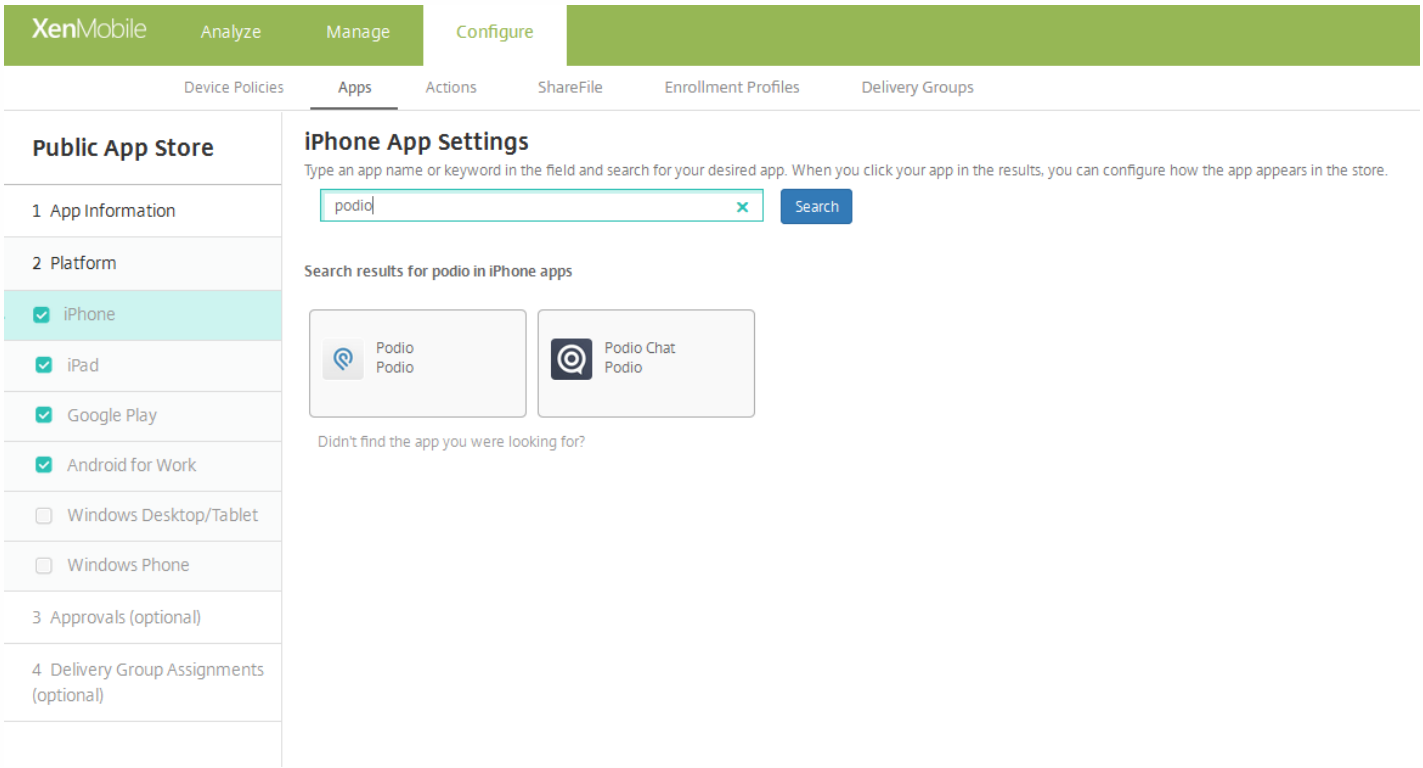
- **Name**: Geben Sie einen aussagekräftigen Namen für die App ein. Dieser Name wird in der Tabelle der Apps unter **App-Name** angezeigt.
- **Beschreibung**: Geben Sie optional eine Beschreibung der App ein.
- **App-Kategorie**: Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen möchten. Weitere Informationen über App-Kategorien finden Sie unter Erstellen von App-Kategorien.

5. Klicken Sie auf **Weiter**. Die Seite **Plattform** wird angezeigt.

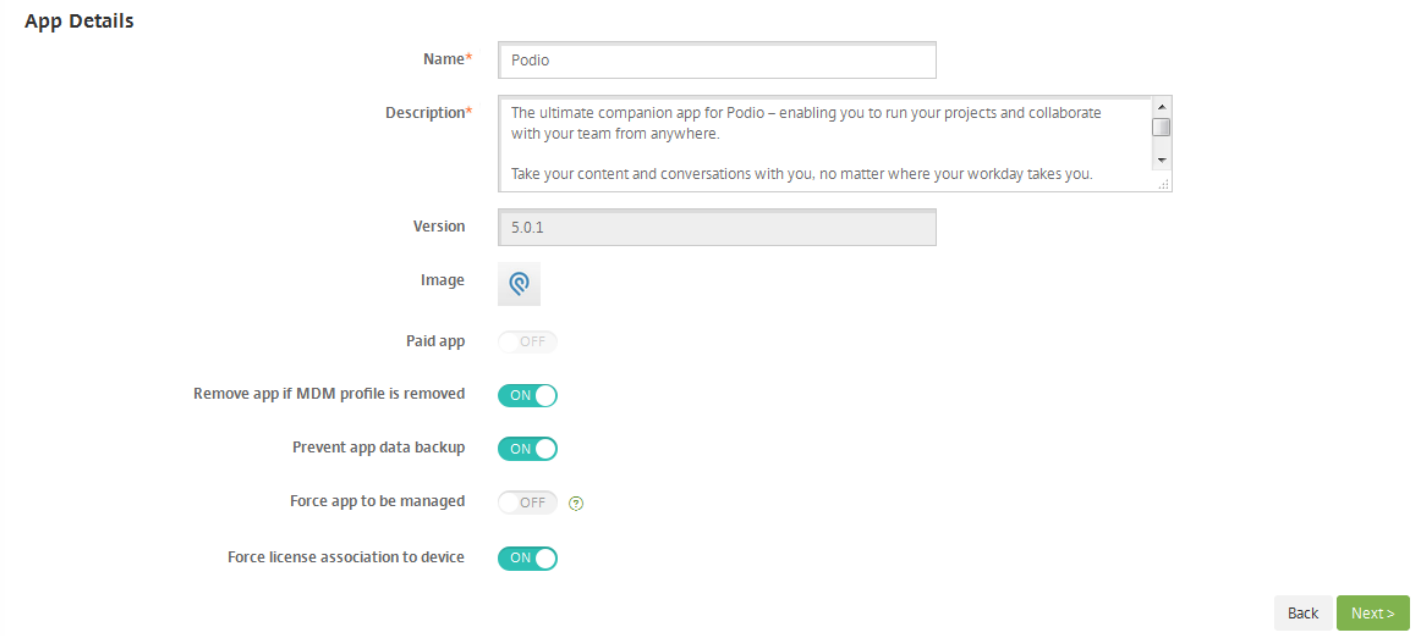
6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 10.

7. Geben Sie den Namen der App in das Suchfeld ein und klicken Sie auf **Suchen**. Es werden die Apps angezeigt, die den Suchkriterien entsprechen. Die folgende Abbildung zeigt das Ergebnis der Suche nach "podio".



8. Klicken Sie auf die gewünschte App. Die Felder im Bereich **App-Details** (Name, Beschreibung, Versionsnummer und zugeordnetes Bild) enthalten bereits Informationen zu der gewählten App.

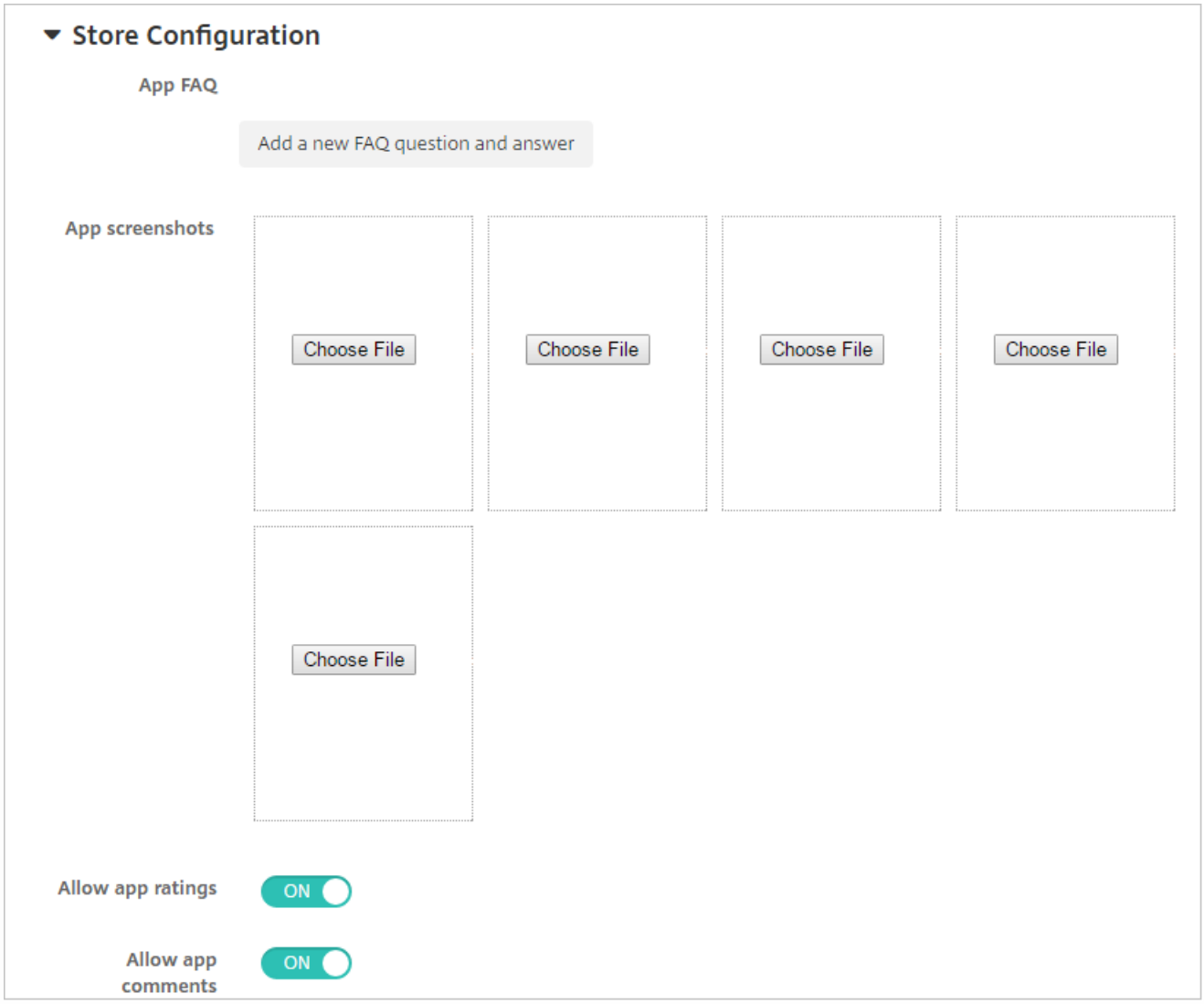


9. Konfigurieren Sie die folgenden Einstellungen:

- Falls erforderlich, ändern Sie Namen und Beschreibung der App.
- Das Feld **Kostenpflichtige App** ist vorkonfiguriert und kann nicht geändert werden.
- **App entfernen, wenn MDM-Profil entfernt wird**: Wählen Sie aus, ob die App entfernt werden soll, wenn das MDM-Profil entfernt wird. Der Standardwert ist **Ein**.
- **App-Datenbackup verhindern**: Wählen Sie aus, ob die App Daten sichern können soll. Der Standardwert ist **Ein**.
- **Verwaltung der App erzwingen**: Wählen Sie aus, ob Benutzer bei Installation der App als nicht verwaltet aufgefordert werden, die Verwaltung der App auf nicht betreuten Geräten zuzulassen. Der Standardwert ist **AUS**. Verfügbar in iOS 9.0 und höher.
- **Lizenzzuordnung zu Gerät erzwingen**: Wählen Sie aus, ob Apps, die mit aktivierter Gerätezuordnung entwickelt wurden, Geräten statt Benutzern zugewiesen werden sollen. Verfügbar in iOS 9 und höher. Wenn die App keine Zuweisung zu Geräten unterstützt, kann dieses Feld nicht geändert werden.

10. Konfigurieren Sie die Bereitstellungsregeln.

11. Erweitern Sie **XenMobile Store-Konfiguration**.

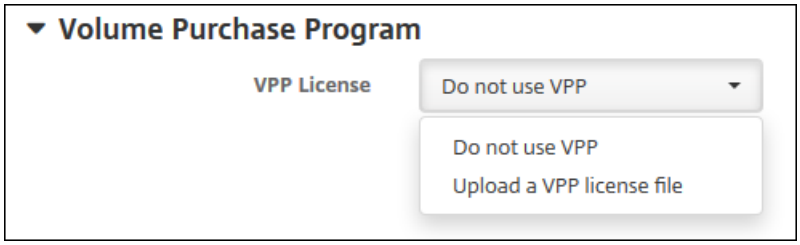


Sie können optional FAQ oder Screenshots für die App zur Anzeige im XenMobile Store hinzufügen. Sie können außerdem festlegen, ob Benutzer die App bewerten oder kommentieren können.

- 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 XenMobile 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. Der Standardwert ist "ON".
  - **App-Kommentare zulassen**: Wählen Sie aus, ob eine Kommentierung der App durch die Benutzer zugelassen werden soll.

12. Erweitern Sie **Programm für Volumenlizenzen (VPP)** oder **Massenkauf** bei Android for Work.

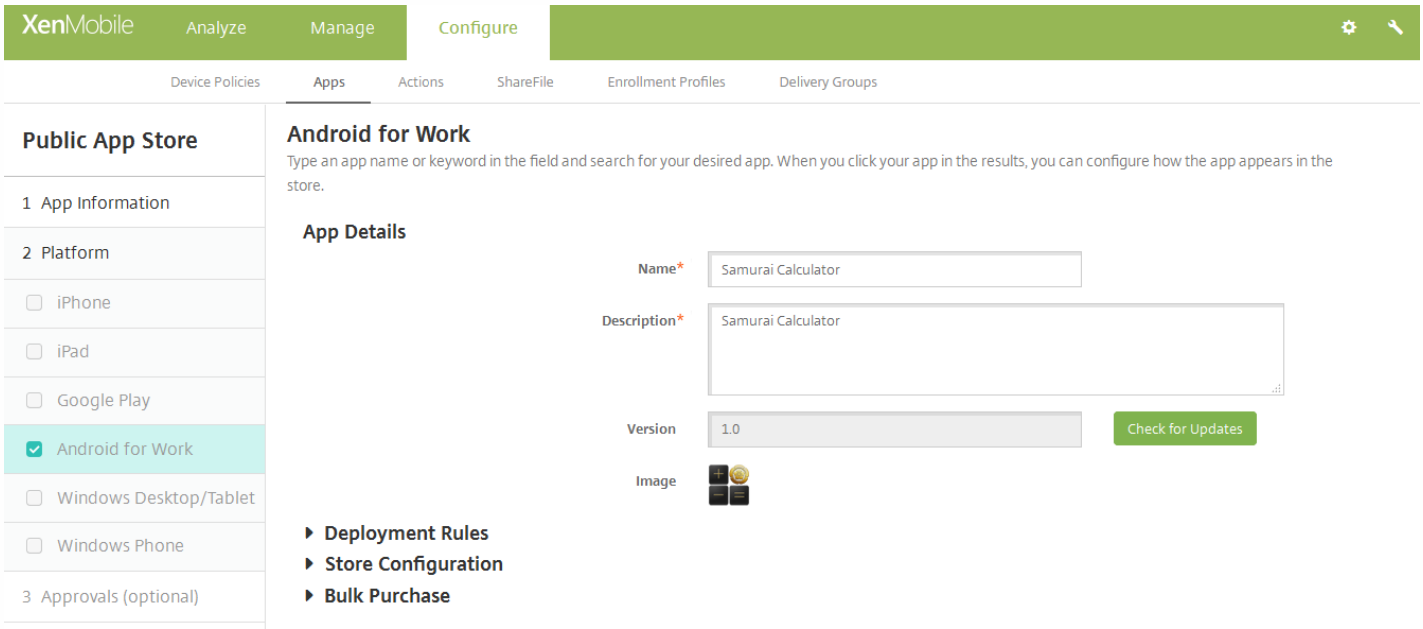
Führen Sie für das Programm für Volumenlizenzen (VPP) die folgenden Schritte aus.



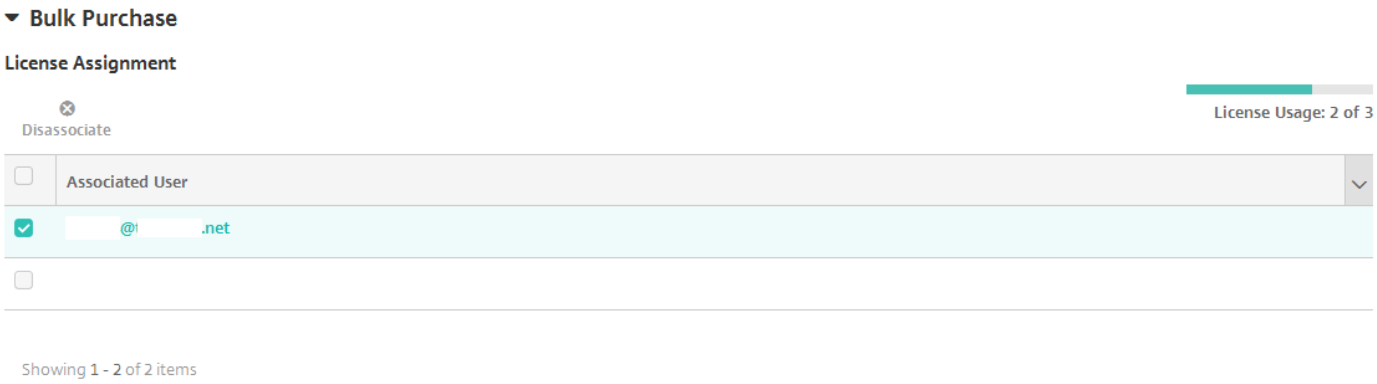
a. Klicken Sie in der Liste **VPP-Lizenz** auf **VPP-Lizenzdatei hochladen**, wenn XenMobile auf die App eine VPP-Lizenz anwenden können soll.

b. Importieren Sie die Lizenz über das angezeigte Dialogfeld.

Für einen Massenkauf für Android for Work erweitern Sie den Bereich **Massenkauf**.



In der Tabelle für die Lizenzzuweisung sehen Sie, wie viele der verfügbaren Lizenzen für die App verwendet werden. 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.



13. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.

Wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist, verwenden Sie Workflows. Wenn Sie keine Genehmigungsworkflows einrichten müssen, fahren Sie mit dem nächsten Schritt fort.

Konfigurieren Sie folgende Einstellungen, 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.

14. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.

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 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

17. Klicken Sie auf **Speichern**.

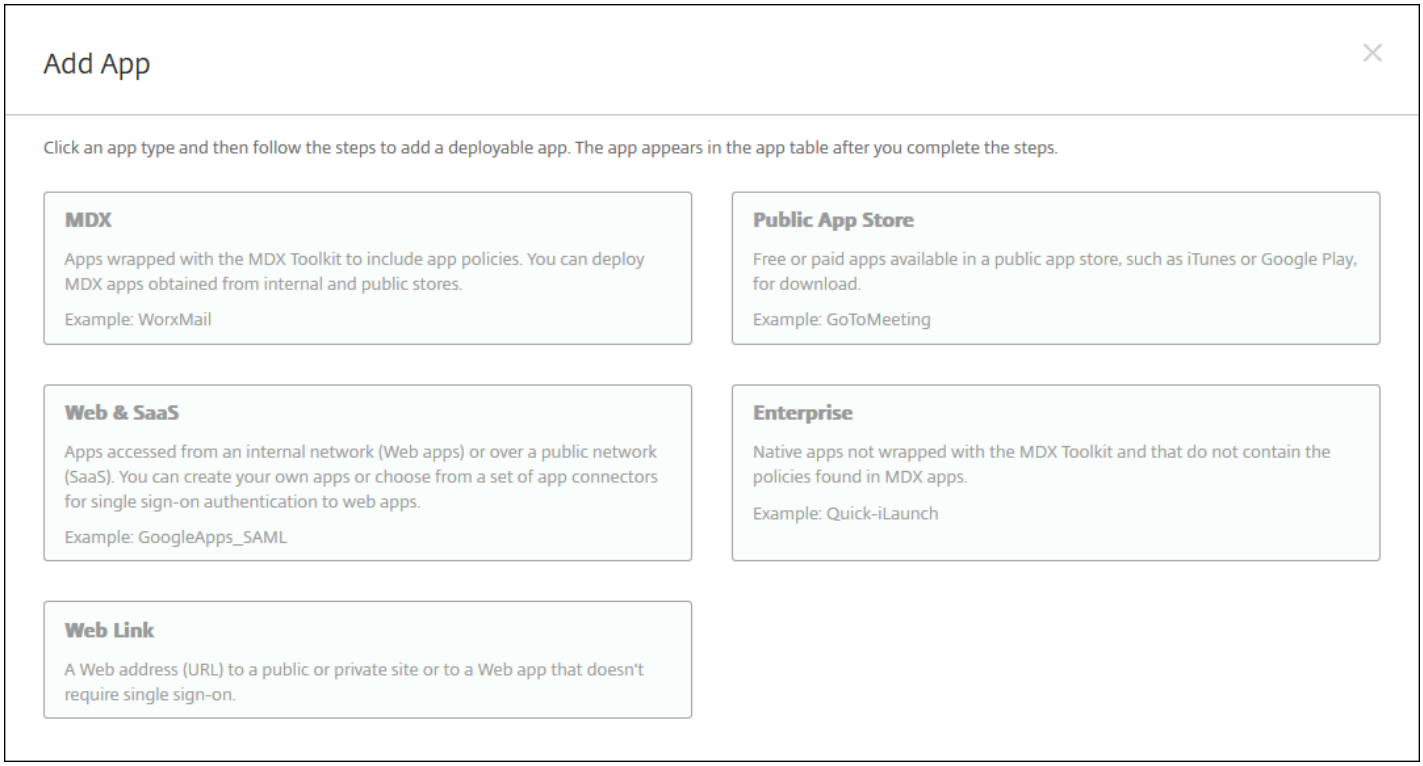
Hinzufügen von Web- und SaaS-Apps

Mit der XenMobile-Konsole können Sie Benutzern SSO-Zugriff (Single Sign-On) auf Mobil-, Unternehmens-, Web- und SaaS-Apps gewähren. Zur Aktivierung von Apps für SSO können Sie Vorlagen für Anwendungsconnectors verwenden. Eine Liste der in XenMobile verfügbaren Connectortypen finden Sie unter Anwendungsconnectortypen. Sie können beim Hinzufügen einer Web- oder SaaS-App auch einen eigenen Connector erstellen.

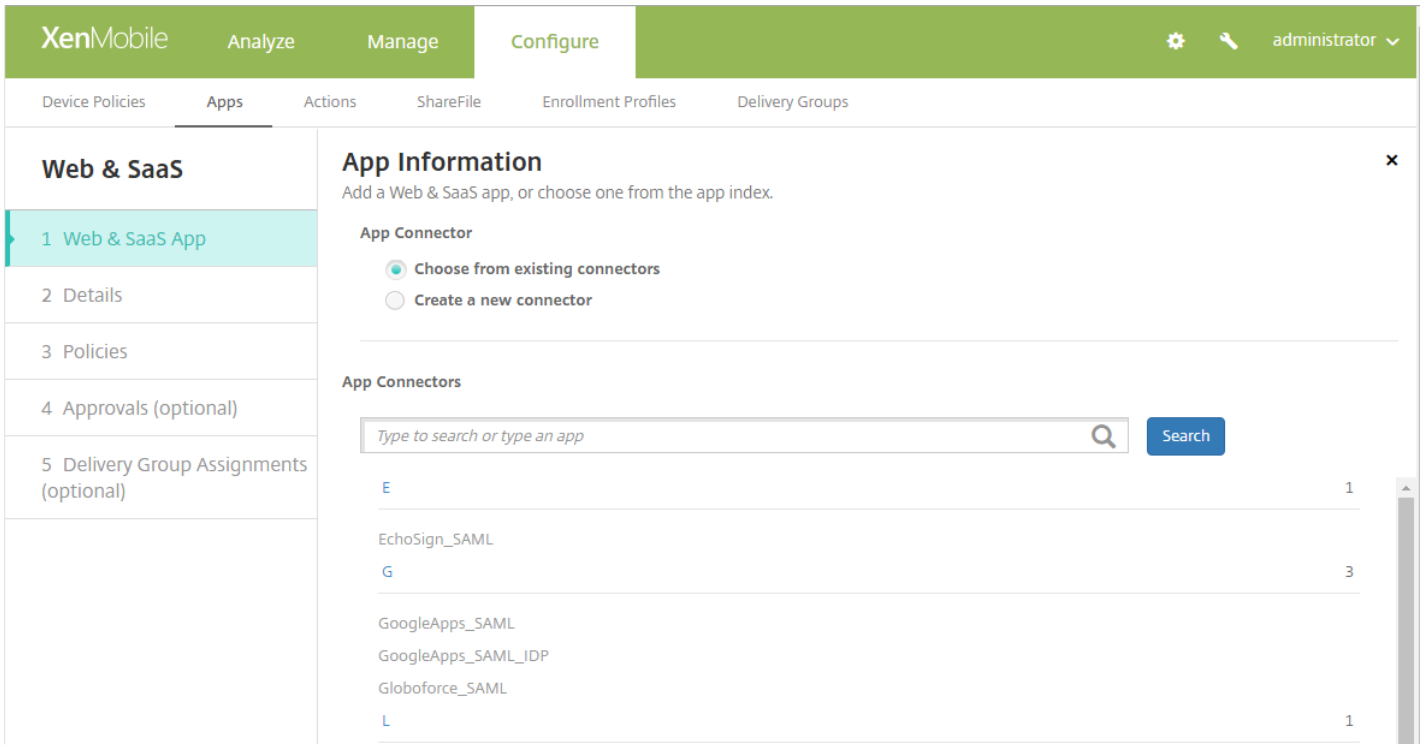
Wenn eine App nur für SSO verfügbar ist, speichern Sie nach der oben beschriebenen Konfiguration die Einstellungen. Die App wird dann auf der Registerkarte **Apps** in der XenMobile-Konsole angezeigt.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren** > **Apps**. Die Seite **Apps** wird geöffnet.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



3. Klicken Sie auf **Web & SaaS**. Die Seite **App-Informationen** wird angezeigt.



4. Konfigurieren Sie, wie nachfolgend beschrieben, einen vorhandenen oder neuen App-Connector.

Konfigurieren eines vorhandenen App-Connectors

Auf der Seite **App-Informationen** ist **Vorhandenen Connector wählen** bereits ausgewählt (siehe Abbildung oben). Klicken Sie in der Liste **App-Connectors** auf den gewünschten Connector. Die Informationen zu dem App-Connector werden angezeigt.

Konfigurieren Sie folgende Einstellungen:

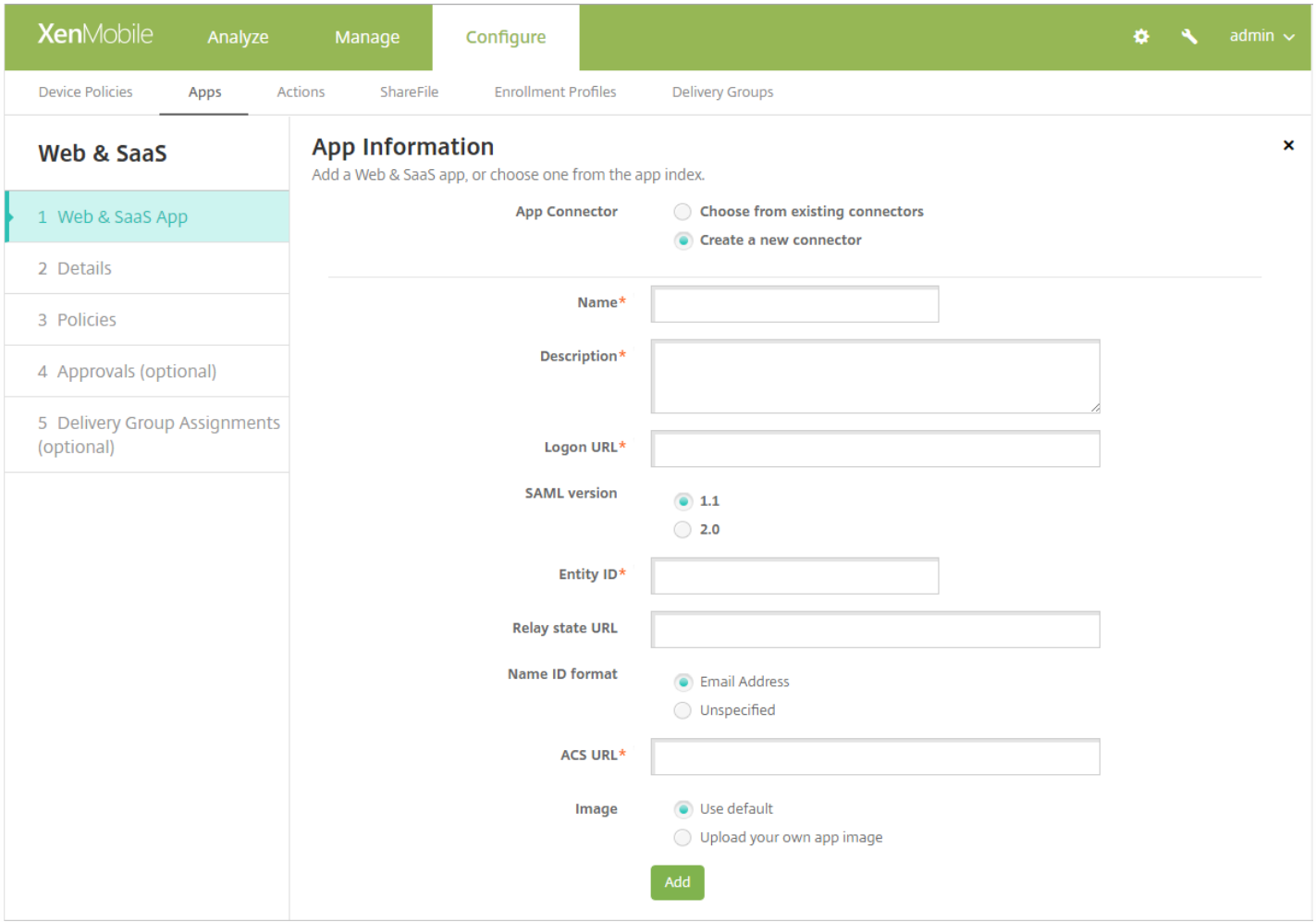
- **App-Name**: Übernehmen Sie den Standardnamen oder geben Sie einen neuen Namen ein.
- **App-Beschreibung**: Übernehmen Sie die Standardbeschreibung oder geben Sie eine eigene Beschreibung ein.
- **URL**: Übernehmen Sie die Standard-URL oder geben Sie die Webadresse für die App ein. Je nach ausgewähltem Connector enthält dieses Feld eventuell einen Platzhalter, den Sie ersetzen müssen, bevor Sie mit der nächsten Seite fortfahren können.
- **Domänenname**: Geben Sie ggf. den Domänennamen der App ein. Diese Angabe ist erforderlich.
- **App wird im internen Netzwerk gehostet**: Klicken Sie auf Ein, wenn die App auf einem Server im internen Netzwerk ausgeführt wird. Wenn Benutzer von einem Remotestandort aus eine Verbindung mit der internen Anwendung herstellen, muss dies über NetScaler Gateway erfolgen. Wenn Sie diese Option auf **ON** festlegen, wird das VPN-Schlüsselwort der App hinzugefügt, sodass Benutzer eine Verbindung über NetScaler Gateway herstellen können. Der Standardwert ist **AUS**.
- **App-Kategorie**: Klicken Sie optional in der Liste auf eine Kategorie, der Sie die App zuweisen möchten.
- **Benutzerkontoprovisioning**: Wählen Sie aus, ob für die App Benutzerkonten erstellt werden sollen. Wenn Sie den Globoforce_SAML-Connector verwenden, müssen Sie diese Option aktivieren, um eine nahtlose SSO-Integration zu

gewährleisten.

- Wenn Sie **Benutzerkontoprovisioning** aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **Dienstkonto**
    - **Benutzername**: Geben Sie den Namen des App-Administrators ein. Diese Angabe ist erforderlich.
    - **Kennwort** Geben Sie das Kennwort des App-Administrators ein. Diese Angabe ist erforderlich.
  - **Benutzerkonto**
    - **Nach Ende des Benutzeranspruchs**: Klicken Sie auf die Aktion, die ausgeführt werden soll, wenn Benutzer keinen Zugriff auf die App mehr haben. Der Standardwert ist Konto deaktivieren. Mögliche Optionen:
      - Konto deaktivieren
      - Konto beibehalten
      - Konto entfernen
  - **Benutzernamenregel**
    - Führen für jede Benutzernamenregel, die Sie hinzufügen möchten, folgende Schritte aus:
      - **Benutzerattribute**: Klicken Sie auf die Benutzerattribute, die Sie der Regel hinzufügen möchten.
      - **Länge (Zeichen)**: Geben Sie die Anzahl der Zeichen des Benutzerattributs ein, die im Benutzernamen verwendet werden sollen. Die Standardeinstellung ist **Alle**.
      - **Regel**: Jedes hinzugefügte Benutzerattribut wird automatisch an die Benutzernamenregel angehängt.
- **Kennwortanforderung**
  - **Länge**: Geben Sie die Mindestlänge des Kennworts ein. Der Standardwert ist **8**.
- **Kennwortablauf**
  - **Gültigkeit (Tage)** Geben Sie die Anzahl Tage ein, die das Kennwort gültig sein soll. Gültige Werte sind **0–90**. Der Standardwert ist 90.
  - **Kennwort nach Ablauf automatisch zurücksetzen**: Wählen Sie aus, ob Kennwörter nach Ablauf automatisch zurückgesetzt werden sollen. Der Standardwert ist **AUS**. Wenn Sie diese Option nicht aktivieren, können die Benutzer die App nicht mehr öffnen, wenn ihr Kennwort abgelaufen ist.

Konfigurieren eines neuen App-Connectors

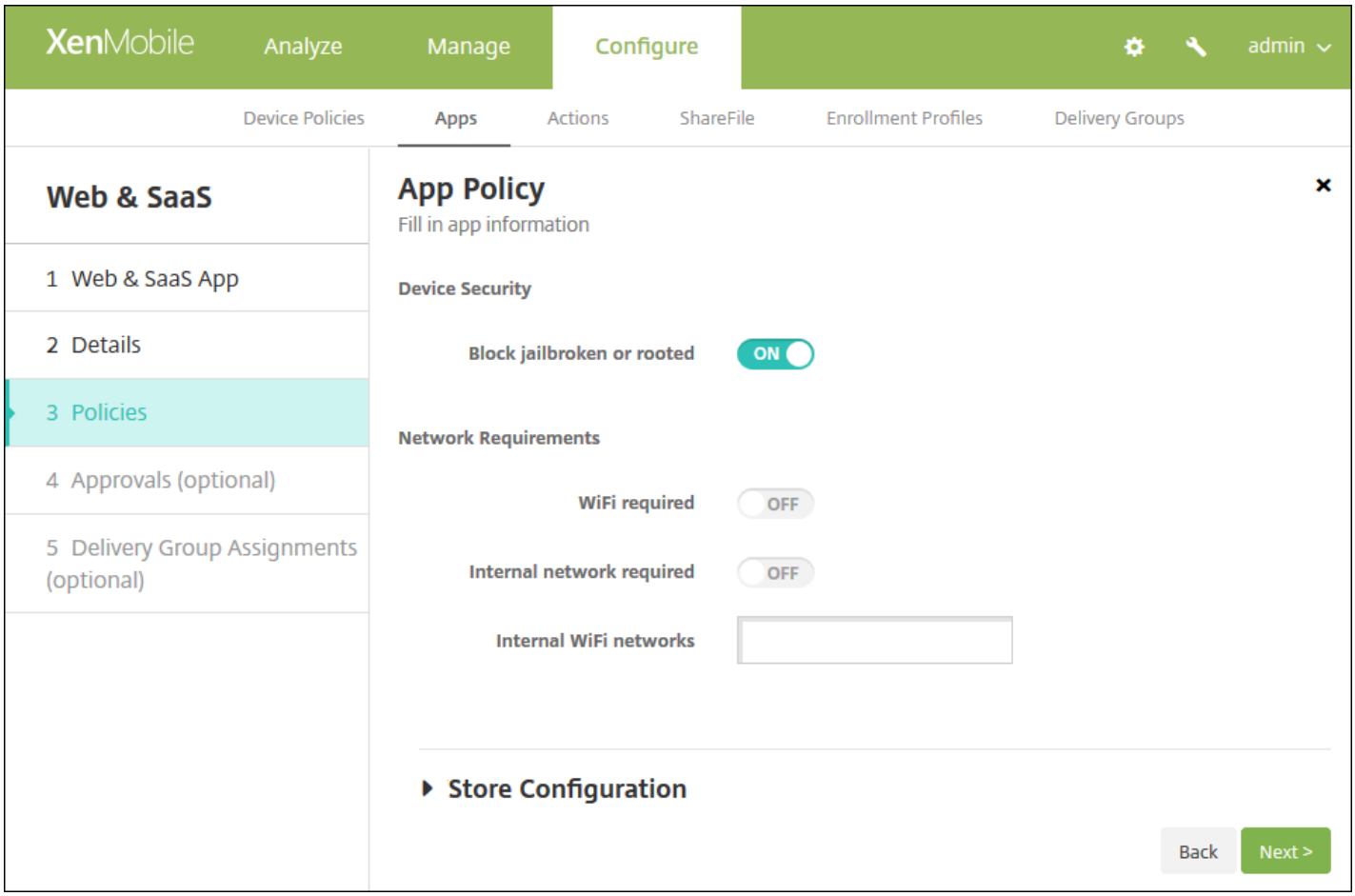
Klicken Sie auf der Seite **App-Informationen** auf **Neuen Connector erstellen**. Die Felder zu dem App-Connector werden angezeigt.



Konfigurieren Sie folgende Einstellungen:

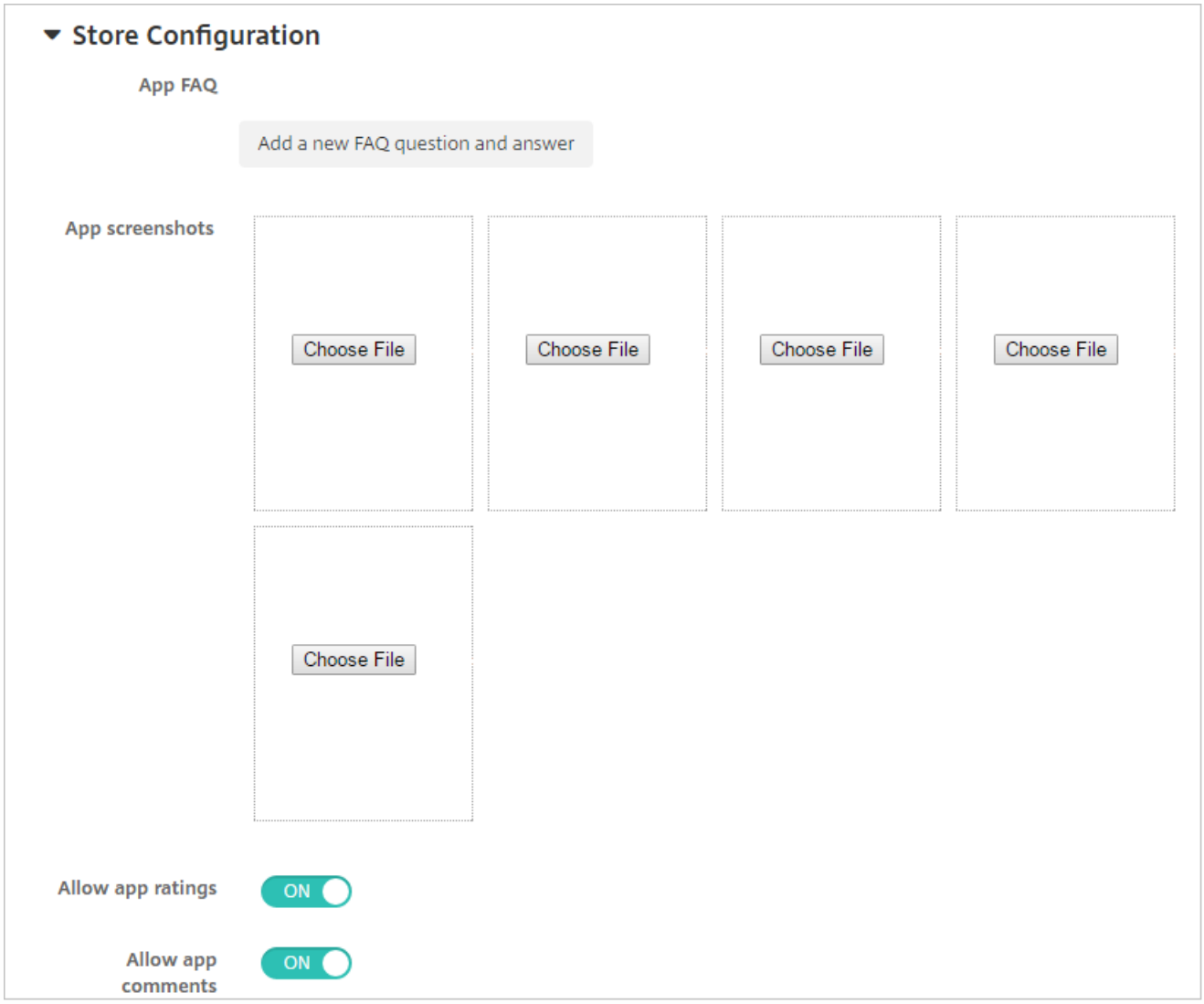
- **Name**: Geben Sie einen Namen für den Connector ein. Diese Angabe ist erforderlich.
- **Beschreibung:** Geben Sie eine Beschreibung für den Connector ein. Diese Angabe ist erforderlich.
- **Anmelde-URL**: Geben Sie die URL für die Anmeldung der Benutzer bei der Website ein, bzw. kopieren Sie die URL und fügen Sie sie hier ein. Wenn die App, die Sie hinzufügen möchten, beispielsweise eine Anmeldeseite hat, öffnen Sie einen Webbrowser und gehen Sie zu der Anmeldeseite. Beispiel: http://www.example.com/logon. Diese Angabe ist erforderlich.
- **SAML-Version**: Wählen Sie **1.1** oder **2.0** aus. Der Standardwert ist **1.1**.
- **Entitäts-ID**: Geben Sie die Identität für die SAML-Anwendung ein.
- **Relayzustands-URL**: Geben Sie die Webadresse für die SAML-Anwendung ein. Der Wert unter "Relayzustands-URL" ist die Antwort-URL der App.
- **Namens-ID-Format**: Wählen Sie **E-Mail-Adresse** oder **Keine Angabe** aus. Die Standardeinstellung ist **E-Mail-Adresse**.
- **ACS-URL**: Geben Sie die URL für den Assertion Consumer Service des Identitätsanbieters oder Dienstanbieters ein. Die ACS-URL ermöglicht das Single Sign-On für Benutzer.
- **Bild**: Geben Sie an, ob Sie das Citrix Standardbild verwenden oder ein eigenes App-Bild hochladen möchten. Der Standardwert ist "Standard verwenden".
  - Wenn Sie ein Bild hochladen möchten, klicken Sie auf **Durchsuchen**, navigieren Sie zu dem Speicherort der Bilddatei und wählen Sie diese aus. Die Datei muss das Format .png haben, JPEG- und GIF-Dateien können nicht hochgeladen werden. Eine benutzerdefinierte Grafik kann später nicht mehr geändert werden.
  - Wenn Sie fertig sind, klicken Sie auf **Hinzufügen**. Die Seite **Details** wird angezeigt.

5. Klicken Sie auf **Weiter**. Die Seite **App-Richtlinie** wird angezeigt.



- Konfigurieren Sie folgende Einstellungen:
  - **Gerätesicherheit**
    - **Mit Jailbreak oder Root blockieren**: Wählen Sie aus, ob Geräte mit Jailbreak und gerootete Geräte vom Zugriff auf die App ausgeschlossen werden sollen. Der Standardwert ist **Ein**.
  - **Netzwerkanforderungen**
    - **WiFi erforderlich**: Wählen Sie aus, ob zum Ausführen der App eine WiFi-Verbindung erforderlich sein soll. Der Standardwert ist **AUS**.
    - **Internes Netzwerk erforderlich**: Wählen Sie aus, ob zum Ausführen der App ein internes Netzwerk erforderlich sein soll. Der Standardwert ist **AUS**.
    - **Interne WiFi-Netzwerke**: Wenn Sie "WiFi erforderlich" aktiviert haben, geben Sie hier die internen WiFi-Netzwerke an, die verwendet werden sollen.

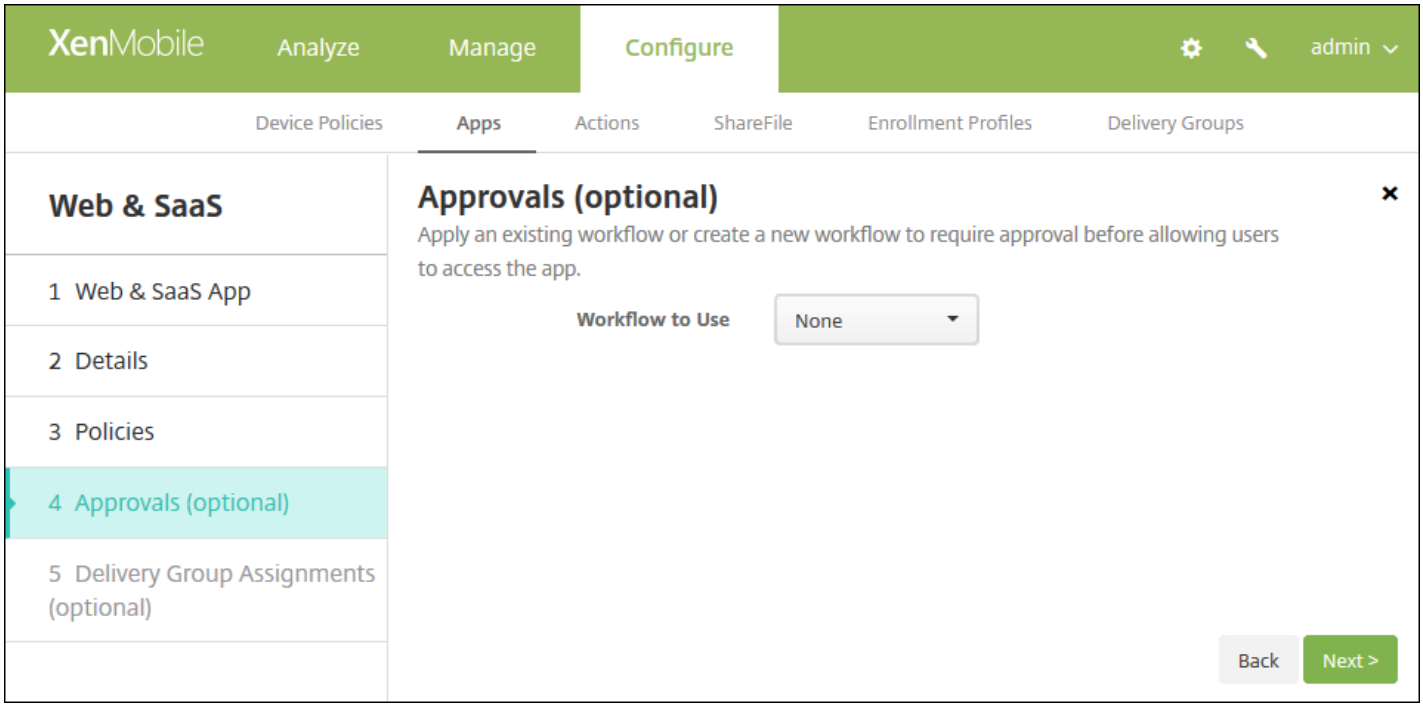
6. Erweitern Sie **XenMobile Store-Konfiguration**.



Sie können optional FAQ oder Screenshots für die App zur Anzeige im XenMobile 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 XenMobile 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. Der Standardwert ist **EIN**.
  - **App-Kommentare zulassen**: Wählen Sie aus, ob eine Kommentierung der App durch die Benutzer zugelassen werden soll. Der Standardwert ist **EIN**.

7. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.



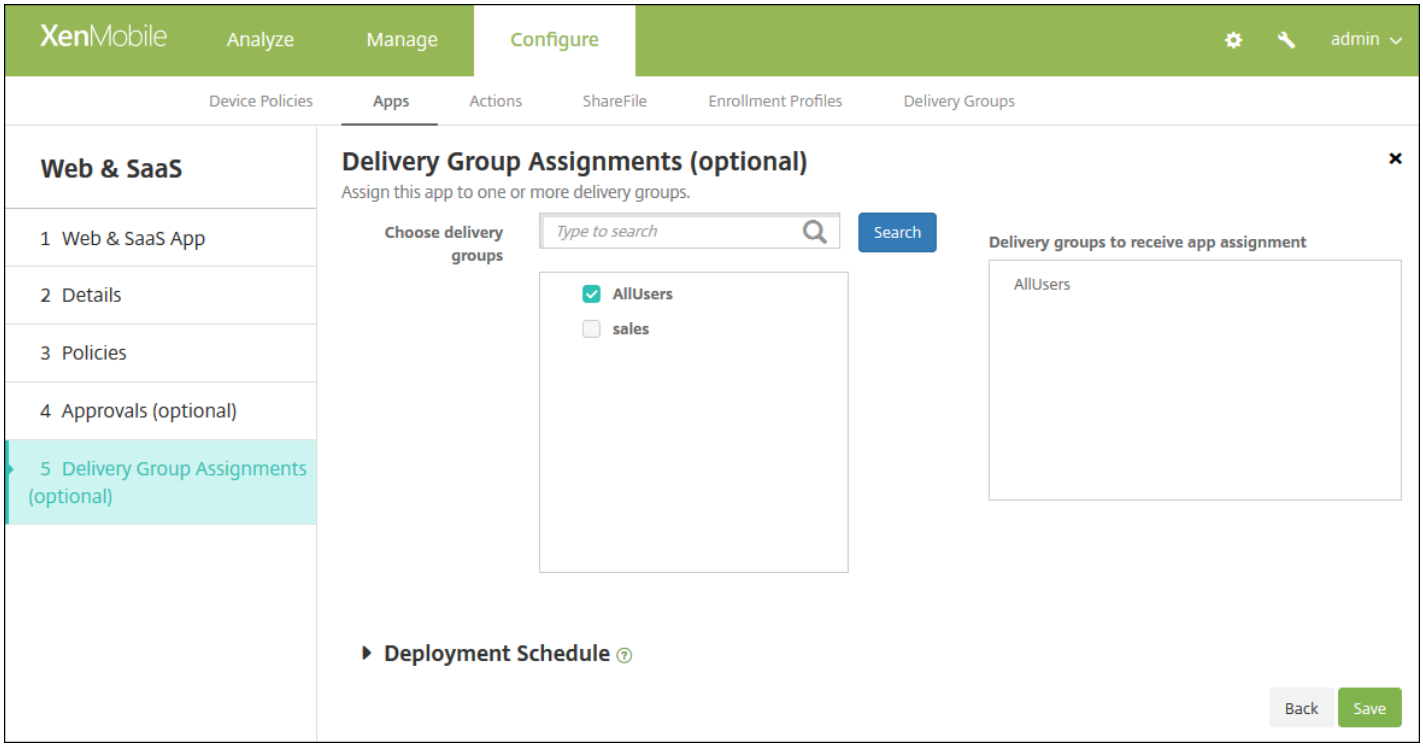
Wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist, verwenden Sie Workflows. Wenn Sie keine Genehmigungsworkflows einrichten müssen, fahren Sie mit Schritt 8 fort.

Konfigurieren Sie folgende Einstellungen, 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.

8. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** 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 "always-on" ist für iOS-Geräte nicht verfügbar.

- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

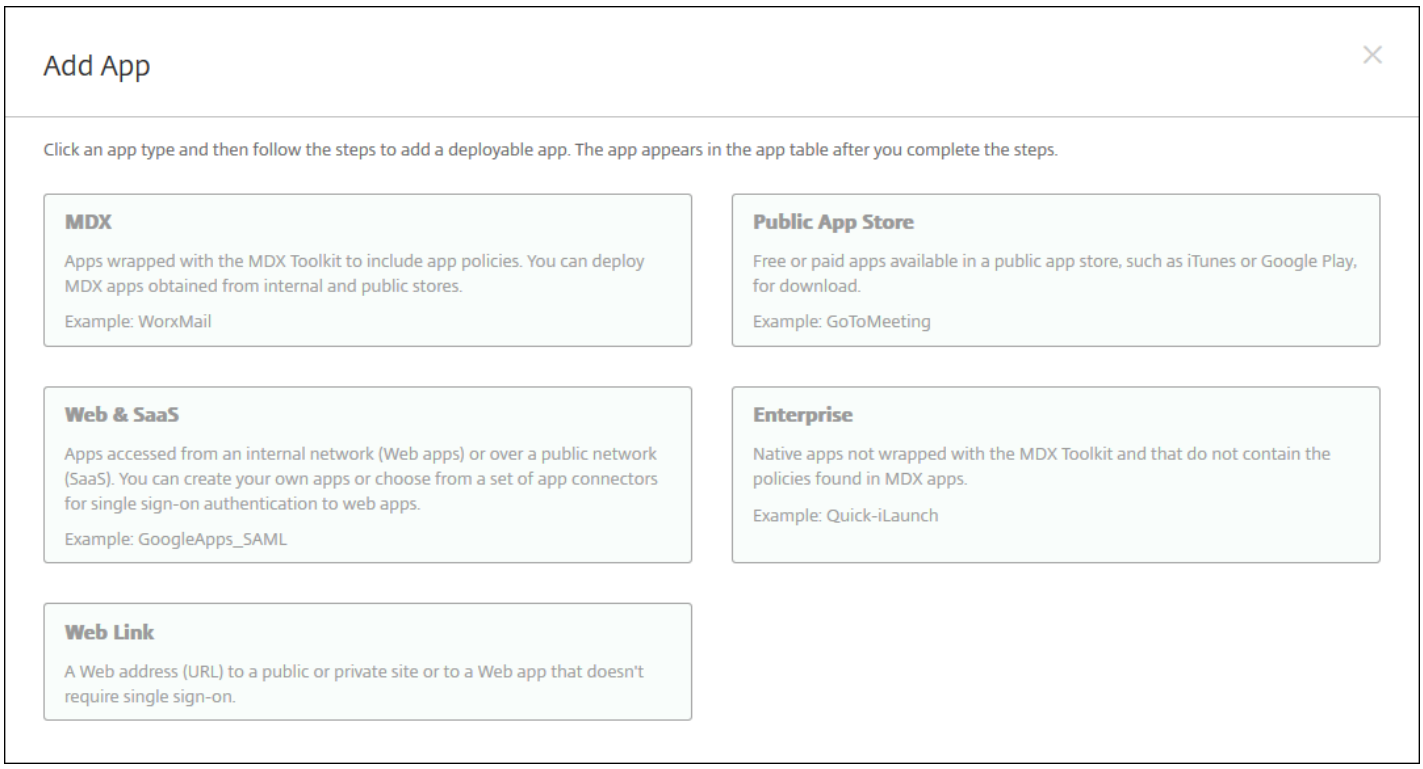
Hinzufügen von Unternehmensapps

Unternehmensapps in XenMobile sind native Apps, die nicht mit dem MDX Toolkit umschlossen wurden und nicht die Richtlinien für MDX-Apps enthalten. Sie können Unternehmensapps mit der Registerkarte **Apps** der XenMobile-Konsole hochladen. Unternehmensapps unterstützen folgende Plattformen (und die entsprechenden Dateitypen):

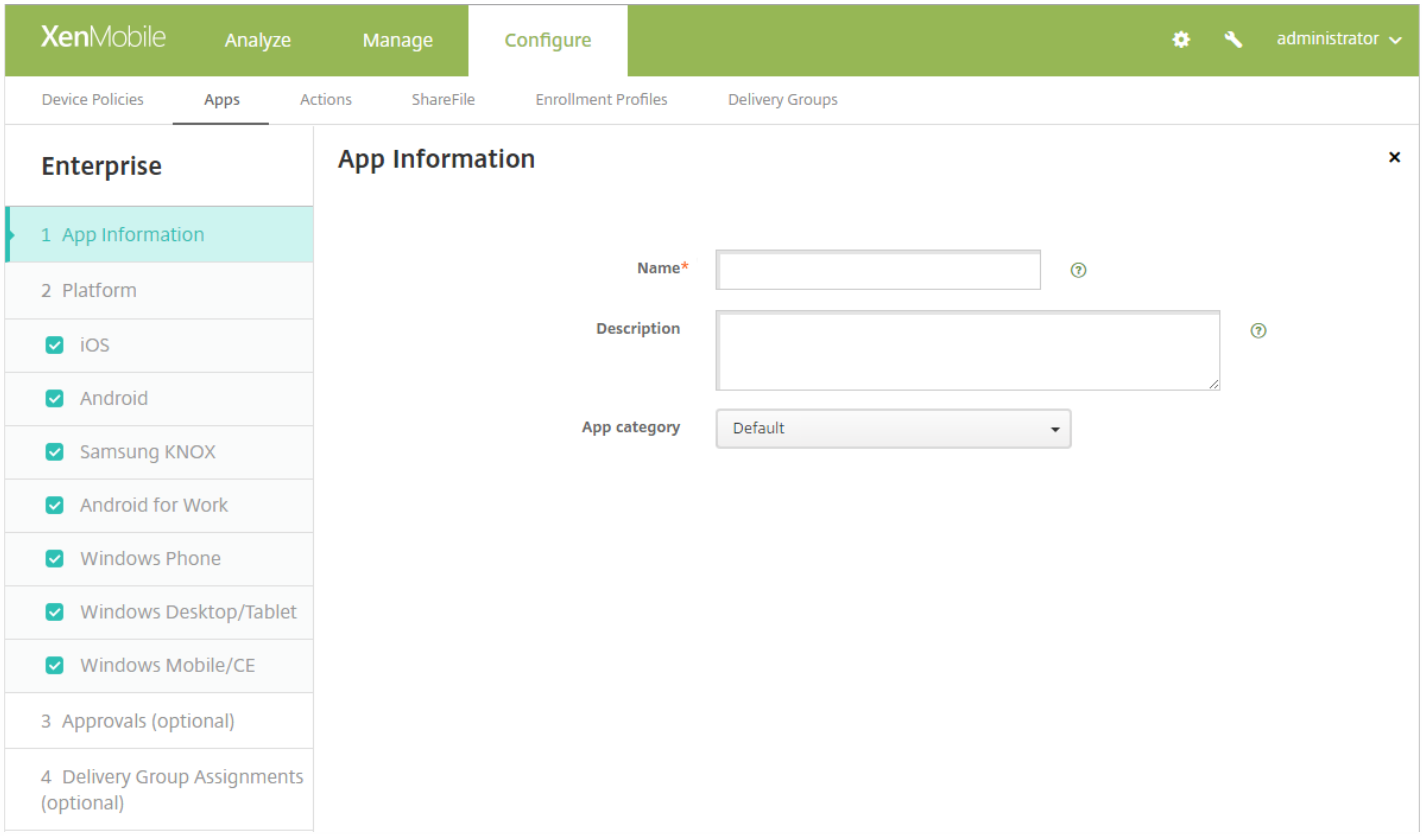
- iOS (.ipa)
- Android (.apk)
- Samsung KNOX (.apk)
- Android for Work (.apk)
- Windows Phone (.xap oder .appx)
- Windows Tablet (.appx)
- Windows Mobile/CE (.cab)

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren** > **Apps**. Die Seite **Apps** wird geöffnet.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



3. Klicken Sie auf **Enterprise**. Die Seite **App-Informationen** wird angezeigt.



4. Geben Sie auf der Seite **App-Informationenen** die folgenden Informationen ein:

- **Name**: Geben Sie einen aussagekräftigen Namen für die App ein. Dieser Name wird in der Tabelle der Apps unter "App-Name" angezeigt.
- **Beschreibung**: Geben Sie optional eine Beschreibung der App ein.
- **App-Kategorie**: Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen möchten. Weitere Informationen über App-Kategorien finden Sie unter Erstellen von App-Kategorien in XenMobile.

5. Klicken Sie auf **Weiter**. Die Seite **Plattform** 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 10.

7. Klicken Sie für jede ausgewählte Plattform auf **Durchsuchen**, navigieren Sie zum Speicherort der zu importierenden Datei und wählen Sie diese aus.

8. Klicken Sie auf **Weiter**. Die Seite mit den App-Informationen für die Plattform wird angezeigt.

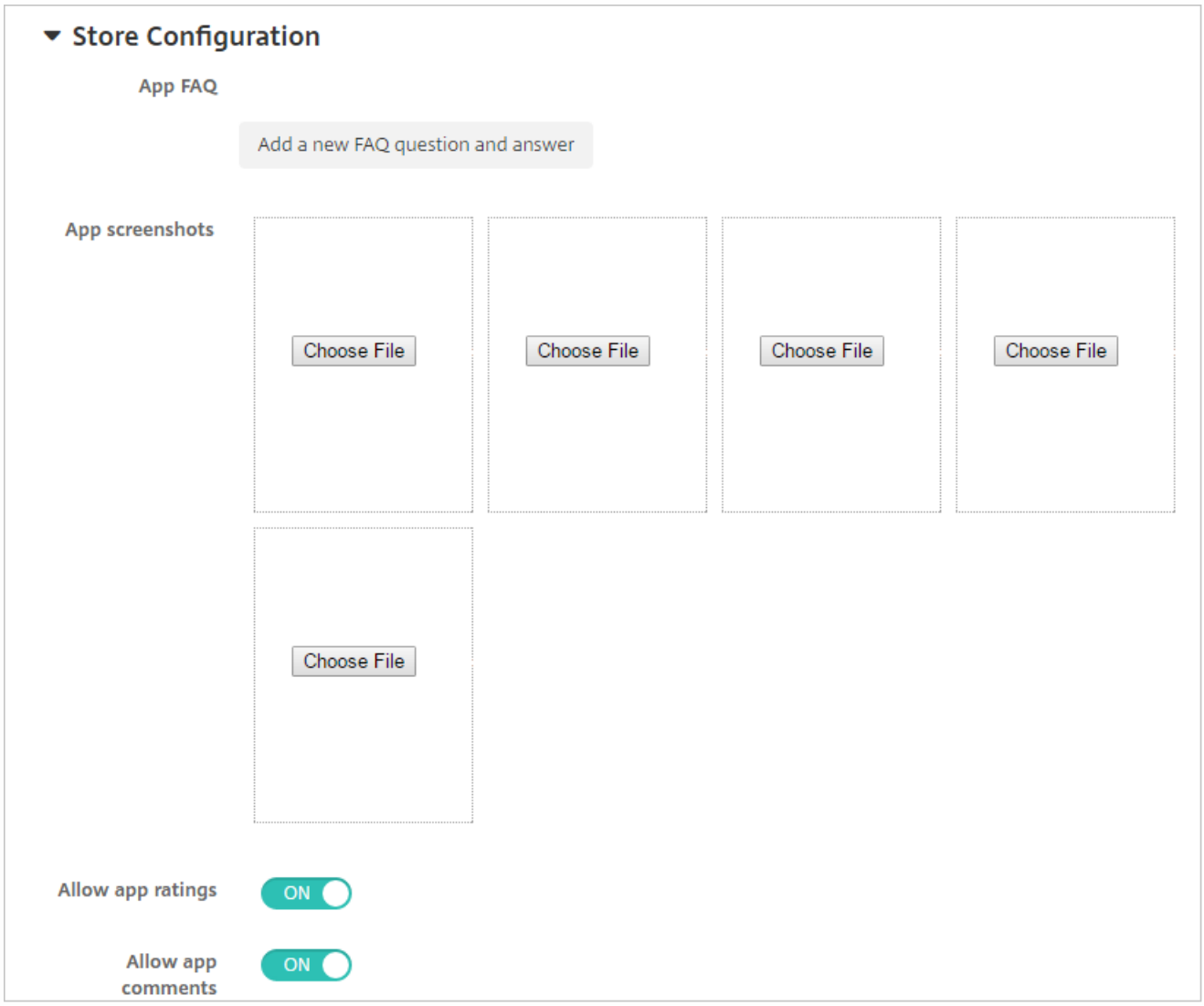
9. Konfigurieren Sie die Einstellungen für die Plattform, z. B.:

- **Dateiname**: Geben Sie optional einen neuen Namen für die App ein.
- **App-Beschreibung**: Geben Sie optional eine Beschreibung für die App ein.
- **App-Version**: Sie können dieses Feld nicht ändern.
- **OS-Version (Minimum)**: Geben Sie die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.

- **OS-Version (Maximum)**: Geben Sie die neueste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
- **Ausgeschlossene Geräte**: Geben Sie optional Hersteller oder Gerätemodelle an, auf denen die App nicht ausgeführt werden kann.
- **App entfernen, wenn MDM-Profil entfernt wird**: Wählen Sie aus, ob die App von Geräten entfernt werden soll, wenn das MDM-Profil entfernt wird. Der Standardwert ist **EIN**.
- **App-Datenbackup verhindern**: Wählen Sie aus, ob die App Daten sichern können soll. Der Standardwert ist **EIN**.
- **Verwaltung der App erzwingen**: Wenn Sie eine nicht verwaltete App installieren, wählen Sie **EIN**, wenn Benutzer nicht betreuter Geräte aufgefordert werden sollen, die Verwaltung der App zuzulassen. Kommt ein Benutzer der Aufforderung nach, wird die App verwaltet. Diese Einstellung gilt für iOS 9.x-Geräte.

10. Konfigurieren Sie die Bereitstellungsregeln.

11. Erweitern Sie **XenMobile Store-Konfiguration**.

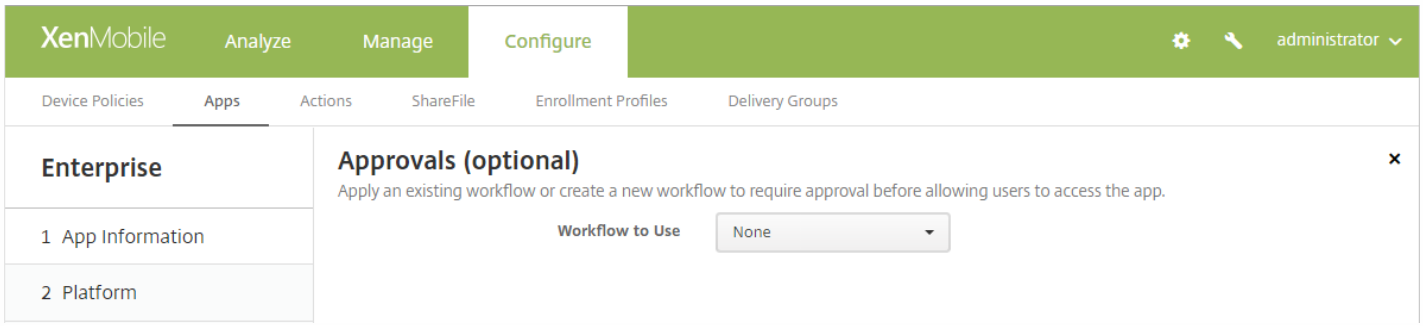


Sie können optional FAQ oder Screenshots für die App zur Anzeige im XenMobile Store hinzufügen. Sie können außerdem festlegen, ob Benutzer die App bewerten oder kommentieren können.

- 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 XenMobile 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. Der Standardwert ist **EIN**.
- **App-Kommentare zulassen**: Wählen Sie aus, ob eine Kommentierung der App durch die Benutzer zugelassen werden soll. Der Standardwert ist **EIN**.

12. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.



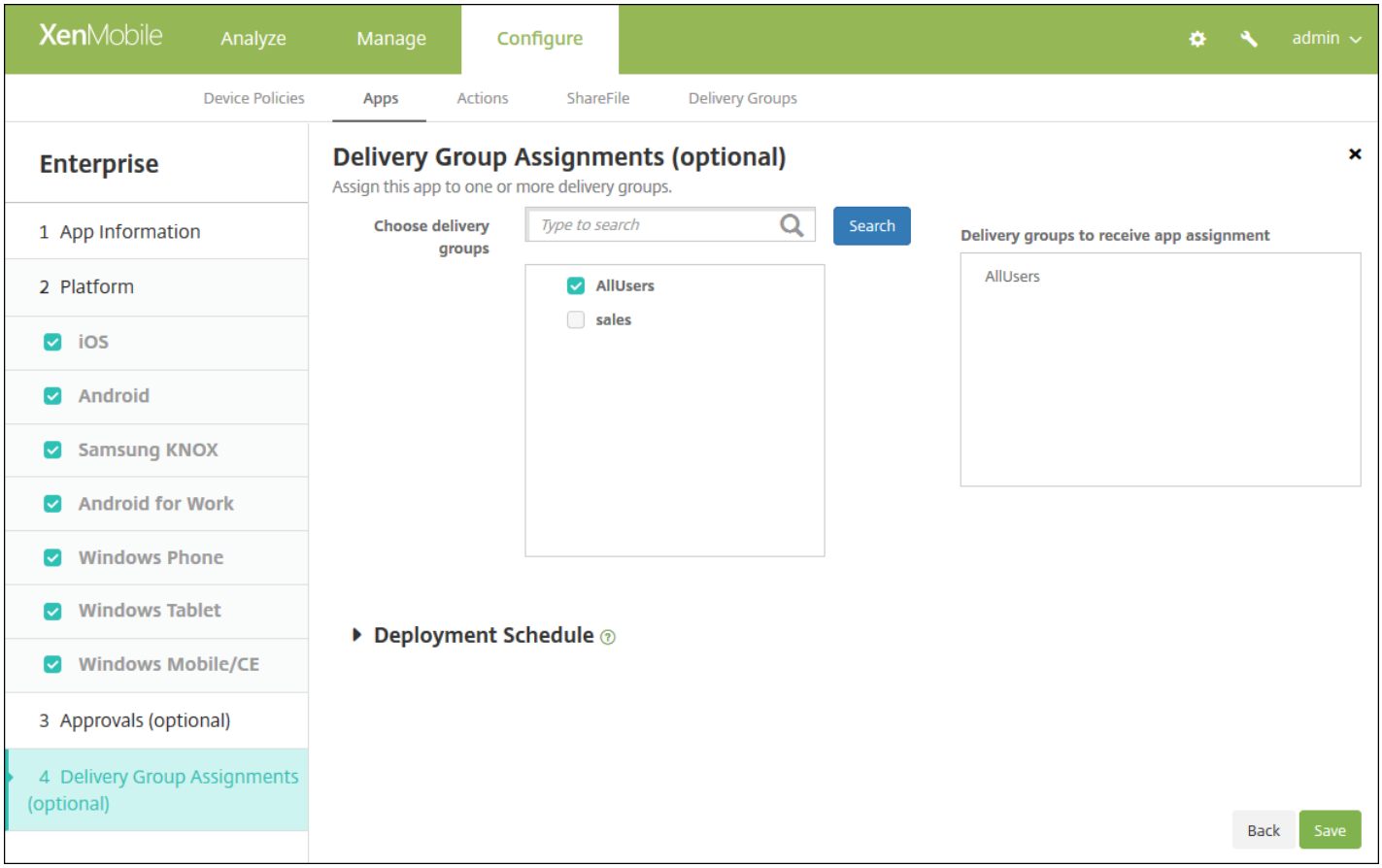
Wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist, verwenden Sie Workflows. Wenn Sie keine Genehmigungsworkflows einrichten müssen, fahren Sie mit Schritt 13 fort.

Konfigurieren Sie folgende Einstellungen, 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.

13. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.



14. 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.

15. 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

16. Klicken Sie auf **Speichern**.

Hinzufügen von Weblinks

In XenMobile können Sie eine Webadresse (URL) für eine öffentliche oder private Website oder eine Web-App, die kein Single Sign-On erfordert, einrichten.

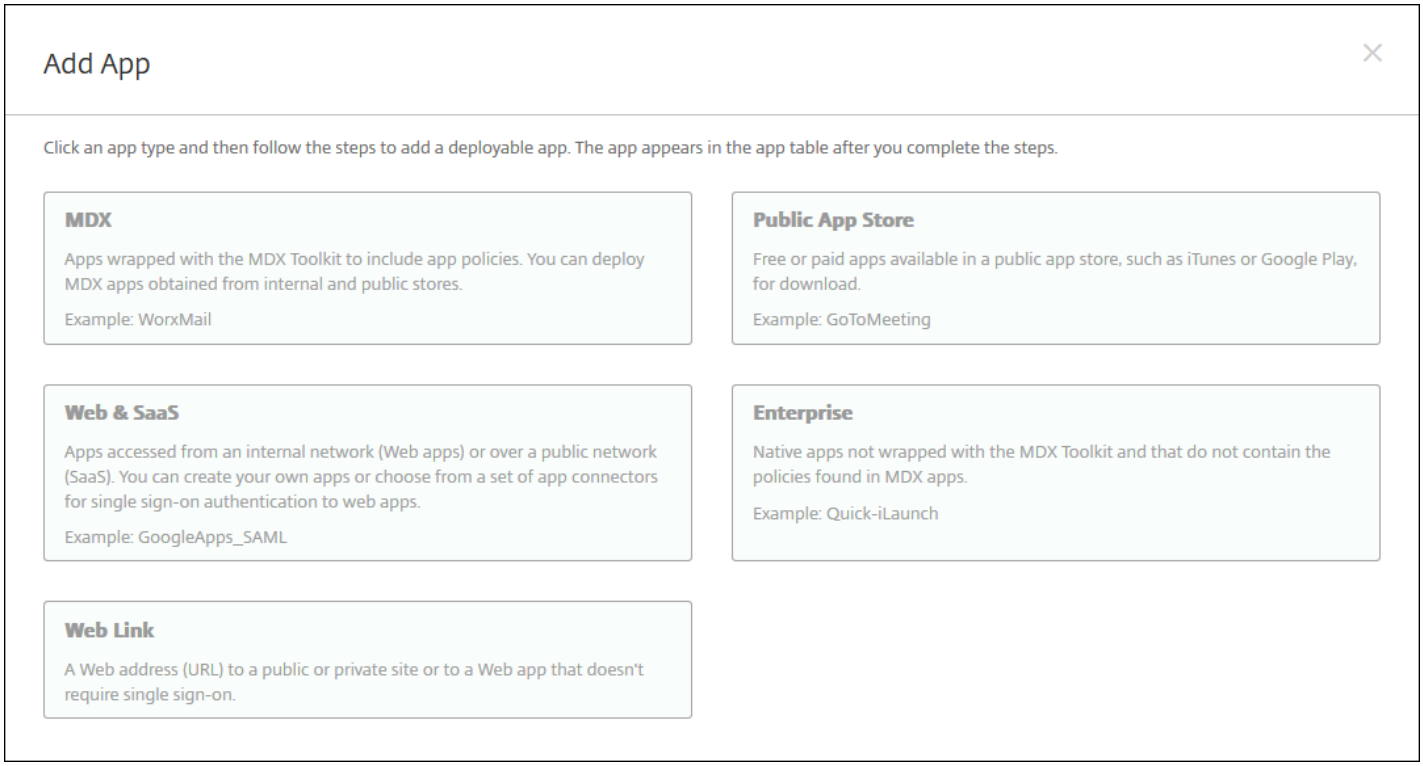
Sie können Weblinks über die Registerkarte **Apps** in der XenMobile-Konsole konfigurieren. Wenn Sie die Konfiguration des Weblinks abgeschlossen haben, wird der Link als Symbol in der Liste der App-Tabelle angezeigt. Der Link wird mit der Liste der verfügbaren Anwendungen und Desktops angezeigt, wenn Benutzer sich bei Secure Hub anmelden.

Für den hinzuzufügenden Link müssen Sie die folgenden Informationen angeben:

- Name für den Link
- Beschreibung des Links
- Webadresse (URL)
- Kategorie
- Rolle
- Bild im PNG-Format (optional)

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

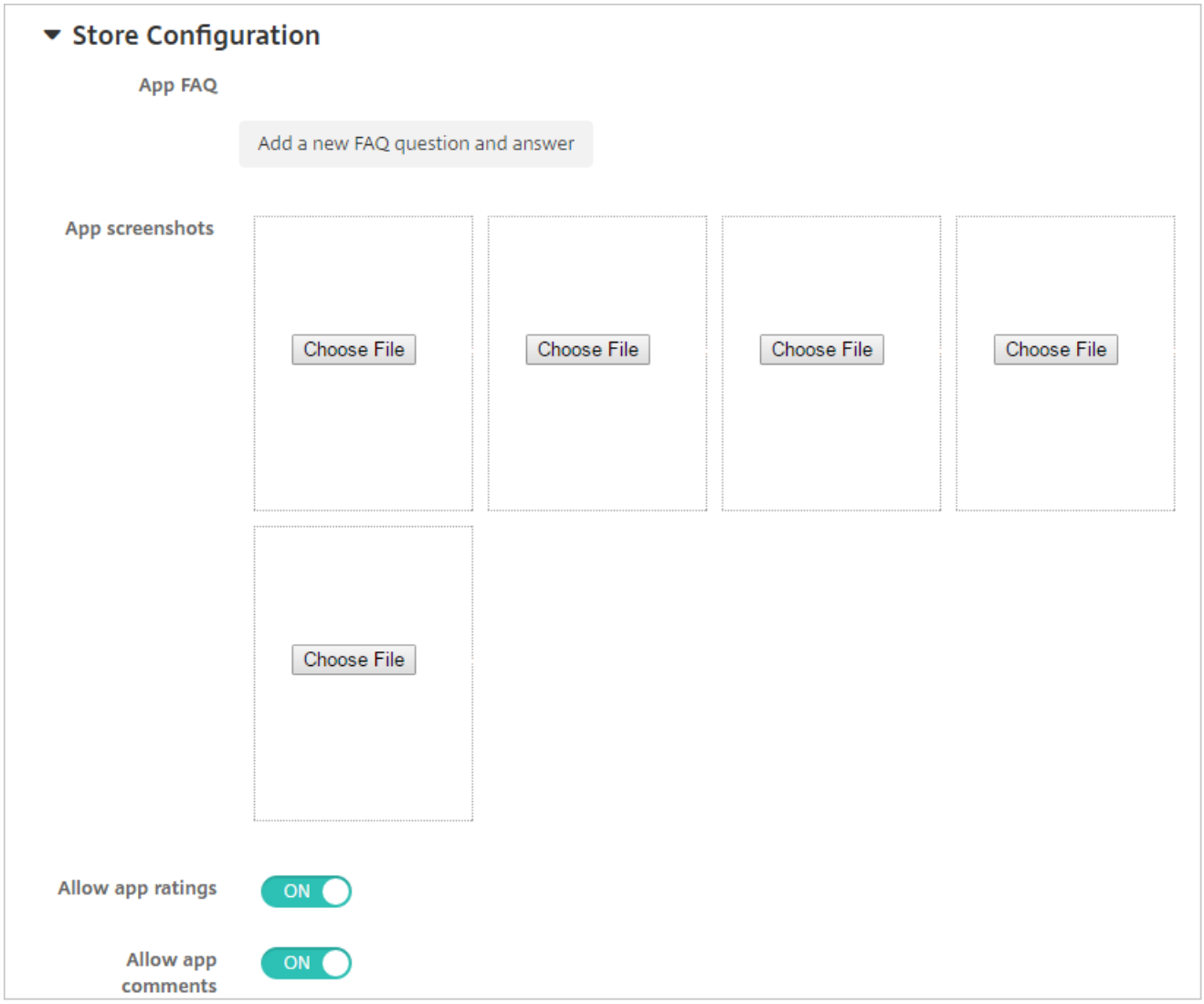


3. Klicken Sie auf **Weblinks**. Die Seite **App-Informationen** wird angezeigt.

4. Konfigurieren Sie die folgenden Einstellungen:

- **App-Name**: Übernehmen Sie den Standardnamen oder geben Sie einen neuen Namen ein.
- **App-Beschreibung**: Übernehmen Sie die Standardbeschreibung oder geben Sie eine eigene Beschreibung ein.
- **URL**: Übernehmen Sie die Standard-URL oder geben Sie die Webadresse für die App ein. Je nach ausgewähltem Connector enthält dieses Feld eventuell einen Platzhalter, den Sie ersetzen müssen, bevor Sie mit der nächsten Seite fortfahren können.
- **App wird im internen Netzwerk gehostet**: Klicken Sie auf Ein, wenn die App auf einem Server im internen Netzwerk ausgeführt wird. Wenn Benutzer von einem Remotestandort aus eine Verbindung mit der internen Anwendung herstellen, muss dies über NetScaler Gateway erfolgen. Wenn Sie diese Option auf **Ein** festlegen, wird das VPN-Schlüsselwort der App hinzugefügt, sodass Benutzer eine Verbindung über NetScaler Gateway herstellen können. Der Standardwert ist **AUS**.
- **App-Kategorie**: Klicken Sie optional in der Liste auf eine Kategorie, der Sie die App zuweisen möchten.
- **Bild**: Geben Sie an, ob Sie das Citrix Standardbild verwenden oder ein eigenes App-Bild hochladen möchten. Der Standardwert ist "Standard verwenden".
  - Wenn Sie ein Bild hochladen möchten, klicken Sie auf **Durchsuchen**, navigieren Sie zu dem Speicherort der Bilddatei und wählen Sie diese aus. Die Datei muss das Format .png haben, JPEG- und GIF-Dateien können nicht hochgeladen werden. Eine benutzerdefinierte Grafik kann später nicht mehr geändert werden.

5. Erweitern Sie **XenMobile Store-Konfiguration**.



Sie können optional FAQ oder Screenshots für die App zur Anzeige im XenMobile 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 XenMobile 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. Der Standardwert ist **EIN**.
  - **App-Kommentare zulassen**: Wählen Sie aus, ob eine Kommentierung der App durch die Benutzer zugelassen werden soll. Der Standardwert ist **EIN**.

6. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.

7. 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.

8. 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 "always-on" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

9. Klicken Sie auf **Speichern**.

Aktivieren von Microsoft 365-Apps

Sie können den MDX-Container öffnen, um Secure Mail, Secure Web und ShareFile die Übertragung von Daten und Dokumenten an Microsoft Office 365-Apps zu ermöglichen. Weitere Informationen finden Sie unter Zulassen der sicheren Interaktion mit Office 365-Apps.

Erstellen und Verwalten von Workflows

Sie können das Erstellen und Entfernen von Benutzerkonten mit Workflows verwalten. Damit ein Workflow verwendet werden kann, müssen Sie die Personen in Ihrer Organisation ermitteln, die zum Genehmigen von Benutzerkontenanforderungen berechtigt sind. Anschließend können Sie mit der Workflowvorlage Benutzerkontenanforderungen erstellen und genehmigen.

Beim ersten Einrichten von XenMobile konfigurieren Sie Einstellungen für Workflow-E-Mails. Diese müssen festgelegt werden, bevor Sie Workflows verwenden können. Sie können die Einstellungen für Workflow-E-Mails jederzeit ändern. Diese Einstellungen umfassen E-Mail-Server, Port, E-Mail-Adresse und Angaben dazu, ob die Anforderung zum Erstellen des Benutzerkontos genehmigt werden muss.

Workflows können in XenMobile an zwei Stellen konfiguriert werden:

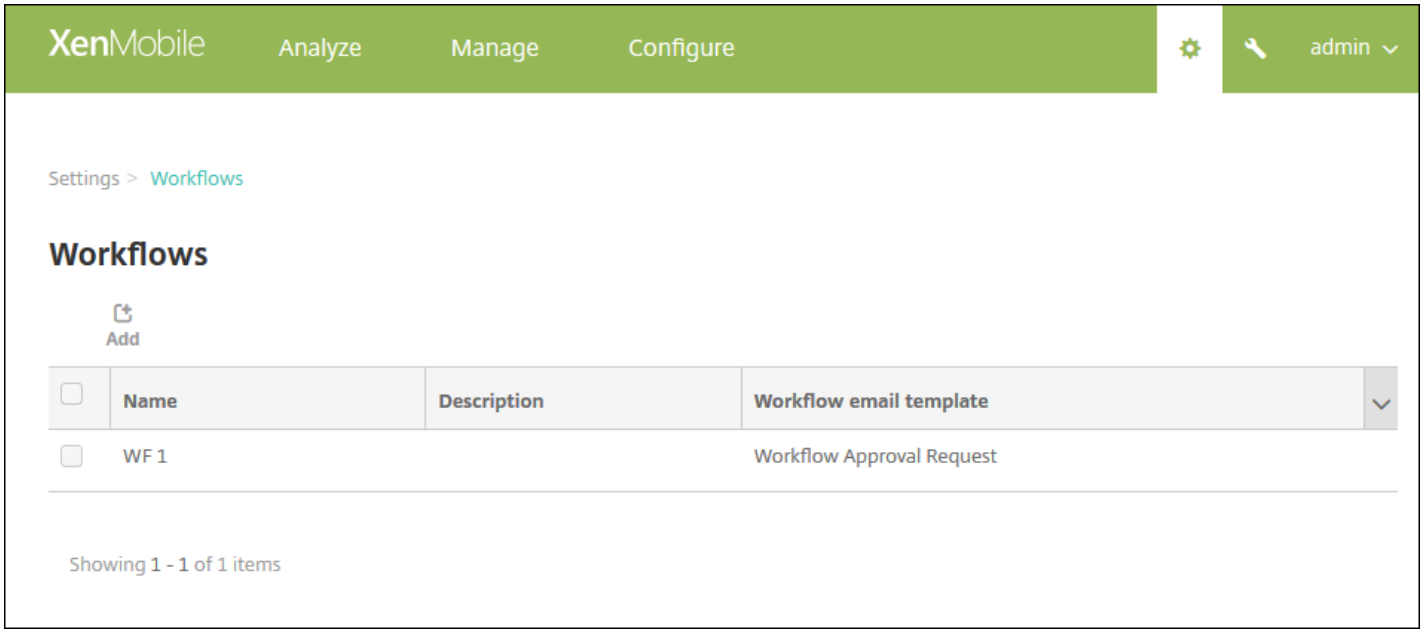
- Auf der Seite Workflows in der XenMobile-Konsole: Auf der Seite Workflows können Sie mehrere Workflows zur Verwendung mit App-Konfigurationen verwenden. Wenn Sie Workflows auf der Seite Workflows konfigurieren, können Sie den Workflow während des Konfigurierens der App auswählen.
- Wenn Sie einen Anwendungsconnector konfigurieren, geben Sie in der App einen Workflow-Namen an und konfigurieren anschließend die Personen, die die Benutzerkontoanforderung genehmigen können.

Sie können bis zu drei Ebenen für die Genehmigung von Benutzerkonten durch leitende Mitarbeiter zuweisen. Wenn noch weitere Personen zum Genehmigen eines Benutzerkontos berechtigt sein sollen, können Sie anhand des Namens oder der

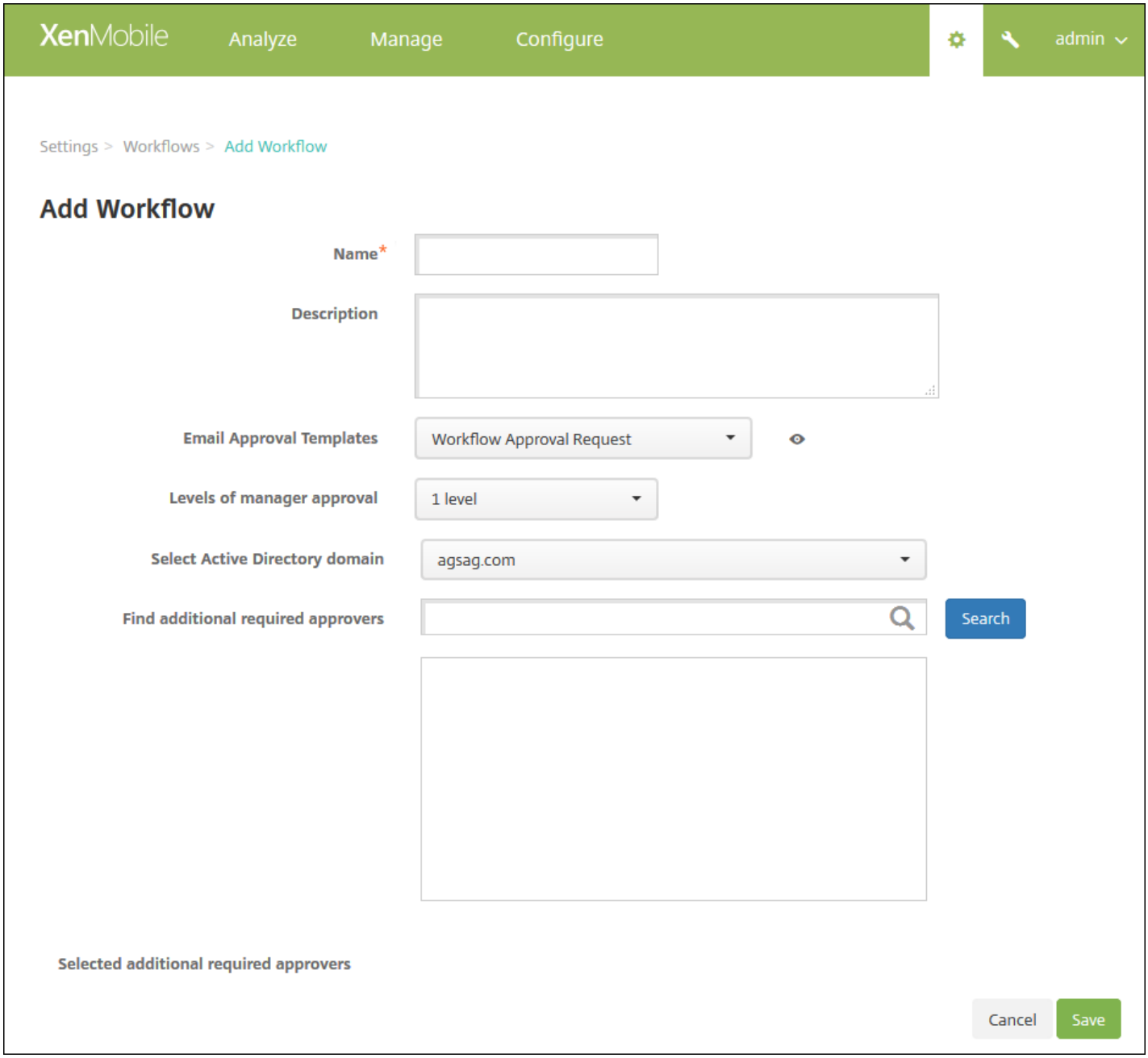
E-Mail-Adresse weitere genehmigende Personen suchen und auswählen. Wenn XenMobile die Person gefunden hat, können Sie sie zum Workflow hinzufügen. Alle Personen im Workflow erhalten E-Mails zum Genehmigen oder Ablehnen des neuen Benutzerkontos.

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

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

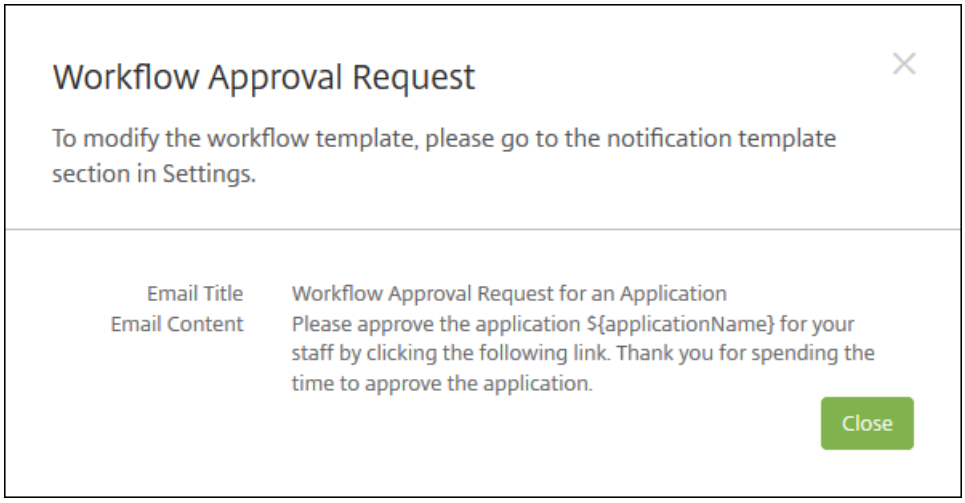


3. Klicken Sie auf **Hinzufügen**. Die Seite **Add Workflow** wird angezeigt.



4. 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. Sie erstellen E-Mail-Vorlagen im Bereich Benachrichtigungsvorlagen der XenMobile-Konsole unter Einstellungen. Wenn Sie auf das Augensymbol rechts neben dem Feld klicken, wird folgendes Dialogfeld 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.

5. Klicken Sie auf **Speichern**. Der erstellte Workflow wird auf der Seite **Workflows** angezeigt.

Nach dem Erstellen des Workflows können Sie dessen Details und die mit ihm verbundenen Apps anzeigen oder den Workflow löschen. Ein einmal erstellter Workflow kann nicht mehr geändert werden. Wenn ein Workflow mit anderen Genehmigungsebenen oder Freigabeberechtigten benötigt wird, müssen Sie einen neuen erstellen.

Anzeigen von Details und Löschen eines Workflows

1. Wählen Sie auf der Seite **Workflows** in der Liste der Workflows einen Workflow durch Klicken auf die Zeile in der Tabelle oder Aktivieren des Kontrollkästchens neben dem Workflow aus.

2. Klicken Sie zum Löschen des Workflows auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf **Delete**.

Wichtig: Sie können diesen Vorgang nicht rückgängig machen.

App-Connectortypen

Feb 24, 2017

In der folgenden Tabelle finden Sie die Connectors und Connectortypen, die in XenMobile beim Hinzufügen einer Web- oder SaaS-App verfügbar sind. Sie können beim Hinzufügen einer Web- oder SaaS-App auch einen neuen Connector hinzufügen.

Die Tabelle enthält Angaben dazu, ob ein Connector die Benutzerkontenverwaltung unterstützt, mit der neue Konten automatisch oder mit einem Workflow erstellt werden können.

Connectorname	Single Sign-On SAML	Unterstützt Benutzerkontenverwaltung
Echosign_SAML	J	J
Globoforce_SAML		**Hinweis**: Wenn Sie diesen Connector verwenden, müssen Sie User Management für Provisioning aktivieren, um eine nahtlose SSO-Integration zu gewährleisten.
GoogleApps_SAML	J	J
GoogleApps_SAML_IDP	J	J
Lynda_SAML	J	J
Office365_SAML	J	J
Salesforce_SAML	J	J
Salesforce_SAML_SP	J	J
SandBox_SAML	J	
SuccessFactors_SAML	J	
ShareFile_SAML	J	
ShareFile_SAML_SP	J	
WebEx_SAML_SP	J	J

Durchführen eines Upgrades von MDX- oder Unternehmensapps

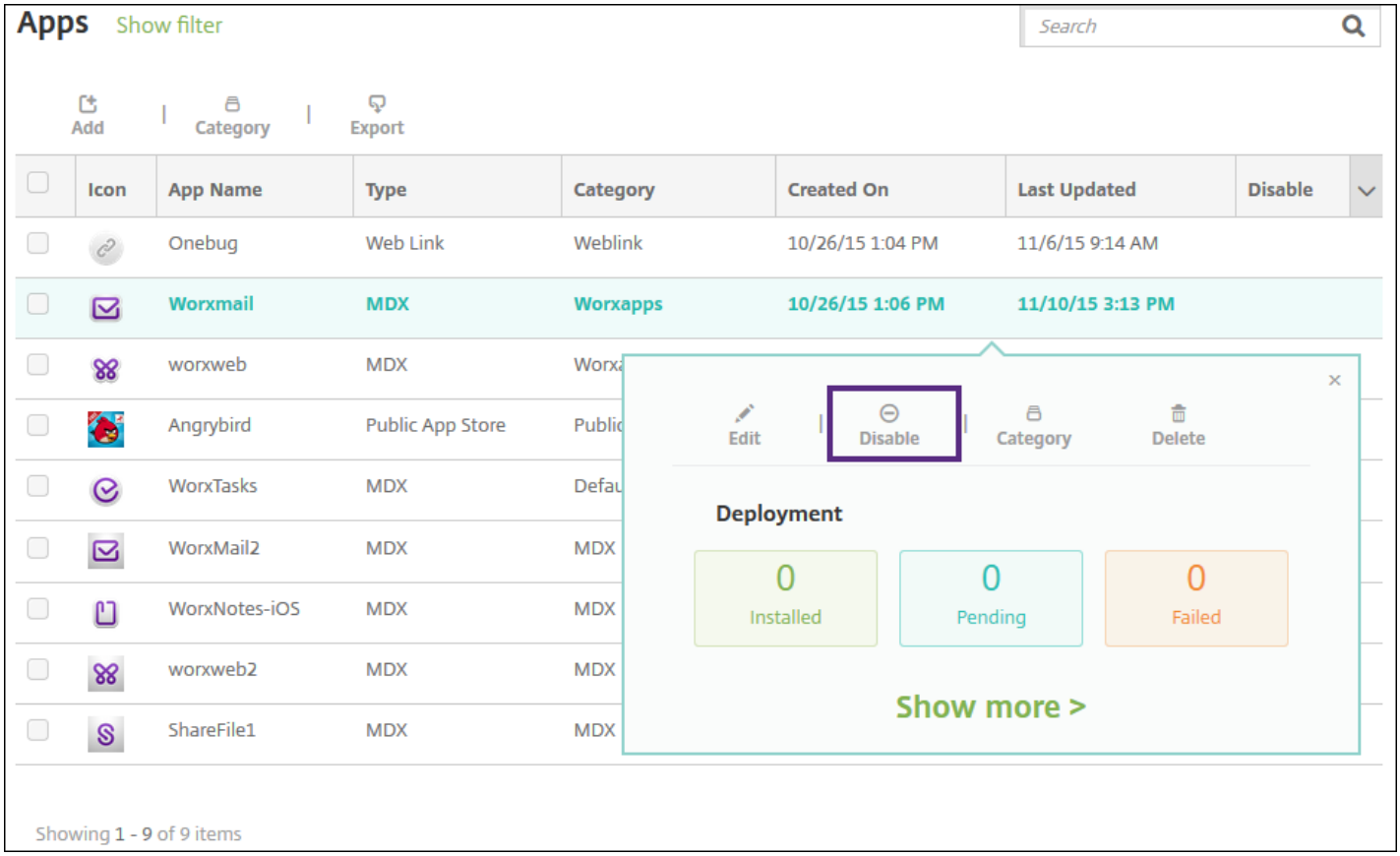
Feb 24, 2017

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 3 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**.



- Klicken Sie im Bestätigungsdialogfeld auf **Deaktivieren**. In der Spalte *Deaktivieren* der App wird nun **Deaktiviert** angezeigt.

Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
	Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

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.

3. Klicken Sie in der App-Tabelle auf das Kontrollkästchen neben der App, die aktualisiert werden soll, oder auf deren Zeile.

4. Klicken Sie im angezeigten Menü auf **Bearbeiten**. Die Seite **App-Informationen** wird angezeigt, die ursprünglich für die App ausgewählte Plattform ist ausgewählt.

5. Konfigurieren Sie die folgenden Einstellungen:

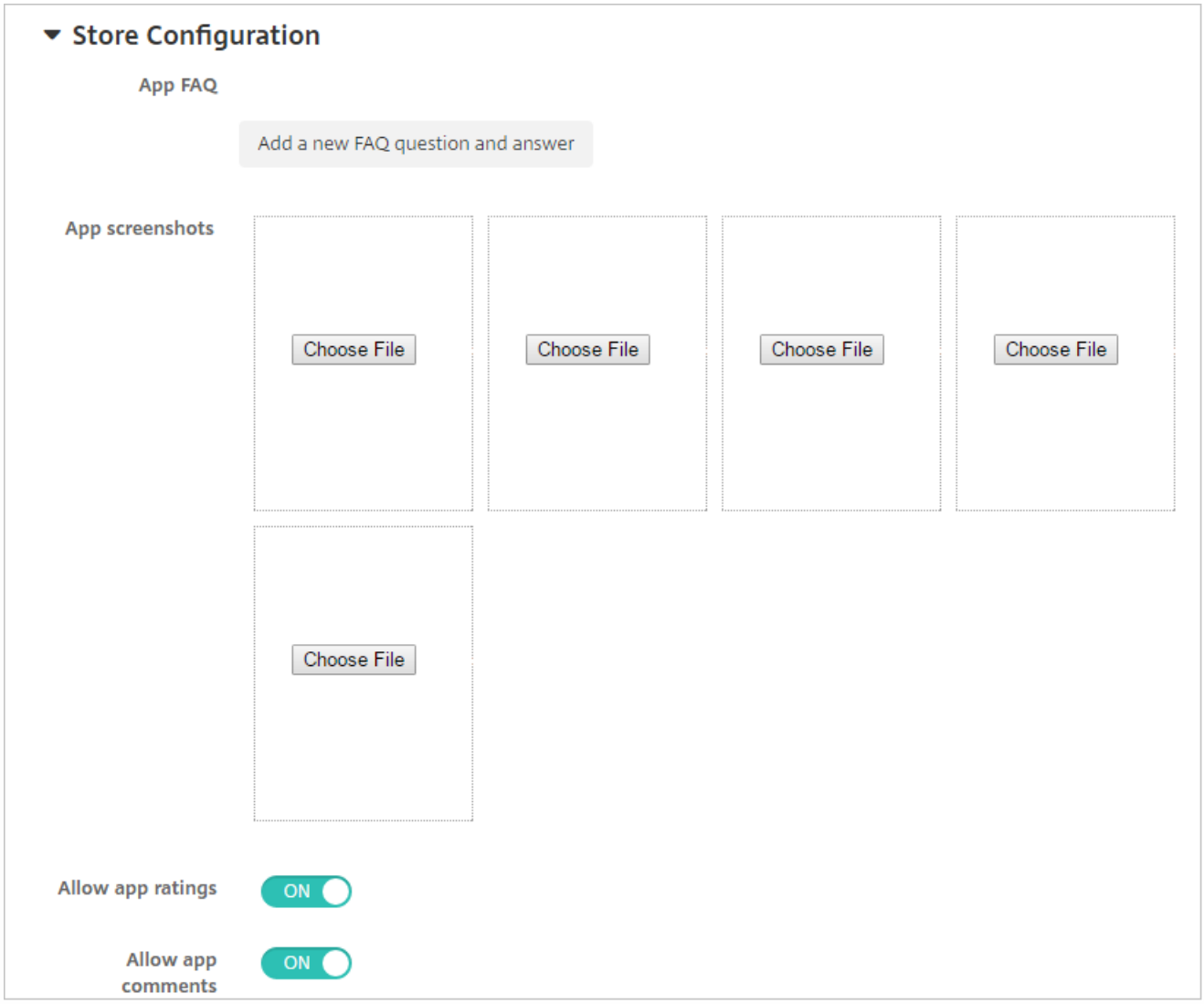
- **Name**: Ändern Sie optional den Namen der App.
- **Beschreibung**: Ändern Sie optional die App-Beschreibung.
- **App-Kategorie**: Ändern Sie optional die App-Kategorie.

6. 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 XenMobile Store-Konfigurationen (siehe Schritt 8).

7. Konfigurieren der Bereitstellungsregeln

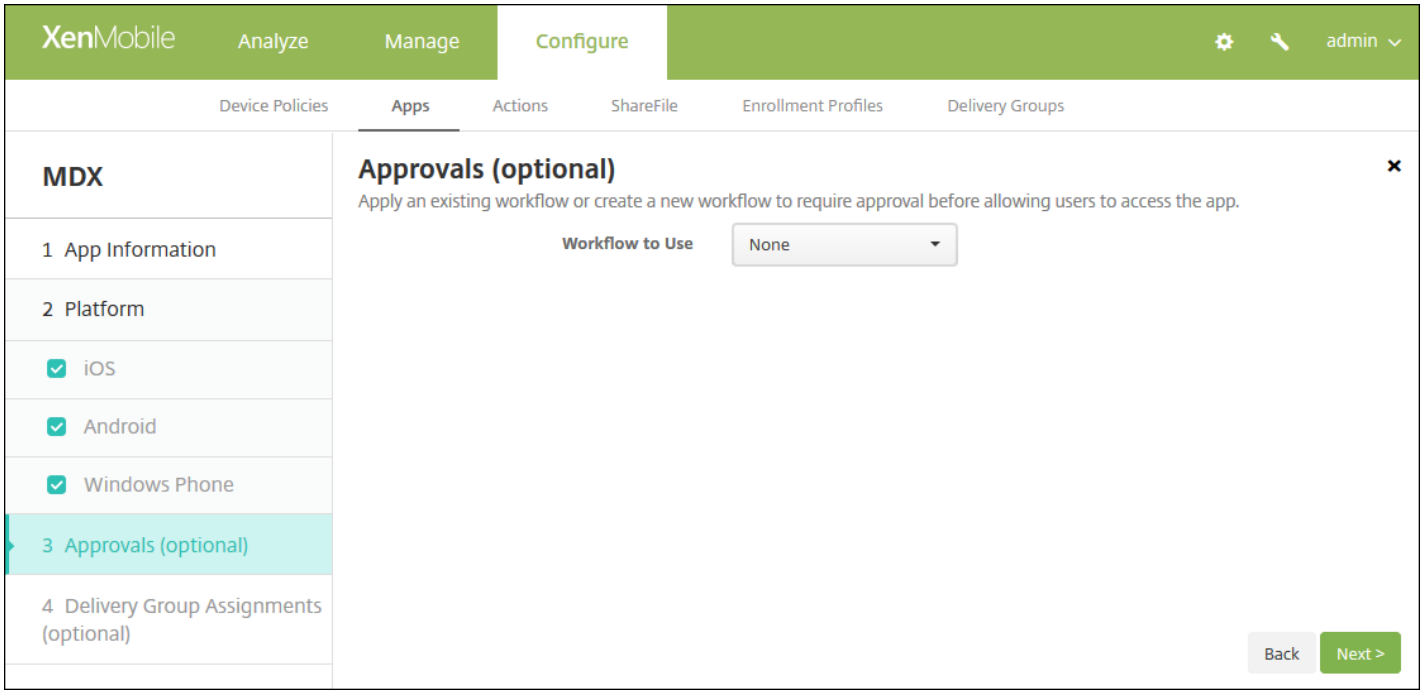
8. Erweitern Sie **Store-Konfiguration**.



Sie können optional FAQ oder Screenshots für die App zur Anzeige im XenMobile 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 XenMobile 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. Der Standardwert ist **EIN**.
  - **App-Kommentare zulassen**: Wählen Sie aus, ob eine Kommentierung der App durch die Benutzer zugelassen werden soll. Der Standardwert ist **EIN**.

9. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.



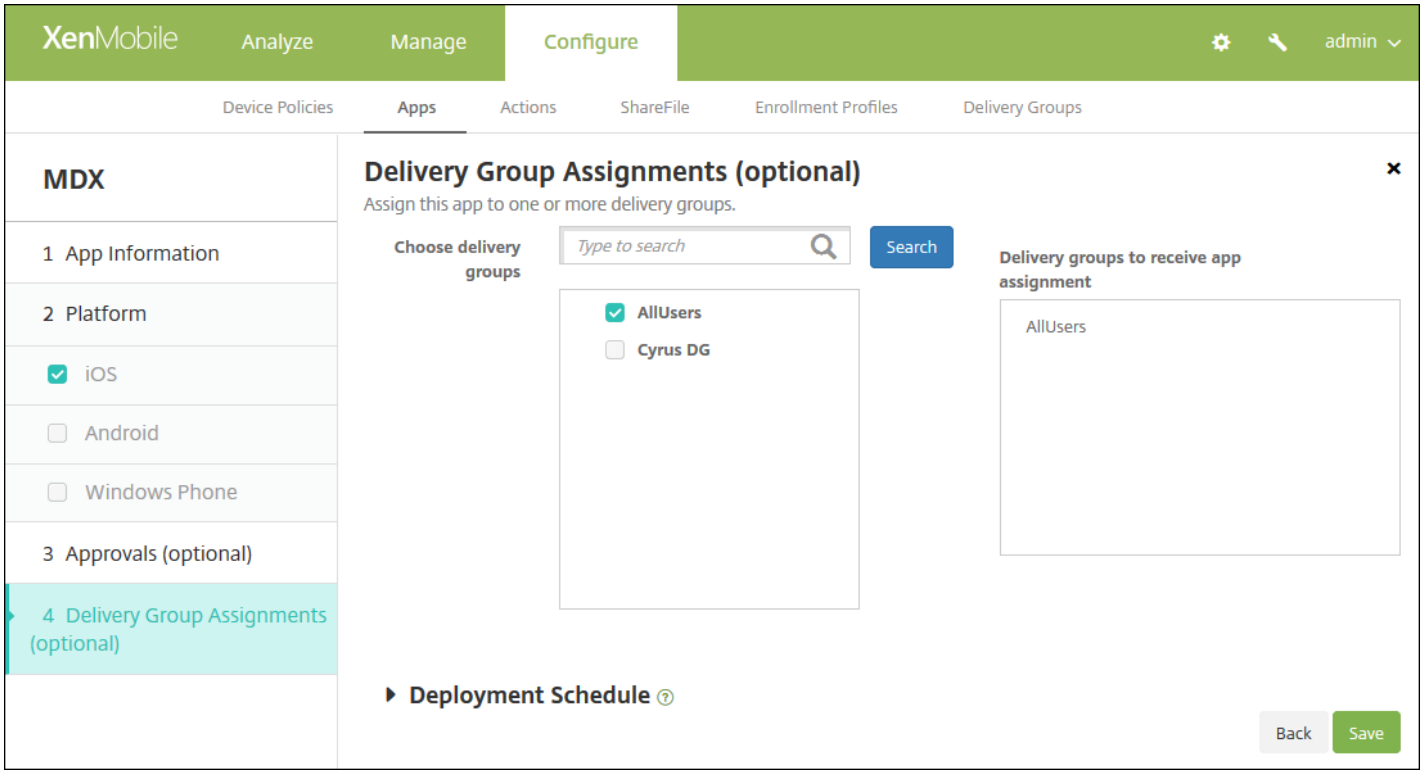
10. Wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist, verwenden Sie Workflows. Wenn Sie keine Genehmigungsworkflows einrichten müssen, fahren Sie mit Schritt 11 fort.

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.

11. Klicken Sie auf **Weiter**. Die Seite **Zuweisungen für Bereitstellungsgruppen** wird angezeigt.



12. 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.

13. 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 "always-on" ist für iOS-Geräte nicht verfügbar.

- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

14. Klicken Sie auf **Speichern**. Die Seite **Apps** wird angezeigt.

15. 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.

MDX-App-Richtlinien auf einen Blick

Feb 24, 2017

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.

Branding für XenMobile Store und Citrix Secure Hub

Feb 24, 2017

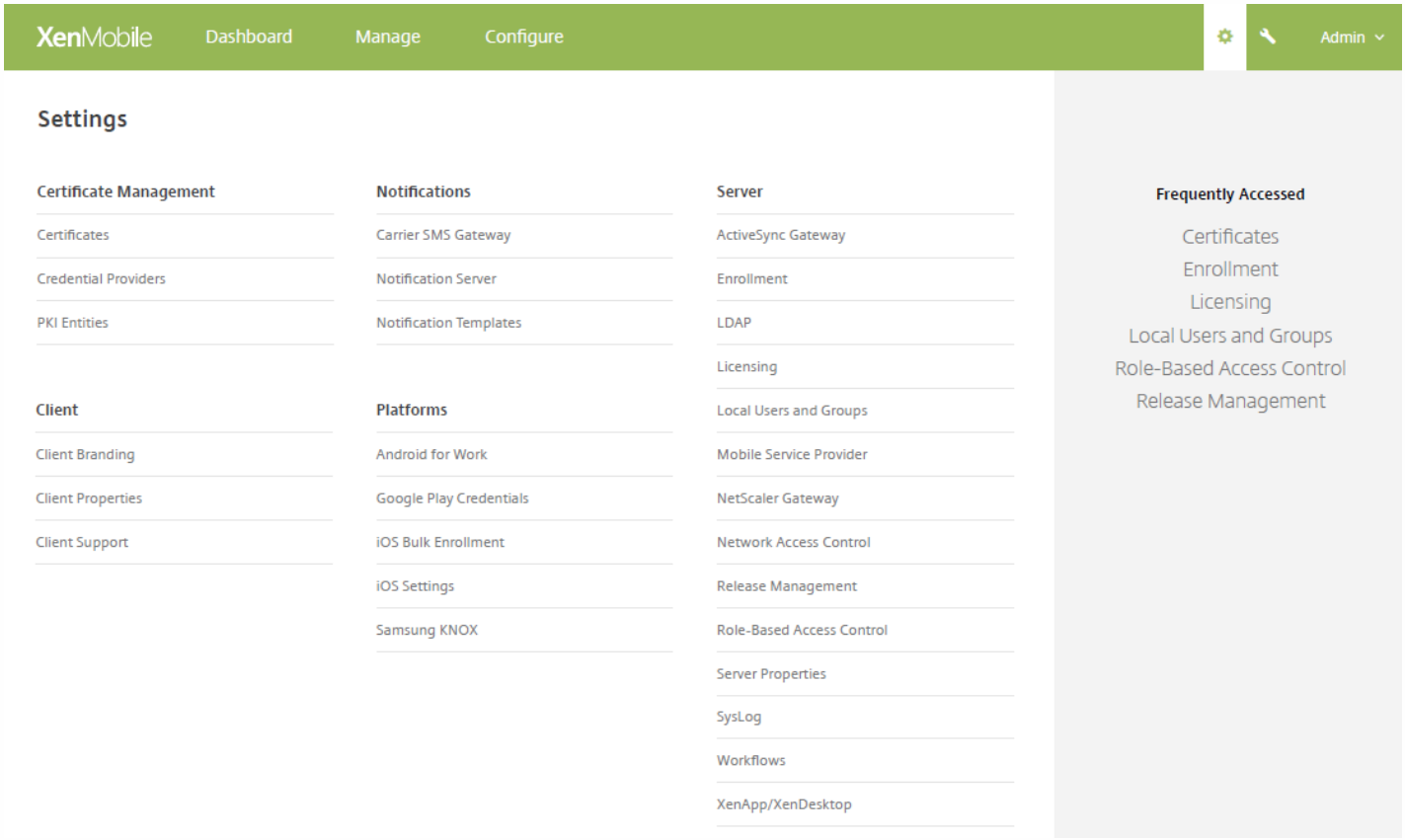
Sie können festlegen, wie Apps im Store angezeigt werden, und Secure Hub und dem XenMobile Store für mobile iOS- und Android-Geräte ein Logo hinzufügen.

Hinweis: Stellen Sie zu Beginn des Arbeitsgangs sicher, dass das benutzerdefinierte Bild bereitsteht.

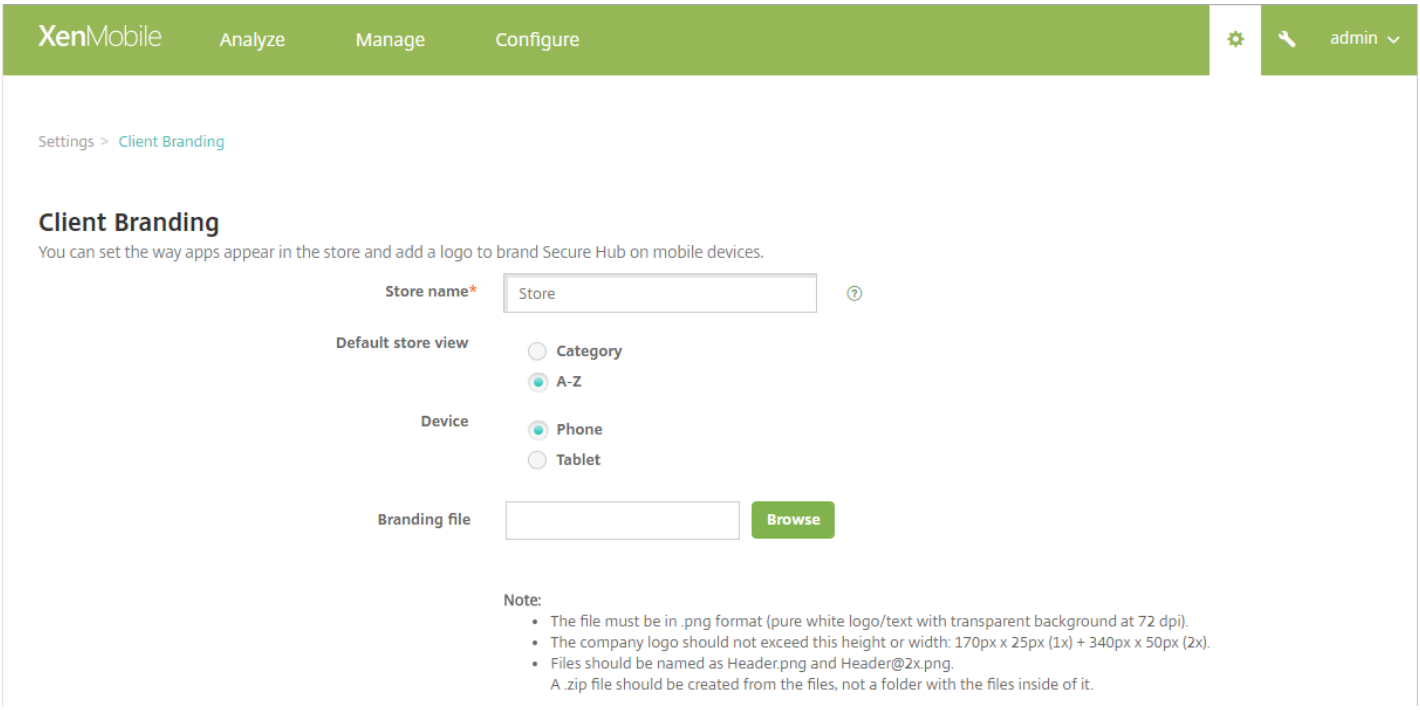
Das benutzerdefinierte Bild muss folgende Anforderungen erfüllen:

- 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.

Citrix Launcher

Apr 24, 2017

Mit Citrix Launcher können Sie die Benutzererfahrung für über XenMobile bereitgestellte Android-Geräte anpassen. Die Mindestversion von Android, die für die Secure Hub-Verwaltung von Citrix Launcher unterstützt wird, ist Android 4.0.3. Mit der **Launcher-Konfigurationsrichtlinie** können Sie folgende Citrix Launcher-Beschränkungen auf Geräteebene steuern:

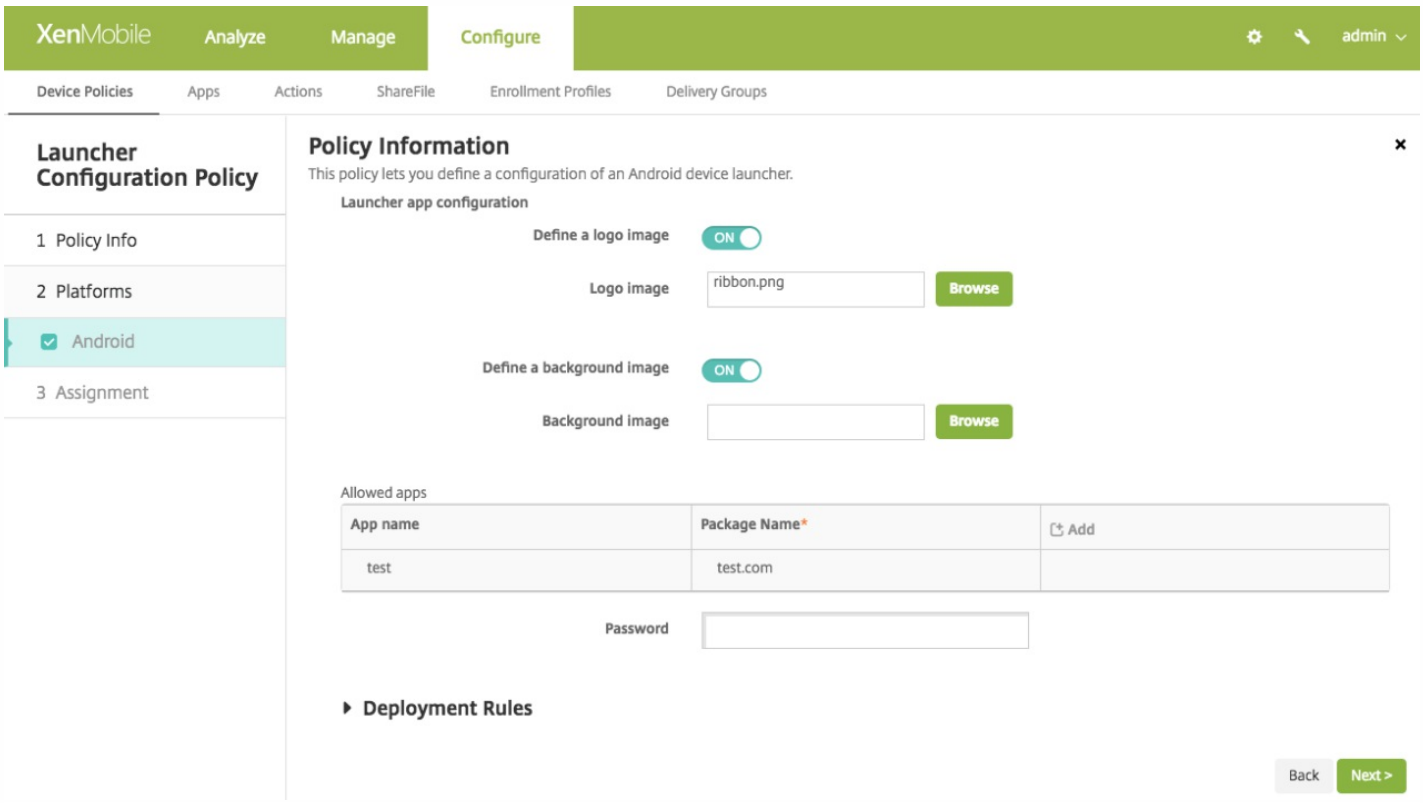
- Verwalten von Android-Geräten, sodass Benutzer nur auf von Ihnen festgelegte Apps Zugriff haben
- Optionale Angabe eines benutzerdefinierten Logos als Citrix Launcher-Symbol sowie eines benutzerdefinierten Hintergrundbilds für Citrix Launcher
- Festlegen eines Kennworts, das die Benutzer zum Beenden von Launcher eingeben müssen

Der Geräte-Launcher bietet integrierten Zugriff auf die Geräteeinstellungen für WiFi, Bluetooth, Gerätepasscode und andere Einstellungen. Citrix Launcher ist nicht als zusätzliche Sicherheitsstufe gedacht.

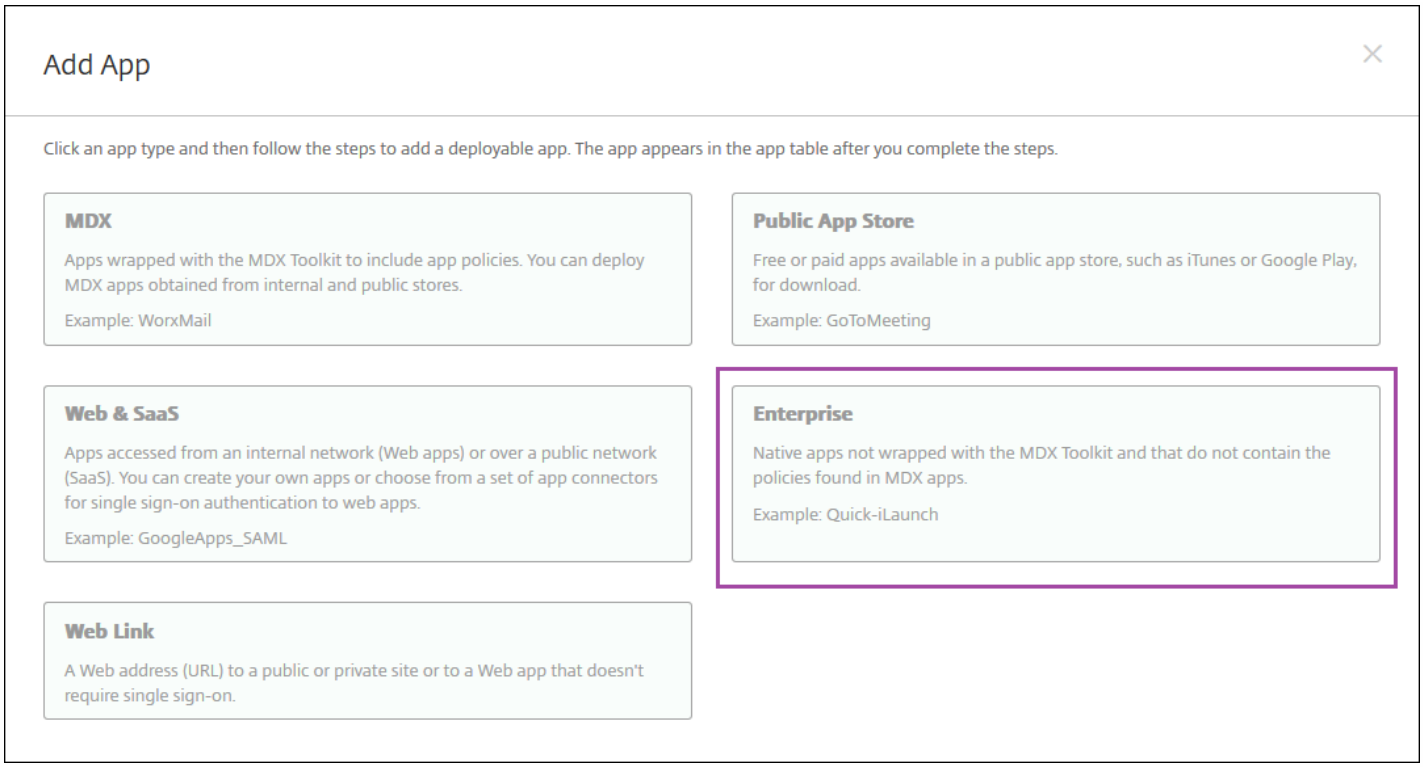
Das Verfahren zum Bereitstellen von Citrix Launcher für Android-Geräte ist folgendes:

1. Laden Sie die Citrix Launcher-App von der Citrix Downloadseite für Ihre XenMobile-Edition herunter. Der Dateiname lautet CitrixLauncher.apk. Die Datei kann ohne Umschließen in XenMobile hochgeladen werden.

2. Fügen Sie die Launcher-Konfigurationsrichtlinie hinzu: Gehen Sie zu **Konfigurieren > Geräterichtlinien**, klicken Sie auf **Hinzufügen** und beginnen Sie im Dialogfeld **Neue Richtlinie hinzufügen** mit der Eingabe von **Launcher**. Weitere Informationen finden Sie unter Launcher-Konfigurationsrichtlinie.

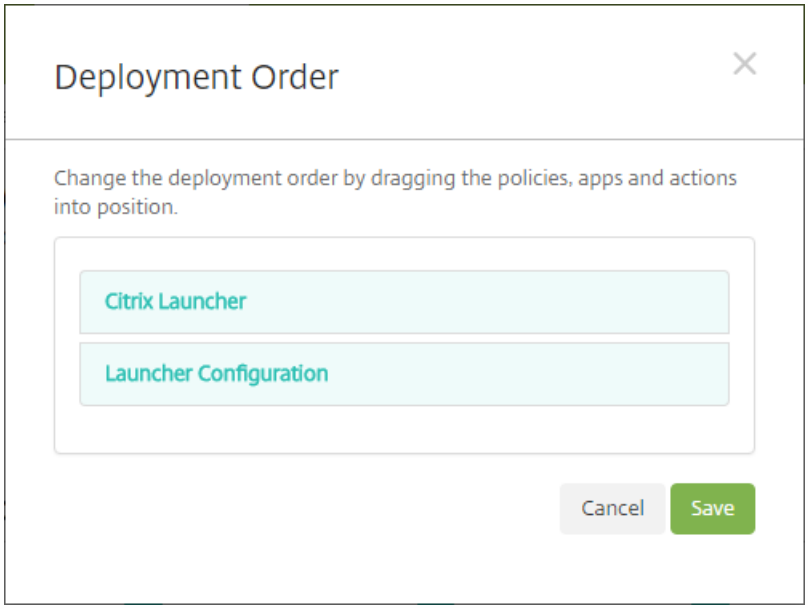


3. Fügen Sie die Citrix Launcher-App in XenMobile als Unternehmensapp hinzu. Klicken Sie unter **Konfigurieren > Apps** auf **Hinzufügen**. Klicken Sie dann auf **Enterprise**. Weitere Informationen finden Sie unter Hinzufügen einer Unternehmensapp.



4. Erstellen Sie über **Konfigurieren > Bereitstellungsgruppen** eine Bereitstellungsgruppe für Citrix Launcher mit der folgenden Konfiguration:

- Fügen Sie auf der Seite **Richtlinien** die **Launcher-Konfigurationsrichtlinie** hinzu.
- Ziehen Sie auf der Seite **Apps** die App **Citrix Launcher** auf **Erforderliche Apps**.
- Klicken Sie auf der Seite **Zusammenfassung** auf **Bereitstellungsreihenfolge** und vergewissern Sie sich, dass die App **Citrix Launcher** vor der Richtlinie **Launcher-Konfiguration** steht.



Weitere Informationen finden Sie unter Bereitstellen von Ressourcen.

iOS-Programm für Volumenlizenzen (Volume Purchase Program, VPP)

Feb 24, 2017

Sie können die Lizenzierung von iOS-Apps mit dem Programm für Volumenlizenzen von Apple (Volume Purchase Program, VPP) verwalten, einer einfachen, skalierbaren Lösung zum Verwalten des Bedarfs an Inhalten eines Unternehmens. Das VPP vereinfacht Suche, Erwerb und Verteilung von Apps und anderen Daten in großer Zahl.

Mit dem VPP können Sie über XenMobile Apps (einschließlich XenMobile- und anderer MDX-Apps) direkt auf Geräte verteilen oder den Benutzern Inhalte unter Einsatz einlösbarer Codes zuweisen. Sie konfigurieren Einstellungen für das VPP in XenMobile.

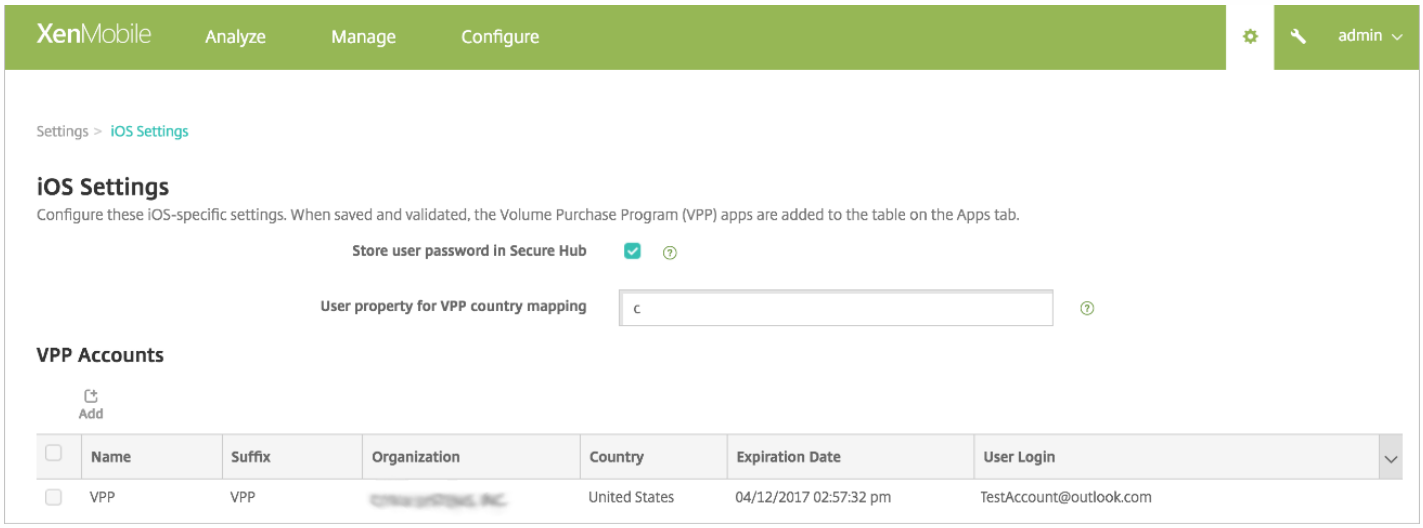
In diesem Artikel wird die Verwendung des VPP für verwaltete Lizenzen behandelt, welche die Verteilung von Apps über XenMobile ermöglichen. Wenn Sie derzeit Einlösungscodes verwenden und auf die verwaltete Verteilung umstellen möchten, lesen Sie den Apple-Supportartikel Umstellung im Rahmen des Programms für Volumenlizenzen von Einlösecodes auf verwaltete Verteilung.

Weitere Informationen über das VPP finden Sie unter http://www.apple.com/business/vpp/. Gehen Sie zur Registrierung beim VPP zu https://deploy.apple.com/qforms/open/register/index/avs . Für den Zugriff auf Ihren VPP-Store in iTunes gehen Sie zu https://vpp.itunes.apple.com/?l=de.

Wenn Sie die iOS VPP-Einstellungen in XenMobile gespeichert und geprüft haben, werden die erworbenen Apps der Tabelle auf der Registerkarte **Konfigurieren > Apps** 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 **Plattform** auf **iOS-Einstellungen**. Die Seite **iOS-Einstellungen** wird angezeigt.



3. Konfigurieren Sie folgende Einstellungen:

- **Benutzerkennwort in Secure Hub speichern**: Wählen Sie aus, ob ein Benutzername mit Kennwort in Secure Hub für die XenMobile-Authentifizierung gespeichert werden soll. Standardmäßig werden die Anmeldeinformationen mit dieser

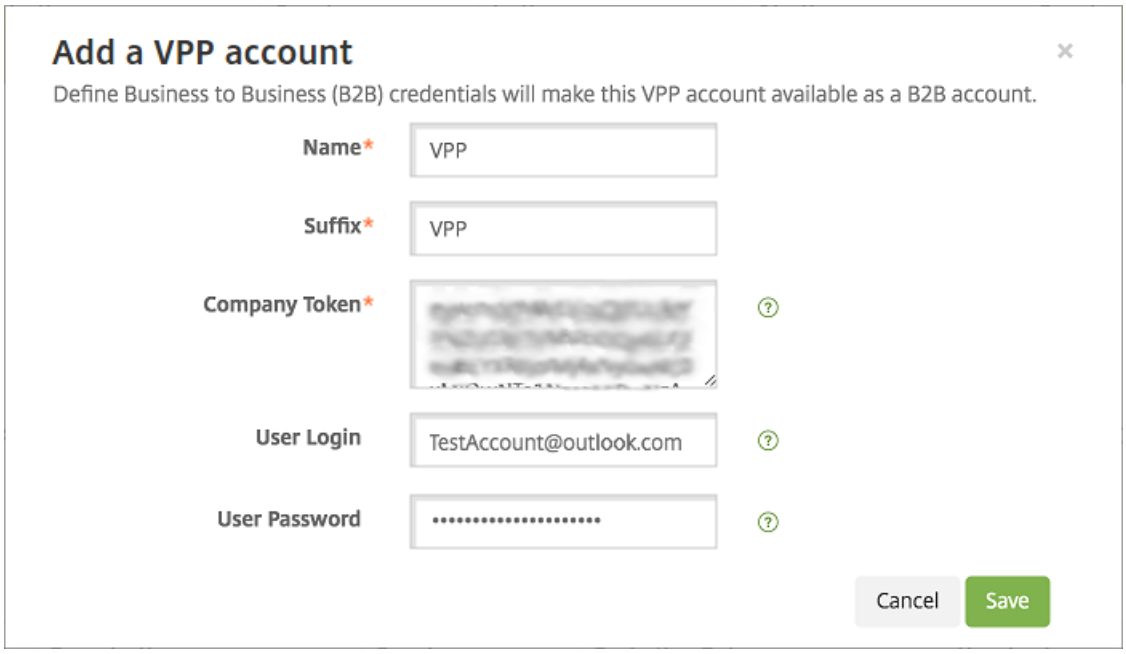
sicheren Methode gespeichert.

- **Benutzereigenschaft für VPP-Länderzuordnung**: Geben Sie einen Code ein, um das Herunterladen aus landesspezifischen App-Stores zuzulassen.

  Diese Zuweisung wird von XenMobile 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:

Hinweis: Wenn Sie Apple Configurator 1 verwenden, laden Sie eine Lizenzdatei wie folgt hoch: Gehen Sie zu **Konfigurieren > Apps**, rufen Sie eine Plattformseite auf und erweitern Sie **Programm für Volumenlizenzen (VPP)**.

- **Name**: Geben Sie einen Namen für das VPP-Konto ein.
- **Suffix**: Geben Sie das Suffix ein, das mit dem Namen von Apps angezeigt werden soll, die über das VPP-Konto erworben wurden. Beispiel: Bei Eingabe von **VPP** wird die App Secure Mail in der Anwendungsliste als **Secure Mail - VPP** angezeigt.
- **Unternehmenstoken**: Kopieren Sie das von Apple erhaltene VPP-Diensttoken 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 des Administrators eines autorisierten VPP-Kontos ein, das für den Import von benutzerdefinierten B2B-Apps verwendet wird.
- **Benutzerkennwort**: Geben Sie optional das Administratorkennwort für das VPP-Konto ein.

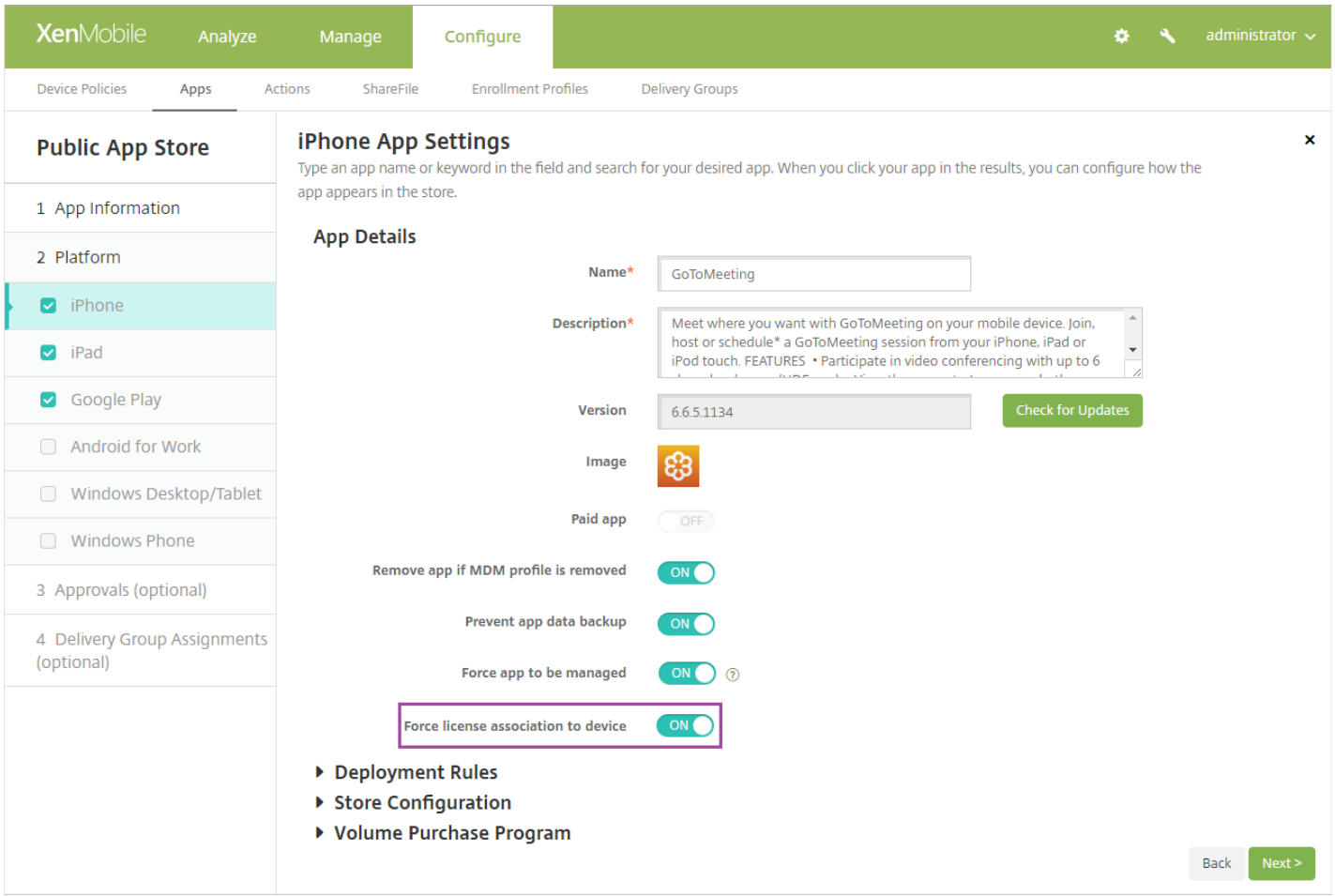
5. Klicken Sie auf **Speichern**, um das Dialogfeld zu schließen.

6. Klicken Sie auf **Speichern**, um die iOS-Einstellungen zu speichern.

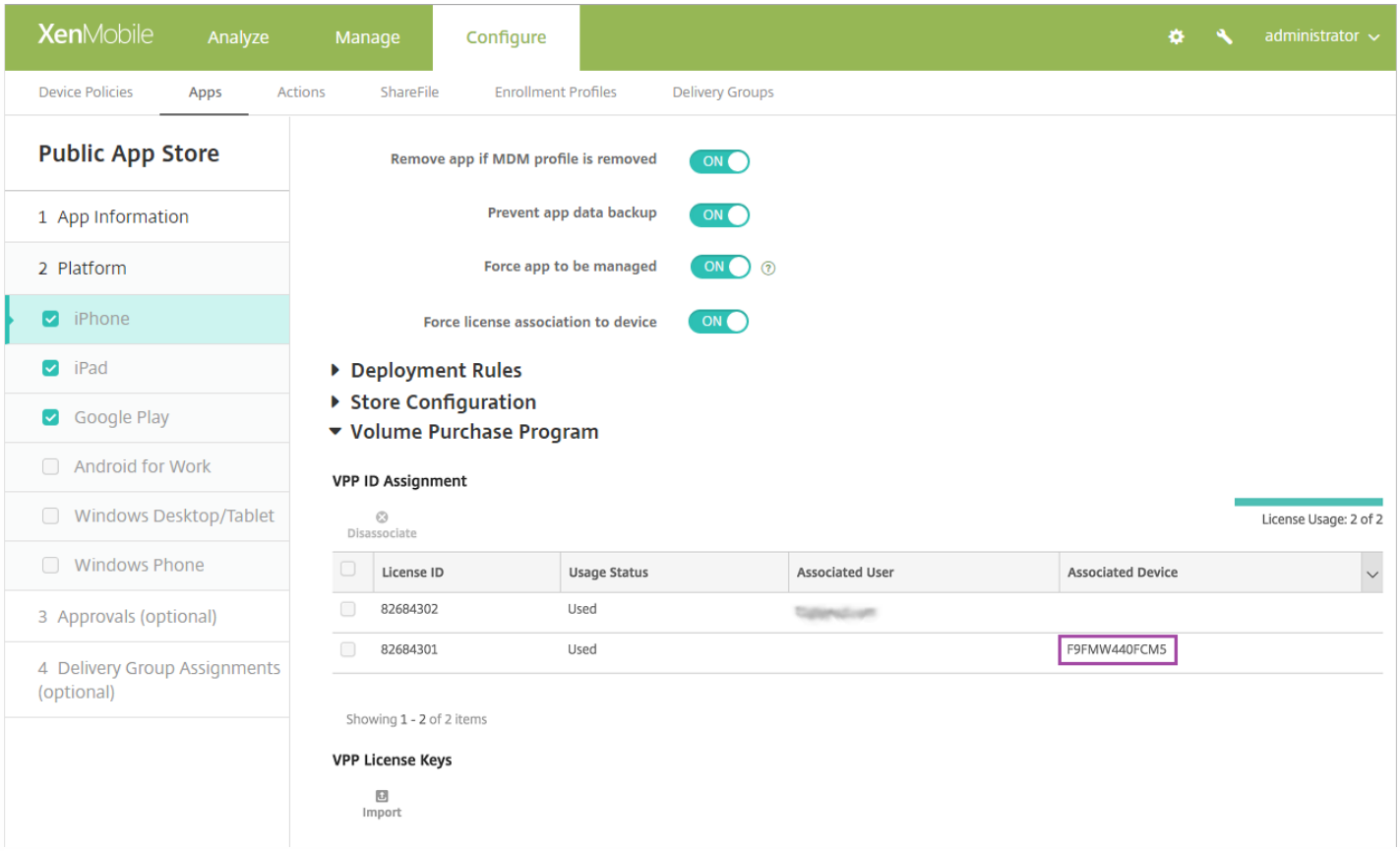
Es wird nun gemeldet, dass die Apps in XenMobile der Liste auf der Seite **Konfigurieren > Apps** hinzugefügt werden. Auf der Seite **Konfigurieren > Apps** werden die Namen der aus Ihrem VPP-Konto erhaltenen Apps mit dem von Ihnen angegebenen Suffix angezeigt.

Sie können jetzt die Einstellungen für VPP-Apps konfigurieren und anschließend die Richtlinieneinstellungen für Bereitstellungsgruppen und Geräte für die VPP-Apps. Wenn Sie diese Konfiguration abgeschlossen haben, können Benutzer ihre Geräte registrieren. Die folgenden Hinweise sollten bei diesen Verfahren berücksichtigt werden.

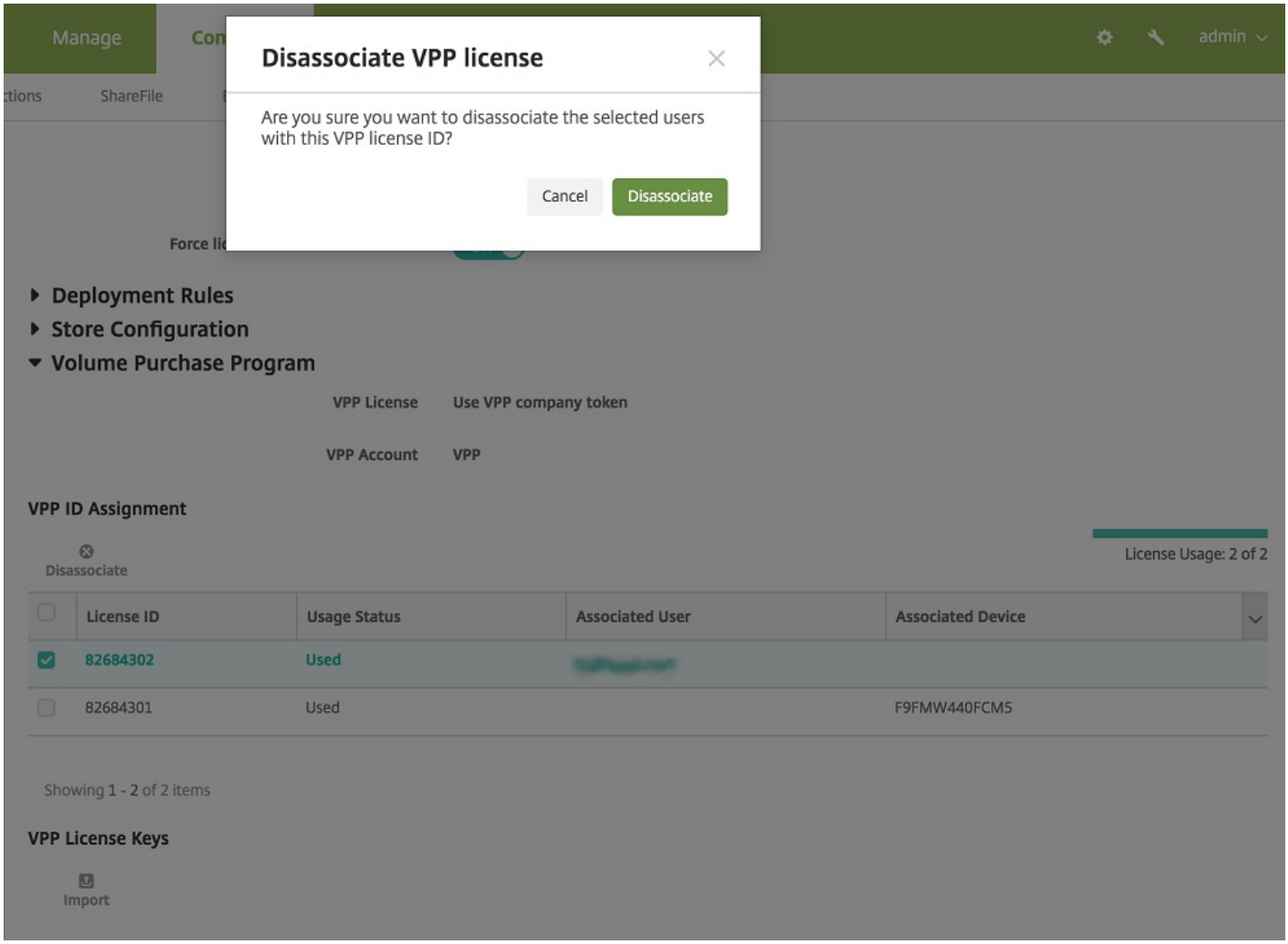
- Beim Konfigurieren der VPP-App-Einstellungen (**Konfigurieren > Apps**) aktivieren Sie **Lizenzzuordnung zu Gerät erzwingen**. Ein Vorteil der Verwendung des VPP und DEP von Apple für betreute Geräte besteht in der Möglichkeit, Apps über XenMobile auf Geräteebene anstatt auf Benutzerebene zuzuweisen. Damit muss kein Gerät mit Apple-ID verwendet werden, die Benutzer erhalten keine Einladung zur Teilnahme beim VPP-Programm und sie können Apps ohne Anmeldung bei ihrem iTunes-Konto herunterladen.



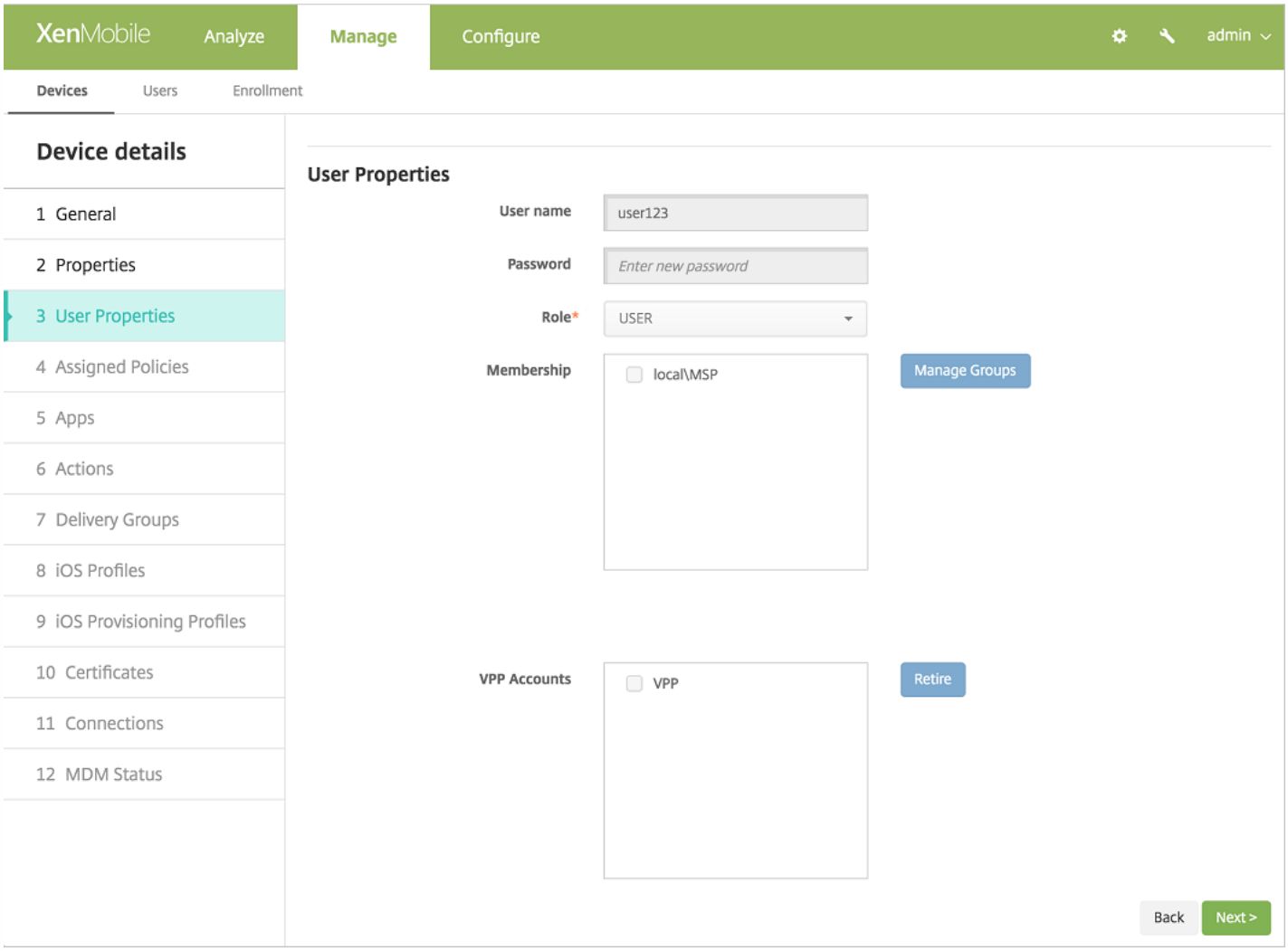
Erweitern Sie zum Anzeigen der VPP-Info für eine App **Programm für Volumenlizenzen (VPP)**. In der Tabelle **VPP-ID Zuweisung** ist die Lizenz einem Gerät zugeordnet. Die Geräteseriennummer wird in der Spalte **Zugeordnetes Gerät** angezeigt. Wenn der Benutzer das Token entfernt und es dann wieder importiert, wird anstelle der Seriennummer aufgrund von Apple-Datenschutzeinschränkungen **ausgeblendet** angezeigt.



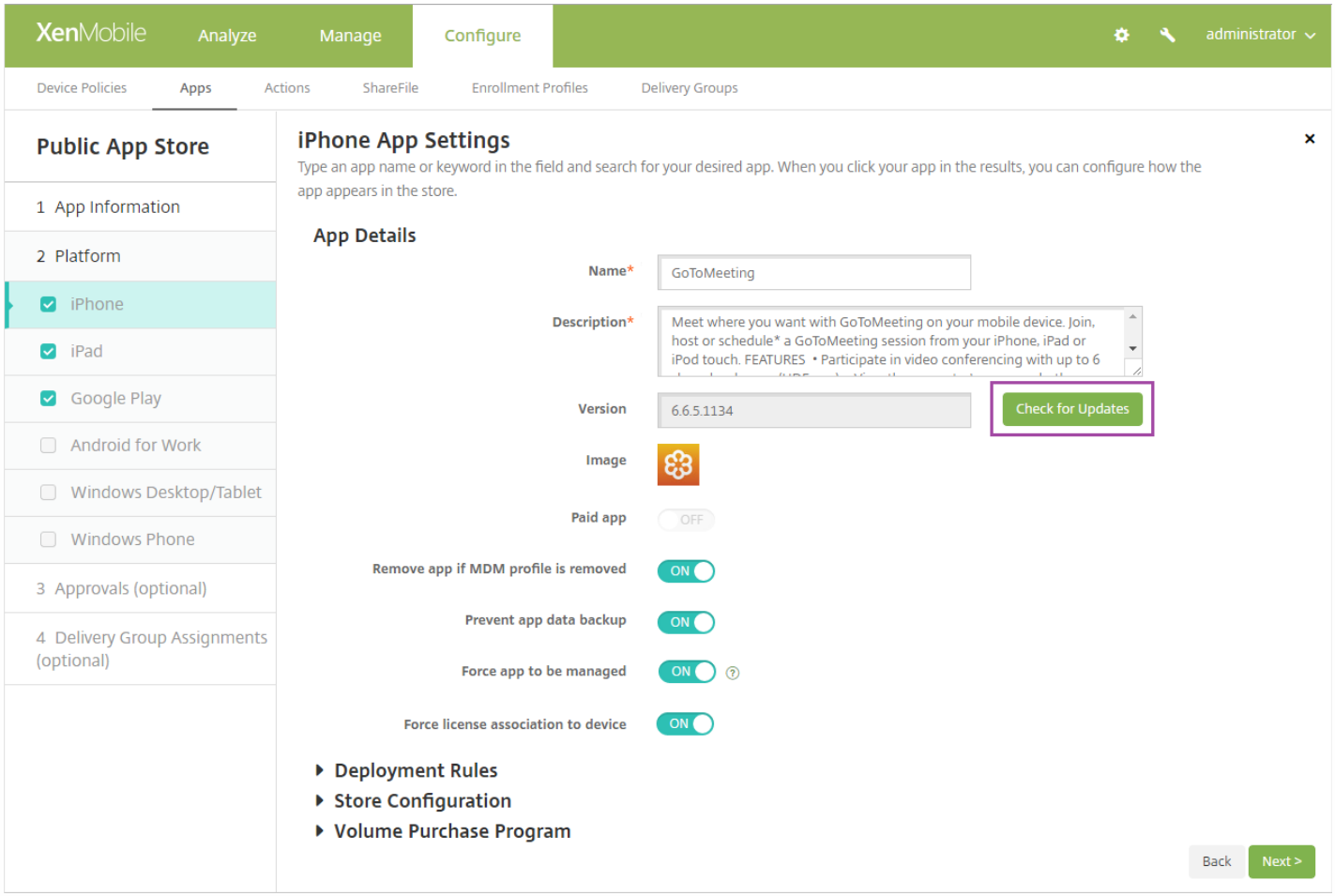
Um eine Lizenzzuweisung aufzuheben, klicken Sie auf die Zeile der Lizenz und dann auf **Zuweisung aufheben**.



Wenn Sie VPP-Lizenzen Benutzern zuordnen, integriert XenMobile Benutzer in Ihr VPP-Konto und ordnet deren iTunes-ID dem VPP-Konto zu. Die iTunes-ID der Benutzer wird dem Unternehmen und dem XenMobile-Server nie angezeigt. Apple erstellt die Zuweisung transparent, um den Datenschutz für die Benutzer zu gewährleisten. Sie können einen Benutzer aus dem VPP-Programm entfernen, um die Zuweisung aller Lizenzen des Benutzerkontos aufzuheben. Zum Entfernen eines Benutzers gehen Sie zu **Verwalten > Geräte**.



- Wenn Sie eine App einer Bereitstellungsgruppe zuweisen wird diese in XenMobile standardmäßig als optionale App behandelt. Um sicherzustellen, dass XenMobile die App Geräten bereitstellt, gehen Sie zu **Konfigurieren > Bereitstellungsgruppen** und verschieben Sie auf der Seite **Apps** die App in die Liste **Erforderliche Apps**.
- Wenn ein Update für eine App aus einem öffentlichen Store verfügbar wird und die App per Push über das VPP installiert wurde, wird sie auf Geräten nicht automatisch, sondern erst dann aktualisiert, wenn nach Updates gesucht und die Updates angewendet werden. Beispiel: Zum Installieren per Push eines Updates für Secure Hub (bei Zuweisung zu Geräten und nicht Benutzern) klicken Sie unter **Konfigurieren > Apps** auf einer Plattformseite auf **Nach Updates suchen** und wenden Sie das Update an.



XenApp und XenDesktop über Citrix Secure Hub

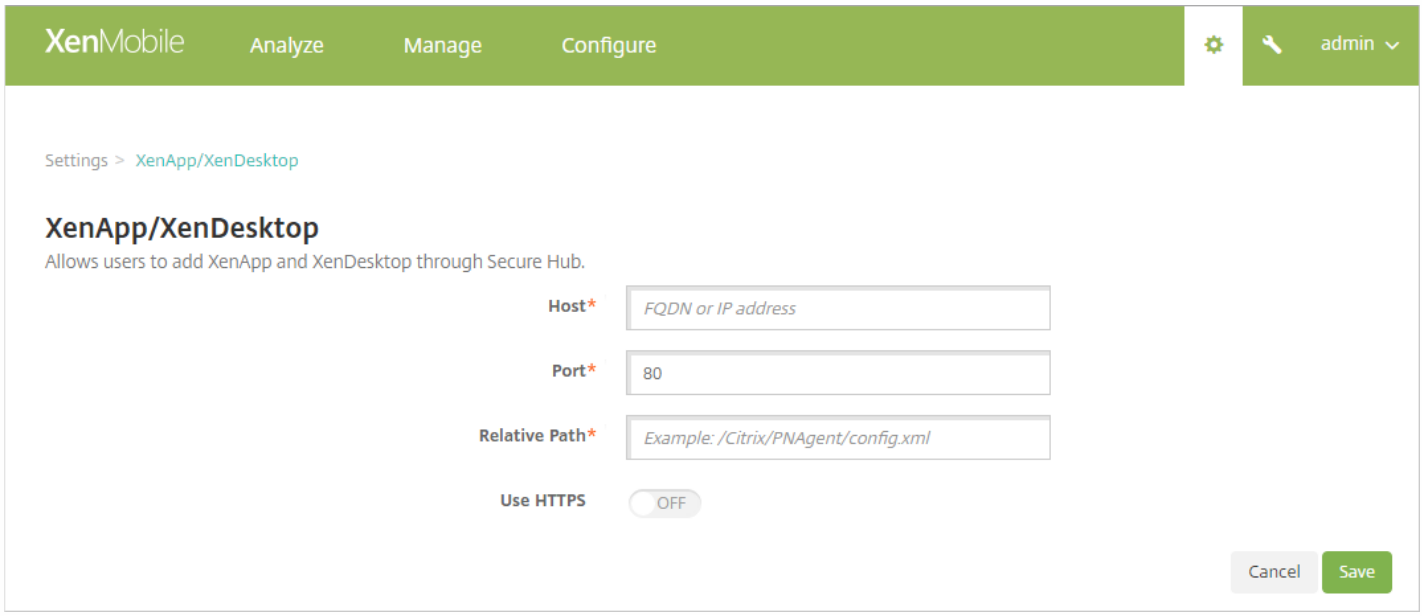
Feb 24, 2017

XenMobile kann Apps aus XenApp und XenDesktop sammeln und Benutzern von Mobilgeräten im XenMobile Store zur Verfügung stellen. Die Benutzer abonnieren Apps direkt im XenMobile Store und starten sie über Secure Hub. Citrix 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**.

Bereitstellen von Ressourcen

Feb 24, 2017

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 doppelte oder widersprüchliche 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 Geräterichtlinien angeben, um die Bereitstellung dieser Elemente zu steuern. Sie können festlegen, dass eine Bereitstellung sofort, zu einem bestimmten Datum und einer bestimmten Uhrzeit oder basierend auf Bereitstellungsbedingungen stattfindet.

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

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

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

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

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

Berechnungsschritte:

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

Bereitstellungszeitplan gelten. Der Sortieralgorithmus ist wie folgt:

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

b. Bei einem Gleichstand zwischen Bereitstellungsgruppen werden Ressourcen von Bereitstellungsgruppen nach dem Bereitstellungsgruppennamen sortiert. Beispiel: Ressourcen von Bereitstellung Gruppe A werden vor denen aus Bereitstellungsgruppe B einsortiert.

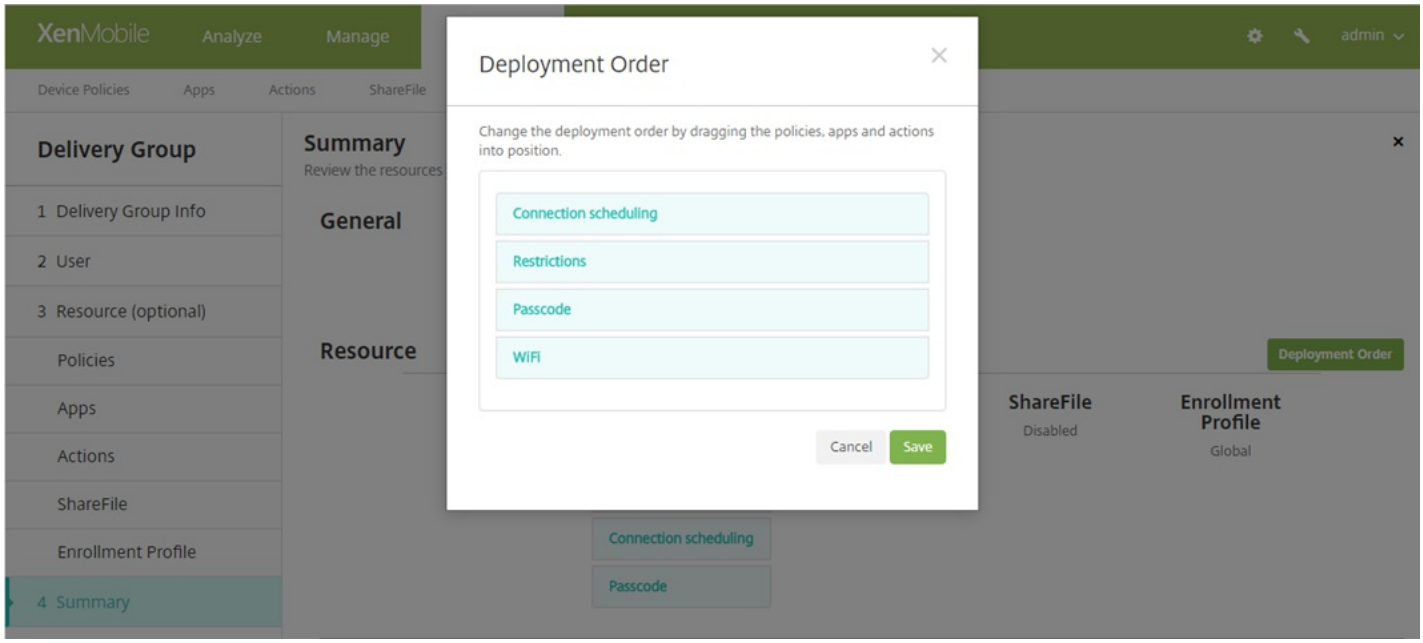
c. Wurde eine benutzerdefinierte Bereitstellungsreihenfolge für Ressourcen in einer Bereitstellungsgruppe angegeben, muss sie beim Sortieren erhalten bleiben. Sonst die Ressourcen in der Bereitstellungsuppe nach Ressourcenname sortieren.

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

Ressourcen, denen eine benutzerdefinierte Reihenfolge zugeordnet ist, werden vor Ressourcen bereitgestellt, für die keine benutzerdefinierte Reihenfolge festgelegt wurde. Eine Ressource kann in mehreren dem Benutzer zugewiesenen Bereitstellungsgruppen sein. Wie oben erwähnt werden durch den Berechnungsalgorithmus redundante Ressourcen entfernt und nur die erste Ressource der Liste bereitgestellt. Durch dieses Entfernen doppelter Ressourcen erzwingt XenMobile die vom XenMobile-Administrator festgelegte Reihenfolge.

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.

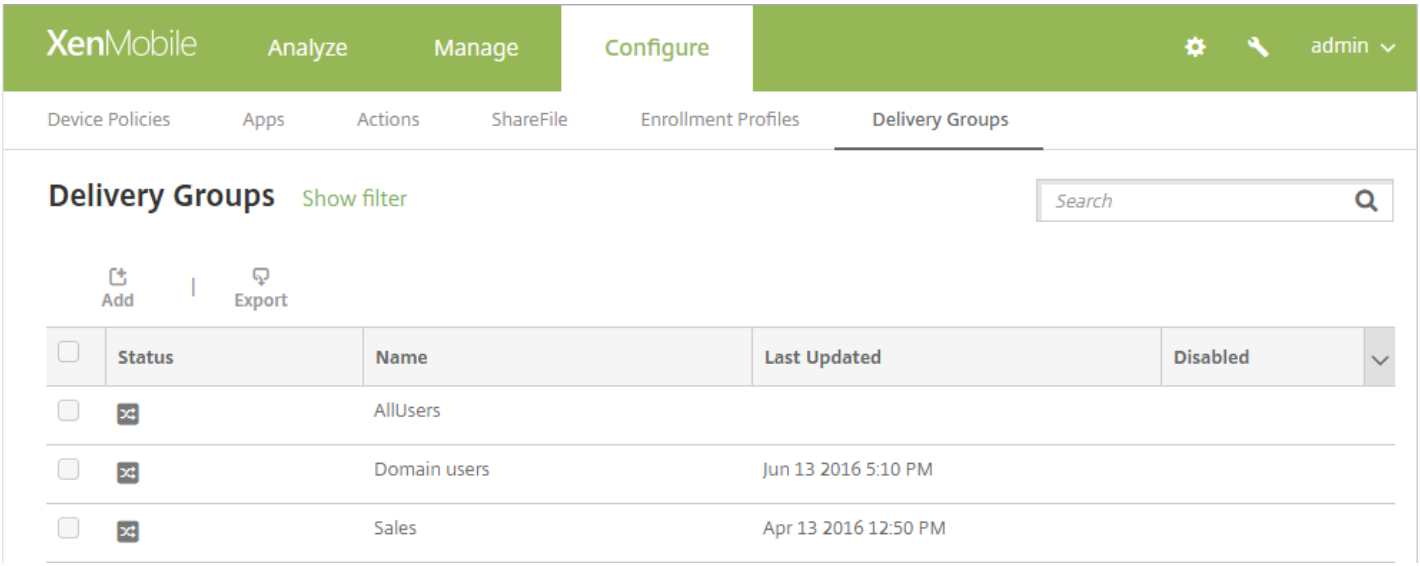


Würden Bereitstellungsgruppen durch den Algorithmus nur nach Namen sortiert, dann würde die Bereitstellung beginnend mit der Bereitstellungsgruppe "Kontomanager 1" in der Reihenfolge **WiFi**, **Passcode**, **Verbindungszeitplan**, **Einschränkungen**

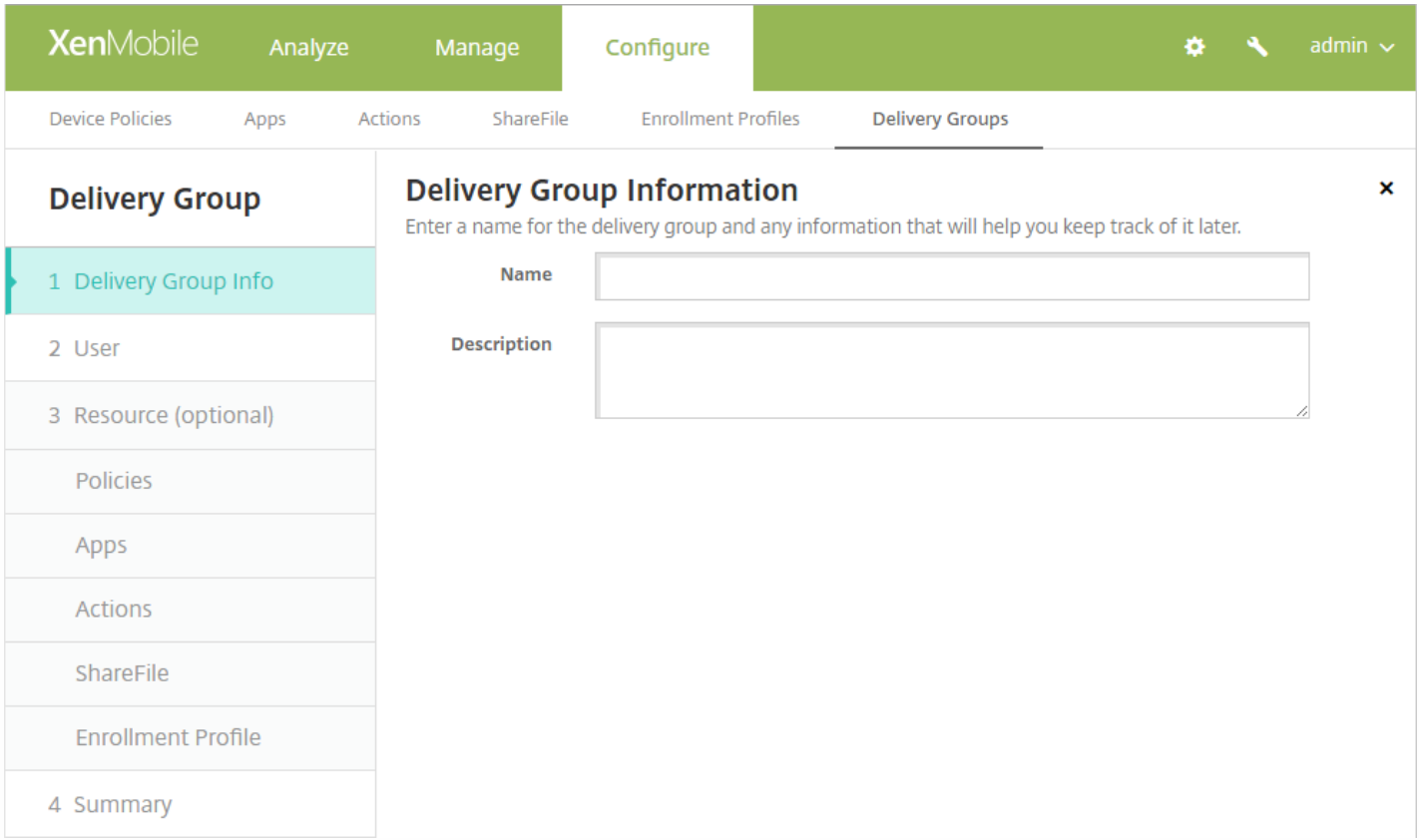
erfolgen. Die Richtlinien **Passcode** und **WiFi** für die Bereitstellungsgruppe "Kontomanager 2" würden als Duplikate ignoriert.

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.

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



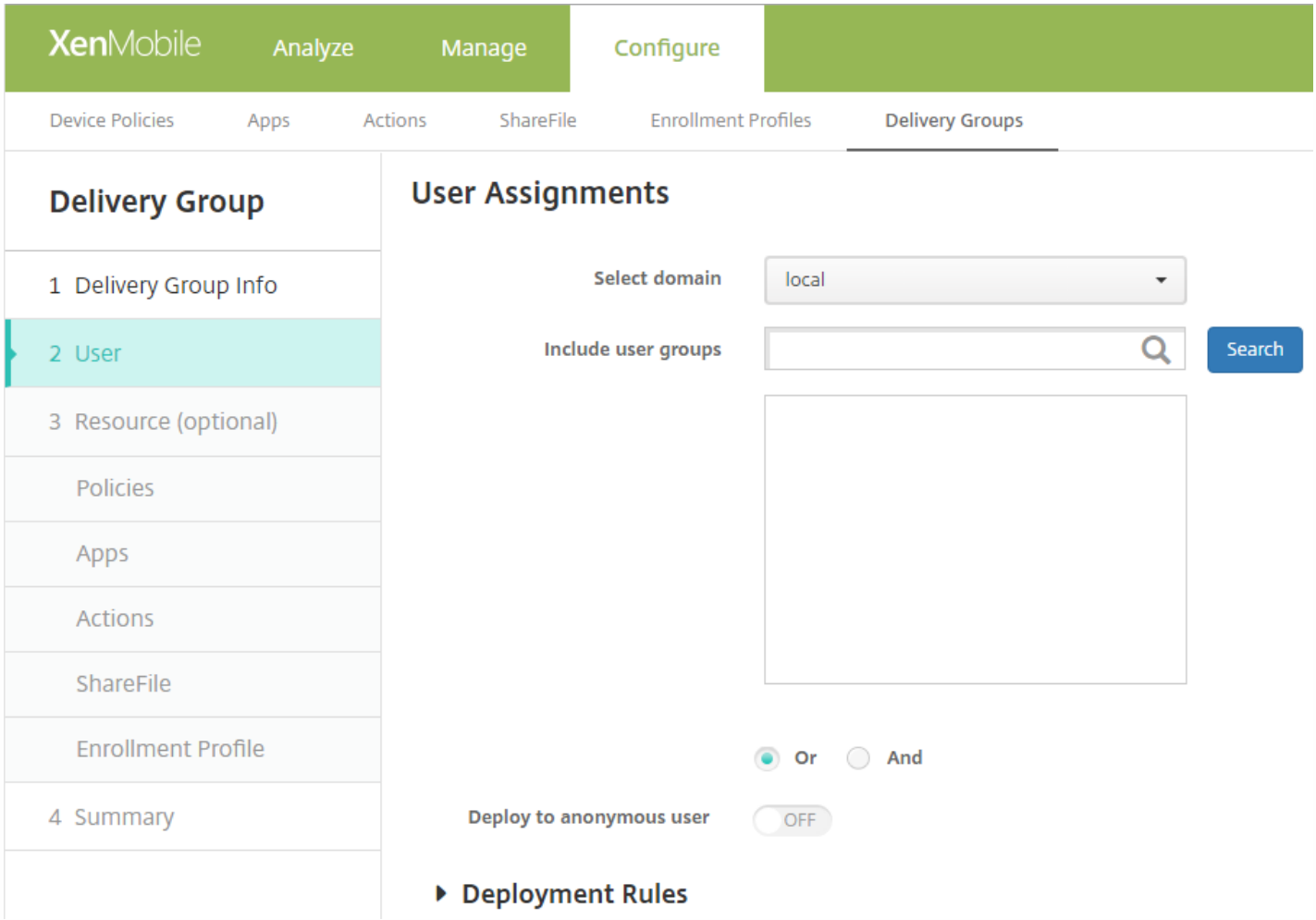
2. Klicken Sie auf der Seite **Bereitstellungsgruppen** auf **Hinzufügen**. Die Seite **Bereitstellungsgruppeninformationen** wird angezeigt.



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 anzuzeigen. 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).

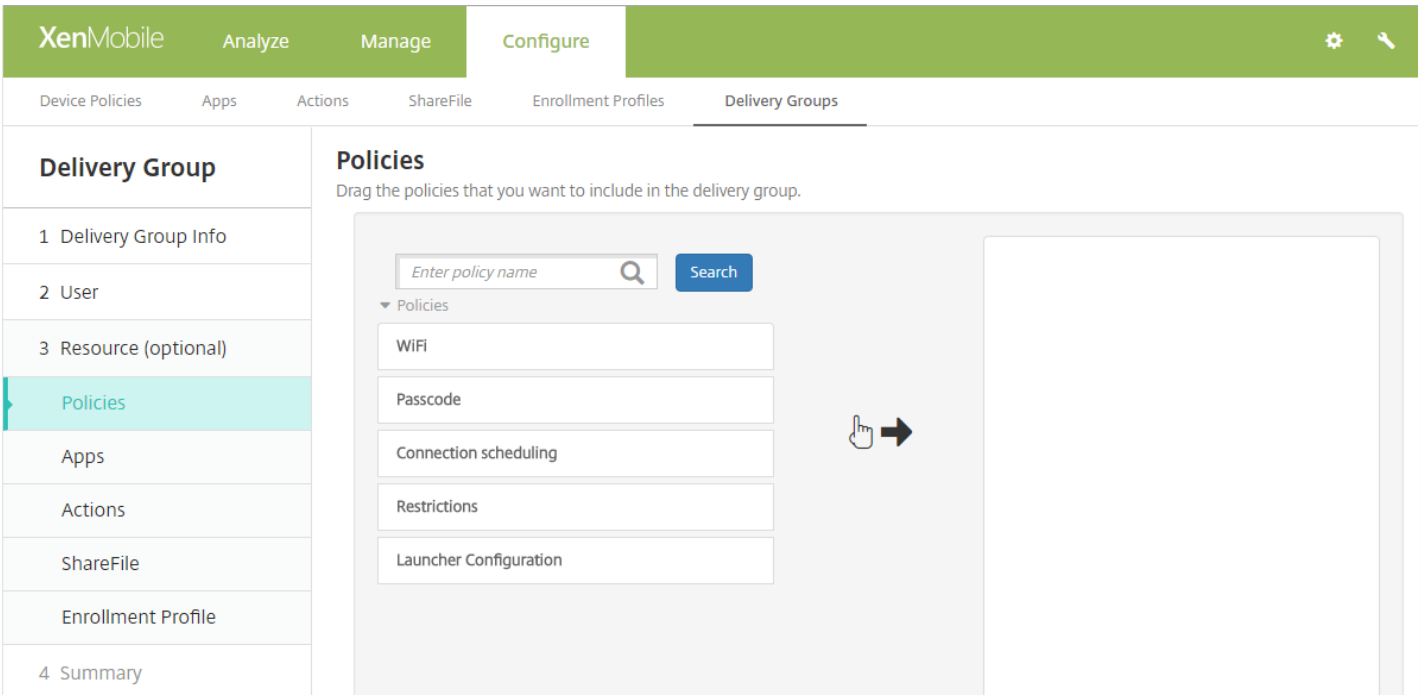
- **Für anonyme Benutzer bereitstellen**: Wählen Sie aus, ob die Bereitstellung auch für nicht authentifizierte Benutzer in der Bereitstellungsgruppe erfolgen soll.

  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

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. Zum Überspringen einer Ressource klicken Sie auf **Zusammenfassung**.

Hinzufügen von Richtlinien



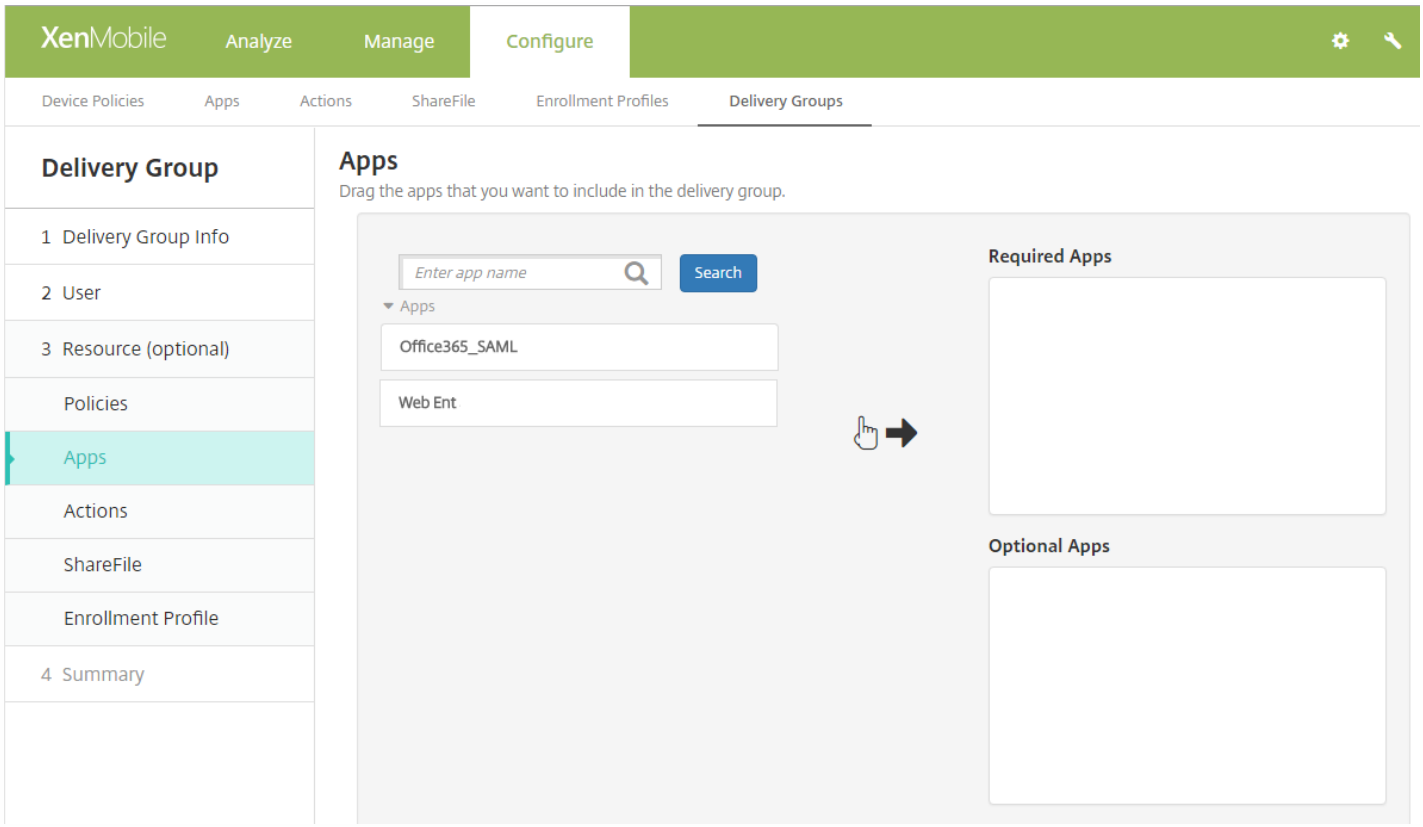
1. Führen für jede Richtlinie, die Sie hinzufügen möchten, folgende Schritte aus:

- 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



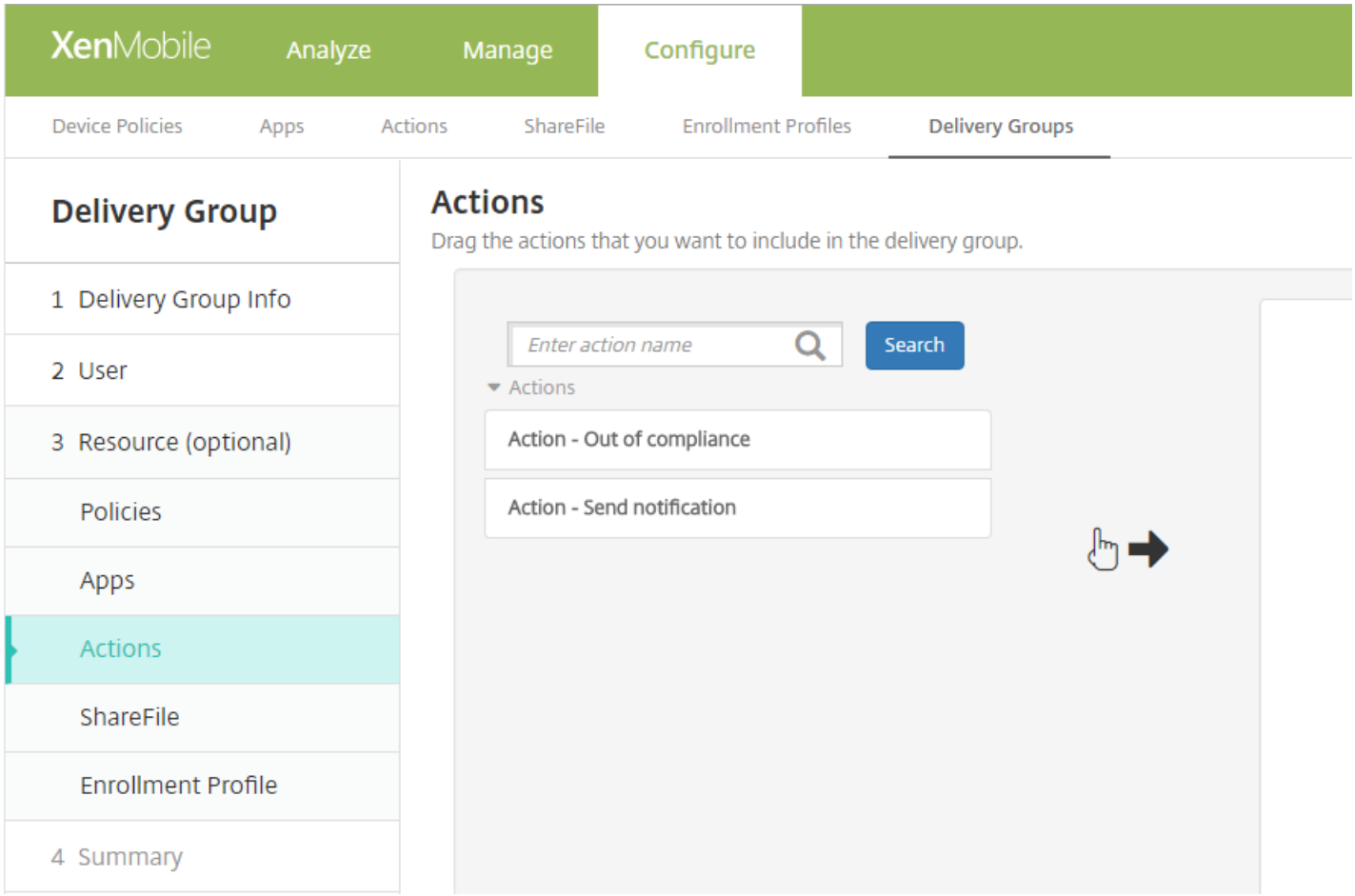
1. Führen für jede App, die Sie hinzufügen möchten, folgende Schritte aus:

- 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



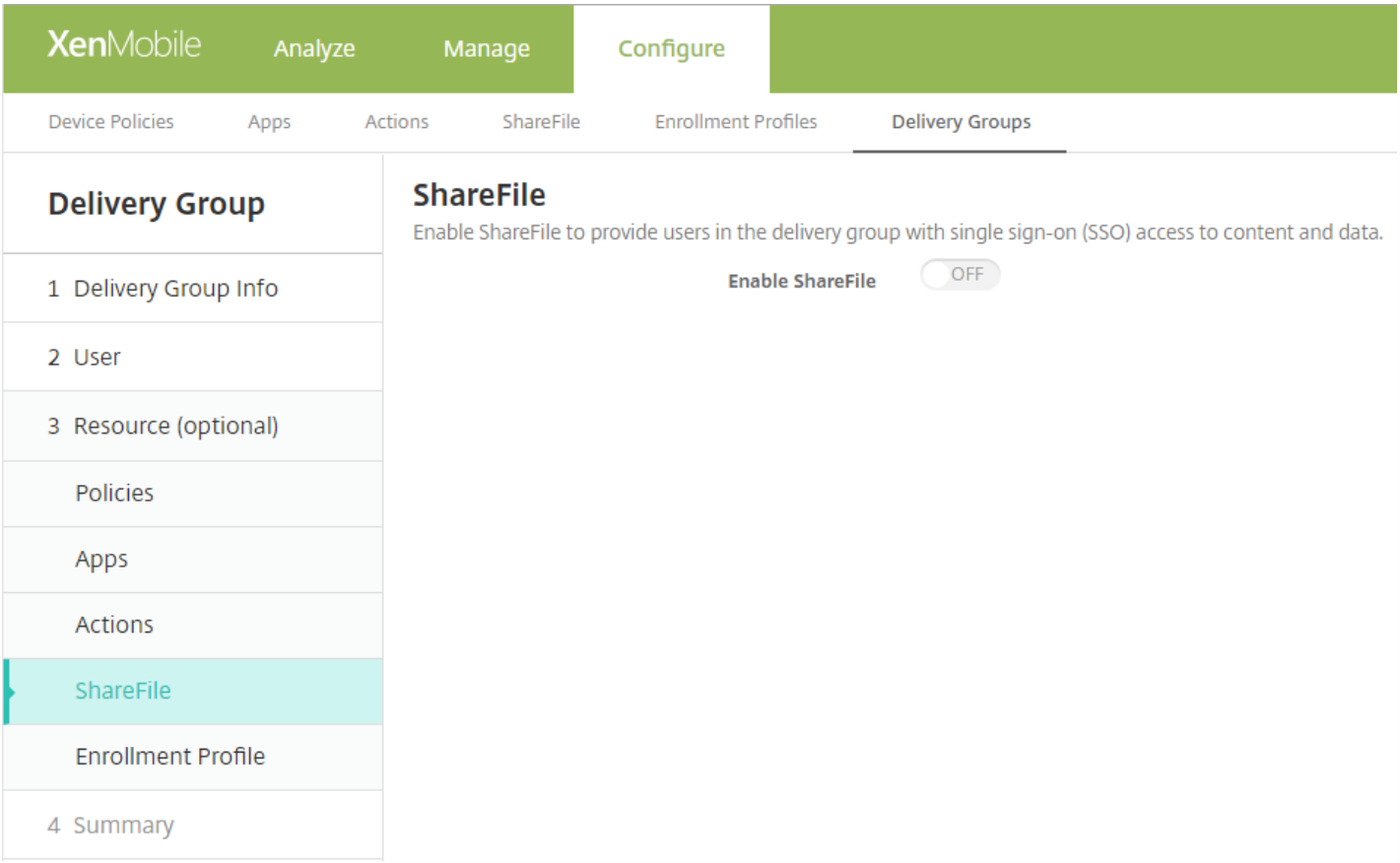
1. Führen für jede Aktion, die Sie hinzufügen möchten, folgende Schritte aus:

- 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.

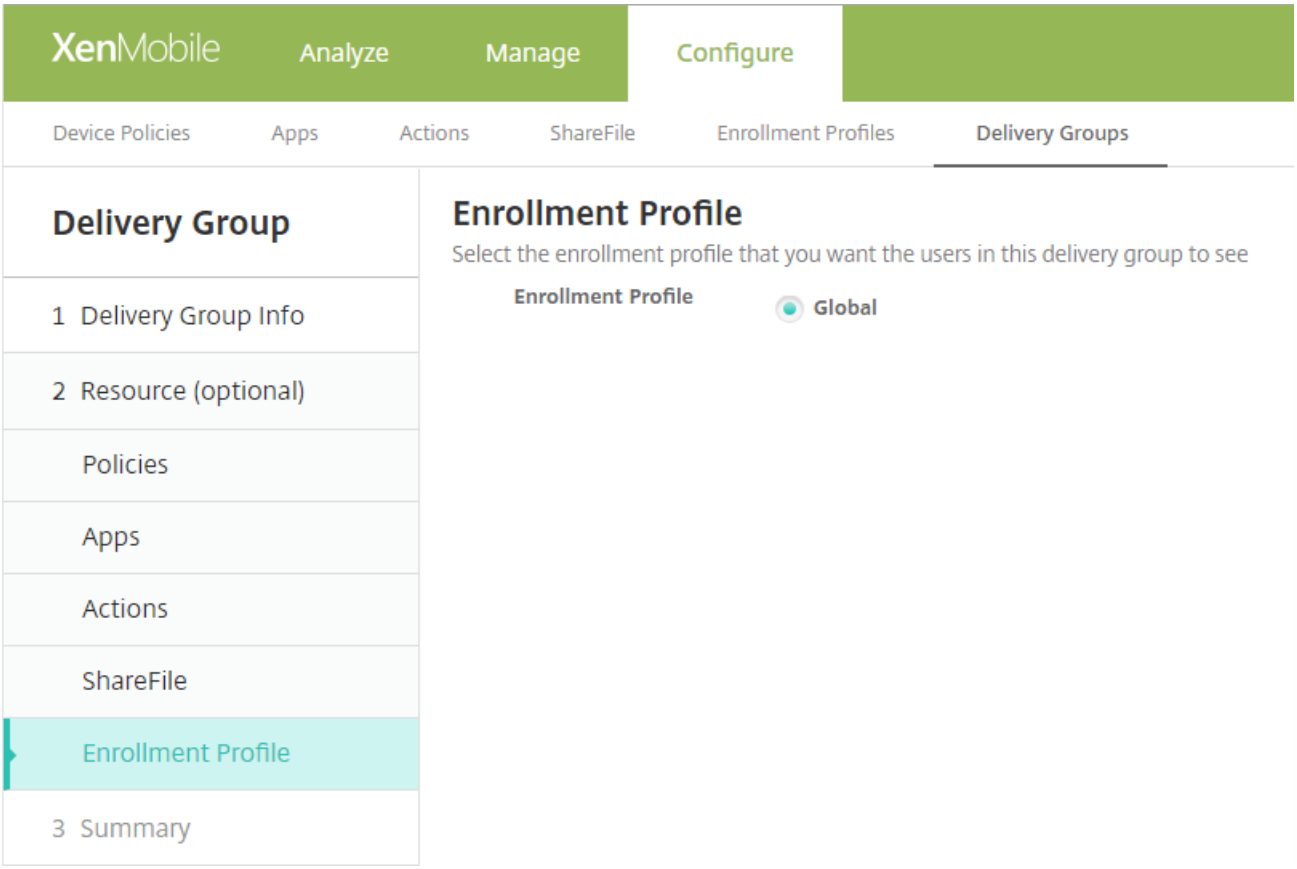
ShareFile aktivieren



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.

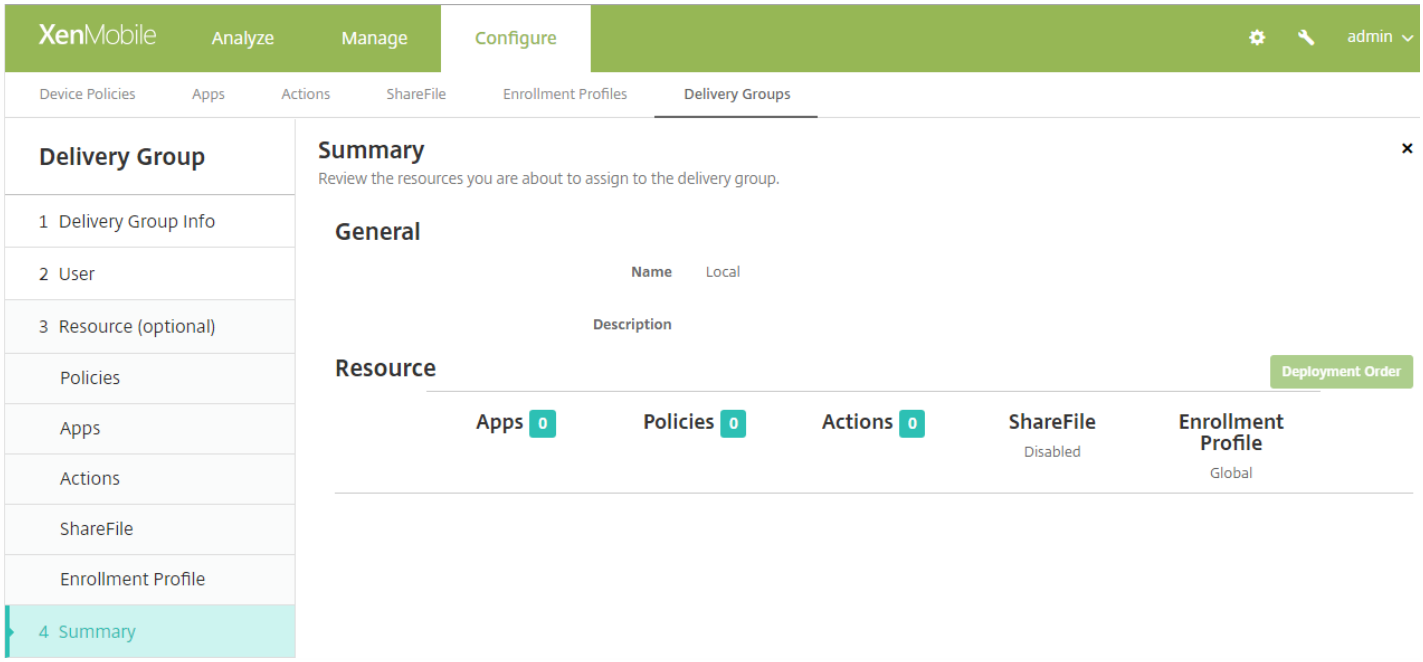
2. Klicken Sie auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt.



1. Konfigurieren Sie folgende Einstellung:

- **Registrierungsprofil**: Wählen Sie ein Registrierungsprofil aus. Anweisungen zum Erstellen von Registrierungsprofilen finden Sie unter Geräteregistrierungslimit.

2. Klicken Sie auf **Weiter**. Die Zusammenfassungsseite wird angezeigt.



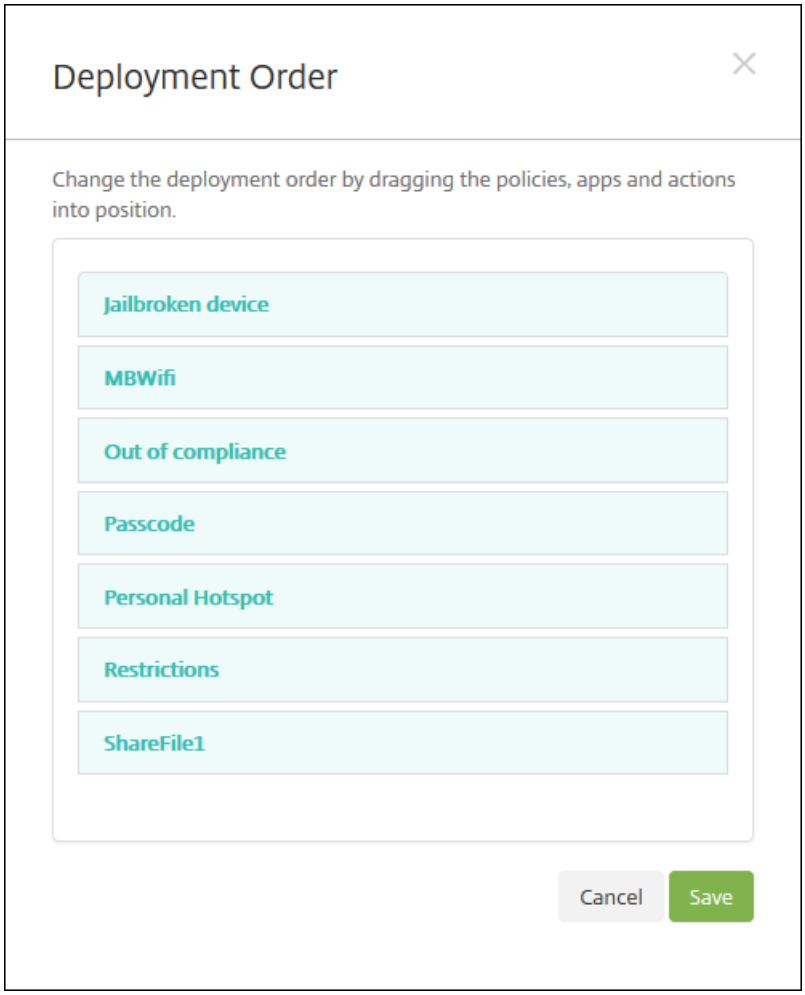
Auf der Seite **Zusammenfassung** können Sie die Optionen überprüfen, die Sie für die Bereitstellungsgruppe konfiguriert haben, und die Bereitstellungsreihenfolge der Ressourcen ändern. Auf der Seite "Zusammenfassung" werden die Ressourcen nach Kategorie angezeigt. Die Bereitstellungsreihenfolge ist hier nicht ersichtlich.

1. Klicken Sie auf **Zurück**, um auf vorherige Seiten aufzurufen, wenn Sie Änderungen vornehmen müssen.

2. Klicken Sie auf **Bereitstellungsreihenfolge**, um die Reihenfolge anzuzeigen und ggf. zu ändern.

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

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.

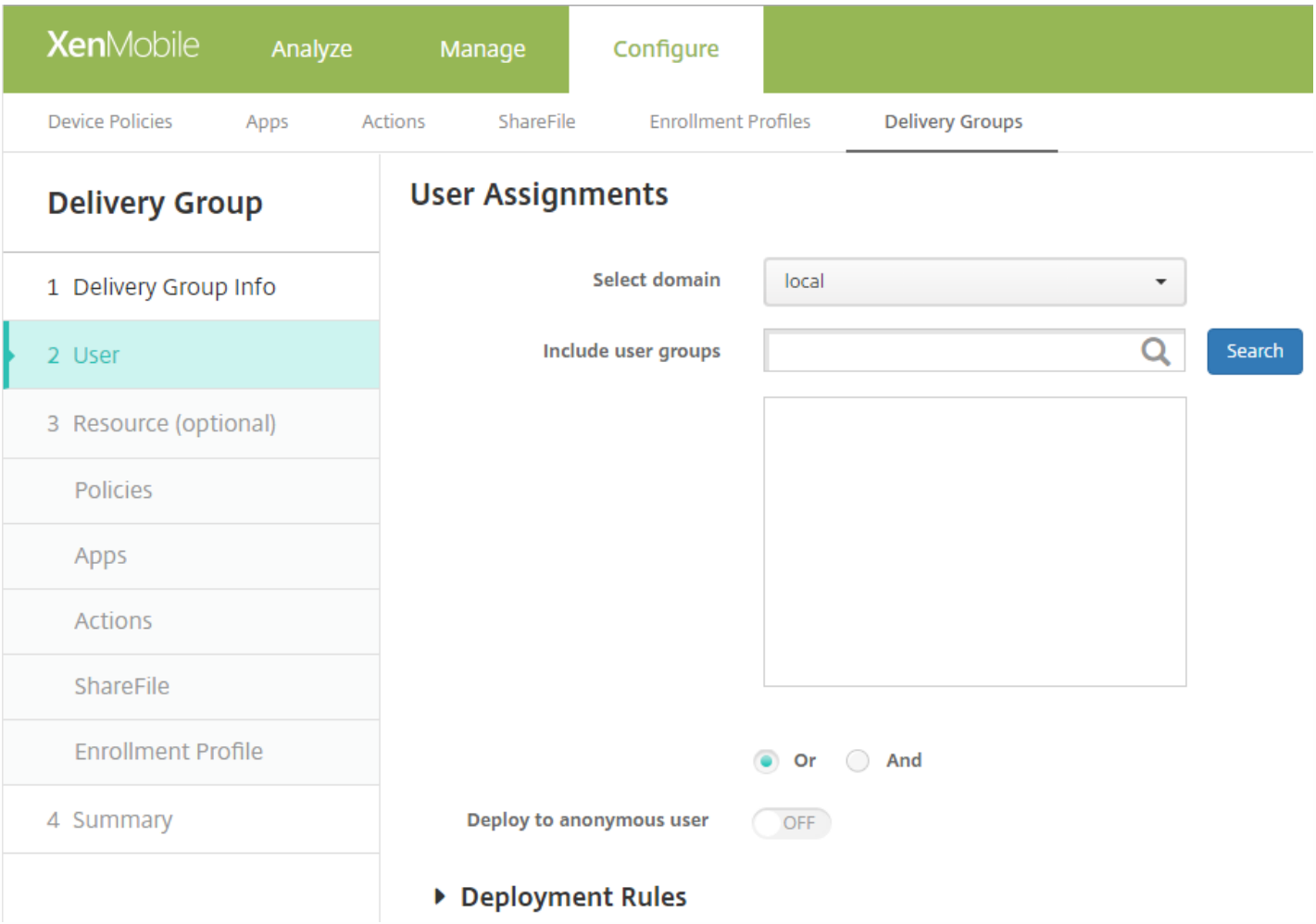
1. Wählen Sie auf der Seite **Bereitstellungsgruppen** die gewünschte Bereitstellungsgruppe aus, indem Sie auf das Kontrollkästchen neben ihrem Namen oder auf die Zeile mit ihrem Namen klicken, und klicken Sie auf **Bearbeiten**. Die Seite **Bereitstellungsgruppeninformationen** wird zur Bearbeitung 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 Bereitstellungsgruppe 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.

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.

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 XenMobile 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.
- Zur Bereitstellung für eine einzelne Bereitstellungsgruppe klicken Sie auf das Kontrollkästchen neben ihrem Namen oder auf die Zeile mit ihrem Namen.

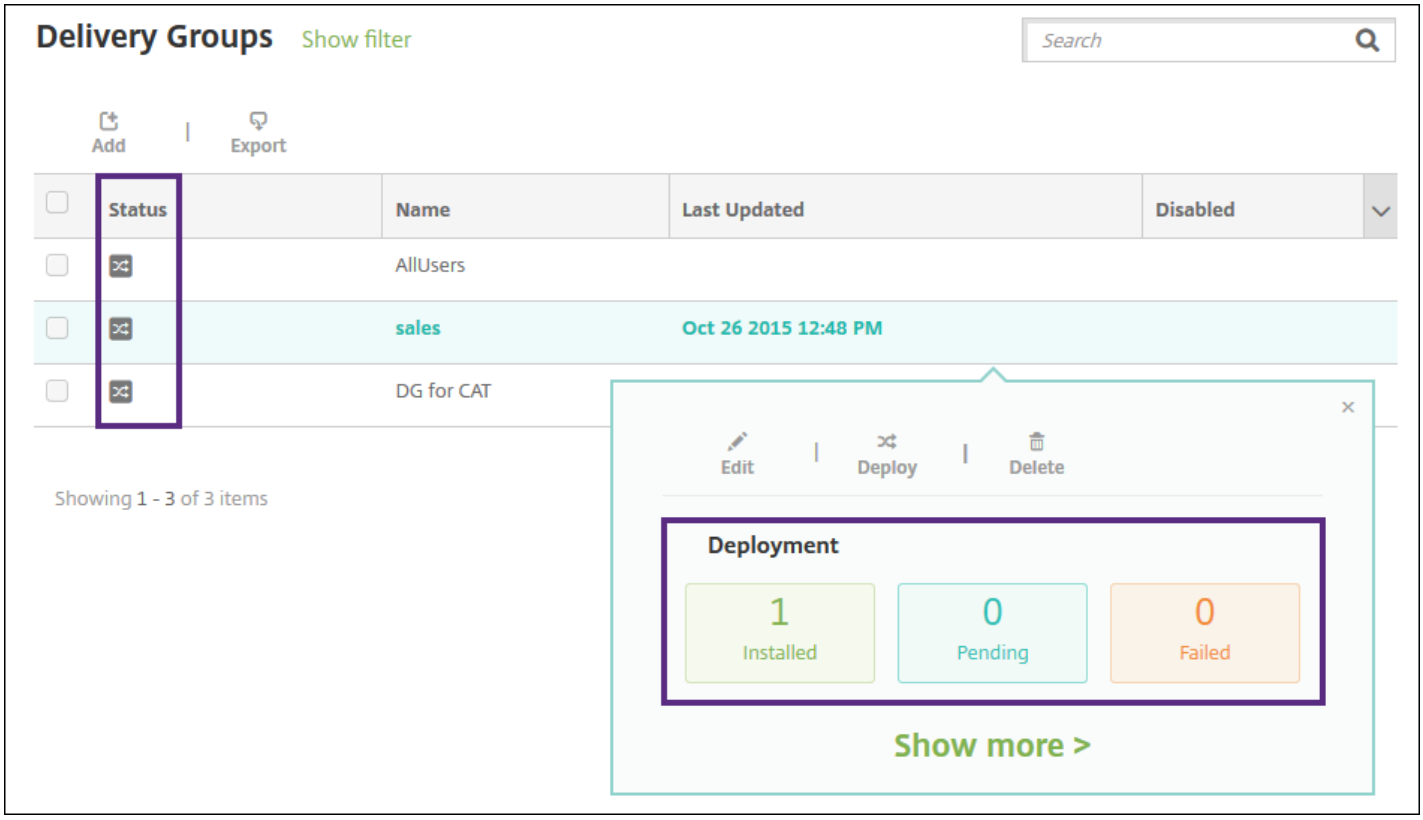
2. Klicken Sie auf **Bereitstellen**.

Hinweis: Der Befehl **Bereitstellen** wird, je nachdem wie Sie die einzelne Bereitstellungsgruppe ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

Vergewissern Sie sich, dass die Gruppen, für die Sie Apps, Richtlinien und Aktionen bereitstellen möchten, aufgelistet sind, und klicken Sie dann auf **Bereitstellen**. Die Bereitstellung von Apps, Richtlinien und Aktionen für die ausgewählten Gruppen erfolgt 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.



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.

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.

Makros

Feb 24, 2017

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

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

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

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

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

Ein Makro kann folgendes Format haben:

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

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

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

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

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

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

Automatisierte Aktionen

Apr 24, 2017

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.

Für Fälle, in denen ein Gerät auf "nicht richtlinientreu" gesetzt wird und der Benutzer entsprechende Korrekturen vornimmt, sodass das Gerät wieder den Richtlinien entspricht, müssen Sie eine Richtlinie konfigurieren, durch die ein Paket bereitgestellt wird, das das Gerät wieder auf "richtlinientreu" setzt.

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

In diesem Artikel wird erläutert, wie Sie automatisierte Aktionen in XenMobile hinzufügen, bearbeiten und filtern und wie Sie Aktionen zum Sperren und Löschen von Apps im Nur-MAM-Modus konfigurieren.

> ## 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 Erstellen und Aktualisieren von Benachrichtigungsvorlagen in XenMobile.

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.

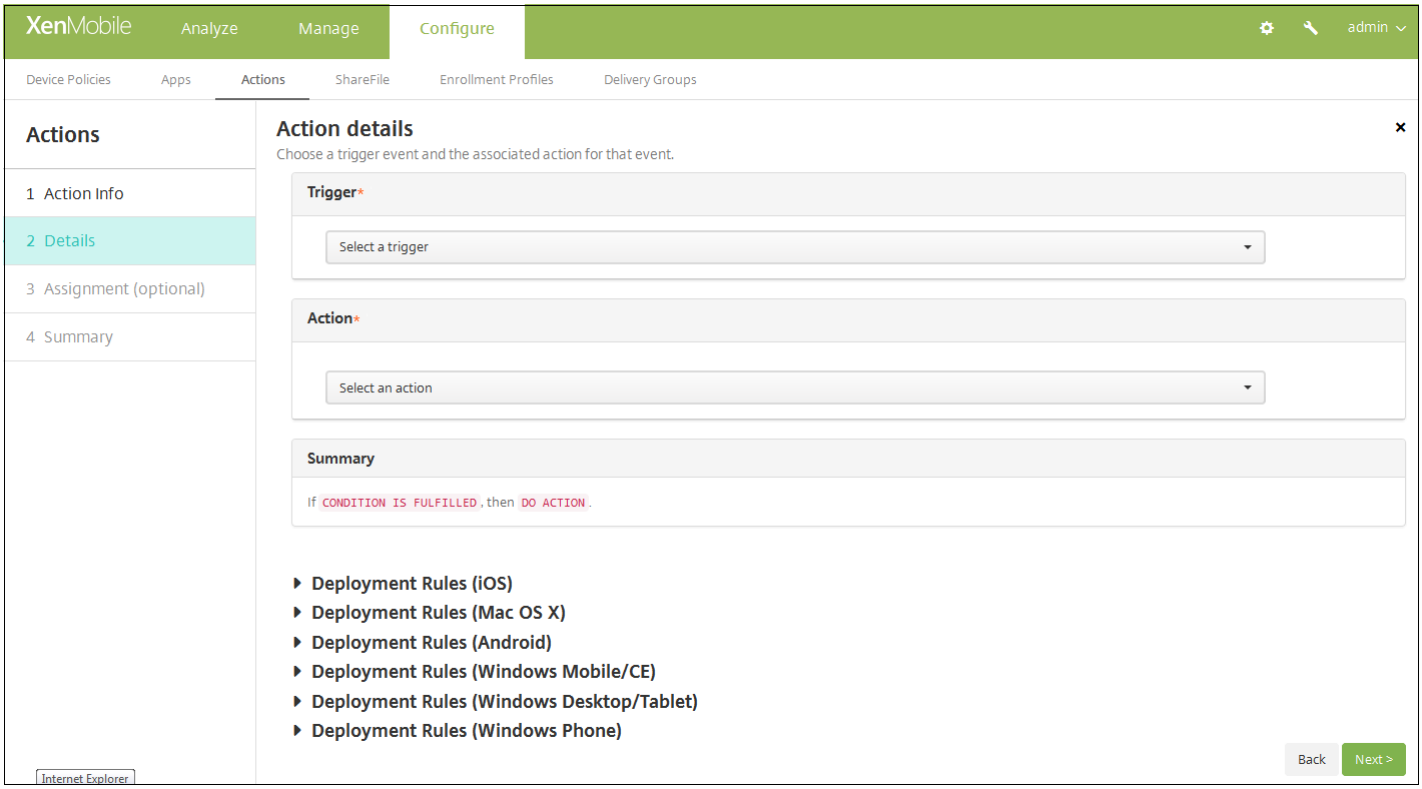
3. Die Seite **Aktionsinformationen** wird angezeigt.

4. Konfigurieren Sie auf der Seite **Aktionsinformationen** die folgenden Informationen:

- **Name**: Geben Sie einen Namen zur eindeutigen 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. Gilt nicht für den 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.

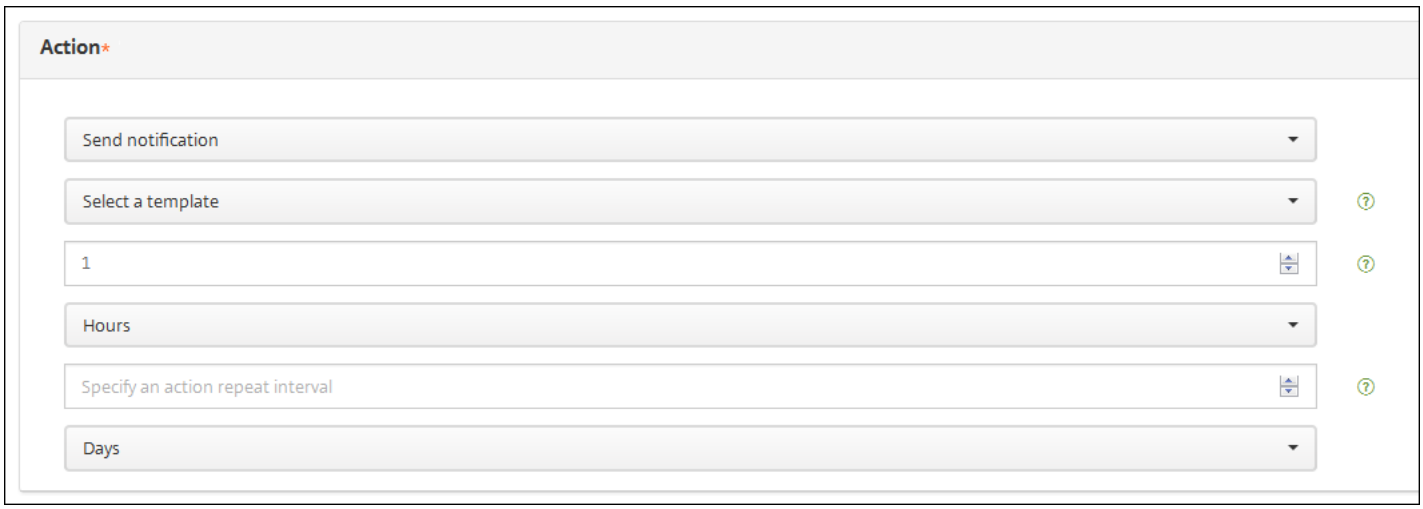
8. Klicken Sie in der Liste **Aktion** auf die Aktion, die ausgeführt werden soll, wenn das Auslösekriterium erfüllt wird. Mit Ausnahme von **Benachrichtigung senden** können Sie für alle Optionen einen Zeitraum festlegen, in dem Benutzer das für den Auslöser ursächliche Problem beheben können. Wenn 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 gegebenenfalls zugehöriger 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. Weitere Informationen finden Sie unter "Aktionen für App-Sperre und App löschen im Nur-MAM-Modus" weiter unten.
- **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.Weitere Informationen finden Sie unter "Aktionen für App-Sperre und App löschen im Nur-MAM-Modus" weiter unten.
- **Geräte als nicht richtlinientreu markieren**: Das Gerät wird als nicht richtlinientreu markiert.
- **Benachrichtigung senden**: Senden einer Nachricht an den Benutzer.

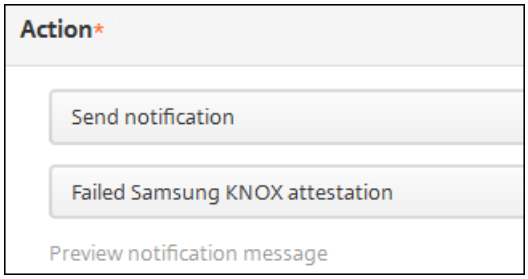
Bei Auswahl von **Benachrichtigung senden** können Sie in den restlichen Schritten dieses Verfahrens nachlesen, wie Sie eine Benachrichtigung senden.

9. Wählen Sie in der nächsten Liste die Vorlage für die Benachrichtigung aus.Für das ausgewählte Ereignis relevante Benachrichtigungsvorlagen werden angezeigt, es sei denn, für einen Benachrichtigungstyp gibt es noch keine Vorlage. In diesem Fall werden Sie aufgefordert, eine Vorlage zu konfigurieren. Erstellen Sie eine Vorlage mit der Option Benachrichtigungsvorlage in **Einstellungen**.

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 zum Einrichten von Benachrichtigungsvorlagen finden Sie unter Erstellen und Aktualisieren von Benachrichtigungsvorlagen in XenMobile.



Hinweis: Nach Auswahl der Vorlage können Sie diese in der Vorschau 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 erstellt wurde.

12. Nach dem Konfigurieren der Aktionsdetails können Sie für jede Plattform separat Bereitstellungsregeln festlegen. Führen Sie hierfür Schritt 13 für jede gewünschte Plattform aus.

13. Konfigurieren Sie die Bereitstellungsregeln.

14. Nach dem Konfigurieren der Bereitstellungsregeln für die Aktion klicken Sie auf **Weiter**.Die Zuweisungsseite **Aktionen** wird angezeigt, auf der Sie die Aktion Bereitstellungsgruppen zuweisen können. Dieser Schritt ist optional.

15. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, um nach einer Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen zur Zuweisung der Richtlinie 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. Der Standardwert ist **EIN**.Wenn Sie **AUS** wählen, müssen keine anderen Optionen konfiguriert werden.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Der Standardwert 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. Der Standardwert ist **Bei jeder Verbindung**.

- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Der Standardwert ist **AUS**. **Hinweis**: Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**. Diese Option gilt nicht für iOS.

17. Klicken Sie auf **Weiter**.Die Seite **Zusammenfassung** wird angezeigt, auf der Sie die Konfiguration der Aktion prüfen können.

18. Klicken Sie auf **Speichern**, um die Aktion zu speichern.

Sie können 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.

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** eine Aktion.

Berücksichtigen Sie bei diesem Schritt Folgendes:

Wenn der Auslösertyp **Ereignis** und der Wert nicht **Active Directory, deaktivierter Benutzer** ist, werden die Aktionen **App löschen** und **App sperren** nicht angezeigt.

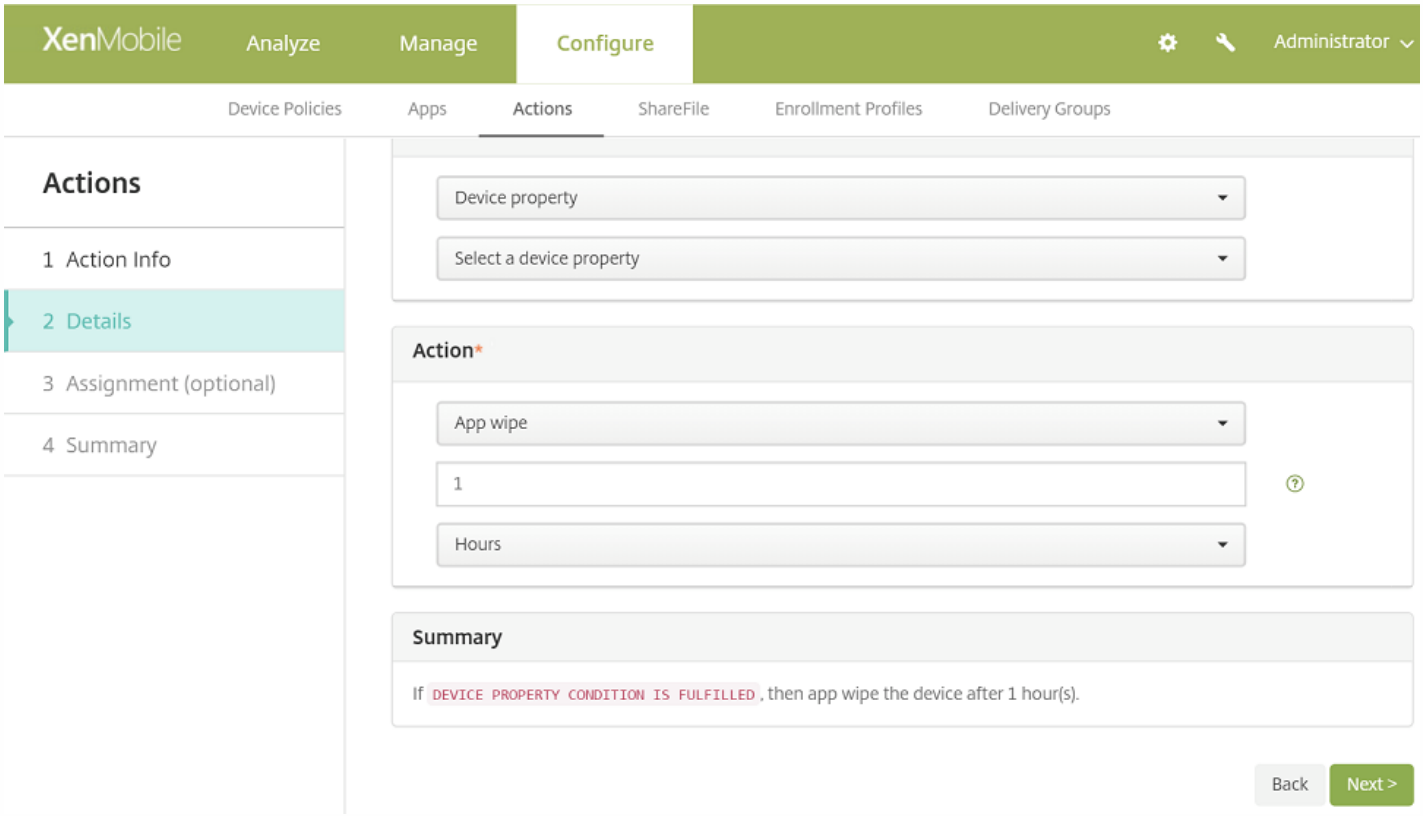
Wenn der Auslöser **Geräteeigenschaft** und der Wert **MDM-Modus 'Verloren' aktiviert** ist, werden die folgenden Aktionen nicht angezeigt:

- Gerät selektiv löschen
- Gerät vollständig löschen
- Gerät widerrufen

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 Konfigurieren von Rollen mit RBAC.

> ## Hinweis
>
> Wenn Sie den Auslöser auf **Ereignis** festlegen, wird als Wiederholungsintervall automatisch mindestens 1 Stunde festgelegt. Das Gerät muss eine Aktualisierung der Richtlinien zur Synchronisierung mit dem Server ausführen, damit Benachrichtigung empfangen werden. Normalerweise erfolgt die Synchronisierung eines Geräts mit dem Server, wenn der Benutzer sich anmeldet oder die Richtlinien manuell über Secure Hub aktualisiert.

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



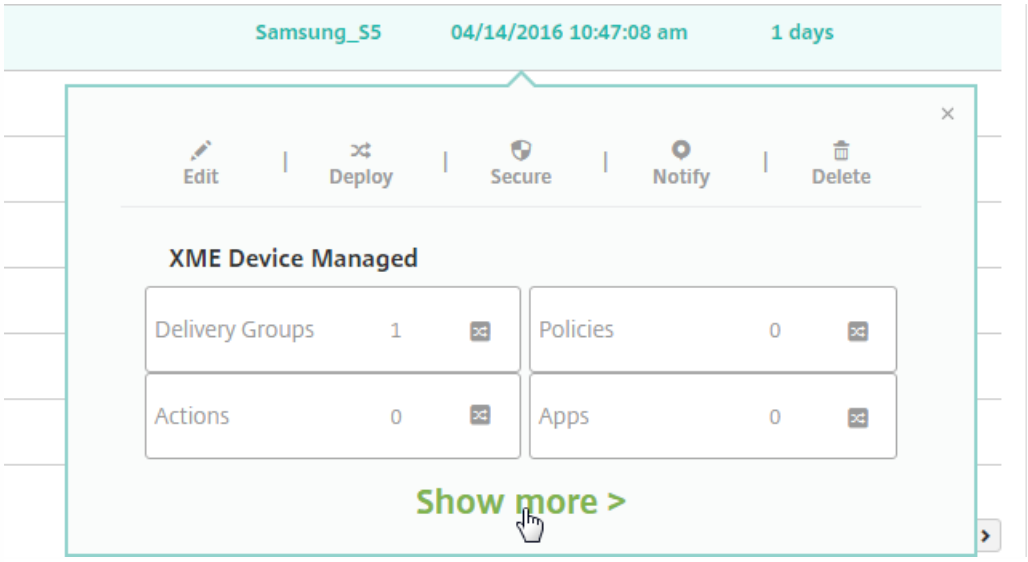
6. Konfigurieren Sie die Bereitstellungsregeln und klicken Sie auf **Weiter**.

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

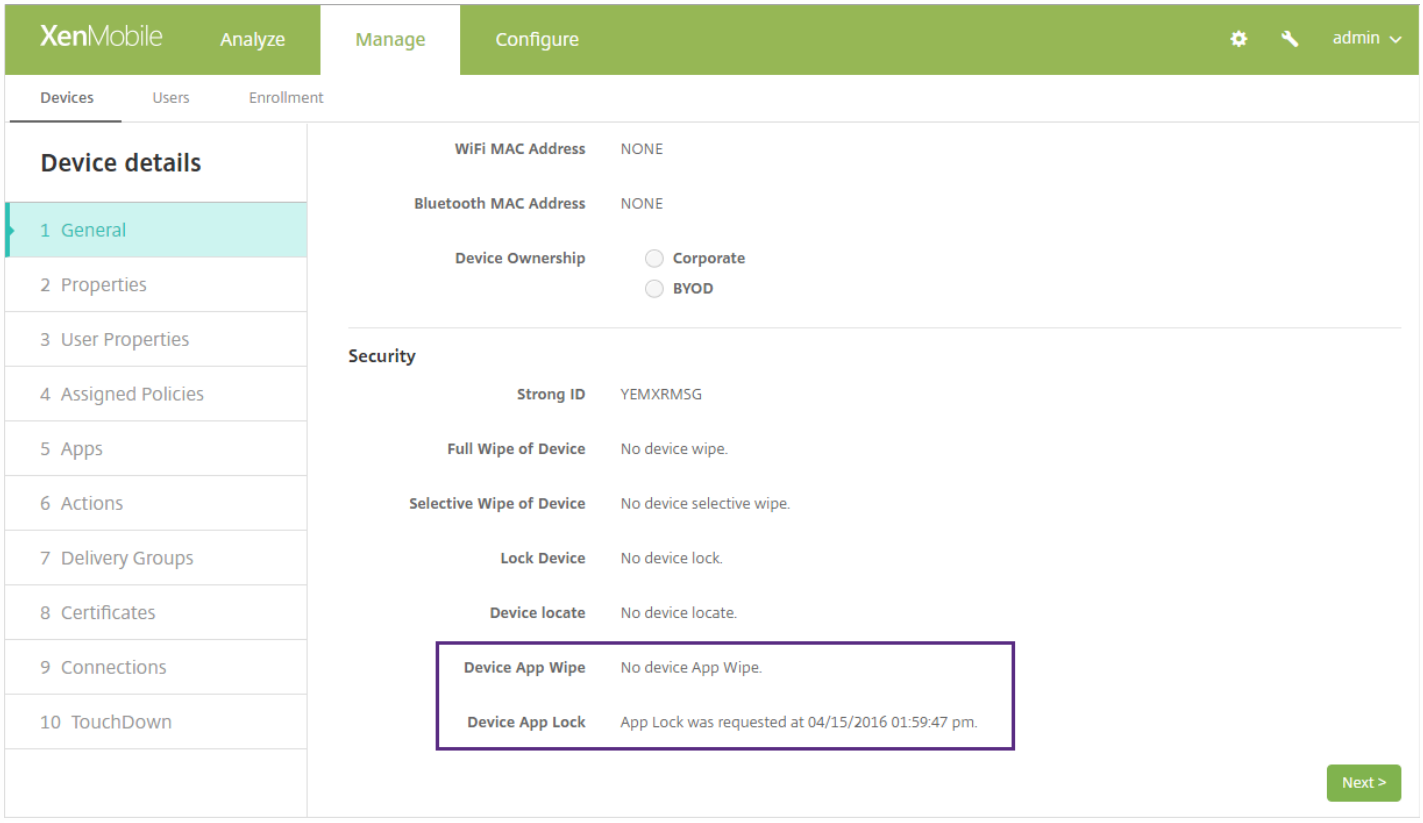
8. Klicken Sie auf **Speichern**.

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.



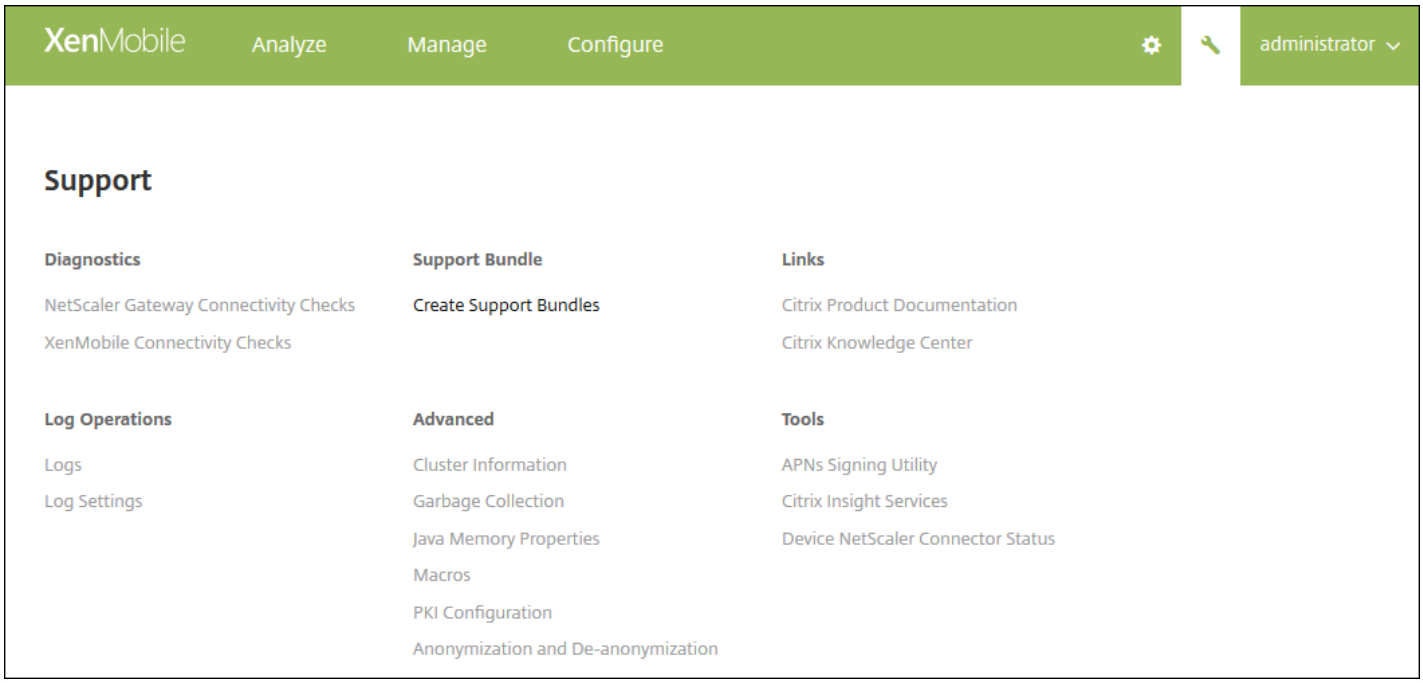
Überwachen und Support

Feb 24, 2017

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

Berichte

Apr 24, 2017

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

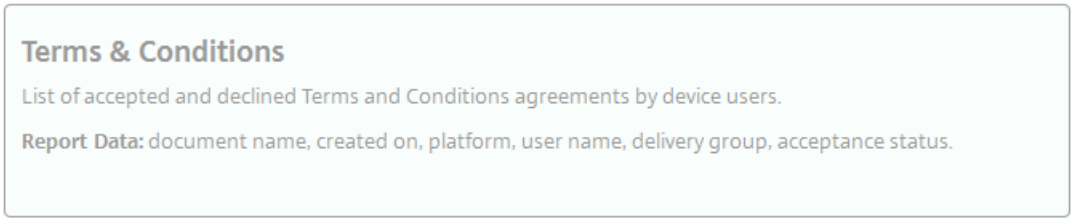
- **Apps nach Geräten & Benutzer**: Liste der verwalteten Apps, die Benutzer auf ihren Geräten haben In diesem Bericht sind nicht die persönlichen, auf dem Gerät installierten Apps enthalten.
- **AGB**: Benutzerliste mit Informationen dazu, ob die Benutzer die AGB akzeptiert oder abgelehnt haben
- **Top 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 aller registrierten Geräte
- **Apps nach Plattform**: Liste der Apps und App-Versionen sortiert nach Geräteplattform und -version
- **Gesperrte Apps nach Geräten & Benutzer**: Liste der gesperrten Apps, die Benutzer auf ihren Geräten haben
- **Geräte & Apps**: Liste der Geräte, auf denen verwaltete Apps ausgeführt werden

Die Berichte haben das CSV-Format und können mit Programmen wie Microsoft Excel geöffnet werden.

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.

Alle Berichte enthalten eine Beschreibung der Informationen, die in dem Bericht gesammelt werden, und die spezifischen Berichtsdaten. Beispiel:



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.

Die folgende Abbildung enthält einen Teil des Berichts "Top 25 Apps" wie er in Microsoft Excel angezeigt wird:

	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORIES	AVAILABLE_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	GoToMeeting	6.6.4.1127	Default	10/17/2016 14:21		7	7	0	0	Public App Store
3	Secure Web - Inception	10.4.0-11	Default	10/17/2016 14:37	citrix.com	7	6	0	1	MDX
4	Secure Mail	10.4.1-221	Default	10/17/2016 16:06	citrix.com	6	5	0	1	MDX
5	Twitter	6.64	appstore	10/17/2016 17:04		3	3	0	0	Public App Store
6	Salesforce1	11.0.3	Default	12/14/2016 17:52		2	2	0	0	Public App Store

Important

Benutzerdefinierte Berichte können zwar mit SQL Server erstellt werden, dies wird von Citrix jedoch nicht empfohlen. Die Verwendung der SQL Server-Datenbank auf diese Weise kann unvorhersehbare Konsequenzen für die XenMobile-Bereitstellung haben. Wenn Sie diese Methode der Berichterstellung verwenden möchten, verwenden Sie für SQL-Abfragen ein Konto mit Nur-Lesezugriff.

Mobilfunkanbieter

Feb 24, 2017

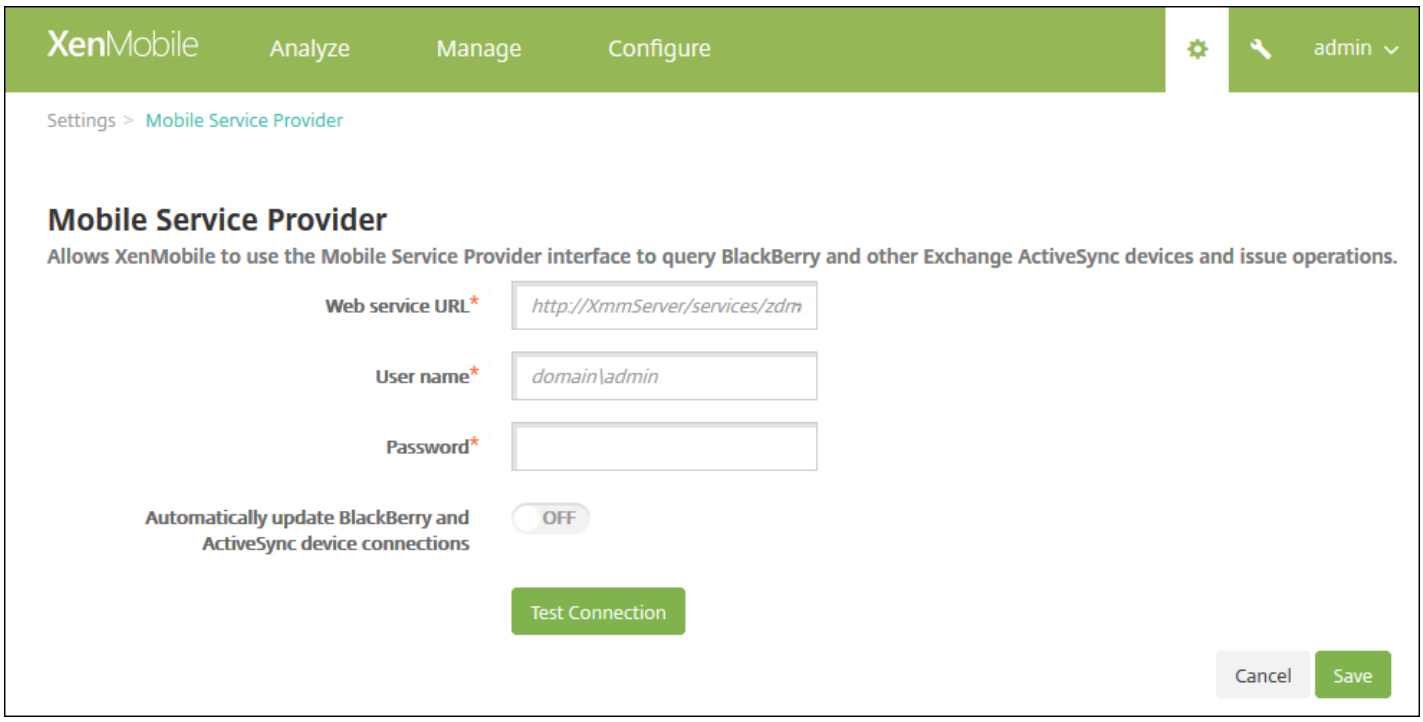
Sie können XenMobile für die Verwendung der Mobilfunkanbieter-Schnittstelle zum Abfragen von BlackBerry- und Exchange ActiveSync-Geräten und Auslösen von Vorgängen konfigurieren.

Beispiel: Ihr Unternehmen hat 1000 Benutzer und jeder Benutzer hat mindestens ein Gerät oder sogar mehrere Geräte. Nachdem Sie allen Benutzern mitgeteilt haben, dass sie ihre Geräte bei XenMobile zur Verwaltung registrieren sollen, wird auf der XenMobile-Konsole die Anzahl der Geräte angezeigt, die Benutzer registrieren. Durch Konfigurieren dieser Einstellung können Sie festlegen, wie viele Geräte eine Verbindung mit Exchange Server herstellen. Sie haben so folgende Möglichkeiten:

- Prüfen, ob es noch Benutzer gibt, die ihre Geräte registrieren müssen
- Befehle an Benutzergeräte senden, sodass diese eine Verbindung mit Exchange Server herstellen (z. B. für Datenlöschungen)

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.
- Geben Sie unter **Benutzername** 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**.

SysLog

Feb 24, 2017

Sie können XenMobile zum Senden von Protokolldateien an einen syslog-Server konfigurieren. Sie brauchen den Hostnamen oder die IP-Adresse des Servers.

Syslog ist ein Standardprotokoll für die Protokollierung mit zwei Komponenten: einem Überwachungsmodul (dies wird auf dem Gerät ausgeführt) und einem Server, der auf einem Remotesystem ausgeführt werden kann. Syslog verwendet UDP (User Data Protocol) für Datenübertragungen. 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:

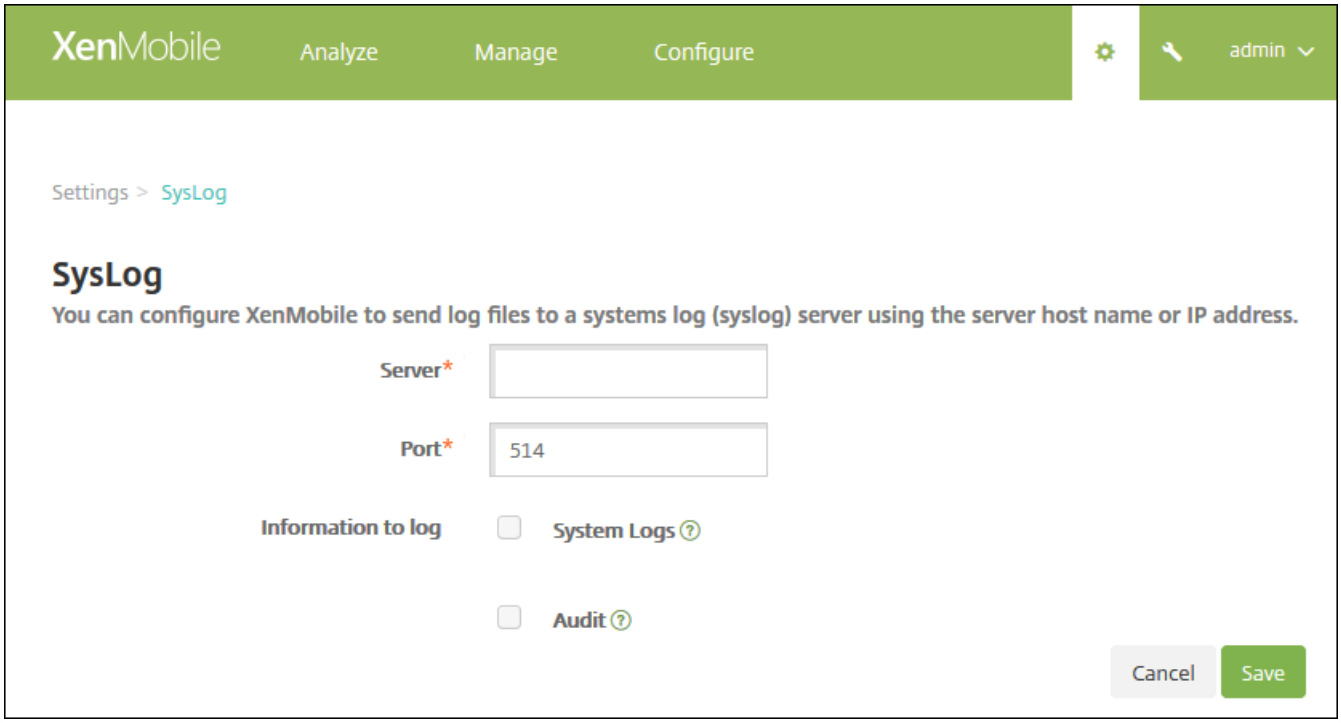
- IP-Adresse des Geräts, das die Protokollmeldung generiert hat
- Zeitstempel
- Meldungstyp
- Dringlichkeitsstufe des Ereignisses (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- Meldungstext

Sie können anhand dieser Informationen die Ursache einer Warnung analysieren und ggf. Maßnahmen ergreifen.

> ## Hinweis
>
> In XenMobile Service (Cloud)-Bereitstellungen 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 folgende Einstellungen:

- **Server**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des syslog-Servers ein.
- **Port**: Geben Sie die Portnummer ein. In der Standardeinstellung ist der 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.

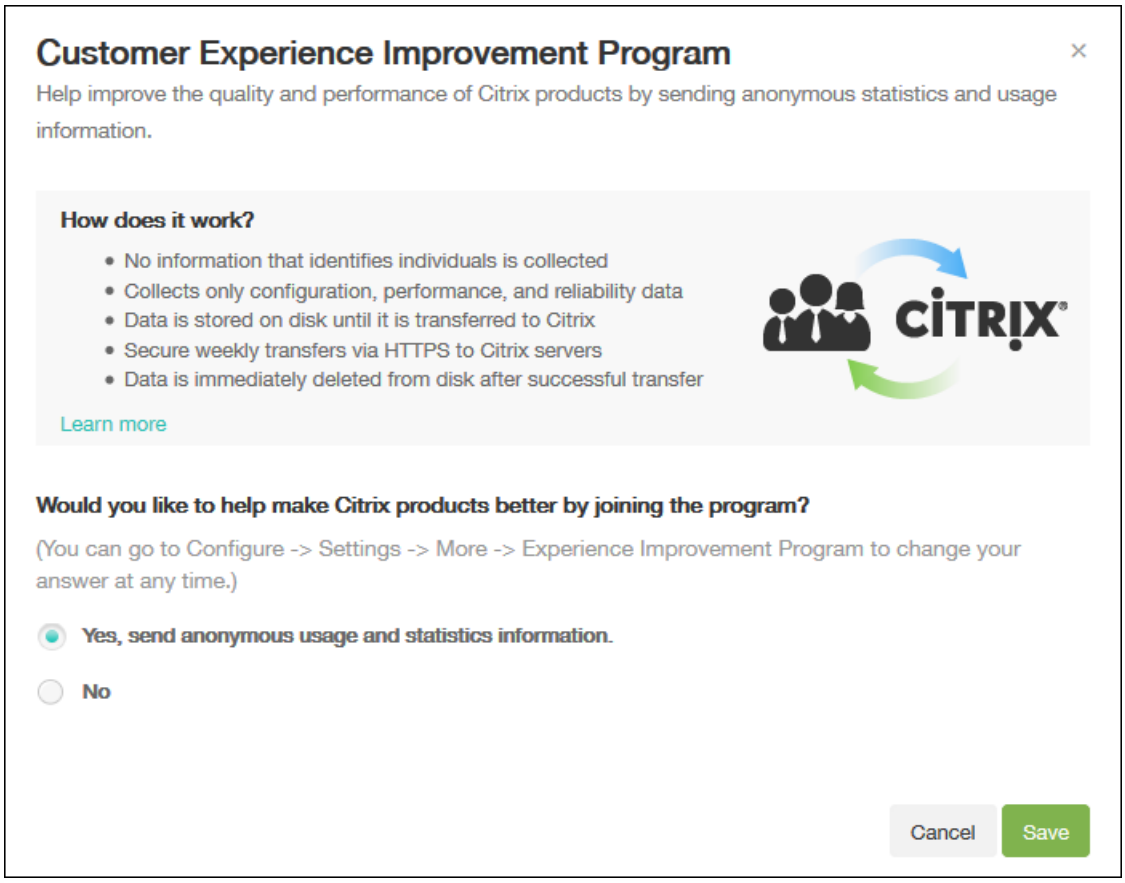
4. Klicken Sie auf **Speichern**.

Programm zur Verbesserung der Benutzerfreundlichkeit

Feb 24, 2017

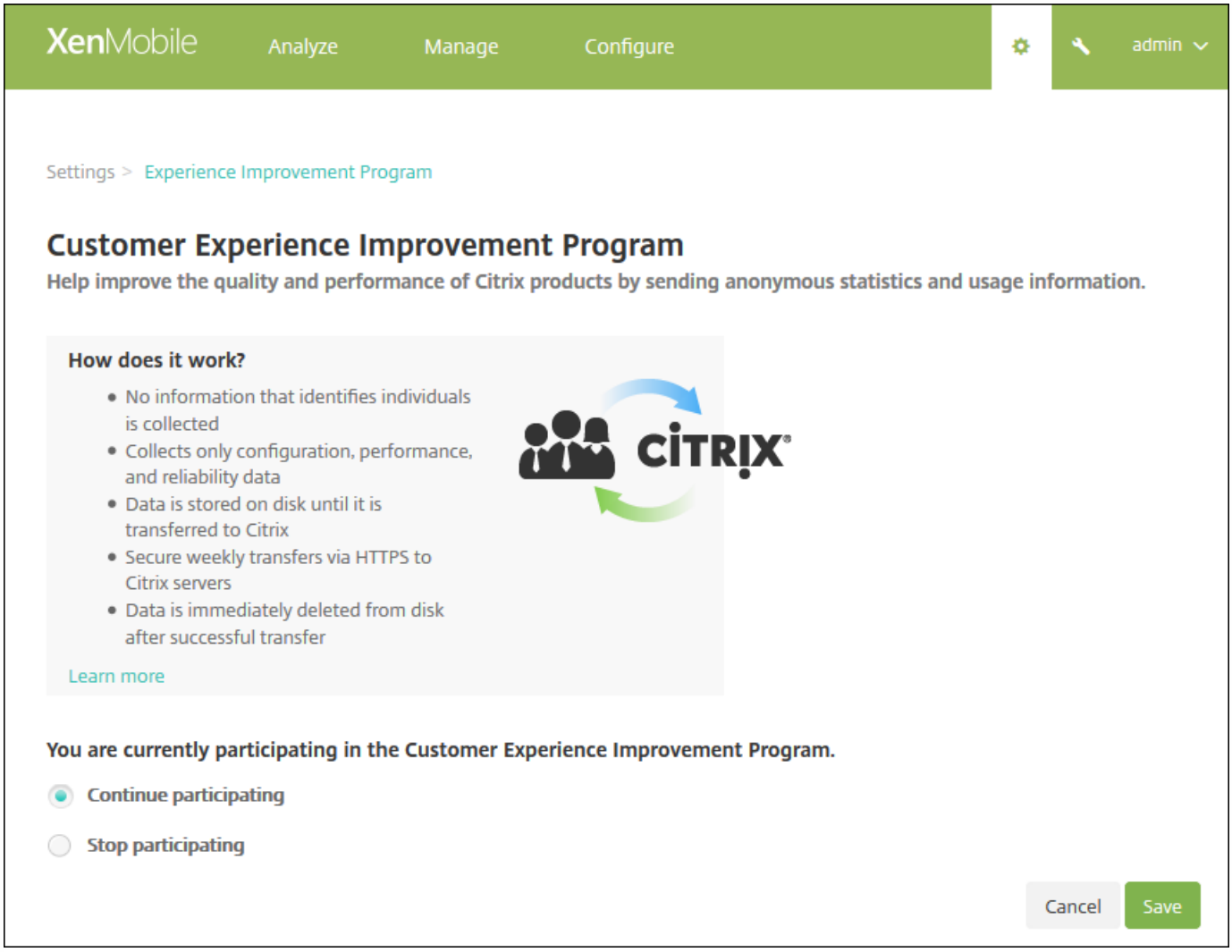
Durch das Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) werden anonyme Konfigurations- und Verwendungsdaten aus XenMobile gesammelt und automatisch an Citrix gesendet. Mit diesen Daten kann Citrix die Qualität, Zuverlässigkeit und Leistung von XenMobile verbessern. Die Teilnahme 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.

Bei der ersten Installation von XenMobile, oder wenn Sie ein Update durchführen, wird das folgende Dialogfeld mit einer Aufforderung zur Teilnahme angezeigt.



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**.

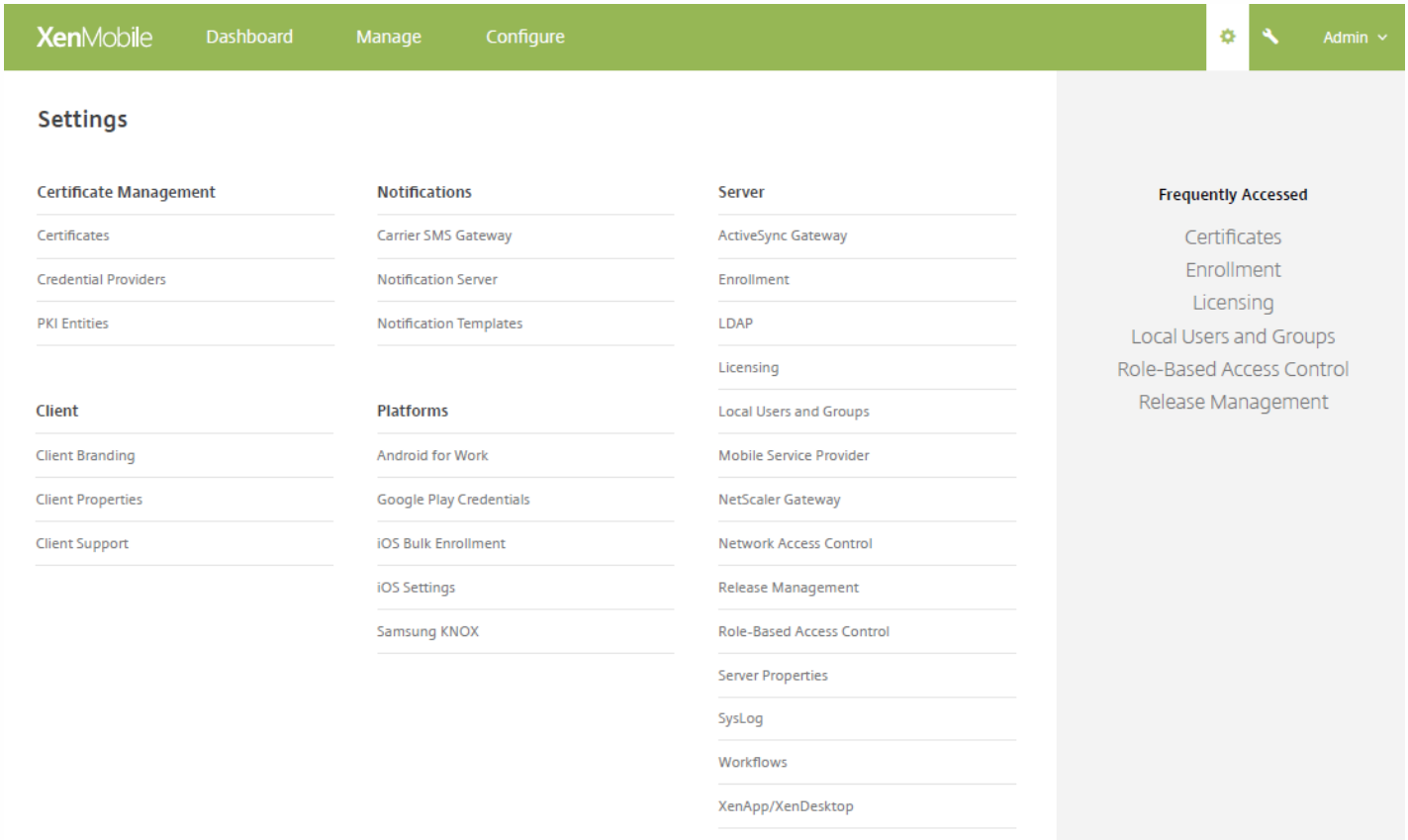
GotoAssist und Remote Support

Apr 24, 2017

Sie können den Benutzern verschiedene Möglichkeiten der Kontaktaufnahme mit dem Support mittels E-Mail-Adressen und Telefonnummern anbieten. Wenn die Benutzer von ihrem Gerät aus Unterstützung anfordern, sehen sie die Optionen, die Sie festgelegt haben.

Sie können auch konfigurieren, wie Benutzer von ihren Geräten Protokolle an den Helpdesk senden. Sie können die Protokolle so konfigurieren, dass sie direkt oder per e-Mail gesendet werden.

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 zum Konfigurieren einer Telefonnummer und E-Mail-Adresse und geben Sie an, wie das Gerät Protokolle an den Helpdesk senden soll.

- **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 Protokolle direkt an ShareFile gesendet. Ansonsten werden die

Protokolle an XenMobile gesendet und dann per E-Mail an den Helpdesk geschickt. 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 jedoch deaktivieren und ein Serverproblem auftritt, 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**.

Durch Remote Support können Helpdesk-Mitarbeiter die Steuerung verwalteter Windows- und Android-Mobilgeräte übernehmen.

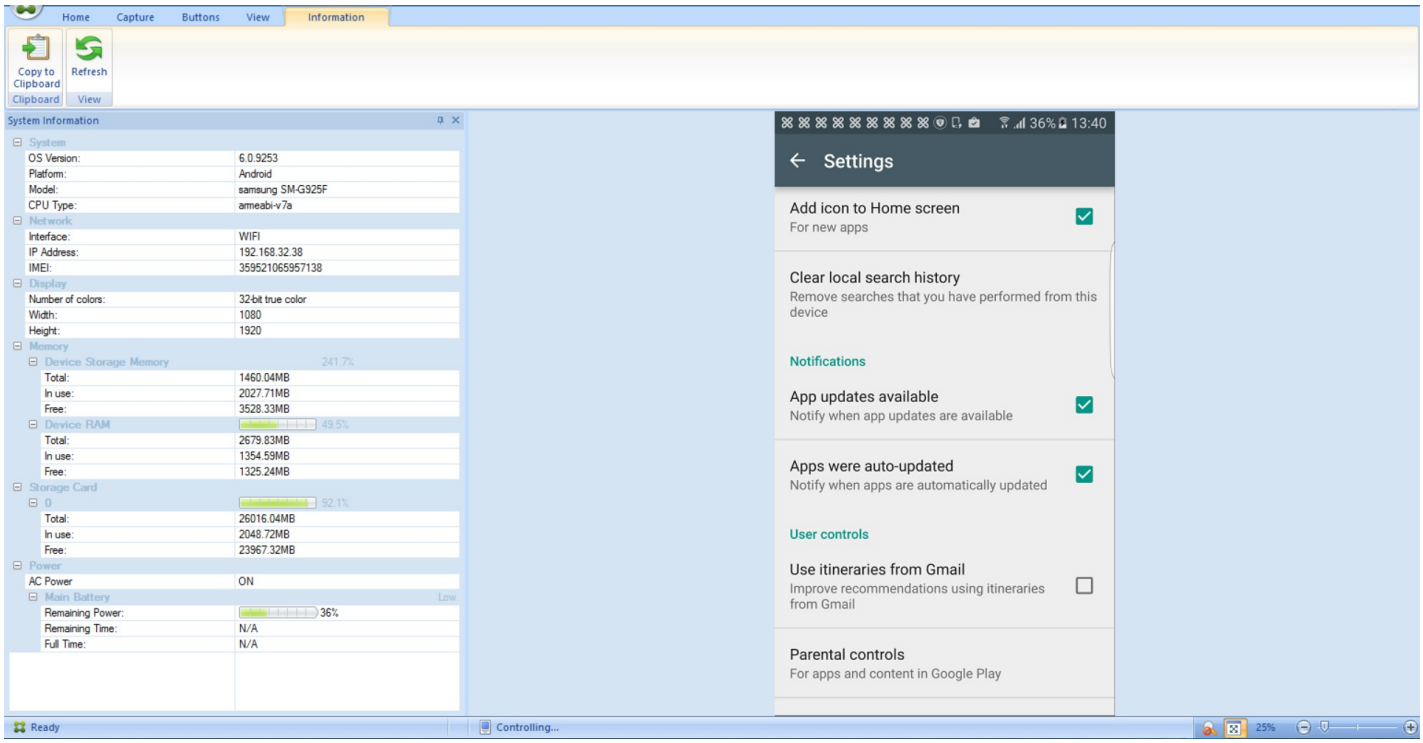
Remotesupport ist auf allen Windows-Mobilgeräten, auf Android Samsung SAFE-Geräten und auf Geräten, die nicht von Samsung stammen, verfügbar.

Screencast wird nur auf Samsung KNOX-Geräten unterstützt.

Die Remotesteuerung von iOS-Geräten wird nicht unterstützt.

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, das eine Darstellung des gesteuerten Geräts zeigt.



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 einer oder mehreren Instanzen von XenMobile 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 für XenMobile
- Ausführen des Task-Managers des Geräts, in dem aktive Prozesse angezeigt und beendet werden können und 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 "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:

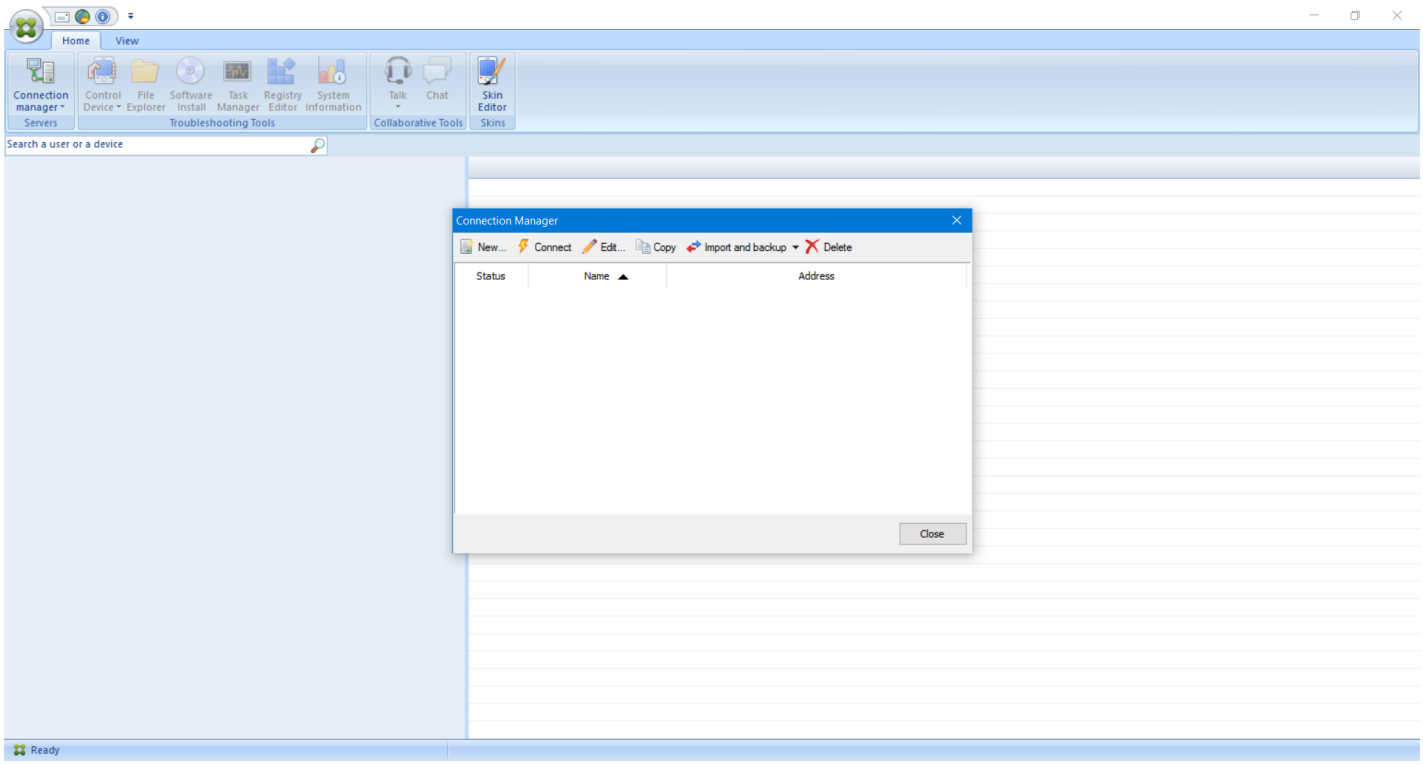
- /S: zur Installation der Remote Support-Software mit den Standardparametern
- /D=dir: zum Angeben eines benutzerdefinierten Installationsverzeichnisses

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, den Sie in der MDM-Tunnelrichtlinie definieren. Die Tunnelrichtlinie ist eine Richtlinie für Android- und Windows Mobile-/CE-Geräte. Definieren Sie den App-Tunnel, bevor Sie eine Verbindung zwischen Remote Support und XenMobile herstellen können. Weitere Informationen finden Sie unter App-Tunnelrichtlinien für Geräte.

1. Starten Sie die Remote Support-Software und melden Sie sich mit Ihren XenMobile-Anmeldeinformationen an.

2. Klicken Sie im Verbindungs-Manager auf **Neu**.



3. Geben Sie im Dialogfeld **Connection Configuration** auf der Registerkarte **Server** folgende Werte ein:

a. 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.

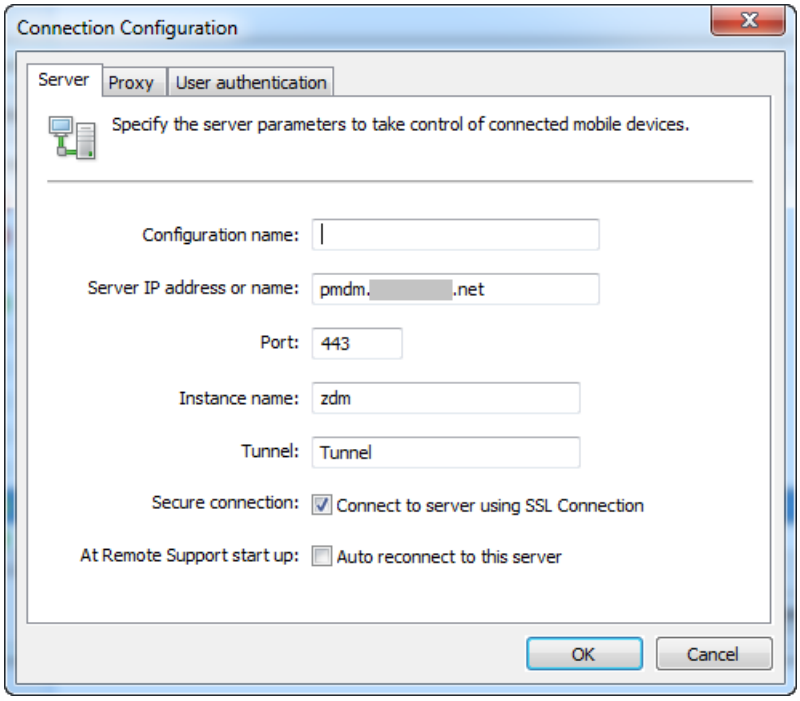
c. Geben Sie in **Port** eine TCP-Portnummer gemäß der XenMobile-Serverkonfiguration ein.

Geben Sie in **Instance name** einen Instanznamen ein, wenn XenMobile Teil einer Bereitstellung mit mehreren Mandanten ist.

e. Geben Sie in **Tunnel** den Namen der Tunnelrichtlinie ein.

f. Aktivieren Sie das Kontrollkästchen **Connect to server using SSL Connection**.

g. 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:

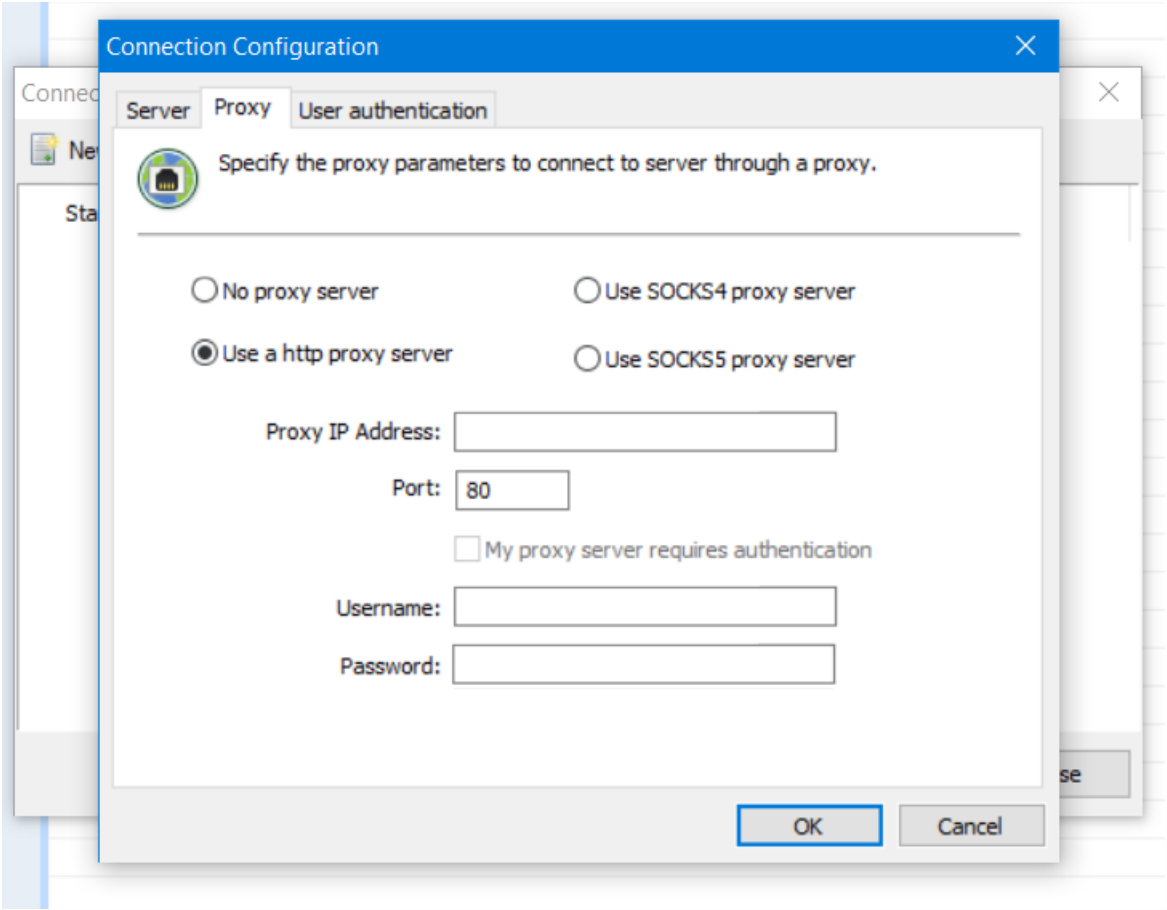
a. Geben Sie in **Proxy IP Address** die IP-Adresse des Proxyservers ein.

Geben Sie in **Port** die Nummer des TCP-Ports des Proxyservers ein.

c. Aktivieren Sie das Kontrollkästchen **My proxy server requires authentication**, wenn der Proxyserver eine Authentifizierung erfordert, um Datenverkehr zuzulassen.

d. Geben Sie in **Benutzername** den Benutzernamen für die Authentifizierung auf dem Proxyserver ein.

e. Geben Sie in **Kennwort** das Kennwort für die Authentifizierung auf dem Proxyserver ein.



5. Aktivieren Sie auf der Registerkarte **Benutzerauthentifizierung** 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.

  Bei Premiumsupport müssen Sie die Geräterichtlinie für Samsung MDM-Lizenzschlüssel in der XenMobile-Konsole konfigurieren. Wenn Sie diese Richtlinie konfigurieren, wählen Sie nur die Plattform **Samsung KNOX** . Sie müssen die

Samsung SAFE-Plattform für dieses Szenario nicht konfigurieren, da der ELM-Schlüssel bei der Registrierung bei XenMobile automatisch auf Samsung-Geräten bereitgestellt wird. Weitere Informationen finden Sie unter Samsung MDM-Richtlinien für Geräte.

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-Konsole 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 **Anzeigen** 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. Sie können mit gesteuerten Geräten folgendermaßen 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

Erstellen von Secure Hub- und GoToAssist-Supportoptionen

Feb 24, 2017

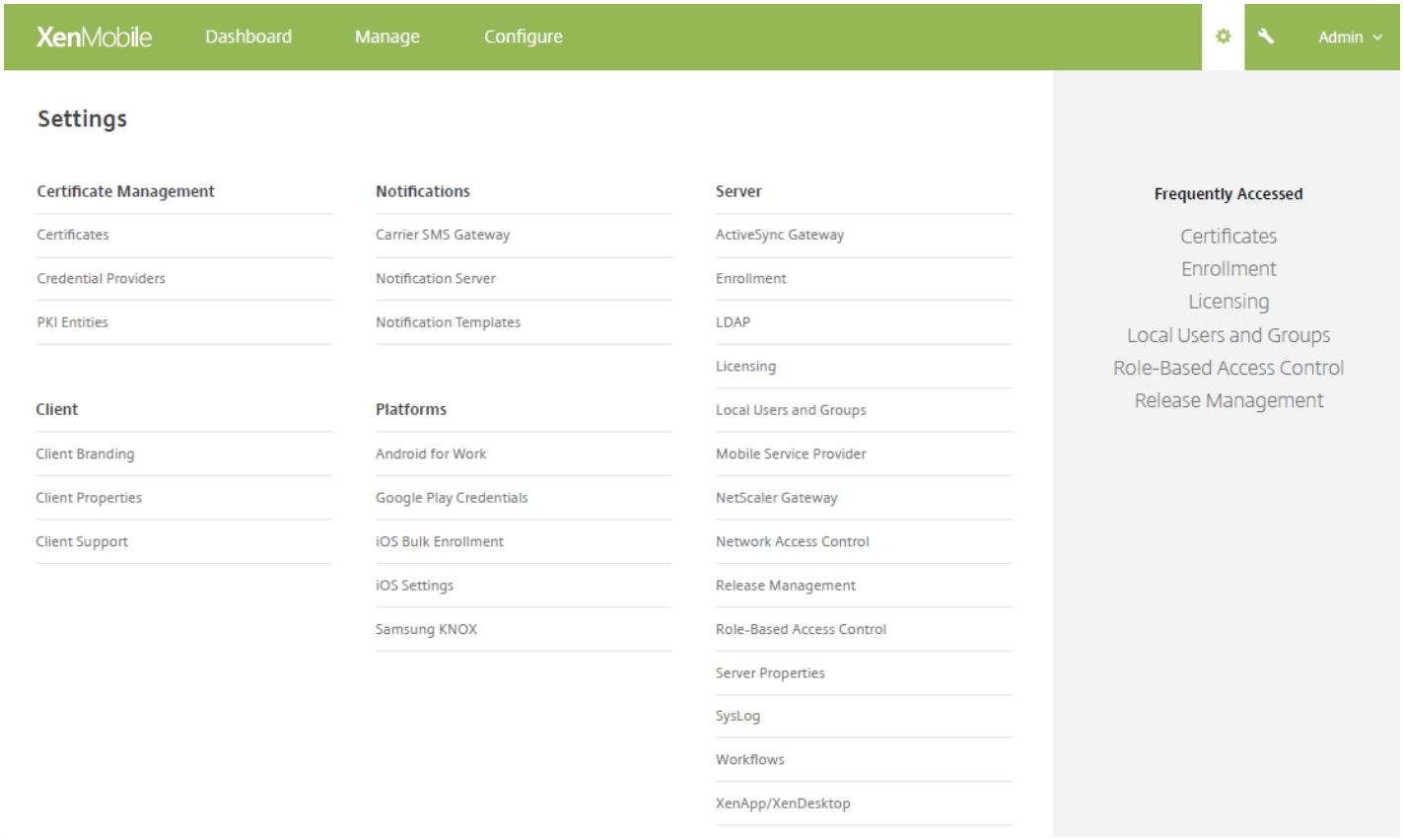
Sie können festlegen, wie Apps im Store angezeigt werden, und Secure Hub und dem XenMobile Store für mobile iOS- und Android-Geräte ein Logo hinzufügen.

Hinweis: Stellen Sie zu Beginn des Arbeitsgangs sicher, dass das benutzerdefinierte Bild bereitsteht.

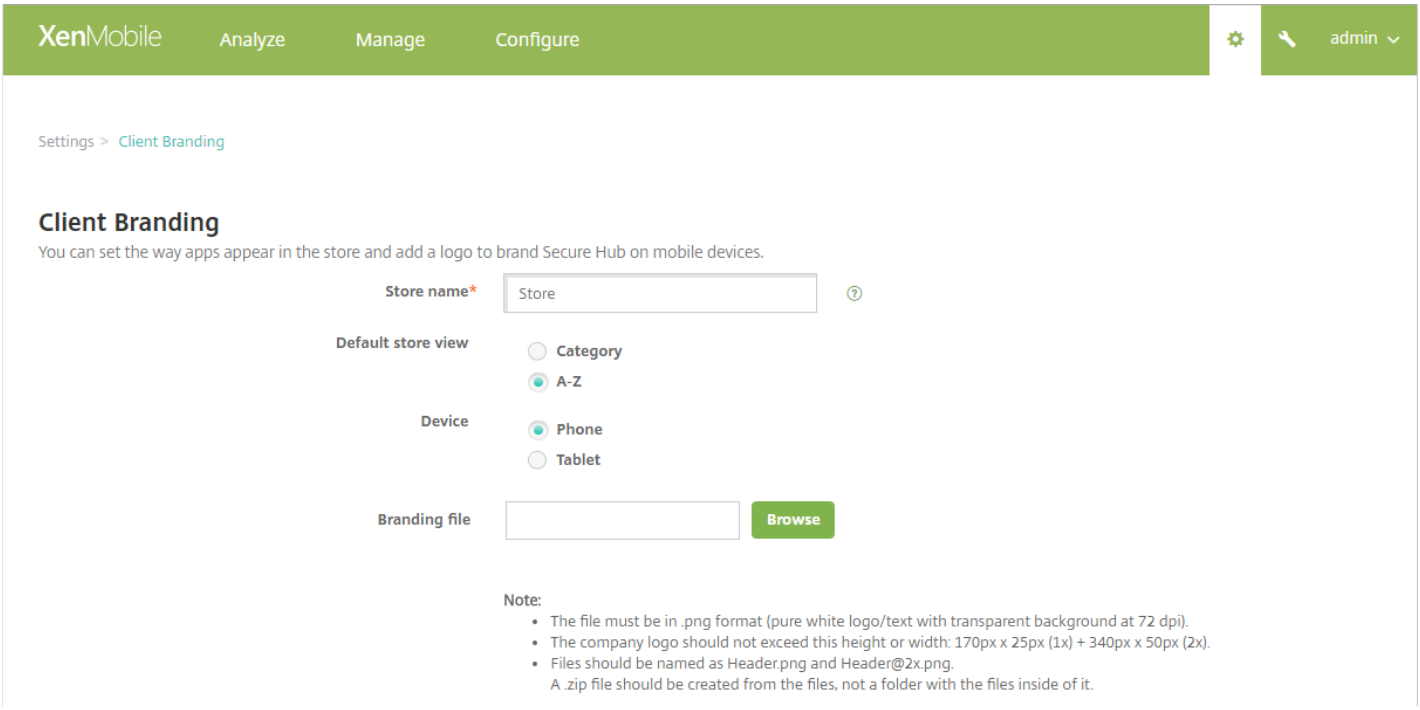
Das benutzerdefinierte Bild muss folgende Anforderungen erfüllen:

- 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.



3. 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**: Zum Wählen einer Bilddatei oder einer ZIP-Datei mit Bildern für das Branding klicken Sie auf **Durchsuchen** und navigieren Sie zu deren Speicherort.

4. Klicken Sie auf **Speichern**.

Zum Bereitstellen dieses Pakets auf den Geräten müssen Sie ein Bereitstellungspaket erstellen und bereitstellen.

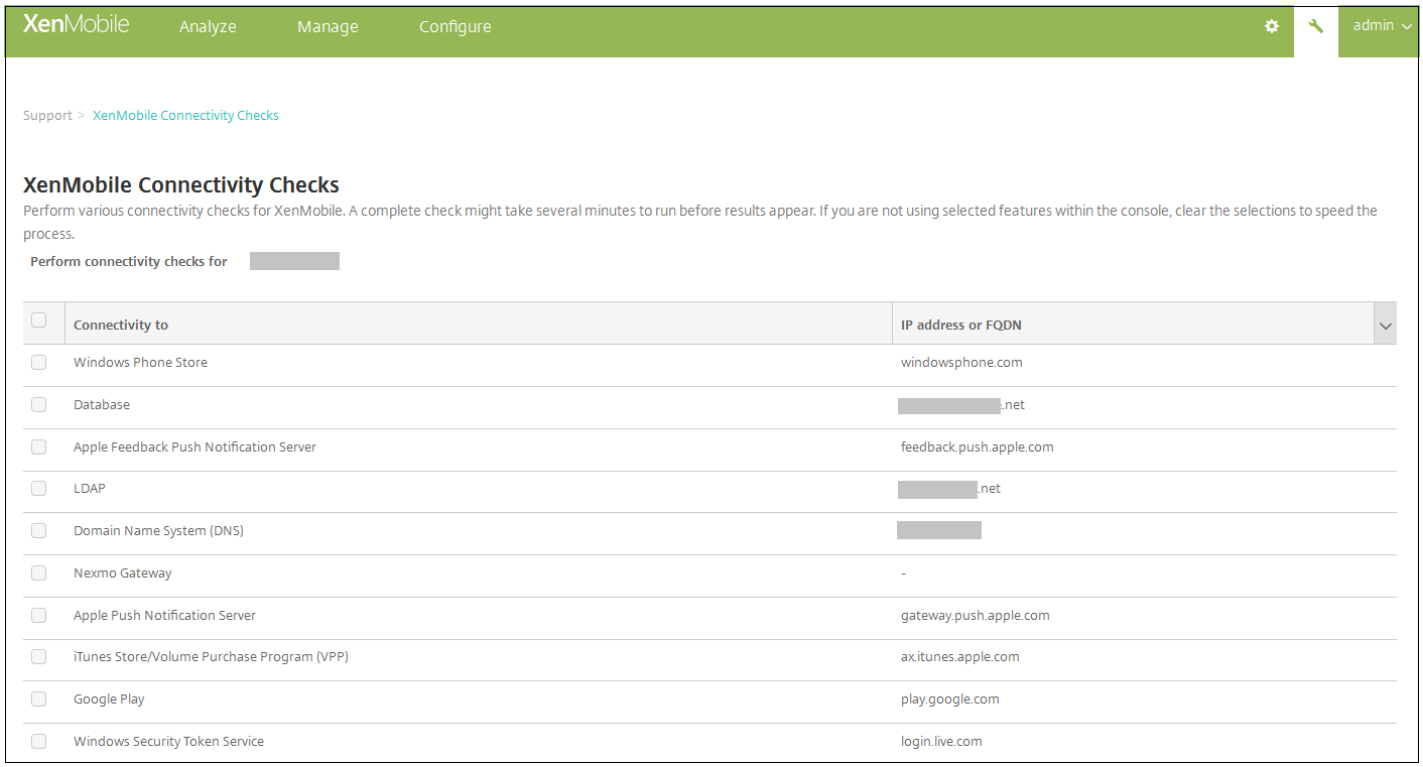
Konnektivitätsprüfungen

Apr 24, 2017

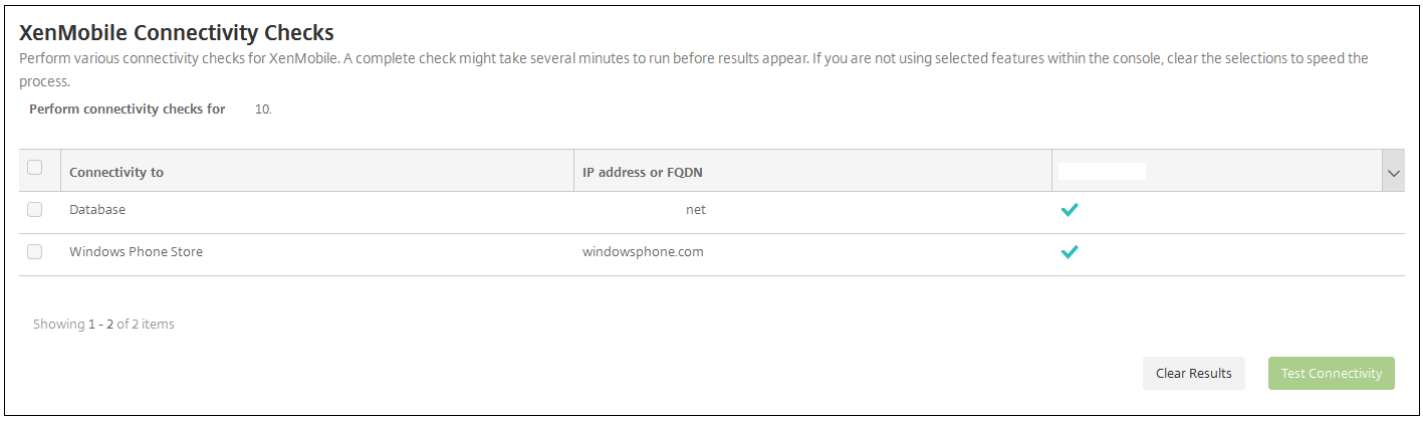
Über die Seite **Support** können Sie die Verbindung zwischen XenMobile und NetScaler Gateway sowie XenMobile und anderen Servern und Speicherorten prüfen.

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

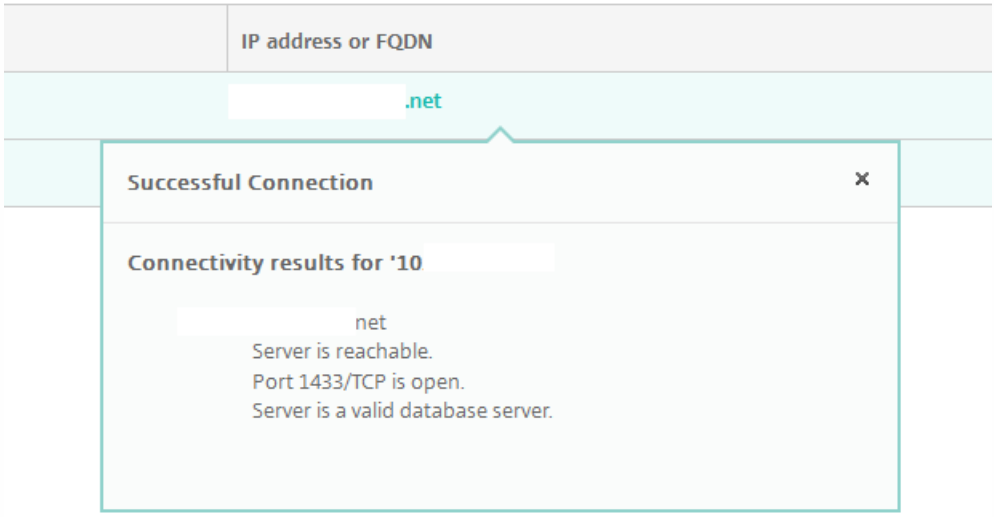
2. Klicken Sie unter **Diagnose** auf **XenMobile-Konnektivitätsprüfung**.Die Seite **XenMobile-Konnektivitätsprüfung** wird angezeigt. Wenn die XenMobile-Umgebung Clusterknoten enthält, werden alle Knoten angezeigt.



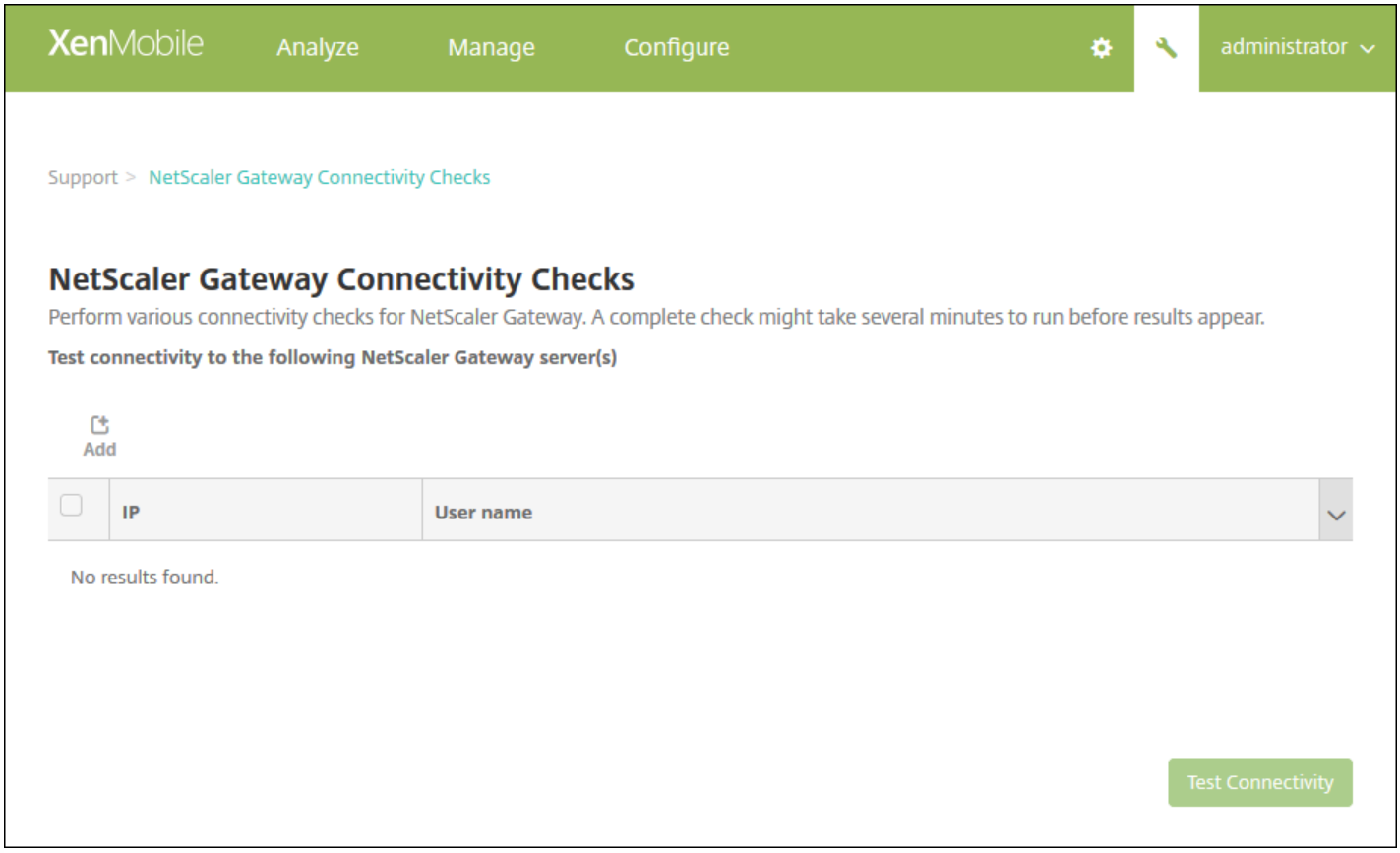
2. Wählen Sie die Server aus, deren Verbindung geprüft werden soll, und klicken Sie dann auf **Konnektivität testen**.Die Testergebnisseite wird angezeigt.



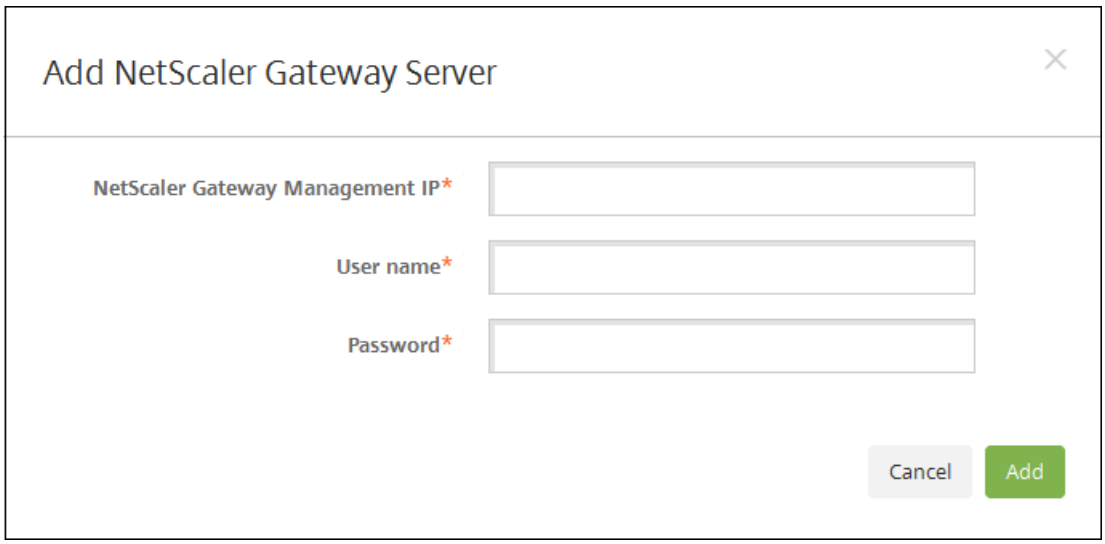
3. Wählen Sie einen Server in der Tabelle mit den Testergebnissen aus, um detaillierte Ergebnisse für den Server anzuzeigen.



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. Wählen Sie den NetScaler Gateway-Server aus und klicken Sie dann auf **Test Connectivity**.

Die Ergebnisse werden in einer Tabelle angezeigt.

7. Wählen Sie einen Server in der Tabelle mit den Testergebnissen aus, um detaillierte Ergebnisse für den Server anzuzeigen.

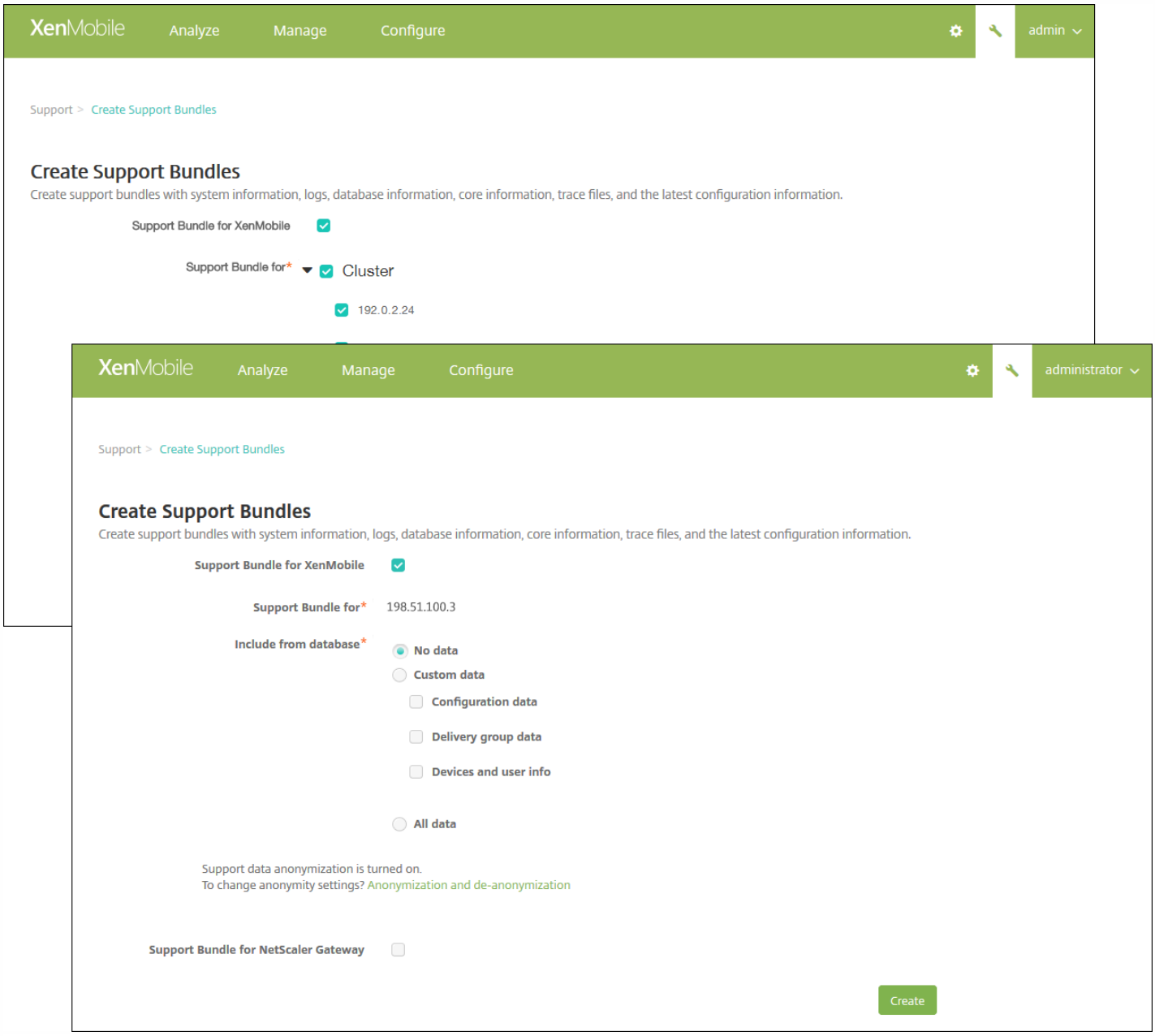
Supportpakete

Feb 24, 2017

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.



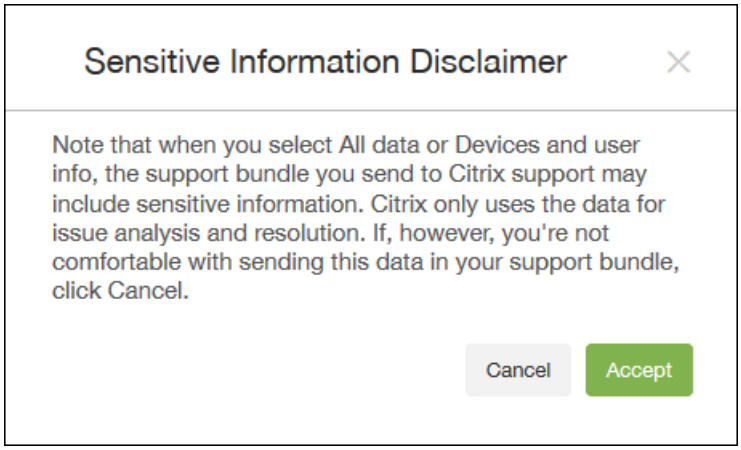
3. Stellen Sie sicher, dass das Kontrollkästchen **Supportpaket für XenMobile** aktiviert ist.

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 (standardmäßig sind alle Optionen ausgewählt):
  - **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.

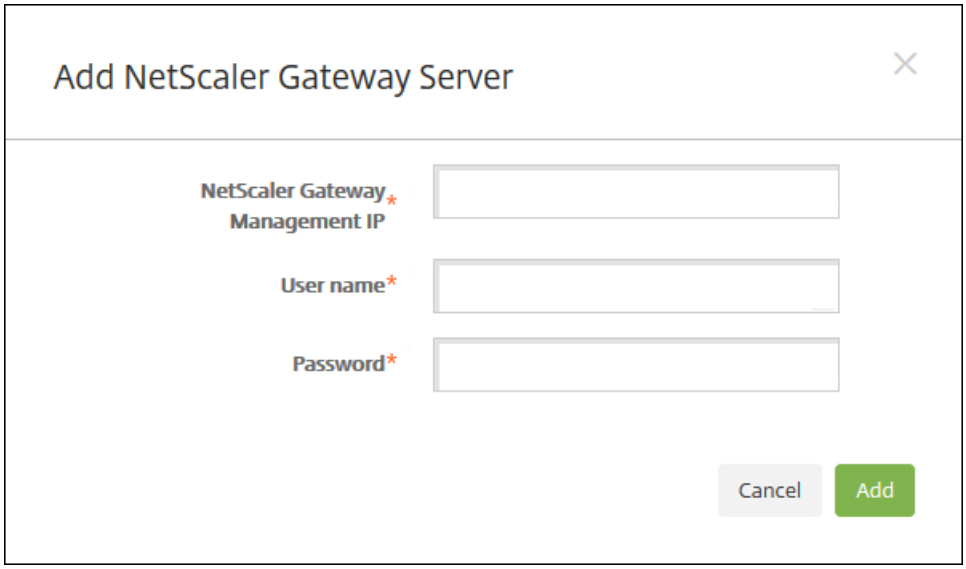


6. Die Option **Anonymisierung von Supportdaten ist aktiviert** gibt an, dass Daten in der Standardeinstellung anonymisiert werden, d. h. vertrauliche Benutzer-, Server- und Netzwerkdaten werden in Supportpaketen anonymisiert.

Zum Ändern dieser Einstellung klicken Sie auf **Anonymisierung und Deanonymisierung**. Weitere Informationen finden Sie unter Anonymisierung von Daten in Supportpaketen.

7. Wählen Sie das Kontrollkästchen **Supportpaket für NetScaler Gateway**, wenn Sie Supportpakete von NetScaler Gateway einschließen möchten, und führen Sie die folgenden Schritte aus:

a. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **NetScaler Gateway-Server hinzufügen** wird angezeigt.



b. 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.

c. 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.

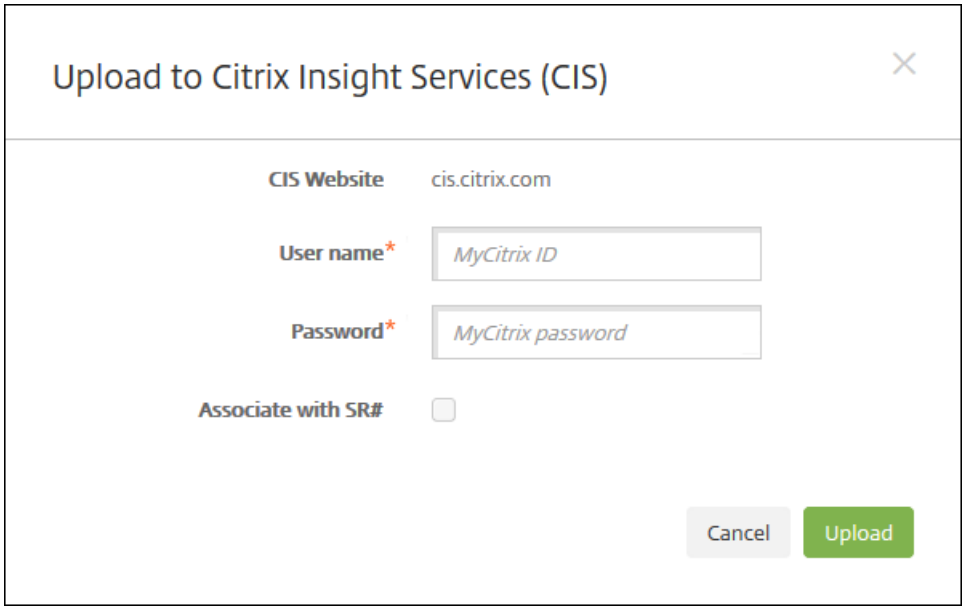
8. Wiederholen Sie Schritt 7 zum Hinzufügen weiterer NetScaler Gateway-Supportpakete nach Bedarf.

9. Klicken Sie auf **Erstellen**. Das Supportpaket wird erstellt und zwei neue Schaltfläche werden angezeigt: **Upload zu CIS** und **Zu Client herunterladen**.

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 den Computer

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.

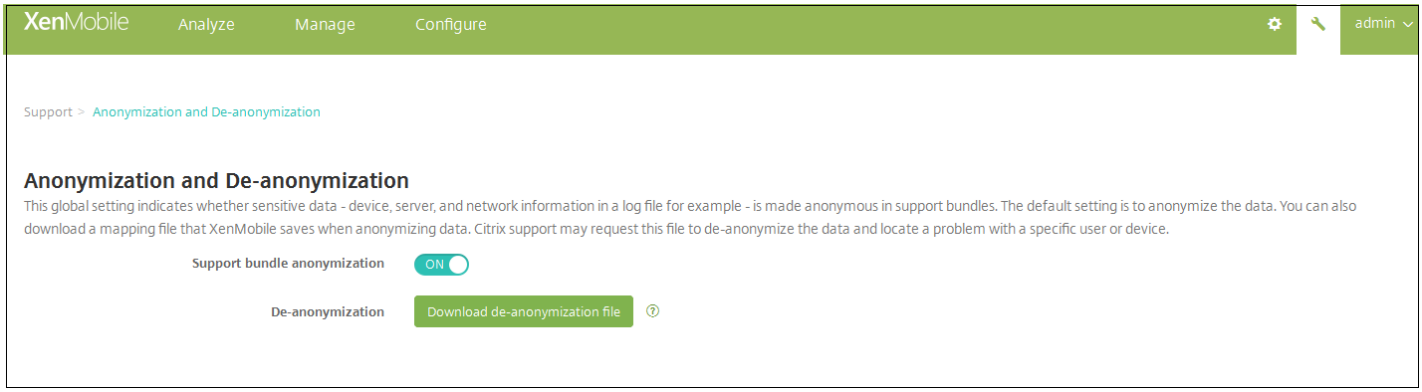
Anonymisierung von Daten in Supportpaketen

Feb 24, 2017

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. Der Standardwert 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.

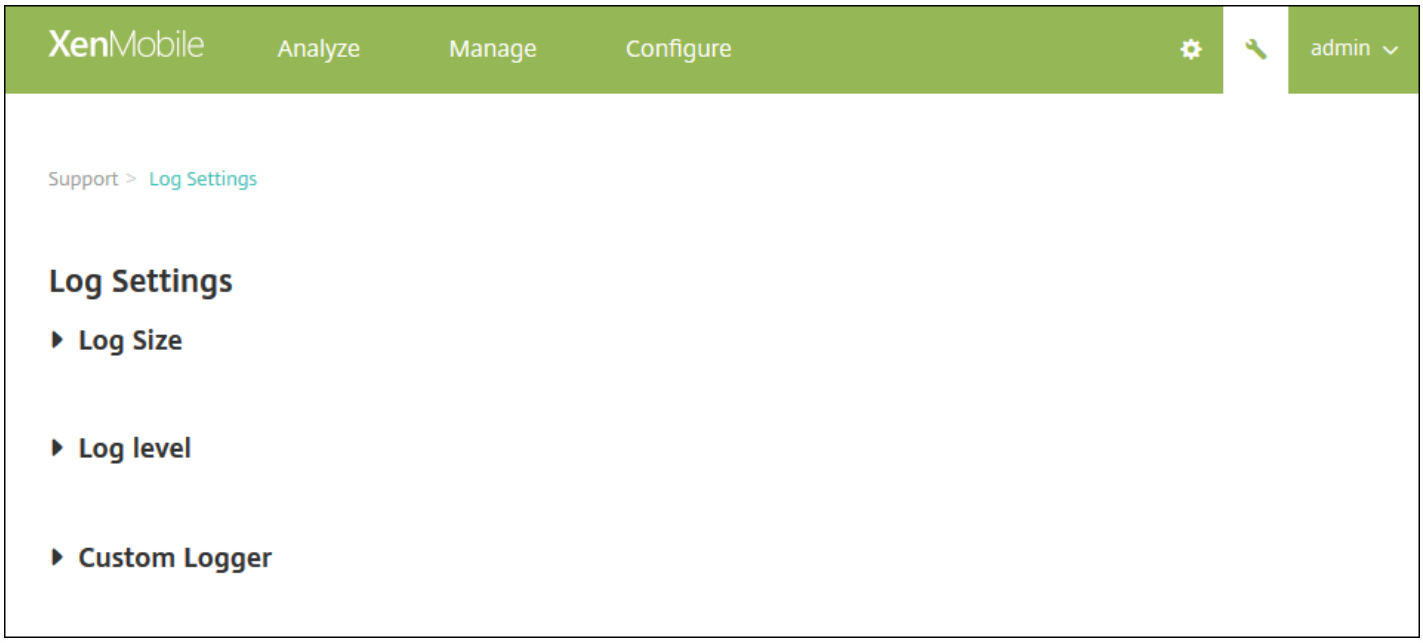
Protokolle

Feb 24, 2017

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.

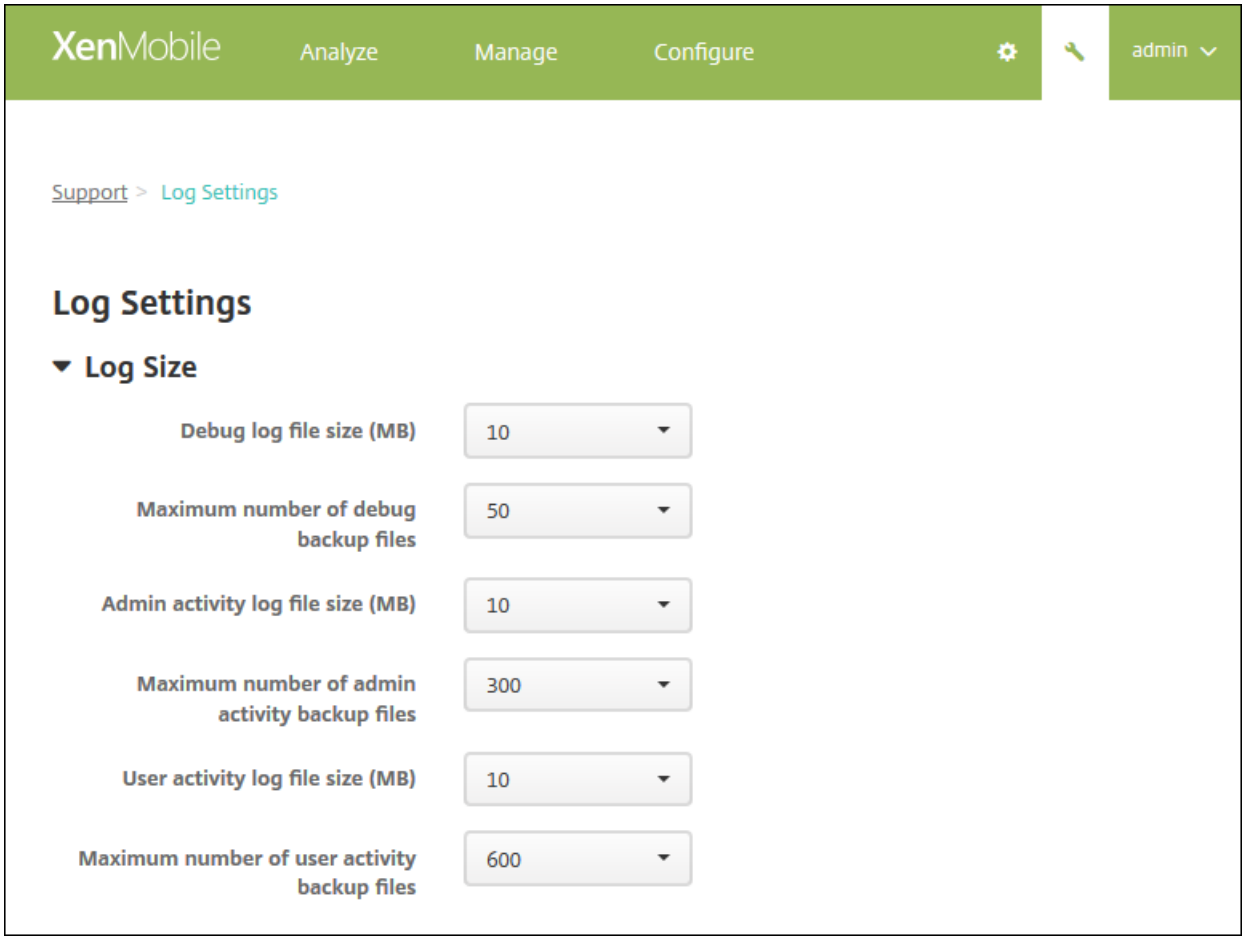


Auf der Seite **Protokolleinstellungen** können Sie folgende Einstellungen ändern:

- **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:

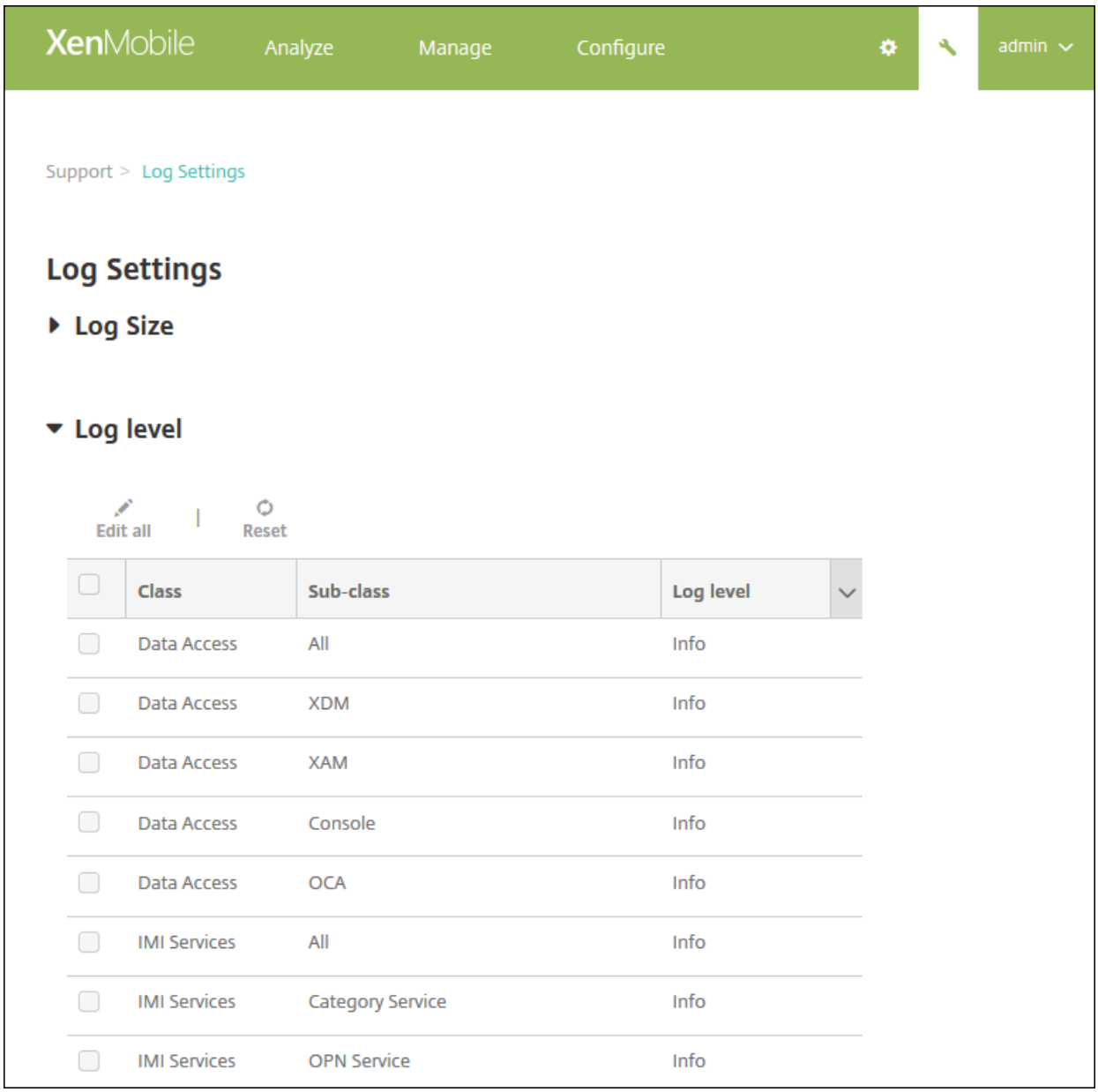
- **Dateigröße des Debugprotokolls (MB)**: Klicken Sie in der Liste auf eine Größe zwischen 5 MB und 20 MB, um die maximale Größe der Debugdatei zu ändern. Die Standarddateigröße ist **10 MB**.
- **Maximale Anzahl der Debugbackupdateien**: Wählen Sie in der Liste aus, wie viele Sicherungskopien der Debugdatei 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.

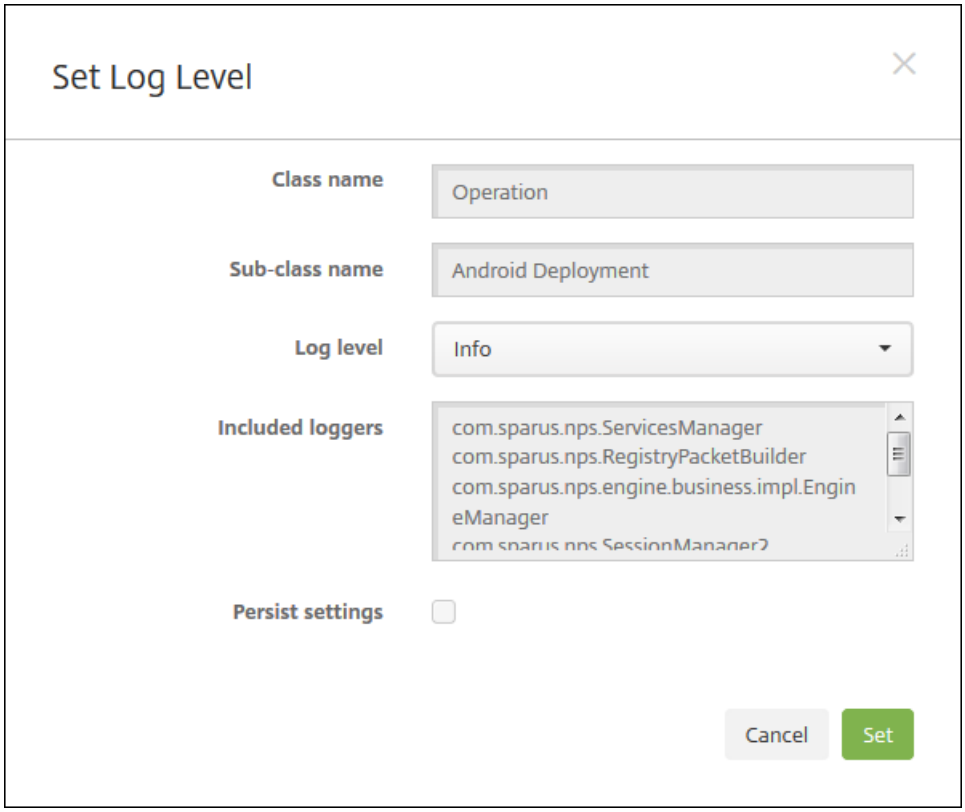
1. Erweitern Sie **Protokollebene** auf der Seite **Protokolleinstellungen**. Die Tabelle mit allen Protokollklassen wird angezeigt.



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.

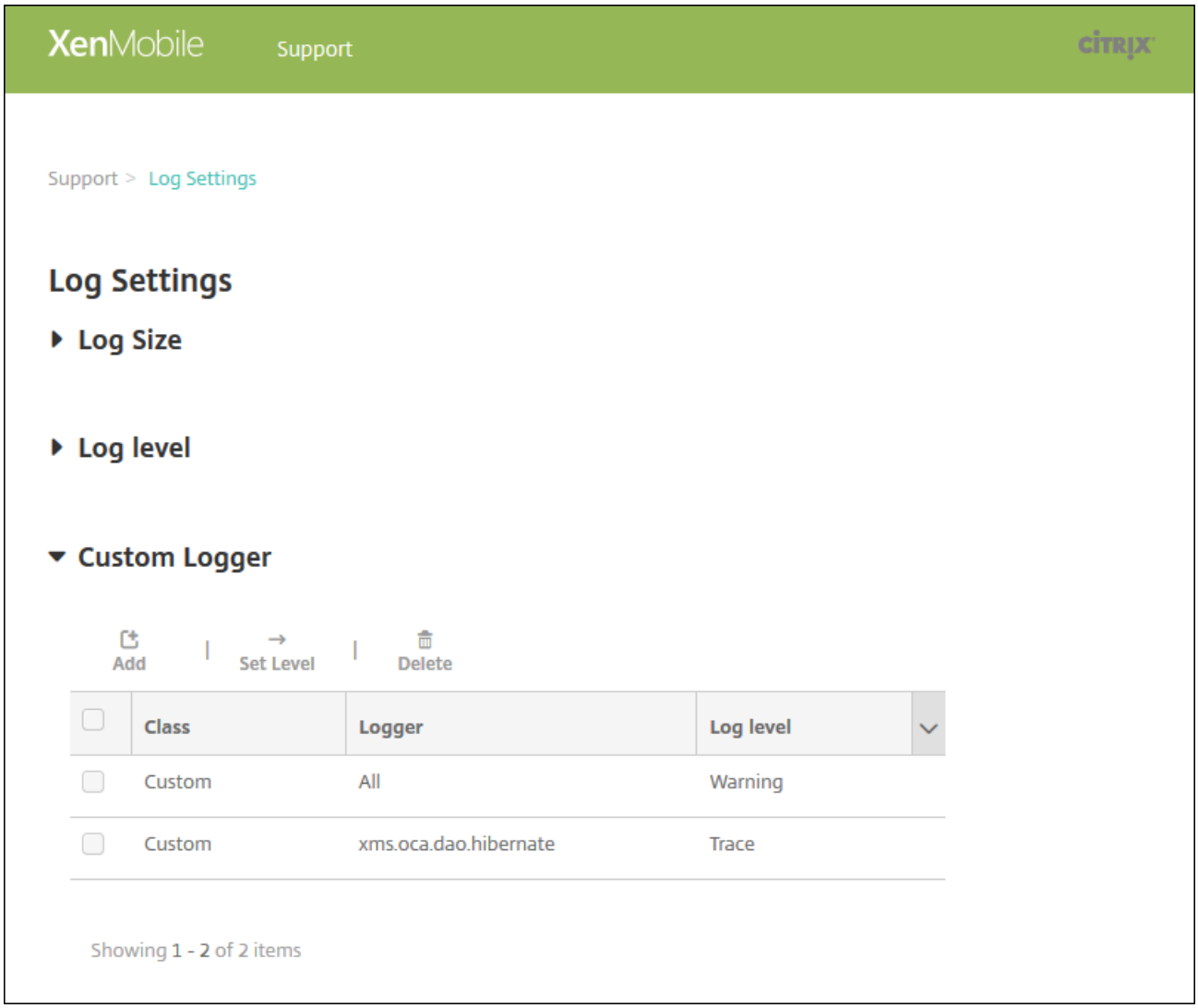


- **Klassenname**: Wenn Sie die Auswahl für alle Klassen ändern, wird in diesem Feld All angezeigt, ansonsten werden die einzelnen Klassennamen angezeigt. Das Feld kann nicht bearbeitet werden.
- **Unterklassenname**: Wenn Sie die Protokollebene für alle Klassen ändern, wird in diesem Feld "Alle" angezeigt, 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.

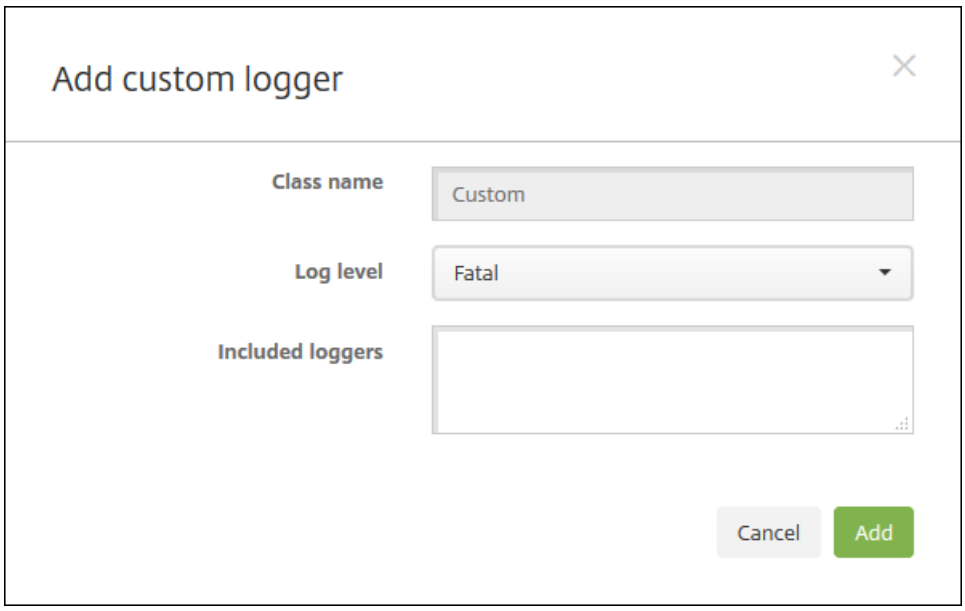
3. Klicken Sie auf **Festlegen**, um die Änderungen zu übergeben.

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.



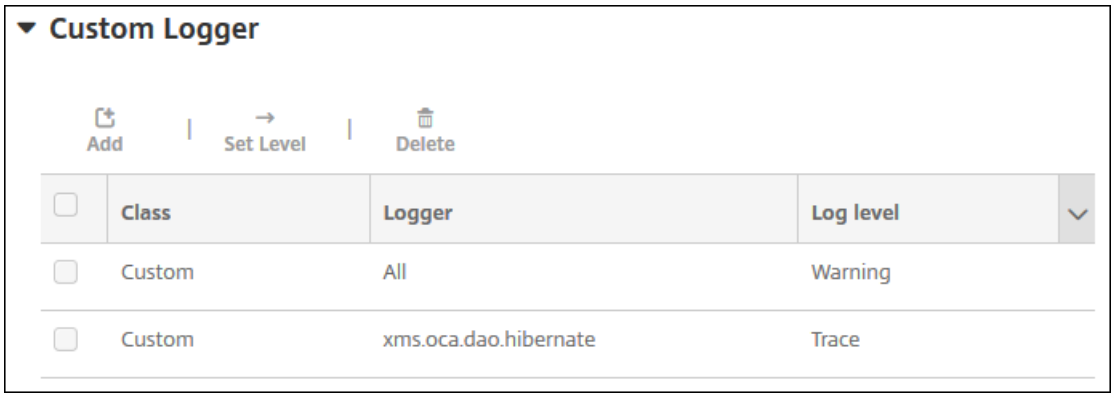
2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Benutzerdefinierte Protokollierung hinzufügen** wird angezeigt.



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.

XenMobile Analyzer

Apr 24, 2017

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.

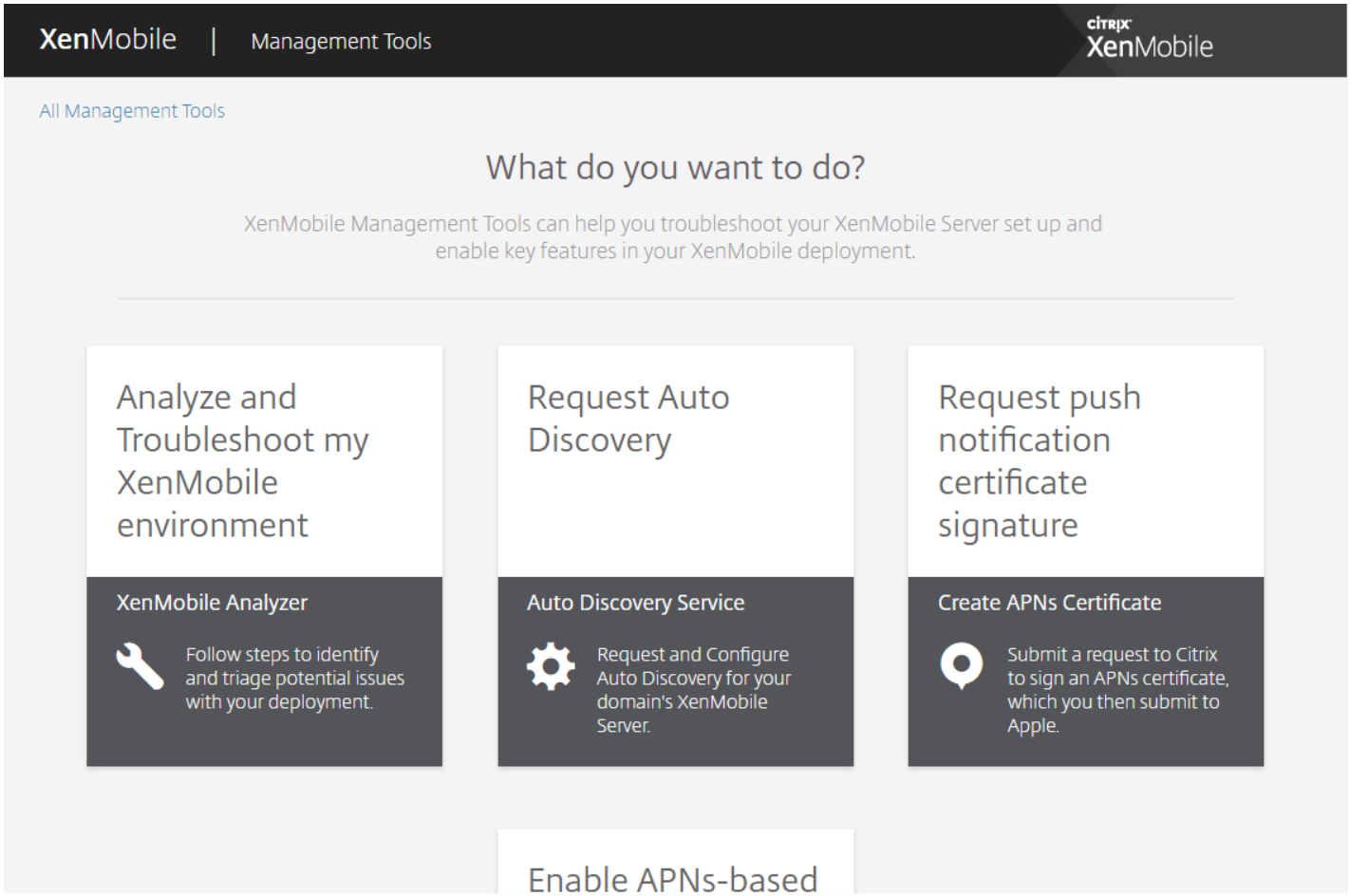
XenMobile Analyzer – Hauptfeatures

- 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.
- Tests der Erreichbarkeit von Intranetsites für Secure Web.
- Prüfung des Autodiscovery-Diensts für Secure Mail.
- Single Sign-On-Prüfungen (SSO) für ShareFile.
- Benutzerdefinierte Portunterstützung für NetScaler.
- Unterstützung für nicht englischsprachige Browser.

Voraussetzungen

Produkt	Unterstützte Version
XenMobile-Server	10.3.0 und höher
NetScaler Gateway	10.5 und höher
Simulation der Clientregistrierung	iOS und Android

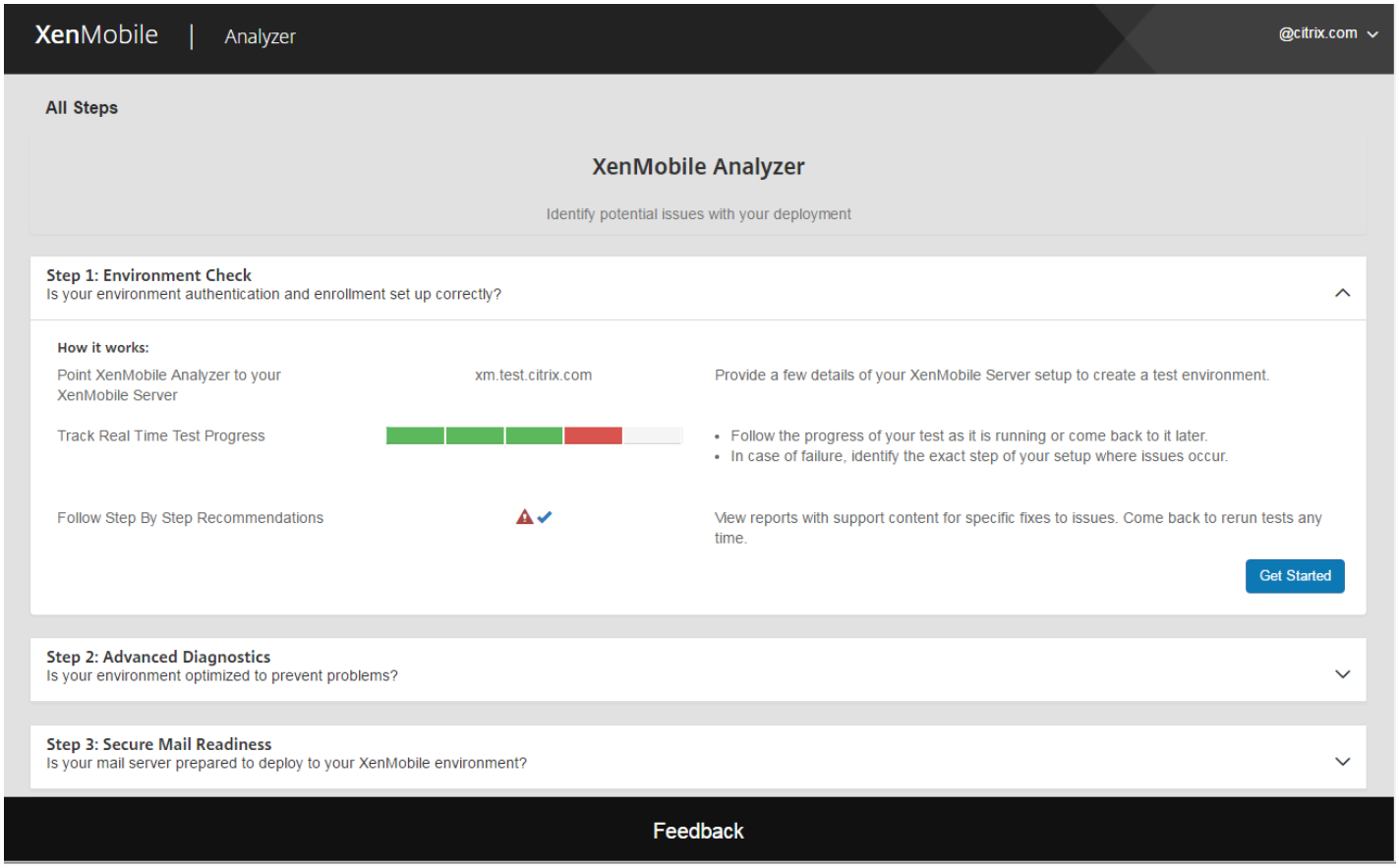
Mit Ihren Citrix Anmeldeinformationen können Sie auf das Tool unter https://xenmobiletools.citrix.com zugreifen. Die XenMobile-Seite für Verwaltungstools wird geöffnet. Klicken Sie hier auf **Analyze and Troubleshoot my XenMobile Environment**, um XenMobile Analyzer zu starten.



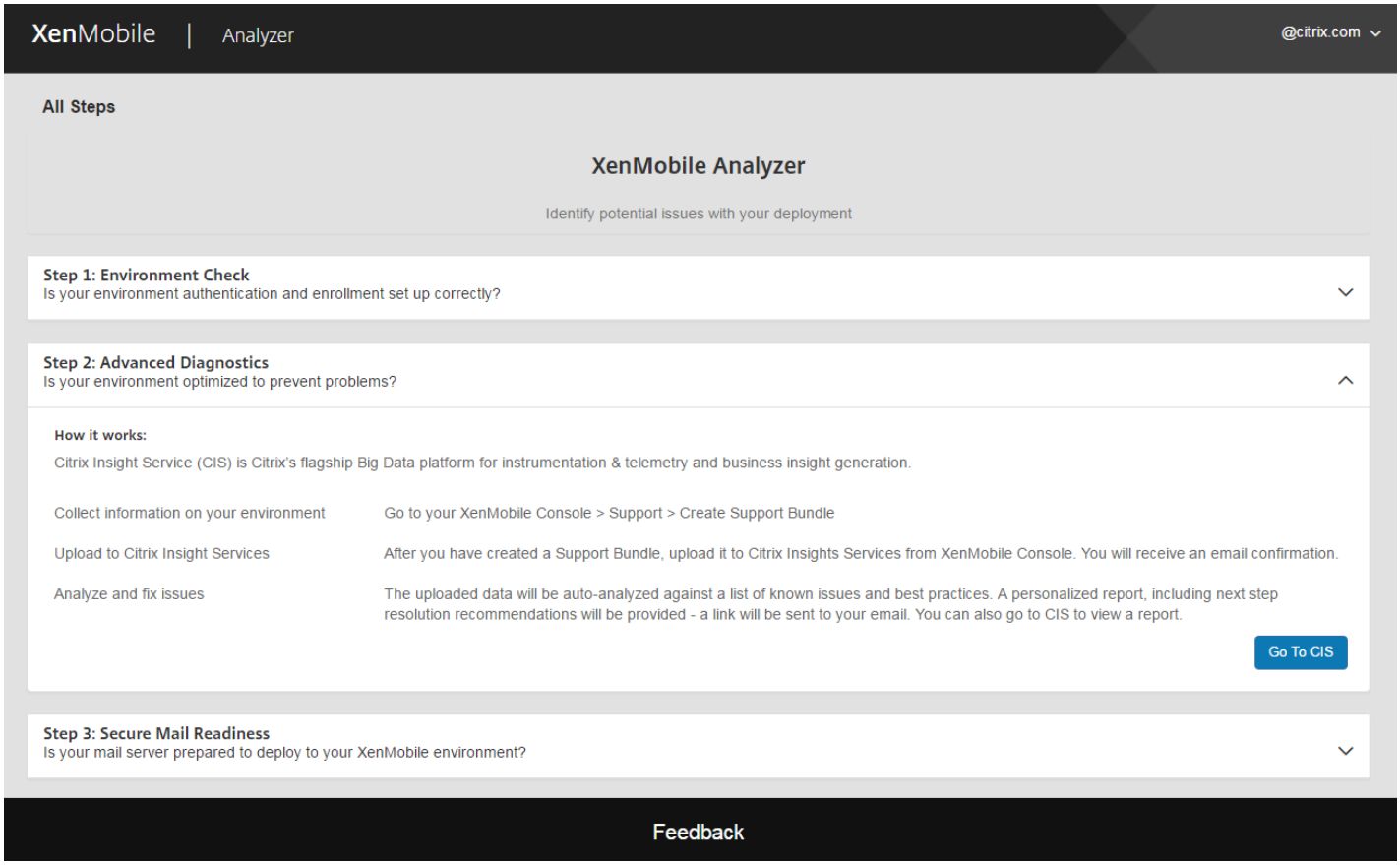
XenMobile Analyzer umfasst fünf Hauptschritte, die Sie durch den Selektierungsvorgang führen. Auf diese Weise lässt sich die Anzahl an Supporttickets reduzieren, wodurch sich die Kosten verringern.

Führen Sie die folgenden Schritte aus:

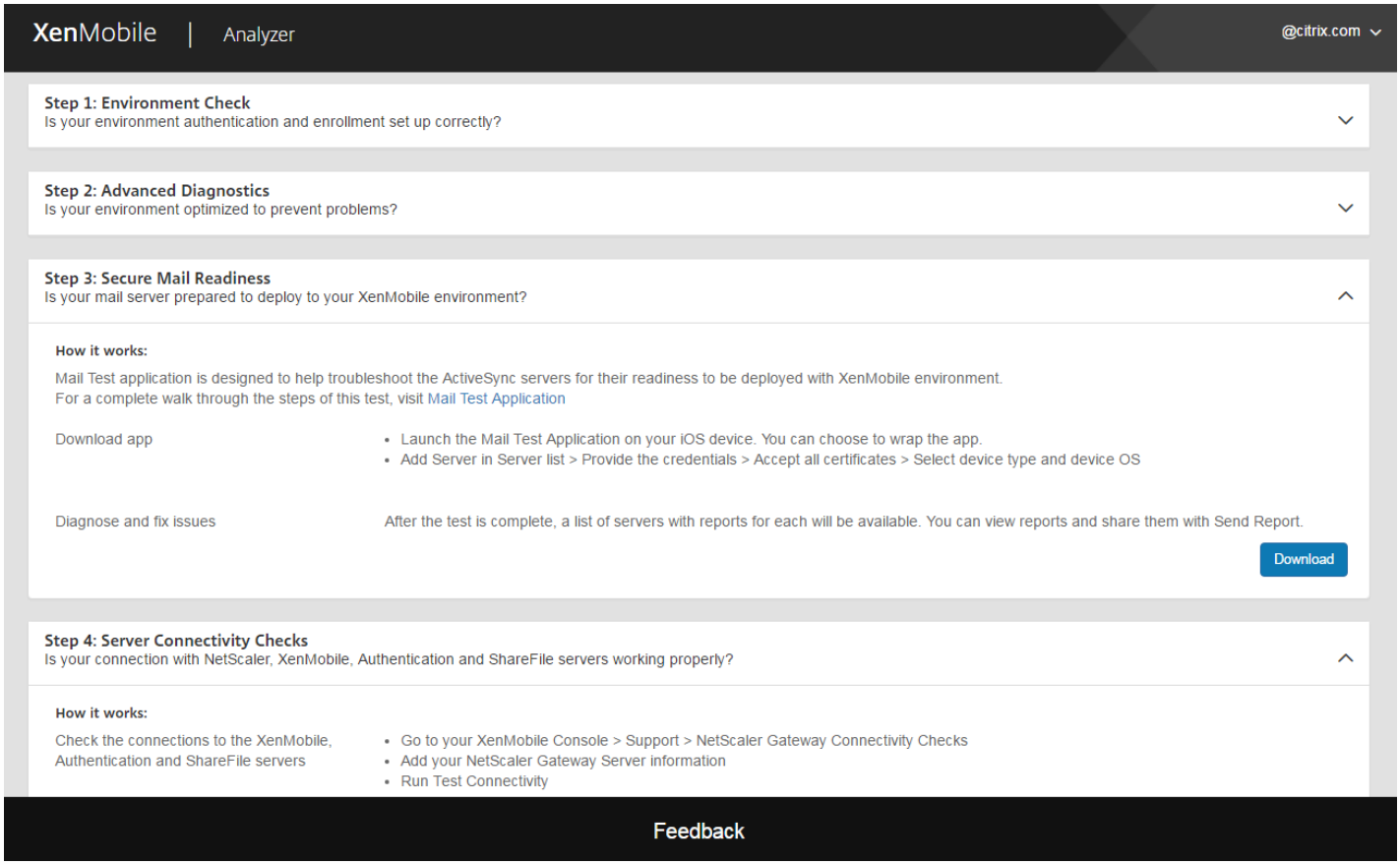
1. **Environment Check**: In diesem Schritt richten Sie Tests ein, um das Setup auf Probleme zu prüfen. Der Schritt bietet auch Empfehlungen und Lösungen zu Problemen bei der Registrierung und Authentifizierung von Geräten und Benutzern.



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.

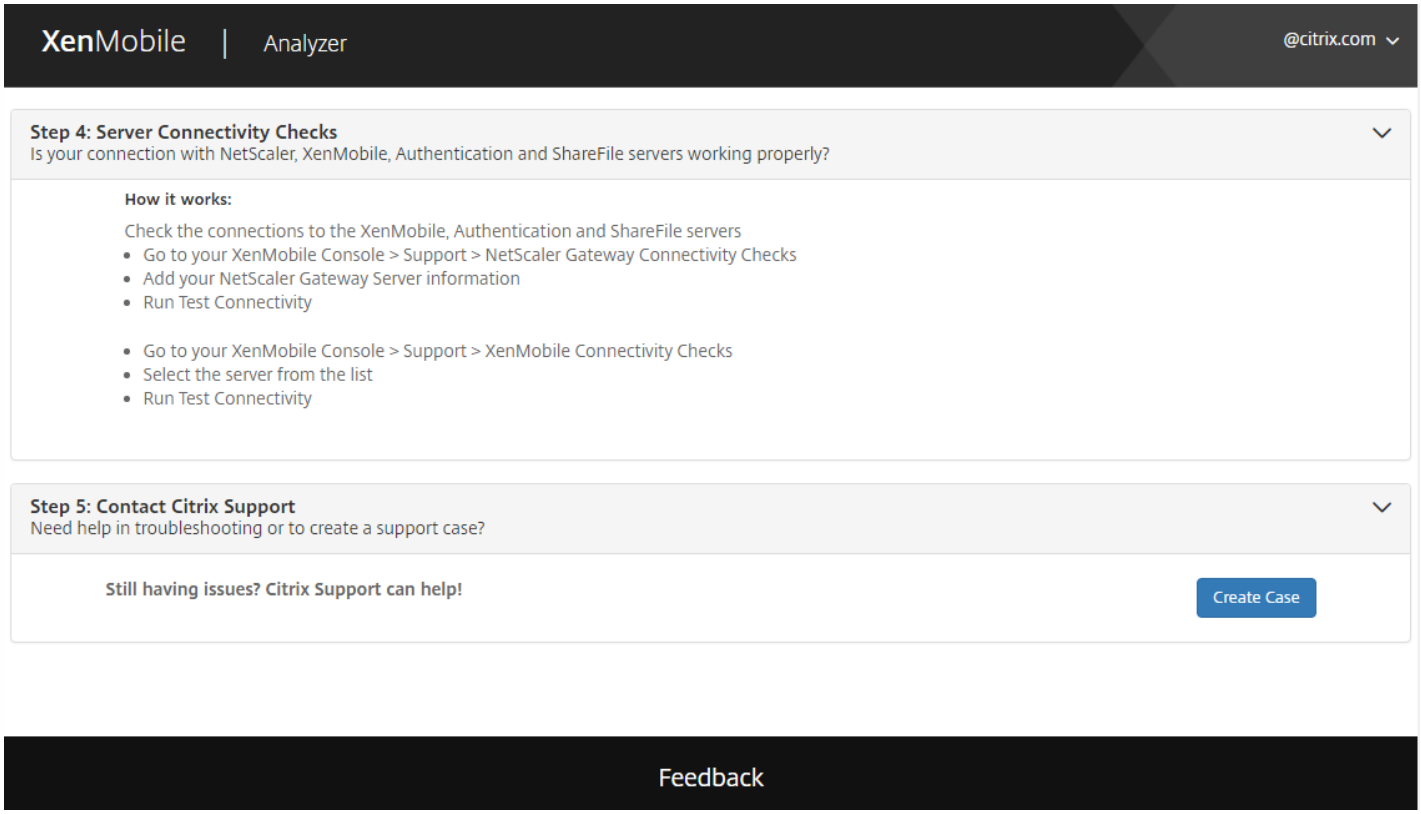


3. **Secure Mail Readiness**: In diesem Schritt werden Sie zum Download der Anwendung XenMobile Exchange ActiveSync Test geleitet. Die Anwendung unterstützt Sie bei den Vorbereitungen, damit sichergestellt ist, dass die ActiveSync-Server für die Bereitstellung mit einer XenMobile-Umgebung bereit sind.



4. **Server Connectivity Checks**: In diesem Schritt testen Sie die Konnektivität Ihrer Server.

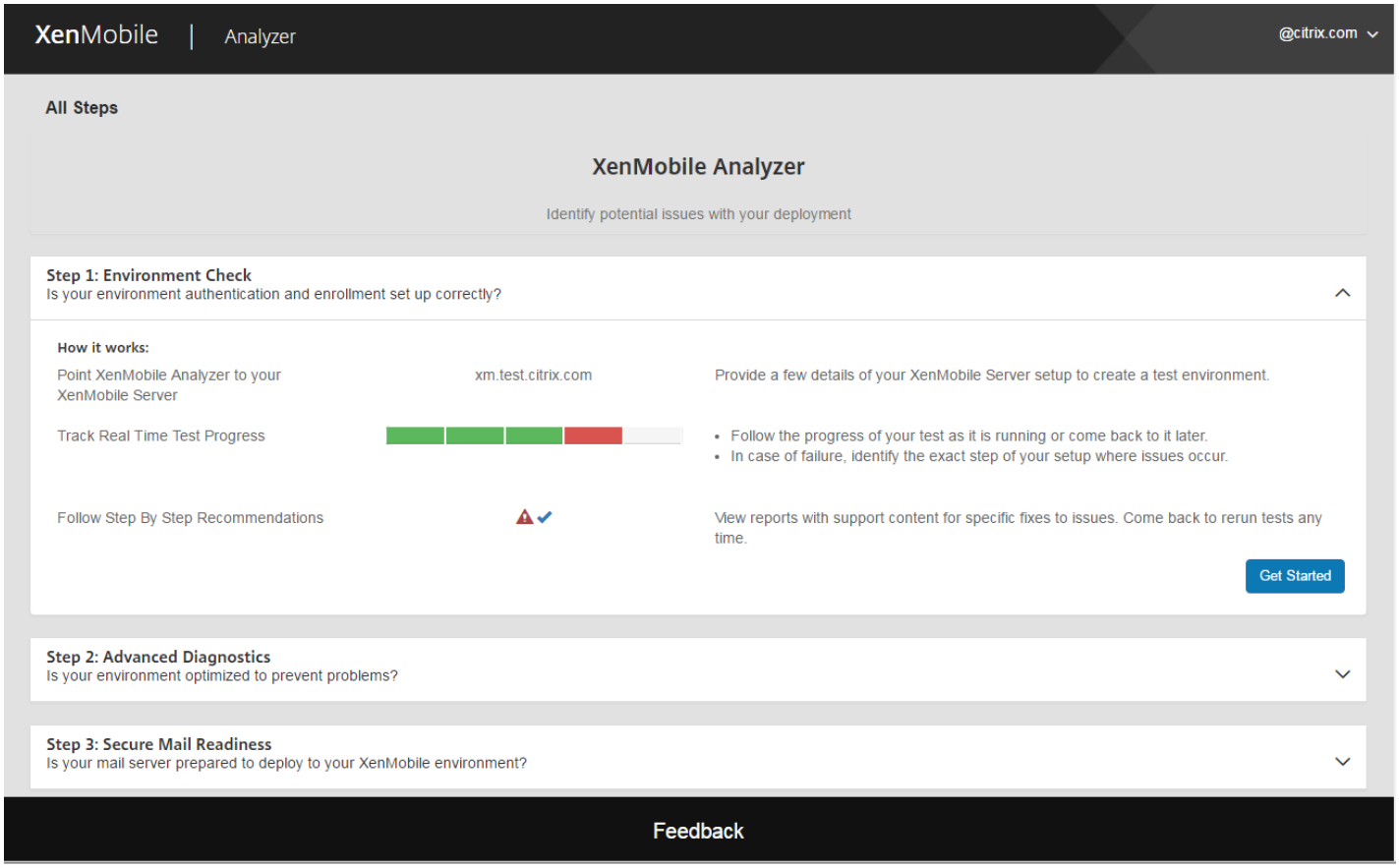
5. **Contact Citrix Support**: In diesem Schritt werden Sie zur Supportsite weitergeleitet, wo Sie einen Citrix Supportfall erstellen können, wenn Sie immer noch Probleme haben.



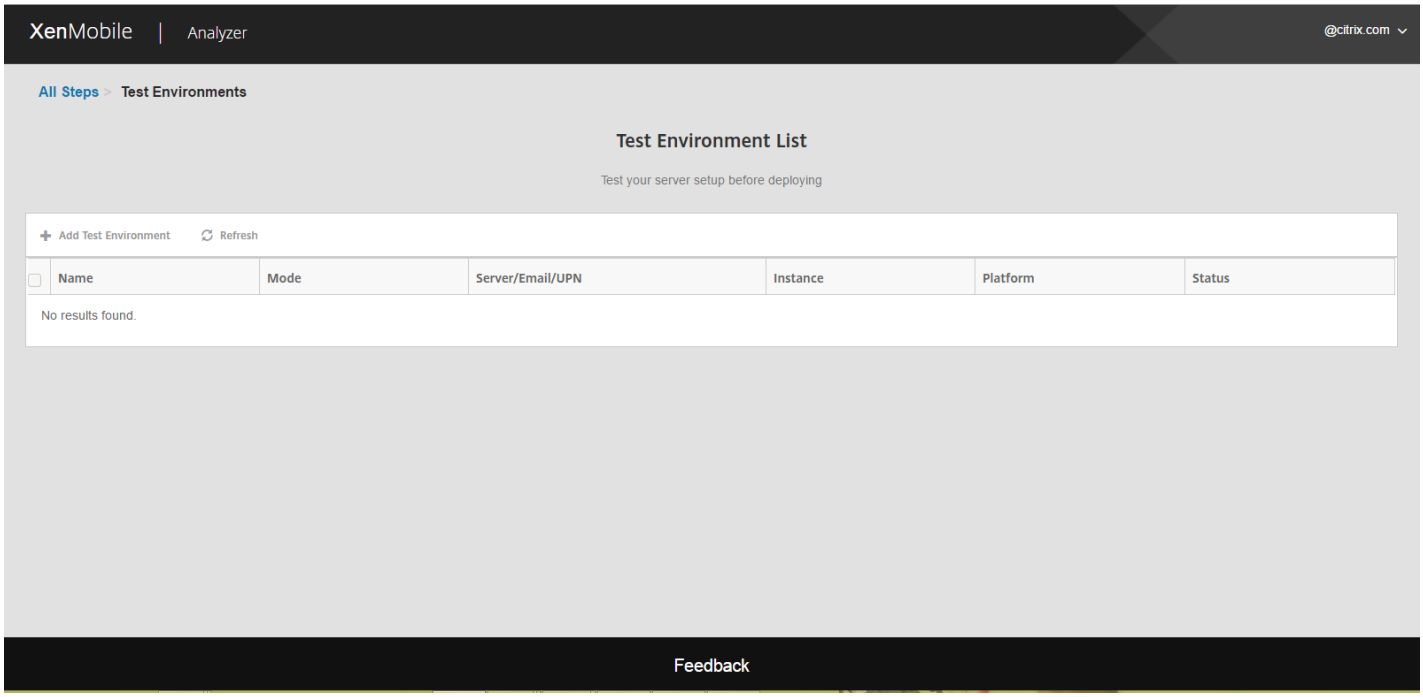
In den folgenden Abschnitten werden die Schritte detailliert erläutert.

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**.

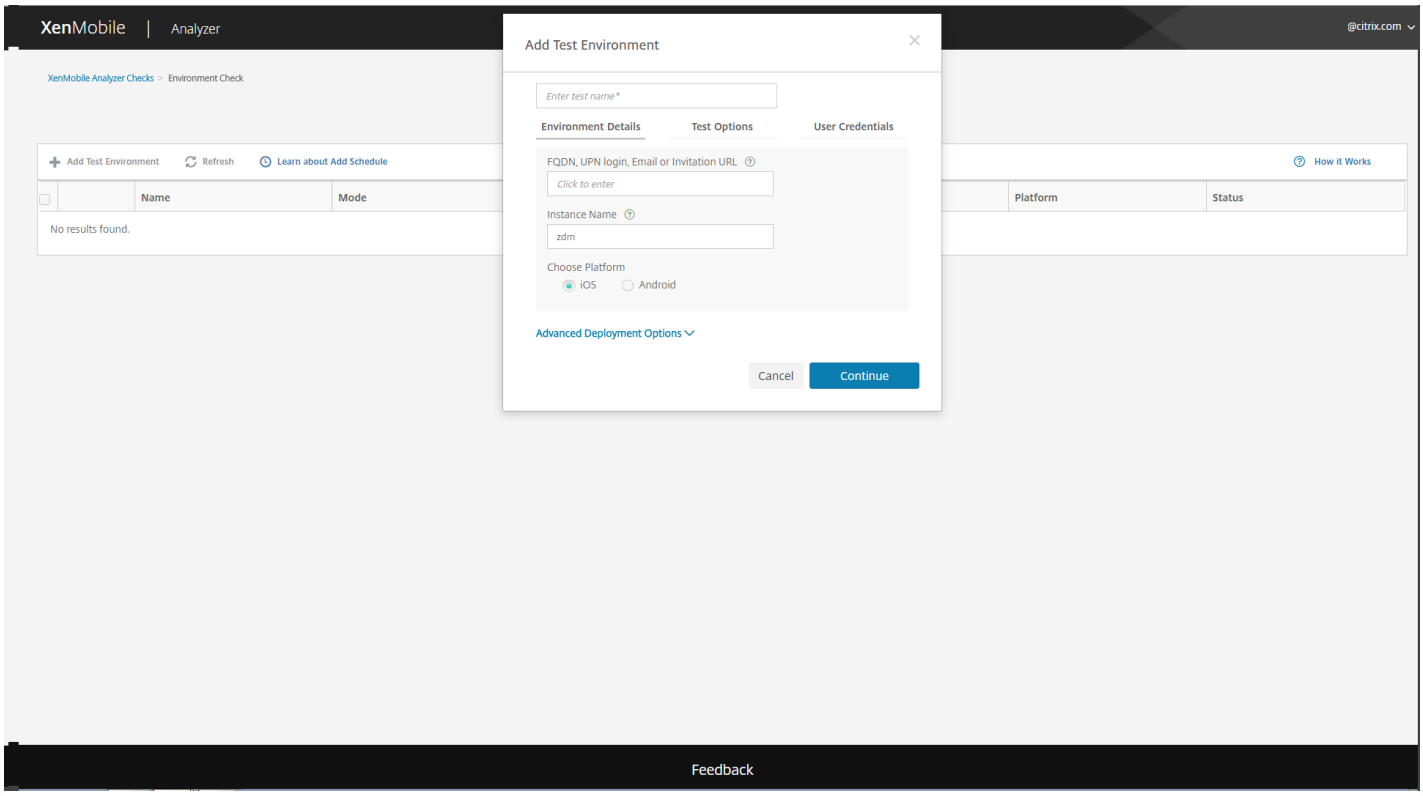


3. Klicken Sie auf **Add Test Environment**.



4. Führen Sie im Dialogfeld **Add Test Environment** die folgenden Schritte aus:

Zu dem Screenshot oben muss erwähnt werden, dass Worx Home jetzt Secure Hub heißt.



a. Geben Sie einen eindeutigen Namen für den Test ein, damit Sie den Test zukünftig leicht identifizieren können.

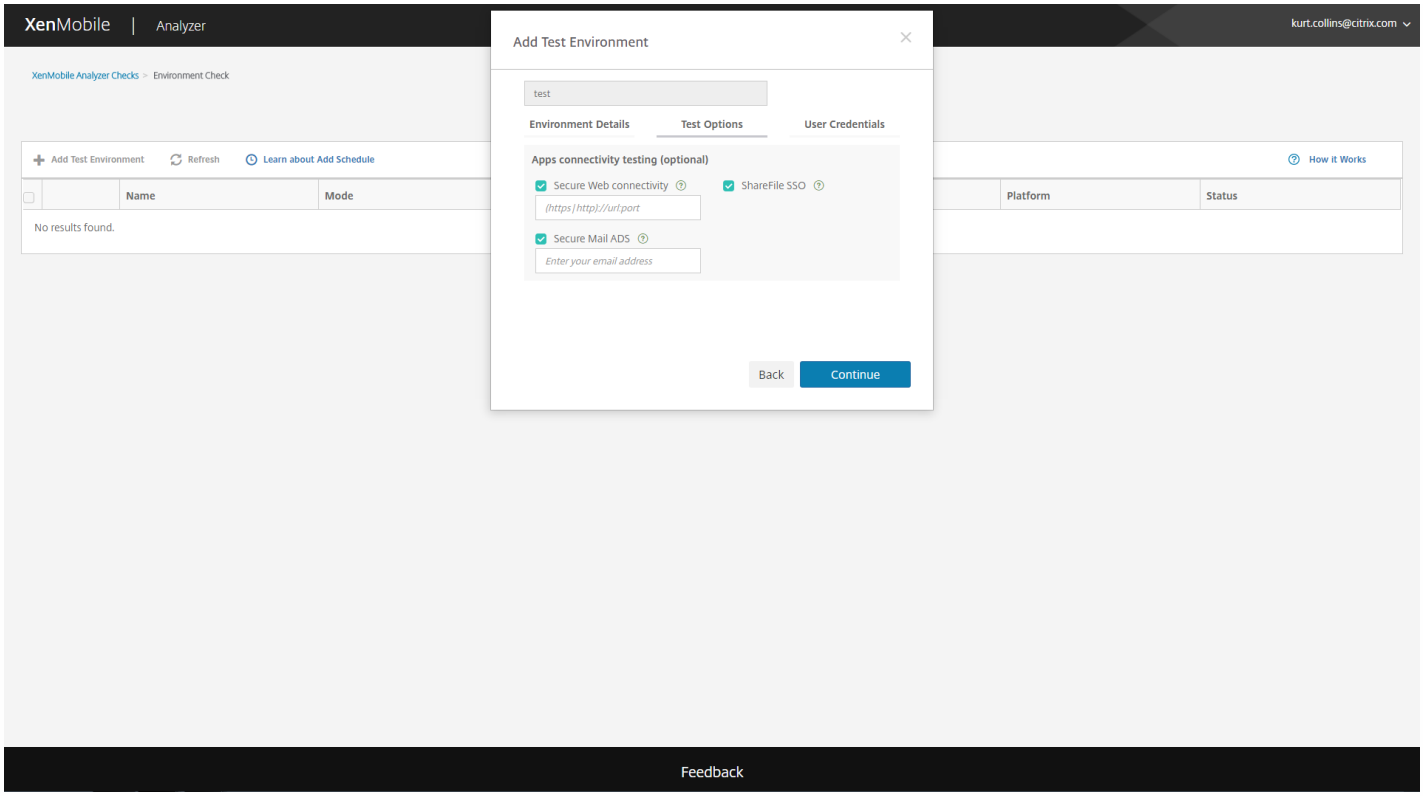
b. Geben Sie im Feld **FQDN, UPN login, Email or URL Invitation** die Informationen ein, die für den Zugriff auf den Server verwendet werden sollen.

c. Wenn Sie eine benutzerdefinierte Instanz verwenden, geben Sie den Wert in **XMS Instance** ein.

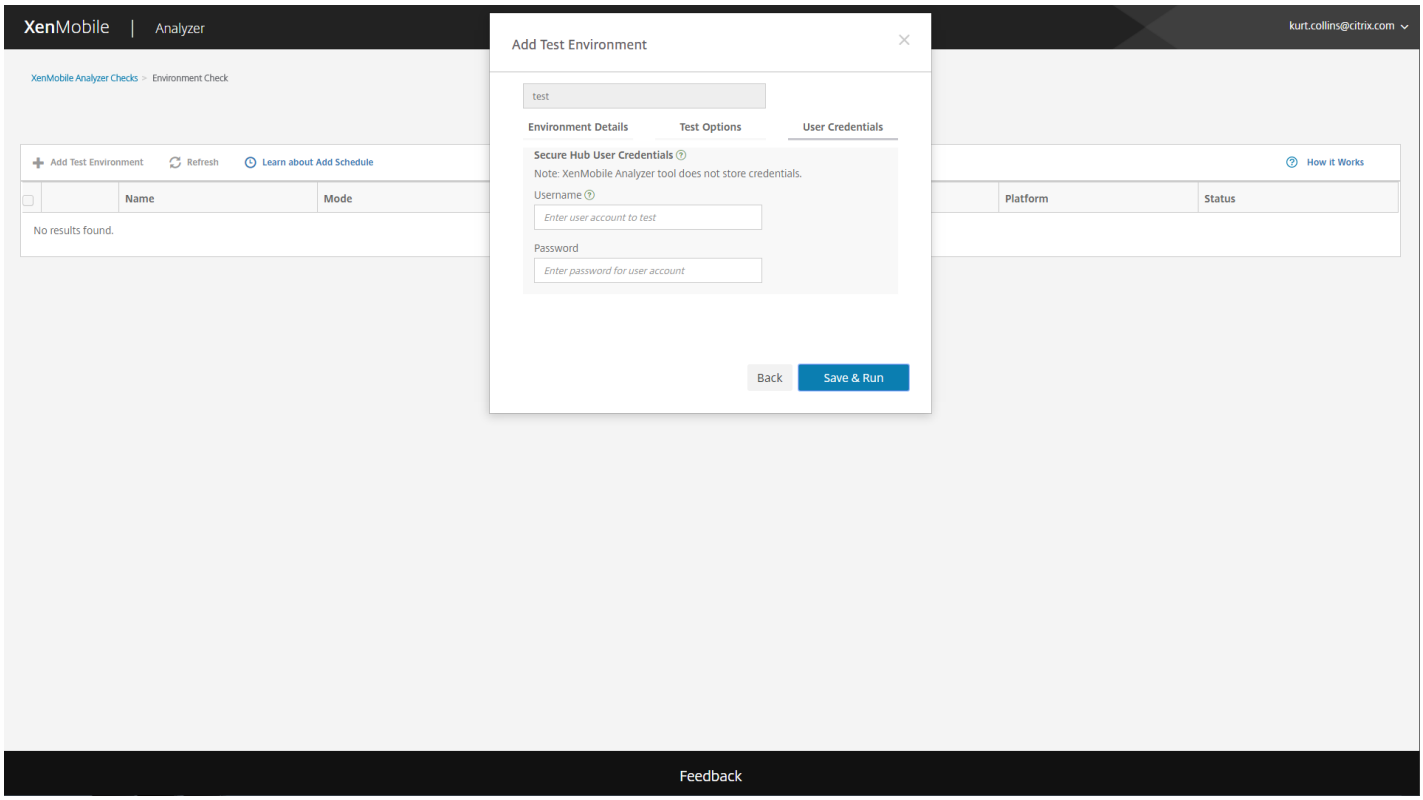
d. Wählen Sie unter **Choose Platform** entweder **iOS** oder **Android** als Plattform für die Tests aus.

e. Wenn Sie **Advanced Deployment Options** in der Liste **Deployment Mode** erweitern, können Sie den XenMobile-Bereitstellungsmodus auswählen. Es stehen die Optionen **Enterprise (MDM + MAM)**, **App Management (MAM)** und **Device Managment (MDM)** zur Verfügung.

Zu dem Screenshot oben muss erwähnt werden, dass Worx Home jetzt Secure Hub heißt.



5. Klicken Sie auf **Continue**.



Zu dem Screenshot oben muss erwähnt werden, dass WorxWeb jetzt Secure Web und WorxMail jetzt Secure Mail heißt.

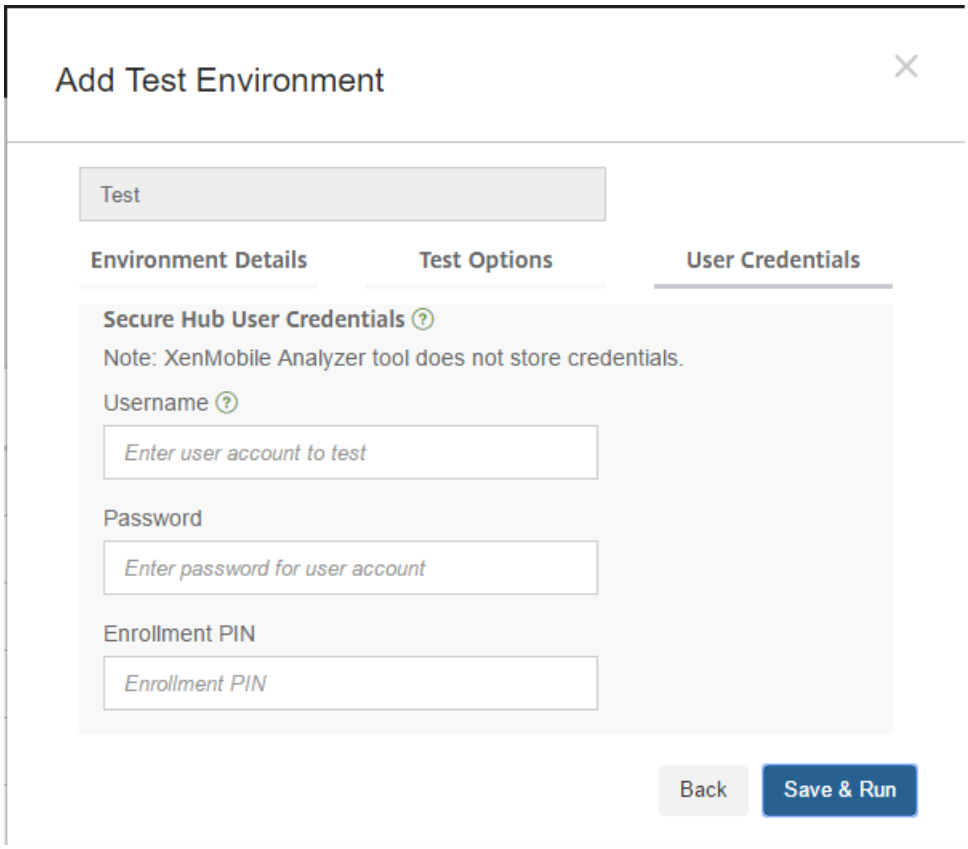
6. Sie können die auf Anwendungsebene auszuführenden Tests auswählen. Wählen Sie einen oder mehrere der folgenden Tests:

a. **Secure Web micro VPN Connectivity with intranet sites**: Geben Sie eine Intranet-URL an. Das Tool testet die Erreichbarkeit der URL. Dadurch werden mögliche Konnektivitätsprobleme in der Secure Web-App erkannt, die beim Versuch, Intranet-URLs zu erreichen, auftreten können.

b. **Secure Mail ADS**: Geben Sie die E-Mail-Adresse eines Benutzers an. Hiermit wird die Autodiscovery des Microsoft Exchange-Servers in der XenMobile-Umgebung getestet. Es wird ermittelt, ob es Probleme im Zusammenhang mit Secure Mail Autodiscovery gibt.

c.**ShareFile SSO**: Bei diesem Test werden die ShareFile-DNS-Auflösung und das ShareFile-SSO mit den angegebenen Anmeldeinformationen geprüft.

7. Klicken Sie auf **Continue**.

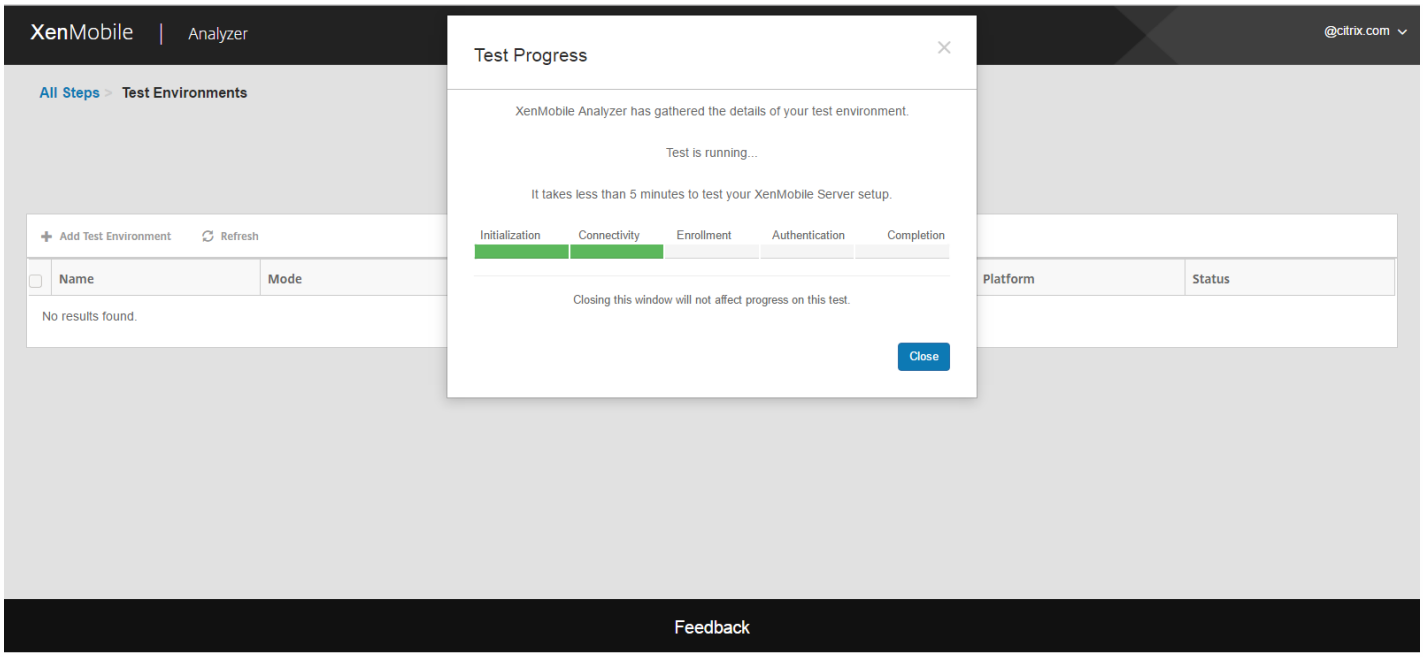


8. Abhängig von Ihrem Serversetup werden ggf. andere Felder zur Eingabe von Anmeldeinformationen angezeigt. Mögliche Felder sind **Username** allein, **Username** und **Password** oder **Username**, **Password** und **Enrollment PIN.**

9. Nachdem Sie diese Informationen eingegeben haben, klicken Sie auf **Save & Run**, um die Tests zu starten.

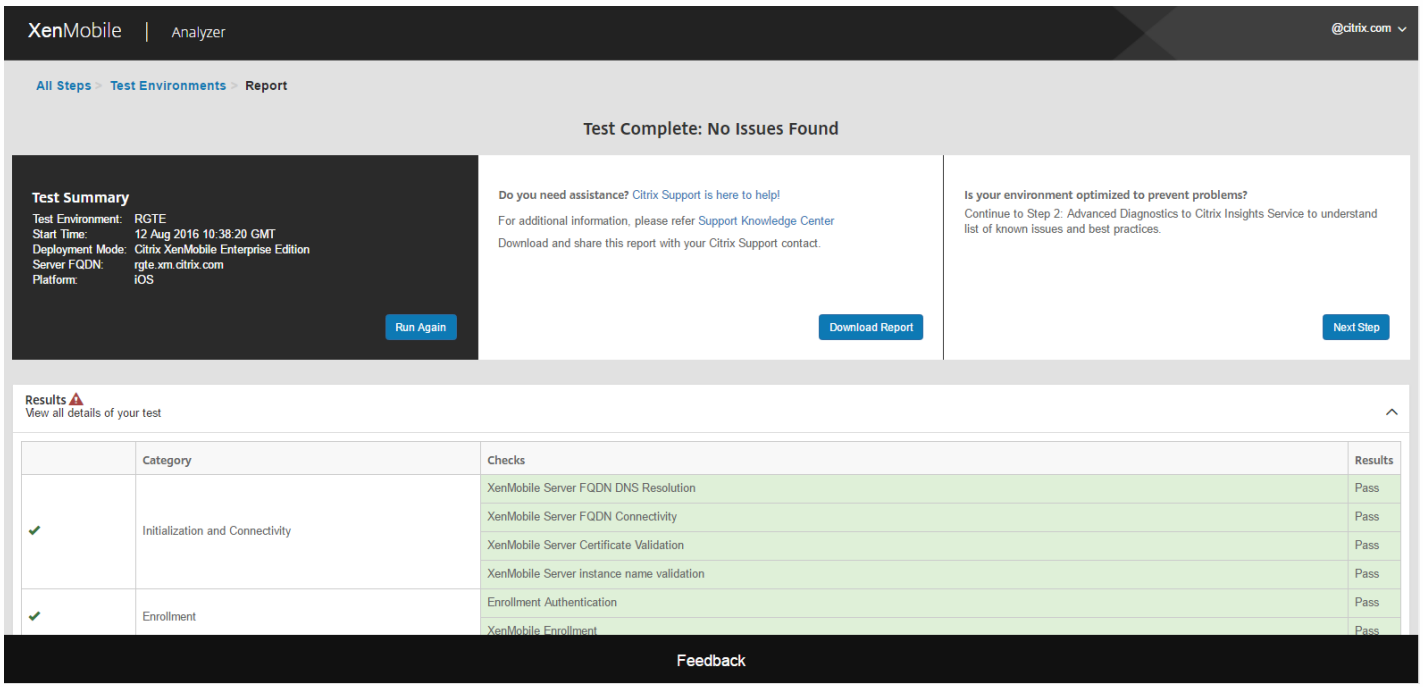
Eine Statusanzeige wird angezeigt. Sie können das Statusdialogfeld offen lassen oder schließen, die Tests werden fortgesetzt.

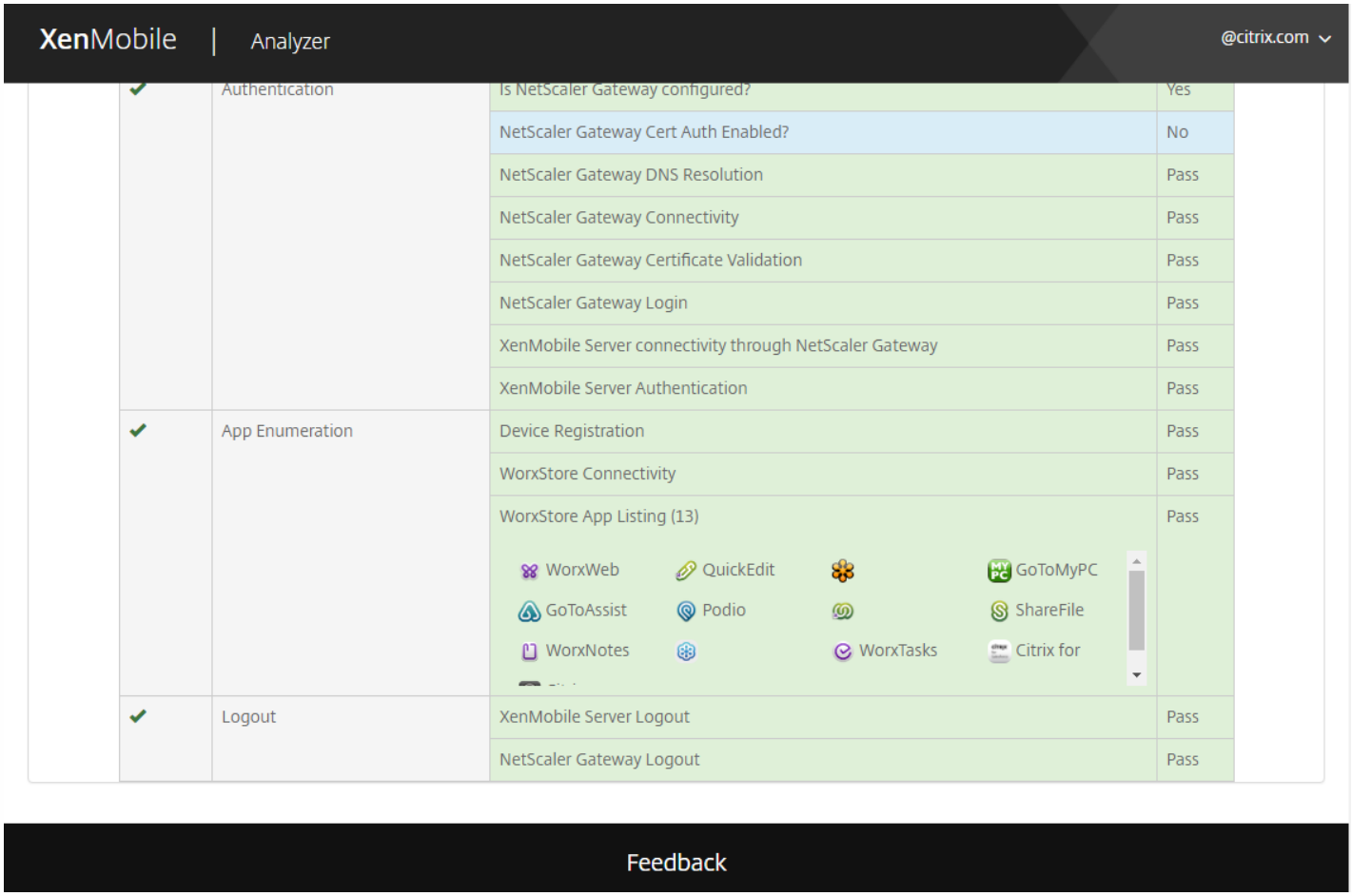
Bestandene Tests werden grün angezeigt. Nicht bestandene Tests werden rot angezeigt.



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.





Zu dem obigen Screenshot ist zu erwähnen, dass WorxWeb mittlerweile Secure Web heißt, WorxNotes heißt jetzt Secure Notes, WorxTasks heißt Secure Tasks und WorxStore heißt XenMobile Store.

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, die das Tool ausgeführt hat, sowie die Ergebnisse anzuzeigen.

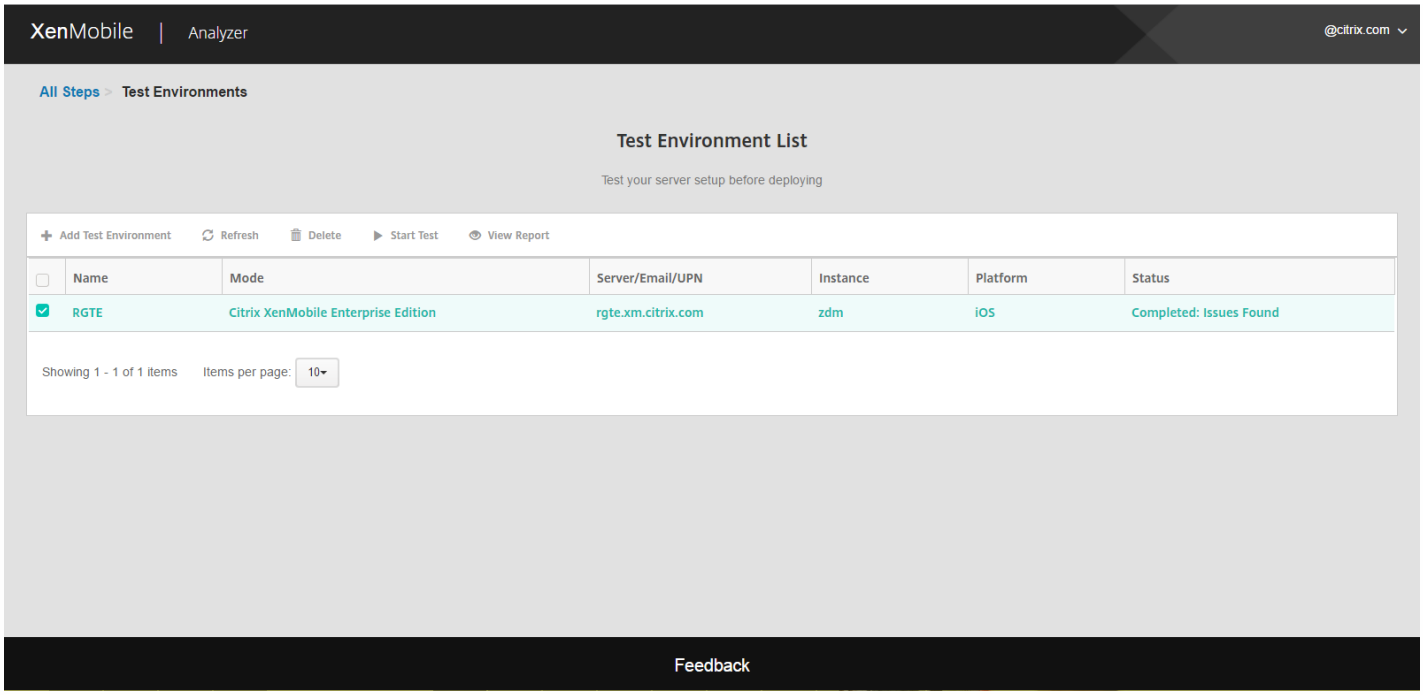
   a. Durch Klicken auf **Download Report** laden Sie den Bericht herunter.

   b. Wenn Sie zur Liste mit den Testumgebungen zurückkehren möchten, klicken Sie auf **Test Environments**.

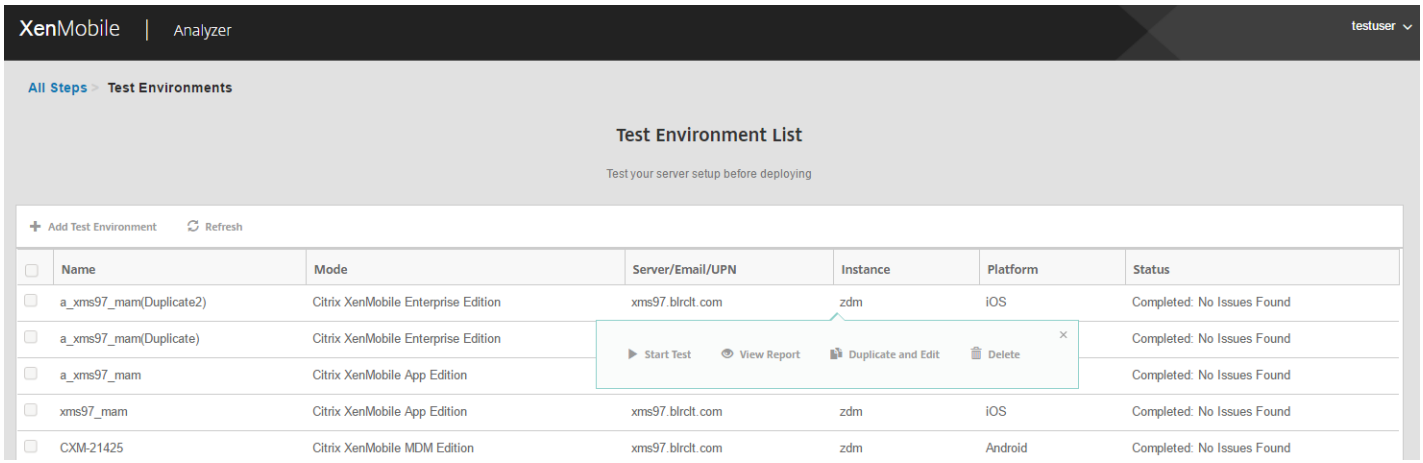
   c.Zum Wiederholen des Tests klicken Sie auf **Run Again**.

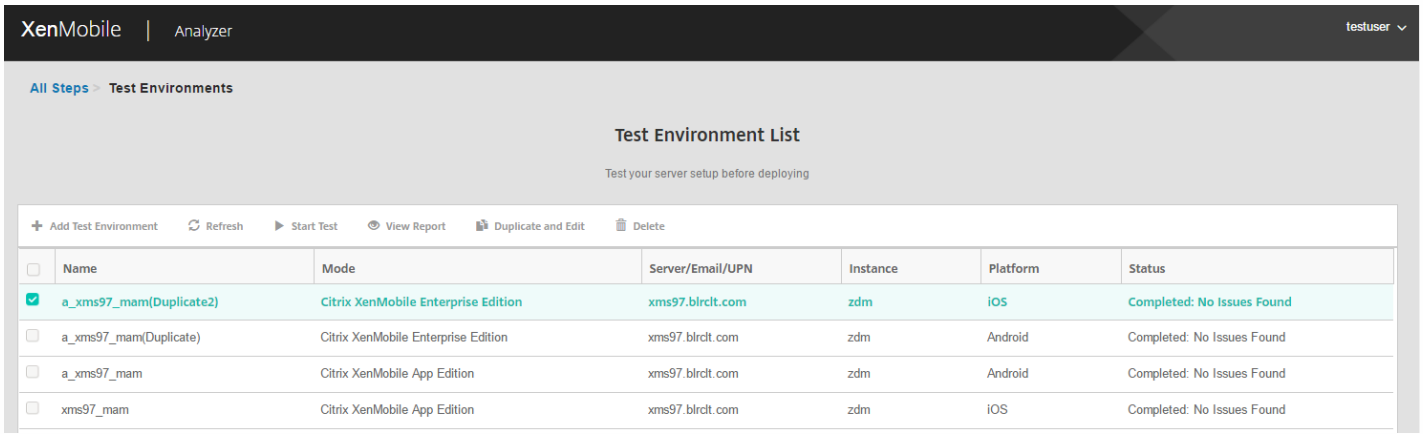
   d. Wenn Sie einen anderen Test wiederholen möchten, wechseln Sie zu **Test Environments**, wählen Sie den Test aus und klicken Sie auf **Start Test**.

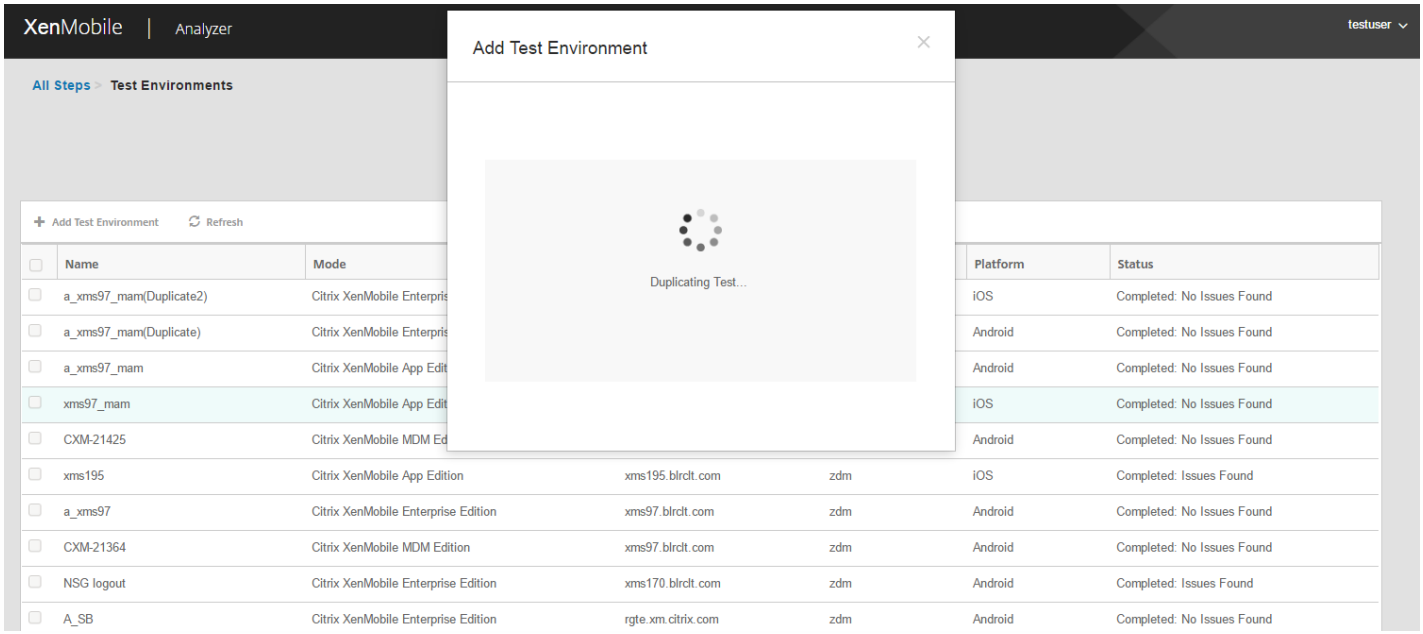
   e. Zum Fortfahren mit dem nächsten Schritt von XenMobile Analyzer klicken Sie auf **Next Step**.

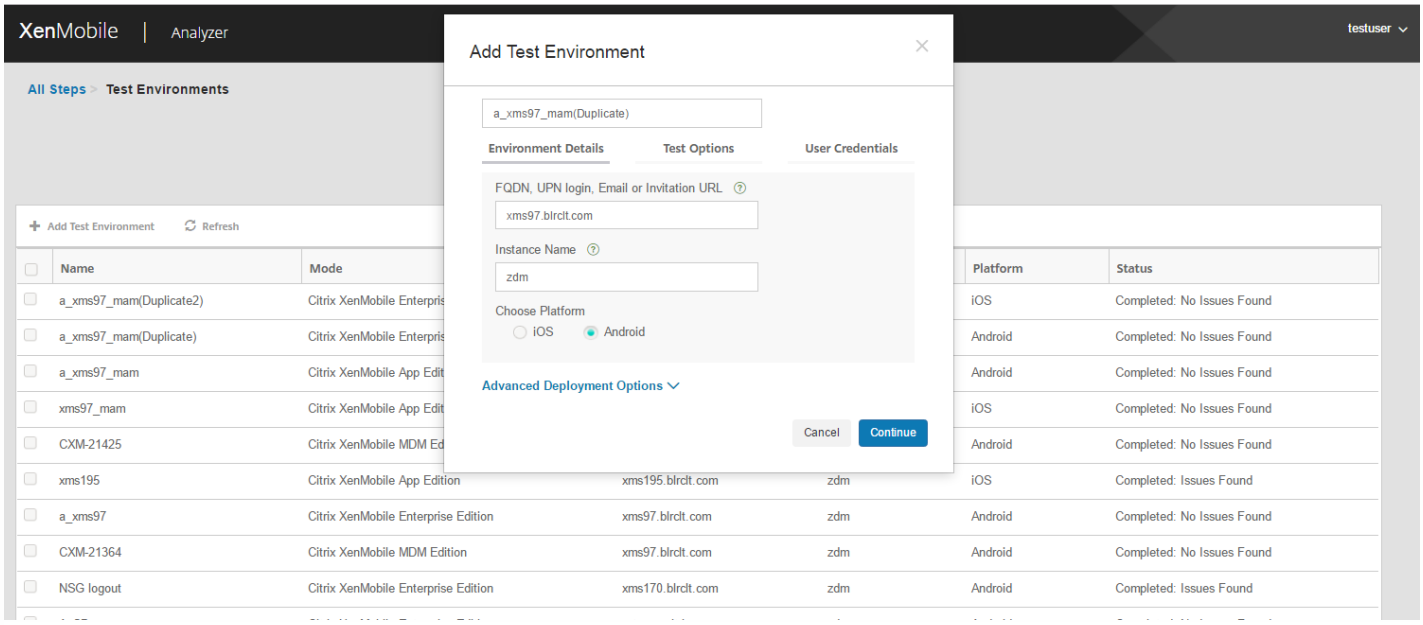


10. Sie können auf der Seite "Test Environments" Tests kopieren und bearbeiten. Dazu wählen Sie einen Test aus und klicken Sie dann auf **Duplicate and Edit**. Es wird dann eine Kopie des ausgewählten Tests erstellt und das Dialogfeld "Add Test Environment" geöffnet, in dem Sie den Test ändern können.









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**: In diesem Schritt werden Sie angewiesen, Informationen über Ihre Umgebung zu sammeln und die Informationen an Citrix Insight Services hochzuladen. Das Tool analysiert Ihre Daten und erstellt einen personalisierten Bericht mit empfohlenen Lösungen.

- **Step 3** - **Secure Mail Readiness**: Dieser Schritt führt Sie durch das Herunterladen und Ausführen der XenMobile 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.
- Bei den Tests der Secure Web-Intranetkonnektivität ist die Eingabe mehrerer URLs in das Textfeld nicht zulässig.
- Das Secure Hub-Feature zur Authentifizierung gemeinsam genutzter Geräte wird nicht unterstützt.
- Secure Web-Tests prüfen nur die Verbindung mit den eingegebenen URLs und nicht die Authentifizierung bei den zugehörigen Sites.
- Für PIN-basierte Authentifizierungsmodi werden Sie bei Auswahl des Secure Mail ADS-Tests aufgefordert, für die Ausführung des Tests ein Kennwort einzugeben. Das Kennwort dient nicht zur Registrierung oder Authentifizierung.

Behobene Probleme

Die folgenden Probleme mit XenMobile Analyzer wurden behoben:

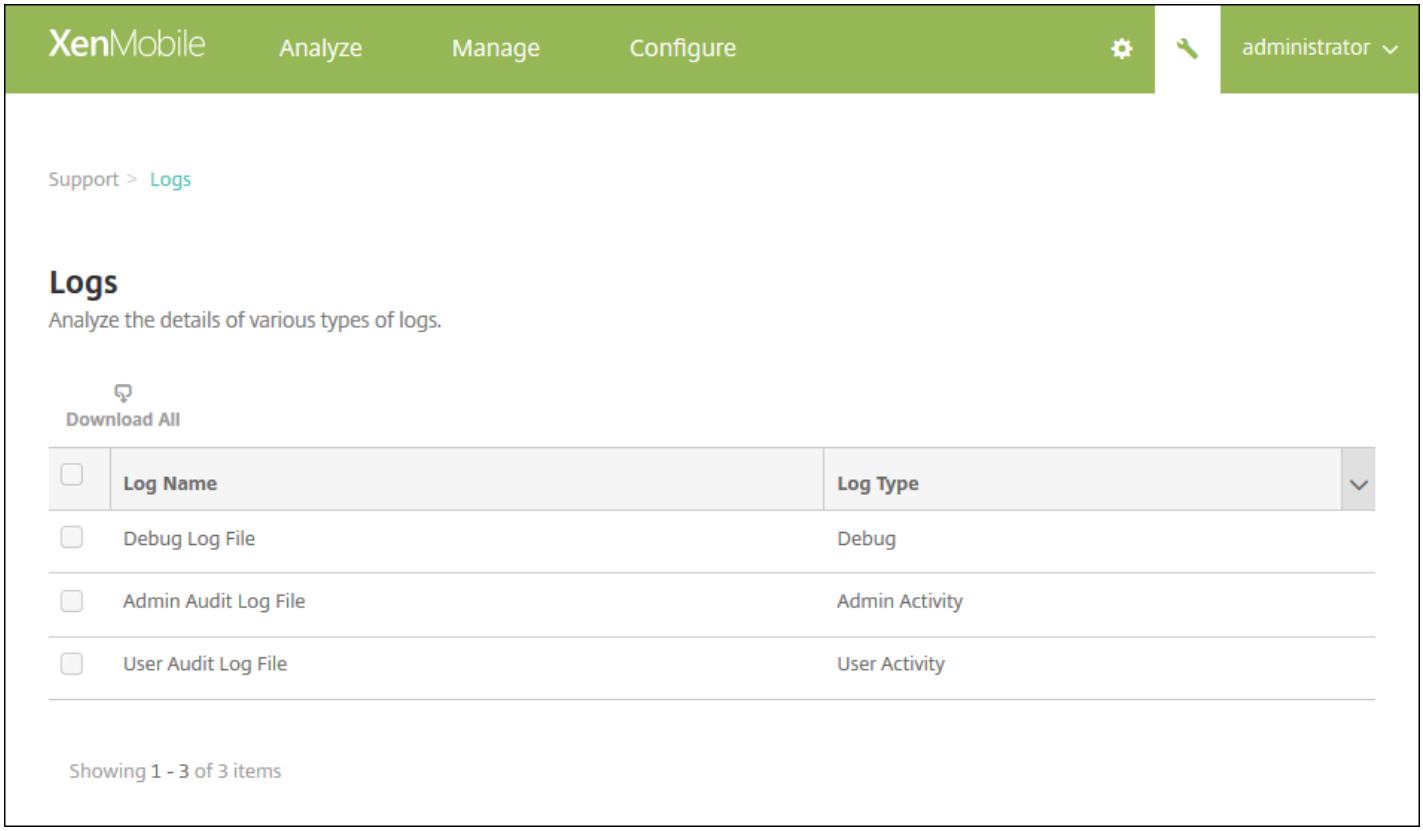
- Wenn Sie eine Registrierungseinladung testen, wird der Test bestanden, die Registrierungseinladung wird jedoch nicht eingelöst.

Anzeigen und Analysieren von Protokolldateien in XenMobile

Feb 24, 2017

1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite **Support** wird geöffnet.

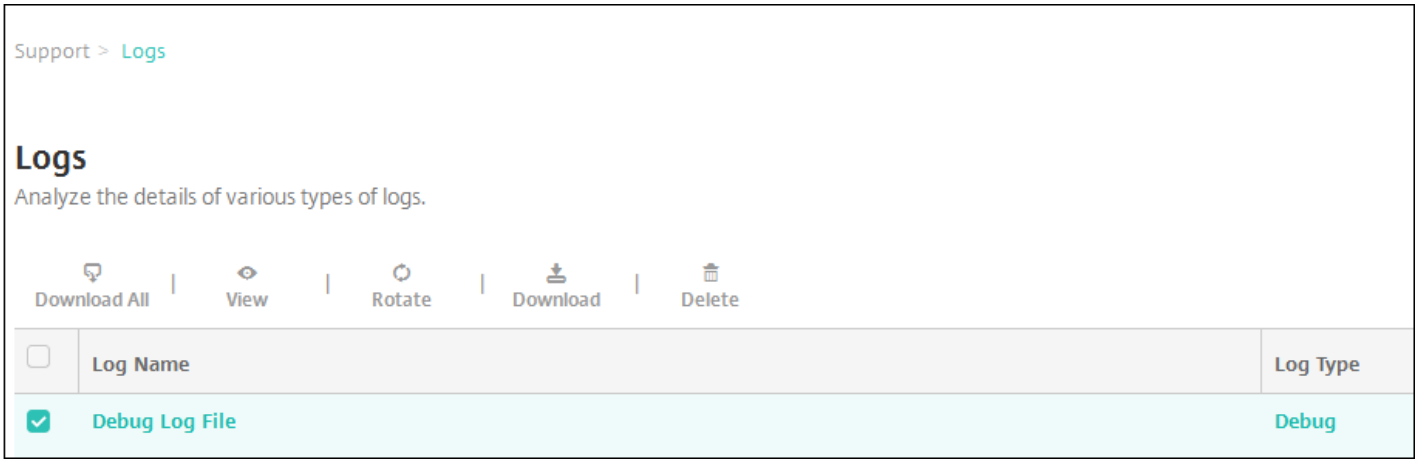
2. Klicken Sie unter **Protokollvorgänge** auf **Protokolle**. Die Seite **Protokolle** wird angezeigt. Einzelne Protokolle werden in einer Tabelle angezeigt.



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.

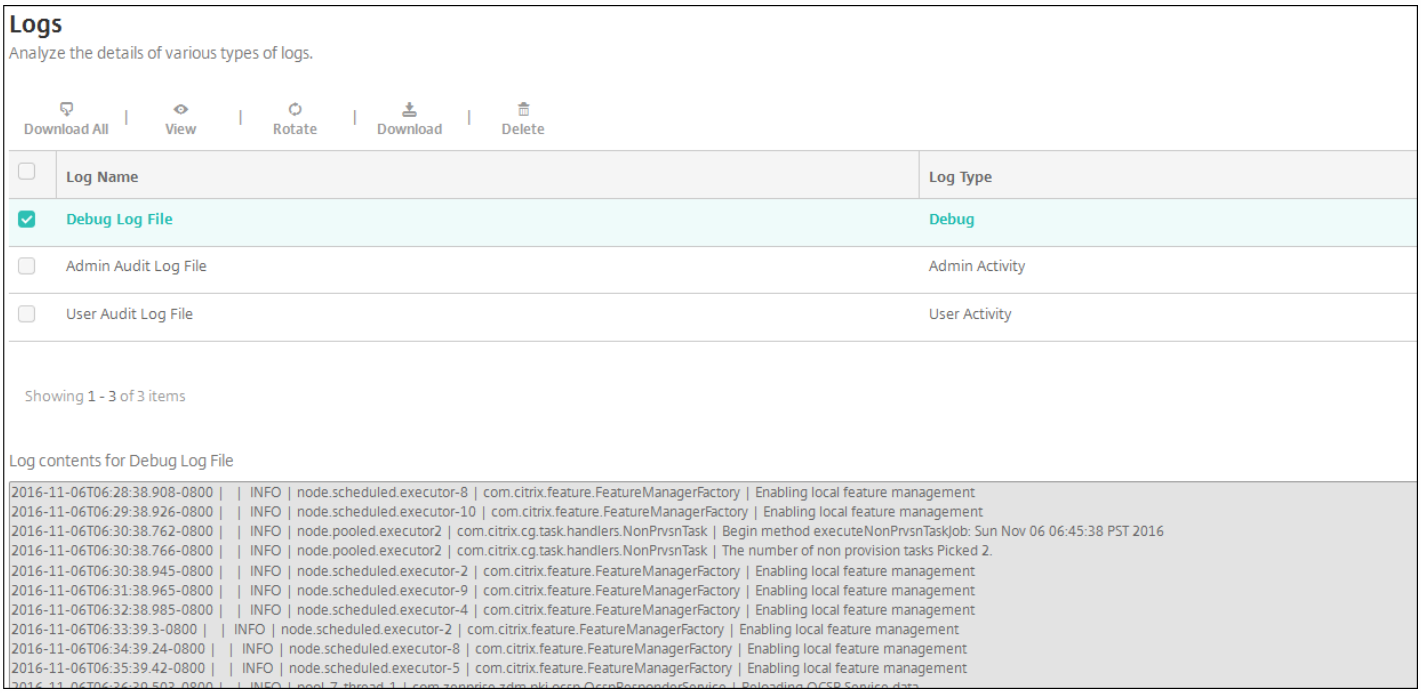


Hinweis:

- Wenn Sie mehr als eine Protokolldatei auswählen, sind nur die Aktionen **Alle herunterladen** und **Archivieren** 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.



REST APIs

Feb 24, 2017

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 für 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.

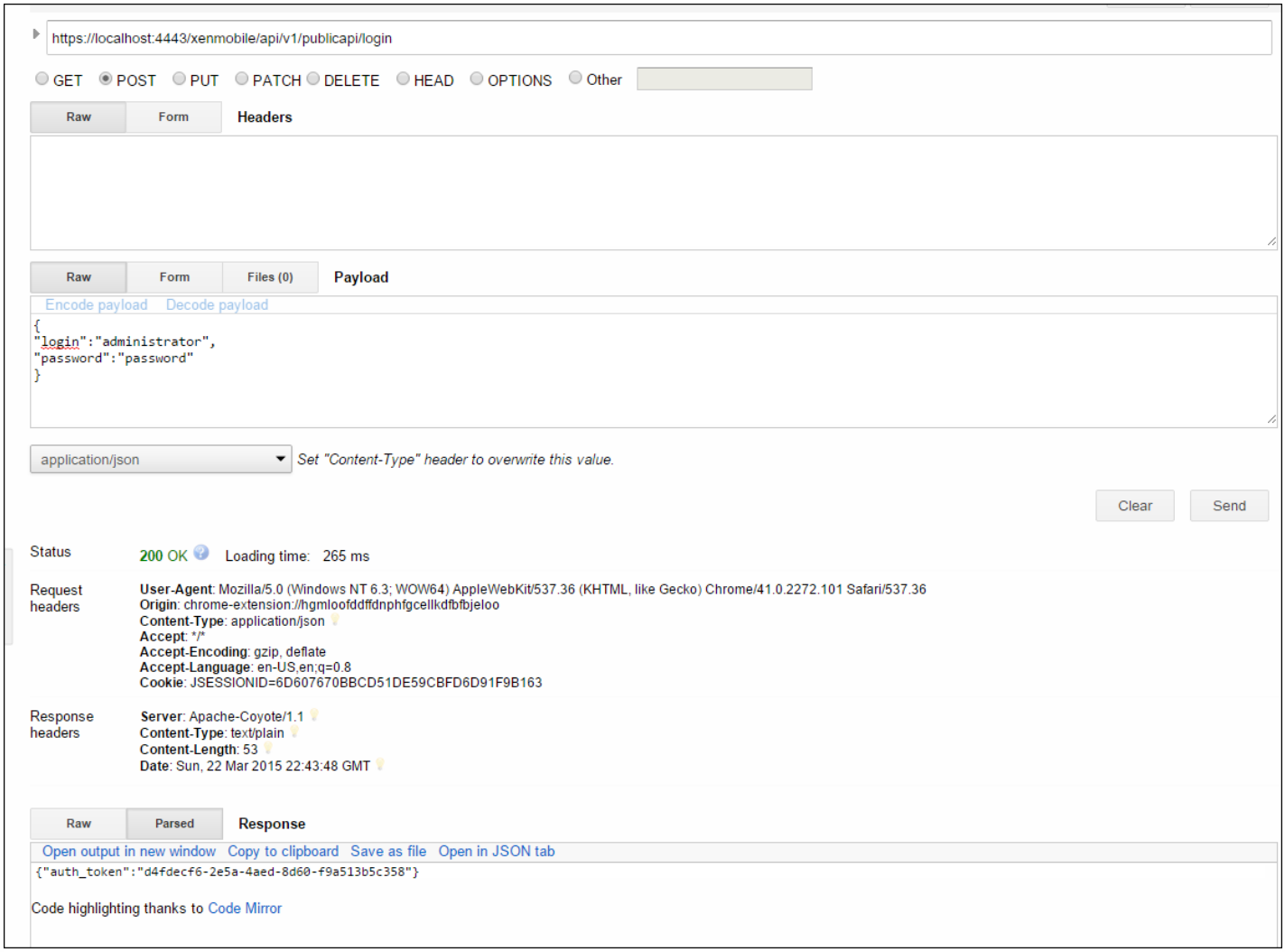
Login

URL: https://<hostname>:<portnummer>/xenmobile/api/v1/authentication/login

Anforderung: { "login":"administrator", "password":"password" }

Methodentyp: POST

Inhaltstyp: application/json



SOAP APIs

Feb 24, 2017

Citrix unterstützt SOAP-Webdienst-APIs nicht mehr. Verwenden Sie stattdessen die REST-APIs. Weitere Informationen finden Sie unter REST-APIs.

XenMobile Mail Manager 10.x

Feb 24, 2017

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 unter dem Namen "IgnorableErrors" für jeden Fehler, der ignoriert werden soll, hinzu. Fügen Sie dem Knoten "IgnorableErrors" einen untergeordneten Knoten "Fehler" mit dem entsprechenden Text im Abschnitt "CDATA" hinzu. 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 manchmal nicht bei Abfragen für Active Directory-Gruppen mit 1000 oder mehr Benutzern. [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]

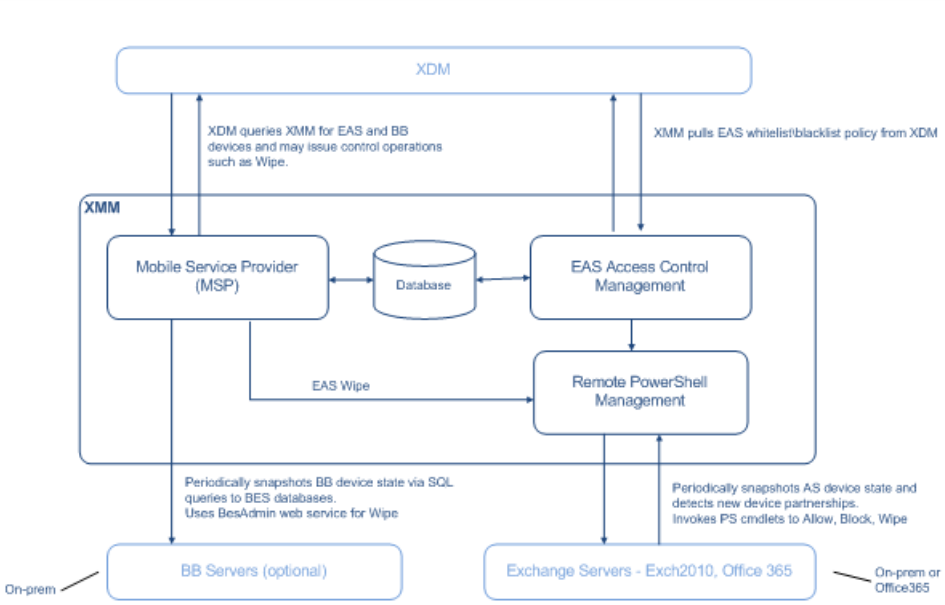
Beim ersten größeren Snapshot nach der Erstinstallation trat gelegentlich ein Fehler auf, der verhinderte, dass XenMobile Mail Manager

einen weiteren größeren Snapshot ausführen konnte, bis der XenMobile Mail Manager-Dienst neu gestartet wurde. Dieser Fehler tritt nicht mehr auf. [CXM-5536]

Architektur

Feb 24, 2017

Die folgende Abbildung zeigt die wichtigsten Komponenten von XenMobile Mail Manager. Ein detailliertes Architekturdiagramm finden Sie im Artikel "Reference Architecture for On-Premises Deployments" des XenMobile-Bereitstellungshandbuchs.



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

Feb 24, 2017

Die folgenden Mindestsystemanforderungen müssen für XenMobile Mail Manager erfüllt verwenden:

- Windows Server 2012 R2, Windows Server 2008 R2 (Englisch-Sprachversion erforderlich)
- Microsoft SQL Server 2016, SQL Server 2012, SQL Server 2012 Express LocalDB oder SQL Server Express 2008
- 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

E-Mail-Clients auf Geräten

Nicht alle E-Mail-Clients geben konstant dieselbe ActiveSync-ID für das Gerät zurück. Da XenMobile Mail Manager eine eindeutige ActiveSync-ID für jedes Gerät erwartet, werden nur E-Mail-Clients unterstützt, die konstant dieselbe eindeutige ActiveSync-ID für jedes Gerät generieren.Folgende E-Mail-Clients wurden von Citrix getestet und funktionieren einwandfrei:

- HTC-nativer E-Mail-Client
- Samsung-nativer E-Mail-Client
- iOS-nativer E-Mail-Client
- TouchDown für Smartphones

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 von Set-AdServerSettings -ViewEntireForest $true gewährt werden.
- 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. Laut dem Blogbeitrag You Don't Have to Be An Administrator to Run Remote PowerShell Commands kann Set-PSSessionConfiguration verwendet werden, um diese Anforderung zu umgehen, eine Erläuterung dieses Befehls geht jedoch über den Rahmen des vorliegenden Dokuments hinaus.
- Exchange Server muss für die Unterstützung von Remote-PowerShell-Anfragen über HTTP konfiguriert sein. Normalerweise ist nur ein Administrator erforderlich, der folgenden PowerShell-Befehl auf dem Exchange Server ausführt: WinRM QuickConfig.
- Exchange hat zahlreiche Einschränkungsrichtlinien. Eine davon steuert, wie viele gleichzeitige PowerShell-Verbindungen pro Benutzer zugelassen sind. In Exchange 2010 ist die Standardzahl gleichzeitiger Verbindungen pro Benutzer 18. Wenn dieses Limit erreicht ist, kann XenMobile Mail Manager keine Verbindung mit Exchange Server herstellen. Es gibt Methoden zum Ändern der Zahl der maximal zulässigen gleichzeitigen Verbindungen über PowerShell, dies geht jedoch über den Rahmen der vorliegenden Dokumentation hinaus. Bei entsprechendem Interesse lesen Sie die Exchange-Dokumentation zu Einschränkungsrichtlinien für die Remoteverwaltung per PowerShell.

Anforderungen für Office 365 Exchange

- **Berechtigungen**: 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
- **Privilegien**: 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.
- **Einschränkungsrichtlinien**: Exchange hat zahlreiche Einschränkungsrichtlinien. Eine davon steuert, wie viele gleichzeitige PowerShell-Verbindungen pro Benutzer zugelassen sind. In Office 365 kann ein Benutzer standardmäßig drei gleichzeitige Verbindungen haben. 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

Feb 24, 2017

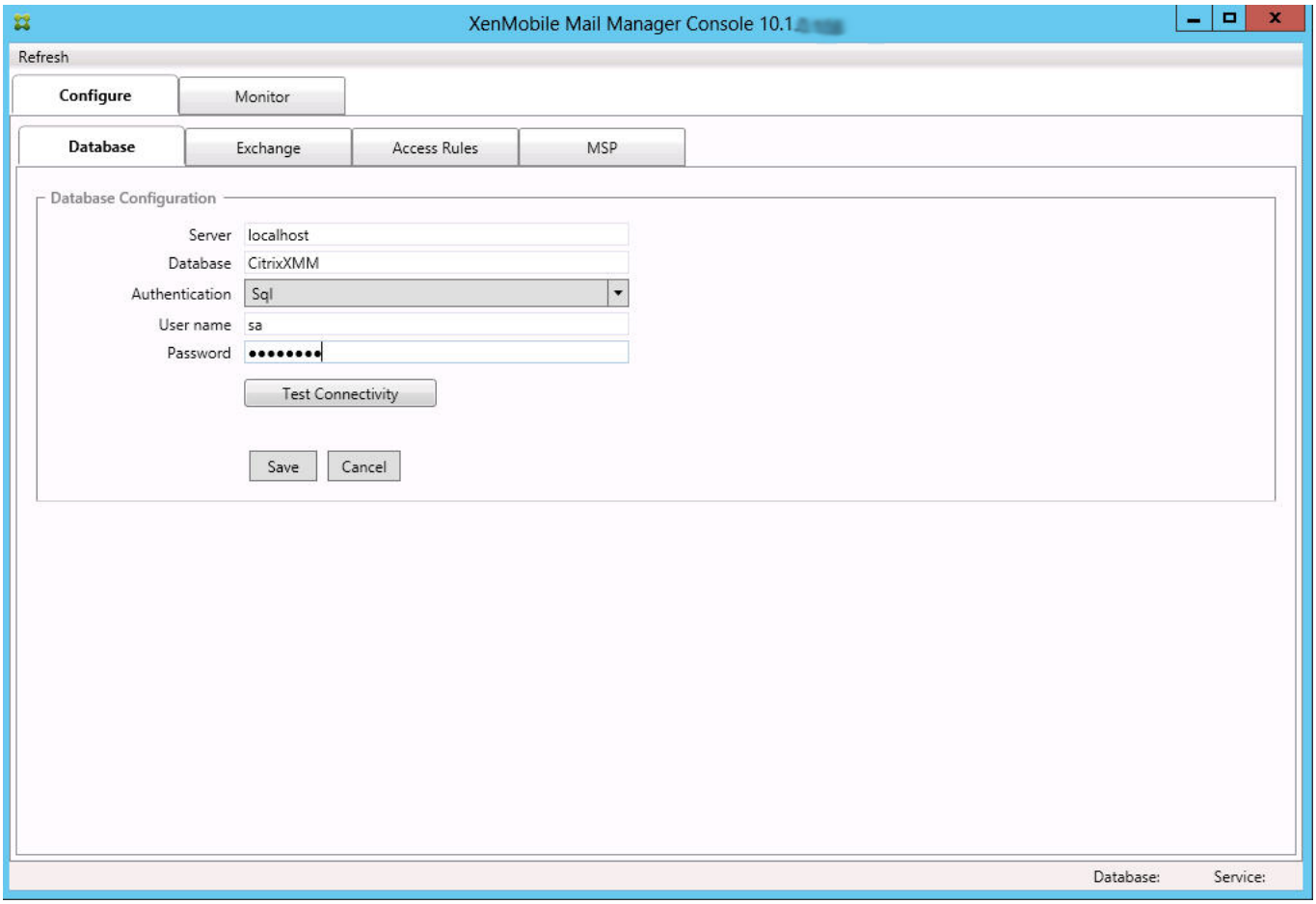
1. Klicken Sie auf die Datei XmmSetup.msi und folgen Sie den Anweisungen des Installers zum Installieren von XenMobile Mail Manager.

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.

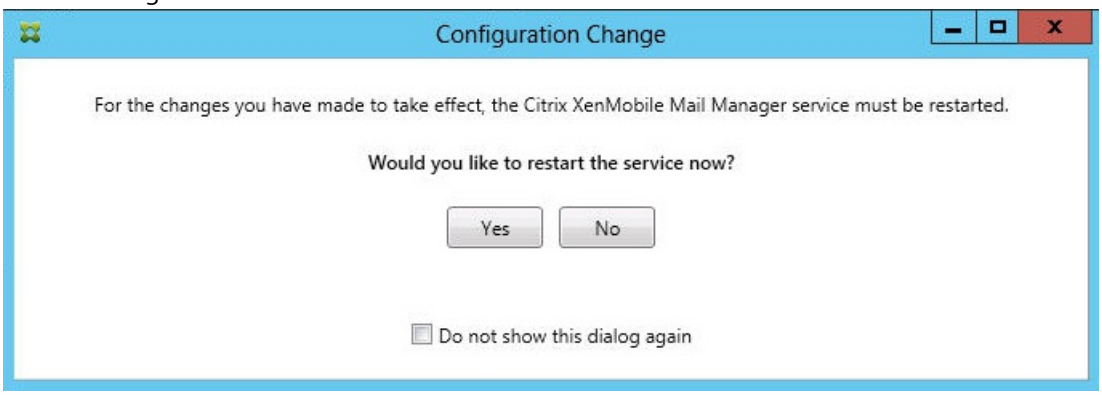
3. Konfigurieren Sie die folgenden Datenbankeigenschaften:
   1. Wählen Sie die Registerkarte **Configure** > **Database**.
   2. Geben Sie den Namen des SQL Server-Computers ein (standardmäßig "localhost").
   3. Behalten Sie den Standarddatenbanknamen "CitrixXmm" bei.
   4. Wählen Sie einen der folgenden 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.

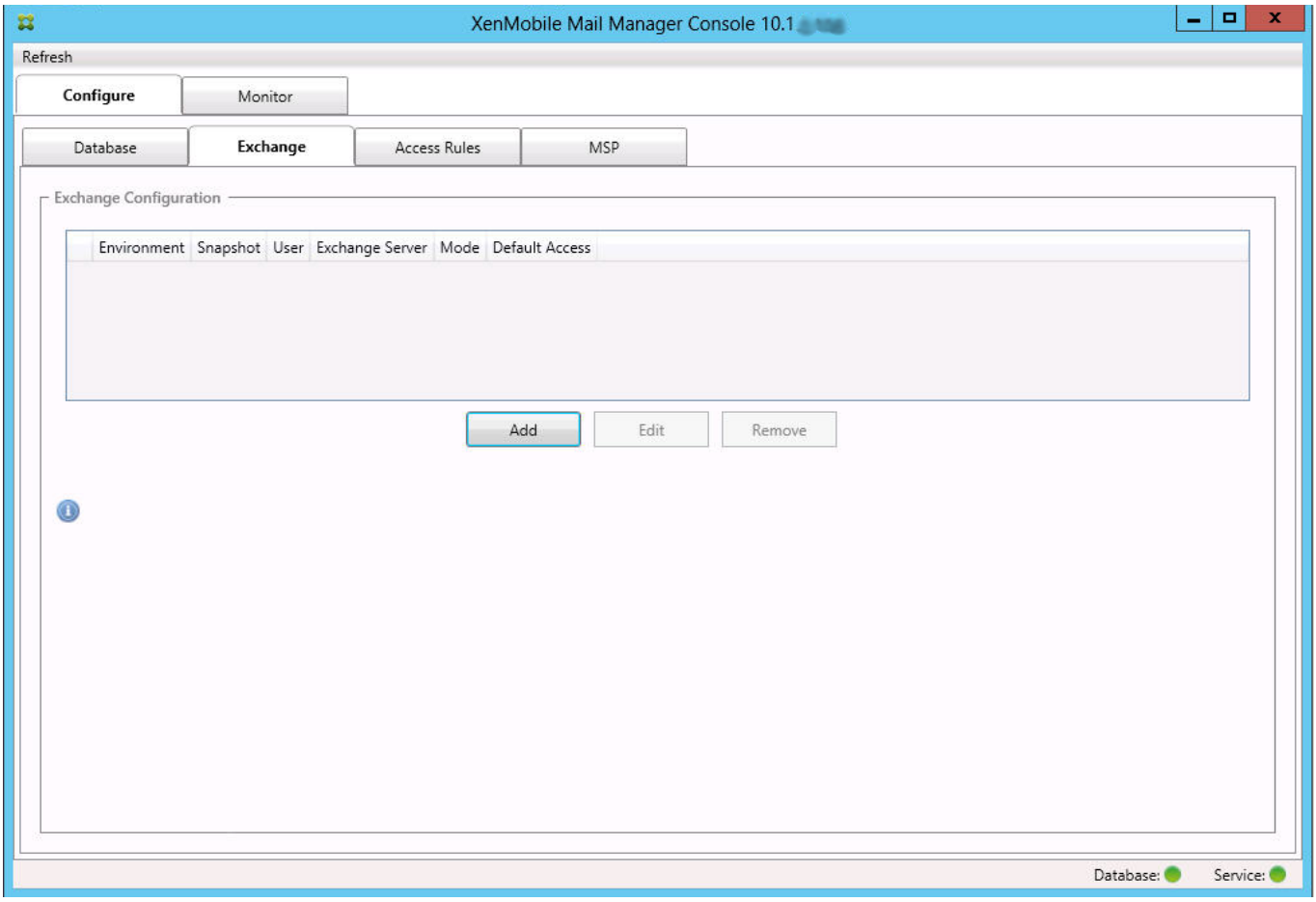
5. Klicken Sie auf **Test Connectivity**, um zu prüfen, ob eine Verbindung mit dem SQL Server hergestellt werden kann, und klicken Sie auf **Save**.



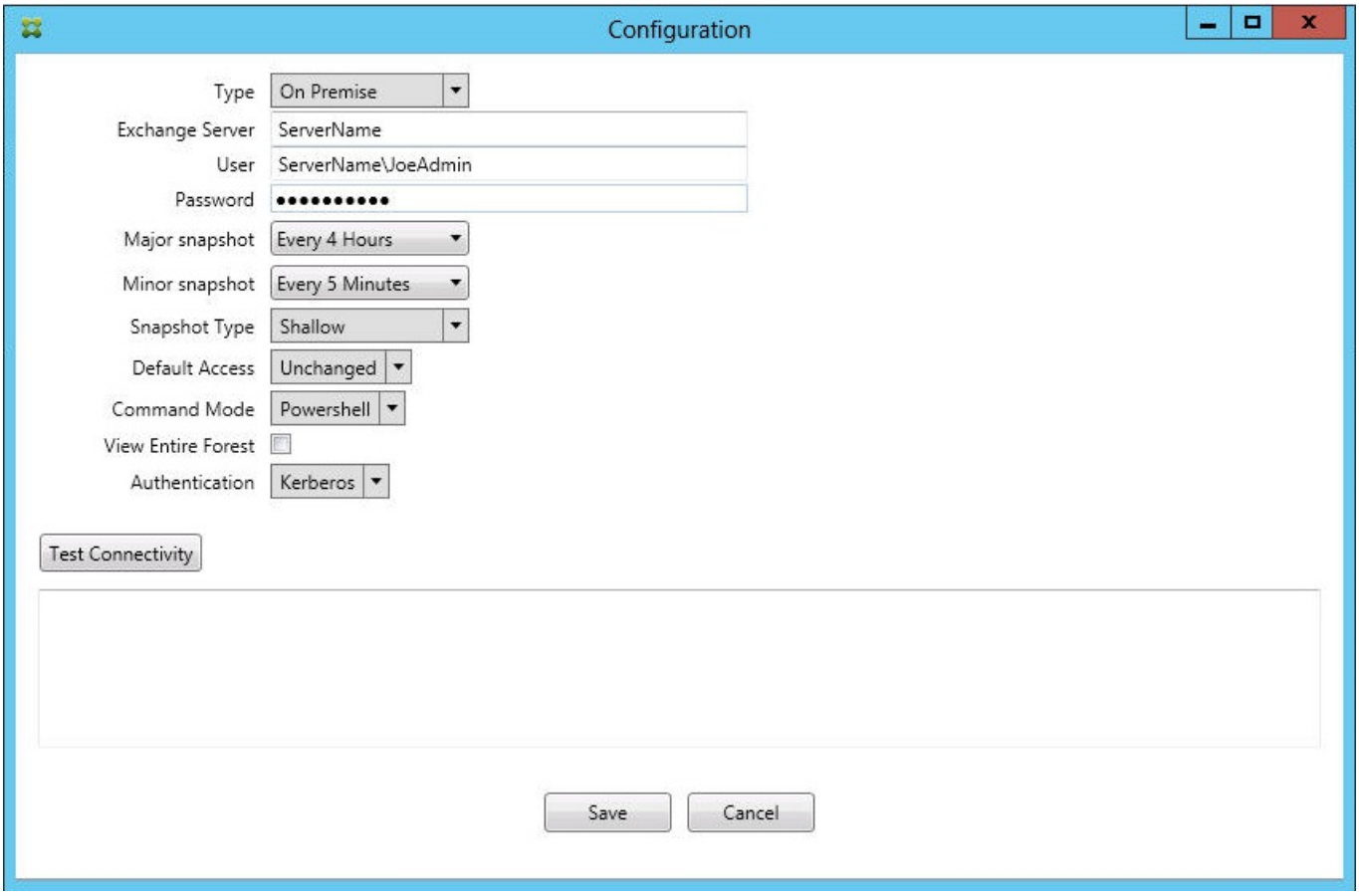
4. Eine Meldung fordert Sie zum Neustarten des Diensts auf. Klicken Sie auf **Yes**.



5. Konfigurieren Sie einen oder mehrere Exchange Server:
   1. Wenn Sie eine einzelne Exchange-Umgebung verwalten, müssen Sie nur einen Server angegeben. Wenn Sie mehrere Exchange-Umgebungen verwalten, müssen Sie für jede einen separaten Exchange Server-Computer festlegen.
   2. Wählen Sie die Registerkarte **Configure > Exchange**.



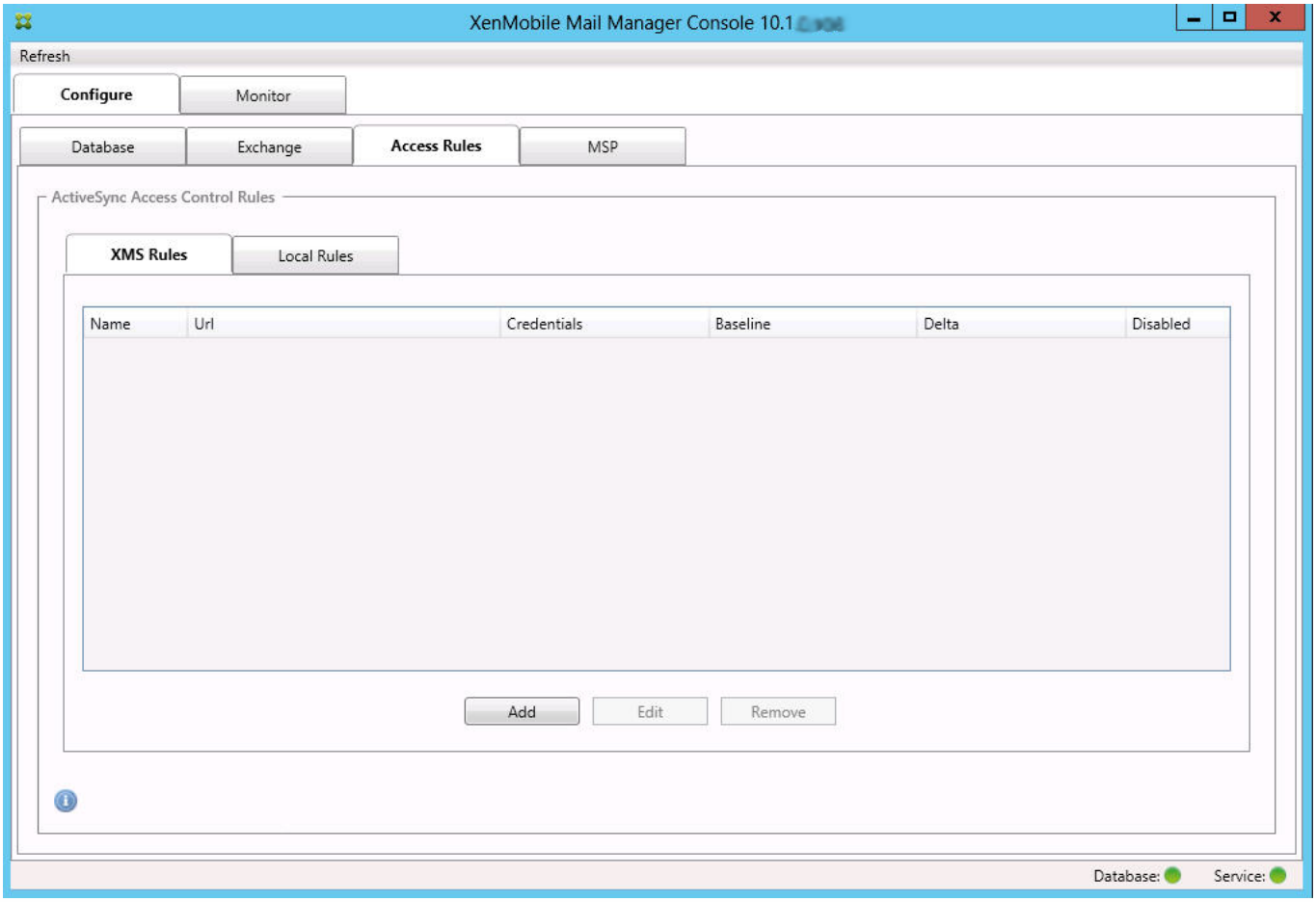
3. Klicken Sie auf **Add**.
4. Wählen Sie den Typ der Exchange Server-Umgebung aus: entweder **On Premise** oder **Office 365**.



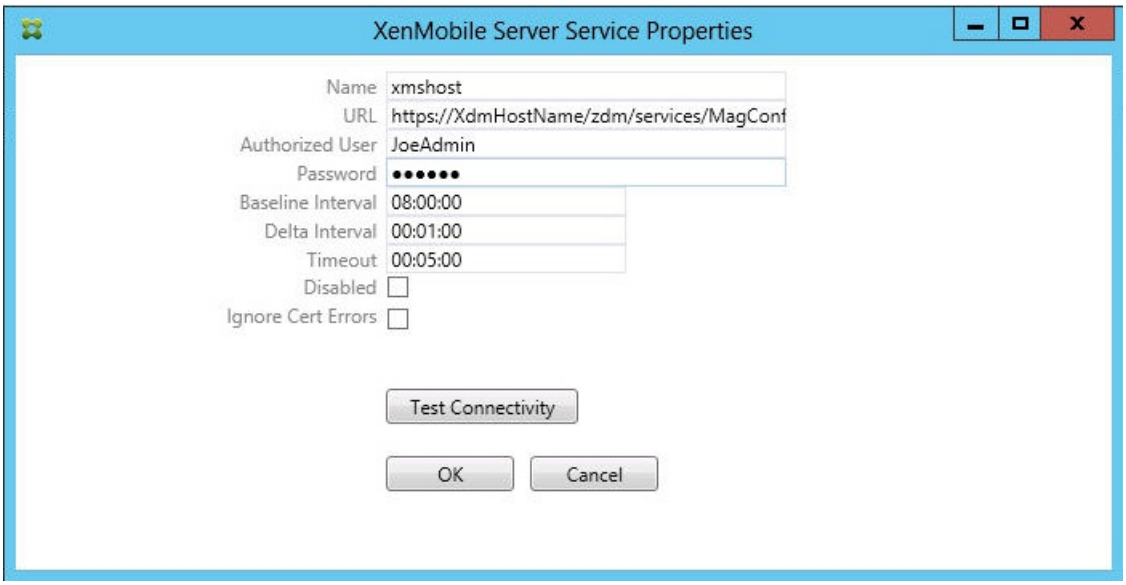
5. Wenn Sie **On Premise** auswählen, geben Sie den Namen des für Remote-PowerShell-Befehle verwendeten Exchange Servers ein.
6. Geben Sie den Benutzernamen einer Windows-Identität ein, die die unter "Anforderungen" aufgeführten Berechtigungen auf dem Exchange Server-Computer hat.
7. Geben Sie für **Password** das Kennwort des Benutzers ein.
8. Wählen Sie den Zeitplan zum Ausführen größerer Snapshots. Bei einem größeren Snapshot wird jede Exchange ActiveSync-Partnerschaft ermittelt.
9. Wählen Sie den Zeitplan zum Ausführen kleinerer Snapshots. Bei einem kleineren Snapshot werden neu erstellte Exchange ActiveSync-Partnerschaften ermittelt.
10. Wählen Sie den Snapshottyp aus: **Deep** oder **Shallow**. Flache Snapshots (Shallow) werden in der Regel viel schneller erstellt und reichen zur Ausführung aller Funktionen der Exchange ActiveSync-Zugriffssteuerung von XenMobile Mail Manager aus. Tiefe Snapshots (Deep) brauchen wesentlich länger und sind nur erforderlich, wenn Mobile Service Provider für ActiveSync aktiviert ist (dadurch kann XenMobile nicht verwaltete Geräte abfragen).
11. 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 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 aus: **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**.

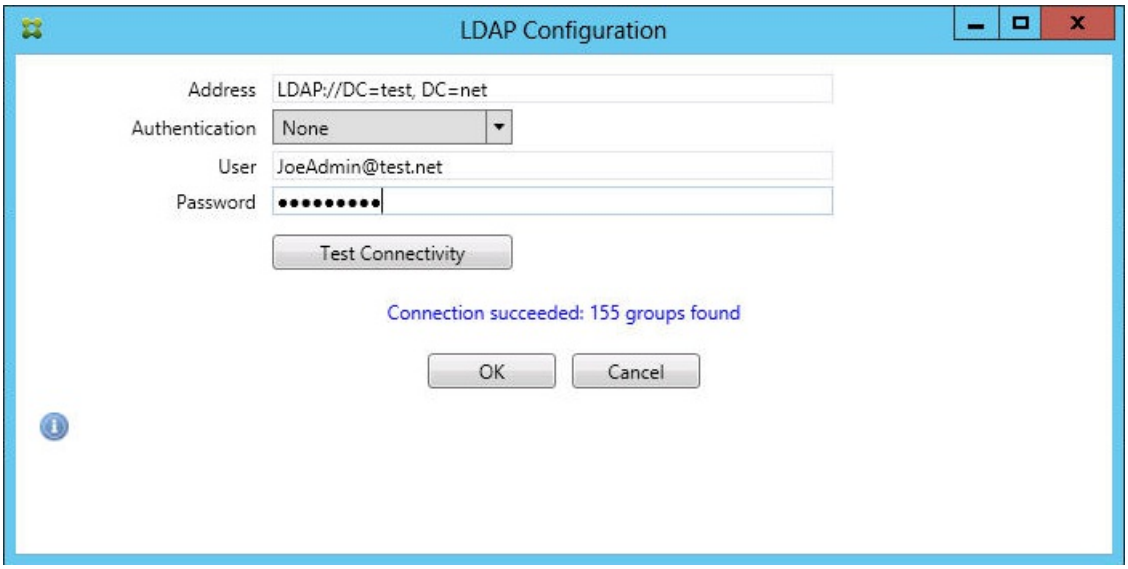


    3. Klicken Sie auf **Add**.



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.

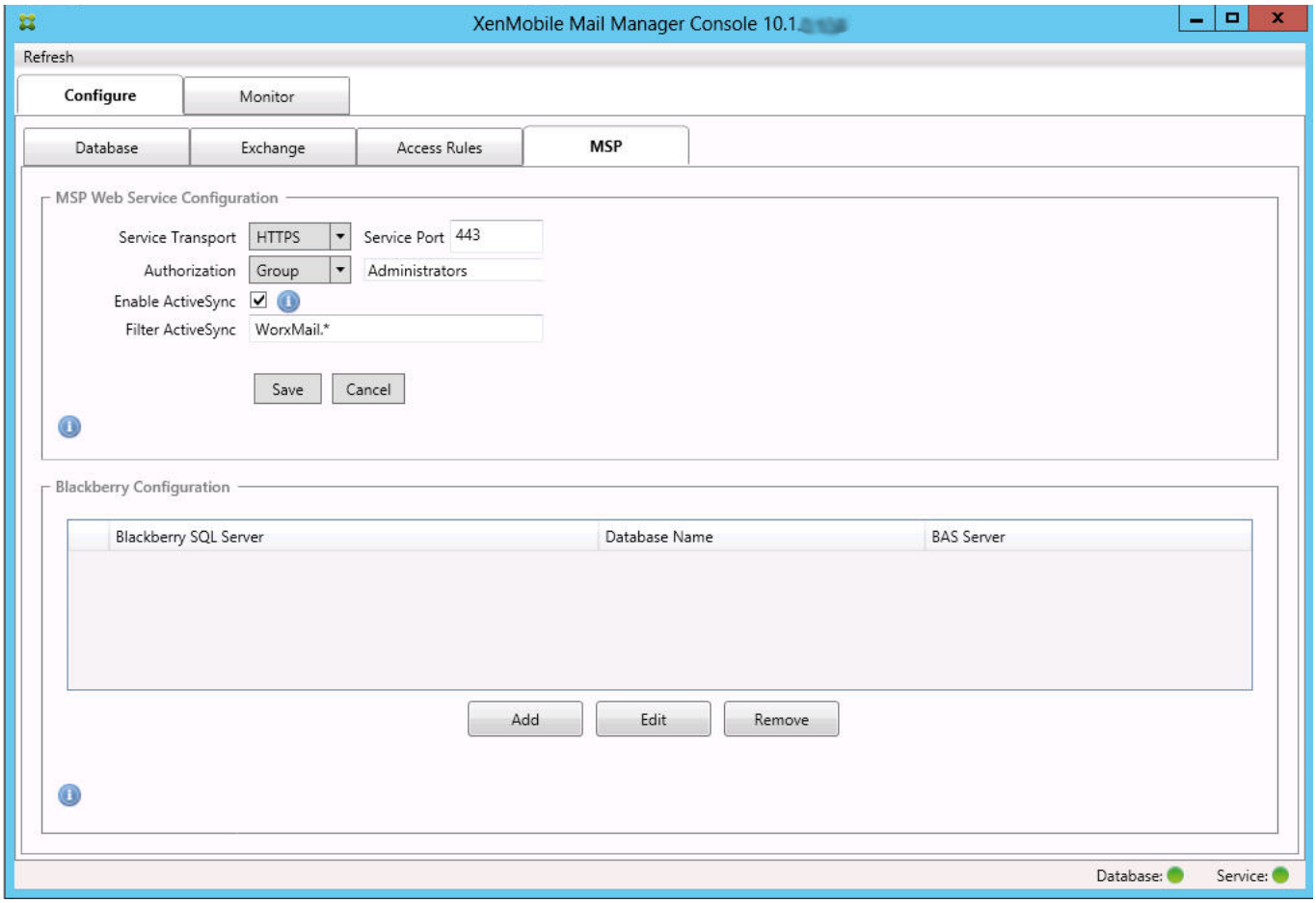


   2. Sie können lokale Regeln basierend auf den Parametern **ActiveSync Device ID**, **Device Type**, **AD Group**, **User** oder **UserAgent** hinzufügen. Wählen Sie in der Liste den geeigneten Schlüssel aus. Weitere Informationen finden Sie unter

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**.

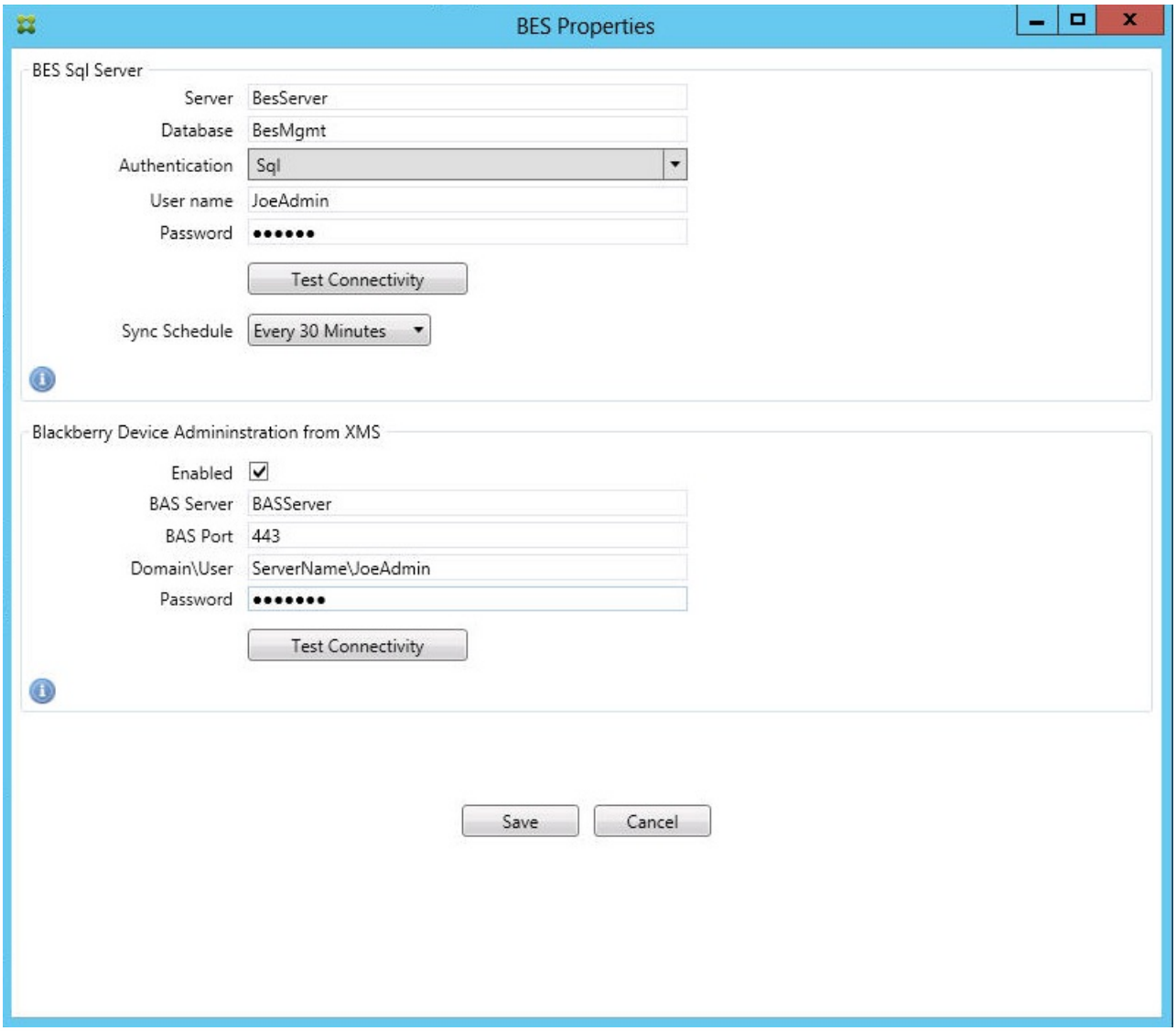
8. Konfigurieren des Mobile Service Provider-Diensts
   Hinweis: Der Mobile Service Provider-Dienst ist optional und nur erforderlich, wenn auch XenMobile für die Verwendung der Mobile Service Provider-Schnittstelle zum Abfragen nicht verwalteter Geräte konfiguriert ist.
   1. Wählen Sie die Registerkarte **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 "Secure Mail.*" 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.

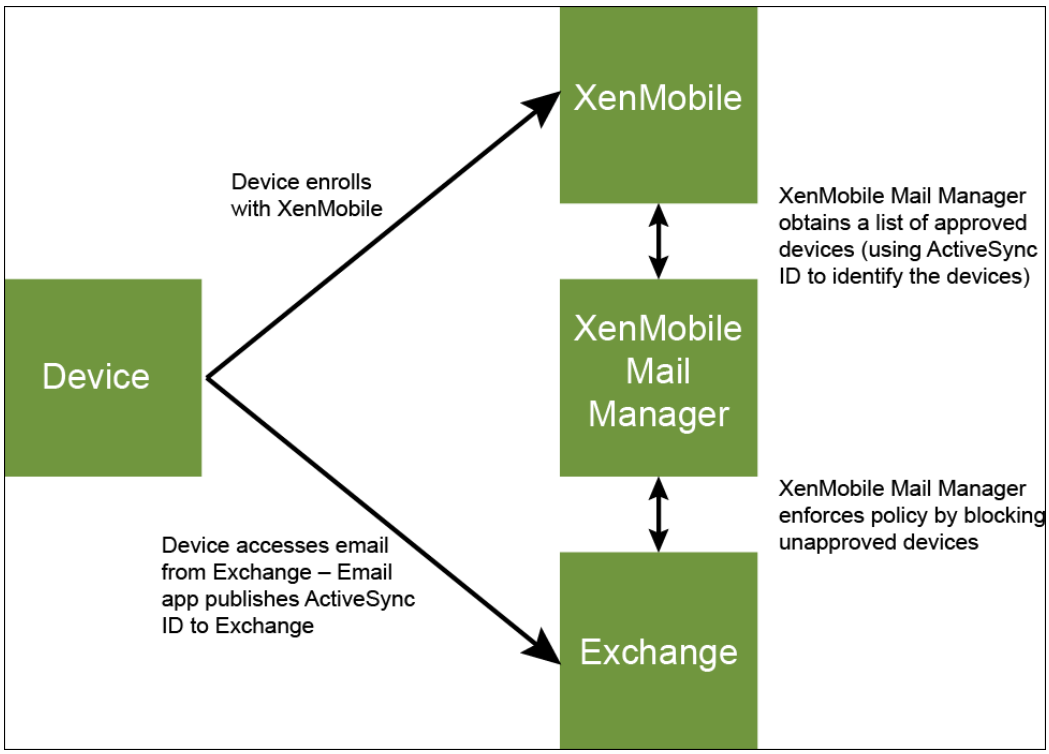
5. Wenn Sie **SQL authentication** auswählen, geben Sie Benutzernamen und Kennwort ein.
6. Legen Sie den Parameter **Sync Schedule** fest. Nach diesem Zeitplan erfolgt eine regelmäßige Verbindung mit dem BES SQL-Server zur Prüfung auf Aktualisierungen an Geräten.
7. Klicken Sie auf **Test Connectivity**, 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

Feb 24, 2017

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. Secure Hub 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

Feb 24, 2017

XenMobile Mail Manager bietet eine regelbasierte Methode zur dynamischen Konfiguration der Zugriffssteuerung für Exchange ActiveSync-Geräte. XenMobile Mail Manager-Zugriffsregeln bestehen aus zwei Teilen: einem Abgleichausdruck und dem gewünschten Zugriffszustand (Zulassen oder Blockieren). Eine Regel kann gegen ein Exchange ActiveSync-Gerät ausgewertet werden, um zu ermitteln, ob die Regel auf das Gerät zutrifft, d. h. ob der Abgleichausdruck auf das Gerät zutrifft. Es gibt mehrere Arten von Abgleichausdrücken, eine Regel kann beispielsweise auf alle Geräten eines bestimmten Typs, eine bestimmte Exchange ActiveSync-Geräte-ID, alle Geräte eines bestimmten Benutzers usw. zutreffen.
Beim Hinzufügen, Entfernen und Umordnen von Regeln in der Regelliste kann die Liste jederzeit mit einem Klick auf die Schaltfläche **Abbrechen** auf den Zustand zurückgesetzt werden, den sie beim ersten Öffnen hatte. Wenn Sie nicht auf die Schaltfläche **Speichern** klicken, gehen jegliche Änderungen in diesem Fenster verloren, wenn Sie das Konfigurationstool schließen.

XenMobile Mail Manager bietet drei Regeltypen: lokale Regeln, XenMobile-Serverregeln (XDM-Regeln) und die Standardzugriffsregel.

Lokale Regeln: Diese haben die höchste Priorität, d. h. sobald eine lokale Regel auf ein Gerät zutrifft, wird die Regelauswertung eingestellt. Es werden weder die XenMobile-Serverregeln noch die Standardzugriffsregel konsultiert. Lokale Regeln werden in Bezug auf XenMobile Mail Manager lokal über die Registerkarte Konfigurieren > Zugriffsregeln > Lokale Regeln 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-Serverregeln Diese 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-Serverregel zu, wird der gewünschte Zugriffszustand durch die Standardzugriffsregel bestimmt.

- **Default Access – Allow**: Geräte, auf die weder eine lokale noch eine XenMobile-Serverregel zutrifft, werden alle zugelassen.
- **Default Access – Block**: Geräte, auf die weder eine lokale noch eine XenMobile-Serverregel zutrifft, werden alle blockiert.
- **Default Access - Unchanged**: Bei Geräten, auf die weder eine lokale noch eine XenMobile-Serverregel 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
- XenMobile-Serverregeln
- Standardzugriffsregel

Sobald eine Regel zutrifft, wird die Auswertung beendet. Trifft beispielsweise eine lokale Regel auf ein Gerät zu, erfolgt für dieses keine Auswertung der XenMobile-Serverregeln 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

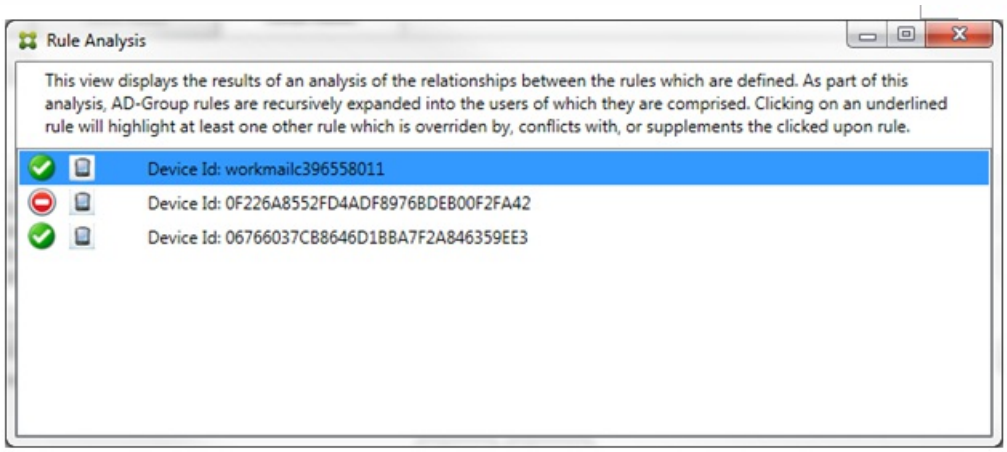
weisende grüne Pfeile angezeigt. Ein nach oben weisender Pfeil zeigt an, dass es Nebenregeln gibt, die vor der primären Regel stehen. Ein nach unten weisender Pfeil zeigt an, dass es Nebenregeln gibt, die nach der primären Regel stehen. Es kann immer nur eine primäre Regel aktiv sein.

- **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.

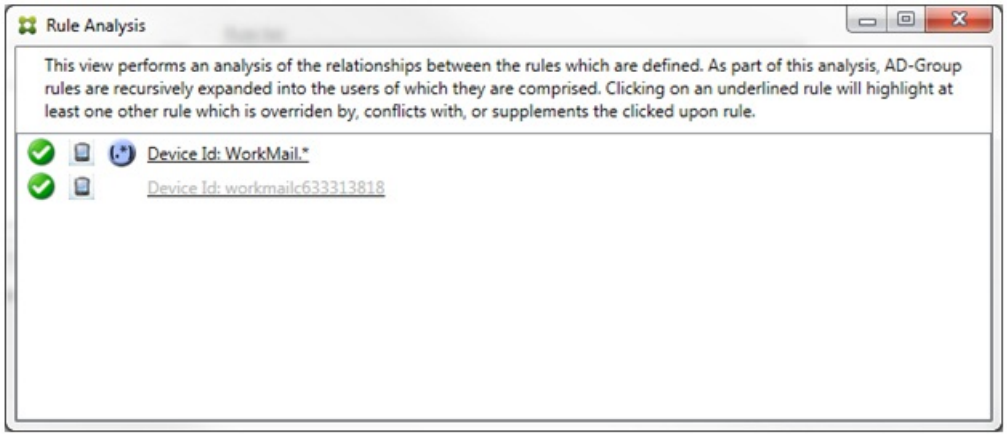
Darstellung des Regeltyps im Dialogfeld zur Regelanalyse

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.

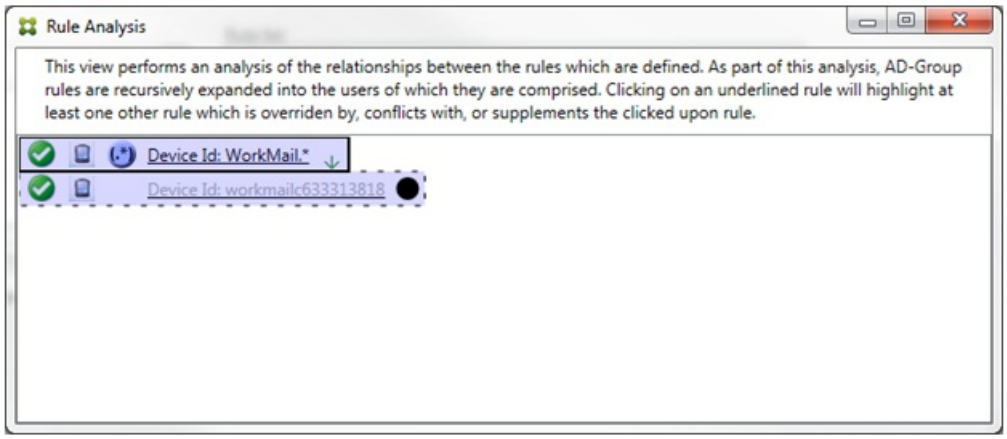
Im Fenster "Rule Analysis" ist ein Kontrollkästchen, bei dessen Aktivierung nur die Regeln angezeigt werden, die Konflikte, Überschreibungen, Redundanzen oder Ergänzungen sind.



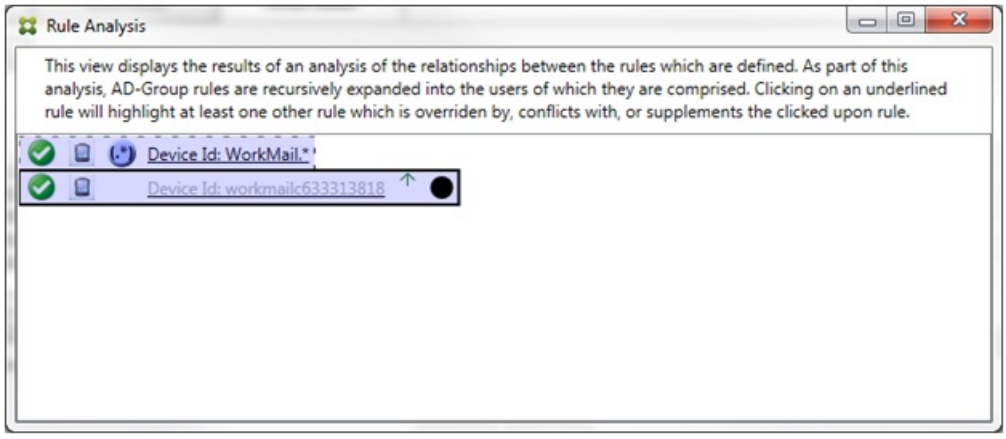
Wenn eine Außerkraftsetzung vorliegt, werden mindestens zwei Regeln unterstrichen dargestellt: die primäre Regel und die Nebenregel(n). Mindestens eine Nebenregel erscheint in einer helleren Schrift, um anzuzeigen, dass sie durch eine höhere Regel außer Kraft gesetzt wird. Sie können auf die außer Kraft 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:

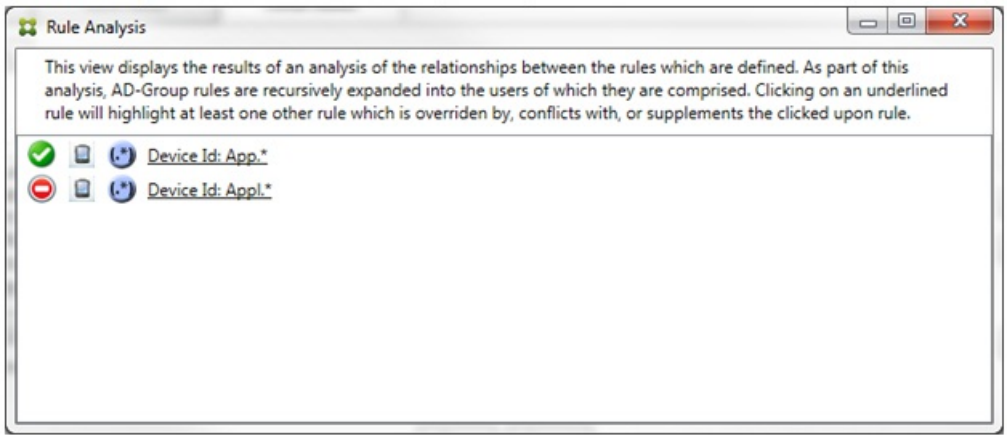


In diesem Beispiel ist die Regel mit regelmäßigen Ausdrücken WorkMail.* die primäre Regel (angezeigt durch den durchgehenden Rahmen) und die normale Regel workmailc633313818 ist eine Nebenregel (angezeigt durch den gestrichelten Rahmen). Der schwarze Punkt neben der Nebenregel weist deutlich darauf hin, 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:

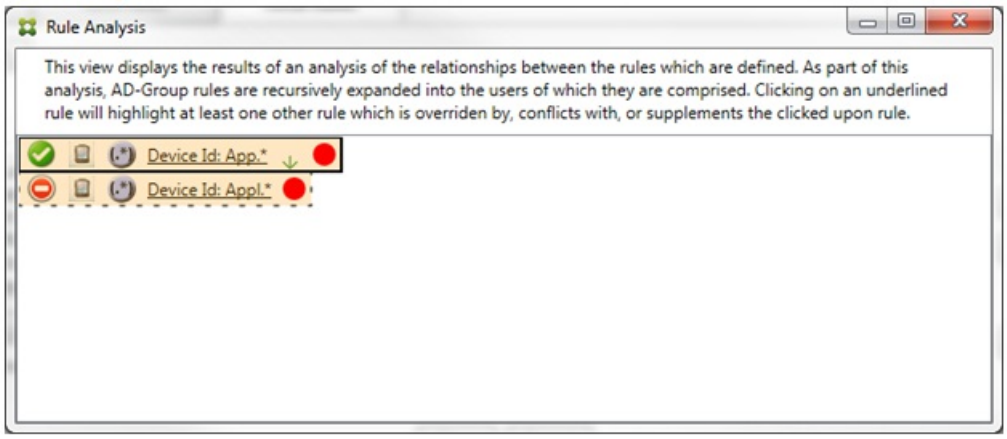


Im vorherigen Beispiel ist die Regel mit regelmäßigen Ausdrücken WorkMail.* die Nebenregel (angezeigt durch den gestrichelten Rahmen) und die normale Regel workmailc633313818 ist eine primäre Regel (angezeigt durch den durchgehenden Rahmen). In diesem einfachen Beispiel ist der Unterschied nicht groß. 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:

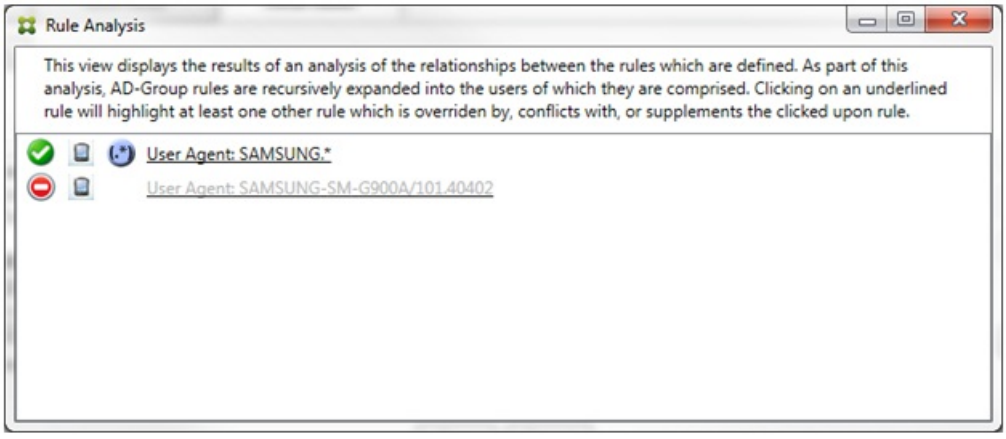


Eine Untersuchung der beiden Regeln mit regelmäßigen Ausdrücken ergibt, dass die erste alle Geräte, deren ID "App" enthält, zulässt und die zweite alle Geräte, deren ID "Appl" enthält, blockiert. Obwohl die zweite Regel alle Geräte, deren ID "Appl" enthält, blockiert, wird kein Gerät, auf das die Regel zutrifft, je blockiert, da die zulassende Regel eine höhere Priorität hat. Nach dem Klicken auf die erste Regel wird das Dialogfeld folgendermaßen angezeigt:



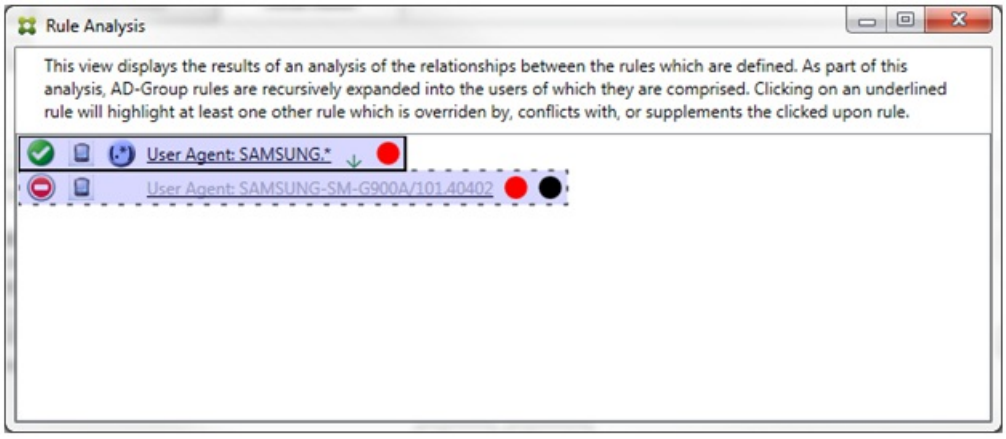
Im vorherigen Szenario wird sowohl die primäre Regel (mit dem regelmäßigen Ausdruck "App.*") und die Nebenregel (mit dem regelmäßigen Ausdruck "Appl.*") gelb markiert angezeigt. Dies ist ein einfacher optischer Warnhinweis auf den Umstand, dass mehrere Regeln mit regelmäßigem Ausdruck für ein einzelnes 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.



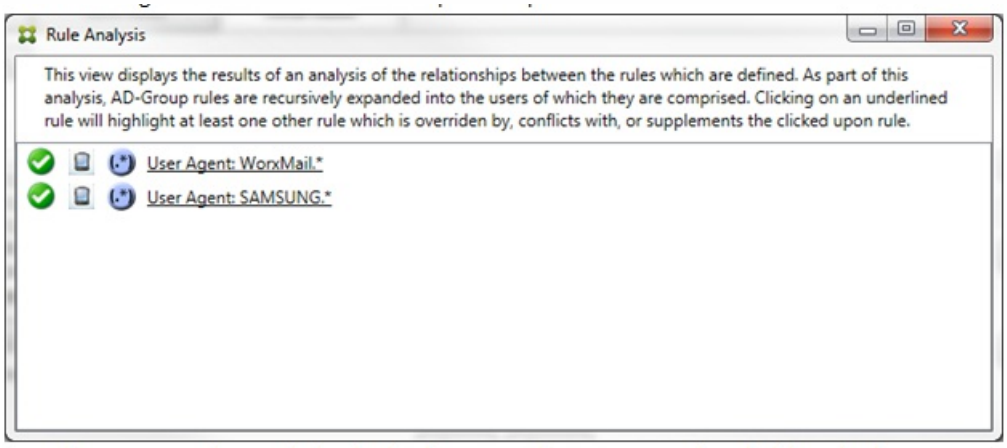
Im vorherigen Beispiel ist leicht zu erkennen, dass die erste Regel (mit dem regelmäßigen Ausdruck SAMSUNG.*) die nächste Regel (normale Regel SAMSUNG-SM-G900A/101.40402) außer Kraft setzt und überdies ein Konflikt beim Zugriffszustand (primäre Regel = Zulassen, Nebenregel = Blockieren) vorliegt. Die 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:

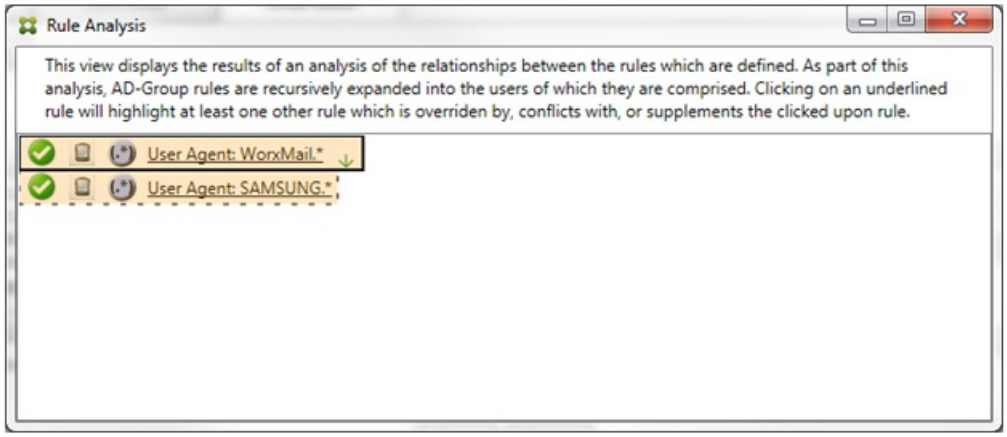


Die primäre Regel (mit dem regelmäßigen Ausdruck SAMSUNG.*) ist mit einem roten Punkt gekennzeichnet, um anzuzeigen, dass ihr Zugriffszustand im Widerspruch mit dem von mindestens einer Nebenregel steht. Die Nebenregel (normale Regel SAMSUNG-SM-G900A/101.40402) ist mit einem roten Punkt gekennzeichnet, 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:



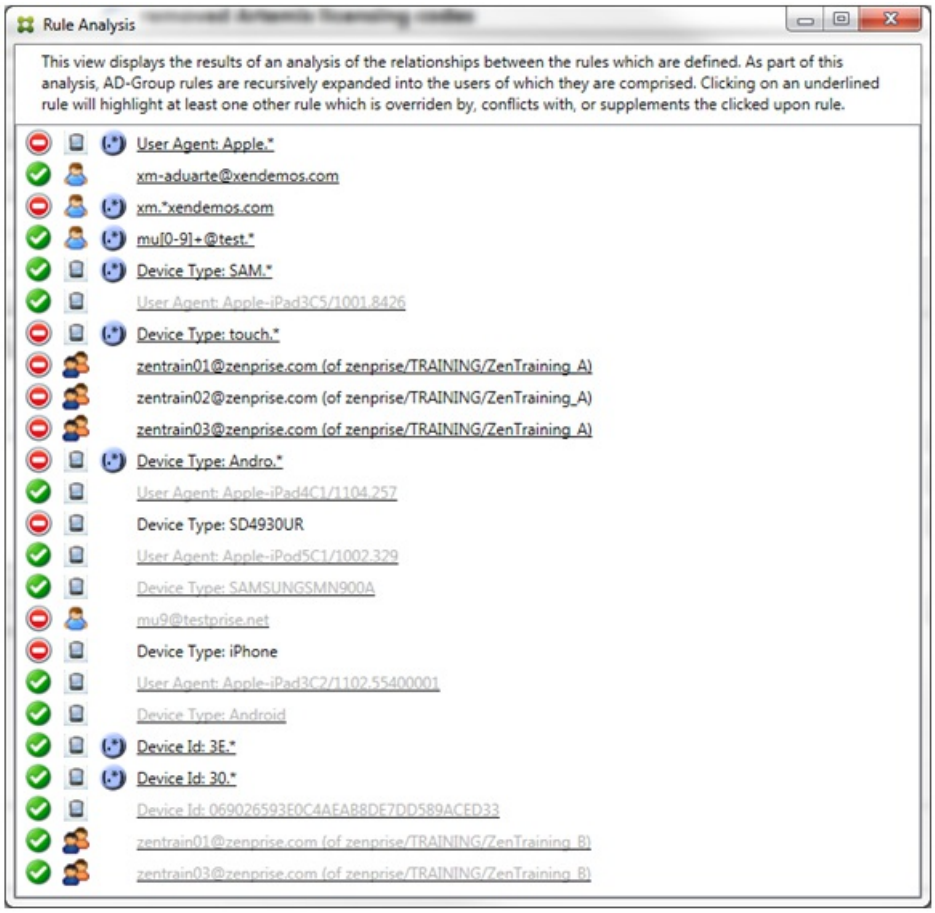
Es ist leicht zu erkennen, dass beide Regeln solche mit regelmäßigen Ausdrücken sind, und beide auf das Feld "ActiveSync device ID" in XenMobile Mail Manager angewendet werden. Nach dem Klicken auf die erste Regel sieht das Dialogfeld folgendermaßen aus:



Die primäre Regel (mit dem regelmäßigen Ausdruck WorxMail.*) ist gelb hinterlegt, 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

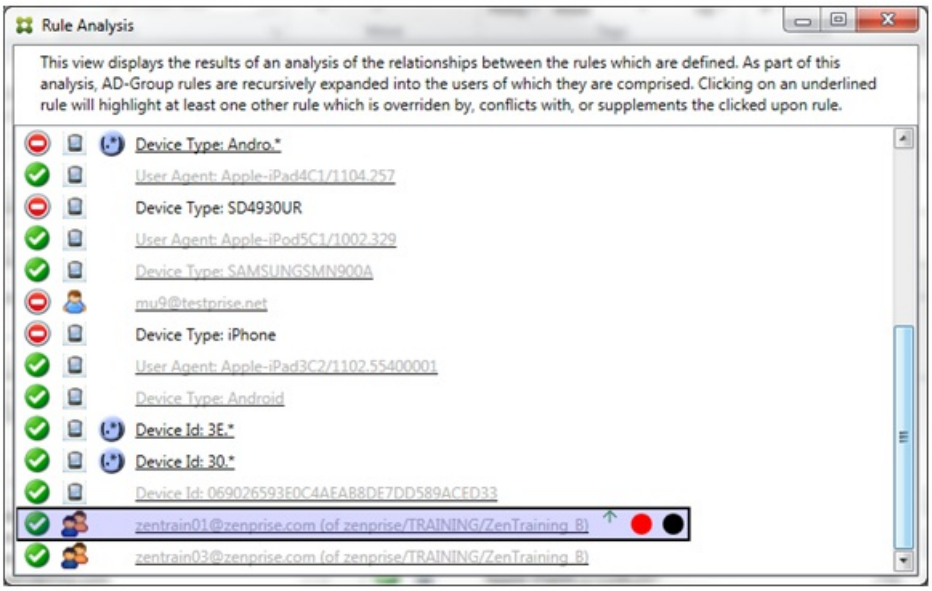
Es sind viele Außerkraftsetzungen, Konflikte oder Ergänzungen möglich, die hier nicht alle mit einem Beispiel vorgestellt werden können. Im Folgenden werden anhand eines Negativbeispiels die immensen Vorzüge des visuellen Konstrukts der Regelanalyse gezeigt. Die meisten Elemente in der folgenden Abbildung 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.

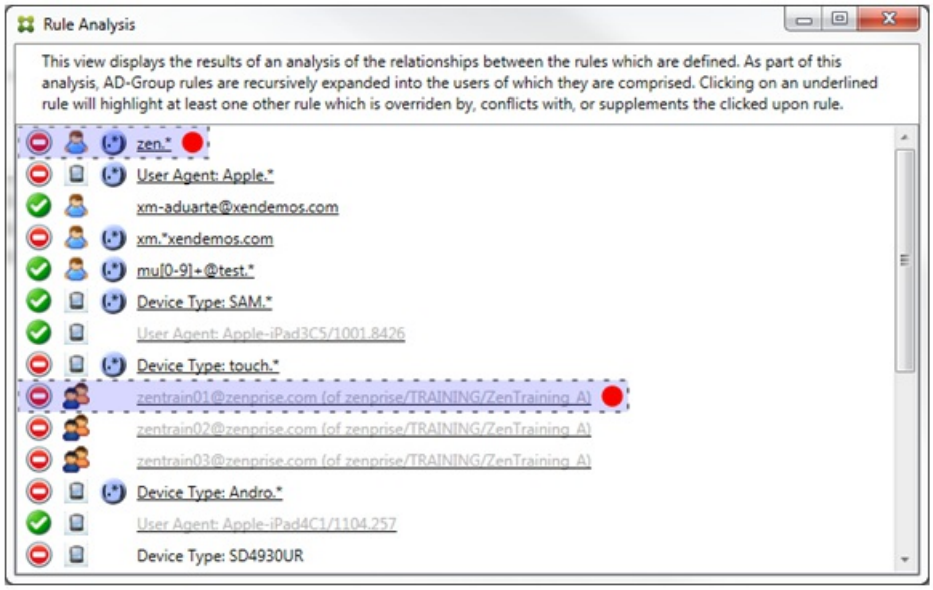
Beispiel 1: In diesem Beispiel wird untersucht, warum zentrain01@zenprise.com außer Kraft gesetzt wurde.



Die primäre Regel (AD-Gruppenregel zenprise/TRAINING/ZenTraining B, bei der zentrain01@zenprise.com Mitglied ist) hat die folgenden Merkmale:

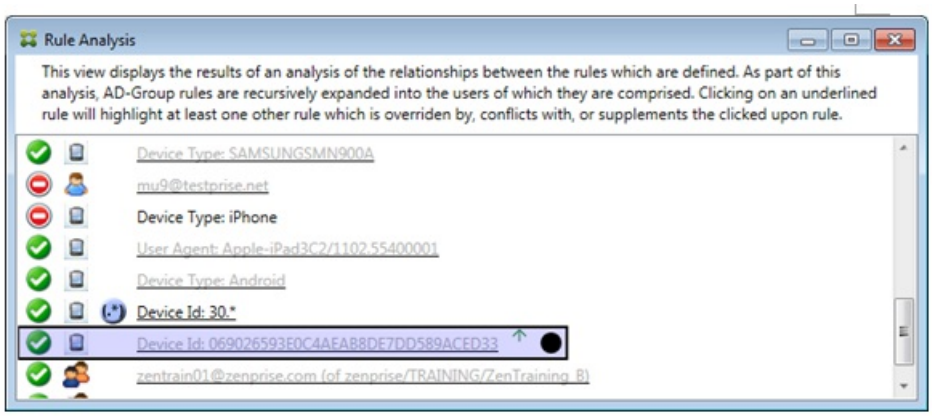
- Sie ist blau unterlegt und wird von einem durchgehenden Rahmen umgeben.
- Sie hat einen nach oben weisenden grünen Pfeil, was anzeigt, dass alle Nebenregeln weiter oben sind.
- Sie ist mit einem roten und einem schwarzen Punkt gekennzeichnet, um anzuzeigen, dass erstens mindestens eine Nebenregel einen 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:



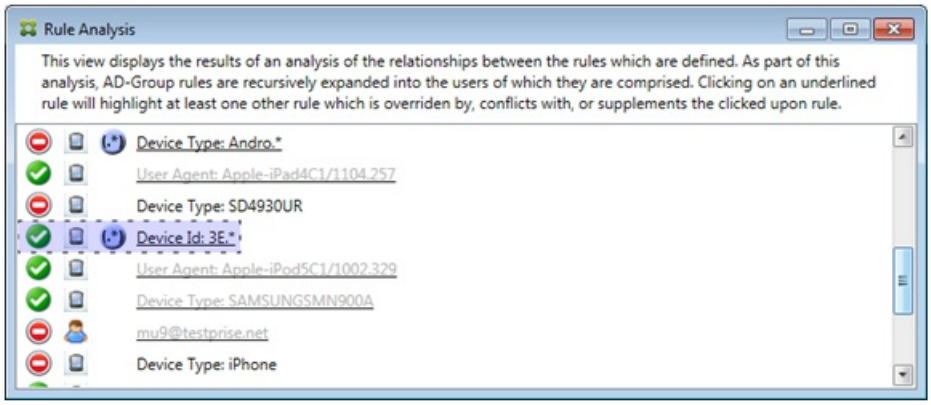
In diesem Fall gibt es zwei Nebenregeln, die die primäre Regel außer Kraft setzen: die Regel mit regelmäßigem Ausdruck zen.* und die normale Regel zentrain01@zenprise.com (von zenprise/TRAINING/ZenTraining A). Bei der letzteren Nebenregel besteht das Problem darin, dass die Active Directory-Gruppenregel 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.

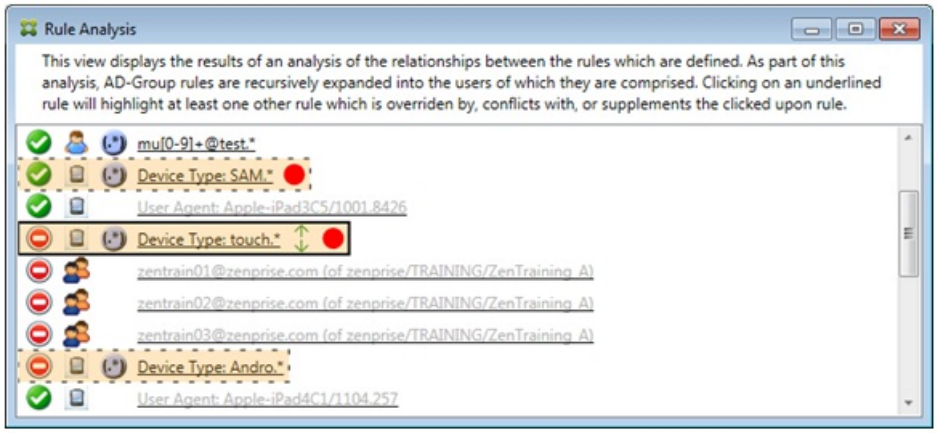
Analysieren einer Ergänzung und eines Konflikts

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

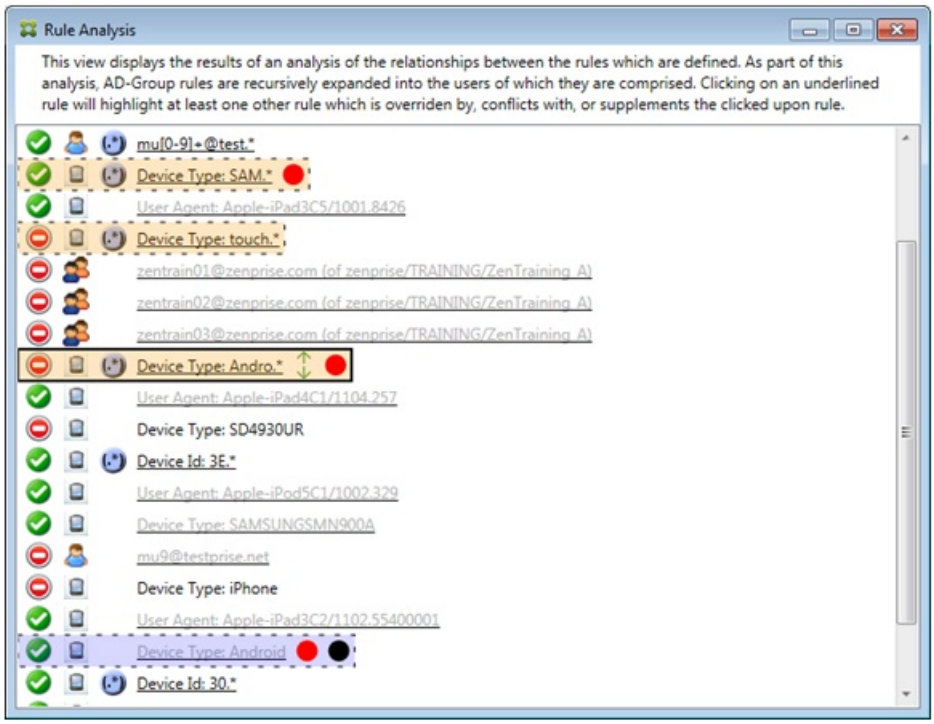
ein Konflikt mit der primären Regel besteht, bei welcher der Zugriffszustand auf Blockieren festgelegt ist.

- 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

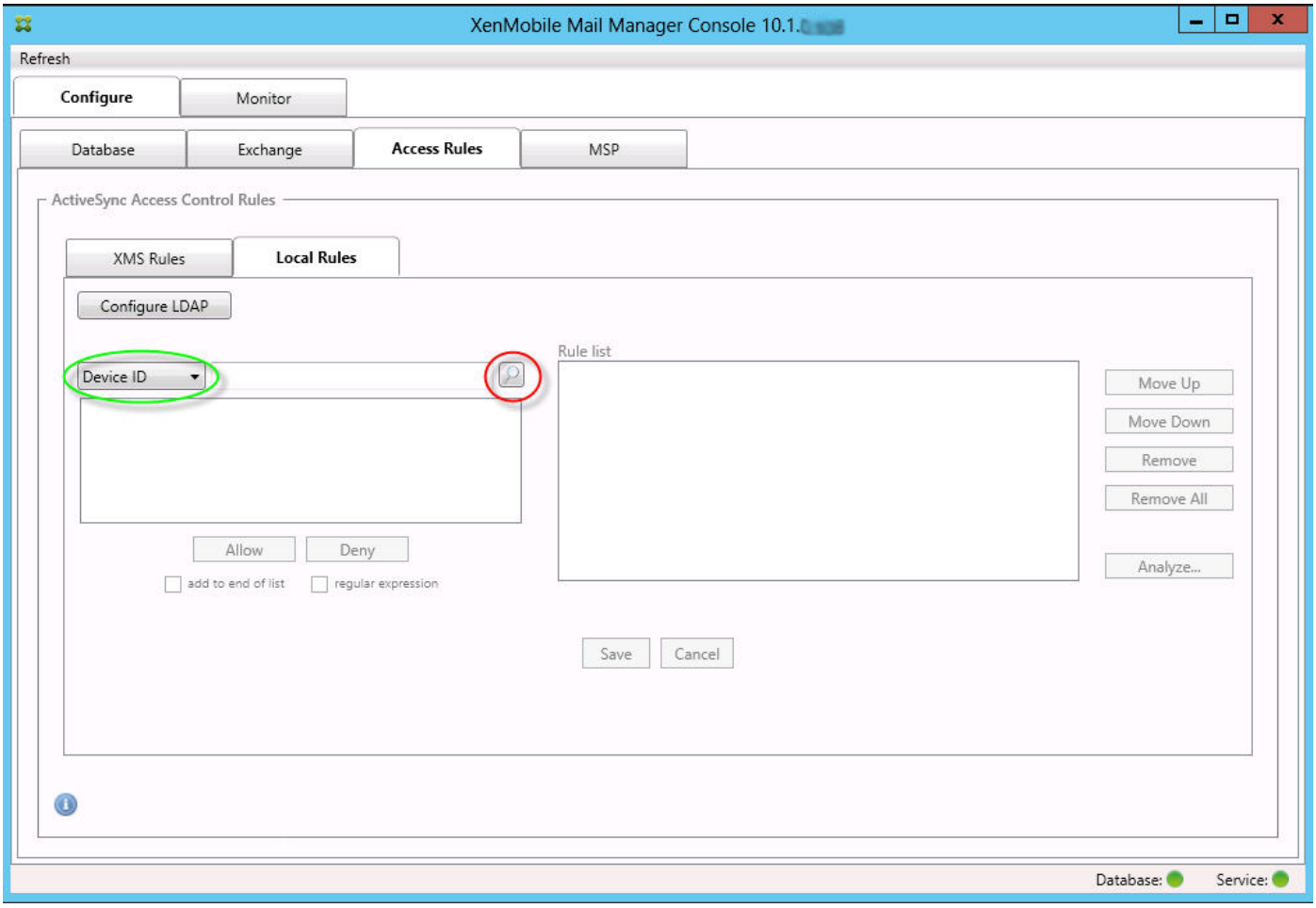
In diesem Beispiel wird demonstriert, dass Regelbeziehungen immer aus der Sicht der primären Regel dargestellt werden. Im vorherigen Beispiel wurde gezeigt, was beim Klicken auf die Gerätetypregel mit dem regelmäßigen Ausdruck touch.* angezeigt wird. Wird auf die Nebenregel Andro.* geklickt, werden andere Nebenregeln markiert.



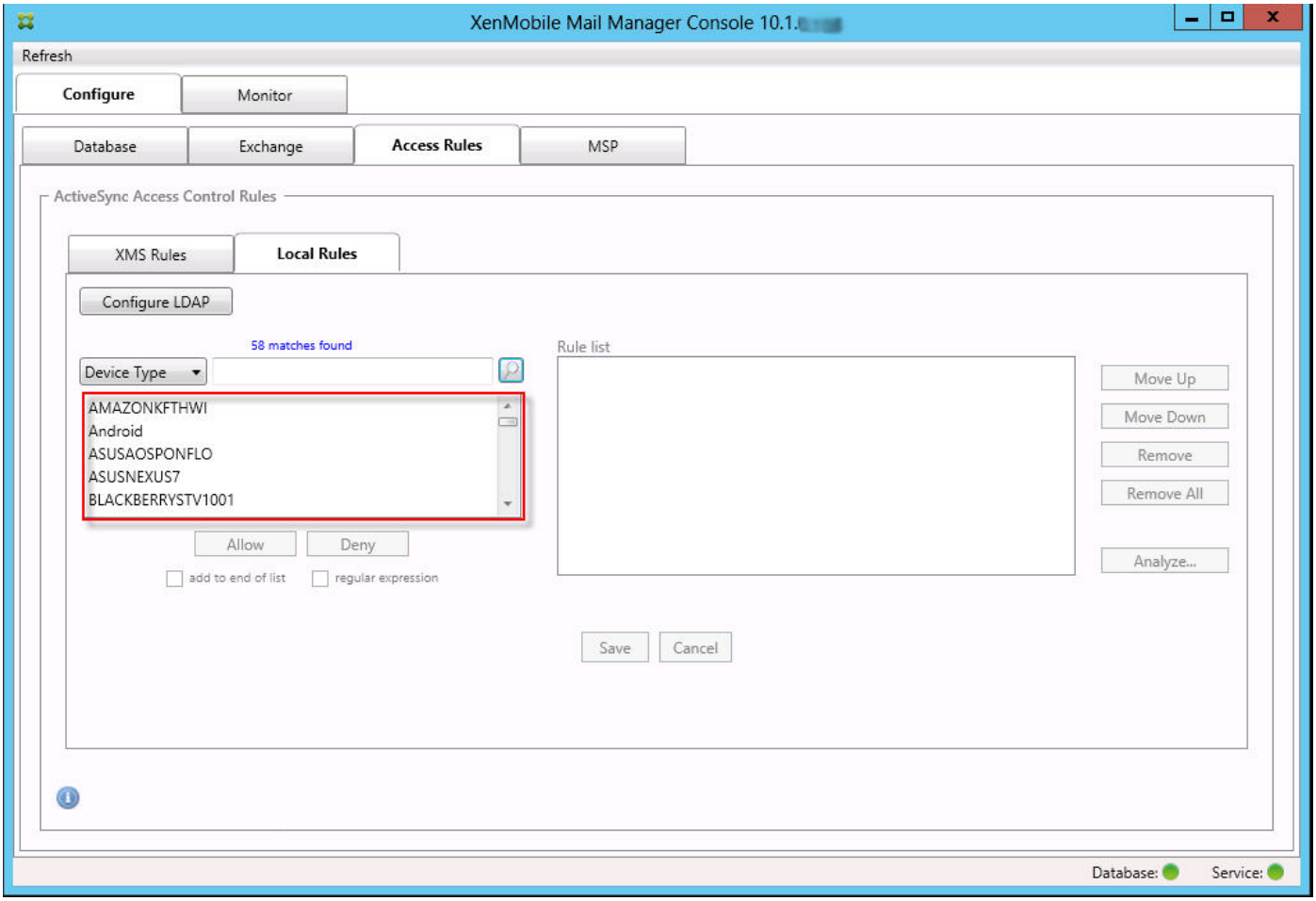
In diesem Beispiel wird eine außer Kraft gesetzte Regel, die Teil der Regelbeziehung ist, gezeigt. Diese Regel ist die normale ActiveSync-Gerätetypregel "Android", die außer Kraft gesetzt ist (sichtbar an der helleren Schrift und dem schwarzen Punkt) und deren Zugriffszustand mit dem der primären ActiveSync-Gerätetypregel 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.

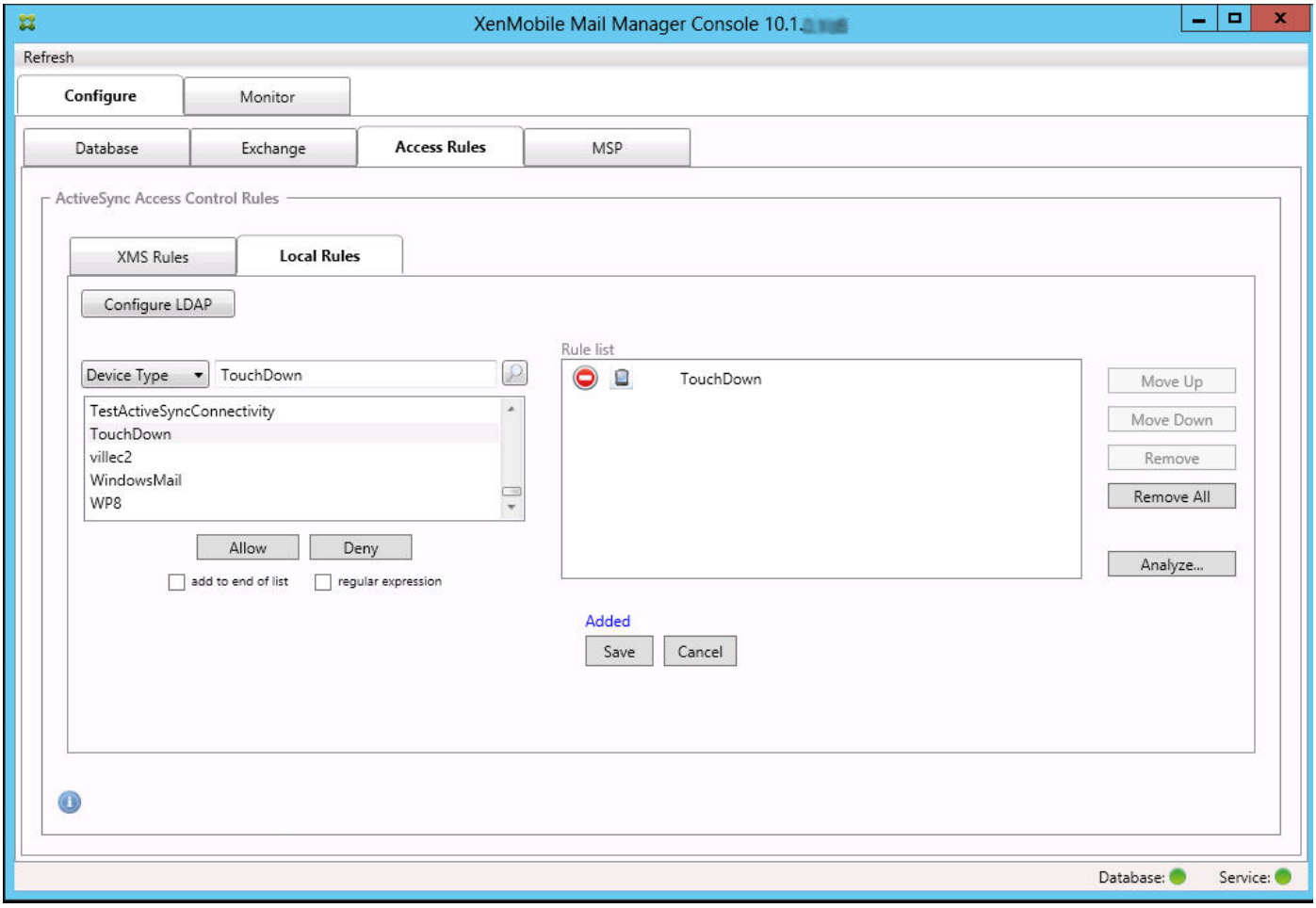


2. Wählen Sie in der Liste Device ID das Feld aus, für das Sie die lokale Regel erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld Device Type ausgewählt, die Übereinstimmungen werden unterhalb 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.

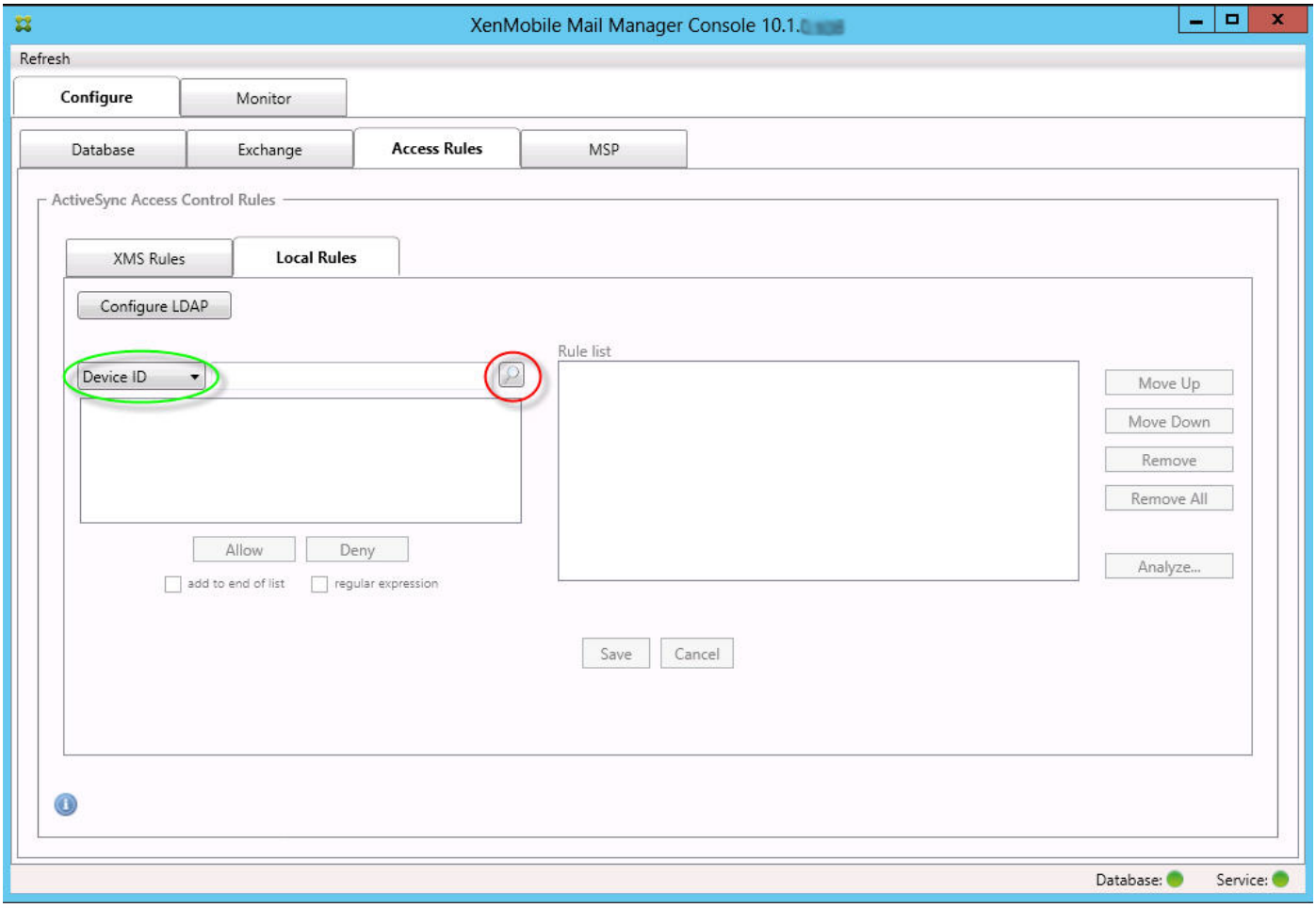


Hinzufügen eines regelmäßigen Ausdrucks

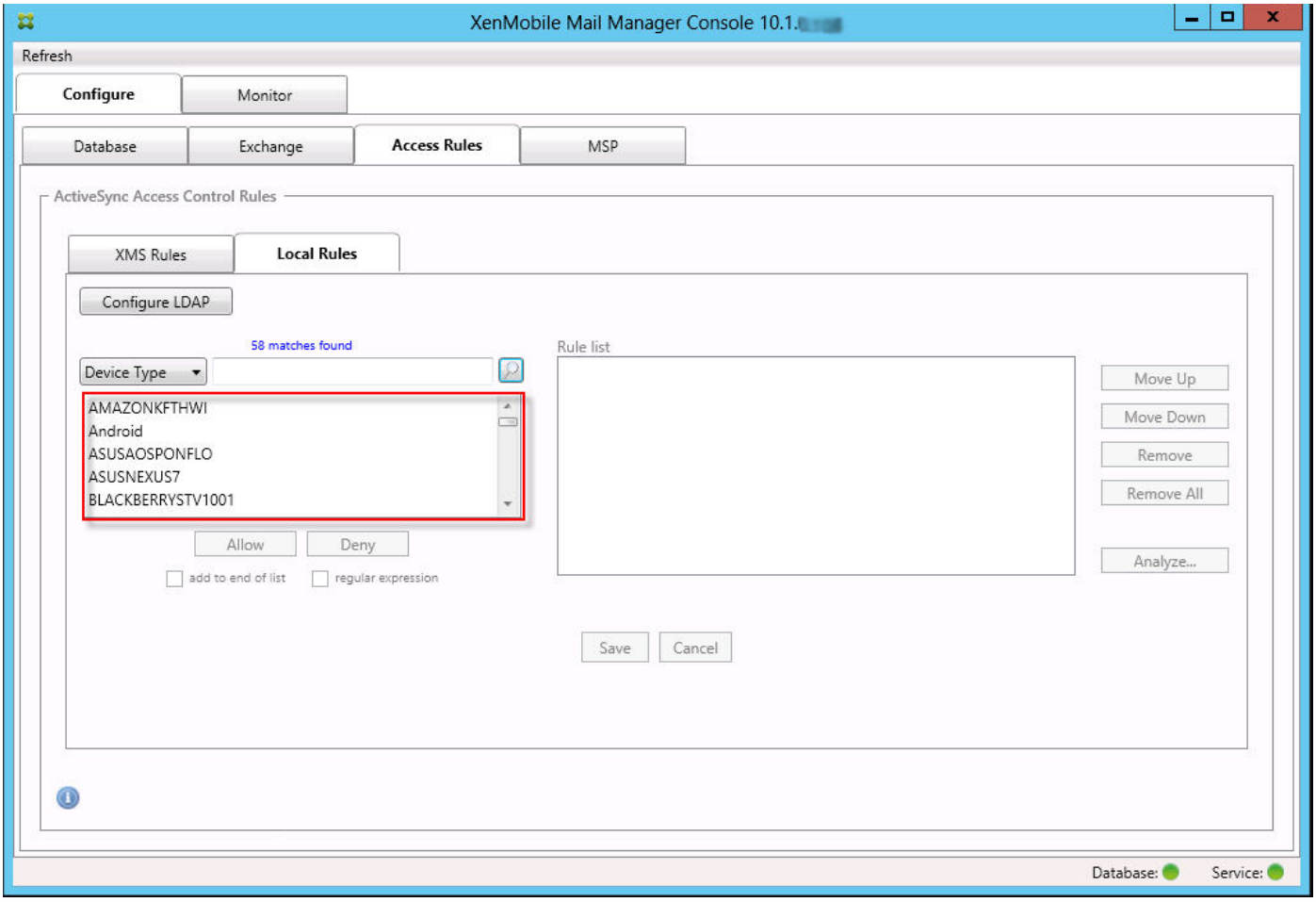
Lokale Regeln mit regelmäßigen Ausdrücken sind an folgendem Symbol zu erkennen: (.*). Zum Hinzufügen einer Regel mit regelmäßigem Ausdruck können Sie entweder einen Wert aus der Ergebnisliste für ein spezifisches Feld als Grundlage verwenden (sofern bereits ein größerer Snapshot durchgeführt wurde) oder den regelmäßigen Ausdruck selbst eingeben.

Erstellen eines regelmäßigen Ausdrucks mit einem vorhandenen Feldwert

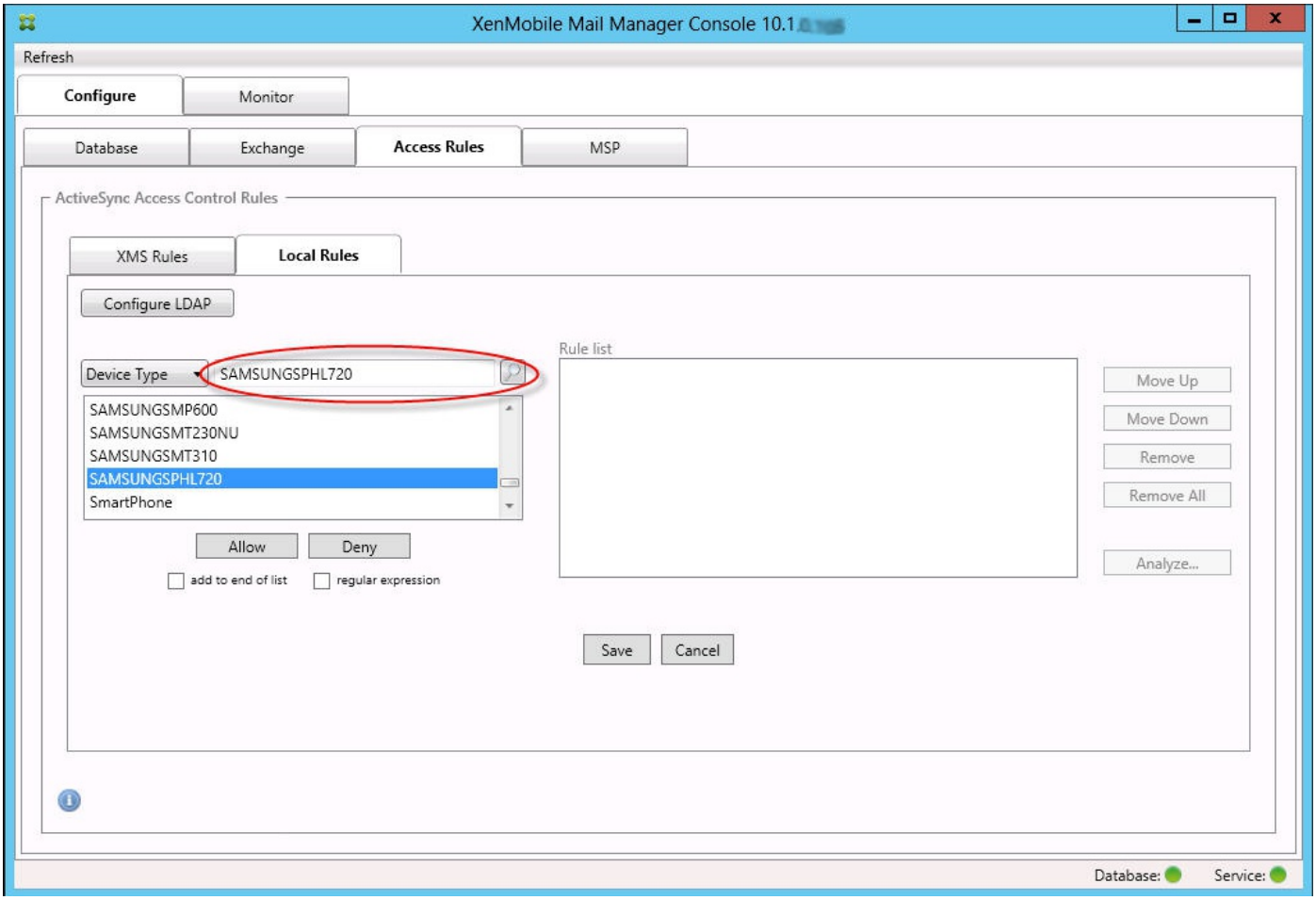
1. Klicken Sie auf die Registerkarte Access Rules.



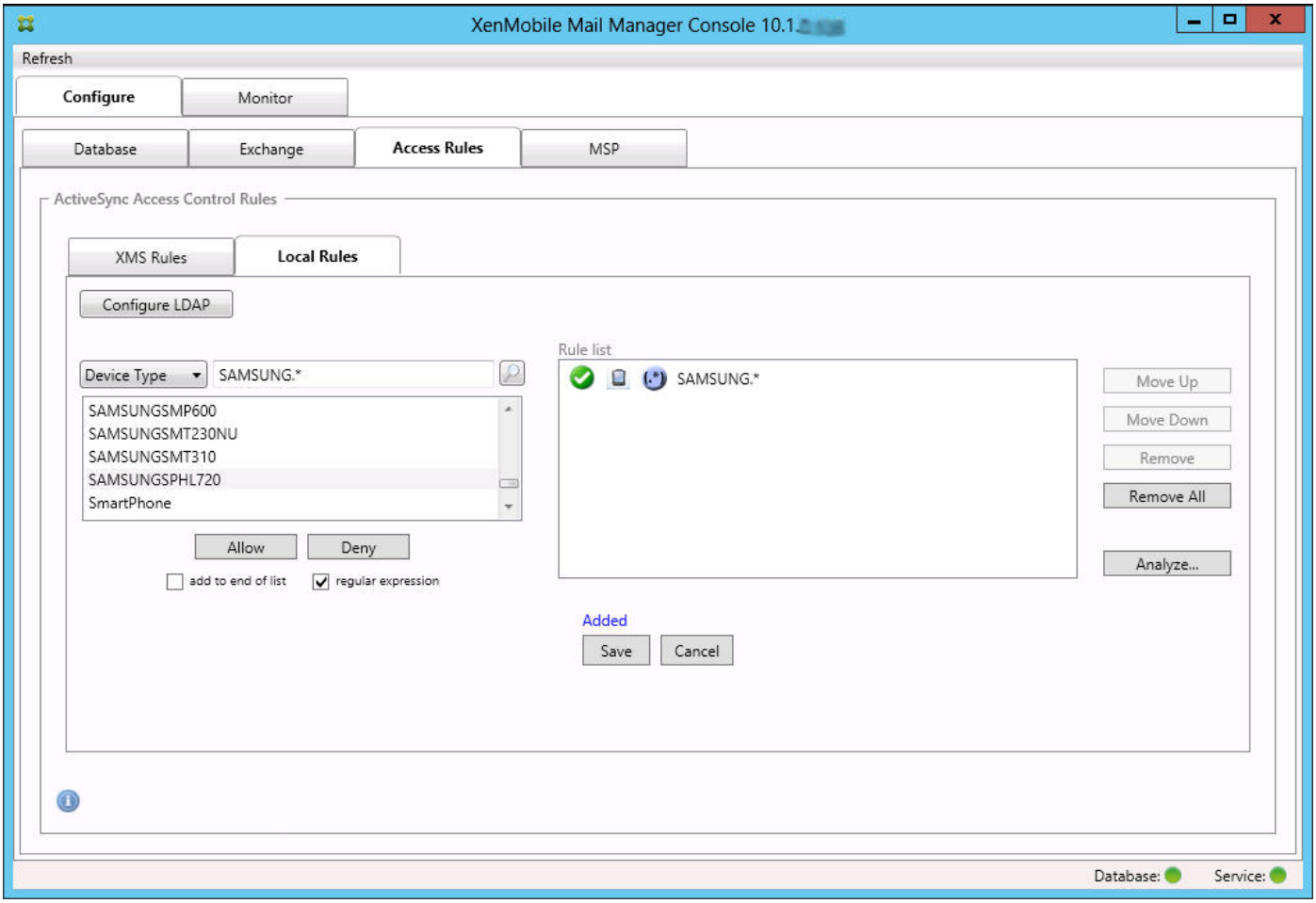
2. Wählen Sie in der Liste Device ID das Feld aus, für das Sie die lokale Regel mit einem regelmäßigen Ausdruck erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld Device Type ausgewählt, 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.

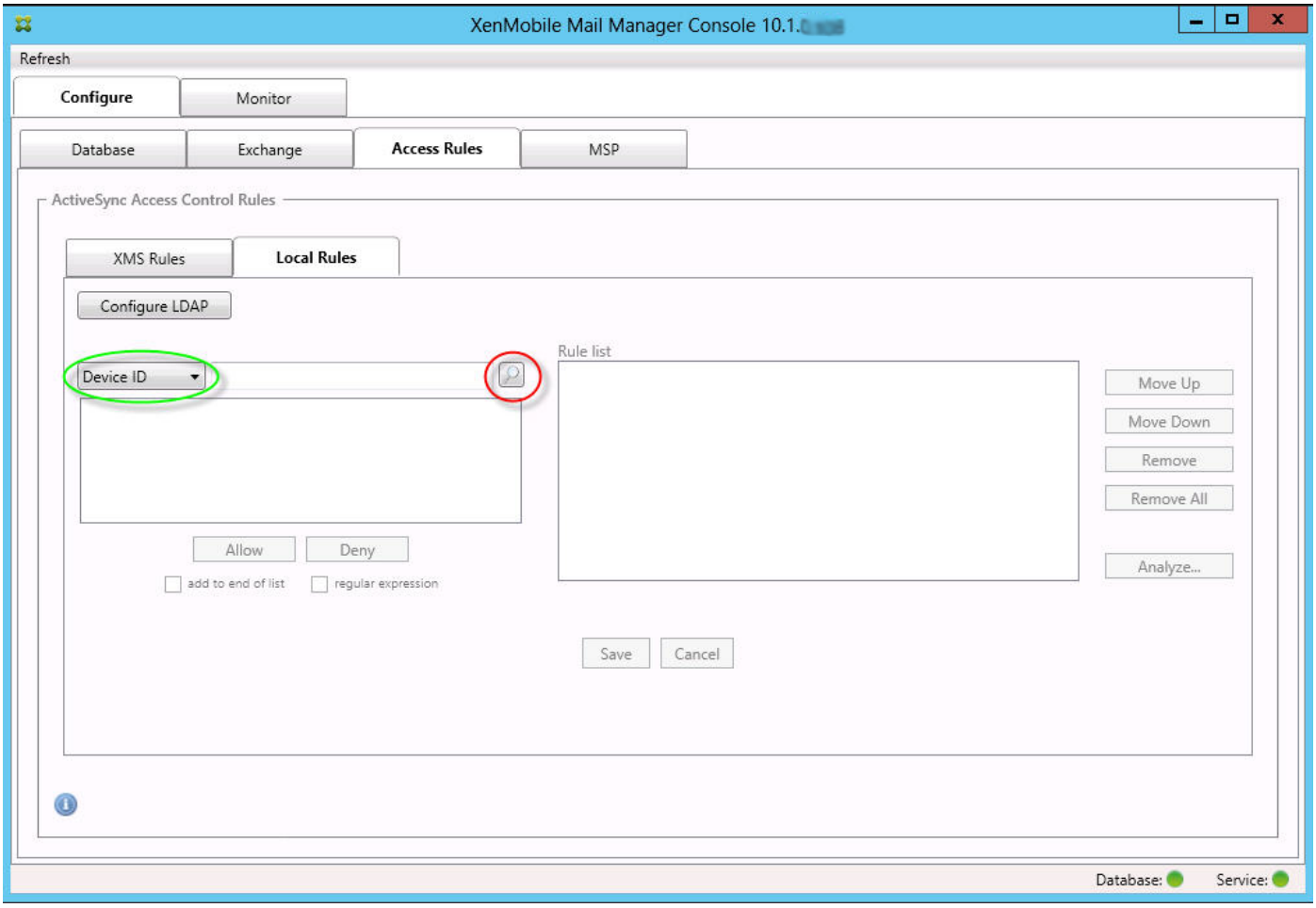


5. Damit alle Gerätetypen, deren Gerätetypwert "Samsung" enthält, zugelassen werden, fügen Sie eine Regel mit regelmäßigem Ausdruck wie folgt hinzu:
   1. Klicken Sie in das Textfeld des ausgewählten Elements.
   2. Ändern Sie den Text SAMSUNGSPHL720 in SAMSUNG.*
   3. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist.
   4. Klicken Sie auf Allow.

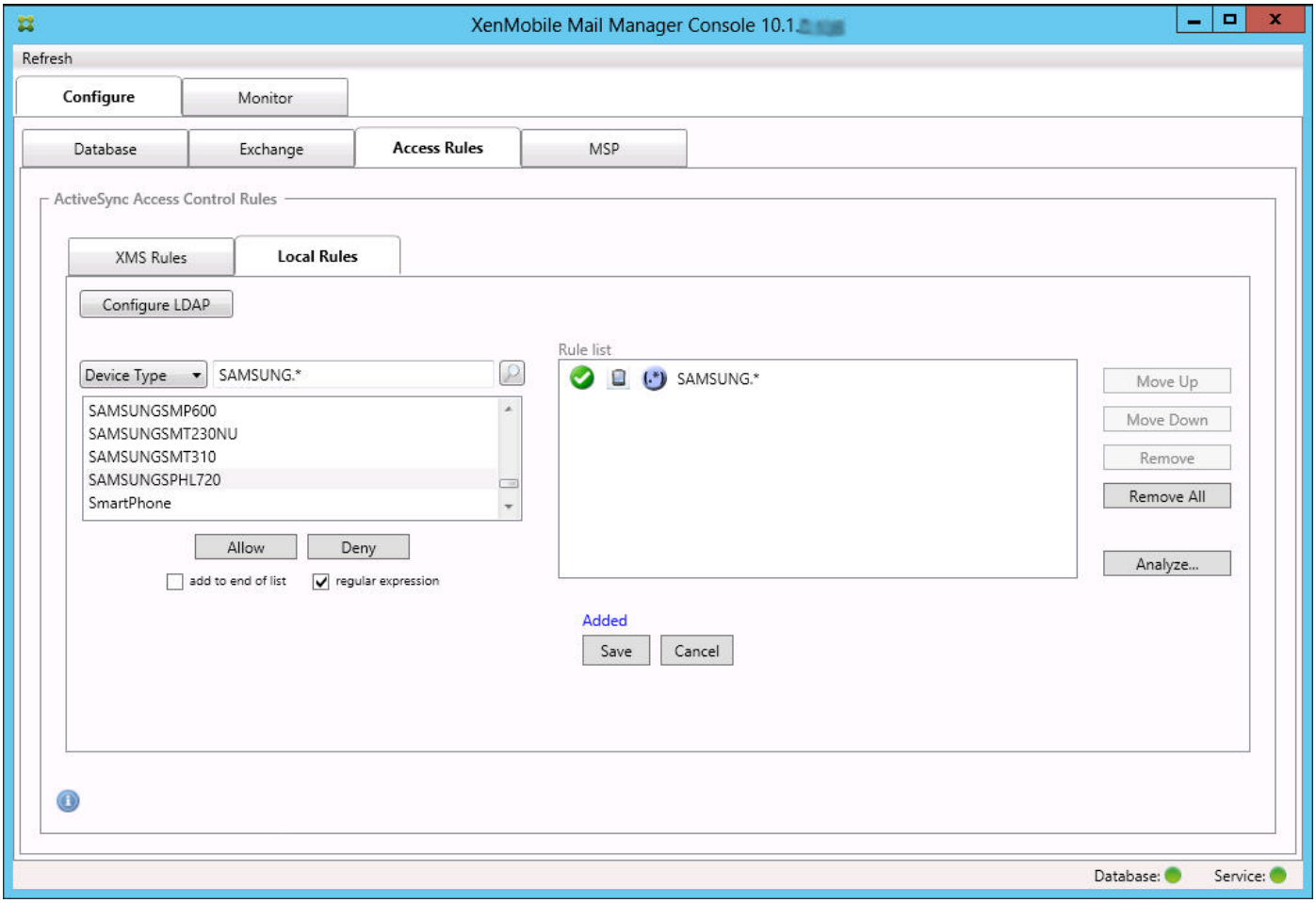


Erstellen einer Zugriffsregel

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.



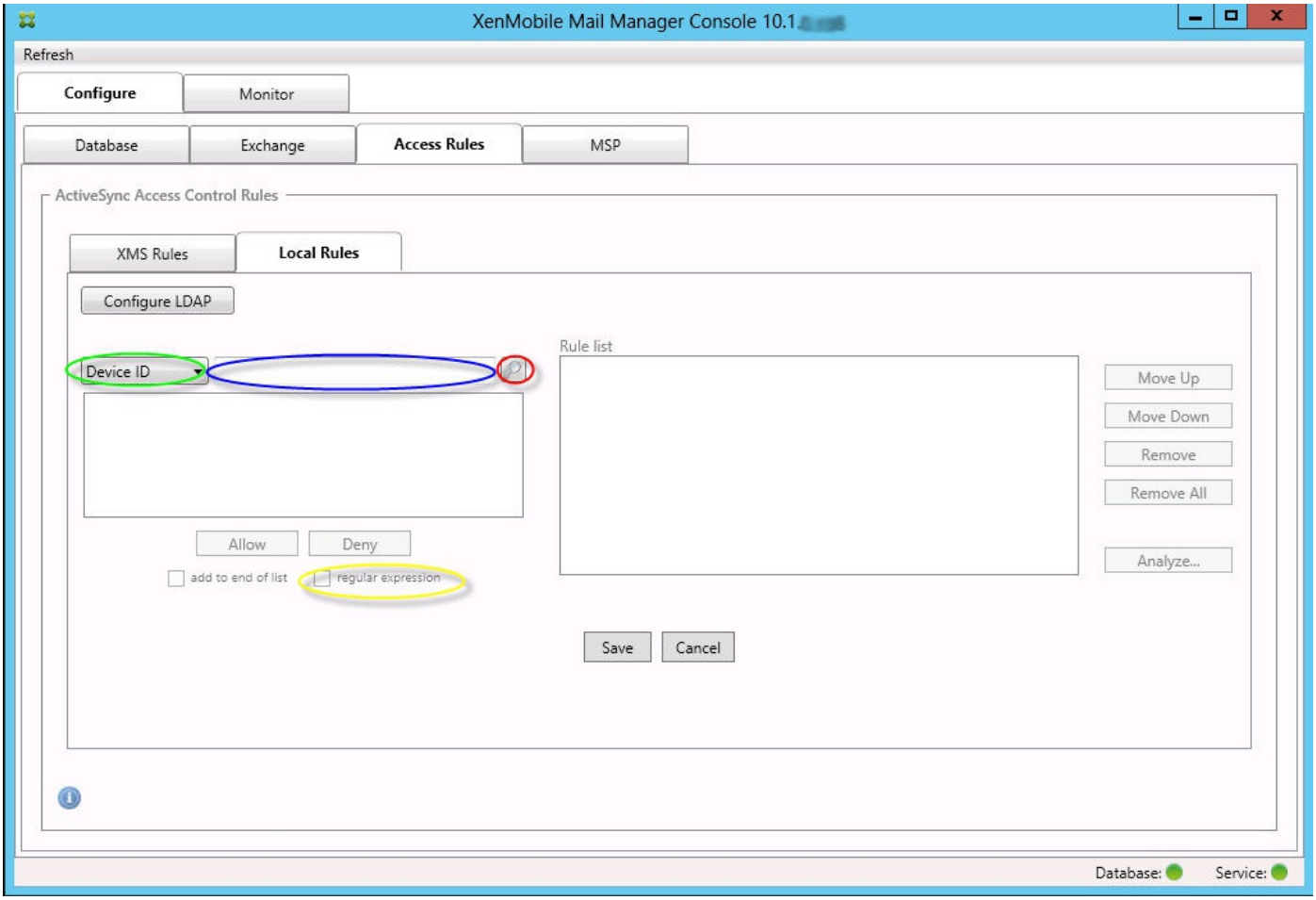
3. Wählen Sie das Feld aus, gegen das der Abgleich stattfinden soll. In diesem Beispiel ist dies Device Type.
4. Geben Sie den regelmäßigen Ausdruck ein. In diesem Beispiel ist dies samsung.*
5. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist, und klicken Sie auf Allow oder Deny. In diesem Beispiel lautet die Auswahl Allow und das Endergebnis ist wie folgt:



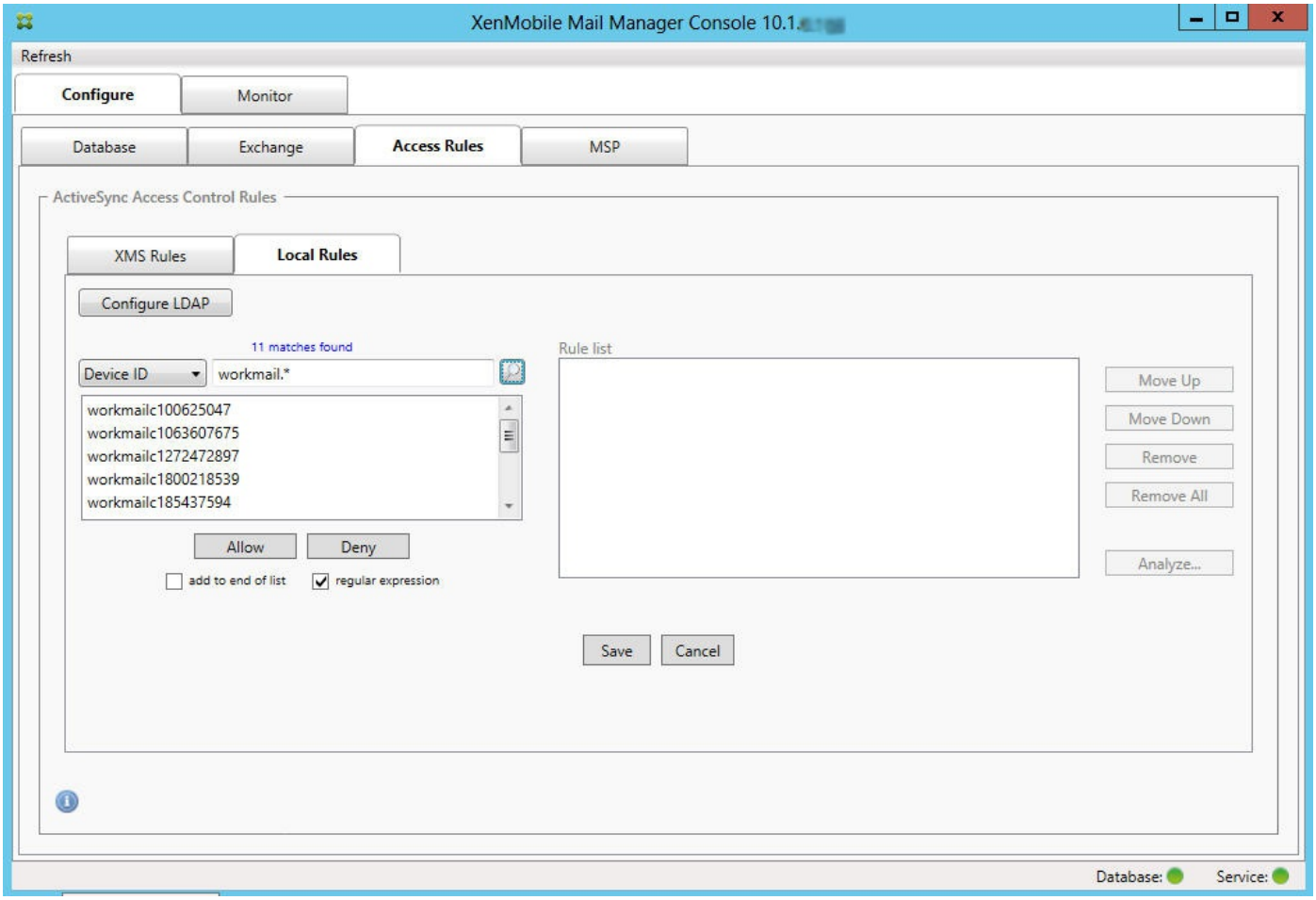
Suchen von Geräten

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.



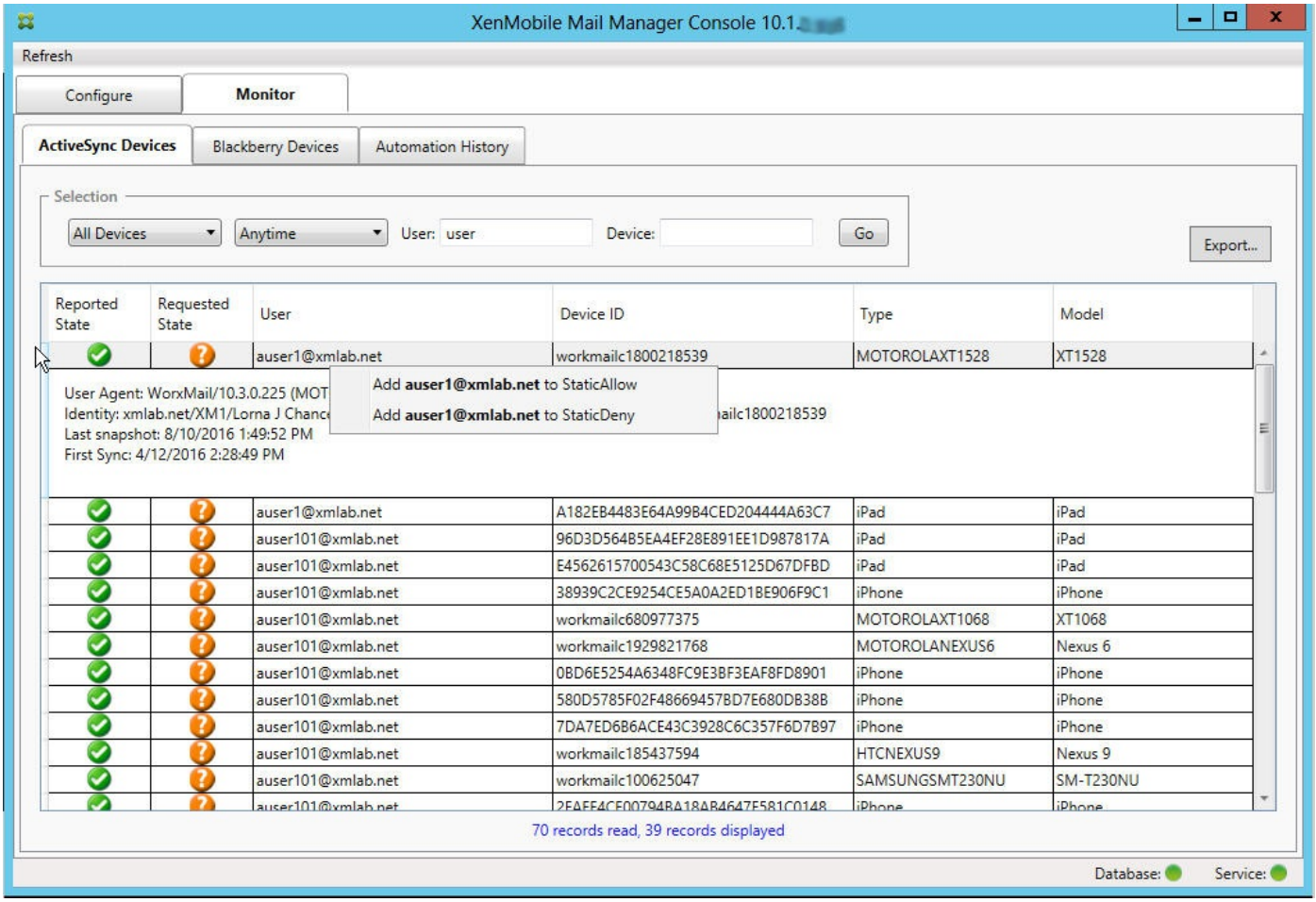
3. Klicken Sie in das Textfeld des ausgewählten Elements (blau in der Abbildung oben) und geben Sie workmail.* ein.
4. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist, und klicken Sie auf das Lupensymbol, damit Übereinstimmungen angezeigt werden (siehe folgende Abbildung).



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

Feb 24, 2017

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

Feb 24, 2017

In folgender Protokolldatei von XenMobile Mail Manager werden Fehler und andere Betriebsinformationen aufgezeichnet: <Installationsordner>\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.

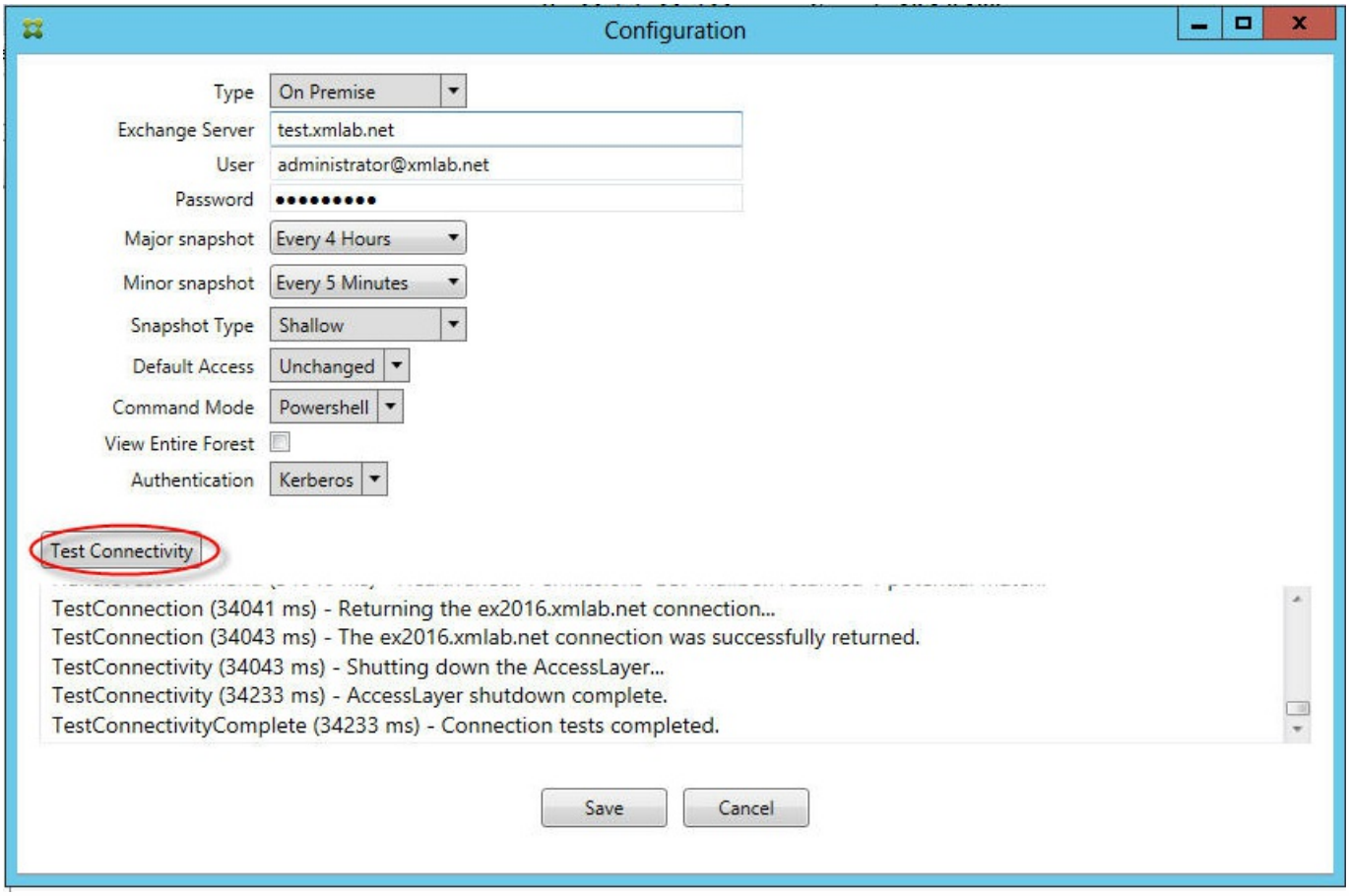
  Wenn die integrierte Windows-Authentifizierung konfiguriert ist, muss das Benutzerkonto von XenMobile Mail Manager als zulässige SQL-Anmeldung konfiguriert sein. Standardmäßig ist das Konto des XenMobile Mail Manager-Diensts das lokale System, es kann aber in jedes beliebige Konto, das über lokale Administratorprivilegien 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 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

Feb 24, 2017

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" des XenMobile-Bereitstellungshandbuchs.