XenMobile Server: Aktuelles Release

Contents

Versionshinweise für Rolling Patches

January 6, 2022

Dieser Abschnitt enthält die Versionshinweise für aktuelle XenMobile Server-Rolling Patches. Über die nachfolgenden Links können Sie Informationen zu behobenen und bekannten Problemen, Featureänderungen und erforderlichen Maßnahmen anzeigen.

Das neueste Rolling Patch enthält alle Fixes aus der vorherigen Rolling Patches für das gleiche Release.

Versionshinweise für Patches der aktuellen Version	Datum der Veröffentlichung
10.14 Rolling Patch 3	22. Dez 2021
10.14 Rolling Patch 2	Dec 15, 2021
10.14 Rolling Patch 1	19. Nov 2021

Versionshinweise für Patches früherer Versionen	Datum der Veröffentlichung
10.13 Rolling Patch 6	Dec 21, 2021
10.13 Rolling Patch 5	Dec 15, 2021
10.13 Rolling Patch 4	11. August 2021
10.13 Rolling Patch 3	13. Mai 2021
10.13 Rolling Patch 2	25. Februar 2021
10.13 Rolling Patch 1	8. Januar 2021
10.12 Rolling Patch 11	Dec 21, 2021
10.12 Rolling Patch 10	16. Dez 2021
10.12 Rolling Patch 9	8. Okt 2021
10.12 Rolling Patch 8	2. Juni 2021
10.12 Rolling Patch 7	29. März 2021
10.12 Rolling Patch 6	26. Januar 2021
10.11 Rolling Patch 7	18. November 2020
10.10 Rolling Patch 6	22. Juli 2020

Versionshinweise für XenMobile Server 10.14 Rolling Patch 3

January 5, 2022

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.14 Rolling Patch 3 beschrieben.

Dieses Release enthält Fehlerbehebungen.

Informationen zu früheren Patches für XenMobile Server 10.14.0 finden Sie unter Versionshinweise für Rolling Patches.

Versionshinweise für XenMobile Server 10.13 Rolling Patch 6

January 5, 2022

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.13 Rolling Patch 6 beschrieben.

Dieses Release enthält Fehlerbehebungen.

Informationen zu früheren Patches für XenMobile Server 10.13.0 finden Sie unter Versionshinweise für Rolling Patches.

Versionshinweise für XenMobile Server 10.12 Rolling Patch 11

January 5, 2022

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.12 Rolling Patch 11 beschrieben.

Dieses Release enthält Fehlerbehebungen.

Informationen zu früheren Patches für XenMobile Server 10.12.0 finden Sie unter Versionshinweise für Rolling Patches.

Versionshinweise für XenMobile Server 10.12 Rolling Patch 10

January 5, 2022

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.12 Rolling Patch 10 beschrieben.

Dieses Release enthält Fehlerbehebungen.

Informationen zu früheren Patches für XenMobile Server 10.12.0 finden Sie unter Versionshinweise für Rolling Patches.

Versionshinweise für XenMobile Server 10.14 Rolling Patch 2

January 5, 2022

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.14 Rolling Patch 2 beschrieben.

Informationen zu früheren Patches für XenMobile Server 10.14.0 finden Sie unter Versionshinweise für Rolling Patches.

Behobenes Problem

In XenMobile Server beobachten Sie zu Spitzenzeiten eine hohe CPU-Auslastung für Serverknoten. [CXM-102568]

Versionshinweise für XenMobile Server 10.13 Rolling Patch 5

January 5, 2022

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.13 Rolling Patch 5 beschrieben.

Neue Features

- **Unterstützung für Windows 11-Geräte.** Sie können jetzt den XenMobile Server verwenden, um Windows 11-Geräte zu verwalten. Weitere Informationen finden Sie in der Liste der unterstützten Betriebssysteme. [CXM-99998]
- **Konfigurieren Sie den Verbindungsmodus und die Netzwerkpriorität für macOS.** Aktivieren Sie in der Wi-Fi-Geräterichtlinie die Einstellung **Verbindungsmodus** für macOS-Geräte, um festzulegen, wie Benutzer eine Verbindung zum Netzwerk herstellen. Das Gerät kann den Benutzer dann mit den Systemanmeldeinformationen oder den im Anmeldefenster eingegebenen Anmeldeinformationen authentifizieren. Wenn Sie mehrere Netzwerke haben, geben Sie

eine Ziffer im Feld **Priorität** ein, um die Priorität der Netzwerkverbindung zu definieren. Das Gerät wählt dann das Netzwerk mit der niedrigsten Ziffer. Weitere Informationen finden Sie in den macOS-Einstellungen unter Wi-Fi-Geräterichtlinie. [CXM-100533]

- XenMobile Server kann keine Gruppenlizenzen mit Google synchronisieren, da die Unterstützung für Gruppenlizenzen auf Android Enterprise-Geräten von Google nicht mehr unterstützt wird. Weitere Informationen finden Sie in diesem Artikel. [CXM-101309]

Informationen zu früheren Patches für XenMobile Server 10.13.0 finden Sie unter Versionshinweise für Rolling Patches.

Behobene Probleme

- Nach der Registrierung eines Geräts mit iOS 15 oder macOS 12 wird das MDM-Konfigurationsprofil als “Nicht verifiziert” angezeigt. [CXM-99380]
- Auf Geräten installierte Apple Volume Purchase-Apps werden automatisch auf die aktuelle Version aktualisiert, wenn die Einstellung für **Automatische App-Updates** deaktiviert ist. [CXM-99723]
- Wenn Sie in der XenMobile Server-Konsole die Einstellungen einer App ändern, um alle Plattformen zu löschen, und speichern, wird die App nicht unter **Konfigurieren > Apps**aufgeführt. [CXM-99850]
- Auf einigen Android Enterprise-Geräten werden Bereitstellungsgruppen und zugewiesene Richtlinien oder Apps zeitweise nicht angewendet. [CXM-101554]
- Auf dem XenMobile Server beobachten Sie zu Spitzenzeiten eine hohe CPU-Auslastung für Serverknoten. [CXM-102450]
- Auf iOS-Geräten, die im Nur-MDM-Modus registriert sind, können Sie keine Apps über Browser hinzufügen, die von Secure Hub aus dem App Store geöffnet wurden. Sie erhalten den folgenden Fehler: **Ihre Anmeldung ist abgelaufen. Melden Sie sich neu an.** [CXM-102604]
- Unter XenMobile Server Version 10.13 können Sie den Storage Zones Controller nicht mit ausschließlich StorageZone Connectors verbinden und konfigurieren. [CXM-102655]
- Auf XenMobile Server-Versionen 10.13 RP1 und höher funktioniert der XenMobile-Internode-Konnektivitäts-Trap der SNMP-Überwachung nicht. [CXM-102788]

Versionshinweise für XenMobile Server 10.14 Rolling Patch 1

January 5, 2022

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.14 Rolling Patch 1 beschrieben.

Neue Features

- **Unterstützung für Windows 11-Geräte.** Sie können jetzt XenMobile verwenden, um Windows 11-Geräte zu verwalten. Weitere Informationen finden Sie in der Liste der unterstützten Betriebssysteme. [CXM-99999]
- **Konfigurieren Sie den Verbindungsmodus und die Netzwerkpriorität für macOS.** Aktivieren Sie in der Wi-Fi-Geräterichtlinie die Einstellung **Verbindungsmodus** für macOS-Geräte, um festzulegen, wie Benutzer eine Verbindung zum Netzwerk herstellen. Das Gerät kann den Benutzer dann mit den Systemanmeldeinformationen oder den im Anmeldefenster eingegebenen Anmeldeinformationen authentifizieren. Wenn Sie mehrere Netzwerke haben, geben Sie eine Ziffer im Feld **Priorität** ein, um die Priorität der Netzwerkverbindung zu definieren. Das Gerät wählt dann das Netzwerk mit der niedrigsten Ziffer. Weitere Informationen finden Sie in den macOS-Einstellungen unter Wi-Fi-Geräterichtlinie. [CXM-100879]
- XenMobile Server kann keine Gruppenlizenzen mit Google synchronisieren, da die Unterstützung für Gruppenlizenzen auf Android Enterprise-Geräten von Google nicht mehr unterstützt wird. Weitere Informationen finden Sie in diesem Artikel. [CXM-101209]

Bekannte Probleme

Registrierte Geräte, die von macOS 11 oder früher auf macOS 12 aktualisiert wurden, oder neu auf macOS12 registrierte Geräte können unter **Systemeinstellungen > Profile** auf dem Gerät als “Nicht verifiziert” angezeigt werden. Weitere Informationen und ein Workaround finden Sie in diesem Support-Artikel.[CXM-101843]

Behobene Probleme

- Nach der Registrierung eines Geräts mit iOS 15 oder macOS 12 wird das MDM-Konfigurationsprofil als **Nicht verifiziert** angezeigt. [CXM-99379]
- Wenn Sie in der XenMobile Server-Konsole die Einstellungen einer App ändern, um alle Plattformen zu löschen, und speichern, wird die App nicht unter **Konfigurieren > Apps**aufgeführt. [CXM-99851]
- Sie können Citrix Launcher auf der Android Enterprise-Plattform nicht beenden. Sie erhalten den folgenden Fehler: **Falsches Kennwort**. [CXM-100975]
- Auf XenMobile Server Version 10.14 können Sie die Richtlinie zum Importieren von iOS- und macOS-Profilen nicht bearbeiten. [CXM-102393]

Versionshinweise für XenMobile Server 10.12 Rolling Patch 9

January 5, 2022

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.12 Rolling Patch 9 beschrieben.

Neue Features

Unterstützung für Android 12. XenMobile Server unterstützt jetzt Android 12 auf Android Enterprise-Geräten. Eine Zusammenfassung der Vorteile für Sicherheit und Datenschutz finden Sie in der Google-Dokumentation für Android. [CXM-97765]

Unterstützung für Windows 11-Geräte. Sie können jetzt den XenMobile Server verwenden, um Windows 11-Geräte zu verwalten. Weitere Informationen finden Sie in der Liste der unterstützten Betriebssysteme. [CXM-99995]

Behobene Probleme

Auf Geräten installierte Apple Volume Purchase-Apps werden automatisch auf die aktuelle Version aktualisiert, wenn die Einstellung für **Automatische App-Updates** deaktiviert ist. [CXM-95985]

Auf XenMobile Server Version 10.12 wird beim Zugriff auf **Gerätedetails** eine Fehlermeldung angezeigt. Dieser Fehler tritt auf, wenn die Geräteeigenschaft einen Wert in **”“** hat. [CXM-97953]

Wenn Sie in der XenMobile Server-Konsole die Einstellungen einer App ändern, um alle Plattformen zu deaktivieren und zu speichern, wird die App nicht unter **Konfigurieren > Apps**aufgeführt. [CXM-99708]

Versionshinweise für XenMobile Server 10.13 Rolling Patch 4

September 24, 2021

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.13 Rolling Patch 4 beschrieben.

Neue Features

Unterstützung für Android 12. XenMobile Server unterstützt jetzt Updates von Android Enterprise-Geräten auf Android 12. Eine Zusammenfassung der Vorteile für Sicherheit und Datenschutz finden Sie in der Android-Dokumentation.

Informationen zu früheren Patches für XenMobile Server 10.13.0 finden Sie unter Versionshinweise für Rolling Patches.

Behobene Probleme

- Die Servereigenschaft `ios.mdm.apns.connectionPoolSize` wird ausgeblendet, wenn Sie zur HTTP/2-basierten API für APNs wechseln. [CXM-95479]
- Unter XenMobile Server Version 10.12 können Sie die VPP-Eigenschaften für bestimmte Apps nicht ändern. [CXM-96854]
- Die erforderlichen Web-Apps werden auf Nur-MDM-Geräten nicht automatisch installiert. [CXM-97477]
- Wenn Sie auf XenMobile Server Version 10.13 den Proxyserver über die **Befehlszeilenschnittstelle** konfigurieren, können Sie keine Benachrichtigungen an Secure Hub auf iOS-Geräten senden. [CXM-97807]
- Auf XenMobile Server Version 10.13 wird beim Zugriff auf **Gerätedetails** eine Fehlermeldung angezeigt. Dieser Fehler tritt auf, wenn die Geräteeigenschaft einen Wert in **”“** hat. [CXM-97951]

Versionshinweise für XenMobile Server 10.12 Rolling Patch 8

June 11, 2021

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.12 Rolling Patch 8 beschrieben.

Neue Features

Erneuerung des Secure Hub-APNs-Zertifikats. Das Secure Hub-APNs-Zertifikat (Apple Push Notification Service) für XenMobile Server 10.12 läuft am 17. Juni 2021 ab. Dieses Update erneuert das Secure Hub APNs-Zertifikat, das am 7. Mai 2022 abläuft. [CXM-94513]

Behobene Probleme

- Die Geräteeigenschaften von Geräten mit macOS 10.14+ werden nicht immer direkt nach der Registrierung in der XenMobile Server-Konsole angezeigt. Nach dem Geräteneustart werden die Geräteeigenschaften wie erwartet angezeigt. [CXM-94221]
- Bei XenMobile Server 10.12 kann ShareFile zeitweise keine Verbindung herstellen. [CXM-95419]

Versionshinweise für XenMobile Server 10.13 Rolling Patch 3

May 21, 2021

In diesen Versionshinweisen werden Erweiterungen sowie behobene und bekannte Probleme in XenMobile Server 10.13 Rolling Patch 3 beschrieben.

Neue Features

Erneuerung des Secure Hub-APNs-Zertifikats. Das Secure Hub-APNs-Zertifikat (Apple Push Notification Service) für XenMobile Server 10.13 läuft am 17. Juni 2021 ab. Dieses Update erneuert das Secure Hub APNs-Zertifikat, das am 7. Mai 2022 abläuft. [CXM-94070]

Alternativer Port für APNs-Benachrichtigungen. XenMobile Server unterstützt jetzt die Verwendung von Port 2197 als Alternative zu Port 443. Port 2197 wird zum Senden von APNs-Benachrichtigungen an `api.push.apple.com` und für den Erhalt von Feedback von dort verwendet. Der Port verwendet die HTTP/2-basierte APNs-Anbieter-API. Der Standardwert der Servereigenschaft `apns.http2.alternate.port.enabled` ist **`false`**. Um den alternativen Port zu verwenden, aktualisieren Sie die Servereigenschaft und starten Sie den Server neu. [CXM-93911]

Behobene Probleme

Die Geräteeigenschaften von Geräten mit macOS 10.14+ werden nicht immer direkt nach der Registrierung in der XenMobile Server-Konsole angezeigt. Nach dem Geräteneustart werden die Geräteeigenschaften wie erwartet angezeigt. [CXM-94150]

Wenn Sie die Einstellungen **System-Apps aktivieren** und **Anwendungen deaktivieren** für dieselbe App in der Richtlinie “Einschränkungen” aktivieren, wird die App im Arbeitsprofil angezeigt. [CXM-94097]

Wenn Sie SNMP-Benutzer zur XenMobile Server-Konsole hinzufügen, erscheinen die Benutzer nicht in der Liste der **SNMP-Überwachungsbenutzer** oder die SNMP-Agents werden inaktiv. [CXM-93199]

In XenMobile Server wird für NetScaler Gateway-Verbindungsprüfungen kein Ergebnis angezeigt. [CXM-93134]

In der XenMobile Server-Konsole wird nicht das richtige Ablaufdatum für das Stammzertifikat angezeigt. [CXM-93133]

Neue Features in XenMobile Server 10.14

January 5, 2022

Fortgesetzte Unterstützung von in Citrix ADC veralteten Classic-Richtlinien

Einige auf Classic-Richtlinien basierende Features gelten laut Ankündigung von Citrix in Citrix ADC ab Version 12.0 Build 56.20 als veraltet. Diese Hinweise für Citrix ADC haben keine Auswirkungen auf bestehende XenMobile Server-Integrationen mit Citrix Gateway. XenMobile Server unterstützt weiterhin die Classic-Richtlinien. Es sind keine Maßnahmen erforderlich.

XenMobile Migration Service

Wenn Sie die On-Premises-Version von XenMobile Server verwenden, hilft Ihnen unser kostenloser XenMobile Migration Service beim Start in Endpoint Management. Für die Migration von XenMobile Server zu Citrix Endpoint Management ist keine erneute Registrierung von Geräten erforderlich.

Wenden Sie sich an Ihren lokalen Citrix Vertriebsmitarbeiter oder Citrix Partner, um die Migration zu starten. Siehe XenMobile Migration Service.

Ankündigung für das Einstellen der Unterstützung

Weitere Vorabinformationen zu den Citrix XenMobile-Features, die schrittweise entfernt werden, finden Sie unter Einstellung von Features und Plattformen.

Vor dem Upgrade von Endpunkten auf iOS 14.5

Citrix empfiehlt, dass Sie vor dem Upgrade eines Endpunkts auf iOS 14.5 die folgenden Aktionen ausführen, um App-Abstürze zu verringern:

- Aktualisieren Sie Citrix Secure Mail und Secure Web auf Version 21.2.X oder höher. Siehe Durchführen eines Upgrades von MDX- oder Unternehmensapps.
- Bei Verwendung des MDX Toolkits umschließen Sie alle iOS-Anwendungen von Drittanbietern mit MDX Toolkit 21.3.X oder höher. Die neueste Version des MDX Toolkit finden Sie auf der Downloadseite.

Vor dem Upgrade von on-premises Citrix ADC

Das Upgrade von on-premises Citrix ADC auf bestimmte Versionen kann zu einem Single Sign-On-Fehler führen. Single Sign-On bei Citrix Files oder die ShareFile-Domänen-URL in einem Browser mit der Option **Mitarbeiteranmeldung** führt zu einem Fehler. Der Benutzer kann sich nicht anmelden.

Workaround für das Problem: Aktivieren Sie Single Sign-On global, indem Sie folgenden Befehl von der ADC-Befehlszeilenschnittstelle auf Citrix Gateway ausführen (sofern dies noch nicht erfolgt ist):

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


Weitere Informationen:

- Citrix ADC Release (Feature Phase) 13.0 Build 67.39/67.43
- Beeinträchtigte Single Sign-On-Konfigurationen

Nachdem Sie den Workaround ausgeführt haben, können Benutzer sich mit der Option “Mitarbeiteranmeldung” in einem Browser per Single Sign-On an Citrix Files oder der ShareFile-Domänen-URL authentifizieren. [CXM-88400]

Vor dem Upgrade auf XenMobile 10.14 (on-premises)

Einige Systemanforderungen haben sich geändert. Weitere Informationen finden Sie unter Systemanforderungen und Kompatibilität sowie XenMobile-Kompatibilität.

1. Wenn die virtuelle Maschine mit dem zu aktualisierenden XenMobile Server weniger als 8 GB RAM hat, sollten Sie den RAM auf mindestens 8 GB erhöhen.
2. Aktualisieren Sie den Citrix Lizenzserver auf 11.16 oder höher, bevor Sie die aktuelle Version von XenMobile Server 10.14 installieren.

   Die neueste Version von XenMobile erfordert Citrix Lizenzserver 11.16 (Mindestversion).

   > **Hinweis:**
   >
   > Das Customer Success Services-Datum (bisher “Subscription Advantage”-Datum) in XenMobile 10.14 ist der 15. September 2021. Das Customer Success Services-Datum der Citrix Lizenz muss nach diesem Datum liegen.
   >
   > Das Datum wird neben der Lizenz auf dem Lizenzserver angezeigt. Wenn Sie die aktuelle Version von XenMobile mit einer älteren Lizenzserverumgebung verbinden, schlägt die Konnektivitätsprüfung fehl und der Lizenzserver kann nicht konfiguriert werden.

   Zum Verlängern des Datums für Ihre Lizenz laden Sie die aktuelle Lizenzdatei vom Citrix Portal herunter und laden Sie sie in den Lizenzserver hoch. Siehe Customer Success Services.
3. Clusterumgebungen: Für die Bereitstellung von iOS-Richtlinien und -Apps auf Geräten mit iOS 11 oder später gilt folgende Anforderung. Ist Citrix Gateway für SSL-Persistenz konfiguriert, müssen Sie auf allen XenMobile Server-Knoten Port 80 öffnen.
4. Empfehlung: Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine zum Erstellen eines Systemsnapshots. Sichern Sie außerdem die Konfigurationsdatenbank des Systems. Sollten bei einem Upgrade Probleme auftreten, können Sie mit vollständigen Backups eine Wiederherstellung vornehmen.

Ausführen des Upgrades

Ab diesem Release unterstützt XenMobile VMware ESXi 7.0. Führen Sie ein Upgrade auf 10.14 durch, bevor Sie ESXi 7.0 installieren oder auf diese Version upgraden.

Sie können ein direktes Upgrade auf XenMobile 10.14 von XenMobile 10.13.x oder 10.12.x ausführen. Um das Upgrade durchzuführen, laden Sie die neueste verfügbare Binärdatei herunter: https://www.citrix.com/downloads. Navigieren Sie zu **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. Klicken Sie auf der Kachel der XenMobile Server-Software für Ihren Hypervisor auf **Datei herunterladen**.

Verwenden Sie zum Hochladen des Upgrades die Seite **Releasemanagement** der XenMobile-Konsole. Siehe Upgrade über die Seite "Releasemanagement".

Nach dem Upgrade

Wenn Funktionen, die ausgehende Verbindungen nutzen, nicht mehr funktionieren und Sie die Verbindungskonfiguration nicht geändert haben, überprüfen Sie das XenMobile Server-Protokoll auf Fehlermeldungen wie etwa "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer".

- Ein Fehler bei der Zertifikatvalidierung bedeutet, dass Sie die Hostnamenüberprüfung auf dem XenMobile-Server deaktivieren müssen.
- In der Standardeinstellung ist die Hostnamenüberprüfung für ausgehende Verbindungen mit Ausnahme des Microsoft PKI-Servers aktiviert.
- Wenn die Hostnamenüberprüfung Fehler in der Bereitstellung verursacht, ändern Sie die Servereigenschaft `disable.hostname.verification` in **`true`**. Der Standardwert dieser Eigenschaft ist **`false`**.

Änderungen bei der Plattformunterstützung

- **iOS 15:** XenMobile Server und mobile Produktivitätsapps von Citrix Apps sind mit iOS 15 kompatibel, unterstützen aber derzeit keine neuen iOS 15-Features.
- **Android 12:** XenMobile Server unterstützt Android 12. Informationen dazu, wie sich die Außerbetriebnahme von Google Device Administration APIs auf Geräte mit Android 10+ auswirkt, finden Sie unter Migration von der Geräteverwaltung zu Android Enterprise. Lesen Sie auch diesen Citrix-Blog.

Geräterichtlinien

- Zur besseren Integration von Google-Einstellungen und weiteren Vereinfachung der Konfiguration haben wir allen Registrierungsmodi für Android Enterprise zwei Einstellungen hinzugefügt.

  - **Bluetooth-Freigabe zulassen:** Wenn diese Option deaktiviert ist, können Benutzer keine ausgehende Bluetooth-Freigabe auf ihrem Gerät einrichten.
  - **App-Deinstallation zulassen:** Ermöglicht Benutzern die Deinstallation von Apps aus dem verwalteten Google Play Store.

  Außerdem haben wir die Einstellung **Drahtloses Upgrade zulassen** von der Einschränkungsrichtlinie in die Richtlinie "OS-Updates" verschoben.

  Weitere Informationen zu diesen Änderungen finden Sie unter Geräteeinschränkungsrichtlinie und Geräterichtlinie für OS-Updates.

- Die Einschränkungseinstellungen für Android Enterprise wurden aus Gründen der Übersichtlichkeit umstrukturiert. In einigen Fällen wurden die Einstellungsnamen geringfügig geändert. Weitere Informationen zu dieser Umstrukturierung finden Sie unter Android Enterprise-Einstellungen.
- Sie können verwaltete Apps auf Android Enterprise-Geräten jetzt automatisch aktualisieren. Weitere Informationen finden Sie unter Verwaltete Apps automatisch aktualisieren.
- Sie können eine Liste von Dateitypen konfigurieren, die mit der Dateirichtlinie hochgeladen werden können. Die folgenden Dateitypen können nicht hochgeladen werden, selbst wenn Sie sie dieser Positivliste hinzufügen:

  - CAB
  - APPX
  - IPA
  - APK
  - XAP
  - MDX
  - .exe

  Weitere Informationen finden Sie unter Servereigenschaften.

Geräteregistrierung

- Sie können jetzt verschiedene Registrierungsprofile für iOS- und Android-Geräte erstellen. XenMobile Server unterstützt eine Reihe von Registrierungsprofilen mit verschiedenen Registrierungstypen. Weitere Informationen finden Sie unter Registrierungsprofile.
- Vollständig verwaltete Geräte ab Android 11 werden im Modus "Arbeitsprofil auf unternehmenseigenen Geräten" registriert. Durch den neuen Modus werden private und geschäftliche Profile auf einem Gerät noch stärker getrennt. Diese Änderung ermöglicht eine größere Kontrolle über das verwaltete Profil und bietet Benutzern mehr Datenschutz für ihr persönliches Profil. Weitere Informationen finden Sie unter Android Enterprise und Servereigenschaften.

- Sie können jetzt weitere Setupbildschirme angeben, die beim Einrichten von iOS- oder macOS-Geräten zu überspringen sind.
  - iOS
    - **Wiederherstellung abgeschlossen:** Verhindert, dass Benutzer sehen, ob eine Wiederherstellung während des Setups abgeschlossen wird. Für iOS 14.0 und höher.
    - **Aktualisierung abgeschlossen:** Verhindert, dass Benutzer sehen, ob ein Softwareupdate während des Setups abgeschlossen wird. Für iOS 14.0 und höher.
  - macOS
    - **Bedienungshilfen:** Verhindert, dass Benutzer automatisch Erläuterungen per Sprachausgabe hören. Nur verfügbar, wenn das Gerät mit dem Ethernet verbunden ist. Für macOS 11 und höher.
    - **Biometrie:** Verhindert, dass Benutzer Touch ID und Face ID einrichten. Für macOS 10.12.4 und höher.
    - **True Tone:** Verhindert, dass Benutzer Vierkanalsensoren einrichten, um den Weißabgleich des Displays dynamisch anzupassen. Für macOS 10.13.6 und höher.
    - **Apple Pay:** Verhindert, dass Benutzer Apple Pay einrichten. Wenn diese Einstellung deaktiviert ist, müssen Benutzer Touch ID und Apple-ID einrichten. Stellen Sie sicher, dass die Einstellungen **Apple-ID** und **Biometrie** deaktiviert sind. Für macOS 10.12.4 und höher.
    - **Bildschirmzeit:** Verhindert, dass Benutzer die Bildschirmzeit aktivieren. Für macOS 10.15 und höher.

  Weitere Informationen zum Konfigurieren von Setupoptionen finden Sie unter Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm.

Anzeigen von Updateprotokolldateien

Eine neue Option mit dem Namen **Display update log file** ist in der Befehlszeilenschnittstelle **Logs** des **Troubleshooting Menu** verfügbar. Mit dieser Option können Sie eine Liste des Updateprotokollinhalts anzeigen und die Effizienz der Problembehandlung erhöhen. Weitere Informationen zu den Befehlszeilenschnittstellen-Tools finden Sie unter Optionen für die Befehlszeilenschnittstelle.

Fehlerprotokolldatei

Beim Anzeigen von Protokollen unter **Problembehandlung und Support > Protokolle** können Sie nun ein Protokoll anzeigen, in dem aus dem Debugprotokoll gefilterte Fehler angezeigt werden. Weitere Informationen finden Sie unter Anzeigen von Protokolldateien in XenMobile.

Servereigenschaften

- Durch Konfigurieren der Servereigenschaft `afw.allow.legacy.apps` können Sie entscheiden, ob Legacy-Android-Apps auf Android Enterprise-Apps bereitgestellt werden. Weitere Informationen finden Sie unter Servereigenschaften.
- XenMobile Server unterstützt jetzt die Verwendung von Port 2197 als Alternative zu Port 443. Port 2197 wird zum Senden und Empfangen von APNs-Benachrichtigungen von `api.push.apple.com` verwendet. Der Port verwendet die HTTP/2-basierte APNs-Anbieter-API. Der Standardwert der Servereigenschaft `apns.http2.alternate.port.enabled` ist **`false`**. Um Port 2197 zu verwenden, aktualisieren Sie die Servereigenschaft und starten Sie den Server neu.
- Die Kennwortvalidierung verhindert Benutzer mit schwachen Kennwörtern. Wenn für die Eigenschaft `enable.password.strength.validation` der Wert **`true`** festgelegt wurde, können Sie keine lokalen Benutzer mit schwachen Kennwörtern erstellen.

Verbesserung der Liste virtueller VPN-Server

Wenn der VPN-Servername nicht `_XM_XenMobileGetway` enthält, wählt der XenMobile Server den ersten verfügbaren virtuellen VPN-Server in der Liste aus.

Unterstützung für Citrix Launcher

XenMobile Server unterstützt Citrix Launcher auf Android Enterprise-Geräten. Weitere Informationen finden Sie unter Launcher-Konfigurationsrichtlinie.

Überarbeitung der Farben für XenMobile Server

XenMobile Server ist konform mit Citrix Branding-Farbaktualisierungen.

Neue Features in XenMobile Server 10.13

January 5, 2022

XenMobile Server 10.13 (PDF-Download)

Fortgesetzte Unterstützung von in Citrix ADC veralteten Classic-Richtlinien

Einige auf Classic-Richtlinien basierende Features gelten laut Ankündigung von Citrix in Citrix ADC ab Version 12.0 Build 56.20 als veraltet. Diese Hinweise für Citrix ADC haben keine Auswirkungen auf

bestehende XenMobile Server-Integrationen mit Citrix Gateway. XenMobile Server unterstützt weiterhin die Classic-Richtlinien. Es sind keine Maßnahmen erforderlich.

XenMobile Migration Service

Wenn Sie die On-Premises-Version von XenMobile Server verwenden, hilft Ihnen unser kostenloser XenMobile Migration Service beim Start in Endpoint Management. Die Migration von XenMobile Server zu Citrix Endpoint Management erfordert keine erneute Registrierung von Geräten.

Wenden Sie sich an Ihren lokalen Citrix Vertriebsmitarbeiter oder Citrix Partner, um die Migration zu starten. Siehe XenMobile Migration Service.

Ankündigung für das Einstellen der Unterstützung

Weitere Vorabinformationen zu den Citrix XenMobile-Features, die schrittweise entfernt werden, finden Sie unter Einstellung von Features und Plattformen.

Vor dem Upgrade von Endpunkten auf iOS 14.5

Citrix empfiehlt, dass Sie vor dem Upgrade eines Endpunkts auf iOS 14.5 die folgenden Aktionen ausführen, um App-Abstürze zu verringern:

- Aktualisieren Sie Citrix Secure Mail und Secure Web auf Version 21.2.X oder höher. Siehe Durchführen eines Upgrades von MDX- oder Unternehmensapps.
- Bei Verwendung des MDX Toolkits umschließen Sie alle iOS-Anwendungen von Drittanbietern mit MDX Toolkit 21.3.X oder höher. Die neueste Version des MDX Toolkit finden Sie auf der Downloadseite.

Vor dem Upgrade von on-premises Citrix ADC

Das Upgrade von on-premises Citrix ADC auf bestimmte Versionen kann zu einem Single Sign-On-Fehler führen. Single Sign-On bei Citrix Files oder die ShareFile-Domänen-URL in einem Browser mit der Option **Mitarbeiteranmeldung** führt zu einem Fehler. Der Benutzer kann sich nicht anmelden.

Workaround für das Problem: Aktivieren Sie Single Sign-On global, indem Sie folgenden Befehl von der ADC-Befehlszeilenschnittstelle auf Citrix Gateway ausführen (sofern dies noch nicht erfolgt ist):

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

Weitere Informationen:

- Citrix ADC Release (Feature Phase) 13.0 Build 67.39/67.43

- Beeinträchtigte Single Sign-On-Konfigurationen

Nachdem Sie den Workaround ausgeführt haben, können Benutzer sich mit der Option Mitarbeiteranmeldung in einem Browser per Single Sign-On an Citrix Files oder der ShareFile-Domänen-URL authentifizieren. [CXM-88400]

Vor dem Upgrade auf XenMobile 10.13 (on-premises)

Einige Systemanforderungen haben sich geändert. Weitere Informationen finden Sie unter Systemanforderungen und Kompatibilität sowie XenMobile-Kompatibilität.

1. Wenn die virtuelle Maschine mit dem zu aktualisierenden XenMobile Server weniger als 8 GB RAM hat, sollten Sie den RAM auf mindestens 8 GB erhöhen.
2. Aktualisieren Sie den Citrix Lizenzserver auf 11.16 oder höher, bevor Sie die aktuelle Version von XenMobile Server 10.13 installieren.

   Die neueste Version von XenMobile erfordert Citrix Lizenzserver 11.16 (Mindestversion).

   > **Hinweis:**
   >
   > Das Customer Success Services-Datum (bisher "Subscription Advantage"-Datum) in XenMobile 10.13 ist der 29. September 2020. Das Customer Success Services-Datum der Citrix Lizenz muss nach diesem Datum liegen.
   >
   > Das Datum wird neben der Lizenz auf dem Lizenzserver angezeigt. Wenn Sie die aktuelle Version von XenMobile mit einer älteren Lizenzserverumgebung verbinden, schlägt die Konnektivitätsprüfung fehl und der Lizenzserver kann nicht konfiguriert werden.

   Zum Verlängern des Datums für Ihre Lizenz laden Sie die aktuelle Lizenzdatei vom Citrix Portal herunter und laden Sie sie in den Lizenzserver hoch. Siehe Customer Success Services.
3. Clusterumgebungen: Für die Bereitstellung von iOS-Richtlinien und -Apps auf Geräten mit iOS 11 oder später gilt folgende Anforderung. Ist Citrix Gateway für SSL-Persistenz konfiguriert, müssen Sie auf allen XenMobile Server-Knoten Port 80 öffnen.
4. Empfehlung: Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine zum Erstellen eines Systemsnapshots. Sichern Sie außerdem die Konfigurationsdatenbank des Systems. Sollten bei einem Upgrade Probleme auftreten, können Sie mit vollständigen Backups eine Wiederherstellung vornehmen.

Ausführen des Upgrades

Ab diesem Release unterstützt XenMobile VMware ESXi 7.0. Führen Sie ein Upgrade auf 10.13 durch, bevor Sie ESXi 7.0 installieren oder auf diese Version upgraden.

Sie können ein direktes Upgrade auf XenMobile 10.13 von XenMobile 10.12.x oder 10.11.x ausführen. Um das Upgrade durchzuführen, laden Sie die neueste verfügbare Binärdatei herunter: https://www.citrix.com/downloads. Navigieren Sie zu **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. Klicken Sie auf der Kachel der XenMobile Server-Software für Ihren Hypervisor auf **Datei herunterladen**.

Verwenden Sie zum Hochladen des Upgrades die Seite **Releasemanagement** der XenMobile-Konsole. Siehe Upgrade über die Seite "Releasemanagement".

Nach dem Upgrade

Wenn Funktionen, die ausgehende Verbindungen nutzen, nicht mehr funktionieren und Sie die Verbindungskonfiguration nicht geändert haben, überprüfen Sie das XenMobile Server-Protokoll auf Fehlermeldungen wie etwa "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer."

- Ein Fehler bei der Zertifikatvalidierung bedeutet, dass Sie die Hostnamenüberprüfung auf dem XenMobile-Server deaktivieren müssen.
- In der Standardeinstellung ist die Hostnamenüberprüfung für ausgehende Verbindungen mit Ausnahme des Microsoft PKI-Servers aktiviert.
- Wenn die Hostnamenüberprüfung Fehler in der Bereitstellung verursacht, ändern Sie die Servereigenschaft `disable.hostname.verification` in **`true`**. Der Standardwert dieser Eigenschaft ist **`false`**.

Änderungen bei der Plattformunterstützung

- **iOS 14:** XenMobile Server und mobile Produktivitätsapps von Citrix Apps sind mit iOS 14 kompatibel, unterstützen aber derzeit keine neuen iOS 14-Features. Verwenden Sie das MDX Toolkit 20.8.5 oder höher oder bereiten Sie die Apps mit dem MAM-SDK vor.
- **Android 11:** XenMobile Server unterstützt Android 11. Informationen dazu, wie sich die Außerbetriebnahme von Google Device Administration APIs auf Geräte mit Android 10+ auswirkt, finden Sie unter Migration von der Geräteverwaltung zu Android Enterprise. Lesen Sie auch diesen Citrix-Blog.

Konfigurieren mehrerer Geräte- und App-Verwaltungsmodi in einer Umgebung

Sie können jetzt eine einzelne XenMobile-Site für die Unterstützung mehrerer Registrierungskonfigurationen konfigurieren. Die Rolle der Registrierungsprofile wurde um Registrierungseinstellungen für die Geräte- und App-Verwaltung erweitert.

Registrierungsprofile unterstützen mehrere Anwendungsfälle und Gerätemigrationspfade in einer XenMobile-Konsole. Anwendungsfälle:

- Mobilgeräteverwaltung (nur MDM)
- Mobilgeräteverwaltung + Mobilanwendungsverwaltung (MAM)
- Nur MAM
- Registrierung unternehmenseigener Geräte
- BYOD-Registrierung (Möglichkeit des Abwählens der MDM-Registrierung)
- Migration von der Android-Geräteadministratorregistrierung zur Android Enterprise-Registrierung (vollständig verwaltet, Arbeitsprofil, dediziertes Gerät)

Registrierungsprofile ersetzen die nun veraltete Servereigenschaft `xms.server.mode`. Diese Änderung wirkt sich nicht auf bestehende Bereitstellungsgruppen und registrierte Geräte aus.

Wenn Sie keine dedizierten Geräte registrieren müssen, können Sie das Feature deaktivieren, indem Sie die Servereigenschaft `enable.multimode.xms` auf **`false`** festlegen. Siehe Servereigenschaften.

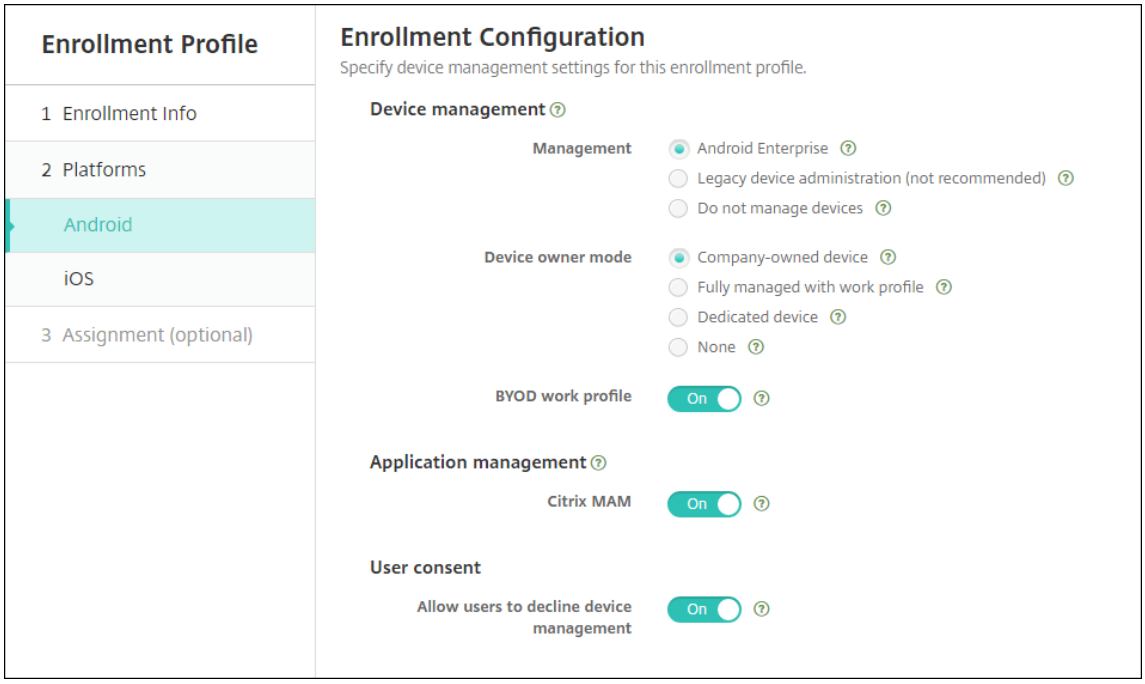
Die folgende Tabelle zeigt den automatisierten Migrationspfad von der Servereigenschaft zum neuen Registrierungsprofilfeature:

Servereigenschaft	Neuer Verwaltungsmodus
ENT-Modus (iOS)	Apple-Geräteregistrierung bei Citrix MAM
ENT-Modus (Android)	Legacygeräteverwaltung mit Citrix MAM
ENT-Modus (Android Enterprise)	Arbeitsprofil, vollständig verwaltet (zuvor COPE), mit Citrix MAM
MAM-Modus (iOS und Android)	Citrix MAM
MDM-Modus (iOS)	Apple-Geräteregistrierung
MDM-Modus (Android)	Legacygeräteverwaltung
MDM-Modus (Android Enterprise)	Arbeitsprofil, vollständig verwaltet

Wenn Sie eine Bereitstellungsgruppe erstellen, können Sie ihr ein Registrierungsprofil anfügen. Wenn Sie kein Registrierungsprofil anfügen, fügt XenMobile das globale Registrierungsprofil an.

Registrierungsprofile bieten die folgenden Geräteverwaltungsfunktionen:

- **Einfachere Migration vom Android-Legacymodus (Android-Geräteadministrator) zu Android Enterprise.** Für Android Enterprise-Geräte steht ein Gerätebesitzermodus zur Auswahl: vollständig verwaltet, Arbeitsprofil, vollständig verwaltet oder dediziert. Siehe Android Enterprise.



Bei diesem Upgrade wird die bestehende XenMobile-Konfiguration für den Servermodus und unter **Einstellungen > Android Enterprise** den neuen Registrierungsprofileinstellungen wie folgt zugeordnet.

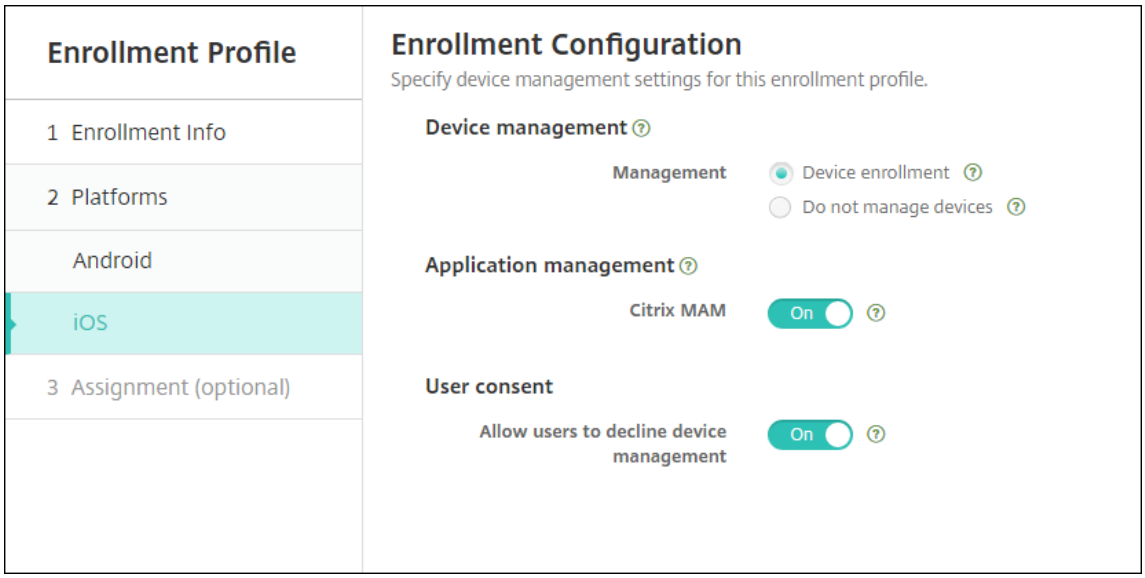
Bestehende Konfiguration	Verwaltungseinstellung	Gerätebesitzermodus	Citrix MAM
MDM. Verwaltetes Google Play (Android Enterprise)	Android Enterprise	Arbeitsprofil, vollständig verwaltet	Aus
MDM; G Suite (Legacy-Geräteadministrator)	Legacy-Geräteadministrator	–	Aus
MAM	Geräte nicht verwalten	–	Ein
MDM+MAM. Verwaltetes Google Play (Android Enterprise)	Android Enterprise*	Arbeitsprofil, vollständig verwaltet	Ein
MDM+MAM; G Suite (Legacy-Geräteadministrator)	Legacy-Geräteadministrator*	–	Ein

*Wenn eine Registrierung erforderlich ist, ist **Benutzer dürfen Geräteverwaltung ablehnen**

auf **Aus** festgelegt.

Nach dem Upgrade spiegeln die aktuellen Registrierungsprofile diese Zuweisung wider. Überlegen Sie ggf. die Erstellung weiterer Registrierungsprofile für neue Anwendungsfälle nach dem Umstieg vom Legacymodus.

- **Vereinfachte iOS-Verwaltung.** iOS-Geräte können als verwaltete oder nicht verwaltete Geräte registriert werden.



Bei diesem Upgrade werden bestehende Konfigurationen den neuen Registrierungsprofileinstellungen wie folgt zugeordnet.

Servermodus	Verwaltungseinstellung	Citrix MAM
MDM	Geräteregistrierung	Aus
MAM	Geräte nicht verwalten	Ein
MDM+MAM	Geräteregistrierung	Ein

Wenn eine Registrierung erforderlich ist, ist **Benutzer dürfen Geräteverwaltung ablehnen** auf **Aus** festgelegt.

Für verbesserte Registrierungsprofile gelten folgende Einschränkungen:

- Das Feature der verbesserten Registrierungsprofile ist für Einladungen zur Authentifizierung per Einmal-PIN oder zur zweistufigen Authentifizierung nicht verfügbar.

Siehe Registrierungsprofile.

Unterstützung für die aktuelle HTTP/2-basierte APNs-Anbieter-API

Apple stellt die Unterstützung für das Legacy-APNs-Binärprotokoll am 31. März 2021 ein. Apple empfiehlt, stattdessen die Verwendung der HTTP/2-basierten APNS-Anbieter-API zu verwenden. XenMobile Server unterstützt jetzt die HTTP/2-basierte API. Weitere Informationen finden Sie unter "Apple Push Notification Service Update" auf https://developer.apple.com/. Informationen zum Überprüfen der Konnektivität zu APNs finden Sie unter Konnektivitätsprüfungen.

Die folgenden Versionen von XenMobile Server unterstützen standardmäßig die HTTP/2-basierte API:

- XenMobile Server 10.13
- XenMobile Server 10.12 Rolling Patch 5 und höher

Wenn Sie die folgenden Versionen von XenMobile Server verwenden, müssen Sie die Servereigenschaft **apple.apns.http2** hinzufügen, um die Unterstützung zu aktivieren:

- XenMobile Server 10.12 Rolling Patches 2-4 und höher
- XenMobile Server 10.11 Rolling Patch 5 und höher

Wir unterstützen XenMobile Server 10.11 nicht mehr und empfehlen ein Upgrade auf die neueste Version.

Verwenden eines gerätezertifikatbasierten IPsec-VPN mit vielen iOS-Geräten

Anstelle des Konfigurierens einer VPN-Geräterichtlinie und einer Geräterichtlinie für Anmeldeinformationen für jedes iOS-Gerät, für das ein gerätezertifikatbasiertes IPSec-VPN erforderlich ist, können Sie den Prozess automatisieren.

1. Konfigurieren Sie eine iOS-VPN-Geräterichtlinie mit dem Verbindungstyp **Always On IKEv2**.
2. Wählen Sie als Geräteauthentifizierungsmethode **Gerätezertifikat basiert auf Geräteidentität**.
3. Wählen Sie den zu verwendenden **Geräteidentitätstyp**.
4. Führen Sie mit der REST-API einen Massenimport der Gerätezertifikate aus.

Weitere Informationen zum Konfigurieren der VPN-Geräterichtlinie finden Sie unter VPN-Geräterichtlinie. Informationen zum Durchführen eines Massenimports von Zertifikaten finden Sie unter Massenupload von Zertifikaten mit der REST-API).

Automatische Updates für Apple Volume Purchase-Apps

Wenn Sie ein Volume Purchase-Konto hinzufügen (**Einstellungen > iOS-Einstellungen**), können Sie jetzt automatische Updates für alle iOS-Apps aktivieren. Weitere Informationen finden Sie in der Einstellung **Automatische App-Updates** in Apple Volume Purchase.

Kennwortanforderungen für lokales Benutzerkonto

Stellen Sie sicher, dass Sie beim Hinzufügen oder Bearbeiten eines lokalen Benutzerkontos in der XenMobile-Konsole die aktuellen Kennwortanforderungen erfüllen.

Weitere Informationen finden Sie unter Hinzufügen eines lokalen Benutzerkontos.

- **Kennwortanforderungen:** Erfüllen Sie beim Hinzufügen oder Bearbeiten eines lokalen Benutzerkontos in der XenMobile Server-Konsole die aktuellen Kennwortanforderungen. Siehe Hinzufügen eines lokalen Benutzerkontos.
- **Sperre des lokalen Benutzerkontos:** Wenn ein Benutzer die maximale Anzahl aufeinanderfolgender ungültiger Anmeldeversuche erreicht, wird das lokale Benutzerkonto für 30 Minuten gesperrt. Das System verweigert alle weiteren Authentifizierungsversuche, bis die Sperrfrist abgelaufen ist. Um das Konto in der XenMobile Server-Konsole zu entsperren, gehen Sie zu **Verwalten > Benutzer**, wählen das Benutzerkonto und klicken auf **Lokalen Benutzer entsperren**. Siehe Entsperren eines lokalen Benutzerkontos.

Geräterichtlinien

Für Android Enterprise-Geräte wurden neue Geräterichtlinien und -einstellungen hinzugefügt.

Ausblenden des Taskleistensymbols auf Android Enterprise-Geräten

Sie können nun auswählen, ob das Symbol für die Taskleiste auf Android Enterprise-Geräten angezeigt oder verborgen wird. Siehe XenMobile-Optionsrichtlinie für Geräte.

Zusätzliche Zertifikatverwaltungsfunktionen für Android Enterprise-Geräte im Arbeitsprofilmodus oder im vollständig verwalteten Modus

Zusätzlich zur Installation von Zertifizierungsstellen im verwalteten Schlüsselspeicher können Sie nun die folgenden Features verwalten:

- **Konfigurieren der von bestimmten verwalteten Apps verwendeten Zertifikate.** Die Richtlinie für Anmeldeinformationen für Android Enterprise enthält jetzt die Einstellung **Apps, die die Zertifikate verwenden**. Sie können die Apps angeben, die die vom in der Richtlinie ausgewählten Anmeldeinformationsanbieter ausgestellten Benutzerzertifikate verwenden sollen. Apps erhalten während der Laufzeit ohne Benutzereingriff Zugriff auf Zertifikate. Zur Verwendung von Zertifikaten für alle Apps lassen Sie die App-Liste leer. Siehe Anmeldeinformationsrichtlinie.
- **Entfernen von Zertifikaten aus dem verwalteten Schlüsselspeicher oder Deinstallieren aller Zertifikate, die nicht von der System-Zertifizierungsstelle stammen, ohne Benutzereingriff** Siehe Anmeldeinformationsrichtlinie.

- **Verhindern, dass Benutzer im Schlüsselspeicher gespeicherte Anmeldeinformationen ändern.** Die Einschränkungsrichtlinie für Android Enterprise enthält jetzt die Einstellung **Benutzer darf Benutzeranmeldeinformationen konfigurieren**. Die Standardeinstellung ist **Ein**. Weitere Informationen finden Sie unter Geräteeinschränkungsrichtlinie.

Einfachere Verwendung des Zertifikatalias in verwalteten Android Enterprise-Konfigurationen

Verwenden Sie die neue Einstellung **Zertifikatalias** in der Geräterichtlinie **Anmeldeinformationen** mit der Geräterichtlinie **Verwaltete Android Enterprise-Konfigurationen**. Dadurch können sich Apps ohne Benutzeraktion im VPN authentifizieren. Statt das Alias für Anmeldeinformationen in den App-Protokollen zu suchen erstellen Sie sie es. Erstellen Sie das Alias, indem Sie es im Feld **Zertifikatalias** der Richtlinie **Verwaltete Android Enterprise-Konfigurationen** eingeben. Geben Sie dann denselben Zertifikatalias in der Einstellung **Zertifikatalias** in der Geräterichtlinie **Anmeldeinformationen** ein. Siehe Richtlinie für verwaltete Android Enterprise-Konfigurationen und Anmeldeinformationsrichtlinie.

Steuerung der Einstellung “Use one lock” auf Android Enterprise-Geräten

Mit der neuen Einstellung **Einheitlichen Passcode aktivieren** in der Geräterichtlinie **Passcode** können Sie festlegen, ob ein Gerät einen separaten Passcode für Gerät und Arbeitsprofil benötigt. Zuvor konnten Benutzer dieses Verhalten mit der Einstellung **Use one lock** auf dem Gerät steuern. Wenn **Einheitlichen Passcode aktivieren** auf **Ein** gesetzt ist, können Benutzer denselben Passcode für ihr Gerät und ihr Arbeitsprofil verwenden. Wenn **Einheitlichen Passcode aktivieren** auf **Aus** gesetzt ist, können Benutzer nicht denselben Passcode für das Gerät und das Arbeitsprofil verwenden. Die Standardeinstellung ist **Aus**. Die Einstellung **Einheitlichen Passcode aktivieren** ist für Android Enterprise-Geräte ab Android 9.0 verfügbar. Weitere Informationen finden Sie unter Passcode-Geräterichtlinie.

Anzeigen nicht richtlinientreuer Apps und Verknüpfungen auf Android Enterprise-Geräten

Die Passcode-Geräterichtlinie für Android Enterprise verfügt über die neue Einstellung **Apps und Verknüpfungen anzeigen, während der Passcode nicht richtlinientreu ist**. Aktivieren Sie die Einstellung, damit Apps und Verknüpfungen sichtbar bleiben, wenn der Gerätepasscode nicht mehr richtlinientreu ist. Citrix empfiehlt, dass Sie eine automatisierte Aktion erstellen, um das Gerät als nicht richtlinientreu zu kennzeichnen, wenn der Passcode nicht richtlinientreu ist. Weitere Informationen finden Sie unter Passcode-Geräterichtlinie.

Deaktivieren der Druckfunktion auf Android Enterprise-Arbeitsprofilgeräten oder vollständig verwalteten Geräten

In der Einschränkungsrichtlinie können Sie mit der Einstellung **Don't allow printing** festlegen, ob Benutzer einen auf dem Android Enterprise-Gerät verfügbaren Drucker verwenden können. Siehe Android Enterprise-Einstellungen.

Zulassen von Apps auf dedizierten Geräten durch Hinzufügen ihres Paketnamens zur Kiosk-Richtlinie

Sie können jetzt Paketnamen eingeben, die Sie für Android Enterprise zulassen möchten. Siehe Android Enterprise-Einstellungen.

Verwalten von Keyguard-Features für das Android Enterprise-Arbeitsprofil und vollständig verwaltete Geräte

Android Keyguard verwaltet die Sperrbildschirme für Gerät und Arbeitsprofil. Mit der Geräterichtlinie für die Keyguard-Verwaltung können Sie Folgendes steuern:

- Keyguard-Verwaltung auf Arbeitsprofilgeräten. Sie können die Funktionen steuern, die Benutzern zur Verfügung stehen, bevor sie den Geräte-Keyguard und den Arbeitsprofil-Keyguard entsperren. Beispielsweise können Benutzer standardmäßig das Entsperren per Fingerabdruck verwenden und unredigierte Benachrichtigungen auf dem Sperrbildschirm anzeigen. Sie können auch über die Richtlinie "Keyguard-Verwaltung" die gesamte biometrische Authentifizierung für Geräte mit Android ab Version 9.0 deaktivieren.
- Keyguard-Verwaltung auf vollständig verwalteten und dedizierten Geräten. Sie können festlegen, ob Funktionen wie "Trust Agents" und "Sichere Kamera" vor dem Entsperren des Keyguard-Bildschirms verfügbar sind. Sie können jedoch auch alle Keyguard-Funktionen deaktivieren.

Siehe Geräterichtlinie für die Keyguard-Verwaltung.

Veröffentlichen von Unternehmensapps für Android Enterprise in der XenMobile-Konsole

Sie müssen sich nicht mehr für ein Google Play-Entwicklerkonto registrieren, wenn Sie eine private Android Enterprise-App hinzufügen. Die XenMobile-Konsole öffnet eine Benutzeroberfläche des verwalteten Google Play-Stores, über die Sie die APK-Datei hochladen und veröffentlichen können. Weitere Informationen finden Sie unter Hinzufügen einer Unternehmensapp.

Veröffentlichen von Web-Apps für Android Enterprise in der XenMobile-Konsole

Sie müssen nicht mehr zum verwalteten Google Play-Store oder zum Google Developer-Portal gehen, um Android Enterprise-Web-Apps für XenMobile zu veröffentlichen. Wenn Sie unter **Konfigurieren > Apps > Weblink** auf **Hochladen** klicken, wird eine Benutzeroberfläche des verwalteten Google Play Store geöffnet, in der Sie die Datei hochladen und speichern können. Genehmigung und Veröffentlichung der App dauert etwa 10 Minuten. Weitere Informationen finden Sie unter Hinzufügen von Weblinks.

Massenupload von Zertifikaten mit der XenMobile Server-REST-API auf iOS-Geräte

Wenn der Upload einzelner Zertifikate nicht praktikabel ist, können Sie mit der XenMobile Server-REST-API einen Massenupload auf iOS-Geräte ausführen.

1. Konfigurieren Sie eine iOS-VPN-Geräterichtlinie mit dem Verbindungstyp **Always On IKEv2**.
2. Wählen Sie als Geräteauthentifizierungsmethode **Gerätezertifikat basiert auf Geräteidentität**.
3. Wählen Sie den zu verwendenden **Geräteidentitätstyp**.
4. Führen Sie mit der REST-API einen Massenimport der Gerätezertifikate aus.

Informationen zum Konfigurieren der VPN-Geräterichtlinie finden Sie unter VPN-Geräterichtlinie. Informationen zum Durchführen eines Massenimports von Zertifikaten finden Sie unter Massenupload von Zertifikaten mit der REST-API auf iOS-Geräte.

Aktualisieren von Verschlüsselungsschlüsseln

Die Option **Refresh encryption keys** wurde den erweiterten Einstellungen der XenMobile-Befehlszeilenschnittstelle hinzugefügt. Mit der Option können Sie die Verschlüsselungsschlüssel für einzelne Knoten aktualisieren. Siehe Optionen des Menüs “System”.

Unterstützung für ESXi 7.0

Ab diesem Release unterstützt XenMobile VMware ESXi 7.0. Führen Sie ein Upgrade auf 10.13 durch, bevor Sie ESXi 7.0 installieren oder auf diese Version upgraden.

Neue Servereigenschaften

Die folgenden Servereigenschaften sind jetzt verfügbar:

- **Allow hostnames for iOS App Store links:** Zum Hochladen öffentlicher App Store-Apps für iOS mithilfe der öffentlichen APIs anstelle der Konsole können Sie eine Liste zulässiger Hostnamen konfigurieren.

- **Local user account lockout limit:** Konfigurieren Sie die Anzahl möglicher Anmeldeversuche für lokale Benutzer, bevor ihr Konto gesperrt wird.
- **Local user account lockout time:** Konfigurieren Sie, wie lange lokale Benutzer nach zu vielen fehlgeschlagenen Anmeldeversuchen ausgesperrt werden.
- **Maximum size of file upload restriction enabled:** Aktivieren Sie die Beschränkung der Dateigröße für hochgeladene Dateien.
- **Maximum size of file upload allowed:** Legen Sie die maximale Dateigröße für hochgeladene Dateien fest.

Ausführliche Informationen zu diesen Eigenschaften finden Sie unter Servereigenschaften.

Self-Service-Datenträgerbereinigung

Das **Troubleshooting Menu** der Befehlszeilenschnittstelle enthält die neue Option **Disk Usage**. Mit dieser Option können Sie eine Liste der Coredump- und Supportpaket-Dateien anzeigen. Nach dem Anzeigen der Liste können Sie alle Dateien über die Befehlszeile löschen. Weitere Informationen zu den Befehlszeilenschnittstellen-Tools finden Sie unter Optionen für die Befehlszeilenschnittstelle.

Neue Features in XenMobile Server 10.12

January 5, 2022

XenMobile Server 10.12 (PDF-Download)

XenMobile Migration Service

Wenn Sie die On-Premises-Version von XenMobile Server verwenden, hilft Ihnen unser kostenloser XenMobile Migration Service beim Start in Endpoint Management. Die Migration von XenMobile Server zu Citrix Endpoint Management erfordert keine erneute Registrierung von Geräten.

Wenden Sie sich an Ihren lokalen Citrix Vertriebsmitarbeiter oder Citrix Partner, um die Migration zu starten. Weitere Informationen finden Sie unter XenMobile Migration Service.

Ankündigung für das Einstellen der Unterstützung

Weitere Vorabinformationen zu den Citrix XenMobile-Features, die schrittweise entfernt werden, finden Sie unter Einstellung von Features und Plattformen.

Vorbereiten Ihrer Android-Geräte auf bevorstehende Änderungen

Das Veralten dieser Features hat Auswirkungen auf Ihre Android- und Android Enterprise-Geräte:

- Geräteadministrator-Registrierungen für Android 10:
  - **31. Juli 2020:** Citrix beendet Neuregistrierungen für die Android-Legacygeräteverwaltung.
  - **1. November 2020:** Google stuft die Legacygeräteverwaltungs-API als veraltet ein. Android 10-Geräte, die mit Legacygeräteverwaltung ausgeführt werden, funktionieren nicht mehr.
- MDX-Verschlüsselung:
  - **1. August 2020:** Die Migration von MDX-Verschlüsselung zu Plattformverschlüsselung wird von Citrix für mobile Produktivitätsapps von Citrix und für MDX-Apps von Drittanbietern durchgesetzt.
  - **1. September 2020:** MDX-Verschlüsselung erreicht das Ende des Lebenszyklus.

Für Geräte, die in der Legacygeräteverwaltung registriert sind

- Wenn Sie keine MDX-Verschlüsselung verwenden, ist keine Aktion erforderlich.
- Wenn Sie die MDX-Verschlüsselung verwenden, müssen Sie Android-Geräte vor dem 31. Juli 2020 zu Android Enterprise migrieren. Geräte mit Android 10 müssen sich mit Android Enterprise registrieren bzw. erneut registrieren. Diese Anforderung betrifft auch Android-Geräte im Nur-MAM-Modus. Siehe Migration von der Geräteverwaltung zu Android Enterprise.

Für Geräte, die bereits in Android Enterprise registriert sind (Stand 31.07.2020)

- Wenn Sie die Apps mit der Android Enterprise-Plattform veröffentlicht haben, wird die Verschlüsselung bereits über Android Enterprise verarbeitet. Es ist keine Aktion erforderlich.
- Wenn Sie die Apps mit der Android-Legacyplattform veröffentlicht haben, müssen Sie die Apps vor dem 31.07.2020 erneut mit Android Enterprise veröffentlichen.

Vor dem Upgrade auf XenMobile 10.12 (on-premises)

Einige Systemanforderungen haben sich geändert. Weitere Informationen finden Sie unter Systemanforderungen und Kompatibilität sowie XenMobile-Kompatibilität.

1. Aktualisieren Sie den Citrix Lizenzserver auf 11.16 oder höher, bevor Sie die aktuelle Version von XenMobile Server 10.12 installieren.

   Die neueste Version von XenMobile erfordert Citrix Lizenzserver 11.16 (Mindestversion).

   > **Hinweis:**
   >
   > Wenn Sie Ihre eigene Lizenz für die Preview verwenden möchten, berücksichtigen Sie, dass

> das Customer Success Services-Datum (bisher “Subscription Advantage”-Datum) in XenMobile 10.12 der 20. Januar 2020 ist. Das Customer Success Services-Datum der Citrix Lizenz muss nach diesem Datum liegen.
>
> Das Datum wird neben der Lizenz auf dem Lizenzserver angezeigt. Wenn Sie die aktuelle Version von XenMobile mit einer älteren Lizenzserverumgebung verbinden, schlägt die Konnektivitätsprüfung fehl und der Lizenzserver kann nicht konfiguriert werden.

Zum Verlängern des Datums für Ihre Lizenz laden Sie die aktuelle Lizenzdatei vom Citrix Portal herunter und laden Sie sie in den Lizenzserver hoch. Weitere Informationen finden Sie unter Customer Success Services.

2. Clusterumgebungen: Für die Bereitstellung von iOS-Richtlinien und -Apps auf Geräten mit iOS 11 oder später gilt folgende Anforderung. Ist Citrix Gateway für SSL-Persistenz konfiguriert, müssen Sie auf allen XenMobile Server-Knoten Port 80 öffnen.
3. Wenn die virtuelle Maschine, auf der die zu aktualisierende XenMobile Server-Instanz ausgeführt wird, weniger als 4 GB RAM hat, erhöhen Sie den RAM auf mindestens 4 GB. Beachten Sie, dass der empfohlene Mindest-RAM für Produktionsumgebungen bei 8 GB liegt.
4. Empfehlung: Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine zum Erstellen eines Systemsnapshots. Sichern Sie außerdem die Konfigurationsdatenbank des Systems. Sollten bei einem Upgrade Probleme auftreten, können Sie mit vollständigen Backups eine Wiederherstellung vornehmen.

Ausführen des Upgrades

Sie können ein direktes Upgrade auf XenMobile 10.12 von XenMobile 10.11.x oder 10.10.x ausführen. Um das Upgrade durchzuführen, laden Sie die neueste verfügbare Binärdatei herunter: https://www.citrix.com/downloads. Navigieren Sie zu **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. Klicken Sie auf der Kachel der XenMobile Server-Software für Ihren Hypervisor auf **Datei herunterladen**.

Verwenden Sie zum Hochladen des Upgrades die Seite **Releasemanagement** der XenMobile-Konsole. Weitere Informationen finden Sie unter Upgrade über die Seite “Releasemanagement”.

Nach dem Upgrade

Nach dem Upgrade auf XenMobile 10.12 (on-premises):

Wenn Funktionen, die ausgehende Verbindungen nutzen, nicht mehr funktionieren und Sie die Verbindungskonfiguration nicht geändert haben, überprüfen Sie das XenMobile Server-Protokoll auf Fehlermeldungen wie etwa “Unable to connect to the VPP Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer.”

Ein Fehler bei der Zertifikatvalidierung bedeutet, dass Sie die Hostnamenüberprüfung unter XenMobile Server deaktivieren müssen. In der Standardeinstellung ist die Hostnamenüberprüfung für ausgehende Verbindungen mit Ausnahme des Microsoft PKI-Servers aktiviert. Wenn die Hostnamenüberprüfung Fehler in der Bereitstellung verursacht, ändern Sie die Servereigenschaft `disable.hostname.verification` in **`true`**. Der Standardwert dieser Eigenschaft ist **`false`**.

Zusätzliche Unterstützung für iOS 13

XenMobile Server unterstützt Geräte, die auf iOS 13 aktualisiert wurden. Das Upgrade hat folgende Auswirkungen für Ihre Benutzer:

- Während der Registrierung werden im iOS-Setupassistant einige neue Optionsfenster angezeigt. Apple hat den iOS-Setupassistant für iOS 13 um neue Optionsfenster erweitert. Die neuen Optionen sind auf der Seite **Einstellungen > Apple Device Enrollment Program (DEP)** in dieser Version enthalten. Sie können diese Bildschirme in XenMobile Server überspringen. Die Seiten werden Benutzern auf iOS 13-Geräten angezeigt.
- Einige Einstellungen der Einschränkungsrichtlinie, die in iOS-Vorgängerversionen auf betreuten oder nicht betreuten Geräten verfügbar waren, sind für iOS 13+ nur auf betreuten Geräten verfügbar. Die aktuellen QuickInfos der XenMobile Server-Konsole zeigen bislang nicht an, dass diese Einstellungen nur für betreute Geräte mit iOS 13+ gelten.
  - Hardwaresteuerelemente zulassen:
    - FaceTime
    - Installieren von Apps
  - Apps zulassen:
    - iTunes Store
    - Safari
    - Safari > automatisch ausfüllen
  - Netzwerk - iCloud-Aktionen zulassen:
    - iCloud-Dokumente & -Daten
  - Einstellungen nur für Betreute Geräte - Zulassen:
    - Game Center > Freunde hinzufügen
    - Game Center > Multiplayerspiele
  - Medieninhalte - Zulassen:
    - Anstößige Musik, Podcasts und iTunes U-Inhalte

Diese Einschränkungen gelten wie folgt:

- Wenn ein Gerät mit iOS 12 (oder niedriger) bei XenMobile Server registriert ist und dann auf iOS 13 aktualisiert wird, gelten die vorherigen Einschränkungen für betreute und nicht betreute Geräte.

- Wenn sich ein nicht betreutes Geräte mit iOS ab Version 13 bei XenMobile Server registriert, gelten die vorherigen Einstellungen nur für betreute Geräte.
- Wenn ein betreutes Gerät mit iOS ab Version 13 sich bei XenMobile Server anmeldet, gelten die vorherigen Einschränkungen nur für betreute Geräte.

Apple Volume Purchase Program-Migration auf Apple Business Manager (ABM) und Apple School Manager (ASM)

Unternehmen und Institutionen, die das Apple Volume Purchase Program (VPP) nutzen, müssen vor dem 1. Dezember 2019 auf Apps und Bücher im Apple Business Manager oder Apple School Manager migrieren.

Lesen Sie vor der Migration von VPP-Konten in XenMobile diesen Apple-Supportartikel.

Wenn Ihre Organisation oder Schule nur das Volume Purchase Program (VPP) verwendet, können Sie sich bei ABM/ASM anmelden und dann bestehende VPP-Käufer zu Ihrem neuen ABM-/ASM-Konto einladen. Navigieren Sie für ASM zu https://school.apple.com. Navigieren Sie für ABM zuhttps://business.apple.com.

Aktualisieren Ihres VPP-Kontos in XenMobile:

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf **iOS-Einstellungen**. Die Konfigurationsseite für das **Programm für Volumenlizenzen** wird angezeigt.
3. Stellen Sie sicher, dass Ihr ABM- oder ASM-Konto dieselbe App-Konfiguration wie Ihr vorheriges VPP-Konto hat.
4. Laden Sie im ABM- oder ASM-Portal einen aktuellen Token herunter.
5. Führen Sie in der XenMobile-Konsole die folgenden Schritte aus:
    a) Bearbeiten Sie das vorhandene Volume Purchase-Konto mit den aktualisierten Tokeninformationen für diesen Standort.
    b) Bearbeiten Sie Ihre ABM- oder ASM-Anmeldeinformationen. Ändern Sie das Suffix nicht.
    c) Klicken Sie zweimal auf **Speichern**.

Weitere Informationen:

- Apple-Bereitstellungsprogramm
- Massenregistrierung von Apple-Geräten

Unterstützung für COPE-Geräte mit Android Enterprise

XenMobile Server unterstützt vollständig verwaltete Android Enterprise-Geräte mit Arbeitsprofil, die früher als COPE-Geräte (Unternehmenseigentum, vom Benutzer verwaltet) bezeichnet wurden. Diese Android Enterprise-Geräte sind vollständig verwaltet und besitzen zusätzlich ein Arbeitsprofil. Sie können separate Richtlinieneinstellungen für Gerät und Arbeitsprofil festlegen. Für diese Version:

- Mit den folgenden Geräterichtlinien können Sie separate Richtlinieneinstellungen für Gerät und Arbeitsprofil festlegen: Anmeldeinformationen, Passcode und Einschränkungen.
- Sie können die Standortmoduseinstellung der Standortrichtlinie auf das COPE-Gerät anwenden, jedoch nicht auf das Arbeitsprofil auf dem COPE-Gerät. Weitere Einstellungen der Standortrichtlinie für Geräte sind für COPE-Geräte nicht verfügbar.
- Sie können die Sicherheitsaktion “Sperren” auf das Gerät oder auf das Arbeitsprofil anwenden.

Geräterichtlinien

Bei vollständig verwalteten Android Enterprise-Geräten mit Arbeitsprofil (COPE-Geräten) können mithilfe von Geräterichtlinien separate Einstellungen auf das gesamte Gerät bzw. das Arbeitsprofil angewendet werden. In der XenMobile Server-Konsole ermöglichen einige Geräterichtlinien das Anwenden dieser separaten Einstellungen. Mit separaten Geräterichtlinien können Sie bei vollständig verwalteten Geräterichtlinien mit Arbeitsprofil Einstellungen nur auf das gesamte Gerät oder auf das Arbeitsprofil anwenden.

Sicherheitsaktionen

Für vollständig verwalteter Android Enterprise-Geräte mit Arbeitsprofil (COPE-Geräte) gilt Folgendes:

- Die Sicherheitsaktion “Sperren” kann separat auf das Gerät oder auf das Arbeitsprofil angewendet werden.
- Alle übrigen Sicherheitsaktionen können auf das Gerät angewendet werden.

Registrierungsprofile steuern Registrierungsoptionen für Android-Geräte

Registrierungsprofile steuern jetzt, wie Android-Geräte registriert werden, wenn Android Enterprise für Ihre XenMobile-Bereitstellung aktiviert ist. Registrierungsprofile legen fest, ob Android-Geräte im Android Enterprise-Standardmodus (vollständig verwaltet oder Arbeitsprofil) oder im Legacymodus (Geräteadministrator) registriert werden.

Standardmäßig registriert das globale Registrierungsprofil neue und werkseitig zurückgesetzte Android Enterprise-Geräte als vollständig verwaltete Geräte und registriert BYOD Android Enterprise-Geräte als Arbeitsprofilgeräte. Weitere Informationen finden Sie unter Android Enterprise.

Vorbereiten von Android-Legacygeräten für Android Enterprise als Standardregistrierung

In naher Zukunft wird der Geräteadministratormodus der Geräteverwaltung von Google nicht mehr unterstützt. Kunden wird daher empfohlen, alle Android-Geräte im Gerätebesitzermodus oder Profilbesitzermodus zu verwalten. (Weitere Informationen finden Sie unter Geräteadministrator – Einstellung der Unterstützung in den Entwicklerhandbüchern von Google Android Enterprise.) Android Enterprise ist jetzt Standardregistrierungsoption für Android-Geräte.

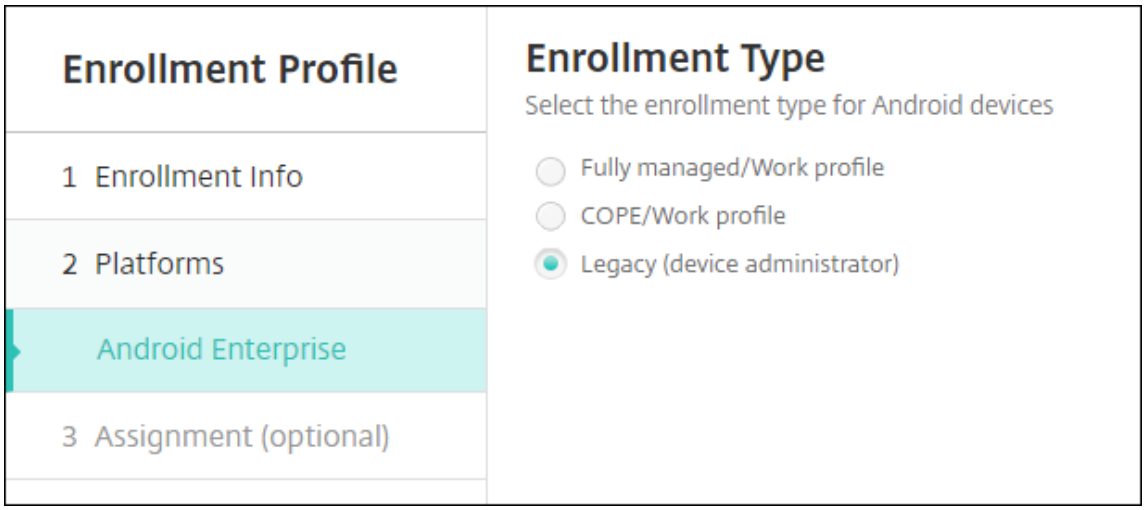
Diese Änderung bedeutet, dass alle neu oder erneut registrierten Android-Geräte als Android Enterprise-Geräte registriert werden, wenn Android Enterprise für Ihre XenMobile-Bereitstellung aktiviert ist.

Als Vorbereitung auf diese Änderung ermöglicht XenMobile jetzt das Erstellen von Registrierungsprofilen, die steuern, wie Android-Geräte registriert werden.

Ihre Organisation ist möglicherweise nicht bereit, mit der Verwaltung von Android-Legacygeräten im Gerätebesitzer- oder Profilbesitzermodus zu beginnen. In diesem Fall können Sie sie weiterhin im Geräteadministratormodus verwalten. Erstellen Sie ein Registrierungsprofil für Legacygeräte und registrieren Sie alle registrierten Legacygeräte neu.

Erstellen eines Registrierungsprofils für Legacygeräte:

1. Gehen Sie in der XenMobile-Konsole zu **Konfigurieren > Registrierungsprofile**.
2. Wenn Sie ein Registrierungsprofil hinzufügen möchten, klicken Sie auf **Hinzufügen**. Geben Sie auf der Seite “Registrierungsinfo” einen Namen für das Registrierungsprofil ein.
3. Klicken Sie auf **Weiter** oder wählen Sie **Android Enterprise** unter **Plattformen**. Die Seite “Registrierungskonfiguration” wird angezeigt.
4. Legen Sie **Verwaltung** auf **Legacygeräteverwaltung** fest. Klicken Sie auf **Weiter** oder wählen Sie **Zuordnung (optional)**. Der Bildschirm für die Bereitstellungsgruppenzuweisung wird angezeigt.



5. Wählen Sie die Bereitstellungsgruppe(n) mit den Administratoren, die dedizierte Geräte registrieren sollen. Klicken Sie auf **Speichern**.

Um das Legacygerät weiterhin im Geräteadministratormodus zu verwalten, registrieren Sie es mit diesem Profil oder registrieren Sie es neu. Sie registrieren Geräteadministratorgeräte ähnlich wie Arbeitsprofilgeräte, indem Benutzer Secure Hub herunterladen und eine Registrierungsserver-URL angeben.

Weitere Informationen zur Unterstützung von Endpoint Management für den Übergang zu Android Enterprise finden Sie im Blog Android Enterprise as default for Citrix Endpoint Management service.

Vereinfachte App-Verwaltung für Android Enterprise

Sie müssen nicht mehr zum verwalteten Google Play-Store oder zum Google Developer-Portal gehen, um Apps für XenMobile Server zu genehmigen oder zu veröffentlichen. Daher dauert die Genehmigung und Veröffentlichung von Apps etwa 10 Minuten statt Stunden.

Genehmigen von Android Enterprise-Apps für den öffentlichen App-Store in der XenMobile Server-Konsole. Sie können nun Apps für den verwalteten Google Play-Store genehmigen, ohne die XenMobile Server-Konsole zu verlassen. Wenn Sie einen App-Namen in das Suchfeld eingeben, werden im verwalteten Google Play Store Anweisungen zum Genehmigen und Speichern der App angezeigt. Ihre App wird dann in den Ergebnissen angezeigt, sodass Sie zugehörige Details konfigurieren können. Siehe Hinzufügen von Apps aus einem öffentlichen App-Store.

Hinzufügen von MDX-Apps für Android Enterprise. Die XenMobile Server-Konsole unterstützt jetzt Android Enterprise als Plattform für die Bereitstellung von MDX-Apps. Weitere Informationen finden Sie unter Hinzufügen von MDX-Apps.

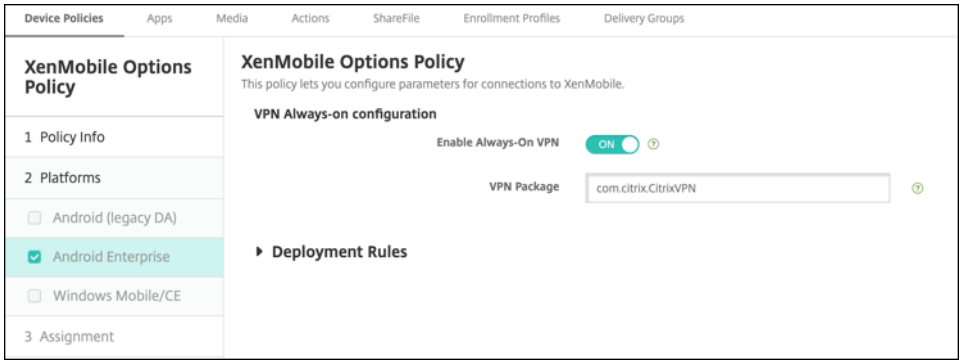
Genehmigen von MDX-Apps für Android Enterprise in der XenMobile Server-Konsole. Sie können nun Apps für den verwalteten Google Play-Store für Android Enterprise genehmigen, ohne die XenMobile Server-Konsole zu verlassen. Nachdem Sie eine MDX-Datei hochgeladen haben, werden im verwalteten Google Play-Store Anweisungen zum Genehmigen und Speichern der App angezeigt. Siehe Hinzufügen von MDX-Apps.

Unterstützung für Always-On-VPN für Android Enterprise

Mit der XenMobile Server-Optionsrichtlinie für Geräte können Sie nun Always-On-VPN für Android Enterprise aktivieren.

Wenn Sie VPN-Profile für Android Enterprise konfigurieren, geben Sie unter **VPN-Standardprofil** den Namen des VPN-Profils ein. XenMobile nutzt dieses Profil, wenn Benutzer in der Benutzeroberfläche der Citrix SSO-App nicht auf ein bestimmtes Profil, sondern auf die Verbindungsoption tippen. Wenn dieses Feld leer gelassen wird, wird das Hauptprofil für die Verbindung verwendet. Wenn nur ein Profil

konfiguriert ist, wird es als Standardprofil markiert. Für Always-On-VPN muss dieses Feld auf den Namen des VPN-Profils gesetzt werden, das für das Always-On-VPN verwendet werden soll.



Konfigurieren der Produktschiene für Android Enterprise-Apps

Wenn Sie eine App aus dem öffentlichen App-Store oder eine MDX-App für Android Enterprise hinzufügen, können Sie festlegen, welche Produktversion Sie auf Benutzergeräte übertragen möchten. Wenn Sie beispielsweise ein spezielles Testprodukt haben, können Sie es auswählen und einer bestimmten Bereitstellungsgruppe zuweisen. Weitere Informationen zum Rollout Ihrer Version finden Sie im Google Play Help Center. Informationen zum Konfigurieren der Produktschiene finden Sie unter Hinzufügen von MDX-Apps oder Hinzufügen von Apps aus einem öffentlichen App-Store.

Erzwingen einer Passcodezurücksetzung für macOS-Benutzer

Wenn ein macOS-Gerät ein Konfigurationsprofil mit Passcoderichtlinie empfängt, müssen Benutzer einen Passcode eingeben, der die Richtlinieneinstellungen erfüllt. Eine Passcodezurücksetzung kann nun von Ihnen erzwungen werden, wenn ein Benutzer sich das nächste Mal authentifiziert. Aktivieren Sie in der Passcoderichtlinie für macOS (10.13 und höher) die neue Einstellung **Passcodezurücksetzung erzwingen**. Weitere Informationen über die Richtlinie finden Sie unter Passcoderichtlinien für Geräte.

Neue Features in XenMobile Server 10.11

January 6, 2022

XenMobile Server 10.11 (PDF-Download)

XenMobile Migration Service

Wenn Sie die On-Premises-Version von XenMobile Server verwenden, hilft Ihnen unser kostenloser XenMobile Migration Service beim Start in Endpoint Management. Die Migration von XenMobile Server

zu Citrix Endpoint Management erfordert keine erneute Registrierung von Geräten.

Wenden Sie sich an Ihren lokalen Citrix Vertriebsmitarbeiter oder Citrix Partner, um die Migration zu starten. Weitere Informationen finden Sie unter XenMobile Migration Service.

Apple Volume Purchase Program-Migration auf Apple Business Manager (ABM) und Apple School Manager (ASM)

Unternehmen und Institutionen, die das Apple Volume Purchase Program (VPP) nutzen, müssen vor dem 1. Dezember 2019 auf Apps und Bücher im Apple Business Manager oder Apple School Manager migrieren.

Lesen Sie vor der Migration von VPP-Konten in XenMobile diesen Apple-Supportartikel.

Wenn Ihre Organisation oder Schule nur das Volume Purchase Program (VPP) verwendet, können Sie sich bei ABM/ASM anmelden und dann bestehende VPP-Käufer zu Ihrem neuen ABM-/ASM-Konto einladen. Navigieren Sie für ASM zu https://school.apple.com. Navigieren Sie für ABM zuhttps://business.apple.com.

Aktualisieren Ihres Volume Purchase-Kontos (früher VPP-Konto) in XenMobile:

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf **Volume Purchase**. Die Konfigurationsseite **Volume Purchase** wird angezeigt.
3. Stellen Sie sicher, dass Ihr ABM- oder ASM-Konto dieselbe App-Konfiguration wie Ihr vorheriges VPP-Konto hat.
4. Laden Sie im ABM- oder ASM-Portal einen aktuellen Token herunter.
5. Führen Sie in der XenMobile-Konsole die folgenden Schritte aus:
    a) Bearbeiten Sie das vorhandene Volume Purchase-Konto mit den aktualisierten Tokeninformationen für diesen Standort.
    b) Bearbeiten Sie Ihre ABM- oder ASM-Anmeldeinformationen. Ändern Sie das Suffix nicht.
    c) Klicken Sie zweimal auf **Speichern**.

Zusätzliche Unterstützung für iOS 13

> **Wichtig:**
>
> Vorbereitung von Geräteupgrades auf iOS 12+: Der Verbindungstyp “Citrix VPN” in der VPN-Geräterichtlinie für iOS unterstützt iOS 12+ nicht. Löschen Sie Ihre VPN-Geräterichtlinie und erstellen Sie eine neue mit dem Verbindungstyp “Citrix SSO”.
>
> Die Citrix VPN-Verbindung funktioniert bei zuvor bereitgestellten Geräten nach dem Löschen der

> VPN-Geräterichtlinie weiterhin. Die neue Konfiguration der VPN-Geräterichtlinie wird bei der Benutzerregistrierung in XenMobile Server 10.11 wirksam.

XenMobile Server unterstützt Geräte, die auf iOS 13 aktualisiert wurden. Das Upgrade hat folgende Auswirkungen für Ihre Benutzer:

- Während der Registrierung werden im iOS-Setupassistant einige neue Optionsfenster angezeigt. Apple hat den iOS-Setupassistant für iOS 13 um neue Optionsfenster erweitert. Die neuen Optionen sind nicht auf der Seite **Einstellungen > Apple Device Enrollment Program (DEP)** in dieser Version enthalten. Daher können Sie diese Bildschirme in XenMobile Server nicht überspringen. Die Seiten werden Benutzern auf iOS 13-Geräten angezeigt.
- Einige Einstellungen der Einschränkungsrichtlinie, die in iOS-Vorgängerversionen auf betreuten oder nicht betreuten Geräten verfügbar waren, sind für iOS 13+ nur auf betreuten Geräten verfügbar. Die aktuellen QuickInfos der XenMobile Server-Konsole zeigen bislang nicht an, dass diese Einstellungen nur für betreute Geräte mit iOS 13+ gelten.
  - Hardwaresteuerelemente zulassen:
    - FaceTime
    - Installieren von Apps
  - Apps zulassen:
    - iTunes Store
    - Safari
    - Safari > automatisch ausfüllen
  - Netzwerk - iCloud-Aktionen zulassen:
    - iCloud-Dokumente & -Daten
  - Einstellungen nur für Betreute Geräte - Zulassen:
    - Game Center > Freunde hinzufügen
    - Game Center > Multiplayerspiele
  - Medieninhalte - Zulassen:
    - Anstößige Musik, Podcasts und iTunes U-Inhalte

Diese Einschränkungen gelten wie folgt:

- Wenn ein Gerät mit iOS 12 (oder niedriger) bei XenMobile Server registriert ist und dann auf iOS 13 aktualisiert wird, gelten die vorherigen Einschränkungen für betreute und nicht betreute Geräte.
- Wenn sich ein nicht betreutes Geräte mit iOS ab Version 13 bei XenMobile Server registriert, gelten die vorherigen Einstellungen nur für betreute Geräte.
- Wenn ein betreutes Gerät mit iOS ab Version 13 sich bei XenMobile Server anmeldet, gelten die vorherigen Einschränkungen nur für betreute Geräte.

Anforderungen für vertrauenswürdige Zertifikate in iOS 13 und macOS 15

Apple hat neue Anforderungen für TLS-Serverzertifikate. Stellen Sie sicher, dass alle Zertifikate den neuen Apple-Anforderungen entsprechen. Siehe Apple-Veröffentlichung https://support.apple.com/en-us/HT210176. Hilfe zum Verwalten von Zertifikaten finden Sie unter Hochladen von Zertifikaten in XenMobile.

Upgrade von GCM auf FCM

Seit dem 10. April 2018 ist Google Cloud Messaging (GCM) veraltet. Google hat den GCM-Server und die Client-APIs am 29. Mai 2019 entfernt.

> **Wichtige Anforderungen:**
>
> - Führen Sie ein Upgrade auf die aktuelle Version von XenMobile Server durch.
> - Führen Sie ein Upgrade auf die aktuelle Version von Secure Hub durch.

Google empfiehlt, sofort ein Upgrade auf Firebase Cloud Messaging (FCM) durchzuführen, um die neuen Funktionen von FCM zu nutzen. Informationen von Google finden Sie unter https://developers.google.com/cloud-messaging/faq und https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html.

Um weiterhin Pushbenachrichtigungen an Ihre Android-Geräte zu unterstützen: Wenn Sie GCM mit XenMobile Server verwenden, migrieren Sie zu FCM. Aktualisieren Sie dann XenMobile Server mit dem neuen FCM-Schlüssel, den Sie in der Firebase Cloud Messaging Console finden.

Die folgenden Schritte zeigen den Registrierungsworkflow bei Verwendung vertrauenswürdiger Zertifikate.

Upgradeschritte:

1. Folgen Sie für das Upgrade von GCM auf FCM den Informationen von Google.
2. Kopieren Sie in der Firebase Cloud Messaging Console Ihren neuen FCM-Schlüssel. Sie brauchen ihn für den nächsten Schritt.
3. Gehen Sie in der XenMobile Server-Konsole zu **Einstellungen > Firebase Cloud Messaging** und konfigurieren Sie Ihre Einstellungen.

Geräte wechseln zu FCM, wenn sie das nächste Mal bei XenMobile Server einchecken und eine Richtlinienaktualisierung durchführen. Aktualisieren der Richtlinien in Secure Hub erzwingen: Gehen Sie in Secure Hub zu **Einstellungen > Geräteinformationen** und tippen Sie auf **Richtlinie aktualisieren**. Weitere Informationen zum Konfigurieren von FCM finden Sie unter Firebase Cloud Messaging.

XenMobile Migration Service

Wenn Sie die On-Premises-Version von XenMobile Server verwenden, hilft Ihnen unser XenMobile Migration Service beim Start in Endpoint Management. Die Migration von XenMobile Server zu Citrix

Endpoint Management erfordert keine erneute Registrierung von Geräten.

Weitere Informationen erhalten Sie bei Ihrem lokalen Citrix Vertriebsmitarbeiter, Systems Engineer oder Citrix Partner. In diesen Blogs wird der XenMobile Migration Service erläutert:

New XenMobile Migration Service

Making the Case for XenMobile in the Cloud

Vor dem Upgrade auf XenMobile 10.11 (on-premises)

Einige Systemanforderungen haben sich geändert. Weitere Informationen finden Sie unter Systemanforderungen und Kompatibilität sowie XenMobile-Kompatibilität.

1. Aktualisieren Sie den Citrix Lizenzserver auf 11.15.x oder höher, bevor Sie die aktuelle Version von XenMobile Server 10.11 installieren.

   Die neueste Version von XenMobile erfordert Citrix License Server 11.15 (Mindestversion).

   > **Hinweis:**
   >
   > Wenn Sie Ihre eigene Lizenz für die Preview verwenden möchten, berücksichtigen Sie, dass das Customer Success Services-Datum (bisher "Subscription Advantage"-Datum) in XenMobile 10.11 der 9. April 2019 ist. Das Customer Success Services-Datum der Citrix Lizenz muss nach diesem Datum liegen.
   >
   > Das Datum wird neben der Lizenz auf dem Lizenzserver angezeigt. Wenn Sie die aktuelle Version von XenMobile mit einer älteren Lizenzserverumgebung verbinden, schlägt die Konnektivitätsprüfung fehl und der Lizenzserver kann nicht konfiguriert werden.

   Zum Verlängern des Datums für Ihre Lizenz laden Sie die aktuelle Lizenzdatei vom Citrix Portal herunter und laden Sie sie in den Lizenzserver hoch. Weitere Informationen finden Sie unter Customer Success Services.

2. Clusterumgebungen: Für die Bereitstellung von iOS-Richtlinien und -Apps auf Geräten mit iOS 11 oder später gilt folgende Anforderung. Ist Citrix Gateway für SSL-Persistenz konfiguriert, müssen Sie auf allen XenMobile Server-Knoten Port 80 öffnen.
3. Wenn die virtuelle Maschine, auf der die zu aktualisierende XenMobile Server-Instanz ausgeführt wird, weniger als 4 GB RAM hat, erhöhen Sie den RAM auf mindestens 4 GB. Beachten Sie, dass der empfohlene Mindest-RAM für Produktionsumgebungen bei 8 GB liegt.
4. Empfehlung: Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine zum Erstellen eines Systemsnapshots. Sichern Sie außerdem die Konfigurationsdatenbank des Systems. Sollten bei einem Upgrade Probleme auftreten, können Sie mit vollständigen Backups eine Wiederherstellung vornehmen.

Ausführen des Upgrades

Sie können ein direktes Upgrade auf XenMobile 10.11 von XenMobile 10.10.x oder 10.9.x ausführen. Um das Upgrade durchzuführen, laden Sie die neueste verfügbare Binärdatei herunter: https://www.citrix.com/downloads. Navigieren Sie zu **Citrix Endpoint Management (und Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**. Klicken Sie auf der Kachel der XenMobile Server-Software für Ihren Hypervisor auf **Datei herunterladen**.

Verwenden Sie zum Hochladen des Upgrades die Seite **Releasemanagement** der XenMobile-Konsole. Weitere Informationen finden Sie unter Upgrade über die Seite "Releasemanagement".

Nach dem Upgrade

Nach dem Upgrade auf XenMobile 10.11 (on-premises):

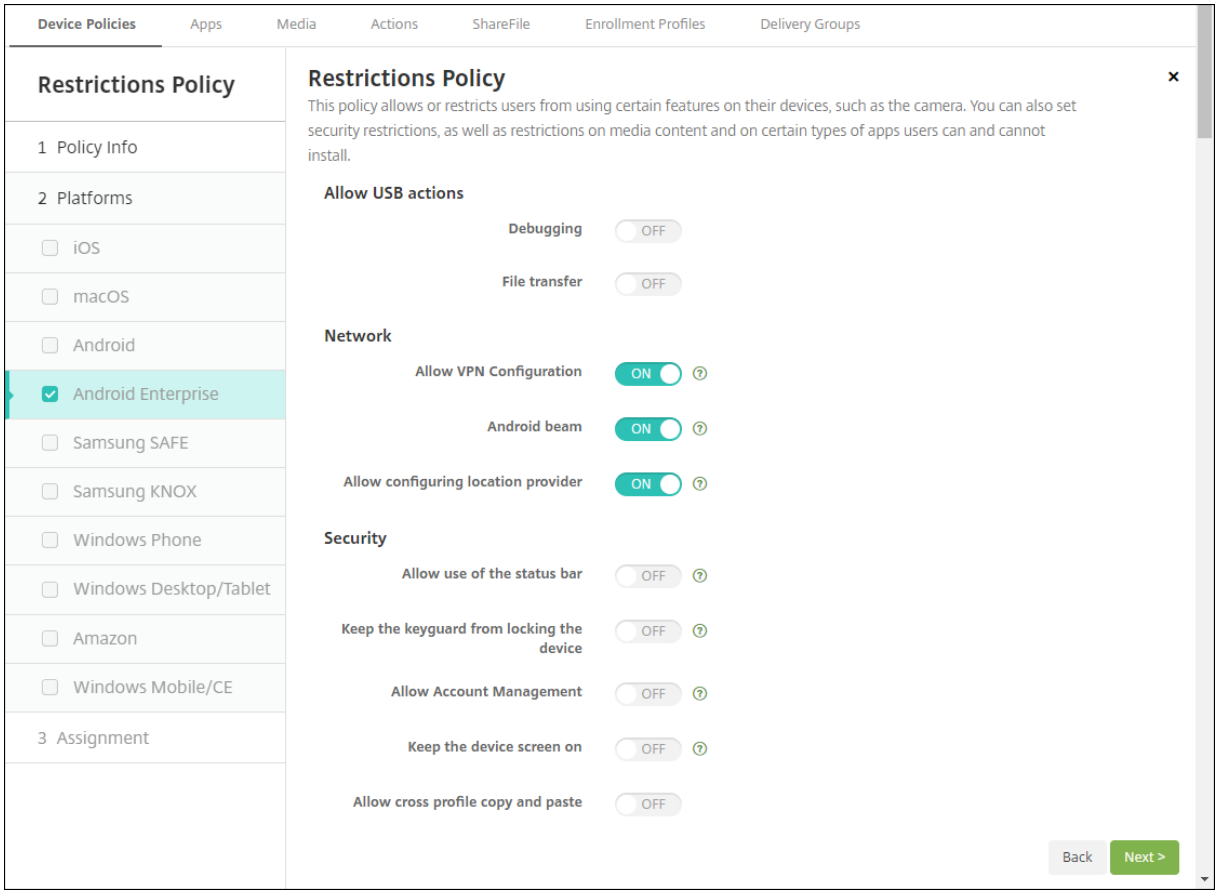
Wenn Funktionen, für die ausgehende Verbindungen eingesetzt werden, nicht mehr funktionieren und Sie die Verbindungskonfiguration nicht geändert haben, überprüfen Sie das XenMobile Server-Protokoll auf Fehlermeldungen wie etwa "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer."

Ein Fehler bei der Zertifikatvalidierung bedeutet, dass Sie die Hostnamenüberprüfung unter XenMobile Server deaktivieren müssen. In der Standardeinstellung ist die Hostnamenüberprüfung für ausgehende Verbindungen mit Ausnahme des Microsoft PKI-Servers aktiviert. Wenn die Hostnamenüberprüfung Fehler in der Bereitstellung verursacht, ändern Sie die Servereigenschaft `disable.hostname.verification` in **`true`**. Der Standardwert dieser Eigenschaft ist **`false`**.

Neue und aktualisierte Geräterichtlinieneinstellungen für Android Enterprise-Geräte

Vereinheitlichte Richtlinien für Samsung Knox und Android Enterprise. Für Android Enterprise-Geräte auf Samsung Knox 3.0 oder höher und Android 8.0 oder höher: Knox und Android Enterprise werden in einer einheitlichen Geräte- und Profilverwaltungslösung zusammengefasst.
Konfigurieren Sie Knox-Einstellungen auf der Android Enterprise-Seite der folgenden Geräterichtlinien:

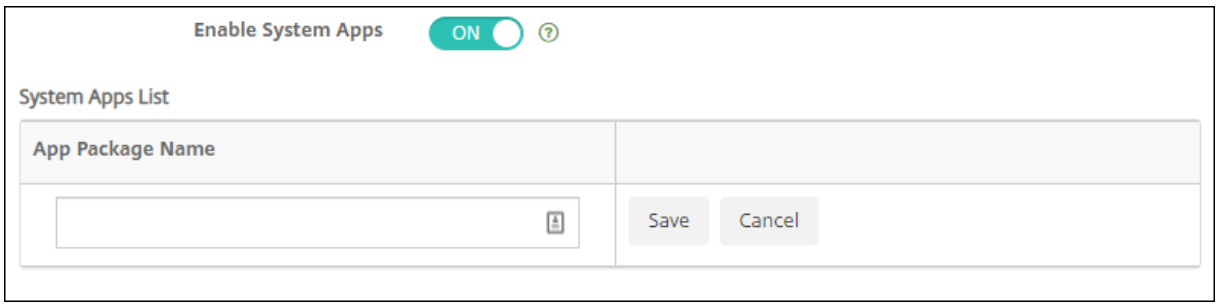
- **Geräterichtlinie für OS-Updates.** Enthält Einstellungen für Samsung Enterprise-FOTA-Updates.
- **Passcode-Geräterichtlinie.**
- **Geräterichtlinie für Samsung MDM-Lizenzschlüssel.** Konfiguriert den Knox-Lizenzschlüssel.
- **Einstellungen der Einschränkungsrichtlinie.**



App-Bestandsrichtlinie für Android Enterprise. Sie können jetzt einen Bestand der Android Enterprise-Apps auf verwalteten Geräten abrufen. Siehe App-Bestandsrichtlinie für Geräte.

Greifen Sie auf alle Google Play-Apps im verwalteten Google Play Store zu. Mit der Servereigenschaft für Zugriff auf alle Apps im **verwalteten Google Play Store** werden alle Apps aus dem öffentlichen Google Play Store vom verwalteten Google Play Store aus zugänglich gemacht. Wenn Sie diese Eigenschaft auf **Wahr** setzen, werden die Apps aus dem öffentlichen Google Play Store für alle Android Enterprise-Benutzer zugelassen. Mit der Geräteeinschränkungsrichtlinie können Administratoren dann den Zugriff auf diese Apps steuern.

Aktivieren von System-Apps auf Android Enterprise-Geräten. Damit Benutzer vorinstallierte System-Apps im Android Enterprise-Arbeitsprofilmodus oder vollständig verwalteten Modus ausführen können, konfigurieren Sie die Geräteeinschränkungsrichtlinie. Diese Konfiguration gewährt dem Benutzer Zugriff auf Standardgeräte-Apps wie Kamera, Galerie und andere. Um den Zugriff auf eine bestimmte App zu beschränken, legen Sie App-Berechtigungen mit der Geräterichtlinie App-Berechtigungen für Android Enterprise fest.



Unterstützung für dedizierte Geräte mit Android Enterprise XenMobile unterstützt jetzt die Verwaltung dedizierter Geräte (bisher “COSU”-Geräte).

Dedizierte Android Enterprise-Geräte sind vollständig verwaltete Einzweckgeräte. Diese Geräte beschränken Sie auf eine oder wenige Apps, die zum Ausführen der für den vorgegebenen Zweck erforderlichen Aufgaben notwendig sind. Außerdem verhindern Sie, dass Benutzer weitere Apps aktivieren oder andere Aktionen auf dem Gerät ausführen.

Informationen zur Bereitstellung von Android Enterprise-Geräten finden Sie unter Provisioning von dedizierten Android Enterprise-Geräten.

Richtlinie umbenannt. Die Android Enterprise App-Einschränkungsrichtlinie wurde entsprechend geänderter Google-Terminologie in “verwaltete Android Enterprise-Konfigurationen” umbenannt. Siehe Geräterichtlinie für verwaltete Android Enterprise-Konfigurationen.

Sperren und Kennwort zurücksetzen für Android Enterprise

XenMobile unterstützt jetzt die Sicherheitsaktion “Sperren und Kennwort zurücksetzen” für Android Enterprise-Geräte. Die Geräte müssen im Arbeitsprofilmodus registriert sein und Android 8.0 oder höher ausführen.

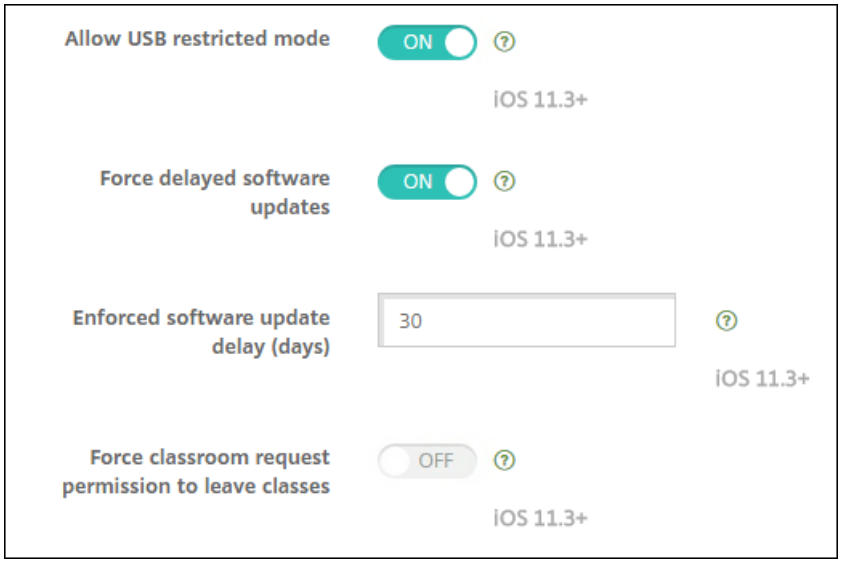
- Der gesendete Passcode sperrt das Arbeitsprofil. Das Gerät ist nicht gesperrt.
- Wird kein Passcode gesendet oder der gesendete Code erfüllt nicht die Passcode-Anforderungen:
  - Und es ist noch kein Passcode im Arbeitsprofil festgelegt, wird das Gerät gesperrt.
  - Und es ist bereits ein Passcode im Arbeitsprofil festgelegt, wird das Arbeitsprofil gesperrt, nicht aber das Gerät.

Weitere Informationen zu den Sicherheitsaktionen für “Sperren und Kennwort zurücksetzen” finden Sie unter Sicherheitsaktionen.

Neue Richtlinieneinstellungen zu Geräteeinschränkungen für iOS oder macOS

- **Nicht verwaltete Apps lesen verwaltete Kontakte:** Optional. Nur verfügbar, wenn **Dokumente von verwalteten Apps in nicht verwalteten Apps** deaktiviert ist. Wenn diese Richtlinie aktiviert ist, können nicht verwaltete Apps Daten aus den Kontakten verwalteter Konten lesen. Die Standardeinstellung ist **Aus**. Verfügbar ab iOS 12.

- **Verwaltete Apps schreiben nicht verwaltete Kontakte:** Optional. Wenn diese Option aktiviert ist, dürfen verwaltete Apps Kontakte in Kontakte nicht verwalteter Konten schreiben. Wenn **Dokumente von verwalteten Apps in nicht verwalteten Apps** aktiviert ist, hat diese Einschränkung keine Auswirkungen. Die Standardeinstellung ist **Aus**. Verfügbar ab iOS 12.
- **Kennwörter autom. ausfüllen:** Optional. Wenn diese Option deaktiviert ist, können Benutzer die Funktionen zum automatischen Ausfüllen von Kennwörtern oder zum automatischen Erstellen starker Kennwörter nicht verwenden. Die Standardeinstellung ist **Ein**. Verfügbar ab iOS 12 und macOS 10.14.
- **Kennwortanforderung bei Geräten in der Nähe:** Optional. Wenn die Option deaktiviert ist, fordern Benutzergeräte keine Kennwörter von Geräten in der Nähe an. Die Standardeinstellung ist **Ein**. Verfügbar ab iOS 12 und macOS 10.14.
- **Kennwort teilen:** Optional. Wenn diese Option deaktiviert ist, können Benutzer ihre Kennwörter nicht per AirDrop teilen. Die Standardeinstellung ist **Ein**. Verfügbar ab iOS 12 und macOS 10.14.
- **Automatisches Datum und Uhrzeit erzwingen:** betreut. Wenn diese Option aktiviert ist, können die Benutzer die Option **Allgemein > Datum & Uhrzeit > Automatisch einstellen** nicht deaktivieren. Die Standardeinstellung ist **Aus**. Verfügbar ab iOS 12.
- **Eingeschränkten USB-Modus zulassen:** nur für betreute Geräte verfügbar. Mit “Ein” kann das Gerät immer mit USB-Zubehör verbunden werden, solange es gesperrt ist. Die Standardeinstellung ist **Ein**. Verfügbar ab iOS 11.3.
- **Verzögerte Softwareupdates erzwingen:** nur für betreute Geräte verfügbar. Wenn diese Option auf **Ein** gesetzt, wird die Sichtbarkeit von Softwareupdates für die Benutzer verzögert. Der Benutzer sieht ein Softwareupdate erst, nachdem die festgelegte Anzahl von Tagen seit Veröffentlichung des Softwareupdates verstrichen ist. Die Standardeinstellung ist **Aus**. Verfügbar ab iOS 11.3 und macOS 10.13.4.
- **Erzwungene Verzögerung für Softwareupdate (Tage):** nur für betreute Geräte verfügbar. Diese Einschränkung ermöglicht es dem Administrator festzulegen, für wie lange das Softwareupdate auf dem Gerät verzögert wird. Der Maximalwert beträgt 90 Tage und der Standardwert ist **30**. Verfügbar ab iOS 11.3 und macOS 10.13.4.
- **Um Erlaubnis zum Verlassen von Klassen fragen:** nur für betreute Geräte verfügbar. Mit **Ein** müssen Teilnehmer, die in einem nicht verwalteten Kurs mit Classroom registriert sind, zum Verlassen des Kurses eine Genehmigung von der Lehrkraft anfordern. Die Standardeinstellung ist **Aus**. Verfügbar ab iOS 11.3.



Weitere Informationen finden Sie unter Geräteeinschränkungsrichtlinie.

Aktualisierung der Exchange-Geräterichtlinie für iOS bzw. macOS

Zusätzliche S/MIME-Exchange-Signatur- und Verschlüsselungseinstellungen ab iOS 12. Die Exchange-Geräterichtlinie enthält jetzt Einstellungen zum Konfigurieren von S/MIME-Signatur und -verschlüsselung.

S/MIME-Signatur:

- **Anmeldeinformationen für Signieridentität:** Wählen Sie die Anmeldeinformationen für die Signatur aus.
- **S/MIME-Signatur von Benutzer überschreibbar:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Signierung in Einstellungen des Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**.
- **UUID für S/MIME-Signaturzertifikat von Benutzer überschreibbar:** Mit **Ein** können Benutzer in den Einstellungen ihrer Geräte wählen, welche Anmeldeinformationen für die Signatur verwendet werden. Die Standardeinstellung ist **Aus**.

S/MIME-Verschlüsselung:

- **Anmeldeinformationen für Verschlüsselungsidentität:** Wählen Sie die Anmeldeinformationen für die Verschlüsselung aus.
- **S/MIME-Option für einzelne Nachrichten aktivieren:** Mit **Ein** wird Benutzern für jede Nachricht, die sie erstellen, eine Option zum Aktivieren oder Deaktivieren der S/MIME-Verschlüsselung angezeigt. Die Standardeinstellung ist **Aus**.
- **Standardmäßige S/MIME-Verschlüsselung von Benutzer überschreibbar:** Mit **Ein** können Benutzer in den Einstellungen ihrer Geräte auswählen, ob S/MIME standardmäßig aktiviert ist. Die Standardeinstellung ist **Aus**.

- **UUID für S/MIME-Verschlüsselungszertifikat von Benutzer überschreibbar:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Verschlüsselungsidentität und Verschlüsselung in den Einstellungen des Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**.

Exchange-OAuth-Einstellungen ab iOS 12. Sie können die Verbindung mit Exchange so konfigurieren, dass OAuth für die Authentifizierung verwendet wird.

Exchange OAuth-Einstellungen ab macOS 10.14. Sie können die Verbindung mit Exchange so konfigurieren, dass OAuth für die Authentifizierung verwendet wird. Für die OAuth-Authentifizierung können Sie die Anmelde-URL für Umgebungen ohne automatische Erkennung angeben.

Siehe Exchange-Geräterichtlinie.

Aktualisierung der E-Mail-Geräterichtlinie für iOS

Zusätzliche S/MIME-Exchange-Signatur- und Verschlüsselungseinstellungen ab iOS 12. Die E-Mail-Geräterichtlinie enthält Einstellungen zum Konfigurieren von S/MIME-Signatur und -verschlüsselung.

S/MIME-Signatur:

- **S/MIME-Signatur aktivieren:** Wählen Sie, ob dieses Konto S/MIME-Signaturen unterstützt. Die Standardeinstellung ist **Ein**. Wenn Sie **Ein** wählen, werden folgende Felder eingeblendet.
  - **S/MIME-Signatur von Benutzer überschreibbar:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Signierung in Einstellungen des Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
  - **UUID für S/MIME-Signaturzertifikat von Benutzer überschreibbar:** Mit **Ein** können Benutzer in den Einstellungen ihrer Geräte wählen, welche Anmeldeinformationen für die Signatur verwendet werden. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.

S/MIME-Verschlüsselung:

- **S/MIME-Verschlüsselung aktivieren:** Wählen Sie, ob dieses Konto S/MIME-Verschlüsselung unterstützt. Die Standardeinstellung ist **Aus**. Wenn Sie **Ein** wählen, werden folgende Felder eingeblendet.
  - **S/MIME-Option für einzelne Nachrichten aktivieren:** Mit **Ein** wird Benutzern für jede Nachricht, die sie erstellen, eine Option zum Aktivieren oder Deaktivieren der S/MIME-Verschlüsselung angezeigt. Die Standardeinstellung ist **Aus**.
  - **Standardmäßige S/MIME-Verschlüsselung von Benutzer überschreibbar:** Mit **Ein** können Benutzer in den Einstellungen ihrer Geräte auswählen, ob S/MIME standardmäßig aktiviert ist. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
  - **UUID für S/MIME-Verschlüsselungszertifikat von Benutzer überschreibbar:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Verschlüsselungsidentität und Verschlüsselung

in den Einstellungen des Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.

Siehe E-Mail-Geräterichtlinie.

Geräterichtlinie für App-Benachrichtigungen für iOS

Für die Geräterichtlinie für App-Benachrichtigungen sind die folgenden Einstellungen ab iOS 12 verfügbar.

- **In CarPlay anzeigen:** Wählen Sie **Ein**, damit Benachrichtigungen in Apple CarPlay angezeigt werden. Die Standardeinstellung ist **Ein**.
- **Kritische Warnung aktivieren:** Bei der Einstellung **Ein** kann eine App eine Benachrichtigung als kritische Benachrichtigung markieren, die die Einstellungen für "Nicht stören" und "Klingel" ignoriert. Die Standardeinstellung ist **Aus**.

Siehe Geräterichtlinie für App-Benachrichtigungen.

Unterstützung für geteilte iPads mit Apple Education

Die XenMobile-Integration mit Apple Education unterstützt jetzt geteilte iPads. Mehrere Schüler in einem Klassenzimmer können ein iPad für verschiedene Fächer teilen, die von einem oder mehreren Lehrern unterrichtet werden.

Sie oder die Lehrkräfte registrieren geteilte iPads und stellen dann Geräterichtlinien, Apps und Medien auf den Geräten bereit. Die Teilnehmer geben dann ihre Apple ID-Anmeldeinformationen an, um sich bei dem geteilten iPad anzumelden. Wenn Sie zuvor eine Richtlinie "Bildungseinrichtung - Konfiguration" für Lernende bereitgestellt haben, melden diese sich nicht mehr als "Anderer Benutzer" an, um Geräte gemeinsam zu nutzen.

Voraussetzungen für geteilte iPads

- Beliebiges iPad Pro, iPad 5. Generation, iPad Air 2 oder später und iPad mini 4 oder später
- Mindestens 32 GB Speicherplatz
- Betreut

Weitere Informationen finden Sie unter Konfigurieren von geteilten iPads.

Änderung bezüglich RBAC-Berechtigungen

Die RBAC-Berechtigung "Lokale Benutzer hinzufügen/löschen" wird jetzt in zwei Berechtigungen unterteilt: "Lokale Benutzer hinzufügen" und "Lokale Benutzer löschen".

Weitere Informationen finden Sie unter Konfigurieren von Rollen mit RBAC.

Hinweise zu Drittanbietern

January 5, 2022

Dieses Release von XenMobile enthält ggf. Software von Drittanbietern, die gemäß den in den folgenden Dokumenten aufgeführten Bestimmungen lizenziert ist:

XenMobile: Hinweise zu Drittanbietern

Einstellung von Features und Plattformen

January 5, 2022

Die Ankündigungen in diesem Artikel informieren Sie frühzeitig über XenMobile Server-Features, die in Kürze veraltet sind. Dies gibt Ihnen die Möglichkeit, rechtzeitig notwendige Geschäftsentscheidungen zu treffen. Citrix überwacht die Nutzung von Features und Feedback, um den geeigneten Zeitpunkt für eine Außerbetriebnahme zu wählen. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element. Informationen zum Produktlebenszyklus-Support finden Sie unter Supportrichtlinie für Produktlebenszyklen.

Veraltete und entfernte Produkte und Features

In der folgenden Liste werden die XenMobile Server-Features angezeigt, die veraltet sind oder entfernt wurden.

Veraltete Elemente werden nicht sofort entfernt. Citrix bietet für veraltete Elemente weiterhin Support, bis diese in einer zukünftigen Version entfernt werden.

Entfernte Elemente wurden entfernt oder werden in XenMobile Server nicht mehr unterstützt.

Weitere Informationen über mobile Produktivitätsapps am Ende des Lebenszyklus finden Sie unter Ende des Lebenszyklus und veraltete Apps.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Knox Mobile Enrollment (Legacy-Geräteadmin)	Unterstützung für Knox Mobile Enrollment (KME) im Legacy-Geräteadmin-Modus für alle Android-Versionen läuft aus.	4. Mai 2021	Zieltermin: 30. Juni 2021	Verwenden Sie KME für die Registrierung im Android Enterprise-Modus. Android Enterprise wird von Android 8, 9, 10, 11 unterstützt.
Mobile Apps und Workspace-Apps von Citrix für Android 7.x und iOS 12.x	Veraltet: Unterstützung für Secure Hub, Secure Mail, Secure Web und Citrix Workspace-App für Android 7.x und iOS 12.x.	April 2021	Zieltermin: Juni 2021	Verwenden Sie mindestens die aktuelle Version und die Vorversion jeder gängigen Betriebssystem-plattform. Ältere Geräte bleiben registriert. Legacygeräte werden jedoch von Citrix nicht getestet und erhalten keinen technischen Support.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Abgeleitete Anmeldeinformationen	Die Unterstützung für abgeleitete Anmeldeinformationen und die Citrix Derived Credentials Manager-App läuft aus.	25. März 2021	Ziel: 2. Quartal 2021	Unter iOS finden Sie eine Liste der für iOS unterstützten Authentifizierungstypen.
Internet Explorer 11	Die Unterstützung von Internet Explorer für die XenMobile Server-Konsole läuft aus.	Januar 2021	Januar 2021	Verwenden Sie die neueste Version folgender Webbrowser: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Unterstützung für RSA-Softwaretoken in Android	Die Unterstützung für das direkte Importieren von RSA-Softtoken in Secure Hub für Android läuft aus.	Januar 2021	Februar 2021	Sie können den RSA-Softtoken in der RSA Secure ID-App importieren, die in Google Play verfügbar ist. Sie können den Token dann für die Citrix Gateway-Authentifizierung verwenden.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Android - Sony	Die Android-Unterstützung auf Sony-Geräten und in Sony-spezifischen Richtlinien läuft ab.	Januar 2021	Februar 2021	Verwenden Sie Android Enterprise.
Android - HTC	Die Android-Unterstützung auf HTC-Geräten und in HTC-spezifischen Richtlinien läuft ab.	Januar 2021	Februar 2021	Verwenden Sie Android Enterprise.
Drittanbieterkomponente des XenMobile-Dashboards	Wir werden eine Drittanbieterkomponente, die als Teil des XenMobile-Dashboards verwendet wird, als veraltet einstufen.	Dezember 2020	Januar 2021	Um das Dashboard weiterhin zu verwenden, führen Sie ein Upgrade auf XenMobile 10.12 oder höher durch

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Apps, die auf Android Enterprise-Geräten für den Modus “Legacygerätev-erwaltung” veröffentlicht wurden	Für die Plattform “Legacy-Geräteadmin” veröffentlichte Apps werden von Citrix nicht länger auf Geräten bereitgestellt, die in Android Enterprise registriert sind.	Oktober 2020	November 2020	Veröffentlichen Sie Apps auf Android Enterprise-Geräten für die Plattform “Android Enterprise”. Erstellen Sie auf Geräten mit Legacygeräteverwaltung eine separate Bereitstellungsgruppe für Apps, die Sie weiterhin für “Legacy-Geräteadmin” veröffentlichen möchten.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Ports für ausgehende APNs-Benachrichtigungen	Apple stellt die Unterstützung für das Legacy-APNs-Binärprotokoll am 31. März 2021 ein. Apple empfiehlt, stattdessen die Verwendung der HTTP/2-basierten APNS-Anbieter-API zu verwenden. Im Zusammenhang mit dieser Änderung läuft die Unterstützung für Ports 2195 und 2196 aus, die zum Senden von APNs-Benachrichtigungen an `*.push.apple.com` verwendet wurden.	Oktober 2020	Ziel: April 2021	Verwenden Sie stattdessen Port 443 oder 2197. Siehe Öffnen von XenMobile-Ports zum Verwalten von Geräten.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Samsung SEAMS-Container	Unterstützung für den Samsung SEAMS-Container läuft aus.	Juni 2020	August 2020	Verwenden Sie die Samsung Knox Service Plug-In (KSP)-App für Android Enterprise. Siehe Hinzufügen der KSP-App (Knox-Service-Plug-In).
Selbstsignierte SSL-Zertifikate (Secure Sockets Layer)	Die Unterstützung für selbstsignierte SSL-Zertifikate ist für alle Geräteplattformen veraltet.	May 2020		Ersetzen Sie Ihr vorhandenes selbst signiertes Zertifikat durch ein vertrauenswürdiges SSL-Zertifikat einer etablierten Zertifizierungsstelle (ZS).

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Signaturalgorithm für zertifikatbasierte Authentifizierung (Nicht-FIPS und schwache Verschlüsselungsverfahren)	Die Unterstützung für folgende Signaturalgorithmen ist veraltet: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA SHA1withDSA, RIPEMD160withRS RIPEMD128withRS RIPEMD256withRS	May 2020	Januar 2021	Wenn Sie in der XenMobile-Konsole eine Zertifikatsignieranforderung für einen Anmeldeinformationsanbieter erstellen (**Einstellungen > Anmeldeinformationsanbieter > Zertifikatsignieranforderung**), wählen Sie ein stärkeres Verschlüsselungsverfahren.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Datenbankserver	Unterstützung für Microsoft SQL Server 2014 und früher läuft aus.	Oktober 2021	August 2022	Aktualisieren Sie das System auf eine der folgenden unterstützten Versionen: Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13 oder Microsoft SQL Server 2019 CTP 3.2. Siehe Liste der unterstützten Server unter Systemanforderungen und Kompatibilität.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Hypervisors	Unterstützung für Citrix XenServer 6.5.x und früher, VMware ESXi 5.5 Update 3 und früher und Hyper-V 2012 gilt jetzt als veraltet.	May 2020	August 2020	Aktualisieren Sie das System auf eine der folgenden unterstützten Versionen: Citrix Hypervisor 8.0 und später, Citrix XenServer 7.0 und höher, VMware (ESXi 6.0, ESXi 6.5.0 Update 3, ESXi 6.7 Update 2 Patch 10 oder ESXi 7.0) oder Hyper-V (Windows Server 2016 oder Windows Server 2019).
Citrix Launcher	Unterstützung für die Citrix Launcher-App läuft aus.	May 2020	August 2020 (aus App-Store entfernen)	Provisioning dedizierter Geräte als Kiosk. Weitere Informationen finden Sie unter Alternativen für Citrix Launcher.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Mobile Apps und Workspace-Apps von Citrix für Android 6.x und iOS 11.x	Veraltet: Unterstützung für Secure Hub, Secure Mail, Secure Web und Citrix Workspace-App für Android 6.x und iOS 11.x.	April 2020	Juni 2020	Verwenden Sie mindestens die aktuelle Version und die Vorversion jeder gängigen Betriebssystem-plattform.
MDX Toolkit und MDX Service	Einstellung der Unterstützung für MDX Toolkit und MDX Service zugunsten des Mobile App Management (MAM) SDKs. In der Übergangsphase können Sie mit MDX umschlossene und MAM SDK-Apps verwenden.	März 2020	Ziel: März 2022 (für MDX Toolkit) und September 2021 (für MDX Service)	Verwenden Sie zur weiteren Verwaltung Ihrer Unternehmen-sanwendungen das MAM SDK.
MDX: alternativer Gatewayserver	Veraltet: verstärkte Au-thentifizierung für iOS- und Android-Geräte.	März 2020	Zieltermin: September 2021	Keine Alternative

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
MDX: Micro-VPN (Volltunnelmodus)	Veraltet: vollständiger VPN-Tunnel für iOS- und Android-Geräte.	März 2020	Zieltermin: September 2021	Verwenden Sie den MAM SDK Web SSO-Modus oder erstellen Sie eine Pro-App-VPN-Richtlinie mit dem Verbindungstyp “Citrix SSO”.
MDX: PAC-Dateiunterstützun	Unterstützung für PAC-Datei (Proxy Automatic Configuration) mit einem vollständigen VPN-Tunnel für iOS- und Android-Geräte eingestellt.	März 2020	Zieltermin: September 2021	Verwenden Sie Citrix Gateway für die Verbindung über einen Proxyserver, um Zugriff auf interne Netzwerke zu erhalten.
Unterstützung für gemeinsam genutzte MDX-Geräte	Veraltet: Unterstützung gemeinsam genutzter Geräte für MDX-Apps.	März 2020	Zieltermin: September 2021	Verwenden Sie für Android Enterprise die Unterstützung für gemeinsam genutzte Geräte für MDM. Verwenden Sie für iOS Apple School Manager oder GroundControl.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Neue Registrierungen für die Geräteverwaltung in Android 10	Die neue oder erneute Registrierung von Android 10-Geräten im Modus “Legacygeräteverwaltung” wird nicht mehr unterstützt. Bereits registrierte Geräte funktionieren weiterhin.	Februar 2020	September 2020	Registrieren Sie neue Geräte ab Android 10 in Android Enterprise.
Modus “Legacygeräteverwaltung” für Android 10-Geräte	Ende der Google-Unterstützung für einige Device Administration-APIs. Nach dem Upgrade von Citrix Secure Hub auf Android API-Stufe 29 werden Android 10-Geräte, die im Geräteverwaltungsmodus registriert sind, von Citrix nicht mehr unterstützt.	Februar 2020	November 2020	Migrieren Sie Android 10-Geräte auf Android Enterprise.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
MDX-Verschlüsselung	Veraltet: MDX-Verschlüsselung und MDX-Verschlüsselungsfe in der XenMobile Konsole.	Oktober 2019	September 2020	Aktivieren Sie die iOS- oder Android-Plattformverschlüsselung über unsere Verschlüs-selungsverwal-tung mit zusätzlicher Compliance-Überprüfung. Sie müssen die Migration weg von der MDX-Verschlüsselung bis Juli 2020 testen und planen.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Passcode-Geräterichtlinie: Einstellung **Keine Einschränkungen** für Android Enterprise	Android Enterprise-Geräte mit Android 7 oder höher unterstützen nur mit Zeicheneinschränkungen erstellte Passcodes. Wenn Sie zuvor **Erforderliche Zeichen** auf **Keine Einschränkung** festgelegt hatten, ändert sich durch dieses Update der Wert in **Nur Ziffern**.	Februar 2019	Mai 2019	Diese Änderung wirkt sich nicht auf die derzeitige Erfahrung bei der Anmeldung aus.
Remotesupport	Der Remotesupportclient für geclusterte on-premises XenMobile Server-Bereitstellungen ist veraltet.	Januar 2019	August 2020	Keine Alternative

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Secure Hub Network Extensions für iOS	Veraltet ab Secure Hub Release 20.3.0: Network Extension-Framework zur Anpassung der Netzwerkfea-tures für iOS-Geräte.	October 2018	März 2020	Keine Alternative
TLS-Versionen 1.0 und 1.1	Um die Sicherheit von XenMobile weiter zu erhöhen, wird jetzt jede Kommunikation über TLS 1.0 und 1.1 von Citrix blockiert. Aufgrund seiner schwächeren Sicherheit werden TLS 1.0 und TLS 1.1 vom Payment Card Industry Security Standards Council nicht mehr unterstützt.	Juni 2018	März 2019	Upgrade auf TLS 1.2.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Windows Mobile/CE	Die Unterstützung für Windows Mobile/CE-Geräte läuft aus.	April 2018	September 2020	Verwenden Sie Desktops und Laptops mit Windows 10.
Android TouchDown	DigiCert hat die Unterstützung für Android TouchDown eingestellt. Citrix wird die Seite zur Android TouchDown-Plattform aus der Exchange-Geräterichtlinie entfernen.	Juli 2018	2021	Empfehlung: Verwenden Sie Citrix Secure Mail.

Behobene Probleme

September 24, 2021

Die folgenden Probleme wurden in XenMobile 10.14 behoben:

- Nach dem Upgrade auf XMS 10.12 gibt es Probleme mit der Dashboardanzeige auf der XenMobile Server-Konsole. [CXM-88918]
- Die Registrierung bei Apple-Bereitstellungsprogrammen (früher DEP) schlägt auf Apple-Geräten fehl, wenn Generic PKI konfiguriert ist. [CXM-89978]
- Wenn Sie sich mit rollenbasierter Zugriffssteuerung (RBAC) anmelden, sind zusätzliche Berechtigungen zum Bearbeiten von Registrierungsprofilen erforderlich. [CXM-89985]
- Auf der XenMobile Server-Konsole können Sie die Richtlinie **Verwaltete Android Enterprise-Konfigurationen** für die Chrome-App nicht bearbeiten. [CXM-89986]
- Wenn Sie auf der iOS-Plattform eine VPN-Richtlinie mit dem Verbindungstyp **AlwaysOn IKEv2-Doppelkonfiguration**bearbeiten, tritt ein Fehler auf. [CXM-90010]

- Die Registrierung von Android Enterprise-Geräten mit **SamAccountName** schlägt fehl und Sie erhalten den folgenden Fehler: “Work profile deleted, wiping profile”. [CXM-90049]
- Die Datenbank akzeptiert Benutzernamen nicht, die mit dem Kleinbuchstaben “u” beginnen. [CXM-90722]
- Auf der XenMobile Server-Konsole wird die ICCID (Integrated Circuit Card ID) für Geräte angezeigt, in die keine SIM-Karte eingelegt ist. [CXM-90845]
- Die Registrierung des Apple Device Enrollment Program (DEP) schlägt auf Geräten mit iOS 14 fehl. [CXM-91697]
- In der XenMobile Server-Konsole wird nicht das richtige Ablaufdatum für das Stammzertifikat angezeigt. [CXM-91961]
- In XenMobile Server wird für NetScaler Gateway-Verbindungsprüfungen kein Ergebnis angezeigt. [CXM-93129]
- Wenn Sie SNMP-Benutzer zur XenMobile Server-Konsole hinzufügen, erscheinen die Benutzer nicht in der Liste der *SNMP-Überwachungsbenutzer* oder die SNMP-Agents werden inaktiv. [CXM-93197]
- Wenn Sie die Einstellungen **System-Apps aktivieren** und **Anwendungen deaktivieren** für dieselbe App in der Geräteeinschränkungsrichtlinie aktivieren, wird die App trotzdem im Arbeitsprofil angezeigt. [CXM-93671]
- Die Servereigenschaft `ios.mdm.apns.connectionPoolSize` wird ausgeblendet, wenn Sie zur HTTP/2-basierten API für APNs wechseln. [CXM-95478]
- Unter XenMobile Server Version 10.12 können Sie die VPP-Eigenschaften für bestimmte Apps nicht ändern. [CXM-96796]
- Auf Geräten installierte Apple Volume Purchase-Apps werden automatisch auf die aktuelle Version aktualisiert, wenn die Einstellung für **Automatische App-Updates** deaktiviert ist. [CXM-96855]
- Wenn Sie auf XenMobile Server Version 10.13 den Proxyserver über die **Befehlszeilenschnittstelle** konfigurieren, können Sie keine Benachrichtigungen an Secure Hub auf iOS-Geräten senden. [CXM-97609]
- Auf XenMobile Server Version 10.13 wird beim Zugriff auf **Gerätedetails** eine Fehlermeldung angezeigt. Dieser Fehler tritt auf, wenn die Geräteeigenschaft einen Wert in **”“** hat. [CXM-97952]
- Informationen zu behobenen Problemen in Rolling Patch 10.13.0 finden Sie unter:
  - XenMobile Server 10.13.0 Rolling Patch 4
  - XenMobile Server 10.13.0 Rolling Patch 3
  - XenMobile Server 10.13.0 Rolling Patch 2

Verwandte Informationen

- XenMobile Support Knowledge Center

Änderungen bei der Plattformunterstützung

Bekannte Probleme

January 5, 2022

Bei XenMobile 10.14 ist folgendes Problem bekannt:

- Nach dem Importieren eines XenMobile Server 10.8- oder 10.9-Images in VMware ESXi 6.7 oder 6.5 Update 2 und einem Neustart der VM wird die Konfigurationsanwendung nicht gestartet, XenMobile Server wechselt in den Wiederherstellungsmodus und die IP-Einstellungen werden gelöscht. Erstellen Sie als Workaround eine neue VM mit einer VMXNET3-Netzwerkkarte und verbinden Sie sie mit der Datenbank der VM, die in den Wiederherstellungsmodus versetzt wurde. [CXM-54581]
- Nach der Registrierung eines Geräts mit iOS 15 oder macOS 12 wird das MDM-Konfigurationsprofil als “Nicht verifiziert” angezeigt. [CXM-98525]
- Nach dem Upgrade auf Android 12 werden Geräte, die im Arbeitsprofilmodus erneut registriert wurden, zweimal in der Geräteverwaltungstabelle angezeigt. [CXM-99712]
- Nach dem Senden eines Ortungsbefehls an ein in MDM registriertes Gerät mit Android 12 wird ein weißer Bildschirm angezeigt, der beim Starten von Secure Hub dauerhaft geladen wird. [CXM-99878]
- Informationen zu bekannten Problemen im Zusammenhang mit mobilen Produktivitätsapps finden Sie unter Secure Hub, Secure Mail und Secure Web.
- Informationen zu bekannten Problemen in der aktuellen Version des Rolling Patch Release 10.13.0 finden Sie unter:
  - Versionshinweise für XenMobile Server 10.13 Rolling Patch 4

Verwandte Informationen

- XenMobile Support Knowledge Center

Architektur

January 5, 2022

Welche XenMobile-Komponenten Sie in der XenMobile-Architektur bereitstellen, hängt von den Anforderungen des Unternehmens an die Geräte- bzw. App-Verwaltung ab. Die Komponenten von XenMobile sind modular und bauen aufeinander auf. Ihre Bereitstellung enthält beispielsweise Citrix Gateway:

- Citrix Gateway ermöglicht Benutzern Remotezugriff auf mobile Apps und überwacht Benutzergerätetypen.
- Sie verwalten diese Apps und Geräte in XenMobile.

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 Citrix Gateway eine Verbindung herstellen. Die Verbindung bietet Zugriff auf Apps und Desktops im internen Netzwerk.
- 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 mobile Apps: Benutzer können auf ihre Web-, SaaS- und mobilen Apps von XenMobile über Secure Hub zugreifen.
- Windows-basierte Apps 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 dieser Funktionen für On-Premises-XenMobile Server empfiehlt Citrix die Bereitstellung von XenMobile-Komponenten in der folgenden Reihenfolge:

- Citrix Gateway. Sie können Einstellungen in Citrix Gateway für die Kommunikation mit XenMobile, StoreFront oder dem Webinterface mit dem Konfigurationsassistenten konfigurieren. Vor der Verwendung des Konfigurationsassistenten in Citrix Gateway müssen Sie eine der folgenden Komponenten installieren, damit Sie die Kommunikation damit einrichten können: XenMobile, StoreFront oder das Webinterface.
- 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.

- MAM-SDK oder MDX Toolkit. Die MDX-Technologie erreicht das Ende des Lebenszyklus (EOL) im März 2022. Um die Verwaltung Ihrer Unternehmensanwendungen fortzusetzen, müssen Sie das MAM-SDK integrieren.

  Das MAM-SDK (Mobile Application Management) bietet MDX-Funktionalität, die nicht von den iOS- und Android-Plattformen abgedeckt ist. Sie können iOS- oder Android-Apps MDX-fähig machen und sichern. Sie stellen diese Apps entweder in einem internen Store oder in öffentlichen App-Stores zur Verfügung. Siehe MDX App SDK.

- StoreFront (optional): Sie können den Zugriff auf Windows-basierte Anwendungen und virtuelle Desktops von StoreFront über Verbindungen mit Receiver bereitstellen.
- Citrix Files (optional). Wenn Sie Citrix Files 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 Citrix Content Collaboration finden Sie auf der Support-Website für Content Collaboration.

XenMobile unterstützt die Geräteverwaltung und App-Verwaltung über die XenMobile-Konsole. 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 Citrix ADC kann die Last für den XenMobile-Server weiter vermindern und den Durchsatz erhöhen. Weitere Informationen zum Einrichten von Clustering für XenMobile durch die Konfiguration von zwei virtuellen IP-Adressen zum Lastausgleich in Citrix ADC finden Sie unter Clustering.

Weitere Informationen zum Konfigurieren von XenMobile für eine Notfallwiederherstellungsbereitstellung finden Sie im XenMobile-Bereitstellungshandbuch unter Disaster Recovery. Dieser Artikel enthält ein Architekturdiagramm.

In den folgenden Abschnitten werden verschiedene Referenzarchitekturen für die XenMobile-Bereitstellung beschrieben. Architekturdiagramme finden Sie im XenMobile-Bereitstellungshandbuch unter Reference Architecture for On-Premises Deployments und Architecture. Eine vollständige Liste der Ports finden Sie unter Portanforderungen (lokal) und Portanforderungen (Cloud).

Mobilgeräteverwaltungsmodus (MDM-Modus)

> **Wichtig:**
>
> Wenn Sie den ursprünglich konfigurierten MDM-Modus in den ENT-Modus ändern, müssen Sie darauf achten, dass Sie die gleiche (Active Directory)-Authentifizierung verwenden. Die Änderung des Authentifizierungsmodus nach der Benutzerregistrierung wird in XenMobile nicht

> unterstützt. Weitere Informationen finden Sie unter Upgrade von XenMobile MDM Edition auf Enterprise Edition.

XenMobile MDM Edition stellt mobile Geräteverwaltung bereit. Informationen zu unterstützten Plattformen finden Sie unter Unterstützte Gerätebetriebssysteme. Wenn Sie nur die MDM-Features von XenMobile verwenden möchten, stellen Sie XenMobile im MDM-Modus bereit. Dies gilt beispielsweise für folgende Funktionen:

- Bereitstellen von Geräterichtlinien und Apps
- Abrufen von Bestandsverzeichnissen
- Ausführen von Aktionen an Geräten, z. B. Löschen von Geräten

Bei dem empfohlenen Modell ist XenMobile Server in der DMZ, eine optionale Platzierung hinter Citrix ADC bietet mehr Schutz für XenMobile.

Mobilanwendungsverwaltungsmodus (MAM-Modus)

MAM, auch als Nur-MAM-Modus bezeichnet, bietet mobile App-Verwaltung. Informationen zu unterstützten Plattformen finden Sie unter Unterstützte Gerätebetriebssysteme. Wenn Sie planen, nur die MAM-Features von XenMobile zu verwenden und keine Geräte für MDM zu registrieren, stellen Sie XenMobile im MAM-Modus bereit. Dies gilt beispielsweise für folgende Funktionen:

- Sichern von Apps und Daten auf BYO-Mobilgeräten
- Bereitstellen mobiler Unternehmensapps
- Sperren von Apps und Löschen ihrer Daten

Die Geräte dürfen nicht für die Mobilgeräteverwaltung (MDM) registriert sein.

Bei diesem Bereitstellungsmodell ist XenMobile Server hinter Citrix Gateway. Dies bietet zusätzlichen Schutz für XenMobile.

MDM+MAM-Modus

Die gemeinsame Verwendung des MDM- und MAM-Modus ermöglicht die Verwaltung mobiler Apps sowie von Daten und Mobilgeräten. Informationen zu unterstützten Plattformen finden Sie unter Unterstützte Gerätebetriebssysteme. Wenn Sie planen, die MDM- und MAM-Features von XenMobile zu verwenden, stellen Sie XenMobile im ENT-Modus (Enterprise) bereit. Sie möchten beispielsweise Folgendes durchführen:

- Verwalten eines vom Unternehmen bereitgestellten Geräts mithilfe von MDM
- Bereitstellen von Geräterichtlinien und Apps
- Abrufen eines Bestandsverzeichnisses
- Löschen von Geräten
- Bereitstellen mobiler Unternehmensapps

- Sperren von Apps und Löschen der Daten auf Geräten

Bei dem empfohlenen Bereitstellungsmodell ist XenMobile Server in der DMZ hinter Citrix Gateway. Dies bietet zusätzlichen Schutz für XenMobile.

XenMobile im internen Netzwerk: Eine andere Bereitstellungsoption besteht darin, einen lokalen XenMobile-Server im internen Netzwerk statt in der DMZ zu platzieren. Diese Bereitstellungsoption wird verwendet, wenn Sicherheitsrichtlinien vorschreiben, dass nur Netzwerkgeräte in der DMZ sein dürfen. In dieser Bereitstellung ist XenMobile Server nicht in der DMZ. Daher ist es nicht erforderlich, Ports in der internen Firewall zu öffnen, um Zugriff auf SQL- und PKI-Server über die DMZ zu gewähren.

Systemanforderungen und Kompatibilität

January 5, 2022

> **Hinweis:**
>
> In diesem Artikel werden Systemanforderungen für und Kompatibilität von XenMobile Server 10.14 behandelt. Informationen zu den Systemanforderungen von Endpoint Management finden Sie unter Systemanforderungen.

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

- XenMobile-Kompatibilität
- Unterstützte Gerätebetriebssysteme
- Portanforderungen
- Skalierbarkeit
- Lizenzierung
- FIPS 140-2-Compliance
- Sprachunterstützung

Für die Ausführung von XenMobile 10.14 gelten die folgenden Mindestanforderungen:

- Eines der Folgenden:
  - Citrix Hypervisor 8.1 oder 8.0 oder Citrix XenServer (unterstützte Versionen: 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2); Einzelheiten siehe XenServer
  - VMware (unterstützte Versionen: ESXi 6.0, ESXi 6.5.0 Update 3 oder ESXi 6.7 Update 2 Patch 10, ESXi 7.0 Update 2a); Einzelheiten siehe ESXi 6.7-Workaround und VMware
  - Hyper-V (unterstützte Versionen: Windows Server 2016 und Windows Server 2019); Einzelheiten siehe Hyper-V
- Endpoint Management Connector für Exchange ActiveSync 10.1.10 oder Citrix Gateway Connector für Exchange ActiveSync 8.5.3.19

- Dual-Core-Prozessor
- Vier virtuelle CPUs
- 8 GB RAM für Produktionsumgebungen; 4 GB RAM für Testumgebungen und für Machbarkeitsstudien genutzte Umgebungen
- 50 GB Speicherplatz
- Citrix Lizenzserver 11.16.

  Aktualisieren Sie Ihren Lizenzserver, bevor Sie den XenMobile Server aktualisieren.

ESXi 6.7-Workaround

Zur einwandfreien Ausführung von ESXi 6.7 müssen Sie den folgenden Workaround implementieren.

1. Extrahieren Sie mit dem OVF-Tool von VMware die von citrix.com heruntergeladene OVA-Datei. Das OVF-Tool können Sie von der VMware-Website unter https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491 herunterladen.
2. Es werden drei Dateien extrahiert. Laden Sie die VMDK-Datei in Ihren Datenspeicher hoch.
3. Erstellen Sie eine neue virtuelle Maschine.
   a) Benennen Sie die virtuelle Maschine und wählen Sie als Kompatibilitätsoption **ESX/ESXi 4.x**.
   b) Wählen Sie als Gastbetriebssystemfamilie **Linux**.
   c) Wählen Sie als Gastbetriebssystemfamilie **Other 2.6.x Linux (64-bit)**.
   d) Wählen Sie als Datenspeicher **Default**.
   e) Entfernen Sie bei der Anpassung die Standardfestplatte, den USB-Controller und das CD/DVD-Laufwerk.
   f) Wählen Sie unter “Network” als Adaptertyp **VMXNET3**.
   g) Wählen Sie in ESXi, sofern Ihre Datenträger lokal sind, **SCSI Controller** nd **LSI Logic Parallel**. Bei Verwendung eines freigegebenen Laufwerks wählen Sie **VMware Paravirtual**.
   h) Klicken Sie auf “Next”, um die VM-Erstellung abzuschließen.
4. Gehen Sie zu Ihrem Datenspeicher und kopieren Sie die zuvor hochgeladene VMDK-Datei. Kopieren Sie die Datei in das VM-Verzeichnis, das Sie für XenMobile erstellt haben.
5. Wählen Sie auf der ESXi-Weboberfläche die VM, und bearbeiten Sie die Einstellungen.
6. Klicken Sie auf **Add Hard disk**.
7. Wählen Sie die zuvor kopierte VMDK-Datei aus und fügen Sie sie der VM an.
8. Klicken Sie auf **Speichern**.
9. Fahren Sie die VM hoch.

Systemanforderungen für Citrix Gateway

Für die Ausführung von Citrix Gateway mit XenMobile 10.14 gelten die folgenden Mindestanforderungen:

- Citrix Gateway (on-premises). Unterstützte Versionen: 12.1 oder höher
- Außerdem ist Kommunikation mit Active Directory und somit ein Dienstkonto erforderlich. Sie benötigen nur Abfrage- und Lesezugriff.

XenMobile 10.14-Datenbankanforderungen

Für XenMobile ist eine der folgenden Datenbanken erforderlich:

- Microsoft SQL Server

  XenMobile unterstützt eine Microsoft SQL Server-Datenbank in einer der folgenden unterstützten Versionen: Weitere Informationen zu Microsoft SQL Server-Datenbanken und ihren Hardwareanforderungen finden Sie in der Microsoft-Dokumentation.

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

  Die Microsoft SQL Server-Datenbankanforderungen hängen auch von der Größe Ihrer Bereitstellung ab. Weitere Informationen zu Microsoft SQL Server-Datenbankanforderungen für die Größe Ihrer Bereitstellung finden Sie unter Skalierbarkeit.

  XenMobile unterstützt SQL Basic-Verfügbarkeitsgruppen (AlwaysOn-Verfügbarkeitsgruppen) und SQL-Clustering für hohe Datenbankverfügbarkeit.

  Citrix empfiehlt die Remote-Verwendung von Microsoft SQL.

  Informationen zum Upgrade von Microsoft SQL finden Sie im Microsoft-Artikel Upgrade von SQL Server.

- PostgreSQL (nur für Testumgebungen) PostgreSQL wird mit XenMobile ausgeliefert. Sie können es lokal oder remote in Testumgebungen verwenden. Eine Datenbankmigration wird nicht unterstützt. In einer Testumgebung erstellte Datenbanken können nicht in eine Produktionsumgebung übertragen werden.

  Alle XenMobile-Editionen unterstützen Remote PostgreSQL 9.5.1 und 9.5.11 für Windows mit den folgenden Einschränkungen: Nicht empfohlen für Produktionsumgebungen. Unterstützung für bis zu 300 Geräte. Verwenden Sie einen lokalen SQL Server für mehr als 300 Geräte. Keine Unterstützung für Clustering

SQL Server-Dienstkontoanforderungen

Das in XenMobile zu verwendende SQL Server-Dienstkonto muss die Rollenberechtigung `DBcreator` aufweisen. Notieren Sie das SQL Server-Kontokennwort, das Sie bei der XenMobile Server-Installation angeben. Das Kennwort ist erforderlich, wenn Sie die XenMobile-Datenbank bei einer XenMobile Server-Wiederherstellung klonen müssen.

Schützen Sie die SQL Server-Datenbanken mit Transparent Data Encryption (TDE). Lassen Sie keinen externen Zugriff auf SQL Server-Ports zu, wie in der Referenzarchitektur in Referenzarchitektur für On-Premises-Bereitstellungen gezeigt.

Weitere Informationen über SQL Server-Dienstkonten finden Sie auf den folgenden Seiten in der Microsoft-Dokumentation. Diese Links verweisen auf Informationen für SQL Server 2014. Wenn Sie eine andere Version verwenden, wählen Sie sie in der Liste **Andere Versionen** aus:

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

Kompatibilität mit Virtual Apps and Desktops

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

StoreFront-Kompatibilität

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

Weitere Kompatibilitätsangaben

- Endpoint Management Connector für Exchange ActiveSync 10.1.10
  - Kein Test für ältere Versionen
- Citrix Gateway Connector für Exchange ActiveSync 8.5.3.19
  - Kein Test für ältere Versionen

XenMobile-Kompatibilität

January 5, 2022

> **Hinweis:**
>
> In diesem Artikel wird die Kompatibilität von XenMobile Server behandelt. Informationen zu mit Endpoint Management getesteten Komponenten finden Sie unter Endpoint Management-Kompatibilität.

Um die neuen Features, Fixes und Richtlinienaktualisierungen zu verwenden, empfiehlt Citrix, die neueste Version der folgenden Komponenten zu installieren:

- Citrix empfiehlt, das MAM-SDK (Mobile Application Management) in iOS- und Android-Unternehmensapps zu integrieren, um MDX-Funktionen auf diese Apps anzuwenden.

  Das MDX Toolkit erreicht das Ende des Lebenszyklus (EOL) im März 2022. Um die Verwaltung Ihrer Unternehmensapps fortzusetzen, müssen Sie das MAM-SDK integrieren.

In diesem Artikel werden die Versionen der unterstützten XenMobile-Komponenten, die integriert werden können, zusammengefasst.

Kompatibilität und Upgradepfade

Die neuesten Versionen von Secure Hub, MDX Toolkit und von mobilen Produktivitätsapps sind mit der aktuellen sowie der vorherigen Version von XenMobile Server kompatibel.

Für die aktuelle Version der mobilen Produktivitätsapps ist die aktuelle Version von Secure Hub erforderlich. Die beiden Vorgängerversionen der Apps sind mit der aktuellen Version von Secure Hub kompatibel. Weitere Informationen finden Sie unter Citrix Product Matrix.

Citrix unterstützt die Verteilung von XenMobile-Produktivitätsapps nur über einen öffentlichen App-Store.

XenMobile Server (on-premises)

- Citrix unterstützt ein Upgrade von den letzten zwei Versionen von XenMobile Server.
- Neueste Version von XenMobile Server: XenMobile Server 10.14
- Upgrade von:
  - XenMobile Server 10.13.x
  - XenMobile Server 10.12.x

Mobile Produktivitätsapps

Die Benutzer haben Zugang zu mobilen Produktivitätsapps über die öffentlichen App-Stores. Für die aktuelle Version der mobilen Produktivitätsapps ist die aktuelle Version von Secure Hub erforderlich. Die beiden Vorgängerversionen der Apps sind mit der aktuellen Version von Secure Hub kompatibel.

Weitere Informationen zum schrittweisen Release der mobilen Produktivitätsapps über einen Zeitraum von zwei Wochen finden Sie im Releasezeitplan. Weitere Supportinformationen finden Sie unter Unterstützung für Mobile Produktivitätsapps.

MAM-SDK

Das MAM-SDK bietet MDX-Funktionalität, die nicht von den iOS- und Android-Plattformen abgedeckt ist. Sie stellen diese Apps entweder in einem internen Store oder in öffentlichen App-Stores zur Verfügung. Siehe MDX App SDK.

MDX Toolkit

Die MDX-Technologie erreicht das Ende des Lebenszyklus (EOL) im September 2021. Um die Verwaltung Ihrer Unternehmensanwendungen fortzusetzen, müssen Sie das MAM-SDK integrieren.

Citrix unterstützt die letzten drei Releases (n.n.n) des MDX Toolkit. Siehe Neue Features im MDX Toolkit.

Browserunterstützung

Die XenMobile Server-Konsole erfordert einen der folgenden unterstützten Webbrowser:

- Aktuelle Version von Google Chrome
- Aktuelle Version von Mozilla Firefox
- Aktuelle Version von Microsoft Edge
- Aktuelle Version von Apple Safari

Unterstützte Gerätebetriebssysteme

January 5, 2022

> **Hinweis:**
>
> In diesem Artikel werden die von XenMobile Server 10.13 unterstützten Gerätebetriebssysteme behandelt. Informationen zu Betriebssystemen mit Unterstützung für Endpoint Management

> finden Sie unter Unterstützte Gerätebetriebssysteme.

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

Die Informationen zu unterstützten Geräteplattformen in diesem Artikel gelten auch für den XenMobile Connector für Exchange ActiveSync und den Citrix Gateway Connector für Exchange ActiveSync.

Die neusten Versionen der mobilen Produktivitätsapps sowie unterstützte Geräte für die MDX-Verschlüsselung finden Sie unter Unterstützung für mobile Produktivitätsapps.

> **Hinweis:**
>
> Citrix unterstützt mindestens die aktuelle Version und die Vorversion jeder gängigen Betriebssystemplattform. Nicht alle Features der neueren Endpoint Management-Versionen funktionieren auf älteren Plattformen.
>
> Ankündigungen zu veralteten Funktionen finden Sie unter Einstellung von Features und Plattformen.

Liste der unterstützten Betriebssysteme

Citrix XenMobile unterstützt folgende Betriebssysteme:

> **Hinweis:**
>
> Die Unterstützung für die Android 7.x- und iOS 12.x-Versionen von Secure Hub, Secure Mail, Secure Web und Citrix Workspace-App endete im April 2021.

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

  Informationen zu Android 10+ finden Sie unter Überlegungen zu Android.

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

  XenMobile und mobile Citrix Apps sind mit iOS 14.x kompatibel, unterstützen aber derzeit nicht alle neuen iOS 14.x-Features. Verwenden Sie zum Umschließen unternehmensinterner Unternehmens-Apps für iOS 14.x das MDX Toolkit 21.8.5 oder höher bzw. bereiten Sie die Apps mit dem MAM-SDK vor.

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

  XenMobile und mobile Citrix Apps sind mit iPadOS 14.x kompatibel, unterstützen aber derzeit nicht alle neuen iPadOS 14.x-Features.

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

XenMobile und mobile Citrix Apps sind mit macOS 11 kompatibel, unterstützen aber derzeit nicht alle neuen macOS 11-Features.

- **Windows-Desktops und -Tablets:** (nur MDM) Windows 10 und Windows 11
- **Windows Phone:** (nur MDM) Windows Phone 8.1, Windows Phone 10, Windows 10 RS4 und RS5
- **Windows Mobile/CE:** (nur MDM). Die Unterstützung von Windows Mobile-/CE-Geräten ist seit dem zweiten Quartal 2018 eingestellt.
- **Samsung SAFE und Knox:** Auf kompatiblen Samsung-Geräten bietet XenMobile Unterstützung und Erweiterung von Samsung for Enterprise- (SAFE) und Samsung Knox-Richtlinien. XenMobile erfordert die Aktivierung der SAFE-APIs, bevor SAFE-Richtlinien und -Einschränkungen bereitgestellt werden können. Stellen Sie hierzu einem Gerät den integrierten ELM-Schlüssel (Enterprise License Management) von Samsung bereit. Weitere Informationen finden Sie unter Geräterichtlinie für Samsung MDM-Lizenzschlüssel.

Überlegungen zu Android

Vor dem Upgrade auf Android 10 oder später: Informationen dazu, wie sich die Außerbetriebnahme von Google Device Administration APIs auf Geräte mit Android 10 auswirkt, finden Sie unter Migration von der Geräteverwaltung zu Android Enterprise.

- Citrix empfiehlt, dass Sie die Registrierung von Android 10-Geräten im Legacy-Android-Geräteverwaltungsmodus vermeiden. Google stellt Device Administration APIs ein, was sich auf Geräte mit Android 10+ auswirkt. Nach Ablauf der API-Unterstützung schlägt die Registrierung von Android 10+-Geräten im Legacy-Geräteverwaltungsmodus fehl. Citrix unterstützt die Registrierung von Android 11-Geräten im Geräteverwaltungsmodus nicht.
- Citrix empfiehlt, Android Enterprise für Android 10-Geräte zu verwenden. Weitere Informationen finden Sie unter Migration von der Geräteverwaltung zu Android Enterprise.
- Die Änderung der Google API wirkt sich nicht auf Geräte aus, die im Nur-MAM-Modus registriert sind.

Upgradevorbereitung:

- Stellen Sie sicher, dass Ihre Serverinfrastruktur mit Sicherheitszertifikaten kompatibel ist, die über einen übereinstimmenden Hostnamen in der subjectAltName-Erweiterung (SAN) verfügen.
- Zum Überprüfen eines Hostnamens muss der Server ein Zertifikat mit einem passenden SAN bereitstellen. Citrix vertraut Zertifikaten nur dann, wenn sie ein SAN enthalten, der dem Hostnamen entspricht.

Portanforderungen

January 5, 2022

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

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

Öffnen Sie die folgenden Ports, damit Benutzer über Citrix Gateway Verbindungen von Citrix Secure Hub, Citrix Receiver und dem Citrix Gateway Plug-In zu den folgenden Komponenten herstellen können:

- XenMobile
- StoreFront
- Citrix Virtual Apps and Desktops
- Citrix Gateway Connector für Exchange ActiveSync
- Andere interne Netzwerkressourcen, z. B. Intranet-Websites

Um Datenverkehr für Launch Darkly von Citrix ADC zu aktivieren, können Sie die in diesem Artikel im Support Knowledge Center aufgeführten IP-Adressen verwenden.

Weitere Informationen zu Citrix Gateway finden Sie in der Citrix Gateway-Dokumentation. Diese Dokumentation enthält Informationen zur Citrix ADC-IP-Adresse (NSIP), IP-Adresse des virtuellen Servers (VIP) und Subnetz-IP-Adresse (SNIP).

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.	Citrix Gateway, XenMobile	DNS-Server

TCP-Port	Beschreibung	Quelle	Ziel
80	Citrix Gateway leitet die VPN-Verbindung mit der internen Netzwerksressource durch die zweite Firewall. Dies geschieht in der Regel, wenn Benutzer sich mit dem Citrix Gateway Plug-In anmelden.	Citrix 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; Citrix Gateway STA	Virtuelle Apps oder Desktops
123 (TCP und UDP)	Wird für Network Time Protocol-Dienste (NTP) verwendet.	Citrix Gateway; XenMobile	NTP-Server
389	Wird für unsichere LDAP-Verbindungen verwendet.	Citrix Gateway; XenMobile	LDAP-Authentifizierungsserver oder Microsoft-Active Directory
443	Wird für Verbindungen zwischen StoreFront und Citrix Receiver und zwischen Receiver für Web und Virtual Apps and Desktops verwendet.	Internet	Citrix Gateway

TCP-Port	Beschreibung	Quelle	Ziel
443	Wird für Verbindungen mit XenMobile zur Bereitstellung von Web-, Mobil- und SaaS-Apps verwendet.	Internet	Citrix Gateway
443	Wird für die allgemeine Gerätekommunikation mit XenMobile Server verwendet.	XenMobile	XenMobile
443	Wird für Verbindungen von mobilen Geräten zu XenMobile für die Registrierung verwendet.	Internet	XenMobile
443	Wird für Verbindungen von XenMobile zum Citrix Gateway Connector für Exchange ActiveSync verwendet.	XenMobile	Citrix Gateway Connector für Exchange ActiveSync
443	Wird für Verbindungen vom Citrix Gateway Connector für Exchange ActiveSync zu XenMobile verwendet.	Citrix Gateway Connector für Exchange ActiveSync	XenMobile

TCP-Port	Beschreibung	Quelle	Ziel
443	Wird für die Callback-URL in Bereitstellungen ohne Zertifikatauthentifizierung verwendet.	XenMobile	Citrix Gateway
514	Wird für Verbindungen zwischen XenMobile und einem syslog-Server verwendet.	XenMobile	syslog-Server
636	Wird für sichere LDAP-Verbindungen verwendet.	Citrix Gateway; XenMobile	LDAP-Authentifizierungsserver oder Active Directory
1494	Wird für ICA-Verbindungen mit Windows-basierten Anwendungen im internen Netzwerk verwendet. Citrix empfiehlt, diesen Port geöffnet zu lassen.	Citrix Gateway	Virtuelle Apps oder Desktops
1812	Wird für RADIUS-Verbindungen verwendet.	Citrix Gateway	RADIUS-Authentifizierungsserver

TCP-Port	Beschreibung	Quelle	Ziel
2598	Wird für Verbindungen mit Windows-basierten Anwendungen im internen Netzwerk unter Einsatz der Sitzungszuverlässigkeit verwendet. Citrix empfiehlt, diesen Port geöffnet zu lassen.	Citrix Gateway	Virtuelle Apps oder Desktops
3268	Wird für unsichere LDAP-Verbindungen mit dem globalen Microsoft-Katalog verwendet.	Citrix Gateway; XenMobile	LDAP-Authentifizierungsserver oder Active Directory
3269	Wird für sichere LDAP-Verbindungen mit dem globalen Microsoft-Katalog verwendet.	Citrix Gateway; XenMobile	LDAP-Authentifizierungsserver oder Active Directory
9080	Wird für HTTP-Datenverkehr zwischen Citrix ADC und dem Citrix Gateway Connector für Exchange ActiveSync verwendet.	Citrix ADC	Citrix Gateway Connector für Exchange ActiveSync
30001	Verwaltungs-API für die Erstbereitstellung des HTTPS-Diensts	Internes LAN	XenMobile Server

TCP-Port	Beschreibung	Quelle	Ziel
9443	Wird für HTTPS-Datenverkehr zwischen Citrix ADC und dem Citrix Gateway Connector für Exchange ActiveSync verwendet.	Citrix ADC	Citrix Gateway Connector für Exchange ActiveSync
45000; 80	Wird in Clusterbereitstellungen für die Kommunikation zwischen zwei XenMobile-VM verwendet. Port 80 ist für die Kommunikation zwischen Knoten und für den SSL-Offload bestimmt.	XenMobile	XenMobile
8443	Wird für die Registrierung, den XenMobile Store und die Mobilanwendungsverwaltung (MAM) verwendet.	XenMobile; Citrix Gateway; Geräte; Internet	XenMobile

TCP-Port	Beschreibung	Quelle	Ziel
4443	Wird von Administratoren für den Zugriff auf die XenMobile-Konsole über einen Browser verwendet. Wird außerdem für den Download von Protokollen und Supportpaketen für alle XenMobile-Clusterknoten von einem Knoten verwendet.	Zugriffspunkt (Browser); 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
161	Wird für den SNMP-Datenverkehr mit UDP-Protokoll verwendet.	SNMP-Manager	XenMobile
162	Wird zum Senden von SNMP-Traps von XenMobile an den SNMP-Manager verwendet. XenMobile ist die Quelle und der SNMP-Manager ist das Ziel.	XenMobile	SNMP-Manager

Öffnen von XenMobile-Ports zum Verwalten von Geräten

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

TCP-Port	Beschreibung	Quelle	Ziel
25	Standard-SMTP-Port für den XenMobile-Benachrichtigungsdien 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, Google Play (muss 80 verwenden) oder Windows Phone Store. Wird für Apple Volume Purchase verwendet. Wird zum Veröffentlichen von Apps aus den App-Stores unter iOS, Secure Hub für Android oder Secure Hub für Windows Phone verwendet.	XenMobile	`ax.apps.apple.com` und `*.mzstatic.com`; `vpp.itunes.apple.com`; `login.live.com`; `*.notify.windows.com`; `play.google.com`, `android.clients.google.com`, `android.l.google.com`
80 oder 443	Wird für ausgehende Verbindungen zwischen XenMobile und Nexmo SMS Notification Relay verwendet.	XenMobile	Nexmo SMS Relay-Server

TCP-Port	Beschreibung	Quelle	Ziel
389	Wird für unsichere LDAP-Verbindungen verwendet.	XenMobile	LDAP-Authentifizierungsserver oder Active Directory
443	Wird für die Registrierung und das Agent-Setup für Android und Windows Mobile verwendet.	Internet	XenMobile
443	Wird für die Registrierung und das Agent-Setup für Android- und Windows-Geräte und den MDM-Client für Remotesupport verwendet.	Internet - LAN und Wi-Fi	XenMobile
1433	Wird standardmäßig für Verbindungen mit einem Remotedatenbankserver verwendet (optional).	XenMobile	SQL Server
443 oder 2197	Wird zum Senden von APNs-Benachrichtigungen an `*.push.apple.com` verwendet.	XenMobile	Internet (APNs-Hosts mit öffentlicher IP-Adresse 17.0.0.0/8)
5223	Wird für ausgehende APNs-Verbindungen von iOS-Geräten an `*.push.apple.com` verwendet.	iOS-Geräte	Internet (APNs-Hosts mit öffentlicher IP-Adresse 17.0.0.0/8)

TCP-Port	Beschreibung	Quelle	Ziel
8081	Wird für die App-Tunnel des optionalen MDM-Remotesupportclients verwendet. Standardwert: 8081.	Remotesupportclient	XenMobile
8443	Für die Registrierung von iOS- und Windows Phone-Geräten.	Internet; LAN und Wi-Fi	XenMobile

Portanforderungen für die Verbindung mit dem AutoDiscovery Service

Diese Portkonfiguration gewährleistet, dass auf Android-Geräten mit Secure Hub für Android über das interne Netzwerk auf den Citrix AutoDiscovery Service (ADS) zugegriffen werden kann. Sie benötigen Zugriff auf ADS, um über ADS bereitgestellte Sicherheitsupdates herunterzuladen.

> **Hinweis:**
>
> ADS-Verbindungen unterstützen Ihren Proxyserver eventuell nicht. Lassen Sie in diesem Szenario zu, dass die ADS-Verbindung den Proxy-Server umgeht.

Wenn Sie Zertifikatpinning aktivieren möchten, treffen Sie folgende Vorbereitungen:

- **Sammeln von XenMobile Server- und Citrix ADC-Zertifikaten:** Die Zertifikate müssen im PEM-Format vorliegen und öffentlich sein, d. h. keine privaten Schlüssel sind zulässig.
- **Öffnen Sie einen Supportfall beim Citrix Support zum Aktivieren von Zertifikatpinning:** Bei diesem Prozess werden Ihre Zertifikate angefordert.

Zertifikatpinning erfordert, dass Geräte vor der Registrierung eine Verbindung mit ADS herstellen. Damit wird sichergestellt, dass Secure Hub über die aktuellen Sicherheitsinformationen verfügt. Für eine Registrierung in Secure Hub muss das Gerät mit ADS verbunden sein. 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 für Android möglich ist, öffnen Sie Port 443 für die folgenden IP-Adressen und FQDNs:

FQDN	IP-Adresse	Port	IP- und Port-Nutzung
ads.xm.cloud.com	34.194.83.188	443	Secure Hub - ADS-Kommunikation
ads.xm.cloud.com	34.193.202.23	443	Secure Hub - ADS-Kommunikation

> **Hinweis:**
>
> Bei Secure Hub-Versionen vor 10.6.15 lautet der FQDN discovery.mdm.zenprise.com. Öffnen Sie Port 443 für die IP-Adressen 52.5.138.94 und 52.1.30.122.

Netzwerkanforderungen für Android Enterprise

Weitere Informationen zu den ausgehenden Verbindungen beim Einrichten von Netzwerkumgebungen für Android Enterprise finden Sie im Google-Hilfeartikel Android Enterprise Network Requirements.

Portanforderungen für XenMobile

Die folgenden Zielhosts müssen vom Netzwerk erreichbar sein, um ein Managed Google Play-Unternehmen zu erstellen und auf den Managed Google Play iFrame zuzugreifen. Google hat den Managed Google Play iFrame für EMM-Entwickler freigegeben, um die Suche und Genehmigung von Apps zu vereinfachen. Um Managed Play iFrame verwenden zu können, muss der Browser, von dem aus Sie auf die XenMobile-Konsole zugreifen, Zugriff auf Google Play haben.

Zielhost	**Port**	**Beschreibung**
play.google.com	TCP/443	Wird für die Anmeldung an Google Play Store und Play Enterprise verwendet
*.googleapis.com	TCP/443	Wird für Google Mobile Management, Google APIs, Google Play Store APIs verwendet
accounts.youtube.com, accounts.google.com	TCP/443	Für die Kontoauthentifizierung
apis.google.com	TCP/443	Für GCM und andere Google-Webdienste

Zielhost	Port	Beschreibung
ogs.google.com	TCP/443	Für iFrame-UI-Elemente
notifications.google.com	TCP/443	Für Desktop- und Mobilbenachrichtigungen
fonts.googleapis.com, *.gstatic.com, *.googleusercontent.com	TCP/443	Für benutzergenerierte Google Fonts-Inhalte. Zum Beispiel die App-Symbole im Store
cri.pki.goog, ocsp.pki.goog	TCP/443	Wird für die Zertifikatvalidierung verwendet

Skalierbarkeit und Leistung

January 5, 2022

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-Bereitstellungen.

“Skalierbarkeit” bedeutet in diesem Zusammenhang die Fähigkeit registrierter Geräte, zeitgleich eine Wiederverbindung mit der Bereitstellung herzustellen.

- *Skalierbarkeit* ist die maximale Anzahl registrierter Geräte in der Bereitstellung.
- *Anmelderate* ist die maximale Rate der Wiederverbindungen vorhandener Geräte mit der Bereitstellung.

Die Daten in diesem Artikel sind aus Tests von Bereitstellungen einer Größenordnung von 10.000 bis 75.000 Geräten abgeleitet. Bei den Tests wurden mobile Geräte mit bekannten Arbeitslasten verwendet.

Alle Tests wurden mit XenMobile Enterprise Edition durchgeführt.

Außerdem wurde Citrix Gateway 8200 eingesetzt. Ein Citrix ADC-Gerät mit einer ähnlichen oder mehr Kapazität sollte ein ähnliches oder höheres Maß an Skalierbarkeit und Leistung erzielen.

Nachfolgend finden Sie eine Zusammenfassung des Skalierbarkeits-Testergebnisses.

Zusammenfassung des Skalierbarkeits-Testergebnisses (Bereitstellungen von bis zu 75.000 Geräten)

Anmelderate (Wiederverbindungsrate vorhandener Benutzer): bis zu 9.375 Geräte pro Stunde

Verwendete Konfiguration:

- Citrix Gateway
- MPX 8200
- XenMobile Enterprise Edition
- XenMobile Server-Cluster mit 7 Knoten
- Datenbank: externe Microsoft SQL Server-Datenbank

Testergebnis nach Gerätezahl und Hardwarekonfiguration

Anzahl der Geräte	12.500	30.000	60.000	75.000
Wiederverbindung vorhandener Geräte pro Stunde	1.250	3750	7500	9.375
XenMobile Server – Modus	Eigenständig	Cluster	Cluster	Cluster
XenMobile Server – Cluster	Nicht zutreffend	3	5	7
XenMobile Server – virtuelles Gerät	Speicher = 8 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 = 4 GB RAM; vCPUs = 2	Speicher = 8 GB RAM; vCPUs = 4	Speicher = 16 GB RAM; vCPUs = 4	Speicher = 16 GB RAM; vCPUs = 4
Externe Microsoft SQL Server-Datenbank	Speicher = 8 GB RAM; vCPUs = 4	Speicher = 16 GB RAM; vCPUs = 8	Speicher = 24 GB RAM; vCPUs = 16	Speicher = 24 GB RAM; vCPUs = 16

Skalierbarkeitsprofil

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 und SaaS	20	20
Aktionen	50	
Bereitstellungsgruppen	20	
Active Directory-Gruppen pro Bereitstellungsgruppe	10	
SQL		
Anzahl der Datenbanken	1	

Geräteverbindungen und App-Aktivitäten

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 Geräte bei der Wiederverbindung alle geltenden Sicherheitsrichtlinien abrufen und den XenMobile Server-Knoten so einer höheren Last als normal aussetzen. Bei nachfolgenden Wiederverbindungen werden nur geänderte oder neue Richtlinien per Push auf iOS-Geräten bereitgestellt, sodass die Last auf den XenMobile Server-Knoten 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 Reference Architecture for On-Premises Deployments im Abschnitt “Core MAM+MDM Reference Architecture”.

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 12.000 Geräte gleichzeitig.

Lizenzierung

January 5, 2022

> **Wichtig:**
>
> Das Zurückgeben und Ändern von Citrix Lizenzen hat sich zum 4. November 2020 geändert. Informationen zu den Änderungen am Portal “Manage Licenses” auf Citrix.com und “My Licensing Tools” in Partner Central finden Sie im Citrix Support-Artikel https://support.citrix.com/article/CTX285157.

Bei XenMobile wird die Citrix Lizenzierung zum Verwalten von Lizenzen verwendet. XenMobile Server und Citrix Gateway erfordern eine Lizenz.

Weitere Informationen zur Citrix Gateway-Lizenzierung finden Sie in der Citrix Gateway-Dokumentation. Informationen über die Citrix Lizenzierung finden Sie unter The Citrix Licensing System.

Nach dem Erwerb von XenMobile Server 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.

Anforderungen

- Aktualisieren Sie den Citrix Lizenzserver auf 11.16.x oder höher, bevor Sie die aktuelle Version von XenMobile Server installieren. Ältere Versionen des Lizenzservers unterstützt die aktuelle Version von XenMobile nicht.
- 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.
- 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 ein Backup der Konfigurationsdatei speichern, sind alle Lizenzdateien darin enthalten. Wenn Sie jedoch XenMobile erneut installieren, ohne zuvor die Konfigurationsdatei zu sichern, brauchen Sie die Originallizenzdateien.

Informationen zur XenMobile-Lizenzierung

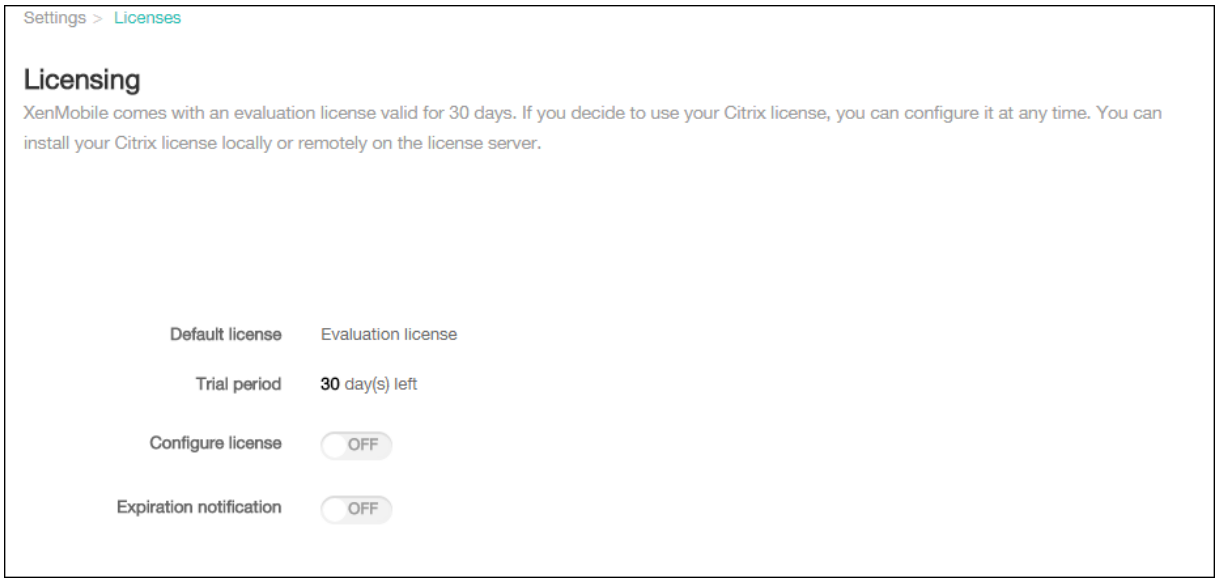
Ohne Lizenz kann XenMobile zu Evaluierungszwecken voll funktionsfähig für einen Zeitraum von 30 Tagen ausgeführt werden. Der Testmodus ist nur einmal möglich, der 30-tägige Kulanzzeitraum beginnt mit der Installation von XenMobile. Der Zugriff auf die XenMobile-Webkonsole ist nie gesperrt, unabhängig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

So finden Sie die Lizenzierungsseite in der XenMobile-Konsole

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



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

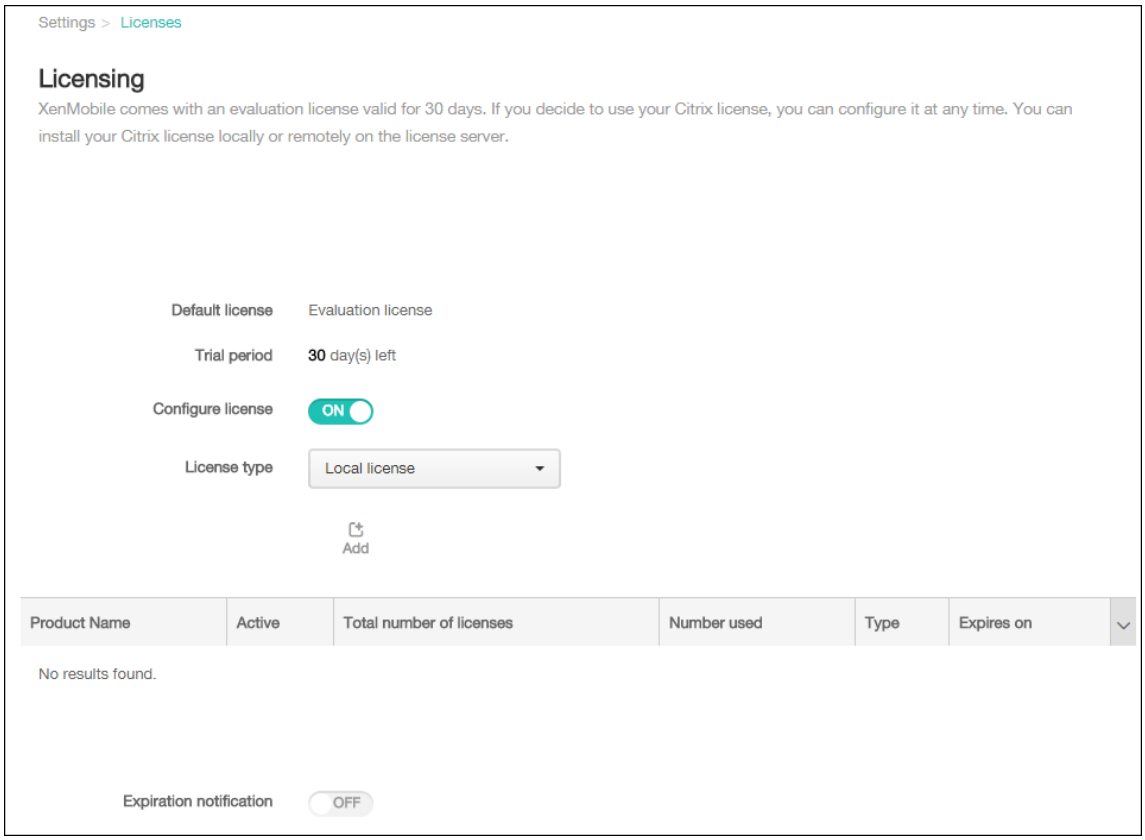
Hinzufügen einer lokalen Lizenz

Werden neue Lizenzen hinzugefügt, erscheinen sie in der Tabelle. Die zuerst hinzugefügte Lizenz wird automatisch aktiviert. Wenn Sie mehrere Lizenzen derselben Kategorie (z. B. Enterprise) und desselben Typs hinzufügen, werden diese in einer einzigen Tabellenzeile angezeigt. In diesen Fällen verstehen sich die Angaben unter **Gesamtanzahl Lizenzen** und **Anzahl verwendet** in Kombination als Gesamtzahl der Lizenzen. Das Datum unter **Ablauf am** ist das Ablaufdatum der aktuellsten Lizenz.

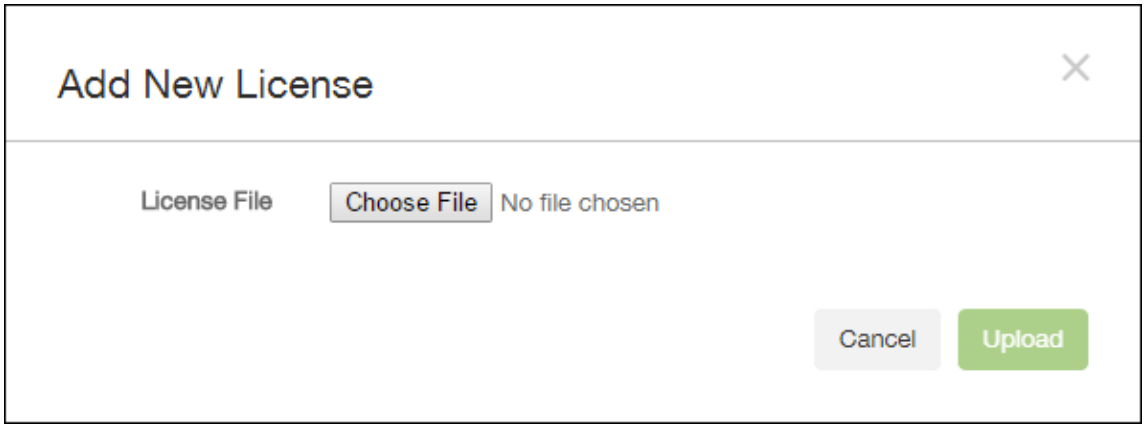
Sie können alle lokalen Lizenzen über die XenMobile-Konsole verwalten.

1. Beziehen Sie eine Lizenzdatei über den Simple License Service, die License Administration Console oder direkt über Ihr Konto auf Citrix.com. Weitere Informationen finden Sie in der Dokumentation für die Citrix Lizenzierung.
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.

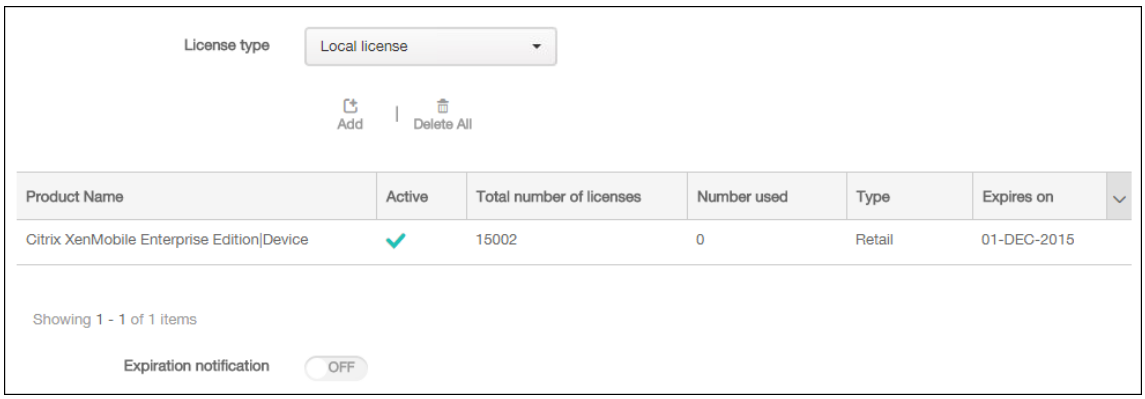
4. Legen Sie für **Lizenz konfigurieren** den Wert **Ein** fest. Die Liste **Lizenztyp**, die Schaltfläche **Hinzufügen** und die Tabelle **Lizenzierung** werden angezeigt. Die Tabelle **Lizenzierung** enthält die Lizenzen, die Sie mit XenMobile verwendet haben. Wenn Sie noch keine Citrix Lizenz hinzugefügt 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 zum Speicherort der Lizenzdatei.
7. Klicken Sie auf **Upload**. Die Lizenz wird lokal hochgeladen und in der Tabelle angezeigt.



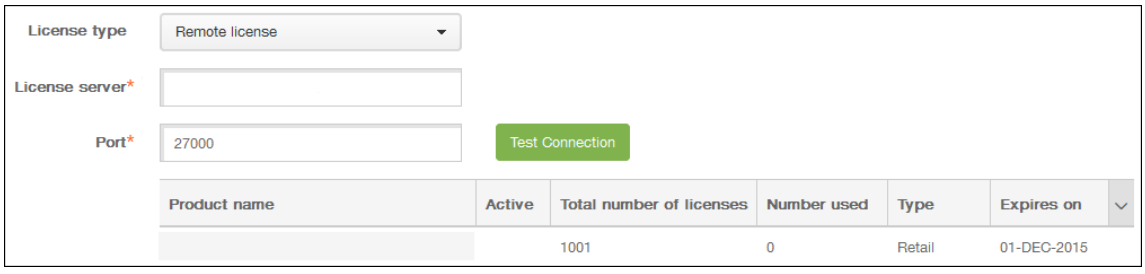
8. Wenn die Lizenz in der Tabelle auf der Seite **Lizenzierung** angezeigt wird, aktivieren Sie sie. Ist dies die erste Lizenz in der Tabelle, wird sie automatisch aktiviert.

Hinzufügen einer Remote-Lizenz

Verwenden Sie den Remoteserver der Citrix Lizenzierung zum Verwalten *aller* Lizenzierungsaktivitäten. Weitere Informationen finden Sie unter Lizenzieren des Produkts.

1. Importieren Sie das Lizenzserver-Zertifikat in XenMobile Server (**Einstellungen > Zertifikate**).
2. In der Standardeinstellung ist die Hostnamenüberprüfung für ausgehende Verbindungen mit Ausnahme des Microsoft PKI-Servers aktiviert. Wenn die Hostnamenüberprüfung Fehler in der Bereitstellung verursacht, ändern Sie die Servereigenschaft **disable.hostname.verification** in **True**. Der Standardwert dieser Eigenschaft ist **false**.

   Wenn die Überprüfung des Hostnamens fehlschlägt, enthält das Serverprotokoll Fehler wie z. B. “Unable to connect to the volume purchase Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”.
3. Legen Sie auf der Seite **Lizenzierung** den Wert für **Lizenz konfigurieren** auf **Ein** fest. Die Liste **Lizenztyp**, die Schaltfläche **Hinzufügen** und die Tabelle **Lizenzierung** werden angezeigt. Die Tabelle **Lizenzierung** enthält die Lizenzen, die Sie mit XenMobile verwendet haben. Wenn Sie noch keine Citrix Lizenz hinzugefügt haben, ist die Tabelle leer.
4. Legen Sie für **Lizenztyp** den Wert **Remotelizenz** fest. Die Schaltfläche **Hinzufügen** wird durch die Felder **Lizenzserver** und **Port** und die Schaltfläche **Verbindung testen** ersetzt.

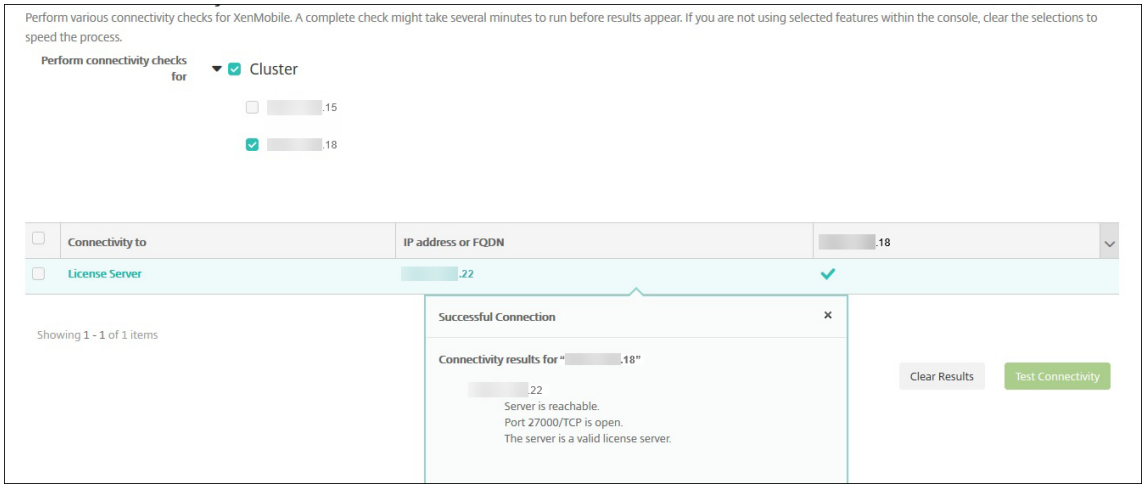


5. Konfigurieren Sie folgende Einstellungen:
   - **Lizenzserver:** Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Remoteservers für die Lizenzierung ein.
   - **Port:** Übernehmen Sie den Standardport oder geben Sie die Portnummer für die Kommunikation mit dem Lizenzserver ein.
6. 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, bestätigt XenMobile Folgendes:

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

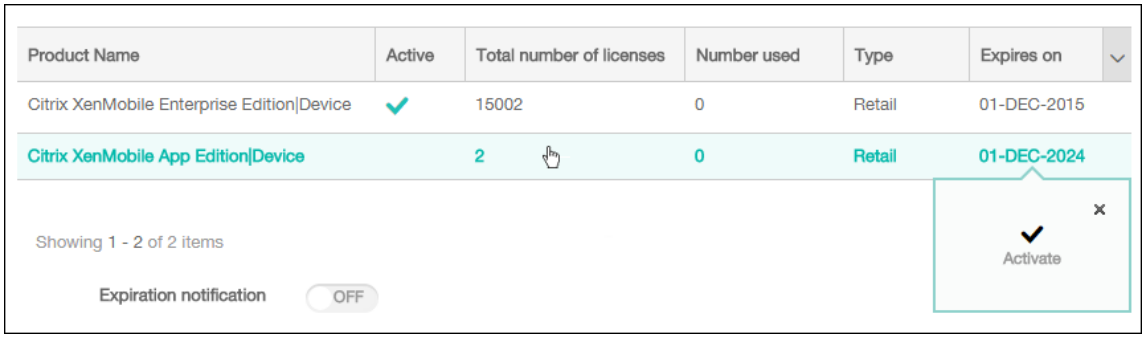
   Kann die Verbindung nicht hergestellt werden, lesen Sie die angezeigte Fehlermeldung, nehmen Sie die erforderlichen Korrekturen vor und klicken Sie dann erneut auf **Verbindung testen**.



Aktivieren einer anderen Lizenz

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

1. Klicken Sie auf der Seite **Lizenzierung** in der **Lizenzierungstabelle** auf die Zeile der Lizenz, die Sie aktivieren möchten. Am Zeilenende wird **Aktivieren** zur Bestätigung eingeblendet.



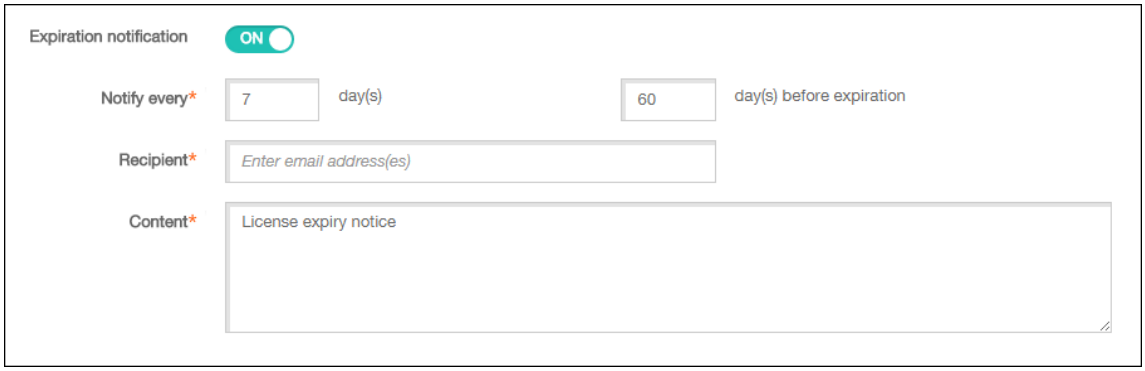
2. Klicken Sie auf **Aktivieren**. Das Dialogfeld **Aktivieren** wird angezeigt.
3. Klicken Sie auf **Aktivieren**. Die ausgewählte Lizenz wird aktiviert.

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

Einrichten einer automatischen Ablaufbenachrichtigung

Nach Aktivierung einer Remote- oder lokalen Lizenz können Sie XenMobile so konfigurieren, dass Sie oder eine andere Person 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 folgende 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, die dem Benutzer angezeigt wird.

3. Klicken Sie auf **Speichern**. Gemäß Ihren Einstellungen 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-Compliance

January 5, 2022

Die FIPS-Norm (Federal Information Processing Standard) wird vom US-Institut für Normung (National Institute of Standards and Technologies, NIST) herausgegeben. FIPS beschreibt die Sicherheitsanforderungen für kryptographische Module in Sicherheitssystemen. FIPS 140-2 ist die zweite Version dieser Norm. Informationen zu vom NIST validierten FIPS 140-Modulen finden Sie unter NIST Computer Security Resource Center.

> **Wichtig:**
>
> - Sie können den XenMobile FIPS-Modus nur bei der ersten Installation aktivieren.
> - XenMobile für die Mobilgeräteverwaltung, XenMobile für die Verwaltung mobiler Apps und XenMobile MDM+MAM 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-validierte kryptographische Module von Citrix und Apple verwendet. Unter Android werden für alle kryptographischen Vorgänge mit ruhenden Daten FIPS-validierte die kryptographischen Module der Plattform verwendet, die vom Gerätehersteller bereitgestellt werden. Weitere Informationen zu den Modulen der Gerätehersteller erhalten Sie von Ihrem Citrix Mitarbeiter.

Für alle kryptographischen Vorgänge an ruhenden und in der Übertragung befindlichen Daten für die Mobilgeräteverwaltung (MDM) auf unterstützten Windows-Geräten werden FIPS-validierte kryptographische Module verwendet.

Für alle kryptographischen Vorgänge an ruhenden und in der Übertragung befindlichen Daten in XenMobile MDM werden FIPS-validierte kryptographische Module verwendet. Bei allen ruhenden und in der Übertragung befindlichen Daten für MDM-Datenflüsse werden von Ende zu Ende FIPS-kompatible kryptografische Module verwendet. Diese umfasst die oben beschriebenen kryptografischen Vorgänge für Mobilgeräte sowie zwischen Mobilgeräten und Citrix Gateway.

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

Sprachunterstützung

November 10, 2020

Mobile Produktivitätsapps und die XenMobile-Konsole sind für Englisch und für andere Sprachen ausgelegt. Diese Unterstützung umfasst erweiterte 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 https://support.citrix.com/article/CTX119253.

Dieser Artikel enthält eine Liste der in der aktuellen Version von XenMobile unterstützten Sprachen.

XenMobile-Konsole und das Selbsthilfeportal

- Französisch
- Deutsch
- Spanisch
- Japanisch
- Koreanisch
- Portugiesisch
- Vereinfachtes Chinesisch

Mobile Produktivitätsapps

Ein X bedeutet, dass die App in der jeweiligen Sprache zur Verfügung steht.

iOS und Android

Sprache	Secure Hub	Secure Mail	Secure Web	QuickEdit
Japanisch	X	X	X	X
Vereinfachtes Chinesisch	X	X	X	X
Traditionelles Chinesisch	X	X	X	X
Französisch	X	X	X	X
Deutsch	X	X	X	X
Spanisch	X	X	X	X
Koreanisch	X	X	X	X

Sprache	Secure Hub	Secure Mail	Secure Web	QuickEdit
Portugiesisch	X	X	X	X
Niederländisch	X	X	X	X
Italienisch	X	X	X	X
Dänisch	X	X	X	X
Schwedisch	X	X	X	X
Hebräisch	X	X	X	Nur iOS
Arabisch	X	X	X	X
Russisch	X	X	X	X
Türkisch	X	X	Nur Android	-
Polnisch	X	X	X	-

Windows

Sprache	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

Unterstützung für Sprachen mit Schreibrichtung von rechts nach links

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.

App	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X

App	iOS	Android
QuickEdit	X	X

Installation und Konfiguration

January 5, 2022

Vorbereitung

Die nachfolgende Prüfliste enthält die Voraussetzungen und Einstellungen für die Installation von XenMobile im eigenen Rechenzentrum. 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 die gesamte XenMobile-Umgebung finden Sie im XenMobile-Bereitstellungshandbuch.

Installationsanweisungen finden Sie unter Installieren von XenMobile weiter unten.

Prüfliste zur Installationsvorbereitung

Grundlegende Netzwerkverbindung

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 und Citrix Gateway	
Notieren Sie die öffentliche und lokale IP-Adresse.		
Sie brauchen diese IP-Adressen beim Konfigurieren der Firewall für die Netzwerkadressübersetzung (NAT).	XenMobile Citrix Gateway	
Notieren Sie die Subnetzmaske.	XenMobile und Citrix Gateway	
Notieren Sie die DNS-IP-Adressen.	XenMobile und Citrix Gateway	
Notieren Sie die WINS-Server-IP-Adressen (falls zutreffend).	Citrix Gateway	
Notieren Sie den Hostnamen von Citrix Gateway.	Citrix Gateway	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 Citrix Gateway konfigurieren.	Citrix 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 Citrix Gateway konfiguriert ist	Citrix Gateway	
Einen externen DNS-Eintrag für Citrix Gateway	Citrix 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.	Citrix Gateway	Zum Konfigurieren des Benutzernamens für den Web-Proxy können Sie den sAMAccountName oder den UPN (User Principal Name) verwenden	XenMobile und Citrix Gateway	
Notieren Sie die IP-Adresse des Standardgateways.	XenMobile und Citrix Gateway	
Notieren Sie die System-IP-Adresse (NSIP) und Subnetzmaske.	Citrix Gateway	
Notieren Sie die Subnetz-IP-Adresse (NSIP) und Subnetzmaske.	Citrix Gateway	
Notieren Sie die IP-Adresse und den FQDN des virtuellen Citrix Gateway-Servers aus dem Zertifikat. Wenn Sie mehrere virtuelle Server konfigurieren müssen, notieren Sie alle virtuellen IP-Adressen und FQDNs aus den Zertifikaten.	Citrix Gateway	
Notieren Sie die internen Netzwerke, auf die Benutzer über Citrix Gateway zugreifen können. Beispiel: 10.10.0.0/24 Geben Sie alle internen Netzwerke und Netzwerksegmente an, auf die Benutzer zugreifen müssen, wenn sie eine Verbindung mit Secure Hub oder dem Citrix Gateway Plug-In herstellen und Split-Tunneling auf “Ein” gesetzt ist.	Citrix Gateway	
Stellen Sie sicher, dass zwischen XenMobile Server, Citrix Gateway, dem externen Microsoft SQL Server-Computer und dem DNS-Server Netzwerkkonnektivität besteht.	XenMobile und Citrix Gateway	

Lizenzierung

Für XenMobile müssen Sie Lizenzierungsoptionen für Citrix Gateway und XenMobile erwerben. Informationen über die Citrix Lizenzierung finden Sie unter The Citrix Licensing System.

Voraussetzung	Komponente	Speicherort notieren
Universelle Lizenzen erhalten Sie auf der Citrix Website. Weitere Informationen finden Sie unter “Lizenzierung” in der Dokumentation zu Citrix Gateway.	Citrix Gateway, XenMobile und Citrix Lizenzserver	

Zertifikate

XenMobile und Citrix 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
———	———	—–
Beziehen und installieren Sie die erforderlichen Zertifikate.	XenMobile und Citrix Gateway	

Ports

Öffnen Sie Ports, um die Kommunikation mit XenMobile-Komponenten zu ermöglichen.

Voraussetzung	Komponente	Hinweise
Öffnen der Ports für XenMobile	XenMobile und Citrix Gateway	

Datenbank

XenMobile erfordert eine konfigurierte Datenbankverbindung. Das XenMobile-Repository erfordert eine Microsoft SQL Server-Datenbank in einer der unterstützten Versionen, die unter Systemanforderungen und Kompatibilität aufgeführt sind. Citrix empfiehlt die Remote-Verwendung von Microsoft SQL. PostgreSQL wird mit XenMobile ausgeliefert. Verwenden Sie PostgreSQL lokal oder remote *ausschließlich* in Testumgebungen.

XenMobile verwendet standardmäßig den jTDS-Datenbanktreiber. Weitere Informationen zur Verwendung des Microsoft JDBC-Treibers für on-premises Installationen von XenMobile Server finden Sie unter SQL Server-Treiber.

Voraussetzung	Komponente	Hinweise
IP-Adresse und Port des Microsoft SQL Server-Computers. Das in XenMobile zu verwendende SQL Server-Dienstkonto muss die Rollenberechtigung “DBcreator” aufweisen.	XenMobile	

Active Directory-Einstellungen

Voraussetzung	Komponente	Hinweise
————	———	————
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 und Citrix Gateway
Notieren Sie den Domänennamen für Active Directory.	XenMobile und Citrix Gateway
Notieren Sie das Active Directory-Dienstkonto (erfordert Benutzer-ID, Kennwort und Domänenalias).
XenMobile verwendet das Dienstkonto für Active Directory-Abfragen.	XenMobile und Citrix Gateway	
Notieren Sie den Benutzerbasis-DN. Dies ist die Verzeichnisebene, die Benutzer enthält. Beispiel: `cn=users,dc=ace,dc=com`. Citrix Gateway und XenMobile verwenden dies für Active Directory-Abfragen.	XenMobile und Citrix Gateway	
Notieren Sie den Gruppenbasis-DN. Dies ist die Verzeichnisebene, die Gruppen enthält. Citrix Gateway und XenMobile verwenden dies für Active Directory-Abfragen.	XenMobile und Citrix Gateway	

Verbindungen zwischen XenMobile und Citrix 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.	Citrix Gateway	
Notieren Sie die Callback-URL.	XenMobile	

Benutzerverbindungen: Zugriff auf Citrix Virtual Apps and Desktops und Citrix Secure Hub

Citrix empfiehlt, dass Sie Einstellungen für Verbindungen zwischen XenMobile und Citrix Gateway und zwischen XenMobile und Secure Hub mit dem Konfigurationsassistenten in Citrix ADC konfigurieren. Sie erstellen einen zweiten virtuellen Server, um Benutzerverbindungen von Citrix Receiver und Web-Browsern zu aktivieren. Sie schaffen eine Verbindung zu Windows-basierten Anwendungen und

virtuellen Desktops in Virtual Apps and Desktops. Citrix empfiehlt, dass Sie auch diese Einstellungen mit dem Konfigurationsassistenten in Citrix ADC konfigurieren.

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

Flussdiagramm für die Bereitstellung von XenMobile

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

1. Systemanforderungen und -kompatibilität
2. Installation und Konfiguration

3 und 4. Prüfliste zur Installationsvorbereitung (in diesem Artikel)

5. Konfigurieren von XenMobile im Eingabeaufforderungsfenster (in diesem Artikel)

6. Konfigurieren von XenMobile in einem Webbrowser (in diesem Artikel)

7. Konfigurieren von Einstellungen für die XenMobile-Umgebung

8. Portanforderungen

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. Vermeiden Sie Zeitzonenprobleme, die beim Synchronisieren der Uhrzeit auf dem XenMobile-Server mit einem Hypervisor auftreten können, indem Sie XenMobile auf einen NTP-Server verweisen lassen. Verwenden Sie hierzu die XenMobile-Befehlszeilenschnittstelle (siehe Optionen für die Befehlszeilenschnittstelle).

Voraussetzungen für XenServer bzw. VMware ESXi: 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.

Voraussetzungen für Hyper-V: 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 R2 mit aktiviertem Hyper-V und aktivierten Rollen auf einem Computer mit ausreichenden Systemressourcen. Beim Installieren der Hyper-V-Rolle müssen Sie die Netzwerkkarten auf dem Server angeben, den Hyper-V zum Erstellen von virtuellen Netzwerken verwenden soll. Sie können einige NICs für den Host reservieren.
- Löschen Sie die Datei Virtual Machines/<*buildspezfische UUID*>.xml.
- Verschieben Sie die Datei Legacy/<*buildspezfische UUID*>.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.

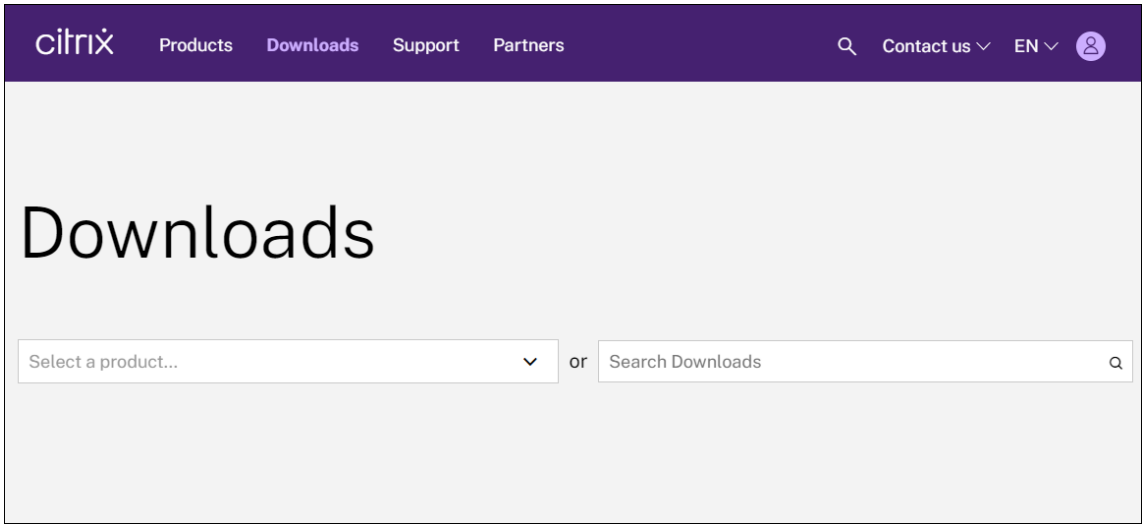
FIPS 140-2-Modus: Zur Installation von XenMobile Server im FIPS-Modus müssen die unter Konfigurieren von FIPS erläuterten Voraussetzungen erfüllt werden.

Download der XenMobile-Produktsoftware

Sie können Produktsoftware von der Citrix Website herunterladen. Melden Sie sich bei der Website an und navigieren Sie über den Link “Downloads” zu der Seite mit der Software, die Sie herunterladen möchten.

Herunterladen der Software für XenMobile

1. Rufen Sie die Citrix Website auf.
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 Produktliste auf **Citrix Endpoint Management (und Citrix XenMobile Server)**. Die Seite “Citrix Endpoint Management (und Citrix XenMobile Server)” wird automatisch angezeigt.



5. Erweitern Sie **XenMobile Server (on-premises)**.

6. Erweitern Sie **Produktsoftware**.
7. Klicken Sie auf **XenMobile Server 10**.
8. Klicken Sie auf **Jump to Download** und wählen Sie das virtuelle Image, das zum Installieren von XenMobile verwendet werden soll. Alternativ scrollen Sie auf der Seite nach unten, um die Schaltfläche **Download File** für das gewünschte Image zu finden.
9. Folgen Sie den Anweisungen auf dem Bildschirm, um die Software herunterzuladen.

Herunterladen der Software für Citrix Gateway

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

1. Rufen Sie die Citrix Website auf.
2. Wenn Sie noch nicht an 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 **Citrix Gateway**.
5. Klicken Sie auf **Go**. Die Seite Citrix Gateway wird angezeigt.
6. Erweitern Sie auf der Seite "Citrix Gateway" die Version von Citrix Gateway, die Sie ausführen.
7. Klicken Sie auf unter **Firmware** auf die Gerätesoftwareversion, die Sie herunterladen möchten.

   > **Hinweis:**
   >
   > Sie können auch **Virtual Appliances** auswählen, um Citrix ADC 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 der gewünschten Version auf **Download** für das gewünschte virtuelle Gerät.
10. Folgen Sie den Anweisungen auf dem Bildschirm, um die Software herunterzuladen.

Konfigurieren von XenMobile für die Erstverwendung

1. Konfigurieren Sie IP-Adresse, Subnetzmaske, Standardgateway, DNS-Server und weitere Einstellungen für XenMobile über die XenCenter- oder vSphere-Befehlszeilenkonsole.

> **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.

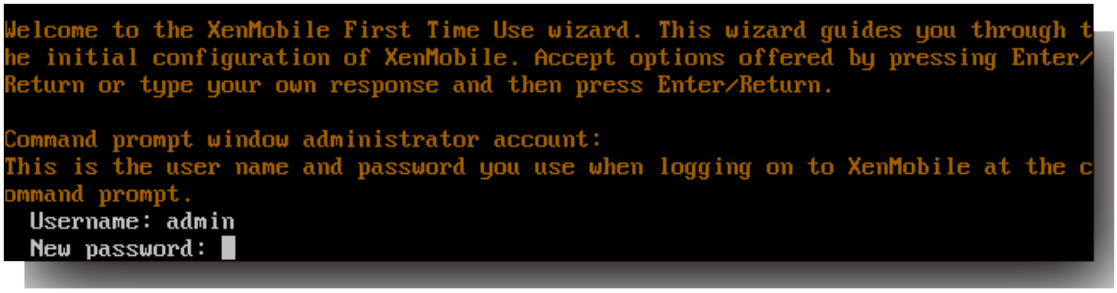
2. Greifen Sie auf die XenMobile-Verwaltungskonsole ausschließlich über den vollqualifizierten Domänennamen von XenMobile Server oder die IP-Adressen des Knotens zu.
3. Melden Sie sich an und folgen Sie den Anweisungen auf den Bildschirmen für die Erstanmeldung.

Konfigurieren von XenMobile im Eingabeaufforderungsfenster

1. Importieren Sie die virtuelle XenMobile-Maschine in Citrix XenServer bzw. VMware ESXi oder Microsoft Hyper-V. Weitere Informationen finden Sie in der Dokumentation zu XenServer bzw. Hyper-V und VMware.
2. Wählen Sie im Hypervisor die importierte XenMobile-VM 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.

   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 acht Zeichen enthalten.
   - Das Kennwort muss mindestens drei der folgenden Komplexitätskriterien erfüllen:
     - Großbuchstaben (A bis Z)
     - Kleinbuchstaben (a bis z)
     - Ziffern (0 bis 9)
     - Sonderzeichen (z. B. ! ## $ %)



Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt.

4. Geben Sie die folgenden Netzwerkinformationen gefolgt von **y** ein, um die Einstellungen zu übergeben:
   a) IP-Adresse von XenMobile Server
   b) Netzmaske
   c) Standardgateway (IP-Adresse des Standardgateways in der DMZ)
   d) Primärer DNS-Server (IP-Adresse des DNS-Servers)
   e) Sekundärer DNS-Server (optional)

> **Hinweis:**
>
> Die in diesem und den folgenden Abbildungen gezeigten Adressen sind nicht funktional und dienen nur als Beispiel.

5. Geben Sie **y** ein, um die Sicherheit zu erhöhen, indem Sie eine zufällige Passphrase zur Verschlüsselung generieren lassen, oder **n**, um eine eigene Passphrase anzugeben. Citrix mit **y** eine zufällige Passphrase zu erzeugen.

   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:**
   >
   > Geben Sie eine eigene Passphrase ein, wenn Sie Ihre Umgebung um weitere Server erweitern möchten. Wenn Sie eine zufällige Passphrase wählen, können Sie sie nicht anzeigen.


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

6. Aktivieren Sie optional FIPS (Federal Information Processing Standard). Einzelheiten zu FIPS finden Sie unter FIPS. Stellen Sie sicher, dass die unter Konfigurieren von FIPS mit XenMobile erläuterten Voraussetzungen erfüllt sind.

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

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

```
Database connection:
  Local or remote [l/r]: r
  Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
  Use SSL [y/n]: n
  Server:          .10
  Port: 5432
  Username: postgres
  Password:
```

   - Es kann eine lokale oder eine remote Datenbank verwendet werden. Geben Sie **l** für lokal oder **r** remote ein.
   - Wählen Sie den Datenbanktyp aus. Geben Sie **mi** für Microsoft SQL oder **p** für PostgreSQL ein.

     Wichtig:

     - Citrix empfiehlt die Remote-Verwendung von Microsoft SQL. PostgreSQL wird mit XenMobile ausgeliefert. Verwenden Sie PostgreSQL lokal oder remote *ausschließlich* in Testumgebungen.
     - Eine Datenbankmigration wird nicht unterstützt. In einer Testumgebung erstellte Datenbanken können nicht in eine Produktionsumgebung übertragen werden.

   - Geben Sie optional **y** ein, damit SSL-Authentifizierung für die Datenbank verwendet wird.
   - Geben Sie den vollqualifizierten Domänennamen (FQDN) des XenMobile-Hostservers ein. Dieser Hostserver wird sowohl für die Geräteverwaltung als auch für die Anwendungsverwaltung eingesetzt.
   - Geben Sie die Datenbankportnummer ein, wenn sie sich von der Standardportnummer unterscheidet. Der Standardport für Microsoft SQL ist 1433, der Standardport für PostgreSQL ist 5432.

- Geben Sie den Benutzernamen des Datenbankadministrators ein.
- Geben Sie das Kennwort des Datenbankadministrators ein.
- Geben Sie den Datenbanknamen ein.
- Drücken Sie die **Eingabetaste**, um die Datenbankeinstellungen zu übergeben.

8. Geben Sie optional **y** ein, 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. Führen Sie das Setup auf allen Clusterknoten aus.

9. Geben Sie den vollqualifizierten Domänennamen (FQDN) von XenMobile Server ein.

10. Drücken Sie die **Eingabetaste**, um die Einstellungen zu übergeben.
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. Geben Sie **y** ein, wenn Sie dasselbe Kennwort für alle Public Key-Infrastruktur-Zertifikate verwenden möchten. Informationen zum XenMobile PKI-Feature finden Sie unter Hochladen von Zertifikaten.


```
The wizard will now generate an internal Public Key Infrastructure (PKI):
 - A root certificate
 - An intermediate certificate to issue device certificates during enrollment
 - An intermediate certificate to issue an SSL certificate
 - An SSL certificate for your connectors
  Do you want to use the same password for all the certificates of the PKI [y]:
  New password:
  Re-enter new password:
```

> **Wichtig:**
>
> Wenn Sie Knoten oder Instanzen von XenMobile in Clustern verwenden möchten, geben Sie identische Kennwörter für die nachfolgenden Knoten an.

14. Geben Sie das neue Kennwort ein und dann zur Bestätigung erneut.

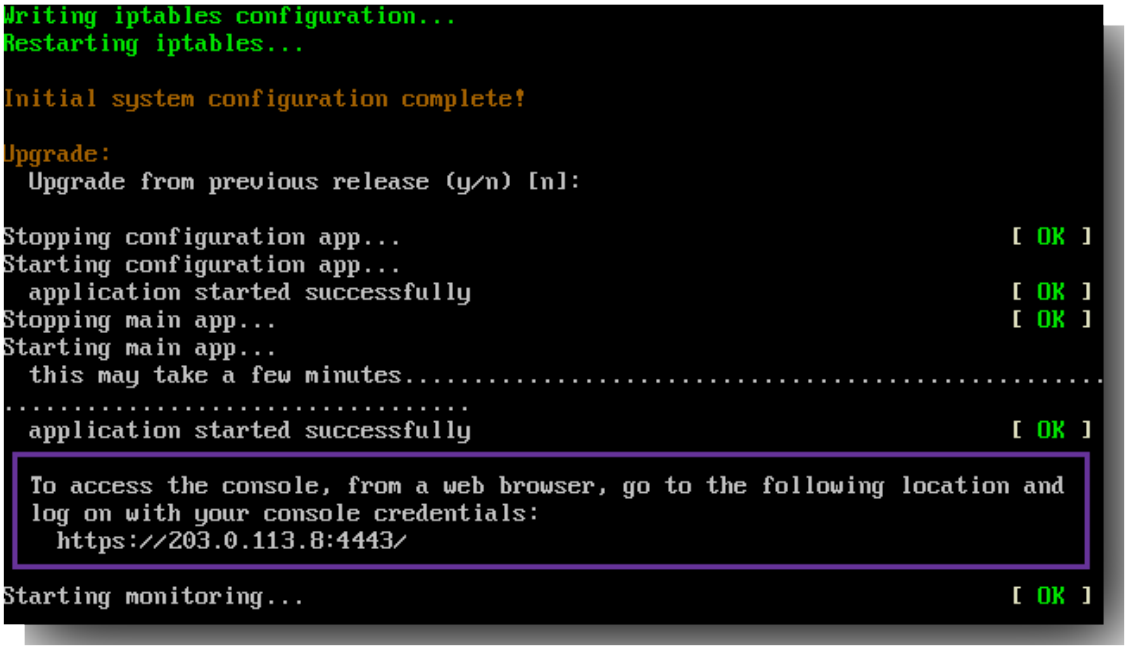
    Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt.

15. Drücken Sie die **Eingabetaste**, um die Einstellungen zu übergeben.
16. Erstellen Sie ein Administratorkonto für die Anmeldung an der XenMobile-Konsole mit einem Webbrowser. Notieren Sie die Anmeldeinformationen für die spätere Verwendung.

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile cons
ole through a web browser.
  Username [administrator]: administrator
  Password:
  Re-enter new password:
```

> **Hinweis:**
>
> Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt.

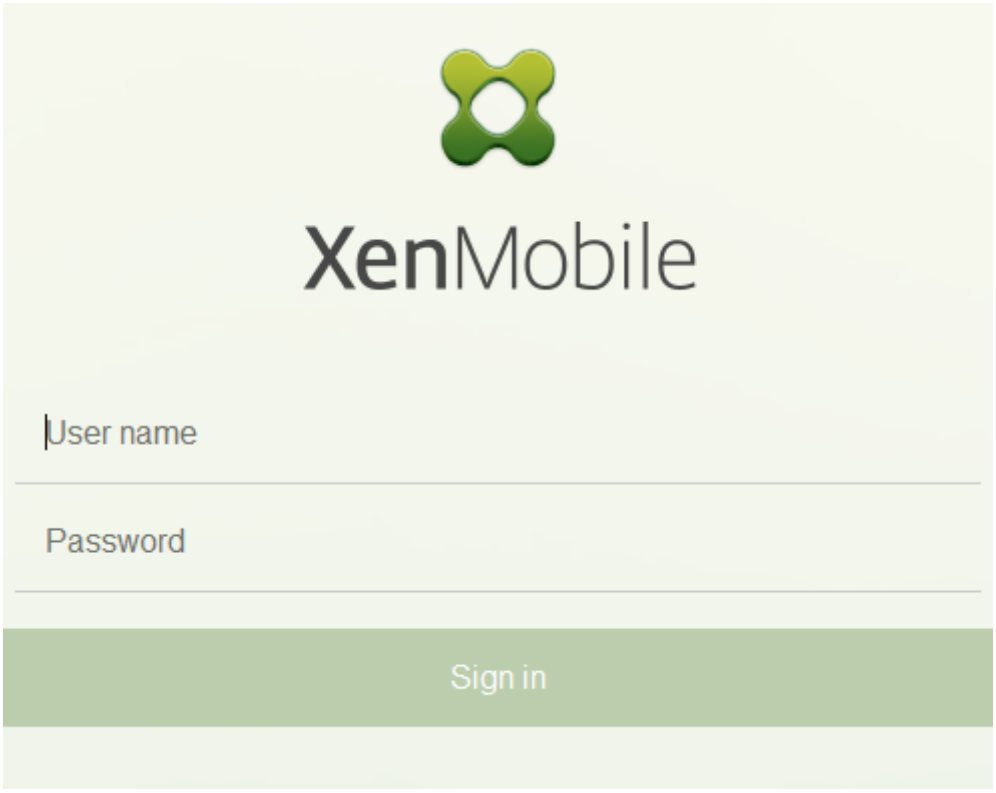
17. Drücken Sie die **Eingabetaste**, um die Einstellungen zu übergeben. Die anfängliche Systemkonfiguration wird gespeichert.
18. Geben Sie zur Beantwortung der Frage, ob es sich um ein Upgrade handelt, **n** ein, da es sich um eine Neuinstallation handelt.
19. Kopieren Sie die vollständige nun angezeigte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



Konfigurieren von XenMobile in einem Webbrowser

Nach Abschließen des erstens 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 **Lizenzierung** 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 **Zertifikate** 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 Citrix Gateway, wenn die Umgebung dies erfordert. Informationen zum Konfigurieren von Citrix Gateway finden Sie unter Citrix Gateway und XenMobile und Configuring Settings for Your XenMobile Environment.

> **Hinweis:**
>
> - Sie können Citrix Gateway am Rand der internen Netzwerks (Intranet) bereitstellen. Dadurch entsteht ein sicherer zentraler Zugriffspunkt auf alle Server, Apps und anderen Netzwerkressourcen im internen Netzwerk. In dieser Bereitstellung müssen alle Remotebenutzer eine Verbindung mit Citrix Gateway herstellen, bevor sie auf Ressourcen im internen Netzwerk zugreifen können.
> - Obwohl Citrix 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. Einzelheiten zur Konfiguration der LDAP-Verbindung finden Sie unter LDAP-Konfiguration.
9. Konfigurieren Sie den Benachrichtigungsserver zum Senden von Nachrichten an Benutzer. Informationen zum Konfigurieren des Benachrichtigungsservers finden Sie unter Benachrichtigungen.

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

Konfigurieren von FIPS in XenMobile

January 5, 2022

Der FIPS-Modus (Federal Information Processing Standards) in XenMobile unterstützt Kunden der US-Regierung, indem für alle Verschlüsselungsvorgänge ausschließlich FIPS 140-2-zertifizierte Bibliotheken verwendet werden. Durch die Installation von XenMobile Server im FIPS-Modus wird sichergestellt, dass alle Daten für den XenMobile-Client und den -Server die Anforderungen von FIPS 140-2 erfüllen. Dies gilt für ruhende Daten und Daten in der Übertragung.

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

- Verwenden Sie externes SQL Server 2014 für die XenMobile-Datenbank. Der SQL Server muss für sichere SSL-Kommunikation konfiguriert sein. Anweisungen zum Konfigurieren der sicheren SSL-Kommunikation mit SQL Server finden Sie unter Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager).
- Für die sichere SSL-Kommunikation installieren Sie ein vertrauenswürdiges SSL-Zertifikat einer renommierten Zertifizierungsstelle (ZS) auf dem SQL Server-Rechner. SQL Server 2014 akzeptiert keine Platzhalterzertifikate. Citrix empfiehlt, dass Sie ein SSL-Zertifikat mit dem FQDN des SQL Servers anfordern.

Konfigurieren des FIPS-Modus

Sie können den FIPS-Modus nur bei der Ersteinrichtung von XenMobile Server aktivieren. Nach der Installation kann FIPS nicht mehr aktiviert werden. Wenn Sie planen, den FIPS-Modus zu verwenden, müssen Sie daher von Anfang XenMobile Server mit dem FIPS-Modus installieren. Bei XenMobile-Clustern muss FIPS außerdem auf allen Clusterknoten aktiviert werden. Im selben Cluster ist keine Kombination aus XenMobile Server-Rechnern mit und ohne FIPS möglich.

Die XenMobile-Befehlszeilenschnittstelle enthält die Option **Toggle FIPS mode**, die nicht zur Verwendung in der Produktion vorgesehen ist. Die Option ist für die Diagnose gedacht und wird auf XenMobile-Produktionsservern nicht unterstützt.

1. Aktivieren Sie **FIPS mode** bei der Erstinstallation.
2. Laden Sie das Stammzertifizierungsstellenzertifikat für den SQL Server hoch.
3. Geben Sie den Namen und den Port des SQL Servers sowie die Anmeldeinformationen für den SQL Server und den Namen der für XenMobile zu erstellenden Datenbank an.

   > **Hinweis:**
   >
   > Sie können eine SQL-Anmeldung oder ein Active Directory-Konto für den Zugriff auf den SQL Server verwenden. Den Anmeldeinformationen muss die Rolle “DBcreator” zugewiesen sein.

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 wird der Text **In FIPS Compliant Mode** angezeigt.

Importieren von Zertifikaten

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

Voraussetzungen für SQL

1. Die Verbindung zwischen der SQL-Instanz und XenMobile muss sicher sein und es muss sich um SQL Server Version 2012 oder SQL Server 2014 handeln. Informationen zum Schützen der Verbindung finden Sie unter Aktivieren der SSL-Verschlüsselung für eine Instanz von SQL Server mit der Microsoft Management Console.

2. Wenn der Dienst nicht ordnungsgemäß neu gestartet wird, 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 nach dem importierten 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 die **MMC** und starten Sie den SQL-Dienst.
3. Stellen Sie sicher, dass der SQL-Dienst ordnungsgemäß 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 **Regeln beim Fehlschlagen der Auftragsüberwachung**.
6. Stellen Sie sicher, dass die Zertifikatdatei (.cer) nicht blockiert ist.
7. Navigieren Sie vom lokalen Server aus in einem Browser zum Speicherort der CER-Datei: `https://localhost/certname.cer`. Der Text des Stammzertifikats wird im Browser angezeigt.
8. Wenn das Stammzertifikat nicht im Webbrowser angezeigt wird, stellen Sie wie folgt sicher, dass ASP auf dem IIS-Server aktiviert ist.

a) Öffnen Sie den Server-Manager.

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

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

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

9. Gehen Sie zu `https://localhost/cert.cer`.

   Weitere Informationen finden Sie unter Webserver (IIS).

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

Importieren des Stammzertifikats während der FIPS-Erstkonfiguration

Wenn Sie die Erstkonfiguration von XenMobile in der Befehlszeilenkonsole durchführen, müssen Sie die folgenden Einstellungen festlegen, um das Stammzertifikat zu importieren. Installationsanweisungen 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: `https://<FQDN of IIS server>/cert.cer`
- Server: *FQDN des SQL Server-Computers*
- Port: 1433
- User name: Dienstkonto, das die Berechtigungen zum Erstellen der Datenbank besitzt (`domain\username`).
- Password: Das Kennwort für das Dienstkonto.
- Datenbankname: ein Name Ihrer Wahl.

Aktivieren des FIPS-Modus auf Mobilgeräten

Standardmäßig ist der FIPS-Modus auf Mobilgeräten deaktiviert. Legen Sie zum Aktivieren des FIPS-Modus unter **Einstellungen > Clienteigenschaften** die Eigenschaft **Enable FIPS Mode** auf **true** fest. Weitere Informationen finden Sie unter Clienteigenschaften.

Konfigurieren von Clustering

January 5, 2022

Zum Konfigurieren von Clustering konfigurieren Sie die folgenden beiden virtuellen IP-Adressen für den Lastausgleich in Citrix ADC.

- **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 Citrix Gateway mit XenMobile-Knoten, die in einem Cluster konfiguriert sind. In XenMobile wird standardmäßig der gesamte Netzwerkverkehr von Citrix Gateway an die virtuelle IP-Adresse für den Lastausgleich auf Port 8443 geleitet.

In diesem Artikel wird erläutert, wie Sie eine neue XenMobile-VM (virtuelle Maschine) erstellen und sie mit einer vorhandenen VM zusammenführen. Dadurch wird ein Clustersetup erstellt.

Voraussetzungen

- Sie haben den erforderlichen XenMobile-Knoten vollständig konfiguriert.
- Konfigurieren Sie NTP auf allen Clusterknoten und für die XenMobile-Datenbank. Das Clustering funktioniert nur dann ordnungsgemäß, wenn alle Server dieselbe Zeiteinstellung haben.
- Eine öffentliche IP-Adresse für MDM L-Band und eine private IP-Adresse für MAM.
- Serverzertifikate
- Sie haben eine freie IP für die virtuelle IP-Adresse von Citrix Gateway.
- Bei XenMobile-Bereitstellung im Cluster und im Nur-MDM- oder Enterprise-Modus (MDM+MAM): Passen Sie Ihre Citrix ADC-Konfiguration für den Lastausgleich an und verwenden Sie die **Persistenz "Quell-IP"** für alle Citrix ADC MDM-Load Balancer, also alle virtuellen Server, die für die Ports 8443 und 443 eingerichtet sind. Führen Sie diese Konfiguration vor dem Upgrade von Benutzergeräten auf iOS 11 durch. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX227406 im Citrix Knowledge Center.
- Um Apps aus dem XenMobile Store auf Geräten mit iOS 11 zu installieren, müssen Sie Port 80 auf dem XenMobile Server aktivieren.

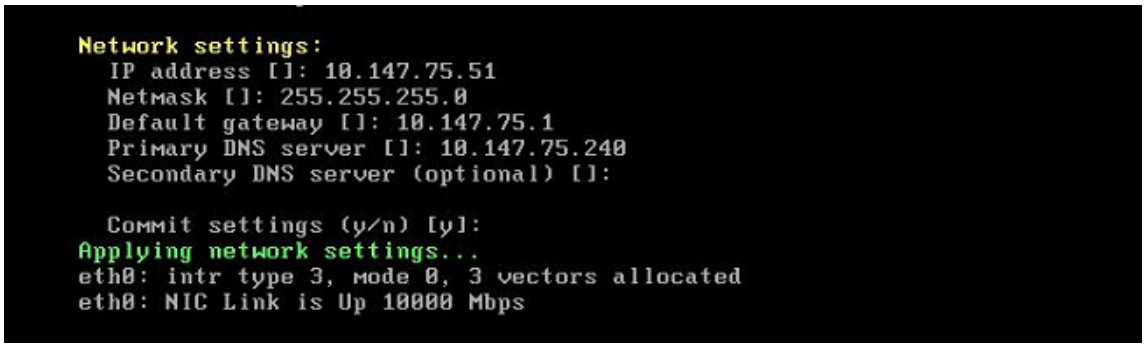
Referenzarchitekturdiagramme für XenMobile 10.x in Clusterkonfigurationen finden Sie unter Architektur.

Installieren der XenMobile-Clusterknoten

Basierend auf der Anzahl der erforderlichen Knoten erstellen Sie 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.

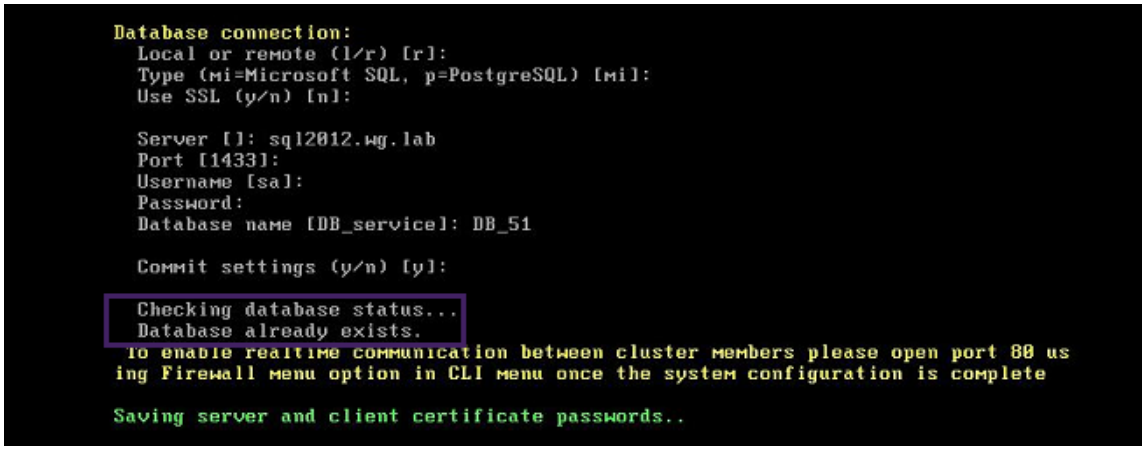
2. Geben Sie Einstellungen für die Netzwerkkonfiguration gemäß der folgenden Abbildung an.



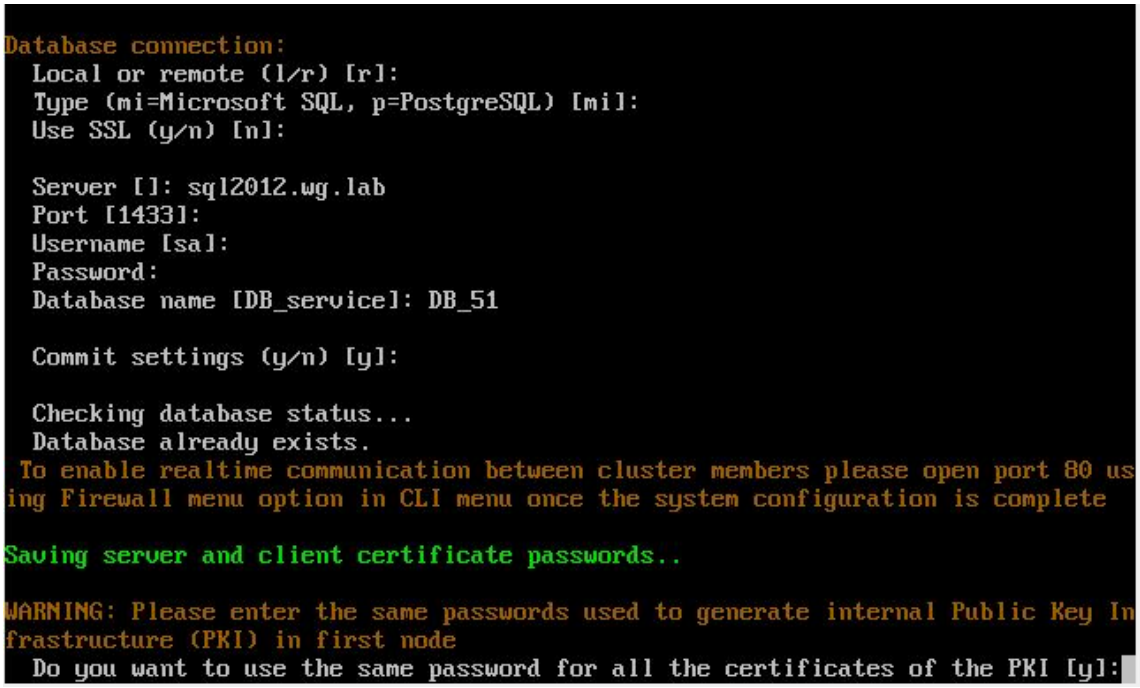
3. Wenn Sie das Standardkennwort für den Schutz von Daten verwenden möchten, geben Sie **y** ein. Ansonsten geben Sie **n** gefolgt von einem neuen Kennwort ein.

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

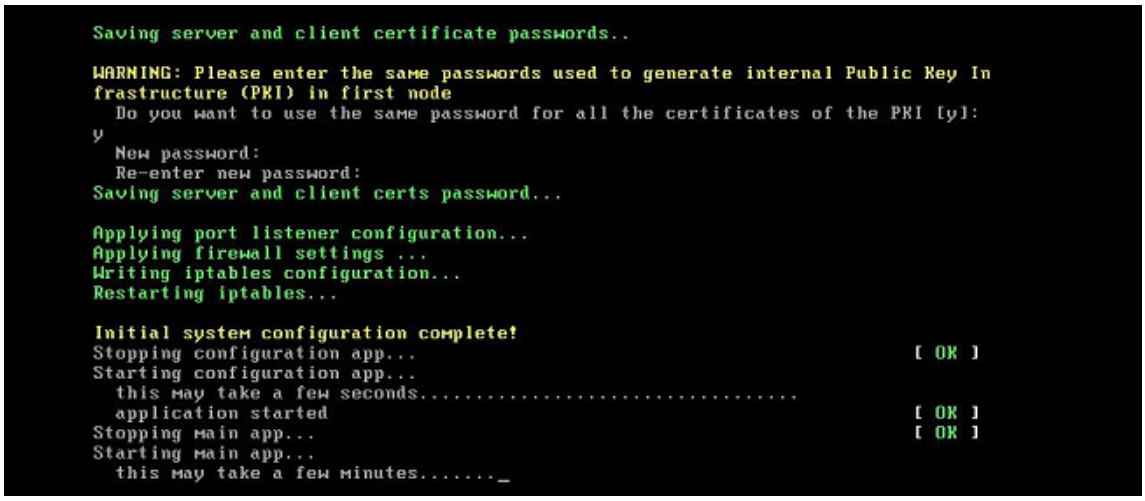
5. Konfigurieren Sie die Datenbank so, dass auf dieselbe Datenbank verwiesen wird wie bei der zuvor vollständig konfigurierten VM. Es wird gemeldet, dass die Datenbank bereits vorhanden ist.



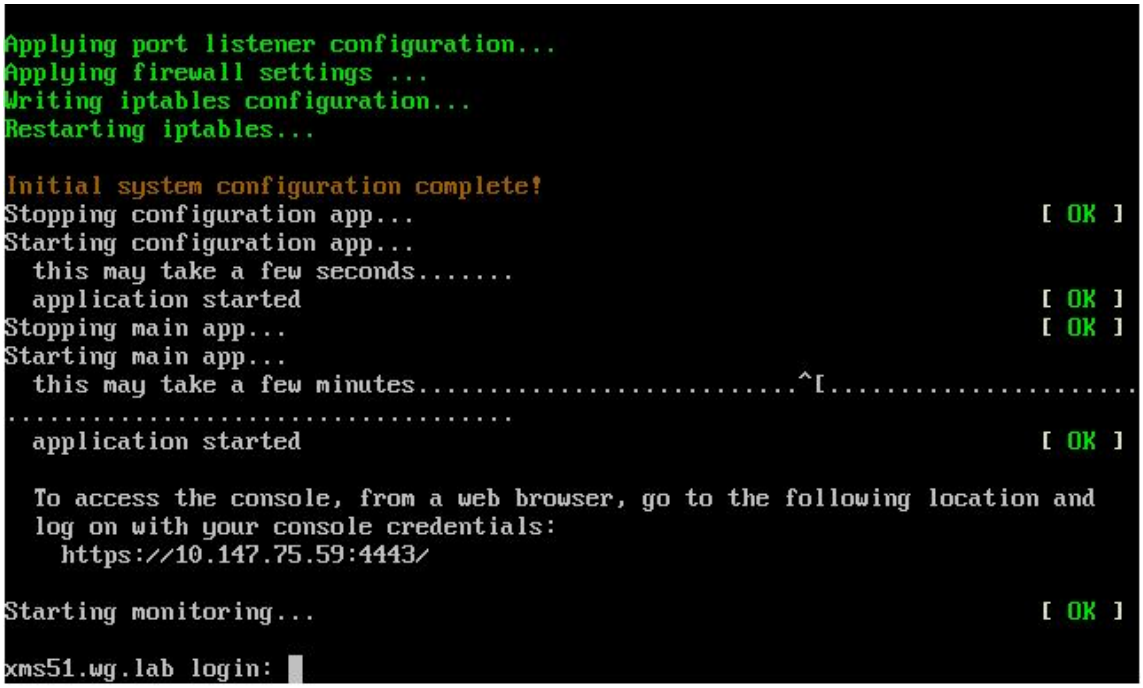
6. Geben Sie die gleichen Kennwörter für die Zertifikate ein, die Sie für die erste VM angegeben haben.



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



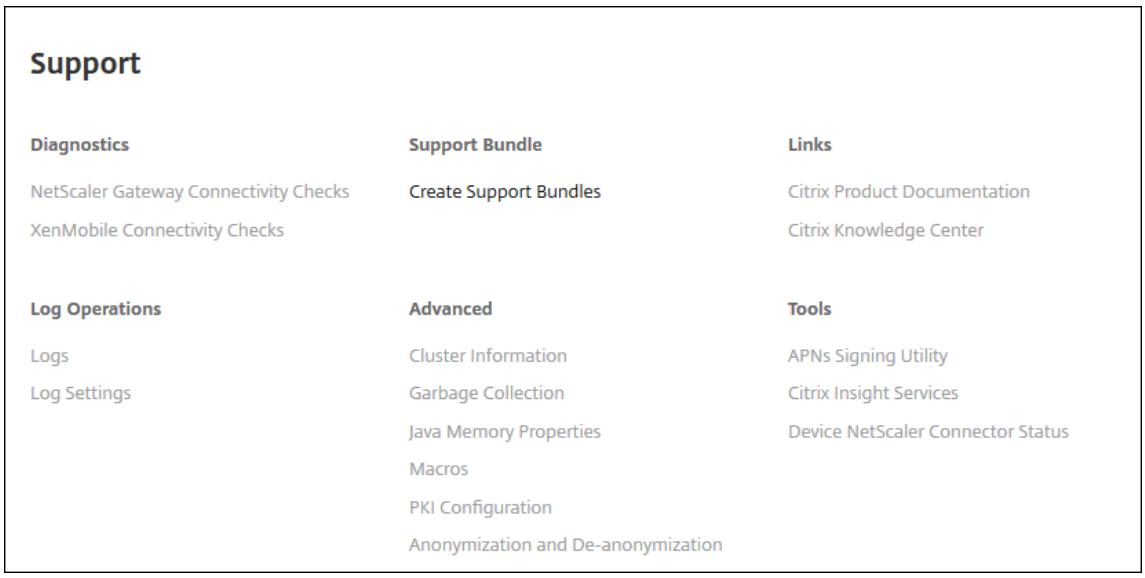
7. Wenn die Konfiguration abgeschlossen ist, wird der Server neu gestartet und das Anmeldedialogfeld wird angezeigt.



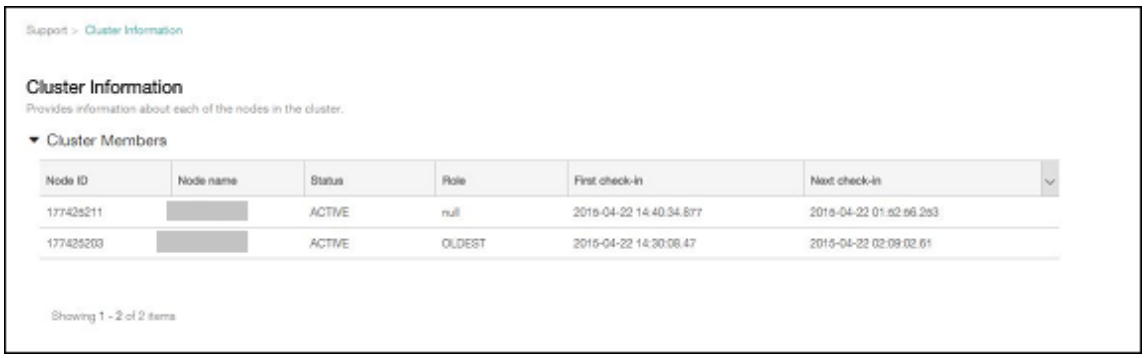
> **Hinweis:**
>
> Das Anmeldedialogfeld ist das gleiche wie für die erste VM. Die Übereinstimmung zeigt Ihnen, dass beide VMs den gleichen Datenbankserver verwenden.

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.

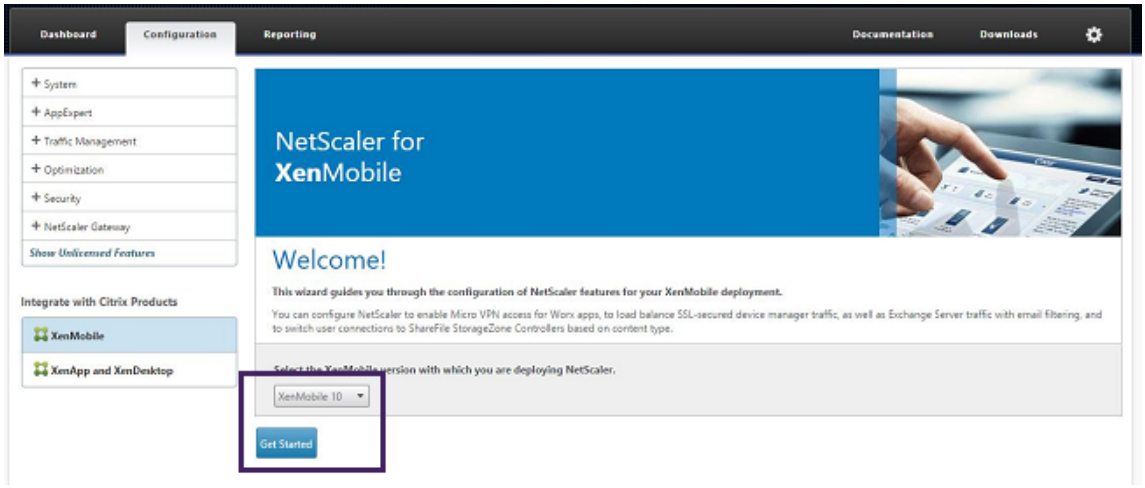


Sie können auf die gleiche Weise noch weitere Knoten hinzufügen. Der erste zum Cluster hinzugefügte Knoten hat die Rolle **Älteste**. Anschließend hinzugefügte Knoten haben die Rolle **Keine** oder **Null**.

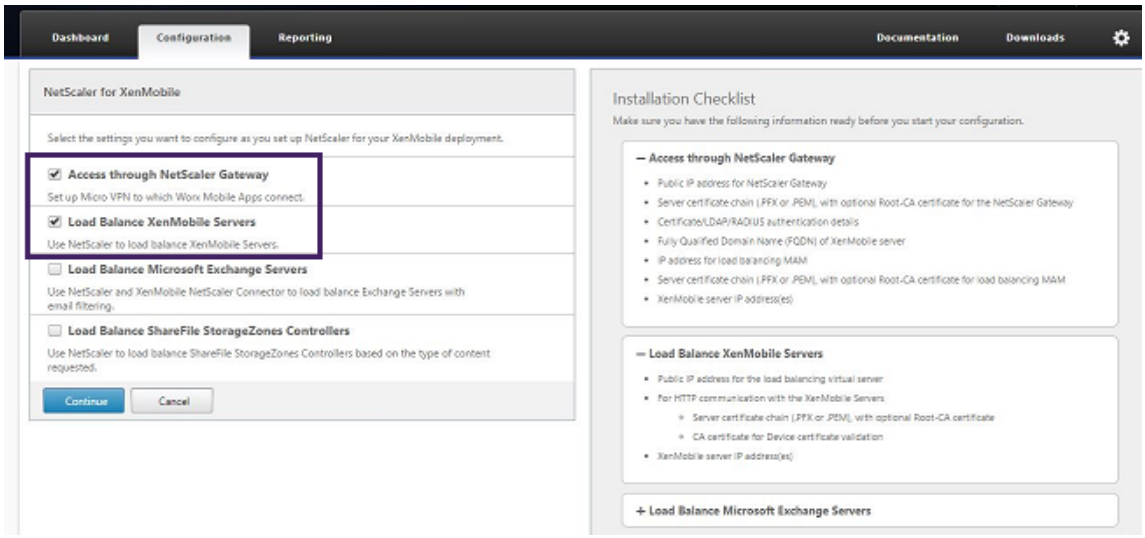
Konfigurieren von Lastausgleich für den XenMobile-Cluster in Citrix ADC

Nachdem Sie die erforderlichen Knoten als Mitglieder des XenMobile-Clusters hinzugefügt haben, führen Sie für die Knoten den Lastausgleich durch, um auf die Cluster zugreifen zu können. Verwenden Sie für den Lastausgleich den XenMobile-Assistenten in Citrix ADC. Nachfolgend wird erläutert, wie der Lastausgleich bei XenMobile mit dem Assistenten durchgeführt wird.

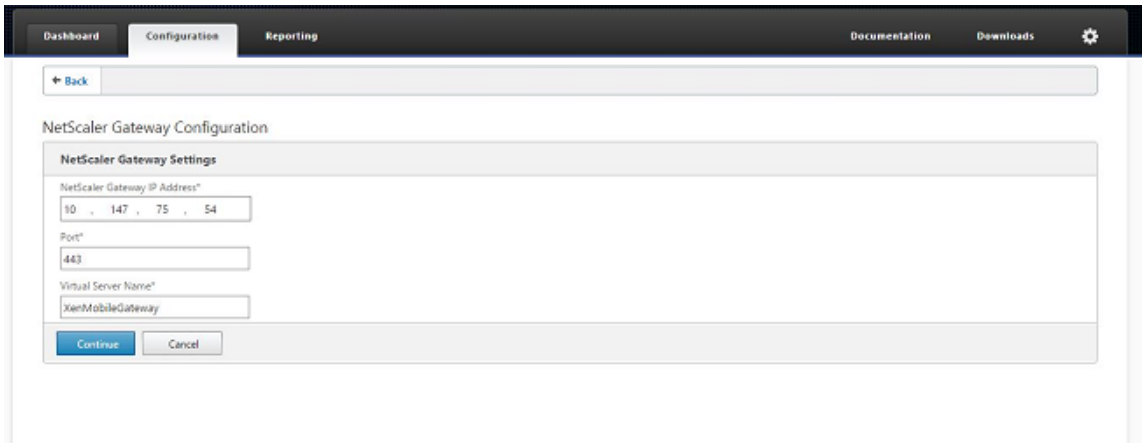
1. Melden Sie sich bei Citrix ADC an.
2. Klicken Sie auf der Registerkarte “Configuration” auf **XenMobile** und dann auf **Get Started**.



3. Wählen Sie das Kontrollkästchen **Access through Citrix Gateway** und das Kontrollkästchen **Load Balance XenMobile Servers** und klicken Sie auf **Continue**.



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

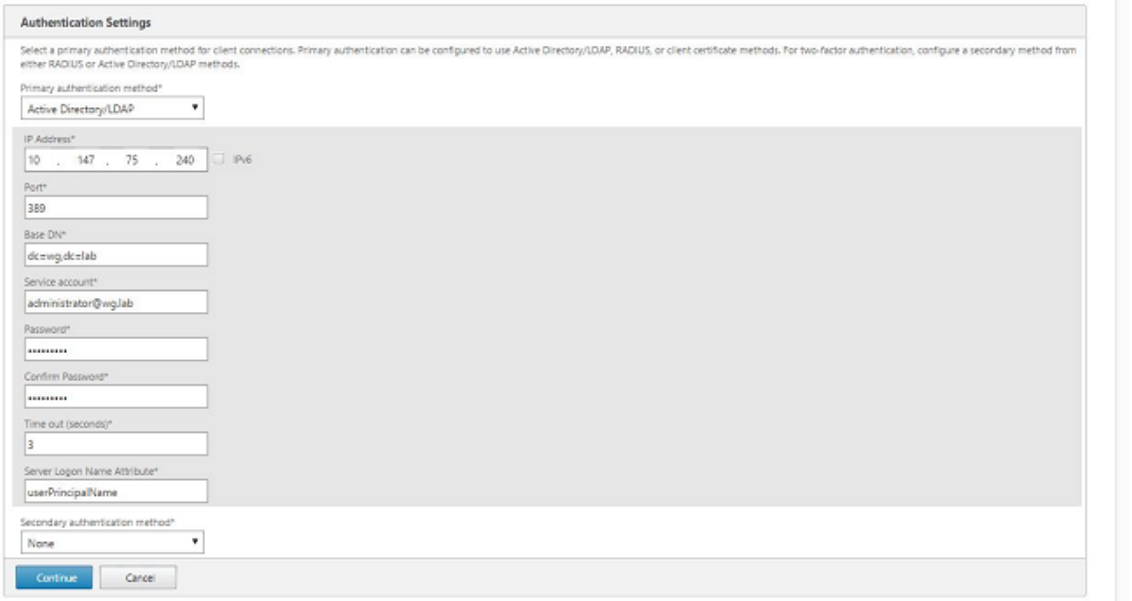


5. Binden Sie das Serverzertifikat an die virtuelle Citrix Gateway-IP-Adresse, indem Sie einen der

folgenden Schritte ausführen und klicken Sie dann auf **Continue**.

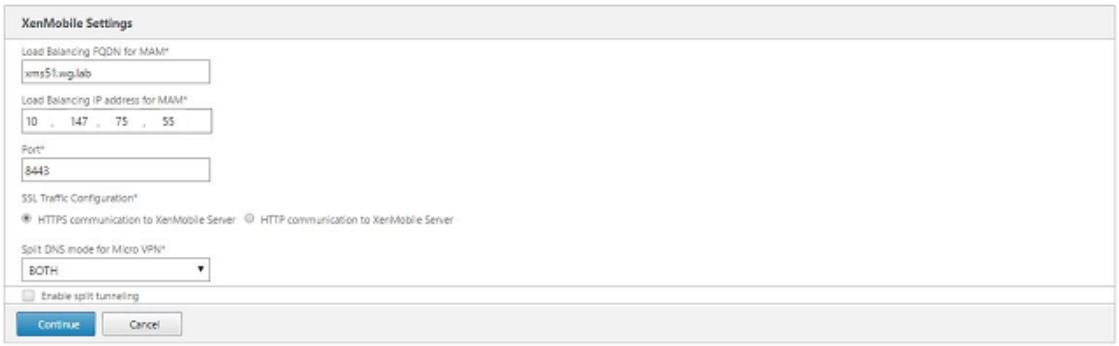
- Wählen Sie für **Use existing certificate** das Serverzertifikat aus der Liste aus.
- Klicken Sie auf die Registerkarte **Install Certificate**, um ein neues Serverzertifikat hochzuladen.

6. Geben Sie die Authentifizierungsserver-Details ein und klicken Sie auf **Continue**.



> **Hinweis:**
>
> Stellen Sie sicher, dass der Wert von “Server Logon Name Attribute” mit dem der XenMobile-LDAP-Konfiguration übereinstimmt.

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

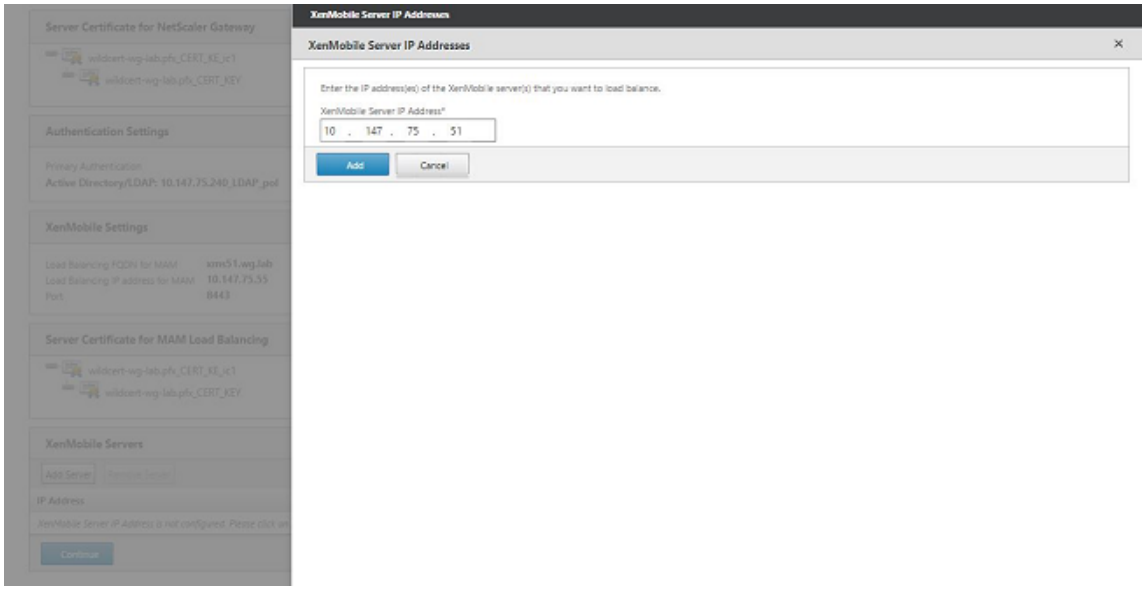


> **Hinweis:**
>
> Stellen Sie sicher, dass der FQDN der virtuellen IP-Adresse für den MAM-Lastausgleich und der FQDN von XenMobile identisch sind.

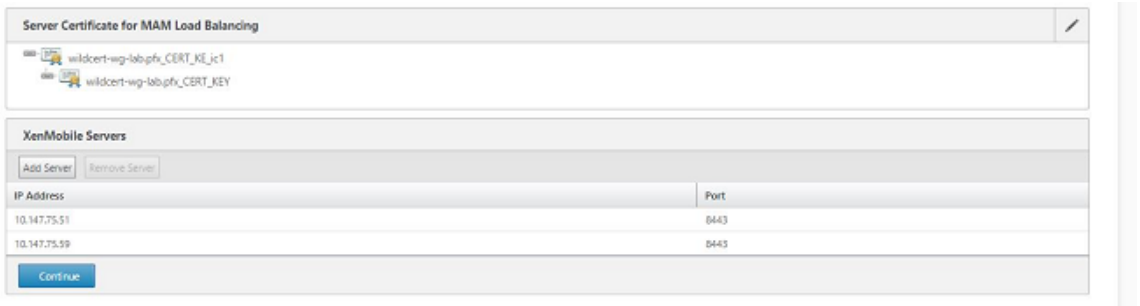
8. Wenn Sie den SSL-Bridge-Modus (HTTPS) verwenden möchten, wählen Sie **HTTPS communication to XenMobile Server**. Wenn Sie SSL-Offload verwenden möchten, wählen Sie **HTTP communication to XenMobile Server** (siehe Abbildung oben). Für die Zwecke dieses Artikels nehmen wir SSL-Brückenmodus (HTTPS).
9. Binden Sie das Serverzertifikat für die virtuelle IP-Adresse für den MAM-Lastausgleich und klicken Sie auf “Continue”.

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

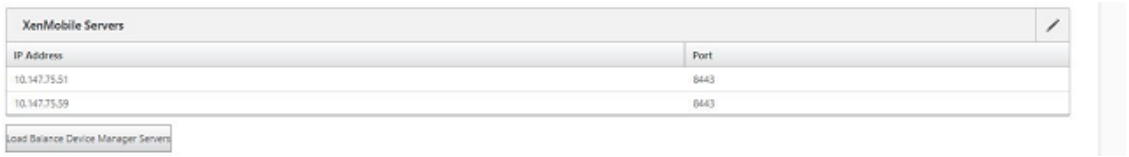
11. Geben Sie die IP-Adresse des XenMobile-Knotens ein und klicken Sie auf “Add”.



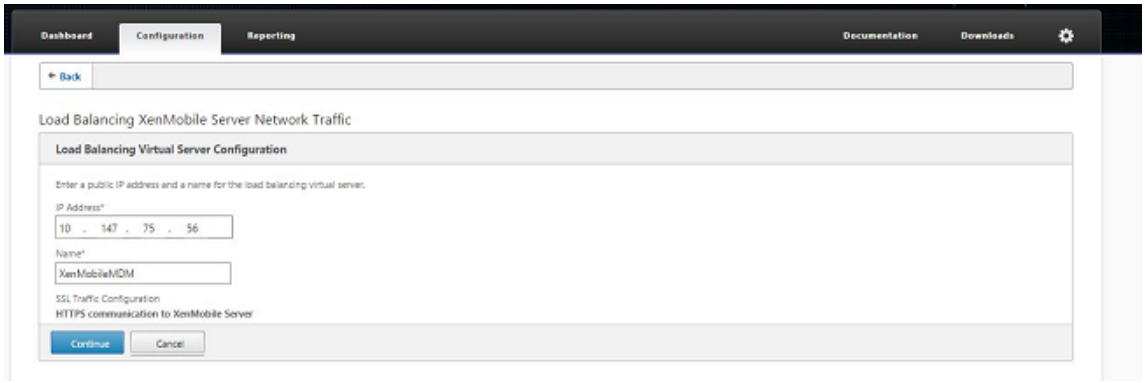
12. Wiederholen Sie die Schritte 10 und 11, um weitere XenMobile-Knoten hinzuzufügen, die Teil des XenMobile-Clusters sind. Sie sehen dann alle XenMobile-Knoten, die Sie hinzugefügt haben. Klicken Sie auf Weiter.



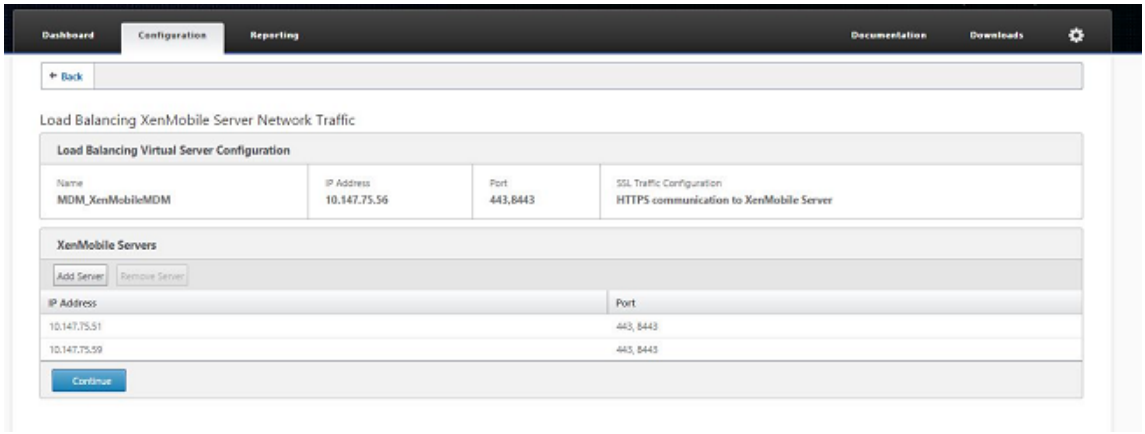
13. Klicken Sie auf **Load Balance Device Manager Servers**, um mit der Konfiguration des MDM-Lastausgleichs fortzufahren.



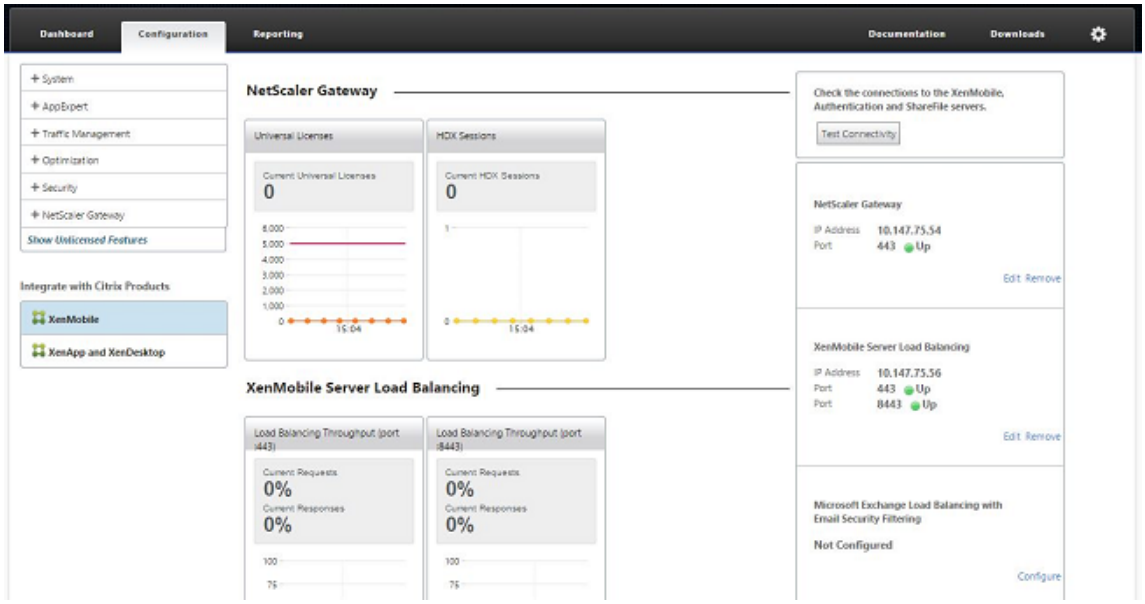
14. Geben Sie die IP-Adresse für den MDM-Lastausgleich ein und klicken Sie auf **Continue**.



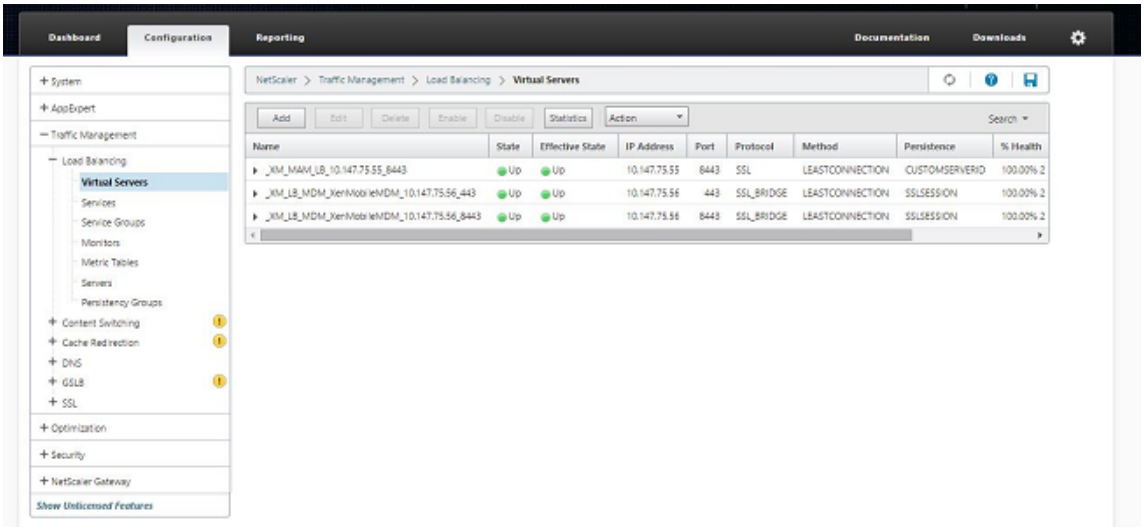
15. Sobald Sie die XenMobile-Knoten in der Liste sehen, klicken Sie auf **Continue** und dann auf “Done”, um den Vorgang abzuschließen.



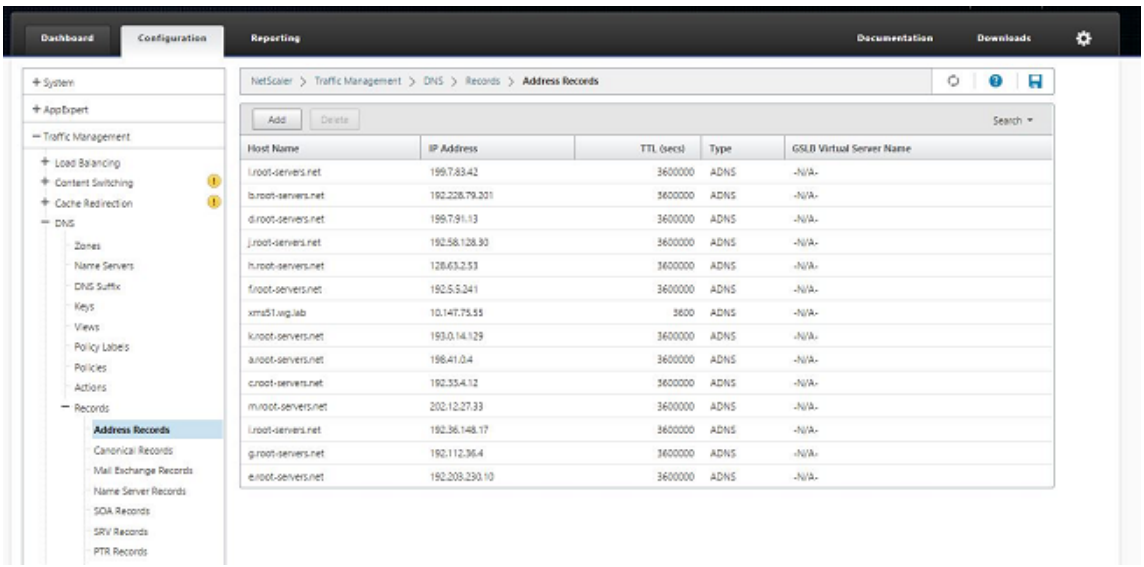
Der Status der virtuellen IP-Adresse wird auf der Seite “XenMobile” angezeigt.



16. Zur Überprüfung des einwandfreien Funktionierens der virtuellen IP-Adressen gehen Sie auf der Registerkarte “Configuration” zu **Traffic Management > Load Balancing > Virtual Servers**.



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



Leitfaden zur Notfallwiederherstellung

January 5, 2022

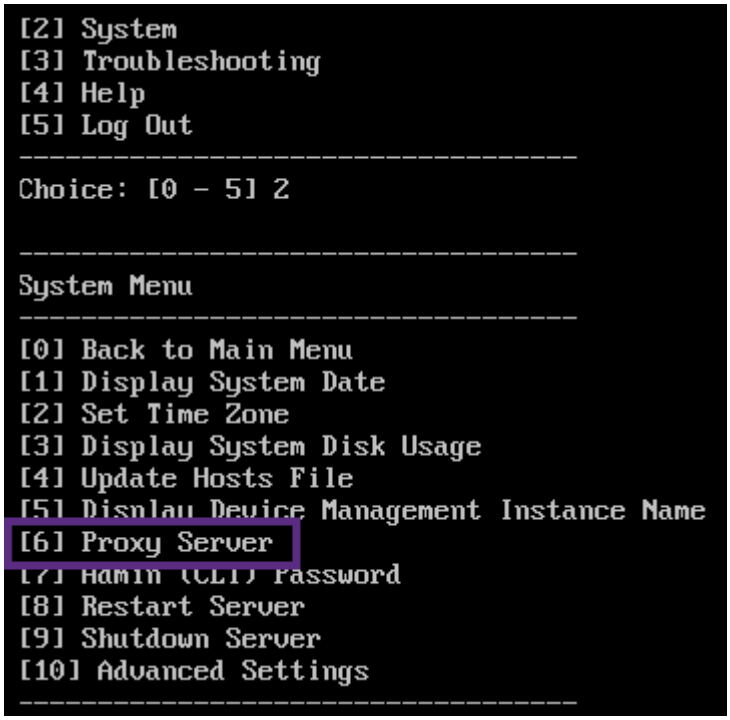
Sie können XenMobile-Bereitstellungen mit mehreren Sites für die Notfallwiederherstellung und einer Aktiv-Passive-Failoverstrategie einrichten. Weitere Informationen finden Sie im XenMobile-Bereitstellungshandbuch unter Disaster Recovery.

Aktivieren von Proxyservern

January 5, 2022

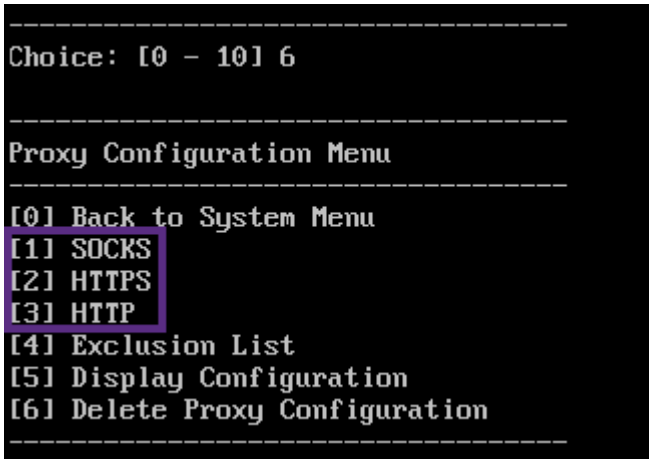
Zum Steuern von ausgehendem Internetverkehr können Sie in XenMobile einen Proxyserver für den Verkehr einrichten. Den Proxyserver richten Sie über die Befehlszeilenschnittstelle (CLI) ein. Zum Einrichten des Proxyservers müssen Sie das System neu starten.

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.



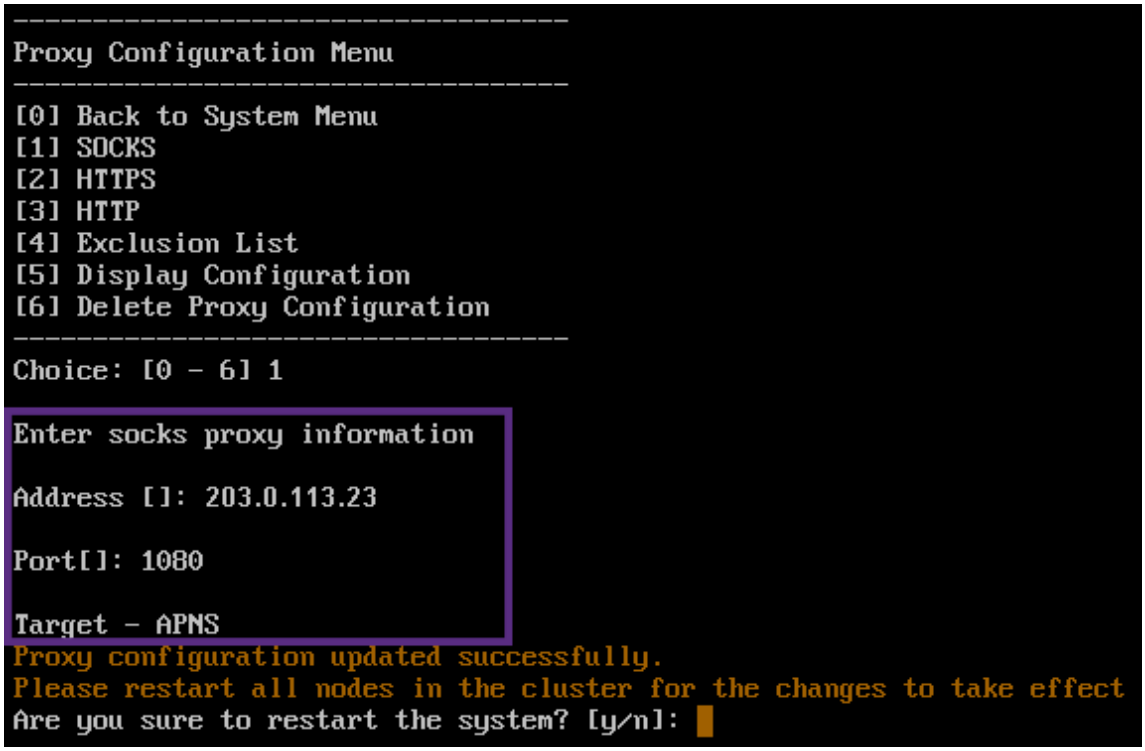
3. Geben Sie im Menü für die Proxykonfiguration **1**, um SOCKS zu wählen.

   Bevor Sie dieses Setup speichern, müssen Sie auch HTTPS konfigurieren. Der Proxy funktioniert nur, wenn Sie die SOCKS- und HTTPS-Einstellungen in derselben Konfiguration speichern.

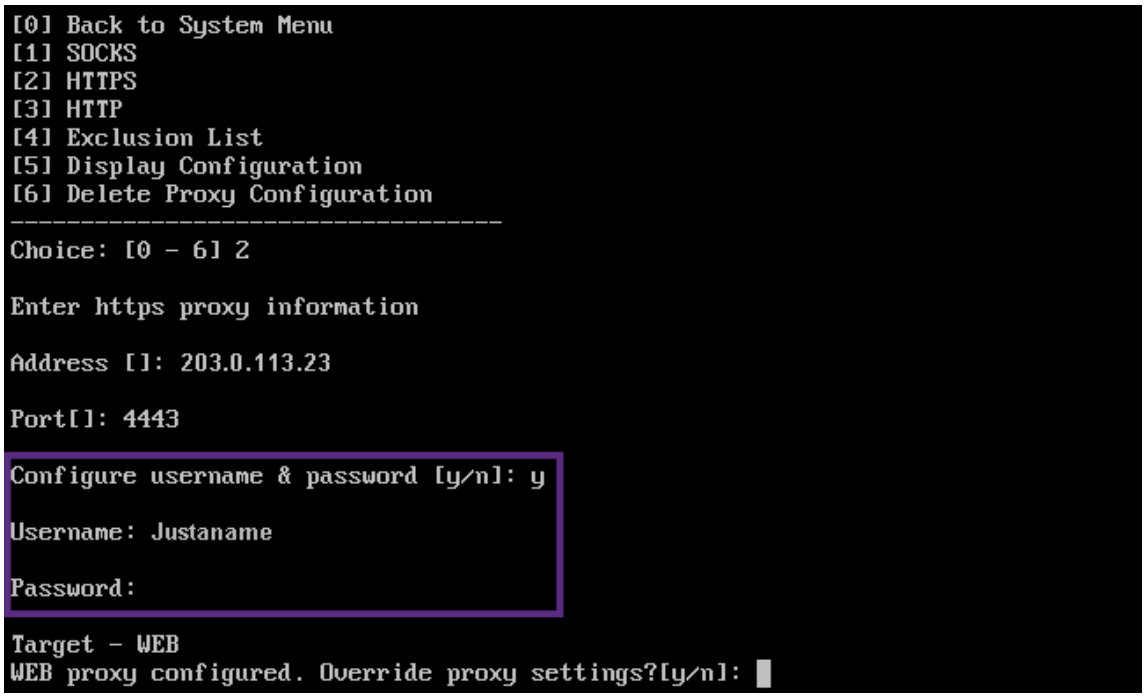


4. Geben Sie IP-Adresse, Portnummer und Ziel des Proxyservers ein. In der folgenden Tabelle sind die für die Proxyservertypen unterstützten Zieltypen aufgeführt.

Proxytyp	Unterstützte Ziele
SOCKS	APNs
HTTP	APNS, Web, PKI
HTTPS	Web, PKI
HTTP mit Authentifizierung	Web, PKI
HTTPS mit Authentifizierung	Web, PKI



5. Geben Sie **n** ein, geben Sie **2**ein, um HTTPS auszuwählen, und geben Sie dann die IP-Adresse des Proxyservers, die Portnummer und das Ziel ein.
6. Wenn Sie einen Benutzernamen und ein Kennwort für die Authentifizierung auf dem Proxyserver konfigurieren möchten, geben Sie **y** ein, gefolgt vom Benutzernamen und Kennwort.



7. Geben Sie **y** ein, um das Setup zu speichern.

Konfigurieren von SQL Server

January 5, 2022

Für Verbindungen zu SQL Server von einem On-Premises-Server von XenMobile können Sie einen der folgenden Treiber verwenden:

- Standardtreiber
- jTDS
- Microsoft Java Database Connectivity (JDBC)-Treiber

Der jTDS-Treiber ist in folgenden Situationen der Standardtreiber:

- Sie installieren XenMobile Server im eigenen Rechenzentrum.
- Sie führen ein Upgrade von XenMobile Server durch und XenMobile Server ist für die Verwendung des jTDS-Treibers konfiguriert.

Für beide Treiber unterstützt XenMobile die SQL Server-Authentifizierung oder die Windows-Authentifizierung. Für diese Kombinationen von Authentifizierung und Treiber kann SSL aktiviert oder deaktiviert sein.

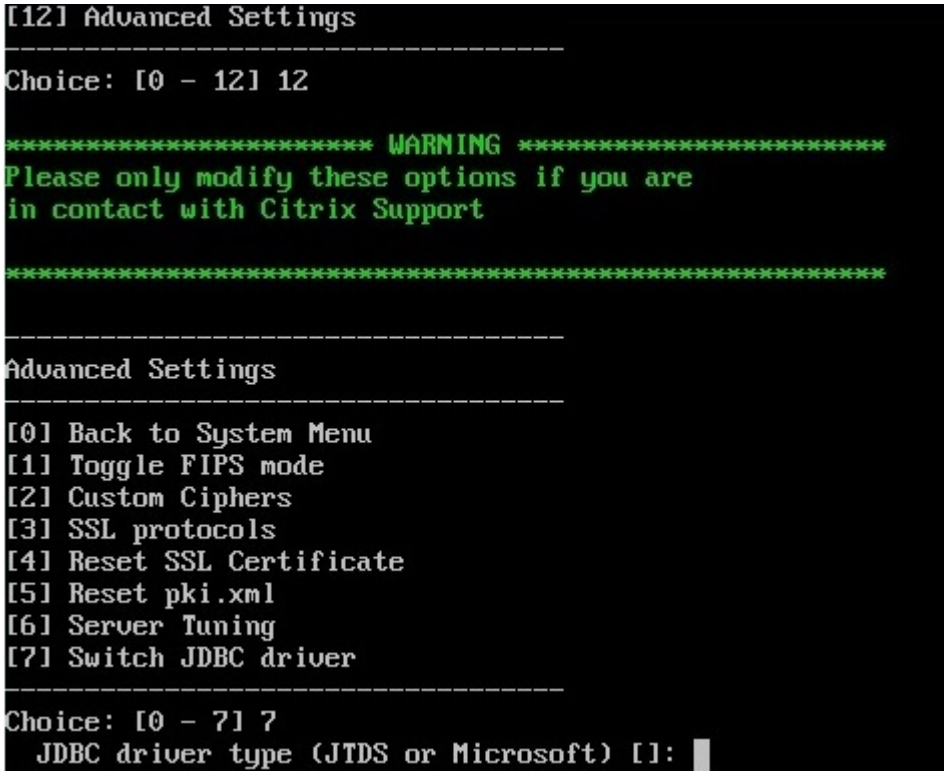
Bei Verwendung der Windows-Authentifizierung mit dem Microsoft JDBC-Treiber nutzt dieser die integrierte Authentifizierung mit Kerberos. XenMobile sendet dann eine Datenabfrage an das Schlüsselverteilungszentrum (KDC) von Kerberos. Wenn die erforderlichen Informationen nicht verfügbar sind, fordert die Befehlszeilenschnittstelle (CLI) von XenMobile die IP-Adresse des Active Directory-Servers an.

Um vom jTDS-Treiber zum JDBC-Treiber zu wechseln, stellen Sie eine SSH-Verbindung zu allen XenMobile Server-Knoten her und verwenden dann die XenMobile-Befehlszeilenschnittstelle für die Konfiguration. Die Schrittfolge hängt von der aktuellen jTDS-Treiberkonfiguration ab, wie nachfolgend beschrieben.

Wechsel zu Microsoft JDBC (SQL Server-Authentifizierung)

Für dieses Verfahren benötigen Sie Benutzernamen und Kennwort von SQL Server.

1. Stellen Sie eine SSH-Verbindung mit allen XenMobile Server-Knoten her.
2. Geben Sie im Hauptmenü der XenMobile-Befehlszeilenschnittstelle **2** ein, um das **Systemmenü** auszuwählen.
3. Geben Sie **12** ein, um “Advanced Settings” auszuwählen.
4. Geben Sie **7** ein, um “Switch JDBC driver” auszuwählen, und geben Sie **m** für Microsoft ein.



5. Geben Sie **y** ein, wenn Sie zur Auswahl der SQL-Authentifizierung aufgefordert werden, und geben Sie den Benutzernamen und das Kennwort für SQL Server ein.
6. Wiederholen Sie die Schritte für jeden XenMobile Server-Knoten.
7. Starten Sie jeden XenMobile Server-Knoten neu.

Wechsel zu Microsoft JDBC (SSL ist deaktiviert; Windows-Authentifizierung)

Für dieses Verfahren benötigen Sie Benutzernamen und Kennwort von Active Directory, den Bereich des Kerberos Schlüsselverteilungscenters (KDC) und den KDC-Benutzernamen.

1. Stellen Sie eine SSH-Verbindung mit allen XenMobile Server-Knoten her.
2. Geben Sie im Hauptmenü der XenMobile-Befehlszeilenschnittstelle **2** ein, um das **Systemmenü** auszuwählen.
3. Geben Sie **12** ein, um “Advanced Settings” auszuwählen.
4. Geben Sie **7** ein, um “Switch JDBC driver” auszuwählen, und geben Sie **m** ein.
5. Geben Sie auf die Frage, ob Sie die SQL Server-Authentifizierung verwenden möchten, **n** ein.
6. Geben Sie nach Aufforderung den für den SQL-Server konfigurierten Benutzernamen und das Kennwort für Active Directory ein.

7. Wenn der Bereich des Kerberos Schlüsselverteilungscenters (KDC) nicht automatisch erkannt wird, werden Sie von XenMobile zur Eingabe der KDC-Details aufgefordert, einschließlich des FQDN des SQL-Servers.
8. Geben Sie auf die Frage, ob Sie SSL verwenden möchten, **n** ein. XenMobile speichert die Konfiguration. Wenn XenMobile die Konfiguration aufgrund eines Fehlers nicht speichern kann, werden eine Fehlermeldung und die eingegebenen Informationen angezeigt.
9. Wiederholen Sie die Schritte für jeden XenMobile Server-Knoten.
10. Starten Sie jeden XenMobile Server-Knoten neu.

Ändern des XenMobile-Datenbankkennworts

Folgen Sie den nachfolgenden Anweisungen zum Ändern des XenMobile-Datenbankkennworts (beispielsweise wenn Sie vom Citrix Support dazu aufgefordert werden).

Wenn für den SQL Server die Windows-Authentifizierung verwendet wird, ändern Sie das Datenbankkennwort in Active Directory. Aktualisieren Sie dann das Datenbankadministratorkonto auf dem Datenbankserver, um die Kennwortänderung zu synchronisieren. Anschließend können Sie das Kennwort in XenMobile wie folgt ändern.

> **Wichtig:**
>
> - Planen Sie ein Wartungsfenster zum Ändern des Datenbankkennworts in XenMobile. Eine Kennwortänderung muss bei heruntergefahrenem System erfolgen.
> - Stellen Sie sicher, dass beim Ändern des Kennworts alle XenMobile-Knoten mit dem Netzwerk verbunden sind. Nachdem Sie das Kennwort geändert haben, starten Sie XenMobile neu.
>
>   If you don't restart XenMobile after a password change, XenMobile goes into recovery mode. In that case, revert to the old password in SQL server, restart XenMobile, and change the password again.

1. Stellen Sie sicher, dass alle XenMobile Server-Knoten ausgeführt werden. Fahren Sie in einer Clusterumgebung alle Knoten hoch.
2. Blockieren Sie von Geräten eingehenden Datenverkehr zu XenMobile am Citrix ADC-Load Balancer, indem Sie die virtuellen Server deaktivieren.
3. Melden Sie sich zum Ändern des Datenbankkennworts in SQL Server bei der XenMobile-CLI an, gehen Sie zu **Configuration > Database** und geben Sie das geänderte Kennwort ein, wenn Sie dazu aufgefordert werden:

```
Server []: <ipAddress>
Port [1433]: 1433
```



```
Username [sa]: <userName>
Password: <****>
<!--NeedCopy-->
```

4. Wählen Sie **y**, um den Server neu zu starten.
5. Wiederholen Sie Schritt 3 und 4 für alle anderen Knoten im Cluster.
6. Entsperren Sie den von Geräten eingehenden Datenverkehr am Citrix ADC-Load Balancer, indem Sie die virtuellen Server aktivieren.

Servereigenschaften

January 5, 2022

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

Einige Eigenschaften sind benutzerdefinierte Schlüssel. Zum Hinzufügen eines benutzerdefinierten Schlüssels klicken Sie auf **Hinzufügen** und wählen dann unter **Schlüssel** die Option **Benutzerdefinierter Schlüssel**.

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

Servereigenschaften – Definitionen

Immer Gerät hinzufügen

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

AG Clientzertifikatausstellung - Drosselungsintervall

- Der Kulanzzeitraum zwischen dem Generieren von Zertifikaten. Dieses Intervall verhindert, dass XenMobile in kurzer Zeit mehrere Zertifikate für ein Gerät generiert. Citrix empfiehlt, diesen Wert nicht zu ändern. Der Standardwert ist **30** Minuten.

Ausführungszeit für Auditprotokollbereinigung

- Die Startzeit der Auditprotokollbereinigung im Format HH:MM AM/PM. Beispiel: 04:00 AM. Standardeinstellung ist **02:00** Uhr.

Bereinigungsintervall für Auditprotokoll (in Tagen)

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

Auditprotokollierung

- Bei Einstellung von **Falsch** werden Benutzeroberflächenereignisse nicht erfasst. Die Standardeinstellung ist **Falsch**.

Auditprotokollaufbewahrung (in Tagen)

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

auth.ldap.connect.timeout and auth.ldap.read.timeout

- Bei einer langsamen LDAP-Antwort empfiehlt Citrix das Hinzufügen von Servereigenschaften für die folgenden benutzerdefinierten Schlüssel.
  - Schlüssel: **Benutzerdefinierter Schlüssel**
  - Schlüssel: **auth.ldap.connect.timeout**
  - Wert: **60000**
  - Anzeigename: **auth.ldap.connect.timeout**
  - Beschreibung: **Zeitlimit für LDAP-Verbindung**
  - Schlüssel: **Benutzerdefinierter Schlüssel**
  - Schlüssel: **auth.ldap.read.timeout**
  - Wert: **60000**
  - Anzeigename: **auth.ldap.read.timeout**
  - Beschreibung: **LDAP-Lesezeitlimit**

Zertifikatserneuerung (in Sekunden)

- Der Zeitpunkt in Sekunden vor Ablauf eines Zertifikats, zu dem XenMobile die Verlängerung beginnt. Wenn ein Zertifikat beispielsweise am 30. Dezember abläuft und die 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).

Verbindungstimeout

- Zeitdauer in Minuten, nach deren Ablauf XenMobile bei Sitzungsinaktivität die TCP-Verbindung zum Gerät beendet. Die Sitzung bleibt geöffnet. Gültig für Android- und Windows CE-Geräte und für Remote Support. Der Standardwert ist **5** Minuten.

Verbindungstimeout zum Microsoft-Zertifizierungsserver

- Die Zeitdauer in Sekunden, die XenMobile auf eine Antwort vom Zertifikatserver wartet. Erhöhen Sie diesen Wert bei langsamem Zertifikatserver oder hohem Netzwerkdatenverkehr auf 60 Sekunden oder mehr. Ein Zertifikatserver, der nach 120 Sekunden nicht reagiert, erfordert Wartungsmaßnahmen. Der Standardwert ist **15000** Millisekunden (15 Sekunden).

Standardbereitstellungskanal

- Legt fest, wie XenMobile Ressourcen für ein Gerät bereitstellt: auf der Benutzerebene (**DEFAULT_TO_USER**) oder auf Geräteebene. Der Standardwert ist **DEFAULT_TO_DEVICE**.

Protokollbereinigung bereitstellen (in Tagen)

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

Überprüfung des Hostnamens deaktivieren

- In der Standardeinstellung ist die Hostnamenüberprüfung für ausgehende Verbindungen mit Ausnahme des Microsoft PKI-Servers aktiviert. Wenn die Überprüfung des Hostnamens fehlschlägt, enthält das Serverprotokoll Fehler wie z. B. “Unable to connect to the volume purchase Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”. Wenn die Hostnamenüberprüfung Fehler in der Bereitstellung verursacht, ändern Sie diese Servereigenschaft in **Wahr**. Der Standardwert ist **Falsch**.

SSL-Serverüberprüfung deaktivieren

- Bei der Einstellung **Wahr** ist die Überprüfung des SSL-Serverzertifikats deaktiviert, wenn die folgenden Bedingungen alle zutreffen:

  - Sie haben die zertifikatbasierte Authentifizierung auf XenMobile Server aktiviert.
  - Das Zertifikat wurde vom Microsoft-Zertifizierungsstellenserver ausgestellt.
  - Das Zertifikat wurde von einer internen Zertifizierungsstelle signiert, deren Stammzertifikat XenMobile Server als nicht vertrauenswürdig ansieht.

Der Standardwert ist **Wahr**.

Konsole aktivieren

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

Absturzberichterstellung

- Bei der Einstellung **Wahr** sammelt Citrix Absturzberichte und Diagnosedaten zur Behandlung von Problemen mit Secure Hub für iOS und Android. Bei der Einstellung **Falsch** werden keine Daten gesammelt. Der Standardwert ist **Wahr**.

Hibernate-Statistikprotokollierung für Diagnosezwecke aktivieren/deaktivieren

- Wenn **Wahr** festgelegt wird, wird die Hibernate-Statistikprotokollierung aktiviert, um die Behandlung bei Problemen mit der Anwendungsleistung zu erleichtern. 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. Die Standardeinstellung ist **Falsch**.

Enable macOS OTAE

- Bei der Einstellung **Falsch** wird die Verwendung von Registrierungslinks für macOS-Geräte verhindert, sodass die Benutzer die Registrierung nur über eine Registrierungseinladung vornehmen können. Der Standardwert ist **Wahr**.

Benachrichtigungsauslöser aktivieren

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

force.server.push.required.apps

- Ermöglicht die erzwungene Bereitstellung erforderlicher Apps auf Android- und iOS-Geräten in Situationen wie den folgenden:
  - Sie laden eine neue App hoch und legen sie als erforderlich fest.
  - Sie legen eine vorhandene App als erforderlich fest.
  - Ein Benutzer löscht eine erforderliche App.
  - Es gibt ein Secure Hub-Update.

Die erzwungene Bereitstellung erforderlicher Apps ist standardmäßig auf **Falsch** festgelegt. Erstellen Sie den benutzerdefinierten Schlüssel und legen Sie den **Wert** auf **Wahr** fest, um die erzwungene Bereitstellung zu aktivieren. Bei der erzwungenen Bereitstellung werden erforderliche MDX-Apps, einschließlich Unternehmensapps und Apps aus dem öffentlichen Store, sofort aktualisiert. Das Upgrade erfolgt selbst, wenn Sie eine MDX-Richtlinie mit einem Kulanzzeitraum für App-Upgrades konfiguriert haben und ein Benutzer angibt, dass er die App später aktualisieren möchte.

- Schlüssel: **Benutzerdefinierter Schlüssel**
- Schlüssel: **force.server.push.required.apps**
- Wert: **Falsch**
- Anzeigename: **force.server.push.required.apps**
- Beschreibung: **Bereitstellung erforderlicher Apps erzwingen**

Vollständiger Pull von zulässigen und abgelehnten ActiveSync-Benutzern

- Zeitdauer (in Sekunden), die XenMobile für den Abruf einer vollständigen Liste (Basiswert) aller zulässigen und abgelehnten ActiveSync-Benutzer benötigt. Der Standardwert ist **28800** Sekunden.

hibernate.c3p0.idle_test_period

- Diese XenMobile Server-Eigenschaft ist ein benutzerdefinierter Schlüssel, mit dem die Leerlaufzeit (in Sekunden) festgelegt wird, bevor eine Verbindung automatisch überprüft wird. Konfigurieren Sie den Schlüssel wie im Folgenden beschrieben. Die Standardeinstellung ist **30**.
- Schlüssel: **Benutzerdefinierter Schlüssel**
- Schlüssel: **hibernate.c3p0. idle_test_period**
- Wert: **30**
- Anzeigename: **hibernate.c3p0. idle_test_period =*nnn***
- Beschreibung: **Leerlaufzeit vor Ruhezustand**

hibernate.c3p0.max_size

- Dieser benutzerdefinierte Schlüssel legt fest, wie viele Verbindungen zur SQL Server-Datenbank von XenMobile maximal geöffnet werden können. XenMobile verwendet den für diesen benutzerdefinierten Schlüssel eingegebenen Wert als Obergrenze. Die Verbindungen werden nur bei Bedarf geöffnet. Wählen Sie Ihre Einstellungen je nach Kapazität des Datenbankservers. Weitere Informationen finden Sie unter Tuning XenMobile Operations. Konfigurieren Sie den Schlüssel wie im Folgenden beschrieben. Der Standardwert ist **1000**.
- Schlüssel: **hibernate.c3p0.max_size**
- Wert: **1000**
- Anzeigename: **hibernate.c3p0.max_size**
- Beschreibung: **DB-Verbindungen mit SQL**

hibernate.c3p0.min_size

- Dieser benutzerdefinierte Schlüssel legt fest, wie viele Verbindungen zur SQL Server-Datenbank von XenMobile mindestens geöffnet werden. Konfigurieren Sie den Schlüssel wie im Folgenden beschrieben. Der Standardwert ist **100**.
- Schlüssel: **hibernate.c3p0.min_size**
- Wert: **100**
- Anzeigename: **hibernate.c3p0.min_size**
- Beschreibung: **DB-Verbindungen mit SQL**

hibernate.c3p0.timeout

- Dieser benutzerdefinierte Schlüssel definiert den Wert für Leerlauftimeouts (in Sekunden). Die Standardeinstellung ist **120**.
- Schlüssel: **Benutzerdefinierter Schlüssel**
- Schlüssel: **hibernate.c3p0.timeout**
- Wert: **120**
- Anzeigename: **hibernate.c3p0.timeout**
- Beschreibung: **Timeout bei Datenbankleerlauf**

Gibt an, ob Telemetrie aktiviert ist

- 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**.

Inaktivitätstimeout in Minuten

- Wird für die Servereigenschaft **Timeouttyp für Webservices** der Wert **INACTIVITY_TIMEOUT** festgelegt, definiert diese Eigenschaft, nach wie vielen Minuten XenMobile einen inaktiven Administrator abmeldet, der folgende Schritte ausgeführt hat:
  - Zugriff auf die XenMobile-Konsole über die öffentliche XenMobile API für REST-Dienste.
  - Zugriff auf eine beliebige Drittanbieter-App über die öffentliche XenMobile API für REST-Dienste. Ein Timeoutwert von **0** bedeutet, dass ein inaktiver Benutzer angemeldet bleibt.

Der Standardwert ist **5**.

Registrierung für iOS-Geräteverwaltung: Automatische Installation aktiviert

- Bei der Einstellung “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.

Registrierung für iOS-Geräteverwaltung: Erster Schritt verzögert

- Dieser Wert gibt an, wie lange das Programm bei der Geräteregistrierung nach Eingabe der Anmeldeinformationen wartet, bis das Stammzertifikat der Zertifizierungsstelle angefordert wird. Citrix empfiehlt, dass Sie diese Eigenschaft nur bearbeiten, wenn Probleme mit der Netzwerklatenz oder Geschwindigkeit auftreten. Legen Sie in diesem Fall den Wert auf maximal 5000 Millisekunden (5 Sekunden) fest. Der Standardwert ist **1000** Millisekunden (1 Sekunde).

Registrierung für iOS-Geräteverwaltung: Letzter Schritt verzögert

- 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 auf maximal 5000 Millisekunden (5 Sekunden) fest. Der Standardwert ist **1000** Millisekunden (1 Sekunde).

iOS-Geräteverwaltung: Identitätsübermittlungsmodus

- 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-Geräteverwaltung: Größe des Identitätsschlüssels

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

Identitätsverlängerung bei der iOS-Geräteverwaltung in Tagen

- 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, stellt XenMobile ein neues Zertifikat aus, wenn ein Gerät 9 Tage vor dem Ablauf eine Verbindung herstellt. Der Standardwert ist **30** Tage.

iOS APNs-Kennwort des privaten MDM-Schlüssels

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

Inaktivitätsdauer bevor das Gerät getrennt wird

- Gibt an, wie lange ein Gerät inaktiv bleiben kann (einschließlich der letzten Authentifizierung), bevor XenMobile die Verbindung trennt. Der Standardwert ist **7** Tage.

MAM Only Device Max

- Dieser benutzerdefinierte Schlüssel beschränkt die Anzahl der Nur-MAM-Geräte, die jeder Benutzer registrieren kann. Konfigurieren Sie den Schlüssel wie im Folgenden beschrieben. Ein **Wert** von **0** ermöglicht die Registrierung einer unbegrenzten Anzahl an Geräten.
- Schlüssel: **number.of.mam.devices.per.user**
- Wert: **5**
- Anzeigename: **MAM Only Device Max**
- Beschreibung: **Begrenzt die Anzahl der MAM-Geräte, die jeder Benutzer registrieren kann.**

MaxNumberOfWorker

- Zahl der beim Importieren eine großen Anzahl von Volume Purchase-Lizenzen verwendeten Threads. Der Standardwert ist **3**. Ist eine weitere Optimierung erforderlich, können Sie die Zahl der Threads erhöhen. Bei einer größeren Anzahl von Threads (z. B. 6) führt ein Volume Purchase-Import jedoch zu einer hohen CPU-Auslastung.

Single Sign-On für Citrix ADC

- Bei der Einstellung **Falsch** ist das Rückruffeature von XenMobile beim Single Sign-On von Citrix ADC bei XenMobile deaktiviert. Wenn die Citrix Gateway-Konfiguration eine Rückruf-URL enthält, prüft XenMobile mit dem Rückruffeature die Citrix Gateway-Sitzungs-ID. Die Standardeinstellung ist **Falsch**.

Anzahl der aufeinanderfolgenden fehlgeschlagenen 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 siehe Servereigenschaft **Gibt an, ob Telemetrie aktiviert ist.**. XenMobile setzt den Wert auf **0** zurück, wenn ein Upload erfolgreich ist.

Anzahl der Benutzer pro Gerät

- 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 der inkrementellen Änderung der zulässigen und abgelehnten Benutzer

- 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.

Lesetimeout für Microsoft-Zertifizierungsserver

- 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 Zertifikatserver, der nach 120 Sekunden nicht reagiert, erfordert Wartungsmaßnahmen. Der Standardwert ist **15000** Millisekunden (15 Sekunden).

REST Web Services

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

Ruft Geräteinformationen in Blöcken der angegebenen Größe ab

- Dieser Wert wird intern für das Multithreading beim Geräteexport verwendet. Bei einem höheren Wert werden mehr Geräte pro Thread analysiert. Ist der Wert niedriger, werden zum Abrufen der Geräte mehr Threads verwendet. Eine Verringerung des Wertes kann die Leistung abgerufener Exporte und Gerätelisten verbessern, jedoch auch den verfügbaren Speicher reduzieren. Der Standardwert ist **1000**.

Sitzungsprotokollbereinigung (in Tagen)

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

Servermodus

- 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. Standardmäßig ist der Servermodus unabhängig vom Lizenztyp **ENT**.

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 Servermodus, wenn dieser **ENT** oder **MDM** ist. Wenn der Servermodus **MAM** ist, ist der effektive Servermodus ENT.

XenMobile fügt den Servermodus dem Serverprotokoll jedes Mal hinzu, 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.

Content Collaboration-Konfigurationstyp

- Gibt den Citrix Files-Speichertyp an. **ENTERPRISE** aktiviert den Citrix Files Enterprise-Modus. **CONNECTORS** limitiert den Zugriff auf Speicherzonenconnectors, die Sie über die XenMobile-Konsole erstellen. Der Standardwert ist **NONE**. Dabei wird die Startansicht des Bildschirms **Konfigurieren > ShareFile** angezeigt, wo Sie zwischen Citrix Files Enterprise und Connectors wählen können. Der Standardwert ist **NONE**.

Statisches Timeout in Minuten

- Wird für die Servereigenschaft **Timeouttyp für Webservices** der Wert **STATIC_TIMEOUT** festgelegt, definiert diese Eigenschaft, nach wie vielen Minuten XenMobile einen Administrator abmeldet, der folgende Schritte ausgeführt hat:
  - Zugriff auf die XenMobile-Konsole über die öffentliche XenMobile API für REST-Dienste
  - Zugriff auf eine beliebige Drittanbieter-App über die öffentliche XenMobile API für REST-Dienste

Der Standardwert ist **60**.

Unterdrückung von Agentnachrichten auslösen

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

Unterdrückung der Agent-Signaltöne

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

Nicht authentifizierter App-Download für Android-Geräte

- Mit der Einstellung **Wahr** können Sie selbstgehostete Apps auf Android-Geräte herunterladen, auf denen Android Enterprise ausgeführt wird. XenMobile benötigt diese Eigenschaft, wenn in Android Enterprise die Option zum Bereitstellen einer statischen Download-URL im Google Play Store aktiviert ist. In diesem Fall dürfen Download-URLs kein Einmalticket (definiert durch die Servereigenschaft **XAM-Einmalticket**) mit dem Authentifizierungstoken enthalten. Die Standardeinstellung ist **Falsch**.

Nicht authentifizierter App-Download für Windows-Geräte

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

ActiveSync-ID zum Löschen von Gerät mit ActiveSync verwenden

- Bei der Einstellung **Wahr** verwendet der Endpoint Management Connector für Exchange ActiveSync die ActiveSync-ID als Argument für die asWipeDevice-Methode. Der Standardwert ist **Falsch**.

Benutzerdefinierte Geräteeigenschaften N

- Wird nur für Windows CE-Geräte verwendet. Dieser benutzerdefinierte Schlüssel ermöglicht den Abruf von Eigenschaften, die Sie in der Registrierung von Windows CE-Geräten erstellen. Sobald diese Eigenschaften der XenMobile-Datenbank hinzugefügt sind, können Sie Bereitstellungsregeln basierend auf dem Wert der Eigenschaften erstellen.
- Schlüssel: **Benutzerdefinierter Schlüssel**
- Schlüssel: **device.properties.userDefinedN**
- Wert: *administrator-defined*
- Anzeigename: *administrator-defined*
- Beschreibung: *administratordefiniert*

Nur Benutzer von Exchange

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

VP-Basisintervall

- Der Mindestzeitraum, während dem XenMobile Volume Purchase-Lizenzen von Apple erneut importiert. Durch Aktualisierung der Lizenzinformationen wird sichergestellt, dass in XenMobile alle Änderungen widergespiegelt werden, beispielsweise das manuelle Löschen einer importierten App aus Volume Purchase. Standardmäßig aktualisiert XenMobile die Volume Purchase-Lizenzbasis mindestens alle **720** Minuten.

Wenn Sie zahlreiche Volume Purchase-Lizenzen installiert haben (beispielsweise über 50.000), empfiehlt Citrix die Verlängerung des Basisintervalls, um die Importhäufigkeit und den Mehraufwand zu verringern, der beim Importieren von Lizenzen entsteht. Wenn Sie davon ausgehen, dass Apple häufig Änderungen an den Volume Purchase-Lizenzen vornimmt, rät Citrix dazu, den Wert zu verringern, damit XenMobile fortlaufend mit den Änderungen aktualisiert wird. Das Mindestintervall zwischen zwei Basiswerten beträgt 60 Minuten. Darüber hinaus führt XenMobile alle 60 Minuten einen Delta-Import durch, um alle Änderungen seit dem letzten Importvorgang zu erfassen. Dadurch kann das Intervall zwischen Basiswerten auf bis zu 119 Minuten steigen, wenn das Volume Purchase-Basisintervall auf 60 Minuten festgelegt ist.

Timeouttyp für Webservices

- 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**.

Windows Phone MDM-Zertifikat mit erweiterter Gültigkeit (5 Jahre)

- Die Gültigkeitsdauer des von MDM für Windows Phone und Tablet ausgestellten Gerätezertifikats. Geräte verwenden ein Gerätezertifikat, um sich während der Geräteverwaltung beim MDM-Server zu authentifizieren. Bei Einstellung auf **Wahr** ist die Gültigkeitsdauer fünf Jahre. Bei Einstellung auf **Falsch** ist die Gültigkeitsdauer zwei Jahre. Der Standardwert ist **Wahr**.

Windows WNS Channel - Number of Days Before Renewal

- ChannelURI-Verlängerungszeit. Der Standardwert ist **10** Tage.

Windows WNS Heartbeat Interval

- Zeitspanne, die XenMobile wartet, bevor es eine Verbindung mit einem Gerät herstellt, nachdem es alle drei Minuten fünfmal eine Verbindung mit ihm hergestellt hat. Der Standardwert ist **6** Stunden.

XAM-Einmalticket

- Gültigkeitsdauer eines Tokens für die einmalige Authentifizierung (OTT) zum Download einer App in Millisekunden. Diese Eigenschaft wird mit den Eigenschaften **Nicht authentifizierter App-Download für Android-Geräte** und **Nicht authentifizierter App-Download für Windows-Geräte** verwendet. Diese Eigenschaften legen fest, ob nicht authentifizierte App-Downloads zulässig sind. Der Standardwert ist **3600000**.

Maximales Inaktivitätsintervall (in Minuten) für das XenMobile MDM-Selbsthilfeportal

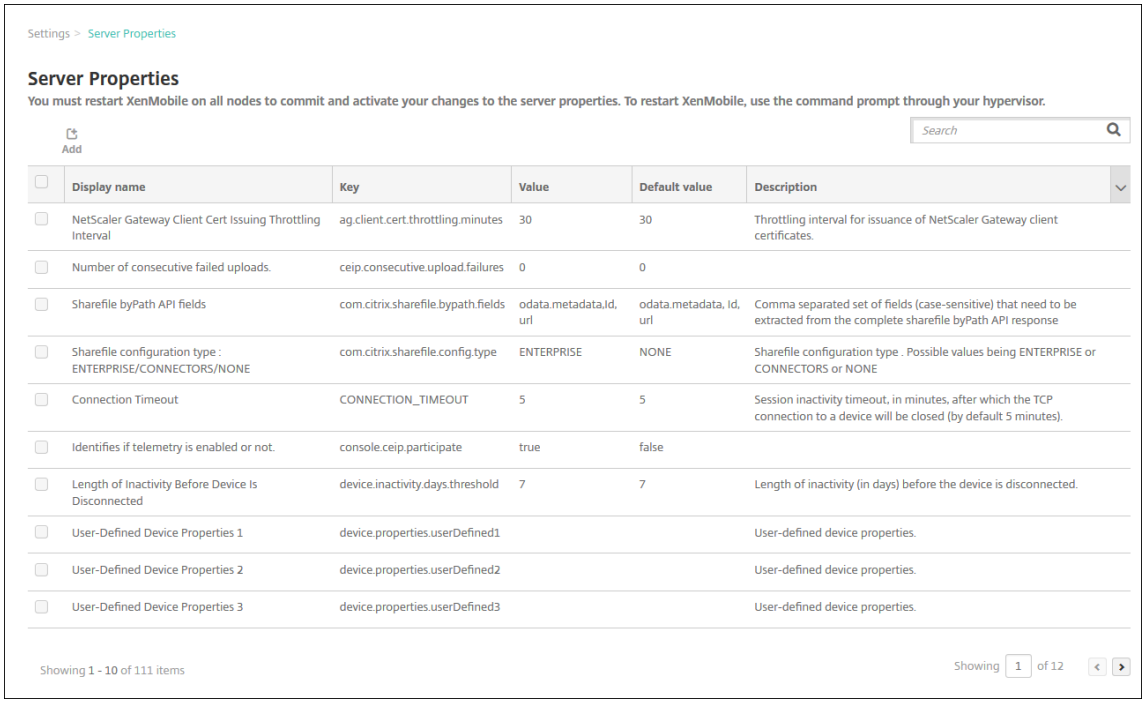
- Die Anzahl der Minuten, nach denen ein inaktiver Benutzer vom XenMobile-Selbsthilfeportal abgemeldet wird. Ein Timeoutwert von **0** bedeutet, dass ein inaktiver Benutzer angemeldet bleibt. Der Standardwert ist **30**.

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.

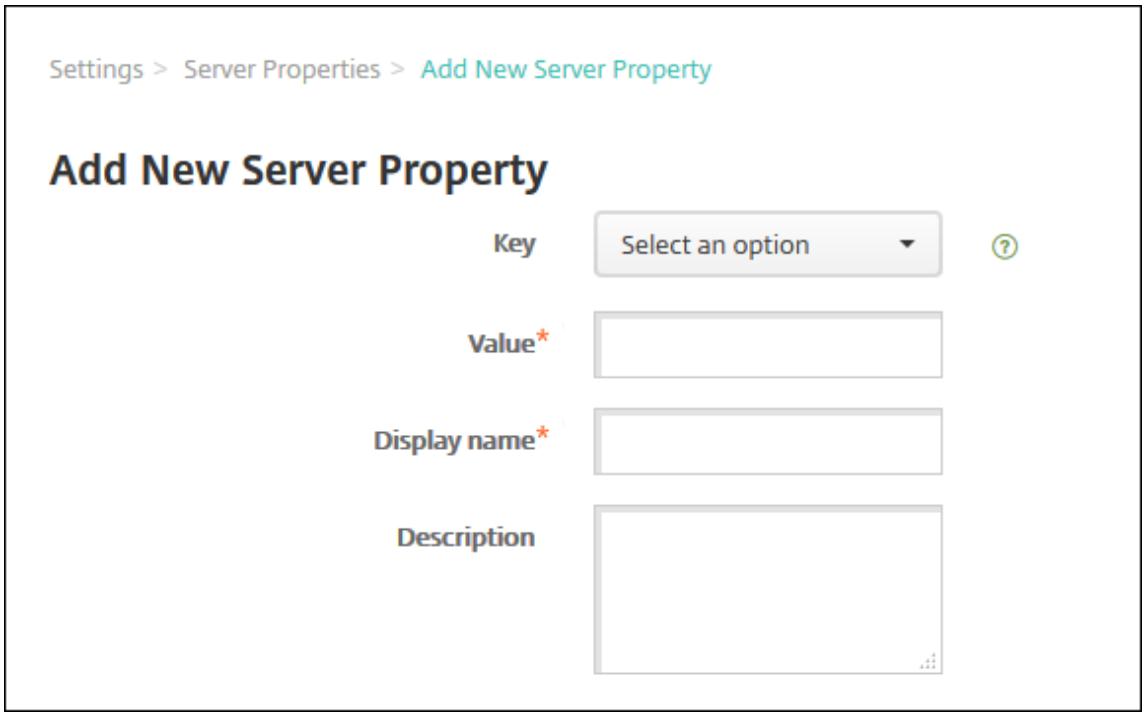
> **Hinweis:**
>
> Zum Neustarten von XenMobile verwenden Sie die Eingabeaufforderung durch den Hypervisor.

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.



Hinzufügen von Servereigenschaften

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. Wenden Sie sich an den Citrix Support, bevor Sie die Eigenschaftswerte bearbeiten oder einen speziellen Schlüssel anfordern.
- Wert: Geben Sie abhängig vom ausgewählten 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.

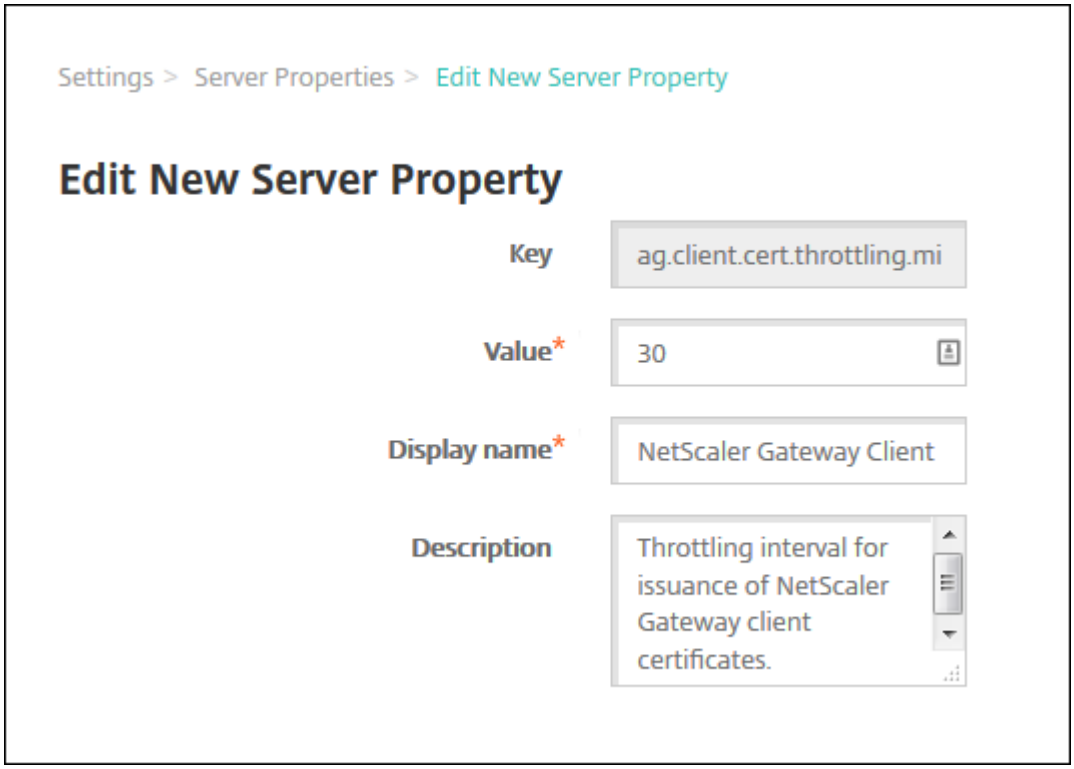
3. Klicken Sie auf **Speichern**.

Bearbeiten von Servereigenschaften

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

   Wenn Sie das Kontrollkästchen neben einer Servereigenschaft aktivieren, wird oberhalb der Liste der Servereigenschaften ein Optionsmenü angezeigt. Klicken Sie an eine andere Stelle in der Liste, um das Menü mit den Optionen rechts daneben zu öffnen.

2. Klicken Sie auf **Edit**. Die Seite **Neue Servereigenschaft bearbeiten** wird angezeigt.



3. Ändern Sie nach Bedarf die folgenden Informationen:
   - Schlüssel: Sie können dieses Feld nicht ändern.
   - Wert: Wert der Eigenschaft.
   - Anzeigename: Name der Eigenschaft.
   - Beschreibung: Beschreibung der Eigenschaft.

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

Löschen von Servereigenschaften

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

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

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

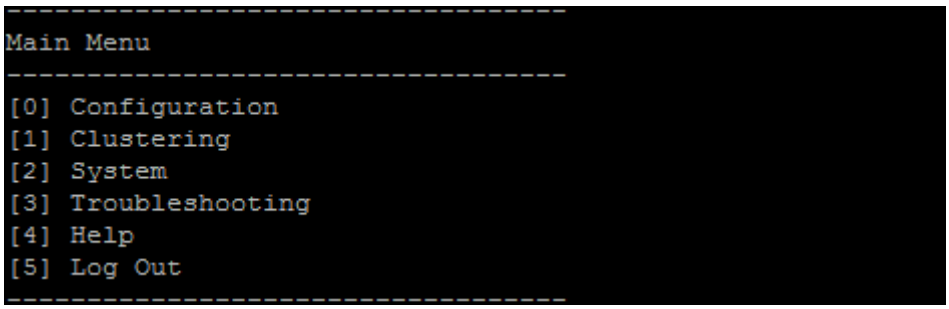
Optionen für die Befehlszeilenschnittstelle

January 5, 2022

Für eine On-Premises-Installation von XenMobile Server können Sie auf die Optionen der Befehlszeilenschnittstelle (CLI) zugreifen:

- **Mit dem Hypervisor, in dem XenMobile installiert ist:** 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, wenn SSH für die Firewall aktiviert ist:** Melden Sie sich bei Ihrem Administratorkonto für XenMobile an.

Mit der CLI können Sie verschiedene Aufgaben zur Konfiguration und Problembehandlung durchführen. Die folgende Abbildung zeigt das Hauptmenü der CLI.



Optionen des Menüs “Configuration”

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


```
-----------------------------------
Configuration Menu
-----------------------------------
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----------------------------------
```

[1] Network

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  IP address [10.207.87.75]:10.200.87.75
  Netmask [255.255.254.0]:255.255.254.0
  Default gateway [10.207.86.1]:10.200.86.1
  Primary DNS server [10.207.86.50]:10.200.86.50
  Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]:
```


[2] Firewall

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

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

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

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

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

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

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

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

[3] Database

```
  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]:
```

Optionen des Menüs “Clustering”

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

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

[1] Show Cluster Status

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```

[2] Enable/Disable cluster

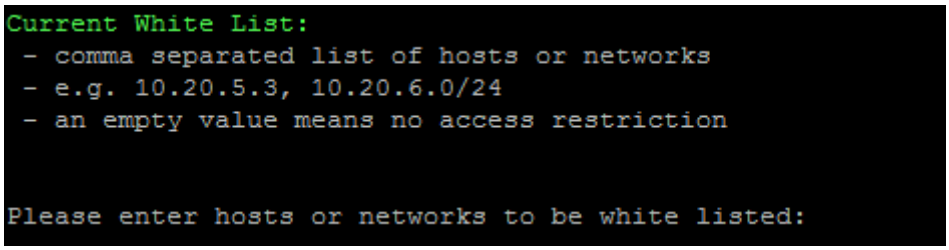
Wenn Sie das Clustering aktivieren, wird die folgende Meldung angezeigt:

```
To enable real-time communication between cluster members, please open port
 80 using the Firewall menu option in CLI menu. Also configure Access white
 list under Firewall settings for restricted access.
```

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 SSL-Offloading aktivieren oder deaktivieren wird die folgende Meldung angezeigt:

```
Enabling SSL offload opens port 80 for everyone. Please configure Access
white list under Firewall settings for restricted access.
```

[5] Display Hazelcast Cluster

Wenn Sie Hazelcast-Cluster anzeigen, werden die folgenden Optionen angezeigt:

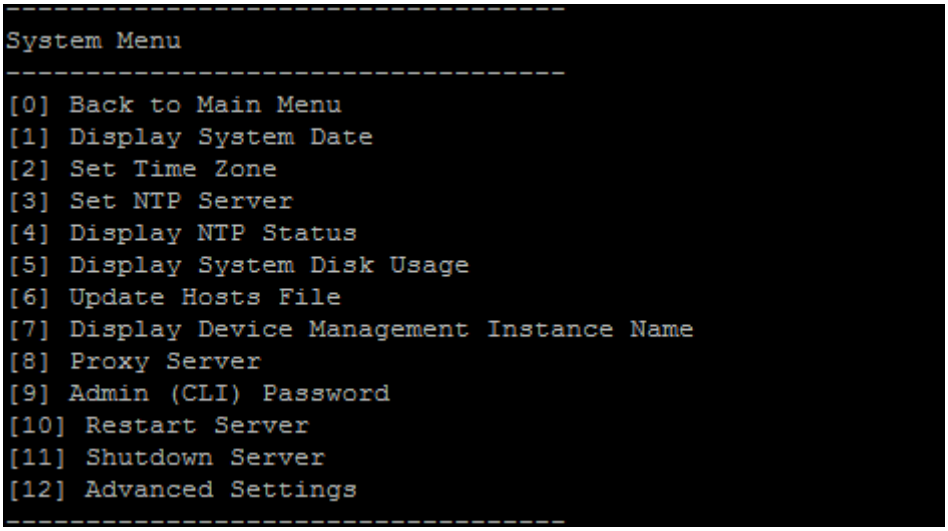
Hazelcast Cluster Members:

[Aufgeführte IP-Adressen]

> **Hinweis:**
>
> Ist der konfigurierte Knoten nicht Teil des Clusters, müssen Sie den Knoten neu starten.

Optionen des Menüs “System”

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



Mit “Set NTP Server” können Sie Informationen zum NTP-Server festlegen. Vermeiden Sie Zeitzonenprobleme, die beim Synchronisieren der Uhrzeit auf dem XenMobile-Server mit einem Hypervisor auftreten können, indem Sie XenMobile auf einen NTP-Server verweisen lassen. Starten Sie alle Clusterserver neu, nachdem Sie diese Option geändert haben.

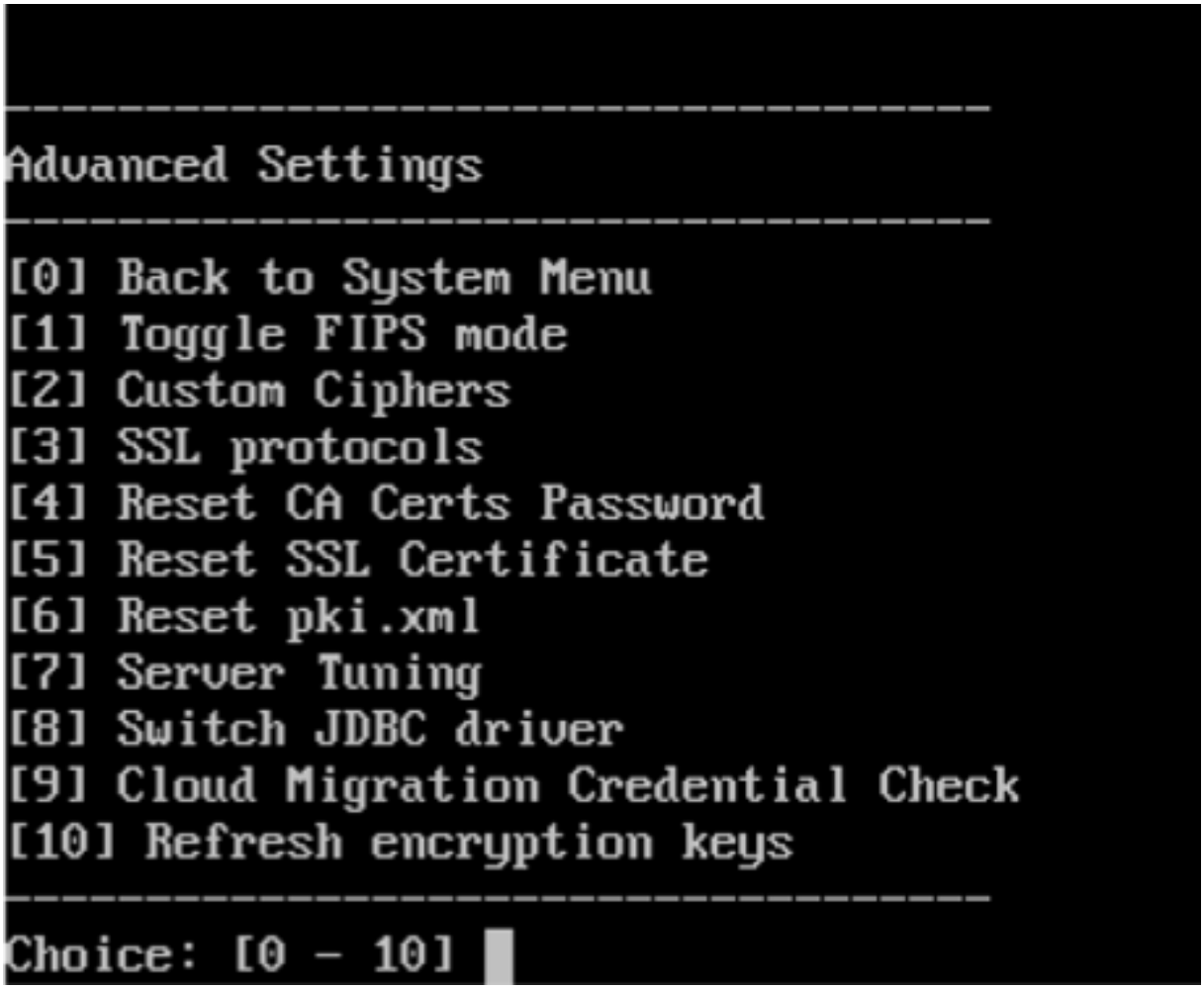
Sie können den Speicherplatz auch über den Menübefehl **[5]Display System Disk Usage** überprüfen.

Informationen zum Herunterfahren von Serverknoten

Wenn Sie einen einzelnen Serverknoten in einem Cluster herunterfahren, können andere Knoten in der Regel die Arbeitslast bewältigen, wenn sie die unter Skalierbarkeit und Leistung dokumentierten Anforderungen erfüllen. Die Auswirkung kann variieren, je nachdem, wie viele Knoten gleichzeitig ausfallen, wie viele Benutzer es insgesamt gibt und wie lange die Knoten ausfallen.

- Benutzer können weiter auf Secure Hub und den Store zugreifen.
- Benutzer können weiter auf bereitgestellte verwaltete Apps zugreifen und sie starten, wenn ein verfügbarer Knoten die Anzahl der Benutzer verarbeiten kann. Verbindungen sind möglicherweise langsamer, was zu langsamerem Einchecken von Geräten führt.
- Geräterichtlinien funktionieren weiterhin, sofern nicht alle Knoten ausgefallen sind. Abhängig von den Ressourcen und der Anzahl der Geräte werden Richtlinien möglicherweise langsamer bereitgestellt.

[12] Advanced Settings



SSL protocols: standardmäßig alle zulässigen Protokolle. Geben Sie nach der Aufforderung **New SSL protocols to enable** die Protokolle ein, die Sie aktivieren möchten. Alle Protokolle, die Sie nicht eingeben, werden von XenMobile deaktiviert. Beispiel: Zum Deaktivieren von TLSv1 geben Sie `TLSv1.2,TLSv1.1` ein und anschließend **y**, um XenMobile Server neu zu starten.

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

Die Optionen für **Switch JDBC driver** sind **jTDS** und **Microsoft JDBC**. Der Standardtreiber ist jTDS. Weitere Informationen über den Wechsel zum Microsoft JDBC-Treiber finden Sie unter SQL Server-Treiber.

Optionen des Menüs “Troubleshooting”

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
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

[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 debug log file
[2] Display update 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
-----------------------------------
```

[4] Disk Usage

```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

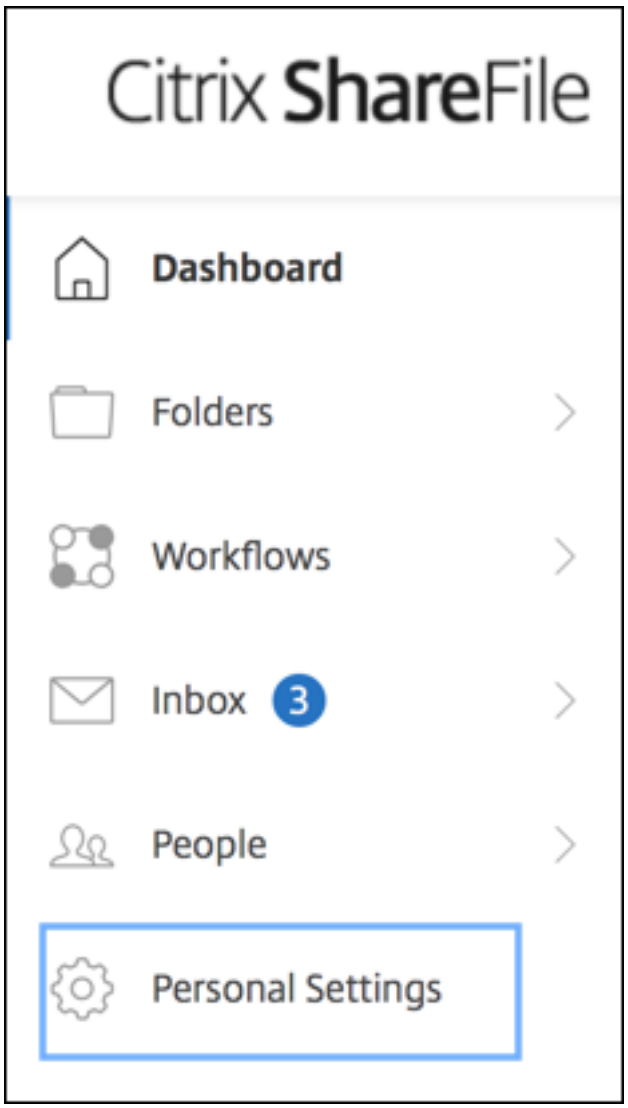
Hochladen eines Supportpakets mit Citrix Files als FTP-Site

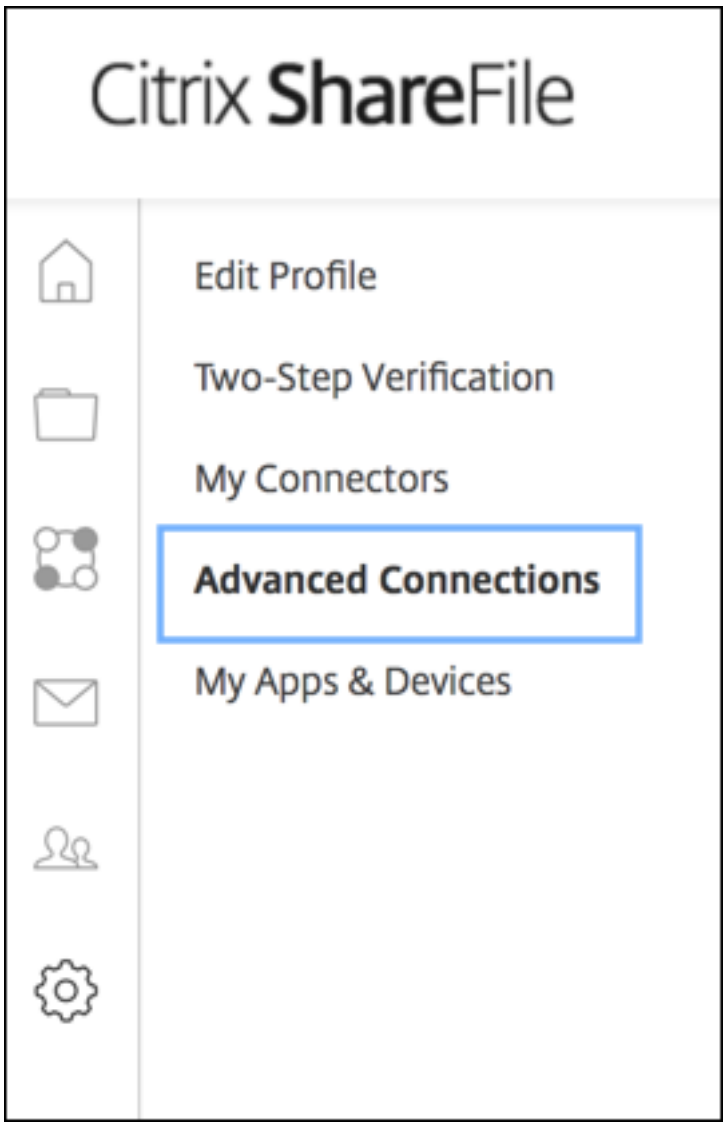
Vor dem Hochladen eines Supportpakets konfigurieren Sie die folgenden Voraussetzungen in Citrix Files:

1. Überprüfen Sie die FTP-Anmeldedetails.

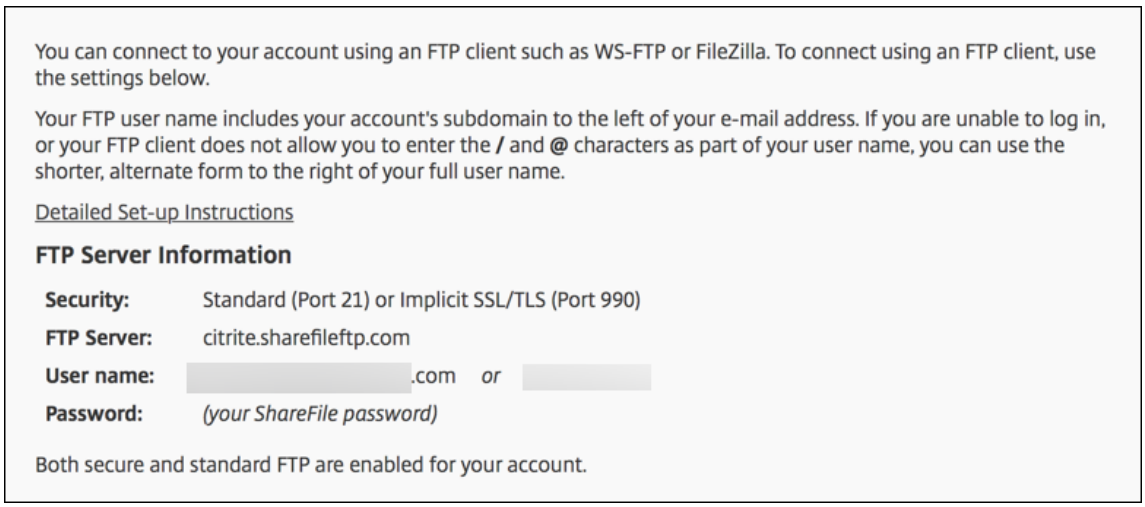
   a. Öffnen Sie https://citrix.sharefile.com in einem Webbrowser.

   b. Klicken Sie auf **Personal Settings** und dann auf **Advanced connections**.





c. Überprüfen Sie, ob in den FTP-Serverinformationen als Benutzername eine alphanumerische Benutzer-ID und die Standardangaben für Subdomäne/Benutzername angezeigt werden.


You can connect to your account using an FTP client such as WS-FTP or FileZilla. To connect using an FTP client, use the settings below.

Your FTP user name includes your account's subdomain to the left of your e-mail address. If you are unable to log in, or your FTP client does not allow you to enter the / and @ characters as part of your user name, you can use the shorter, alternate form to the right of your full user name.

Detailed Set-up Instructions

FTP Server Information

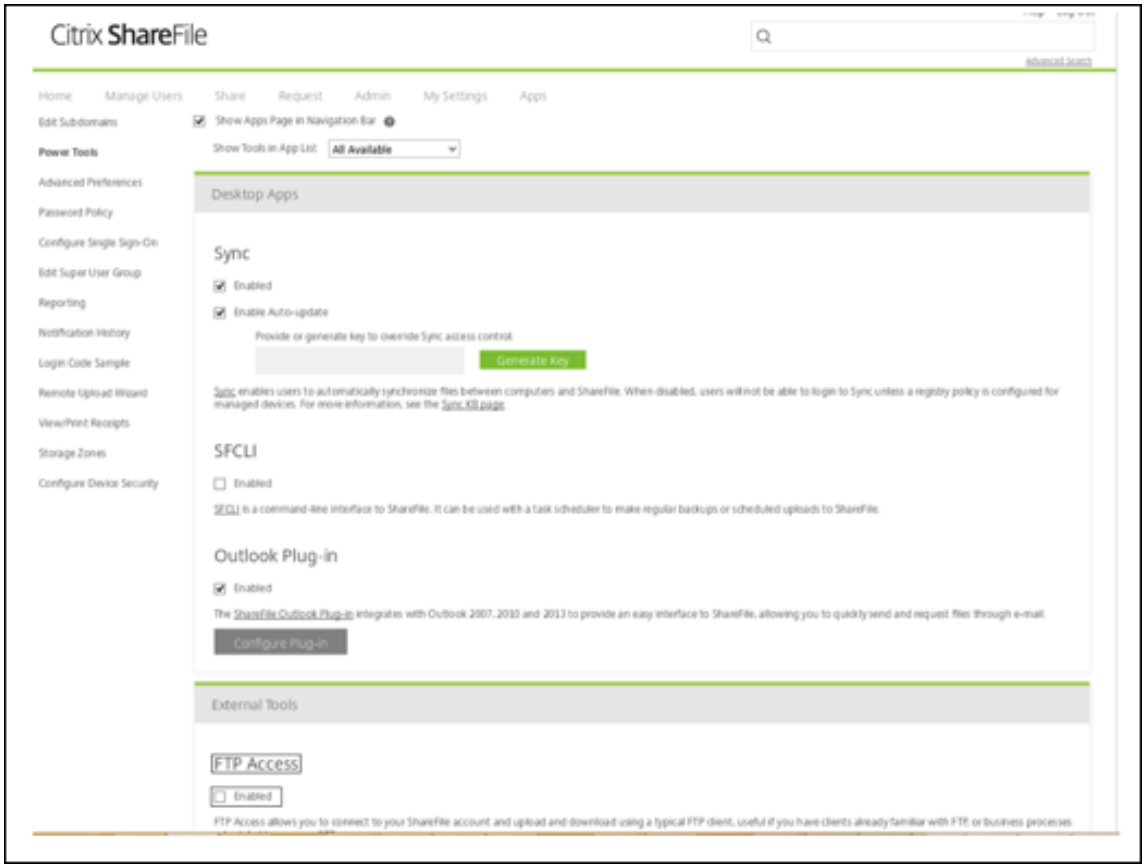
Security:	Standard (Port 21) or Implicit SSL/TLS (Port 990)
FTP Server:	citrite.sharefileftp.com
User name:	.com *or*
Password:	*(your ShareFile password)*

Both secure and standard FTP are enabled for your account.

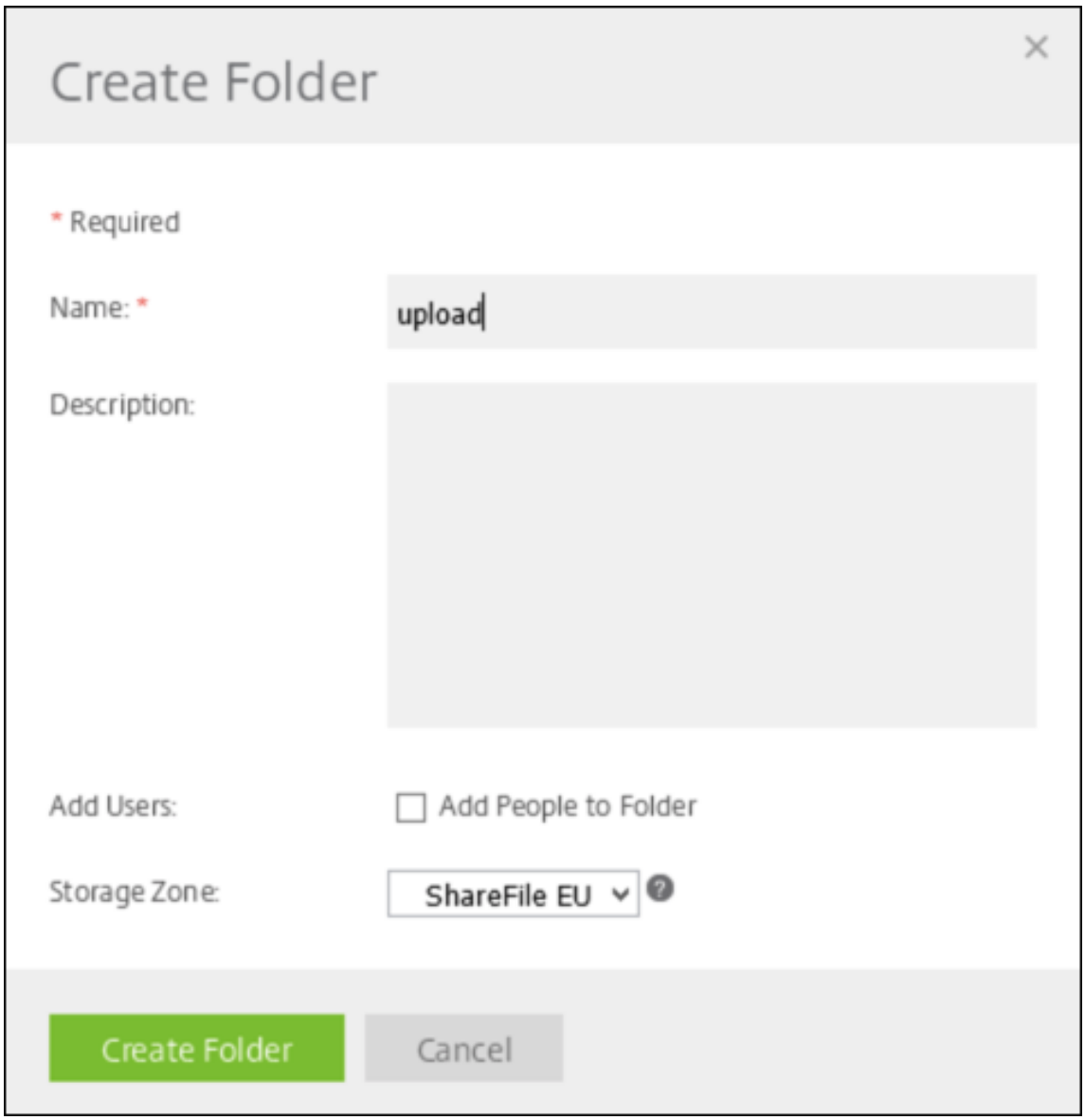
> **Hinweise:**
>
> - Die Datei, die Sie von XenMobile hochladen, ist ein Linux CLI-basierter FTP-Client. Daher können Sie keinen umgekehrten Schrägstrich () und At-Zeichen (@) als Teil Ihres Benutzernamens eingeben.
> - Wenn die alphanumerische Benutzer-ID nicht angezeigt wird, können Sie diese Benutzer-ID von Ihrem Content Collaboration-Administrator oder dem Content Collaboration-Support anfordern.

2. Überprüfen Sie, ob der Citrix Files-Server für die FTP-Kommunikation und FTPS aktiviert ist. Im Idealfall erlauben Content Collaboration-Administratoren, dass ein Benutzerkonto für die FTP-Kommunikation geöffnet werden kann. Manchmal ist jedoch nur die FTPS-Kommunikation erlaubt.

   Ein Benutzer mit Administratorrechten kann diese Einstellung überprüfen und aktivieren. Dies erfolgt durch Klicken auf **Settings**, **Admin Settings**, **Advanced Preferences**und dann auf **Enable ShareFile Tools**. Prüfen Sie in **External Apps**, **FTP Access**, dass das Kontrollkästchen **Enable** ausgewählt ist.



3. Erstellen Sie einen freigegebenen Ordner, der dann vom FTP-Client als Verzeichnis für Dateiuploads verwendet wird. Klicken Sie auf **Home**, **Folders** und dann auf **Personal Folders**.
4. Klicken Sie ganz rechts auf das Pluszeichen (+), klicken Sie auf **Create Folder** und geben Sie einen Namen für den Ordner ein.



5. Wählen Sie in der XenMobile Server-CLI unter **Main Menu** die Option **Troubleshooting > Support Bundle**. Wählen Sie dann unter **Support Bundle Menu** die Option **Generate Support Bundle**.

> **Hinweis:**
>
> Wenn bereits ein Supportpaket vorhanden ist, geben Sie bei entsprechender Aufforderung **y** ein, um das Paket zu überschreiben.

6. Laden Sie das Supportpaket auf den FTP-Server hoch:

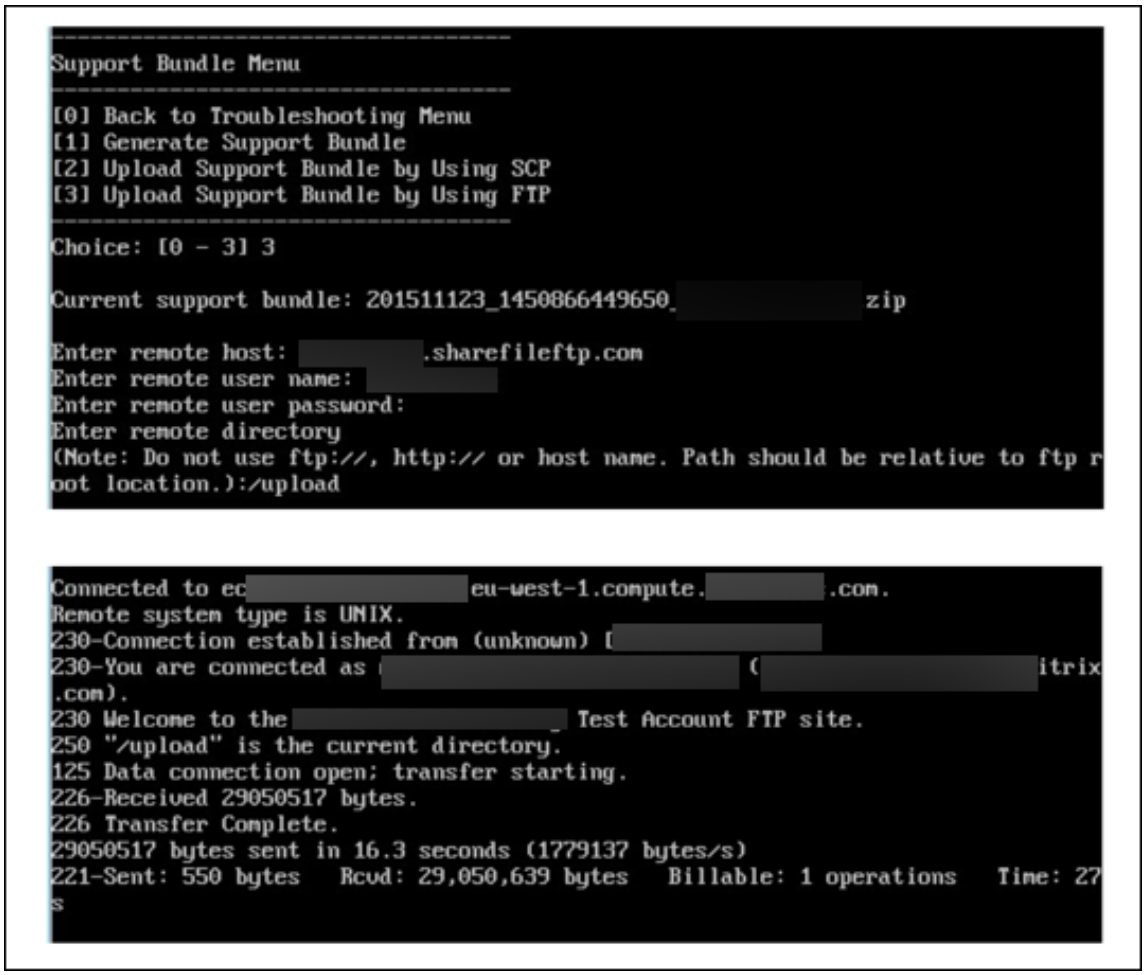
   a. Wählen Sie **Upload Support Bundle by using FTP**.

   b. **Enter remote Host:** Geben Sie auf Aufforderung Ihren FTP-Servernamen ein. Wenn Citrix Files als FTP-Server verwendet wird, geben Sie Ihren Firmennamen ein, gefolgt vom Namen der Citrix Files-FTP-Site. Beispiel: citrix.sharefileftp.com.

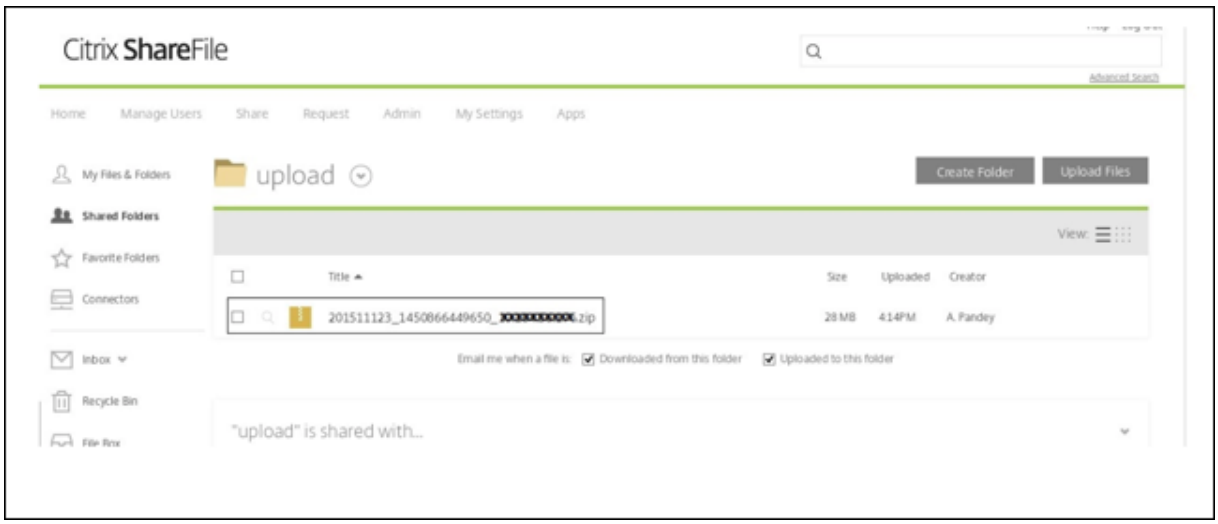
c. **Enter remote user name:** Geben Sie auf Aufforderung die alphanumerische Benutzer-ID ein.

d. **Enter remote user password** Geben Sie auf Aufforderung Ihr Kennwort ein.

e. **Enter remote directory:** Geben Sie auf Aufforderung den Namen des in Citrix Files erstellten freigegebenen Ordners ein und drücken Sie die **Eingabetaste**.



Sie sehen dann das hochgeladene Supportpaket im freigegebenen Ordner, den Sie in Citrix Files erstellt haben.



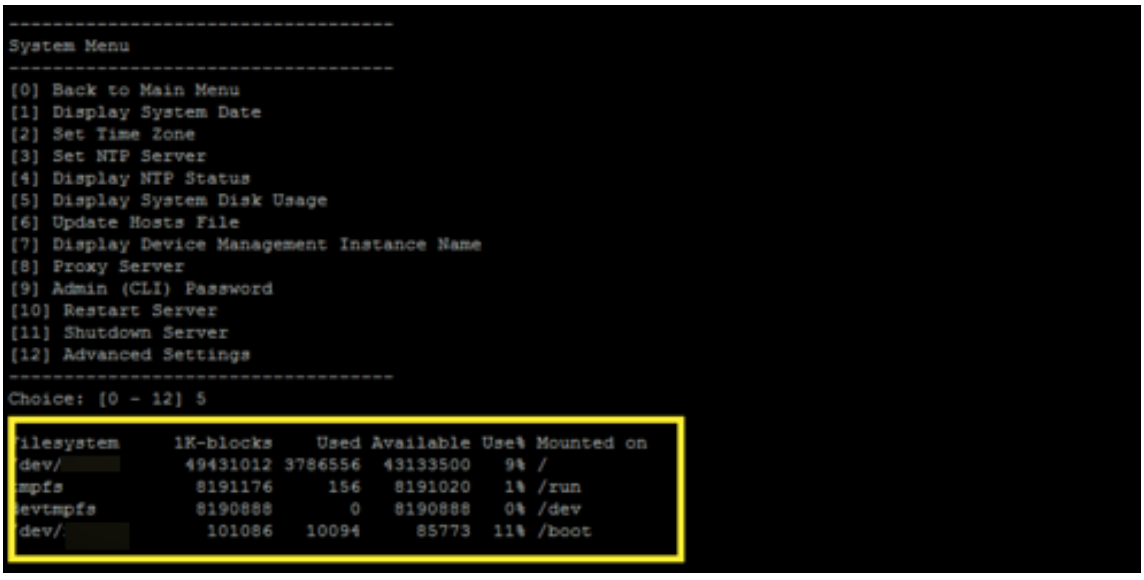
Weitere Informationen zu Citrix Files FTP finden Sie in diesem Citrix Knowledge Center-Artikel.

Speicherplatzüberprüfung

Sie können den Systemspeicher wie folgt in der CLI überprüfen:

1. Wählen Sie unter “Main Menu” die Option **System Menu**.
2. Wählen Sie unter **System Menu** die Option **Display System Disk Usage**.

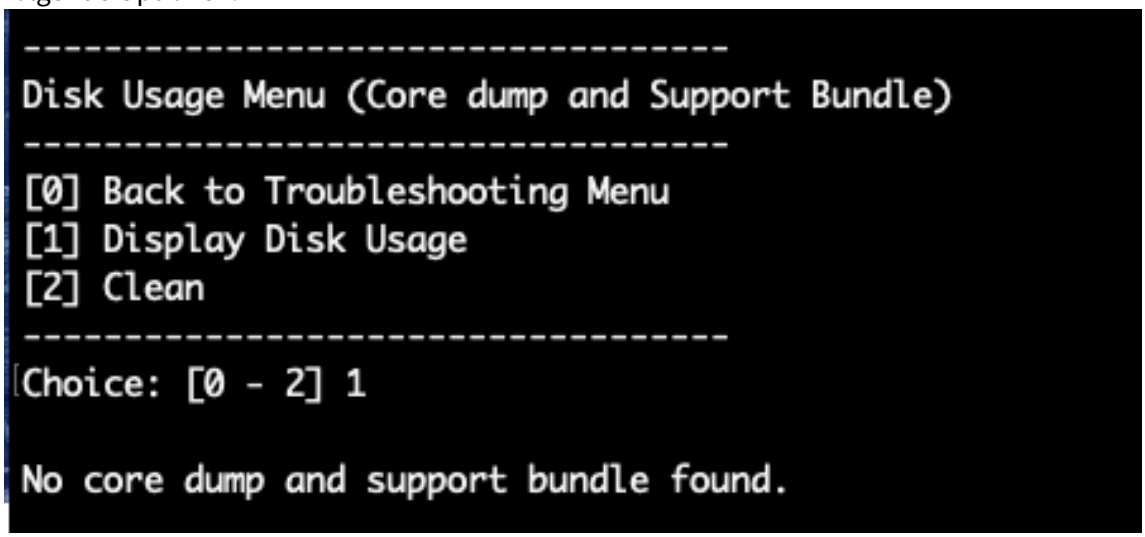
   Die Dateisysteminformationen werden angezeigt.



Ausführen einer Self-Service-Datenträgerbereinigung

Der Datenträger kann über die CLI wie folgt bereinigt werden:

1. Wählen Sie im **Troubleshooting Menu** die Option **Disk Usage**. Das **Disk Usage Menu** bietet folgende Optionen:



2. Geben Sie 1 ein, um die Coredump- und Supportpaket-Dateien aufzulisten. Wenn keine Dateien vorhanden sind, wird die folgende Meldung angezeigt: **No core dump and support bundles found.**
3. Geben Sie 2 ein, um die gescannte Coredump- und Supportpaket-Datei zu bereinigen

Workflows für erste Schritte mit der XenMobile-Konsole

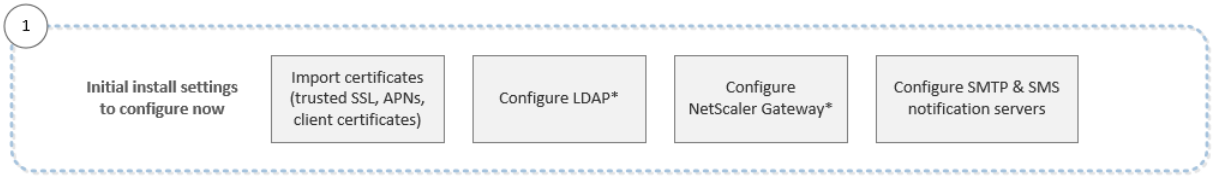
January 5, 2022

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 im Artikel zur XenMobile-Kompatibilität.

Workflow für erste Einstellungen

Wenn Sie XenMobile über die Befehlszeilenkonsole und anschließend in der XenMobile-Konsole konfiguriert haben, wird das Dashboard geöffnet. Sie können nicht zu den Bildschirmen für die Erstkonfiguration zurückkehren. Wenn Sie einige Konfigurationen bei der Installation übersprungen haben, können Sie die folgenden Einstellungen in der Konsole konfigurieren. Bevor Sie Benutzer, Apps und Geräte hinzufügen, empfiehlt sich das Festlegen dieser Installationseinstellungen. Klicken Sie zunächst in der 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 und Abschnitten der Citrix Produktdokumentation:

- Authentifizierung
- Citrix 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. Weitere Informationen finden Sie unter Google Play Launch.
- Erstellen eines Android Enterprise-Administratorkontos. Details finden Sie unter Android Enterprise.
- Lassen Sie Ihre Domäne von Google überprüfen. Weitere Informationen finden Sie unter Domain für Google Workspace bestätigen.
- Aktivieren Sie APIs und erstellen Sie ein Dienstkonto für Android Enterprise. Weitere Informationen finden Sie in der Hilfe für Android Enterprise.

iOS

- Erstellen Sie eine Apple-ID und ein Developer-Konto. Informationen finden Sie unter Apple Developer Program.
- Erstellen Sie ein APNs-Zertifikat. Wenn Sie iOS-Geräte in XenMobile Server verwalten möchten, benötigen Sie ein APNs-Zertifikat von Apple. Wenn Sie Push-Benachrichtigungen für die Secure Mail-Bereitstellung verwenden, benötigen Sie ebenfalls ein APNs-Zertifikat von Apple. Weitere 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 Secure Mail für iOS.
- Erstellen Sie ein Volume Purchase-Unternehmenstoken. Weitere Informationen finden Sie unter Apple Volume Purchasing Program.

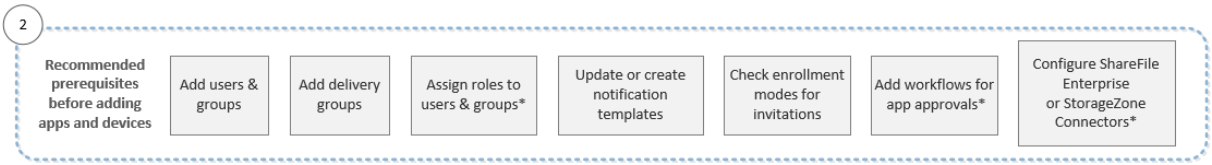
Windows

- Erstellen Sie ein Entwicklerkonto für den Microsoft Windows-Store. Weitere Informationen finden Sie unter Kontotypen, Standorte und Gebühren.
- Beschaffen Sie eine Herausgeber-ID für den Microsoft Windows-Store. Weitere Informationen finden Sie unter Verwalten Ihrer Kontoeinstellungen und Profilinformationen.
- Beschaffen Sie ein Unternehmenszertifikat von DigiCert. Weitere Informationen finden Sie unter Company app distribution for Windows Phone.
- Stellen Sie sicher, dass Sie ein öffentliches SSL-Zertifikat haben, wenn Sie XenMobile-Autodiscovery für die Registrierung von Windows Phone-Geräten verwenden möchten. Weitere Informationen finden Sie unter XenMobile Autodiscovery Service.
- Erstellen Sie ein Anwendungsregistrierungstoken (AET). Weitere Informationen finden Sie unter How to generate an application enrollment token for Windows Phone.

Workflow für Konsolenvoraussetzungen

Der Workflow zeigt Voraussetzungen, deren Konfiguration vor dem Hinzufügen von Apps und Geräten erforderlich ist.

> **Hinweis:**
>
> Die mit einem Sternchen gekennzeichneten Elemente sind optional.



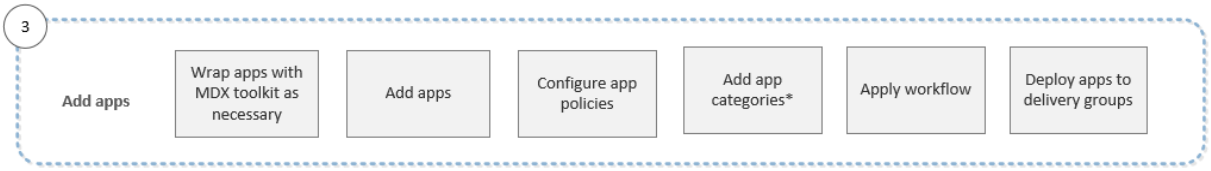
Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden Artikeln und Abschnitten der Citrix Produktdokumentation:

- Benutzerkonten, Rollen und Registrierungseinstellungen
- Bereitstellen von Ressourcen
- Konfigurieren von Rollen mit RBAC
- Benachrichtigungen
- Anwenden von Workflows
- Verwenden von Citrix Content Collaboration mit XenMobile

Workflow beim Hinzufügen von Apps

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 und Abschnitten der Citrix Produktdokumentation:

- Informationen zum MDX Toolkit
- Hinzufügen von Apps
- MDX-Richtlinien auf einen Blick
- Anwenden von Workflows
- Bereitstellen von Ressourcen

Workflow beim Hinzufügen von Geräten

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

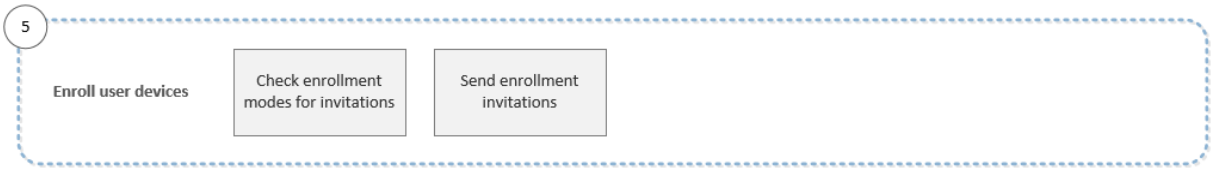
> **Hinweis:**
>
> Die mit einem Sternchen gekennzeichneten Elemente sind optional.

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

- Geräte
- Unterstützte Gerätebetriebssysteme
- Bereitstellen von Ressourcen
- Support und Überwachung
- Automatisierte Aktionen

Workflow beim Registrieren von Benutzergeräten

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



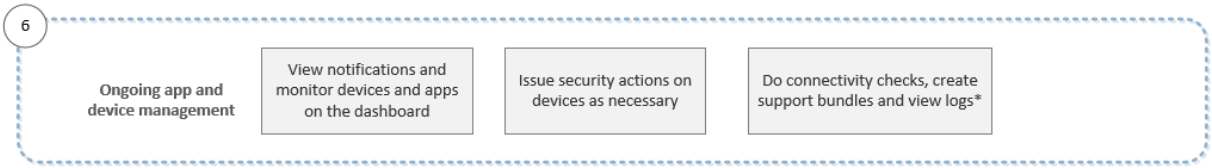
Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden Artikeln der Citrix Produktdokumentation:

- Benutzerkonten, Rollen und Registrierungseinstellungen
- Benachrichtigungen

Workflow bei der Verwaltung von Apps und Geräten

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

> **Hinweis:**
>
> Die mit einem Sternchen gekennzeichneten Elemente sind optional.



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

Zertifikate und Authentifizierung

January 5, 2022

Mehrere Komponenten spielen bei der Authentifizierung in XenMobile eine Rolle:

- **XenMobile Server:** In XenMobile Server legen Sie Registrierungssicherheit und die Registrierungserfahrung fest. Optionen für das Onboarding von Benutzern:
  - Registrierung für alle oder nur auf Einladung.
  - Zweistufige oder dreistufigen Authentifizierung. Sie können in den Clienteigenschaften in XenMobile die Authentifizierung mit Citrix PIN aktivieren und die Komplexität sowie das Ablaufdatum der PIN konfigurieren.

- **Citrix ADC:** Citrix ADC ermöglicht das Beenden von Micro-VPN-SSL-Sitzungen. Citrix ADC bietet zudem Sicherheit bei der Datenübertragung im Netzwerk und ermöglicht das Definieren der Authentifizierungserfahrung beim Zugriff auf Apps durch Benutzer.
- **Secure Hub:** Secure Hub und XenMobile Server wirken bei der Registrierung zusammen. Secure Hub ist auf Geräten die Entität, die mit Citrix ADC kommuniziert: Wenn eine Sitzung abläuft, erhält Secure Hub ein Authentifizierungsticket von Citrix ADC und übergibt es an die MDX-Apps. Citrix empfiehlt das Zertifikatpinning zum Schutz vor Man-in-the-Middle-Angriffen. Weitere Informationen finden Sie in diesem Abschnitt im Secure Hub-Artikel zum Zertifikatpinning.

  Secure Hub moderiert zudem den MDX-Sicherheitscontainer durch Übertragen von Richtlinien, Erstellen einer Sitzung mit Citrix ADC 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 Citrix ADC und erzwingen Einschränkungen für den Offlinemodus sowie die Einhaltung von Clientrichtlinien (z. B. Timeouts).

Weitere Informationen zur Konfiguration der Authentifizierung und eine Übersicht über die 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 bzw. mit Domäne und Sicherheitstoken
- Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne
- PKI-Entitäten
- Anmeldeinformationsanbieter
- APNs-Zertifikate
- SAML für Single Sign-On mit Citrix Files
- Einstellungen des Microsoft Azure Active Directory-Servers
- So senden Sie ein Zertifikat an Geräte zur Authentifizierung am Wi-Fi-Server: Wi-Fi-Geräterichtlinie
- Senden eines eindeutigen Zertifikats, das nicht für die Authentifizierung verwendet wird, z. B. des Zertifikats einer internen Stammzertifizierungsstelle, oder einer bestimmten Richtlinie: Anmeldeinformationsrichtlinie

Zertifikate

XenMobile generiert bei der Installation ein selbstsigniertes SSL-Zertifikat (Secure Socket Layer) zum Sichern der Kommunikation mit dem Server. Sie müssen das SSL-Zertifikat durch ein vertrauenswürdiges SSL-Zertifikat einer 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. Bei konfigurierter Clientzertifikatauthentifizierung geben die Benutzer ihre Citrix PIN für Single Sign-On (SSO) ein, um Zugriff auf XenMobile-aktivierte Apps zu erhalten. 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
Citrix Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Stamm (Citrix Gateway konvertiert PFX automatisch in PEM).
XenMobile Server	.p12 (.pfx auf Windows-basierten Computern)	SSL, SAML, APNs (XenMobile generiert während des Installationsprozesses auch eine vollständige PKI.) Wichtig: XenMobile Server unterstützt keine Zertifikate mit der Erweiterung “.pem”. Für die Verwendung eines PEM-Zertifikats müssen Sie die PEM-Datei in ein Zertifikat und einen Schlüssel unterteilen und diese einzeln in XenMobile Server importieren.
StoreFront	PFX (PKCS #12)	SSL, Stamm

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

Für Citrix Gateway und XenMobile Server empfiehlt Citrix das Abrufen von Serverzertifikaten einer öffentlichen Zertifizierungsstelle, z. B. Verisign, DigiCert oder Thawte. Sie können eine Zertifikatsignieranforderung (CSR) mit dem Citrix 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 Citrix Gateway oder XenMobile installieren.

> **Wichtig: Anforderungen für vertrauenswürdige Zertifikate in iOS, iPadOS und macOS**
>
> Apple stellt neue Anforderungen an TLS-Serverzertifikate. Stellen Sie sicher, dass alle Zertifikate den neuen Apple-Anforderungen entsprechen. Siehe Apple-Veröffentlichung https://support.apple.com/en-us/HT210176.
>
> Apple verkürzt die Gültigkeitsdauer von TLS-Serverzertifikaten. Diese Änderung betrifft nur Serverzertifikate, die nach September 2020 ausgestellt werden. Siehe Apple-Veröffentlichung https://support.apple.com/en-us/HT211025.

Hochladen von Zertifikaten in XenMobile

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, wählen Sie ein Serverzertifikat aus, das die kontextabhängigen Kriterien erfüllt. Beispiel: Sie konfigurieren die Integration von XenMobile in Ihrer Microsoft-Zertifizierungsstelle. Die Verbindung mit der Microsoft-Zertifizierungsstelle erfordert eine Authentifizierung mit einem Clientzertifikat.

In diesem Abschnitt finden Sie allgemeine Anleitungen zum Hochladen von Zertifikaten. Einzelheiten zum Erstellen, Hochladen und Konfigurieren von Clientzertifikaten finden Sie unter Authentifizierung mit Clientzertifikat oder Zertifikat 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

Sie haben zwei Optionen zum Hochladen von Zertifikaten:

- Einzelupload auf die Konsole.
- Massenupload mit der REST-API auf iOS-Geräte.

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

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

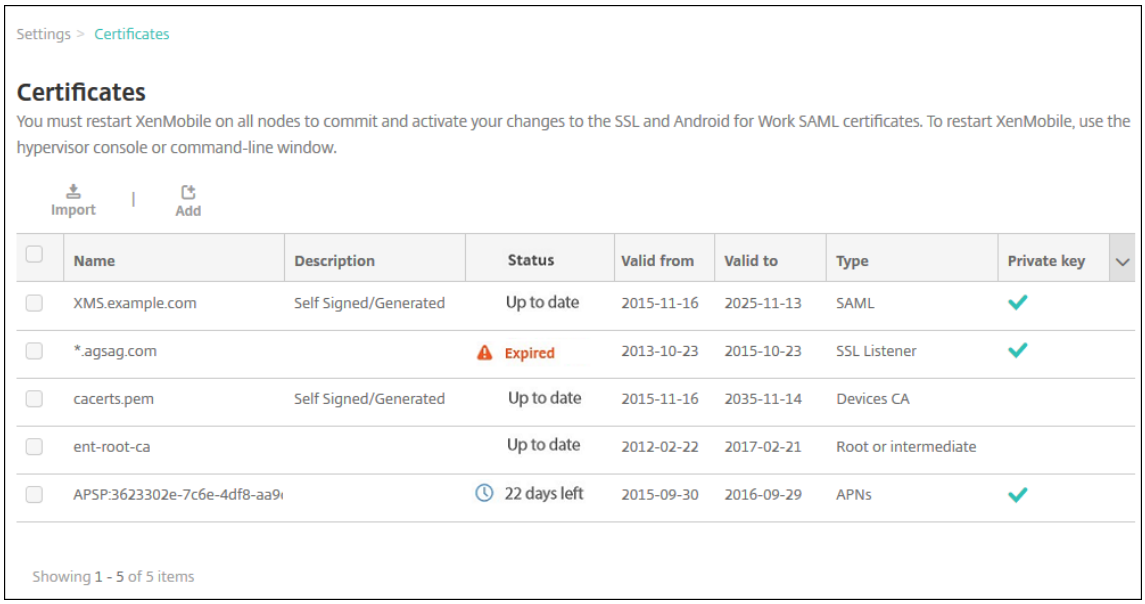
Sie können das ZS-Zertifikat (ohne privaten Schlüssel) hochladen, das von der Zertifizierungsstelle zum Signieren von Zertifikatsanforderungen verwendet wird. Sie können auch ein SSL-Clientzertifikat (mit privatem Schlüssel) für die Clientauthentifizierung hochladen.

Beim Konfigurieren der Entität der Microsoft-Zertifizierungsstelle müssen Sie das ZS-Zertifikat angeben. Dieses wählen Sie aus der Liste aller Serverzertifikate aus, die ZS-Zertifikate sind. 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

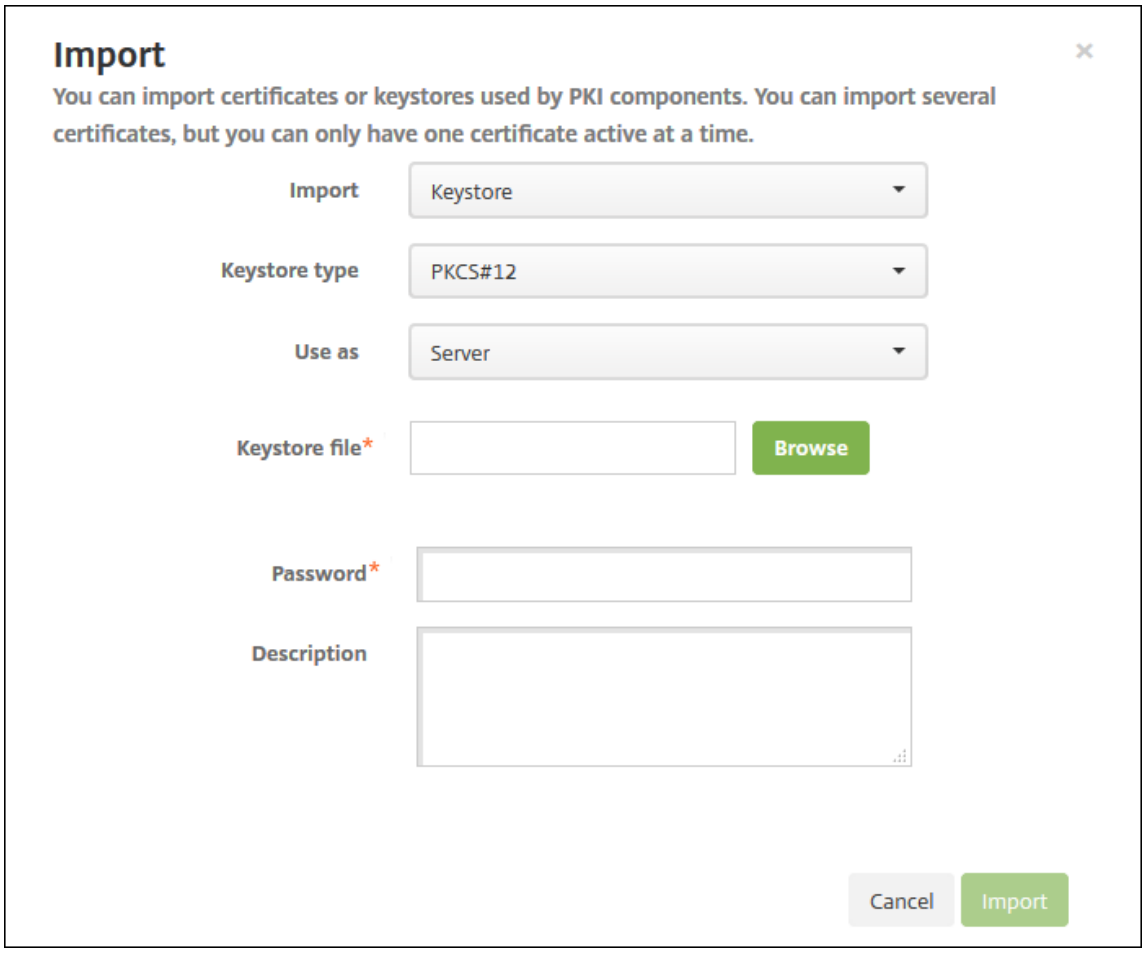
Schlüsselspeicher sind Repositorys mit Sicherheitszertifikaten und können als solche mehrere Einträge enthalten. Beim Laden aus einem Schlüsselspeicher werden Sie aufgefordert, das Alias des gewünschten Eintrags anzugeben. Wenn Sie kein Alias angeben, wird der erste Eintrag aus dem Speicher geladen. 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 Sie das Zertifikat verwenden möchten. Es gibt folgende Optionen:
  - **Server**. Serverzertifikate sind Zertifikate, die funktional von 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 auf Servern, Websites und für Apps bereitstellen.
  - **APNs**. APNs-Zertifikate von Apple 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.

Importieren eines Zertifikats

Beim Importieren eines Zertifikats aus einer Datei oder einem Schlüsselspeichereintrag versucht XenMobile die Erstellung einer Zertifikatkette aus der Eingabe. XenMobile importiert alle Zertifikate in dieser Kette, um jeweils einen Serverzertifikateintrag zu erstellen. 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.

Sie können 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 von 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.

Massenupload von Zertifikaten mit der REST-API auf iOS-Geräte

Wenn der Upload einzelner Zertifikate nicht praktikabel ist, können Sie mit der REST-API einen Massenupload auf iOS-Geräte ausführen. Diese Methode unterstützt Zertifikate im Format .p12. Weitere Informationen zur REST-API finden Sie unter REST-APIs.

1. Benennen Sie jede Zertifikatdatei um und verwenden Sie dabei das Format `device_identity_value.p12`. `device_identity_value` kann für die IMEI, Seriennummer oder MEID jedes Geräts stehen.

   Beispiel: Sie verwenden die Seriennummern als ID. Für ein Gerät mit der Seriennummer `A12BC3D4EFGH` nennen Sie die Zertifikatdatei, die Sie auf dem Gerät installieren möchten, `A12BC3D4EFGH.p12`.

2. Erstellen Sie eine Textdatei, um die Kennwörter für die P12-Zertifikate zu speichern. Geben Sie in dieser Datei die ID und das Kennwort für jedes Gerät auf einer neuen Zeile ein. Verwenden Sie das Format `device_identity_value=password`. Beispiel:

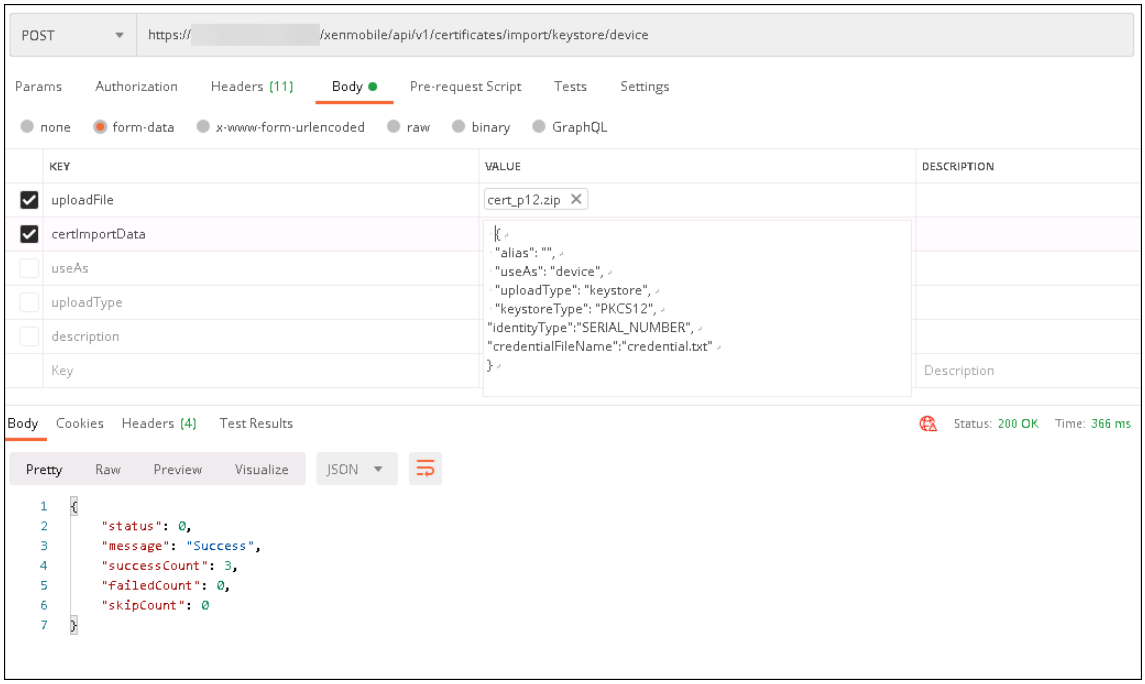
   ```
   A12BC3D4EFGH.p12=password1!
   A12BC3D4EFIJ.p12=password2@
   A12BC3D4EFKL.p12=password3#
   <!--NeedCopy-->
   ```

3. Komprimieren Sie alle Zertifikate und die von Ihnen erstellte Textdatei in eine ZIP-Datei.
4. Starten Sie den REST API-Client, melden Sie sich bei XenMobile an und rufen Sie ein Authentifizierungstoken ab.
5. Importieren Sie die Zertifikate und fügen Sie Folgendes in den Nachrichtentext ein:

   ```
   {

       "alias": "",
       "useAs": "device",
       "uploadType": "keystore",
   ```

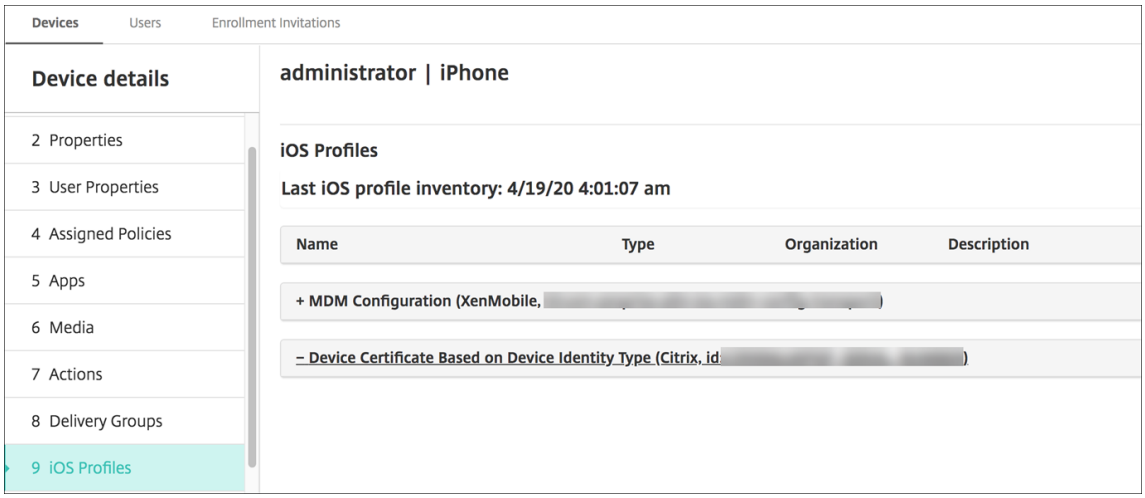


```
    "keystoreType": "PKCS12",
    "identityType":"SERIAL_NUMBER",          # identity type can be
       "SERIAL_NUMBER","IMEI","MEID"
    "credentialFileName":"credential.txt"    # The credential file
       name in .zip
 }

<!--NeedCopy-->
```



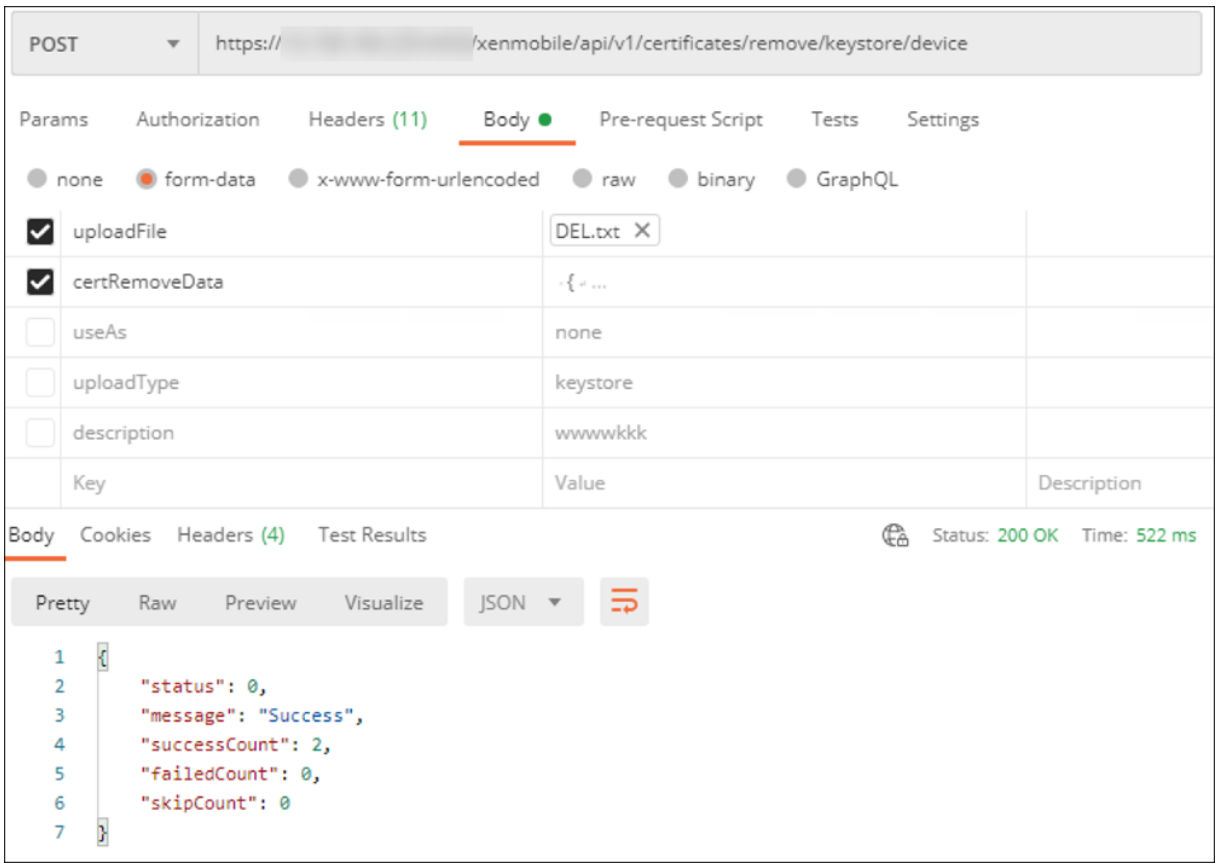
6. Erstellen Sie eine VPN-Richtlinie mit dem Anmeldeinformationstyp **Always on IKEv2** und der Geräteauthentifizierungsmethode **Gerätezertifikat basierend auf Geräteidentität**. Wählen Sie den **Geräteidentitätstyp** aus, den Sie für die Benennung der Zertifikatdateien verwendet haben Weitere Informationen finden Sie unter VPN-Geräterichtlinie.

7. Registrieren Sie ein iOS-Gerät und warten Sie die Bereitstellung der VPN-Richtlinie ab. Überprüfen Sie die Zertifikatinstallation anhand der MDM-Konfiguration auf dem Gerät. Sie können auch die Geräteinformationen in der XenMobile-Konsole überprüfen.



Sie können auch eine Massenlöschung von Zertifikaten ausführen, indem Sie eine Textdatei mit dem Wert von `device_identity_value` für jedes zu löschende Zertifikat erstellen. Rufen Sie in der REST API die Lösch-API auf und verwenden Sie die folgende Anforderung, wobei Sie `device_identity_value` durch die entsprechende ID ersetzen:

```
1 ```
2 {
3
4     "identityType"="device_identity_value"
5  }
6
7 <!--NeedCopy--> ```
```

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, können Sie den vorhandenen Eintrag entweder ersetzen oder löschen.

Dies ist die effektivste Methode, Ihre Zertifikate in der XenMobile-Konsole zu aktualisieren: Klicken Sie in der oberen rechten Ecke der Konsole auf das Zahnradsymbol, um die Seite **Einstellungen** zu öffnen. Klicken Sie dann 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.

Verlängern von Zertifikaten

XenMobile Server-intern werden folgende Zertifizierungsstellen für PKI verwendet: Stamm-ZS, Geräte-ZS und Server-ZS. Diese Zertifizierungsstellen werden als logische Gruppe klassifiziert und erhalten einen Gruppennamen. Wenn eine neue XenMobile Server-Instanz bereitgestellt wird, werden die drei Zertifizierungsstellen generiert und erhalten den Gruppennamen “default”.

Sie können die Zertifizierungsstellen für unterstützte iOS-, macOS- und Android-Geräte über die XenMobile Server-Konsole oder die öffentliche REST-API erneuern. Registrierte Windows-Geräte müssen von den Benutzern erneut registriert werden, damit sie eine neue Geräte-ZS erhalten.

Mit folgenden APIs ist das Erneuern bzw. Neugenerieren der XenMobile Server-internen PKI-Zertifizierungsstellen und das Verlängern der von ihnen ausgestellten Gerätezertifikate möglich.

- Gruppenzertifizierungsstellen erstellen
- Neue ZS aktivieren und alte deaktivieren
- Gerätezertifikat in einer konfigurierten Liste von Geräten verlängern. Registrierte Geräte funktionieren weiterhin ohne Unterbrechung. Ein Gerätezertifikat wird ausgegeben, wenn ein Gerät eine Verbindung zum Server herstellt.
- Liste der Geräte zurückgeben, die noch die alte ZS verwenden.
- Alte Zertifizierungsstelle löschen, wenn alle Geräte die neue erhalten haben

Informationen finden Sie im PDF-Dokument Public API for REST Services in folgenden Abschnitten:

- Section 3.16.58, Renew Device Certificate
- Section 3.23, Internal PKI CA Groups

Die Konsole **Manage Devices** enthält die Sicherheitsaktion **Certificate Renewal**, mit der das Registrierungszertifikat auf einem Gerät verlängert wird.

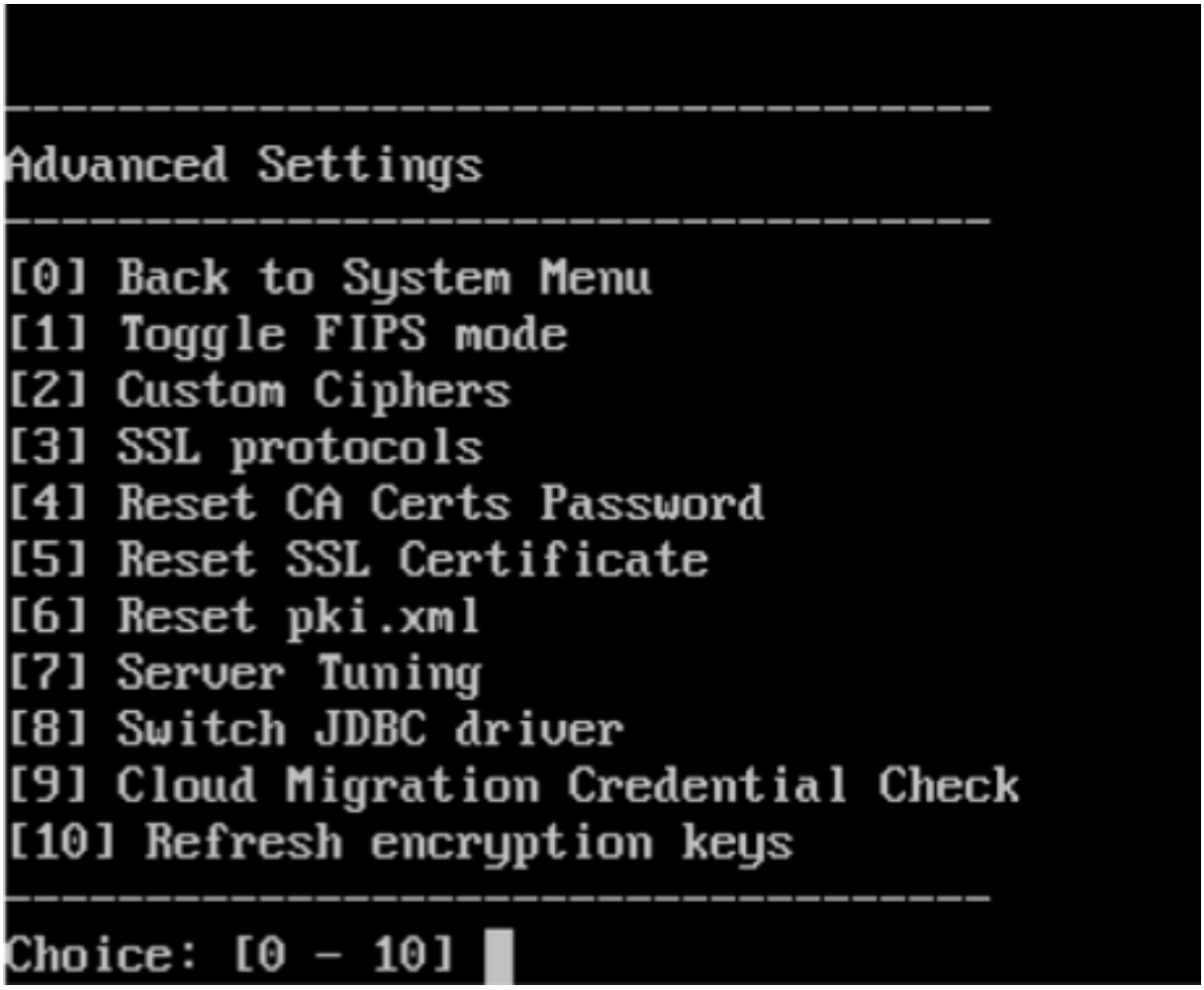
Voraussetzungen

- Das Feature zum Aktualisieren von Zertifikaten ist standardmäßig deaktiviert. Legen Sie zum Aktivieren des Features zum Aktualisieren von Zertifikaten den Wert der Servereigenschaft **refresh.internal.ca** auf **true** fest.

> **Wichtig:**
>
> Ist Citrix ADC für SSL-Offload eingerichtet, stellen Sie beim Generieren eines neuen Zertifikats sicher, dass Sie den Load Balancer mit der neuen cacert.perm aktualisieren. Weitere Informationen zum Citrix Gateway-Setup finden Sie unter So verwenden Sie den SSL-Offload-Modus für Citrix ADC VIPs.

CLI-Option zum Zurücksetzen des Server-ZS-Zertifikatkennworts für Clusterknoten

Nach dem Erstellen eines Server-ZS-Zertifikats auf einem XenMobile Server-Knoten verwenden Sie die XenMobile-CLI, um das Zertifikatkennwort auf anderen Clusterknoten zurückzusetzen. Wählen Sie im CLI-Hauptmenü **System > Advanced Settings > Reset CA certs password**. Wenn Sie das Kennwort zurücksetzen, obwohl es kein neues ZS-Zertifikat gibt, setzt XenMobile das Kennwort nicht zurück.



Verwalten der XenMobile-Zertifikate

Es empfiehlt sich, eine Liste der in einer XenMobile-Bereitstellung verwendeten Zertifikate zu erstellen und insbesondere Ablaufdatum und verknüpfte Kennwörter zu notieren. 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 (Citrix Files)
  - Stamm- und Zwischenzertifikate für die zuvor genannten Zertifikate und andere interne Ressourcen (StoreFront, Proxy usw.)
  - APNs-Zertifikat für die Verwaltung von iOS-Geräten
  - Internes APNs-Zertifikat für Secure Hub-Benachrichtigungen von XenMobile Server
  - PKI-Benutzerzertifikat für die Verbindung mit der PKI

- MDX Toolkit
  - Apple Developer-Zertifikat
  - Apple-Provisioningprofil (pro Anwendung)
  - APNs-Zertifikat von Apple (zur Verwendung für Citrix Secure Mail)
  - Android-Schlüsselspeicherdatei
  - Windows Phone – DigiCert-Zertifikat

  Das MAM-SDK umschließt Apps nicht und erfordert daher kein Zertifikat.
- Citrix ADC
  - SSL-Zertifikat für MDM-FQDN
  - SSL-Zertifikat für Gateway-FQDN
  - SSL-Zertifikat für ShareFile StorageZones Controller-FQDN
  - SSL-Zertifikat für Exchange-Lastausgleich (Abladung der Konfiguration)
  - SSL-Zertifikat für StoreFront-Lastausgleich
  - Stamm- und Zwischenzertifikate für die o. g. Zertifikate

XenMobile-Richtlinie für den Zertifikatablauf

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 (ZS) fordert Sie vor dem Ablaufdatum zur Verlängerung des SSL-Zertifikats auf.

APNs-Zertifikat für Citrix Secure Mail

APNs-Zertifikate laufen jeweils nach einem Jahr ab. Erstellen Sie vor dem Ablaufen ein APNs-SSL-Zertifikat und aktualisieren Sie es im Citrix Portal. Läuft das Zertifikat ab, verursacht dies für Benutzer Inkonsistenzen bei Secure Mail-Pushbenachrichtigungen. Außerdem können Sie keine weiteren Push-benachrichtigungen für Ihre Apps senden.

APNs-Zertifikat für die Verwaltung von iOS-Geräten

Zum Registrieren und Verwalten von iOS-Geräten bei bzw. mit XenMobile müssen Sie ein APNs-Zertifikat von Apple 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: Die Benachrichtigung enthält die folgenden Informationen:

```
1 The following Apple Push Notification Service certificate, created for
    Apple ID CustomerID will expire on Date. Revoking or allowing this
    certificate to expire will require existing devices to be re-
    enrolled with a new push certificate.
2
3 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.
4
5 Thank You,
6
7 Apple Push Notification Service
8 <!--NeedCopy-->
```

MDX Toolkit (iOS-Verteilungszertifikat)

Für alle nicht aus dem Apple App Store stammenden Apps, die auf einem physischen iOS-Gerät ausgeführt werden, gelten folgend Anforderungen:

- Signieren Sie die App mit einem Provisioningprofil.
- Signieren Sie die App mit einem entsprechenden Verteilungszertifikat.

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.CompanyName.ProductName`.
2. Wählen Sie im Apple Enterprise Developer-Portal **Provisioning Profiles > Distribution** und erstellen Sie ein Provisioningprofil zum hausinternen Gebrauch. 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 Zertifikate von XenMobile Server gültig sind, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der XenMobile-Konsole auf **Einstellungen > Zertifikate**.

2. Vergewissern Sie sich, dass alle Zertifikate (APNs-, SSL- Listener-, Stamm- und Zwischenzertifikate) gültig sind.

Android-Schlüsselspeicher

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.

DigiCert-Zertifikat für Windows Phone-Geräte

DigiCert 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 Windows Marketplace. Weitere Informationen finden Sie unter DigiCert Code Signing Certificates for Windows Phone in der DigiCert-Dokumentation.

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

Citrix ADC

Weitere Informationen zur Handhabung des Zertifikatablaufs bei Citrix ADC finden Sie unter How to handle certificate expiry on NetScaler im Knowledge Center des Citrix Supports.

Ein abgelaufenes Citrix ADC-Zertifikat hindert Benutzer daran, Geräte zu registrieren und auf den Store zuzugreifen. Das abgelaufene Zertifikat verhindert außerdem, dass Benutzer bei der Verwendung von Secure Mail eine Verbindung mit Exchange Server herstellen. Darüber hinaus können Benutzer keine HDX-Apps anzeigen und öffnen (je nachdem, welches Zertifikat abgelaufen ist).

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

- SSL-Zertifikat für MDM-FQDN
- SSL-Zertifikat für Gateway-FQDN
- SSL-Zertifikat für ShareFile StorageZones Controller-FQDN
- SSL-Zertifikat für Exchange-Lastausgleich (Abladung der Konfiguration)
- SSL-Zertifikat für StoreFront-Lastausgleich
- Stamm- und Zwischenzertifikate für die o. g. Zertifikate

Citrix Gateway und XenMobile

January 5, 2022

Wenn Sie Citrix Gateway mit XenMobile konfigurieren, richten Sie die Authentifizierungsmethode für den Remotegerätezugriff auf das interne Netzwerk ein. Mit dieser Funktionalität können Apps auf einem Mobilgerät auf Unternehmensserver im Intranet zugreifen. XenMobile erstellt ein Micro-VPN von den Apps zu Citrix Gateway.

Sie können Citrix Gateway zur Verwendung mit XenMobile konfigurieren, indem Sie ein Skript aus XenMobile exportieren und auf Citrix Gateway ausführen.

Voraussetzungen für die Verwendung des Skripts zur Citrix Gateway-Konfiguration

Citrix ADC-Anforderungen:

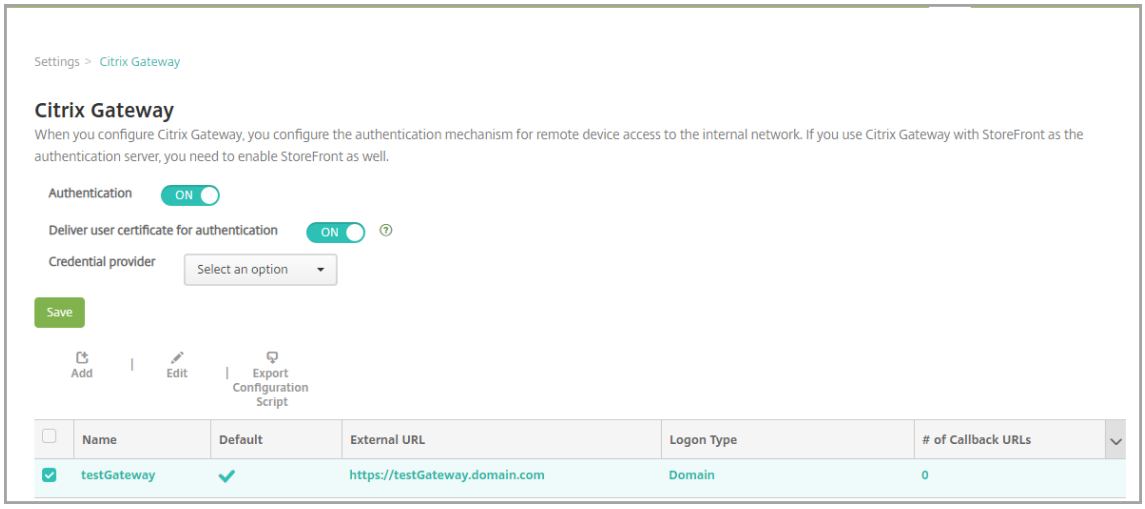
- Citrix ADC (Mindestversion 11.0, Build 70.12).
- Citrix ADC-IP-Adresse ist konfiguriert und verfügt über Konnektivität mit dem LDAP-Server (es sei denn, für LDAP ist ein Lastausgleich eingerichtet).
- Citrix ADC-Subnetz-IP-Adresse (SNIP) ist konfiguriert, verfügt über Konnektivität mit den erforderlichen Back-End-Servern und über Zugriff auf das öffentliche Netzwerk über Port 8443/TCP.
- DNS kann öffentliche Domänen auflösen.
- Citrix ADC ist per Plattform-/Universell- oder Testlizenz lizenziert. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX126049.
- Ein Citrix Gateway-SSL-Zertifikat wurde hochgeladen und in Citrix ADC installiert. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX136023.

Anforderungen für XenMobile:

- XenMobile Server (Mindestversion 10.6).
- LDAP-Server ist konfiguriert.

Konfigurieren der Authentifizierung für den Remotezugriff von Geräten auf das interne Netzwerk

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Server** auf **Citrix Gateway**. Die Seite **Citrix Gateway** wird angezeigt. In dem folgenden Beispiel ist eine Citrix Gateway-Instanz vorhanden.

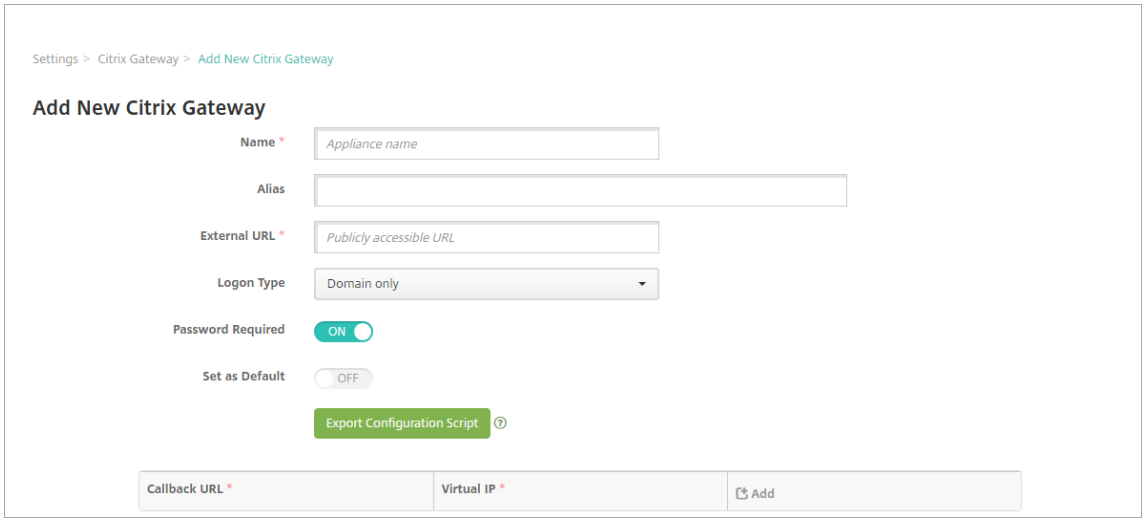


3. Konfigurieren Sie folgende Einstellungen:
   - **Authentifizierung:** Wählen Sie aus, ob die Authentifizierung aktiviert werden soll. Die Standardeinstellung ist **Ein**.
   - **Benutzerzertifikat für Authentifizierung bereitstellen:** Wählen Sie aus, ob XenMobile das Authentifizierungszertifikat zusammen mit Secure Hub verwenden soll, sodass Citrix Gateway die Clientzertifikatauthentifizierung abwickeln kann. Die Standardeinstellung ist **Aus**.
   - **Anmeldeinformationsanbieter:** Klicken Sie in der Liste auf den gewünschten Anmeldeinformationsanbieter. Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.
4. Klicken Sie auf **Speichern**.

Hinzufügen einer Citrix Gateway-Instanz

Nach dem Speichern der Authentifizierungseinstellungen fügen Sie XenMobile eine Citrix Gateway-Instanz hinzu.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Server** auf **Citrix Gateway**. Die Seite **Citrix Gateway** wird angezeigt.
3. Klicken Sie auf **Hinzufügen**. Die Seite **Neues Citrix Gateway hinzufügen** wird angezeigt.



4. Konfigurieren Sie folgende Einstellungen:

   - **Name:** Geben Sie einen Namen für die Citrix Gateway-Instanz ein.
   - **Alias:** Geben Sie optional einen Aliasnamen für Citrix Gateway ein.
   - **Externe URL:** Geben Sie die öffentlich zugängliche URL für Citrix Gateway ein. Beispiel: `https://receiver.com`.
   - **Anmeldetyp:** Wählen Sie einen Anmeldetyp. Zur Auswahl stehen **Nur Domäne**, **Nur Sicherheitstoken**, **Domäne und Sicherheitstoken**, **Zertifikat**, **Zertifikat und Domäne** und **Zertifikat und Sicherheitstoken**. Der Standardwert des Felds **Kennwort erforderlich** ändert sich je nach der Auswahl unter **Anmeldetyp**. Die Standardeinstellung ist **Nur Domäne**.

   Wenn Sie mehrere Domänen haben, verwenden Sie **Zertifikat und Domäne**. Informationen zum Konfigurieren der Authentifizierung für mehrere Domänen mit XenMobile und Citrix Gateway finden Sie unter Konfigurieren der Authentifizierung für mehrere Domänen.

   Wenn Sie **Zertifikat und Sicherheitstoken** verwenden, müssen Sie zur Unterstützung von Secure Hub einige zusätzliche Konfigurationen auf dem Citrix Gateway ausführen. Weitere Informationen finden Sie unter Configuring XenMobile for Certificate and Security Token Authentication.

   Weitere Informationen finden Sie unter Authentifizierung im Bereitstellungshandbuch.

   - **Kennwort erforderlich:** Wählen Sie aus, ob die Kennwortauthentifizierung erzwungen werden soll. Der Standardwert variiert je nach gewähltem **Anmeldetyp**.
   - **Als Standard setzen:** Wählen Sie aus, ob die Citrix Gateway-Instanz als Standard verwendet werden soll. Die Standardeinstellung ist **Aus**.
   - **Konfigurationsskript exportieren:** Klicken Sie auf die Schaltfläche, um ein Konfigurationspaket zu exportieren, das Sie in Citrix Gateway hochladen und zur Konfiguration der XenMobile-Einstellungen verwenden. Weitere Informationen finden Sie im Anschluss

an diese Schritte unter “Konfigurieren eines On-Premises-Citrix Gateways für XenMobile Server”.

- **Rückruf-URL** und **Virtuelle IP-Adresse**: Speichern Sie die Einstellungen, bevor Sie diese Felder hinzufügen. Informationen finden Sie weiter unten unter Hinzufügen einer Rückruf-URL und einer virtuellen IP-Adresse für das Citrix Gateway-VPN.

5. Klicken Sie auf **Speichern**.

   Die neue Citrix Gateway-Instanz wird hinzugefügt und in der Tabelle angezeigt. Zum Bearbeiten oder Löschen einer Instanz klicken Sie auf deren Namen in der Liste.

Konfigurieren eines Citrix Gateway für XenMobile Server

Zum Konfigurieren eines On-Premises-Citrix Gateways für XenMobile führen Sie die folgenden, im vorliegenden Artikel erläuterten allgemeinen Schritte aus:

1. Laden Sie ein Skript und zugehörige Dateien von XenMobile Server herunter. Aktuelle und detaillierte Anweisungen finden Sie in der Readmedatei des Skripts.
2. Vergewissern Sie sich, dass Ihre Umgebung die Voraussetzungen erfüllt.
3. Aktualisieren Sie das Skript gemäß Ihrer Umgebung.
4. Führen Sie das Skript auf Citrix ADC aus.
5. Testen Sie die Konfiguration.

Mit dem Skript werden die folgenden, für XenMobile erforderlichen Citrix Gateway-Einstellungen konfiguriert:

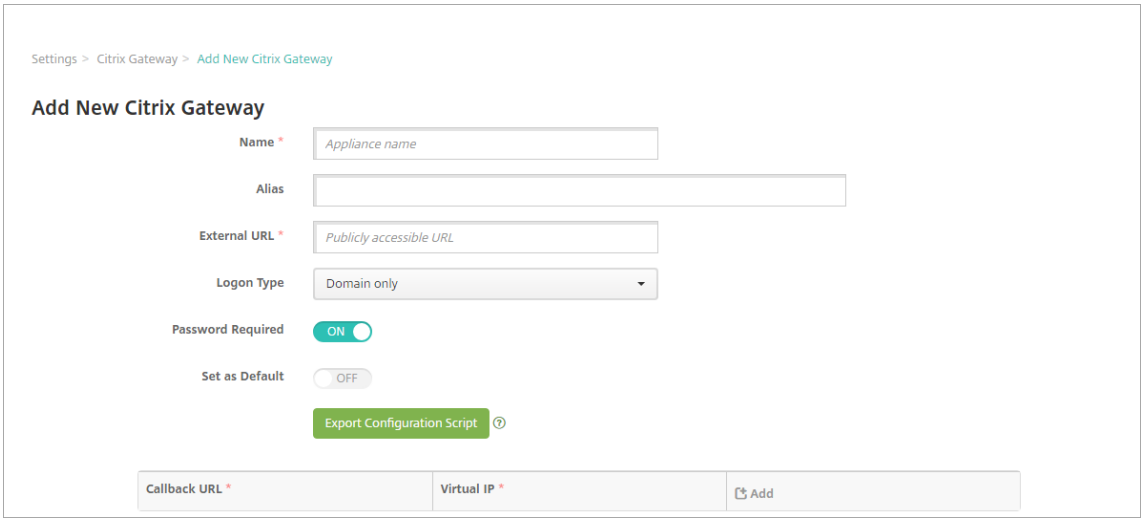
- Virtuelle Citrix Gateway-Server für MDM und MAM
- Sitzungsrichtlinien für virtuelle Citrix Gateway-Server
- XenMobile Server-Daten
- Authentifizierungsrichtlinien und Aktionen für den virtuellen Citrix Gateway-Server
  Das Skript beschreibt die Einstellungen der LDAP-Konfiguration.
- Datenverkehrsaktionen und Richtlinien für den Proxyserver
- Profil für den clientlosen Zugriff
- Statischer lokaler DNS-Eintrag auf Citrix ADC
- Andere Bindungen: Dienstrichtlinie, ZS-Zertifikat

Mit dem Skript wird folgende Konfiguration nicht erstellt:

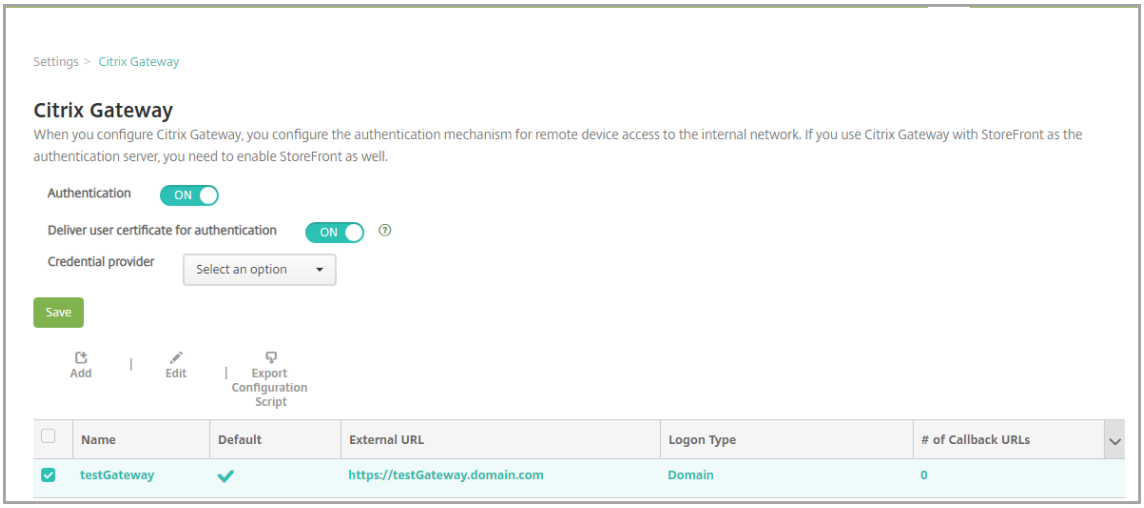
- Exchange-Lastausgleich
- Citrix Files-Lastausgleich
- ICA-Proxykonfiguration
- SSL-Offload

Herunterladen, Aktualisieren und Ausführen des Skripts

1. Wenn Sie ein Citrix Gateway hinzufügen, klicken Sie auf der Seite **Neues Citrix Gateway hinzufügen** auf **Konfigurationsskript exportieren**.



Wenn Sie eine Citrix Gateway-Instanz hinzufügen, klicken Sie auf **Speichern** bevor Sie das Skript exportieren: Kehren Sie zur Seite **Einstellungen > Citrix Gateway** zurück, wählen Sie das Citrix ADC, klicken Sie auf **Konfigurationsskript exportieren** und klicken Sie dann auf **Herunterladen**.

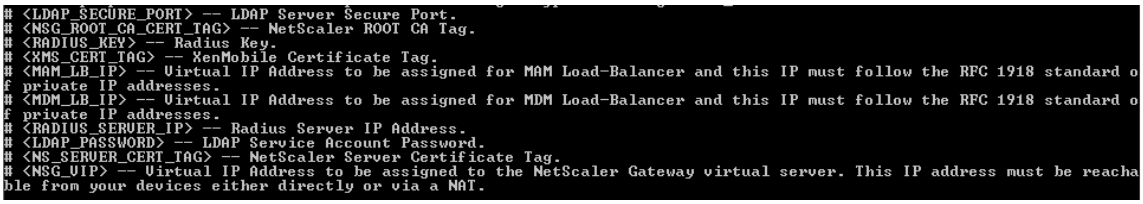


Nachdem Sie auf **Konfigurationsskript exportieren** geklickt haben, erstellt XenMobile ein TAR.GZ-Skriptpaket. Das Skriptpaket enthält Folgendes:

- Infodatei mit detaillierten Anweisungen
- Skript mit den Citrix ADC-CLI-Befehlen zum Konfigurieren der erforderlichen Komponenten in Citrix ADC
- Öffentliches Stamm-ZS-Zertifikat und Zwischenzertifikat von XenMobile Server (diese Zertifikate für SSL-Offload werden im aktuellen Release nicht benötigt)

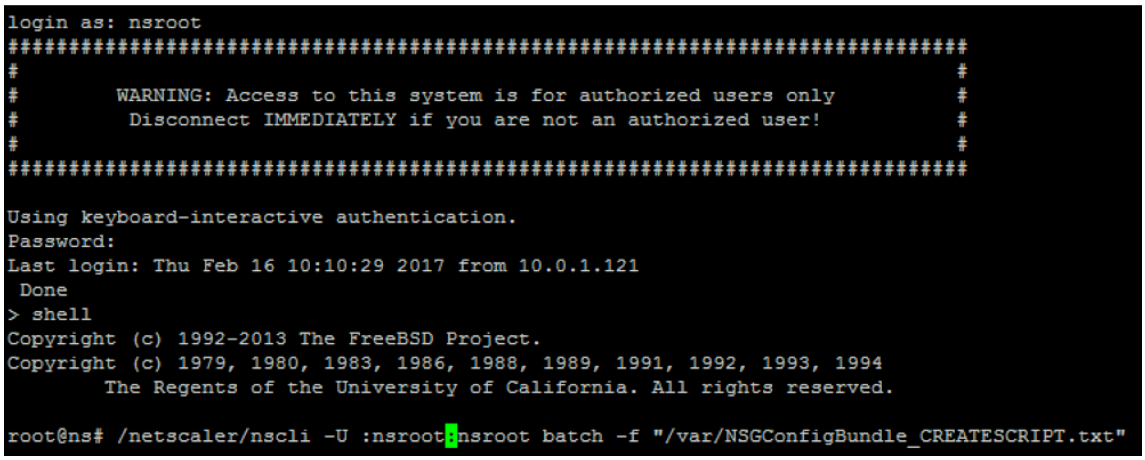
- Skript mit den Citrix ADC-CLI-Befehlen zum Entfernen der Citrix ADC-Konfiguration

2. Ersetzen Sie in dem Skript “NSGConfigBundle_CREATESCRIPT” alle Platzhalter durch die Daten Ihrer Umgebung.

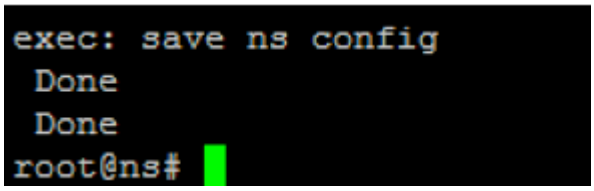


3. Führen Sie das bearbeitete Skript in der Citrix ADC-Bash-Shell gemäß den Anweisungen in der im Skriptpaket enthaltenen Readmedatei aus. Beispiel:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management
 Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

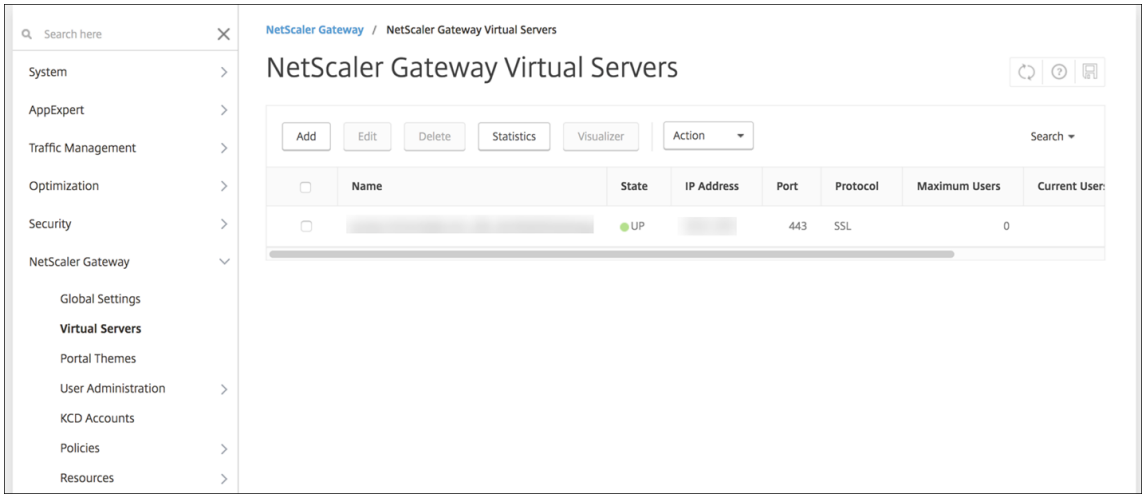


Nach Abschluss der Skriptausführung werden die folgenden Zeilen angezeigt:

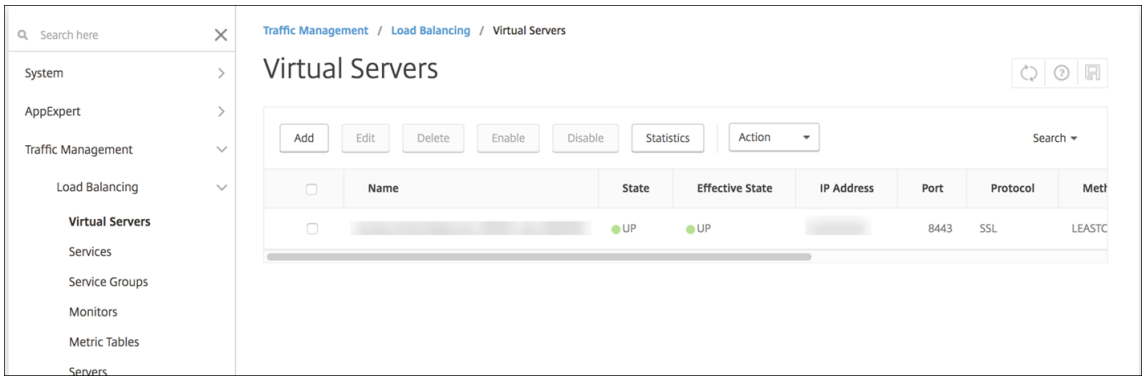


Testen der Konfiguration

1. Überprüfen Sie, ob für den virtuellen Citrix Gateway-Server der Zustand **UP** angezeigt wird.



2. Überprüfen Sie, ob für den virtuellen Lastausgleichsserver der Zustand **UP** angezeigt wird.



3. Öffnen Sie einen Webbrowser, stellen Sie eine Verbindung mit der Citrix Gateway-URL her und versuchen Sie, sich zu authentifizieren. Wenn die Authentifizierung fehlschlägt, wird folgende Meldung angezeigt: HTTP Status 404 - Not Found
4. Registrieren Sie ein Gerät für MDM und MAM.

Hinzufügen einer Rückruf-URL und einer virtuellen IP-Adresse für das Citrix Gateway-VPN

Nach dem Hinzufügen der Citrix Gateway-Instanz können Sie eine Callback-URL hinzufügen und eine virtuelle IP-Adresse für Citrix Gateway angeben. Diese Einstellungen sind optional, können aber für zusätzliche Sicherheit konfiguriert werden, insbesondere dann, wenn XenMobile Server in der DMZ ist.

1. Wählen Sie unter **Einstellungen > Citrix Gateway** die Citrix Gateway-Instanz und klicken Sie auf **Bearbeiten**.
2. Klicken Sie in der Tabelle auf **Hinzufügen**.

3. Geben Sie für **Rückruf-URL** den vollqualifizierten Domänennamen (FQDN) ein. Die Rückruf-URL dient zur Überprüfung, ob eine Anforderung von Citrix Gateway stammt.

   Die Rückruf-URL muss in eine IP-Adresse aufgelöst werden, die den XenMobile-Server erreichen kann. Die Rückruf-URL kann eine externe Citrix Gateway-URL oder eine andere URL sein.

4. Geben Sie die **Virtuelle IP** für Citrix Gateway ein und klicken Sie auf **Speichern**.

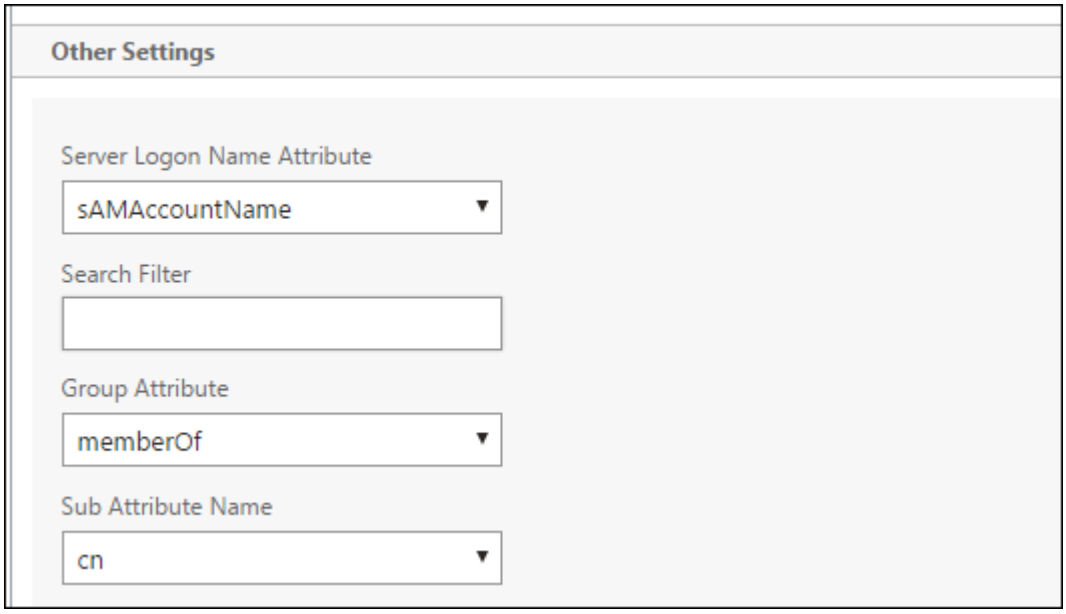
Konfigurieren der Authentifizierung für mehrere Domänen

Wenn Sie mehrere XenMobile Server-Instanzen haben (z. B. für die Test-, die Entwicklungs- und die Produktionsumgebung), konfigurieren Sie Citrix Gateway für die zusätzlichen Umgebungen manuell. (Sie können den Citrix ADC für XenMobile-Assistenten nur einmal verwenden.)

Konfigurieren von Citrix Gateway

Führen Sie zum Konfigurieren von Citrix Gateway-Authentifizierungsrichtlinien und einer Sitzungsrichtlinie für eine Umgebung mit mehreren Domänen folgende Schritte aus:

1. Erweitern Sie im Konfigurationsprogramm für Citrix Gateway auf der Registerkarte **Configuration** die Optionen **Citrix Gateway > Policies > Authentication**.
2. Klicken Sie im Navigationsbereich auf **LDAP**.
3. Klicken Sie zum Bearbeiten des LDAP-Profils. Ändern Sie **Server Logon Name Attribute** in **userPrincipalName** bzw. das Attribut, das Sie für Suchen verwenden möchten. Notieren Sie sich das von Ihnen angegebene Attribut, damit Sie es zur Hand haben, wenn Sie LDAP-Einstellungen in der XenMobile-Konsole konfigurieren.

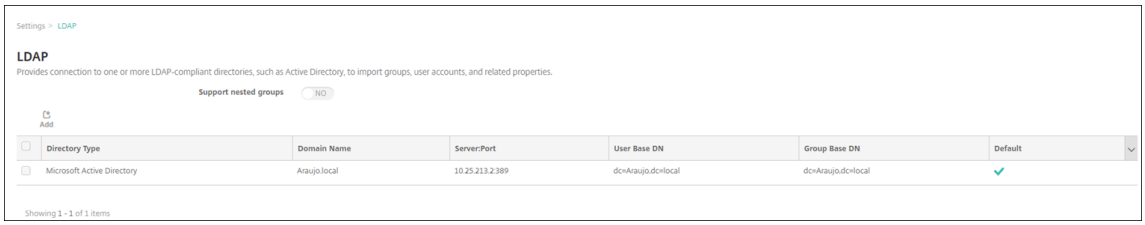


4. Wiederholen Sie diese Schritte für jede LDAP-Richtlinie. Für jede Domäne ist eine separate LDAP-Richtlinie erforderlich.
5. Geben Sie in der an den virtuellen Citrix Gateway-Server gebundenen Sitzungsrichtlinie zu **Edit session profile > Published Applications**. Stellen Sie sicher, dass **Single Sign-On Domain** leer ist.

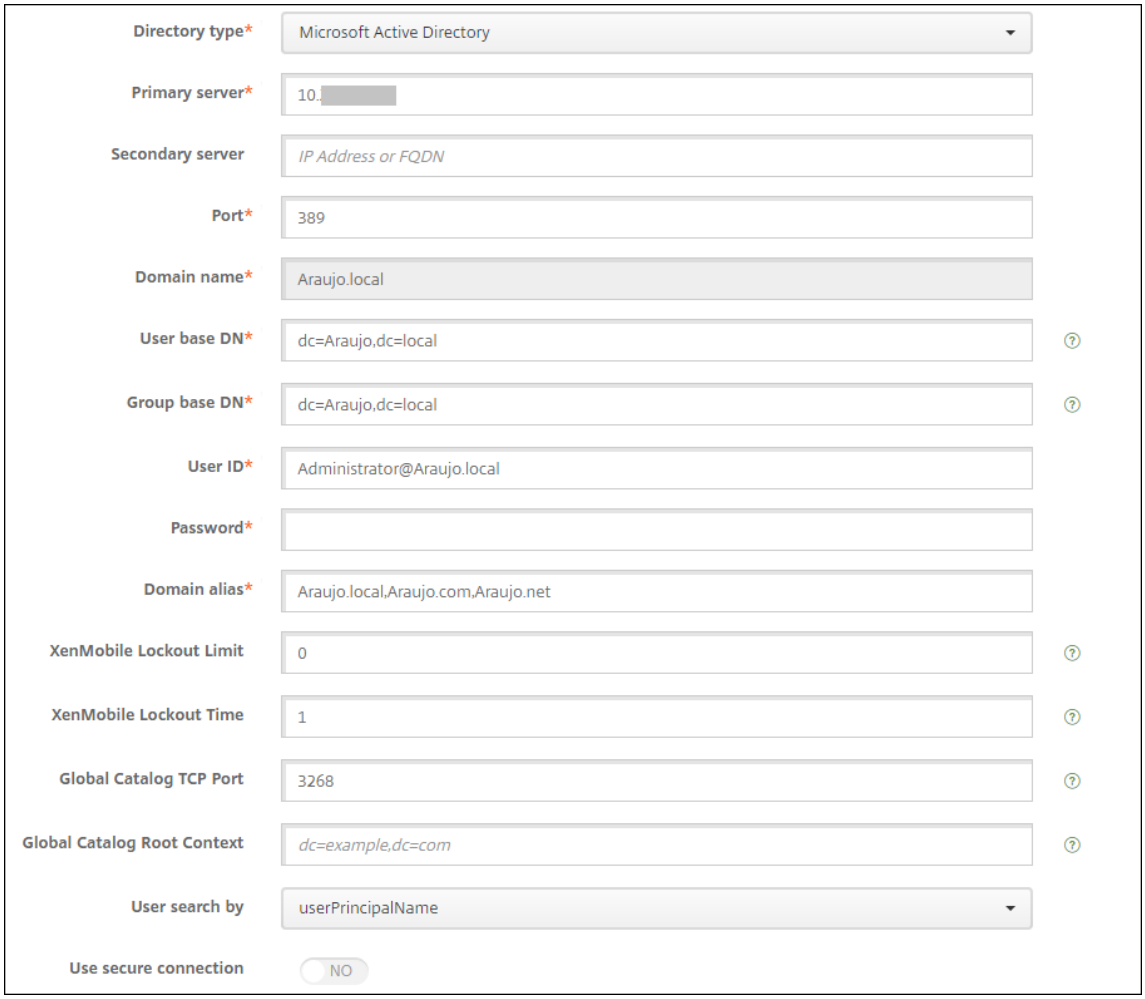
XenMobile Server-Konfiguration

Führen Sie zum Konfigurieren von LDAP für eine XenMobile-Umgebung mit mehreren Domänen die folgenden Schritte aus:

1. Gehen Sie in der XenMobile-Konsole zu **Einstellungen > LDAP** und fügen Sie ein Verzeichnis hinzu bzw. wählen Sie eines zum Bearbeiten aus.



2. Geben Sie die Informationen an.
   - Geben Sie unter **Domänenalias** jede Domäne an, die für die Benutzerauthentifizierung verwendet werden soll. Trennen Sie die Domänen durch Kommas ohne Leerzeichen ab. Beispiel: `domain1.com,domain2.com,domain3.com`
   - Stellen Sie sicher, dass die Angabe im Feld **Benutzersuche nach** mit der Angabe unter **Server Logon Name Attribute** in der LDAP-Richtlinie von Citrix Gateway übereinstimmt.



Verwerfen eingehender Verbindungsanforderungen an bestimmte URLs

Wenn Citrix Gateway in Ihrer Umgebung für SSL-Offload konfiguriert ist, soll das Gateway möglicherweise eingehende Verbindungsanforderungen für bestimmte URLs verwerfen.

Wenn Sie diese zusätzliche Sicherheit brauchen, konfigurieren Sie die beiden virtuellen MDM Load Balancer-Server (einer für Port 443 und einer für Port 8443) in Citrix Gateway. Verwenden Sie die folgenden Informationen als Vorlage für Ihre Einstellungen.

> **Wichtig:**
>
> Die folgenden Updates gelten nur für ein Citrix Gateway, das für SSL-Offload konfiguriert ist.

1. Erstellen Sie einen Mustersatz mit dem Namen `XMS_DropURLs`.

```
1 add policy patset XMS_DropURLs
2 <!--NeedCopy-->
```


2. Fügen Sie dem neuen Mustersatz die folgenden URLs hinzu. Passen Sie diese Liste nach Bedarf an.

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6

bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5

bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4

bind policy patset XMS_DropURLs /zdm/log.jsp -index 3

bind policy patset XMS_DropURLs /zdm/login.jsp -index 2

bind policy patset XMS_DropURLs /zdm/console -index 1
<!--NeedCopy-->
```

3. Erstellen Sie eine Richtlinie, um den gesamten Datenverkehr an diese URLs zu löschen, es sei denn, die Verbindungsanforderung stammt aus dem angegebenen Subnetz.

```
add responder policy XMS_DROP_pol  “CLIENT.IP.SRC.IN_SUBNET
    (192.168.0.0/24).NOT &&
HTTP.REQ.URL.CONTAINS_ANY(” XMS_DropURLs” )”  DROP -comment "Allow
     only subnet 192.168.0.0/24 to access these URLs. All other
    connections are DROPed"
<!--NeedCopy-->
```

4. Binden Sie die neue Richtlinie an beide virtuellen MDM Load Balancer-Server (Port 443 und 8443).

```
bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST

bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST
<!--NeedCopy-->
```

Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken

January 5, 2022

XenMobile unterstützt die domänenbasierte Authentifizierung unter Verwendung eines oder mehrerer Lightweight Directory Access Protocol-konformer Verzeichnisse. Sie können in XenMobile eine Verbindung mit einem oder mehreren Verzeichnissen konfigurieren und mit 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.

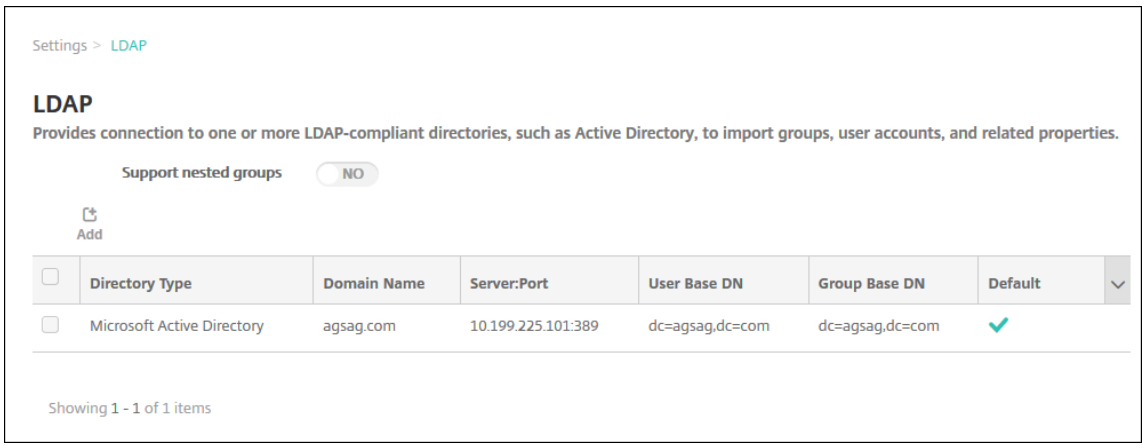
LDAP wird häufig zur Bereitstellung von Single Sign-On (SSO) für Benutzer eingesetzt, bei dem ein Kennwort (pro Benutzer) für mehrere Dienste verwendet wird. Mit Single Sign-On melden sich die Benutzer einmal bei der Unternehmenswebsite an und erhalten so authentifizierten Zugriff auf das Unternehmensintranet.

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.

> **Wichtig:**
>
> Der Authentifizierungsmodus kann nicht von Domänenauthentifizierung in einen anderen Authentifizierungsmodus geändert werden, nachdem Benutzer die Geräte bei XenMobile registriert haben.

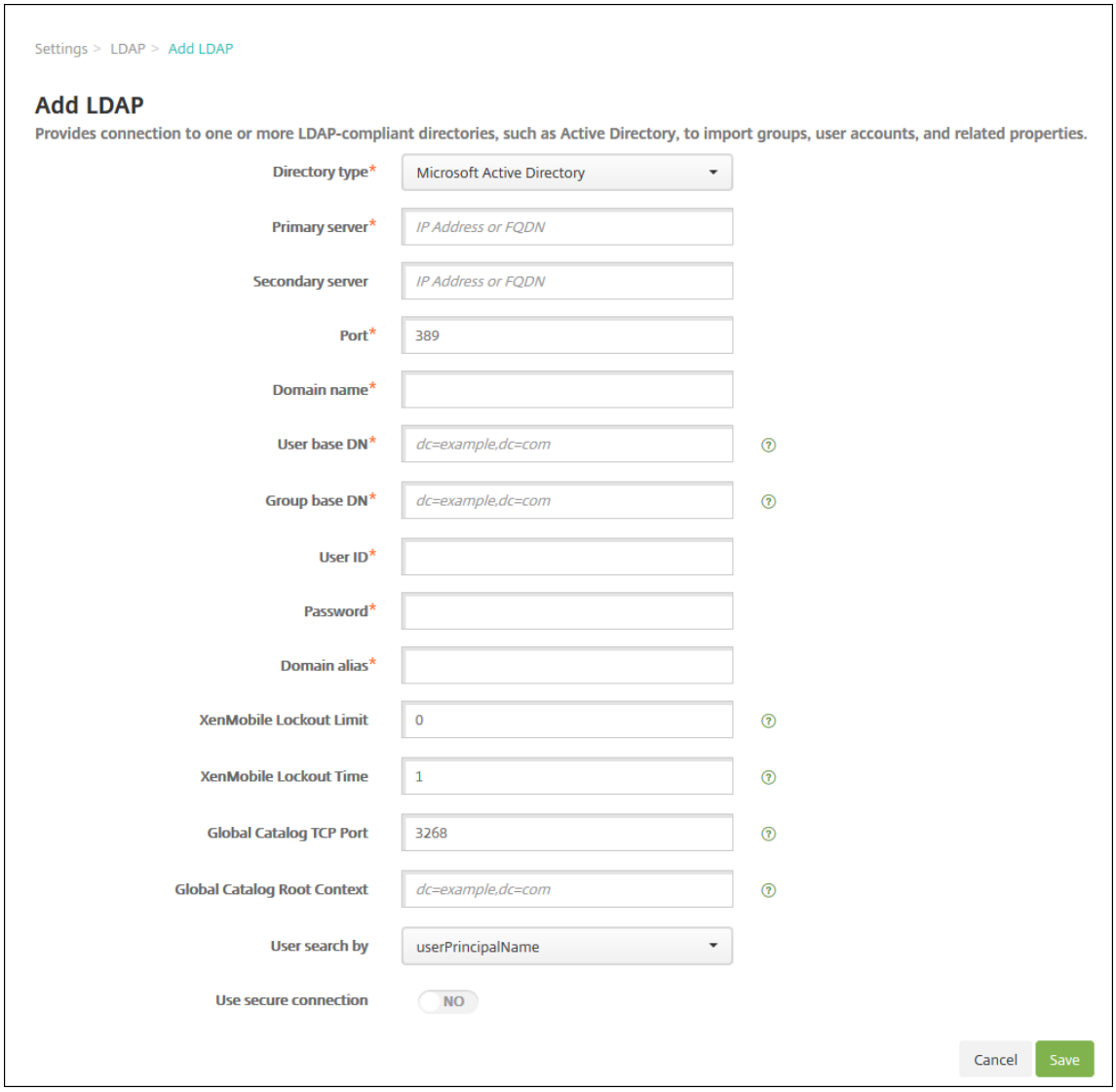
Konfigurieren von LDAP-Verbindungen in XenMobile

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Server** auf **LDAP**. Die Seite **LDAP** wird angezeigt. Auf dieser Seite können Sie LDAP-konforme Verzeichnisse hinzufügen, bearbeiten und löschen (siehe Anweisungen im vorliegenden Artikel).



Hinzufügen von LDAP-kompatiblen Verzeichnissen

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



2. Konfigurieren Sie folgende Einstellungen:

   - **Verzeichnistyp:** Klicken Sie in der Liste auf den Verzeichnistyp. Die Standardeinstellung ist **Microsoft Active Directory**.
   - **Primärer Server:** Geben Sie den für LDAP verwendeten primären Server an. Sie können die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) eingeben.
   - **Sekundärer Server:** Geben Sie optional die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) für den sekundären Server (sofern konfiguriert) ein. 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.

- **Domänenname:** Geben Sie den Domänennamen ein.
- **Basis-DN für Benutzer:** Geben Sie den Speicherort von Benutzern in Active Directory über einen eindeutigen Bezeichner ein. Syntaxbeispiele: `ou=users`, `dc=example` oder `dc=com`.
- **Basis-DN für Gruppen:** Geben Sie den 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.
- **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. Wenn Sie die Einstellung für den **Domänenalias** nach der Registrierung ändern, müssen sich Benutzer neu registrieren.
- **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. Der Wert **0** bedeutet, dass Benutzer nicht gezwungen sind, nach einer Sperrung zu warten.
- **TCP-Port für globalen Katalog:** Geben Sie die TCP-Portnummer des Servers für den globalen Katalog ein. Die Standard-TCP-Portnummer ist **3268**. Verwenden Sie für SSL-Verbindungen die Portnummer **3269**.
- **Stammkontext für globalen Katalog:** Geben Sie optional den Stammkontext für den globalen Katalog ein, der eine Suche im globalen Katalog von Active Directory ermöglicht. Diese Suchfunktion existiert zusätzlich zu der Standard-LDAP-Suche und ermöglicht die Suche in jeder Domäne ohne Angabe des Domänennamens.
- **Benutzersuche nach:** Klicken Sie in der Liste auf **userPrincipalName** oder **sAMAccountName**. Der Standardwert ist **userPrincipalName**. Wenn Sie die Einstellung **Benutzersuche nach** nach der Registrierung ändern, müssen sich Benutzer neu registrieren.
- **Sichere Verbindung verwenden:** Wählen Sie aus, ob sichere Verbindungen verwendet werden sollen. Die Standardeinstellung ist **NEIN**.

3. Klicken Sie auf **Speichern**.

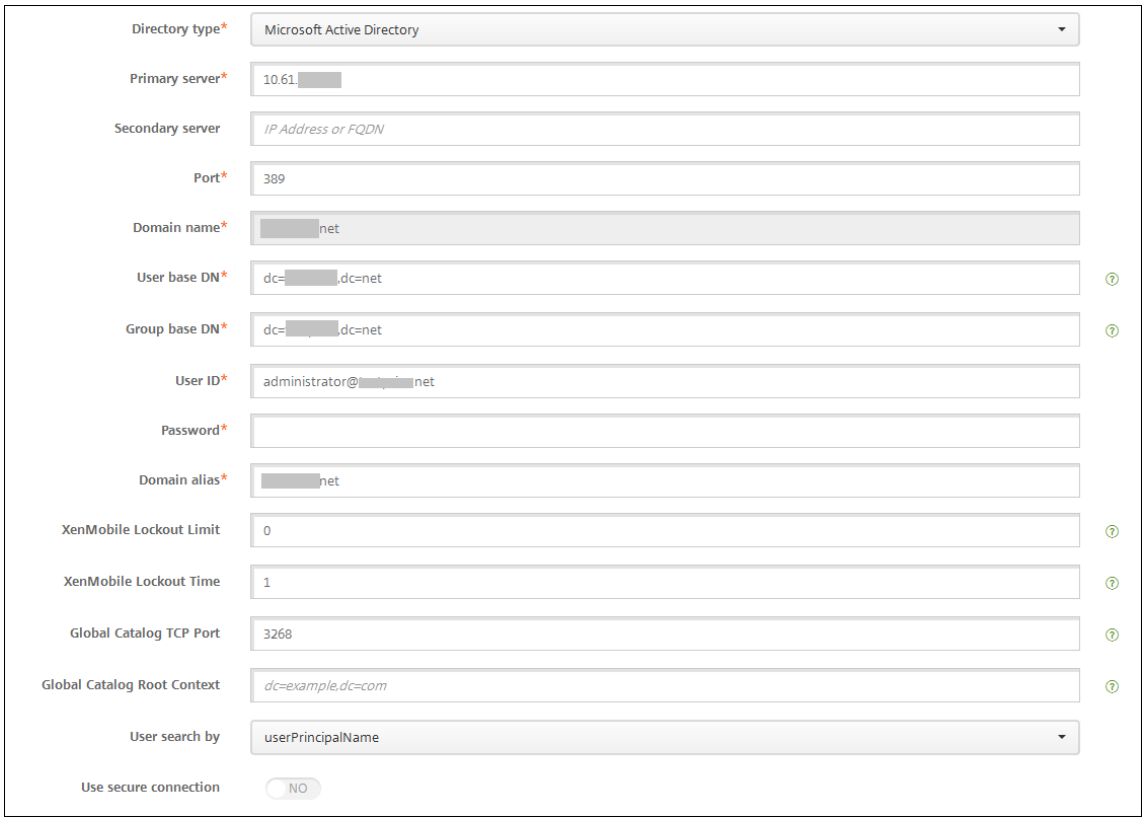
Bearbeiten LDAP-kompatibler Verzeichnisse

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

   Wenn Sie das Kontrollkästchen neben einem Verzeichnis aktivieren, wird das Menü mit den Op-

tionen oberhalb der LDAP-Liste angezeigt. Wenn Sie an eine andere Stelle in der Liste klicken, wird das Menü mit den Optionen rechts daneben angezeigt.

2. Klicken Sie auf **Edit**. Die Seite **LDAP bearbeiten** wird angezeigt.



3. Ändern Sie nach Bedarf die folgenden Informationen:

   - **Verzeichnistyp:** Klicken Sie in der Liste auf den Verzeichnistyp.
   - **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=groupname` ein. Beispielsweise `cn=users`, `dc=servername`, `dc=net`, wobei

`cn=users` der Gruppenname ist. `DN` und `servername` sind der Name des Servers, auf dem Active Directory ausgeführt wird.

- **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. Wenn Sie die Einstellung für den **Domänenalias** nach der Registrierung ändern, müssen sich Benutzer neu registrieren.
- **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. Der Wert **0** bedeutet, dass Benutzer nicht gezwungen sind, nach einer Sperrung zu 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**. Wenn Sie die Einstellung **Benutzersuche nach** nach der Registrierung ändern, müssen sich Benutzer neu registrieren.
- **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 beizubehalten.

Löschen LDAP-kompatibler Verzeichnisse

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

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

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

Konfigurieren der Authentifizierung für mehrere Domänen

Informationen zum Konfigurieren von XenMobile Server zur Verwendung mehrerer Domänensuffixe in einer LDAP-Konfiguration finden Sie in der Dokumentation zur Citrix Endpoint Management unter Konfigurieren der Authentifizierung für mehrere Domänen. Das Verfahren ist bei der On-Premises-Version von XenMobile Server und der Endpoint Management-Cloudversion identisch.

Konfigurieren der Authentifizierung mit Domäne und Sicherheitstoken

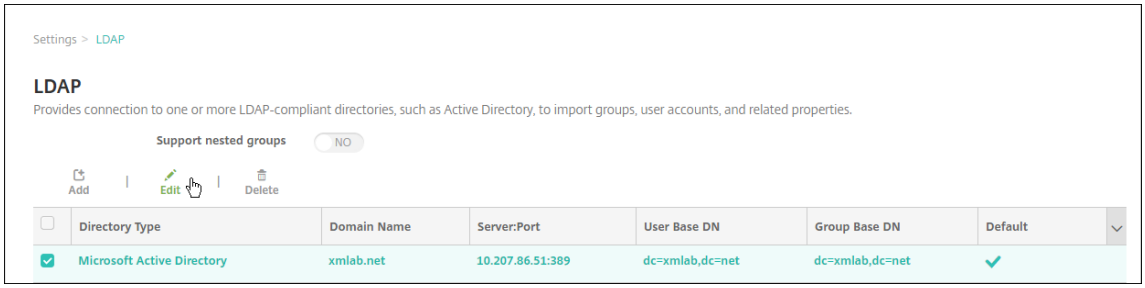
Sie können XenMobile konfigurieren, sodass Benutzer sich mit ihren LDAP-Anmeldeinformationen und einem Einmalkennwort authentifizieren müssen. Dabei wird das RADIUS-Protokoll verwendet.

Die optimale Benutzerfreundlichkeit erreichen Sie, wenn Sie diese Konfiguration mit der Citrix-PIN und der Active Directory-Kennwortzwischenspeicherung kombinieren. Die Benutzer müssen dann ihre LDAP-Benutzernamen und -Kennwörter nicht wiederholt eingeben. Die Benutzer geben Benutzernamen und Kennwörter für die Registrierung sowie bei Kennwortablauf und Kontosperrung ein.

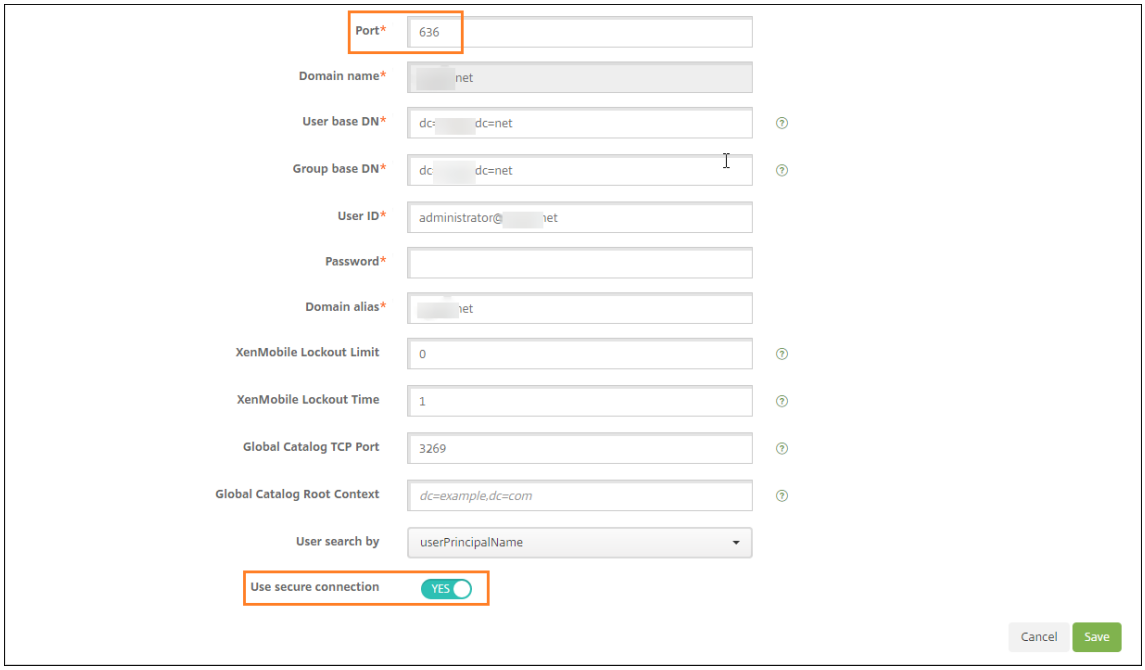
Konfigurieren von LDAP-Einstellungen

Wenn Sie LDAP für die Authentifizierung verwenden möchten, müssen Sie ein SSL-Zertifikat von einer Zertifizierungsstelle in XenMobile installieren. Weitere Informationen finden Sie unter Hochladen von Zertifikaten in XenMobile.

1. Klicken Sie in **Einstellungen** auf **LDAP**.
2. Wählen Sie **Microsoft Active Directory** und klicken Sie auf **Bearbeiten**.



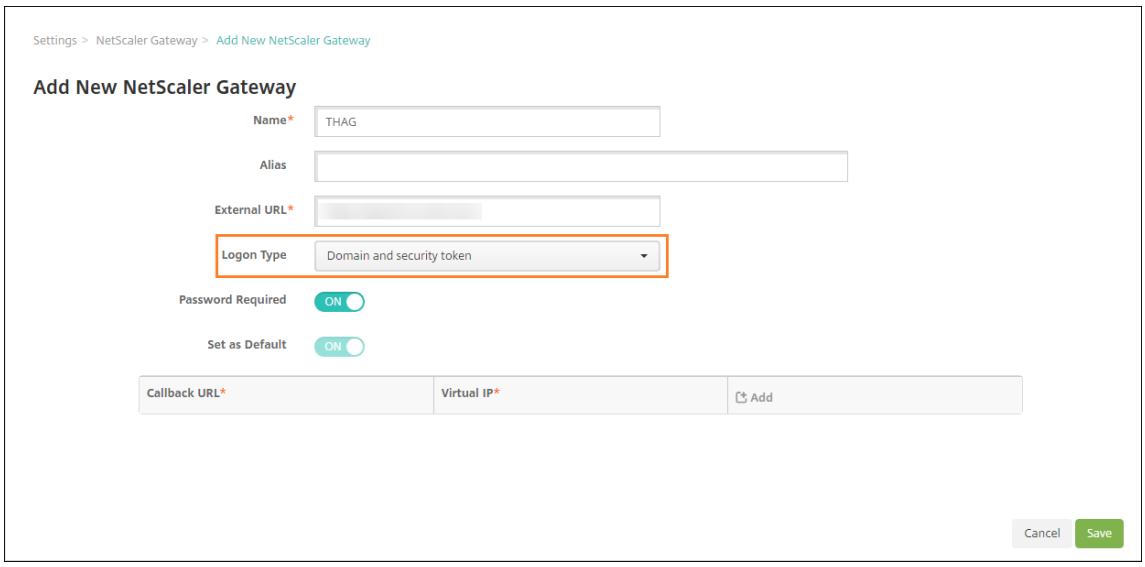
3. Überprüfen Sie, ob der Port auf **636** für sichere LDAP-Verbindungen oder auf **3269** für sichere Microsoft LDAP-Verbindungen festgelegt ist.
4. Legen Sie **Sichere Verbindung verwenden** auf **Ja** fest.



Konfigurieren von Citrix Gateway-Einstellungen

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

1. Klicken unter **Einstellungen** auf **Citrix Gateway**.
2. Wählen Sie das **Citrix Gateway** und klicken Sie auf **Bearbeiten**.
3. Wählen Sie unter **Anmeldetyp** die Option **Domäne und Sicherheitstoken**.



Aktivieren der Citrix-PIN und der Zwischenspeicherung von Benutzerkennwörtern

Um die Citrix-PIN und die Zwischenspeicherung von Benutzerkennwörtern zu aktivieren, gehen Sie zu **Einstellungen > Clienteigenschaften** und aktivieren Sie die Kontrollkästchen **Enable Citrix-PIN Authentication** und **Enable User Password Caching**. Weitere Informationen finden Sie unter Clienteigenschaften.

Konfigurieren von Citrix Gateway für die Authentifizierung mit Domäne und Sicherheitstoken

Konfigurieren Sie Citrix Gateway-Sitzungsprofile und Richtlinien für die virtuellen Server, die mit XenMobile verwendet werden. Weitere Informationen finden Sie in der Dokumentation zu Citrix Gateway.

Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne

January 5, 2022

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 das beste Gleichgewicht zwischen Sicherheit und Benutzererfahrung. Die Authentifizierung per Zertifikat und Domäne bietet die besten SSO-Möglichkeiten in Kombination mit der von der zweistufigen Authentifizierung unter Citrix ADC gebotenen Sicherheit.

Die optimale Benutzerfreundlichkeit erreichen Sie, wenn Sie die Authentifizierung per Zertifikat und Domäne mit der Citrix-PIN und Active Directory-Kennwortcaching kombinieren. Die Benutzer müssen dann ihre LDAP-Benutzernamen und -Kennwörter nicht wiederholt eingeben. Die Benutzer geben Benutzernamen und Kennwörter für die Registrierung sowie bei Kennwortablauf und Kontosperrung ein.

> **Wichtig:**
>
> Der Authentifizierungsmodus kann nicht von Domänenauthentifizierung in einen anderen Authentifizierungsmodus geändert werden, nachdem Benutzer die Geräte bei XenMobile registriert haben.

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 für die Authentifizierung bei der XenMobile-Umgebung verwendet wird, und stellt dieses bereit.

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

In Hochsicherheitsumgebungen stellt die Verwendung von LDAP-Anmeldeinformationen außerhalb der Organisation in öffentlichen oder unsicheren Netzwerken eine große Sicherheitsbedrohung dar. In solchen Umgebungen 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, XenMobile Server und dann Citrix 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 Citrix Gateway, um ein Benutzerzertifikat für die Authentifizierung bereitzustellen.

Informationen über die Citrix Gateway-Konfiguration finden Sie in folgenden Artikeln der Citrix ADC-Dokumentation:

- Clientauthentifizierung
- SSL-Profilinfrastruktur
- Konfigurieren und Binden einer Richtlinie für die Clientzertifikatauthentifizierung

Voraussetzungen

- Vermeiden Sie beim Erstellen einer Microsoft-Zertifikatdiensteentitätsvorlage die Verwendung von Sonderzeichen. Verwenden in Vorlagennamen beispielsweise nicht folgende Zeichen: `: ! $ ()## % + * ~ ? | { } []`
- Deaktivieren Sie für Windows Phone 8.1-Geräte mit Zertifikatauthentifizierung und SSL-Offload die Wiederverwendung von SSL-Sitzungen für Port 443 auf beiden virtuellen Lastausgle-

ichsservern in Citrix ADC. Führen Sie hierfür auf diesen virtuellen Servern den folgenden Befehl für Port 443 aus:

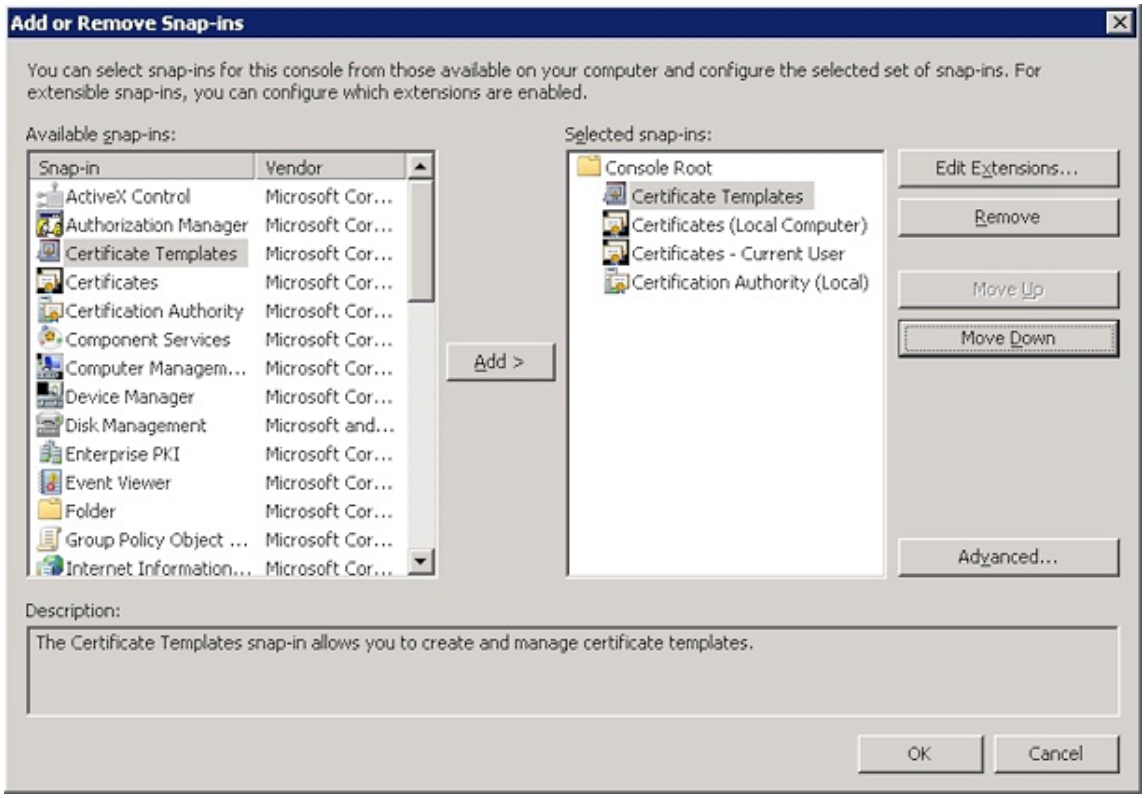
```
set ssl vserver <ssl lb vserver> sessReuse DISABLE
```

Mit der SSL-Sitzungswiederverwendung werden einige Optimierungen von Citrix ADC deaktiviert, was zu einer Leistungsminderung bei Citrix ADC führen kann.

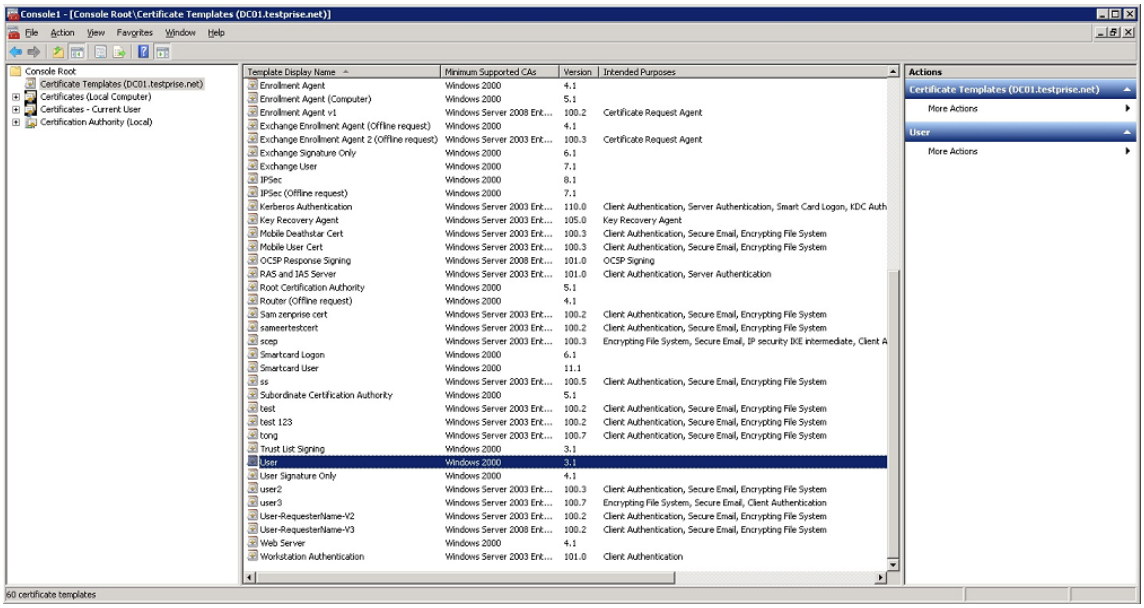
- Informationen zum Konfigurieren der zertifikatbasierten Authentifizierung für Exchange ActiveSync finden Sie in diesem Microsoft-Blog. Konfigurieren Sie die Serversite für die Zertifizierungsstelle, so dass Exchange ActiceSync Clientzertifikate anfordert.
- Wenn Sie private Serverzertifikate zum Schützen des ActiveSync-Datenverkehrs an Exchange Server verwenden, müssen die mobilen Geräte alle erforderlichen 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”. Wählen Sie für beide Anwendungen unter **SSL-Einstellungen** die Option **SSL erforderlich** aus.

Fügen Sie der Microsoft Management Console ein Zertifikat-Snap-In hinzu

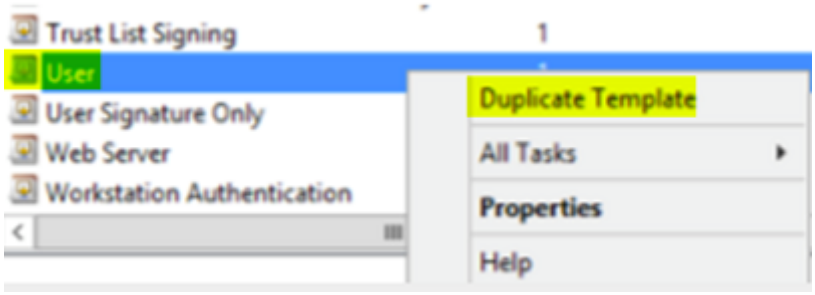
1. Öffnen Sie die Konsole und klicken Sie auf **Snap-In hinzufügen/entfernen**.
2. Fügen Sie die folgenden Snap-Ins hinzu:
   - Zertifikatvorlagen
   - Zertifikate (lokaler Computer)
   - Zertifikate – aktueller Benutzer
   - Zertifizierungsstelle (lokal)



3. Erweitern Sie **Zertifikatvorlagen**.



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

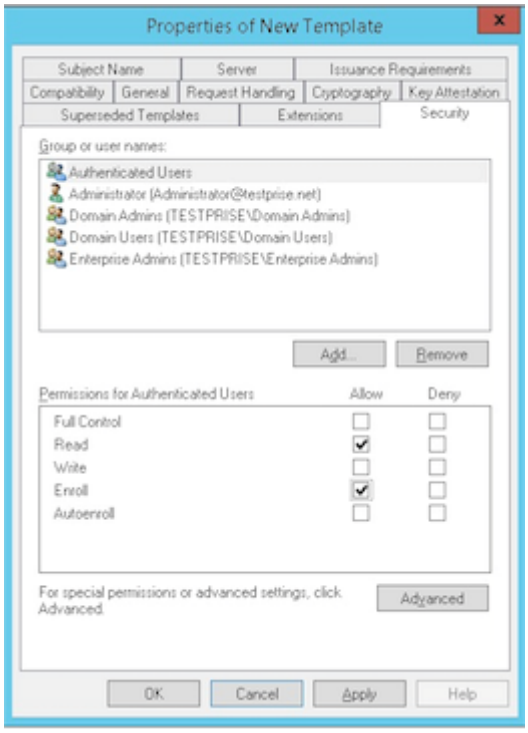


5. Geben Sie den Anzeigenamen der Vorlage an.

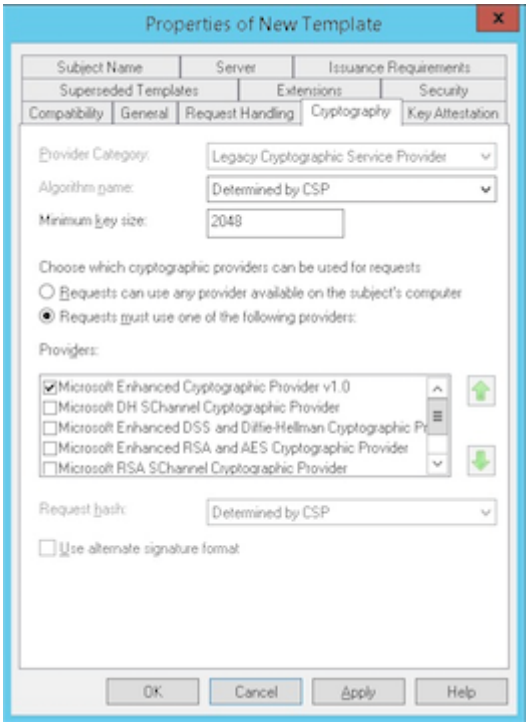
> **Wichtig:**
>
> Aktivieren Sie das Kontrollkästchen für **Zertifikat in Active Directory veröffentlichen** nur bei Bedarf. Wenn diese Option aktiviert ist, werden alle Benutzerclientzertifikate in Active Directory erstellt, wodurch die Active Directory-Datenbank überladen werden kann.

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.

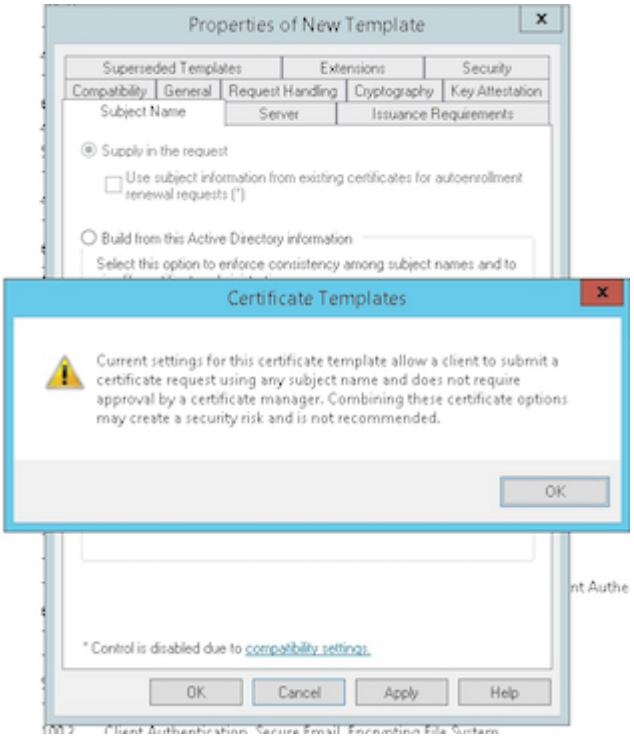
7. Wählen Sie unter **Sicherheit** in der Spalte **Zulassen** die Option **Registrieren** für die authentifizierten Benutzer aus.



8. Geben Sie unter **Kryptografie** die Schlüsselgröße an. Sie geben die Schlüsselgröße später bei der XenMobile-Konfiguration ein.

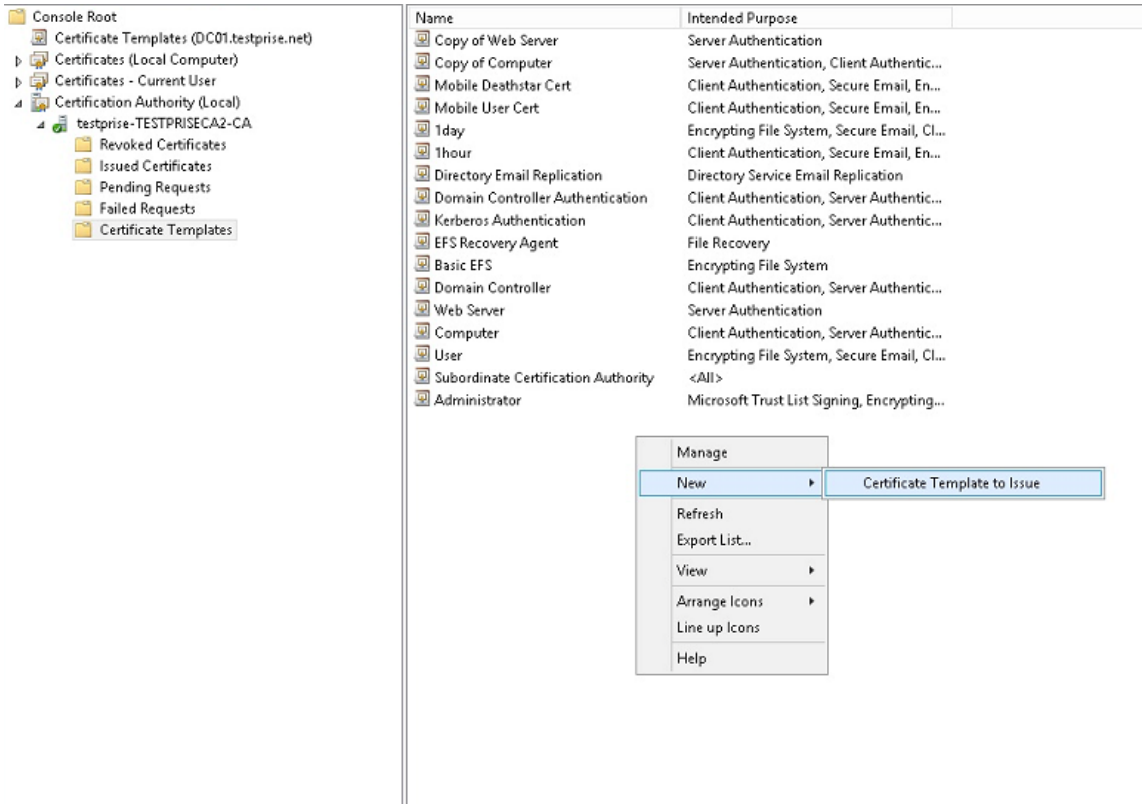


9. Wählen Sie unter **Antragstellername** die Option **Informationen werden in der Anforderung angegeben** aus. Wenden Sie die Änderungen an und speichern Sie.

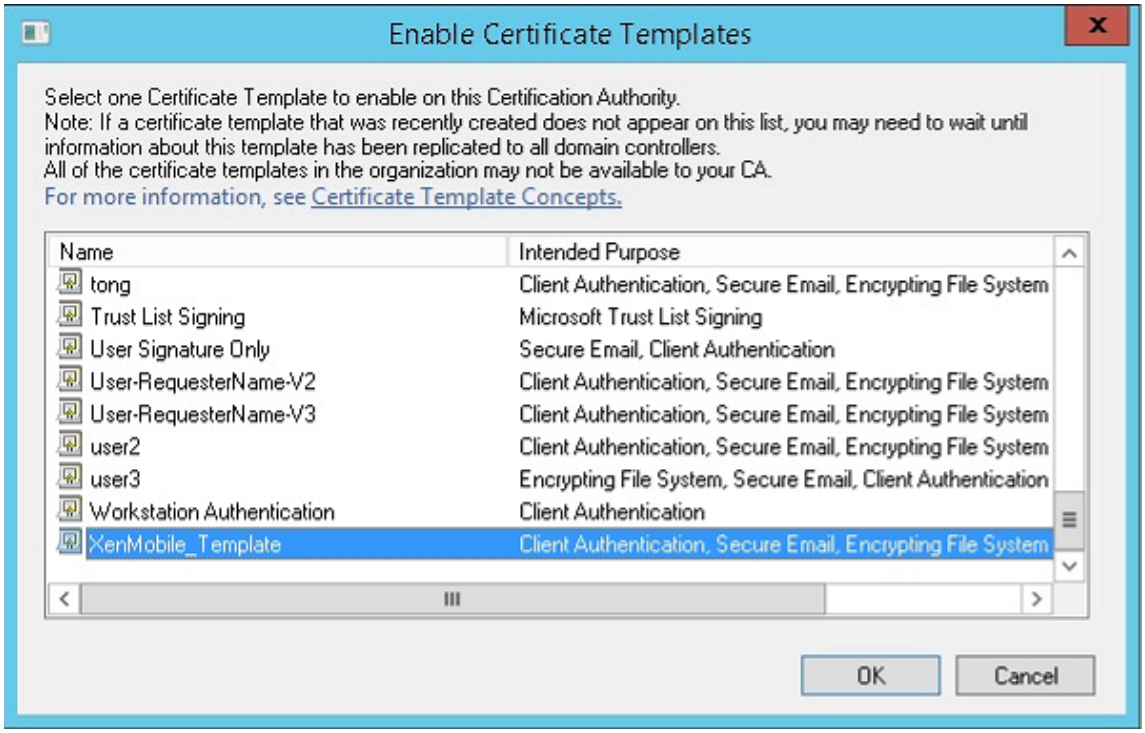


Hinzufügen der Vorlage zur Zertifizierungsstelle

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**.

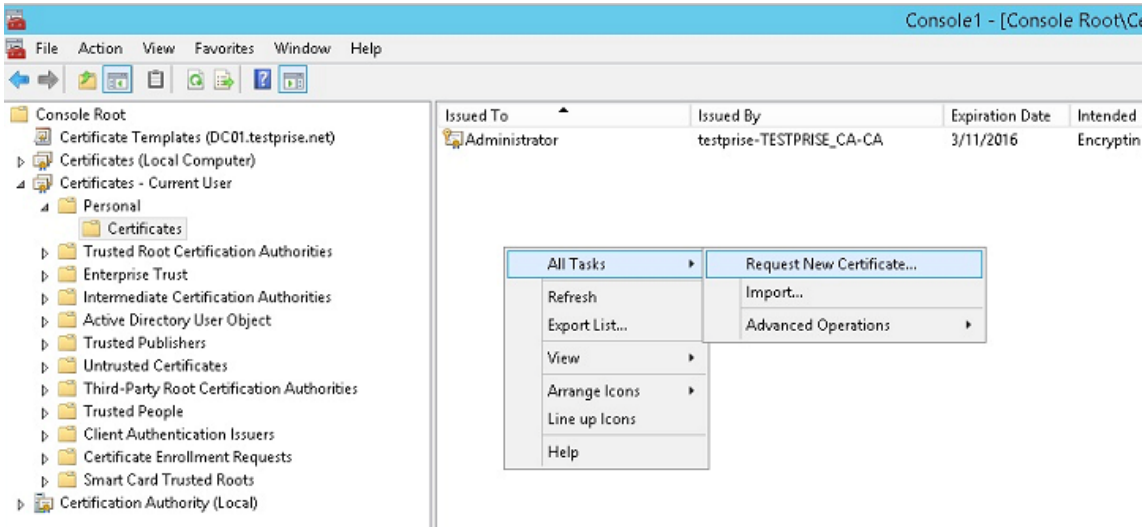


3. Wählen Sie die im vorherigen Schritt erstellte Vorlage und klicken Sie auf **OK**, um sie der **Zertifizierungsstelle** hinzuzufügen.

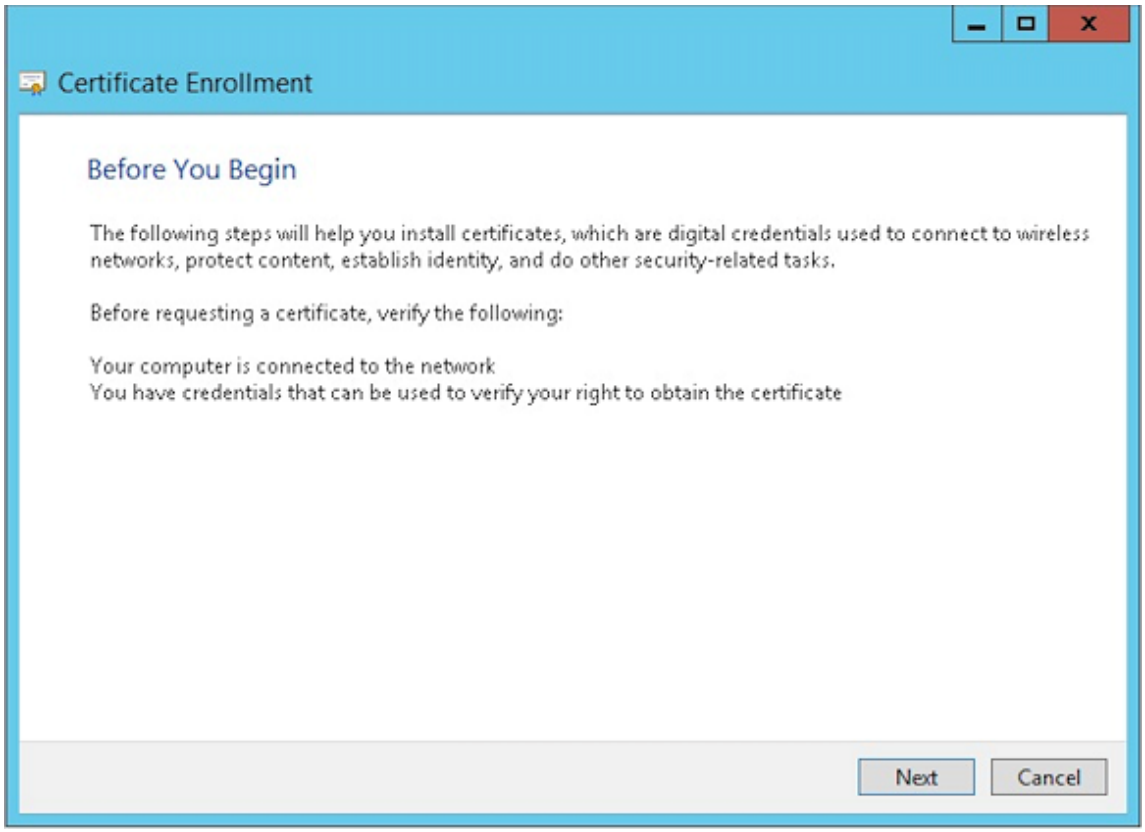


Erstellen eines PFX-Zertifikats vom ZS-Server

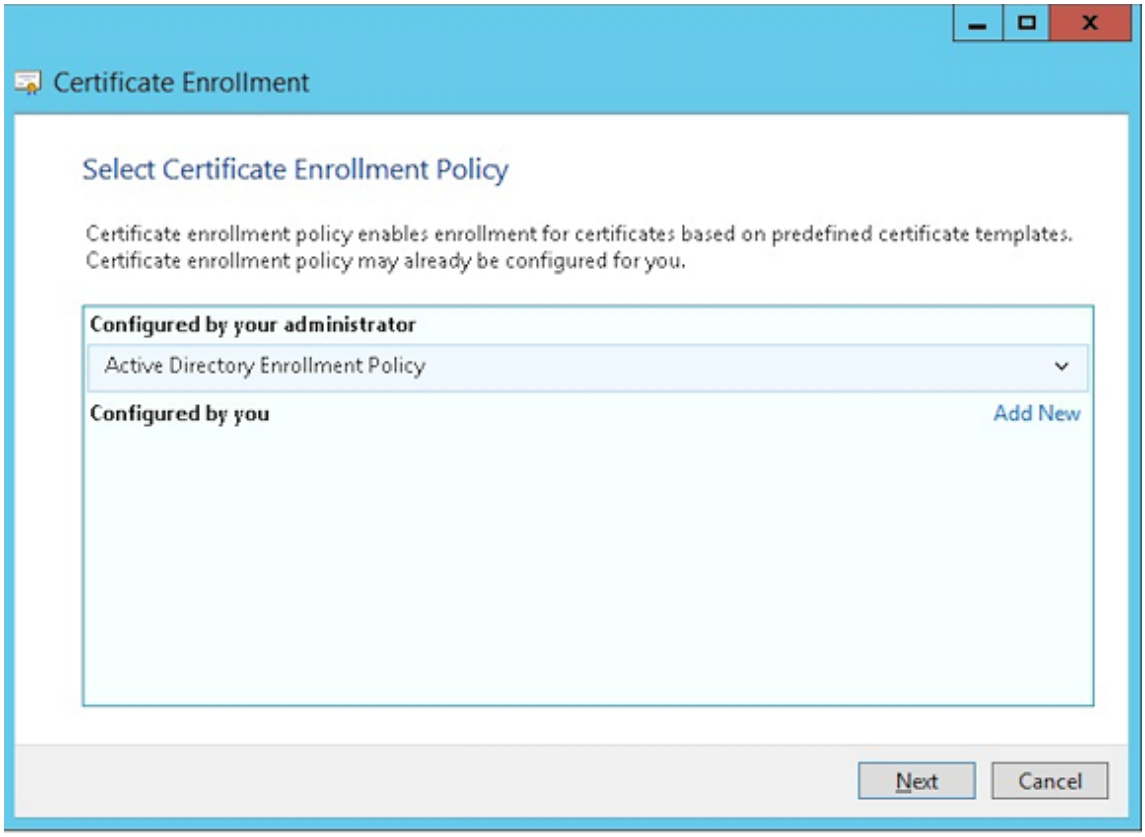
1. Erstellen Sie mit dem Dienstkonto, mit dem Sie sich angemeldet haben, ein PFX-Benutzerzertifikat. Diese PFX-Datei wird in XenMobile hochgeladen, um ein Benutzerzertifikat im Namen der Benutzer anzufordern, die ihre Geräte registrieren.
2. Erweitern Sie **Zertifikate** unter **Aktueller Benutzer**.
3. Klicken Sie mit der rechten Maustaste in den rechten Bereich und klicken Sie auf **Neues Zertifikat anfordern**.



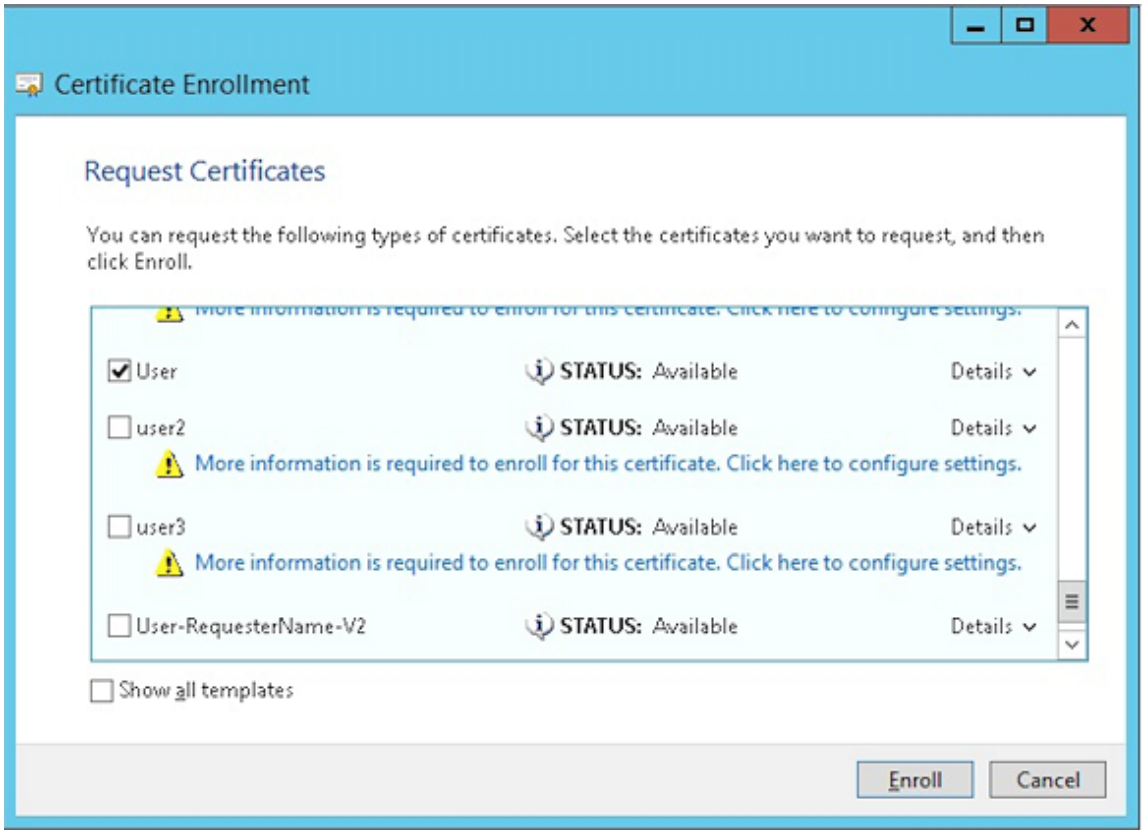
4. Der Bildschirm **Zertifikatregistrierung** wird angezeigt. Klicken Sie auf **Weiter**.



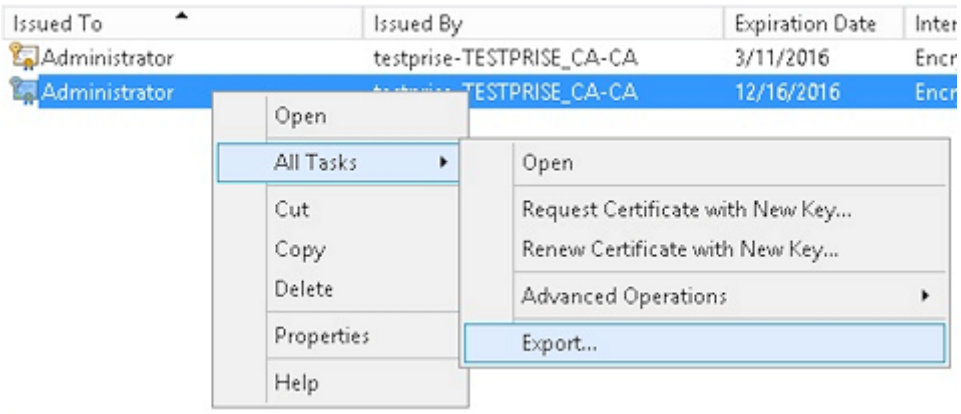
5. Wählen Sie **Active Directory-Registrierungsrichtlinie** und klicken Sie auf **Weiter**.



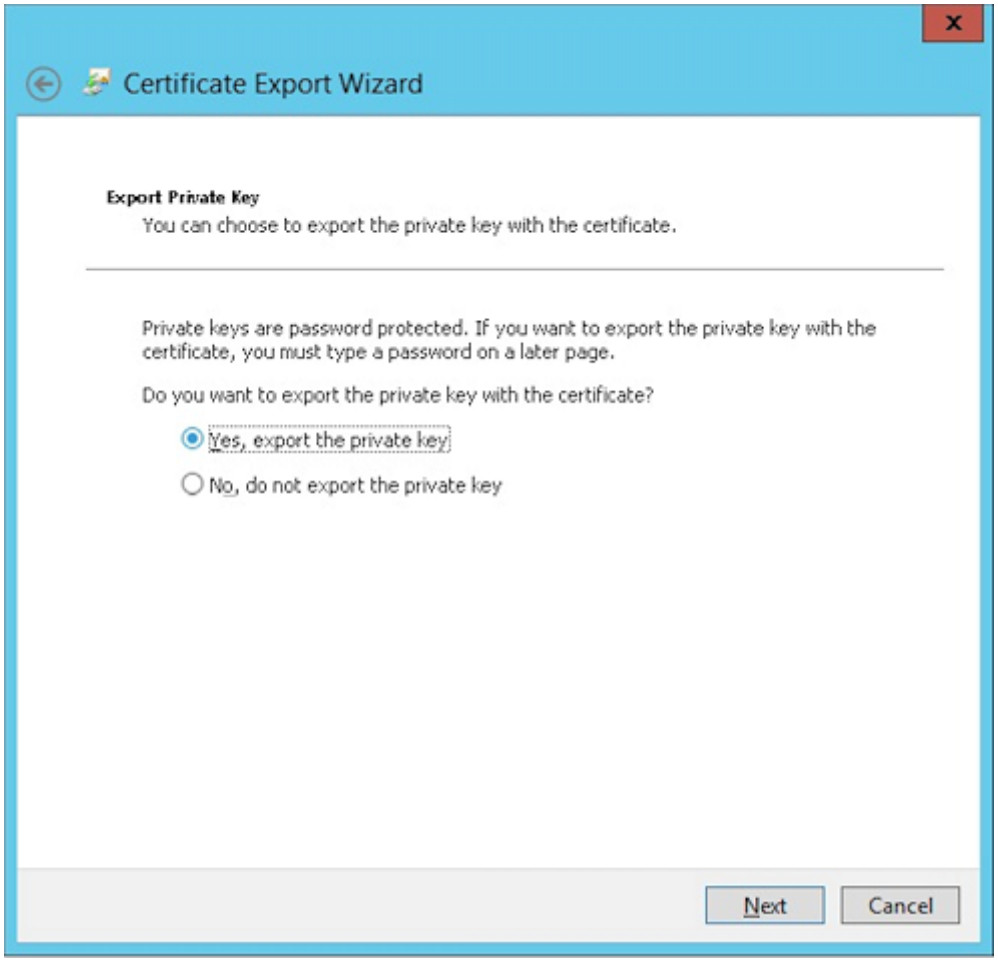
6. Wählen Sie die Vorlage **Benutzer** und klicken Sie auf **Registrieren**.



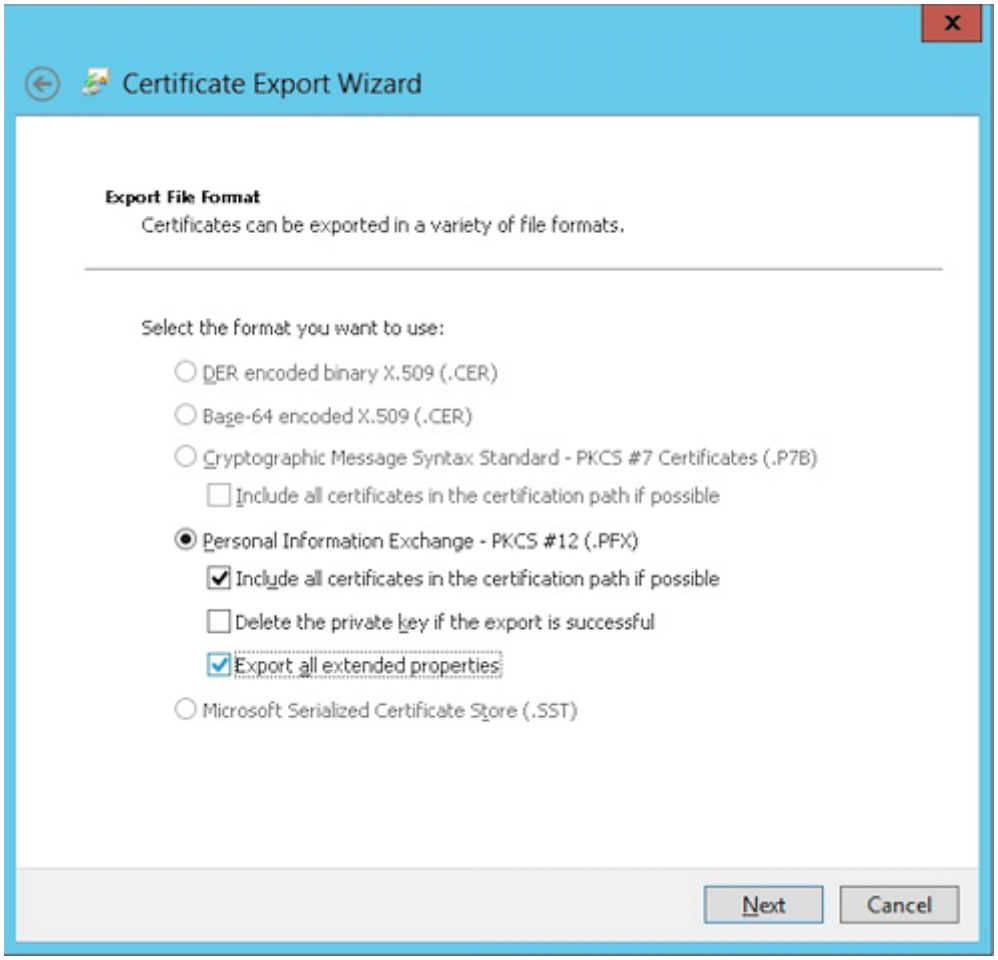
7. Exportieren Sie die PFX-Datei, die Sie im vorherigen Schritt erstellt haben.



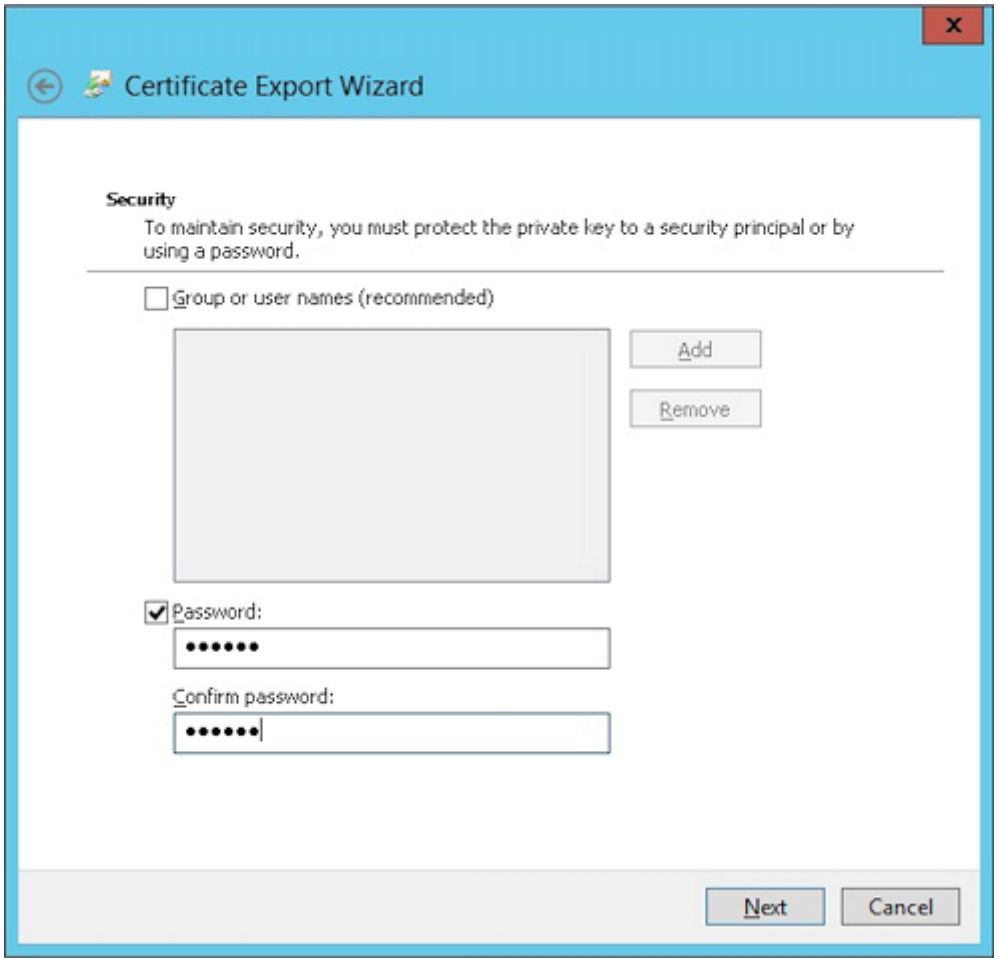
8. Klicken Sie auf **Ja, privaten Schlüssel exportieren**.



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



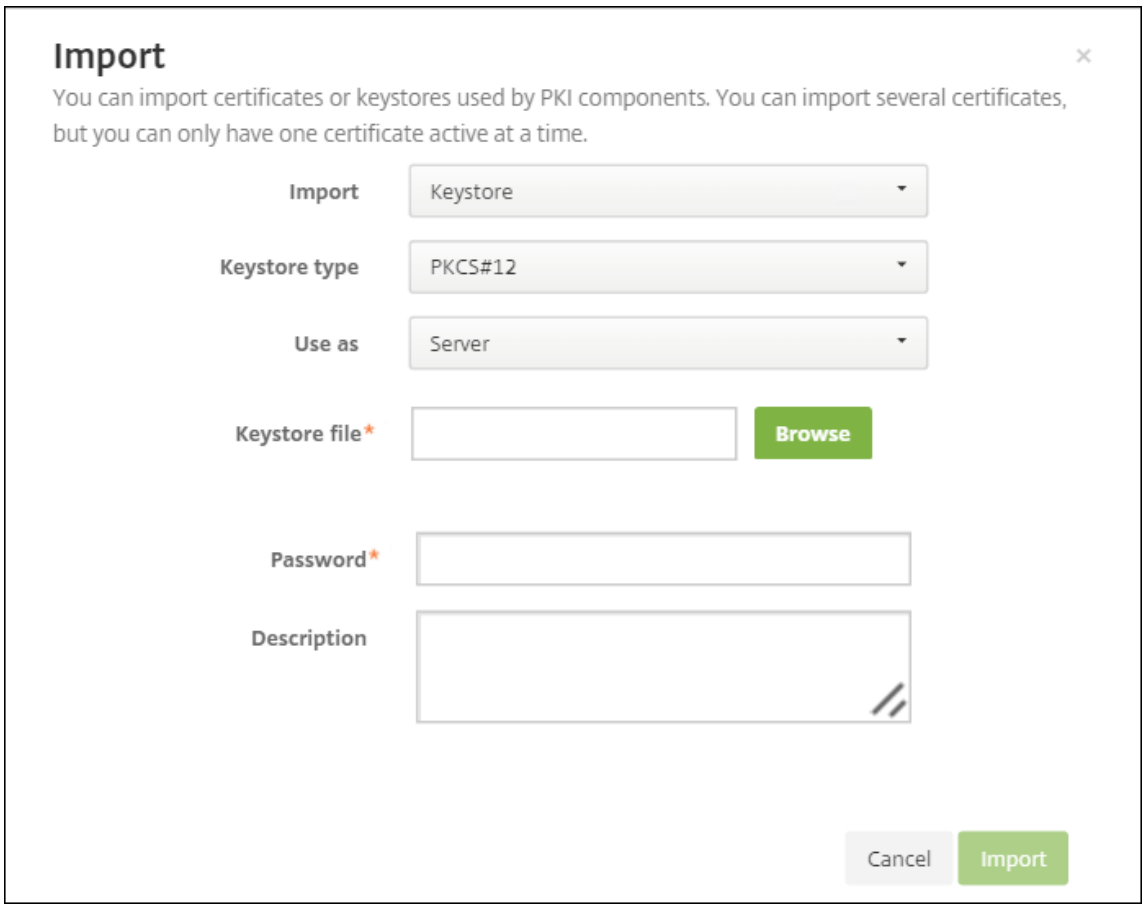
10. Legen Sie ein Kennwort für den Upload des Zertifikats in XenMobile fest.



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. Die Seite **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.

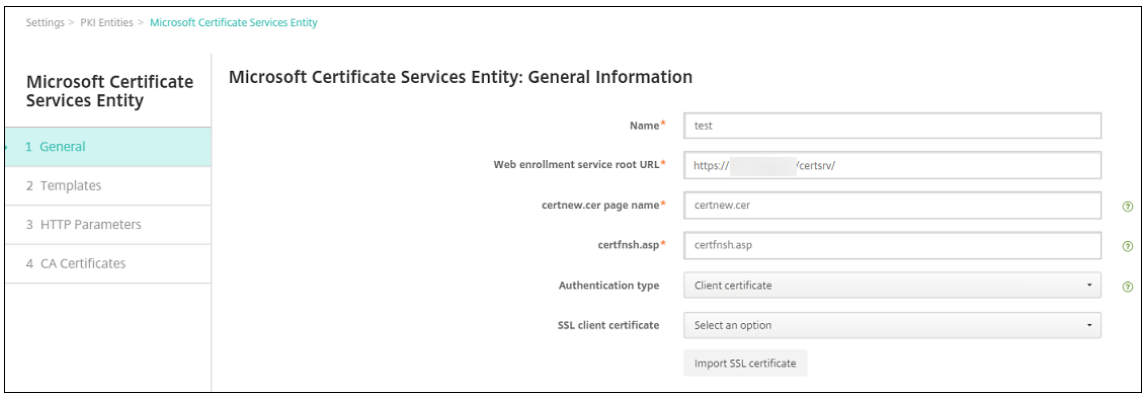


4. Klicken Sie auf **Importieren**.
5. Prüfen Sie, ob das Zertifikat richtig installiert wurde. Ein richtig installiertes Zertifikat wird als Benutzerzertifikat angezeigt.

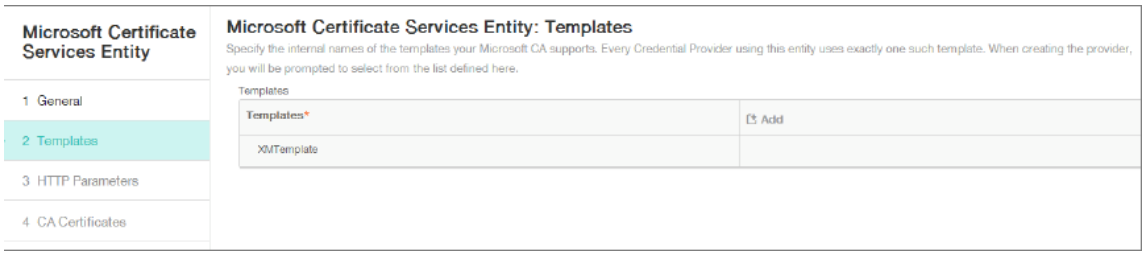
Erstellen der PKI-Entität für die zertifikatbasierte Authentifizierung

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

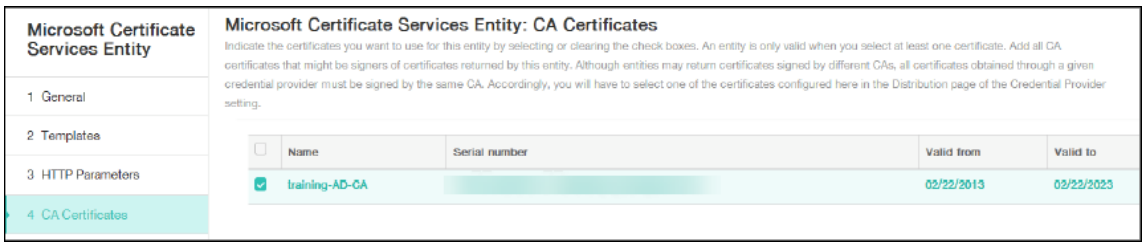
- **SSL-Clientzertifikat:** Wählen Sie das Benutzerzertifikat aus, das zum Ausstellen des XenMobile-Clientzertifikats verwendet werden soll.



4. Fügen Sie unter **Vorlagen** die Vorlage hinzu, die Sie beim Konfigurieren des Microsoft-Zertifikats erstellt haben. Fügen Sie keine Leerzeichen hinzu.



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.

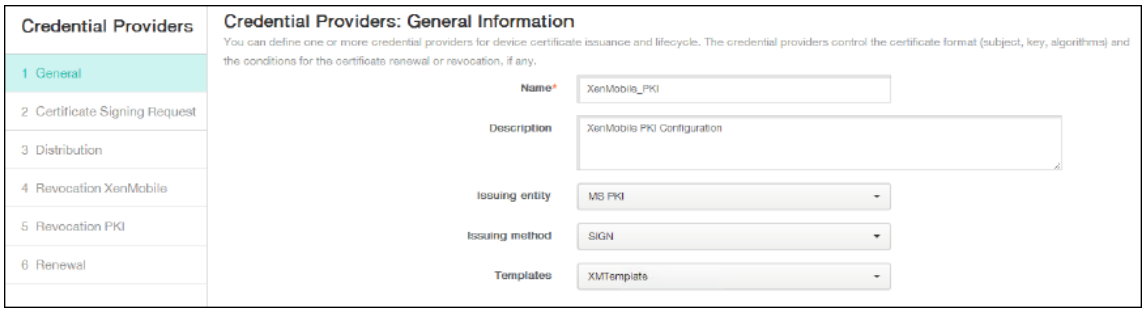


7. Klicken Sie auf **Speichern**.

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:** SHA256withRSA
   - **Antragsstellername:** `cn=$user.username`

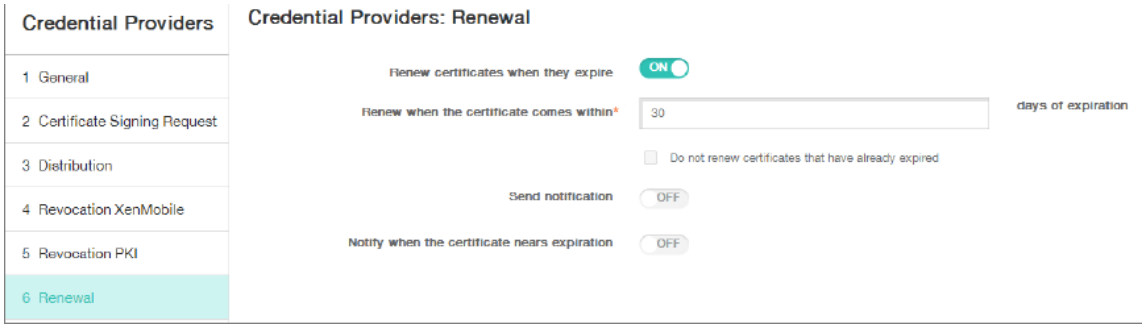
   Klicken Sie für **Alternative Antragstellernamen** auf **Hinzufügen** und geben Sie die folgenden Parameter ein:

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

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

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

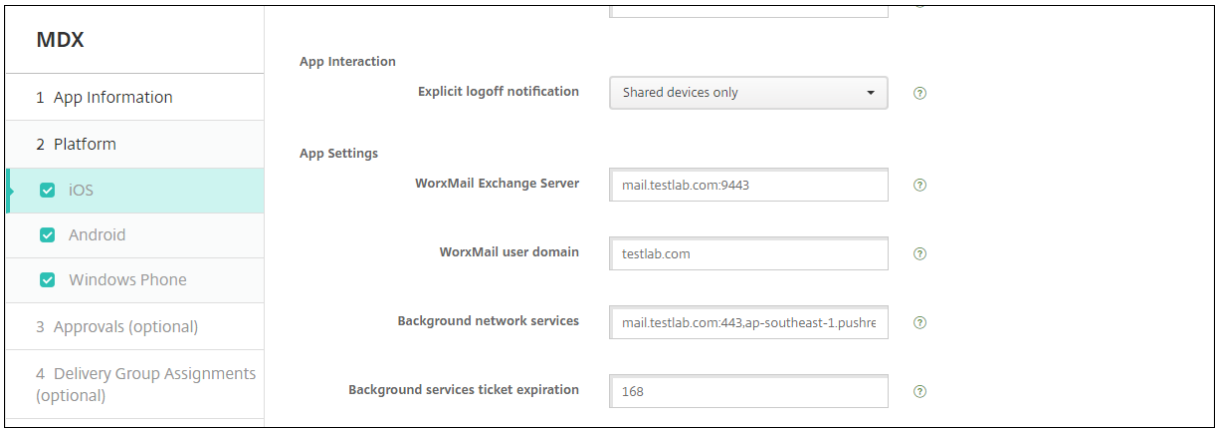
6. Legen Sie für die zwei folgenden Abschnitte **XenMobile-Sperrung** und **PKI-Sperrung** die Parameter nach Bedarf fest. In diesem Beispiel werden beide Optionen übersprungen.
7. Klicken Sie auf **Verlängerung**.
8. Wählen Sie für **Zertifikate erneuern, wenn sie ablaufen** die Option **EIN**.
9. Behalten Sie für alle anderen Einstellungen die Standardwerte bei oder ändern Sie sie nach Bedarf.



10. Klicken Sie auf **Speichern**.

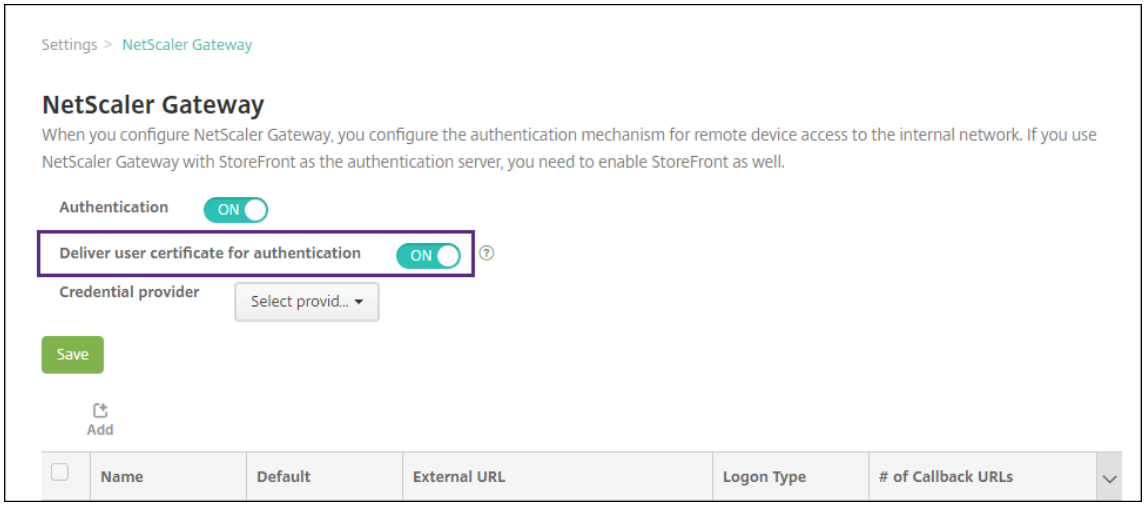
Konfigurieren von Secure Mail für die zertifikatbasierte Authentifizierung

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

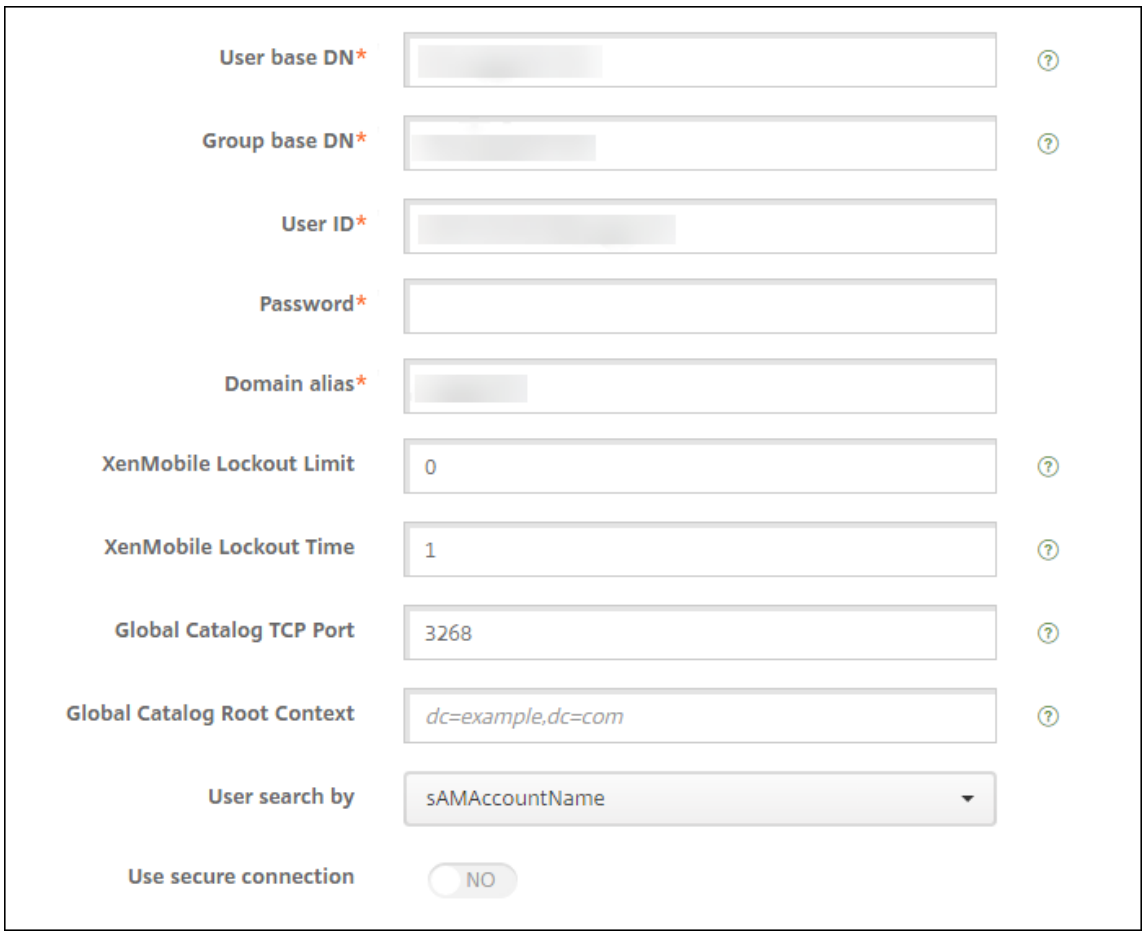


Konfigurieren der Citrix ADC-Zertifikatbereitstellung in XenMobile

1. Melden Sie sich bei der XenMobile-Konsole an und klicken Sie auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Server** auf **Citrix Gateway**.
3. Wenn Citrix Gateway noch nicht hinzugefügt wurde, klicken Sie auf **Hinzufügen** und legen Sie folgende Einstellungen fest:
   - **Externe URL:** `https://YourCitrixGatewayURL`
   - **Anmeldetyp:** Zertifikat und Domäne
   - **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. Zum Verwenden von sAMAccount-Attributen anstelle des UPN (Benutzerprinzipalname) in den Benutzerzertifikaten 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**.



Aktivieren der Citrix-PIN und der Zwischenspeicherung von Benutzerkennwörtern

Um die Citrix-PIN und die Zwischenspeicherung von Benutzerkennwörtern zu aktivieren, gehen Sie zu **Einstellungen > Clienteigenschaften** und aktivieren Sie die Kontrollkästchen **Enable Citrix-PIN Authentication** und **Enable User Password Caching**. Weitere Informationen finden Sie unter Clienteigenschaften.

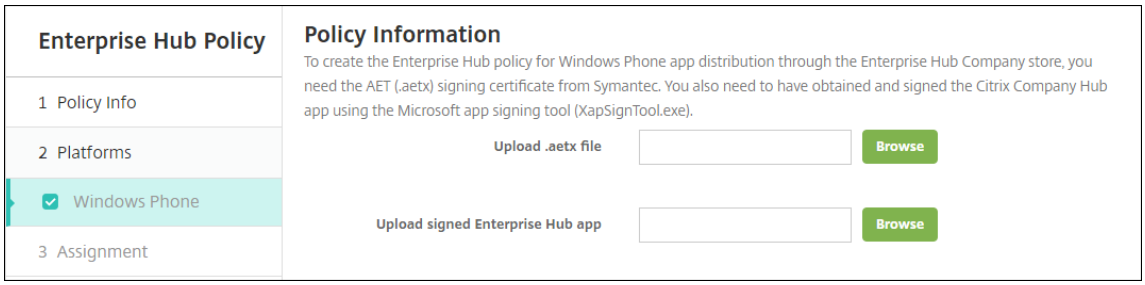
Erstellen einer Enterprise Hub-Richtlinie für Windows Phone

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

> **Hinweis:**
>
> Stellen Sie sicher, dass sowohl AETX- als auch Secure Hub-Dateien:
>
> - das gleiche Unternehmenszertifikat vom Zertifikatanbieter verwenden.
> - die gleiche Publisher-ID aus dem Windows Store-Entwicklerkontenprofil verwenden.

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

2. Klicken Sie auf **Hinzufügen** und dann unter **Mehr > XenMobile-Agent** auf **Enterprise Hub**.
3. Nach Eingabe eines Namens für die Richtlinie wählen Sie die richtige `.AETX`-Datei und signierte Secure Hub-App für den Enterprise Hub aus.



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

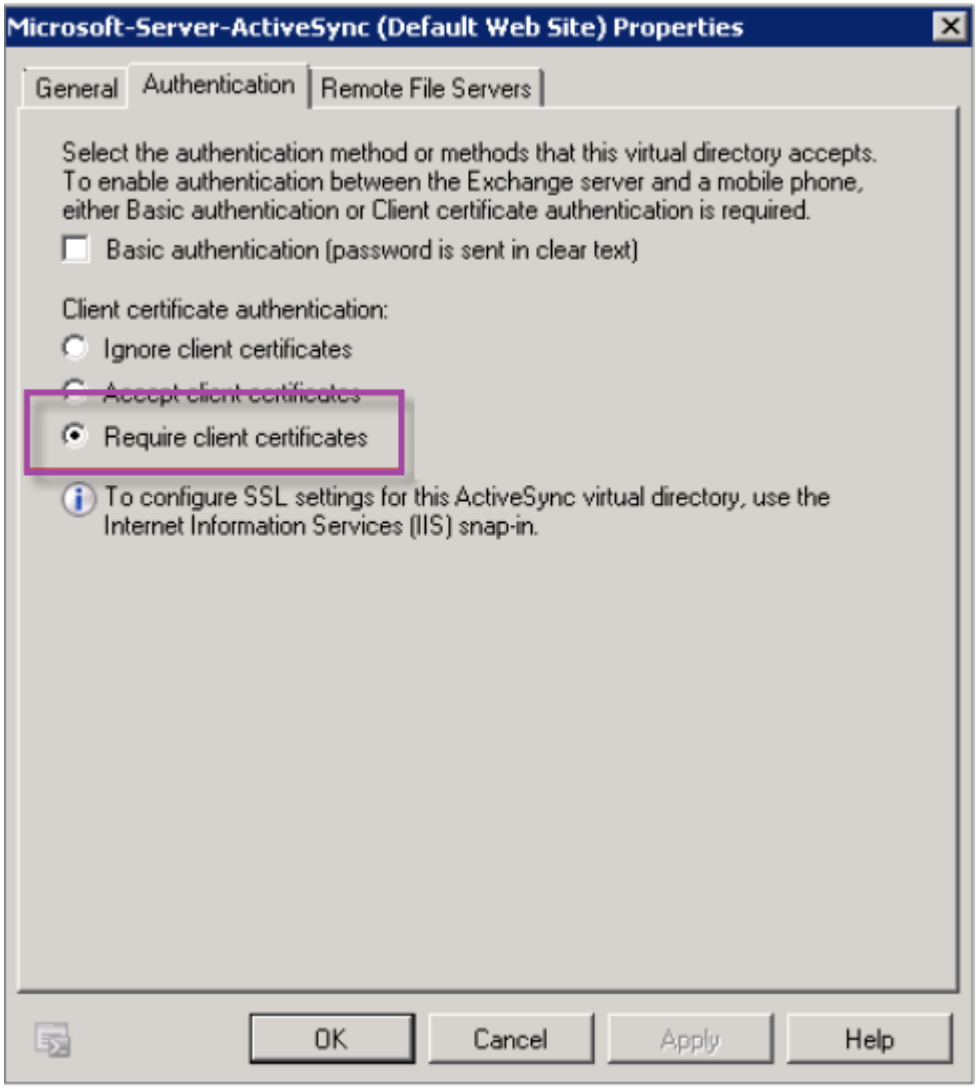
Problembehandlung bei der Clientzertifikatkonfiguration

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

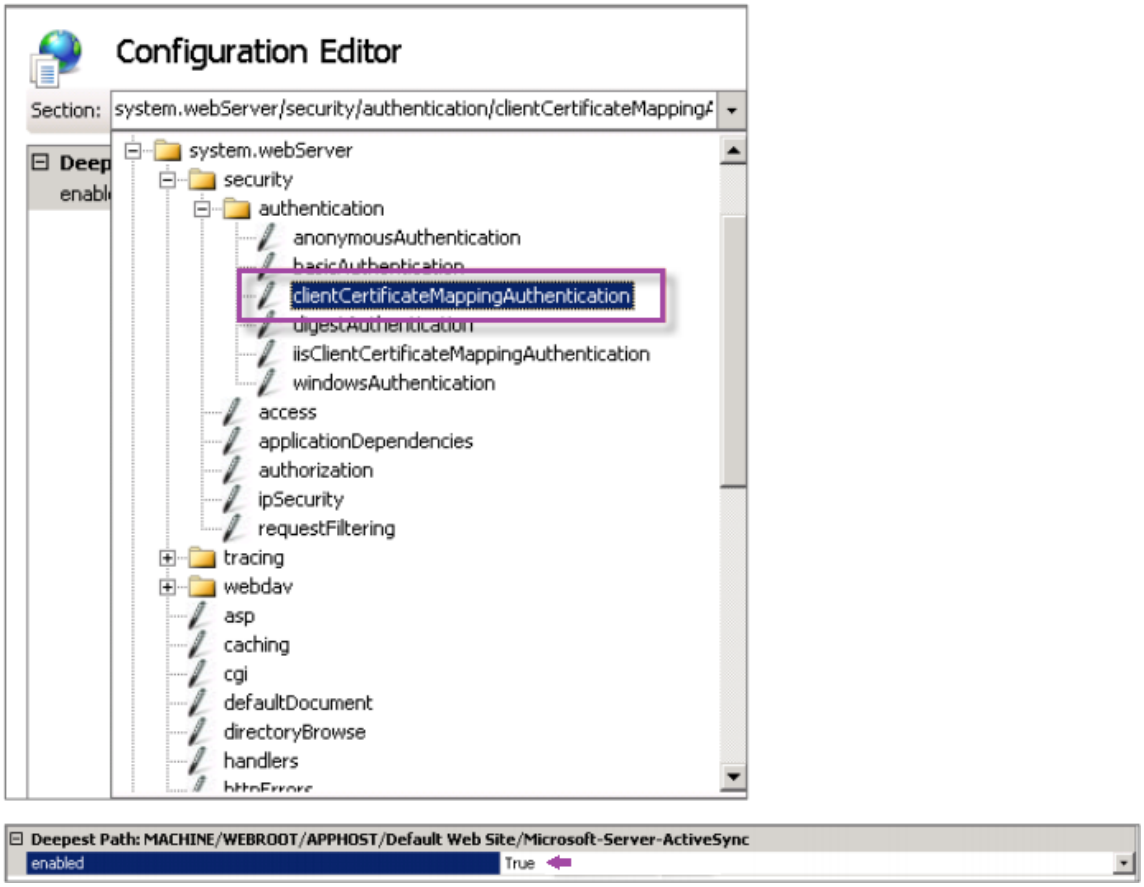
1. Der Benutzer registriert sein mobiles Gerät.
2. XenMobile fordert den Benutzer auf, eine Citrix PIN zu erstellen.
3. Der Benutzer wird an den XenMobile Store weitergeleitet.
4. Wenn Benutzer Secure Mail starten, fordert XenMobile sie nicht auf, die Benutzeranmeldeinformationen einzugeben, um das Postfach zu konfigurieren. 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 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 auf dem Microsoft Exchange Server für die Site **Microsoft-Server-ActiveSync** die Authentifizierung über Clientzertifikatzuordnung aktiviert ist. Standardmäßig ist die Authentifizierung über Clientzertifikatzuordnung deaktiviert. Die Option befindet sich unter **Konfigurationseditor > Sicherheit > Authentifizierung**.



Klicken Sie nach der Auswahl von **True** auf **Anwenden**, damit die Änderungen wirksam werden.

4. Überprüfen Sie die Citrix 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.

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:

   Citrix Gateway-Anmeldeinformationen: Requested credential, CertId=

Überprüfen, ob die Clientzertifikataushandlung aktiviert wurde

1. Führen Sie den Befehl `netsh` 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=609da5df280d1f54a7deb714fb2c54
    appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreNam
    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, überprüfen Sie Folgendes:

- Der Anwendungsregistrierungstoken (AETX-Datei) wird mit XenMobile über die Enterprise Hub-Richtlinie bereitgestellt.
- Der Anwendungsregistrierungstoken wurde mit dem gleichen Enterprise-Zertifikat des Zertifikatanbieters erstellt, das zum Umschließen und zum Signieren von den Apps Secure Mail und Secure Hub verwendet wird.
- Zum Signieren und Umschließen von Secure Hub, Secure Mail und Anwendungsregistrierungstoken wird die gleiche Aussteller-ID verwendet.

PKI-Entitäten

January 5, 2022

Eine XenMobile-PKI-Entität ist eine Komponente, die PKI-Vorgänge (Ausstellung, Sperrung und Statusinformationen) durchführt. Dies sind interne oder externe Komponenten von XenMobile. Interne Komponenten werden als eigenverwaltet bezeichnet. Externe Komponenten sind Teil Ihrer Unternehmensinfrastruktur.

XenMobile unterstützt folgende Arten von PKI-Entitäten:

- Generic PKIs (GPKIs)

Die Unterstützung von XenMobile Server für GPKIs umfasst DigiCert Managed PKI.

- Microsoft Zertifikatdienste
- Eigenverwaltete CAs

XenMobile unterstützt die folgenden Zertifizierungsstellenserver:

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

Allgemeine PKIs – 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. wiederhergestellten Zertifikate signiert. Diese PKI-Entität kann abgerufene oder neu signierte Zertifikate, die von einer beliebigen Zahl verschiedener Zertifizierungsstellen signiert wurden, zurückgeben.

Stellen Sie das Zertifikat jeder dieser Zertifizierungsstellen als Teil der PKI-Entitätskonfiguration bereit. Hierfür laden Sie die Zertifikate in XenMobile hoch und referenzieren sie dann in der PKI-Entität. Bei eigenverwalteten Zertifizierungsstellen gehört das Zertifikat implizit zur signierenden Zertifizierungsstelle. Bei externen Entitäten müssen Sie das Zertifikat manuell definieren.

> **Wichtig:**
>
> Zur Vermeidung von Problemen bei der Authentifizierung registrierter Geräte verwenden Sie beim Erstellen einer Microsoft-Zertifikatdiensteentitätsvorlage keine Sonderzeichen im Vorlagennamen. Beispiele für Sonderzeichen: `! : $ ( )## % + * ~ ? | { } [ ]`

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 (CSR) entgegennehmen, an die PKI übertragen und neu signierte Zertifikate zurückgeben.

- **Fetch:** Der Adapter kann vorhandene Zertifikate und Schlüsselpaare (je nach Eingabeparametern) von der PKI abrufen bzw. 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. So gibt es beispielsweise GPKI-Grafikadapter für RSA und Entrust.

Der GPKI-Adapter veröffentlicht als SOAP-Webdienst-Endpunkt eine selbstbeschreibende WSDL-Definition (Web Services Description Language). Das Erstellen einer GPKI-PKI-Entität geschieht durch Bereitstellen dieser WSDL-Definition für XenMobile über eine URL oder durch Hochladen der Datei selbst.

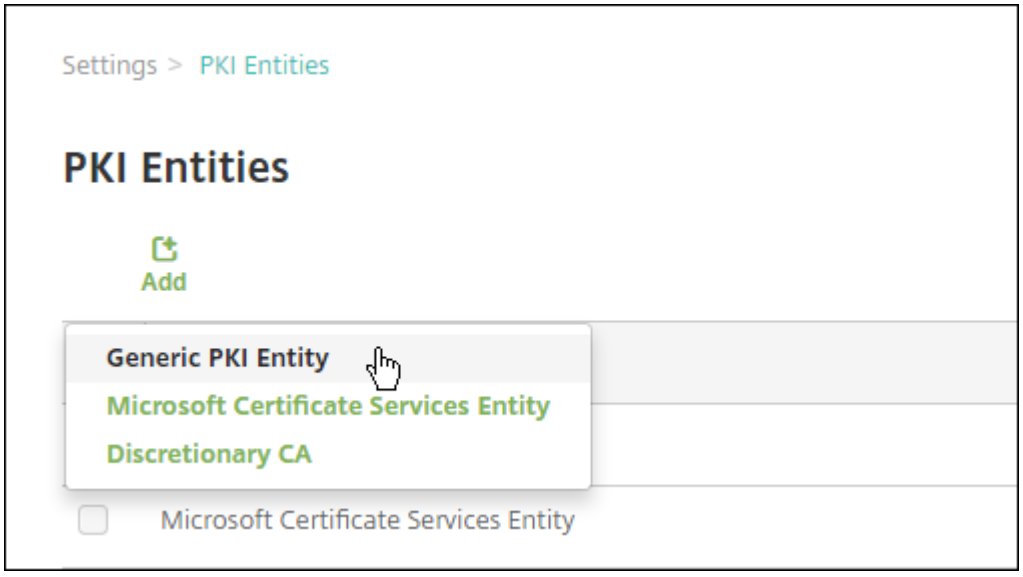
Unterstützung für die einzelnen PKI-Vorgänge ist bei einem Adapter optional. Wenn ein Adapter einen bestimmten Vorgang unterstützt, hat der Adapter die entsprechende Funktion (sign, fetch oder revoke). Jeder Funktion können diverse Benutzerparameter zugeordnet werden.

Benutzerparameter sind Parameter, die der GPKI-Adapter für einen bestimmten Vorgang definiert und für die Sie in XenMobile die Werte angeben müssen. XenMobile ermittelt durch Analyse der WSDL, welche Vorgänge ein Adapter 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 generischen PKI

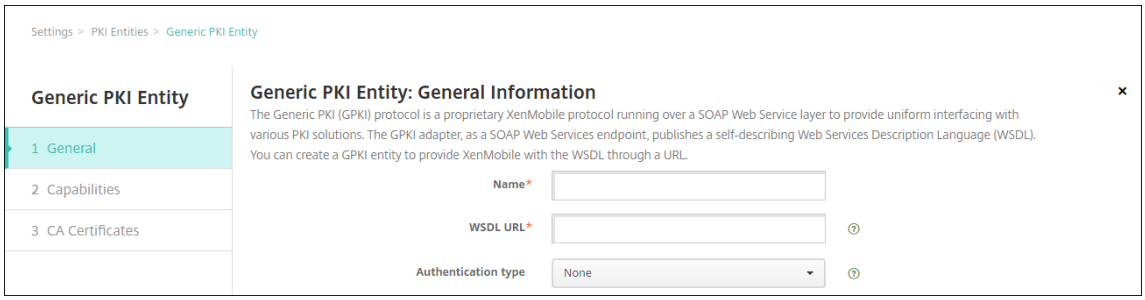
1. Klicken Sie in der XenMobile-Konsole auf **Einstellungen > PKI-Entitäten**.
2. Klicken Sie auf der Seite **PKI-Entitäten** auf **Hinzufügen**.

   Ein Menü der PKI-Entitätstypen 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.

   Entitäten können zwar von verschiedenen Zertifizierungsstellen signierte Zertifikate zurückgeben, es müssen jedoch alle von einem bestimmten Zertifikatanbieter abgerufenen Zertifikate von derselben Zertifizierungsstelle signiert sein. Wählen Sie daher 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.

DigiCert-verwaltete PKI

Die Unterstützung von XenMobile Server für GPKIs umfasst DigiCert Managed PKI (auch als MPKI bezeichnet). In diesem Abschnitt wird beschrieben, wie Sie Windows Server und XenMobile Server für DigiCert Managed PKI einrichten.

Voraussetzungen

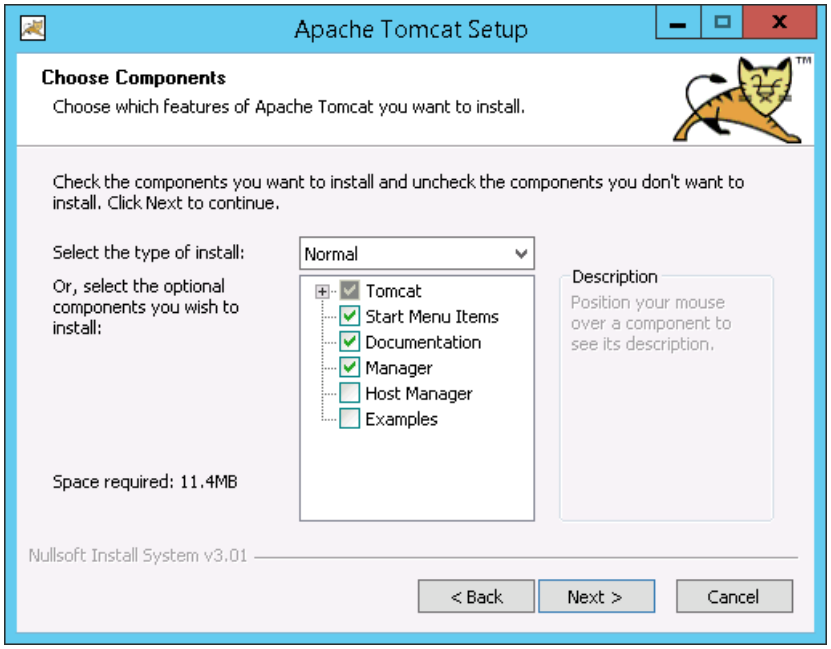
- Zugriff auf die DigiCert Managed PKI-Infrastruktur
- Windows Server 2012 R2-Server mit folgenden (im vorliegenden Artikel beschriebenen) Komponenten:
  - Java
  - Apache Tomcat
  - DigiCert PKI-Client
  - Portecle
- Zugriff auf die XenMobile-Downloadseite

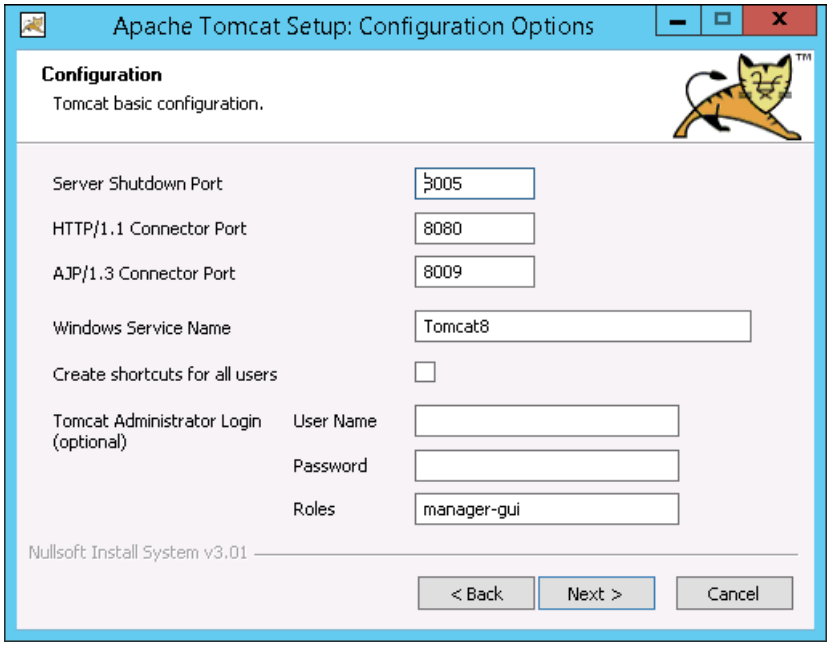
Installieren von Java unter Windows Server

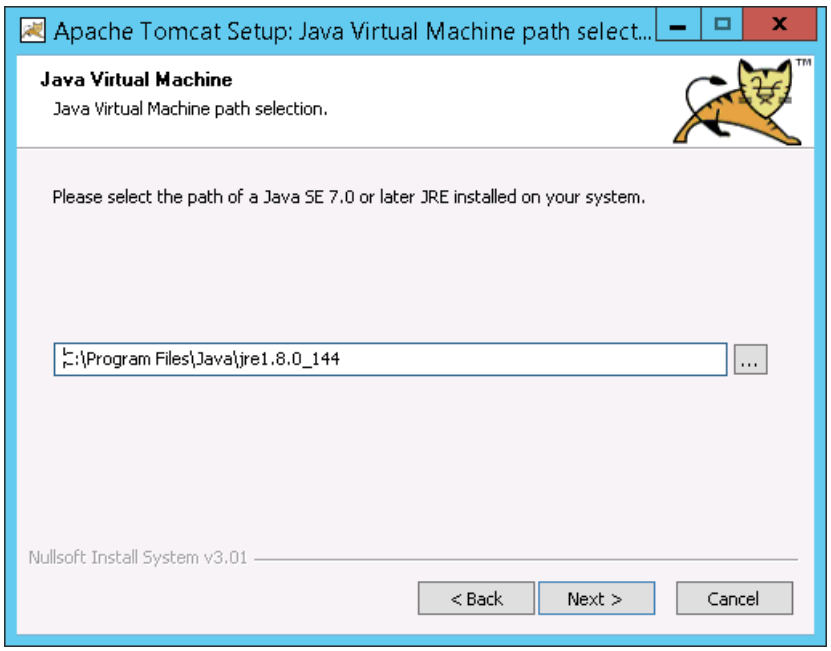
Laden Sie Java von https://java.com/en/download/faq/java_win64bit.xml herunter und installieren Sie es. Klicken Sie im Dialogfeld “Sicherheitswarnung” auf **Ausführen**.

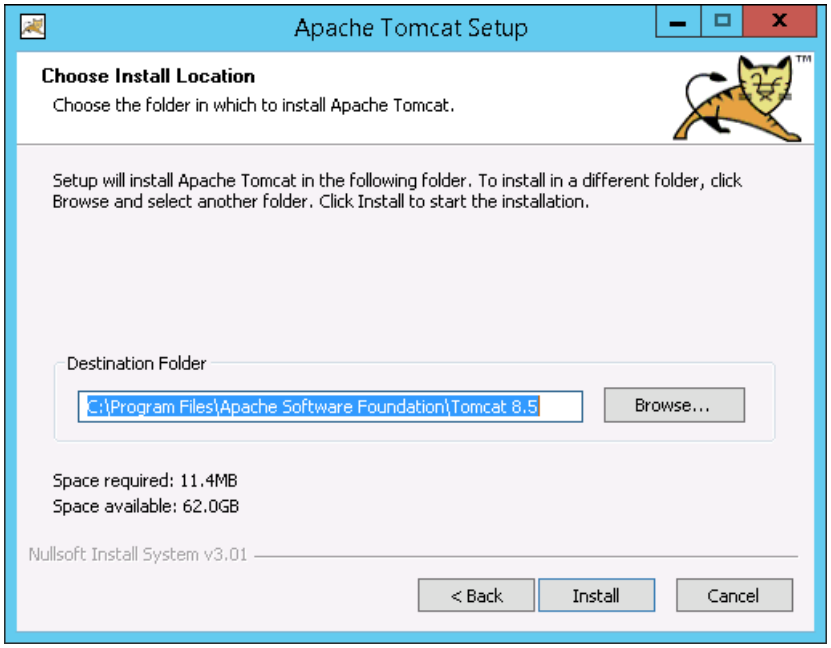
Installieren von Apache Tomcat unter Windows Server

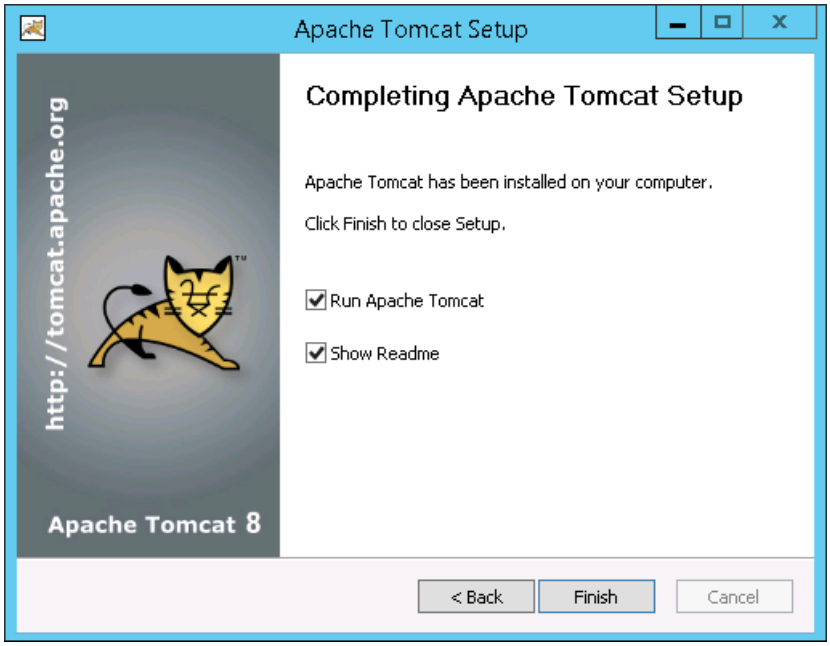
Laden Sie das 32- oder 64-Bit-Windows-Installationsprogramm für Apache Tomcat von https://tomcat.apache.org/download-80.cgi herunter und installieren Sie es. Klicken Sie im Dialogfeld “Sicherheitswarnung” auf **Ausführen**. Führen Sie die Einrichtung von Apache Tomcat anhand der nachfolgenden Beispiele als Leitfaden aus.



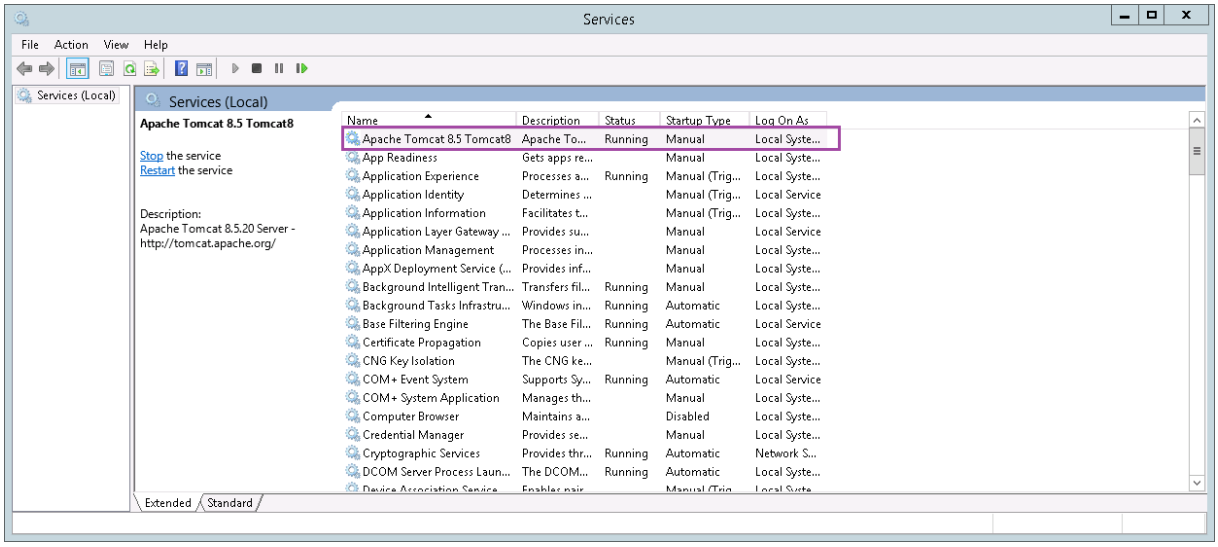


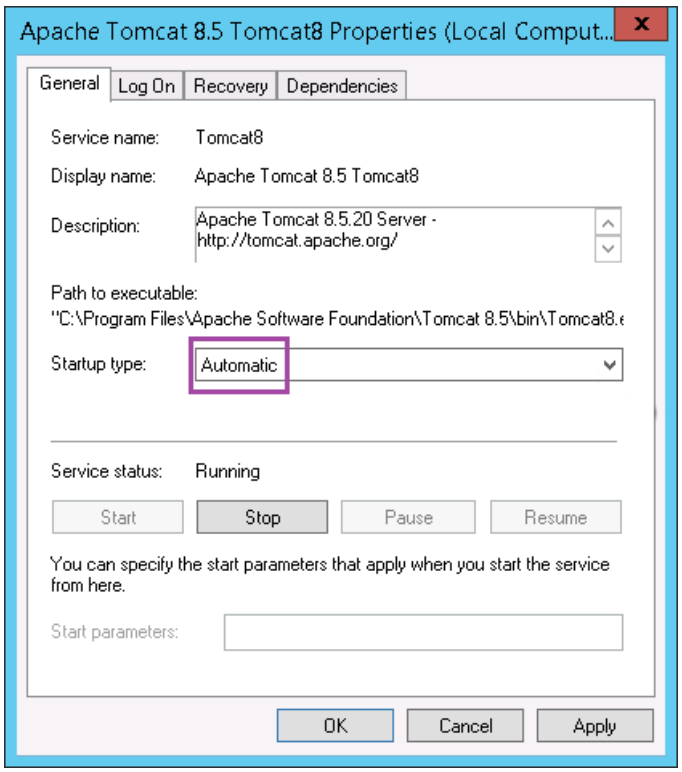






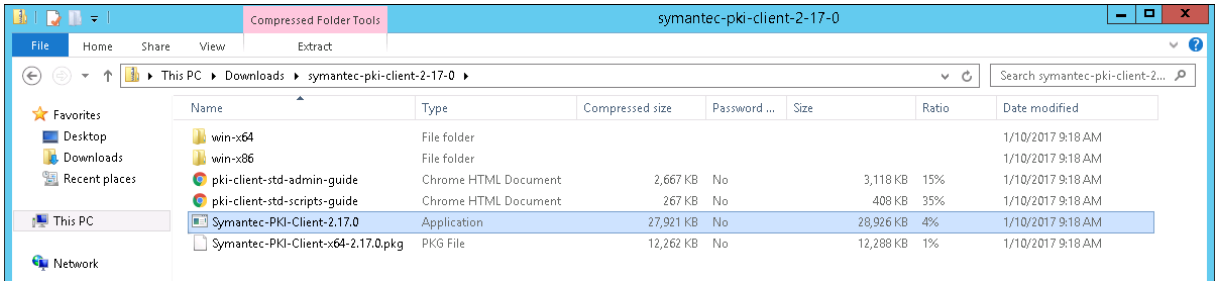
Ändern Sie dann in den Windows-Diensten den **Starttyp** von **Manuell** in **Automatisch**.

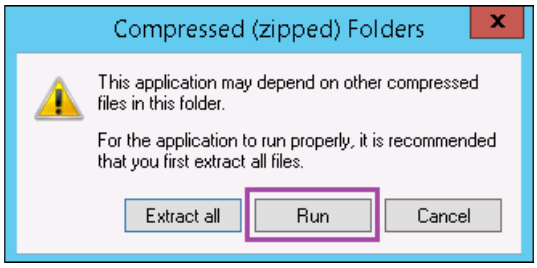




Installieren des DigiCert PKI-Client unter Windows Server

Laden Sie das Installationsprogramm aus der PKI Manager-Konsole hoch. Wenn Sie nicht auf diese Konsole zugreifen können, laden Sie das Installationsprogramm von der DigiCert-Supportseite How to download DigiCert PKI Client herunter. Entpacken Sie das Installationsprogramm und führen Sie es aus.





Klicken Sie im Dialogfeld “Sicherheitswarnung” auf **Ausführen**. Folgen Sie den Anweisungen

im Installationsprogramm, um die Einrichtung abzuschließen. Wenn das Installationsprogramm abgeschlossen ist, werden Sie zum aufgefordert, einen Neustart auszuführen.

Installieren von Portecle unter Windows Server

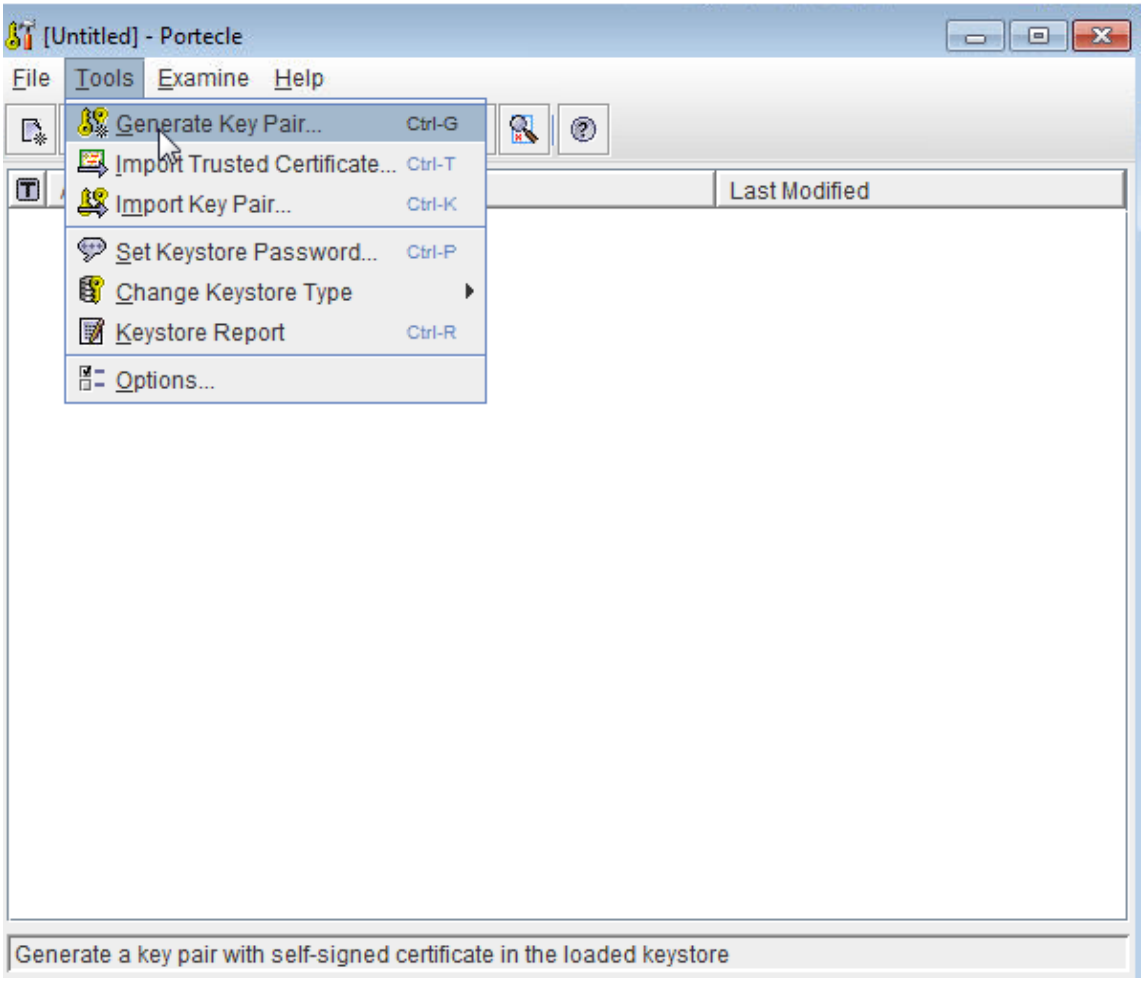
Laden Sie das Installationsprogramm von https://sourceforge.net/projects/portecleinstall/files/ herunter, entpacken Sie es und führen Sie es aus.

Generieren des Registrierungsstellenzertifikats für DigiCert Managed PKI

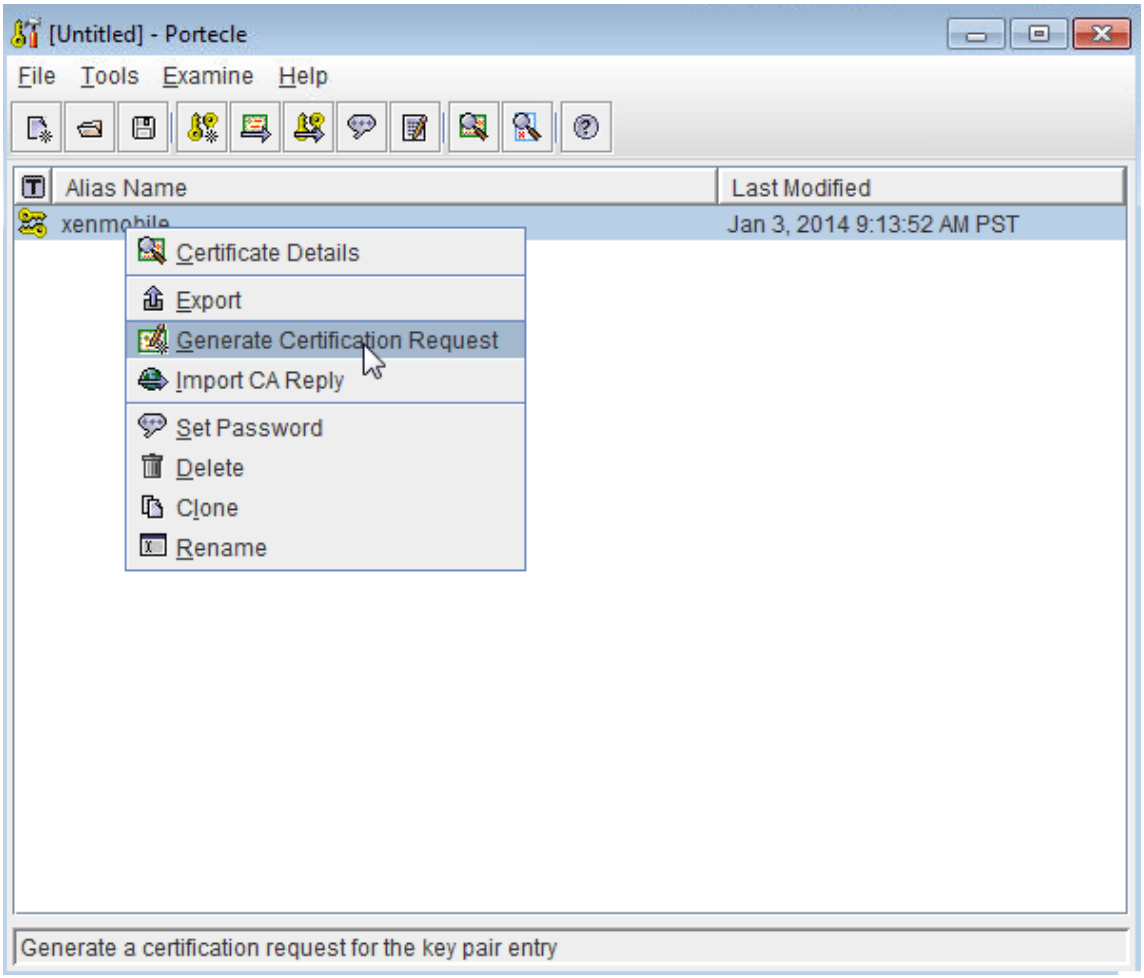
Der Schlüsselspeicher für die Clientzertifikatauthentifizierung ist in einem Zertifikat der Registrierungsstelle (RA) mit dem Namen RA.jks enthalten. Nachfolgend wird beschrieben, wie Sie das Zertifikat mit Portecle erstellen. Sie können das RA-Zertifikat auch über die Befehlsschnittstelle (CLI) von Java generieren.

In diesem Artikel wird auch beschrieben, wie Sie das RA-Zertifikat und öffentliche Zertifikate hochladen.

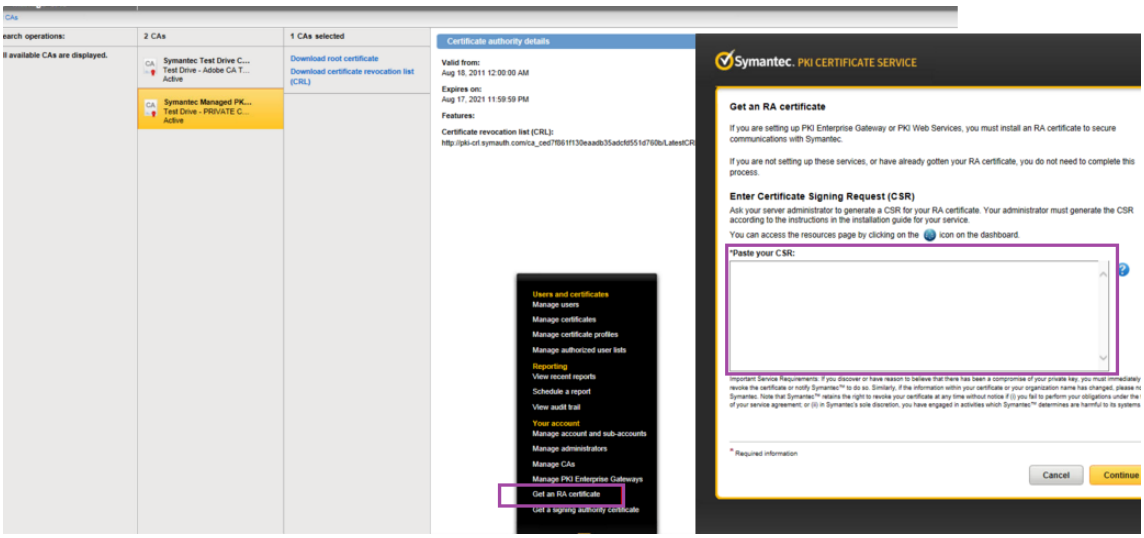
1. Navigieren Sie in Portecle zu **Tools > Generate Key Pair**, geben Sie die erforderlichen Informationen ein und generieren Sie das Schlüsselpaar.



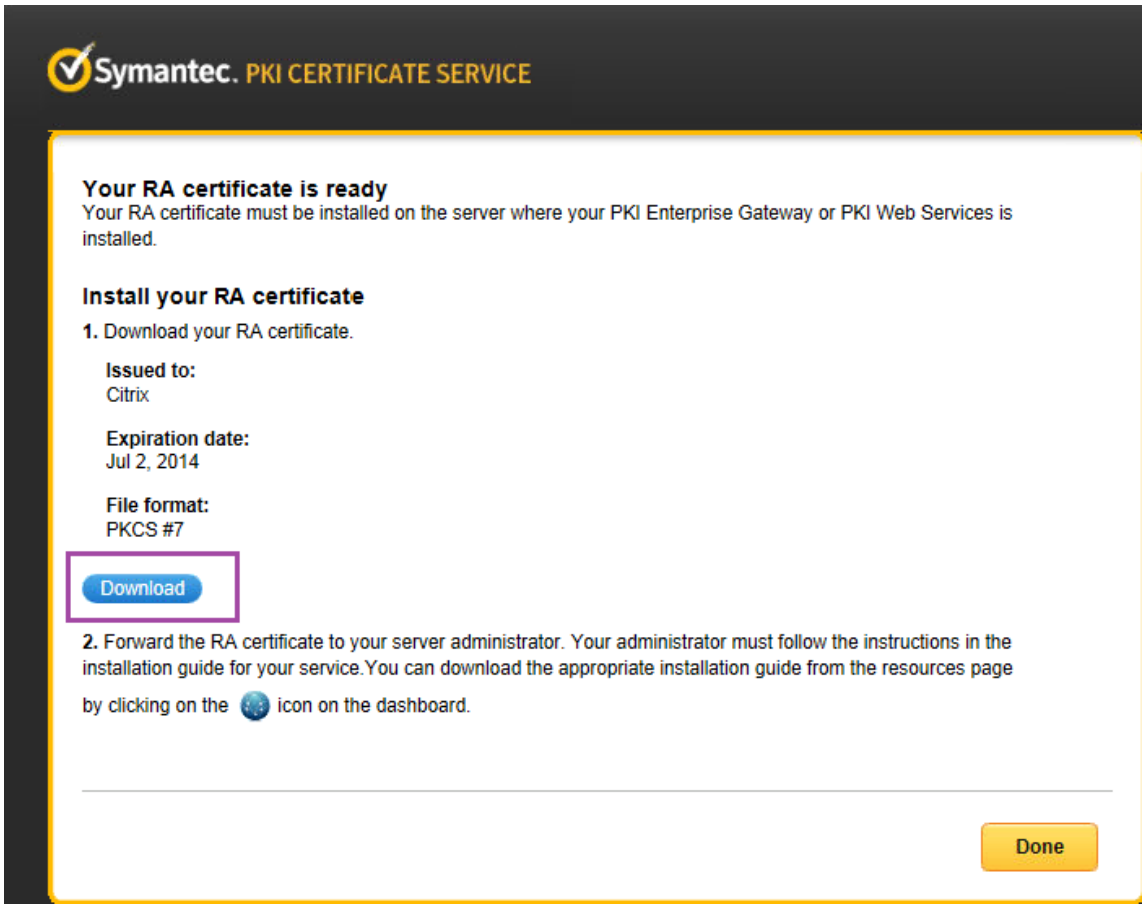
2. Klicken Sie mit der rechten Maustaste auf das Schlüsselpaar und klicken Sie auf **Generate Certification Request**, um die Zertifizierungsanforderung zu erstellen.



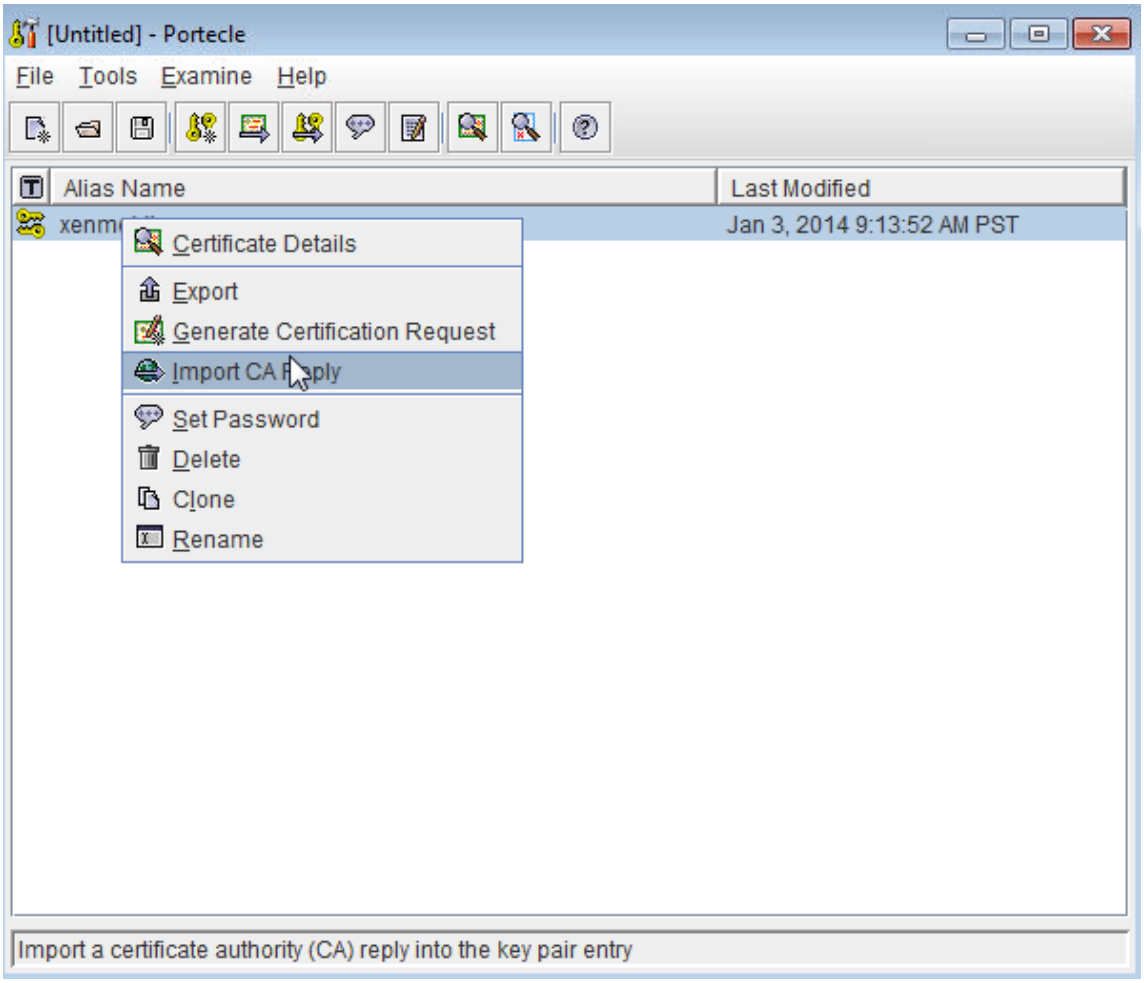
3. Kopieren Sie die Zertifikatsignieranforderung.
4. Erstellen Sie im DigiCert PKI Manager ein RA-Zertifikat: Klicken Sie auf **Settings** und dann auf **Get a RA Certificate**. Fügen Sie die CSR ein und klicken Sie auf **Continue**.



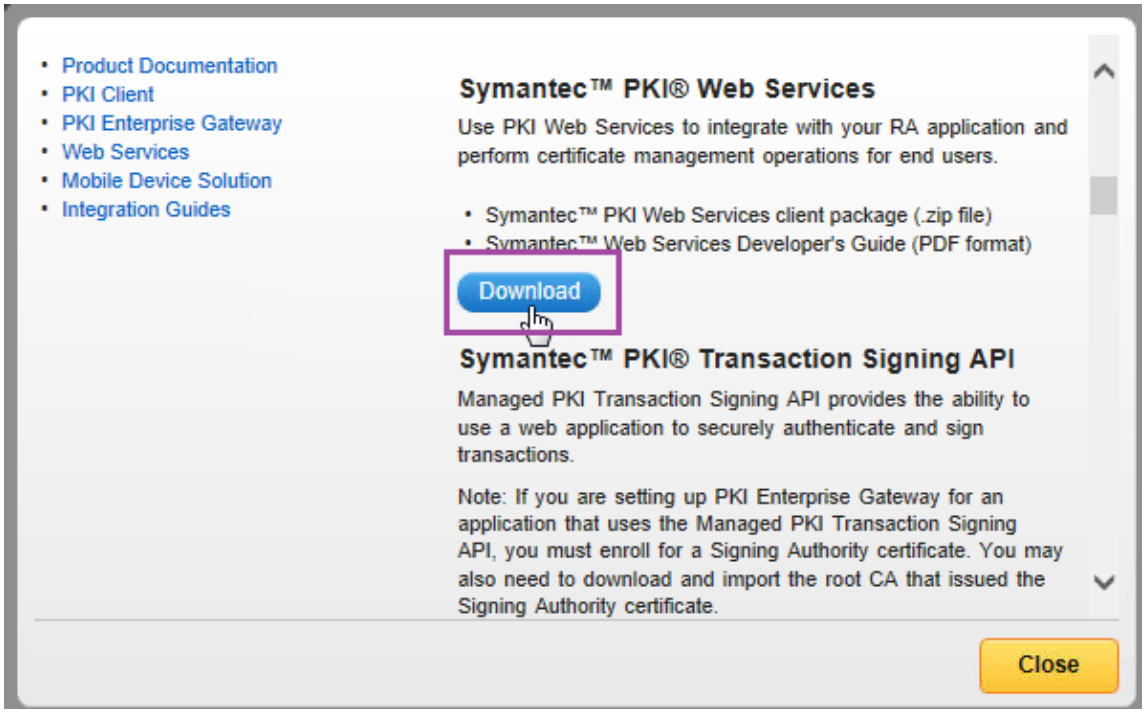
5. Klicken Sie auf **Download**, um das erstellte RA-Zertifikat herunterzuladen.



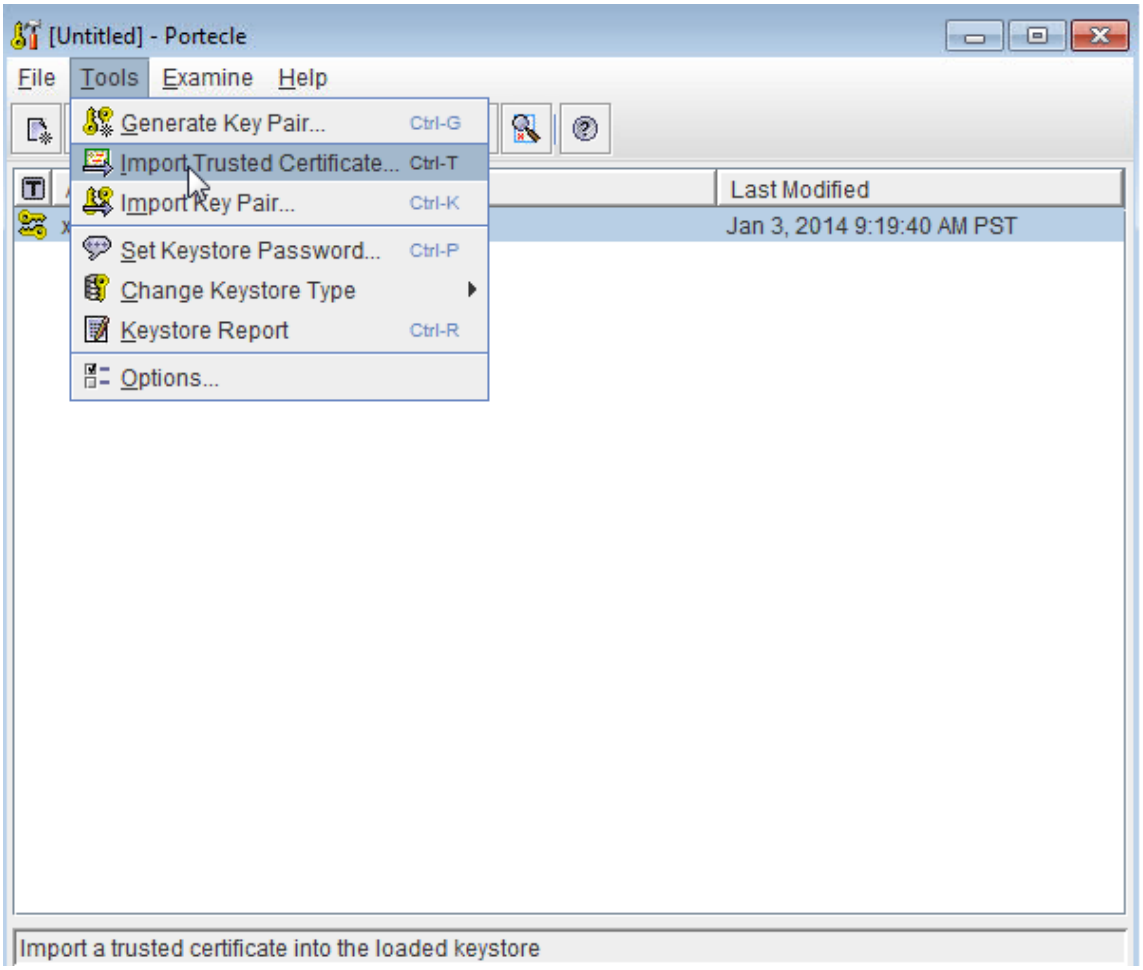
6. Importieren Sie das RA-Zertifikat in Portecle: Klicken Sie mit der rechten Maustaste auf das Schlüsselpaar und klicken Sie auf **Import CA Reply**.



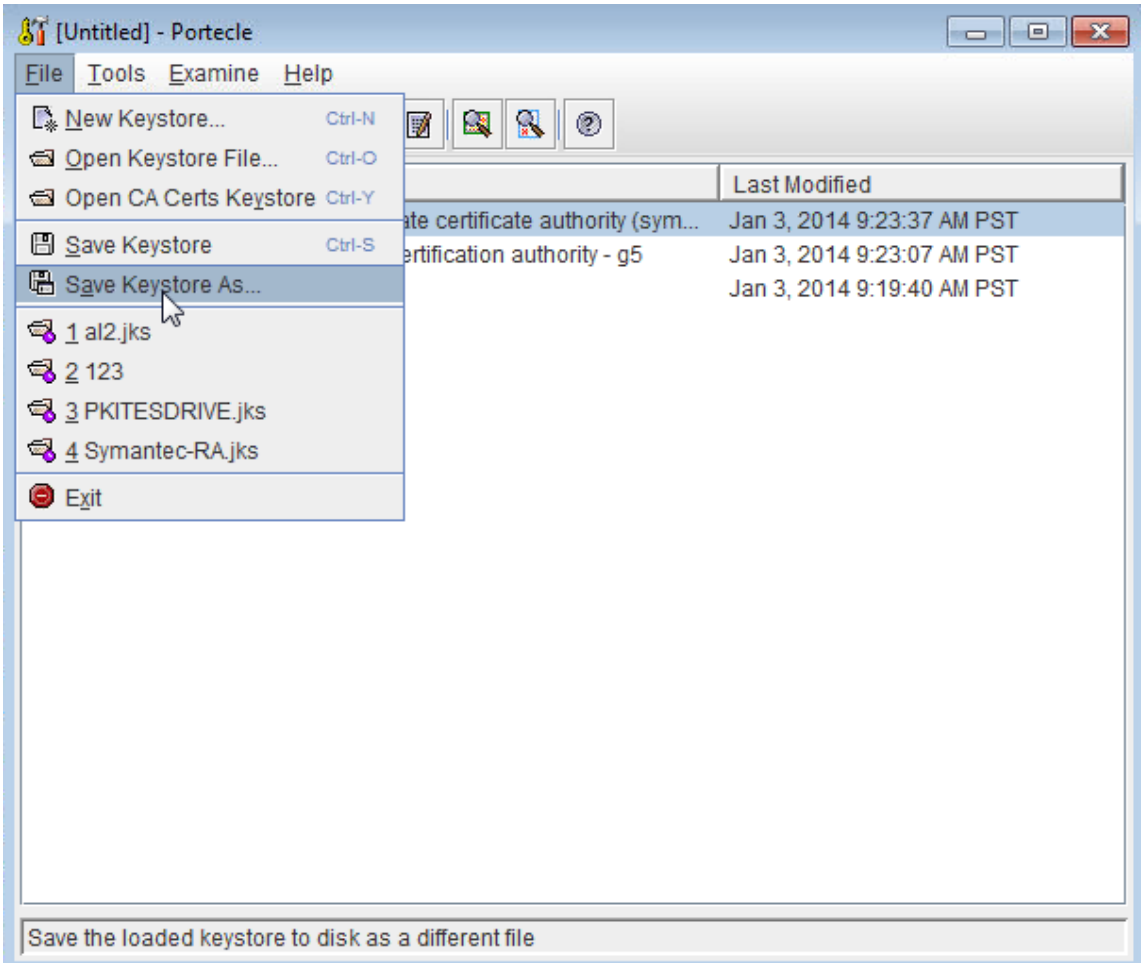
7. Gehen Sie im DigiCert PKI Manager zu **Resources > Web Services** und laden Sie die ZS-Zertifikate herunter.



8. Importieren Sie die Zwischen- und Stammzertifikate der Registrierungsstelle in Portecle in den Schlüsselspeicher: Gehen Sie zu **Tools > Import Trusted Certificates**.



9. Speichern Sie nach dem ZS-Import den Schlüsselspeicher als RA.jks im Verzeichnis C:\DigiCert des Windows-Servers.



Konfigurieren von DigiCert PKI Adapter unter Windows Server

1. Melden Sie sich als Administrator bei Windows Server an.
2. Laden Sie die zuvor erstellte Datei RA.jks hoch. Laden Sie zudem die öffentlichen Zertifikate (cacerts.jks) für den Symantec MPKI-Server hoch.
3. Laden Sie die Symantec PKI Adapter-Datei herunter:
   a) Gehen Sie zu https://www.citrix.com/downloads.
   b) Navigieren Sie zu **Citrix Endpoint Management (und Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10 > Tools**.
   c) Klicken Sie auf der Kachel **Symantec PKI-Adapter** auf **Download File**.
   d) Entpacken Sie die Datei und kopieren Sie die Dateien in das Laufwerk C: des Windows Server-Computers:
      - custom_gpki_adapter.properties
      - Symantec.war

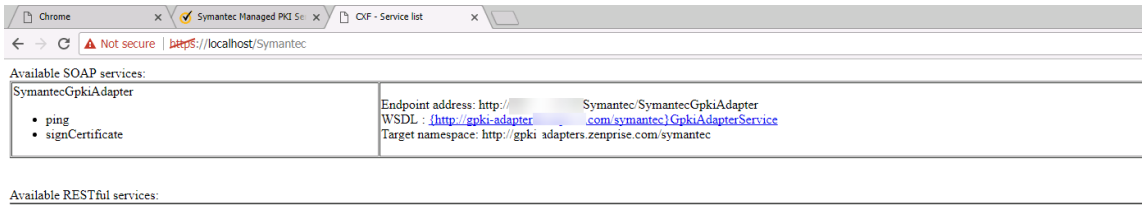
4. Öffnen Sie custom_gpki_adapter.properties im Editor und bearbeiten Sie die folgenden Werte:

```
Gpki.CaSvc.Url=https://<managed PKI URL>

# keystore for client-cert auth

keyStore=C:\Symantec\RA.jks

# truststore for server with self-signed root CA

trustStore=C:\Symantec\cacerts.jks
<!--NeedCopy-->
```

5. Kopieren Sie Symantec.war unter den Ordner `<tomcat dir>\webapps` und starten Sie Tomcat.
6. Vergewissern Sie sich, dass die Anwendung bereitgestellt wurde: Öffnen Sie einen Webbrowser und navigieren Sie zu `https://localhost/Symantec`.
7. Navigieren Sie zum Ordner `<tomcat dir>\webapps\Symantec\WEB-INF\classes` und bearbeiten Sie gpki_adapter.properties. Ändern Sie die Eigenschaft **CustomProperties** so, dass sie auf die Datei custom_gpki_adapter unter dem Ordner C:\Symantec verweist:

   ```
   CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties
   ```

8. Starten Sie Tomcat neu, navigieren Sie zu `https://localhost/Symantec` und kopieren Sie die Endpunktadresse. Im nächsten Abschnitt fügen Sie diese Adresse beim Konfigurieren des PKI-Adapters ein.

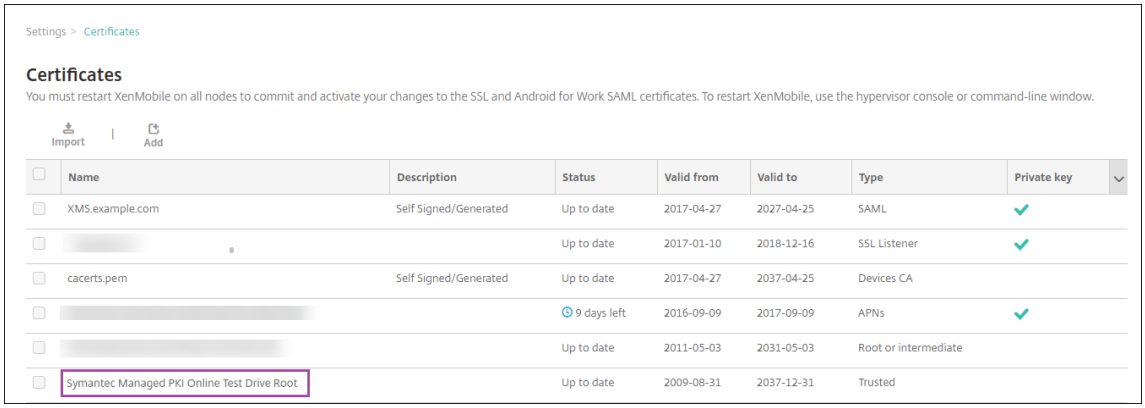


Konfigurieren von XenMobile Server für DigiCert Managed PKI

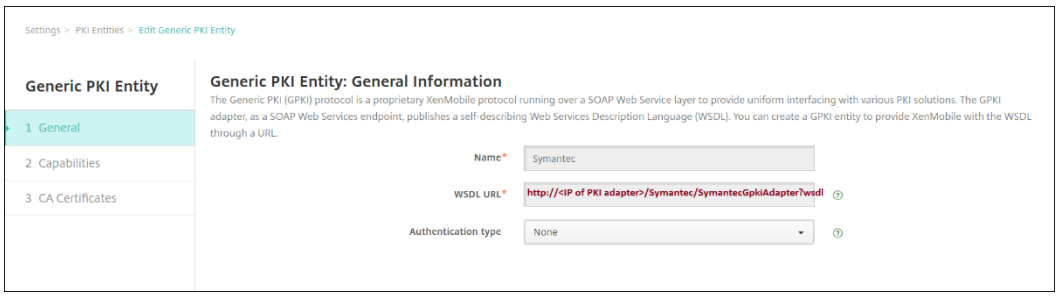
Richten Sie Windows Server ein, bevor Sie die folgende Konfiguration für XenMobile Server durchführen.

Importieren der DigiCert-ZS-Zertifikate und Konfigurieren der PKI-Entität

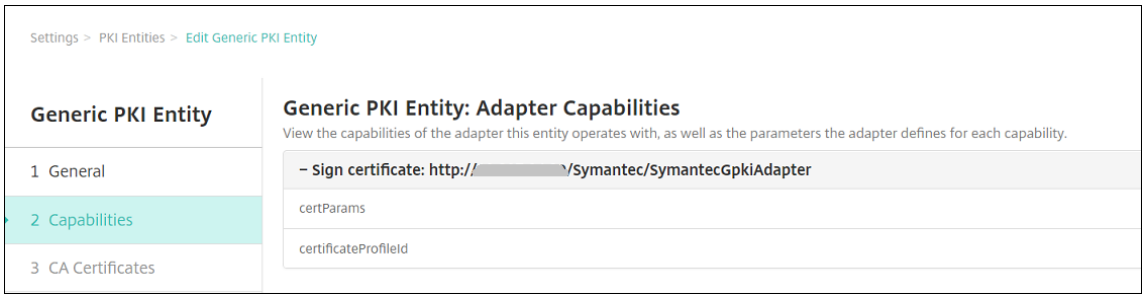
1. Importieren Sie die DigiCert-ZS-Zertifikate, welche das Endbenutzerzertifikat ausstellen: Klicken Sie auf in der XenMobile Server-Konsole unter **Einstellungen > Zertifikate** auf **Importieren**.



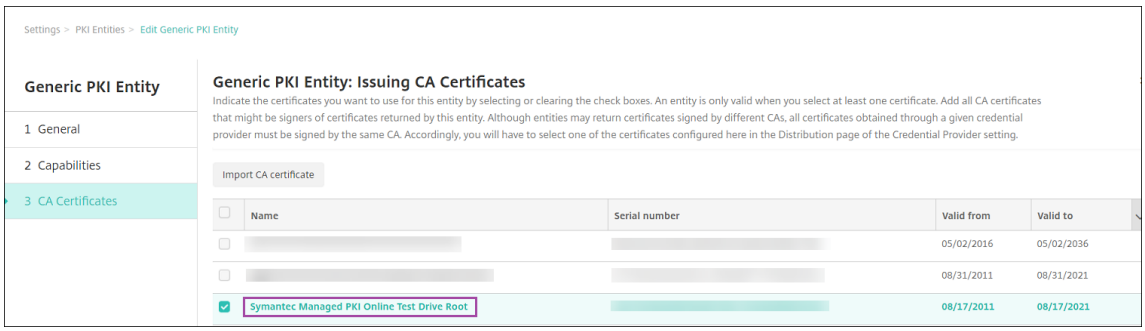
2. Fügen Sie die PKI-Entität hinzu und konfigurieren Sie sie: Klicken Sie unter **Einstellungen > PKI-Entitäten** auf **Hinzufügen** und wählen Sie dann **Generic PKI-Entität**. Fügen Sie unter **WSDL-URL** die beim Konfigurieren des PKI-Adapters (siehe vorheriger Abschnitt) kopierte Endpunktadresse ein und hängen Sie `?wsdl` an (siehe Abb. unten).



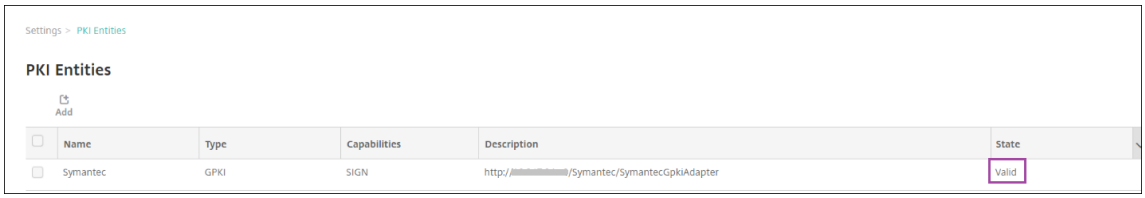
3. Klicken Sie auf **Weiter**. XenMobile füllt die Parameternamen aus der WSDL ein.



4. Klicken Sie auf **Weiter**, wählen Sie das richtige ZS-Zertifikat und klicken Sie auf **Speichern**.

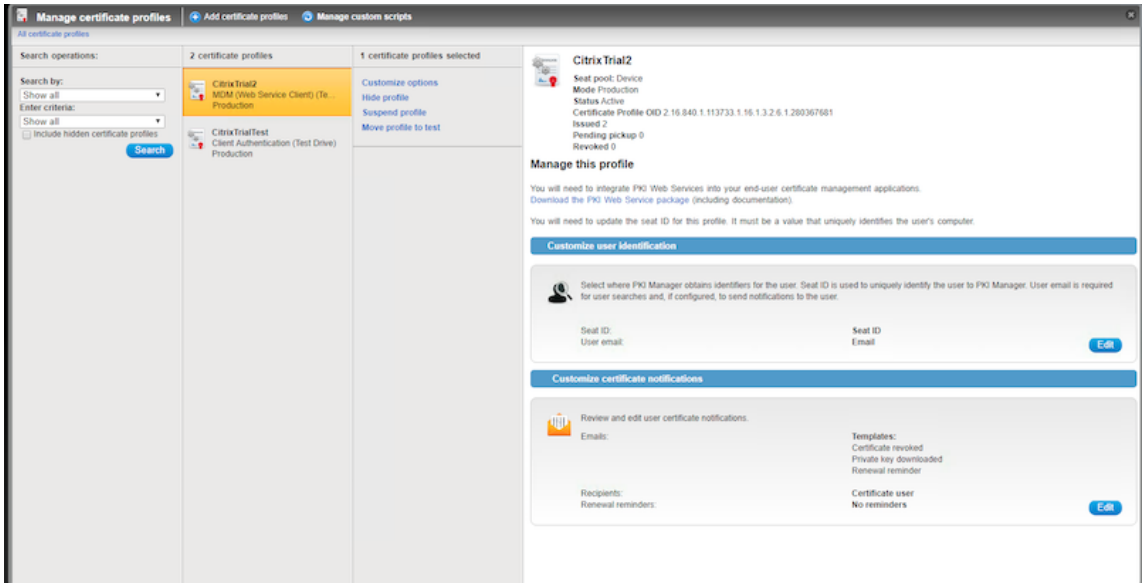


5. Vergewissern Sie sich auf der Seite **Einstellungen > PKI-Entitäten**, dass die von Ihnen hinzugefügte PKI-Entität als **Status** die Option **Gültig** zeigt.



Erstellen eines Anmeldeinformationsanbieters für DigiCert Managed PKI

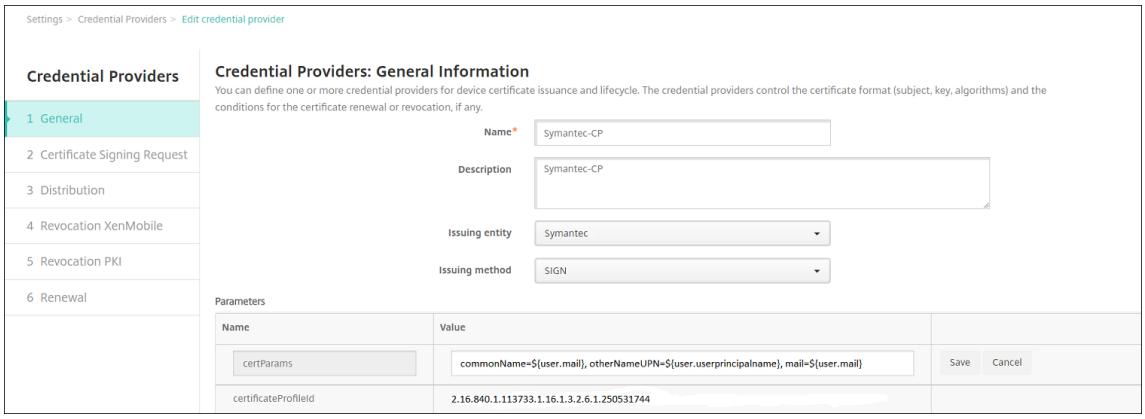
1. Kopieren Sie in der DigiCert PKI Manager-Konsole die **Zertifikatprofil-OID** aus der Zertifikatvorlage.



2. Klicken Sie in der XenMobile Server-Konsole unter **Einstellungen > Anmeldeinformationsanbieter** auf **Hinzufügen** und konfigurieren Sie die Einstellungen wie nachfolgend beschrieben.

   - **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, wenn Sie künftig Details über den Anmeldeinformationsanbieter benötigen.
   - **Ausstellende Entität:** Wählen Sie die ausstellende Entität.
   - **Ausstellungsmethode:** Wählen Sie **Zertifikat signieren** als Methode für den Bezug von Zertifikaten von der konfigurierten Entität.
   - **certParams:** Fügen Sie den folgenden Wert hinzu: **commonName=${user.mail},otherNameUPN=${u**

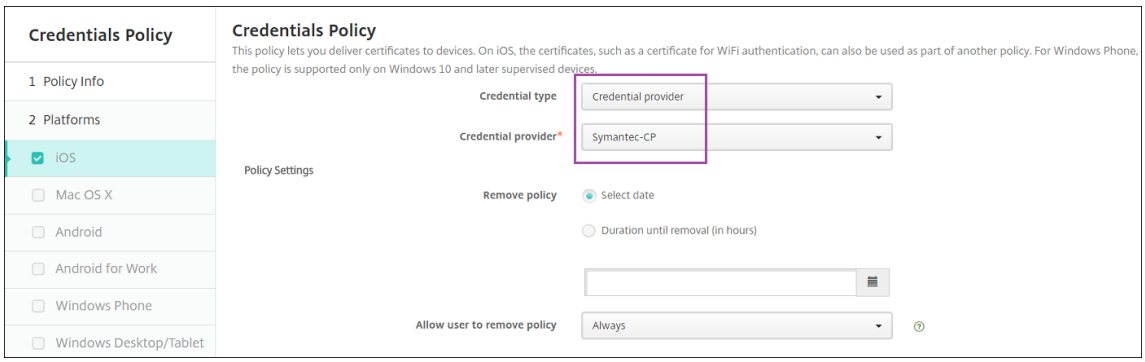
- **certificateProfileid:** Fügen Sie die in Schritt 1 kopierte Zertifikatprofil-OID ein.



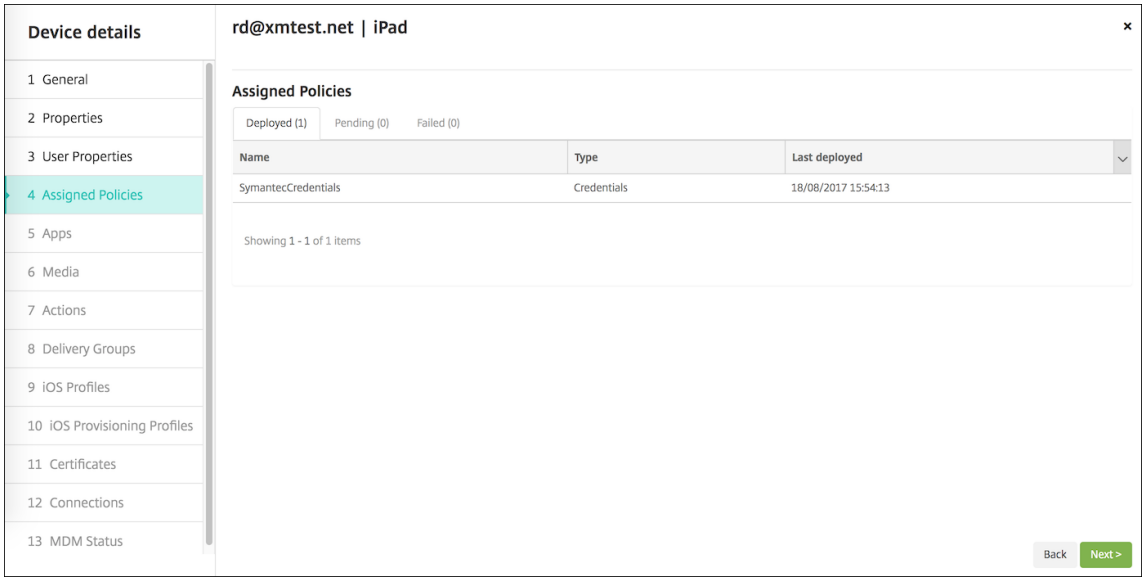
3. Klicken Sie auf **Weiter**. Akzeptieren Sie auf den verbleibenden Seiten (bis “Verlängerung”) die Standardeinstellungen. Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Testen der Konfiguration und Problembehandlung

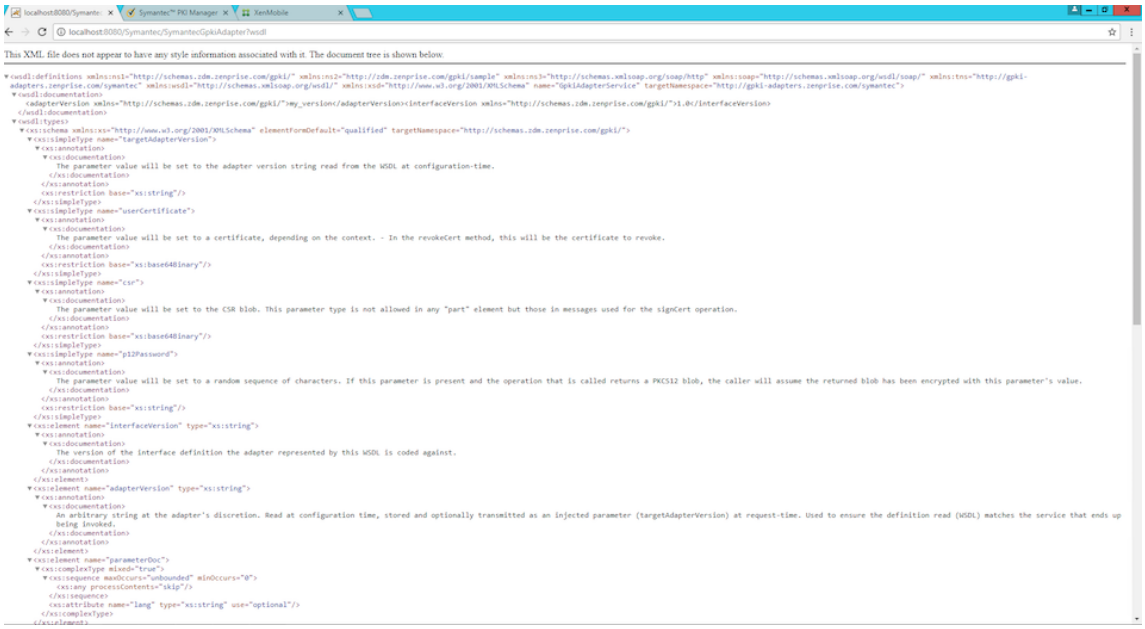
1. Erstellen Sie eine Anmeldeinformationsrichtlinie: Klicken Sie unter **Konfigurieren > Geräterichtlinien** auf **Hinzufügen**. Beginnen Sie mit der Eingabe von **Anmeldeinformationen** und klicken Sie dann auf **Anmeldeinformationen**.
2. Geben Sie einen **Richtliniennamen** ein.
3. Konfigurieren Sie die Plattformeinstellungen wie folgt:
   - **Anmeldeinformationstyp:** Wählen Sie **Anmeldeinformationsanbieter**.
   - **Anmeldeinformationsanbieter:** Wählen Sie den DigiCert-Anbieter.



4. Wenn Sie mit der Plattformeinstellung fertig sind, weisen Sie die Richtlinie auf der Seite **Zuweisung** Bereitstellungsgruppen zu und klicken Sie auf **Speichern**.
5. Um zu prüfen, ob die Richtlinie auf Geräten bereitgestellt wurde, wählen Sie auf der Seite **Verwalten > Geräte** ein Gerät, klicken Sie auf **Bearbeiten** und klicken Sie dann auf **Zugewiesene Richtlinien**. Das folgende Beispiel zeigt eine erfolgreiche Bereitstellung.



Wenn die Richtlinie nicht bereitgestellt wurde, melden Sie sich bei Windows Server an und überprüfen Sie, ob die WSDL ordnungsgemäß geladen wird.



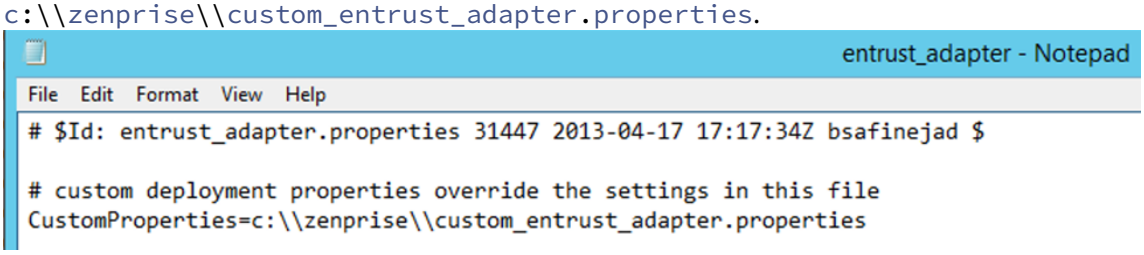
Zur weiteren Problembehandlung prüfen Sie die Tomcat-Protokolle unter `<tomcat dir>\logs\catalina.<current date>`.

Entrust PKI-Adapter

Anstelle der DigiCert Managed PKI können Sie auch den Entrust PKI-Adapter installieren. Lesen Sie vor der Installation des Adapters die Schritte zum Installieren von Java und Apache Tomcat unter Windows Server im Abschnitt DigiCert-verwaltete PKI dieses Artikels.

Installieren des Entrust PKI-Adapters

1. Laden Sie die Entrust PKI Adapter-Datei herunter:
   a) Gehen Sie zu https://www.citrix.com/downloads.
   b) Navigieren Sie zu **Citrix Endpoint Management (und Citrix XenMobile Server) > XenMobile Server > Product Software > XenMobile Server 10 > Tools**.
   c) Klicken Sie auf der Kachel **Entrust PKI Adapter** auf **Download File**.
   d) Extrahieren Sie die Datei entrust.war aus der heruntergeladenen ZIP-Datei und speichern Sie sie im Verzeichnis C:\Programme(x86)\Apache Software Foundation\Tomcat 8.5\webapps.
2. Bearbeiten Sie unter C:\Programme (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes die Datei entrust_adapter.properties und definieren Sie CustomProperties als `c:\\zenprise\\custom_entrust_adapter.properties`.



3. Erstellen Sie auf dem Laufwerk C: ein Zenprise-Verzeichnis und eine neue Datei namens custom_entrust_adapter.properties.
4. Bearbeiten Sie die Datei mit dem folgenden Inhalt. Achten Sie darauf, Entrust.MdmSvc.URL, AdminUserId und AdminPassword entsprechend zu ersetzen.

   ~

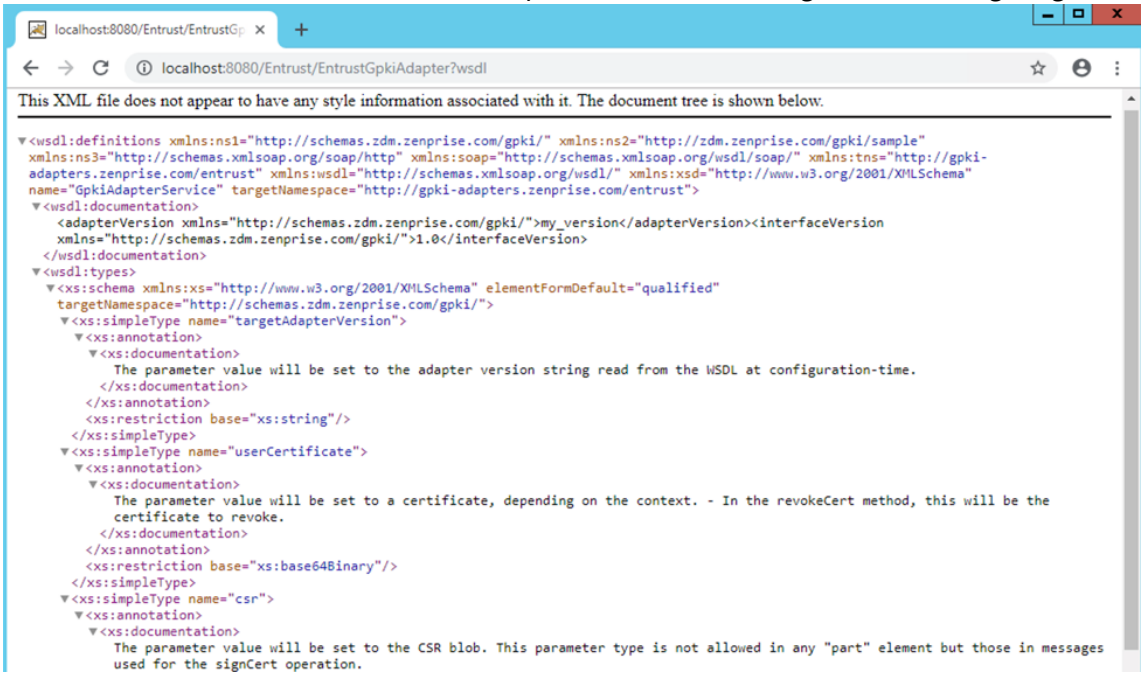
   # geben Sie hier die richtige URL ein für AS/IG
   Entrust.MdmSvc.Url=https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8

```
# set to 1 or true to force user creation from passed user and
    group parameters if using IG and user does not exist
CreateUser=

# set the credentials for the endpoint
AdminUserId=`[User ID]`
AdminPassword=`[password]`


# keystore for client-cert auth
#keyStore=
#keyStorePassword=
#keyStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and .
    jks files
```



```
13
14 # truststore for server with self-signed root CA
15 #trustStore=
16 #trustStorePassword=
17 #trustStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and
       .jks files
18 ~
```

5. Starten Sie den Tomcat-Dienst neu. Navigieren Sie zu C:\Programme (x86)\Apache Software Foundation\Tomcat 8.5\logs und öffnen Sie Catalina_201x-MM-DD.log. Vergewissern Sie sich, dass keine Fehler vorliegen und dass die folgende Zeile angezeigt wird:
   `13-Nov-2018 09:02:35.319 INFO [localhost-startStop-1] org.apache.cxf.endpoint.ServerImpl.initDestination Setting the server's publish address to be /EntrustGpkiAdapter`
6. Navigieren Sie zu `http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl` oder zur öffentlichen URL Ihres Servers, und überprüfen Sie, ob die richtige XML-Datei angezeigt wird.



Konfigurieren von XenMobile für den Entrust-PKI-Adapter

1. Melden Sie sich an der XenMobile-Konsole an und navigieren Sie zu **Einstellungen > PKI-Entitäten**. Klicken Sie auf **Hinzufügen > Generic PKI-Entität**.
2. Geben Sie die folgenden Informationen ein:
   - **Name:** Geben Sie einen Namen für die PKI-Entität ein.
   - **WSDL-URL:** Geben Sie die öffentliche URL Ihres Servers ein.

- **Authentifizierungstyp:** Wählen Sie 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.
- **Ressourcenstandort:** Wählen Sie **Eigener Ressourcenstandort**.
- **Zulässige relative Pfade:** Geben Sie ein: `/Entrust/*`.

3. Nach dem Konfigurieren der PKI-Entität kehren Sie zur Seite **Einstellungen** zurück und fügen einen **Anmeldeinformationsanbieter** hinzu.
4. Wählen Sie auf der Registerkarte **Allgemein** Ihre Entrust-Entität als **Ausstellende Entität** und **SIGNIEREN** als **Ausstellungsmethode** aus.
5. Konfigurieren Sie auf der Registerkarte **Zertifikatsignieranforderung** folgende Einstellungen:
   - **Schlüsselalgorithmus: RSA**
   - **Schlüsselgröße:** 2048
   - **Signaturalgorithmus: SHA256withRSA**
   - **Antragstellername:** cd=$user.username
   - **Alternative Antragstellernamen:** Optional. Wir empfehlen Folgendes:
     - **Typ: Benutzerprinzipalname**
     - **Wert:** $user.userprincipalname

     > **Hinweis:**
     > Wenn Sie eine Einstellung auf dem Adapter ändern, passen Sie die Konfiguration des Anmeldeinformationsanbieters mit der folgenden Schrittfolge an.
6. Nach der Konfiguration des Anmeldeinformationsanbieters navigieren Sie zu **Konfigurieren > Geräterichtlinien** und fügen eine Anmeldeinformationsrichtlinie hinzu.
7. Konfigurieren Sie die Richtlinie für die Betriebssysteme, die Sie verwenden möchten. Wählen Sie auf den Konfigurationsseiten der einzelnen Betriebssysteme unter **Anmeldeinformationstyp** die Option **Anmeldeinformationsanbieter**. Wählen Sie im Menü für **Anmeldeinformationen** den zuvor konfigurierten Anmeldeinformationsanbieter.

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). Wenn die Microsoft-ZS ein Citrix Gateway-Benutzerzertifikat erstellt, unterstützt Citrix Gateway Verlängerung und Sperrung für diese Zertifikate.

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

der Webschnittstelle für die Zertifikatdienste.

Hinzufügen einer Microsoft-Zertifikatdiensteentität

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben und dann auf **PKI-Entitäten**.
2. Klicken Sie auf der Seite **PKI-Entitäten** auf **Hinzufügen**.

   Ein Menü der PKI-Entitätstypen wird angezeigt.
3. Klicken Sie auf **Microsoft Zertifikatdiensteentität**.

   Die Seite **Microsoft Zertifikatdiensteentität: Allgemeine Informationen** wird angezeigt.
4. Konfigurieren Sie auf der Seite **Microsoft Zertifikatdiensteentität: Allgemeine Informationen** folgende Einstellungen:

   - **Name:** Geben Sie einen Namen für die neue Entität ein. Der Name von Entitäten muss eindeutig sein.
   - **Stamm-URL des Webregistrierungsdiensts:** Geben Sie die Stamm-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:** Wählen Sie 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 **Verbindung testen** um sicherzustellen, dass der Server erreichbar ist. Andernfalls wird eine Meldung angezeigt, dass die Verbindung fehlgeschlagen ist. Überprüfen Sie die Konfigurationseinstellungen.
6. 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.

7. 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.
8. 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. Benutzerdefinierte Parameter sind nur für angepasste Skripts nützlich, die auf der Zertifizierungsstelle ausgeführt werden.
9. 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 für XenMobile die Signierer der Zertifikate angeben, die das System über diese Entität erhält. Wenn das ZS-Zertifikat erneuert wurde, aktualisieren Sie es in XenMobile. XenMobile wendet die Änderung transparent auf die Entität an.
10. Wählen Sie auf der Seite **Microsoft Zertifikatdiensteentität: ZS-Zertifikate** die Zertifikate aus, die Sie für die Entität verwenden möchten.
11. Klicken Sie auf **Speichern**.

    Die Entität wird in der Tabelle der PKI-Entitäten angezeigt.

Citrix ADC-Zertifikatsperrliste

XenMobile unterstützt Zertifikatsperrlisten (CRL) nur für Drittanbieterzertifizierungsstellen. Wenn Sie eine Microsoft-Zertifizierungsstelle konfiguriert haben, wird in XenMobile zum Verwalten der Zertifikatsperre Citrix ADC verwendet.

Bedenken Sie beim Konfigurieren der Clientzertifikatauthentifizierung, ob Sie die Citrix ADC-Einstellung für Zertifikatsperrlisten (CRL) **Enable CRL Auto Refresh** konfigurieren. Dadurch wird sichergestellt, dass Benutzer von Geräten im ausschließlichen MAM-Modus keine Authentifizierung mit einem existierenden Zertifikat am Gerät durchführen können.

XenMobile stellt ein neues Zertifikat aus, da es Benutzer nicht daran hindert, ein Benutzerzertifikat zu generieren, nachdem eines gesperrt wurde. 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 ZS aktivieren. Wird die OCSP-Unterstützung aktiviert, fügt die Zertifizierungsstelle den von ihr ausgestellten Zertifikaten die Erweiterung `id-pe-authorityInfoAccess` hinzu. Die Erweiterung verweist auf die XenMobile-internen OCSP-Responder im folgenden Verzeichnis:

```
https://<server>/<instance>/ocsp
```

Wenn Sie den OCSP-Dienst konfigurieren, müssen Sie ein OCSP-Signaturzertifikat für die eigenverwaltete Entität angeben. Sie können das Zertifizierungsstellenzertifikat selbst als Signaturzertifikat verwenden. Um eine unnötige Offenlegung des privaten Schlüssels Ihrer Zertifizierungsstelle zu vermeiden (dies wird empfohlen), erstellen Sie ein von der eigenverwalteten Zertifizierungsstelle signiertes Delegate-OCSP-Signaturzertifikat und schließen Sie folgende Erweiterung ein: `id-kp-OCSPSigning extendedKeyUsage`.

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**.

   Ein Menü der PKI-Entitätstypen wird angezeigt.
3. Klicken Sie auf **Eigenverwaltete ZS**.

   Die Seite **Eigenverwaltete ZS: Allgemeine Informationen** wird angezeigt.
4. Führen Sie auf der Seite **Eigenverwaltete ZS: Allgemeine Informationen** 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** in XenMobile 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 der Erweiterung `keyUsage keyEncryption` sowie ein RA-Signaturzertifikat mit der Erweiterung `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 die Erweiterung `AuthorityInfoAccess` (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

January 5, 2022

Anmeldeinformationsanbieter sind die Zertifikatkonfigurationen, die Sie in den verschiedenen Teilen des XenMobile-Systems verwenden. Anmeldeinformationsanbieter definieren die Quellen, Parameter und Lebenszyklen von Zertifikaten. Die entsprechenden Vorgänge finden unabhängig davon statt, ob Zertifikate Teil der Gerätekonfiguration oder eigenständig sind (d. h. per Push auf Geräte übertragen 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 Erneuerungseinstellungen von D, wenn C aktualisiert wird. Die Sperreinstellungen für D gelten, wenn C gelöscht oder wenn D widerrufen wird.

Dies bedeutet, dass der Anmeldeinformationsanbieter in XenMobile Folgendes bestimmt:

- Die Quelle für Zertifikate.

- Die Methode des Bezugs von Zertifikaten: Signieren eines neuen Zertifikats oder Abruf (Wiederherstellung) eines vorhandenen Zertifikat-/Schlüsselpaars.
- Die Parameter für die Ausstellung/Wiederherstellung von Zertifikaten. Beispielsweise CSR-Parameter wie Schlüssellänge, Schlüsselalgorithmus und Zertifikaterweiterungen.
- Die Art und Weise, in der Zertifikate auf Geräten bereitgestellt werden.
- Die Sperrbedingungen. Zwar werden alle Zertifikate bei Beenden der Verwaltungsbeziehung in XenMobile gesperrt, durch die Konfiguration kann jedoch auch eine frühere Sperrung festgelegt sein. Zum Beispiel kann die Konfiguration festlegen, dass ein Zertifikat widerrufen wird, wenn die zugehörige Gerätekonfiguration gelöscht wird. Außerdem kann unter bestimmten Bedingungen die Sperrung eines Zertifikats in XenMobile an die Back-End-PKI (Public Key-Infrastruktur) gesendet werden. Das bedeutet, dass die Zertifikatsperrung in XenMobile eine Zertifikatssperrung in der PKI verursachen kann.
- Erneuerungseinstellungen Zertifikate, die über einen bestimmten Anmeldeinformationsanbieter bezogen werden, können automatisch erneuert werden, wenn sie kurz vor dem Ablauf stehen. Unabhängig davon können Benachrichtigungen ausgegeben werden, wenn sich das Ablaufdatum nähert.

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

Methoden der Zertifikatausstellung

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

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

Ein Anmeldeinformationsanbieter verwendet 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 bestimmten 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 des SCEP-Protokolls als Delegate (erweiterte Registrierungsstelle) für die tatsächliche Zertifizierungsstelle fungiert. XenMobile muss dem Client nachweisen, dass die Berechtigung hierzu vorliegt. Diese Berechtigung ist durch das Hochladen 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 laden Sie die Zertifikate in XenMobile hoch und verknüpfen sie mit dem Anmeldeinformationsanbieter.

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
Registrierung von Windows Phone und Tablet	Nein	Nein

Kontext	SCEP unterstützt	SCEP erforderlich
Konfiguration von Windows Phone und Tablet	Nein, mit Ausnahme der Wi-Fi-Richtlinie, die für Windows Phone 8.1, Windows 10 und Windows 11 unterstützt wird	Nein

Zertifikatsperre

Es gibt drei Arten der Sperre.

- **Interne Sperre** Die interne Sperre wirkt sich auf den von XenMobile gepflegten Zertifikatstatus aus. XenMobile berücksichtigt diesen Status beim Bewerten eines vorgelegten Zertifikats und beim Bereitstellen von OCSP-Statusinformationen für ein Zertifikat. Die Konfiguration des Anmeldeinformationsanbieters bestimmt, wie sich diverse Bedingungen auf diesen Status auswirken. Beispielsweise kann durch den Anmeldeinformationsanbieter festgelegt sein, dass 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 unter den in der Konfiguration des Anmeldeinformationsanbieters festgelegten Bedingungen intern von XenMobile gesperrt wird. 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.

Diese drei Arten schließen einander nicht aus, sondern ergänzen einander. Eine externe Sperre kann eine interne Sperre zur Folge haben. Eine interne Sperre wirkt sich möglicherweise auf eine externe Sperre aus.

Zertifikaterneuerung

Eine Zertifikaterneuerung besteht aus der Sperre des bestehenden Zertifikats und der Ausstellung eines neuen Zertifikats.

In XenMobile wird vor Sperrung des vorhandenen Zertifikats versucht, das neue Zertifikat abzurufen, um eine Dienstunterbrechung zu vermeiden, wenn die Ausstellung fehlschlägt. Bei verteilter (SCEP-gestützter) Bereitstellung erfolgt die Sperrung auch erst, wenn das Zertifikat erfolgreich auf einem

Gerät installiert wurde. Andernfalls erfolgt die Sperrung, bevor das neue Zertifikat an das Gerät gesendet wird. Die Sperrung ist unabhängig vom Erfolg oder Fehlschlagen der Zertifikatinstallation.

Die Sperrungskonfiguration erfordert die Angabe eines bestimmten Zeitraums (in Tagen). Wenn ein Gerät eine Verbindung herstellt, wird vom Server geprüft, ob das `NotAfter`-Datum für das Zertifikat nach dem aktuellen Datum minus dem angegebenen Zeitraum liegt. Wenn das Zertifikat diese Bedingung erfüllt, versucht XenMobile, das Zertifikat zu erneuern.

Erstellen eines Anmeldeinformationsanbieters

Die Schritte beim Konfigurieren eines Anmeldeinformationsanbieters variieren hauptsächlich nach ausgewählter ausstellender Entität und Ausstellungsmethode. Sie können zwischen Anmeldeinformationsanbietern unterscheiden, die eine interne oder eine externe Entität verwenden:

- Eigenverwaltete, XenMobile-interne Entitäten sind interne Entitäten. Die Ausstellungsmethode bei eigenverwalteten Zertifizierungsstellen ist immer “sign”. Das bedeutet, dass bei jeder Ausstellung von XenMobile ein neues Schlüsselpaar mit dem für die Entität ausgewählten ZS-Zertifikat signiert wird. Ob das Schlüsselpaar auf dem Gerät oder auf dem Server generiert wird, hängt von der ausgewählten Verteilungsmethode ab.
- Zu den externen Entitäten, die Teil der Unternehmensinfrastruktur sind, gehören die Microsoft-Zertifizierungsstelle und GPKIs.

Detaillierte Informationen zum Einrichten von DigiCert Managed PKI einschließlich Erstellung des Anmeldeinformationsanbieters finden Sie unter “DigiCert-verwaltete PKI” in PKI-Entitäten.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben und dann auf **Einstellungen > Anbieter für Anmeldeinformationen**.
2. Klicken Sie auf der Seite **Anbieter für Anmeldeinfo** auf **Hinzufügen**.

   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. Das ist zwar ein optionales Feld, eine Beschreibung kann jedoch nützliche Details über den Anmeldeinformationsanbieter bieten.
   - **Ausstellende Entität:** Klicken Sie auf die ausstellende Entität.

- **Ausstellungsmethode:** Klicken Sie auf **Zertifikat signieren** oder **Zertifikat abrufen**, um die Methode auszuwählen, die für den Bezug von Zertifikaten von der konfigurierten Entität verwendet werden soll. Verwenden Sie für die Clientzertifikatauthentifizierung **Zertifikat signieren**.
- Wenn die **Vorlagenliste** verfügbar ist, wählen Sie die Vorlage aus, die Sie für den Anmeldeinformationsanbieter unter der PKI-Entität hinzugefügt haben.

  Die Vorlagen werden verfügbar, wenn Entitäten der Microsoft-Zertifikatdienste über **Einstellungen > PKI-Entitäten** hinzugefügt werden.

4. Klicken Sie auf **Weiter**.

   Die Seite **Anbieter für Anmeldeinformationen: Zertifikatsignieranforderung** wird angezeigt.

5. Konfigurieren Sie auf der Seite **Anmeldeinformationsanbieter: Zertifikatsignieranforderung** die folgenden Einstellungen gemäß Ihrer Zertifikatkonfiguration:

   - **Schlüsselalgorithmus:** Wählen Sie den Schlüsselalgorithmus für das neue Schlüsselpaar. Verfügbare Werte sind **RSA**, **DSA** und **ECDSA**.
   - **Schlüsselgröße:** Geben Sie die Länge des Schlüsselpaars in Bit ein. Diese Angabe ist erforderlich.

     Die zulässigen Werte sind abhängig vom Schlüsseltyp. Die maximale Länge für DSA-Schlüssel beträgt beispielsweise 1024 Bit. Zur Vermeidung falscher Negative, die von der verwendeten Hardware oder Software abhängig sind, erzwingt XenMobile keine Schlüssellängen. Testen Sie Anmeldeinformationsanbieter vor Übernahme in die Produktionsumgebung immer in einer Testumgebung.
   - **Signaturalgorithmus:** Klicken Sie auf einen Wert für das neue Zertifikat. Welche Werte zulässig sind, hängt vom Schlüsselalgorithmus ab.
   - **Antragstellername:** erforderlich. Geben Sie den Distinguished Name des Antragstellers für das neue Zertifikat ein. Beispiel: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \endquotation`

     Verwenden Sie für die Clientzertifikatauthentifizierung beispielsweise die folgenden Einstellungen:

     - **Schlüsselalgorithmus:** RSA
     - **Schlüsselgröße:** 2048
     - **Signaturalgorithmus:** SHA256withRSA
     - **Antragsstellername:** `cn=$user.username`
   - Zum Hinzufügen eines Eintrags zur Tabelle **Alternative Antragsstellernamen** 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`

  Wie beim Antragstellernamen können Sie im Wertefeld XenMobile-Makros verwenden.

6. Klicken Sie auf **Weiter**.

   Die Seite **Anbieter für Anmeldeinformationen: Verteilung** wird angezeigt.

7. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: Verteilung** folgende Schritte aus:

   - Klicken Sie in der Liste **Zertifikat der ausstellenden ZS** auf das angebotene ZS-Zertifikat. Da der Anmeldeinformationsanbieter eine eigenverwaltete Zertifizierungsstelle verwendet, erhält er immer das für die Entität selbst konfigurierte ZS-Zertifikat. Die Aufführung hier erfolgt aus Gründen der Konsistenz mit Konfigurationen, in denen externe Entitäten verwendet werden
   - Wählen Sie für **Verteilungsmodus wählen** eine der folgenden Methoden zum Generieren und Verteilen von Schlüsseln aus:
     - **Bevorzugt zentralisiert: Schlüssel serverseitig generieren:** Citrix empfiehlt diese Option. Sie unterstützt alle von XenMobile unterstützten Plattformen und ist erforderlich, wenn die Citrix 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.

8. Klicken Sie auf **Weiter**.

   Die Seite **Anbieter für Anmeldeinformationen: XenMobile-Sperrung** wird angezeigt. Auf dieser Seite konfigurieren Sie die Bedingungen, unter denen XenMobile Zertifikate, die über diese Anbieterkonfiguration ausgestellt wurden, intern als gesperrt kennzeichnet.

9. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: XenMobile-Sperrung** folgende Schritte aus:

   - Wählen Sie für **Ausgestellte Zertifikate widerrufen** eine der Optionen zur Angabe des Zeitpunkts aus, an dem Zertifikate gesperrt werden sollen.
   - Soll XenMobile eine Benachrichtigung bei Sperrung des Zertifikats senden, 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 Entity ausgewählte PKI gesendet.

10. Klicken Sie auf **Weiter**.

    Die Seite **Anbieter für Anmeldeinformationen: PKI-Sperrung** wird 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.

11. 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 **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.

      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 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.

12. Klicken Sie auf **Weiter**.

    Die Seite **Anbieter für Anmeldeinformationen: Verlängerung** wird angezeigt. Auf dieser Seite können Sie für XenMobile die Ausführung folgender Schritte festlegen:

    - Zertifikat erneuern. Sie können optional bei Erneuerung des Zertifikats eine entsprechende Benachrichtigung senden und optional bereits abgelaufene Zertifikate von diesem Vorgang ausschließen.
    - Versand einer Benachrichtigung für Zertifikate, deren Ablauf kurz bevorsteht

13. Gehen Sie auf der Seite **Anbieter für Anmeldeinformationen: Verlängerung** folgendermaßen vor, um Zertifikate bei Ablauf zu verlängern:

    Legen Sie für **Zertifikate erneuern, wenn sie ablaufen** die Option **Ein** fest. Weitere Felder werden angezeigt.

    - Geben Sie im Feld **Zertifikat erneuern, wenn es in** die Zeit vor Ablauf des Zertifikats in Tagen ein, zu der die Erneuerung erfolgen soll.
    - Wählen Sie optional **Bereits abgelaufene Zertifikate nicht erneuern** aus. In diesem Zusammenhang bedeutet “bereits abgelaufen”, dass das `NotAfter`-Datum in der Vergangenheit liegt, und nicht, dass das Zertifikat gesperrt wurde. XenMobile erneuert keine Zertifikate, nachdem sie intern gesperrt wurden.

    Wenn XenMobile eine Benachrichtigung bei Verlängerung des Zertifikats senden soll, legen Sie **Benachrichtigung senden** auf **Ein** fest. Wenn XenMobile eine Benachrichtigung bei anstehendem Ablauf des Zertifikats senden soll, legen Sie **Benachrichtigen, wenn Zertifikat bald abläuft** auf **Ein** fest.
    Sie können für beide Einstellungen eine von zwei Benachrichtigungsoptionen auswählen:

    - **Benachrichtigungsvorlage wählen:** Wählen Sie einen vorhandenen Benachrichtigungstext aus und passen Sie ihn ggf. an. Die entsprechenden Vorlagen sind in der Liste Benachrichtigungsvorlage.
    - **Geben Sie die Benachrichtigungsdetails ein:** Geben Sie einen eigenen Text ein. Geben Sie die E-Mail-Adresse des Empfängers, eine Nachricht und die Häufigkeit für das Senden

der Benachrichtigung an.

Geben Sie im Feld **Benachrichtigung bei Zertifikatablauf in** die Zeit vor Ablauf des Zertifikats in Tagen ein, zu der die Benachrichtigung gesendet werden soll.

14. Klicken Sie auf **Speichern**.

    Der neue Anbieter wird in der Tabelle der Anmeldeinformationsanbieter angezeigt.

APNs-Zertifikate

January 5, 2022

> **Wichtig:**
>
> Apple stellt die Unterstützung für das Legacy-APNs-Binärprotokoll am 31. März 2021 ein. Apple empfiehlt, stattdessen die Verwendung der HTTP/2-basierten APNS-Anbieter-API zu verwenden. Ab Version 10.13.0 unterstützt XenMobile Server die HTTP/2-basierte API. Weitere Informationen finden Sie unter "Apple Push Notification Service Update" auf https://developer.apple.com/. Informationen zum Überprüfen der Konnektivität zu APNs finden Sie unter Konnektivitätsprüfungen.

Zum Registrieren und Verwalten von iOS- und macOS-Geräten mit XenMobile müssen Sie ein Zertifikat von Apple für den Apple-Dienst für Push-Benachrichtigungen (Apple Push Notification service, APNs) einrichten.

Workflowzusammenfassung:

- **Schritt 1:** Erstellen einer Zertifikatsignieranforderung (CSR) mit einer der folgenden Methoden:
  - Erstellen einer Zertifikatsignieranforderung mit der Schlüsselbundverwaltung in macOS (empfohlen von Citrix)
  - Erstellen einer Zertifikatsignieranforderung mit Microsoft IIS
  - Erstellen einer Zertifikatsignieranforderung mit Open SSL
- **Schritt 2:** Signieren der CSR in XenMobile Tools
- **Schritt 3:** Übermitteln der signierten Zertifikatsignieranforderung an Apple für den Erhalt eines APNs-Zertifikats
- **Schritt 4:**Abschluss der Zertifikatsignieranforderung und Exportieren einer PKCS#12-Datei auf demselben Computer, der für Schritt 1 verwendet wurde:
  - Erstellen einer PKCS #12-Datei mit der Schlüsselbundverwaltung in macOS
  - Erstellen einer PKCS#12-Datei mit Microsoft IIS
  - Erstellen einer PKCS#12-Datei mit OpenSSL

- **Schritt 5:** Importieren eines APNs-Zertifikats in XenMobile
- **Schritt 6:** Erneuern eines APNs-Zertifikats

Erstellen einer Zertifikatsignieranforderung

Es wird empfohlen, eine Zertifikatsignieranforderung (CSR) mit der Schlüsselbundverwaltung in macOS zu erstellen. Sie können eine CSR auch mit Microsoft IIS oder OpenSSL erstellen.

> **Wichtig:**
>
> - Für die beim Erstellen des Zertifikats verwendete Apple-ID gilt:
>   - The Apple ID must be a corporate ID and not a personal ID.
>   - Record the Apple ID that you use to create the certificate.
>   - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device reenrollment.
> - 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 sämtliche Aktionen für die migrierten Zertifikate im Apple Push Certificates Portal ausführen.

Erstellen einer Zertifikatsignieranforderung mit der Schlüsselbundverwaltung in macOS

1. Starten Sie auf einem Computer mit macOS unter **Anwendungen > Dienstprogramme** die Schlüsselbundverwaltung (Keychain Access).
2. Klicken Sie im Menü **Keychain Access** auf **Certificate Assistant > Request a Certificate From a Certificate Authority**.
3. Der Zertifikatassistent fordert Sie zur Eingabe folgender Informationen auf:
   - **Email Address:** E-Mail-Adresse des Benutzer- bzw. Rollenkontos, das zum Verwalten des Zertifikats verwendet wird.
   - **Common Name:** allgemeiner Name des Benutzer- bzw. Rollenkontos, das zum Verwalten des Zertifikats verwendet wird.
   - **CA Email Address:** E-Mail-Adresse der Zertifizierungsstelle.
4. Wählen Sie **Saved to disk** und **Let me specify key pair information** und klicken Sie auf **Continue**.
5. Geben Sie einen Namen für die CSR-Datei ein, speichern Sie die Datei auf Ihrem Computer und klicken Sie dann auf **Save**.
6. 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.

7. Klicken Sie auf **Done**, wenn der Assistent den Prozess abgeschlossen hat.
8. Als Nächstes signieren Sie die Zertifikatsignieranforderung.

Erstellen einer Zertifikatsignieranforderung mit Microsoft IIS

Der erste Schritt zum Generieren einer APNs-Zertifikatanforderung ist das Erstellen einer Zertifikatsignieranforderung (Certificate Signing Request, CSR). Generieren Sie die CSR für Windows mit Microsoft IIS.

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 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 Dateinamen für die Zertifikatanforderung ein wählen Sie einen Speicherort aus und klicken Sie dann auf **Fertig stellen**.
7. Als Nächstes signieren Sie die Zertifikatsignieranforderung.

Erstellen einer Zertifikatsignieranforderung mit Open SSL

Wenn Sie kein macOS-Gerät oder Microsoft IIS zum Generieren einer Zertifikatsignieranforderung verwenden können, verwenden Sie OpenSSL. Sie können OpenSSL von der OpenSSL-Website herunterladen und installieren.

1. Führen Sie auf dem Computer, auf dem Sie OpenSSL installieren, 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.

   ```
   1 You are about to be asked to enter information that will be
        incorporated into your certificate request.
   2 What you are about to enter is what is called a Distinguished Name
        or a DN.
   3 There are quite a few fields but you can leave some blank
   4 For some fields there will be a default value,
   5 If you enter '.', the field will be left blank.
   6 -----
   7 Country Name (2 letter code) [AU]:US
   8 State or Province Name (full name) [Some-State]:CA
   ```



```
Locality Name (eg, city) []:RWC
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
    Customer
Organizational Unit Name (eg, section) [:Marketing
Common Name (eg, YOUR name) []:John Doe
Email Address []:john.doe@customer.com
<!--NeedCopy-->
```

3. Geben Sie bei der nächsten Meldung ein Kennwort für den privaten CSR-Schlüssel ein.

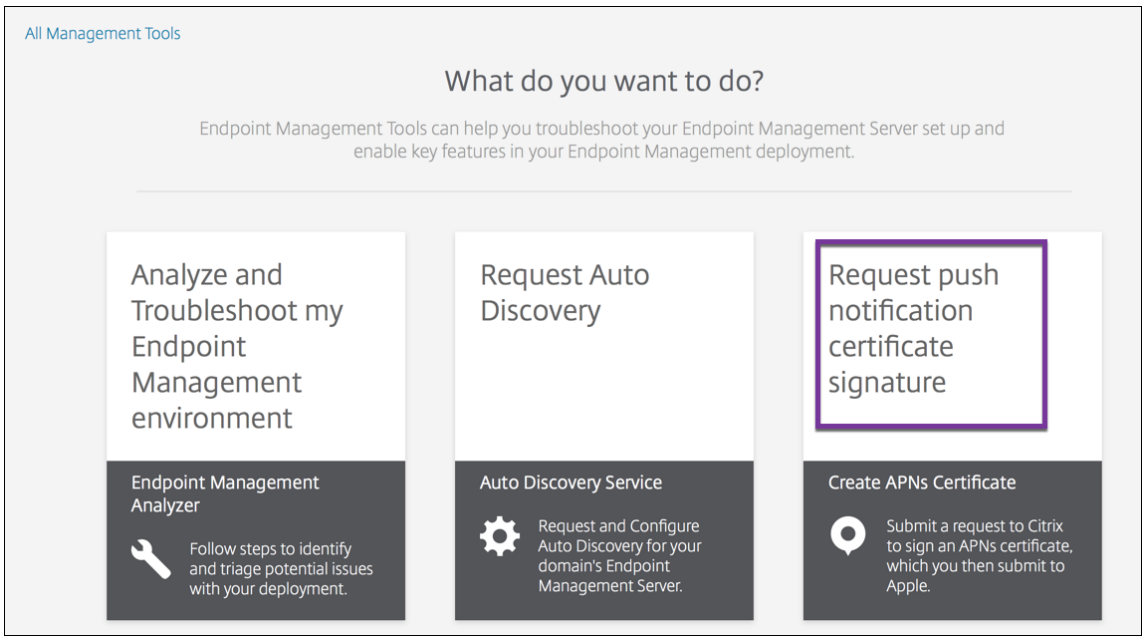
```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
<!--NeedCopy-->
```

4. Um fortzufahren, signieren Sie die Zertifikatsignieranforderung wie im nächsten Abschnitt beschrieben.

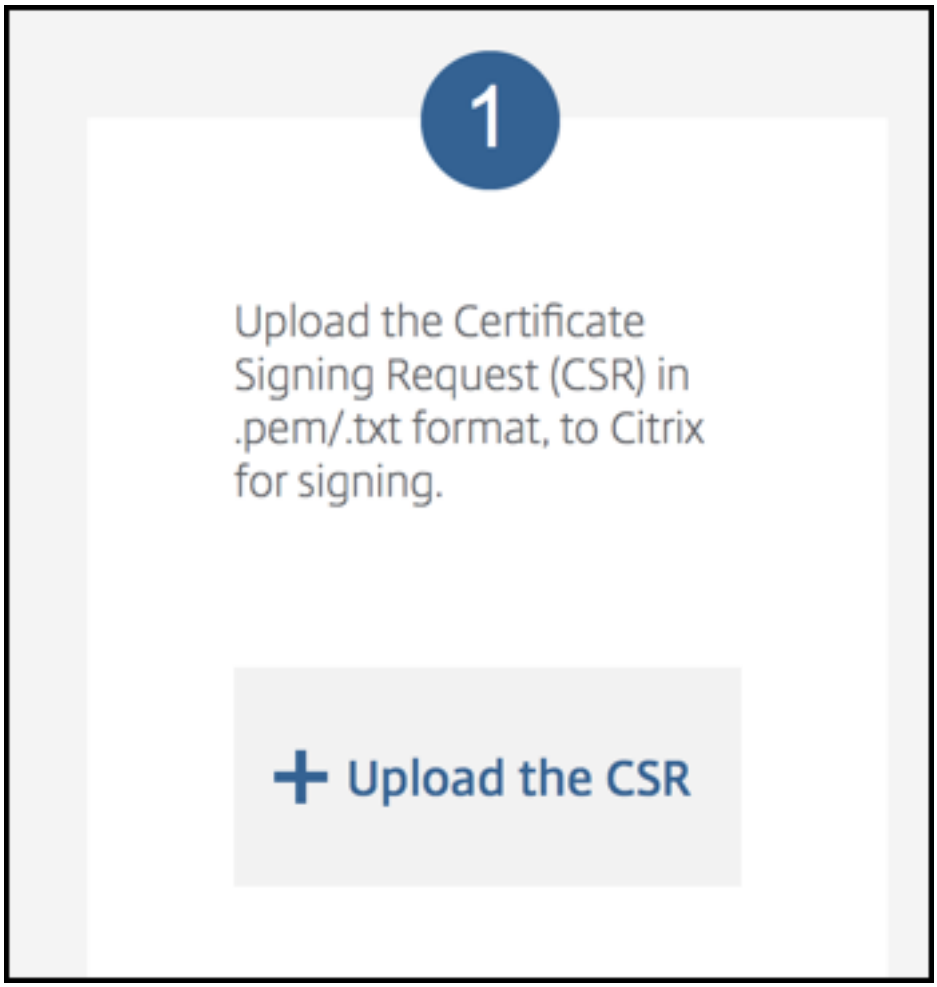
Signieren der Zertifikatsignieranforderung

Um ein Zertifikat mit XenMobile zu verwenden, übermitteln Sie es zum Signieren an Citrix. Citrix signiert die Zertifikatsignieranforderung mit seinem Zertifikat für die Mobilgeräteverwaltung und sendet die signierte Datei im `.plist`-Format zurück.

1. Wechseln Sie in Ihrem Browser zu der Website Endpoint Management Tools und klicken Sie dann auf **Request push notification certificate signature**.



2. Klicken Sie auf der Seite **Creating a new certificate** auf **Upload the CSR**.



3. Navigieren Sie zu dem Zertifikat und wählen Sie es aus.

   Das Zertifikat muss im PEM/TXT-Format vorliegen.

4. Klicken Sie auf der Seite **Endpoint Management APNs CSR Signing** auf **Sign**. Die CSR wird signiert und automatisch im konfigurierten Downloadordner gespeichert.
5. Um fortzufahren, übermitteln Sie die signierte CSR wie im nächsten Abschnitt beschrieben.

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

Nach Erhalt der signierten Zertifikatsignieranforderung (CSR) von Citrix senden Sie diese an Apple, um das APNs-Zertifikat zu erhalten, das Sie in XenMobile importieren müssen.

> **Hinweis:**
>
> Es gibt Berichte über Probleme mit der Anmeldung beim Apple Push Portal. Melden Sie sich

> alternativ beim Apple Developer Portal an und folgen Sie dann diesen Schritten.

1. Rufen Sie in einem Browser das Apple Push Certificates Portal 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**. Eine Bestätigungsmeldung zeigt an, dass der Upload erfolgreich war.
5. Klicken Sie auf **Download**, um das PEM-Zertifikat abzurufen.
6. Um fortzufahren, signieren Sie die Zertifikatsignieranforderung (CSR) und exportieren eine PKCS#12-Datei, wie im nächsten Abschnitt beschrieben.

Abschluss der Zertifikatsignieranforderung und Exportieren einer PKCS#12-Datei

Nach dem Erhalt des APNs-Zertifikats von Apple kehren Sie zu Keychain Access, Microsoft IIS oder OpenSSL zurück, um das Zertifikat in eine PCS#12-Datei zu exportieren.

Eine PKCS#12-Datei enthält die APNs-Zertifikatdatei und Ihren privaten Schlüssel. PFX-Dateien haben normalerweise die Erweiterung .pfx oder .p12. Sie können PFX- und P12-Dateien austauschbar verwenden.

> **Wichtig:**
>
> Citrix empfiehlt, die persönlichen und öffentlichen Schlüssel vom lokalen System zu speichern oder zu exportieren. Sie benötigen die Schlüssel, um auf die APNs-Zertifikate erneut zuzugreifen. Ohne dieselben Schlüssel ist Ihr Zertifikat ungültig, und Sie müssen den gesamten CSR- und APNs-Prozess wiederholen.

Erstellen einer PKCS #12-Datei mit der Schlüsselbundverwaltung in macOS

> **Wichtig:**
>
> Verwenden Sie für diese Aufgabe dasselbe macOS-Gerät, mit dem Sie die Zertifikatsignieranforderung erstellt haben.

1. Suchen Sie auf dem Gerät das Produktidentitätszertifikat (.pem), das Sie von Apple erhalten haben.
2. Starten Sie die Schlüsselbundverwaltung und navigieren Sie zur Registerkarte **Login > My Certificates**. Ziehen Sie das Produktidentitätszertifikat mit der Maus auf das geöffnete Fenster und legen Sie es dort ab.
3. Klicken Sie auf das Zertifikat und dann auf den Pfeil links, um zu überprüfen, ob das Zertifikat den zugehörigen privaten Schlüssel enthält.

4. Zum Exportieren des Zertifikats in das Format PCKS#12 (.pfx) wählen Sie das Zertifikat und den privaten Schlüssel, klicken mit der rechten Maustaste und wählen **Export 2 items**.
5. Geben Sie der Zertifikatdatei einen eindeutigen Namen für die Verwendung mit XenMobile. Verwenden Sie kein Leerzeichen im Namen. Wählen Sie einen Speicherort für das gespeicherte Zertifikat und 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. Die Schlüsselbundverwaltung fordert Sie zur Eingabe des Anmeldekennworts oder des ausgewählten Schlüsselbunds auf. Geben Sie das Kennwort ein und klicken Sie auf **OK**. Das gespeicherte Zertifikat kann nun in XenMobile Server verwendet werden.
8. Weitere Informationen finden Sie unter Importieren eines APNs-Zertifikats in XenMobile.

Erstellen einer PKCS#12-Datei mit Microsoft IIS

> **Wichtig:**
>
> Verwenden Sie für diese Aufgabe denselben IIS-Server, mit dem Sie die Zertifikatsignieranforderung erstellt haben.

1. Öffnen Sie Microsoft IIS.
2. Klicken Sie auf das **Serverzertifikatesymbol**.
3. Klicken Sie im Fenster **Server Certificates** auf **Complete Certificate Request**.
4. Navigieren Sie zu der Datei Certificate.pem von Apple. Geben Sie dann einen Anzeigenamen oder den Zertifikatnamen ein und klicken Sie auf **OK**. Verwenden Sie kein Leerzeichen im Namen.
5. Wählen Sie das in Schritt 4 identifizierte Zertifikat und klicken Sie auf **Export**.
6. Geben Sie einen Speicherort und einen Dateinamen für das PFX-Zertifikat sowie ein Kennwort ein und klicken Sie auf **OK**.

   Sie benötigen das Kennwort für das Zertifikat, um es in XenMobile zu importieren.
7. Kopieren Sie die PFX-Zertifikatdatei auf den Server, auf dem XenMobile installiert werden soll.
8. Weitere Informationen finden Sie unter Importieren eines APNs-Zertifikats in XenMobile.

Erstellen einer PKCS#12-Datei mit OpenSSL

Falls Sie eine Zertifikatsignieranforderung mit OpenSSL erstellen, können Sie damit auch ein APNs-Zertifikat im PFX-Format erstellen.

1. Führen Sie an einer Eingabeaufforderung oder Shell den nachfolgenden Befehl aus. `Customer.privatekey.pem` ist der private Schlüssel aus Ihrer CSR und `APNs_Certificate.pem` das von Apple erhaltene Zertifikat.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
   ```

2. Geben Sie ein Kennwort für die PFX-Datei ein. Merken Sie sich das Kennwort, denn Sie benötigen es wieder, wenn Sie das Zertifikat in XenMobile hochladen.
3. Notieren Sie den Speicherort der PFX-Zertifikatsdatei. Kopieren Sie dann die Datei auf den XenMobile-Server, damit Sie sie mit der Konsole hochladen können.
4. Um fortzufahren, importieren Sie wie im nächsten Abschnitt beschrieben ein APNs-Zertifikat in XenMobile.

Importieren eines APNs-Zertifikats in XenMobile

Nachdem Sie ein neues APNs-Zertifikat empfangen haben, importieren Sie das APNs-Zertifikat in XenMobile – entweder als erstes Zertifikat oder als Ersatz für ein bestehendes Zertifikat.

1. Gehen Sie in der XenMobile-Konsole zu **Einstellungen > Zertifikate**.
2. Klicken Sie auf **Importieren > Schlüsselspeicher**.
3. Wählen Sie unter **Verwenden als** die Option **APNs**.
4. Navigieren Sie zu der PFX- bzw. P12-Datei auf Ihrem Computer.
5. Geben Sie das Kennwort ein und klicken Sie auf **Importieren**.

Weitere Informationen über Zertifikate in XenMobile finden Sie unter Zertifikate und Authentifizierung.

Erneuern eines APNs-Zertifikats

> **Wichtig:**
>
> Wenn Sie zum Erneuern des Zertifikats eine andere Apple-ID verwenden, müssen Sie die Benutzergeräte neu registrieren.

Um ein APNs-Zertifikat zu erneuern, führen Sie die Schritte zum Erstellen eines Zertifikats aus und rufen dann das Apple Push Certificates Portal auf. Verwenden Sie dieses Portal, um das neue Zertifikat hochzuladen. Nach der Anmeldung wird Ihr vorhandenes Zertifikat oder ein aus Ihrem vorherigen Apple Developer-Konto importiertes Zertifikat angezeigt.

Im Portal besteht der einzige Unterschied beim Erneuern des Zertifikats darin, dass Sie auf **Renew** klicken. Sie müssen ein Developer-Konto für das Portal haben, um auf die Website zugreifen zu

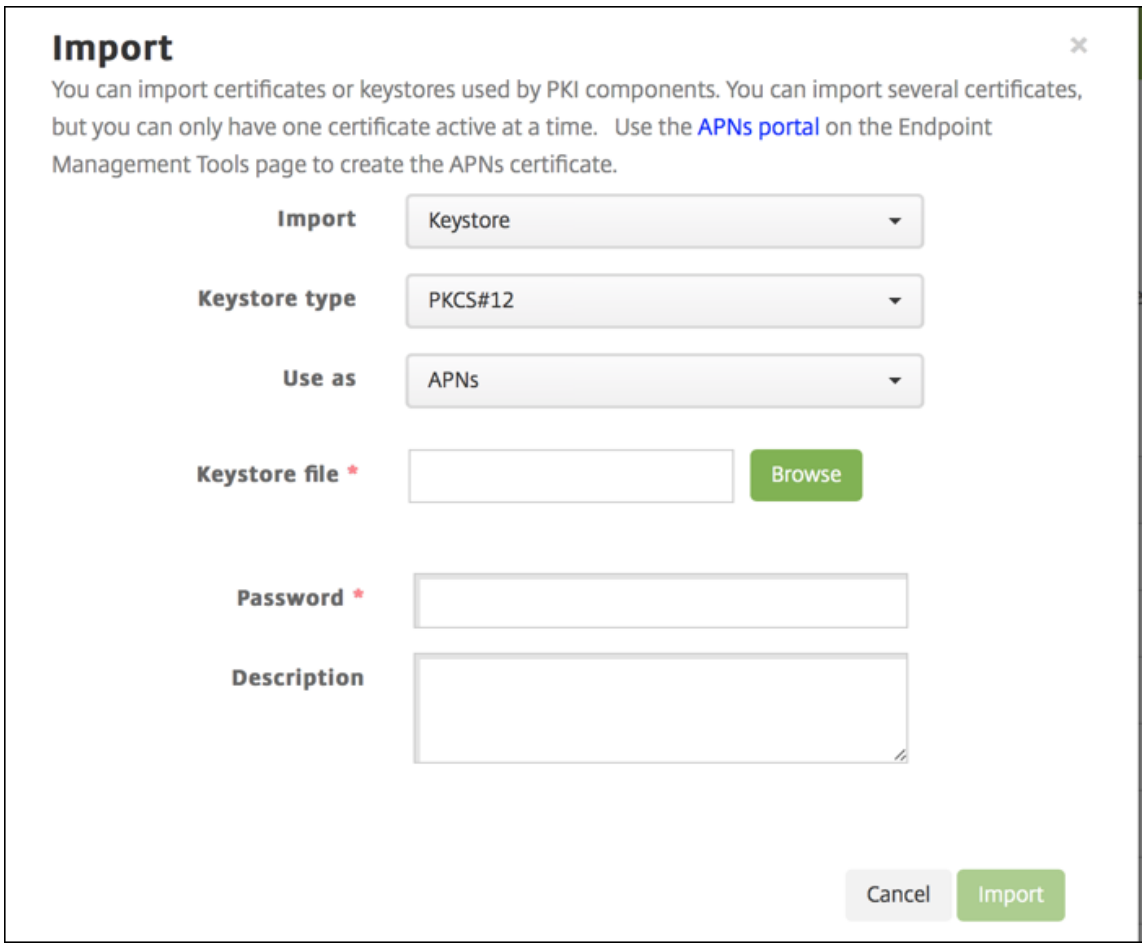
können. Verwenden Sie beim Erneuern des Zertifikats denselben Organisationsnamen und dieselbe Apple-ID.

Um herauszufinden, wann Ihr APNs-Zertifikat abläuft, gehen Sie in der XenMobile-Konsole zu **Konfigurieren > Einstellungen > Zertifikate**. Widerrufen Sie das Zertifikat nicht, falls es abläuft.

1. Generieren Sie eine Zertifikatsignieranforderung mit IIS (Microsoft), Keychain Access (macOS) oder OpenSSL. Weitere Informationen zum Generieren einer Zertifikatsignieranforderung finden Sie unter Erstellen einer Zertifikatsignieranforderung.
2. Gehen Sie in Ihrem Browser zu XenMobile Tools. Klicken Sie dann auf **Request push notification certificate signature**.
3. Klicken Sie auf **+ Upload the CSR**.
4. Navigieren Sie im Dialogfeld zur CSR, klicken Sie auf **Open** und dann auf **Sign**.
5. Wenn Sie eine `.plist`-Datei erhalten, speichern Sie sie.
6. Klicken Sie im Titel von Schritt 3 auf **Apple Push Certificates Portal** und melden Sie sich an.
7. Wählen Sie das zu erneuernde Zertifikat aus und klicken Sie auf **Renew**.
8. Laden Sie die `.plist`-Datei hoch. Sie erhalten dann eine PEM-Datei als Ausgabe. Speichern Sie die PEM-Datei.
9. Schließen Sie mithilfe der PEM-Datei die CSR ab (entsprechend der Methode, die Sie zum Erstellen der CSR in Schritt 1 verwendet haben).
10. Exportieren Sie das Zertifikat als PFX-Datei.

Importieren Sie die PFX-Datei in der XenMobile-Konsole und schließen Sie die Konfiguration wie folgt ab:

1. Gehen Sie zu **Einstellungen > Zertifikate > Importieren**.
2. Wählen Sie im Menü **Importieren** die Option **Schlüsselspeicher**.
3. Wählen Sie im Menü **Schlüsselspeichertyp** die Option **PKCS#12**.
4. Wählen Sie unter **Verwenden als** die Option **APNs**.



5. Klicken Sie für **Schlüsselspeicherdatei** auf **Durchsuchen** und navigieren Sie zu der Datei.
6. Geben Sie unter **Kennwort** das Kennwort für das Zertifikat ein.
7. Geben Sie optional eine **Beschreibung** ein.
8. Klicken Sie auf **Importieren**.

XenMobile zeigt nun wieder die Seite **Zertifikate** an. Die Felder **Name**, **Status**, **Gültig von** und **Gültig bis** werden aktualisiert.

SAML für Single Sign-On mit Citrix Files

January 5, 2022

XenMobile und Citrix Content Collaboration können zur Verwendung von SAML (Security Assertion Markup Language) konfiguriert werden, um SSO-Zugriff (Single Sign-On) auf mobile Citrix Files-Apps bereitzustellen. Diese Funktionalität umfasst:

- Citrix Files-Apps, die MAM-SDK-fähig sind oder Apps, die mit dem MDX Toolkit umschlossen wurden
- Nicht umschlossene Citrix Files-Clients, z. B. die Website, das Outlook-Plug-in oder Synchronisierungsclients
- **Umschlossene Citrix Files-Apps**. Benutzer, die sich bei Citrix Files über die mobile Citrix Files-App anmelden, werden zur Benutzerauthentifizierung und zum Abrufen eines SAML-Tokens an Secure Hub weitergeleitet. Nach einer erfolgreichen Authentifizierung sendet die mobile Citrix Files-App das SAML-Token an Content Collaboration. Nach der Erstanmeldung können Benutzer über SSO auf die mobile Citrix Files-App zugreifen. Sie können außerdem Dokumente aus Content Collaboration an E-Mails in Secure Mail anfügen, ohne sich jedes Mal neu anzumelden.
- **Nicht umschlossene Citrix Files-Clients**. Benutzer, die sich über einen Webbrowser oder einen anderen Citrix Files-Client bei Citrix Files anmelden, werden an XenMobile umgeleitet. XenMobile authentifiziert die Benutzer, die dann einen SAML-Token erhalten, der an Content Collaboration gesendet wird. Nach der ersten Anmeldung können Benutzer auf Citrix Files-Clients über SSO ohne erneute Anmeldung zugreifen.

Zur Verwendung von XenMobile als SAML-Identitätsanbieter (IdP) für Content Collaboration müssen Sie XenMobile wie in diesem Artikel beschrieben für die Verwendung mit Enterprise-Konten konfigurieren. Alternativ können Sie XenMobile für die ausschließliche Zusammenarbeit mit Speicherzonenconnectors konfigurieren. Weitere Informationen finden Sie unter Verwenden von Citrix Content Collaboration mit XenMobile.

Ein detailliertes Architekturdiagramm finden Sie unter Architektur.

Voraussetzungen

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

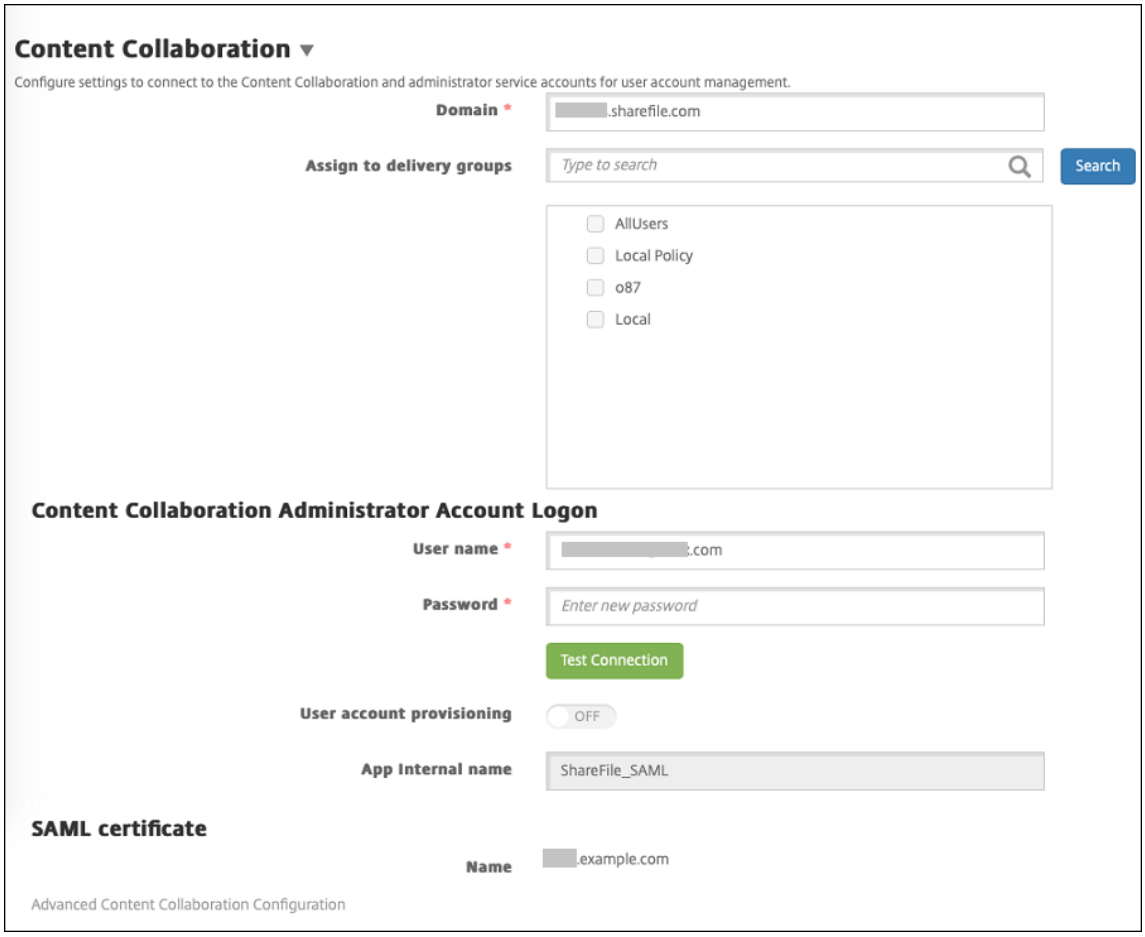
- Das MAM-SDK oder eine kompatible Version des MDX Toolkits (für mobile Citrix Files-Apps).

  Weitere Informationen finden Sie unter XenMobile-Kompatibilität.
- Eine kompatible Version mobiler Citrix Files-Apps und Secure Hub.
- Content Collaboration-Administratorkonto.
- Überprüfte Konnektivität zwischen XenMobile und Content Collaboration.

Konfigurieren des Zugriffs auf Content Collaboration

Bevor Sie SAML für Content Collaboration einrichten, stellen Sie die Zugriffsinformationen für Content Collaboration wie folgt bereit:

1. Klicken Sie in der XenMobile-Webkonsole auf **Konfigurieren > ShareFile**. Die Konfigurationsseite **ShareFile** wird angezeigt. In Ihrer Konsole wird möglicherweise der Begriff “Content Collaboration” anstelle von ShareFile angezeigt.



2. Konfigurieren Sie folgende Einstellungen:

   - **Domäne:** Geben Sie Ihren Content Collaboration-Unterdomänennamen ein. Beispiel: `example.sharefile.com`.
   - **Bereitstellungsgruppen zuweisen:** Suchen Sie nach Bereitstellungsgruppen, die SSO mit Content Collaboration verwenden sollen, oder wählen Sie sie aus.
   - **ShareFile-Administratorkonto**
   - **Benutzername:** Geben Sie den Benutzernamen des Content Collaboration-Administrators ein. Dieses Benutzerkonto muss über Administratorrechte verfügen.
   - **Kennwort:** Geben Sie das Kennwort des Content Collaboration-Administrators ein.
   - **Benutzerkontoprovisioning:** Lassen Sie diese Einstellung deaktiviert. Verwenden Sie das Content Collaboration User Management Tool für das Provisioning von Benutzern. Siehe Provision user accounts and distribution groups.

3. Sie können über die Schaltfläche **Verbindung testen** prüfen, ob Benutzername und Kennwort des Content Collaboration-Administratorkontos für das angegebene Content Collaboration-

Konto authentifiziert werden.

4. Klicken Sie auf **Speichern**.
    - XenMobile und Content Collaboration werden synchronisiert und die Content Collaboration-Einstellungen **ShareFile-Aussteller/Entitäts-ID** und **Anmelde-URL** werden aktualisiert.
    - Auf der Seite **Konfigurieren > ShareFile** wird der **interne App-Name** angezeigt. Sie benötigen diesen Namen, um die in Ändern der SSO-Einstellungen für Citrix Files.com beschriebenen Schritte auszuführen.

Einrichten von SAML für umschlossene Citrix Files MDX-Apps

Sie müssen Citrix Gateway nicht für die Single Sign-On-Konfiguration von umschlossenen Citrix Files MDX-Apps verwenden. Informationen zum Konfigurieren des Zugriffs für nicht umschlossene Citrix Files-Clients wie die Website, das Outlook-Plug-In oder die Sync-Clients finden Sie unter Konfigurieren von Citrix Gateway für andere Citrix Files-Clients.

Die folgenden Schritte gelten für iOS- und Android-Apps und -Geräte. So konfigurieren Sie SAML für umschlossene Citrix Files MDX-Apps:

1. Umschließen Sie die mobile Citrix Files-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 Citrix Files-App hoch. Weitere Informationen zum Hochladen von MDX-Apps finden Sie unter Hinzufügen einer MDX-App zu XenMobile.
3. Überprüfen Sie die SAML-Einstellungen: Melden Sie sich bei Content Collaboration mit den Anmeldeinformationen des Administrators an, die Sie zuvor konfiguriert haben.
4. Vergewissern Sie sich, dass Content Collaboration und XenMobile für dieselbe Zeitzone konfiguriert sind. Stellen Sie sicher, dass in XenMobile die Uhrzeit der konfigurierten Zeitzone angezeigt wird. Ist dies nicht der Fall, kann das SSO fehlschlagen.

Überprüfen der mobilen Citrix Files-App

1. Installieren und konfigurieren Sie Secure Hub auf dem Benutzergerät.
2. Laden Sie die mobile Citrix Files-App aus dem XenMobile-Store herunter und installieren Sie sie.
3. Starten Sie die mobile Citrix Files-App. Citrix Files wird ohne Anforderung von Benutzernamen und Kennwort gestartet.

Überprüfung mit Secure Mail

1. Installieren und konfigurieren Sie Secure Hub gegebenenfalls auf dem Benutzergerät.
2. Laden Sie Secure Mail aus dem XenMobile Store herunter und installieren und konfigurieren Sie das Programm.
3. Öffnen Sie ein neues E-Mail-Formular und tippen Sie auf **Von Citrix Files anfügen**. Die zum Anfügen verfügbaren Dateien werden ohne Anforderung von Benutzernamen und Kennwort angezeigt.

Konfigurieren von Citrix Gateway für andere Citrix Files-Clients

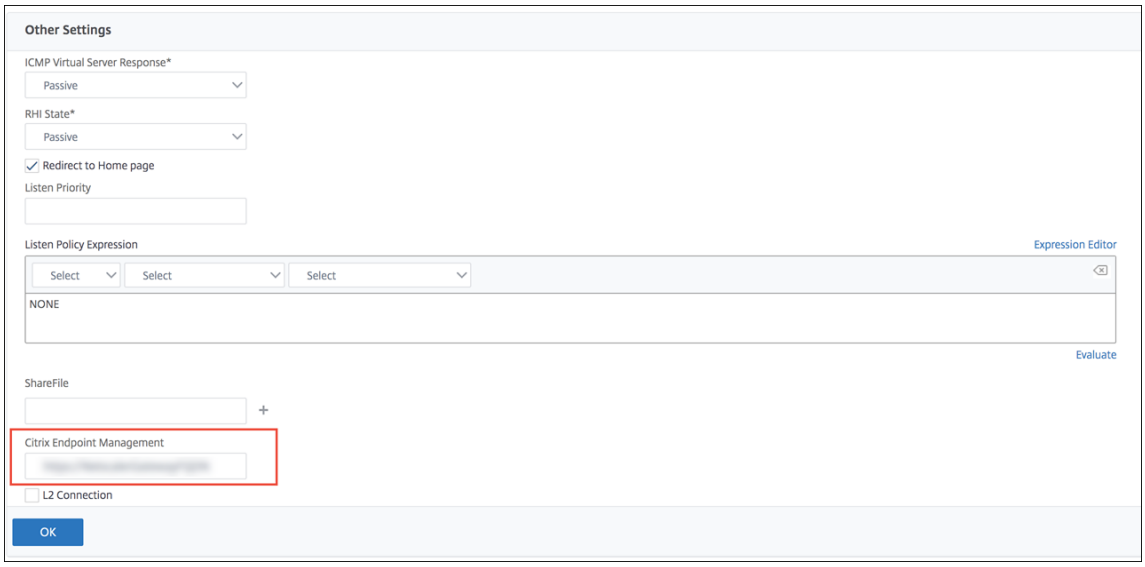
Zum Konfigurieren des Zugriffs für nicht umschlossene Citrix Files-Clients (z. B. Website, Outlook-Plug-In oder Synchronisierungsclients) konfigurieren Sie Citrix Gateway folgendermaßen, damit es die Verwendung von XenMobile als SAML-Identitätsanbieter unterstützt:

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

Deaktivieren der Homepageumleitung

Deaktivieren Sie das Standardverhalten für Anforderungen aus dem /cginfra-Pfad. Dadurch können Benutzer die ursprünglich angeforderte interne URL anstelle der konfigurierten Homepage sehen.

1. Bearbeiten Sie die Einstellungen für den virtuellen Citrix Gateway-Server, der für XenMobile-Anmeldungen verwendet wird. Navigieren Sie in Citrix ADC zu **Other Settings** und deaktivieren Sie das Kontrollkästchen **Redirect to Home Page**.



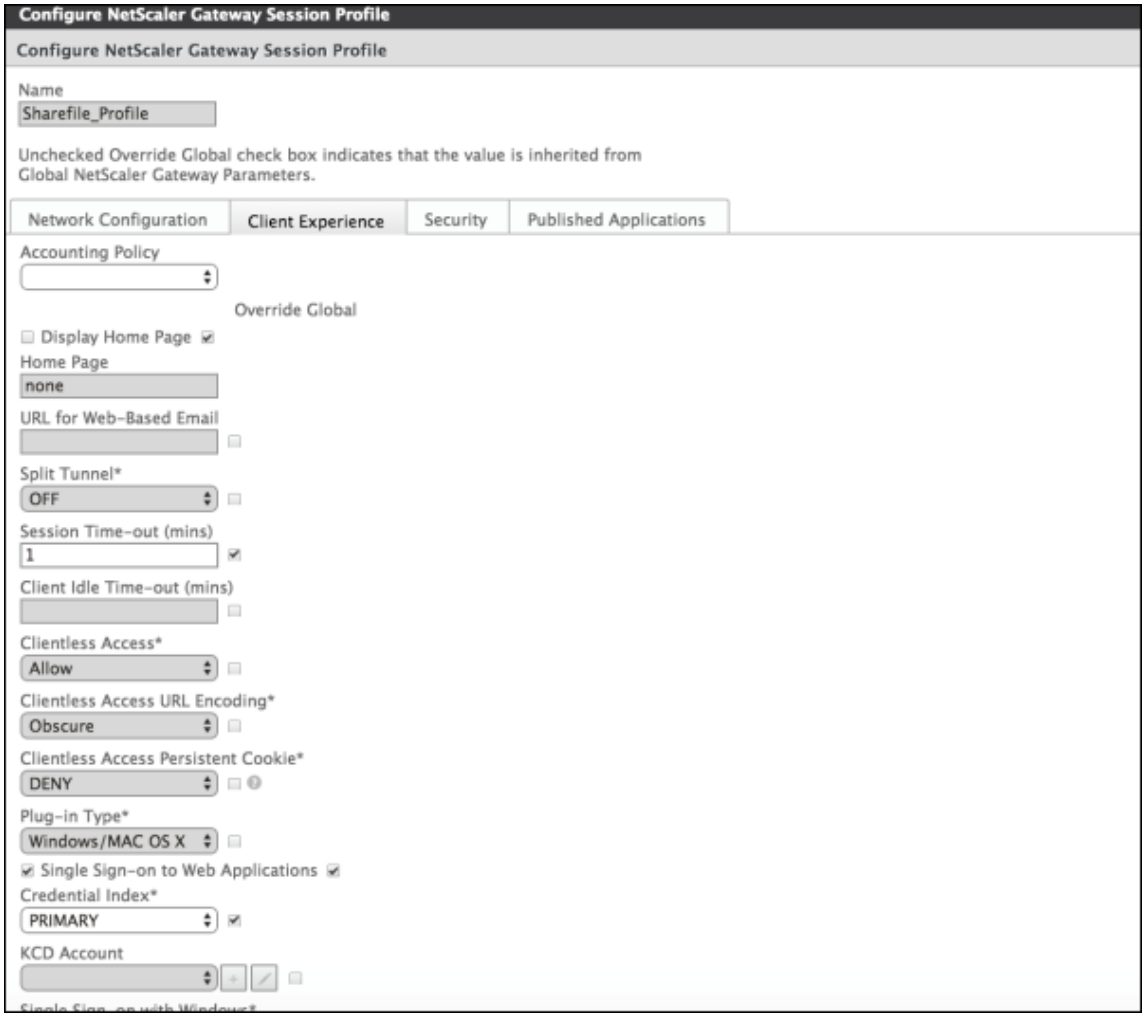
2. Geben Sie unter **ShareFile** (jetzt Content Collaboration genannt) den internen Namen des XenMobile-Servers und die Portnummer ein.
3. Geben Sie unter **Citrix Endpoint Management** Ihre XenMobile-URL ein. Ihre Version von Citrix Gateway verwendet möglicherweise den älteren Produktnamen **AppController**.

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

Erstellen einer Citrix Files-Sitzungsrichtlinie und eines Anforderungsprofils

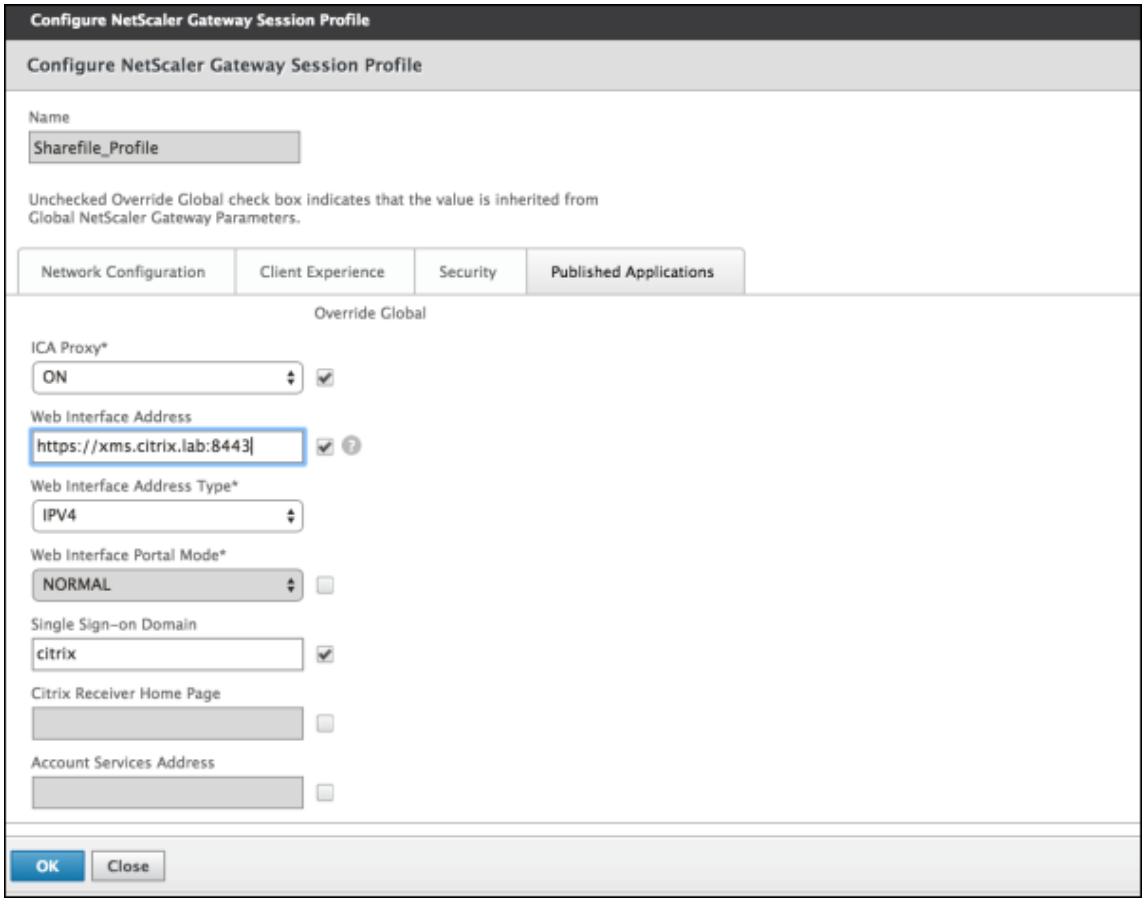
Konfigurieren Sie die folgenden Einstellungen zum Erstellen einer Citrix Files-Sitzungsrichtlinie und eines Anforderungsprofils:

1. Klicken Sie im Konfigurationsprogramm für Citrix Gateway im linken Navigationsbereich auf **Citrix Gateway > Policies > Session**.
2. Erstellen Sie eine Sitzungsrichtlinie. Klicken Sie auf der Registerkarte **Policies** auf **Add**.
3. Geben Sie im Feld **Name** den Ausdruck **ShareFile_Policy** ein.
4. Erstellen Sie eine Aktion durch Klicken auf die **+**-Schaltfläche. Die Seite **Create 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 aus.
  - **Credential Index:** Klicken Sie auf **PRIMARY**.
- Klicken Sie auf die Registerkarte **Published Applications**.

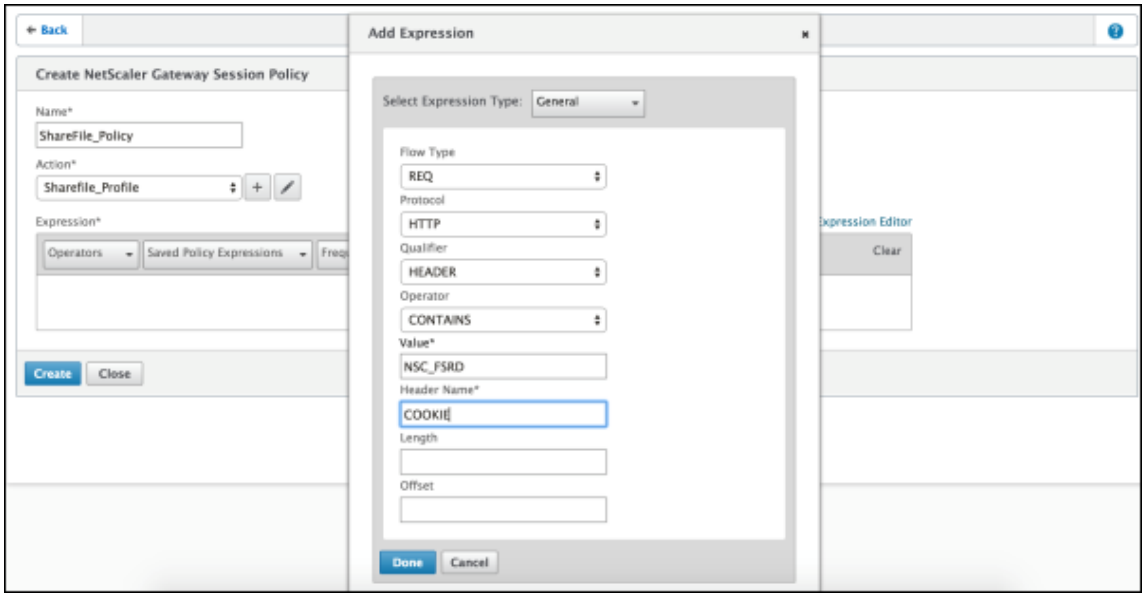


Konfigurieren Sie folgende Einstellungen:

- **ICA Proxy:** Klicken Sie auf **ON**.
- **Web Interface Address:** Geben Sie die XenMobile Server-URL ein.
- **Single Sign-on Domain:** Geben Sie den Namen Ihrer Active Directory-Domäne ein.

  Beim Konfigurieren des Citrix 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.

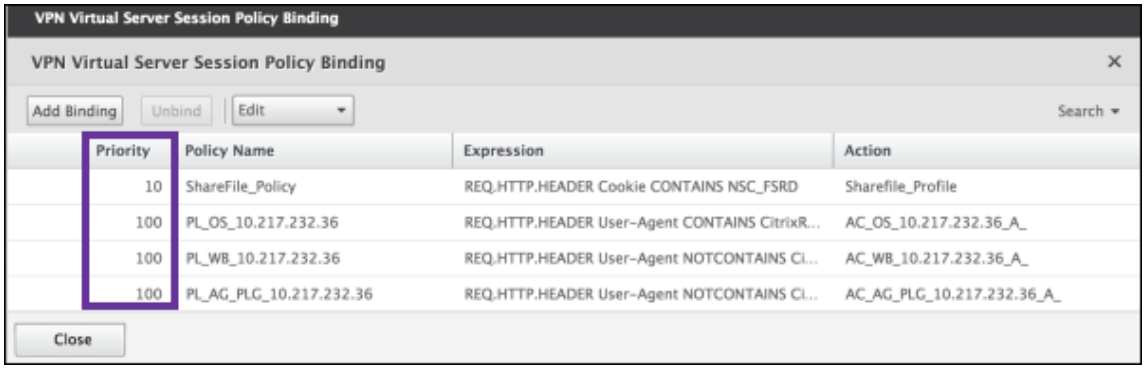
7. Klicken Sie auf **Create** und dann auf **Close**.

Konfigurieren von Richtlinien auf dem virtuellen Citrix Gateway-Server

Konfigurieren Sie die folgenden Einstellungen auf dem virtuellen Citrix Gateway-Server.

1. Klicken Sie im Konfigurationsprogramm für Citrix Gateway im linken Navigationsbereich auf **Citrix Gateway > Virtual Servers**.
2. Klicken Sie im Bereich **Details** auf den virtuellen Citrix Gateway-Server.
3. Klicken Sie auf **Edit**.
4. Klicken Sie auf **Configured policies > Session policies** und dann auf **Add binding**.

5. Wählen Sie **ShareFile_Policy** aus.
6. Bearbeiten Sie die automatisch generierte Prioritätszahl unter **Priority** für die ausgewählte Richtlinie so, dass sie die höchste Priorität (die niedrigste Zahl) vor allen anderen aufgeführten Richtlinien hat. Beispiel:



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

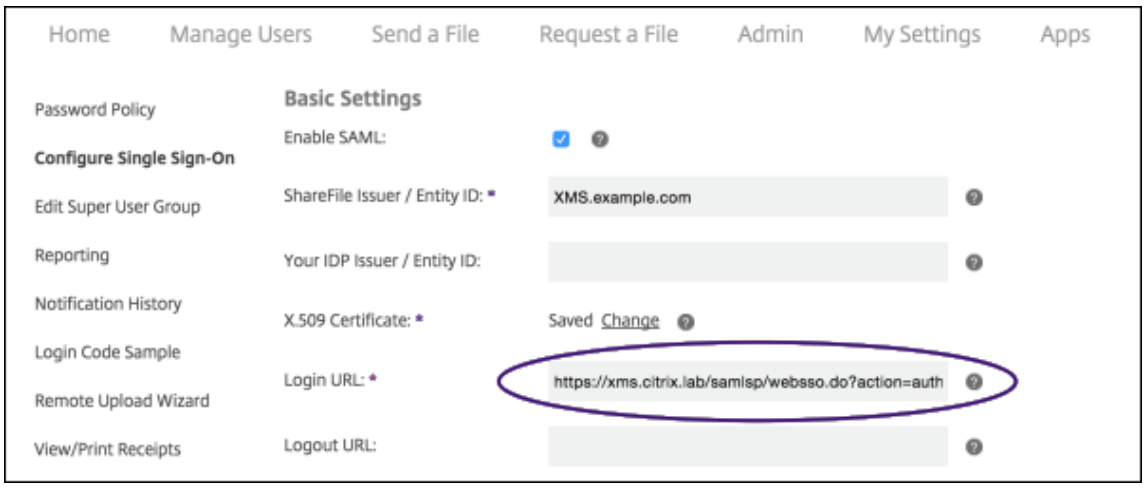
Ändern der SSO-Einstellungen für Citrix Files.com

Nehmen Sie die folgenden Änderungen für mit MDX umschlossene und nicht umschlossene Citrix Files-Apps vor.

> **Wichtig:**
>
> An den internen Anwendungsnamen wird eine neue Nummer angehängt:
>
> - Jedes Mal, wenn Sie die Citrix Files-App bearbeiten oder neu erstellen
> - Jedes Mal, wenn Sie die Content Collaboration-Einstellungen in XenMobile ändern
>
> Daher müssen Sie die Anmelde-URL auf der Citrix Files-Website dem neuen App-Namen entsprechend aktualisieren.

1. Melden Sie sich bei Ihrem Content Collaboration-Konto (`https://<subdomain>.sharefile.com`) als Content Collaboration-Administrator an.
2. Klicken Sie im Content Collaboration-Webinterface auf **Admin** und wählen Sie **Single Sign-On konfigurieren** aus.
3. Bearbeiten Sie den Eintrag im Feld **Anmelde-URL** wie folgt:

   Beispiel für eine **Anmelde-URL** vor der Bearbeitung: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`.



- Geben Sie den externen FQDN des virtuellen Citrix Gateway-Servers plus **/cginfra/https/** vor dem FQDN des XenMobile-Servers und hinter dem FQDN des XenMobile-Servers **8443** ein.

  Beispiel für eine URL nach der Bearbeitung: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

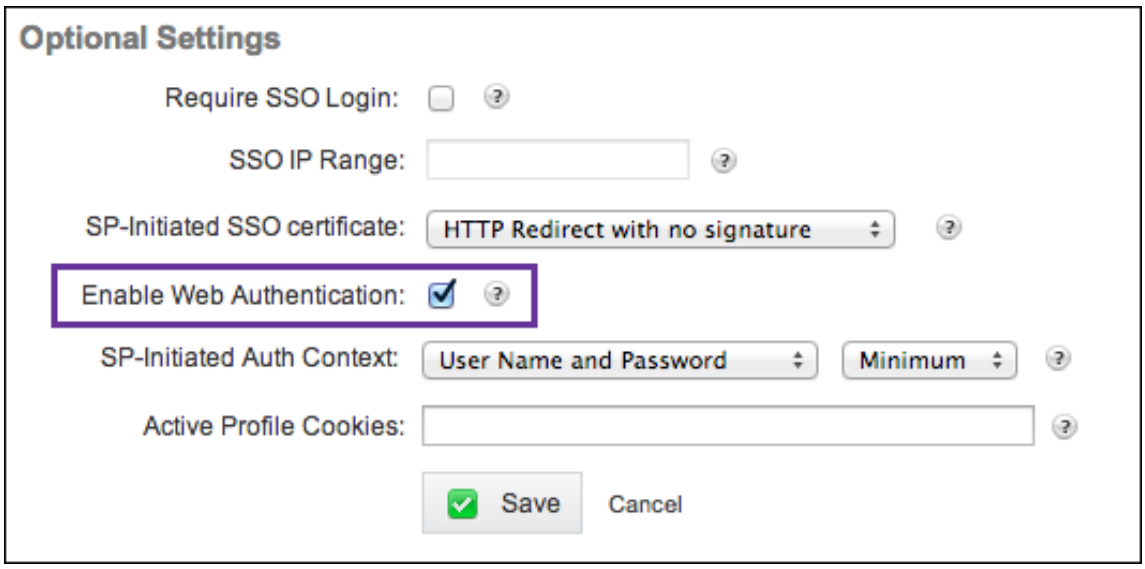
- Ändern Sie den Parameter `&app=ShareFile_SAML_SP` in den internen Citrix Files-App-Namen. Der interne Name lautet standardmäßig `ShareFile_SAML`. Jedes Mal, wenn Sie die Konfiguration ändern, wird eine Zahl an den internen Namen angehängt (`ShareFile_SAML_2`, `ShareFile_SAML_3` usw.). Sie können den **internen App-Namen** auf der Seite **Konfigurieren > ShareFile** nachschlagen.

  Beispiel für eine URL nach der Bearbeitung: `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.

  Beispiel der endgültigen URL: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. Aktivieren Sie unter **Optional Settings** das Kontrollkästchen **Enable Web Authentication**.



Überprüfen der Konfiguration

Überprüfen Sie die Konfiguration wie nachfolgend beschrieben.

1. Geben Sie `https://<subdomain>sharefile.com/saml/login` im Browser ein.

   Sie werden zum Citrix Gateway-Anmeldungsformular umgeleitet. Erfolgt keine Umleitung, überprüfen Sie die oben aufgeführten Konfigurationseinstellungen.

2. Geben Sie die Anmeldeinformationen ein, die Sie für die Citrix Gateway- bzw. XenMobile-Umgebung konfiguriert haben.

   Ihre Citrix Files-Ordner unter `<subdomain>.sharefile.com` werden angezeigt. Wenn keine Citrix Files-Ordner angezeigt werden, prüfen Sie, ob Sie die richtigen Anmeldeinformationen eingegeben haben.

Azure Active Directory als Identitätsanbieter

January 6, 2022

Wenn Sie Azure Active Directory (AAD) als Identitätsanbieter (IdP) konfigurieren, können Benutzer sich bei XenMobile mit ihren Azure-Anmeldeinformationen registrieren.

iOS-, Android-, Windows 10- und Windows 11-Geräte werden unterstützt. iOS- und Android-Geräte werden über Secure Hub registriert. Diese Authentifizierungsmethode steht nur Benutzern zur Verfügung, die sich über Citrix Secure Hub bei MDM registrieren. Geräte, die sich bei MAM registrieren, können sich nicht mit AAD-Anmeldeinformationen authentifizieren. Um Secure Hub mit

MDM+MAM zu verwenden, konfigurieren Sie XenMobile zur Verwendung von Citrix Gateway für die MAM-Registrierung. Weitere Informationen finden Sie unter Citrix Gateway und XenMobile.

Sie können Azure unter **Einstellungen > Authentifizierung > IdP** als Identitätsanbieter konfigurieren. Die Seite **IDP** wurde mit dieser XenMobile-Version neu eingeführt. In älteren XenMobile-Versionen wurde Azure unter **Einstellungen > Microsoft Azure** konfiguriert.

Anforderungen

- Versionen und Lizenzen
  - Für die Registrierung von iOS- und Android-Geräten benötigen Sie Secure Hub 10.5.5.
  - Für die Registrierung von Windows 10 und Windows 11-Geräten benötigen Sie Microsoft Azure Premium-Lizenzen.
- Verzeichnisdienste und Authentifizierung
  - XenMobile Server muss für die zertifikatbasierte Authentifizierung konfiguriert werden.
  - Wenn Sie Citrix ADC für die Authentifizierung verwenden, muss Citrix ADC für die zertifikatbasierte Authentifizierung konfiguriert sein.
  - Die Secure Hub-Authentifizierung erfolgt unter Einsatz von Azure AD gemäß dem in Azure AD definierten Authentifizierungsmodus.
  - Die Verbindung zwischen dem XenMobile Server und Windows Active Directory (AD) muss per LDAP hergestellt werden. Konfigurieren Sie den lokalen LDAP-Server für eine Synchronisierung mit Azure AD.

Authentifizierungsablauf

Wenn ein Gerät über Secure Hub registriert wird und XenMobile für die Verwendung von Azure als Identitätsanbieter konfiguriert ist, ist der Authentifizierungsablauf wie folgt:

1. Benutzer geben auf dem Gerät ihren Benutzernamen und ihr Kennwort für Azure Active Directory im Azure AD-Anmeldebildschirm ein, der in Secure Hub angezeigt wird.
2. Azure AD validiert den Benutzer und sendet ein ID-Token.
3. Secure Hub sendet das ID-Token an den XenMobile Server.
4. XenMobile validiert das ID-Token und die darin enthaltenen Benutzerinformationen. XenMobile gibt eine Sitzungs-ID zurück.

Einrichtung von Azure-Konten

Zur Verwendung von Azure AD als Identitätsanbieter melden Sie sich bei Ihrem Azure-Konto an und nehmen Sie folgende Änderungen vor:

1. Registrieren Sie die benutzerdefinierte Domäne und lassen Sie sie prüfen. Weitere Informationen finden Sie unter Hinzufügen Ihres benutzerdefinierten Domänennamens über das Azure Active Directory-Portal.
2. Erweitern Sie Ihr lokales Verzeichnis auf Azure Active Directory mit Tools zur Verzeichnisintegration. Weitere Informationen finden Sie unter Verzeichnisintegration.

Zur Verwendung von Azure AD zum Registrieren von Windows 10 und Windows 11-Geräten nehmen Sie die folgenden Änderungen an Ihrem Azure-Konto vor:

1. Machen Sie MDM zum zuverlässigen Eintrag in Azure AD. Klicken Sie hierzu auf **Azure Active Directory > Anwendungen** und dann auf **Hinzufügen**.
2. Klicken Sie auf **Anwendung aus dem Katalog hinzufügen**. Wechseln Sie zu **Verwaltung mobiler Geräte** und wählen Sie **Lokale MDM-Anwendung**. Speichern Sie die Einstellungen.

   Wählen Sie "Lokale MDM-Anwendung" selbst dann aus, wenn Sie sich für die Citrix XenMobile-Cloud angemeldet haben. Bei Microsoft gilt jede Anwendung ohne mehrfache Mandanten als lokale MDM-Anwendung.
3. Konfigurieren Sie in der Anwendung die XenMobile Server-Ermittlung, AGB-Endpunkte und APP-ID-URI:

   - **URL für MDM-Ermittlung:** `https://<FQDN>:8443/<instanceName>/wpe`
   - **URL zu den MDM-Nutzungsbedingungen:** `https://<FQDN>:8443/<instanceName>/wpe/tou`
   - **App-ID-URI:** `https://<FQDN>:8443/`
4. Wählen Sie die in Schritt 2 erstellte, lokale MDM-Anwendung. Aktivieren Sie die Option **Geräte für diese Benutzer verwalten**, um MDM für alle Benutzer oder bestimmte Benutzergruppen zu aktivieren.

   Weitere Informationen zur Verwendung von Azure AD für Windows 10 und Windows 11-Geräte finden Sie unter Azure Active Directory integration with MDM.

Konfigurieren von Azure AD als Identitätsanbieter

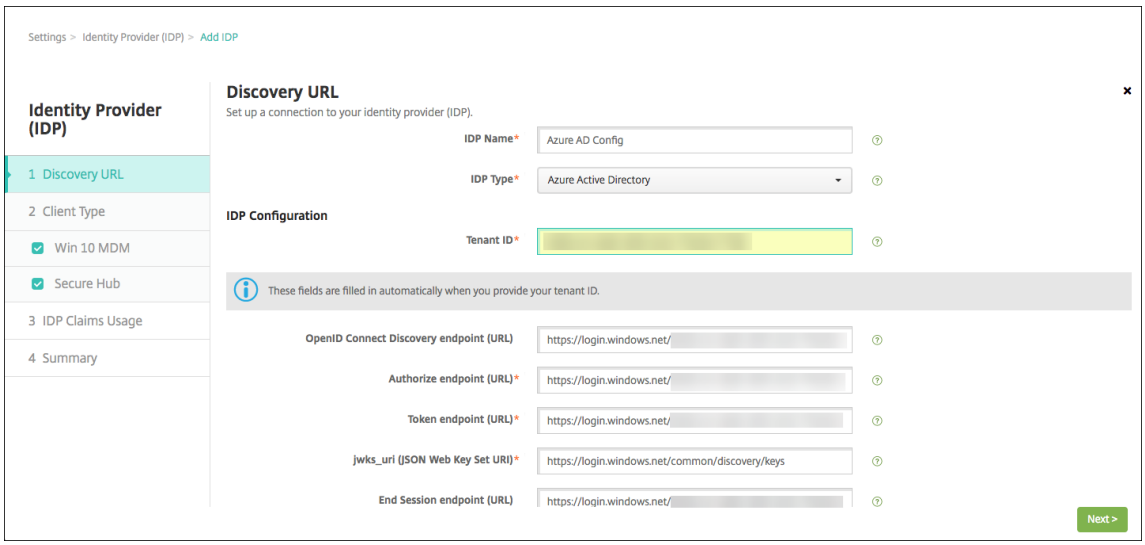
1. Suchen bzw. notieren Sie die benötigten Informationen zu Ihrem Azure-Konto:

   - Mandanten-ID von der Azure-Seite mit den Anwendungseinstellungen
   - Wenn mit Azure AD Windows 10 und Windows 11-Geräte registriert werden sollen, benötigen Sie außerdem Folgendes:
     - **App-ID-URI:** URL des Servers, auf dem XenMobile ausgeführt wird
     - **Client-ID:** eindeutiger Bezeichner Ihrer App von der Azure-Seite "Konfigurieren"
     - **Schlüssel:** von der Azure-Seite mit den Anwendungseinstellungen

2. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
3. Klicken Sie unter **Authentifizierung** auf **Identitätsanbieter (IdP)**. Die Seite **Identitätsanbieter** wird angezeigt.

4. Klicken Sie auf **Hinzufügen**. Die Seite **IdP-Konfiguration** wird angezeigt.
5. Konfigurieren Sie die folgenden Informationen zum Identitätsanbieter:
   - **IdP-Name:** Geben Sie einen Namen für die IdP-Verbindung ein, die Sie erstellen.
   - **IdP-Typ:** Wählen Sie Azure Active Directory als IdP-Typ.
   - **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.

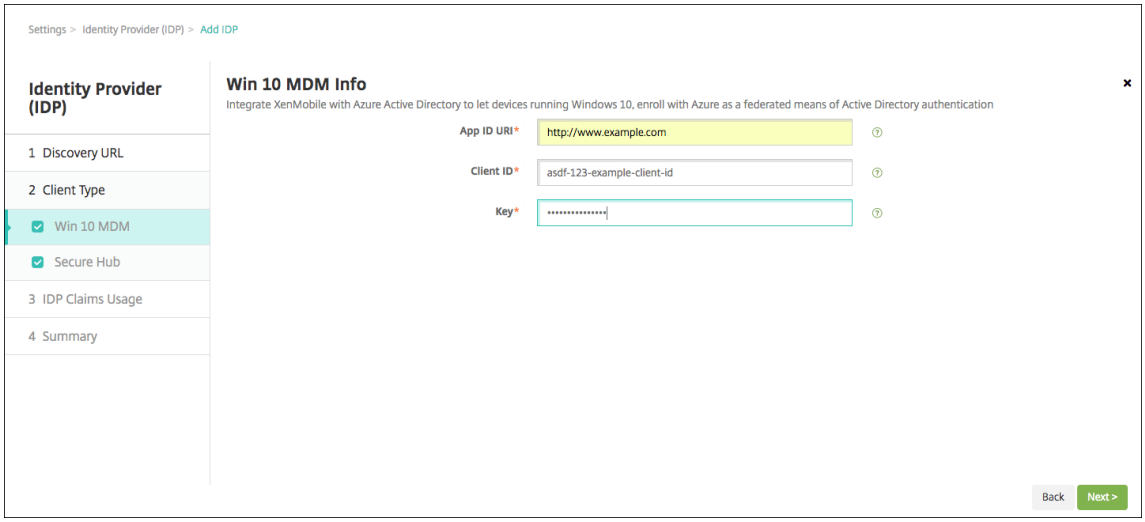
   Beispiel: In `https://manage.windowszaure.com/acmew.onmicrosoft.com##workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...` ist die ID `abc123-abc123-abc123`.



6. Die restlichen Felder werden automatisch ausgefüllt. Wenn sie ausgefüllt sind, klicken Sie auf **Weiter**.

7. Zum Konfigurieren von XenMobile für die MDM-Registrierung von Windows 10 und Windows 11-Geräten unter Einsatz von Azure AD konfigurieren Sie die folgenden Einstellungen: Um diesen optionalen Schritt zu überspringen, deaktivieren Sie **Windows MDM**.

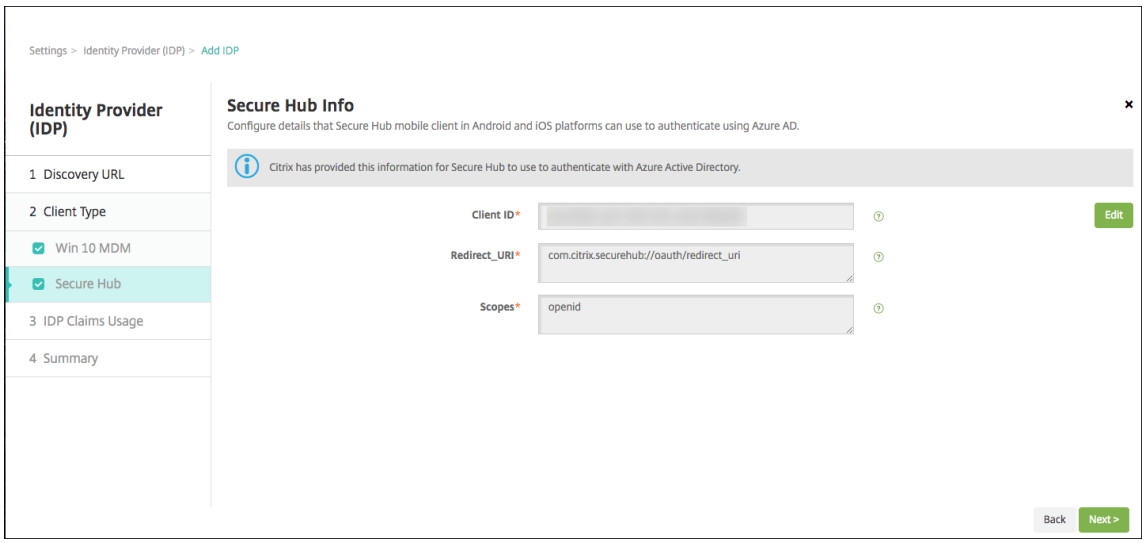
   - **App-ID-URI:** Geben Sie die URL des XenMobile Server-Computers ein, die Sie beim Konfigurieren der Azure-Einstellungen eingegeben haben.
   - **Client-ID:** Kopieren Sie den Wert von der Azure-Seite “Konfigurieren”. De Client-ID ist der eindeutige Bezeichner Ihrer App
   - **Schlüssel:** Kopieren 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.



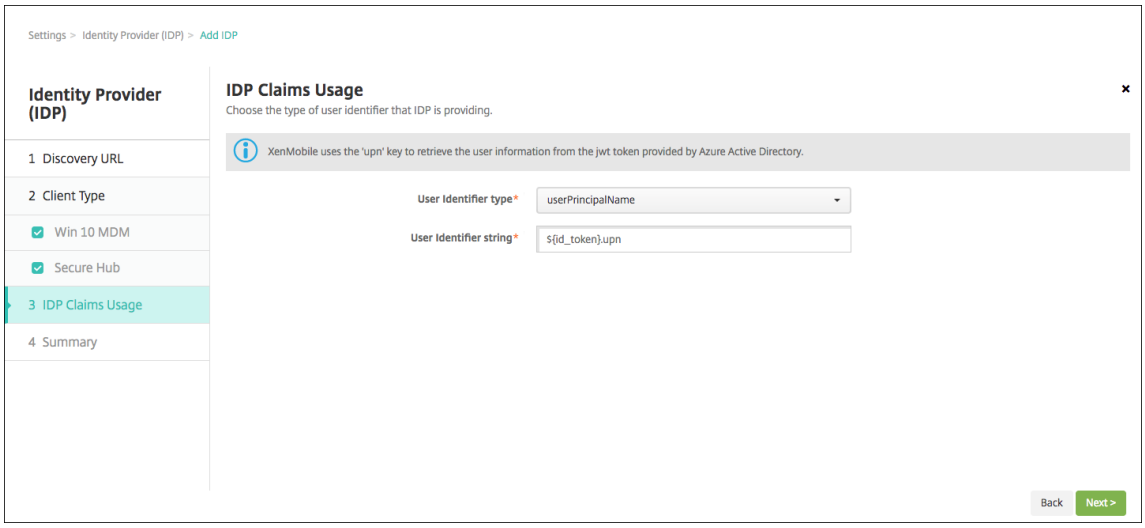
8. Klicken Sie auf **Weiter**.

   Citrix hat Secure Hub bei Microsoft Azure registriert und verwaltet die Informationen. In diesem Bildschirm werden die Details angezeigt, die von Secure Hub für die Kommunikation mit Azure Active Directory verwendet werden. Diese Seite wird künftig verwendet, falls eine Information geändert werden muss. Bearbeiten Sie diese Seite nur, wenn Citrix Sie dazu auffordert.

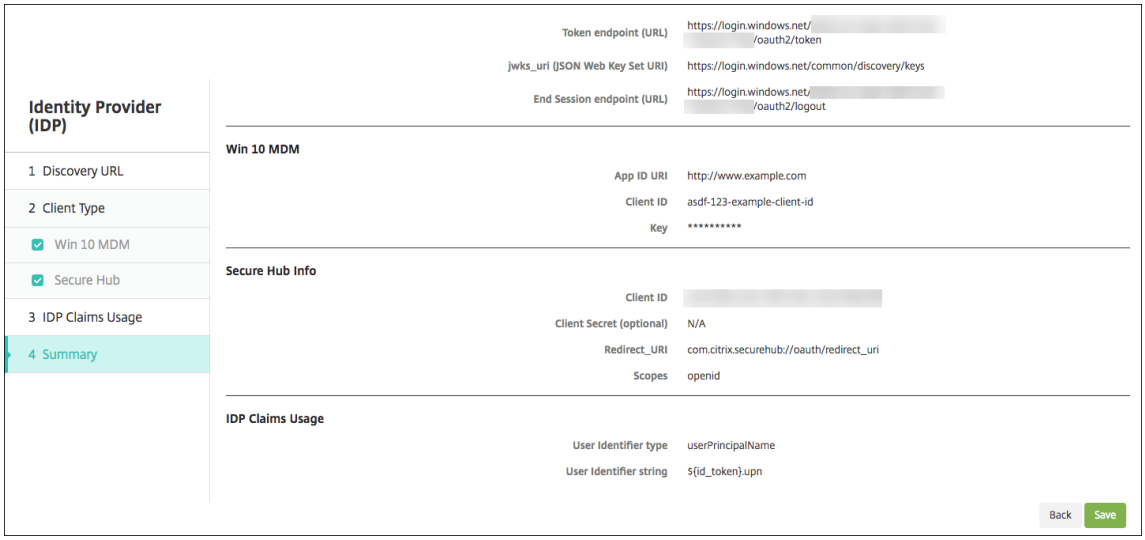
9. Klicken Sie auf **Weiter**.



10. Konfigurieren Sie den Benutzer-ID-Typ, den Ihr Identitätsanbieter bereitstellt:
    - **Benutzer-ID-Typ:** Wählen Sie aus der Liste **userPrincipalName** aus.
    - **Benutzer-ID-Zeichenfolge:** Dieses Feld wird automatisch ausgefüllt.
11. Klicken Sie auf **Weiter**.

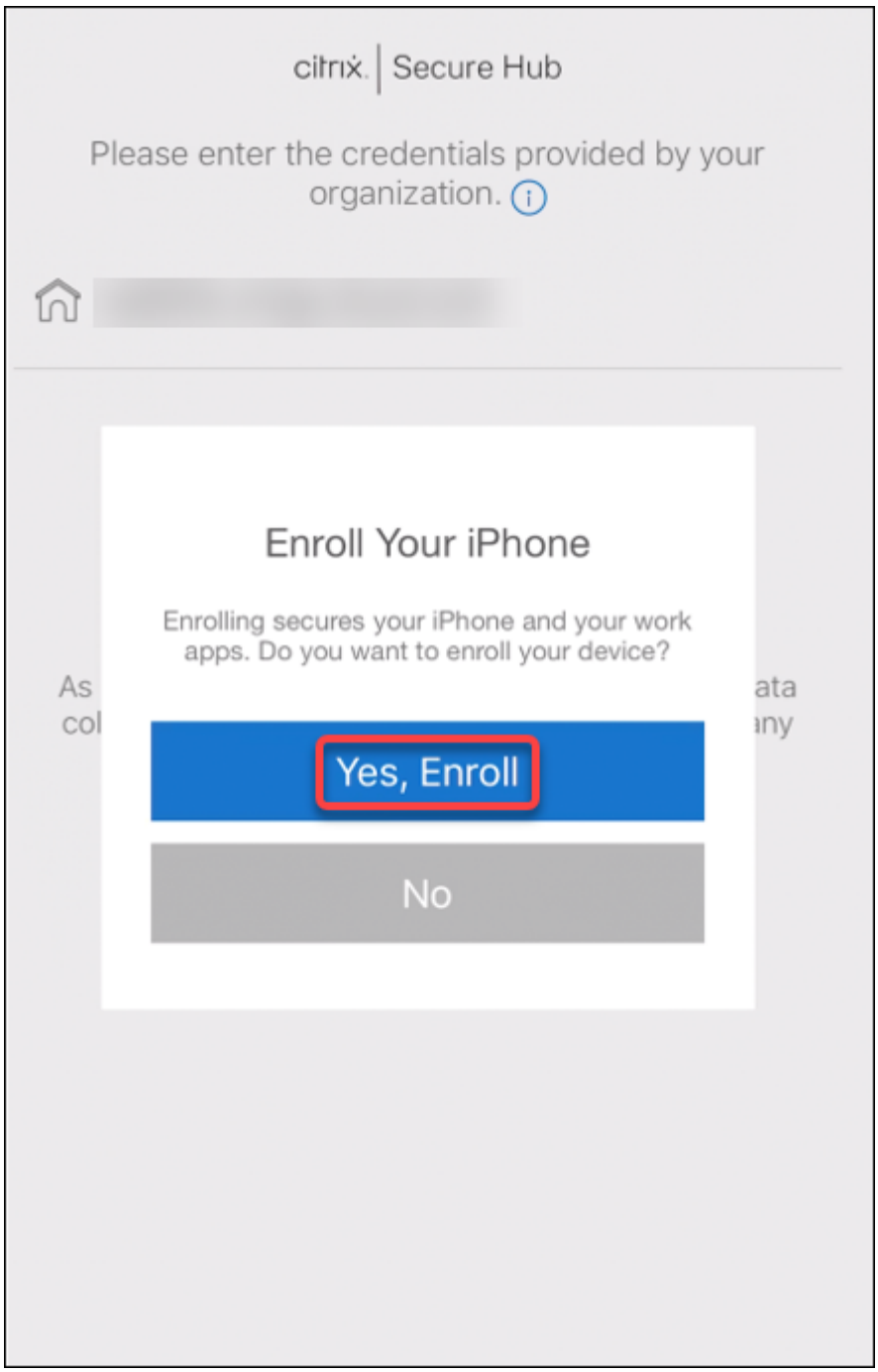


12. Lesen Sie die **Zusammenfassung** und klicken Sie auf **Speichern**.

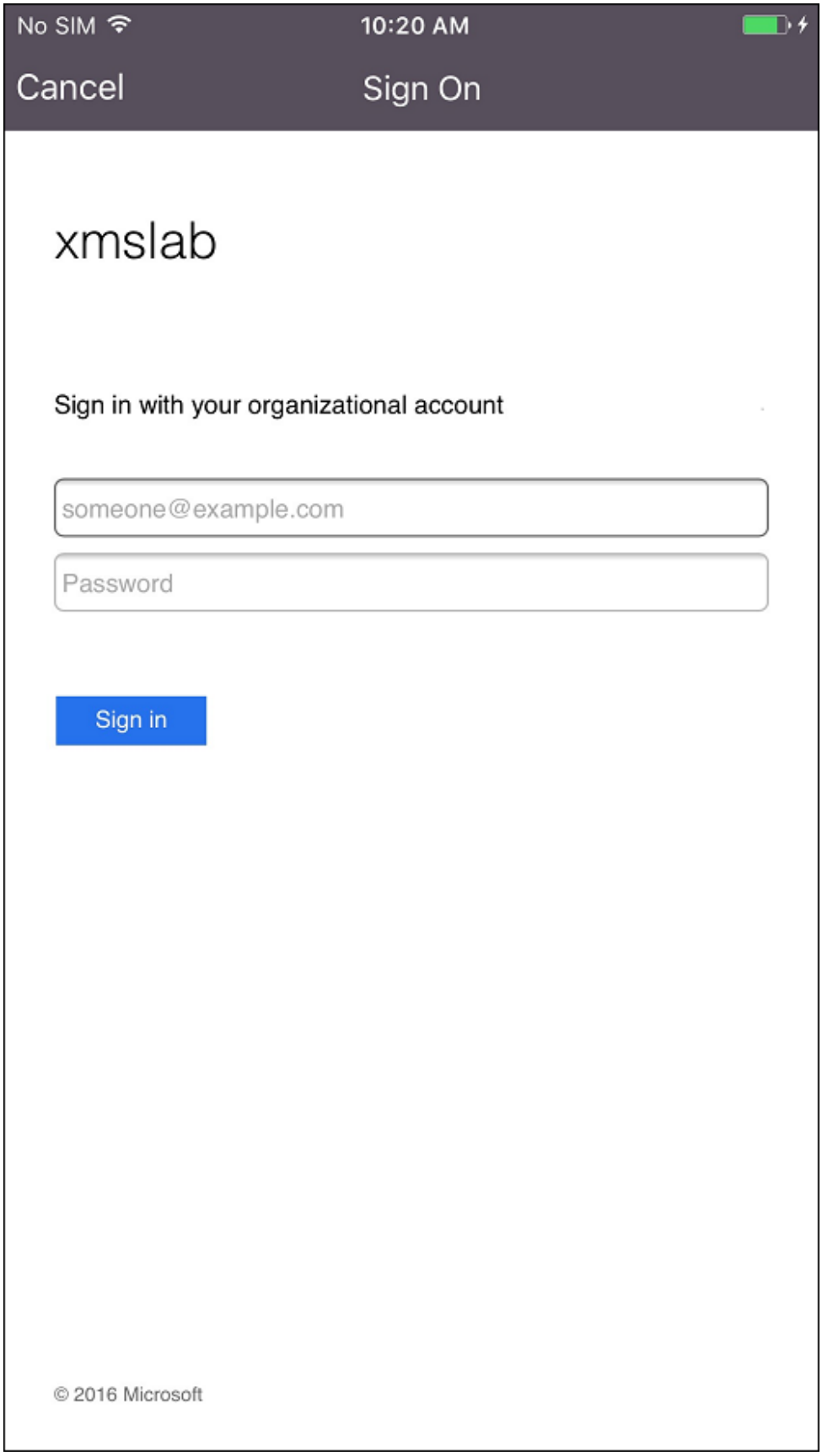


Ablauf für die Benutzer

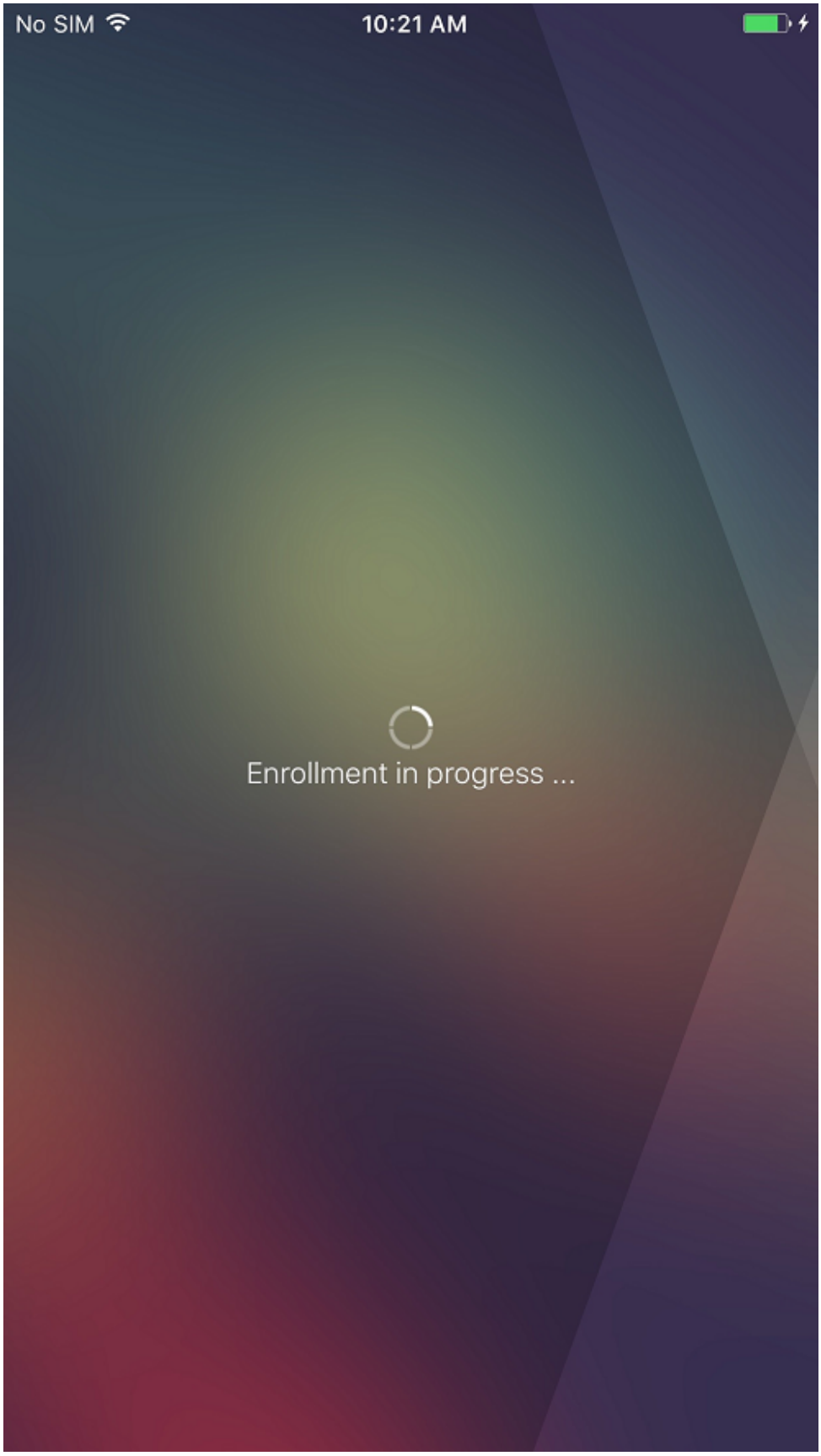
1. Die Benutzer starten Secure Hub. Sie geben dann den vollqualifizierten Domänenamen (FQDN) des XenMobile-Servers, einen Benutzerprinzipalnamen oder eine E-Mail-Adresse ein.

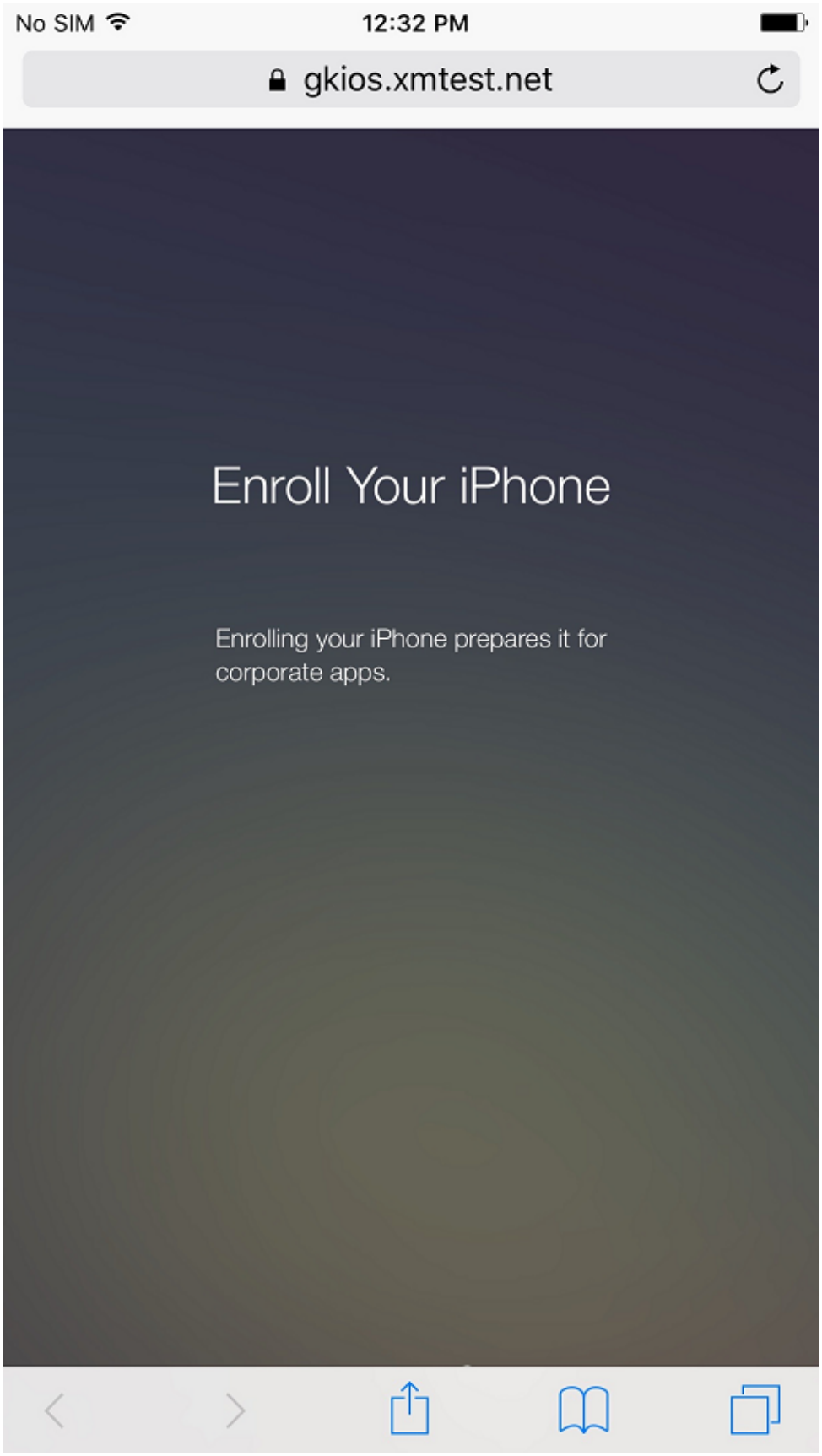


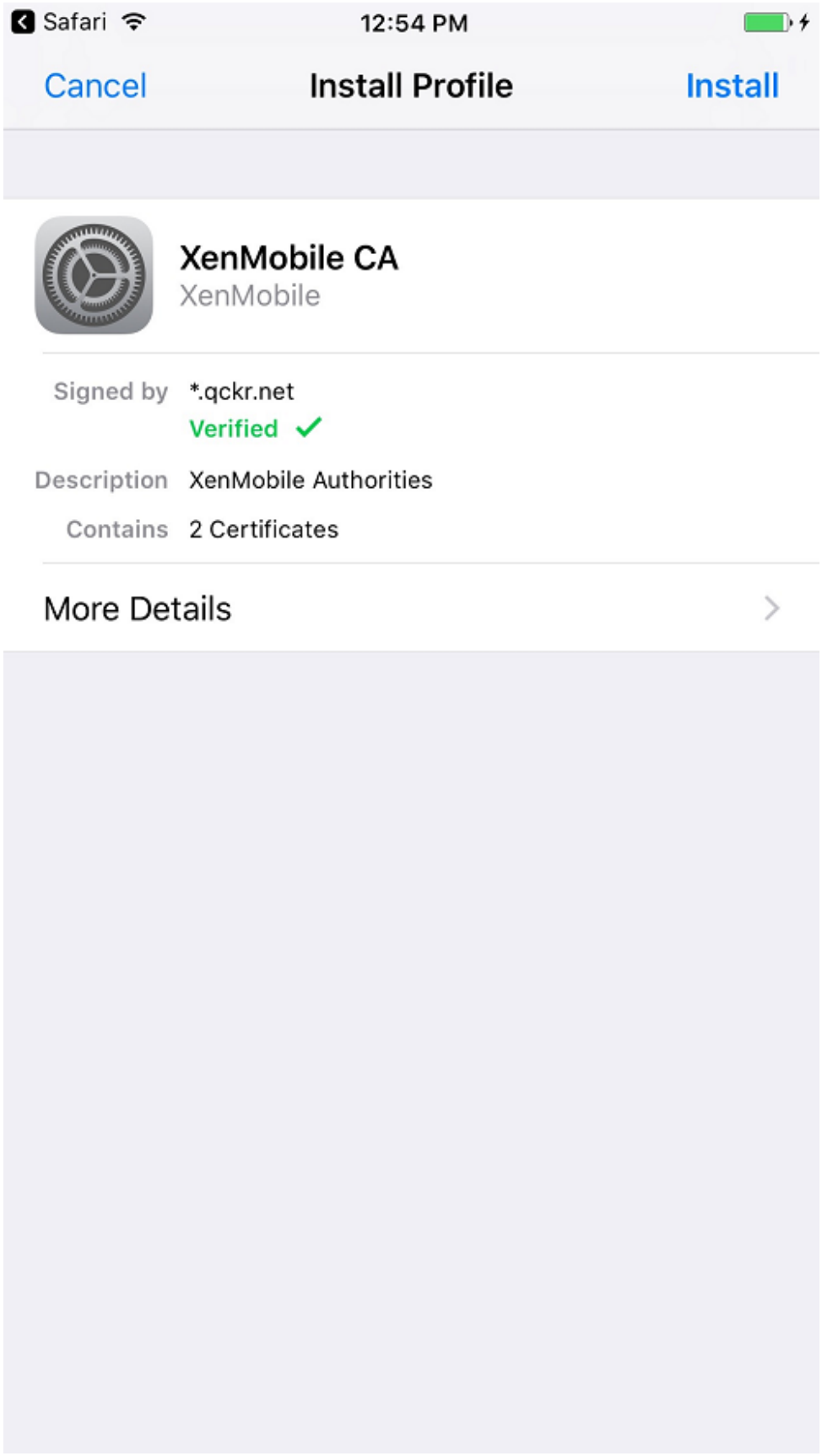
2. Sie klicken anschließend auf **Ja, registrieren**.



3. Die Benutzer melden sich mit ihren Azure AD-Anmeldeinformationen an.







4. Sie führen die Registrierung wie jede andere Art der Registrierung über Secure Hub durch.

> **Hinweis:**
>
> XenMobile unterstützt keine Authentifizierung über Azure Active Directory für Registrierungseinladungen. Wenn Sie eine Registrierungseinladung mit einer Registrierungs-URL senden, authentifizieren sich die Benutzer über LDAP anstelle von Azure AD.

Abgeleitete Anmeldeinformationen

January 5, 2022

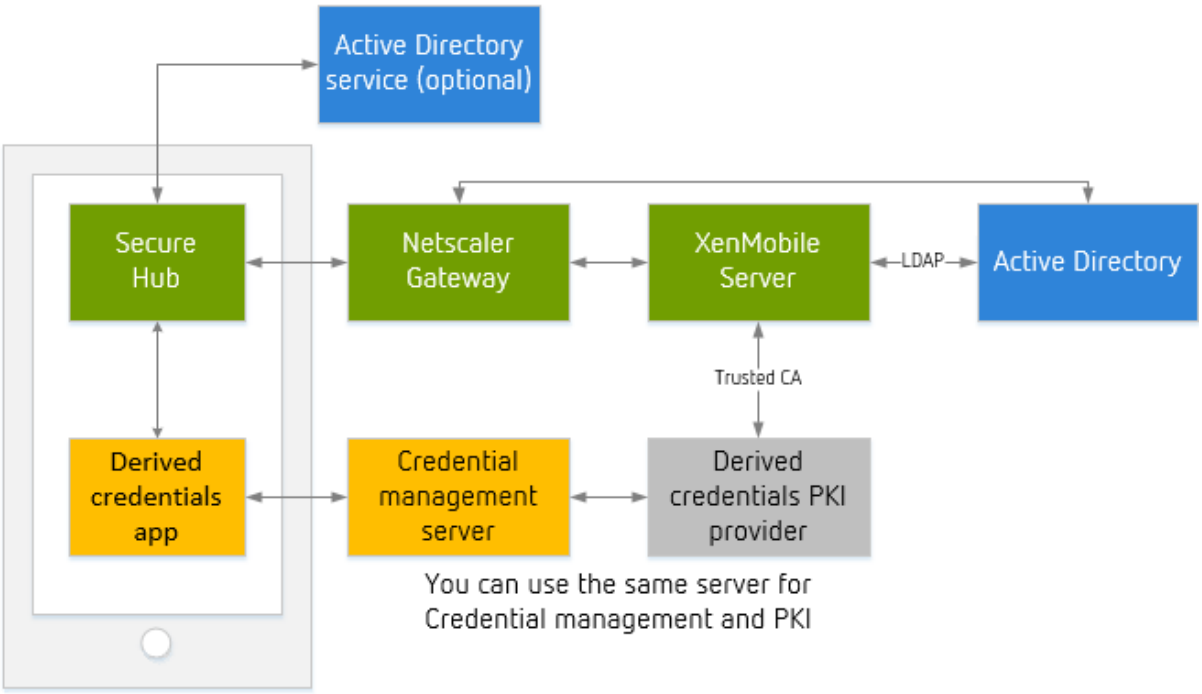
Abgeleitete Anmeldeinformationen bieten eine starke Authentifizierung für mobile Geräte. Eine Smartcard stellt die Anmeldeinformationen bereit, die auf einem Mobilgerät anstelle der Karte residieren. Bei einer Smartcard handelt es sich um eine PIV-Karte (Personal Identity Verification).

Bei den abgeleiteten Anmeldeinformationen handelt es sich um ein Registrierungszertifikat, das die Benutzer-ID, z. B. den UPN, enthält. Die vom Anbieter erhaltenen Anmeldeinformationen speichert XenMobile in einem sicheren Tresor auf dem Gerät.

Abgeleitete Anmeldeinformationen können von XenMobile für die Registrierung und Authentifizierung von Geräten verwendet werden. Wenn XenMobile für abgeleitete Anmeldeinformationen konfiguriert ist, unterstützt es keine Registrierungseinladungen oder andere Registrierungssicherheitsmodi. Citrix unterstützt die Verwendung von abgeleiteten Anmeldeinformationen bei der iOS-Registrierung.

Architektur

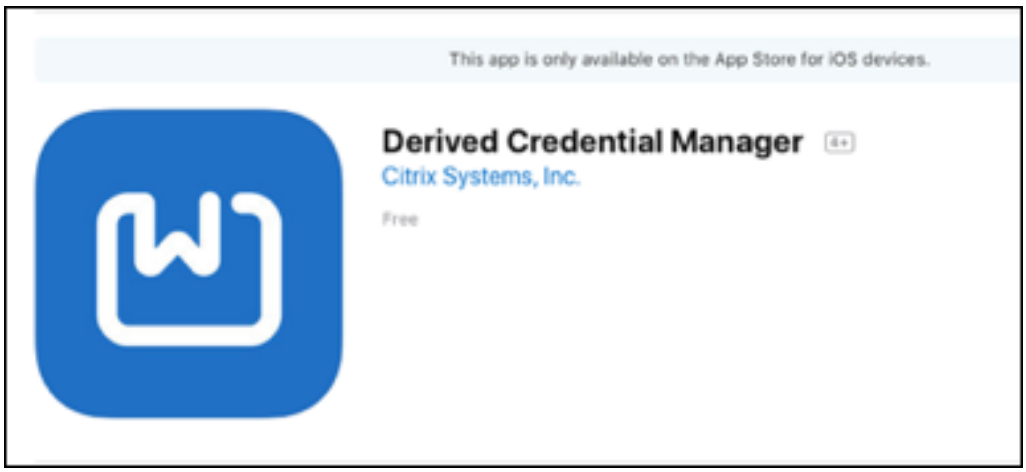
Für die Registrierung stellt XenMobile Server eine Verbindung mit den Komponenten in der nachfolgend dargestellten Reihenfolge her.



- Während der Geräteregistrierung ruft Secure Hub Zertifikate aus der App für abgeleitete Anmeldeinformationen ab.
- Die App für abgeleitete Anmeldeinformationen kommuniziert bei der Registrierung mit dem Verwaltungsserver für Anmeldeinformationen.
- Für den Verwaltungsserver für Anmeldeinformationen und einen PKI-Anbieter von Drittanbietern können Sie denselben oder verschiedene Server verwenden.
- Der XenMobile Server stellt eine Verbindung mit dem Drittanbieter-PKI-Server zum Abrufen von Zertifikaten her.

Anforderungen

- Laden Sie Citrix Secure Hub herunter und installieren Sie es.
- Laden Sie die App gemäß Ihrer Lösung für abgeleitete Anmeldeinformationen herunter und konfigurieren Sie sie:
  - **Entrust Datacard:**
    * Laden Sie Citrix Derived Credential Manager herunter und installieren Sie die App auf den Geräten, *bevor* Sie diese bei XenMobile registrieren. Derived Credentials Manager ist die Identitätsanbieter-App für Citrix. Das Logo sieht folgendermaßen aus:



    * Citrix Derived Credentials Manager unterstützt nur neue Registrierungen. Die Geräte müssen erneut registriert werden.
        · XenMobile Server Version 10.8 oder höher.
        · Erfordert die Geräteregistrierung bei MDM+MAM.
  - **Andere Lösungen für abgeleitete Anmeldeinformationen:** Die meisten anderen Lösungen sind zwar wahrscheinlich mit XenMobile kompatibel, Sie sollten die Integration jedoch vor der Implementierung in der Produktion testen.

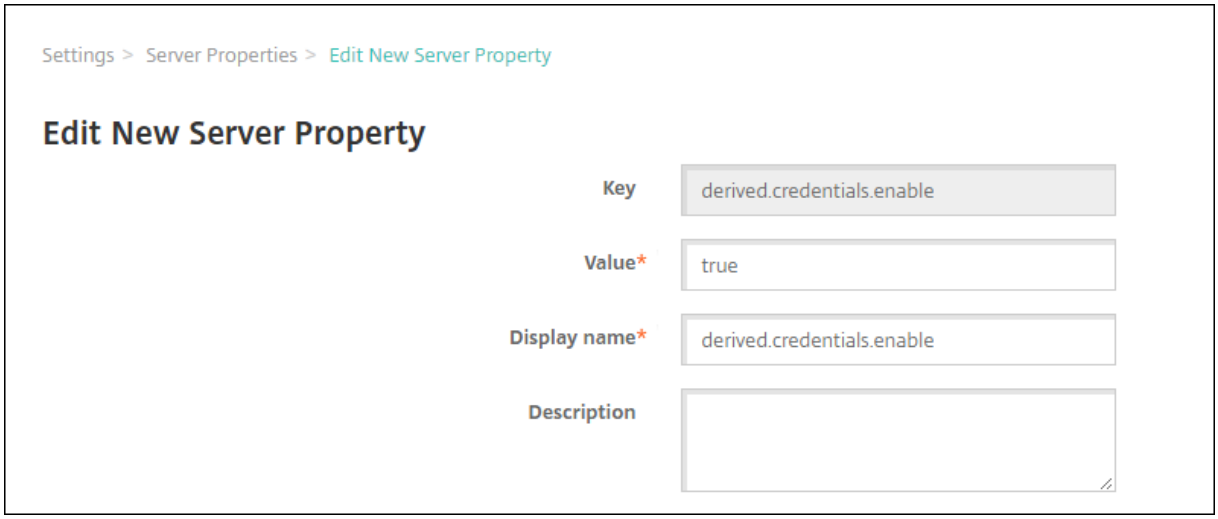
- Muss das Stammzertifikat der Zertifizierungsstelle haben, die Zertifikate an den Anmeldeinformationsanbieterserver ausstellt. Durch diese Einrichtung kann XenMobile bei der Registrierung digital signierte Zertifikate akzeptieren. Informationen zum Hinzufügen der Zertifikate finden Sie unter Zertifikate und Authentifizierung.
  - Wenn die E-Mail-Domäne eines Benutzers sich von der LDAP-Domäne unterscheidet, schließen Sie die E-Mail-Domäne in die Einstellung **Domänenalias** unter **Einstellungen > LDAP** ein. Wenn die Domäne für E-Mail-Adressen beispielsweise `citrix.com` lautet und der Namen der LDAP-Domäne `sample.com`, legen Sie **Domänenalias** auf **`sample.com, citrix.com`** fest.
  - XenMobile unterstützt die Verwendung abgeleiteter Anmeldeinformationen auf gemeinsam genutzten Geräten nicht.
- Benutzerdentitätszertifikate:
  - Der Benutzername im Feld “Subject alternative name” muss in der SubjectAltName-Erweiterung als otherName-, rfc822Name- oder dNSName-Feld formatiert sein. Andere Felder werden nicht unterstützt. Weitere Informationen zu alternativen Antragstellernamen, finden Sie unter https://www.ietf.org/rfc/rfc5280.txt.
  - Die Angabe der Benutzeridentität im Feld “Subject” in Form von E-Mail-Adresse oder CN wird nicht unterstützt.
- Citrix Gateway für Clientzertifikat-Authentifizierung oder Authentifizierung mit Zertifikat und Sicherheitstoken konfiguriert

Aktivieren abgeleiteter Anmeldeinformationen

Standardmäßig enthält die XenMobile-Konsole die Seite **Einstellungen > Abgeleitete Anmeldeinformationen** nicht.

Aktivieren der Schnittstelle für abgeleitete Anmeldeinformationen:

- Gehen Sie zu der Seite **Einstellungen > Servereigenschaften** fügen Sie die Servereigenschaft **derived.credentials.enable** hinzu und legen Sie sie auf **true** fest.

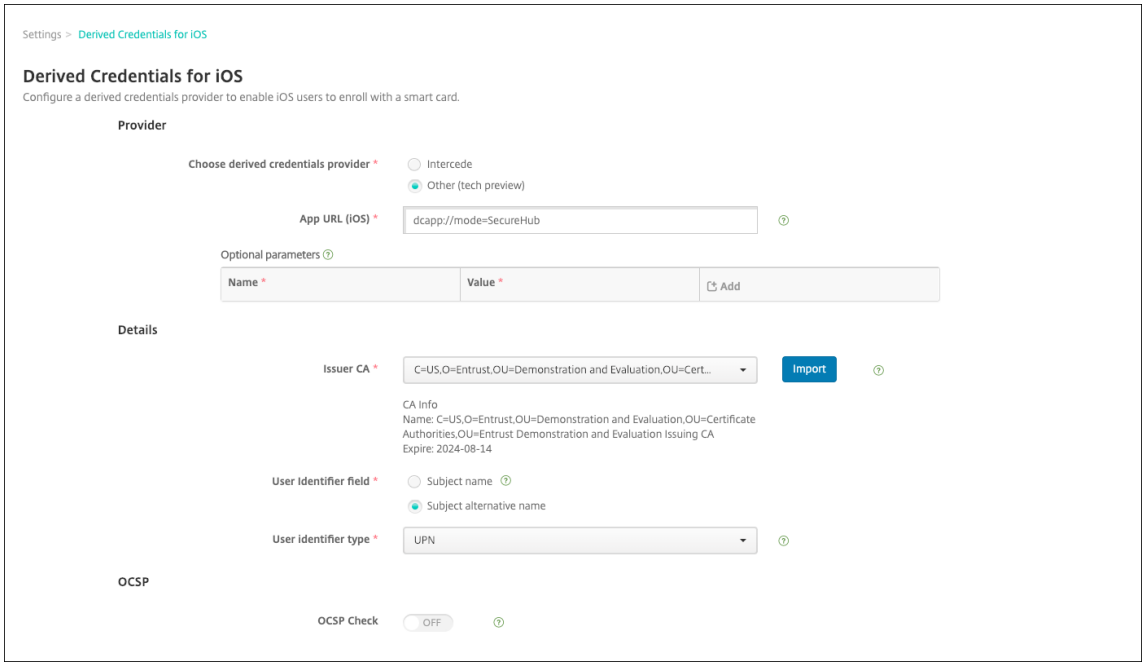


Konfigurieren abgeleiteter Anmeldeinformationen

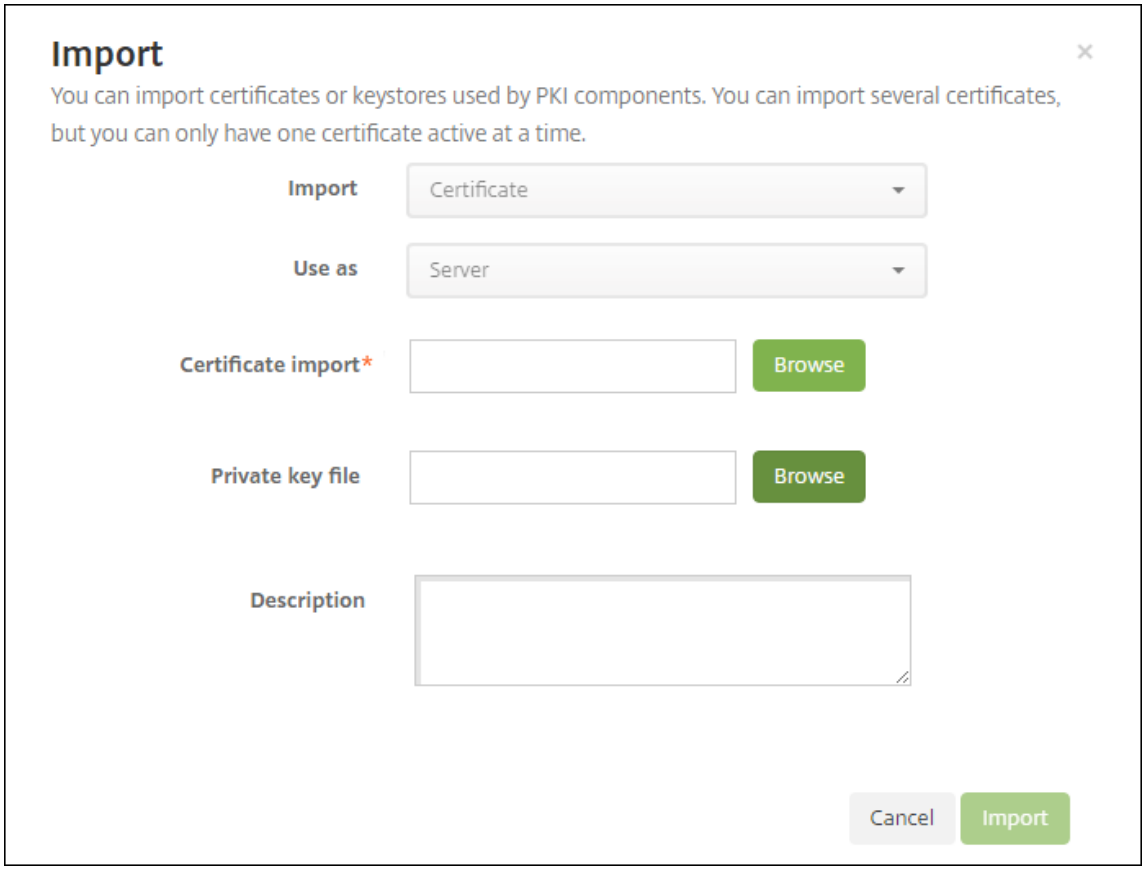
Es wird davon ausgegangen, dass Sie eine funktionierende Konfiguration für den Anbieter für abgeleitete Anmeldeinformationen haben, den Sie in XenMobile integrieren möchten. Sie können XenMobile für die Kommunikation mit dem Server konfigurieren. Sie können außerdem ein ZS-Zertifikat für abgeleitete Anmeldeinformationen wählen, das Sie XenMobile bereits hinzugefügt haben oder Sie importieren das Zertifikat.

Sie können Online Certificate Status Protocol (OCSP) für dieses ZS-Zertifikat aktivieren. Weitere Informationen über OCSP finden Sie unter “Eigenverwaltete Zertifizierungsstellen” im Artikel PKI-Entitäten.

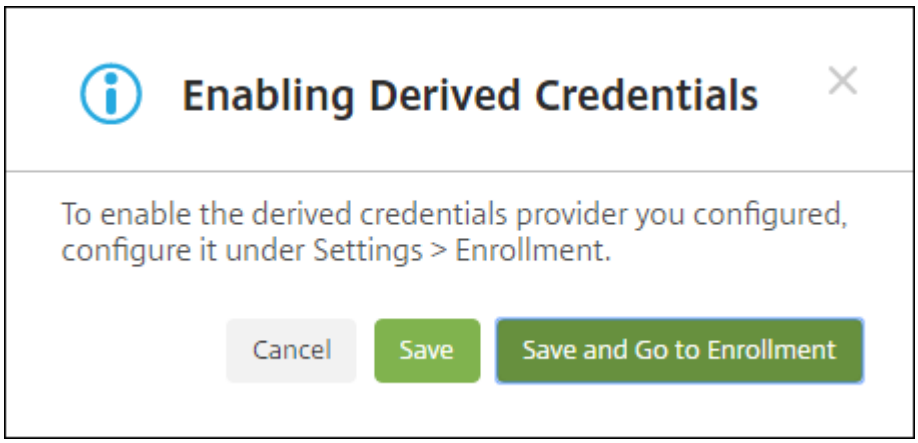
1. Navigieren Sie in der XenMobile-Konsole zu **Einstellungen > Abgeleitete Anmeldeinformationen für iOS**.
2. Wählen Sie unter **Anbieter für abgeleitete Anmeldeinformationen wählen** die Option **Andere** für Entrust Datacard. Geben Sie für **App-URL (iOS)** `dcapp://mode=SecureHub` ein.



3. **Optionale Parameter:** Einige Anbieter für abgeleitete Anmeldeinformationen erfordern evtl. die Angabe von Parametern für die Verbindung. Dabei kann es sich beispielsweise um die URL eines Backend-Servers handeln. Klicken Sie auf **Hinzufügen**, um Parameter anzugeben.
4. Geben Sie ein Zertifikat für abgeleitete Anmeldeinformationen an: Wenn das Zertifikat bereits in XenMobile hochgeladen wurde, wählen Sie es unter **Ausstellende ZS** aus. Klicken Sie andernfalls auf **Importieren**, um ein Zertifikat hinzuzufügen. Das Dialogfeld **Zertifikat importieren** wird angezeigt.
5. Klicken Sie im Dialogfeld **Zertifikat importieren** auf **Durchsuchen**, um zu dem Zertifikat zu navigieren. Klicken Sie dann auf **Durchsuchen** und navigieren Sie zu der Datei mit dem privaten Schlüssel.

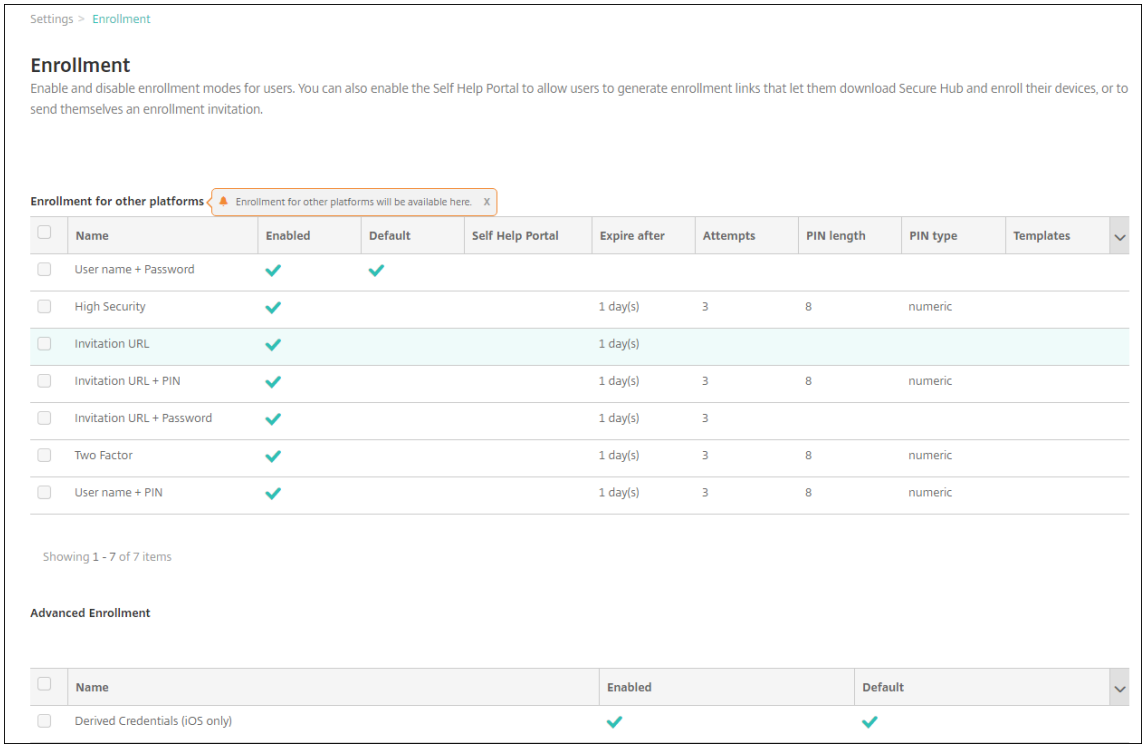


6. Konfigurieren Sie die Einstellungen.
   - Für die Citrix Derived Credential Manager-App: **Benutzer-ID-Feld** ist **Alternativer Antragstellername** und **Benutzer-ID-Typ** ist **userPrincipalName**.
   - Bringen Sie bei Verwendung eines anderen Anbieters diese Informationen beim Hersteller in Erfahrung.
7. Optional können Sie einen OCSP-Responder zum Überprüfen von Zertifikatsperrlisten verwenden. Citrix empfiehlt, einen OCSP-Responder für Sicherheitszwecke zu verwenden. Standardmäßig ist die OCSP-Prüfung auf **Aus** festgelegt.
   - Wenn Sie OCSP für das Zertifizierungsstellenzertifikat aktivieren, wählen Sie eine Option für **Benutzerdefinierte OCSP-URL verwenden**. Standardmäßig extrahiert XenMobile die OCSP-URL aus dem Zertifikat (Option **Zertifikatdefinition für Sperre verwenden**). Zum Angeben einer Responder-URL klicken Sie auf **Benutzerdef. verwenden** und geben Sie die URL ein.
   - **Responder-ZS:** Wählen Sie unter **Responder-ZS** ein Zertifikat. Klicken Sie alternativ auf **Importieren** und steuern Sie über das Dialogfeld **Zertifikat importieren** das Zertifikat an.
8. Klicken Sie auf **Speichern**. Das Dialogfeld **Aktivieren von abgeleiteten Anmeldeinformationen** wird angezeigt.



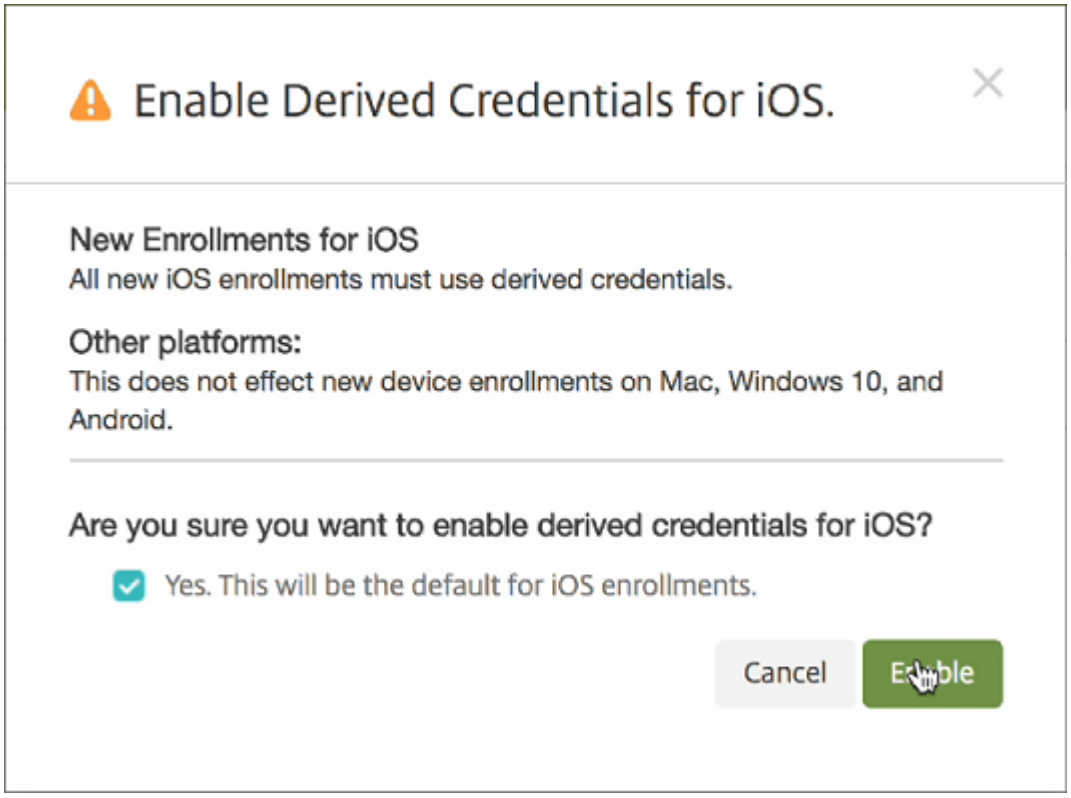
- Zum Aktivieren der Konfiguration für abgeleitete Anmeldeinformationen klicken Sie auf **Speichern**. Zur Verwendung abgeleiteter Anmeldeinformationen müssen Sie außerdem Registrierungseinstellungen konfigurieren.
- Zum Aktivieren der Konfiguration für abgeleitete Anmeldeinformationen und zum direkten Aufrufen von **Einstellungen > Registrierung** klicken Sie auf **Speichern und zur Registrierung gehen**.

9. Abgeleitete Anmeldeinformationen für die Registrierung aktivieren: Wählen Sie auf der Seite **Einstellungen > Registrierung** unter **Erweiterte Registrierung** die Option **Abgeleitete Anmeldeinformationen (nur iOS)** und klicken Sie auf **Aktivieren**.



10. Ein Bestätigungsdialogfeld wird angezeigt. Zum Aktivieren abgeleiteter Anmeldeinformationen

aktivieren Sie das Kontrollkästchen und klicken Sie auf **Aktivieren**.



11. Zum Bearbeiten der Optionen für abgeleitete Anmeldeinformationen für die Registrierung wählen Sie auf der Seite **Einstellungen > Registrierung** die Option **Abgeleitete Anmeldeinformationen (nur iOS)** und klicken Sie auf **Bearbeiten**.

Nach dem Aktivieren abgeleiteter Anmeldeinformationen enthält der **Geräteregistrierungsbericht** in der Spalte **Registrierungsmodus** den Eintrag **derived_credentials**.

> **Wichtig:**
>
> Starten Sie XenMobile Server neu, nachdem Sie den Anbieter für abgeleitete Anmeldeinformationen hinzugefügt haben.

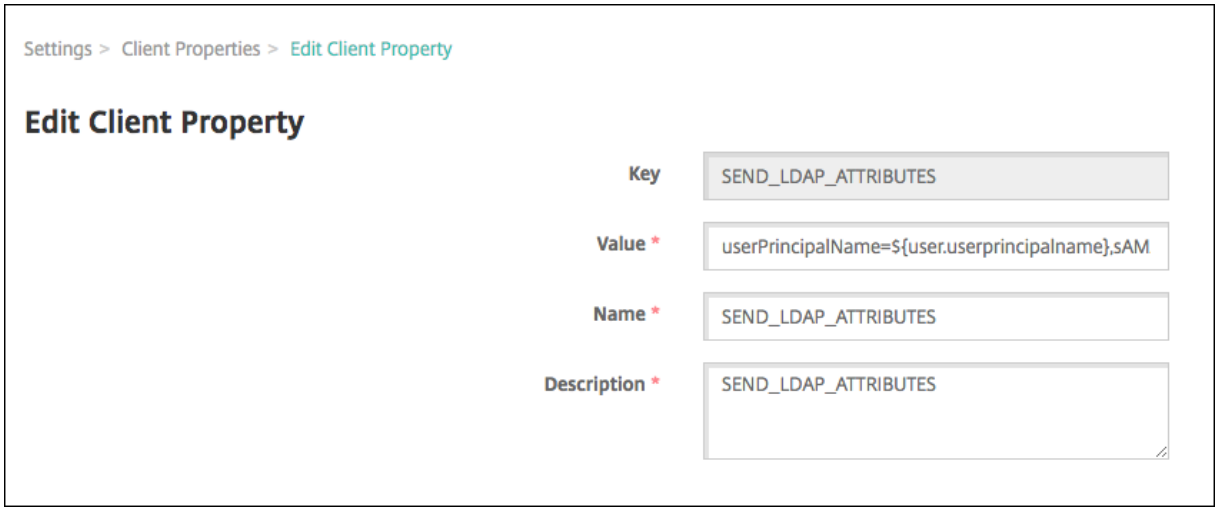
Konfigurieren von XenMobile Server für Secure Mail

Damit Secure Mail abgeleitete Anmeldeinformationen unterstützt, fügen Sie die Clienteigenschaft `SEND_LDAP_ATTRIBUTES` hinzu. Weitere Informationen zum Hinzufügen einer Clienteigenschaft finden Sie unter Clienteigenschaften.

Verwenden Sie die folgenden Informationen für die Clienteigenschaft:

- **Schlüssel:** `SEND_LDAP_ATTRIBUTES`
- **Wert:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.`

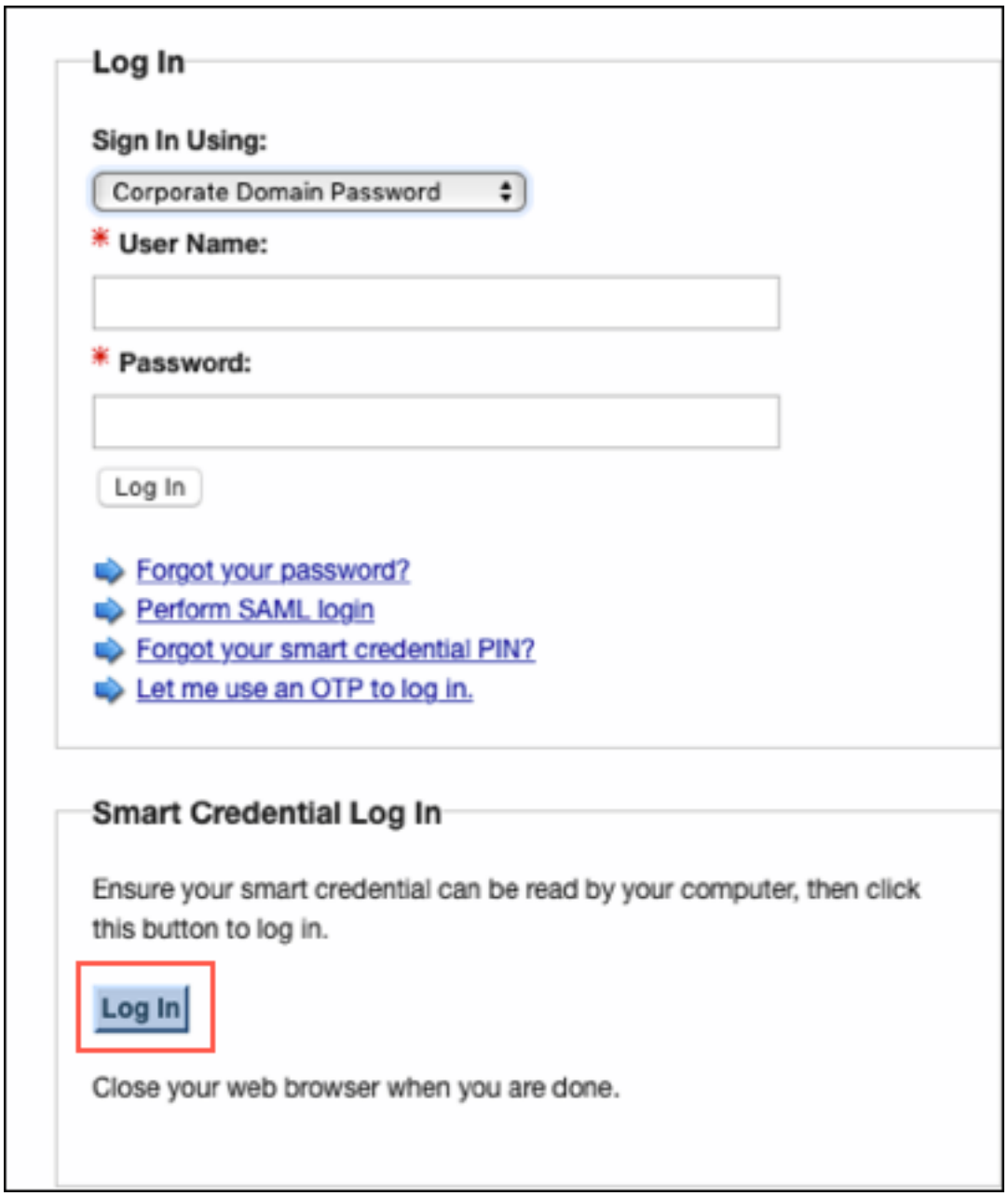

```
    mail }
```



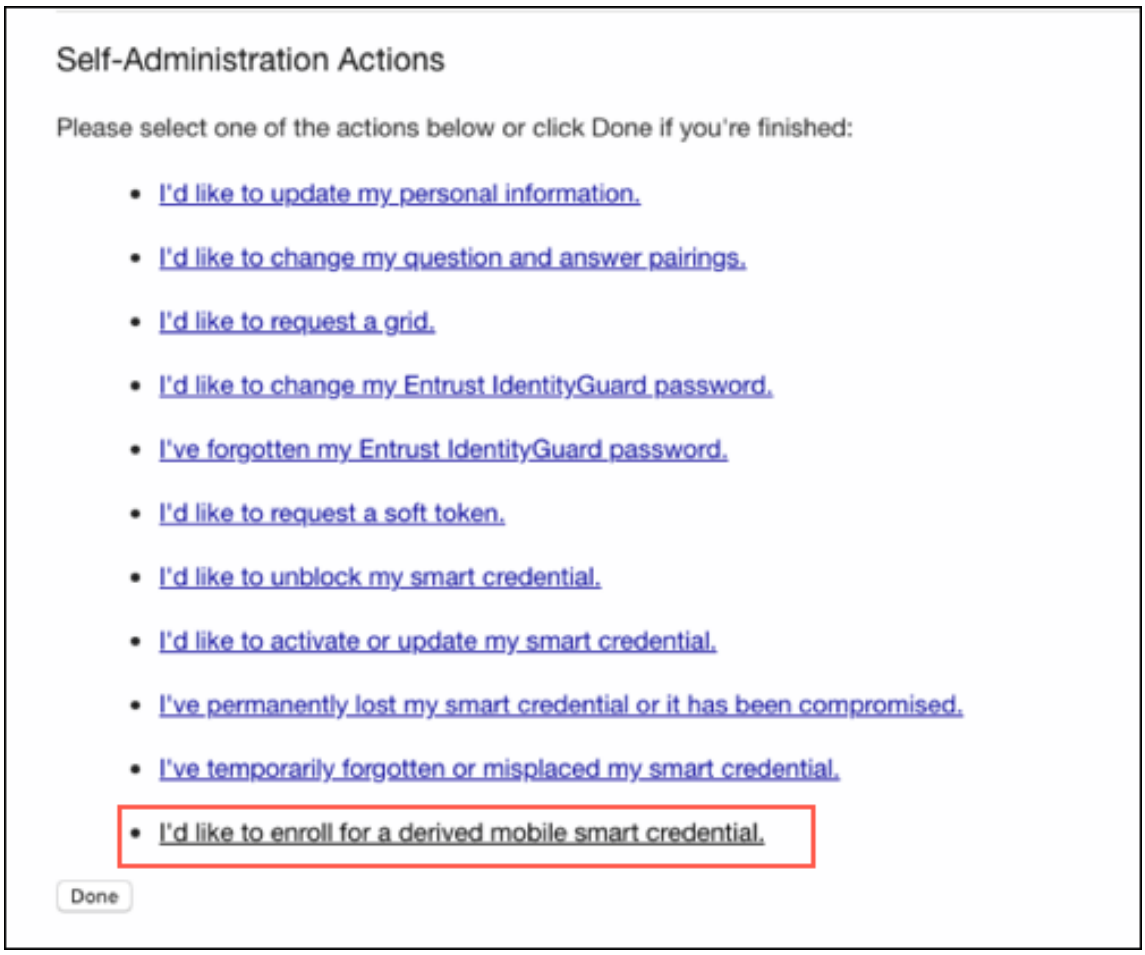
Aktivieren abgeleiteter Anmeldeinformationen mit Entrust Datacard auf iOS-Geräten

> **Hinweis:**
>
> Löschen Sie für die Entrust-Website den Browsercache, wenn Sie die PIV-Karte wechseln.

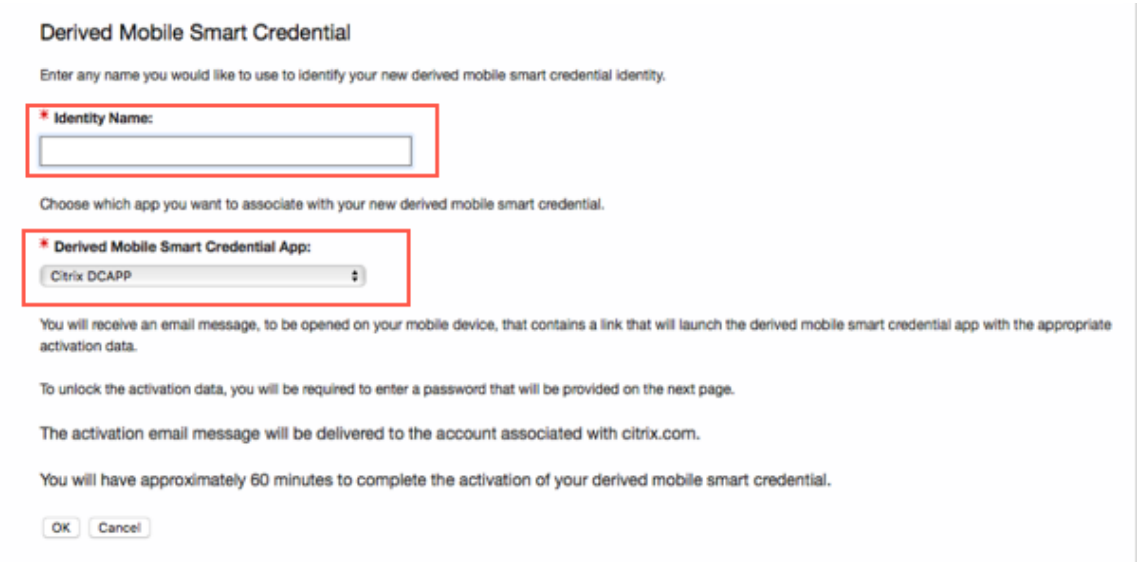
1. Um neue Smart-Anmeldeinformationen anzufordern, verwenden Sie einen Desktopcomputer oder ein beliebiges Gerät zur Anmeldung bei der Entrust-Website. Melden Sie sich mit der Schaltfläche **Smart Credential Login** unten auf der Webseite an. Die Benutzer legen ihre Smartcard in einen an den Desktop angeschlossenen Smartcardleser ein.



2. Wählen Sie unter **Self-Administration Actions** die Option **I'd like to enroll for a derived mobile smart credential** und klicken Sie auf **Done**.



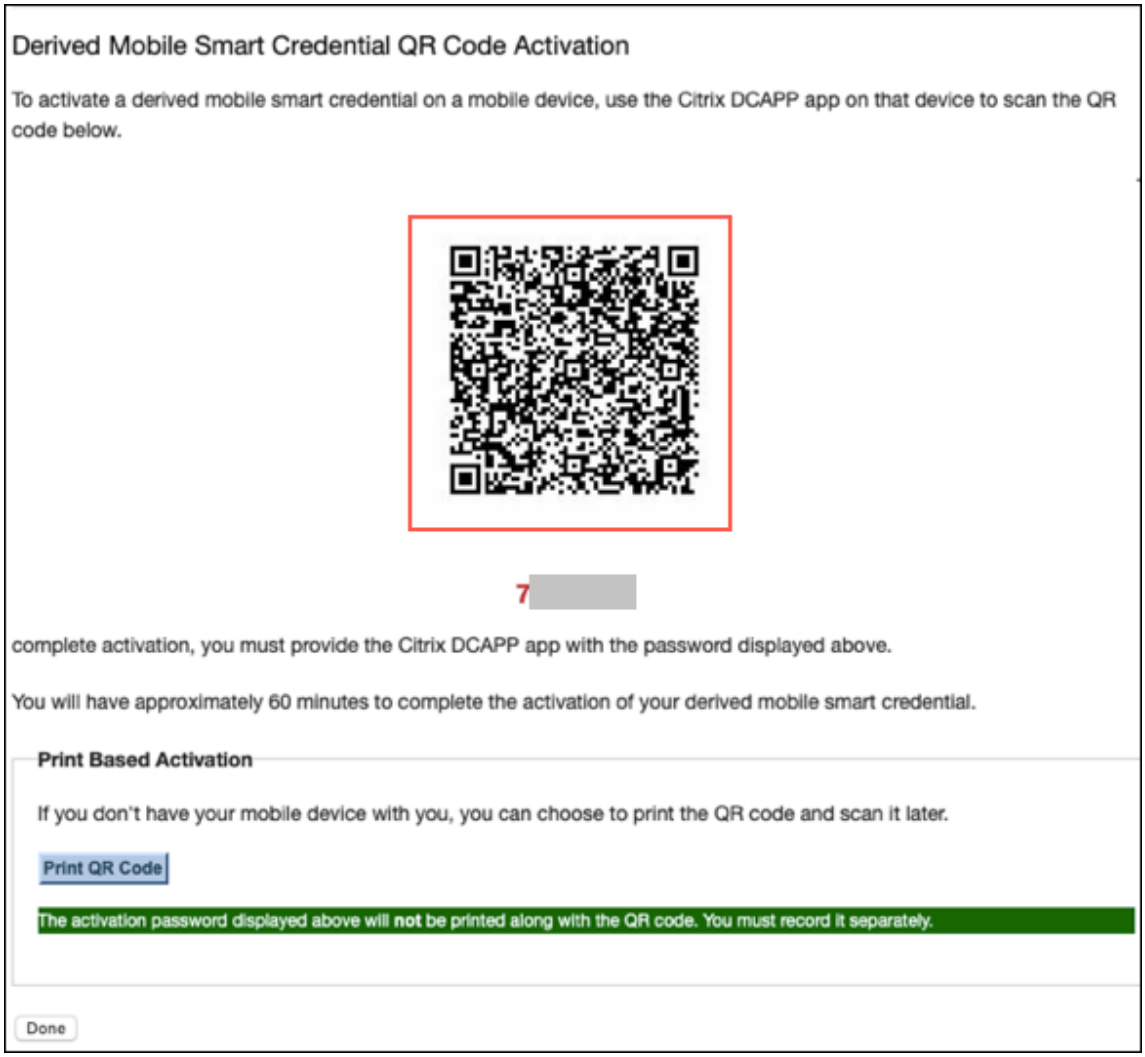
3. Geben Sie auf der Seite **Derived Mobile Smart Credential** den Namen im Feld **Identity Name** ein. Der Benutzer kann einen eindeutigen Namen (Benutzernamen oder ID-Nummer) wählen.
4. Wählen Sie im Menü der App für abgeleitete Anmeldeinformationen **Citrix DCAPP** und klicken Sie auf **Ok**.



Ein Bildschirm zur Aktivierung des QR-Codes wird angezeigt und der Benutzer aufgefordert, den Code mit seinem Mobilgerät zu scannen.

> **Hinweis:**
>
> Standardmäßig läuft der QR-Code nach 3 Minuten ab.

5. Scannen Sie den QR-Code mit **Derived Credential Manager** auf dem Gerät, um die Aktivierung durchzuführen.

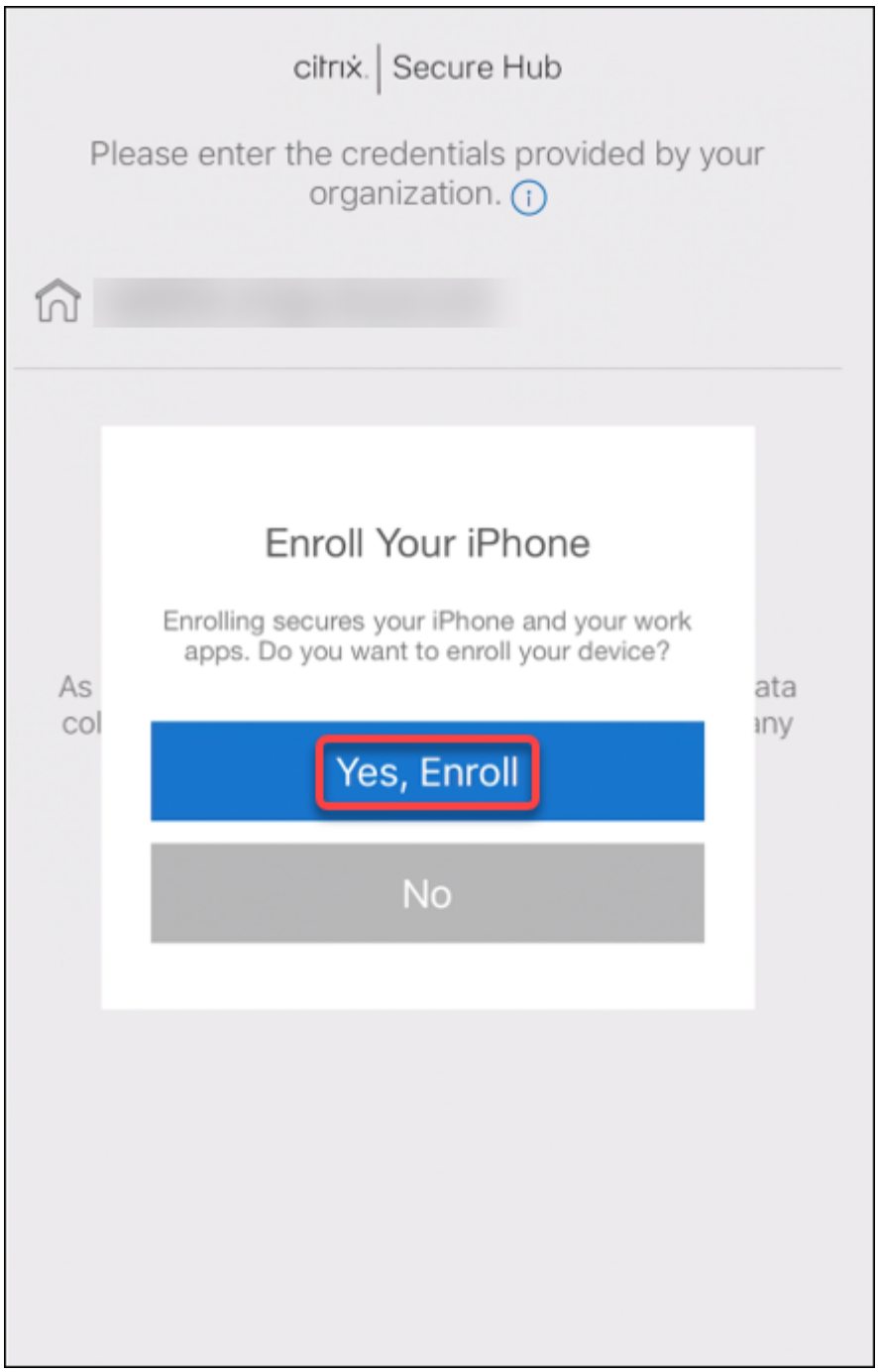


Geräteregistrierung

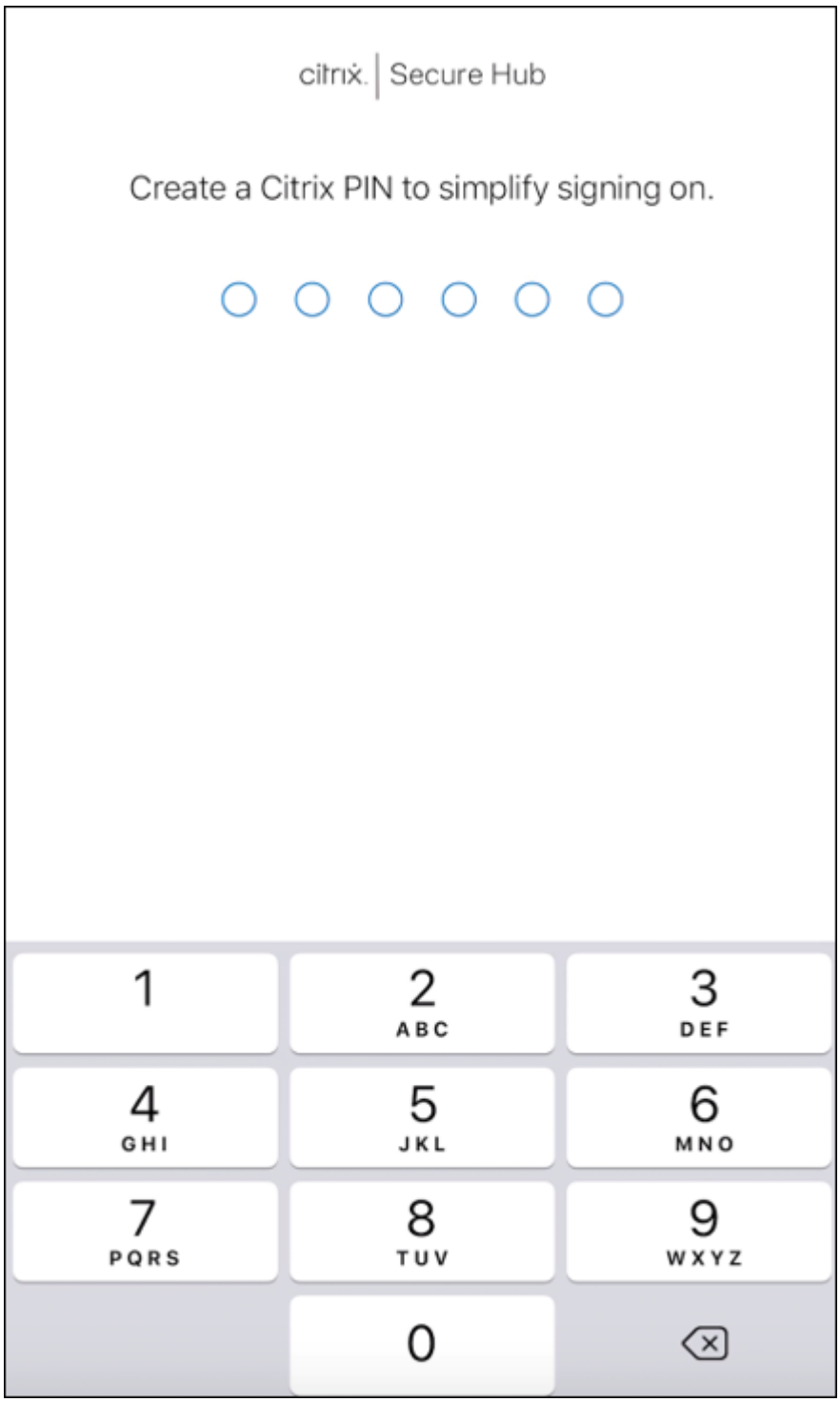
Wenn Sie die weiter oben beschriebene Einrichtung abgeschlossen haben, können die Benutzer ihre Geräte unter Verwendung abgeleiteter Anmeldeinformationen registrieren.

> **Hinweis:**
>
> Die Screenshots in diesem Abschnitt zeigen als Beispiel "Entrust Datacard".

1. Tippen Sie auf **Secure Hub**, um die App zu öffnen. Wenn Sie dazu aufgefordert werden, geben Sie den vollqualifizierten Domänennamen für den XenMobile-Server ein und klicken Sie auf **Weiter**.
2. Klicken Sie auf **Ja, Registrieren**. Die Geräteregistrierung wird in Secure Hub gestartet.

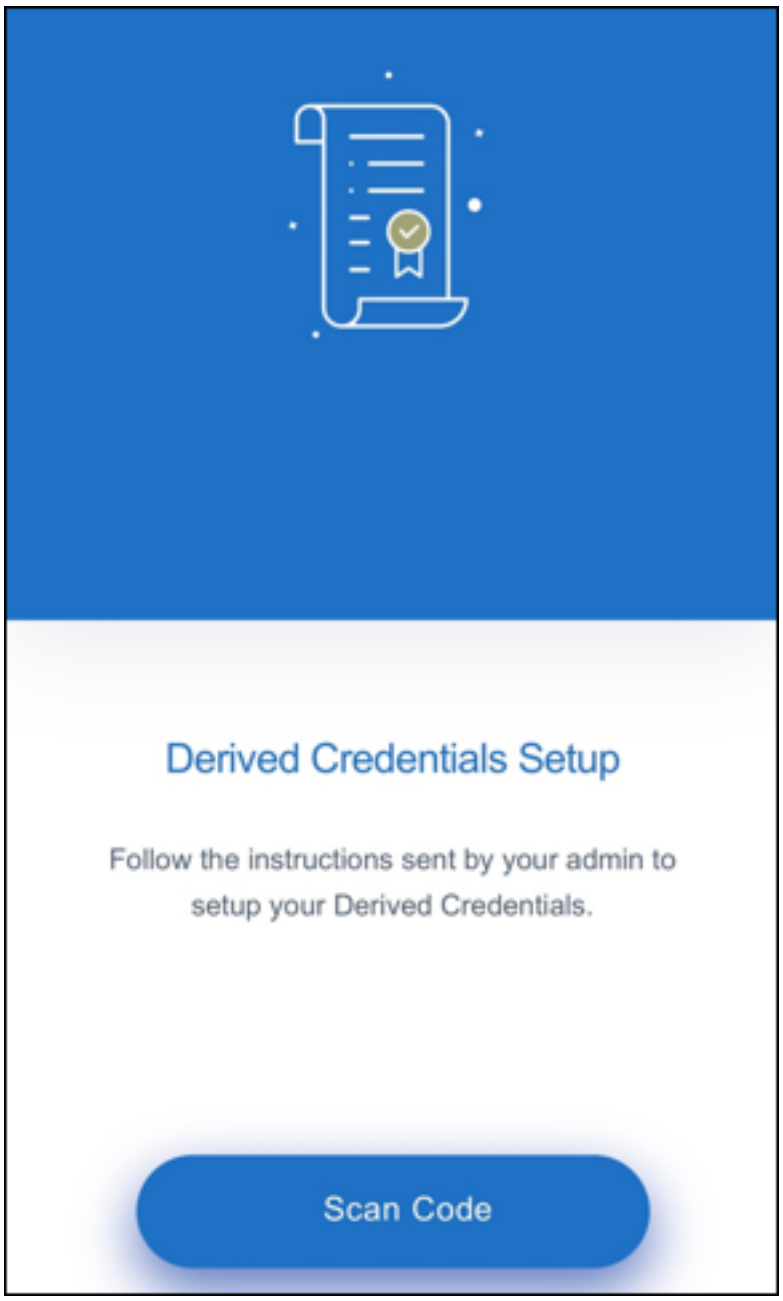


Wenn XenMobile Server abgeleitete Anmeldeinformationen unterstützt, fordert Secure Hub den Benutzer auf, eine Citrix-PIN zu erstellen und zu bestätigen.



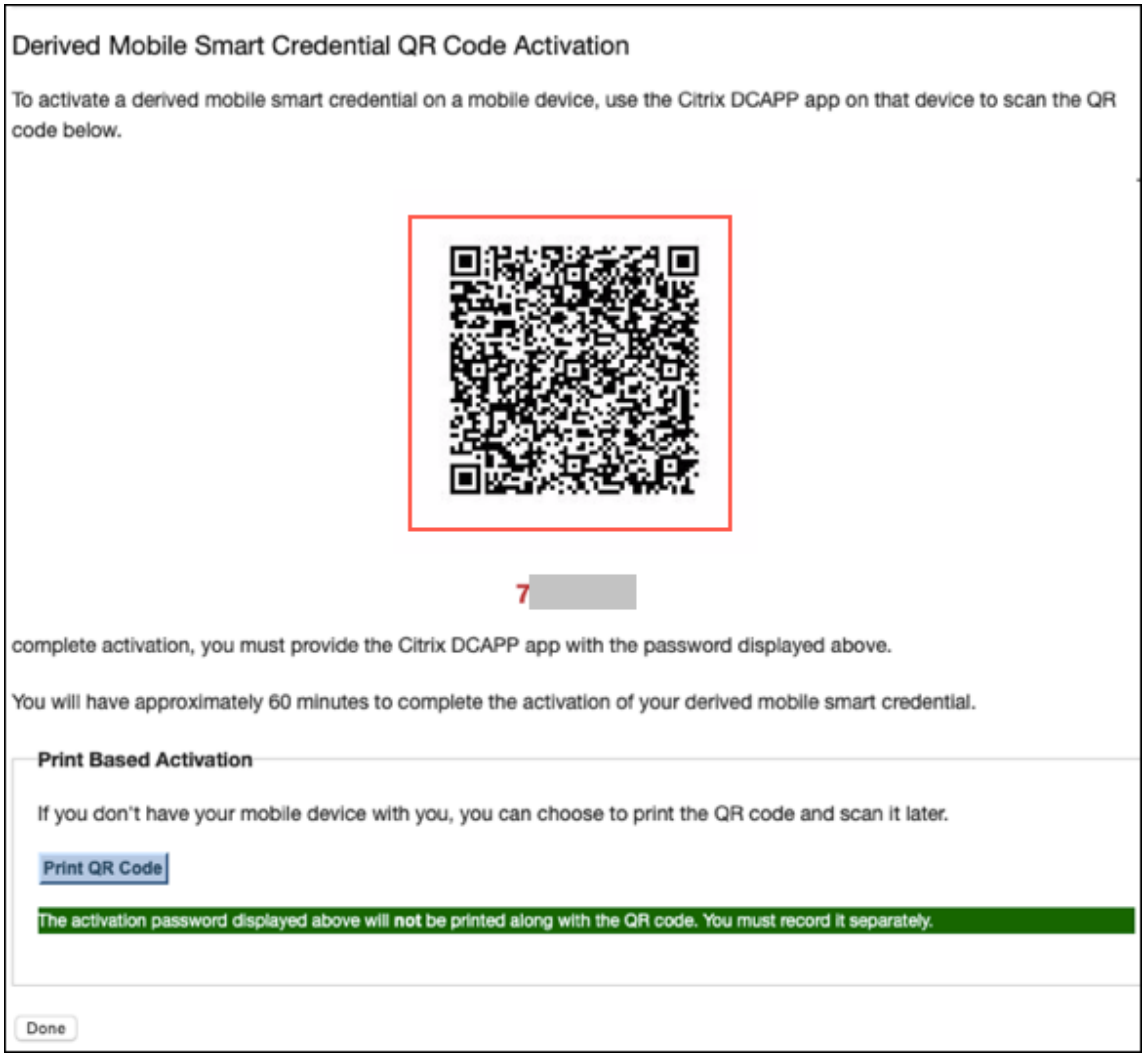
Nach der Bestätigung der Citrix-PIN wird der Begrüßungsbildschirm der App für abgeleitete Anmeldeinformationen angezeigt. Folgen Sie den Anweisungen zum Aktivieren der Smartcard-Anmeldeinformationen.

3. Tippen Sie auf **Scan code**. Die Mobiltelefonkamera wird aktiviert.

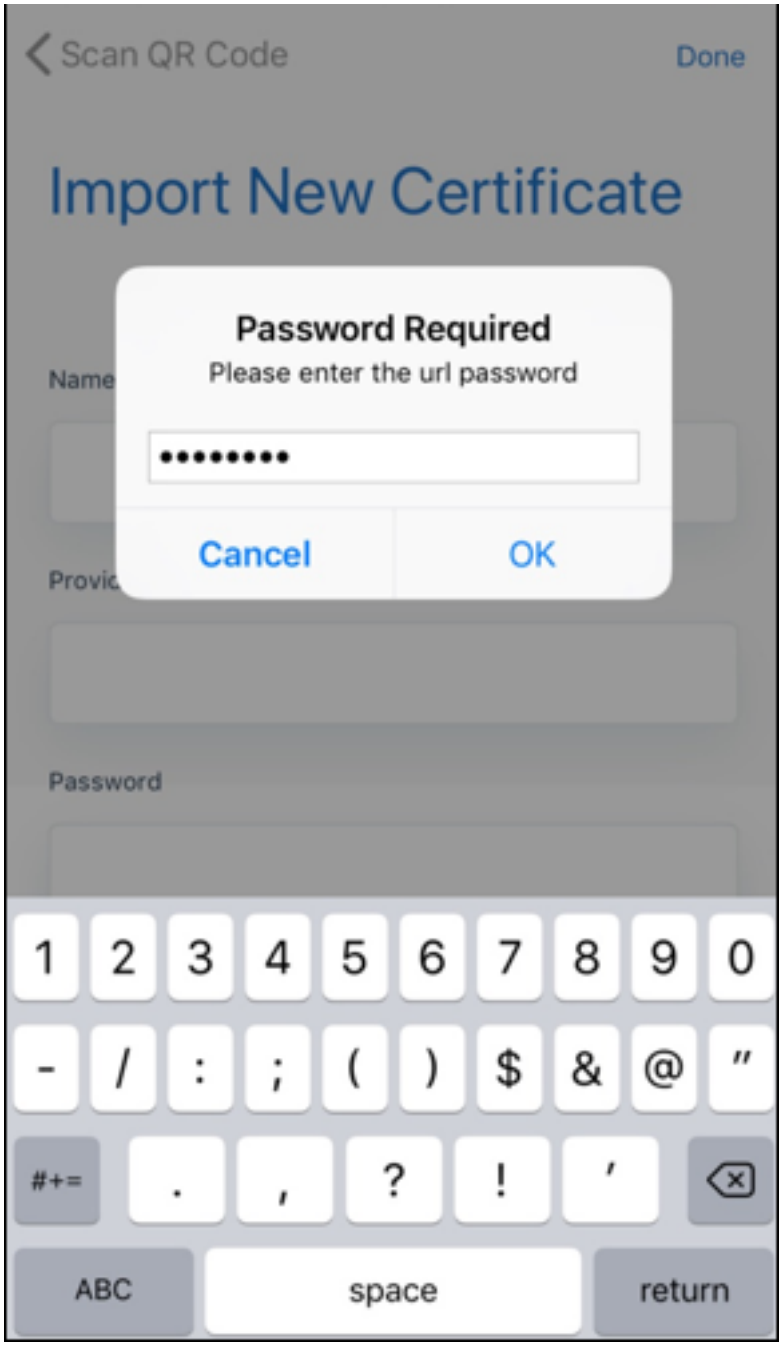


> **Hinweis:**
>
> Um den QR-Code zu scannen, stellen Sie sicher, dass die Kamera und das Mikrofon aktiviert sind und über die erforderlichen Zugriffsberechtigungen verfügen.

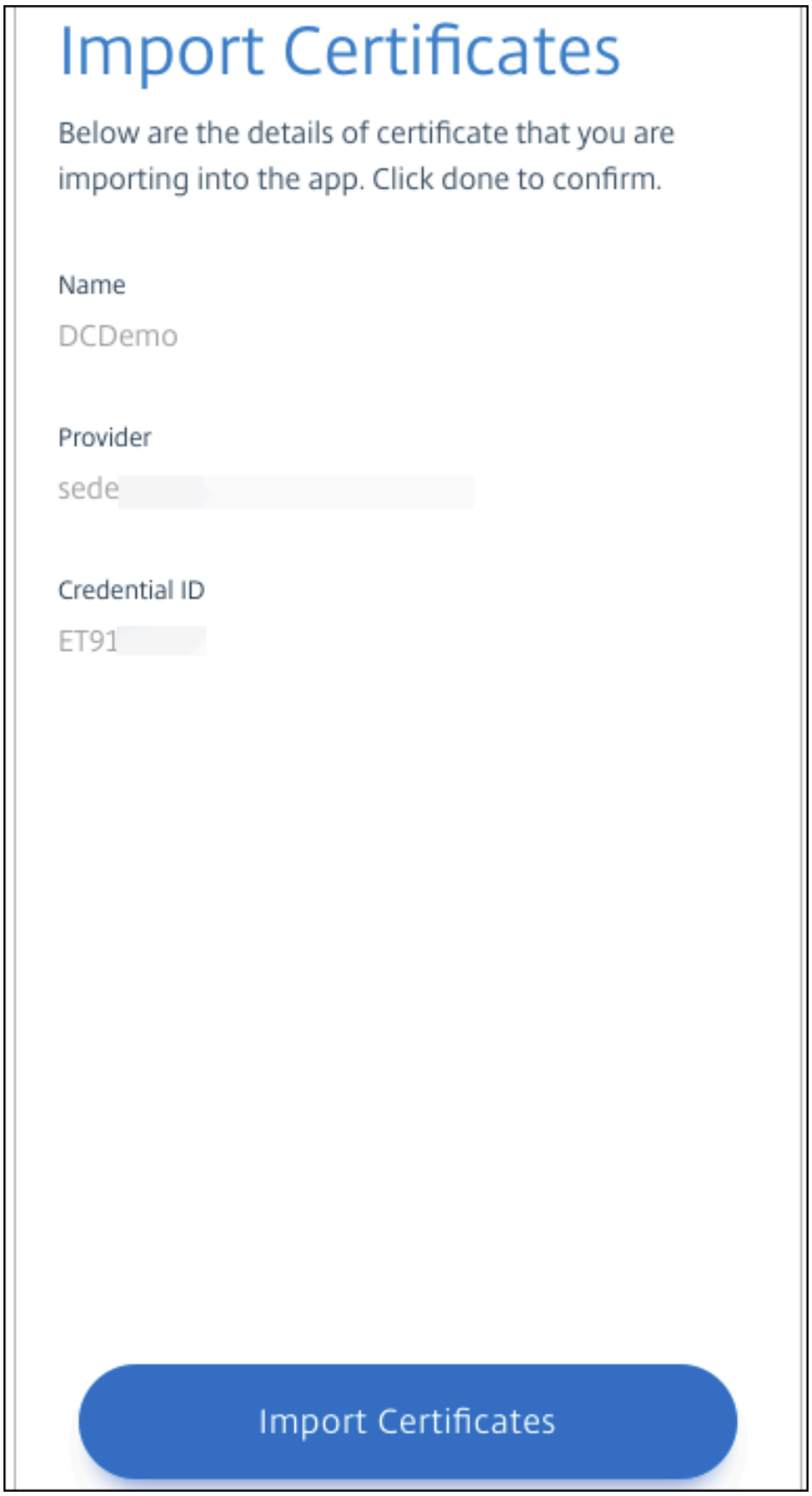
4. Scannen Sie in der App für abgeleitete Anmeldeinformationen den QR-Code, der bei früheren Schritten erstellt wurde.



5. Nach dem Scannen des QR-Codes wird auf dem Bildschirm **Import New Certificate** ein Dialogfeld angezeigt. Geben Sie hier das Kennwort ein und klicken Sie auf **OK**.



Der Bildschirm **Import New Certificate** wird mit automatisch aufgefüllten Feldern angezeigt.



6. Nachdem die Zertifikate erfolgreich hinzugefügt wurden, klicken Sie im Bildschirm **Derived Credentials** auf **Continue to Secure Hub**.

7. Geben Sie in Secure Hub eine neue PIN ein, wenn Sie dazu aufgefordert werden.

   Nach der Authentifizierung der PIN lädt Secure Hub die Zertifikate herunter. Folgen Sie den Anweisungen zum Abschließen der Registrierung.

Anzeigen von Geräteinformationen in der XenMobile-Konsole

- Gehen Sie zu **Verwalten** > **Geräte** und wählen Sie ein Gerät aus, um ein Befehlsfeld anzuzeigen. Klicken Sie auf **Mehr anzeigen**.
- Gehen Sie zu **Analysieren** > **Dashboard**.

Upgrade

September 24, 2021

> **Tipp: XenMobile Migration Service**
>
> Wenn Sie die On-Premises-Version von XenMobile Server verwenden, hilft Ihnen unser kostenloser XenMobile Migration Service beim Start in Endpoint Management. Die Migration von XenMobile Server zu Citrix Endpoint Management erfordert keine erneute Registrierung von Geräten.
>
> Weitere Informationen erhalten Sie bei Ihrem lokalen Citrix Vertriebsmitarbeiter, Systems Engineer oder Citrix Partner. In diesen Blogs wird der XenMobile Migration Service erläutert:
>
> New XenMobile Migration Service
>
> Making the Case for XenMobile in the Cloud

Vor dem Upgrade auf XenMobile 10.14

1. Aktualisieren Sie den Citrix Lizenzserver auf 11.16 oder höher, bevor Sie die aktuelle Version von XenMobile Server 10.14 installieren.

   Die neueste Version von XenMobile erfordert Citrix Lizenzserver 11.16 (Mindestversion).

   Das Customer Success Services-Datum (bisher “Subscription Advantage”-Datum) in XenMobile 10.14 ist der 15. September 2021. Das Customer Success Services-Datum der Citrix Lizenz muss nach diesem Datum liegen. Das Datum wird neben der Lizenz auf dem Lizenzserver angezeigt. Wenn Sie die aktuelle Version von XenMobile mit einer älteren Lizenzserverumgebung verbinden, schlägt die Konnektivitätsprüfung fehl und der Lizenzserver kann nicht konfiguriert werden.

   Zum Verlängern des Datums für Ihre Lizenz laden Sie die aktuelle Lizenzdatei vom Citrix Portal herunter und laden Sie sie in den Lizenzserver hoch. Weitere Informationen finden Sie unter Customer Success Services.

2. Clusterumgebungen: Für die Bereitstellung von iOS-Richtlinien und -Apps auf Geräten mit iOS 11 oder später gilt folgende Anforderung. Ist Citrix Gateway für SSL-Persistenz konfiguriert, müssen Sie auf allen XenMobile Server-Knoten Port 80 öffnen.
3. Wenn die virtuelle Maschine mit dem zu aktualisierenden XenMobile Server weniger als 8 GB RAM hat, sollten Sie den RAM auf mindestens 8 GB erhöhen.
4. Empfehlung: Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine zum Erstellen eines Systemsnapshots. Sichern Sie außerdem die Konfigurationsdatenbank des Systems. Sollten bei einem Upgrade Probleme auftreten, können Sie mit vollständigen Backups eine Wiederherstellung vornehmen.

Ausführen des Upgrades

Sie können ein direktes Upgrade auf XenMobile 10.14 von XenMobile 10.13.x oder 10.12.x ausführen. Um das Upgrade durchzuführen, laden Sie die neueste verfügbare Binärdatei herunter: https://www.citrix.com/downloads. Navigieren Sie zu **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. Klicken Sie auf der Kachel der XenMobile Server-Software für Ihren Hypervisor auf **Datei herunterladen**. Verwenden Sie zum Hochladen des Upgrades die Seite **Releasemanagement** der XenMobile-Konsole.

Upgrade über die Seite “Releasemanagement”

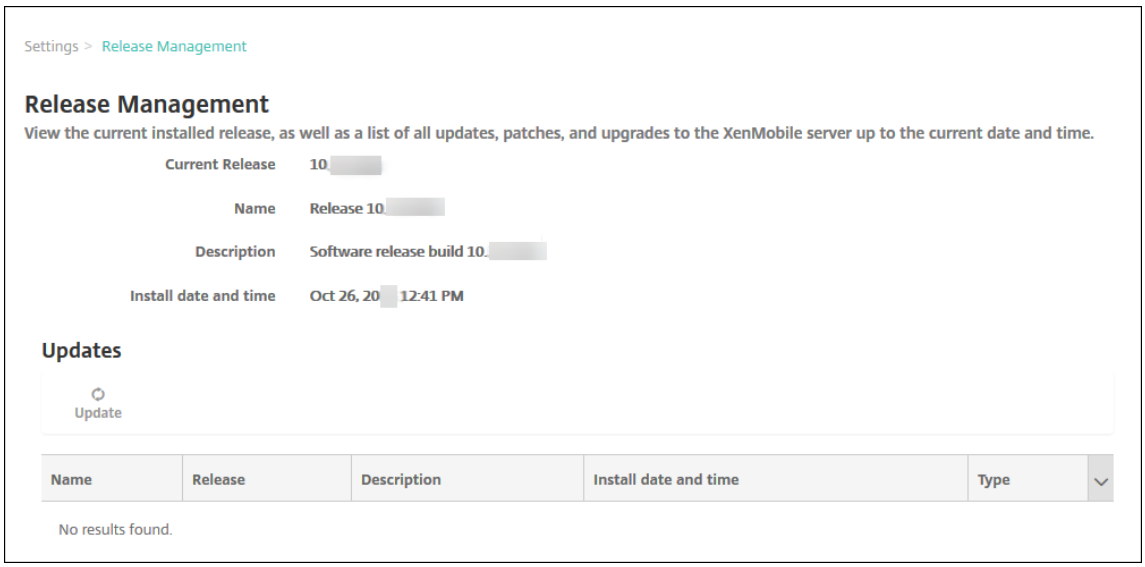
Verwenden Sie die Seite **Releasemanagement** für das Upgrade auf die aktuelle Version von XenMobile Server.

Voraussetzungen:

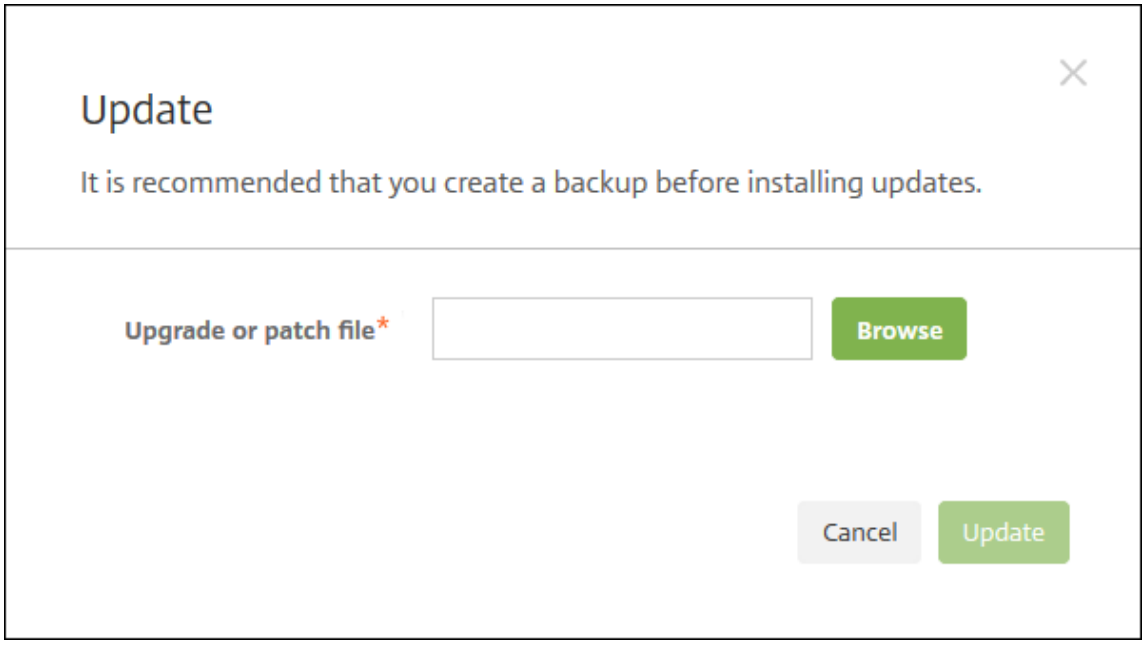
- Lesen Sie die Informationen zu den Systemanforderungen.

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

1. Laden Sie die neueste verfügbare Binärdatei herunter: Gehen Sie zu https://www.citrix.com/downloads. Navigieren Sie zu **Citrix Endpoint Management (und Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**. Klicken Sie auf der Kachel der XenMobile Server-Software für Ihren Hypervisor auf **Datei herunterladen**.
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 heruntergeladenen 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 auf den Zustand vor dem Update zurückgesetzt.

Nach dem Upgrade

Nach einem Upgrade ist ein Neustart von XenMobile erforderlich. Verwenden Sie die XenMobile-CLI für den Neustart von XenMobile Server. Leeren Sie den Browsercache nach dem Neustart des Systems.

Wenn Funktionen, für die ausgehende Verbindungen eingesetzt werden, nicht mehr funktionieren und Sie die Verbindungskonfiguration nicht geändert haben, überprüfen Sie das XenMobile Server-Protokoll auf Fehlermeldungen wie etwa "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer."

Ein Fehler bei der Zertifikatvalidierung bedeutet, dass Sie die Hostnamenüberprüfung unter XenMobile Server deaktivieren müssen. In der Standardeinstellung ist die Hostnamenüberprüfung für ausgehende Verbindungen mit Ausnahme des Microsoft PKI-Servers aktiviert. Wenn die Hostnamenüberprüfung Fehler in der Bereitstellung verursacht, ändern Sie die Servereigenschaft **disable.hostname.verification** in **True**. Der Standardwert dieser Eigenschaft ist **false**.

Citrix veröffentlicht neue Versionen oder wichtige Updates von XenMobile auf Citrix.com. Gleichzeitig wird eine Benachrichtigung an die Kontaktperson jedes Kunden gesendet.

Upgrade von XenMobile-Clusterbereitstellungen

> **Wichtig:**
>
> Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine (VM) zum Erstellen eines Systemsnapshots. Sichern Sie außerdem die Konfigurationsdatenbank des Systems. Sollten bei einem Upgrade Probleme auftreten, können Sie mit vollständigen Backups eine Wiederherstellung vornehmen.

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 über das **Systemmenü** der Befehlszeilenschnittstelle herunter.
3. Starten Sie einen Knoten über das **Systemmenü** der Befehlszeilenschnittstelle und prüfen Sie, ob der Dienst ausgeführt wird.
4. Starten Sie die anderen Knoten nacheinander.

   Falls XenMobile das Update nicht erfolgreich durchführen kann, wird eine Fehlermeldung zu dem Problem angezeigt. XenMobile setzt dann das System auf den Zustand vor dem Update zurück.

Upgrade von XenMobile MDM Edition auf Enterprise Edition

Sie können für iOS- und Android-Geräte ein Upgrade der XenMobile MDM Edition auf die XenMobile Enterprise Edition durchführen.

Voraussetzungen

- Die entsprechende Enterprise-Lizenz.
- Citrix Gateway ist konfiguriert.

Ausführen des Upgrades

1. Gehen Sie zu **Einstellungen > Lizenzierung** und stellen Sie sicher, dass der richtige Lizenztyp der Enterprise Edition hochgeladen wurde.
2. Gehen Sie zu **Einstellungen > Servereigenschaften** und ändern Sie die Eigenschaft **Servermodus** von **MDM** zu **ENT**.
3. Gehen Sie zu **Einstellungen > Citrix Gateway** und konfigurieren Sie die Angaben zu Citrix Gateway. Wählen Sie denselben Authentifizierungsmodus wie für die MDM Edition, nämlich die domänenbasierte Authentifizierung mit Active Directory. Die Änderung des Authentifizierungsmodus nach der Benutzerregistrierung wird in XenMobile nicht unterstützt.
4. Optional: Gehen Sie zu **Einstellungen > Clienteigenschaften** und aktivieren Sie die Authentifizierung mit Citrix-PIN.

Im Anschluss müssen Benutzer folgende Schritte auf dem Gerät ausführen, um in den Enterprise-Modus zu wechseln.

iOS-Benutzer

1. Schließen Sie Secure Hub: Tippen Sie zweimal (schnell) auf die Hometaste des Geräts und schieben Sie die Secure Hub-App nach oben.
2. Öffnen Sie Secure Hub.

Android-Benutzer

1. Öffnen Sie Secure Hub.
2. Gehen Sie zu **Einstellungen > Geräteinformationen**.
3. Klicken Sie auf **Richtlinie aktualisieren**.

Bei aktivierter Authentifizierung mit Citrix-PIN werden Benutzer von Secure Hub aufgefordert, eine PIN zu erstellen. Nach dem Erstellen der PIN wird das Gerät von XenMobile im Enterprise-Modus konfiguriert. In der XenMobile-Konsole werden dann auf der Seite **Verwalten > Geräte** MDM und MAM als aktiver Modus für das Gerät angezeigt.

Benutzerkonten, Rollen und Registrierungseinstellungen

January 5, 2022

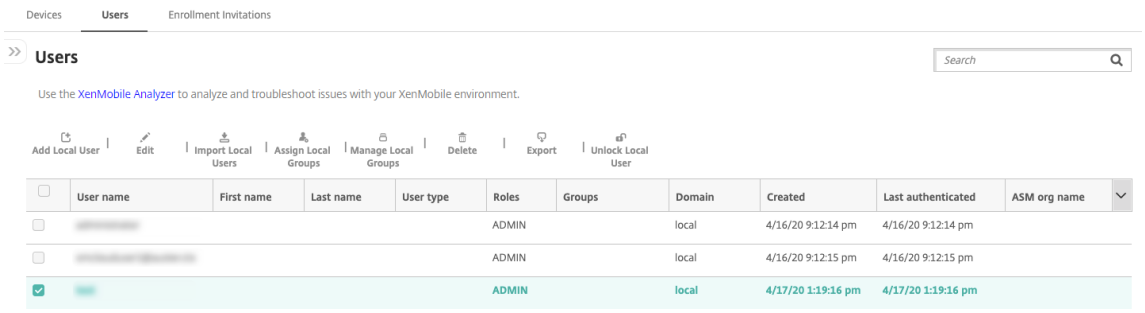
Sie konfigurieren die folgenden Elemente in der XenMobile-Konsole auf der Registerkarte **Verwalten** und der Seite **Einstellungen**. Sofern nicht anders angegeben, finden Sie in diesem Artikel die Schritte für die folgenden Aufgaben.

- Benutzerkonten und Gruppen:
  - Unter **Verwalten > Benutzer** fügen Sie manuell Benutzerkonten hinzu oder verwenden Sie eine CSV-Provisioningdatei, um die Konten zu importieren und lokale Gruppen zu verwalten.
  - Unter **Einstellungen > Workflows** verwenden Sie die Workflows, um das Erstellen und Entfernen von Benutzerkonten zu verwalten.
- Rollen für Benutzerkonten und Gruppen
  - Unter **Einstellungen > Rollenbasierte Zugriffssteuerung** weisen Sie Benutzern und Gruppen vordefinierte Rollen bzw. Berechtigungssätze zu. Diese Berechtigungen steuern den Zugriff der Benutzer auf Systemfunktionen. Weitere Informationen finden Sie unter Konfigurieren von Rollen mit RBAC.
  - Unter **Einstellungen > Benachrichtigungsvorlagen** erstellen oder aktualisieren Sie Benachrichtigungsvorlagen, um sie in automatisierten Aktionen, bei der Registrierung und für Standardbenachrichtigungen an Benutzer zu verwenden. Sie können Benachrichtigungsvorlagen zum Senden von Nachrichten über drei verschiedene Kanäle konfigurieren: Secure Hub, SMTP oder SMS. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Benachrichtigungsvorlagen.
- Registrierungssicherheitsmodus und Registrierungseinladungen
  - Unter **Einstellungen > Registrierung** können Sie bis zu sieben Registrierungssicherheitsmodi konfigurieren und auch Registrierungseinladungen versenden. Jeder Registrierungssicherheitsmodus hat eine eigene Sicherheitsstufe und erforderliche Schritte zum Registrieren von Geräten.
  - Aktivieren der Autodiscovery für die Benutzerregistrierung in XenMobile

Erstellen, Bearbeiten, Entsperren 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.

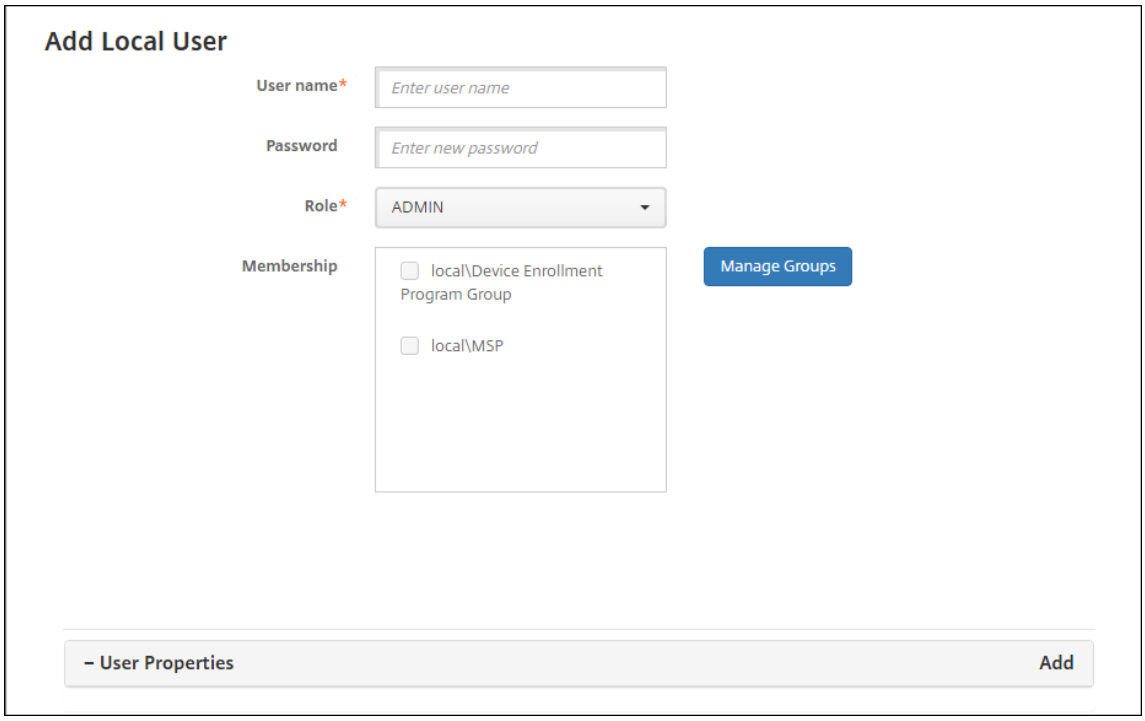
1. Klicken Sie in der XenMobile-Konsole auf **Verwalten > Benutzer**. Die Seite **Benutzer** wird angezeigt.



2. Klicken Sie auf **Filter anzeigen**, um die Liste zu filtern.

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 Namen ein. Dies ist ein erforderliches Feld. Namen dürfen Leerstellen sowie Groß- und Kleinbuchstaben enthalten.
   - **Kennwort:** Geben Sie ein optionales Benutzerkennwort ein. Das Kennwort muss mindestens 14 Zeichen lang sein und alle der folgenden Kriterien erfüllen:
     - Mindestens zwei Ziffern
     - Mindestens ein Groß- und ein Kleinbuchstabe
     - Mindestens ein Sonderzeichen

  - Nutzen Sie keine Wörter, die im Wörterbuch enthalten oder eingeschränkt verwendbar sind, zum Beispiel Ihren Citrix-Benutzernamen oder die E-Mail-Adresse.
  - Verwenden Sie maximal drei aufeinanderfolgende oder identische Zeichen oder Tastaturmuster, also nicht 1111, 1234 oder asdf.
- **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 Eigenschaft zu speichern, oder klicken Sie auf **Abbrechen**.

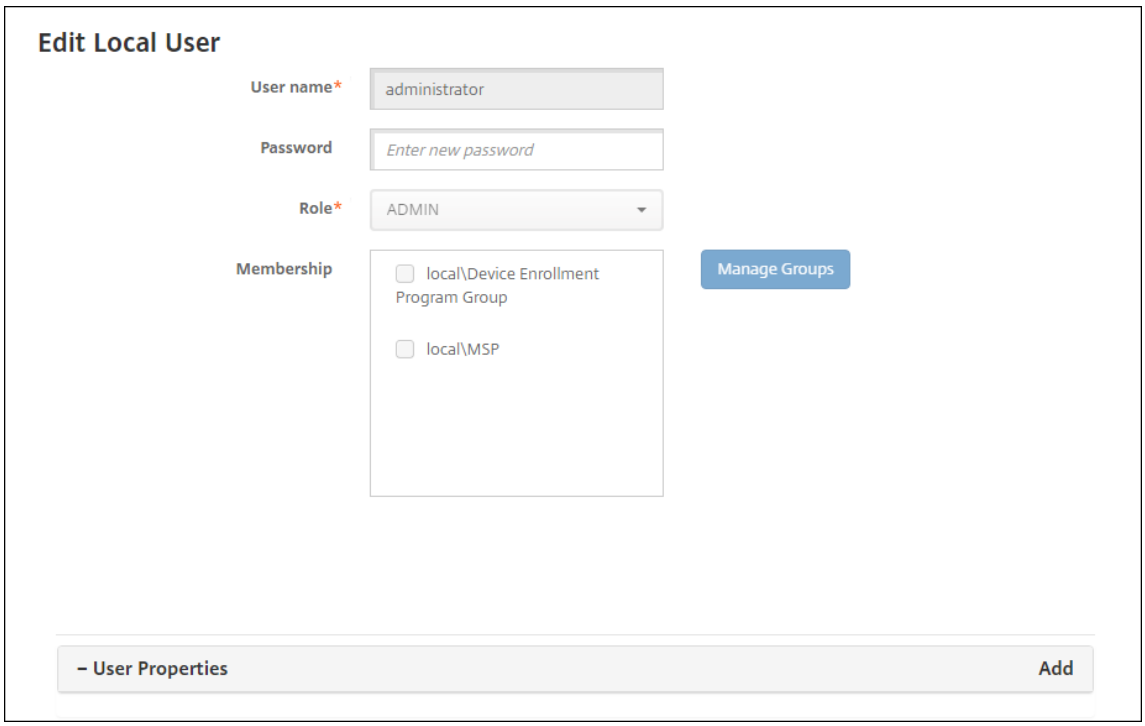
Zum Löschen einer vorhandenen Benutzereigenschaft zeigen Sie auf deren Zeile und klicken Sie auf das X auf der rechten Seite. Die Eigenschaft wird sofort gelöscht.

Zum Bearbeiten einer Benutzereigenschaft klicken Sie 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 Eigenschaft zu speichern, oder klicken Sie auf **Abbrechen**.
     - 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.

Entsperren eines lokalen Benutzerkontos

1. Wählen Sie auf der Seite **Benutzer** in der Liste das Benutzerkonto aus.
2. Klicken Sie auf **Lokalen Benutzer entsperren**. Ein Bestätigungsdialogfeld wird angezeigt.
3. Klicken Sie auf **Entsperren**, um das Benutzerkonto zu entsperren, oder klicken Sie 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.

Sie können mehrere Benutzerkonten auswählen, indem Sie die Kontrollkästchen daneben aktivieren.

1. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt.
2. Klicken Sie zum Löschen des Benutzerkontos auf **Löschen** oder klicken Sie auf **Abbrechen**.

Löschen von Active Directory-Benutzern

Zum Löschen eines oder mehrerer Active Directory-Benutzer wählen Sie den oder die Benutzer aus und klicken Sie auf **Löschen**.

Wenn ein Benutzer, den Sie löschen, registrierte Geräte hat und Sie diese neu registrieren möchten, müssen Sie die Geräte vor der Neuregistrierung löschen. Zum Löschen eines Geräts navigieren Sie zu **Verwalten > Geräte**, wählen Sie das Gerät und klicken Sie auf **Löschen**.

Importieren von Benutzerkonten

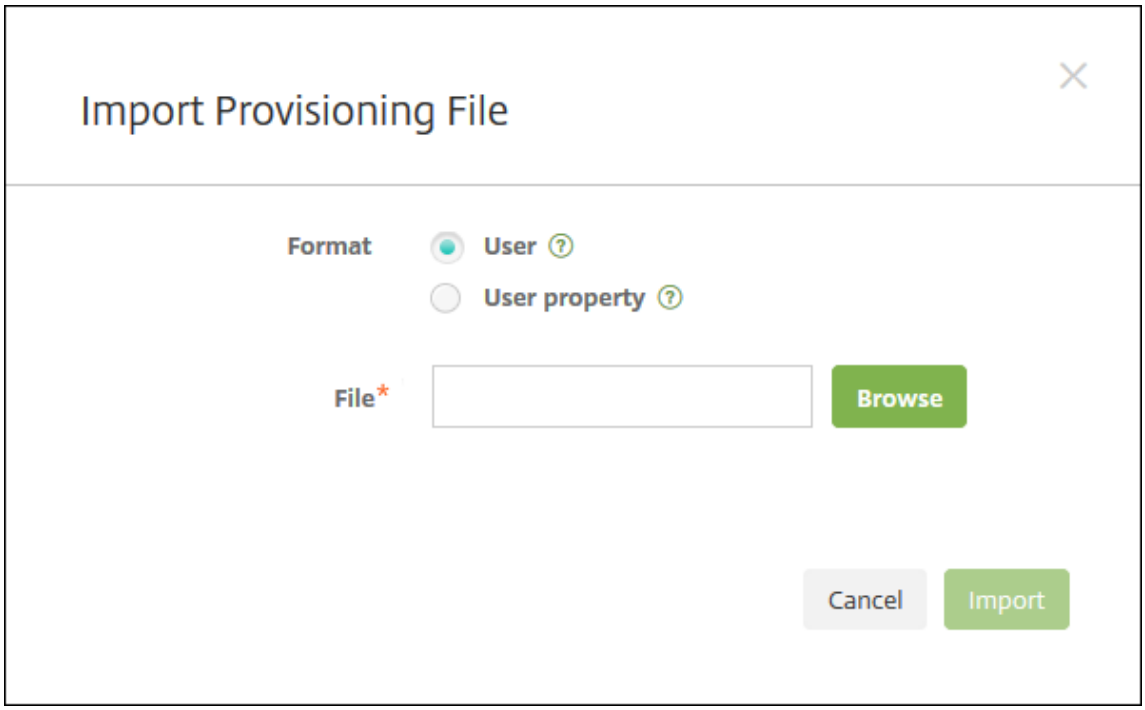
Sie können lokale Benutzerkonten und Eigenschaften aus einer CSV-Datei, einer so genannten Provisioningdatei, importieren, die Sie manuell erstellen können. Informationen zum Formatieren von Provisioningdateien finden Sie unter Provisioningdateiformate.

> **Hinweis:**
>
> - Verwenden Sie für lokale Benutzer den Domänennamen zusammen mit dem Benutzernamen in der Importdatei. Beispiel: Geben Sie username@domain an. Wenn der erstellte oder importierte lokale Benutzer für eine verwaltete Domäne in XenMobile vorgesehen ist, kann der Benutzer 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. Berücksichtigen Sie, dass das Deaktivieren der Domäne sich auf die Registrierung auswirkt. Reaktivieren Sie daher die Standarddomäne nach dem Import der internen Benutzer.

> - Lokale Benutzer können im UPN-Format (Benutzerprinzipalname) angegeben werden. Citrix empfiehlt jedoch, 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. 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

Sie können eine Provisioningdatei manuell erstellen, um Benutzerkonten und Eigenschaften in XenMobile zu importieren. Gültige Formate sind:

- **Felder der Provisioningdatei für Benutzer:** `user;password;role;group1;group2`

- **Felder der Provisioningdatei für Benutzerattribute:** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> **Hinweis:**
>
> - Trennen Sie die Felder in der Provisioningdatei durch Semikola (;). Wenn ein Feld ein Semikolon enthält, schützen Sie es mit einem umgekehrten Schrägstrich (\). Geben Sie beispielsweise die Eigenschaft `propertyV;test;1;2` in der Form `propertyV\\;test\\;1\\;2` in der Provisioningdatei ein.
> - Gültige Werte für **Rolle** sind die vordefinierten Rollen USER, ADMIN, SUPPORT und DEVICE_PROVISIONING sowie alle von Ihnen definierten Rollen.
> - Verwenden Sie den Punkt (.) als Trennzeichen, um Gruppenhierarchien zu erstellen. Verwenden Sie daher keinen Punkt in Gruppennamen.
> - Verwenden Sie Kleinbuchstaben für Eigenschaftsattribute in Attributprovisioningdateien. 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:

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

Ein anderes Beispiel, `AUser0;1.password;USER;ActiveDirectory.test.net`, bedeutet:

- **Benutzer:** `AUser0`
- **Kennwort:** `1.password`
- **Rolle:** `USER`
- **Gruppe:** `ActiveDirectory.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 Registrierungssicherheitsmodi

Konfigurieren Sie bei der Geräteregistrierung einen Sicherheitsmodus, um eine Sicherheitsstufe und eine Benachrichtigungsvorlage für die Geräteregistrierung in XenMobile anzugeben.

XenMobile bietet sieben Registrierungssicherheitsmodi mit verschiedenen Sicherheitsstufen und Schritten, die die Benutzer zum Registrieren von Geräten ausführen müssen. Zum Konfigurieren von Registrierungssicherheitsmodi verwenden Sie in der XenMobile Server-Konsole die Seite **Einstellungen > Registrierung**.

Sie können einige Modi im Selbsthilfeportal zur Verfügung stellen. Benutzer können im Portal Registrierungslinks generieren, mit denen sie ihre Geräte registrieren. Benutzer mit iOS-, iPadOS- und macOS-Geräten, Android Enterprise-Geräten bzw. Android-Legacygeräten können sich optional selbst eine Registrierungseinladung vom Portal senden. Registrierungseinladungen sind für Windows-Geräte nicht verfügbar.

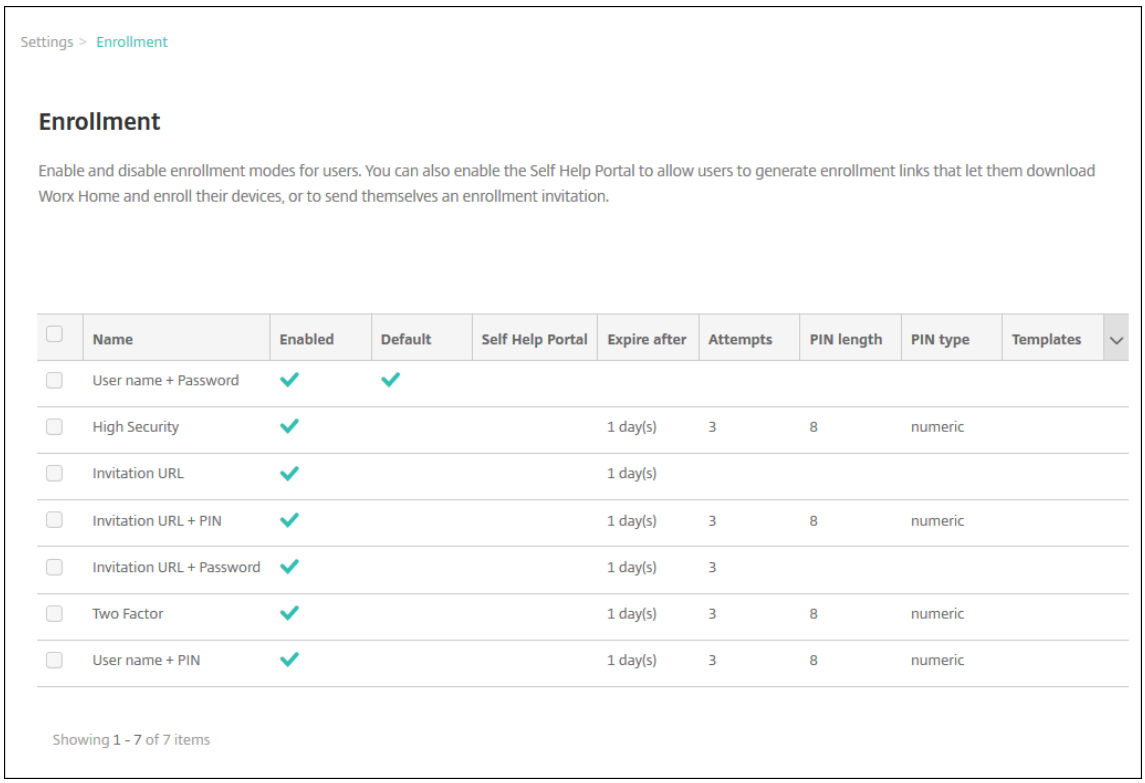
Zum Senden von Registrierungseinladungen verwenden Sie die Seite **Verwalten > Registrierungseinladungen**. Weitere Informationen finden Sie unter Senden von Registrierungseinladungen.

> **Hinweis:**
>
> Wenn Sie benutzerdefinierte Benachrichtigungsvorlagen verwenden möchten, müssen Sie diese vor dem Konfigurieren der Registrierungssicherheitsmodi erstellen. Weitere Informationen über Benachrichtigungsvorlagen finden Sie unter Erstellen und 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 Registrierungssicherheitsmodi. Standardmäßig sind alle Registrierungssicherheitsmodi aktiviert.
3. Wählen Sie einen Registrierungssicherheitsmodus in der Liste zur Bearbeitung aus. Legen Sie diesen Modus als Standard fest, deaktivieren Sie ihn oder erteilen Sie Benutzern Zugriff darauf über das Selbsthilfeportal.

   > **Hinweis:**
   >
   > Wenn Sie das Kontrollkästchen neben einem Registrierungssicherheitsmodus aktivieren, 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.



Folgende Registrierungssicherheitsmodi stehen zur Auswahl:

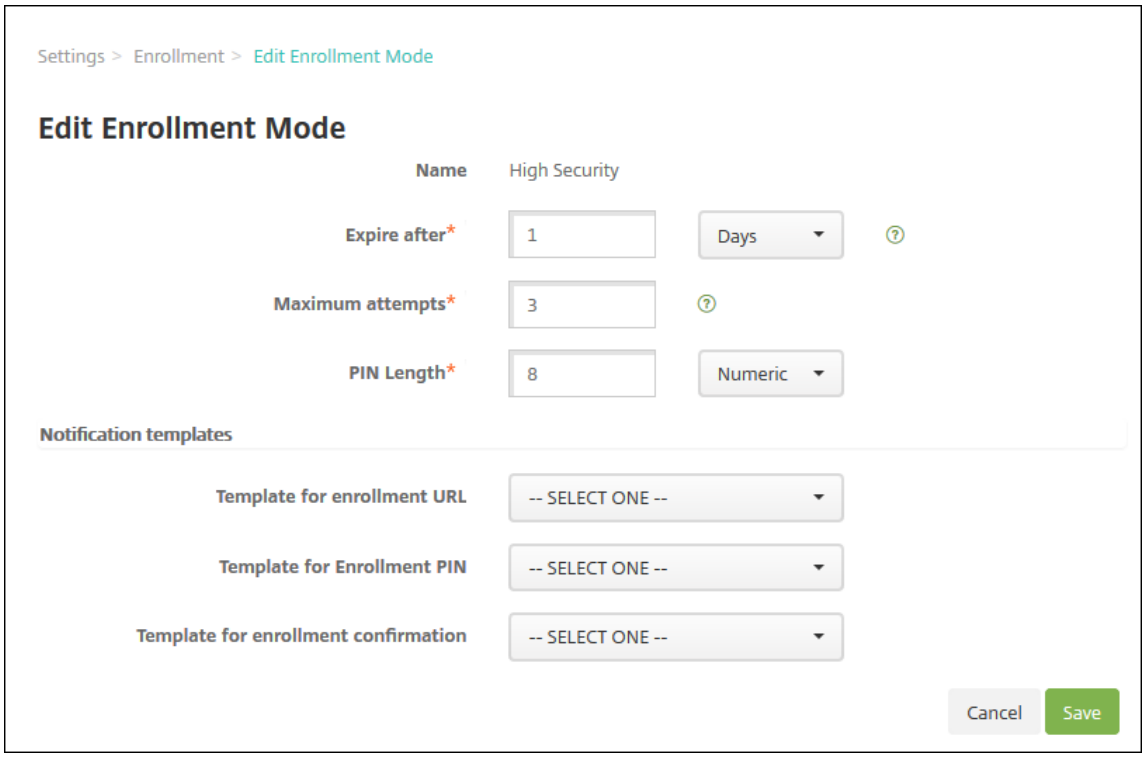
- Benutzername + Kennwort
- Hohe Sicherheit
- Einladungs-URL
- Einladungs-URL + PIN
- Einladungs-URL + Kennwort
- Zweistufige Authentifizierung
- Benutzername + PIN

Mit Registrierungseinladungen können Sie die Registrierung auf Benutzer beschränken, die eine Einladung erhalten haben. Um Registrierungseinladungen zu senden, können Sie nur die Registrierungsicherheitsmodi **Einladungs-URL**, **Einladungs-URL + PIN** oder **Einladungs-URL + Kennwort** verwenden. Für Geräte, die mit **Benutzernamen + Kennwort**, **Zweistufiger Authentifizierung** oder **Benutzername + PIN** registriert werden, müssen Benutzer ihre Anmeldeinformationen manuell in Secure Hub eingeben.

Zur zweistufigen Authentifizierung können Sie Registrierungseinladungen mit Einmal-PIN verwenden. Registrierungseinladungen mit Einmal-PIN steuern die Anzahl der Geräte, die ein Benutzer anmelden kann. OTP-Einladungen sind für Windows-Geräte nicht verfügbar.

Bearbeiten eines Registrierungssicherheitsmodus

1. Wählen Sie in der Liste **Registrierung** einen Registrierungssicherheitsmodus aus und klicken Sie auf **Bearbeiten**. Die Seite **Registrierungsmodus bearbeiten** wird angezeigt. Der ausgewählte Modus bestimmt die angezeigten Optionen.



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.

     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.

     Geben Sie **0** ein, wenn die Anzahl der Versuche beliebig sein soll.

   - **PIN-Länge:** Geben Sie eine Zahl ein, um die Länge der PIN festzulegen.

   - **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. Die Vorlage für Registrierungseinladungen sendet beispielsweise eine E-Mail oder SMS an Benutzer. Das Verfahren hängt von der Konfiguration der Vorlage ab, mit der Benutzer ihre Geräte in XenMobile anmelden können. 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 Registrierungssicherheitsmodus als Standard

Wenn Sie einen Registrierungssicherheitsmodus als Standard festlegen, wird er für alle Geräteregistrierungsanforderungen verwendet, sofern Sie keinen anderen Registrierungssicherheitsmodus auswählen. Wenn kein Registrierungssicherheitsmodus als Standard festgelegt ist, müssen Sie für jede Geräteregistrierung eine eigene Registrierungsanforderung erstellen.

> **Hinweis:**
>
> Sie können nur **Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** als Standardregistrierungssicherheitsmodus festlegen.

1. Wählen Sie **Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** als Standardregistrierungssicherheitsmodus aus.

   Um einen Modus als Standardmodus zu verwenden, müssen Sie ihn zuerst aktivieren.

2. Klicken Sie auf **Standard**. Der ausgewählte Modus ist jetzt der Standardmodus. War zuvor ein anderer Registrierungssicherheitsmodus als Standard festgelegt, ist dieser Modus nun nicht mehr Standardmodus.

Deaktivieren eines Registrierungssicherheitsmodus

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

1. Wählen Sie einen Registrierungssicherheitsmodus aus.

Den Standardregistrierungssicherheitsmodus können Sie nicht deaktivieren. Wenn Sie den Standardregistrierungssicherheitsmodus deaktivieren möchten, müssen Sie zunächst dessen Einstellung als Standard aufheben.

2. Klicken Sie auf **Deaktivieren**. Der Registrierungssicherheitsmodus ist nicht mehr aktiviert.

Aktivieren eines Registrierungssicherheitsmodus im Selbsthilfeportal

Durch Aktivieren eines Registrierungssicherheitsmodus im Selbsthilfeportal können Benutzer ihre Geräte in XenMobile selbst registrieren.

> **Hinweis:**
>
> - Der Registrierungssicherheitsmodus muss aktiviert und an Benachrichtigungsvorlagen gebunden sein, damit er im Selbsthilfeportal zur Verfügung steht.
> - Sie können im Selbsthilfeportal nur jeweils einen Registrierungssicherheitsmodus aktivieren.

1. Wählen Sie einen Registrierungssicherheitsmodus aus.
2. Klicken Sie auf **Selbsthilfeportal**. Der ausgewählte Registrierungssicherheitsmodus steht Benutzern jetzt im Selbsthilfeportal zur Verfügung. Andere für das Selbsthilfeportal aktivierte Modi sind nicht mehr verfügbar.

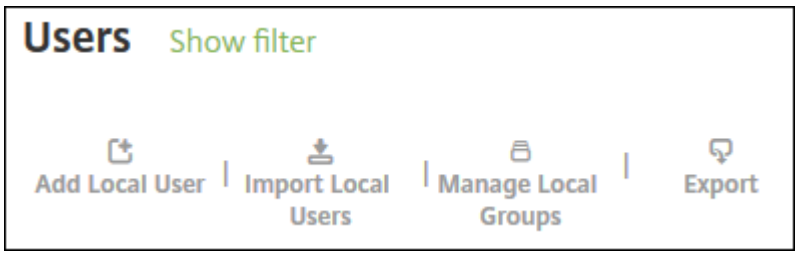
Hinzufügen oder Entfernen von Gruppen

Gruppen werden im Dialogfeld **Gruppen verwalten** in der XenMobile-Konsole auf folgenden Seiten verwaltet: **Benutzer**, **Lokalen Benutzer hinzufügen** oder **Lokalen Benutzer bearbeiten**. Es gibt keinen spezifischen Befehl zum Bearbeiten von Gruppen.

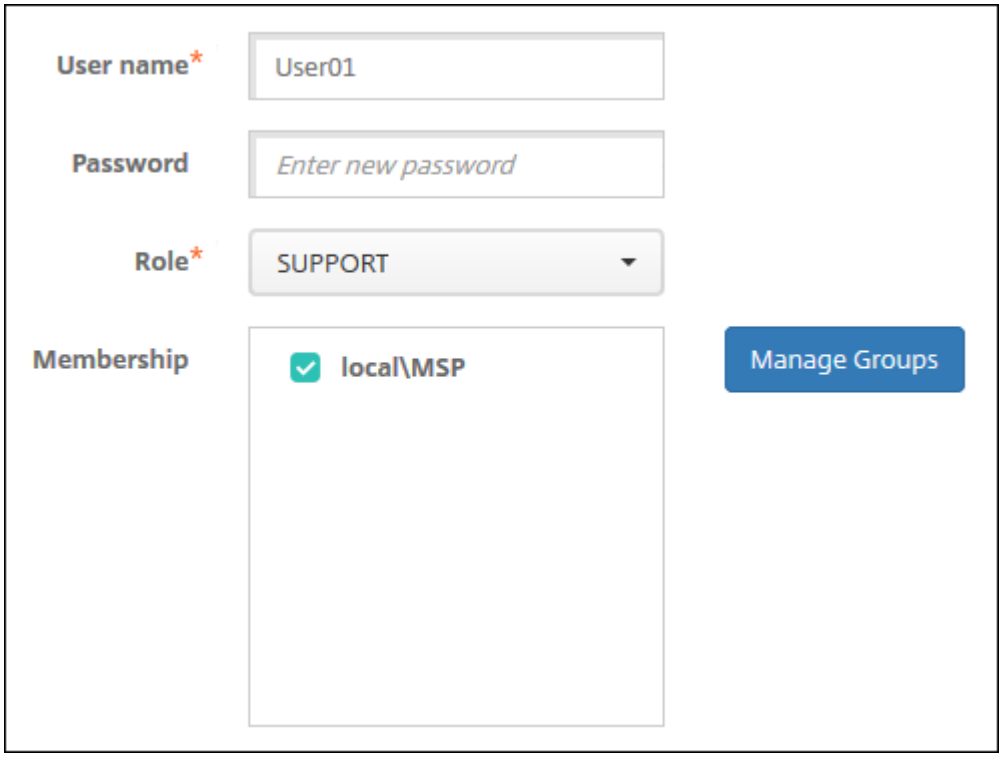
Das Entfernen einer Gruppe hat keine Auswirkungen auf die Benutzerkonten. Beim Entfernen einer Gruppe wird lediglich die Zuordnung von Benutzern zu der Gruppe aufgehoben. Die Benutzer verlieren zudem den Zugriff auf Apps und Profile, die über Bereitstellungsgruppen bereitgestellt werden, die der gelöschten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

Hinzufügen einer lokalen Gruppe

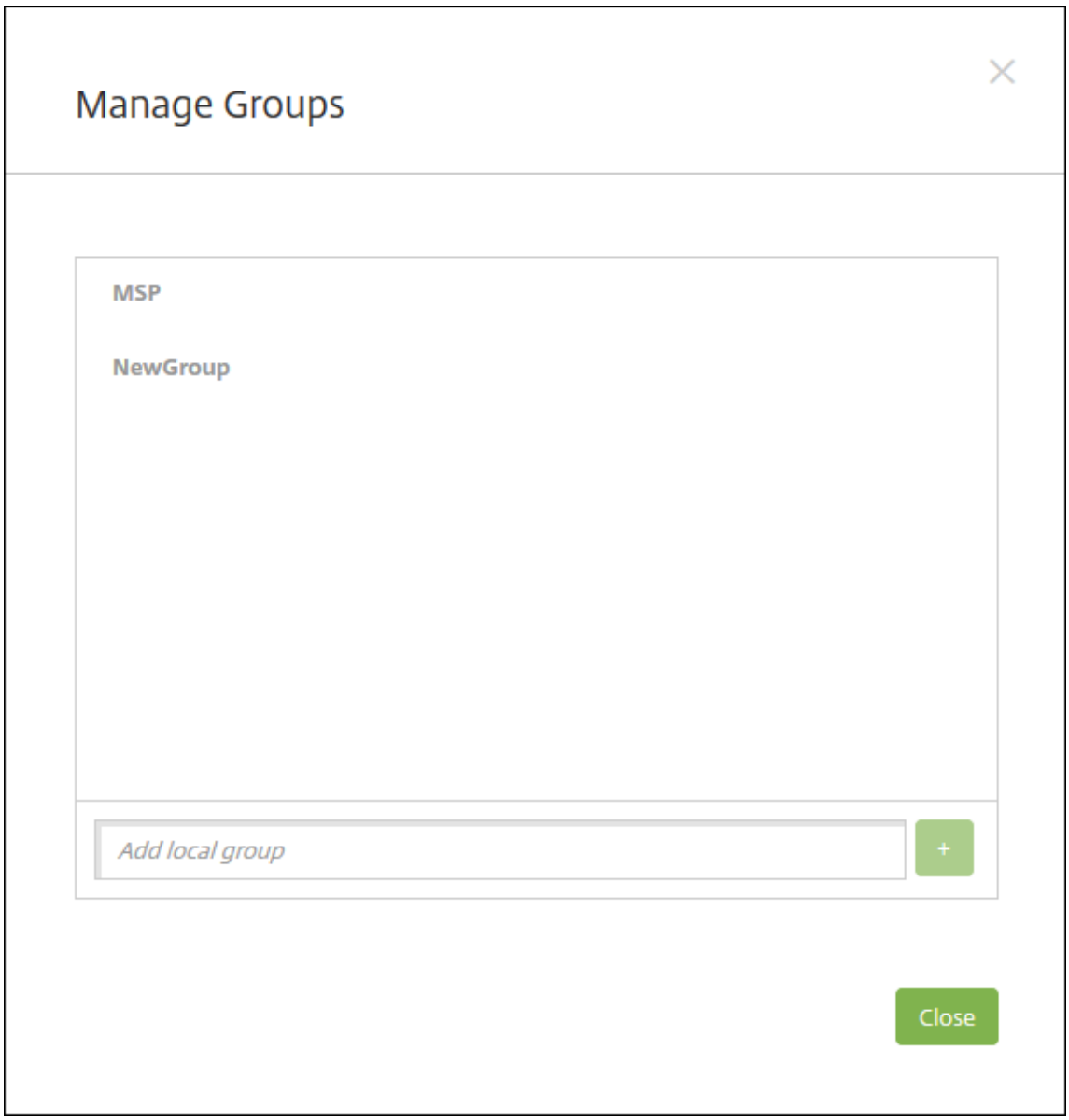
1. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf der Seite **Benutzer** auf **Lokale Gruppen** verwalten.



- 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**.

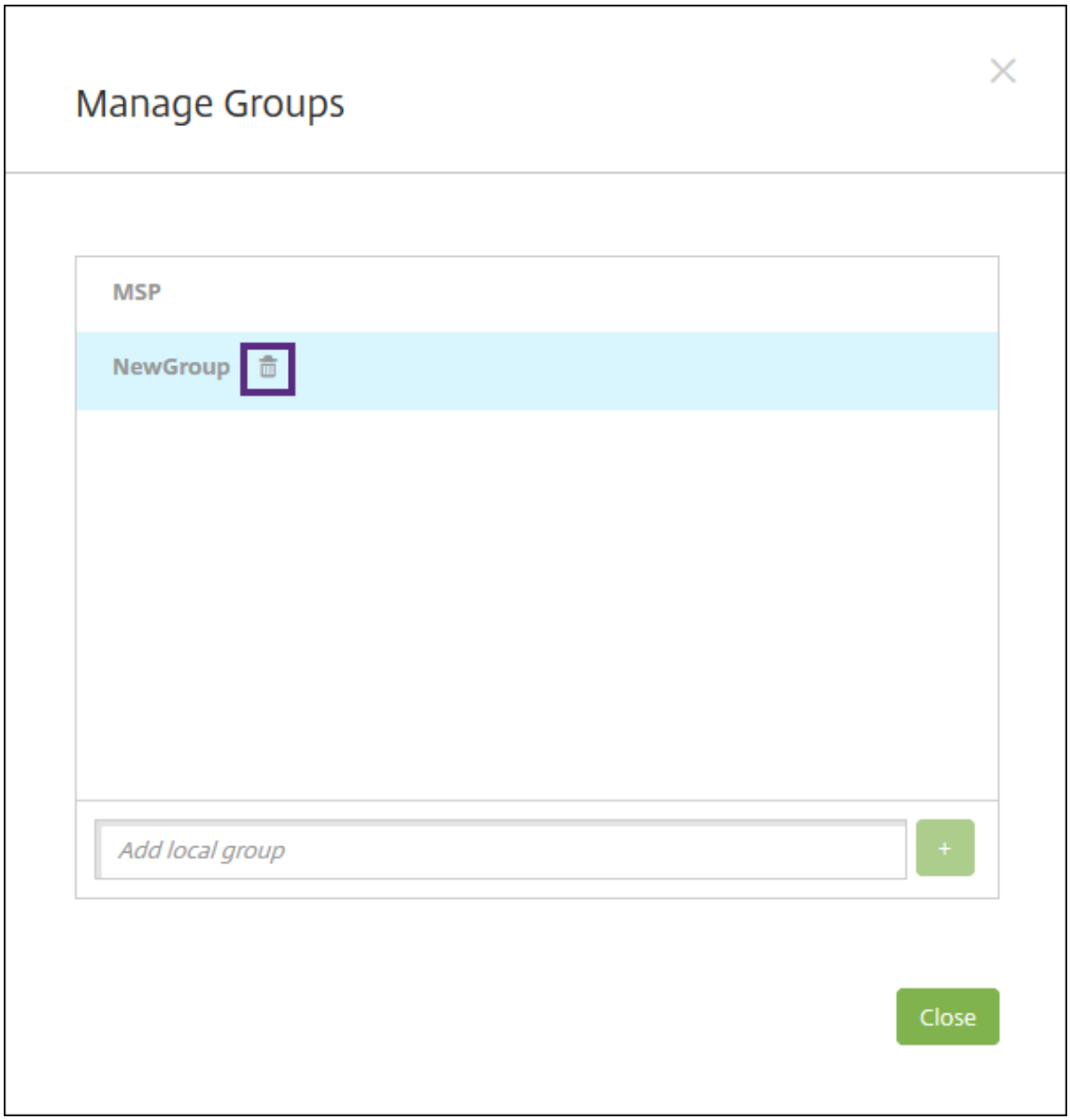
Entfernen einer Gruppe

Das Entfernen einer Gruppe hat keine Auswirkungen auf die Benutzerkonten. Beim Entfernen einer Gruppe wird lediglich die Zuordnung der Benutzer 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 **Manage Groups** auf **Close**.

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.

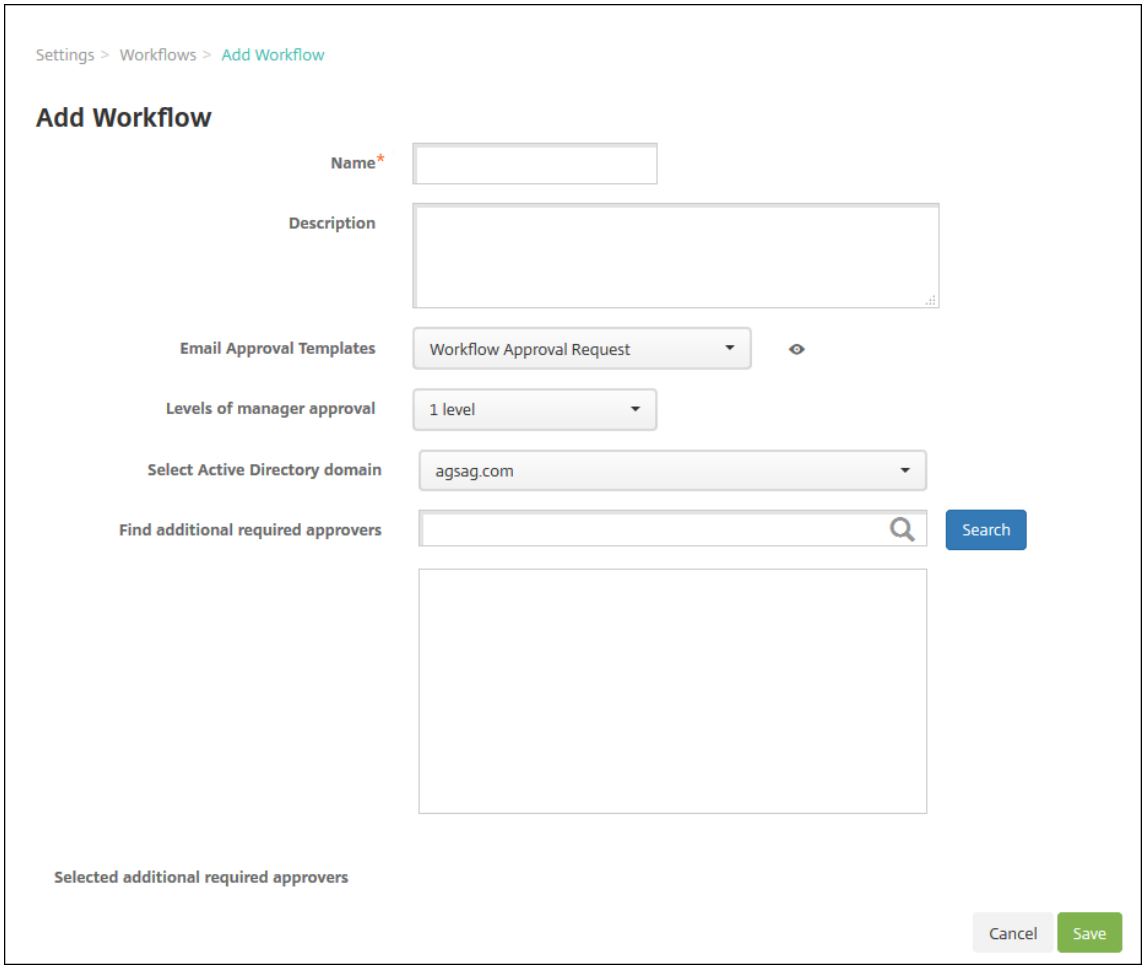
Beim ersten Einrichten von XenMobile konfigurieren Sie Einstellungen für Workflow-E-Mails. Diese müssen festgelegt werden, bevor Sie Workflows verwenden können. Sie können die Einstellungen für Workflow-E-Mails jederzeit ändern. Diese Einstellungen umfassen E-Mail-Server, Port, E-Mail-Adresse und Angaben 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 für 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 ihnen 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 **Add Workflow** 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 in der XenMobile-Konsole unter **Einstellungen** im Bereich **Benachrichtigungsvorlagen**. 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 ver-

wendende Active Directory-Domäne aus.

- **Weitere erforderliche Freigabeberechtigte suchen:** Geben Sie einen Namen 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.
  - Um einen Namen aus der Liste zu entfernen, wählen Sie eine der folgenden Möglichkeiten:
    * 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 **Search**, um das Suchergebnis einzuschränken.
    * Die Namen der Personen in der Liste **Selected additional required approvers** sind im Suchergebnis mit einem Häkchen gekennzeichnet. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Personen, die Sie entfernen möchten.

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, erstellen Sie einen weiteren Workflow.

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 **Delete**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf **Delete**.

   > **Wichtig:**
   >
   > Sie können diesen Vorgang nicht rückgängig machen.

Registrierungsprofile

January 5, 2022

Registrierungsprofile legen Folgendes fest:

- Registrierungsoptionen zur Verwaltung für Android- und iOS-Geräte. Bei Android unterscheiden sich die Registrierungsoptionen für den MDM+MAM (ENT)-Servermodus von denen für den MDM-Modus.
- Registrierungsoptionen zur App-Verwaltung für Android- und iOS-Geräte.
- Andere Optionen der Benutzerregistrierung:
  - Benutzer kann ggf. nur eine bestimmte Anzahl von Geräten registrieren.
    Bei Erreichen des Gerätelimits wird eine entsprechende Fehlermeldung angezeigt.
  - Benutzer kann ggf. die Geräteverwaltung ablehnen.

Mit Registrierungsprofilen können Sie mehrere Anwendungsfälle und Gerätemigrationspfade in einer einzelnen XenMobile Server-Konsole kombinieren. Beispiele für Anwendungsfälle:

- Mobilgeräteverwaltung (nur MDM)
- Mobilgeräteverwaltung + Mobilanwendungsverwaltung (MAM)
- Nur MAM
- Registrierung unternehmenseigener Geräte
- BYOD-Registrierung (Möglichkeit des Abwählens der MDM-Registrierung)
- Migration von der Android-Geräteadministratorregistrierung zur Android Enterprise-Registrierung (vollständig verwaltet, Arbeitsprofil, dediziertes Gerät)

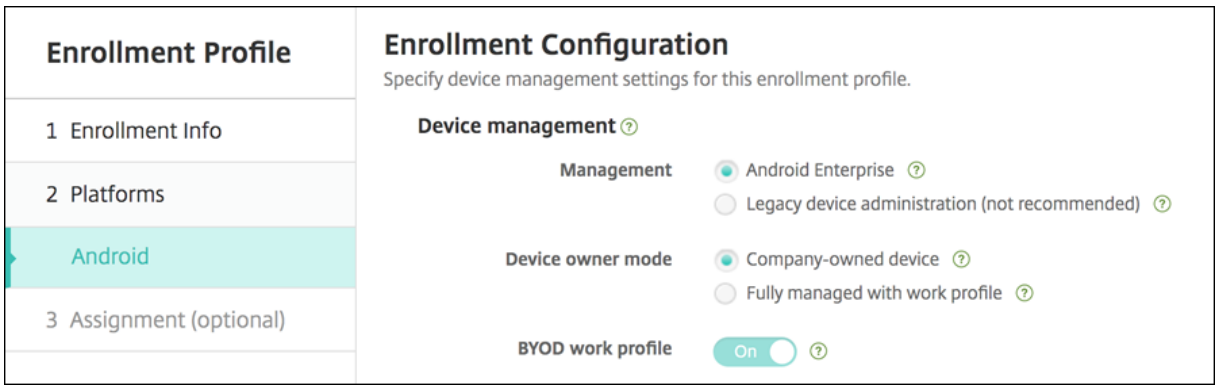
Wenn Sie eine Bereitstellungsgruppe erstellen, können Sie das Standardregistrierungsprofil “Global” verwenden oder ein anderes Registrierungsprofil angeben.

Die Features der Registrierungsprofile hängen von der Plattform ab.

- **Android:** Sie geben den Gerätebesitzermodus an. Beispiel: Vollständig verwaltet, vollständig verwaltet mit Arbeitsprofil und BYOD-Arbeitsprofil. Die Option **Dediziertes Gerät** wird nur angezeigt, wenn Sie eine Enterprise- oder Advanced-Lizenz für XenMobile haben. Neue Geräte registrieren sich standardmäßig bei Android Enterprise und der App-Verwaltung. Die Registrierungssicherheitsmodi **Benutzername + PIN**, **Einladungs-URL**, **Einladungs-URL + PIN** und **Einladungs-URL + Kennwort** sind für Android Enterprise nicht verfügbar.
- **iOS:** Sie geben den Geräteregistrierungstyp an: Geräteregistrierung oder Geräte nicht verwalten. Die iOS-Einstellungen werden nur angezeigt, wenn Sie eine Enterprise- oder Advanced-Lizenz für XenMobile haben. Neue Geräte registrieren sich standardmäßig bei der Apple-Geräteverwaltung und der App-Verwaltung.

Wenn Sie keine dedizierten Android-Geräte bzw. keine Nur-MAM-Registrierung von Android- oder iOS-Geräten benötigen, können Sie die Servereigenschaft `enable.multimode.xms` deaktivieren. Wenn Sie diese Eigenschaft aktiviert lassen, benötigen Sie allerdings nur einen XenMobile-Server zur Verarbeitung aller Registrierungsprofiltypen. Siehe Servereigenschaften.

Wenn Sie `enable.multimode.xms` deaktivieren, sind nur die in diesem Screenshot gezeigten Einstellungen verfügbar:

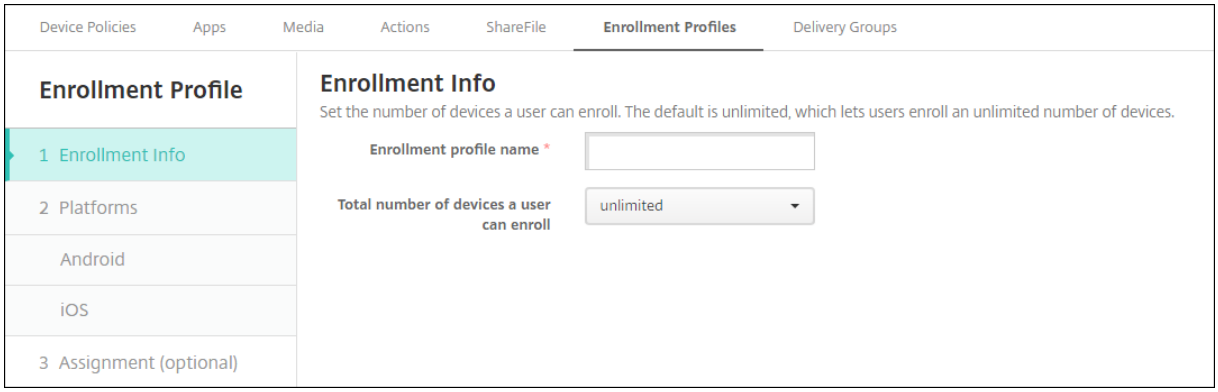


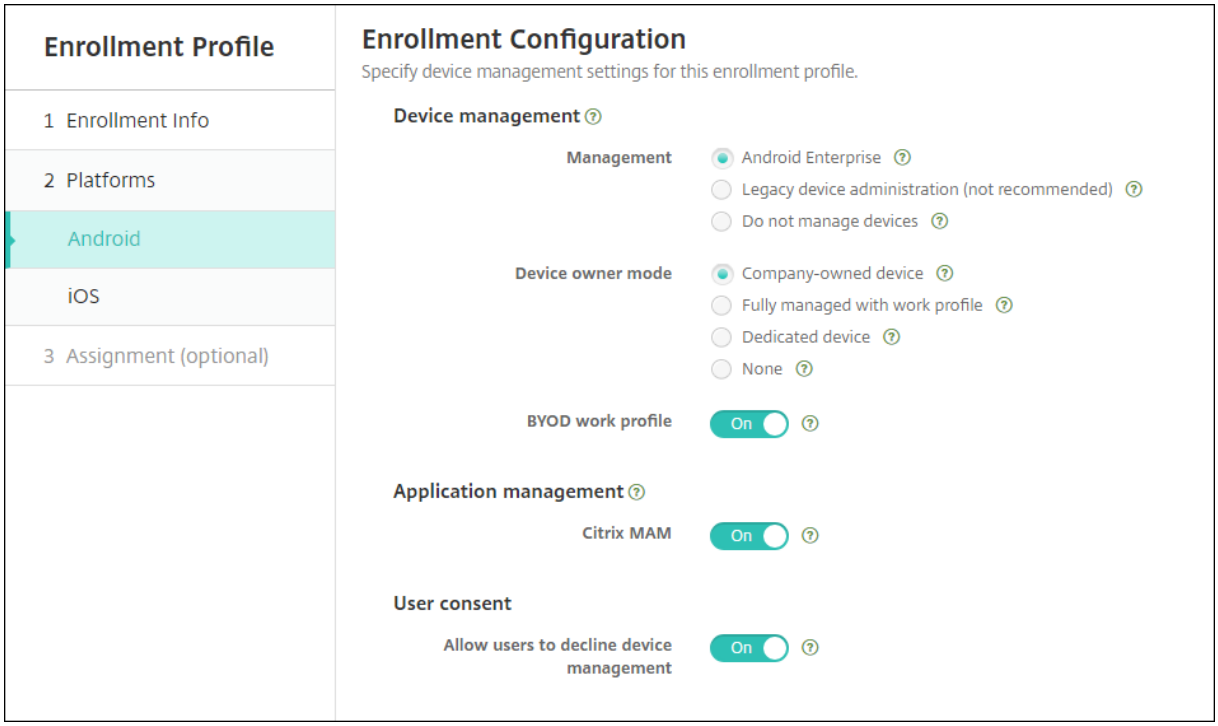
Weitere Einzelheiten zu diesen Einstellungen finden Sie unter Android Enterprise.

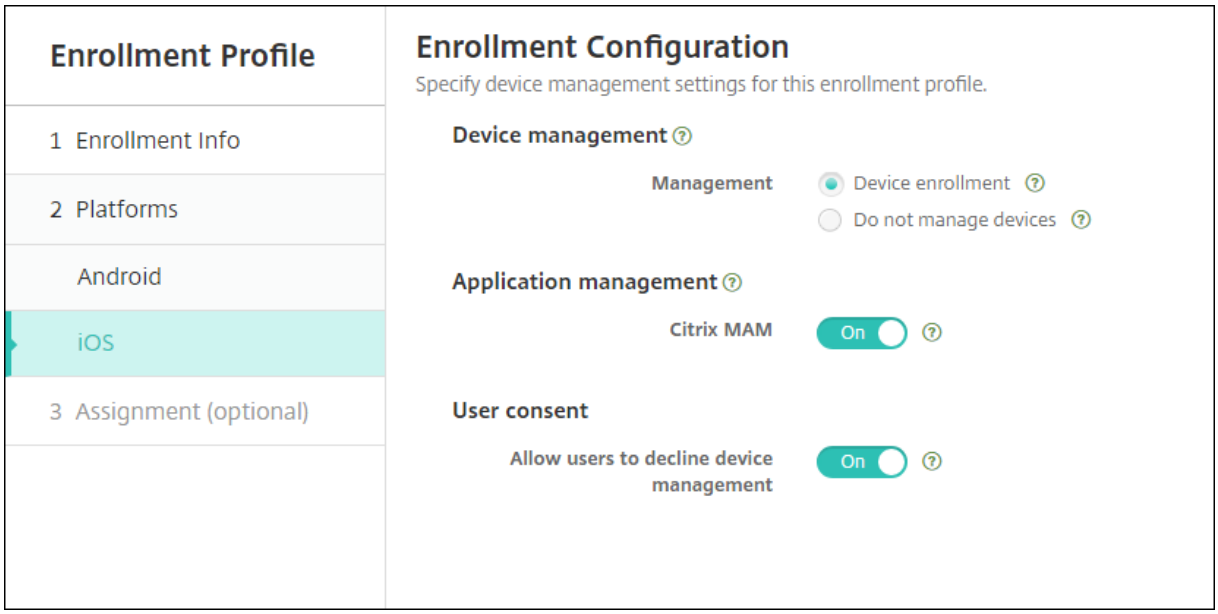
Globales Registrierungsprofil

Das Standardregistrierungsprofil heißt “Global”. Das Profil “Global” eignet sich für Testzwecke, wenn noch keine spezifischen Registrierungsprofile erstellt wurden.

Die folgenden Screenshots zeigen die Standardeinstellungen des globalen Registrierungsprofils.







Registrierungsprofile, Bereitstellungsgruppen und Registrierung

Registrierungsprofil und Bereitstellungsgruppen interagieren wie folgt:

- Sie können dieses Registrierungsprofil einer oder mehreren Bereitstellungsgruppen anfügen.
- Wenn ein Benutzer zu mehreren Bereitstellungsgruppen mit unterschiedlichen Registrierungsprofilen gehört, bestimmt der Name der Bereitstellungsgruppe das verwendete

Registrierungsprofil. XenMobile Server wählt die letzte Bereitstellungsgruppe in der alphabetisch geordneten Bereitstellungsgruppenliste aus. Beispiel:

  - Es gibt zwei Anmeldungsprofile, EP1 und EP2.
  - Es gibt zwei Bereitstellungsgruppen DG1 und DG2.
  - DG1 ist mit EP1 verbunden.
  - DG2 ist mit EP2 verbunden.

  Ist der registrierende Benutzer Mitglied beider Bereitstellungsgruppen, bestimmt XenMobile Server den Registrierungstyp für den Benutzer anhand des Registrierungsprofils EP2.

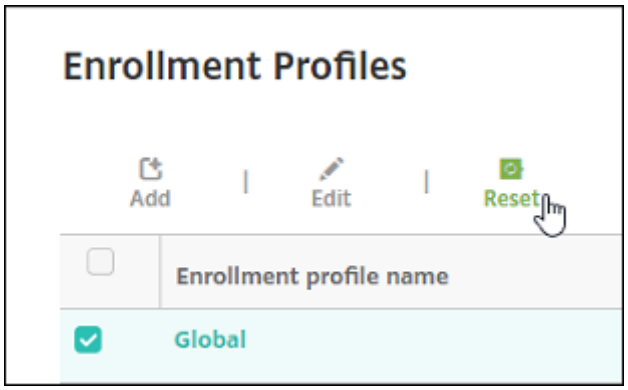
- Die Bereitstellungsreihenfolge gilt nur für Geräte in einer Bereitstellungsgruppe mit einem für MDM (Geräteverwaltung) konfigurierten Registrierungsprofil.
- Nach der Registrierung eines Geräts erfordern manche Änderungen am Registrierungsprofil eine erneute Registrierung:
  - Hinzufügen von MAM zu einem Registrierungsprofil, das für MDM konfiguriert ist.
  - Verschieben eines bei MDM registrierten Geräts in eine für MDM+MAM konfigurierte Bereitstellungsgruppe. Diese Änderung wirkt sich nur auf neue Geräteregistrierungen aus. Die Registrierung vorhandener Geräte ist nicht betroffen.
  - Hinzufügen von MDM zu einem Registrierungsprofil, das für MAM konfiguriert ist.
- Der Wechsel zu einem anderen Registrierungsprofil hat keine Auswirkungen auf Geräte mit bestehender Registrierung. Die Benutzer müssen die Registrierung aufheben und ihre Geräte erneut registrieren, damit die Änderungen wirksam werden.

Erstellen eines Registrierungsprofils

1. Gehen Sie in der XenMobile Server-Konsole zu **Konfigurieren > Registrierungsprofile**.
2. Geben Sie auf der Seite **Registrierungsinfo** einen aussagekräftigen Namen für das Registrierungsprofil ein. Standardmäßig können Benutzer beliebig viele Geräte registrieren. Wählen Sie einen Wert, wenn Sie die Anzahl der Geräte pro Benutzer begrenzen möchten. Das Limit gilt für die Summe aller in MAM oder MDM verwalteten Android- und iOS-Geräte eines Benutzers.
3. Füllen Sie die Plattformseiten aus. Informationen zu plattformspezifischen Registrierungseinstellungen finden Sie unter:
   - Android Enterprise
   - iOS: Unterstützte Registrierungsmethoden
4. Fügen Sie auf der Seite **Zuweisung** dem Registrierungsprofil eine oder mehrere Bereitstellungsgruppen an.

Ein Benutzer kann mehreren Bereitstellungsgruppen mit unterschiedlichen Registrierungsprofilen angehören. In diesem Fall bestimmt der Name der Bereitstellungsgruppe, welches Registrierungsprofil verwendet wird. XenMobile wählt die letzte Bereitstellungsgruppe in der alphabetisch geordneten Bereitstellungsgruppenliste aus. Um Bereitstellungsgruppen zu erstellen, gehen Sie zu **Konfigurieren > Bereitstellungsgruppen**.

Eine Liste der Registrierungsprofile wird auf der Seite **Konfigurieren > Registrierungsprofile** angezeigt. Um das globale Profil zu bearbeiten oder auf die ursprünglichen Standardwerte zurückzusetzen, wählen Sie die Zeile des Profils "Global" aus und klicken Sie auf **Zurücksetzen**. Das globale Profil kann nicht gelöscht werden.



Konfigurieren von Rollen mit RBAC

January 5, 2022

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.

> **Wichtig:**
>
> Durch die RBAC-Berechtigung unter den Einstellungen erhalten Administratoren Vollzugriff, einschließlich der Möglichkeit, eigene Berechtigungen zuzuweisen. Geben Sie diese Zugriffsrechte

> nur Benutzern, die die Möglichkeit haben sollen, alles im Endpoint Management-System zu bearbeiten.

Dieser Artikel enthält folgende Abschnitte:

Administratorrolle

Benutzer mit der vordefinierten Administratorrolle haben Zugriff oder haben keinen Zugriff auf die folgenden Features in XenMobile. Standardmäßig sind **Autorisierter Zugriff** (außer Selbsthilfeportal), **Konsolenfeatures** und **Berechtigungen anwenden** aktiviert.

Autorisierter Zugriff

Konsolenzugriff für Administratoren	Administratoren haben Zugriff auf alle Features der XenMobile-Konsole.
Zugriff auf das Selbsthilfeportal	Administratoren haben keinen Zugriff auf das Selbsthilfeportal.
Registrierung für gemeinsam genutzte Geräte	Administratoren haben nicht die Berechtigung “Registrierung für gemeinsam genutzte Geräte”. Dieses Feature ist für Benutzer gedacht, die gemeinsam genutzte Geräte registrieren müssen.
Remotesupportzugriff	Administratoren haben Remotesupportzugriff.*
Zugriff über öffentliche API	Mit der öffentlichen API für Administratoren können Aktionen, die in der XenMobile-Konsole verfügbar sind, programmatisch durchgeführt werden. Ein Beispiel für solche Aktionen ist das Verwalten von Zertifikaten, Apps, Geräten, Bereitstellungsgruppen und lokalen Benutzern.

Registrierung für COSU-Geräte	Hiermit können Administratoren dedizierte Android Enterprise-Geräte (“COSU-Geräte”) registrieren, wenn dieses Merkmal nicht mit einem Registrierungsprofil konfiguriert ist.

*Durch Remotesupport können Helpdesk-Mitarbeiter die Fernsteuerung verwalteter Windows CE- und Android-Mobilgeräte übernehmen. Screencast wird nur auf Samsung Knox-Geräten unterstützt. Remotesupport ist nicht für geclusterte on-premises XenMobile Server-Bereitstellungen verfügbar. Remote Support ist ab dem 1. Januar 2019 für Neukunden nicht mehr verfügbar. Bestehende Kunden können das Produkt weiterhin verwenden, Citrix stellt jedoch keine Neuerungen oder Fixes bereit.

Konsolenfeatures

Administratoren haben uneingeschränkten Zugriff auf die XenMobile-Konsole.

Dashboard	Das **Dashboard** ist die erste Seite, die Administratoren nach der Anmeldung an der XenMobile-Konsole angezeigt wird. Das **Dashboard** enthält grundlegende Informationen zu Benachrichtigungen und Geräten.
Berichterstellung	Die Seite **Analyse > Berichterstellung** bietet vordefinierte Berichte für die Analyse von App- und Gerätebereitstellungen.
Geräte	Die Seite **Verwalten > Geräte** dient zum Verwalten der Benutzergeräte. Sie können einzelne Geräte auf der Seite hinzufügen oder eine Provisioningdatei zum Hinzufügen mehrerer Geräte in einem Arbeitsgang importieren.
Lokale Benutzer und Gruppen	Auf der Seite **Verwalten > Benutzer** können Sie lokale Benutzer und Gruppen hinzufügen, bearbeiten und löschen.
Registrierung	Auf der Seite **Verwalten > Registrierungseinladungen** geben Sie vor, wie Benutzer zur Registrierung ihrer Geräte in XenMobile eingeladen werden.
Richtlinien	Die Seite **Verwalten > Geräterichtlinien** dient zur Verwaltung von Geräterichtlinien wie VPN und Wi-Fi.
Apps	Auf der Seite **Konfigurieren > Apps** verwalten Sie die Apps, die die Benutzer auf ihren Geräten installieren können.
Medien	Auf der Seite **Konfigurieren > Medien** verwalten Sie die Medien, die die Benutzer auf ihren Geräten installieren können.
Aktion	Auf der Seite **Konfigurieren > Aktionen** verwalten Sie Antworten auf Auslöser.
Registrierungsprofile	Auf der Seite **Konfigurieren > Registrierungsprofile** konfigurieren Sie

Registrierungsprofile (Modi) für die Geräteregistrierung durch die Benutzer. |
Bereitstellungsgruppen	Auf der Seite **Konfigurieren > Bereitstellungsgruppen** verwalten Sie Bereitstellungsgruppen und die ihnen zugeordneten Ressourcen.
Einstellungen	Die Seite **Einstellungen** dient zur Verwaltung der Systemeinstellungen, z. B. von Client- und Servereigenschaften, Zertifikaten und Anmeldeinformationsanbietern. **Wichtig:** Diese Einstellungen umfassen die RBAC-Berechtigung. Durch die RBAC-Berechtigung erhalten Administratoren Vollzugriff, einschließlich der Möglichkeit, eigene Berechtigungen zuzuweisen. Geben Sie diese Zugriffsrechte nur Benutzern, die die Möglichkeit haben sollen, alles im Endpoint Management-System zu bearbeiten.	
Support	Die Seite **Problembehandlung und Support** ermöglicht die Behandlung von Problemen, z. B. die Ausführung einer Diagnose und das Generieren von Protokollen.

Geräte

Administratoren greifen in jedem Bereich der Konsole auf Gerätefeatures zu, indem sie Geräteeinschränkungen festlegen, Benachrichtigungen für Geräte einrichten und senden, Apps auf den Geräten verwalten usw.

Gerät vollständig löschen	Löschen aller Daten und Apps von einem Gerät und, sofern vorhanden, dessen Speicherkarten.
Einschränkungen deaktivieren	Entfernen einer oder mehrerer Geräteeinschränkungen.
Gerät selektiv löschen	Löschen aller Unternehmensdaten und -Apps von einem Gerät, private Daten und Apps bleiben erhalten.
Standorte anzeigen	Anzeigen des Standorts eines Geräts und Festlegen geografischer Einschränkungen. Optionen: Gerät orten, Standort eines Geräts anzeigen, Gerätetracking, Standort eines Geräts verfolgen.
Lock device	Sperren eines Geräts, sodass es nicht verwendet werden kann.
Unlock device	Remoteentsperren eines Geräts, sodass es verwendet werden kann.
Container sperren	Remotesperren des Unternehmenscontainers auf einem Gerät.

Container entsperren	Remoteentsperren des Unternehmenscontainers auf einem Gerät.
Containerkennwort zurücksetzen	Zurücksetzen des Containerkennworts.
Umgehung der Aktivierungssperre für ASM DEP aktivieren	Speichern eines Umgehungscodes auf einem betreuten iOS-Gerät bei aktivierter Aktivierungssperre. Wenn Sie die Daten auf dem Gerät löschen müssen, verwenden Sie diesen Code, um die Aktivierungssperre automatisch aufzuheben.
Gerät klingeln lassen	Remoteauslösen des Klingeltons auf einem Windows-Gerät in voller Lautstärke für 5 Minuten.
Gerät neu starten	Neustarten von Windows-Geräten über die XenMobile-Konsole.
Auf Gerät bereitstellen	Senden von Apps, Benachrichtigungen, Einschränkungen usw. an ein Gerät.
Gerät bearbeiten	Ändern der Einstellungen auf dem Gerät.
Benachrichtigung an Gerät	Senden von Benachrichtigungen an ein Gerät.
Gerät hinzufügen/löschen	Hinzufügen oder Löschen von Geräten in XenMobile.
Geräte importieren	Importieren einer Gerätegruppe aus einer Datei in XenMobile.
Gerätetabelle exportieren	Sammeln von Geräteinformationen auf der Geräteseite und Exportieren in eine CSV-Datei.
Gerät widerrufen	Verhindern der Herstellung einer Verbindung zwischen einem Gerät und XenMobile.
App-Sperre	Verhindern des Zugriffs auf alle Apps auf einem Gerät. Unter Android können sich Benutzer nicht bei XenMobile anmelden. Unter iOS können Benutzer sich anmelden, jedoch nicht auf Apps zugreifen.

App löschen	Diese Aktion 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.
Softwarebestand anzeigen	Anzeigen einer Liste der auf einem Gerät installierten Software.
AirPlay-Synchronisierung anfordern	Anforderung, AirPlay-Streaming zu starten.
AirPlay-Synchronisierung beenden	AirPlay-Streaming beenden.
Modus “Verloren” aktivieren	Unter **Verwalten > Geräte** können Sie betreute Geräte in den Modus “Verloren” versetzen, damit das betreute Gerät mit dem Sperrbildschirm gesperrt wird. Der Modus “Verloren” ermöglicht außerdem das Orten verlorener und gestohlener Geräte.
Modus ‘Verloren’ deaktivieren	Unter **Verwalten > Geräte** können Sie den Modus “Verloren” für Geräte deaktivieren, die auf diesen Modus eingestellt sind.
OS-Update für Gerät	Sie können die Geräterichtlinie “OS-Update steuern” auf Geräten bereitstellen.
Gerät herunterfahren	Fährt Windows-Geräte über die XenMobile-Konsole herunter.
Gerät neu starten	Neustarten von iOS-Geräten über die XenMobile-Konsole.

Lokale Benutzer und Gruppen

Administratoren verwalten auf der Seite **Verwalten > Benutzer** in XenMobile lokale Benutzer und Gruppen.

Lokale Benutzer hinzufügen
Lokale Benutzer löschen

Lokale Benutzer bearbeiten
Lokale Benutzer importieren
Lokalen Benutzer exportieren
Lokale Benutzergruppen
Lokale Benutzersperr-ID abrufen
Lokale Benutzersperr-ID löschen

Registrierung

Administratoren können Registrierungseinladungen hinzufügen und löschen, Benachrichtigungen an Benutzer senden und die Registrierungstabelle in eine CSV-Datei exportieren.

Registrierung hinzufügen/löschen	Hinzufügen und Entfernen einer Registrierungseinladung an einen Benutzer oder eine Gruppe.
Benutzer benachrichtigen	Senden einer Registrierungseinladung an einen Benutzer oder eine Gruppe.
Registrierungseinladungstabelle exportieren	Sammeln von Registrierungsinformationen auf der Seite “Registrierung” und Exportieren in eine CSV-Datei.

Richtlinien

Richtlinie hinzufügen/löschen	Hinzufügen und Entfernen von Geräte- und App-Richtlinien.
Richtlinie bearbeiten	Ändern einer Geräte- oder App-Richtlinie.
Richtlinie hochladen	Hochladen einer Geräte- oder App-Richtlinie.
Richtlinie klonen	Kopieren einer Geräte- oder App-Richtlinie.
Richtlinie deaktivieren	Deaktivieren einer App-Richtlinie.

Richtlinie exportieren	Sammeln von Richtlinieninformationen auf der Seite “Geräterichtlinien” und Exportieren in eine CSV-Datei.
Richtlinie zuweisen	Zuweisen einer Richtlinie zu einer oder mehreren Bereitstellungsgruppen.

App

Administratoren verwalten Apps auf der Seite **Konfigurieren > Apps** in XenMobile.

App-Store- oder Unternehmensapp hinzufügen/löschen	Hinzufügen oder Entfernen von öffentlichen App Store-Apps oder Unternehmensapps (nicht MDX-fähig).
App-Store- oder Unternehmensapp bearbeiten	Ändern von öffentlichen App Store-Apps oder Unternehmensapps (nicht MDX-fähig).
MDX-, Web- und SaaS-App hinzufügen/löschen	Hinzufügen bzw. Entfernen von MDX-fähigen Apps, Apps aus dem internen Netzwerk (Web-Apps) oder Apps aus einem öffentlichen Netzwerk (SaaS) zu bzw. aus XenMobile.
MDX-, Web- und SaaS-App bearbeiten	Ändern einer MDX-fähigen App, einer App aus dem internen Netzwerk (Web-App) oder einer App aus einem öffentlichen Netzwerk (SaaS) in XenMobile.
Kategorie hinzufügen/löschen	Hinzufügen oder Löschen einer Kategorie für die Anzeige von Apps im XenMobile Store.
Öffentliche App/Unternehmensapp Bereitstellungsgruppe zuweisen	Zuweisen von öffentlichen App-Store-Apps oder nicht MDX-fähigen Apps zu einer Bereitstellungsgruppe.
MDX-/Weblink-/SaaS-App einer Bereitstellungsgruppe zuweisen	Zuweisen von MDX-fähigen Apps, Apps ohne erforderlichen Single Sign-On (WebLink) oder Apps aus einem öffentlichen Netzwerk (SaaS) zu einer Bereitstellungsgruppe.

App-Tabelle exportieren	Sammeln von App-Informationen auf der App-Seite und Exportieren in eine CSV-Datei.

Medien

Verwalten von Medien, die aus einem öffentlichen App-Store oder über eine Volume Purchase-Lizenz erworben wurden.

App-Store- oder Unternehmensbücher hinzufügen/löschen
Öffentliche bzw. Unternehmensbücher Bereitstellungsgruppe zuweisen
App-Store- oder Unternehmensbücher bearbeiten

Aktion

Aktion hinzufügen/löschen	Hinzufügen oder Löschen einer Aktion, die über einen Auslöser (Ereignis, Geräte oder Benutzereigenschaft oder Name der installierten App) und die zugehörigen Antwort definiert wird.
Aktion bearbeiten	Ändern einer Aktion, die über einen Auslöser (Ereignis, Geräte oder Benutzereigenschaft oder Name der installierten App) und die zugehörigen Antwort definiert wird.
Aktion einer Bereitstellungsgruppe zuweisen	Zuweisen einer Aktion zu einer Bereitstellungsgruppe für die Bereitstellung auf den Benutzergeräten.
Aktion exportieren	Sammeln von Aktionsinformationen auf der Aktionen-Seite und Exportieren in eine CSV-Datei.

Bereitstellungsgruppe

Administratoren verwalten Bereitstellungsgruppen auf der Seite **Konfigurieren > Bereitstellungsgruppen**.

Bereitstellungsgruppe hinzufügen/löschen	Erstellen oder Löschen einer Bereitstellungsgruppe zum Hinzufügen bzw. Löschen der angegebenen Benutzer und optional von Richtlinien, Apps und Aktionen.
Bereitstellungsgruppe bearbeiten	Ändern einer Bereitstellungsgruppe zum Ändern der angegebenen Benutzer und optional von Richtlinien, Apps und Aktionen.
Bereitstellungsgruppe bereitstellen	Verfügbarmachen einer Bereitstellungsgruppe.
Bereitstellungsgruppe exportieren	Sammeln von Informationen zu einer Bereitstellungsgruppe auf der Seite mit den Bereitstellungsgruppen und Exportieren in eine CSV-Datei.

Registrierungsprofil

Verwalten von Registrierungsprofilen.

Registrierungsprofil hinzufügen/löschen
Registrierungsprofil bearbeiten
Registrierungsprofil der Bereitstellungsgruppe zuweisen

Einstellungen

Administratoren konfigurieren diverse Einstellungen auf der Seite **Einstellungen**.

RBAC	RBAC-Zuweisung, Zuweisen von Rollen. **Wichtig:** Durch diese Berechtigung erhalten Administratoren Vollzugriff, einschließlich der Möglichkeit, eigene Berechtigungen zuzuweisen. Geben Sie diese Zugriffsrechte nur Benutzern, die die Möglichkeit haben sollen, alles im Endpoint Management-System zu bearbeiten.
LDAP	Verwalten LDAP-kompatibler Verzeichnisse, z. B. von Active Directory, zum Importieren von Gruppen, Benutzerkonten und zugehörigen Eigenschaften.
Lizenz	Für lokale XenMobile Server-Umgebungen. Verwalten der Citrix Lizenzen.
Registrierung	Aktivieren von Registrierungssicherheitsmodi für Benutzer und das Selbsthilfeportal.
Releasemanagement	Anzeigen des aktuell installierten Release. Inklusive Releasemanagementupdate.
Zertifikate	Bearbeiten von APNs-Zertifikaten, Zertifikat-SSL-Listener
Benachrichtigungsvorlagen	Erstellen von Benachrichtigungsvorlagen zur Verwendung für automatisierte Aktionen, die Registrierung und Standardbenachrichtigungen an Benutzer.
Workflows	Verwalten von Erstellen, Genehmigen und Entfernen von Benutzerkonten für die Verwendung mit App-Konfigurationen.
Anmeldeinformationsanbieter	Hinzufügen von Anmeldeinformationsanbietern mit Berechtigung zum Ausstellen von Gerätezertifikaten. Die Anmeldeinformationsanbieter steuern das Zertifikatformat und die Bedingungen für die Verlängerung und Sperrung von Zertifikaten.

PKI-Entitäten	Verwalten von Public Key-Infrastrukturentitäten (allgemeine, Microsoft Zertifikatdienste oder eigenverwaltete ZS).
PKI-Verbindung testen	Verwenden Sie die Schaltfläche “Verbindung testen” auf der Seite **Einstellungen > PKI-Entitäten**, um sicherzustellen, dass der Server erreichbar ist.
Clienteigenschaften	Verwalten diverser Eigenschaften auf den Benutzergeräten, z. B. Passcodetyp, -sicherheit oder -ablauf.
Clientsupport	Festlegen der Methoden, mit denen Benutzer sich an den hauseigenen Support wenden können (E-Mail, Telefon oder Supportticket per E-Mail).
Clientbranding	Erstellen eines benutzerdefinierten Storenamens und von Standardansichten für den XenMobile Store. Hinzufügen eines benutzerdefinierten Logos für den XenMobile Store oder Secure Hub.
SMS-Gateway des Netzbetreibers	Einrichten von Netzbetreiber-SMS-Gateways zum Konfigurieren von Benachrichtigungen, die XenMobile durch SMS-Gateway sendet.
Benachrichtigungsserver	Einrichten eines SMTP-Gatewayservers zum Senden von E-Mail an Benutzer.
ActiveSync-Gateway	Verwalten des Benutzerzugriffs für Benutzer und Geräte über Regeln und Eigenschaften.
Apple-Bereitstellungsprogramm	Hinzufügen eines Apple-Bereitstellungsprogrammkontos zu XenMobile.
Apple Configurator-Geräteregistrierung	Konfigurieren von Apple Configurator-Einstellungen in XenMobile.
iOS-/Volume Purchase-Einstellungen	Hinzufügen von Apple Volume Purchase-Konten.

Mobilfunkanbieter	Verwenden der Mobilfunkanbieterschnittstelle zum Abfragen von BlackBerry- und anderen Exchange ActiveSync-Geräten und zum Auslösen von Vorgängen.
Citrix Gateway	Für lokale XenMobile Server-Umgebungen. Citrix Gateway hinzufügen. Auswählen, ob die Authentifizierung aktiviert werden soll, und ob Benutzerzertifikate für die Authentifizierung per Push installiert werden sollen. Auswählen eines Anmeldeinformationsanbieters.
Netzwerkzugriffssteuerung (NAC)	Festlegen der Bedingungen zum Einordnen von Geräten als nicht richtlinientreu und entsprechendem Entzug des Zugriffs auf das Netzwerk.
Samsung Knox	Aktivieren und Deaktivieren von XenMobile für die Abfrage der REST-APIs des Samsung Knox-Nachweisservers.
Servereigenschaften	Hinzufügen und Ändern von Servereigenschaften. Erfordert einen Neustart von XenMobile auf allen Knoten.
Syslog	Für lokale XenMobile Server-Umgebungen. Senden von Protokolldateien an einen Systemprotokollserver (Syslog-Server) unter Verwendung von dessen Hostnamen oder IP-Adresse.
XenApp und XenDesktop	Benutzer dürfen Virtual Apps and Desktops über Secure Hub hinzufügen.

Citrix Files	XenMobile mit Enterprise-Konten: Konfigurieren Sie Einstellungen für Verbindungen mit dem Content Collaboration-Konto und dem Administratordienstkonto, um Benutzerkonten zu verwalten. Eine Citrix Files-Domäne und Administratoranmeldeinformationen sind erforderlich. XenMobile mit Speicherzonenconnectors: Konfigurieren Sie XenMobile zum Verweisen auf Netzwerkfreigaben und SharePoint-Speicherorte, die in Speicherzonenconnectors definiert sind.
Programm zur Verbesserung der Benutzerfreundlichkeit	Für lokale XenMobile Server-Umgebungen. Entscheidung für oder gegen die Übermittlung anonymer Statistiken und von Nutzungsinformationen an Citrix.
Microsoft Azure	Für lokale XenMobile Server-Umgebungen. Integrieren von XenMobile in Microsoft Azure.
Android Enterprise	Konfigurieren der Android Enterprise-Servereinstellungen.
Identitätsanbieter (IdP)	Konfigurieren eines Identitätsanbieters.
XenMobile Tools	Zugriff auf die XenMobile Tools-Seite.
SNMP-Konfiguration	Aktivieren von SNMP für XenMobile Server-Knoten. Bearbeiten oder Hinzufügen von Überwachungsbenutzern, Einrichten des SNMP-Managers, in dem Trap-Benachrichtigungen angezeigt werden, und Konfigurieren von Trap-Intervallen und -Schwellenwerten.

Support

Administratoren können verschiedene Supportaufgaben erledigen.

Citrix Gateway-Konnektivitätsprüfung	Durchführen diverser Verbindungsprüfungen für Citrix Gateway nach IP-Adresse. Erfordert Benutzernamen und Kennwort.
XenMobile-Konnektivitätsprüfung	Durchführen von Konnektivitätsprüfungen für bestimmte XenMobile-Features, z. B. Datenbank, DNS oder Google-Abonnement.
Supportpakete erstellen	Für lokale XenMobile Server-Umgebungen. Erstellen einer Datei für den Versand an den Citrix Support zur Problembehandlung. Enthält Systeminformationen, Protokolle, Datenbankinformationen, Kernspeicherinformationen, Ablaufverfolgungsdateien und die aktuellen Konfigurationsinformationen für XenMobile bzw. Citrix Gateway.
Citrix-Produktdokumentation	Zugriff auf die öffentliche Citrix Website mit der Dokumentation zu XenMobile.
Citrix Knowledge Center	Zugriff auf die Citrix Support-Website für die Suche nach Wissensdatenbankartikeln.
Logs	Zugriff auf und Analyse der Informationen in den Debug-, Administratoraudit- und Benutzerauditprotokolldateien.
Clusterinformationen	Für lokale XenMobile Server-Umgebungen. Zugriff auf Informationen zu den einzelnen Knoten in einer Clusterumgebung.
Speicherbereinigung	Für lokale XenMobile Server-Umgebungen. Zugriff auf Informationen über Speicherobjekte, die nicht mehr verwendet werden.
Java-Speichereigenschaften	Für lokale XenMobile Server-Umgebungen. Zugriff auf einen Snapshot der Java-Speichernutzung sowie Arbeitsspeicher- und Speicherpooldetails.

Makros	Auffüllen der Benutzer- oder Geräteeigenschaftsdaten im Textfeld von Profilen, einer Benachrichtigung oder einer Registrierungsvorlage. Konfigurieren einer einzelnen Richtlinie und Bereitstellen der Richtlinie für eine große Benutzergruppe, wobei für jeden Zielbenutzer benutzerspezifische Werte angezeigt werden.
Konfigurieren von PKI	Importieren und Exportieren von PKI-Konfigurationsinformationen.
Hilfsprogramm für APNs-Signierung	Senden einer Anforderung für ein APNs-Signaturzertifikat und Hochladen eines Secure Mail-APNs-Zertifikats für iOS.
Citrix Insight Services	Hochladen von Protokollen an Citrix Insight Services (CIS) für Hilfe bei verschiedenen Problemen.
Citrix Gateway Connector für Exchange ActiveSync - Gerätestatus	Fragen Sie den Status des Geräts in XenMobile ab. Der Status wird an den Citrix Gateway Connector für Exchange ActiveSync basierend auf der Geräte-ID in ActiveSync gesendet.
Anonymisierung und Deanonymisierung	Für lokale XenMobile Server-Umgebungen. Beim Erstellen von Supportpaketen in XenMobile werden vertrauliche Benutzer-, Server- und Netzwerkdaten standardmäßig anonymisiert. Sie können dieses Verhalten unter **Support > Anonymisierung und Deanonymisierung** in **Erweitert** ändern.
Protokolleinstellungen	Anpassen der Protokollebene oder Hinzufügen einer benutzerdefinierten Protokollierung.

Gruppenzugriff einschränken

Administratoren können auf alle Benutzergruppen Berechtigungen anwenden.

Geräteprovisioningrolle

> **Wichtig:**
>
> Die Geräteprovisioningrolle gilt nur für Windows CE-Geräte.

Benutzer mit der vordefinierten Rolle “Geräteprovisioning” haben eingeschränkten Zugriff auf Konsolenfeatures. Standardmäßig ist ihre Berechtigung auf alle Benutzergruppen festgelegt und sie können diese Einstellung nicht ändern.

Konsolenfeatures

Benutzer mit der Geräteprovisioningrolle haben den folgenden eingeschränkten Zugriff auf die XenMobile-Konsole. Standardmäßig sind die folgenden Features aktiviert.

Geräte

Gerät bearbeiten	Ändern der Einstellungen auf dem Gerät.
Gerät hinzufügen/löschen	Hinzufügen oder Löschen von Geräten in XenMobile.

Einstellungen

Geräteprovisioningbenutzer können auf die Seite **Einstellungen** zugreifen, jedoch keine Features konfigurieren.

Supportrolle

Benutzer mit der Supportrolle haben Zugriff auf Remotesupport. Standardmäßig gelten ihre Berechtigung für alle Benutzergruppen und sie können diese Einstellung nicht ändern.

Benutzerrolle

Benutzer mit der Benutzerrolle haben den folgenden eingeschränkten Zugriff auf XenMobile.

Autorisierter Zugriff

Selbsthilfeportal	Benutzer haben nur Zugriff auf das Selbsthilfeportal in XenMobile.

Konsolenfeatures

Benutzer haben den folgenden eingeschränkten Zugriff auf die XenMobile-Konsole.

Geräte

Gerät vollständig löschen	Löschen aller Daten und Apps von einem Gerät und, sofern vorhanden, dessen Speicherkarten.
Gerät selektiv löschen	Löschen aller Unternehmensdaten und -Apps von einem Gerät, private Daten und Apps bleiben erhalten.
Standorte anzeigen	Anzeigen des Standorts eines Geräts und Festlegen geografischer Einschränkungen. Optionen: Gerät orten, Standort eines Geräts anzeigen, Gerätetracking, Standort eines Geräts verfolgen.
Lock device	Remotesperren eines Geräts, sodass es nicht verwendet werden kann.
Unlock device	Remoteentsperren eines Geräts, sodass es verwendet werden kann.
Container sperren	Remotesperren des Unternehmenscontainers auf einem Gerät.
Container entsperren	Remoteentsperren des Unternehmenscontainers auf einem Gerät.
Containerkennwort zurücksetzen	Zurücksetzen des Containerkennworts.

Umgehung der Aktivierungssperre für ASM DEP aktivieren	Speichern eines Umgehungscodes auf einem betreuten iOS-Gerät bei aktivierter Aktivierungssperre. Wenn Sie die Daten auf dem Gerät löschen müssen, verwenden Sie diesen Code, um die Aktivierungssperre automatisch aufzuheben.
Gerät klingeln lassen	Remoteauslösen des Klingeltons auf einem Windows-Gerät in voller Lautstärke für 5 Minuten.
Gerät neu starten	Neustarten von Windows-Geräten.
Softwarebestand anzeigen	Anzeigen einer Liste der auf einem Gerät installierten Software.

Registrierung

Registrierung hinzufügen/löschen	Hinzufügen und Entfernen einer Registrierungseinladung an einen Benutzer oder eine Gruppe.
Benutzer benachrichtigen	Senden einer Registrierungseinladung an einen Benutzer oder eine Gruppe.

Gruppenzugriff einschränken

Für alle vier Standardrollen ist diese Berechtigung standardmäßig festgelegt. Sie kann auf alle Benutzergruppen angewendet werden. Sie können die Rolle nicht bearbeiten.

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:** gewährt vollen Zugriff auf das System.
- **Geräteprovisioning:** gewährt Zugriff auf Grundfunktionen der Geräteverwaltung für Windows CE-Geräte.
- **Support:** gewährt 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 und anpassen, um ihre Benutzerrollen zu erstellen. Sie können den Rollen 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. Angenommen, Benutzer der Gruppe “ADGroupA” können Geräte von Managern orten und Benutzer der Gruppe “ADGroupB” können eine Datenlöschung auf Mitarbeitergeräten durchführen. In diesem Fall kann ein Benutzer, der beiden Gruppen angehört, Geräte von Managern und Mitarbeitern suchen und eine Datenlöschung darauf durchführen.

> **Hinweis:**
>
> Lokale Benutzer dürfen nur eine Rolle zugewiesen bekommen.

Mit dem RBAC-Feature in XenMobile ist Folgendes möglich:

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

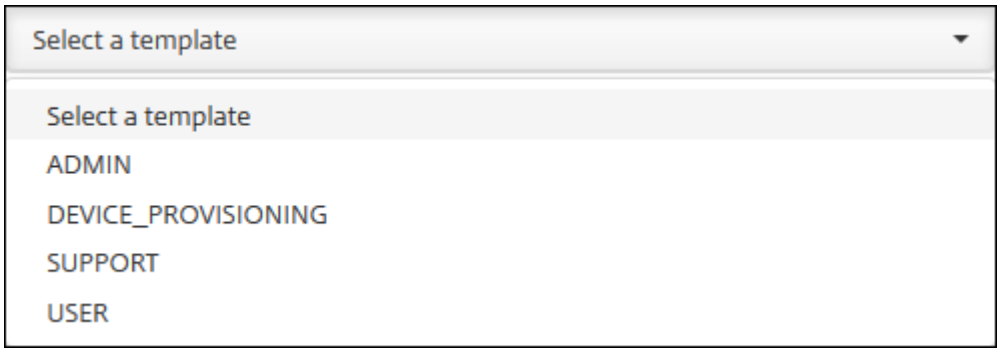
1. Gehen Sie in der XenMobile-Konsole zu **Einstellungen > Rollenbasierte Zugriffssteuerung**. Die Seite **Rollenbasierte Zugriffssteuerung** wird angezeigt. Sie enthält die Standardbenutzerrollen sowie alle von Ihnen zuvor hinzugefügten Rollen.

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

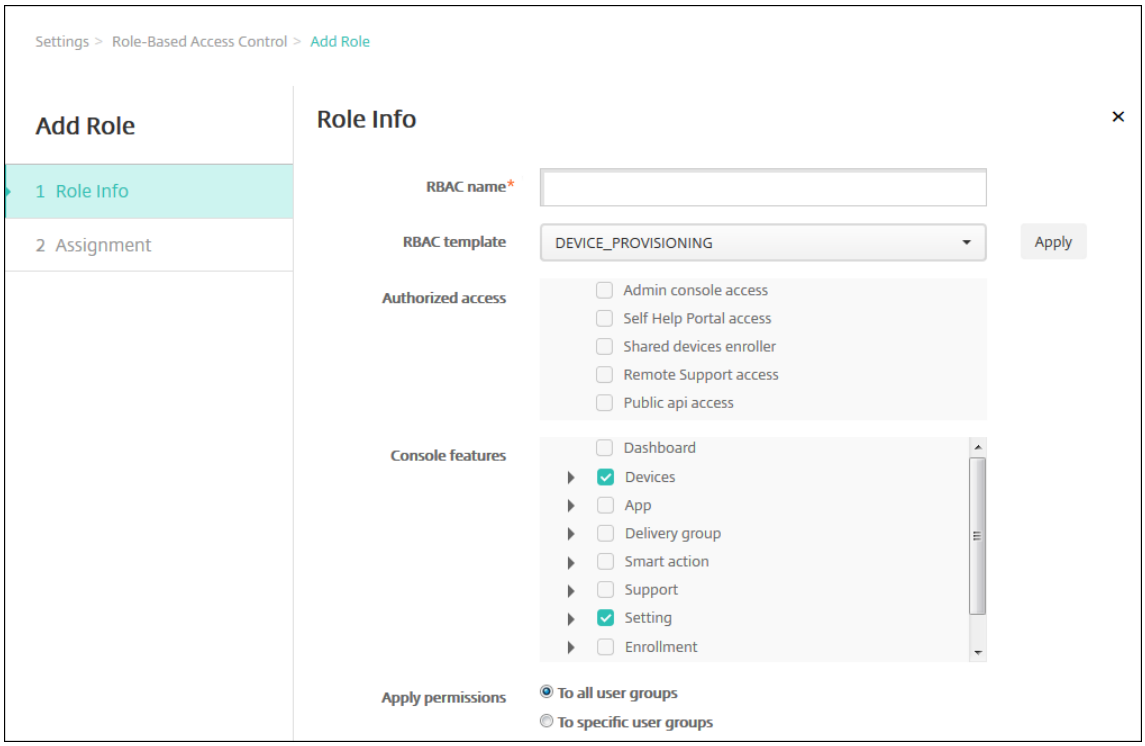
2. Klicken Sie auf **Hinzufügen**, um eine Benutzerrolle hinzuzufügen. Klicken Sie zum Bearbeiten einer Rolle auf das Stiftsymbol rechts daneben. Klicken Sie zum Löschen einer Rolle auf das Papierkorbsymbol rechts daneben. Sie können die Standardbenutzerrollen nicht löschen.
   - Wenn Sie auf **Hinzufügen** 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.
3. Geben Sie die folgenden Informationen zum Erstellen oder Bearbeiten einer 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 Systemfunktio-

nen 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.



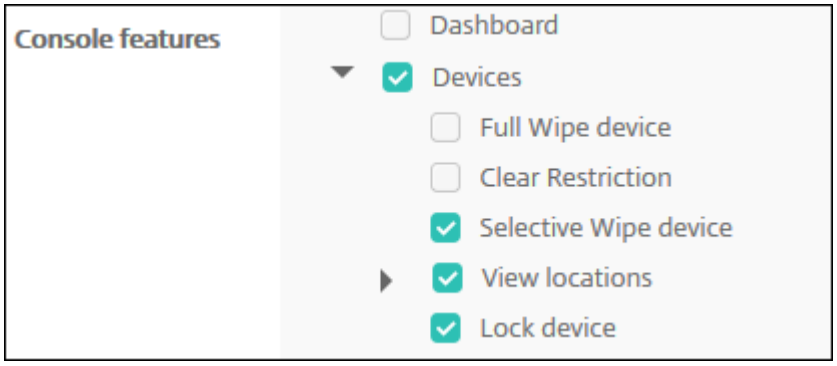
4. Klicken Sie auf **Anwenden** bei dem ausgewählten Feld **RBAC-Vorlage**, um die Bereiche **Autorisierter Zugriff** und **Konsolenfeatures** gemäß den vordefinierten Berechtigungen der ausgewählten Vorlage einzustellen.



5. Aktivieren bzw. deaktivieren Sie die Kontrollkästchen unter **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. Durch Klicken auf das oberste Kontrollkästchen wird der Zugriff auf diesen Konsolenbereich verhindert. Wählen Sie

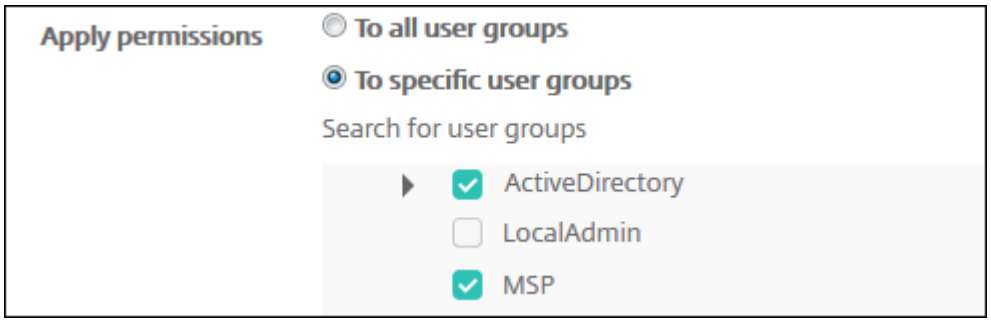
einzelne Optionen unterhalb der obersten Ebene, um diese Optionen zu aktivieren. Beispiel: In der folgenden Abbildung werden die Optionen **Gerät vollständig löschen** und **Einschränkungen deaktivieren** für Benutzer, denen die Rolle zugewiesen ist, nicht angezeigt. Die aktivierten Optionen werden angezeigt.



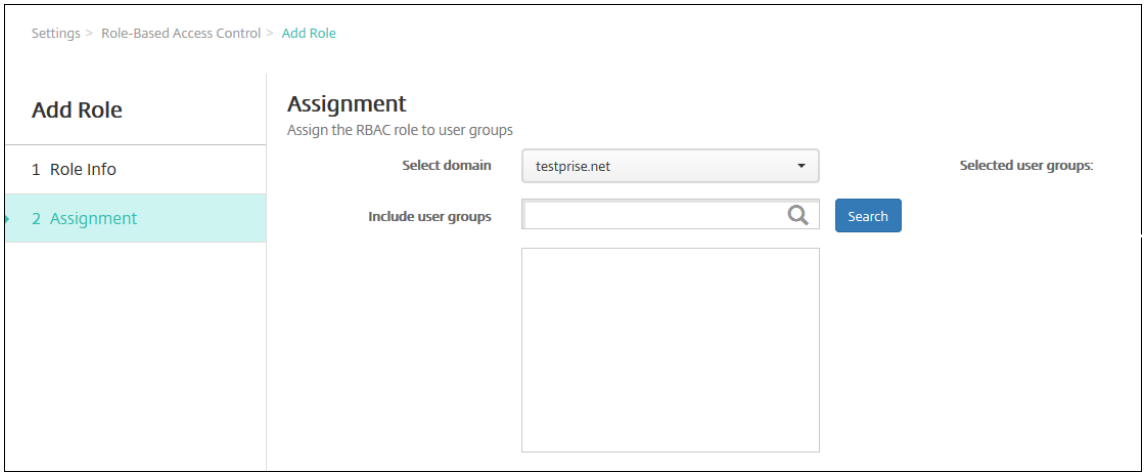
6. **Berechtigungen anwenden:** Wählen Sie eine oder mehrere Benutzergruppen aus, um einzuschränken, welche Gruppen der Administrator verwalten kann. Wenn Sie auf **Auf bestimmte Benutzergruppen** klicken, wird eine Liste mit Gruppen angezeigt, in der Sie eine oder mehrere Gruppen auswählen können.

   Beispiel: Ein RBAC-Administrator verfügt über Berechtigungen für die Benutzergruppen “ActiveDirectory” und “MSP”:

   - Der Administrator kann nur Informationen für Benutzer anzeigen, die in “ActiveDirectory”, “MSP” oder in beiden Gruppen sind.
   - Der Administrator kann keine anderen lokalen Benutzer oder AD-Benutzer anzeigen. Der Administrator kann Benutzer anzeigen, die Mitglieder einer untergeordneten Gruppe dieser Gruppen sind.
   - Der Administrator kann Einladungen senden an:
     - die Berechtigungsgruppen und ihre untergeordneten Gruppen
     - die Benutzer, die Mitglieder der Berechtigungsgruppen und ihrer untergeordneten Gruppen sind

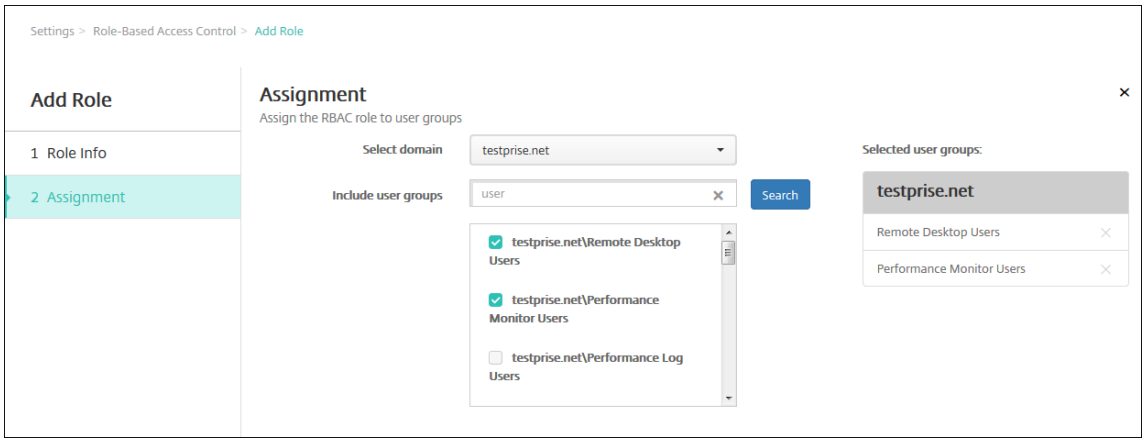


7. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** wird angezeigt.



8. Geben Sie die folgenden Informationen zum Zuweisen der Rolle zu Benutzergruppen ein.

   - **Domäne auswählen:** Klicken Sie in der Liste auf eine Domäne.
   - **Benutzergruppen 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 mit dem entsprechenden Namen 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.

9. Klicken Sie auf **Speichern**.

Benachrichtigungen

January 5, 2022

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. Hierzu gehören beispielsweise 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 (unter Verwendung automatisierter Aktionen), wenn bestimmte Bedingungen erfüllt sind. Beispiel:
  - Wenn ein Benutzergerät aufgrund mangelnder Richtlinientreue von der Unternehmensdomäne blockiert wird.
  - Wenn für ein Gerät Jailbreak oder Rooting durchgeführt wurde.

Details zu automatisierten 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.

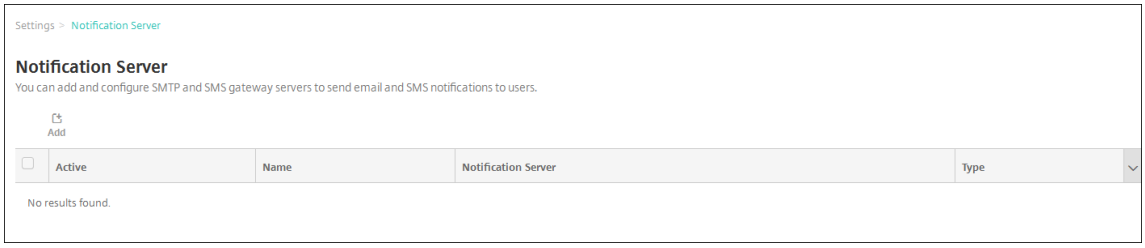
Sie können auch ein Netzbetreiber-SMS-Gateway in XenMobile einrichten, um Benachrichtigungen zu konfigurieren, die über das SMS-Gateway eines Netzbetreibers gesendet werden. Netzbetreiber nutzen SMS-Gateways für den Versand oder Empfang von Textnachrichten an bzw. von einem Telekommunikationsnetz. Standardisierte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

Voraussetzungen

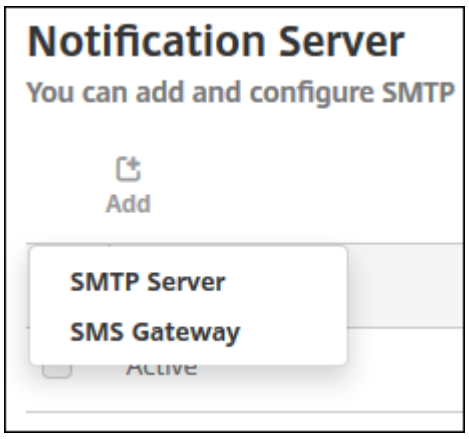
- Bringen Sie vor der Konfiguration des SMS-Gateways beim zuständigen Systemadministrator die Serverinformationen in Erfahrung. Wichtig ist, ob der SMS-Server auf einem internen Unternehmensserver gehostet wird oder Teil eines gehosteten E-Mail-Diensts ist. In diesem Fall benötigen Sie Informationen von der Website des Dienstanbieters.
- Konfigurieren Sie den SMTP-Benachrichtigungsserver zum Senden von Nachrichten an Benutzer. Wenn der Server intern gehostet wird, bringen Sie die Konfigurationsinformationen beim Systemadministrator in Erfahrung. Handelt es sich bei dem Server um einen gehosteten E-Mail-Dienst, suchen Sie nach den entsprechenden Konfigurationsinformationen auf der Website des Dienstanbieters.
- Sie können einen aktiven SMTP-Server und einen aktiven SMS-Server gleichzeitig verwenden. Beide Kommunikationskanäle erlauben eine aktive Konfiguration.
- Öffnen Sie Port 25 über XenMobile, das sich in der DMZ befindet, um zum SMTP-Server im internen Netzwerk zurückzuverweisen. Auf diese Weise kann XenMobile Benachrichtigungen erfolgreich senden.

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.

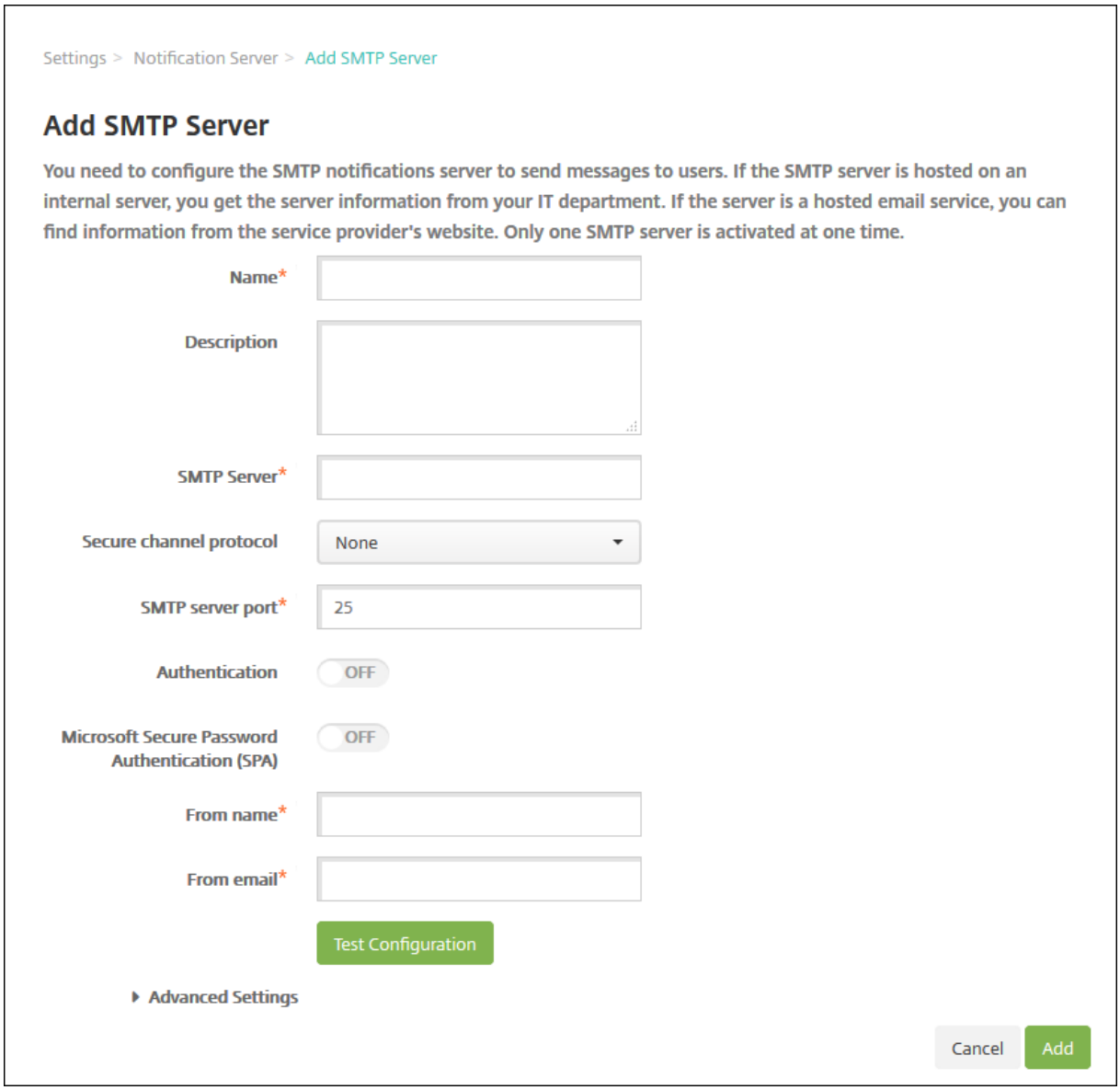


3. Klicken Sie auf **Hinzufügen**. Ein Menü mit Optionen zum Konfigurieren eines SMTP-Servers oder SMS-Gateways wird angezeigt.



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

Hinzufügen eines SMTP-Servers



1. Konfigurieren Sie folgende 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 anzugeben (sofern dieser für die sichere Authentifizierung konfiguriert ist). Die Standardeinstellung 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 fest-

gelegt.

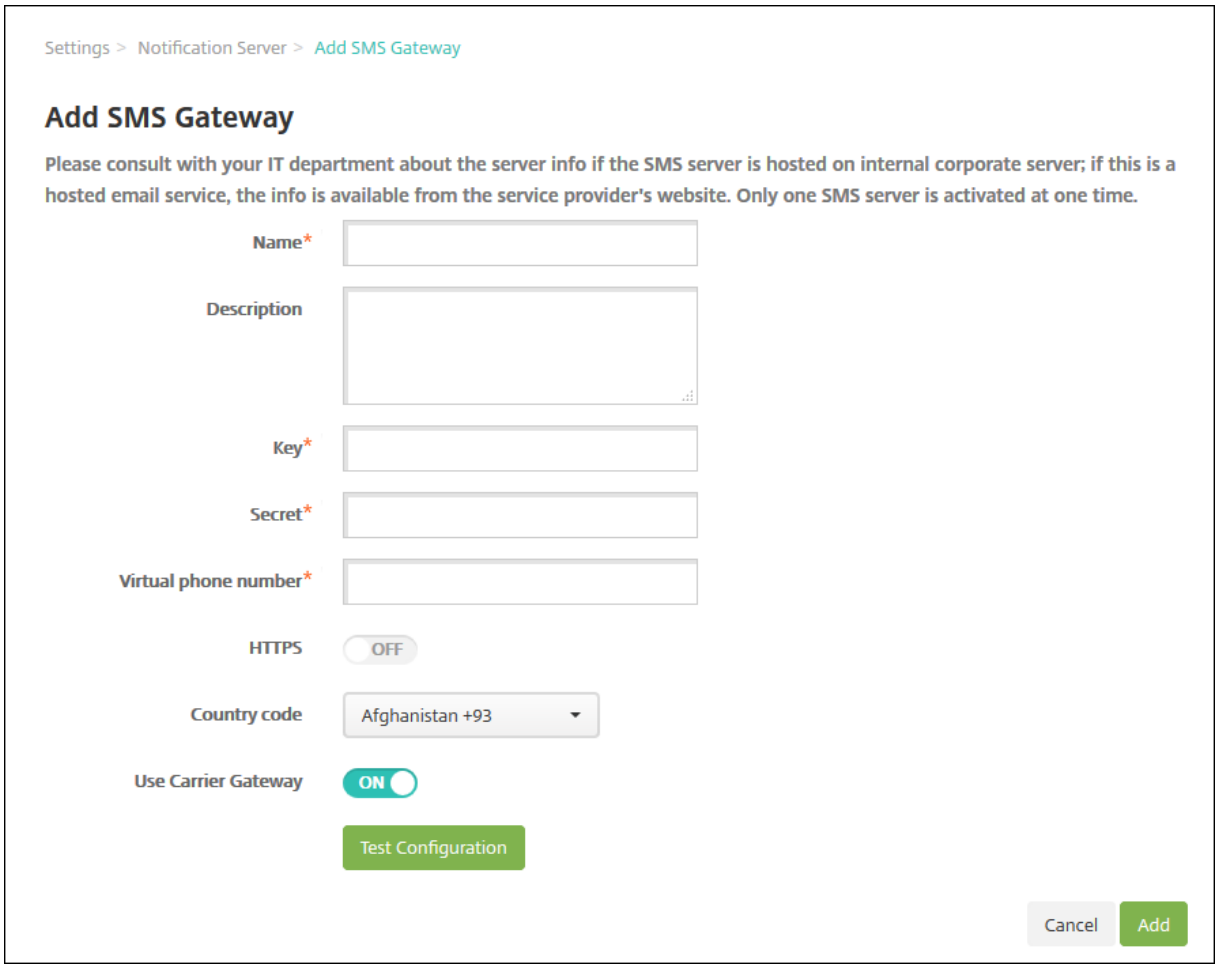
- **Authentifizierung:** Wählen Sie **EIN** oder **AUS**. Die Standardeinstellung ist **Aus**.
- Wenn Sie **Authentifizierung** aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **Benutzername:** Geben Sie den Benutzernamen für die Authentifizierung ein.
  - **Kennwort:** Geben Sie das Kennwort des Benutzers für die Authentifizierung ein.
- **Microsoft Gesicherte Kennwortauthentifizierung (SPA):** Wenn für den SMTP-Server SPA verwendet wird, klicken Sie auf **EIN**. Die Standardeinstellung ist **Aus**.
- **Von (Name):** Geben Sie den Namen ein, der in Benachrichtigungs-E-Mails von diesem Server im **Absenderfeld** angezeigt werden soll. Beispiel: Corporate IT.
- **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. Die Standardeinstellung 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 SMS-Gateways



Hinweis:

XenMobile unterstützt für Textnachrichten nur Nexmo. Wenn Sie noch kein Konto für Nexmo Messaging haben, erstellen Sie eines auf deren 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. Die Standardeinstellung ist **Aus**.

> **Wichtig:**
>
> Übernehmen Sie die Einstellung **EIN** für HTTPS, es sei denn, Sie werden vom Citrix Support dazu aufgefordert, sie auf **AUS** zu setzen.

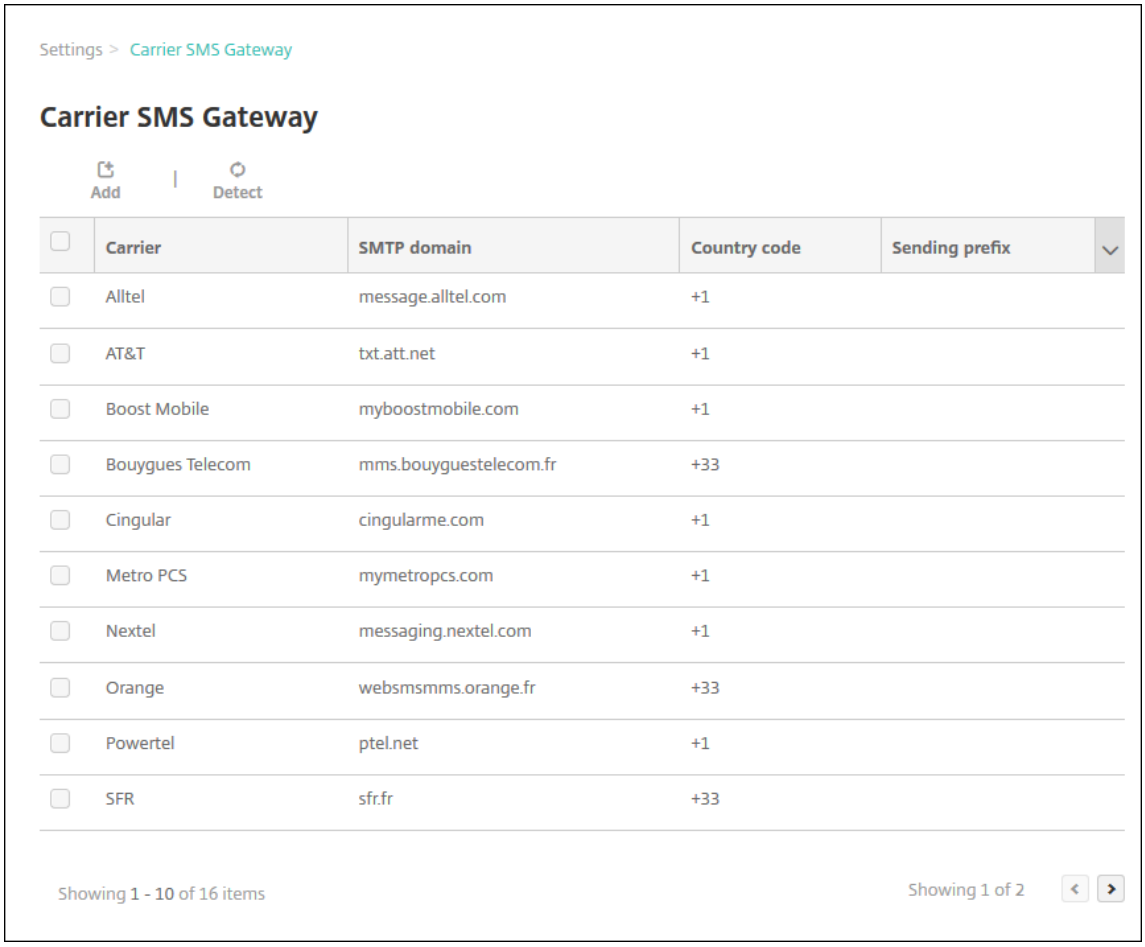
- **Ländercode:** Klicken Sie in der Liste auf die Standard-SMS-Ländervorwahl für Empfänger in Ihrem Unternehmen. Dieses Feld beginnt immer mit +. Der Standardwert ist **Afghanistan +93**.

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.
3. Klicken Sie auf **Hinzufügen**.

Hinzufügen eines Netzbetreiber-SMS-Gateways

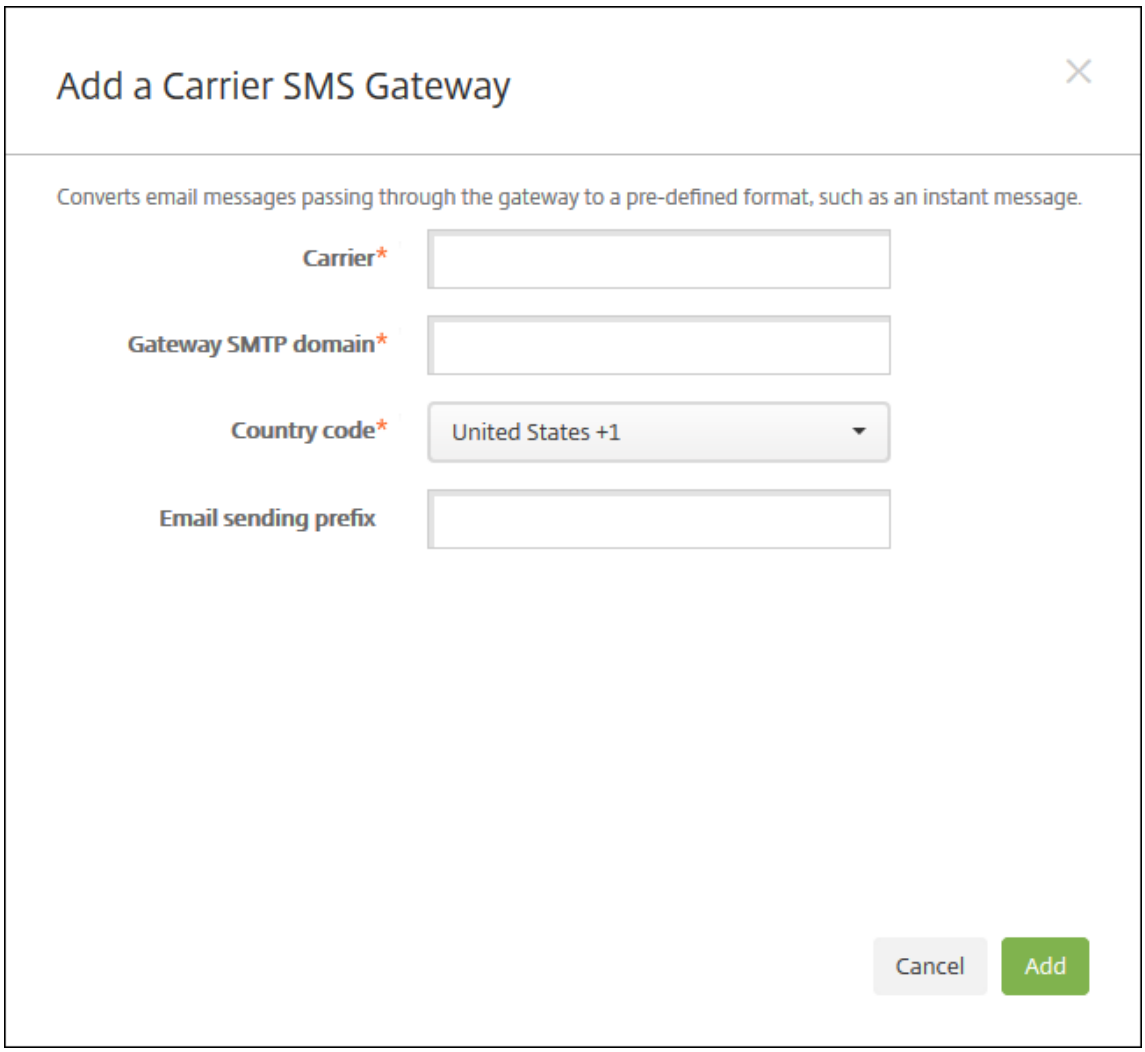
Sie können ein Netzbetreiber-SMS-Gateway in XenMobile einrichten, um Benachrichtigungen zu konfigurieren, die über das SMS-Gateway eines Netzbetreibers gesendet werden. Netzbetreiber nutzen SMS-Gateways für den Versand oder Empfang von Textnachrichten an bzw. von einem Telekommunikationsnetz. Standardisierte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

4. Konfigurieren Sie folgende 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.

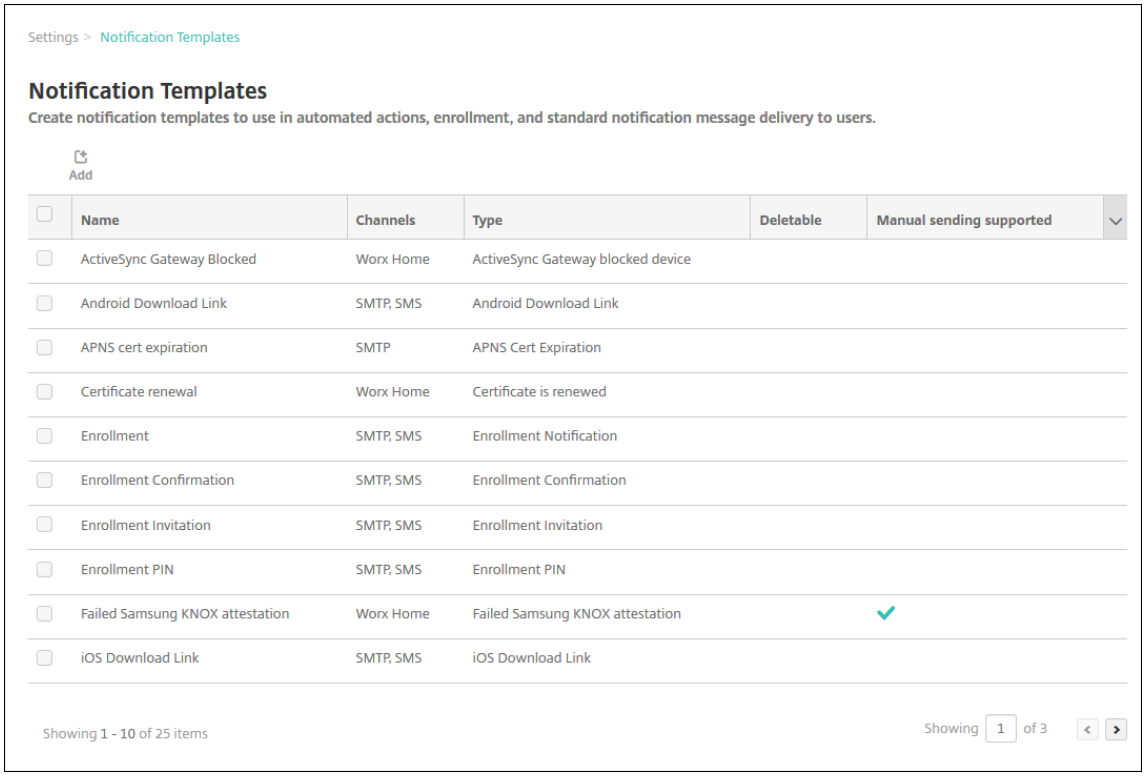
Erstellen und Aktualisieren von Benachrichtigungsvorlagen

Sie können Benachrichtigungsvorlagen in XenMobile erstellen und aktualisieren, die in automatisierten Aktionen, bei der Registrierung und für Standardbenachrichtigungen an Benutzer verwendet werden. 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 an die Seite **Benachrichtigungsserver** unter **Einstellung** weitergeleitet. Nach der Einrichtung der gewünschten Kanäle können Sie zur Seite **Benachrichtigungsvorlage** zurückkehren, um mit dem Hinzufügen bzw. Ändern von Benachrichtigungsvorlagen fortzufahren.

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

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 bestimmter Vorlagentypen wird “Manuelles Senden wird unterstützt” angezeigt. Diese 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)}

     > **Hinweis:**
     >
     > Die XenMobile Server-Konsole enthält im Englischen die Begriffe “Blacklist” und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

   - ${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. Informationen zur Verwendung von Makros in einer Nachricht finden Sie unter Makros.
- **Audiodatei:** Wählen Sie den Benachrichtigungston aus, der bei Empfang einer Benachrichtigung ausgegeben werden soll.

SMTP:

- **Aktivieren:** Klicken Sie hier zum Aktivieren dieses Benachrichtigungskanals.

  Sie können die SMTP-Benachrichtigung erst aktivieren, nachdem Sie 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. Informationen zur Verwendung von Makros in einer Nachricht finden Sie unter Makros.

SMS:

- **Aktivieren:** Klicken Sie hier zum Aktivieren dieses Benachrichtigungskanals.

Sie können die SMTP-Benachrichtigung erst aktivieren, nachdem Sie den SMTP-Server 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 SMS-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. Informationen zur Verwendung von Makros in einer Nachricht finden Sie unter Makros.

4. 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 eine 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

Sie können nur Benachrichtigungsvorlagen löschen, die Sie hinzugefügt haben. Sie können vordefinierte Benachrichtigungsvorlagen nicht löschen.

1. Wählen Sie eine vorhandene Benachrichtigungsvorlage aus.
2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt.
3. Klicken Sie auf **Löschen**, um die Benachrichtigungsvorlage zu löschen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

Geräte

January 5, 2022

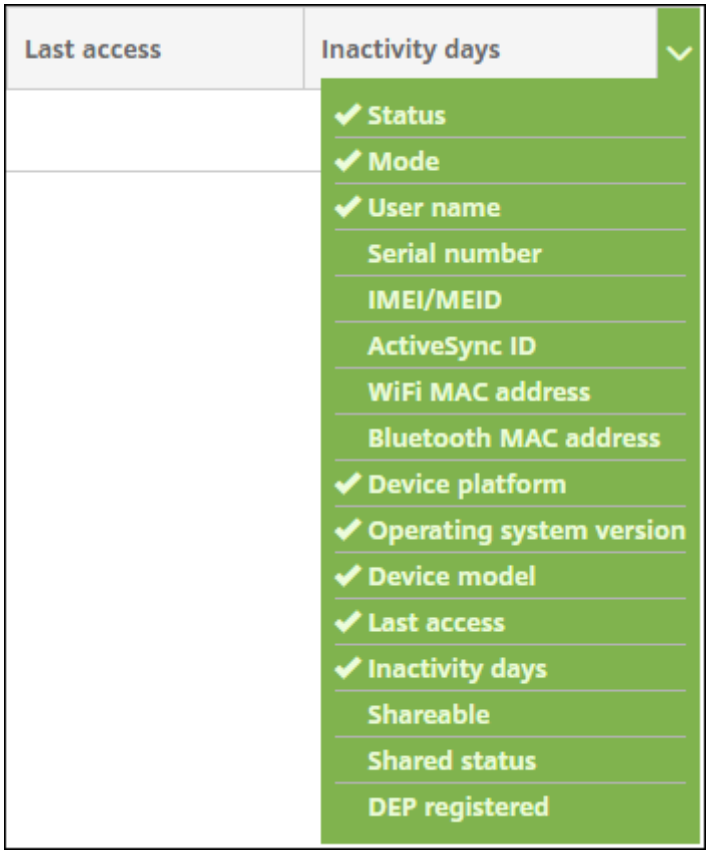
Citrix XenMobile kann verschiedenste Gerätetypen in einer einzigen Verwaltungskonsole bereitstellen, verwalten, sichern und inventarisieren.

In der XenMobile Server-Datenbank 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 Geräte-Provisioningdateiformate weiter unten in diesem Artikel.

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**, **Geräteplattform**, **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. Wählen Sie dann zusätzliche Spaltenüberschriften für die Anzeige in der Tabelle, bzw. deaktivieren Sie Spaltenüberschriften, die nicht angezeigt werden sollen.

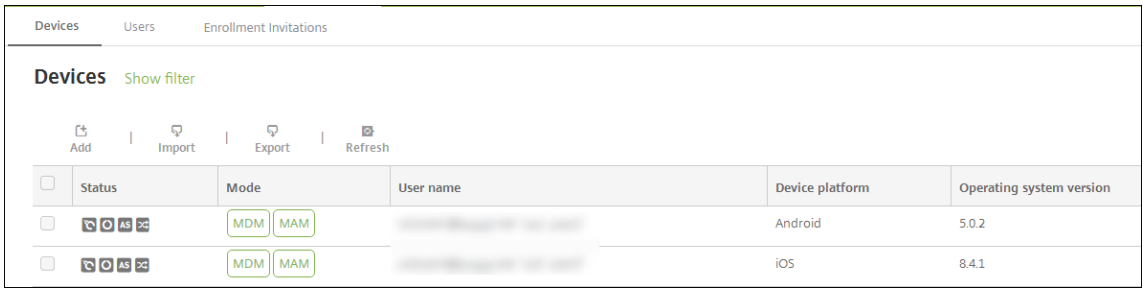


Sie können Geräte manuell hinzufügen, Geräte aus einer Geräteprovisioningdatei importieren,

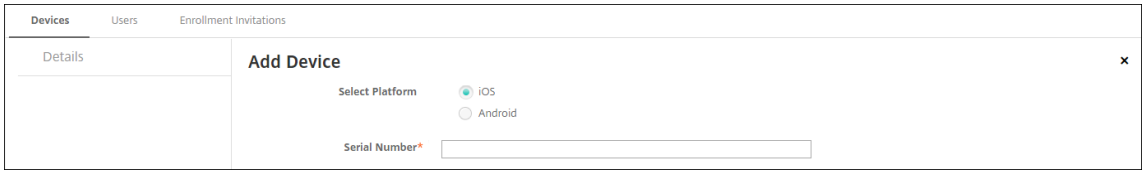
Gerätedetails bearbeiten, Sicherheitsaktionen durchführen und Benachrichtigungen an Geräte senden. Sie können auch alle Gerätedaten aus der Tabelle in eine CSV-Datei exportieren, um einen benutzerdefinierten Bericht zu erstellen. Es werden alle Geräteattribute exportiert. Wenn Sie Filter anwenden, werden diese beim Erstellen der CSV-Datei von XenMobile berücksichtigt.

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:

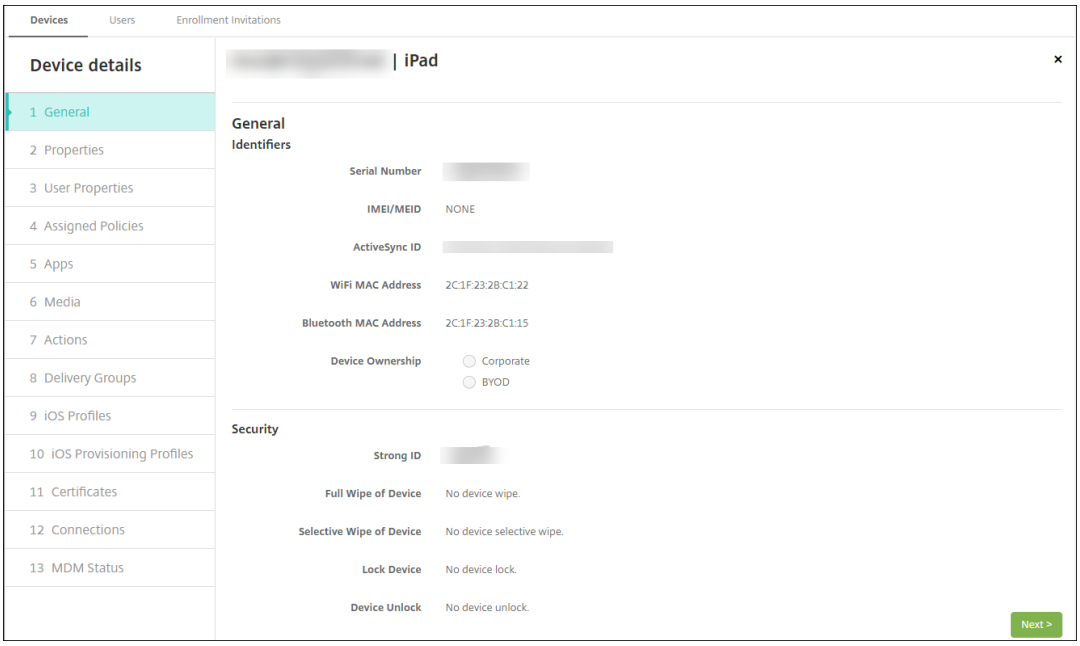
   - **Plattform wählen:** Klicken Sie auf **iOS** oder **Android**.
   - **Seriennummer:** Geben Sie die Seriennummer des Geräts ein.
   - **IMEI/MEID:** Geben Sie optional die IMEI/MEID des Geräts ein (nur Android-Geräte).

4. Klicken Sie auf **Hinzufügen**. Die Tabelle **Geräte** wird angezeigt. Das hinzugefügte Gerät befindet sich am Ende der Liste. Wählen Sie 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 aktivieren, wird das Menü mit den Optionen oberhalb der Liste angezeigt. Wenn Sie an eine andere Stelle in der Liste klicken, wird das Menü mit den Optionen rechts daneben angezeigt.

   - XenMobile Server im Enterprise- (XME) oder MDM-Modus konfiguriert
   - LDAP konfiguriert
   - Bei Verwendung lokaler Gruppen und Benutzer:
     - Eine oder mehrere lokale Gruppen

  - Lokale Benutzer, die lokalen Gruppen zugewiesen sind
  - Bereitstellungsgruppen, die lokalen Gruppen zugeordnet sind
- Bei Verwendung von Active Directory:
  - Bereitstellungsgruppen, die Active Directory-Gruppen zugeordnet sind



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 zudem **Sicherheitseigenschaften** aufgeführt, z. B. starke ID, Gerätesperrung, Umgehen der Aktivierungssperre und weitere plattformspezifische Informationen. Das Feld **Gerät vollständig löschen** enthält den Benutzer-PIN-Code. Der Benutzer muss den Code eingeben, anschließend erfolgt die Löschung. Wenn der Benutzer den Code vergessen hat, können Sie ihn hier nachsehen.

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 aus. Gültige Werte für jede Eigenschaft finden Sie in der PDF Device property names and values.

   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. XenMobile löscht das Element sofort.

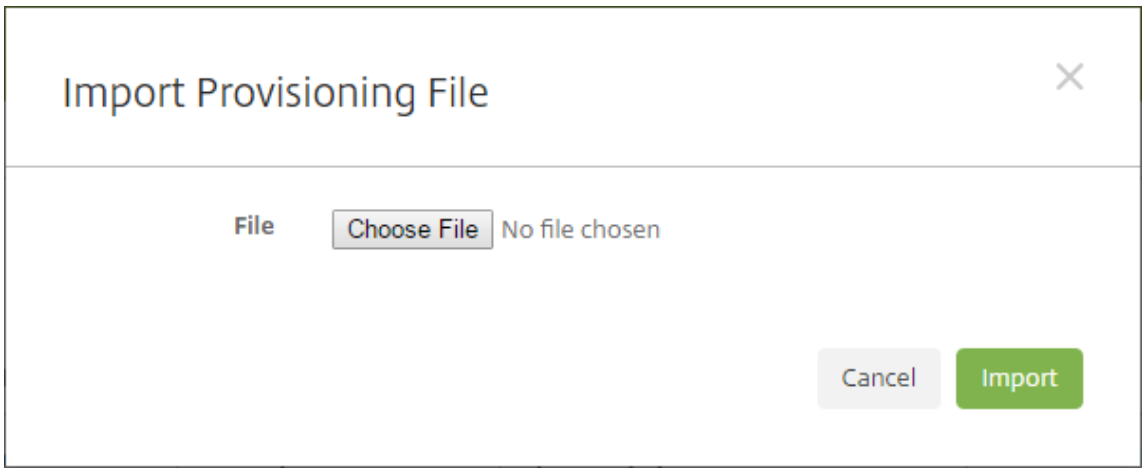
7. Die verbleibenden Abschnitte mit **Gerätedetails** enthalten zusammenfassende Informationen zu dem Gerät.

    - **Benutzereigenschaften:** Zeigt RBAC-Rollen, Gruppenmitgliedschaften, Volume Purchase-Konten und Eigenschaften des Benutzers an. Auf dieser Seite können Sie ein Volume Purchase-Konto deaktivieren.
    - **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 fehlgeschlagenen App-Bereitstellungen der letzten Bestandsaufnahme an. Es werden App-Name, ID, Typ und weitere Informationen angezeigt.
    - **Medien:** zeigt die Anzahl der erfolgreichen, ausstehenden und fehlgeschlagenen Medienbereitstellungen der letzten Bestandsaufnahme an.
    - **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 aus, 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.
    - **MDM-Status:** zeigt Informationen wie MDM-Status, Zeitpunkt der letzten Pushbenachrichtigung und letzte Geräteantwortzeit an.

Importieren von Geräten aus einer Provisioningdatei

Sie können die Datei eines Mobilfunkanbieters oder Geräteherstellers oder Ihre eigene Provisioningdatei importieren. Weitere Informationen finden Sie unter Geräte-Provisioningdateiformate in diesem Artikel.

1. Gehen Sie zu **Verwalten > Geräte** und klicken Sie auf **Importieren**. Das Dialogfeld **Provisioningdatei importieren** wird angezeigt.

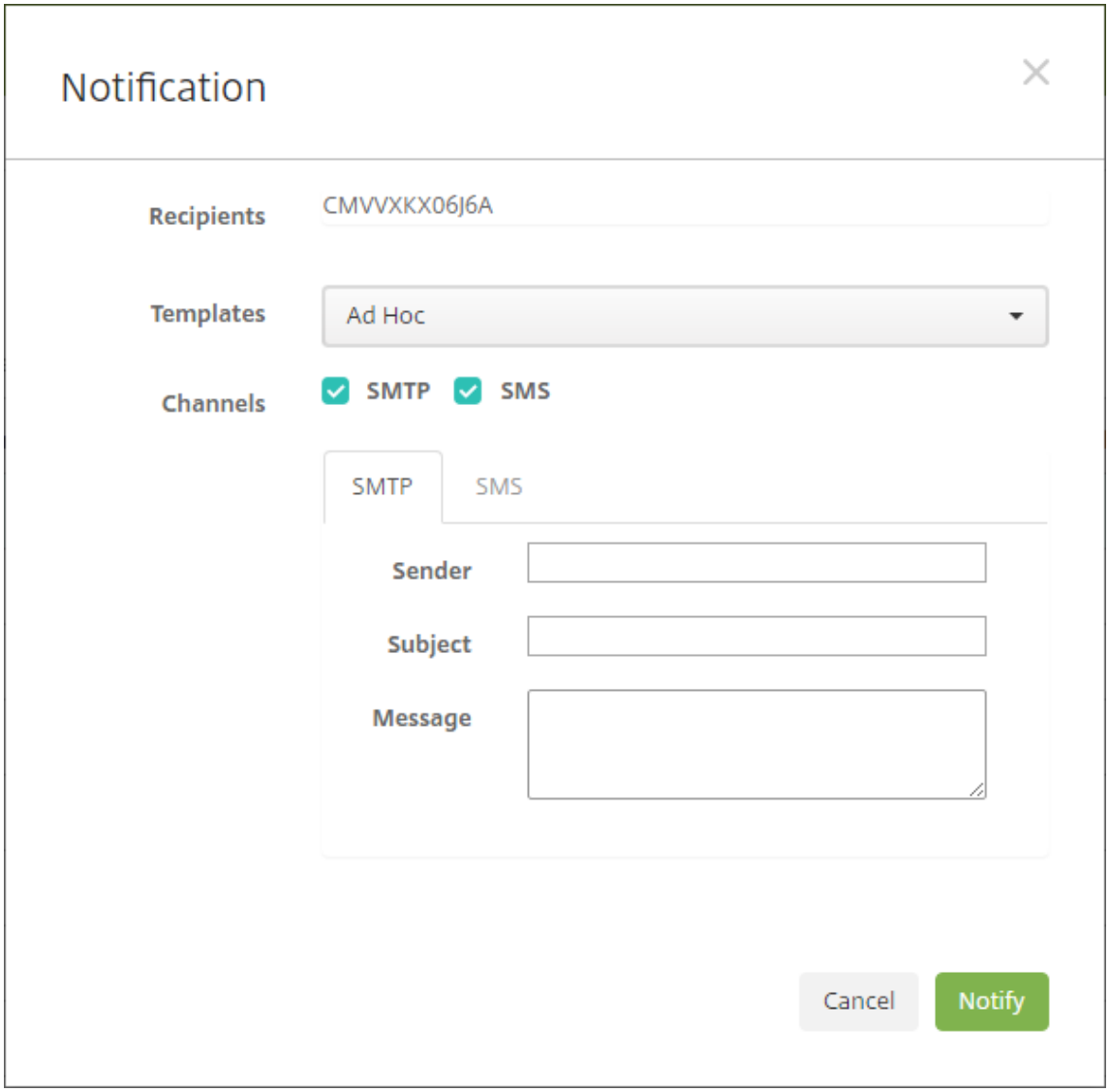


2. Klicken Sie auf **Datei wählen** und navigieren Sie zu der Datei, die Sie importieren möchten.
3. Klicken Sie auf **Importieren**. Die importierte Datei wird der Tabelle **Geräte** hinzugefügt.
4. Zum Bearbeiten der Geräteinformationen wählen Sie die Datei und klicken Sie auf **Bearbeiten**. Informationen über die Seiten mit den **Gerätedetails** finden Sie unter Manuelles Hinzufügen von Geräten.

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 sollen.



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**.

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**. XenMobile extrahiert die Informationen in der gefilterten Tabelle **Geräte** und konvertiert sie in eine CSV-Datei.
3. Bei Erscheinen der entsprechenden Aufforderung öffnen oder speichern Sie die CSV-Datei.

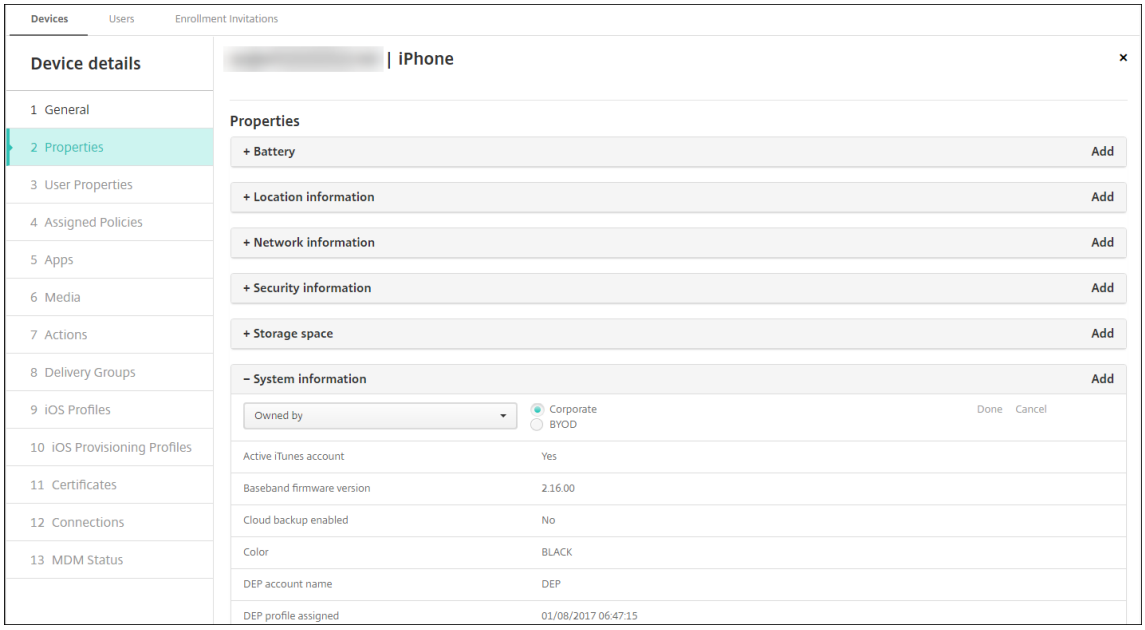
Geräte manuell per Tag kennzeichnen

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. Sie können Geräte auch wie folgt manuell kennzeichnen.

1. Fügen Sie dem Gerät über die Registerkarte **Geräte** in der XenMobile-Konsole eine Eigenschaft hinzu.
2. Fügen Sie die Eigenschaft **Besitz von** hinzu und wählen Sie entweder **Unternehmen** oder **BYOD** (Privatgerät).



Geräte-Provisioningdateiformate

Viele Mobilfunkanbieter und Mobilgerätehersteller geben Listen autorisierter Mobilgeräte heraus. Sie können diese Listen verwenden, statt lange Mobilgerätelisten manuell einzugeben. 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

Beachten Sie Folgendes:

- Gültige Werte für jede Eigenschaft finden Sie in der PDF Device property names and values.
- 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:

  ```
  propertyV;test;1;2
  ```

  Schützen Sie das Semikolon wie unten dargestellt:

  ```
  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:

```
`1050BF3F51730108161006551059039l;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F51730108161006551059039l;25244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F51730108161006551059039l;35244201625379903;iOS;test;
4050BF3F51730108161006551059039l;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

Jede Zeile der Datei enthält ein Gerät. Der erste Eintrag in dem Beispiel oben bedeutet Folgendes:

- SerialNumber: `1050BF3F51730108161006551059039l`
- IMEI: `15244201625379901`

- OperatingSystemFamily: `WINDOWS`
- PropertyName: `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

ActiveSync-Gateway

January 5, 2022

ActiveSync ist ein Protokoll zur Synchronisierung mobiler Daten von Microsoft. ActiveSync synchronisiert Daten auf Handheld-Geräten und PC bzw. Laptops.

Sie können ActiveSync-Gatewayregeln in XenMobile konfigurieren. Basierend auf diesen Regeln können Sie Geräten den Zugriff auf ActiveSync-Daten bewilligen oder verweigern. Wenn Sie beispielsweise die Regel "Missing Required Apps" aktivieren, prüft XenMobile per App-Zugriffsrichtlinie auf erforderliche Apps und verweigert den Zugriff auf ActiveSync-Daten, wenn die erforderlichen Apps fehlen. 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: Diese Aktion ist die Standardeinstellung für das ActiveSync-Gateway. Das Gateway erstellt eine Liste aller Geräte, die keines der anderen Filterkriterien erfüllen, und lässt den Zugriff zu bzw. blockiert ihn für diese Geräte. Wenn keine Regel zutrifft, ist die Standardaktion Implizit zulassen.

Inaktive Geräte: Prüft, ob ein Gerät entsprechend dem Wert unter "Inaktivitätsschwellenwert (Tage)" in den Servereigenschaften inaktiv ist.

Fehlende Pflicht-Apps: Prüft, ob auf einem Gerät Apps fehlen, die in einer App-Zugriffsrichtlinie definiert sind.

Nicht empfohlene Apps: Prüft, ob ein Gerät nicht empfohlene Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind.

Nicht richtlinientreues Kennwort: Prüft, ob das Benutzerkennwort richtlinientreu ist. Auf iOS- und Android-Geräten kann XenMobile feststellen, ob das aktuelle Kennwort des Geräts die an das Gerät gesendete Kennwortrichtlinie erfüllt. Auf iOS-Geräten haben Benutzer beispielsweise 60 Minuten, um ein Kennwort festzulegen, wenn XenMobile eine Kennwortrichtlinie an das Gerät sendet. Bevor der Benutzer das Kennwort festlegt, ist das Kennwort u. U. nicht richtlinientreu.

Nicht richtlinientreue Geräte: Prüft anhand der Eigenschaft für nicht richtlinientreue Geräte, ob ein Gerät richtlinientreu ist. Diese Eigenschaft wird normalerweise von automatisierten Aktionen geändert oder von einem Dritten durch Verwenden von XenMobile-APIs.

Widerrufenstatus: Prüft, ob das Gerätezertifikat widerrufen worden ist. Ein widerrufenes Gerät kann erst erneut registriert werden, wenn es wieder autorisiert ist.

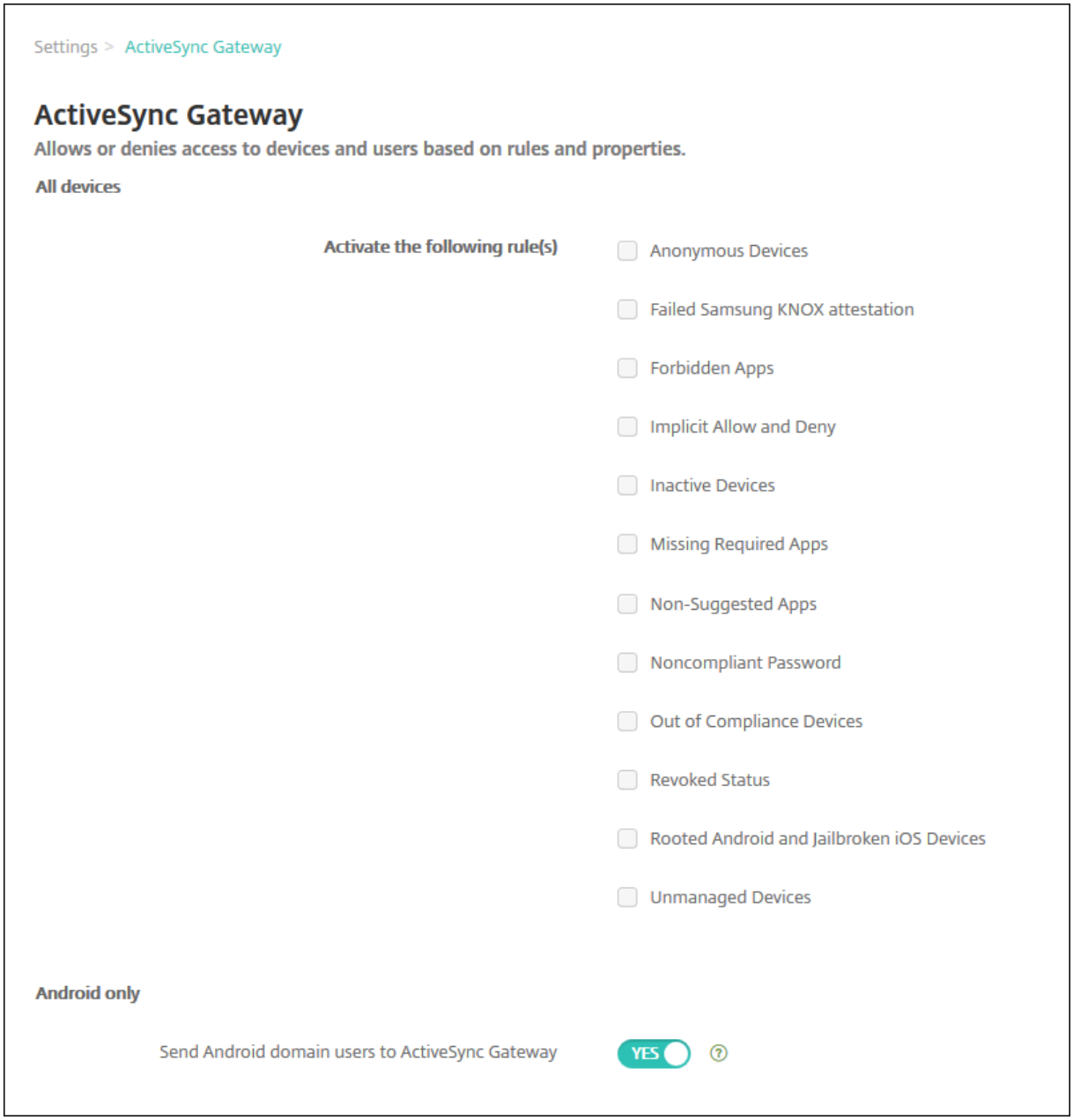
Android-Geräte mit Rooting oder iOS-Geräte mit Jailbreak: Prüft, ob auf einem Android- oder iOS-Gerät ein Jailbreak vorliegt.

Nicht verwaltete Geräte: Prüft, ob ein Gerät verwaltet, d. h. von XenMobile kontrolliert wird. Beispielsweise wird ein bei MAM registriertes Gerät 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.

Konfigurieren der Einstellungen für ActiveSync-Gateway

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.



1. Wählen Sie unter **Folgende Regel(n) aktivieren** eine oder mehrere Regeln aus, die Sie aktivieren möchten.
2. 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.
3. Klicken Sie auf **Speichern**.

Migration von der Geräteverwaltung zu Android Enterprise

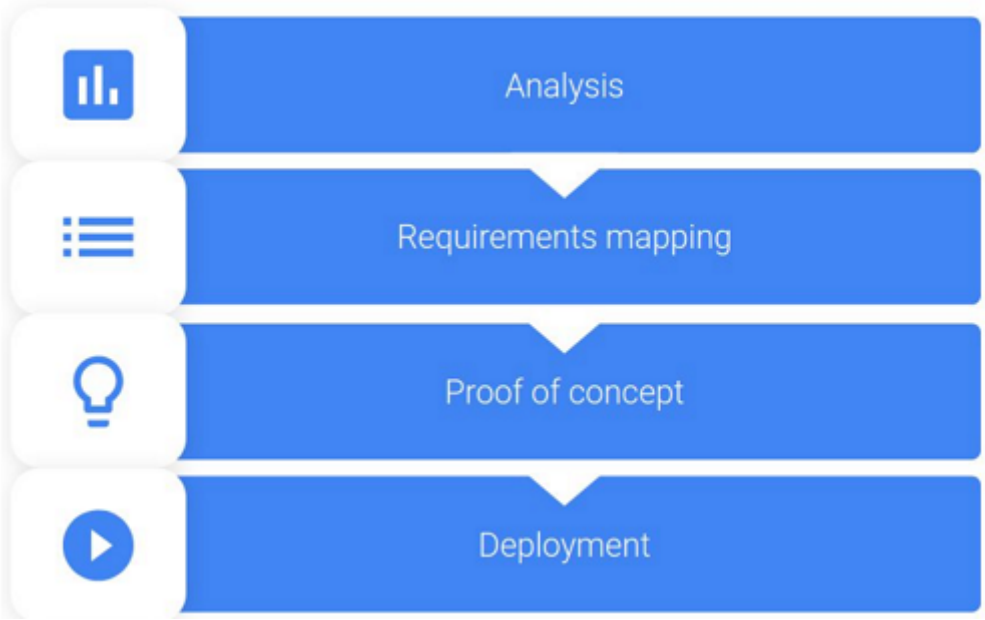
February 18, 2020

Dieser Artikel enthält Überlegungen und Empfehlungen zur Migration von Androids Legacy-Geräteverwaltung auf Android Enterprise. Google stellt die Unterstützung für Android Device Administration APIs ein. Diese APIs unterstützten Unternehmensapps auf Android-Geräten. Android Enterprise ist die moderne Verwaltungslösung, die von Google und Citrix empfohlen wird.

XenMobile verwendet zukünftig Android Enterprise als Standardverfahren zur Registrierung von Android-Geräten. Nach Ablauf der API-Unterstützung schlägt die Registrierung für Android Q-Geräte im Geräteverwaltungsmodus fehl.

Android Enterprise bietet Unterstützung für vollständig verwaltete Geräte und für Arbeitsprofilgeräte. Im Android Enterprise Migration Bluebook, einer Publikation von Google, werden die Unterschiede von Legacy-Geräteverwaltung und Android Enterprise ausführlich erläutert. Wir empfehlen Ihnen, diese Migrationshinweise von Google zu lesen.

Die Publikation enthält auch eine Beschreibung der vier Phasen der Migration der Geräteverwaltung und bietet folgendes Diagramm. Dieser Artikel enthält spezifische Empfehlungen für XenMobile für die Migrationsphasen.



> Diagramm aus dem Android Enterprise Migration Bluebook.
> Veröffentlicht mit Zustimmung von Google.

Auswirkungen der nicht mehr unterstützten Geräteverwaltung

Die folgenden Device Administration APIs werden von Google zukünftig nicht mehr unterstützt. Diese APIs funktionieren auf Geräten mit Android Q nicht mehr, nachdem Sie Secure Hub aktualisiert haben:

- Kamera deaktivieren: Steuert den Zugriff auf Gerätekameras.
- Kennwortablauf: Zwingt Benutzer, ihr Kennwort nach einem konfigurierbaren Zeitraum zu ändern.
- Kennwort beschränken: Legt restriktive Kennwortanforderungen fest.

Die veralteten APIs haben keine Auswirkungen auf Geräte, die im Nur-MAM-Modus von Citrix registriert sind.

Empfehlungen

Die folgenden Empfehlungen gelten für Geräte im Legacy-Geräteverwaltungsmodus von Android, für nicht registrierte Geräte und für im Nur-MAM-Modus von Citrix registrierte Geräte.

Geräteregistrierungsstatus	Empfohlene Aktion
Bestandsgerät ist im Geräteverwaltungsmodus registriert und kann auf Android Q aktualisiert werden.	Bevor Sie das Gerät auf Android Q aktualisieren, migrieren Sie vom Geräteverwaltungsmodus zu Android Enterprise.
Bestandsgerät ist im Geräteverwaltungsmodus registriert. Das Gerät kann nicht auf Android Q aktualisiert werden.	Das Gerät kann im Geräteverwaltungsmodus verbleiben. Planen Sie jedoch einen Wechsel zu Android Enterprise bei der Aktualisierung des Geräts.
Bestandsgerät ist im Geräteverwaltungsmodus registriert und wurde auf Android Q aktualisiert.	Migrieren Sie vom Geräteverwaltungsmodus zu Android Enterprise, bevor Google die API-Unterstützung einstellt. In der XenMobile-Konsole wird eine Warnmeldung für diese Geräte angezeigt.
Neugerät, das mit Android Q geliefert wird und im Geräteverwaltungsmodus registriert ist.	Migrieren Sie vom Geräteverwaltungsmodus zu Android Enterprise, bevor Google die API-Unterstützung einstellt. In der XenMobile-Konsole wird eine Warnmeldung für diese Geräte angezeigt.
Neugerät, das mit Android Q geliefert wird oder auf Android Q aktualisiert werden kann. Das Gerät ist nicht registriert.	Verwenden Sie Android Enterprise für alle neuen Geräte.

Geräteregistrierungsstatus	Empfohlene Aktion
Neu- oder Bestandsgerät mit Android Q wird im Geräteverwaltungsmodus registriert, nachdem Google die Unterstützung der APIs beendet hat.	Um die Auswirkungen veralteter Google-APIs zu vermeiden, empfiehlt Citrix die Migration zu Android Enterprise, bevor Google die API-Unterstützung einstellt. Nach dem Ende der Unterstützung schlägt die Registrierung dieser Geräte fehl.
Neu- oder Bestandsgeräte, die im Nur-MAM-Modus von Citrix registriert sind	Keine Aktion erforderlich. Die veralteten Google APIs haben keine Auswirkungen auf Geräte im Nur-MAM-Modus.

Analyse

Die Analysephase der Migration umfasst Folgendes:

- Verständnis Ihres Legacy-Android-Setups
- Dokumentation Ihres Legacy-Setups, um Legacy-Features und Android Enterprise-Features einander zuzuordnen

Empfohlene Analyse

1. Bewerten Sie Android Enterprise auf XenMobile: Vollständig verwaltet, vollständig verwaltet mit Arbeitsprofil, dediziertes Gerät, Arbeitsprofil (BYOD).
2. Analysieren Sie Ihre aktuellen Geräteverwaltungsfeatures im Vergleich zu Android Enterprise.
3. Dokumentieren Sie die Anwendungsfälle Ihrer Geräteverwaltung.

Dokumentieren der Anwendungsfälle Ihrer Geräteverwaltung:

1. Erstellen Sie eine Tabelle und listen Sie die aktuellen Richtliniengruppen in der XenMobile-Konsole auf.
2. Erstellen Sie separate Anwendungsfälle auf der Basis der vorhandenen Richtliniengruppen.
3. Dokumentieren Sie für jeden Anwendungsfall Folgendes:
    - Name
    - Geschäftsinhaber
    - Benutzeridentitätsmodell
    - Geräteanforderungen
        - Sicherheit
        - Verwaltung

        - Benutzerfreundlichkeit
    - Gerätebestand
        - Marke und Modell
        - Betriebssystemversion
    - Apps
4. Führen Sie für jede App Folgendes auf:
    - App-Name
    - Paketname
    - Hostmethode
    - App ist öffentlich oder privat
    - App ist obligatorisch (true/false)

Anforderungszuordnung

Ermitteln Sie anhand der abgeschlossenen Analyse Ihre Android Enterprise-Featureanforderungen.

Empfohlene Anforderungszuordnung

1. Bestimmen Sie den Verwaltungsmodus und die Registrierungsmethode:
    - Arbeitsprofil (BYOD): Neuregistrierung erforderlich. Kein Zurücksetzen auf Werkseinstellungen erforderlich.
    - Vollständig verwaltet: Zurücksetzen auf Werkseinstellung erforderlich. Registrieren Sie Geräte per QR-Code, NFC-Übertragung, DPC-ID (Device Policy Controller), Zero Touch.
2. Erstellen Sie eine App-Migrationsstrategie.
3. Ordnen Sie den Android Enterprise-Features Anwendungsfallanforderungen zu. Dokumentieren Sie das Feature für jede Gerätanforderung, die der Anforderung und ihrer entsprechenden Android-Version am ehesten entspricht.
4. Bestimmen Sie das Android-Mindestbetriebssystem basierend auf den Featureanforderungen (7.0, 8.0, 9.0).
5. Wählen Sie ein Identitätsmodell:
    - Empfohlen: verwaltetes Google Play-Konto
    - Google G Suite-Konten nur als Google Cloud-Identitätskunde verwenden
6. Erstellen Sie eine Gerätestrategie:
    - Keine Aktion: Geräte besitzen OS-Mindestversion

- Upgrade: Geräte unterstützen das unterstützte Betriebssystem und können aktualisiert werden
- Ersetzen: Geräte können nicht auf das unterstützte Betriebssystem aktualisiert werden

Empfohlene App-Migrationsstrategie

Nach dem Abschluss der Anforderungszuordnungen verschieben Sie die Apps von der Android-Plattform auf die Android Enterprise-Plattform. Weitere Informationen zum Veröffentlichen von Apps finden Sie unter Hinzufügen von Apps.

- Apps im öffentlichen App-Store
  1. Wählen Sie die zu migrierenden Apps aus. Bearbeiten Sie die Apps, indem Sie die Google Play-Einstellung deaktivieren und **Android Enterprise** als Plattform auswählen.
  2. Wählen Sie die Bereitstellungsgruppe aus. Verschieben Sie obligatorische Apps in die Liste **Erforderliche Apps** in der Bereitstellungsgruppe.

  Nach dem Speichern einer App wird sie im Google Play Store angezeigt. Bei vorhandenem Arbeitsprofil werden Apps im Google Play Store im Arbeitsprofil angezeigt.
- Private (Unternehmens-)Apps

  Private Apps werden intern oder von einem Drittanbieter entwickelt. Es wird empfohlen, private Apps mit Google Play zu veröffentlichen.
  1. Wählen Sie die zu migrierenden Apps aus, und bearbeiten Sie sie, indem Sie **Android Enterprise** als Plattform auswählen.
  2. Laden Sie die APK-Datei hoch und konfigurieren Sie die App-Einstellungen.
  3. Veröffentlichen Sie die App in der erforderlichen Bereitstellungsgruppe.
- MDX-Apps
  1. Wählen Sie die zu migrierenden Apps aus, und bearbeiten Sie sie, indem Sie **Android Enterprise** als Plattform auswählen.
  2. Laden Sie die MDX-Datei hoch. Durchlaufen Sie den App-Genehmigungsprozess.
  3. Wählen Sie die MDX-Richtlinien aus.

  Für Enterprise MDX-Apps empfehlen wir, diese im SDK-Modus zu umschließen:
  - Option 1: Hosten Sie die APK in Google Play mit einem Entwicklerkonto, das Ihrer Organisation privat zugewiesen wurde. Veröffentlichen Sie die MDX-Datei in XenMobile.
  - Option 2: Veröffentlichen Sie die App aus XenMobile als Unternehmensapp. Veröffentlichen Sie die APK in XenMobile und wählen Sie die Plattform **Android Enterprise** für die MDX-Datei.

Migration der Citrix Geräterichtlinien

Wenn Richtlinien für Android- und Android Enterprise-Plattformen verfügbar sind, bearbeiten Sie die Richtlinie und wählen als Plattform **Android Enterprise** aus.

Berücksichtigen Sie für Android Enterprise den Registrierungsmodus. Einige Richtlinienoptionen sind nur für Geräte im Arbeitsprofilmodus oder im vollständig verwalteten Modus verfügbar.

Proof of concept

Nach der Migration von Apps in Android Enterprise können Sie in einem Migrationstest prüfen, ob alle Features ordnungsgemäß funktionieren.

Empfohlenes Testsetup

1. Richten Sie die Bereitstellungsinfrastruktur ein:
    - Erstellen Sie eine Bereitstellungsgruppe für den Android Enterprise-Test.
    - Konfigurieren Sie Android Enterprise in XenMobile.
2. Richten Sie Benutzer-Apps ein.
3. Konfigurieren Sie Android Enterprise-Features.
4. Weisen Sie der Android Enterprise-Bereitstellungsgruppe Richtlinien zu.
5. Testen und bestätigen Sie die Features.
6. Erstellen Sie für jeden Anwendungsfall eine Anleitung für den Gerätesetup.
7. Dokumentieren Sie die Schritte für den Benutzersetup.

Bereitstellung

Sie können nun den Android Enterprise-Setup bereitstellen und Benutzer auf die Migration vorbereiten.

Empfohlene Bereitstellungsstrategie

Die von Citrix empfohlene Bereitstellungsstrategie besteht darin, alle Produktionssysteme für Android Enterprise zu testen und anschließend die Gerätemigration abzuschließen.

- In diesem Szenario verwenden Benutzer weiterhin Legacy-Geräte mit ihrer aktuellen Konfiguration. Richten Sie neue Geräte für die Verwaltung mit Android Enterprise ein.
- Migrieren Sie bestehende Geräte nur, wenn ein Upgrade oder ein Austausch erforderlich ist.

- Nutzen Sie bestehende Geräte bis zum Ende des Lebenszyklus, und führen Sie anschließend eine Migration zur Android Enterprise-Verwaltung durch. Alternativ führen Sie eine Migration durch, wenn Geräte aufgrund von Verlust oder Beschädigung ersetzt werden müssen.

Android Enterprise

January 6, 2022

Android Enterprise ist eine Sammlung von Tools und Diensten, die von Google als Unternehmensverwaltungslösung für Android-Geräte bereitgestellt werden. Bei Einsatz von Android Enterprise gilt:

- Sie verwalten firmeneigene Android-Geräte und private Android-Arbeitsgeräte (BYOD) mit XenMobile.
- Sie können das gesamte Gerät oder ein separates Profil auf dem Gerät verwalten. Das separate Profil isoliert geschäftliche Konten, Apps und Daten von persönlichen Konten, Apps und Daten.
- Sie können damit auch dedizierte Einzweckgeräte verwalten, z. B. Geräte für die Bestandsverwaltung. Eine Übersicht über Android Enterprise-Funktionen von Google finden Sie unter Android Enterprise Management.

Ressourcen:

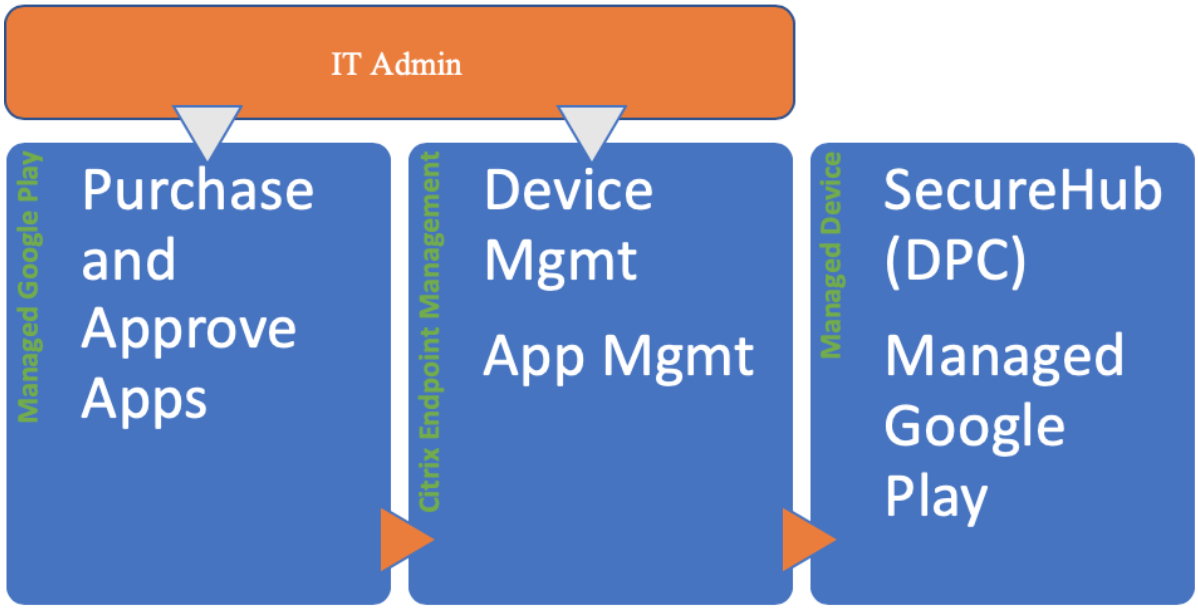
- Eine Liste mit Begriffen und Definitionen für Android Enterprise finden Sie unter Android Enterprise terminology im Google Android Enterprise-Entwicklerhandbuch. Diese Liste wird von Google häufig aktualisiert.
- Informationen zu Android-Betriebssystemen, die von XenMobile unterstützt werden, finden Sie unter Unterstützte Gerätebetriebssysteme.
- Weitere Informationen zu den ausgehenden Verbindungen beim Einrichten von Netzwerkumgebungen für Android Enterprise finden Sie im Google-Hilfeartikel Android Enterprise Network Requirements.

Wenn Sie XenMobile mit verwaltetem Google Play zur Verwendung von Android Enterprise integrieren, erstellen Sie ein Unternehmen. Google definiert ein Unternehmen als Bindeglied zwischen der Organisation und Ihrer EMM-Lösung (Enterprise Mobile Management). Alle Benutzer und Geräte, die die Organisation über Ihre Lösung verwaltet, gehören zu diesem Unternehmen.

Ein Unternehmen für Android Enterprise besteht aus drei Komponenten: einer EMM-Lösung, einer DPC-App (Device Policy Controller) und einer Google-Plattform für Unternehmensapps. Wenn Sie XenMobile und Android Enterprise kombinieren, besteht die Komplettlösung aus folgenden Komponenten:

- **XenMobile:** Endpunktverwaltungslösung von Citrix. XenMobile ist die einheitliche XenMobile-Lösung für einen sicheren digitalen Workspace. XenMobile bietet IT-Administratoren die Möglichkeit, Geräte und Apps für ihre Organisationen zu verwalten.
- **Citrix Secure Hub:** Die DPC-App von Citrix. Secure Hub ist das Launchpad für XenMobile. Secure Hub ermöglicht das Durchsetzen von Richtlinien auf dem Gerät.
- **Verwaltetes Google Play:** Googles Plattform für Unternehmensapps, die mit XenMobile integriert ist. Die Google Play EMM-API legt App-Richtlinien fest und verteilt Apps.

Diese Abbildung zeigt die Interaktion von Administratoren mit den Komponenten und die Interaktion der Komponenten untereinander.



Verwenden von verwaltetem Google Play mit XenMobile

> **Hinweis:**
>
> Sie können Citrix über verwaltetes Google Play oder über Google Workspace als Ihren EMM-Anbieter registrieren. Im Folgenden wird die Verwendung von Android Enterprise mit verwaltetem Google Play beschrieben. Wenn Ihre Organisation Google Workspace für den App-Zugriff verwendet, können Sie es mit Android Enterprise verwenden. Siehe Kunden mit Legacy Android Enterprise für Google Workspace (ehemals G Suite).

Wenn Sie verwaltetes Google Play verwenden, stellen Sie verwaltete Google Play-Konten für Geräte und Endbenutzer bereit. Über verwaltete Google Play-Konten können Benutzer auf verwaltetes Google Play zugreifen und Apps installieren und verwenden, die Sie zur Verfügung stellen. Wenn Ihre Organisation den Identitätsdienst eines Drittanbieters verwendet, können Sie verwaltete Google Play-Konten mit den bestehenden Identitätskonten verknüpfen.

Da dieser Unternehmenstyp nicht an eine Domäne gebunden ist, können Sie für jede Organisation mehrere Unternehmen erstellen. Beispielsweise kann sich jede Abteilung oder Region in einer Organisation als ein eigenes Unternehmen anmelden, um separate Gruppen von Geräten und Apps zu verwalten.

Für XenMobile-Administratoren bietet verwaltetes Google Play neben der Benutzererfahrung und den App Store-Features von Google Play diverse Verwaltungsfunktionen für Unternehmen. Sie verwenden verwaltetes Google Play zum Hinzufügen, Erwerben und Genehmigen von Apps für die Bereitstellung in dem Android Enterprise-Workspace von Geräten. Über Google Play können Sie öffentliche Apps, private Apps und Apps von Drittanbietern bereitstellen.

Für Benutzer von verwalteten Geräten ist verwaltetes Google Play der Store für Unternehmensapps. Benutzer können Apps durchsuchen, App-Details anzeigen und sie installieren. Im Gegensatz zur öffentlichen Google Play-Version können Benutzer vom verwalteten Google Play nur die Apps installieren, die Sie ihnen zur Verfügung stellen.

Szenarien und Betriebsmodi der Gerätebereitstellung

Das Szenario der Gerätebereitstellung legt fest, wer Besitzer der bereitgestellten Geräte ist und wie Sie sie verwalten. Geräteprofile beziehen sich auf die Art und Weise, wie der DPC Richtlinien auf Geräten verwaltet und durchsetzt.

Ein Arbeitsprofil isoliert geschäftliche Konten, Apps und Daten von persönlichen Konten, Apps und Daten. Weitere Informationen zu Arbeitsprofilen finden Sie in der Google Android Enterprise-Hilfe unter Was ist ein Arbeitsprofil?.

> **Wichtig:**
>
> Beim Update von Android Enterprise-Geräten auf Android 11 migriert Google Geräte, mit der Einstellung “Vollständig verwaltet mit Arbeitsprofil” zu einem neuartigen Arbeitsprofil mit verbesserter Sicherheit. Weitere Informationen finden Sie unter Changes ahead for Android Enterprise’s Fully Managed with Work Profile.

Geräteverwaltung	Anwendungsfälle	Arbeitsprofil	Persönliches Profil	Hinweise
Unternehmenseig Geräte (vollständig verwaltet)	Unternehmenseig Geräte, die nur für den geschäftlichen Einsatz bestimmt sind	Nein	Ja. Der DPC kann geräteweite Aktionen ausführen, z. B. die Konnektivität für das Gerät konfigurieren, globale Einstellungen konfigurieren und die Werkseinstellungen zurücksetzen.	Nur für neue oder auf die Werkseinstellungen zurückgesetzte Geräte.
Vollständig verwaltet mit Arbeitsprofil	Unternehmenseigen Geräte, die für den geschäftlichen und privaten Einsatz bestimmt sind	Ja	Ja. Es werden zwei DPC-Kopien auf den Geräten ausgeführt, wobei ein DPC das Gerät im Gerätebesitzermodus und der zweite das Arbeitsprofil im Profilbesitzermodus verwaltet. Sie können separate Richtlinien für Gerät und Arbeitsprofil festlegen.	Solche Geräte wurden früher als COPE-Geräte (Unternehmenseigentum, vom Benutzer verwaltet) bezeichnet.

Geräteverwaltung	Anwendungsfälle	Arbeitsprofil	Persönliches Profil	Hinweise
Dedizierte Geräte*	Unternehmenseig Geräte, die für einen einzigen Anwendungsfall konfiguriert sind, z. B. digitale Werbetechnik oder Ticketdruck	Nein	Ja. Sie stellen nur die erforderlichen Apps bereit und verhindern, dass Benutzer weitere Apps hinzufügen.	Dedizierte Geräte wurden früher auch als unternehmen-seigene Einzweckgeräte (COSU) bezeichnet.
BYOD-Arbeitsprofil**	Private Geräte, die im Arbeit-sprofilmodus registriert sind (auch “Profilbe-sitzermodus”)	Ja	Ja. Der DPC verwaltet nur das Arbeitsprofil, nicht das gesamte Gerät.	Diese Geräte müssen nicht neu oder auf die Werkseinstellun-gen zurückgesetzt sein.

* Die Benutzer können ein dediziertes Gerät gemeinsam verwenden. Wenn sich ein Benutzer bei einer App auf einem dedizierten Gerät anmeldet, ist sein Arbeitsstatus nicht gerätebezogen, sondern App-bezogen.

** Zebra-Geräte können in XenMobile nicht als Geräte im BYOD-Arbeitsprofilmodus verwendet wer-den. XenMobile unterstützt Zebra-Geräte als vollständig verwaltete Geräte und als Geräte im Legacy-Modus (auch als Geräteadministratormodus bezeichnet).

Informationen zum Migrieren vom Legacymodus zum Gerätebesitzer- oder Profilbesitzermodus finden Sie unter Migration von der Geräteverwaltung zu Android Enterprise.

Authentifizierungsmethoden

Registrierungsprofile bestimmen, ob Android-Geräte bei MAM, MDM oder MDM+MAM registriert wer-den, wobei im letzteren Modus die Benutzer ggf. MDM abwählen können.

Weitere Informationen zum Festlegen der Sicherheitsstufe und zum Registrierungsverfahren finden Sie unter Konfigurieren von Registrierungssicherheitsmodi.

XenMobile unterstützt die folgenden Authentifizierungsverfahren für Android-Geräte, die in MDM+MAM registriert sind. Weitere Informationen finden Sie in den Artikeln unter Zertifikate

und Authentifizierung.

- Domäne
- Domäne plus Sicherheitstoken
- Clientzertifikat
- Clientzertifikat plus Domäne
- Identitätsanbieter:
  - Azure Active Directory
  - Citrix Identitätsanbieter

Eine weitere, selten verwendete Authentifizierungsmethode ist das Clientzertifikat plus Sicherheitstoken. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX215200.

Anforderungen

Vor dem Einsatz von Android Enterprise ist Folgendes erforderlich:

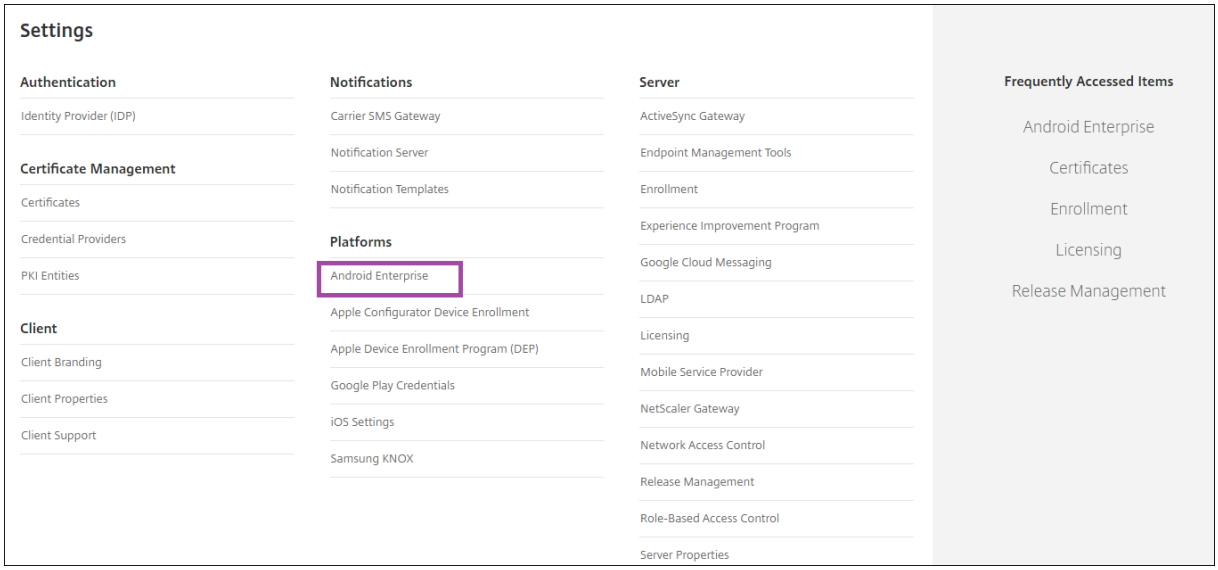
- Konten und Anmeldeinformationen:
  - Ein Google-Unternehmenskonto zum Einrichten von Android Enterprise mit verwaltetem Google Play
  - Ein Citrix-Kundenkonto zum Download der aktuellen MDX-Dateien
  - Ein Google-Entwicklerkonto zum Bereitstellen privater Apps (optional)
- Konfiguration von Firebase Cloud Messaging (FCM) für XenMobile Weitere Informationen hierzu finden Sie unter Firebase Cloud Messaging.
- Knox Premium-Lizenzen für Samsung Knox Mobile Enrollment (optional)

Verbinden von XenMobile mit Google Play

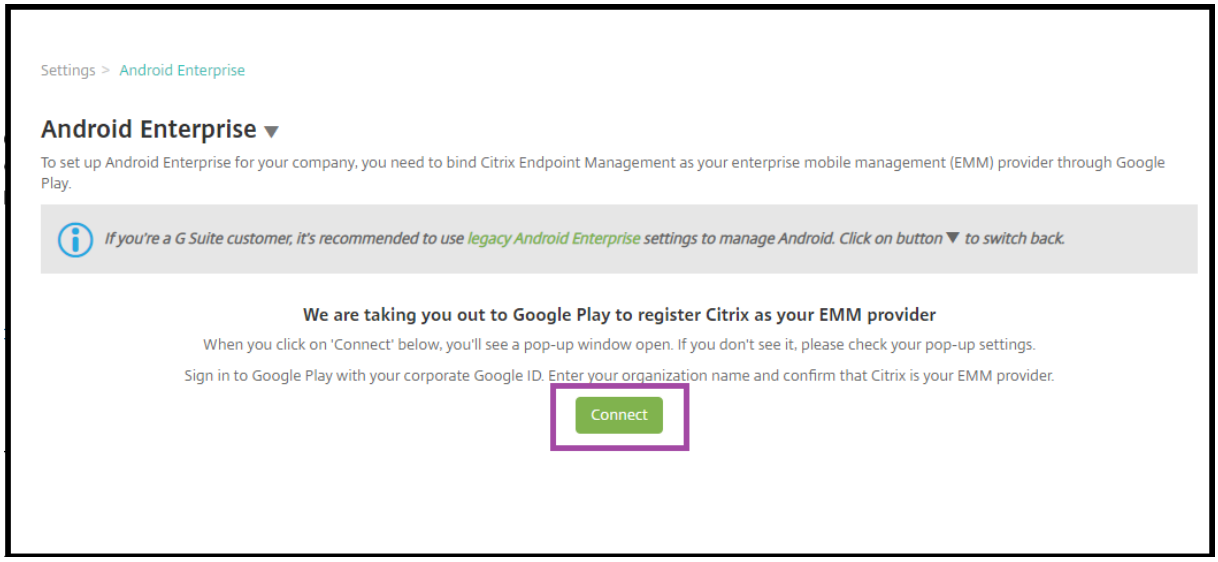
Um Android Enterprise für Ihre Organisation einzurichten, registrieren Sie Citrix über verwaltetes Google Play als EMM-Anbieter. Dieses Setup verbindet verwaltetes Google Play mit XenMobile und erstellt ein Unternehmen für Android Enterprise in XenMobile.

Sie benötigen ein Google-Unternehmenskonto, um sich bei Google Play anzumelden.

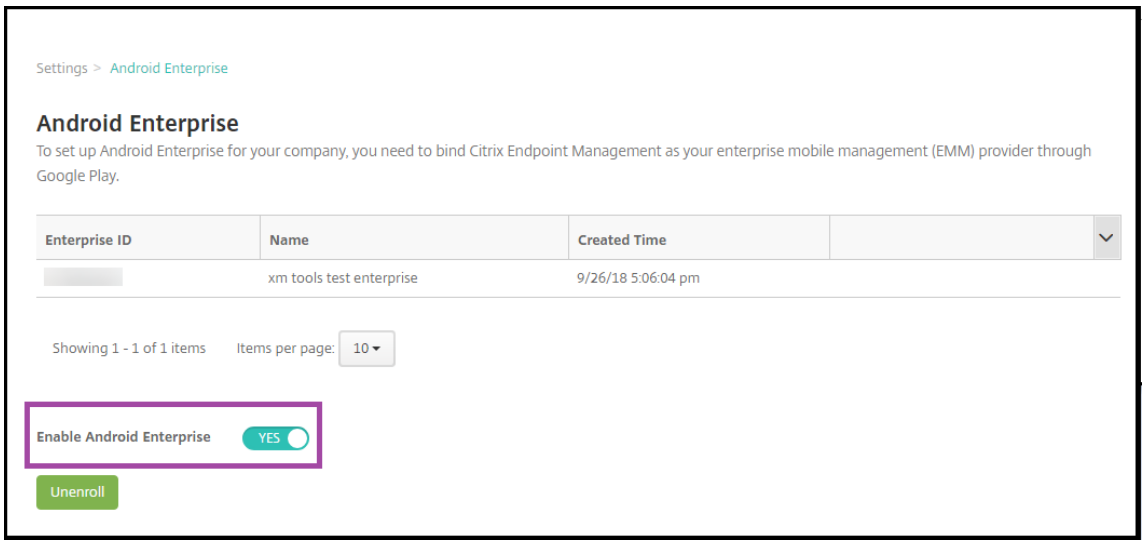
1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Gehen Sie zu **Einstellungen > Android Enterprise**.



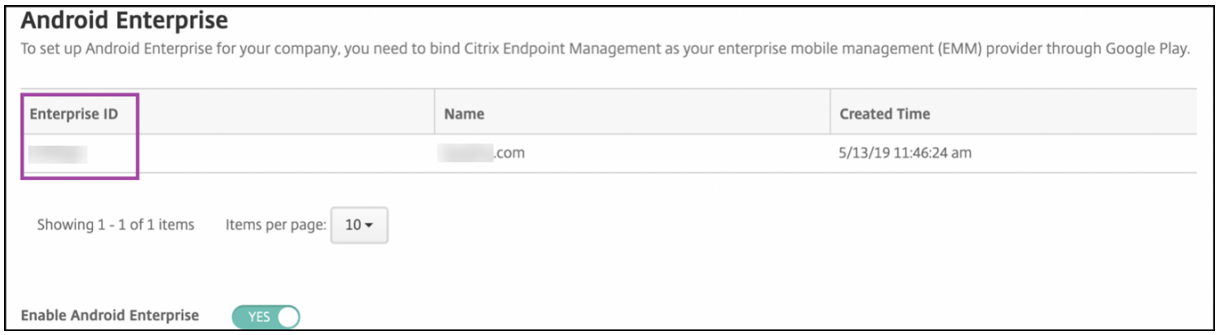
1. Klicken Sie auf **Verbinden**. Google Play wird geöffnet.



1. Melden Sie sich mit den Anmeldeinformationen für Ihr Google-Unternehmenskonto bei Google Play an. Geben Sie den Namen Ihrer Organisation ein und bestätigen Sie, dass Citrix Ihr EMM-Anbieter ist.
2. Eine Unternehmens-ID wurde für Android Enterprise hinzugefügt. Um Android Enterprise zu aktivieren, schieben Sie **Android Enterprise aktivieren** auf **Ja**.



Ihre Enterprise-ID wird in der XenMobile-Konsole angezeigt.



Ihre Umgebung ist mit Google verbunden und kann Geräte verwalten. Sie können nun Apps für Benutzer bereitstellen.

XenMobile kann verwendet werden, um Benutzern mobile Produktivitätsapps von Citrix, MDX-Apps, Apps aus dem öffentlichen App-Store, Web- und SaaS-Apps, Unternehmensapps und Weblinks zur Verfügung zu stellen. Weitere Informationen zu diesen App-Typen und zu ihrer Bereitstellung finden Sie unter Hinzufügen von Apps.

Im folgenden Abschnitt wird gezeigt, wie mobile Produktivitätsapps bereitgestellt werden.

Bereitstellen mobiler Produktivitätsapps von Citrix für Android Enterprise-Benutzer

Zum Bereitstellen mobiler Produktivitätsapps von Citrix für Android Enterprise-Benutzer sind folgende Schritte erforderlich.

1. Veröffentlichen Sie die Apps als MDX-Apps. Siehe Konfigurieren von Apps als MDX-Apps.
2. Konfigurieren Sie die Regeln für die Sicherheitsabfrage, die die Benutzer für den Zugriff auf die Arbeitsprofile auf ihren Geräten verwenden. Siehe Konfigurieren der Richtlinie für die Sicherheitsabfrage.

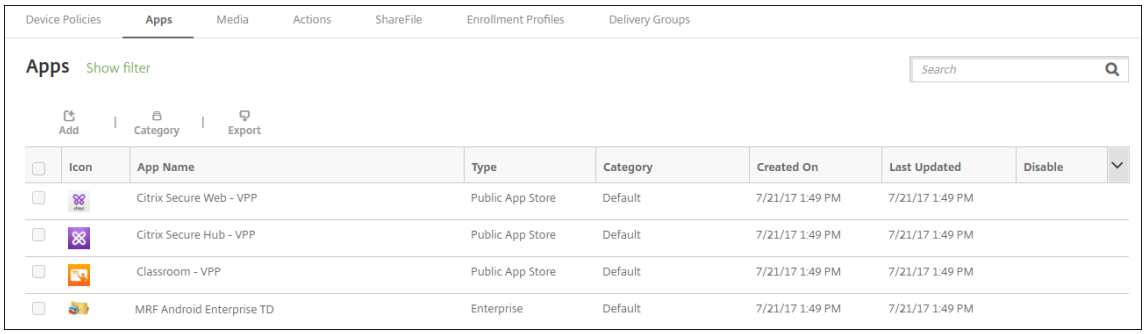
Die veröffentlichten Apps sind für Geräte verfügbar, die in Ihrem Android Enterprise-Unternehmen registriert sind.

> **Hinweis:**
>
> Wenn Sie einem Android-Benutzer eine App für Android Enterprise aus dem öffentlichen App-Store bereitstellen, wird dieser Benutzer automatisch bei Android Enterprise registriert.

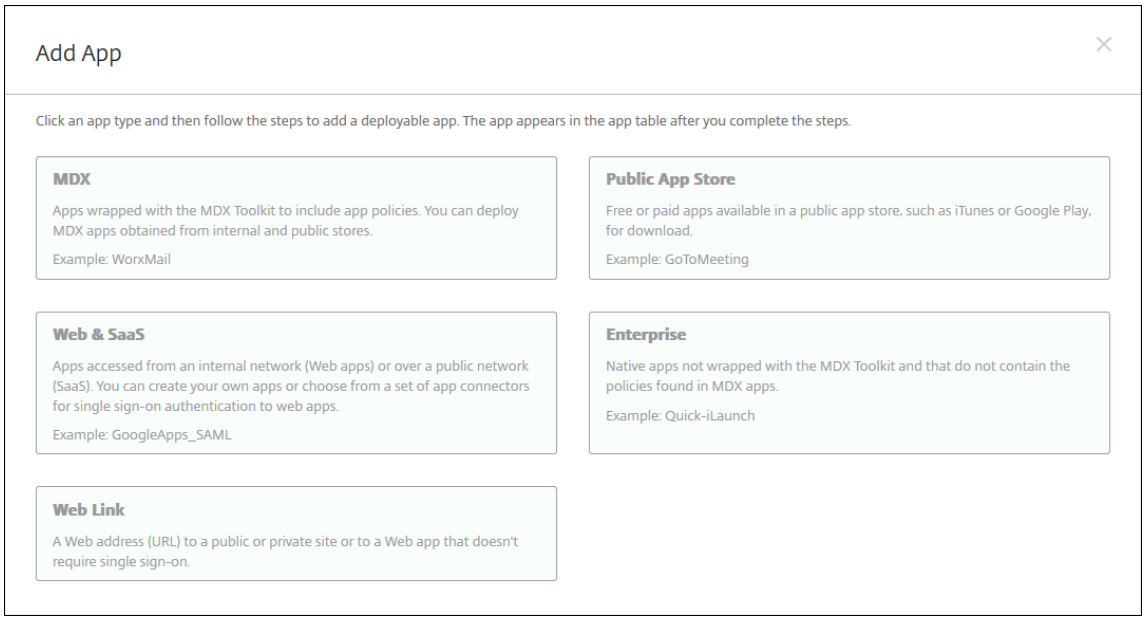
Konfigurieren von Apps als MDX-Apps

Gehen Sie zum Konfigurieren einer Citrix Produktivitätsapp als MDX-App für Android Enterprise folgendermaßen vor:

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

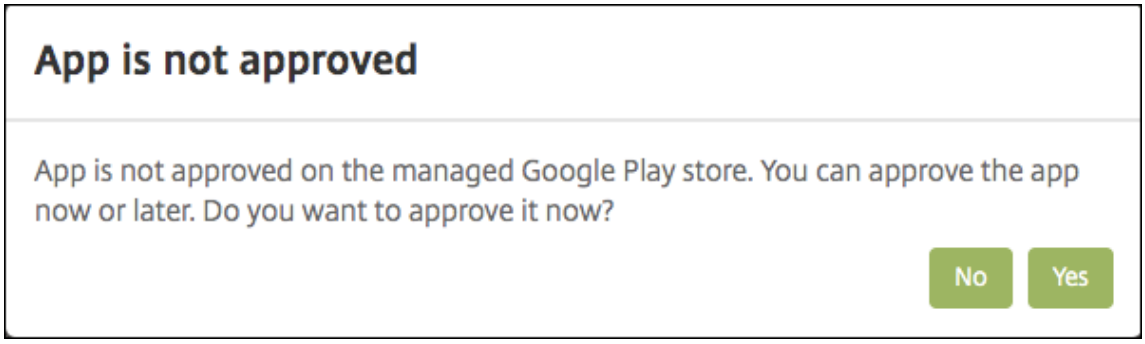


2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

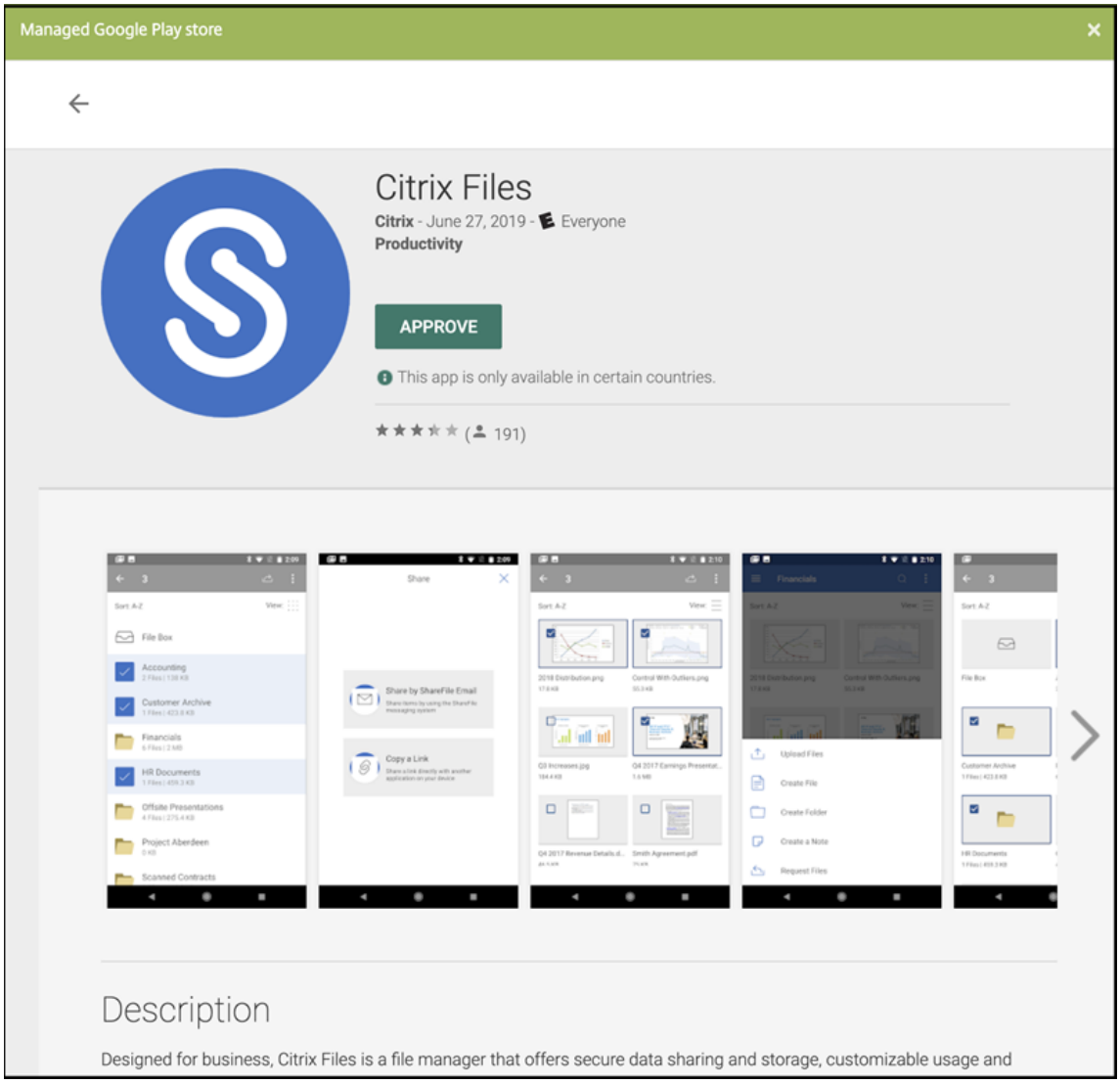


3. Klicken Sie auf **MDX**. Die Seite **App-Informationen** wird angezeigt.
4. Wählen Sie links **Android Enterprise** als Plattform aus.

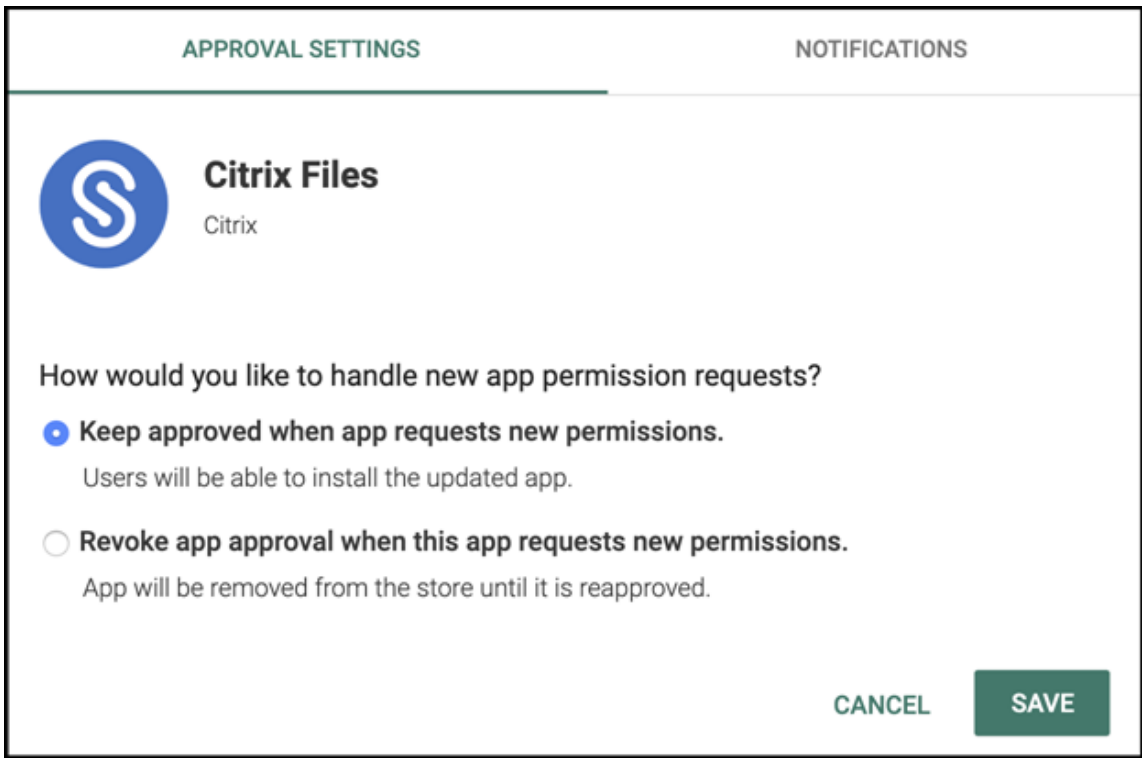
5. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** angezeigt.
   - **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.
   - **App-Kategorie:** Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen möchten. Weitere Informationen zu App-Kategorien finden Sie unter App-Kategorien.
6. Klicken Sie auf **Weiter**. Die Seite **Android Enterprise MDX-App** wird angezeigt.
7. Klicken Sie auf **Hochladen** und navigieren Sie zum Speicherort der MDX-Dateien für die App. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**.
8. Es wird eine Meldung angezeigt, wenn die angehängte Anwendung eine Genehmigung des verwalteten Google Play-Stores erfordert. Klicken Sie auf **Ja**, um die Anwendung zu genehmigen, ohne die XenMobile-Konsole zu verlassen.



9. Wenn die Seite des verwalteten Google Play-Stores geöffnet wird, klicken Sie auf **Approve**.

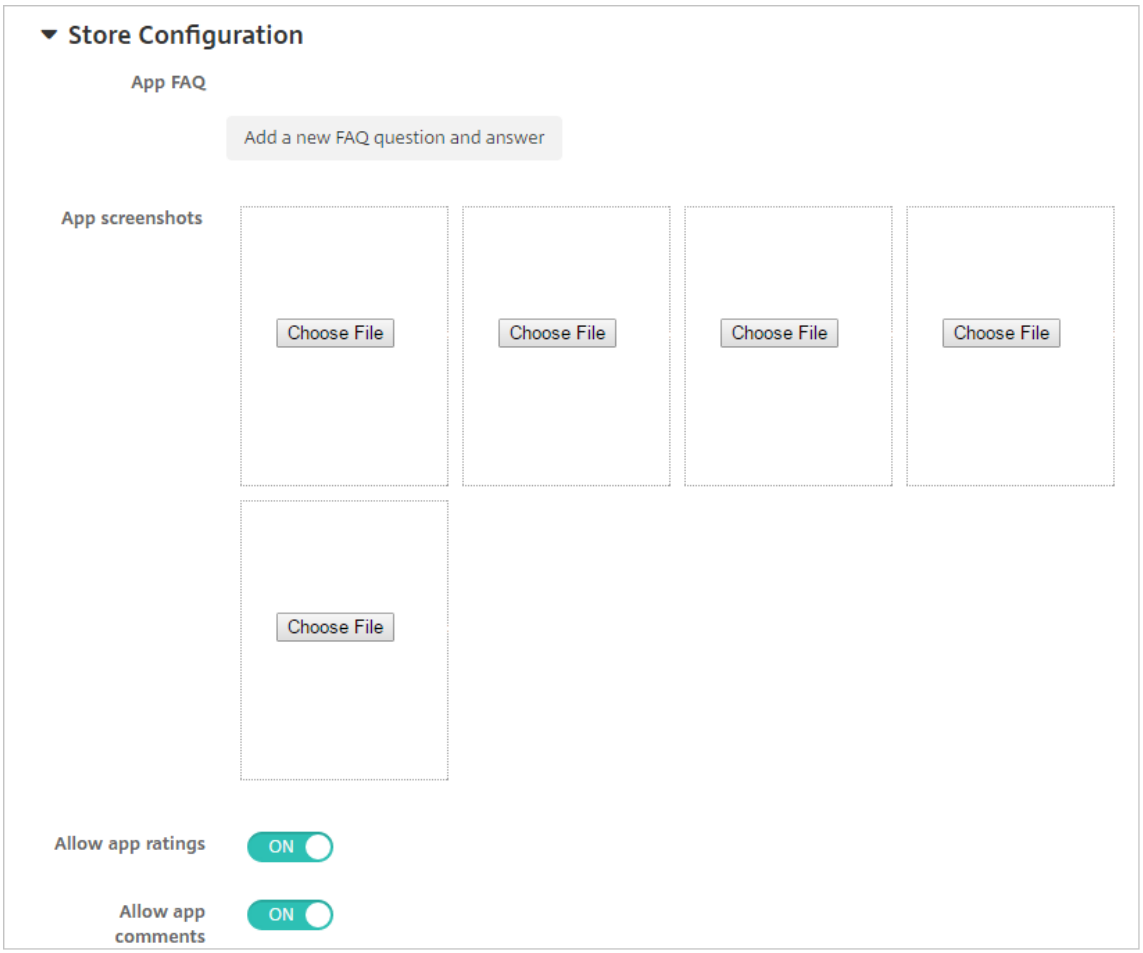


10. Klicken Sie erneut auf **Approve**.
11. Wählen Sie **Keep approved when app requests new permissions** aus. Klicken Sie auf **Speichern**.



12. Wenn die App genehmigt und gespeichert wurde, werden weitere Einstellungen auf der Seite angezeigt. Konfigurieren Sie folgende Einstellungen:
    - **Dateiname:** Geben Sie den Dateinamen der App ein.
    - **App-Beschreibung:** Geben Sie eine Beschreibung für die App ein.
    - **Produktschiene:** Geben Sie an, welche Produktversion Sie auf Benutzergeräte übertragen möchten. Wenn Sie ein spezielles Testprodukt haben, können Sie dies auswählen und Ihren Benutzern zuweisen. Die Standardeinstellung ist Produktion.
    - **App-Version:** Geben Sie optional die Nummer der App-Version ein.
    - **Paket-ID:** URL der App im Google Play-Store.
    - **OS-Version (Minimum):** Geben Sie optional die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
    - **OS-Version (Maximum):** Geben Sie optional 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.
13. Konfigurieren Sie die **MDX-Richtlinien**. Weitere Informationen zu App-Richtlinien für MDX-Apps finden Sie unter MDX-Richtlinien und Überblick über das MAM-SDK.
14. Konfigurieren Sie die Bereitstellungsregeln. Informationen finden Sie unter Bereitstellen von Ressourcen.
15. Erweitern Sie **Storekonfiguration**. Diese Einstellung gilt nicht für Android Enterprise-Apps, die

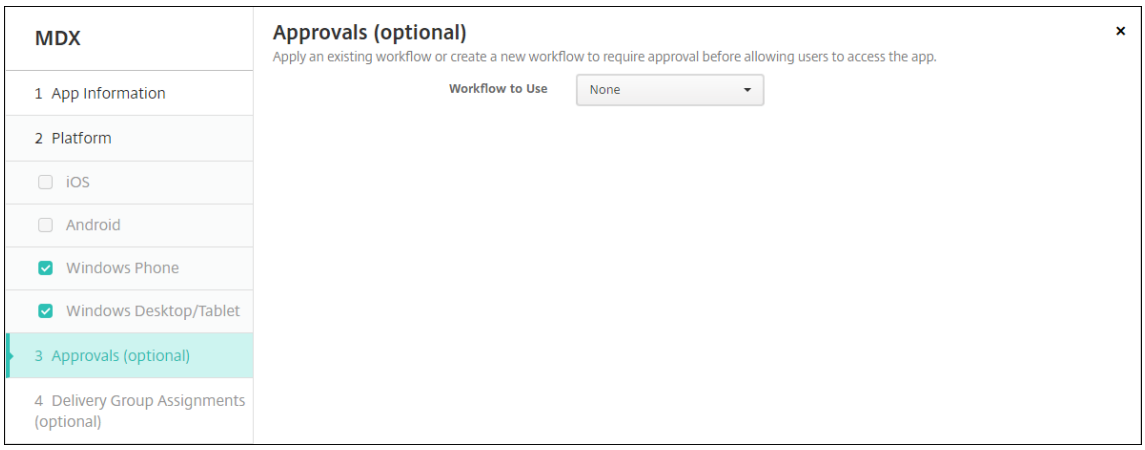
nur im verwalteten Google Play angezeigt werden.



Sie können optional FAQ oder Screenshots für die App zur Anzeige im App-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 App-Store hinzu. Die hochgeladene Grafikdatei muss das Format PNG haben. Sie können keine GIF- oder JPEG-Bilder hochladen.
  - **App-Bewertungen zulassen:** Wählen Sie aus, ob eine Bewertung der App durch die Benutzer zugelassen werden soll. Die Standardeinstellung ist **EIN**.
    App-Kommentare zulassen: Wählen Sie aus, ob eine Kommentierung der App durch die Benutzer zugelassen werden soll. Die Standardeinstellung ist **Ein**.

16. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.



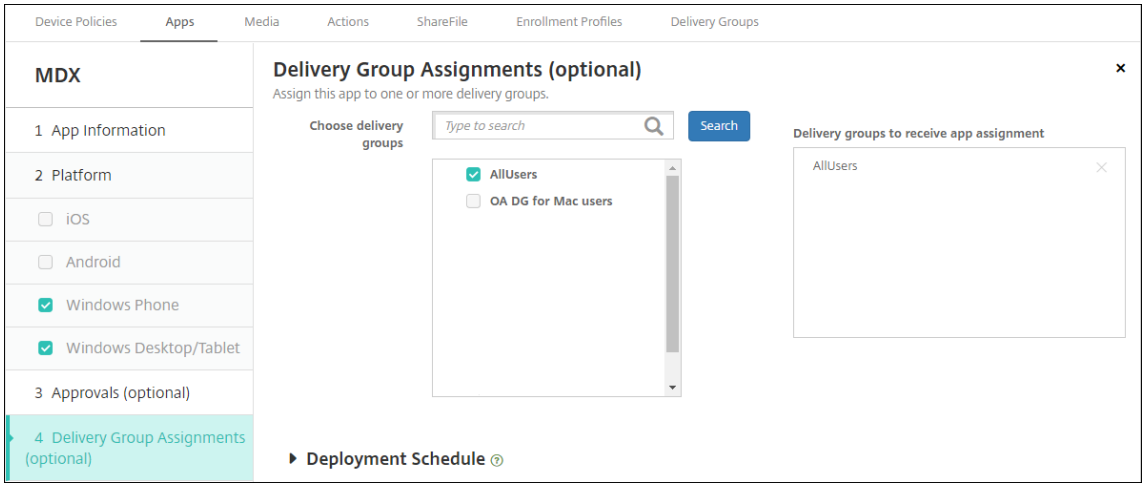
Wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist, verwenden Sie Workflows. Wenn Sie keine Genehmigungsworkflows einrichten möchten, fahren Sie mit Schritt 15 fort.

Konfigurieren Sie folgende Einstellungen zum Erstellen oder Zuweisen eines Workflows:

- **Verwendete Workflows:** Klicken Sie in der Liste auf einen Workflow oder klicken Sie auf **Neuen Workflow erstellen**. Die Standardeinstellung ist **Ohne**.
- Wenn Sie **Neuen Workflow erstellen** ausgewählt haben, konfigurieren Sie die folgenden Einstellungen: Weitere Informationen finden Sie unter Anwenden von Workflows.
- **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 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 **Search**, um das Suchergebnis einzuschränken.
  * Die Namen der Personen in der Liste **Selected additional required approvers** sind im Suchergebnis mit einem Häkchen gekennzeichnet. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Personen, die Sie entfernen möchten.

17. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.



18. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, um nach einer Bereitstellungsgruppe zu suchen, oder wählen Sie eine oder mehrere Gruppen in der Liste aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

19. 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**.
    - 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**.

- Stellen Sie sicher, dass neben **Bereitstellen für immer aktive Verbindungen** die Option **AUS** ausgewählt ist. Die Standardeinstellung ist **AUS**. Die immer aktiven Verbindungen sind für Android Enterprise nicht verfügbar wenn Sie XenMobile erstmals in einer Version ab 10.18.19 verwendet haben. Wir empfehlen diese Verbindungen nicht für Kunden, die XenMobile erstmals in einer Version vor 10.18.19 verwendet haben.

  Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.

  Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

20. Klicken Sie auf **Speichern**.

Wiederholen Sie die Schritte, um eine MDX-App für jede mobile Produktivitätsapp zu konfigurieren.

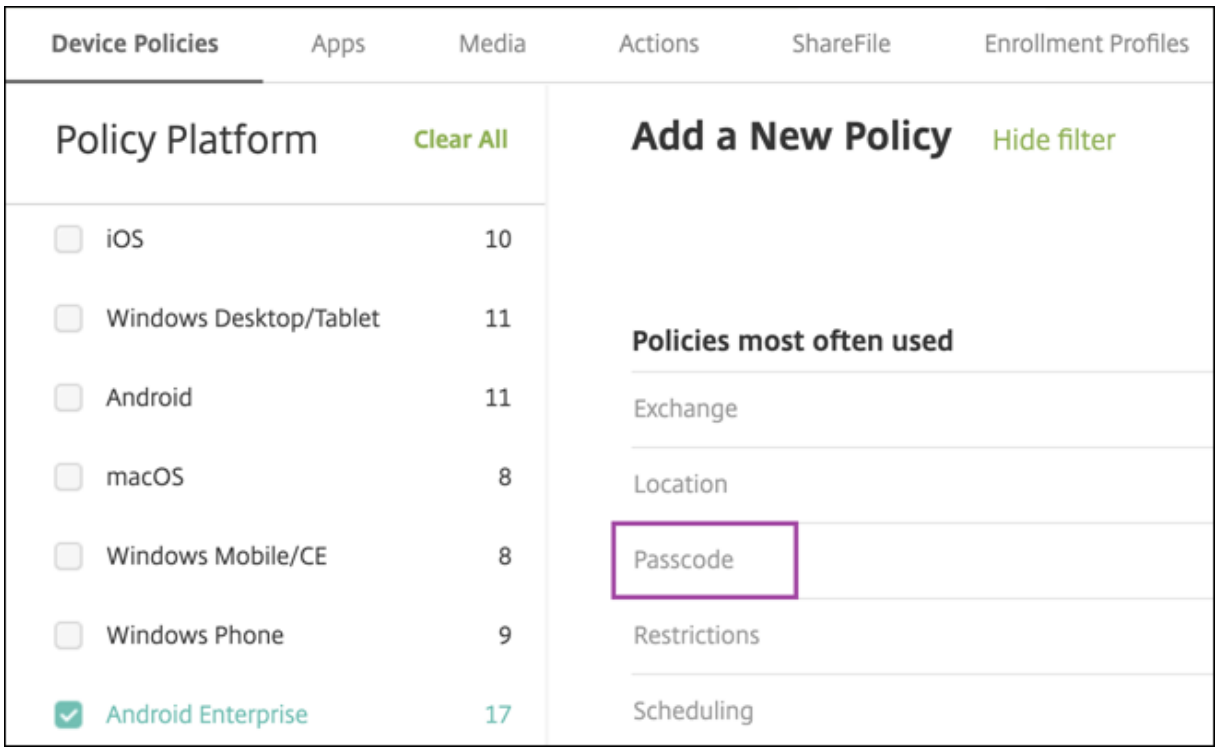
Konfigurieren der Richtlinie für die Sicherheitsabfrage

Die Passcode-Geräterichtlinie in XenMobile konfiguriert die Regeln für die Sicherheitsabfrage, mit der Benutzer auf ihre Geräte bzw. die Android Enterprise-Arbeitsprofile auf ihren Geräten zugreifen. Eine Sicherheitsabfrage kann ein Passcode oder eine biometrische Erkennung sein. Weitere Informationen zur Passcoderichtlinie finden Sie unter Passcoderichtlinien für Geräte.

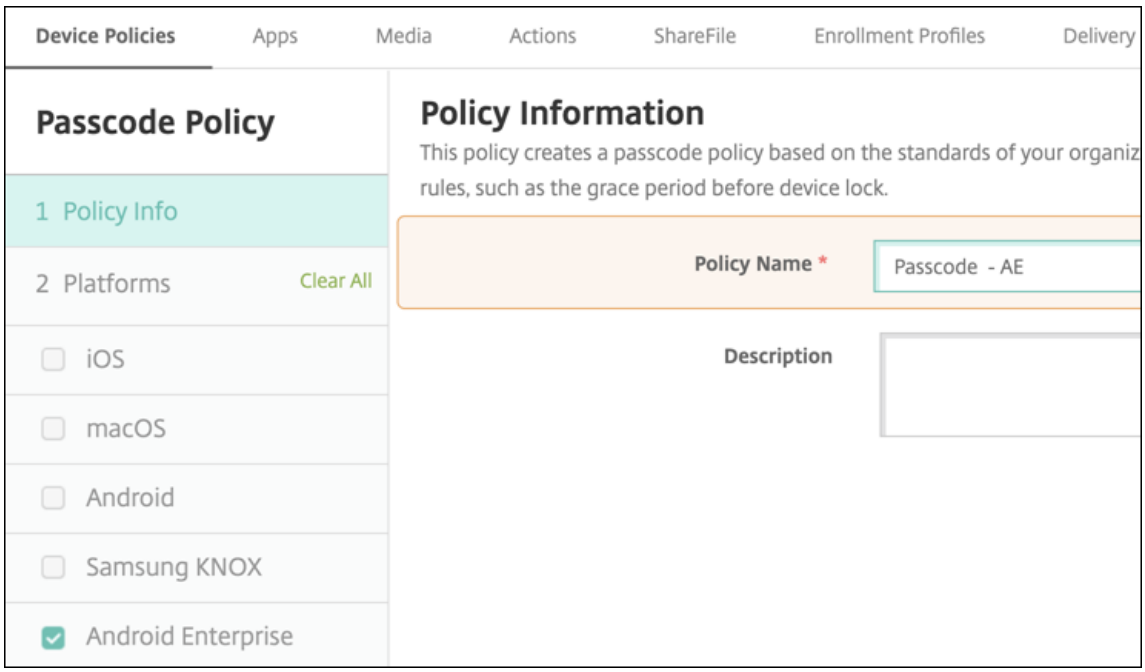
- Wenn in Ihrer Android Enterprise-Bereitstellung auch BYOD-Geräte enthalten sind, konfigurieren Sie die Passcoderichtlinie für das Arbeitsprofil.
- Wenn Ihre Bereitstellung vollständig verwaltete, firmeneigene Geräte umfasst, konfigurieren Sie die Passcoderichtlinie für das Gerät selbst.
- Wenn Ihre Bereitstellung beide Gerätetypen umfasst, konfigurieren Sie beide Arten von Passcoderichtlinien.

Konfigurieren der Passcoderichtlinie:

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Filter einblenden**, um den Bereich **Richtlinienplattform** anzuzeigen. Wählen Sie im Bereich **Richtlinienplattform** die Option **Android Enterprise** aus.
4. Klicken Sie im rechten Fensterbereich auf **Passcode**.



1. Geben Sie einen **Richtliniennamen** ein. Klicken Sie auf **Weiter**.



2. Konfigurieren Sie die Einstellungen für die Passcoderichtlinie.
   - Setzen Sie **Gerätepasscode erforderlich** auf **Ein**, um die verfügbaren Einstellungen für Sicherheitsabfragen für das Gerät anzuzeigen.
   - Setzen Sie **Sicherheitsabfrage für das Arbeitsprofil erforderlich** auf **Ein**, um die verfügbaren Einstellungen für Sicherheitsabfragen für das Arbeitsprofil anzuzeigen.

3. Klicken Sie auf **Weiter**.
4. Weisen Sie die Richtlinie mindestens einer Bereitstellungsgruppe zu.
5. Klicken Sie auf **Speichern**.

Registrierungsprofile erstellen

Registrierungsprofile steuern, wie Android-Geräte registriert werden, wenn Android Enterprise für Ihre XenMobile-Bereitstellung aktiviert ist. Wenn Sie ein Registrierungsprofil für Android Enterprise-Geräte erstellen, können Sie es so konfigurieren, dass neue und auf Werkseinstellungen zurückgesetzte Geräte wie folgt registriert werden:

- Als vollständig verwaltete Geräte
- Als unternehmenseigene Einzweckgeräte (COSU-Geräte)
- Als vollständig verwaltete Geräte mit Arbeitsprofil (COPE-Geräte)

Sie können jedes dieser Android Enterprise-Registrierungsprofile auch so konfigurieren, dass BYOD-Android-Geräte als Arbeitsprofilgeräte registriert werden.

Wenn Android Enterprise für Ihre XenMobile-Bereitstellung aktiviert ist, werden alle neu oder erneut registrierten Android-Geräte als Android Enterprise-Geräte registriert. Standardmäßig registriert das globale Registrierungsprofil neue und werkseitig zurückgesetzte Android-Geräte als vollständig verwaltete Geräte und BYOD Android-Geräte als Arbeitsprofilgeräte.

Wenn Sie Registrierungsprofile erstellen, weisen Sie ihnen Bereitstellungsgruppen zu. Wenn ein Benutzer zu mehreren Bereitstellungsgruppen mit unterschiedlichen Registrierungsprofilen gehört, bestimmt der Name der Bereitstellungsgruppe das verwendete Registrierungsprofil. XenMobile wählt die letzte Bereitstellungsgruppe in der alphabetisch geordneten Bereitstellungsgruppenliste aus. Weitere Informationen finden Sie unter Registrierungsprofile.

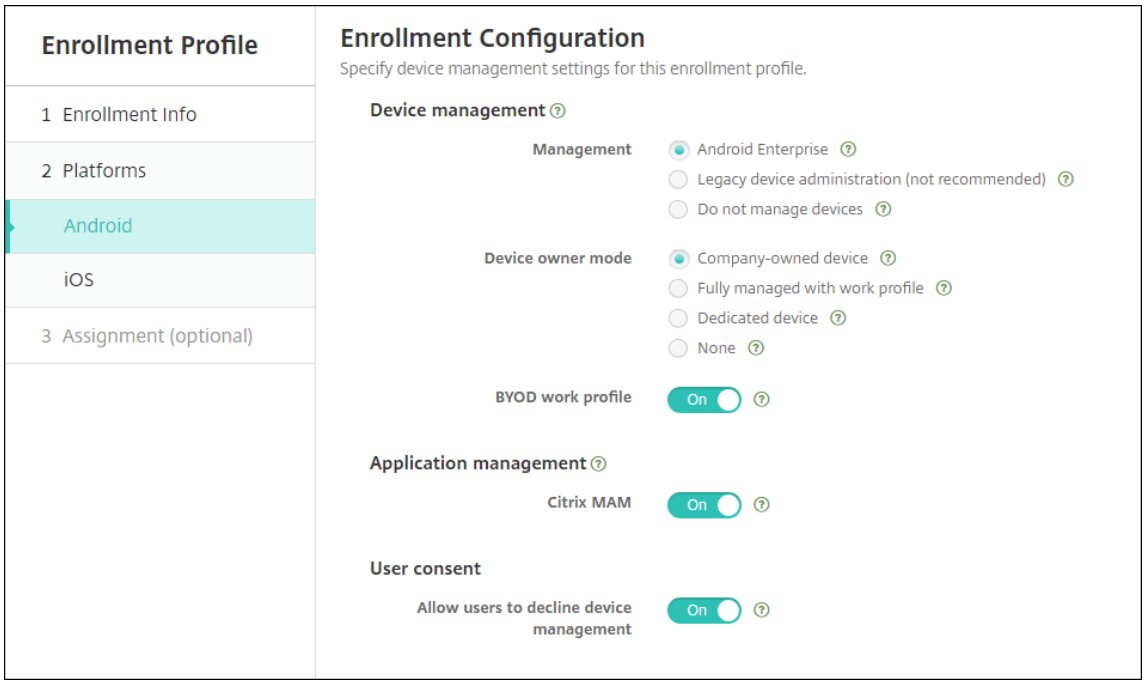
Sie können Registrierungsprofile verwenden, um mehrere Anwendungsfälle wie nur MDM, MDM+MAM und nur MAM zu kombinieren. Der in der Servereigenschaft `xms.server.mode` angegebene XenMobile Server-Lizenztyp bestimmt die Einstellungen, die unter **Konfigurieren > Registrierungsprofile** verfügbar sind.

Hinzufügen eines Registrierungsprofils für vollständig verwaltete Geräte

Das globale Registrierungsprofil registriert Geräte standardmäßig als vollständig verwaltet, Sie können jedoch weitere Registrierungsprofile erstellen, um vollständig verwaltete Geräte zu registrieren.

1. Gehen Sie in der XenMobile-Konsole zu **Konfigurieren > Registrierungsprofile**.
2. Wenn Sie ein Registrierungsprofil hinzufügen möchten, klicken Sie auf **Hinzufügen**. Geben Sie auf der Seite “Registrierungsinfo” einen Namen für das Registrierungsprofil ein.

3. Legen Sie die Anzahl der Geräte fest, die Mitglieder mit diesem Profil registrieren können.
4. Wählen Sie für **Plattformen** die Option **Android** oder klicken Sie auf **Weiter**. Die Seite "Registrierungskonfiguration" wird angezeigt.
5. Legen Sie **Verwaltung** auf **Android Enterprise** fest.
6. Legen Sie den **Gerätebesitzermodus** auf **Unternehmenseigenes Gerät** fest.

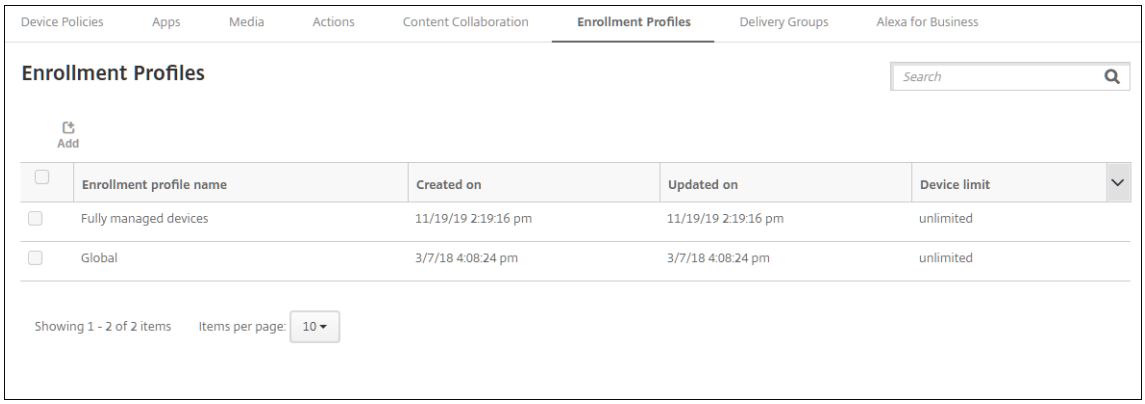


7. Mit **BYOD-Arbeitsprofil** können Sie das Registrierungsprofil so konfigurieren, dass BYOD-Geräte als Arbeitsprofilgeräte registriert werden. Neue Geräte und Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, werden als vollständig verwaltete Geräte registriert.
   - Legen Sie **BYOD-Arbeitsprofil** auf **Ein** fest, um die Registrierung von BYOD-Geräten als Arbeitsprofilgeräte zu ermöglichen. Die Standardeinstellung ist **Ein**.
   - Legen Sie **BYOD-Arbeitsprofil** auf **Aus** fest, um die Registrierung auf vollständig verwaltete Geräte zu beschränken.
8. Wählen Sie aus, ob Geräte bei Citrix MAM registriert werden sollen.
9. Wenn Sie **BYOD-Arbeitsprofil** auf **Ein** festlegen, konfigurieren Sie die Einstellung "Zustimmung des Benutzers". Sollen die Benutzer von BYOD-Arbeitsprofilgeräten die Geräteverwaltung bei der Registrierung ihrer Geräte ablehnen können, legen Sie **Benutzer dürfen Geräteverwaltung ablehnen** auf **Ein** fest.

   Wenn **BYOD-Arbeitsprofil** auf **Ein** festgelegt wurde, ist die Option **Benutzer dürfen Geräteverwaltung ablehnen** standardmäßig auf **Ein** festgelegt. Wenn **BYOD-Arbeitsprofil** auf **Aus** festgelegt wurde, ist die Option **Benutzer dürfen Geräteverwaltung ablehnen** deaktiviert.

10. Wählen Sie **Zuweisung (Optionen)**. Der Bildschirm für die Bereitstellungsgruppenzuweisung wird angezeigt.
11. Wählen Sie die Bereitstellungsgruppe(n) mit den Administratoren, die voll verwaltete Geräte registrieren sollen. Klicken Sie auf **Speichern**.

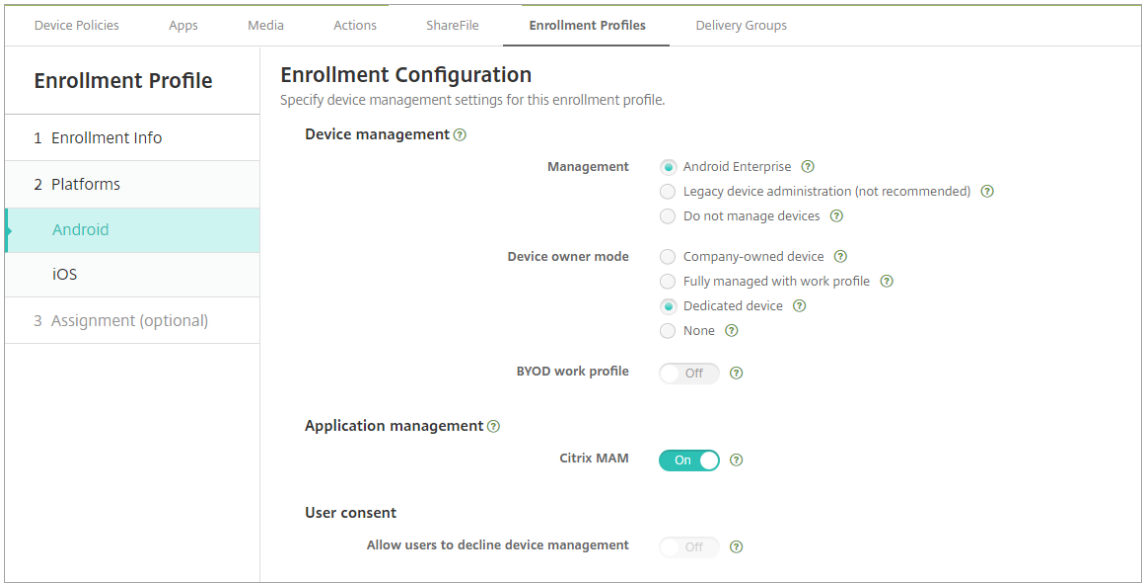
    Die Seite “Registrierungsprofil” wird mit dem von Ihnen hinzugefügten Profil angezeigt.



Hinzufügen eines Registrierungsprofil für dedizierte Geräte

Wenn Ihre XenMobile-Bereitstellung dedizierte Geräte enthält, registriert ein einzelner XenMobile-Administrator oder eine kleine Gruppe von Administratoren viele dedizierte Geräte. Damit diese Administratoren alle erforderlichen Geräte registrieren können, erstellen Sie für sie ein Registrierungsprofil unter Zulassung einer unbegrenzten Anzahl an Geräten pro Benutzer.

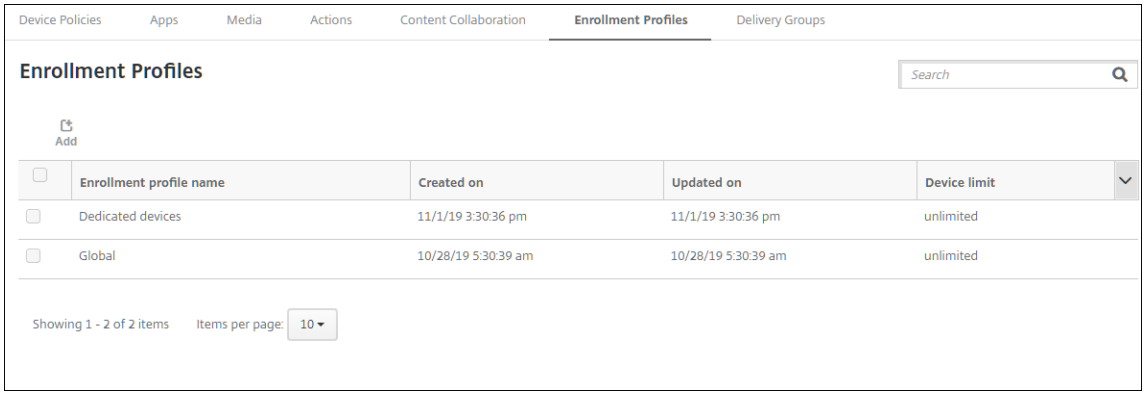
1. Gehen Sie in der XenMobile-Konsole zu **Konfigurieren > Registrierungsprofile**.
2. Wenn Sie ein Registrierungsprofil hinzufügen möchten, klicken Sie auf **Hinzufügen**. Geben Sie auf der Seite “Registrierungsinfo” einen Namen für das Registrierungsprofil ein. Legen Sie für die Anzahl der Geräte, die Mitglieder mit diesem Profil registrieren können, “Unbegrenzt” fest.
3. Wählen Sie für **Plattformen** die Option **Android** oder klicken Sie auf **Weiter**. Die Seite “Registrierungskonfiguration” wird angezeigt.
4. Legen Sie **Verwaltung** auf **Android Enterprise** fest.
5. Legen Sie den **Gerätebesitzermodus** auf **Dediziertes Gerät** fest.



6. Mit **BYOD-Arbeitsprofil** können Sie das Registrierungsprofil so konfigurieren, dass BYOD-Geräte als Arbeitsprofilgeräte registriert werden. Neue Geräte und Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, werden als dedizierte Geräte registriert. Legen Sie **BYOD-Arbeitsprofil** auf **Ein** fest, um die Registrierung von BYOD-Geräten als Arbeitsprofilgeräte zu ermöglichen. Legen Sie **BYOD-Arbeitsprofil** auf **Aus** fest, um die Registrierung auf unternehmenseigene Geräte zu beschränken. Die Standardeinstellung ist **Ein**.
7. Wählen Sie aus, ob Geräte bei Citrix MAM registriert werden sollen.
8. Wenn Sie **BYOD-Arbeitsprofil** auf **Ein** festlegen, konfigurieren Sie die Einstellung “Zustimmung des Benutzers”. Sollen die Benutzer von BYOD-Arbeitsprofilgeräten die Geräteverwaltung bei der Registrierung ihrer Geräte ablehnen können, legen Sie **Benutzer dürfen Geräteverwaltung ablehnen** auf **Ein** fest.

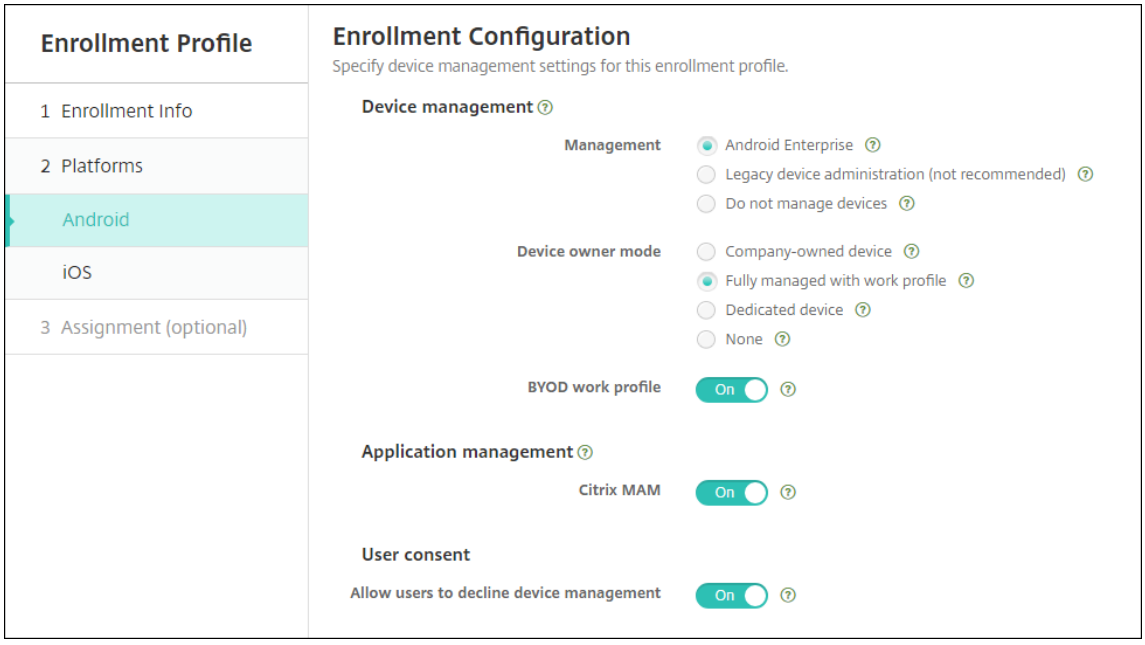
   Wenn **BYOD-Arbeitsprofil** auf **Ein** festgelegt wurde, ist die Option **Benutzer dürfen Geräteverwaltung ablehnen** standardmäßig auf **Ein** festgelegt. Wenn **BYOD-Arbeitsprofil** auf **Aus** festgelegt wurde, ist die Option **Benutzer dürfen Geräteverwaltung ablehnen** deaktiviert.
9. Wählen Sie **Zuweisung (Optionen)**. Der Bildschirm für die Bereitstellungsgruppenzuweisung wird angezeigt.
10. Wählen Sie die Bereitstellungsgruppe(n) mit den Administratoren, die dedizierte Geräte registrieren sollen. Klicken Sie auf **Speichern**.

    Die Seite “Registrierungsprofil” wird mit dem von Ihnen hinzugefügten Profil angezeigt.



Hinzufügen eines Registrierungsprofils für vollständig verwaltete Geräte mit Arbeitsprofil

1. Gehen Sie in der XenMobile-Konsole zu **Konfigurieren > Registrierungsprofile**.
2. Wenn Sie ein Registrierungsprofil hinzufügen möchten, klicken Sie auf **Hinzufügen**. Geben Sie auf der Seite “Registrierungsinfo” einen Namen für das Registrierungsprofil ein.
3. Legen Sie die Anzahl der Geräte fest, die Mitglieder mit diesem Profil registrieren können.
4. Wählen Sie für **Plattformen** die Option **Android** oder klicken Sie auf **Weiter**. Die Seite “Registrierungskonfiguration” wird angezeigt.
5. Legen Sie **Verwaltung** auf **Android Enterprise** fest. Legen Sie den **Gerätebesitzermodus** auf **Vollständig verwaltet mit Arbeitsprofil** fest.



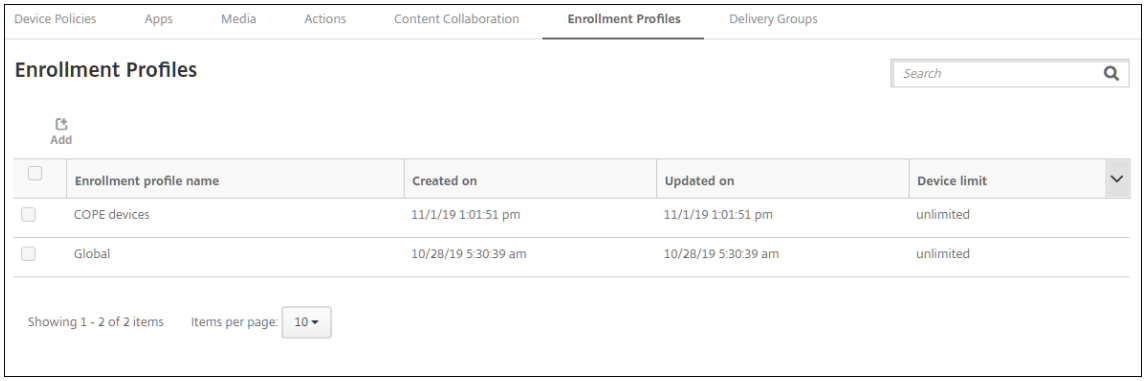
6. Mit **BYOD-Arbeitsprofil** können Sie das Registrierungsprofil so konfigurieren, dass BYOD-Geräte als Arbeitsprofilgeräte registriert werden. Neue Geräte und Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, werden als vollständig verwaltete Geräte mit

Arbeitsprofil registriert. Legen Sie **BYOD-Arbeitsprofil** auf **Ein** fest, um die Registrierung von BYOD-Geräten als Arbeitsprofilgeräte zu ermöglichen. Legen Sie **BYOD-Arbeitsprofil** auf **Aus** fest, um die Registrierung auf dedizierte Geräte zu beschränken. Die Standardeinstellung ist **Aus**.

7. Wählen Sie aus, ob Geräte bei Citrix MAM registriert werden sollen.
8. Wenn Sie **BYOD-Arbeitsprofil** auf **Ein** festlegen, konfigurieren Sie die Einstellung "Zustimmung des Benutzers". Sollen die Benutzer von BYOD-Arbeitsprofilgeräten die Geräteverwaltung bei der Registrierung ihrer Geräte ablehnen können, legen Sie **Benutzer dürfen Geräteverwaltung ablehnen** auf **Ein** fest.

   Wenn **BYOD-Arbeitsprofil** auf **Ein** festgelegt wurde, ist die Option **Benutzer dürfen Geräteverwaltung ablehnen** standardmäßig auf **Ein** festgelegt. Wenn **BYOD-Arbeitsprofil** auf **Aus** festgelegt wurde, ist die Option **Benutzer dürfen Geräteverwaltung ablehnen** deaktiviert.
9. Wählen Sie **Zuweisung (Optionen)**. Der Bildschirm für die Bereitstellungsgruppenzuweisung wird angezeigt.
10. Wählen Sie die Bereitstellungsgruppe(n) mit den Administratoren, die voll verwaltete Geräte mit Arbeitsprofil registrieren sollen. Klicken Sie auf **Speichern**.

    Die Seite "Registrierungsprofil" wird mit dem von Ihnen hinzugefügten Profil angezeigt.



Hinzufügen eines Registrierungsprofils für Legacygeräte

Google stellt den Geräteadministratormodus für die Geräteverwaltung ein. Google empfiehlt Kunden, alle Android-Geräte im Gerätebesitzermodus oder im Profilbesitzermodus zu verwalten. (Weitere Informationen finden Sie in den Entwicklerhandbüchern zu Google Android Enterprise unter Device admin deprecation.)

Unterstützen dieser Änderung:

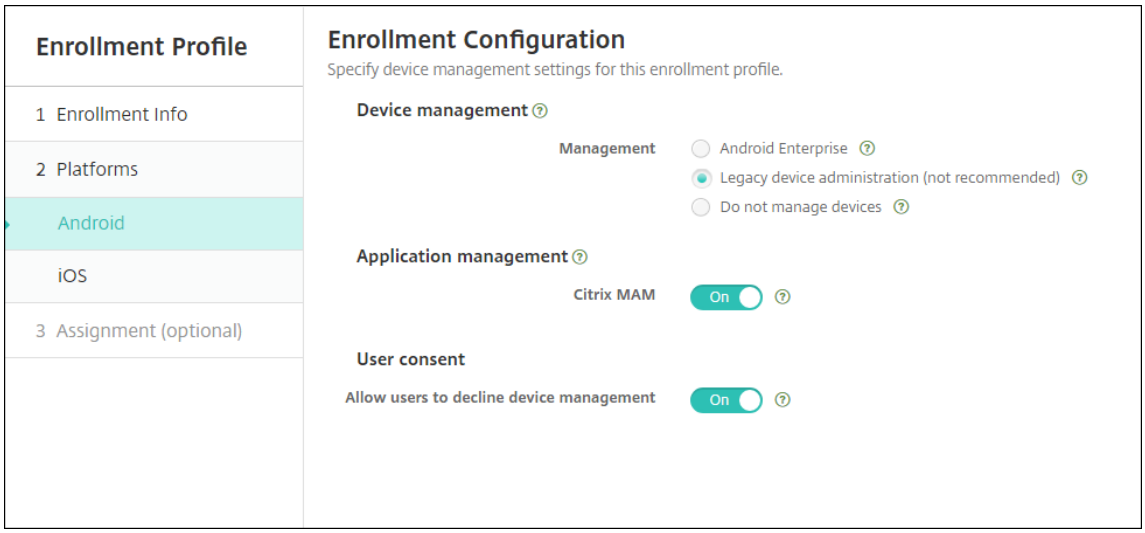
- Für Citrix ist Android Enterprise die Standardoption bei der Registrierung von Android-Geräten.
- Wenn Android Enterprise für Ihre XenMobile-Bereitstellung aktiviert ist, werden alle neu oder erneut registrierten Android-Geräte als Android Enterprise-Geräte registriert.

Ihre Organisation ist unter Umständen noch nicht in der Lage, Android-Legacygeräte mit Android Enterprise zu verwalten. In diesem Fall können Sie sie weiterhin im Geräteadministratormodus verwalten. Alle bereits im Geräteadministratormodus registrierten Geräte werden von XenMobile weiterhin in diesem Modus verwaltet.

Erstellen Sie ein Registrierungsprofil für Legacygeräte, um bei der Neuregistrierung dieser Android-Geräte den Geräteadministratormodus zu verwenden.

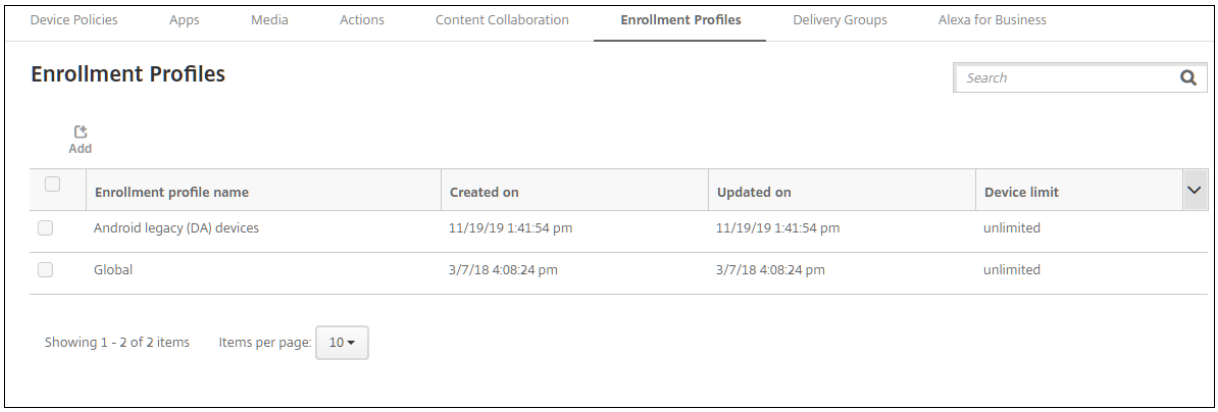
Erstellen eines Registrierungsprofils für Legacygeräte:

1. Gehen Sie in der XenMobile-Konsole zu **Konfigurieren > Registrierungsprofile**.
2. Wenn Sie ein Registrierungsprofil hinzufügen möchten, klicken Sie auf **Hinzufügen**. Geben Sie auf der Seite "Registrierungsinfo" einen Namen für das Registrierungsprofil ein.
3. Legen Sie die Anzahl der Geräte fest, die Mitglieder mit diesem Profil registrieren können.
4. Wählen Sie für **Plattformen** die Option **Android** oder klicken Sie auf **Weiter**. Die Seite "Registrierungskonfiguration" wird angezeigt.
5. Legen Sie **Verwaltung** auf **Legacygeräteverwaltung fest (nicht empfohlen)** . Klicken Sie auf **Weiter**.



6. Wählen Sie aus, ob Geräte bei Citrix MAM registriert werden sollen.
7. Sollen die Benutzer die Geräteverwaltung bei der Registrierung ihrer Geräte ablehnen können, legen Sie **Benutzer dürfen Geräteverwaltung ablehnen** auf **Ein** fest. Die Standardeinstellung ist **Ein**.
8. Wählen Sie **Zuweisung (Optionen)**. Der Bildschirm für die Bereitstellungsgruppenzuweisung wird angezeigt.
9. Wählen Sie die Bereitstellungsgruppe(n) mit den Administratoren, die dedizierte Geräte registrieren sollen. Klicken Sie auf **Speichern**.

Die Seite “Registrierungsprofil” wird mit dem von Ihnen hinzugefügten Profil angezeigt.



Um ein Legacygerät weiterhin im Geräteadministratormodus zu verwalten, registrieren Sie es mit diesem Profil oder registrieren Sie es neu. Sie registrieren Geräteadministratorgeräte ähnlich wie Arbeitsprofilgeräte, indem Benutzer Secure Hub herunterladen und eine Registrierungsserver-URL angeben.

Provisioning von Arbeitsprofilgeräten mit Android Enterprise

Android Enterprise-Arbeitsprofilgeräte sind im Profilbesitzermodus registriert. Diese Geräte müssen nicht neu oder auf die Werkseinstellungen zurückgesetzt sein. BYOD-Geräte werden als Arbeitsprofilgeräte registriert. Die Registrierung ähnelt der Android-Registrierung in XenMobile. Die Benutzer laden Secure Hub aus Google Play herunter und registrieren ihre Geräte.

Standardmäßig sind die Einstellungen **USB-Debugging** und “Unbekannte Quellen” auf einem Gerät deaktiviert, wenn Sie es bei Android Enterprise als Arbeitsprofilgerät registrieren.

Beim Registrieren von Geräten als Arbeitsprofilgerät in Android Enterprise wechseln Sie stets zu Google Play. Aktivieren Sie dort Secure Hub, das dann im persönlichen Profil des Benutzers angezeigt wird.

Provisioning vollständig verwalteter Geräte mit Android Enterprise

Sie können vollständig verwaltete Geräte in der Bereitstellung registrieren, die Sie in den vorherigen Abschnitten eingerichtet haben. Vollständig verwaltete Geräte sind firmeneigene Geräte und werden im Gerätebesitzermodus registriert. Nur neue Geräte oder auf die Werkseinstellungen zurückgesetzte Geräte können im Gerätebesitzermodus registriert werden.

Sie können Geräte mit einer der folgenden Registrierungsmethoden im Gerätebesitzermodus registrieren:

- **DPC-ID-Token:** Bei dieser Registrierungsmethode geben Benutzer beim Einrichten des Geräts die Zeichenfolge `afw##xenmobile` ein. `afw##xenmobile` ist der DPC-ID-Token von Citrix. Der

Token identifiziert das Gerät als von XenMobile verwaltet und lädt Secure Hub vom Google Play Store herunter. Siehe Registrierung von Geräten mit dem Citrix DPC-ID-Token.

- **Datenübertragung per NFC (Near Field Communication):** Bei dieser kontaktlosen Registrierungsmethode erfolgt der Datenaustausch zwischen zwei Geräten über die Nahfeldkommunikation (NFC). Bluetooth, Wi-Fi und andere Kommunikationsmodi sind auf einem neuen Gerät oder einem Gerät mit Werkseinstellungen deaktiviert. NFC ist das einzige Kommunikationsprotokoll, das das Gerät in diesem Zustand verwenden kann. Siehe Registrieren von Geräten per NFC-Datenübertragung.
- **QR-Code:** Die Registrierung per QR-Code empfiehlt sich für verteilte Geräte im Bestand, die NFC nicht unterstützen (z. B. Tablets). Dabei wird der Geräteprofilmodus vom Setupassistenten durch Scannen eines QR-Codes eingerichtet und konfiguriert. Siehe Registrieren von Geräten per QR-Code.
- **Zero Touch:** Mit der Zero-Touch-Registrierung können Sie festlegen, dass Geräte beim ersten Einschalten automatisch registriert werden. Die Zero-Touch-Registrierung wird auf einigen Android-Geräten mit Android 8.0 oder höher unterstützt. Siehe Zero-Touch-Registrierung.
- **Google-Konten:** Benutzer geben die Anmeldeinformationen für ihr Google-Konto ein, um das Provisioning einzuleiten. Diese Option gilt für Unternehmen, die Google Workspace verwenden.

Registrierung von Geräten mit dem Citrix DPC-ID-Token

Benutzer geben `afw##xenmobile` ein, nachdem sie ein neues oder auf die Werkseinstellungen zurückgesetztes Gerät für die Ersteinrichtung eingeschaltet haben und aufgefordert wurden, ein Google-Konto einzugeben. Mit dieser Aktion wird Secure Hub heruntergeladen und installiert. Die Benutzer folgen anschließend den Anweisungen in Secure Hub zum Abschließen der Registrierung.

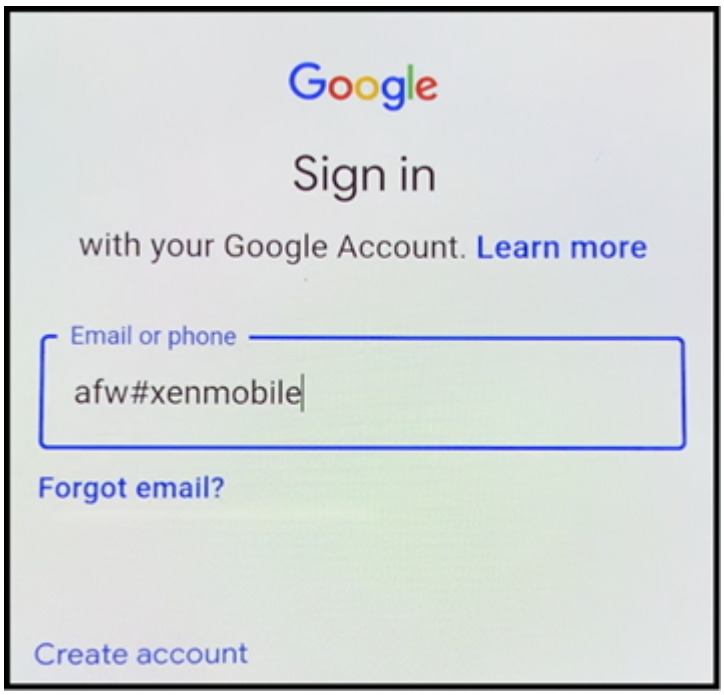
Diese Registrierungsmethode wird für die meisten Kunden empfohlen, da die aktuelle Secure Hub-Version aus Google Play heruntergeladen wird. Im Gegensatz zu anderen Registrierungsmethoden wird Secure Hub nicht zum Herunterladen vom XenMobile-Server bereitgestellt.

Systemanforderungen

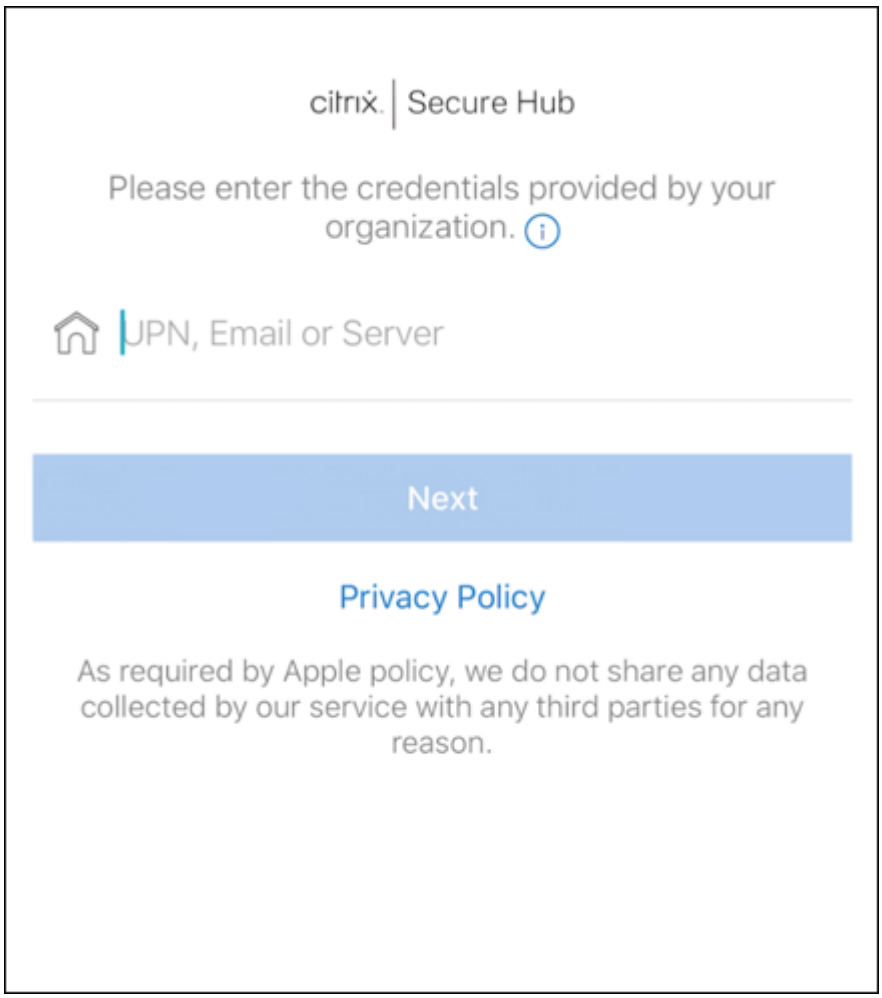
- Wird auf allen Android-Geräten mit Android-OS unterstützt.

Registrieren des Geräts

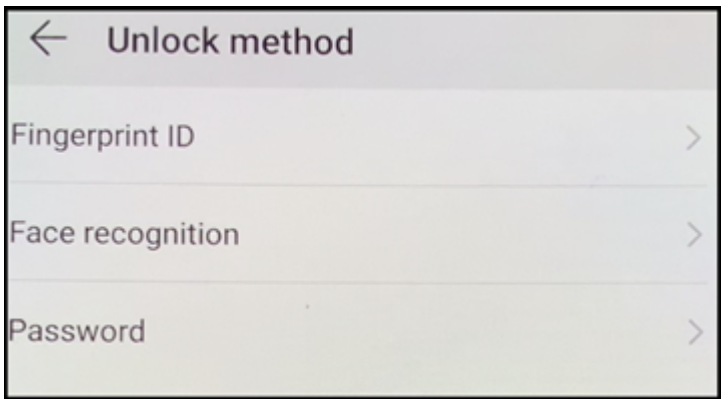
1. Schalten Sie ein neues oder auf die Werkseinstellungen zurückgesetztes Gerät ein.
2. Die Ersteinrichtung des Geräts wird geladen und der Benutzer wird aufgefordert, ein Google-Konto einzugeben. Falls das Gerät den Startbildschirm lädt, überprüfen Sie, ob in der Benachrichtigungsleiste die Benachrichtigung **Finish Setup** angezeigt wird.
3. Geben Sie `afw##xenmobile` im Feld **Email oder phone** ein.



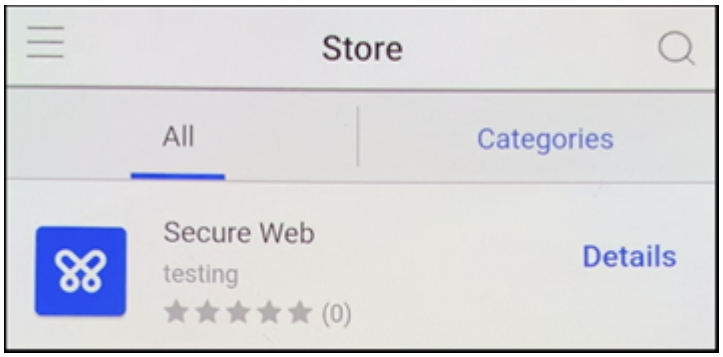
4. Tippen Sie im Android Enterprise-Bildschirm auf **Install**, um Secure Hub zu installieren.
5. Tippen Sie im Secure Hub-Installationsbildschirm auf **Install**.
6. Tippen Sie für alle App-Berechtigungsanforderungen auf **Allow**.
7. Tippen Sie auf **Accept & Continue**, um Secure Hub zu installieren und das Gerät damit zu verwalten.
8. Secure Hub ist installiert und der Standard-Registrierungsbildschirm wird angezeigt. In diesem Beispiel ist AutoDiscovery nicht eingerichtet. Bei aktivierter Funktion können Benutzer ihren Benutzernamen bzw. ihre E-Mail-Adresse eingeben und es wird ein Server für sie gefunden. Geben Sie stattdessen die Registrierungs-URL für die Umgebung ein und tippen Sie auf **Weiter**.



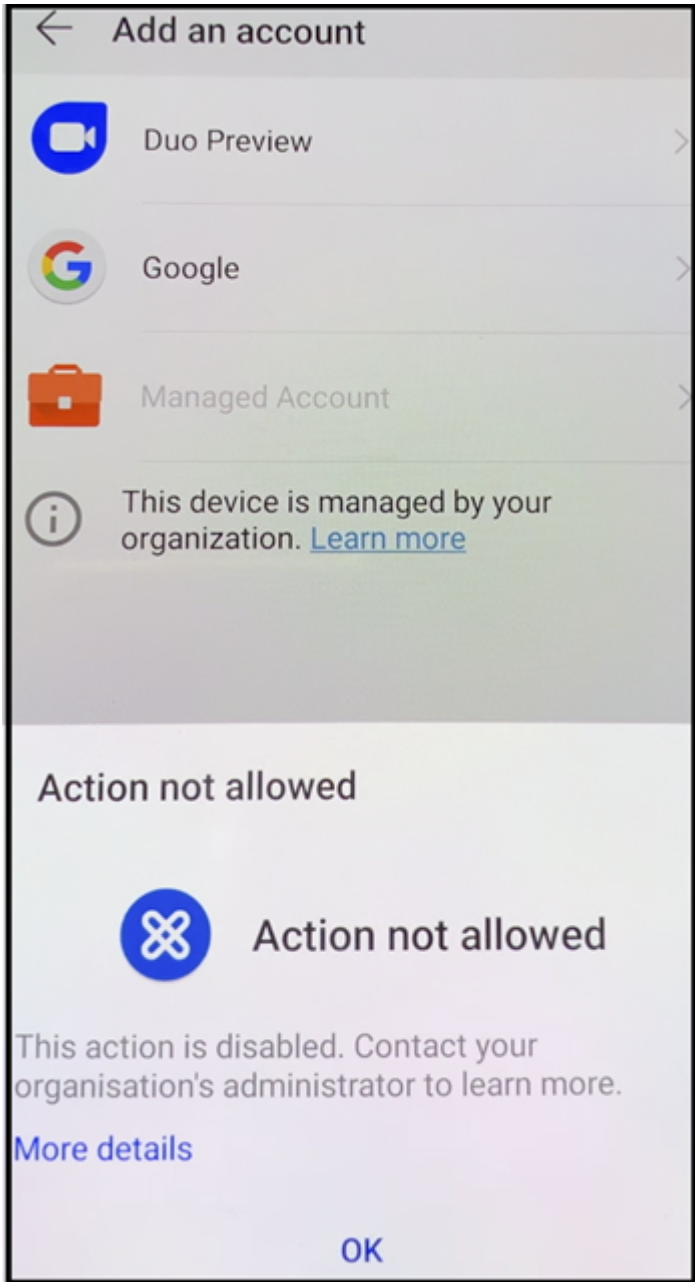
9. In der Standardkonfiguration für XenMobile können Benutzer auswählen, ob sie MAM oder MDM+MAM verwenden. Wenn die Aufforderung angezeigt wird, tippen Sie auf **Ja, Registrieren**, um MDM+MAM auszuwählen.
10. Geben Sie den Benutzernamen und das Kennwort ein und tippen Sie auf **Weiter**.
11. Der Benutzer wird aufgefordert, einen Gerätepasscode zu konfigurieren. Tippen Sie auf **Festlegen** und geben Sie einen Passcode ein.
12. Der Benutzer wird aufgefordert, eine Methode zum Entsperren des Arbeitsprofils zu konfigurieren. Tippen Sie in diesem Beispiel auf **Kennwort** und dann auf **PIN** und geben Sie eine PIN ein.



13. Das Gerät zeigt jetzt **Eigene Apps**, die Startseite von Secure Hub. Tippen Sie auf **Apps aus dem Store hinzufügen**.
14. Tippen Sie zum Hinzufügen von Secure Web auf **Secure Web**.



15. Tippen Sie auf **Hinzufügen**.
16. Secure Hub leitet den Benutzer zum Google Play Store, um Secure Web zu installieren. Tippen Sie auf **Installieren**.
17. Tippen Sie nach der Installation von Secure Web auf **Öffnen**. Geben Sie die URL einer internen Website in die Adressleiste ein, um zu prüfen, ob die Seite geladen wird.
18. Navigieren Sie zu **Einstellungen > Konten** auf dem Gerät. Beachten Sie, dass **Verwaltetes Konto** nicht geändert werden kann. Die Entwickleroptionen zur Bildschirmfreigabe oder für den Remotesupport sind ebenfalls blockiert.



Registrieren von Geräten per NFC-Datenübertragung

Um ein Gerät per NFC-Funktion als vollständig verwaltetes Gerät zu registrieren, sind zwei Geräte erforderlich: Ein Gerät, das auf die Werkseinstellungen zurückgesetzt wurde, und ein Gerät, auf dem das XenMobile Provisioning Tool ausgeführt wird.

Systemanforderungen und Voraussetzungen

- Unterstützte Android-Geräte.

- Ein neues oder auf die Werkseinstellungen zurückgesetztes Gerät, das für Android Enterprise als vollständig verwaltetes Gerät 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 und auf der Citrix Downloadseite verfügbar.

Auf jedem Gerät kann nur ein Android Enterprise-Profil mit verwaltetem Secure Hub installiert sein. Auf jedem Gerät ist nur ein Profil zulässig. Sobald Sie eine zweite DPC-App hinzufügen, wird der installierte Secure Hub entfernt.

Per NFC übertragene Daten

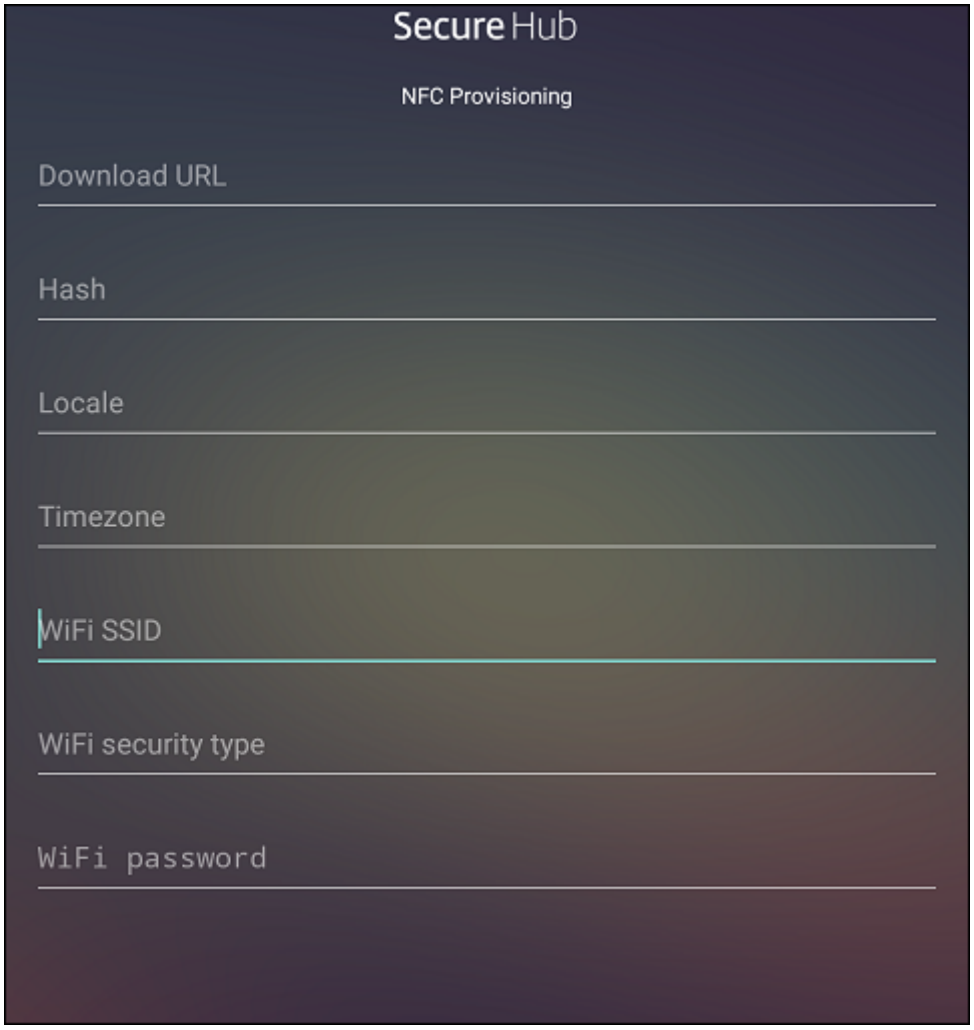
Für das Provisioning eines auf Werkseinstellungen zurückgesetzten Geräts müssen Sie die folgenden Daten per NFC senden, damit Android Enterprise initialisiert wird:

- Paketname der DPC-App, die als Gerätebesitzer fungiert (in diesem Fall Secure Hub).
- Intranet-/Internetspeicherort, von dem das Gerät die DPC-App herunterlädt.
- SHA1-Hash der DPC-App, um zu überprüfen, ob der Download erfolgreich ist.
- Wi-Fi-Verbindungsdetails, sodass ein auf Werkseinstellungen zurückgesetztes Gerät eine Verbindung herstellen und die DPC-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 unter Verwendung 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=<download_location>`

Dies ist der Intranet-/Internetspeicherort der EMM-Anbieter-App. Wenn das auf Werkseinstellungen zurückgesetzte Gerät nach der NFC-Übertragung eine Wi-Fi-Verbindung 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=<SHA1 hash>

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=<wifi ssid>

Dies ist die Wi-Fi-SSID des Geräts, auf dem das Provisioning Tool ausgeführt wird.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

Es werden WEP und WPA2 unterstützt. Wenn das WiFi nicht geschützt ist, muss dieses Feld leer sein.

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

Wenn das WiFi nicht geschützt ist, muss dieses Feld leer sein.

android.app.extra.PROVISIONING_LOCALE=<locale>

Geben Sie die Sprach- und Ländercodes ein. Sprachcodes sind nach ISO 639-1 definierte ISO-Sprachcodes, die aus zwei Kleinbuchstaben bestehen (z. B. en). Ländercodes sind nach ISO 3166-1 definierte ISO-Ländercodes, die aus zwei Großbuchstaben bestehen(z. B. US). 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=<timezone>

Die Zeitzone, in der das Gerät ausgeführt wird. Geben Sie einen Namen im Format Gebiet/Ort ein. Beispiel: America/Los_Angeles für Pacific Time. Wenn Sie keine Zeitzone eingeben, wird sie automatisch eingetragen.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**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 Wi-Fi könnte die Datei nfcprovisioning.txt wie folgt aussehen:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=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=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Abrufen der Citrix Secure Hub-Prüfsumme

Die Secure Hub-Prüfsumme ist ein konstanter Wert: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. Um eine APK-Datei für Secure Hub herunterzuladen, verwenden Sie den folgenden Google Play-Link: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

Abrufen einer App-Prüfsumme

Voraussetzungen:

- Das **apksigner**-Tool aus den Android SDK Build Tools
- OpenSSL-Befehlszeile

Gehen Sie folgendermaßen vor, um die Prüfsumme einer App abzurufen:

1. Laden Sie die APK-Datei der App aus Google Play herunter.
2. Navigieren Sie in der OpenSSL-Befehlszeile zum **apksigner**-Tool: `android-sdk/build-tools/<version>/apksigner` und geben Sie Folgendes ein:

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if
    m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

   Der Befehl gibt eine gültige Prüfsumme zurück.

3. Um den QR-Code zu generieren, geben Sie die Prüfsumme in das Feld `PROVISIONING_DEVICE_ADMIN_SIGN` ein. Beispiel:


```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
     zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"
     qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.
     PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
     play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }

<!--NeedCopy-->
```

Verwendete Bibliotheken

Das Provisioning Tool verwendet die folgenden Bibliotheken im Quellcode:

- v7 `appcompat` Library, Design Support Library und v7 Palette Library von Google unter Apache 2.0-Lizenz

  Weitere Informationen finden Sie im Handbuch zur Support Library Features Guide.

- Butter Knife von Jake Wharton unter Apache-Lizenz 2.0

Registrieren von Geräten per QR-Code

Sie registrieren ein vollständig verwaltetes Gerät per QR-Code, indem Sie zunächst ein JSON-Objekt erstellen und dieses in einen QR-Code umwandeln. Der QR-Code wird mit der Gerätekamera gescannt, um das Gerät zu registrieren.

Systemanforderungen

- Wird auf allen Android-Geräten ab Android 8.0 unterstützt.

Erstellen eines QR-Codes aus einer JSON-Datei

Erstellen Sie eine JSON-Datei mit den folgenden Feldern.

Diese Felder sind erforderlich:

Schlüssel: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Wert: com.zenprise/com.zenprise.configuration.AdminFunction

Schlüssel: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Wert: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Schlüssel: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Wert: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

Diese Felder sind optional:

- **android.app.extra.PROVISIONING_LOCALE:** Geben Sie den Sprach- und den Ländercode ein.

  Sprachcodes sind nach ISO 639-1 definierte ISO-Sprachcodes, die aus zwei Kleinbuchstaben bestehen (z. B. en). Ländercodes sind nach ISO 3166-1 definierte ISO-Ländercodes, die aus zwei Großbuchstaben bestehen(z. B. US). Geben Sie z. B. de_DE für Deutsch/Deutschland ein.

- **android.app.extra.PROVISIONING_TIME_ZONE:** die Zeitzone, in der das Gerät ausgeführt wird.

  Geben Sie einen Namen im Format Gebiet/Ort ein. Beispiel: America/Los_Angeles für Pacific Time. Wenn Sie keine Zeitzone eingeben, wird sie automatisch eingetragen.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Zeit in Millisekunden seit der Unix-Epoche.

  Die Unix-Zeit (auch POSIX-Zeit oder Unix-Zeitstempel) ist die Anzahl der Sekunden, die seit der Epoche, d. h. dem 1. Januar 1970 (Mitternacht UTC-GMT), verstrichen sind. Schaltsekunden werden nicht mitgezählt (in ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Wenn Sie dies auf **true** festlegen, wird die Verschlüsselung während der Profilerstellung übersprungen. Wählen Sie **False**, um die Verschlüsselung während der Profilerstellung zu erzwingen.

Eine JSON-Datei sieht in etwa wie folgt aus:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Überprüfen Sie die JSON-Datei mit einem JSON-Validierungstool (z. B. https://jsonlint.com). Konvertieren Sie die JSON-Zeichenfolge mit einem beliebigen QR-Code-Generator (z. B. https://www.qr-code-generator.com) in einen QR-Code.

Der QR-Code wird von einem auf Werkseinstellungen zurückgesetzten Gerät gescannt, um das Gerät als vollständig verwaltetes Gerät zu registrieren.

Registrieren des Geräts

Nach dem Einschalten eines neuen oder auf die Werkseinstellungen zurückgesetzten Geräts:

1. Tippen Sie sechsmal auf den Begrüßungsbildschirm, um die Registrierung per QR-Code zu starten.
2. Verbinden Sie das Gerät nach Aufforderung mit dem WiFi-Netzwerk. Über das WiFi-Netzwerk wird dann per QR-Code (codiert in der JSON-Datei) auf den Download-Speicherort von Secure Hub zugegriffen.

   Sobald das Gerät mit dem WiFi verbunden ist, lädt es ein Google-Programm zum Lesen des QR-Codes herunter und aktiviert die Kamera.
3. Halten Sie die Kamera über den QR-Code, um ihn zu scannen.

   Android lädt Secure Hub vom Speicherort im QR-Code herunter, validiert die Signatur des Signaturzertifikats, installiert Secure Hub und legt die App als Gerätebesitzer fest.

Weitere Informationen finden Sie in diesem Google-Handbuch für Android EMM-Entwickler: https://developers.google.com/android/work/prov-devices#qr_code_method.

Zero-Touch-Registrierung

Mit der Zero-Touch-Registrierung können Sie festlegen, dass Geräte beim ersten Einschalten als vollständig verwaltete Geräte bereitgestellt werden.

Ihr Geräte-Vertriebspartner erstellt für Sie ein Konto im Android-Portal für die Zero-Touch-Registrierung, einem Online-Tool zum Konfigurieren von Geräten. Im Android-Portal für die Zero-Touch-Registrierung erstellen Sie eine oder mehrere Konfigurationen für die Zero-Touch-Registrierung und wenden diese dann auf die Geräte an, die Ihrem Konto zugewiesen sind. Wenn Benutzer die Geräte dann einschalten, werden sie automatisch bei XenMobile registriert. Die dem Gerät zugewiesene Konfiguration definiert den automatischen Registrierungsprozess.

Systemanforderungen

- Die Zero-Touch-Registrierung wird ab Android 8.0 unterstützt.

Geräte und Kontoinformationen Ihres Vertriebspartners

- Geräte mit Zero-Touch-Registrierung können vom Vertriebspartner des Unternehmens oder einem Google-Partner erworben werden. Eine Liste aller Partner für die Zero-Touch-Registrierung für Android Enterprise finden Sie auf der Android-Website.
- Ein von Ihrem Vertriebspartner erstelltes Android Enterprise-Konto im Portal für die Zero-Touch-Registrierung.

- Von Ihrem Vertriebspartner bereitgestellte Anmeldeinformationen für das Android Enterprise-Konto im Portal für die Zero-Touch-Registrierung.

Erstellen einer Zero-Touch-Konfiguration

Geben Sie beim Erstellen einer Zero-Touch-Konfiguration die Konfigurationsdetails in einem benutzerdefinierten JSON-Objekt an.

Mit diesem JSON-Objekt konfigurieren Sie, dass das Gerät sich beim von Ihnen angegebenen XenMobile-Server registriert. Ersetzen Sie "URL" im Beispiel durch die URL Ihres Servers.

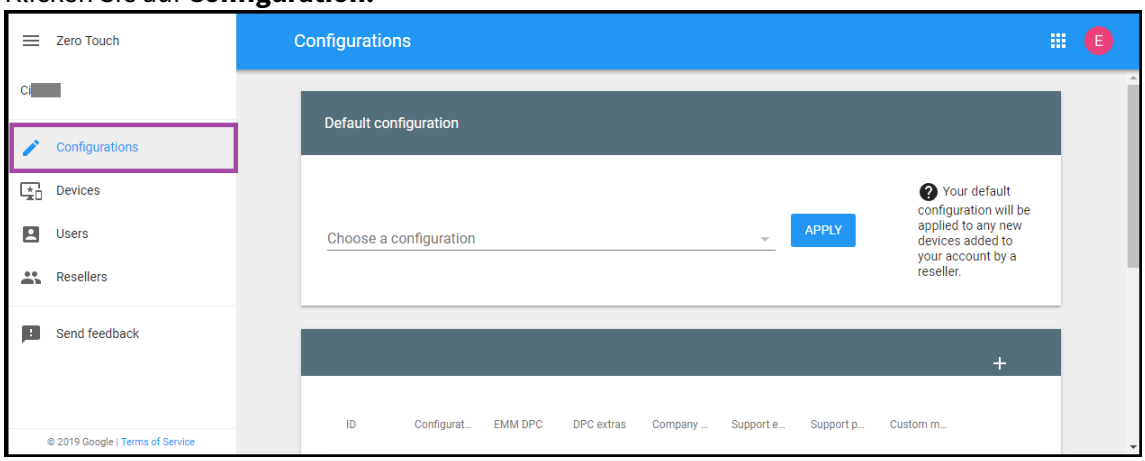
```
1        {
2
3            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6                "serverURL":"URL",
7            }
8
9         }
10
11 <!--NeedCopy-->
```

Mit einem optionalen JSON-Objekt mit zusätzlichen Parametern können Sie Ihre Konfiguration weiter anpassen. Im folgenden Beispiel sind der XenMobile-Server sowie der Benutzername und das Kennwort festgelegt, mit denen Geräte sich in dieser Konfiguration am Server anmelden.

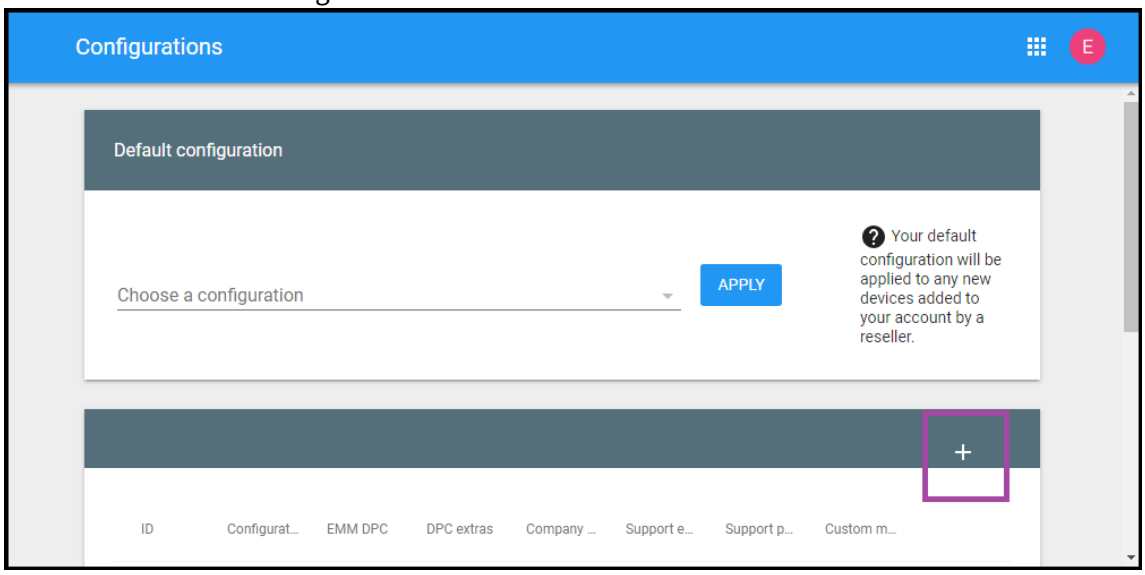
```
1       {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4            {
5
6                "serverURL":"URL",
7                "xm_username":"username",
8                "xm_password":"password"
9             }
10
11              }
12
13    <!--NeedCopy-->
```

1. Navigieren Sie zum Android-Portal für die Zero-Touch-Registrierung unter https://partner.android.com/zerotouch. Melden Sie sich mit den Kontoinformationen an, die Sie vom Vertriebspartner Ihres Zero-Touch-Geräts erhalten haben.

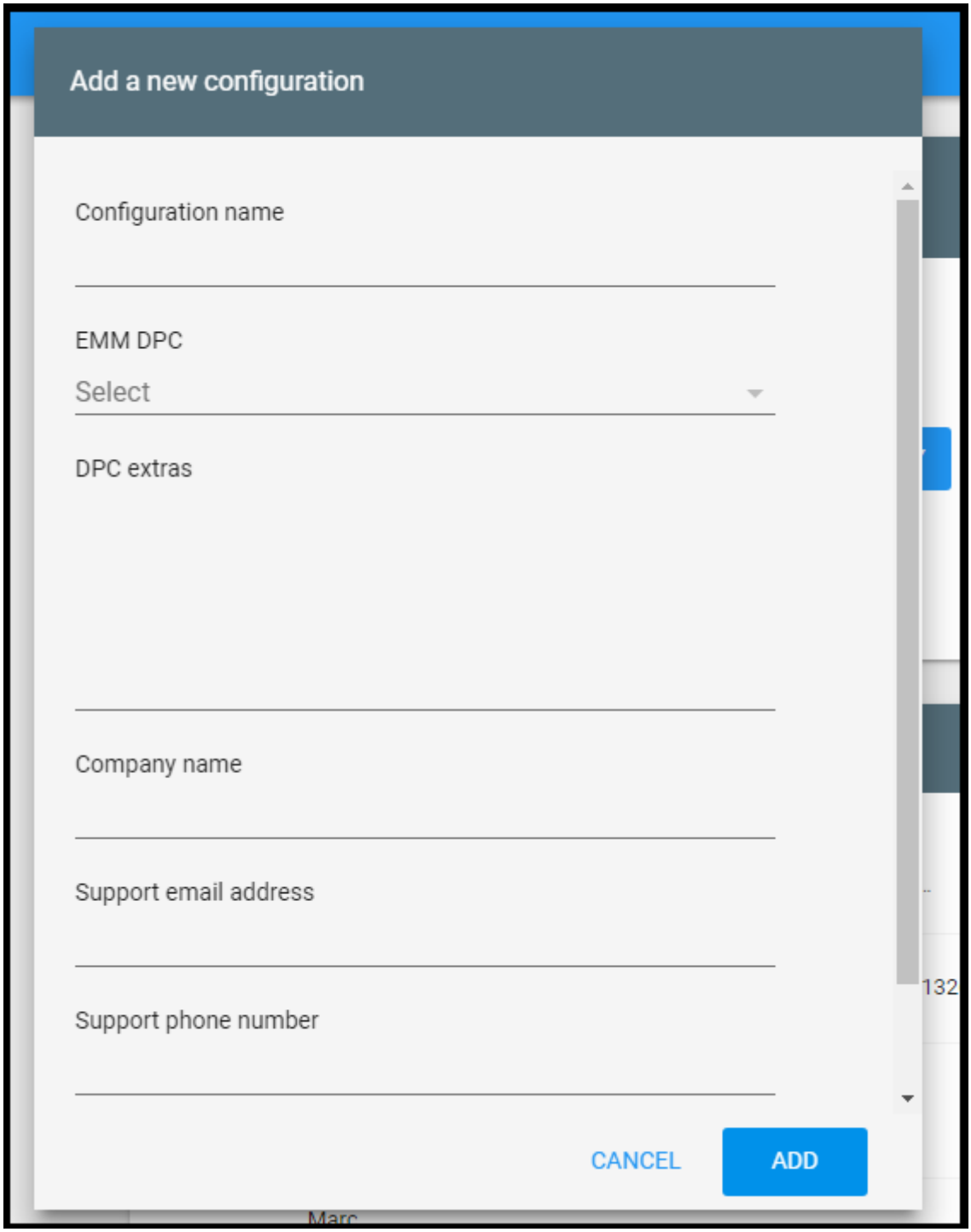
2. Klicken Sie auf **Configuration.**



3. Klicken Sie über der Konfigurationstabelle auf **+**.



4. Geben Sie im angezeigten Konfigurationsfenster Ihre Konfigurationsinformationen ein.

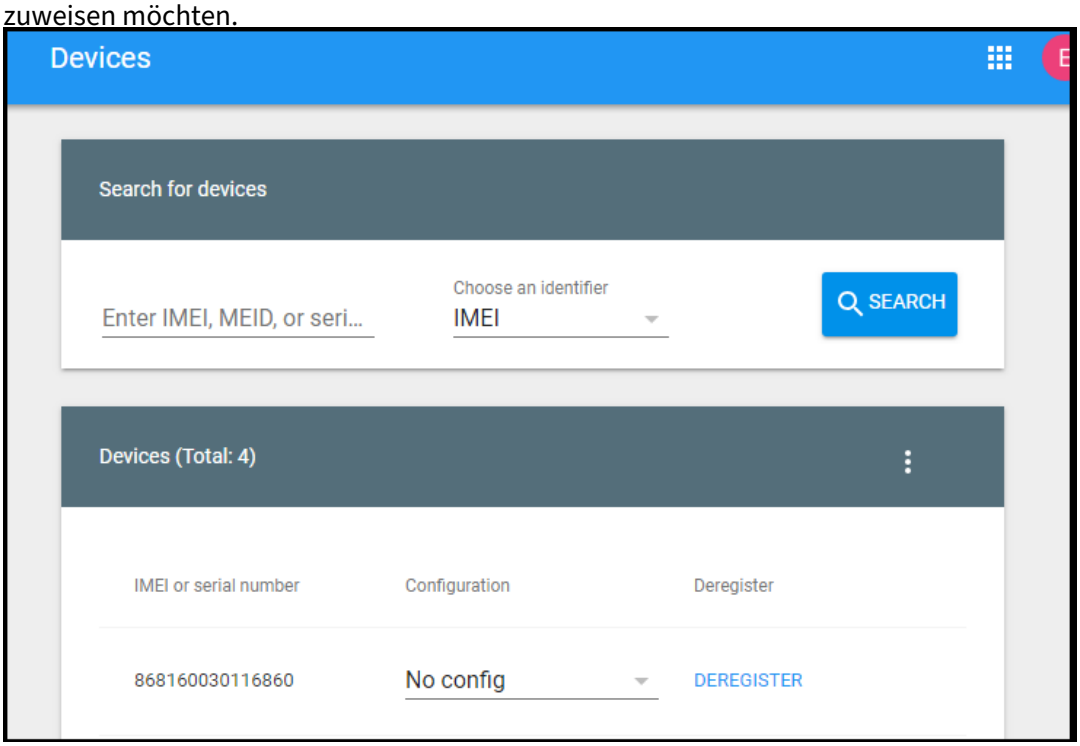


- **Configuration name:** Geben Sie den für diese Konfiguration gewählten Namen ein.
- **EMM DPC:** Wählen Sie **Citrix Secure Hub**.
- **DPC extras:** Fügen Sie hier Ihren benutzerdefinierten JSON-Text ein.
- **Company name:** Geben Sie den Namen ein, der beim Provisioning auf Ihren Android Enterprise-Geräten mit Zero-Touch-Registrierung angezeigt werden soll.
- **Support email address:** Geben Sie eine E-Mail-Adresse für Supportanfragen von

Benutzern ein. Diese Adresse wird vor dem Provisioning auf Ihren Android Enterprise-Geräten mit Zero-Touch-Registrierung angezeigt.

- **Support phone number:** Geben Sie eine Telefonnummer für Supportanfragen von Benutzern ein. Diese Telefonnummer wird vor dem Provisioning auf Ihren Android Enterprise-Geräten mit Zero-Touch-Registrierung angezeigt.
- **Custom Message:** Erläutern Sie optional in ein oder zwei Sätzen, wie Benutzer Sie erreichen können oder was mit dem Gerät geschieht. Diese benutzerdefinierte Nachricht wird vor dem Provisioning auf Ihren Android Enterprise-Geräten mit Zero-Touch-Registrierung angezeigt.

5. Klicken Sie auf **Hinzufügen**.
6. Zum Erstellen weiterer Konfigurationen wiederholen Sie die Schritte 2 bis 4.
7. Anwenden einer Konfiguration auf ein Gerät:
   a) Klicken Sie im Android-Portal für die Zero-Touch-Registrierung auf **Devices**.
   b) Suchen Sie das Gerät in der Geräteliste und wählen Sie die Konfiguration aus, die Sie ihm zuweisen möchten.



   c) Klicken Sie auf **Aktualisieren**.

Über eine CSV-Datei können Sie eine Konfiguration auf mehrere Geräte anwenden.

Informationen zum Anwenden einer Konfiguration auf mehrere Geräte finden Sie im Android Enterprise-Hilfethema Zero-Touch-Registrierung für IT-Administratoren. Dieses Android Enterprise-Hilfethema enthält weitere Informationen, wie Sie Konfigurationen verwalten und auf Geräte

anwenden.

Provisioning von dedizierten Geräten mit Android Enterprise

Dedizierte Android Enterprise-Geräte sind vollständig verwaltete Einzweckgeräte. Dedizierte Geräte werden auch als unternehmenseigene Einzweckgeräte (COSU) bezeichnet. Diese Geräte beschränken Sie auf eine oder wenige Apps, die zum Ausführen der für den vorgegebenen Zweck erforderlichen Aufgaben notwendig sind. Außerdem verhindern Sie, dass Benutzer weitere Apps aktivieren oder andere Aktionen auf dem Gerät ausführen.

Registrieren Sie dedizierte Geräte mit einer der Registrierungsmethoden, die für andere vollständig verwaltete Geräte verwendet werden, wie unter Provisioning vollständig verwalteter Geräte in Android Enterprise beschrieben. Für das Provisioning dedizierter Geräte ist vor der Registrierung ein zusätzliches Setup erforderlich.

Provisioning dedizierter Geräte:

- Fügen Sie ein Registrierungsprofil für die XenMobile-Administratoren hinzu, denen Sie die Registrierung von dedizierten Geräten bei XenMobile gestatten möchten. Siehe Registrierungsprofile erstellen.
- Setzen Sie die Apps, auf die das dedizierte Gerät zugreifen soll, auf eine Positivliste.
- Legen Sie optional für zugelassene Apps fest, dass diese den LockTask-Modus zulassen. Im gesperrten Task-Modus wird eine App an den Gerätebildschirm angeheftet, wenn der Benutzer sie öffnet. Es gibt keine Hometaste, und die Zurück-Taste ist deaktiviert. Der Benutzer beendet die App mit einer in der App programmierten Aktion, z. B. Abmelden.
- Registrieren Sie jedes Gerät im hinzugefügten Registrierungsprofil.

Systemanforderungen

- Die Registrierung dedizierter Geräte ist ab Android 6.0 möglich.

Zulassen von Apps und Festlegen des LockTask-Modus

Über die Kioskgeräterichtlinie können Sie Apps zulassen (d. h. auf die Positivliste setzen) und den LockTask-Modus festlegen. Secure Hub- und Google Play-Dienste sind standardmäßig zugelassen.

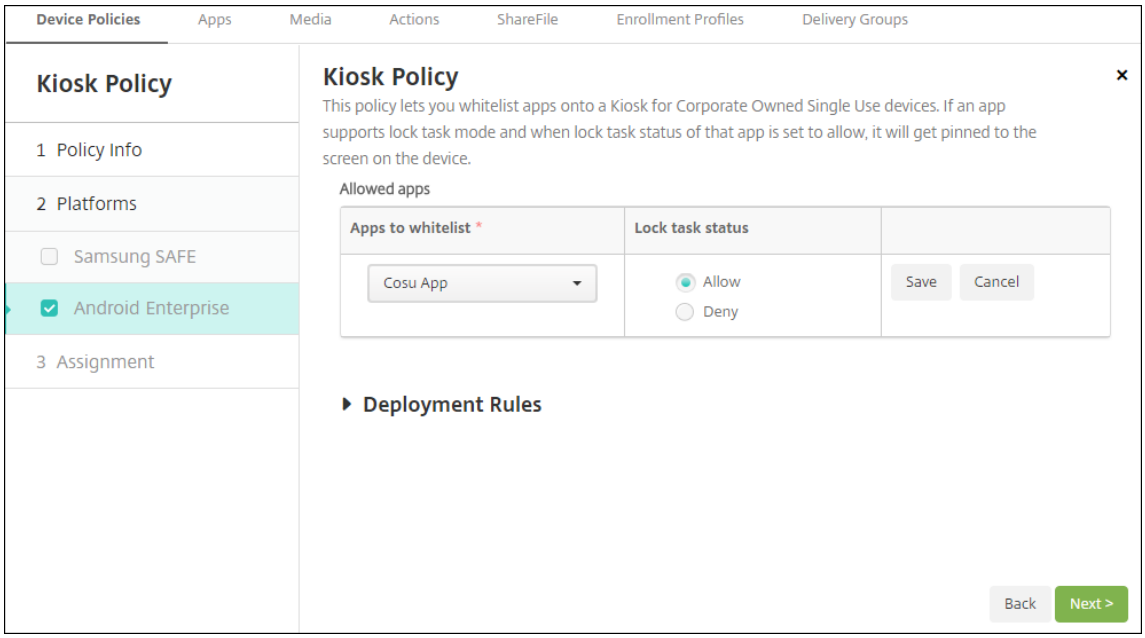
Hinzufügen der Kioskrichtlinie

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 “Sicherheit” auf **Kiosk**. Die Seite **Kioskrichtlinie** wird angezeigt.

4. Wählen Sie unter “Plattformen” die Option **Android Enterprise**. Deaktivieren Sie andere Plattformen.
5. Geben Sie im Bereich Richtlinieninformationen den **Richtliniennamen** und optional eine **Beschreibung** ein.
6. Klicken Sie auf **Weiter** und dann auf **Hinzufügen**.
7. Zum Zulassen einer App und Festlegen des LockTask-Modus gehen Sie wie folgt vor:

   Wählen Sie die gewünschte App aus der Liste aus.

   Wählen Sie **Zulassen**, um festzulegen, dass die App an den Gerätebildschirm angeheftet wird, wenn der Benutzer die App startet. Wählen Sie **Verweigern**, um festzulegen, dass die App nicht angeheftet werden soll. Die Standardeinstellung ist **Zulassen**.

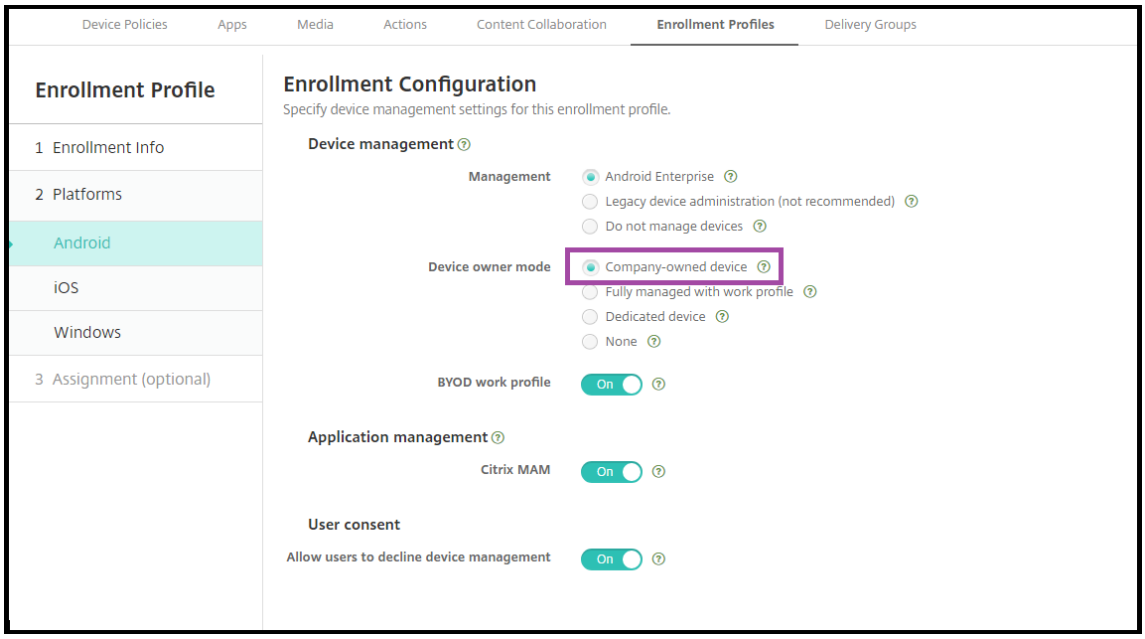


8. Klicken Sie auf **Speichern**.
9. Klicken Sie zum Zulassen einer weiteren App und Festlegen des LockTask-Modus auf **Hinzufügen**.
10. Konfigurieren Sie Bereitstellungsregeln und wählen Sie Bereitstellungsgruppen. Weitere Informationen finden Sie unter Geräterichtlinien.

Registrieren des Geräts

1. Klicken Sie auf **Weiter** oder wählen Sie **Android** unter **Plattformen** aus. Die Seite “Registrierungskonfiguration” wird angezeigt.
2. Legen Sie **Verwaltung** auf **Android Enterprise** fest.

3. Legen Sie den **Gerätebesitzermodus** auf **Unternehmenseigenes Gerät** fest.



4. Wählen Sie **Zuweisung (Optionen)**. Der Bildschirm für die Bereitstellungsgruppenzuweisung wird angezeigt.
5. Wählen Sie die Bereitstellungsgruppe(n) mit den Administratoren, die dedizierte Geräte registrieren sollen. Klicken Sie auf **Speichern**.

Wenn Sie **BYOD-Arbeitsprofil** im Registrierungsprofil aktiviert haben, werden Geräte, die nicht neu sind oder auf die Werkseinstellungen zurückgesetzt wurden, als Arbeitsprofilgeräte registriert. Siehe Provisioning von Arbeitsprofilgeräten mit Android Enterprise.

Provisioning vollständig verwalteter Android Enterprise-Geräte mit Arbeitsprofil (COPE-Geräte)

Vollständig verwaltete Geräte mit Arbeitsprofil, früher auch als COPE-Geräte bezeichnet, sind unternehmenseigene Geräte, die für geschäftliche und private Zwecke verwendet werden. Ihre Organisation verwaltet die gesamten Geräte. Sie können einige Richtlinien auf das Gerät und andere Richtlinien auf das Arbeitsprofil anwenden.

In der XenMobile-Konsole werden vollständig verwaltete Geräte mit Arbeitsprofil wie folgt angezeigt:

- Als Gerätebesitzer wird “Unternehmen” angegeben.
- Als Android Enterprise-Installationstyp wird “COPE (Unternehmenseigentum, vom Benutzer verwaltet)” angegeben.

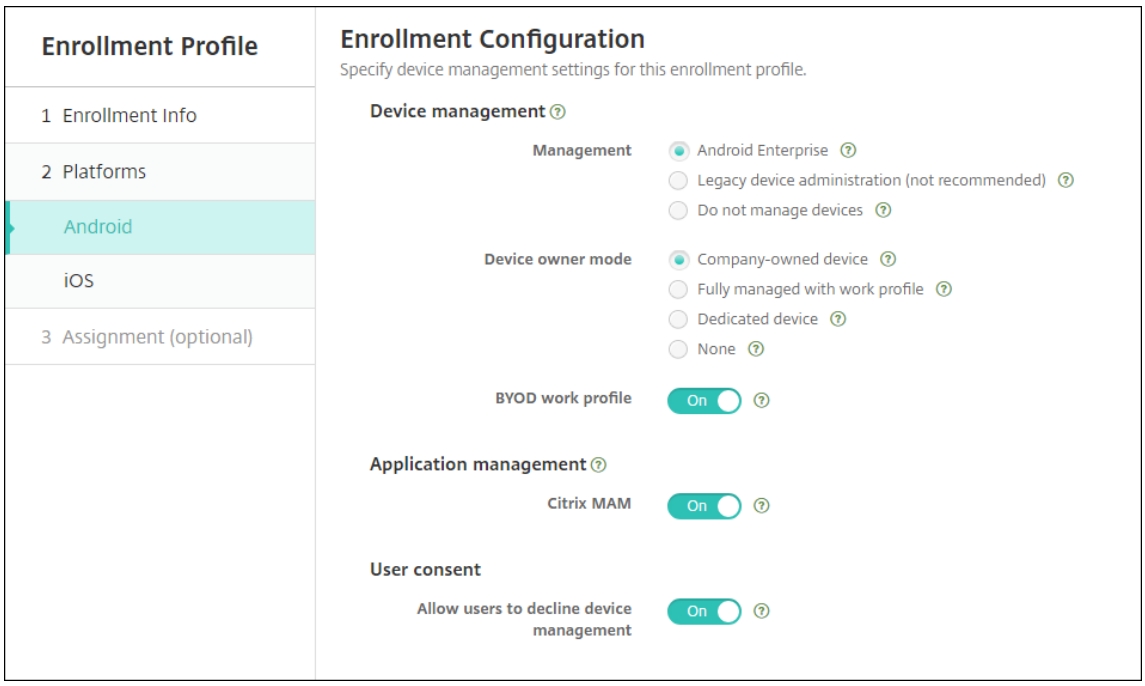
Systemanforderungen

- Die Registrierung vollständig verwalteter Geräte mit Arbeitsprofil wird ab Android 8.0 bis zu Android 10.x unterstützt.

Hinzufügen eines Registrierungsprofils für vollständig verwaltete Geräte mit Arbeitsprofil

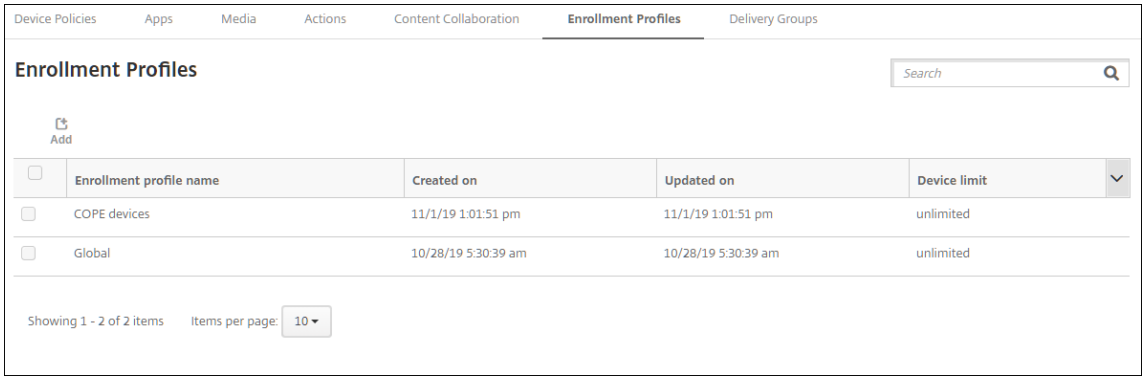
Erstellen Sie ein Registrierungsprofil für vollständig verwaltete Geräte mit Arbeitsprofil. Die Administratoren in den Bereitstellungsgruppen, die diesem Registrierungsprofil zugewiesen sind, können vollständig verwaltete Geräte mit Arbeitsprofil dann registrieren. Damit diese Administratoren alle erforderlichen Geräte registrieren können, erstellen Sie für sie ein Registrierungsprofil unter Zulassung einer unbegrenzten Anzahl an Geräten pro Benutzer. Weisen Sie dieses Profil einer Bereitstellungsgruppe mit den Administratoren zu, die vollständig registrierte Geräte mit Arbeitsprofil registrieren werden.

1. Gehen Sie in der XenMobile-Konsole zu **Konfigurieren > Registrierungsprofile**.
2. Wenn Sie ein Registrierungsprofil hinzufügen möchten, klicken Sie auf **Hinzufügen**. Geben Sie auf der Seite “Registrierungsinfo” einen Namen für das Registrierungsprofil ein. Legen Sie für die Anzahl der Geräte, die Mitglieder mit diesem Profil registrieren können, “Unbegrenzt” fest.
3. Klicken Sie auf **Weiter** oder wählen Sie **Android Enterprise** unter **Plattformen**. Die Seite “Registrierungskonfiguration” wird angezeigt.
4. Wählen Sie als **Registrierungsart** eine der folgenden Optionen:
    - **Vollständig verwaltet/Arbeitsprofil:** Neue Geräte oder Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, werden als vollständig verwaltete Geräte registriert. Bei registrierten BYOD-Geräten verwalten Sie nur ein Arbeitsprofil.
    - **COPE/Arbeitsprofil:** Neue Geräte oder Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, werden als vollständig verwaltete Geräte mit Arbeitsprofil registriert. Bei registrierten BYOD-Geräten verwalten Sie nur ein Arbeitsprofil.



5. Wählen Sie **Zuordnung (optional)** oder klicken Sie auf **Weiter**. Der Bildschirm für die Bereitstellungsgruppenzuweisung wird angezeigt.
6. Wählen Sie die Bereitstellungsgruppe(n) mit den Administratoren, die dedizierte Geräte registrieren sollen. Klicken Sie auf **Speichern**.

   Die Seite “Registrierungsprofil” wird mit dem von Ihnen hinzugefügten Profil angezeigt.



Wenn ein Benutzer zu mehreren Bereitstellungsgruppen mit unterschiedlichen Registrierungsprofilen gehört, bestimmt der Name der Bereitstellungsgruppe das verwendete Registrierungsprofil. XenMobile wählt die letzte Bereitstellungsgruppe in der alphabetisch geordneten Bereitstellungsgruppenliste aus.

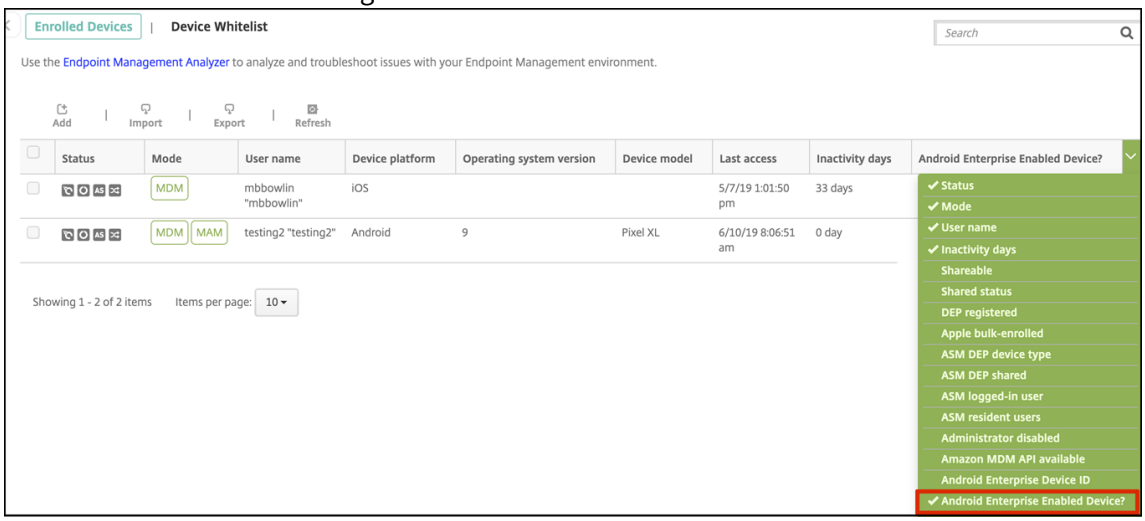
Registrieren des Geräts

Neue Geräte und Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, werden per DPC-ID-Token, NFC-Übertragung oder QR-Code als vollständig verwaltete Geräte mit Arbeitsprofil registriert. Weitere Informationen finden Sie unter Registrierung von Geräten mit dem Citrix DPC-ID-Token, Registrieren von Geräten per NFC-Datenübertragung oder Registrieren von Geräten per QR-Code.

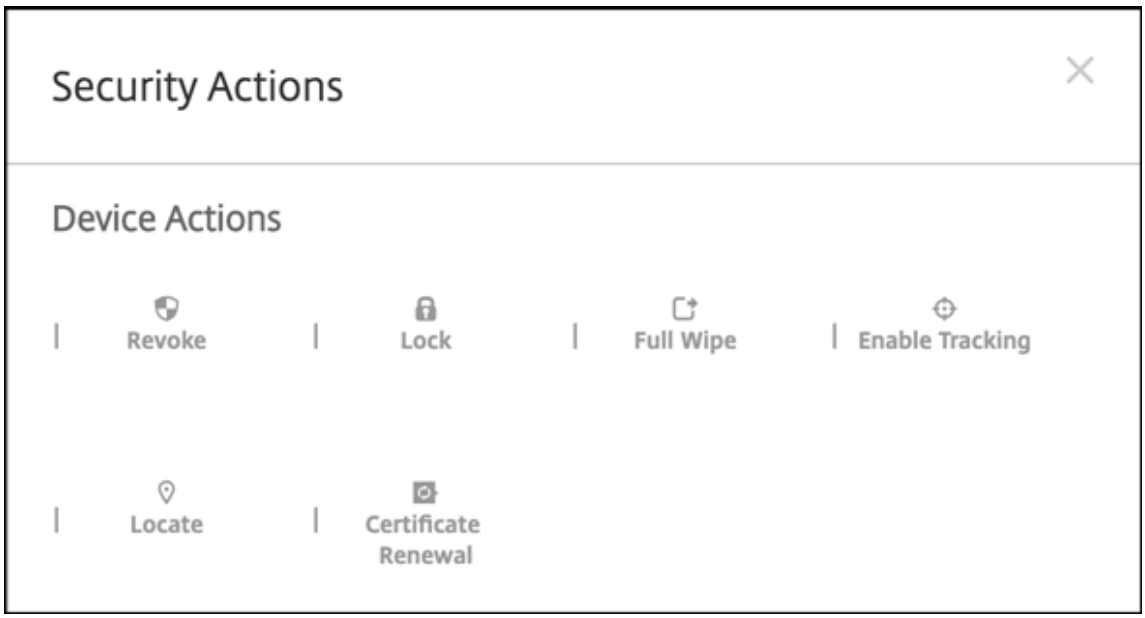
Geräte, die nicht neu oder auf die Werkseinstellungen zurückgesetzt sind, werden als Arbeitsprofilgeräte registriert, wie unter Provisioning von Arbeitsprofilgeräten mit Android Enterprise beschrieben.

Anzeige von Android Enterprise-Geräten in der XenMobile-Konsole

1. Gegen Sie in der XenMobile-Konsole zu **Verwalten > Geräte**.
2. Klicken Sie hier auf das Menü am rechten Tabellenrand, um die Spalte **Für Android Enterprise aktiviertes Gerät?** hinzuzufügen.



3. Um verfügbare Sicherheitsaktionen anzuzeigen, wählen Sie ein vollständig verwaltetes Gerät und klicken auf **Sicher**. Wenn das Gerät vollständig verwaltet ist, ist die Aktion **Vollständig löschen** verfügbar, **Selektiv löschen** jedoch nicht. Dieser Unterschied liegt daran, dass das Gerät nur Apps aus dem verwalteten Google Play Store zulässt. Der Benutzer kann keine Apps aus dem öffentlichen Store installieren. Ihre Organisation verwaltet alle Inhalte auf dem Gerät.



Konfigurieren von App- und Geräterichtlinien für Android Enterprise

Einen Überblick über die Richtlinien, die auf App- und Geräteebene gelten, finden Sie unter Unterstützte Geräte- und MDX-Richtlinien für Android Enterprise.

Wissenswertes über Richtlinien:

- **Schutz vor Datenverlust:** Apps sind im XenMobile MAM-Container durch Verschlüsselung und andere mobile DLP-Technologien vor Datenverlust geschützt. Verwenden Sie das Citrix MAM-SDK, oder MDX Toolkit, um Apps MDX-fähig zu machen.
- **Geräteeinschränkungen:** Es gibt zahlreiche Geräteeinschränkungen, mit denen Sie Features wie die folgenden steuern können:
  - Verwendung der Gerätekamera
  - Verwendung von Kopieren und Einfügen zwischen geschäftlichen und privaten Profilen
- **Pro-App-VPN:** Mit der Geräterichtlinie für verwaltete Konfigurationen können Sie VPN-Profile für Android Enterprise konfigurieren.
- **E-Mail-Richtlinie:** Wir empfehlen die Verwendung der Geräterichtlinie für verwaltete Konfigurationen, um Apps zu konfigurieren.

In dieser Tabelle sind alle für Android Enterprise-Geräte verfügbaren Geräterichtlinien aufgeführt.

> **Wichtig:**
>
> Für Geräte, die bei Android Enterprise registriert werden und MDX-Apps verwenden: Sie können einige Einstellungen über MDX und Android Enterprise steuern. Verwenden Sie die am wenigsten restriktiven Richtlinieneinstellungen für MDX und steuern Sie die Richtlinie über Android Enter-

> prise.

Android Enterprise-App-Berechtigungen	Verwaltete Android Enterprise-Konfigurationen	App-Bestand
App-Deinstallation	Verwaltete Apps automatisch aktualisieren	OS-Update steuern
Anmeldeinformationen	Benutzerdefiniertes XML	Exchange
Dateien	Keyguard-Verwaltung	Kiosk
Standort	Passcode	Einschränkungen
Samsung MDM-Lizenzschlüssel	Planung	Wi-Fi
XenMobile-Optionen		

Geräterichtlinien für vollständig verwaltete Geräte mit Arbeitsprofil (COPE-Geräte)

Bei vollständig verwalteten Geräten mit Arbeitsprofil (COPE-Geräten) können mithilfe von Geräterichtlinien separate Einstellungen auf das gesamte Gerät bzw. das Arbeitsprofil angewendet werden. Mit separaten Geräterichtlinien können Sie bei vollständig verwalteten Geräterichtlinien mit Arbeitsprofil Einstellungen nur auf das gesamte Gerät oder auf das Arbeitsprofil anwenden.

Richtlinie	Gültig für
Android Enterprise-App-Berechtigungen	Arbeitsprofil
Verwaltete Android Enterprise-Konfigurationen	Arbeitsprofil
App-Bestand	Arbeitsprofil
App-Deinstallation	Arbeitsprofil
Verwaltete Apps automatisch aktualisieren	Arbeitsprofil
OS-Update steuern	Nicht zutreffend
Anmeldeinformationen	Arbeitsprofil
Benutzerdefiniertes XML	Nicht zutreffend
Exchange	Nicht zutreffend
Dateien	Arbeitsprofil

Richtlinie	Gültig für
Keyguard-Verwaltung	Geräte- und Arbeitsprofil
Kiosk	Nicht zutreffend
Standort	Gerät (nur Standortmodus)
Passcode	Geräte- und Arbeitsprofil
Einschränkungen	Geräte- und Arbeitsprofil (separate Richtlinien für Gerät und Arbeitsprofil erstellen)
Samsung MDM-Lizenzschlüssel	Nicht zutreffend
Planung	Arbeitsprofil
Wi-Fi	Gerät
XenMobile-Optionen	Arbeitsprofil

Siehe auch Unterstützte Geräte- und MDX-Richtlinien für Android Enterprise und Überblick über das MAM-SDK.

Sicherheitsaktionen

Android Enterprise unterstützt die folgenden Sicherheitsaktionen. Eine Beschreibung der einzelnen Sicherheitsaktionen finden Sie unter Sicherheitsaktionen.

Sicherheitsaktionen	Arbeitsprofil	Vollständig verwaltet
Zertifikaterneuerung	Ja	Ja
Vollständig löschen	Nein	Ja
Suchen	Ja	Ja
Sperren	Ja	Ja
Lock and Reset Password	Nein	Ja
Notify (Ring)	Ja	Ja
Widerrufen	Ja	Ja
Selektiv löschen	Ja	Nein

Hinweise zu Sicherheitsaktionen

- Die Sicherheitsaktion zur Ortung funktioniert nur, wenn in der Standortrichtlinie der Standortmodus für das Gerät auf **Hohe Genauigkeit** oder **Akku schonen** festgelegt ist. Weitere Informationen finden Sie unter Standortrichtlinie für Geräte.
- Auf Arbeitsprofilgeräten mit Android-Versionen vor Android 8.0 gilt Folgendes:
  - Die Aktion “Sperren und Kennwort zurücksetzen” wird nicht unterstützt.
- Auf Arbeitsprofilgeräten mit Android 8.0 oder höher gilt Folgendes:
  - Der gesendete Passcode sperrt das Arbeitsprofil. Das Gerät selbst wird nicht gesperrt.
  - Wenn kein Passcode im Arbeitsprofil festgelegt ist:
    - Wenn kein Passcode gesendet wird oder der gesendete Passcode nicht den Anforderungen entspricht, wird das Gerät gesperrt.
  - Wenn ein Passcode für das Arbeitsprofil festgelegt ist:
    - Wenn kein Passcode gesendet wird oder der gesendete Passcode nicht den Anforderungen entspricht, wird nur das Arbeitsprofil gesperrt (nicht das Gerät selbst).
- Auf vollständig verwalteten Geräte mit Arbeitsprofil (COPE-Geräte):
  - Sie können die Sicherheitsaktion “Sperren” auf das Gerät oder auf das Arbeitsprofil anwenden.

Registrierung für Android Enterprise-Unternehmen aufheben

Wenn Sie Ihr Android Enterprise-Unternehmen nicht mehr verwenden möchten, können Sie die Registrierung des Unternehmens aufheben.

> **Warnung:**
>
> Nachdem Sie die Registrierung eines Unternehmens aufheben, werden Android Enterprise-Apps auf Geräten, die bereits registriert wurden, auf die Standardeinstellungen zurückgesetzt. Google verwaltet die Geräte nicht mehr. Wenn Sie sich bei einem neuen Android Enterprise-Unternehmen registrieren, müssen Sie Apps für das neue Unternehmen von verwaltetem Google Play genehmigen. Anschließend können Sie die Apps in der XenMobile-Konsole aktualisieren.

Nachdem die Registrierung des Android Enterprise-Unternehmens aufgehoben wurde:

- Für Geräte und Benutzer, die über das Unternehmen registriert sind, wurden die Android Enterprise-Apps auf die Standardeinstellung zurückgesetzt. Zuvor angewendete Richtlinien für verwaltete Android Enterprise-Konfigurationen haben keine Wirkung mehr auf Vorgänge.
- XenMobile verwaltet Geräte, die über das Unternehmen registriert sind. Aus Sicht von Google werden diese Geräte nicht verwaltet. Sie können keine neuen Android Enterprise-Apps hinzufügen. Sie können keine Richtlinien für verwaltete Android Enterprise-Konfigurationen anwen-

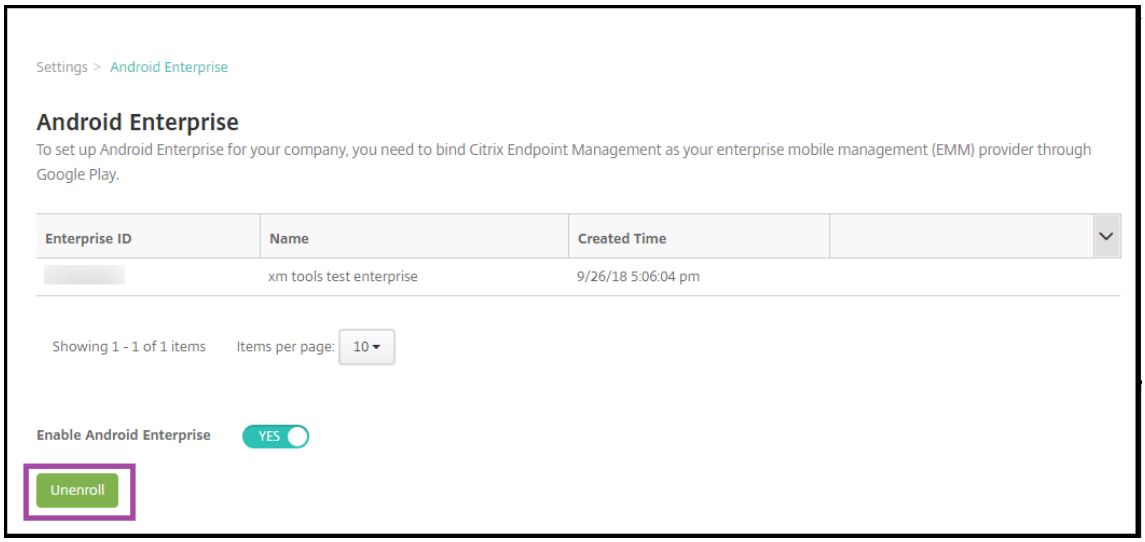
den. Sie können auf diese Geräte andere Richtlinien anwenden, z. B. Planung, Kennwort und Einschränkungen.
- Wenn Sie versuchen, Geräte in Android Enterprise zu registrieren, werden sie als Android-Geräte und nicht als Android Enterprise-Geräte registriert.

Heben Sie die Registrierung eines Android Enterprise-Unternehmens über die XenMobile Server-Konsole und XenMobile Tools auf.

Wenn Sie diese Aufgabe ausführen, öffnet XenMobile ein Popupfenster für XenMobile Tools. Bevor Sie beginnen, sollten Sie sicherstellen, dass XenMobile im verwendeten Browser die Berechtigung hat, Popupfenster zu öffnen. In einigen Browsern, wie Google Chrome, müssen Sie die Popupblockierung deaktivieren und die Adresse der XenMobile-Site der Positivliste des Popupblockers hinzufügen.

Registrierung für Android Enterprise-Unternehmen aufheben:

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite Einstellungen wird angezeigt.
2. Klicken Sie auf der Seite “Einstellungen” auf **Android Enterprise**.
3. Klicken Sie auf **Registrierung aufheben**.



Verteilen von Android Enterprise-Apps

January 5, 2022

XenMobile verwaltet Apps, die auf Geräten bereitgestellt werden. Sie können folgende Arten von Android Enterprise-Apps organisieren und bereitstellen.

- **Verwaltete App Store-Apps:** Die sind kostenlose oder kostenpflichtige Apps, die im verwalteten Google Play Store verfügbar sind. Beispiel: GoToMeeting.

- **MDX:** Apps, die mit dem MAM-SDK vorbereitet oder mit MDX Service oder MDX Toolkit umschlossen wurden. Diese Apps enthalten MDX-Richtlinien. Sie erhalten MDX-Apps über interne Quellen und öffentliche Stores. Stellen Sie mobile Produktivitätsapps von Citrix als MDX-Apps bereit.
- **Unternehmen:** Private Apps, die Sie selbst entwickeln oder von einer anderen Quelle beziehen. Sie stellen diese Apps Ihren Benutzern über den verwalteten Google Play Store zur Verfügung. Der verwaltete Google Play Store ist der Google Store für Unternehmensapps.
- **MDX-fähige private Apps**: Unternehmensapps, die mit dem MAM-SDK vorbereitet oder mit dem MDX Toolkit umschlossen wurden.

Es gibt zwei Möglichkeiten, Unternehmensapps und MDX-fähige private Apps hinzuzufügen.

- Fügen Sie die Apps der XenMobile-Konsole als Unternehmensapps hinzu, wie in diesem Artikel unter Unternehmensapps und MDX-fähige private Apps beschrieben.
- Veröffentlichen Sie die Apps direkt im verwalteten Google Play Store mit Ihrem Google-Entwicklerkonto. Fügen Sie dann die Apps der XenMobile-Konsole als Apps aus dem verwalteten App-Store hinzu. Weitere Informationen finden Sie unter Apps aus dem verwalteten App-Store.

Wenn Sie Apps mit Ihrem Google-Entwicklerkonto veröffentlichen und dann zur XenMobile-Konsole wechseln, ist der App-Besitzer unterschiedlich. Verwalten Sie Ihre Apps in diesem Fall an beiden Standorten. Citrix empfiehlt, Ihre Apps mit der einen oder anderen Methode hinzuzufügen.

Wenn Sie selbstverwaltete Apps aus dem verwalteten Google Play Store entfernen müssen, erstellen Sie ein Ticket bei Google. Entwickler können Apps aus dem verwalteten Google Play Store deaktivieren, aber nicht löschen.

Die folgenden Abschnitte enthalten detaillierte Angaben zur Konfiguration von Android Enterprise-Apps. Informationen zum Verteilen von Apps finden Sie unter Hinzufügen von Apps. Dieser Artikel enthält folgende Informationen:

- Die allgemeinen Workflows zum Hinzufügen von Web- und SaaS-Apps oder Weblinks
- Der erforderliche App-Workflow für Unternehmensapps und Apps aus dem öffentlichen Store
- Workflow zum Bereitstellen von Unternehmensapps über das Citrix Netzwerk für die Inhaltsübermittlung (CDN) für Unternehmensapps

Apps aus dem verwalteten App-Store

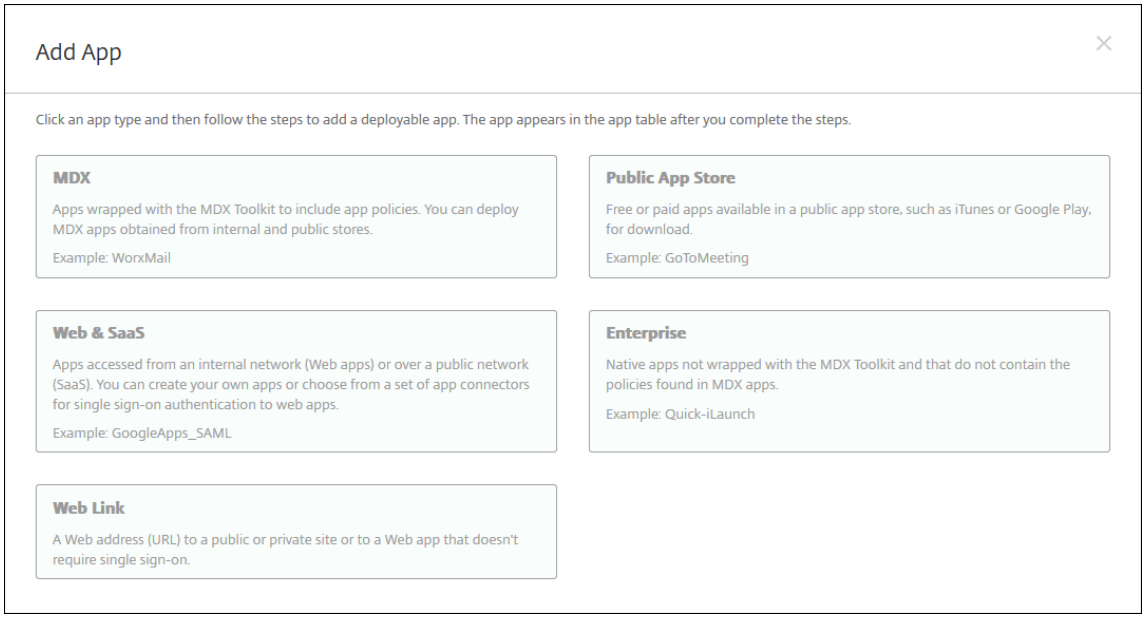
Sie können kostenlose und kostenpflichtige Apps aus dem verwalteten Google Play Store in XenMobile hinzufügen.

> **Hinweis:**
>
> Um alle Apps in Google Play über den verwalteten Google Play-Store zugänglich zu machen, ver-

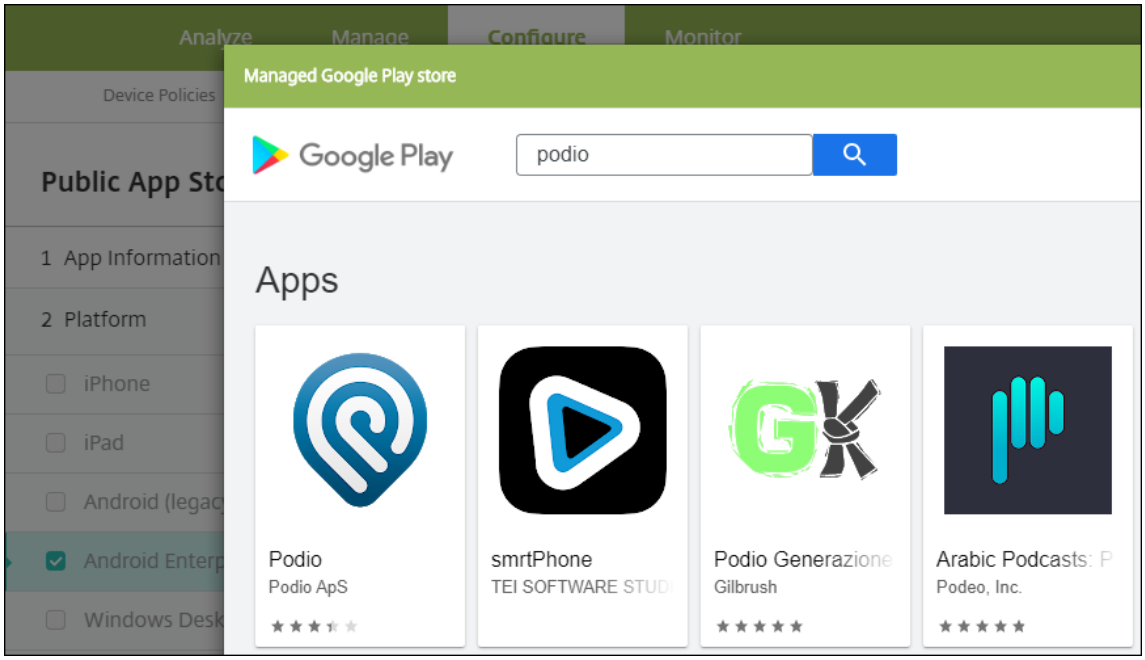
> wenden Sie die Servereigenschaft **Zugriff auf alle Apps im verwalteten Google Play Store**. Siehe Servereigenschaften. Wenn Sie diese Eigenschaft auf **Wahr** setzen, können alle Android Enterprise-Benutzer auf Apps aus dem öffentlichen Google Play Store zugreifen. Mit der Einschränkungsrichtlinie können Sie dann den Zugriff auf diese Apps steuern.

Schritt 1: Hinzufügen und Konfigurieren von Apps

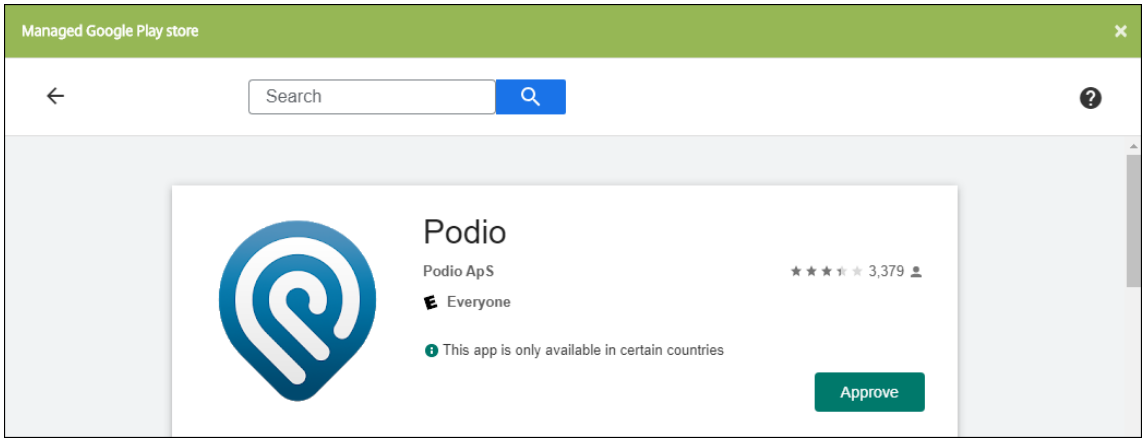
1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **Öffentlicher App-Store**.



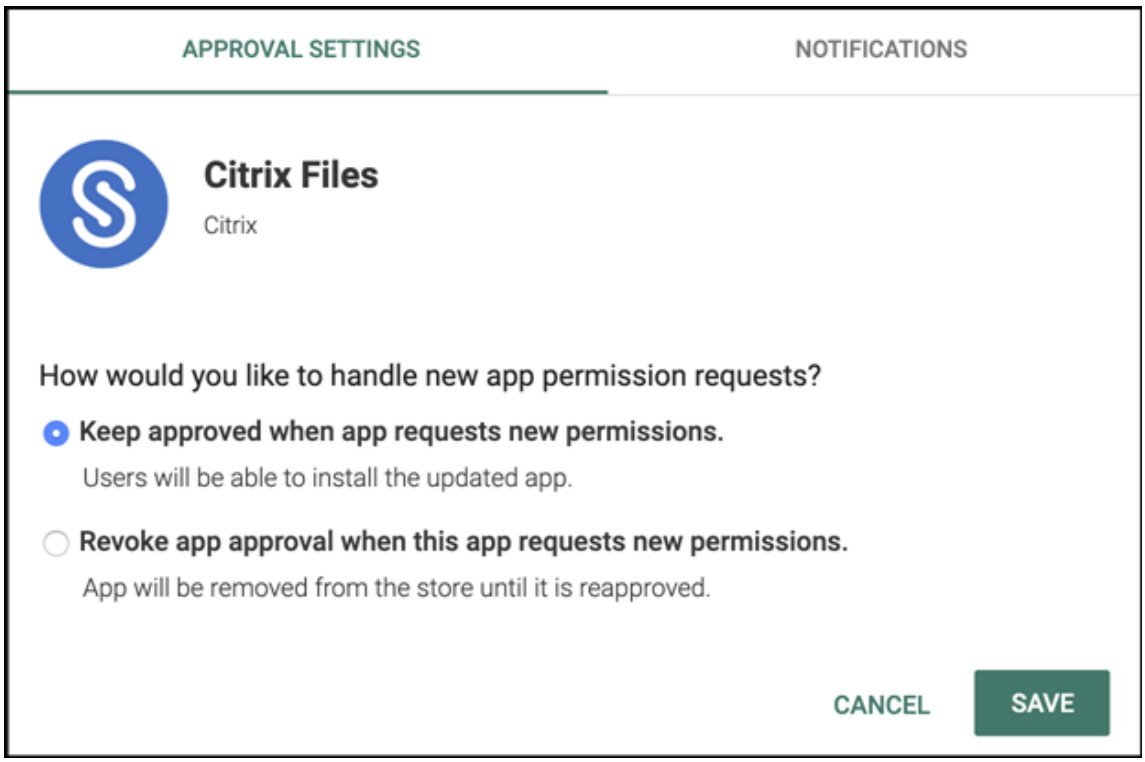
3. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** angezeigt.
   - **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.
   - **App-Kategorie:** Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen möchten. Weitere Informationen zu App-Kategorien finden Sie unter App-Kategorien.
4. Wählen Sie als Plattform **Android Enterprise**.
5. Geben Sie den App-Namen oder die Paket-ID in das Suchfeld ein und klicken Sie auf **Suchen**. Sie finden die Paket-ID im Google Play-Store. Die ID kann der URL der App entnommen werden. Beispielsweise ist `com.Slack` die Paket-ID in `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.



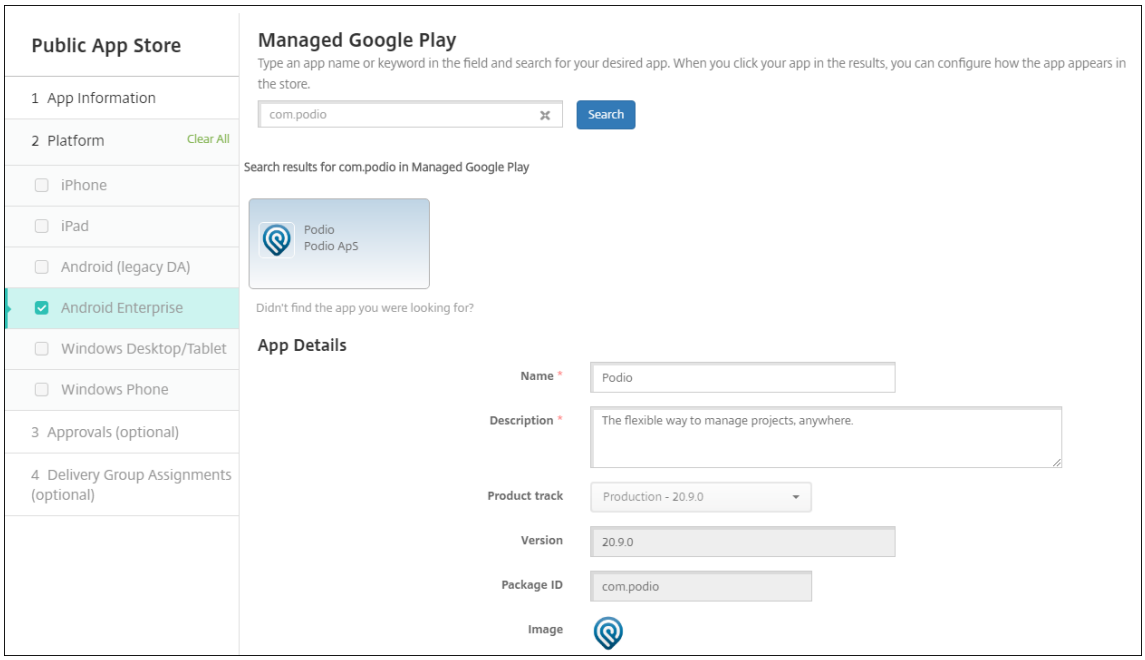
6. Es werden die Apps angezeigt, die den Suchkriterien entsprechen. Klicken Sie auf die gewünschte App und dann auf **Approve**.



7. Klicken Sie erneut auf **Approve**.
8. Wählen Sie **Keep approved when app requests new permissions** aus. Klicken Sie auf **Speichern**.



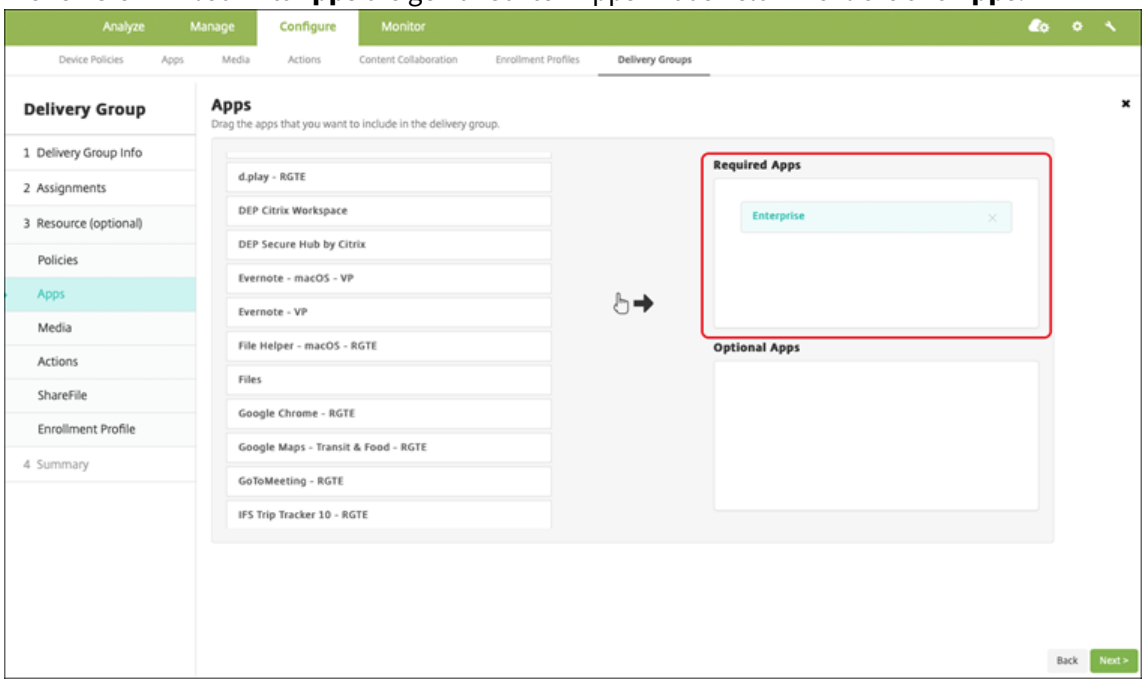
9. Klicken Sie auf das App-Symbol und konfigurieren Sie **Name** und **Beschreibung** der App.



10. Weisen Sie der App beliebige Bereitstellungsgruppen zu und klicken Sie auf **Speichern**. Informationen finden Sie unter Bereitstellen von Ressourcen.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen** und wählen Sie die von Ihnen konfigurierte Bereitstellungsgruppe aus. Klicken Sie auf **Edit**.
2. Ziehen Sie im Abschnitt **Apps** die gewünschten Apps in das Feld **Erforderliche Apps**.



3. Klicken Sie auf der Seite **Zusammenfassung** auf **Speichern**.
4. Wählen Sie auf der Seite **Bereitstellungsgruppen** die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.

MDX-Apps

Fügen Sie MDX-Dateien in XenMobile hinzu und konfigurieren Sie App-Details und Richtlinieneinstellungen. Um mobile Produktivitätsapps von Citrix für Android Enterprise zu konfigurieren, fügen Sie sie als MDX-Apps hinzu. Informationen über die für die einzelnen Geräteplattformen verfügbaren App-Richtlinien finden Sie hier:

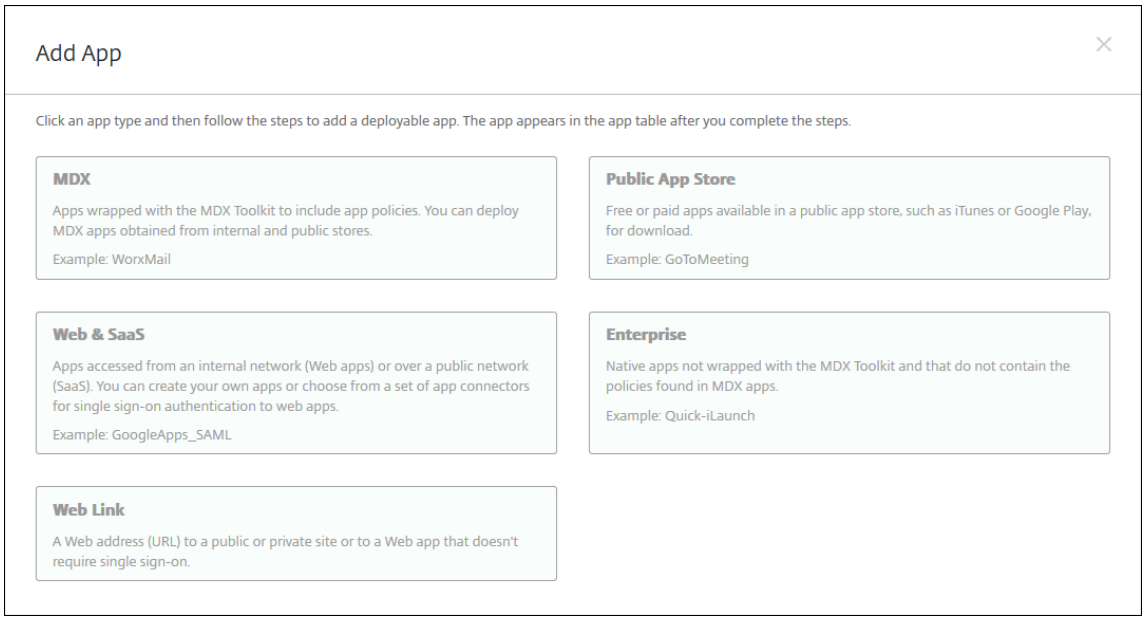
- Überblick über das MAM-SDK
- MDX-Richtlinien auf einen Blick

Schritt 1: Hinzufügen und Konfigurieren von Apps

1. Laden Sie für mobile Produktivitätsapps von Citrix die MDX-Dateien aus dem öffentlichen Store herunter: Gehen Sie zu https://www.citrix.com/downloads. Navigieren Sie zu **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

   Für andere Arten von MDX-Apps benötigen Sie die MDX-Datei.

2. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



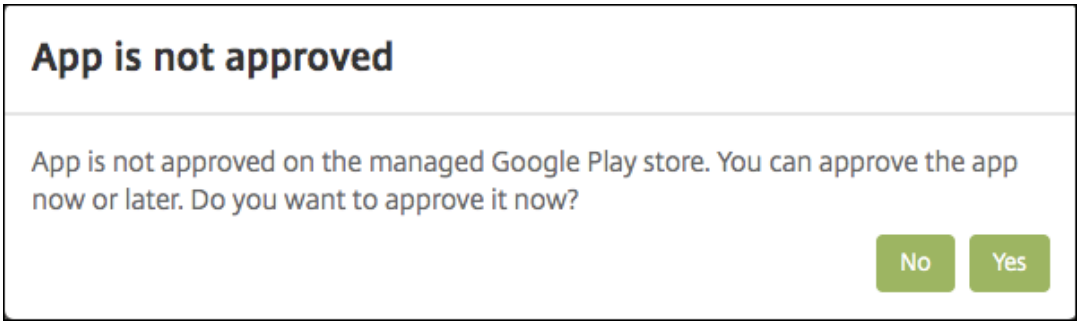
3. Klicken Sie auf **MDX**. Die Seite **App-Informationen** für MDX wird angezeigt. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:

   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** 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 zu App-Kategorien finden Sie unter App-Kategorien.

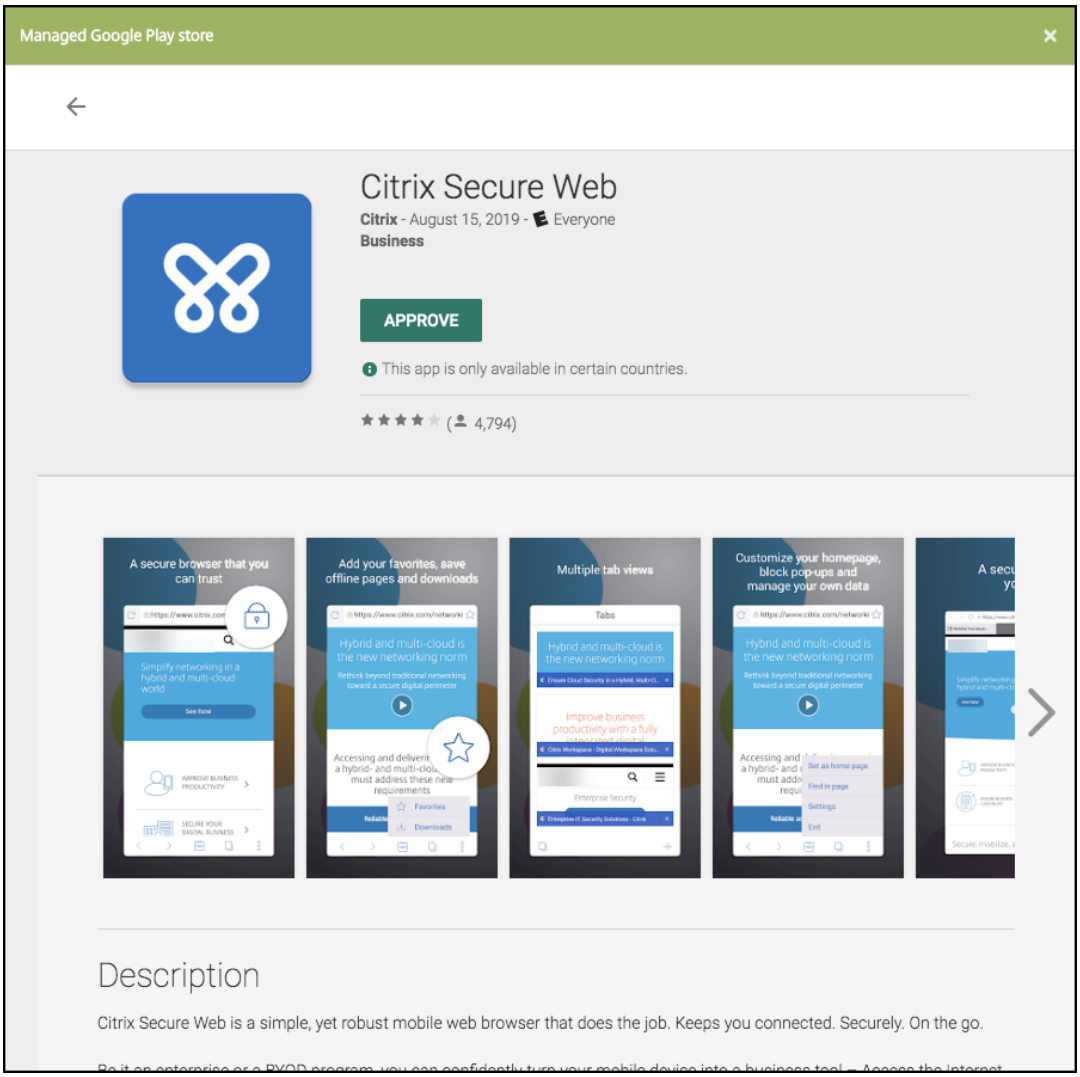
4. Wählen Sie als Plattform **Android Enterprise**.

5. Klicken Sie auf **Upload** und navigieren Sie zur MDX-Datei. Android Enterprise unterstützt nur mit dem MAM-SDK oder MDX Toolkit vorbereitete Apps.

   - Es wird eine Meldung angezeigt, wenn die angehängte Anwendung eine Genehmigung des verwalteten Google Play-Store erfordert. Klicken Sie auf **Ja**, um die Anwendung zu genehmigen, ohne die XenMobile-Konsole zu verlassen.



Sobald der verwaltete Google Play Store geöffnet ist, folgen Sie den Anweisungen, um die App zu genehmigen und zu speichern.



Wenn Sie die App erfolgreich hinzufügen, wird die Seite **App-Detail** angezeigt.

6. Konfigurieren Sie folgende Einstellungen:

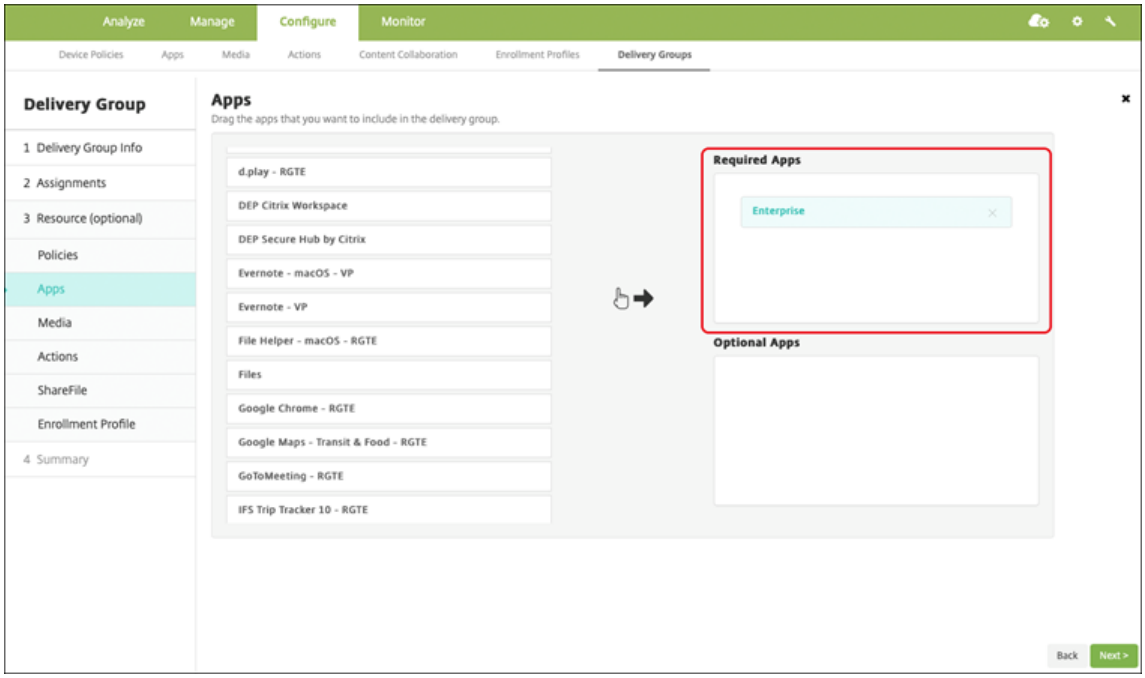
- **Dateiname:** Geben Sie den Dateinamen der App ein.
- **App-Beschreibung:** Geben Sie eine Beschreibung für die App ein.
- **App-Version:** Geben Sie optional die Nummer der App-Version ein.
- **Paket-ID:** Geben Sie die Paket-ID für die App ein, die Sie aus dem verwalteten Google Play Store erhalten haben.
- **OS-Version (Minimum):** Geben Sie optional die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
- **OS-Version (Maximum):** Geben Sie optional 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.

7. Konfigurieren Sie die **MDX-Richtlinien**. MDX-Richtlinien variieren je nach Plattform und bieten Optionen für Richtlinienbereiche wie Authentifizierung, Gerätesicherheit und App-Einschränkungen. In der Konsole kann eine QuickInfo mit einer Beschreibung der Richtlinien angezeigt werden. Informationen über die für die einzelnen Geräteplattformen verfügbaren App-Richtlinien finden Sie hier:
   - Überblick über das MAM-SDK
   - MDX-Richtlinien auf einen Blick
8. Konfigurieren Sie Bereitstellungsregeln und Storekonfiguration.
9. Weisen Sie der App beliebige Bereitstellungsgruppen zu und klicken Sie auf **Speichern**. Informationen finden Sie unter Bereitstellen von Ressourcen.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen** und wählen Sie die von Ihnen konfigurierte Bereitstellungsgruppe aus. Klicken Sie auf **Edit**.
2. Ziehen Sie im Abschnitt **Apps** die gewünschten Apps in das Feld **Erforderliche Apps**.



3. Klicken Sie auf der Seite **Zusammenfassung** auf **Speichern**.
4. Wählen Sie auf der Seite **Bereitstellungsgruppen** die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.

Unternehmensapps

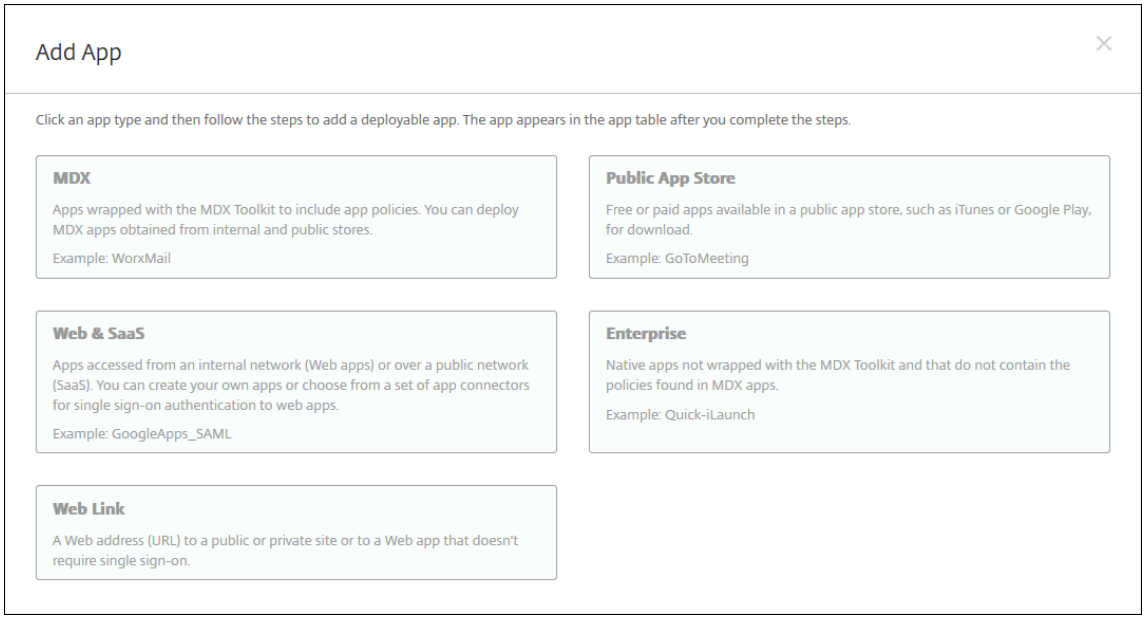
Unternehmensapps stellen private Apps dar, die nicht mit dem MAM-SDK oder MDX Toolkit vorbereitet wurden. Sie entwickeln diese Apps selbst oder beziehen sie direkt aus anderen Quellen. Um eine Unternehmensapp hinzuzufügen, benötigen Sie die mit der App verknüpfte APK-Datei. Befolgen Sie hierbei die Best Practices für private Apps von Google.

Schritt 1: Hinzufügen und Konfigurieren von Apps

Fügen Sie die App hinzu. Hierfür gibt es zwei Möglichkeiten:

- Veröffentlichen Sie die App direkt im verwalteten Google Play Store und fügen Sie sie der XenMobile-Konsole als App aus dem verwalteten Play Store hinzu. Folgen Sie den Angaben in der Google-Dokumentation zum Veröffentlichen privater Apps und führen Sie dann die Schritte im Abschnitt Apps aus dem verwalteten App-Store aus.
- Fügen Sie die App der XenMobile-Konsole als Unternehmensapp hinzu. Führen Sie hierfür die folgenden Schritte aus:

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

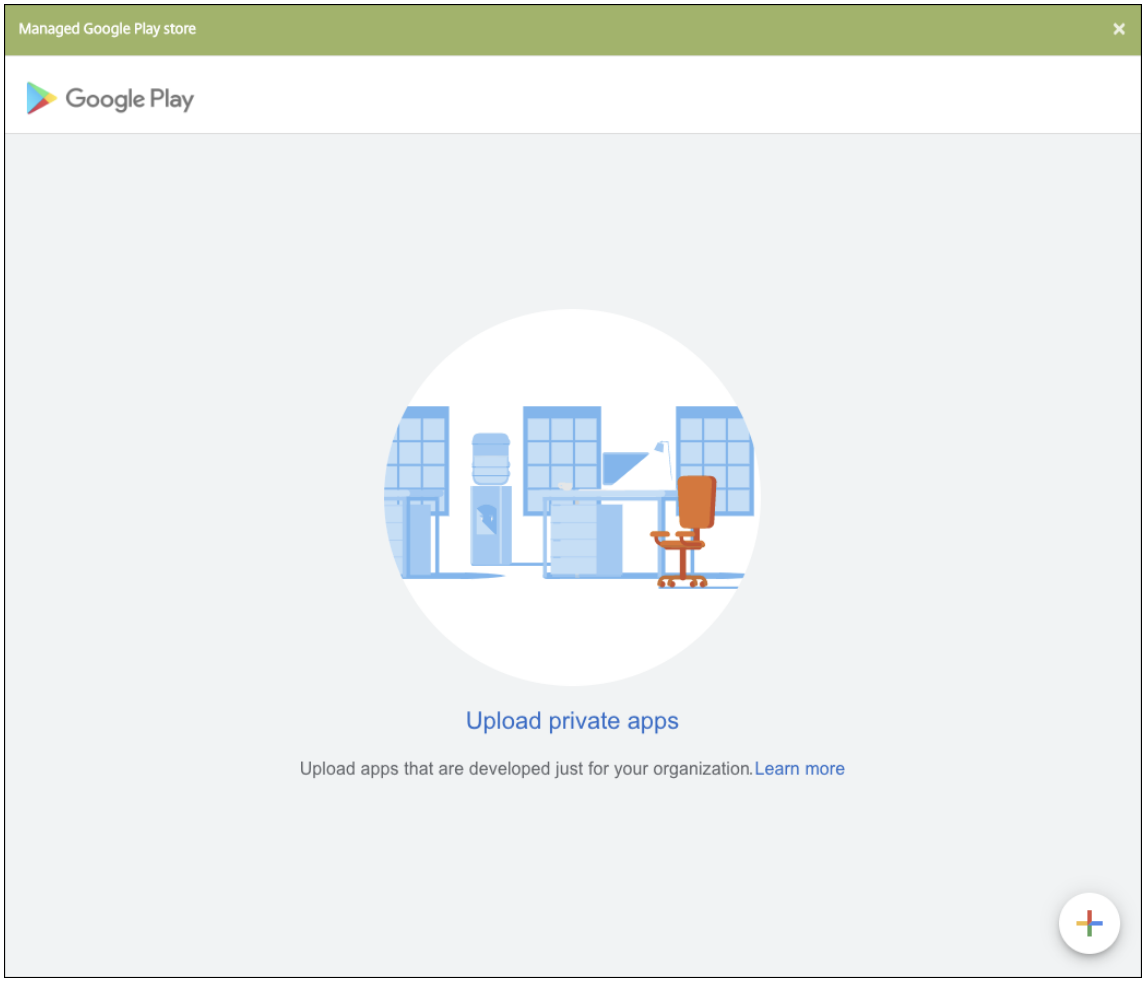


2. Klicken Sie auf **Enterprise**. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:

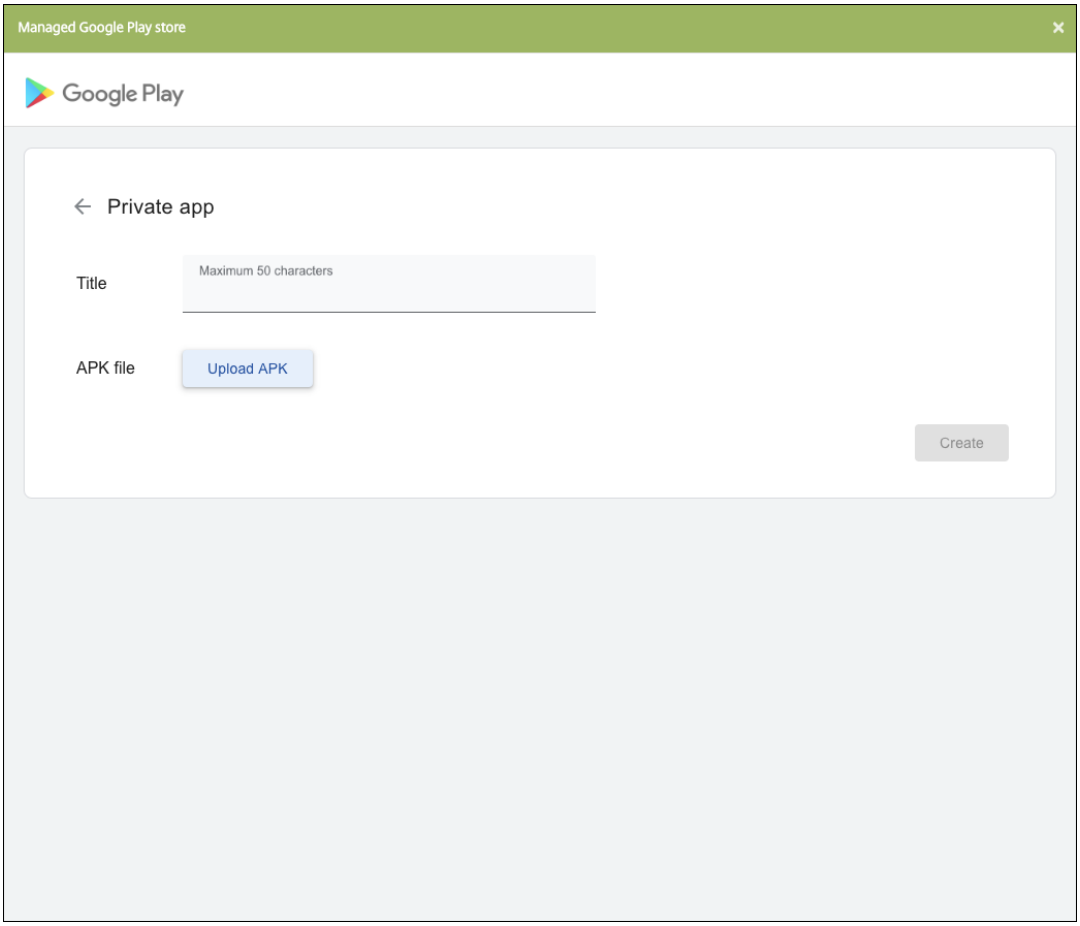
    - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name” in der Tabelle “Apps” angezeigt.
    - **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.

- **App-Kategorie:** Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen möchten. Weitere Informationen zu App-Kategorien finden Sie unter App-Kategorien.

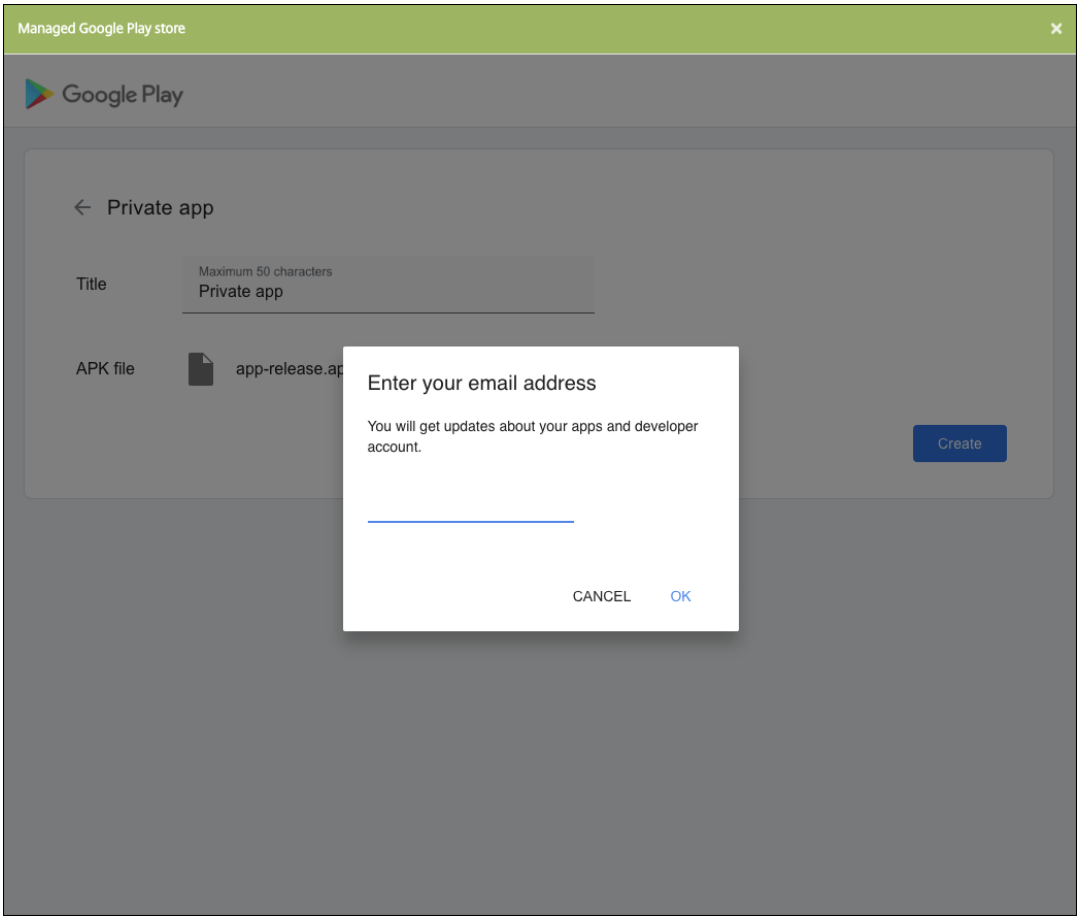
3. Wählen Sie als Plattform **Android Enterprise**.
4. Die Schaltfläche **Upload** öffnet den verwalteten Google Play Store. Sie müssen sich nicht für ein Entwicklerkonto registrieren, um eine private App zu veröffentlichen. Klicken Sie auf das **Plus-Symbol** in der unteren rechten Ecke, um fortzufahren.



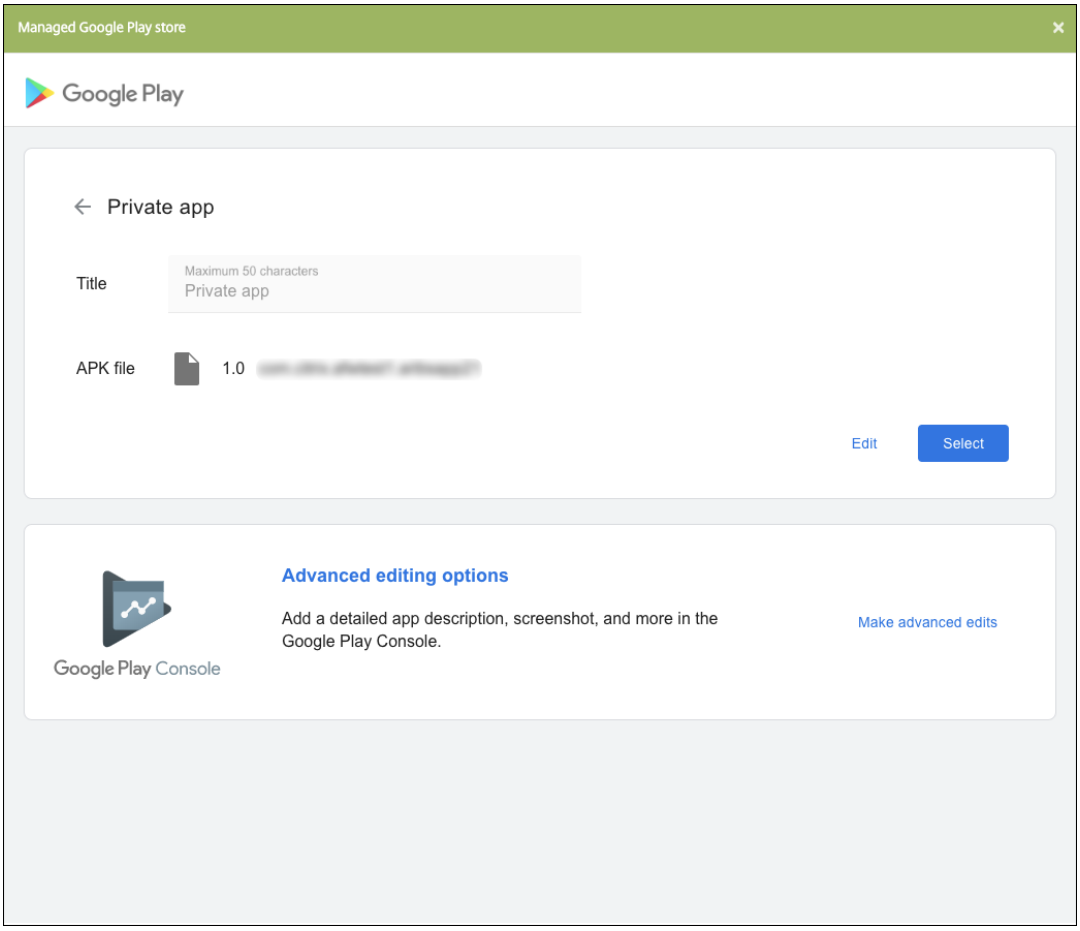
   a) Geben Sie den Namen für Ihre App ein und laden Sie die APK-Datei hoch. Wenn Sie fertig sind, klicken Sie auf **Erstellen**. Es kann bis zu 10 Minuten dauern, bis Ihre private App veröffentlicht wird.



b) Geben Sie eine E-Mail-Adresse ein, um Updates zu Ihren Apps zu erhalten.



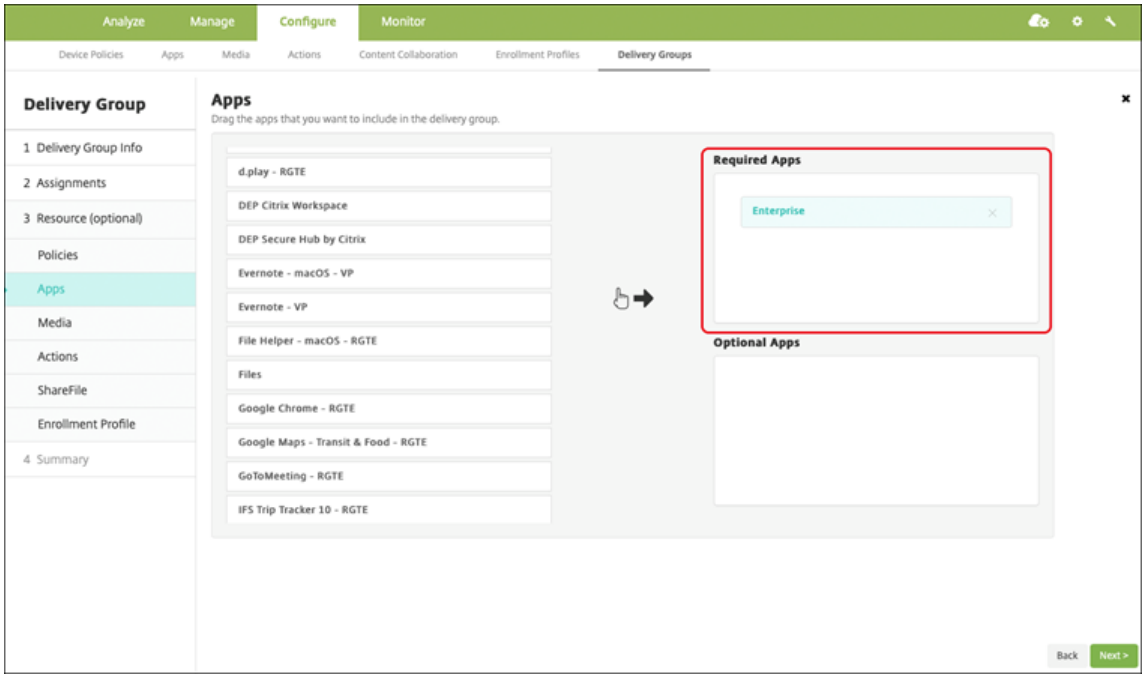
c) Nach dem Veröffentlichen Ihrer App klicken Sie auf das Symbol der privaten App. Um eine App-Beschreibung hinzuzufügen, das App-Symbol zu ändern oder eine andere Aktion auszuführen, klicken Sie auf **Make advanced edits**. Andernfalls klicken Sie auf **Select**, um die App-Informationsseite zu öffnen.



5. Klicken Sie auf **Weiter**. Die Seite mit den App-Informationen für die Plattform wird angezeigt.
6. 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.
   - **Paket-ID:** Eindeutige Kennung Ihrer App.
   - **OS-Version (Minimum):** Geben Sie optional die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
   - **OS-Version (Maximum):** Geben Sie optional 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.
7. Konfigurieren Sie Bereitstellungsregeln und Storekonfiguration.
8. Weisen Sie der App beliebige Bereitstellungsgruppen zu und klicken Sie auf **Speichern**. Informationen finden Sie unter Bereitstellen von Ressourcen.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen** und wählen Sie die von Ihnen konfigurierte Bereitstellungsgruppe aus. Klicken Sie auf **Edit**.
2. Ziehen Sie im Abschnitt **Apps** die gewünschten Apps in das Feld **Erforderliche Apps**.



3. Klicken Sie auf der Seite **Zusammenfassung** auf **Speichern**.
4. Wählen Sie auf der Seite **Bereitstellungsgruppen** die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.

MDX-fähige private Apps

Hinzufügen von Android Enterprise-Apps als MDX-fähige Unternehmensapps:

1. Erstellen Sie eine private Android Enterprise-App und machen Sie sie MDX-fähig.
2. Fügen Sie die App der XenMobile-Konsole hinzu.
   - Hosten und veröffentlichen Sie die Apps im verwalteten Google Play Store.
   - Fügen Sie die App der XenMobile-Konsole als Unternehmensapp hinzu.
3. Fügen Sie die MDX-Datei zu XenMobile hinzu.

Wenn Sie Apps über den Google Play Store hosten und veröffentlichen möchten, wählen Sie nicht die Signatur mit Google-Zertifikat. Signieren Sie die App mit demselben Zertifikat, das verwendet wurde, um die App MDX-fähig zu machen. Weitere Informationen zum Veröffentlichen von Apps finden Sie in der Google-Dokumentation zum Veröffentlichen Ihrer App und Signieren Ihrer App. Das MAM-SDK umschließt Apps nicht und erfordert daher nur das Zertifikat, das für die Entwicklung der App verwendet wurde.

Weitere Informationen zum Veröffentlichen privater Apps über die Google Play-Konsole finden Sie in der Google-Dokumentation zum Veröffentlichen privater Apps über die Google Play-Konsole.

Informationen zum Veröffentlichen einer App über XenMobile finden Sie in den folgenden Abschnitten.

Vorbereiten einer privaten Android Enterprise-App

Wenn Sie eine private Android Enterprise-App erstellen, beachten Sie die Hinweise von Google unter Best practices for private apps.

Nachdem Sie eine private Android Enterprise-App erstellt haben, integrieren Sie das MAM-SDK in die App oder umschließen die App mit dem MDX Toolkit. Fügen Sie dann die erstellten Dateien XenMobile hinzu.

Zum Aktualisieren der App laden Sie eine aktualisierte APK-Datei hoch. Mit den folgenden Schritten umschließen Sie Apps mit dem MDX Toolkit.

1. Erstellen Sie Ihre private Android Enterprise-App und generieren Sie eine signierte APK-Datei.
2. Die folgende Beispieldatei enthält alle bekannten Richtlinien, von denen einige möglicherweise nicht für Ihre Umgebung gelten. Alle nicht verwendeten Einstellungen werden ignoriert. Erstellen Sie eine XML-Datei mit den folgenden Parametern:

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
            NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
        <AllowedWifiNetworks/>
        <UpgradeGracePeriod>168</UpgradeGracePeriod>
        <WipeDataOnAppLock>false</WipeDataOnAppLock>
```



```
22          <ActivePollPeriod>60</ActivePollPeriod>
23          <PublicFileAccessLimitsList/>
24          <CutAndCopy>Unrestricted</CutAndCopy>
25          <Paste>Unrestricted</Paste>
26          <DocumentExchange>Unrestricted</DocumentExchange>
27          <OpenInExclusionList/>
28          <InboundDocumentExchange>Unrestricted</
               InboundDocumentExchange>
29          <InboundDocumentExchangeWhitelist/>
30          <connectionSecurityLevel>TLS</connectionSecurityLevel>
31          <DisableCamera>false</DisableCamera>
32          <DisableGallery>false</DisableGallery>
33          <DisableMicrophone>false</DisableMicrophone>
34          <DisableLocation>false</DisableLocation>
35          <DisableSms>false</DisableSms>
36          <DisableScreenCapture>false</DisableScreenCapture>
37          <DisableSensor>false</DisableSensor>
38          <DisableNFC>false</DisableNFC>
39          <BlockLogs>false</BlockLogs>
40          <DisablePrinting>false</DisablePrinting>
41          <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
               MvpnNetworkAccess>
42          <MvpnSessionRequired>False</MvpnSessionRequired>
43          <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44          <DisableLocalhostConnections>false</
               DisableLocalhostConnections>
45          <CertificateLabel/>
46          <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47          <DefaultLoggerLevel>15</DefaultLoggerLevel>
48          <MaxLogFiles>2</MaxLogFiles>
49          <MaxLogFileSize>2</MaxLogFileSize>
50          <RedirectSystemLogs>false</RedirectSystemLogs>
51          <EncryptLogs>false</EncryptLogs>
52          <GeofenceLongitude>0</GeofenceLongitude>
53          <GeofenceLatitude>0</GeofenceLatitude>
54          <GeofenceRadius>0</GeofenceRadius>
55          <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56          <Authentication>OfflineAccessOnly</Authentication>
57          <ReauthenticationPeriod>480</ReauthenticationPeriod>
58          <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59      </Policies>
60  </MobileAppPolicies>
61  <!--NeedCopy-->
```

3. Umschließen Sie die App mit dem MDX Toolkit. Informationen zur Verwendung des MDX Toolkits

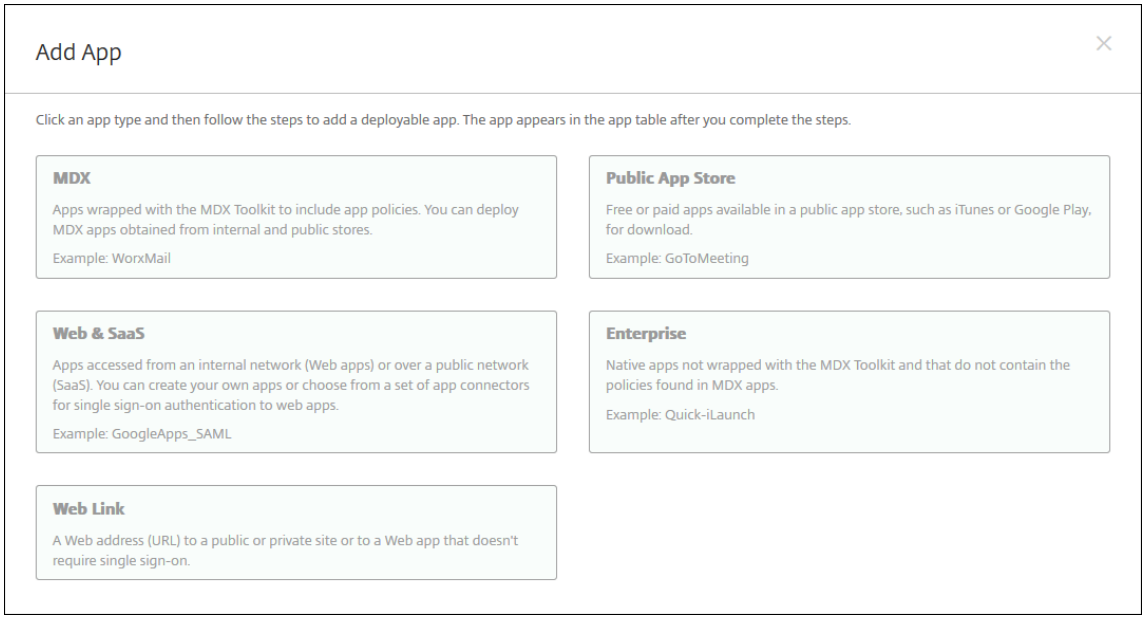
finden Sie unter Umschließen von mobilen Android-Apps.

Setzen Sie den Parameter **apptype** auf **Premium**. Verwenden Sie die XML-Datei aus dem vorherigen Schritt im nachfolgend beschriebenen Befehl.

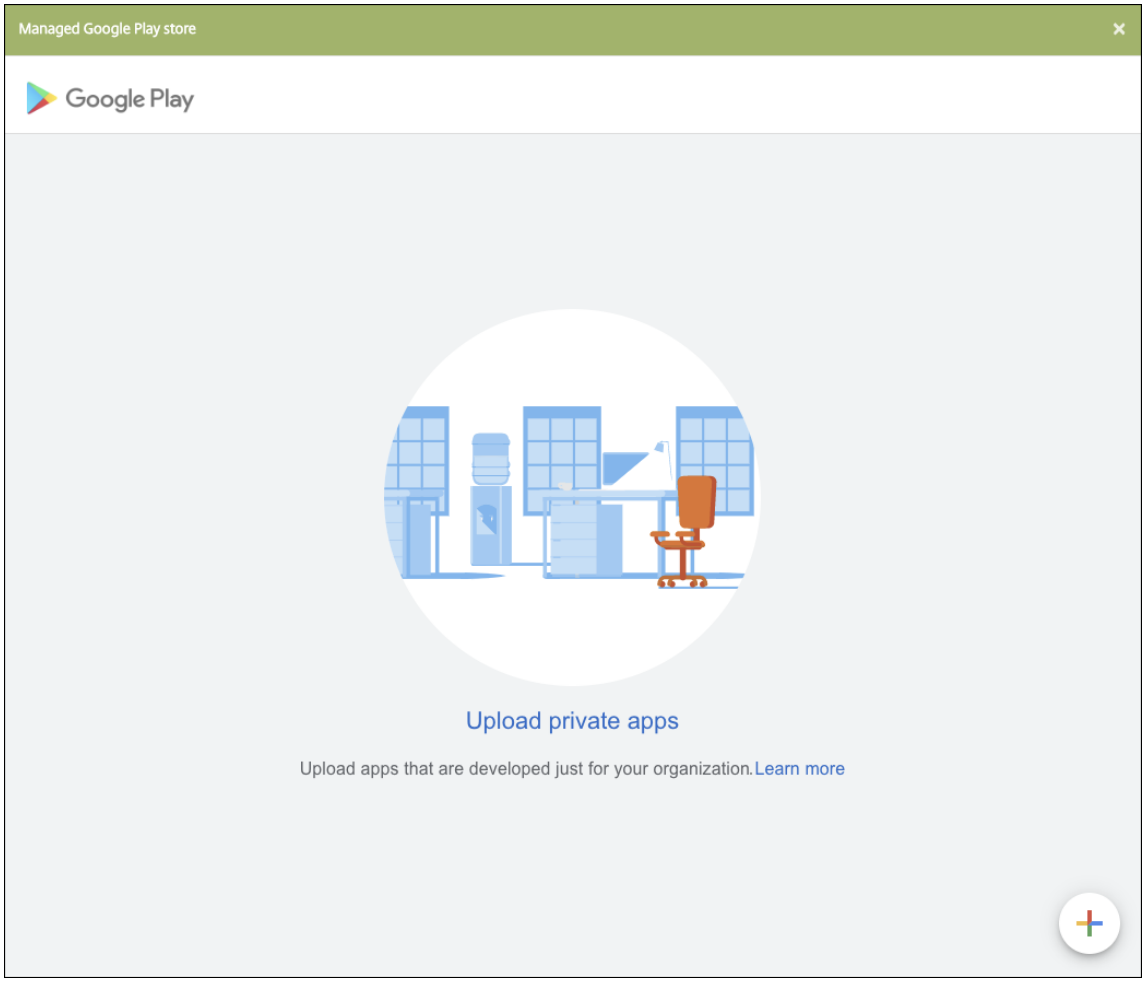
Wenn Sie die Store-URL für die App kennen, legen Sie den Parameter **storeURL** auf diese Store-URL fest. Benutzer laden die veröffentlichte App von der Store-URL herunter.

In diesem Beispiel wird ein MDX Toolkit-Befehl zum Umschließen der App "SampleAEapp" verwendet:

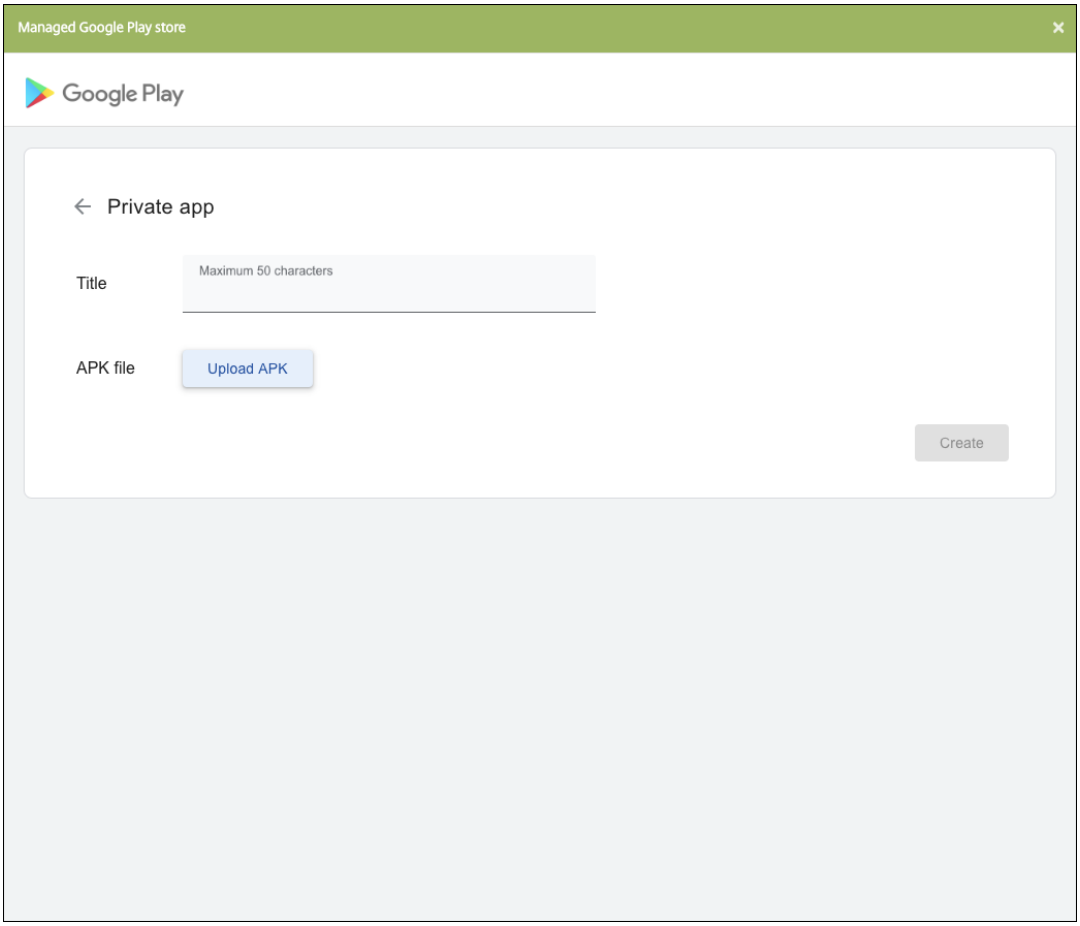
```
```
 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
    Duser.variant
 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
 -MinPlatform 5.0
 -keystore /MyKeystore
 -storepass mystorepwd123
 -keyalias key0
 -keypass mykeypwd123
 -storeURL "https://play.google.com/store/apps/details?id=
    SampleAEappPackage"
 -appType Premium
 -premiumMdxPolicies <Path to Premium policy XML>
<!--NeedCopy--> ```
```

Durch Umschließen der App werden eine umschlossene APK-Datei und eine MDX-Datei generiert.

#### Hinzufügen der umschlossenen APK-Datei

Fügen Sie die App hinzu. Hierfür gibt es zwei Möglichkeiten:

- Veröffentlichen Sie die App direkt im verwalteten Google Play Store und fügen Sie sie der XenMobile-Konsole als App aus dem verwalteten Play Store hinzu. Folgen Sie den Angaben in der Google-Dokumentation zum Veröffentlichen privater Apps und führen Sie dann die Schritte im Abschnitt Apps aus dem verwalteten App-Store aus.
- Fügen Sie die App der XenMobile-Konsole als Unternehmensapp hinzu. Führen Sie hierfür die folgenden Schritte aus:

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.

 
```



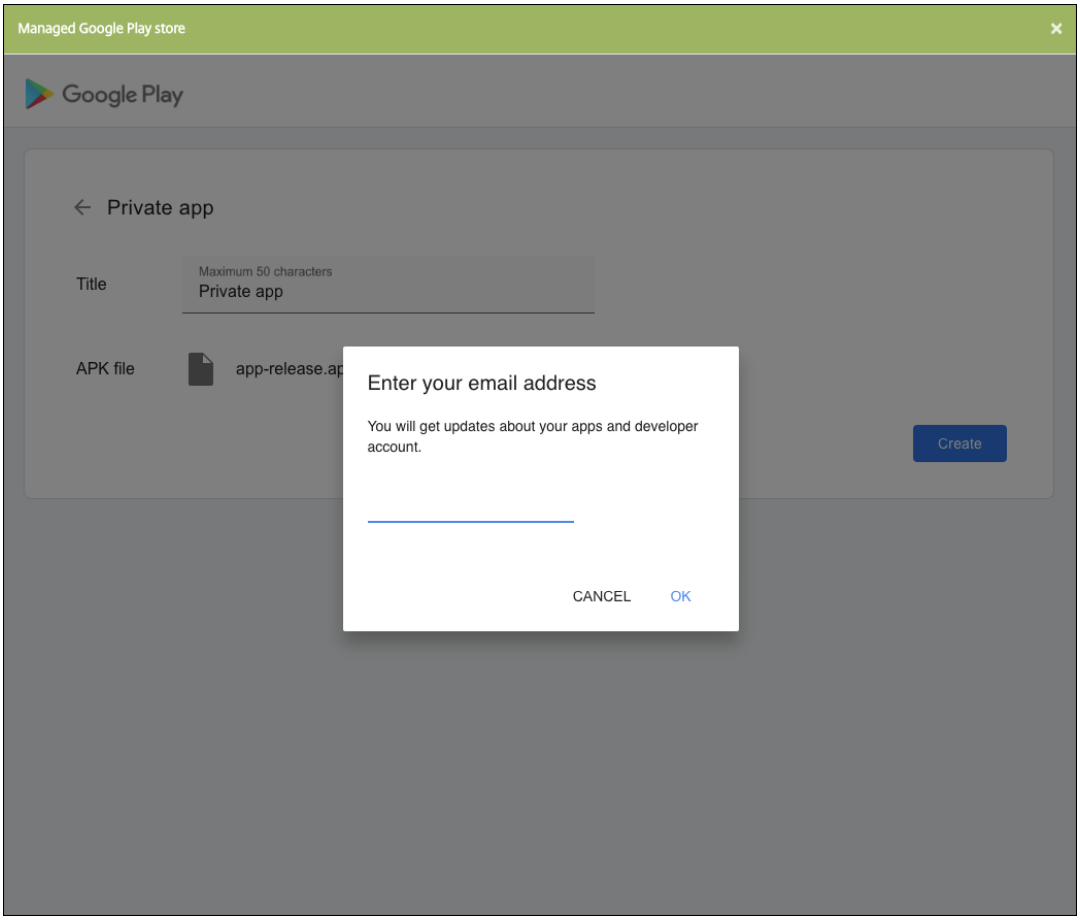
3. Klicken Sie auf **Enterprise**. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name” in der Tabelle “Apps” angezeigt.
   - **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.
   - **App-Kategorie:** Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen möchten. Weitere Informationen zu App-Kategorien finden Sie unter App-Kategorien.
4. Wählen Sie als Plattform **Android Enterprise**.
5. Die Schaltfläche **Upload** öffnet den verwalteten Google Play Store. Sie müssen sich nicht für ein Entwicklerkonto registrieren, um eine private App zu veröffentlichen. Klicken Sie auf das **Plus-Symbol** in der unteren rechten Ecke, um fortzufahren.



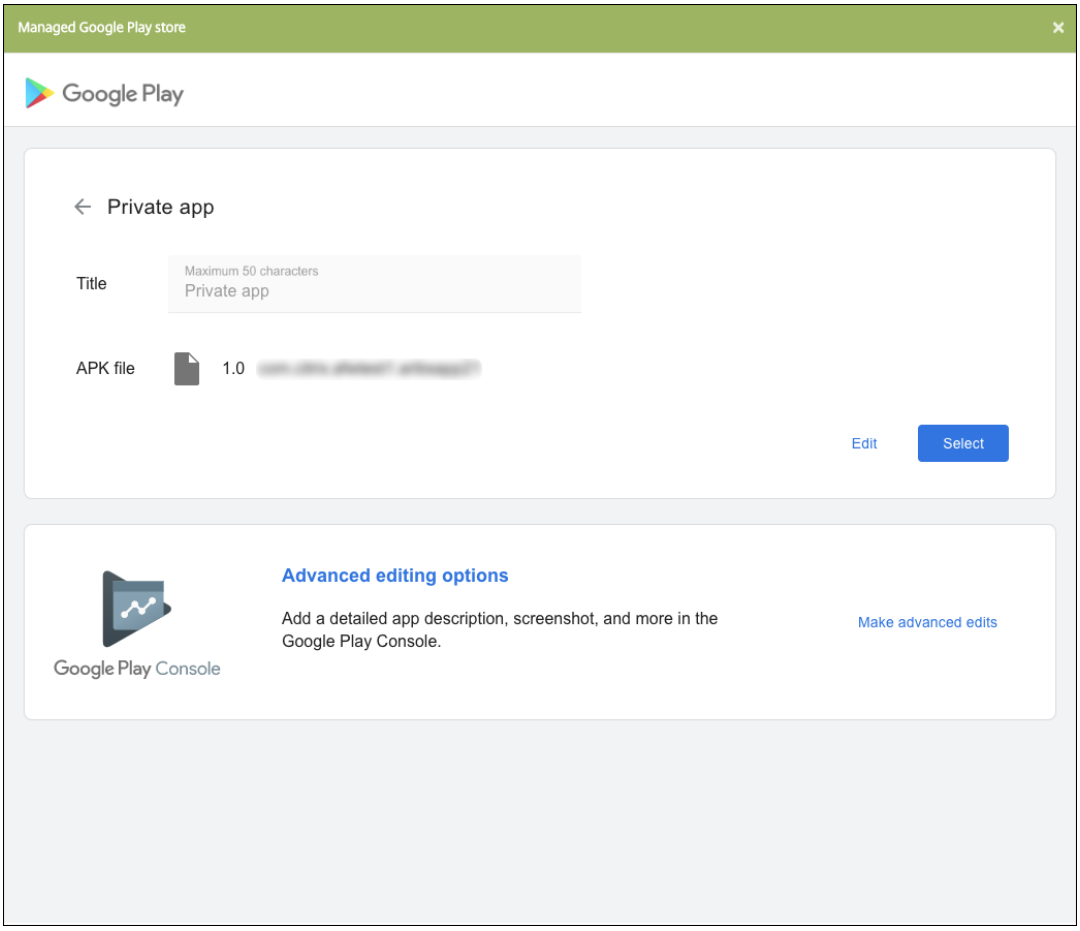
a) Geben Sie den Namen für Ihre App ein und laden Sie die APK-Datei hoch. Wenn Sie fertig sind, klicken Sie auf **Erstellen**. Es kann bis zu 10 Minuten dauern, bis Ihre private App veröffentlicht wird.



b) Geben Sie eine E-Mail-Adresse ein, um Updates zu Ihren Apps zu erhalten.



c) Nachdem Ihre App veröffentlicht wurde, klicken Sie auf das Symbol der privaten App und dann auf **Auswählen**, um die App-Informationsseite zu öffnen.



6. Klicken Sie auf **Weiter**. Die Seite mit den App-Informationen für die Plattform wird angezeigt.
7. 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.
   - **Paket-ID:** Eindeutige Kennung Ihrer App.
   - **OS-Version (Minimum):** Geben Sie optional die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
   - **OS-Version (Maximum):** Geben Sie optional 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.
8. Konfigurieren Sie Bereitstellungsregeln und Storekonfiguration.
9. Klicken Sie auf der Seite **Android Enterprise-Unternehmensapp** auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.

   Informationen zum Verwenden von Workflows für die Anforderung einer Genehmigung vor

dem App-Zugriff durch Benutzer finden Sie unter Anwenden von Workflows. Wenn Sie keinen Genehmigungsworkflow benötigen, fahren Sie mit Schritt 13 fort.

10. Klicken Sie auf **Weiter**.
11. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt. Auf dieser Seite ist keine Aktion erforderlich. Sie konfigurieren die Bereitstellungsgruppen und den Bereitstellungszeitplan für die App beim Hinzufügen der MDX-Datei. Klicken Sie auf **Speichern**.

Optional: Hinzufügen oder Ändern der Store-URL

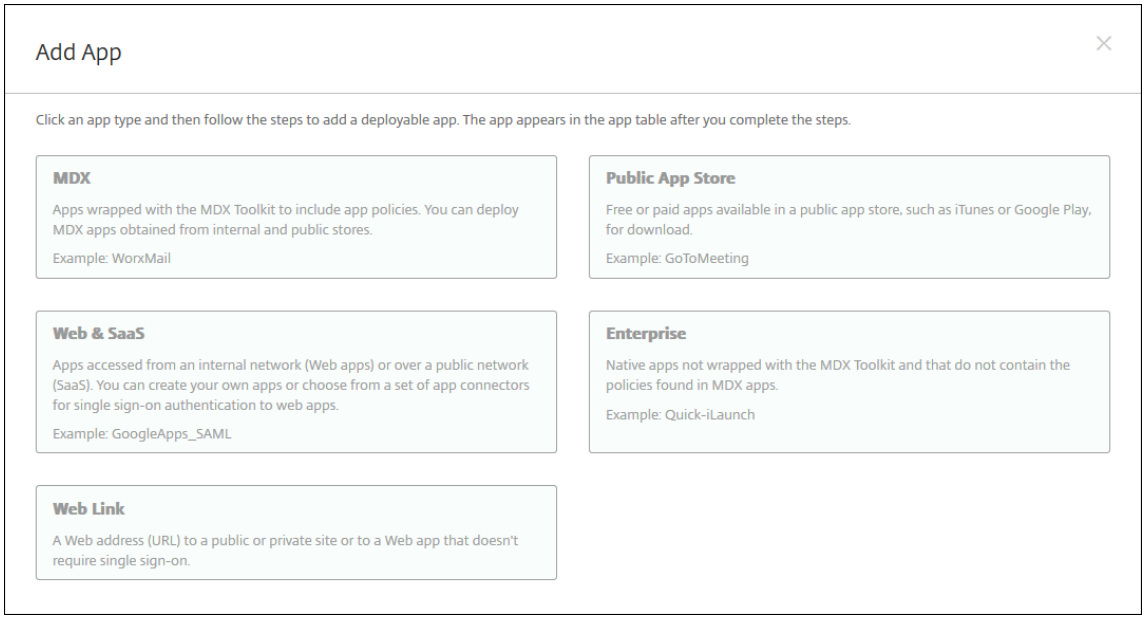
Wenn Sie die Store-URL beim Umschließen der App nicht kennen, fügen Sie sie jetzt hinzu.

1. Zeigen Sie die App im verwalteten Google Play Store an. Beim Auswählen der App wird die Store-URL in der Adressleiste des Browsers angezeigt. Kopieren Sie den Paketnamen der App aus dem URL-Formular. Beispiel: `https://play.google.com/store/apps/details?id=SampleAEappPackage`. Die URL, die Sie kopieren, beginnt vielleicht mit `https://play.google.com/work/`. Stellen Sie sicher, dass Sie `work` in `store` ändern.
2. Fügen Sie die Store-URL mit dem MDX Toolkit zur MDX-Datei hinzu:

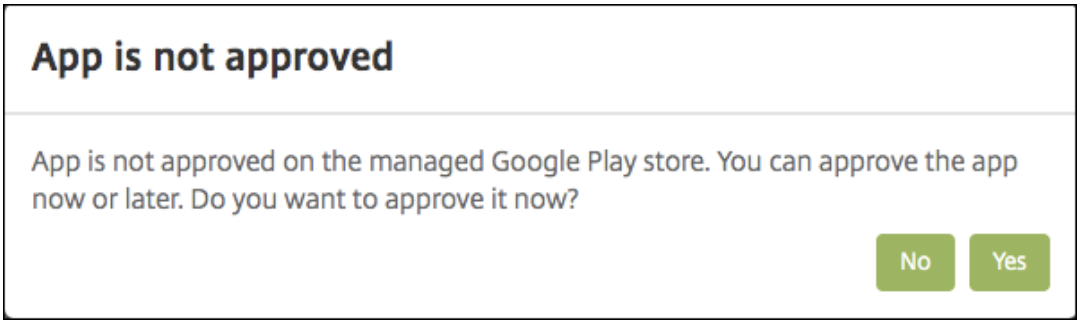
```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
   SampleAEappPackage"
<!--NeedCopy-->
```

Hinzufügen der MDX-Datei

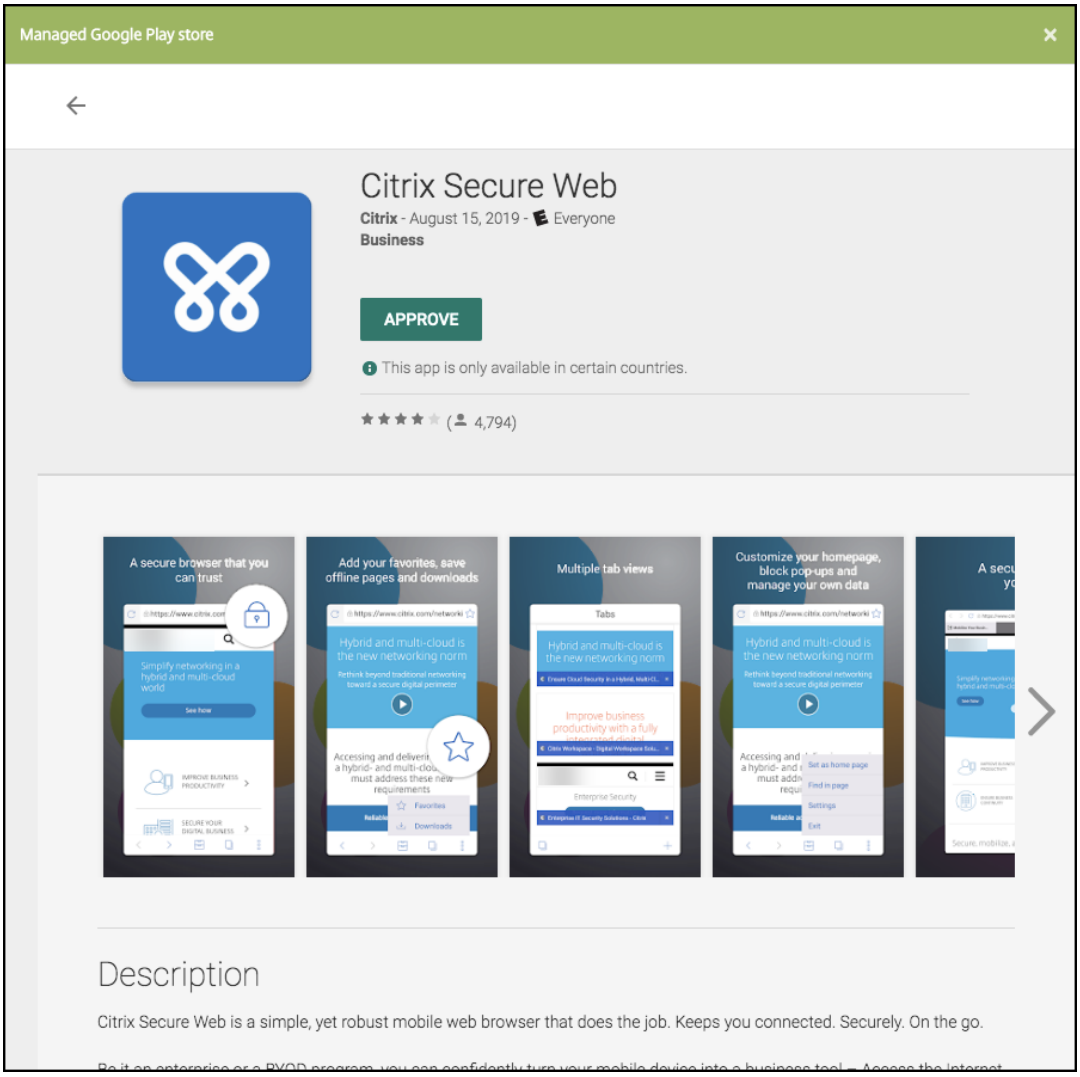
1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



2. Klicken Sie auf **MDX**. Die Seite **App-Informationen** für MDX wird angezeigt. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** 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 zu App-Kategorien finden Sie unter App-Kategorien.
3. Wählen Sie als Plattform **Android Enterprise**.
4. Klicken Sie auf **Upload** und navigieren Sie zur MDX-Datei. Android Enterprise unterstützt nur mit dem MDX Toolkit umschlossene Apps.
   - Es wird eine Meldung angezeigt, wenn die angehängte Anwendung eine Genehmigung des verwalteten Google Play-Store erfordert. Klicken Sie auf **Ja**, um die Anwendung zu genehmigen, ohne die XenMobile-Konsole zu verlassen.



Sobald der verwaltete Google Play Store geöffnet ist, folgen Sie den Anweisungen, um die App zu genehmigen und zu speichern.



Wenn Sie die App erfolgreich hinzufügen, wird die Seite **App-Detail** angezeigt.

5. Konfigurieren Sie folgende 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.
- **Paket-ID:** Geben Sie die Paket-ID für die App ein, die Sie aus dem verwalteten Google Play Store erhalten haben.
- **OS-Version (Minimum):** Geben Sie optional die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
- **OS-Version (Maximum):** Geben Sie optional 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.

6. Konfigurieren Sie die **MDX-Richtlinien**. MDX-Richtlinien variieren je nach Plattform und bieten Optionen für Richtlinienbereiche wie Authentifizierung, Gerätesicherheit und App-Einschränkungen. In der Konsole kann eine QuickInfo mit einer Beschreibung der Richtlinien angezeigt werden. Informationen über die für die einzelnen Geräteplattformen verfügbaren App-Richtlinien finden Sie hier:

   - Überblick über das MAM-SDK
   - MDX-Richtlinien für Drittanbieter-Apps auf einen Blick

7. Konfigurieren Sie Bereitstellungsregeln und Storekonfiguration.

   Die Option **Bereitstellen für immer aktive Verbindungen** gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.

   Die Option “Always-On”:

   - Ist nicht verfügbar für Kunden, die Android Enterprise sowie Endpoint Management in einer Version ab 10.18.19 verwenden
   - Wird nicht empfohlen für Kunden, die Android Enterprise sowie Endpoint Management in einer Version vor 10.18.19 verwenden

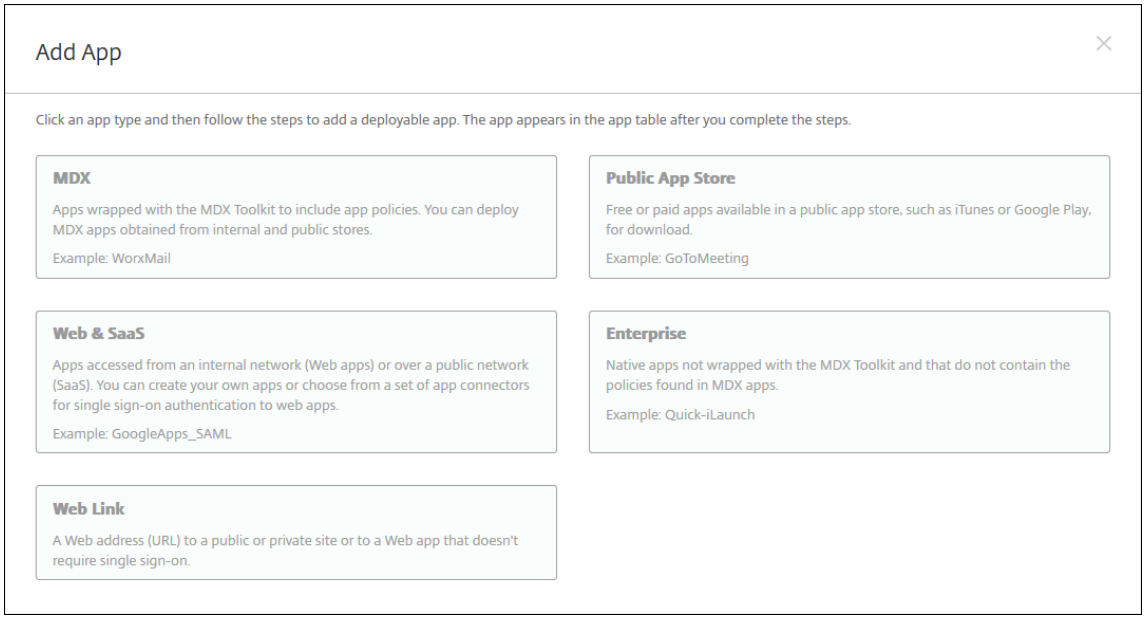
   Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

8. Weisen Sie der App beliebige Bereitstellungsgruppen zu und klicken Sie auf **Speichern**. Informationen finden Sie unter Bereitstellen von Ressourcen.

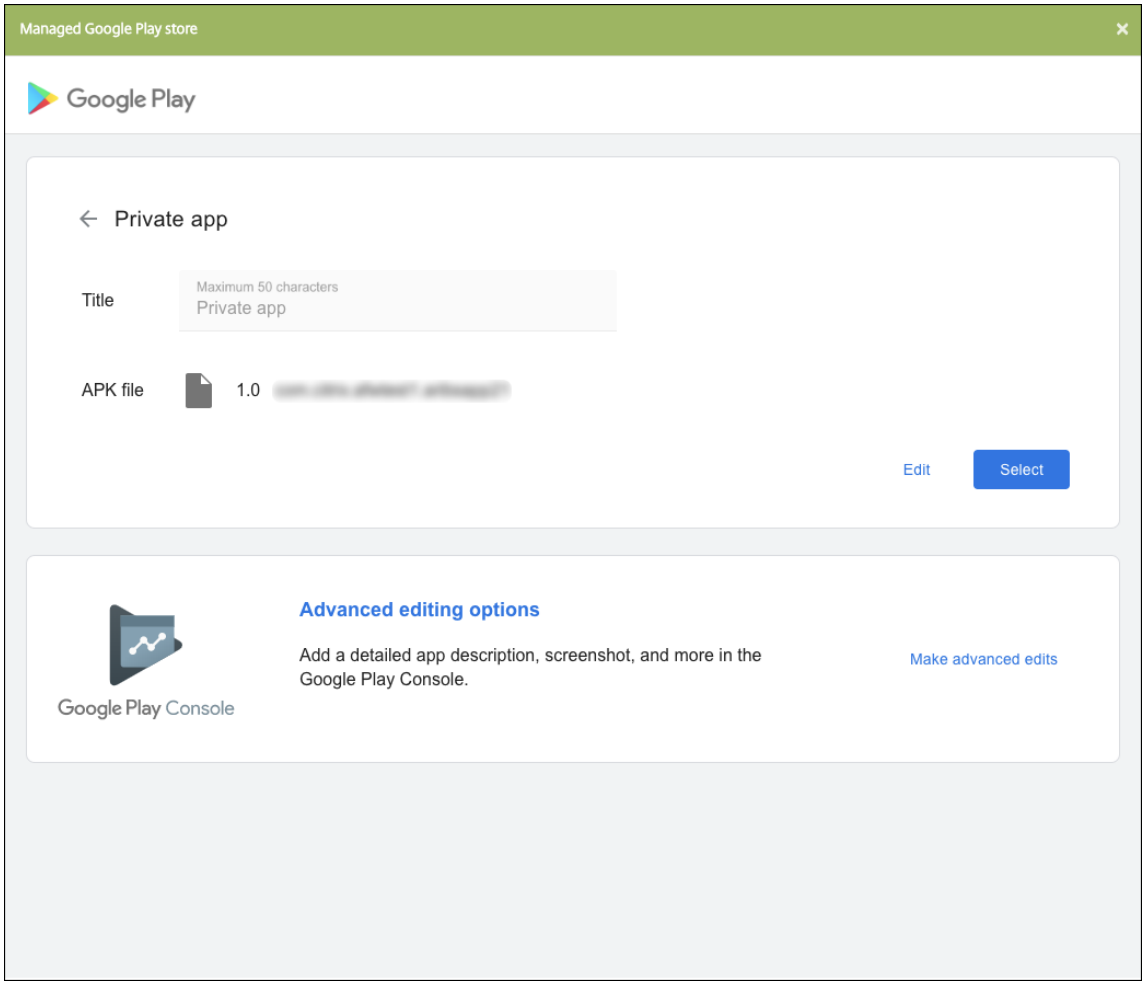
Aktualisieren der App

Zum Aktualisieren der Android Enterprise-App müssen Sie eine aktualisierte APK-Datei umschließen und hochladen:

1. Umschließen Sie die APK-Datei für die aktualisierte App mit dem MAM-SDK oder MDX Toolkit.
2. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps**. Die Seite **Apps** wird geöffnet.



3. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.
4. Klicken Sie auf **Enterprise**. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name” in der Tabelle “Apps” 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 zu App-Kategorien finden Sie unter App-Kategorien.
5. Wählen Sie als Plattform **Android Enterprise**.
6. Klicken Sie auf **Weiter**. Die Seite **Android Enterprise-Unternehmensapp** wird angezeigt.
7. Klicken Sie auf **Upload**.
8. Wählen Sie die zu aktualisierende App auf der Seite des verwalteten Google Play Store aus.
9. Klicken Sie auf der Seite der App-Informationen neben dem APK-Dateinamen auf **Bearbeiten**.



10. Navigieren Sie zur neuen APK-Datei und laden Sie sie hoch.
11. Klicken Sie auf der Seite des verwalteten Google Play Store auf **Speichern**.

Kunden mit Legacy Android Enterprise für Google Workspace (ehemals G Suite)

January 5, 2022

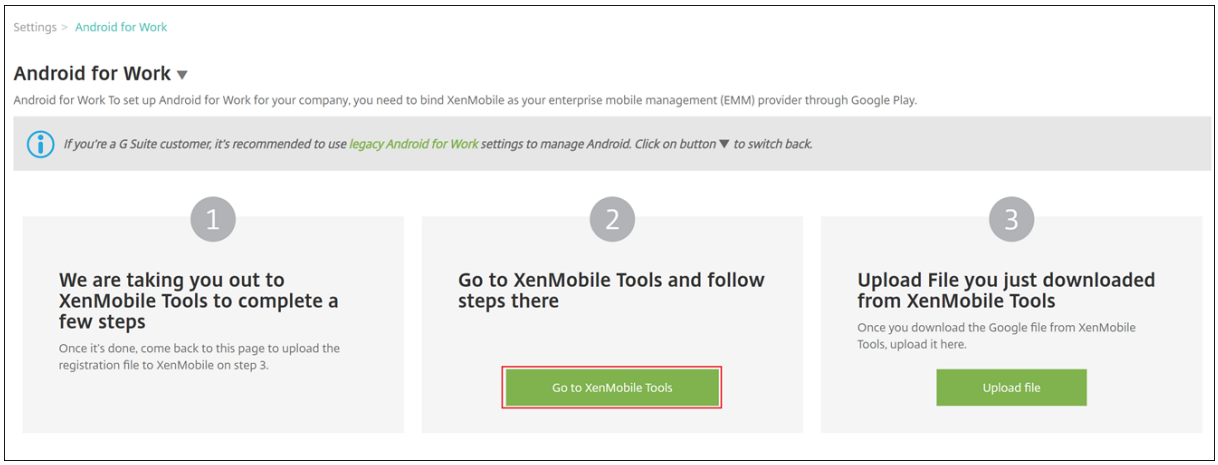
Kunden mit Google Workspace (ehemals G Suite) müssen die Legacy Android Enterprise-Einstellungen zum Konfigurieren von Legacy Android Enterprise verwenden.

Anforderungen für Legacy Android Enterprise:

- 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
- Arbeitsprofil auf den Geräten eingerichtet

Um die Legacy Android Enterprise zu konfigurieren, klicken Sie in den XenMobile-Einstellungen auf der Seite **Android Enterprise** auf **Legacy Android Enterprise** .



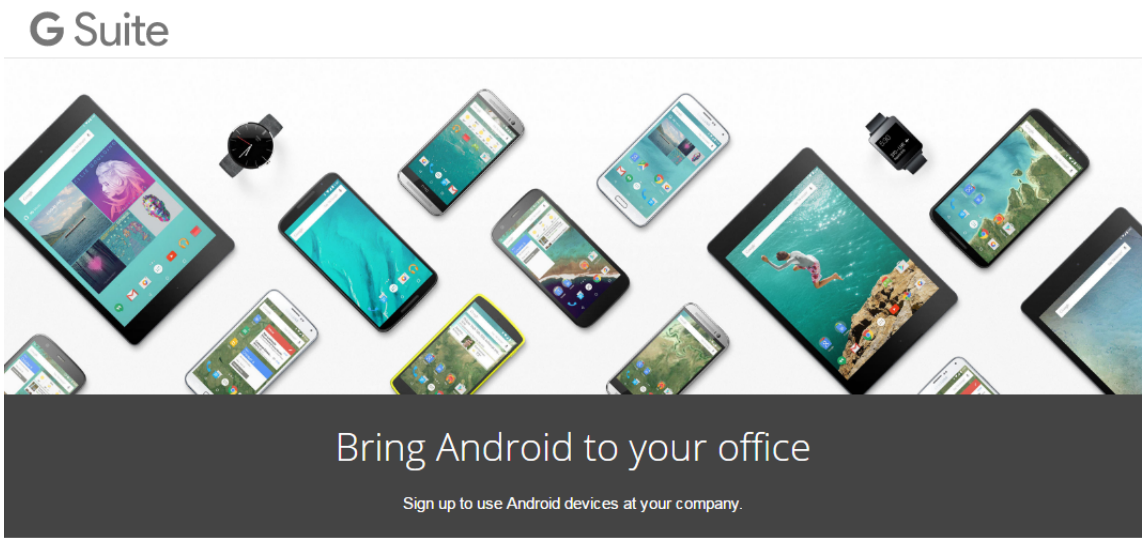
Erstellen eines Android Enterprise-Kontos

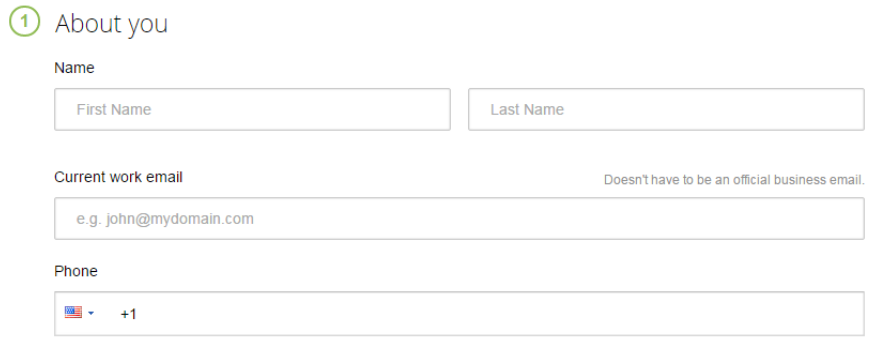
Bevor Sie ein Android Enterprise-Konto einrichten können, müssen Sie Ihren Domainnamen bei Google bestätigen.

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

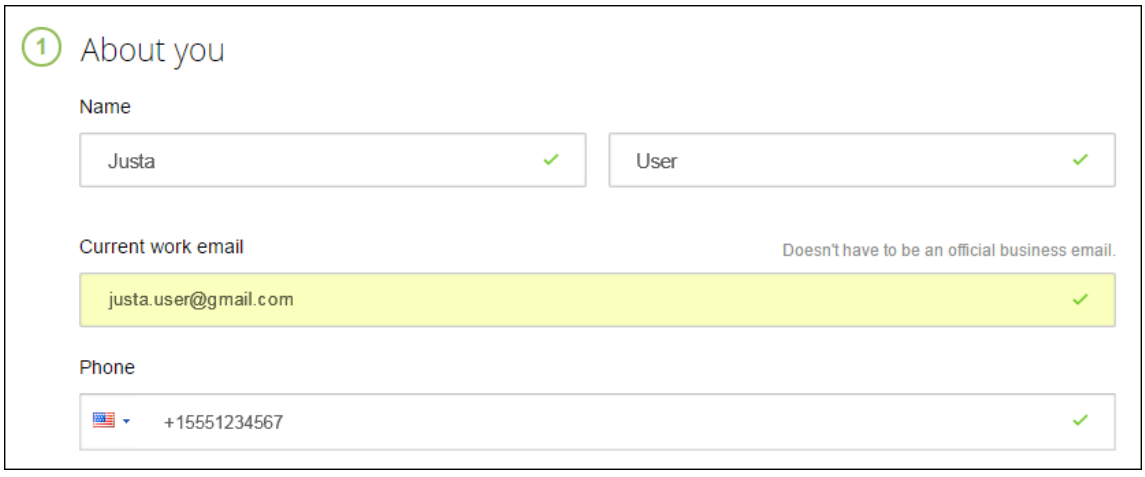
1. Navigieren Sie zu https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

   Auf der nachfolgend gezeigten Seite geben Sie die Administrator- und Unternehmensinformationen ein.

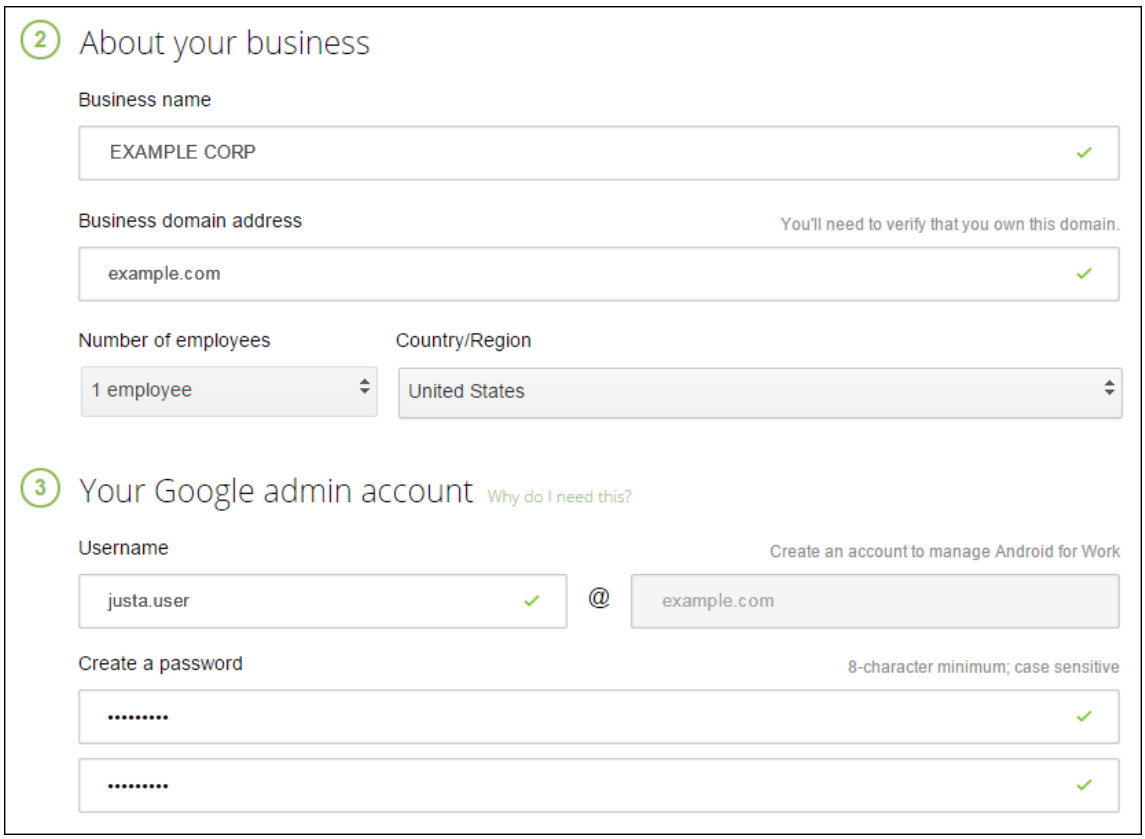




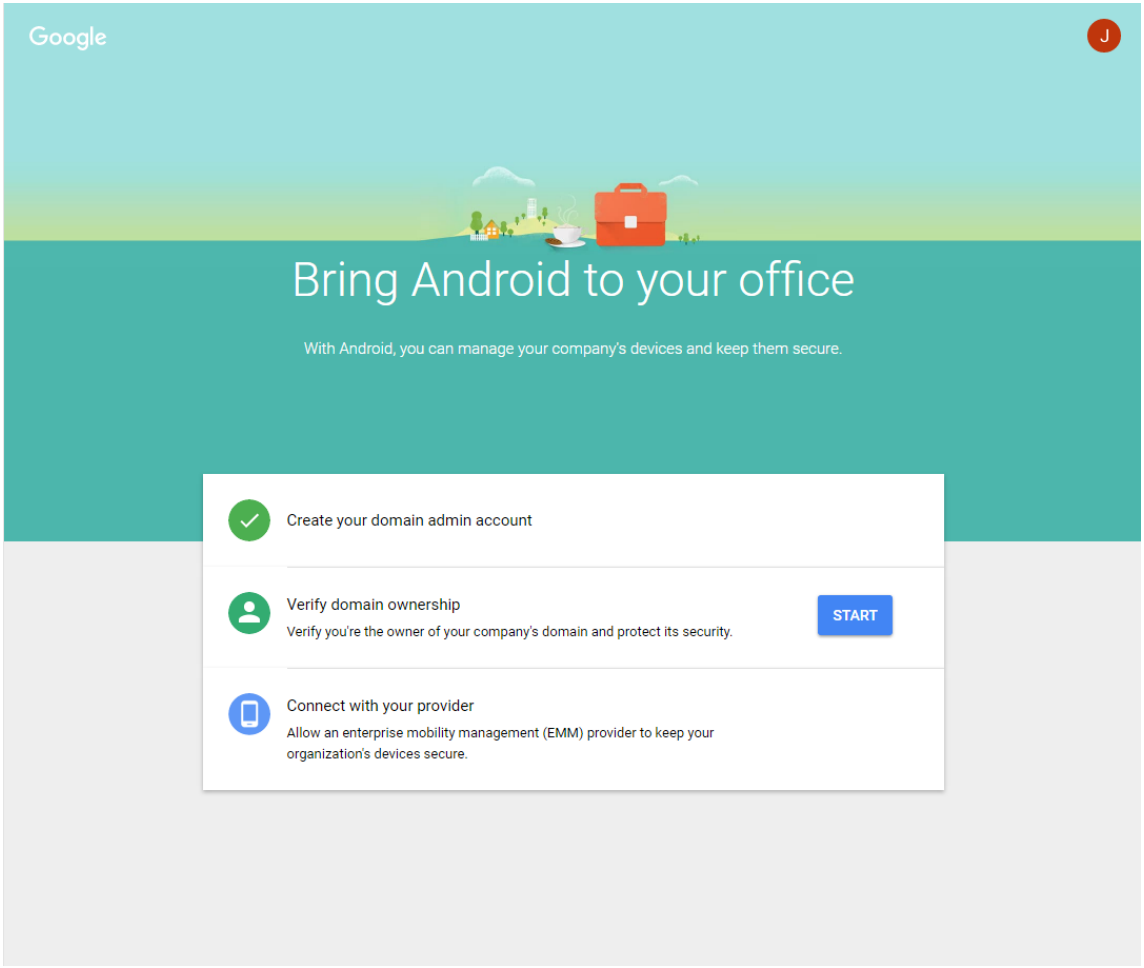
2. Geben Sie Ihre Administratorinformationen ein.



3. 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

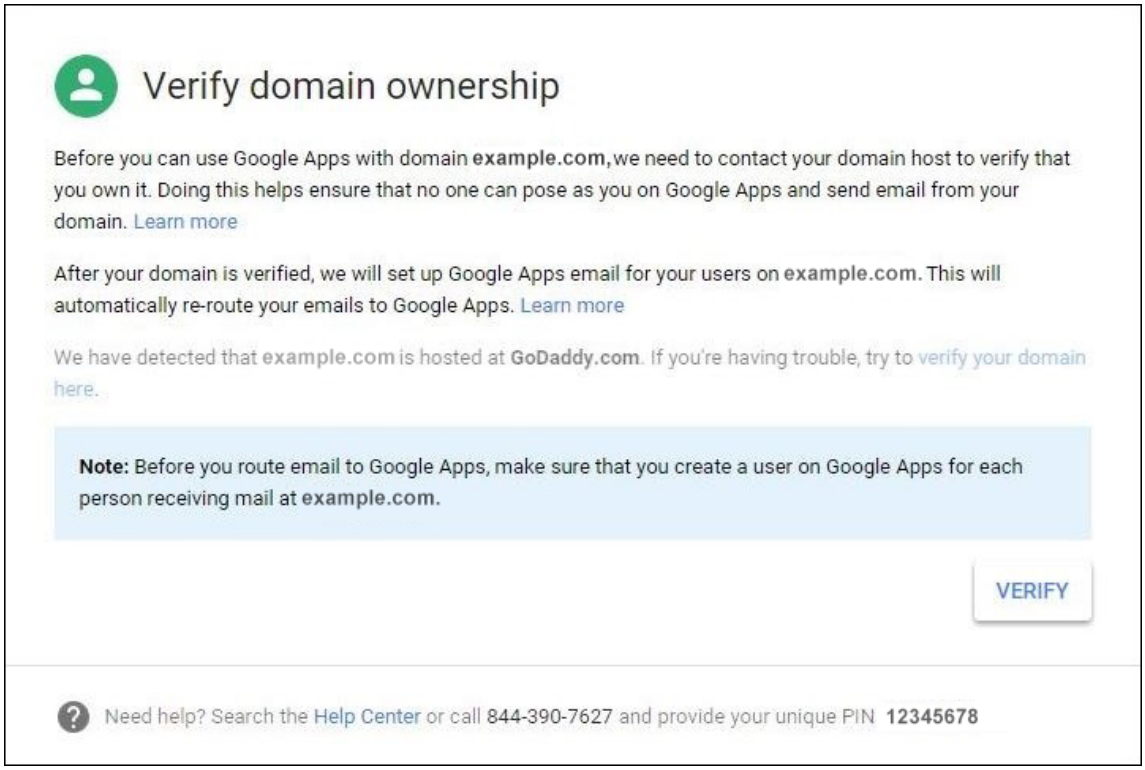
Zur Verifizierung Ihrer Domäne durch Google gibt es folgende Methoden:

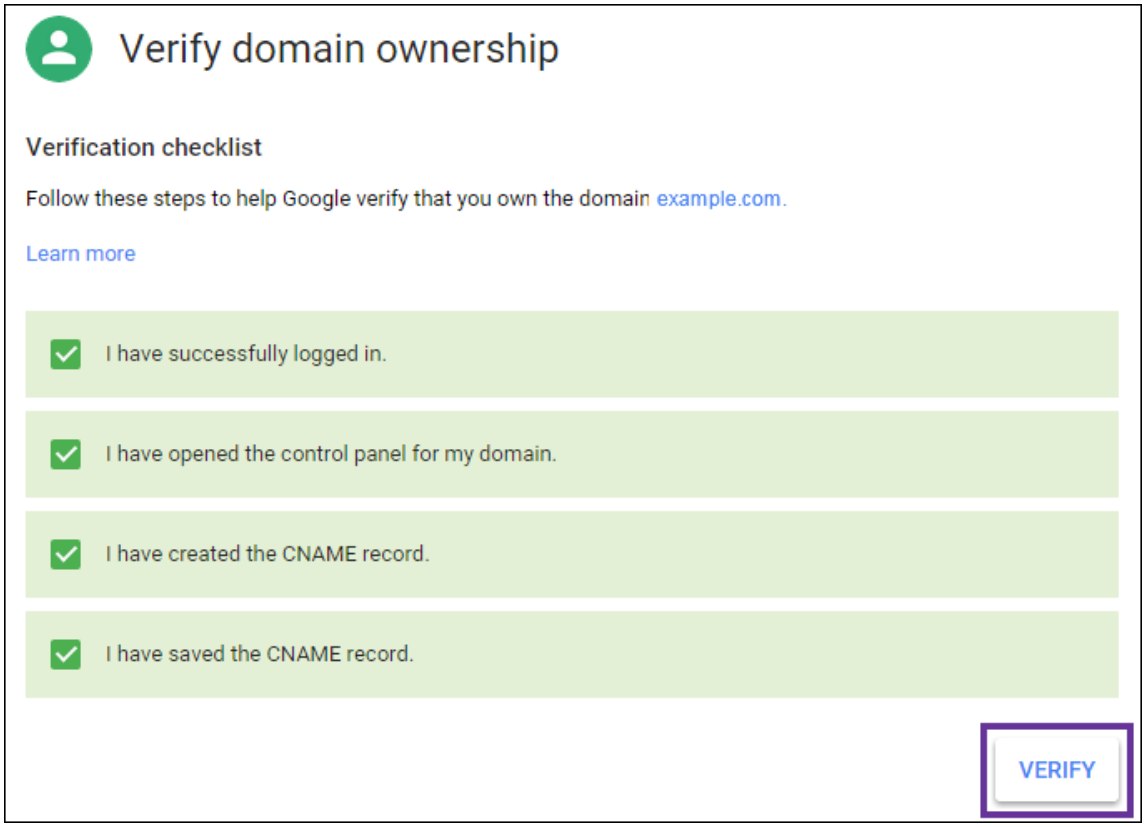
- Hinzufügen eines TXT- oder CNAME-Datensatzes zu der Website Ihres Domänenhosts.
- Hochladen einer HTML-Datei auf den Webserver Ihrer Domäne.
- Hinzufügen eines `<meta>`-Tags zu Ihrer Homepage. Google empfiehlt die Verwendung der ersten Methode. Die Schritte zum Überprüfen Ihrer Domäneneigentümerschaft werden in diesem Artikel nicht behandelt, Informationen finden Sie unter https://support.google.com/a/answer/6248925.

1. Klicken Sie auf **Start**, um die Domänenüberprüfung zu beginnen.

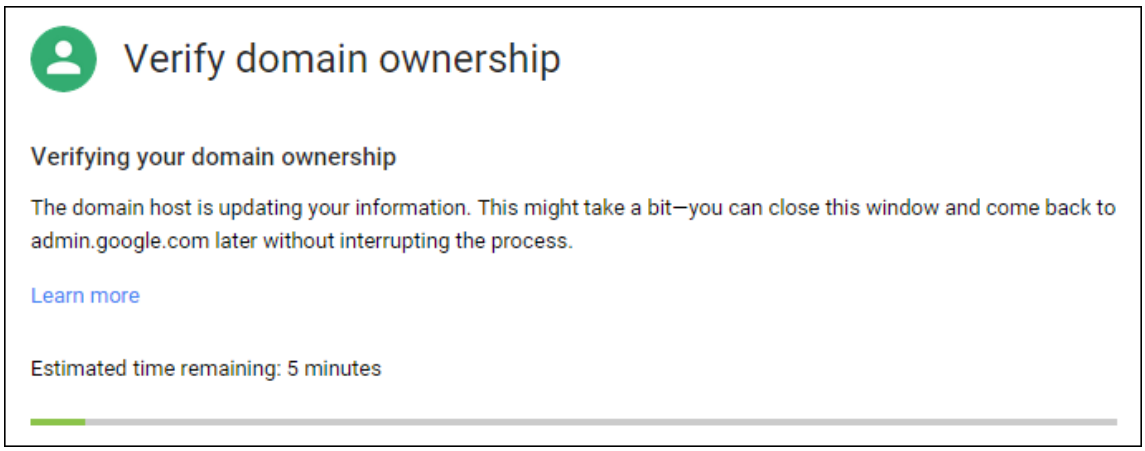
   Die Seite **Verify domain ownership** wird angezeigt. Folgen Sie den angezeigten Anweisungen zum Überprüfen Ihrer Domäne.

2. Klicken Sie auf **Verify**.

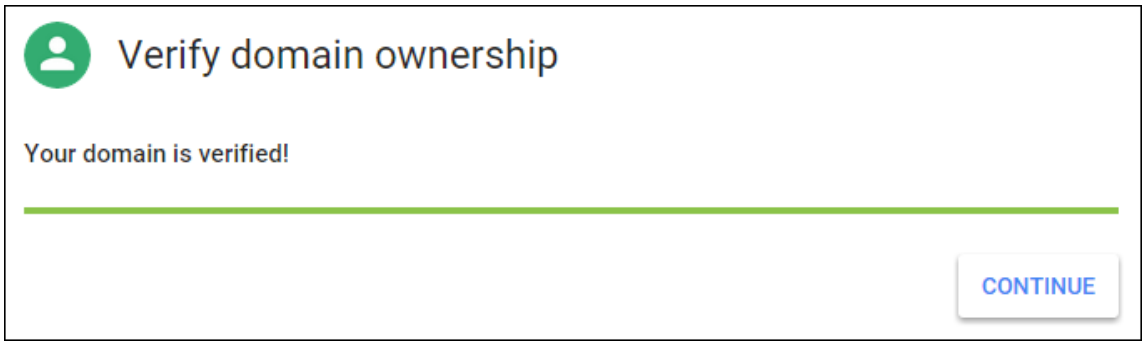




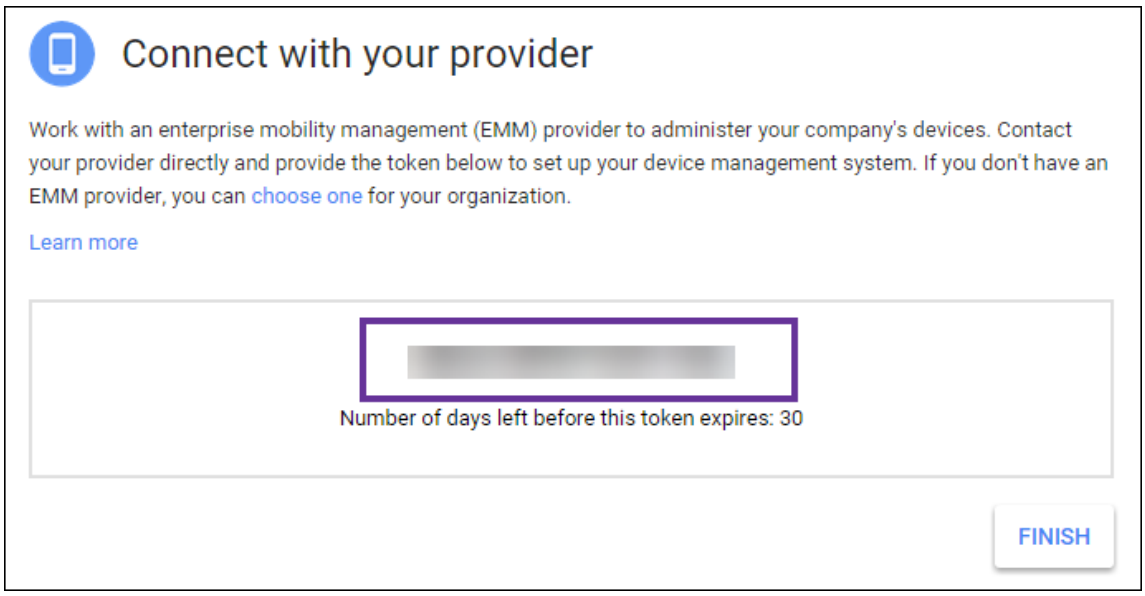
3. Google überprüft die Eigentümerschaft der Domäne.



4. Nach einer erfolgreichen Überprüfung wird die folgende Seite angezeigt. Klicken Sie auf **Weiter**.



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



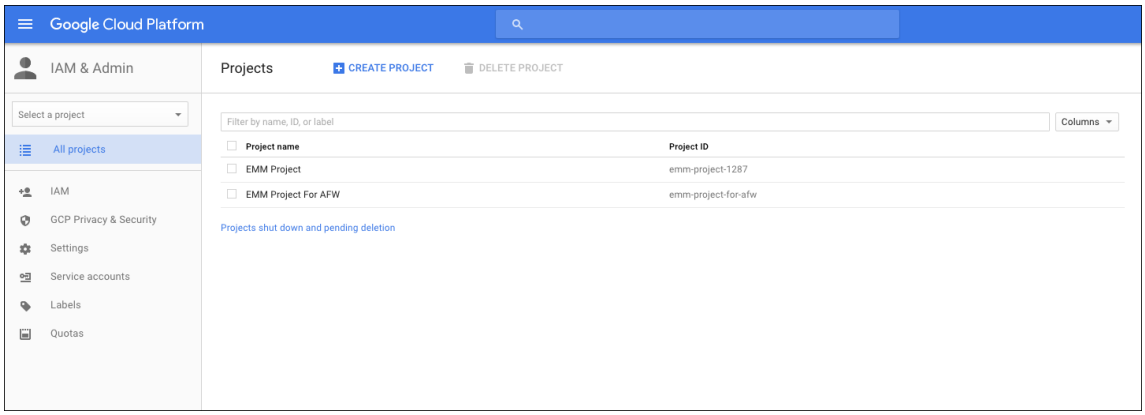
6. Klicken Sie auf **Finish**, um das Einrichten von Android Enterprise abzuschließen. Es wird eine Seite mit der Meldung angezeigt, dass Ihre Domäne erfolgreich verifiziert wurde.

Nach dem Erstellen eines Android Enterprise-Dienstkontos können Sie sich bei der Google Admin-Konsole anmelden und die Einstellungen Ihrer Mobilitätsverwaltung festlegen.

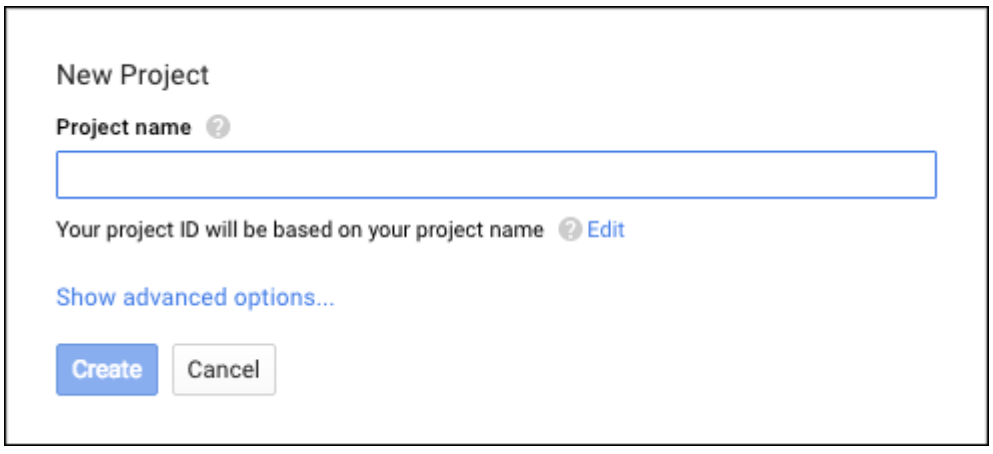
Einrichten eines Android Enterprise-Dienstkontos und Herunterladen eines Android Enterprise-Zertifikats

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.

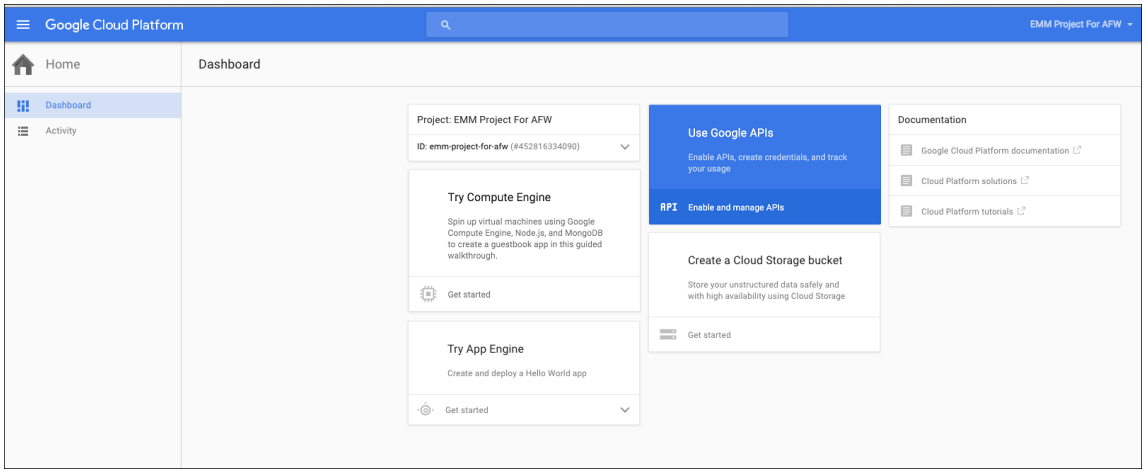
1. Rufen Sie in einem Webbrowser https://console.cloud.google.com/project auf und melden Sie sich mit Ihren Anmeldeinformationen als Google-Administrator an.
2. Klicken Sie in der Liste **Projects** auf **Create project**.



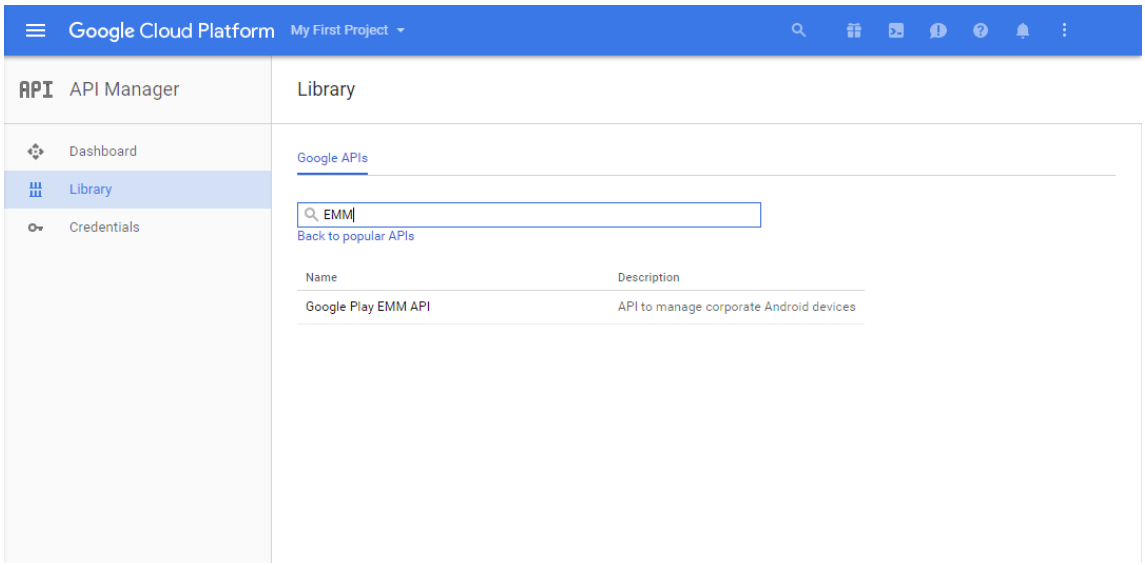
3. Geben Sie unter **Project name** einen Namen für das Projekt ein.



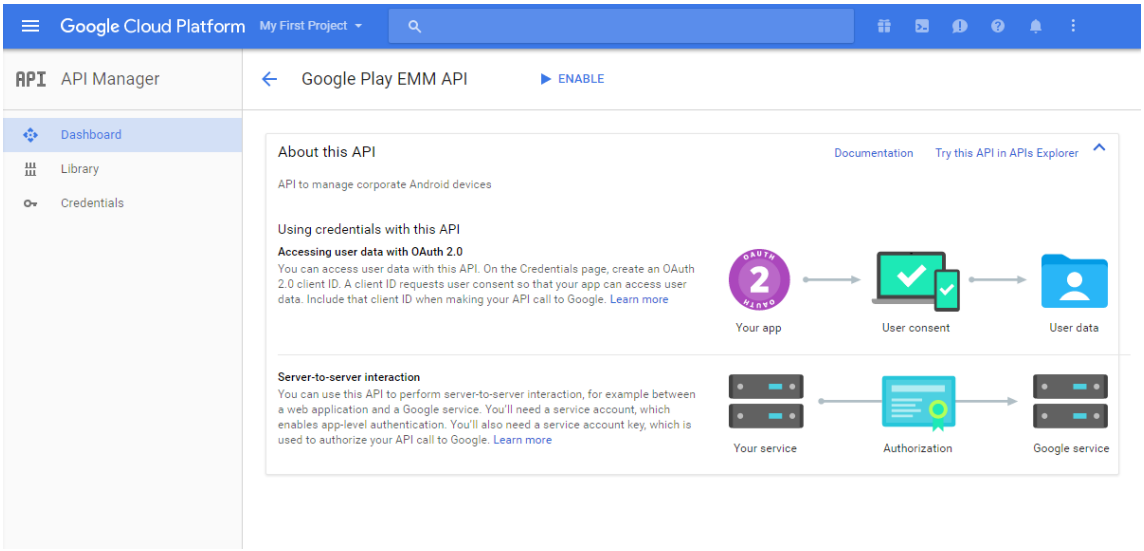
4. Klicken Sie im Dashboard auf **Use Google APIs**.



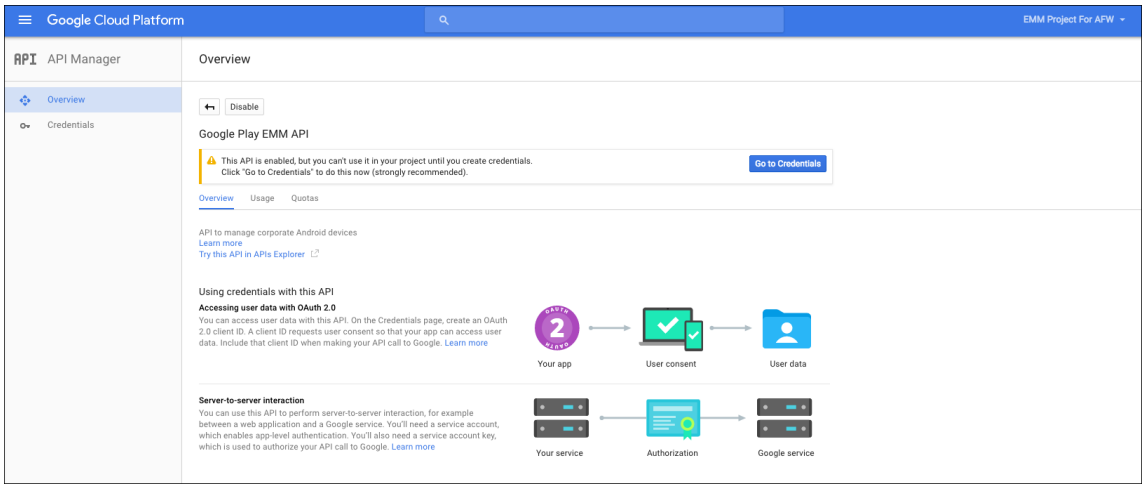
5. Klicken Sie auf **Library** geben Sie für **Search** den Text **EMM** ein und klicken Sie auf das Suchergebnis.



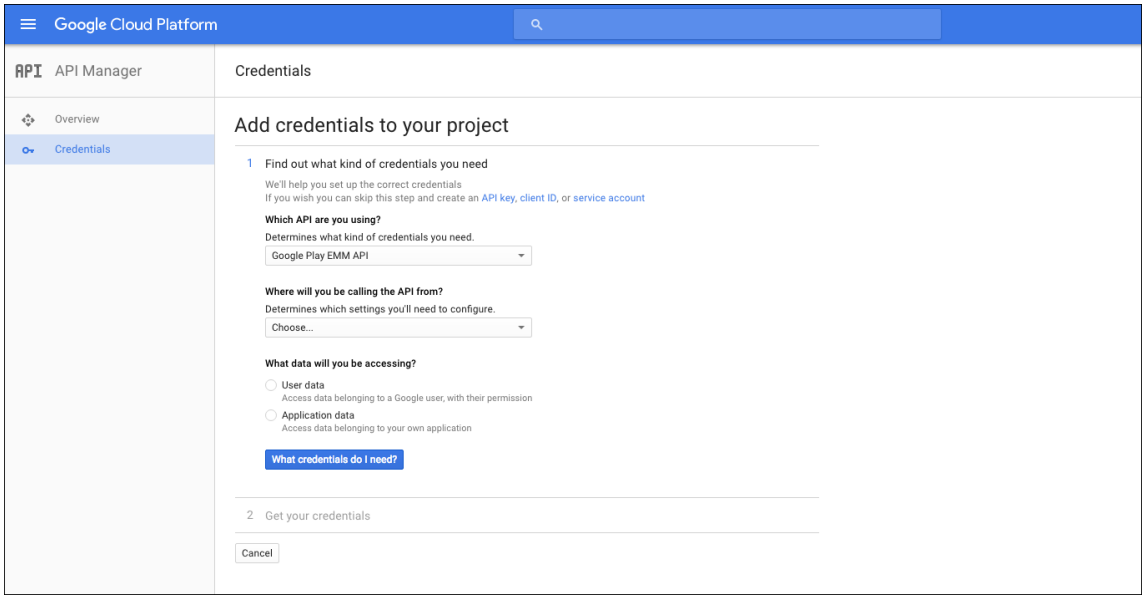
6. Klicken Sie auf der Seite **Overview** auf **Enable**.



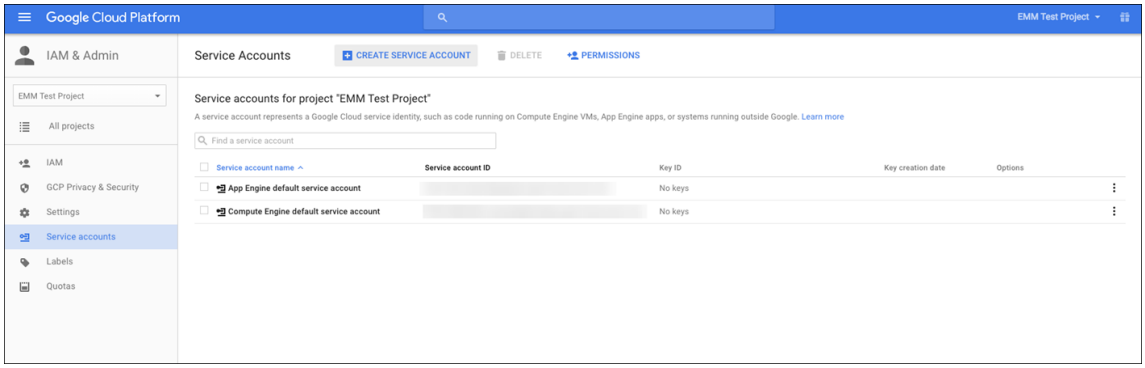
7. Klicken Sie neben **Google Play EMM API** auf **Go to Credentials**.



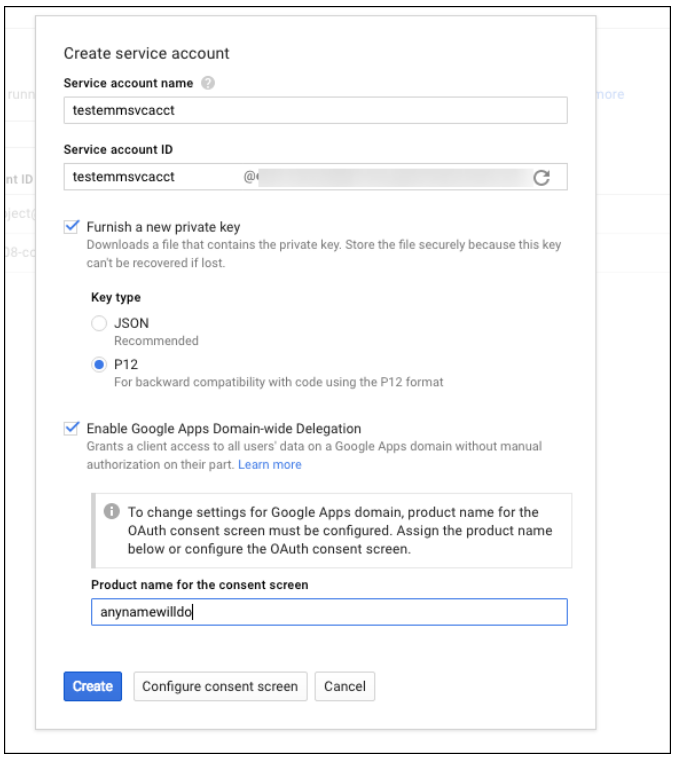
8. Klicken Sie in der Liste **Add credentials to our project** unter Schritt 1 auf **service account**.



9. Klicken Sie auf der Seite **Service Accounts** auf **Create Service Account**.

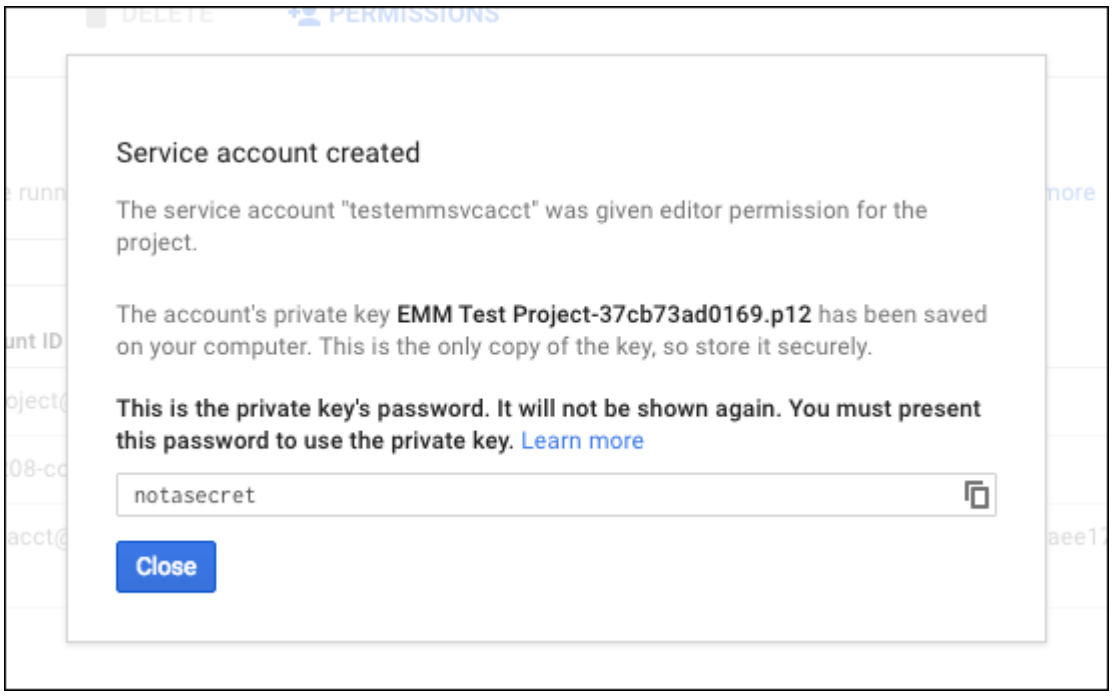


10. Geben Sie unter **Create service account** einen Namen für das Konto ein und aktivieren Sie das Kontrollkästchen **Furnish a new private key**. Klicken Sie auf **P12**, aktivieren Sie das Kontrollkästchen **Enable Google Apps Domain-wide Delegation** und klicken Sie auf **Create**.

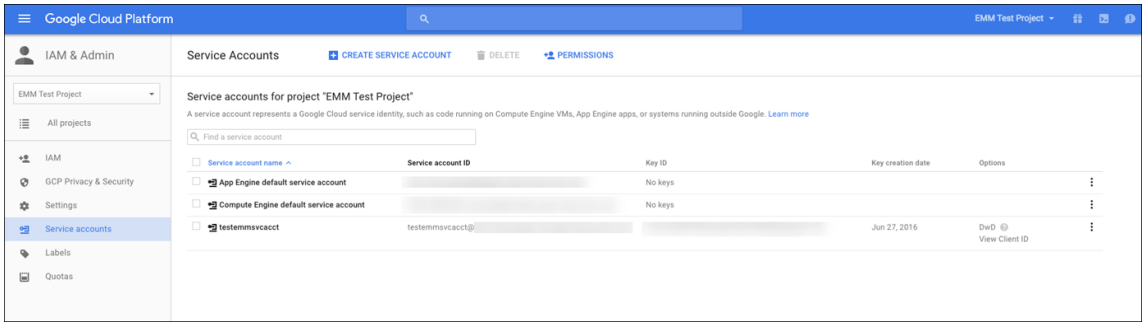


Die Zertifikatdatei (P12-Datei) wird auf Ihren Computer heruntergeladen. Speichern Sie das Zertifikat an einem sicheren Ort.

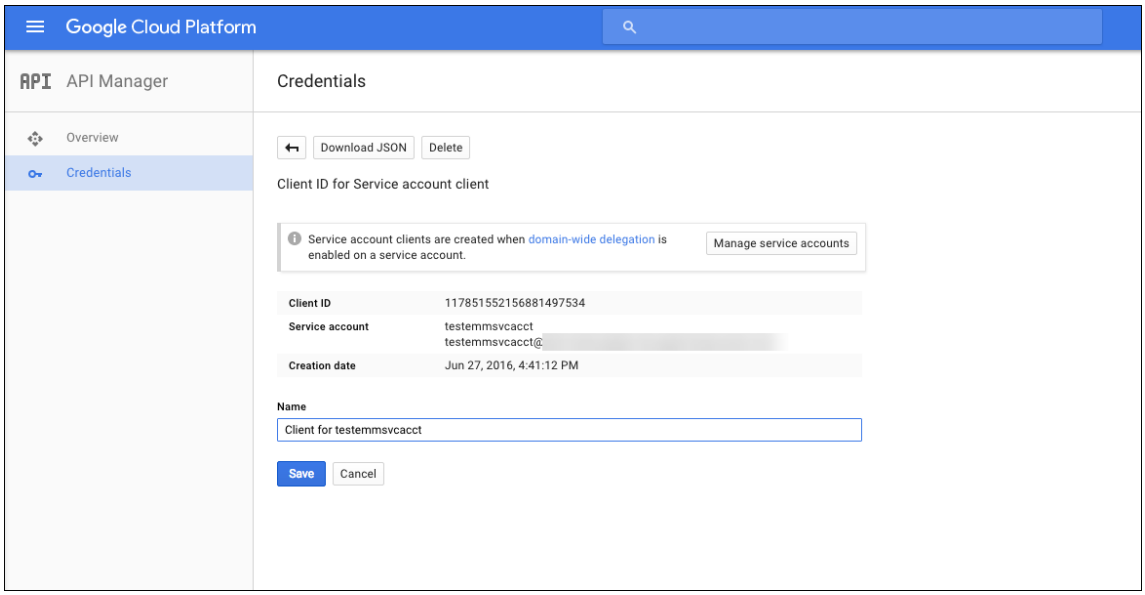
11. Klicken Sie auf der Seite **Service account created** auf **Close**.



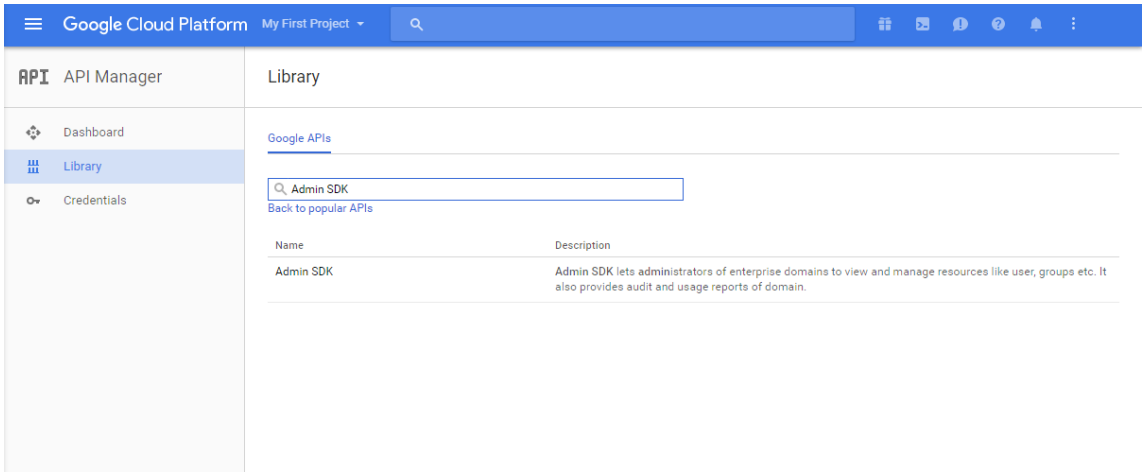
12. Klicken Sie unter **Permissions** auf **Service accounts** und dann unter **Options** für Ihr Dienstkonto auf **View Client ID**.



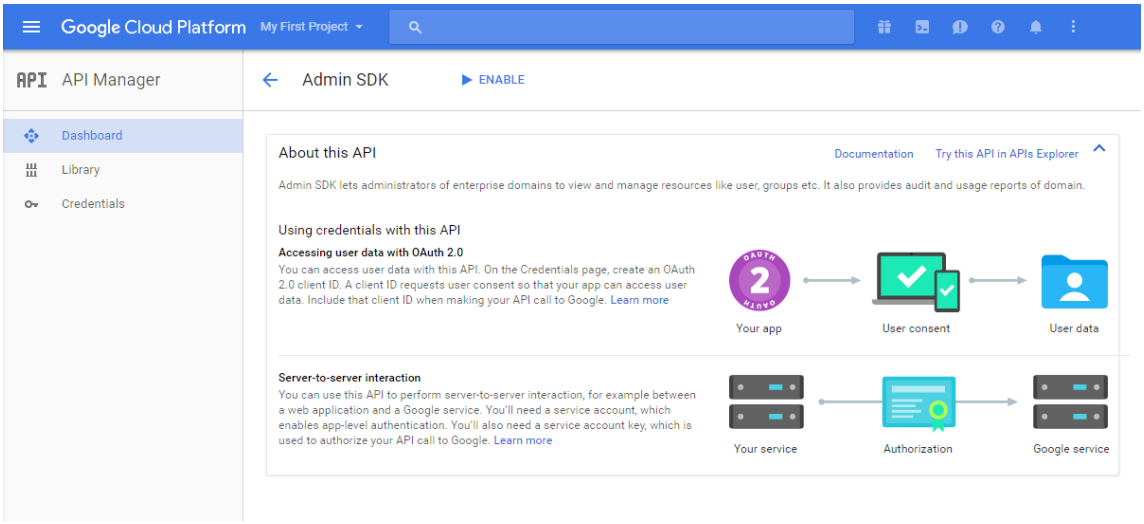
13. Die für die Kontoautorisierung auf der Google Admin-Konsole erforderlichen Informationen werden angezeigt. Kopieren Sie die **Client ID** und die **Service account ID** an einen Speicherort, an dem Sie die Informationen später abrufen können. Sie müssen diese Informationen mit dem Domänennamen an den Citrix Support senden, damit sie auf eine Positivliste gesetzt werden.



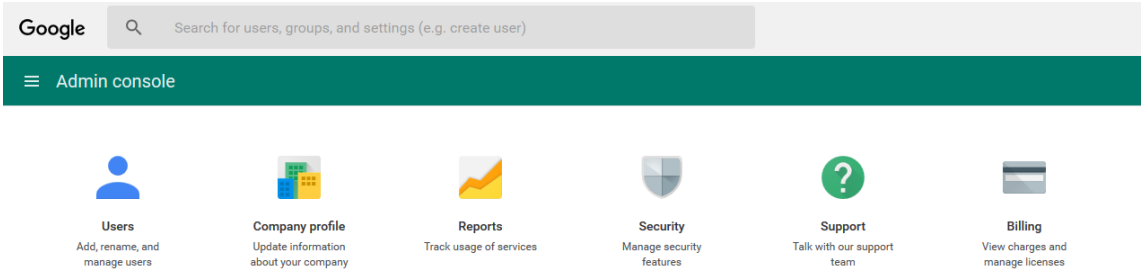
14. Suchen Sie auf der Seite **Library** den Eintrag **Admin SDK** und klicken Sie auf das Suchergebnis.



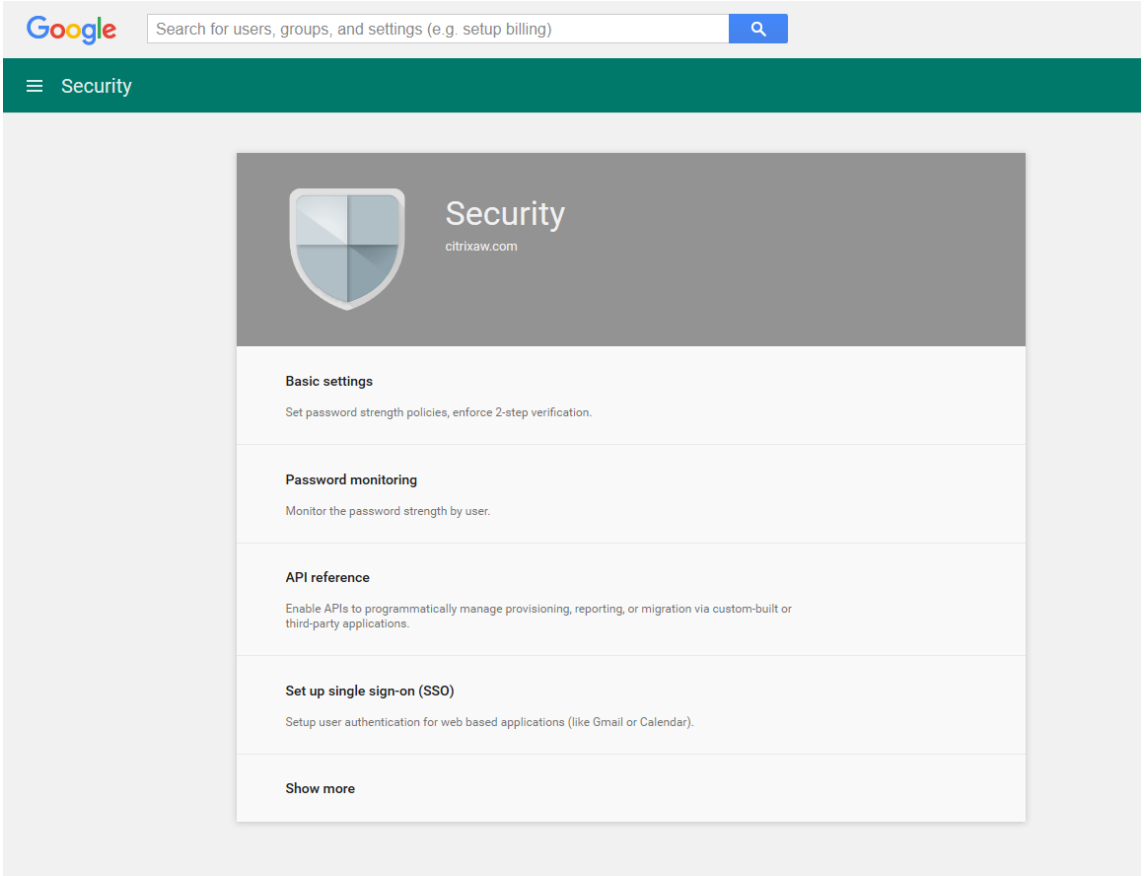
15. Klicken Sie auf der Seite **Overview** auf **Enable**.

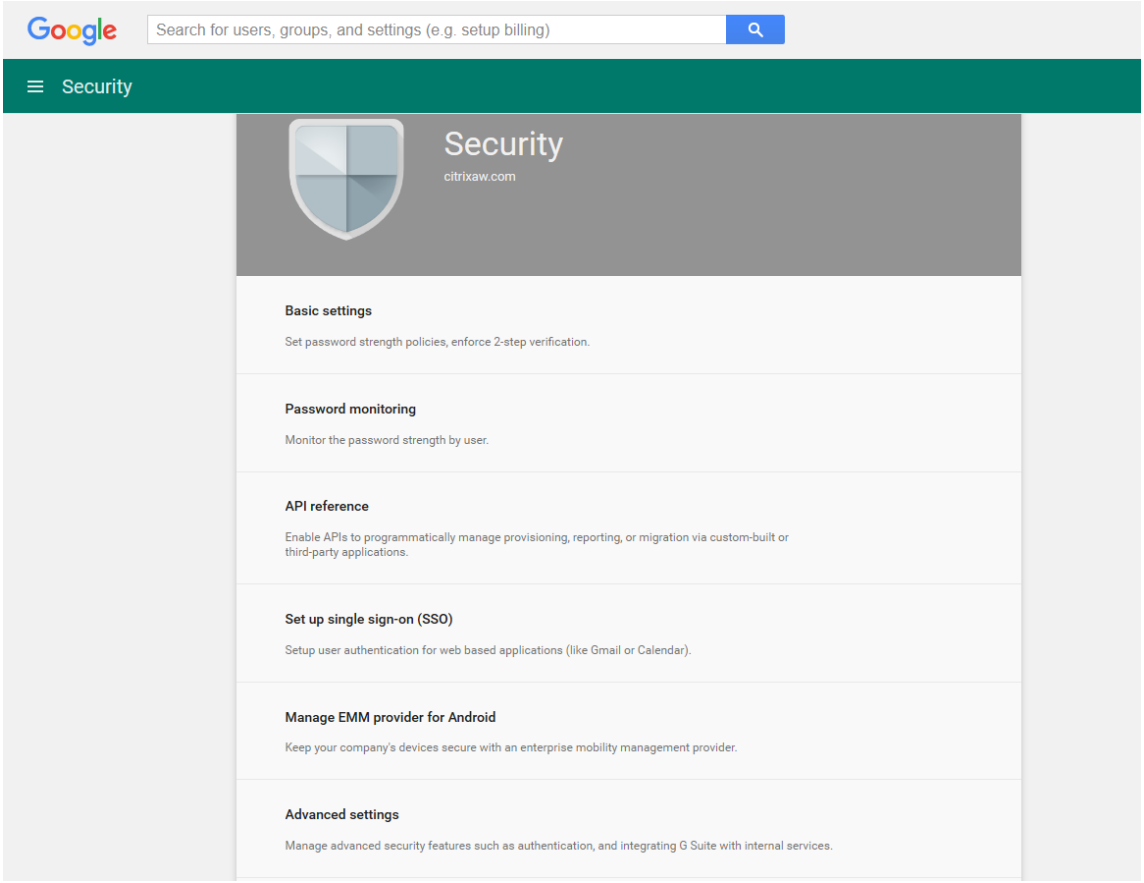


16. Öffnen Sie die Google Admin-Konsole für Ihre Domäne und klicken Sie auf **Security**.

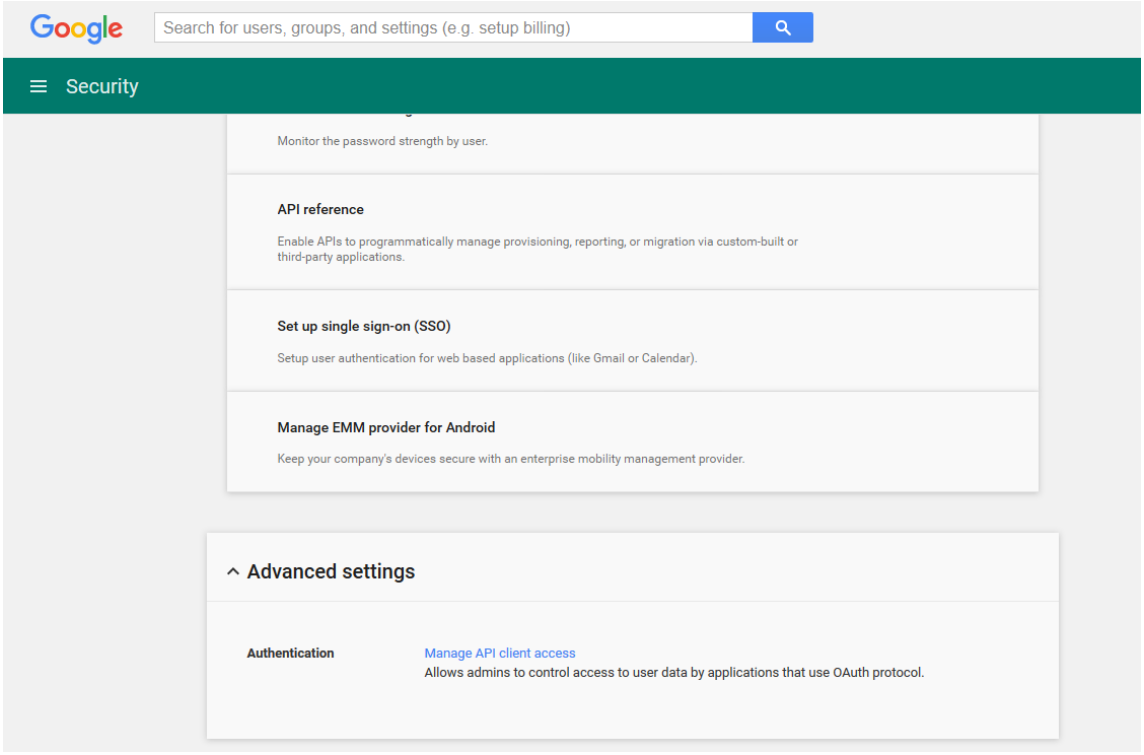


17. Klicken Sie auf der Seite **Settings** auf **Show more** und dann auf **Advanced settings**.

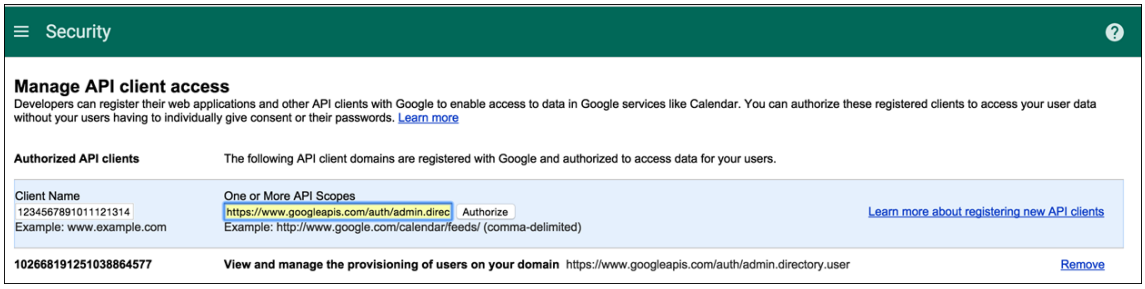




18. Klicken Sie auf **Manage API client access**.



19. Geben Sie unter **Client Name** die Client-ID ein, die Sie zuvor gespeichert haben, geben Sie unter **One or More API Scopes** den Text `https://www.googleapis.com/auth/admin.directory.user` ein und klicken Sie auf **Authorize**.



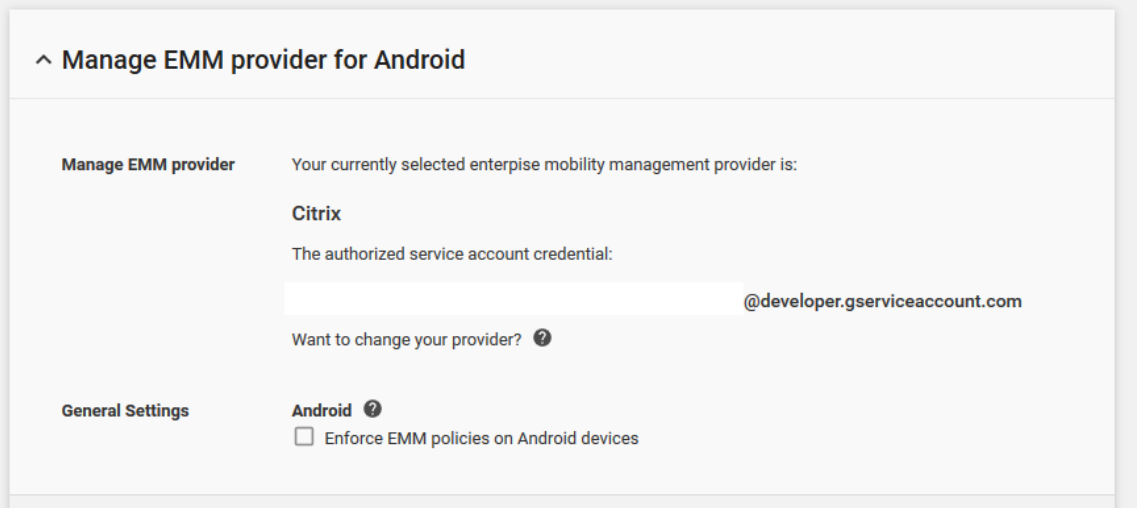
Binden an EMM

Bevor Sie Android-Geräte mit XenMobile verwalten können, müssen Sie dem technischen Support von Citrix den Namen Ihrer Domäne, das Dienstkonto und den 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 Enterprise-Konto bei Google nun an Citrix als EMM-Anbieter gebunden ist.

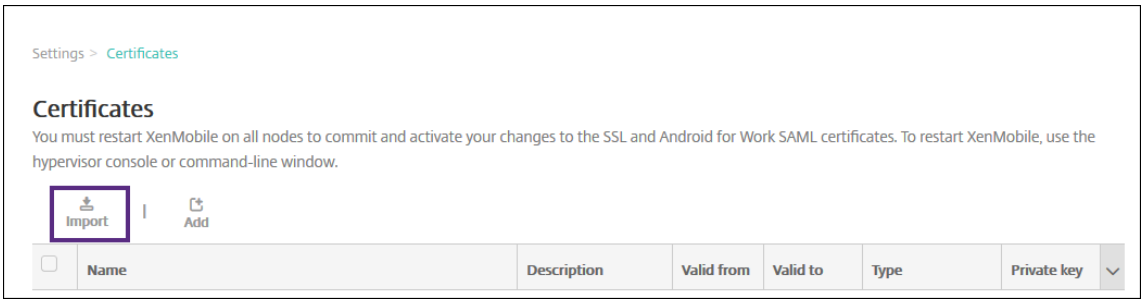
   Nach der Prüfung der Tokenbindung können Sie XenMobile zum Verwalten der Android-Geräte verwenden. Importieren Sie das P12-Zertifikat, das Sie in Schritt 14 erstellt haben. Richten Sie den Android Enterprise-Server ein, aktivieren Sie das SAML-basierte Single Sign-On und definieren Sie mindestens eine Android Enterprise-Richtlinie.



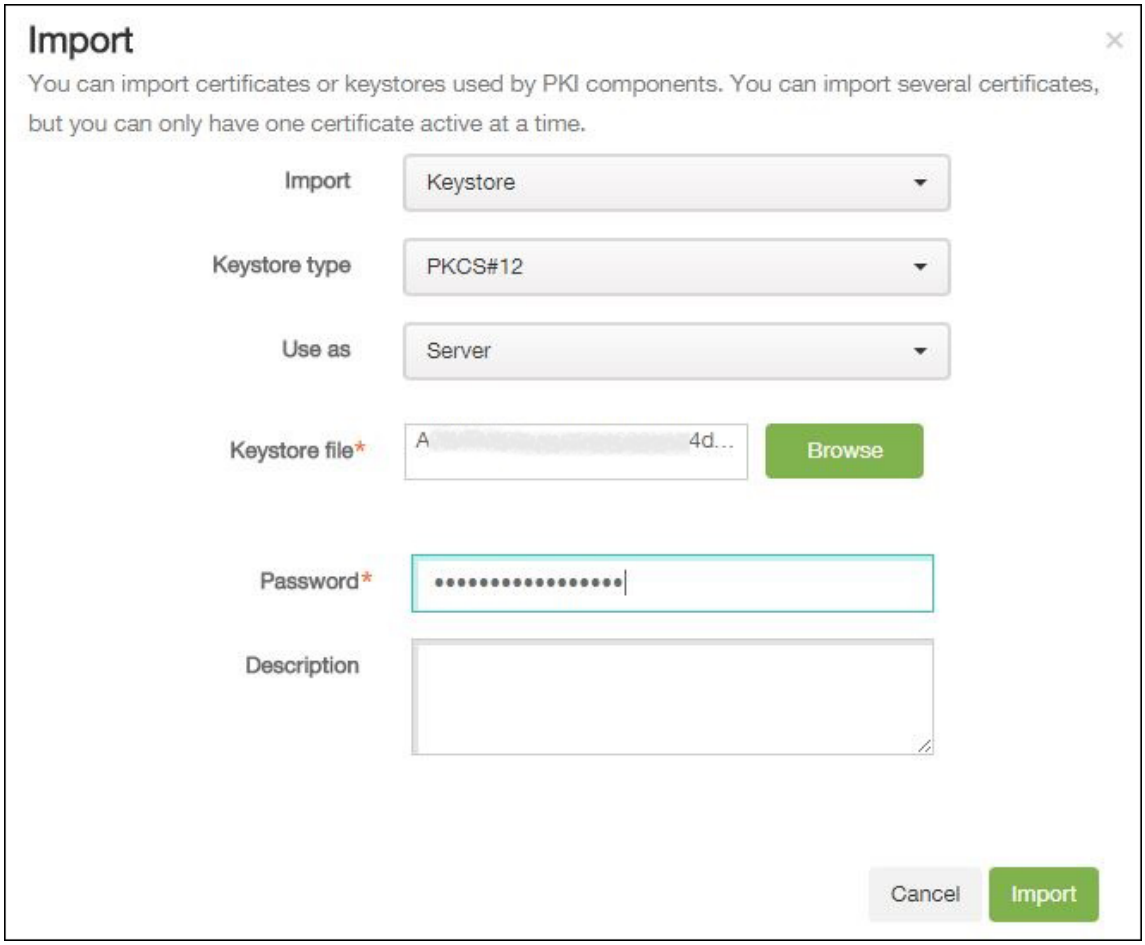
Importieren des P12-Zertifikats

Führen Sie die folgenden Schritte zum Importieren des Android Enterprise-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.



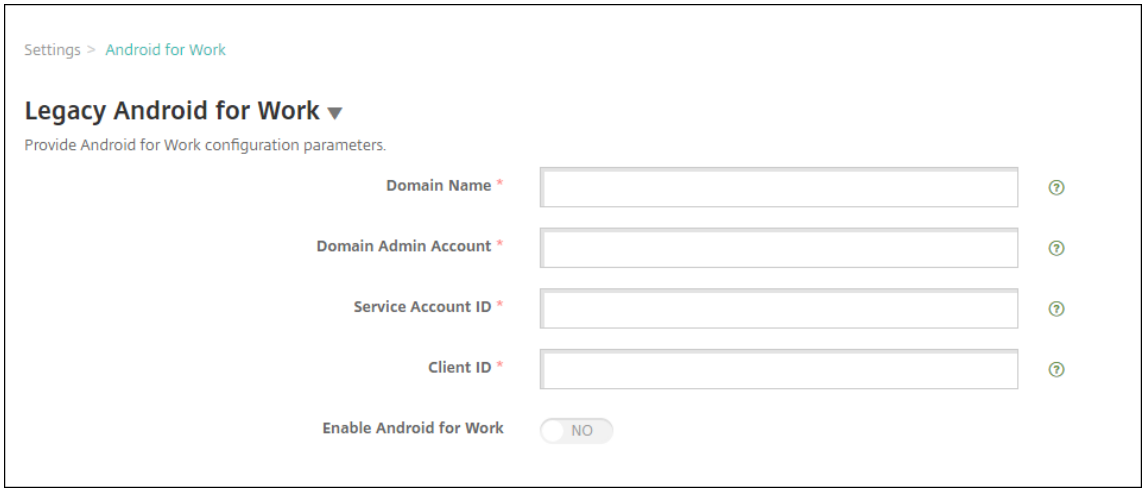
Konfigurieren Sie die folgenden Einstellungen:

- **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**.

Einrichten der Android Enterprise-Servereinstellungen

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

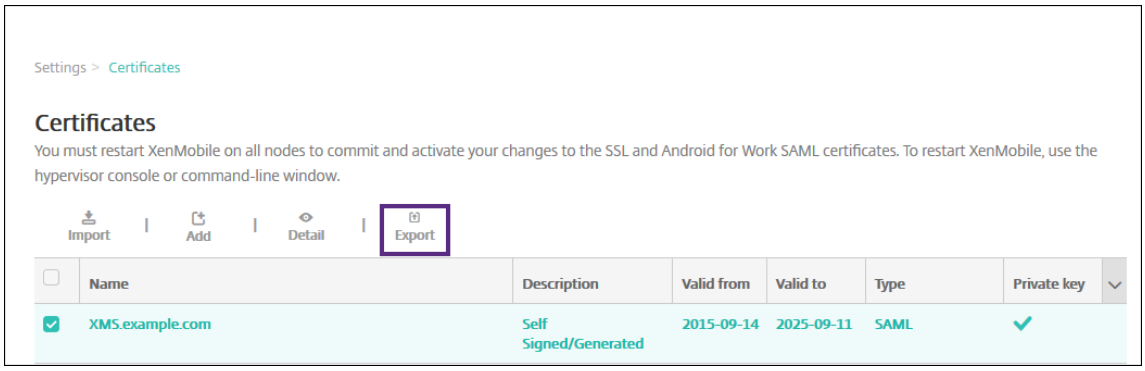


Konfigurieren Sie die folgenden Einstellungen und klicken Sie dann auf **Speichern**.

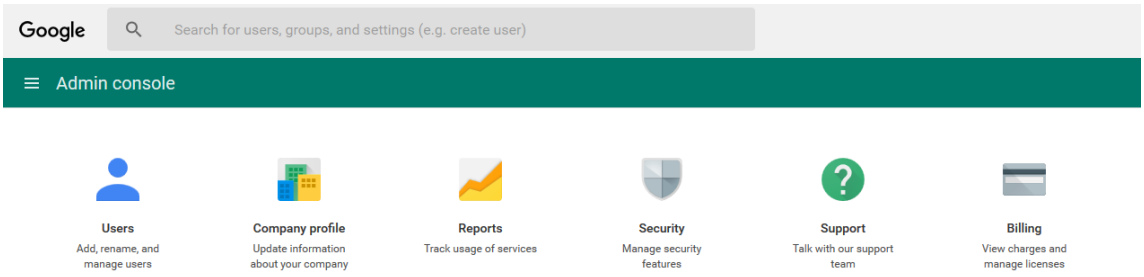
- **Domänenname:** Geben Sie den Namen der Android Enterprise-Domäne ein, z. B. domain.com.
- **Domänenadministratorkonto:** Geben Sie Ihren Domänenadministrator-Benutzernamen ein, z. B. das für das Google Developer Portal verwendete E-Mail-Konto.
- **Dienstkonto-ID:** Geben Sie die ID Ihres Dienstkontos ein, z. B. die dem Google-Dienstkonto zugeordnete E-Mail-Adresse (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`).
- **Client-ID:** Geben Sie die numerische ID Ihres Google-Dienstkontos ein.
- **Android Enterprise aktivieren:** Wählen Sie aus, ob Android Enterprise aktiviert oder deaktiviert werden soll.

Aktivieren des SAML-basierten Single Sign-Ons

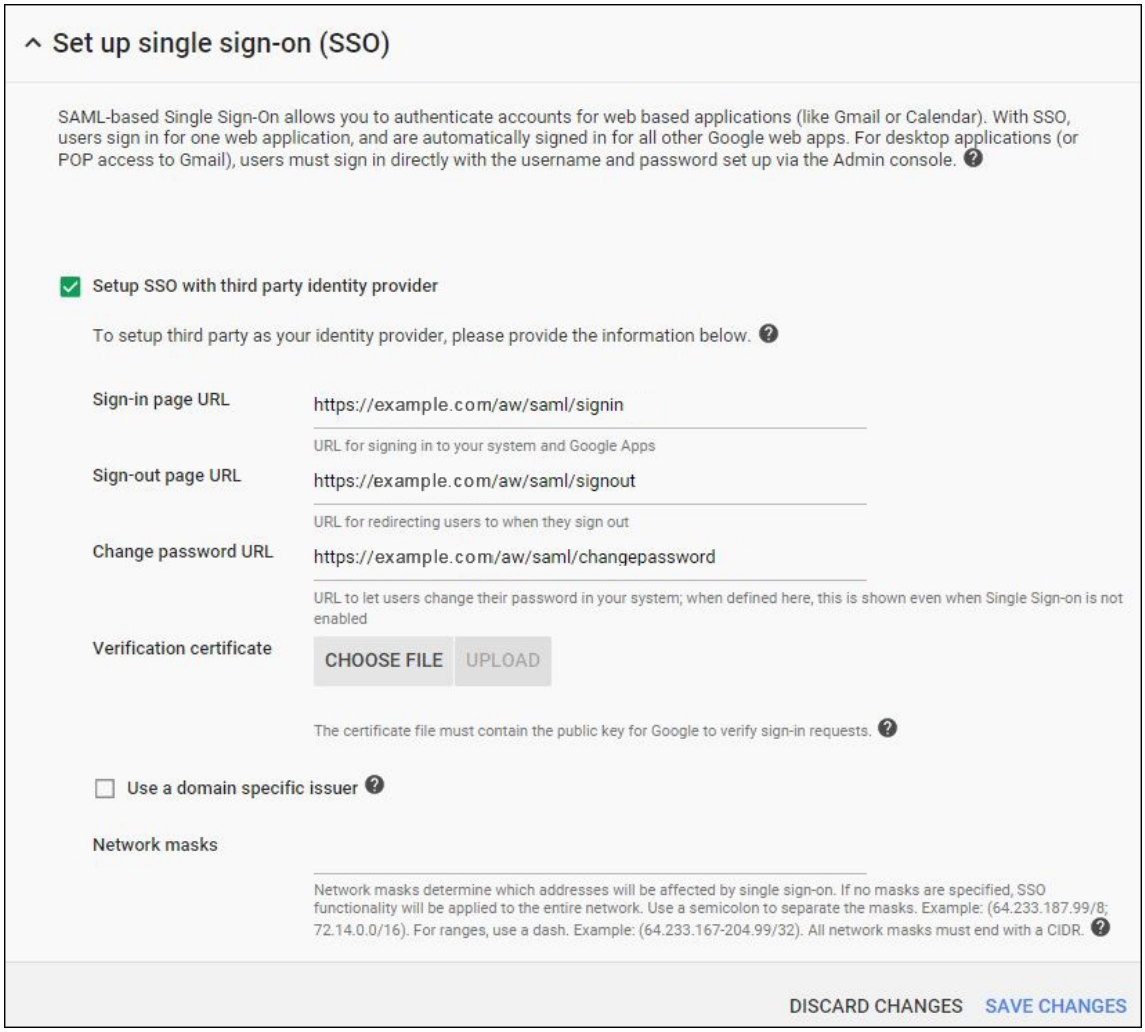
1. Melden Sie sich bei der XenMobile-Konsole an.
2. Klicken Sie auf das Zahnradsymbol rechts oben in der Konsole. Die Seite **Einstellungen** wird angezeigt.
3. Klicken Sie auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.



4. Klicken Sie in der Liste der Zertifikate auf das SAML-Zertifikat.
5. Klicken Sie auf **Exportieren** und speichern Sie das Zertifikat auf Ihrem Computer.
6. Melden Sie sich beim Google-Verwaltungsportal mit Ihren Android Enterprise-Administratoranmeldeinforma an. Informationen zum Zugriff auf das Portal finden Sie unter Google-Verwaltungsportal.
7. Klicken Sie auf **Sicherheit**.



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

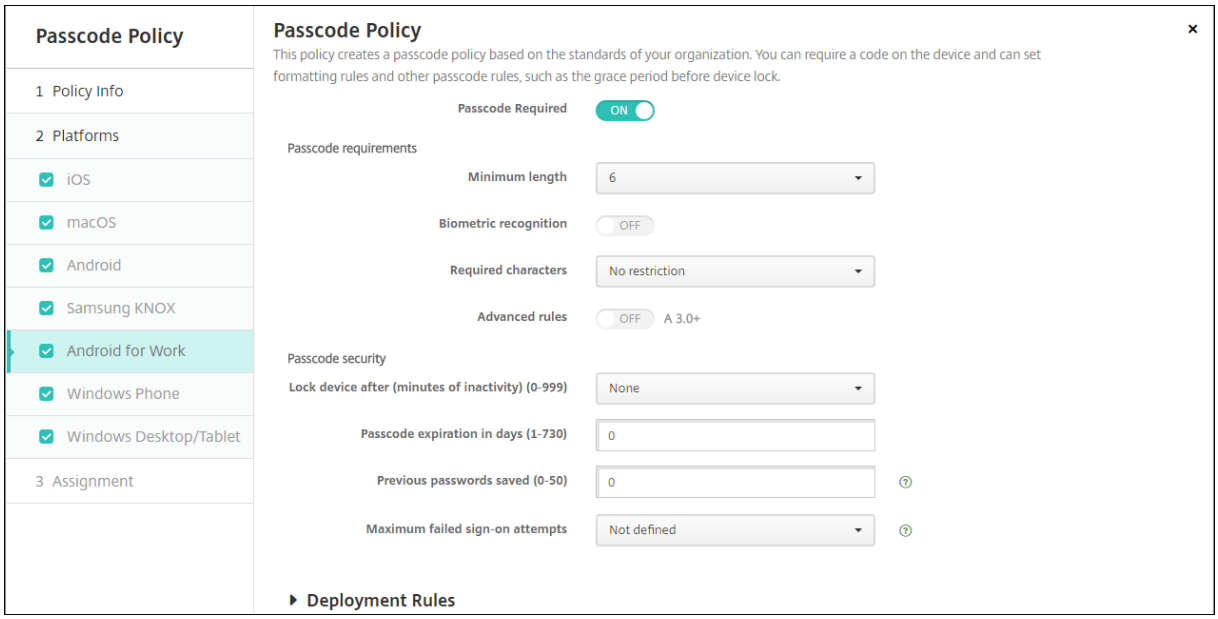


- **Sign-in page URL:** Geben Sie die URL der Seite an, über die Benutzer sich bei Ihrem System und Google Apps anmelden. Beispiel: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **Sign-out page URL:** Geben Sie die URL an, an die die Benutzer weitergeleitet werden, wenn sie sich abmelden. Beispiel: `https://<Xenmobile-FQDN>/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://<Xenmobile-FQDN>/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.

9. Klicken Sie auf **SAVE CHANGES**.

Einrichten einer Android Enterprise-Richtlinie

Richten Sie eine Passcode-Richtlinie ein, sodass Benutzer bei der ersten Registrierung einen Passcode auf ihrem Gerät festlegen müssen.



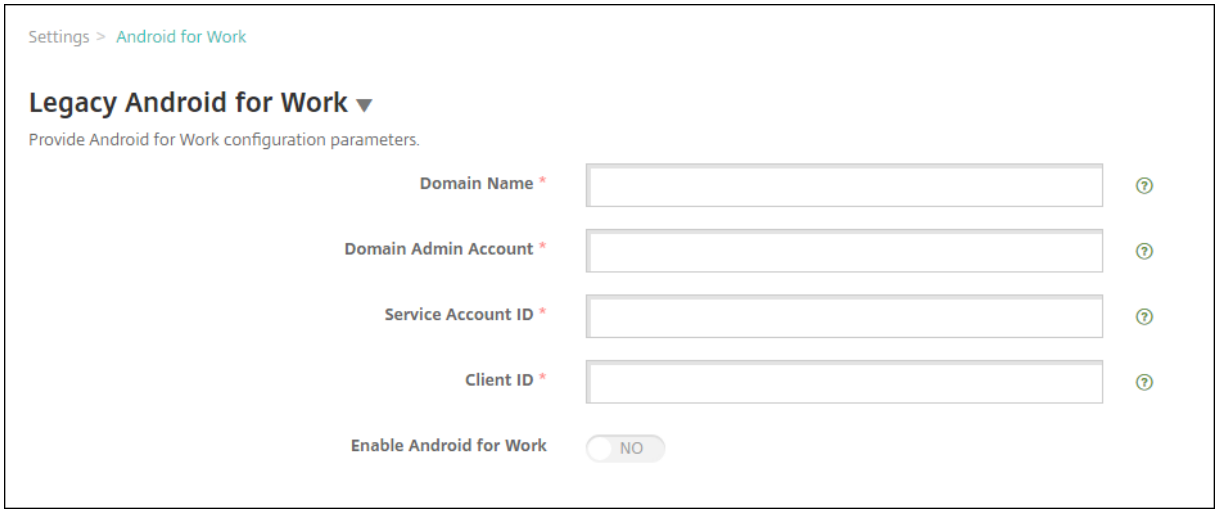
Grundlegende Schritte zum Einrichten einer Geräterichtlinie:

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 Enterprise** und konfigurieren Sie die Einstellungen für die Richtlinie.
6. Weisen Sie die Richtlinie einer Bereitstellungsgruppe zu.

Konfigurieren der Android Enterprise-Kontoeinstellungen

Bevor Sie Android-Apps und Richtlinien auf Benutzergeräten verwalten können, müssen Sie eine Domäne und Kontoinformationen für Android Enterprise in XenMobile einrichten. Zunächst müssen Sie Android Enterprise-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 **Plattformen**auf **Android Enterprise**. Die Konfigurationsseite **Android Enterprise** wird angezeigt.



1. Konfigurieren Sie auf der Seite **Android Enterprise** 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.
   - **Client-ID:** Geben Sie die ID Ihres Google-Dienstkontos ein.
   - **Android Enterprise aktivieren:** Wählen Sie aus, ob Android Enterprise aktiviert werden soll.
2. Klicken Sie auf **Speichern**.

Einrichten von Google Workspace-Partnerzugriff für XenMobile

Einige Endpunktverwaltungsfunktionen für Chrome verwenden Google-Partner-APIs für die Kommunikation zwischen XenMobile und Ihrer Google Workspace-Domäne. Beispielsweise benötigt XenMobile die APIs für Geräterichtlinien, die Chrome-Features wie den Incognitomodus und den Gastmodus verwalten.

Zum Aktivieren dieser Partner-APIs richten Sie Ihre Google Workspace-Domäne in der XenMobile-Konsole ein und konfigurieren anschließend Ihr Google Workspace-Konto.

Einrichten Ihrer Google Workspace-Domäne (ehemals G Suite) in XenMobile

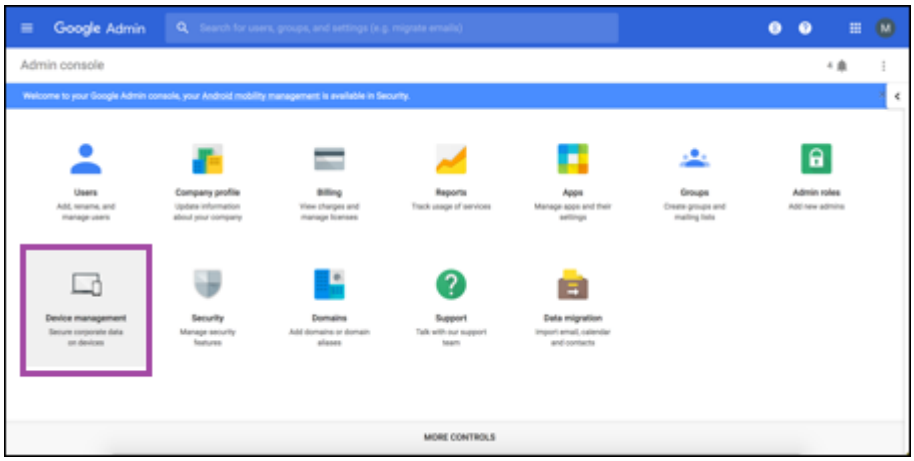
Um die Kommunikation zwischen XenMobile und den APIs in Ihrer Google Workspace-Domäne zu aktivieren, gehen Sie zu **Einstellungen > Google Chrome-Konfiguration** und konfigurieren Sie die Einstellungen.

- **G Suite-Domäne:** Die Google Workspace-Domäne mit den von XenMobile benötigten APIs.
- **G Suite-Administratorkonto:** Das Administratorkonto für Ihre G Suite-Domäne.

- **G Suite-Client-ID:** Die Client-ID für Citrix. Konfigurieren Sie mit diesem Wert den Partnerzugriff für Ihre Google Workspace-Domäne.
- **G Suite-Unternehmens-ID:** Die Unternehmens-ID für Ihr Konto mit den Angaben Ihres Google Enterprise-Kontos.

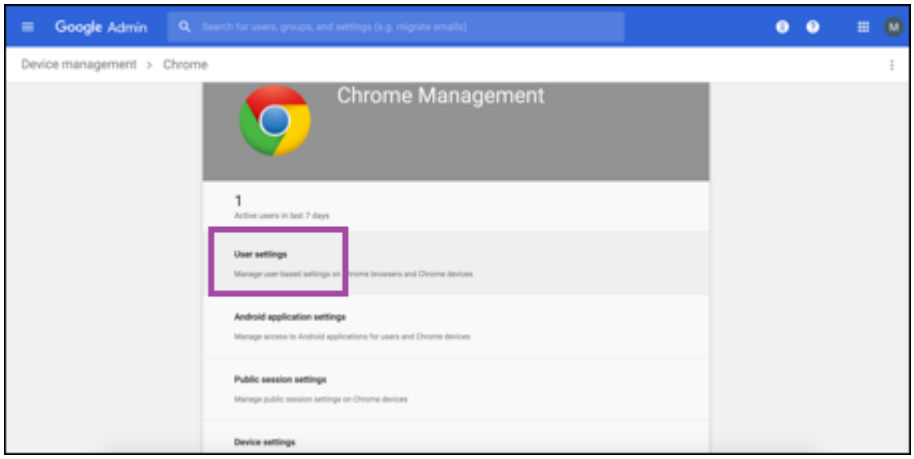
Aktivieren des Partnerzugriffs für Geräte und Benutzer in Ihrer Google Workspace-Domäne

1. Melden Sie sich an der Google Admin-Konsole an: https://admin.google.com
2. Klicken Sie auf **Device Management**.



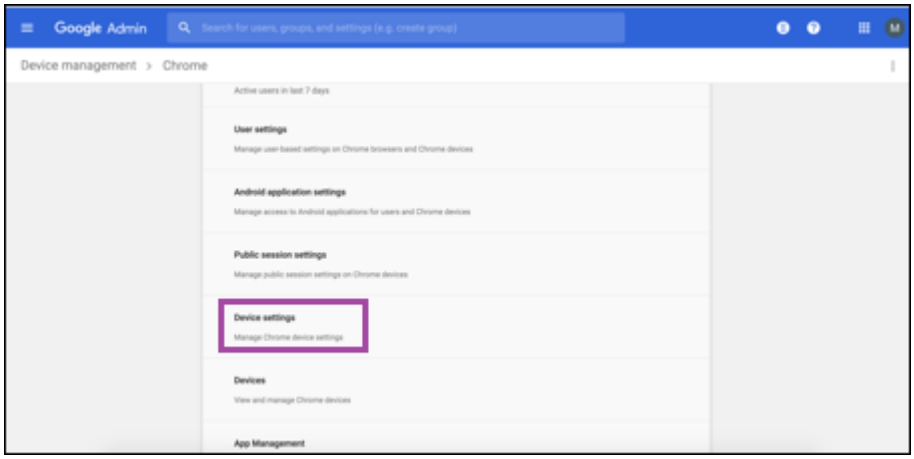
3. Klicken Sie auf **Chrome management**.

4. Klicken Sie auf **User settings**.



5. Suchen Sie nach **Chrome Management - Partner Access**.

6. Aktivieren Sie das Kontrollkästchen **Enable Chrome Management - Partner Access**.
7. Stimmen Sie zu, dass Sie den Partnerzugriff verstehen und aktivieren möchten. Klicken Sie auf **Speichern**.
8. Klicken Sie auf der Chrome-Verwaltungsseite auf **Device Settings**.



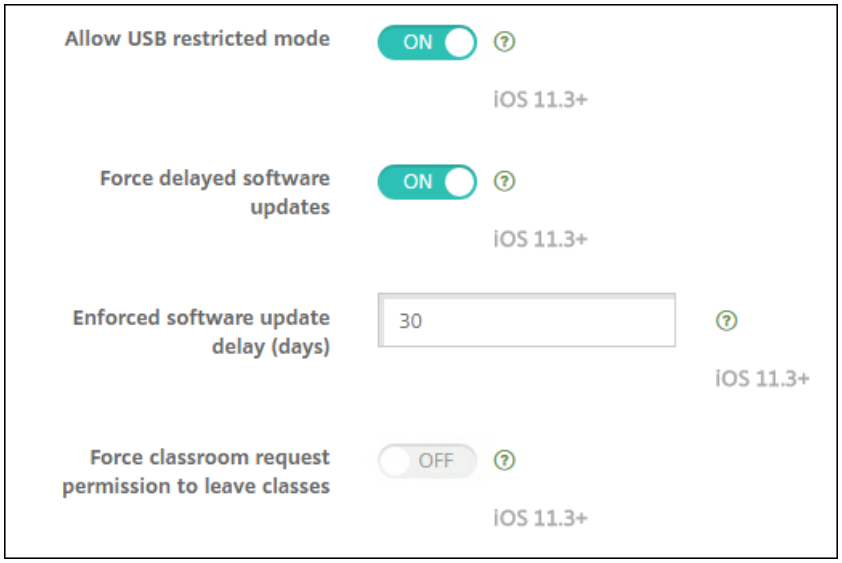
9. Suchen Sie nach **Chrome Management - Partner Access**.

10. Aktivieren Sie das Kontrollkästchen **Enable Chrome Management - Partner Access**.
11. Stimmen Sie zu, dass Sie den Partnerzugriff verstehen und aktivieren möchten. Klicken Sie auf **Speichern**.
12. Wechseln Sie zur Seite **Security** und klicken Sie auf **Advanced Settings**.

13. Klicken Sie auf **Manage API client access**.
14. Gehen Sie in der XenMobile-Konsole zu **Einstellungen > Google Chrome-Konfiguration** und kopieren Sie den Wert für Google Workspace Client ID. Kehren Sie zur Seite **Manage API client Access** zurück und fügen Sie den kopierten Wert in das Feld **Client name** ein.
15. Fügen Sie unter **One or More API Scopes** die URL hinzu: `https://www.googleapis.com/auth/chromedevicemanagementapi`

16. Klicken Sie auf **Authorize**.

    Die Meldung “Your settings have been saved” wird angezeigt.



Registrieren von Android Enterprise-Geräten

Wenn Benutzer bei der Geräteregistrierung einen Benutzernamen oder eine Benutzer-ID eingeben müssen: Das akzeptierte Format hängt davon ab, ob in XenMobile der Benutzerprinzipalname (UPN) oder der SAM-Kontoname für die Benutzersuche konfiguriert ist.

Wenn die Benutzer in XenMobile über den UPN gesucht werden, müssen sie einen UPN in diesem Format eingeben:

- *username@domain*

Wenn die Benutzer in XenMobile über SAM gesucht werden, müssen sie die SAM in einem dieser Formate eingeben:

- *username@domain*
- *domain\username*

Bestimmen des konfigurierten Benutzernamentyps im XenMobile Server

1. Klicken Sie in der Konsole von XenMobile Server rechts oben auf das Zahnradsymbol. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf **LDAP**, um die Konfiguration der LDAP-Verbindung anzuzeigen.
3. Prüfen Sie unten auf der Seite, welche Einstellung im Feld **Benutzersuche nach** ausgewählt ist:
    - Bei **userPrincipalName** ist XenMobile Server für UPN konfiguriert.
    - Bei **sAMAccountName** ist XenMobile Server für SAM konfiguriert.

Registrierung für Android Enterprise-Unternehmen aufheben

Sie können die Registrierung eines Android Enterprise-Unternehmens über die XenMobile Server-Konsole und XenMobile Tools aufheben.

Wenn Sie diese Aufgabe ausführen, öffnet XenMobile Server ein Popupfenster für XenMobile Tools. Bevor Sie beginnen, sollten Sie sicherstellen, dass XenMobile Server im verwendeten Browser die Berechtigung hat, Popupfenster zu öffnen. In einigen Browsern, wie Google Chrome, müssen Sie die Popupblockierung deaktivieren und die Adresse der XenMobile-Site der Positivliste des Popupblockers hinzufügen.

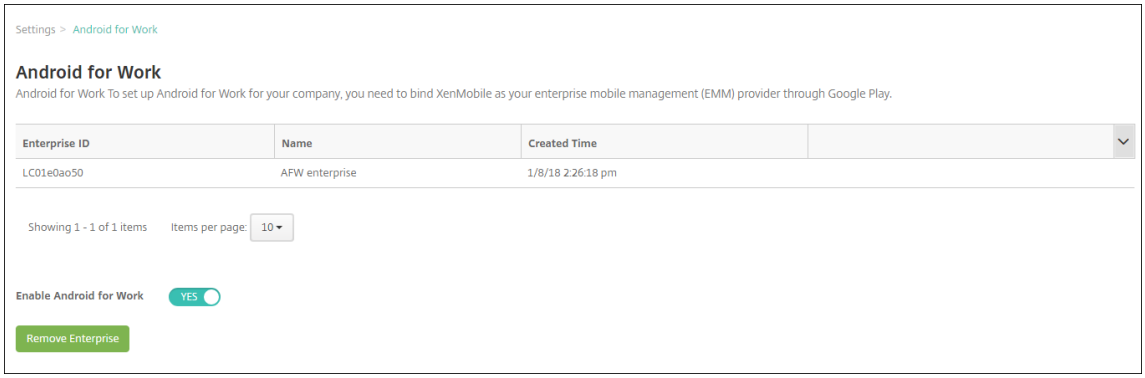
> **Warnung:**
>
> Nachdem die Registrierung eines Unternehmens aufgehoben wurde, werden Android Enterprise-Apps auf Geräten, die bereits registriert wurden, auf die Standardeinstellungen zurückgesetzt. Die Geräte werden dann nicht mehr von Google verwaltet. Für die Neuregistrierung in einem Android Enterprise-Unternehmen ist möglicherweise eine weitere Konfiguration erforderlich, um die vorherige Funktionalität wiederherzustellen.

Nachdem die Registrierung des Android Enterprise-Unternehmens aufgehoben wurde:

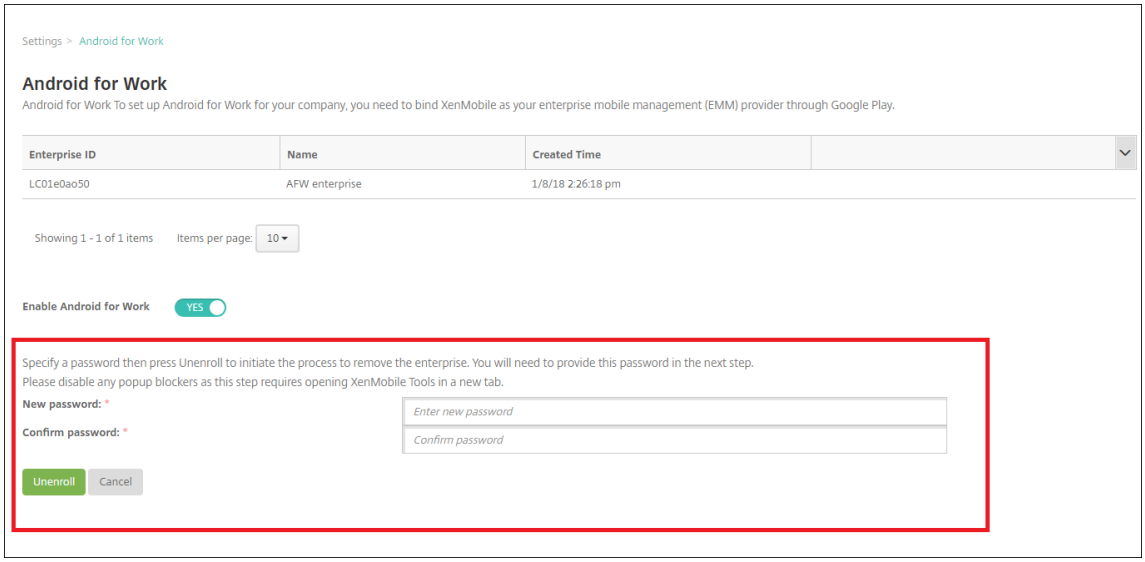
- Für Geräte und Benutzer, die über das Unternehmen registriert sind, wurden die Android Enterprise-Apps auf die Standardeinstellung zurückgesetzt. Android Enterprise App-Berechtigungen und Android Enterprise App-Beschränkungsrichtlinien, die zuvor angewendet wurden, haben keine Wirkung mehr auf Vorgänge.
- Über das Unternehmen registrierte Geräte werden zwar von XenMobile verwaltet, sind jedoch aus der Perspektive von Google nicht verwaltet. Es können keine neuen Android Enterprise-Apps hinzugefügt werden. Sie können keine Android Enterprise App-Berechtigungen oder Android Enterprise App-Einschränkungsrichtlinien anwenden. Sie können weiterhin auf diese Geräte andere Richtlinien anwenden, z. B. Planung, Kennwort und Einschränkungen.
- Wenn Sie versuchen, Geräte in Android Enterprise zu registrieren, werden sie als Android-Geräte und nicht als Android Enterprise-Geräte registriert.

Registrierung für Android Enterprise-Unternehmen aufheben:

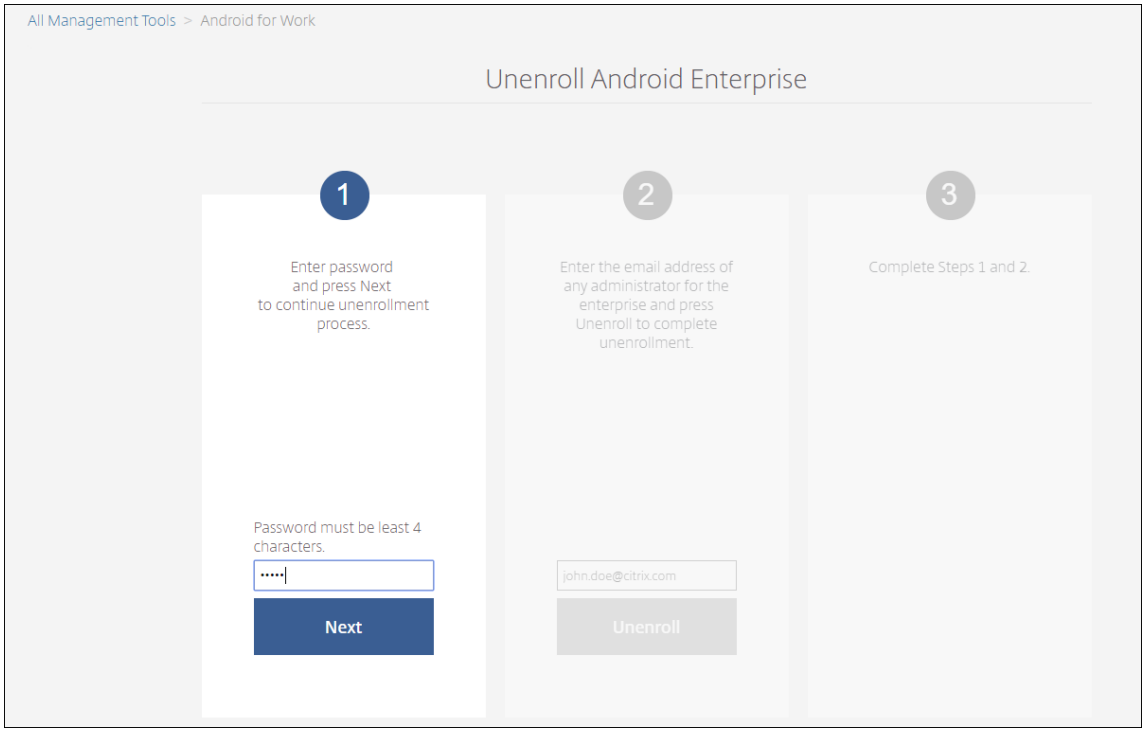
1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite Einstellungen wird angezeigt.
2. Klicken Sie auf der Seite “Einstellungen” auf **Android Enterprise**.
3. Klicken Sie auf **Unternehmen entfernen**.



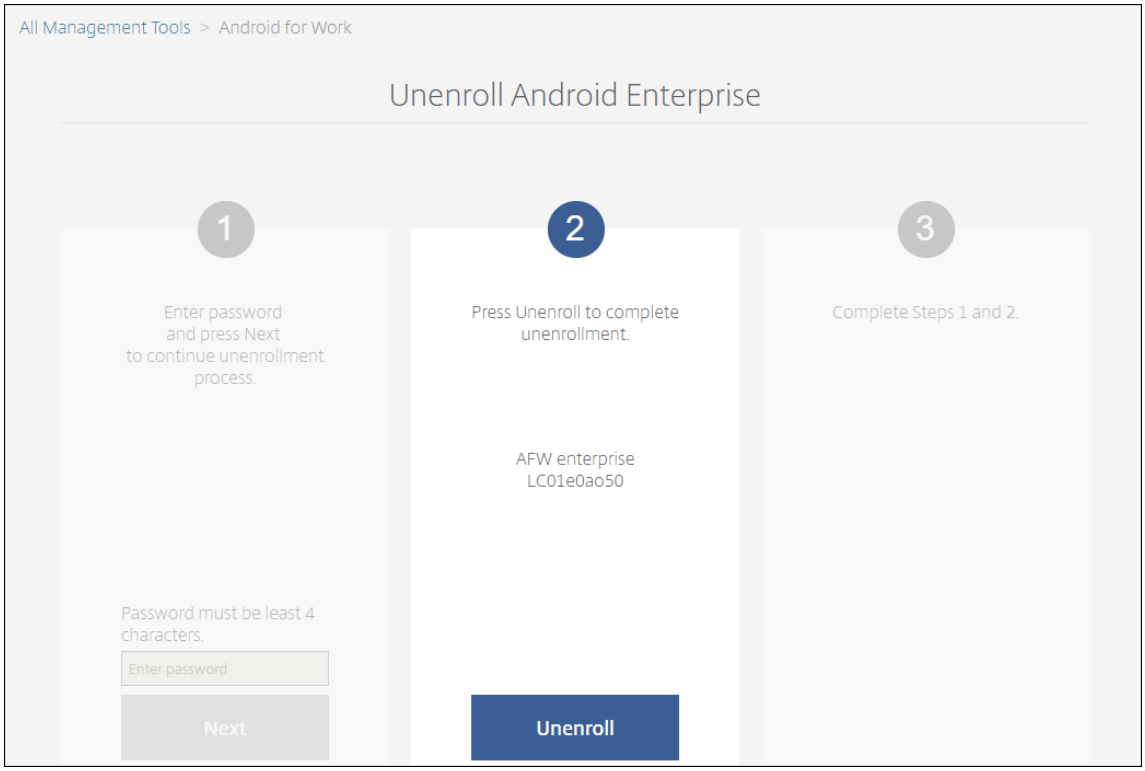
4. Geben Sie ein Kennwort an. Dies ist für den nächsten Schritt erforderlich, um das Aufheben der Registrierung abzuschließen. Klicken Sie dann auf **Registrierung aufheben**.



5. Wenn die XenMobile Tools-Seite geöffnet wird, geben Sie das Kennwort ein, das Sie im vorherigen Schritt erstellt haben.



6. Klicken Sie auf **Registrierung aufheben**.



Provisioning vollständig verwalteter Geräte in Android Enterprise

Nur unternehmenseigene Geräte können als vollständig verwaltete Geräte in Android Enterprise verwendet werden. Auf vollständig verwalteten Geräten wird nicht nur das Arbeitsprofil, sondern das gesamte Gerät vom Unternehmen oder der Organisation gesteuert. Sie sind ein vom Unternehmen verwaltetes Gerät.

Vollständig verwaltete Geräte können in XenMobile durch folgende Verfahren registriert werden:

- **afw#xenmobile:** Bei dieser Registrierungsmethode gibt der Benutzer beim Einrichten des Geräts die Zeichen “afw#xenmobile” ein. Das Token identifiziert das Gerät als von XenMobile verwaltet und lädt Secure Hub herunter.
- **QR-Code:** Die Bereitstellung per QR-Code empfiehlt sich für verteilte Geräte im Bestand, die NFC nicht unterstützen (z. B. Tablets). Sie eignet sich für Geräte im Bestand, die auf Werkseinstellungen zurückgesetzt wurden. Bei dieser Methode werden vollständig verwaltete Geräte vom Setupassistenten durch Scannen eines QR-Codes eingerichtet und konfiguriert.
- **Datenübertragung per NFC (Near Field Communication):** Die Registrierung per NFC eignet sich für Geräte im Bestand, die auf Werkseinstellungen zurückgesetzt wurden. Bei dieser Art der kontaktlosen Übertragung erfolgt der Datenaustausch zwischen zwei Geräten über die Nahfeldkommunikation (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.

afw#xenmobile

Die Registrierungsmethode wird nach Einschalten eines neuen oder werkseitig zurückgesetzten Geräts für die Ersteinrichtung verwendet. Die Benutzer geben “afw#xenmobile” ein, wenn sie zum Angeben eines Google-Kontos aufgefordert werden. Mit dieser Aktion wird Secure Hub heruntergeladen und installiert. Die Benutzer folgen anschließend den Anweisungen in Secure Hub zum Abschließen der Registrierung.

Diese Registrierungsmethode wird für die meisten Kunden empfohlen, da die aktuelle Secure Hub-Version aus Google Play heruntergeladen wird. Im Gegensatz zu anderen Registrierungsmethoden wird Secure Hub nicht zum Herunterladen vom XenMobile-Server bereitgestellt.

Voraussetzungen:

- Wird auf allen Android-Geräten ab Android 5.0 unterstützt.

QR-Code

Sie registrieren ein Gerät per QR-Code im Gerätemodus, indem Sie zunächst eine JSON-Datei erstellen und diese in einen QR-Code umwandeln. Der QR-Code wird mit der Gerätekamera gescannt, um das Gerät zu registrieren.

Voraussetzungen:

- Wird auf allen Android-Geräten ab Android 7.0 unterstützt.

Erstellen eines QR-Codes aus einer JSON-Datei

Erstellen Sie eine JSON-Datei mit den folgenden Feldern.

Diese Felder sind erforderlich:

Schlüssel: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Wert: com.zenprise/com.zenprise.configuration.AdminFunction

Schlüssel: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Wert: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Schlüssel: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Wert: `https://path/to/securehub.apk`

> **Hinweis:**
>
> Falls Secure Hub als Unternehmensapp auf dem Citrix XenMobile Server hochgeladen wird, kann der Download über `https://<fqdn>:4443/*instanceName*/worxhome.apk` erfolgen. Der Pfad zur APK-Datei für Secure Hub muss über das Wi-Fi-Netzwerk erreichbar sein, mit dem das Gerät während des Provisioning verbunden ist.

Diese Felder sind optional:

- **android.app.extra.PROVISIONING_LOCALE:** Geben Sie den Sprach- und den Ländercode ein.

  Sprachcodes sind nach ISO 639-1 definierte ISO-Sprachcodes, die aus zwei Kleinbuchstaben bestehen (z. B. en). Ländercodes sind nach ISO 3166-1 definierte ISO-Ländercodes, die aus zwei Großbuchstaben bestehen(z. B. US). Geben Sie z. B. de_DE für Deutsch/Deutschland ein.

- **android.app.extra.PROVISIONING_TIME_ZONE:** die Zeitzone, in der das Gerät ausgeführt wird.

  Geben Sie einen Namen im Format Gebiet/Ort ein. Beispiel: America/Los_Angeles für Pacific Time. Wenn Sie keine Zeitzone eingeben, wird sie automatisch eingetragen.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Zeit in Millisekunden seit der Unix-Epoche.

  Die Unix-Zeit (auch POSIX-Zeit oder Unix-Zeitstempel) ist die Anzahl der Sekunden, die seit der Epoche, d. h. dem 1. Januar 1970 (Mitternacht UTC-GMT), verstrichen sind. Schaltsekunden werden nicht mitgezählt (in ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Wenn Sie dies auf **true** festlegen, wird die Verschlüsselung während der Profilerstellung übersprungen. Wählen Sie **False**, um die Verschlüsselung während der Profilerstellung zu erzwingen.

Eine JSON-Datei sieht in etwa wie folgt aus:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "                                                ",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Überprüfen Sie die JSON-Datei mit einem JSON-Validierungstool (z. B. https://jsonlint.com). Konvertieren Sie die JSON-Zeichenfolge mit einem beliebigen QR-Code-Generator (z. B. https://goqr.me) in einen QR-Code.

Der QR-Code wird von einem auf Werkseinstellungen zurückgesetzten Gerät gescannt, um das Gerät im Modus für vom Unternehmen verwaltete Geräte zu registrieren.

Registrieren des Geräts

Um ein Gerät als vollständig verwaltetes Gerät zu registrieren, muss es auf die Werkseinstellungen zurückgesetzt sein.

1. Tippen Sie sechsmal auf den Begrüßungsbildschirm, um die Registrierung per QR-Code zu starten.
2. Verbinden Sie das Gerät nach Aufforderung mit dem WiFi-Netzwerk. Über das WiFi-Netzwerk wird dann per QR-Code (codiert in der JSON-Datei) auf den Download-Speicherort von Secure Hub zugegriffen.

   Sobald das Gerät mit dem WiFi verbunden ist, lädt es ein Google-Programm zum Lesen des QR-Codes herunter und aktiviert die Kamera.
3. Halten Sie die Kamera über den QR-Code, um ihn zu scannen.

   Android lädt Secure Hub vom Speicherort im QR-Code herunter, validiert die Signatur des Signaturzertifikats, installiert Secure Hub und legt die App als Gerätebesitzer fest.

Weitere Informationen finden Sie in diesem Google-Handbuch für Android EMM-Entwickler: https://developers.google.com/android/work/prov-devices#qr_code_method.

NFC-Übertragung

Um ein Gerät per NFC-Funktion als vollständig verwaltetes Gerät zu registrieren, sind zwei Geräte erforderlich: Ein Gerät, das auf die Werkseinstellungen zurückgesetzt wurde, und ein Gerät, auf dem das XenMobile Provisioning Tool ausgeführt wird.

Voraussetzungen:

- Wird auf allen Android-Geräten mit Android 5.0, 5.1, 6.0 und höher unterstützt.

- Eine XenMobile Server-Version 10.4, die für Android Enterprise aktiviert ist.
- Ein neues oder auf die Werkseinstellungen zurückgesetztes Gerät, das für Android Enterprise als vollständig verwaltetes Gerät 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 10.4 und auf der Citrix Downloadseite verfügbar.

Jedes Gerät kann nur ein Android Enterprise-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.

Per NFC übertragene Daten

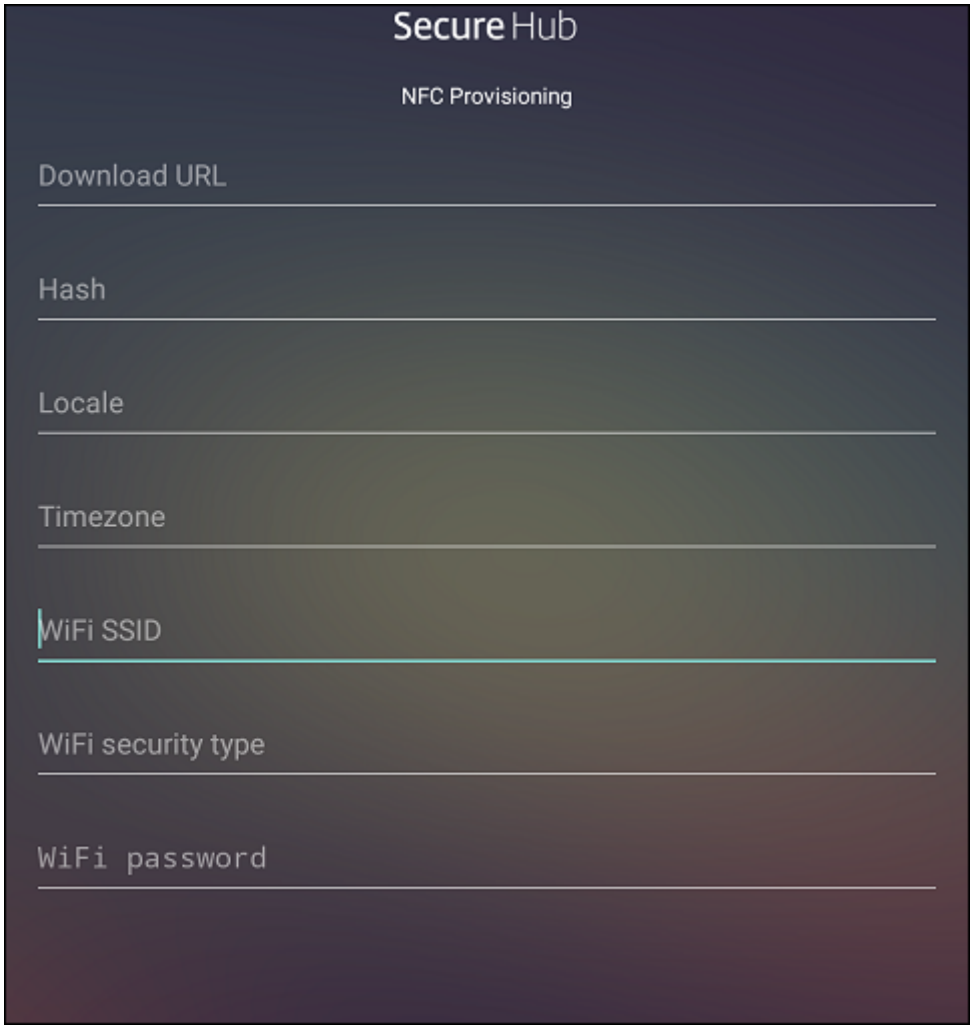
Für das Provisioning eines auf Werkseinstellungen zurückgesetzten Geräts müssen Sie die folgenden Daten per NFC senden, damit Android Enterprise initialisiert wird:

- Paketname der EMM-Anbieter-App, die als Gerätebesitzer fungiert (in diesem Fall Secure Hub).
- Intranet-/Internetspeicherort, von dem das Gerät die EMM-Anbieter-App herunterlädt.
- SHA1-Hash der EMM-Anbieter-App, um zu überprüfen, ob der Download erfolgreich ist.
- Wi-Fi-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=<download_location>`

Dies ist der Intranet-/Internetspeicherort der EMM-Anbieter-App. Wenn das auf Werkseinstellungen zurückgesetzte Gerät nach der NFC-Übertragung eine Wi-Fi-Verbindung 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=<SHA1 hash>

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=<wifi ssid>

Dies ist die Wi-Fi-SSID des Geräts, auf dem das Provisioning Tool ausgeführt wird.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

Es werden WEP und WPA2 unterstützt. Wenn das WiFi nicht geschützt ist, muss dieses Feld leer sein.

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

Wenn das WiFi nicht geschützt ist, muss dieses Feld leer sein.

android.app.extra.PROVISIONING_LOCALE=<locale>

Geben Sie die Sprach- und Ländercodes ein. Sprachcodes sind nach ISO 639-1 definierte ISO-Sprachcodes, die aus zwei Kleinbuchstaben bestehen (z. B. en). Ländercodes sind nach ISO 3166-1 definierte ISO-Ländercodes, die aus zwei Großbuchstaben bestehen(z. B. US). 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=<timezone>

Die Zeitzone, in der das Gerät ausgeführt wird. Geben Sie einen Namen im Format Gebiet/Ort ein. Beispiel: America/Los_Angeles für Pacific Time. Wenn Sie keine Zeitzone eingeben, wird sie automatisch eingetragen.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**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 Wi-Fi könnte die Datei nfcprovisioning.txt wie folgt aussehen:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=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=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Abrufen der Secure Hub-Prüfsumme

Wenn Sie die Prüfsumme einer App abrufen möchten, fügen Sie die App als Unternehmensapp hinzu.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps** und dann auf **Hinzufügen**.

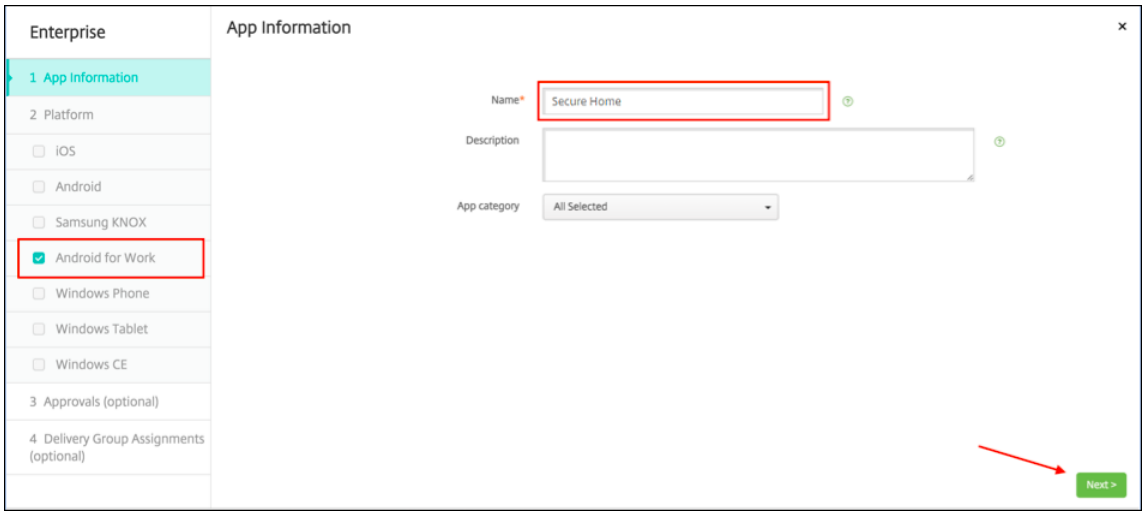
   Das Fenster **Apps hinzufügen** wird angezeigt.

2. Klicken Sie auf **Enterprise**.

   Die Seite **App-Informationen** wird angezeigt.

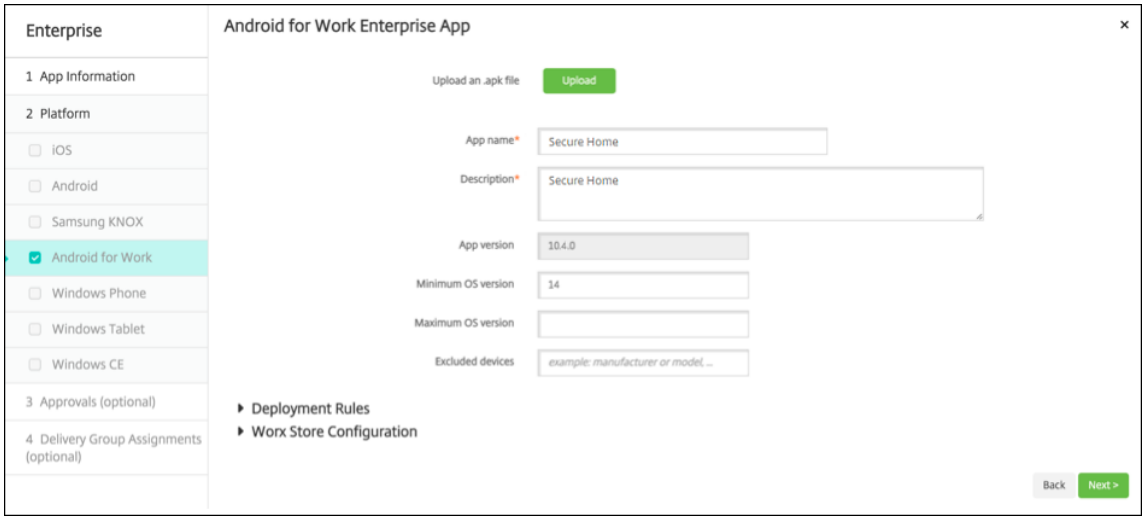
3. Wählen Sie die folgende Konfiguration und klicken Sie auf **Weiter**.

   Die Seite **Android Enterprise-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**, um die Seite zum Herunterladen der JSON-Datei für den Upload in Google Play aufzurufen. Für Secure Hub ist kein Upload in Google Play erforderlich, aber Sie benötigen die JSON-Datei, um den SHA1-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 muss URL-geeignet sein.

   - Konvertieren Sie alle **+**-Symbole in **-**
   - Konvertieren Sie alle **/**-Symbol in **_**
   - Ersetzen Sie **\u003d** am Ende 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, Design Support Library und v7 Palette Library von Google unter Apache 2.0-Lizenz

  Weitere Informationen finden Sie im Handbuch zur Support Library Features Guide.

- Butter Knife von Jake Wharton unter Apache-Lizenz 2.0

Provisioning von Arbeitsprofilgeräten in Android Enterprise

Auf Arbeitsprofilgeräten in Android Enterprise können Sie private und geschäftliche Bereiche sicher voneinander trennen. BYOD-Geräte können beispielsweise als Arbeitsprofilgerät verwendet werden. Die Registrierung im Arbeitsprofilgeräte ähnelt der Android-Registrierung in XenMobile. Die Benutzer laden Secure Hub aus Google Play herunter und registrieren ihre Geräte.

Standardmäßig sind die Einstellungen USB-Debugging und Unbekannte Quellen auf einem Gerät deaktiviert, wenn Sie es bei Android Enterprise als Arbeitsprofilgerät registrieren.

> **Tipp:**
>
> Beim Registrieren von Geräten als Arbeitsprofilgerät in Android Enterprise wechseln Sie stets zu Google Play. Aktivieren Sie dort Secure Hub, das dann im persönlichen Profil des Benutzers angezeigt wird.

iOS

January 5, 2022

Zum Verwalten von iOS-Geräten in XenMobile Server müssen Sie ein Zertifikat von Apple für den Apple-Dienst für Push-Benachrichtigungen (Apple Push Notification service, APNs) einrichten. Weitere Informationen finden Sie unter APNs-Zertifikate.

Registrierungsprofile bestimmen, ob iOS-Geräte bei MDM+MAM registriert werden und die Benutzer ggf. MDM abwählen können. XenMobile Server unterstützt die folgenden Authentifizierungstypen für iOS-Geräte in MDM+MAM. Weitere Informationen finden Sie in den Artikeln unter Zertifikate und Authentifizierung.

- Domäne
- Domäne plus Sicherheitstoken
- Clientzertifikat
- Clientzertifikat plus Domäne

> **Anforderungen für vertrauenswürdige Zertifikate in iOS 13:**
>
> Apple hat neue Anforderungen für TLS-Serverzertifikate. Stellen Sie sicher, dass alle Zertifikate den neuen Apple-Anforderungen entsprechen. Siehe Apple-Veröffentlichung https://support.apple.com/en-us/HT210176. Hilfe zum Verwalten von Zertifikaten finden Sie unter Hochladen von Zertifikaten in XenMobile Server.

Informationen zu unterstützten Betriebssystemen finden Sie unter Unterstützte Gerätebetriebssysteme.

Kompatibilität mit iOS 14

XenMobile Server und mobile Citrix Apps sind mit iOS 14 kompatibel, unterstützen aber derzeit keine neuen iOS 14-Features.

Bei betreuten iOS-Geräten können Sie Software-Upgrades um bis zu 90 Tage verzögern. Verwenden Sie in der Einschränkungsrichtlinie für iOS die folgenden Einstellungen:

- **Verzögerte Softwareupdates erzwingen**
- **Erzwungene Verzögerung für Softwareupdate**

Siehe iOS-Einstellungen. Diese Einstellungen sind für Geräte im Benutzerregistrierungsmodus oder im nicht betreuten Modus (vollständiges MDM) nicht verfügbar.

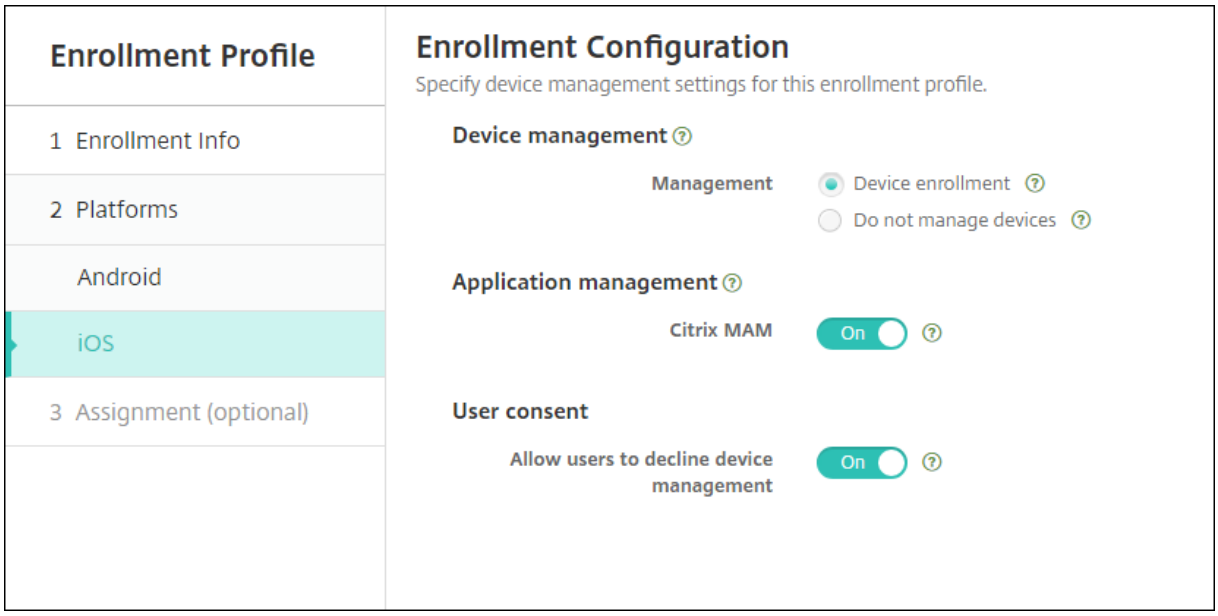
Apple-Hostnamen, die offen bleiben müssen

Einige Apple-Hostnamen müssen offen bleiben, um den ordnungsgemäßen Betrieb von iOS, macOS und Apple App Store sicherzustellen. Das Blockieren dieser Hostnamen kann sich auf die Installation, Aktualisierung und den ordnungsgemäßen Betrieb von iOS, iOS-Apps, MDM-Betrieb und Geräte- und App-Registrierung auswirken. Weitere Informationen finden Sie unter https://support.apple.com/en-us/HT201999.

Unterstützte Registrierungsmethoden

Über Registrierungsprofile legen Sie fest, wie iOS-Geräte verwaltet werden. Sie können die Geräteregistrierung auswählen oder sich gegen die MDM-Registrierung entscheiden.

Um Registrierungseinstellungen für iOS-Geräte zu konfigurieren, gehen Sie **zu Konfigurieren > Registrierungsprofile > iOS**.



In der folgenden Tabelle sind die Registrierungsmethoden aufgelistet, die XenMobile Server für iOS-Geräte unterstützt:

Methode	Unterstützt
Apple-Bereitstellungsprogramm	Ja
Apple School Manager	Ja
Apple Configurator	Ja
Manuelle Registrierung	Ja
Registrierungseinladungen	Ja

Apple bietet Programme zur Geräteregistrierung (DEP = Device Enrollment Program) für Unternehmen und Bildungseinrichtungen an. Für Unternehmenskonten müssen Sie sich beim Apple-Bereitstellungsprogramm registrieren, um das Apple-DEP zum Registrieren und Verwalten von Geräten in XenMobile Server zu verwenden. Das Programm wird für iOS und macOS-Geräte angeboten. Siehe Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm.

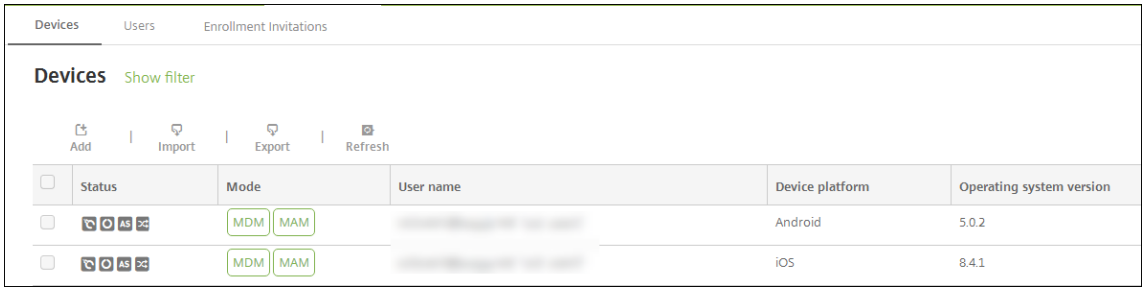
Für Bildungskonten erstellen Sie ein Apple School Manager-Konto. Bei Apple School Manager sind das Deployment Program und Volume Purchase kombiniert. Apple School Manager ist ein Apple-Bereitstellungsprogramm für Bildungseinrichtungen. Weitere Informationen finden Sie unter Integration von Apple Bildung-Features.

Sie können das Apple-Bereitstellungsprogramm für die Massenregistrierung von iOS- und macOS-Geräten verwenden. Sie können diese Geräte direkt bei Apple, einem autorisierten Apple-Vertriebspartner oder einem Netzbetreiber zu kaufen. Sie können auch den Apple Configurator zum Registrieren von iOS-Geräten verwenden. Dabei spielt es keine Rolle, ob die Geräte direkt bei Apple erworben wurden. Weitere Informationen finden Sie unter Massenregistrierung von Apple-Geräten.

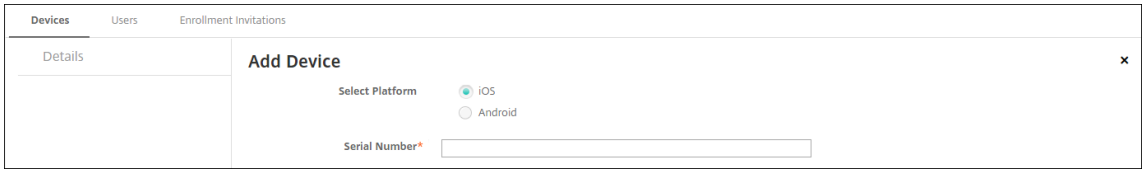
Manuelles Hinzufügen eines iOS-Geräts

Führen Sie folgende Schritte aus, um ein iOS-Gerät manuell hinzuzufügen (beispielsweise zu Testzwecken).

1. Klicken Sie in der XenMobile Server-Konsole auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.



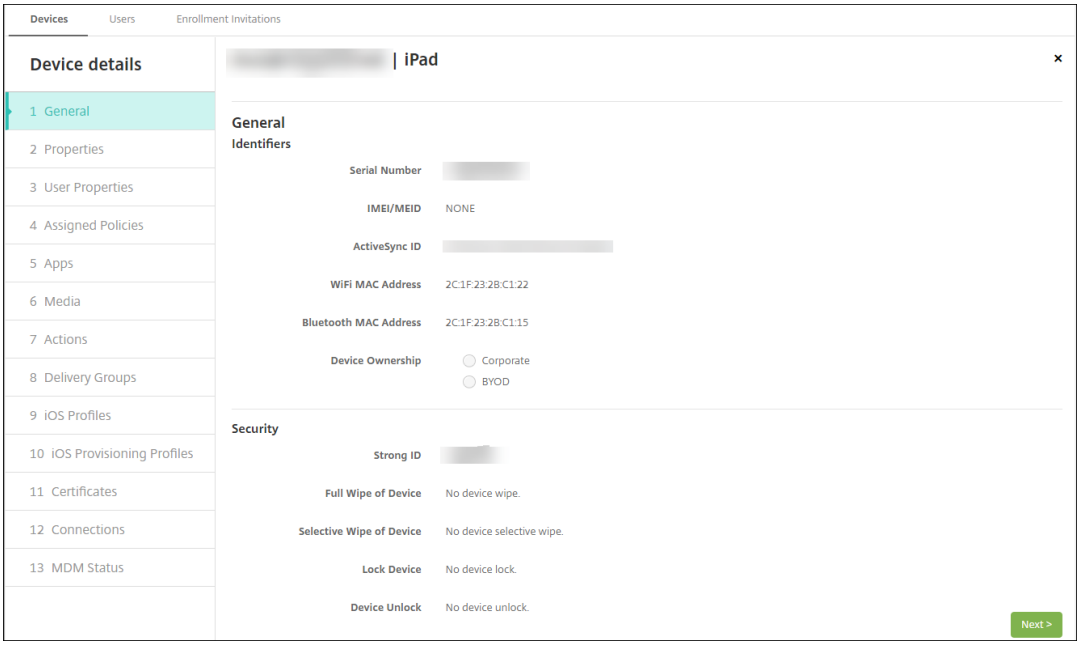
2. Klicken Sie auf **Hinzufügen**. Die Seite **Gerät hinzufügen** wird angezeigt.



3. Konfigurieren Sie folgende Einstellungen:
   - **Plattform wählen:** Klicken Sie auf **iOS**.
   - **Seriennummer:** Geben Sie die Seriennummer des Geräts ein.
4. Klicken Sie auf **Hinzufügen**. Die Tabelle **Geräte** wird angezeigt. Das hinzugefügte Gerät befindet sich am Ende der Liste. Um die Gerätedetails zu überprüfen, wählen Sie das hinzugefügte Gerät aus und klicken Sie in dem nun angezeigten Menü auf **Bearbeiten**.

> **Hinweis:**
>
> Wenn Sie das Kontrollkästchen neben einem Gerät aktivieren, wird das Menü mit den Optionen oberhalb der Liste angezeigt. Wenn Sie an eine andere Stelle in der Liste klicken, wird das Menü mit den Optionen rechts daneben angezeigt.

- LDAP konfiguriert
- Bei Verwendung lokaler Gruppen und Benutzer:
  - Eine oder mehrere lokale Gruppen
  - Lokale Benutzer, die lokalen Gruppen zugewiesen sind
  - Bereitstellungsgruppen, die lokalen Gruppen zugeordnet sind
- Bei Verwendung von Active Directory:
  - Bereitstellungsgruppen, die Active Directory-Gruppen zugeordnet sind



5. Auf der Seite **Allgemein** werden **Gerätekennungen** aufgeführt, z. B. die Seriennummer und weitere plattformspezifische Informationen. Wählen Sie für **Gerätebesitz** die Option **Unternehmen** oder **BYOD**.

   Auf der Seite **Allgemein** werden zudem **Sicherheitseigenschaften** aufgeführt, z. B. starke ID, Gerätesperrung, Umgehen der Aktivierungssperre und weitere plattformspezifische Informationen. Das Feld **Gerät vollständig löschen** enthält den Benutzer-PIN-Code. Der Benutzer muss den Code eingeben, anschließend erfolgt die Löschung. Wenn der Benutzer den Code vergessen hat, können Sie ihn hier nachsehen.

6. Auf der Seite **Eigenschaften** werden die von XenMobile Server 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 aus. Gültige Werte für jede Eigenschaft finden Sie in der PDF Device property names and values.

   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. XenMobile Server löscht das Element sofort.

7. Die verbleibenden Abschnitte mit **Gerätedetails** enthalten zusammenfassende Informationen zu dem Gerät.

   - **Benutzereigenschaften:** Zeigt RBAC-Rollen, Gruppenmitgliedschaften, Volume Purchase-Konten und Eigenschaften des Benutzers an. Auf dieser Seite können Sie

ein Volume Purchase-Konto deaktivieren.

- **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 fehlgeschlagenen App-Bereitstellungen der letzten Bestandsaufnahme an. Es werden App-Name, ID, Typ und weitere Informationen angezeigt. Eine Beschreibung von iOS- und macOS-Bestandsschlüsseln, z. B. **HasUpdateAvailable**, finden Sie unter Mobile Device Management (MDM) Protocol.
- **Medien:** zeigt die Anzahl der erfolgreichen, ausstehenden und fehlgeschlagenen Medienbereitstellungen der letzten Bestandsaufnahme an.
- **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 aus, 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 Verwaltungsstatus.
- **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.
- **MDM-Status:** zeigt Informationen wie MDM-Status, Zeitpunkt der letzten Pushbenachrichtigung und letzte Geräteantwortzeit an.

Konfigurieren von iOS-Geräterichtlinien

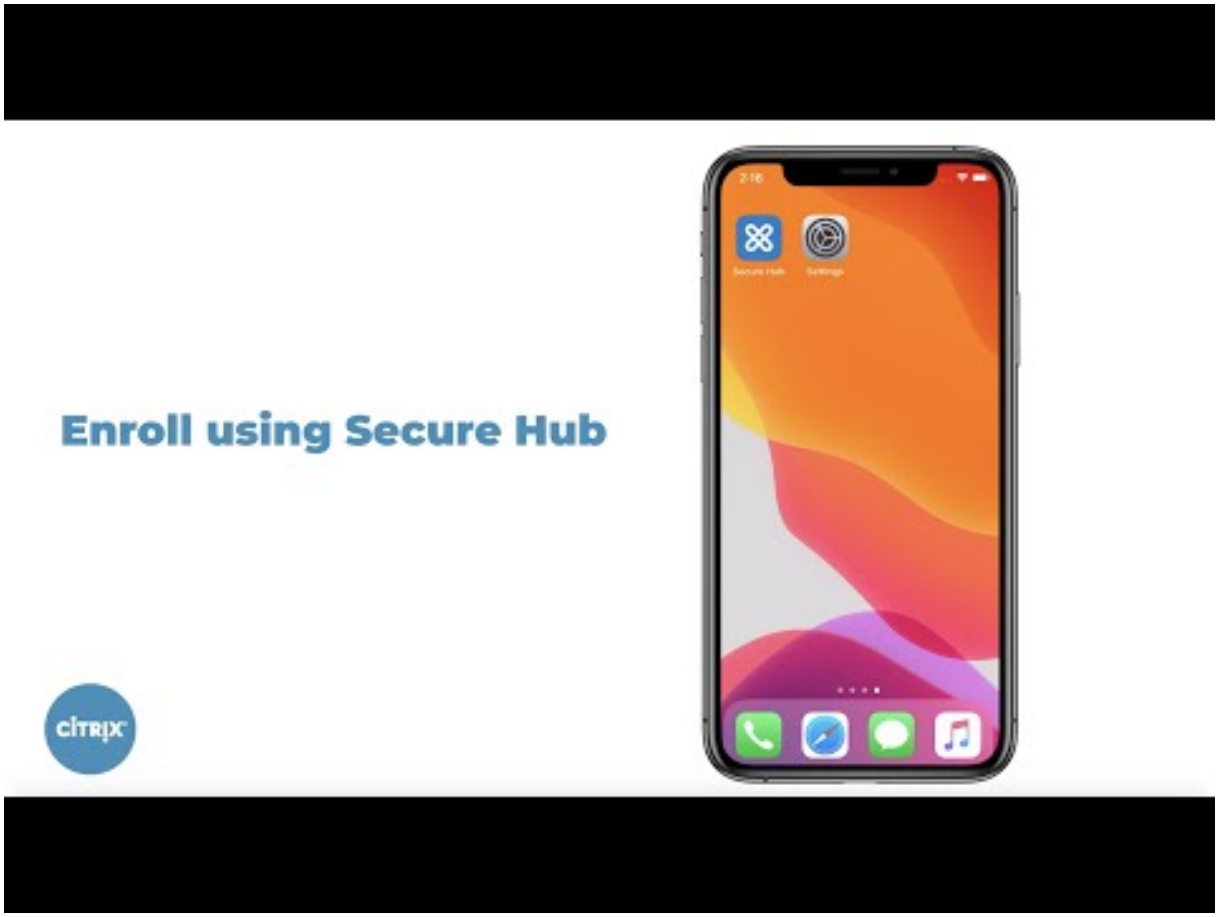
Verwenden Sie diese Richtlinien, um zu konfigurieren, wie XenMobile Server mit Geräten mit iOS interagiert. In dieser Tabelle sind alle für iOS-Geräte verfügbaren Geräterichtlinien aufgeführt.

AirPlay-Synchronisierung	AirPrint	APN
App-Zugriff	App-Attribute	App-Konfiguration

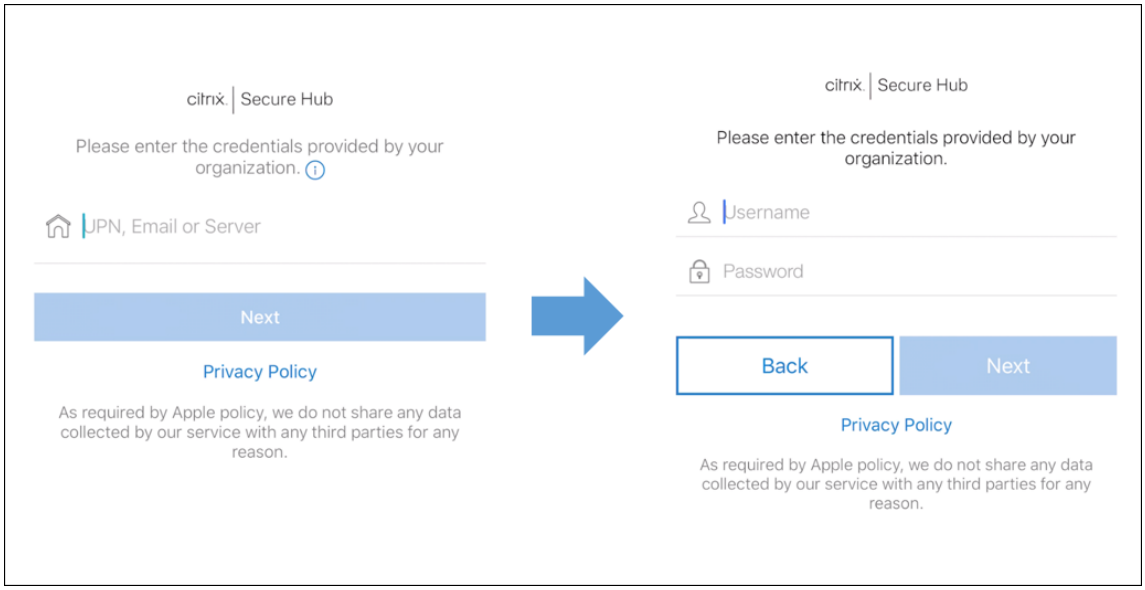
App-Bestand	App-Sperre	App-Netzwerkauslastung
App-Deinstallation	App-Benachrichtigungen	Kalender (CalDAV)
Mobilfunk	Kontakte (CardDAV)	OS-Update steuern
Anmeldeinformationen	Gerätename	Bildungseinrichtung - Konfiguration
Exchange	Schriftart	Layout für Homebildschirm
Importieren von iOS- und macOS-Profilen	LDAP	Standort
E-Mail	Verwaltete Domänen	MDM-Optionen
Informationen zum Unternehmen	Passcode	Persönlicher Hotspot
Profilentfernung	Provisioningprofil	Entfernen des Provisioningprofils
Proxy	Einschränkungen	Roaming
SCEP	Geteiltes iPad - maximale Anzahl residenter Benutzer	Geteiltes iPad - Kulanzzeitraum für Passcodesperre
SSO-Konto	Store	Abonnierte Kalender
AGB	VPN	Hintergrundbild
Webinhaltsfilter	Webclip	Wi-Fi

Registrieren von iOS-Geräten

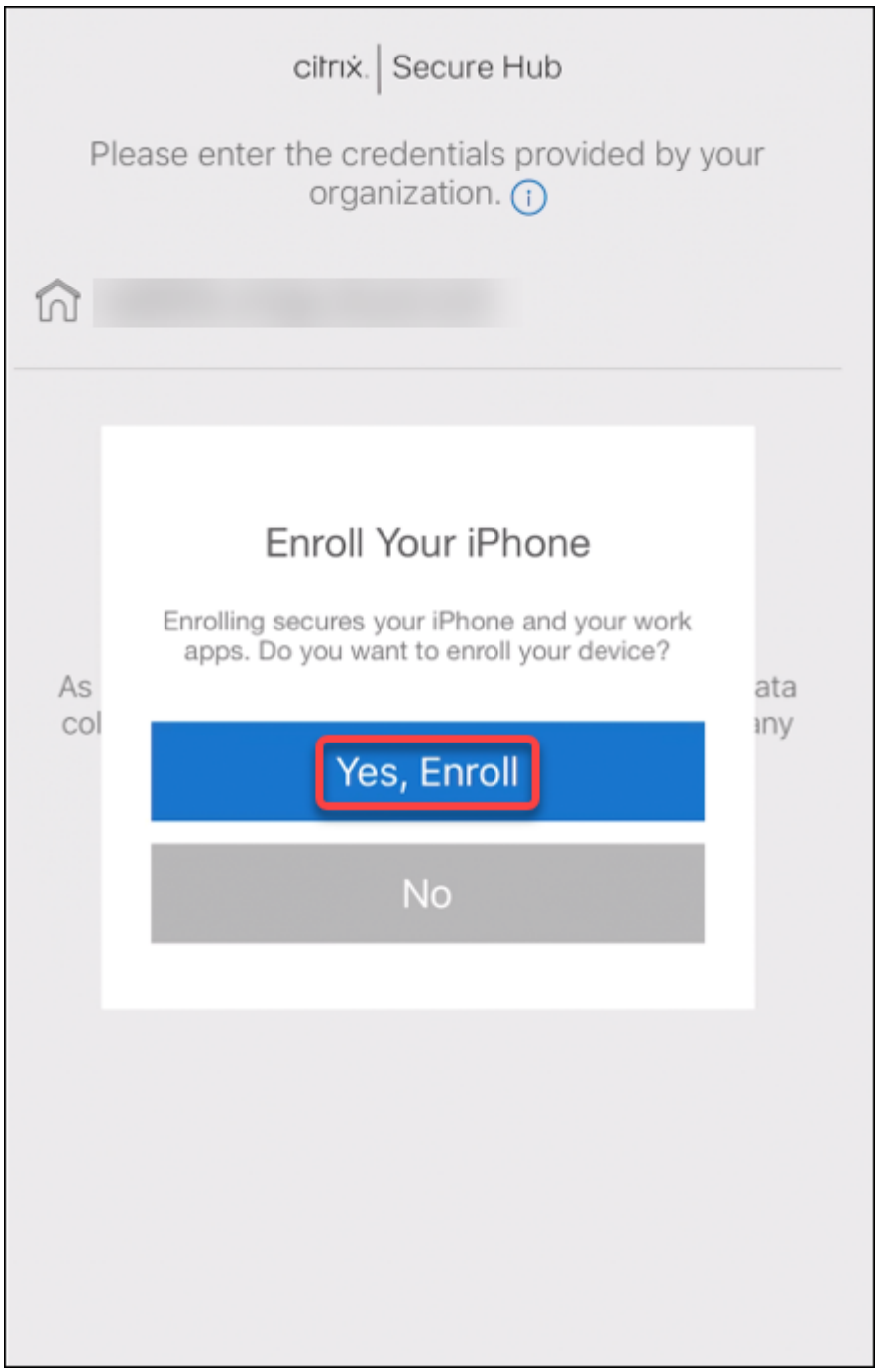
In diesem Abschnitt wird erläutert, wie Benutzer iOS-Geräte (12.2 oder höher) in XenMobile Server registrieren. Weitere Informationen zur iOS-Registrierung finden Sie in folgendem Video:



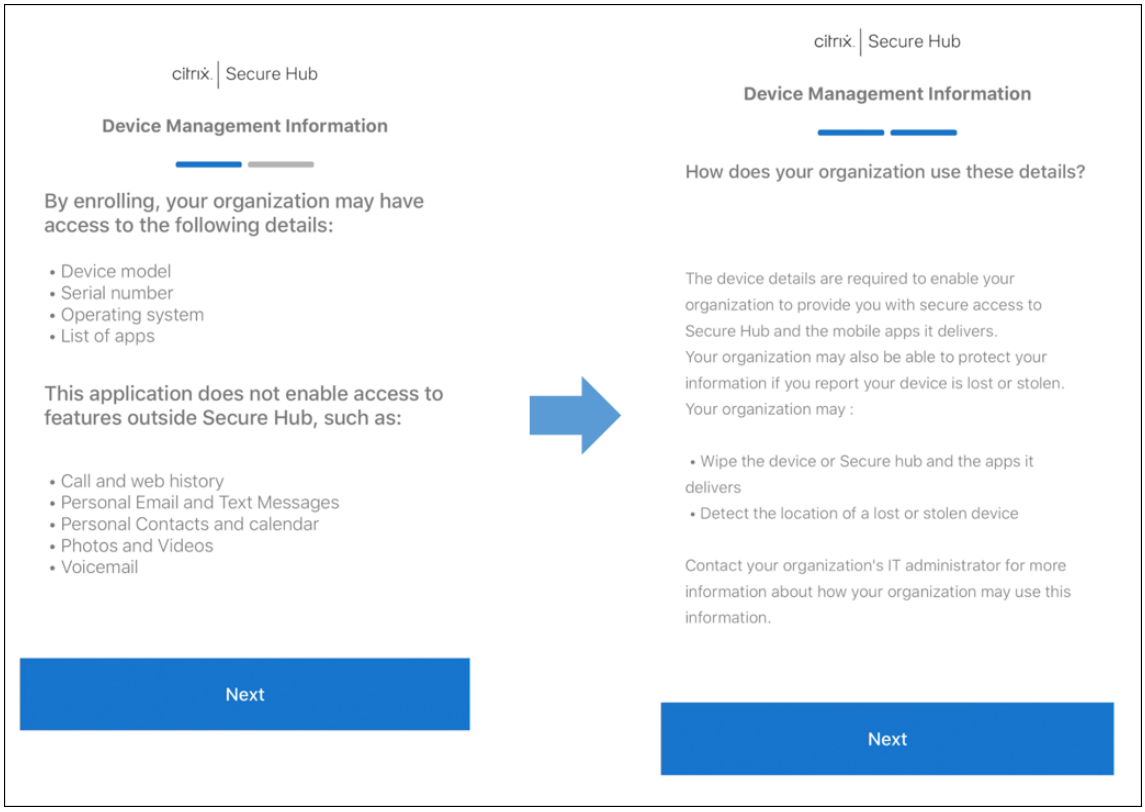
1. Rufen Sie auf dem iOS-Gerät den Apple-Store auf, laden Sie die Citrix Secure Hub-App herunter und tippen Sie auf die App.
2. Wenn Sie aufgefordert werden, die App zu installieren, tippen Sie auf **Weiter** und dann auf **Installieren**.
3. Wenn Secure Hub installiert ist, tippen Sie auf **Öffnen**.
4. Geben Sie Ihre geschäftlichen Anmeldeinformationen ein, z. B. den Namen des XenMobile Server-Servers, Ihren Benutzerprinzipalnamen oder Ihre E-Mail-Adresse. Klicken Sie dann auf **Weiter**.



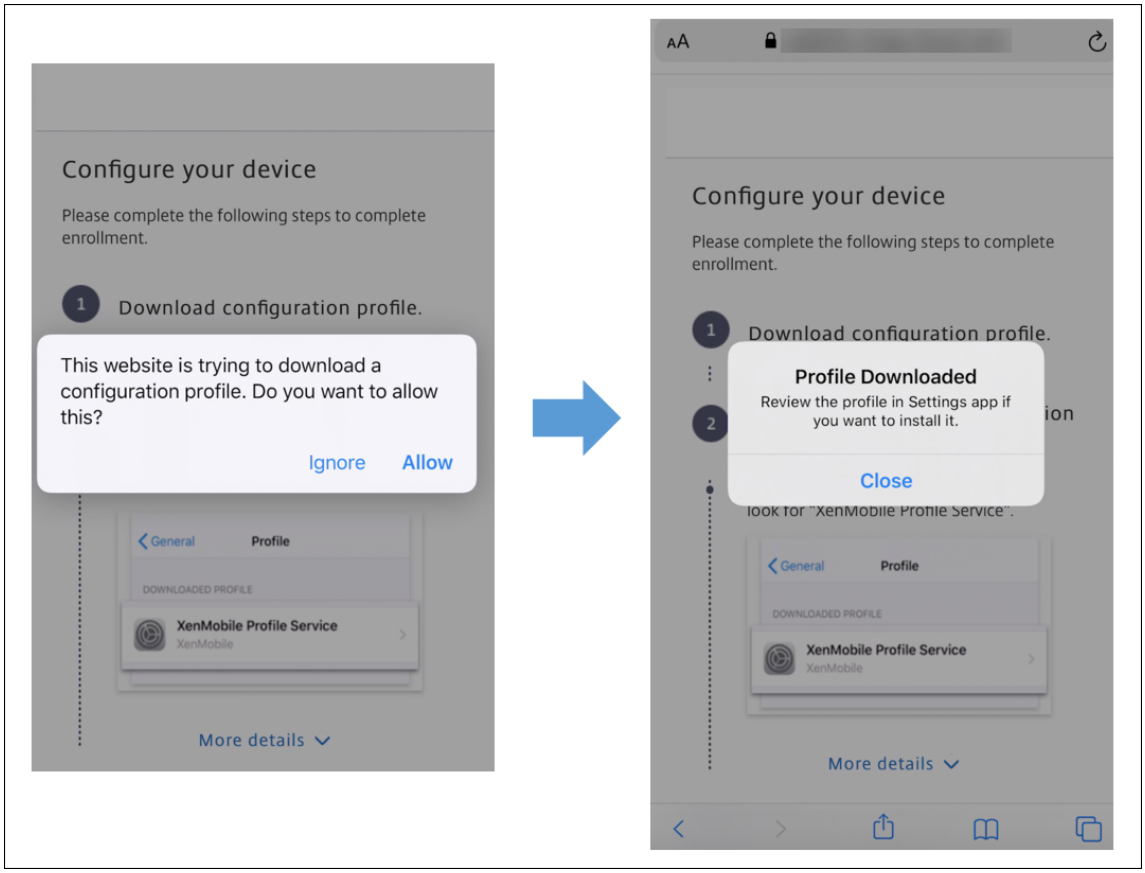
5. Tippen Sie auf **Ja, Registrieren**, um Ihr iOS-Gerät zu registrieren.



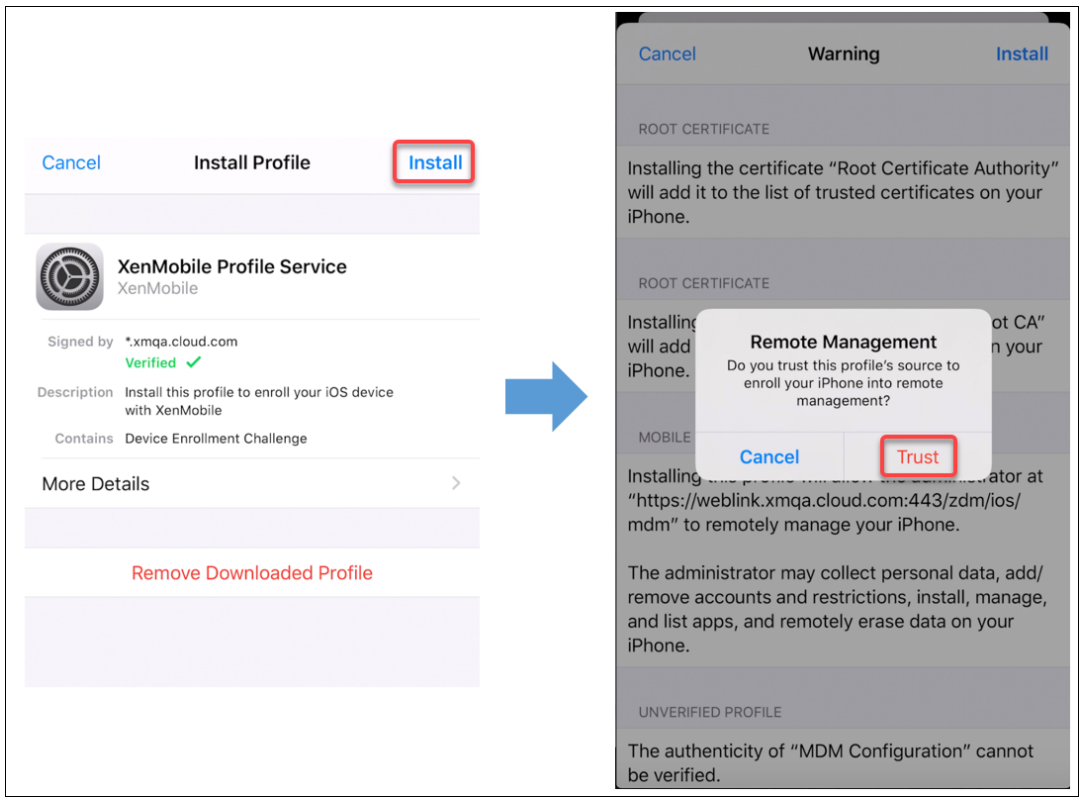
6. Eine Liste der von XenMobile Server erfassten Daten wird angezeigt. Klicken Sie auf **Weiter**. Eine Erläuterung, wie die Daten von der Organisation verwendet werden, wird angezeigt. Klicken Sie auf **Weiter**.



7. Nach Eingabe der Anmeldeinformationen tippen Sie auf **Zulassen**, wenn Sie dazu aufgefordert werden, um das Konfigurationsprofil herunterzuladen. Tippen Sie nach dem Herunterladen des Konfigurationsprofils auf **Schließen**.



8. Installieren Sie das iOS-Zertifikat in den Geräteeinstellungen und fügen Sie das Gerät der Vertrauensliste hinzu.
    - Zum Hinzufügen des Profils gehen Sie zu **Einstellungen > Allgemein > Profil > XenMobile Profile Service** und tippen auf **Installieren**.
    - Tippen Sie im Benachrichtigungsfenster auf **Vertrauensstellung**, um Ihr Gerät bei der Remoteverwaltung zu registrieren.



9. Öffnen Sie nach erfolgreicher Registrierung Secure Hub. Wenn Sie sich bei MDM+MAM registrieren, werden zunächst Ihre Anmeldeinformationen überprüft. Danach werden Sie aufgefordert, Ihre Citrix-PIN zu erstellen und diese zu bestätigen.
10. Nach Abschluss des Workflows ist das Gerät registriert. Sie können nun auf den App-Store zugreifen und Apps für die Installation auf dem iOS-Gerät anzeigen.

Sicherheitsaktionen

iOS unterstützt die folgenden Sicherheitsaktionen. Eine Beschreibung der einzelnen Sicherheitsaktionen finden Sie unter Sicherheitsaktionen.

Aktivierungssperre umgehen	App-Sperre	App löschen
ASM-Aktivierungssperre	Zertifikaterneuerung	Einschränkungen deaktivieren
Modus "Verloren" aktivieren/deaktivieren	Tracking aktivieren/deaktivieren	Vollständig löschen
Suchen	Sperren	Klingeln
AirPlay-Synchronisierung anfordern/beenden	Neustart/Herunterfahren	Wiederrufen/Autorisieren

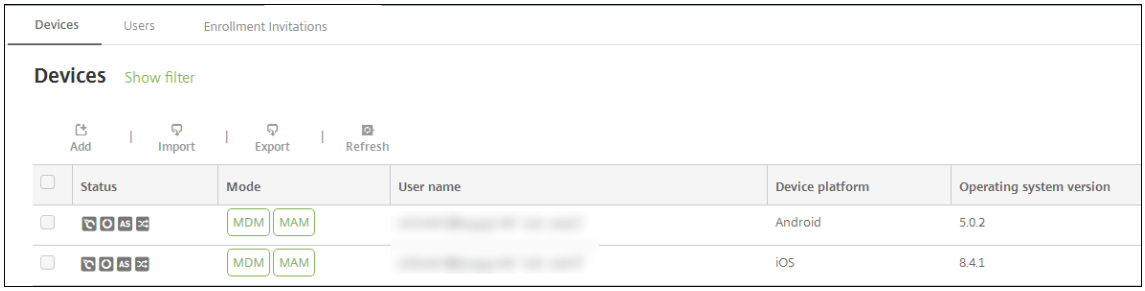
Selektiv löschen	Unlock

Sperren von iOS-Geräten

Sie können ein verlorenes iOS-Gerät sperren und eine entsprechende Nachricht und Telefonnummer auf dem Sperrbildschirm anzeigen lassen.

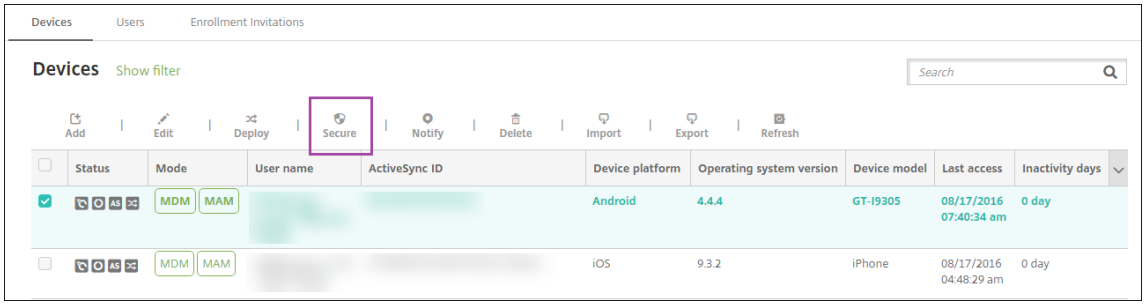
Zum Anzeigen einer Nachricht und Telefonnummer auf einem gesperrten Gerät muss die Richtlinie Passcode in der XenMobile Server-Konsole auf **wahr** festgelegt werden. Alternativ können Benutzer den Passcode auf dem Gerät auch manuell aktivieren.

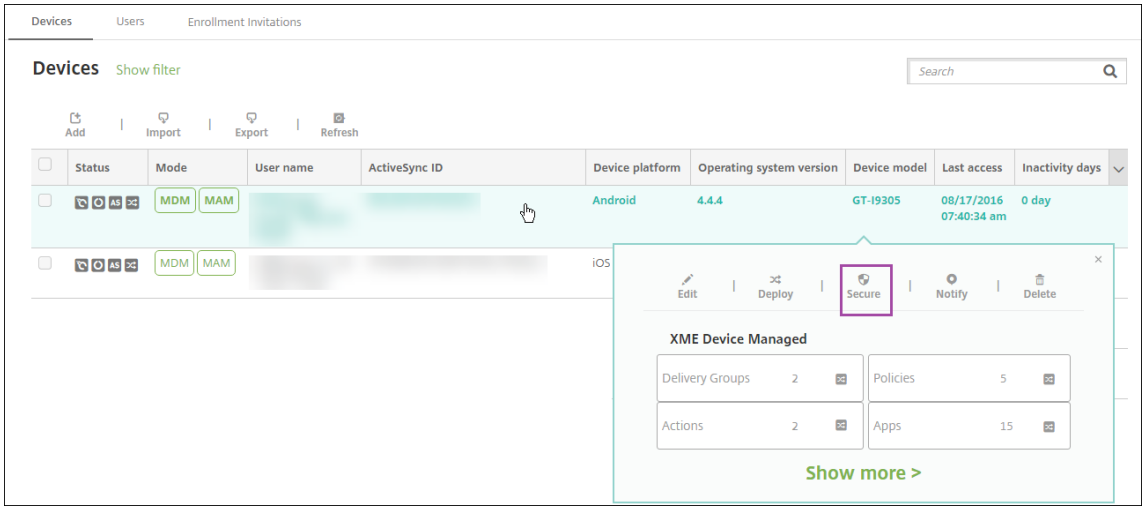
1. Klicken Sie auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.



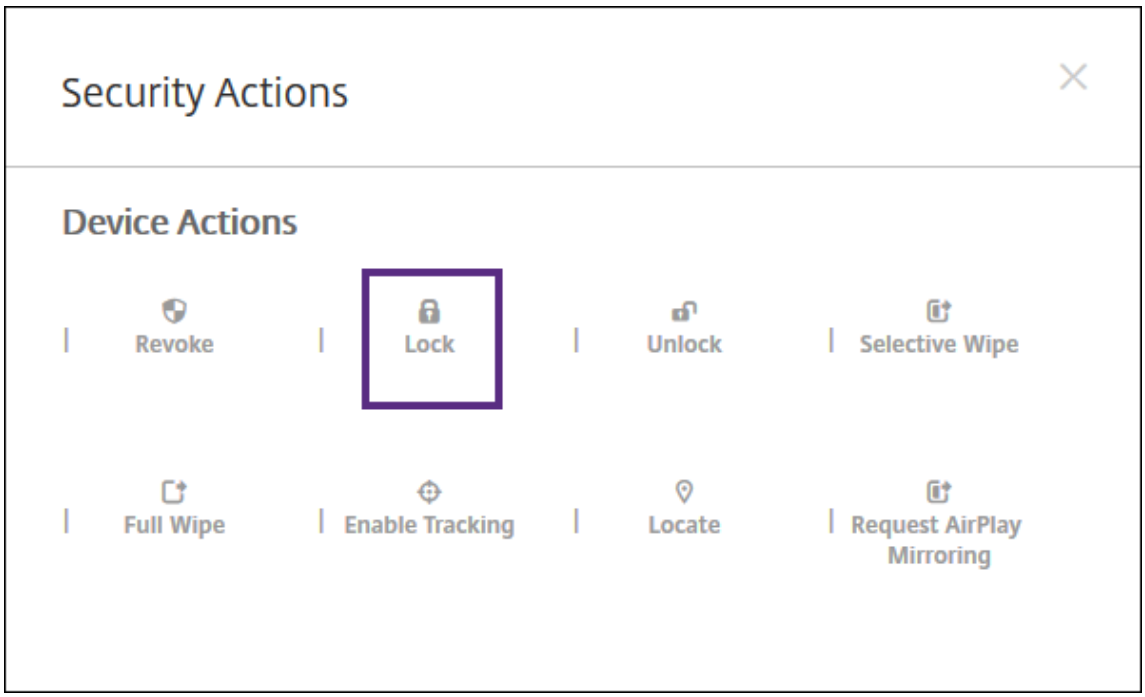
2. Wählen Sie das iOS-Gerät aus, das Sie sperren möchten.

   Aktivieren Sie das Kontrollkästchen neben einem Gerät, um das Menü mit den Optionen oberhalb der Liste anzuzeigen. Klicken Sie an eine andere Stelle in der Liste, um das Menü mit den Optionen rechts daneben anzuzeigen.

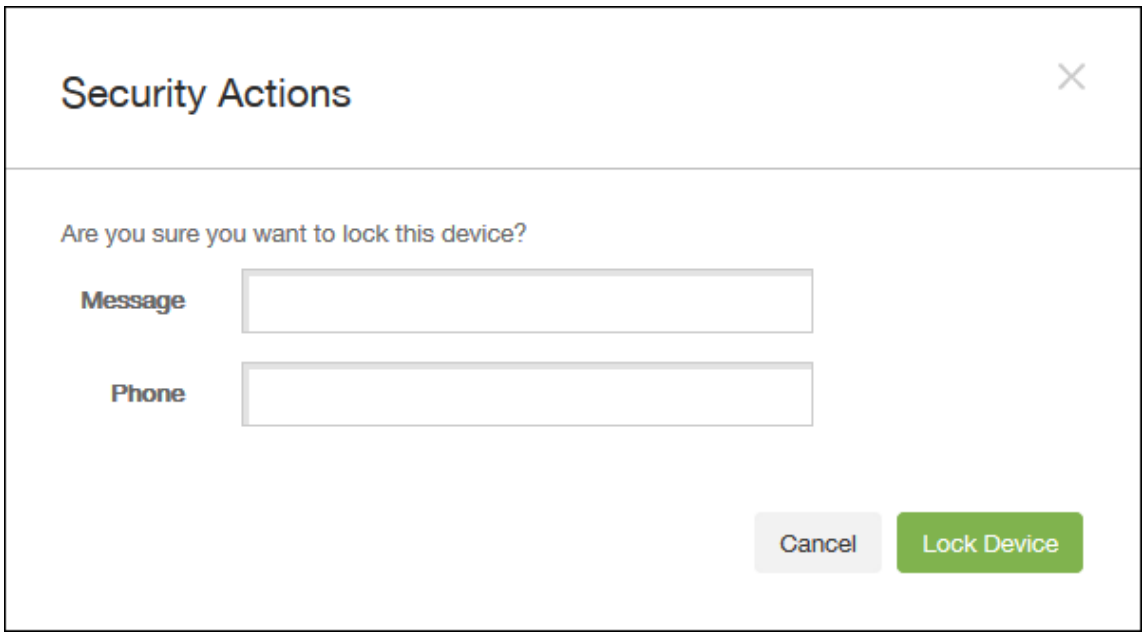




3. Wählen Sie im Menü “Optionen” die Option **Sicherheit**. Das Dialogfeld **Sicherheitsaktionen** wird angezeigt.



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.

   iOS hängt die Wörter “Lost iPad” an alles an, was Sie im Feld **Nachricht** eingeben.

   Wenn Sie das Feld **Nachricht** leer lassen und eine Telefonnummer angeben, wird die Meldung “Besitzer anrufen” auf dem Sperrbildschirm des Geräts angezeigt.

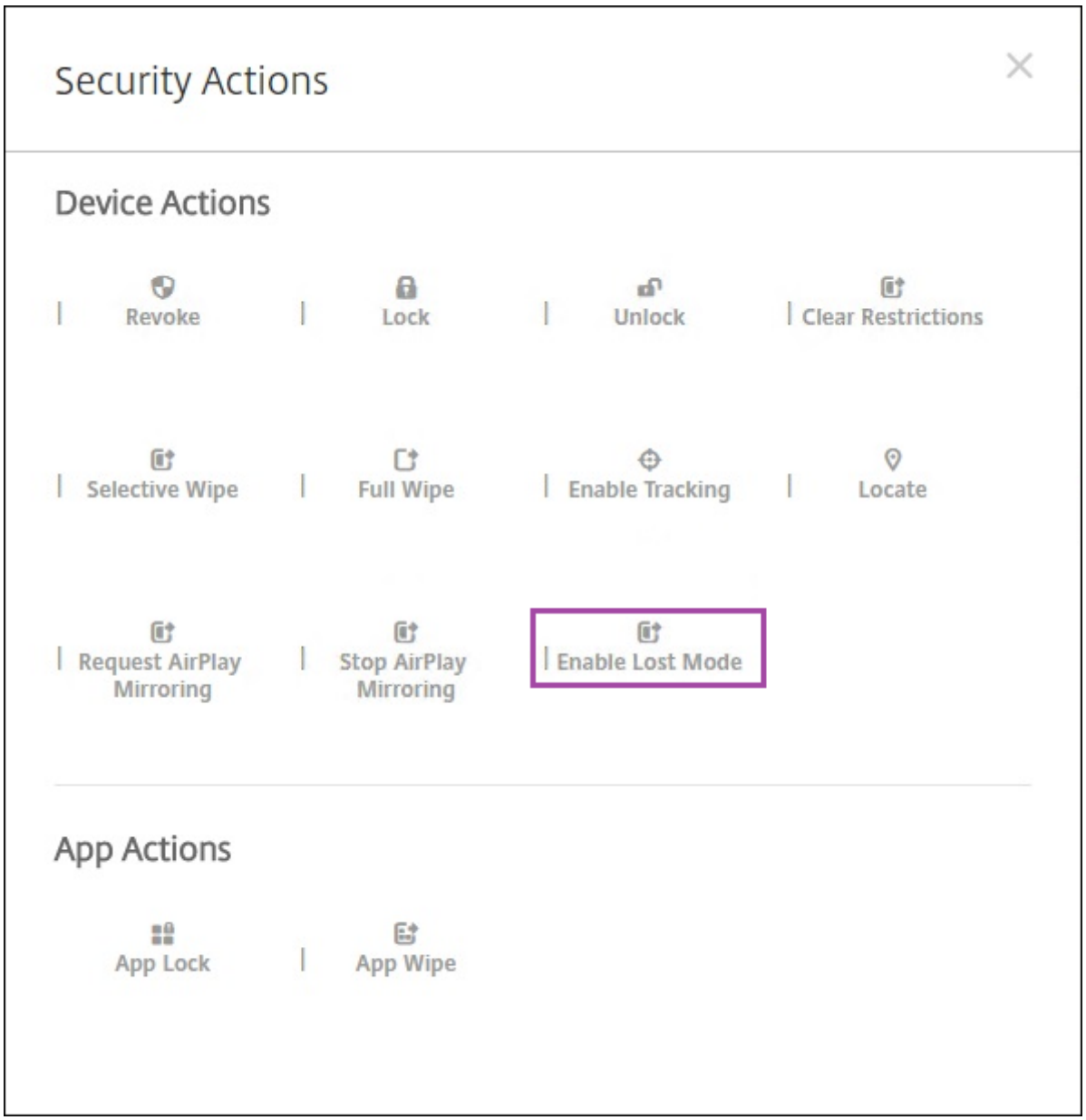
6. Klicken Sie auf **Gerät sperren**.

Versetzen von iOS-Geräten in den Modus “Verloren”

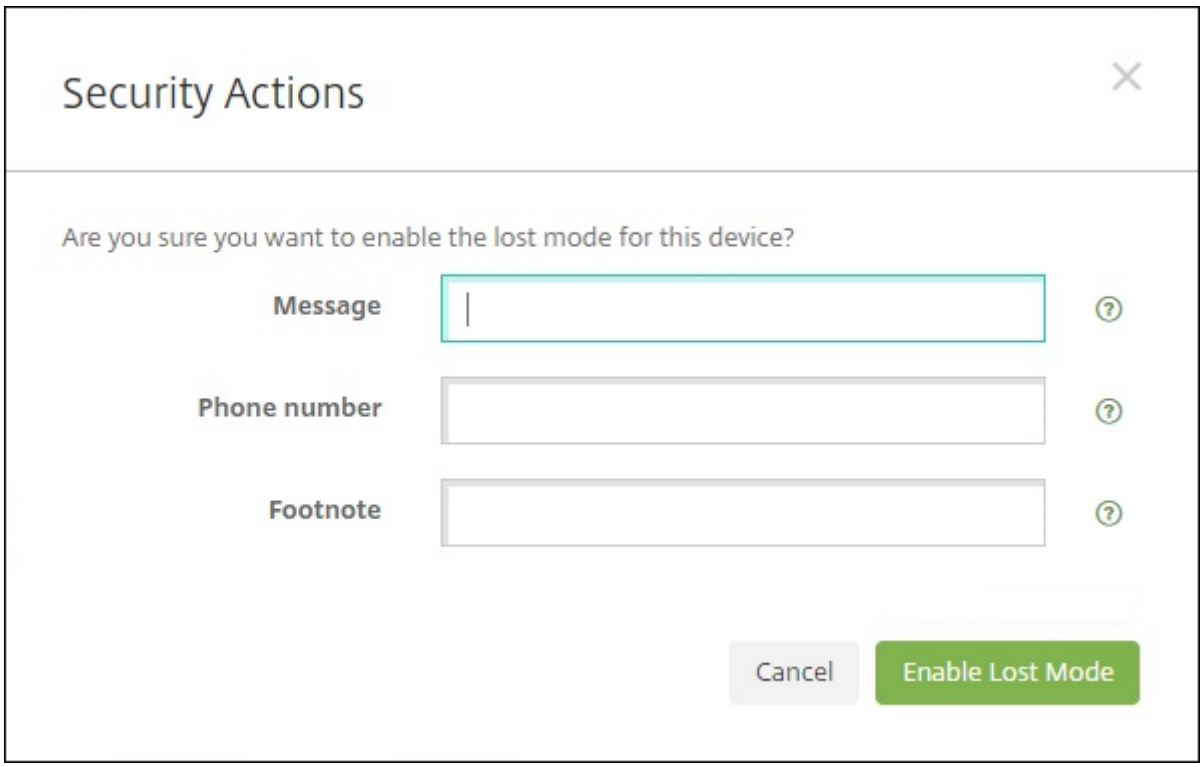
Die Geräteeigenschaft “XenMobile Server-Modus ‘Verloren”’ versetzt iOS-Geräte in den Modus “Verloren”. Im Gegensatz zum von Apple verwalteten Modus “Verloren” muss ein Benutzer beim Modus “Verloren” in XenMobile Server keine der folgenden Aktionen ausführen, um sein Gerät zu suchen: Konfigurieren der Einstellung **Find My iPhone/iPad** oder Aktivieren der Ortungsdienste für Citrix Secure Hub.

Im XenMobile Server-Modus “Verloren” kann ein Gerät nur über XenMobile Server entsperrt werden. (Wenn Sie hingegen das XenMobile Server-Feature zum Sperren von Geräten verwenden, können die Benutzer Geräte direkt durch Eingabe eines von Ihnen bereitgestellten PIN-Codes entsperren.)

Aktivieren oder Deaktivieren des Modus “Verloren”: Gehen Sie zu **Verwalten > Geräte**, wählen Sie ein betreutes iOS-Gerät aus und klicken Sie auf **Sicherheit**. Klicken Sie dann auf **Modus ‘Verloren’ aktivieren** oder **Modus ‘Verloren’ deaktivieren**.

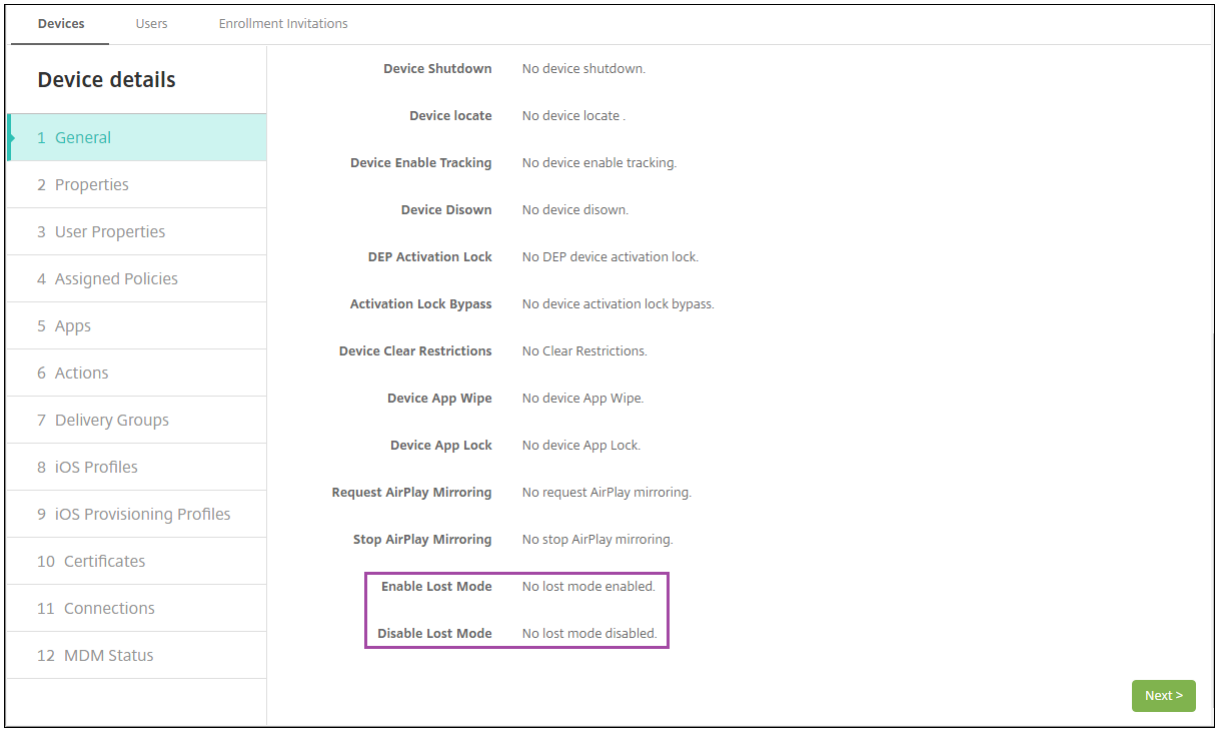


Wenn Sie auf **Modus 'Verloren' aktivieren** klicken, geben Sie die Informationen ein, die auf dem Gerät angezeigt werden sollen, wenn es im Modus "Verloren" ist.

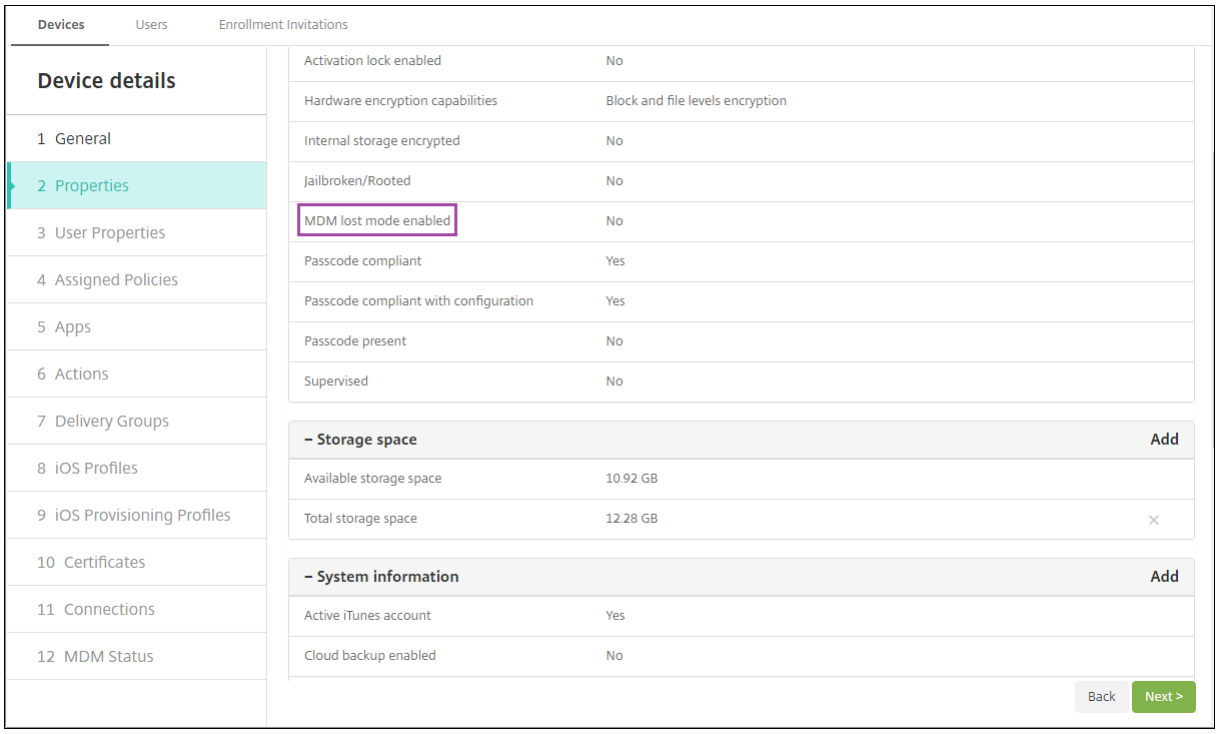


Verwenden Sie eine der folgenden Methoden, um den Status des Modus “Verloren” zu überprüfen:

- Überprüfen Sie im Fenster **Sicherheitsaktionen**, ob die Schaltfläche auf **Modus ‘Verloren’ deaktivieren** gesetzt ist.
- Zeigen Sie über **Verwalten > Geräte** auf der Registerkarte **Allgemein** unter **Sicherheit** die letzte Aktion zum Aktivieren oder Deaktivieren des Modus “Verloren” an.



- Überprüfen Sie unter **Verwalten > Geräte** auf der Registerkarte **Eigenschaften**, ob die Einstellung **MDM-Modus “Verloren” aktiviert** richtig festgelegt ist.



Wenn Sie den XenMobile Server-Modus “Verloren” auf iOS-Geräten aktivieren, ändert sich die XenMobile Server-Konsole wie folgt:

- In der über **Konfigurieren > Aktionen** aufgerufenen Liste **Aktionen** sind die folgenden automatisierten Aktionen nicht enthalten: **Gerät widerrufen**, **Gerät selektiv löschen** und **Gerät vollständig löschen**.
- In der über **Verwalten > Geräte** aufgerufenen Liste **Sicherheitsaktionen** sind die Geräteaktionen **Widerrufen** und **Selektiv löschen** nicht mehr enthalten. Sie können weiterhin eine Sicherheitsaktion verwenden, um die Aktion **Vollständig löschen** nach Bedarf auszuführen.

iOS hängt die Wörter "Lost iPad" an alles an, was Sie im Feld **Nachricht** des Bildschirms **Sicherheitsaktionen** eingeben.

Wenn Sie das Feld **Nachricht** leer lassen und eine Telefonnummer angeben, wird die Meldung "Besitzer anrufen" auf dem Sperrbildschirm des Geräts angezeigt.

Umgehen einer iOS-Aktivierungssperre

Die Aktivierungssperre ist ein Feature von "Mein iPhone/iPad suchen", mit dem das Reaktivieren von verlorenen oder gestohlenen betreuten Geräten verhindert wird. Die Aktivierungssperre erfordert die Eingabe der Apple-ID und des Benutzerkennworts, bevor ein beliebiger Benutzer "Mein iPhone/iPad suchen" deaktivieren, die Daten auf dem Gerät löschen oder das Gerät neu aktivieren kann. Für Geräte im Besitz Ihres Unternehmens kann ein Umgehen der Aktivierungssperre erforderlich sein, um Geräte zurückzusetzen oder neu zuzuweisen.

Zum Einrichten der Aktivierungssperre müssen Sie die XenMobile Server-Geräterichtlinie "MDM-Optionen" konfigurieren und bereitstellen. Dann können Sie ein Gerät über die XenMobile Server-Konsole ohne Eingabe der Apple-Anmeldeinformationen des Benutzers verwalten. Aktivieren Sie auf der XenMobile Server-Konsole die Sicherheitsaktion "Aktivierungssperre umgehen", um trotz Aktivierungssperre keine Apple-Anmeldeinformationen eingeben zu müssen.

Nehmen wir folgendes Beispiel: Ein Benutzer bringt ein verlorenes Telefon zurück oder möchte ein Gerät vor oder nach einem vollständigen Löschen einrichten. Die dabei geforderte Eingabe der Anmeldeinformationen für das Apple App Store-Konto können Sie umgehen, indem Sie in der XenMobile Server-Konsole die Sicherheitsaktion "Aktivierungssperre umgehen" aktivieren.

Geräteanforderungen für das Umgeben der Aktivierungssperre

- Betreuter Modus mit Apple Configurator oder Apple-Bereitstellungsprogramm
- Konfiguration mit iCloud-Konto
- "Mein iPhone/iPad suchen" ist aktiviert
- Bei XenMobile Server registriert
- Bereitgestellte Geräterichtlinie "MDM-Optionen" mit aktivierter Aktivierungssperre

Umgehen einer Aktivierungssperre vor dem vollständigen Löschen eines Geräts:

1. Wählen Sie unter **Verwalten > Geräte** das Gerät, klicken Sie auf **Sicherheit** und dann auf **Aktivierungssperre umgehen**.
2. Löschen Sie das Gerät. Die Aktivierungssperre wird während des Gerätesetups nicht angezeigt.

Umgehen einer Aktivierungssperre nach dem vollständigen Löschen eines Geräts:

1. Setzen Sie das Gerät zurück oder löschen Sie es. Die Aktivierungssperre wird während des Gerätesetups angezeigt.
2. Wählen Sie unter **Verwalten > Geräte** das Gerät, klicken Sie auf **Sicherheit** und dann auf **Aktivierungssperre umgehen**.
3. Tippen Sie auf dem Gerät auf die Taste "Zurück". Der Homebildschirm wird angezeigt.

Beachten Sie Folgendes:

- Fordern Sie die Benutzer auf, "Mein iPhone/iPad suchen" nicht zu deaktivieren. Löschen Sie das Gerät nicht vollständig. In beiden Fällen wird der Benutzer aufgefordert, das Kennwort des iCloud-Kontos einzugeben. Nach der Kontovalidierung wird dem Benutzer kein Bildschirm zum Aktivieren des iPhones/iPads angezeigt, nachdem alle Inhalte und Einstellungen gelöscht wurden.
- Für Geräte mit generiertem Code zum Umgehen der Aktivierungssperre und aktivierter Aktivierungssperre: Wenn Sie das Gerät vollständig löschen und danach die Aktivierungsseite für das iPhone/iPad nicht umgehen können, müssen Sie das Gerät nicht aus XenMobile Server löschen. Sie oder der Benutzer können sich direkt an den Apple-Support wenden, um das Gerät entsperren zu lassen.
- Während einer Hardwareinventur ruft XenMobile Server den Code zum Umgehen der Aktivierungssperre von einem Gerät ab. Wenn ein Umgehungscode verfügbar ist, wird er vom Gerät an XenMobile Server gesendet. Um den Umgehungscode dann vom Gerät zu entfernen, aktivieren Sie in der XenMobile Server-Konsole die Sicherheitsaktion "Aktivierungssperre umgehen". Damit haben XenMobile Server und Apple den erforderlichen Umgehungscode, um das Gerät zu entsperren.
- Die Sicherheitsaktion "Aktivierungssperre umgehen" stützt sich auf die Verfügbarkeit eines Apple-Diensts. Wenn die Aktion nicht funktioniert, können Sie ein Gerät auf folgende Weise entsperren. Geben Sie auf dem Gerät manuell die Anmeldeinformationen des iCloud-Kontos ein. Alternativ können Sie das Feld "Benutzername" leer lassen und den Umgehungscode im Feld "Kennwort" eingeben. Zum Ermitteln der Umgehungscodes wählen Sie das Gerät unter **Verwalten > Geräte** aus, klicken auf **Bearbeiten** und dann auf **Eigenschaften**. Der **Code zum Umgehen der Aktivierungssperre** steht unter **Sicherheitsinformationen**.

macOS

January 5, 2022

Zum Verwalten von macOS-Geräten in XenMobile müssen Sie ein Zertifikat von Apple für den Apple-Dienst für Push-Benachrichtigungen (Apple Push Notification service, APNs) einrichten. Weitere Informationen finden Sie unter APNs-Zertifikate.

XenMobile registriert macOS Geräte bei MDM. XenMobile unterstützt die folgenden Authentifizierungstypen für macOS-Geräte in MDM.

- Domäne
- Domäne plus Einmalkennwort
- Einladungs-URL + Einmalkennwort

> **Anforderungen für vertrauenswürdige Zertifikate in macOS 15:**
>
> Apple hat neue Anforderungen für TLS-Serverzertifikate. Stellen Sie sicher, dass alle Zertifikate den neuen Apple-Anforderungen entsprechen. Siehe Apple-Veröffentlichung https://support.apple.com/en-us/HT210176. Hilfe zum Verwalten von Zertifikaten finden Sie unter Hochladen von Zertifikaten in XenMobile.

Die macOS-Geräteverwaltung kann über folgendes Standardverfahren gestartet werden:

1. Konfigurieren der macOS-Geräterichtlinien.
2. Registrieren der macOS-Geräte.
3. Einrichten von Sicherheitsaktionen für Apps und Geräte. Weitere Informationen finden Sie unter Sicherheitsaktionen.

Informationen zu unterstützten Betriebssystemen finden Sie unter Unterstützte Gerätebetriebssysteme.

Apple-Hostnamen, die offen bleiben müssen

Einige Apple-Hostnamen müssen offen bleiben, um den ordnungsgemäßen Betrieb von iOS, macOS und Apple App Store sicherzustellen. Das Blockieren dieser Hostnamen kann sich auf die Installation, Aktualisierung und den ordnungsgemäßen Betrieb von iOS, iOS-Apps, MDM-Betrieb und Geräte- und App-Registrierung auswirken. Weitere Informationen finden Sie unter https://support.apple.com/en-us/HT201999.

Unterstützte Registrierungsmethoden

In der folgenden Tabelle werden die Registrierungsmethoden aufgelistet, die XenMobile für macOS-Geräte unterstützt:

Methode	Unterstützt
Apple-Bereitstellungsprogramm	Ja
Apple School Manager	Ja
Apple Configurator	Nein
Manuelle Registrierung	Ja
Registrierungseinladungen	Ja

Apple bietet Programme zur Geräteregistrierung (DEP = Device Enrollment Program) für Unternehmen und Bildungseinrichtungen an. Für Unternehmenskonten müssen Sie sich beim Apple-Bereitstellungsprogramm registrieren, um das Apple-DEP zum Registrieren und Verwalten von Geräten in XenMobile zu verwenden. Das Programm wird für iOS und macOS-Geräte angeboten. Siehe Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm.

Für Bildungskonten erstellen Sie ein Apple School Manager-Konto. Bei Apple School Manager sind das Deployment Program und Volume Purchase kombiniert. Apple School Manager ist ein Apple-Bereitstellungsprogramm für Bildungseinrichtungen. Weitere Informationen finden Sie unter Integration von Apple Bildung-Features.

Sie können das Apple-Bereitstellungsprogramm für die Massenregistrierung von iOS- und macOS-Geräten verwenden. Sie können diese Geräte direkt bei Apple, einem autorisierten Apple-Vertriebspartner oder einem Netzbetreiber zu kaufen.

Konfigurieren der macOS-Geräterichtlinien

Verwenden Sie diese Richtlinien, um zu konfigurieren, wie XenMobile mit Geräten mit macOS interagiert. In dieser Tabelle werden alle für macOS-Geräte verfügbaren Geräterichtlinien aufgeführt.

AirPlay-Synchronisierung	App-Bestand	Kalender (CalDAV)
Kontakte (CardDAV)	OS-Update steuern	Anmeldeinformationen
Gerätename	Exchange	FileVault
Firewall	Schriftart	Importieren von iOS- und macOS-Profilen
LDAP	E-Mail	Passcode
Profilentfernung	Einschränkungen	SCEP

VPN	Webclip	Wi-Fi

Registrieren der macOS-Geräte

XenMobile bietet zwei Registrierungsmethoden für Geräte, auf denen macOS ausgeführt wird. Beide Methoden ermöglichen macOS-Benutzern die Registrierung per Funk direkt über das Gerät.

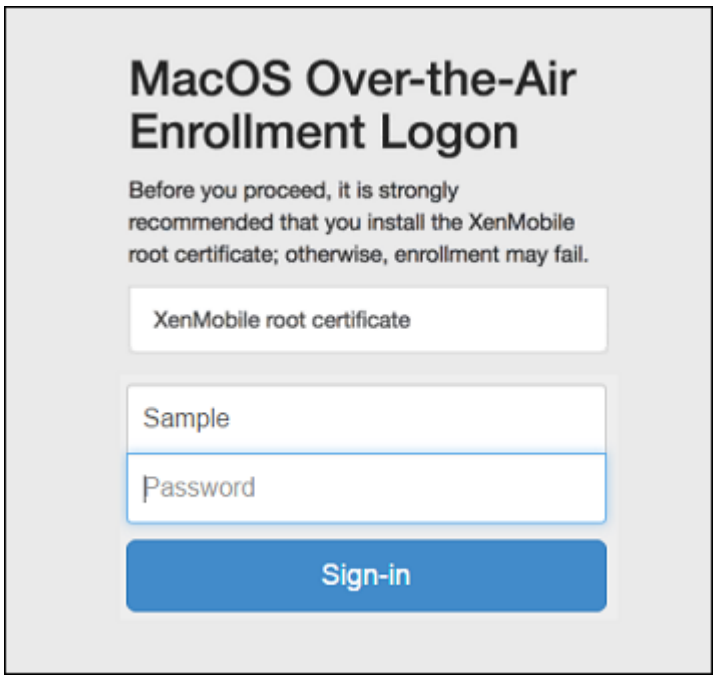
- **Senden einer Registrierungseinladung:** Bei dieser Registrierungsmethode können Sie jeden der folgenden Registrierungssicherheitsmodi für macOS-Geräte festlegen:
  - Benutzername + Kennwort
  - Benutzername + PIN
  - Zweistufige Authentifizierung

  Wenn der Benutzer die Anweisungen in der Registrierungseinladung befolgt, wird eine Registrierungsseite angezeigt, auf der sein Name bereits eingetragen ist.
- **Senden von Registrierungslinks:** Bei dieser Registrierungsmethode für macOS-Geräte erhält der Benutzer einen Registrierungslink, den er in Safari oder Chrome öffnen kann. Der Benutzer registriert sich dann mit seinem Benutzernamen und Kennwort.

  Soll die Registrierung per Installationslink auf macOS-Geräten nicht verwendet werden, legen Sie die Servereigenschaft **Enable macos.OTAE** auf **false** fest. macOS-Geräte können dann nur per Registrierungseinladung registriert werden.

Senden von Registrierungseinladungen an macOS-Benutzer

1. Fügen Sie eine Registrierungseinladung für macOS-Benutzer hinzu. Siehe Erstellen von Registrierungseinladungen.
2. Wenn ein Benutzer die Einladung erhält und auf den Link klickt, wird in Safari folgende Seite angezeigt: Der Benutzername wird von XenMobile eingetragen. Wenn Sie den Registrierungssicherheitsmodus **Zweistufig** auswählen, wird ein weiteres Feld angezeigt.



3. Die Benutzer installieren die benötigten Zertifikate. Ob Benutzer zur Installation von Zertifikaten aufgefordert werden, hängt davon ab, ob Sie ein öffentlich vertrauenswürdiges SSL-Zertifikat und ein öffentlich vertrauenswürdiges digitales Signaturzertifikat für macOS konfiguriert haben. Informationen über Zertifikate finden Sie unter Zertifikate und Authentifizierung.
4. Der Benutzer gibt die angeforderten Anmeldeinformationen ein.

   Die Mac-Geräterichtlinien werden installiert. Sie können macOS-Geräte nun mit XenMobile genauso verwalten wie Mobilgeräte.

Senden von Installationslinks an macOS-Benutzer

1. Senden Sie den Registrierungslink `https://serverFQDN:8443/instanceName/macos/otae`, den die Benutzer in Safari oder Chrome öffnen können.
   - **serverFQDN** ist 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.
   - **instanceName**, oft als `zdm` dargestellt, ist der Name, der bei der Serverinstallation angegeben wird.

   Weitere Informationen zum Senden von Installationslinks finden Sie unter Senden einer Registrierungseinladung:.

2. Die Benutzer installieren die benötigten Zertifikate. Wenn Sie ein öffentlich vertrauenswürdiges SSL-Zertifikat und ein digitales Signaturzertifikat für iOS und macOS konfiguriert haben, wird den Benutzern die Aufforderung zum Installieren von Zertifikaten angezeigt. Informationen über Zertifikate finden Sie unter Zertifikate und Authentifizierung.
3. Die Benutzer melden sich bei ihren Macs an.

   Die Mac-Geräterichtlinien werden installiert. Sie können macOS-Geräte nun mit XenMobile genauso verwalten wie Mobilgeräte.

Sicherheitsaktionen

macOS unterstützt die folgenden Sicherheitsaktionen. Eine Beschreibung der einzelnen Sicherheitsaktionen finden Sie unter Sicherheitsaktionen.

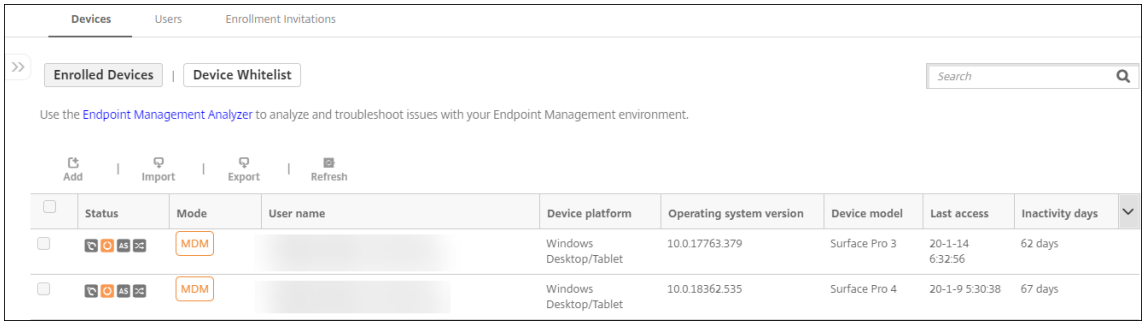
Widerrufen	Sperren	Selektiv löschen
Vollständig löschen	Zertifikaterneuerung	

Sperren von macOS-Geräten

Sie können verlorene macOS-Geräte auch remote sperren. XenMobile sperrt das Gerät. Anschließend wird ein PIN-Code generiert und im Gerät festgelegt. Für den Zugriff auf das Gerät muss die PIN eingegeben werden. Verwenden Sie **Sperren abbrechen**, um ein Gerät über die XenMobile-Konsole zu entsperren.

Mit der Geräterichtlinie Passcode können Sie weitere Einstellungen konfigurieren, die mit dem PIN-Code verknüpft sind. Weitere Informationen finden Sie unter macOS-Einstellungen.

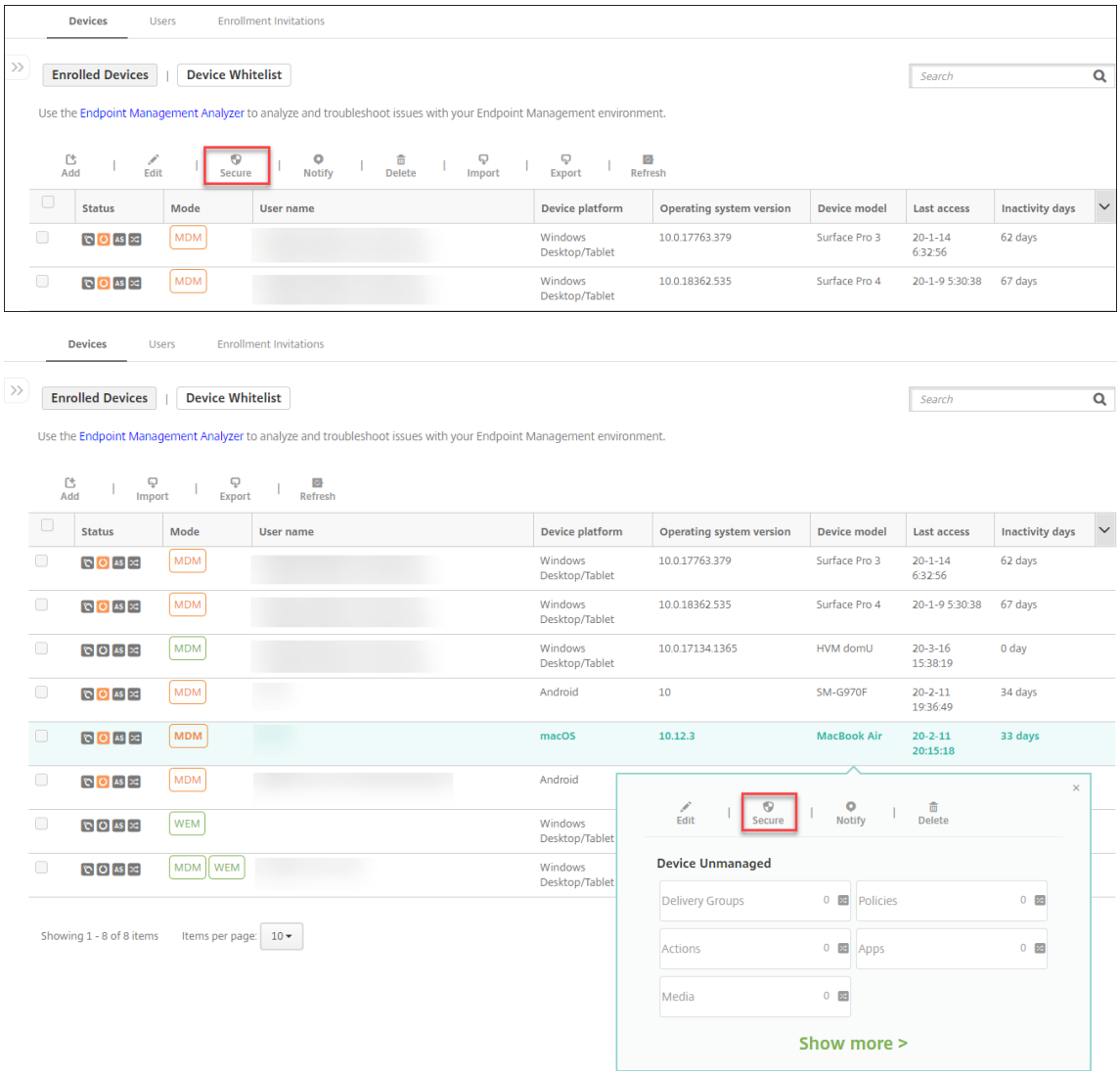
1. Klicken Sie auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.



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

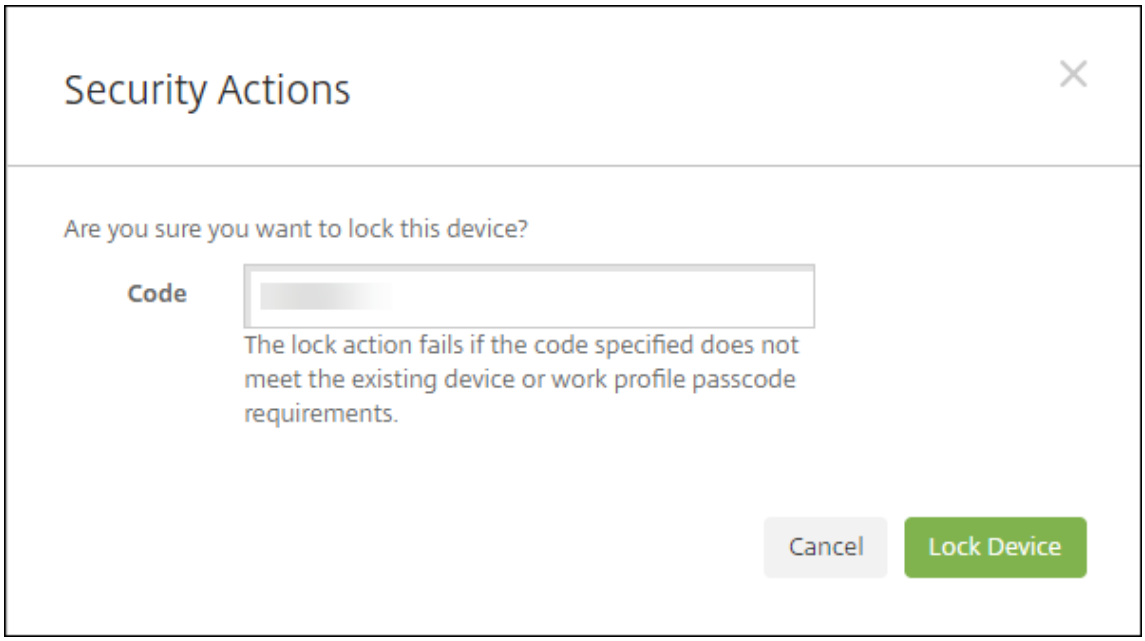
   Aktivieren Sie das Kontrollkästchen neben einem Gerät, um das Menü mit den Optionen ober-

halb der Liste anzuzeigen. Sie können auch auf ein aufgelistetes Element klicken, um das Menü mit den Optionen rechts daneben anzuzeigen.



3. Wählen Sie im Menü “Optionen” die Option **Sicherheit**. Das Dialogfeld **Sicherheitsaktionen** wird angezeigt.

4. Klicken Sie auf **Sperren**. Das Bestätigungsdialogfeld **Sicherheitsaktionen** wird angezeigt.



5. Klicken Sie auf **Gerät sperren**.

> **Wichtig:**
>
> Anstelle des von XenMobile generierten Codes können Sie auch einen Passcode festlegen. Die Sperraktion schlägt fehl, wenn der angegebene Code nicht den Passcodeanforderungen des Geräts oder vorhandenen Arbeitsprofils entspricht.

Massenregistrierung von Apple-Geräten

January 5, 2022

Es gibt zwei Möglichkeiten, um viele iOS-, iPadOS- und macOS-Geräte gleichzeitig bei XenMobile zu registrieren.

- Verwenden Sie das Apple-Bereitstellungsprogramm, um iOS-, iPadOS- und macOS-Geräte zu registrieren, die Sie direkt bei Apple, einem autorisierten Apple-Wiederverkäufer oder einem Netzbetreiber erworben haben. Dies gilt auch für geteilte iPads. XenMobile unterstützt das Apple-Bereitstellungsprogramm für Apple Business Manager (ABM) und Apple School Manager (ASM) für Bildungseinrichtungen. Dieser Artikel beschreibt, wie Sie mehrere Geräte in Ihr ABM-Konto integrieren. Informationen zur Registrierung bei ABM und zum Verbinden Ihres ABM-Kontos mit XenMobile finden Sie unter Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm. Informationen zu Apple School Manager-Konten finden Sie unter Integration von Apple Bildung-Features.

  Für die Registrierung von macOS-Geräten erfordert XenMobile, dass auf diesen Geräten macOS 10.10 oder höher ausgeführt wird.

- Sie können auch Apple Configurator 2 zum Registrieren von iOS-Geräten verwenden. Dabei spielt es keine Rolle, ob die Geräte direkt bei Apple erworben wurden.

Mit ABM:

- Die Geräte müssen nicht vorbereitet werden. Stattdessen übermitteln Sie die Seriennummern oder Bestellnummern der Geräte über ABM, um die Geräte zu konfigurieren und zu registrieren.
- Nachdem die Geräte von XenMobile registriert wurden, können Sie sie Benutzern aushändigen, die die Geräte dann direkt verwenden können. Durch das Einrichten von Geräten per ABM können Sie einige Schritte im Setupassistenten eliminieren, die die Benutzer beim ersten Starten ihres Geräts ausführen müssten.
- Weitere Informationen zum Einrichten von ABM finden Sie in der Dokumentation unter Apple Business Manager.

Verwendung von Apple Configurator 2:

- Sie fügen iOS-Geräte an einen Apple-Computer unter macOS 10.7.2 oder höher sowie an die Apple Configurator 2-App an. Sie bereiten die iOS-Geräte vor und konfigurieren Richtlinien über Apple Configurator 2.
- Nach dem Bereitstellen der Geräte mit den erforderlichen Richtlinien erhalten die Geräte beim ersten Verbindungsaufbau mit XenMobile Richtlinien von XenMobile. Sie können dann mit dem Verwalten der Geräte beginnen.
- Weitere Informationen über die Verwendung von Apple Configurator 2 finden Sie in der Apple Configurator-Hilfe.

Voraussetzungen

Öffnen Sie die erforderlichen Ports für die Verbindung zwischen XenMobile und Apple. Weitere Informationen finden Sie unter Portanforderungen.

Integrieren des Apple Business Manager-Kontos in XenMobile

Wenn Sie kein ABM-Konto bei XenMobile eingerichtet haben, führen Sie die folgenden Schritte zum Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm aus.

- Registrierung bei Apple Business Manager
- Verbinden des Apple Business Manager-Kontos mit XenMobile
- Bestellen von Bereitstellungsprogramm-fähigen Geräten
- Verwalten von Bereitstellungsprogramm-fähigen Geräten

Festlegen eines Standardservers für die Massenregistrierung

Um einem MDM-Server viele iOS-, iPadOS- und macOS-Geräte gleichzeitig zuzuweisen, können Sie XenMobile als Standardserver festlegen.

1. Melden Sie sich als Administrator oder Geräteregistrierungsverwalter bei Apple Business Manager an.
2. Klicken Sie in der Randleiste auf **Settings > Device Management Settings**.
3. Wählen Sie einen vorhandenen MDM-Server. Klicken Sie unter **Default Device Assignment** auf **Change**. Wählen Sie den XenMobile-Standardserver für jeden Gerätetyp. Klicken Sie auf **Fertig**.

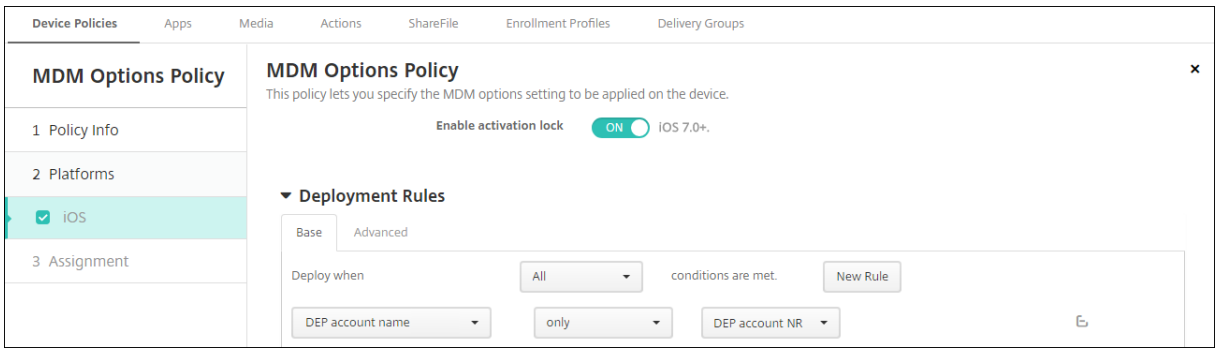
Konfigurieren der Bereitstellungsregeln von Geräterichtlinien und Apps für ABM-Konten

Sie können ABM-Konten mit verschiedenen Geräterichtlinien und Apps verknüpfen, indem Sie den Abschnitt **Bereitstellungsregeln** unter **Konfigurieren > Geräterichtlinien** und **Konfigurieren > Apps** verwenden. Sie können für eine Richtlinie oder App Folgendes festlegen:

- Wird nur für ein bestimmtes ABM-Konto bereitgestellt.
- Wird auf allen ABM-Konten mit Ausnahme des ausgewählten Kontos bereitgestellt.

Die Liste der ABM-Konten enthält nur Konten mit dem Status “Aktiviert” oder “Deaktiviert”. Wenn das ABM-Konto deaktiviert ist, gehört das ABM-Gerät nicht zu diesem Konto. Deshalb stellt XenMobile die App oder Richtlinie nicht auf dem Gerät bereit.

In folgendem Beispiel wird eine Geräterichtlinie ausschließlich auf Geräten mit dem ABM-Kontonamen “ABM Account NR” bereitgestellt.

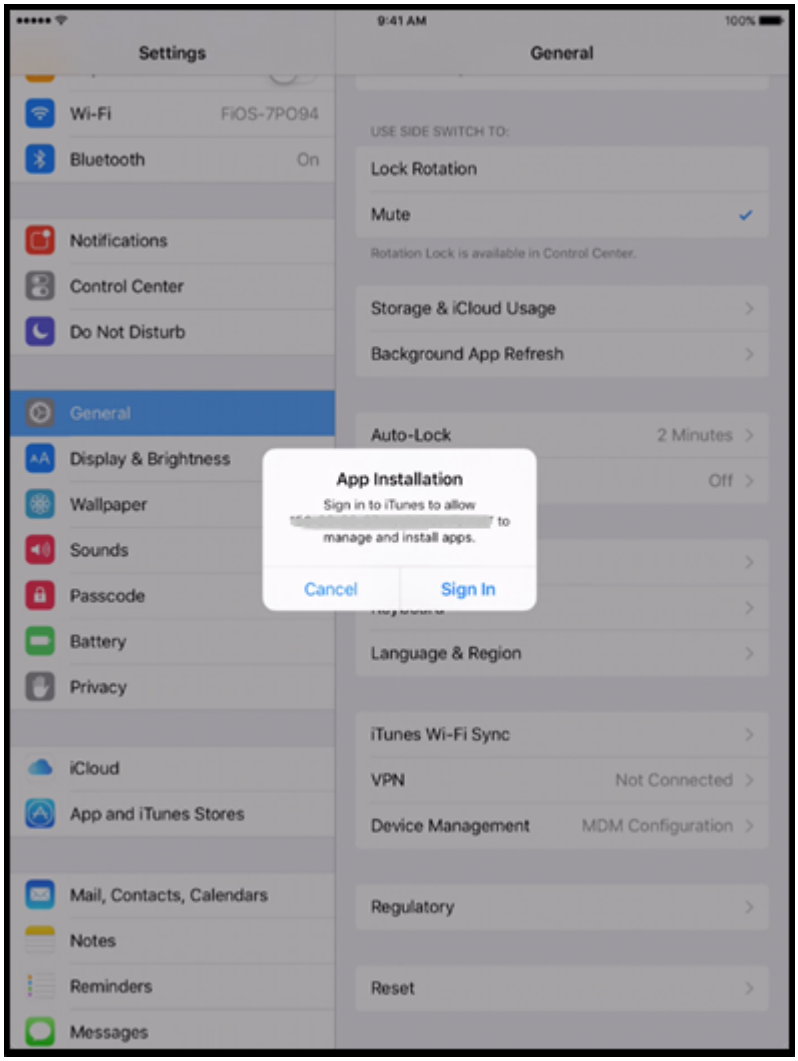


Benutzererfahrung beim Registrieren eines Apple-Bereitstellungsprogramm-fähigen Geräts

Benutzer registrieren ein Apple-Bereitstellungsprogramm-fähiges Gerät mit den folgenden Schritten.

1. Benutzer starten ihr Apple-Bereitstellungsprogramm-fähiges Gerät.
2. Die Apple-Bereitstellungsprogramm-Konfiguration, die Sie in der XenMobile-Konsole konfiguriert haben, wird für das Apple-Bereitstellungsprogramm-fähige Gerät bereitgestellt.
3. Benutzer konfigurieren die anfänglichen Einstellungen auf ihrem Gerät.
4. Das Gerät startet automatisch die XenMobile-Geräteregistrierung.
5. Benutzer fahren mit der Konfiguration weiterer Einstellungen auf ihrem Gerät fort.
6. Benutzer werden im Homebildschirm unter Umständen aufgefordert, sich beim Apple App Store anzumelden, um Citrix Secure Hub herunterladen zu können.

   > **Hinweis:**
   >
   > Dieser Schritt ist optional, wenn Sie XenMobile für die Bereitstellung der Secure Hub-App mit der gerätebasierten Volume Purchase-Zuweisung konfigurieren. In diesem Fall muss kein Apple App Store-Konto erstellt oder vorhandenes Konto verwendet werden.



7. Die Benutzer öffnen Secure Hub und geben ihre Anmeldeinformationen ein. Entsprechend der Richtlinie müssen Benutzer unter Umständen eine Citrix-PIN erstellen und verifizieren.

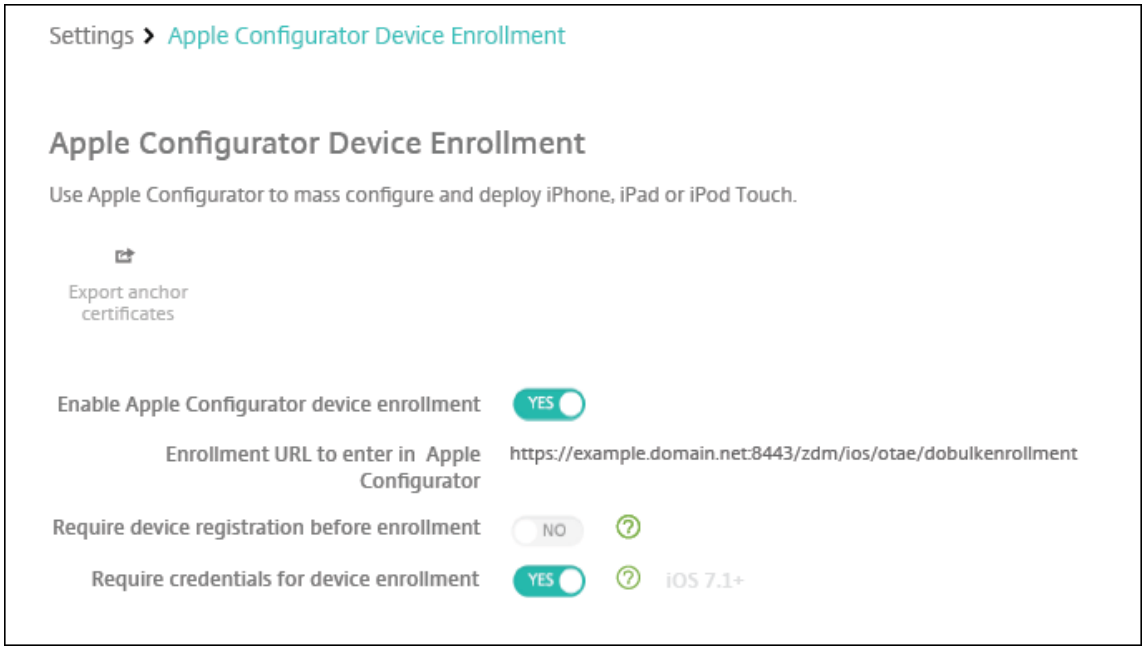
   XenMobile stellt dem Gerät alle verbleibenden notwendigen Apps zur Verfügung.

Konfigurieren von Apple Configurator 2-Einstellungen

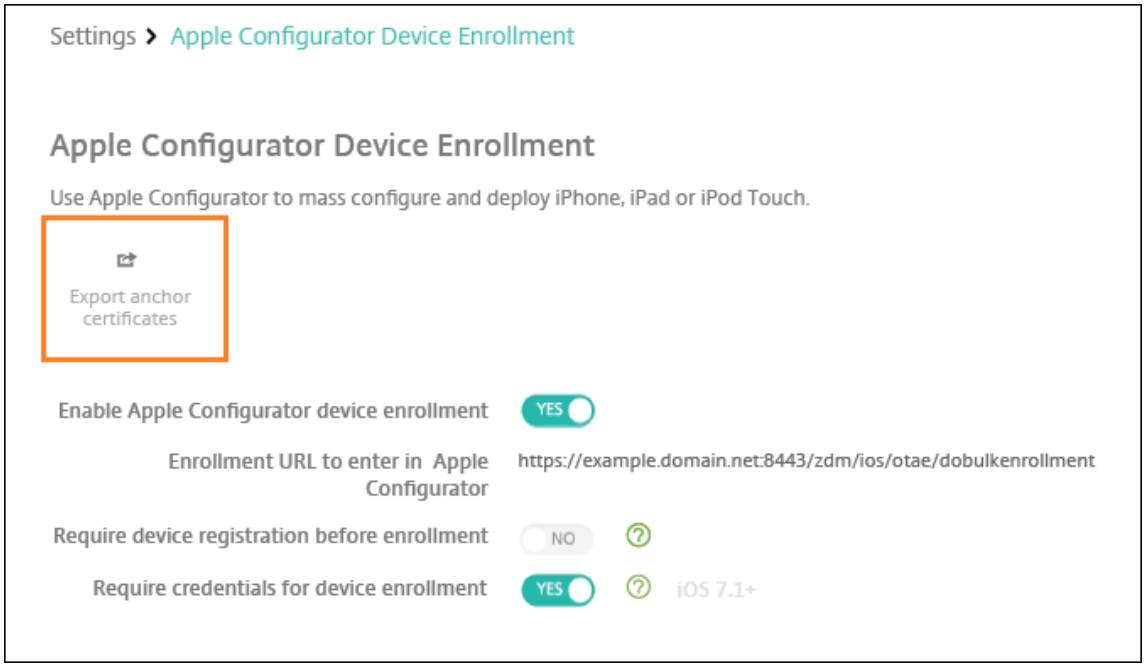
Sie können große Mengen an iPhone- und iPad-Geräten auch mit Apple Configurator 2 anstelle von Apple Business Manager konfigurieren und bereitstellen.

Schritt 1: Konfigurieren von Einstellungen in XenMobile

1. Navigieren Sie in der XenMobile-Konsole zu **Einstellungen > Apple Configurator-Geräteregistrierung**.



2. Wählen Sie für **Apple Configurator - Geräteregistrierung aktivieren** die Einstellung **Ja**.
3. Die **Registrierungs-URL zum Eingeben in Apple Configurator** ist ein schreibgeschütztes Feld. Die Einstellung liefert die URL für den XenMobile-Server, der mit Apple kommuniziert. Kopieren Sie diese URL, um sie beim Konfigurieren der Einstellungen in Apple Configurator 2 einzufügen. Die Registrierungs-URL entspricht dem vollqualifizierten Domänennamen (z. B. `mdm.server.url.com`) oder der IP-Adresse des XenMobile-Servers.
4. Setzen Sie **Geräteregistrierung vor der Apple Registrierung** auf **Ja**, um zu verhindern, dass unbekannte Geräte registriert werden. Hinweis: Wenn die Einstellung **Ja** lautet, müssen Sie die konfigurierten Geräte vor der Registrierung unter **Verwalten > Geräte** in XenMobile manuell oder über eine CSV-Datei hinzufügen.
5. Setzen Sie **Anmeldeinformationen für Geräteregistrierung erforderlich** auf **Ja**, damit Benutzer von iOS-Geräten bei der Registrierung ihre Anmeldeinformationen eingeben müssen. In der Standardeinstellung ist dies nicht erforderlich.
6. Hinweis: Wenn XenMobile Server ein vertrauenswürdiges SSL-Zertifikat verwendet, überspringen Sie diesen Schritt. Klicken Sie auf **Export Anchor Certs** und speichern Sie die Datei certchain.pem im macOS-Schlüsselbund (Anmeldung oder System).



Schritt 2: Konfigurieren der Einstellungen in Apple Configurator 2

1. Installieren Sie Apple Configurator 2 aus dem App-Store.
2. Schließen Sie Geräte mit USB-Kabel am Dock-Anschluss eines Mac-Computers an, auf dem Apple Configurator 2 ausgeführt wird. Sie können bis zu 30 verbundene Geräte gleichzeitig 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.
3. Starten Sie Apple Configurator 2. Der Configurator zeigt alle Geräte an, die Sie für die Betreuung vorbereiten können.
4. Vorbereiten eines Geräts für die Betreuung:
   - Wählen Sie **Supervise devices**, wenn Sie ein Gerät durch regelmäßige Neuanwendung einer Konfiguration steuern möchten. Klicken Sie auf **Weiter**.

     > **Wichtig:**
     >
     > 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.

   - Klicken Sie in iOS auf **Latest** für die neueste iOS-Version, die Sie installieren möchten.
5. Wählen Sie unter **Enroll in MDM Server** einen MDM-Server. Um einen neuen Server hinzuzufügen, klicken Sie auf **Next**.

6. Geben Sie unter **Define an MDM Server** einen Namen für den Server ein und fügen Sie die URL des MDM-Servers aus der XenMobile-Konsole ein.
7. Wählen Sie unter **Assign to organization** eine Organisation für die Betreuung des Geräts aus.

   Weitere Informationen zur Vorbereitung von Geräten mit Apple Configurator 2 finden Sie auf der Seite Prepare devices der Apple Configurator-Hilfe.
8. Schalten Sie zur Vorbereitung jedes Gerät ein, um den iOS-Setupassistenten zu starten, der es für die erste Verwendung vorbereitet.

Zuweisen von Geräten aus Apple Configurator 2 zu Apple Business Manager

Sie können iPhone- und iPad-Geräte von Apple Configurator 2 aus mit Ihrem Apple Business Manager-Konto verknüpfen. Hinzugefügte Geräte werden im Abschnitt **Geräte** angezeigt. Diese Geräte enthalten keine Registrierungseinstellungen mehr, die über Apple Configurator 2 zugewiesen wurden. Weitere Informationen finden Sie unter Zuweisen von aus Apple Configurator 2 zu Apple Business Manager hinzugefügten Geräten.

Erneuern oder Aktualisieren von Zertifikaten mit dem Apple-Bereitstellungsprogramm

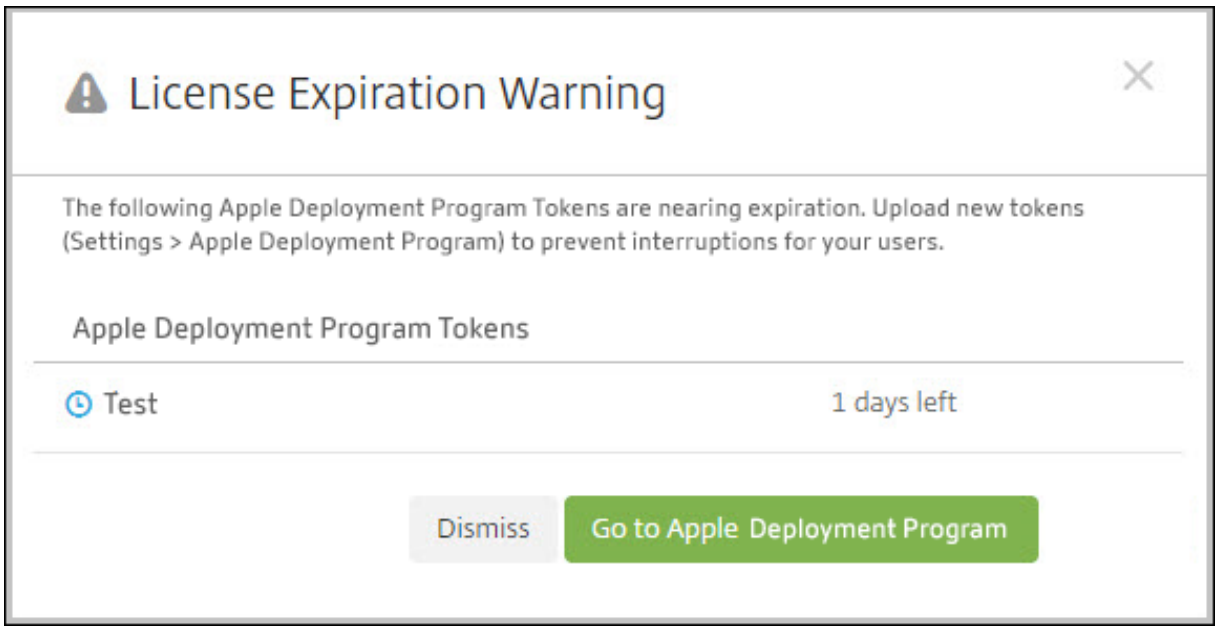
Wenn das XenMobile-SSL-Zertifikat (Secure Sockets Layer) erneuert wird, laden Sie ein neues Zertifikat in der XenMobile-Konsole unter **Einstellungen > Zertifikate** hoch. Klicken Sie im Dialogfeld **Importieren** unter **Verwenden als** auf **SSL-Listener**, damit das Zertifikat für SSL verwendet wird. 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 dem Apple-Bereitstellungsprogramm und XenMobile neu zu erstellen, wenn Sie das SSL-Zertifikat erneuern oder aktualisieren. Sie können Ihre Einstellungen für das **Apple-Bereitstellungsprogramm** jedoch jederzeit neu konfigurieren, indem Sie die vorstehenden Schritte in diesem Artikel ausführen.

Weitere Informationen zum Apple-Bereitstellungsprogramm finden Sie in der Dokumentation von Apple.

Erneuern der Verbindung zwischen dem Apple-Bereitstellungsprogramm und XenMobile

XenMobile zeigt eine Lizenzablaufwarnung an, wenn Ihr Servertoken für die automatisierte Geräteregistrierung abläuft.



Ersetzen Sie den Token von Apple School Manager/Apple Business Manager.

Schritt 1: Hochladen eines öffentlichen Schlüssels von XenMobile Server

1. Gehen Sie in der XenMobile-Konsole zu **Einstellungen > Apple-Bereitstellungsprogramm**, um einen öffentlichen Schlüssel herunterzuladen.

Schritt 2: Erstellen und Herunterladen einer Servertokendatei aus dem Apple-Konto

1. Melden Sie sich bei Apple Business Manager an, um den Token herunterzuladen.
2. Öffnen Sie **Einstellungen** und wählen Sie den Server aus, von dem Sie ein Token benötigen. Klicken Sie auf **Edit**.
3. Laden Sie unter **MDM Server Settings** den neuen öffentlichen Schlüssel hoch, den Sie von XenMobile heruntergeladen haben, und speichern Sie die Änderungen.
4. Klicken Sie auf **Token herunterladen**, um den neuen Token herunterzuladen.

Schritt 3: Hochladen einer Servertokendatei in XenMobile

1. Gehen Sie in Citrix XenMobile zu **Einstellungen > Apple-Bereitstellungsprogramm**.
2. Wählen Sie das Deployment Program-Konto aus, klicken Sie auf **Bearbeiten** und laden Sie die Servertokendatei hoch.
3. Klicken Sie auf **Weiter** und speichern Sie die Änderungen.

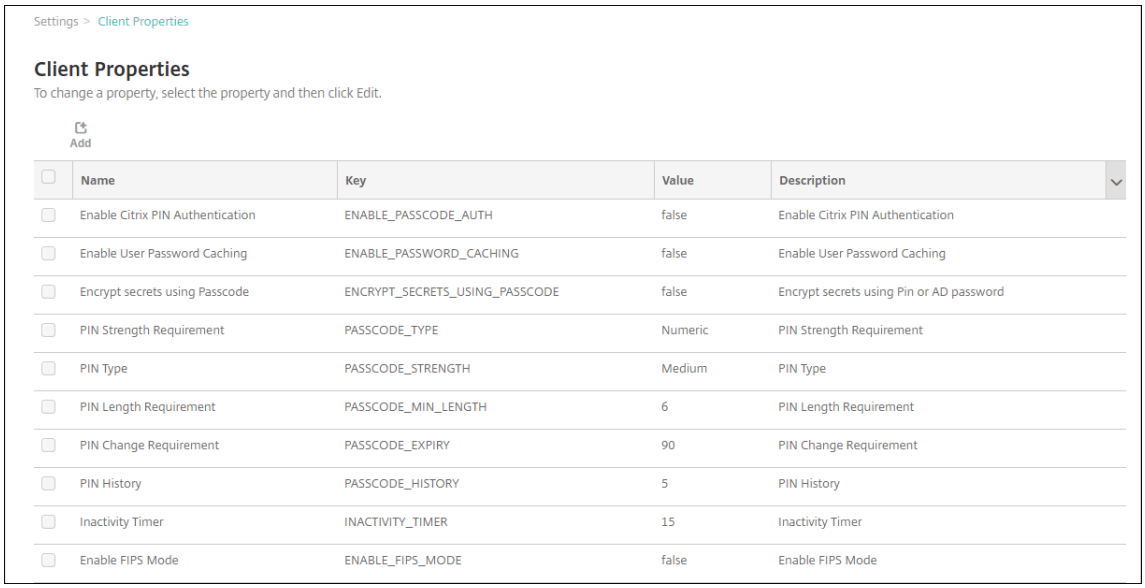
Clienteigenschaften

January 5, 2022

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 Secure Hub und bei einigen neuen Releases von Client-Apps ändern. Informationen zu den häufig konfigurierten Clienteigenschaften finden Sie unter Referenz der Clienteigenschaften weiter unten in diesem Artikel.

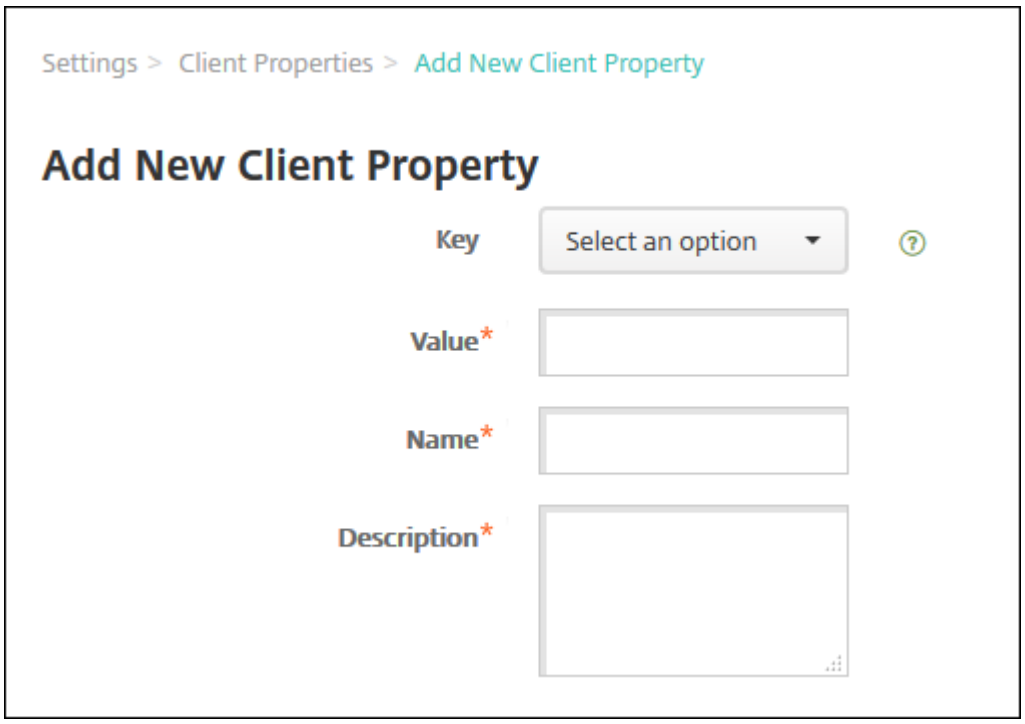
1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Client** auf **Clienteigenschaften**. Die Seite **Clienteigenschaften** wird angezeigt. Auf dieser Seite können Sie Clienteigenschaften hinzufügen, bearbeiten und löschen.



Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

Hinzufügen einer Clienteigenschaft

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

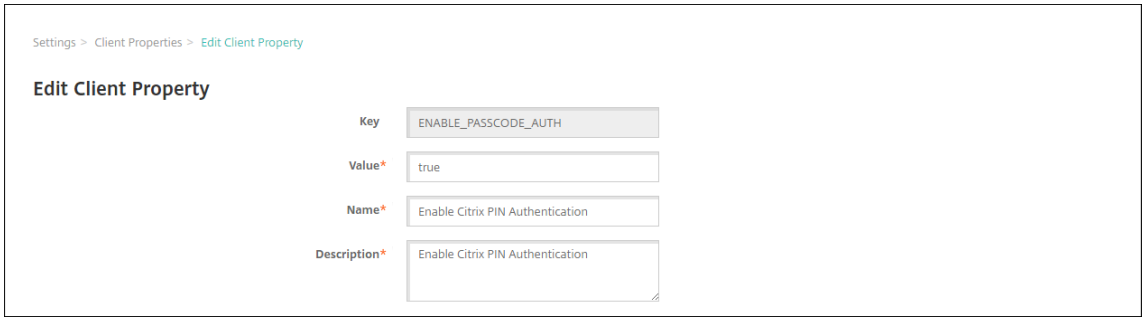


2. Konfigurieren Sie folgende Einstellungen:
   - **Schlüssel:** Klicken Sie in der Liste auf den Eigenschaftsschlüssel, den Sie hinzufügen möchten. Wichtig: Wenden Sie sich vor dem Aktualisieren der Einstellungen an den Citrix Support. Sie können einen speziellen Schlüssel anfordern.
   - **Wert:** Wert der ausgewählten Eigenschaft.
   - **Name:** Name der Eigenschaft.
   - **Beschreibung:** Beschreibung der Eigenschaft.
3. Klicken Sie auf **Speichern**.

Bearbeiten einer Clienteigenschaft

1. Wählen Sie in der Tabelle **Clienteigenschaften** die zu bearbeitende Clienteigenschaft aus.

   Wenn Sie das Kontrollkästchen neben einer Clienteigenschaft aktivieren, wird oberhalb der Liste der Clienteigenschaften ein Optionsmenü angezeigt. Wenn Sie an eine andere Stelle in der Liste klicken, wird das Menü mit den Optionen rechts daneben angezeigt.
2. Klicken Sie auf **Edit**. 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 Eigenschaft beizubehalten.

Löschen einer Clienteigenschaft

1. Wählen Sie in der Tabelle **Clienteigenschaften** die gewünschte Clienteigenschaft aus.

   Sie können mehrere zu löschende Eigenschaften auswählen, indem Sie die Kontrollkästchen daneben aktivieren.
2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf **Delete**.

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 festgelegten Zeit der Inaktivität (in Tagen). Nach Ablauf der Zeit können die Apps nicht mehr verwendet werden. 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 festgelegt haben und der Benutzer die Apps über 30 Tage 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
  - Verwenden Sie diese Eigenschaft, um Benutzer daran zu hindern, Protokolle von ihren Geräten zu sammeln und hochzuladen. Diese Eigenschaft deaktiviert die Protokollierung für Secure Hub und alle installierten MDX-Apps. Die Benutzer können über die Support-Seite keine Protokolle für Apps senden. Obwohl das Dialogfeld für die E-Mail-Erstellung angezeigt wird, werden keine Protokolle angehängt. Eine Meldung gibt an, dass die Protokollierung deaktiviert ist. Diese Einstellung verhindert außerdem, die Aktualisierung der Protokolleinstellungen in der XenMobile-Konsole für Secure Hub- und MDX-Apps.

    Wenn diese Eigenschaft auf **true** festgelegt wird, wird die Eigenschaft **App-Protokolle blockieren** in Secure Hub ebenfalls auf **true** eingestellt. Die Protokollierung für MDX-Apps wird daher beim Anwenden der neuen Richtlinie eingestellt.
  - Mögliche Werte: **true** oder **false**
  - Standardwert: **false** (Protokollierung nicht deaktiviert)
- **ENABLE_CRASH_REPORTING**
  - Anzeigename: Absturzberichterstellung
  - Bei der Einstellung **Wahr** sammelt Citrix Absturzberichte und Diagnosedaten zur Behandlung von Problemen mit Secure Hub für iOS und Android. Bei der Einstellung **Falsch** werden keine Daten gesammelt.
  - Mögliche Werte: **true** oder **false**
  - Standardwert: **true**
- **ENABLE_CREDENTIAL_STORE**
  - Anzeigename: Enable Credential Store

  - Wenn Sie den Anmeldeinformationsspeicher aktivieren, geben Android- oder iOS-Benutzer ihr Kennwort einmalig beim Zugriff auf mobile Produktivitätsapps ein. Sie können den Anmeldeinformationsspeicher verwenden. Dabei spielt es keine Rolle, ob Sie Citrix-PIN aktivieren. Wenn Sie Citrix-PIN nicht aktivieren, geben Benutzer ihr Active Directory-Kennwort ein. XenMobile unterstützt die Verwendung von Active Directory-Kennwörtern mit dem Anmeldeinformationsspeicher ausschließlich für Secure Hub und öffentliche Store-Apps. Wenn Sie Active Directory-Kennwörter mit dem Anmeldeinformationsspeicher verwenden, bietet XenMobile keine Unterstützung für die PKI-Authentifizierung.
  - Für die automatische Registrierung bei Secure Mail müssen Sie diese Eigenschaft auf **true** setzen.
  - Navigieren Sie zum Konfigurieren dieser benutzerdefinierten Clientrichtlinie zu **Einstellungen > Clienteigenschaften**, fügen Sie den benutzerdefinierten Schlüssel **ENABLE_CREDENTIAL_STORE** hinzu und setzen Sie den **Wert** auf **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_PASSCODE_AUTH**
  - Anzeigename: Enable Citrix 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.

    Bei der Offlineauthentifizierung wird die Citrix-PIN lokal validiert und die Benutzer können auf die gewünschte App bzw. den gewünschten Inhalt zugreifen. Bei der Onlineauthentifizierung wird mit der Citrix PIN oder dem Citrix Passcode das Active Directory-Kennwort bzw. -Zertifikat entsperrt und zur Authentifizierung bei XenMobile übertragen.

    Wenn für ENABLE_PASSCODE_AUTH “true” und für ENABLE_PASSWORD_CACHING “false” festgelegt ist, wird bei der Onlineauthentifizierung immer das Kennwort angefordert, da dieses in Secure Hub nicht gespeichert wird.
  - Mögliche Werte: **true** oder **false**
  - Standardwert: **false**

- **ENABLE_PASSWORD_CACHING**
  - Anzeigename: Enable User Password Caching
  - Über diese Eigenschaft werden Active Directory-Kennwörter lokal auf den Mobilgeräten zwischengespeichert. Wenn Sie diese Eigenschaft auf **true** setzen, müssen Sie auch die Eigenschaft **ENABLE_PASSCODE_AUTH** auf **true** setzen. Wenn "Benutzerkennwort-caching" 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 benötigt XenMobile die Citrix PIN, selbst wenn die Clienteigenschaft **ENABLE_PASSCODE_AUTH** auf **false** gesetzt 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. Mit diesem Feature werden in regelmäßigen Abständen anonyme Konfigurations- und Nutzungsdaten an Citrix gesendet. Mit den 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 Secure Hub. Wenn Sie diese Einstellung ändern, tritt der neue Wert erst in Kraft, wenn sich der Benutzer das nächste Mal bei Secure Hub (alter Name: "Worx Home") anmeldet.

  - Mögliche Werte: **true** oder **false**
  - Standardwert: **true**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - Anzeigename: Encrypt secrets using Passcode
  - Mit dieser Eigenschaft werden vertrauliche Daten auf Geräten in einem Geheimtresor statt in einem plattformbasierten systemeigenen Speicher (z. B. iOS-Schlüsselbund) gespeichert. Diese Eigenschaft ermöglicht eine starke Verschlüsselung von Schlüsselartefakten und erzeugt Benutzerentropie. Mit "Benutzerentropie" wird eine vom Benutzer generierte zufällige PIN bezeichnet, 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, 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 legen Sie die Einstellung "App-Passcode" auf "Ein" fest. Wenn "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 die Benutzer das nächste Mal zur Authentifizierung aufgefordert werden.

    Für iOS steuert "Inactivity Timer" auch den Zugriff auf Secure Hub für MDX- und Nicht-MDX-Apps.
  - Mögliche Werte: beliebige Ganzzahl
  - Standardwert: **15** (Minuten)

- **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 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 (empfohlene) Werte: **1** bis **99**. Zur Vermeidung von PIN-Zurücksetzungen 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 PIN-Ablauf 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** (Tage)

- **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 Citrix-PIN oder seinen Passcode zurücksetzt.
  - Mögliche Werte: **1** bis **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 Citrix-PIN bzw. einen Passcode zu erstellen.
  - Mögliche Werte: beliebige Ganzzahl
  - Standardwert: **15**

- **PASSCODE_MIN_LENGTH**
  - Anzeigename: PIN Length Requirement
  - Diese Eigenschaft definiert die Mindestlänge der Citrix-PIN.
  - Mögliche Werte: **4** bis **10**
  - 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 Erstellen einer Citrix-PIN bzw. eines Citrix Passcodes aufgefordert, wenn sie sich das nächste Mal authentifizieren.

- Mögliche Werte: **Low**, **Medium**, **High** oder **Strong**
- Standardwert: **Medium**
- Die Kennwortregeln für die einzelnen Sicherheitseinstellungen gemäß PASSCODE_TYPE-Einstellung sind wie folgt:

Regeln für numerische Passcodes:

Passcodestärke	Regeln für numerischen Passcodetyp	Zugelassen	Nicht zulässig
Niedrig	Alle Ziffern, beliebige Reihenfolge zugelassen	444444, 123456, 654321	
Mittel (Standardeinstellung)	Alle Ziffern dürfen nicht identisch oder aufeinanderfolgend sein.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
Hoch	Angrenzende Ziffern dürfen nicht identisch sein.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Gut	Verwenden Sie eine Ziffer maximal zweimal. Verwenden Sie drei oder mehr aufeinanderfolgende Ziffern nicht mehrfach hintereinander. Verwenden Sie drei oder mehr aufeinanderfolgende Ziffern nicht in umgekehrter Reihenfolge.	102983, 085085, 824673, 132312	132132, 131313, 902030

Regeln für alphanumerische Passcodes:

Passcodestärke	Regeln für alphanumerischen Passcodetyp	Zugelassen	Nicht zulässig
Niedrig	Muss mindestens eine Ziffer und einen Buchstaben enthalten.	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
Mittel (Standardeinstellung)	Zusätzlich zu den Regeln für die Sicherheitseinstellung “Niedrig” gilt, dass Buchstaben und alle Ziffern nicht identisch sein dürfen. Es dürfen keine aufeinanderfolgenden Buchstaben und Ziffern verwendet werden.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa oder aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, oder cba123
Hoch	Muss mindestens einen Großbuchstaben und einen Kleinbuchstaben enthalten.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Gut	Muss mindestens eine Ziffer, ein Sonderzeichen, einen Großbuchstaben und einen Kleinbuchstaben enthalten.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **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.
  - Standardwert: **72** Stunden (3 Tage)

- **SEND_LDAP_ATTRIBUTES**
  - Für Nur-MAM-Bereitstellungen von Android-, iOS oder macOS-Geräten können Sie XenMobile so konfigurieren, dass Benutzer, die sich bei Secure Hub mit E-Mail-Anmeldeinformationen registrieren, automatisch bei Secure Mail registriert werden. Die Benutzer müssen dann zur Anmeldung bei Secure Mail keine zusätzlichen Informationen angeben und keine weiteren Schritte unternehmen.
  - 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:

    ```
    <property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,email=user@site.com\,user@site.com" name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - Bei dieser Eigenschaft behandelt XenMobile Kommas als Abschlusszeichen. Wenn ein Attributwert ein Komma enthält, stellen Sie diesem einen umgekehrten Schrägstrich voran. Der umgekehrte Schrägstrich verhindert, dass den Client das Komma als Attributwertende interpretiert. Schreiben Sie den umgekehrten Schrägstrich `"\\"`.

- **HIDE_THREE_FINGER_TAP_MENU**
  - Wenn diese Eigenschaft nicht festgelegt oder auf **false** gesetzt ist, können Benutzer auf das Menü “Ausgeblendete Features” zugreifen, indem sie mit drei Fingern auf das Gerät tippen. Über das Menü “Ausgeblendete Features” konnten Benutzer Anwendungsdaten zurücksetzen. Wenn Sie diese Eigenschaft auf **true** setzen, deaktivieren Sie den Benutzerzugriff auf das Menü “Ausgeblendete Features”.
  - Zum Konfigurieren dieser globalen Clientrichtlinie gehen Sie zu **Einstellungen > Clienteigenschaften**, fügen den benutzerdefinierten Schlüssel **HIDE_THREE_FINGER_TAP_MENU** hinzu und legen den **Wert** fest.
- **TUNNEL_EXCLUDE_DOMAINS**
  - Anzeigename: Tunnel Exclude Domains
  - Standardmäßig schließt MDX einige von XenMobile-SDKs und -Apps für verschiedene Features verwendete Dienstendpunkte vom Micro-VPN-Tunneling aus. Zu diesen Endpunkten gehören Dienste wie Google Analytics, Citrix Cloud- und Active Directory-Dienste, die nicht über Unternehmensnetzwerke geroutet werden müssen. Verwenden Sie diese Clienteigenschaft, um die Standardliste der ausgeschlossenen Domänen außer Kraft zu setzen.
  - Zum Konfigurieren dieser globalen Clientrichtlinie gehen Sie zu **Einstellungen > Clienteigenschaften**, fügen den benutzerdefinierten Schlüssel **TUNNEL_EXCLUDE_DOMAINS** hinzu und legen den **Wert** fest.
  - Wert: Um die Standardliste durch die Domänen zu ersetzen, die Sie vom Tunneling ausschließen möchten, geben Sie eine durch Kommas getrennte Liste von Domänensuffixen ein. Um alle Domänen im Tunneling einzuschließen, geben **none** ein. Standardwert:

    ```
    app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test
    .citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.
    launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net
    ,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf
    -staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,
    stream.launchdarkly.com
    ```

Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm

January 5, 2022

Apple bietet Programme zur Geräteregistrierung (DEP = Device Enrollment Program) für Unternehmen und Bildungseinrichtungen an. Für Unternehmenskonten müssen Sie sich beim Apple-Bereitstellungsprogramm registrieren, um Apple Business Manager (ABM) oder Apple School

Manager (ASM) zum Registrieren und Verwalten von Geräten in XenMobile zu verwenden. Das Programm wird für iOS, iPadOS und macOS-Geräte angeboten.

Das Apple-Bereitstellungsprogramm (DEP) ist nur für Organisationen und nicht für einzelne Personen verfügbar. Sie müssen umfangreiche Unternehmensdaten bereitstellen, um ein Apple-Bereitstellungsprogramm-Konto zu erstellen. Deshalb kann es eine Weile dauern, Kontogenehmigungen anzufordern und zu erhalten.

Für Bildungskonten erstellen Sie ein Apple School Manager-Konto. Bei ASM sind Apple-Bereitstellungsprogramm und Apple Volume Purchase kombiniert. Ein Apple School Manager-Konto können Sie auf der Apple School-Website erstellen.

Registrieren beim Apple-Bereitstellungsprogramm

Zum Registrieren bei Apple Business Manager gehen Sie zu business.apple.com. Klicken Sie auf **Enroll now**, um ein neues Konto zu beantragen. Verwenden Sie am besten eine E-Mail-Adresse für Ihr Unternehmen, z. B. deployment@company.com. Die Registrierung kann einige Tage dauern. Nachdem Sie Ihre Anmeldeinformationen erhalten haben, befolgen Sie die Schritte in Apple Business Manager, um ein Konto zu erstellen.

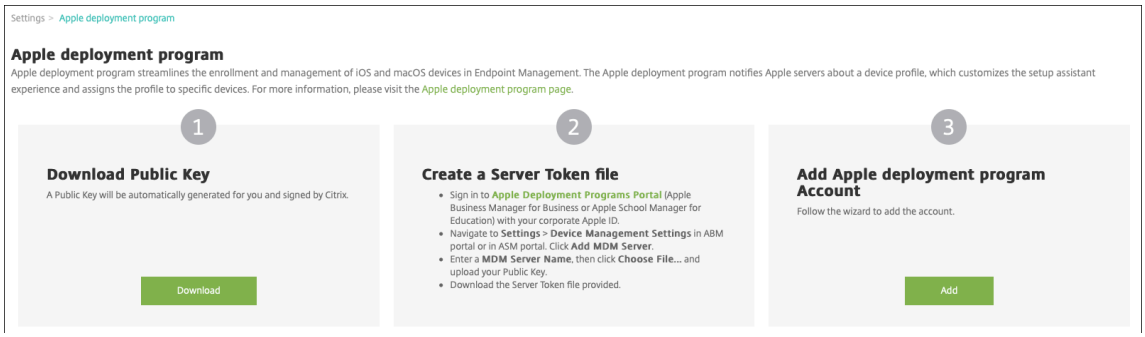
> **Hinweis:**
>
> Informationen zu Konten für Schulen und Universitäten finden Sie unter Integration von Apple Bildung-Features.

Verbinden des Apple Business Manager-Kontos mit XenMobile

Geben Sie zum Herstellen einer Verbindung zwischen dem Apple Business Manager-Konto und der XenMobile-Bereitstellung Informationen in der XenMobile-Konsole und in Apple Business Manager ein. Führen Sie folgende Schritte aus:

Schritt 1: Hochladen eines öffentlichen Schlüssels von XenMobile Server

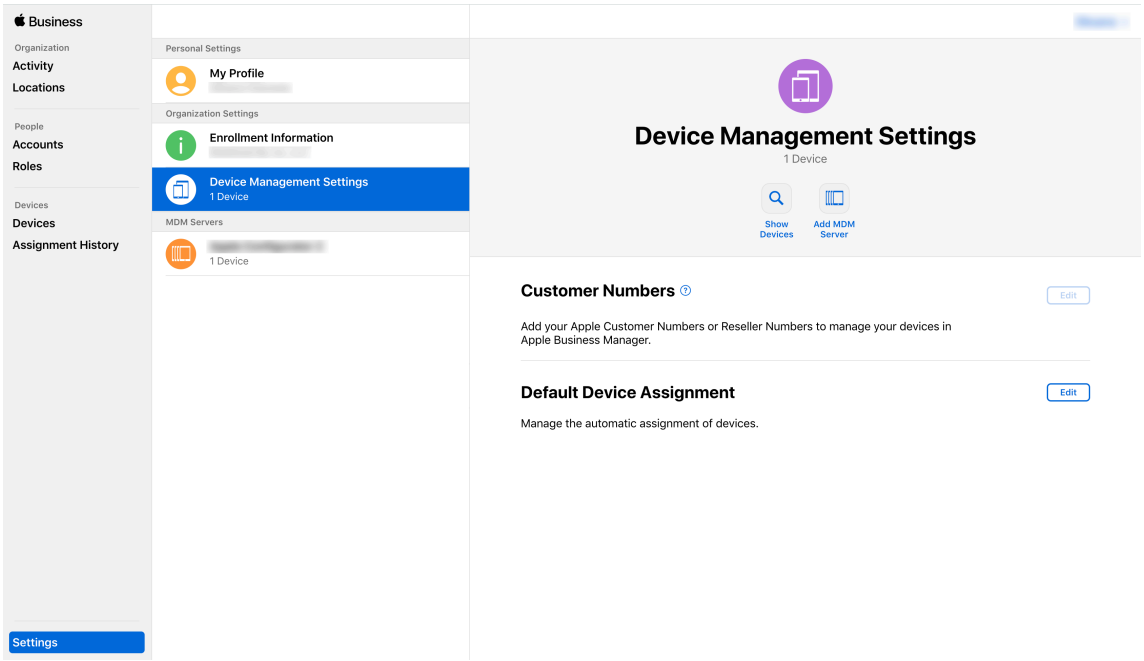
1. Gehen Sie in der XenMobile-Konsole zu **Einstellungen > Apple-Bereitstellungsprogramm**.



2. Klicken Sie unter **Öffentlichen Schlüssel herunterladen** auf **Herunterladen**.

Schritt 2: Erstellen und Herunterladen einer Servertokendatei aus dem Apple-Konto

1. Melden Sie sich als Administrator oder Geräteregistrierungsverwalter bei Apple Business Manager an.
2. Klicken Sie unten in der Randleiste auf **Settings** und dann auf **Device Management Settings > Add MDM Server**.



3. Geben Sie in der Einstellung **MDM Server Name** einen Namen für den XenMobile-Server ein. Der von Ihnen eingegebene Servername dient Ihnen als Referenz. Er ist nicht die URL oder der Name des Servers.
4. Klicken Sie unter **Upload Public Key** auf **Choose File**. Laden Sie den öffentlichen Schlüssel hoch, den Sie von XenMobile heruntergeladen haben, und speichern Sie die Änderungen.
5. Klicken Sie auf **Download Token**, um die Servertokendatei auf Ihren Computer herunterzuladen.

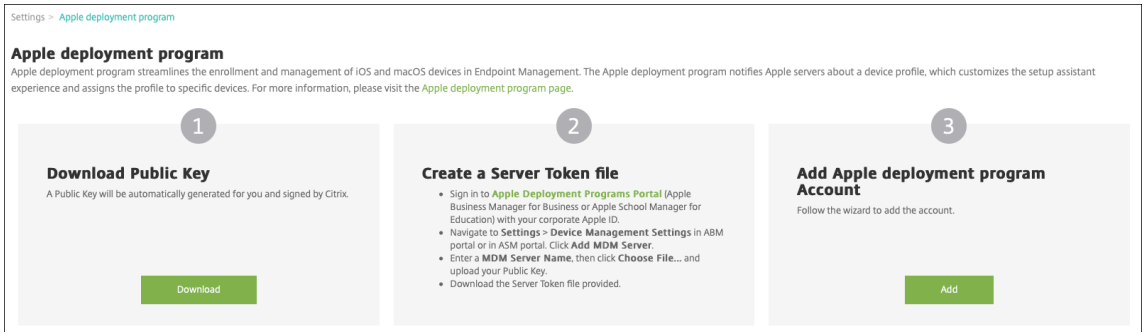
   Sie müssen die Servertokendatei hochladen, wenn Sie das ABM-Konto zu XenMobile hinzufügen. Nach dem Import der Tokendatei werden Ihre ABM-Tokeninformationen in der XenMobile-Konsole angezeigt.
6. Klicken Sie unter **Default Device Assignment** auf **Change**. Wählen Sie aus, wie Sie Geräte zuweisen möchten, und geben Sie die angeforderten Informationen ein. Weitere Informationen finden Sie im ABM-Benutzerhandbuch.

Schritt 3: Hinzufügen eines ABM-Kontos zu XenMobile

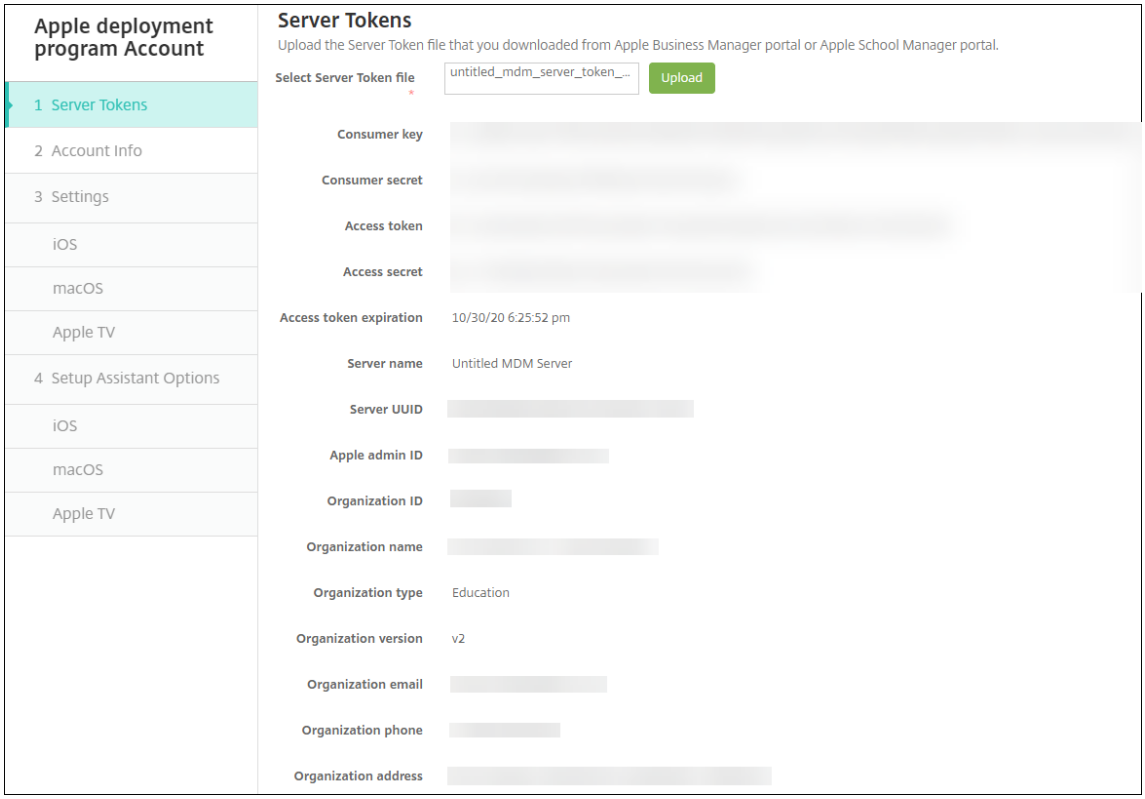
Sie können mehrere ABM-Konten zu XenMobile hinzufügen. Dieses Feature ermöglicht die Verwendung verschiedener Registrierungseinstellungen sowie verschiedener Optionen im Setupassistenten je nach Land, Abteilung usw. Anschließend verknüpfen Sie die ABM-Konten mit verschiedenen Geräterichtlinien.

Sie können beispielsweise alle ABM-Konten aus verschiedenen Ländern auf einem XenMobile-Server zentralisieren, um dort alle ABM-Geräte zu importieren und zu überwachen. Durch Anpassen der Registrierungseinstellungen und Setupassistentenoptionen nach Abteilung, Organisationshierarchie oder einer anderen Struktur bieten Richtlinien unternehmensweit die jeweils erwartete Funktionalität und Benutzer erhalten geeignete Unterstützung.

1. Rufen Sie in der XenMobile-Konsole **Einstellungen > Apple Deployment Program** auf und klicken Sie unter **Apple Deployment Program-Konto hinzufügen** auf **Hinzufügen**.

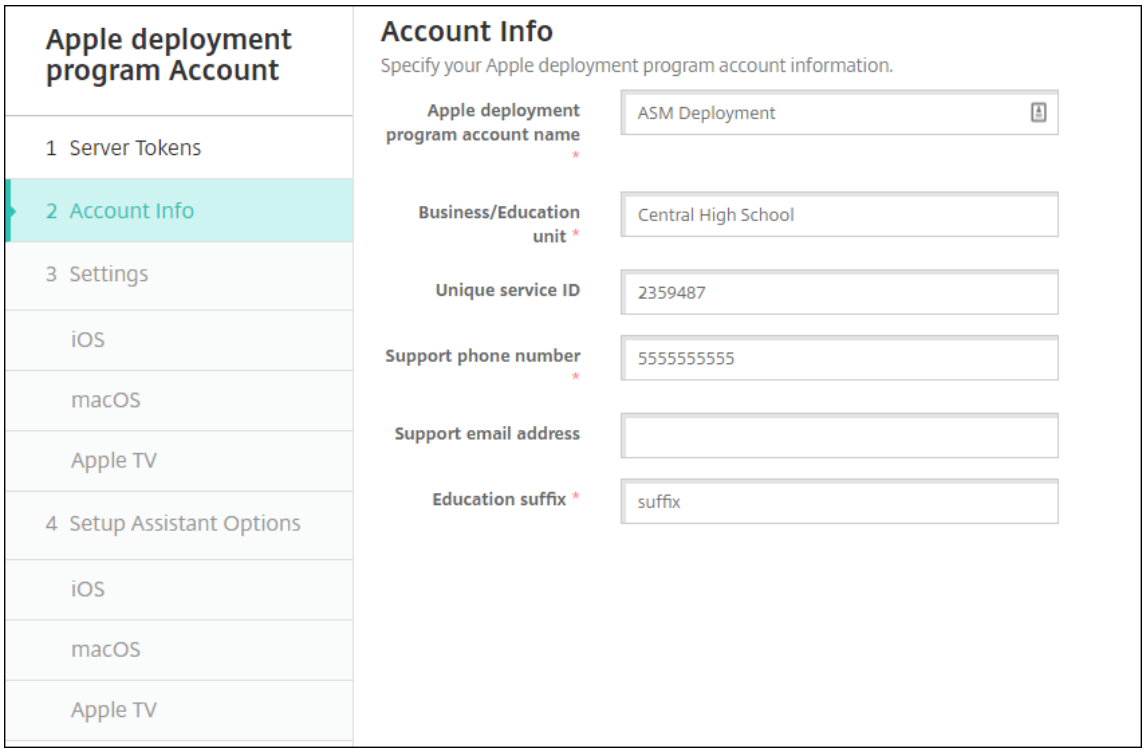


2. Geben Sie auf der Seite **Servertoken** die Servertokendatei ein und klicken Sie dann auf **Hochladen**.



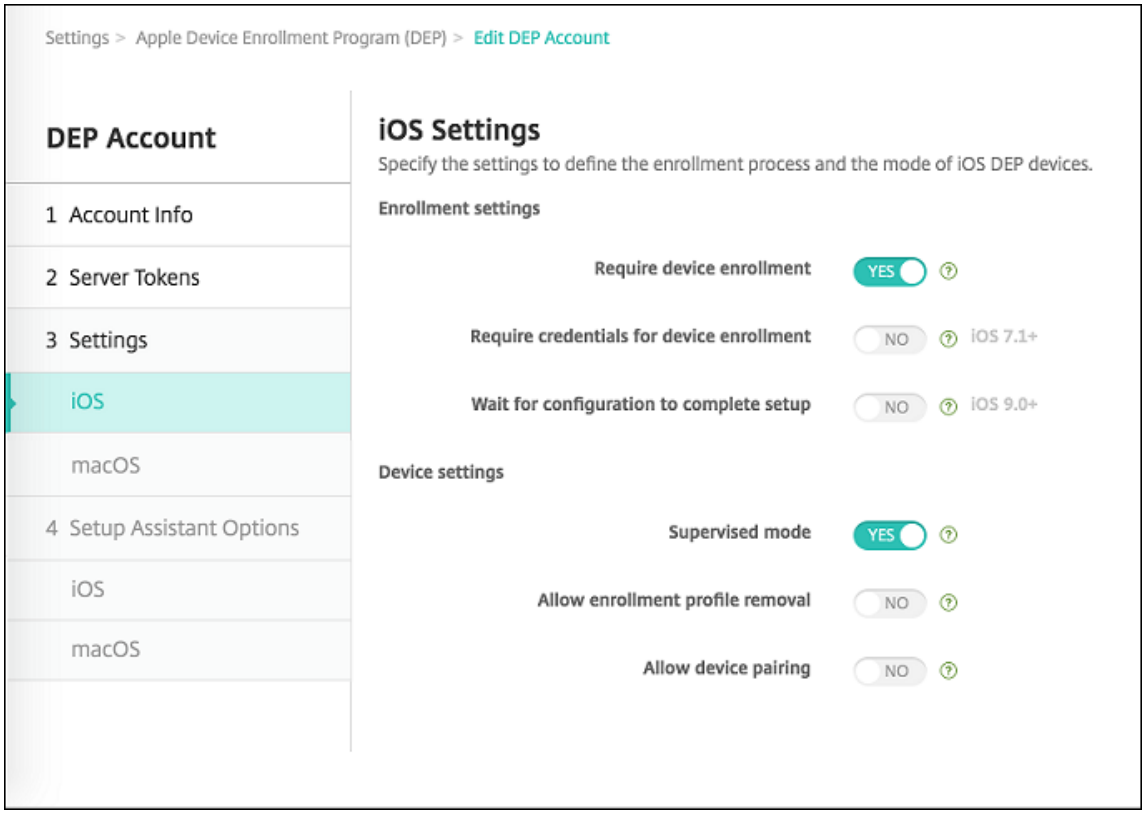
Die Informationen zum Servertoken werden angezeigt.

3. Geben Sie auf der Seite **Kontoinformationen** folgende Einstellungen an:



- **Apple-Bereitstellungsprogramm-Kontoname:** Ein eindeutiger Name für dieses Apple-Bereitstellungsprogramm-Konto. Verwenden Sie Namen, die die Organisation der Apple-Bereitstellungsprogramm-Konten widerspiegelt, beispielsweise nach Land oder Organisationshierarchie.
- **Geschäftseinheit:** Die Unternehmenseinheit oder Abteilung, der das Gerät zugewiesen ist. Diese Angabe ist erforderlich.
- **Eindeutige Dienst-ID:** Eine optionale eindeutige ID zur weiteren Identifizierung des Kontos.
- **Telefonnummer vom Support:** Eine Telefonnummer, unter der Benutzer beim Setup Hilfe anfordern können. Diese Angabe ist erforderlich.
- **E-Mail-Adresse vom Support:** Eine optionale E-Mail-Adresse des Supports, die Benutzern zur Verfügung steht.

4. Geben Sie unter **iOS-Einstellungen** die folgenden Einstellungen an:



Registrierungseinstellungen:

- **Geräteregistrierung erforderlich:** Wählen Sie aus, ob Benutzer Geräte registrieren müssen. Die Standardeinstellung ist **Ja**.
- **Anmeldeinformationen für Geräteregistrierung erforderlich:** Wählen Sie aus, ob Benutzer bei der ABM-Registrierung ihre Anmeldeinformationen eingeben müssen. Citrix empfiehlt, dass alle Benutzer während der Geräteregistrierung ihre Anmeldeinformatio-

nen eingeben müssen, damit nur autorisierte Benutzer Geräte registrieren können. Die Standardeinstellung ist **Ja**.

Wenn Sie ABM vor dem ersten Einrichten aktivieren und diese Option nicht auswählen, erstellt XenMobile die ABM-Komponenten. Dabei werden Komponenten wie ABM-Benutzer, Secure Hub, Softwarebestand und ABM-Bereitstellungsgruppe erstellt. Wenn Sie diese Option auswählen, werden die Komponenten nicht von XenMobile erstellt. Wenn Sie später die Option deaktivieren, können Benutzer, die ihre Anmeldeinformationen nicht eingegeben haben, die ABM-Registrierung nicht ausführen, da diese ABM-Komponenten nicht vorhanden sind. Zum Hinzufügen von ABM-Komponenten deaktivieren und reaktivieren Sie in diesem Fall das ABM-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 Einstellung ist nur für Geräte im betreuten Modus verfügbar. Die Standardeinstellung ist **Nein**.
- Laut Apple-Dokumentation funktionieren die folgenden Befehle möglicherweise nicht, wenn ein Gerät im Setupassistentenmodus ausgeführt wird:
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

Geräteeinstellungen:

- **Betreuter Modus:** Diese Option muss auf **Ja** festgelegt werden, wenn Sie Apple Configurator zum Verwalten über ABM registrierter Geräte verwenden oder wenn **Abschluss der Konfiguration abwarten** aktiviert ist. Die Standardeinstellung ist **Ja**. Informationen, wie Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus.
- **Entfernen des Registrierungsprofils zulassen:** Wählen Sie aus, ob auf Geräten ein Profil verwendet werden darf, das remote entfernt werden kann. Die Standardeinstellung ist **Nein**.
- **Koppeln von Geräten zulassen:** Wählen Sie aus, ob über ABM registrierte Geräte mit Apple Music und dem Apple Configurator verwaltet werden dürfen. Die Standardeinstellung ist **Nein**.

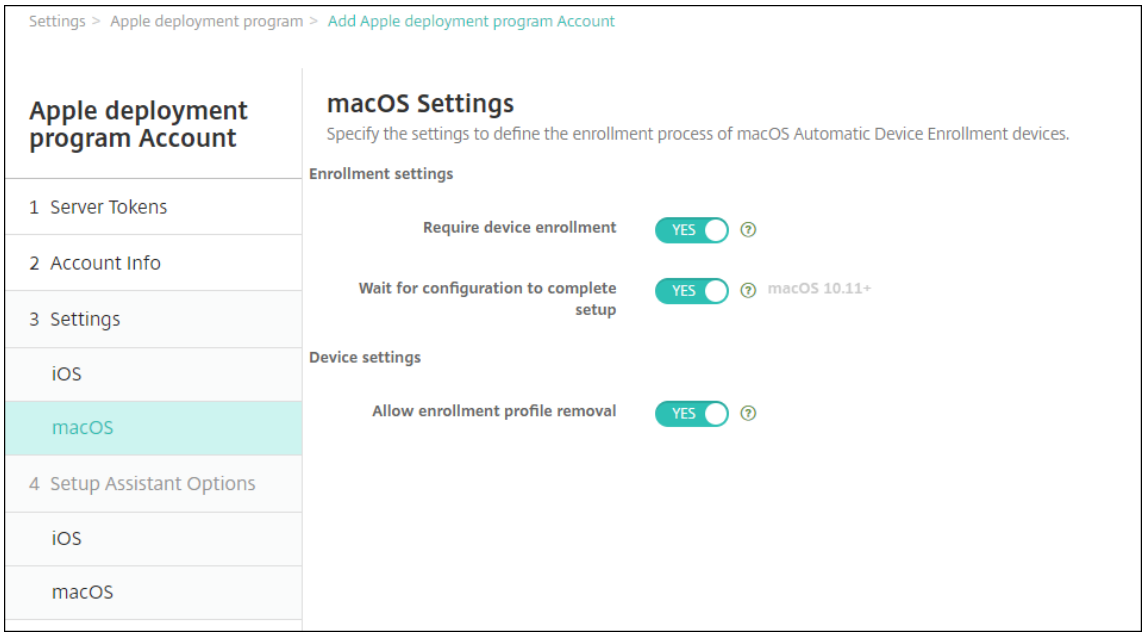
Überwachungsidentitäten

Wenn Sie das GroundControl-Tool verwenden, können Sie ein Zertifikat hinzufügen, um Folgendes zu tun:

- Außerkraftsetzung von Kopplungseinschränkungen, um die Eingabeaufforderung „Trust this host“ zu vermeiden.
- Eskalieren von verwalteten Geräteaktionen über USB, um Profilinstallationen und andere Aktivitäten ohne Benutzeraktion auszuführen. Damit kann GroundControl den Einzel-App-Modus und die Gerätesperre beim Auschecken aktivieren.
- Wiederherstellen eines Backups auf ABM-Geräten.

Weitere Informationen zu GroundControl finden Sie auf der GroundControl-Website.

5. Geben Sie unter **macOS-Einstellungen** die folgenden Einstellungen an:



Registrierungseinstellungen:

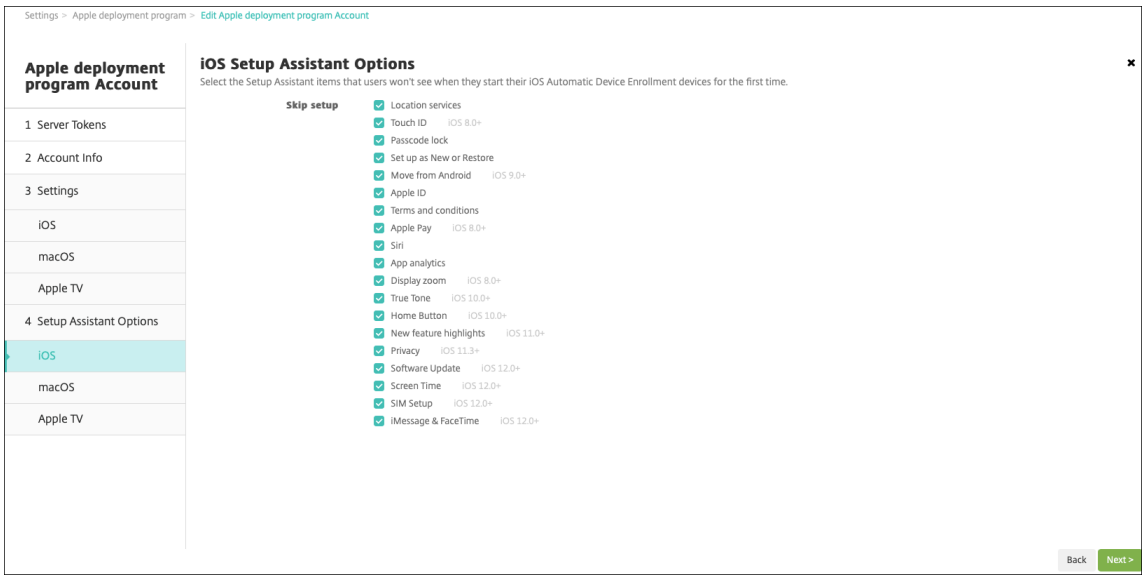
- **Geräteregistrierung erforderlich:** Wählen Sie aus, ob Benutzer Geräte registrieren müssen. Die Standardeinstellung ist **Ja**.
- **Abschluss der Konfiguration abwarten:** Bei **Ja** wird das macOS-Gerät im Setupassistenten erst dann fortgesetzt, wenn der MDM-Ressourcenpasscode auf dem Gerät bereitgestellt wird. Diese Bereitstellung steht vor der Erstellung des lokalen Kontos zur Verfügung. Diese Einstellung ist für Geräte unter macOS 10.11 und höher verfügbar. Die Standardeinstellung ist **Nein**.

Geräteeinstellungen:

- **Entfernen des Registrierungsprofils zulassen:** Wählen Sie aus, ob auf Geräten ein Profil verwendet werden darf, das remote entfernt werden kann. Die Standardeinstellung ist **Nein**.

6. Wählen Sie unter **Optionen des iOS-Setupassistenten** die Schritte aus, die beim ersten Gerätestart durch Benutzer übersprungen werden sollen. Wenn ein Bildschirm übersprun-

gen wird, verwendet das zugehörige Feature die Standardeinstellungen. Benutzer können übersprungene Features nach Abschluss des Setups konfigurieren, sofern Sie den Zugriff darauf nicht komplett beschränken. Weitere Informationen zum Einschränken des Zugriffs auf Features finden Sie unter Geräteeinschränkungsrichtlinie. Alle Optionen sind standardmäßig deaktiviert. In den folgenden Beschreibungen wird erläutert, was die Auswahl einer Einstellung bewirkt.

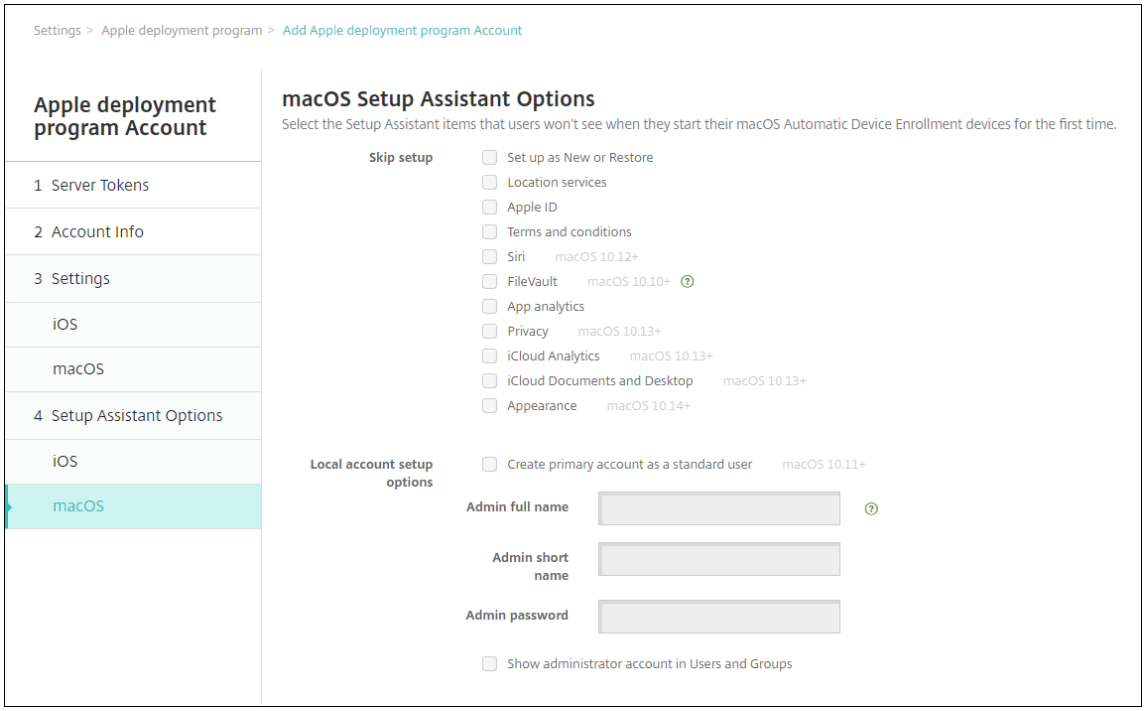


- **Ortungsdienste:** Verhindert, dass Benutzer den Ortungsdienst auf dem Gerät einrichten.
- **Touch ID:** Verhindert, dass Benutzer Touch ID oder Face ID auf iOS-Geräten einrichten.
- **Passcodesperre:** Verhindert, dass Benutzer einen Passcode für das Gerät einrichten. Wenn kein Passcode existiert, können Benutzer Touch ID oder Apple Pay nicht verwenden.
- **Neu einrichten oder wiederherstellen:** Verhindert, dass Benutzer das Gerät als neu oder als Backup von einer iCloud oder aus dem Apple App Store einrichten.
- **Verschieben von Android:** Verhindert, das Benutzer Daten von einem Android-Gerät auf ein iOS-Gerät übertragen. Diese Option ist nur verfügbar, wenn **Neu einrichten oder wiederherstellen** aktiviert wurde (d. h. der Schritt wird übersprungen).
- **Apple-ID:** Verhindert, dass Benutzer eine verwaltete Apple-ID für das Gerät einrichten.
- **AGB:** Verhindert, dass Benutzer die Nutzungsbedingungen zur Verwendung des Geräts lesen und akzeptieren.
- **Apple Pay:** Verhindert, dass Benutzer Apple Pay einrichten. Wenn diese Einstellung deaktiviert ist, müssen Benutzer Touch ID und Apple-ID einrichten. Stellen Sie sicher, dass diese Einstellungen deaktiviert sind.
- **Siri:** Verhindert, dass Benutzer Siri konfigurieren.
- **App-Analyse**: Verhindert, dass Benutzer einrichten, ob Absturzdaten und Nutzungsstatistiken an Apple weitergegeben werden sollen.
- **Anzeigezoom:** Verhindert, dass Benutzer den Anzeigezoom (Standard oder verkleinert/vergrößert) auf iOS-Geräten einrichten.

- **True Tone:** Verhindert, dass Benutzer Vierkanalsensoren einrichten, um den Weißabgleich des Displays dynamisch anzupassen.
- **Hometaste:** Verhindert, dass Benutzer den Feedbackstil der Hometaste einrichten.
- **Neue Feature-Highlights:** Verhindert, dass Benutzer Bildschirme sehen, auf denen Informationen über neue Funktionen der Apple-Software angezeigt werden.
- **Datenschutz:** Verhindert, dass Benutzer die Seite "Daten und Datenschutz" sehen. Für iOS 11.3 und höher.
- **Softwareupdate:** Verhindert, dass Benutzer iOS auf die neueste Version aktualisieren. Für iOS 12.0 und höher.
- **Bildschirmzeit:** Verhindert, dass Benutzer die Bildschirmzeit aktivieren. Für iOS 12.0 und höher.
- **SIM-Setup:** Verhindert, dass Benutzer einen Mobilfunkplan einrichten. Für iOS 12.0 und höher.
- **iMessage & FaceTime:** Verhindert, dass Benutzer iMessage und FaceTime aktivieren. Für iOS 12.0 und höher.
- **Darstellung:** Verhindert, dass Benutzer den Erscheinungsbildmodus aktivieren. Für iOS 13.0 und höher.
- **Willkommen:** Verhindert, dass Benutzer den Bildschirm **Erste Schritte** anzeigen. Für iOS 13.0 und höher.
- **Wiederherstellung abgeschlossen:** Verhindert, dass Benutzer sehen, ob eine Wiederherstellung während des Setups abgeschlossen wird. Für iOS 14.0 und höher.
- **Aktualisierung abgeschlossen:** Verhindert, dass Benutzer sehen, ob ein Softwareupdate während des Setups abgeschlossen wird. Für iOS 14.0 und höher.

Das ABM-Konto wird unter **Einstellungen > Apple-Bereitstellungsprogramm** angezeigt.

7. Wählen Sie unter **Optionen des macOS-Setupassistenten** die Schritte aus, die beim ersten Gerätestart durch die Benutzer übersprungen werden. Wenn ein Bildschirm übersprungen wird, verwendet das zugehörige Feature die Standardeinstellungen. Benutzer können übersprungene Features nach Abschluss des Setups konfigurieren, sofern Sie den Zugriff darauf nicht komplett beschränken. Weitere Informationen zum Einschränken des Zugriffs auf Features finden Sie unter Geräteeinschränkungsrichtlinie. Alle Optionen sind standardmäßig deaktiviert. In den folgenden Beschreibungen wird erläutert, was die Auswahl einer Einstellung bewirkt.



- **Neu einrichten oder wiederherstellen:** Verhindert, dass Benutzer das Gerät als neu oder als Time Machine-Backup einrichten oder eine Systemmigration durchführen.
- **Ortungsdienste:** Verhindert, dass Benutzer den Ortungsdienst auf dem Gerät einrichten. Für macOS 10.11 und höher.
- **Apple-ID:** Verhindert, dass Benutzer eine verwaltete Apple-ID für das Gerät einrichten.
- **AGB:** Verhindert, dass Benutzer die Nutzungsbedingungen zur Verwendung des Geräts lesen und akzeptieren.
- **Siri:** Verhindert, dass Benutzer Siri konfigurieren. Für macOS 10.12 und höher.
- **FileVault:** Verwendung von FileVault zum Verschlüsseln des Startvolumes. XenMobile wendet die FileVault-Einstellung nur an, wenn das System ein einziges lokales Benutzerkonto hat und das Konto an iCloud angemeldet ist.

  Sie können die Funktion “macOS FileVault-Datenträgerverschlüsselung” verwenden, um das Systemvolume durch Verschlüsselung der Inhalte zu schützen (https://support.apple.com/en-us/HT204837). Wenn Sie den Setupassistenten auf einem veralteten tragbaren Mac-Modell ausführen, für das FileVault nicht aktiviert ist, werden Sie unter Umständen dazu aufgefordert, dieses Feature zu aktivieren. Die Eingabeaufforderung wird sowohl auf neuen Systemen als auch auf Systemen angezeigt, die auf OS X 10.10 oder 10.11 aktualisiert wurden. Voraussetzung für die Anzeige der Eingabeaufforderung ist jedoch, dass das System ein einzelnes lokales Administratorkonto aufweist, das bei iCloud angemeldet ist.
- **App-Analyse**: Verhindert, dass Benutzer einrichten, ob Absturzdaten und Nutzungsstatis-

tiken an Apple weitergegeben werden sollen.

- **Datenschutz:** Verhindert, dass Benutzer die Seite “Daten und Datenschutz” sehen. Für macOS 10.13 und höher.
- **iCloud-Analyse:** Verhindert, dass Benutzer auswählen, ob sie iCloud-Diagnosedaten an Apple senden. Für macOS 10.13 und höher.
- **iCloud-Dokumente und -Desktop:** Verhindert, dass Benutzer iCloud-Desktop und -Dokumente einrichten. Für macOS 10.13 und höher.
- **Darstellung:** Verhindert, dass Benutzer den Erscheinungsbildmodus aktivieren. Für macOS 10.14 und höher.
- **Bedienungshilfen:** Verhindert, dass Benutzer automatisch Erläuterungen per Sprachausgabe hören. Nur verfügbar, wenn das Gerät mit dem Ethernet verbunden ist. Für macOS 11 und höher.
- **Biometrie:** Verhindert, dass Benutzer Touch ID und Face ID einrichten. Für macOS 10.12.4 und höher.
- **True Tone:** Verhindert, dass Benutzer Vierkanalsensoren einrichten, um den Weißabgleich des Displays dynamisch anzupassen. Für macOS 10.13.6 und höher.
- **Apple Pay:** Verhindert, dass Benutzer Apple Pay einrichten. Wenn diese Einstellung deaktiviert ist, müssen Benutzer Touch ID und Apple-ID einrichten. Stellen Sie sicher, dass die Einstellungen **Apple-ID** und **Biometrie** deaktiviert sind. Für macOS 10.12.4 und höher.
- **Bildschirmzeit:** Verhindert, dass Benutzer die Bildschirmzeit aktivieren. Für macOS 10.15 und höher.
- **Setupoptionen für lokales Konto:** Geben Sie die Einstellungen zum Erstellen eines Administratorkontos auf dem Gerät an. Benutzer melden sich mit diesen Informationen bei ihrem macOS-Gerät an. XenMobile erstellt das Konto mit den angegebenen Informationen.
  - **Erstellen Sie ein primäres Konto als Standardbenutzer:** Anstatt diesem Benutzer Administratorrechte auf dem Gerät zu gewähren, erstellt XenMobile den Benutzer mit Standardberechtigungen. Da macOS ein Administratorkonto erfordert, erstellt XenMobile zunächst ein Administratorkonto, erstellt dann ein neues Standardkonto und legt es als primäres Konto fest.
  - **Vollständiger Administratorname:** Geben Sie den Namen ein, den das System für das Administratorkonto anzeigt.
  - **Kurzname des Administrators:** Geben Sie den Namen ein, den das Gerät für den Basisordner und in der Shell anzeigt.
  - **Administratorkennwort:** Geben Sie ein sicheres Kennwort für das Administratorkonto ein.

- **Administratorkonto in "Benutzer und Gruppen" anzeigen:** Wenn diese Option deaktiviert ist, wird das Administratorkonto nicht unter **Benutzer und Gruppen** in den macOS-Einstellungen angezeigt. Wenn Sie das primäre Konto als Standardbenutzer erstellen, aktivieren Sie diese Einstellung, um das von XenMobile erstellte Administratorkonto auszublenden.

Bestellen von Deployment Program-fähigen Geräten

Sie können Deployment Program-fähige Geräte direkt bei Apple oder für Deployment Program autorisierten Wiederverkäufern und Netzbetreibern bestellen. Geben Sie für die Bestellung bei Apple Ihre Apple Kunden-ID im Apple-Bereitstellungsprogramm-Portal ein. Mit Ihrer Kunden-ID kann Apple die erworbenen Geräte mit Ihrem Apple-Bereitstellungsprogramm-Konto verknüpfen.

Wenn Sie bei einem Wiederverkäufer oder Netzbetreiber bestellen, fragen Sie Ihren Apple Wiederverkäufer oder Netzbetreiber, ob sie am Apple-Bereitstellungsprogramm teilnehmen. Fragen Sie beim Kauf der Geräte nach der Apple-Bereitstellungsprogramm-ID des Wiederverkäufers. Apple benötigt diese Informationen, wenn Sie Ihren Apple-Bereitstellungsprogramm-Wiederverkäufer zu Ihrem Apple-Bereitstellungsprogramm-Konto hinzufügen. Nach dem Hinzufügen der Apple-Bereitstellungsprogramm-ID für den Wiederverkäufer erhalten Sie eine Deployment Program-Kunden-ID. Geben Sie die Deployment Program-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 Apple-Website zur Geräteregistrierung.

Verwalten von Deployment Program-fähigen Geräten

Nach dem Versand Ihrer Bestellung können Sie iOS-, iPadOS- und macOS-Geräte mit Ihrem XenMobile-Server verknüpfen.

1. Melden Sie sich als Administrator oder Geräteregistrierungsverwalter bei Apple Business Manager an.
2. Klicken Sie in der Randleiste auf **Devices**. Geräte, die Sie direkt bei Apple erworben haben, werden automatisch angezeigt. Informationen zum Zuweisen von Geräten aus Apple Configurator 2 zu Apple Business Manager finden Sie im Apple Business Manager-Benutzerhandbuch.
3. Wählen Sie in der Liste ein Gerät oder die Gesamtzahl der Geräte aus und klicken Sie auf **Edit Device Management**. Sie haben zwei Optionen:
   - Um ein Gerät einem MDM-Server zuzuweisen, wählen Sie unter **Assign to Server** den Namen Ihres XenMobile-Servers. Klicken Sie auf **Weiter**.
     Um Apple Business Manager viele neue Geräte gleichzeitig zuzuweisen, legen Sie einen XenMobile-Standardserver für die Bereitstellung fest. Weitere Informationen finden Sie unter Festlegen eines Standardservers für die Massenregistrierung.
   - Um die Zuweisung eines Geräts zum XenMobile-Server aufzuheben, wählen Sie **Unassign**.

Ihre Apple-Bereitstellungsprogramm-Geräte sind nun dem ausgewählten XenMobile-Server zugewiesen.

Wenn Sie ein iOS-, iPadOS- oder macOS-Gerät zur Wartung einsenden, müssen Sie das Gerät aus Apple Business Manager entfernen. Wenn Sie das gewartete Gerät zurückerhalten, müssen Sie das Gerät dem XenMobile-Server neu zuweisen. Wenn Sie das Gerät austauschen, können Sie dem XenMobile-Server ein neues Gerät mit einer Bestellnummer zuweisen.

Überprüfen des Verlaufs der zugewiesenen Geräte:

1. Melden Sie sich als Administrator oder Geräteregistrierungsverwalter bei Apple Business Manager an.
2. Klicken Sie in der Randleiste auf **Assignment History**. Wählen Sie dann eine Zuweisung aus, um weitere Informationen anzuzeigen.
3. Klicken Sie auf **Download**, um eine CSV-Datei mit den Seriennummern aller zugewiesenen und nicht zugewiesenen Geräte herunterzuladen.

Sie können iOS-, iPadOS- und macOS-Geräte aus Apple Business Manager entfernen, wenn das Gerät verkauft oder gestohlen wurde oder nicht repariert werden kann.

1. Melden Sie sich als Administrator oder Geräteregistrierungsverwalter bei Apple Business Manager an.
2. Klicken in der Randleiste auf **Devices** und suchen Sie nach einem Gerät.
3. Wählen Sie ein Gerät aus und klicken Sie auf **Release Device**. Bestätigen Sie im Dialogfeld Ihre Änderungen, um das Gerät aus dem Programm zu entfernen. Um iOS- und iPadOS-Geräte wieder hinzuzufügen, verwenden Sie Apple Configurator 2. macOS-Geräte können nicht mit Apple Configurator 2 erneut hinzugefügt werden.

Registrieren von Geräten

January 6, 2022

Für die sichere Remoteverwaltung von Benutzergeräten registrieren Sie diese bei XenMobile. 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.

Die Registrierung über Azure Active Directory wird für iOS-, Android- und Windows 10- und Windows 11-Geräte unterstützt. Weitere Informationen zum Konfigurieren von Azure als Identitätsanbieter (IdP) finden Sie unter XenMobile-Integration mit Azure Active Directory als Identitätsanbieter.

> **Hinweis:**
>
> Vor dem Registrieren von iOS-Geräten müssen Sie ein APNs-Zertifikat anfordern. Einzelheiten finden Sie unter Zertifikate und Authentifizierung.

Zum Aktualisieren der Konfigurationsoptionen für Benutzer und Geräte verwenden Sie die Seite **Verwalten > Registrierungseinladungen**. Weitere Informationen finden Sie unter Senden einer Registrierungseinladung in diesem Artikel.

Android-Geräte

> **Hinweis:**
>
> Informationen zur Registrierung von Android Enterprise-Geräten finden Sie unter Android Enterprise.

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 **Next** und dann auf **Install**.
3. Wenn Secure Hub installiert ist, tippen Sie auf **Öffnen**.
4. Geben Sie Ihre geschäftlichen Anmeldeinformationen ein, z. B. den Namen des XenMobile-Servers, Ihren Benutzerprinzipalnamen oder Ihre E-Mail-Adresse. 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 nachdem, wie XenMobile konfiguriert ist, werden Sie möglicherweise aufgefordert, eine Citrix PIN zu erstellen. Mit dieser PIN können Sie sich bei Secure Hub und anderen XenMobile-aktivierten Apps wie Secure Mail und Citrix Files anmelden. 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 Geräten bereitgestellt werden, werden die Benutzer zur Installation der Apps aufgefordert. 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. Aktionen können jedoch nicht auf dem Gerät ausgeführt werden. 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:

   - Streichen Sie von der linken Seite des Bildschirms, um den Bereich “Einstellungen” zu öffnen.
   - Tippen Sie auf **Einstellungen** gefolgt von **Konten** und dann auf **Konto löschen**.

   Auf einem Tablet:

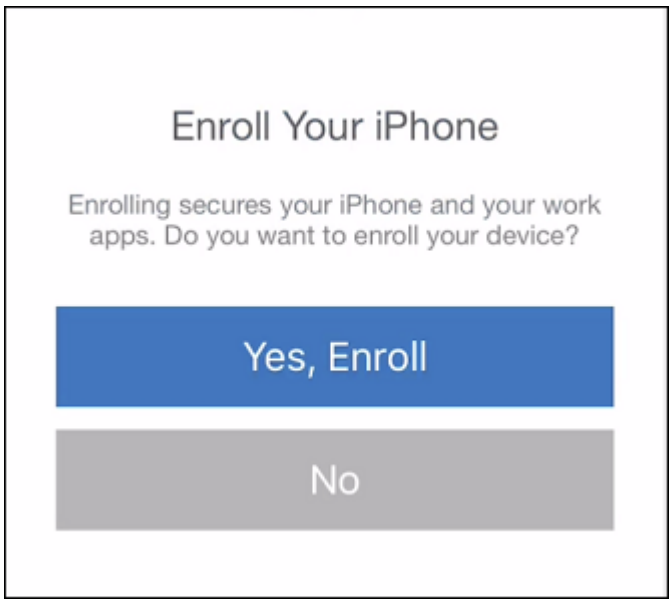
   - Tippen Sie auf den Pfeil neben Ihrer E-Mail-Adresse in der oberen rechten Ecke.
   - Tippen Sie auf **Einstellungen** gefolgt von **Konten** und dann auf **Konto löschen**.
3. Tippen Sie auf **Neu registrieren**. Eine Meldung wird angezeigt, um zu bestätigen, dass Sie das Gerät erneut registrieren 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.

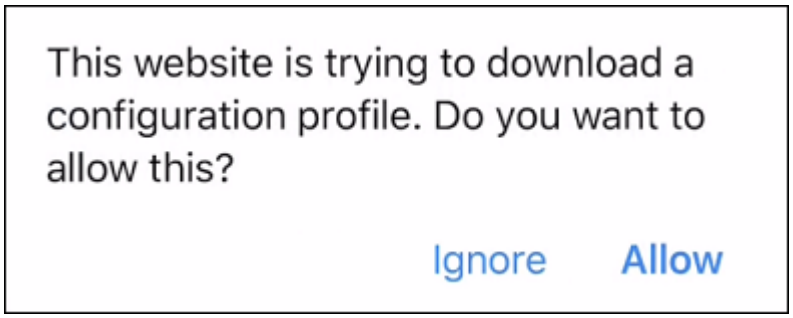
Registrieren von iOS-Geräten

In diesem Abschnitt wird erläutert, wie Benutzer iOS-Geräte (12.2 oder höher) in XenMobile Server registrieren. Weitere Informationen zur iOS-Registrierung finden Sie in folgendem Video:

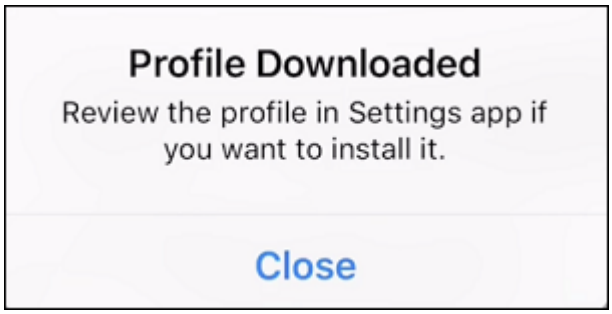
1. Rufen Sie auf dem iOS-Gerät den Apple-Store auf, laden Sie die Citrix Secure Hub-App herunter und tippen Sie auf die App.
2. Wenn Sie aufgefordert werden, die App zu installieren, tippen Sie auf **Weiter** und dann auf **Installieren**.
3. Wenn Secure Hub installiert ist, tippen Sie auf **Öffnen**.
4. Geben Sie Ihre geschäftlichen Anmeldeinformationen ein, z. B. den Namen des XenMobile-Servers, Ihren Benutzerprinzipalnamen oder Ihre E-Mail-Adresse. Klicken Sie dann auf **Weiter**.
5. Tippen Sie auf **Ja, Registrieren**, um Ihr iOS-Gerät zu registrieren.



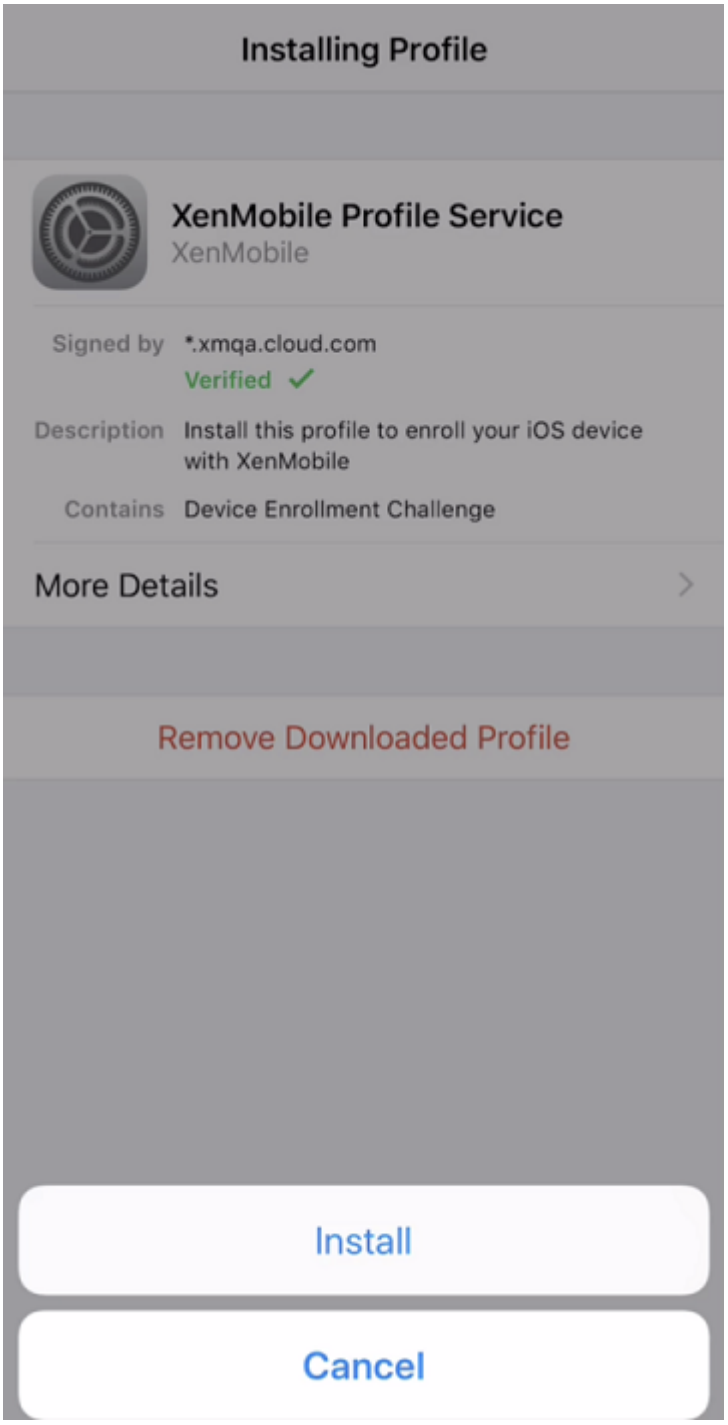
6. Nach Eingabe der Anmeldeinformationen tippen Sie auf **Zulassen**, wenn Sie dazu aufgefordert werden, um das Konfigurationsprofil herunterzuladen.



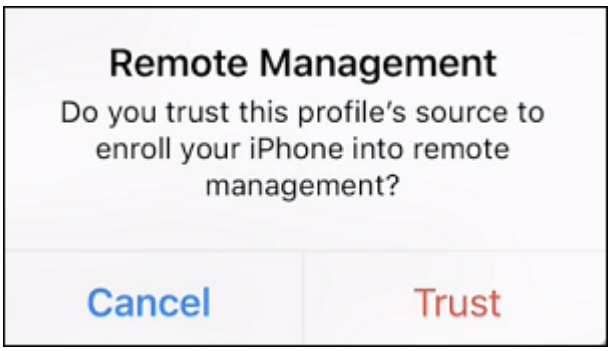
7. Tippen Sie nach dem Herunterladen des Konfigurationsprofils auf **Schließen**.



8. Installieren Sie das iOS-Zertifikat in den Geräteeinstellungen und fügen Sie das Gerät der Vertrauensliste hinzu.
    - Zum Hinzufügen des Profils gehen Sie zu **Einstellungen > Allgemein > Profil > XenMobile Profile Service** und tippen auf **Installieren**.



- Tippen Sie im Benachrichtigungsfenster auf **Vertrauensstellung**, um Ihr Gerät bei der Remoteverwaltung zu registrieren.



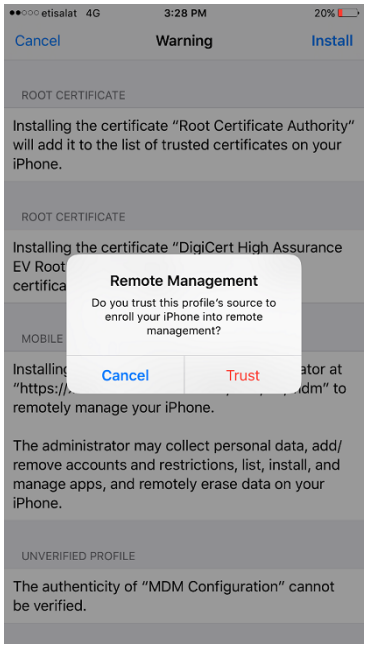
9. Melden Sie sich bei Secure Hub an. Wenn Sie sich bei MDM+MAM registrieren, werden zunächst Ihre Anmeldeinformationen überprüft. Danach werden Sie aufgefordert, Ihre Citrix-PIN zu erstellen und diese zu bestätigen.
10. Nach Abschluss des Workflows ist das Gerät registriert. Sie können nun auf den App-Store zugreifen und Apps für die Installation auf dem iOS-Gerät anzeigen.

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.

macOS-Geräte

XenMobile bietet zwei Registrierungsmethoden für Geräte, auf denen macOS ausgeführt wird. Beide Methoden ermöglichen macOS-Benutzern die Registrierung per Funk direkt über das Gerät.

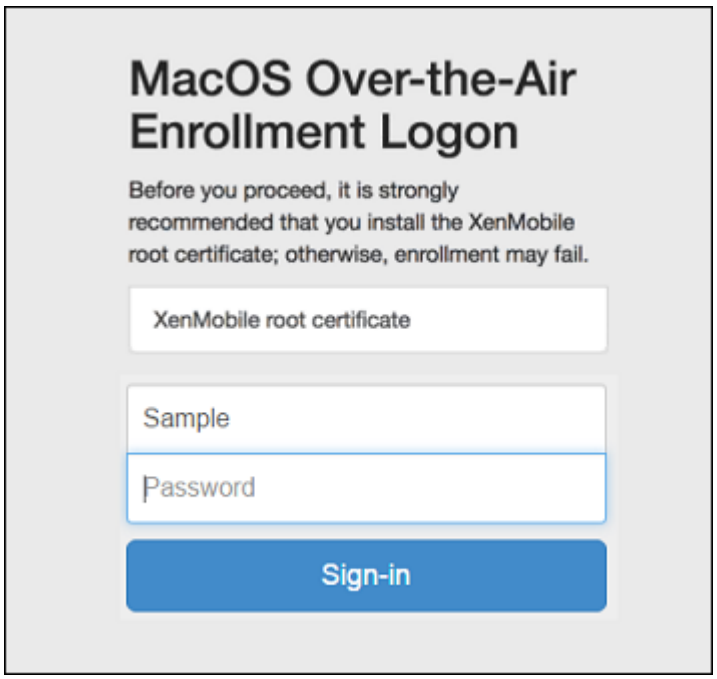
- **Senden einer Registrierungseinladung:** Bei dieser Registrierungsmethode können Sie jeden der folgenden Registrierungssicherheitsmodi für macOS-Geräte festlegen:
  - Benutzername + Kennwort
  - Benutzername + PIN
  - Zweistufig

  Wenn der Benutzer die Anweisungen in der Registrierungseinladung befolgt, wird eine Registrierungsseite angezeigt, auf der sein Name bereits eingetragen ist.
- **Senden von Installationslinks:** Bei dieser Registrierungsmethode für macOS-Geräte erhält der Benutzer einen Registrierungslink, den er in Safari oder Chrome öffnen kann. Der Benutzer registriert sich dann mit seinem Benutzernamen und Kennwort.

  Soll die Registrierung per Installationslink auf macOS-Geräten nicht verwendet werden, legen Sie die Servereigenschaft **Enable macos.OTAE** auf **false** fest. macOS-Geräte können dann nur per Registrierungseinladung registriert werden.

Senden von Registrierungseinladungen

1. Richten Sie optional macOS-Geräterichtlinien in der XenMobile-Konsole ein. Weitere Informationen zu Geräterichtlinien finden Sie unter Geräterichtlinien.
2. Fügen Sie eine Registrierungseinladung für macOS-Benutzer hinzu. Weitere Informationen finden Sie unter Senden einer Registrierungseinladung in diesem Artikel.
3. Wenn ein Benutzer die Einladung erhält und auf den Link klickt, wird in Safari folgende Seite angezeigt: Der Benutzername wird von XenMobile eingetragen. Wenn Sie den Registrierungssicherheitsmodus **Zweistufig** auswählen, wird ein weiteres Feld angezeigt.



4. Die Benutzer installieren die benötigten Zertifikate. Ob Benutzer zur Installation von Zertifikaten aufgefordert werden, hängt davon ab, ob Sie ein öffentlich vertrauenswürdiges SSL-Zertifikat und ein öffentlich vertrauenswürdiges digitales Signaturzertifikat für macOS konfiguriert haben. Weitere Informationen über Zertifikate finden Sie unter Zertifikate und Authentifizierung.
5. Der Benutzer gibt die angeforderten Anmeldeinformationen ein.

   Die Mac-Geräterichtlinien werden installiert. Sie können Macs nun mit XenMobile genauso verwalten wie Mobilgeräte.

Senden von Installationslinks

1. Richten Sie optional macOS-Geräterichtlinien in der XenMobile-Konsole ein. Weitere Informationen zu Geräterichtlinien finden Sie unter Geräterichtlinien.
2. Senden Sie den Registrierungslink `https://serverFQDN:8443/instanceName/macos/otae`, den die Benutzer in Safari oder Chrome öffnen können.
   - **serverFQDN** ist 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.
   - **instanceName**, oft als “zdm” dargestellt, ist der Name, der bei der Serverinstallation angegeben wird.

Weitere Informationen zum Senden von Installationslinks finden Sie unter Senden von Installationslinks.

3. Die Benutzer installieren die benötigten Zertifikate. Wenn Sie ein öffentlich vertrauenswürdiges SSL-Zertifikat und ein 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 und Authentifizierung.
4. Die Benutzer melden sich bei ihren Macs an.

   Die Mac-Geräterichtlinien werden installiert. Sie können Macs nun mit XenMobile genauso verwalten wie Mobilgeräte.

Windows-Geräte

> **Hinweis:**
>
> Dieser Abschnitt enthält Verweise auf Windows Phone 8.1-Geräte, für die Microsoft am 11. Juli 2017 das Ende des Supports bekanntgegeben hat. XenMobile unterstützt Windows Phone 8.1-Geräte nur für die MDM-Registrierung.

Windows 10- und Windows 11-Geräte werden mit Microsoft Azure als Active Directory-Verbundauthentifizierung registriert. Sie können Microsoft Azure AD Windows 10- und Windows 11-Geräte mit einem der folgenden Verfahren hinzufügen:

- Registrierung bei MDM im Rahmen des Standardbeitritts zu Azure AD beim ersten Einschalten des Geräts
- Registrierung bei MDM im Rahmen des Beitritts zu Azure AD unter Verwendung der Seite “Windows-Einstellungen” nach dem Konfigurieren des Geräts

Sie können in XenMobile Geräte mit folgenden Windows-Betriebssystemen registrieren:

- Windows 10 Phone
- Windows 10
- Windows 11
- Windows Phone 8.1

Benutzer können sich direkt über ihre Geräte registrieren.

> **Hinweis:**
>
> Benutzer von Windows 10 RS2 Phone- und Tablet-Geräten werden bei der Neuregistrierung nicht zur Eingabe der Server-URL aufgefordert. Starten Sie als Workaround das Gerät neu. Alternativ tippen Sie auf dem Bildschirm mit der E-Mail-Adresse auf das X für den Aufbau der Verbindung mit einem Dienst und navigieren Sie zu der Seite **Server-URL**. Dies ist ein Drittanbieterproblem.

Sie müssen Autodiscovery und den Windows-Ermittlungsdienst für die Benutzerregistrierung aktivieren, um die Verwaltung von unterstützten Windows-Geräten zu ermöglichen.

Bevor Benutzer von Windows-Geräten sich über Azure registrieren können, müssen Sie die Servereinstellungen zu Microsoft Azure in XenMobile konfigurieren. Weitere Informationen finden Sie unter Einstellungen des Microsoft Azure Active Directory-Servers.

Registrieren von Windows-Geräten mit Autodiscovery

Um die Verwaltung von Windows-Geräten zu ermöglichen, empfiehlt Citrix, dass Sie den Autodiscovery-Dienst und den Windows-Ermittlungsdienst konfigurieren. Weitere Informationen finden Sie unter XenMobile Autodiscovery Service.

1. Prüfen Sie auf dem Gerät auf Updates und installieren Sie alle verfügbaren Windows-Updates.
2. Für Windows 10 und Windows 11: Tippen Sie im Menü "Charms" auf **Einstellungen** und dann auf **Konten > Arbeitsplatz oder Schule > Mit Arbeitsplatz oder Schule verbinden**. Für Windows 8.1-Telefone: Tippen Sie auf **PC-Einstellungen > Netzwerk > Arbeitsbereich**.
3. Windows 10 und Windows 11: Geben Sie Ihre geschäftliche E-Mail-Adresse ein und tippen Sie auf **Weiter**. Windows 8.1: Tippen Sie auf **Geräteverwaltung einschalten**. Zur Registrierung als lokaler Benutzer geben Sie eine nicht vorhandene E-Mail-Adresse mit dem richtigen Domänennamen (z. B. `foo@mydomain.com`) ein. Dies ermöglicht die Umgehung einer bekannten Microsoft-Einschränkung, 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 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. Für Windows 10 und Windows 11: Geben Sie im Dialogfeld **Nutzungsbedingungen** an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie dann auf **Annehmen**. Für Windows 8.1: Geben Sie im Dialogfeld **Apps und Dienste des IT-Administrators zulassen** an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie auf **Einschalten**.

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.

2. Für Windows 10 und Windows 11: Tippen Sie im Menü “Charms” auf **Einstellungen** und dann auf **Konten > Arbeitsplatz oder Schule > Mit Arbeitsplatz oder Schule verbinden**. Für Windows 8.1: Tippen Sie auf **PC-Einstellungen > Netzwerk > Arbeitsbereich**.
3. Geben Sie Ihre geschäftliche E-Mail-Adresse ein.
4. Windows 10 und Windows 11: Wenn Autodiscovery nicht konfiguriert ist, wird eine Option zur Eingabe der Serverinformationen (siehe Schritt 5) angezeigt. Für Windows 8.1: Wenn das **automatische Erkennen der Serveradresse** auf **Aktiviert** gesetzt ist, tippen Sie darauf, um die Option auf **Aus** zu setzen.
5. Windows 10 und Windows 11: Geben Sie im Feld **Serveradresse eingeben** folgende Adresse ein: `https://serverfqdn:8443/serverInstance/wpe`.

   Wenn für SSL-Verbindungen ohne Authentifizierung eine andere Portnummer als 8443 verwendet wird, geben Sie die verwendete Portnummer mit der Adresse ein.

   Für Windows 8.1: Geben Sie die Serveradresse im folgenden Format ein: `https://serverfqdn:8443/serverInstance/Discovery.svc`.

   Wenn für SSL-Verbindungen ohne Authentifizierung eine andere Portnummer als 8443 verwendet wird, geben Sie die verwendete Portnummer mit der Adresse ein.
6. Geben Sie das Kennwort ein.
7. Für Windows 10 und Windows 11: Geben Sie im Dialogfeld **Nutzungsbedingungen** an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie dann auf **Annehmen**. Für Windows 8.1: Geben Sie im Dialogfeld **Apps und Dienste des IT-Administrators zulassen** an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie auf **Einschalten**.

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 von XenMobile Server. 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**.
   - Windows 10 und Windows 11: Tippen Sie je nach Version entweder auf **Konten > Arbeitsplatz oder Schule > Mit Arbeitsplatz oder Schule verbinden** oder auf **Konten > Arbeitsplatzzugriff > Für MDM-Verwaltungsdienst registrieren**.

- Für Windows 8.1: Tippen Sie 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://<xenmobile_server>:<portnumber>/<instancename>/wpe`. Beispiel: `https://mycompany.mdm.com:8443/zdm/wpe`.

   > **Hinweis:**
   >
   > Die Portnummer muss gemäß der vorliegenden Implementierung geändert werden. Es muss der gleiche Port verwendet werden wie für die iOS-Registrierung.

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 das Konto unter Windows Phone 8.1 hinzugefügt wurde, wird die Option **Unternehmensapp 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.

6. Tippen Sie unter Windows Phone 8.1 im Bildschirm **Konto hinzugefügt** auf **Fertig**.

7. 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-, macOS-, Android Enterprise-Geräten und Android-Legacygeräten senden. Sie können auch einen Installationslink an Benutzer mit iOS- oder Android Enterprise-Geräten oder Android-Legacygeräten senden.

Registrierungseinladungen werden wie folgt gesendet:

- Registrierungseinladungen für einzelne lokale oder Active Directory-Benutzer erhalten die Benutzer per SMS unter der von Ihnen angegebenen Telefonnummer und dem von Ihnen angegebenen Netzbetreibernamen.
- Registrierungseinladungen für Gruppen erhalten die Benutzer per SMS. Active Directory-Benutzer mit einer in Active Directory verzeichneten E-Mail-Adresse und Mobiltelefonnummer erhalten die Einladung. Lokale Benutzer erhalten die Einladung über die in den Benutzereigenschaften angegebene E-Mail-Adresse und Telefonnummer.

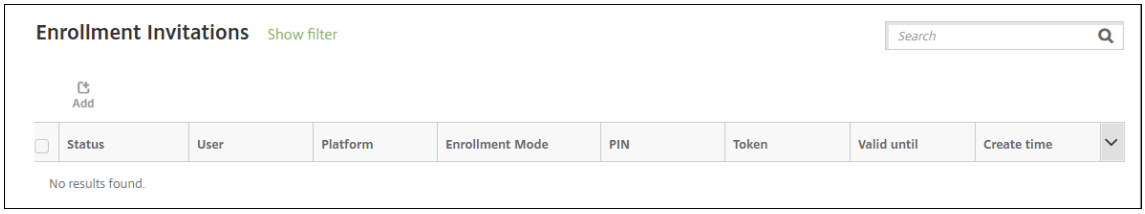
Nach der Registrierung werden die betreffenden Geräte unter **Verwalten > Geräte** als verwaltet angezeigt. Der Status der Einladungs-URL wird als **Angenommen** angezeigt.

Voraussetzungen

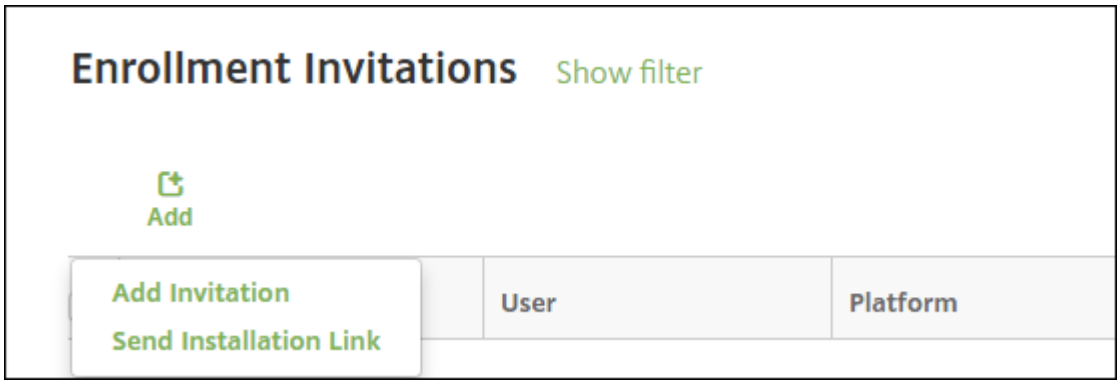
- XenMobile Server im Enterprise- (XME) oder MDM-Modus konfiguriert
- LDAP konfiguriert
- Bei Verwendung lokaler Gruppen und Benutzer:
  - Eine oder mehrere lokale Gruppen
  - Lokale Benutzer, die lokalen Gruppen zugewiesen sind
  - Bereitstellungsgruppen, die lokalen Gruppen zugeordnet sind
- Bei Verwendung von Active Directory:
  - Bereitstellungsgruppen, die Active Directory-Gruppen zugeordnet sind

Erstellen von Registrierungseinladungen

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



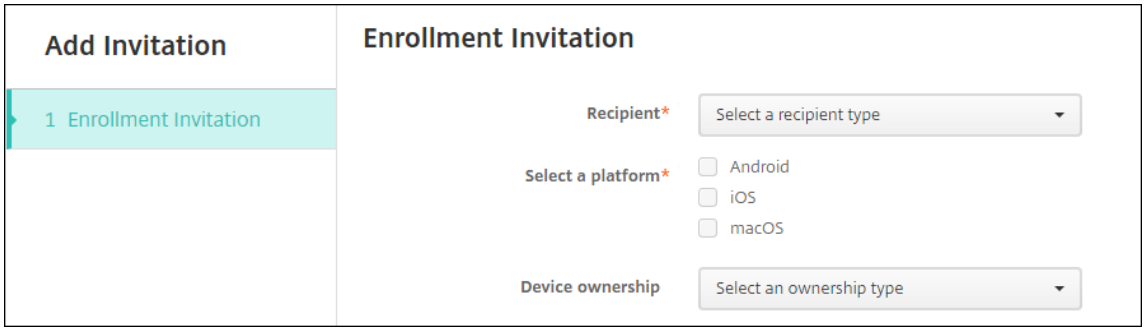
2. Klicken Sie auf **Hinzufügen**. Ein Menü mit Registrierungsoptionen wird eingeblendet.



   - Zum Senden einer Registrierungseinladung an einen Benutzer oder eine Gruppe klicken Sie auf **Einladung hinzufügen**.
   - Zum Senden eines Installationslinks an eine Reihe von Benutzern über SMTP oder per SMS klicken Sie auf **Installationslink senden**.

   Das Senden von Registrierungseinladungen und Installationslinks wird weiter unten beschrieben.

3. Klicken Sie auf **Einladung hinzufügen**. Die Seite **Registrierungseinladung** wird angezeigt.



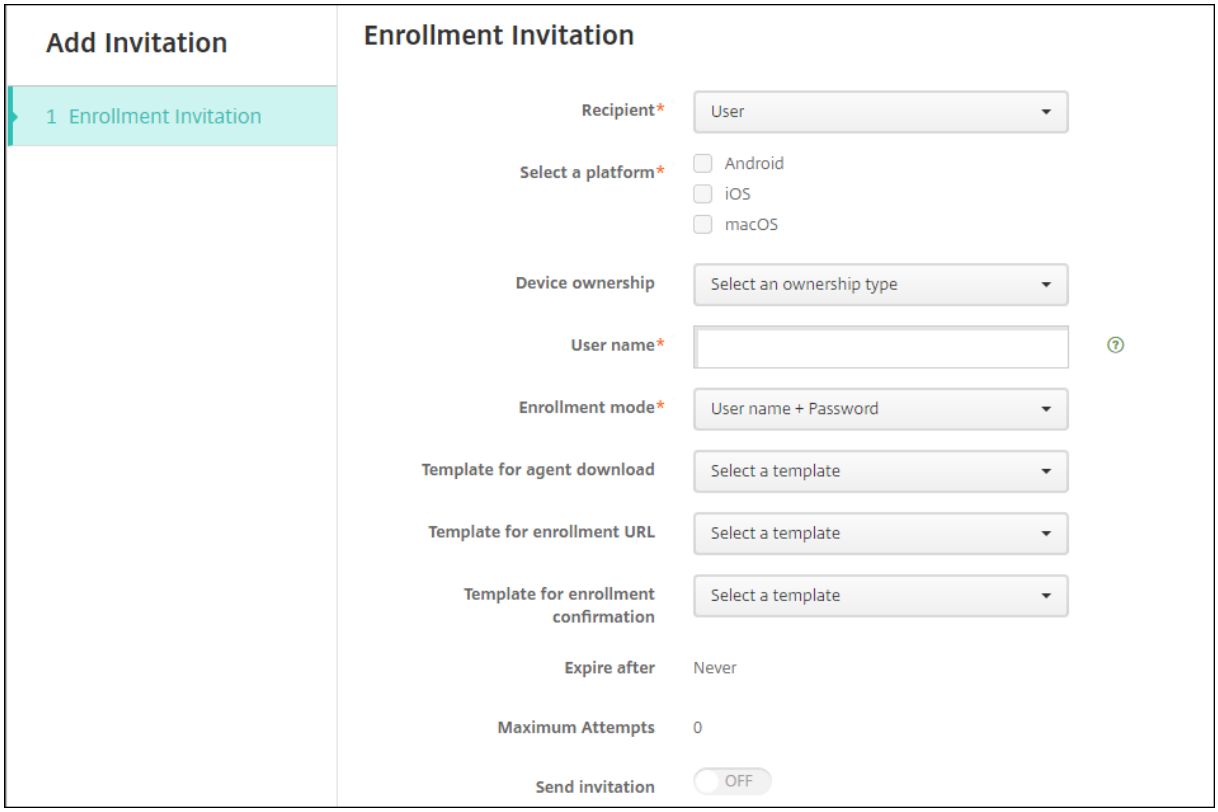
4. Konfigurieren Sie folgende Einstellungen:

   - **Empfänger:** Wählen Sie **Gruppe** oder **Benutzer**.
   - **Wählen Sie eine Plattform:** Bei Auswahl von **Gruppe** für **Empfänger** sind alle Plattformen ausgewählt. Sie können die Plattformauswahl ändern. Bei Auswahl von **Benutzer** für **Empfänger** ist keine Plattform ausgewählt. Wählen Sie eine Plattform.

     Um eine Registrierungseinladung für Android Enterprise-Geräte zu erstellen, wählen Sie **Android > Android Enterprise**.
   - **Gerätebesitz:** Wählen Sie **Unternehmen** oder **Mitarbeiter**.

   Es werden die in den folgenden Abschnitten beschriebenen Einstellungen für Benutzer oder Gruppen angezeigt.

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 in XenMobile Server oder als Active Directory-Benutzer vorliegen. Stellen Sie bei lokalen Benutzern sicher, dass die E-Mail Eigenschaft eingestellt ist, damit Benachrichtigungen an sie gesendet werden können. Bei Active Directory-Benutzern muss LDAP konfiguriert sein.
    - **Geräteinfo:** Diese Einstellung wird nicht angezeigt, wenn Sie mehrere Plattformen oder nur macOS wählen. Wählen Sie **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:** Diese Einstellung wird nicht angezeigt, wenn Sie mehrere Plattformen oder nur macOS wählen. Geben Sie optional die Telefonnummer des Benutzers ein.
    - **Netzbetreiber:** Diese Einstellung wird nicht angezeigt, wenn Sie mehrere Plattformen oder nur macOS wählen. Wählen Sie einen Netzbetreiber für die Zuordnung zu der Telefonnummer des Benutzers.
    - **Registrierungsmodus:** Wählen Sie den Registrierungssicherheitsmodus für Benutzer. Die Standardeinstellung ist **Benutzername + Kennwort**. Einige der folgenden Optionen stehen nicht für alle Plattformen zur Verfügung:
        - Benutzername + Kennwort

- Hohe Sicherheit
- Einladungs-URL
- Einladungs-URL + PIN
- Einladungs-URL + Kennwort
- Zweistufig
- Benutzername + PIN

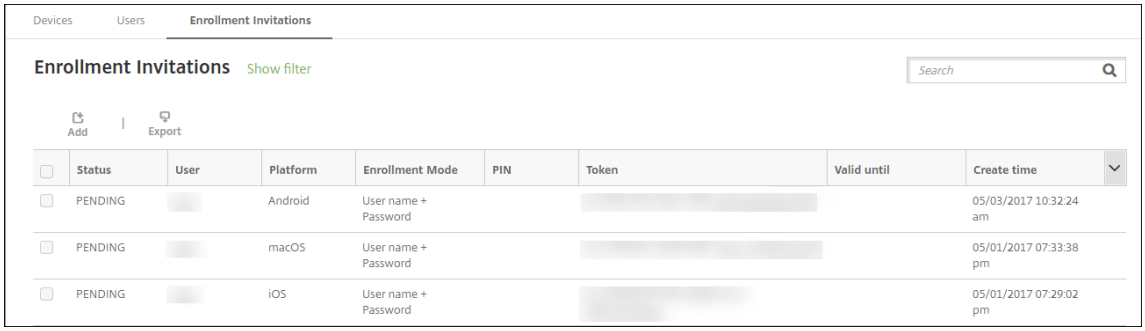
Um Registrierungseinladungen zu senden, können Sie nur die Registrierungsicherheitsmodi **Einladungs-URL**, **Einladungs-URL + PIN** oder **Einladungs-URL + Kennwort** verwenden. Für Geräte, die mit **Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** registriert werden, müssen Benutzer ihre Anmeldeinformationen manuell in Secure Hub eingeben.

Eine PIN für die Registrierung wird auch als “Einmal-PIN” bezeichnet. Solche PINs gelten nur bei der Registrierung.

> **Hinweis:**
>
> Wenn Sie einen Registrierungssicherheitsmodus mit PIN auswählen, wird das Feld **Vorlage für Registrierungs-PIN** eingeblendet, in dem Sie auf **Registrierungs-PIN** klicken.

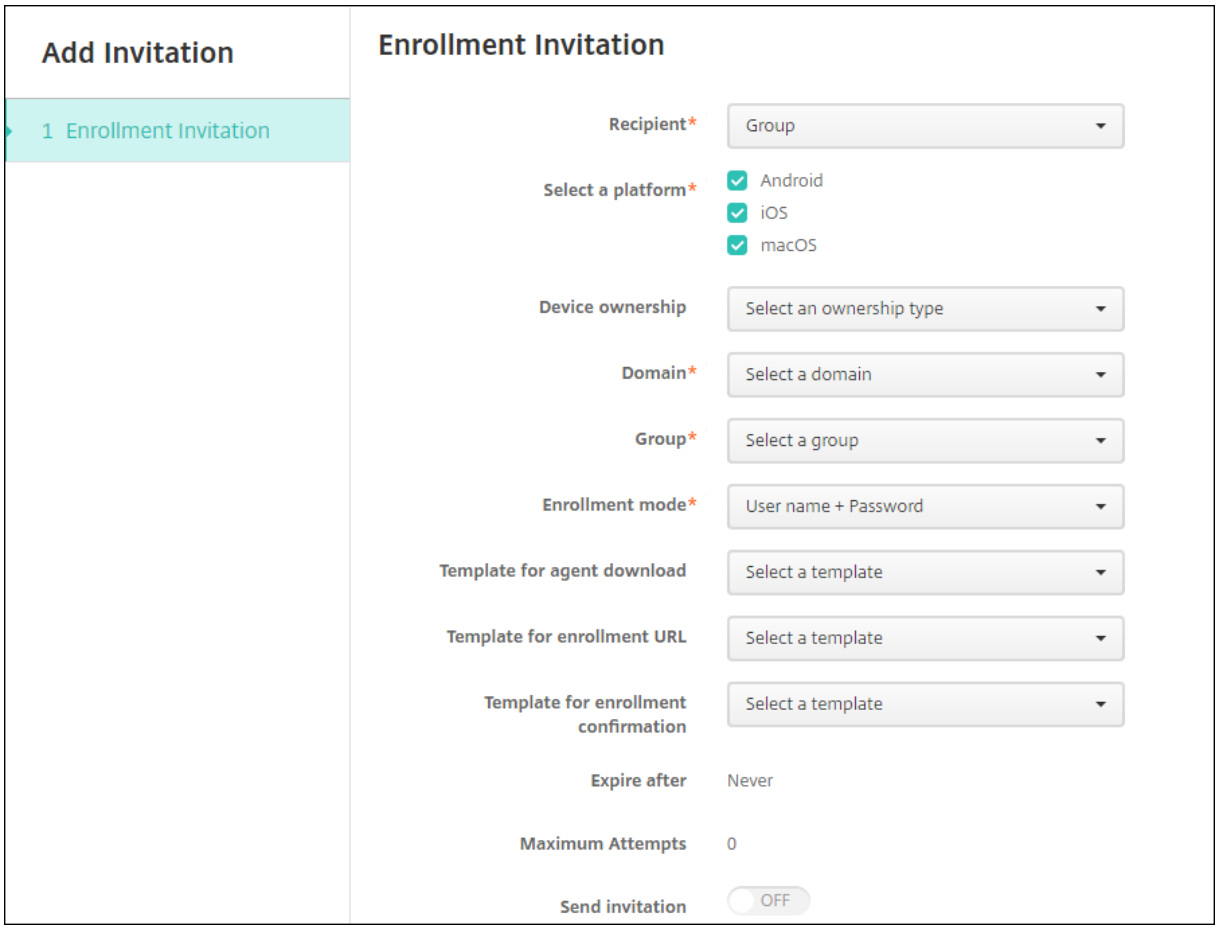
- **Vorlage für Agentdownload:** Wählen Sie die Downloadlinkvorlage **Downloadlink**. Diese Vorlage ist für alle unterstützten Plattformen vorgesehen.
- **Vorlage für Registrierungs-URL:** Wählen Sie **Registrierungseinladung**.
- **Vorlage für Registrierungsbestätigung:** Wählen Sie **Registrierungsbestätigung**.
- **Ablauf nach:** Dieses Feld wird ausgefüllt, wenn Sie den Registrierungsmodus konfigurieren. Es gibt an, wann die Registrierung abläuft. Weitere Informationen zum Konfigurieren von Registrierungssicherheitsmodi finden Sie unter Konfigurieren von Registrierungssicherheitsmodi.
- **Versuche maximal:** Dieser Wert wird festgelegt, wenn Sie den **Registrierungsmodus** konfigurieren. Er gibt an, wie oft der Registrierungsprozess maximal durchgeführt wird. Weitere Informationen zum Konfigurieren von Registrierungssicherheitsmodi finden Sie unter Konfigurieren von Registrierungssicherheitsmodi.
- **Einladung senden:** Wählen Sie **EIN**, um die Einladung sofort zu senden. Wählen Sie **AUS**, um die Einladung ohne zu senden in die Tabelle auf der Seite **Registrierungseinladungen** einzufügen.

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 **Registrierungseinladungen** aufgeführt.



Senden einer Registrierungseinladung an eine Gruppe

Die folgende Abbildung zeigt die Einstellungen zum Konfigurieren einer Registrierungseinladung für eine Gruppe.



1. Konfigurieren Sie folgende Einstellungen:
   - **Domäne:** Wählen Sie die Domäne der Gruppe, die die Einladung erhalten soll.
   - **Gruppe:** Wählen Sie die Gruppe, die die Einladung erhalten soll.
   - **Registrierungsmodus:** Wählen Sie die gewünschte Registrierungsmethode. Die Standardeinstellung ist **Benutzername + Kennwort**. Einige der folgenden Optionen stehen

nicht für alle Plattformen zur Verfügung:
- Benutzername + Kennwort
- Hohe Sicherheit
- Einladungs-URL
- Einladungs-URL + PIN
- Einladungs-URL + Kennwort
- Zweistufig
- Benutzername + PIN

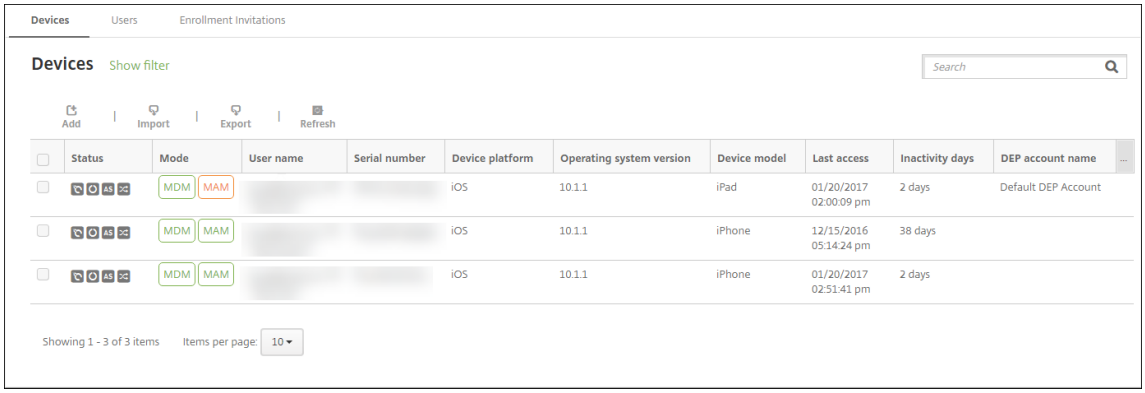
Um Registrierungseinladungen zu senden, können Sie nur die Registrierungsicherheitsmodi **Einladungs-URL**, **Einladungs-URL + PIN** oder **Einladungs-URL + Kennwort** verwenden. Für Geräte, die mit **Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** registriert werden, müssen Benutzer ihre Anmeldeinformationen manuell in Secure Hub eingeben.

Es werden nur die Registrierungssicherheitsmodi angezeigt, die für die ausgewählten Plattformen zulässig sind.

> **Hinweis:**
>
> Wenn Sie einen Registrierungssicherheitsmodus mit PIN auswählen, wird das Feld **Vorlage für Registrierungs-PIN** eingeblendet, in dem Sie auf **Registrierungs-PIN** klicken.

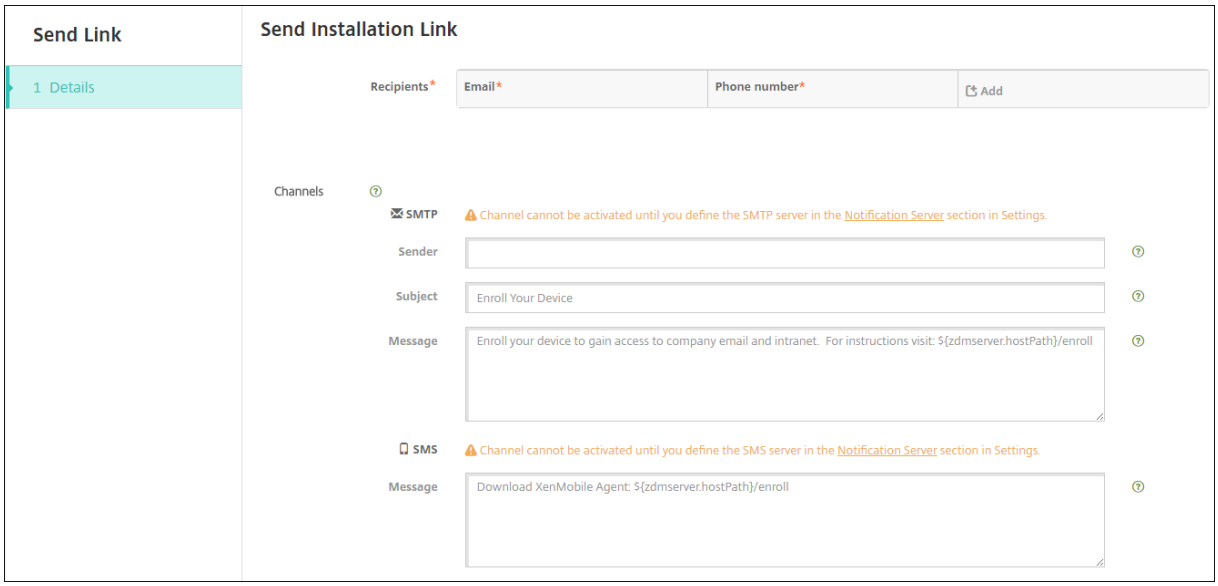
- **Vorlage für Agentdownload:** Wählen Sie die Downloadlinkvorlage **Downloadlink**. Diese Vorlage ist für alle unterstützten Plattformen vorgesehen.
- **Vorlage für Registrierungs-URL:** Wählen Sie **Registrierungseinladung**.
- **Vorlage für Registrierungsbestätigung:** Wählen Sie **Registrierungsbestätigung**.
- **Ablauf nach:** Dieses Feld wird ausgefüllt, wenn Sie den Registrierungsmodus konfigurieren. Es gibt an, wann die Registrierung abläuft. Weitere Informationen zum Konfigurieren von Registrierungssicherheitsmodi finden Sie unter Konfigurieren von Registrierungssicherheitsmodi.
- **Versuche maximal:** Dieser Wert wird festgelegt, wenn Sie den “Registrierungsmodus” konfigurieren. Er gibt an, wie oft der Registrierungsprozess maximal durchgeführt wird. Weitere Informationen zum Konfigurieren von Registrierungssicherheitsmodi finden Sie unter Konfigurieren von Registrierungssicherheitsmodi.
- **Einladung senden:** Wählen Sie **EIN**, um die Einladung sofort zu senden. Wählen Sie **AUS**, um die Einladung ohne zu senden in die Tabelle auf der Seite **Registrierungseinladungen** einzufügen.

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 **Registrierungseinladung** 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. Weitere Informationen finden Sie unter [Benachrichtigungen](/de-de/xenmobile/server/users/notifications.html



1. Konfigurieren Sie die Einstellungen und klicken Sie auf **Speichern**.
   - **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.

> **Hinweis:**
>
> Zum Löschen eines 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. Details 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 Unternehmensapps 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:**
>
> Wird in der Umgebung sAMAccountName verwendet, müssen Benutzer nach dem Erhalt der Einladung auf den Link klicken und dann den Benutzernamen ändern, um die Authentifizierung abzuschließen. Der Benutzername wird in der Form sAMAccountName@domänenname.com angezeigt. Die Benutzer müssen den Teil “@domänenname.com” entfernen.

Registrierungssicherheitsmodi nach Plattform

Die folgende Tabelle enthält Sicherheitsmodi, mit denen Sie Benutzergeräte registrieren können. Ein **Ja** in der Tabelle zeigt an, welche Geräteplattformen bestimmte Registrierungs- und Verwaltungsmodi mit unterschiedlichen Registrierungsprofilen unterstützen.

MDM-Registrierung	MAM-Registrierung auf Citrix Gateway	Registrierungssicherheitsmodus	Unterstützung verschiedener Registrierungsprofilmodi	Android (Legacy)	Android Enterprise	iOS (Benutzerregistrierungsmodus)	iOS	macOS	Windows
Azure AD und Okta als Identitätsanbieter über Citrix Cloud	Clientzer	MDM+M/ oder MDM	Ja	Ja	Ja	Ja	Ja	Nein	Nein

MDM-Registrierung	MAM-Registrierung	Sicherheitsanforderungen	Unterstützung verschiedener Registrierungsmodi	Android (Legacy)	Android Enterprise	iOS (Benutzerregistrierung)	iOS	macOS	Windows
Benutzername + Kennwort	LDAP, LDAP + Clientzertifikat, nur Clientzertifikat	MDM+MAM, MDM oder MAM (Nur-MAM-Modus unterstützt keine Clientzertifikate auf Citrix Gateway)	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Einladung-URL	Clientzer	MDM+M oder MDM	Ja	Ja	Ja	Nein	Ja	Nein	Nein
Einladungs-URL + PIN	Clientzertifikat	MDM+MAM oder MDM	Ja	Ja	Ja	Nein	Ja	Nein	Nein
Einladung-URL + Kennwort	LDAP, LDAP + Clientzertifikat, nur Clientzertifikat	MDM+M oder MDM	Ja	Ja	Ja	Nein	Ja	Nein	Nein

MDM-Registrierung	MAM-Registrierung auf Citrix Gateway	Registrierungssicherheitsmodus	Unterstützung verschiedener Registrierungsprofile	Android (Legacy)	Android Enterprise	iOS (Benutzerregistrierung)	iOS	macOS	Windows
Zweistufige Authentifizierung (Benutzername + Kennwort + PIN)	LDAP, LDAP + Clientzertifikat, nur Clientzertifikat	MDM+MAM oder MDM	Ja	Ja	Ja	Nein	Ja	Ja	Nein
Benutze + PIN	Clientze	MDM+M oder MDM	Ja	Ja	Ja	Nein	Ja	Ja	Nein

Im Folgenden wird beschrieben, wie sich die Registrierungssicherheitsmodi auf iOS-, Android- und Android Enterprise-Geräten verhalten:

- **Benutzername + Kennwort** (Standard)
  - Sendet Benutzern eine Benachrichtigung mit einer Registrierungs-URL. Klickt der Benutzer auf die URL, wird Secure Hub geöffnet. Der Benutzer gibt einen Benutzernamen und ein Kennwort ein, um das Gerät in XenMobile zu registrieren.
- **Einladungs-URL**
  - Sendet Benutzern eine Benachrichtigung mit einer Registrierungs-URL. Klickt der Benutzer auf die URL, wird Secure Hub geöffnet. Der Name des XenMobile Servers und die Schaltfläche **Ja, registrieren** werden angezeigt. Der Benutzer tippt auf **Ja, registrieren**, um das Gerät in XenMobile zu registrieren.
- **Einladungs-URL + PIN**
  - Sendet Benutzern die folgenden E-Mails:
    * Eine E-Mail mit einer Registrierungs-URL, mit der der Benutzer das Gerät über Secure Hub in XenMobile registrieren kann.
    * Eine E-Mail mit einer Einmal-PIN, die der Benutzer bei der Registrierung des Geräts zusammen mit seinem Active Directory-Kennwort (bzw. dem lokalen Kennwort) eingeben muss

  - In diesem Modus registrieren sich Benutzer nur über die Registrierungs-URL in der Benachrichtigung. Wenn ein Benutzer eine Einladungsbenachrichtigung verliert, kann er keine Registrierung durchführen. Sie können jedoch eine neue Einladung senden.
- **Einladungs-URL + Kennwort**
  - Sendet Benutzern eine Benachrichtigung mit einer Registrierungs-URL. Klickt der Benutzer auf die URL, wird Secure Hub geöffnet. Der Name des XenMobile Servers und ein Feld zur Eingabe eines Kennworts werden eingeblendet.
- **Zweistufig**
  - Sendet Benutzern eine Benachrichtigung mit einer Registrierungs-URL und einer Einmal-PIN. Klickt der Benutzer auf die URL, wird Secure Hub geöffnet. Es werden der Name des XenMobile Servers und zwei Felder zur Eingabe von Kennwort und PIN eingeblendet.
- **Benutzername + PIN**
  - Sendet Benutzern die folgenden E-Mails:
    * Eine E-Mail mit einer Registrierungs-URL zum Herunterladen und Installieren von Secure Hub. Wenn Secure Hub geöffnet wird, wird der Benutzer zur Eingabe eines Benutzernamens und Kennworts aufgefordert, um sein Gerät in XenMobile zu registrieren.
    * Eine E-Mail mit einer Einmal-PIN, die der Benutzer bei der Registrierung des Geräts zusammen mit seinem Active Directory-Kennwort (bzw. dem lokalen Kennwort) eingeben muss
  - Wenn ein Benutzer eine Einladungsbenachrichtigung verliert, kann er keine Registrierung durchführen. Sie können jedoch eine neue Einladung senden.

Im Folgenden wird beschrieben, wie sich die Registrierungssicherheitsmodi auf macOS-Geräten verhalten:

- **Benutzername + Kennwort**
  - Sendet Benutzern eine Benachrichtigung mit einer Registrierungs-URL. Wenn der Benutzer auf die URL klickt, wird der Safari-Browser geöffnet. Eine Registrierungsseite wird angezeigt, auf der der Benutzer aufgefordert wird, einen Benutzernamen und ein Kennwort einzugeben, um sein Gerät in XenMobile zu registrieren.
- **Zweistufig**
  - Sendet Benutzern eine Benachrichtigung mit einer Registrierungs-URL und einer Einmal-PIN. Wenn der Benutzer auf die URL klickt, wird der Safari-Browser geöffnet. Eine Anmeldeseite mit zwei Feldern zur Eingabe von Kennwort und PIN wird geöffnet.
- **Benutzername + PIN**
  - Sendet Benutzern die folgenden E-Mails:
    * Eine E-Mail mit einer Registrierungs-URL. Wenn der Benutzer auf die URL klickt, wird der Safari-Browser geöffnet. Eine Registrierungsseite wird angezeigt, auf der der Benutzer aufgefordert wird, einen Benutzernamen und ein Kennwort einzugeben, um sein Gerät in XenMobile zu registrieren.

    * Eine E-Mail mit einer Einmal-PIN, die der Benutzer bei der Registrierung des Geräts zusammen mit seinem Active Directory-Kennwort (bzw. dem lokalen Kennwort) eingeben muss
  - Wenn ein Benutzer eine Einladungsbenachrichtigung verliert, kann er keine Registrierung durchführen. Sie können jedoch eine neue Einladung senden.

Sie können keine Registrierungseinladungen an Windows-Geräte senden. Benutzer von Windows-Geräten registrieren diese direkt über das Gerät.

Firebase Cloud Messaging

January 5, 2022

> **Hinweis:**
>
> Firebase Cloud Messaging (FCM) war zuvor als Google Cloud Messaging (GCM) bekannt. Bei einigen Beschriftungen und Meldungen für die XenMobile-Konsole wird GCM-Terminologie verwendet.

Citrix empfiehlt, dass Sie mit Firebase Cloud Messaging (FCM) steuern, wie und wann Android-Geräte eine Verbindung zu XenMobile herstellen. Ist XenMobile für FCM konfiguriert, sendet es Verbindungsbenachrichtigungen an Android-Geräte, die für FCM aktiviert sind. Jede Sicherheitsaktion und jeder Bereitstellungsbefehl löst eine Pushbenachrichtigung aus, sodass der Benutzer aufgefordert wird, erneut eine Verbindung mit XenMobile herzustellen.

Wenn ein Gerät nach Abschluss der in diesem Artikel beschriebenen Konfigurationsschritte eingecheckt wird, wird es beim FCM-Dienst in XenMobile Server registriert. Über diese Verbindung können Ihr XenMobile-Dienst und Ihr Gerät mittels FCM nahezu in Echtzeit miteinander kommunizieren. Die FCM-Registrierung funktioniert bei neuen und zuvor registrierten Geräten.

Wenn XenMobile sich mit dem Gerät verbinden muss, stellt es eine Verbindung zum FCM-Dienst her. Dieser benachrichtigt das Gerät, das dann eine Verbindung herstellt. Verbindungen dieser Art ähneln dem Verfahren, das Apple für seinen Push-Benachrichtigungsdienst verwendet.

Voraussetzungen

- Neuester Secure Hub-Client
- Anmeldeinformationen für Google Developer-Konto
- Google Play auf FCM-aktivierten Android-Geräten installiert

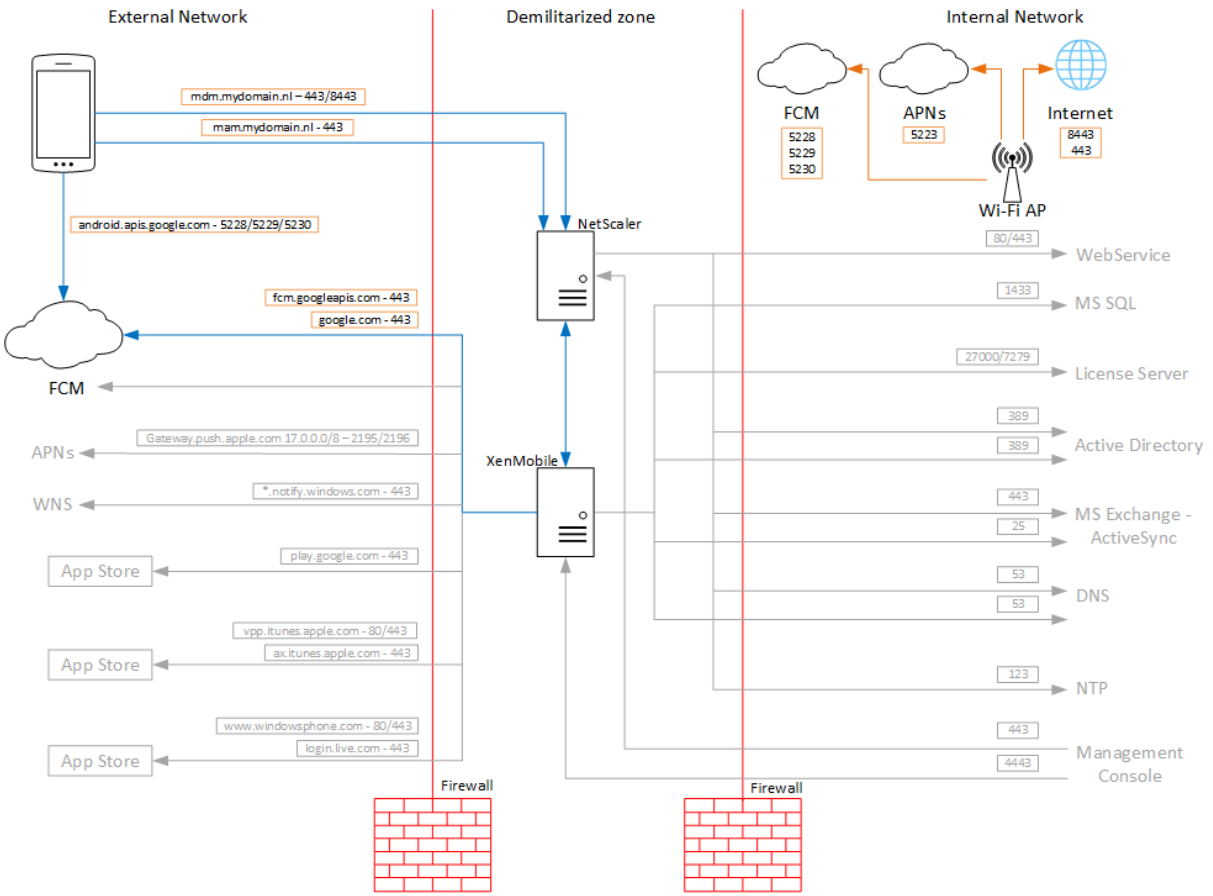
Firewallports

- Öffnen Sie Port 443 in XenMobile für `fcm.googleapis.com` und `Google.com`.
- Öffnen Sie ausgehende Internetkommunikation für Geräte-Wi-Fi auf den Ports 5228, 5229 und 5230.
- Um ausgehende Verbindungen zuzulassen, empfiehlt FCM, die Ports 5228 bis 5230 ohne IP-Einschränkungen auf die Positivliste zu setzen. Falls Sie IP-Beschränkungen benötigen, empfiehlt FCM, alle IP-Adressen in den IPv4- und IPv6-Blöcken auf die Positivliste zu setzen. Diese Blöcke sind in der Google ASN 15169 aufgelistet. Aktualisieren Sie diese Liste monatlich.

Weitere Informationen finden Sie unter Portanforderungen.

Architektur

In diesem Diagramm ist der Kommunikationsfluss für FCM im externen und internen Netzwerk dargestellt.

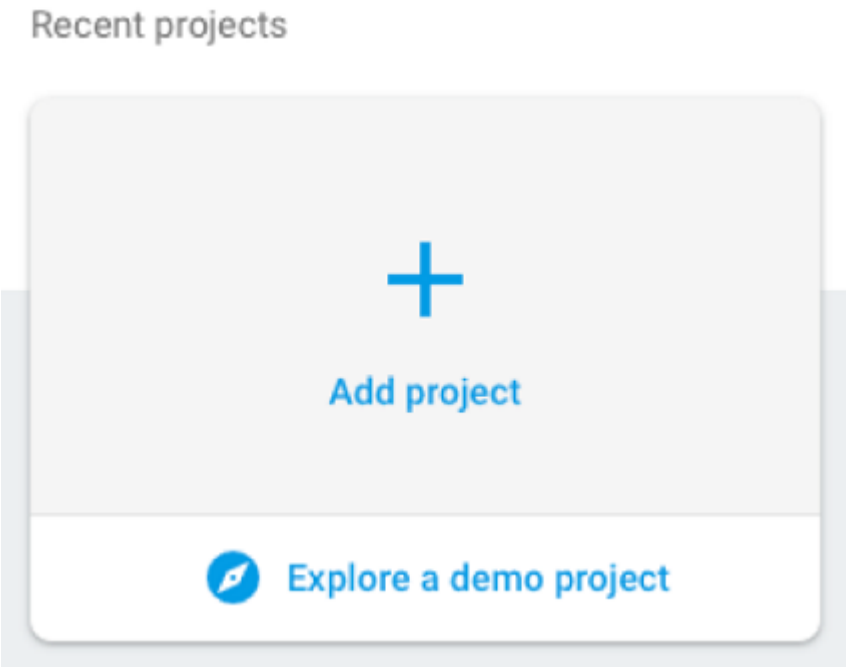


Konfigurieren Ihres Google-Kontos für FCM

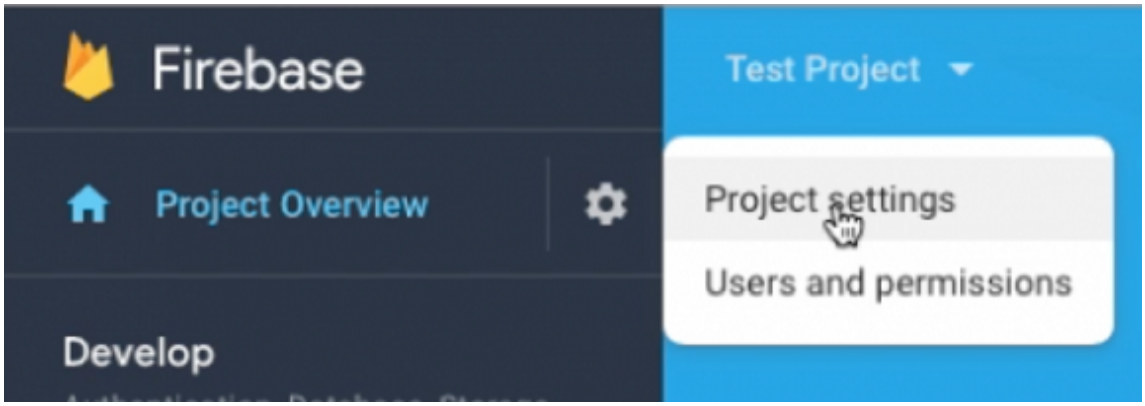
1. Melden Sie sich bei der folgenden URL mit den Anmeldeinformationen für Ihr Google Developer-Konto an:

   https://console.firebase.google.com/

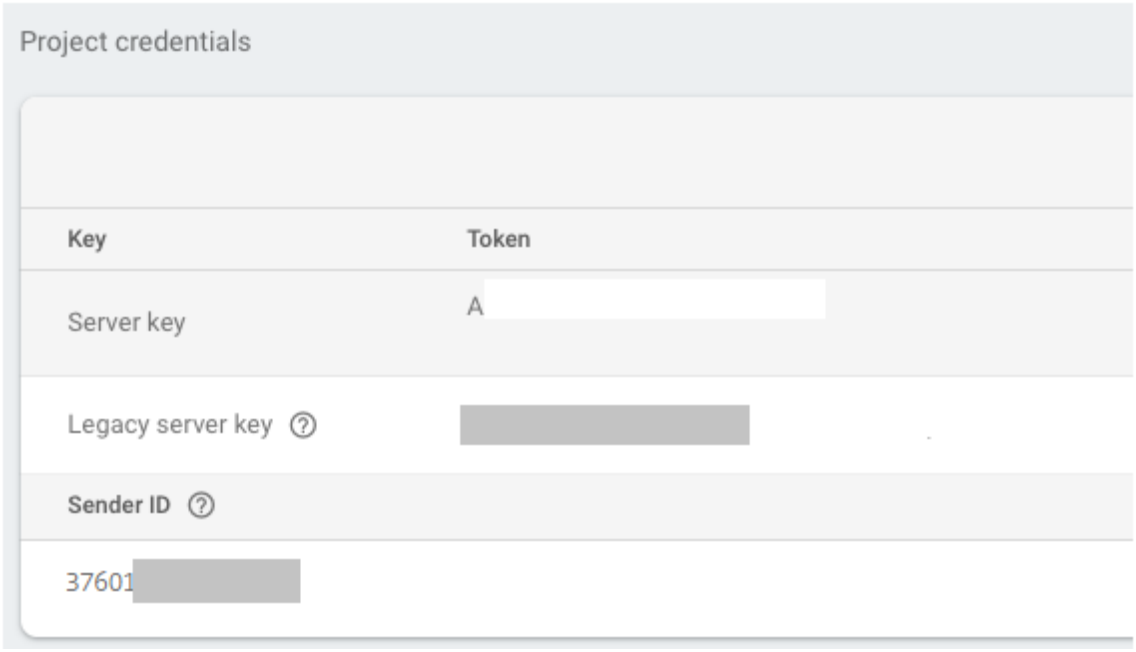
2. Klicken Sie auf **Add project**.



3. Klicken Sie nach dem Erstellen des Projekts auf **Project settings**.



4. Klicken Sie auf die Registerkarte **Cloud Messaging** . Kopieren Sie die Werte für den **Serverschlüssel** und die **Absender-ID**. Im nächsten Schritt fügen Sie diese Werte in der XenMobile-Konsole ein. Seit Oktober 2016 müssen Serverschlüssel in der Firebase-Konsole erstellt werden.

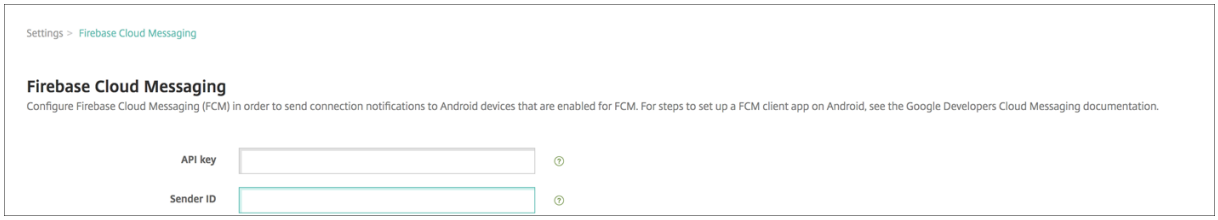


Schritte zum Einrichten einer FCM-Client-App unter Android finden Sie in diesem Cloud Messaging-Artikel für Google Developer: https://firebase.google.com/docs/cloud-messaging/android/client.

Konfigurieren von XenMobile für FCM

Gehen Sie in der XenMobile-Konsole zu **Einstellungen > Firebase Cloud Messaging**.

- Bearbeiten Sie den **API-Schlüssel** und geben Sie den Firebase Cloud Messaging-**Serverschlüssel** ein, den Sie im letzten Schritt der Konfiguration von Firebase Cloud Messaging kopiert haben.
- Bearbeiten Sie die **Absender-ID** und geben Sie den Wert der **Absender-ID** ein, die Sie im vorherigen Vorgang kopiert haben.

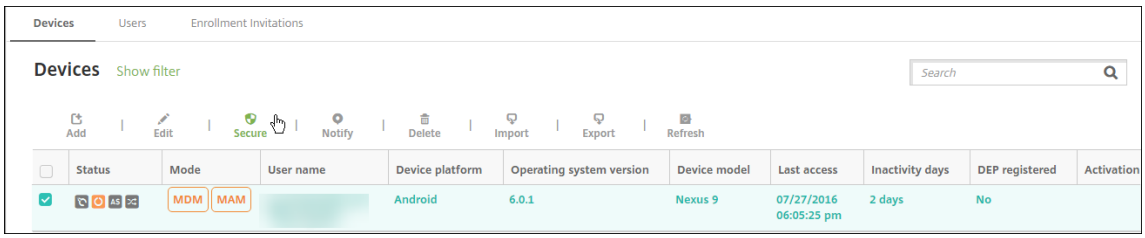


Nachdem Sie das Setup abgeschlossen haben, können Sie Ihre Zeitplanrichtlinie für Geräte entfernen oder die Richtlinie ändern, sodass sie seltener eine Verbindung herstellt.

Testen der Konfiguration

1. Registrieren Sie ein Android-Gerät.
2. Lassen Sie das Gerät eine Zeit lang inaktiv, sodass die Verbindung mit XenMobile 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.

Integration von Apple Bildung-Features

January 5, 2022

Sie können XenMobile für die Mobilgeräteverwaltung (MDM) in einer Umgebung mit Apple Bildung verwenden. XenMobile unterstützt Apple School Manager (ASM) und die Classroom-App für iPad. Mit der XenMobile-Richtlinie “Bildung - Konfiguration” können die Geräte von Lehrkräften und Lernenden zur Verwendung der Apple-Produkte für Bildungskunden konfiguriert werden.

Sie stellen Lehrkräften und Lernenden vorkonfigurierte und betreute iPads bereit. Die Konfiguration umfasst die ASM-Registrierung bei XenMobile, eine verwaltete Apple-ID mit einem neuen Kennwort und erforderliche Volume Purchase-Apps sowie iBooks.

Hauptelemente der XenMobile-Unterstützung für Apple Bildung-Features

Apple School Manager

ASM ist ein Service, mit dem Sie iOS/iPadOS-Geräte und macOS-Laptops für Bildungseinrichtungen einrichten, bereitstellen und verwalten können. Über das webbasierte Portal von ASM können IT-Administratoren folgende Aufgaben erledigen:

- Apple-Bereitstellungsprogrammgeräte diversen MDM-Servern zuweisen
- Volume Purchase-Lizenzen für Apps und iBooks erwerben
- **Verwaltete Apple-IDs** en gros erstellen: Diese Apple-IDs ermöglichen den Zugriff auf Apple-Dienste, wie z. B. das Speichern von Dokumenten in iCloud Drive und die Anmeldung zu Apple App Store-Kursen.

Sie können mehrere ASM-Konten zu XenMobile hinzufügen. Dieses Feature ermöglicht beispielsweise die Verwendung verschiedener Registrierungseinstellungen und Optionen im Setupassistenten je nach Abteilung oder Fakultät einer Bildungseinrichtung. Anschließend verknüpfen Sie die ASM-Konten mit verschiedenen Geräterichtlinien.

Nachdem Sie ein ASM-Konto zur XenMobile-Konsole hinzugefügt haben, ruft XenMobile die Unterrichts- und Dienstplaninformationen ab. Bei der Geräteeinrichtung werden in XenMobile folgende Schritte ausgeführt:

- Geräteregistrierung
- Installation der von Ihnen für die Bereitstellung konfigurierten Ressourcen, z. B. Geräterichtlinien (Bildungseinrichtung - Konfiguration, Homebildschirmlayout usw.).
- Außerdem werden die über das Volume Purchase erworbenen Apps und iBooks installiert.

Sie stellen Lehrkräften und Lernenden vorkonfigurierte Geräte bereit. Wenn ein Gerät verloren geht oder gestohlen wird, können Sie das MDM-Feature “Modus ‘Verloren”’ verwenden, um es zu sperren und zu orten.

Classroom-App für iPad

Die Classroom-App für iPad ermöglicht Lehrkräften die Verbindung mit und Verwaltung von Geräten der Lernenden. Mit ihr können sie Gerätebildschirme anzeigen, Apps auf iPads öffnen und Weblinks teilen und öffnen.

Classroom steht im App-Store kostenlos zur Verfügung. Sie laden die App in die XenMobile-Konsole hoch. Anschließend konfigurieren Sie die App mit der Geräterichtlinie “Bildungseinrichtung - Konfiguration” die Sie auf den Geräten der Lehrkräfte bereitstellen.

Weitere Informationen zu den Apple-Features für Bildungseinrichtungen finden Sie auf der Apple-Website zum Bereich Bildung und in der Apple-Implementierungsreferenz für den Bildungsbereich.

Voraussetzungen

- Citrix Gateway
- Für MDM+MAM konfiguriertes Registrierungsprofil
- Apple iPad 3. Generation (Mindestversion) oder iPad Mini mit iOS 9.3 (Mindestversion)

> **Hinweis:**
>
> XenMobile validiert ASM-Benutzerkonten nicht anhand von LDAP oder Active Directory. Sie können XenMobile jedoch mit LDAP oder Active Directory verbinden, um Benutzer und Geräte zu verwalten, die nicht mit Lehrkräften oder Lernenden von ASM in Verbindung stehen. Beispielsweise können Sie über Active Directory anderen ASM-Mitgliedern (z. B. IT-Administratoren) Secure Mail und Secure Web zur Verfügung zu stellen.
>
> Da ASM-Lehrkräfte und -Lernende lokale Benutzer sind, müssen Sie auf ihren Geräten Citrix Secure Hub nicht bereitstellen.
>
> Die MAM-Registrierung mit Citrix Gateway-Authentifizierung unterstützt keine lokalen Benutzer (nur Active Directory-Benutzer). Aus diesem Grund stellt XenMobile nur erforderliche Volume Purchase-Apps und -iBooks auf den Geräten von Lehrkräften und Lernenden bereit.

Voraussetzungen für geteilte iPads

- Beliebiges iPad Pro, iPad 5. Generation, iPad Air 2 oder später und iPad mini 4 oder später
- Mindestens 32 GB Speicherplatz
- Betreut

Konfigurieren von Apple School Manager und XenMobile

Folgen Sie nach dem Kauf von iPads bei Apple oder einem autorisierten Apple-Händler/-Netzbetreiber dem Workflow in diesem Abschnitt, um Ihr ASM-Konto und die Geräte einzurichten. Der Workflow enthält Schritte, die Sie im ASM-Portal und in der XenMobile-Konsole ausführen müssen.

Konfigurieren Sie gemäß diesen Anweisungen Ihre Integration für iPads, die jeweils von nur einem Schüler genutzt werden und für iPads der Lehrkräfte. Informationen zum Konfigurieren von geteilten iPads finden Sie unter Konfigurieren von geteilten iPads.

Schritt 1: Erstellen eines Apple School Manager-Kontos und Ausführen des Setups mit dem Assistenten

Wenn Sie ein Upgrade vom Apple-Bereitstellungsprogramm planen, lesen Sie den Apple-Supportartikel Upgrade your institution to ASM. Zum Erstellen Ihres ASM-Kontos folgen Sie den

Anweisungen unter https://school.apple.com/. Wenn Sie sich das erste Mal bei ASM anmelden, wird der Setupassistent geöffnet.

- Informationen zu den ASM-Voraussetzungen, zum Setupassistenten und zu Verwaltungsaufgaben finden Sie im Apple School Manager-Benutzerhandbuch.
- Verwenden Sie beim Einrichten von ASM einen Domänennamen, der sich vom Domänennamen für Active Directory unterscheidet. Fügen Sie dem Domänennamen für ASM beispielsweise das Präfix `appleid` an.
- Wenn Sie ASM mit Ihrem Dienstplan verbinden, erstellt ASM verwaltete Apple-IDs für Lehrkräfte und Lernende. Die Dienstplandaten umfassen Lehrkräfte, Lernende und Unterrichtsstunden. Weitere Informationen zum Hinzufügen von Dienstplandaten zu ASM finden Sie im in der oben erwähnten ASM-Benutzerdokumentation.
- Sie können das Format der verwalteten Apple-ID für Ihre Institution anpassen (siehe ASM-Benutzerdokumentation).

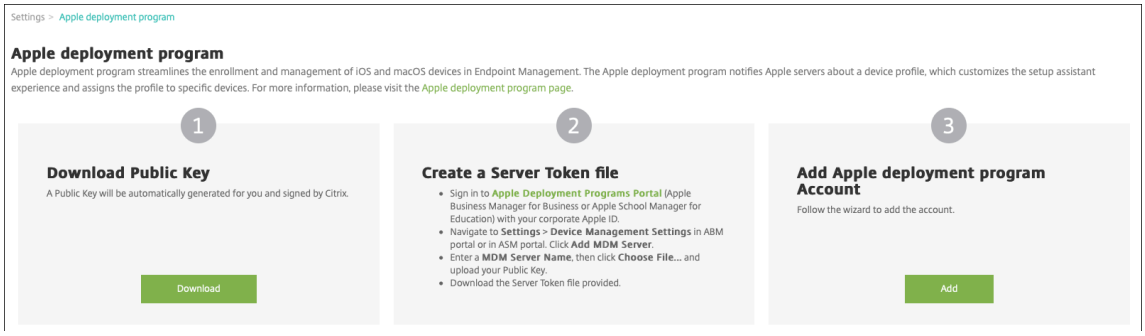
  > **Wichtig:**
  >
  > Ändern Sie keine verwalteten Apple-IDs, nachdem Sie ASM-Informationen in XenMobile importiert haben.

- Wenn Sie Geräte über Wiederverkäufer oder Netzbetreiber erworben haben, verknüpfen Sie die Geräte mit ASM. Weitere Informationen finden Sie in der ASM-Benutzerdokumentation.

Schritt 2: Konfigurieren von XenMobile als MDM-Server für Apple School Manager und Konfigurieren der Gerätezuordnungen

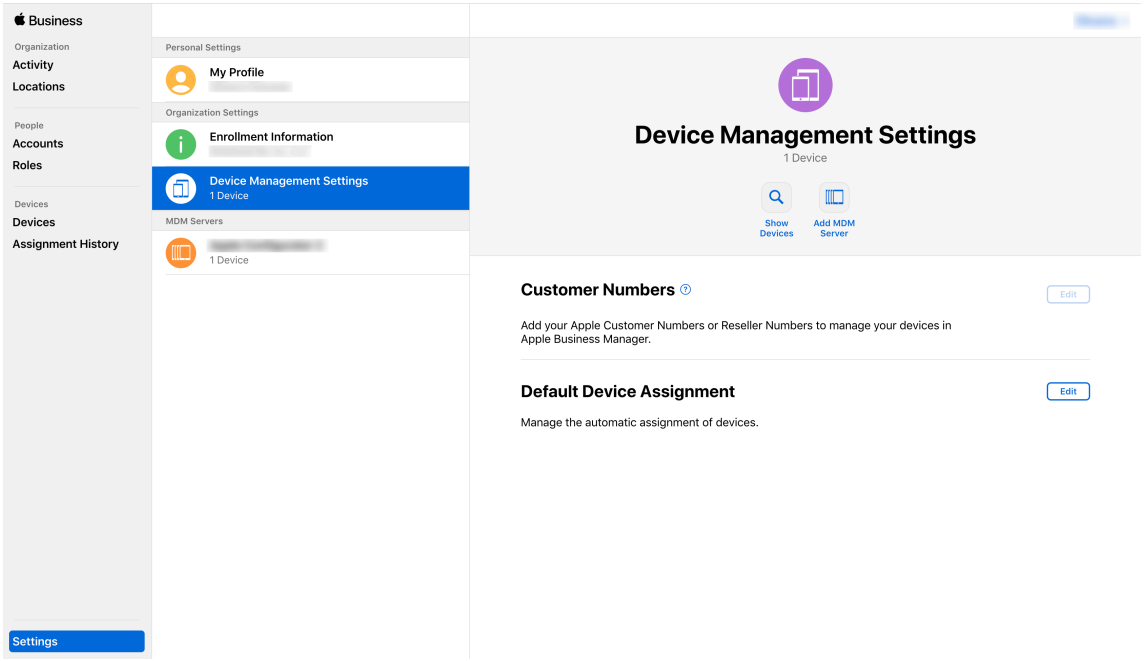
Das ASM-Portal enthält eine Registerkarte **MDM Server**. Sie benötigen für dieses Setup die Datei mit dem öffentlichen Schlüssel von XenMobile.

1. Laden Sie den öffentlichen Schlüssel für XenMobile auf Ihren lokalen Computer herunter: Gehen Sie in der XenMobile-Konsole zu **Einstellungen > Apple-Bereitstellungsprogramm**.

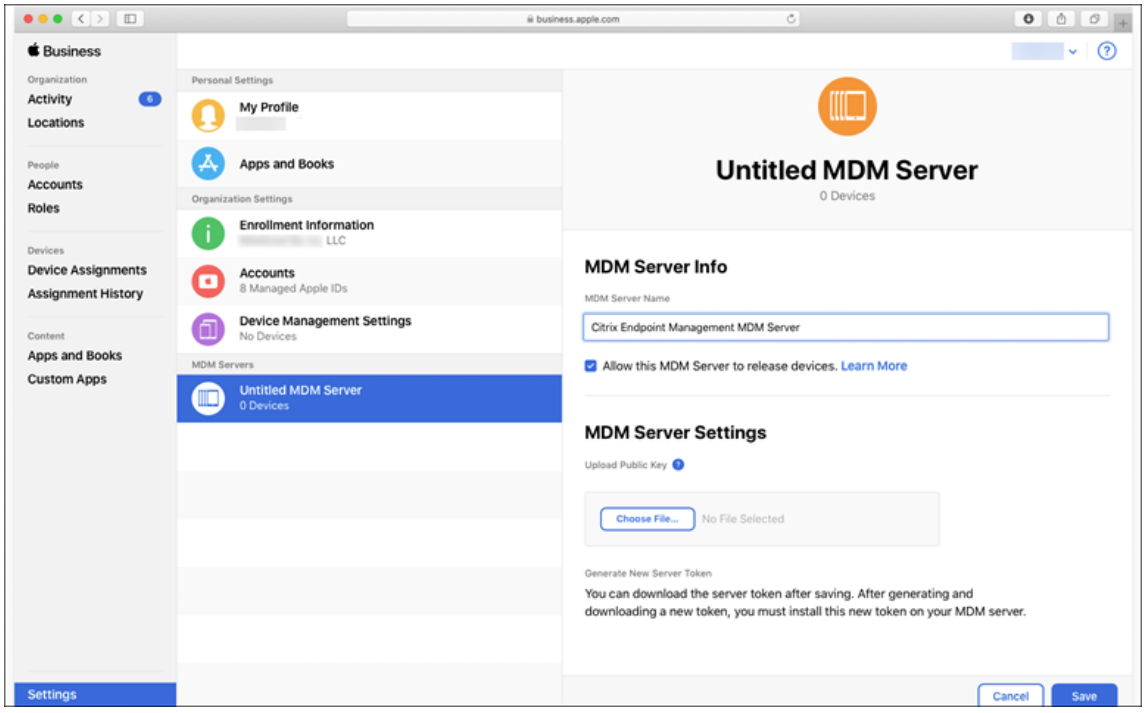


2. Klicken Sie unter **Öffentlichen Schlüssel herunterladen** auf **Herunterladen** und speichern Sie die PEM-Datei.

3. Klicken Sie im Portal **Apple School Manager** auf **Settings** und dann auf **Device Management Settings**. Klicken Sie auf **Add MDM Server**.

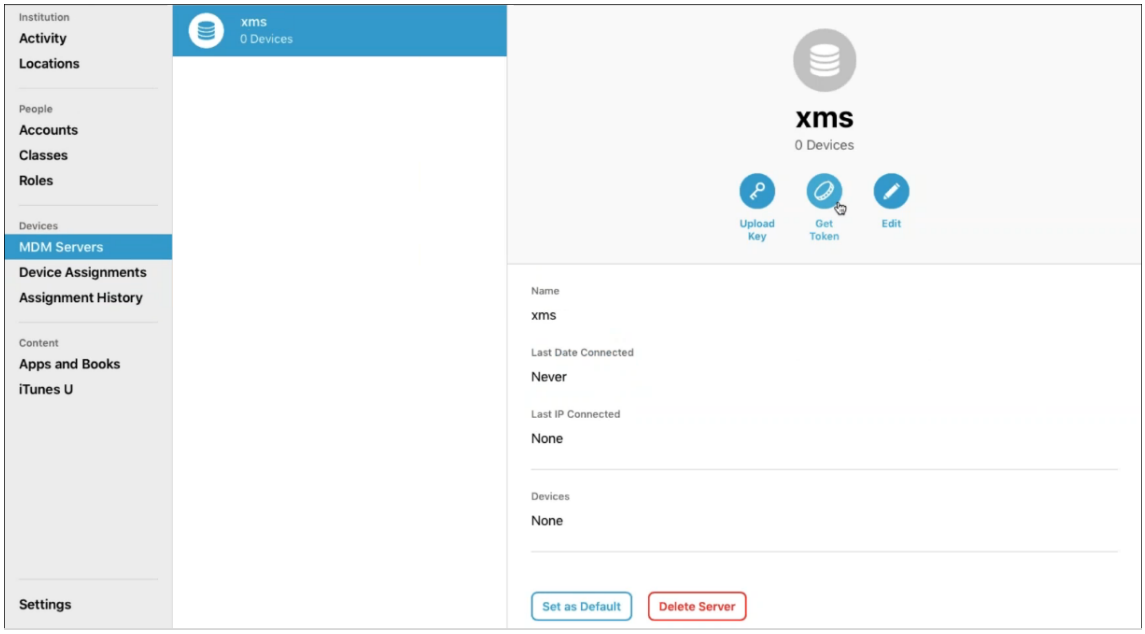


4. Geben Sie einen Namen für XenMobile ein. Der von Ihnen eingegebene Servername dient als Referenz und ist nicht die URL oder der Name des Servers. Klicken Sie unter **Upload Public Key** auf **Choose File**.



5. Laden Sie den von XenMobile heruntergeladenen öffentlichen Schlüssel hoch und klicken Sie auf **Save**.

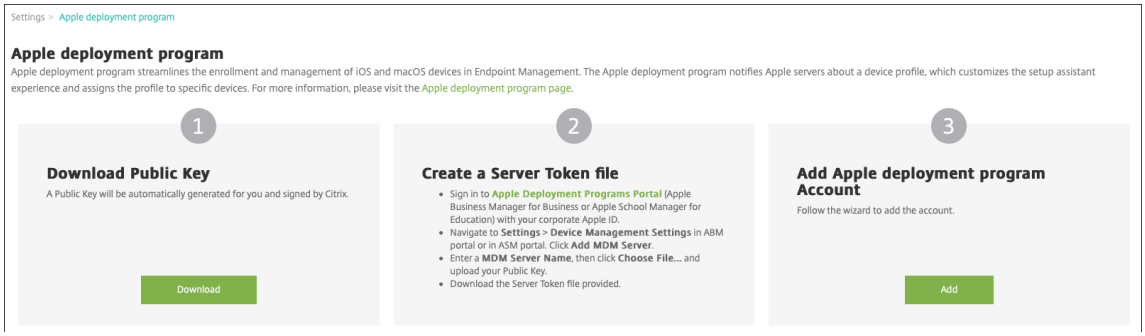
6. Generieren Sie einen Servertoken: Klicken Sie auf **Download Token**, um die Servertokendatei auf Ihrem Computer herunterzuladen.



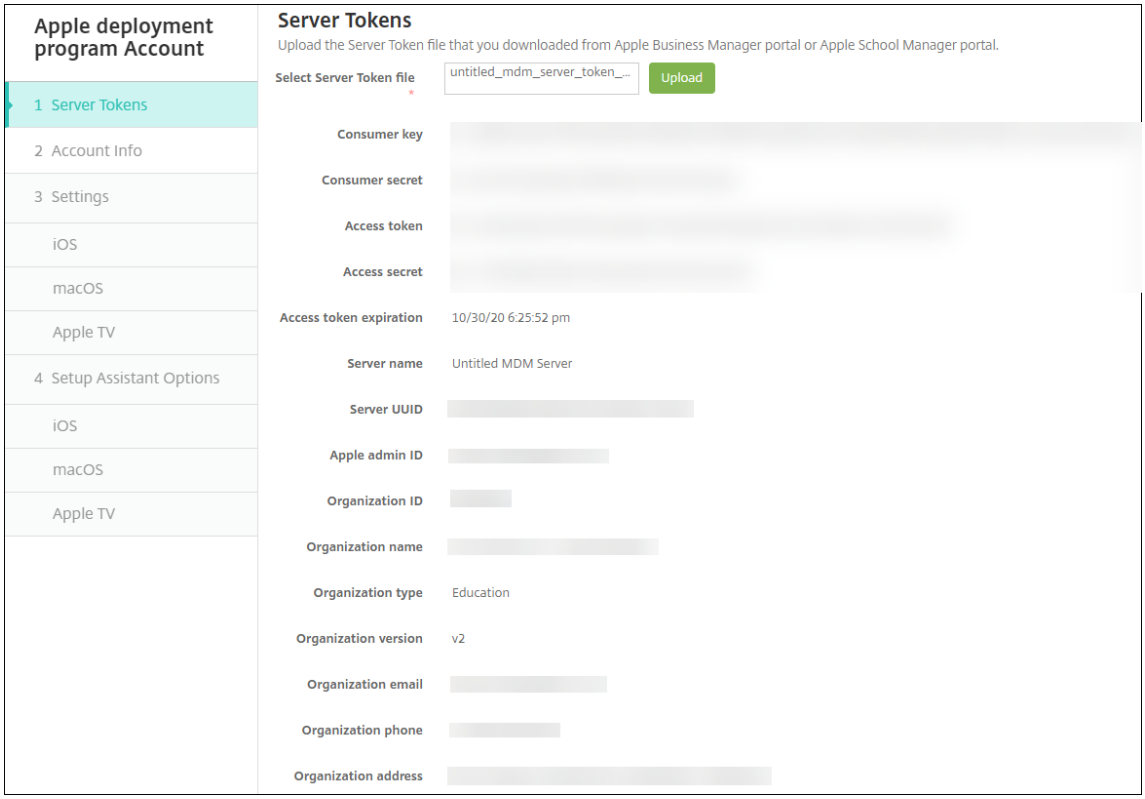
7. Klicken Sie unter **Default Device Assignment** auf **Change**. Wählen Sie aus, wie Sie Geräte zuweisen möchten, und geben Sie die angeforderten Informationen ein. Weitere Informationen finden Sie in der ASM-Benutzerdokumentation.

Schritt 3: Hinzufügen des Apple School Manager-Kontos zu XenMobile

1. Rufen Sie in der XenMobile-Konsole **Einstellungen > Apple Deployment Program** auf und klicken Sie unter **Apple Deployment Program-Konto hinzufügen** auf **Hinzufügen**.



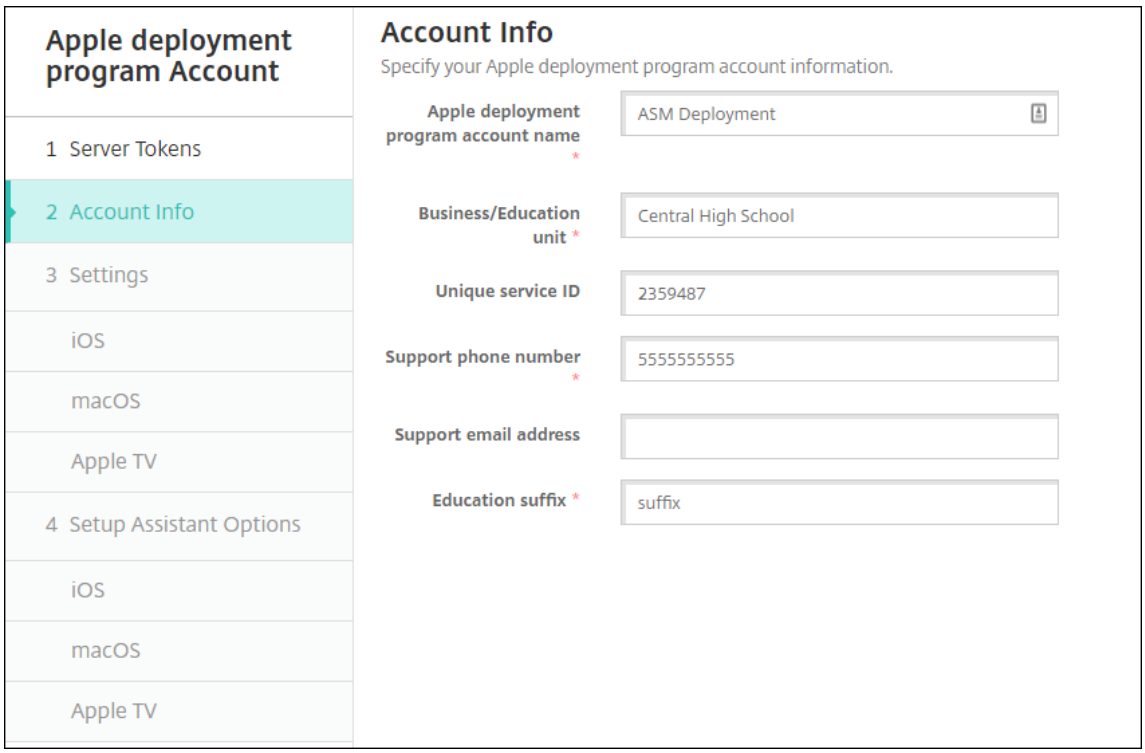
2. Klicken Sie auf der Seite **Servertoken** auf **Hochladen** und wählen Sie den Servertoken (eine P7M-Datei), den Sie vom ASM-Portal heruntergeladen haben. Die Tokeninformationen werden angezeigt.



Hinweise:

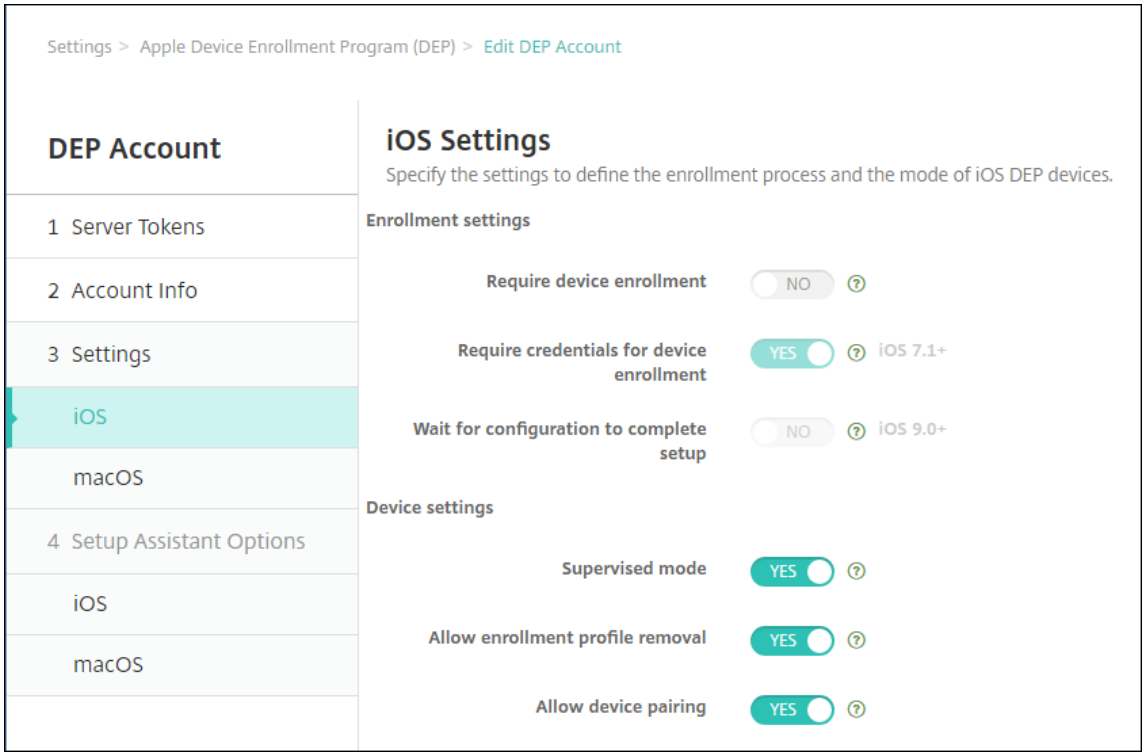
- **Organisations-ID** ist Ihre Kunden-ID für das Apple-Bereitstellungsprogramm.
- ASM-Konten verwenden als **Organisationstyp** die Einstellung **Bildung** und als **Organisationsversion** die Einstellung **v2**.

3. Geben Sie auf der Seite **Kontoinformationen** folgende Einstellungen an:



- **Apple-Bereitstellungsprogramm-Kontoname:** Ein eindeutiger Name für dieses Apple-Bereitstellungsprogramm-Konto. Verwenden Sie Namen, die die Organisation der Apple-Bereitstellungsprogramm-Konten widerspiegelt, beispielsweise nach Land oder Organisationshierarchie.
- **Geschäftseinheit:** die Bildungseinrichtung bzw. Abteilung für die Gerätezuweisung. Diese Angabe ist erforderlich.
- **Eindeutige Dienst-ID:** Eine optionale eindeutige ID zur weiteren Identifizierung des Kontos.
- **Telefonnummer vom Support:** Eine Telefonnummer, unter der Benutzer beim Setup Hilfe anfordern können. Diese Angabe ist erforderlich.
- **E-Mail-Adresse vom Support:** Eine optionale E-Mail-Adresse des Supports, die Benutzern zur Verfügung steht.
- **Suffix der Bildungseinrichtung:** Kennzeichnen die Klassen für ein bestimmtes ASM Deployment Program-Konto. (Das Volume Purchase-Suffix kennzeichnet Apps und iBooks für ein bestimmtes Volume Purchase-Konto.) Es wird empfohlen, für beide Konten, das ASM Deployment Program und den ASM Volume Purchase, das gleiche Suffix zu verwenden.

4. Klicken Sie auf **Weiter**. Geben Sie unter **iOS-Einstellungen** die folgenden Einstellungen an:



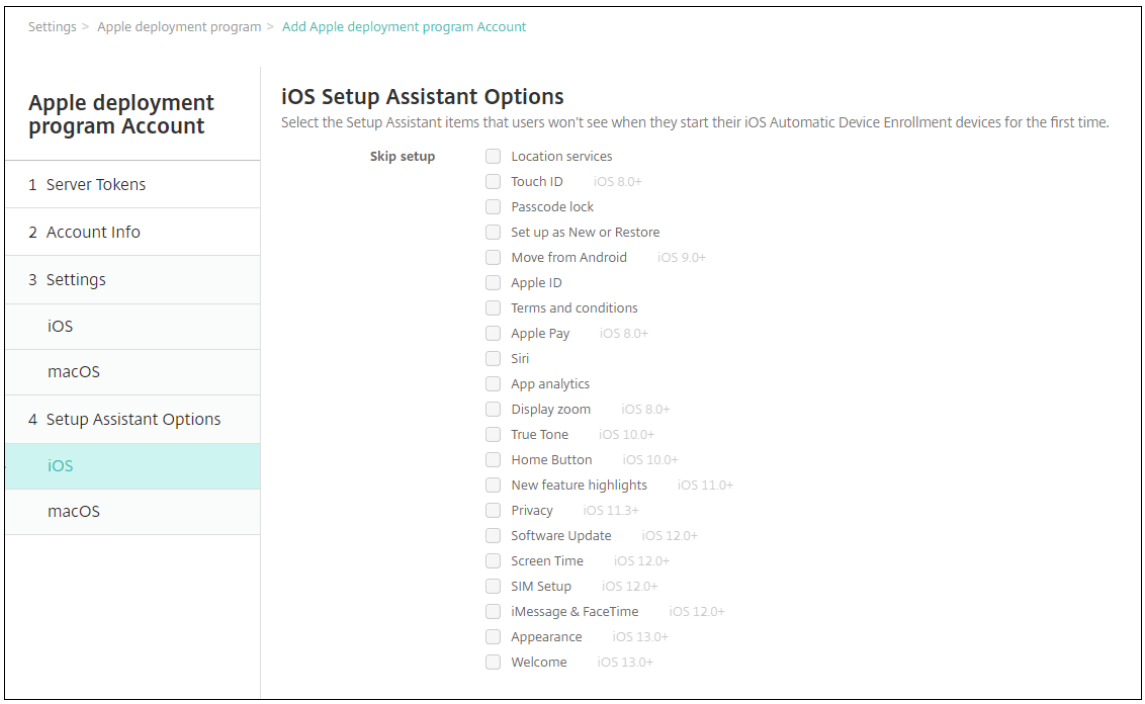
- **Registrierungseinstellungen**
  - **Geräteregistrierung erforderlich:** gibt an, ob Benutzer Geräte registrieren müssen. Ändern Sie die Einstellung in **Nein**.
  - **Anmeldeinformationen für Geräteregistrierung erforderlich:** gibt an, ob Benutzer bei der Apple-Bereitstellungsprogrammregistrierung ihre Anmeldeinformationen eingeben müssen. Für die Integration von ASM in XenMobile ist diese Einstellung standardmäßig auf **Ja** festgelegt und kann nicht geändert werden. Das Apple-Bereitstellungsprogramm erfordert Anmeldeinformationen für Geräteregistrierung.
  - **Abschluss der Konfiguration abwarten:** Wählen Sie aus, ob Geräte im Setupassistentenmodus verbleiben müssen, bis alle erforderlichen MDM-Ressourcen auf den Geräten bereitgestellt wurden. Für die ASM-Integration in XenMobile ist diese Einstellung standardmäßig auf **Nein** festgelegt. Laut Apple-Dokumentation funktionieren die folgenden Befehle möglicherweise nicht, wenn ein Gerät im Setupassistentenmodus ausgeführt wird:
    - InviteToProgram
    - InstallApplication
    - InstallMedia
    - ApplyRedemptionCode
- **Geräteeinstellungen**
  - **Betreuungsmodus:** versetzt iOS-Geräte in den betreuten Modus. Übernehmen Sie

die Standardeinstellung **Ja**. Informationen, wie Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus.

- **Freigabemodus:** Freigabemodus auf iPads aktivieren. Geräte, die die Mindestanforderungen nicht erfüllen, können nicht gemeinsam genutzt werden.
- **Entfernen des Registrierungsprofils zulassen:** Für die ASM-Integration lassen Sie zu, dass Benutzer das Registrierungsprofil vom Gerät entfernen. Ändern Sie die Einstellung in **Ja**.
- **Koppeln von Geräten zulassen:** Für die ASM-Integration müssen Sie die Gerätekopplung zulassen, damit eine Konfiguration über Apple App Store und Apple Configurator möglich ist. Ändern Sie die Einstellung in **Ja**.

5. Wählen Sie unter **Optionen des iOS-Setupassistenten** die Schritte aus, die beim ersten Gerätestart durch die Benutzer übersprungen werden. Standardmäßig umfasst der Setupassistent alle Schritte. Das Entfernen von Schritten aus dem Setupassistenten verbessert die Benutzererfahrung.

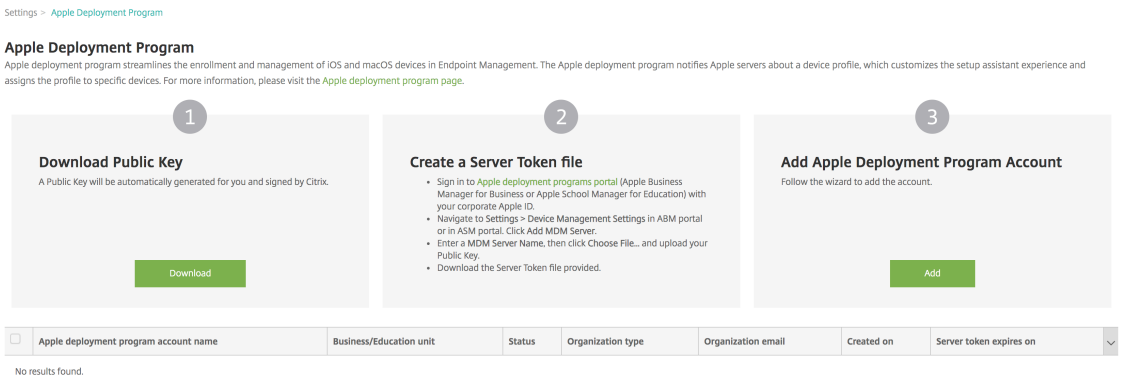
> **Wichtig:**
>
> Citrix empfiehlt dringend, dass Sie die Schritte **Apple-ID** und **AGB** beibehalten. Diese Schritte ermöglichen Lehrkräften und Lernenden die Eingabe ihrer neuen Kennwörter für die verwaltete Apple-ID und die Zustimmung zu den Nutzungsbedingungen.



- **Ortungsdienste:** Einrichten der Ortungsdienste auf dem Gerät

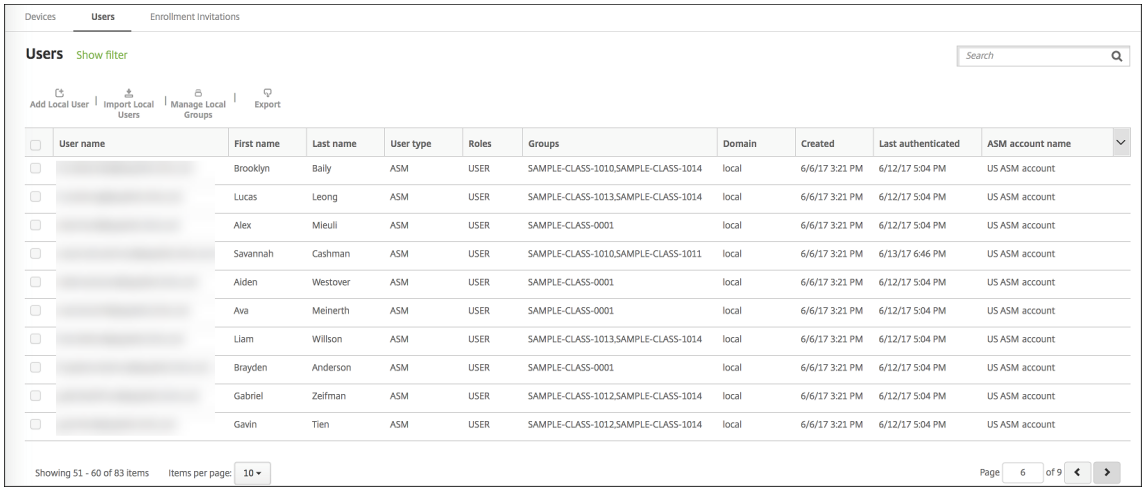
- **Touch ID:** Einrichten von Touch ID auf iOS-Geräten.
- **Passcodesperre:** Erstellen einer Passcodesperre für das Gerät.
- **Neu einrichten oder wiederherstellen:** Einrichten des Geräts als neu oder als Backup von einer iCloud oder aus dem Apple App Store.
- **Verschieben von Android:** Aktivieren der Datenübertragung von einem Android-Gerät auf ein iOS-Gerät . Diese Option ist nur verfügbar, wenn **Neu einrichten oder wiederherstellen** aktiviert wurde (d. h. der Schritt wird übersprungen).
- **Apple-ID:** Einrichten einer Apple-ID für das Gerät. Citrix empfiehlt, dass Sie dieses Kontrollkästchen aktivieren, um den Schritt einzubeziehen.
- **AGB:** Akzeptieren der Nutzungsbedingungen für die Verwendung des Geräts. Citrix empfiehlt, dass Sie dieses Kontrollkästchen aktivieren, um den Schritt einzubeziehen.
- **Apple Pay:** Einrichten von Apple Pay auf iOS-Geräten
- **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 iOS-Geräten
- **True Tone:** Einrichten der True Tone-Anzeige auf iOS-Geräten
- **Hometaste:** Einrichten der Empfindlichkeit des Hometastenbildschirms auf iOS-Geräten
- **Neue Feature-Highlights:** Einrichten der Informationsbildschirme für das Onboarding “Access the Dock from Anywhere” und “Switch Between Recent Apps” auf Geräten mit iOS 11.0 (Mindestversion).
- **Datenschutz:** Verhindern, dass Benutzern beim Einrichten von Apple-Bereitstellungsprogrammgeräten der Bereich “Datensammlung und Datenschutz” angezeigt wird. Für iOS 11.3 und höher.
- **Softwareupdate:** Verhindert, dass Benutzer den Bildschirm für obligatorische Softwareupdates beim Einrichten der Apple-Bereitstellungsprogrammgeräte sehen. Für iOS 12.0 und höher.
- **Bildschirmzeit:** Verhindert, dass Benutzer den Bildschirm “Bildschirmzeit” beim Einrichten der Apple-Bereitstellungsprogrammgeräte sehen. Für iOS 12.0 und höher.
- **SIM-Setup:** Verhindert, dass Benutzern beim Einrichten der Apple-Bereitstellungsprogrammgeräte den Bildschirm zum Hinzufügen eines Mobilnetzabos sehen. Für iOS 12.0 und höher.
- **iMessage & FaceTime:** Verhindert, dass Benutzern beim Einrichten der Apple-Bereitstellungsprogrammgeräte den Bildschirm für iMessage und FaceTime sehen. Für iOS 12.0 und höher.

6. Das Konto wird unter **Einstellungen > Apple-Bereitstellungsprogramm** angezeigt. Zum Testen der Verbindung zwischen XenMobile und Ihrem ASM-Konto wählen Sie das Konto aus und klicken auf **Konnektivität testen**.



Eine Statusmeldung wird angezeigt.

Nach einigen Minuten werden die Benutzerkonten aus ASM auf der Seite **Verwalten > Benutzer** angezeigt. XenMobile erstellt lokale Benutzerkonten basierend auf der importierten verwalteten Apple ID für jeden Benutzer. Im folgenden Beispiel lautet das Domänennamenpräfix benutzerdefinierter Apple-IDs für Benutzerkonten `appleid`.

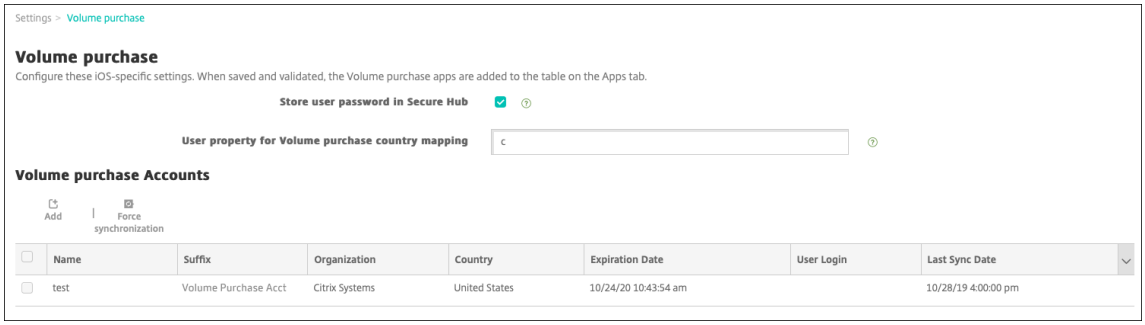


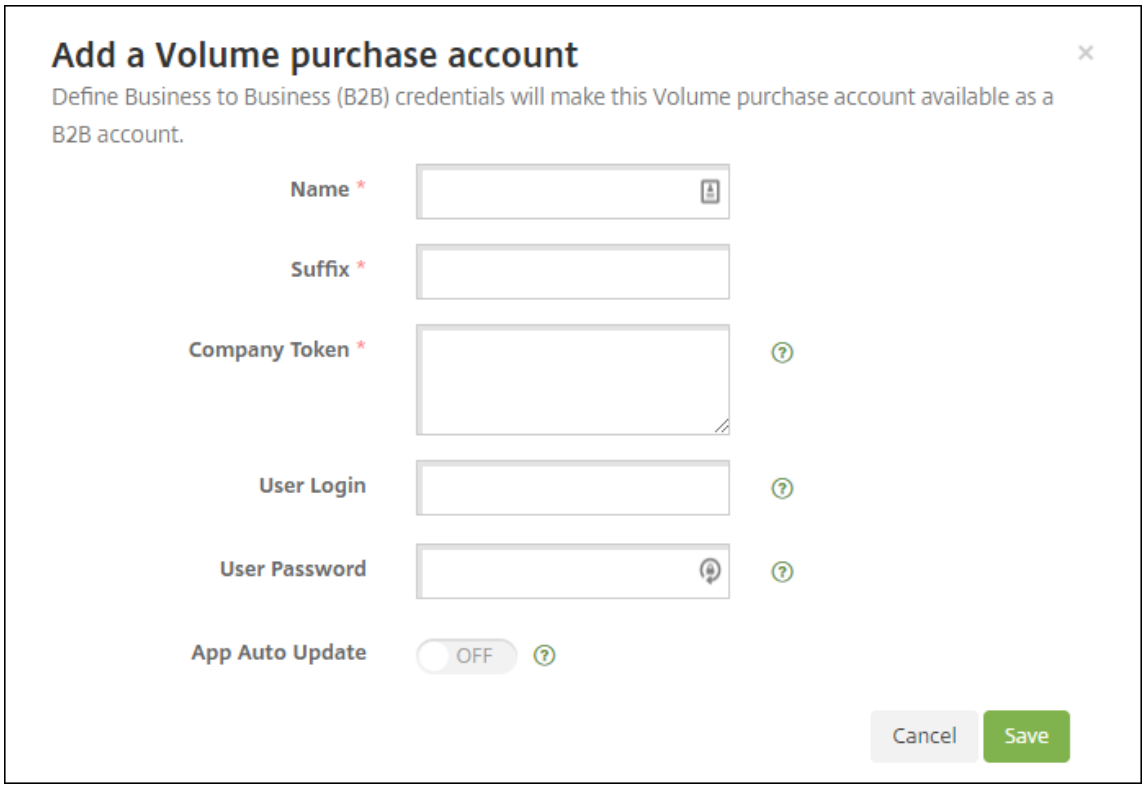
Um alle Benutzer für ein bestimmtes ASM-Konto zu finden, geben Sie den Kontonamen in den Benutzersuchfilter ein.

Schritt 4: Konfigurieren eines Education Volume Purchase-Kontos für Apple School Manager

In diesem Abschnitt verweisen Sie XenMobile auf das Volume Purchase-Konto, das Sie zum Kauf von Volume Purchase-Lizenzen für Apps und iBooks verwenden.

1. Zum Konfigurieren eines Education Volume Purchase-Kontos für ASM folgen Sie den Anweisungen unter Apple Volume Purchase. Im Bildschirm “Volume Purchase-Konto hinzufügen” müssen Sie ein Unternehmenstoken eingeben. Laden Sie den Token direkt über Ihr Education Volume Purchase-Konto herunter und fügen Sie ihn auf dem Bildschirm **Volume Purchase-Konto hinzufügen** ein.





2. Warten Sie einige Minuten auf den Import der Volume Purchase-Lizenzen in XenMobile.

Schritt 5: Hinzufügen von Kennwörtern für Apple School Manager-Benutzer

Nachdem Sie ein ASM-Konto hinzugefügt haben, importiert XenMobile Klassen und Benutzer aus ASM. XenMobile behandelt Klassen als lokale Gruppen, daher werden Sie in der Konsole als "Gruppe" angezeigt. Wenn eine Klasse in ASM einen Gruppennamen hat, weist XenMobile der Klasse den Gruppennamen zu. Andernfalls verwendet XenMobile die Quellsystem-ID als Gruppennamen. XenMobile verwendet den Kursnamen nicht als Klassennamen, da Kursnamen in ASM nicht eindeutig sind.

XenMobile erstellt auf Basis der verwalteten Apple-IDs lokale Benutzer des Typs **ASM**. Die Benutzer sind lokal, da ASM die Anmeldeinformationen unabhängig von allen externen Datenquellen erstellt. Daher verwendet XenMobile keinen Verzeichnisserver, um diese neuen Benutzer zu authentifizieren.

ASM sendet keine temporären Benutzerkennwörter an XenMobile. Sie können sie aus einer CSV-Datei importieren oder manuell hinzufügen. Gehen Sie zum Importieren temporärer Benutzerkennwörter folgendermaßen vor:

1. Beziehen Sie die CSV-Datei, die von ASM beim Erstellen temporärer Kennwörter für die verwaltete Apple-ID generiert wurde.
2. Ersetzen Sie in der CSV-Datei die temporären Kennwörter durch neue Kennwörter, die die Benutzer bei der Registrierung bei XenMobile angeben. Es gibt hier keine Einschränkungen im Hinblick auf den Kennworttyp.

   Die Einträge in der CSV-Datei haben folgendes Format: `user@appleid.citrix.com`, `Firstname`,`Middle`,`Lastname`,`Password123!`

   Wobei:

   Benutzer: `user@appleid.citrix.com`

   Vorname: `Firstname`

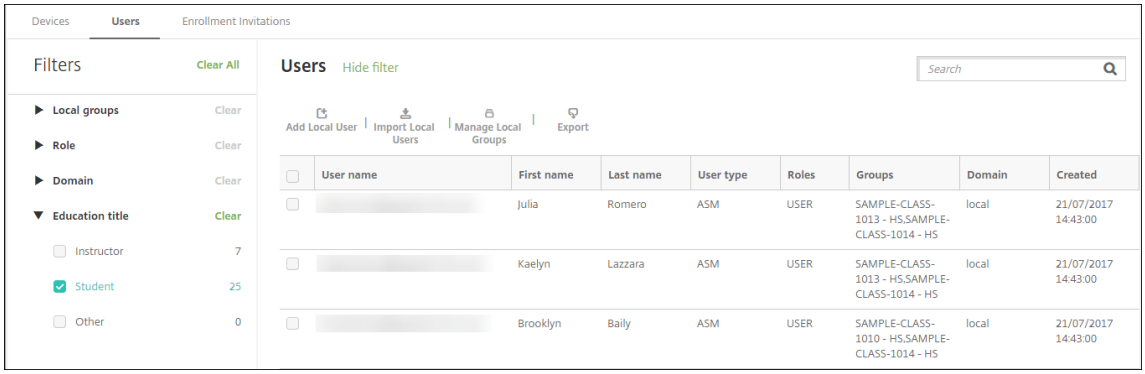
   Weiterer Vorname: `Middle`

   Nachname: `Lastname`

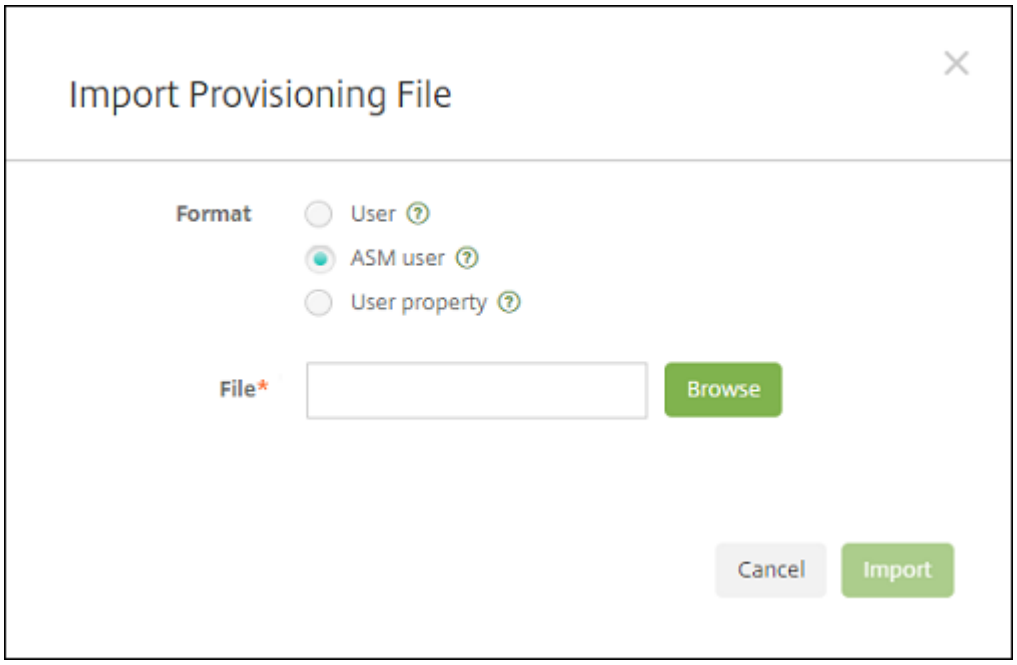
   Kennwort: `Password123!`
3. Klicken Sie in der XenMobile-Konsole auf **Verwalten > Benutzer**. Die Seite **Benutzer** wird angezeigt.

   Das Beispiel der Seite **Verwalten > Benutzer** zeigt eine Liste der Benutzer, die aus ASM importiert wurde. In der Liste **Benutzer**:

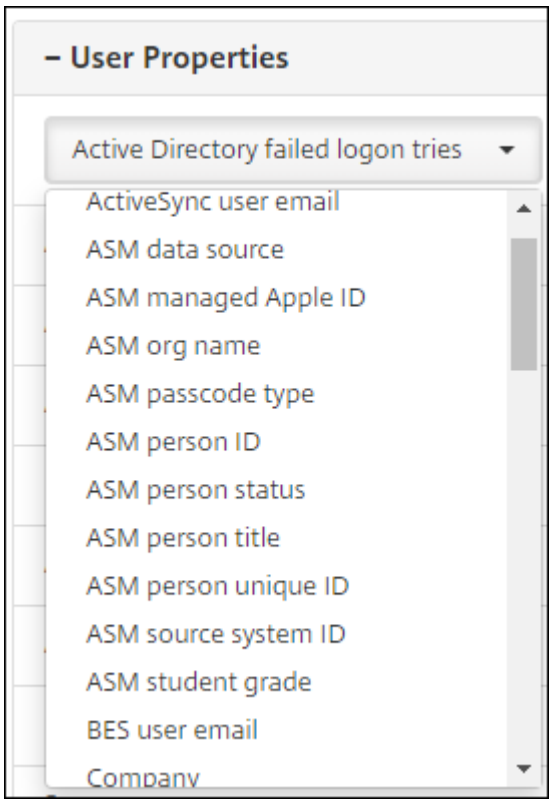
   - **Benutzername** enthält die verwaltete Apple-ID.
   - Der Benutzertyp ist **ASM**, d. h. das Konto stammt aus ASM.
   - Unter **Gruppen** werden die Klassen angezeigt.



4. Klicken Sie auf **Lokale Benutzer importieren**. Das Dialogfeld **Provisioningdatei importieren** wird angezeigt.
5. Wählen Sie für “Format” **ASM-Benutzer**, navigieren Sie zu der in Schritt 2 bearbeiteten CSV-Datei und klicken Sie auf **Importieren**.



6. Zum Anzeigen der Eigenschaften eines lokalen Benutzers wählen Sie diesen aus und klicken Sie auf **Bearbeiten**.



Zusätzlich zu den Namenseigenschaften stehen folgende ASM-Eigenschaften zur Verfügung:

- **ASM-Datenquelle:** Datenquelle der Klasse, z. B. **CSV** oder **SFTP**.
- **ASM-verwaltete Apple-ID:** Eine verwaltete Apple-ID kann den Namen Ihrer Organisation und `appleid` enthalten. Beispiel: johnappleseed@appleid.myschool.edu. XenMobile erfordert eine verwaltete Apple-ID für die Authentifizierung.
- **ASM-Organisationsname:** Name, den Sie dem Konto in XenMobile gegeben haben.
- **ASM-Passcodetyp:** Kennwortrichtlinie für die Person: **Komplex**, ein Kennwort (nicht für Lernende) aus mindestens acht Zahlen und Buchstaben, **Vier** Zahlen oder **Sechs** Zahlen.
- **ASM eindeutige Personen-ID:** Bezeichner für den Benutzer.
- **ASM-Personenstatus:** gibt an, ob die verwaltete Apple-ID **aktiv** oder **inaktiv** ist. Dieser Status wird “Aktiv”, wenn der Benutzer sein neues Kennwort für das verwaltete Apple-ID-Konto eingegeben hat.
- **ASM-Anrede:** Lehrkraft, Schüler oder Andere.
- **ASM eindeutige Personen-ID:** eindeutiger Bezeichner für den Benutzer.
- **ASM-Quellsystem-ID:** Bezeichner für die Systemquelle.
- **ASM-Klassenstufe:** Klassenstufe des Lernenden (wird von Lehrkräften nicht verwendet).

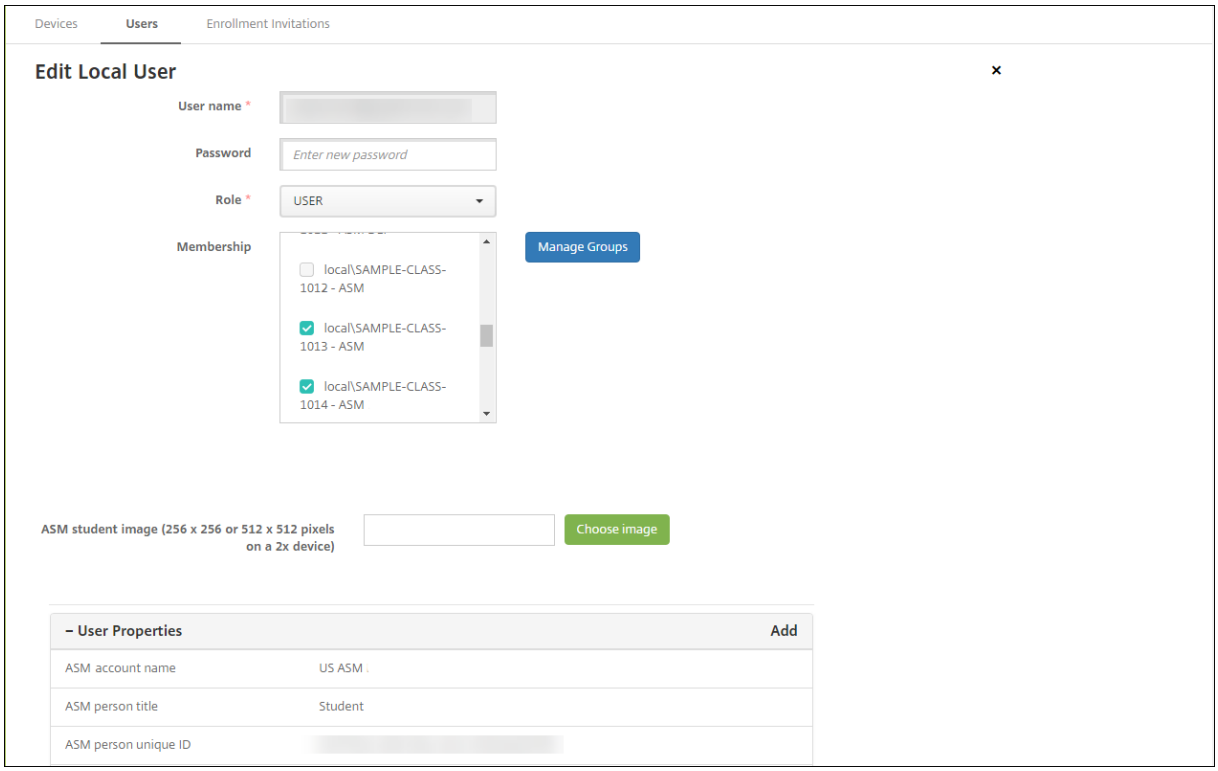
Schritt 6: Hinzufügen von Fotos der Lernenden (optional)

Sie können ein Foto jedes Lernenden hinzufügen. Wenn die Lehrkräfte die Classroom-App von Apple verwenden, erscheinen die Fotos in dieser App.

Empfehlungen für Fotos:

- Auflösung: 256 x 256 Pixel (512 x 512 Pixel auf einem 2x-Gerät)
- Format: JPEG, PNG oder TIFF

Um ein Foto hinzuzufügen, wählen Sie unter **Verwalten > Benutzer** einen Benutzer aus, klicken Sie auf **Bearbeiten** und dann auf **Bild auswählen**.



Schritt 7: Hinzufügen von Ressourcen und Bereitstellungsgruppen zu XenMobile

Eine Bereitstellungsgruppe bestimmt die Ressourcen, die Benutzerkategorien bereitgestellt werden sollen. Sie können beispielsweise eine Bereitstellungsgruppe für Lehrkräfte und Lernende erstellen. Alternativ können Sie mehrere Bereitstellungsgruppen erstellen, um Apps, Medien und Richtlinien für unterschiedliche Lehrkräfte oder Lernende anzupassen. Sie könnten eine oder mehrere Bereitstellungsgruppen pro Klasse erstellen. Sie können auch eine oder mehrere Bereitstellungsgruppen für Verwaltungs- und andere Mitarbeiter Ihrer Bildungseinrichtung erstellen.

Zu den Ressourcen, die Sie für Benutzergeräte bereitstellen, gehören Geräterichtlinien, Volume Purchase-Apps und iBooks.

- Geräterichtlinien:

  Wenn Lehrkräfte die Classroom-App verwenden, ist die Geräterichtlinie “Bildung - Konfiguration” erforderlich. Überlegen Sie anhand anderer Geräterichtlinien, wie Sie die iPads für Lehrkräfte und Lernende konfigurieren und einschränken möchten.

- Volume Purchase-Apps:

  XenMobile erfordert, dass Sie Volume Purchase-Apps für Bildungsbenutzer als erforderliche Apps bereitstellen. Die Bereitstellung solcher Volume Purchase-Apps als optional wird nicht von XenMobile unterstützt.

  Wenn Sie Apple Classroom verwenden, stellen Sie die App nur für Geräte von Lehrkräften bereit.

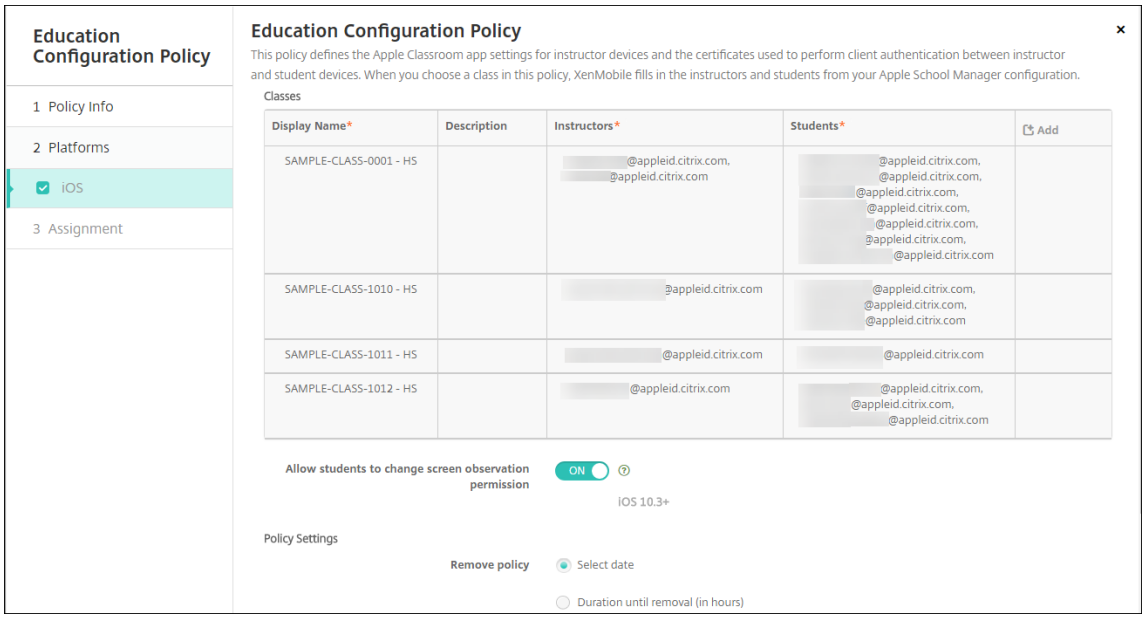
  Stellen Sie alle anderen Apps bereit, die Sie Lehrkräften oder Lernenden zur Verfügung stellen möchten. Bei dieser Lösung wird Citrix Secure Hub nicht verwendet und muss daher nicht für Lehrkräfte oder Lernende bereitgestellt werden.

- Volume Purchase-iBooks:

  Wenn XenMobile eine Verbindung mit Ihrem ASM-Konto hergestellt hat, werden Ihre gekauften iBooks in der XenMobile-Konsole unter **Konfigurieren > Medien** angezeigt. Der auf der Seite aufgelisteten iBooks können Bereitstellungsgruppen hinzugefügt werden. XenMobile unterstützt nur das Hinzufügen von iBooks als erforderliche Medien.

Wenn Sie mit der Planung von Ressourcen und Bereitstellungsgruppen für Lehrkräfte und Lernende fertig sind, können Sie sie in der XenMobile-Konsole erstellen.

1. Erstellen Sie alle Geräterichtlinien, die Sie auf Geräten für Lehrkräfte oder Lernende bereitstellen möchten. Weitere Informationen über die Geräterichtlinie zur Konfiguration für Bildung finden Sie unter Geräterichtlinie “Bildung - Konfiguration”.

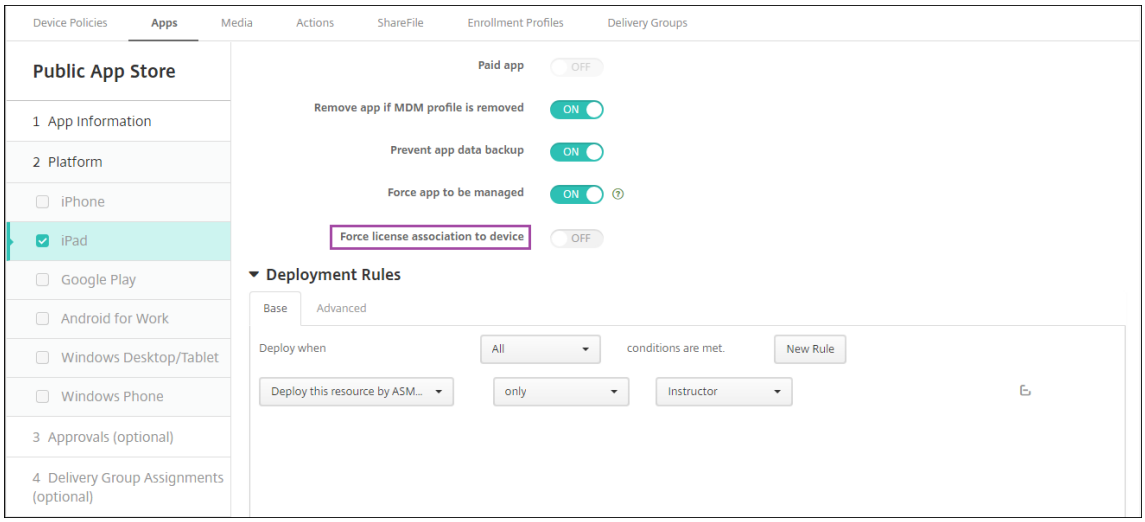


Informationen zu Geräterichtlinien finden Sie unter Geräterichtlinien und in den Artikeln zu den einzelnen Richtlinien.

2. Konfigurieren Sie Apps (**Konfigurieren > Apps**) und iBooks (**Konfigurieren > Media**).

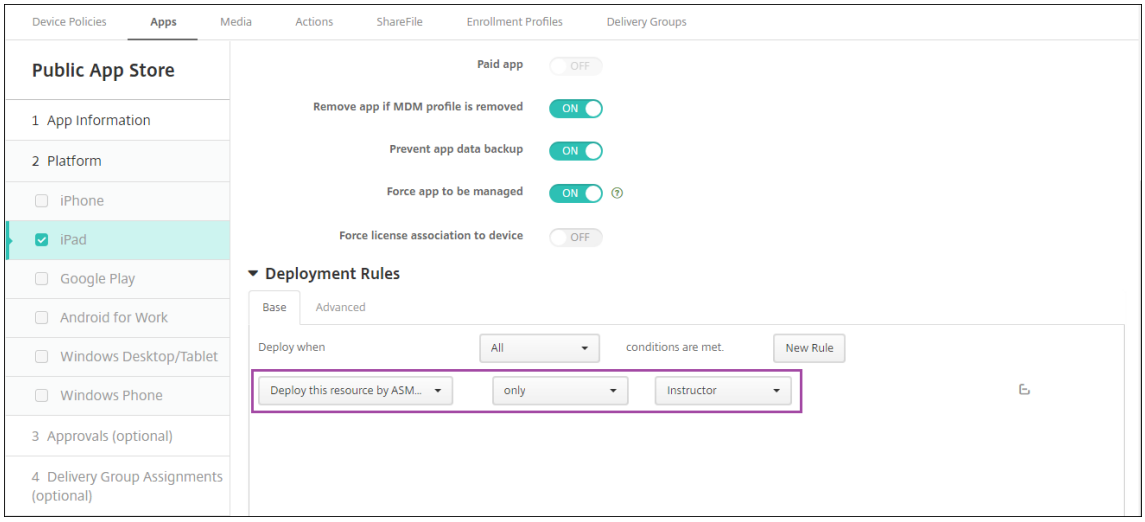
   - Standardmäßig weist XenMobile Apps und iBooks auf Benutzerebene zu. Bei der ersten Bereitstellung erhalten Lehrkräfte und Lernende eine Aufforderung zur Registrierung bei ASM. Nach Annahme der Einladung erhalten die Nutzer ihre ASM-Apps und iBooks bei der nächsten Bereitstellung (innerhalb von sechs Stunden). Citrix empfiehlt, die Bereitstellung von Apps und iBooks für neue ASM-Benutzer zu erzwingen. Wählen Sie hierfür die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.

     Sie können Apps (jedoch keine iBooks) auf Geräteebene zuweisen. Ändern Sie hierfür die Einstellung **Lizenzzuordnung zu Gerät erzwingen** in **Ein**. Wenn Sie Apps auf Geräteebene zuweisen, erhalten die Benutzer keine Einladung zur Teilnahme an Apple Volume Purchase.



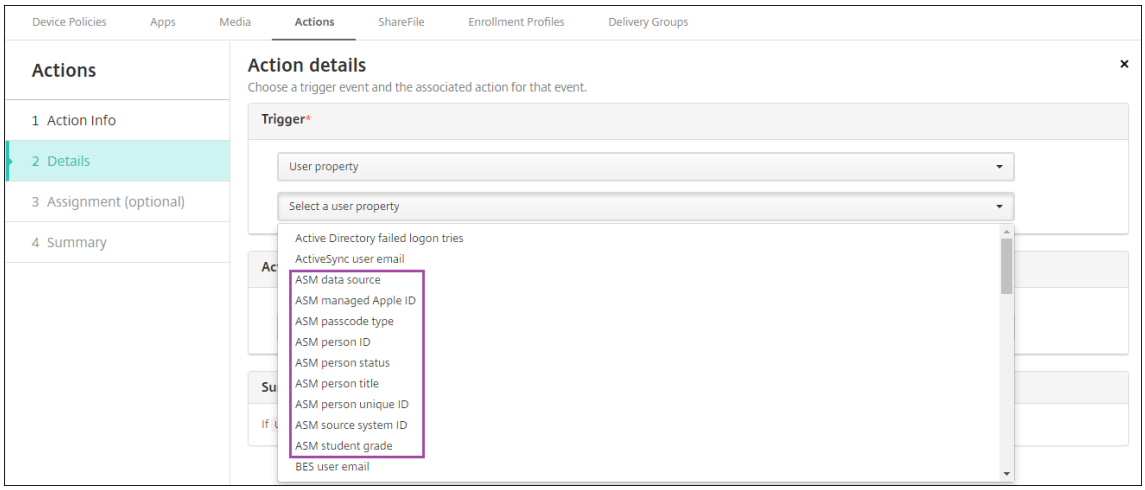
   - Um eine App nur für Lehrkräfte bereitzustellen, wählen Sie eine Bereitstellungsgruppe aus, die nur Lehrkräfte umfasst, oder verwenden Sie die folgende Bereitstellungsregel:

```
1  Deploy this resource by ASM device type
2  only
3  Instructor
4  <!--NeedCopy-->
```

- Informationen zum Hinzufügen von Volume Purchase-Apps finden Sie unter Hinzufügen von Apps aus einem öffentlichen App-Store.

3. Optional. Erstellen Sie Aktionen basierend auf den ASM-Benutzereigenschaften. Beispielsweise können Sie eine Aktion zum Senden einer Benachrichtigung an die Geräte von Lernenden erstellen, wenn eine neue App installiert wird. Sie können u. a. auch eine Aktion erstellen, die von einer Benutzereigenschaft ausgelöst wird (siehe folgendes Beispiel).



Zum Erstellen einer Aktion gehen Sie zu **Konfigurieren > Aktionen**. Informationen zum Konfigurieren von Aktionen finden Sie unter Automatisierte Aktionen.

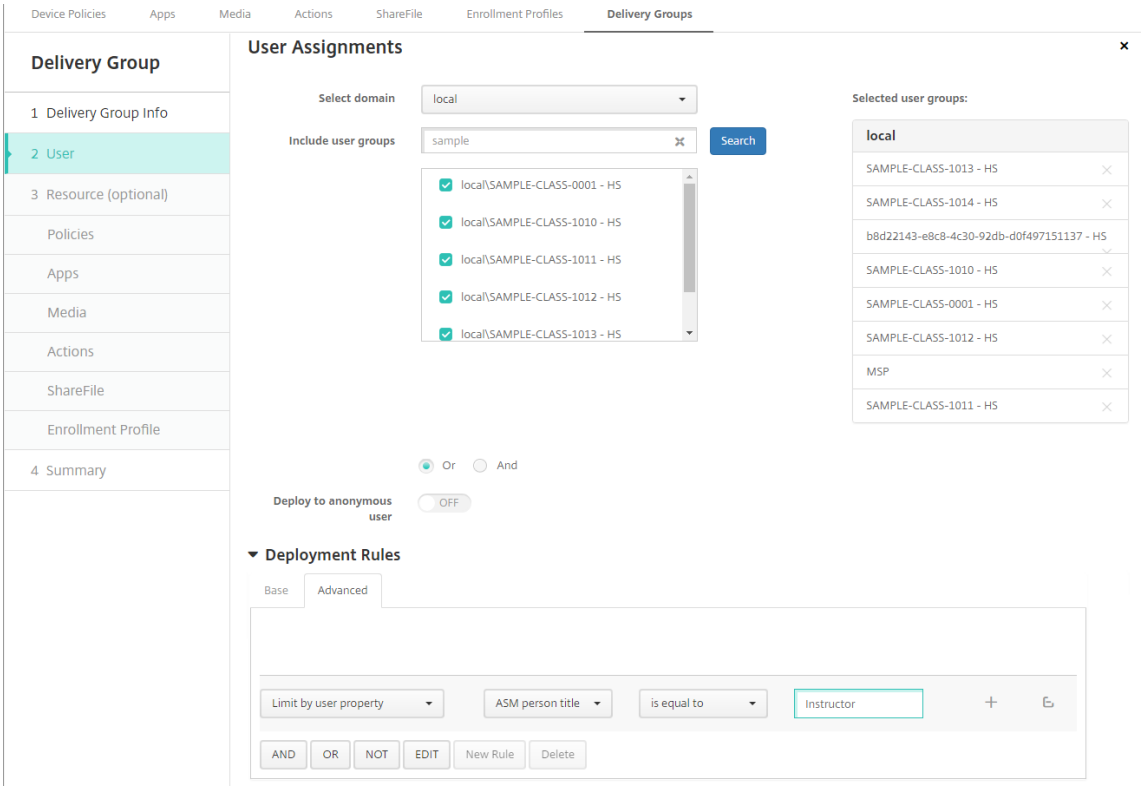
4. Erstellen Sie unter **Konfigurieren > Bereitstellungsgruppen** Bereitstellungsgruppen für Lehrkräfte und Lernende. Wählen Sie die Klassen aus, die aus ASM importiert wurden. Erstellen Sie außerdem eine Bereitstellungsregel für Lehrkräfte und Studenten.

   Die folgenden Benutzerzuweisungen gelten beispielsweise für Lehrkräfte. Die Bereitstellungsregel lautet:

```
1 Limit by user property
```

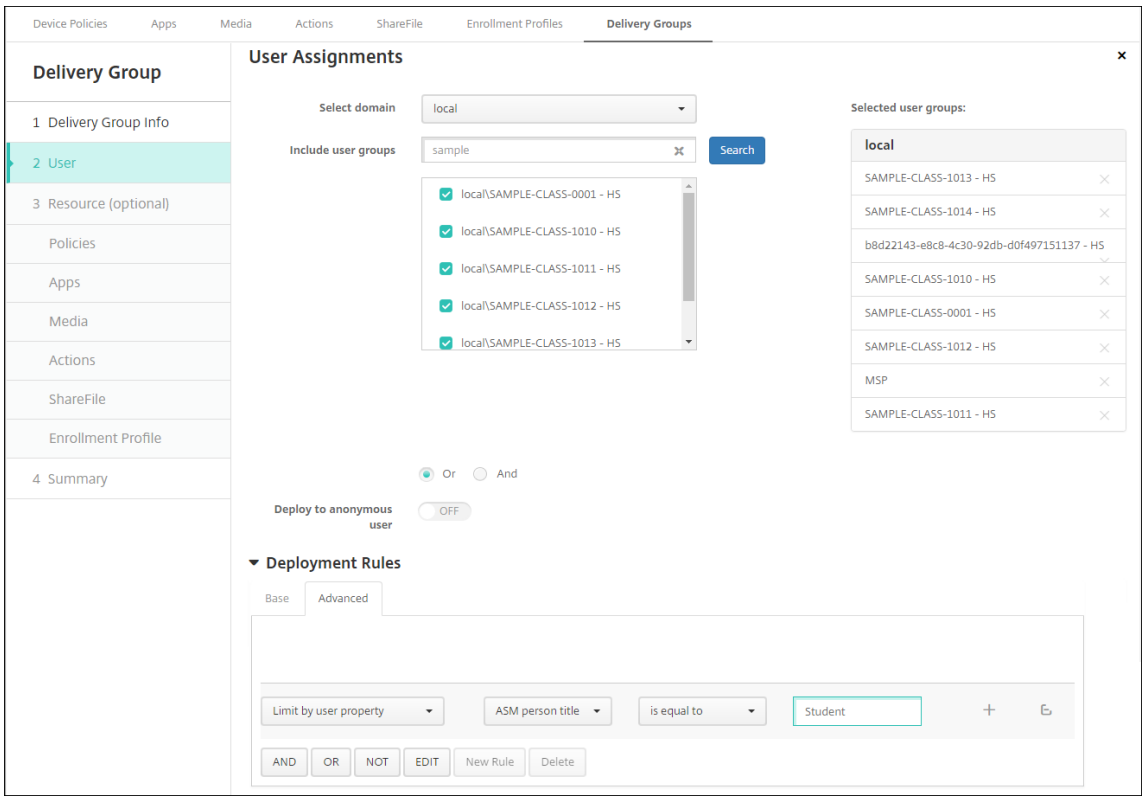


```
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```

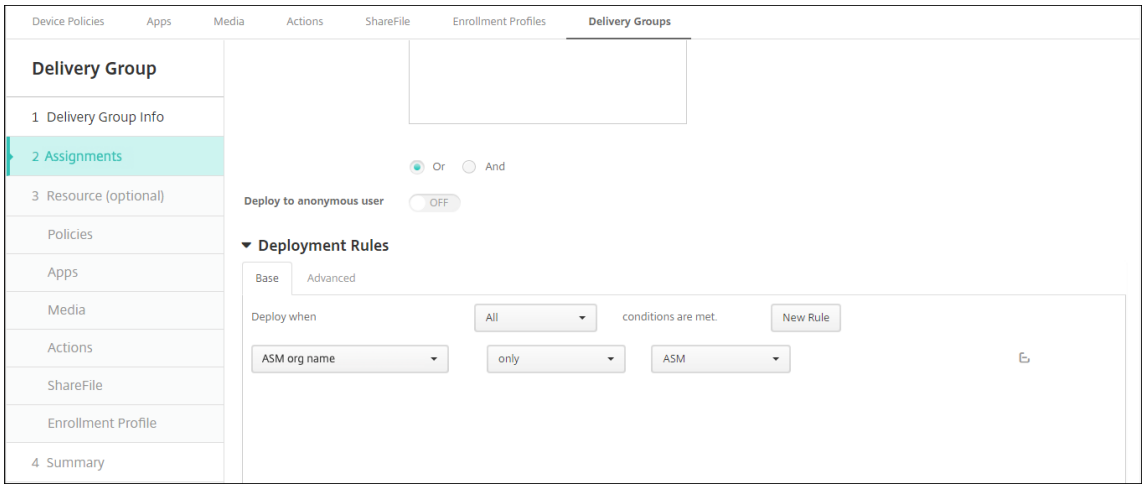


Die folgenden Benutzerzuweisungen gelten für Lernende. Die Bereitstellungsregel lautet:

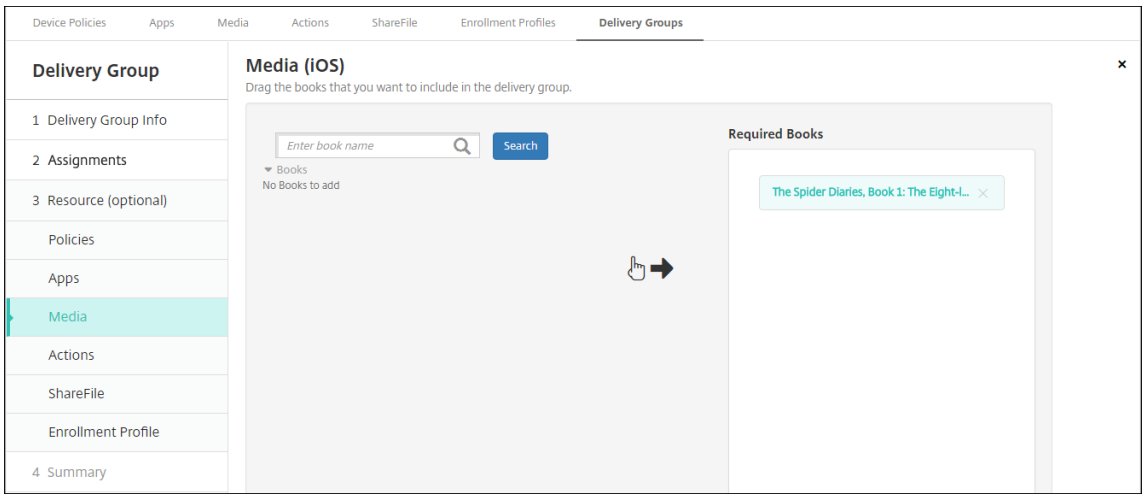
```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

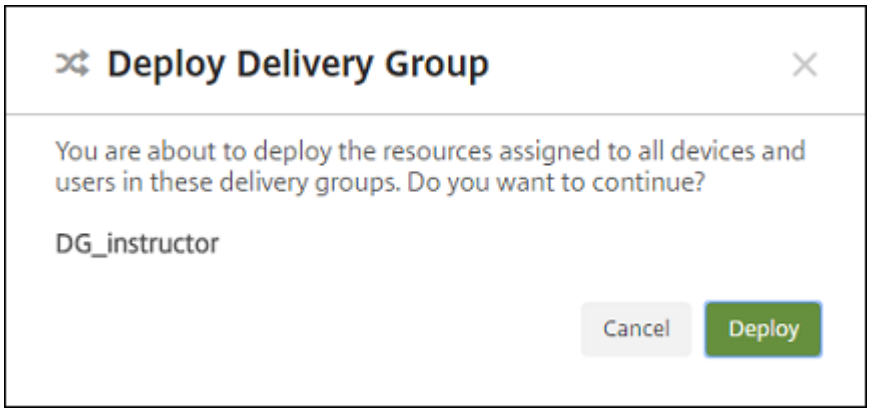
Sie können Bereitstellungsgruppen auch nach einer auf dem ASM-Organisationsnamen basierenden Bereitstellungsregel filtern.



5. Weisen Sie den Bereitstellungsgruppen Ressourcen zu. Das folgende Beispiel zeigt ein iBook in einer Bereitstellungsgruppe.



Das folgende Beispiel zeigt das Bestätigungsdialogfeld, das angezeigt wird, wenn Sie eine Bereitstellungsgruppe auswählen und auf **Bereitstellen** klicken.



Weitere Informationen finden Sie unter Bereitstellen von Ressourcen in den Abschnitten “Bearbeiten einer Bereitstellungsgruppe” und “Bereitstellen in Bereitstellungsgruppen”.

Schritt 8: Testen der Registrierung von Geräten der Benutzer

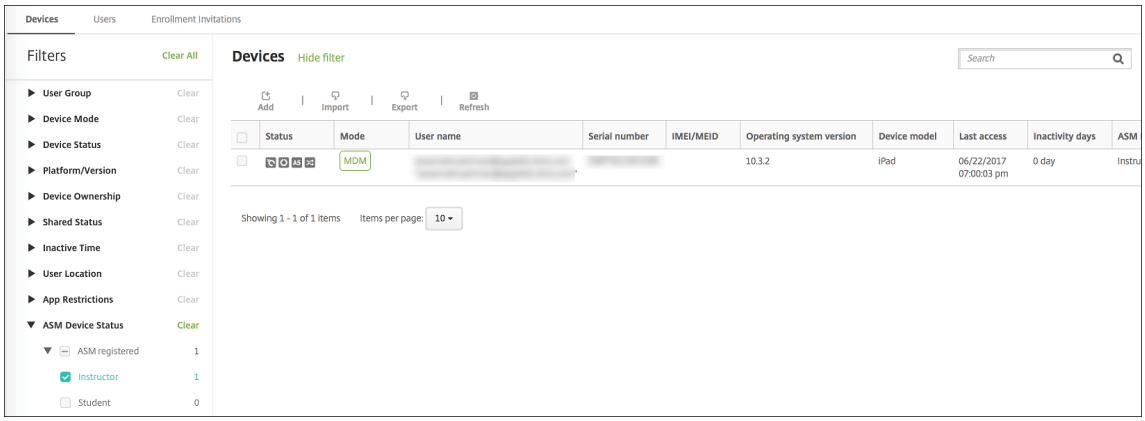
Sie können Geräte von Lehrkräften und Lernenden mit einer der folgenden Methoden registrieren:

- Eine Verwaltungskraft kann die Geräte mithilfe des Benutzerkennworts registrieren, das Sie in der XenMobile-Konsole festlegen. Dadurch können Sie Benutzern Geräte zur Verfügung stellen, die bereits mit Apps und Medien eingerichtet sind.
- Die Benutzer melden sich bei Erhalt ihres Geräts mit dem von Ihnen angegebenen Benutzerkennwort an. Nach Abschluss der Registrierung sendet XenMobile Geräterichtlinien, Apps und Medien an die Geräte.

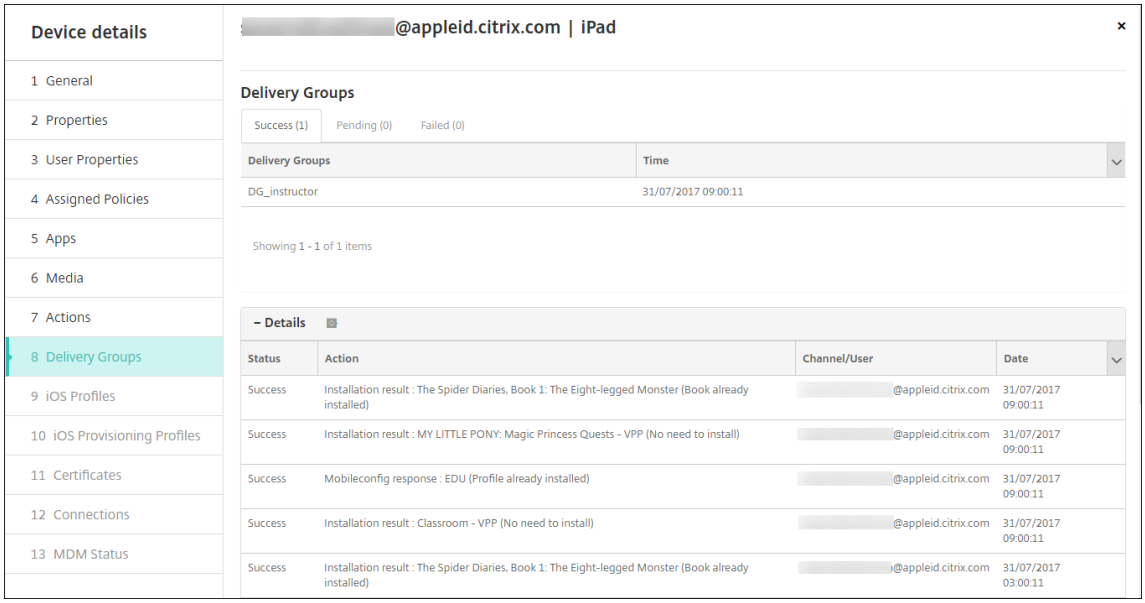
Verwenden Sie zum Testen der Registrierung Apple-Bereitstellungsprogrammgeräte, die mit ASM verknüpft sind.

1. Wenn die Geräte nicht mit ASM verknüpft sind, löschen Sie die Geräteinhalte und -einstellungen durch eine Rücksetzung auf die Werkseinstellungen.
2. Registrieren Sie ein ASM-Gerät mit einer Lehrkraft. Registrieren Sie anschließend ein ASM-Gerät mit einem Lernenden.
3. Prüfen Sie unter **Verwalten > Geräte**, ob beide ASM-Geräte im Nur-MDM-Modus registriert sind.

   Sie können die Seite **Geräte** nach ASM-Gerätestatus filtern: **ASM registriert**, **ASM-Freigabe**, **Lehrkraft** und **Schüler**.



4. Um zu überprüfen, ob die MDM-Ressourcen für jedes Gerät richtig bereitgestellt wurden, wählen Sie das Gerät, klicken Sie auf **Bearbeiten** und überprüfen Sie die verschiedenen Seiten.



Schritt 9: Verteilen der Geräte

Apple empfiehlt, die Geräte an Lehrkräfte und Lernende bei einer entsprechenden Veranstaltung zu verteilen.

Wenn die Geräte nicht vorregistriert sind, stellen Sie den Benutzern zudem Folgendes zur Verfügung:

- XenMobile-Kennwort für die Registrierung
- Temporäres ASM-Kennwort für die verwaltete Apple-ID

Für die Benutzer läuft die Inbetriebnahme folgendermaßen ab:

1. Wenn ein Benutzer sein Gerät nach der Rücksetzung auf die Werkseinstellungen zum ersten Mal startet, wird er von XenMobile im Registrierungsbildschirm zur Registrierung seines Geräts aufgefordert.
2. Der Benutzer gibt sein Kennwort für die verwaltete Apple-ID an sowie das Kennwort, mit dem er sich bei XenMobile authentifiziert.
3. Bei der Einrichtung der Apple-ID wird der Benutzer aufgefordert, sein Kennwort für die verwaltete Apple-ID und das temporäre Kennwort für ASM anzugeben. Durch diese Elemente werden Benutzer beim Apple-Service authentifiziert.
4. Der Benutzer wird aufgefordert, ein Kennwort für seine verwaltete Apple-ID zum Schutz seiner Daten in iCloud zu erstellen.
5. Am Ende des Setupassistenten beginnt XenMobile mit der Installation von Richtlinien, Apps und Medien auf dem Gerät. Für Apps und iBooks, die auf Benutzerebene zugewiesen wurden, fordert der Assistent Lehrkräfte und Lernende auf, sich bei Volume Purchase zu registrieren. Nach Annahme der Einladung erhalten die Nutzer ihre Volume Purchase-Apps und iBooks bei der nächsten Bereitstellung (innerhalb von sechs Stunden).

Konfigurieren von geteilten iPads

Mehrere Schüler in einem Klassenzimmer können ein iPad für verschiedene Fächer teilen, die von einem oder mehreren Lehrern unterrichtet werden.

Sie oder die Lehrkräfte registrieren geteilte iPads und stellen dann Geräterichtlinien, Apps und Medien auf den Geräten bereit. Die Schüler geben dann ihre Apple ID-Anmeldeinformationen an, um sich bei dem geteilten iPad anzumelden. Wenn Sie zuvor eine Richtlinie “Bildungseinrichtung - Konfiguration” für Lernende bereitgestellt haben, melden diese sich nicht mehr als “Anderer Benutzer” an, um Geräte gemeinsam zu nutzen.

XenMobile verwendet zwei Kommunikationskanäle für geteilte iPads: den Systemkanal für den Gerätebesitzer (Lehrkraft) und den Benutzerkanal für den aktuellen Benutzer (Lernender). XenMobile sendet über diese Kanäle die entsprechenden MDM-Befehle für die von Apple unterstützten Ressourcen.

Über den Systemkanal bereitgestellte Ressourcen:

- Geräterichtlinien, z. B. Bildungseinrichtung - Konfiguration, Meldung auf Sperrbildschirm, maximale Anzahl residenter Benutzer und Passcodesperre - Kulanzzeitraum

- Gerätebasierte Volume Purchase-Apps

  Apple unterstützt auf geteilten iPads weder Unternehmensapps noch benutzerbasierte Volume Purchase-Apps. Auf einem geteilten iPad installierte Apps stehen global und nicht für einzelne Benutzer zur Verfügung.

- Benutzerbasierte Volume Purchase-iBooks

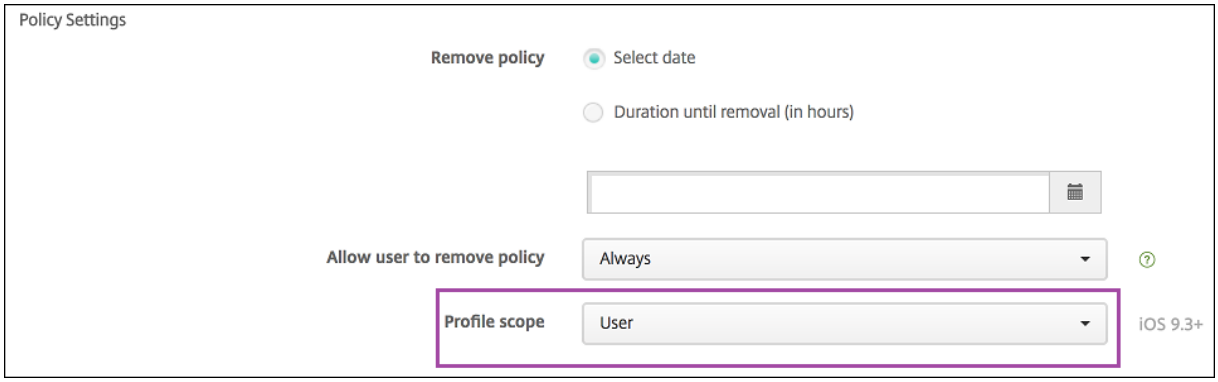
  Apple unterstützt die Zuweisung benutzerbasierter Volume Purchase-iBooks auf geteilten iPads.

Über den Benutzerkanal bereitgestellte Ressourcen:

- Geräterichtlinien: App-Benachrichtigungen, Homebildschirmlayout und Einschränkungen

  XenMobile unterstützt nur diese Geräterichtlinien über den Benutzerkanal.

Beim Konfigurieren von Geräterichtlinien geben Sie den Bereitstellungskanal in der Richtlinieneinstellung **Gültigkeitsbereich für Profil** an.



Zum Entfernen von Geräterichtlinien, die Sie über den Benutzerkanal bereitgestellt haben, müssen Sie als **Bereitstellungsumfang** für die Richtlinie "Profilentfernung" die Option **Benutzer** auswählen.

Allgemeiner Arbeitsablauf

Normalerweise stellen Sie Lehrkräften vorkonfigurierte und betreute iPads zur Verfügung. Die Lehrkräfte verteilen die Geräte dann an die Schüler. Wenn Sie Lehrkräften keine vorinstallierten iPads zum Teilen geben, müssen Sie ihnen ihr XenMobile-Serverkennwort mitteilen, damit sie die Geräte registrieren können.

Der allgemeine Arbeitsablauf zum Konfigurieren und Registrieren geteilter iPads ist wie folgt:

1. Sie fügen mit der XenMobile-Konsole ASM-Konten mit aktiviertem **Freigabemodus** hinzu (**Einstellungen > Apple Deployment Program**). Weitere Informationen finden Sie weiter unten unter "Verwalten von ASM-Konten für geteilte iPads".
2. Sie fügen in XenMobile die erforderlichen Geräterichtlinien, Apps und Medien gemäß den Informationen in diesem Abschnitt hinzu. Sie weisen die Ressourcen Bereitstellungsgruppen zu.

3. Sie bitten die Lehrkräfte, auf den geteilten iPads eine Rücksetzung auf die Werkseinstellungen durchzuführen. Der Remoteverwaltungsbildschirm für die Registrierung wird angezeigt.
4. Die Lehrkräfte registrieren die geteilten iPads.
   XenMobile stellt konfigurierte Ressourcen für jedes registrierte, geteilte iPad bereit. Nach einem automatischen Neustart können die Schüler die Geräte teilen. Eine Anmeldeseite wird auf dem iPad angezeigt.
5. Der Schüler wählt jeweils die Klasse und gibt seine verwaltete Apple-ID und sein vorläufiges ASM-Kennwort ein.
   Es erfolgt die Authentifizierung des iPads bei ASM und der Schüler wird aufgefordert, ein ASM-Kennwort zu erstellen. Bei der nächsten Anmeldung auf dem geteilten iPad gibt der Schüler das neue ASM-Kennwort ein.
6. Es kann sich dann ein weiterer Schüler, der das iPad verwendet, unter Wiederholung des vorigen Schritts anmelden.

Verwalten von ASM-Konten für geteilte iPads

Wenn Sie XenMobile bereits für Apple Bildung verwenden, haben Sie in XenMobile ein für nicht geteilte Geräte (z. B. Geräte der Lehrkräfte) konfiguriertes ASM-Konto. Sie können ASM und den XenMobile-Server parallel für geteilte und nicht geteilte Geräte verwenden.

XenMobile unterstützt folgende Bereitstellungsszenarien:

- Einige geteilte iPads pro Klasse

  In diesem Szenario weisen Sie die geteilten iPads einer Klasse zu. Die iPads bleiben im Klassenzimmer. Lehrkräfte, die verschiedene Fächer in dieser Klasse unterrichten, verwenden dieselben iPads.

- Einige geteilte iPads pro Lehrkraft

  In diesem Szenario weisen Sie die geteilten iPads einer Lehrkraft zu, die die iPads in verschiedenen Klassen verwendet.

Einteilen geteilter iPads in Gerätegruppen

In ASM können Sie Geräte in Gruppen einteilen, indem Sie mehrere MDM-Server erstellen. Wenn Sie geteilte iPads einem MDM-Server zuweisen, erstellen Sie eine Gerätegruppe für jede Gruppe pro Klasse oder pro Lehrkraft geteilter iPads.

- Gruppe 1 geteilter iPads > Gerätegruppe 1 MDM-Server
- Gruppe 2 geteilter iPads > Gerätegruppe 2 MDM-Server
- Gruppe N geteilter iPads > Gerätegruppe N MDM-Server

Hinzufügen von ASM-Konten für jede Gerätegruppe

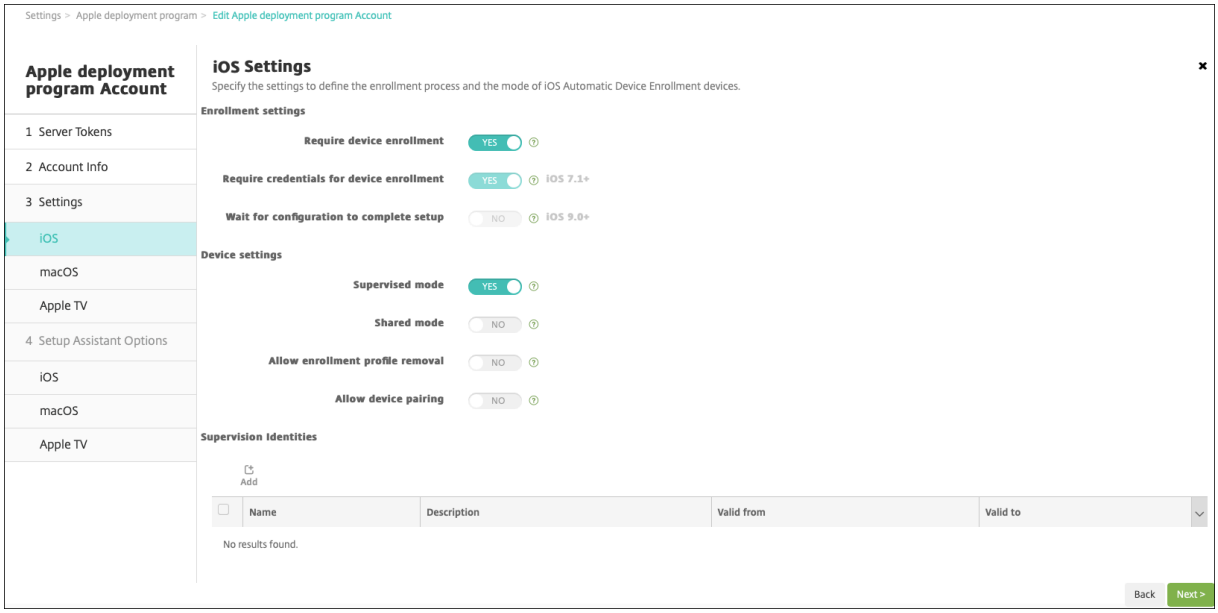
Wenn Sie über die XenMobile-Konsole mehrere ASM-Konten erstellen, importieren Sie automatisch Gruppen geteilter iPads (eine für jede Klasse oder jede Lehrkraft):

- Gerätegruppe 1 MDM-Server > Konto der Gerätegruppe 1
- Gerätegruppe 2 MDM-Server > Konto der Gerätegruppe 2
- Gerätegruppe N MDM-Server > Konto der Gerätegruppe N

Für geteilte iPads gelten folgende Anforderungen:

- Ein ASM-Konto pro Gerätegruppe, für das folgende Einstellungen aktiviert sind:
  - **Geräteregistrierung erforderlich**
  - **Betreuter Modus**
  - **Freigabemodus**
- Verwenden Sie für alle ASM-Konten einer Bildungseinrichtung das gleiche **Suffix der Bildungseinrichtung**.

Um ein Konto hinzuzufügen, gehen Sie zu **Einstellungen > Apple-Bereitstellungsprogramm**.

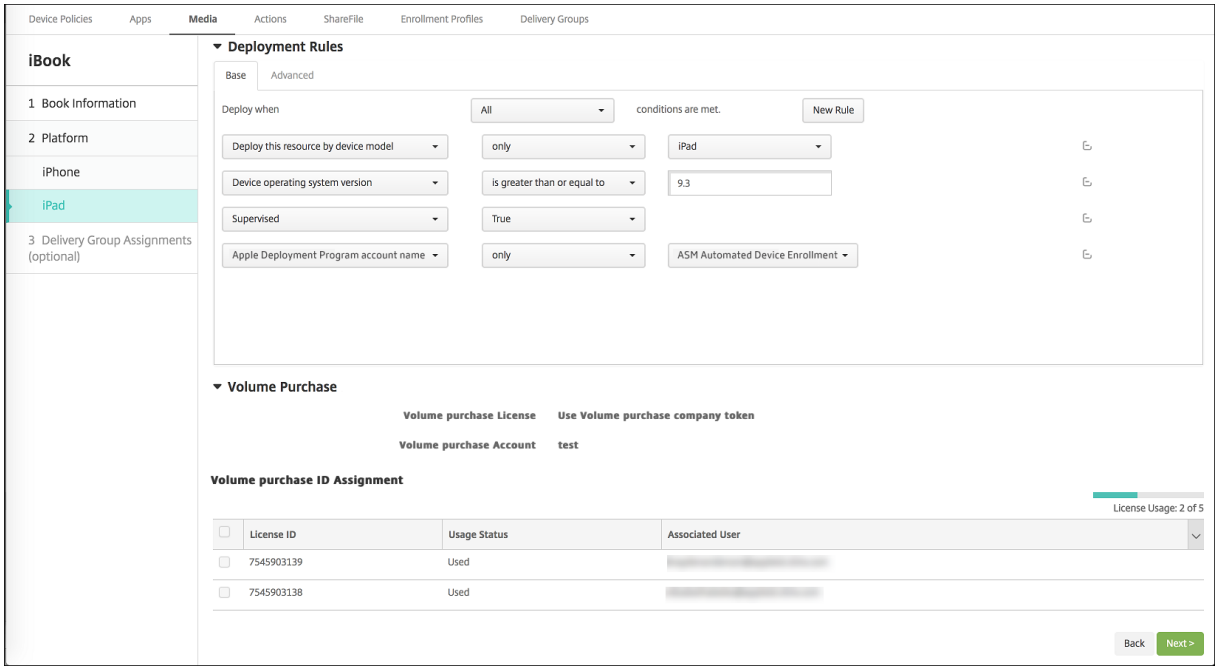


Apps für geteilte iPads

Geteilte iPads unterstützen die Zuweisung von gerätebasierten Volume Purchase-Apps. Vor dem Bereitstellen einer App auf einem geteilten iPad sendet XenMobile eine Anforderung an den Apple Volume Purchase-Server, um Volume Purchase-Lizenzen Geräten zuzuweisen. Um die Volume Purchase-Zuweisungen zu überprüfen, gehen Sie zu **Konfigurieren > Apps > iPad** und erweitern Sie **Volume Purchase**.

Medien für geteilte iPads

Geteilte iPads unterstützen die Zuweisung von benutzerbasierten Volume Purchase-iBooks. Vor dem Bereitstellen von iBooks auf einem geteilten iPad sendet XenMobile eine Anforderung an den Apple Volume Purchase-Server, um Schülern Volume Purchase-Lizenzen zuzuweisen. Um die Volume Purchase-Zuweisungen zu überprüfen, gehen Sie zu **Konfigurieren > Medien > iPad** und erweitern Sie **Volume Purchase**.



Bereitstellungsregeln für geteilte iPads

Bei der Bereitstellung geteilter iPads gelten die Regeln auf der Ebene der Bereitstellungsgruppe nicht, da sie sich auf Benutzereigenschaften beziehen. Fügen Sie zum Filtern der Richtlinien, Apps und Medien für jede Gerätegruppe eine Bereitstellungsregel für die Ressourcen basierend auf dem Namen des Kontos hinzu. Beispiel:

- Legen Sie für das Konto der Gerätegruppe 1 folgende Bereitstellungsregel fest:

```
1   Apple Deployment Program account name
2   Only
3   Device Group 1 account
4
5   <!--NeedCopy-->
```

- Legen Sie für das Konto der Gerätegruppe 2 folgende Bereitstellungsregel fest:

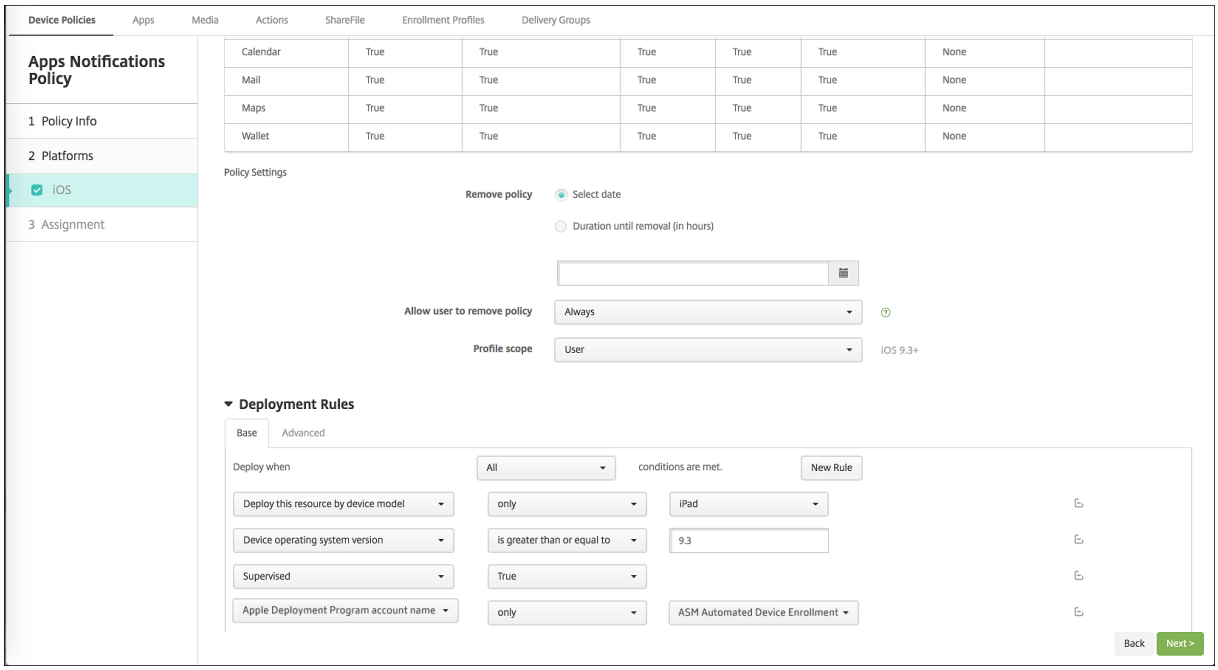
```
1   Apple Deployment Program account name
2   Only
```



```
Device Group 2 account

<!--NeedCopy-->
```

- Legen Sie für das Konto der Gerätegruppe N folgende Bereitstellungsregel fest:

```
Apple Deployment Program account name
Only
Device Group N account

<!--NeedCopy-->
```



Wenn Sie die Apple Classroom-App nur Lehrkräften (für nicht geteilte iPads) bereitstellen möchten, filtern Sie die Ressourcen anhand des ASM-Teilen-Status mit folgenden Bereitstellungsregeln:

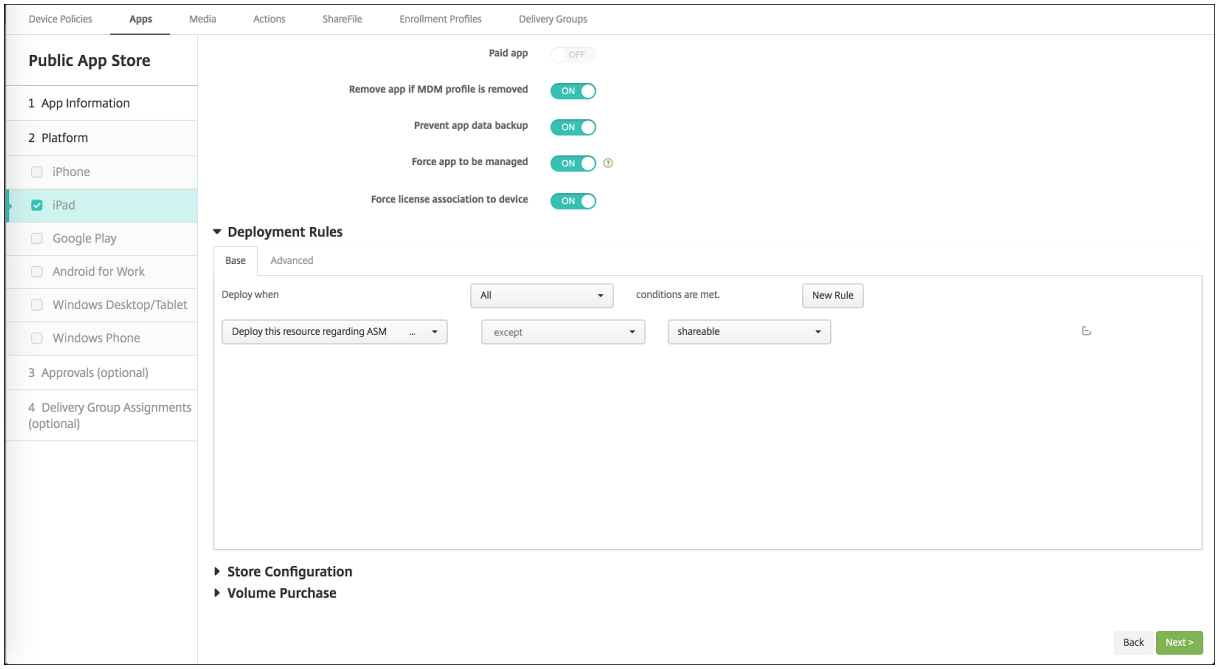
```
Deploy this resource regarding ASM shared mode
only
unshared

<!--NeedCopy-->
```

Oder:

```
Deploy this resource regarding ASM shared mode
except
shareable

```



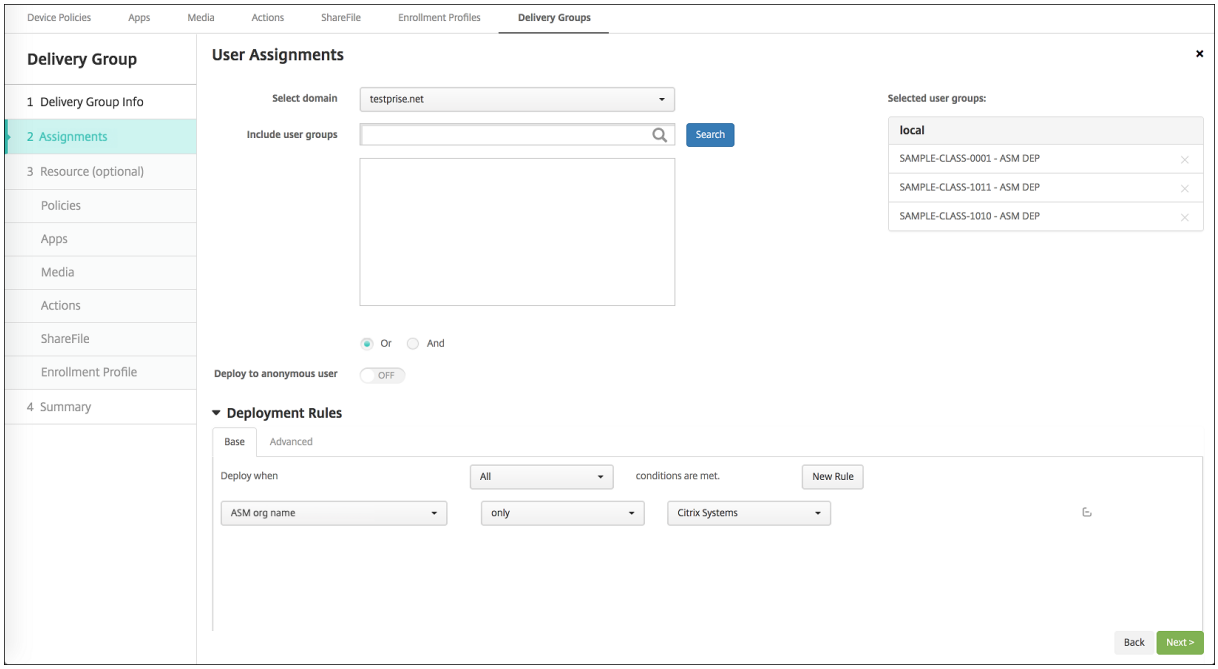
```
5 <!--NeedCopy-->
```



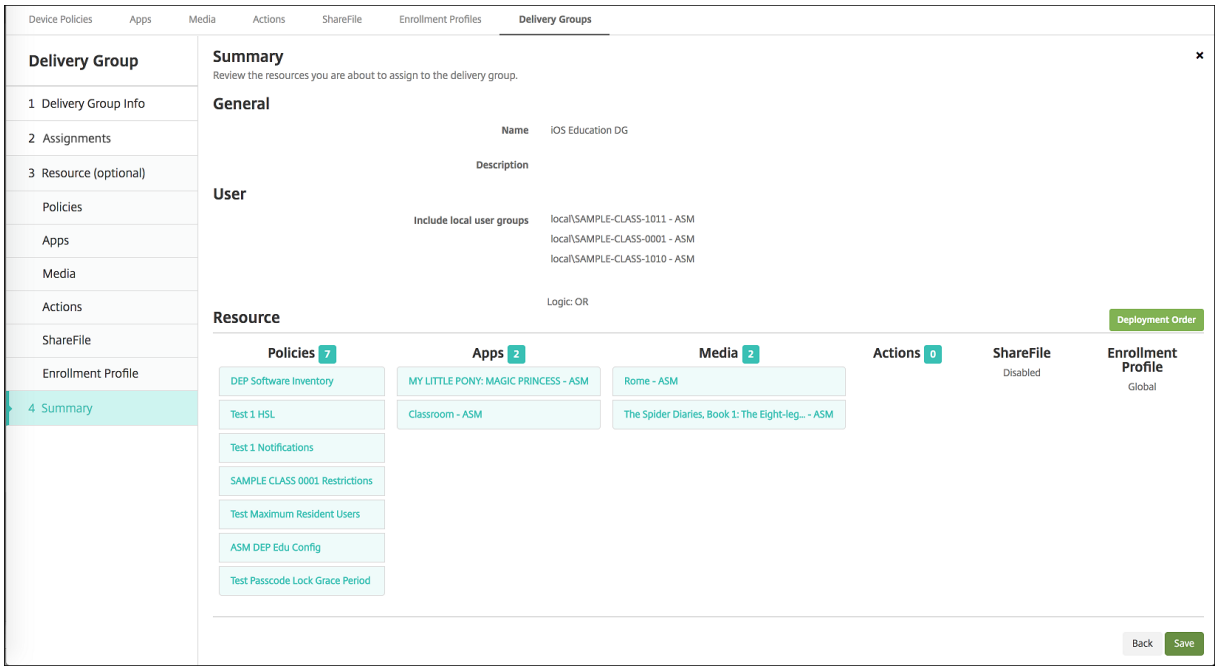
Bereitstellungsgruppen für geteilte iPads

Für die Bereitstellungsgruppe für jede Lehrkraft:

- Konfigurieren Sie eine Bereitstellungsgruppe. Weisen Sie für die Lehrkraft alle in der Richtlinie “Bildung - Konfiguration” definierten Klassen zu.



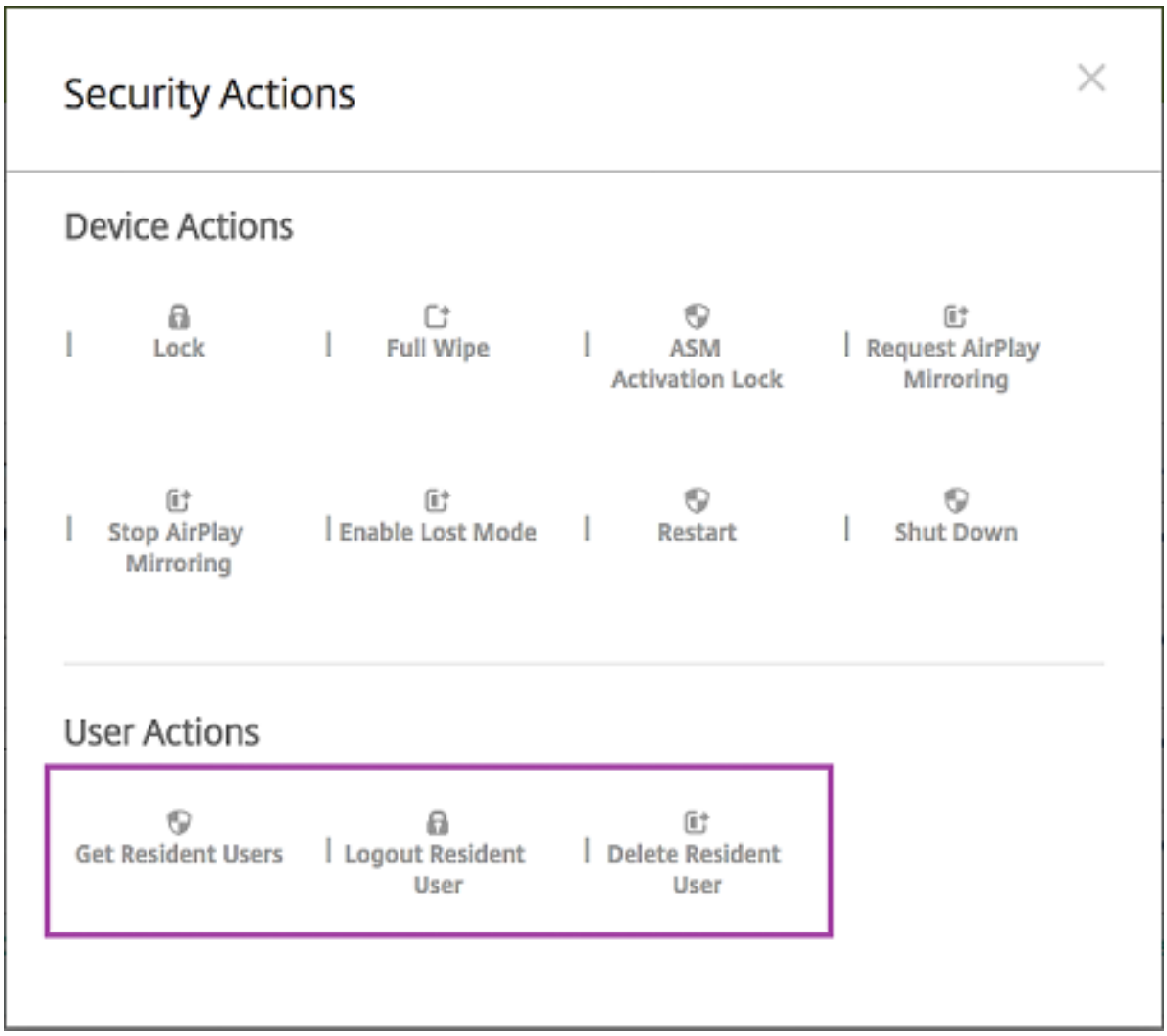
- Die Bereitstellungsgruppe muss folgende MDM-Ressourcen enthalten:
  - Geräterichtlinien:
    * Bildungseinrichtung - Konfiguration
    * Meldung auf Sperrbildschirm
    * App-Benachrichtigungen
    * Layout für Homebildschirm
    * Einschränkungen
    * Maximale Anzahl residenter Benutzer
    * Passcodesperre - Kulanzzeitraum
  - Erforderliche Volume Purchase-Apps
  - Erforderliche Volume Purchase-iBooks



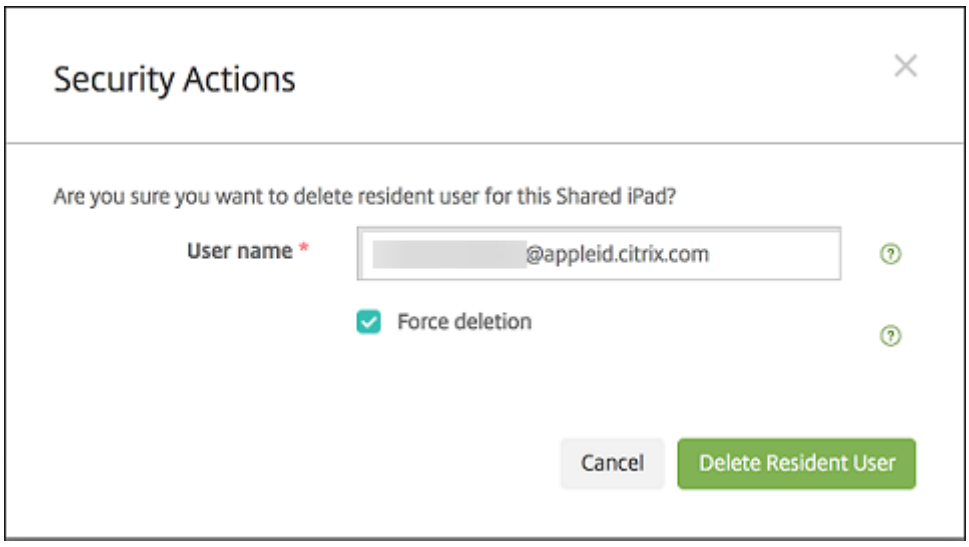
Sicherheitsaktionen für geteilte iPads

Neben den bestehenden Sicherheitsaktionen können Sie für geteilte iPads folgende Sicherheitsaktionen verwenden:

- **Residente Benutzer abrufen:** ruft die Liste der Benutzer ab, die auf dem aktuellen Gerät aktive Konten haben. Diese Aktion erzwingt eine Synchronisierung zwischen Gerät und XenMobile-Konsole.
- **Residenten Benutzer abmelden:** erzwingt die Abmeldung des aktuellen Benutzers.
- **Residenten Benutzer löschen:** löscht die aktuelle Sitzung für einen bestimmten Benutzer. Der Benutzer kann sich erneut anmelden.



Nachdem Sie auf **Residenten Benutzer löschen** geklickt haben, können Sie den Benutzernamen angeben.

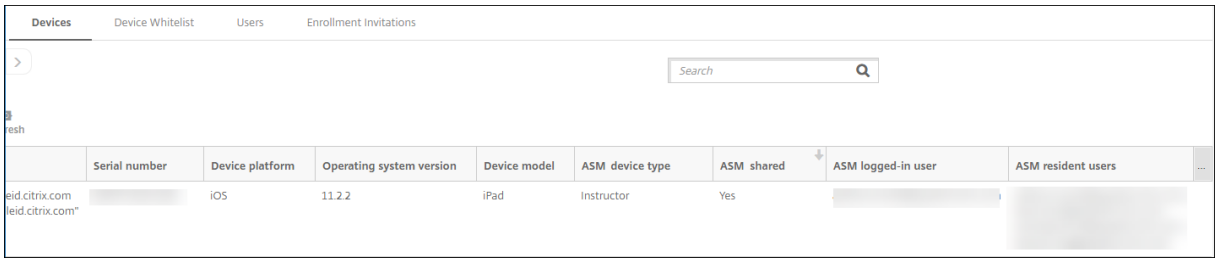


Ergebnisse von Sicherheitsaktionen werden auf den Seiten **Verwalten > Geräte > Allgemein** und **Verwalten > Geräte > Bereitstellungsgruppen** angezeigt.

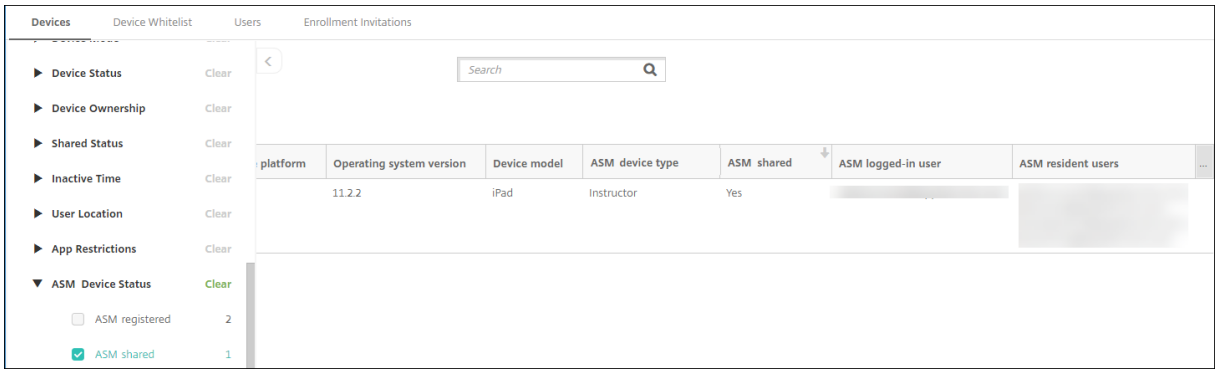
Aufrufen von Informationen über geteilte iPads

Informationen über geteilte iPads finden Sie auf der Seite **Verwalten > Geräte**.

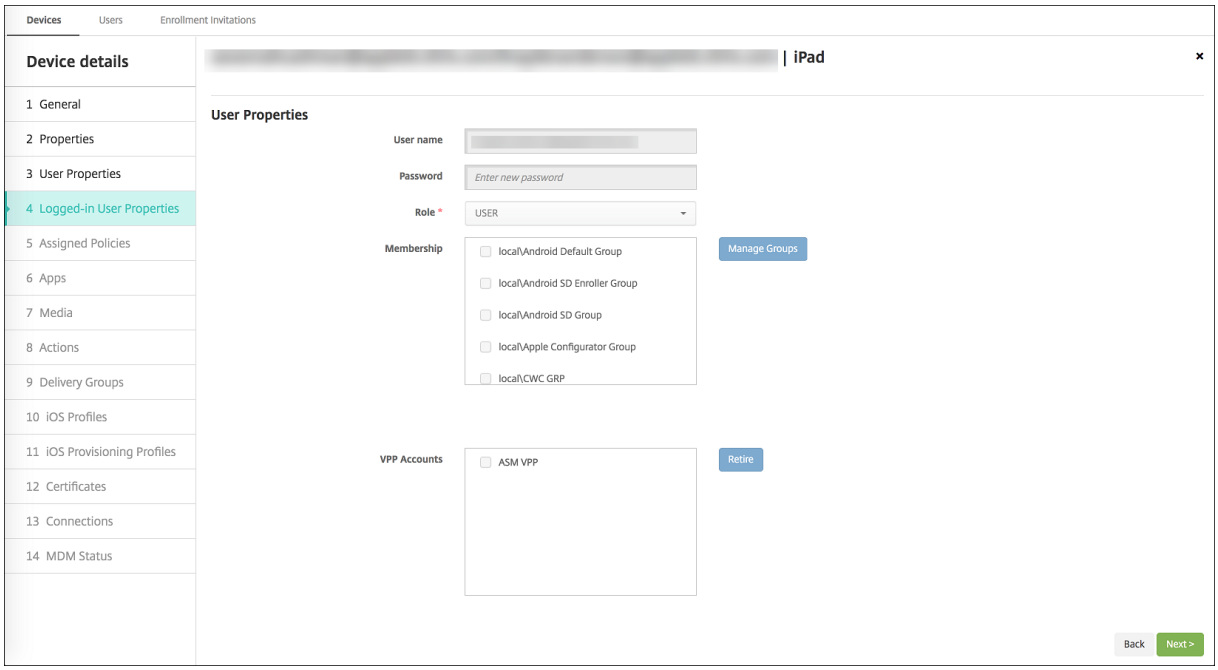
- Es stehen folgende Informationen zur Verfügung:
  - Ob ein Gerät geteilt wird (**ASM-Freigabe**)
  - Wer bei dem geteilten Gerät angemeldet ist (**Angemeldeter ASM-Benutzer**)
  - Alle Benutzer, die dem geteilten Gerät zugewiesen sind (**ASM residente Benutzer**)

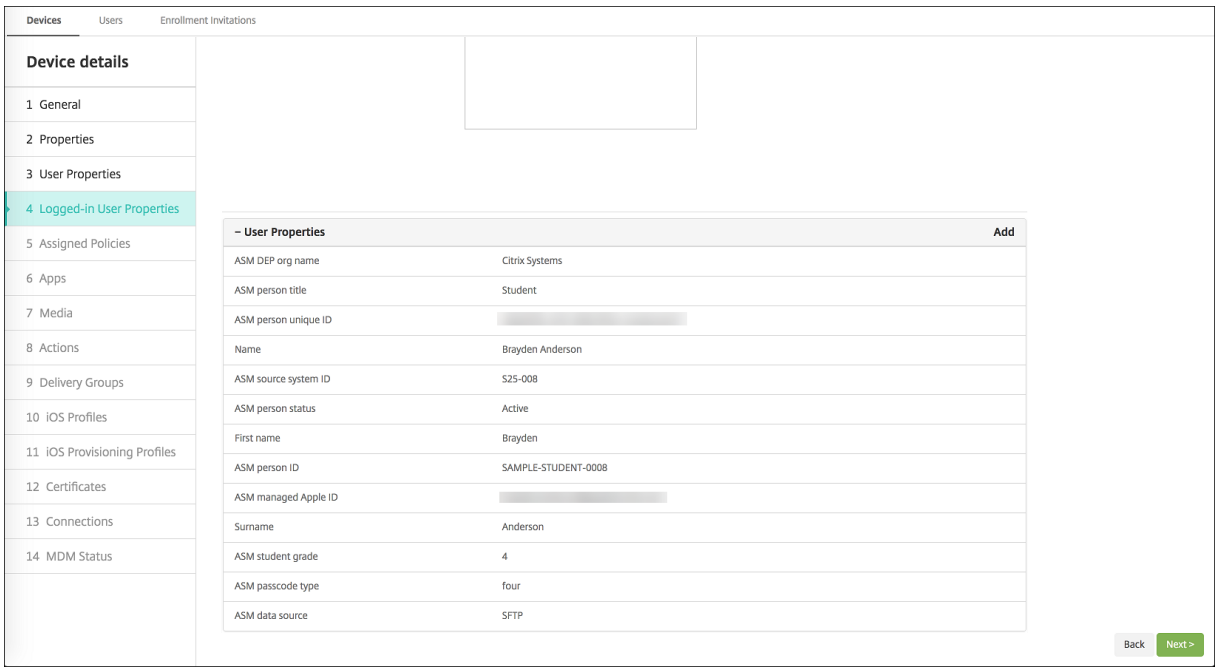


- Sie können die Geräteliste nach ihrem **ASM-Gerätestatus** filtern:

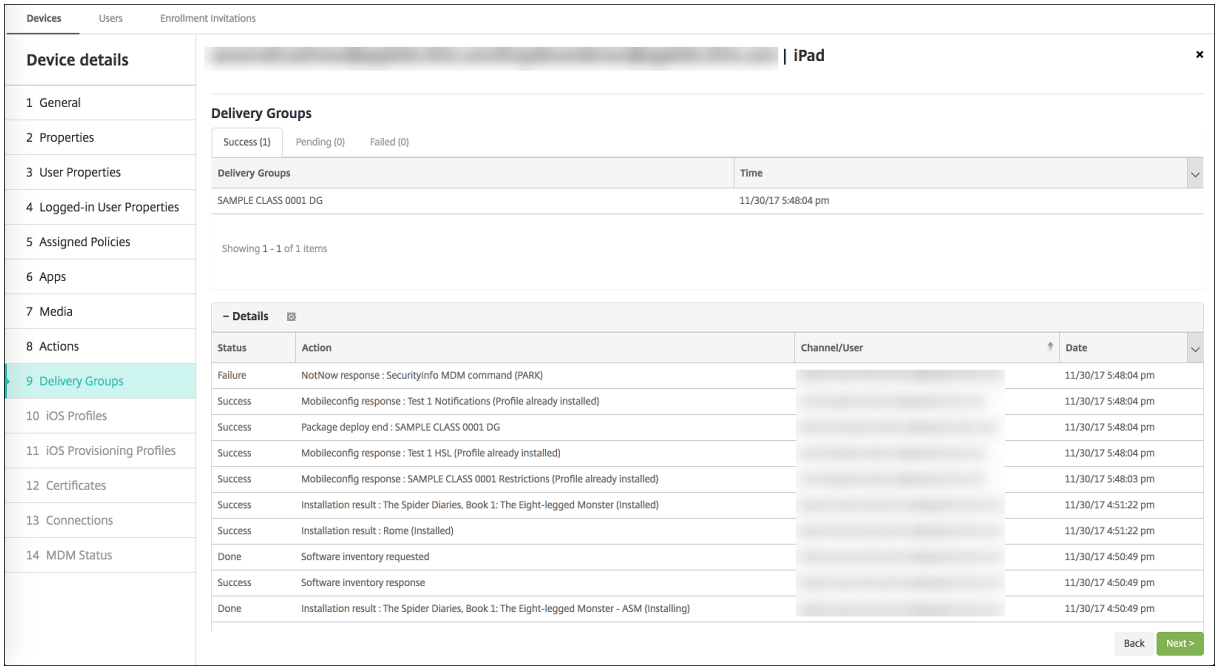


- Sie können Details zu dem bei einem geteilten iPad angemeldeten Benutzer auf der Seite **Verwalten > Geräte > Angemeldeter Benutzer - Eigenschaften** anzeigen.

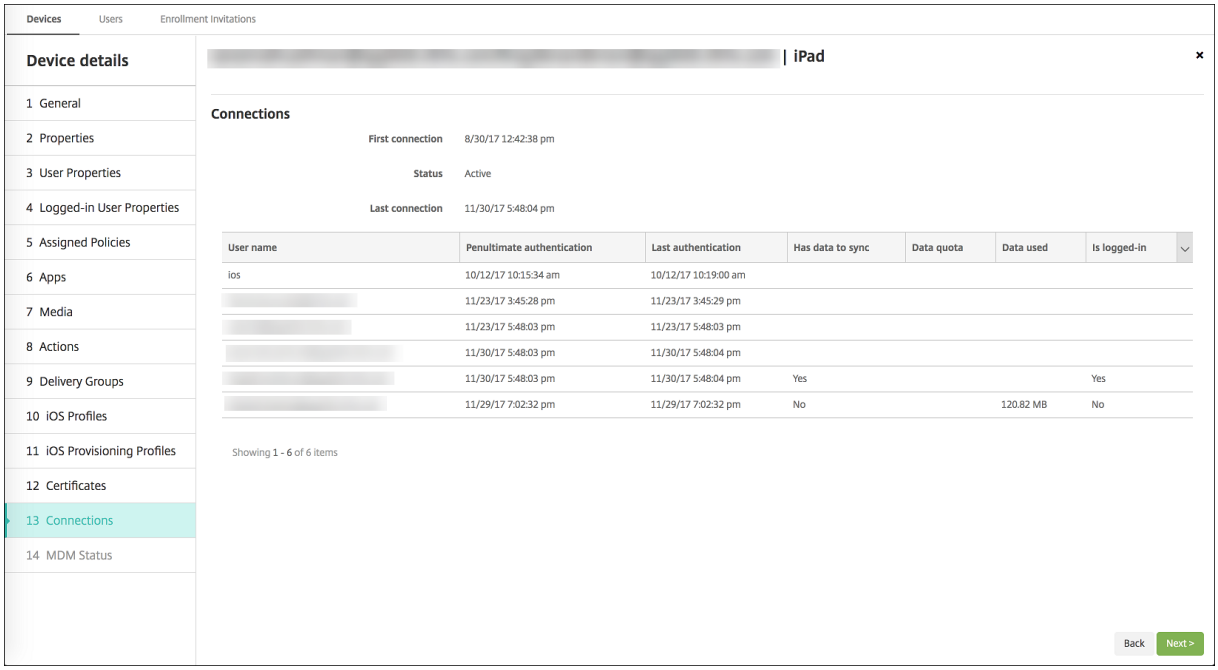




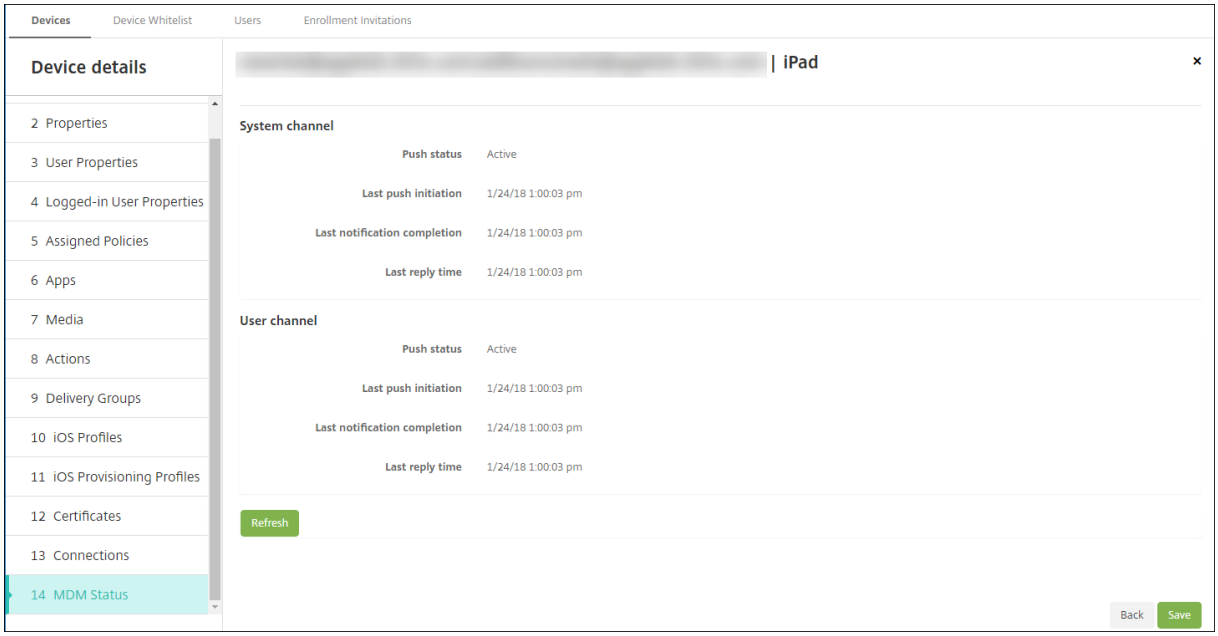
- Informationen zu dem für die Bereitstellung von Ressourcen für Lehrkräfte und Benutzer in einer Bereitstellungsgruppe verwendeten Kanal finden Sie auf der Seite **Verwalten > Geräte > Bereitstellungsgruppen**. In der Spalte **Kanal/Benutzer** werden der Typ (**System** oder **Benutzer**) und der Empfänger (Lehrkraft oder Lernende) angezeigt.



- Es stehen folgende Informationen zu residenten Benutzern zur Verfügung:
  - **Zu synchronisierende Daten vorhanden:** Gibt an, ob Daten des Benutzers zur Synchronisierung mit der Cloud vorhanden sind.
  - **Datenkontingent:** das für den Benutzer festgelegte Datenkontingent in Byte. Ein Kontingent wird möglicherweise nicht angezeigt, wenn Benutzerkontingente vorübergehend deaktiviert sind oder für den Benutzer nicht erzwungen werden.
  - **Verwendete Daten:** die von dem Benutzer verwendete Datenmenge in Byte. Es kann vorkommen, dass kein Wert angezeigt wird, wenn beim Erfassen der Informationen durch das System ein Fehler auftritt.
  - **Ist angemeldet:** zeigt an, ob der Benutzer beim Gerät angemeldet ist.



- Sie können den Pushstatus für beide Kanäle anzeigen.



Verwalten von Lehrkräften, Lernenden und Unterrichtsdaten

Beim Verwalten von Lehrkräften, Lernenden und Unterrichtsdaten ist Folgendes zu beachten:

- Ändern Sie keine verwalteten Apple-IDs, nachdem Sie ASM-Informationen in XenMobile importiert haben. Auch XenMobile verwendet ASM-Benutzer-IDs zur Identifizierung von Benutzern.

- Wenn Sie in ASM Unterrichtsdaten hinzufügen oder ändern, nachdem Sie eine oder mehrere Geräterichtlinien “Bildungseinrichtung - Konfiguration” erstellt haben, bearbeiten Sie die Richtlinien und stellen Sie sie erneut bereit.
- Bei Änderung der Lehrkraft für eine Klasse nach Bereitstellung der Geräterichtlinie “Bildung - Konfiguration” vergewissern Sie sich, dass die Richtlinie in der XenMobile-Konsole aktualisiert wird, und stellen Sie sie dann erneut bereit.
- Wenn Sie die Benutzereigenschaften im ASM-Portal aktualisieren, aktualisiert XenMobile diese Eigenschaften auch in der Konsole. XenMobile erhält jedoch die ASM-Titeleigenschaft (Lehrkraft, Schüler oder Andere) nicht auf die gleiche Weise wie andere Eigenschaften. Wenn Sie den ASM-Titel in ASM ändern, führen Sie daher die folgenden Schritte durch, um diese Änderung in XenMobile zu übernehmen:

Zum Verwalten der Daten:

1. Aktualisieren Sie im ASM-Portal die Klassenstufe und löschen Sie die Lehrkraftstufe.
2. Wenn Sie ein Lernendenkonto in ein Lehrkraftkonto geändert haben, entfernen Sie den Benutzer aus der Liste der Lernenden in der Klasse. Fügen Sie den Benutzer dann der Liste der Lehrkräfte derselben oder einer anderen Klasse hinzu.

   Wenn Sie ein Lehrkraftkonto in ein Lernendenkonto geändert haben, entfernen Sie den Benutzer aus der Klasse. Fügen Sie den Benutzer dann der Liste der Lernenden derselben oder einer anderen Klasse hinzu. Ihre Änderungen werden bei der nächsten Synchronisierung (standardmäßig alle fünf Minuten) oder beim Abrufen (standardmäßig alle 24 Stunden) in der XenMobile-Konsole angezeigt.
3. Bearbeiten Sie die Geräterichtlinie “Bildung - Konfiguration”, um die Änderung zu übernehmen und stellen Sie sie erneut bereit.

   - Wenn Sie einen Benutzer aus dem ASM-Portal löschen, löscht XenMobile diesen Benutzer nach einem Abruf auch aus der XenMobile-Konsole.

     Sie können das Intervall zwischen zwei Basiswerten reduzieren, indem Sie den Wert der folgenden Servereigenschaft ändern: **bulk.enrollment.fetchRosterInfoDelay** (Standardwert ist **1440** Minuten).
   - Wenn ein Lernender zu einer Klasse hinzukommt, nachdem Sie Ressourcen bereitgestellt haben, erstellen Sie eine Bereitstellungsgruppe für diesen einen Lernenden und stellen Sie ihm dann die Ressourcen bereit.
   - Wenn ein Lernender oder eine Lehrkraft das temporäre Kennwort verliert, veranlassen Sie, dass die Person sich an den ASM-Administrator wendet. Der Administrator kann das temporäre Kennwort bereitstellen oder ein neues generieren.

Verwalten eines verlorenen oder gestohlenen Geräts, das mit dem Apple-Bereitstellungsprogramm Apple School Manager (ASM) bereitgestellt und registriert ist

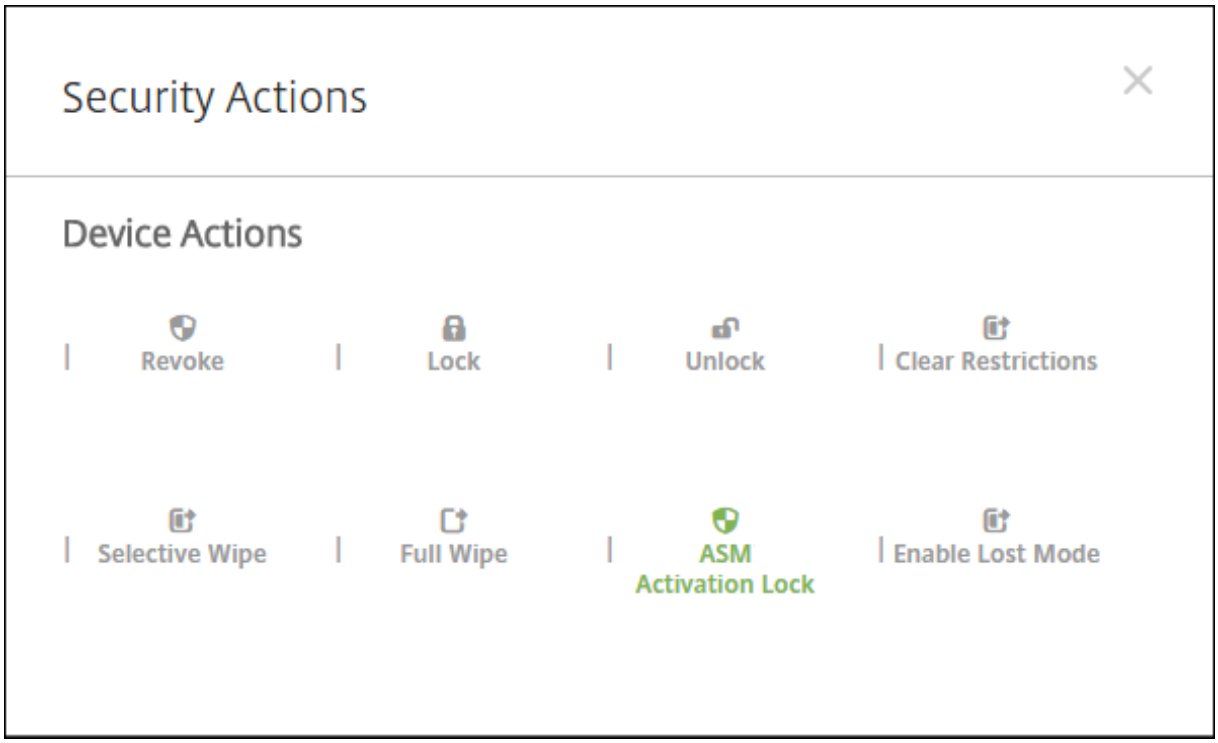
Der Apple-Service Find My iPhone/iPad enthält ein Feature zur Aktivierungssperre. Die Aktivierungssperre verhindert, dass nicht autorisierte Benutzer ein verlorenes oder gestohlenes Gerät, das beim Apple-Bereitstellungsprogramm registriert ist, verwenden oder verkaufen.

XenMobile enthält die Sicherheitsaktion **ASM-Aktivierungssperre**, mit der Sie einen Sperrcode an Geräte senden, die mit dem ASM-Apple-Bereitstellungsprogramm registriert sind.

Wenn Sie die Sicherheitsaktion **ASM-Aktivierungssperre** verwenden, kann XenMobile Geräte orten, ohne dass der Find My iPhone/iPad-Service vom Benutzer aktiviert werden muss. Wenn ein ASM-Gerät auf die Werkseinstellungen zurückgesetzt wurde oder alle Daten auf dem Gerät gelöscht wurden, gibt der Benutzer seine verwaltete Apple-ID und sein Kennwort zum Entsperren des Geräts an.

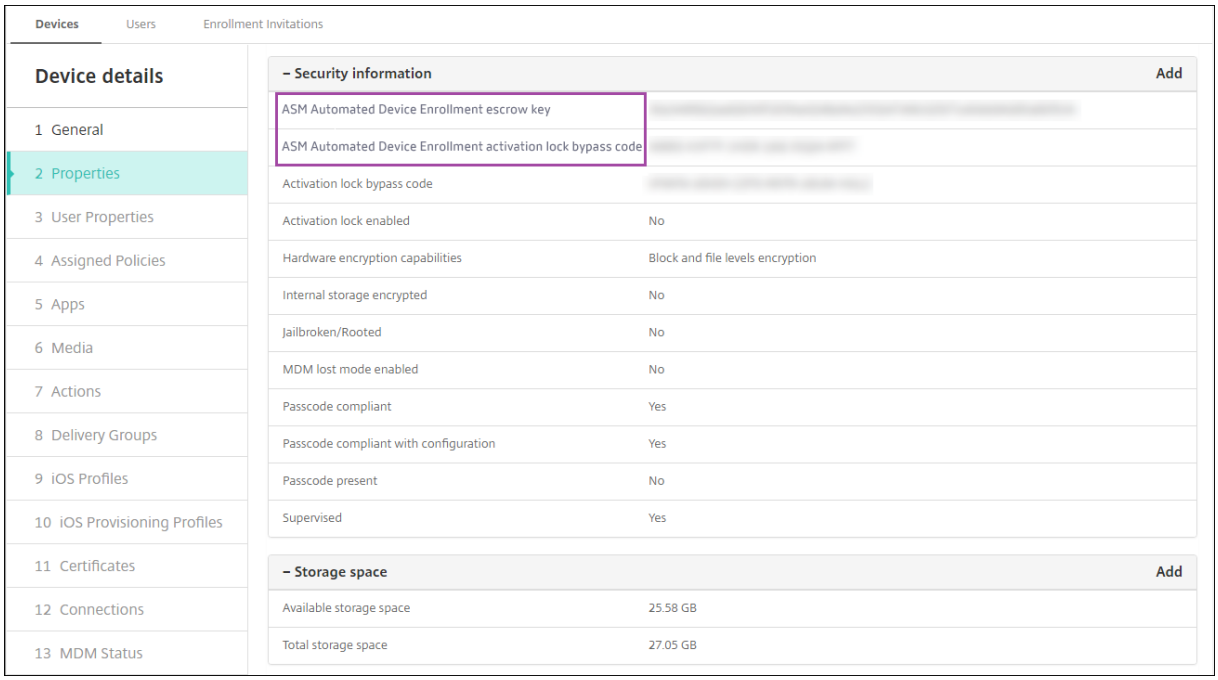
Zum Entsperren von Geräten über die Konsole klicken Sie auf die Sicherheitsaktion **Aktivierungssperre umgehen**. Weitere Informationen zur Umgehung von Aktivierungssperren finden Sie unter Umgehen einer iOS-Aktivierungssperre. Der Benutzer kann auch die Anmeldung leer lassen und den Code zum Umgehen der **ASM-Aktivierungssperre** als Kennwort eingeben. Diese Informationen stehen auf der Registerkarte **Eigenschaften** unter **Gerätedetails** zur Verfügung.

Um die Aktivierungssperre festzulegen, wählen Sie unter **Verwalten > Geräte** das Gerät aus, klicken Sie auf **Sicherheit** und dann auf **ASM-Aktivierungssperre**.

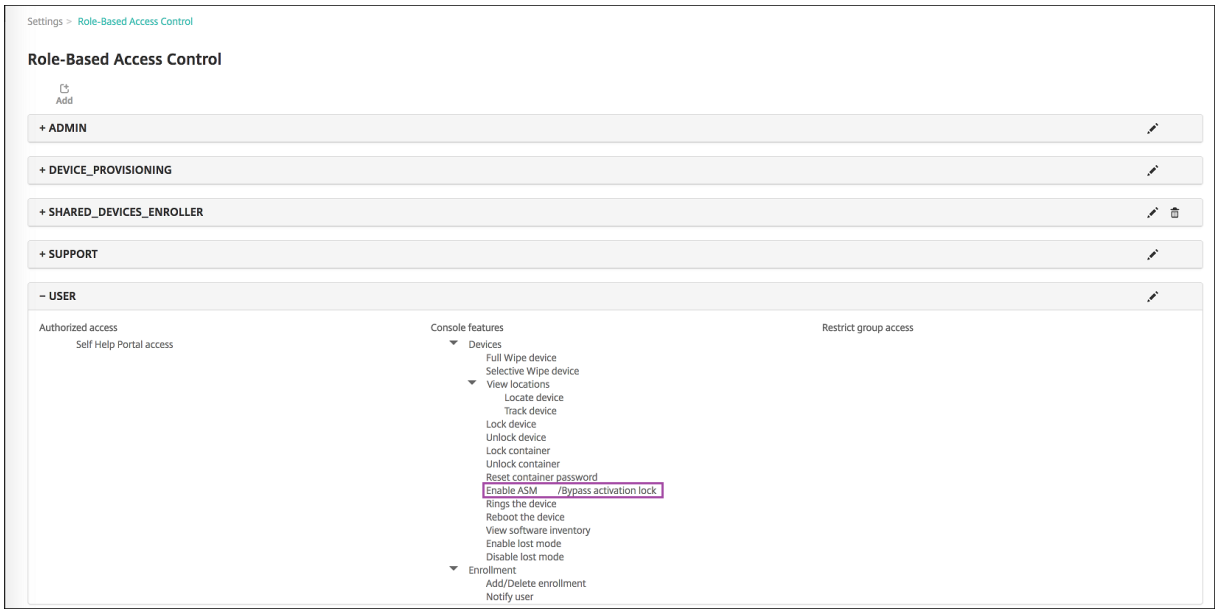


Die Eigenschaften **Hinterlegter ASM-Schlüssel** und **Code zum Umgehen der ASM-Aktivierungssperre**

werden unter **Gerätedetails** angezeigt.



Die RBAC-Berechtigung für eine ASM-Aktivierungssperre ist **Geräte > Umgehung der Aktivierungssperre für ASM aktivieren**.



Verteilen von Apple-Apps

January 5, 2022

XenMobile verwaltet Apps, die auf Geräten bereitgestellt werden. Sie können folgende Arten von iOS/iPadOS- und macOS-Apps organisieren und bereitstellen.

- **Öffentlicher App-Store (nur iOS/iPadOS):** Kostenlose oder kostenpflichtige Apps in einem öffentlichen App-Store, z. B. Apple App Store oder Google Play. Beispiel: GoToMeeting.
- **Unternehmen (iOS/iPadOS/macOS):** Native Apps, die nicht MDX-fähig sind und keine Richtlinien für MDX-Apps enthalten.
- **MDX (nur iOS/iPadOS):** Apps, die mit dem MAM-SDK vorbereitet oder mit dem MDX Toolkit umschlossen wurden. Diese Apps enthalten MDX-Richtlinien. Sie erhalten MDX-Apps über interne Quellen und öffentliche Stores.
- **Volume Purchase (iOS/iPadOS/macOS):** Apps mit Lizenzen, die über das Apple-Programm für Volumenlizenzen verwaltet werden.
- **Benutzerdefinierte iOS-Apps (nur iOS/iPadOS):** Proprietäre Business-to-Business-Apps, die intern oder von einem Drittanbieter entwickelt wurden.

Weitere Informationen zu den einzelnen App-Typen finden Sie unter Hinzufügen von Apps.

Für einige Bereitstellungen ist ein ABM (Apple Business Management)- oder ein ASM (Apple School Management)-Konto erforderlich. Weitere Informationen finden Sie in den folgenden Abschnitten.

Für jeden App-Typ und jede Verteilungsmethode gibt Citrix bestimmte Konfigurationsempfehlungen. Informationen zum Verteilen von Apps für andere Plattformen finden Sie unter Hinzufügen von Apps. Die folgenden Abschnitte enthalten detaillierte Angaben zur iOS-App-Konfiguration.

Allgemeine Schritte für die App-Verteilung

Szenario	Schritt 1: Verknüpfen von Konten	Schritt 2: Hinzufügen und Konfigurieren von Apps	Schritt 3: Konfigurieren von Bereitstellungsgruppen und Bereitstellen von Apps
Apps aus dem öffentlichen App-Store, einschließlich mobiler Apps von Citrix	Nicht zutreffend	**In XenMobile:** Gehen Sie zu **Konfigurieren > Apps** und fügen Sie Apps für iPhone oder iPad aus dem **öffentlichen App-Store** hinzu. Konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In XenMobile:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.
Apps aus öffentlichem App-Store, bereitgestellt mit Apple Volume Purchase, einschließlich mobiler Apps von Citrix	Registrieren Sie sich in einem Apple-Bereitstellungsprogramm. **In XenMobile:** Gehen Sie zu **Einstellungen > Volume Purchase**, um Ihr Volume Purchase-Konto hinzuzufügen.	**In ABM oder ASM:** Kaufen Sie Apps in "Apps and Books" und fügen Sie sie hinzu. **In XenMobile:** Gehen Sie zu **Konfigurieren > Apps**, konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In XenMobile:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.

Szenario	Schritt 1: Verknüpfen von Konten	Schritt 2: Hinzufügen und Konfigurieren von Apps	Schritt 3: Konfigurieren von Bereitstellungsgruppen und Bereitstellen von Apps
Unternehmensapps	Nicht zutreffend	**In XenMobile:** Gehen Sie zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen** und dann auf **Unternehmen**. Laden Sie die IPA-Datei hoch. Konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In XenMobile:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.
MDX-Apps	Nicht zutreffend	**In XenMobile:** Gehen Sie zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen** und dann auf **MDX**. Stellen Sie sicher, dass Sie **iPad**/**iPhone** als Plattform ausgewählt haben. Laden Sie die MDX-Datei hoch. Konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In XenMobile:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.

Szenario	Schritt 1: Verknüpfen von Konten	Schritt 2: Hinzufügen und Konfigurieren von Apps	Schritt 3: Konfigurieren von Bereitstellungsgruppen und Bereitstellen von Apps
MDX-Apps, die mit Apple Volume Purchase verteilt werden	Registrieren Sie sich in einem Apple-Bereitstellungsprogram **In XenMobile:** Gehen Sie zu **Einstellungen > Volume Purchase**, um Ihr Volume Purchase-Konto hinzuzufügen.	**In ABM:** Kaufen Sie MDX-Apps in “Apps and Books” und fügen Sie sie hinzu. Verknüpfen Sie die App mit Ihrem ABM-Konto. **In XenMobile:** Gehen Sie zu **Konfigurieren > Apps**, konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In XenMobile:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.
Benutzerdefinierte Apps	Registrieren Sie sich in einem Apple-Bereitstellungsprogramm **In XenMobile:** Gehen Sie zu **Einstellungen > Volume Purchase**, um Ihr Volume Purchase-Konto hinzuzufügen.	**In ABM:** Fügen Sie Ihre App als private App zum App-Store hinzu. Verknüpfen Sie die App mit Ihrem ABM-Konto. **In XenMobile:** Gehen Sie zu **Konfigurieren > Apps**, konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In XenMobile:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.

Szenario	Schritt 1: Verknüpfen von Konten	Schritt 2: Hinzufügen und Konfigurieren von Apps	Schritt 3: Konfigurieren von Bereitstellungsgruppen und Bereitstellen von Apps
MDX-fähige benutzerdefinierte Apps	Registrieren Sie sich in einem Apple-Bereitstellungsprogram **In XenMobile:** Gehen Sie zu **Einstellungen > Volume Purchase**, um Ihr Volume Purchase-Konto hinzuzufügen.	**In ABM:** Fügen Sie Ihre App als private App zum App-Store hinzu. Verknüpfen Sie die App mit Ihrem ABM-Konto. **In XenMobile:** Gehen Sie zu **Konfigurieren > Apps** und laden Sie die MDX-Datei hoch. Konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In XenMobile:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.

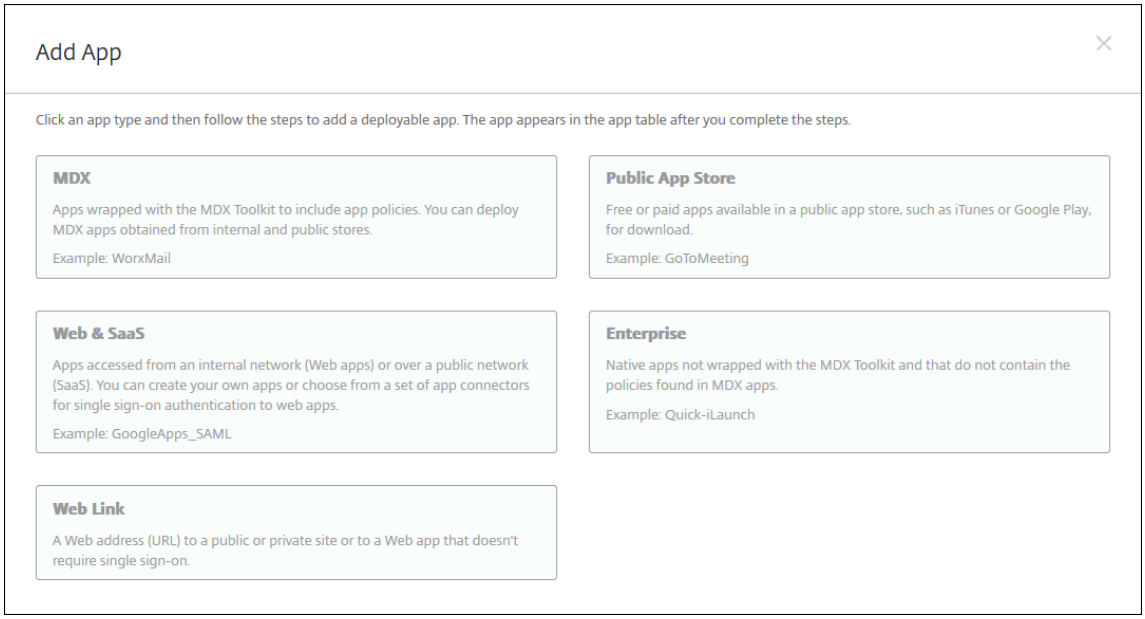
Apps aus öffentlichem App-Store

Sie können kostenlose und kostenpflichtige Apps aus dem App Store zu XenMobile hinzufügen.

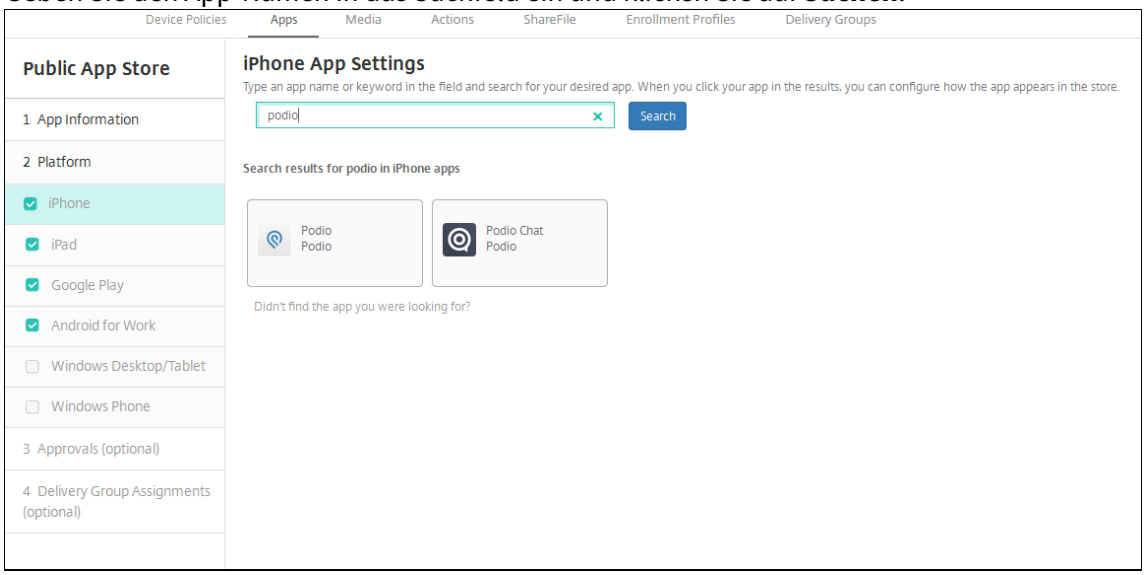
Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Nein
Verfügbar auf	iOS/iPadOS

Schritt 1: Hinzufügen und Konfigurieren von Apps

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **Öffentlicher App-Store**.



3. Wählen Sie als Plattform **iPhone** oder **iPad**.
4. Geben Sie den App-Namen in das Suchfeld ein und klicken Sie auf **Suchen**.

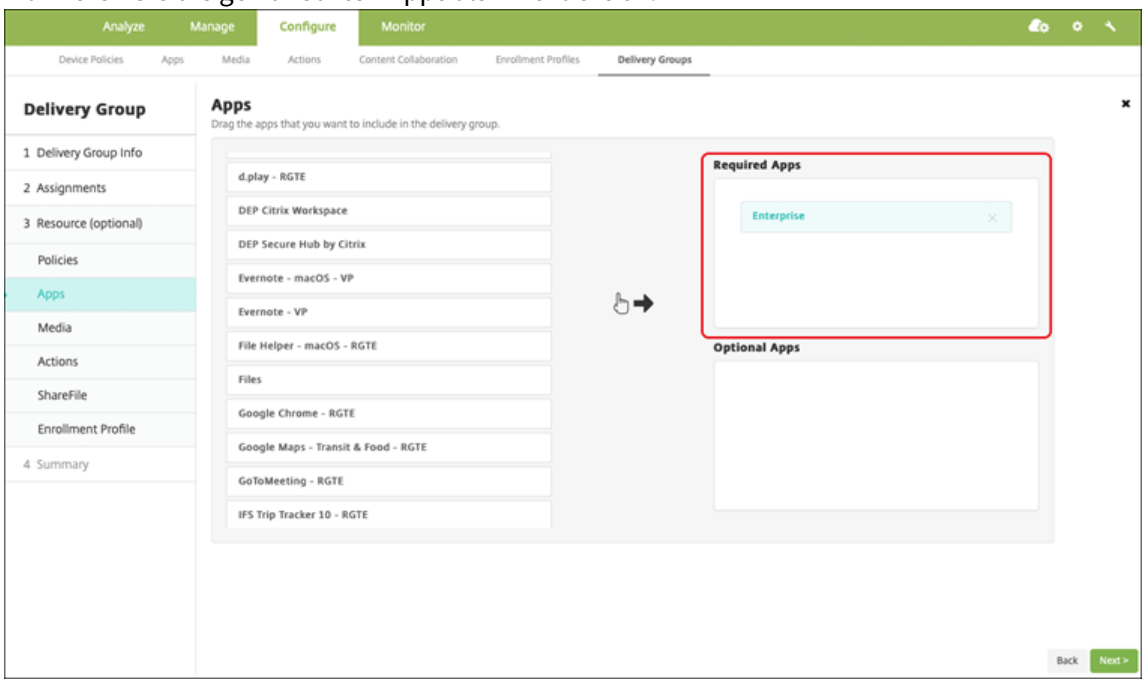


5. Es werden die Apps angezeigt, die den Suchkriterien entsprechen. Klicken Sie auf die gewünschte App.
6. Weisen Sie der App eine Bereitstellungsgruppe zu und klicken Sie auf **Speichern**.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**.
2. Wählen Sie die zu konfigurierende App aus und klicken Sie auf **Bearbeiten**.
3. Citrix empfiehlt, das Feature **Verwaltung der App erzwingen** zu aktivieren.
4. Weisen Sie eine oder mehrere Bereitstellungsgruppen zu und klicken Sie auf **Speichern**.

5. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen > Apps**.
6. Markieren Sie die gewünschten Apps als **Erforderlich**.



7. Gehen Sie zurück zu **Konfigurieren > Bereitstellungsgruppen**.
8. Wählen Sie die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.
9. Benutzer werden aufgefordert, die App zu installieren. Sobald sie dies akzeptieren, wird die App im Hintergrund installiert.

Apps aus öffentlichem App-Store, bereitgestellt mit Apple Volume Purchase

Sie können iOS/iPadOS-App-Lizenzen über das Apple-Programm für Volumenlizenzen (Apple Volume Purchase) verwalten. Führen Sie folgende Schritte aus, um Volume Purchase-Apps zu XenMobile hinzuzufügen.

Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Ja
Verfügbar auf	iOS/iPadOS/macOS

Schritt 1: Verknüpfen von Konten

1. Registrieren Sie sich bei Apple Business Manager (ABM) oder Apple School Manager (ASM). Weitere Informationen zu diesen Programmen finden Sie in der Dokumentation von Apple.
2. Verknüpfen Sie Ihr ABM/ASM-Konto mit XenMobile. Weitere Informationen zum Verknüpfen von Volume Purchase-Konten finden Sie unter Apple Volume Purchase.
3. Aktivieren Sie beim Hinzufügen des Volume Purchase-Kontos die Funktion **Automatische App-**

Updates. Damit wird sichergestellt, dass Apps auf Benutzergeräten automatisch aktualisiert werden, wenn ein Update im Apple Store erscheint.

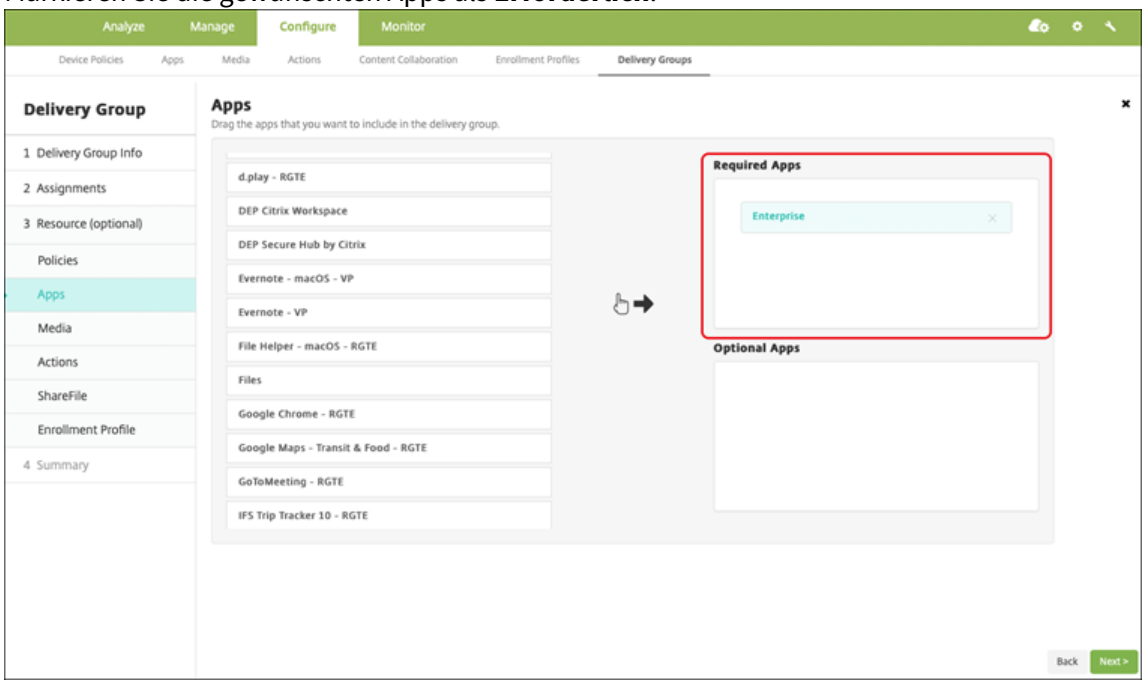
Schritt 2: Abrufen von Apps und Lizenzen von Apple

Fügen Sie Apps zu Ihrem ABM/ASM-Konto hinzu. Sie können Apps hinzufügen, die Sie im Apple App Store oder in Apple Books erworben haben (nur iOS/iPadOS). Denken Sie daran, dass Sie alle Apps kaufen müssen, auch wenn diese kostenlos sind.

Informationen dazu, wie Sie Apps in Ihrem Unternehmen zur Verfügung stellen, finden Sie in der Dokumentation von Apple.

Schritt 3: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**.
2. Wählen Sie die zu konfigurierende Volume Purchase-App aus und klicken Sie auf **Bearbeiten**.
3. Wählen Sie als Plattform **iPhone**, **iPad** oder **macOS**.
4. Citrix empfiehlt, das Feature **Verwaltung der App erzwingen** (nur iOS/iPadOS) zu aktivieren.
5. Weisen Sie eine oder mehrere Bereitstellungsgruppen zu und klicken Sie auf **Speichern**.
6. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen > Apps**.
7. Markieren Sie die gewünschten Apps als **Erforderlich**.



8. Gehen Sie zurück zu **Konfigurieren > Bereitstellungsgruppen**.
9. Wählen Sie die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.
10. Benutzer werden aufgefordert, die App zu installieren. Sobald sie dies akzeptieren, wird die App im Hintergrund installiert.

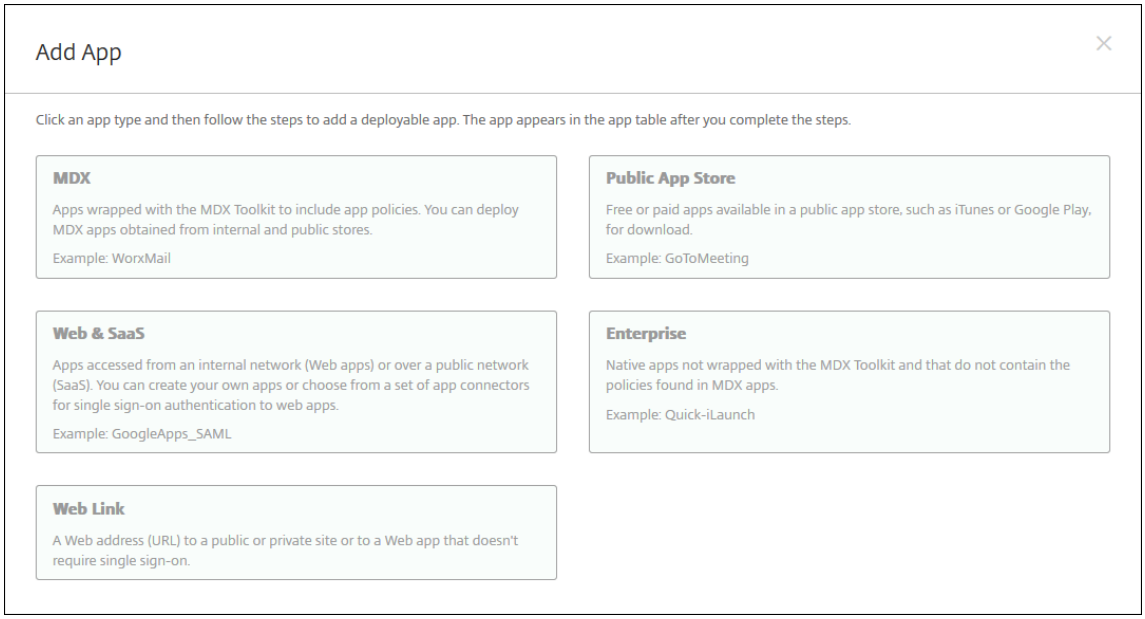
Unternehmensapps

Sie können auch native Apps hinzufügen, denen keine MDX-Richtlinien zugeordnet wurden. Führen Sie folgende Schritte aus, um Apps hinzuzufügen, die nicht im App-Store vorhanden sind.

Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Ja
OS	iOS/iPadOS/macOS

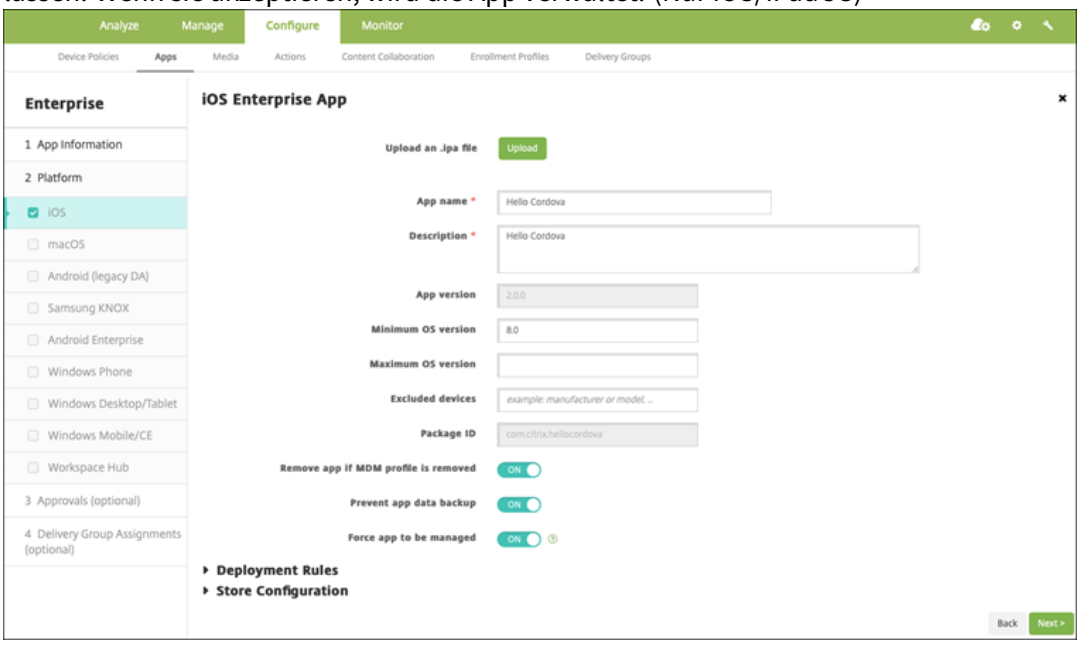
Schritt 1: Hinzufügen und Konfigurieren von Apps

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **Enterprise**.



3. Konfigurieren Sie Folgendes auf der Seite **App-Informationen**:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name” in der Tabelle “Apps” 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.
4. Klicken Sie auf **Weiter**. Die Seite **Plattform** wird angezeigt.
5. Wählen Sie als Plattform **iPhone**, **iPad** oder **macOS**.
6. Hochladen der IPA-Datei (iOS/iPadOS) bzw. der PKG-Datei (macOS)
7. Klicken Sie auf **Weiter**. Die Seite mit den **App-Details** wird angezeigt.
8. Konfigurieren Sie folgende Einstellungen:
   - **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 optional die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
   - **OS-Version (Maximum):** Geben Sie optional 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. Die Standardeinstellung ist “EIN” (nur iOS/iPadOS).
   - **App-Datenbackup verhindern:** Wählen Sie aus, ob die App Daten sichern können soll. Die Standardeinstellung ist “EIN” (nur iOS/iPadOS).

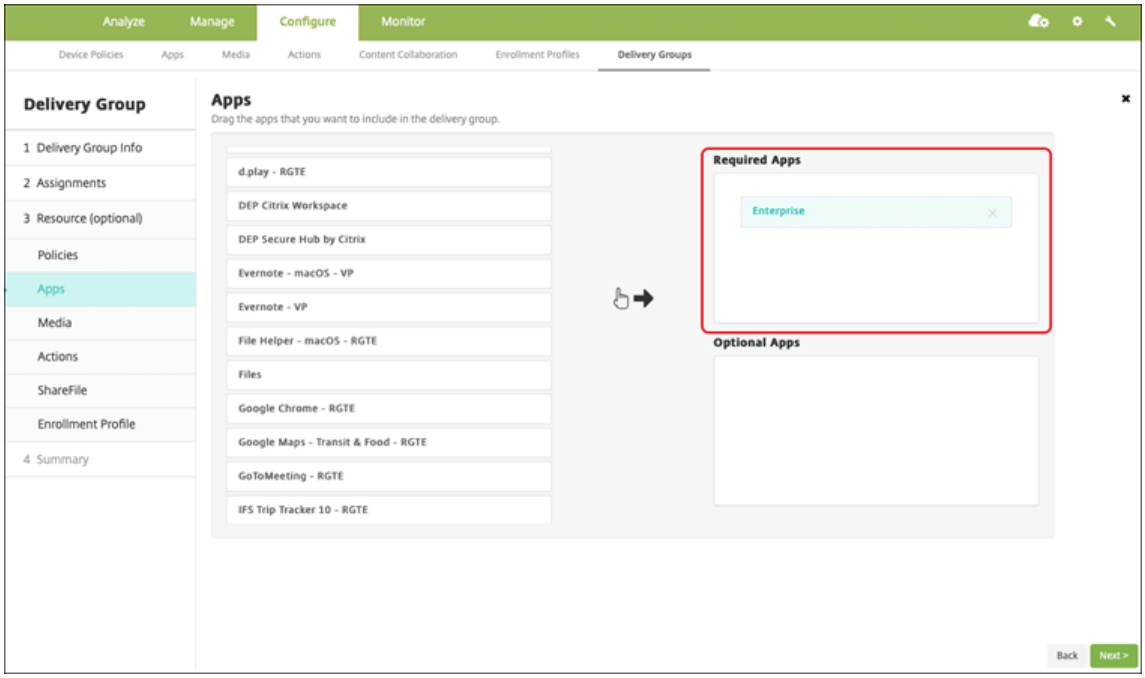
- **Verwaltung der App erzwingen:** Wenn Sie eine nicht verwaltete App installieren, wählen Sie **Ein**, um Benutzer nicht betreuter Geräte aufzufordern, die Verwaltung der App zuzulassen. Wenn sie akzeptieren, wird die App verwaltet. (Nur iOS/iPadOS)



9. Weisen Sie der App eine Bereitstellungsgruppe zu und klicken Sie auf **Speichern**.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Bereitstellungsgruppen**. Wählen Sie die zu konfigurierende Bereitstellungsgruppe aus und klicken Sie auf die Seite **Apps**.
2. Markieren Sie die gewünschten Apps als **Erforderlich**.



3. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen**.
4. Wählen Sie die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.
5. Benutzer werden aufgefordert, die App zu installieren. Sobald sie dies akzeptieren, wird die App im Hintergrund installiert.

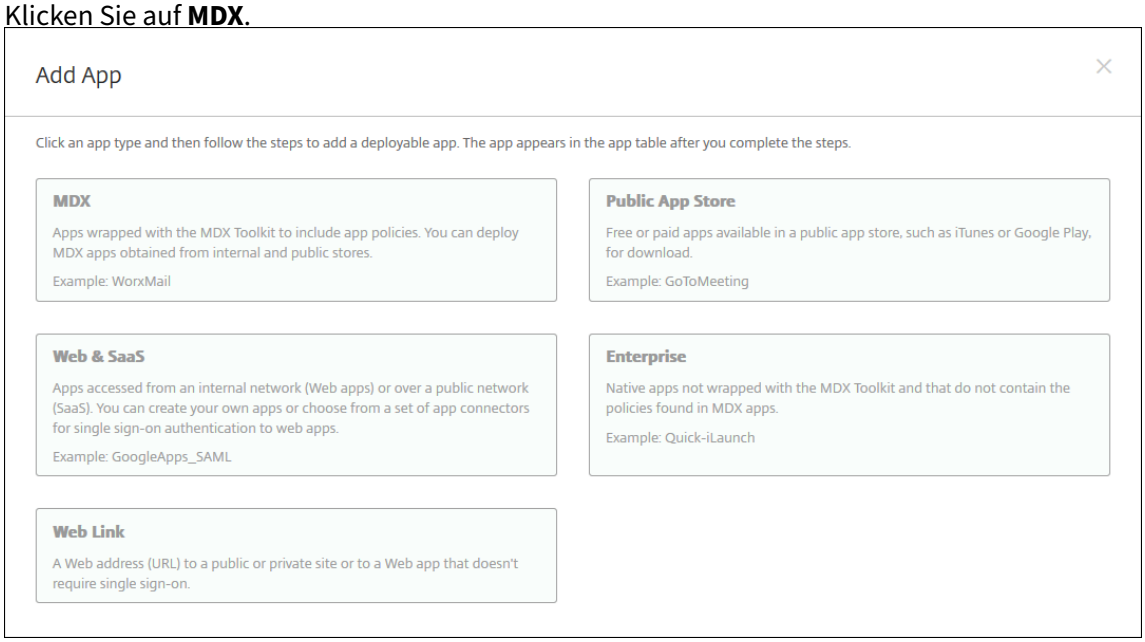
MDX-Apps

Um MDX-bezogene Richtlinien und Sicherheitsfunktionen zu verwenden, fügen Sie MAM-SDK-fähige Apps oder Apps, die mit MDX umschlossen wurden, hinzu. Sie können MDX-Apps mit oder ohne Volume Purchase bereitstellen.

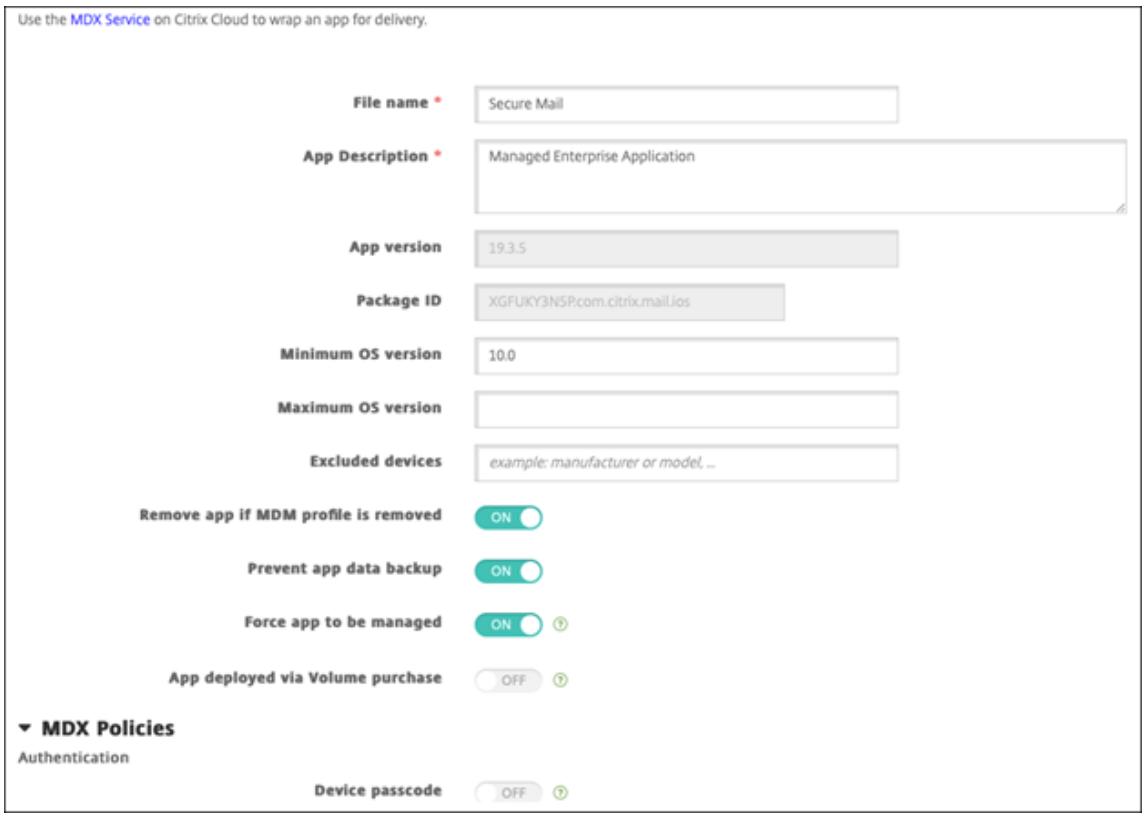
Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Ja
Verfügbar unter	iOS/iPadOS

Schritt 1: Hinzufügen und Konfigurieren von Apps

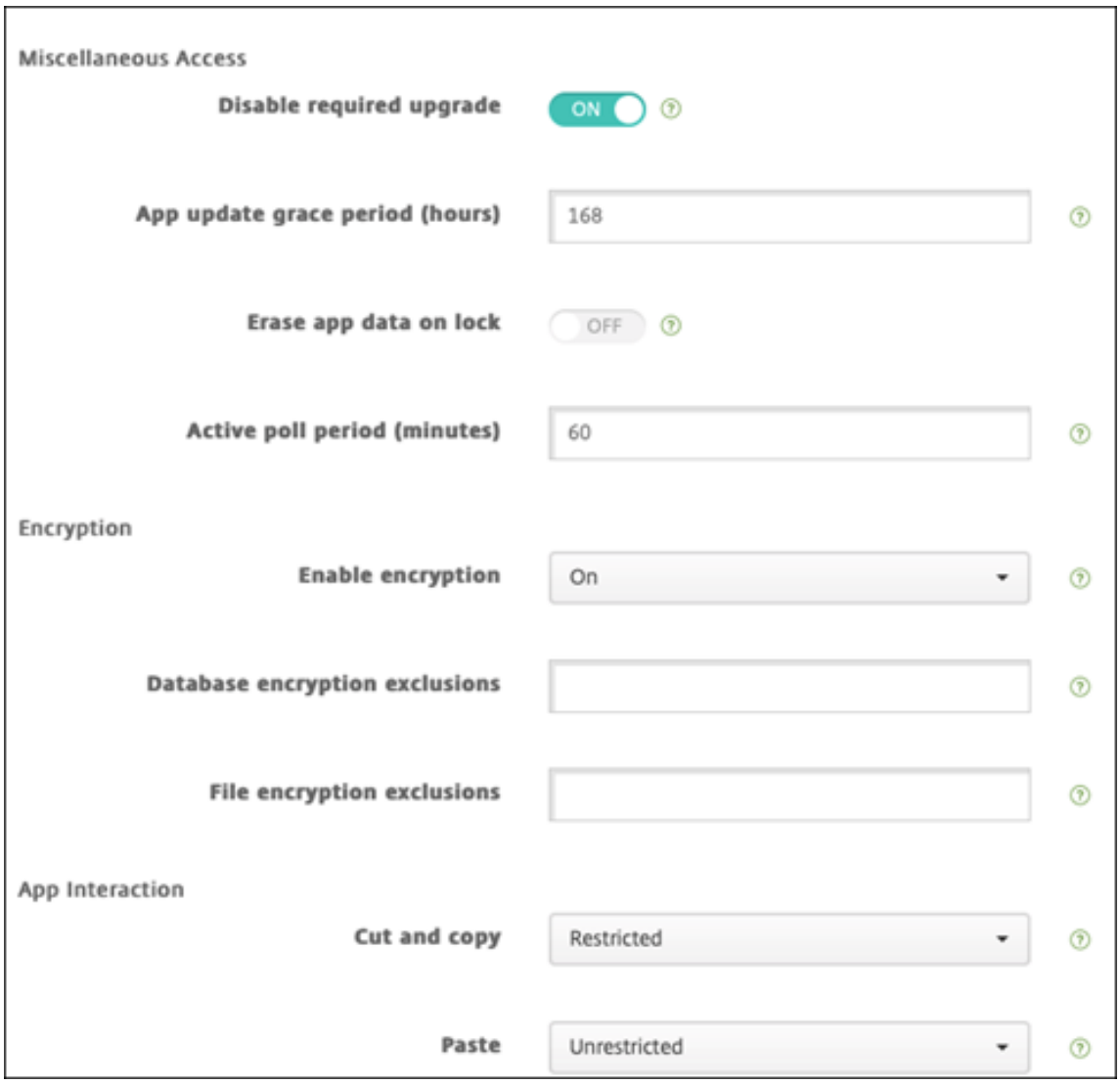
1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **MDX**.



3. Wählen Sie als Plattform **iPhone** oder **iPad**.
4. Laden Sie die MDX-Datei hoch.
5. Konfigurieren Sie die App-Details. Wählen Sie für **App wird per Volume Purchase bereitgestellt** die Einstellung **Aus**. Citrix empfiehlt außerdem, das Feature **Verwaltung der App erzwingen** zu aktivieren.



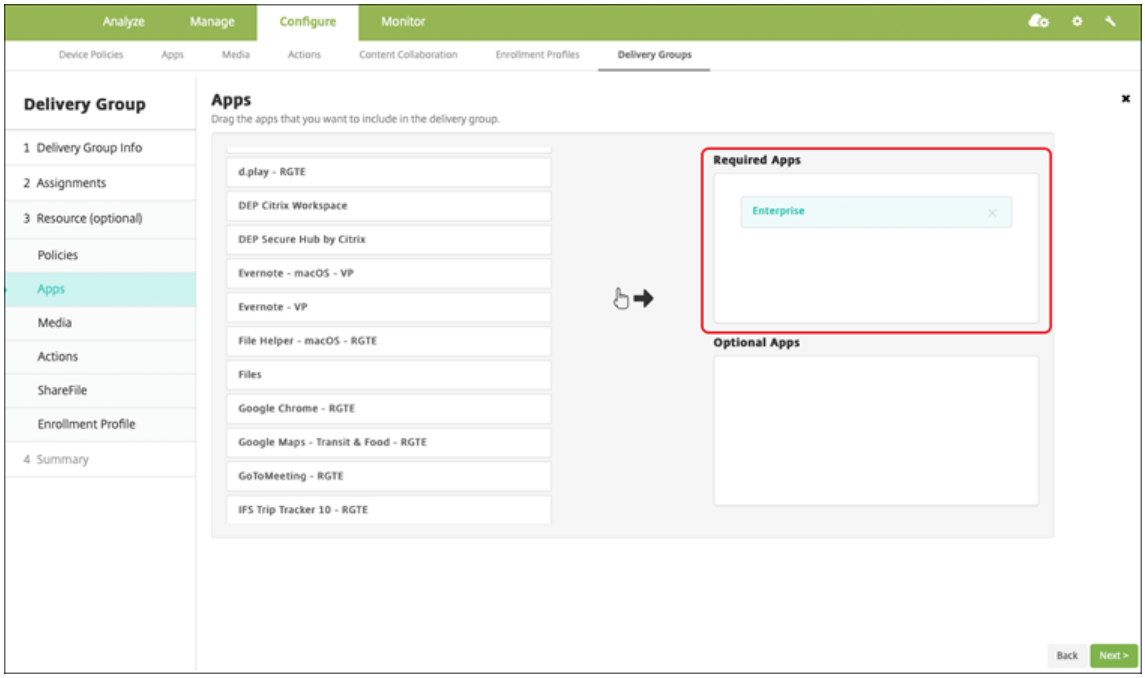
6. Konfigurieren Sie die MDX-Richtlinien. Wählen Sie für **Erforderliches Upgrade deaktivieren** die Einstellung **Ein**.



7. Weisen Sie der App eine Bereitstellungsgruppe zu und klicken Sie auf **Speichern**.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Bereitstellungsgruppen > Apps**.
2. Markieren Sie die gewünschten Apps als **Erforderlich**.



3. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen**.
4. Wählen Sie die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.
5. Benutzer werden aufgefordert, die App zu installieren. Sobald sie dies akzeptieren, wird die App im Hintergrund installiert.

MDX-Apps, die mit Apple Volume Purchase verteilt werden

Um MDX-bezogene Richtlinien und Sicherheitsfunktionen zu verwenden, fügen Sie MAM-SDK-fähige Apps oder Apps, die mit MDX umschlossen wurden, hinzu. Um Apps mit Volume Purchase bereitzustellen, müssen die Apps im App-Store vorhanden sein.

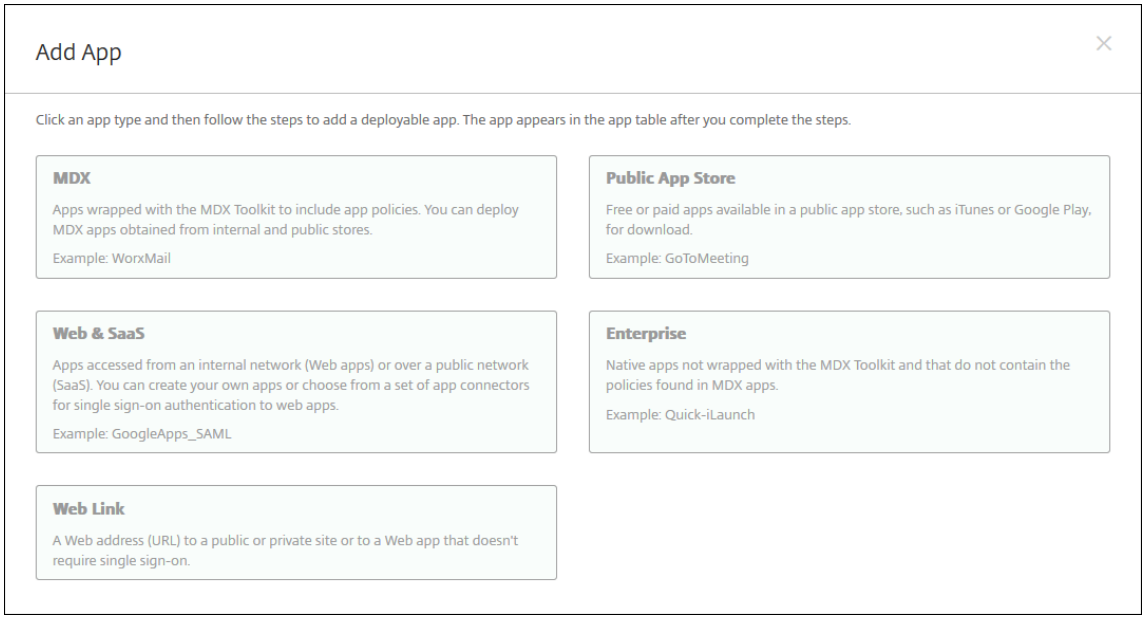
Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Ja
Verfügbar auf	iOS/iPadOS

Schritt 1: Verknüpfen von Konten

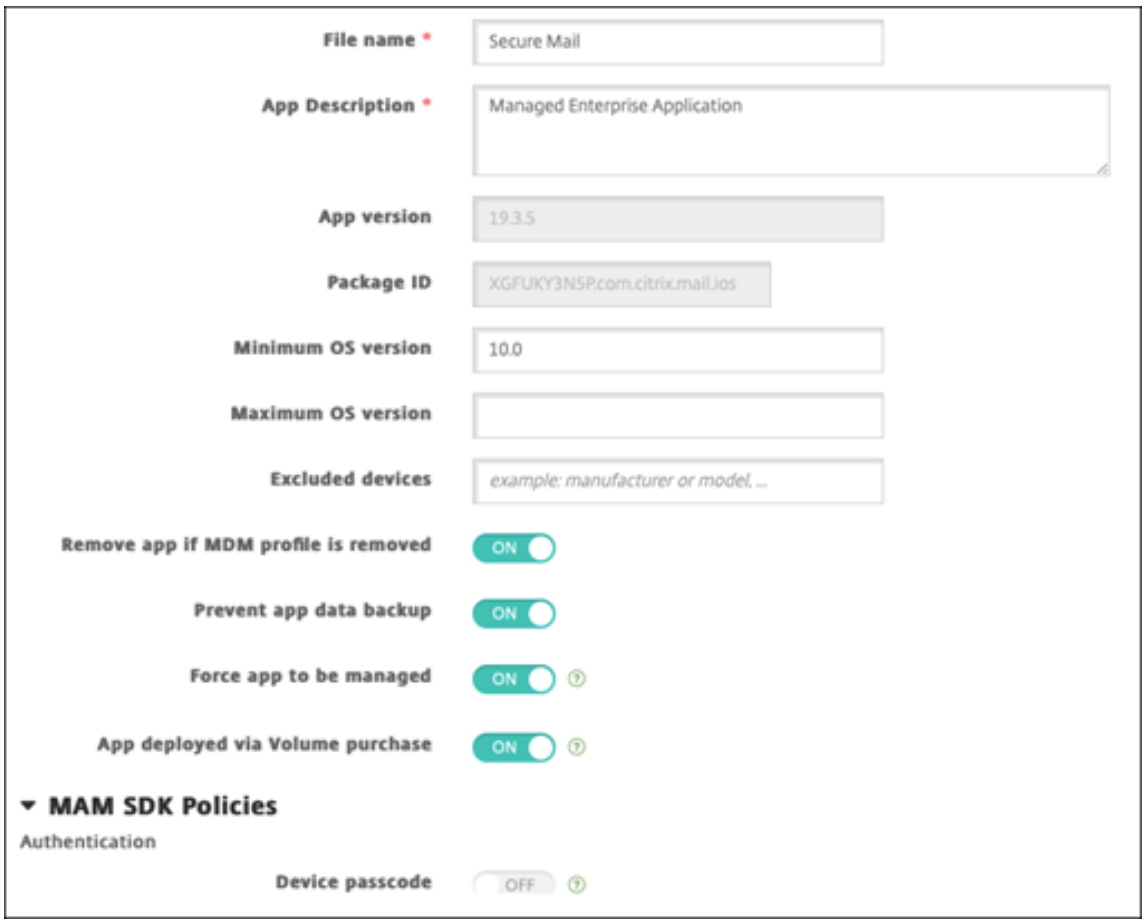
1. Registrieren Sie sich bei Apple Business Manager (ABM) oder Apple School Manager (ASM). Weitere Informationen zu diesen Programmen finden Sie in der Dokumentation von Apple.
2. Verknüpfen Sie Ihr ABM/ASM-Konto mit XenMobile. Weitere Informationen zum Verknüpfen von Volume Purchase-Konten finden Sie unter Apple Volume Purchase.
3. Aktivieren Sie beim Hinzufügen des Volume Purchase-Kontos die Funktion **Automatische App-Updates**. Damit wird sichergestellt, dass Apps auf Benutzergeräten automatisch aktualisiert werden, wenn ein Update im Apple Store erscheint.

Schritt 2: Hinzufügen und Konfigurieren von Apps

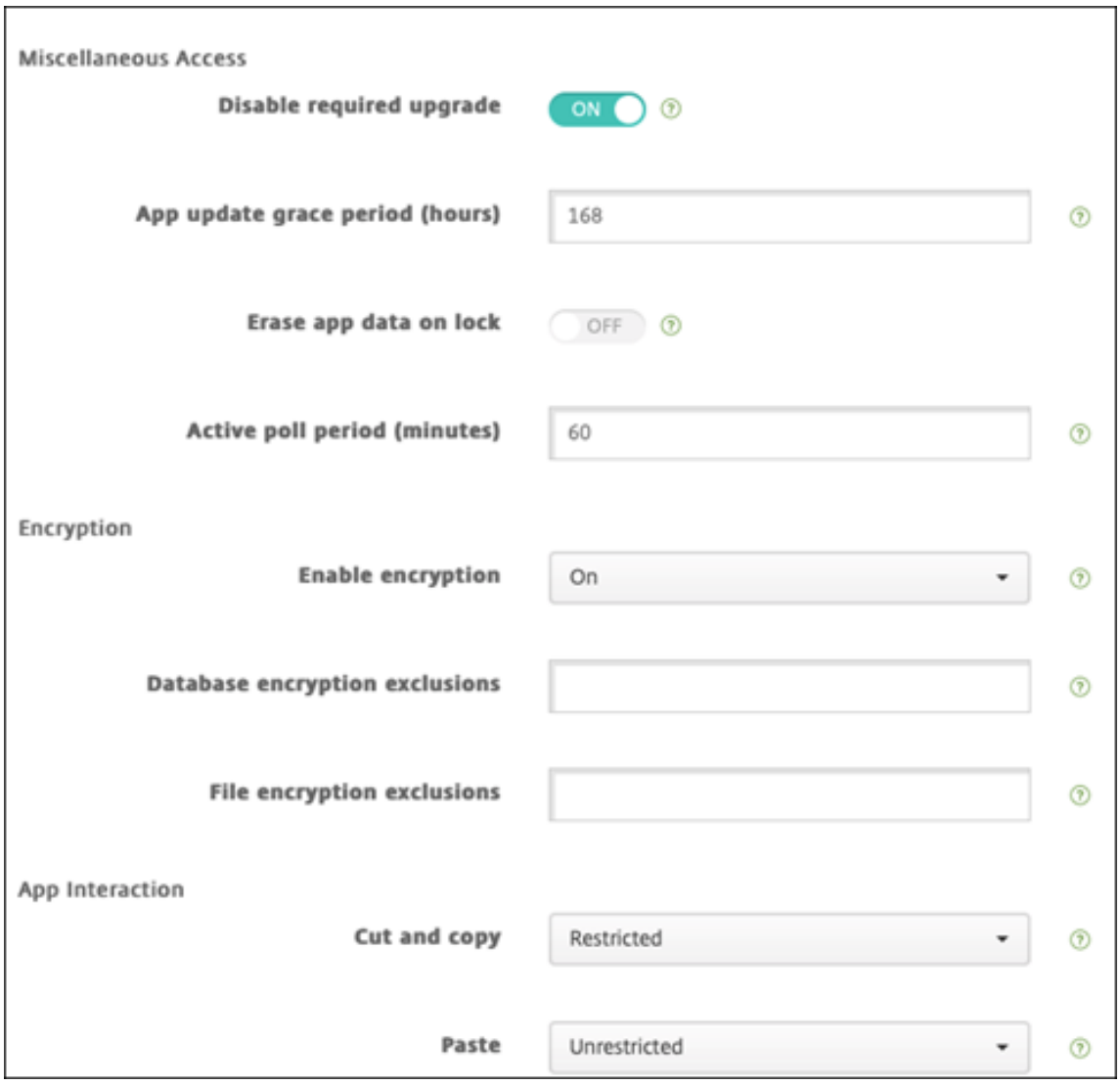
1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **MDX**.



3. Wählen Sie als Plattform **iPhone** oder **iPad**.
4. Laden Sie die MDX-Datei hoch.
5. Konfigurieren Sie die App-Details. Wählen Sie für **App wird per Volume Purchase bereitgestellt** die Einstellung **Ein**. Citrix empfiehlt außerdem, das Feature **Verwaltung der App erzwingen** zu aktivieren.



6. Konfigurieren Sie die MDX-Richtlinien. Wählen Sie für **Erforderliches Upgrade deaktivieren** die Einstellung **Ein**.

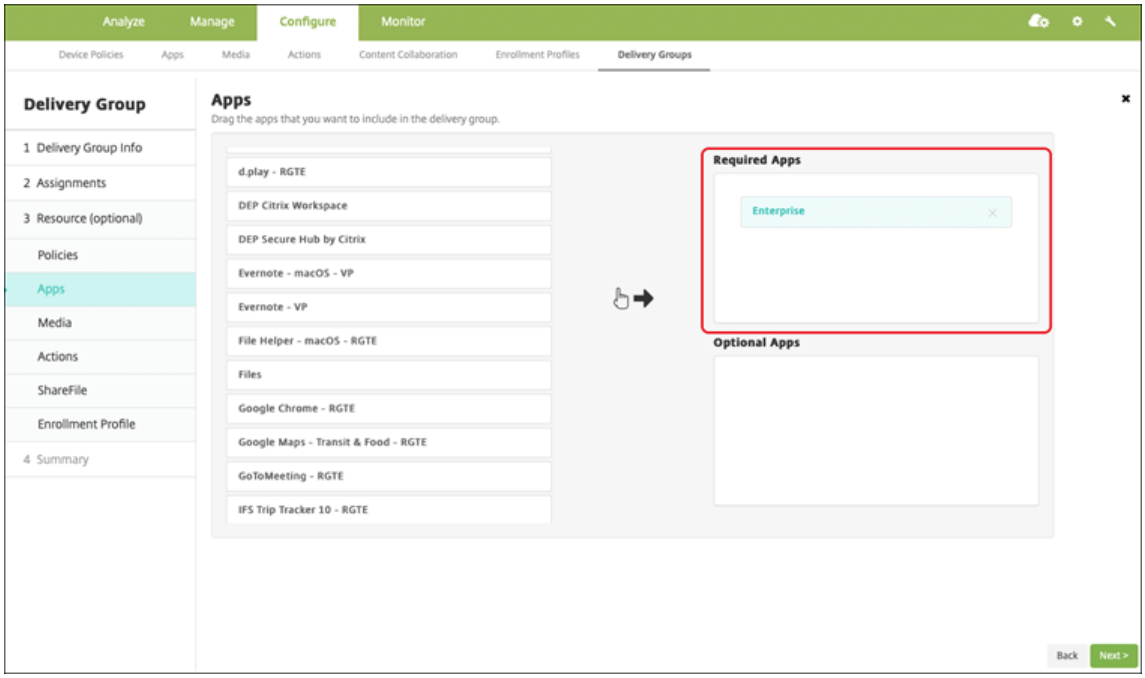


7. Weisen Sie der App eine Bereitstellungsgruppe für jede Plattform zu und klicken Sie auf **Speichern**.

Diese Konfiguration führt zu zwei Einträgen für diese App in der App-Liste. Wenn Sie eine zu konfigurierende App auswählen, wählen Sie eine App vom **Typ MDX** aus.

Schritt 3: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Bereitstellungsgruppen > Apps**.
2. Markieren Sie die gewünschten Volume Purchase-Apps als **Erforderlich**.



3. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen**.
4. Wählen Sie die Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.
5. Benutzer werden aufgefordert, die App zu installieren. Sobald sie dies akzeptieren, wird die App im Hintergrund installiert.

Benutzerdefinierte Apps

Benutzerdefinierte Apps sind proprietäre Business-to-Business-Apps. Mit XenMobile und Apple Volume Purchase können Sie proprietäre Apps privat und sicher verteilen. Sie können die Apps an Partner, Kunden, Franchisenehmer und interne Mitarbeiter verteilen.

Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Ja
Verfügbar auf	iOS/iPadOS

Anforderungen für benutzerdefinierte Apps

- Apple Business Manager- oder Apple School Manager-Konto
- Apple Volume Purchase-Konto (Geräte mit iOS 7 oder höher erforderlich)
- Registrieren Sie Geräte in XenMobile über einen der folgenden Apple-Registrierungsmodi:
  - Automatisierte Geräteregistrierung
  - Geräteregistrierung
  - Benutzerregistrierung

Schritt 1: Verknüpfen von Konten

Um benutzerdefinierte Apps mithilfe von Volume Purchase bereitzustellen, verknüpfen Sie Ihr Volume Purchase-Konto mit XenMobile.

1. Registrieren Sie sich bei Apple Business Manager (ABM). Weitere Informationen zu diesen Programmen finden Sie in der Dokumentation von Apple.
2. Verknüpfen Sie Ihr ABM-Konto mit XenMobile. Weitere Informationen zum Verknüpfen von Volume Purchase-Konten finden Sie unter Apple Volume Purchase.
3. Aktivieren Sie beim Hinzufügen des Volume Purchase-Kontos die Funktion **Automatische App-Updates**. Damit wird sichergestellt, dass Apps auf Benutzergeräten automatisch aktualisiert werden, wenn ein Update im Apple Store erscheint.

Schritt 2: Konfigurieren von Apps in ABM

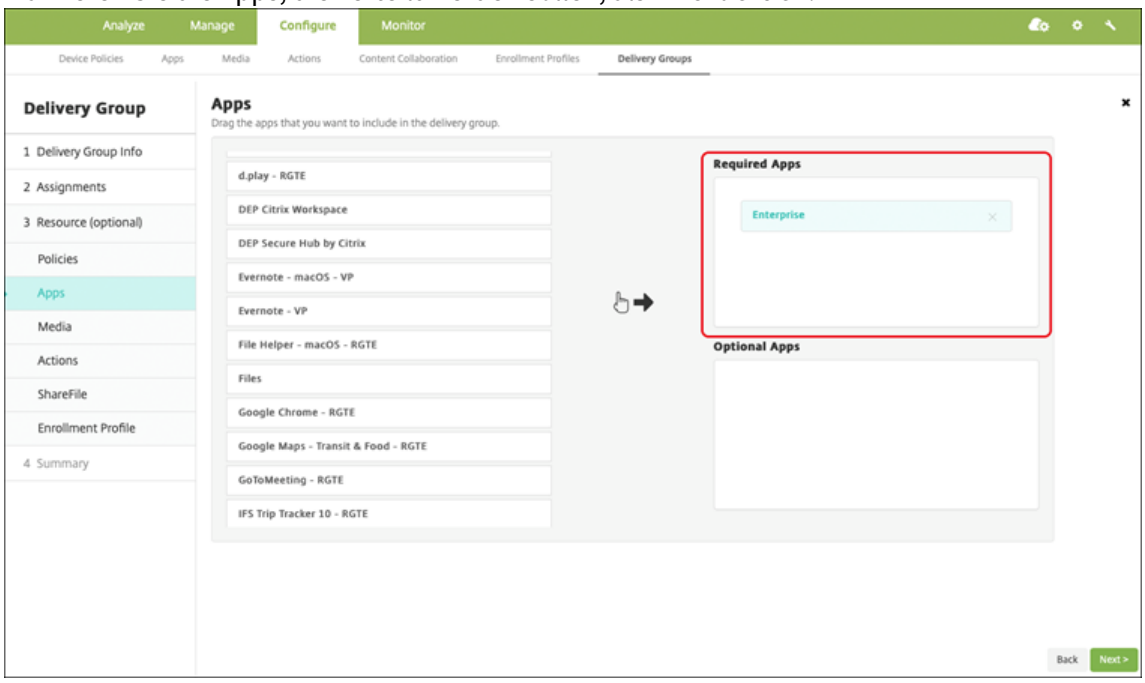
Fügen Sie Apps in Ihrem ABM-Konto hinzu. Sie können eigene benutzerdefinierte Apps hochladen und verteilen oder Lizenzen für benutzerdefinierte Apps anderer Organisationen erwerben. Weitere Informationen zum Hinzufügen und Aktivieren benutzerdefinierter Apps in ABM finden Sie in der Dokumentation von Apple.

Schritt 3: Hinzufügen und Konfigurieren von Apps in XenMobile

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**. Volume Purchase-Apps werden in der Liste der Apps angezeigt.
2. Wählen Sie die App aus, die Sie konfigurieren möchten. Klicken Sie auf **Edit**.
3. Wählen Sie als Plattform **iPhone**, **iPad** oder **macOS**.
4. Wählen Sie die Bereitstellungsgruppen aus, an die die App verteilt werden soll. Klicken Sie auf **Speichern**.

Schritt 4: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Bereitstellungsgruppen > Apps**.
2. Markieren Sie die Apps, die verteilt werden sollen, als **Erforderlich**.



3. Gehen Sie zurück zu **Konfigurieren > Bereitstellungsgruppen**.
4. Wählen Sie die gewünschte Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.
5. Benutzer erhalten eine Anforderung zum Bereitstellen von Apps. Apps werden im Hintergrund installiert, nachdem Benutzer sie akzeptiert haben.

MDX-fähige benutzerdefinierte Apps

Um MDX-bezogene Richtlinien und Sicherheitsfunktionen zu verwenden, fügen Sie benutzerdefinierte Apps hinzu, die MAM-SDK-fähig sind oder mit MDX umschlossen wurden.

Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Ja
Verfügbar auf	iOS/iPadOS

Schritt 1: Verknüpfen von Konten

Um benutzerdefinierte Apps mithilfe von Volume Purchase bereitzustellen, verknüpfen Sie Ihr Volume Purchase-Konto mit XenMobile.

1. Registrieren Sie sich bei Apple Business Manager (ABM). Weitere Informationen zu diesen Programmen finden Sie in der Dokumentation von Apple.
2. Verknüpfen Sie Ihr ABM-Konto mit XenMobile. Weitere Informationen zum Verknüpfen von Volume Purchase-Konten finden Sie unter Apple Volume Purchase.

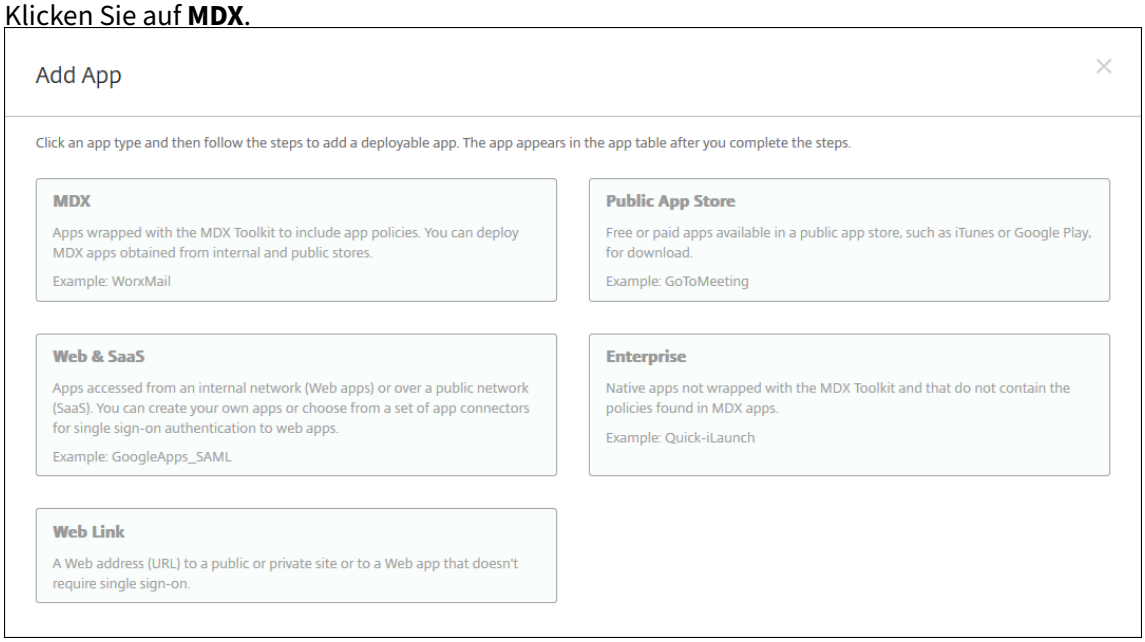
3. Aktivieren Sie beim Hinzufügen des Volume Purchase-Kontos die Funktion **Automatische App-Updates**. Damit wird sichergestellt, dass Apps auf Benutzergeräten automatisch aktualisiert werden, wenn ein Update im Apple Store erscheint.

Schritt 2: Konfigurieren von Apps in ABM

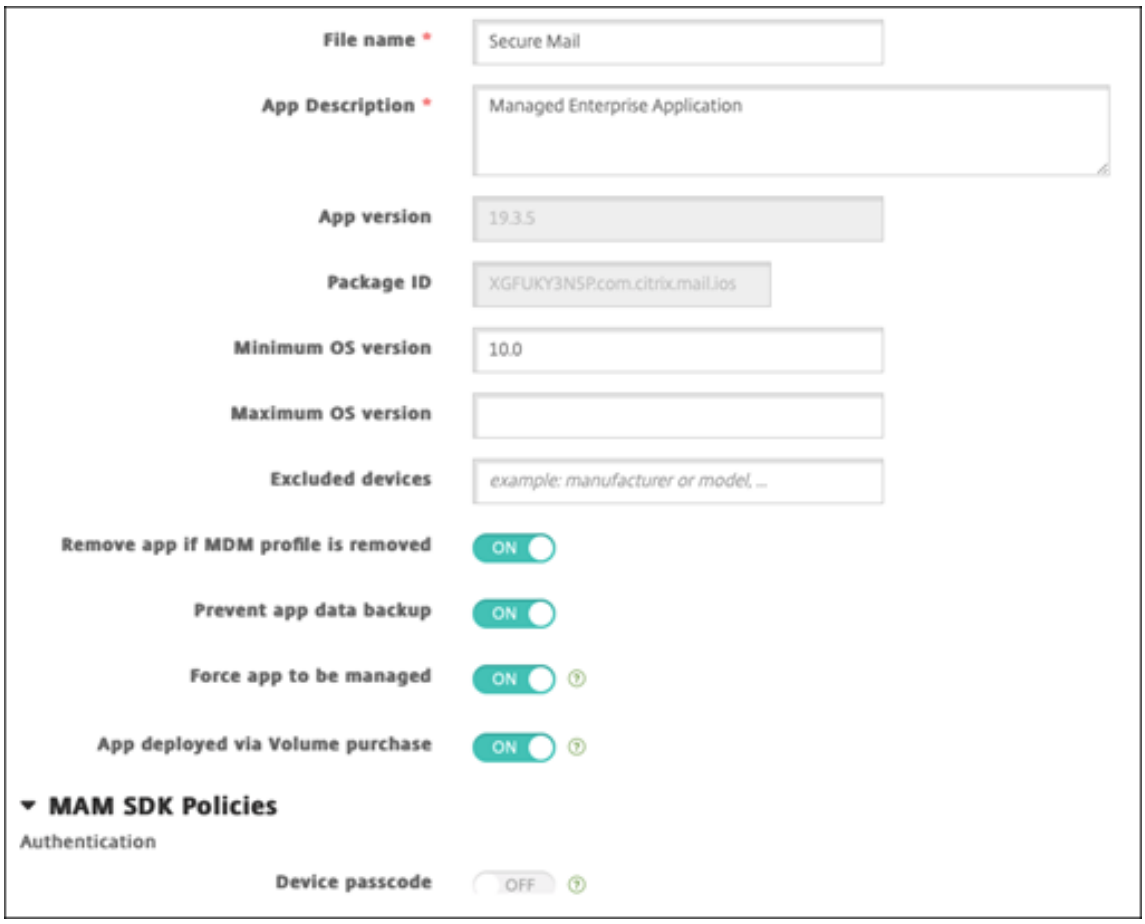
Fügen Sie Apps in Ihrem ABM-Konto hinzu. Sie können eigene benutzerdefinierte Apps hochladen und verteilen oder Lizenzen für benutzerdefinierte Apps anderer Organisationen erwerben. Weitere Informationen zum Hinzufügen und Aktivieren benutzerdefinierter Apps in ABM finden Sie in der Dokumentation von Apple.

Schritt 3: Hinzufügen und Konfigurieren von Apps in XenMobile

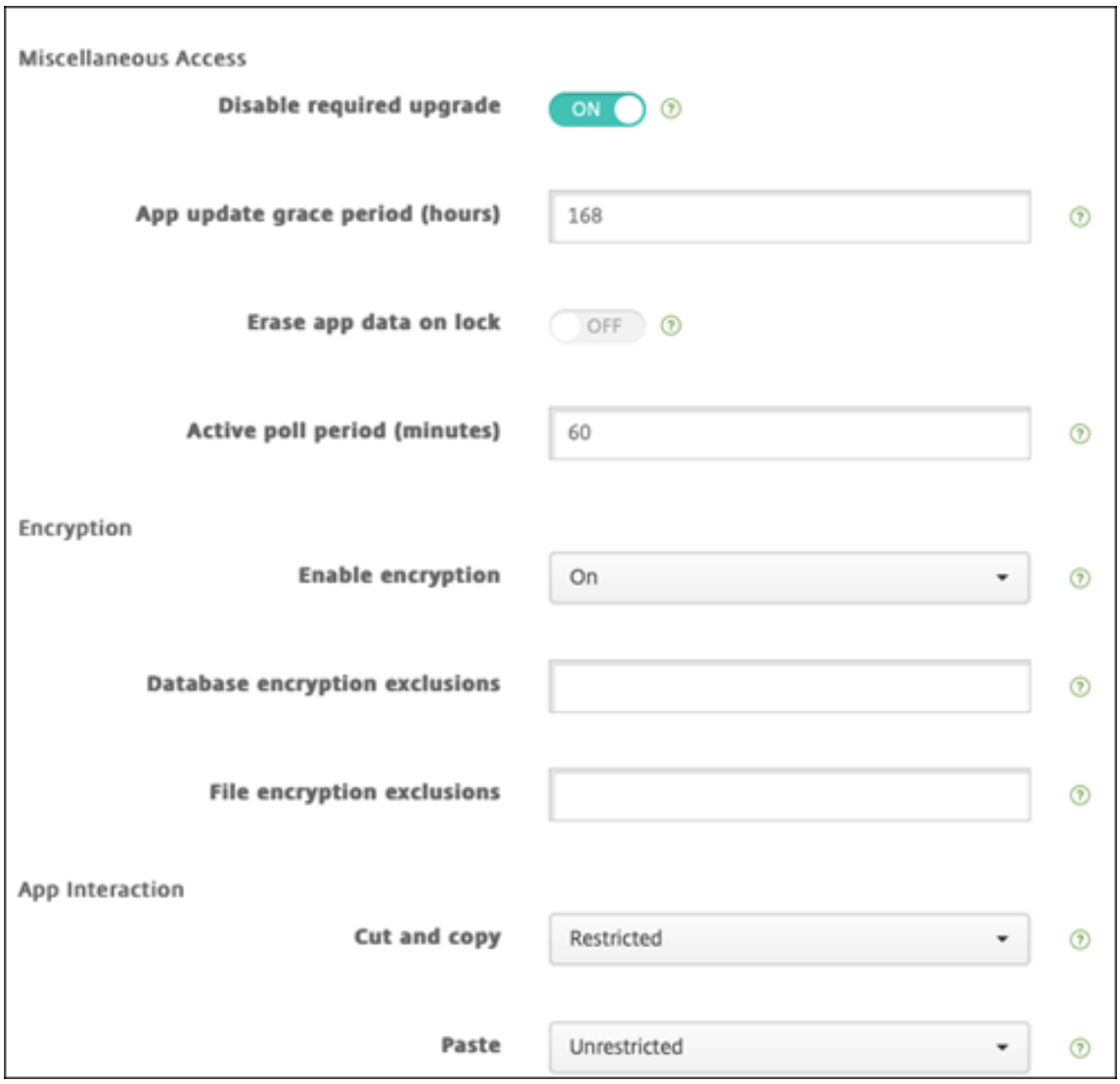
1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **MDX**.



3. Wählen Sie als Plattform **iPhone** oder **iPad**.
4. Laden Sie die MDX-Datei für die hinzuzufügende App hoch.
5. Konfigurieren Sie die App-Details. Wählen Sie für **App wird per Volume Purchase bereitgestellt** die Einstellung **Ein**. Citrix empfiehlt außerdem, das Feature **Verwaltung der App erzwingen** zu aktivieren.



6. Konfigurieren Sie die MDX-Richtlinien. Wählen Sie für **Erforderliches Upgrade deaktivieren** die Einstellung **Ein**.

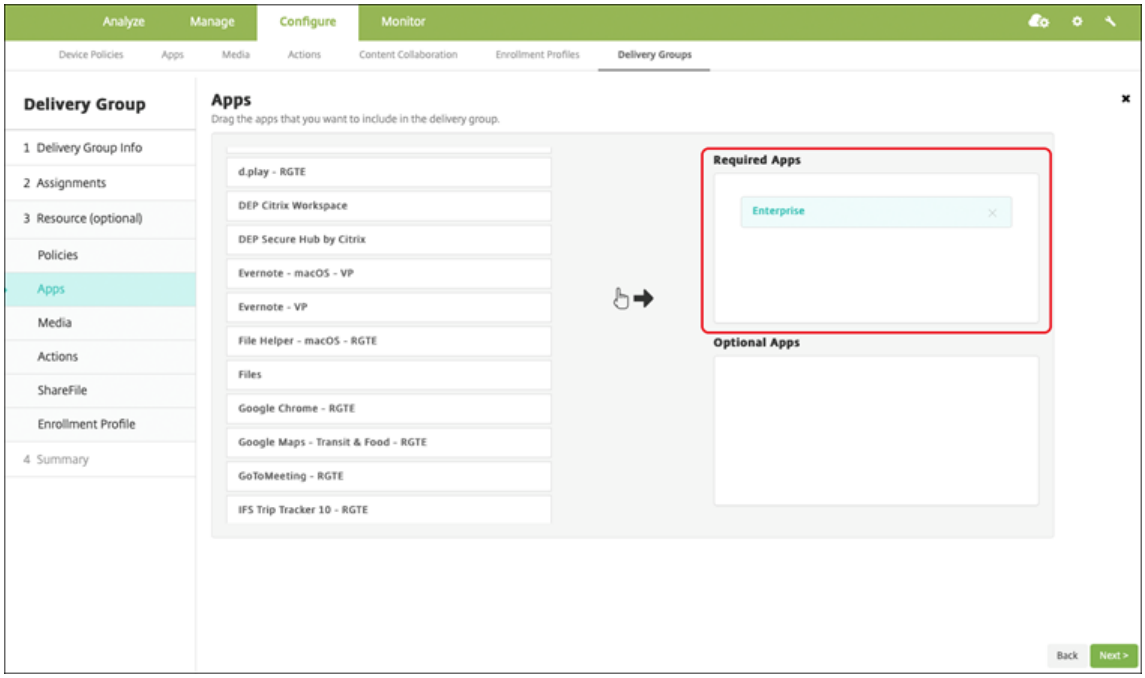


7. Weisen Sie der App eine Bereitstellungsgruppe zu und klicken Sie auf **Speichern**.

Diese Konfiguration führt zu zwei Einträgen für diese App in der App-Liste. Wenn Sie eine zu konfigurierende App auswählen, wählen Sie eine App vom **Typ MDX** aus.

Schritt 4: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps**. Volume Purchase-Apps werden in der Liste der Apps angezeigt.
2. Wählen Sie die App aus, die Sie konfigurieren möchten. Klicken Sie auf **Edit**.
3. Wählen Sie die Bereitstellungsgruppen aus, an die die App auf jeder Plattform verteilt werden soll. Klicken Sie auf **Speichern**.
4. Gehen Sie zurück zu **Konfigurieren > Bereitstellungsgruppen > Apps**.
5. Markieren Sie die Apps, die verteilt werden sollen, als **Erforderlich**.



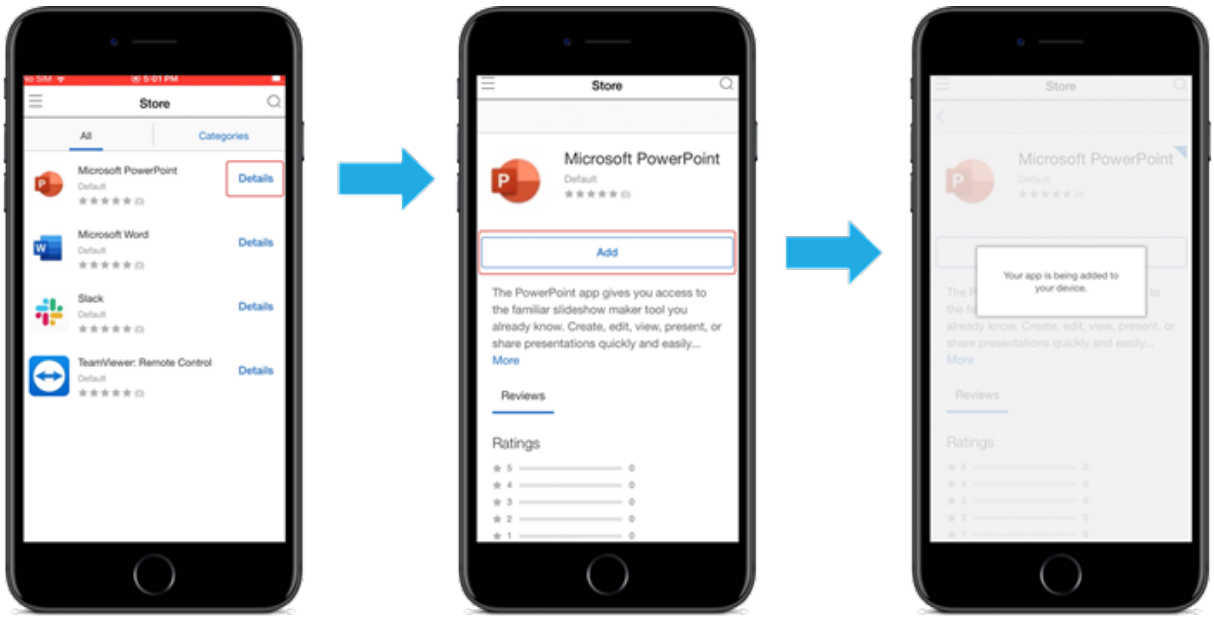
6. Gehen Sie zurück zu **Konfigurieren > Bereitstellungsgruppen**.
7. Wählen Sie die gewünschte Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.
8. Benutzer erhalten eine Anforderung zum Bereitstellen von Apps. Apps werden im Hintergrund installiert, nachdem sie akzeptiert wurden.

Optionale Apps (nur iOS/iPadOS)

Citrix empfiehlt, Apps als **Erforderlich** bereitzustellen. Erforderliche Apps werden automatisch auf Benutzergeräten installiert, wodurch die Interaktion minimiert wird. Wenn dieses Feature aktiviert ist, können Apps auch automatisch aktualisiert werden.

Optionale Apps ermöglichen Benutzern die Auswahl der zu installierenden Apps. Benutzer müssen die Installation jedoch manuell über Secure Hub initiieren.

Zu Installation optionaler Apps müssen Benutzer Secure Hub starten, den **Store** aufrufen, die **Details** für die gewünschte App auswählen und auf **Hinzufügen** klicken.



Netzwerkzugriffssteuerung (NAC)

January 5, 2022

Sie können mit Ihrer NAC-Lösung (Network Access Control, NAC) die Bewertung der Gerätesicherheit durch Endpoint Management für Android- und Apple-Geräte erweitern. Die NAC-Lösung nutzt die XenMobile-Sicherheitsbewertung, um Authentifizierungsentscheidungen zu erleichtern. Nach dem Konfigurieren des NAC-Geräts werden die in XenMobile konfigurierten Geräterichtlinien und NAC-Filter erzwungen.

Die Verwendung von XenMobile mit einer NAC-Lösung ermöglicht QoS und eine gezieltere Steuerung für Geräte innerhalb Ihres Netzwerks. Eine Zusammenfassung der Vorteile einer Integration von NAC mit XenMobile finden Sie unter Zugriffssteuerung.

Citrix unterstützt die folgenden Lösungen für die Integration mit XenMobile:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix übernimmt keine Gewährleistung für die Integration anderer NAC-Lösungen.

Bei vorhandenem NAC-Gerät in Ihrem Netzwerk:

- XenMobile unterstützt NAC als Endpunktsicherheitsfeature für Geräte mit iOS, Android Enterprise und Android.
- Sie können Filter in XenMobile aktivieren, um Geräte anhand von Regeln oder Eigenschaften als (nicht) richtlinientreu für NAC festzulegen. Beispiel:
  - Wenn ein verwaltetes Gerät in XenMobile nicht die vorgegebenen Kriterien erfüllt, wird es als nicht richtlinientreu eingestuft. Ein NAC-Gerät blockiert dann nicht richtlinientreue Geräte in Ihrem Netzwerk.
  - Wenn auf einem verwalteten Gerät in XenMobile nicht richtlinientreue Apps installiert sind, kann ein NAC-Filter die VPN-Verbindung blockieren. Ein nicht richtlinientreues Benutzergerät kann dann nicht über das VPN auf Apps oder Websites zugreifen.
  - Wenn Sie Citrix Gateway für NAC verwenden, können Sie durch Aktivieren von Split-Tunneling verhindern, dass das Citrix Gateway Plug-In unnötigen Netzwerkverkehr an Citrix Gateway sendet. Weitere Informationen zum Split-Tunneling finden Sie unter Konfigurieren von Split-Tunneling.

Unterstützte NAC-Richtlinientreuefilter

XenMobile Server 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. Informationen zu dieser Richtlinie finden Sie unter App-Zugriffsrichtlinien für Geräte.

Inaktive Geräte: Prüft, ob ein Gerät entsprechend dem Wert unter **Inaktivitätsschwellenwert (Tage)** in den **Servereigenschaften** 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 Geräteeigenschaft wird normalerweise von automatisierten Aktionen geändert oder von Drittanbietern, die XenMobile-APIs verwenden.

Widerrufenstatus: Prüft, ob das Gerätezertifikat widerrufen worden ist. Ein widerrufenes Gerät kann erst erneut registriert werden, wenn es wieder autorisiert ist.

Android-Geräte mit Rooting oder iOS-Geräte mit Jailbreak: Prüft, ob auf einem Android- oder iOS-Gerät ein Jailbreak vorliegt.

Nicht verwaltete Geräte: Prüft, ob ein Gerät verwaltet, d. h. von XenMobile kontrolliert wird. Beispielsweise wird ein bei MAM registriertes Gerät 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. Das NAC-Gerät blockiert diese Geräte in Ihrem Netzwerk.

Konfigurationsübersicht

Es wird empfohlen, die NAC-Komponenten in der angegebenen Reihenfolge zu konfigurieren.

1. Konfigurieren von Geräterichtlinien zur Unterstützung von NAC:

   Für iOS-Geräte: Siehe Konfigurieren der VPN-Geräterichtlinie zur Unterstützung von NAC.

   Für Android Enterprise-Geräte: Siehe Erstellen einer verwalteten Android Enterprise-Konfiguration für Citrix SSO.

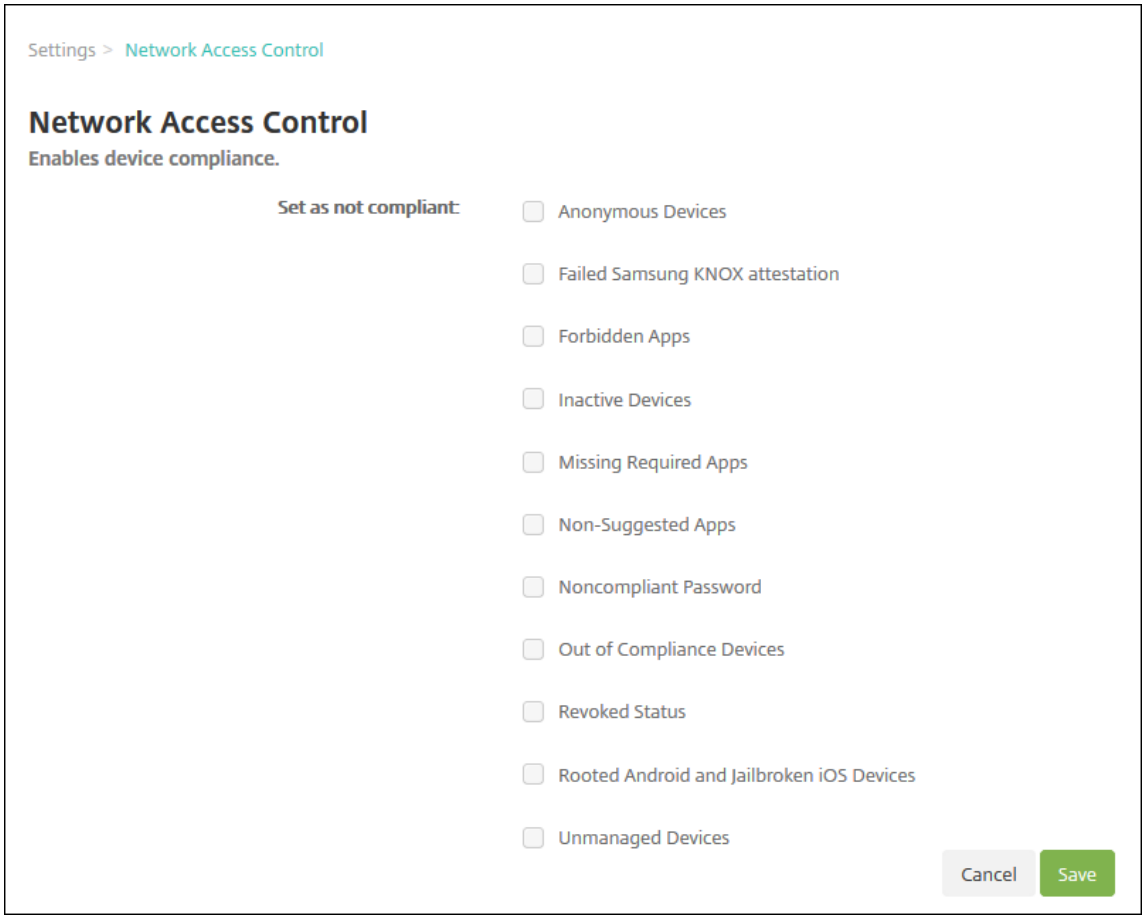
   Für Android-Geräte: Siehe Konfigurieren des Citrix SSO-Protokolls für Android.

2. Aktivieren von NAC-Filtern in XenMobile.
3. Konfigurieren einer NAC-Lösung:
   - Citrix Gateway, beschrieben unter Aktualisieren der Citrix Gateway-Richtlinien zur Unterstützung von NAC

     Erfordert Installation von Citrix SSO auf Geräten. Siehe Citrix Gateway-Clients.
   - Cisco ISE: Siehe Cisco-Dokumentation.
   - ForeScout: Siehe ForeScout-Dokumentation.

Aktivieren von NAC-Filtern in XenMobile

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



2. Aktivieren Sie die Kontrollkästchen für die gewünschten Filter unter **Als nicht richtlinientreu einstellen**.
3. Klicken Sie auf **Speichern**.

Aktualisieren der Citrix Gateway-Richtlinien zur Unterstützung von NAC

Sie müssen Authentifizierungs- und VPN-Sitzungsrichtlinien vom Typ “Advanced” (nicht “Classic”) auf dem virtuellen VPN-Server konfigurieren.

Mit diesen Schritten wird ein Citrix Gateway mit einem der folgenden Merkmale aktualisiert:

- Es ist in eine XenMobile Server-Umgebung integriert.
- Es ist nicht Teil der XenMobile Server-Umgebung, sondern für VPN eingerichtet und kann XenMobile erreichen.

Führen Sie auf dem virtuellen VPN-Server in einem Konsolenfenster die nachfolgend aufgeführten Schritte aus. (Die hier gezeigten IP-Adressen haben Beispielcharakter.)

1. Entfernen Sie alle Richtlinien des Typs “Classic” und heben Sie deren Bindung auf, sofern Sie solche Richtlinien auf Ihrem virtuellen VPN-Server verwenden. Geben Sie Folgendes ein, um dies zu überprüfen:

   ```
   show vpn vserver <VPN_VServer>
   ```

   Entfernen Sie alle Einträge im Ergebnis, die das Wort “Classic” enthalten. Beispiel: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   Geben Sie Folgendes ein, um die Richtlinie zu entfernen:

   ```
   unbind vpn vserver <VPN_VServer> -policy <policy_name>
   ```

2. Erstellen Sie die entsprechende Sitzungsrichtlinie des Typs “Advanced”, indem Sie Folgendes eingeben:

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   Beispiel: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Binden Sie die Richtlinie an den virtuellen VPN-Server, indem Sie Folgendes eingeben:

   ```
   bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100
   ```

4. Erstellen Sie einen virtuellen Authentifizierungsserver, indem Sie Folgendes eingeben:

   ```
   add authentication vserver <authentication vserver name> <service type>
    <ip address>
   ```

   Beispiel: `add authentication vserver authvs SSL 0.0.0.0`
   In dem Beispiel bedeutet `0.0.0.0`, dass der virtuelle Authentifizierungsserver nicht öffentlich ist.

5. Binden Sie ein SSL-Zertifikat an den virtuellen Server, indem Sie Folgendes eingeben:

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver
   certificate>
   ```

   Beispiel: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Ordnen Sie dem virtuellen Authentifizierungsserver ein Authentifizierungsprofil vom virtuellen VPN-Server zu. Erstellen Sie zunächst das Authentifizierungsprofil, indem Sie Folgendes eingeben:

   ```
   add authentication authnProfile <profile name> -authnVsName <authentication
    vserver name>
   ```

   Beispiel:

   ```
   add authentication authnProfile xm_nac_prof -authnVsName authvs
   ```


7. Weisen Sie das Authentifizierungsprofil dem virtuellen VPN-Server zu, indem Sie Folgendes eingeben:

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   Beispiel:

   ```
   set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
   ```

8. Überprüfen Sie die Verbindung von Citrix Gateway zu einem Gerät, indem Sie Folgendes eingeben:

   ```
   curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check --
   header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   Diese Abfrage überprüft beispielsweise die Konnektivität, indem sie den Status der Richtlinientreue für das erste registrierte Gerät in der Umgebung (`deviceid_1`) abruft:

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-
   Citrix-VPN-Device-ID: deviceid_1"
   ```

   Bei Erfolg ähnelt das Ergebnis dem folgenden Beispiel.

   ```
   1 HTTP/1.1 200 OK
   2 < Server: Apache-Coyote/1.1
   3 < X-Citrix-Device-State: Non Compliant
   4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   5 <!--NeedCopy-->
   ```

9. Wenn der vorherige Schritt erfolgreich ist, erstellen Sie die Webauthentifizierungsaktion für XenMobile. Erstellen Sie zuerst einen Richtlinienausdruck zum Extrahieren der Geräte-ID aus dem iOS-VPN-Plug-In. Geben Sie Folgendes ein:

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).
   TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. Senden Sie die Anforderung an XenMobile, indem Sie Folgendes eingeben: In diesem Beispiel ist die XenMobile Server IP `10.207.87.82` und der FQDN ist `example.em.server.com:4443`.

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
     4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "
    Host: example.em.server.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+
    xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.
    RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ
    (\"Compliant\")"
    ```

    Die erfolgreiche Ausgabe für XenMobile NAC lautet `HTTP status 200 OK`. Der Header `X-Citrix-Device-State` muss den Wert `Compliant` haben.

11. Erstellen Sie eine Authentifizierungsrichtlinie, der die Aktion zugeordnet werden soll, indem Sie Folgendes eingeben:

    ```
    add authentication Policy <policy name> -rule <rule> -action <web
    authentication action>
    ```

    Beispiel: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Konvertieren Sie die bestehende LDAP-Richtlinie in eine Richtlinie des Typs “Advanced”, indem Sie Folgendes eingeben:

    ```
    add authentication Policy <policy_name> -rule <rule> -action <LDAP
    action name>
    ```

    Beispiel: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Fügen Sie eine Richtlinienbezeichnung für die LDAP-Richtlinie hinzu, indem Sie Folgendes eingeben:

    ```
    add authentication policylabel <policy_label_name>
    ```

    Beispiel: `add authentication policylabel ldap_pol_label`

14. Ordnen Sie die Richtlinienbezeichnung der LDAP-Richtlinie zu, indem Sie Folgendes eingeben:

    ```
    bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol
     -priority 100 -gotoPriorityExpression NEXT
    ```

15. Verbinden Sie ein richtlinientreues Gerät, um einen NAC-Test durchzuführen und den Erfolg der LDAP-Authentifizierung zu überprüfen. Geben Sie Folgendes ein:

    ```
    bind authentication vserver <authentication vserver> -policy <web
    authentication policy> -priority 100 -nextFactor <ldap policy label> -
    gotoPriorityExpression END
    ```

16. Fügen Sie die Benutzeroberfläche für die Zuordnung zu dem virtuellen Authentifizierungsserver hinzu. Geben Sie den folgenden Befehl ein, um die Geräte-ID abzurufen:

    ```
    add authentication loginSchemaPolicy <schema policy>-rule <rule> -
    action lschema_single_factor_deviceid
    ```

17. Binden Sie den virtuellen Authentifizierungsserver, indem Sie Folgendes eingeben:

    ```
    bind authentication vserver authvs -policy lschema_xm_nac_pol -priority
     100 -gotoPriorityExpression END
    ```

18. Erstellen Sie eine LDAP-Authentifizierungsrichtlinie des Typs “Advanced” zum Aktivieren der Secure Hub-Verbindung. Geben Sie Folgendes ein:


```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP

bind authentication vserver authvs -policy ldap_xm_test_pol -priority
110 -gotoPriorityExpression NEXT
```

Samsung Knox

January 5, 2022

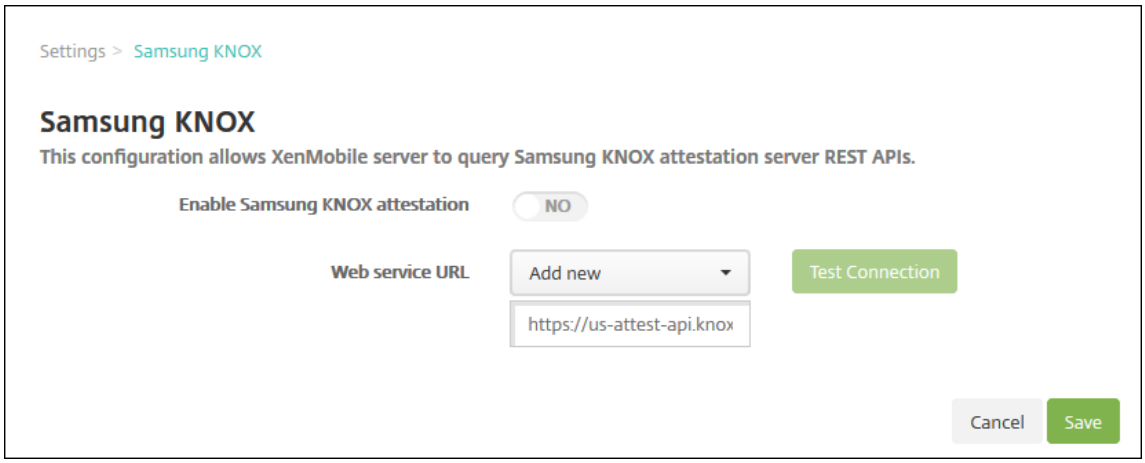
Samsung bietet verschiedene Lösungen an, die mit XenMobile Server kompatibel sind.

- XenMobile unterstützt und erweitert die Samsung Knox-Richtlinien auf kompatiblen Samsung-Geräten.
- Das Knox-Service-Plug-In (KSP) ist eine App, die einige Features der Knox Platform for Enterprise (KPE) unterstützt. Informationen von Samsung über KPE finden Sie unter Konfigurieren von Knox Platform for Enterprise und Überblick.

Sie können XenMobile für die Abfrage der REST-APIs des Samsung Knox-Nachweisservers konfigurieren.

Samsung Knox nutzt Hardwaresicherheitsmerkmale mit mehreren Schutzstufen für Betriebssystem und Apps. Eine Schutzstufe besteht im Nachweis auf der Plattform. Ein Nachweisserver bietet die Überprüfung der Kernsystemsoftware eines Mobilgeräts (z. B. Bootloader und Kernel). Die Verifizierung erfolgt 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. Die Standardeinstellung ist **NEIN**.
4. Wenn Sie **Samsung KNOX-Nachweis aktivieren** auf **JA** festlegen, wird die Option **Webdienst-URL** aktiviert. Führen Sie dann in der Liste einen der folgenden Schritte aus:
   - Klicken Sie auf den geeigneten Nachweisserver.
   - 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**.

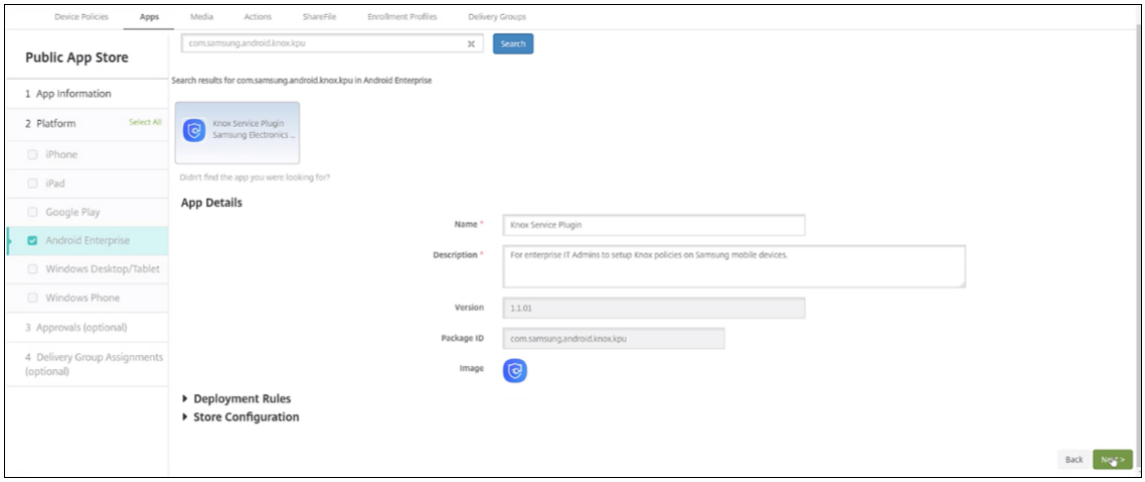
> **Hinweis:**
>
> Verwenden Sie Samsung Knox Mobile Enrollment, um mehrere Samsung Knox-Geräte bei XenMobile (oder einem beliebigen Manager für mobile Geräte) zu registrieren, ohne Geräte einzeln manuell zu konfigurieren. Weitere Informationen finden Sie unter Samsung Knox Massenregistrierung.

Hinzufügen der KSP-App (Knox-Service-Plug-In)

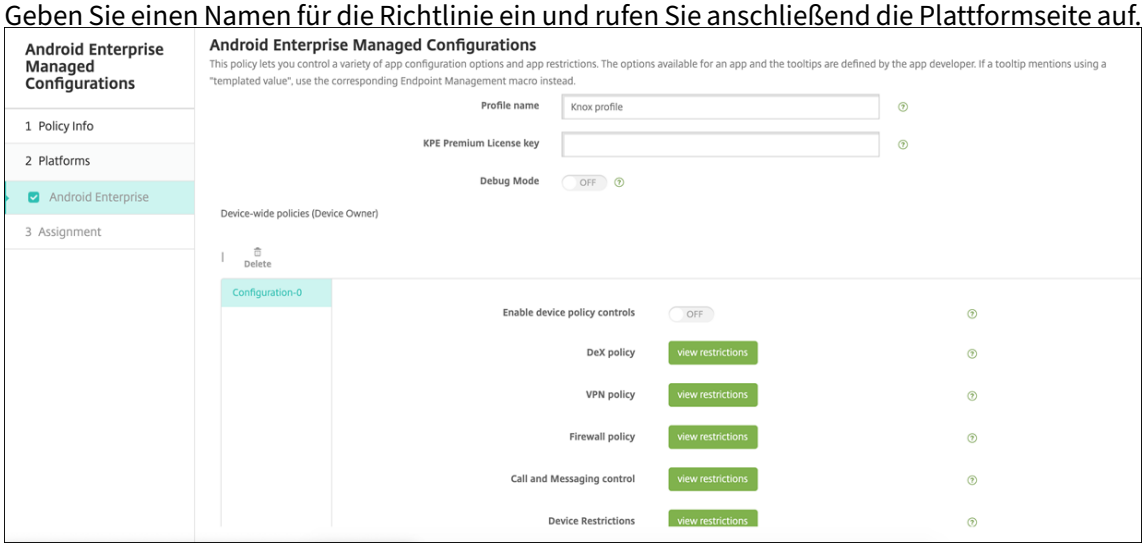
Wenn Sie Android Enterprise mit Knox verwenden möchten, fügen Sie das Knox-Service-Plug-In (KSP) in XenMobile hinzu. Die KSP-App verwendet AndroidOEMConfig, um Funktionen wie Sicherheitsrichtlinien, eine flexible VPN-Konfiguration und die biometrische Authentifizierung zu unterstützen. Mit AndroidOEMConfig können OEMs und Endpoint Mobility Manager (EMM) benutzerdefinierte OEM-APIs unterstützen. Diese APIs decken Anwendungsfälle ab, die nicht von Android Enterprise unterstützt werden.

Weitere Informationen zu KSP finden Sie im Knox Service Plug-In Admin Guide.

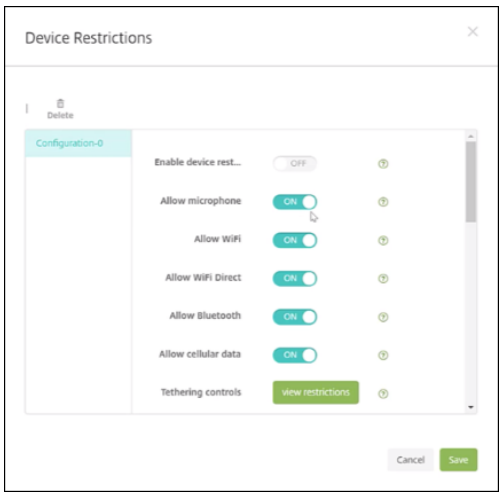
1. Melden Sie sich in Ihrem Google-Konto an und navigieren Sie zu `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`. Genehmigen Sie die KSP-App (Knox-Service-Plug-In).
2. Melden Sie sich an der XenMobile-Konsole an und fügen Sie das Knox-Service-Plug-In als öffentliche App Store-App hinzu. Weitere Informationen zum Hinzufügen von Apps aus dem öffentlichen App Store finden Sie unter Hinzufügen von Apps aus einem öffentlichen App-Store.



3. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Geräterichtlinien**. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie auf **Verwaltete Android Enterprise-Konfigurationen**. Wählen Sie im angezeigten Dialogfeld den Menüeintrag **Knox Service Plugin**. Weitere Informationen zur Richtlinie für verwaltete Android Enterprise-Konfigurationen finden Sie unter Richtlinie für verwaltete Android Enterprise-Konfigurationen.
5. Geben Sie einen Namen für die Richtlinie ein und rufen Sie anschließend die Plattformseite auf.



6. Geben Sie auf der Plattformseite einen **Profilnamen** für Ihr Knox-Profil und den **KPE-Premiumlizenzschlüssel** von Samsung ein. Die Richtlinien, die unter diesen Feldern angezeigt werden, stammen aus der Knox-Bereitstellung. Weitere Informationen zu Knox-Richtlinien finden Sie in dem weiter oben genannten Dokument “Knox Service Plug-in Admin Guide”.



7. Klicken Sie auf **Weiter** und konfigurieren Sie Bereitstellungsregeln für die Richtlinie.
8. Klicken Sie auf **Speichern**.

Samsung Knox-Massenregistrierung

January 5, 2022

Verwenden Sie Knox Mobile Enrollment, um mehrere Samsung Knox-Geräte in XenMobile (oder einem beliebigen Manager für mobile Geräte) zu registrieren, ohne Geräte einzeln manuell zu konfigurieren. Die Registrierung muss bei der Erstverwendung oder nach dem Zurücksetzen auf die Werkseinstellungen ausgeführt werden. Administratoren können Benutzernamen und Kennwörter auch direkt an das Gerät weitergeben, sodass Benutzer bei der Registrierung keine Informationen eingeben müssen.

> **Hinweis:**
>
> Das Setup für Knox Mobile Enrollment hat nichts mit dem XenMobile Knox-Container zu tun. Weitere Informationen zu Knox Mobile Enrollment finden Sie im Knox Mobile Enrollment Admin Guide.

Voraussetzungen für Knox Mobile Enrollment

- XenMobile muss konfiguriert sein (einschließlich Lizenzen und Zertifikate) und ausgeführt werden.
- Secure Hub-APK-Datei: Sie laden die Datei bei der Einrichtung von Knox Mobile Enrollment hoch.
- Eine Liste der KME-Anforderungen finden Sie unter Einführung in Knox Mobile Enrollment.
- Lizenz für Samsung Knox Platform for Enterprise (PKE), erforderlich für die Anwendung von Geräterichtlinien. Geben Sie den Lizenzschlüssel in der XenMobile-Geräterichtlinie “Knox Platform for Enterprise” ein.

Herunterladen der Secure Hub APK-Datei

Laden Sie Citrix Secure Hub für Android aus dem Google Play-Store herunter.

Konfigurieren von Firewallausnahmen

Konfigurieren Sie für den Zugriff auf Knox Mobile Enrollment die folgenden Ausnahmen. Einige dieser Firewallausnahmen sind für alle Geräte erforderlich und einige sind spezifisch für die geografische Region des Geräts.

Region des Geräts	URL	Port	Ziel
Alle	https://gslb.secb2b.com	443	Globaler Load Balancer für die Initiierung von Knox Mobile Enrollment
Alle	https://gslb.secb2b.com	80	Globaler Load Balancer für die Initiierung von Knox Mobile Enrollment auf einigen limitierten Legacy-Geräten
Alle	umc-cdn.secb2b.com	443	Samsung Agent-Update-Server
Alle	bulkenrollment.s3.amazonaws.com	80	EULAs für Knox Mobile Enrollment
Alle	eula.secb2b.com	443	EULAs für Knox Mobile Enrollment
Alle	us-be-api-mssl.samsungknox.com	443	Samsung-Server für IMEI-Überprüfung
Vereinigte Staaten	https://us-segd-api.secb2b.com	443	Samsung Enterprise Gateway für die US-Region
Europa	https://eu-segd-api.secb2b.com	443	Samsung Enterprise Gateway für die Region Europa

Region des Geräts	URL	Port	Ziel
China	`https://china-segd-api.secb2b.com`	443	Samsung Enterprise Gateway für die Region China

> **Hinweis:**
>
> Eine vollständige Liste der Firewall-Ausnahmen finden Sie im Knox Mobile Enrollment Admin Guide.

Zugreifen auf Knox Mobile Enrollment

Folgen Sie der Samsung-Dokumentation unter Get started with KME, um Zugriff auf Knox Mobile Enrollment zu erhalten.

Einrichten von Knox Mobile Enrollment

Wenn Sie Zugriff auf Knox Mobile Enrollment erhalten haben, melden Sie sich im Knox-Portal an.

Die Registrierung umfasst die folgenden allgemeinen Schritte.

1. Erstellen Sie ein MDM-Profil mit den Informationen und Einstellungen Ihrer MDM-Konsole.

   Das MDM-Profil zeigt den Geräten an, wie eine Verbindung mit dem MDM hergestellt wird.

2. Fügen Sie Ihrem MDM-Profil Geräte hinzu.

   Laden Sie dazu eine CSV-Datei mit Geräteinformationen hoch oder installieren und verwenden Sie die Knox-Bereitstellungs-App aus Google Play.

3. Samsung benachrichtigt Sie, wenn der Gerätebesitz verifiziert ist.

4. Stellen Sie Benutzern die MDM-Anmeldeinformationen bereit. Weisen Sie die Benutzer an, sich über Wi-Fi mit dem Internet zu verbinden und die Registrierungsaufforderung für ihre Geräte zu akzeptieren.

Erstellen eines MDM-Profils

Befolgen Sie die Schritte in der Samsung-Dokumentation unter Profilkonfiguration.

Wenn folgende Felder oder Schritte angezeigt werden, konfigurieren Sie sie wie folgt:

- **Pick your MDM:** Wählen Sie **Citrix** aus dem Menü aus. Nur für Gerätebesitzerprofile.

- **MDM Agent APK:** nur für Gerätebesitzerprofile. Geben Sie die URL zum Herunterladen der Secure Hub-APK-Datei ein: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

  Die APK-Datei kann auf einem beliebigen Server sein, solange die Geräte während der Registrierung darauf zugreifen können. Bei der Registrierung führt ein Gerät folgende Schritte aus:

  - Download von Secure Hub von der APK-Download-URL.
  - Installation von Secure Hub.
  - Öffnen von Secure Hub mit den nachfolgend beschriebenen benutzerdefinierten JSON-Daten.

  Die Groß-/Kleinschreibung des APK-Dateinamens muss mit der Schreibweise in der URL übereinstimmen. Beispiel: Wenn der Dateiname nur aus Kleinbuchstaben besteht, muss er auch in der URL in Kleinbuchstaben eingegeben werden.

- **MDM Server URI:** Geben Sie keinen MDM-Server-URI an. XenMobile unterstützt das Samsung MDM-Protokoll nicht.

- **Custom JSON Data:** Secure Hub erfordert die Adresse des XenMobile-Servers und den Benutzernamen und das Kennwort für die Registrierung. Sie können diese Informationen in der JSON bereitstellen, damit Secure Hub sie nicht bei den Benutzern anfordert. Secure Hub fordert die Benutzer nur dann zur Eingabe von Serveradresse, Benutzernamen und Kennwort auf, wenn das Feld in der JSON weggelassen wird.

  Format für benutzerdefinierte JSON-Daten:

  ```
  { "serverURL": "URL", "xm_username":"Username", "xm_password":"Password
  "}
  ```

  In diesem für die Massenregistrierung typischen Beispiel fordert Secure Hub die Benutzer bei der Registrierung nicht zur Eingabe der Serveradresse oder ihrer Anmeldeinformationen auf:

  ```
  { "serverURL":"https://example.com/zdm", "xm_username":"userN", "
  xm_password":"password1234"}
  { "serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2"
  , "xm_password":"password7890"}
  ```

  In diesem für Kiosk-basierte Geräte typischen Beispiel fordert Secure Hub die Benutzer zur Eingabe ihrer Anmeldeinformationen auf:

  ```
  { "serverURL":"https://example.com/zdm"}
  ```

  Sie können auch benutzerdefiniertes JSON für die Zero-Touch-Registrierung für Android Enterprise eingeben.

  ```
  1       {
  ```



```
2
3           "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4           {
5
6               "serverURL":"URL","xm_username":"username","
                    xm_password":"password"
7            }
8
9       }
10
11  <!--NeedCopy-->
```

Wenn ein Gerät die Registrierung beginnt, lädt es Secure Hub von der angegebenen URL herunter, installiert und öffnet es.

Weitere Konfiguration

Weitere Konfigurationshinweise finden Sie auf den folgenden Seiten der Samsung-Dokumentation:

- Gerätekonfiguration: Große Mengen an Geräten hinzufügen.
- App zur Bereitstellung von Samsung Knox: Registrierung von Geräten über Bluetooth, NFC oder Wi-Fi Direct.
- Knox Mobile Enrollment: Weitere Informationen zu Samsung Knox finden Sie in der Samsung-Dokumentation.

Registrieren von Geräten mit einer Knox-API vor Version 2.4

Auf Geräten mit einer Knox-API-Version vor 2.4 wird die Massenregistrierung nicht automatisch bei der Ersteinrichtung des Geräts gestartet. Benutzer müssen die Registrierung selbst initiieren. Hierfür laden sie den neuen Mobile Enrollment-Client von einer Samsung-Site herunter und starten die Registrierung.

Der heruntergeladene Enrollment-Client verwendet das MDM-Profil und die APKs, die im Knox-Massenregistrierungsportal für die Knox 2.4/2.4.1-Geräte konfiguriert wurden.

In der Regel sind die folgenden Schritte auszuführen:

1. Schalten Sie das Gerät ein und stellen Sie eine Verbindung mit Wi-Fi her. Wenn Mobile Enrollment nicht startet oder Wi-Fi nicht verfügbar ist, führen Sie folgende Schritte aus:
   a) Navigieren Sie zu Samsung Knox Mobile Enrollment.
   b) Tippen Sie auf die Schaltfläche **Next**, um Geräte über eine mobile Verbindung zu registrieren.
2. Wenn **Enroll with Knox** angezeigt wird, tippen Sie auf **Continue**.

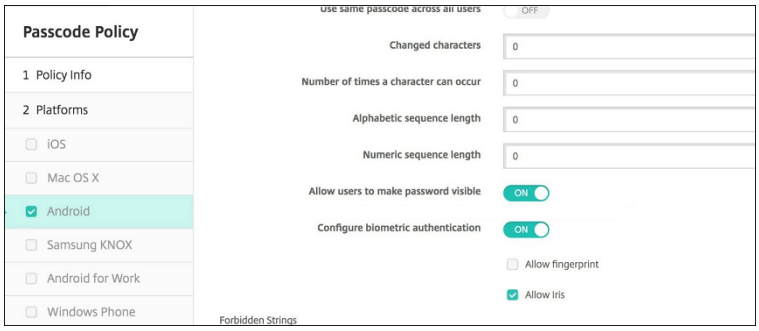
3. Lesen Sie die Lizenzvereinbarung (falls verfügbar). Tippen Sie auf **Next**.
4. Geben Sie bei Aufforderung unter **User ID** und **Password** die vom IT-Administrator bereitgestellten Informationen ein.

Nun werden die Anmeldeinformationen des Benutzers überprüft und das Gerät wird von der IT-Umgebung Ihres Unternehmens registriert.

Aktivieren und Deaktivieren der biometrischen Authentifizierung für Samsung-Geräte

XenMobile unterstützt die Authentifizierung per Fingerabdruck oder Iriserkennung (auch als biometrische Authentifizierung bezeichnet). Sie können die biometrische Authentifizierung für Samsung-Geräte ohne Aktion der Benutzer aktivieren und deaktivieren. Wenn Sie die biometrische Authentifizierung in XenMobile deaktivieren, können Benutzer und Drittanbieter-Apps das Feature nicht aktivieren.

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 Option **Android** oder **Samsung Knox**.
7. Wählen Sie unter **Biometrische Authentifizierung konfigurieren** die Einstellung **Ein** (ON).
8. Bei Auswahl von **Android** unter **Samsung SAFE** aktivieren Sie die Option **Fingerabdruck zulassen** oder **Iriserkennung zulassen** oder beides.



Sicherheitsaktionen

January 5, 2022

Auf der Seite **Verwalten** > **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.

- **Aktivierungssperre umgehen:** entfernt die Aktivierungssperre auf betreuten iOS-Geräten vor der Geräteaktivierung. Dieser Befehl erfordert keine persönliche Apple-ID und kein Kennwort seitens des Benutzers.
- **App-Sperre:** verhindert den Zugriff auf alle Apps auf einem Gerät. Auf Android-Geräten können Benutzer sich nach Eintreten einer App-Sperre nicht bei XenMobile anmelden. Unter iOS können Benutzer sich anmelden, jedoch nicht auf Apps zugreifen.
- **App löschen:** Entfernt das Benutzerkonto aus Secure Hub und hebt die Registrierung des Geräts auf. Benutzer können sich erst wieder registrieren, wenn Sie die Aktion **Löschen der Apps rückgängig machen** ausführen.
- **ASM-Deployment Program-Aktivierungssperre:** Erstellt einen Code zum Umgehen der Aktivierungssperre für iOS-Geräte, die bei Apple School Manager-DEP registriert sind.
- **Einschränkungen deaktivieren:** Dieser Befehl ermöglicht auf betreuten iOS-Geräten das Deaktivieren des vom Benutzer festgelegten Einschränkungskennworts und der Einschränkungseinstellungen durch XenMobile Server.
- **Modus 'Verloren' aktivieren:** versetzt betreute iOS-Geräte in den Modus "Verloren" und sendet eine Nachricht, Telefonnummer und Fußnote an das Gerät zur Anzeige. Mit "Modus 'Verloren' deaktivieren" wird der Modus "Verloren" auf Geräten wieder aufgehoben.
- **Tracking aktivieren:** Mit diesem Befehl kann XenMobile auf Android- oder iOS-Geräten den Standort bestimmter Geräte mit einer von Ihnen definierten Frequenz abfragen. Um Gerätekoordinaten und -position auf einer Karte anzuzeigen, gehen Sie zu **Verwalten > Geräte**, wählen Sie ein Gerät aus, und klicken Sie dann auf **Bearbeiten**. Die Geräteinformationen finden Sie auf der Registerkarte **Allgemein** unter **Sicherheit**. Verwenden Sie **Tracking aktivieren**, um das Gerät kontinuierlich zu verfolgen. Secure Hub meldet den Standort regelmäßig, wenn das Gerät läuft.
- **Vollständig löschen:** löscht sofort alle Daten und Apps von Geräten, einschließlich Speicherkarten.
  - Bei Android-Geräten kann diese Anforderung auch die Option zum Löschen von Daten auf Speicherkarten umfassen.

  - Für vollständig verwaltete Android Enterprise-Geräte mit Arbeitsprofil (COPE-Geräte) können Sie eine vollständige Löschung durchführen, nachdem das Arbeitsprofil durch selektives Löschen entfernt wurde.
  - Bei iOS- und macOS-Geräten erfolgt die Löschung sofort, selbst wenn ein Gerät gesperrt ist. Für iOS 11-Geräte (Mindestversion): Wenn Sie die vollständige Löschung bestätigen, können Sie entscheiden, ob Sie den Mobilfunktarif auf dem Gerät beibehalten.
  - Bei Windows Phone-Geräten werden durch eine vollständige Löschung sämtliche XenMobile-Informationen sowie alle Benutzerdaten gelöscht. Zu diesen Benutzerdaten gehören persönliche Inhalte wie Apps, E-Mail, Kontakte und Medien.
  - Nach einer Datenlöschung auf Geräten mit Windows Mobile 6 oder einer älteren Windows Mobile-Version muss das Gerät u. U. zum Laden des ursprünglichen Betriebssystems und/oder der ursprünglichen Software an den Hersteller zurückgeschickt werden.
  - Wenn der Benutzer das Gerät ausschaltet, bevor der Inhalt der Speicherkarte gelöscht ist, kann er möglicherweise weiterhin auf Gerätedaten zugreifen.
  - Sie können die Löschanforderung noch so lange abbrechen, bis sie an das Gerät gesendet wurde.

- **Orten:** Dient zur Suche nach einem Gerät und zeigt den Gerätestandort einschließlich Karte auf der Seite **Verwalten > Geräte** unter **Gerätedetails > Allgemein** an. Orten ist eine einmalige Aktion. Mit **Orten** wird der aktuelle Gerätestandort angezeigt, wenn Sie die Aktion ausführen. Um das Gerät über einen längeren Zeitraum hinweg zu verfolgen, verwenden Sie **Tracking aktivieren**.
  - Wenn Sie diese Aktion auf Android-Geräte (außer Android Enterprise) oder auf Android Enterprise-Geräte (unternehmenseigene oder BYOD) anwenden, berücksichtigen Sie Folgendes:
    * Die Verwendung von **Orten** erfordert eine Berechtigung, die der Benutzer bei der Registrierung erteilt. Der Benutzer kann das Erteilen der Berechtigung unterlassen. Wenn der Benutzer die Berechtigung bei der Registrierung nicht erteilt hat, fordert XenMobile beim Senden des Befehls **Orten** erneut eine Berechtigung an.
  - Beachten Sie beim Anwenden dieser Funktion auf iOS- oder Android Enterprise-Geräte folgende Einschränkungen:
    * Für Android Enterprise-Geräte funktioniert diese Anforderung nur, wenn in der Standortrichtlinie für Geräte der Standortmodus für das Gerät auf **Hohe Genauigkeit** oder **Akku schonen** festgelegt ist.
    * Bei iOS-Geräten ist dieser Befehl nur erfolgreich, wenn die Geräte im MDM-Modus “Verloren” sind.

- **Sperren:** Sperrt ein Gerät remote. Diese Aktion ist nützlich, wenn ein Gerät vermisst wird und Sie nicht wissen, ob es gestohlen wurde. XenMobile generiert dann einen PIN-Code und stellt

ihn für das Gerät ein. Für den Zugriff auf das Gerät muss die PIN eingegeben werden. Verwenden Sie **Sperren abbrechen**, um ein Gerät über die XenMobile-Konsole zu entsperren.

- **Sperren und Kennwort zurücksetzen:** Sperrt Geräte remote und setzt den Passcode zurück.
  - Wird nicht unterstützt auf Geräten, die in Android Enterprise im Arbeitsprofilmodus registriert sind und auf denen Android-Versionen vor Android 8.0 ausgeführt werden.
  - Auf in Android Enterprise im Arbeitsprofilmodus registrierten Geräten mit Android 8.0 oder höher tritt Folgendes auf:
    * Der gesendete Passcode sperrt das Arbeitsprofil. Das Gerät ist nicht gesperrt.
    * Wenn kein Passcode gesendet wird oder der gesendete Passcode nicht den Anforderungen entspricht und noch kein Passcode im Arbeitsprofil festgelegt ist, wird das Gerät gesperrt.
    * Wenn kein Passcode gesendet wird oder der gesendete Passcode nicht den Anforderungen entspricht, aber bereits ein Passcode im Arbeitsprofil festgelegt ist, wird nur das Arbeitsprofil gesperrt und nicht das Gerät.
- **Benachrichtigen (Klingeln):** gibt einen Ton auf Android-Geräten aus.
- **Neu starten:** Startet Windows 10- und Windows 11-Geräte neu. Bei Windows-Tablets und -PCs erscheint die Meldung "System wird bald neu gestartet" und der Neustart erfolgt fünf Minuten später. Bei Windows Phone erfolgt der Neustart nach einigen Minuten ohne Warnung der Benutzer.
- **AirPlay-Synchronisierung anfordern/AirPlay-Synchronisierung beenden:** startet bzw. beendet die AirPlay-Synchronisierung auf betreuten iOS-Geräten.
- **Neu starten/Herunterfahren:** startet betreute iOS-Geräte sofort bzw. fährt sie sofort herunter.
- **Widerrufen:** verhindert die Herstellung einer Verbindung zwischen Geräten und XenMobile Server.
- **Sperren/Autorisieren (iOS, macOS):** führt die gleichen Aktionen aus wie "Selektiv löschen". Nach einer Sperrung können Sie Geräte neu autorisieren, um sie erneut zu registrieren.
- **Klingeln:** spielt einen Ton auf betreuten iOS-Geräten ab, wenn diese im Modus "Verloren" sind. Der Ton wird abgespielt, bis Sie den Modus "Verloren" des Geräts deaktivieren oder der Benutzer den Ton deaktiviert.
- **Selektiv löschen:** löscht alle Unternehmensdaten und -Apps von Geräten, private Daten und Apps bleiben erhalten. Nach einer selektiven Löschung kann der Benutzer das Gerät erneut registrieren.
  - Beim selektiven Löschen auf einem Android-Gerät wird dieses nicht von Device Manager und dem Unternehmensnetzwerk getrennt. Um zu verhindern, dass das Gerät auf Device Manager zugreift, müssen Sie außerdem die Gerätezertifikate widerrufen.

  - Durch selektives Löschen werden Android-Geräte außerdem widerrufen. Sie können das Gerät erst dann erneut registrieren, wenn Sie es neu autorisiert oder von der Konsole gelöscht haben.
  - Für vollständig verwaltete Android Enterprise-Geräte mit Arbeitsprofil (COPE-Geräte) können Sie eine vollständige Löschung durchführen, nachdem das Arbeitsprofil durch selektives Löschen entfernt wurde. Sie können das Gerät aber auch mit demselben Benutzernamen neu registrieren. Bei der Neuregistrierung des Geräts wird das Arbeitsprofil neu erstellt.
  - Bei Geräten mit aktivierter Samsung Knox-API wird beim selektiven Löschen auch der Samsung Knox-Container entfernt.
  - Bei iOS- und macOS-Geräten werden mit diesem Befehl sämtliche über MDM installierten Profile entfernt.
  - Auf Windows-Geräten wird beim selektiven Löschen auch der Inhalt des Profilordners aller gerade bei dem Gerät angemeldeter Benutzer entfernt. Webclips, die Sie den Benutzern über eine Konfiguration bereitstellen, werden beim selektiven Löschen nicht entfernt. Zum Entfernen von Webclips müssen die Benutzer die Registrierung ihres Geräts manuell aufheben. Geräte, auf denen eine selektive Löschung durchgeführt wurde, können nicht erneut registriert werden.
  - Beim selektiven Löschen auf Windows Phone-Geräten wird das Unternehmenstoken entfernt, das die Installation von Apps auf dem Gerät durch XenMobile ermöglicht. Außerdem werden alle XenMobile-Zertifikate und -Konfigurationen von den Geräten entfernt. Windows Phone-Geräte, auf denen eine selektive Löschung durchgeführt wurde, können nicht erneut registriert werden.

- **Entsperren:** löscht den Passcode, der beim Sperren an das Gerät gesendet wurde. Mit dem Befehl wird das Gerät nicht entsperrt.

Auf der Seite **Verwalten > Geräte** werden unter **Gerätedetails** außerdem Sicherheitseigenschaften aufgeführt. Dazu gehören Starke ID, Gerätesperrung, Umgehen der Aktivierungssperre und weitere plattformspezifische Informationen. Das Feld **Gerät vollständig löschen** enthält den Benutzer-PIN-Code. Der Benutzer muss den Code eingeben, anschließend erfolgt die Löschung. Wenn der Benutzer den Code vergessen hat, können Sie ihn hier nachsehen.

Sicherheitsaktionen für Android-Geräte

Sicherheitsaktionen	Android (außer für Android Enterprise-Geräte)	Android Enterprise (BYOD)	Android Enterprise (Unternehmensbesitz)
App-Sperre	Ja	Nein	Nein
App löschen	Ja	Nein	Nein

Sicherheitsaktionen	Android (außer für Android Enterprise-Geräte)	Android Enterprise (BYOD)	Android Enterprise (Unternehmensbesitz)
Vollständig löschen	Ja	Nein	Ja
Suchen	Ja: Bei Geräten mit Android 6.0 und höher muss der Benutzer zur Verwendung der Suchfunktion bei der Registrierung eine Suchberechtigung erteilt haben. Der Benutzer kann das Erteilen der Berechtigung ablehnen. Wenn der Benutzer die Berechtigung bei der Registrierung nicht erteilt hat, fordert XenMobile sie beim Senden des Suchbefehls erneut an.	Ja: Bei Geräten mit Android 6.0 und höher muss der Benutzer zur Verwendung der Suchfunktion bei der Registrierung eine Suchberechtigung erteilt haben. Der Benutzer kann das Erteilen der Berechtigung ablehnen. Wenn der Benutzer die Berechtigung bei der Registrierung nicht erteilt hat, fordert XenMobile sie beim Senden des Suchbefehls erneut an.	Ja: Bei Geräten mit Android 6.0 und höher muss der Benutzer zur Verwendung der Suchfunktion bei der Registrierung eine Suchberechtigung erteilt haben. Der Benutzer kann das Erteilen der Berechtigung ablehnen. Wenn der Benutzer die Berechtigung bei der Registrierung nicht erteilt hat, fordert XenMobile sie beim Senden des Suchbefehls erneut an.
Sperren	Ja	Ja	Ja
Lock and Reset Password	Ja	Nein	Ja
Notify (Ring)	Ja	Ja	Ja
Widerrufen	Ja	Ja	Ja
Selektiv löschen	Ja	Ja	Nein

Sicherheitsaktionen für iOS- und macOS-Geräte

Sicherheitsaktionen	iOS	macOS
Aktivierungssperre umgehen	Ja	Nein
App-Sperre	Ja	Nein
App löschen	Ja	Nein
Aktivierungssperre für ASM-Bereitstellungsprogramm	Ja	Nein
Einschränkungen deaktivieren	Ja	Nein
Modus “Verloren” aktivieren/deaktivieren	Ja	Nein
Tracking aktivieren/deaktivieren	Ja	Nein
Vollständig löschen	Ja	Ja
Suchen	Ja	Nein
Sperren	Ja	Ja
Klingeln	Ja	Ja
AirPlay-Synchronisierung anfordern/beenden	Ja	Nein
Neustart/Herunterfahren	Ja	Nein
Wiederrufen/Autorisieren	Ja	Ja
Selektiv löschen	Ja	Ja
Unlock	Ja	Nein

Sicherheitsaktionen für Windows-Geräte

Sicherheitsaktionen	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Suchen	Ja	Ja	Nein
Sperren	Ja	Ja	Ja
Lock and Reset Password	Ja	Nein	Ja
Führen Sie einen Neustart aus.	Ja	Ja	Nein

Sicherheitsaktionen	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Widerrufen	Ja	Ja	Ja
Klingeln	Ja	Nein	Ja
Selektiv löschen	Ja	Ja	Ja
Löschen	Ja	Ja	Ja

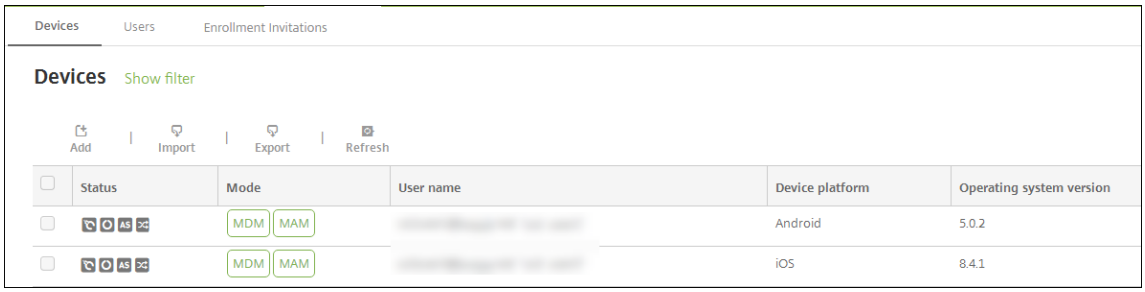
Der Rest dieses Artikels enthält Anweisungen zum Ausführen diverser Sicherheitsaktionen. Sie können einige Aktionen automatisieren. Weitere Informationen hierzu finden Sie unter Automatisierte Aktionen.

Sperren von iOS-Geräten

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.

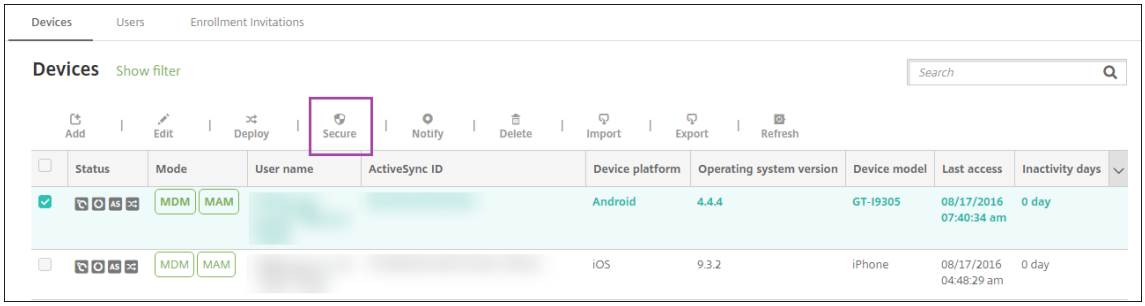
Zum Anzeigen einer Nachricht und Telefonnummer auf einem gesperrten Gerät muss die Richtlinie Passcode in der XenMobile-Konsole auf **wahr** festgelegt werden. Alternativ können Benutzer den Passcode auf dem Gerät auch manuell aktivieren.

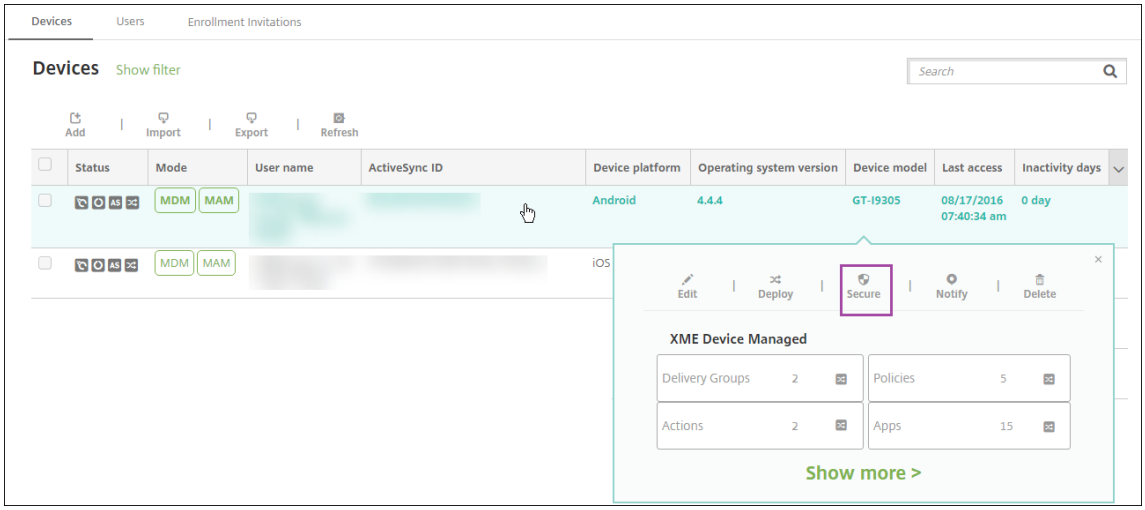
1. Klicken Sie auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.



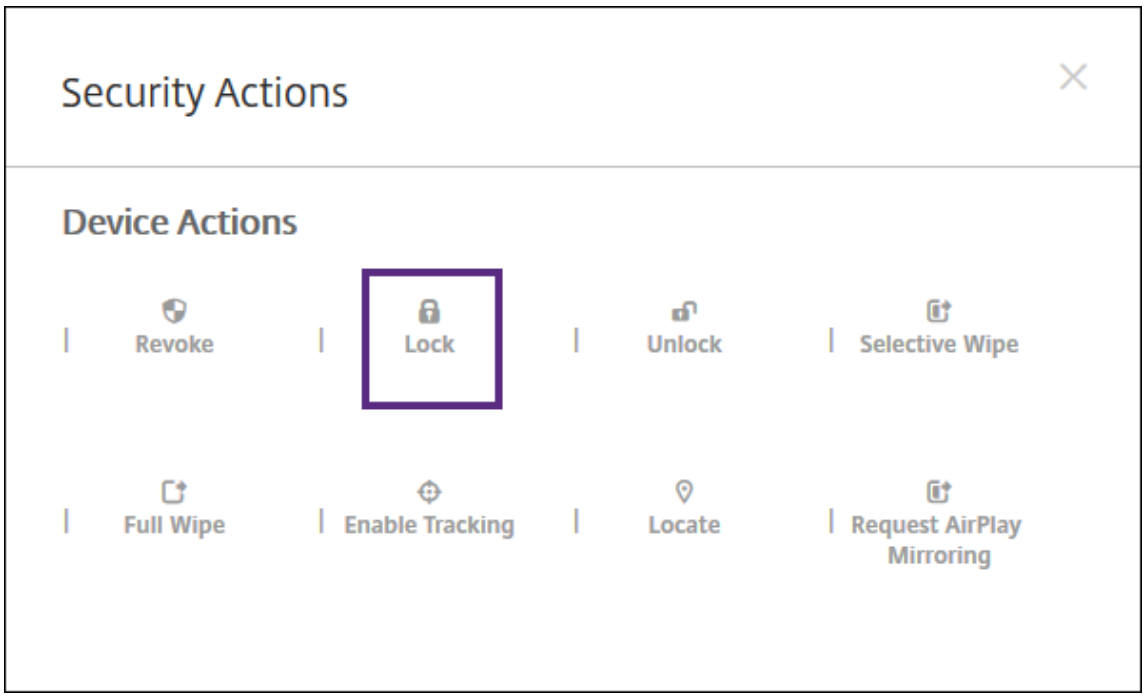
2. Wählen Sie das iOS-Gerät aus, das Sie sperren möchten.

   Wenn Sie das Kontrollkästchen neben einem Gerät aktivieren, wird das Menü mit den Optionen oberhalb der Liste angezeigt. Wenn Sie an eine andere Stelle in der Liste klicken, wird das Menü mit den Optionen rechts daneben angezeigt.

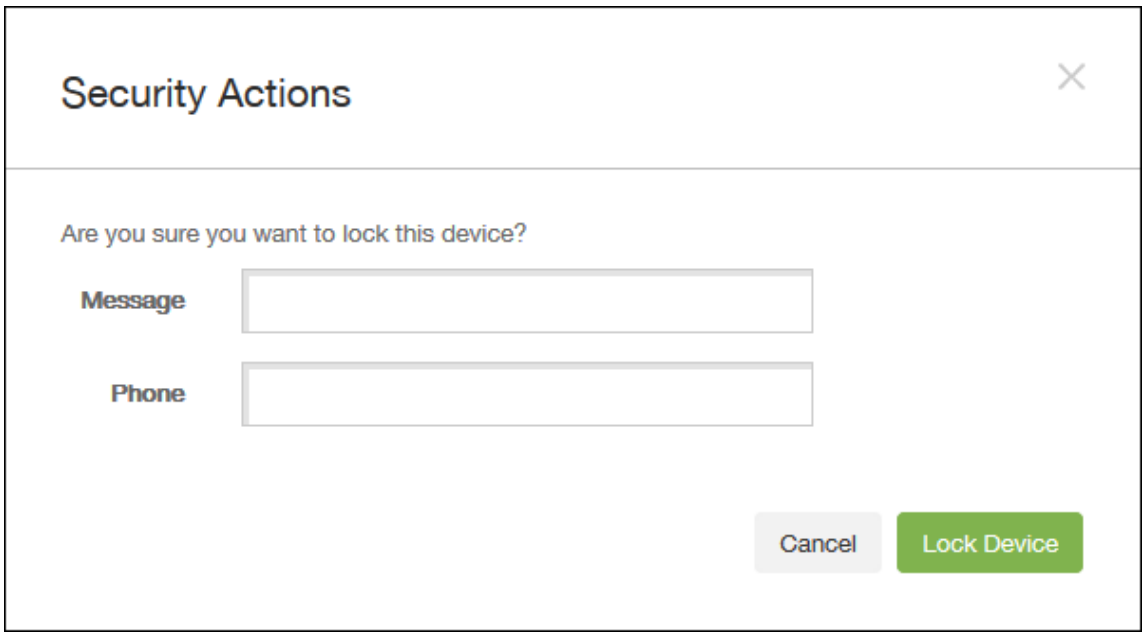




3. Wählen Sie im Menü “Optionen” die Option **Sicherheit**. Das Dialogfeld **Sicherheitsaktionen** wird angezeigt.



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.

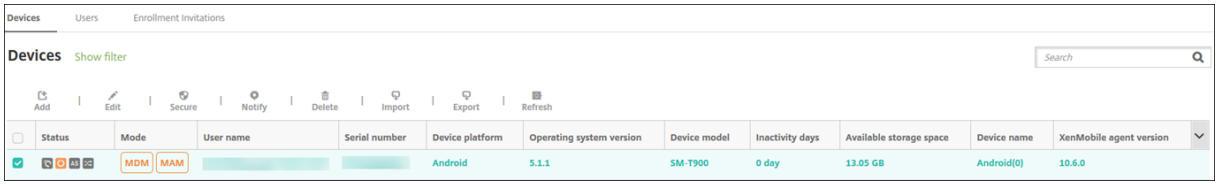
   iPhones ab iOS 7: Wenn Sie das Feld **Nachricht** leer lassen und eine Telefonnummer angeben, wird die Meldung "Besitzer anrufen" auf dem Sperrbildschirm des Geräts angezeigt.

6. Klicken Sie auf **Gerät sperren**.

Entfernen von Geräten aus der XenMobile-Konsole

> **Wichtig:**
>
> Wenn Sie ein Gerät aus der XenMobile-Konsole entfernen, verbleiben verwaltete Apps und Daten auf dem Gerät. Informationen zum Entfernen verwalteter Apps und Daten Geräten finden Sie weiter unten in diesem Artikel unter "Löschen von Geräten".

Zum Entfernen eines Geräts aus der XenMobile-Konsole navigieren Sie zu **Verwalten > Geräte**, wählen Sie ein verwaltetes Gerät und klicken Sie auf **Löschen**.



Durchführen einer selektiven Löschung

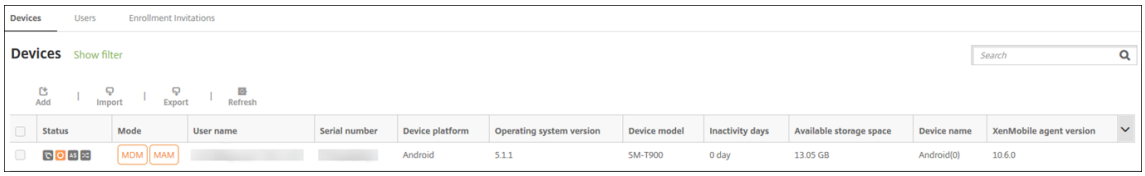
1. Navigieren Sie zu **Verwalten > Geräte**, wählen Sie ein verwaltetes Gerät aus und klicken Sie auf **Sicherheit**.
2. Klicken Sie unter **Sicherheitsaktionen** auf **Selektiv löschen**.
3. Android-Geräte: Klicken Sie nach der Datenlöschung auf **Sicherheitsaktionen** > **Widerrufen**, um das Gerät vom Unternehmensnetzwerk zu trennen.

   Wenn Sie die Löschanforderung vor deren Ausführung zurücknehmen möchten, klicken Sie auf **Sicherheitsaktionen** > **Selektives Löschen abbrechen**.

Löschen von Geräten

Bei diesem Vorgang werden verwaltete Anwendungen und Daten aus dem Gerät entfernt und das Gerät aus der Liste der Geräte der XenMobile-Konsole gelöscht. Mit der öffentlichen REST-API von Endpoint Management können Sie Geräte in großen Mengen löschen.

1. Navigieren Sie zu **Verwalten > Geräte**, wählen Sie ein verwaltetes Gerät aus und klicken Sie auf **Sicherheit**.
2. Klicken Sie auf **Selektiv löschen**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Selektives Löschen durchführen**.
3. Um sich zu vergewissern, dass der Löschbefehl erfolgreich war, aktualisieren Sie die Seite **Verwalten > Geräte**. Eine gelbe Färbung für MDM und MAM in der Spalte **Modus** zeigt an, dass der Löschbefehl erfolgreich war.



4. Wählen Sie auf der Seite **Verwalten > Geräte** ein verwaltetes Gerät aus und klicken Sie auf **Löschen**. Wenn Sie dazu aufgefordert werden, klicken Sie erneut auf **Löschen**.

Sperren, Entsperren, Löschen und Aufheben der Löschung von Apps

1. Navigieren Sie zu **Verwalten > Geräte**, wählen Sie ein verwaltetes Gerät aus und klicken Sie auf **Sicherheit**.
2. Klicken Sie unter **Sicherheitsaktionen** auf die App-Aktion.

   Sie können im Feld **Sicherheitsaktionen** auch den Status eines Geräts für einen Benutzer überprüfen, dessen Konto deaktiviert oder aus Active Directory gelöscht wurde. Wenn die Aktionen

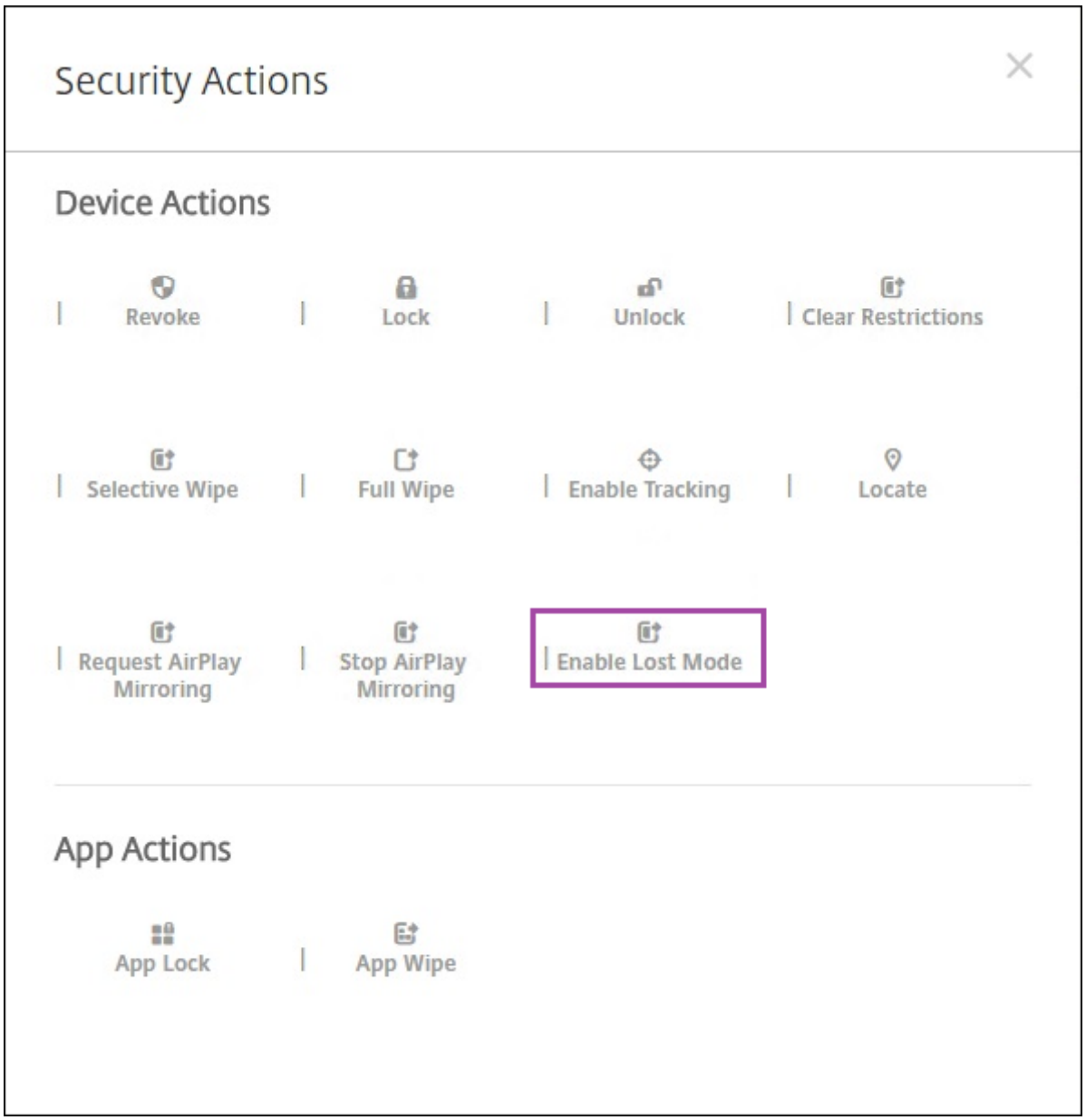
"App-Sperre aufheben" oder "Löschen der Apps rückgängig machen" vorhanden sind, gibt es Apps, die gesperrt oder gelöscht wurden.

Versetzen von iOS-Geräten in den Modus "Verloren"

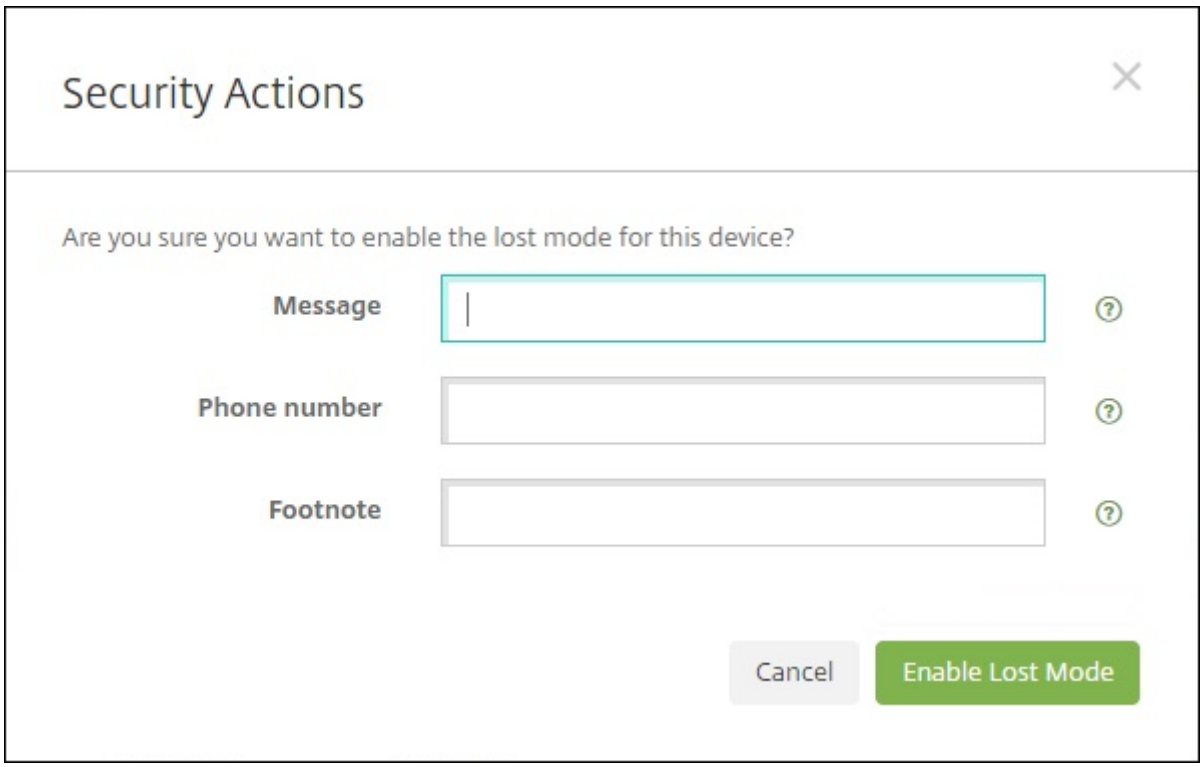
Die Geräteeigenschaft "XenMobile-Modus 'Verloren"' versetzt iOS-Geräte in den Modus "Verloren". Im Gegensatz zum von Apple verwalteten Modus "Verloren" muss ein Benutzer beim Modus "Verloren" in XenMobile keine der folgenden Aktionen ausführen, um sein Gerät zu suchen: Konfigurieren der Einstellung **Find My iPhone/iPad** oder Aktivieren der Ortungsdienste für Citrix Secure Hub.

Im XenMobile-Modus "Verloren" kann ein Gerät nur über XenMobile Server entsperrt werden. (Wenn Sie hingegen das XenMobile-Feature zum Sperren von Geräten verwenden, können die Benutzer Geräte direkt durch Eingabe eines von Ihnen bereitgestellten PIN-Codes entsperren.)

Aktivieren oder Deaktivieren des Modus "Verloren": Gehen Sie zu **Verwalten > Geräte**, wählen Sie ein betreutes iOS-Gerät aus und klicken Sie auf **Sicherheit**. Klicken Sie dann auf **Modus 'Verloren' aktivieren** oder **Modus 'Verloren' deaktivieren**.

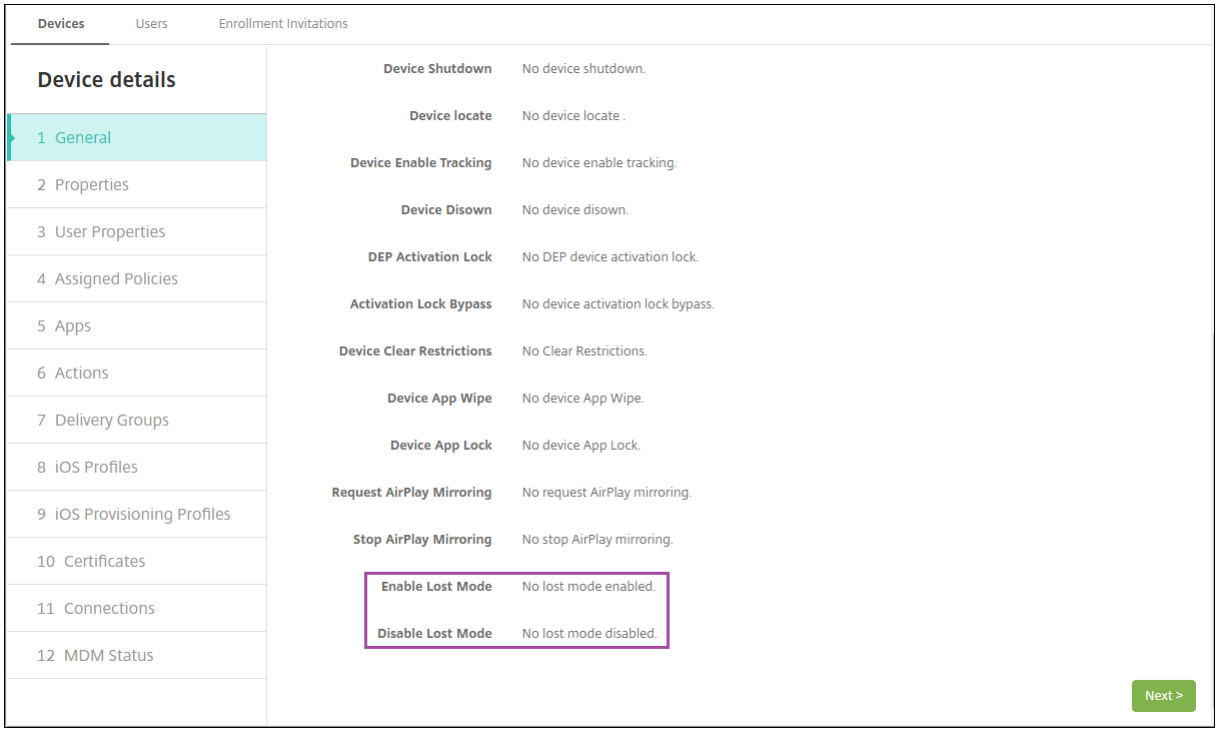


Wenn Sie auf **Modus 'Verloren' aktivieren** klicken, geben Sie die Informationen ein, die auf dem Gerät angezeigt werden sollen, wenn es im Modus "Verloren" ist.

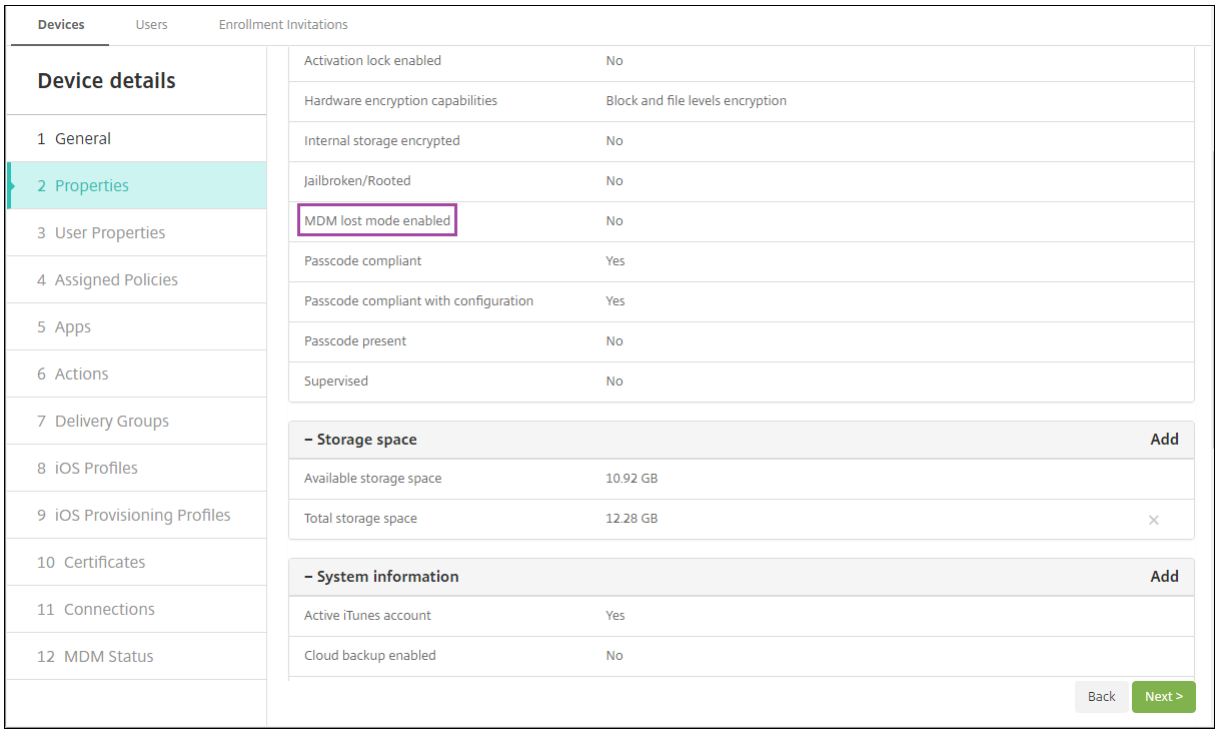


Verwenden Sie eine der folgenden Methoden, um den Status des Modus “Verloren” zu überprüfen:

- Überprüfen Sie im Fenster **Sicherheitsaktionen**, ob die Schaltfläche auf **Modus ‘Verloren’ deaktivieren** gesetzt ist.
- Zeigen Sie über **Verwalten > Geräte** auf der Registerkarte **Allgemein** unter **Sicherheit** die letzte Aktion zum Aktivieren oder Deaktivieren des Modus “Verloren” an.



- Überprüfen Sie unter **Verwalten > Geräte** auf der Registerkarte **Eigenschaften**, ob die Einstellung **MDM-Modus “Verloren” aktiviert** richtig festgelegt ist.



Wenn Sie den XenMobile-Modus “Verloren” auf iOS-Geräten aktivieren, ändert sich die XenMobile-Konsole wie folgt:

- In der über **Konfigurieren > Aktionen** aufgerufenen Liste **Aktionen** sind die folgenden automatisierten Aktionen nicht enthalten: **Gerät widerrufen**, **Gerät selektiv löschen** und **Gerät vollständig löschen**.
- In der über **Verwalten > Geräte** aufgerufenen Liste **Sicherheitsaktionen** sind die Geräteaktionen **Widerrufen** und **Selektiv löschen** nicht mehr enthalten. Sie können weiterhin eine Sicherheitsaktion verwenden, um die Aktion **Vollständig löschen** nach Bedarf auszuführen.

iPads ab iOS 7: iOS hängt die Wörter "Lost iPad" an alles an, was Sie im Feld **Nachricht** des Bildschirms **Sicherheitsaktionen** 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.

Umgehen einer iOS-Aktivierungssperre

Die Aktivierungssperre ist ein Feature von "Mein iPhone/iPad suchen", mit dem das Reaktivieren von verlorenen oder gestohlenen betreuten Geräten verhindert wird. Die Aktivierungssperre erfordert die Eingabe der Apple-ID und des Benutzerkennworts, bevor ein beliebiger Benutzer "Mein iPhone/iPad suchen" deaktivieren, die Daten auf dem Gerät löschen oder das Gerät neu aktivieren kann. Für Geräte im Besitz Ihres Unternehmens kann ein Umgehen der Aktivierungssperre erforderlich sein, um Geräte zurückzusetzen oder neu zuzuweisen.

Zum Einrichten der Aktivierungssperre müssen Sie die XenMobile-Geräterichtlinie "MDM-Optionen" konfigurieren und bereitstellen. Dann können Sie ein Gerät über die XenMobile-Konsole ohne Eingabe der Apple-Anmeldeinformationen des Benutzers verwalten. Aktivieren Sie auf der XenMobile-Konsole die Sicherheitsaktion "Aktivierungssperre umgehen", um trotz Aktivierungssperre keine Apple-Anmeldeinformationen eingeben zu müssen.

Nehmen wir folgendes Beispiel: Ein Benutzer bringt ein verlorenes Telefon zurück oder möchte ein Gerät vor oder nach einem vollständigen Löschen einrichten. Die dabei geforderte Eingabe der Anmeldeinformationen für das iTunes-Konto können Sie umgehen, indem Sie in der XenMobile-Konsole die Sicherheitsaktion "Aktivierungssperre umgehen" aktivieren.

Geräteanforderungen für das Umgeben der Aktivierungssperre

- iOS 7.1 (Mindestversion)
- Betreuter Modus mit Apple Configurator oder Apple DEP
- Konfiguration mit iCloud-Konto
- "Mein iPhone/iPad suchen" ist aktiviert
- Gerät ist bei XenMobile registriert
- Bereitgestellte Geräterichtlinie "MDM-Optionen" mit aktivierter Aktivierungssperre

Umgehen einer Aktivierungssperre vor dem vollständigen Löschen eines Geräts:

1. Wählen Sie unter **Verwalten > Geräte** das Gerät, klicken Sie auf **Sicherheit** und dann auf **Aktivierungssperre umgehen**.
2. Löschen Sie das Gerät. Die Aktivierungssperre wird während des Gerätesetups nicht angezeigt.

Umgehen einer Aktivierungssperre nach dem vollständigen Löschen eines Geräts:

1. Setzen Sie das Gerät zurück oder löschen Sie es. Die Aktivierungssperre wird während des Gerätesetups angezeigt.
2. Wählen Sie unter **Verwalten > Geräte** das Gerät, klicken Sie auf **Sicherheit** und dann auf **Aktivierungssperre umgehen**.
3. Tippen Sie auf dem Gerät auf die Taste "Zurück". Der Homebildschirm wird angezeigt.

Beachten Sie Folgendes:

- Fordern Sie die Benutzer auf, "Mein iPhone/iPad suchen" nicht zu deaktivieren. Löschen Sie das Gerät nicht vollständig. In beiden Fällen wird der Benutzer aufgefordert, das Kennwort des iCloud-Kontos einzugeben. Nach der Kontovalidierung wird dem Benutzer kein Bildschirm zum Aktivieren des iPhones/iPads angezeigt, nachdem alle Inhalte und Einstellungen gelöscht wurden.
- Für Geräte mit generiertem Code zum Umgehen der Aktivierungssperre und aktivierter Aktivierungssperre: Wenn Sie das Gerät vollständig löschen und danach die Aktivierungsseite für das iPhone/iPad nicht umgehen können, müssen Sie das Gerät nicht aus XenMobile löschen. Sie oder der Benutzer können sich direkt an den Apple-Support wenden, um das Gerät entsperren zu lassen.
- Während einer Hardwareinventur ruft XenMobile den Code zum Umgehen der Aktivierungssperre von einem Gerät ab. Wenn ein Umgehungscode verfügbar ist, wird er vom Gerät an XenMobile gesendet. Um den Umgehungscode dann vom Gerät zu entfernen, aktivieren Sie in der XenMobile-Konsole die Sicherheitsaktion "Aktivierungssperre umgehen". Damit haben XenMobile Server und Apple den erforderlichen Umgehungscode, um das Gerät zu entsperren.
- Die Sicherheitsaktion "Aktivierungssperre umgehen" stützt sich auf die Verfügbarkeit eines Apple-Diensts. Wenn die Aktion nicht funktioniert, können Sie ein Gerät auf folgende Weise entsperren. Geben Sie auf dem Gerät manuell die Anmeldeinformationen des iCloud-Kontos ein. Alternativ können Sie das Feld "Benutzername" leer lassen und den Umgehungscode im Feld "Kennwort" eingeben. Zum Ermitteln der Umgehungscodes wählen Sie das Gerät unter **Verwalten > Geräte** aus, klicken auf **Bearbeiten** und dann auf **Eigenschaften**. Der **Code zum Umgehen der Aktivierungssperre** steht unter **Sicherheitsinformationen**.

Gemeinsam genutzte Geräte

January 5, 2022

XenMobile ermöglicht die Konfiguration von Geräten, die von mehreren Benutzern verwendet werden können. 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

Sie können alle unterstützten iOS- und Android-Geräte als gemeinsam genutzte Geräte verwenden. Eine Liste der unterstützten Geräte finden Sie unter Unterstützte Gerätebetriebssysteme.

MDM-Registrierung

- Auf iOS- und Android-Tablets und -Telefonen verfügbar. Die einfache Registrierung per Apple-Bereitstellungsprogramm wird für gemeinsam genutzte Geräte unter XenMobile Enterprise nicht unterstützt. Verwenden Sie in diesem Modus für gemeinsam genutzte Geräte ein autorisiertes Apple-Bereitstellungsprogramm.
- Clientzertifikatauthentifizierung, Citrix PIN, Touch ID, Benutzerentropie und zweistufige Authentifizierung werden nicht unterstützt.

MDM+MAM-Registrierung

- Nur für iOS- und Android-Geräte verfügbar.
- Nur die Authentifizierung mit Active Directory-Benutzernamen und Kennwort wird unterstützt.
- Clientzertifikatauthentifizierung, Secure Hub-Passcode, Touch ID, Benutzerentropie und zweistufige Authentifizierung werden nicht unterstützt.
- Unterstützt keine Nur-MAM-Registrierung. Die Geräte müssen in MDM registriert werden.
- Unterstützt nur Secure Mail, Secure Web und die mobile ShareFile-App. Unterstützt keine HDX-Apps.
- Unterstützt nur Active Directory-Benutzer. Unterstützt keine lokalen Benutzer und Gruppen.
- Für ein Update auf MDM+MAM ist die erneute Registrierung nur per MDM verwalteter gemeinsam genutzter Geräte erforderlich.
- Benutzer können keine nativen Apps auf den Geräten freigeben.
- Nach dem Download während der Erstregistrierung werden mobile Produktivitätsapps nicht neu heruntergeladen, wenn sich ein neuer Benutzer am Gerät anmeldet.
- Damit Sie unter Android die Daten der einzelnen Benutzer für Sicherheitszwecke isolieren können, legen Sie die Richtlinie für die Unzulässigkeit von Geräten mit **Rooting** in der XenMobile-Konsole auf **Ein** fest.

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: Weitere Informationen finden Sie unter Erstellen, Bearbeiten, Entsperren und Löschen lokaler Benutzerkonten.
- Bereitstellungsgruppe mit Basisrichtlinien, Apps und Aktionen erstellen, die auf den Benutzer des gemeinsam genutzten Geräts angewendet werden sollen: Siehe Bereitstellen von Ressourcen.

Voraussetzungen für die MDM+MAM-Registrierung

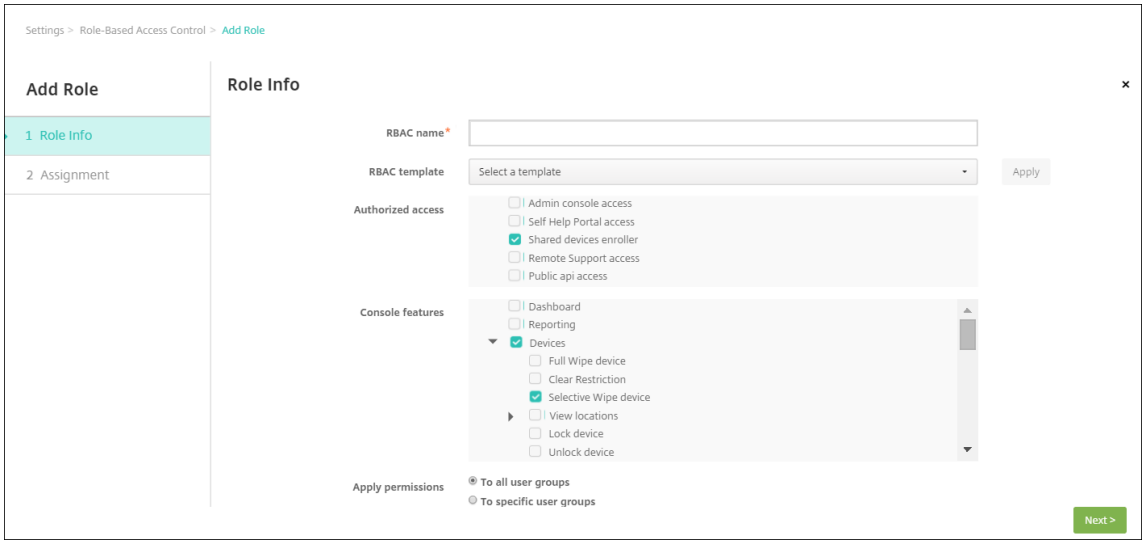
1. Erstellen Sie eine Active Directory-Gruppe. Geben Sie ihr einen aussagekräftigen Namen, z. B. **Registrierer gemeinsam genutzter Geräte**.
2. Fügen Sie der Gruppe die Active Directory-Benutzer hinzu, die freigegebene Geräte registrieren. Wenn Sie für diesen Zweck ein neues Konto verwenden möchten, erstellen Sie einen neuen Active Directory-Benutzer (z. B. **sdenroll**) und fügen Sie den Benutzer der Active Directory-Gruppe hinzu.

Konfigurieren eines gemeinsam genutzten Geräts

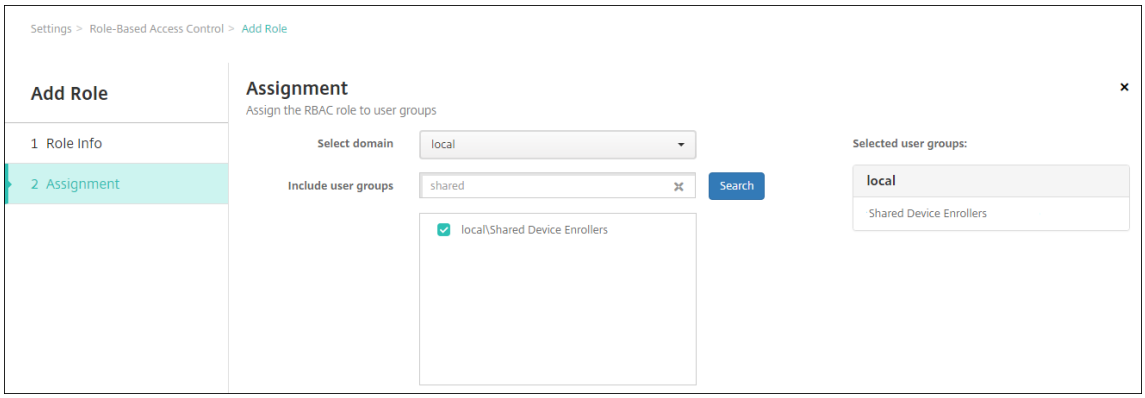
Mit den folgenden Schritten konfigurieren Sie ein gemeinsam genutztes Gerät.

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**. Die Seite **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.

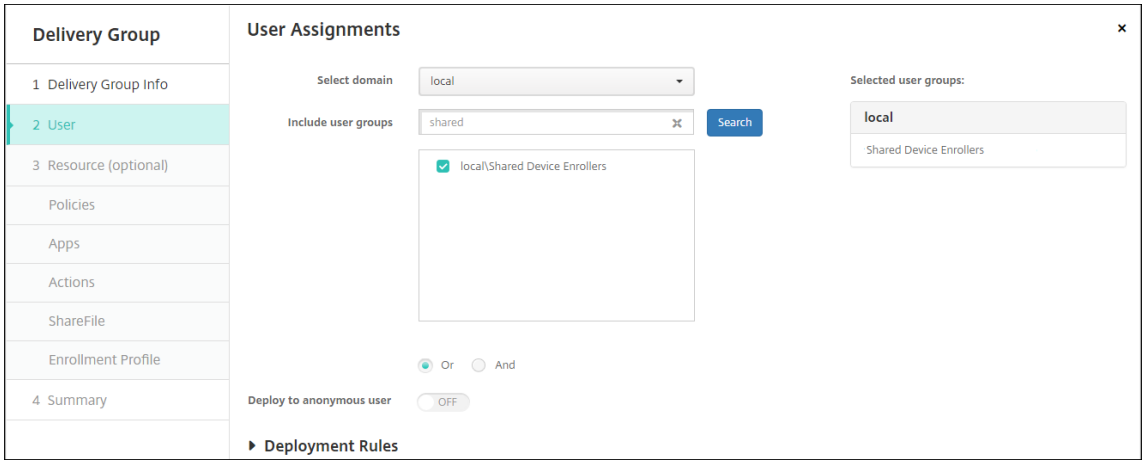
   Behalten Sie die Standardeinstellung **Auf alle Benutzergruppen** für **Berechtigungen anwenden** bei oder weisen Sie bestimmten Active Directory-Benutzergruppen Berechtigungen mit der Option **Auf bestimmte Benutzergruppen** zu.



Klicken Sie auf **Weiter**, um den Bildschirm **Zuweisung** anzuzeigen. Weisen Sie die Registrierungsrolle für gemeinsam genutzte Geräte der Active Directory-Gruppe zu, die Sie für Registrierungsbenutzer für gemeinsam genutzte Geräte in Schritt 1 unter “Voraussetzungen” erstellt haben. In der folgenden Abbildung 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. Weisen Sie dann die Bereitstellungsgruppe der Active Directory-Gruppe des Registrierungsbenutzers 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 Bereitstellen von Ressourcen.
7. Zum Beenden der gemeinsamen Gerätenutzung führen Sie einen selektiven Löschvorgang durch, um das Benutzerkonto für die Registrierung des gemeinsam genutzten Geräts zu löschen. Löschen Sie alle bereitgestellten Apps und Richtlinien von dem Gerät.

Benutzererfahrung bei gemeinsam genutzten Geräten

MDM-Registrierung

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. Meldet sich der Benutzer wieder ab, werden Richtlinien und Apps, die nicht zur Registrierung des gemeinsam genutzten Geräts gehören, entfernt. Die Registrierungsressourcen für das gemeinsam genutzte Gerät bleiben intakt.

MDM+MAM-Registrierung

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. Secure Hub blockiert neue Anmeldungen, bis die Richtlinien, Apps und Daten, die mit dem vorherigen Benutzer verknüpft sind, entfernt wurden.

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 sollen. 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

XenMobile Autodiscovery Service

January 5, 2022

Der Autodiscoverydienst vereinfacht die Registrierung von Benutzern über eine E-Mail-basierte URL-Erkennung. Citrix Workspace-Kunden erhalten mit dem Autodiscoverydienst zudem Features wie die Registrierungsüberprüfung, das Zertifikatpinning sowie weitere Vorteile. Der in Citrix Cloud gehostete Dienst ist wichtiger Bestandteil vieler XenMobile-Bereitstellungen.

Der Autodiscoverydienst bietet folgende Vorteile:

- Benutzer können ihre Geräte mit den Anmeldeinformationen für das Unternehmensnetzwerk registrieren.
- Benutzer müssen keine Details zur XenMobile Server-Adresse eingeben.
- Der Benutzername wird im Benutzerprinzipalnamenformat (UPN) eingegeben Beispiel: `user@mycompany.com`.

Die Verwendung des Autodiscoverydiensts wird für Umgebungen mit hohem Sicherheitsbedarf empfohlen. Der Autodiscoverydienst unterstützt das Zertifikatpinning mit öffentlichem Schlüssel und verhindert auf diese Weise Man-in-the-Middle-Angriffe. Zertifikatpinning stellt sicher, dass das von Ihrem Unternehmen signierte Zertifikat bei der Kommunikation zwischen Citrix-Clients und XenMobile verwendet wird. Wenden Sie sich an den Citrix Support, um das Zertifikatpinning für Ihre XenMobile-Sites zu konfigurieren. Informationen über das Zertifikatpinning finden Sie unter Zertifikatpinning.

Für den Zugriff auf den Autodiscoverydienst navigieren Sie zu https://adsui.cloud.com (Unternehmen) oder https://adsui.cem.cloud.us (Behörden).

Voraussetzungen

- Der neue Autodiscoverydienst in Citrix Cloud erfordert die neueste Version von Secure Hub:
  - Für iOS: Secure Hub Version 21.6.0 oder höher
  - Für Android: Secure Hub Version 21.8.5 oder höher

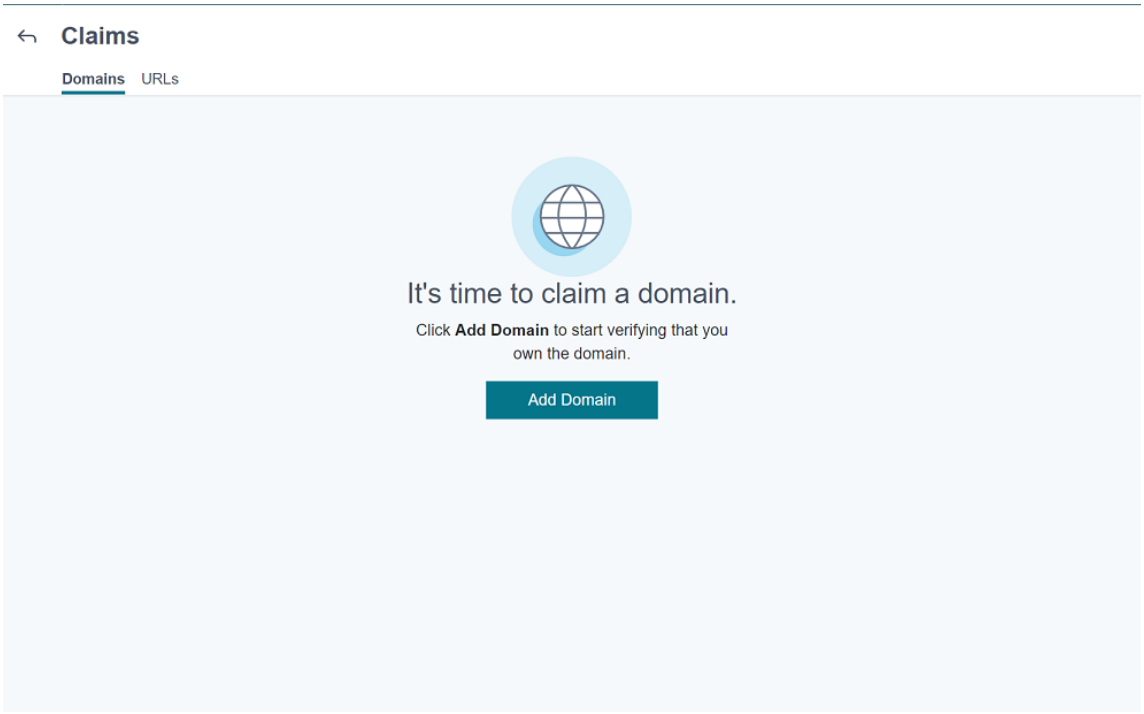
    Bei Geräten mit früheren Versionen von Secure Hub kann es zu Dienstausfällen kommen.
- Um auf den neuen AutoDiscovery-Dienst zugreifen zu können, benötigen Sie ein Citrix Cloud-Administratorkonto mit Vollzugriff. Der AutoDiscovery-Dienst unterstützt keine Administratorkonten mit benutzerdefiniertem Zugriff. Wenn Sie kein Konto haben, finden Sie Informationen unter Registrierung bei Citrix Cloud.

  Citrix hat alle vorhandenen AutoDiscovery-Datensätze ohne Betriebsunterbrechung in Citrix Cloud migriert. Die migrierten Datensätze werden nicht automatisch in der neuen Konsole angezeigt. Sie müssen Domänen im neuen AutoDiscovery-Dienst zurückfordern, um die Inhaberschaft nachzuweisen. Weitere Informationen finden Sie unter CTX312339.

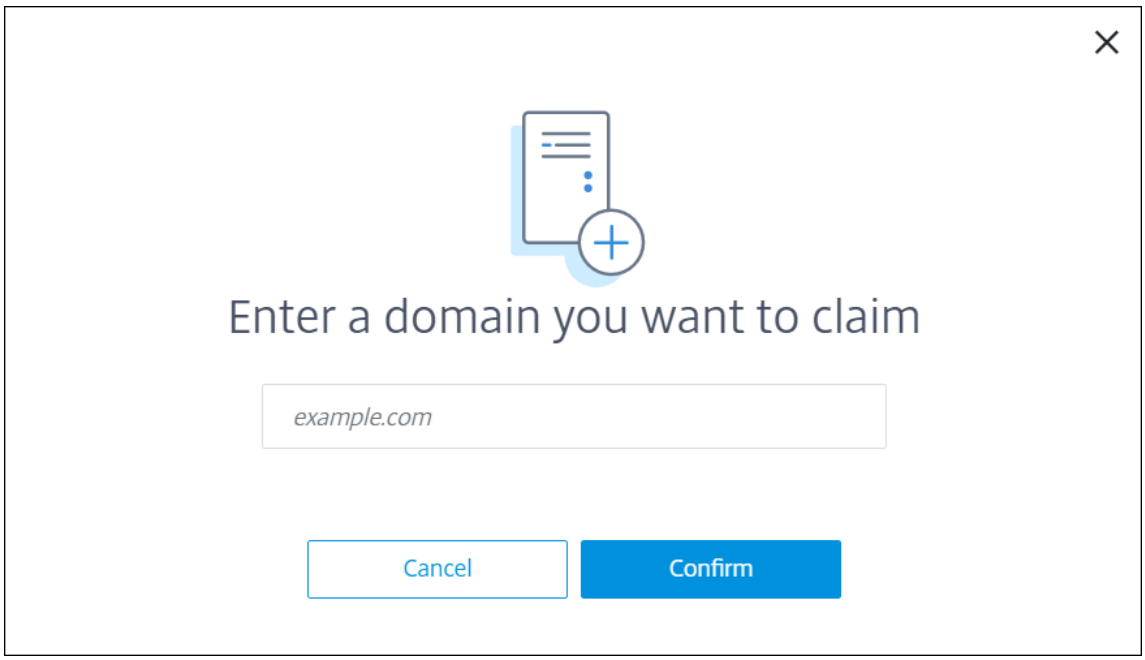
- Bevor Sie den Autodiscoverydienst für Ihre Endpoint Management-Bereitstellungen verwenden, müssen Sie Ihre Domäne verifizieren und beanspruchen. Sie können bis zu 10 Domänen beanspruchen. Die verifizierte und beanspruchte Domäne wird dann mit dem Autodiscoverydienst verknüpft. Um mehr als 10 Domänen zu beanspruchen, erstellen Sie ein SRE-Ticket oder kontaktieren Sie den technischen Support von Citrix.
- Verwenden Sie die Einstellung MAM-Port anstelle von Citrix Gateway-FQDN, um MAM-Datenverkehr an Ihr Datencenter zu leiten. Wenn Sie einen vollqualifizierten Domänennamen zusammen mit dem Port von Citrix Gateway eingeben, verwendet das Clientgerät die Konfiguration aus der Einstellung **MAM-Port**.
- Wenn ein Werbeblocker das Öffnen der Site verhindert, müssen Sie ihn für die gesamte Website deaktivieren.

Beanspruchen einer Domäne

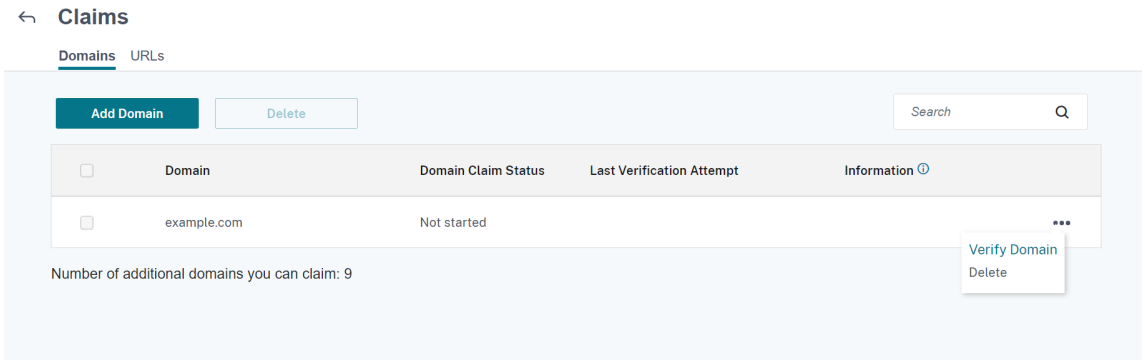
1. Klicken Sie auf der Registerkarte **Ansprüche > Domänen** auf **Domäne hinzufügen**.



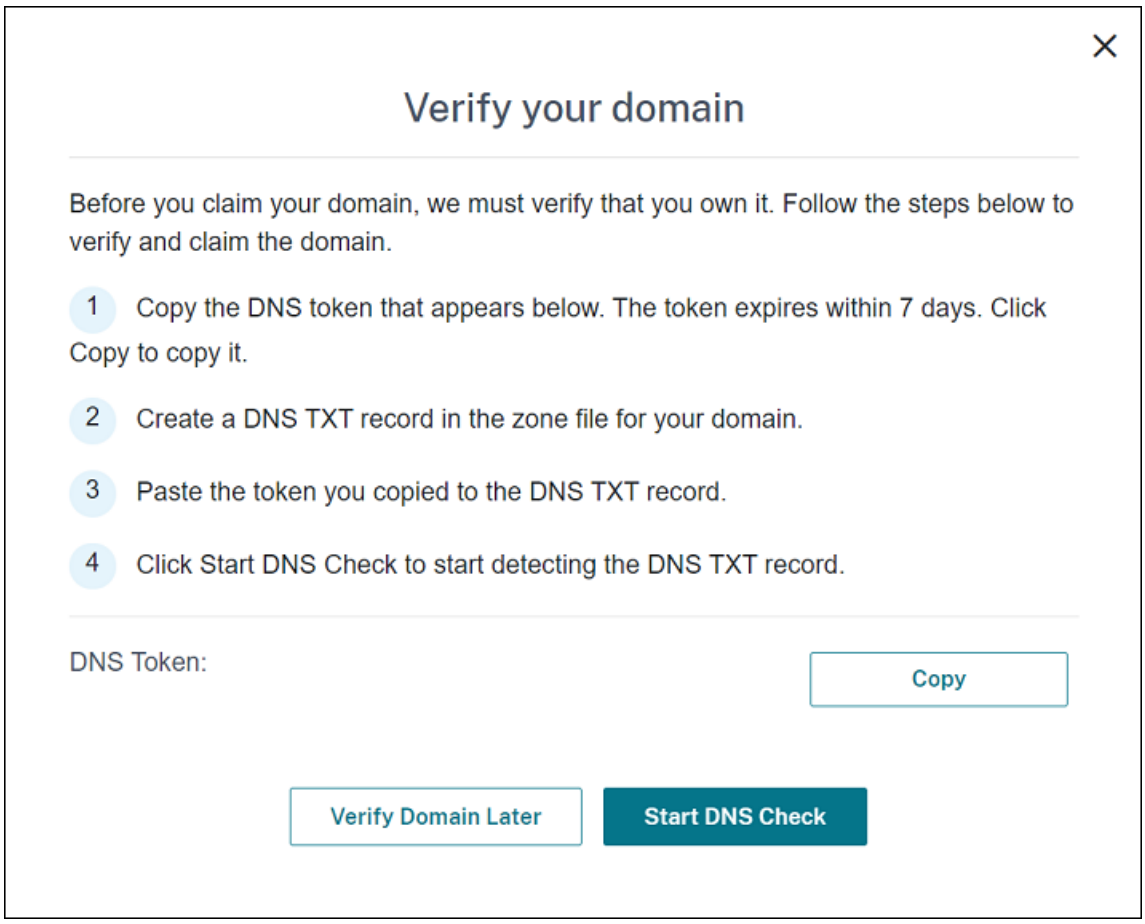
2. Geben Sie in dem Dialogfeld, das geöffnet wird, den Domänennamen Ihrer XenMobile-Umgebung ein und klicken Sie dann auf **Bestätigen**. Ihre Domäne wird unter **Ansprüche > Domänen** angezeigt.



3. Klicken Sie in der hinzugefügten Domäne auf die Auslassungspunkte (…) und wählen Sie **Domäne überprüfen**, um die Verifizierung zu starten. Die Seite **Überprüfen Ihrer Domäne** wird angezeigt.



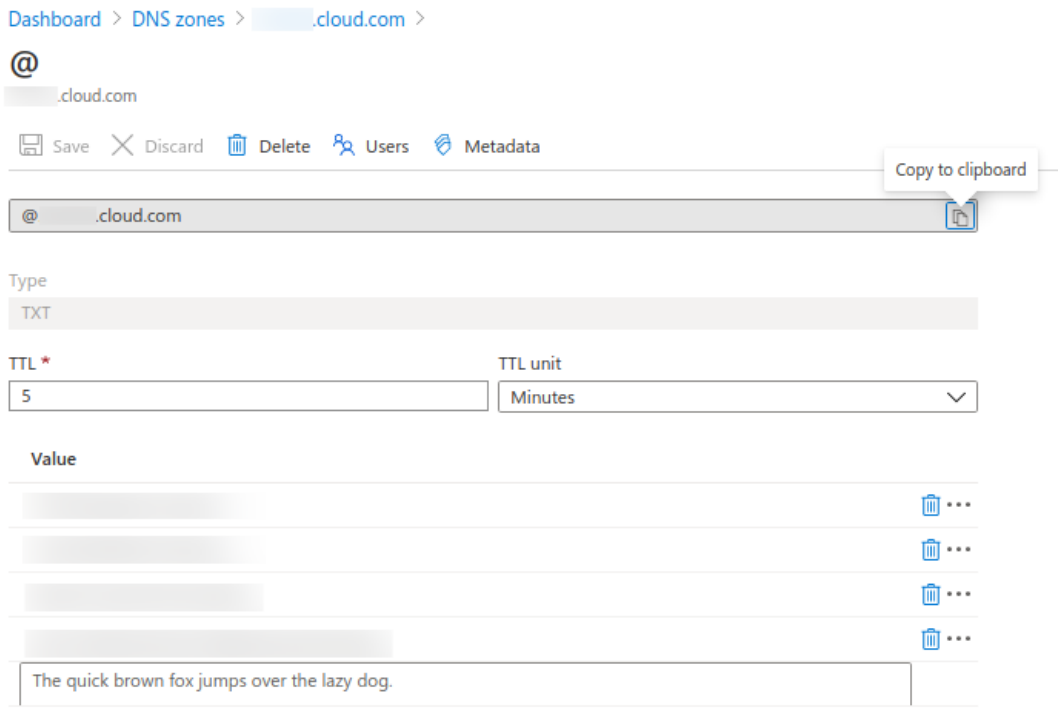
4. Folgen Sie auf der Seite **Überprüfen Ihrer Domäne** den Anweisungen, um zu verifizieren, dass Sie die Domäne besitzen.



a) Klicken Sie auf **Kopieren**, um den DNS-Token in die Zwischenablage zu kopieren.

b) Erstellen Sie einen DNS-TXT-Datensatz in der Zonendatei für Ihre Domäne. Gehen Sie dazu zum Portal Ihres Domänenhostinganbieters und fügen Sie den kopierten DNS-Token hinzu.

   Der folgende Screenshot zeigt ein Portal des Domänenhostinganbieters an. Ihr Portal kann anders aussehen.



c) Klicken Sie in Citrix Cloud auf der Seite **Überprüfen Ihrer Domäne** auf **DNS-Prüfung starten**, damit Ihr DNS-TXT-Datensatz erkannt wird. Wenn Sie die Domäne später überprüfen möchten, klicken Sie auf **Domäne später überprüfen**.

Die Überprüfung dauert in der Regel rund eine Stunde. Es kann jedoch bis zu zwei Tage dauern, bis eine Rückmeldung erfolgt. Sie können sich während der Statusüberprüfung abmelden und erneut anmelden.

Nach Abschluss der Konfiguration ändert sich der Status Ihrer Domäne von **Ausstehend** in **Verifiziert**.

5. Nachdem Sie Ihre Domäne beansprucht haben, geben Sie Informationen zum Autodiscoverydienst ein. Klicken Sie auf die Auslassungspunkte (…) der hinzugefügten Domäne und dann auf die Option zum **Hinzufügen von Endpoint Management-Informationen**. Die Seite **Informationen zum Autodiscoverydienst** wird angezeigt.
6. Geben Sie die folgenden Informationen ein und klicken Sie auf **Speichern**.
   - **Server-FQDN für Endpoint Management:** Geben Sie den vollqualifizierten Domänennamen von XenMobile Server ein. Beispiel: `example.xm.cloud.com`. Diese Einstellung wird für MDM- und MAM-Datenverkehr verwendet.
   - **Citrix Gateway-FQDN:** Geben Sie den vollqualifizierten Domänennamen von Citrix Gateway in der Form FQDN oder FQDN:Port ein. Beispiel: `example.com`. Diese

Einstellung wird verwendet, um MAM-Verkehr an Ihr Datencenter zu leiten. Bei Nur-MDM-Bereitstellungen lassen Sie dieses Feld leer.

> **Hinweis:**
>
> Citrix empfiehlt, dass Sie die Einstellung **MAM-Port** anstelle von **Citrix Gateway-FQDN** verwenden, um MAM-Datenverkehr zu steuern. Wenn Sie einen vollqualifizierten Domänennamen zusammen mit dem Port von Citrix Gateway eingeben, verwendet das Clientgerät die Konfiguration aus der Einstellung **MAM-Port**.

- **Instanzname:** Geben Sie den Instanznamen von XenMobile Server ein, den Sie oben konfiguriert haben. Wenn Sie sich bezüglich Ihres Instanznamens nicht sicher sind, sollten Sie den Standardwert **zdm** übernehmen.
- **MDM-Port:** Geben Sie den Port ein, der für den MDM-Datenverkehr und die MDM-Registrierung verwendet werden soll. Für Cloud-basierte Dienste lautet die Standardeinstellung 443.
- **MAM-Port:** Geben Sie den Port ein, der für MAM-Datenverkehr, MAM-Registrierung, iOS-Registrierung und App-Enumeration verwendet werden soll. Für Cloud-basierte Dienste lautet die Standardeinstellung 8443.

Anfordern von AutoDiscovery für Windows-Geräte

Wenn Windows-Geräte registriert werden sollen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie eine Supportanfrage beim Citrix Support, um Windows AutoDiscovery zu aktivieren.
2. Beziehen Sie ein öffentlich signiertes SSL-Zertifikat ohne Platzhalter für `enterpriseenrollment.mycompany.com`. Der Teil `mycompany.com` ist die Domäne mit den Konten, die die Benutzer für die Registrierung verwenden. Senden Sie das SSL-Zertifikat in PFX-Format und das zugehörige Kennwort im Anhang Ihrer Supportanfrage.

   Wenn Sie mehrere Domänen zum Registrieren von Windows-Geräten verwenden möchten, können Sie auch ein Multidomänen-Zertifikat mit der folgenden Struktur verwenden:

   - 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.)
3. 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.xm.cloud.com zu.

Wenn sich ein Windows-Gerätebenutzer mit einem UPN anmeldet, führt der Citrix Registrierungsserver Folgendes aus:

- Bereitstellung der Details von XenMobile Server.
- Anweisen des Geräts, ein gültiges Zertifikat von XenMobile anzufordern.

An diesem Punkt können Sie alle unterstützten Geräte registrieren. Fahren Sie mit dem nächsten Abschnitt fort, um die Bereitstellung von Ressourcen für Geräte vorzubereiten.

Geräterichtlinien

January 5, 2022

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 zusammenfassende Beschreibung jeder Geräterichtlinie finden Sie unter Übersicht über Geräterichtlinien in diesem Artikel.

> **Hinweis:**
>
> Bei Konfiguration Ihrer Umgebung mit Gruppenrichtlinienobjekten (GPOs):
>
> Berücksichtigen Sie die folgende Regel beim Konfigurieren der XenMobile-Geräterichtlinien für Windows 10- und Windows 11-Geräte. Wenn eine Richtlinie auf einem oder mehreren registrierten Geräten Konflikte verursacht, hat die an das GPO angepasste Richtlinie Vorrang.

Informationen zu den vom Android Enterprise-Container unterstützten Richtlinien finden Sie unter Android Enterprise.

Voraussetzungen

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

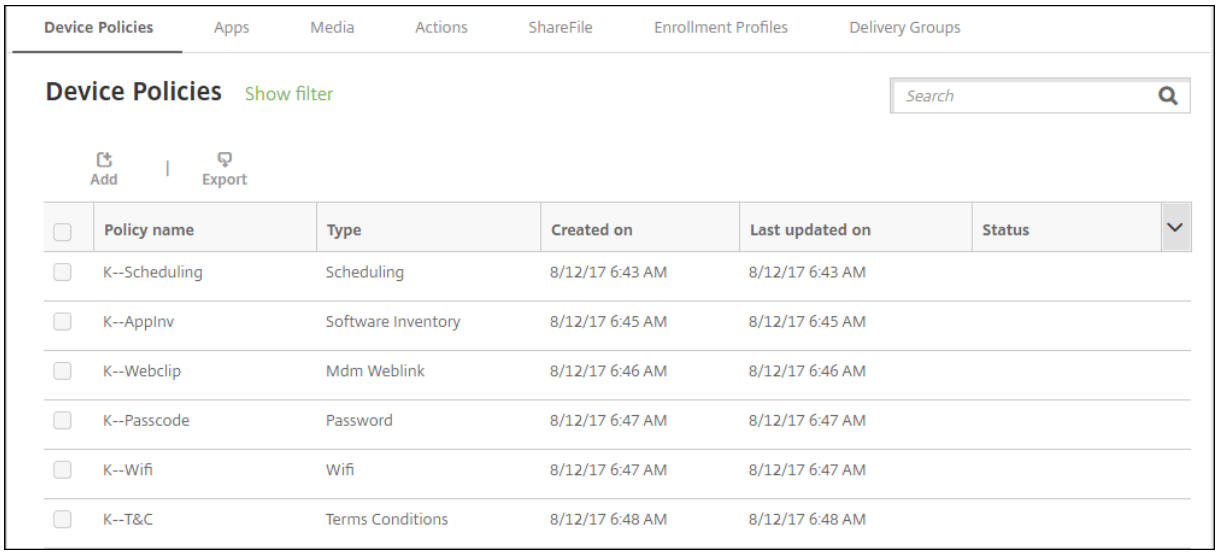
Hinzufügen einer Geräterichtlinie

Das Erstellen einer Geräterichtlinie besteht im Wesentlichen aus folgenden Schritten:

1. Benennen und Beschreiben der Richtlinie
2. Konfigurieren der Richtlinie für eine oder mehrere Plattformen
3. Erstellen von Bereitstellungsregeln (optional)

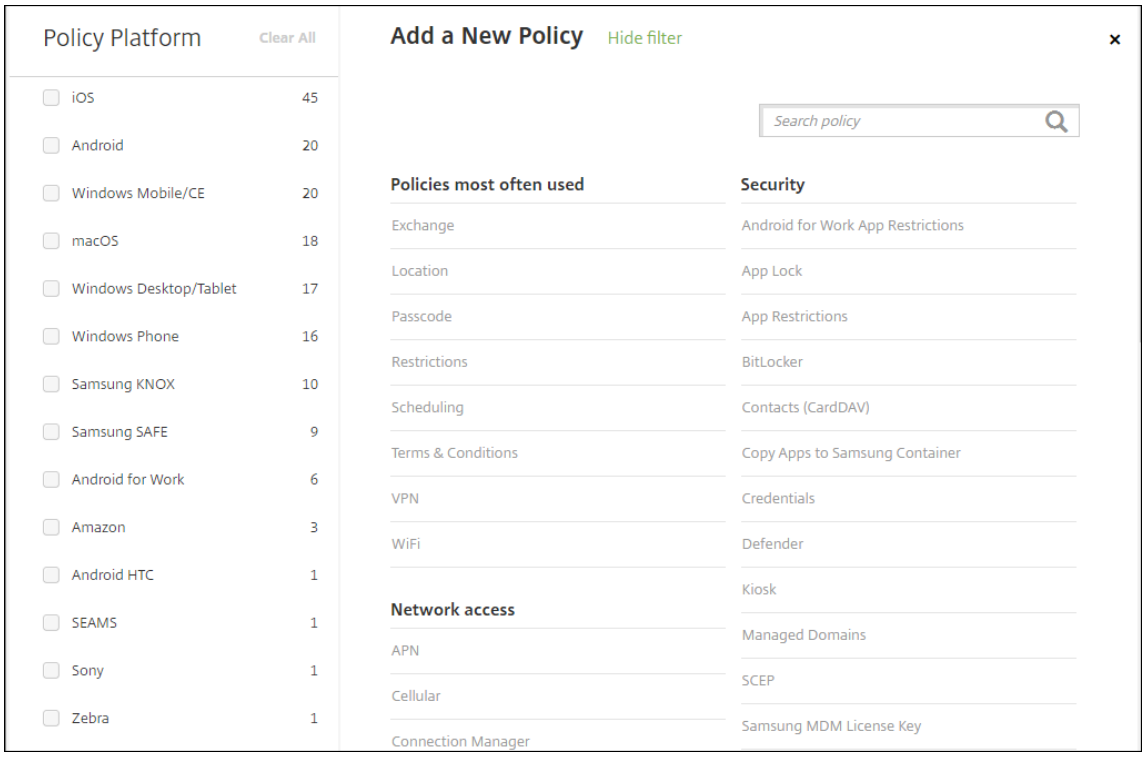
4. Zuweisen der Richtlinie zu Bereitstellungsgruppen
5. Konfigurieren des Bereitstellungszeitplans (optional)

Zum Erstellen und Verwalten der Geräterichtlinien gehen Sie zu **Konfigurieren > Geräterichtlinien**.



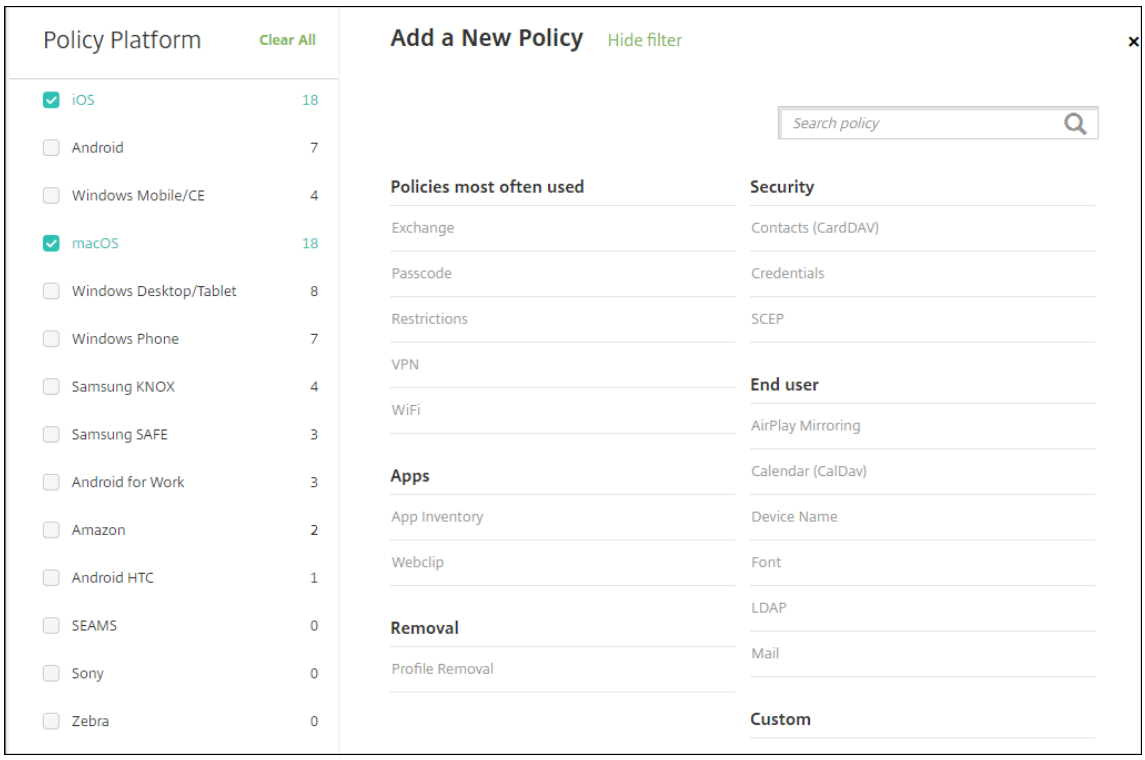
Hinzufügen einer Richtlinie

1. Klicken Sie auf der Seite **Geräterichtlinien** auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.



2. Klicken Sie auf eine oder mehrere Plattformen, um die zugehörigen Richtlinien anzuzeigen.

Klicken Sie auf eine Richtlinie, um das Hinzufügen fortzusetzen.



Sie können auch den Namen der Richtlinie in das Suchfeld eingeben. Während der Eingabe werden die möglichen Treffer eingeblendet. Wenn die Richtlinie in der Liste ist, klicken Sie darauf. Nur die ausgewählte Richtlinie verbleibt in den Suchergebnissen. Klicken Sie darauf, um die Seite **Richtlinieninformationen** für diese Richtlinie zu öffnen.

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.
4. Geben Sie die erforderlichen Informationen auf der Seite **Policy Information** ein und klicken Sie dann auf **Next**. 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. Eine Richtlinie kann je nach Plattform unterschiedlich sein. Nicht alle Richtlinien gelten für alle Plattformen.

   Einige Seiten enthalten Tabellen mit Elementen. Zum Löschen eines vorhandenen Elements zeigen Sie auf dessen Zeile und klicken auf das Papierkorbsymbol auf der rechten Seite. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**.

   Zum Bearbeiten eines Eintrags zeigen Sie auf dessen Zeile und klicken auf das Stiftsymbol auf der rechten Seite.

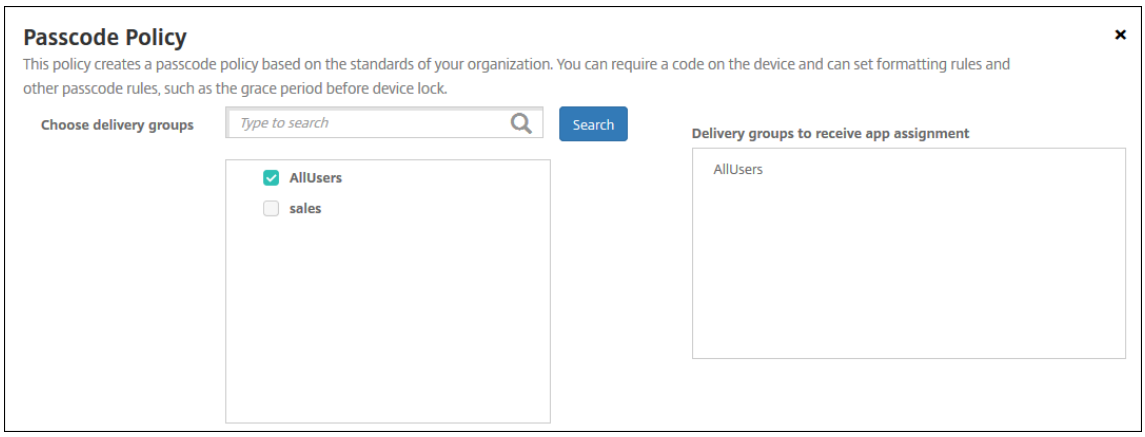
Konfigurieren von Bereitstellungsregeln, Zuweisungen und Zeitplan

Weitere Informationen zum Konfigurieren der Bereitstellungsregeln finden Sie unter Bereitstellen von Ressourcen.

1. Erweitern Sie auf einer Plattformseite **Bereitstellungsregeln** und konfigurieren Sie folgende Einstellungen. Standardmäßig wird die Registerkarte **Basis** angezeigt.
   - Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist **Alle**.
   - Klicken Sie auf **Neue Regel**, um Bedingungen zu definieren.
   - Klicken Sie in der Liste auf Bedingungen wie **Gerätebesitz** oder **BYOD**.
   - Klicken Sie erneut auf **Neue Regel**, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte **Erweitert**, um die Regeln mit booleschen Optionen zu kombinieren. Die Bedingungen, die Sie auf der Registerkarte **Basis** ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   - Klicken Sie auf **UND**, **ODER** oder **NICHT**.
   - Wählen Sie in den Listen die Bedingungen aus, die der Regel hinzugefügt werden sollen. Klicken Sie anschließend rechts auf das Pluszeichen (**+**), um die Bedingung zur Regel hinzuzufügen.

     Sie können jederzeit auf eine Bedingung und dann auf **BEARBEITEN** klicken, um die Bedingung zu ändern, oder auf **Löschen**, um die Bedingung zu löschen.
   - Klicken Sie auf **Neue Regel**, um eine weitere Bedingung hinzuzufügen.
4. Klicken Sie auf **Weiter**, um zur nächsten Plattformseite bzw., wenn alle Plattformseiten ausgefüllt sind, zur Seite **Zuweisung** zu gehen.
5. Wählen Sie auf der Seite **Assignments** die Bereitstellungsgruppen aus, auf die die Richtlinie angewendet werden soll. Wenn Sie auf eine Bereitstellungsgruppe klicken, wird deren Name im Feld **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

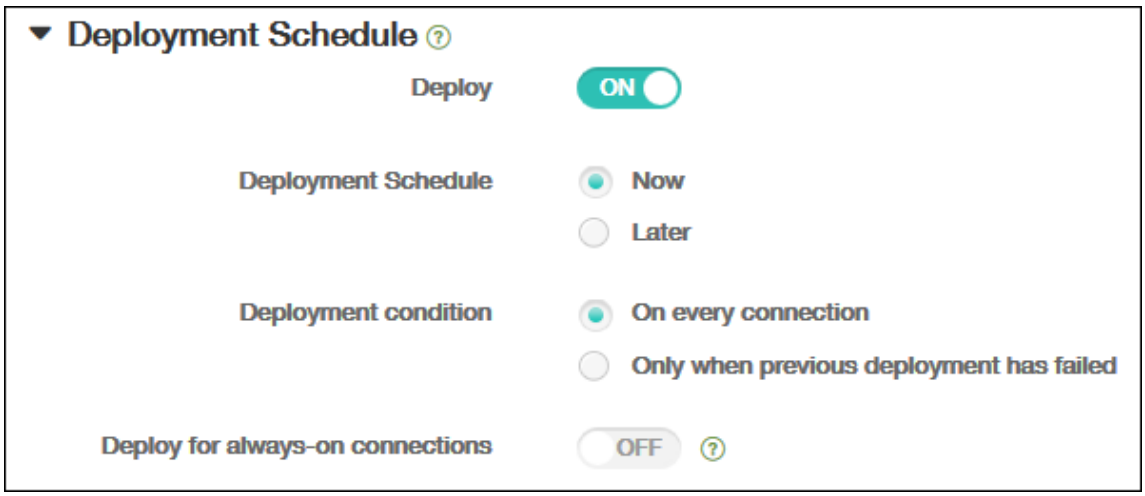
   Das Feld **Bereitstellungsgruppen für App-Zuweisung** wird erst eingeblendet, wenn Sie auf eine Bereitstellungsgruppe klicken.



6. Erweitern Sie auf der Seite **Zuweisung** die Option **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**.
   - 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 konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.



7. Klicken Sie auf **Speichern**.

   Die Richtlinie wird in der Tabelle **Geräterichtlinien** angezeigt.

Entfernen einer Geräterichtlinie von einem Gerät

Die Schritte zum Entfernen einer Geräterichtlinie von einem Gerät sind plattformabhängig.

- Android

  Zum Entfernen einer Geräterichtlinie von einem Android-Gerät verwenden Sie die Geräterichtlinie "XenMobile-Deinstallation". Weitere Informationen finden Sie unter XenMobile-Deinstallationsrichtlinie.

- iOS und macOS

  Zum Entfernen einer Geräterichtlinie von einem iOS- oder macOS-Gerät verwenden Sie die Geräterichtlinie für Profilentfernung. Auf iOS- und macOS-Geräten sind alle Richtlinien Bestandteil des MDM-Profils. Daher können Sie eine Geräterichtlinie für Profilentfernung nur für die Richtlinie erstellen, die Sie entfernen möchten. Die übrigen Richtlinien und das Profil verbleiben auf dem Gerät. Weitere Informationen finden Sie unter Geräterichtlinie für Profilentfernung.

- Windows 10 und Windows 11

  Sie können eine Geräterichtlinie nicht direkt von einem Windows-Desktop- oder -Tablet entfernen. Verwenden Sie stattdessen eine der folgenden Methoden:

  - Heben Sie die Registrierung des Geräts auf und übertragen Sie einen neuen Richtliniensatz an das Gerät. Benutzer registrieren sich dann neu, um fortzufahren.
  - Übertragen Sie eine Sicherheitsaktion, um das Gerät selektiv zu löschen. Mit dieser Aktion werden sämtliche Unternehmensapps und -daten vom Gerät entfernt. Anschließend

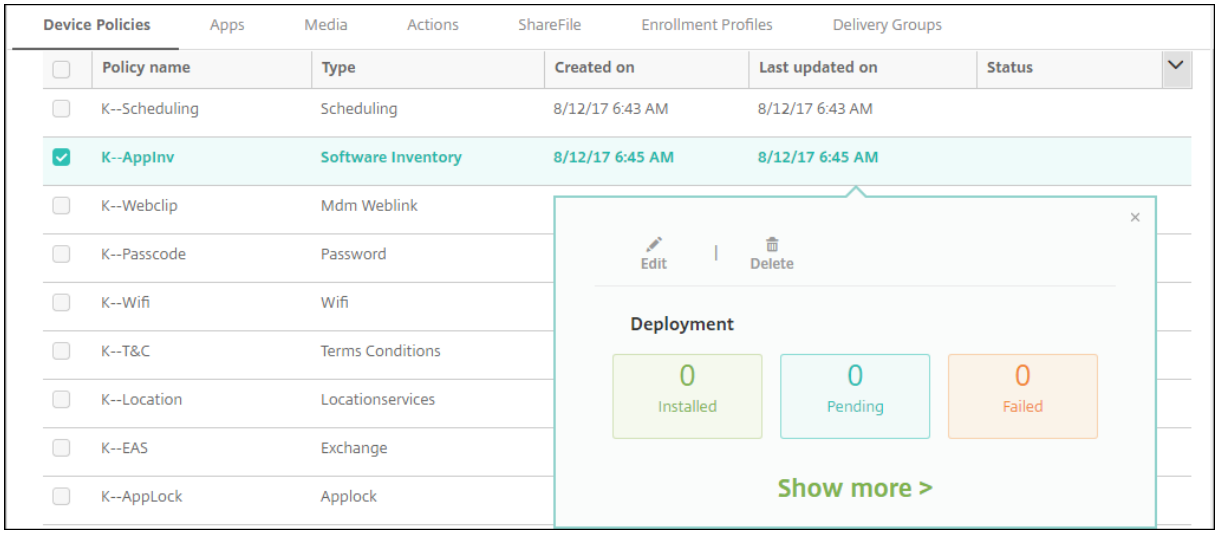
entfernen Sie die Geräterichtlinie aus einer Bereitstellungsgruppe, die nur dieses Gerät enthält, und übertragen die Bereitstellungsgruppe an das Gerät. Benutzer registrieren sich dann neu, um fortzufahren.

- Chrome OS

  Zum Entfernen einer Geräterichtlinie von einem Chrome OS-Gerät können Sie die Geräterichtlinie aus einer Bereitstellungsgruppe entfernen, die nur dieses Gerät enthält. Anschließend übertragen Sie die Bereitstellungsgruppe an das Gerät.

Bearbeiten einer Geräterichtlinie

Zum Bearbeiten einer Richtlinie aktivieren Sie das Kontrollkästchen neben der Richtlinie, um das Menü der Optionen oberhalb der Richtlinienliste anzuzeigen. Sie können auch auf eine Richtlinie in der Liste klicken, um das Menü mit den Optionen rechts daneben anzuzeigen.



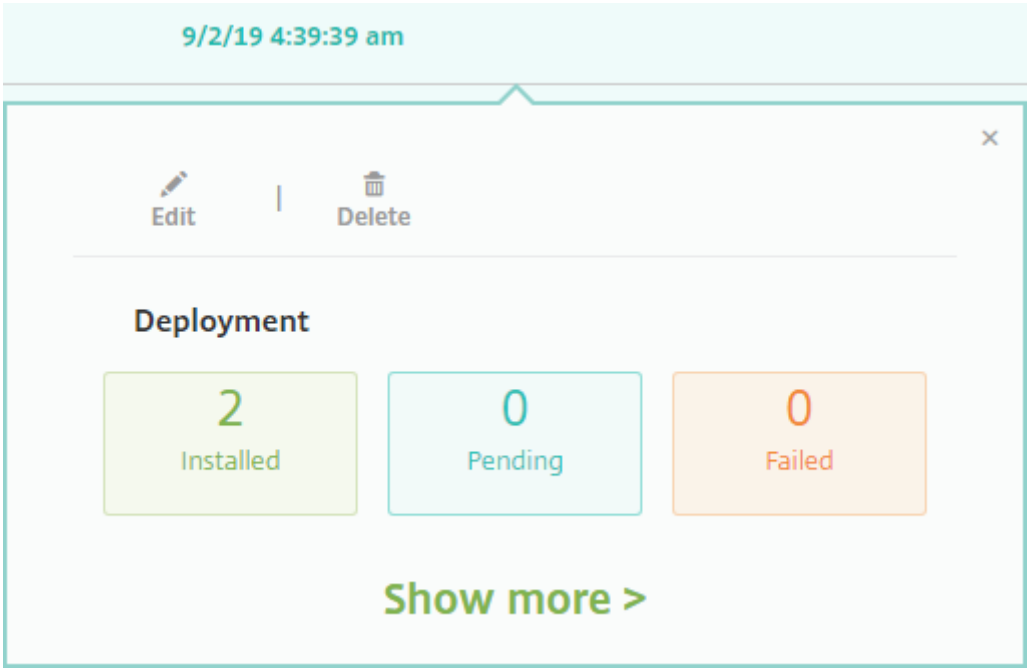
Um Details zur Richtlinie anzuzeigen, klicken Sie auf **Mehr anzeigen**.

Um alle Standardeinstellungen für eine Geräterichtlinie zu bearbeiten, klicken Sie auf **Bearbeiten**.

Wenn Sie auf **Löschen** klicken, wird ein Bestätigungsdialogfeld angezeigt. Klicken Sie erneut auf **Löschen**, um die Richtlinie zu löschen.

Überprüfen des Richtlinienbereitstellungstatus

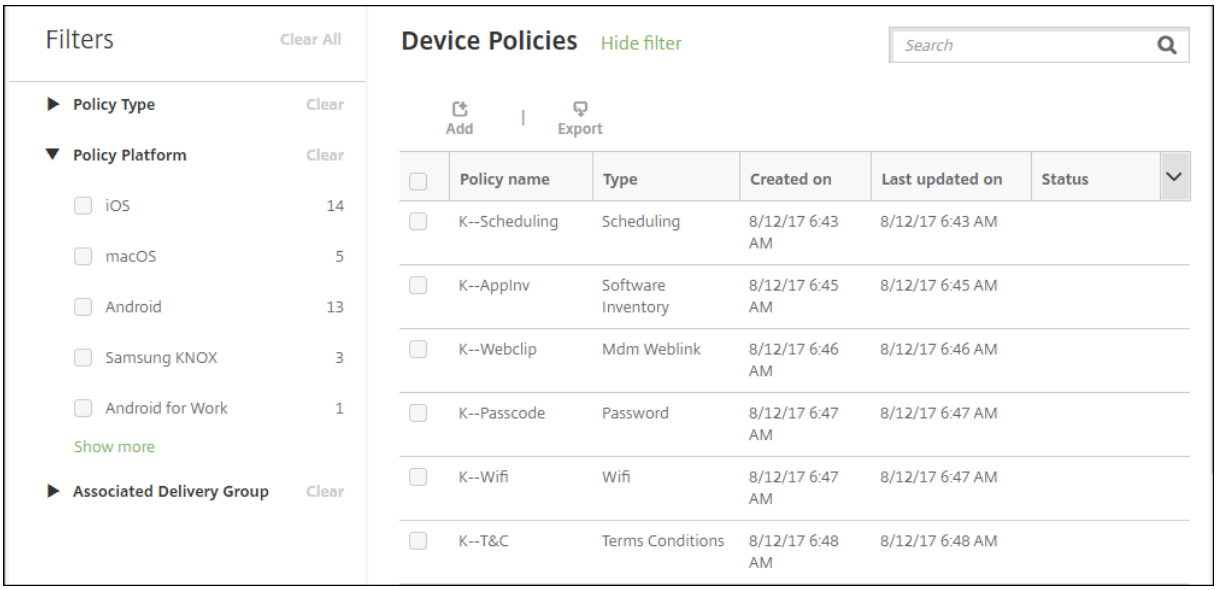
Klicken Sie auf der Seite **Konfigurieren > Geräterichtlinien** auf eine Richtlinienzeile, um den Bereitstellungsstatus zu überprüfen.



Bei ausstehender Bereitstellung einer Richtlinie können Benutzer die Richtlinie über Secure Hub aktualisieren, indem sie auf **Einstellungen > Geräteinformationen > Richtlinie aktualisieren**tippen.

Filtern der Liste hinzugefügter Geräterichtlinien

Sie können die Liste der hinzugefügten Richtlinien nach Richtlinientyp, Plattform und zugeordneter Bereitstellungsgruppe filtern. Klicken Sie auf der Seite **Konfigurieren > Geräterichtlinien** auf **Filter einblenden**. Aktivieren Sie in der Liste die Kontrollkästchen der Elemente, die Sie anzeigen möchten.



Klicken Sie auf **Diese Ansicht speichern**, um den Filter zu speichern. Der Name des Filters wird dann

auf einer Schaltfläche unter der Schaltfläche **Diese Ansicht speichern** angezeigt.

Übersicht über Geräterichtlinien

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
AirPlay-Synchronisierung	Hiermit fügen Sie bestimmte AirPlay-Geräte (z. B. einen weiteren Mac-Computer) zu iOS-Geräten hinzu. Sie können Geräte auch einer Positivliste für betreute Geräte hinzuzufügen. Benutzer sind dann auf die AirPlay-Geräte auf der Positivliste beschränkt.
AirPrint	Hiermit fügen Sie AirPrint-Drucker der AirPrint-Druckerliste auf iOS-Geräten hinzu. Diese Richtlinie erleichtert die Pflege von Umgebungen, bei denen Drucker und Geräte in verschiedenen Subnetzen sind.
App-Berechtigungen in Android Enterprise	Hiermit können Sie konfigurieren, was geschieht, wenn Android Enterprise-Apps in Firmenprofilen Berechtigungsanfragen erhalten, die von Google als “gefährlich” eingestuft werden.
App-Einschränkungen in Android Enterprise	Hiermit aktualisieren Sie die Einschränkungen für Android-Apps.
APN	Hiermit definieren Sie die Einstellungen für die Verbindung zwischen den Geräten und dem General Packet Radio Service (GPRS) eines Netzbetreibers. Diese Einstellung ist bei den meisten neuen Telefonen bereits definiert. Verwenden Sie diese Richtlinie, wenn Ihr Unternehmen keinen Consumer-APN verwendet, über den mit Mobilgeräten eine Verbindung zum Internet hergestellt werden kann.
App-Zugriff	Definiert eine Liste der Apps, die auf dem Gerät erforderlich, optional verfügbar oder gesperrt sind. Sie können dann eine automatisierte Aktion erstellen, mit der die Reaktion auf die Richtlinientreue von Geräten gesteuert wird.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
App-Attribute	Hiermit geben Sie Attribute für iOS-Geräte an (z. B. eine Paket-ID für die verwaltete App oder die ID für den VPN-Zugriff pro App).
App-Konfiguration	Hiermit konfigurieren Sie für Apps, die eine verwaltete Konfiguration unterstützen, verschiedene Einstellungen und Verhaltensweisen. Dazu wird eine XML-Konfigurationsdatei (eine sogenannte Eigenschaftenliste oder “plist”) auf iOS-Geräten bereitgestellt. Oder Sie stellen Schlüssel/Wert-Paare auf Windows 10-Telefonen bzw. Desktops oder Tablets bereit, auf denen Windows 10 oder Windows 11 ausgeführt werden.
App-Bestand	Hiermit können Sie einen Bestand der Apps auf verwalteten Geräten abrufen. XenMobile vergleicht dann die vorhandenen Apps mit den App-Zugriffsrichtlinien, die auf diesen Geräten bereitgestellt sind. Auf diese Weise können Sie Apps erkennen, die auf einer App-Positivliste oder einer App-Sperrliste stehen, und entsprechende Maßnahmen ergreifen.
App-Sperre	Hiermit definieren Sie eine Liste von Apps, die Benutzer auf iOS- oder bestimmten Android-Geräten ausführen oder nicht ausführen können.
App-Netzwerkauslastung	Hiermit legen Sie Netzwerkauslastungsregeln fest, um vorzugeben, wie Netzwerke, z. B. mobile Datennetzwerke, 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.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
App-Einschränkungen	Hiermit werden Sperrlisten für Apps erstellt, die nicht von Benutzern auf Samsung Knox-Geräten installiert werden sollen. Sie können auch Positivlisten für Apps erstellen, die Benutzer installieren dürfen.
App-Deinstallation	Hiermit entfernen Sie Apps von Benutzergeräten.
Einschränkungen für App-Deinstallation	Hiermit geben Sie die Apps an, die Benutzer deinstallieren können, sowie die Apps, die sie nicht deinstallieren dürfen.
App-Benachrichtigungen	Hiermit steuern Sie, wie iOS-Benutzer Benachrichtigungen von bestimmten Apps erhalten.
Verwaltete Apps automatisch aktualisieren	Steuert, wie installierte verwaltete Apps auf Android Enterprise-Geräten aktualisiert werden.
BitLocker	Hiermit werden die auf der BitLocker-Benutzeroberfläche auf Windows 10- und Windows 11-Geräten angebotenen Einstellungen konfiguriert.
Browser	Hiermit legen Sie fest, ob der Browser auf den Benutzergeräten verwendet werden kann und welche Browserfunktionen verfügbar sind.
Kalender (CalDAV)	Hiermit wird auf iOS- oder macOS-Geräten ein Kalenderkonto (CalDAV) hinzugefügt. Mit dem CalDAV-Konto können Benutzer Kalendereinträge mit jedem Server synchronisieren, der CalDAV unterstützt.
Mobilfunk	Hiermit werden mobile Netzwerkeinstellungen konfiguriert.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Verbindungsmanager	Hiermit 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)	Hiermit wird auf iOS- oder macOS-Geräten ein iOS-Kontaktkonto (CardDAV) hinzugefügt. Mit dem CardDAV-Konto können Benutzer Kontaktdaten mit jedem Server synchronisieren, der CardDAV unterstützt.
OS-Update steuern	Hiermit werden aktuelle Betriebssystemupdates auf unterstützten, betreuten Geräten bereitgestellt.
Apps in Samsung Container kopieren	Hiermit werden für unterstützte Samsung-Geräte die bereits auf dem Gerät installierten Apps in einen KNOX-Container kopiert. Apps im KNOX-Container sind nur dann verfügbar, wenn die Benutzer sich beim KNOX-Container anmelden.
Anmeldeinformationen	Ermöglicht eine in die Public Key-Infrastruktur in XenMobile integrierte Authentifizierung. Dies kann beispielsweise eine PKI-Entität, ein Schlüsselspeicher, ein Anmeldeinformationsanbieter oder ein Serverzertifikat sein.
Benutzerdefiniertes XML	Hiermit können Sie Features wie das Geräteprovisioning, die Gerätefeatureaktivierung, die Gerätekonfiguration und die Fehlerverwaltung anpassen.
Defender	Hiermit werden Windows Defender-Einstellungen für Windows 10 und Windows 11 für Desktops und Tablets konfiguriert.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Dateien und Ordner löschen	Hiermit werden bestimmte Dateien und Ordner von Windows Mobile-/CE-Geräten gelöscht.
Registrierungsschlüssel und -werte löschen	Hiermit werden bestimmte Registrierungsschlüssel und -werte von Windows Mobile-/CE-Geräten gelöscht.
Device Health Attestation	Hiermit wird festgelegt, dass Windows 10- und Windows 11-Geräte ihren Integritätsstatus melden. Dazu senden sie bestimmte Daten und Laufzeitinformationen zur Analyse an den Health Attestation Service (HAS). 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 konfiguriert haben.
Gerätename	Hiermit werden die Namen für iOS- und macOS-Geräte festgelegt. Sie können Makros, Text oder eine Kombination daraus verwenden, um einen Gerätenamen festzulegen.
Bildungseinrichtung - Konfiguration	Hiermit werden die Geräte von Lehrkräften und Lernenden zur Verwendung der Apple-Bildungprodukte konfiguriert werden. Wenn Lehrkräfte die Classroom-App verwenden, ist die Geräterichtlinie “Bildung - Konfiguration” erforderlich.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Unternehmenshub	Hiermit werden Apps über den Unternehmenshub-Unternehmensstore an Windows Phone-Geräte verteilt. XenMobile unterstützt nur eine Unternehmenshubrichtlinie für einen Modus von Windows Phone-Secure Hub. So dürfen Sie beispielsweise nicht mehrere Unternehmenshubrichtlinien mit verschiedenen Versionen von Secure Hub für XenMobile Enterprise Edition erstellen. Sie können nur die erste Unternehmenshubrichtlinie bei der Geräteregistrierung bereitstellen.
Exchange	Hiermit aktivieren Sie ActiveSync-E-Mail für den systemeigenen E-Mail-Client auf dem Gerät.
Dateien	Hiermit fügen Sie XenMobile Skriptdateien hinzu, um bestimmte Funktionen für Benutzer auszuführen. Sie können auch Dokumentdateien hinzufügen, die Benutzern von Android-Geräten auf ihren Geräten zugänglich sein sollen. Beim Hinzufügen einer Datei können Sie festlegen, in welchem Verzeichnis diese auf dem Gerät gespeichert werden soll.
FileVault	Mit dieser Richtlinie können Sie die FileVault-Geräteverschlüsselung auf registrierten macOS-Geräten aktivieren. Außerdem können Sie festlegen, wie oft ein Benutzer das Einrichten von FileVault bei der Anmeldung überspringen kann. Für macOS 10.7 und höher verfügbar.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Firewall	Hiermit werden Firewalleinstellungen konfiguriert. Geben Sie IP-Adressen, Ports und Hostnamen an, die Sie auf Geräten blockieren oder zulassen möchten. Sie können außerdem die Proxy- und Proxyumleitungseinstellungen konfigurieren.
Schriftart	Hiermit fügen Sie iOS- und macOS-Geräten zusätzliche Schriftarten hinzu. Schriftarten müssen im Format TrueType (.ttf) oder OpenType (.oft) vorliegen. XenMobile bietet keine Unterstützung für Schriftsammlungen (.ttc oder .otc).
Layout für Homebildschirm	Gibt das Layout von Apps und Ordnern für den iOS-Homebildschirm auf betreuten iOS-Geräten der Version 9.3 und höher an.
Importieren von iOS- und macOS-Profilen	Hiermit importieren Sie XML-Dateien für die Konfiguration von iOS- und macOS-Geräten in XenMobile. Die Datei enthält Gerätesicherheitsrichtlinien und -einschränkungen, die Sie mit Apple Configurator vorbereitet haben.
Keyguard-Verwaltung	Steuert die Funktionen, die Benutzern zur Verfügung stehen, bevor sie den Geräte-Keyguard und den Arbeitsprofil-Keyguard entsperren. Sie können Geräte-Keyguardfunktionen auch für vollständig verwaltete und dedizierte Geräte steuern. Beispielsweise können Sie Sperrbildschirmfunktionen wie “Entsperren per Fingerabdruck”, “Trust Agents” und “Benachrichtigungen” deaktivieren.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Kiosk	Hiermit beschränken Sie die Verwendung von Apps auf Samsung SAFE-Geräten. Sie können den Einsatz vorhandener Apps auf eine oder mehrere Apps begrenzen. 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 im Kioskmodus angezeigt werden sollen.
Launcher-Konfiguration	Hiermit legen Sie die Einstellungen für Citrix Launcher auf Android-Geräten fest, z. B. zugelassene Apps und ein benutzerdefiniertes Logobild als Launcher-Symbol.
LDAP	Diese Richtlinie bietet Informationen zum LDAP-Server für iOS-Geräte und alle erforderlichen Kontoinformationen, beispielsweise den Hostnamen des LDAP-Servers. Die Richtlinie umfasst auch eine Reihe von LDAP-Suchrichtlinien für Abfragen beim LDAP-Server.
Standort	Hiermit können Sie den Standort der Geräte auf einer Karte abrufen, vorausgesetzt auf dem Gerät ist GPS für Secure Hub aktiviert. Nach dem Bereitstellen dieser Richtlinie auf dem Gerät können Sie einen Ortungsbefehl von XenMobile Server senden. Das Gerät antwortet dann mit den Standortkoordinaten. XenMobile unterstützt auch Richtlinien zum Geofencing und Gerätetracking.
E-Mail	Hiermit wird ein E-Mail-Konto auf iOS- oder macOS-Geräten konfiguriert.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Verwaltete Domänen	Hiermit werden verwaltete Domänen für E-Mail und den Safari-Browser definiert. Mit verwalteten Domänen können Sie zum Schutz von Unternehmensdaten steuern, welche Apps Dokumente, die mit Safari heruntergeladen wurden, öffnen können. Für betreute iOS-Geräte der Version 8 und höher können Sie mithilfe von URLs oder Unterdomänen festlegen, wie Benutzer Dokumente, Anlagen und über den Browser heruntergeladene Objekte öffnen können.
MDM-Optionen	Hiermit wird die Aktivierungssperre des Features “Mein iPhone/iPad suchen” auf betreuten Geräten mit iOS 7.0 und höher verwaltet.
Informationen zum Unternehmen	Hiermit geben Sie die Unternehmensinformationen für Warnmeldungen an, die von XenMobile auf iOS-Geräten bereitgestellt werden.
Passcode	Hiermit können Sie einen PIN-Code oder ein Kennwort auf einem verwalteten Gerät erzwingen. Sie können die Komplexität des Passcodes und Timeouts auf dem Gerät einstellen.
Persönlicher Hotspot	Hiermit können Benutzer sich auch dann mit dem Internet verbinden, wenn sie nicht in Reichweite eines WLAN-Netzwerks sind. Benutzer können das Feature für persönliche Hotspots auf dem iOS-Gerät nutzen, um eine Internetverbindung per Mobilnetz herzustellen.
Profilentfernung	Hiermit wird das App-Profil von iOS- bzw. macOS-Geräten entfernt.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Provisioningprofil	Hiermit legen Sie ein Provisioningprofil zur Unternehmensverteilung fest, das dann an Geräte gesendet wird. Bei Entwicklung und Codesignatur einer iOS-Unternehmensapp fügen Sie in der Regel auch ein Provisioningprofil hinzu. Dieses Profil ist erforderlich, damit die App auf einem iOS-Gerät ausgeführt werden kann. Wenn das Provisioningprofil fehlt oder abgelaufen ist, stürzt die App ab, wenn der Benutzer darauf tippt.
Entfernen des Provisioningprofils	Hiermit werden iOS-Provisioningprofile entfernt.
Proxy	Hiermit können Sie globale HTTP-Proxyeinstellungen für Geräte mit Windows Mobile/CE und iOS festlegen. Sie können nur eine globale HTTP-Proxyrichtlinie pro Gerät bereitstellen.
Registrierung	Hiermit werden die Registrierungsschlüssel und -werte zum Verwalten von Windows Mobile-/CE-Geräten definiert. In der Registrierung von Windows Mobile und Windows CE werden Daten zu Apps, Treibern, Benutzereinstellungen und Konfigurationseinstellungen gespeichert.
Remotesupport	Diese Richtlinie ermöglicht den Remotezugriff auf Samsung KNOX-Geräte. Remote Support ist ab dem 1. Januar 2019 für Neukunden nicht mehr verfügbar. Bestehende Kunden können das Produkt weiterhin verwenden, Citrix stellt jedoch keine Neuerungen oder Fixes bereit.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Einschränkungen	Diese Richtlinie bietet unzählige Möglichkeiten, Features und Funktionalität auf verwalteten Geräten zu steuern und zu sperren. Einschränkungsoptionen sind beispielsweise das Deaktivieren der Kamera oder des Mikrofons, das Durchsetzen von Roamingregeln und ein gesteuerter Zugriff auf Drittanbieterdienste, wie App-Stores.
Roaming	Hiermit können Sie vorgeben, ob auf iOS- bzw. Windows Mobile-/CE-Geräten das Sprach- und Datenroaming zugelassen wird. Bei deaktiviertem Sprachroaming wird das Datenroaming ebenfalls automatisch deaktiviert.
Samsung MDM-Lizenzschlüssel	Hiermit wird der integrierte Samsung Enterprise License Management-Schlüssel (ELM) festgelegt, der auf Geräten bereitgestellt werden muss, bevor Sie SAFE-Richtlinien und -Einschränkungen bereitstellen können. XenMobile unterstützt zudem den Dienst Samsung E-FOTA (Enterprise Firmware-Over-The-Air). XenMobile unterstützt und erweitert Samsung for Enterprise- (SAFE) und Samsung KNOX-Richtlinien.
Planung	Diese Richtlinie ist für Android- und Windows Mobile-Geräte erforderlich, damit sie für MDM-Verwaltung, App-Push und Richtlinienbereitstellung erneut eine Verbindung mit XenMobile Server herstellen. Wenn Sie diese Richtlinie nicht an Geräte senden und Google FCM nicht aktiviert haben, kann das Gerät keine Verbindung mit dem Server herstellen.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
SCEP	Hiermit können Sie iOS- und macOS-Geräte für den Empfang eines Zertifikats von einem externen SCEP-Server konfigurieren. Sie können Zertifikate auch mit SCEP von einer mit XenMobile verbundenen PKI an das Gerät übermitteln. Erstellen Sie dazu eine PKI-Entität und einen PKI-Anbieter im verteilten Modus.
SSO-Konto	Hiermit erstellen Sie Single Sign-On-Konten (SSO), damit Benutzer nach einmaliger Anmeldung auf XenMobile und interne Unternehmensressourcen zugreifen können. Sie müssen keine Anmeldeinformationen auf dem Gerät speichern. Die Unternehmensanmeldeinformationen eines SSO-Kontos werden von XenMobile für alle Apps verwendet, einschließlich Apps aus dem App-Store. Diese Richtlinie ist mit der Kerberos-Authentifizierung kompatibel. Verfügbar für iOS.
Speicherverschlüsselung	Hiermit verschlüsseln Sie den internen und externen Speicher. Bei einigen Geräten wird hiermit verhindert, dass Benutzer eine Speicherkarte auf ihren Geräten verwenden.
Abonnierte Kalender	Hiermit wird der Kalenderliste auf iOS-Geräten ein abonnierter Kalender hinzugefügt. Denken Sie daran, dass Sie einen Kalender zunächst abonnieren müssen, bevor Sie ihn der Liste der abonnierten Kalender auf den Geräten der Benutzer hinzufügen können.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
AGB	Diese Richtlinie erfordert, dass Benutzer die Richtlinien Ihres Unternehmens akzeptieren, die den Zugriff auf das Unternehmensnetzwerk regeln. Wenn Benutzer ihr Gerät bei XenMobile registrieren, müssen sie die Nutzungsbestimmungen akzeptieren, damit sie ihr Gerät registrieren können. Lehnen sie die Nutzungsbedingungen ab, wird die Registrierung abgebrochen.
Tunnel zulassen	Diese Richtlinie wird nur für den Remotesupport verwendet. Durch Remote Support können Helpdesk-Mitarbeiter die Fernsteuerung verwalteter Windows CE- und Android-Mobilgeräte übernehmen. Remotesupport ist nicht für geclusterte on-premises XenMobile Server-Bereitstellungen verfügbar. Remote Support ist ab dem 1. Januar 2019 für Neukunden nicht mehr verfügbar. Bestehende Kunden können das Produkt weiterhin verwenden, Citrix stellt jedoch keine Neuerungen oder Fixes bereit.
VPN	Diese Richtlinie ermöglicht den Zugriff auf Back-End-Systeme, die Legacy-VPN-Gatewaytechnologie verwenden. Die VPN-Gateway-Verbindungsinformationen ermöglichen die Bereitstellung auf Geräten. XenMobile unterstützt mehrere VPN-Anbieter, darunter Cisco AnyConnect, Juniper und Citrix VPN. Wenn Ihr VPN-Gateway diese Option unterstützt, kann diese Richtlinie mit einer Zertifizierungsstelle verbunden und VPN bei Bedarf aktiviert werden.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Hintergrundbild	Hiermit wird eine PNG- oder JPG-Datei hinzugefügt, um Hintergrundbilder auf dem Sperr- und/oder Homebildschirm von iOS-Geräten festzulegen. Zum Verwenden verschiedener Hintergrundbilder auf iPads und iPhones erstellen Sie unterschiedliche Richtlinien, die Sie dann den entsprechenden Benutzern bereitstellen.
Webinhaltsfilter	Hiermit werden Webinhalte auf iOS-Geräten gefiltert. XenMobile verwendet die automatische Filterfunktion von Apple in Verbindung mit Ihren Sperr- und Positivlisten für Websites. Nur verfügbar für betreute iOS-Geräte.
Webclip	Hiermit platzieren Sie Verknüpfungen (“Webclips”) zu Websites, sodass sie neben den Apps auf den Benutzergeräten angezeigt werden. Für iOS-, macOS- und Android-Geräte können Sie Symbole für die Webclips angeben. Bei Windows-Tablets sind nur eine Beschriftung und eine URL erforderlich.
Wi-Fi	Diese Richtlinie ermöglicht Administratoren das Bereitstellen von WiFi-Routerdetails auf verwalteten Geräten. Die Routerdetails umfassen die SSID sowie Authentifizierungs- und Konfigurationsdaten.
Windows CE-Zertifikat	Hiermit werden Windows Mobile-/CE-Zertifikate von einer externen PKI erstellt und auf Benutzergeräten bereitgestellt.
Windows Information Protection	Hiermit werden die Anwendungen angegeben, die Windows Information Protection erfordern, und es wird die Erzwingungsebene festgelegt. Die Richtlinie gilt für betreute Geräte mit Windows 10 und Windows 11.

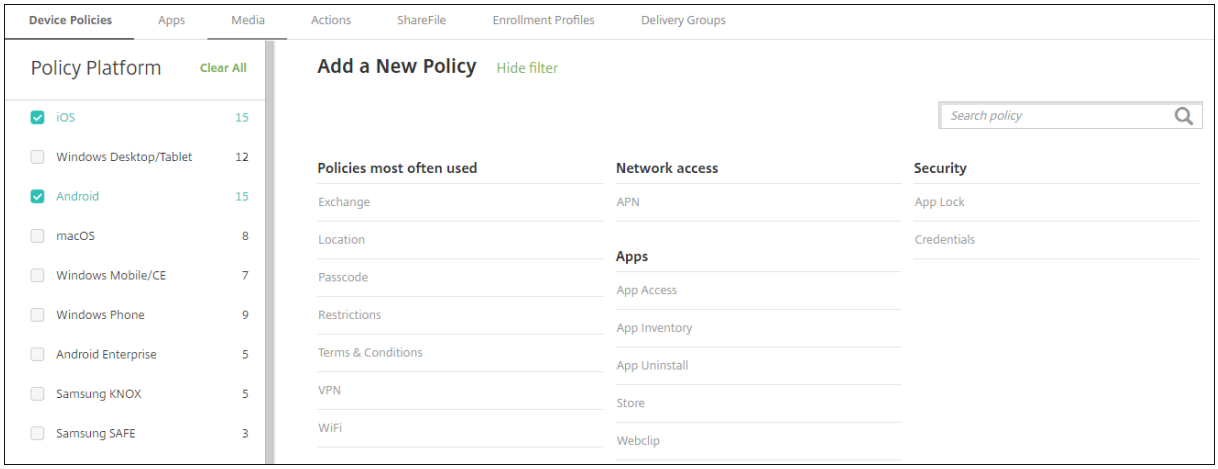
Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
XenMobile Store	Hiermit geben Sie an, ob ein Webclip des XenMobile Store auf dem Homebildschirm von Benutzergeräten angezeigt wird.
XenMobile-Optionen	Hiermit konfigurieren Sie das Secure Hub-Verhalten für Verbindungen zwischen XenMobile und Android- bzw. Windows Mobile-/CE-Geräten.
XenMobile-Deinstallation	Hiermit können Sie XenMobile von Android- und Windows Mobile-/CE-Geräten deinstallieren. Wenn diese Richtlinie bereitgestellt wird, entfernt sie XenMobile von allen Geräten in der Bereitstellungsgruppe.

Geräterichtlinien nach Plattform

January 5, 2022

Anzeige der pro Plattform verfügbaren Richtlinien:

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Jede Geräteplattform wird in einer Liste im Bereich **Richtlinienplattform** angezeigt. Wenn dieser Bereich nicht geöffnet ist, klicken Sie auf **Filter einblenden**.
4. Um eine Liste aller für eine Plattform verfügbaren Richtlinien anzuzeigen, wählen Sie die Plattform aus. Um eine Liste der Richtlinien anzuzeigen, die für mehrere Plattformen verfügbar sind, wählen Sie jede dieser Plattformen aus. Eine Richtlinie wird dann nur in der Liste angezeigt, wenn sie für jede ausgewählte Plattform gilt.



Die aktuelle Version von XenMobile unterstützt Geräterichtlinien für folgende Plattformen:

- Amazon
- Android
- Android Enterprise
- Android Zebra
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Windows 10 und Windows 11 Desktop/Tablet
- Windows 10 Phone
- Windows Mobile/CE

Informationen zu den in der aktuellen Version von XenMobile unterstützten Geräten finden Sie unter Unterstützte Geräteplattformen.

> **Hinweis:**
>
> Bei Konfiguration Ihrer Umgebung mit Gruppenrichtlinienobjekten (GPOs):
>
> Berücksichtigen Sie die folgende Regel beim Konfigurieren der XenMobile-Geräterichtlinien für Windows 10 und Windows 11. Wenn eine Richtlinie auf einem oder mehreren registrierten Geräten Konflikte verursacht, hat die an das GPO angepasste Richtlinie Vorrang.

Geräterichtlinie für die AirPlay-Synchronisierung

January 5, 2022

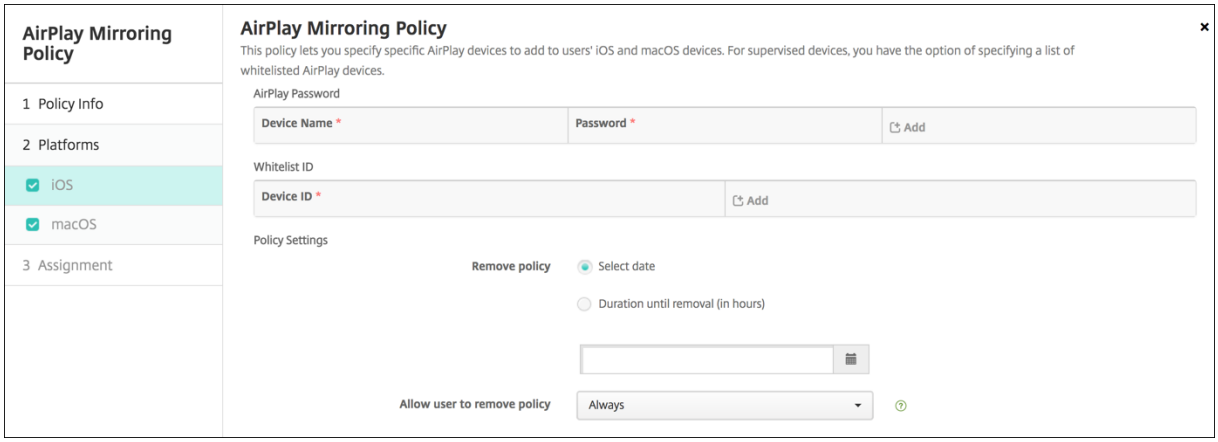
Die Apple AirPlay-Funktion ermöglicht es Benutzern, die Anzeige auf einem Gerätedisplay auf einen anderen Mac-Computer zu übertragen.

Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen spezifischer AirPlay-Geräte (z. B. einen anderen Mac-Computer) einrichten und zu iOS-Geräten hinzufügen. Zudem können Sie Geräte zu einer Positivliste betreuter Geräte hinzufügen, sodass Benutzer nur die AirPlay-Geräte in 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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



- **AirPlay-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:

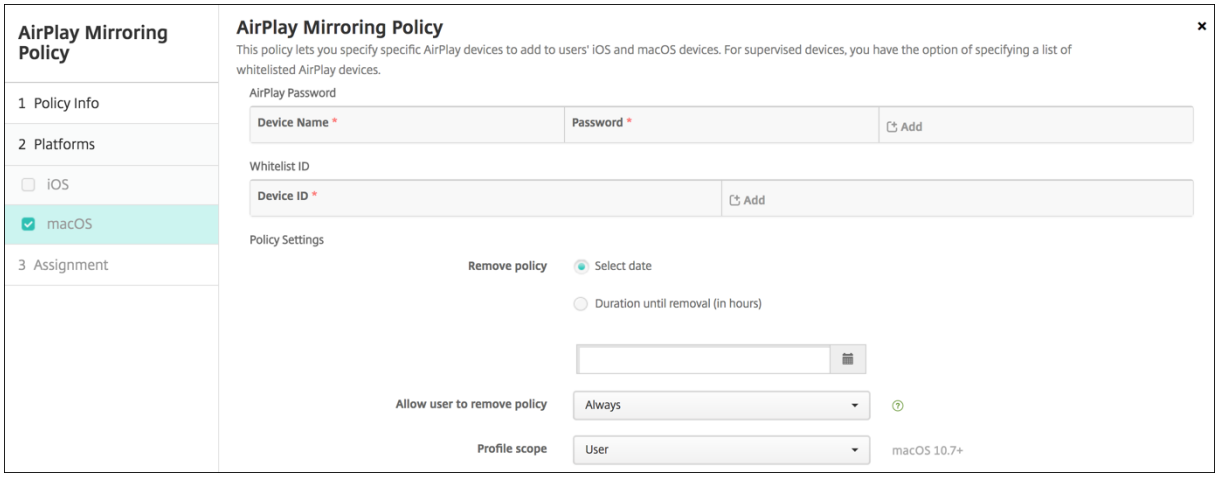
  > **Hinweis:**
  >
  > Die XenMobile Server-Konsole enthält im Englischen die Begriffe “Blacklist” und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe

> (Positiv- und Sperrliste) bleiben unverändert.

  - **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.

- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.

macOS-Einstellungen



- **AirPlay-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 Geräte-IDs 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.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

AirPrint-Geräterichtlinie

April 16, 2020

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.

Die Richtlinie gilt für iOS 7.0 und höher.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die IP-Adresse und den Ressourcenpfad für jeden Drucker haben.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

Richtlinie für verwaltete Android Enterprise-Konfigurationen

January 5, 2022

Mit der Richtlinie für verwaltete Android Enterprise-Konfigurationen können Sie verschiedene App-Konfigurationsoptionen und App-Einschränkungen steuern. Der App-Entwickler legt fest, welche Optionen und QuickInfos für eine App verfügbar sind. Wenn in einer QuickInfo von einem "Vorlagenwert" gesprochen wird, verwenden Sie stattdessen das entsprechende XenMobile-Makro. Weitere Informationen finden Sie unter Remote configuration overview(auf der Android-Entwicklerwebsite) und Makros.

Die App-Konfigurationseinstellungen können folgende Elemente umfassen:

- App-E-Mail-Einstellungen
- Zulassen oder Blockieren von URLs für einen Webbrowser
- Option für eine gesteuerte Synchronisierung von App-Inhalten über eine Mobilfunkverbindung oder nur über eine Wi-Fi-Verbindung

Weitere Informationen zu den Einstellungen für Ihre Apps erhalten Sie vom App-Entwickler.

Voraussetzungen

- Schließen Sie die Aufgaben zum Android Enterprise-Setup auf Google ab und verbinden Sie Android Enterprise mit verwaltetem Google Play. Weitere Informationen finden Sie unter Android Enterprise.

- Hinzufügen von Android Enterprise-Apps in XenMobile Weitere Informationen finden Sie unter Hinzufügen von Apps in XenMobile.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Anforderungen für Pro-App-VPNs

Um ein Pro-App-VPN für AE zu erstellen, müssen Sie zusätzlich zur Konfiguration der Richtlinie "Verwaltete Android Enterprise-Konfigurationen" zusätzliche Schritte ausführen. Außerdem müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- On-Premises Citrix Gateway
- Die folgenden Anwendungen sind auf dem Gerät installiert:
  - Citrix SSO
  - Citrix Secure Hub

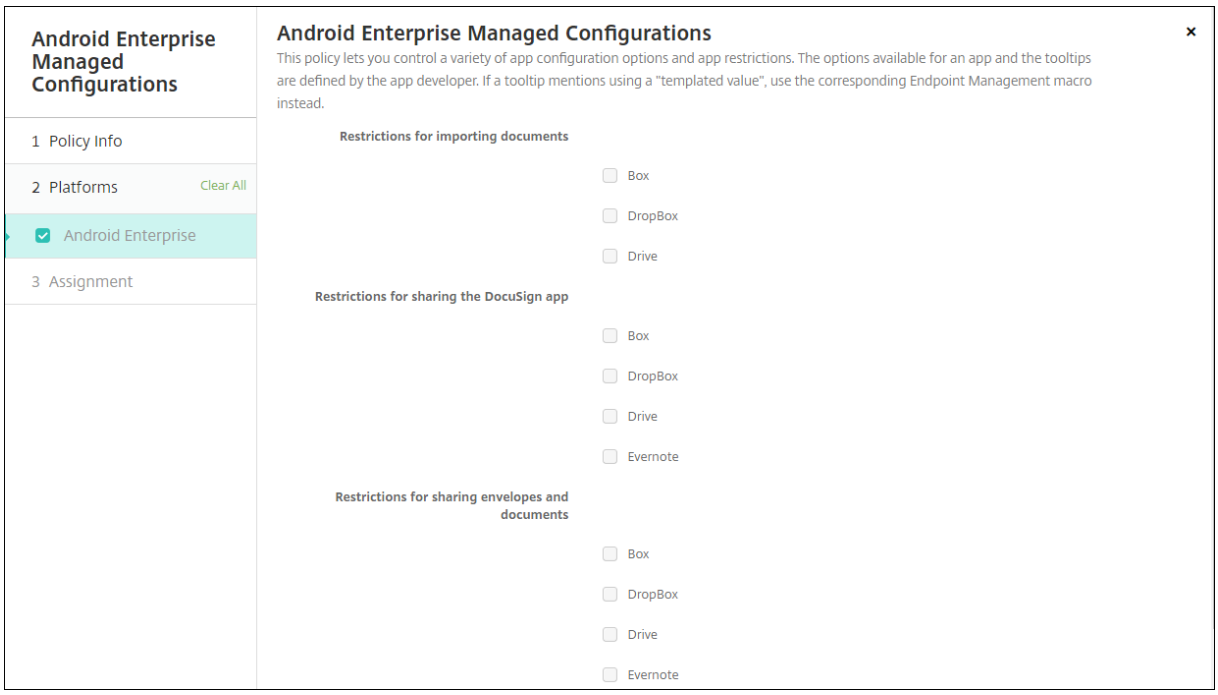
Ein allgemeiner Workflow zur Konfiguration eines Pro-App-VPN für AE-Geräte ist wie folgt:

1. Konfigurieren Sie ein VPN-Profil wie in diesem Artikel beschrieben.
2. Konfigurieren Sie Citrix ADC so, dass es Datenverkehr vom Pro-App-VPN akzeptiert. Weitere Informationen finden Sie unter Setup des vollständigen VPNs in Citrix Gateway.

Android Enterprise-Einstellungen

Nachdem Sie eine Richtlinie für verwaltete Android Enterprise-Konfigurationen hinzugefügt haben, werden Sie zur Auswahl einer App aufgefordert. Wenn XenMobile keine Android Enterprise-Apps hinzugefügt wurden, können Sie nicht fortfahren.

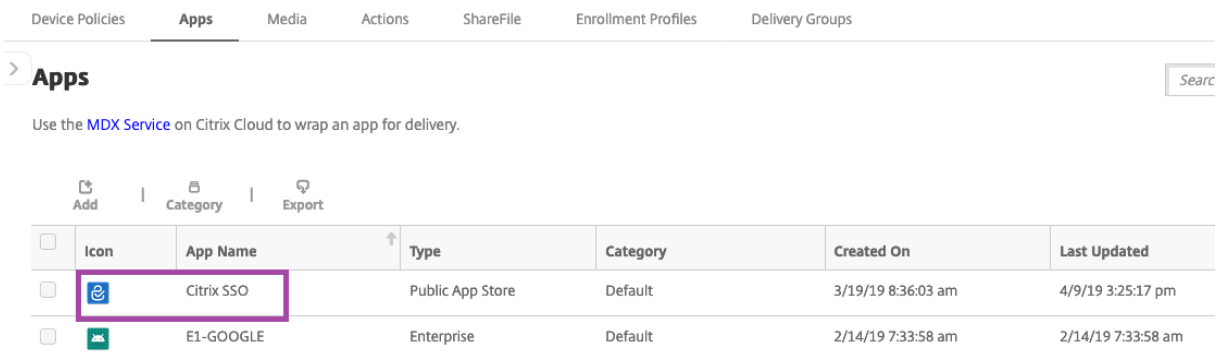
Nachdem Sie eine App ausgewählt haben, konfigurieren Sie die Richtlinieneinstellungen. Die Einstellungen sind App-spezifisch.



Konfigurieren von VPN-Profilen für Android Enterprise

Mit der Citrix SSO-App und der Geräterichtlinie für verwaltete Android Enterprise-Konfigurationen können Sie VPN-Profile für Android Enterprise-Geräte bereitstellen.

Fügen Sie zunächst Citrix SSO als Google Play Store-App zur XenMobile-Konsole hinzu. Siehe Hinzufügen von Apps aus einem öffentlichen App-Store.

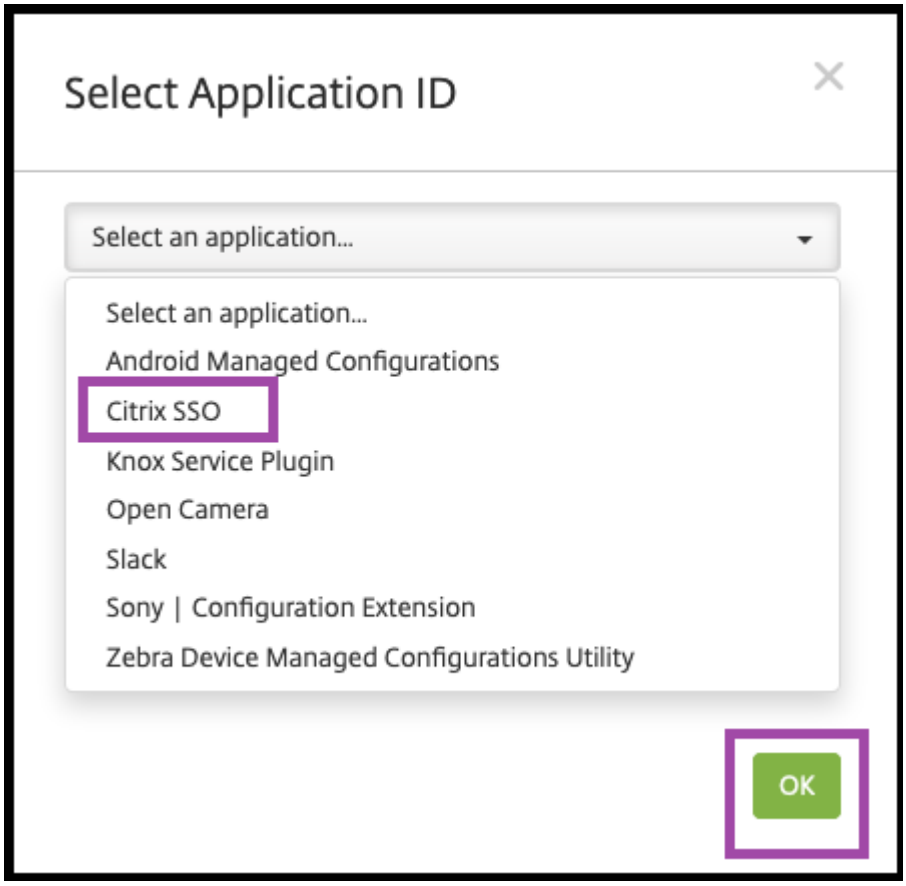


Erstellen einer verwalteten Android Enterprise-Konfiguration für Citrix SSO

Konfigurieren Sie zum Erstellen von VPN-Profilen die Geräterichtlinie für verwaltete Android Enterprise-Konfigurationen für Citrix SSO. Geräte mit installierter Citrix SSO-App und bereitgestellter Richtlinie können auf die von Ihnen erstellten VPN-Profile zugreifen.

Sie benötigen Ihren Citrix Gateway-FQDN und -Port.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**. Klicken Sie auf **Hinzufügen**.
2. Wählen Sie **Android Enterprise**. Klicken Sie auf **Verwaltete Android Enterprise-Konfigurationen**.
3. Im dann angezeigten Fenster **Anwendungs-ID auswählen** wählen Sie **Citrix SSO** aus der Liste aus und klicken auf **OK**.



4. Geben Sie einen Namen und eine Beschreibung für Ihre VPN-Konfiguration mit Citrix SSO ein. Klicken Sie auf **Weiter**.

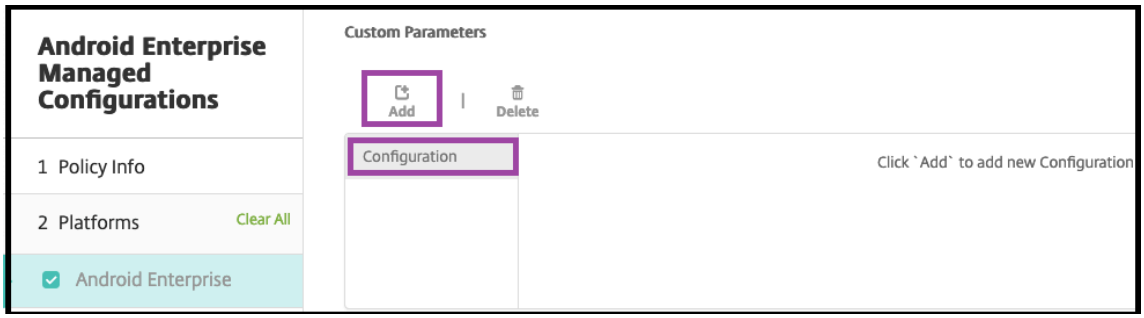
5. Konfigurieren Sie VPN-Profilparameter.

   - **VPN-Profilname.** Geben Sie einen Namen für das VPN-Profil ein. Wenn Sie mehrere VPN-Profile erstellen, verwenden Sie für jedes Profil einen eindeutigen Namen. Wenn Sie keinen Namen angeben, wird die im Feld **Serveradresse** eingegebene Adresse als VPN-Profilname verwendet.
   - **Serveradresse(*).** Geben Sie Ihren Citrix Gateway-FQDN ein. Geben Sie auch den Citrix Gateway-Port ein, wenn Sie nicht Port 443 verwenden. Verwenden Sie das URL-Format. Beispiel: `https://gateway.mycompany.com:8443`.
   - **Benutzername (optional).** Geben Sie den Benutzernamen an, den Endbenutzer für die Authentifizierung beim Citrix Gateway verwenden. Sie können für dieses Feld auch das XenMobile-Makro {user.username} verwenden. (Siehe Makros.) Wenn Sie keinen Benutzernamen angeben, werden Benutzer beim Herstellen einer Verbindung mit Citrix Gateway aufgefordert, einen Benutzernamen anzugeben.
   - **Kennwort (optional).** Geben Sie das Kennwort an, das Endbenutzer für die Authentifizierung beim Citrix Gateway verwenden. Wenn Sie kein Kennwort angeben, werden Benutzer beim Herstellen einer Verbindung mit Citrix Gateway aufgefordert, ein Kennwort anzugeben.
   - **Zertifikatalias (optional).** Geben Sie ein Zertifikatalias ein. Der Zertifikatalias erleichtert der App den Zugriff auf das Zertifikat. Wenn derselbe Zertifikatalias mit der Anmeldeinformationsrichtlinie verwendet wird, ruft die App automatisch das Zertifikat ab und authentifiziert das VPN.
   - **Pro-App-VPN-Typ (optional).** Wenn Sie mit Pro-App-VPN beschränken, welche Apps das VPN verwenden, können Sie diese Einstellung konfigurieren. Bei Auswahl von **Zulassen**

wird der Netzwerkdatenverkehr für die in der **App-Liste für Pro-App-VPN** aufgeführten App-Paketnamen über das VPN geleitet. Der Netzwerkverkehr aller anderen Apps wird nicht über das VPN geleitet. Bei Auswahl von **Nicht zulassen** wird der Netzwerkdatenverkehr für die in der **App-Liste für Pro-App-VPN** aufgeführten App-Paketnamen nicht über das VPN geleitet. Der Netzwerkverkehr aller anderen Apps wird über das VPN geleitet. Die Standardeinstellung ist **Zulassen**.

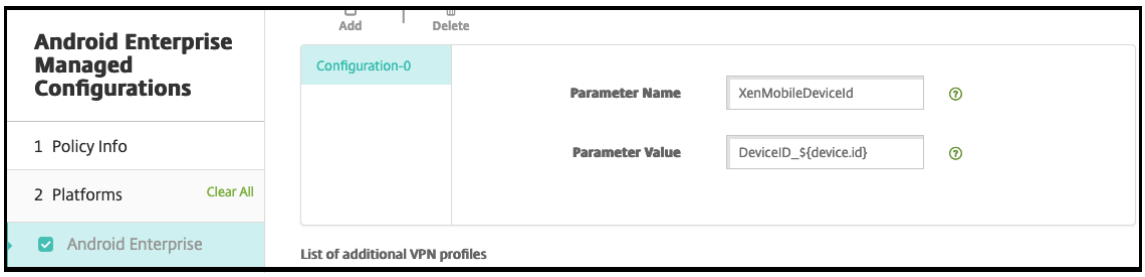
- **App-Liste für Pro-App-VPN.** Eine Liste aller Apps, deren Datenverkehr auf dem VPN zugelassen oder blockiert ist, festgelegt durch den Wert für **Pro-App-VPN-Typ**. Die App-Paketnamen sind durch Kommas oder Semikolons in der Liste getrennt. Die Groß- und Kleinschreibung wird berücksichtigt und die Schreibweise der App-Paketnamen in der Liste müssen mit dem Namen im Google Play Store identisch sein. Diese Liste ist optional. Beim Provisioning eines geräteweiten VPNs lassen Sie die Liste unausgefüllt.
- **VPN-Standardprofil.** Geben Sie den Namen des VPN-Profils ein, das verwendet werden soll, wenn Benutzer in der Benutzeroberfläche der Citrix SSO-App nicht auf ein bestimmtes Profil, sondern auf die Verbindungsoption tippen. Wenn dieses Feld leer gelassen wird, wird das Hauptprofil für die Verbindung verwendet. Wenn nur ein Profil konfiguriert ist, wird es als Standardprofil markiert. Für Always-On-VPN muss dieses Feld auf den Namen des VPN-Profils gesetzt werden, das für das Always-On-VPN verwendet werden soll.
- **Benutzerprofile deaktivieren.** Bei der Einstellung EIN können Benutzer keine eigenen VPNs auf ihren Geräten erstellen. Bei der Einstellung AUS können Benutzer eigene VPNs auf ihren Geräten erstellen. Die Standardeinstellung ist AUS.
- **Nicht vertrauenswürdige Server blockieren.** Wählen Sie die Einstellung “Aus”, wenn Sie ein selbstsigniertes Zertifikat für Citrix Gateway verwenden oder wenn das Stammzertifikat für die Zertifizierungsstelle, die das Citrix Gateway-Zertifikat ausstellt, nicht in der Liste der Systemzertifizierungsstellen aufgeführt ist. Bei der Einstellung “Ein” wird das Citrix Gateway-Zertifikat vom Android-Betriebssystem überprüft. Wenn die Validierung fehlschlägt, wird die Verbindung nicht zugelassen. Der Standardwert ist EIN.

6. Optional können Sie benutzerdefinierte Parameter erstellen. Die benutzerdefinierten Parameter **XenMobileDeviceId** und **UserAgent** werden unterstützt. Wählen Sie die aktuelle VPN-Konfiguration und klicken Sie auf **Hinzufügen**.



   a) Erstellen Sie einen benutzerdefinierten Parameter:

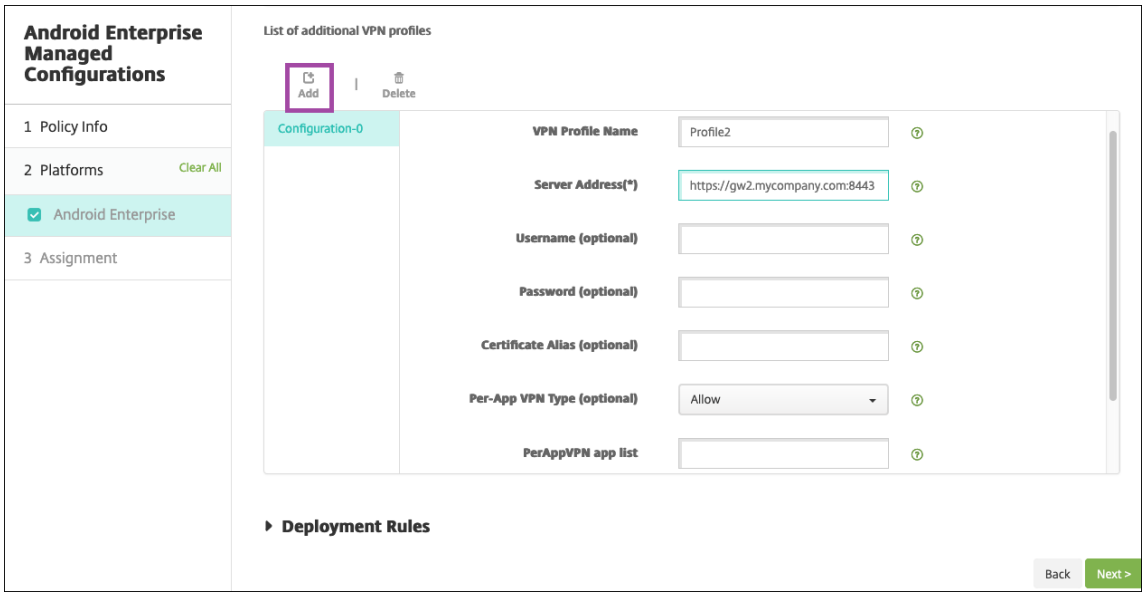
   - **Parametername.** Geben Sie **XenMobileDeviceId** ein. Dies ist die Geräte-ID, die für die Netzwerkzugriffsprüfung basierend auf der Geräteregistrierung in XenMobile verwendet wird. Wenn das Gerät von XenMobile registriert und verwaltet wird, wird die VPN-Verbindung zugelassen. Andernfalls schlägt die Authentifizierung bei der VPN-Einrichtung fehl.
   - **Parameterwert.** Damit der Registrierungs- und Verwaltungsstatus von Geräten in XenMobile bestimmt werden kann, wird der Wert für XenMobileDeviceID auf `DeviceID_${ device.id }` festgelegt.



a) Zum Erstellen eines weiteren benutzerdefinierten Parameters klicken Sie erneut auf **Hinzufügen**. Erstellen Sie diesen benutzerdefinierten Parameter.

- **Parametername.** Geben Sie **UserAgent** ein. Dieser Text wird zur zusätzlichen Prüfung von Citrix Gateway an den User-Agent-HTTP-Header angehängt. Der Wert dieses Textes wird während der Kommunikation mit Citrix Gateway von der Citrix SSO-App an den User-Agent-HTTP-Header angehängt.
- **Parameterwert.** Geben Sie den Text ein, den Sie an den User-Agent-HTTP-Header anhängen möchten. Dieser Text muss den Vorgaben für den HTTP-User-Agent entsprechen.

7. Optional können Sie weitere VPN-Profilkonfigurationen erstellen. Klicken Sie unter der Liste der Konfigurationen auf **Hinzufügen**. Eine neue Konfiguration wird in der Liste angezeigt. Wählen Sie die neue Konfiguration aus und wiederholen Sie Schritt 5 und optional Schritt 6.



8. Wenn Sie alle gewünschten VPN-Profile erstellt haben, klicken Sie auf **Weiter**.
9. Konfigurieren Sie Bereitstellungsregeln für diese verwaltete Konfiguration für Citrix SSO.
10. Klicken Sie auf **Speichern**.

Diese verwaltete Konfiguration für Citrix SSO wird nun in der Liste der konfigurierten Geräterichtlinien angezeigt.

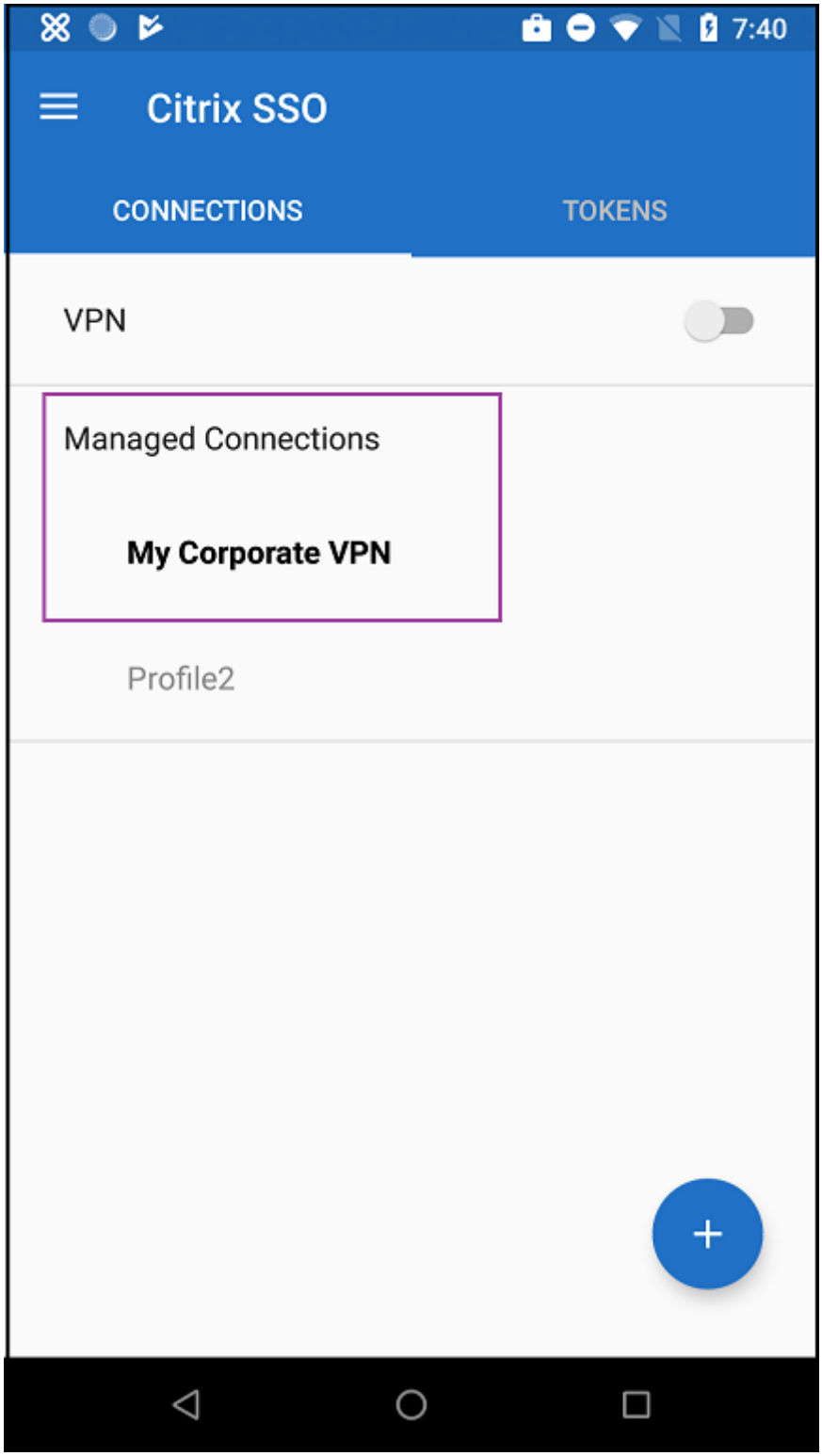
Zum Aktivieren von Always-On für die konfigurierten VPN-Profile, setzen Sie die XenMobile-Optionsrichtlinie für Geräte.

> **Hinweis:**
> Citrix Secure Hub 19.5.5 oder höher ist für Always-On-VPN für Android Enterprise erforderlich.

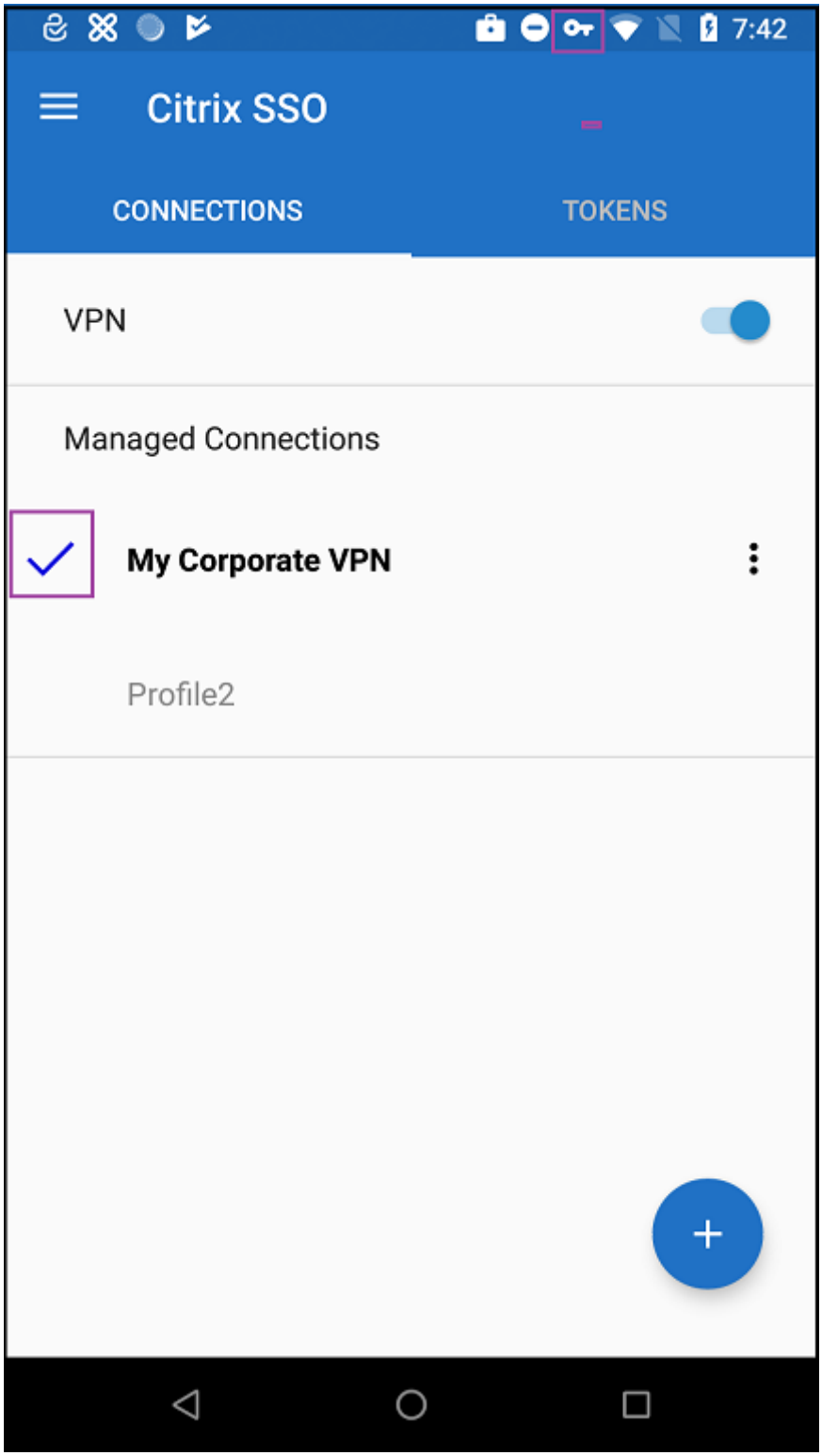
Zugriff vom Gerät auf VPN-Profile

Für den Zugriff auf die von Ihnen erstellten VPN-Profile installieren Android Enterprise-Benutzer Citrix SSO aus dem Google Play Store.

Die konfigurierten VPN-Profile werden im Bereich **Verwaltete Verbindungen** der App angezeigt. Benutzer tippen auf das gewünschte VPN-Profil, um eine Verbindung herzustellen.



Nachdem Benutzer sich authentifiziert und eine Verbindung hergestellt haben, wird neben dem VPN-Profil ein Häkchen angezeigt. Das Schlüsselsymbol zeigt an, dass eine Verbindung zum VPN vorliegt.



Verwalten von Android-Geräten von Zebra mit Zebra OEMConfig

Verwalten Sie Android-Geräte von Zebra mit OEMConfig-Tool von Zebra Technologies. Weitere Informationen zu Zebra OEMConfig finden Sie auf der Website von Zebra Technologies.

XenMobile unterstützt Zebra OEMConfig ab Version 9.2. Informationen zu den Systemanforderungen für die Installation von Zebra OEMConfig auf Geräten finden Sie unter OEMConfig-Setup auf der Website von Zebra Technologies.

Fügen Sie zunächst die App Zebra OEMConfig als Google Play Store-App zur XenMobile-Konsole hinzu. Siehe Hinzufügen von Apps aus einem öffentlichen App-Store.

Erstellen einer verwalteten Android Enterprise-Konfiguration für Zebra OEMConfig

Konfigurieren Sie die Geräterichtlinie für verwaltete Android Enterprise-Konfigurationen für die Zebra OEMConfig-App. Die Richtlinie gilt für Zebra-Geräte, auf denen die Zebra OEMConfig-App installiert und die Richtlinie bereitgestellt ist.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**. Klicken Sie auf **Hinzufügen**.
2. Wählen Sie **Android Enterprise**. Klicken Sie auf **Verwaltete Android Enterprise-Konfigurationen**.
3. Im dann angezeigten Fenster **Anwendungs-ID auswählen** wählen Sie **ZebraOEMConfig powered by MX** aus der Liste aus und klicken auf **OK**.
4. Geben Sie einen Namen und eine Beschreibung für Ihre Zebra OEMConfig-Konfiguration ein. Klicken Sie auf **Weiter**.
5. Geben Sie einen Namen für die Zebra OEMConfig-Konfiguration ein.
6. Konfigurieren Sie die verfügbaren Parameter. Beispiel:
    - Zum Deaktivieren der Kamera an der Vorderseite des Geräts wählen Sie **Camera Configuration** und legen **Use of Front Camera** auf **Off** fest.
    - Um das Zeitformat zu ändern, wählen Sie **Clock Configuration** und legen für **Time Format** die Option **12** für 12-Stunden-Format oder **24** für 24-Stunden-Format fest.

Eine Liste und Beschreibungen aller verfügbaren Konfigurationen finden Sie unter Verwaltete Zebra-Konfigurationen auf der Website von Zebra Technologies.

1. Optional können Sie weitere Zebra OEMConfig-Konfigurationen erstellen. Klicken Sie unter der Liste der Konfigurationen auf **Hinzufügen**. Eine neue Konfiguration wird in der Liste angezeigt. Wählen Sie die neue Konfiguration aus und konfigurieren Sie die Parameter.
2. Wenn Sie alle gewünschten Zebra OEMConfig Konfigurationen erstellt haben, klicken Sie auf **Weiter**.
3. Konfigurieren Sie Bereitstellungsregeln für diese verwaltete Konfiguration für Zebra OEMConfig.

4. Klicken Sie auf **Speichern**.

Android Enterprise-App-Berechtigungen

November 9, 2020

Sie können konfigurieren, was geschieht, wenn Android Enterprise-Apps in Firmenprofilen Berechtigungsanfragen erhalten, die von Google als “gefährlich” eingestuft werden. Legen Sie fest, ob Benutzer eine Aufforderung erhalten, die angeforderte Berechtigung zu gewähren oder zu verweigern. Dieses Feature gilt für Geräte mit Android 7.0 und höher.

Google definiert Berechtigungen als “gefährlich”, wenn die App damit Zugriff auf Daten oder Ressourcen erhält, die private Benutzerinformationen betreffen oder die sich auf gespeicherte Benutzerdaten bzw. auf die Ausführung anderer Apps auswirken können. Beispielsweise ist die Möglichkeit, die Benutzerkontakte zu lesen, eine gefährliche Berechtigung.

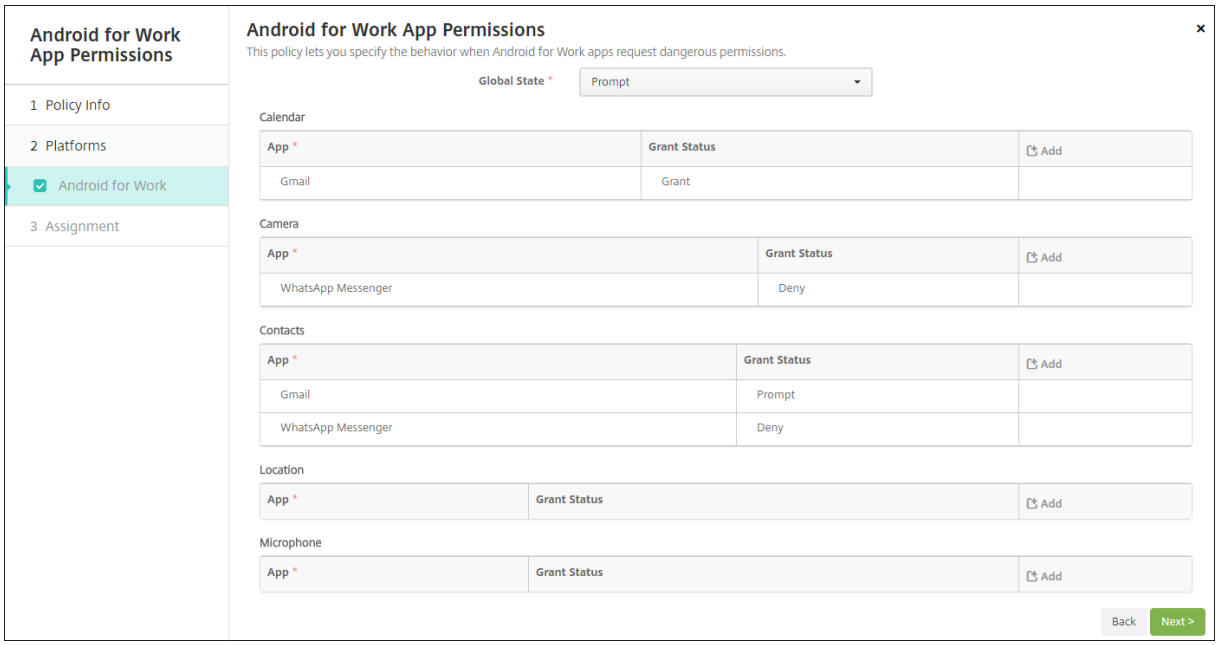
Sie können einen globalen Status konfigurieren, der das Verhalten bei allen Anfragen zu gefährlichen Berechtigungen steuert, die an Android Enterprise-Apps in Firmenprofilen gesendet werden. Außerdem können Sie für jede App das Verhalten für einzelne Berechtigungsgruppen (gemäß Google-Definition) festlegen. Diese individuell festgelegten Einstellungen überschreiben den globalen Status.

Weitere Informationen zur Google-Definition von Berechtigungsgruppen finden Sie im Android Developers Guide unter “Permission groups”.

Standardmäßig werden Benutzer aufgefordert, angeforderte gefährliche Berechtigungen zu gewähren oder zu verweigern.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android Enterprise-Einstellungen



- **Globaler Status:** steuert das Verhalten für alle angeforderten gefährlichen Berechtigungen. Klicken Sie in der Liste auf **Auffordern**, **Gewähren** oder **Verweigern**.
  - **Auffordern:** Benutzer werden aufgefordert, angeforderte gefährliche Berechtigungen zu gewähren oder zu verweigern.
  - **Gewähren:** Alle angeforderten gefährlichen Berechtigungen werden gewährt. Der Benutzer erhält keine Aufforderung.
  - **Verweigern:** Alle angeforderten gefährlichen Berechtigungen werden verweigert. Der Benutzer erhält keine Aufforderung.

  Die Standardeinstellung **Auffordern**.
- Definieren Sie für jede Berechtigungsgruppe und für jede App ein individuelles Vorgehen. Um das Verhalten für eine Berechtigungsgruppe zu konfigurieren, klicken Sie auf **Hinzufügen** und wählen dann unter **App** eine App aus der Liste aus. Wenn Sie System-Apps für Android Enterprise konfigurieren, klicken Sie auf **Neu hinzufügen** und geben Sie den Namen des Anwendungspakets ein, das Sie in der Einschränkungsrichtlinie aktiviert haben. Wählen Sie unter "Status gewähren" die Option **Auffordern**, **Gewähren** oder **Verweigern**. Dieser Status setzt den globalen Status außer Kraft.
  - **Auffordern:** Benutzer werden aufgefordert, gefährliche Berechtigungen, die von dieser Berechtigungsgruppe für die App angefordert wurden, zu gewähren oder zu verweigern.
  - **Gewähren:** Gefährliche Berechtigungen, die von dieser Berechtigungsgruppe für die App angefordert wurden, werden gewährt. Der Benutzer erhält keine Aufforderung.
  - **Verweigern:** Gefährliche Berechtigungen, die von dieser Berechtigungsgruppe für die App angefordert wurden, werden verweigert. Der Benutzer erhält keine Aufforderung.

Die Standardeinstellung **Auffordern**.

- Klicken Sie neben App und “Status gewähren” auf **Speichern**.
- Um der Berechtigungsgruppe weitere Apps hinzuzufügen, klicken Sie erneut auf **Hinzufügen** und wiederholen Sie die Schrittfolge.
- Nachdem Sie jeder gewünschten Berechtigungsgruppe einen Status zugewiesen haben, klicken Sie auf **Weiter**.

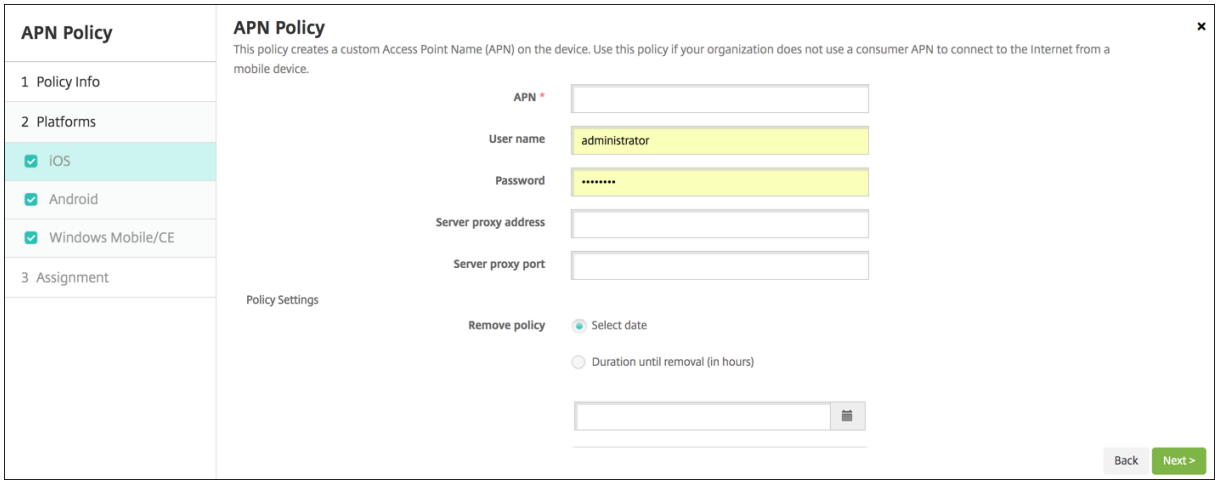
APN-Geräterichtlinie

January 5, 2022

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

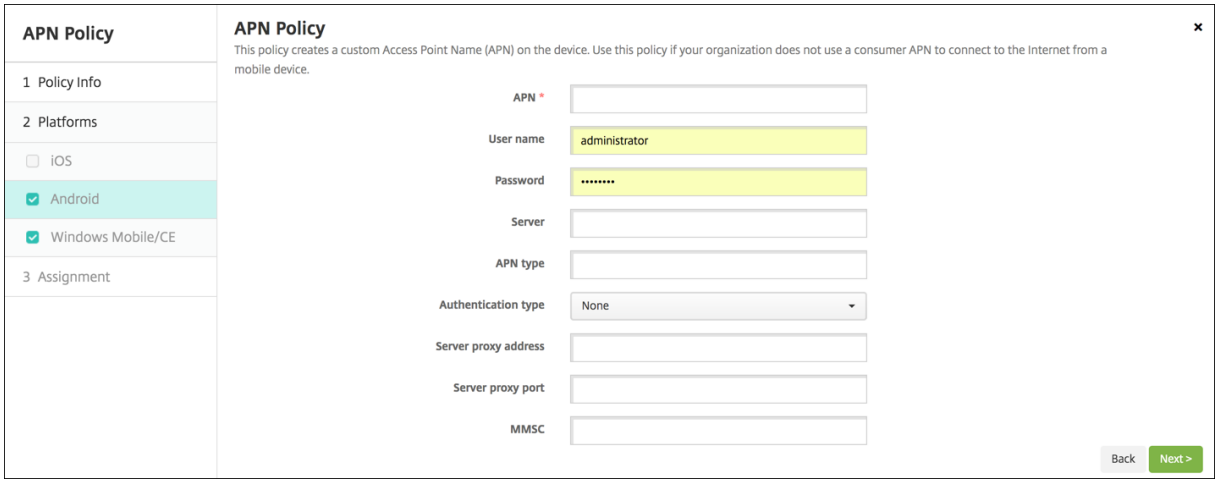
iOS-Einstellungen



- **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 gibt den Benutzernamen für diesen APN an. Fehlt der Benutzername, fordert das Gerät die Zeichenfolge während der Profilinstallation an.

- **Kennwort:** Das Kennwort für den Benutzer dieses APN. Für höhere Sicherheit ist das Kennwort codiert. Fehlt es, fordert das Gerät die Zeichenfolge während der Profilinstallation an.
- **Serverproxyadresse:** Die IP-Adresse oder URL des APN-Proxys.
- **Serverproxyport:** Die 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 Stunden)**.
  - 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.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

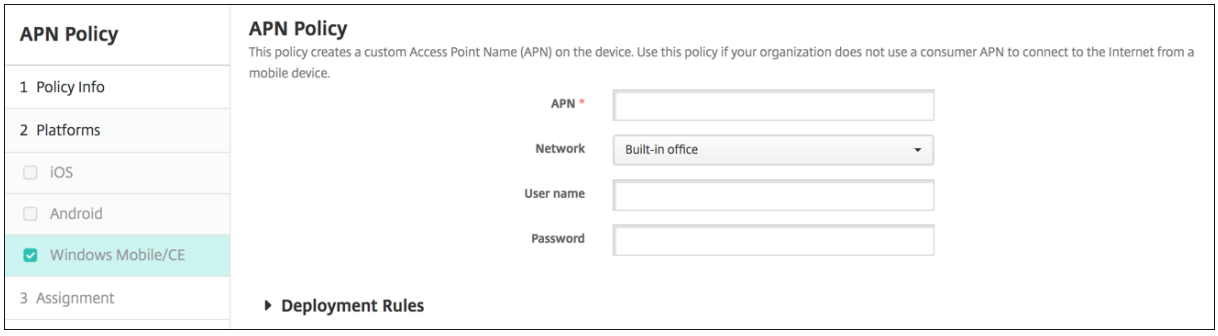
Android-Einstellungen



- **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 gibt den Benutzernamen für diesen APN an. Fehlt der Benutzername, fordert das Gerät die Zeichenfolge während der Profilinstallation an.

- **Kennwort:** Das Kennwort für den Benutzer dieses 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. Die Standardeinstellung ist “Ohne”.
- **Serverproxyadresse:** Die IP-Adresse oder URL des APN-HTTP-Proxys des Netzbetreibers.
- **Serverproxyport:** Die 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 benötigen bestimmte Protokolle (z. B. MM1,… MM11).
- **MMS-Port:** Der Port des MMS-Proxyservers.

Windows Mobile-/CE-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 gibt den Benutzernamen für diesen APN an. Fehlt der Benutzername, fordert das Gerät die Zeichenfolge während der Profilinstallation an.
- **Kennwort:** Das Kennwort für den Benutzer dieses APN. Für höhere Sicherheit ist das Kennwort codiert. Fehlt es, fordert das Gerät die Zeichenfolge während der Profilinstallation an.

App-Zugriffsrichtlinie für Geräte

August 20, 2019

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 Richtlinie in XenMobile für welche Liste von Apps gilt.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Plattformeinstellungen

- **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.

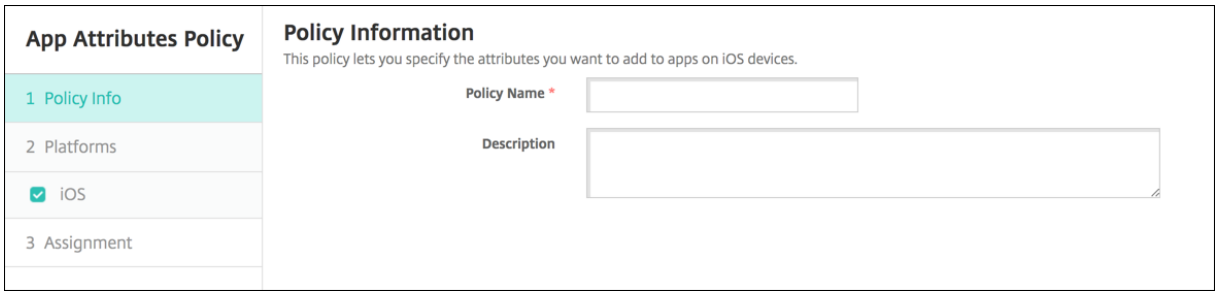
Geräterichtlinie für App-Attribute

April 17, 2019

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).

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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.

App-Konfigurationsrichtlinie für Geräte

January 5, 2022

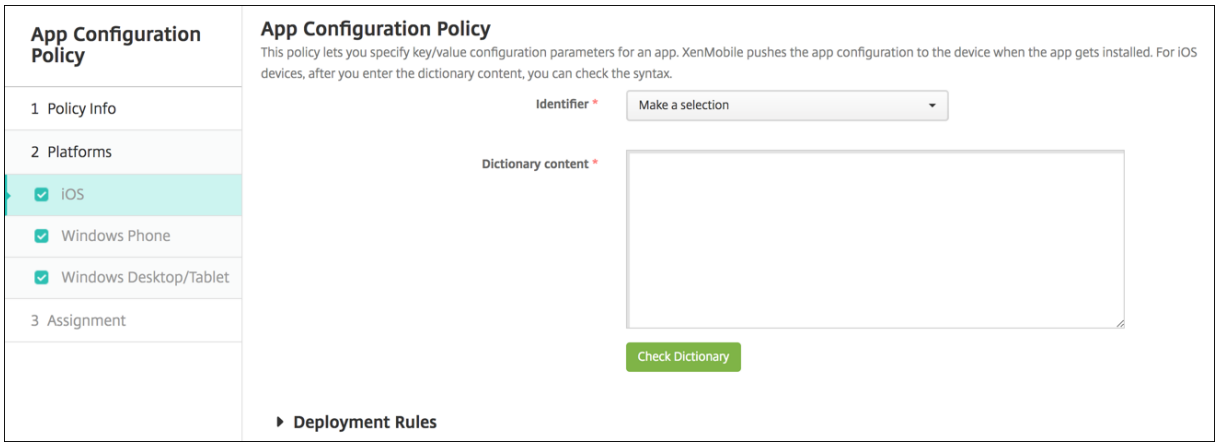
Sie können Apps, die eine verwaltete Konfiguration unterstützen, remote konfigurieren, indem Sie Folgendes bereitstellen:

- Eine XML-Konfigurationsdatei (eine sogenannte Eigenschaftenliste oder “plist”) auf iOS-Geräten
- Oder Schlüssel/Wert-Paare für Windows 10 Phone oder Tablet oder Desktopgeräte, auf denen Windows 10 oder Windows 11 ausgeführt wird.

Die Konfiguration legt mehrere Einstellungen und Verhaltensweisen der App fest. XenMobile verschiebt die Konfiguration per Push auf die Geräte, wenn der Benutzer die App installiert. Die Einstellungen und Verhaltensweisen, die Sie selbst konfigurieren können, hängen von der App ab und gehen über den Umfang dieses Artikels hinaus.

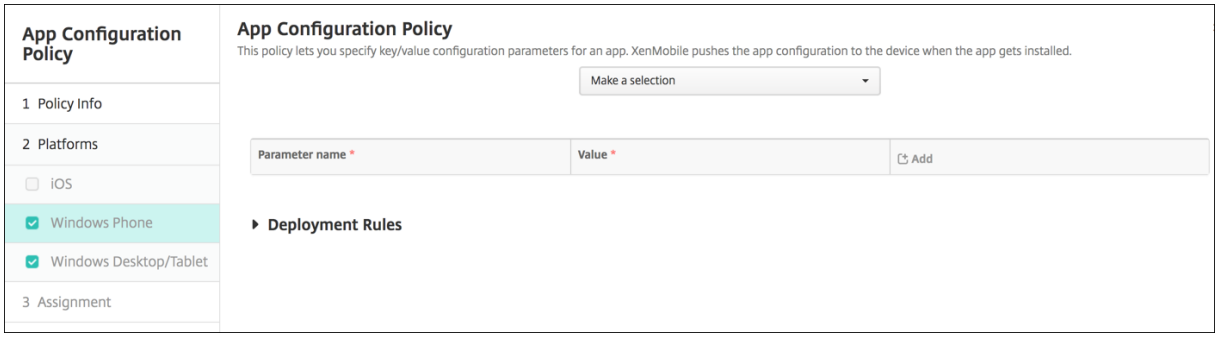
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

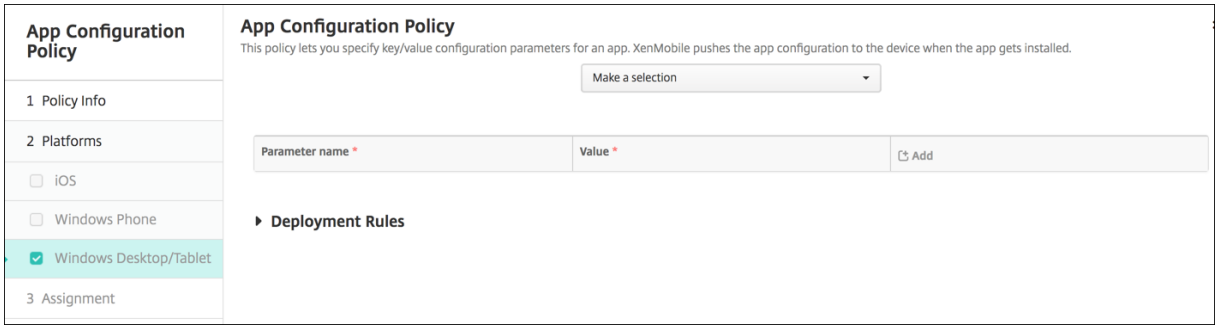
iOS-Einstellungen



- **Bezeichner:** Klicken Sie in der Liste auf die gewünschte App oder auf **Hinzufügen**, um der Liste eine App hinzuzufügen.
  - Wenn Sie auf **Hinzufügen** klicken, geben Sie den App-Bezeichner in dem nun eingeblendeten Feld ein.
- **Wörterbuchinhalt:** Geben Sie die Konfigurationsinformationen der XML-Eigenschaftenliste (plist) ein, bzw. kopieren Sie sie und fügen Sie ein.
- Klicken Sie auf **Wörterbuch prüfen**. XenMobile prüft die XML-Datei. Werden keine Fehler gefunden, wird unterhalb des Inhaltsfelds **Gültige XML** angezeigt. Werden unterhalb des Inhaltsfelds Syntaxfehler angezeigt, müssen Sie sie korrigieren, bevor Sie fortfahren können.

Windows Phone- oder Desktop-/Tablet-Einstellungen





- Klicken Sie in der Liste **Auswählen** auf die App, die Sie konfigurieren möchten, oder auf **Hinzufügen**, um der Liste eine neue App hinzuzufügen.
  - Wenn Sie auf **Hinzufügen** geklickt haben, geben Sie den Paketfamiliennamen in dem nun eingeblendeten Feld ein.
- Für jeden Konfigurationsparameter, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Parametername:** Geben Sie den Schlüsselnamen einer Anwendungseinstellung für das Windows-Gerät ein. Informationen zu Windows-App-Einstellungen finden Sie in der Dokumentation von Microsoft.
  - **Wert:** Geben Sie den Wert für den angegebenen Parameter ein.
  - Klicken Sie auf **Hinzufügen**, um den Parameter hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

App-Bestandsrichtlinie für Geräte

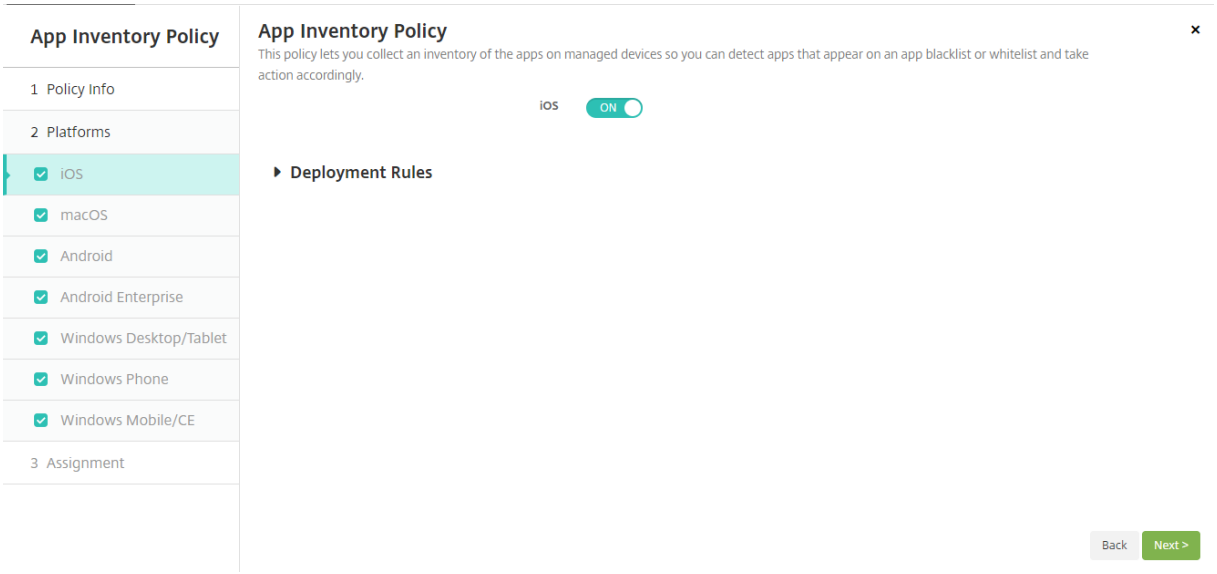
July 15, 2020

Mit der App-Bestandsrichtlinie können Sie einen Bestand der Apps auf verwalteten Geräten abrufen. XenMobile kann dann die vorhandenen Apps mit den App-Zugriffsrichtlinien vergleichen, die auf diesen Geräten bereitgestellt sind. Auf diese Weise können Sie Apps erkennen, die auf einer App-Sperrliste oder einer App-Positivliste stehen, und entsprechende Maßnahmen ergreifen.

Sie können Anwendungszugriffsrichtlinien für iOS-, macOS-, Android-, Android Enterprise-, Windows Desktop-/Tablet-, Windows Mobile-/CE- und Windows Phone-Geräte erstellen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Plattformeinstellungen



- Behalten Sie für jede ausgewählte Plattform den Standardwert bei oder klicken Sie auf **Aus**. Die Standardeinstellung ist **Ein**.

Geräterichtlinie zum Sperren von Apps

January 5, 2022

Über die Geräterichtlinie zum Sperren von Apps können Sie eine Liste der Apps erstellen, die auf dem Gerät ausgeführt werden dürfen, oder eine Liste der Apps, die 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.

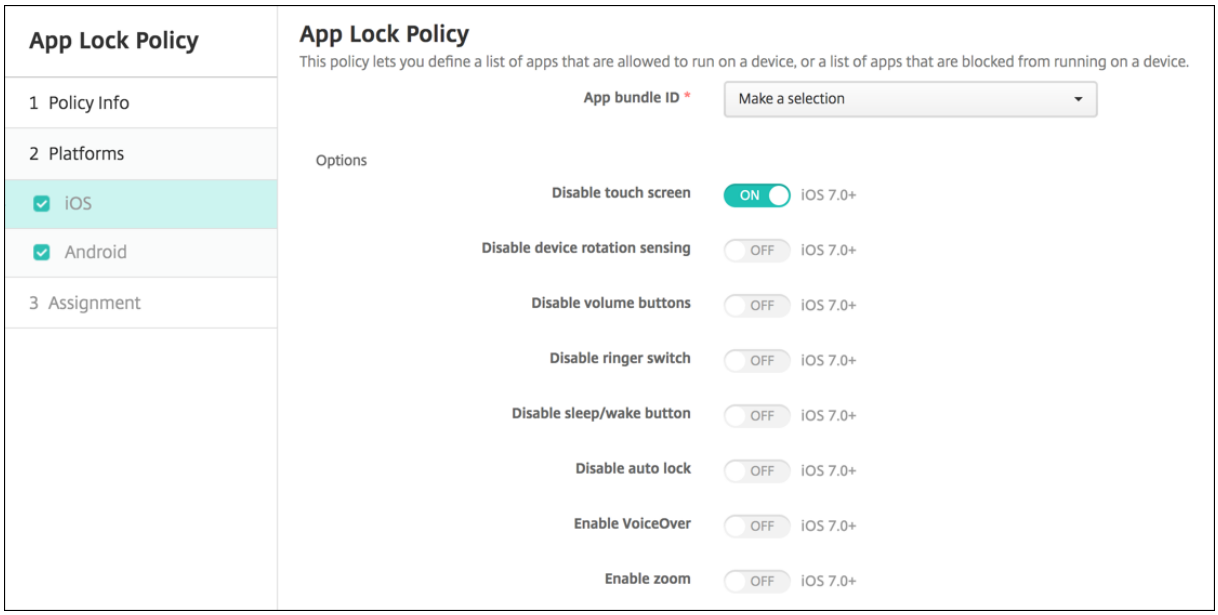
Auf iOS-Geräten können Sie auch nur eine iOS-App pro Richtlinie auswählen. Das bedeutet, dass Benutzer ihr Gerät nur zum Ausführen einer einzigen App verwenden können. Außer den Optionen, die ausdrücklich zulässig sind, wenn die Richtlinie für die App-Sperre erzwungen wird, können sie keine anderen Aktivitäten 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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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 ist **Aus** mit Ausnahme von "Touchscreen deaktivieren" (Standardwert **Ein**).
  - Touchscreen deaktivieren
  - Geräteausrichtungserkennung deaktivieren
  - Lautstärketasten deaktivieren
  - Ruftonschalter deaktivieren

    Wenn **Ruftonschalter deaktivieren** auf "Ein" festgelegt 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. Die

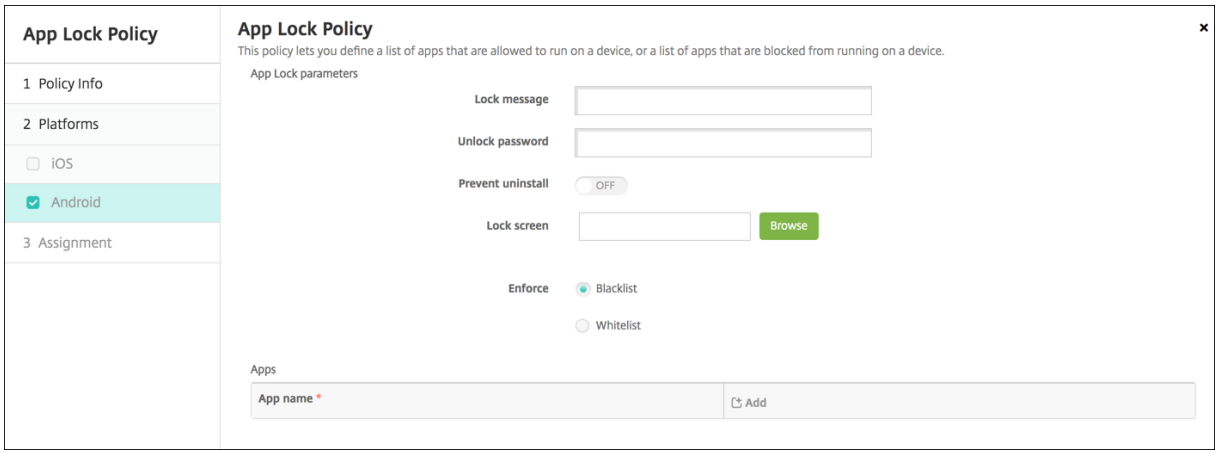
Standardeinstellung für alle Optionen ist **Aus**.

- Anpassen von VoiceOver zulassen
- Anpassen von Zoom zulassen
- Anpassen von Farbumkehrung zulassen
- Anpassen von AssistiveTouch zulassen

- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

Android-Einstellungen

> **Hinweis:**
>
> Sie können die App für Android-Einstellungen nicht über die Geräterichtlinie zum Sperren von Apps blockieren.



- **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. Die Standardeinstellung ist **Aus**.
  - **Sperrbildschirm:** Wählen Sie das auf dem Sperrbildschirm angezeigte Bild aus, indem Sie auf “Durchsuchen” klicken und zum Speicherort der Datei navigieren.
  - **Erzwingen:** Klicken Sie auf **Sperrliste**, um eine Liste von Apps zu erstellen, deren Aus-

führung auf den Geräten nicht zulässig ist, oder auf **Positivliste**, um eine Liste von Apps zu erstellen, deren Ausführung auf den Geräten zulässig ist.

> **Hinweis:**
> Die XenMobile Server-Konsole enthält im Englischen die Begriffe “Blacklist” und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

- **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.

Richtlinie für die App-Netzwerkauslastung

January 5, 2022

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Roaming für mobile Daten zulassen:** Wählen Sie aus, ob die angegebenen Apps beim Roaming eine Mobilfunkdatenverbindung herstellen können. Die Standardeinstellung ist **Aus**.
- **Mobile Daten zulassen:** Wählen Sie aus, ob die angegebenen Apps eine Mobilfunkdatenverbindung verwenden können. Die Standardeinstellung 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 eine App-ID ein.

– Klicken Sie auf **Speichern**, um die App der Liste hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

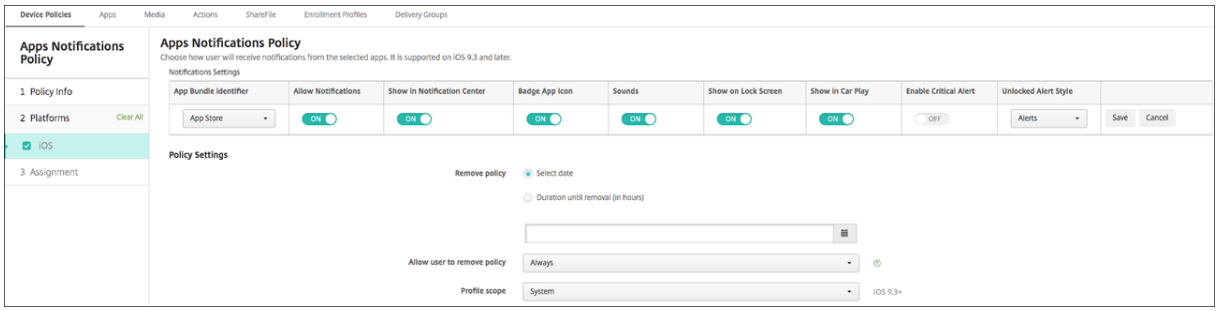
Geräterichtlinie für App-Benachrichtigungen

April 16, 2020

Mit der App-Benachrichtigungsrichtlinie können Sie steuern, wie iOS-Benutzer Benachrichtigungen von bestimmten Apps erhalten. Die Richtlinie wird auf Geräten mit iOS 9.3 oder Nachfolgeversionen unterstützt.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



- **App-Paket-ID:** Geben Sie die Apps an, auf die Sie die Richtlinie anwenden möchten.
- **Benachrichtigungen zulassen:** Wählen Sie **Ein**, um Benachrichtigungen zuzulassen.
- **Im Mitteilungszentrale anzeigen:** Wählen Sie **Ein**, um Benachrichtigungen in der Mitteilungszentrale der Geräte anzuzeigen.
- **Kennzeichenzähler:** Wählen Sie **Ein**, um einen Kennzeichenzähler mit Benachrichtigungen anzuzeigen.
- **Töne:** Wählen Sie **Ein**, um bei Benachrichtigungen Töne abzuspielen.
- **Im Sperrbildschirm:** Wählen Sie **Ein**, um Benachrichtigungen im Sperrbildschirm der Benutzergeräte anzuzeigen.
- **In CarPlay anzeigen:** Wählen Sie **Ein**, damit Benachrichtigungen in Apple CarPlay angezeigt werden. Verfügbar in iOS 12 und höher. Die Standardeinstellung ist **Ein**.
- **Kritische Warnung aktivieren:** Bei der Einstellung **Ein** kann eine App eine Benachrichtigung als kritische Benachrichtigung markieren, die die Einstellungen für “Nicht stören” und “Klingel” ignoriert. Verfügbar in iOS 12 und höher. Die Standardeinstellung ist **Aus**.

- **Hinweisstil (entsperrt):** Wählen Sie in der Liste **Keine**, **Banner** oder **Warnungen**, um das Erscheinungsbild von Hinweisen bei entsperrtem Gerät zu konfigurieren.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur unter iOS 9.3 und höher verfügbar.

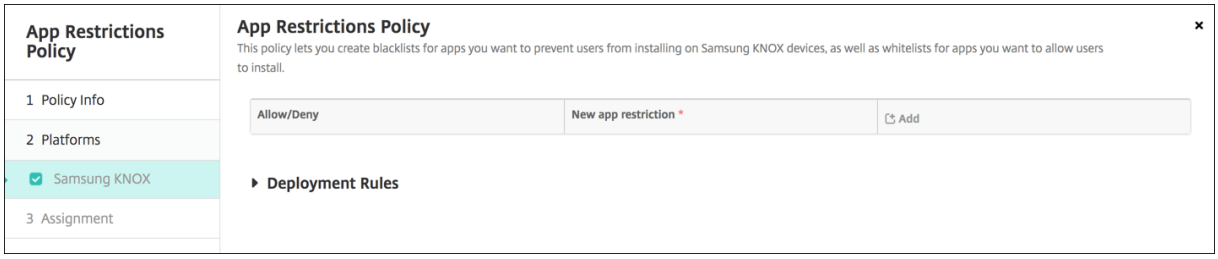
App-Einschränkungsrichtlinie

July 15, 2020

Sie können Sperrlisten für Apps erstellen, die von Benutzern nicht auf Samsung Knox-Geräten installiert werden sollen. Sie können auch Positivlisten für Apps erstellen, die Benutzer installieren dürfen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Samsung KNOX-Einstellungen



Klicken Sie für jede App, die Sie der Liste "Zulassen/Verweigern" 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 Liste “Zulassen/Verweigern” hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

App-Tunnelrichtlinie für Geräte

January 5, 2022

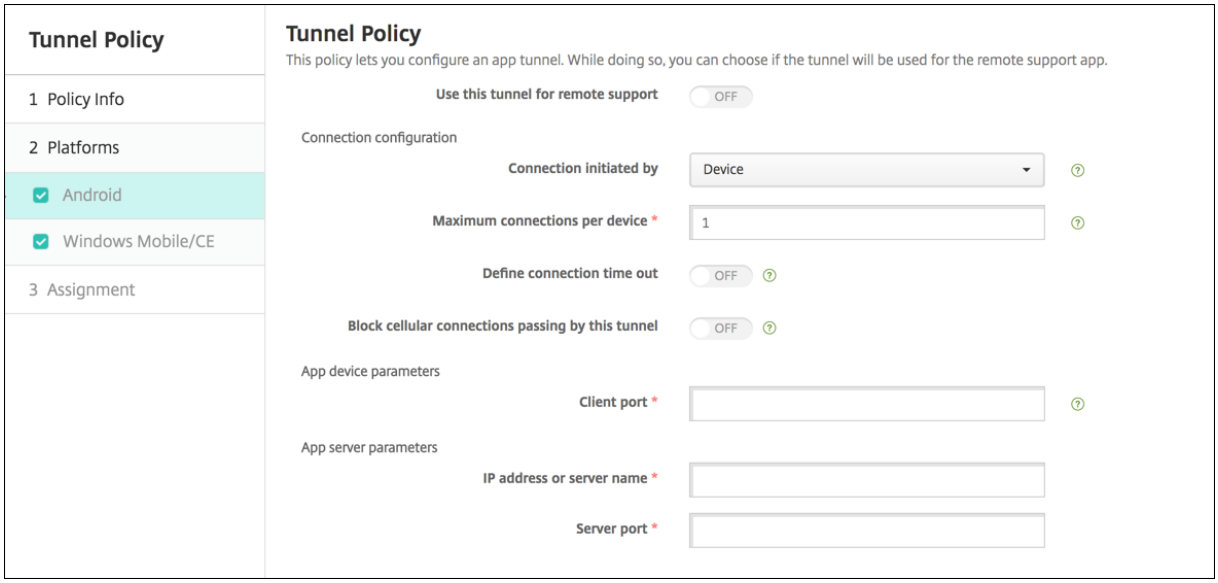
> **Wichtig:**
>
> Die App-Tunnelrichtlinie wird nur für den Remotesupport verwendet. Informationen zum Remotesupport finden Sie unter Supportoptionen und Remotesupport. Remote Support ist ab dem 1. Januar 2019 für Neukunden nicht mehr verfügbar. Bestehende Kunden können das Produkt weiterhin verwenden, Citrix stellt jedoch keine Neuerungen oder Fixes bereit.

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.

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android-Einstellungen



- **Tunnel für Remotesupport verwenden:** Geben Sie an, ob der Tunnel für Remotesupport verwendet werden soll.

  Die Konfigurationsschritte unterscheiden sich je nachdem, ob Sie hier Remotesupport auswählen.

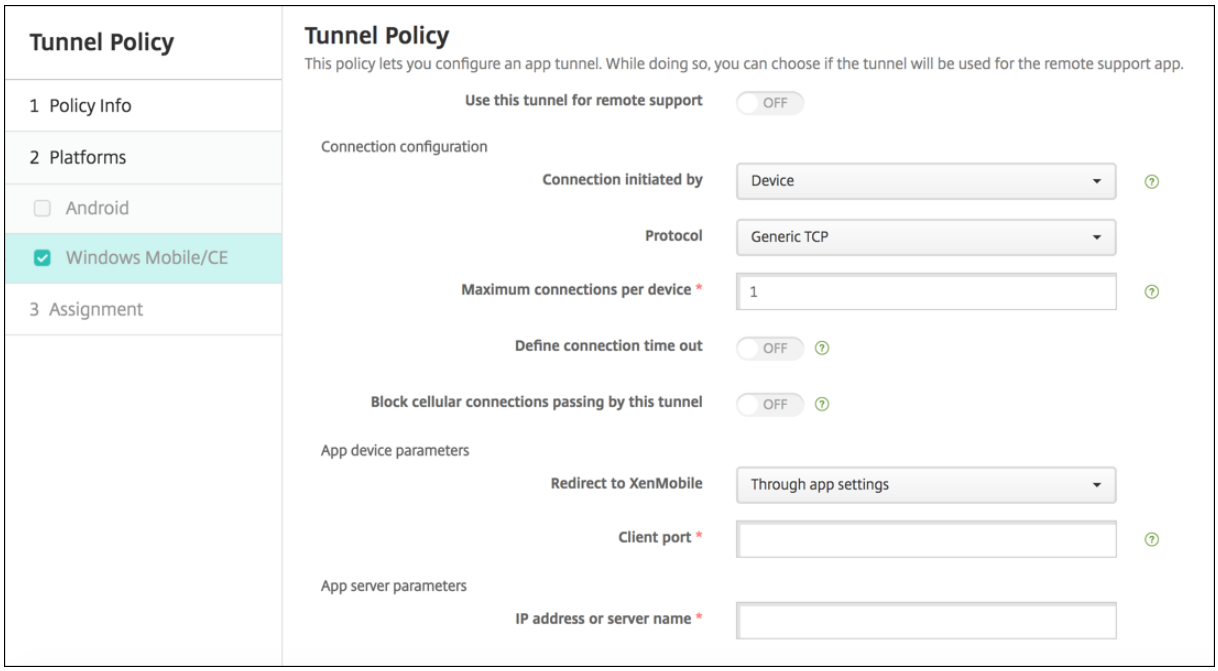
- Wenn Sie Remotesupport nicht auswählen, führen Sie folgende Schritte aus:
  - **Verbindung initiiert von:** Klicken Sie auf **Gerät** oder **Server**, um die Quelle für die Aufnahme der Verbindung anzugeben.
  - **Maximale Verbindungen pro Gerät:** Geben Sie die Zahl der gleichzeitig zulässigen TCP-Verbindungen 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. Mit dieser Einstellung werden WLAN- und USB-Verbindungen nicht blockiert.

Windows Mobile-/CE-Einstellungen



- **Tunnel für Remotesupport verwenden:** Geben Sie an, ob der Tunnel für Remotesupport verwendet werden soll.

Die Konfigurationsschritte unterscheiden sich je nachdem, ob Sie hier Remotesupport auswählen.

- Wenn Sie Remotesupport nicht auswählen, führen Sie folgende Schritte aus:
  - **Verbindung initiiert von:** Klicken Sie auf **Gerät** oder **Server**, um die Quelle für die Aufnahme der Verbindung anzugeben.
  - **Protokoll:** Klicken Sie in der Liste auf das Protokoll, das verwendet werden soll. Der Standardwert ist **Generisches TCP**.
  - **Maximale Verbindungen pro Gerät:** Geben Sie die Zahl der gleichzeitig zulässigen TCP-Verbindungen für die App ein. Dieses Feld gilt nur für geräteseitig initiierte Verbindungen.
  - **Verbindungstimeout definieren:** Wählen Sie aus, ob festgelegt werden soll, wie lange eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
    - **Verbindungstimeout:** Wenn Sie für **Verbindungstimeout definieren** die Option **Ein** festgelegt haben, geben Sie hier die Zeitdauer in Sekunden ein, die eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
  - **Mobilnetzverbindungen durch diesen Tunnel blockieren:** Wählen Sie aus, ob der Tunnel beim Roaming blockiert werden soll.

> **Hinweis:**
> WiFi- und USB-Verbindungen werden nicht blockiert.

  - **Umleiten zu XenMobile:** Klicken Sie in der Liste auf die Methode des Verbindungsaufbaus zwischen Gerät und XenMobile. Der Standardwert ist **Über App-Einstellungen**.
    * Bei Verwendung von **Mit einem lokalen Alias** geben Sie 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. WLAN- und USB-Verbindungen werden nicht blockiert.

App-Deinstallationsrichtlinie

April 17, 2019

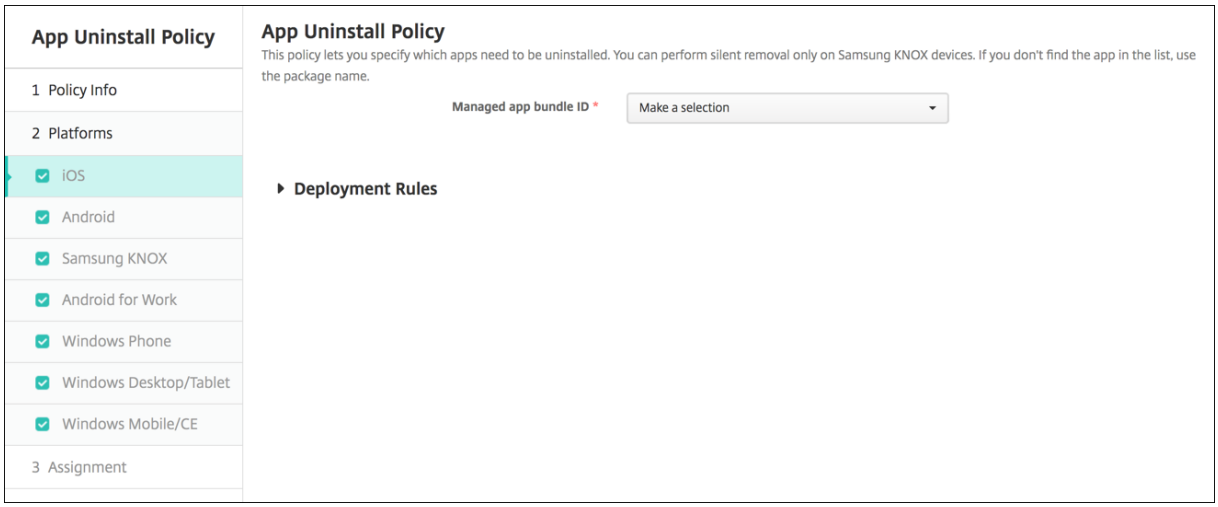
Sie können App-Deinstallationsrichtlinien für die folgenden Plattformen erstellen: iOS, Android, Samsung KNOX, Android Enterprise, Windows-Desktop/Tablet und Windows Mobile/CE. Mit einer App-Deinstallationsrichtlinie können Sie Apps von Benutzergeräten entfernen. Gründe für das Entfernen von Apps sind 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, sobald diese Richtlinie auf den Benutzergeräten bereitgestellt wird. Bei allen Geräten mit Ausnahme von Samsung KNOX-Geräten werden Benutzer dazu aufgefordert, die entsprechende App zu deinstallieren. Benutzer von Samsung KNOX-Geräten erhalten keine

Aufforderung, die App zu deinstallieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



- **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.

Alle anderen Plattformeinstellungen

- **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 **Hinzufügen**, 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.

Automatische Deinstallation einer Unternehmensapp nach Installation der entsprechenden App aus dem öffentlichen App-Store

Sie können XenMobile so konfigurieren, dass die Unternehmensversion von Citrix-Apps bei der Installation der Version aus dem öffentlichen App-Store entfernt wird. Durch dieses Feature wird verhin-

dert, dass auf Benutzergeräten zwei identische App-Symbole angezeigt werden, nachdem die Version aus dem öffentlichen App-Store installiert wurde.

Eine Bereitstellungsbedingung der App-Deinstallationsrichtlinie veranlasst XenMobile, ältere Apps bei der Installation der neuen Version von Benutzergeräten zu entfernen. Dieses Feature ist nur für verwaltete iOS-Geräte verfügbar, die mit XenMobile Server im Enterprise-Modus (XME) verbunden sind.

Konfigurieren einer Bereitstellungsregel mit der Bedingung "Name der installierten App"

- Geben Sie die **Paket-ID für verwaltete App** für die Unternehmensapp an.
- Fügen Sie eine Regel hinzu: Klicken Sie auf **Neue Regel** und wählen Sie dann wie im Beispiel gezeigt **Name der installierten App** und **ist gleich**. Geben Sie die App-Paket-ID für die App im öffentlichen App-Store ein.

In diesem Beispiel wird die Unternehmensversion der App (com.citrix.mail) von XenMobile entfernt, wenn die App-Version aus dem öffentlichen App-Store (com.citrix.mail.ios) auf einem Gerät in den angegebenen Bereitstellungsgruppen installiert wird.

Einschränkungsrichtlinie für die App-Deinstallation

October 25, 2018

Sie können vorgeben, welche Apps Benutzer von einem Samsung SAFE- oder Amazon-Gerät deinstallieren dürfen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Samsung SAFE- bzw. Amazon-Einstellungen

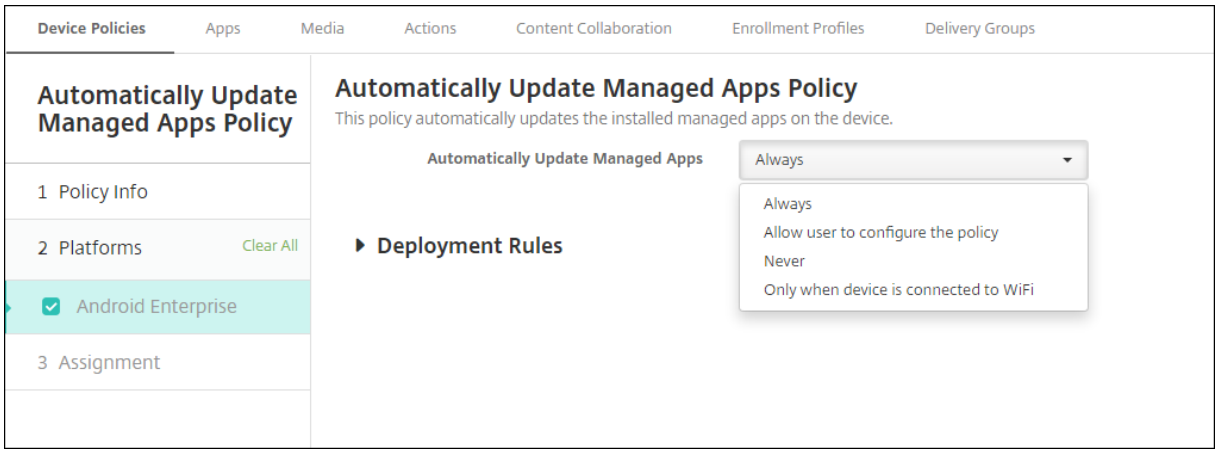
- **Einstellungen zum Einschränken der App-Deinstallation:** Klicken Sie für jede Regel, die Sie hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name:** Klicken Sie in der Liste auf eine vorhandene App oder klicken Sie auf **Hinzufügen**, um eine neue App hinzuzufügen.
  - **Regel:** Wählen Sie aus, ob Benutzer die App deinstallieren können. Gemäß Standardeinstellung ist eine Deinstallation zulässig.
  - Klicken Sie auf **Speichern** oder **Abbrechen**.

Verwaltete Apps automatisch aktualisieren

January 21, 2021

Mit dieser Richtlinie steuern Sie, wie installierte verwaltete Apps auf Android Enterprise-Geräten aktualisiert werden. Sie können die Fähigkeit von Benutzern zum Zulassen automatischer App-Updates auf ihren Geräten beschränken. Wenn Sie die Steuerung automatischer App-Updates durch Benutzer zulassen, können diese im verwalteten Google Play Store Richtlinien für automatische App-Updates festlegen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.



Wählen Sie **Verwaltete Apps automatisch aktualisieren**.

- **Immer:** Aktiviert automatische App-Updates. **Immer** ist die Standardeinstellung.
- **Benutzer darf Richtlinie konfigurieren:** Benutzer können die Richtlinie für automatische App-Updates für das Gerät im verwalteten Google Play Store konfigurieren.
- **Nie:** Deaktiviert automatische App-Updates.
- **Nur wenn das Gerät mit WLAN verbunden ist:** Lässt automatische App-Updates nur zu, wenn das Gerät mit dem Wi-Fi verbunden ist.

BitLocker-Geräterichtlinie

January 5, 2022

Windows 10 und Windows 11 enthalten ein Feature zur Festplattenverschlüsselung namens BitLocker, das zusätzlichen Datei- und Systemschutz vor unbefugtem Zugriff auf verlorene oder gestohlene Windows-Geräte bietet. Zur Erhöhung der Sicherheit können Sie BitLocker mit TPM-Chips (Trusted Platform Module) der Version 1.2 oder höher verwenden. Ein TPM-Chip handhabt kryptographische Vorgänge, generiert und speichert kryptographische Schlüssel und limitiert deren Verwendung.

Ab Windows 10 Build 1703 kann BitLocker über MDM-Richtlinien gesteuert werden. Über die BitLocker-Geräterichtlinie in XenMobile konfigurieren Sie die Einstellungen im BitLocker-Assistenten auf Windows 10 und Windows 11-Geräten. Auf Geräten, auf denen BitLocker aktiviert ist, kann BitLocker

die Benutzer beispielsweise dazu auffordern auszuwählen, wie sie ihr Laufwerk beim Start entsperren, ihren Wiederherstellungsschlüssel sichern und eine Festplatte entsperren möchten. Über die BitLocker-Geräterichtlinie wird außerdem vorgegeben, ob:

- BitLocker auf Geräten ohne TPM-Chip aktiviert werden soll.
- Wiederherstellungsoptionen auf der BitLocker-Benutzeroberfläche angezeigt werden sollen.
- der Schreibzugriff auf Festplatten- oder Wechsellaufwerke verweigert werden soll, wenn BitLocker nicht aktiviert ist.

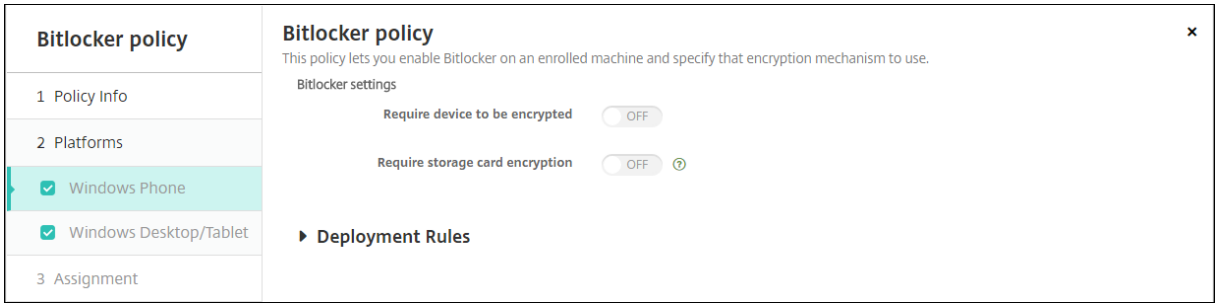
> **Hinweis:**
>
> Nachdem die BitLocker-Verschlüsselung auf einem Gerät gestartet wurde, können Sie die BitLocker-Einstellungen auf dem Gerät nicht mehr ändern, indem Sie eine aktualisierte BitLocker-Geräterichtlinie bereitstellen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Anforderungen

- Die BitLocker-Geräterichtlinie erfordert Windows 10 und Windows 11 Enterprise Edition.
- Bereiten Sie vor der Bereitstellung der BitLocker-Geräterichtlinie Ihre Umgebung für die Verwendung von BitLocker vor. Ausführliche Informationen von Microsoft, einschließlich Systemanforderungen und zur Einrichtung von BitLocker, finden Sie unter BitLocker und den zugehörigen Unterabschnitten.

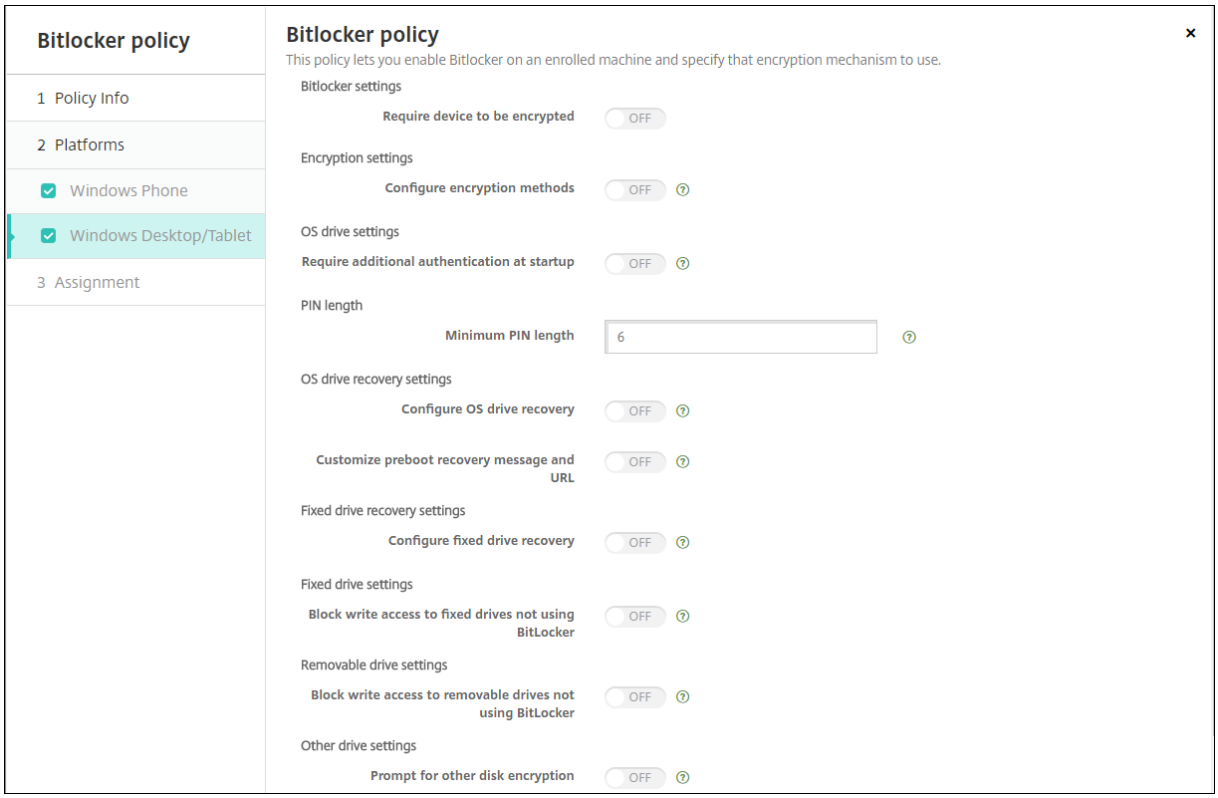
Windows Phone-Einstellungen



- **Geräteverschlüsselung erforderlich:** legt fest, ob Benutzer zum Aktivieren der BitLocker-Verschlüsselung auf Windows Phone-Systemkarten aufgefordert werden sollen. Bei Auswahl von **Ein** wird auf den Geräten nach Abschluss der Registrierung eine Meldung angezeigt, dass das Unternehmen eine Geräteverschlüsselung vorschreibt. Entscheidet sich der Benutzer gegen die Geräteverschlüsselung, erhält er keinen Schreibzugriff auf die Systemkarte. Bei Auswahl von **Aus** erfolgt keine Aufforderung an den Benutzer. Ob das Gerät verschlüsselt wird, wird dann durch die BitLocker-Richtlinie bestimmt. Die Standardeinstellung ist **Aus**.

- **Speicherkartenverschlüsselung erforderlich:** legt fest, ob Benutzer zum Aktivieren der BitLocker-Verschlüsselung auf Windows Phone-Speicherkarten aufgefordert werden sollen. Bei Auswahl von **Ein** ist für den Schreibzugriff für die Karte die Speicherkartenverschlüsselung erforderlich. Die Standardeinstellung ist **Aus**.

Windows-Desktop-/Tablet-Einstellungen



- **Geräteverschlüsselung erforderlich:** legt fest, ob Benutzer zum Aktivieren der BitLocker-Verschlüsselung auf Windows-Desktops/-Tablets aufgefordert werden sollen. Bei Auswahl von **Ein** wird auf den Geräten nach Abschluss der Registrierung eine Meldung angezeigt, dass das Unternehmen eine Geräteverschlüsselung vorschreibt. Bei Auswahl von **Aus** erfolgt keine Aufforderung und es gelten die Einstellungen der BitLocker-Richtlinie. Die Standardeinstellung ist **Aus**.
- **Verschlüsselungsmethoden konfigurieren:** legt die Verschlüsselungsmethoden für spezifische Laufwerktypen fest. Bei Auswahl von **Aus** fordert der BitLocker-Assistent den Benutzer zur Auswahl der Verschlüsselungsmethode für einen Laufwerkstyp auf. Die Standard-Verschlüsselungsmethode für alle Laufwerke ist XTS-AES 128 Bit. Die Verschlüsselungsmethode für Wechsellaufwerke ist AES-CBC 128-Bit. Bei Auswahl von **Ein** verwendet BitLocker die in der Richtlinie angegebene Verschlüsselungsmethode. Bei Auswahl von **Aus** werden folgende zusätzlichen Einstellungen angezeigt: **Betriebssystemlaufwerk**, **Festplattenlaufwerk** und **Wechsellaufwerk**. Wählen Sie die Standard-Verschlüsselungsmethode für jeden

Laufwerkstyp. Die Standardeinstellung ist **Aus**.

- **Zusätzliche Authentifizierung beim Start erforderlich:** gibt an, ob eine zusätzliche Authentifizierung beim Gerätestart erforderlich ist. Außerdem wird durch diese Einstellung festgelegt, ob BitLocker auf Geräten ohne TPM-Chip zugelassen werden soll. Bei Auswahl von **Aus** kann die BitLocker-Verschlüsselung auf Geräten ohne TPM nicht verwendet werden. Informationen zu TPM finden Sie in dem Microsoft-Artikel Trusted Platform Module – Technologieübersicht. Bei Auswahl von **Ein** werden die folgenden zusätzlichen Einstellungen angezeigt: Die Standardeinstellung ist **Aus**.
  - **BitLocker auf Geräten ohne TPM-Chip blockieren:** Auf Geräten ohne TPM-Chip veranlasst BitLocker, dass die Benutzer ein Kennwort zum Entsperren oder einen Startschlüssel erstellen müssen. Der Startschlüssel wird auf einem USB-Laufwerk gespeichert, das der Benutzer vor dem Start mit dem Gerät verbinden muss. Das Kennwort zum Entsperren muss mindestens acht Zeichen enthalten. Die Standardeinstellung ist **Aus**.
  - **TPM-Start:** Auf Geräten mit TPM-Chip gibt es vier Modi zum Entsperren (nur TPM, TPM + PIN, TPM + Schlüssel und TPM + PIN + Schlüssel). Der TPM-Start gilt für den Modus "Nur TPM", in dem die Verschlüsselungsschlüssel auf dem TPM-Chip gespeichert werden. In diesem Modus müssen Benutzer keine zusätzlichen Daten zum Entsperren angeben. Das Benutzergerät wird beim Neustart automatisch mit dem Verschlüsselungsschlüssel des TPM-Chips entsperrt. Standardwert ist **TPM zulassen**.
  - **PIN für TPM-Start:** Diese Einstellung entspricht dem Entsperrmodus TPM + PIN. Die PIN kann bis zu 20 Ziffern enthalten. Über die Einstellung **PIN-Mindestlänge** können Sie die Mindestlänge der PIN festlegen. Die Benutzer konfigurieren die PIN bei der BitLocker-Einrichtung und geben sie beim Start des Geräts ein.
  - **Schlüssel für TPM-Start**: Diese Einstellung entspricht dem Entsperrmodus TPM + Schlüssel. Der Startschlüssel wird auf einem USB-Laufwerk oder einem anderen Wechsellaufwerk gespeichert, das der Benutzer vor dem Start mit dem Gerät verbinden muss.
  - **Schlüssel und PIN für TPM-Start:** Diese Einstellung entspricht dem Entsperrmodus TPM + PIN + Schlüssel.

    Wenn die Entsperrung erfolgreich ist, wird das Betriebssystem geladen. Wenn die Entsperrung fehlschlägt, wird das Gerät in den Wiederherstellungsmodus versetzt.
- **PIN-Mindestlänge:** die Mindestlänge der TPM-Start-PIN. Der Standardwert ist **6**.
- **OS-Laufwerkswiederherstellung konfigurieren:** Wenn die Entsperrung fehlschlägt, fordert BitLocker den Benutzer zur Eingabe des konfigurierten Wiederherstellungsschlüssels auf. Über diese Einstellung werden die Wiederherstellungsoptionen für das Betriebssystemlaufwerk konfiguriert, die den Benutzern zur Verfügung stehen, wenn sie nicht über das Kennwort zum Entsperren oder den USB-Startschlüssel verfügen. Die Standardeinstellung ist **Aus**.

- **Zertifikatsbasierten Agent für Datenwiederherstellung zulassen:** gibt an, ob ein zertifikatsbasierter Agent für die Datenwiederherstellung zugelassen werden soll. Fügen Sie einen Agent für die Datenwiederherstellung aus "Richtlinien öffentlicher Schlüssel" hinzu (befindet sich in der Gruppenrichtlinien-Verwaltungskonsole bzw. im lokalen Gruppenrichtlinien-Editor). Weitere Informationen zu Agents für die Datenwiederherstellung finden Sie im Microsoft-Artikel BitLocker Group Policy settings. Die Standardeinstellung ist **Aus**.
- **48-Bit-Wiederherstellungskennwort für die OS-Laufwerkswiederherstellung erstellen:** gibt an, ob die Verwendung eines Kennworts für die Wiederherstellung zugelassen oder erzwungen werden soll. BitLocker erstellt das Kennwort und speichert es in einer Datei oder einem Microsoft-Cloudkonto. Der Standardwert ist **48-Bit-Kennwort zulassen**.
- **256-Bit-Wiederherstellungsschlüssel erstellen:** gibt an, ob die Verwendung eines Schlüssels für die Wiederherstellung zugelassen oder erzwungen werden soll. Ein Wiederherstellungsschlüssel ist eine auf einem USB-Laufwerk gespeicherte BEK-Datei. Der Standardwert ist **256-Bit-Wiederherstellungsschlüssel zulassen**.
- **Optionen für OS-Laufwerkswiederherstellung ausblenden:** gibt an, ob Wiederherstellungsoptionen auf der Benutzeroberfläche von BitLocker angezeigt werden sollen. Mit **Ein** werden keine Wiederherstellungsoptionen in der BitLocker-Oberfläche angezeigt. In diesem Fall registrieren Sie die Geräte bei Active Directory, speichern Sie die Wiederherstellungsoptionen in Active Directory und legen Sie für **Wiederherstellungsinfo in AD DS speichern** die Einstellung **Ein** fest. Die Standardeinstellung ist **Aus**.
- **Wiederherstellungsinfo in AD DS speichern:** gibt an, ob die Wiederherstellungsoptionen in Active Directory-Domänendienste gespeichert werden sollen. Die Standardeinstellung ist **Aus**.
- **In AD DS gespeicherte Wiederherstellungsinfo konfigurieren:** gibt an, ob das BitLocker-Wiederherstellungskennwort bzw. Wiederherstellungskennwort und Schlüsselpaket in den Active Directory-Domänendiensten gespeichert werden sollen. Das Speichern des Schlüsselpakets unterstützt die Wiederherstellung von Daten von einem physisch beschädigten Laufwerk. Standardwert ist **Wiederherstellungskennwort sichern**.
- **BitLocker nach dem Speichern von Wiederherstellungsinfo in AD DS aktivieren:** gibt an, ob Benutzer daran gehindert werden sollen, BitLocker zu aktivieren, wenn ihr Gerät nicht mit der Domäne verbunden ist und die Sicherung der BitLocker-Wiederherstellungsinformationen in Active Directory erfolgreich ist. Bei Auswahl von **Ein** muss ein Gerät mit der Domäne verbunden sein, damit BitLocker gestartet werden kann. Die Standardeinstellung ist **Aus**.

- **Preboot-Wiederherstellungsmeldung und -URL anpassen:** gibt an, ob BitLocker eine angepasste Meldung plus URL auf dem Wiederherstellungsbildschirm anzeigen soll. Bei Auswahl von **Ein** werden die folgenden zusätzlichen Einstellungen angezeigt: **Standardwiederherstellungsmeldung und -URL verwenden**, **Leere Wiederherstellungsmeldung und -URL verwenden**, **Benutzerdefinierte Wiederherstellungsmeldung verwenden** und **Benutzerdefinierte Wiederherstellungs-URL verwenden**. Bei Auswahl von **Aus** werden die Standardwiederherstellungsmeldung und -URL angezeigt. Die Standardeinstellung ist **Aus**.
- **Wiederherstellung von Festplattenlaufwerk konfigurieren:** konfiguriert die Wiederherstellungsoptionen für Benutzer eines mit BitLocker verschlüsselten Festplattenlaufwerks. BitLocker zeigt den Benutzern keine Meldung über die Festplattenverschlüsselung an. Um eine Festplatte beim Start zu entsperren, gibt der Benutzer ein Kennwort an oder verwendet eine Smartcard. Die nicht in dieser Richtlinie enthaltenen Entsperrungseinstellungen werden auf der BitLocker-Oberfläche angezeigt, wenn ein Benutzer die BitLocker-Verschlüsselung auf einer Festplatte aktiviert. Weitere Informationen über die zugehörigen Einstellungen finden Sie weiter oben unter **OS-Laufwerkswiederherstellung konfigurieren**. Die Standardeinstellung ist **Aus**.
- **Schreibzugriff auf Festplattenlaufwerke blockieren, die nicht BitLocker verwenden:** Bei Auswahl von **Ein** können Benutzer nur auf lokale Festplattenlaufwerke schreiben, wenn diese mit BitLocker verschlüsselt sind. Die Standardeinstellung ist **Aus**.
- **Schreibzugriff auf Wechseldatenträger blockieren, die nicht BitLocker verwenden:** Bei Auswahl von **Ein** können Benutzer nur auf lokale Wechseldatenträger schreiben, wenn diese mit BitLocker verschlüsselt sind. Konfigurieren Sie diese Einstellung je nachdem, ob Ihre Organisation Schreibzugriff auf andere organisationseigene Wechseldatenträger zulässt. Die Standardeinstellung ist **Aus**.
- **Eingabeaufforderung für andere Festplattenverschlüsselung:** ermöglicht das Deaktivieren der Warnungsaufforderung für andere Datenträgerverschlüsselungen auf Geräten. Die Standardeinstellung ist **Aus**.

Browserrichtlinie für Geräte

October 25, 2018

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Samsung SAFE- und Samsung KNOX-Einstellungen

- **Browser deaktivieren:** Wählen Sie aus, ob der Samsung-Browser auf den Geräten vollständig deaktiviert werden soll. Die Standardeinstellung 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.

Kalenderrichtlinie

January 5, 2022

Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen eines Kalenderkontos (CalDAV) zu iOS- oder macOS-Geräten einrichten, damit die Benutzer Kalendereinträge mit einem beliebigen Server, der CalDAV unterstützt, synchronisieren können.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Kontobeschreibung:** Geben Sie eine Kontobeschreibung ein. Diese Angabe ist erforderlich.
- **Hostname:** Geben Sie die Adresse des CalDAV-Servers ein. Diese Angabe ist erforderlich.
- **Port:** Geben Sie den Port für die Verbindung mit dem CalDAV-Server ein. Diese Angabe ist erforderlich. Der Standardwert ist **8443**.
- **Principal URL:** Geben Sie die Basis-URL des Kalenders des Benutzers ein.
- **Benutzername:** Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.

- **Kennwort:** Geben Sie ein optionales Benutzerkennwort ein.
- **SSL verwenden:** Wählen Sie aus, ob für die Verbindung mit dem CalDAV-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **Ein**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-Einstellungen

- **Kontobeschreibung:** Geben Sie eine Kontobeschreibung ein. Diese Angabe ist erforderlich.
- **Hostname:** Geben Sie die Adresse des CalDAV-Servers ein. Diese Angabe ist erforderlich.
- **Port:** Geben Sie den Port für die Verbindung mit dem CalDAV-Server ein. Diese Angabe ist erforderlich. Der Standardwert ist **8443**.
- **Principal URL:** Geben Sie die Basis-URL des Kalenders des Benutzers ein.
- **Benutzername:** Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.
- **Kennwort:** Geben Sie ein optionales Benutzerkennwort ein.
- **SSL verwenden:** Wählen Sie aus, ob für die Verbindung mit dem CalDAV-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **Ein**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.

- **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Mobilfunkgeräterichtlinie

April 16, 2020

Mit dieser Richtlinie können Sie Einstellungen für das Mobilfunknetz auf iOS-Geräten konfigurieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **APN anfügen**
  - **Name:** Name für die Konfiguration.
  - **Authentifizierungstyp:** Klicken Sie in der Liste auf das Challenge Handshake Authentication-Protokoll (**CHAP**) oder das Password Authentication-Protokoll (**PAP**). Die Standardeinstellung ist **PAP**.
  - **Benutzername** und **Kennwort:** Benutzername und Kennwort für die Authentifizierung.
- **APN**
  - **Name:** Name für die APN-Konfiguration (Access Point Name).
  - **Authentifizierungstyp:** Klicken Sie in der Liste auf **CHAP** oder **PAP**. Die Standardeinstellung ist **PAP**.
  - **Benutzername** und **Kennwort:** Benutzername und Kennwort für die Authentifizierung.
  - **Proxyserver:** Netzwerkadresse des Proxyservers.
  - **Proxyserverport:** Port des Proxyservers.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

Verbindungsmanagerrichtlinie

May 24, 2019

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Mobile-/CE-Einstellungen

> **Hinweis:**
>
> **Büro (integriert)** bedeutet, dass alle Verbindungen zum Intranet Ihres Unternehmens gehen. **Internet (integriert)** bedeutet, dass alle Verbindungen zum Internet gehen.

- **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)**.

Verbindungszeitplanrichtlinie für Geräte

January 6, 2022

> **Wichtig:**
>
> Citrix empfiehlt, dass Sie Firebase Cloud Messaging (FCM) verwenden, um Verbindungen von Android-, Android Enterprise- und Chrome OS-Geräten mit XenMobile Server zu steuern. Informationen zur Verwendung von FCM finden Sie unter Firebase Cloud Messaging.

Wenn Sie FCM nicht verwenden, können Sie Richtlinien für die Verbindungszeitplanung erstellen, um zu steuern, wie und wann Benutzergeräte eine Verbindung zu XenMobile Server herstellen.

Sie können festlegen, dass Benutzer eine Verbindung manuell herstellen oder dass die Geräte in einem festgelegten Zeitrahmen eine Verbindung herstellen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

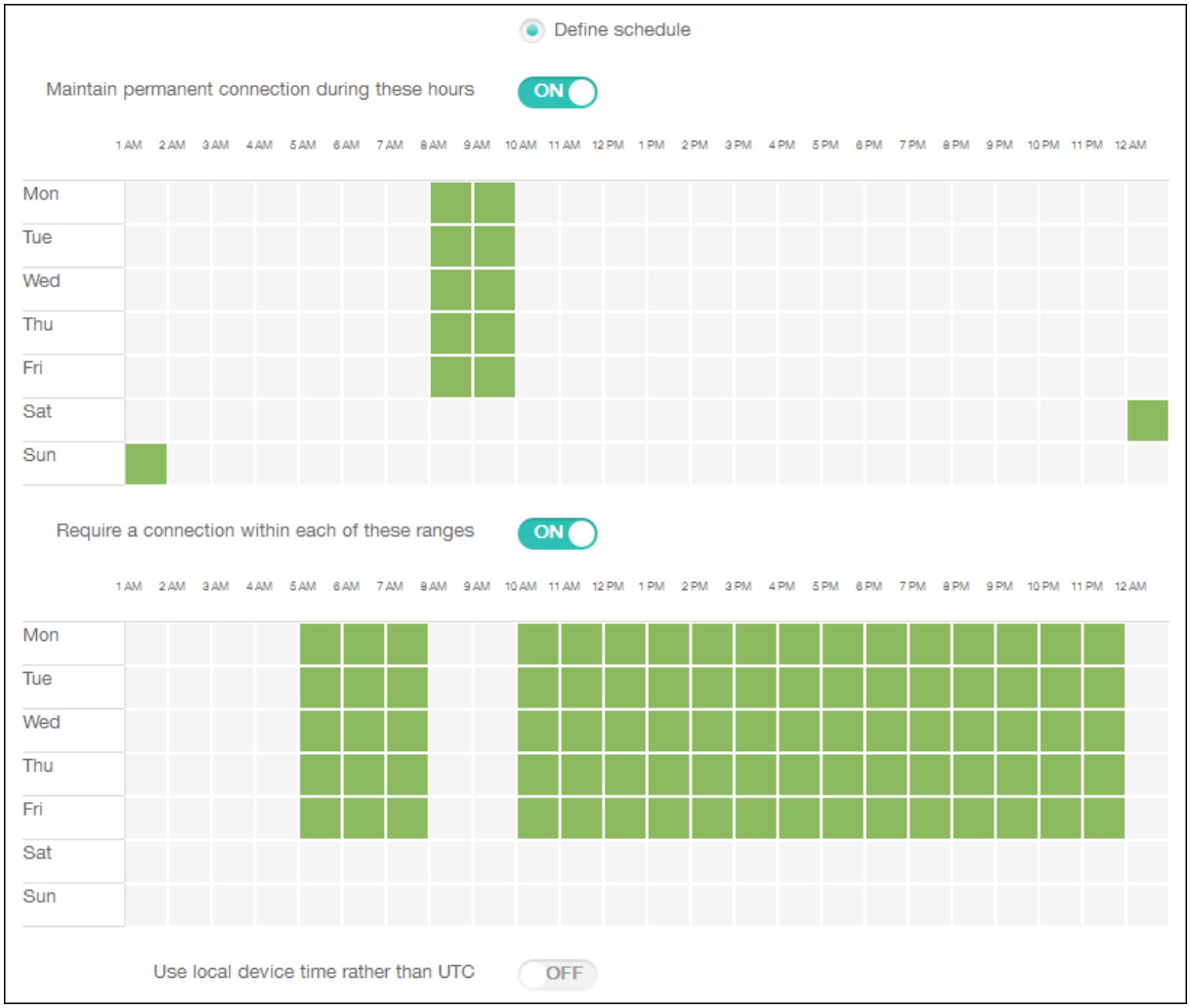
Plattformeinstellungen

- **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.



Geräterichtlinie für Kontakte (CardDAV)

January 5, 2022

Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen eines iOS-Kontaktekontos (CardDAV) zu iOS- oder macOS-Geräten einrichten, damit die Benutzer Kontaktdaten mit einem beliebigen Server, der CardDAV unterstützt, synchronisieren können.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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. Die Standardeinstellung ist **Ein**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-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. Die Standardeinstellung ist **Ein**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Geräterichtlinie zum Steuern von Betriebssystemupdates

September 24, 2021

Mit der Geräterichtlinie “OS-Updates steuern” können Sie Folgendes bereitstellen:

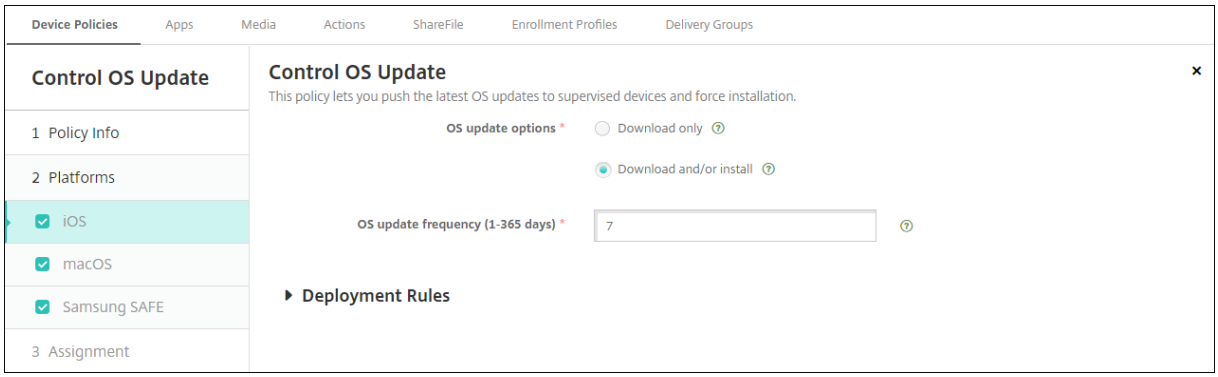
- Die aktuellen Betriebssystemupdates auf betreuten iOS-Geräten.

  Die Geräterichtlinie für Betriebssystemupdates funktioniert nur bei betreuten und im Apple-Bereitstellungsprogramm registrierten Geräten.
- Die neuesten Betriebssystem- und App-Updates für DEP-registrierte macOS-Geräte, auf denen macOS 10.11.5 und höher ausgeführt wird.
- Die aktuellen Betriebssystemupdates auf betreuten Samsung SAFE-Geräten.

Bei Samsung SAFE-Geräten sendet XenMobile die Richtlinie zum Steuern von Betriebssystemupdates an Secure Hub, von wo die Richtlinie dann auf das Gerät angewendet wird. Auf der Seite **Verwalten > Geräte** wird angezeigt, wann XenMobile Server die Richtlinie sendet und wenn das Gerät die Richtlinie erhält.

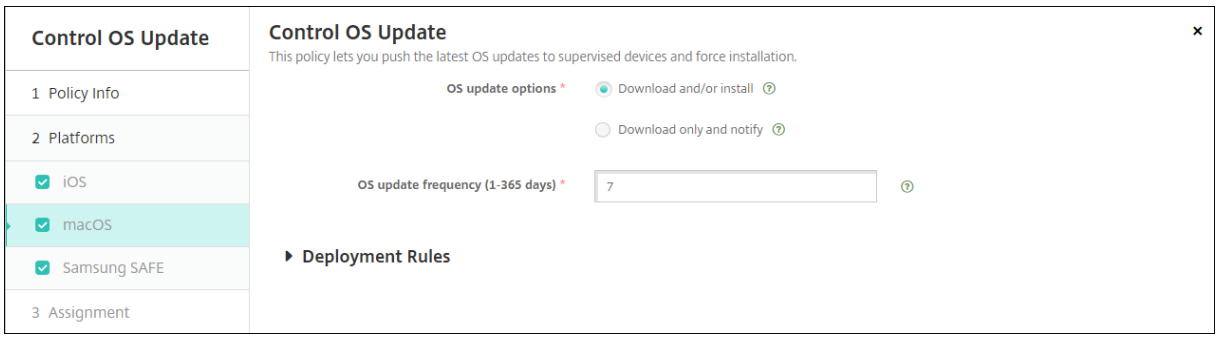
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



- **OS-Updateoptionen:** Durch beide Optionen werden die aktuellen Updates auf betreute Geräte gemäß der Einstellung **OS-Updatehäufigkeit** heruntergeladen. Der Benutzer wird zum Installieren von Updates aufgefordert. Die Aufforderung wird nach dem Entsperren des Geräts angezeigt.
- **OS-Updatehäufigkeit:** legt fest, wie häufig XenMobile das Gerätebetriebssystem überprüft und aktualisiert. Die Standardeinstellung ist **7** Tage.

macOS-Einstellungen



- **OS-Updateoptionen:** Durch beide Optionen werden die aktuellen macOS-Updates gemäß der Einstellung **OS-Updatehäufigkeit** heruntergeladen. Sie können wählen, ob die Updates installiert werden oder ob der Benutzer nur benachrichtigt wird, dass Updates verfügbar sind.

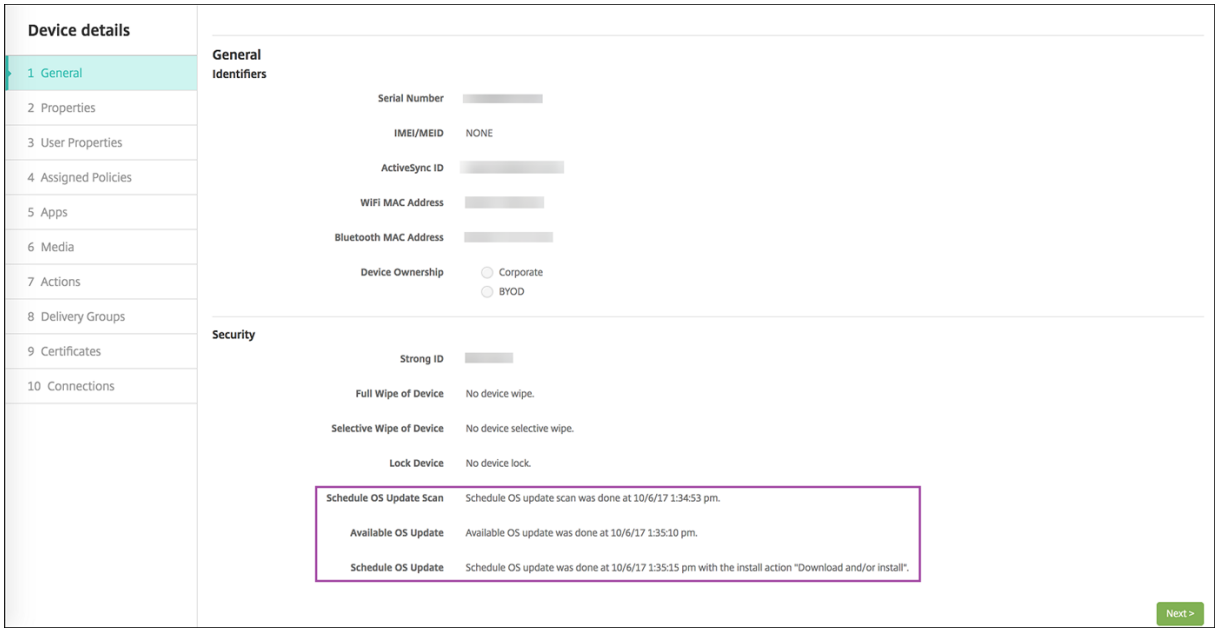
- **OS-Updatehäufigkeit:** legt fest, wie häufig XenMobile das Gerätebetriebssystem überprüft und aktualisiert. Die Standardeinstellung ist **7** Tage.

Statusabfragen für iOS- und macOS-Update-Aktionen

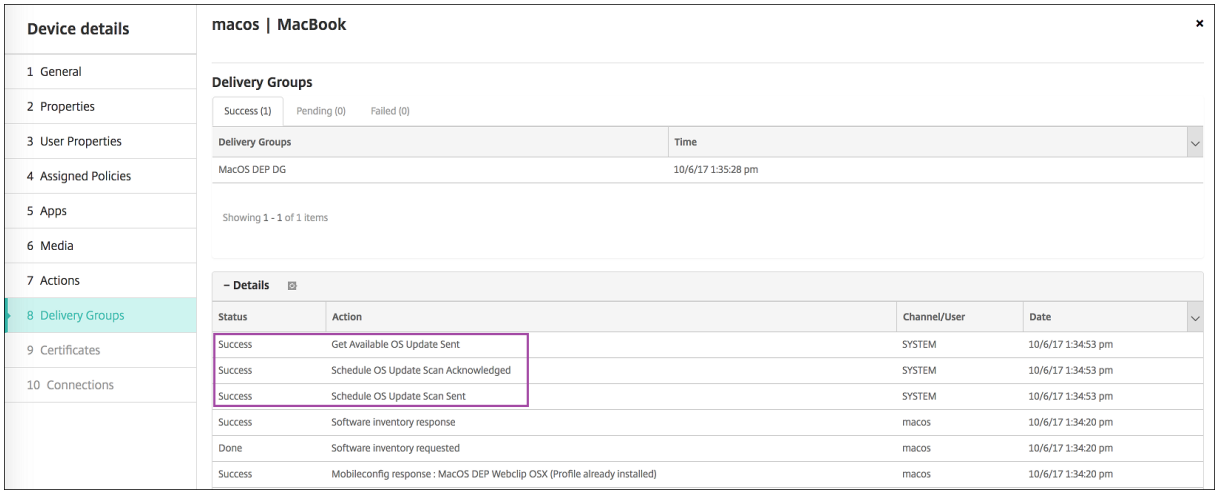
Unter iOS und macOS stellt XenMobile die Richtlinie zum Steuern von Betriebssystemupdates nicht auf Geräten bereit. Stattdessen sendet XenMobile über die Richtlinie folgende MDM-Befehle an Geräte:

- OS-Updatescan planen: Das Gerät wird aufgefordert, im Hintergrund nach Betriebssystemupdates zu suchen. (optional für iOS)
- Verfügbares OS-Update: Eine Liste verfügbarer Betriebssystemupdates wird vom Gerät abgerufen.
- OS Update planen: Das Gerät wird zum Durchführen von macOS-Updates, App-Updates oder beidem aufgefordert. Das Gerätebetriebssystem legt damit selbst fest, wann Betriebssystem- und App-Updates heruntergeladen und installiert werden.

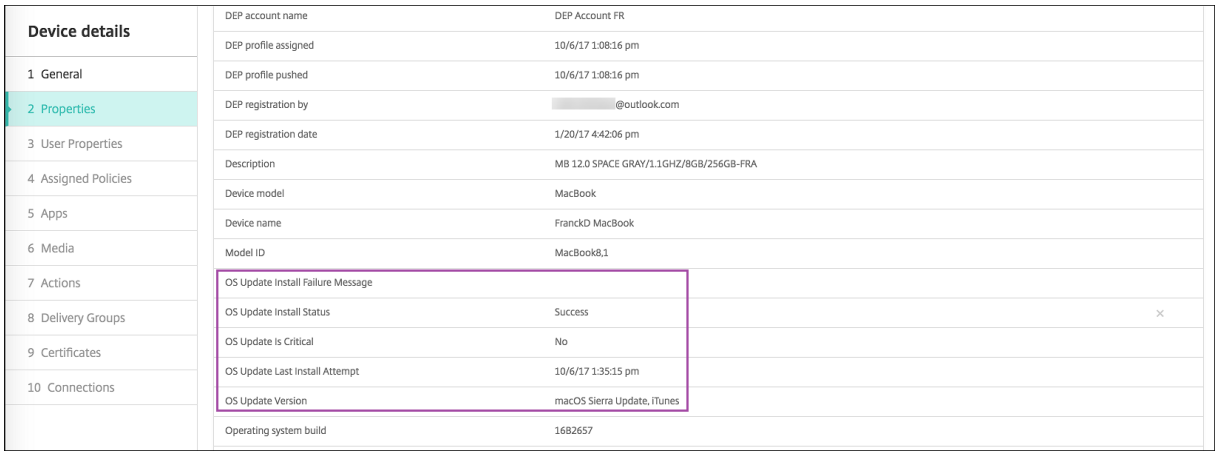
Auf der Seite **Verwalten > Geräte > Gerätedetails** wird der Status geplanter und verfügbarer OS-Updatescans und geplanter macOS- und App-Updates angezeigt.

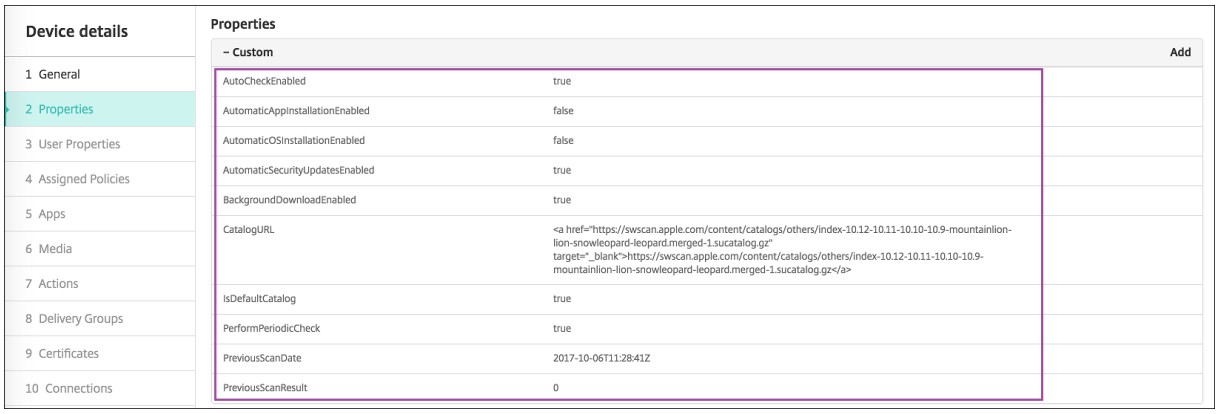


Weitere Informationen zum Status der Updateaktionen finden Sie auf der Seite **Verwalten > Geräte > Gerätedetails (Bereitstellungsgruppen)**.



Weitere Informationen, z. B. verfügbare Betriebssystemupdates und Angaben zum letzten Installationsversuch, finden Sie auf der Seite **Verwalten > Geräte > Gerätedetails (Eigenschaften)**.

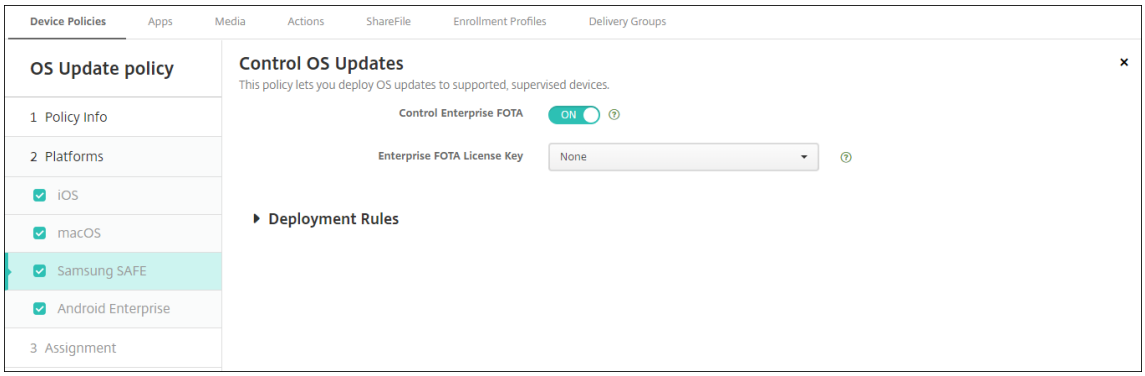




Samsung SAFE-Einstellungen

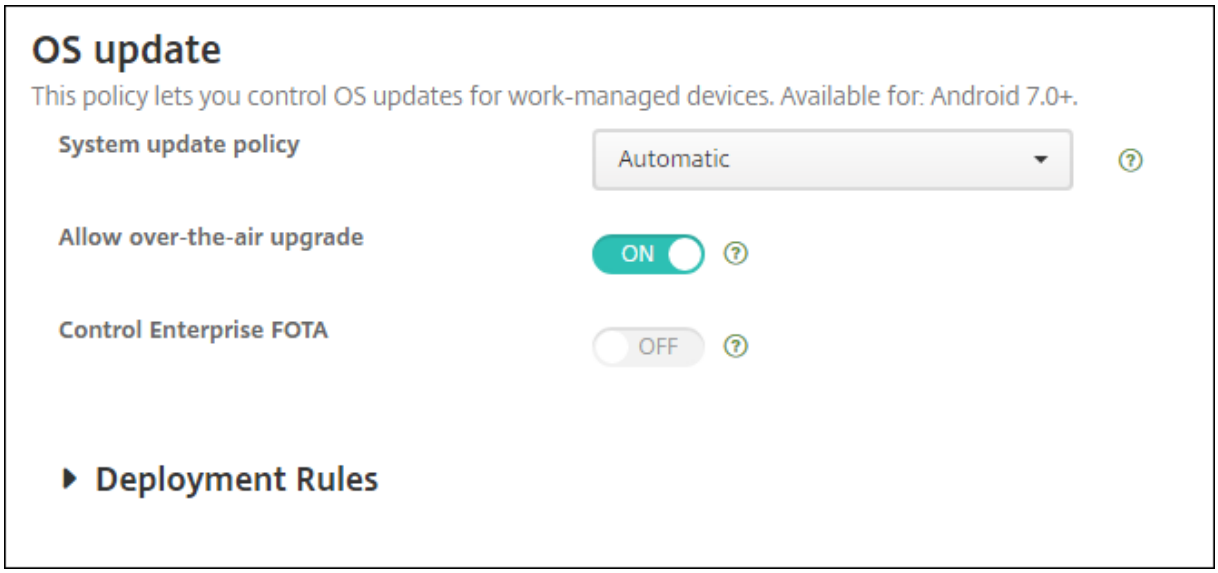
Mit Samsung Enterprise FOTA (E-FOTA) können Sie festlegen, wann Geräte aktualisiert werden und welche Firmwareversion verwendet werden soll. Verwenden von E-FOTA:

1. Erstellen Sie eine Geräterichtlinie für Samsung-MDM-Lizenzschlüssel mit den Schlüsseln und Lizenzinformationen, die Sie von Samsung erhalten haben. Weitere Informationen finden Sie unter Geräterichtlinie für Samsung MDM-Lizenzschlüssel.
2. Erstellen Sie eine Geräterichtlinie zum Steuern von Betriebssystemupdates, um Enterprise FOTA zu aktivieren.



   - **Enterprise FOTA:** Wählen Sie **Ein**.
   - **Enterprise FOTA-Lizenzschlüssel:** Wählen Sie den Namen der Samsung MDM-Lizenzschlüsselrichtlinie aus.

Android Enterprise-Einstellungen



- **Systemupdate:** Diese Richtlinie legt fest, wann Systemupdates durchgeführt werden. Wenn Sie die Einstellung **Enterprise FOTA steuern** aktivieren, werden Updates automatisch ausgeführt, ungeachtet der Konfiguration für diese Einstellung.
  - **Automatisch:** Das Update wird installiert, sobald es verfügbar ist.
  - **Im Wartungsfenster:** Das Update wird automatisch im Rahmen des täglichen Wartungsfensters installiert, das unter **Startzeit** und **Endzeit** definiert ist.

        * **Startzeit:** Start des Wartungsfensters, angegeben in Minuten (**0**–**1440**) nach Mitternacht in der lokalen Zeitzone des Geräts. Die Standardeinstellung ist **0**.
        * **Endzeit:** Ende des Wartungsfensters, angegeben in Minuten (**0**–**1440**) nach Mitternacht in der lokalen Zeitzone des Geräts. Die Standardeinstellung ist **120**.
    - **Verschieben:** Der Benutzer kann die Installation des Updates bis zu 30 Tage verschieben.
- **Drahtloses Upgrade zulassen:** Wenn diese Option deaktiviert ist, können Benutzergeräte keine drahtlosen Softwareupdates empfangen. Die Standardeinstellung ist **Ein**.
- **Enterprise FOTA steuern:** Wenn diese Option aktiviert ist, suchen Samsung-Geräte nach dem neuesten Update und installieren es automatisch. Wenn diese Option deaktiviert ist, können Benutzer nach Updates suchen und diese manuell installieren. Für Android Enterprise-Geräte mit Samsung Knox 3.0 oder höher. Die Standardeinstellung ist **Aus**.
    - **Enterprise FOTA-Lizenzschlüssel:** Wählen Sie den gewünschten Lizenzschlüssel zur Suche nach Updates aus. Sie können diese Einstellung in der Samsung MDM-Lizenzschlüsselrichtlinie konfigurieren. Für Android Enterprise-Geräte mit Samsung Knox 3.0 oder höher. Standardwert ist **Ohne**. Der Schlüssel kann mit der Geräterichtlinie **Samsung MDM-Lizenzschlüssel** festgelegt werden. Weitere Informationen finden Sie unter Geräterichtlinie für Samsung MDM-Lizenzschlüssel.

Richtlinie zum Kopieren von Apps in den Samsung-Container

January 5, 2022

Für bereits auf Geräten installierte Apps können Sie festlegen, dass diese auf unterstützten Samsung-Geräten in einen KNOX-Container kopiert werden. Weitere Informationen zu den unterstützten Geräten finden Sie auf der Website von Samsung unter Geräte mit Knox.

Apps im KNOX-Container sind nur dann verfügbar, wenn die Benutzer sich beim KNOX-Container anmelden.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Voraussetzungen

- Registrieren Sie das Gerät in XenMobile
- Stellen Sie die Samsung MDM-Schlüssel (ELM und KLM) bereit. Eine Anleitung hierzu finden Sie unter Geräterichtlinie für Samsung MDM-Lizenzschlüssel.
- Installieren Sie Apps auf dem Gerät.
- Initialisieren Sie KNOX auf dem Gerät, um Apps in der KNOX-Container zu kopieren.

Plattformeinstellungen

- **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**.

Anmeldeinformationsrichtlinie

January 5, 2022

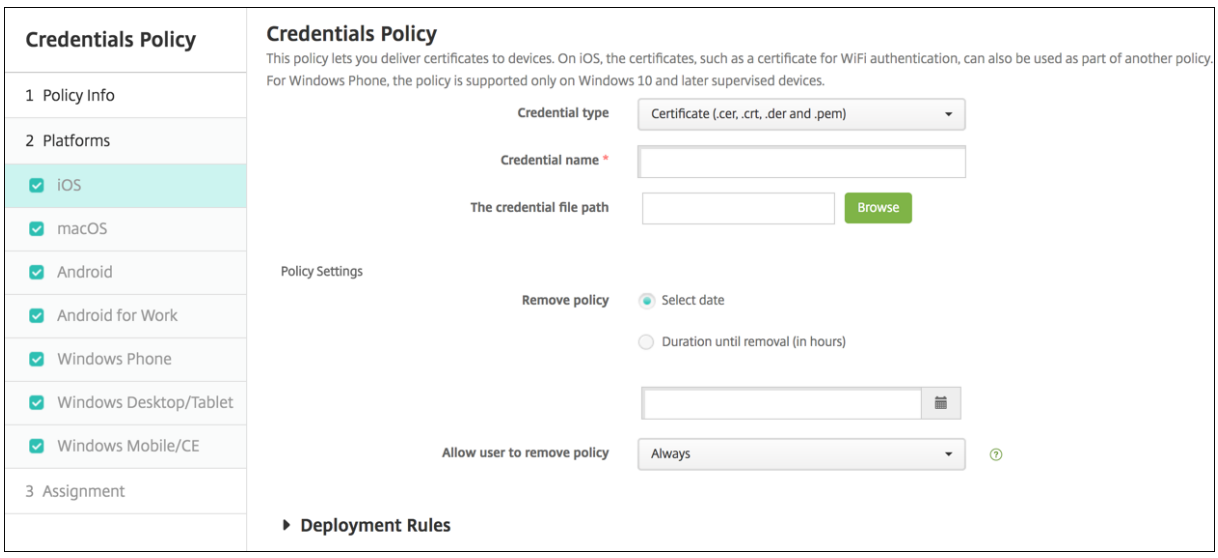
Anmeldeinformationsrichtlinien verweisen auf eine in XenMobile konfigurierte PKI. Die PKI-Konfiguration kann beispielsweise eine PKI-Entität, einen Schlüsselspeicher, einen Anmeldeinformationsanbieter oder ein Serverzertifikat umfassen. Weitere Informationen über Anmeldeinformationen finden Sie unter Zertifikate und Authentifizierung.

Jede unterstützte Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

> **Hinweis:**
>
> Vor dem Erstellen dieser Richtlinie müssen Sie die Anmeldeinformationen für jede Plattform sowie jegliche Zertifikate und Kennwörter zusammenstellen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

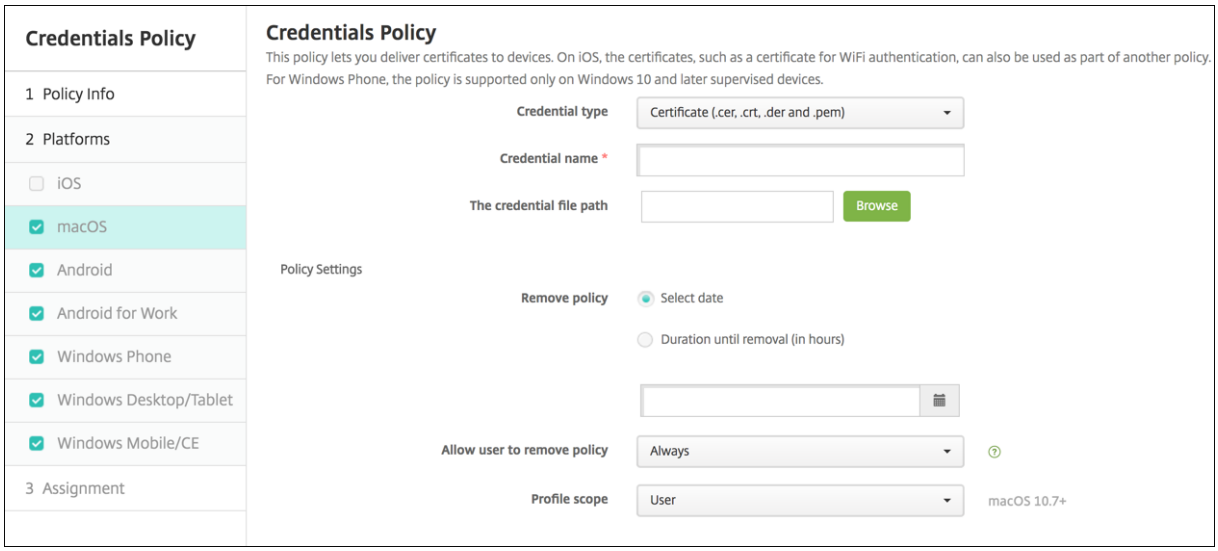
iOS-Einstellungen



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:** Wählen Sie die Anmeldeinformationsdatei, indem Sie auf “Durchsuchen” klicken und zum Speicherort navigieren.
  - **Schlüsselspeicher**
    - **Name der Anmeldeinformationen:** Geben Sie einen eindeutigen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad:** Wählen Sie die Anmeldeinformationsdatei, indem Sie auf “Durchsuchen” klicken und zum Speicherort navigieren.
    - **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**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

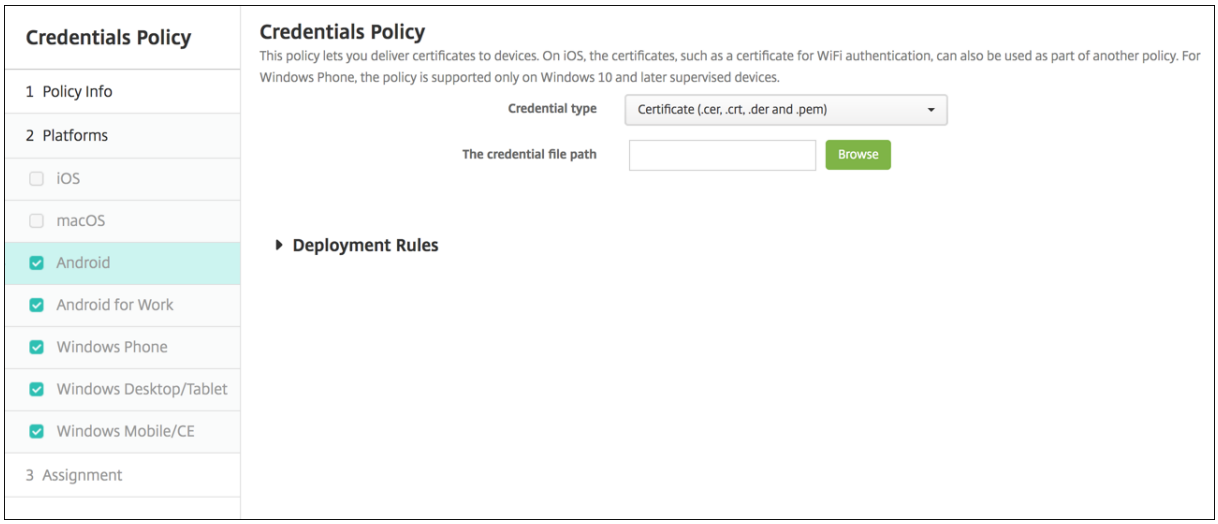
- **Anmeldeinformationstyp:** Klicken Sie in der Liste auf den Typ der Anmeldeinformationen für diese Richtlinie und geben Sie für die ausgewählten Anmeldeinformationen die folgenden Informationen an:
  - **Zertifikat**
    - **Name der Anmeldeinformationen:** Geben Sie einen eindeutigen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad:** Wählen Sie die Anmeldeinformationsdatei, indem Sie auf **Durchsuchen** klicken und zum Speicherort navigieren.
  - **Schlüsselspeicher**
    - **Name der Anmeldeinformationen:** Geben Sie einen eindeutigen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad:** Wählen Sie die Anmeldeinformationsdatei, indem Sie auf **Durchsuchen** klicken und zum Speicherort navigieren.
    - **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**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stun-**

den)

  * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.

- **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
- **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Android-Einstellungen

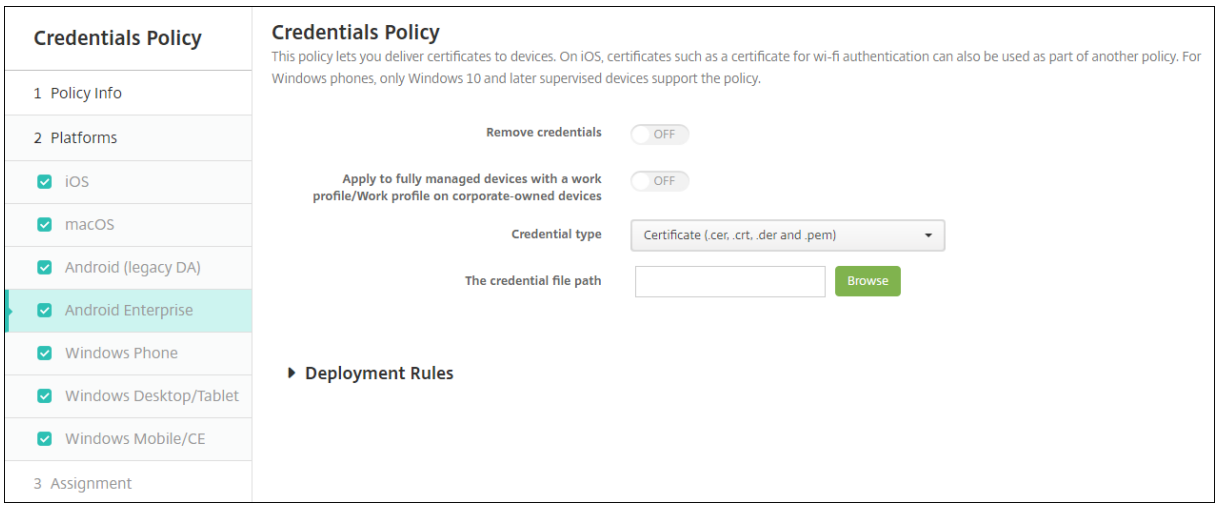


Konfigurieren Sie die folgenden Einstellungen:

- **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:** Wählen Sie die Anmeldeinformationsdatei, indem Sie auf “Durchsuchen” klicken und zu dem Speicherort der Datei navigieren.
  - **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.

Android Enterprise-Einstellungen



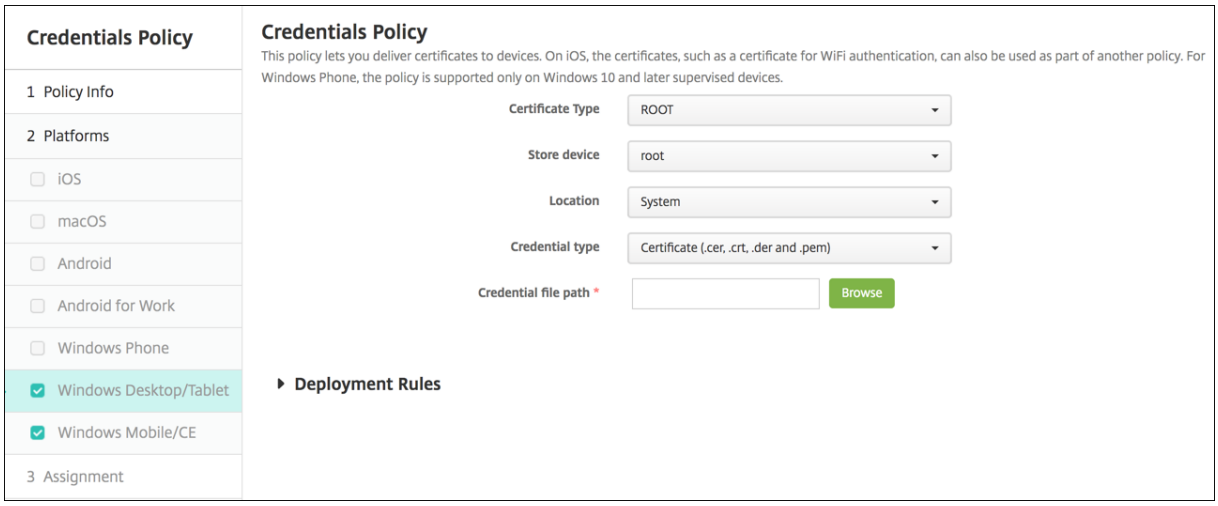
Konfigurieren Sie, wie in XenMobile die Richtlinieneinstellungen angewendet werden:

- **Anmeldeinformationen entfernen:** Legen Sie dies auf **Ein** fest, um die folgenden Einstellungen zu konfigurieren. Die Standardeinstellung ist **Aus**.
    - **Benutzeranmeldeinformationen entfernen:** entfernt Zertifikate aus dem verwalteten Schlüsselspeicher. Die Standardeinstellung ist **Aus**.
    - **Vertrauenswürdige Stammzertifikate entfernen:** deinstalliert alle Zertifikate, die von einer anderen als einer Systemzertifizierungsstelle stammen. Die Standardeinstellung ist **Aus**.
- **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil bzw. Arbeitsprofil auf unternehmenseigenen Geräten anwenden:** Ermöglicht das Konfigurieren von Einstellungen für die Richtlinie “Anmeldeinformationen” für vollständig verwaltete Geräte mit Arbeitsprofil. Bei der Einstellung **Ein** gelten die konfigurierten Einstellungen für Anmeldeinformationen nur für das Arbeitsprofil. Bei der Einstellung **Aus** gelten die konfigurierten Einstellungen für Anmeldeinformationen nur für das Gerät. Die Standardeinstellung ist **Aus**.

Konfigurieren der Einstellungen für die Anmeldeinformationen:

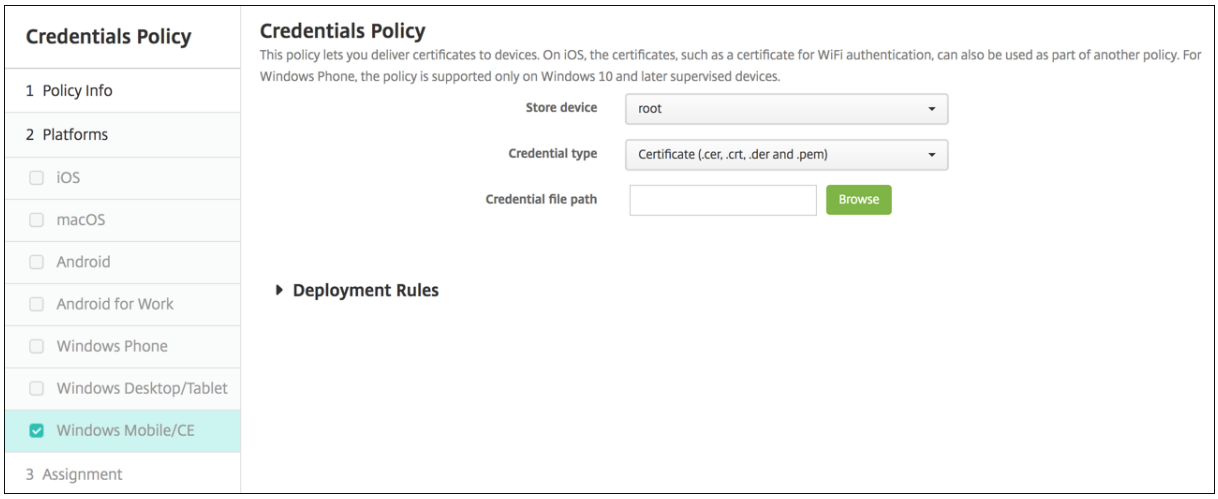
- **Anmeldeinformationstyp:** Klicken Sie in der Liste auf den Typ der Anmeldeinformationen für diese Richtlinie und geben Sie für die ausgewählten Anmeldeinformationen die folgenden Informationen an:
  - **Zertifikat**
    - **Anmeldeinformationsdateipfad:** Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
  - **Schlüsselspeicher**
    - **Anmeldeinformationsdateipfad:** Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
    - **Zertifikatalias:** Ein Zertifikatalias erleichtert Apps den Zugriff auf das Zertifikat. Konfigurieren Sie einen Zertifikatalias in der Geräterichtlinie für verwaltete Android Enterprise-Konfigurationen. Geben Sie dann den Alias in das Feld **Zertifikatalias** in der Geräterichtlinie “Anmeldeinformationen” ein. Apps rufen das Zertifikat ab und authentifizieren das VPN ohne Benutzereingriff.
    - **Kennwort:** Geben Sie das Schlüsselspeicherkennwort für die Anmeldeinformationen ein.
  - **Serverzertifikat**
    - **Serverzertifikat:** Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
  - **Anmeldeinformationsanbieter**
    - **Zertifikatalias:** Ein Zertifikatalias erleichtert Apps den Zugriff auf das Zertifikat. Konfigurieren Sie einen Zertifikatalias in der Geräterichtlinie für verwaltete Android Enterprise-Konfigurationen. Geben Sie dann den Alias in das Feld **Zertifikatalias** in der Geräterichtlinie “Anmeldeinformationen” ein. Apps rufen das Zertifikat ab und authentifizieren das VPN ohne Benutzereingriff.
    - **Anmeldeinformationsanbieter:** Klicken Sie in der Liste auf den Namen des Anmeldeinformationsanbieters.
    - **Apps verwenden Zertifikate:** Um Apps anzugeben, die ohne Benutzereingabe auf Anmeldeinformationen dieses Anbieters zugreifen dürfen, klicken Sie auf **Hinzufügen**, wählen eine App und klicken auf **Speichern**.

Windows Desktop/Tablet-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:** Für Windows 10- und Windows 11-Tablets ist **System** der einzige Speicherort.
  - **Anmeldeinformationstyp:** Für Windows 10- und Windows 11-Tablets 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:** Für Windows 10- und Windows 11-Tablets ist **System** der einzige Speicherort.
- **Anmeldeinformationstyp:** Für Windows 10- und Windows 11-Tablets 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.

Windows Mobile-/CE-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 Stammzertifikaten.
  - **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:** Wählen Sie die Anmeldeinformationsdatei, indem Sie auf **Durchsuchen** klicken und zu dem Speicherort der Datei navigieren.

Benutzerdefinierte XML-Geräterichtlinie

March 31, 2021

Sie können benutzerdefinierte XML-Richtlinien in XenMobile erstellen, um die folgenden Features auf unterstützten Windows- und Zebra-Android- und Android Enterprise-Geräten anzupassen:

- 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

> **Hinweis:**
>
> Verwenden Sie das Zeichen "%" beim Erstellen von XML-Inhalten mit Vorsicht. Das Zeichen "%" wird in XML dafür verwendet, um XML-Sonderzeichen zu schützen. Um % in einem Namen zu verwenden, codieren Sie es als %25.

Windows-Geräte: 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.

Zebra-Android- und Android Enterprise-Geräte: Zum Erstellen einer eigenen XML-Konfiguration wird MX Management System (MXMS) verwendet. Das Erstellen eigener XML-Konfigurationen per MXMS-API geht über den Rahmen dieses Artikels hinaus. Informationen zur Verwendung von MXMS finden Sie unter About MX auf der Website von Zebra.

> **Hinweis:**
>
> Wird auf einem Windows 10 RS2 Phone-Gerät eine benutzerdefinierte XML-Richtlinie oder eine Einschränkungsrichtlinie zum Deaktivieren von Internet Explorer bereitgestellt, verbleibt der Browser im aktivierten Status. Starten Sie als Workaround das Gerät neu. Dies ist ein Drittanbieterproblem.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Einstellungen für Windows Phone, Windows-Desktop/Tablet, Zebra-Android und Android Enterprise

- **XML-Inhalt:** Geben Sie den benutzerdefinierten XML-Code ein, den Sie der Richtlinie hinzufügen möchten, oder kopieren und fügen Sie ihn ein.

  Nach dem Klick auf **Weiter** überprüft XenMobile die Syntax des XML-Inhalts. Syntaxfehler werden unterhalb des Inhaltsfelds angezeigt. Korrigieren Sie alle Fehler, bevor Sie fortfahren.

  Werden keine Syntaxfehler gefunden, wird die Zuweisungsseite **Benutzerdefiniertes XML** angezeigt.

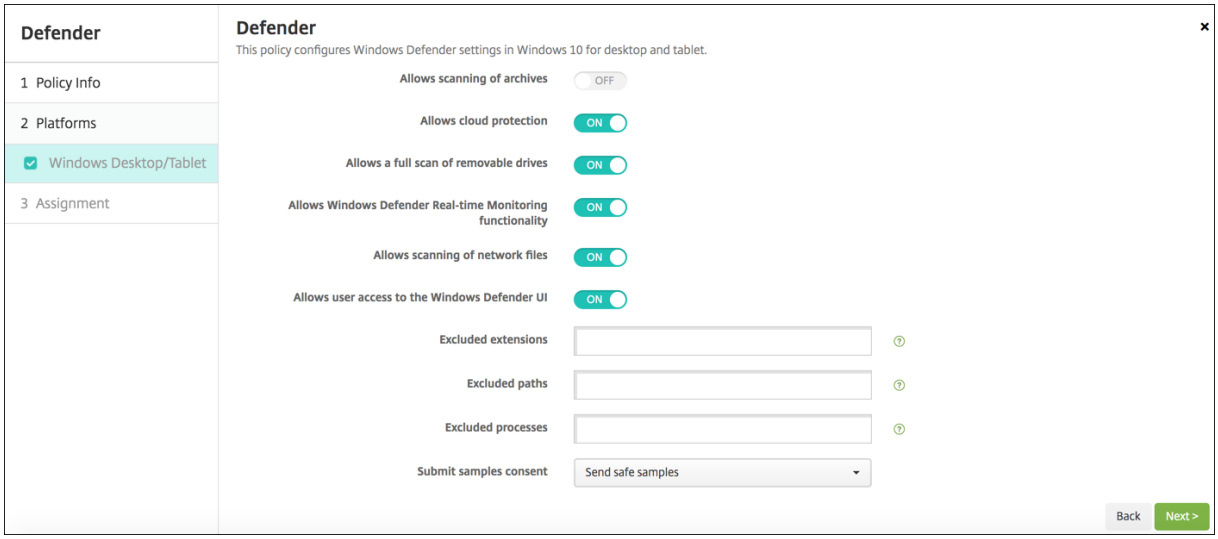
Defender-Geräterichtlinie

January 5, 2022

Bei Windows Defender handelt es sich um ein Programm zum Schutz gegen Malware, das im Lieferumfang von Windows 10 und Windows 11 enthalten ist. Sie können die XenMobile-Geräterichtlinie namens Defender verwenden, um die Microsoft Defender-Richtlinie für Windows 10 und Windows 11 für Desktop und Tablet zu konfigurieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows-Desktop-/Tablet-Einstellungen



- **Ermöglicht das Scannen von Archiven:** ermöglicht oder verweigert Defender das Scannen von Archiven. Die Standardeinstellung ist **Aus**.
- **Ermöglicht Cloud-Schutz:** ermöglicht oder verweigert Defender das Senden von Informationen über Malware-Aktivitäten an Microsoft. Die Standardeinstellung ist **Ein**.
- **Ermöglicht einen vollständigen Scan von Wechseldatenträgern:** ermöglicht oder verweigert Defender das Scannen von Wechseldatenträgern, wie z. B. USB-Sticks. Die Standardeinstellung ist **Ein**.
- **Ermöglicht die Windows Defender-Echtzeitüberwachung:** Die Standardeinstellung ist **Ein**.
- **Ermöglicht das Scannen von Netzwerkdateien:** ermöglicht oder verweigert Defender das Scannen von Netzwerkdateien. Die Standardeinstellung ist **Ein**.
- **Ermöglicht den Benutzerzugriff auf die Benutzeroberfläche von Windows Defender:** gibt an, ob Benutzer auf die Windows Defender-Benutzeroberfläche zugreifen dürfen. Diese Einstellung wird beim nächsten Start des Benutzergeräts wirksam. Wenn diese Einstellung auf **Aus**

gesetzt ist, erhalten Benutzer keine Windows Defender-Benachrichtigungen. Die Standardeinstellung ist **Ein**.

- **Ausgeschlossene Erweiterungen:** die Erweiterungen, die aus Echtzeit- oder geplanten Scans ausgeschlossen werden sollen. Verwenden Sie zum Trennen von Erweiterungen das Zeichen **|**. Beispiel: “lib|obj”.
- **Ausgeschlossene Pfade:** Pfade, die aus Echtzeit- oder geplanten Scans ausgeschlossen werden sollen. Verwenden Sie zum Trennen von Pfaden das Zeichen **|**. Beispiel: “C:\Example|C:\Example1”.
- **Ausgeschlossene Prozesse:** Prozesse, die aus Echtzeit- oder geplanten Scans ausgeschlossen werden sollen. Verwenden Sie zum Trennen von Prozessen das Zeichen **|**. Beispiel: “C:\Example.exe|C:\Example1.exe”.
- **Vereinbarte Proben senden:** steuert das Senden von Proben zur weiteren Analyse an Microsoft-Dateien, um herauszufinden, ob diese bösartig sind. Optionen: **Immer auffordern**, **Sichere Proben senden**, **Nie senden**, **Alle Proben senden**. Die Standardeinstellung lautet **Sichere Proben senden**.

Geräterichtlinie zum Löschen von Dateien und Ordnern

October 25, 2018

Sie können in XenMobile eine Richtlinie erstellen, mit der bestimmte Dateien und Ordner von Windows Mobile-/CE-Geräten gelöscht werden.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Mobile-/CE-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 Datei oder den Ordner zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.

Geräterichtlinie zum Löschen von Registrierungsschlüssel und -werten

October 25, 2018

Sie können in XenMobile eine Richtlinie erstellen, mit der bestimmte Registrierungsschlüssel und -werte von Windows Mobile-/CE-Geräten gelöscht werden.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Mobile-/CE-Einstellungen

- **Folgende Registrierungsschlüssel und -werte löschen:** Klicken Sie für jeden Registrierungsschlüssel und -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 zu verwerfen.

Integritätsnachweisrichtlinie für Geräte

January 5, 2022

Sie können in XenMobile festlegen, dass Windows 10 und Windows 11-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
- Apple-Bereitstellungsprogramm-Richtlinie
- 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 Device HealthAttestation CSP.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Konfigurieren von DHA mit Microsoft Cloud

Fügen Sie eine DHA-Richtlinie für den Integritätsnachweis hinzu und konfigurieren Sie diese Einstellung für jede von Ihnen ausgewählte Plattform:

- **Device Health Attestation aktivieren:** Wählen Sie aus, ob ein Integritätsnachweis erforderlich sein soll. Die Standardeinstellung ist **Aus**.

Konfigurieren von DHA mit einem lokalen Windows DHA-Server

Um DHA on-premises zu aktivieren, konfigurieren Sie zunächst einen DHA-Server. Anschließend erstellen Sie eine XenMobile Server-Richtlinie zum Aktivieren des lokalen DHA-Diensts.

1. Um einen DHA-Server zu konfigurieren, installieren Sie die DHA-Serverrolle auf einer Maschine mit Windows Server 2016 Technical Preview 5 oder höher. Weitere Informationen finden Sie unter Konfigurieren eines lokalen DHA-Servers zum Nachweis der Geräteintegrität.
2. Fügen Sie eine DHA-Richtlinie hinzu und konfigurieren Sie diese Einstellungen:
    - **Device Health Attestation aktivieren:** Wählen Sie **Ein**.
    - **Health Attestation Service lokal konfigurieren:** Wählen Sie **Ein**.
    - **FQDN für lokalen DHA-Server:** Geben Sie den vollqualifizierten Domänennamen des DHA-Servers ein.
    - **Lokale DHA-API-Version:** Wählen Sie die Version des auf dem DHA-Server installierten Diensts.

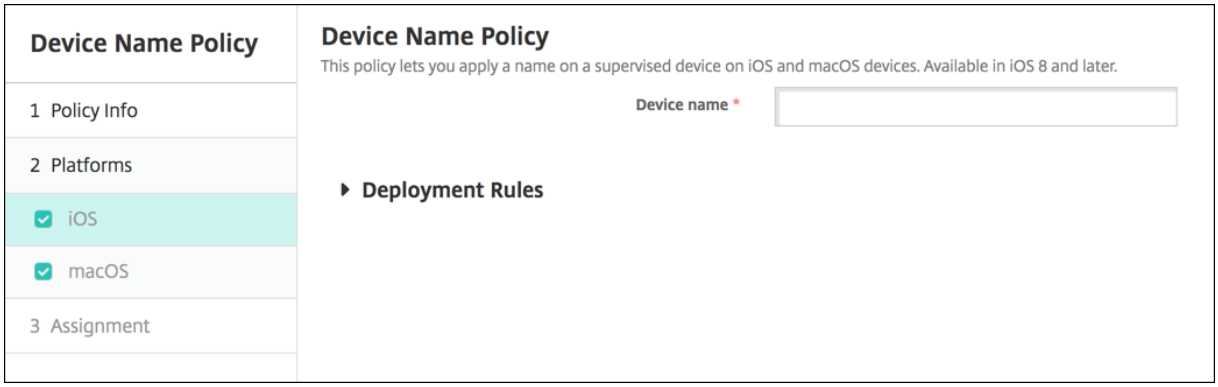
Richtlinien für Gerätenamen

January 5, 2022

Sie können für überwachte iOS- und macOS-Geräte die Namen festlegen, 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 zu Makros finden Sie unter Makros in XenMobile.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS- und macOS-Einstellungen



- **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.

Geräterichtlinie “Bildung - Konfiguration”

November 9, 2020

Die Geräterichtlinie “Bildung - Konfiguration” definiert Folgendes:

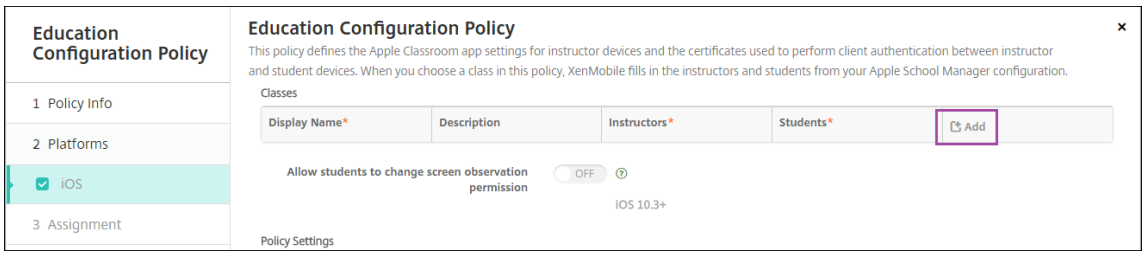
- Einstellungen der Apple Classroom-App für Geräte der Lehrkräfte
- Die Zertifikate für die Clientauthentifizierung zwischen den Geräten der Lehrkräfte und der Lernenden

Wenn Sie in dieser Richtlinie eine Klasse auswählen, werden in der XenMobile-Konsole die Lehrkräfte und Lernenden aus Ihrer Apple School Manager-Konfiguration eingetragen. Erstellen Sie eine Richtlinie, wenn die Apple Classroom App-Einstellungen in dieser Richtlinie für alle Klassen gleich sind.

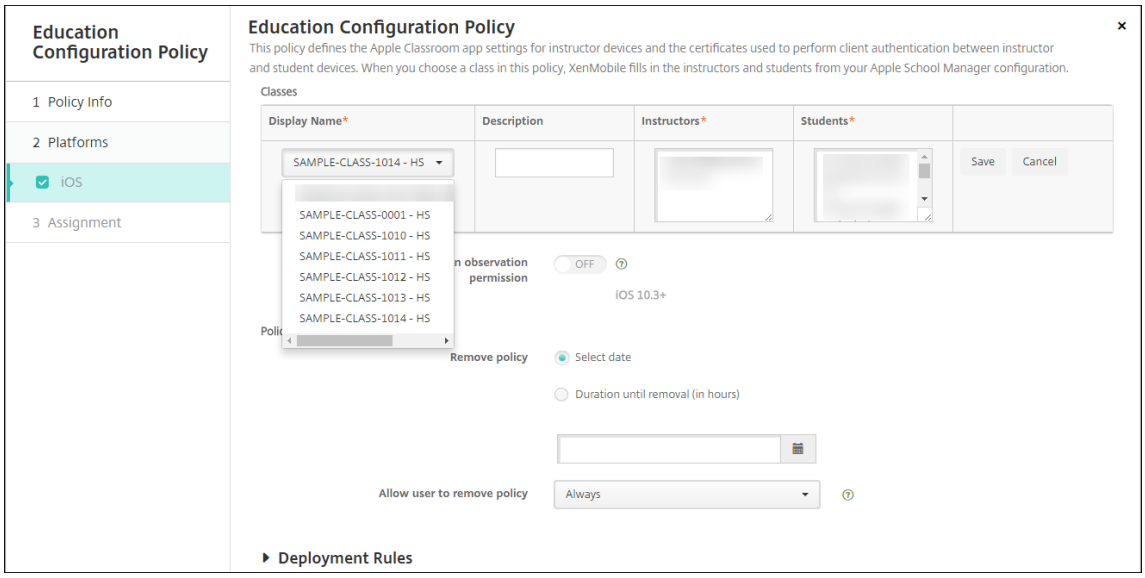
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

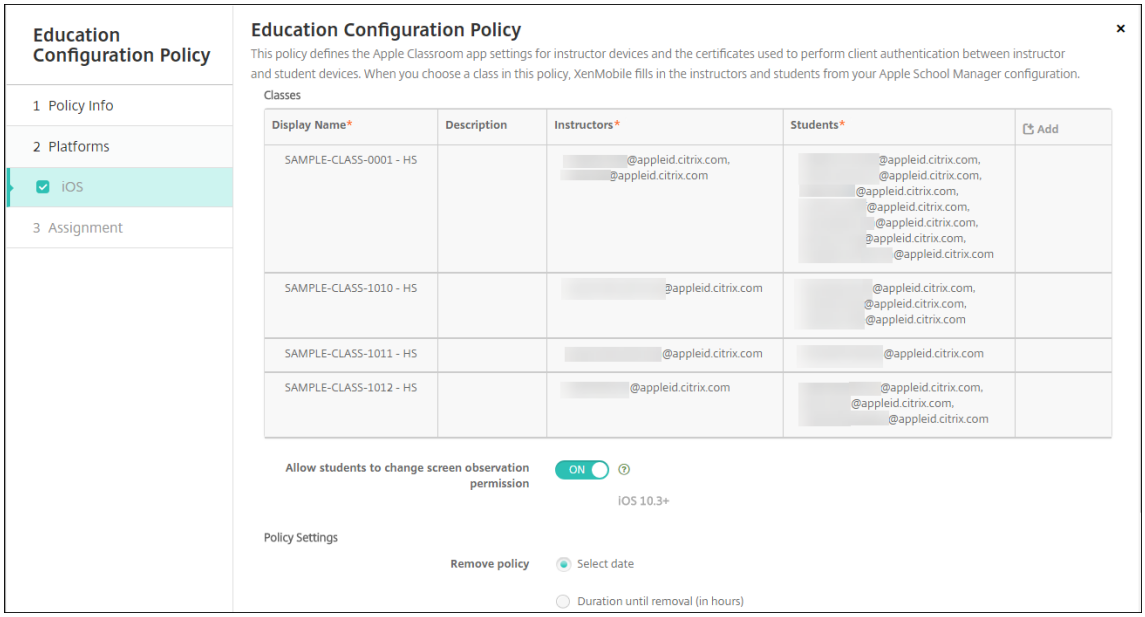
- **Klassen:** Um eine Klasse hinzuzufügen, klicken Sie auf **Hinzufügen**.



Klicken Sie dann auf die Liste **Anzeigename**. Eine Liste der Klassen von Ihrem verbundenen Apple School Manager-Konto wird angezeigt.



Wenn Sie eine Klasse unter **Anzeigename** auswählen, werden die Lehrkräfte und Lernenden von XenMobile automatisch eingetragen. Fügen Sie weitere Klassen hinzu.

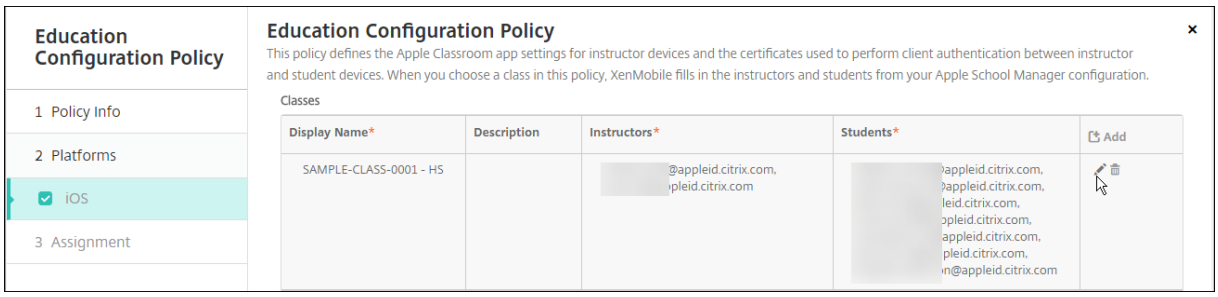


- **Schüler dürfen Berechtigung für Bildschirmansicht ändern:** Wenn diese Option auf **Ein** festgelegt wird, können Lernende in verwalteten Klassen wählen, ob sie der Lehrkraft das Betrachten des Bildschirms auf ihren Geräten gestatten möchten. Die Standardeinstellung ist **Aus**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.

Bearbeiten von Klasseninformationen in der Richtlinie

Sie können einer Klasse eine Beschreibung hinzufügen (“Anzeigename” in der Classroom-App). Sie können außerdem Lehrkräfte und Lernende hinzufügen und entfernen. In XenMobile werden solche Änderungen an Ihrem Apple School Manager-Konto nicht gespeichert. Weitere Informationen finden Sie unter “Verwalten der Daten von Lehrkräften und Lernenden” im Artikel Integration von Apple Bildung-Features.

Zeigen Sie mit der Maus auf die Spalte **Hinzufügen** der Klasse, die Sie bearbeiten möchten, und klicken Sie auf das Bleistiftsymbol.



Um eine Klasse aus der Richtlinie zu löschen, zeigen Sie mit der Maus auf die Spalte **Hinzufügen** der Klasse und klicken Sie dann auf das Papierkorbsymbol.

Unternehmenshub-Geräterichtlinie

October 17, 2019

Mit einer Unternehmenshub-Geräterichtlinie für Windows Phone können Sie Apps über den Unternehmenshub-Unternehmensstore an Geräte verteilen.

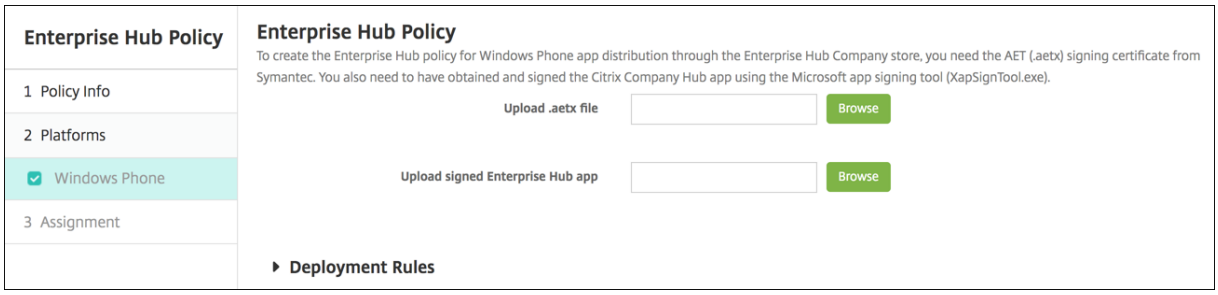
Zum Erstellen der Richtlinie benötigen Sie Folgendes:

- Ein AET-Signaturzertifikat (.aetx) von DigiCert
- 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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Phone-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.

Exchange-Geräterichtlinie

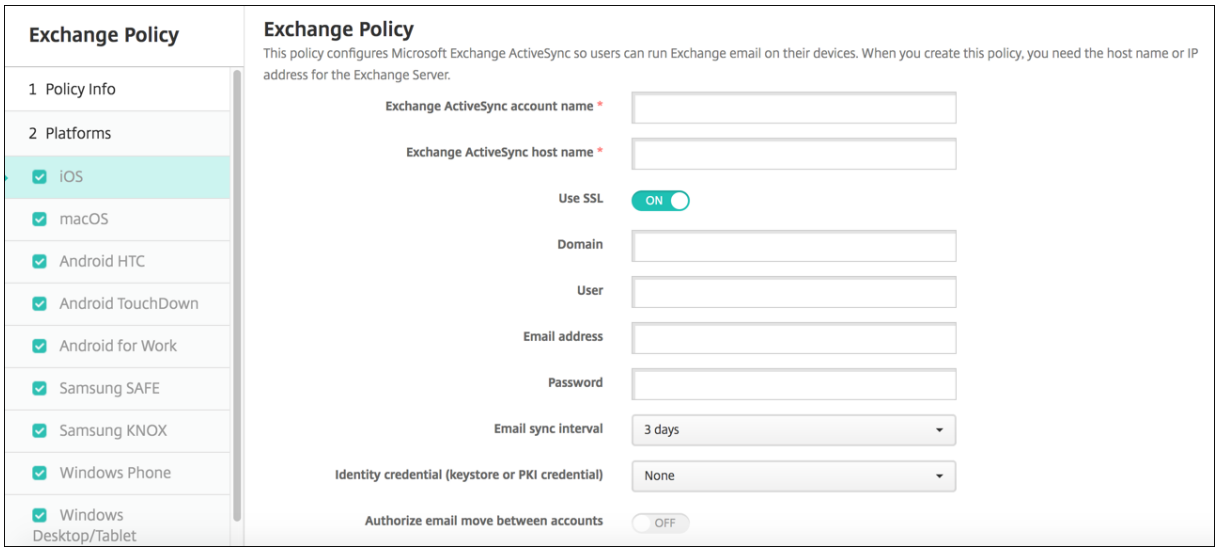
January 5, 2022

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. Sie können Richtlinien für iOS, macOS, Android Enterprise, Samsung SAFE, Samsung KNOX, Windows Phone und Windows Tablet erstellen. Jede Plattform erfordert andere Werte. Diese werden in den folgenden Abschnitten detailliert beschrieben:

Zum Erstellen dieser Richtlinie benötigen Sie den Hostnamen oder die IP-Adresse des Exchange Server-Computers. Informationen zu den ActiveSync-Einstellungen finden Sie in dem Microsoft-Artikel ActiveSync CSP.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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. Die Standardeinstellung ist **Ein**.
- **Domäne:** Geben Sie die Domäne ein, in der sich der Exchange-Server befindet. Sie können in diesem Feld das Systemmakro “$user.domainname” verwenden, um die Domänennamen der Benutzer automatisch zu suchen.
- **Benutzer:** Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro “$user.username” verwenden, um die Benutzernamen automatisch zu suchen.
- **E-Mail-Adresse:** Geben Sie die vollständige E-Mail-Adresse ein. Sie können in diesem Feld das Systemmakro “$user.mail” verwenden, um die E-Mail-Konten der Benutzer automatisch zu suchen.
- **OAuth verwenden:** Mit **Ein** verwendet die Verbindung OAuth für die Authentifizierung. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
- **Kennwort:** Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein. Diese Einstellung wird nicht angezeigt, wenn **OAuth verwenden** auf **Ein** festgelegt ist.
- **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, wenn Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert. Die Standardeinstellung ist **Ohne**.
- **Verschieben von E-Mails zwischen Konten autorisieren:** Geben Sie vor, ob Benutzer E-Mails

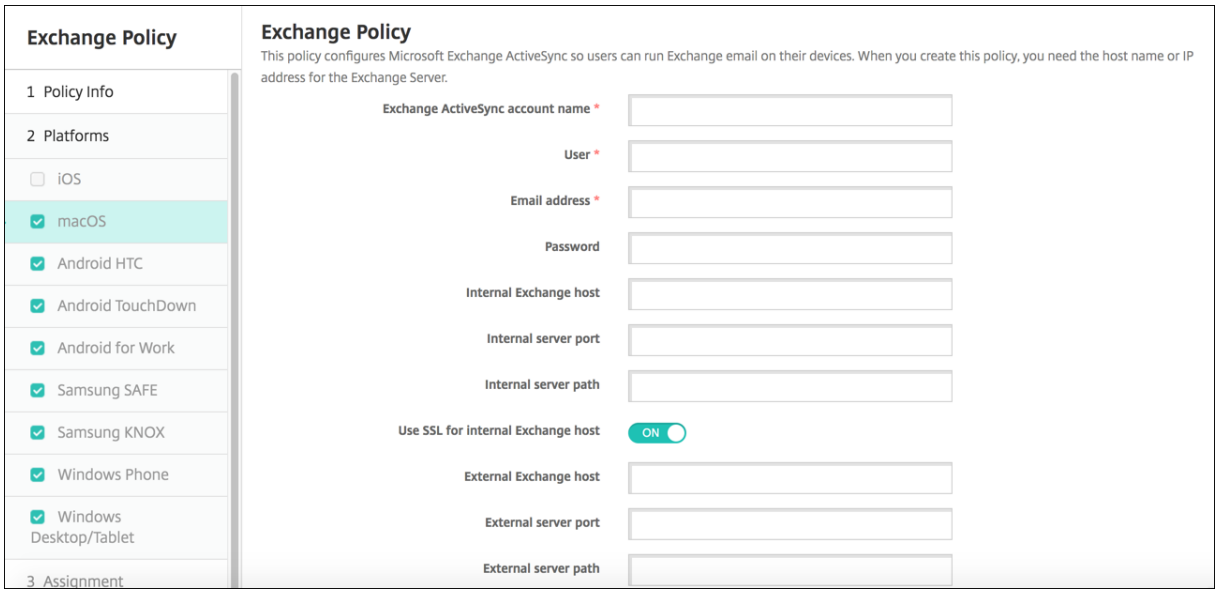
von diesem Konto in ein anderes Konto verschieben und von einem anderen Konto aus weiterleiten dürfen und ob sie von einem anderen Konto aus antworten dürfen. Die Standardeinstellung ist **Aus**.

- **E-Mail nur von Mailanwendung senden:** Wählen Sie aus, ob Benutzer E-Mails nur mit der iOS-E-Mail-App senden dürfen. Die Standardeinstellung ist **Aus**.
- **Synchronisierung aktueller E-Mails deaktivieren:** Wählen Sie aus, ob eine Synchronisierung zuletzt verwendeter Adressen durch die Benutzer verhindert werden soll. Die Standardeinstellung ist **Aus**. Diese Option gilt nur für iOS 6.0 und höher.
- **S/MIME-Signatur aktivieren:** Wählen Sie, ob dieses Konto S/MIME-Signaturen unterstützt. Die Standardeinstellung ist **Ein**. Wenn Sie **Ein** wählen, werden folgende Felder eingeblendet.
  - **Anmeldeinformationen für Signieridentität:** Wählen Sie die Anmeldeinformationen für die Signatur aus.
  - **S/MIME-Signatur von Benutzer überschreibbar:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Signierung in Einstellungen des Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
  - **UUID für S/MIME-Signaturzertifikat von Benutzer überschreibbar:** Mit **Ein** können Benutzer in den Einstellungen ihrer Geräte wählen, welche Anmeldeinformationen für die Signatur verwendet werden. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
- **S/MIME-Verschlüsselung aktivieren:** Wählen Sie, ob dieses Konto S/MIME-Verschlüsselung unterstützt. Die Standardeinstellung ist **Aus**. Wenn Sie **Ein** wählen, werden folgende Felder eingeblendet.
  - **Anmeldeinformationen für Verschlüsselungsidentität:** Wählen Sie die Anmeldeinformationen für die Verschlüsselung aus.
  - **S/MIME-Option für einzelne Nachrichten aktivieren:** Mit **Ein** wird Benutzern für jede Nachricht, die sie erstellen, eine Option zum Aktivieren oder Deaktivieren der S/MIME-Verschlüsselung angezeigt. Die Standardeinstellung ist **Aus**.
  - **Standardmäßige S/MIME-Verschlüsselung von Benutzer überschreibbar:** Mit **Ein** können Benutzer in den Einstellungen ihrer Geräte auswählen, ob S/MIME standardmäßig aktiviert ist. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
  - **UUID für S/MIME-Verschlüsselungszertifikat von Benutzer überschreibbar:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Verschlüsselungsidentität und Verschlüsselung in den Einstellungen des Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen

anzugeben.

* **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

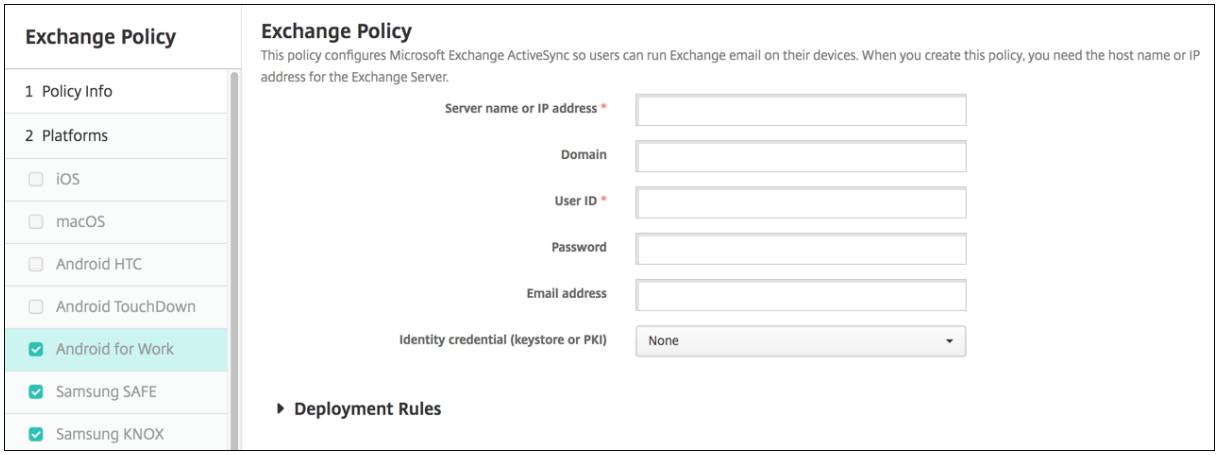
macOS-Einstellungen



- **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 “$user.username” verwenden, um die Benutzernamen automatisch zu suchen.
- **E-Mail-Adresse:** Geben Sie die vollständige E-Mail-Adresse ein. Sie können in diesem Feld das Systemmakro “$user.mail” verwenden, um die E-Mail-Konten der Benutzer automatisch zu suchen.
- **OAuth verwenden:** Mit **Ein** verwendet die Verbindung OAuth für die Authentifizierung. Die Standardeinstellung ist **Aus**. Diese Option gilt für macOS 10.14 und höher.
- **OAuth-Anmelde-URL:** Gibt die Anmelde-URL an, die in eine Webansicht für die Authentifizierung mit OAuth geladen wird, wenn Sie Autodiscovery nicht verwenden. Dieses Feld wird angezeigt, wenn **OAuth verwenden** auf **Ein** gesetzt ist.
- **Kennwort:** Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein. Diese Einstellung wird nicht angezeigt, wenn **OAuth verwenden** auf **Ein** festgelegt ist.
- **Interner Exchange-Host:** Soll intern ein anderer Exchange-Hostname verwendet werden als extern, geben Sie einen internen Exchange-Hostnamen ein.

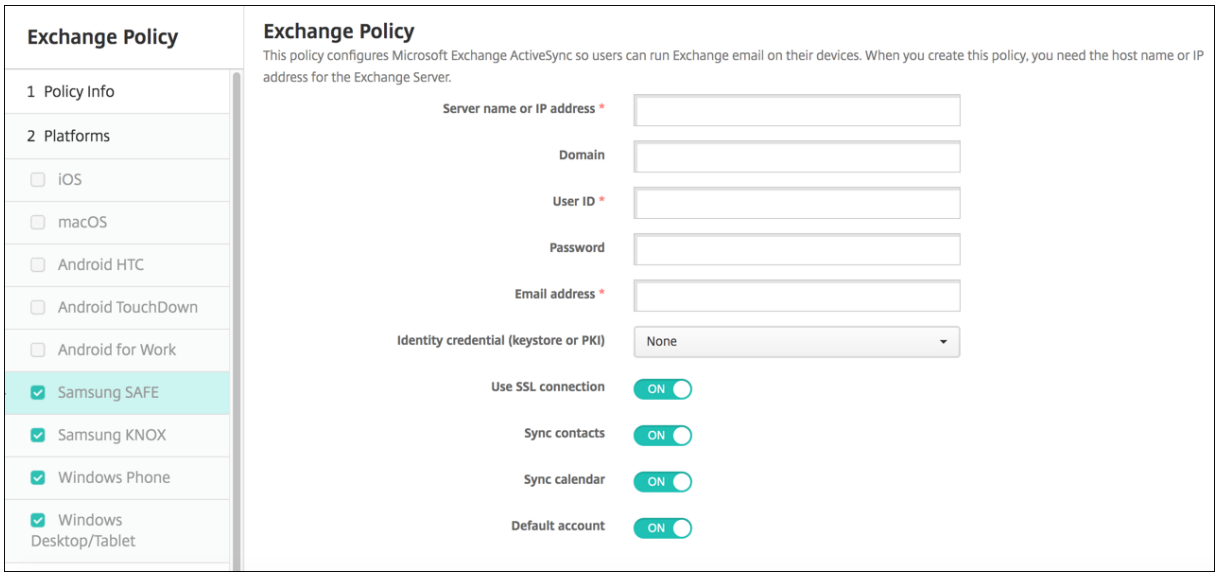
- **Interner Serverport:** Soll intern ein anderer Exchange-Serverport verwendet werden als extern, geben Sie eine interne Exchange-Serverportnummer ein.
- **Interner Serverpfad:** Soll intern ein anderer Exchange-Serverpfad verwendet werden als extern, geben Sie einen internen Exchange-Serverpfad ein.
- **SSL für internen Exchange-Host verwenden:** Wählen Sie aus, ob zwischen Benutzergeräten und dem internen Exchange-Host sichere Verbindungen verwendet werden sollen. Die Standardeinstellung 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. Die Standardeinstellung ist **Ein**.
- **Mail Drop zulassen:** Legen Sie fest, ob Benutzer Dateien zwischen zwei Macs ohne Verbindung mit einem vorhandenen Netzwerk drahtlos teilen können. Die Standardeinstellung ist **Aus**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Android Enterprise



- **Servername oder IP-Adresse:** Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.
- **Domäne:** Geben Sie die Domäne ein, in der sich der Exchange-Server befindet. Sie können in diesem Feld das Systemmakro “$user.domainname” verwenden, um die Domänennamen der Benutzer automatisch zu suchen.
- **Benutzer-ID:** Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro “$user.username” verwenden, um die Benutzernamen automatisch zu suchen.
- **Kennwort:** Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.
- **E-Mail-Adresse:** Geben Sie die vollständige E-Mail-Adresse ein. Sie können in diesem Feld das Systemmakro “$user.mail” verwenden, um die E-Mail-Konten der Benutzer automatisch zu suchen.
- **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen):** Klicken Sie in dieser Liste optional auf Identitätsanmeldeinformationen, wenn Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert. Die Standardeinstellung ist **Ohne**.

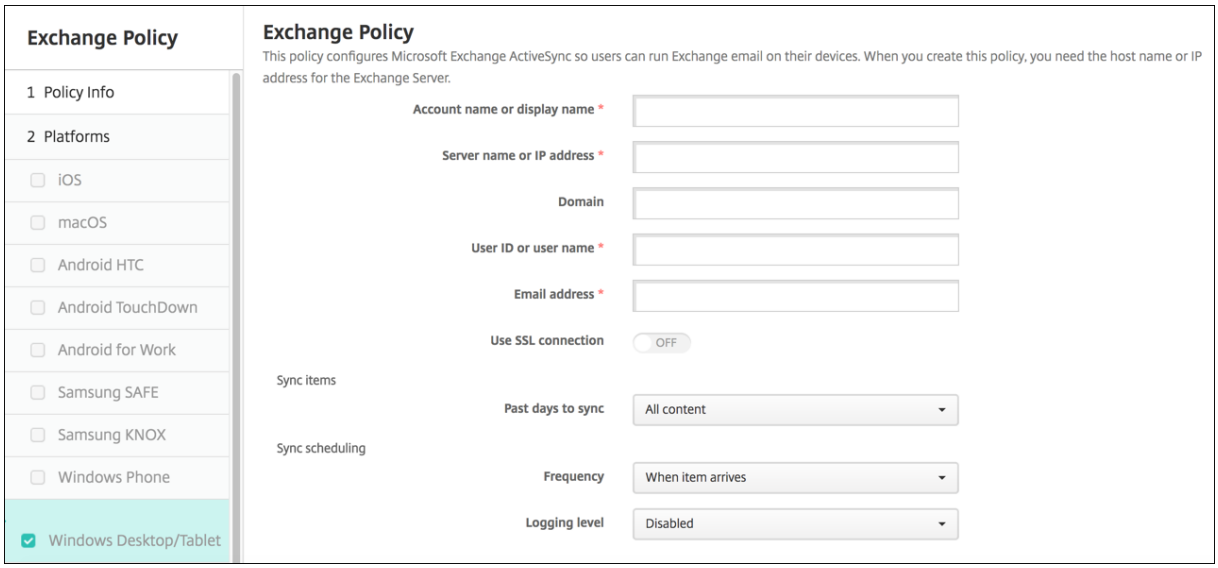
Samsung SAFE- und Samsung KNOX-Einstellungen



- **Servername oder IP-Adresse:** Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.
- **Domäne:** Geben Sie die Domäne ein, in der sich der Exchange-Server befindet. Sie können in diesem Feld das Systemmakro “$user.domainname” verwenden, um die Domänennamen der Benutzer automatisch zu suchen.
- **Benutzer-ID:** Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro “$user.username” verwenden, um die Benutzernamen automatisch zu suchen.
- **Kennwort:** Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.
- **E-Mail-Adresse:** Geben Sie die vollständige E-Mail-Adresse ein. Sie können in diesem Feld das Systemmakro “$user.mail” verwenden, um die E-Mail-Konten der Benutzer automatisch zu suchen.
- **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen):** Klicken Sie in dieser Liste optional auf Identitätsanmeldeinformationen, wenn Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert.
- **SSL-Verbindung verwenden:** Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Die Standardeinstellung ist **Ein**.
- **Kontakte synchronisieren:** Wählen Sie aus, ob die Synchronisierung von Kontakten zwischen den Benutzergeräten und dem Exchange Server ermöglicht werden soll. Die Standardeinstellung ist **Ein**.
- **Kalender synchronisieren:** Wählen Sie aus, ob die Synchronisierung des Kalenders zwischen den Benutzergeräten und dem Exchange Server ermöglicht werden soll. Die Standardeinstellung 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. Die Standardeinstellung ist **Ein**.

Windows Phone- und Windows Desktop-/Tablet-Einstellungen



Hinweis:

Mit dieser Richtlinie kann das Benutzerkennwort nicht festgelegt werden. 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 sich der Exchange-Server befindet. Sie können in diesem Feld das Systemmakro “$user.domainname” verwenden, um die Domänennamen der Benutzer automatisch zu suchen.
- **Benutzer-ID oder Benutzername:** Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro “$user.username” verwenden, um die Benutzernamen automatisch zu suchen.
- **E-Mail-Adresse:** Geben Sie die vollständige E-Mail-Adresse ein. Sie können in diesem Feld das Systemmakro “$user.mail” verwenden, um die E-Mail-Konten der Benutzer automatisch zu suchen.
- **SSL-Verbindung verwenden:** Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Die Standardeinstellung ist **Aus**.
- **Zu synchronisierende Tage:** Wählen Sie in der Liste, 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**.

Dateirichtlinie

May 4, 2021

Sie können Dateien hinzufügen und Benutzern für den Zugriff über Android- und Android Enterprise-Geräte bereitstellen. Sie geben das Verzeichnis an, in dem Sie die Datei auf dem Gerät speichern möchten. Angenommen, Sie möchten Benutzern ein Geschäftsdokument oder eine PDF-Datei zukommen lassen. Stellen Sie die Datei auf den Geräten bereit und informieren Sie die Benutzer, wo sie sich befindet.

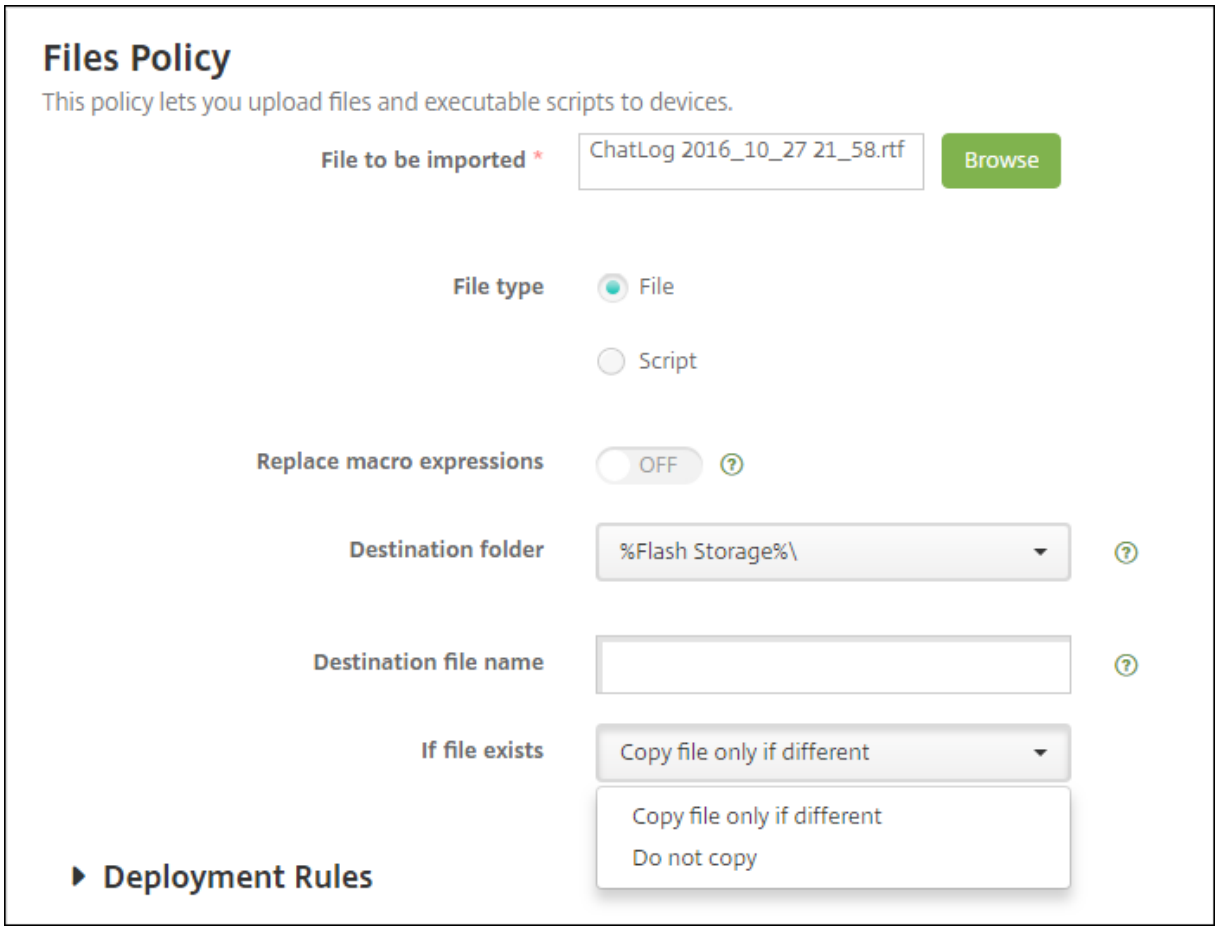
Android-Geräte unterstützen nativ keine Skriptausführung. Zur Skriptausführung wird Software von Drittanbietern benötigt.

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

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android Enterprise-Einstellungen



- **Zu importierende Datei:** Klicken Sie zur Auswahl der zu importierenden Datei auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.
- **Dateityp:** Wählen Sie **Datei** oder **Skript** aus.
- **Sofort ausführen:** Wenn Sie **Skript** auswählen, wird die Option **Sofort ausführen** angezeigt. Wenn Sie diese Einstellung aktivieren, passiert nichts. Die Benutzer müssen das Skript manuell ausführen. **Makroausdrücke ersetzen:** Wählen Sie, ob die Namen von Makrotoken in einem Skript durch eine Geräte- oder Benutzereigenschaft ersetzt werden. Informationen zur Makrosyntax finden Sie unter Makros. Die Standardeinstellung 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 jeder Pfad-ID verwenden.
- **Zieldateiname:** Optional. Geben Sie einen Dateinamen ein, wenn Sie den Namen vor der Bereitstellung auf einem Gerät ändern müssen.
- **Wenn Datei existiert:** Wählen Sie in der Liste aus, ob eine vorhandene Datei kopiert werden soll. Die Standardeinstellung ist **Datei nur kopieren, wenn unterschiedlich**.

Android-Einstellungen

- **Zu importierende Datei:** Klicken Sie zur Auswahl der zu importierenden Datei auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.
- **Dateityp:** Wählen Sie **Datei** oder **Skript** aus.
- **Sofort ausführen:** Wenn Sie **Skript** auswählen, wird die Option **Sofort ausführen** angezeigt. Wenn Sie diese Einstellung aktivieren, passiert nichts. Die Benutzer müssen das Skript manuell ausführen. **Makroausdrücke ersetzen:** Wählen Sie, ob die Namen von Makrotoken in einem Skript durch eine Geräte- oder Benutzereigenschaft ersetzt werden. Die Standardeinstellung 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.

Windows Mobile-/CE-Einstellungen

- **Zu importierende Datei:** Klicken Sie zur Auswahl der zu importierenden Datei auf "Durchsuchen" und navigieren Sie zum Speicherort der Datei.
- **Dateityp:** Wählen Sie **Datei** oder **Skript** aus.
- **Sofort ausführen:** Wenn Sie **Skript** auswählen, wird **Sofort ausführen** angezeigt. Legen Sie fest, ob das Skript ausgeführt werden soll, sobald die Datei hochgeladen wurde. Die Standardeinstellung ist **Aus**.
- **Makroausdrücke ersetzen:** Wählen Sie, ob die Namen von Makrotoken in einem Skript durch eine Geräte- oder Benutzereigenschaft ersetzt werden. Die Standardeinstellung 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%\
  - %My Documents%\
  - %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. Die Standardeinstellung ist **Aus**.
- **Versteckte Datei:** Wählen Sie aus, ob die Datei aus der Liste ausgeblendet werden soll. Die Standardeinstellung ist **Aus**.

FileVault-Geräterichtlinie

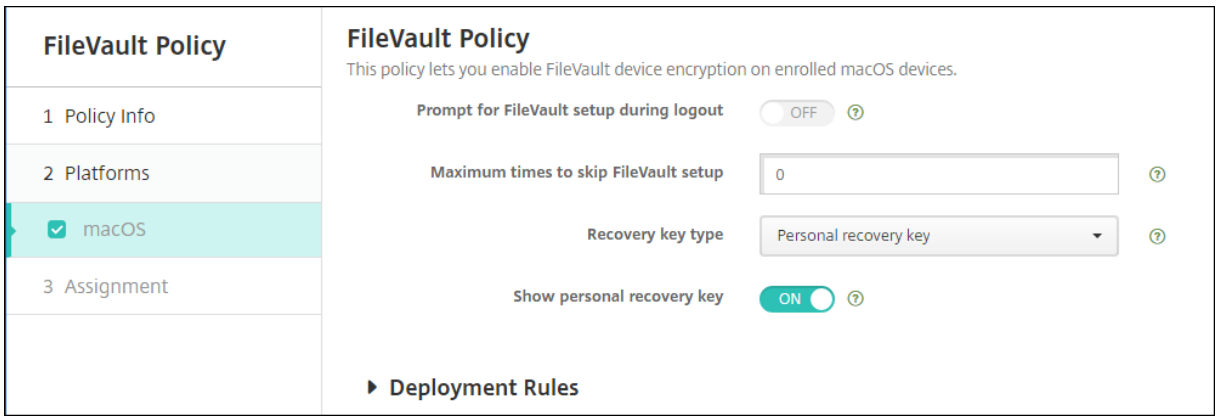
January 5, 2022

Die macOS-FileVault-Datenträgerverschlüsselung schützt das Systemvolume durch Verschlüsselung der Inhalte. Wenn FileVault auf einem macOS-Gerät aktiviert ist, meldet sich der Benutzer bei jedem Start des Geräts mit seinem Kontokennwort an. Verliert der Benutzer sein Kennwort, kann er die Festplatte mit einem Wiederherstellungsschlüssel entsperren und sein Kennwort zurücksetzen.

Die XenMobile-Geräterichtlinie "FileVault" aktiviert Bildschirme zur FileVault-Benutzereinrichtung und konfiguriert Einstellungen wie z. B. den Wiederherstellungsschlüssel. Informationen zu FileVault finden Sie beim Apple-Support unter https://support.apple.com.

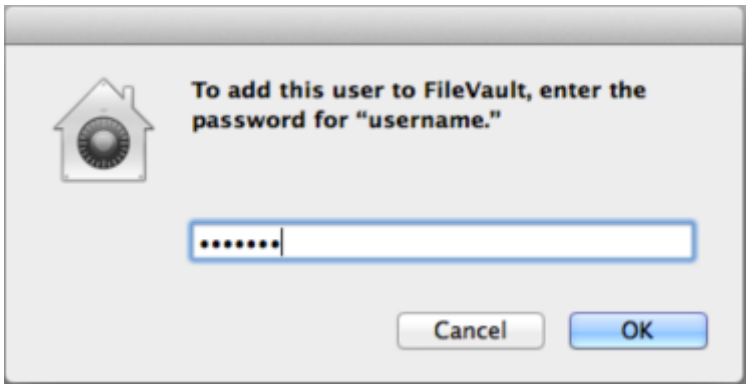
Zum Hinzufügen der FileVault-Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**.

macOS-Einstellungen

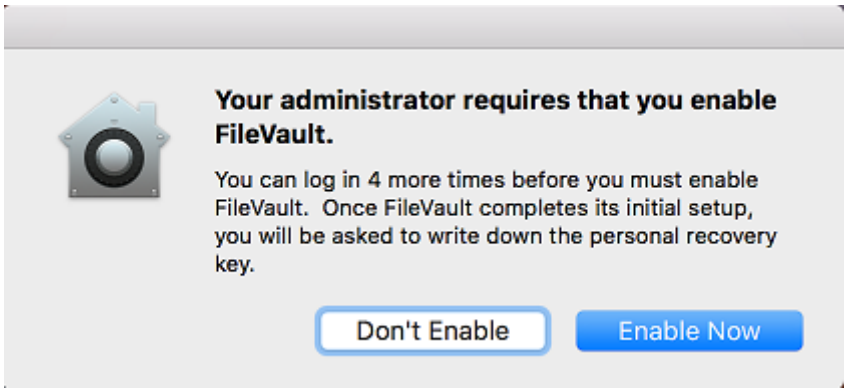


- **Beim Abmelden zum Einrichten von FileVault auffordern:** Wenn diese Option auf **Ein** festgelegt ist, wird der Benutzer bei den nächsten N Abmeldungen aufgefordert, FileVault zu aktivieren. Die Zahl der Abmeldungen (N) wird über die Option **Male, die das Einrichten von FileVault übersprungen werden darf** festgelegt. Bei Auswahl von **Aus** wird die Aufforderung zur Eingabe des FileVault-Kennworts nicht angezeigt.

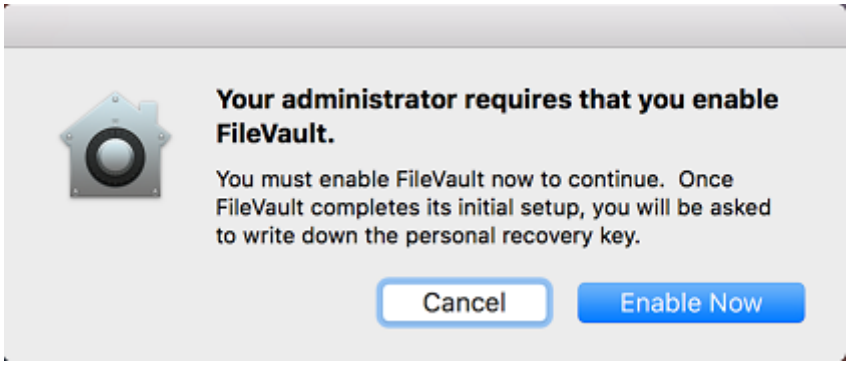
Nachdem Sie die FileVault Richtlinie mit dieser Einstellung bereitgestellt haben, wird der folgende Bildschirm angezeigt, wenn ein Benutzer das Gerät abmeldet. Der Bildschirm bietet dem Benutzer die Möglichkeit, FileVault vor dem Abmelden zu aktivieren.

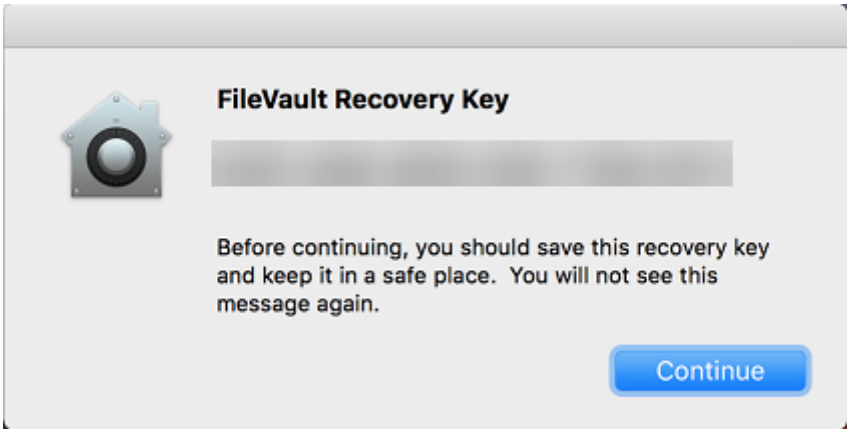


Wenn **Male, die das Einrichten von FileVault übersprungen werden darf** nicht 0 ist: Nachdem Sie die FileVault-Richtlinie ohne diese Einstellung bereitgestellt haben, wird bei der Anmeldung des Benutzers der folgende Bildschirm angezeigt.



Wenn für **Male, die das Einrichten von FileVault übersprungen werden darf** der Wert 0 ist oder der Benutzer die Einrichtung so oft wie zulässig übersprungen hat, wird der folgende Bildschirm angezeigt:





Geräterichtlinie für Schriftarten

April 16, 2020

Sie können in XenMobile eine Geräterichtlinie einrichten, mit der zusätzliche Schriftarten auf iOS- und macOS-Geräten hinzugefügt werden. Schriftarten müssen im Format TrueType (.ttf) oder OpenType (.oft) vorliegen. Schriftsammlungen (.ttc oder .otc) werden nicht unterstützt.

Für iOS gilt die Richtlinie nur ab Version 7.0 und höher.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-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**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Geräterichtlinie für Homebildschirmlayout

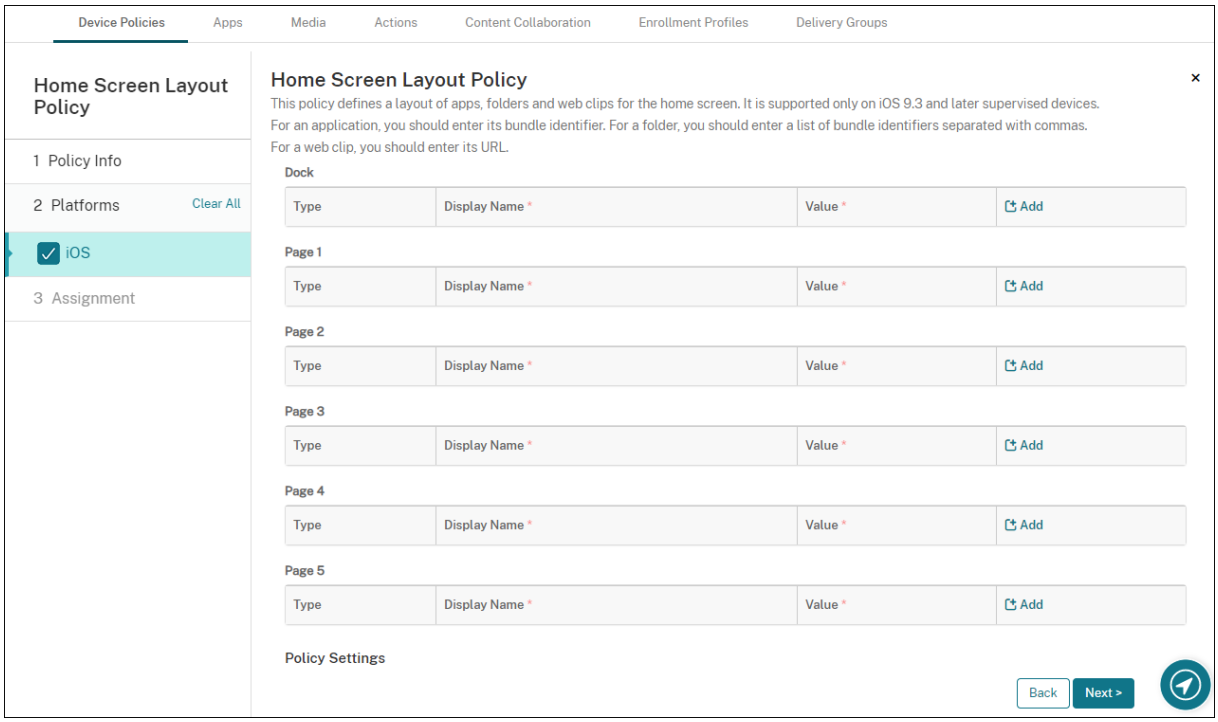
March 31, 2021

Sie können die Anordnung von Apps und Ordnern auf dem iOS-Homebildschirm angeben. Die Geräterichtlinie für das Homebildschirmlayout gilt für betreute Geräte mit iOS 9.3 und höher.

> **Wichtig:**
>
> Wenn mehrere Richtlinien für das Homebildschirmlayout auf einem Gerät bereitgestellt werden, führt dies zu einem iOS-Fehler auf dem Gerät. Diese Einschränkung gilt unabhängig davon, ob Sie den Homebildschirm über diese XenMobile-Richtlinie oder den Apple Configurator definieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

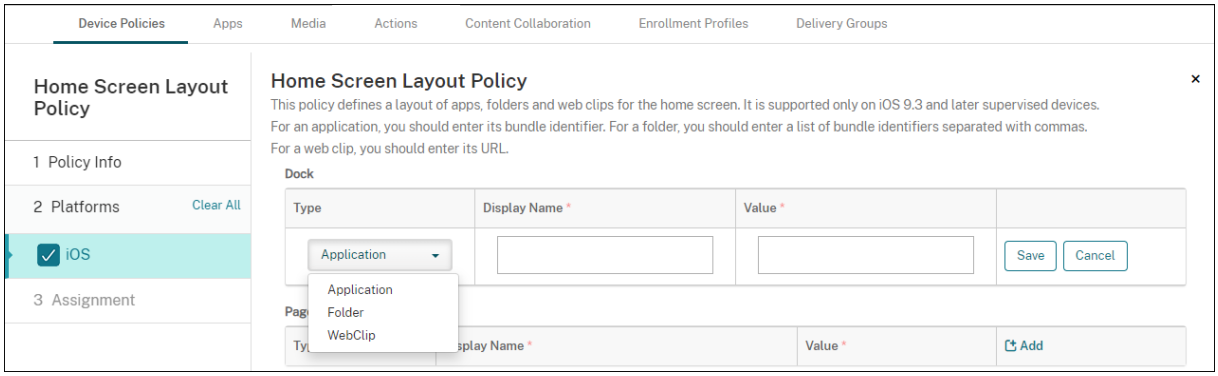
iOS-Einstellungen



- Klicken Sie für jeden der Bildschirmbereiche, die Sie konfigurieren möchten (wie **Dock** oder **Seite 1**) auf **Hinzufügen**.
- **Typ:** Wählen Sie **Anwendung**, **Ordner** oder **Webclip**.

  Die Einstellung **Eingeschränkte App-Verwendung > Nur einige Apps zulassen** in der Geräteeinschränkungsrichtlinie kann zu einer fehlerhaften Anzeige von Webclips auf dem Homebildschirm führen. Damit Webclips ordnungsgemäß angezeigt werden, führen Sie einen der folgenden Schritte aus:

  - Setzen Sie **Eingeschränkte App-Verwendung** auf **Alle Apps zulassen** oder **Einige Apps nicht zulassen**.
  - Wenn Sie für **Einschränkte App-Verwendung** die Option **Nur einige Apps zulassen** verwenden, fügen eine App mit der Paket-ID `com.apple.webapp` hinzu, um Webclips zuzulassen.



- **Anzeigename:** der Name, der auf dem Homebildschirm für die App oder den Ordner angezeigt wird.
- **Wert:** Geben Sie für Apps die Paket-ID ein. Für Ordner geben Sie eine Liste mit Paket-IDs ein (durch Kommas getrennt). Für Webclips geben Sie die Paket-ID `com.apple.webClip.managed` ein und konfigurieren die URL des Webclips in der Webclip-Richtlinie. Wenn mehr als ein Webclip-Wert mit derselben URL vorhanden ist, bleibt das Verhalten auf Geräten mit iOS 11.3 und höher nicht definiert.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur unter iOS 9.3 und höher verfügbar.

Richtlinie zum Importieren von iOS- und macOS-Profilen

January 5, 2022

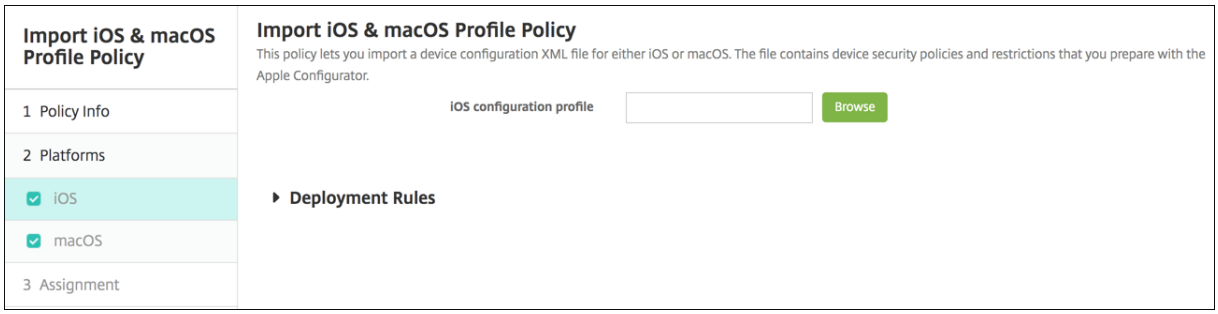
Sie können XML-Dateien für die Konfiguration von iOS- und macOS-Geräten in XenMobile importieren. Die Datei enthält Gerätesicherheitsrichtlinien und -einschränkungen, die Sie mit Apple Configurator vorbereitet haben.

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 unter Apple Configurator Support.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS- und macOS-Einstellungen



- **iOS-Konfigurationsprofil** oder **macOS-Konfigurationsprofil**: Klicken Sie zur Auswahl der Konfigurationsdatei auf **Durchsuchen**, navigieren Sie zum Speicherort der Datei und wählen Sie diese aus.

Versetzen eines iOS-Geräts mit Apple Configurator in den betreuten Modus

Zur Verwendung des Apple Configurators brauchen Sie einen Apple-Computer mit macOS 10.7.2 oder höher.

> **Wichtig:**
>
> 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 den 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**.

Geräterichtlinie für die Keyguard-Verwaltung

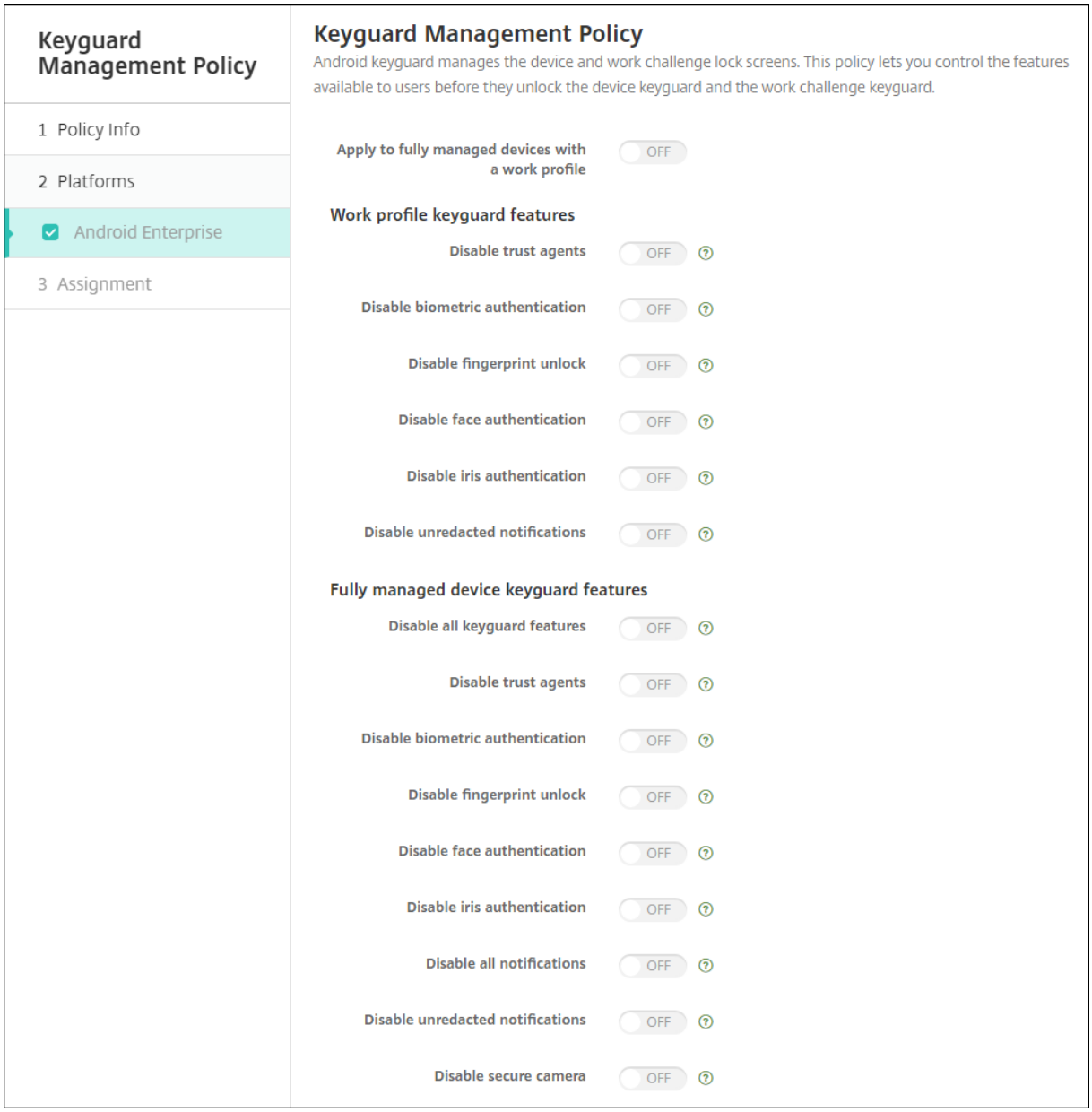
December 21, 2020

Android Keyguard verwaltet die Sperrbildschirme für Gerät und Arbeitsprofil. Mit dieser Richtlinie können Sie Funktionen für den Android Enterprise Arbeitsprofil-Keyguard und erweiterte Funktionen für den Geräte-Keyguard steuern. Sie können Folgendes steuern:

- Keyguard-Verwaltung auf Arbeitsprofilgeräten. Sie können die Funktionen steuern, die Benutzern zur Verfügung stehen, bevor sie den Geräte-Keyguard und den Arbeitsprofil-Keyguard entsperren. Beispielsweise können Benutzer standardmäßig das Entsperren per Fingerabdruck verwenden und unredigierte Benachrichtigungen auf dem Sperrbildschirm anzeigen.
- Keyguard-Verwaltung auf vollständig verwalteten und dedizierten Geräten. Sie können festlegen, ob Funktionen wie “Trust Agents” und “Sichere Kamera” vor dem Entsperren des Keyguard-Bildschirms verfügbar sind. Sie können jedoch auch alle Keyguard-Funktionen deaktivieren.
- Keyguard-Verwaltung auf vollständig verwalteten Geräten mit Arbeitsprofil. Mit einer Richtlinie zur Keyguard-Verwaltung können Sie separate Einstellungen auf Gerät und Arbeitsprofil anwenden.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android Enterprise-Einstellungen



- **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil anwenden:** Ermöglicht das Konfigurieren von Richtlinieneinstellungen zur Keyguard-Verwaltung für vollständig verwaltete Geräte mit Arbeitsprofil.

  Bei der Einstellung **Ein** können Sie auf vollständig verwalteten Geräten mit Arbeitsprofil separate Einstellungen auf das Gerät und das Arbeitsprofil anwenden.

  Bei der Einstellung **Aus** können Sie Einstellungen auf Arbeitsprofilgeräte oder auf vollständig verwaltete Geräte anwenden. Einstellungen, die Sie für Arbeitsprofile konfigurieren, gelten nur für Arbeitsprofilgeräte. Einstellungen, die Sie für vollständig verwaltete Geräte konfigurieren,

gelten nur für vollständig verwaltete Geräte.

Die Standardeinstellung ist **Aus**.

- **Keyguard-Funktionen für Arbeitsprofil:** Steuert, ob die folgenden Funktionen vor dem Entsperren eines Arbeitsprofil-Keyguards (Sperrbildschirm) verfügbar sind.
  - **Trust Agents deaktivieren:** Bei Wahl von **Aus** können Trust Agents auf sicheren Keyguard-Displays agieren, wenn eine Sicherheitsabfrage im Arbeitsprofil festgelegt ist. Mit der Einstellung **Ein** werden alle Trust Agents im Arbeitsprofil deaktiviert. Die Standardeinstellung ist **Aus**.
  - **Biometrische Authentifizierung deaktivieren:** Ist diese Option auf **Aus** festgelegt, ist die biometrische Authentifizierung auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage im Arbeitsprofil festgelegt ist. Wählen Sie **Ein**, um die biometrische Authentifizierung für das Arbeitsprofil zu deaktivieren. Die Einstellung deaktiviert das Entsperren per Fingerabdruck, Gesichts- und Iriserkennung. Die Standardeinstellung ist **Aus**. Android 9.0 und höher.
  - **Entsperren per Fingerabdruck deaktivieren:** Mit **Ein** ist das Entsperren per Fingerabdruck auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage im Arbeitsprofil festgelegt ist. Mit **Aus** ist das Entsperren per Fingerabdruck im Arbeitsprofil aktiviert. Die Standardeinstellung ist **Aus**.
  - **Gesichtsauthentifizierung deaktivieren:** Ist diese Option auf **Aus** festgelegt, ist die Gesichtsauthentifizierung auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage im Arbeitsprofil festgelegt ist. Wählen Sie **Ein**, um die Gesichtsauthentifizierung für das Arbeitsprofil zu deaktivieren. Die Standardeinstellung ist **Aus**. Android 9.0 und höher.
  - **Irisauthentifizierung deaktivieren:** Ist diese Option auf **Aus** festgelegt, ist die Irisauthentifizierung auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage im Arbeitsprofil festgelegt ist. Wählen Sie **Ein**, um die Irisauthentifizierung für das Arbeitsprofil zu deaktivieren. Die Standardeinstellung ist **Aus**. Android 9.0 und höher.
  - **Unredigierte Benachrichtigungen deaktivieren:** Bei Wahl von **Aus** werden redigierte und unredigierte Benachrichtigungen auf sicheren Keyguard-Displays angezeigt. Bei Wahl von **Ein** werden unredigierte Benachrichtigungen deaktiviert und nur redigierte Benachrichtigungen angezeigt. Die Standardeinstellung ist **Aus**.
- **Keyguard-Funktionen eines vollständig verwalteten Geräts:** Steuert, ob die folgenden Funktionen verfügbar sind, bevor Benutzer den Geräte-Keyguard (Sperrbildschirm) entsperren. Diese Funktionen gelten für vollständig verwaltete oder dedizierte Geräte.
  - **Alle Keyguard-Funktionen deaktivieren:** Bei Wahl von **Aus** sind alle aktuellen und zukünftigen Keyguard-Anpassungen auf den sicheren Keyguard-Displays verfügbar. Bei der Einstellung **Ein** sind alle Keyguard-Anpassungen deaktiviert. Die Standardeinstellung ist **Aus**.

- **Trust Agents deaktivieren:** Mit **Aus** können Trust Agents auf sicheren Keyguard-Displays agieren. Bei der Einstellung **Ein** sind Trust Agents deaktiviert. Die Standardeinstellung ist **Aus**.
- **Biometrische Authentifizierung deaktivieren:** Ist diese Option auf **Aus** festgelegt, ist die biometrische Authentifizierung auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage für das Gerät festgelegt ist. Wählen Sie **Ein**, um die biometrische Authentifizierung für das Gerät zu deaktivieren. Die Einstellung deaktiviert das Entsperren per Fingerabdruck, Gesichts- und Iriserkennung. Die Standardeinstellung ist **Aus**. Android 9.0 und höher.
- **Entsperren per Fingerabdruck deaktivieren:** Mit **Aus** ist das Entsperren per Fingerabdruck auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage für das Gerät festgelegt ist. Mit **Ein** ist das Entsperren per Fingerabdruck für das Gerät deaktiviert. Die Standardeinstellung ist **Aus**.
- **Gesichtsauthentifizierung deaktivieren:** Ist diese Option auf **Aus** festgelegt, ist die Gesichtsauthentifizierung auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage für das Gerät festgelegt ist. Wählen Sie **Ein**, um die Gesichtsauthentifizierung für das Gerät zu deaktivieren. Die Standardeinstellung ist **Aus**. Android 9.0 und höher.
- **Irisauthentifizierung deaktivieren:** Ist diese Option auf **Aus** festgelegt, ist die Irisauthentifizierung auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage für das Gerät festgelegt ist. Wählen Sie **Ein**, um die Irisauthentifizierung für das Gerät zu deaktivieren. Die Standardeinstellung ist **Aus**. Android 9.0 und höher.
- **Alle Benachrichtigungen deaktivieren:** Bei Wahl von **Aus** werden alle Benachrichtigungen auf sicheren Keyguard-Displays angezeigt. Bei der Einstellung **Ein** werden alle Benachrichtigungen angezeigt. Die Standardeinstellung ist **Aus**.
- **Unredigierte Benachrichtigungen deaktivieren:** Bei Wahl von **Aus** werden redigierte und unredigierte Benachrichtigungen auf sicheren Keyguard-Displays angezeigt. Bei Wahl von **Ein** werden unredigierte Benachrichtigungen deaktiviert und nur redigierte Benachrichtigungen angezeigt. Die Standardeinstellung ist **Aus**.
- **Sichere Kamera deaktivieren:** Bei Wahl von **Aus** ist die sichere Kamera auf sicheren Keyguard-Displays verfügbar. Bei der Einstellung **Ein** ist die sichere Kamera deaktiviert. Die Standardeinstellung ist **Aus**.

Kioskgeräterichtlinie

January 6, 2022

Mit der Kioskrichtlinie können Sie Geräte auf den Kioskmodus und ausführbare Apps beschränken. XenMobile steuert nicht, welcher Teil des Geräts im Kioskmodus gesperrt wird. Das Gerät verwaltet die Einstellungen des Kioskmodus, nachdem Sie die Richtlinie bereitgestellt haben.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

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 Firebase Cloud Messaging für Android-Geräte, wie in Firebase Cloud Messaging beschrieben. Dadurch können Android-Geräte eine Verbindung mit XenMobile herstellen.
3. Fügen Sie wie nachfolgend beschrieben eine Kioskrichtlinie hinzu.
4. Weisen Sie die drei Geräterichtlinien den entsprechenden Bereitstellungsgruppen zu. Überlegen Sie, ob Sie diesen Bereitstellungsgruppen weitere Richtlinien, z. B. eine App-Bestandsrichtlinie, hinzufügen möchten.

   Zum Deaktivieren des Kioskmodus für Geräte erstellen Sie eine 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 Kioskgeräterichtlinie

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.

Samsung SAFE-Einstellungen

Sie können festlegen, dass nur bestimmte Apps 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.

- **Kioskmodus:** Klicken Sie auf **Aktivieren** oder **Deaktivieren**. Die Standardeinstellung 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 jeder sich an Ihr Unternehmen wenden, um ein verlorenes Gerät zu finden. Gilt nur für MDM 4.0 und höher.
- **Navigationsleiste zulassen:** Wählen Sie aus, ob Benutzer im Kioskmodus die Navigationsleiste anzeigen und verwenden können sollen. Gilt nur für MDM 4.0 und höher. Die Standardeinstellung ist **Ein**.
- **Mehrfenstermodus zulassen:** Wählen Sie aus, ob Benutzer im Kioskmodus mehrere Fenster verwenden können sollen. Gilt nur für MDM 4.0 und höher. Die Standardeinstellung ist **Ein**.
- **Statusleiste zulassen:** Wählen Sie aus, ob Benutzer im Kioskmodus die Statusleiste anzeigen können sollen. Gilt nur für MDM 4.0 und höher. Die Standardeinstellung ist **Ein**.
- **Systemleiste zulassen:** Wählen Sie aus, ob Benutzer im Kioskmodus die Systemleiste anzeigen können sollen. Die Standardeinstellung ist **Ein**.
- **Task-Manager zulassen:** Wählen Sie aus, ob Benutzer im Kioskmodus den Task-Manager anzeigen und verwenden können sollen. Die Standardeinstellung ist **Ein**.
- **Allgemeinen SAFE-Passcode ändern:** Diese Einstellung trägt dazu bei, ungewollte Änderungen des allgemeinen SAFE-Passcodes zu verhindern. Bei Auswahl von **Aus** können Sie den allgemeinen SAFE-Passcode nicht ändern. Die Standardeinstellung ist **Aus**.
- **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. Die Standardeinstellung 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. Die Standardeinstellung 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.

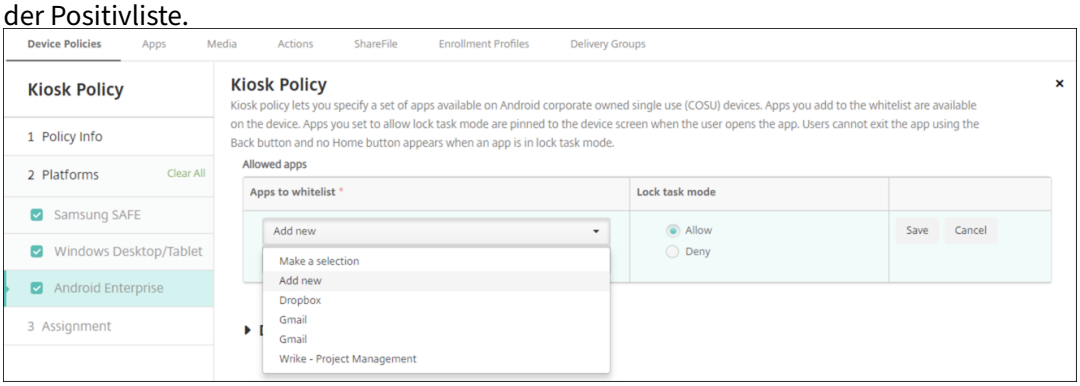
Android Enterprise-Einstellungen

Sie können für dedizierte Android Enterprise-Geräte, auch COSU-Geräte genannt (Corporate Owned Single Use), Apps auf eine Positivliste setzen und den LockTask-Modus festlegen. Secure Hub- und Google Play-Dienste stehen standardmäßig auf der Positivliste.

Um eine App zuzulassen, klicken Sie auf **Hinzufügen**. Sie können mehrere Apps zulassen. Weitere Informationen finden Sie unter Android Enterprise.

> **Hinweis:**
>
> Die XenMobile Server-Konsole enthält im Englischen die Begriffe “Blacklist” und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

- **Apps auf Positivliste:** Wählen Sie die gewünschte App aus der Liste aus oder geben Sie den Paketnamen der App ein.
  - Klicken Sie auf **Hinzufügen**, um den Paketnamen der App einzugeben, die in der Liste angezeigt werden soll.
  - Wählen Sie die App aus der Liste aus. Die Liste enthält Apps, die in XenMobile Server hochgeladen wurden. Secure Hub- und Google Play-Dienste stehen standardmäßig auf der Positivliste.



- **LockTask-Modus:** Wählen Sie **Zulassen**, um festzulegen, dass die App an den Gerätebildschirm angeheftet wird, wenn der Benutzer die App startet. Wählen Sie **Verweigern**, um festzulegen, dass die App nicht angeheftet werden soll. Secure Hub- und Google Play-Dienste sind standardmäßig zugelassen. Die Standardeinstellung ist **Zulassen**.

Im gesperrten Task-Modus wird eine App an den Gerätebildschirm angeheftet, wenn der Benutzer sie öffnet. Es gibt keine Hometaste, und die Zurück-Taste ist deaktiviert. Der Benutzer beendet die App mit einer in der App programmierten Aktion, z. B. Abmelden.

Launcher-Konfigurationsrichtlinie

September 24, 2021

Mit Citrix Launcher können Sie die Benutzererfahrung für über XenMobile bereitgestellte Android-Geräte anpassen. Citrix Launcher und die Launcher-Konfigurationsrichtlinie sind nicht mit Android Enterprise kompatibel.

Mit einer Launcher-Konfigurationsrichtlinie können Sie folgende Citrix Launcher-Features steuern:

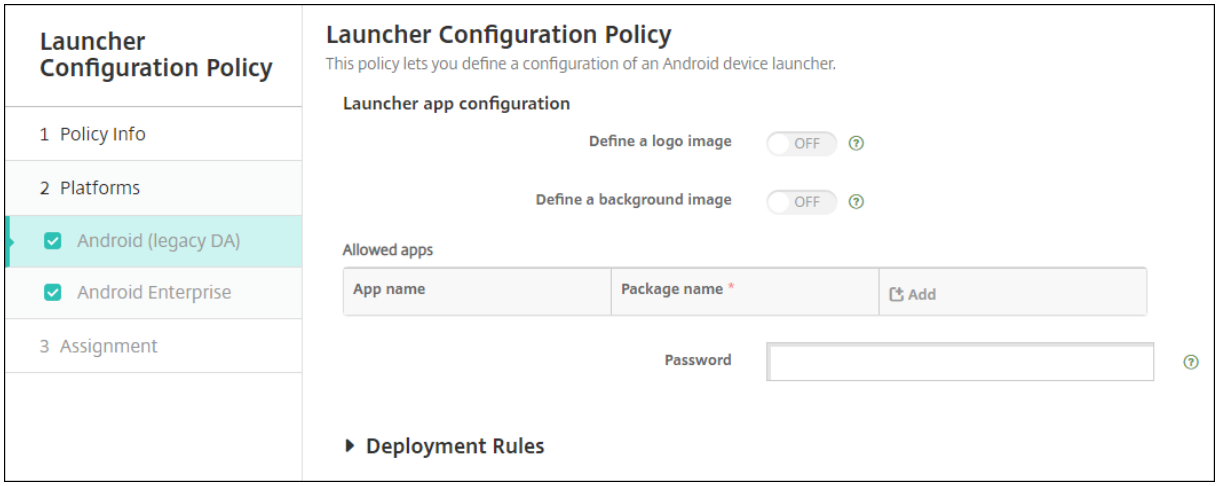
- Verwalten von Android-Geräten, sodass Benutzer nur auf von Ihnen festgelegte Apps Zugriff haben
- Optionale Angabe eines benutzerdefinierten Logos als Citrix Launcher-Symbol sowie eines benutzerdefinierten Hintergrundbilds für Citrix Launcher
- Festlegen eines Kennworts, das die Benutzer zum Beenden 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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Einstellungen für Android (Legacy-Geräteadmin) und Android Enterprise



- **Logobild definieren:** Wählen Sie aus, ob ein benutzerdefiniertes Logobild als Citrix Launcher-Symbol verwendet werden soll. Die Standardeinstellung ist **Aus**.
- **Logobild:** Wenn Sie **Logobild** definieren aktivieren, klicken Sie auf **Durchsuchen,** navigieren Sie zu der Datei mit dem gewünschten Bild und wählen Sie sie 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. Die Standardeinstellung 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.
- **Zulässige 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.
- **Kennwort:** Kennwort, das die Benutzer zum Beenden von Citrix Launcher eingeben müssen.

LDAP-Geräterichtlinie

January 5, 2022

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Kontobeschreibung:** Geben Sie eine optionale Kontobeschreibung ein.
- **Kontobenutzername:** Geben Sie optional einen Benutzernamen ein.
- **Kontokennwort:** Geben Sie ein optionales Kennwort ein. Verwenden Sie dieses Feld nur bei verschlüsselten Profilen.
- **LDAP-Hostname:** Geben Sie den Hostnamen des LDAP-Servers ein. Diese Angabe ist erforderlich.
- **SSL verwenden:** Wählen Sie aus, ob für die Verbindung mit dem LDAP-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **Ein**.
- **Sucheinstellungen:** Fügen Sie die Sucheinstellungen für Abfragen beim LDAP-Server hinzu. Sie können beliebig viele Sucheinstellungen eingeben, es ist jedoch mindestens eine erforderlich, damit das Konto einen Nutzen hat. Klicken Sie auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **Beschreibung:** Geben Sie eine Beschreibung der Sucheinstellung ein. Diese Angabe ist erforderlich.

  - **Bereich:** Wählen Sie **Basis**, **Eine Ebene** oder **Unterstruktur**, um die Suchtiefe 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.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-Einstellungen

- **Kontobeschreibung:** Geben Sie eine optionale Kontobeschreibung ein.
- **Kontobenutzername:** Geben Sie optional einen Benutzernamen ein.
- **Kontokennwort:** Geben Sie ein optionales Kennwort ein. Verwenden Sie dieses Feld nur bei verschlüsselten Profilen.
- **LDAP-Hostname:** Geben Sie den Hostnamen des LDAP-Servers ein. Diese Angabe ist erforderlich.
- **SSL verwenden:** Wählen Sie aus, ob für die Verbindung mit dem LDAP-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **Ein**.
- **Sucheinstellungen:** Fügen Sie die Sucheinstellungen für Abfragen beim LDAP-Server hinzu. Sie können beliebig viele Sucheinstellungen eingeben, es ist jedoch mindestens eine erforderlich, damit das Konto einen Nutzen hat. Klicken Sie auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **Beschreibung:** Geben Sie eine Beschreibung der Sucheinstellung ein. Diese Angabe ist erforderlich.
  - **Bereich:** Wählen Sie **Basis**, **Eine Ebene** oder **Unterstruktur**, um die Suchtiefe 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.
- **Richtlinieneinstellungen**
    - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
        * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
        * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
    - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
    - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

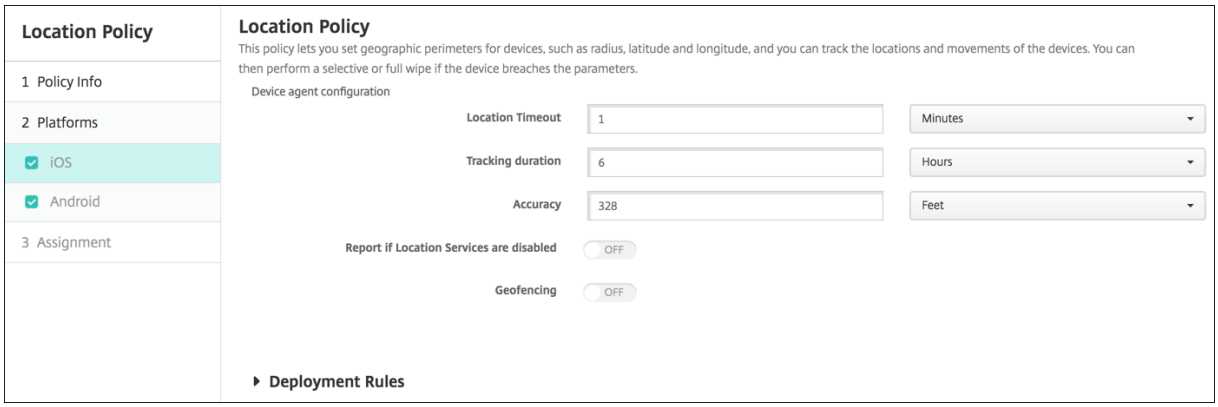
Standortrichtlinie für Geräte

January 5, 2022

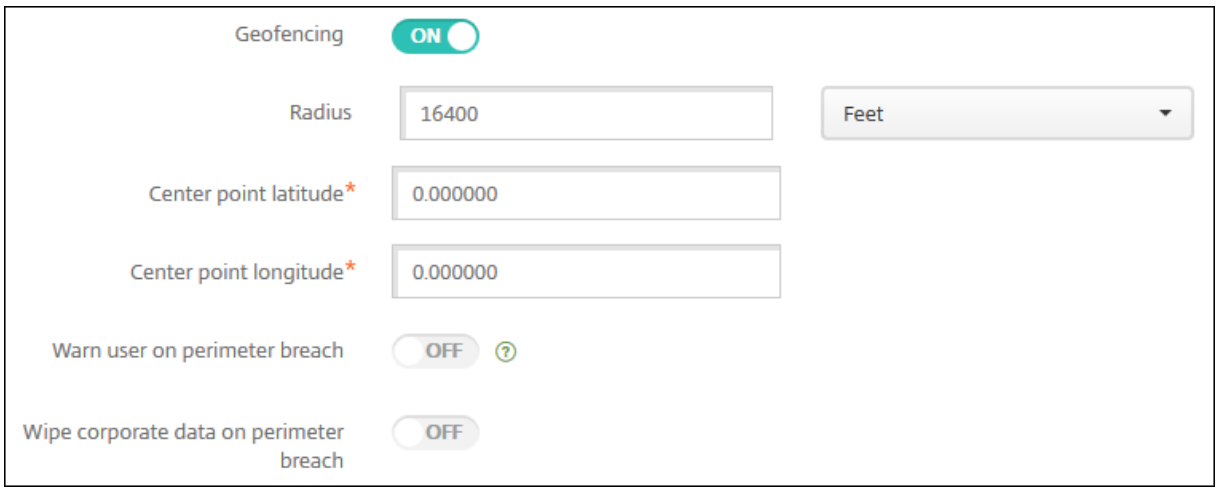
Mit einer Standortrichtlinie legen Sie in XenMobile geografische Grenzen fest. Wenn ein Benutzer den durch die Grenze (*Geofence*) festgelegten Bereich verlässt, kann XenMobile bestimmte Aktionen ausführen. Beispielsweise können Sie festlegen, dass Benutzer bei Verletzung des definierten Umkreises eine Warnmeldung erhalten. Sie können die Richtlinie auch so konfigurieren, dass Unternehmensdaten bei einer Umkreisverletzung sofort oder mit einer gewissen Verzögerung gelöscht werden. Informationen zu Sicherheitsmaßnahmen wie Tracking oder Ortung eines Geräts finden Sie unter Sicherheitsaktionen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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. Die Standardeinstellung ist **Aus**.
- **Geofencing**

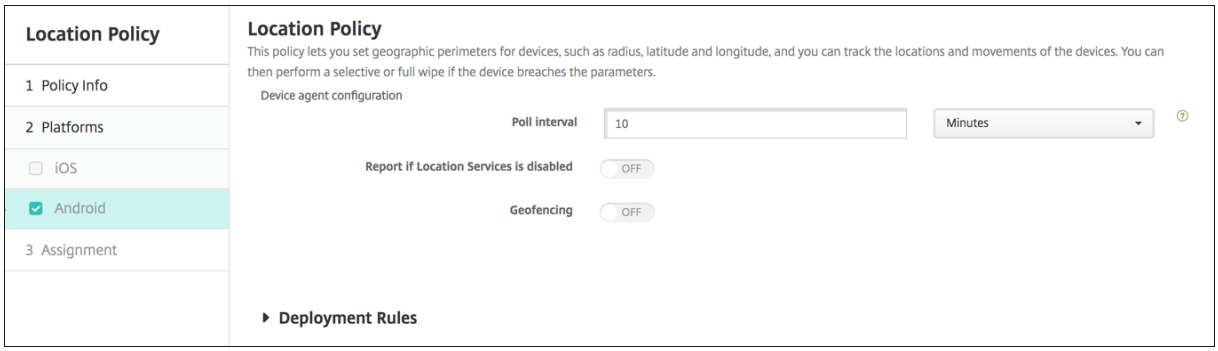


Bei Auswahl von Geofencing konfigurieren Sie die folgenden Einstellungen:

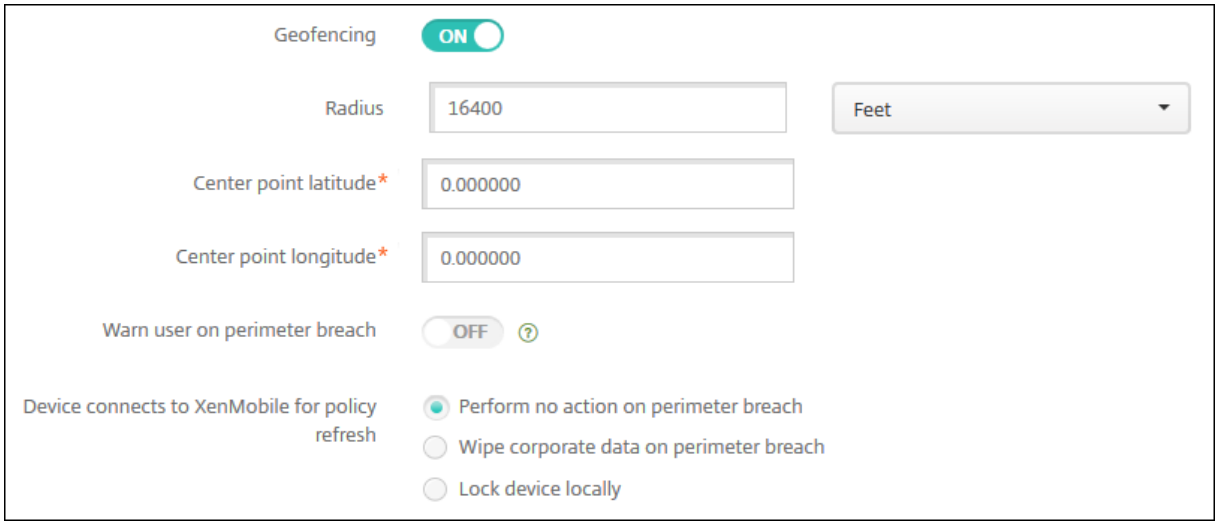
- **Radius:** Geben Sie zur Messung des Radius eine Ziffer ein und klicken Sie dann in der Liste auf die zu verwendenden Einheiten. Der Standardwert ist 16.400 Fuß. Gültige Werte für den Radius:
  - 164-164000 Fuß

  - 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. Die Standardeinstellung 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. Die Standardeinstellung 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. Diese Einstellung gibt Benutzern die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor XenMobile eine selektive Datenlöschung auf ihrem Gerät durchführt. Die Standardeinstellung ist 0 Sekunden.

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. Die Standardeinstellung 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. Die Standardeinstellung ist **Aus**.
- **Geofencing**



Bei Auswahl von Geofencing konfigurieren Sie die folgenden Einstellungen:

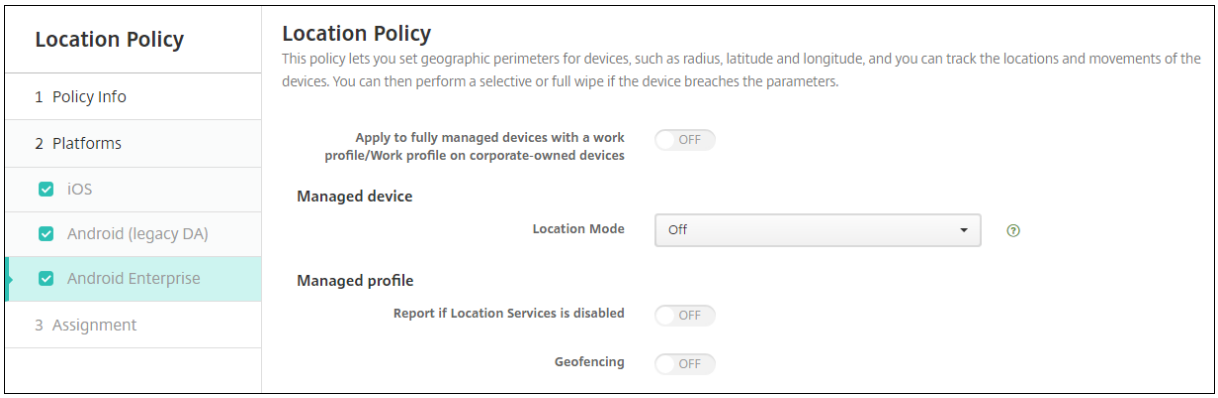
- **Radius:** Geben Sie zur Messung des Radius eine Ziffer ein und klicken Sie dann in der Liste auf die zu verwendenden Einheiten. Der Standardwert ist 16.400 Fuß. Gültige Werte für den Radius:
  - 164-164000 Fuß
  - 1-50 Kilometer
  - 50-50000 Meter
  - 54-54680 Yard
  - 1-31 Meilen
- **Breitengrad 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. Die Standardeinstellung ist **Aus**. Zum Anzeigen der Warnmeldung ist keine Verbindung mit XenMobile erforderlich.
- **Gerät mit XenMobile zur Richtlinienaktualisierung verbinden:** Wählen Sie eine der folgenden Optionen aus, die durchgeführt werden soll, wenn Benutzer den Bereich verlassen:
  - **Bei Umkreisverletzung keine Aktion durchführen:** Nichts tun. 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. Diese Einstellung gibt Benutzern die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor XenMobile eine selektive Datenlöschung auf ihrem Gerät durchführt. Die Standardeinstellung 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. Diese Einstellung gibt Benutzern die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor XenMobile ihr Gerät sperrt. Die Standardeinstellung ist 0 Sekunden.

Android Enterprise-Einstellungen

Damit die Android-Standortverfolgung funktioniert, müssen die folgenden Anforderungen erfüllt sein:

- Android 8.5 oder höher
- Einstellung "Standortfreigabe zulassen" in der Beschränkungsrichtlinie für Android Enterprise aktiviert
- Verbindungszeitplan (Firebase Cloud Messaging empfohlen)



Auf vollständig verwaltete Geräte mit einem Arbeitsprofil anwenden

Für vollständig verwaltete Geräte mit Arbeitsprofil ist nur die Einstellung "Standortmodus" verfügbar.

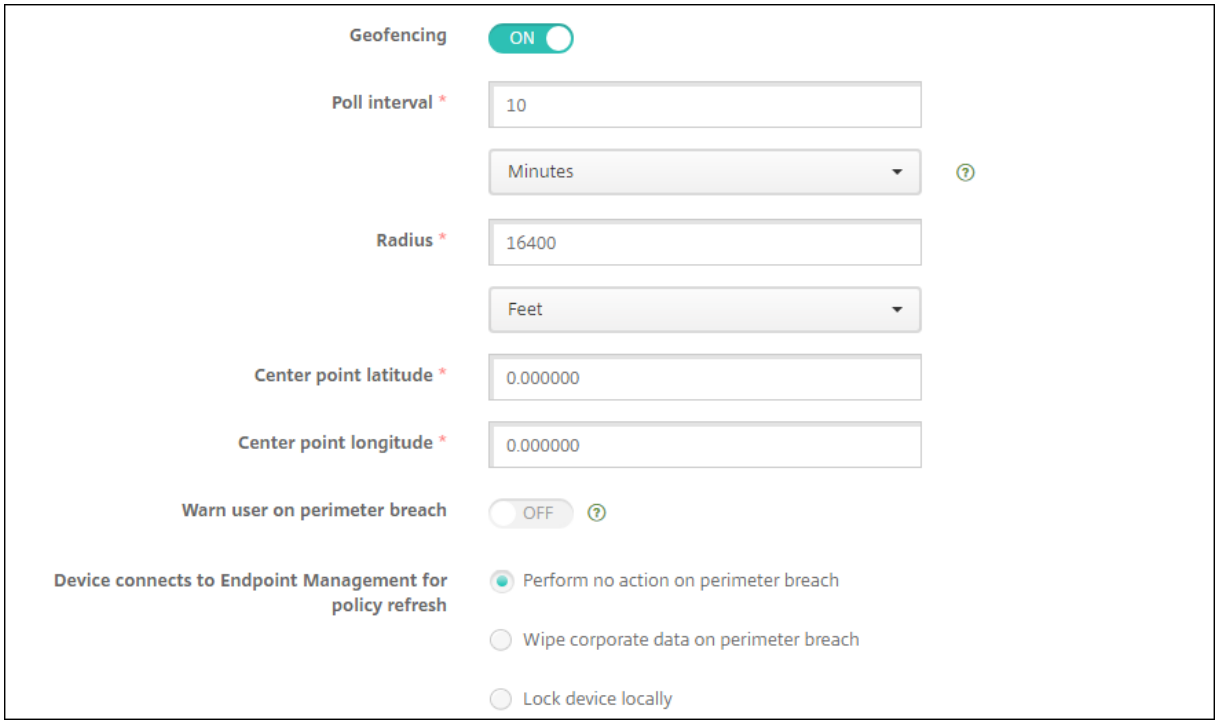
- **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil bzw. Arbeitsprofil auf unternehmenseigenen Geräten anwenden:** Ermöglicht das Konfigurieren des Standortmodus für vollständig verwaltete Geräte mit Arbeitsprofil. Bei der Einstellung "Ein" konfigurieren Sie die Einstellungen für den Standortmodus für das Arbeitsprofil:
  - **Deaktivierte Ortungsdienste melden:** Wählen Sie, ob das Gerät einen Bericht an XenMobile Server senden soll, wenn der Benutzer das GPS deaktiviert. Die Standardeinstellung ist **Aus**.
  - **Geofencing:** Siehe Einstellungen unter Verwaltetes Gerät.

Wenn **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil bzw. Arbeitsprofil auf unternehmenseigenen Geräten anwenden** deaktiviert ist, gelten die Einstellungen für das verwaltete

Gerät und das Arbeitsprofil, wie in den folgenden Abschnitten dargestellt. Die Standardeinstellung ist **Aus**.

Verwaltetes Gerät

- **Standortmodus:** Geben Sie den Grad der Standorterkennung an, der aktiviert werden soll. Sie können die Sicherheitsaktion zur Ortung nur verwenden, wenn der Standortmodus auf Hohe Genauigkeit oder Akku schonen festgelegt ist. Die Standardeinstellung ist Hohe Genauigkeit.
  - **Hohe Genauigkeit:** Ermöglicht alle Ortungsmethoden, einschließlich GPS, Netzwerke und andere Sensoren.
  - **Nur Sensoren:** Ermöglicht nur GPS und andere Sensoren.
  - **Akku schonen:** Aktiviert nur den Netzwerkanbieter.
  - **Aus:** Deaktiviert die Standorterkennung.
- **Geofencing:**



Bei Auswahl von **Geofencing** konfigurieren Sie die folgenden Einstellungen:

- **Abrufintervall:** Geben Sie eine Ziffer ein und klicken Sie auf **Minuten**, **Stunden** oder **Tage**, um festzulegen, wie häufig XenMobile Server den Gerätestandort abrufen soll. Gültige Werte sind 1-1440 Minuten, 1-24 Stunden oder eine beliebige Anzahl an Tagen. Die Standardeinstellung ist **10** Minuten. Wenn dieser Wert auf weniger als 10 Minuten festgelegt wird, kann dies die Akkulaufzeit des Geräts nachteilig beeinflussen.
- **Radius:** Geben Sie zur Messung des Radius eine Ziffer ein und klicken Sie auf die zu verwendenden Einheiten. Die Standardeinstellung ist **5000 Meter** (**16400 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. Wählen Sie zum Prüfen des Werts unter **Verwalten > Geräte** das Gerät und klicken Sie auf **Sicher** gefolgt von **Orten**. Nach dem Suchen des Geräts meldet XenMobile Server dessen Standort auf der Seite **Gerätedetails > Allgemein** unter **Sicherheit**.
- **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. Die Standardeinstellung ist **Aus**. Zum Anzeigen der Warnmeldung ist keine Verbindung mit XenMobile Server erforderlich.
- **Gerät mit XenMobile Server zur Richtlinienaktualisierung verbinden:** Wählen Sie eine der folgenden Optionen aus, die durchgeführt werden soll, wenn Benutzer den Bereich verlassen:
  - **Bei Umkreisverletzung keine Aktion durchführen:** Nichts tun. 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 auf **Sekunden** oder **Minuten**, um die Dauer der Verzögerung bis zum Löschen der Unternehmensdaten von den Geräten festzulegen. Durch die Verzögerung haben Benutzer die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor XenMobile Server eine selektive Datenlöschung auf ihrem Gerät durchführt. Die Standardeinstellung ist **0 Sekunden**.
  - **Gerät lokal sperren:** Sperren Sie die Geräte der Benutzer nach einer bestimmten Zeit. Wenn Sie diese Option aktivieren, wird das Feld **Verzögerung beim Sperren** angezeigt.
    - Geben Sie eine Ziffer ein und klicken Sie auf **Sekunden** oder **Minuten**, um die Dauer der Verzögerung bis zum Sperren der Geräte festzulegen. Durch die Verzögerung haben Benutzer die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor XenMobile Server ihr Gerät sperrt. Die Standardeinstellung ist **0 Sekunden**.

Verwaltetes Profil

- **Deaktivierte Ortungsdienste melden:** Wählen Sie, ob das Gerät einen Bericht an XenMobile Server senden soll, wenn der Benutzer das GPS deaktiviert. Die Standardeinstellung ist **Aus**.
- **Geofencing:** Siehe Einstellungen unter Verwaltetes Gerät.

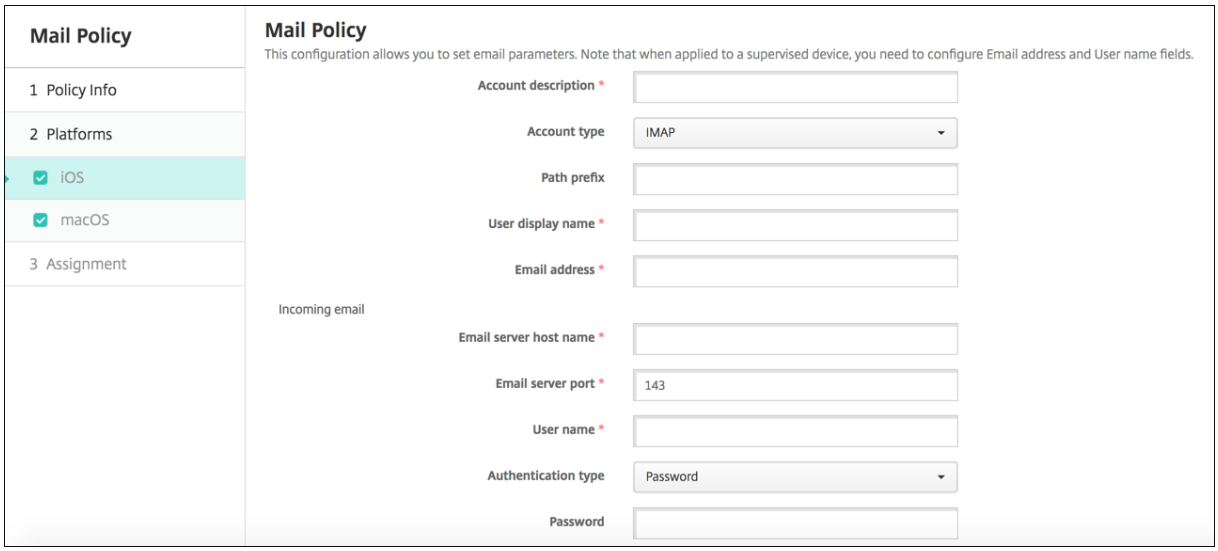
E-Mail-Geräterichtlinie

January 5, 2022

Sie können in XenMobile eine E-Mail-Richtlinie hinzufügen, um ein E-Mail-Konto auf iOS- oder macOS-Geräten zu konfigurieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS- und macOS-Einstellungen



- **Kontobeschreibung:** Geben Sie eine Kontobeschreibung zur Anzeige in den E-Mail- und Einstellungs-Apps ein. Diese Angabe ist erforderlich.
- **Kontotyp:** Wählen Sie **IMAP** oder **POP** als Protokoll für die Konten. Die Standardeinstellung ist **IMAP**. Wenn Sie **POP** auswählen, wird die im nächsten Schritt erwähnte Option **Pfadpräfix** ausgeblendet.
- **Pfadpräfix:** Geben Sie **INBOX** oder das Präfix des IMAP-E-Mail-Kontopfads ein. 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-Mails ein. Diese Angabe ist erforderlich.
  - **Port des E-Mail-Servers:** Geben Sie die Portnummer des Servers für eingehende E-Mails ein. Die Standardeinstellung 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 bis zum @-Zeichen. Diese Angabe ist erforderlich.
  - **Authentifizierungstyp:** Wählen Sie 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-Mails ein.
  - **SSL verwenden:** Wählen Sie aus, ob der Server für eingehende E-Mails Secure Socket Layer verwenden soll. Die Standardeinstellung 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-Mails ein. Diese Angabe ist erforderlich.
  - **Port des E-Mail-Servers:** Geben Sie die Portnummer des Servers für ausgehende E-Mails ein. Wenn Sie keinen Port angeben, wird der Standardport des angegebenen Protokolls verwendet.
  - **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 bis zum @-Zeichen. Diese Angabe ist erforderlich.
  - **Authentifizierungstyp:** Wählen Sie die Authentifizierungsmethode, die Sie verwenden möchten. Der Standardwert ist **Kennwort**.
  - **Kennwort:** Geben Sie ein optionales Kennwort für den Server für ausgehende E-Mails ein.
  - **Ausgehendes Kennwort gleich eingehendem:** Wählen Sie aus, ob für aus- und eingehende E-Mails dasselbe Kennwort verwendet wird. Der Standardwert ist **Aus**, was bedeutet, dass die Kennwörter unterschiedlich sind.
  - **SSL verwenden:** Wählen Sie aus, ob der Server für ausgehende E-Mail Secure Socket Layer verwenden soll. Die Standardeinstellung ist **Aus**.
- **Richtlinie**
  - **Verschieben von E-Mails zwischen Konten autorisieren:** Geben Sie vor, ob Benutzer E-Mails 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. Die Standardeinstellung ist **Aus**.
  - **E-Mail nur von Mailanwendung senden:** Wählen Sie aus, ob Benutzer E-Mails 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. Die Standardeinstellung ist **Aus**. Diese Option gilt nur für iOS 6.0 und höher.
- **Mail Drop zulassen:** Wählen Sie aus, ob Apple Mail Drop für Geräte mit iOS 9.2 und höher zulässig sein soll. Die Standardeinstellung ist **Aus**.
- **S/MIME-Signatur aktivieren:** Wählen Sie, ob dieses Konto S/MIME-Signaturen unterstützt. Die Standardeinstellung ist **Ein**. Wenn Sie **Ein** wählen, werden folgende Felder eingeblendet.
  - **Anmeldeinformationen für Signieridentität:** Wählen Sie die Anmeldeinformationen für die Signatur aus.
  - **S/MIME-Signatur von Benutzer überschreibbar:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Signierung in Einstellungen des Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
  - **UUID für S/MIME-Signaturzertifikat von Benutzer überschreibbar:** Mit **Ein** können Benutzer in den Einstellungen ihrer Geräte wählen, welche Anmeldeinformationen für die Signatur verwendet werden. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
- **S/MIME-Verschlüsselung aktivieren:** Wählen Sie, ob dieses Konto S/MIME-Verschlüsselung unterstützt. Die Standardeinstellung ist **Aus**. Wenn Sie **Ein** wählen, werden folgende Felder eingeblendet.
  - **Anmeldeinformationen für Verschlüsselungsidentität:** Wählen Sie die Anmeldeinformationen für die Verschlüsselung aus.
  - **S/MIME-Option für einzelne Nachrichten aktivieren:** Mit **Ein** wird Benutzern für jede Nachricht, die sie erstellen, eine Option zum Aktivieren oder Deaktivieren der S/MIME-Verschlüsselung angezeigt. Die Standardeinstellung ist **Aus**.
  - **Standardmäßige S/MIME-Verschlüsselung von Benutzer überschreibbar:** Mit **Ein** können Benutzer in den Einstellungen ihrer Geräte auswählen, ob S/MIME standardmäßig aktiviert ist. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
  - **UUID für S/MIME-Verschlüsselungszertifikat von Benutzer überschreibbar:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Verschlüsselungsidentität und Verschlüsselung in den Einstellungen des Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.

- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Mit den Optionen **Datum auswählen** oder **Zeit bis zum Entfernen (in Stunden)** können Sie festlegen, dass die Richtlinie zu einem späteren Zeitpunkt entfernt wird.

- **Benutzer darf Richtlinie entfernen:** Mit den Optionen **Immer**, **Passcode erforderlich** oder **Nie** können Sie festlegen, ob und wie Benutzer die Richtlinie entfernen können.
- **Profilbereich:** Wählen Sie aus, ob die Richtlinie pro **Benutzer** oder für das gesamte **System** angewendet wird (nur für macOS).

Geräterichtlinie für verwaltete Domänen

January 5, 2022

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.

Für betreute Geräte mit iOS 8 und höher geben Sie durch Angabe von URLs oder Unterdomänen vor, wie Benutzer Dokumente, Anlagen und über Browser heruntergeladene Objekte öffnen können. Für betreute Geräte mit iOS 9.3 und höher können Sie die URLs angeben, über die Benutzer Kennwörter in Safari speichern können.

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.

Für Elemente wie Dokumente, Anlagen oder heruntergeladene Objekte: Versucht ein Benutzer ein Element über Safari von einer Domäne 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.

Für betreute Geräte, auch wenn Sie keine Safari-Domänen mit automatisch ausgefülltem Kennwort angeben: Wenn das Gerät für mehrere kurzzeitige Benutzer konfiguriert ist, können die Benutzer keine Kennwörter speichern. Wenn das Gerät nicht für mehrere kurzzeitige Benutzer konfiguriert ist, können die Benutzer alle Kennwörter speichern.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

Angeben von Domänen:

Format	Beschreibung
`example.com`	Jeder Pfad unter `example.com` wird als verwaltet behandelt, nicht aber `site.example.com/`.
`foo.example.com`	Jeder Pfad unter `foo.example.com` wird als verwaltet behandelt, nicht aber `example.com/` und `bar.example.com/`.
`\*.example.com`	Jeder Pfad unter `foo.example.com` oder `bar.example.com` wird als verwaltet behandelt, nicht aber `example.com/`.
`example.com/sub`	`example.com/sub` und jeder Pfad darunter wird als verwaltet behandelt, nicht aber `example.com/`.
`foo.example.com/sub`	Jeder Pfad unter `foo.example.com/sub` wird als verwaltet behandelt, nicht aber `example.com`, `example.com/sub`, `foo.example.com/` und `bar.example.com/sub`.
`\*.example.com/sub`	Jeder Pfad unter `foo.example.com/sub` und `bar.example.com/sub` wird als verwaltet behandelt, nicht aber `example.com` und `foo.example.com/`.

Regeln:

- Das einleitende “www” und nachstehende Schrägstriche bei URLs werden beim Domänenvergleich ignoriert.
- Wenn ein Eintrag eine Portnummer enthält, werden nur Adressen mit dieser Portnummer als verwaltet behandelt. Andernfalls werden nur die Standardports als verwaltet behandelt (Port 80 für HTTP und 443 für HTTPS). Beispielsweise entspricht Muster `*.example.com:8080` `https://site.example.com:8080/page.html` aber nicht `https://site.example.com/page.html`, während Muster `*.example.com` `https://site.example.com/page.html` und `https://site.example.com/page.html` aber nicht `https://site.example.com:8080/page.html` entspricht.
- Definitionen verwalteter Safari-Webdomänen sind kumulativ. Beim Abgleich einer URL-Anforderung werden von allen verwalteten Safari-Webdomänen-Nutzlasten definierte Muster verwendet.

Einstellungen:

- **Verwaltete Domänen**
  - **Nicht markierte E-Mail-Domänen:** Klicken Sie 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 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.
  - **Safari-Domänen mit autom. Ausfüllen von Kennwörtern:** Klicken Sie für jede Domäne mit automatischem Ausfüllen, die Sie der Liste hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
    * **Safari-Domäne mit autom. Ausfüllen von Kennwörtern:** Geben Sie die Domäne zum automatischen Ausfüllen ein.
    * Klicken Sie auf **Speichern**, um die Domäne zum automatischen Ausfüllen zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

MDM-Optionsrichtlinien für Geräte

January 5, 2022

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 eines iOS-Geräts mit dem Apple Configurator in den betreuten Modus.

Die Aktivierungssperre ist ein Feature von "Mein iPhone/iPad suchen", mit dem das Reaktivieren von verlorenen oder gestohlenen betreuten Geräten verhindert wird. Die Aktivierungssperre erfordert die

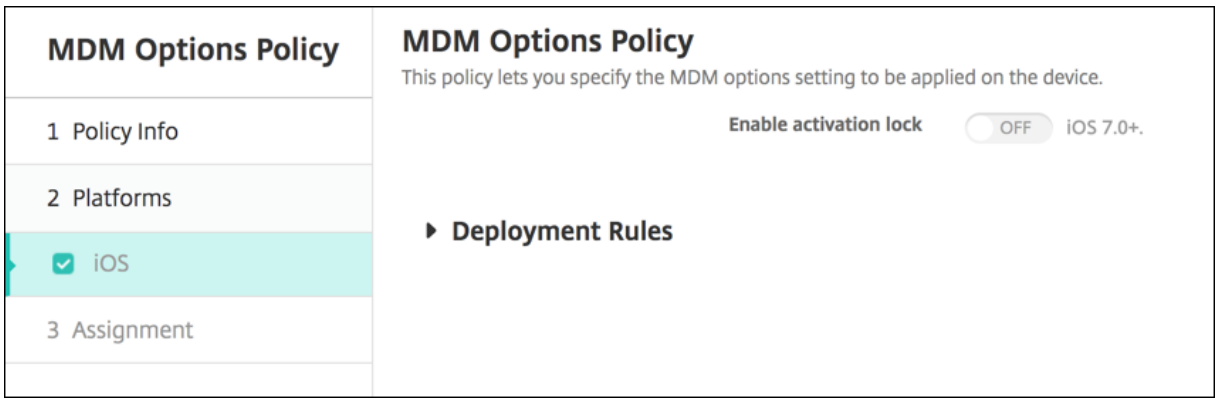
Eingabe der Apple-ID und des Benutzerkennworts, bevor ein beliebiger Benutzer “Mein iPhone/iPad suchen” deaktivieren, die Daten auf dem Gerät löschen oder das Gerät neu aktivieren kann. Für Geräte im Besitz Ihres Unternehmens kann ein Umgehen der Aktivierungssperre erforderlich sein, um Geräte zurückzusetzen oder neu zuzuweisen.

Zum Einrichten der Aktivierungssperre müssen Sie die XenMobile-Geräterichtlinie “MDM-Optionen” konfigurieren und bereitstellen. Dann können Sie ein Gerät über die XenMobile-Konsole ohne Eingabe der Apple-Anmeldeinformationen des Benutzers verwalten. Aktivieren Sie auf der XenMobile-Konsole die Sicherheitsaktion “Aktivierungssperre umgehen”, um trotz Aktivierungssperre keine Apple-Anmeldeinformationen eingeben zu müssen.

Nehmen wir folgendes Beispiel: Ein Benutzer bringt ein verlorenes Telefon zurück oder möchte ein Gerät vor oder nach einem vollständigen Löschen einrichten. Die dabei geforderte Eingabe der Anmeldeinformationen für das iTunes-Konto können Sie umgehen, indem Sie in der XenMobile-Konsole die Sicherheitsaktion “Aktivierungssperre umgehen” aktivieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



- **Aktivierungssperre aktivieren:** Wählen Sie aus, ob die Aktivierungssperre auf den Geräten aktiviert werden soll, auf denen Sie die Richtlinie bereitstellen. Die Standardeinstellung ist **Aus**.

Nach dem Aktivieren der Aktivierungssperre durch Bereitstellen der Richtlinie “MDM-Optionen”: Die Sicherheitsaktion **Aktivierungssperre umgehen** wird angezeigt, wenn Sie diese Geräte auf der Seite **Verwalten > Geräte** auswählen und auf **Sicherheit** klicken. Durch das Umgehen der Aktivierungssperre können Sie die Aktivierungssperre von betreuten Geräten vor der Aktivierung des Geräts entfernen, ohne die Apple-ID und das Benutzerkennwort zu kennen. Sie können den Befehl zum Umgehen einer Aktivierungssperre vor oder nach einem vollständigen Löschen aller Inhalte an ein Gerät senden. Weitere Informationen finden Sie im Artikel “Sicherheitsaktionen” unter Umgehen einer iOS-Aktivierungssperre.

Geräterichtlinie für Unternehmensinformationen

October 25, 2018

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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.

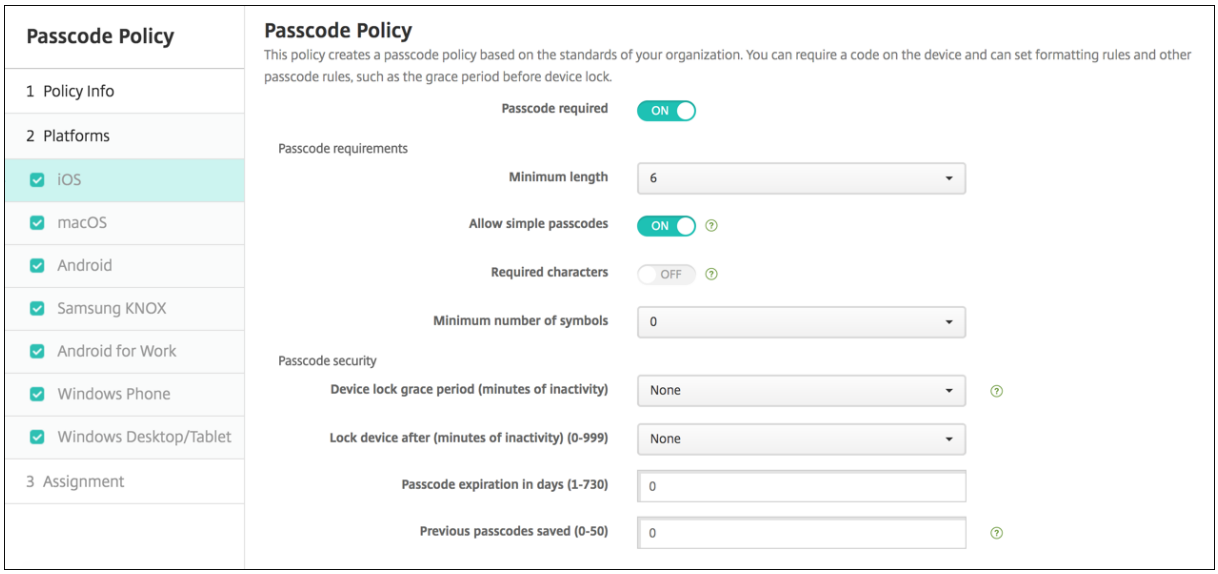
Passcode-Geräterichtlinie

January 5, 2022

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, macOS, Android, Android Enterprise, Samsung KNOX, Windows Phone und Windows Desktop/Tablet erstellen. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

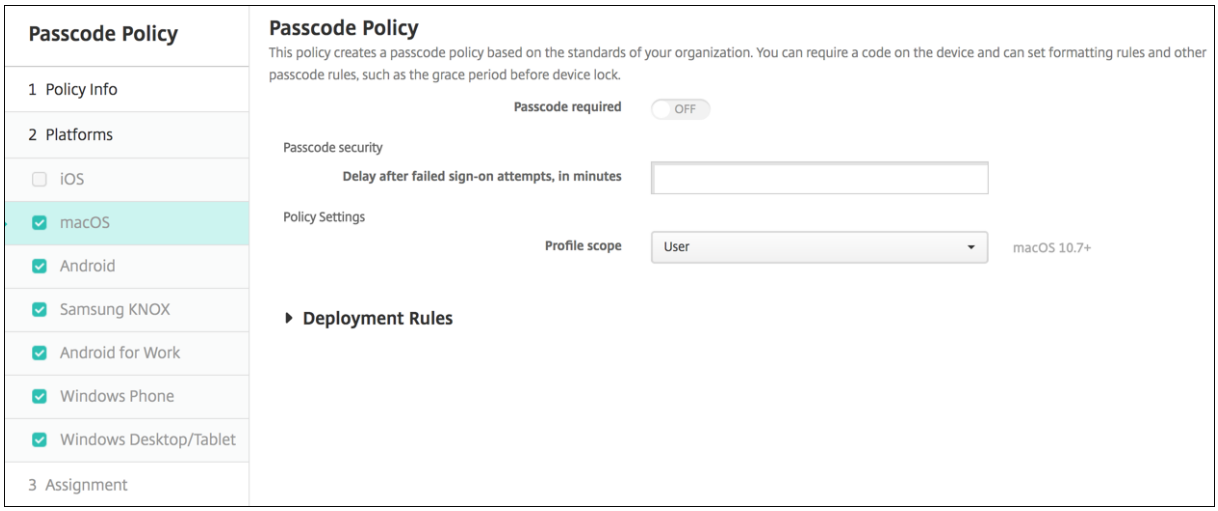


- **Passcode erforderlich:** Wählen Sie diese Option aus, um einen Passcode anzufordern und die Konfigurationsoptionen für die iOS-Passcoderichtlinie anzuzeigen. Die Seite wird erweitert, damit Sie die Einstellungen für Passcodeanforderungen, Passcodesicherheit und Richtlinieneinstellungen konfigurieren 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. Die Standardeinstellung ist **Ein**.
  - **Erforderliche Zeichen:** Wählen Sie aus, ob Passcodes mindestens einen Buchstaben enthalten sollen. Die Standardeinstellung ist **Aus**.
  - **Mindestanzahl von Symbolen:** Klicken Sie in der Liste auf die Anzahl der Symbole, die ein Passcode enthalten muss. Die Standardeinstellung 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. Die Standardeinstellung 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. Die Standardeinstellung 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. Die Standardeinstellung ist **0**. Dies bedeutet, dass der Passcode nie abläuft.
  - **Vorherige Kennwörter speichern (0-50):** Geben Sie an, wie viele verwendete Ken-

nwörter gespeichert werden sollen. Die Benutzer können kein gespeichertes Kennwort wiederverwenden. Gültige Werte sind 0–50. Die Standardeinstellung 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**.

macOS-Einstellungen

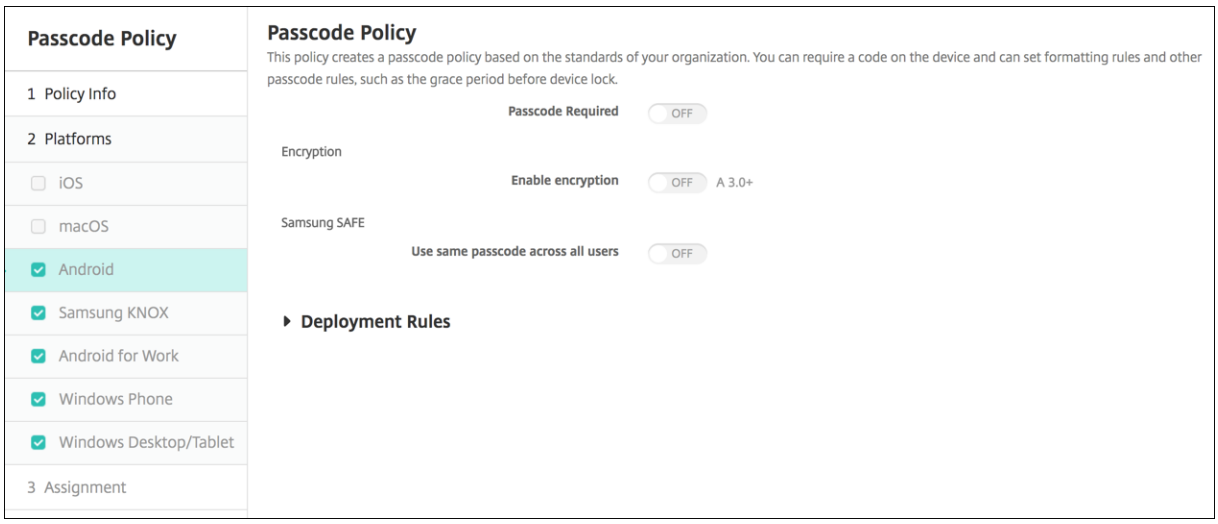


- **Passcode erforderlich:** Wählen Sie diese Option aus, um einen Passcode anzufordern und die Konfigurationsoptionen für die iOS-Passcoderichtlinie anzuzeigen. Die Seite wird erweitert, damit Sie die Einstellungen für Passcodeanforderungen, Passcodesicherheit und Richtlinieneinstellungen konfigurieren können.
- Wenn Sie **Passcode erforderlich** nicht aktivieren, geben Sie für **Verzögerung (in Minuten) nach fehlgeschlagenen Anmeldeversuchen** den Zeitraum in Minuten ein, bis ein Benutzer erneut versuchen darf, seinen Passcode einzugeben.
- Wenn Sie **Passcode erforderlich** auswählen, konfigurieren Sie die folgenden Einstellungen:
- **Passcodeanforderungen**
  - **Mindestlänge:** Klicken Sie in der Liste auf die Mindestlänge für den Passcode. Der Standardwert ist **6**.
  - **Einfache Passcodes zulassen:** Wählen Sie aus, ob einfache Passcodes zugelassen werden sollen. Einfache Passcodes sind Zeichenfolgen mit wiederholten oder sequenziellen Zeichen. Die Standardeinstellung ist **Ein**.
  - **Erforderliche Zeichen:** Wählen Sie aus, ob Passcodes mindestens einen Buchstaben enthalten sollen. Die Standardeinstellung ist **Aus**.
  - **Mindestanzahl von Symbolen:** Klicken Sie in der Liste auf die Anzahl der Symbole, die ein Passcode enthalten muss. Die Standardeinstellung 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. Die Standardeinstellung 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. Die Standardeinstellung 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. Die Standardeinstellung ist **0**. Dies 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. Die Standardeinstellung 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 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 einen Passcode eingeben kann.
- **Passcodezurücksetzung erzwingen:** Wenn ein Benutzer sich das nächste Mal authentifiziert, muss er seinen Code zurücksetzen.

- **Richtlinieneinstellungen**
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Android-Einstellungen



> **Hinweis:**
>
> Der Standardwert für Android ist **Aus**.

- **Passcode erforderlich:** Wählen Sie diese Option aus, um einen Passcode anzufordern 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 "Erforderliche Zeichen" ausgeblendet. Die Standardeinstellung ist **Aus**.
  - **Erforderliche Zeichen:** Klicken Sie in der Liste auf "Keine Einschränkung", "Ziffern und Buchstaben", "Nur Ziffern" oder "Nur Buchstaben", um die Zusammensetzung des Passcodes vorzugeben. Die Standardeinstellung ist Keine Einschränkung.
  - **Erweiterte Regeln:** Wählen Sie aus, ob erweiterte Passcoderegeln angewendet werden sollen. Diese Option ist für Android 3.0 und höher verfügbar. Die Standardeinstellung 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. Die Standardeinstellung 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. Die Standardeinstellung ist **0**. Dies 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. Die Standardeinstellung 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 gelöscht werden. Die Standardeinstellung ist **Nicht definiert**.

- **Verschlüsselung**
  - **Verschlüsselung aktivieren:** Wählen Sie aus, ob 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.

    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**

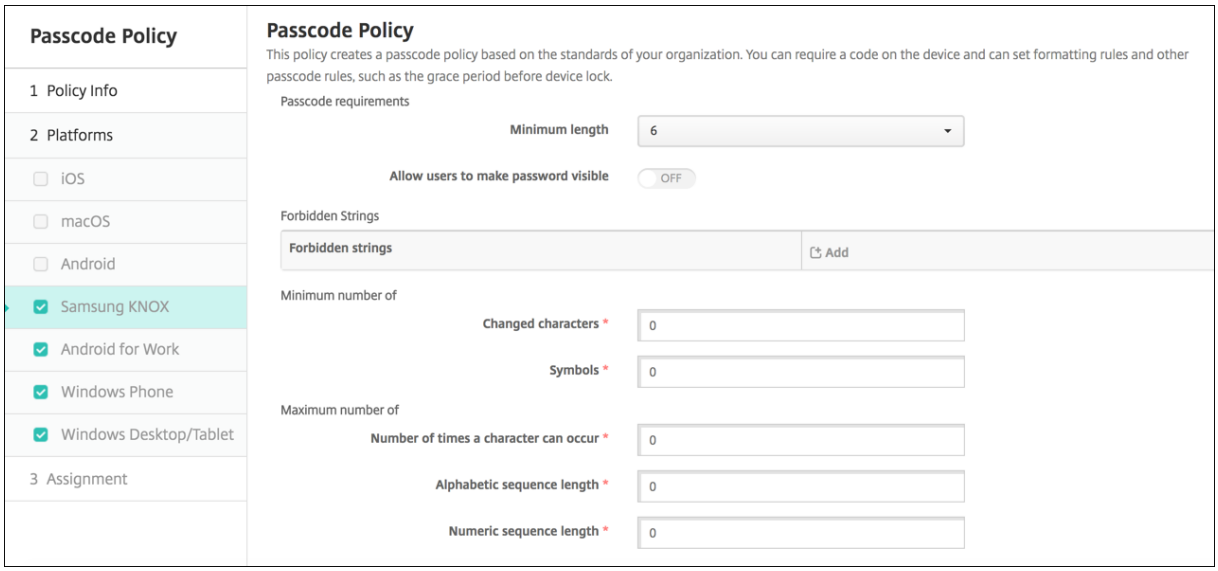
> **Hinweis:**
>
> Workaround für die Deaktivierung der Gesichts- oder Iriserkennung auf Samsung SAFE-Geräten: Erstellen Sie eine Einschränkungsrichtlinie für Samsung SAFE. Aktivieren Sie in der Einschränkungsrichtlinie die Option **Anwendungen deaktivieren** und fügen Sie `com.samsung.android.bio.face.service` oder `com.samsung.android.server.iris` der Tabelle hinzu. Stellen Sie dann die Einschränkungsrichtlinie bereit.

  - **Gleichen Passcode für alle Benutzer verwenden:** Wählen Sie aus, ob der gleiche Passcode für alle Benutzer verwendet werden soll. Die Standardeinstellung 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. Die Standardeinstellung ist **0**.
    - **Maximale Häufigkeit:** Geben Sie an, wie oft ein Zeichen in einem Passcode höchstens vorkommen darf. Die Standardeinstellung ist **0**.
    - **Länge der alphabetischen Sequenz:** Geben Sie die maximal zulässige Länge einer Reihe alphabetisch geordneter Zeichen in einem Passcode an. Die Standardeinstellung ist **0**.
    - **Länge der numerischen Sequenz:** Geben Sie die maximal zulässige Länge einer Reihe numerisch geordneter Zeichen in einem Passcode an. Die Standardeinstellung

ist **0**.

* **Benutzer dürfen Kennwort anzeigen:** Wählen Sie aus, ob Benutzern das Anzeigen des Passcodes ermöglicht werden soll. Die Standardeinstellung ist **Ein**.
* **Biometrische Authentifizierung konfigurieren:** Wählen Sie aus, ob die biometrische Authentifizierung aktiviert werden soll. Die Standardeinstellung ist **Aus**. Wenn Sie **Ein** wählen, können Sie folgende Optionen festlegen:
  - **Fingerabdruck zulassen:** Wählen Sie diese Option, um Benutzern die Authentifizierung per Fingerabdruck zu ermöglichen.
  - **Iriserkennung zulassen:** Wählen Sie diese Option, um Benutzern die Authentifizierung per Iriserkennung zu ermöglichen.
* **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.

Samsung KNOX-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

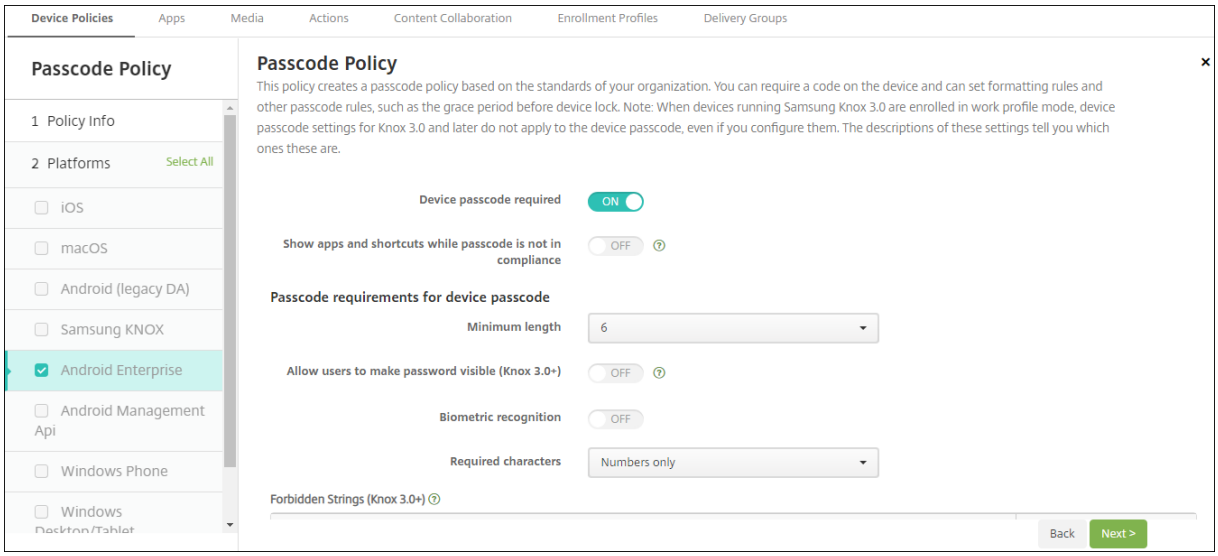
Passcodes ermöglicht werden soll.

- **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.

- **Mindestanzahl**
  - **Geänderte Zeichen:** Geben Sie an, wie viele Zeichen die Benutzer gegenüber dem vorherigen Passcode ändern müssen. Die Standardeinstellung ist **0**.
  - **Symbole:** Geben Sie die erforderliche Mindestzahl der Symbole in einem Passcode vor. Die Standardeinstellung ist **0**.
- **Maximale Anzahl**
  - **Maximale Häufigkeit:** Geben Sie an, wie oft ein Zeichen in einem Passcode höchstens vorkommen darf. Die Standardeinstellung ist **0**.
  - **Länge der alphabetischen Sequenz:** Geben Sie die maximal zulässige Länge einer Reihe alphabetisch geordneter Zeichen in einem Passcode an. Die Standardeinstellung ist **0**.
  - **Länge der numerischen Sequenz:** Geben Sie die maximal zulässige Länge einer Reihe numerisch geordneter Zeichen in einem Passcode an. Die Standardeinstellung ist **0**.
- **Passcodesicherheit**
  - **Gerät sperren nach (Minuten Inaktivität):** Klicken Sie in der Liste auf die Anzahl Sekunden, die ein Gerät inaktiv sein darf, bevor es gesperrt wird. Die Standardeinstellung 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. Die Standardeinstellung ist **0**. Dies 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. Die Standardeinstellung 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 der KNOX-Container und die KNOX-Daten von einem Gerät gelöscht werden. Be-

nutzer müssen den KNOX-Container nach dem Löschen neu initialisieren. Die Standardeinstellung ist **Nicht definiert**.

Android Enterprise-Einstellungen



Für Android Enterprise-Geräte können Sie festlegen, dass ein Passcode für das Gerät oder eine Sicherheitsabfrage für das Android Enterprise-Arbeitsprofil oder beides erforderlich ist.

Für Geräte mit Android 8.0 oder höher und Samsung Knox 3.0 und höher konfigurieren Sie die Einstellungen für Samsung Knox auf der Seite **Android Enterprise**. Für Geräte, auf denen frühere Versionen von Android oder Samsung Knox ausgeführt werden, verwenden Sie die Seite **Samsung Knox**.

> **Hinweis:**
>
> Wenn Geräte, auf denen Samsung Knox 3.0 ausgeführt wird, als Arbeitsprofilgeräte registriert sind, werden Einstellungen zum Gerätepasscode, die in Knox 3.0 und höher konfiguriert sind, nicht auf den Gerätepasscode angewandt.

- **Gerätepasscode erforderlich:** Erfordert einen Passcode auf dem Gerät. Konfigurieren Sie bei der Einstellung **Ein** die Einstellungen unter **Passcodeanforderungen für Gerätepasscode** und **Passcodesicherheit für Gerätepasscode**. Die Standardeinstellung ist **Aus**.
- **Apps und Verknüpfungen anzeigen, während der Passcode nicht richtlinientreu ist:** Bei Auswahl von **Ein** werden Apps und Verknüpfungen auf dem Gerät nicht ausgeblendet, wenn der Passcode nicht richtlinientreu ist. Bei Auswahl von **Aus** werden Apps und Verknüpfungen ausgeblendet, wenn der Passcode nicht richtlinientreu ist. Wenn Sie diese Einstellung aktivieren, empfiehlt Citrix, dass Sie eine automatisierte Aktion erstellen, um das Gerät als nicht richtlinientreu zu kennzeichnen, wenn der Passcode nicht richtlinientreu ist. Die Standardeinstellung ist **Aus**.
- **Passcodeanforderungen für Gerätepasscode:**

- **Mindestlänge:** Legt die Mindestlänge für den Passcode fest. Der Standardwert ist 6.
- **Benutzer dürfen Kennwort anzeigen:** Für Geräte mit Samsung Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist. Nur für vollständig verwaltete Geräte. Diese Einstellung gilt nicht für Geräte, die als Arbeitsprofilgeräte registriert sind. Ermöglicht Benutzern, das Kennwort sichtbar zu machen. Die Standardeinstellung ist **Aus**.
- **Biometrische Erkennung:**Aktiviert die biometrische Erkennung. Bei der Einstellung **Ein** wird das Feld **Erforderliche Zeichen** ausgeblendet. Die Standardeinstellung ist **Aus**.
- **Erforderliche Zeichen:** Legt die erforderlichen Zeichentypen für Passcodes fest. Zur Auswahl stehen **Keine Einschränkung**, **Ziffern und Buchstaben**, **Nur Ziffern** und **Nur Buchstaben**. Verwenden Sie **Keine Einschränkung** nur für Geräte mit Android 7.0. Bei Android 7.1 und höher funktioniert die Einstellung **Keine Einschränkung** nicht. Die Standardeinstellung ist **Ziffern und Buchstaben**.
- **Verbotene Zeichenfolgen:** Für Geräte mit Samsung Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist. Nur für vollständig verwaltete Geräte. Diese Einstellung gilt nicht für Geräte, die als Arbeitsprofilgeräte registriert sind. Gibt Zeichenfolgen an, die nicht als Passcodes verwendet werden können. Durch das Konfigurieren verbotener Zeichenfolgen verhindern Sie, dass Benutzer unsichere, einfach zu erratende Zeichenfolgen (“Kennwort”, “Willkommen”, “123456”, “111111” usw.) verwenden können. Zum Ausschluss einer Zeichenfolge klicken Sie auf **Hinzufügen** und geben die Zeichenfolge ein, die von Benutzern nicht verwendet werden soll. Klicken Sie dann auf **Speichern**, um die Zeichenfolge hinzuzufügen, oder auf **Abbrechen**, um das Hinzufügen der Zeichenfolge abzubrechen.
- **Erweiterte Regeln:** Wendet erweiterte Regeln zu zulässigen Zeichentypen in Passcodes an. Konfigurieren Sie bei der Einstellung **Ein** die Einstellungen unter **Mindestanzahl** und **Maximale Anzahl**. Diese Einstellung steht für Geräte mit Android-Versionen vor 5.0 nicht zur Verfügung. Die Standardeinstellung ist **Aus**.
- **Mindestanzahl:**
  - **Symbole:** Legt die Mindestanzahl der Symbole fest. Die Standardeinstellung ist **0**.
  - **Buchstaben:** Legt die Mindestanzahl der Buchstaben fest. Die Standardeinstellung ist **0**.
  - **Kleinbuchstaben:** Legt die Mindestanzahl der Kleinbuchstaben fest. Die Standardeinstellung ist **0**.
  - **Großbuchstaben:** Legt die Mindestanzahl der Großbuchstaben fest. Die Standardeinstellung ist **0**.
  - **Ziffern oder Symbole:** Legt die Mindestanzahl der Ziffern oder Symbole fest. Die Standardeinstellung ist **0**.
  - **Ziffern:** Legt die Mindestanzahl der Ziffern fest. Die Standardeinstellung ist **0**.
  - **Geänderte Zeichen:** Für Geräte mit Samsung Knox 3.0 und höher, für die ein gültiger

Knox-Lizenzschlüssel konfiguriert ist. Nur für vollständig verwaltete Geräte. Diese Einstellung gilt nicht für Geräte, die als Arbeitsprofilgeräte registriert sind. Legt fest, wie viele Zeichen die Benutzer im Vergleich zum vorherigen Passcode ändern müssen. Die Standardeinstellung ist **0**.

  - **Maximale Anzahl:** Für Geräte mit Samsung Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist. Nur für vollständig verwaltete Geräte. Diese Einstellung gilt nicht für Geräte, die als Arbeitsprofilgeräte registriert sind.
    * **Maximale Häufigkeit:** Legt fest, wie oft ein Zeichen in einem Passcode höchstens vorkommen darf. Die Standardeinstellung ist **0**, was bedeutet, dass keine Höchstgrenze festgelegt ist.
    * **Länge der alphabetischen Sequenz:** Legt die maximal zulässige Länge einer Reihe alphabetisch geordneter Zeichen in einem Passcode fest. Die Standardeinstellung ist **0**, was bedeutet, dass keine Höchstgrenze festgelegt ist.
    * **Länge der numerischen Sequenz:** Legt die maximal zulässige Länge einer Reihe numerisch geordneter Zeichen in einem Passcode fest. Die Standardeinstellung ist **0**, was bedeutet, dass keine Höchstgrenze festgelegt ist.

- **Passcodesicherheit für Gerätepasscode:**
  - **Gerät nach fehlgeschlagenen Anmeldeversuchen löschen:** Legt die Anzahl fehlgeschlagener Anmeldeversuche fest, nach deren Ablauf das Gerät vollständig gelöscht wird. Die Standardeinstellung ist **Nicht definiert**.
  - **Gerät sperren nach (Minuten Inaktivität) (0-999):** Legt die Anzahl der Minuten fest, die ein Gerät inaktiv sein darf, bevor es gesperrt wird. Die Standardeinstellung ist **Ohne**.
  - **Passcodeablauf in Tagen (1-730 Tage):** Legt die Anzahl der Tage fest, nach denen der Passcode ablaufen soll. Gültige Werte sind 1-730. Die Standardeinstellung ist **0**. Dies bedeutet, dass der Passcode nie abläuft.
  - **Vorherige Kennwörter speichern (0-50):** Legt fest, wie viele verwendete Kennwörter gespeichert werden sollen. Die Benutzer können kein gespeichertes Kennwort wiederverwenden. Gültige Werte sind 0-50. Die Standardeinstellung ist **0**, was bedeutet, dass Benutzer Kennwörter wiederverwenden können.
  - **Gerät nach fehlgeschlagenen Anmeldeversuchen sperren:** Für Geräte mit Samsung Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist. Nur für vollständig verwaltete Geräte. Diese Einstellung gilt nicht für Geräte, die als Arbeitsprofilgeräte registriert sind. Legt die Anzahl fehlgeschlagener Anmeldeversuche fest, nach deren Ablauf das Gerät gesperrt wird. Die Standardeinstellung ist **Nicht definiert**.
- **Sicherheitsabfrage für das Arbeitsprofil erforderlich:** Erzwingt eine Sicherheitsabfrage, bevor Benutzer auf Apps in einem Android Enterprise-Arbeitsprofil zugreifen können. Für Geräte mit Android 7.0 und höher. Konfigurieren Sie bei der Einstellung **Ein** die Einstellungen unter **Passcodeanforderungen für die Sicherheitsabfrage für Arbeitsprofil**und **Passcodesicherheit für die Sicherheitsabfrage für Arbeitsprofil**. Die Standardeinstellung ist

Aus.

- **Passcodeanforderungen für die Sicherheitsabfrage für Arbeitsprofile:**
  - **Mindestlänge:** Legt die Mindestlänge für den Passcode fest. Die Standardeinstellung ist 6.
  - **Benutzer dürfen Kennwort anzeigen:** Für Geräte mit Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist. Ermöglicht Benutzern, das Kennwort sichtbar zu machen. Die Standardeinstellung ist **Aus**.
  - **Biometrische Erkennung:**Aktiviert die biometrische Erkennung. Bei der Einstellung **Ein** wird das Feld **Erforderliche Zeichen** ausgeblendet. Die Standardeinstellung ist **Aus**.
  - **Erforderliche Zeichen:** Legt die erforderlichen Zeichentypen für Passcodes fest. Zur Auswahl stehen **Keine Einschränkung**, **Ziffern und Buchstaben**, **Nur Ziffern** und **Nur Buchstaben**. Verwenden Sie **Keine Einschränkung** nur für Geräte mit Android 7.0. Bei Android 7.1 und höher funktioniert die Einstellung **Keine Einschränkung** nicht. Die Standardeinstellung ist **Ziffern und Buchstaben**.
  - **Verbotene Zeichenfolgen:** Für Geräte mit Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist. Gibt Zeichenfolgen an, die nicht als Passcodes verwendet werden können. Durch das Konfigurieren verbotener Zeichenfolgen verhindern Sie, dass Benutzer unsichere, einfach zu erratende Zeichenfolgen (“Kennwort”, “Willkommen”, “123456”, “111111” usw.) verwenden können. Zum Ausschluss einer Zeichenfolge klicken Sie auf **Hinzufügen** und geben die Zeichenfolge ein, die von Benutzern nicht verwendet werden soll. Klicken Sie dann auf **Speichern**, um die Zeichenfolge hinzuzufügen, oder auf **Abbrechen**, um das Hinzufügen der Zeichenfolge abzubrechen.
  - **Erweiterte Regeln:** Wendet erweiterte Regeln zu zulässigen Zeichentypen in Passcodes an. Konfigurieren Sie bei der Einstellung **Ein** die Einstellungen unter **Mindestanzahl** und **Maximale Anzahl**. Diese Einstellung steht für Geräte mit Android-Versionen vor 5.0 nicht zur Verfügung. Die Standardeinstellung ist **Aus**.
  - **Mindestanzahl:**
    - **Symbole:** Legt die Mindestanzahl der Symbole fest. Die Standardeinstellung ist **0**.
    - **Buchstaben:** Legt die Mindestanzahl der Buchstaben fest. Die Standardeinstellung ist **0**.
    - **Kleinbuchstaben:** Legt die Mindestanzahl der Kleinbuchstaben fest. Die Standardeinstellung ist **0**.
    - **Großbuchstaben:** Legt die Mindestanzahl der Großbuchstaben fest. Die Standardeinstellung ist **0**.
    - **Ziffern oder Symbole:** Legt die Mindestanzahl der Ziffern oder Symbole fest. Die Standardeinstellung ist **0**.
    - **Ziffern:** Legt die Mindestanzahl der Ziffern fest. Die Standardeinstellung ist **0**.
    - **Geänderte Zeichen:** Für Geräte mit Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist. Legt fest, wie viele Zeichen die Benutzer im Vergleich

zum vorherigen Passcode ändern müssen. Die Standardeinstellung ist **0**.

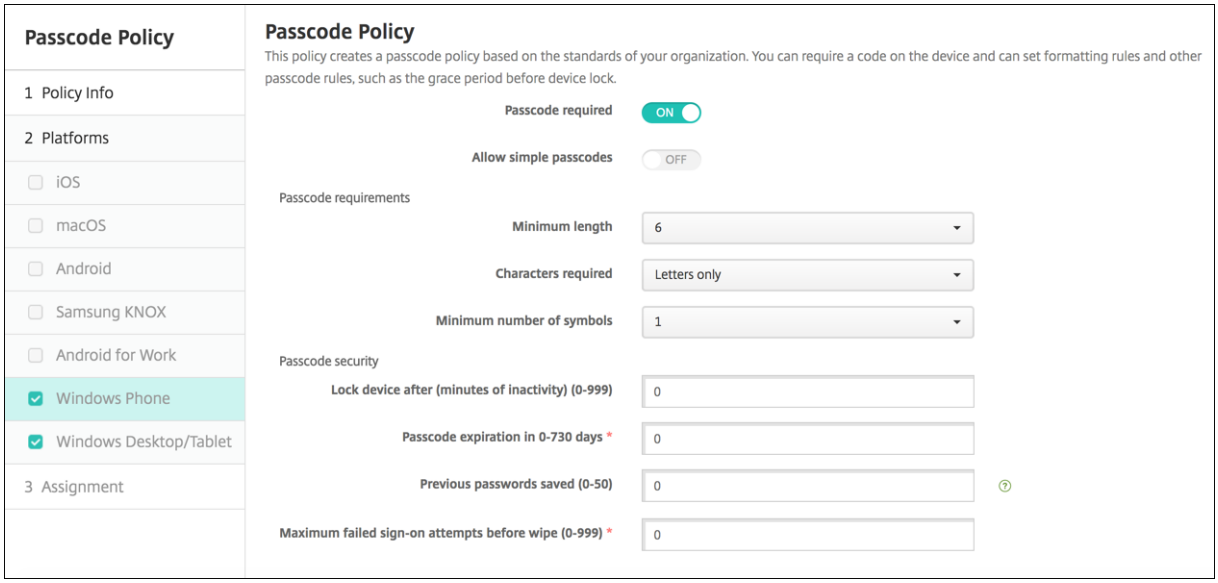
- **Maximale Anzahl:** Für Geräte mit Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist.
  - **Maximale Häufigkeit:** Legt fest, wie oft ein Zeichen in einem Passcode höchstens vorkommen darf. Die Standardeinstellung ist **0**, was bedeutet, dass keine Höchstgrenze festgelegt ist.
  - **Länge der alphabetischen Sequenz:** Legt die maximal zulässige Länge einer Reihe alphabetisch geordneter Zeichen in einem Passcode fest. Die Standardeinstellung ist **0**, was bedeutet, dass keine Höchstgrenze festgelegt ist.
  - **Länge der numerischen Sequenz:** Legt die maximal zulässige Länge einer Reihe numerisch geordneter Zeichen in einem Passcode fest. Die Standardeinstellung ist **0**, was bedeutet, dass keine Höchstgrenze festgelegt ist.
- **Einheitlichen Passcode aktivieren:** Bei Auswahl von **Ein** verwenden Benutzer denselben Passcode für ihr Gerät und ihr Arbeitsprofil. Bei Auswahl von **Aus**:
  - Benutzer müssen unterschiedliche Passcodes für ihr Gerät und ihr Arbeitsprofil verwenden.
  - Die Einstellung **Use one Lock**, mit der Benutzer nur einen Passcode für ihr Gerät und ihr Arbeitsprofil verwenden können, ist deaktiviert. Benutzer können sie nicht aktivieren.
  - Wenn die Passcodeanforderung für die Sicherheitsabfrage des Arbeitsprofils komplexer ist als der Gerätepasscode: Wenn Benutzer die Einstellung **Use one lock** aktiviert haben, werden sie aufgefordert, ihre Passcodes für das Arbeitsprofil zu ändern.

  Die Standardeinstellung ist **Aus**. Verfügbar ab Android 9.0.

- **Passcodesicherheit für die Sicherheitsabfrage für Arbeitsprofile**
  - **Container nach fehlgeschlagenen Anmeldeversuchen löschen:** Legt die Anzahl fehlgeschlagener Anmeldeversuche fest, nach deren Ablauf das Arbeitsprofil samt Daten vom Gerät gelöscht werden. Benutzer müssen das Arbeitsprofil nach dem Löschen neu initialisieren. Die Standardeinstellung ist **Nicht definiert**.
  - **Container sperren nach (Minuten Inaktivität):** Legt die Anzahl der Minuten fest, die ein Gerät inaktiv sein darf, bevor das Arbeitsprofil gesperrt wird. Die Standardeinstellung ist **Ohne**.
  - **Passcodeablauf in Tagen (1-730 Tage):** Legt die Anzahl der Tage fest, nach denen der Passcode ablaufen soll. Gültige Werte sind 1-730. Die Standardeinstellung ist **0**. Dies bedeutet, dass der Passcode nie abläuft.
  - **Vorherige Kennwörter speichern (0-50):** Legt fest, wie viele verwendete Kennwörter gespeichert werden sollen. Die Benutzer können kein gespeichertes Kennwort wiederverwenden. Gültige Werte sind 0-50. Die Standardeinstellung ist **0**, was bedeutet, dass Benutzer Kennwörter wiederverwenden können.

- **Container nach fehlgeschlagenen Anmeldeversuchen sperren:** Für Geräte mit Knox 3.0 und höher, für die ein gültiger Knox-Lizenzschlüssel konfiguriert ist. Legt die Anzahl fehlgeschlagener Anmeldeversuche fest, nach deren Ablauf das Gerät gesperrt wird. Die Standardeinstellung ist **Nicht definiert**.

Windows Phone-Einstellungen

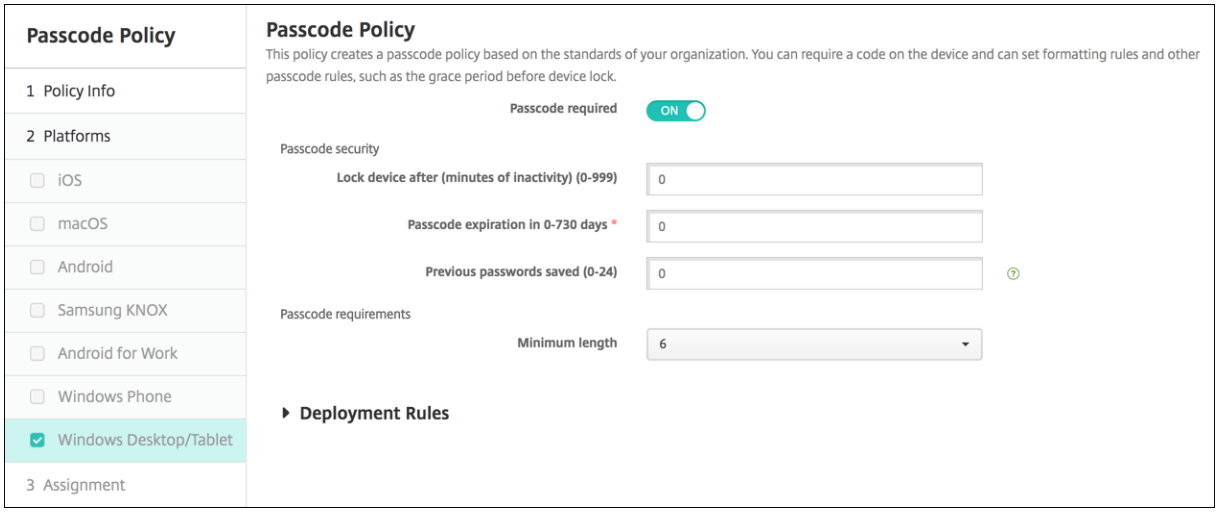


- **Passcode erforderlich:** Deaktivieren Sie diese Option, wenn für Windows Phone-Geräte kein Passcode erforderlich sein soll. Die Standardeinstellung ist **Ein**, ein Passcode ist also erforderlich. Die Seite wird verkleinert und die nachfolgend aufgeführten Optionen werden ausgeblendet, wenn Sie diese Einstellung nicht aktivieren.
- **Einfache Passcodes zulassen:** Wählen Sie aus, ob einfache Passcodes zugelassen werden sollen. Einfache Passcodes sind Zeichenfolgen mit wiederholten oder sequenziellen Zeichen. Die Standardeinstellung 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. Die Standardeinstellung ist **Nur Buchstaben**.
  - **Mindestanzahl von Symbolen:** Klicken Sie in der Liste auf die Anzahl der 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. Die Standardeinstellung ist **0**.
  - **Passcodeablauf in 0-730 Tagen:** Geben Sie die Anzahl der Tage ein, nach denen der Pass-

code ablaufen soll. Gültige Werte sind 0-730. Die Standardeinstellung ist **0**. Dies 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. Die Standardeinstellung 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. Die Standardeinstellung ist **0**.

Windows Desktop/Tablet-Einstellungen



- **Komfortanmeldung nicht zulassen:** Wählen Sie aus, ob Benutzern der Zugriff auf ihre Geräte über Bildkennwörter oder Biometrieanmeldungen gestattet werden soll. Die Standardeinstellung 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. Die Standardeinstellung ist **0**. Dies 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. Die Standardeinstellung 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. Die Standardeinstellung ist **0**.

Richtlinien für persönliche Hotspots

October 25, 2018

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Persönlichen Hotspot deaktivieren:** Wählen Sie aus, ob das Feature für persönliche Hotspots auf den Geräten aktiviert oder deaktiviert werden soll. Die Standardeinstellung ist **Aus**. Die persönlichen Hotspots werden auf Benutzergeräten 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.

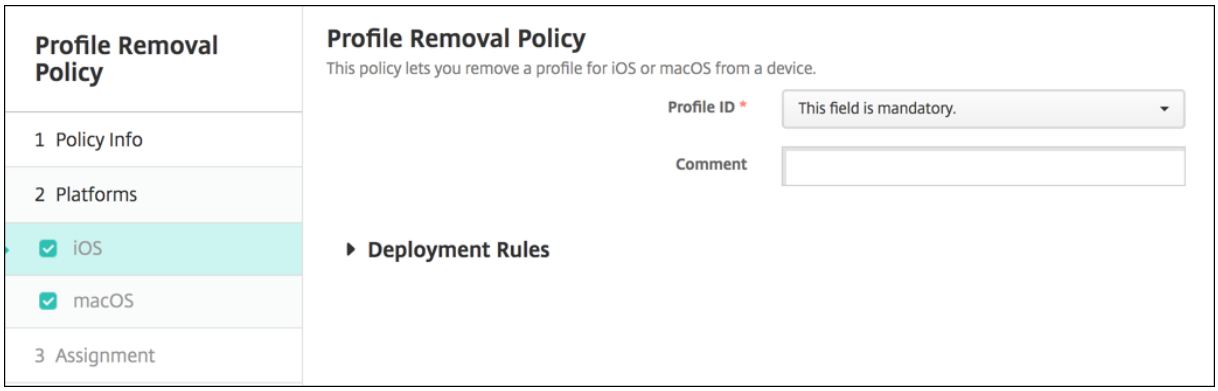
Geräterichtlinie für Profilentfernung

January 5, 2022

Sie können eine Richtlinie zum Entfernen von App-Profilen in XenMobile erstellen. Bei ihrer Bereitstellung entfernt die Richtlinie das App-Profil von iOS- bzw. macOS-Geräten.

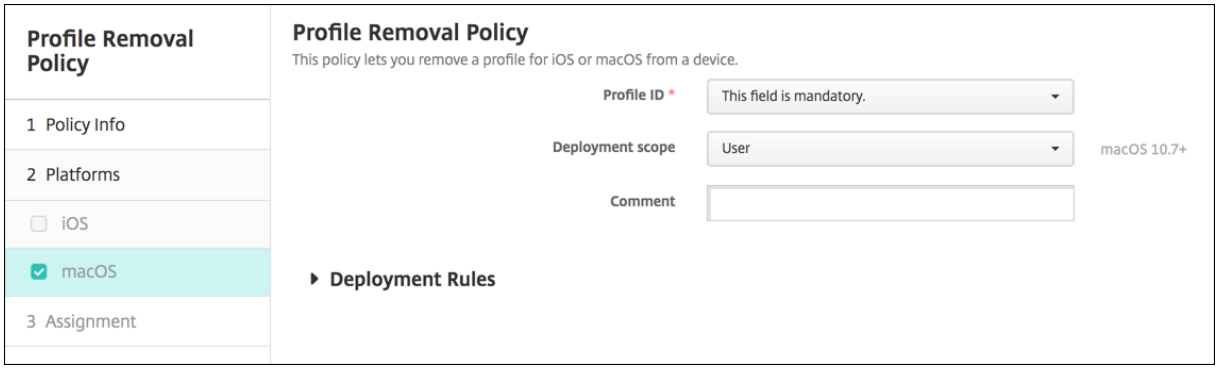
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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.

macOS-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**. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.
- **Kommentar:** Geben Sie optional einen Kommentar ein.

Provisioningprofilrichtlinie

April 16, 2020

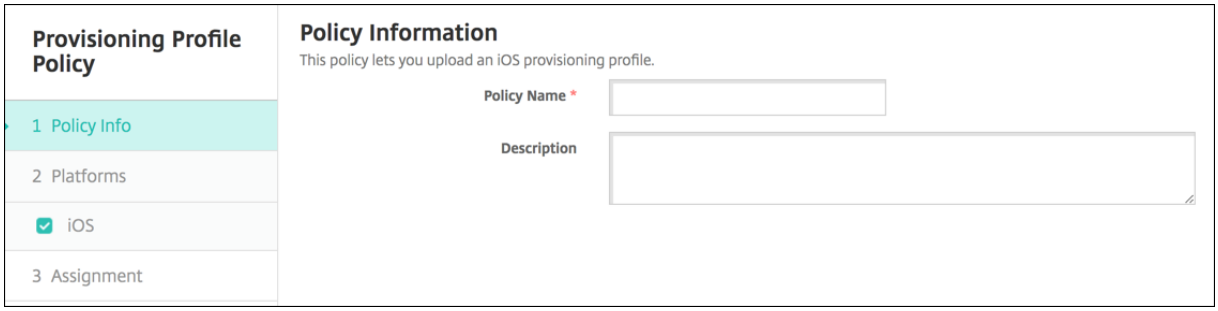
Beim Entwickeln und Signieren einer iOS-Unternehmensapp wird normalerweise ein Provisioningprofil eingeschlossen, das gemäß Apple für die Ausführung der App auf iOS-Geräten erforderlich ist. Wenn das Provisioningprofil fehlt oder abgelaufen ist, stürzt die App ab, wenn der Benutzer darauf tippt.

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.

Vor dem Erstellen einer Provisioningprofilrichtlinie müssen Sie eine Provisioningprofildatei erstellen. Weitere Informationen finden Sie im Apple-Artikel über das Erstellen eines Entwicklungsprovisioningprofils: Apple Developer-Website.

iOS-Einstellungen



- **iOS-Provisioningprofil:** Wählen Sie die zu importierende Provisioningprofildatei aus, indem Sie auf **Durchsuchen** klicken und dann zum Speicherort der Datei navigieren.

Richtlinie zum Entfernen von Provisioningprofilen

October 22, 2020

Sie können iOS-Provisioningprofile mit Geräterichtlinien entfernen. Weitere Informationen zu Provisioningprofilen finden Sie unter Provisioningprofilrichtlinie.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **iOS-Provisioningprofil:** Klicken Sie in der Liste auf das Provisioningprofil, das Sie entfernen möchten.
- **Kommentar:** Geben Sie optional einen Kommentar ein.

Proxy-Geräterichtlinie

January 5, 2022

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Voraussetzungen

Versetzen Sie vor dem Bereitstellen dieser Richtlinie alle iOS-Geräte, für die Sie eine globale HTTP-Proxyrichtlinie festlegen möchten, in den betreuten Modus. Einzelheiten finden Sie unter Versetzen eines iOS-Geräts mit Apple Configurator in den betreuten Modus oder Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm.

Legen Sie Bereitstellungsregeln für die Geräteregistrierung fest, bevor Sie die Proxyrichtlinie an die Geräte senden.

iOS-Einstellungen

- **Proxykonfiguration:** Klicken Sie auf **Manuell** oder **Automatisch**, um festzulegen, wie der Proxy auf den Geräten der Benutzer konfiguriert wird.
  - Bei Auswahl von **Manuell** konfigurieren Sie die folgenden Einstellungen:
    * **Hostname oder IP-Adresse des Proxyservers:** Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein. Diese Angabe ist erforderlich.
    * **Port für den Proxyserver:** Geben Sie die Portnummer des Proxyservers ein. Diese Angabe ist erforderlich.
    * **Benutzername:** Geben Sie optional einen Benutzernamen für die Authentifizierung beim Proxyserver ein.
    * **Kennwort:** Geben Sie optional ein Kennwort für die Authentifizierung beim Proxyserver ein.

  - Bei Auswahl von **Automatisch** konfigurieren Sie die folgenden Einstellungen:
    * **Proxy-PAC-URL:** Geben Sie die URL der PAC-Datei zur Bestimmung der Proxykonfiguration ein.
    * **Direkte Verbindung zulassen, wenn PAC nicht erreichbar ist:** Wählen Sie aus, ob Benutzer eine direkte Verbindung mit dem Ziel herstellen dürfen, wenn die PAC-Datei nicht erreichbar ist. Die Standardeinstellung ist **Ein**. Diese Option ist nur für iOS 7.0 und höher verfügbar.

- **Proxyumgehung zulassen für Zugriff auf Captive-Netzwerke:** Wählen Sie aus, ob die Proxyumgehung für den Zugriff auf Captive-Netzwerke zulässig sein soll. Die Standardeinstellung ist **Aus**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

Windows Mobile-/CE-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 Standardeinstellung ist **80**.
- **Benutzername:** Geben Sie optional einen Benutzernamen für die Authentifizierung beim Proxyserver ein.

- **Kennwort:** Geben Sie optional ein Kennwort für die Authentifizierung beim Proxyserver ein.
- **Domänenname:** Geben Sie optional einen Domänennamen ein.
- **Aktivieren:** Wählen Sie aus, ob der Proxyserver aktiviert werden soll. Die Standardeinstellung ist **Ein**.

Registrierungsrichtlinie

October 25, 2018

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Gerätерichtlinien.

Windows Mobile-/CE-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.

Geräterichtlinie für Remotesupport

January 5, 2022

> **Hinweis:**
>
> Für on-premises XenMobile Server-Bereitstellungen: Durch Remotesupport können Helpdesk-Mitarbeiter die Fernsteuerung verwalteter Windows CE- und Android-Mobilgeräte übernehmen. Screencast wird nur auf Samsung KNOX-Geräten unterstützt.
>
> Remotesupport wird nicht für geclusterte on-premises XenMobile Server-Bereitstellungen unterstützt.
>
> Weitere Informationen finden Sie unter Supportoptionen und Remotesupport.

Sie erstellen eine Remotesupportrichtlinie in XenMobile, um Remotezugriff auf unterstützte Windows- und Android-Geräte zu erhalten. Sie können Support zweierlei Art konfigurieren:

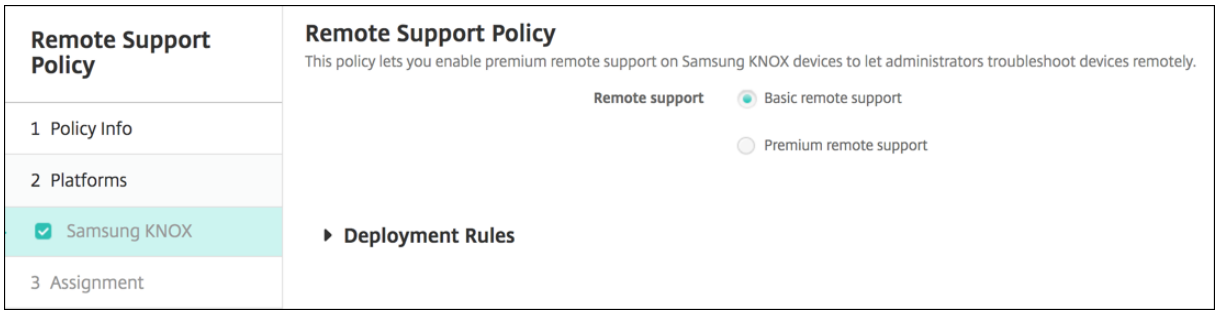
- **Einfacher Remotesupport**: Der einfache Support ermöglicht das Anzeigen von Diagnoseinformationen zum Gerät, z. B. Systeminformationen, ausgeführte Prozesse, Task-Manager (Arbeitsspeicher und CPU-Nutzung), Inhalt des Ordners für installierte Software usw.
- **Premiumremotesupport:** Remotesteuerung des Gerätebildschirms, u. a.:
  - Steuerung mit Farben im Hauptfenster oder in einem eigenen, unverankerten Fenster
  - Erstellen einer VoIP-Sitzung zwischen Helpdesk und Benutzer
  - Konfigurieren von Einstellungen
  - Erstellen einer Chatsitzung zwischen Helpdesk und Benutzer

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 der App-Tunnel-Remotesupportrichtlinie und der Samsung KNOX-Remotesupportrichtlinie auf den Geräten der Benutzer

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android- und Windows CE-Einstellungen



- **Remotesupport:** Wählen Sie **Einfacher Remotesupport** oder **Premiumremotesupport** aus. Die Standardeinstellung ist **Einfacher Remotesupport**.

Geräteeinschränkungsrichtlinie

January 5, 2022

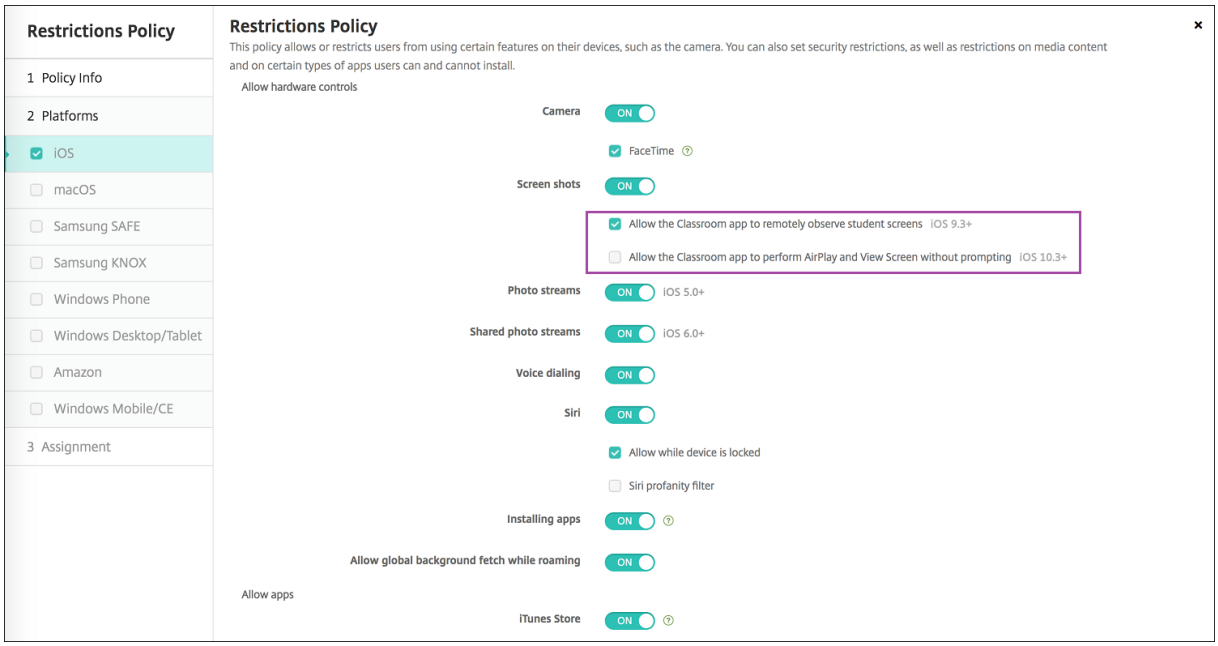
Die Geräterichtlinie für Einschränkungen lässt bestimmte Features oder Funktionen wie z. B. die Kamera auf Benutzergeräten zu oder schränkt sie ein. Sie können außerdem Einschränkungen für Sicherheit und Medieninhalte festlegen und vorgeben, welche App-Typen Benutzer installieren können. Die meisten Einschränkungen sind standardmäßig auf **Ein** bzw. *zugelassen* festgelegt. Die wichtigsten Ausnahmen bilden das Feature "iOS-Sicherheit - Erzwingen" sowie alle Windows-Tablet-Features, die standardmäßig auf **Aus** bzw. *nicht zugelassen* festgelegt sind.

Wird auf einem Windows 10 RS2 Phone-Gerät eine benutzerdefinierte XML-Richtlinie oder eine Einschränkungsrichtlinie zum Deaktivieren von Internet Explorer bereitgestellt, verbleibt der Browser im aktivierten Status. Starten Sie als Workaround das Gerät neu. Dies ist ein Drittanbieterproblem.

> **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 ihrem Gerät nicht verwenden.
>
> **Screen shots**: Bei Auswahl von **Ein** können Benutzer Screenshots auf den Geräten erstellen. Bei Auswahl von **Aus** können Benutzer keine Screenshots auf den Geräten erstellen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



Einige Einstellungen der Einschränkungsrichtlinie für iOS gelten nur für bestimmte iOS-Versionen, wie hier und auf der Seite zur Einschränkungsrichtlinie der XenMobile-Konsole beschrieben ist.

Einstellungen der iOS-Einschränkungsrichtlinie gelten ggf., wenn das Gerät im Benutzer-Registrierungsmodus, im nicht betreuten Modus (vollständiges MDM) oder im betreuten Modus registriert ist. Die folgende Tabelle zeigt die Registrierungsmodi für jede Einschränkungsrichtlinieneinstellung für iOS 13 und höher.

Wie bereits erwähnt, stehen einige Einstellungen, die zuvor im betreuten und im nicht betreuten Modus verfügbar waren, ab iOS 13 nur auf betreuten Geräten zur Verfügung. Es gelten folgende Regeln:

- Wenn sich ein betreutes Geräte mit iOS 13+ bei XenMobile registriert, gelten die Einstellungen für das Gerät.
- Wenn sich ein nicht betreutes Gerät mit iOS 13+ bei XenMobile registriert, gelten die Einstellungen nicht für das Gerät.
- Wenn ein Gerät mit iOS 12 (oder niedriger), das bereits bei XenMobile registriert ist, auf iOS 13 aktualisiert wird, werden keine Änderungen vorgenommen. Die Einstellungen gelten für das Gerät wie vor dem Upgrade.

Informationen, wie Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus.

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Hardwaresteuereleme zulassen			
Kamera	Nein	Ja	Ja
FaceTime	Nein	Nein (neu in iOS 13)	Ja
Screenshots	Ja	Nein	Ja
Classroom-App erlauben, die Bildschirme von Schülern remote zu beobachten	Nein	Nein	Ja
Classroom-App die Verwendung von AirPlay und Bildschirmansicht ohne Aufforderung ermöglichen	Nein	Nein	Ja
Fotostreams	Nein	Ja	Ja
Freigegebene Fotostreams	Nein	Ja	Ja
Sprachwahl	Nein	Ja	Ja
Siri	Ja	Ja	Ja
Zulassen, während Gerät gesperrt ist	Ja	Ja	Ja
Siri-Obszönitätenfilter	Nein	Nein	Ja
Installieren von Apps	Nein	Nein (neu in iOS 13)	Ja
Globale Hintergrundabfrage beim Roaming zulassen	Nein	Ja	Ja
Apps zulassen			
iTunes Store	Nein	Nein (neu in iOS 13)	Ja
In-App-Käufe	Nein	Ja	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
iTunes-Kennwort für Käufe erforderlich	Nein	Ja	Ja
Safari	Nein	Nein (neu in iOS 13)	Ja
Automatisch ausfüllen	Nein	Nein (neu in iOS 13)	Ja
Betrugswarnung erzwingen	Ja	Ja	Ja
JavaScript aktivieren	Nein	Ja	Ja
Popups blockieren	Nein	Ja	Ja
Cookies annehmen	Nein	Ja	Ja
Netzwerk - iCloud-Aktionen zulassen			
iCloud-Dokumente & -Daten	Nein	Nein (neu in iOS 13)	Ja
iCloud-Backup	Nein	Ja	Ja
iCloud-Schlüsselbund	Nein	Ja	Ja
iCloud-Fotobibliothek	Nein	Ja	Ja
Sicherheit - Erzwingen			
Verschlüsselte Backups	Ja	Ja	Ja
Beschränktes Ad-Tracking	Nein	Ja	Ja
Passcode bei erster AirPlay-Kopplung	Ja	Ja	Ja
Gekoppelte Apple Watch verwendet Wrist Detect	Ja	Ja	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Freigeben von verwalteten Dokumenten mit AirDrop	Ja	Ja	Ja
Sicherheit - Zulassen			
Nicht vertrauenswürdige SSL-Zertifikate akzeptieren	Nein	Ja	Ja
Automatisches Update für Zertifikatsvertrauen-seinstellungen	Nein	Ja	Ja
Dokumente von verwalteten Apps in nicht verwalteten Apps	Ja	Ja	Ja
Nicht verwaltete Apps lesen verwaltete Kontakte	Nein	Nein	Ja
Verwaltete Apps schreiben nicht verwaltete Kontakte	Nein	Nein	Ja
Dokumente von nicht verwalteten Apps in verwalteten Apps	Ja	Ja	Ja
Senden von Diagnose-informationen an Apple	Ja	Ja	Ja
Touch ID zum Entsperren von Gerät	Nein	Ja	Ja
Passbook-Benachrichtigungen bei Sperre	Nein	Ja	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Übergabe	Nein	Ja	Ja
iCloud-Synchronisierung für verwaltete Apps	Ja	Ja	Ja
Backup von Unternehmensbüchern	Ja	Ja	Ja
Synchronisieren von Notizen und Markierungen in Unternehmensbüchern	Ja	Ja	Ja
Internetergebnisse in Spotlight	Nein	Ja	Ja
Vertrauensstellung für Unternehmensapp	Nein	Ja	Ja
Einstellungen nur für Betreute Geräte - Zulassen			
Alle Inhalte und Einstellungen löschen	Nein	Nein	Ja
Konfigurationsbeschränkungen	Nein	Nein	Ja
Podcasts	Nein	Nein	Ja
Installation von Konfigurationsprofilen	Nein	Nein	Ja
Fingerabdruckänderun	Nein	Nein	Ja
Installieren von Apps vom Gerät	Nein	Nein	Ja
Tastenkombinationen	Nein	Nein	Ja
Gekoppelte Apple Watch	Nein	Nein	Ja
Passcodeänderung	Nein	Nein	Ja
Gerätenamensänderung	Nein	Nein	Ja
Hintergrundbildänderu	Nein	Nein	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Automatischer Download von Apps	Nein	Nein	Ja
AirDrop	Nein	Nein	Ja
iMessage	Nein	Nein	Ja
Benutzergenerierte Inhalte in Siri	Nein	Nein	Ja
iBooks	Nein	Nein	Ja
Apps entfernen	Nein	Ja	Ja
Game Center	Nein	Nein (neu in iOS 13)	Ja
Freunde hinzufügen	Nein	Nein	Ja
Multiplayer-Gaming	Nein	Nein (neu in iOS 13)	Ja
Kontoeinstellungen bearbeiten	Nein	Nein	Ja
Einstellungen für mobile Daten in App ändern	Nein	Nein	Ja
Einstellungen für mobile Daten in App ändern	Nein	Nein	Ja
Einstellungen für Freundesuche ändern	Nein	Nein	Ja
Kopplung mit Nicht-Configurator-Hosts	Nein	Nein	Ja
Tastaturvorhersage	Nein	Nein	Ja
Tastatur mit Autokorrektur	Nein	Nein	Ja
Tastatur mit Rechtschreibprüfung	Nein	Nein	Ja
Definition nachschlagen	Nein	Nein	Ja
Einzelne App-Paket-ID			
Nachrichten	Nein	Nein	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Apple Music	Nein	Nein	Ja
iTunes Radio	Nein	Nein	Ja
Benachrichtigungsänderung	Nein	Nein	Ja
Eingeschränkte App-Verwendung	Nein	Nein	Ja
Änderung der Übermittlung von Diagnosedaten	Nein	Nein	Ja
Bluetooth-Änderung	Nein	Nein	Ja
Diktat zulassen	Nein	Nein	Ja
Nur Wi-Fi-Netzwerken beitreten, die von einer Wi-Fi-Richtlinie installiert wurden	Nein	Nein	Ja
Classroom-App die Verwendung von AirPlay und Bildschirmansicht ohne Aufforderung ermöglichen	Nein	Nein	Ja
Classroom-App das Sperren einer App und des Geräts ohne Aufforderung erlauben	Nein	Nein	Ja
Automatische Teilnahme an Klassen der Classroom-App ohne Aufforderung	Nein	Nein	Ja
AirPrint zulassen	Nein	Nein	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Speichern von AirPrint-Anmeldeinformationen in Schlüsselbund zulassen	Nein	Nein	Ja
Ermittlung von AirPrint-Druckern mit iBeacons zulassen	Nein	Nein	Ja
AirPrint nur bei Zielen mit vertrauenswürdigen Zertifikaten zulassen	Nein	Nein	Ja
VPN-Konfigurationen hinzufügen	Nein	Nein	Ja
Einstellungen für Mobilnetzabo ändern	Nein	Nein	Ja
Entfernen von System-Apps	Nein	Nein	Ja
Einrichten neuer Geräte in der Nähe	Nein	Nein	Ja
Eingeschränkten USB-Modus zulassen	Nein	Nein	Ja
Verzögerte Softwareupdates erzwingen	Nein	Nein	Ja
Erzwungene Verzögerung für Softwareupdate	Nein	Nein	Ja
Um Erlaubnis zum Verlassen von Klassen fragen	Nein	Nein	Ja
Automatisches Datum und Uhrzeit erzwingen	Nein	Nein	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Kennwörter autom. ausfüllen	Nein	Nein	Ja
Kennwortanforderung bei Geräten in der Nähe	Nein	Nein	Ja
Kennwort teilen	Nein	Nein	Ja
Sicherheit - Auf Sperrbildschirm anzeigen			
Kontrollzentrum	Ja	Ja	Ja
Benachrichtigung	Ja	Ja	Ja
Heuteansicht	Ja	Ja	Ja
Medieninhalte - Zulassen			
Anstößige Musik, Podcasts und iTunes U-Inhalte	Nein	Nein (neu in iOS 13)	Ja
Sexuelle Inhalte in iBooks	Nein	Ja	Ja
Bewertungsregion	Nein	Ja	Ja
Filme	Nein	Ja	Ja
Fernsehsendungen	Nein	Ja	Ja
Apps	Nein	Ja	Ja

- **Hardwaresteuerelemente zulassen**
  - **Kamera:** Verwendung der Kamera von Geräten zulassen.
    - **FaceTime:** Verwendung von FaceTime auf Geräten zulassen. Für betreute iOS-Geräte.
  - **Screenshots:** Erstellen von Screenshots auf Geräten zulassen.
    - **Classroom-App erlauben, die Bildschirme von Schülern remote zu beobachten:** Wenn diese Einschränkung deaktiviert ist, können Lehrkräfte die Bildschirme von Lernenden nicht mit der Classroom-App remote beobachten. In der Standardeinstellung ist die Einschränkung aktiviert, d. h. Lehrkräfte können die App zum Beobachten der Bildschirme verwenden. Die Einstellung **Classroom-App die Verwendung von AirPlay und Bildschirmansicht ohne Aufforderung ermöglichen** legt fest, ob Ler-

nende eine Aufforderung erhalten, die Bildschirmansicht durch die Lehrkraft zuzulassen. Für betreute iOS-Geräte.

* **Classroom-App die Verwendung von AirPlay und Bildschirmansicht ohne Aufforderung ermöglichen:** Wenn diese Einschränkung ausgewählt ist, kann die Lehrkraft AirPlay und Bildschirmansichten ausführen, ohne dass der Lernende zur Erteilung einer entsprechenden Berechtigung aufgefordert wird. Die Einstellung ist standardmäßig deaktiviert. Für betreute iOS-Geräte.

- **Fotostreams:** Verwendung von MyPhotoStream zum Teilen von Fotos über iCloud für alle eigenen iOS-Geräte zulassen.
- **Freigegebene Fotostreams:** Verwendung von iCloud Photo Sharing zum Teilen von Fotos mit Kollegen, Freunden und Familie zulassen.
- **Sprachwahl:** aktiviert Sprachwahl auf Benutzergeräten.
- **Siri:** lässt die Verwendung von Siri zu.
  * **Zulassen, während Gerät gesperrt ist:** Verwendung von Siri bei gesperrtem Gerät zulassen.
  * **Siri-Obszönitätenfilter:** Schimpfwortfilter von Siri aktivieren. Standardmäßig ist dieses Feature eingeschränkt, d. h. es wird kein Schimpfwortfilter verwendet.
    Weitere Informationen zu Siri und Sicherheit finden Sie unter Richtlinien für Siri und die Diktierfunktion.
- **Apps installieren:** App-Installation durch Benutzer zulassen. Für betreute iOS-Geräte.
- **Globale Hintergrundabfrage beim Roaming zulassen:** automatische Synchronisierung von E-Mail-Konten mit iCloud im Roamingbetrieb zulassen. Bei Auswahl von **Aus** wird die globale Hintergrundabfrage beim Roaming von iOS-Telefonen deaktiviert. Die Standardeinstellung ist **Ein**.

- **Apps zulassen**
  - **iTunes Store:** Zugriff auf iTunes Store zulassen. Für betreute iOS-Geräte.
  - **In-App-Käufe:** Zulassen, dass Benutzer In-App-Käufe machen.
    * **iTunes-Kennwort für Käufe erforderlich:** Kennwort für In-App-Käufe anfordern. Standardmäßig ist dieses Feature eingeschränkt, d. h. für In-App-Käufe ist kein Kennwort erforderlich.
  - **Safari:** Zugriff auf Safari zulassen. Für betreute iOS-Geräte.
    * **Automatisch ausfüllen:** Einrichtung des automatischen Ausfüllens für Benutzernamen und Kennwörter in Safari zulassen.
    * **Betrugswarnung erzwingen:** Wenn diese Einstellung aktiviert ist und Benutzer eine Phishing-verdächtige Website besuchen, warnt Safari die Benutzer. Standardmäßig ist dieses Feature eingeschränkt, d. h. es werden keine Warnungen ausgegeben.
    * **JavaScript aktivieren:** Ausführung von JavaScript in Safari zulassen.
    * **Popups blockieren:** Popups beim Besuch von Websites blockieren. Standardmäßig ist dieses Feature eingeschränkt, d. h. es werden keine Popups blockiert.

  - **Cookies annehmen:** Legen Sie fest, in welchem Maß Cookies akzeptiert werden sollen. Wählen Sie in der Liste eine Option zum Zulassen oder Einschränken von Cookies aus. In der Standardeinstellung **Immer** können Cookies von allen Websites in Safari gespeichert werden. Die anderen Optionen sind **Nur aktuelle Website**, **Nie** und **Nur von besuchten Websites**.

- **Netzwerk - iCloud-Aktionen zulassen**
  - **iCloud-Dokumente und -Daten:** Synchronisierung von Dokumenten und Daten mit iCloud zulassen. Für betreute iOS-Geräte.
  - **iCloud-Backup:** Sicherung von Geräten in iCloud zulassen.
  - **iCloud-Schlüsselbund:** Speichern von Kennwörtern, Wi-Fi-Netzwerkinformationen, Kreditkartendaten und anderen Informationen im iCloud-Schlüsselbund zulassen.
  - **Cloudfotobibliothek:** Zugriff auf iCloud-Fotobibliothek zulassen.
- **Sicherheit - Erzwingen**

  Standardmäßig sind folgende Features eingeschränkt, d. h. keine Sicherheitsfeatures sind aktiviert.
  - **Verschlüsselte Backups:** Verschlüsseln von Sicherungen in iCloud erzwingen.
  - **Beschränktes Ad-Tracking:** Gezieltes Ad-Tracking sperren.
  - **Passcode bei erster AirPlay-Kopplung:** Prüfung AirPlay-aktivierter Geräte über einen einmaligen, auf dem Bildschirm angezeigten Code vor der Verwendung von AirPlay erzwingen.
  - **Gekoppelte Apple Watch verwendet Wrist Detect:** Zur Verwendung der **Handgelenkserkennung** gekoppelte Apple Watch vorschreiben.
  - **Freigeben von verwalteten Dokumenten mit AirDrop:** Wenn Sie diese Option auf **Ein** festlegen, erscheint AirDrop als nicht verwaltetes Ablageziel.
- **Sicherheit - Zulassen**
  - **Nicht vertrauenswürdige SSL-Zertifikate akzeptieren:** Akzeptieren nicht vertrauenswürdiger SSL-Zertifikate von Websites zulassen.
  - **Automatisches Update für Zertifikatvertrauensstellungsoptionen:** Automatisches Update vertrauenswürdiger Zertifikate zulassen.
  - **Dokumente von verwalteten Apps in nicht verwalteten Apps:** Übertragen von Daten von verwalteten Apps (Unternehmensapps) in nicht verwaltete (private) Apps zulassen.
  - **Dokumente von nicht verwalteten Apps in verwalteten Apps:** Übertragen von Daten von nicht verwalteten (privaten) Apps in verwaltete Apps (Unternehmensapps) zulassen.
  - **Senden von Diagnoseinformationen an Apple:** Senden anonymer Diagnosedaten über Benutzergeräte an Apple zulassen.
  - **Touch ID zum Entsperren von Gerät:** Entsperren von Geräten per Fingerabdruck zulassen.

- **Passbook-Benachrichtigungen bei Sperre:** Anzeige von Passbook-Benachrichtigungen auf dem Sperrbildschirm zulassen.
- **Übergabe:** Übertragung von Aktivitäten von einem iOS-Gerät zu einem iOS-Gerät in der Nähe zulassen.
- **iCloud-Synchronisierung für verwaltete Apps:** Synchronisierung verwalteter Apps mit iCloud zulassen.
- **Backup von Unternehmensbüchern:** Sicherung von Unternehmensbüchern in iCloud zulassen.
- **Synchronisieren von Notizen und Markierungen in Unternehmensbüchern:** Synchronisierung der von Benutzern in Unternehmensbüchern erstellten Anmerkungen und Markierungen mit iCloud zulassen.
- **Vertrauensstellung für Unternehmensapp:** Vertrauensstellung für Unternehmensapps zulassen. Unternehmensapps sind alle Apps, die für Ihre Organisation benutzerdefiniert sind. Sie können intern entwickelt sein oder bei einem externen Anbieter erworben werden. Weitere Informationen finden Sie unter Install custom enterprise apps on iOS.
- **Internetergebnisse in Spotlight:** Anzeige von Suchergebnissen aus dem Internet neben solchen vom Gerät in Spotlight zulassen.
- **Nicht verwaltete Apps lesen verwaltete Kontakte:** Optional. Nur verfügbar, wenn **Dokumente von verwalteten Apps in nicht verwalteten Apps** deaktiviert ist. Wenn diese Richtlinie aktiviert ist, können nicht verwaltete Apps Daten aus den Kontakten verwalteter Konten lesen. Die Standardeinstellung ist **Aus**. Verfügbar ab iOS 12.
- **Verwaltete Apps schreiben nicht verwaltete Kontakte:** Optional. Wenn diese Option aktiviert ist, dürfen verwaltete Apps Kontakte in Kontakte nicht verwalteter Konten schreiben. Wenn **Dokumente von verwalteten Apps in nicht verwalteten Apps** aktiviert ist, hat diese Einschränkung keine Auswirkungen. Die Standardeinstellung ist **Aus**. Verfügbar ab iOS 12.

- **Einstellungen nur für Betreute Geräte - Zulassen**

  Diese Einstellungen gelten nur für überwachte Geräte. 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.

  - **Alle Inhalte und Einstellungen löschen:** Löschen aller Inhalte und Einstellungen von den Geräten zulassen.
  - **Konfigurationsbeschränkungen:** Konfigurieren von Jugendschutzeinstellungen auf den Geräten zulassen.
  - **Podcasts:** Download und Synchronisierung von Podcasts zulassen.
  - **Installation von Konfigurationsprofilen:** Installation eines anderen Konfigurationsprofils als des von Ihnen bereitgestellten zulassen.

- **Fingerabdruckänderung:** Ändern und Löschen des Touch ID-Fingerabdrucks zulassen.
- **Installieren von Apps vom Gerät:** App-Installation durch Benutzer zulassen. Wenn Sie diese Einstellung deaktivieren, können Endbenutzer keine neuen Apps installieren. Der App Store ist deaktiviert und das zugehörige Symbol wird vom Homebildschirm entfernt.
- **Tastenkombinationen:** Erstellung benutzerdefinierter Tastenkombinationen für häufig verwendete Wörter und Sätze zulassen.
- **Gekoppelte Uhr:** Koppeln einer Apple Watch mit einem betreuten Gerät zulassen.
- **Passcodeänderung:** Passcodeänderung auf betreuten Geräten zulassen.
- **Gerätenamensänderung:** Gerätenamensänderung auf Geräten zulassen.
- **Hintergrundbildänderung:** Ändern des Hintergrundbilds auf Geräten zulassen.
- **Automatischer Download von Apps:** Herunterladen von Apps zulassen.
- **AirDrop:** Teilen von Fotos, Videos, Websites, Orten usw. mit nahegelegenen iOS-Geräten zulassen.
- **iMessage:** Verwenden von iMessage für den Versand von SMS über Wi-Fi zulassen.
- **Benutzergenerierte Inhalte in Siri:** Abfrage benutzergenerierter Inhalte vom Internet durch Siri zulassen. Verbraucher, keine Journalisten im eigentlichen Sinn, erstellen benutzergenerierte Inhalte. Inhalte auf Twitter oder Facebook sind beispielsweise benutzergeneriert.
- **iBooks:** Verwendung der iBooks-App zulassen.
- **Apps entfernen:** Entfernen von Apps von den Geräten zulassen.
- **Game Center:** Spielen von Onlinespielen über Game Center auf den Geräten zulassen.
  * **Freunde hinzufügen:** Senden von Aufforderungen an Freunde zum Spielen zulassen.
  * **Multiplayer-Gaming:** Starten eines Spiels mit mehreren Spielern auf Geräten zulassen.
- **Kontoeinstellungen bearbeiten:** Ändern der Gerätekontoeinstellungen zulassen.
- **Einstellungen für mobile Daten in App ändern:** Ändern der Verwendung mobiler Daten durch Apps zulassen.
- **Einstellungen für Freundesuche ändern:** Ändern der Einstellungen für "Find My Friends" zulassen.
- **Kopplung mit Nicht-Configurator-Hosts:** Festlegen des Zielgerätetyps für die Kopplung durch Administrator zulassen. Wenn Sie diese Einstellung deaktivieren, ist keine Kopplung möglich, es sei denn, auf dem überwachenden Host wird Apple Configurator ausgeführt. Ist kein Zertifikat für den überwachenden Host konfiguriert, ist die Kopplung gänzlich deaktiviert.

- **Tastaturvorhersage:** Verwendung der Tastatur mit Texterkennung zur Anzeige von Wortvorschlägen bei der Texteingabe zulassen. Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Benutzer Zugriff auf vorgeschlagene Wörter haben, etwa bei der Verarbeitung standardisierter Texte.
- **Tastatur mit Autokorrektur:** Verwendung der automatischen Korrektur bei der Texteingabe zulassen. Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Benutzer Zugriff auf korrigierte Wörter haben, etwa bei der Verarbeitung standardisierter Texte.
- **Tastatur mit Rechtschreibprüfung:** Verwendung der Rechtschreibprüfung bei der Texteingabe zulassen. Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Benutzer Zugriff auf die Rechtschreibprüfung haben, etwa bei der Verarbeitung standardisierter Texte.
- **Definition nachschlagen:** Verwendung der Funktion zum Nachschlagen von Definitionen bei der Texteingabe zulassen. Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Benutzer Zugriff auf Definitionen haben, etwa bei der Verarbeitung standardisierter Texte.
- **Einzelne App-Paket-ID:** Erstellen einer Liste von Apps, die die Kontrolle über das Gerät haben und eine Interaktion mit anderen Apps oder Funktionen verhindern.
  Um eine App hinzuzufügen, klicken Sie auf **Hinzufügen**, geben Sie einen **App-Namen** ein und klicken Sie auf **Speichern**. Wiederholen Sie diesen Vorgang für jede App, die Sie hinzufügen möchten.
- **News:** Verwendung der News-App zulassen.
- **Apple Music:** Verwendung von Apple Music zulassen. Wenn Sie Apple Music nicht zulassen, wird die Musik-App im klassischen Modus ausgeführt.
- **iTunes Radio:** Verwendung von iTunes Radio zulassen.
- **Benachrichtigungsänderung:** Änderung von Benachrichtigungseinstellungen durch Benutzer zulassen.
- **Eingeschränkte App-Verwendung:** Nutzung aller Apps bzw. Nutzung oder Nichtnutzung der Apps zulassen, basierend auf den bereitgestellten Paket-IDs. Gilt nur für betreute Geräte. Wenn Sie **Only allow some apps** auswählen, fügen Sie eine App mit der Paket-ID `com.apple.webapp` hinzu, um Webclips zuzulassen.

  > **Hinweis:**
  >
  > Ab iOS 11 führte Apple Änderungen an den Richtlinien ein, die für App-Einschränkungen verfügbar sind. Apple lässt nicht mehr zu, dass Sie den Zugriff auf die App "Einstellungen" und die App "Telefon" verweigern, indem Sie das entsprechende iOS-Anwendungspaket einschränken.

  Nach dem Blockieren von Apps durch Konfigurieren und Bereitstellen der Einschränkungsrichtlinie: Wenn Sie einige oder sämtliche dieser Apps zu einem späteren

Zeitpunkt zulassen möchten und die Einschränkungsrichtlinie entsprechend ändern und bereitstellen, ändert dies nicht die Einschränkungen. Die Änderungen werden in diesem Fall nicht auf das iOS-Profil angewendet. Entfernen Sie zunächst das iOS-Profil mit der Richtlinie zur Profilentfernung und stellen Sie anschließend die aktualisierte Geräteeinschränkungsrichtlinie bereit.

Wenn Sie diese Einstellung in **Nur einige Apps zulassen** ändern: Vor dem Bereitstellen dieser Richtlinie sollten Benutzer, die mit dem Apple-Bereitstellungsprogramm registrierte Geräte verwenden, sich über den Setupassistenten an ihrem Apple-Konto anmelden. Andernfalls müssen Benutzer möglicherweise die zweistufige Authentifizierung auf ihren Geräten deaktivieren, um die Anmeldung an ihrem Apple-Konto und den Zugriff auf zulässige Apps zu ermöglichen.

- **Änderung der Übermittlung von Diagnosedaten:** Änderung der Einstellungen zur Übermittlung von Diagnose- und App-Analysedaten auf der Seite **Einstellungen > Diagnose & Nutzungsdaten** durch die Benutzer zulassen.
- **Bluetooth-Änderung:** Änderung von Bluetooth-Einstellungen durch Benutzer zulassen.
- **Diktierfunktion zulassen:** nur betreute Geräte. Wenn diese Einschränkung auf **Aus** festgelegt ist, können weder die Diktierfunktion noch die Umwandlung von Sprache-in-Text verwendet werden. Die Standardeinstellung ist **Ein**.
- **Nur WiFi-Netzwerken beitreten, die von einer WiFi-Richtlinie installiert wurden:** optional verfügbar. Nur betreut. Wenn diese Einschränkung auf **Ein** festgelegt ist, kann ein Gerät nur dann auf ein Wi-Fi-Netzwerk zugreifen, wenn dieses über ein Konfigurationsprofil festgelegt wurde. Die Standardeinstellung ist **Aus**.
- **Classroom-App die Verwendung von AirPlay und Bildschirmansicht ohne Aufforderung ermöglichen:** Wenn diese Einschränkung ausgewählt ist, kann die Lehrkraft AirPlay und Bildschirmansichten ausführen, ohne dass der Lernende zur Erteilung einer entsprechenden Berechtigung aufgefordert wird. Die Einstellung ist standardmäßig deaktiviert. Für betreute iOS-Geräte.
- **Classroom-App das Sperren einer App und des Geräts ohne Aufforderung erlauben:** Wenn diese Einschränkung auf **Ein** festgelegt ist, ist das Sperren von Geräten auf eine App und das Sperren von Geräten ohne Aufforderung an die Benutzer möglich. Die Standardeinstellung ist **Aus**. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).
- **Automatische Teilnahme an Klassen der Classroom-App ohne Aufforderung:** Wenn diese Einschränkung auf **Ein** festgelegt ist, werden Benutzer automatisch und ohne Aufforderung Classroom-Klassen hinzugefügt. Die Standardeinstellung ist **Aus**. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).
- **AirPrint zulassen:** Wenn diese Einschränkung auf **Aus** festgelegt ist, können Benutzer nicht über AirPrint drucken. Die Standardeinstellung ist **Ein**. Wenn diese Einschränkung

auf **Ein** festgelegt ist, erscheinen die nachfolgend aufgeführten zusätzlichen Einschränkungen. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).

  * **Speichern von AirPrint-Anmeldeinformationen in Schlüsselbund zulassen:** Wenn diese Einschränkung deaktiviert ist, werden AirPrint-Benutzername und -Kennwort nicht im Schlüsselbund gespeichert. Die Einstellung ist standardmäßig aktiviert. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).
  * **Ermittlung von AirPrint-Druckern mit iBeacons zulassen:** Wenn diese Einschränkung deaktiviert ist, ist die iBeacon-Erkennung von AirPrint-Druckern deaktiviert. Dies verhindert ein Netzwerkverkehrs-Phishing durch gefälschte AirPrint-Bluetooth-Beacons. Die Einstellung ist standardmäßig aktiviert. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).
  * **AirPrint nur bei Zielen mit vertrauenswürdigen Zertifikaten zulassen:** Wenn diese Einschränkung aktiviert ist, können die Benutzer AirPrint nur für Ziele mit vertrauenswürdigen Zertifikaten verwenden. Die Einstellung ist standardmäßig deaktiviert. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).

- **Hinzufügen von VPN-Konfigurationen:** Wenn diese Einschränkung auf **Aus** festgelegt ist, können die Benutzer keine VPN-Konfigurationen erstellen. Die Standardeinstellung ist **Ein**. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).
- **Einstellungen für Mobilnetzabo ändern:** Wenn diese Einschränkung auf **Aus** festgelegt ist, können die Benutzer keine Mobilnetzabo-Einstellungen ändern. Die Standardeinstellung ist **Ein**. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).
- **System-Apps entfernen:** Wenn diese Einschränkung auf **Aus** festgelegt ist, können die Benutzer keine System-Apps von Geräten entfernen. Die Standardeinstellung ist **Ein**. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).
- **Einrichten neuer Geräte in der Nähe:** Wenn diese Einschränkung auf “Aus” festgelegt ist, können die Benutzer keine neuen Geräte in der Nähe einrichten. Die Standardeinstellung ist Ein. Für Geräte im betreuten Modus mit iOS 11 (Mindestversion).
- **Eingeschränkten USB-Modus zulassen:** Mit **Ein** kann das Gerät immer mit USB-Zubehör verbunden werden, solange es gesperrt ist. Die Standardeinstellung ist **Ein**. Nur verfügbar für betreute Geräte mit iOS 11.3 oder höher.
- **Verzögerte Softwareupdates erzwingen:** Mit **Ein** wird die Sichtbarkeit von Softwareupdates für Benutzer verzögert. Der Benutzer sieht ein Softwareupdate erst, nachdem die festgelegte Anzahl von Tagen seit Veröffentlichung des Softwareupdates verstrichen ist. Die Standardeinstellung ist **Aus**. Nur verfügbar für betreute Geräte mit iOS 11.3 oder höher.
- **Erzwungene Verzögerung für Softwareupdate(Tage):** Sie können eine Anzahl von Tagen angeben, um die ein Softwareupdate auf dem Gerät verzögert werden soll. Die

maximale Verzögerung ist **90** Tage. Die Standardeinstellung ist **30** Tage. Nur verfügbar für betreute Geräte mit iOS 11.3 oder höher.

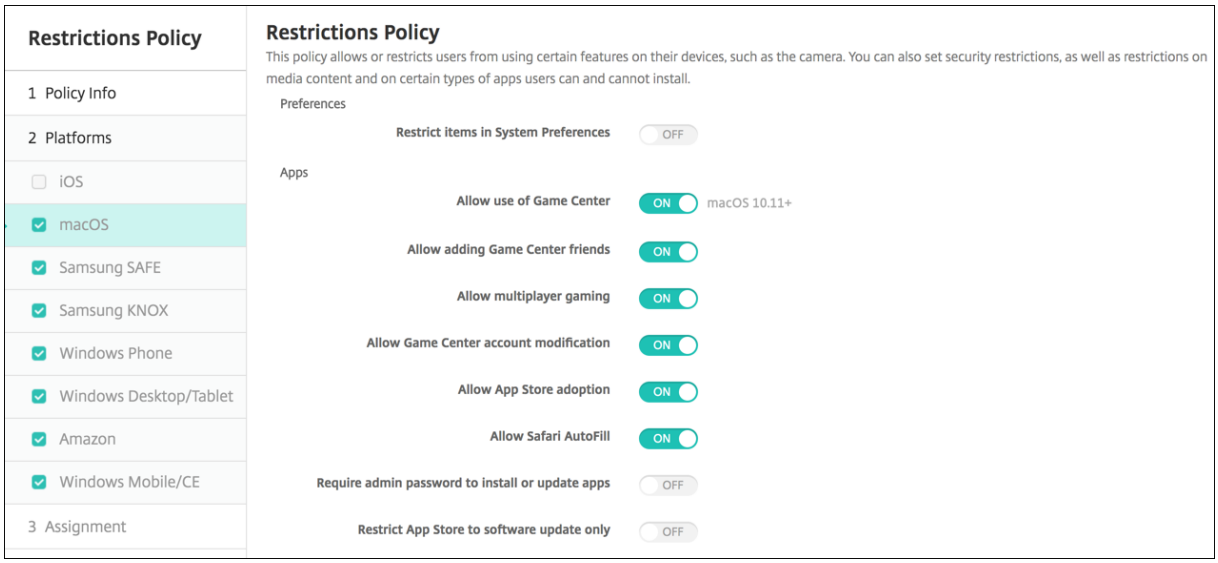
- **Um Erlaubnis zum Verlassen von Klassen fragen:** Mit **Ein** müssen Schüler, die in einem nicht verwalteten Kurs mit Classroom registriert sind, beim Verlassen des Kurses eine Genehmigung vom Lehrer anfordern. Die Standardeinstellung ist **Aus**. Nur verfügbar für betreute Geräte mit iOS 11.3 oder höher.
- **Automatisches Datum und Uhrzeit erzwingen:** Ermöglicht, Datum und Uhrzeit auf betreuten Geräten automatisch einzustellen. Mit **Ein** können die Gerätebenutzer **Automatisch einstellen** unter **Allgemein > Datum/Zeit** nicht deaktivieren. Die Zeitzone auf dem Gerät wird nur aktualisiert, wenn das Gerät den Standort ermitteln kann. Also, wenn ein Gerät eine Mobilfunkverbindung oder eine Wi-Fi-Verbindung hat und die Ortungsdienste aktiviert sind. Die Standardeinstellung ist **Aus**. Nur verfügbar für betreute Geräte mit iOS 12 oder höher.
- **Kennwörter autom. ausfüllen:** Optional. Wenn diese Option deaktiviert ist, können Benutzer die Funktionen zum automatischen Ausfüllen von Kennwörtern oder zum automatischen Erstellen starker Kennwörter nicht verwenden. Die Standardeinstellung ist **Ein**. Verfügbar ab iOS 12.
- **Kennwortanforderung bei Geräten in der Nähe:** Optional. Wenn die Option deaktiviert ist, fordern Benutzergeräte keine Kennwörter von Geräten in der Nähe an. Die Standardeinstellung ist **Ein**. Verfügbar ab iOS 12.
- **Kennwort teilen:** Optional. Wenn diese Option deaktiviert ist, können Benutzer ihre Kennwörter nicht per AirDrop teilen. Die Standardeinstellung ist **Ein**. Verfügbar ab iOS 12.

- **Sicherheit - Auf Sperrbildschirm anzeigen**
  - **Kontrollzentrum:** Zugriff auf das Kontrollzentrum auf dem Sperrbildschirm zulassen. Damit können Benutzer Einstellungen für Flugmodus, Wi-Fi, Bluetooth, den Nicht stören-Modus und die Ausrichtungssperre einfach ändern.
  - **Benachrichtigung:** Anzeige von Mitteilungen auf dem Sperrbildschirm zulassen.
  - **Heuteansicht:** Anzeige der Ansicht “Heute” mit Informationen wie Wetter und aktuelle Kalendereinträge auf dem Sperrbildschirm zulassen.
- **Medieninhalte - Zulassen**
  - **Anstößige Musik, Podcasts und iTunes U-Inhalte:** anstößige Inhalte auf den Geräten zulassen.
  - **Sexuelle Inhalte in iBooks:** Download freizügiger Inhalte aus iBooks zulassen.
  - **Bewertungsregion:** Region, aus der die Wertungen für den Jugendschutz abgerufen werden sollen. Klicken Sie in der Liste auf das gewünschte Land. Die Standardeinstellung ist **United States**.

  - **Filme:** Legen Sie fest, ob Filme auf den Geräten zugelassen werden sollen. Wenn Sie Filme zulassen, legen Sie optional die Wertungen für Filme fest. Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken von Filmen. Die Standardeinstellung ist “Alle Filme zulassen”.
  - **Fernsehsendungen:** Legen Sie fest, ob Fernsehsendungen auf den Geräten zugelassen werden sollen. Wenn Sie Fernsehsendungen zulassen, legen Sie optional die Wertungen für Fernsehsendungen fest. Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken von Fernsehsendungen. Die Standardeinstellung ist “Alle Fernsehsendungen zulassen”.
  - **Apps:** Legen Sie fest, ob Apps auf den Geräten zugelassen werden sollen. Wenn Sie Apps zulassen, legen Sie optional die Wertungen für Apps fest. Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken von Apps. Die Standardeinstellung ist “Alle Apps zulassen”.

- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur unter iOS 9.3 und höher verfügbar.

macOS-Einstellungen



- **Einstellungen**
  - **Elemente in den Systemeinstellungen beschränken:** Zugriff der Benutzer auf Systemeinstellungen zulassen oder beschränken. Die Standardeinstellung ist **Aus**, d. h. Benutzer haben vollen Zugriff auf Systemeinstellungen. Wenn Sie diese Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
    * Wählen Sie im **Systemeinstellungsbereich** aus, welche Einstellungen aktiviert bzw. deaktiviert werden sollen. Standardmäßig sind alle Einstellungen auf **Ein** festgelegt.
      - Benutzer & Gruppen
      - General
      - Bedienungshilfen
      - App Store
      - Softwareupdate
      - Bluetooth
      - CDs & DVDs
      - Datum & Uhrzeit
      - Desktop & Bildschirmschoner
      - Monitore
      - Dock
      - Energie sparen
      - Erweiterungen
      - FibreChannel
      - iCloud
      - Ink
      - Internetaccounts
      - Tastatur

- Sprache & Text
- Mission Control
- Maus
- Netzwerk
- Benachrichtigungen
- Kindersicherung
- Drucker & Scanner
- Profile
- Sicherheit und Datenschutz
- Freigeben
- Ton
- Diktat & Sprache
- Spotlight
- Startvolume
- Time Machine
- Trackpad
- Xsan

- **Apps**
  - **Game Center zulassen:** Spielen von Onlinespielen über Game Center zulassen Die Standardeinstellung ist **Ein**.
  - **Hinzufügen von Game Center-Freunden zulassen:** Senden von Aufforderungen an Freunde zum Spielen zulassen. Die Standardeinstellung ist **Ein**.
  - **Multiplayer-Gaming zulassen:** Starten eines Spiels mit mehreren Spielern auf Geräten zulassen. Die Standardeinstellung ist **Ein**.
  - **Game Center-Kontoänderung zulassen:** Zulassen, dass Benutzer ihre Game Center-Kontoeinstellungen ändern. Die Standardeinstellung ist **Ein**.
  - **Übernahme in App Store zulassen:** Übernahme in OS X vorhandener Apps in den App-Store zulassen bzw. beschränken. Die Standardeinstellung ist **Ein**.
  - **Autom. ausfüllen in Safari zulassen:** Automatisches Ausfüllen von Onlineformularfeldern mit gespeicherten Kennwörtern, Adressen und anderen grundlegenden Informationen zulassen. Die Standardeinstellung ist **Ein**.
  - **Admin-Kennwort zum Installieren oder Aktualisieren von Apps erforderlich:** Festlegen, dass zum Installieren oder Aktualisieren von Apps ein Administratorkennwort eingegeben werden muss. Die Standardeinstellung ist **Aus**, d. h. kein Administratorkennwort ist erforderlich.
  - **App Store auf Softwareaktualisierungen beschränken:** App Store auf Updates beschränken, d. h. alle Registerkarten im App Store mit Ausnahme von “Updates” sind deaktiviert. Die Standardeinstellung ist **Aus**, d. h. der Vollzugriff auf den App Store wird zugelassen.

  - **Öffnen von Apps beschränken:** Festlegen, welche Apps die Benutzer verwenden können. Die Standardeinstellung ist AUS, d. h. alle Apps können verwendet werden. Wenn Sie diese Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
    * **Zulässige Apps:** Klicken Sie auf **Hinzufügen**, geben Sie den Namen und die Paket-ID einer App ein, deren Start zugelassen werden soll, und klicken Sie dann auf **Speichern**. Wiederholen Sie diese Schritte für jede App, deren Öffnung zugelassen werden soll.
    * **Unzulässige Ordner:** Klicken Sie auf **Hinzufügen**, geben Sie den Pfad zu dem Ordner ein, auf den Benutzer keinen Zugriff haben sollen (z. B. /Applications/Utilities), und klicken Sie auf **Speichern**. Wiederholen Sie diese Schritte für alle Ordner, auf die die Benutzer keinen Zugriff erhalten sollen.
    * **Zulässige Ordner:** Klicken Sie auf **Hinzufügen**, geben Sie den Pfad zu dem Ordner ein, auf den Benutzer Zugriff haben sollen (z. B. /Applications/Utilities), und klicken Sie auf **Speichern**. Wiederholen Sie diese Schritte für alle Ordner, auf die die Benutzer Zugriff erhalten sollen.
- **Widgets**
  - **Nur die folgenden Dashboard-Widgets ausführen:** Ausführung von Dashboard-Widgets, wie Weltuhr oder Rechner zulassen oder beschränken. Die Standardeinstellung ist **Aus**, d. h. Benutzer haben vollen Zugriff auf alle Widgets. Wenn Sie diese Option aktivieren, konfigurieren Sie die folgende Einstellung:
    * **Zulässige Widgets:** Klicken Sie auf **Hinzufügen**, geben Sie den Namen und die ID eines Widgets ein, dessen Ausführung Sie zulassen möchten, und klicken Sie auf **Speichern**. Wiederholen Sie diesen Schritt für jedes Widget, dessen Ausführung Sie zulassen möchten.
- **Medien**
  - **AirDrop zulassen:** Teilen von Fotos, Videos, Websites, Orten usw. mit nahegelegenen iOS-Geräten zulassen.
- **Freigeben**
  - **Neue Freigabedienste automatisch aktivieren:** Wählen Sie aus, ob Freigabedienste automatisch aktiviert werden sollen.
  - **E-Mail:** Wählen Sie aus, ob gemeinsam genutzte Postfächer zulässig sein sollen.
  - **Facebook:** Wählen Sie aus, ob gemeinsam genutzte Facebook-Konten zulässig sein sollen.
  - **Videodienste - Flickr, Vimeo, Tudou und Youku:** Wählen Sie aus, ob gemeinsam genutzte Videodienste zulässig sein sollen.
  - **Zu Aperture hinzufügen:** Wählen Sie aus, ob das gemeinsame Hinzufügen zu Aperture zulässig sein soll.
  - **Sina Weibo:** Wählen Sie aus, ob gemeinsam genutzte Sina Weibo-Mikroblogging-Konten zulässig sein sollen.
  - **Twitter:** Wählen Sie aus, ob gemeinsam genutzte Twitter-Konten zulässig sein sollen.

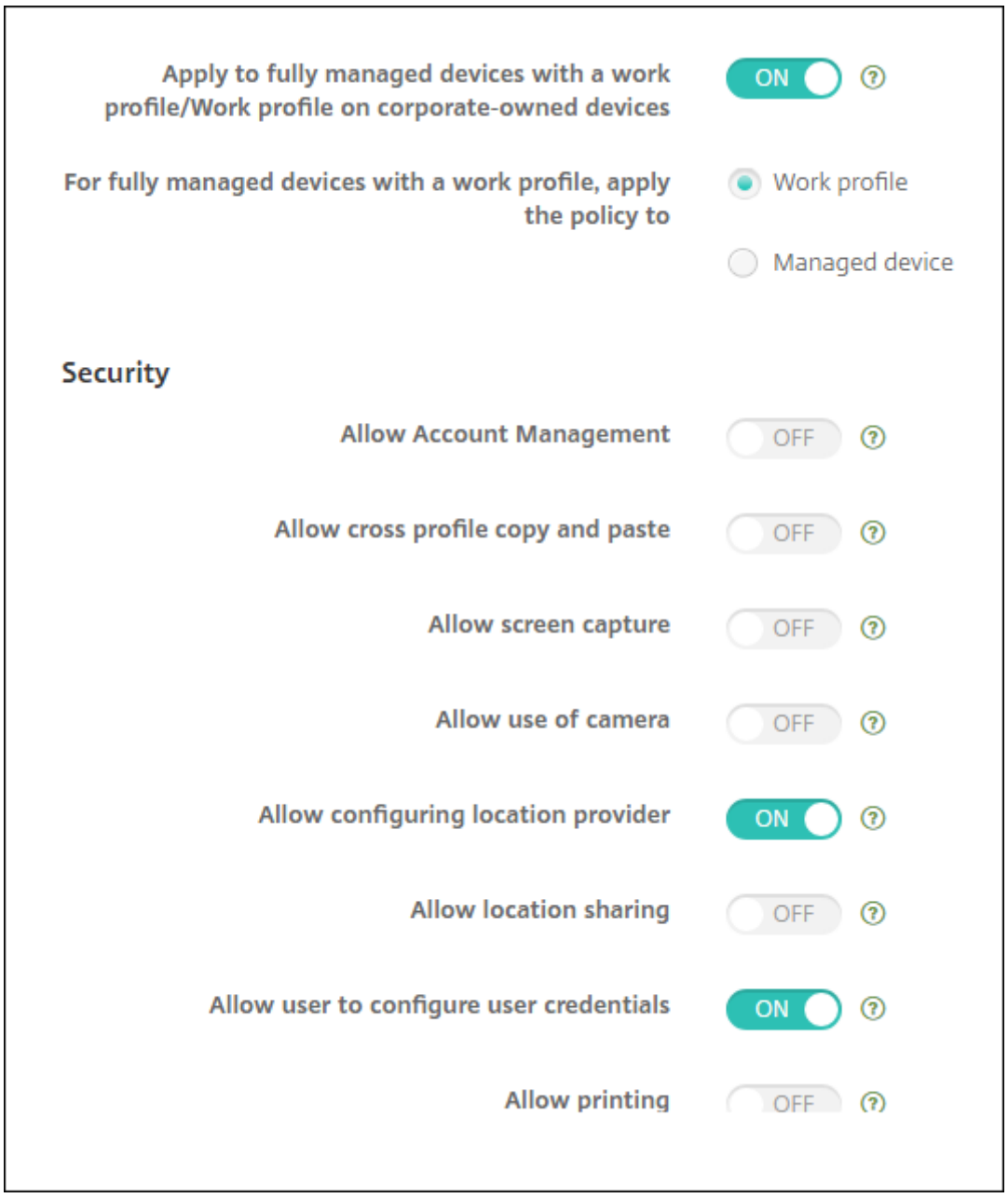
  - **Nachrichten:** Wählen Sie aus, ob der gemeinsame Zugriff auf Nachrichten zulässig sein soll.
  - **Zu iPhoto hinzufügen:** Wählen Sie aus, ob das gemeinsame Hinzufügen zu iPhoto zulässig sein soll.
  - **Zu Leseliste hinzufügen:** Wählen Sie aus, ob das gemeinsame Hinzufügen zu Leselisten zulässig sein soll.
  - **AirDrop:** Wählen Sie aus, ob gemeinsam genutzte AirDrop-Konten zulässig sein sollen.
- **Funktionalität**
  - **Desktopbild sperren:** Wählen Sie aus, ob Benutzern das Ändern des Desktopbilds gestattet werden soll. Die Standardeinstellung ist **Aus**, d. h. Benutzer können das Desktopbild ändern.
  - **Verwendung der Kamera zulassen:** Wählen Sie aus, ob Benutzern die Verwendung der Kamera auf Macs gestattet werden soll. Die Standardeinstellung ist **Aus**, d. h. die Benutzer können die Kamera nicht verwenden.
  - **Apple Music-Dienst:** Verwendung des Apple Music-Diensts zulassen (macOS 10.12 und höher). Wenn Sie Apple Music nicht zulassen, wird die Musik-App im klassischen Modus ausgeführt. Gilt nur für betreute Geräte. Die Standardeinstellung ist **Ein**.
  - **Spotlight-Vorschläge zulassen:** Wählen Sie aus, ob Benutzern die Verwendung von Spotlight-Vorschlägen für die Suche auf ihrem Macintosh-Computer aus Internet, iTunes und App-Store gestattet sein soll. Die Standardeinstellung ist **Aus**, d. h. die Benutzer können keine Spotlight-Vorschläge verwenden.
  - **Look Up zulassen:** Wählen Sie aus, ob Benutzern das Nachschlagen der Definition von Wörtern über das Kontextmenü oder das Spotlight-Suchmenü gestattet sein soll. Die Standardeinstellung ist “AUS”, d. h. die Benutzer können LookUp auf ihrem Macintosh-Computer nicht verwenden.
  - **iCloud-Kennwort für lokale Konten verwenden:** Wählen Sie aus, ob Benutzern die Anmeldung bei ihrem Macintosh-Computer mit ihrer Apple-ID und dem iCloud-Kennwort gestattet sein soll. Wenn Sie diese Richtlinie aktivieren, können sich Benutzer auf dem Macintosh-Computer bei *allen* Anmeldebildschirmen mit denselben Anmeldeinformationen anmelden. Die Standardeinstellung ist **Ein**, d. h. die Benutzer können für den Zugriff auf ihre Macintosh-Computer ihre Apple-ID und ihr iCloud-Kennwort verwenden.
  - **iCloud-Dokumente & Daten zulassen:** Wählen Sie aus, ob Benutzern der Zugriff auf Dokumente und Daten in der iCloud von ihrem Macintosh-Computer aus gestattet werden soll. Die Standardeinstellung ist **Aus**, d. h. die Benutzer können von ihrem Macintosh-Computer aus nicht auf iCloud-Daten zugreifen.
    - **iCloud-Desktop und -Dokumente zulassen:** (macOS 10.12.4 und höher) standardmäßig aktiviert.
  - **iCloud-Schlüsselbundsynchronisierung zulassen:** iCloud-Schlüsselbundsynchronisierung zulassen (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.

- **iCloud Mail zulassen:** Verwendung von iCloud Mail zulassen (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.
- **iCloud-Kontakte zulassen:** Verwendung von iCloud-Kontakten zulassen (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.
- **iCloud-Kalender zulassen:** Verwendung von iCloud-Kalendern zulassen (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.
- **iCloud-Erinnerungen zulassen:** Verwendung von iCloud-Erinnerungen zulassen (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.
- **iCloud-Lesezeichen zulassen:** Synchronisierung mit iCloud-Lesezeichen zulassen (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.
- **iCloud-Notizen zulassen:** Verwendung von iCloud-Notizen zulassen (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.
- **iCloud-Fotos zulassen:** Wenn Sie diese Option auf **Aus** festlegen, werden sämtliche nicht vollständig heruntergeladenen iCloud Photo Library-Fotos aus dem lokalen Gerätespeicher gelöscht (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.
- **Automatisches Entsperren zulassen:** Informationen über diese Option und Apple Watch finden Sie unter https://www.imore.com/auto-unlock (macOS 10.12 und höher). Die Standardeinstellung ist **Ein**.
- **Entsperren des Macs durch Touch ID zulassen:** (macOS 10.12.4 und höher). Die Standardeinstellung ist **Ein**.
- **Verzögerte Softwareupdates erzwingen:** Mit **Ein** wird die Sichtbarkeit von Softwareupdates für Benutzer verzögert. Der Benutzer sieht ein Softwareupdate erst, nachdem die festgelegte Anzahl von Tagen seit Veröffentlichung des Softwareupdates verstrichen ist. Die Standardeinstellung ist **Aus**. Nur für überwachte Geräte verfügbar, auf denen macOS 10.13.4 und höher ausgeführt wird.
- **Erzwungene Verzögerung für Softwareupdate(Tage):** gibt an, um wie viele Tage ein Softwareupdate auf dem Gerät verzögert werden soll. Das Maximum ist 90 Tage. Die Standardeinstellung ist **30**. Nur für überwachte Geräte verfügbar, auf denen macOS 10.13.4 und höher ausgeführt wird.
- **Kennwörter autom. ausfüllen:** Optional. Wenn diese Option deaktiviert ist, können Benutzer die Funktionen zum automatischen Ausfüllen von Kennwörtern oder zum automatischen Erstellen starker Kennwörter nicht verwenden. Die Standardeinstellung ist **Ein**. Verfügbar ab macOS 10.14.
- **Kennwortanforderung bei Geräten in der Nähe:** Optional. Wenn die Option deaktiviert ist, fordern Benutzergeräte keine Kennwörter von Geräten in der Nähe an. Die Standardeinstellung ist **Ein**. Verfügbar ab macOS 10.14.
- **Kennwort teilen:** Optional. Wenn diese Option deaktiviert ist, können Benutzer ihre Kennwörter nicht per AirDrop teilen. Die Standardeinstellung ist **Ein**. Verfügbar ab macOS 10.14.

Android-Einstellungen

- **Kamera:** Verwendung der Kamera von Geräten zulassen. Bei Auswahl von **Aus** ist die Kamera deaktiviert. Die Standardeinstellung ist **Ein**.

Android Enterprise-Einstellungen



Wenn ein neues oder auf die Werkseinstellungen zurückgesetztes Android-Gerät im Arbeitsprofilmodus registriert wird, werden Geräte mit Android 8.0-10.x als vollständig verwaltetes Gerät mit einem Arbeitsprofil registriert. Geräte ab Android 11 werden als Arbeitsprofil auf unternehmen-

seigenem Gerät registriert. Die Einschränkungsrichtlinie kann entweder auf das Arbeitsprofil auf dem Gerät oder auf das verwaltete Gerät angewendet werden.

Auf Geräten, die im Modus “Arbeitsprofil auf unternehmenseigenem Gerät” registriert sind, sind die folgenden Einschränkungen nur für das Arbeitsprofil verfügbar:

- Backupdienst zulassen
- Aktivieren von System-Apps
- Verhindern, dass Keyguard das Gerät sperrt
- Verwendung der Statusleiste zulassen
- Gerätebildschirm eingeschaltet lassen
- Benutzersteuerung der Anwendungseinstellungen zulassen
- Benutzer darf Benutzeranmeldeinformationen konfigurieren
- VPN-Konfiguration zulassen
- USB-Massenspeicher zulassen
- Zurücksetzen auf Werkseinstellungen zulassen
- App-Deinstallation zulassen
- Nicht-Google Play-Apps zulassen
- Kopieren und Einfügen zwischen Profilen zulässig
- App-Verifizierung aktivieren
- Kontoverwaltung zulassen
- Drucken zulassen
- NFC zulassen
- Hinzufügen von Benutzern zulassen

Standardmäßig sind die Einstellungen **USB-Debugging und Unbekannte Quellen** auf einem Gerät deaktiviert, wenn es bei Android Enterprise im Arbeitsprofilmodus registriert ist.

Konfigurieren Sie für Geräte mit Android 8.0-10.x und Samsung Knox 3.0 und höher die Einstellungen für Samsung Knox und Samsung SAFE auf der Seite **Android Enterprise**. Verwenden Sie für Geräte, auf denen frühere Versionen von Android oder Samsung Knox ausgeführt werden, die Seiten **Samsung Knox** und **Samsung SAFE**.

Samsung-Einschränkungen gelten nicht für Geräte, die im Modus “Arbeitsprofil auf unternehmenseigenem Gerät” registriert sind. Verwenden Sie das Knox-Service-Plug-In (KSP), um Samsung-Einschränkungen auf diese Geräte anzuwenden. Weitere Informationen finden Sie in der Samsung-Dokumentation.

Wir empfehlen, für die neuesten Samsung Knox-Verwaltungsfunktionen Samsung Knox 3.4 oder höher zu verwenden.

- **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil bzw. Arbeitsprofil auf unternehmenseigenen Geräten anwenden:** Ermöglicht das Konfigurieren von Einstellungen für die Einschränkungsrichtlinie für vollständig verwaltete Geräte mit Arbeitsprofil. Bei der

Einstellung **Ein** wählen Sie eine der folgenden Optionen:

- **Arbeitsprofil:** Die konfigurierten Einschränkungen gelten nur für das Arbeitsprofil auf dem Gerät.
- **Verwaltetes Gerät:** Die konfigurierten Einschränkungen gelten nur für das Gerät.

Bei der Einstellung **Aus** gelten die konfigurierten Einstellungen für Anmeldeinformationen nur für das Gerät, mit Ausnahme der Einschränkungen, die explizit für das Arbeitsprofil gelten. Die Standardeinstellung ist **Aus**.

Wenn **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil bzw. Arbeitsprofil auf unternehmenseigenen Geräten anwenden** deaktiviert ist, konfigurieren Sie die diese Einstellungen:

- **Sicherheit**
  - **Kontoverwaltung zulassen:** Ermöglicht die Kontenverwaltung im Arbeitsprofil und auf verwalteten Geräten. Die Standardeinstellung ist **Aus**.
  - **Kopieren und Einfügen zwischen Profilen zulässig:** Bei Auswahl von **Ein** können Benutzer die Zwischenablage zum Kopieren und Einfügen zwischen Apps im Android Enterprise-Profil und Apps im privaten Bereich verwenden. Die Standardeinstellung ist **Aus**.
  - **Screenshot zulassen:** Ermöglicht Benutzern, einen Screenshot des Gerätebildschirms zu machen. Die Standardeinstellung ist **Aus**.
  - **Verwendung der Kamera zulassen:** Ermöglicht Benutzern, Bilder und Videos mit der Gerätekamera aufzunehmen. Die Standardeinstellung ist **Aus**.
  - **VPN-Konfiguration zulassen:** Ermöglicht Benutzern das Erstellen von VPN-Konfigurationen. Für Geräte im Arbeitsprofilmodus mit Android 6 und höher und für vollständig verwaltete Geräte. Die Standardeinstellung ist **Ein**.
  - **Backupdienst zulassen:** Ermöglicht Benutzern die Sicherung von Anwendungs- und Systemdaten auf den Geräten. Die Standardeinstellung ist **Ein**.
  - **NFC zulassen:** Ermöglicht Benutzern das Senden von Webseiten, Fotos, Videos oder anderen Inhalten an andere Geräte über NFC. Für MDM 4.0 und höher. Die Standardeinstellung ist **Ein**.
  - **Konfigurieren von Standortermittlung zulassen:** Ermöglicht Benutzern, GPS auf ihren Geräten einzuschalten. Für Android API 28 und höher. Die Standardeinstellung ist **Ein**.
  - **Standortfreigabe zulassen:** Bei verwalteten Profilen kann der Gerätebesitzer diese Einstellung außer Kraft setzen. Die Standardeinstellung ist **Aus**.

    > **Tipp:**
    >
    > Mit einer Standortrichtlinie können Sie in XenMobile geografische Grenzen festlegen.

> Weitere Informationen finden Sie unter Standortrichtlinie für Geräte.

- **Benutzer darf Benutzeranmeldeinformationen konfigurieren:** Geben Sie an, ob Benutzer Anmeldeinformationen im verwalteten Schlüsselspeicher konfigurieren dürfen. Die Standardeinstellung ist **Ein**.
- **Drucken zulassen:** Wenn diese Option auf **Ein** festgelegt ist, können Benutzer jeden Drucker verwenden, auf den ihr Gerät Zugriff hat. Die Standardeinstellung ist **Aus**. Verfügbar ab Android 9.
- **USB-Debugging zulassen:** Der Standardwert ist **Aus**.

- **Apps**
  - **System-Apps aktivieren:** Ermöglicht Benutzern das Ausführen vorinstallierter Geräteapps. Die Standardeinstellung ist **Aus**. Um bestimmte Apps zu aktivieren, klicken Sie in der Tabelle **Liste der System-Apps** auf **Hinzufügen**.
    - **Liste der System-Apps:** Eine Liste der System-Apps, die Sie auf dem Gerät aktivieren möchten. Wählen Sie für **System-Apps aktivieren** die Einstellung **Ein** und fügen Sie den App-Paketnamen hinzu. Um den Paketnamen für eine System-App zu suchen, können Sie mit der Android Debug Bridge (`adb`) den Android-Paketmanager (`pm`)-Befehl aufrufen. Beispielsweise `adb shell "pm list packages -f name"`, wobei "name" Teil des Paketnamens ist. Weitere Informationen finden Sie unter https://developer.android.com/studio/command-line/adb. Für Android Enterprise-Geräte können Sie die App-Berechtigungen über die Richtlinie App-Berechtigungen für Android Enterprise einschränken.
  - **Anwendungen deaktivieren:** Sperrt die Apps auf einer definierten Liste, sodass sie nicht ausgeführt werden können. Die Standardeinstellung ist **Aus**. Zum Deaktivieren einer installierten App ändern Sie die Einstellung auf **Ein** und klicken Sie in der Tabelle **Anwendungsliste** auf **Hinzufügen**.
    - **Anwendungsliste:** Liste der Apps, die Sie blockieren möchten. Legen Sie **Anwendungen deaktivieren** auf **Ein** fest und fügen Sie die App hinzu. Geben Sie den Namen des App-Pakets ein. Durch Ändern und Bereitstellen einer App-Liste wird die vorherige App-Liste überschrieben. Wenn Sie beispielsweise com.example1 und com.example2 deaktivieren und später die Liste in com.example1 und com.example3 ändern, wird com.example.2 in XenMobile aktiviert.
  - **App-Verifizierung aktivieren:** Ermöglicht dem Betriebssystem die Überprüfung von Apps auf schädliches Verhalten. Die Standardeinstellung ist **Ein**.
  - **Google Apps aktivieren:** Ermöglicht Benutzern das Herunterladen von Apps von Google Mobile Services auf das Gerät. Die Standardeinstellung ist **Ein**.
  - **App nicht aus Google Play zulassen:** Installation von Apps aus einem anderen Store als Google Play zulassen. Die Standardeinstellung ist **Aus**.
  - **Benutzersteuerung der Anwendungseinstellungen zulassen:** Ermöglicht Benutzern

das Deinstallieren und Deaktivieren einer App, das Leeren des Cache und das Löschen von Daten, das erzwungene Anhalten einer App und das Löschen der Standardeinstellungen. Die Benutzer führen diese Aktionen über die Einstellungs-App aus. Die Standardeinstellung ist **Aus**.

- **App-Deinstallation zulassen:** Ermöglicht Benutzern die Deinstallation von Apps aus dem verwalteten Google Play Store. Die Standardeinstellung ist **Aus**. Um diese Einstellung anzuzeigen, aktivieren Sie die Servereigenschaft `afw.restriction.policy.v2`. Weitere Informationen zu Servereigenschaften finden Sie unter Servereigenschaften.

- **BYOD-Arbeitsprofil**
  - **App-Widgets für Arbeitsprofil auf dem Startbildschirm zulassen:** Wenn für diese Einstellung **Ein** festgelegt ist, können Benutzer Arbeitsprofil-App-Widgets auf dem Startbildschirm des Geräts platzieren. Wenn für diese Einstellung **Aus** festgelegt ist, können Benutzer keine Arbeitsprofil-App-Widgets auf dem Startbildschirm des Geräts platzieren. Die Standardeinstellung ist **Aus**.
    - **Apps mit zulässigen Widgets:** Eine Liste der Apps, die Sie auf dem Startbildschirm zulassen möchten. Wählen Sie für **App-Widgets für Arbeitsprofil auf dem Startbildschirm zulassen** die Einstellung **Ein** und fügen Sie die App hinzu. Klicken Sie auf **Hinzufügen** und wählen Sie in der Liste die App, deren Widgets Sie auf dem Homebildschirm zulassen möchten. Klicken Sie auf **Speichern**. Wiederholen Sie diesen Vorgang, um weitere App-Widgets zuzulassen.
  - **Kontakte des Firmenprofils in Gerätekontakten zulassen:** Zeigt Kontakte aus dem verwalteten Android Enterprise-Profil im übergeordneten Profil für eingehende Anrufe an (Android 7.0 und höher). Die Standardeinstellung ist **Aus**.

- **Nur vollständig verwaltetes Gerät**
  - **Hinzufügen von Benutzern zulassen:** Ermöglicht Benutzern das Hinzufügen neuer Benutzer auf einem Gerät. Die Standardeinstellung ist **Ein**.
  - **Datenroaming zulassen:** Ermöglicht Benutzern die Verwendung mobiler Daten beim Roaming. Die Standardeinstellung ist “Aus”, d. h. Roaming ist auf den Geräten deaktiviert. Die Standardeinstellung ist **Aus**.
  - **SMS zulassen:** Ermöglicht Benutzern das Senden und Empfangen von SMS-Nachrichten. Die Standardeinstellung ist **Aus**.
  - **Verwendung der Statusleiste zulassen:** Wenn diese Einstellung auf **Ein** gesetzt ist, aktiviert sie die Statusleiste auf verwalteten und dedizierten Geräten (“COSU-Geräte”). Diese Einstellung deaktiviert Benachrichtigungen, Schnelleinstellungen und andere Bildschirmüberlagerungen, die das Ausschalten des Vollbildmodus ermöglichen. Die Benutzer können Benachrichtigungen in den Systemeinstellungen anzeigen. Für Android 6.0 und höher. Die Standardeinstellung ist **Aus**.
  - **Bluetooth zulassen:** Ermöglicht Benutzern die Verwendung von Bluetooth. Die Standard-

einstellung ist **Ein**.

  * **Bluetooth-Freigabe zulassen:** Wenn diese Option deaktiviert ist, können Benutzer keine ausgehende Bluetooth-Freigabe auf ihrem Gerät einrichten. Die Option ist standardmäßig aktiviert. Um diese Einstellung anzuzeigen, aktivieren Sie die Servereigenschaft `afw.restriction.policy.v2`. Weitere Informationen zu Servereigenschaften finden Sie unter Servereigenschaften.

- **Konfigurieren von Datum und Uhrzeit zulassen:** Ermöglicht Benutzern das Ändern von Datum und Uhrzeit auf ihren Geräten. Die Standardeinstellung ist **Ein**.
- **Zurücksetzen auf Werkseinstellungen zulassen:** Ermöglicht Benutzern das Zurücksetzen der Geräte auf die werkseitige Voreinstellung. Die Standardeinstellung ist **Ein**.
- **Gerätebildschirm eingeschaltet lassen:** Wenn diese Einstellung auf **Ein** festgelegt ist, bleibt der Gerätebildschirm eingeschaltet, solange das Gerät am Stromnetz angeschlossen ist. Die Standardeinstellung ist **Aus**.
- **USB-Massenspeicher zulassen:** Übertragung großer Datendateien zwischen Benutzergeräten und einem Computer über eine USB-Verbindung zulassen. Die Standardeinstellung ist **Ein**.
- **Mikrofon zulassen:** Ermöglicht Benutzern die Verwendung des Gerätemikrofons. Die Standardeinstellung ist **Ein**.
- **Tethering zulassen:** Ermöglicht Benutzern das Konfigurieren mobiler Hotspots und das Tethering von Daten. Die Standardeinstellung ist **Aus**.
- **Verhindern, dass der Tastenschutz das Gerät sperrt:** Wird diese Einstellung auf **Ein** festgelegt, deaktiviert sie den Tastenschutz des Sperrbildschirms auf verwalteten und dedizierten Geräten (“COSU-Geräte”). Die Standardeinstellung ist **Aus**.
- **Wi-Fi-Änderungen zulassen:** Wenn diese Option auf **Ein** festgelegt ist, können die Benutzer das Wi-Fi ein- und ausschalten und eine Verbindung mit Wi-Fi-Netzwerken herstellen. Die Standardeinstellung ist **Ein**.
- **Dateiübertragung zulassen:** Ermöglicht Dateiübertragungen über USB. Die Standardeinstellung ist **Aus**.

- **Samsung**

  - **TIMA-Schlüsselspeicher aktivieren:** Der TIMA-Schlüsselspeicher bietet einen TrustZone-basierten, sicheren Speicher für symmetrische Schlüssel. RSA-Schlüsselpaare und -Zertifikate werden zur Speicherung an den Standard-Schlüsselspeicheranbieter geleitet. Die Standardeinstellung ist **Aus**.
  - **Freigabeliste zulassen:** Ermöglicht Benutzern das Teilen von Inhalten zwischen Apps in der Liste “Freigeben über”. Die Standardeinstellung ist **Ein**.
  - **Überwachungsprotokoll aktivieren:** Erstellen von Ereignisüberwachungsprotokollen für die forensische Analyse von Geräten aktivieren. Die Standardeinstellung ist **Aus**.

- **Samsung: Nur vollständig verwaltetes Gerät**

- **Überprüfung von ODE vertrauenswürdigem Start aktivieren:** Verwenden der ODE-Prüfung auf vertrauenswürdigen Start zur Erstellung einer Vertrauenskette zwischen Bootloader und Systemimage. Die Standardeinstellung ist **Ein**.
- **Nur Notruf zulassen:** Ermöglicht Benutzern das Aktivieren des Modus "Nur Notruf" auf den Geräten. Die Standardeinstellung ist **Aus**.
- **Firmwarewiederherstellung zulassen:** Ermöglicht Benutzern das Wiederherstellen der Firmware auf den Geräten. Die Standardeinstellung ist **Ein**.
- **Schnelle Verschlüsselung zulassen:** Ausschließliche Verschlüsselung des verwendeten Speicherplatzes zulassen. Diese Verschlüsselung ist die Alternative zur vollständigen Datenträgerverschlüsselung, bei der alle Daten verschlüsselt werden. Zu diesen Daten gehören Einstellungen, Anwendungsdaten, heruntergeladene Dateien und Anwendungen, Medien und Dateien anderer Art. Die Standardeinstellung ist **Ein**.
- **Common Criteria-Modus aktivieren:** Schalten von Geräten in den Common Criteria-Modus. Die Common Criteria-Konfiguration erzwingt strenge Sicherheitsvorgänge. Die Standardeinstellung ist **Ein**.
- **Neustartbanner aktivieren:** Beim Geräteneustart eine Benachrichtigung oder ein Banner über die vom Department of Defense genehmigte Systemnutzung anzeigen. Die Standardeinstellung ist **Aus**.
- **Einstellungsänderungen zulassen:** Ermöglicht Benutzern das Ändern von Einstellungen auf ihren vollständig verwalteten Geräten. Die Standardeinstellung ist **Ein**.
- **Datennutzung im Hintergrund aktivieren:** Datensynchronisierung im Hintergrund für Apps zulassen. Für vollständig verwaltete Geräte. Die Standardeinstellung ist **Ein**.
- **Zwischenablage zulassen:** Kopieren von Daten in die Zwischenablage von Geräten zulassen.
  - **Freigeben der Zwischenablage zulassen:** Teilen von Inhalten in der Zwischenablage zwischen Geräten und Computern zulassen (MDM 4.0 und höher).
- **Hometaste zulassen:** Ermöglicht Benutzern die Verwendung der **Hometaste** auf vollständig verwalteten Geräten. Die Standardeinstellung ist **Ein**.
- **Vorgegebenen Standort zulassen:** Ermöglicht Benutzern das Vortäuschen eines GPS-Standorts. Für vollständig verwaltete Geräte. Die Standardeinstellung ist **Aus**.
- **NFC:** Ermöglicht Benutzern die Verwendung von NFC auf vollständig verwalteten Geräten (MDM 3.0 und höher). Die Standardeinstellung ist **Ein**.
- **Ausschalten zulassen:** Ermöglicht Benutzern das Ausschalten von vollständig verwalteten Geräten (MDM 3.0 und höher). Die Standardeinstellung ist **Ein**.
- **Wi-Fi direkt zulassen:** Ermöglicht Benutzern die direkte Verbindung mit einem anderen Gerät über ihre Wi-Fi-Verbindung. Die Standardeinstellung ist **Ein**. Bei der Einstellung **Ein** müssen Sie die Einstellung **Wi-Fi-Änderungen zulassen** aktivieren.
- **SD-Karte zulassen:** Ermöglicht Benutzern die Verwendung einer SD-Karte (sofern verfügbar) für die Geräte. Die Standardeinstellung ist **Ein**.

- **USB-Hostspeicher zulassen:** Verwendung der Geräte als USB-Host bei Verbindung eines USB-Geräts mit den Geräten zulassen. Die Geräte müssen hierbei USB-Geräte mit Strom versorgen. Die Standardeinstellung ist **Ein**.
- **Sprachwahl zulassen:** Ermöglicht Benutzern die Verwendung der Sprachwahl auf den Geräten (MDM 4.0 und höher). Die Standardeinstellung ist **Ein**.
- **S Beam zulassen:** Ermöglicht Benutzern das Teilen von Inhalten über NFC und Wi-Fi Direct (MDM 4.0 und höher). Die Standardeinstellung ist **Ein**.
- **S Voice zulassen:** Ermöglicht Benutzern die Verwendung des intelligenten persönlichen Assistenten und Wissensnavigators auf Geräten (MDM 4.0 und höher). Die Standardeinstellung ist **Ein**.
- **USB-Tethering zulassen:** Ermöglicht Benutzern die gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die USB-Verbindung des Geräts. Die Standardeinstellung ist **Aus**. Wenn die Einstellung auf **Ein** festgelegt wird, muss auch die Einstellung **Tethering zulassen** auf **Ein** festgelegt werden.
- **Bluetooth-Tethering zulassen:** gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die Bluetooth-Verbindung des Geräts zulassen. Die Standardeinstellung ist **Aus**. Wenn die Einstellung auf **Ein** festgelegt wird, muss auch die Einstellung **Tethering zulassen** auf **Ein** festgelegt werden.
  * **Bluetooth-Freigabe zulassen:** Wenn diese Option deaktiviert ist, können Benutzer keine ausgehende Bluetooth-Freigabe auf ihrem Gerät einrichten. Die Option ist standardmäßig aktiviert. Um diese Einstellung anzuzeigen, aktivieren Sie die Servereigenschaft `afw.restriction.policy.v2`. Weitere Informationen zu Servereigenschaften finden Sie unter Servereigenschaften.
- **Wi-Fi-Tethering zulassen:** gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die Wi-Fi-Verbindung des Geräts zulassen. Die Standardeinstellung ist **Aus**. Wenn die Einstellung auf **Ein** festgelegt wird, muss auch die Einstellung **Tethering zulassen** auf **Ein** festgelegt werden.
- **Eingehende MMS zulassen:** Ermöglicht Benutzern den Empfang von MMS-Nachrichten. Die Standardeinstellung ist **Aus**. Wird die Einstellung auf **Ein** festgelegt, müssen Sie auch **SMS zulassen** aktivieren.
- **Ausgehende MMS zulassen:** Ermöglicht Benutzern das Senden von MMS-Nachrichten. Die Standardeinstellung ist **Aus**. Wird die Einstellung auf **Ein** festgelegt, müssen Sie auch **SMS zulassen** aktivieren.
- **Eingehende SMS zulassen:** Ermöglicht Benutzern den Empfang von SMS-Nachrichten. Die Standardeinstellung ist **Aus**. Wird die Einstellung auf **Ein** festgelegt, müssen Sie auch **SMS zulassen** aktivieren.
- **Ausgehende SMS zulassen:** Ermöglicht Benutzern das Senden von SMS-Nachrichten. Die Standardeinstellung ist **Aus**. Wird die Einstellung auf **Ein** festgelegt, müssen Sie auch **SMS zulassen** aktivieren.

- **Mobile Netzwerke konfigurieren:** Ermöglicht Benutzern die Verwendung ihrer Mobilfunkdatenverbindung. Die Standardeinstellung ist **Aus**.
- **Pro Tag beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Tag übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
- **Pro Woche beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Woche übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
- **Pro Monat beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Monat übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
- **Nur sichere VPN-Verbindungen zulassen:** Ermöglicht Benutzern, nur sichere Verbindungen zu verwenden (MDM 4.0 oder höher). Die Standardeinstellung ist **Ein**.
- **Audioaufzeichnung zulassen:** Ermöglicht Benutzern Audioaufzeichnungen auf den Geräten (MDM 4.0 und höher). Die Standardeinstellung ist **Ein**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Mikrofon zulassen** aktivieren.
- **Videoaufzeichnung zulassen:** Ermöglicht Benutzern Videoaufzeichnungen auf den Geräten (MDM 4.0 und höher). Die Standardeinstellung ist **Aus**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Verwenden der Kamera zulassen** aktivieren.
- **Pushnachrichten beim Roaming zulassen:** Ermöglicht die Verwendung mobiler Daten für Pushnachrichten. Die Standardeinstellung ist **Aus**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Datenroaming zulassen** aktivieren.
- **Automatische Synchronisierung beim Roaming zulassen:** Ermöglicht die Verwendung mobiler Daten für die Synchronisierung. Die Standardeinstellung ist **Aus**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Datenroaming zulassen** aktivieren.
- **Sprachanrufe beim Roaming zulassen:** Benutzern erlauben, Mobilfunkdaten für Sprachanrufe zu verwenden. Die Standardeinstellung ist **Aus**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Datenroaming zulassen** aktivieren.

- **Samsung: Knox-Container/Vollständig verwaltetes Gerät**
  - **Sperrprüfung aktivieren:** Prüfung auf gesperrte Zertifikate aktivieren. Die Standardeinstellung ist **Aus**.

- **Samsung: Nur Knox-Container**
  - **Apps in Container verschieben:** Ermöglicht Benutzern das Verschieben von Apps zwischen dem Knox-Container und dem privaten Bereich auf Geräten. Die Standardeinstellung ist **Ein**.
  - **Multifaktorauthentifizierung erzwingen:** Benutzer müssen einen Fingerabdruck und eine weitere Authentifizierungsmethode, z. B. Kennwort oder PIN zum Öffnen ihrer Geräte verwenden. Die Standardeinstellung ist **Ein**.

- **Authentifizierung für Container erzwingen:** Verwendung einer anderen Authentifizierungsmethode beim Öffnen des KNOX-Containers als beim Entsperren des Geräts. Die Standardeinstellung ist **Ein**.
- **Sichere Tastatur verwenden:** Benutzer zur Verwendung einer sicheren Tastatur im Knox-Container zwingen. Die Standardeinstellung ist **Ein**.

- **Samsung: DeX**
  - **Samsung DeX aktivieren:** Ermöglicht, dass unterstützte Knox-fähige Geräte im Samsung DeX-Modus ausgeführt werden. Samsung Knox 3.1 (Mindestversion) erforderlich. Die Standardeinstellung ist **Ein**. Informationen zu den Samsung DeX-Geräteanforderungen und zum Einrichten von Samsung DeX finden Sie in der Samsung-Dokumentation für Entwickler.
    * **Ethernet nur im DeX-Modus zulassen:** Aktivieren Sie die Verwendung von Ethernet im Samsung DeX-Modus. Mobilfunkdaten, Wi-Fi und Tethering (Wi-Fi, Bluetooth und USB) sind im DeX-Modus eingeschränkt. Der Standardwert ist nicht aktiviert.
    * **Bild für Dex-Logo hochladen:** Wählen Sie diese Einstellung, um ein PNG-Bild anzugeben, das als Symbol für Samsung DeX verwendet werden soll.
    * **DeX-Bildschirmtimeout:** Geben Sie die Leerlaufzeit an (in Sekunden), nach deren Ablauf der DeX-Bildschirm ausgeschaltet wird. Um den Timeout zu deaktivieren, geben Sie **0** ein. Die Standardeinstellung ist **1200** Sekunden (20 Minuten).
    * **App-Verknüpfung in Samsung DeX hinzufügen:** Geben Sie einen App-Paketnamen ein, um für die App eine Verknüpfung in DeX hinzuzufügen. Um einen App-Paketnamen zu suchen, gehen Sie zu Google Play und wählen die App aus. Die URL enthält den Paketnamen: `https://play.google.com/store/apps/details?id=<package.name><!--NeedCopy-->`.
    * **App-Verknüpfung aus Samsung DeX entfernen:** Geben Sie einen App-Paketnamen an, um eine Verknüpfung aus DeX zu entfernen. Gehen Sie zu Google Play, um App-Paketnamen zu suchen.
    * **App-Pakete zum Deaktivieren in Samsung DeX:** Geben Sie eine durch Trennzeichen getrennte Liste der App-Pakete an, die Sie im Samsung DeX-Modus blockieren möchten. Beispiel: `"com.android.chrome", "com.google.android.gm"<!--NeedCopy-->`.

Wenn **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil anwenden** aktiviert ist und für **Richtlinie bei vollständig verwalteten Geräten mit einem Arbeitsprofil anwenden auf:** die Einstellung **Arbeitsprofil** gewählt ist, konfigurieren Sie diese Einstellungen:

- **Sicherheit**
  - **Kontoverwaltung zulassen:** Ermöglicht die Kontenverwaltung im Arbeitsprofil und auf verwalteten Geräten. Die Standardeinstellung ist **Aus**.
  - **Kopieren und Einfügen zwischen Profilen zulässig:** Bei Auswahl von **Ein** können

Benutzer die Zwischenablage zum Kopieren und Einfügen zwischen Apps im Android Enterprise-Profil und Apps im privaten Bereich verwenden. Die Standardeinstellung ist **Aus**.

- **Screenshot zulassen:** Ermöglicht Benutzern, einen Screenshot des Gerätebildschirms zu machen. Die Standardeinstellung ist **Aus**.
- **Verwendung der Kamera zulassen:** Ermöglicht Benutzern, Bilder und Videos mit der Gerätekamera aufzunehmen. Die Standardeinstellung ist **Aus**.
- **Konfigurieren von Standortermittlung zulassen:** Ermöglicht Benutzern, GPS auf ihren Geräten einzuschalten. Für Android API 28 und höher. Die Standardeinstellung ist **Ein**.
- **Standortfreigabe zulassen:** Bei verwalteten Profilen kann der Gerätebesitzer diese Einstellung außer Kraft setzen. Die Standardeinstellung ist **Aus**.

  > **Tipp:**
  >
  > Mit einer Standortrichtlinie können Sie in XenMobile geografische Grenzen festlegen. Weitere Informationen finden Sie unter Standortrichtlinie für Geräte.

- **Benutzer darf Benutzeranmeldeinformationen konfigurieren:** Geben Sie an, ob Benutzer Anmeldeinformationen im verwalteten Schlüsselspeicher konfigurieren dürfen. Die Standardeinstellung ist **Ein**.
- **Drucken zulassen:** Wenn diese Option auf **Ein** festgelegt ist, können Benutzer jeden Drucker verwenden, auf den ihr Gerät Zugriff hat. Die Standardeinstellung ist **Aus**. Verfügbar ab Android 9.

- **Apps**
  - **System-Apps aktivieren:** Ermöglicht Benutzern das Ausführen vorinstallierter Geräteapps. Die Standardeinstellung ist **Aus**. Um bestimmte Apps zu aktivieren, klicken Sie in der Tabelle **Liste der System-Apps** auf **Hinzufügen**.
    - **Liste der System-Apps:** Eine Liste der System-Apps, die Sie auf dem Gerät aktivieren möchten. Wählen Sie für **System-Apps aktivieren** die Einstellung **Ein** und fügen Sie den App-Paketnamen hinzu. Um den Paketnamen für eine System-App zu suchen, können Sie mit der Android Debug Bridge (`adb`) den Android-Paketmanager (`pm`)-Befehl aufrufen. Beispielsweise `adb shell "pm list packages -f name"`, wobei “name” Teil des Paketnamens ist. Weitere Informationen finden Sie unter https://developer.android.com/studio/command-line/adb. Für Android Enterprise-Geräte können Sie die App-Berechtigungen über die Richtlinie App-Berechtigungen für Android Enterprise einschränken.
  - **Anwendungen deaktivieren:** Sperrt die Apps auf einer definierten Liste, sodass sie nicht ausgeführt werden können. Die Standardeinstellung ist **Aus**. Zum Deaktivieren einer in-

stallierten App ändern Sie die Einstellung auf **Ein** und klicken Sie in der Tabelle **Anwendungsliste** auf **Hinzufügen**.

  * **Anwendungsliste:** Liste der Apps, die Sie blockieren möchten. Legen Sie **Anwendungen deaktivieren** auf **Ein** fest und fügen Sie die App hinzu. Geben Sie den Namen des App-Pakets ein. Durch Ändern und Bereitstellen einer App-Liste wird die vorherige App-Liste überschrieben. Wenn Sie beispielsweise com.example1 und com.example2 deaktivieren und später die Liste in com.example1 und com.example3 ändern, wird com.example.2 in XenMobile aktiviert.

- **App-Verifizierung aktivieren:** Ermöglicht dem Betriebssystem die Überprüfung von Apps auf schädliches Verhalten. Die Standardeinstellung ist **Ein**.
- **Google Apps aktivieren:** Ermöglicht Benutzern das Herunterladen von Apps von Google Mobile Services auf das Gerät. Die Standardeinstellung ist **Ein**.
- **App nicht aus Google Play zulassen:** Installation von Apps aus einem anderen Store als Google Play zulassen. Die Standardeinstellung ist **Aus**.
- **Benutzersteuerung der Anwendungseinstellungen zulassen:** Ermöglicht Benutzern das Deinstallieren und Deaktivieren einer App, das Leeren des Cache und das Löschen von Daten, das erzwungene Anhalten einer App und das Löschen der Standardeinstellungen. Die Benutzer führen diese Aktionen über die Einstellungs-App aus. Die Standardeinstellung ist **Aus**.
- **App-Deinstallation zulassen:** Ermöglicht Benutzern die Deinstallation von Apps aus dem verwalteten Google Play Store. Die Standardeinstellung ist **Aus**. Um diese Einstellung anzuzeigen, aktivieren Sie die Servereigenschaft `afw.restriction.policy.v2`. Weitere Informationen zu Servereigenschaften finden Sie unter Servereigenschaften.

- **BYOD-Arbeitsprofil**
  - **App-Widgets für Arbeitsprofil auf dem Startbildschirm zulassen:** Wenn für diese Einstellung **Ein** festgelegt ist, können Benutzer Arbeitsprofil-App-Widgets auf dem Startbildschirm des Geräts platzieren. Wenn für diese Einstellung **Aus** festgelegt ist, können Benutzer keine Arbeitsprofil-App-Widgets auf dem Startbildschirm des Geräts platzieren. Die Standardeinstellung ist **Aus**.
    * **Apps mit zulässigen Widgets:** Eine Liste der Apps, die Sie auf dem Startbildschirm zulassen möchten. Wählen Sie für **App-Widgets für Arbeitsprofil auf dem Startbildschirm zulassen** die Einstellung **Ein** und fügen Sie die App hinzu. Klicken Sie auf **Hinzufügen** und wählen Sie in der Liste die App, deren Widgets Sie auf dem Homebildschirm zulassen möchten. Klicken Sie auf **Speichern**. Wiederholen Sie diesen Vorgang, um weitere App-Widgets zuzulassen.
  - **Kontakte des Firmenprofils in Gerätekontakten zulassen:** Zeigt Kontakte aus dem verwalteten Android Enterprise-Profil im übergeordneten Profil für eingehende Anrufe an (Android 7.0 und höher). Die Standardeinstellung ist **Aus**.

- **Samsung**

  - **TIMA-Schlüsselspeicher aktivieren:** Der TIMA-Schlüsselspeicher bietet einen TrustZone-basierten, sicheren Speicher für symmetrische Schlüssel. RSA-Schlüsselpaare und -Zertifikate werden zur Speicherung an den Standard-Schlüsselspeicheranbieter geleitet. Die Standardeinstellung ist **Aus**.
  - **Freigabeliste zulassen:** Ermöglicht Benutzern das Teilen von Inhalten zwischen Apps in der Liste "Freigeben über". Die Standardeinstellung ist **Ein**.
  - **Überwachungsprotokoll aktivieren:** Erstellen von Ereignisüberwachungsprotokollen für die forensische Analyse von Geräten aktivieren. Die Standardeinstellung ist **Aus**.

- **Samsung: Knox-Container/Vollständig verwaltetes Gerät**
  - **Sperrprüfung aktivieren:** Prüfung auf gesperrte Zertifikate aktivieren. Die Standardeinstellung ist **Aus**.

- **Samsung: Nur Knox-Container**
  - **Apps in Container verschieben:** Ermöglicht Benutzern das Verschieben von Apps zwischen dem Knox-Container und dem privaten Bereich auf Geräten. Die Standardeinstellung ist **Ein**.
  - **Multifaktorauthentifizierung erzwingen:** Benutzer müssen einen Fingerabdruck und eine weitere Authentifizierungsmethode, z. B. Kennwort oder PIN zum Öffnen ihrer Geräte verwenden. Die Standardeinstellung ist **Ein**.
  - **Authentifizierung für Container erzwingen:** Verwendung einer anderen Authentifizierungsmethode beim Öffnen des KNOX-Containers als beim Entsperren des Geräts. Die Standardeinstellung ist **Ein**.
  - **Sichere Tastatur verwenden:** Benutzer zur Verwendung einer sicheren Tastatur im Knox-Container zwingen. Die Standardeinstellung ist **Ein**.

Wenn **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil anwenden** aktiviert ist und für **Richtlinie bei vollständig verwalteten Geräten mit einem Arbeitsprofil anwenden auf:** die Einstellung **Verwaltetes Gerät** gewählt ist, konfigurieren Sie diese Einstellungen:

- **Sicherheit**
  - **Kontoverwaltung zulassen:** Ermöglicht die Kontenverwaltung im Arbeitsprofil und auf verwalteten Geräten. Die Standardeinstellung ist **Aus**.
  - **Kopieren und Einfügen zwischen Profilen zulässig:** Bei Auswahl von **Ein** können Benutzer die Zwischenablage zum Kopieren und Einfügen zwischen Apps im Android Enterprise-Profil und Apps im privaten Bereich verwenden. Die Standardeinstellung ist **Aus**.
  - **Screenshot zulassen:** Ermöglicht Benutzern, einen Screenshot des Gerätebildschirms zu machen. Die Standardeinstellung ist **Aus**.

- **Verwendung der Kamera zulassen:** Ermöglicht Benutzern, Bilder und Videos mit der Gerätekamera aufzunehmen. Die Standardeinstellung ist **Aus**.
- **VPN-Konfiguration zulassen:** Ermöglicht Benutzern das Erstellen von VPN-Konfigurationen. Für Geräte im Arbeitsprofilmodus mit Android 6 und höher und für vollständig verwaltete Geräte. Die Standardeinstellung ist **Ein**.
- **Backupdienst zulassen:** Ermöglicht Benutzern die Sicherung von Anwendungs- und Systemdaten auf den Geräten. Die Standardeinstellung ist **Ein**.
- **NFC zulassen:** Ermöglicht Benutzern das Senden von Webseiten, Fotos, Videos oder anderen Inhalten an andere Geräte über NFC. Für MDM 4.0 und höher. Die Standardeinstellung ist **Ein**.
- **Konfigurieren von Standortermittlung zulassen:** Ermöglicht Benutzern, GPS auf ihren Geräten einzuschalten. Für Android API 28 und höher. Die Standardeinstellung ist **Ein**.
- **Standortfreigabe zulassen:** Bei verwalteten Profilen kann der Gerätebesitzer diese Einstellung außer Kraft setzen. Die Standardeinstellung ist **Aus**.

  > **Tipp:**
  >
  > Mit einer Standortrichtlinie können Sie in XenMobile geografische Grenzen festlegen. Weitere Informationen finden Sie unter Standortrichtlinie für Geräte.

- **Benutzer darf Benutzeranmeldeinformationen konfigurieren:** Geben Sie an, ob Benutzer Anmeldeinformationen im verwalteten Schlüsselspeicher konfigurieren dürfen. Die Standardeinstellung ist **Ein**.
- **Drucken zulassen:** Wenn diese Option auf **Ein** festgelegt ist, können Benutzer jeden Drucker verwenden, auf den ihr Gerät Zugriff hat. Die Standardeinstellung ist **Aus**. Verfügbar ab Android 9.
- **USB-Debugging zulassen:** Der Standardwert ist **Aus**.

- **Apps**
  - **System-Apps aktivieren:** Ermöglicht Benutzern das Ausführen vorinstallierter Geräteapps. Die Standardeinstellung ist **Aus**. Um bestimmte Apps zu aktivieren, klicken Sie in der Tabelle **Liste der System-Apps** auf **Hinzufügen**.
    - **Liste der System-Apps:** Eine Liste der System-Apps, die Sie auf dem Gerät aktivieren möchten. Wählen Sie für **System-Apps aktivieren** die Einstellung **Ein** und fügen Sie den App-Paketnamen hinzu. Um den Paketnamen für eine System-App zu suchen, können Sie mit der Android Debug Bridge (`adb`) den Android-Paketmanager (`pm`)-Befehl aufrufen. Beispielsweise `adb shell "pm list packages -f name"`, wobei "name" Teil des Paketnamens ist. Weitere Informationen finden Sie unter https://developer.android.com/studio/command-line/adb. Für Android Enterprise-

Geräte können Sie die App-Berechtigungen über die Richtlinie App-Berechtigungen für Android Enterprise einschränken.

- **Anwendungen deaktivieren:** Sperrt die Apps auf einer definierten Liste, sodass sie nicht ausgeführt werden können. Die Standardeinstellung ist **Aus**. Zum Deaktivieren einer installierten App ändern Sie die Einstellung auf **Ein** und klicken Sie in der Tabelle **Anwendungsliste** auf **Hinzufügen**.
  - **Anwendungsliste:** Liste der Apps, die Sie blockieren möchten. Legen Sie **Anwendungen deaktivieren** auf **Ein** fest und fügen Sie die App hinzu. Geben Sie den Namen des App-Pakets ein. Durch Ändern und Bereitstellen einer App-Liste wird die vorherige App-Liste überschrieben. Wenn Sie beispielsweise com.example1 und com.example2 deaktivieren und später die Liste in com.example1 und com.example3 ändern, wird com.example.2 in XenMobile aktiviert.
- **App-Verifizierung aktivieren:** Ermöglicht dem Betriebssystem die Überprüfung von Apps auf schädliches Verhalten. Die Standardeinstellung ist **Ein**.
- **Google Apps aktivieren:** Ermöglicht Benutzern das Herunterladen von Apps von Google Mobile Services auf das Gerät. Die Standardeinstellung ist **Ein**.
- **App nicht aus Google Play zulassen:** Installation von Apps aus einem anderen Store als Google Play zulassen. Die Standardeinstellung ist **Aus**.
- **Benutzersteuerung der Anwendungseinstellungen zulassen:** Ermöglicht Benutzern das Deinstallieren und Deaktivieren einer App, das Leeren des Cache und das Löschen von Daten, das erzwungene Anhalten einer App und das Löschen der Standardeinstellungen. Die Benutzer führen diese Aktionen über die Einstellungs-App aus. Die Standardeinstellung ist **Aus**.
- **App-Deinstallation zulassen:** Ermöglicht Benutzern die Deinstallation von Apps aus dem verwalteten Google Play Store. Die Standardeinstellung ist **Aus**. Um diese Einstellung anzuzeigen, aktivieren Sie die Servereigenschaft `afw.restriction.policy.v2`. Weitere Informationen zu Servereigenschaften finden Sie unter Servereigenschaften.

- **Nur vollständig verwaltetes Gerät**
  - **Hinzufügen von Benutzern zulassen:** Ermöglicht Benutzern das Hinzufügen neuer Benutzer auf einem Gerät. Die Standardeinstellung ist **Ein**.
  - **Datenroaming zulassen:** Ermöglicht Benutzern die Verwendung mobiler Daten beim Roaming. Die Standardeinstellung ist “Aus”, d. h. Roaming ist auf den Geräten deaktiviert. Die Standardeinstellung ist **Aus**.
  - **SMS zulassen:** Ermöglicht Benutzern das Senden und Empfangen von SMS-Nachrichten. Die Standardeinstellung ist **Aus**.
  - **Verwendung der Statusleiste zulassen:** Wenn diese Einstellung auf **Ein** gesetzt ist, aktiviert sie die Statusleiste auf verwalteten und dedizierten Geräten (“COSU-Geräte”). Diese Einstellung deaktiviert Benachrichtigungen, Schnelleinstellungen und andere Bildschirmüberlagerungen, die das Ausschalten des Vollbildmodus ermöglichen. Die

Benutzer können Benachrichtigungen in den Systemeinstellungen anzeigen. Für Android 6.0 und höher. Die Standardeinstellung ist **Aus**.

- **Bluetooth zulassen:** Ermöglicht Benutzern die Verwendung von Bluetooth. Die Standardeinstellung ist **Ein**.
  - **Bluetooth-Freigabe zulassen:** Wenn diese Option deaktiviert ist, können Benutzer keine ausgehende Bluetooth-Freigabe auf ihrem Gerät einrichten. Die Option ist standardmäßig aktiviert. Um diese Einstellung anzuzeigen, aktivieren Sie die Servereigenschaft `afw.restriction.policy.v2`. Weitere Informationen zu Servereigenschaften finden Sie unter Servereigenschaften.
- **Konfigurieren von Datum und Uhrzeit zulassen:** Ermöglicht Benutzern das Ändern von Datum und Uhrzeit auf ihren Geräten. Die Standardeinstellung ist **Ein**.
- **Zurücksetzen auf Werkseinstellungen zulassen:** Ermöglicht Benutzern das Zurücksetzen der Geräte auf die werkseitige Voreinstellung. Die Standardeinstellung ist **Ein**.
- **Gerätebildschirm eingeschaltet lassen:** Wenn diese Einstellung auf **Ein** festgelegt ist, bleibt der Gerätebildschirm eingeschaltet, solange das Gerät am Stromnetz angeschlossen ist. Die Standardeinstellung ist **Aus**.
- **USB-Massenspeicher zulassen:** Übertragung großer Datendateien zwischen Benutzergeräten und einem Computer über eine USB-Verbindung zulassen. Die Standardeinstellung ist **Ein**.
- **Mikrofon zulassen:** Ermöglicht Benutzern die Verwendung des Gerätemikrofons. Die Standardeinstellung ist **Ein**.
- **Tethering zulassen:** Ermöglicht Benutzern das Konfigurieren mobiler Hotspots und das Tethering von Daten. Die Standardeinstellung ist **Aus**. Wenn diese Einstellung aktiviert ist, sind folgende Einstellungen für Samsung-Geräte verfügbar:
- **Verhindern, dass der Tastenschutz das Gerät sperrt:** Wird diese Einstellung auf **Ein** festgelegt, deaktiviert sie den Tastenschutz des Sperrbildschirms auf verwalteten und dedizierten Geräten (“COSU-Geräte”). Die Standardeinstellung ist **Aus**.
- **Wi-Fi-Änderungen zulassen:** Wenn diese Option auf **Ein** festgelegt ist, können die Benutzer das Wi-Fi ein- und ausschalten und eine Verbindung mit Wi-Fi-Netzwerken herstellen. Die Standardeinstellung ist **Ein**.
- **Dateiübertragung zulassen:** Ermöglicht Dateiübertragungen über USB. Die Standardeinstellung ist **Aus**.

- **Samsung**
  - **TIMA-Schlüsselspeicher aktivieren:** Der TIMA-Schlüsselspeicher bietet einen TrustZone-basierten, sicheren Speicher für symmetrische Schlüssel. RSA-Schlüsselpaare und -Zertifikate werden zur Speicherung an den Standard-Schlüsselspeicheranbieter geleitet. Die Standardeinstellung ist **Aus**.
  - **Freigabeliste zulassen:** Ermöglicht Benutzern das Teilen von Inhalten zwischen Apps in der Liste “Freigeben über”. Die Standardeinstellung ist **Ein**.

  - **Überwachungsprotokoll aktivieren:** Erstellen von Ereignisüberwachungsprotokollen für die forensische Analyse von Geräten aktivieren. Die Standardeinstellung ist **Aus**.

- **Samsung: Nur vollständig verwaltetes Gerät**
  - **Überprüfung von ODE vertrauenswürdigem Start aktivieren:** Verwenden der ODE-Prüfung auf vertrauenswürdigen Start zur Erstellung einer Vertrauenskette zwischen Bootloader und Systemimage. Die Standardeinstellung ist **Ein**.
  - **Nur Notruf zulassen:** Ermöglicht Benutzern das Aktivieren des Modus “Nur Notruf” auf den Geräten. Die Standardeinstellung ist **Aus**.
  - **Firmwarewiederherstellung zulassen:** Ermöglicht Benutzern das Wiederherstellen der Firmware auf den Geräten. Die Standardeinstellung ist **Ein**.
  - **Schnelle Verschlüsselung zulassen:** Ausschließliche Verschlüsselung des verwendeten Speicherplatzes zulassen. Diese Verschlüsselung ist die Alternative zur vollständigen Datenträgerverschlüsselung, bei der alle Daten verschlüsselt werden. Zu diesen Daten gehören Einstellungen, Anwendungsdaten, heruntergeladene Dateien und Anwendungen, Medien und Dateien anderer Art. Die Standardeinstellung ist **Ein**.
  - **Common Criteria-Modus aktivieren:** Schalten von Geräten in den Common Criteria-Modus. Die Common Criteria-Konfiguration erzwingt strenge Sicherheitsvorgänge. Die Standardeinstellung ist **Ein**.
  - **Neustartbanner aktivieren:** Beim Geräteneustart eine Benachrichtigung oder ein Banner über die vom Department of Defense genehmigte Systemnutzung anzeigen. Die Standardeinstellung ist **Aus**.
  - **Einstellungsänderungen zulassen:** Ermöglicht Benutzern das Ändern von Einstellungen auf ihren vollständig verwalteten Geräten. Die Standardeinstellung ist **Ein**.
  - **Datennutzung im Hintergrund aktivieren:** Datensynchronisierung im Hintergrund für Apps zulassen. Für vollständig verwaltete Geräte. Die Standardeinstellung ist **Ein**.
  - **Zwischenablage zulassen:** Kopieren von Daten in die Zwischenablage von Geräten zulassen. Die Standardeinstellung ist **Ein**.
    * **Freigeben der Zwischenablage zulassen:** Teilen von Inhalten in der Zwischenablage zwischen Geräten und Computern zulassen (MDM 4.0 und höher).
  - **Hometaste zulassen:** Ermöglicht Benutzern die Verwendung der **Hometaste** auf vollständig verwalteten Geräten. Die Standardeinstellung ist **Ein**.
  - **Vorgegebenen Standort zulassen:** Ermöglicht Benutzern das Vortäuschen eines GPS-Standorts. Für vollständig verwaltete Geräte. Die Standardeinstellung ist **Aus**.
  - **NFC:** Ermöglicht Benutzern die Verwendung von NFC auf vollständig verwalteten Geräten (MDM 3.0 und höher). Die Standardeinstellung ist **Ein**.
  - **Ausschalten zulassen:** Ermöglicht Benutzern das Ausschalten von vollständig verwalteten Geräten (MDM 3.0 und höher). Die Standardeinstellung ist **Ein**.
  - **Wi-Fi direkt zulassen:** Ermöglicht Benutzern die direkte Verbindung mit einem anderen Gerät über ihre Wi-Fi-Verbindung. Die Standardeinstellung ist **Ein**. Bei der Einstellung **Ein**

müssen Sie die Einstellung **Wi-Fi-Änderungen zulassen** aktivieren.

- **SD-Karte zulassen:** Ermöglicht Benutzern die Verwendung einer SD-Karte (sofern verfügbar) für die Geräte. Die Standardeinstellung ist **Ein**.
- **USB-Hostspeicher zulassen:** Verwendung der Geräte als USB-Host bei Verbindung eines USB-Geräts mit den Geräten zulassen. Die Geräte müssen hierbei USB-Geräte mit Strom versorgen. Die Standardeinstellung ist **Ein**.
- **Sprachwahl zulassen:** Ermöglicht Benutzern die Verwendung der Sprachwahl auf den Geräten (MDM 4.0 und höher). Die Standardeinstellung ist **Ein**.
- **S Beam zulassen:** Ermöglicht Benutzern das Teilen von Inhalten über NFC und Wi-Fi Direct (MDM 4.0 und höher). Die Standardeinstellung ist **Ein**.
- **S Voice zulassen:** Ermöglicht Benutzern die Verwendung des intelligenten persönlichen Assistenten und Wissensnavigators auf Geräten (MDM 4.0 und höher). Die Standardeinstellung ist **Ein**.
- **USB-Tethering zulassen:** Ermöglicht Benutzern die gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die USB-Verbindung des Geräts. Die Standardeinstellung ist **Aus**. Wenn die Einstellung auf **Ein** festgelegt wird, muss auch die Einstellung **Tethering zulassen** auf **Ein** festgelegt werden.
- **Bluetooth-Tethering zulassen:** gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die Bluetooth-Verbindung des Geräts zulassen. Die Standardeinstellung ist **Aus**. Wenn die Einstellung auf **Ein** festgelegt wird, muss auch die Einstellung **Tethering zulassen** auf **Ein** festgelegt werden.
- **Wi-Fi-Tethering zulassen:** gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die Wi-Fi-Verbindung des Geräts zulassen. Die Standardeinstellung ist **Aus**. Wenn die Einstellung auf **Ein** festgelegt wird, muss auch die Einstellung **Tethering zulassen** auf **Ein** festgelegt werden.
- **Eingehende MMS zulassen:** Ermöglicht Benutzern den Empfang von MMS-Nachrichten. Die Standardeinstellung ist **Aus**. Wird die Einstellung auf **Ein** festgelegt, müssen Sie auch **SMS zulassen** aktivieren.
- **Ausgehende MMS zulassen:** Ermöglicht Benutzern das Senden von MMS-Nachrichten. Die Standardeinstellung ist **Aus**. Wird die Einstellung auf **Ein** festgelegt, müssen Sie auch **SMS zulassen** aktivieren.
- **Eingehende SMS zulassen:** Ermöglicht Benutzern den Empfang von SMS-Nachrichten. Die Standardeinstellung ist **Aus**. Wird die Einstellung auf **Ein** festgelegt, müssen Sie auch **SMS zulassen** aktivieren.
- **Ausgehende SMS zulassen:** Ermöglicht Benutzern das Senden von SMS-Nachrichten. Die Standardeinstellung ist **Aus**. Wird die Einstellung auf **Ein** festgelegt, müssen Sie auch **SMS zulassen** aktivieren.
- **Mobile Netzwerke konfigurieren:** Ermöglicht Benutzern die Verwendung ihrer Mobilfunkdatenverbindung. Die Standardeinstellung ist **Aus**.

- **Pro Tag beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Tag übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
- **Pro Woche beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Woche übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
- **Pro Monat beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Monat übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
- **Nur sichere VPN-Verbindungen zulassen:** Ermöglicht Benutzern, nur sichere Verbindungen zu verwenden (MDM 4.0 oder höher). Die Standardeinstellung ist **Ein**.
- **Audioaufzeichnung zulassen:** Ermöglicht Benutzern Audioaufzeichnungen auf den Geräten (MDM 4.0 und höher). Die Standardeinstellung ist **Ein**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Mikrofon zulassen** aktivieren.
- **Videoaufzeichnung zulassen:** Ermöglicht Benutzern Videoaufzeichnungen auf den Geräten (MDM 4.0 und höher). Die Standardeinstellung ist **Aus**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Verwenden der Kamera zulassen** aktivieren.
- **Pushnachrichten beim Roaming zulassen:** Ermöglicht die Verwendung mobiler Daten für Pushnachrichten. Die Standardeinstellung ist **Aus**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Datenroaming zulassen** aktivieren.
- **Automatische Synchronisierung beim Roaming zulassen:** Ermöglicht die Verwendung mobiler Daten für die Synchronisierung. Die Standardeinstellung ist **Aus**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Datenroaming zulassen** aktivieren.
- **Sprachanrufe beim Roaming zulassen:** Benutzern erlauben, Mobilfunkdaten für Sprachanrufe zu verwenden. Die Standardeinstellung ist **Aus**. Bei Einstellung auf **Ein** müssen Sie auch die Einstellung **Datenroaming zulassen** aktivieren.

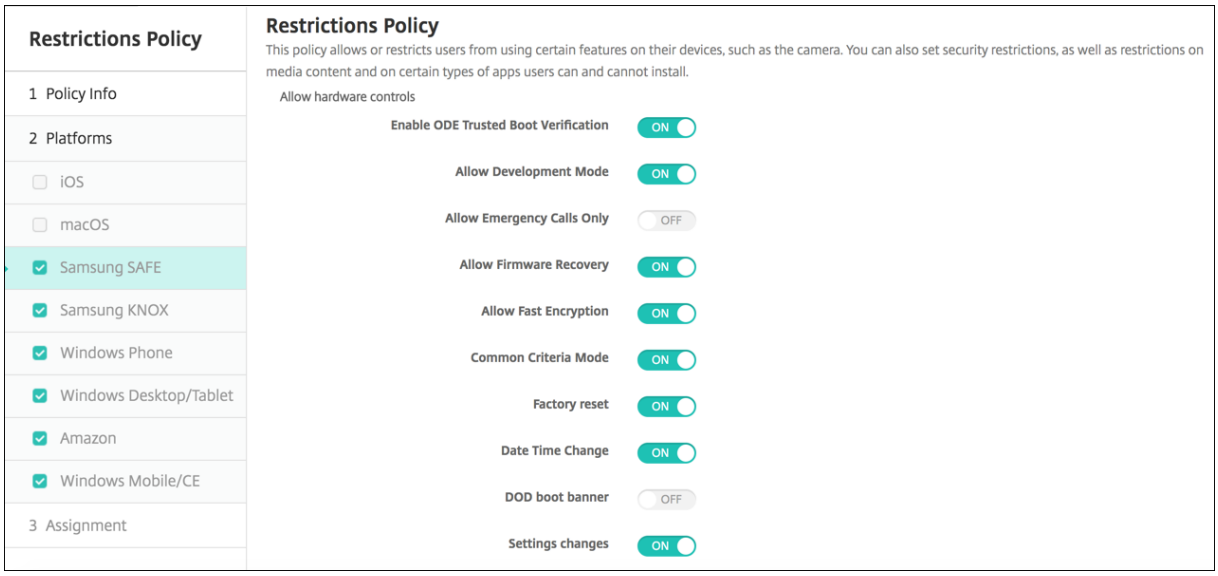
- **Samsung: Knox-Container/Vollständig verwaltetes Gerät**
  - **Sperrprüfung aktivieren:** Prüfung auf gesperrte Zertifikate aktivieren. Die Standardeinstellung ist **Aus**.

- **Samsung: Nur Knox-Container**
  - **Apps in Container verschieben:** Ermöglicht Benutzern das Verschieben von Apps zwischen dem Knox-Container und dem privaten Bereich auf Geräten. Die Standardeinstellung ist **Ein**.
  - **Multifaktorauthentifizierung erzwingen:** Benutzer müssen einen Fingerabdruck und eine weitere Authentifizierungsmethode, z. B. Kennwort oder PIN zum Öffnen ihrer Geräte verwenden. Die Standardeinstellung ist **Ein**.
  - **Authentifizierung für Container erzwingen:** Verwendung einer anderen Authentifizierungsmethode beim Öffnen des KNOX-Containers als beim Entsperren des Geräts.

Die Standardeinstellung ist **Ein**.

- **Sichere Tastatur verwenden:** Benutzer zur Verwendung einer sicheren Tastatur im Knox-Container zwingen. Die Standardeinstellung ist **Ein**.

Samsung SAFE-Einstellungen



Einige Optionen stehen nur in bestimmten APIs zur Samsung-Mobilgeräteverwaltung zur Verfügung. Für diese ist die entsprechende Versionsangabe aufgeführt.

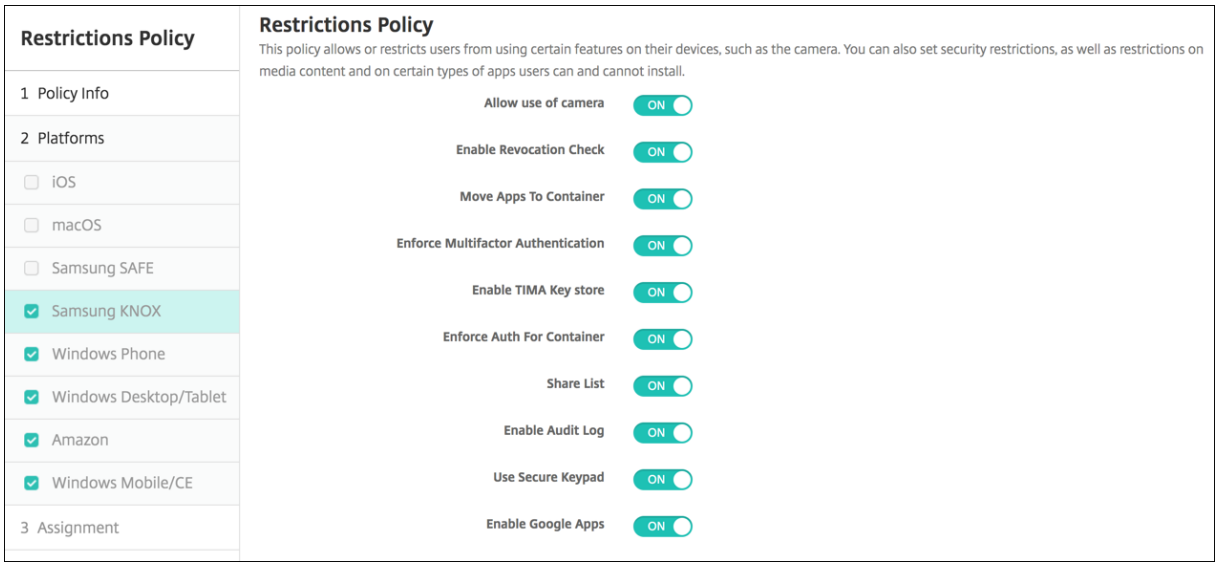
- **Hardwaresteuerelemente zulassen**
  - **Überprüfung von ODE vertrauenswürdigem Start aktivieren:** Verwenden der ODE-Prüfung auf vertrauenswürdigen Start zur Erstellung einer Vertrauenskette zwischen Bootloader und Systemimage.
  - **Entwicklermodus zulassen:** Aktivieren der Entwicklereinstellungen auf Geräten durch die Benutzer zulassen.
  - **Nur Notruf zulassen:** Aktivieren des Modus “Nur Notruf” auf Geräten durch die Benutzer zulassen.
  - **Firmwarewiederherstellung zulassen:** Wiederherstellung der Firmware auf Geräten durch die Benutzer zulassen.
  - **Schnelle Verschlüsselung zulassen:** Ausschließliche Verschlüsselung des verwendeten Speicherplatzes zulassen. Dies ist die Alternative zur vollständigen Datenträgerverschlüsselung, bei der alle Daten, d. h. Einstellungen, Anwendungsdaten, heruntergeladene Dateien und Anwendungen, Medien und Dateien anderer Art verschlüsselt werden.
  - **Common Criteria-Modus**: Schalten von Geräten in den Common Criteria-Modus. Die Common Criteria-Konfiguration erzwingt strenge Sicherheitsvorgänge.
  - **Zurücksetzen auf Herstellereinstellungen:** Zurücksetzen der Geräte auf die werkseitige Voreinstellung zulassen.

  - **Datums-/Uhrzeitänderung:** Änderung von Datum und Uhrzeit auf den Geräten zulassen.
  - **DOD-Startbanner:** Beim Geräteneustart eine Benachrichtigung oder ein Banner über die vom Department of Defense genehmigte Systemnutzung anzeigen.
  - **Einstellungsänderungen:** Ändern von Einstellungen auf Geräten zulassen.
  - **Backup:** Sicherung von Anwendungs- und Systemdaten auf Geräten zulassen.
  - **Drahtloses Upgrade:** Erhalt von Softwareupdates über eine drahtlose Schnittstelle zulassen (MDM 3.0 und höher).
  - **Hintergrunddaten:** Synchronisierung von Daten durch Apps im Hintergrund zulassen.
  - **Kamera:** Verwendung der Kamera von Geräten zulassen.
  - **Zwischenablage:** Kopieren von Daten in die Zwischenablage von Geräten zulassen.
    * **Zwischenablage freigeben:** Teilen von Inhalten in der Zwischenablage zwischen Geräten und Computern zulassen (MDM 4.0 und höher).
  - **Hometaste:** Verwenden der Hometaste auf den Geräten zulassen.
  - **Mikrofon:** Verwendung des Gerätemikrofons zulassen.
  - **Vorgegebener Standort:** Vortäuschung eines GPS-Standorts zulassen.
  - **NFC:** Verwendung von NFC (Near Field Communication) auf Geräten zulassen (MDM 3.0 und höher).
  - **Ausschalten:** Ausschalten des Geräts zulassen (MDM 3.0 und höher).
  - **Screenshot:** Erstellen von Screenshots auf Geräten zulassen.
  - **SD-Karte:** Verwendung einer SD-Karte (sofern verfügbar) für die Geräte zulassen.
  - **Sprachwahl:** Verwendung der Sprachwahl auf den Geräten zulassen (MDM 4.0 und höher).
  - **SBeam:** Teilen von Inhalten über NFC und Wi-Fi Direct zulassen (MDM 4.0 und höher).
  - **SVoice:** Verwendung des intelligenten persönlichen Assistenten und Wissensnavigators auf Geräten zulassen (MDM 4.0 und höher).
  - **Mehrere Benutzer zulassen:** Verwendung eines Geräts durch mehrere Benutzer zulassen (MDM 4.0 und höher). Die Standardeinstellung ist **Aus**.
- **Apps zulassen**
  - **Browser:** Verwendung des Webbrowsers zulassen.
  - **YouTube:** Zugriff auf YouTube zulassen.
  - **Google Play/Marketplace:** Zugriff auf Google Play und Google Apps Marketplace zulassen.
  - **App nicht aus Google Play zulassen:** Download von Apps aus anderen Websites als Google Play und Google Apps Marketplace zulassen. Bei Auswahl von **Ein** können Benutzer in den Sicherheitseinstellungen des Gerätes festlegen, dass Apps aus unbekannten Quellen vertraut wird.
  - **System-Apps anhalten:** Deaktivieren vorinstallierter System-Apps zulassen (MDM 4.0 und höher).
  - **Anwendungen deaktivieren:** Bei Auswahl von **Ein** werden alle Apps einer definierten Liste auf Samsung SAFE-Geräten gesperrt und können nicht ausgeführt werden.

- **Netzwerk**
  - **Eingehende MMS:** Empfang von MMS-Nachrichten zulassen.
  - **Eingehende SMS:** Empfang von SMS-Nachrichten zulassen.
  - **Ausgehende MMS:** Senden von MMS-Nachrichten zulassen.
  - **Ausgehende SMS:** Senden von SMS-Nachrichten zulassen.
  - **VPN-Profile von Benutzern hinzufügen:**
  - **Bluetooth:** Verwendung von Bluetooth zulassen.
    - **Tethering:** gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die Bluetooth-Verbindung des Geräts zulassen.
  - **WiFi:** Verbindung mit WiFi-Netzwerk zulassen.
    - **Tethering:** gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die WiFi-Verbindung des Geräts zulassen.
    - **Direkt:** direkte Verbindung mit einem anderen Gerät über die WiFi-Verbindung zulassen (MDM 4.0 und höher).
    - **Zustandsänderung:** Änderung des WiFi-Verbindungszustands durch Apps zulassen.
    - **Benutzerprofiländerungen:** Ändern von WiFi-Richtlinien durch die Benutzer zulassen. Wenn die Option nicht aktiviert wird, können die Benutzer nur den Benutzernamen und das Kennwort für WiFi ändern. Wenn die Option aktiviert wird, können die Benutzer alle WiFi- Richtlinien ändern.
  - **Tethering:** gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät zulassen.
  - **Mobile Daten:** Verwendung der Mobilfunkverbindung für Daten zulassen.
  - **Roaming zulassen:** Verwendung mobiler Daten beim Roaming zulassen. Die Standardeinstellung ist AUS, d. h. Roaming ist auf den Geräten deaktiviert.
  - **Nur sichere Verbindungen:** nur die Verwendung sicherer Verbindungen zulassen (MDM 4.0 oder höher).
  - **Android Beam:** Senden von Webseiten, Fotos, Videos oder anderen Inhalten an andere Geräte über NFC zulassen (MDM 4.0 und höher).
  - **Audioaufzeichnung:** Audioaufzeichnungen auf den Geräten zulassen (MDM 4.0 und höher).
  - **Videoaufzeichnung:** Videoaufzeichnungen auf den Geräten zulassen (MDM 4.0 und höher).
  - **Ortungsdienste:** Einschalten von GPS auf den Geräten zulassen.
  - **Pro Tag beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Tag übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
  - **Pro Woche beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Woche übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).

  - **Pro Monat beschränken (MB):** Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Monat übertragen dürfen. Die Standardeinstellung ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
- **USB-Aktionen zulassen:** USB- Verbindung zwischen Geräten und Computern zulassen.
  - **Debugging:** Debuggen über USB zulassen.
  - **Hostspeicher:** Verwendung der Geräte als USB-Host bei Verbindung eines USB-Geräts mit den Geräten zulassen. Die Geräte müssen hierbei USB-Geräte mit Strom versorgen.
  - **Massenspeicher:** Übertragung großer Datendateien zwischen Geräten und Computern über eine USB-Verbindung zulassen.
  - **Kies Media Player:** Verwendung von Samsung Kies zum Synchronisieren von Dateien zwischen Gerät und Computer zulassen.
  - **Tethering:** gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über eine USB-Verbindung zulassen.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

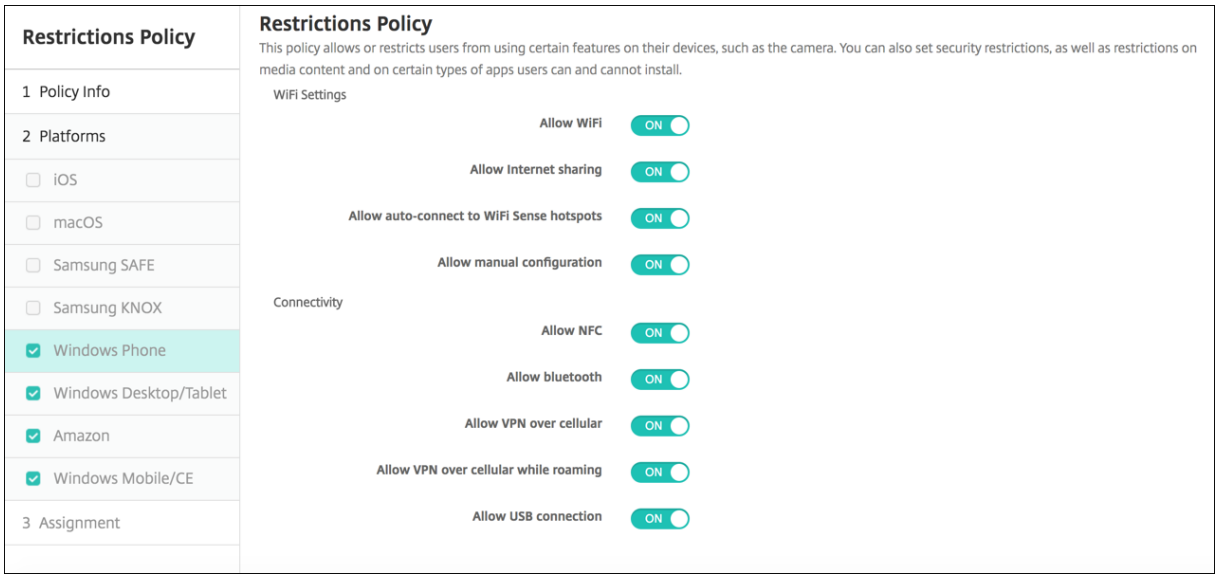
Samsung KNOX-Einstellungen



Diese Optionen stehen nur unter Samsung KNOX Premium (KNOX 2.0) zur Verfügung.

- **Verwendung der Kamera zulassen:** Verwendung der Kamera auf Geräten zulassen.
- **Sperrprüfung zulassen:** Prüfung auf gesperrte Zertifikate aktivieren.
- **Apps in Container verschieben:** Verschieben von Apps zwischen dem KNOX-Container und dem privaten Bereich auf Geräten zulassen.
- **Multifaktorauthentifizierung erzwingen:** Benutzer müssen einen Fingerabdruck und eine weitere Authentifizierungsmethode, z. B. Kennwort oder PIN zum Öffnen ihrer Geräte verwenden.
- **TIMA-Schlüsselspeicher aktivieren:** Der TIMA-Schlüsselspeicher bietet einen TrustZone-basierten, sicheren Speicher für symmetrische Schlüssel. RSA-Schlüsselpaare und -Zertifikate werden zur Speicherung an den Standard-Schlüsselspeicheranbieter geleitet.
- **Authentifizierung für Container erzwingen:** Verwendung einer separaten Authentifizierung zum Öffnen des KNOX-Containers, die sich von der für das Entsperren des Geräts unterscheidet.
- **Freigabeliste:** Teilen von Inhalten zwischen Apps in der Liste “Freigeben über” zulassen.
- **Überwachungsprotokoll aktivieren:** Erstellen von Ereignisüberwachungsprotokollen für die forensische Analyse von Geräten aktivieren.
- **Sichere Tastatur verwenden:** Benutzer zur Verwendung einer sicheren Tastatur im KNOX-Container zwingen.
- **Google Apps aktivieren:** Download von Apps aus Google Mobile Services in den KNOX-Container zulassen.
- **Smartcardauthentifizierung für Browser:** Browserauthentifizierung auf Geräten mit Smartcardleser aktivieren.

Windows Phone- und Windows Desktop-/Tablet-Einstellungen



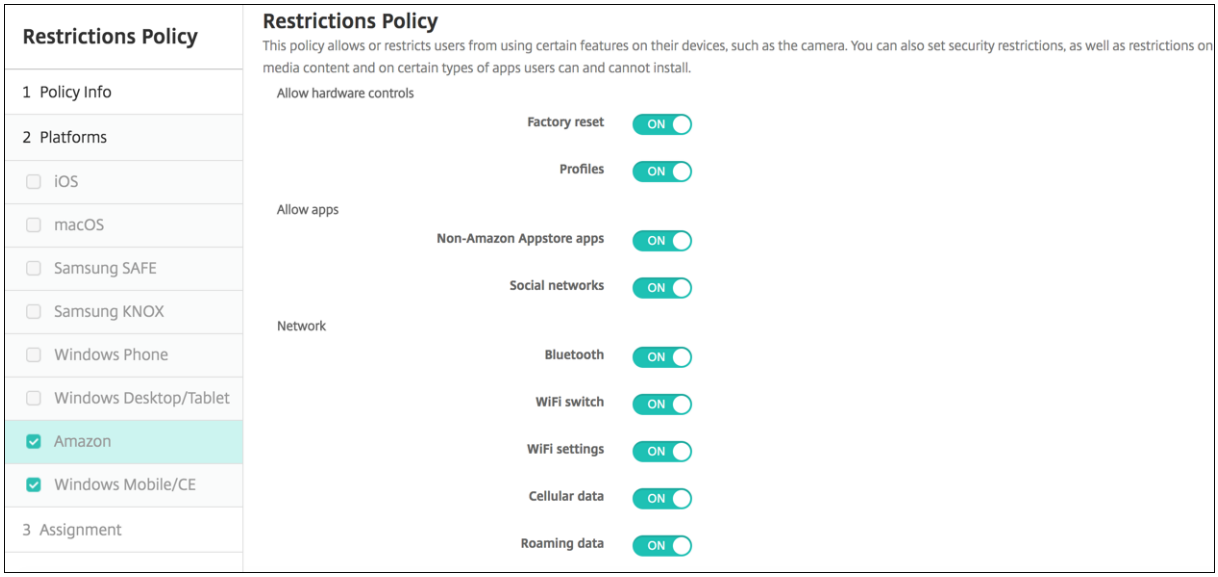
- **WiFi-Einstellungen**
  - **Wi-Fi zulassen:** Verbindung von Geräten mit einem Wi-Fi-Netzwerk zulassen. Nur für Windows Phone.
  - **Internetfreigabe zulassen:** gemeinsame Verwendung der Internetverbindung eines Geräts mit anderen Geräten durch Nutzung des Geräts als WiFi-Hotspot zulassen.
  - **Automatische Verbindung mit WiFi Sense-Hotspots zulassen:** automatische Verbindung von Geräten mit WiFi Sense-Hotspots zulassen. Für diese Option müssen Positionsdienste aktiviert sein. Weitere Informationen zu WiFi Sense für Windows Phone finden Sie in den FAQ zu WiFi Sense.
  - **Manuelle Konfiguration zulassen:** manuelle Konfiguration von WiFi-Verbindungen durch die Benutzer zulassen. Nur für Windows Phone.
- **Verbindungen**
  - **NFC zulassen:** Kommunikation zwischen Geräten und NFC-Tags (Near Field Communication) oder NFC-Sendern zulassen. Nur für Windows Phone.
  - **Bluetooth zulassen:** Verbindungen von Geräten über Bluetooth zulassen. Nur für Windows Phone.
  - **VPN über Mobilnetz zulassen:** Verbindungen zwischen Geräten über ein VPN mit einem mobilen Netzwerk zulassen.
  - **Beim Roaming VPN über Mobilnetz zulassen:** Verbindungen von Geräten über ein VPN im Roamingbetrieb zulassen.
  - **USB-Verbindung zulassen:** Verbindungen zwischen Desktop und Gerätespeicher über USB zulassen. Nur für Windows Phone.
  - **Datenroaming über Mobilnetz zulassen:** Verwendung mobiler Daten beim Roaming zulassen.

- **Konten**
  - **Microsoft-Kontoverbindung zulassen:** Verwendung eines Microsoft-Kontos durch Geräte für Verbindungsauthentifizierung und Dienste ohne E-Mail-Bezug zulassen.
  - **Nicht-Microsoft-E-Mail zulassen:** Hinzufügen Microsoft-externer E-Mail-Konten durch die Benutzer zulassen.
- **Suche:** nur für Windows Phone.
  - **Suche darf Standort verwenden:** Verwendung des Gerätepositionsdiensts durch die Suche zulassen.
  - **Nicht jugendfreie Inhalte filtern:** nicht jugendfreien Inhalt zulassen. Die Standardeinstellung ist **Aus**, d. h. nicht jugendfreier Inhalt wird nicht gefiltert.
  - **Bing Vision darf Bild speichern:** Speichern von bei Bing Vision-Suchen erfassten Bildern zulassen.
- **System**
  - **Speicherkarte zulassen:** Verwendung einer Speicherkarte durch Geräte zulassen.
  - **Telemetrie:** Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken des Versands von Telemetrieinformationen durch Geräte. Die Standardeinstellung ist **Zugelassen**. Andere Optionen sind **Nicht zugelassen** und **Zulässig, außer für sekundäre Datenanforderungen**.
  - **Ortungsdienste zulassen:** Ortungsdienste zulassen.
  - **Vorschau interner Builds zulassen:** Anzeige einer Vorschau interner Microsoft-Builds zulassen.
- **Kamera:** nur für Windows Desktop/Tablet.
  - **Verwenden der Kamera zulassen:** Verwendung der Gerätekamera durch Benutzer zulassen.
- **Bluetooth:** nur für Windows Desktop/Tablet.
  - **Sichtbaren Modus zulassen:** Auffinden des lokalen Geräts durch Bluetooth-Geräte zulassen.
  - **Lokaler Gerätename:** Name für das lokale Gerät.
- **Sicherheit:** nur für Windows Phone.
  - **Manuelle Installation des Stammzertifikats zulassen:** manuelle Installation eines Stammzertifikats durch Benutzer zulassen.
  - **Geräteverschlüsselung erforderlich:** Geräteverschlüsselung erzwingen. Wenn die Verschlüsselung auf einem Gerät aktiviert wurde, kann sie nicht wieder deaktiviert werden. Die Standardeinstellung ist **Aus**.
  - **Kopieren und einfügen zulassen:** Kopieren und Einfügen von Daten auf Geräten zulassen.
  - **Bildschirmaufnahme zulassen:** Erstellen von Screenshots auf Geräten zulassen.
  - **Sprachaufzeichnung zulassen:** Sprachaufzeichnung auf Geräten zulassen.
  - **Speichern unter von Office-Dateien zulassen:** Speichern von Office-Dateien mit der Op-

tion “Speichern unter” zulassen.
  - **Wartungscenterbenachrichtigungen zulassen:** Anzeige von Action Center-Benachrichtigungen auf dem Sperrbildschirm zulassen.
  - **Cortana zulassen:** Verwendung des intelligenten persönlichen Assistenten und Wissensnavigators Cortana auf Geräten zulassen.
  - **Synchronisieren von Geräteeinstellungen zulassen:** Synchronisierung von Einstellungen zwischen Windows Phone 8.1-Geräten im Roamingbetrieb zulassen.
- **Erfahrung:** nur für Windows Desktop/Tablet.
  - **Cortana zulassen:** Verwendung des intelligenten persönlichen Assistenten und Wissensnavigators Cortana auf Geräten zulassen.
  - **Gerätesuche zulassen:** Gerätesuche im Netzwerk zulassen.
  - **Manuelles Aufheben der MDM-Registrierung zulassen:** manuelles Aufheben der Registrierung eines Geräts bei XenMobile MDM zulassen.
  - **Synchronisieren von Geräteeinstellungen zulassen:** Synchronisierung von Einstellungen zwischen Windows 10- und Windows 11-Geräten im Roamingbetrieb zulassen.
- **Bei gesperrtem Gerät:** nur für Windows Desktop/Tablet.
  - **Popups zulassen:** Popup-Benachrichtigungen auf dem Sperrbildschirm zulassen. Nur für Windows Desktop/Tablet.
- **Apps**
  - **Storezugriff zulassen:** Zugriff auf Microsoft Store zulassen. Nur für Windows Phone.
  - **Entsperren durch Entwickler zulassen:** Registrierung von Geräten bei Microsoft und Entwicklung oder Installation von Apps, die nicht im App-Store für Windows Phone sind, zulassen. Nur für Windows Phone.
  - **Webbrowserzugriff zulassen:** Internet Explorer auf Geräten zulassen. Nur für Windows Phone.
  - **Automatische Updates vom App-Store zulassen:** Automatische Aktualisierung von Apps aus dem App-Store zulassen. Nur für Windows Desktop/Tablet.
- **Datenschutz:** nur für Windows Desktop/Tablet.
  - **Eingabepersonalisierung zulassen:** Ausführung der Eingabepersonalisierung zulassen, um die Eingabevorhersage (zum Beispiel für Stift und Bildschirmtastatur) je nach Eingabe des Benutzers weiter zu verbessern.
- **Einstellungen:** nur für Windows Desktop/Tablet.
  - **Autom. Wiedergabe zulassen:** Änderung der Einstellungen für die automatische Wiedergabe zulassen.
  - **Datenoptimierung zulassen:** Änderung der Einstellungen für die Datenoptimierung zulassen.
  - **Datum und Uhrzeit zulassen:** Änderung der Einstellungen für die Zeitangabe zulassen.
  - **Sprache zulassen:** Änderung der Spracheinstellungen zulassen.
  - **Ruhezustand zulassen:** Änderung der Energie- und Standby-Einstellungen zulassen.

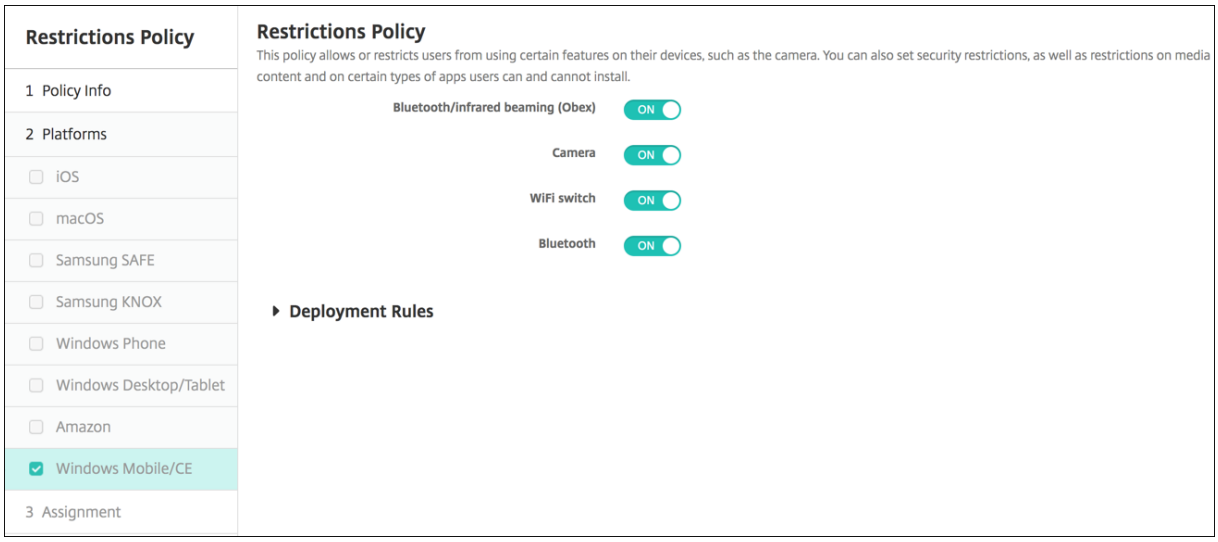
- **Region zulassen:** Änderung der Regionseinstellungen zulassen.
- **Anmeldeoptionen zulassen:** Änderung der Anmeldeeinstellungen zulassen.
- **Unternehmensbereich zulassen:** Änderung der Unternehmensbereichseinstellungen zulassen.
- **Ihr Konto zulassen:** Änderung der Kontoeinstellungen zulassen.

Amazon-Einstellungen



- **Hardwaresteuerelemente zulassen**
  - **Zurücksetzen auf Herstellereinstellungen:** Zurücksetzen der Geräte auf die werkseitige Voreinstellung zulassen.
  - **Profile:** Ändern des Hardwareprofils auf Geräten zulassen.
- **Apps zulassen**
  - **Apps nicht aus dem Amazon App-Shop:** Installation von Apps, die nicht aus dem Amazon App-Shop stammen, auf Geräten zulassen.
  - **Soziale Netzwerke:** Zugriff auf soziale Netzwerke von den Geräten aus zulassen.
- **Netzwerk**
  - **Bluetooth:** Verwendung von Bluetooth zulassen.
  - **WiFi-Switch:** Wechseln des WiFi-Verbindungszustands durch Apps zulassen.
  - **WiFi-Einstellungen:** Ändern der WiFi-Einstellungen zulassen.
  - **Mobile Daten:** Verwendung der Mobilfunkverbindung für Daten zulassen.
  - **Roamingdaten:** Verwendung mobiler Daten beim Roaming zulassen.
  - **Ortungsdienste:** GPS-Verwendung zulassen.
- **USB-Aktionen:**
  - **Debugging:** USB-Verbindungen mit einem Computer für das Debugging zulassen.

Windows Mobile-/CE-Einstellungen



- **Bluetooth-/Infrarotübertragung (OBEX):** OBEX (OBject EXchange Protocol) über Bluetooth oder Infrarot für den Austausch von Daten zwischen Geräten aktivieren.
- **Kamera:** Verwendung der Kamera auf Geräten zulassen.
- **WiFi-Switch:** Wechsel zwischen WiFi-Netzwerken zulassen.
- **Bluetooth:** Bluetooth auf Geräten zulassen.
- **Kamera:** Verwendung der Kamera auf Geräten zulassen.
- **WiFi-Switch:** Wechsel zwischen WiFi-Netzwerken zulassen.
- **Bluetooth:** Bluetooth auf Geräten zulassen.

Roamingrichtlinie

October 25, 2018

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Sprachroaming deaktivieren:** Wählen Sie aus, ob das Sprachroaming deaktiviert werden soll. Wird diese Option deaktiviert, dann wird Datenroaming automatisch auch deaktiviert. Die Stan-

dardeinstellung 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.

Windows Mobile-/CE-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.

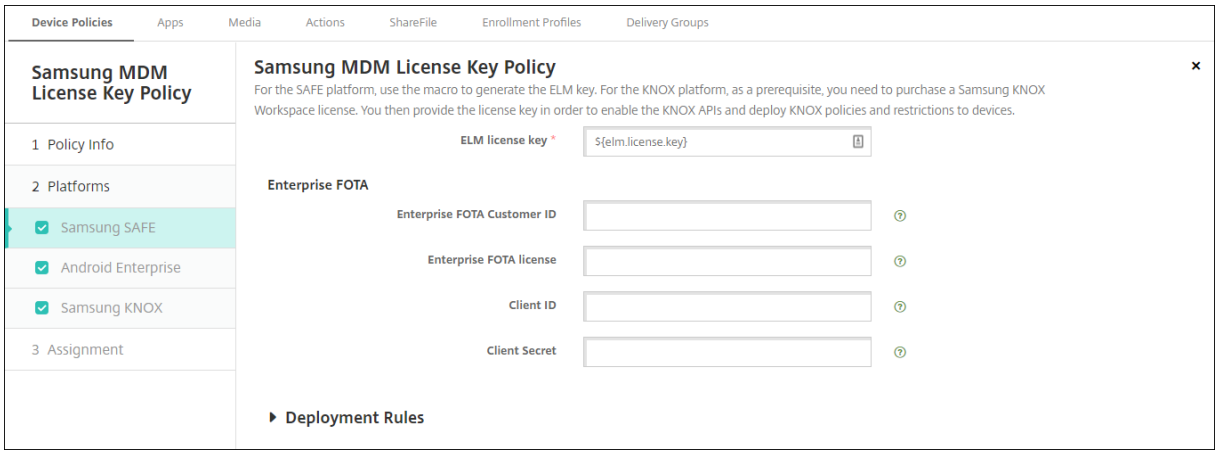
Geräterichtlinie für Samsung MDM-Lizenzschlüssel

January 5, 2022

Hiermit wird der integrierte Samsung Enterprise License Management-Schlüssel (ELM) festgelegt, der auf Geräten bereitgestellt werden muss, bevor Sie SAFE-Richtlinien und -Einschränkungen bereitstellen können. XenMobile unterstützt zudem den Dienst Samsung E-FOTA (Enterprise Firmware-Over-The-Air). XenMobile unterstützt und erweitert Samsung for Enterprise- (SAFE) und Samsung KNOX-Richtlinien.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Samsung SAFE-Einstellungen



- **ELM-Lizenzschlüssel:** XenMobile füllt dieses Feld mit dem Makro zur Erstellung des ELM-Lizenzschlüssels aus. Wenn das Feld leer ist, geben Sie das Makro "${elm.license.key}" ein.

Konfigurieren der Samsung E-FOTA-Einstellungen

Mit Samsung Enterprise Firmware-Over-The-Air (E FOTA) können Sie festlegen, wann Geräte ein Upgrade erhalten sollen und welche Firmwareversion verwendet werden soll. Mit E FOTA können Sie Updates vor dem Bereitstellen auf Kompatibilität mit Ihren Apps testen. Sie können ein Update mit der aktuellen Firmwareversion erzwingen, ohne dass Benutzerinteraktion erforderlich ist.

Samsung unterstützt E FOTA für Samsung Knox 2.7.1-Geräte (Mindestversion), auf denen autorisierte Firmware ausgeführt wird.

XenMobile unterstützt das Hinzufügen von Geräten von der XenMobile-Konsole zu Knox E-FOTA One. Weitere Informationen zum Exportieren einer Geräteliste aus XenMobile finden Sie unter Exportieren der Gerätetabelle. Weitere Informationen zum Hinzufügen eines Geräts zu Knox E-FOTA One finden Sie in der Samsung-Dokumentation.

XenMobile unterstützt die Knox E-FOTA nicht in MDM.

Konfigurieren einer E FOTA-Richtlinie

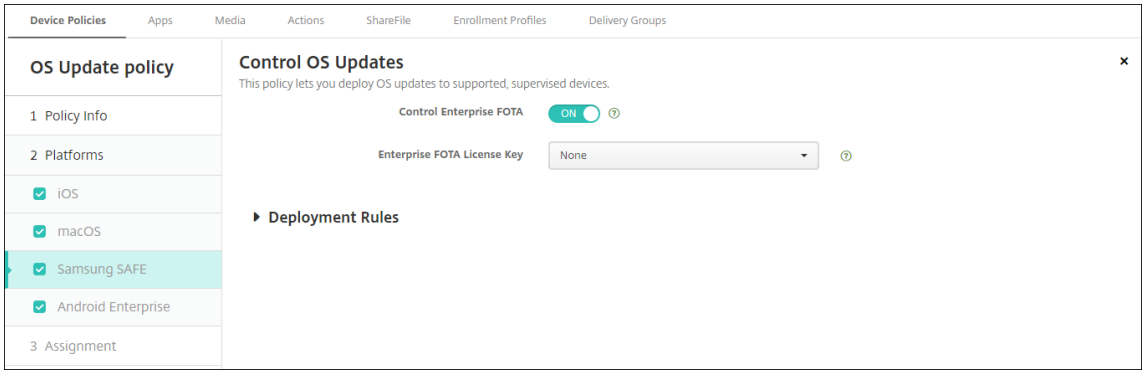
1. Erstellen Sie eine Geräterichtlinie für Samsung-MDM-Lizenzschlüssel mit den Schlüsseln und Lizenzinformationen, die Sie von Samsung erhalten haben. XenMobile Server validiert und registriert dann diese Informationen. Wenn XenMobile ein E-FOTA-Problem erkennt, wird eine entsprechende Fehlermeldung angezeigt. Behandeln Sie das Problem unter Verwendung des angezeigten Codes. Weitere Informationen finden Sie im Developer Guide.

   ELM-Lizenzschlüssel: XenMobile füllt das Feld mit dem Makro zur Erstellung des ELM-Lizenzschlüssels aus. Wenn das Feld leer ist, geben Sie das Makro "${elm.license.key}" ein.

Geben Sie die folgenden, von Samsung beim Kauf des E-FOTA-Pakets erhaltenen Informationen ein:

- **Enterprise FOTA-Kunden-ID**
- **Enterprise FOTA-Lizenz**
- **Client-ID**
- **Geheimer Clientschlüssel**

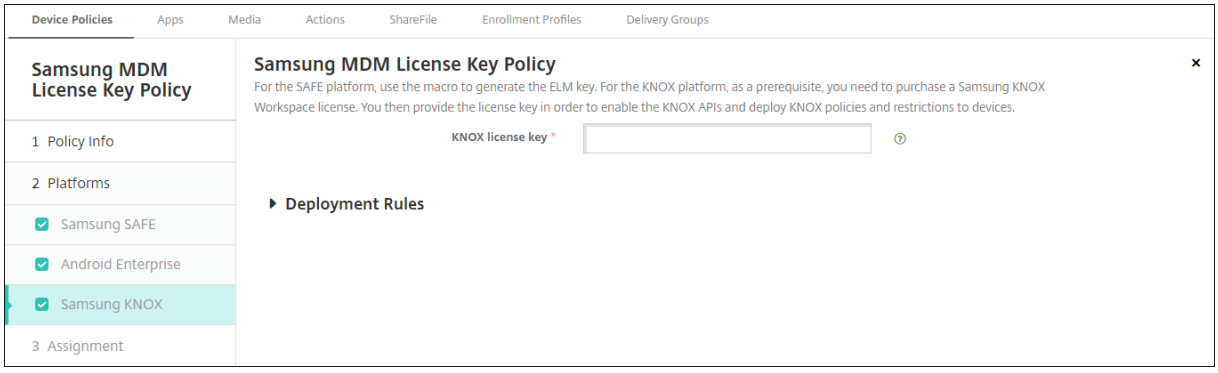
2. Erstellen Sie optional eine Geräterichtlinie “OS-Update steuern”.



- **Enterprise FOTA:** Wählen Sie **Ein**.
- **Enterprise FOTA-Lizenzschlüssel:** Wählen Sie den Namen der in Schritt 1 erstellten Samsung MDM-Lizenzschlüsselrichtlinie.

3. Stellen Sie die “OS-Update steuern”-Richtlinie in Secure Hub bereit.

Einstellungen für Android Enterprise und Samsung KNOX



- **KNOX-Lizenzschlüssel:** Geben Sie den KNOX-Lizenzschlüssel ein, den Sie von Samsung erhalten haben.

Samsung SAFE-Firewallrichtlinie

July 15, 2020

Mit dieser Richtlinie können Sie die Firewall-Einstellungen für Samsung-Geräte konfigurieren. Geben Sie IP-Adressen, Ports und Hostnamen ein, die Sie blockieren oder zulassen möchten. Sie können außerdem Proxy- und Proxyumleitungseinstellungen konfigurieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Samsung SAFE-Einstellungen

- **Hosts zulassen/verweigern:** Klicken Sie für jeden Host, für den Sie den Zugriff zulassen oder blockieren möchten, auf **Hinzufügen** und konfigurieren Sie Folgendes:
  - **Hostname/IP-Adressbereich:** Der Hostname oder die IP-Adresse des gewünschten Hosts.
  - **Port/Portbereich:** Die Portnummer oder der Portbereich.
  - **Regelfilter zulassen/verweigern:** Klicken Sie auf **Positivliste**, um den Zugriff zuzulassen, oder auf **Sperrliste**, um den Zugriff zu blockieren.

    > **Hinweis:**
    > Die XenMobile Server-Konsole enthält im Englischen die Begriffe “Blacklist” und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.
- **Umleitungskonfiguration:** Für jeden Proxy, den Sie konfigurieren möchten, klicken Sie auf **Hinzufügen** und konfigurieren Sie Folgendes:
  - **Hostname/IP-Adressbereich:** Hostname oder die IP-Adresse für die Umleitung per Proxy.
  - **Port/Portbereich:** Portnummer oder der Portbereich für die Umleitung per Proxy.
  - **Proxy-IP:** IP-Adresse des Proxys für die Umleitung per Proxy.
  - **Proxyport:** Port des Proxys für die Umleitung per Proxy.
- **Proxykonfiguration**
  - **Proxy-IP:** IP-Adresse des Proxyservers.
  - **Port:** Port des Proxyservers.

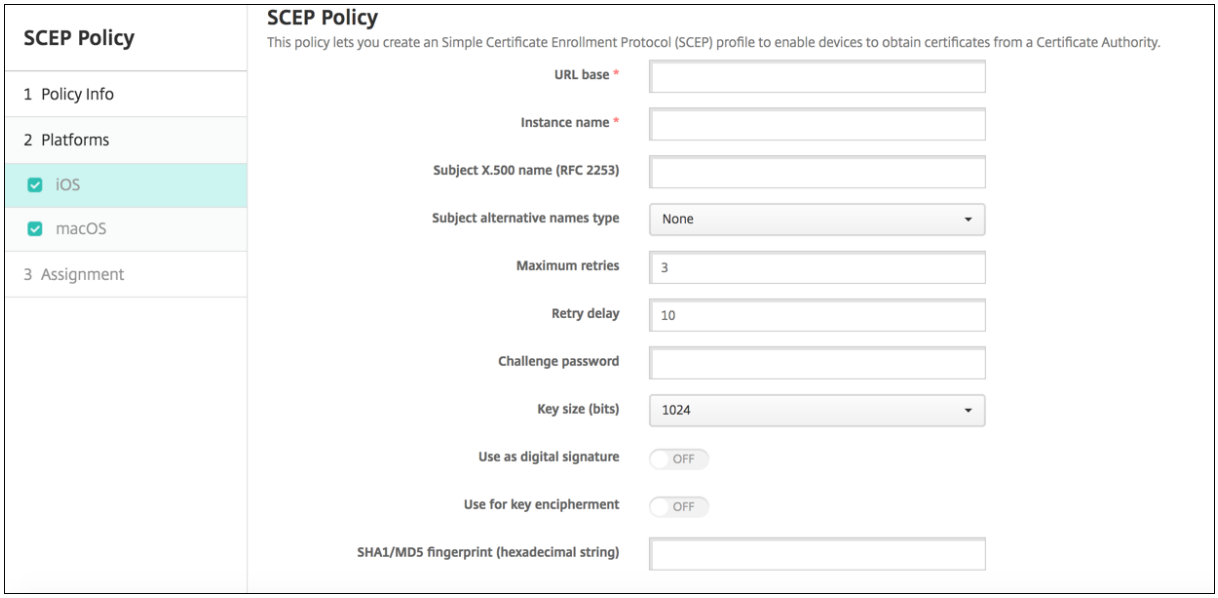
SCEP-Geräterichtlinie

January 5, 2022

Mit dieser Richtlinie können Sie iOS- und macOS-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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

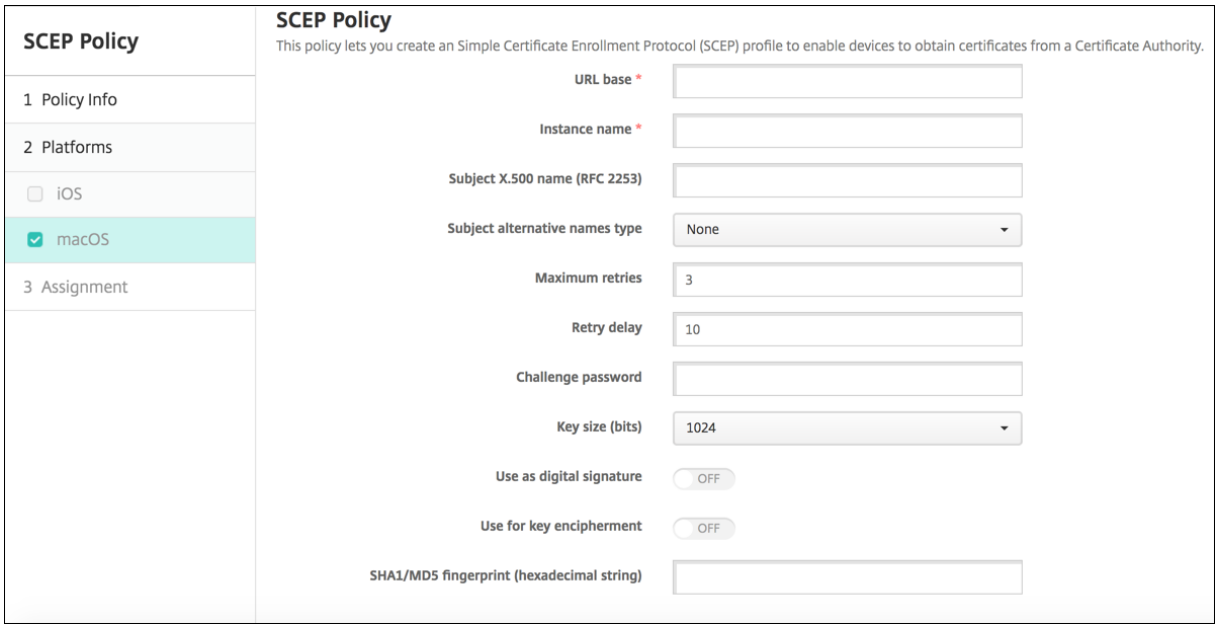
iOS-Einstellungen



- **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.

- **Alternativer Antragstellernamenstyp:** Klicken Sie in der Liste 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):** Wählen Sie **2048** oder höher als Schlüsselgröße in Bit.
- **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 dessen 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**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-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.
- **Alternativer Antragstellernamenstyp:** Klicken Sie in der Liste 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 Wiederhol-

ungsversuchen ein. Der erste Wiederholungsversuch erfolgt ohne Verzögerung. Der Standardwert ist **10**.

- **Kennwort überprüfen:** Geben Sie einen gemeinsamen geheimen Schlüssel ein.
- **Schlüsselgröße (Bit):** Wählen Sie **2048** oder höher als Schlüsselgröße in Bit.
- **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 dessen 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**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

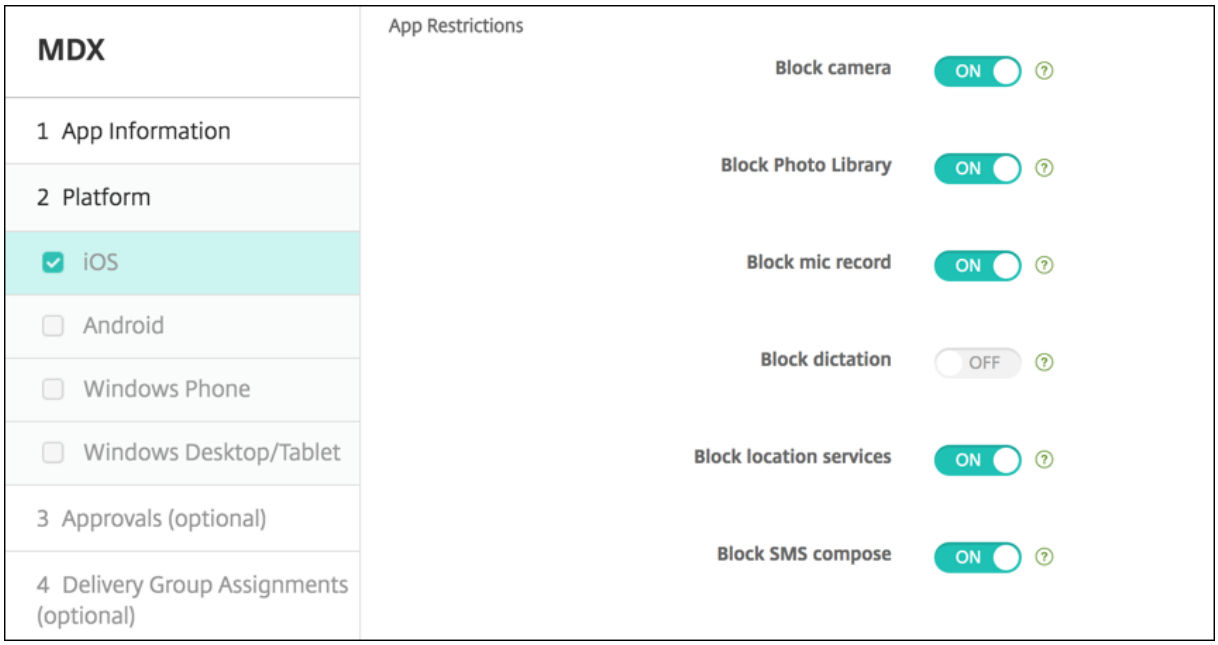
Richtlinien für Siri und die Diktierfunktion

January 5, 2022

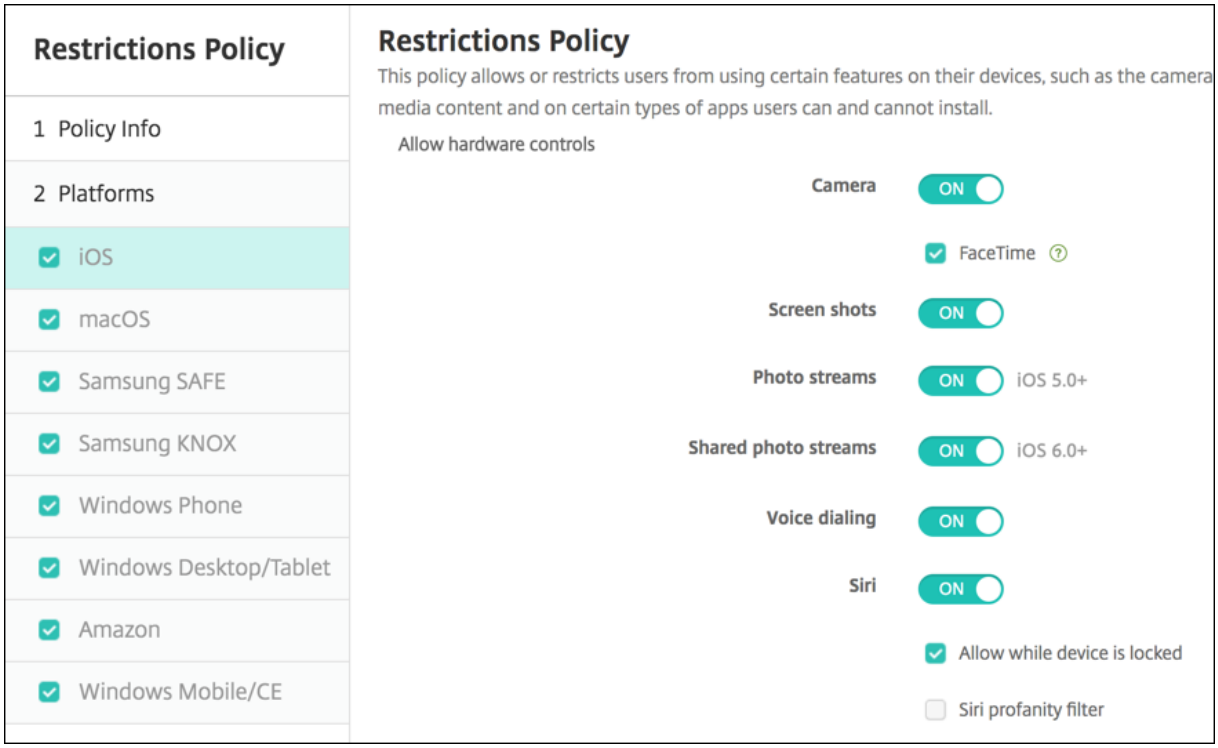
Wenn Benutzer auf einem iOS-Gerät Siri eine Frage stellen oder Text diktieren, werden die Sprachdaten von Apple zur Verbesserung von Siri gesammelt. Die Sprachdaten werden über die cloudbasierten Dienste von Apple gesendet und verlassen somit den sicheren XenMobile-Container. Diktierter Text verbleibt 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** 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 im 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.

SSO-Kontorichtlinie

April 16, 2020

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.

Die Richtlinie gilt nur ab iOS 7.0.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Kontoname:** Geben Sie den Kerberos-SSO-Kontonamen ein, der auf Benutzergeräten 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 über ein iOS-Gerät auf die URL zugreift.
    Wenn ein Benutzer beispielsweise zu einer Website navigiert und von dieser eine Kerberos-Aufforderung ausgegeben wird, unternimmt das iOS-Gerät keinen SSO-Versuch durch Angabe des möglicherweise auf dem Gerät bei einer vorherigen Kerberos-Anmeldung zwischengespeicherten Tokens, wenn sich die Website nicht in der URL-Liste befindet. Der Hostteil der URL muss genau übereinstimmen. `https://shopping.apple.com` ist beispielsweise gültig, `https://*.apple.com` ist nicht gültig.
    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 dieser 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.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.

* **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

Speicherverschlüsselungsrichtlinie für Geräte

January 21, 2021

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.

Sie können Richtlinien für Samsung SAFE- und Windows Phone-Geräte erstellen. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Artikel detailliert beschrieben.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Voraussetzungen

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 Benutzergeräte sind zu mindestens 80 % aufgeladen.
- Für die Geräte muss ein Kennwort mit Zahlen und Buchstaben oder Symbolen erforderlich sein.

Konfigurieren der Samsung SAFE-Einstellungen

- **Internen Speicher verschlüsseln:** Wählen Sie aus, ob der interne Speicher auf Geräten verschlüsselt werden soll. Zum internen Speicher gehört auch der Gerätespeicher. Die Standardeinstellung ist **Ein**.
- **Externen Speicher verschlüsseln:** Wählen Sie aus, ob der externe Speicher auf Geräten verschlüsselt werden soll. Die Standardeinstellung ist **Ein**.

Windows Phone-Einstellungen

- **Geräteverschlüsselung erforderlich:** Wählen Sie aus, ob die Geräte der Benutzer verschlüsselt werden sollen. Die Standardeinstellung ist **Aus**.
- **Speicherkarte deaktivieren:** Wählen Sie aus, ob die Verwendung der Speicherkarte der Geräte unterbunden werden soll. Die Standardeinstellung ist **Aus**.

Store-Geräterichtlinie

January 5, 2022

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 werden soll.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Plattformeinstellungen

Legen Sie für jede Plattform, die Sie konfigurieren, fest, ob ein XenMobile Store-Webclip auf den Geräten angezeigt werden soll. Die Standardeinstellung ist **Ein**.

Richtlinie für abonnierte Kalender

January 5, 2022

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Voraussetzung

Sie müssen einen Kalender zunächst abonnieren, bevor Sie ihn der Liste der abonnierten Kalender auf den Geräten der Benutzer hinzufügen können.

iOS-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 `https://`-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. Die Standardeinstellung ist **Aus**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

AGB-Geräterichtlinie

January 5, 2022

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS- und Android-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. Die Standardeinstellung ist **Aus**.

Windows Phone- und Windows Tablet-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. Die Standardeinstellung ist **Aus**.

VPN-Geräterichtlinie

January 5, 2022

Mit der VPN-Geräterichtlinie konfigurieren Sie die Einstellungen für ein VPN (virtuelles privates Netzwerk) für eine sichere Verbindung zwischen Geräten und Unternehmensressourcen. Sie können die VPN-Richtlinie für die nachstehenden Plattformen konfigurieren. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Artikel detailliert beschrieben.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Anforderungen für Pro-App-VPNs

Sie konfigurieren die Pro-App-VPN-Funktion für die folgenden Plattformen über VPN-Richtlinien:

- iOS
- macOS
- Android (Legacy-Geräteadmin)
- Samsung SAFE
- Samsung Knox

Zum Konfigurieren von VPNs für Android Enterprise-Geräte erstellen Sie für die Citrix SSO-App eine Geräterichtlinie für verwaltete Android Enterprise-Konfigurationen. Weitere Informationen unter Konfigurieren von VPN-Profilen für Android Enterprise.

Für bestimmte Verbindungstypen stehen Pro-App-VPN-Optionen zur Verfügung. In der folgenden Tabelle wird angegeben, wann Pro-App-VPN-Optionen verfügbar sind.

Plattform	Verbindungstyp	Anmerkung
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO oder benutzerdefiniertes SSL.	
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA oder benutzerdefiniertes SSL.	
Android (Legacy-Geräteadmin)	Citrix SSO	
Samsung SAFE	IPSEC, SSL	VPN-Typ ist auf **Generic** eingestellt
Samsung Knox	IPSEC, SSL	VPN-Typ ist auf **Generic** eingestellt

Um ein Pro-App-VPN für iOS- und Android-Geräte (Legacy-DA) mit der Citrix SSO-App zu erstellen, müssen Sie zusätzlich zur VPN-Richtlinienkonfiguration einige Schritte ausführen. Außerdem müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- On-Premises Citrix Gateway
- Die folgenden Anwendungen sind auf dem Gerät installiert:
  - Citrix SSO
  - Citrix Secure Hub

Ein allgemeiner Workflow zur Konfiguration eines Pro-App-VPN für iOS- und Android-Geräte mit der Citrix SSO-App ist wie folgt:

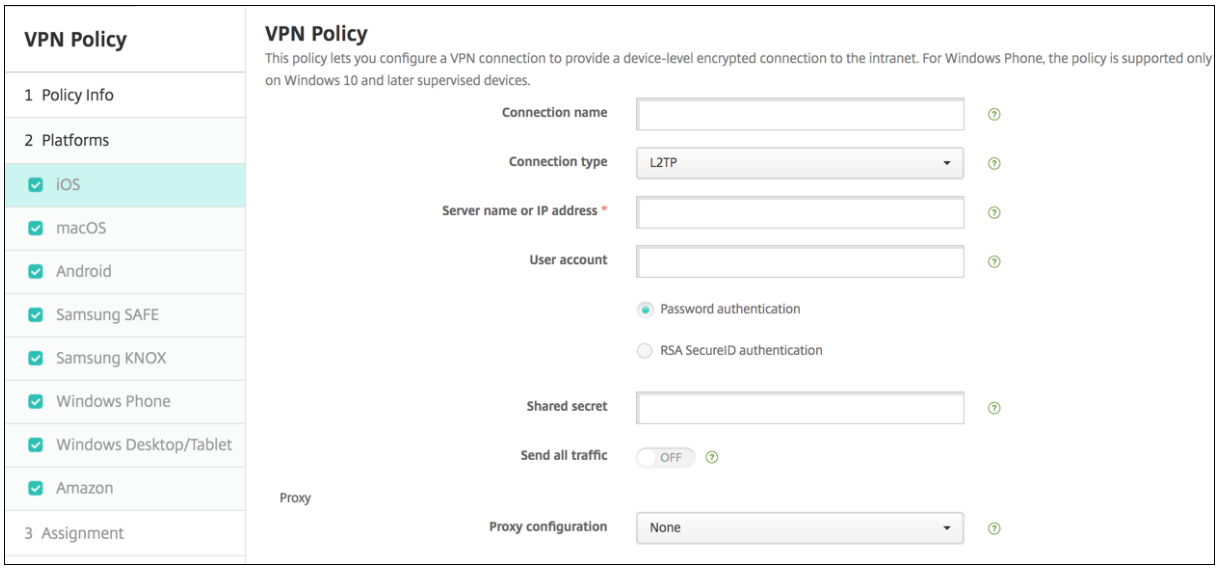
1. Konfigurieren Sie eine VPN-Geräterichtlinie wie in diesem Artikel beschrieben.
   - Informationen zu *iOS* finden Sie unter Konfigurieren des Citrix SSO-Protokolls für iOS. Nachdem Sie das Citrix SSO-Protokoll für iOS über eine VPN-Geräterichtlinie konfiguriert haben, müssen Sie auch eine App-Attributrichtlinie erstellen, um eine App mit der Pro-App-VPN-Richtlinie zu verknüpfen. Weitere Informationen finden Sie unter Konfigurieren des Pro-App-VPN-Zugriffs.
     - Wenn Sie für **Authentifizierungstyp für Verbindung** die Option **Zertifikat** auswählen, müssen Sie zuerst die zertifikatbasierte Authentifizierung für Endpoint Management konfigurieren. Siehe Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne.

- Informationen zu *Android (Legacy-Geräteadmin)* finden Sie unter Konfigurieren des Citrix SSO-Protokolls für Android.
  - Wenn Sie für **Authentifizierungstyp für Verbindung** die Option **Zertifikat** oder **Kennwort und Zertifikat** auswählen, müssen Sie zuerst die zertifikatbasierte Authentifizierung für Endpoint Management konfigurieren. Siehe Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne.

2. Konfigurieren Sie Citrix ADC so, dass es Datenverkehr vom Pro-App-VPN akzeptiert. Weitere Informationen finden Sie unter Setup des vollständigen VPNs in Citrix Gateway.

iOS-Einstellungen

> **Vorbereitung von Geräteupgrades auf iOS 12:**
>
> Der Verbindungstyp “Citrix VPN” in der VPN-Geräterichtlinie für iOS unterstützt iOS 12 nicht. Mit diesen Schritten löschen Sie Ihre VPN-Geräterichtlinie und erstellen eine neue mit dem Verbindungstyp “Citrix SSO”:
>
> 1. Löschen Sie Ihre VPN-Geräterichtlinie für iOS.
> 2. Fügen Sie eine VPN-Geräterichtlinie für iOS hinzu. Wichtige Einstellungen:
>   - **Connection type** = **Citrix SSO**
>   - **Enable per-app VPN** = **On**
>   - **Provider type** = **Packet tunnel**
> 3. Fügen Sie eine Geräterichtlinie “App-Attribute” für iOS hinzu. Wählen Sie für **ID für VPN-Zugriff pro App** die Option **iOS_VPN**.



- **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 Legacy AnyConnect:** Dieser Verbindungstyp erfordert, dass der Cisco AnyConnect VPN-Client auf dem Benutzergerät installiert ist. Cisco lässt den Cisco Legacy AnyConnect-Client auslaufen, der auf einem mittlerweile veralteten VPN-Framework basiert. Weitere Informationen finden Sie im Supportartikel https://support.citrix.com/article/CTX227708. Zur Verwendung des aktuellen Cisco AnyConnect-Clients wählen Sie als **Verbindungstyp** die Option **Benutzerdefiniertes SSL**. Die erforderlichen Einstellungen finden Sie unter "Konfigurieren des benutzerdefinierten SSL-Protokolls" in diesem Abschnitt.
- **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.
- **AlwaysOn IKEv2:** Always-on-Zugriff mit IKEv2.
- **AlwaysOn IKEv2-Doppelkonfiguration:** Always-on-Zugriff über IKEv2-Doppelkonfiguration.
- **Citrix SSO:** Citrix SSO-Client für iOS 12 und höher.
- **Benutzerdefiniertes SSL:** benutzerdefiniertes Secure Socket Layer. Dieser Verbindungstyp ist für den Cisco AnyConnect-Client mit Paket-ID **com.cisco.anyconnect** erforderlich. Geben Sie einen **Verbindungsnamen** für **Cisco AnyConnect** an. Sie können auch die VPN-Richtlinie bereitstellen und einen NAC-Filter (Network Access Control) für iOS-Geräte aktivieren. Der Filter blockiert eine VPN-Verbindung für Geräte, auf denen nicht richtlinientreue Apps installiert sind. Die Konfiguration erfordert spezifische Einstellungen für die iOS-VPN-Richtlinie (siehe folgenden Abschnitt "iOS"). Informationen zu weiteren Einstellungen, die zum Aktivieren des NAC-Filters erforderlich sind, finden Sie unter Netzwerkzugriffssteuerung.

In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt.

Konfigurieren von L2TP für iOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- Wählen Sie **Kennwortauthentifizierung** oder **RSA SecurID-Authentifizierung**.
- **Gemeinsamer geheimer Schlüssel:** Geben Sie den gemeinsamen geheimen Schlüssel für IPsec ein.
- **Gesamten Datenverkehr senden:** Wählen Sie aus, ob der gesamte Datenverkehr über das VPN

geleitet werden soll. Die Standardeinstellung ist **Aus**.

Konfigurieren von PPTP für iOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- Wählen Sie **Kennwortauthentifizierung** oder **RSA SecurID-Authentifizierung**.
- **Verschlüsselungsgrad:** Wählen Sie in der Liste einen Verschlüsselungsgrad aus. Die Standardeinstellung ist **Ohne**.
  - **Ohne:** keine Verschlüsselung verwenden.
  - **Automatisch:** den höchsten vom Server unterstützten Verschlüsselungsgrad verwenden.
  - **Maximum (128 Bit):** Immer 128-Bit-Verschlüsselung verwenden.
- **Gesamten Datenverkehr senden:** Wählen Sie aus, ob der gesamte Datenverkehr über das VPN geleitet werden soll. Die Standardeinstellung ist **Aus**.

Konfigurieren von IPsec für iOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Gemeinsamer geheimer Schlüssel** oder **Zertifikat** aus. Die Standardeinstellung ist **Gemeinsamer geheimer Schlüssel**.
- Bei Auswahl von **Gemeinsamer geheimer Schlüssel** konfigurieren Sie die folgenden Einstellungen:
  - **Gruppenname:** Geben Sie optional einen Gruppennamen ein.
  - **Gemeinsamer geheimer Schlüssel:** Geben Sie optional einen gemeinsamen geheimen Schlüssel ein.
  - **Hybride Authentifizierung:** Wählen Sie aus, ob die Hybridauthentifizierung verwendet werden soll. Bei der hybriden Authentifizierung authentifiziert sich der Server zuerst beim Client und der Client authentifiziert sich dann beim Server. Die Standardeinstellung ist **Aus**.
  - **Zur Kennworteingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihres Kennworts aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
- Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
  - **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
  - **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer ihre PIN eingeben müssen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.

  - **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf für iOS.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**.
- **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.
- **Safari-Domänen:** Klicken Sie auf **Hinzufügen**, um einen Safari-Domänennamen hinzuzufügen.

Konfigurieren von Cisco Legacy AnyConnect für iOS

Für einen Wechsel vom Cisco Legacy AnyConnect-Client zum neuen Cisco AnyConnect-Client verwenden Sie das benutzerdefinierte SSL-Protokoll.

- **Anbieterpaket-ID:** Die Paket-ID für den Legacy AnyConnect-Client ist com.cisco.anyconnect.gui.
- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Gruppe:** Geben Sie optional einen Gruppennamen ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf für iOS.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-

Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.

- **Anbietertyp:** Wählen Sie, ob das Pro-App-VPN als **App-Proxy** oder als **Pakettunnel** bereitgestellt wird. Die Standardeinstellung ist **App-Proxy**.
- **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
  * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren von Juniper SSL für iOS

- **Anbieterpaket-ID:** Wenn das Profil für das Pro-App-VPN die Paket-ID einer App enthält, für die es mehrere VPN-Anbieter desselben Typs gibt, geben Sie hier den zu verwendenden Anbieter an.
- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Bereich:** Geben Sie optional einen Bereichsnamen ein.
- **Rolle:** Geben Sie optional einen Rollennamen ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf für iOS.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-

Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.

- **Anbietertyp:** Wählen Sie, ob das Pro-App-VPN als **App-Proxy** oder als **Pakettunnel** bereitgestellt wird. Die Standardeinstellung ist **App-Proxy**.
- **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
  * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren von F5 SSL für iOS

- **Anbieterpaket-ID:** Wenn das Profil für das Pro-App-VPN die Paket-ID einer App enthält, für die es mehrere VPN-Anbieter desselben Typs gibt, geben Sie hier den zu verwendenden Anbieter an.
- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf für iOS.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen.

  - **Anbietertyp:** Wählen Sie, ob das Pro-App-VPN als **App-Proxy** oder als **Pakettunnel** bereitgestellt wird. Die Standardeinstellung ist **App-Proxy**.
  - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
    * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren von SonicWALL für iOS

- **Anbieterpaket-ID:** Wenn das Profil für das Pro-App-VPN die Paket-ID einer App enthält, für die es mehrere VPN-Anbieter desselben Typs gibt, geben Sie hier den zu verwendenden Anbieter an.
- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Anmeldegruppe oder -domäne:** Geben Sie optional eine Anmeldegruppe oder -domäne ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf für iOS.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen.
  - **Anbietertyp:** Wählen Sie, ob das Pro-App-VPN als **App-Proxy** oder als **Pakettunnel** bereitgestellt wird. Die Standardeinstellung ist **App-Proxy**.

  - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
    * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren von Ariba VIA für iOS

- **Anbieterpaket-ID:** Wenn das Profil für das Pro-App-VPN die Paket-ID einer App enthält, für die es mehrere VPN-Anbieter desselben Typs gibt, geben Sie hier den zu verwendenden Anbieter an.
- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf für iOS.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen.
  - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
    * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den

Vorgang abzubrechen.

Konfigurieren von IKEv2-Protokollen für iOS

Dieser Abschnitt enthält Informationen zu den Einstellungen für die Protokolle IKEv2, AlwaysOn IKEv2 und AlwaysOn IKEv2-Doppelkonfiguration. Konfigurieren Sie für AlwaysOn IKEv2-Doppelkonfiguration alle diese Einstellungen für Mobilfunk- und WLAN-Netzwerke.

- **Deaktivieren der automatischen Verbindung durch Benutzer zulassen:** für AlwaysOn-Protokolle. Wählen Sie, ob Benutzer das Herstellen einer automatischen Verbindung mit dem Netzwerk auf ihren Geräten deaktivieren können. Die Standardeinstellung ist **Aus**.
- **Hostname oder IP-Adresse des Servers:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Lokale ID:** Geben Sie den FQDN oder die IP-Adresse des IKEv2-Clients ein. Diese Angabe ist erforderlich.
- **Remote-ID:** Geben Sie den FQDN oder die IP-Adresse des VPN-Servers ein. Diese Angabe ist erforderlich.
- **Geräteauthentifizierung:** Wählen Sie **Gemeinsamer geheimer Schlüssel**, **Zertifikat** oder **Gerätezertifikat basiert auf Geräteidentität** als Authentifizierungstyp für die Verbindung aus. Die Standardeinstellung ist **Gemeinsamer geheimer Schlüssel**.
  - Wenn Sie **Gemeinsamer geheimer Schlüssel** auswählen, geben Sie einen gemeinsamen geheimen Schlüssel ein.
  - Bei Auswahl von **Zertifikat** wählen Sie die zu verwendenden **Identitätsanmeldeinformationen**. Die Standardeinstellung ist **Ohne**.
  - Wenn Sie **Gerätezertifikat basiert auf Geräteidentität** wählen, wählen Sie den zu verwendenden **Geräteidentitätstyp**. Der Standardwert ist **IMEI**. Zur Verwendung dieser Option importieren Sie Zertifikate en gros mit der REST-API. Siehe Massenupload von Zertifikaten mit der REST-API auf iOS-Geräte. Nur verfügbar, wenn Sie **Always On IKEv2** auswählen.
- **Erweiterte Authentifizierung aktiviert:** Wählen Sie aus, ob das Protokoll für erweiterte Authentifizierung (EAP) aktiviert werden soll. Bei Auswahl von **Ein** geben Sie das **Benutzerkonto** und das **Authentifizierungskennwort** ein.
- **DPD-Intervall (Dead Peer Detection):** Wählen Sie aus, wie oft eine Verbindung mit Peer-Geräten hergestellt werden soll, um sicherzustellen, dass die Geräte erreichbar bleiben. Die Standardeinstellung ist **Ohne**. Optionen:
  - **Ohne:** Dead Peer Detection ist deaktiviert.
  - **Niedrig:** Verbindung mit Peer alle 30 Minuten herstellen.

  - **Mittel:** Verbindung mit Peer alle 10 Minuten herstellen.
  - **Hoch:** Verbindung mit Peer jede Minute herstellen.

- **Mobilität und Multihoming deaktivieren:** Wählen Sie aus, ob dieses Feature deaktiviert werden soll.
- **Interne IPv4-/IPv6-Subnetzattribute verwenden:** Wählen Sie aus, ob dieses Feature aktiviert werden soll.
- **Umleitungen deaktivieren:** Wählen Sie aus, ob Umleitungen deaktiviert werden sollen.
- **NAT-Keep-Alive aktivieren, wenn Gerät im Standbymodus ist:** für AlwaysOn-Protokolle. Keep-Alive-Pakete behalten NAT-Zuordnungen für IKEv2-Verbindungen. Diese Pakete werden in regelmäßigen Abständen gesendet, wenn das Gerät im aktiven Zustand ist. Wenn diese Einstellung auf Ein festgelegt ist, werden Keep-Alive-Pakete auch dann gesendet, wenn das Gerät im Standbymodus ist. Der Standardwert ist 20 Sekunden über Wi-Fi und 110 Sekunden über das Mobilfunknetz. Sie können das Intervall über den Parameter NAT-Keep-Alive-Intervall ändern.
- **NAT-Keep-Alive Intervall (Sekunden):** Der Standardwert ist 20 Sekunden.
- **Perfect Forward Secrecy (PFS) aktivieren:** Wählen Sie, ob dieses Feature aktiviert werden soll.
- **IP-Adressen der DNS-Server:** optional. Liste der DNS-Server-IP-Adressen. Die Liste kann IPv4- und IPv6-Adressen enthalten. Klicken Sie auf **Hinzufügen**, um eine Adresse einzugeben.
- **Domänenname:** optional. Primäre Domäne des Tunnels.
- **Suchdomänen:** optional. Liste von Domänenzeichenfolgen, die verwendet werden, um einteilige Hostnamen vollständig zu qualifizieren.
- **Zusätzliche Domänen für Übereinstimmungen an Auflösungsliste anhängen:** optional. Legt fest, ob die zusätzlichen Domänen für Übereinstimmungen der Liste der Suchdomänen für die Auflösung hinzugefügt werden sollen. Die Standardeinstellung ist **Ein**.
- **Zusätzliche Domänen für Übereinstimmungen:** optional. Liste der Domänenzeichenfolgen zur Bestimmung der DNS-Abfragen, die die Einstellungen der DNS-Auflösung in den DNS-Serveradressen verwenden sollen. Der Schlüssel erstellt eine geteilte DNS-Konfiguration, bei der nur Hosts in bestimmten Domänen über die DNS-Auflösung des Tunnels aufgelöst werden. Hosts, die nicht auf der Liste stehen, werden unter Verwendung der Standard-Systemauflösung aufgelöst.

Wenn dieser Parameter eine leere Zeichenfolge enthält, wird diese Zeichenfolge als die Standarddomäne verwendet. Auf diese Weise werden durch die Split-Tunnel-Konfiguration alle DNS-Abfragen vor den primären DNS-Servern an die VPN-DNS-Server geleitet. Wenn der VPN-Tunnel die Stan-

dardroute des Netzwerks ist, werden die aufgelisteten DNS-Server zur Standardauflösung. Die zusätzlichen Domänen für Übereinstimmungen werden dann ignoriert.

- **IKE SA-Parameter** und **Untergeordnete SA-Parameter**. Konfigurieren Sie folgende Einstellungen für jeden Parameter der Sicherheitszuordnung (SA):
  - **Verschlüsselungsalgorithmus:** Wählen Sie in der Liste den IKE-Verschlüsselungsalgorithmus aus, der verwendet werden soll. Der Standardwert ist **3DES**.
  - **Integritätsalgorithmus:** Wählen Sie in der Liste den Integritätsalgorithmus aus, der verwendet werden soll. Die Standardeinstellung ist **SHA1-96**.
  - **Diffie Hellman-Gruppe:** Wählen Sie in der Liste die Diffie Hellman-Gruppennummer aus. Der Standardwert ist **2**.
  - **IKE-Lebensdauer in Minuten:** Geben Sie eine Ganzzahl zwischen 10 und 1440 für die SA-Lebensdauer ein (Intervall der Schlüsselerneuerung). Der Standardwert ist **1440** Minuten.
- **Dienstausnahmen:** für AlwaysOn-Protokolle. Dienstausnahmen sind Systemdienste, die vom Always-On-VPN ausgenommen sind. Konfigurieren Sie folgende Einstellungen für Dienstausnahmen:
  - **Voicemail:** Wählen Sie in der Liste die gewünschte Behandlung der Voicemail-Ausnahme aus. Der Standardwert ist **Datenverkehr über Tunnel zulassen**.
  - **AirPrint:** Wählen Sie in der Liste die gewünschte Behandlung der AirPrint-Ausnahme aus. Der Standardwert ist **Datenverkehr über Tunnel zulassen**.
  - **Datenverkehr von Captive-Websheet außerhalb des Tunnels zulassen**: Wählen Sie aus, ob Benutzern das Herstellen einer Verbindung mit öffentlichen Hotspots außerhalb des VPN-Tunnels gestattet werden soll. Die Standardeinstellung ist **Aus**.
  - **Datenverkehr von allen Captive-Netzwerk-Apps außerhalb des Tunnels zulassen**: Wählen Sie aus, ob alle Hotspot-Netzwerk-Apps außerhalb des VPN-Tunnels zugelassen werden sollen. Die Standardeinstellung ist **Aus**.
  - **Paket-ID für Captive-Netzwerk-App:** Klicken Sie zur Auswahl der einzelnen Paket-IDs der Hotspot-Netzwerk-Apps, auf die Benutzer zugreifen dürfen, auf **Hinzufügen** und geben Sie die **Paket-ID** der Hotspot-Netzwerk-App ein. Klicken Sie auf **Speichern**, um die App-Paket-ID zu speichern.
- **VPN-Zugriff pro App:** Konfigurieren Sie diese Einstellungen für IKEv2-Verbindungen
  - **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**.
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst

verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.
  - **Safari-Domänen:** Klicken Sie auf **Hinzufügen**, um einen Safari-Domänennamen hinzuzufügen.

- **Proxykonfiguration:** Wählen Sie nach Bedarf das Routing der VPN-Verbindung über einen Proxyserver aus. Standardwert ist **Ohne**.

Konfigurieren des Citrix SSO-Protokolls für iOS

Der Citrix SSO-Client steht hier im Apple-Store https://apps.apple.com/us/app/citrix-sso/id1333396910 zur Verfügung.

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf für iOS.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen.
  - **Anbietertyp:** Wählen Sie, ob das Pro-App-VPN als **App-Proxy** oder als **Pakettunnel** bereitgestellt wird. Die Standardeinstellung ist **App-Proxy**.
  - **Anbietertyp:** Legen Sie dies auf **Pakettunnel** fest.
  - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende

Schritte aus:

* **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
* Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **Benutzerdefiniertes XML:** Für jeden benutzerdefinierten XML-Parameter, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie das Schlüssel/Wert-Paar an. Folgende Parameter sind verfügbar:
  - **disableL3:** deaktiviert VPN auf Systemebene. Nur VPN-Zugriff pro App ist zulässig. Es ist kein **Wert** erforderlich.
  - **useragent:** Ordnet dieser Geräterichtlinie alle Citrix Gateway-Richtlinien zu, die auf VPN-Plug-In-Clients abzielen. Für die vom Plug-In initiierten Anfragen wird der **Wert** für diesen Schlüssel automatisch dem VPN-Plug-In hinzugefügt.

Konfigurieren des benutzerdefinierten SSL-Protokolls für iOS

Nutzen Sie folgende Schrittfolge für den Wechsel vom Cisco Legacy AnyConnect-Client zum Cisco AnyConnect-Client:

1. Konfigurieren Sie die VPN-Geräterichtlinie mit dem benutzerdefinierten SSL-Protokoll. Stellen Sie die Richtlinie auf iOS-Geräten bereit.
2. Laden Sie den Cisco AnyConnect-Client von https://apps.apple.com/us/app/cisco-anyconnect/id1135064690 hoch, fügen Sie die App zu XenMobile hinzu und stellen Sie sie dann auf iOS-Geräten bereit.
3. Entfernen Sie die alte VPN-Geräterichtlinie von iOS-Geräten.

Einstellungen:

- **Benutzerdefinierte SSL-ID (Reverse DNS-Format):** Legen Sie dies auf die Paket-ID fest. Verwenden Sie **com.cisco.anyconnect** für den Cisco AnyConnect-Client.
- **Anbieterpaket-ID:** Wenn die unter **Benutzerdefinierte SSL-ID** angegebene App mehrere VPN-Anbieter des gleichen Typs hat (App-Proxy oder Pakettunnel), geben Sie diese ID an. Verwenden Sie **com.cisco.anyconnect** für den Cisco AnyConnect-Client.
- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.

        * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
        * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf für iOS.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
    - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen.
    - **Anbietertyp:** Der Anbietertyp gibt an, ob es sich um einen VPN-Dienst oder einen Proxy-Dienst handelt. Wählen Sie für VPN-Dienst die Option **Pakettunnel**. Wählen Sie für Proxy-Dienst **App-Proxy**. Wählen Sie **Pakettunnel** für den Cisco AnyConnect-Client.
    - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
        * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
        * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Benutzerdefiniertes XML:** Für jeden benutzerdefinierten XML-Parameter, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
    - **Parametername:** Geben Sie den Namen des gewünschten Parameters ein.
    - **Wert:** Geben Sie den mit **Parametername** verknüpften Wert ein.
    - Klicken Sie auf **Speichern**, um den Parameter zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der VPN-Geräterichtlinie zur Unterstützung von NAC

1. Für die Konfiguration des NAC-Filters muss für den **Verbindungstyp** die Option **Benutzerdefiniertes SSL** verwendet werden.
2. Geben Sie für **Verbindungsname** die Option **VPN** an.
3. Geben Sie für **Benutzerdefinierte SSL-ID** den Text **com.citrix.NetScalerGateway.ios.app** ein.
4. Geben Sie für **Anbieterpaket-ID** den Text **com.citrix.NetScalerGateway.ios.app.vpnplugin** ein.

Die Werte in Schritt 3 und 4 entstammen der erforderlichen Citrix SSO-Installation für die NAC-

Filterung. Sie konfigurieren kein Authentifizierungskennwort. Weitere Informationen zur Verwendung der NAC-Funktion finden Sie unter Netzwerkzugriffssteuerung.

Konfigurieren der Optionen für "VPN bei Bedarf aktivieren" für iOS

- **On-Demand-Domäne:** Klicken Sie für jede gewünschte Domäne und Aktion, die beim Herstellen einer Verbindung erfolgen soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
- **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
- **Aktion:** Wählen Sie in der Liste eine mögliche Aktion aus:
  - **Immer herstellen:** Die Domäne löst immer eine VPN-Verbindung aus.
  - **Nie herstellen:** Die Domäne löst nie eine VPN-Verbindung aus.
  - **Wenn erforderlich herstellen:** Die Domäne löst eine VPN-Verbindung aus, wenn die Auflösung des Domänennamens fehlschlägt. Dieser Fehler tritt auf, wenn der DNS-Server die Domäne nicht auflösen kann, die Verbindung an einen anderen Server umleitet oder wenn beim DNS-Server ein Timeout auftritt.
  - Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **On-Demand-Regeln**
  - **Aktion:** Wählen Sie in der Liste die gewünschte Aktion aus. Die Standardeinstellung ist **EvaluateConnection**. Zulässige Aktionen:
    - **Zulassen:** On-Demand-VPN-Verbindung bei einer entsprechenden Auslösung zulassen.
    - **Verbinden:** Auf jeden Fall eine VPN-Verbindung herstellen.
    - **Trennen:** VPN-Verbindung trennen und bei Zutreffen der Regel keine Wiederverbindung herstellen.
    - **EvaluateConnection:** ActionParameters-Array für jede Verbindung auswerten.
    - **Ignorieren:** Bestehende VPN-Verbindungen beibehalten, bei Zutreffen der Regel jedoch keine Wiederverbindung herstellen.
  - **DNSDomainMatch:** Klicken Sie für jede Domäne, die bei der Suche anhand der Domänenliste von Geräten als Treffer in Betracht gezogen werden soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    - **DNS-Domäne:** Geben Sie den Domänennamen ein. Sie können ein Sternchen (*) als Platzhalter für das Präfix für mehrere Domänen verwenden. Beispiel: *.beispiel.com steht für meinedomäne.beispiel.com, seinedomäne.beispiel.com und ihredomäne.beispiel.com.
    - Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
  - **DNSServerAddressMatch:** Klicken Sie für jede DNS-Server-IP-Adresse im Netzwerk, die als Treffer in Betracht gezogen werden soll, auf **Hinzufügen** und führen Sie folgende

Schritte aus:

  * **Adresse des DNS-Servers:** Geben Sie die gewünschte DNS-Serveradresse ein. Sie können ein Sternchen (*) als Platzhalter für das Suffix für mehrere DNS-Server verwenden. “17.*” entspricht beispielsweise allen DNS-Servern im Subnetz der Klasse A.
  * Klicken Sie auf **Speichern**, um die DNS-Serveradresse zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **InterfaceTypeMatch:** Wählen Sie in der Liste den Hardwaretyp der verwendeten primären Netzwerkschnittstelle aus. Der Standardwert ist **Keine Angabe**. Zulässige Werte:
  * **Keine Angabe:** entspricht Netzwerkschnittstellenhardware aller Typen. Dies ist die Standardeinstellung.
  * **Ethernet:** entspricht Ethernet-Netzwerkschnittstellen.
  * **WiFi:** Entspricht WiFi-Netzwerkschnittstellen.
  * **Mobilnetz:** entspricht Mobilnetzschnittstellen.
- **SSIDMatch:** Klicken Sie für jede SSID, die als Treffer für das aktuelle Netzwerk in Betracht gezogen werden soll, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  * **SSID:** Geben Sie die gewünschte SSID ein. Ist das Netzwerk kein WiFi-Netzwerk oder erscheint die SSID nicht, gibt es keinen Treffer. Zur Einbeziehung aller SSIDs lassen Sie die Liste leer.
  * Klicken Sie auf **Speichern**, um die SSID zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **URLStringProbe:** Geben Sie eine URL für den Abruf ein. Kann die URL ohne Umleitung abgerufen werden, trifft die Regel zu.
- **ActionParameters : Domains:** Klicken Sie für jede Domäne, die durch EvaluateConnection geprüft werden soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
  * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **ActionParameters : DomainAction:** Wählen Sie in dieser Liste die **VPN-Aktionen** für die unter **ActionParameters : Domains** angegebenen Domänen. Die Standardeinstellung ist **ConnectIfNeeded**. Zulässige Aktionen:
  * **ConnectIfNeeded:** Die Domäne löst eine VPN-Verbindung aus, wenn die Auflösung des Domänennamens fehlschlägt. Dieser Fehler tritt auf, wenn der DNS-Server die Domäne nicht auflösen kann, die Verbindung an einen anderen Server umleitet oder wenn beim DNS-Server ein Timeout auftritt.
  * **NeverConnect:** Die Domäne löst nie eine VPN-Verbindung aus.
- **ActionParameters : RequiredDNSServers:** Klicken Sie für jede DNS-Server-IP-Adresse, die zum Auflösen der angegebenen Domänen verwendet werden soll, auf **Hinzufügen** und

führen Sie folgende Schritte aus:

* **DNS-Server:** nur gültig, wenn **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Geben Sie den DNS-Server an, der hinzugefügt werden soll. Dieser Server muss nicht Teil der aktuellen Netzwerkkonfiguration des Geräts sein. Ist der DNS-Server nicht erreichbar, wird eine VPN-Verbindung hergestellt. Bei diesem DNS-Server muss es sich entweder um einen internen DNS-Server oder einen vertrauenswürdigen externen DNS-Server handeln.
* Klicken Sie auf **Speichern**, um den DNS-Server zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.

– **ActionParameters : RequiredURLStringProbe:** Geben Sie optional eine HTTP- oder HTTPS-URL (bevorzugt letztere) zur Prüfung mit einer GET-Anforderung ein. Kann der Hostname der URL nicht aufgelöst werden oder ist der Server nicht erreichbar oder reagiert nicht, wird eine VPN-Verbindung hergestellt. Nur gültig, wenn **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.

– **OnDemandRules : XML content:** Geben Sie eine XML-Konfiguration für On-Demand-Regeln ein bzw. kopieren Sie sie und fügen Sie sie ein.

* Klicken Sie auf **Wörterbuch prüfen**, um den XML-Code zu prüfen. Wenn die XML-Datei gültig ist, wird “Gültige XML” in grün unterhalb von **XML-Inhalt** angezeigt. Wenn sie nicht gültig ist, wird in orange eine Fehlermeldung mit einer Beschreibung des Fehlers angezeigt.

- **Proxy**
  – **Proxykonfiguration:** Wählen Sie in der Liste das Routing der VPN-Verbindung über einen Proxyserver aus. Die Standardeinstellung 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**
  – Wählen Sie unter **Richtlinieneinstellungen** für **Richtlinie entfernen** entweder **Datum auswählen** oder **Zeit bis zum Entfernen (in Stunden)**.
  – Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.

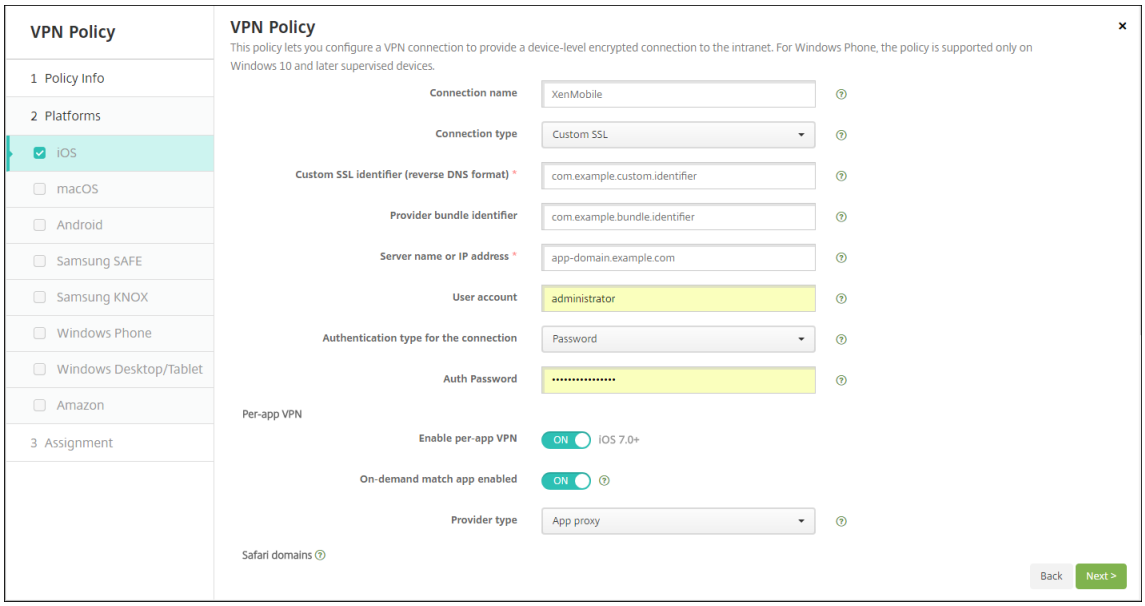
- Wählen Sie in der Liste **Benutzer darf Richtlinie entfernen** entweder **Immer**, **Kennwort erforderlich** oder **Nie**.
- Bei Auswahl von **Kennwort erforderlich** geben Sie für **Kennwort zum Entfernen** das benötigte Kennwort ein.

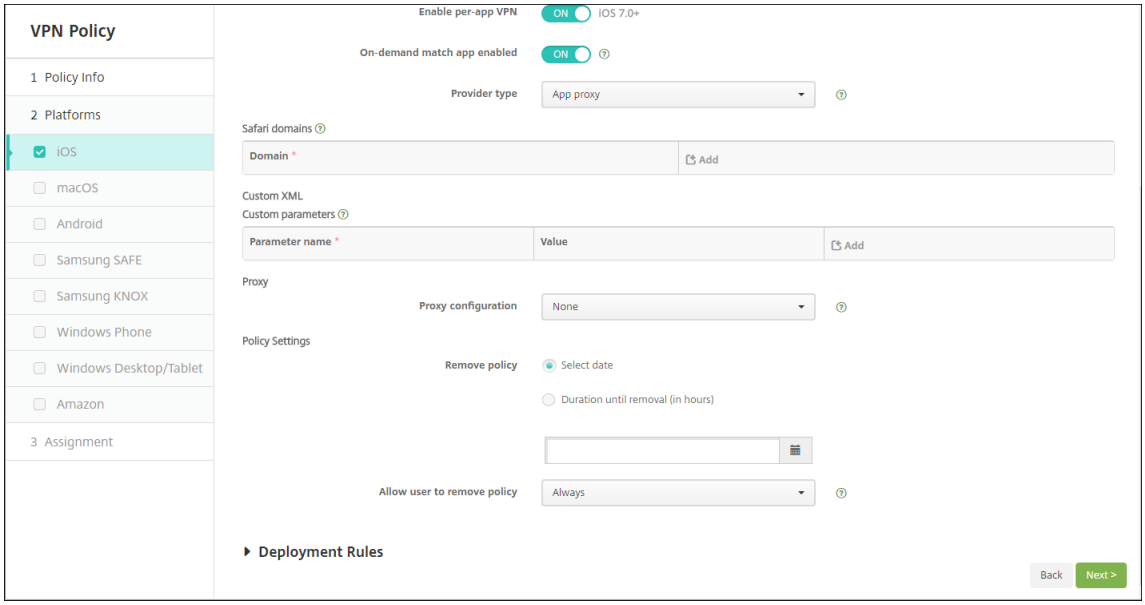
Konfigurieren des Pro-App-VPN-Zugriffs

Die Pro-App-VPN-Optionen für iOS sind für folgende Verbindungstypen verfügbar: Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO und Benutzerdefiniertes SSL.

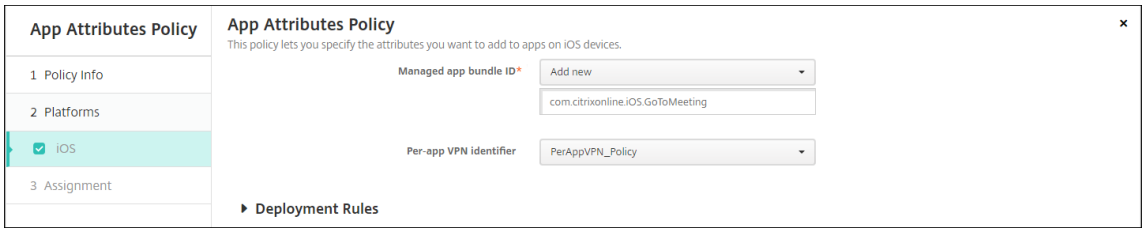
Konfigurieren des Pro-App-VPN-Zugriffs:

1. Erstellen Sie unter **Konfigurieren > Geräterichtlinien** eine VPN-Richtlinie. Beispiel:



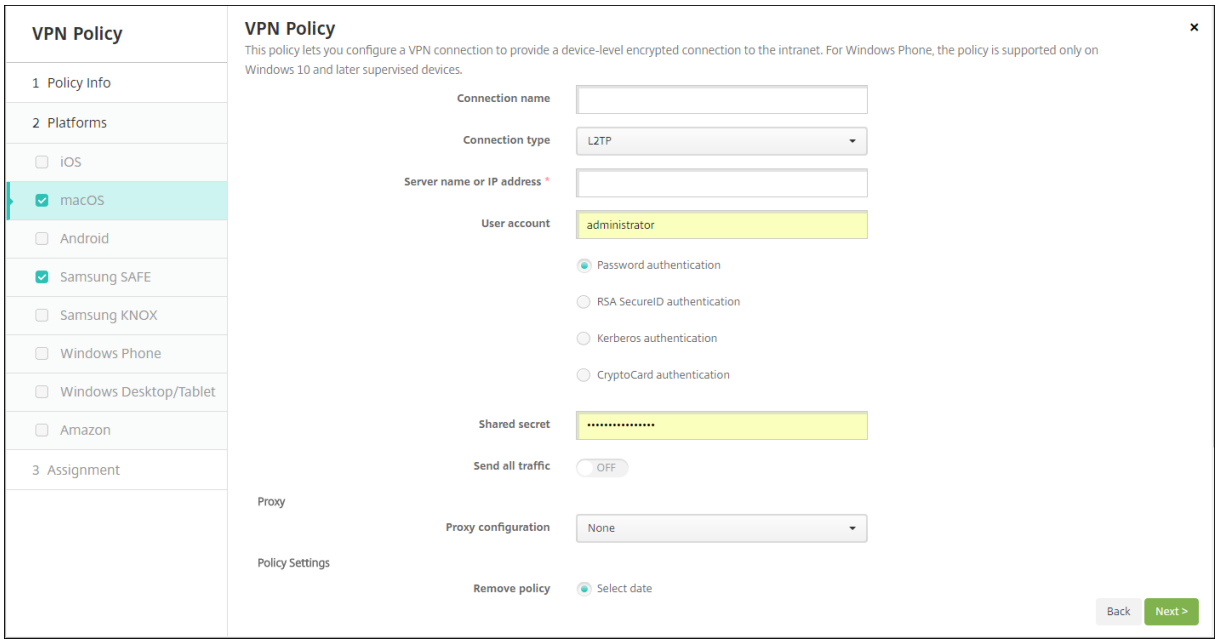


2. Erstellen Sie unter **Konfigurieren > Geräterichtlinien** eine Geräterichtlinie für App-Attribute, um der Pro-VNP-Richtlinie eine App zuzuordnen. Wählen Sie für **ID für VPN-Zugriff pro App** den Namen der in Schritt 1 erstellten VPN-Richtlinie. Wählen Sie für **Paket-ID für verwaltete App** eine Option aus der App-Liste oder geben Sie die Paket-ID ein. (Wenn Sie eine iOS-App-Bestandsrichtlinie bereitstellen, enthält die Liste Apps.)



- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-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.
  - **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 für macOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- Wählen Sie entweder **Kennwortauthentifizierung**, **RSA SecurID-Authentifizierung**, **Kerberos-Authentifizierung** oder **CryptoCard-Authentifizierung** aus. Der Standardwert ist **Kennwortauthentifizierung**.

- **Gemeinsamer geheimer Schlüssel:** Geben Sie den gemeinsamen geheimen Schlüssel für IPsec ein.
- **Gesamten Datenverkehr senden:** Wählen Sie aus, ob der gesamte Datenverkehr über das VPN geleitet werden soll. Die Standardeinstellung ist **Aus**.

Konfigurieren von PPTP für macOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- Wählen Sie entweder **Kennwortauthentifizierung**, **RSA SecurID-Authentifizierung**, **Kerberos-Authentifizierung** oder **CryptoCard-Authentifizierung** aus. Der Standardwert ist **Kennwortauthentifizierung**.
- **Verschlüsselungsgrad:** Wählen Sie den gewünschten Verschlüsselungsgrad aus. Die Standardeinstellung ist **Ohne**.
  - **Ohne:** keine Verschlüsselung verwenden.
  - **Automatisch:** den höchsten vom Server unterstützten Verschlüsselungsgrad verwenden.
  - **Maximum (128 Bit):** Immer 128-Bit-Verschlüsselung verwenden.
- **Gesamten Datenverkehr senden:** Wählen Sie aus, ob der gesamte Datenverkehr über das VPN geleitet werden soll. Die Standardeinstellung ist **Aus**.

Konfigurieren von IPsec für macOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Gemeinsamer geheimer Schlüssel** oder **Zertifikat** aus. Die Standardeinstellung ist **Gemeinsamer geheimer Schlüssel**.
  - Bei Auswahl von **Gemeinsamer geheimer Schlüssel** konfigurieren Sie die folgenden Einstellungen:
    * **Gruppenname:** Geben Sie optional einen Gruppennamen ein.
    * **Gemeinsamer geheimer Schlüssel:** Geben Sie optional einen gemeinsamen geheimen Schlüssel ein.
    * **Hybride Authentifizierung:** Wählen Sie aus, ob die Hybridauthentifizierung verwendet werden soll. Bei der hybriden Authentifizierung authentifiziert sich der Server zuerst beim Client und der Client authentifiziert sich dann beim Server. Die Standardeinstellung ist **Aus**.
    * **Zur Kennworteingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihres Kennworts aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:

    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer ihre PIN eingeben müssen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf.

Konfigurieren von Cisco AnyConnect für macOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Gruppe:** Geben Sie optional einen Gruppennamen ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf.
  - **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
    * **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob eine Pro-App-VPN-Verbindung automatisch hergestellt wird, wenn mit dem Pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.
    * **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und

führen Sie folgende Schritte aus:

- **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
- Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren von Juniper SSL für macOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Bereich:** Geben Sie optional einen Bereichsnamen ein.
- **Rolle:** Geben Sie optional einen Rollennamen ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    - **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    - **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    - **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob eine Pro-App-VPN-Verbindung automatisch hergestellt wird, wenn mit dem Pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.
  - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    - **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
    - Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren von F5 SSL für macOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob eine Pro-App-VPN-Verbindung automatisch hergestellt wird, wenn mit dem Pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.
  - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
    * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren des SonicWALL Mobile Connect-Protokolls für macOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Anmeldegruppe oder -domäne:** Geben Sie optional eine Anmeldegruppe oder -domäne ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein op-

tionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf.
- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob eine Pro-App-VPN-Verbindung automatisch hergestellt wird, wenn mit dem Pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.
  - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
    * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren von Ariba VIA für macOS

- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst wer-

den soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf.

- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Standardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob eine Pro-App-VPN-Verbindung automatisch hergestellt wird, wenn mit dem Pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen. Die Standardeinstellung ist **Aus**.
  - **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
    * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren des benutzerdefinierten SSL-Protokolls für macOS

- **Benutzerdefinierte SSL-ID (Reverse DNS-Format):** Geben Sie den SSL-Bezeichner im Reverse DNS-Format 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.
- **Benutzerkonto:** Geben Sie optional ein Benutzerkonto ein.
  - **Authentifizierungstyp für Verbindung:** Wählen Sie in der Liste entweder **Kennwort** oder **Zertifikat** aus. Der Standardwert ist **Kennwort**.
  - Wenn Sie **Kennwort** auswählen, geben Sie im Feld **Authentifizierungskennwort** ein optionales Authentifizierungskennwort ein.
  - Bei Auswahl von **Zertifikat** konfigurieren Sie die folgenden Einstellungen:
    * **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
    * **Beim Verbinden zur PIN-Eingabe auffordern:** Wählen Sie aus, ob die Benutzer zur Eingabe ihrer PIN aufgefordert werden sollen, wenn sie eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**.
    * **VPN bei Bedarf aktivieren:** Wählen Sie aus, ob eine VPN-Verbindung ausgelöst werden soll, wenn die Benutzer eine Verbindung zum Netzwerk herstellen. Die Standardeinstellung ist **Aus**. Weitere Informationen zum Konfigurieren der Einstellungen, wenn **VPN bei Bedarf aktivieren** auf **Ein** festgelegt wurde, finden Sie unter Konfigurieren der Einstellungen für VPN bei Bedarf.
  - **VPN-Zugriff pro App:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Die Stan-

dardeinstellung ist **Aus**. Wenn Sie die Option aktivieren, konfigurieren Sie die folgenden Einstellungen:

* **App-Übereinstimmung bei Bedarf aktiviert:** Wählen Sie aus, ob pro-App-VPN-Verbindungen automatisch hergestellt werden sollen, wenn mit dem pro-App-VPN-Dienst verknüpfte Apps eine Netzwerkkommunikation beginnen.
* **Safari-Domänen:** Klicken Sie für jede Safari-Domäne, die eine pro-App-VPN-Verbindung auslösen kann und die Sie einschließen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  · **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
  · Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **Benutzerdefiniertes XML:** Für jeden benutzerdefinierten XML-Parameter, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  – **Parametername:** Geben Sie den Namen des gewünschten Parameters ein.
  – **Wert:** Geben Sie den mit **Parametername** verknüpften Wert ein.
  – Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der Optionen für "VPN bei Bedarf aktivieren"

- **On-Demand-Domäne:** Klicken Sie für jede gewünschte Domäne und Aktion, die beim Herstellen einer Verbindung mit der Domäne erfolgen soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  – **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
  – **Aktion:** Wählen Sie in der Liste eine mögliche Aktion aus:
    * **Immer herstellen:** Die Domäne löst immer eine VPN-Verbindung aus.
    * **Nie herstellen:** Die Domäne löst nie eine VPN-Verbindung aus.
    * **Wenn erforderlich herstellen:** Die Domäne löst eine VPN-Verbindung aus, wenn die Auflösung des Domänennamens fehlschlägt. Dieser Fehler tritt auf, wenn der DNS-Server die Domäne nicht auflösen kann, die Verbindung an einen anderen Server umleitet oder wenn beim DNS-Server ein Timeout auftritt.
  – Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **On-Demand-Regeln**
  – **Aktion:** Wählen Sie in der Liste die gewünschte Aktion aus. Die Standardeinstellung ist **EvaluateConnection**. Zulässige Aktionen:
    * **Zulassen:** On-Demand-VPN-Verbindung bei einer entsprechenden Auslösung zulassen.
    * **Verbinden:** Auf jeden Fall eine VPN-Verbindung herstellen.
    * **Trennen:** VPN-Verbindung trennen und bei Zutreffen der Regel keine Wiederverbindung

herstellen.
    * **EvaluateConnection: ActionParameters**-Array für jede Verbindung auswerten.
    * **Ignorieren:** Bestehende VPN-Verbindungen beibehalten, bei Zutreffen der Regel jedoch keine Wiederverbindung herstellen.
- **DNSDomainMatch:** Klicken Sie für jede Domäne, die bei der Suche anhand der Domänenliste von Geräten als Treffer in Betracht gezogen werden soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **DNS-Domäne:** Geben Sie den Domänennamen ein. Sie können ein Sternchen (*) als Platzhalter für das Präfix für mehrere Domänen verwenden. Beispiel: *.beispiel.com steht für meinedomäne.beispiel.com, seinedomäne.beispiel.com und ihredomäne.beispiel.com.
    * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **DNSServerAddressMatch:** Klicken Sie für jede DNS-Server-IP-Adresse im Netzwerk, die als Treffer in Betracht gezogen werden soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **Adresse des DNS-Servers:** Geben Sie die gewünschte DNS-Serveradresse ein. Sie können ein Sternchen (*) als Platzhalter für das Suffix für mehrere DNS-Server verwenden. “17.*” entspricht beispielsweise allen DNS-Servern im Subnetz der Klasse A.
    * Klicken Sie auf **Speichern**, um die DNS-Serveradresse zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **InterfaceTypeMatch:** Klicken Sie in der Liste auf den Hardwaretyp der verwendeten primären Netzwerkschnittstelle. Der Standardwert ist **Keine Angabe**. Zulässige Werte:
    * **Keine Angabe:** entspricht Netzwerkschnittstellenhardware aller Typen. Dies ist die Standardeinstellung.
    * **Ethernet:** entspricht Ethernet-Netzwerkschnittstellen.
    * **WiFi:** Entspricht WiFi-Netzwerkschnittstellen.
    * **Mobilnetz:** entspricht Mobilnetzschnittstellen.
- **SSIDMatch:** Klicken Sie für jede SSID, die als Treffer für das aktuelle Netzwerk in Betracht gezogen werden soll, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
    * **SSID:** Geben Sie die gewünschte SSID ein. Ist das Netzwerk kein WiFi-Netzwerk oder erscheint die SSID nicht, gibt es keinen Treffer. Zur Einbeziehung aller SSIDs lassen Sie die Liste leer.
    * Klicken Sie auf **Speichern**, um die SSID zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **URLStringProbe:** Geben Sie eine URL für den Abruf ein. Kann die URL ohne Umleitung abgerufen werden, trifft die Regel zu.
- **ActionParameters : Domains:** Klicken Sie für jede Domäne, die durch EvaluateConnec-

tion geprüft werden soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **Domäne:** Geben Sie den Namen der hinzuzufügenden Domäne ein.
    * Klicken Sie auf **Speichern**, um die Domäne zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
  - **ActionParameters : DomainAction:** Wählen Sie in dieser Liste die **VPN-Aktionen** für die unter **ActionParameters : Domains** angegebenen Domänen. Die Standardeinstellung ist **ConnectIfNeeded**. Zulässige Aktionen:
    * **ConnectIfNeeded:** Die Domäne löst eine VPN-Verbindung aus, wenn die Auflösung des Domänennamens fehlschlägt. Dieser Fehler tritt auf, wenn der DNS-Server die Domäne nicht auflösen kann, die Verbindung an einen anderen Server umleitet oder wenn beim DNS-Server ein Timeout auftritt.
    * **NeverConnect:** Die Domäne löst nie eine VPN-Verbindung aus.
  - **ActionParameters : RequiredDNSServers:** Klicken Sie für jede DNS-Server-IP-Adresse, die zum Auflösen der angegebenen Domänen verwendet werden soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
    * **DNS-Server:** nur gültig, wenn **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Geben Sie den DNS-Server an, der hinzugefügt werden soll. Dieser Server muss nicht Teil der aktuellen Netzwerkkonfiguration des Geräts sein. Ist der DNS-Server nicht erreichbar, wird eine VPN-Verbindung hergestellt. Bei diesem DNS-Server muss es sich entweder um einen internen DNS-Server oder einen vertrauenswürdigen externen DNS-Server handeln.
    * Klicken Sie auf **Speichern**, um den DNS-Server zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.
  - **ActionParameters : RequiredURLStringProbe:** Geben Sie optional eine HTTP- oder HTTPS-URL (bevorzugt letztere) zur Prüfung mit einer GET-Anforderung ein. Kann der Hostname der URL nicht aufgelöst werden oder ist der Server nicht erreichbar oder reagiert nicht, wird eine VPN-Verbindung hergestellt. Nur gültig, wenn **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
  - **OnDemandRules : XML content:** Geben Sie eine XML-Konfiguration für On-Demand-Regeln ein bzw. kopieren Sie sie und fügen Sie sie ein.
    * Klicken Sie auf **Wörterbuch prüfen**, um den XML-Code zu prüfen. Wenn die XML-Datei gültig ist, wird “Gültige XML” in grün unterhalb von **XML-Inhalt** angezeigt. Wenn sie nicht gültig ist, wird in orange eine Fehlermeldung mit einer Beschreibung des Fehlers angezeigt.

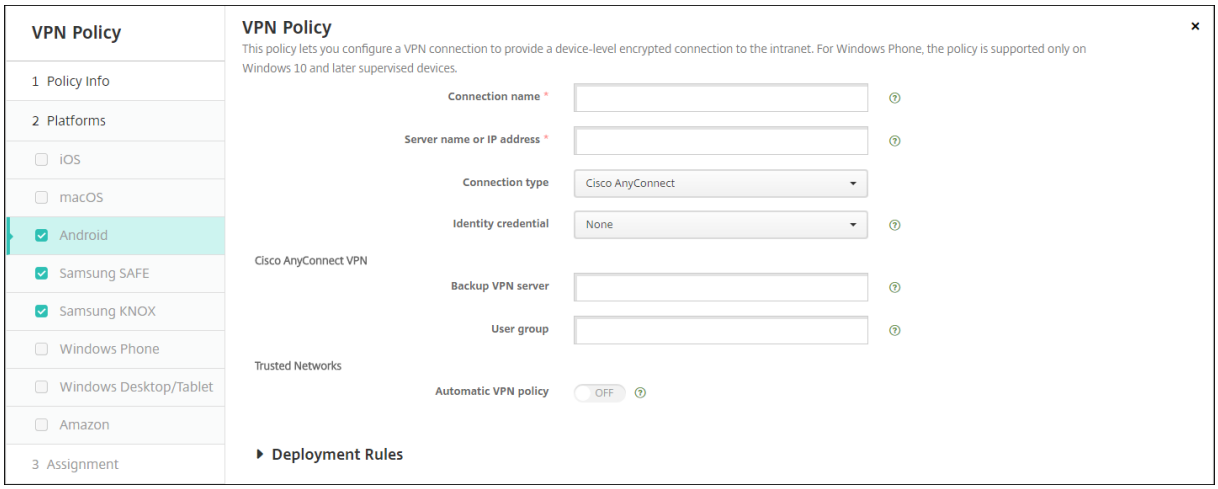
- **Proxy**
  - **Proxykonfiguration:** Wählen Sie in der Liste das Routing der VPN-Verbindung über einen Proxyserver aus. Die Standardeinstellung ist **Ohne**.
    * Bei Auswahl von **Manuell** konfigurieren Sie die folgenden Einstellungen:
      · **Hostname oder IP-Adresse des Proxyservers:** Geben 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.

Android-Einstellungen



Konfigurieren des Cisco AnyConnect VPN-Protokolls für Android

- **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.
- **Identitätsanmeldeinformationen:** Wählen Sie Identitätsanmeldeinformationen in der Liste aus.
- **Backup-VPN-Server:** Geben Sie die Informationen des sekundären VPN-Servers ein.
- **Benutzergruppe:** Geben Sie die Informationen zur Benutzergruppe ein.
- **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:** Wählen Sie die gewünschte Richtlinie in der Liste aus. 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:** Wenn ein Benutzer nach dem Herstellen einer VPN-Sitzung außerhalb eines vertrauenswürdigen Netzwerks ein als vertrauenswürdig konfiguriertes Netzwerk betritt, wird die VPN-Sitzung ausgesetzt. 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:** Wählen Sie die gewünschte Richtlinie in der Liste aus. 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 hat, wenn der Client im vertrauenswürdigen Netzwerk ist, auf **Hinzufügen**, und führen Sie die folgenden Schritte aus:
    * **Domäne:** Geben Sie den Namen der hinzuzufügenden 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 hat, wenn der Client im vertrauenswürdigen Netzwerk ist, 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.

Konfigurieren des Citrix SSO-Protokolls für Android

- **Verbindungsname:** Geben Sie einen Namen für die VPN-Verbindung ein. Diese Angabe ist erforderlich.
- **Servername oder IP-Adresse:** Geben Sie den FQDN oder die IP-Adresse des Citrix Gateway ein.
- **Authentifizierungstyp für Verbindung:** Wählen Sie einen Authentifizierungstyp aus und füllen Sie diejenigen der folgenden Felder aus, die je nach Typ angezeigt werden:
  - **Benutzername** und **Kennwort**: Geben Sie die VPN-Anmeldeinformationen für die **Authentifizierungstypen Kennwort** bzw. **Kennwort und Zertifikat** ein. Optional. Wenn

Sie keine VPN-Anmeldeinformationen angeben, fordert die Citrix VPN-App zur Eingabe von Benutzernamen und Kennwort auf.

- **Identitätsanmeldeinformationen:** Diese Option wird für die **Authentifizierungstypen Zertifikat** und **Kennwort und Zertifikat** angezeigt. Wählen Sie Identitätsanmeldeinformationen aus der Liste aus.

- **Pro-App-VPN aktivieren:** Aktivieren oder deaktivieren Sie diese Option nach Bedarf. Wenn Sie die Option nicht aktivieren, wird der gesamte Datenverkehr durch den Citrix VPN-Tunnel geleitet. Wenn Sie die Option aktivieren, legen Sie die nachfolgend aufgeführten Einstellungen fest. Die Standardeinstellung ist **Aus**.
  - **Positivliste** oder **Sperrliste**: Wenn Sie **Positivliste** wählen, wird der Datenverkehr aller zugelassenen Apps durch den VPN-Tunnel geleitet. Wenn Sie **Sperrliste** wählen, wird der Datenverkehr aller Apps mit Ausnahme der Apps, die auf der Sperrliste stehen, durch den VPN-Tunnel geleitet.

    > **Hinweis:**
    >
    > Die XenMobile Server-Konsole enthält im Englischen die Begriffe “Blacklist” und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

  - **Anwendungsliste:** Geben Sie die zulässigen oder gesperrten Apps an. Klicken Sie auf **Hinzufügen** und geben Sie die App-Paketnamen getrennt durch Kommas ein.

- **Benutzerdefiniertes XML:** Klicken Sie auf **Hinzufügen** und geben Sie benutzerdefinierte Parameter ein. XenMobile unterstützt folgende Parameter für Citrix VPN:
  - **DisableUserProfiles:** Optional. Geben Sie zum Aktivieren des Parameters für **Wert Yes** ein. Wird die Option aktiviert, werden von XenMobile keine von Benutzern hinzugefügte VPN-Verbindungen angezeigt und die Benutzer können keine Verbindungen hinzufügen. Diese globale Einschränkung gilt für alle VPN-Profile.
  - **userAgent:** Zeichenfolge. Sie können eine eigene Benutzeragent-Zeichenfolge für die Übermittlung mit jeder HTTP-Anforderung definieren. Die Benutzeragent-Zeichenfolge wird an den bestehenden Citrix VPN-Benutzeragent angehängt.

Konfigurieren von VPNs zur Unterstützung von NAC

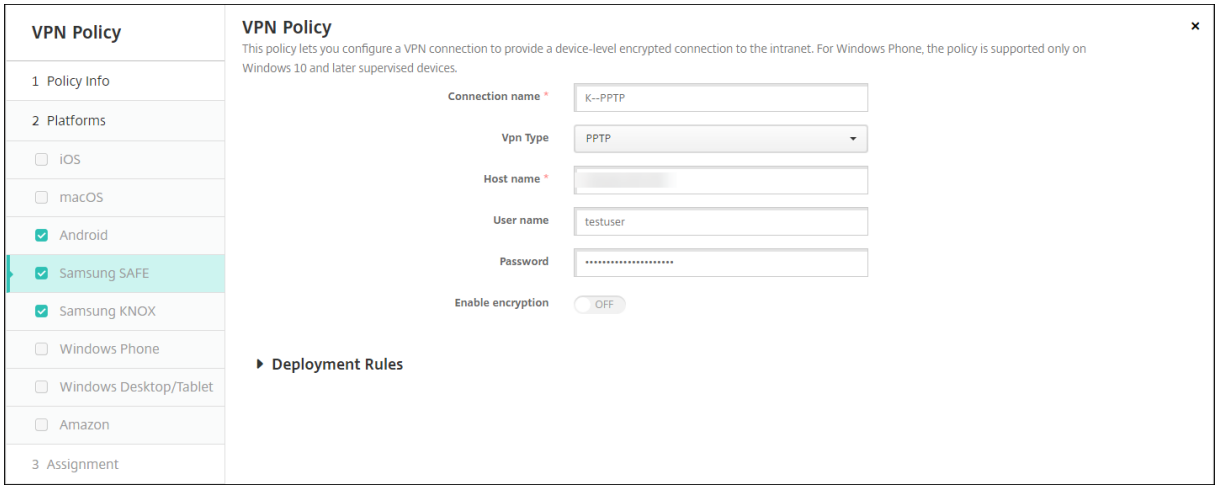
1. Verwenden Sie für die Konfiguration des NAC-Filters als **Verbindungstyp** die Option **Benutzerdefiniertes SSL**.
2. Geben Sie für **Verbindungsname** die Option **VPN** an.
3. Klicken Sie unter **Benutzerdefiniertes XML** auf **Hinzufügen** und führen Sie folgende Schritte aus:

- **Parametername:** Geben Sie **XenMobileDeviceId** ein. Dies ist die Geräte-ID, die für die NAC-Prüfung basierend auf der Geräteregistrierung in XenMobile verwendet wird. Wenn das Gerät von XenMobile registriert und verwaltet wird, wird die VPN-Verbindung zugelassen. Andernfalls schlägt die Authentifizierung bei der VPN-Einrichtung fehl.
- **Wert:** Geben Sie **DeviceID_${device.id}** ein. Dies ist der Wert für den Parameter **XenMobileDeviceId**.
- Klicken Sie auf **Speichern**, um den Parameter zu speichern.

Konfigurieren von VPNs für Android Enterprise

Zum Konfigurieren von VPNs für Android Enterprise-Geräte erstellen Sie für die Citrix SSO-App eine Geräterichtlinie für verwaltete Android Enterprise-Konfigurationen. Weitere Informationen unter Konfigurieren von VPN-Profilen für Android Enterprise.

Samsung SAFE-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.

Konfigurieren von L2TP mit vorinstalliertem Schlüssel für Samsung SAFE

- **Hostname:** Geben Sie den Namen des VPN-Hosts ein. Diese Angabe ist erforderlich.
- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **Vorinstallierter Schlüssel:** Geben Sie den vorinstallierten Schlüssel ein. Diese Angabe ist erforderlich.

Konfigurieren von L2TP mit Zertifikatsprotokoll für Samsung SAFE

- **Hostname:** Geben Sie den Namen des VPN-Hosts ein. Diese Angabe ist erforderlich.
- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.

Konfigurieren von PPTP für Samsung SAFE

- **Hostname:** Geben Sie den Namen des VPN-Hosts ein. Diese Angabe ist erforderlich.
- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **Verschlüsselung aktivieren:** Wählen Sie aus, ob Verschlüsselung für die VPN-Verbindung aktiviert werden soll.

Konfigurieren des Enterprise-Protokolls für Samsung SAFE

- **Hostname:** Geben Sie den Namen des VPN-Hosts ein. Diese Angabe ist erforderlich.
- **Backupserver aktivieren:** Wählen Sie aus, ob ein Backup-VPN-Server aktiviert werden soll. Wenn Sie die Option aktivieren, geben Sie im Feld **Backup-VPN-Server** den FQDN oder die IP-Adresse des sekundären VPN-Servers ein.
- **Benutzerauthentifizierung aktivieren**: Wählen Sie aus, ob die Benutzerauthentifizierung erforderlich sein soll. Wenn Sie diese Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **Benutzername:** Geben Sie einen Benutzernamen ein.
  - **Kennwort:** Geben Sie das Benutzerkennwort ein.
- **Gruppenname:** Geben Sie optional einen Gruppennamen ein.
- **Authentifizierungsmethode:** Wählen Sie in der Liste die gewünschte Authentifizierungsmethode aus. Mögliche Optionen:
  - **Zertifikat:** Verwenden Sie Zertifikatauthentifizierung. Dies ist die Standardeinstellung. Wenn aktiviert, klicken Sie in der Liste **Identitätsanmeldeinformationen** auf die Anmeldeinformationen, die verwendet werden sollen. Die Standardeinstellung ist **Ohne**.

  - **Vorinstallierter Schlüssel:** Verwenden Sie einen vorinstallierten Schlüssel. Wenn Sie diese Option aktivieren, geben Sie im Feld **Vorinstallierter Schlüssel** den gemeinsamen geheimen Schlüssel ein.
  - **Hybrid RSA:** Hybridauthentifizierung mit RSA-Zertifikaten
  - **EAP MD5:** EAP-Peer wird beim EAP-Server authentifiziert, es erfolgt jedoch keine gegenseitige Authentifizierung.
  - **EAP MSCHAPv2:** Verwenden Sie Challenge Handshake Authentication von Microsoft für die gegenseitige Authentifizierung.
- **ZS-Zertifikat:** Wählen Sie in der Liste das Zertifikat aus, das verwendet werden soll. Die Standardeinstellung ist **Ohne**.
- **Standardroute aktivieren:** Wählen Sie aus, ob eine Standardroute zum VPN-Server aktiviert werden soll. Die Standardeinstellung ist **Aus**.
- **Smartcardauthentifizierung aktivieren:** Wählen Sie aus, ob eine Authentifizierung per Smartcard zugelassen werden soll. Die Standardeinstellung ist **Aus**.
- **Mobiloptionen aktivieren:** Wählen Sie aus, ob die Mobiloptionen aktiviert werden sollen. Die Standardeinstellung ist **Aus**.
- **Diffie-Hellman-Gruppenwert (Schlüsselstärke):** Wählen Sie in der Liste die Schlüsselstärke aus, die verwendet werden soll. Die Standardeinstellung ist 0.
- **Split-Tunneltyp:** Wählen Sie in der Liste den gewünschten Split-Tunneltyp aus. Der Standardwert ist **Auto**. Mögliche Optionen:
  - **Auto:** Split-Tunneling wird automatisch verwendet.
  - **Manuell:** Split-Tunneling erfolgt über die IP-Adresse und den Port, die auf dem VPN-Server angegeben wurden.
  - **Deaktiviert:** Split-Tunneling wird nicht verwendet.
- **SuiteB-Typ:** Wählen Sie in der Liste den gewünschten Grad der NSA Suite B-Verschlüsselung aus. Die Standardeinstellung ist **GCM-128**. Mögliche Optionen:
  - **GCM-128:** AES-GCM-Verschlüsselung (128 Bit) verwenden.
  - **GCM-256:** AES-GCM-Verschlüsselung (256 Bit) verwenden.
  - **GMAC-128:** Verwenden Sie AES-GMAC-Verschlüsselung (128 Bit).
  - **GMAC-256:** AES-GMAC-Verschlüsselung (256 Bit) verwenden.
  - **Ohne:** keine Verschlüsselung verwenden.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren des generischen Protokolls für Samsung SAFE

- **Hostname:** Geben Sie den Namen des VPN-Hosts ein. Diese Angabe ist erforderlich.

- **Benutzerauthentifizierung aktivieren**: Wählen Sie aus, ob die Benutzerauthentifizierung erforderlich sein soll. Wenn Sie die Option aktivieren, geben Sie im Feld **Kennwort** das Benutzerkennwort ein.
- **Benutzername:** Geben Sie einen Benutzernamen ein.
- **Paketname für Agent-VPN:** Der Paketname oder die ID der auf dem Gerät installierten VPN, z. B. Mocana oder Pulse Secure.
- **VPN-Verbindungstyp:** Wählen Sie in der Liste entweder **IPSEC** oder **SSL** als Verbindungstyp aus. Die Standardeinstellung ist **IPSEC**. In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen Verbindungstypen erläutert.

Konfigurieren der Einstellungen für IPsec-Verbindungen für Samsung SAFE

- **Identität:** Geben Sie optional einen Bezeichner für diese Konfiguration ein.
- **ID-Typ für IPsec-Gruppe:** Wählen Sie in der Liste den IPsec-Gruppen-ID-Typ aus. Der Standardwert ist **Standard**. Mögliche Optionen:
  - **Standard**
  - **IPv4-Adresse**
  - **Vollqualifizierter Domänenname (FQDN)**
  - **Benutzer-FQDN**
  - **IKE-Schlüssel-ID**
- **IKE-Version:** Wählen Sie in der Liste die gewünschte Internet Key Exchange-Version aus. Der Standardwert ist **IKEv1**.
- **Authentifizierungsmethode:** Wählen Sie in der Liste die gewünschte Authentifizierungsmethode aus. Der Standardwert ist **Zertifikat**. Mögliche Optionen:
  - **Zertifikat:** Verwenden Sie Zertifikatauthentifizierung. Wenn aktiviert, klicken Sie in der Liste **Identitätsanmeldeinformationen** auf die Anmeldeinformationen, die verwendet werden sollen. Die Standardeinstellung ist **Ohne**.
  - **Vorinstallierter Schlüssel:** Verwenden Sie einen vorinstallierten Schlüssel. Wenn Sie diese Option aktivieren, geben Sie im Feld **Vorinstallierter Schlüssel** den gemeinsamen geheimen Schlüssel ein.
  - **Hybrid RSA:** Hybridauthentifizierung mit RSA-Zertifikaten
  - **EAP MD5:** EAP-Peer wird beim EAP-Server authentifiziert, es erfolgt jedoch keine gegenseitige Authentifizierung.
  - **EAP MSCHAPv2:** Verwenden Sie Challenge Handshake Authentication von Microsoft für die gegenseitige Authentifizierung.
  - **CAC-basierte Authentifizierung**: Common Access Card (CAC) für die Authentifizierung verwenden.
- **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus. Die Standardeinstellung ist **Ohne**.
- **ZS-Zertifikat:** Wählen Sie in der Liste das Zertifikat aus, das verwendet werden soll.

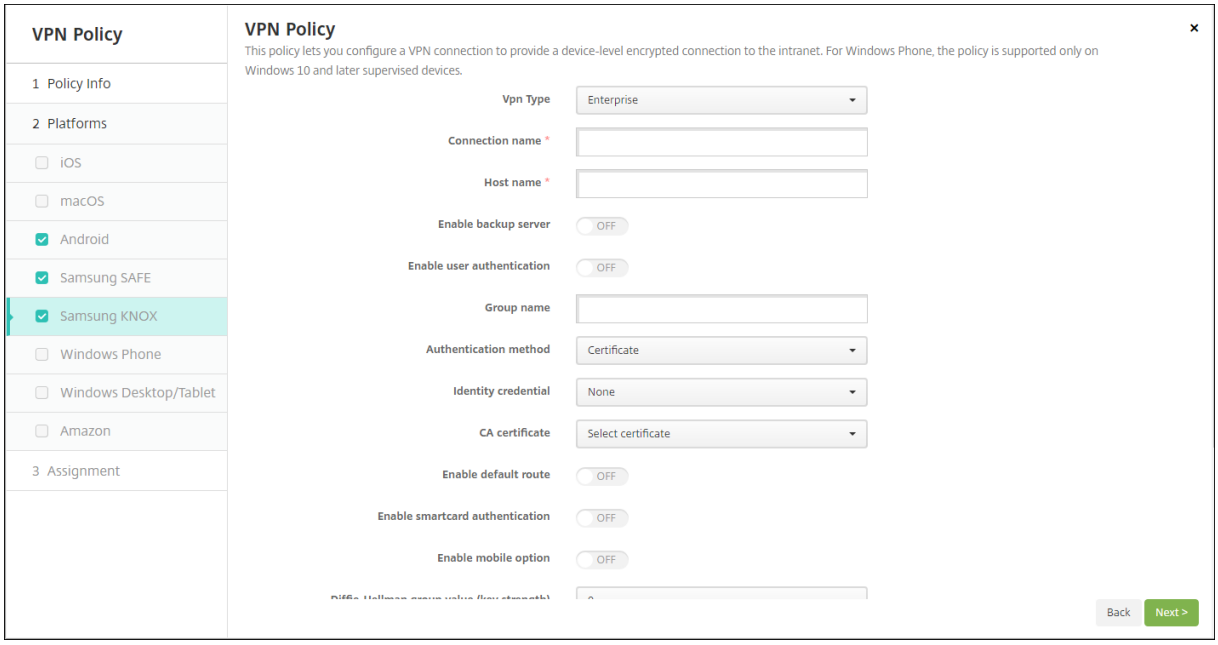
- **Dead Peer Detection aktivieren:** Wählen Sie aus, ob eine Verbindung mit Peers hergestellt werden soll, um sicherzustellen, dass diese erreichbar bleiben. Die Standardeinstellung ist **Aus**.
- **Standardroute aktivieren:** Wählen Sie aus, ob eine Standardroute zum VPN-Server aktiviert werden soll.
- **Mobiloptionen aktivieren:** Wählen Sie aus, ob die Mobiloptionen aktiviert werden sollen.
- **IKE-Lebensdauer in Minuten:** Geben Sie die Zeitdauer in Minuten an, nach der die VPN-Verbindung erneuert werden muss. Die Standardeinstellung ist 1440 Minuten (24 Stunden).
- **IPsec-Lebensdauer in Minuten:** Geben Sie die Zeitdauer in Minuten an, nach der die VPN-Verbindung erneuert werden muss. Die Standardeinstellung ist 1440 Minuten (24 Stunden).
- **Diffie-Hellman-Gruppenwert (Schlüsselstärke):** Wählen Sie in der Liste die Schlüsselstärke aus, die verwendet werden soll. Die Standardeinstellung ist **0**.
- **IKE Phase 1-Schlüsselaustauschmodus:** Wählen Sie als IDE Phase 1-Aushandlungsmodus entweder **Primär** oder **Aggressiv** aus. Der Standardwert ist **Primär**.
  - **Primär:** Bei der Aushandlung werden keine Informationen für mögliche Angreifer offengelegt. Der Modus ist jedoch langsamer als **Aggressiv**.
  - **Aggressiv:** Bei der Aushandlung werden einige Informationen (z. B. die IDs der aushandelnden Peers) für mögliche Angreifer offengelegt. Der Modus ist jedoch schneller als **Primär**.
- **PFS-Wert (Perfect Forward Secrecy):** Wählen Sie aus, ob durch die Verwendung von PFS bei der Neuaushandlung von Verbindungen ein erneuter Schlüsselaustausch erforderlich sein soll.
- **Split-Tunneltyp:** Wählen Sie in der Liste den gewünschten Split-Tunneltyp aus. Mögliche Optionen:
  - **Auto:** Split-Tunneling wird automatisch verwendet.
  - **Manuell:** Split-Tunneling erfolgt über die IP-Adresse und den Port, die auf dem VPN-Server angegeben wurden.
  - **Deaktiviert:** Split-Tunneling wird nicht verwendet.
- **IPsec-Verschlüsselungsalgorithmus:** Vom IPsec-Protokoll verwendete VPN-Konfiguration.
- **IKE-Verschlüsselungsalgorithmus:** Vom IPsec-Protokoll verwendete VPN-Konfiguration.
- **IKE-Integritätsalgorithmus:** Vom IPsec-Protokoll verwendete VPN-Konfiguration.
- **Hersteller:** ein persönliches Profil für generische Agents, die mit der Knox-API kommunizieren.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **VPN-Zugriff pro App:** Für jeden VPN-Zugriff pro App, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **VPN-Zugriff pro App:** VPN-Konfiguration, die die App für die Kommunikation verwendet.
  - Klicken Sie auf **Speichern**, um den VPN-Zugriff pro App zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der Einstellungen für SSL-Verbindungen für Samsung SAFE

- **Authentifizierungsmethode:** Wählen Sie in der Liste die gewünschte Authentifizierungsmethode aus. Die Standardeinstellung ist **Nicht zutreffend**. Mögliche Optionen:
  - **Nicht zutreffend**
  - **Zertifikat:** Verwenden Sie Zertifikatauthentifizierung. Wenn aktiviert, klicken Sie in der Liste **Identitätsanmeldeinformationen** auf die Anmeldeinformationen, die verwendet werden sollen. Die Standardeinstellung ist **Ohne**.
  - **CAC-basierte Authentifizierung**: Common Access Card (CAC) für die Authentifizierung verwenden.
- **ZS-Zertifikat:** Wählen Sie in der Liste das Zertifikat aus, das verwendet werden soll.
- **Standardroute aktivieren:** Wählen Sie aus, ob eine Standardroute zum VPN-Server aktiviert werden soll.
- **Mobiloptionen aktivieren:** Wählen Sie aus, ob die Mobiloptionen aktiviert werden sollen.
- **Split-Tunneltyp:** Wählen Sie in der Liste den gewünschten Split-Tunneltyp aus. Mögliche Optionen:
  - **Auto:** Split-Tunneling wird automatisch verwendet.
  - **Manuell:** Split-Tunneling erfolgt über die IP-Adresse und den Port, die auf dem VPN-Server angegeben wurden.
  - **Deaktiviert:** Split-Tunneling wird nicht verwendet.
- **SSL-Algorithmus:** Geben Sie den SSL-Algorithmus für die Client/Server-Aushandlung ein.
- **Hersteller:** ein persönliches Profil für generische Agents, die mit der Knox-API kommunizieren.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **VPN-Zugriff pro App:** Für jeden VPN-Zugriff pro App, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **VPN-Zugriff pro App:** VPN-Konfiguration, die die App für die Kommunikation verwendet.
  - Klicken Sie auf **Speichern**, um den VPN-Zugriff pro App zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.

- **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
- **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Samsung Knox-Einstellungen



Alle Samsung Knox-Richtlinien gelten ausschließlich innerhalb des Samsung Knox-Containers.

- **VPN-Typ:** Wählen Sie in der Liste den Typ der zu konfigurierenden VPN-Verbindung aus. Zur Auswahl stehen **Unternehmen** (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 für Samsung Knox

- **Verbindungsname:** Geben Sie einen Namen für die Verbindung ein. Diese Angabe ist erforderlich.
- **Hostname:** Geben Sie den Namen des VPN-Hosts ein. Diese Angabe ist erforderlich.
- **Backupserver aktivieren:** Wählen Sie aus, ob ein Backup-VPN-Server aktiviert werden soll.

Wenn Sie die Option aktivieren, geben Sie im Feld **Backup-VPN-Server** den FQDN oder die IP-Adresse des sekundären VPN-Servers ein.

- **Benutzerauthentifizierung aktivieren**: Wählen Sie aus, ob die Benutzerauthentifizierung erforderlich sein soll. Wenn Sie diese Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **Benutzername:** Geben Sie einen Benutzernamen ein.
  - **Kennwort:** Geben Sie das Benutzerkennwort ein.
- **Gruppenname:** Geben Sie optional einen Gruppennamen ein.
- **Authentifizierungsmethode:** Wählen Sie in der Liste die gewünschte Authentifizierungsmethode aus. Mögliche Optionen:
  - **Zertifikat:** Verwenden Sie Zertifikatauthentifizierung. Wählen Sie für die Zertifikatauthentifizierung außerdem in der Liste **Identitätsanmeldeinformationen** die zu verwendenden Anmeldeinformationen aus.
  - **Vorinstallierter Schlüssel:** Verwenden Sie einen vorinstallierten Schlüssel. Wenn Sie diese Option aktivieren, geben Sie im Feld **Vorinstallierter Schlüssel** den gemeinsamen geheimen Schlüssel ein.
  - **Hybrid RSA:** Hybridauthentifizierung mit RSA-Zertifikaten
  - **EAP MD5:** EAP-Peer wird beim EAP-Server authentifiziert, es erfolgt jedoch keine gegenseitige Authentifizierung.
  - **EAP MSCHAPv2:** Verwenden Sie Challenge Handshake Authentication von Microsoft für die gegenseitige Authentifizierung.
- **ZS-Zertifikat:** Wählen Sie in der Liste das Zertifikat aus, das verwendet werden soll.
- **Standardroute aktivieren:** Wählen Sie aus, ob eine Standardroute zum VPN-Server aktiviert werden soll.
- **Smartcardauthentifizierung aktivieren:** Wählen Sie aus, ob eine Authentifizierung per Smartcard zugelassen werden soll. Die Standardeinstellung ist **Aus**.
- **Mobiloptionen aktivieren:** Wählen Sie aus, ob die Mobiloptionen aktiviert werden sollen.
- **Diffie-Hellman-Gruppenwert (Schlüsselstärke):** Wählen Sie in der Liste die Schlüsselstärke aus, die verwendet werden soll. Die Standardeinstellung ist **0**.
- **Split-Tunneltyp:** Wählen Sie in der Liste den gewünschten Split-Tunneltyp aus. Mögliche Optionen:
  - **Auto:** Split-Tunneling wird automatisch verwendet.
  - **Manuell:** Split-Tunneling erfolgt über die IP-Adresse und den Port, die auf dem VPN-Server angegeben wurden.
  - **Deaktiviert:** Split-Tunneling wird nicht verwendet.
- **SuiteB-Typ:** Wählen Sie in der Liste den gewünschten Grad der NSA Suite B-Verschlüsselung aus. Mögliche Optionen:
  - **GCM-128:** AES-GCM-Verschlüsselung (128 Bit) verwenden. Dies ist die Standardeinstellung.

  - **GCM-256:** AES-GCM-Verschlüsselung (256 Bit) verwenden.
  - **GMAC-128:** Verwenden Sie AES-GMAC-Verschlüsselung (128 Bit).
  - **GMAC-256:** AES-GMAC-Verschlüsselung (256 Bit) verwenden.
  - **Ohne:** keine Verschlüsselung verwenden.
- **Weiterleitungsrouten:** Klicken Sie auf **Hinzufügen**, um optional Weiterleitungsrouten hinzuzufügen, sofern Ihr VPN-Server mehrere Routentabellen unterstützt.

Konfigurieren des generischen Protokolls für Samsung Knox

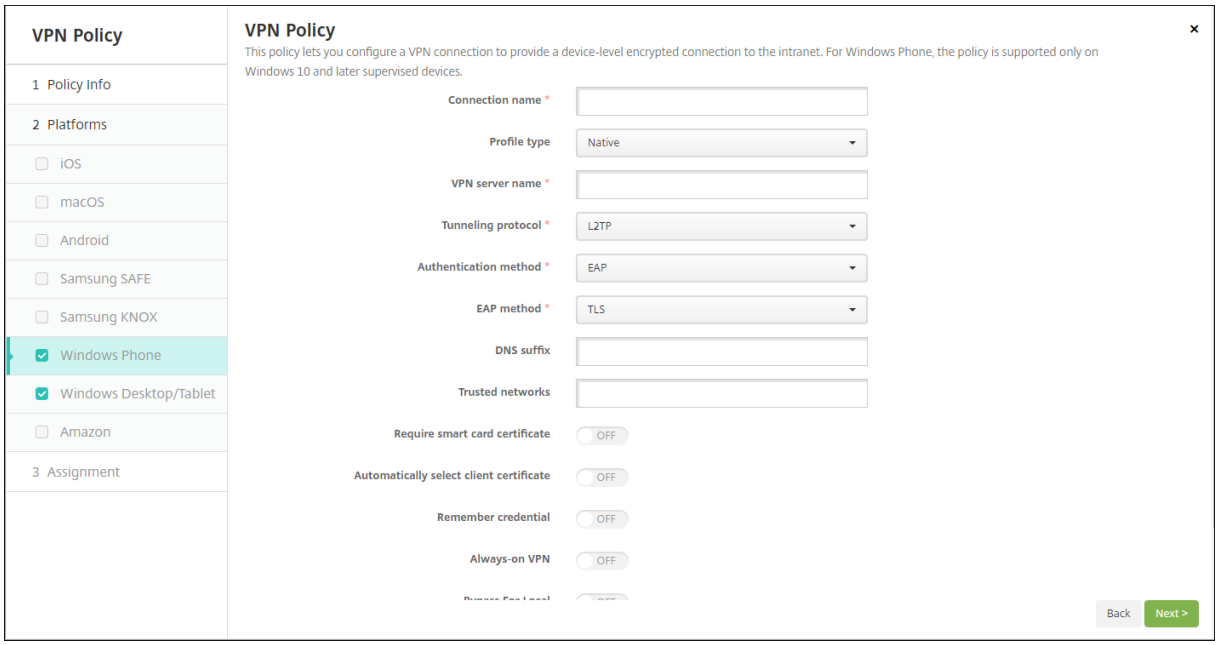
- **Verbindungsname:** Geben Sie einen Namen für die Verbindung ein. Diese Angabe ist erforderlich.
- **Paketname für Agent-VPN:** Der Paketname oder die ID der auf dem Gerät installierten VPN, z. B. Mocana oder Pulse Secure.
- **Hostname:** Geben Sie den Namen des VPN-Hosts ein. Diese Angabe ist erforderlich.
- **Benutzerauthentifizierung aktivieren**: Wählen Sie aus, ob die Benutzerauthentifizierung erforderlich sein soll. Wenn Sie diese Option aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **Benutzername:** Geben Sie einen Benutzernamen ein.
  - **Kennwort:** Geben Sie das Benutzerkennwort ein.
- **Identität:** Geben Sie optional einen Bezeichner für diese Konfiguration ein. Gilt nur, wenn **VPN-Verbindungstyp = IPSEC**.
- **VPN-Verbindungstyp:** Wählen Sie in der Liste entweder **IPSEC** oder **SSL** als Verbindungstyp aus. Die Standardeinstellung ist **IPSEC**. In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen Verbindungstypen erläutert.
- **Konfigurieren der Einstellungen für IPsec-Verbindungen**
  - **ID-Typ für IPsec-Gruppe:** Wählen Sie in der Liste den IPsec-Gruppen-ID-Typ aus. Der Standardwert ist **Standard**. Mögliche Optionen:
    - **Standard**
    - **IPv4-Adresse**
    - **Vollqualifizierter Domänenname (FQDN)**
    - **Benutzer-FQDN**
    - **IKE-Schlüssel-ID**
  - **IKE-Version:** Wählen Sie in der Liste die gewünschte Internet Key Exchange-Version aus. Der Standardwert ist **IKEv1**.
  - **Authentifizierungsmethode:** Wählen Sie in der Liste die gewünschte Authentifizierungsmethode aus. Der Standardwert ist **Zertifikat**. Mögliche Optionen:
    - **Zertifikat:** Verwenden Sie Zertifikatauthentifizierung. Wenn aktiviert, klicken Sie in der Liste **Identitätsanmeldeinformationen** auf die Anmeldeinformationen, die verwendet werden sollen. Die Standardeinstellung ist **Ohne**.
    - **Vorinstallierter Schlüssel:** Verwenden Sie einen vorinstallierten Schlüssel. Wenn Sie

diese Option aktivieren, geben Sie im Feld **Vorinstallierter Schlüssel** den gemeinsamen geheimen Schlüssel ein.
    * **Hybrid RSA:** Hybridauthentifizierung mit RSA-Zertifikaten
    * **EAP MD5:** EAP-Peer wird beim EAP-Server authentifiziert, es erfolgt jedoch keine gegenseitige Authentifizierung.
    * **EAP MSCHAPv2:** Verwenden Sie Challenge Handshake Authentication von Microsoft für die gegenseitige Authentifizierung.
    * **CAC-basierte Authentifizierung**: Common Access Card (CAC) für die Authentifizierung verwenden.
- **ZS-Zertifikat:** Wählen Sie in der Liste das Zertifikat aus, das verwendet werden soll.
- **Dead Peer Detection aktivieren:** Wählen Sie aus, ob eine Verbindung mit Peers hergestellt werden soll, um sicherzustellen, dass diese erreichbar bleiben. Die Standardeinstellung ist **Aus**.
- **Standardroute aktivieren:** Wählen Sie aus, ob eine Standardroute zum VPN-Server aktiviert werden soll.
- **Mobiloptionen aktivieren:** Wählen Sie aus, ob die Mobiloptionen aktiviert werden sollen.
- **IKE-Lebensdauer in Minuten:** Geben Sie die Zeitdauer in Minuten an, nach der die VPN-Verbindung erneuert werden muss. Die Standardeinstellung ist 1440 Minuten (24 Stunden).
- **IPsec-Lebensdauer in Minuten:** Geben Sie die Zeitdauer in Minuten an, nach der die VPN-Verbindung erneuert werden muss. Die Standardeinstellung ist 1440 Minuten (24 Stunden).
- **Diffie-Hellman-Gruppenwert (Schlüsselstärke):** Wählen Sie in der Liste die Schlüsselstärke aus, die verwendet werden soll. Die Standardeinstellung ist **0**.
- **IKE Phase 1-Schlüsselaustauschmodus:** Wählen Sie als IDE Phase 1-Aushandlungsmodus entweder **Primär** oder **Aggressiv** aus. Der Standardwert ist **Primär**.
    * **Primär:** Bei der Aushandlung werden keine Informationen für mögliche Angreifer offengelegt. Der Modus ist jedoch langsamer als **Aggressiv**.
    * **Aggressiv:** Bei der Aushandlung werden einige Informationen (z. B. die IDs der aushandelnden Peers) für mögliche Angreifer offengelegt. Der Modus ist jedoch schneller als **Primär**.
- **PFS-Wert (Perfect Forward Secrecy):** Wählen Sie aus, ob durch die Verwendung von PFS bei der Neuaushandlung von Verbindungen ein erneuter Schlüsselaustausch erforderlich sein soll.
- **Split-Tunneltyp:** Wählen Sie in der Liste den gewünschten Split-Tunneltyp aus. Mögliche Optionen:
    * **Auto:** Split-Tunneling wird automatisch verwendet.
    * **Manuell:** Split-Tunneling erfolgt über die IP-Adresse und den Port, die auf dem VPN-Server angegeben wurden.

        * **Deaktiviert:** Split-Tunneling wird nicht verwendet.
    - **SuiteB-Typ:** Wählen Sie in der Liste den gewünschten Grad der NSA Suite B-Verschlüsselung aus. Die Standardeinstellung ist **GCM-128**. Mögliche Optionen:
        * **GCM-128:** AES-GCM-Verschlüsselung (128 Bit) verwenden.
        * **GCM-256:** AES-GCM-Verschlüsselung (256 Bit) verwenden.
        * **GMAC-128:** Verwenden Sie AES-GMAC-Verschlüsselung (128 Bit).
        * **GMAC-256:** AES-GMAC-Verschlüsselung (256 Bit) verwenden.
        * **Ohne:** keine Verschlüsselung verwenden.
    - **IPsec-Verschlüsselungsalgorithmus:** Vom IPsec-Protokoll verwendete VPN-Konfiguration.
    - **IKE-Verschlüsselungsalgorithmus:** Vom IPsec-Protokoll verwendete VPN-Konfiguration.
    - **IKE-Integritätsalgorithmus:** Vom IPsec-Protokoll verwendete VPN-Konfiguration.
    - **Knox:** Konfigurationen nur für Samsung Knox-Geräte.
    - **Hersteller:** ein persönliches Profil für generische Agents, die mit der Knox-API kommunizieren.
    - **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
        * **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
        * Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
    - **VPN-Zugriff pro App:** Für jeden VPN-Zugriff pro App, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
        * **VPN-Zugriff pro App:** Die VPN-Konfiguration, die die App für die Kommunikation verwendet.
        * Klicken Sie auf **Speichern**, um den VPN-Zugriff pro App zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Konfigurieren der Einstellungen für SSL-Verbindungen**
    - **Authentifizierungsmethode:** Klicken Sie in der Liste auf die gewünschte Authentifizierungsmethode. Mögliche Optionen:
        * **Not Applicable:** No authentication method applies. Dies ist die Standardeinstellung.
        * **Zertifikat:** Verwenden Sie Zertifikatauthentifizierung. Dies ist die Standardeinstellung. Wenn aktiviert, klicken Sie in der Liste Identitätsanmeldeinformationen auf die Anmeldeinformationen, die verwendet werden sollen. Die Standardeinstellung ist Ohne.
        * **CAC-basierte Authentifizierung**: Common Access Card (CAC) für die Authentifizierung verwenden.
    - **ZS-Zertifikat:** Wählen Sie in der Liste das Zertifikat aus, das verwendet werden soll.
    - **Standardroute aktivieren:** Wählen Sie aus, ob eine Standardroute zum VPN-Server aktiviert werden soll.

- **Mobiloptionen aktivieren:** Wählen Sie aus, ob die Mobiloptionen aktiviert werden sollen.
- **Split-Tunneltyp:** Wählen Sie in der Liste den gewünschten Split-Tunneltyp aus. Mögliche Optionen:
  - **Auto:** Split-Tunneling wird automatisch verwendet.
  - **Manuell:** Split-Tunneling erfolgt über die angegebene IP-Adresse und den angegebenen Port.
  - **Deaktiviert:** Split-Tunneling wird nicht verwendet.
- **SuiteB-Typ:** Wählen Sie in der Liste den gewünschten Grad der NSA Suite B-Verschlüsselung aus. Die Standardeinstellung ist GCM-128. Mögliche Optionen:
  - **GCM-128:** AES-GCM-Verschlüsselung (128 Bit) verwenden.
  - **GCM-256:** AES-GCM-Verschlüsselung (256 Bit) verwenden.
  - **GMAC-128:** Verwenden Sie AES-GMAC-Verschlüsselung (128 Bit).
  - **GMAC-256:** AES-GMAC-Verschlüsselung (256 Bit) verwenden.
  - **Ohne: Keine Verschlüsselung verwenden:** Geben Sie den SSL-Algorithmus für die Client/Server-Aushandlung ein.
- **SSL-Algorithmus:** Geben Sie den SSL-Algorithmus für die Client/Server-Aushandlung ein.
- **Knox:** Konfigurationen nur für Samsung Knox-Geräte.
- **Hersteller:** ein persönliches Profil für generische Agents, die mit der Knox-API kommunizieren.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **VPN-Zugriff pro App:** Für jeden VPN-Zugriff pro App, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **VPN-Zugriff pro App:** Die VPN-Konfiguration, die die App für die Kommunikation verwendet.
  - Klicken Sie auf **Speichern**, um den VPN-Zugriff pro App zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Windows Phone-Einstellungen



Die Einstellungen werden nur für betreute Geräte unter Windows 10 und höher unterstützt.

- **Verbindungsname:** Geben Sie einen Namen für die Verbindung ein. Diese Angabe ist erforderlich.
- **Profiltyp:** Wählen Sie in der Liste entweder **Nativ** oder **Plug-In** aus. 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:** Wählen Sie in der Liste den gewünschten VPN-Tunneltyp aus. 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:** Wählen Sie in der Liste die gewünschte Authentifizierungsmethode aus. 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 Tunneltyp auswählen. Bei Auswahl von MSChapV2 wird die Option **Automatisch Windows-Anmeldeinformationen verwenden** angezeigt. Die Standardeinstellung

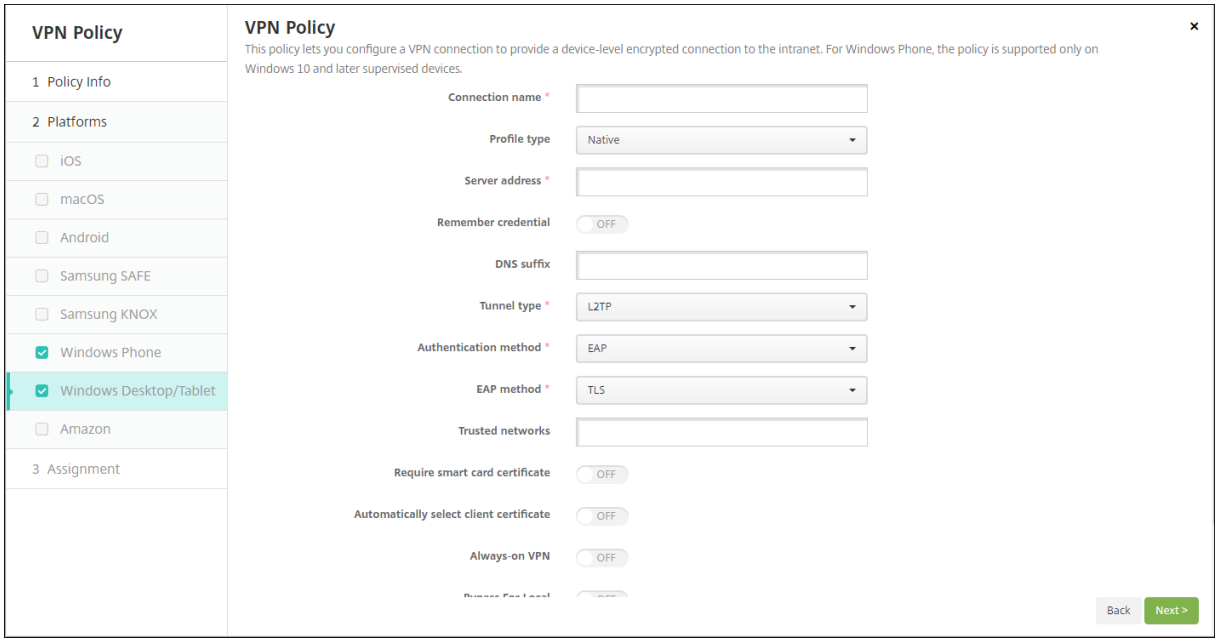
ist **Aus**.

- **EAP-Methode:** Wählen Sie in der Liste die gewünschte EAP-Methode aus. 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:** Geben 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. Die Standardeinstellung ist Aus.
- **Automatisch Clientzertifikat auswählen:** Wählen Sie aus, ob das Clientzertifikat für die Authentifizierung automatisch gewählt werden soll. Die Standardeinstellung 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. Die Standardeinstellung 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. Die Standardeinstellung 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.
  - **Serveradresse:** 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 die Profildatei aus. Informationen zu Format und anderen Details erhalten Sie bei dem Anbieter des Plug-Ins.
  - **DNS Suffix:** Geben 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. Die Standardeinstellung 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. Die Standardeinstellung 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.

Windows Desktop/Tablet-Einstellungen



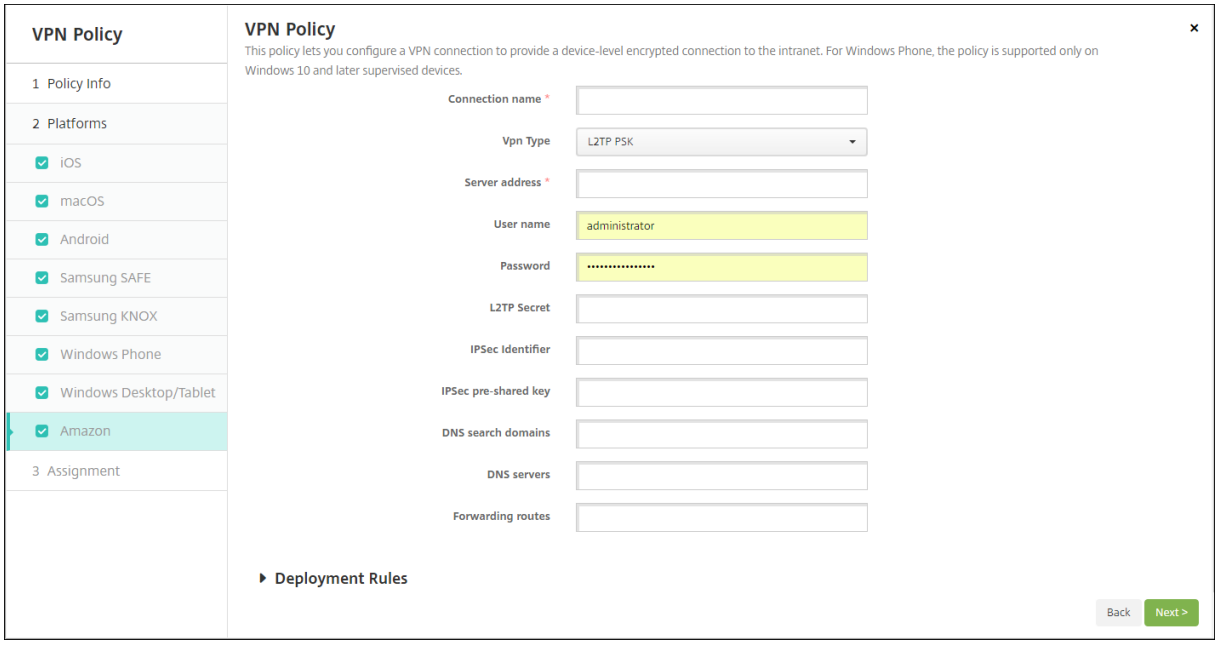
- **Verbindungsname:** Geben Sie einen Namen für die Verbindung ein. Diese Angabe ist erforderlich.
- **Profiltyp:** Wählen Sie in der Liste entweder **Nativ** oder **Plug-In** aus. Der Standardwert ist **Nativ**.
- **Einstellungen für Profiltyp "Nativ":** Diese Einstellungen gelten für in Windows-Geräte integrierte VPNs.
  - **Serveradresse:** Geben Sie den FQDN oder die IP-Adresse des VPN-Servers ein. Diese Angabe ist erforderlich.
  - **Anmeldeinformationen speichern:** Wählen Sie aus, ob die Anmeldeinformationen im Cache gespeichert werden sollen. Die Standardeinstellung ist **Aus**. Wenn diese Option aktiviert ist, werden die Anmeldeinformationen, sofern möglich, gespeichert.
  - **DNS Suffix:** Geben Sie das DNS-Suffix ein.
  - **Tunneltyp:** Wählen Sie in der Liste den gewünschten VPN-Tunneltyp aus. 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:** Wählen Sie in der Liste die gewünschte Authentifizierungsmethode aus. 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 Tunneltyp auswählen.
    - **EAP-Methode:** Wählen Sie in der Liste die gewünschte EAP-Methode aus. 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
    - **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. Die Standardeinstellung ist **Aus**.
    - **Automatisch Clientzertifikat auswählen:** Wählen Sie aus, ob das Clientzertifikat für die Authentifizierung automatisch gewählt werden soll. Die Standardeinstellung ist **Aus**. Diese Option ist nicht verfügbar, wenn **Smartcardzertifikat erforderlich** aktiviert ist.
    - **Always-on VPN:** Wählen Sie aus, ob die VPN-Verbindung immer aktiv sein soll. Die Standardeinstellung 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-Profils:** Die nachfolgenden Einstellungen gelten für VPN-Plug-Ins aus dem Windows-Store, die auf Geräten installiert sind.
    - **Serveradresse:** Geben Sie den FQDN oder die IP-Adresse des VPN-Servers ein. Diese Angabe ist erforderlich.
    - **Anmeldeinformationen speichern:** Wählen Sie aus, ob die Anmeldeinformationen im Cache gespeichert werden sollen. Die Standardeinstellung ist **Aus**. Wenn diese Option aktiviert ist, werden die Anmeldeinformationen, sofern möglich, gespeichert.
    - **DNS Suffix:** Geben Sie das DNS-Suffix 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 die Profildatei aus. Informationen zu Format und anderen Details erhalten Sie bei dem Anbieter des Plug-Ins.
    - **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.

- **Always-on VPN:** Wählen Sie aus, ob die VPN-Verbindung immer aktiv sein soll. Die Standardeinstellung 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.

Amazon-Einstellungen



- **Verbindungsname:** Geben Sie einen Namen für die Verbindung ein.
- **VPN-Typ:** Wählen Sie den Verbindungstyp aus. 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 für Amazon

- **Serveradresse:** Geben Sie die IP-Adresse des VPN-Servers ein.
- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **L2TP-Geheimnis:** Geben Sie den gemeinsamen geheimen Schlüssel ein.
- **IPSec-ID:** Geben Sie den Namen der VPN-Verbindung ein, der auf Geräten beim Herstellen einer Verbindung angezeigt wird.
- **Vorinstallierter IPSec-Schlüssel:** Geben Sie den geheimen Schlüssel ein.
- **DNS-Suchdomänen:** Geben Sie die Domänen ein, die in der Trefferliste bei der Domänensuche auf Geräten angezeigt werden können.
- **DNS-Server:** Geben Sie die IP-Adressen der DNS-Server für die Auflösung der angegebenen Domänen ein.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der L2TP RSA-Einstellungen für Amazon

- **Serveradresse:** Geben Sie die IP-Adresse des VPN-Servers ein.
- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **L2TP-Geheimnis:** Geben Sie den gemeinsamen geheimen Schlüssel ein.
- **DNS-Suchdomänen:** Geben Sie die Domänen ein, die in der Trefferliste bei der Domänensuche auf Geräten angezeigt werden können.
- **DNS-Server:** Geben Sie die IP-Adressen der DNS-Server für die Auflösung der angegebenen Domänen ein.
- **Serverzertifikat:** Wählen Sie in der Liste das Serverzertifikat aus, das verwendet werden soll.
- **ZS-Zertifikat:** Wählen Sie in der Liste das ZS-Zertifikat aus, das verwendet werden soll.
- **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der IPSEC XAUTH PSK-Einstellungen für Amazon

- **Serveradresse:** Geben Sie die IP-Adresse des VPN-Servers ein.
- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **IPSec-ID:** Geben Sie den Namen der VPN-Verbindung ein, der auf Geräten beim Herstellen einer Verbindung angezeigt wird.
- **Vorinstallierter IPSec-Schlüssel:** Geben Sie den gemeinsamen geheimen Schlüssel ein.
- **DNS-Suchdomänen:** Geben Sie die Domänen ein, die in der Trefferliste bei der Domänensuche auf Geräten angezeigt werden können.
- **DNS-Server:** Geben Sie die IP-Adressen der DNS-Server für die Auflösung der angegebenen Domänen ein.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der IPSEC AUTH RSA-Einstellungen für Amazon

- **Serveradresse:** Geben Sie die IP-Adresse des VPN-Servers ein.
- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **DNS-Suchdomänen:** Geben Sie die Domänen ein, die in der Trefferliste bei der Domänensuche auf Geräten angezeigt werden können.
- **DNS-Server:** Geben Sie die IP-Adressen der DNS-Server für die Auflösung der angegebenen Domänen ein.
- **Serverzertifikat:** Wählen Sie in der Liste das Serverzertifikat aus, das verwendet werden soll.
- **ZS-Zertifikat:** Wählen Sie in der Liste das ZS-Zertifikat aus, das verwendet werden soll.
- **Identitätsanmeldeinformationen:** Wählen Sie die gewünschten Identitätsanmeldeinformationen in der Liste aus.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der IPSEC HYBRID RSA-Einstellungen für Amazon

- **Serveradresse:** Geben Sie die IP-Adresse des VPN-Servers ein.

- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **DNS-Suchdomänen:** Geben Sie die Domänen ein, die in der Trefferliste bei der Domänensuche auf Geräten angezeigt werden können.
- **DNS-Server:** Geben Sie die IP-Adressen der DNS-Server für die Auflösung der angegebenen Domänen ein.
- **Serverzertifikat:** Wählen Sie in der Liste das Serverzertifikat aus, das verwendet werden soll.
- **ZS-Zertifikat:** Wählen Sie in der Liste das ZS-Zertifikat aus, das verwendet werden soll.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der PPTP-Einstellungen für Amazon

- **Serveradresse:** Geben Sie die IP-Adresse des VPN-Servers ein.
- **Benutzername:** Geben Sie einen optionalen Benutzernamen ein.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **DNS-Suchdomänen:** Geben Sie die Domänen ein, die in der Trefferliste bei der Domänensuche auf Geräten angezeigt werden können.
- **DNS-Server:** Geben Sie die IP-Adressen der DNS-Server für die Auflösung der angegebenen Domänen ein.
- **PPP-Verschlüsselung (MPPE):** Wählen Sie aus, ob Daten mit Microsoft-Punkt-zu-Punkt-Verschlüsselung (MPPE) verschlüsselt werden sollen. Die Standardeinstellung ist **Aus**.
- **Weiterleitungsrouten:** Wenn Ihr VPN-Server Weiterleitungsrouten unterstützt, klicken Sie für jede gewünschte Weiterleitungsroute auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Weiterleitungsroute:** Geben Sie die IP-Adresse der Weiterleitungsroute ein.
  - Klicken Sie auf **Speichern**, um die Route zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Hintergrundbild-Geräterichtlinie

August 18, 2021

Sie können eine PNG- oder JPG-Datei hinzufügen, um Hintergrundbilder auf dem Sperr- und/oder Homebildschirm von iOS-Geräten festzulegen. Nur verfügbar für betreute Geräte mit iOS 7.1.2 oder höher. 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.

iPhone

Gerät	Bildgröße in Pixeln
iPhone 12 Pro Max	2778 x 1284
iPhone 12 & iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE (2. Generation)	1334 x 750
iPhone 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 Plus	1334 x 750
iPhone 8	1334 x 750

iPad

Gerät	Bildgröße in Pixeln
iPad Pro (1., 2. und 3. Generation, 12,9”)	2732 x 2048
iPad Pro (10,5”)	2224 x 1668
iPad Pro (9,7”)	1536 x 2048
iPad Air 2	2048 x 1536

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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.

Geräterichtlinie für Webinhaltsfilter

January 5, 2022

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Filtertyp:** Klicken Sie in der Liste auf **Integriert** oder **Plug-In** und führen Sie der Auswahl entsprechende Schritte durch. Die Standardeinstellung ist **Integriert**.

Integrierter Filter

- **Webinhaltsfilter**
  - **Automatisches Filtern aktiviert:** Wählen Sie aus, ob der automatische Filter von Apple zum Analysieren von Websites auf nicht geeigneten Inhalt verwendet werden soll. Die Standardeinstellung ist **Aus**.
  - **Zulässige URLs:** Diese Liste wird ignoriert, wenn **Automatisches Filtern** aktiviert auf **Aus** festgelegt ist. Wenn **Automatisches Filtern aktiviert** auf **Ein** festgelegt ist, besteht immer Zugriff auf die Elemente in dieser Liste, unabhängig davon, ob der automatische Filter einen Zugriff zulässt. Für jede URL, die Sie der Positivliste hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen folgende Schritte aus:
    * Geben Sie die URL der zulässigen Website ein. Die URL muss mit `http://` bzw. `https://` beginnen.

        * Klicken Sie auf **Speichern**, um die Website der Positivliste hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
    - **Gesperrte URLs:** Elemente in dieser Liste werden immer blockiert. Für jede URL, die Sie der Sperrliste hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen folgende Schritte aus:
        * Geben Sie die URL der Website ein, die gesperrt werden soll. Die URL muss mit `http://` bzw. `https://` beginnen.
        * Klicken Sie auf **Speichern**, um die Website der Sperrliste hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

          > **Hinweis:**
          > Die XenMobile Server-Konsole enthält im Englischen die Begriffe “Blacklist” und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

- **Positivliste für Lesezeichen**
    - **Positivliste für Lesezeichen:** gibt die Websites an, auf die Benutzer zugreifen können. Um den Zugriff auf Websites zu ermöglichen, fügen Sie deren URL hinzu.
        * **URL:** die URL jeder Website, auf die Benutzer zugreifen können. Um beispielsweise den Zugriff auf den Secure Hub-Store zu ermöglichen, fügen Sie die URL von XenMobile Server zur Liste **URL** hinzu. Die URL muss mit `http://` bzw. `https://` beginnen. Diese Angabe ist erforderlich.
        * **Lesezeichenordner:** Geben Sie optional den Namen eines Lesezeichenordners ein. Wenn dieses Feld leer bleibt, wird das Lesezeichen in den Standardlesezeichenordner eingefügt.
        * **Titel:** Geben Sie einen aussagekräftigen Titel für die Website ein. Beispiel “Google” für die URL `https://google.com`.
        * Klicken Sie auf **Speichern**, um die Website der Positivliste hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

Plug-In-Filter

- **Filtername:** Geben Sie einen eindeutigen Namen für den Filter ein.
- **ID:** Geben Sie die Paket-ID des Filterdienst-Plug-Ins ein.
- **Dienstadresse:** Geben Sie optional eine Serveradresse ein. Gültige Formate sind IP-Adressen, Hostnamen oder URLs.
- **Benutzername:** Geben Sie optional einen Benutzernamen für den Dienst ein.
- **Kennwort:** Geben Sie optional ein Kennwort für den Dienst ein.
- **Zertifikat:** Wählen Sie in der Liste optional ein Identitätszertifikat aus, das für die Authentifizierung des Benutzers bei dem Dienst verwendet werden soll. Die Standardeinstellung ist **Ohne**.

- **WebKit-Datenverkehr filtern:** Wählen Sie aus, ob WebKit-Datenverkehr gefiltert werden soll.
- **Socket-Datenverkehr filtern:** Wählen Sie aus, ob Socket-Datenverkehr gefiltert werden soll.
- **Benutzerdefinierte Daten:** Klicken Sie für jeden benutzerdefinierten Schlüssel, den Sie dem Webfilter hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **Schlüssel:** Geben Sie den benutzerdefinierten Schlüssel ein.
  - **Wert:** Geben Sie einen Wert für den benutzerdefinierten Schlüssel ein.
  - Klicken Sie auf **Speichern**, um den benutzerdefinierten Schlüssel zu speichern, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

Webclip-Geräterichtlinie

January 5, 2022

Sie können Verknüpfungen, bzw. Webclips, für Websites platzieren, sodass sie neben den Apps auf den Benutzergeräten angezeigt werden. Für iOS-, iPadOS-, macOS- und Android-Geräte können Sie eigene Symbole für die Webclips angeben. Bei Windows-Tablets sind nur eine Beschriftung und eine URL erforderlich. Konfigurieren Sie für iOS- und iPadOS-Geräte die Geräterichtlinie "Layout für Homebildschirm", um die von Ihnen erstellten Webclips zu organisieren. Wenn Sie den App-Zugriff unter iOS beschränken, müssen Sie die Einschränkungsrichtlinie so konfigurieren, dass Webclips zugelassen werden. Informationen zum Konfigurieren dieser Richtlinien finden Sie unter Geräterichtlinie für Homebildschirmlayout und Geräteeinschränkungsrichtlinie.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-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. `https://server`.

- **Entfernbar:** Wählen Sie aus, ob Benutzer den Webclip entfernen können. Die Standardeinstellung 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. Die Standardeinstellung ist **Aus**.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-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. `https://server`.
- **Zu aktualisierendes Symbol:** Klicken Sie zur Auswahl des zu aktualisierenden Symbols auf "Durchsuchen" und navigieren Sie zum Speicherort der Datei.

Android-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. Die Standardeinstellung 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.

- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Windows Desktop/Tablet-Einstellungen

- **Name:** Geben Sie die Beschriftung ein, die mit dem Webclip angezeigt werden soll.
- **URL:** Geben Sie die URL des Webclips ein.

Wi-Fi-Geräterichtlinie

January 5, 2022

WiFi-Geräterichtlinien werden in XenMobile über die Seite **Konfigurieren > Geräterichtlinien** erstellt und bearbeitet. Mit Wi-Fi-Richtlinien können Sie festlegen, wie Benutzergeräte mit Wi-Fi-Netzwerken verbunden werden. Definieren Sie hierzu Folgendes:

- Netzwerknamen und -typen
- Authentifizierungs- und Sicherheitsrichtlinien
- Verwendung des Proxyservers
- Weitere auf WiFi bezogene Informationen

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

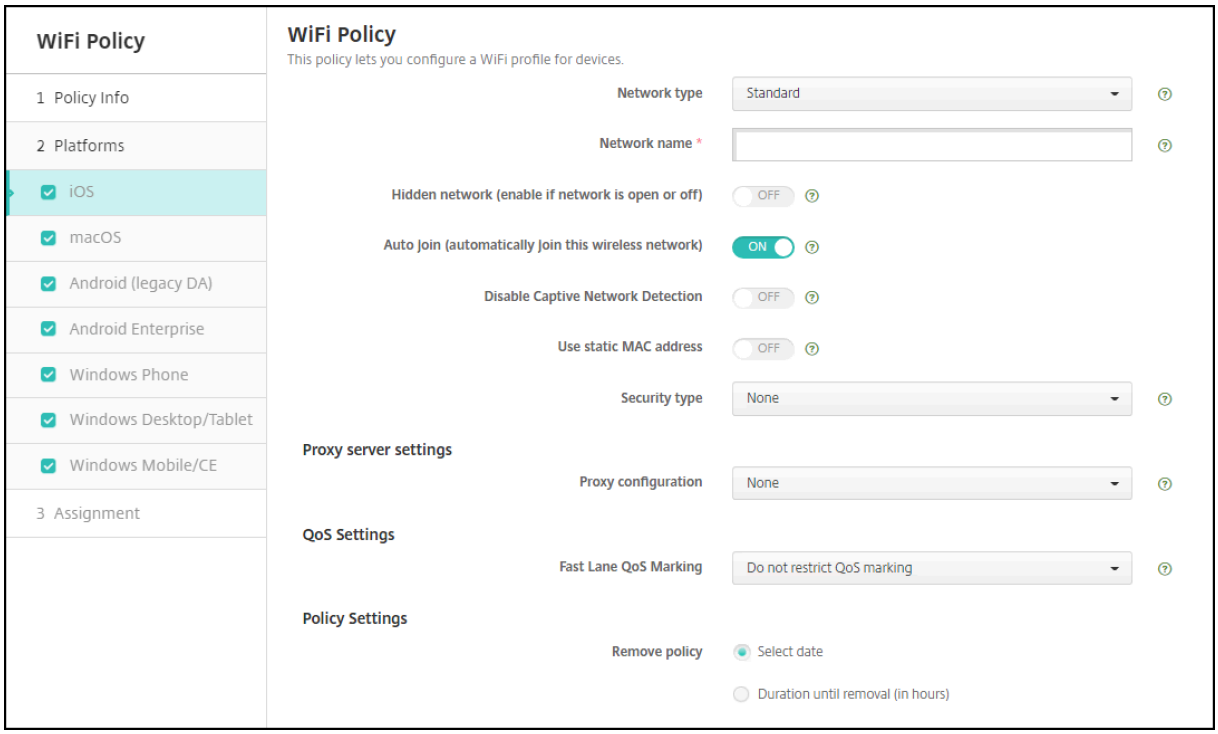
Voraussetzungen

Führen Sie vor dem Erstellen einer 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 Sie alle unter Umständen 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 und seinen Unterartikeln.

iOS-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 für das Gerät 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. Wenn ein iOS-Gerät bereits mit einem anderen Netzwerk verbunden ist, tritt es diesem Netzwerk nicht bei. Der Benutzer muss die Verbindung zum vorherigen Netzwerk trennen, bevor das Gerät au-

tomatisch eine Verbindung herstellt. Die Standardeinstellung ist **Ein**.

- **Statische MAC-Adresse verwenden:** MAC-Adressen sind eindeutige Bezeichner, die ein Gerät innerhalb eines Netzwerks überträgt. Für einen besseren Schutz der Privatsphäre können iOS- und iPadOS-Geräte bei jeder Verbindung mit einem Netzwerk eine andere MAC-Adresse verwenden. Bei Auswahl von **Ein** verwendet das Gerät immer dieselbe MAC-Adresse, wenn es eine Verbindung mit diesem Netzwerk herstellt. Bei Auswahl von **Aus** verwendet das Gerät jedes Mal eine andere MAC-Adresse, wenn es eine Verbindung mit diesem Netzwerk herstellt. Die Standardeinstellung ist **Aus**.
- **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 Enterprise: Für WPA-2 Enterprise müssen Sie Simple Certificate Enrollment Protocol (SCEP) konfigurieren. XenMobile kann das Zertifikat dann an Geräte zur Authentifizierung am WiFi-Server senden. Um SCEP zu konfigurieren, gehen Sie unter **Einstellungen > Anmeldeinformationsanbieter** zur Seite "Verteilung". Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.
  - Beliebig (Unternehmen)

In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

WPA, WPA (Persönlich), Beliebig (Persönlich) für iOS

Kennwort: Geben Sie ein optionales Kennwort ein. Wenn Sie dieses Feld leer lassen, werden die Benutzer bei der Anmeldung ggf. zur Eingabe des Kennwort aufgefordert.

WEP (Unternehmen), WPA (Unternehmen), WPA2 (Unternehmen), Beliebig (Unternehmen) für iOS

Hinweis: Alle hier ausgewählten Einstellungen werden nach den **Proxyservereinstellungen** aufgeführt.

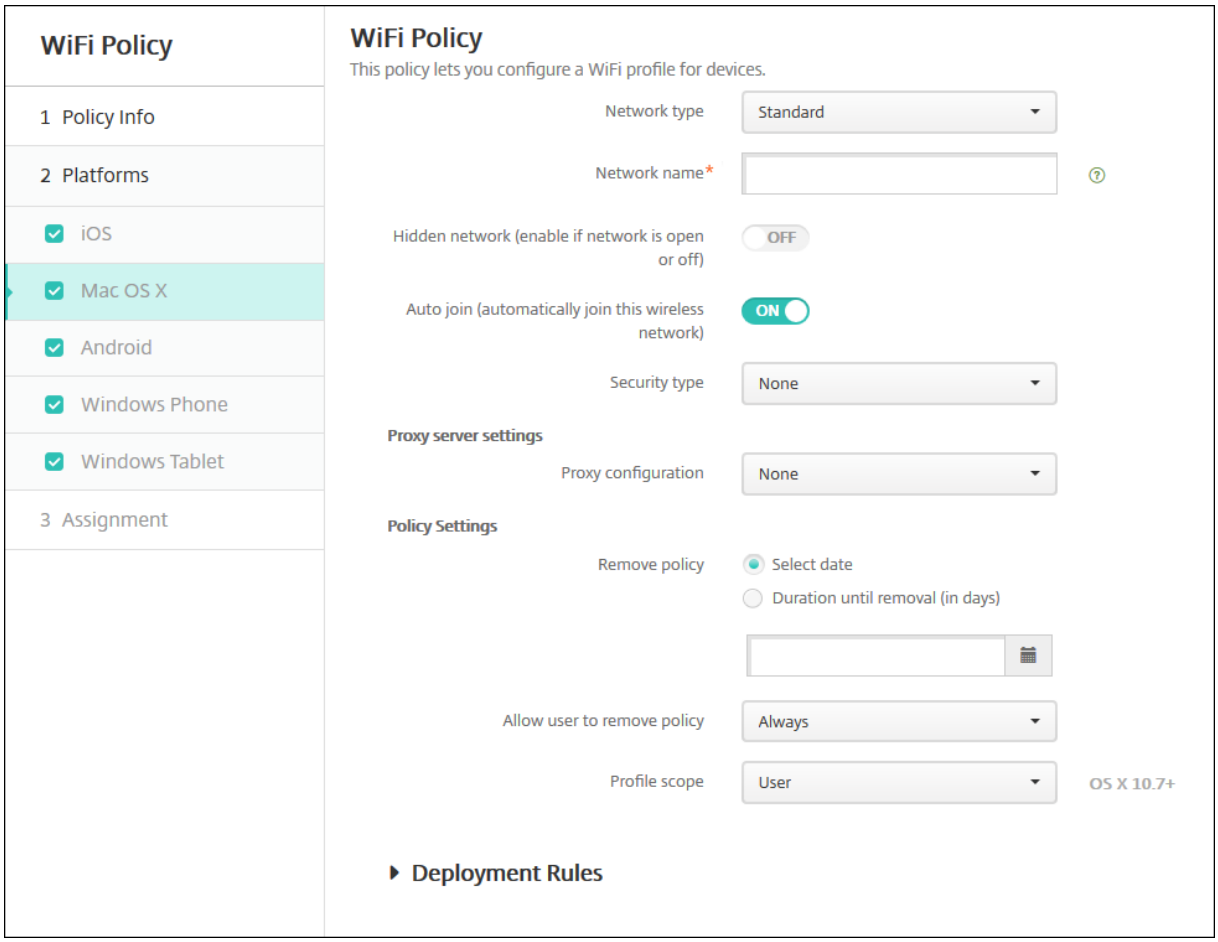
- **Protokolle, akzeptierte EAP-Typen:** Aktivieren Sie die EAP-Typen, die unterstützt werden sollen, und konfigurieren Sie dann die zugehörigen Einstellungen. Die Standardeinstellung ist für alle verfügbaren EAP-Typen **Aus**.
- **Interne Authentifizierung (TTLS):** *nur erforderlich, wenn Sie TTLS aktivieren.* Wählen Sie in der Liste die gewünschte interne Authentifizierungsmethode aus. Optionen: **PAP**, **CHAP**, **MSCHAP**

und **MSCHAPv2**. Der Standardwert ist **MSCHAPv2**.

- **Protokolle, EAP-FAST:** Wählen Sie aus, ob PACs (geschützte Zugriffsanmeldeinformationen) verwendet werden sollen.
  - Legen Sie bei Auswahl von **PAC** verwenden fest, ob eine Provisioning-PAC verwendet werden soll.
    - Bei Auswahl von **Provisioning-PAC** müssen Sie auch angeben, ob ein anonymer TLS-Handshake zwischen dem Endbenutzerclient und XenMobile zulässig ist.
      - **Anonymes PAC-Provisioning**
- **Authentifizierung:**
  - **Benutzername:** Geben Sie einen Benutzernamen ein.
  - **Kennwort für jede Verbindung:** Wählen Sie aus, ob jedes Mal ein Kennwort erforderlich sein soll, wenn die Benutzer sich anmelden.
  - **Kennwort:** Geben Sie ein optionales Kennwort ein. Wenn Sie dieses Feld leer lassen, werden die Benutzer bei der Anmeldung ggf. zur Eingabe des Kennwort aufgefordert.
  - **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen):** Klicken Sie in der Liste auf die gewünschte Art der Identitätsanmeldeinformationen. Die Standardeinstellung ist **Ohne**.
  - **Externe Identität:** *nur erforderlich, wenn Sie* **PEAP**, **TTLS** *oder* **EAP-FAST** aktivieren. Geben Sie den extern sichtbaren Benutzernamen ein. Sie können die Sicherheit durch Verwendung eines allgemeinen Namens wie etwa “Anonym” erhöhen und somit die Anzeige des Benutzernamens vermeiden.
  - **TLS-Zertifikat erforderlich:** Wählen Sie aus, ob ein TLS-Zertifikat erforderlich ist.
- **Vertrauensstellung**
  - **Vertrauenswürdige Zertifikate:** Zum Hinzufügen eines vertrauenswürdigen Zertifikats klicken Sie auf **Hinzufügen** und führen Sie für jedes gewünschte Zertifikat folgende Schritte aus:
    - **Anwendung:** Klicken Sie in der Liste auf die Anwendung, die Sie hinzufügen möchten.
    - Klicken Sie auf **Speichern**, um das Zertifikat hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
  - **Vertrauenswürdige Serverzertifikatnamen:** Zum Hinzufügen allgemeiner Namen von Serverzertifikaten, die als vertrauenswürdig eingestuft werden sollen, klicken Sie auf **Hinzufügen** und führen Sie für jeden hinzuzufügenden Namen folgende Schritte aus:
    - **Zertifikat:** Geben Sie den Namen des Serverzertifikats ein, der hinzugefügt werden soll. Sie können Platzhalter in dem Namen verwenden, z. B. “wpa.*.example.com”.
    - Klicken Sie auf **Speichern**, um den Namen des Zertifikats hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Vertrauensstellungsausnahmen zulassen:** Wählen Sie aus, ob das Dialogfeld zur Vertrauenswürdigkeit von Zertifikaten auf den Geräten angezeigt werden soll, wenn ein Zertifikat nicht vertrauenswürdig ist. Die Standardeinstellung ist **Ein**.

- **Proxyservereinstellungen**
  - **Proxykonfiguration:** Wählen Sie in der Liste **Ohne**, **Manuell** oder **Automatisch** aus, um das Routing der VPN-Verbindung über einen Proxyserver zu einzurichten. Konfigurieren Sie anschließend weitere Optionen. Die Standardeinstellung 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.
    * **Port:** 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. Die Standardeinstellung ist **Ein**. Diese Option ist nur für iOS 7.0 und höher verfügbar.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    * **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    * **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird. Nur für iOS 6.0 und höher verfügbar.

macOS-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 für das Gerät 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. Wenn ein Gerät bereits mit einem anderen Netzwerk verbunden ist, tritt es diesem Netzwerk nicht bei. Der Benutzer muss die Verbindung zum vorherigen Netzwerk trennen, bevor das Gerät automatisch eine Verbindung herstellt. Die Standardeinstellung 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) für macOS

- **Kennwort:** Geben Sie ein optionales Kennwort ein. Wenn Sie dieses Feld leer lassen, werden die Benutzer bei der Anmeldung ggf. zur Eingabe des Kennwort aufgefordert.

WEP (Unternehmen), WPA (Unternehmen), WPA2 (Unternehmen), Beliebig (Unternehmen) für macOS

Hinweis: Alle hier ausgewählten Einstellungen werden nach den **Proxyservereinstellungen** aufgeführt.

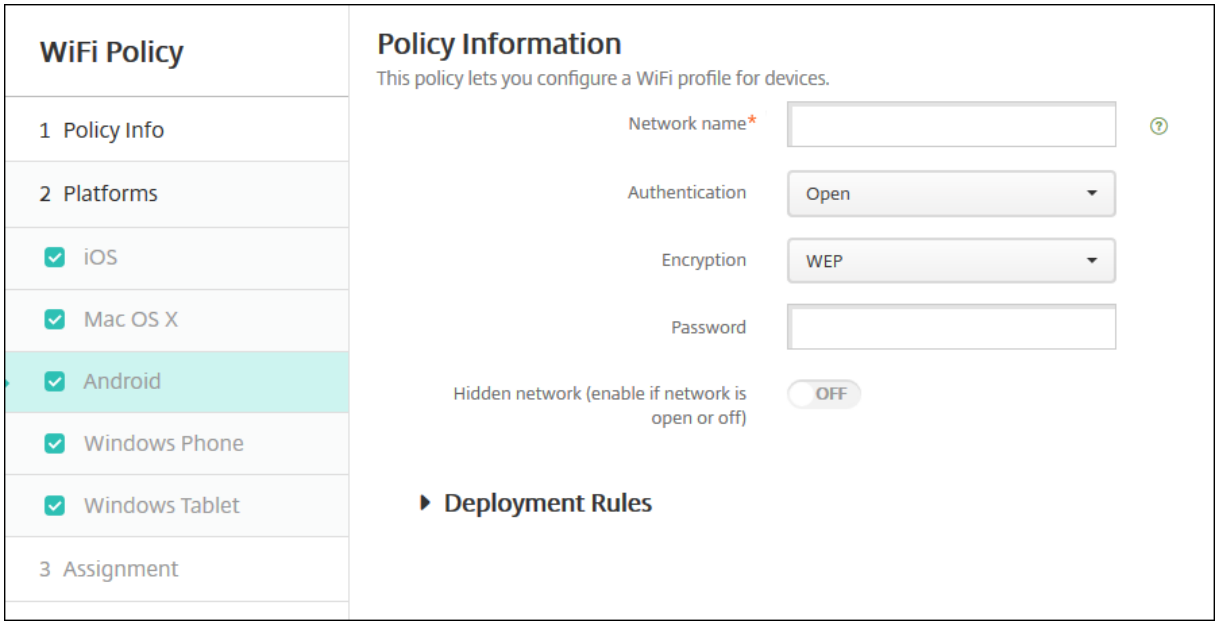
- **Protokolle, akzeptierte EAP-Typen:** Aktivieren Sie die EAP-Typen, die unterstützt werden sollen, und konfigurieren Sie dann die zugehörigen Einstellungen. Die Standardeinstellung ist für alle verfügbaren EAP-Typen **Aus**.
- **Interne Authentifizierung (TTLS):** *nur erforderlich, wenn Sie TTLS aktivieren.* Wählen Sie in der Liste die gewünschte interne Authentifizierungsmethode aus. Optionen: **PAP**, **CHAP**, **MSCHAP** und **MSCHAPv2**. Der Standardwert ist **MSCHAPv2**.
- **Protokolle, EAP-FAST:** Wählen Sie aus, ob PACs (geschützte Zugriffsanmeldeinformationen) verwendet werden sollen.
  - Legen Sie bei Auswahl von **PAC** verwenden fest, ob eine Provisioning-PAC verwendet werden soll.
    * Bei Auswahl von **Provisioning-PAC** müssen Sie auch angeben, ob ein anonymer TLS-Handshake zwischen dem Endbenutzerclient und XenMobile zulässig ist.
      · **Anonymes PAC-Provisioning**
- **Authentifizierung:**
  - **Benutzername:** Geben Sie einen Benutzernamen ein.
  - **Kennwort für jede Verbindung:** Wählen Sie aus, ob jedes Mal ein Kennwort erforderlich sein soll, wenn die Benutzer sich anmelden.
  - **Kennwort:** Geben Sie ein optionales Kennwort ein. Wenn Sie dieses Feld leer lassen, werden die Benutzer bei der Anmeldung ggf. zur Eingabe des Kennwort aufgefordert.
  - **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen):** Klicken Sie in der Liste auf die gewünschte Art der Identitätsanmeldeinformationen. Die Standardeinstellung ist **Ohne**.

  - **Externe Identität:** *nur erforderlich, wenn Sie* **PEAP**, **TTLS** *oder* **EAP-FAST** aktivieren. Geben Sie den extern sichtbaren Benutzernamen ein. Sie können die Sicherheit durch Verwendung eines allgemeinen Namens wie etwa “Anonym” erhöhen und somit die Anzeige des Benutzernamens vermeiden.
  - **TLS-Zertifikat erforderlich:** Wählen Sie aus, ob ein TLS-Zertifikat erforderlich ist.
- **Vertrauensstellung**
  - **Vertrauenswürdige Zertifikate:** Zum Hinzufügen eines vertrauenswürdigen Zertifikats klicken Sie auf **Hinzufügen** und führen Sie für jedes gewünschte Zertifikat folgende Schritte aus:
    * **Anwendung:** Klicken Sie in der Liste auf die Anwendung, die Sie hinzufügen möchten.
    * Klicken Sie auf **Speichern**, um das Zertifikat hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
  - **Vertrauenswürdige Serverzertifikatnamen:** Zum Hinzufügen allgemeiner Namen von Serverzertifikaten, die als vertrauenswürdig eingestuft werden sollen, klicken Sie auf **Hinzufügen** und führen Sie für jeden hinzuzufügenden Namen folgende Schritte aus:
    * **Zertifikat:** Geben Sie den Namen des Serverzertifikats ein, das hinzugefügt werden soll. Sie können Platzhalter in dem Namen verwenden, z. B. “wpa.*.example.com”.
    * Klicken Sie auf **Speichern**, um den Namen des Zertifikats hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Vertrauensstellungsausnahmen zulassen:** Wählen Sie aus, ob das Dialogfeld zum Vertrauen von Zertifikaten auf den Geräten angezeigt werden soll, wenn ein Zertifikat nicht vertrauenswürdig ist. Die Standardeinstellung ist **Ein**.
- **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 einzurichten. Konfigurieren Sie anschließend weitere Optionen. Die Standardeinstellung 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.
    * **Port:** 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 Proxykonfigura-

tion ein.

* **Direkte Verbindung zulassen, wenn PAC nicht erreichbar ist:** Wählen Sie aus, ob Benutzer eine direkte Verbindung mit dem Ziel herstellen dürfen, wenn die PAC-Datei nicht erreichbar ist. Die Standardeinstellung ist **Ein**. Diese Option ist nur für iOS 7.0 und höher verfügbar.

Android-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 Sicherheitstyp, der für die Wi-Fi-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.

Einstellung für Offen/Freigegeben für Android

- **Verschlüsselung:** Wählen Sie in der Liste entweder **Deaktiviert** oder **WEP** aus. Die Standardeinstellung ist **WEP**.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.

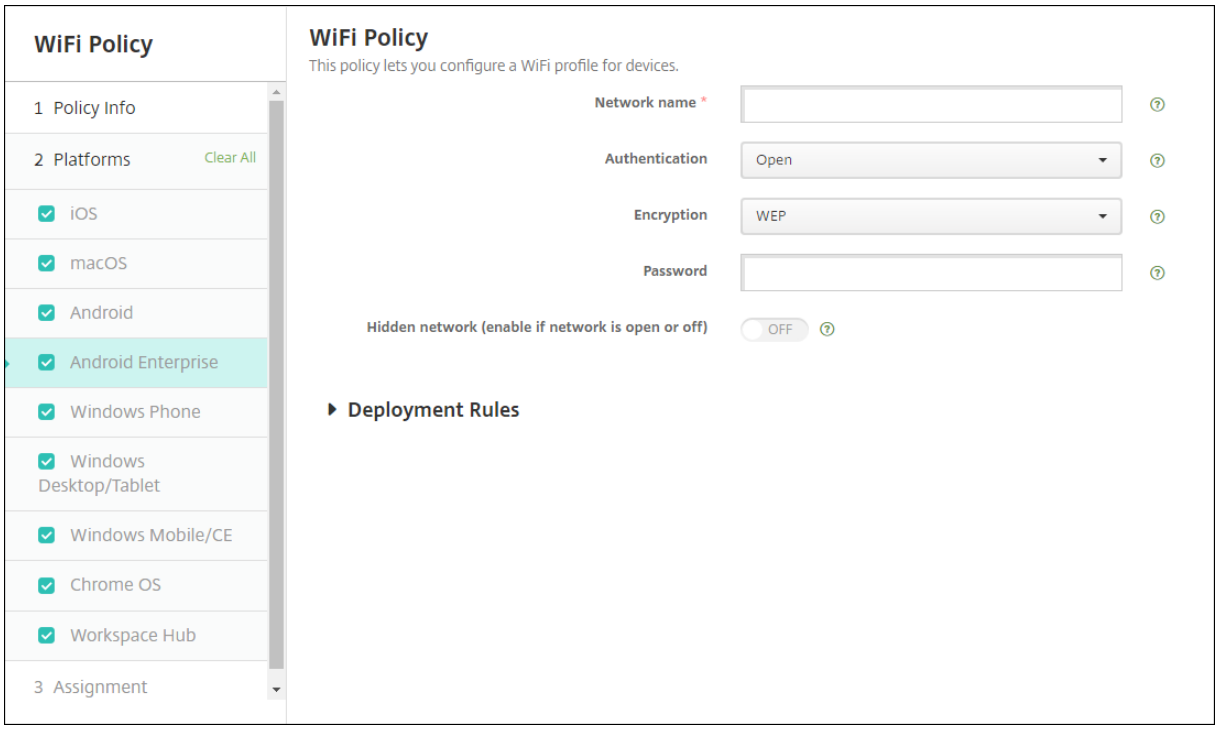
Einstellungen für WPA, WPA-PSK, WPA2, WPA2-PSK für Android

- **Verschlüsselung:** Wählen Sie in der Liste entweder **TKIP** oder **AES** aus. Die Standardeinstellung ist **TKIP**.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.

802.1x-Einstellungen für Android

- **EAP-Typ:** Wählen Sie in der Liste entweder **PEAP**, **TLS** oder **TTLS** aus. Die Standardeinstellung ist **PEAP**.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **Authentifizierungsphase 2:** Wählen Sie in der Liste entweder **Ohne**, **PAP**, **MSCHAP**, **MSCHAPPv2** oder **GTC** aus. Die Standardeinstellung ist **PAP**.
- **Identität:** Geben Sie einen optionalen Benutzernamen und die zugehörige Domäne ein.
- **Anonym:** Geben Sie einen optionalen, extern sichtbaren Benutzernamen ein. Sie können die Sicherheit durch Verwendung eines allgemeinen Namens wie etwa “Anonym” erhöhen und somit die Anzeige des Benutzernamens vermeiden.
- **ZS-Zertifikat:** Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
- **Identitätsanmeldeinformationen:** Klicken Sie in der Liste auf die Identitätsanmeldeinformationen, die verwendet werden sollen. Die Standardeinstellung ist **Ohne**.
- **Ausgeblendetes Netzwerk (aktivieren, wenn Netzwerk offen oder ausgeschaltet ist):** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

Android Enterprise-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 Sicherheitstyp, der für die Wi-Fi-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.

Einstellung für Offen/Freigegeben für Android

- **Verschlüsselung:** Wählen Sie in der Liste entweder **Deaktiviert** oder **WEP** aus. Die Standardeinstellung ist **WEP**.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.

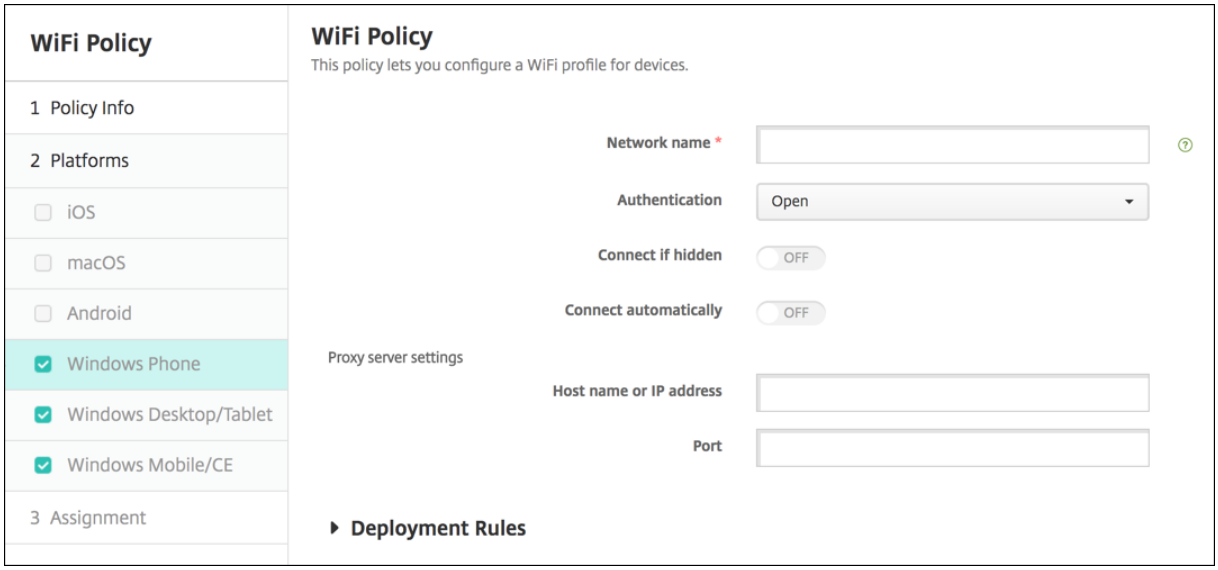
Einstellungen für WPA, WPA-PSK, WPA2, WPA2-PSK für Android

- **Verschlüsselung:** Wählen Sie in der Liste entweder TKIP oder AES aus. Die Standardeinstellung ist TKIP.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.

802.1x-Einstellungen für Android

- **EAP-Typ:** Wählen Sie in der Liste entweder **PEAP**, **TLS** oder **TTLS** aus. Die Standardeinstellung ist **PEAP**.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **Authentifizierungsphase 2:** Wählen Sie in der Liste entweder **Ohne**, **PAP**, **MSCHAP**, **MSCHAPPv2** oder **GTC** aus. Die Standardeinstellung ist **PAP**.
- **Identität:** Geben Sie einen optionalen Benutzernamen und die zugehörige Domäne ein.
- **Anonym:** Geben Sie einen optionalen, extern sichtbaren Benutzernamen ein. Sie können die Sicherheit durch Verwendung eines allgemeinen Namens wie etwa “Anonym” erhöhen und somit die Anzeige des Benutzernamens vermeiden.
- **ZS-Zertifikat:** Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
- **Identitätsanmeldeinformationen:** Klicken Sie in der Liste auf die Identitätsanmeldeinformationen, die verwendet werden sollen. Die Standardeinstellung ist **Ohne**.
- **Ausgeblendetes Netzwerk (aktivieren, wenn Netzwerk offen oder ausgeschaltet ist):** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

Windows Phone-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 Sicherheitstyp, der für die Wi-Fi-Verbindung verwendet werden soll.
  - Offen
  - WPA (Persönlich)
  - WPA-2 (Persönlich)
  - WPA-2 Enterprise: Für WPA-2 Enterprise muss SCEP konfiguriert werden. Nach erfolgter SCEP-Konfiguration kann XenMobile das Zertifikat an Geräte zur Authentifizierung am WiFi-Server senden. Um SCEP zu konfigurieren, gehen Sie zur Seite **Verteilung** unter **Einstellungen > Anmeldeinformationsanbieter**. Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.

In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

Einstellungen für Offen für Windows Phone

- **Verbinden wenn ausgeblendet:** Wählen Sie aus, ob eine Verbindung hergestellt werden soll, wenn das Netzwerk ausgeblendet ist.
- **Automatisch verbinden:** Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

Einstellungen für WPA (Persönlich), WPA-2 und Persönlich für Windows Phone

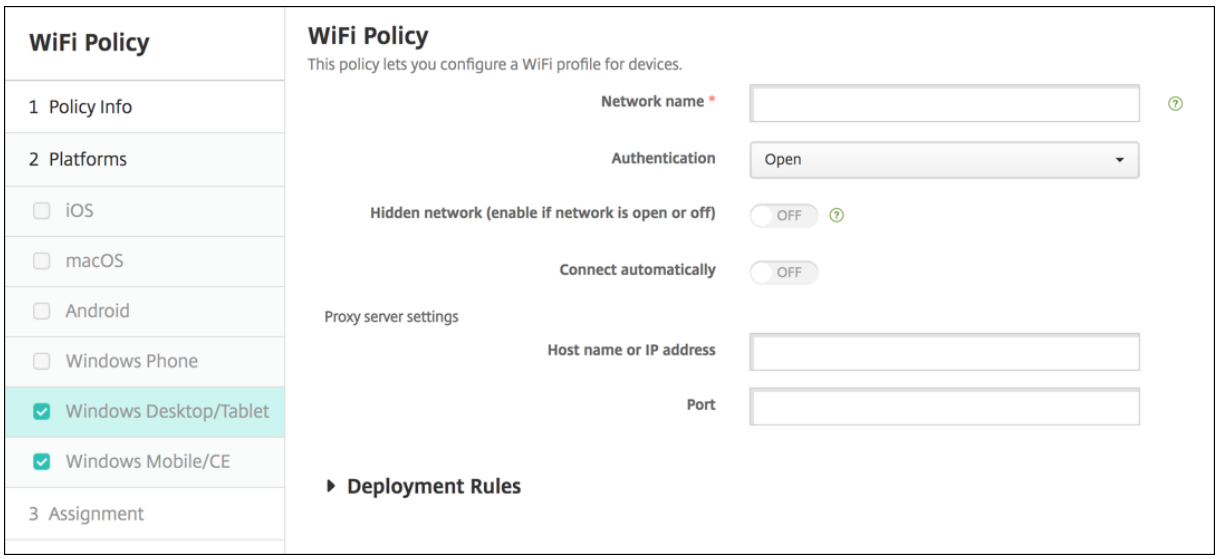
- **Verschlüsselung:** Wählen Sie in der Liste entweder **AES** oder **TKIP** aus, um den Verschlüsselungstyp festzulegen. Die Standardeinstellung ist **AES**.
- **Verbinden wenn ausgeblendet:** Wählen Sie aus, ob eine Verbindung hergestellt werden soll, wenn das Netzwerk ausgeblendet ist.
- **Automatisch verbinden:** Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

Einstellungen für WPA-2 Unternehmen für Windows Phone

- **Verschlüsselung:** Wählen Sie in der Liste entweder **AES** oder **TKIP** aus, um den Verschlüsselungstyp festzulegen. Die Standardeinstellung ist **AES**.
- **EAP-Typ:** Wählen Sie in der Liste entweder **PEAP-MSCHAPv2** oder **TLS** aus, um den EAP-Typ festzulegen. Die Standardeinstellung ist **PEAP-MSCHAPv2**.
- **Verbinden wenn ausgeblendet:** Wählen Sie aus, ob eine Verbindung hergestellt werden soll, wenn das Netzwerk ausgeblendet ist.
- **Automatisch verbinden:** Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

- **Zertifikat per Push über SCEP bereitstellen:** Wählen Sie aus, ob das Zertifikat auf den Benutzergeräten über Simple Certificate Enrollment Protocol bereitgestellt werden soll.
- **Anmeldeinformationsanbieter für SCEP:** Wählen Sie in der Liste die Anmeldeinformationsanbieter für SCEP aus. Die Standardeinstellung ist **Ohne**.
- **Proxyservereinstellungen**
  - **Hostname oder IP-Adresse:** Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein.
  - **Port:** Geben Sie die Portnummer des Proxyservers ein.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
    - **Zeit bis zum Entfernen (in Stunden):** Geben Sie ein, in wie vielen Stunden die Richtlinie entfernt wird.
  - **Benutzer darf Richtlinie entfernen:** Sie können auswählen, wann Benutzer die Richtlinie von ihrem Gerät entfernen dürfen. Wählen Sie **Immer**, **Passcode erforderlich** oder **Nie** aus dem Menü. Wenn Sie **Passcode erforderlich** auswählen, geben Sie den Passcode in das Feld **Passcode zum Entfernen** ein.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Diese Option ist nur für macOS 10.7 und höher verfügbar.

Windows 10- und Windows 11-Einstellungen



- **Authentifizierung:** Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die Wi-Fi-Verbindung verwendet werden soll.
  - Offen
  - WPA (Persönlich)
  - WPA-2 (Persönlich)
  - WPA (Unternehmen)
  - WPA-2 Enterprise: Für WPA-2 Enterprise muss SCEP konfiguriert werden. Nach erfolgter SCEP-Konfiguration kann XenMobile das Zertifikat an Geräte zur Authentifizierung am WiFi-Server senden. Um SCEP zu konfigurieren, gehen Sie zur Seite **Verteilung** unter **Einstellungen > Anmeldeinformationsanbieter**. Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.

In den folgenden Abschnitten werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen.

Einstellungen für Offen für Windows 10 und Windows 11

- **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.

Einstellungen für WPA (Persönlich), WPA-2 und Persönlich für Windows 10 und Windows 11

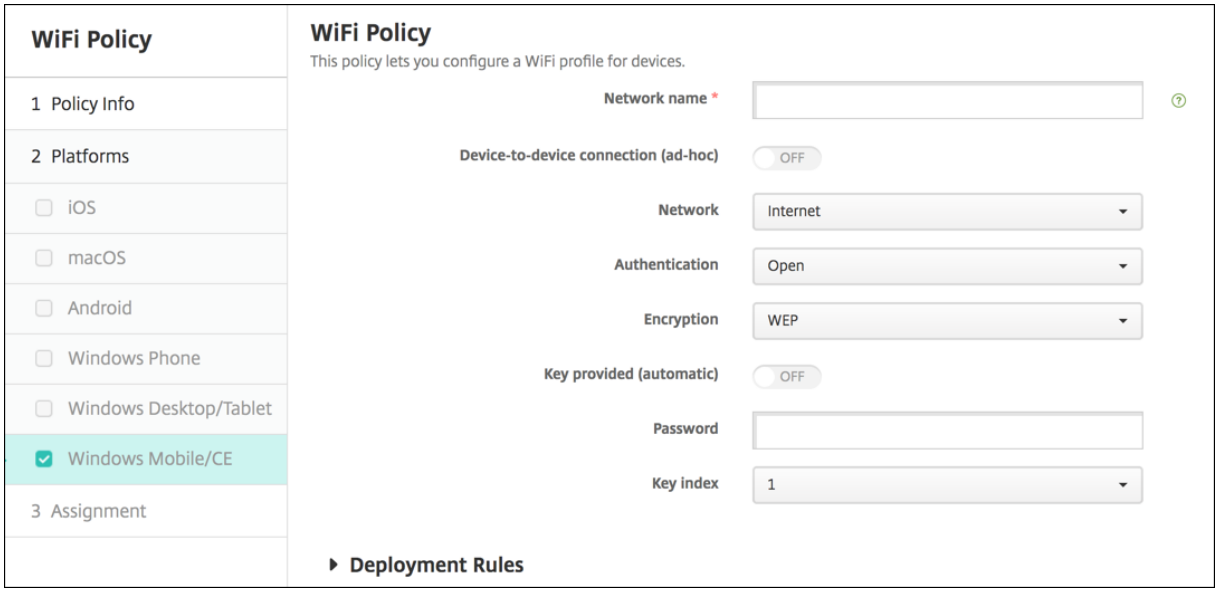
- **Verschlüsselung:** Wählen Sie in der Liste entweder **AES** oder **TKIP** aus, um den Verschlüsselungstyp festzulegen. Die Standardeinstellung ist **AES**.
- **Ausgeblendetes Netzwerk (aktivieren, wenn Netzwerk offen oder ausgeschaltet ist):** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **Automatisch verbinden:** Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

Einstellungen für WPA-2 (Unternehmen) für Windows 10 und Windows 11

- **Verschlüsselung:** Wählen Sie in der Liste entweder **AES** oder **TKIP** aus, um den Verschlüsselungstyp festzulegen. Die Standardeinstellung ist **AES**.
- **EAP-Typ:** Wählen Sie in der Liste entweder **PEAP-MSCHAPv2** oder **TLS** aus, um den EAP-Typ festzulegen. Die Standardeinstellung ist **PEAP-MSCHAPv2**.
- **Verbinden wenn ausgeblendet:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **Automatisch verbinden:** Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

- **Zertifikat per Push über SCEP bereitstellen:** Wählen Sie aus, ob das Zertifikat auf den Benutzergeräten mithilfe von Simple Certificate Enrollment Protocol bereitgestellt werden soll.
- **Anmeldeinformationsanbieter für SCEP:** Wählen Sie in der Liste die Anmeldeinformationsanbieter für SCEP aus. Die Standardeinstellung ist **Ohne**.

Windows Mobile-/CE-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 Internetquelle oder einem Intranet verbunden ist.
- **Authentifizierung:** Klicken Sie in der Liste auf den Sicherheitstyp, der für die Wi-Fi-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.

Einstellungen für Offen für Windows Mobile/CE

- **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.

Einstellungen für WPA (Persönlich), WPA-2 und Persönlich für Windows Mobile/CE

- **Verschlüsselung:** Wählen Sie in der Liste entweder **AES** oder **TKIP** aus, um den Verschlüsselungstyp festzulegen. Die Standardeinstellung ist **AES**.
- **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.

Einstellungen für WPA-2 (Unternehmen) für Windows Mobile/CE

- **Verschlüsselung:** Wählen Sie in der Liste entweder **AES** oder **TKIP** aus, um den Verschlüsselungstyp festzulegen. Die Standardeinstellung ist **AES**.
- **EAP-Typ:** Wählen Sie in der Liste entweder **PEAP-MSCHAPv2** oder **TLS** aus, um den EAP-Typ festzulegen. Die Standardeinstellung ist **PEAP-MSCHAPv2**.
- **Verbinden wenn ausgeblendet:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **Automatisch verbinden:** Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.
- **Zertifikat per Push über SCEP bereitstellen:** Wählen Sie aus, ob das Zertifikat auf den Benutzergeräten mit Simple Certificate Enrollment Protocol (SCEP) bereitgestellt werden soll.
- **Anmeldeinformationsanbieter für SCEP:** Wählen Sie in der Liste die Anmeldeinformationsanbieter für SCEP aus. Die Standardeinstellung ist **Ohne**.
- **Schlüssel (automatisch):** Wählen Sie aus, ob der Schlüssel automatisch bereitgestellt wird. Die Standardeinstellung ist **Aus**.
- **Kennwort:** Geben Sie das Kennwort in diesem Feld ein.
- **Schlüsselindex:** Geben Sie den Schlüsselindex an. Verfügbare Optionen sind **1**, **2**, **3** und **4**.

Windows CE-Geräterichtlinie für Zertifikate

April 17, 2019

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. Weitere Informationen über Zertifikate und PKI-Entitäten finden Sie unter Zertifikate.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows CE-Einstellungen

- **Anmeldeinformationsanbieter:** Klicken Sie in der Liste auf den Anmeldeinformationsanbieter. Die Standardeinstellung 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%\
  - %My Documents%\
  - %Windows%\
- **Zieldateiname:** Geben Sie den Namen der Datei mit den Anmeldeinformationen ein.

Geräterichtlinie für Windows Information Protection

January 5, 2022

Windows Information Protection (WIP, zuvor “Unternehmensdatenschutz” oder auch “EDP”) ist eine Windows-Technologie zum Schutz vor der Preisgabe von Unternehmensdaten. Datenlecks können auftreten, wenn Unternehmensdaten in nicht vom Unternehmen geschützte Apps, von einer App zur anderen oder in Bereiche außerhalb des Unternehmensnetzwerks übertragen werden. Weitere Informationen finden Sie unter Protect your enterprise data using Windows Information Protection (WIP).

Sie können über eine Geräterichtlinie in XenMobile angeben, welche Apps Windows Information Protection erfordern und eine Erzwingungsstufe festlegen. Die Richtlinie “Windows Information Protection” gilt für betreute Telefone, Tablets und Desktops mit Windows 10 oder Windows 11.

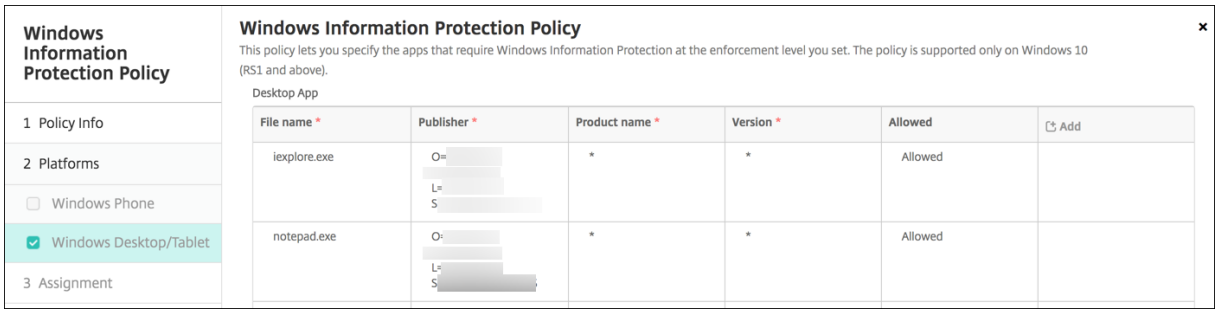
XenMobile enthält einige gebräuchliche Apps und Sie können weitere hinzufügen. Sie geben für die Richtlinie eine Erzwingungsstufe an, die sich auf die Benutzererfahrung auswirkt. Beispiel:

- Unangemessene Dateifreigaben blockieren
- Bei unangemessenen Datenfreigaben warnen und Außerkraftsetzen der Richtlinie durch die Benutzer zulassen
- WIP im Hintergrund ausführen und unangemessene Datenfreigaben zulassen und protokollieren

Um Apps von Windows Information Protection auszuschließen, definieren Sie die Apps in Microsoft AppLocker-XML-Dateien und importieren die Dateien in XenMobile.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows 10- und Windows 11-Einstellungen



- **Desktop-App** (Windows 10 oder Windows 11 Desktop), **Store-App** (Windows 10 Phone und Windows 10 oder Windows 11 Tablet): XenMobile enthält einige gängige Apps, wie im Beispiel oben gezeigt. Sie können diese nach Bedarf bearbeiten oder entfernen.

  Klicken Sie zum Hinzufügen weiterer Apps in der Tabelle **Desktop-App** bzw. **Store-App** auf **Hinzufügen** und geben Sie die App-Informationen ein.

  Zugelassene Apps können Unternehmensdaten lesen, erstellen und aktualisieren. **Abgelehnte** Apps können nicht auf Unternehmensdaten zugreifen. **Ausnahme**-Apps können Unternehmensdaten lesen, jedoch nicht erstellen oder ändern.

  - **AppLocker-XML:** Microsoft stellt eine Liste der Microsoft-Apps bereit, bei denen Kompatibilitätsprobleme mit WIP bekannt sind. Zum Ausschließen dieser Apps aus WIP klicken Sie auf **Durchsuchen**, um die Liste hochzuladen. XenMobile führt die hochgeladene AppLocker-XML und die konfigurierten Desktop- und Store-Apps in der an das Gerät gesendeten Richtlinie zusammen. Weitere Informationen finden Sie unter Recommended deny list for Windows Information Protection.
  - **Erzwingungsstufe:** Wählen Sie aus, wie Windows Information Protection die Datenfreigabe schützen und verwalten soll. Die Standardeinstellung ist **Aus**.
    - **0 - Aus:** WIP ist deaktiviert und schützt bzw. überwacht keine Daten.
    - **1 - Unbeaufsichtigt:** WIP wird im Hintergrund ausgeführt, protokolliert unzulässige Datenfreigabe und blockiert nichts. Sie können die Protokolle über Reporting CSP aufrufen.
    - **2 - Überschreiben:** WIP warnt vor potenziell unsicheren Datenfreigaben. Die Benutzer können die Warnungen außer Kraft setzen und die Daten teilen. In diesem Modus werden Aktionen, einschließlich der Außerkraftsetzungen durch die Benutzer im Überwachungsprotokoll, verzeichnet.

    * **3 - Blockieren:** WIP verhindert, dass Benutzer potenziell unsichere Datenfreigaben vollziehen können.

- **Geschützte Domänen:** die Domänen, die im Unternehmen für die Benutzeridentitäten verwendet werden. Die Liste der Domänen zur Identitätsverwaltung stellen zusammen mit der primären Domäne die Identität Ihres Verwaltungsunternehmens dar. Die erste Domäne in der Liste ist die primäre Unternehmensidentität, die in der Windows-Benutzeroberfläche verwendet wird. Verwenden Sie "|" zum Trennen der einzelnen Listeneinträge. Beispiel: `domain1.com | domain2.com`
- **Datenwiederherstellungszertifikat:** Klicken Sie auf **Durchsuchen** und wählen Sie ein Zertifikat für die Wiederherstellung der Daten verschlüsselter Dateien. Dieses Zertifikat ist mit dem des Datenwiederherstellungsagent (DRA) für EFS (Encrypting File System) identisch, allerdings wird es per MDM anstatt per Gruppenrichtlinie bereitgestellt. Ist kein Zertifikat für die Wiederherstellung vorhanden, erstellen Sie eines. Informationen finden Sie unter "Erstellen eines Datenwiederherstellungszertifikats" im vorliegenden Artikel.
- **Netzwerkdomänennamen:** Liste der Domänen, die die Grenzen des Unternehmens umfassen. WIP schützt den gesamten Datenverkehr an die vollständig qualifizierten Domänen in der Liste. Anhand dieser Einstellung und der Einstellung **IP-Bereich** wird erkannt, ob ein Netzwerkendpunkt zum Unternehmen oder einem privaten Netzwerk gehört. Verwenden Sie Kommas zum Trennen der einzelnen Listeneinträge. Beispiel: corp.beispiel.com,region.beispiel.com
- **IP-Bereich:** Eine Liste der IPv4- und IPv6-Bereiche des Unternehmens, durch die die Computer im Unternehmensnetzwerk definiert sind. WIP betrachtet diese Adressen als sicheres Ziel für die Freigabe von Unternehmensdaten. Verwenden Sie Kommas zum Trennen der einzelnen Listeneinträge. Beispiel:

  `10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **IP-Bereichsliste ist maßgebend:** Soll die automatische Erkennung von IP-Adressbereichen durch Windows verhindert werden legen Sie diese Einstellung auf **Ein** fest. Die Standardeinstellung ist **Aus**.
- **Proxyserver:** Liste der Proxyserver, die das Unternehmen für Unternehmensressourcen verwenden kann. Diese Einstellung ist erforderlich, wenn Sie einen Proxyserver im Netzwerk verwenden. Ohne Proxyserver sind Unternehmensressourcen möglicherweise nicht verfügbar, wenn ein Client sich hinter einem Proxyserver befindet. Beispielsweise sind Ressourcen über bestimmte Wi-Fi-Hotspots in Hotels und Restaurants möglicherweise nicht verfügbar. Verwenden Sie Kommas zum Trennen der einzelnen Listeneinträge. Beispiel:

  `proxy.example.com:80;157.54.11.118:443`

- **Interne Proxyserver:** Liste der Proxyserver, über die Ihre Geräte auf Cloudressourcen zugreifen. Die Verwendung dieses Servertyps bedeutet, dass die Cloudressourcen, mit denen Sie eine Verbindung herstellen, Unternehmensressourcen sind. Setzen Sie keinen der Server der Einstellung **Proxyserver** auf diese Liste, die für den nicht von WIP geschützten Datenverkehr verwendet werden. Verwenden Sie Kommas zum Trennen der einzelnen Listeneinträge. Beispiel:

  ```
  example.internalproxy1.com;10.147.80.50
  ```

- **Cloudressourcen:** Liste der durch WIP geschützten Cloudressourcen. Für jede Cloudressource können Sie optional auch einen Proxyserver in der Liste **Proxyserver** angeben, um den Datenverkehr für diese Cloudressource zu routen. Der gesamte über die **Proxyserver** geleitete Datenverkehr wird als Unternehmensdatenverkehr behandelt. Verwenden Sie Kommas zum Trennen der einzelnen Listeneinträge. Beispiel:

  ```
  domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.
  domain2.com
  ```

- **Bei Sperre Schutz erfordern:** gilt nur für Windows 10 Phone. Bei Einstellung von **Ein** wird außerdem die Passcode-Richtlinie benötigt. Ansonsten schlägt die Bereitstellung der Windows Information Protection-Richtlinie fehl. Wenn diese Richtlinie auf **Ein** festgelegt ist, wird außerdem die Einstellung **Bei Sperre Schutz erfordern** angezeigt. Die Standardeinstellung ist **Aus**.

- **Bei Sperre Schutz erfordern:** gilt nur für Windows 10 Phone. Gibt an, ob Unternehmensdaten mit einem Schlüssel auf einem gesperrten, durch eine Mitarbeiter-PIN geschützten Gerät verschlüsselt werden sollen. Apps können Unternehmensdaten auf gesperrten Geräten nicht lesen. Die Standardeinstellung ist **Ein**.

- **Beim Aufheben der Registrierung WIP-Zertifikat widerrufen:** gibt an, ob lokale Verschlüsselungsschlüssel von einem Benutzergerät widerrufen werden sollen, wenn die Registrierung des Geräts bei Windows Information Protection aufgehoben wird. Nach einem Widerruf von Verschlüsselungsschlüsseln kann der Benutzer nicht mehr auf verschlüsselte Unternehmensdaten zugreifen. Bei Auswahl von **Aus** werden die Schlüssel nicht widerrufen und der Benutzer hat nach dem Aufheben der Registrierung weiterhin Zugriff auf geschützte Dateien. Die Standardeinstellung ist **Ein**.

- **Symbolüberlagerungen anzeigen:** gibt an, ob die Windows Information Protection-Symbolüberlagerung für Unternehmensdateien in Explorer und Unternehmens-App-Kacheln im Startmenü angezeigt werden soll. Die Standardeinstellung ist **Aus**.

Erstellen eines Datenwiederherstellungszertifikats

Ein Datenwiederherstellungszertifikat ist zum Aktivieren der Richtlinie **Windows Information Protection** erforderlich.

1. Öffnen Sie auf der Maschine mit der XenMobile-Konsole eine Eingabeaufforderung und navigieren Sie zu einem Ordner (außer Windows\System32), in dem das Zertifikat erstellt werden soll.
2. Führen Sie folgenden Befehl aus:

   ```
   cipher /r:ESFDRA
   ```

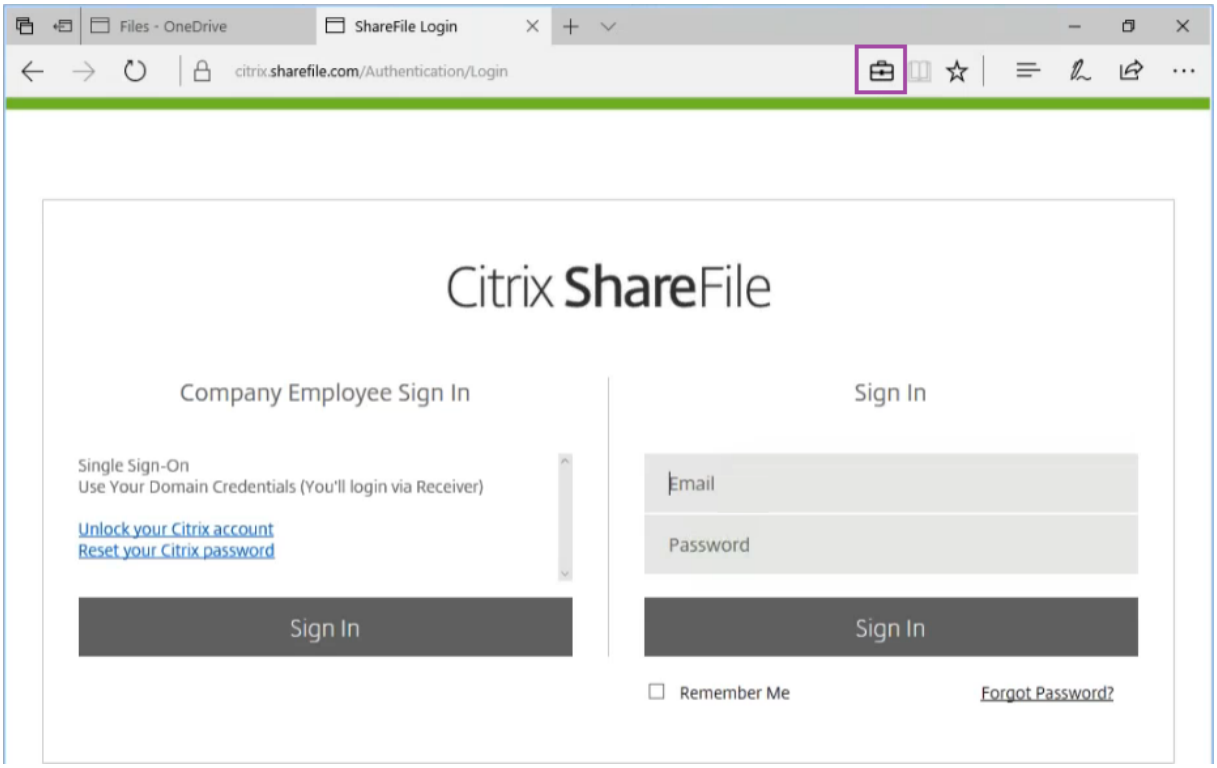
3. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort zum Schutz der Datei mit dem privaten Schlüssel ein.

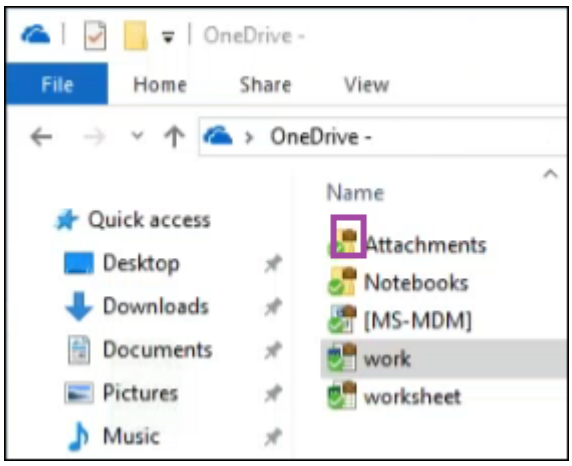
   Der cipher-Befehl erstellt eine CER- und eine PFX-Datei.

4. Navigieren Sie in der XenMobile-Konsole zu **Einstellungen > Zertifikate** und importieren Sie die CER-Datei. Diese gilt für Windows 10- und Windows 11-Tablets und Windows 10-Telefone.

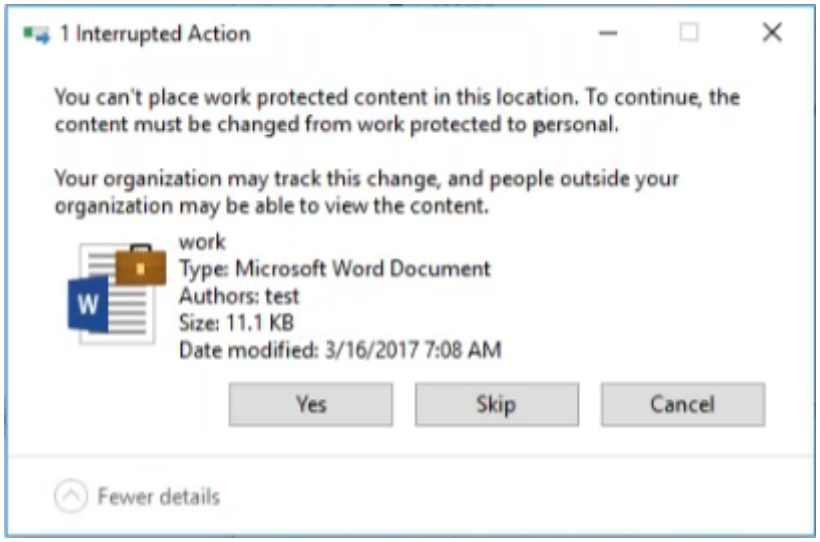
Benutzererfahrung

Wenn Windows Information Protection aktiviert ist, wird für Apps und Dateien folgendes Symbol angezeigt:





Wenn ein Benutzer eine geschützte Datei an einen nicht geschützten Speicherort kopiert oder dort speichert, wird abhängig von der konfigurierten Erzwingungsstufe die folgende Benachrichtigung angezeigt.



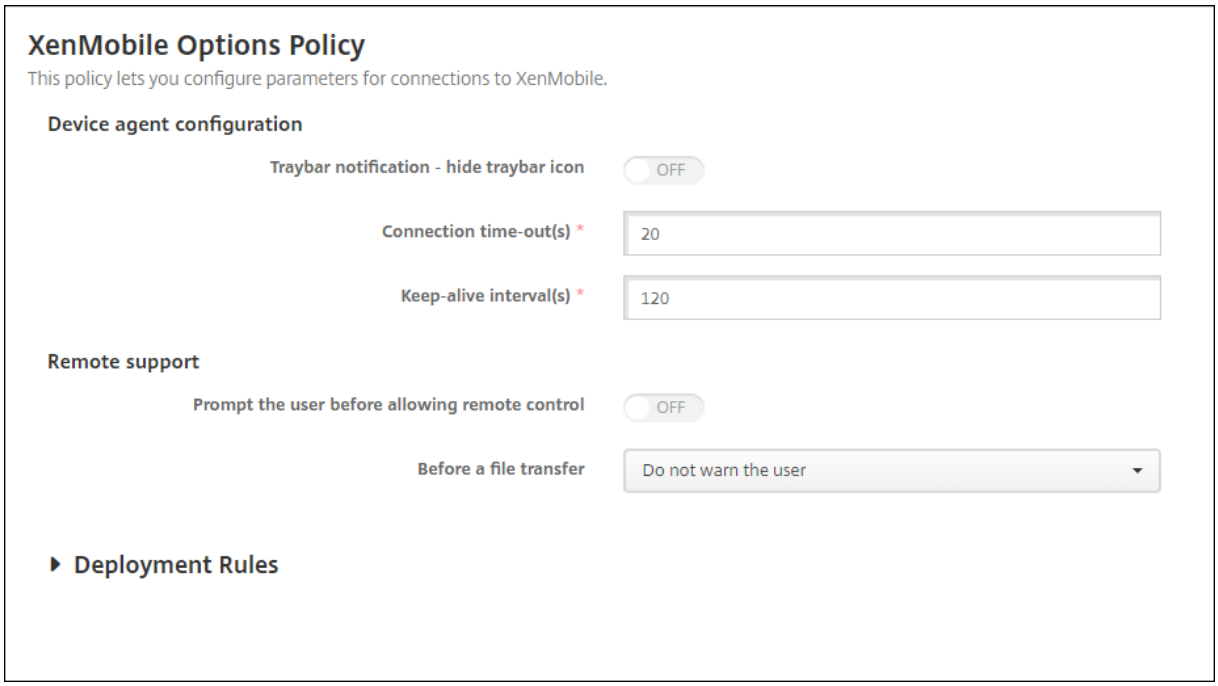
XenMobile-Optionsrichtlinie für Geräte

November 9, 2020

Sie fügen eine XenMobile-Optionsrichtlinie hinzu, um das Secure Hub-Verhalten für Verbindungen zwischen XenMobile und Android- bzw. Windows Mobile/CE-Geräten zu konfigurieren.

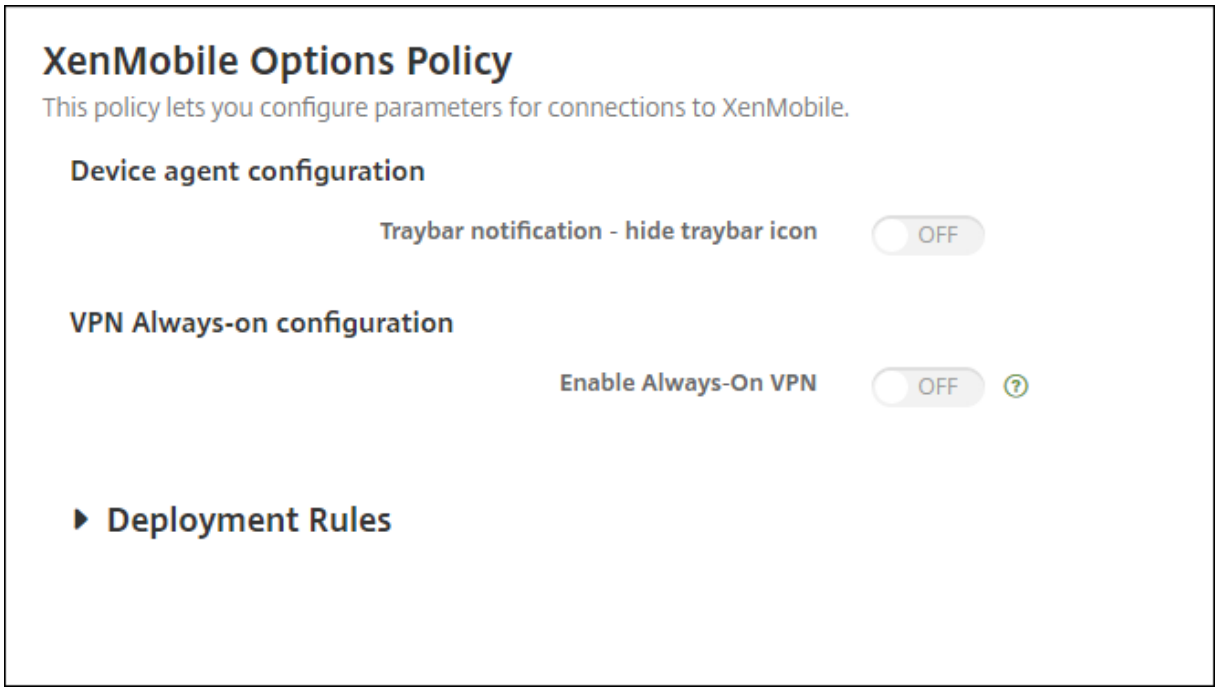
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android-Einstellungen



- **Benachrichtigung im Infobereich - Infobereichssymbol ausblenden:** Wählen Sie aus, ob das Taskleistensymbol angezeigt oder ausgeblendet werden soll. Die Standardeinstellung 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. Die Standardeinstellung 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**.

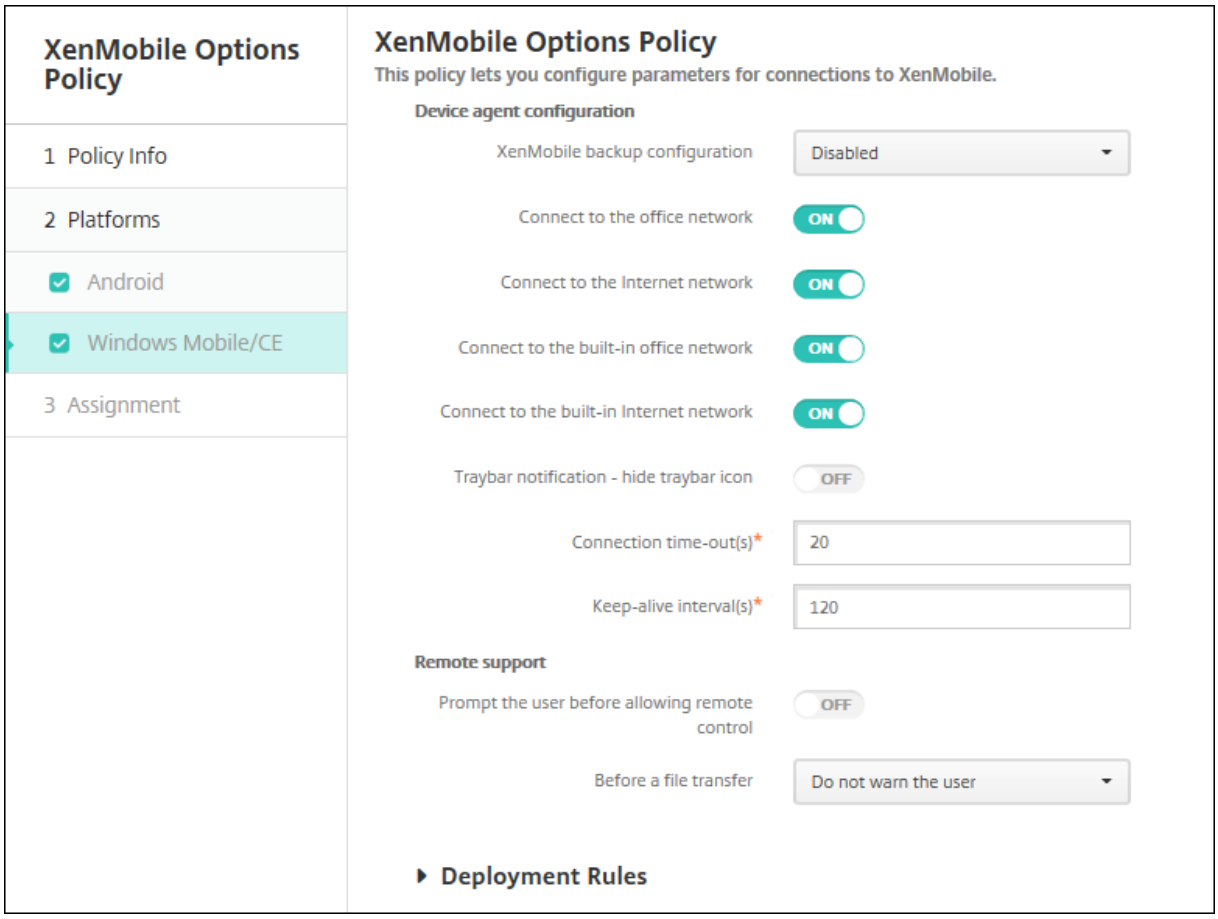
Android Enterprise-Einstellungen



Unterstützt ab Android Version 7.

- **Benachrichtigung im Infobereich - Infobereichssymbol ausblenden:** Wählen Sie aus, ob das Taskleistensymbol angezeigt oder ausgeblendet werden soll. Die Standardeinstellung ist **Aus**.
- **Aktivieren Sie Always-On-VPN.** Wählen Sie aus, ob das Always-On-VPN aktiviert ist. Ist diese Einstellung auf **Ein** gesetzt ist, wird der VPN-Dienst gestartet, wenn das Gerät eingeschaltet wird und wird weiter ausgeführt solange das Gerät eingeschaltet ist. Die Standardeinstellung ist **Aus**.
- **VPN-Paket.** Geben Sie den Paketnamen der VPN-App ein, die das Gerät verwendet. Standardmäßig wird der Paketname der Citrix SSO-App, **com.citrix.CitrixVPN**, automatisch in dieses Feld eingetragen.

Windows Mobile-/CE-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 der Einstellung **Ein** erkennt XenMobile das Netzwerk automatisch.
  - **Mit integriertem Internet-Netzwerk verbinden:** Bei der Einstellung **Ein** erkennt XenMobile das Netzwerk automatisch.
  - **Benachrichtigung im Infobereich - Infobereichssymbol ausblenden:** Wählen Sie aus, ob das Taskleistensymbol angezeigt oder ausgeblendet werden soll. Die Standardeinstellung 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. Die Standardeinstellung 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**.

XenMobile-Deinstallationsrichtlinie

January 5, 2022

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Konfigurieren von Android- und Windows Mobile-/CE-Einstellungen

- **XenMobile von Geräten deinstallieren:** Wählen Sie aus, ob XenMobile von allen Geräten deinstalliert werden soll, für die Sie die Richtlinie bereitstellen. Die Standardeinstellung ist **Aus**.

Hinzufügen von Apps

January 5, 2022

Das Hinzufügen von Apps zu XenMobile bietet Funktionen für die Mobilanwendungsverwaltung (MAM). XenMobile unterstützt Sie bei der Anwendungsbereitstellung, Softwarelizenzierung, Konfiguration und Anwendungslebenszyklusverwaltung.

Die meisten App-Typen müssen zunächst MDX-fähig gemacht werden, bevor Apps an Benutzergeräte verteilt werden können. Eine Einführung in MDX finden Sie unter Informationen zum MDX Toolkit und Überblick über das MAM-SDK.

- Citrix empfiehlt die Verwendung des MAM-SDK, um Apps MDX-fähig zu machen. Sie können Apps auch weiterhin mit MDX umschließen, bis das MDX Toolkit veraltet ist. Siehe Einstellung von Features und Plattformen.
- Sie können das MDX Toolkit nicht zum Umschließen mobiler Produktivitätsapps von Citrix verwenden. Laden Sie die MDX-Dateien der mobilen Produktivitätsapps von Citrix Downloads.

Das Hinzufügen von Apps zur XenMobile-Konsole umfasst folgende Schritte:

- Konfigurieren von App-Einstellungen
- Einteilen von Apps in Kategorien, um sie in Secure Hub zu organisieren (optional)
- Definieren von Workflows zur Genehmigung des App-Zugriffs durch Benutzer (optional)
- Bereitstellen von Apps für Benutzer

Dieser Artikel beschreibt die allgemeinen Workflows zum Hinzufügen von Apps. In den folgenden Artikeln finden Sie plattformspezifische Besonderheiten:

- Verteilen von Android Enterprise-Apps
- Verteilen von Apple-Apps

App-Typen und Features

In der folgenden Tabelle sind alle App-Typen aufgeführt, die Sie mit XenMobile bereitstellen können.

App-Typ	Quellen	Hinweise	Siehe
MDX	iOS- und Android-Apps, die Sie für Ihre Nutzer entwickeln. Mobile Produktivitätsapps von Citrix.	Entwickeln Sie iOS- oder Android-Apps mit dem MAM-SDK oder umschließen Sie sie mit dem MDX Toolkit. Laden Sie für mobile Produktivitätsapps die MDX-Dateien aus dem öffentlichen Store von Citrix Downloads herunter. Fügen Sie die Apps dann zu XenMobile hinzu.	Hinzufügen von MDX-Apps
Öffentlicher App-Store	Kostenlose oder kostenpflichtige Apps aus öffentlichen App-Stores wie Google Play oder dem Apple App Store.	Laden Sie die Apps hoch, machen Sie sie MDX-fähig und fügen Sie die Apps dann zu XenMobile hinzu.	Hinzufügen von Apps aus einem öffentlichen App-Store
Web und SaaS	Ihr internes Netzwerk (Web-Apps) oder ein öffentliches Netzwerk (SaaS).	Citrix Workspace bietet mobiles Single Sign-On für native SaaS-Apps von iOS- und Android-Geräten, die bei MDM registriert sind. Oder verwenden Sie SAML-Connectors (Security Assertion Markup Language) für die Anwendungen.	Hinzufügen von Web- und SaaS-Apps

App-Typ	Quellen	Hinweise	Siehe
Enterprise	Private Apps, einschließlich Win32-Apps, die nicht MDX-fähig sind. Private Android Enterprise-Apps, die MDX-fähig sind. Unternehmensapps befinden sich an CDN-Standorten oder auf XenMobile-Servern.	Fügen Sie die Apps zu XenMobile hinzu.	Hinzufügen einer Unternehmensapp
Weblink	Internet-Webadressen, Intranet-Webadressen oder Web-Apps, für die kein Single Sign-On erforderlich ist.	Konfigurieren Sie Weblinks in XenMobile.	Hinzufügen von Weblinks

Berücksichtigen Sie bei der Planung der App-Verteilung die folgenden Features:

- Automatische Installationen
- Erforderliche und optionale Apps
- App-Kategorien
- Aktivieren von Microsoft 365-Apps
- Anwenden von Workflows
- Branding für den App-Store und Citrix Secure Hub

Automatische Installationen

Citrix unterstützt die unbeaufsichtigte Installation und das Upgrade von iOS-, Android Enterprise- und Samsung-Apps. Bei einer automatischen Installation werden Benutzer nicht aufgefordert, Apps zu installieren, die Sie für das Gerät bereitstellen. Die Apps werden automatisch im Hintergrund installiert.

Voraussetzungen für die automatische Installation:

- Versetzen Sie für iOS das verwaltete iOS-Gerät in den betreuten Modus. Einzelheiten finden Sie unter Richtlinie zum Importieren von iOS- und macOS-Profilen.

- Bei Android Enterprise werden die Apps im Android-Arbeitsprofil auf dem Gerät installiert. Details finden Sie unter Android Enterprise.
- Aktivieren Sie für Samsung-Geräte Samsung Knox auf dem Gerät.

  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.

Erforderliche und optionale Apps

Beim Hinzufügen von Apps zu einer Bereitstellungsgruppe wählen Sie aus, ob sie optional oder erforderlich sind. Citrix empfiehlt, Apps als **Erforderlich** bereitzustellen.

- Erforderliche Apps werden automatisch auf Benutzergeräten installiert, wodurch die Interaktion minimiert wird. Wenn dieses Feature aktiviert ist, können Apps auch automatisch aktualisiert werden.
- Optionale Apps ermöglichen Benutzern die Auswahl der zu installierenden Apps. Benutzer müssen die Installation jedoch manuell über Secure Hub initiieren.

Für als erforderlich markierte Apps können Benutzer u. a. in folgenden Situationen Updates schnell erhalten:

- Sie laden eine neue App hoch und legen sie als erforderlich fest.
- Sie legen eine vorhandene App als erforderlich fest.
- Ein Benutzer löscht eine erforderliche App.
- Es gibt ein Secure Hub-Update.

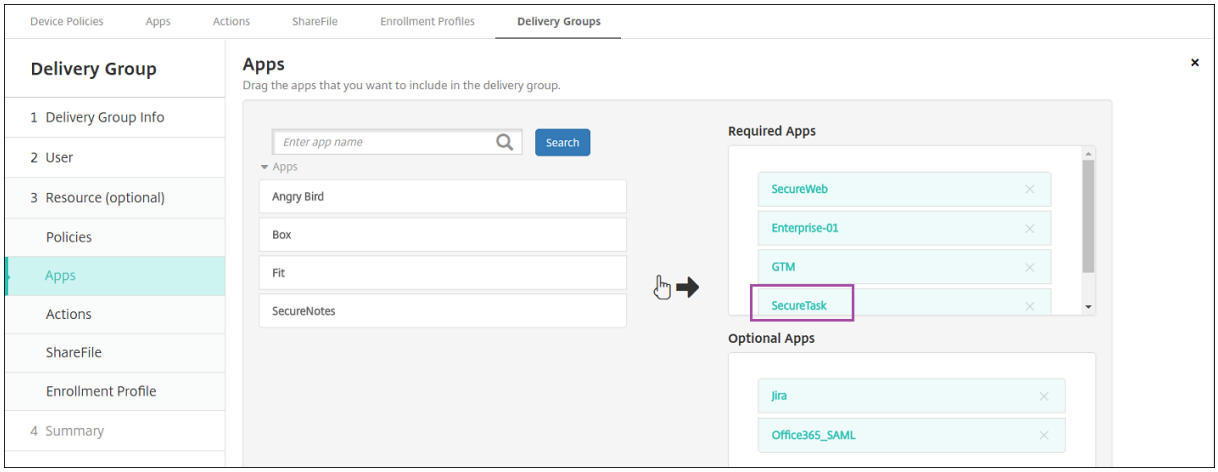
Voraussetzungen für die erzwungene Bereitstellung erforderlicher Apps

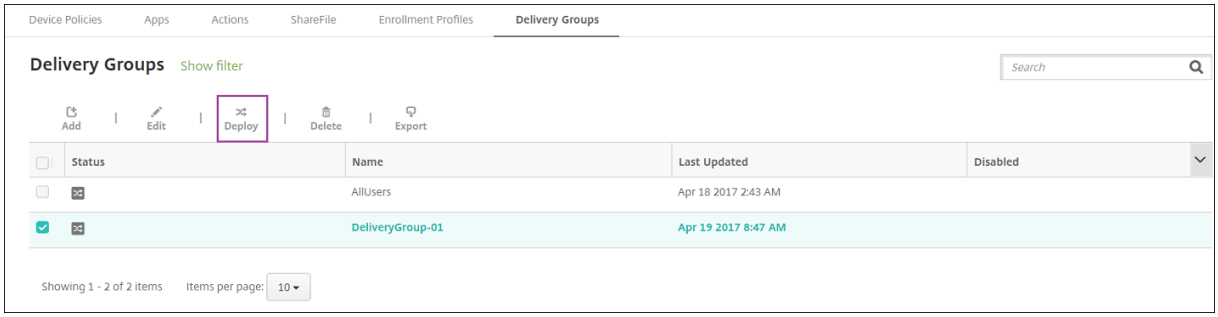
- XenMobile Server 10.6 (Mindestversion)
- Secure Hub 10.5.15 für iOS und 10.5.20 für Android (Mindestversionen)
- MAM-SDK oder MDX Toolkit 10.6 (Mindestversion)
- Benutzerdefinierte Servereigenschaft force.server.push.required.apps

  Die erzwungene Bereitstellung erforderlicher Apps ist standardmäßig deaktiviert. Um dieses Feature zu aktivieren, erstellen Sie eine benutzerdefinierte Schlüsselservereigenschaft. Legen Sie **Schlüssel** und **Anzeigename** auf **force.server.push.required.apps** fest und setzen Sie den **Wert** auf **true**.
- Nach dem Upgrade von XenMobile Server und Secure Hub müssen sich Benutzer mit registrierten Geräten abmelden und dann bei Secure Hub einmal anmelden, um die erforderlichen App-Bereitstellungsupdates zu erhalten.

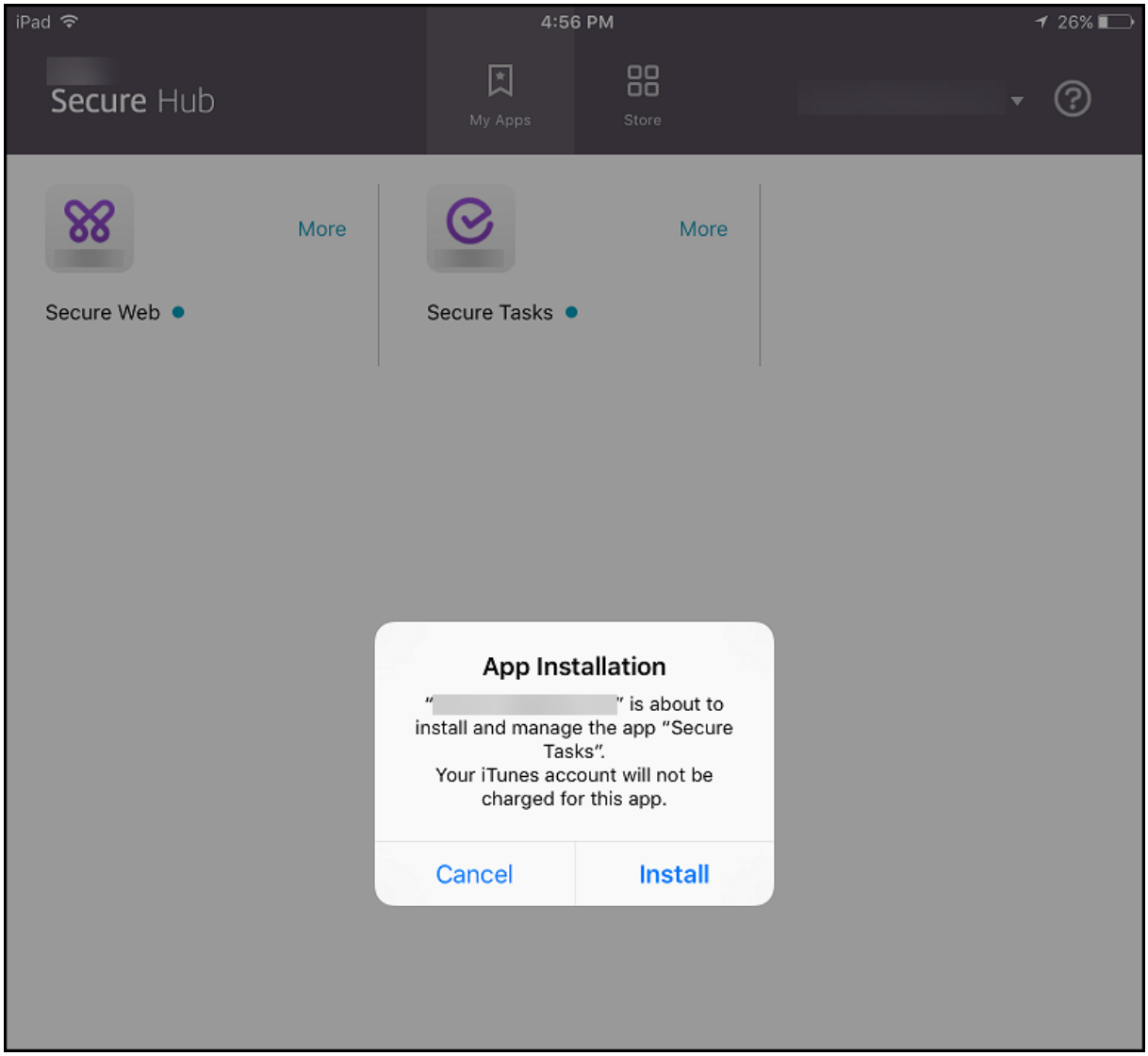
Beispiele

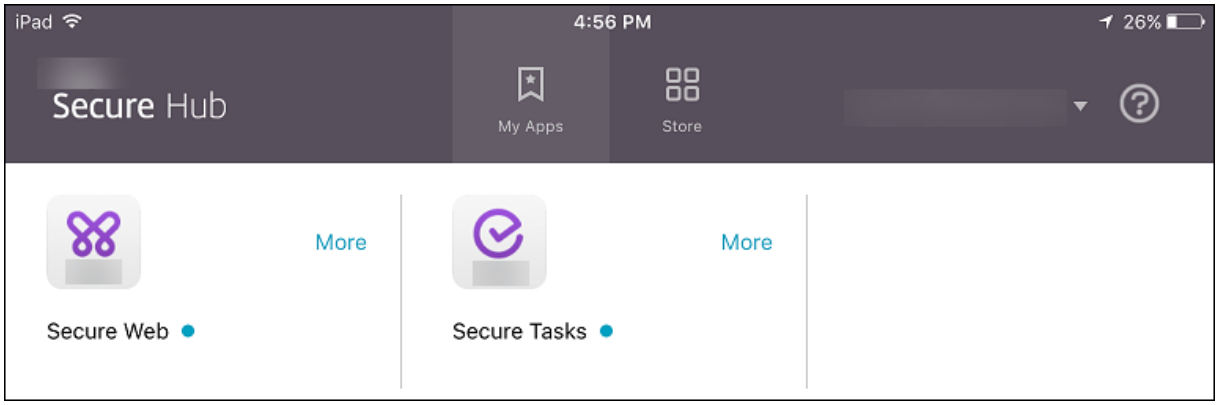
Das folgende Beispiel zeigt die Reihenfolge beim Hinzufügen der App “Secure Tasks” zu einer Bereitstellungsgruppe und dem Bereitstellen der Bereitstellungsgruppe.





Nach der Bereitstellung von Secure Tasks auf dem Gerät eines Benutzers wird dieser von Secure Hub zum Installieren der App aufgefordert.





Wichtig:

Erforderliche MDX-Apps, einschließlich Unternehmensapps und Apps aus dem öffentlichen Store, werden sofort aktualisiert. Das Upgrade erfolgt selbst, wenn Sie eine MDX-Richtlinie mit

> einem Kulanzzeitraum für App-Upgrades konfiguriert haben und ein Benutzer angibt, dass er die App später aktualisieren möchte.

iOS-Workflow für erforderliche Unternehmensapps und Apps aus dem öffentlichen Store

1. Stellen Sie die XenMobile App bei der ersten Registrierung bereit. Die erforderliche App wird im Gerät installiert.
2. Aktualisieren Sie die App in der XenMobile-Konsole.
3. Stellen Sie erforderliche Apps mit der XenMobile-Konsole bereit.
4. Die App auf dem Homebildschirm wird aktualisiert. Bei Apps aus dem öffentlichen Store wird das Upgrade automatisch gestartet. Keine Aufforderung zum Update.
5. Benutzer öffnen die App im Homebildschirm. Apps werden sofort aktualisiert, selbst wenn Sie einen Kulanzzeitraum für App-Updates festlegen und ein Benutzer die Option zum späteren Aktualisieren auswählt.

Android-Workflow für erforderliche Unternehmensapps

1. Stellen Sie die XenMobile App bei der ersten Registrierung bereit. Die erforderliche App wird im Gerät installiert.
2. Stellen Sie erforderliche Apps mit der XenMobile-Konsole bereit.
3. App wird aktualisiert. (Auf Nexus-Geräten wird eine Aufforderung angezeigt, auf Samsung-Geräten eine Installation im Hintergrund durchgeführt.)
4. Benutzer öffnen die App im Homebildschirm. Apps werden sofort aktualisiert, selbst wenn Sie einen Kulanzzeitraum für App-Updates festlegen und ein Benutzer die Option zum späteren Aktualisieren auswählt. (Auf Samsung-Geräten wird eine Installation im Hintergrund ausgeführt.)

Android-Workflow für erforderliche Apps aus dem öffentlichen Store

1. Stellen Sie die XenMobile App bei der ersten Registrierung bereit. Die erforderliche App wird im Gerät installiert.
2. Aktualisieren Sie die App in der XenMobile-Konsole.
3. Stellen Sie erforderliche Apps mit der XenMobile-Konsole bereit. Alternativ können Sie auch den Secure Hub Store auf dem Gerät öffnen. Update-Symbol wird im Store angezeigt.
4. Upgrade startet automatisch. (Bei Nexus-Geräten wird Aufforderung zum Installieren des Updates angezeigt.)
5. Öffnen Sie die App im Homebildschirm. App wird aktualisiert. Keine Aufforderung an Benutzer nach Kulanzzeitraum. (Auf Samsung-Geräten wird eine Installation im Hintergrund ausgeführt.)

Deinstallieren einer App, die als erforderliche App konfiguriert ist

Sie können Benutzern gestatten, eine App zu deinstallieren, die als erforderlich konfiguriert ist. Gehen Sie zu **Konfigurieren> Bereitstellungsgruppen** und verschieben Sie die App aus **Erforderliche Apps** in **Optionale Apps**.

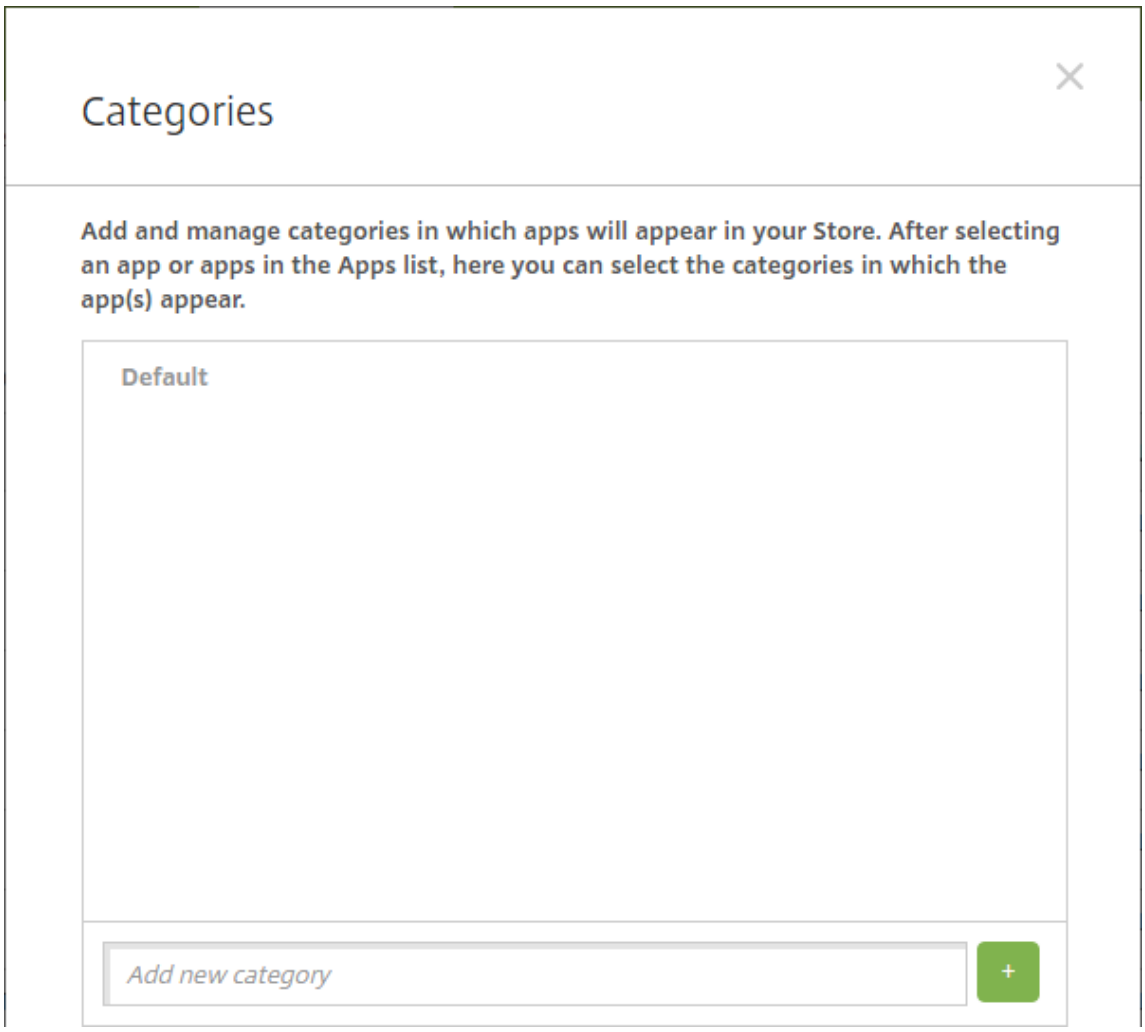
Empfohlen: Verwenden Sie eine spezielle Bereitstellungsgruppe, um eine App vorübergehend in optional zu ändern, sodass bestimmte Benutzer die App deinstallieren können. Sie können dann eine vorhandene erforderliche App in optional ändern, die App für diese Bereitstellungsgruppe bereitstellen und anschließend die App von diesen Geräten deinstallieren. Wenn anschließend für zukünftige Registrierungen für diese Bereitstellungsgruppe die App wieder erforderlich sein soll, setzen Sie die App wieder auf erforderlich.

App-Kategorien

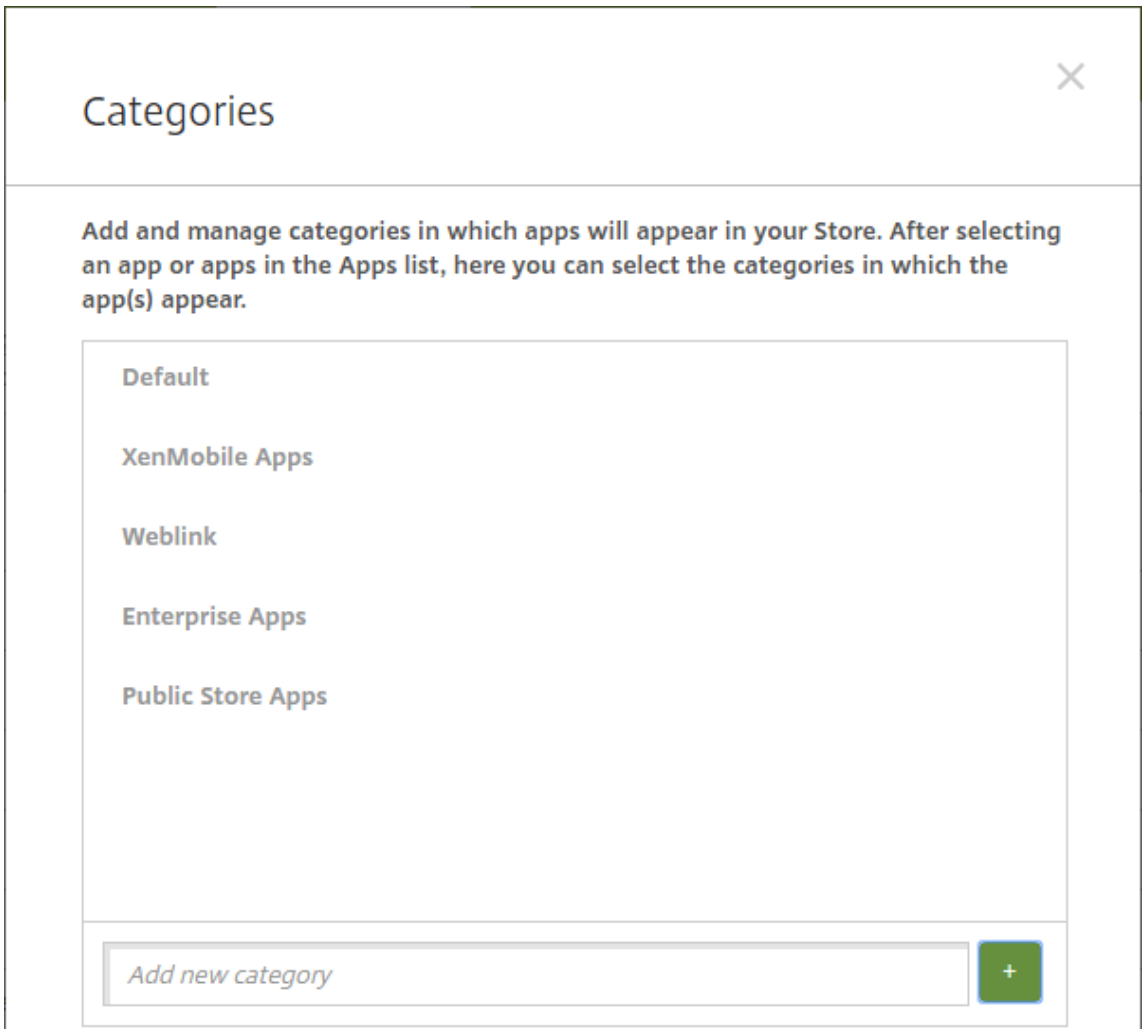
Wenn Benutzer sich bei Secure Hub anmelden, erhalten sie eine Liste der Apps, Weblinks und Stores, die Sie in XenMobile konfiguriert haben. Mit App-Kategorien können Sie dafür sorgen, dass Benutzer nur auf bestimmte Apps, Weblinks oder Stores zugreifen können. Sie können beispielsweise eine Kategorie “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.

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 > Kategorie**. Das Dialogfeld **Kategorien** wird angezeigt.



2. 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.



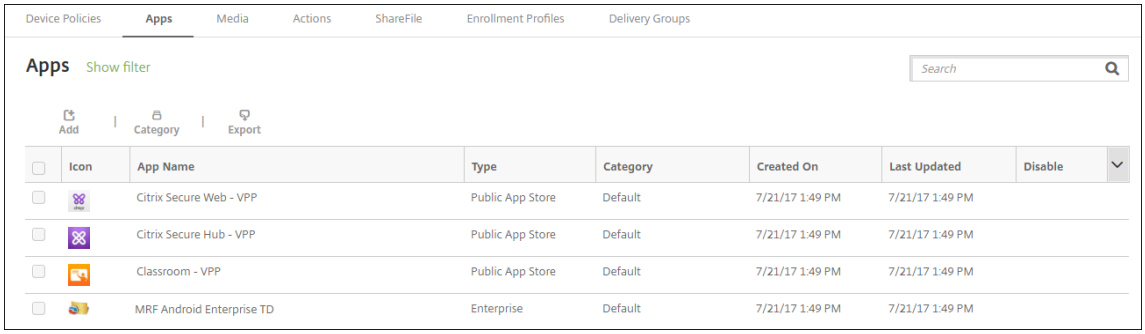
3. Wenn Sie alle Kategorien hinzugefügt haben, schließen Sie das Dialogfeld **Kategorien**.
4. Auf der Seite **Apps** können Sie vorhandene Apps einer neuen Kategorie zuweisen.
    - Wählen Sie die App aus, die Sie kategorisieren möchten.
    - Klicken Sie auf **Edit**. Die Seite **App-Informationen** 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 MDX-Apps

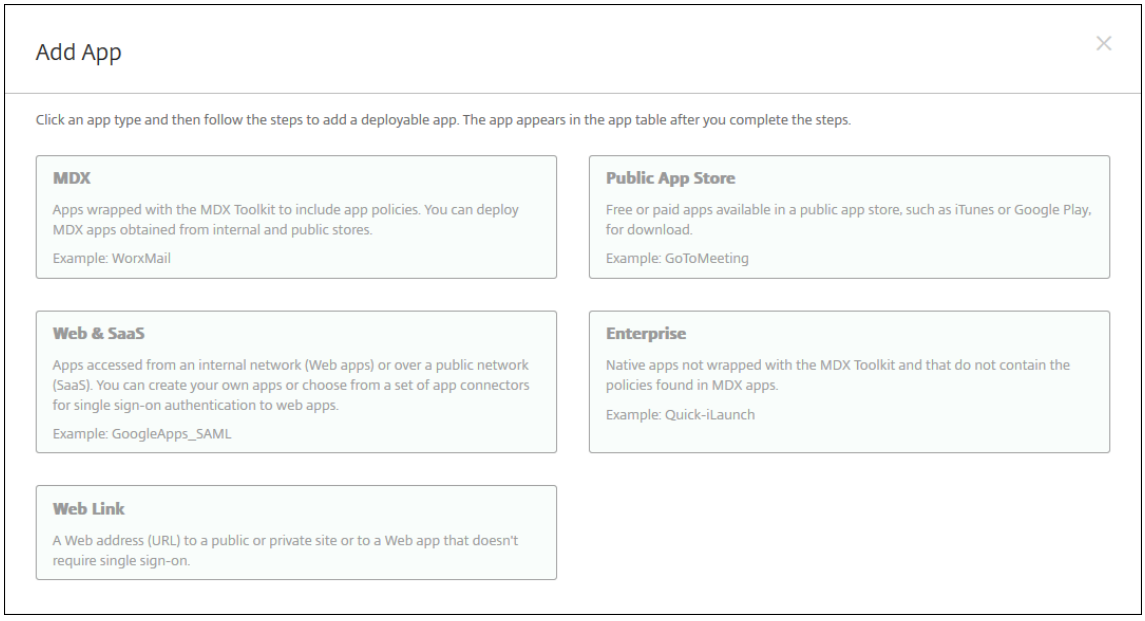
Wenn Sie eine MDX-Datei für eine iOS- oder Android-App erhalten, können Sie die App in XenMobile hochladen. Nach dem Hochladen der App können Sie die App- und Richtlinieneinstellungen konfigurieren. Informationen über die für die einzelnen Geräteplattformen verfügbaren App-Richtlinien finden Sie unter:

- Überblick über das MAM-SDK
- MDX-Richtlinien auf einen Blick

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.

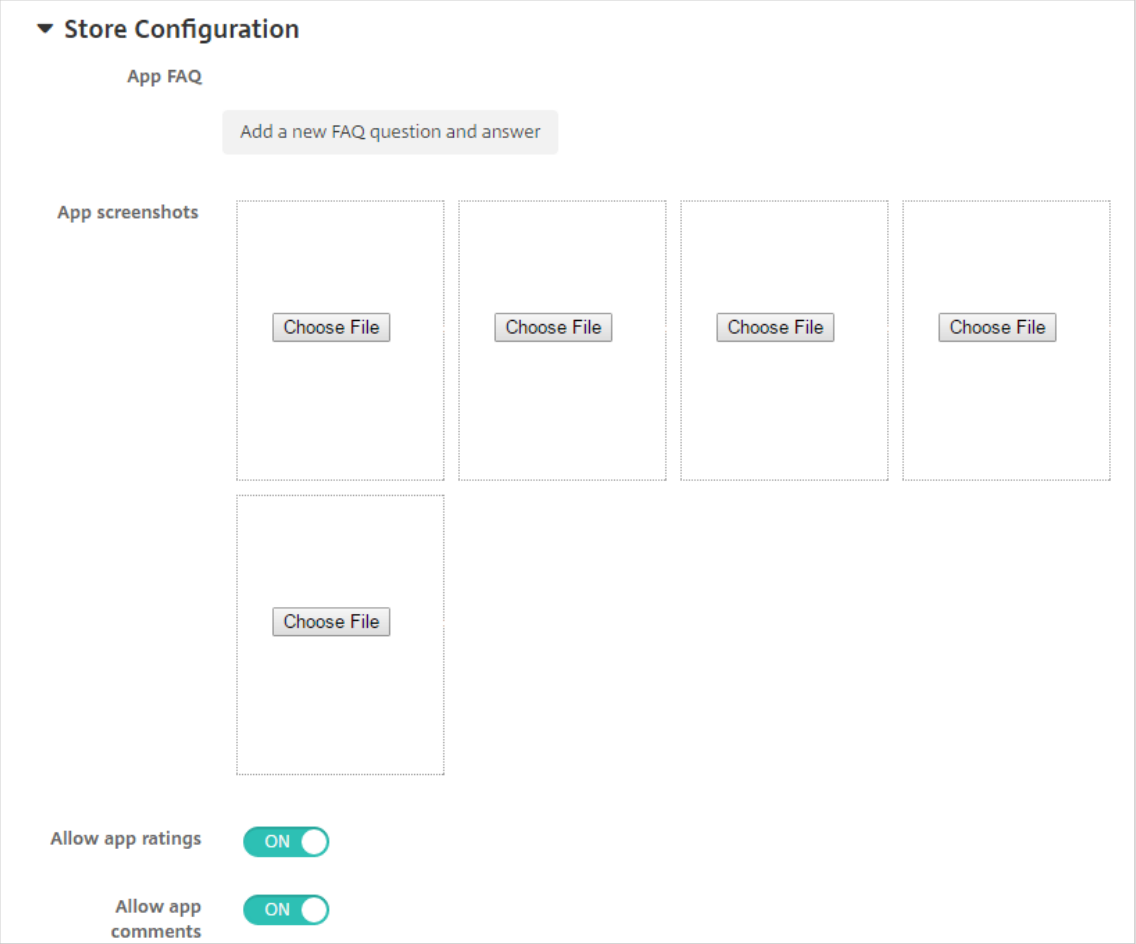


3. Klicken Sie auf **MDX**. Die Seite **App-Informationen** für MDX wird angezeigt.
4. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** angezeigt.
   - **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 zu App-Kategorien finden Sie unter App-Kategorien.

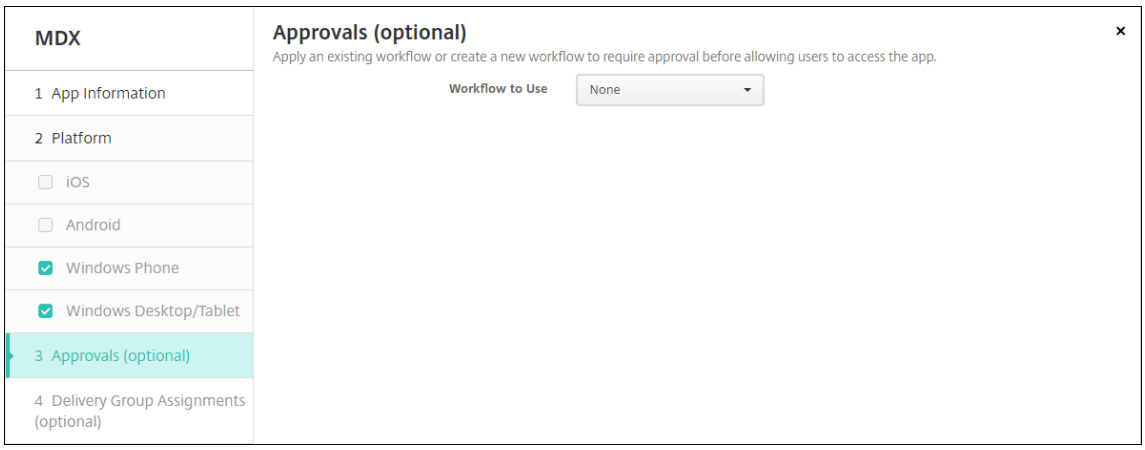
5. Klicken Sie auf **Weiter**. Die Seite **Plattform** wird angezeigt.
6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.
7. Klicken Sie zum Auswählen einer MDX-Datei auf **Upload** und navigieren Sie zum Speicherort der Datei.
8. Konfigurieren Sie auf der Seite **App-Details** diese 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.
   - **Paket-ID:** Geben Sie die Paket-ID für die App ein, die Sie aus dem verwalteten Google Play Store erhalten haben.
   - **OS-Version (Minimum):** Geben Sie optional die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
   - **OS-Version (Maximum):** Geben Sie optional 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 iOS-Geräten entfernt werden soll, wenn das MDM-Profil entfernt wird. Die Standardeinstellung ist **Ein**.
   - **App-Datenbackup verhindern:** Wählen Sie aus, ob Benutzer die App-Daten auf einem iOS-Gerät sichern dürfen. Die Standardeinstellung ist **Ein**.
   - **Produktschiene:** Geben Sie an, welche Produktversion Sie auf iOS-Geräte übertragen möchten. Wenn Sie ein spezielles Testprodukt haben, können Sie dies auswählen und Ihren Benutzern zuweisen. Die Standardeinstellung ist **Produktion**.
   - **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 iOS-Geräten zuzulassen. Die Standardeinstellung ist **Ein**.
   - **App wird per Volume Purchase bereitgestellt:** Wählen Sie aus, ob die App über Apple Volume Purchase bereitgestellt werden soll. Wenn Sie **Ein** auswählen und eine MDX-App mit Volume Purchase bereitstellen, wird in Secure Hub nur die Volume Purchase-Instanz angezeigt. Die Standardeinstellung ist **Aus**.
9. Konfigurieren Sie die **MDX-Richtlinien**. MDX-Richtlinien variieren je nach Plattform und bieten Optionen für Richtlinienbereiche wie Authentifizierung, Gerätesicherheit und App-Einschränkungen. In der Konsole kann eine QuickInfo mit einer Beschreibung der Richtlinien angezeigt werden.

10. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Bereitstellungsregeln.
11. Erweitern Sie **Storekonfiguration**.



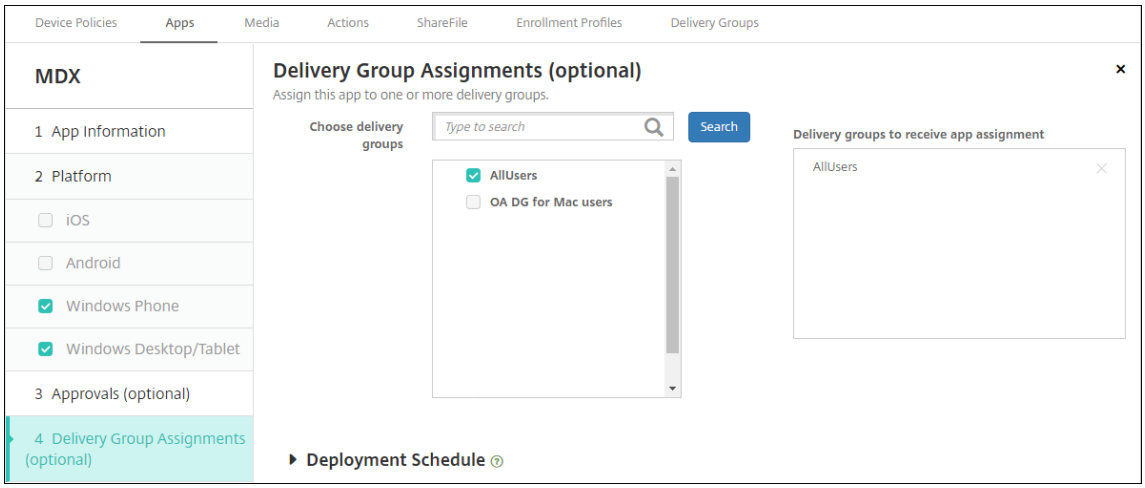
- **App FAQ:** Klicken Sie auf **Fügen Sie eine neue häufig gestellte Frage und deren Antwort hinzu**, um eine FAQ für die App zu erstellen.
- **App-Screenshots für Mobiltelefone/Tablets:** Fügen Sie Screenshots hinzu, die im App Store angezeigt werden.
- **App-Bewertungen zulassen:** Erlauben Sie Benutzern, die App im App Store zu bewerten.
- **App-Kommentare zulassen:** Erlauben Sie Benutzern, Kommentare zur App im App Store zu hinterlassen.

12. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.



Informationen zum Verwenden von Workflows für die Anforderung einer Genehmigung vor dem App-Zugriff durch Benutzer finden Sie unter Anwenden von Workflows. Wenn Sie keine Genehmigungsworkflows einrichten möchten, fahren Sie mit dem nächsten Schritt fort.

13. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.



14. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, um nach einer Bereitstellungsgruppe zu suchen, oder wählen Sie eine oder mehrere Gruppen in der Liste aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

15. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

    - **Bereitstellen:** Wählen Sie aus, ob die App auf Geräten bereitgestellt werden soll. Die Standardeinstellung ist **Ein**.
    - **Bereitstellungszeitplan:** Wählen Sie aus, ob die App **Jetzt** oder **Später** bereitgestellt werden soll. Bei Auswahl von **Später** konfigurieren Sie ein Datum und eine Uhrzeit für die Bereitstellung der App. Die Standardeinstellung ist **Jetzt**.
    - **Bereitstellungsbedingung:** Wählen Sie **Bei jeder Verbindung**, um die App bei jeder Verbindung des Geräts bereitzustellen. Wählen Sie **Nur bei Fehler in der vorherigen**

Bereitstellung, um die App bereitzustellen, wenn das Gerät die App zuvor nicht erhalten hat. Die Standardeinstellung ist **Bei jeder Verbindung**.

Die Option **Bereitstellen für immer aktive Verbindungen** gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.

Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

16. Klicken Sie auf **Speichern**.

Hinzufügen von Apps aus einem öffentlichen App-Store

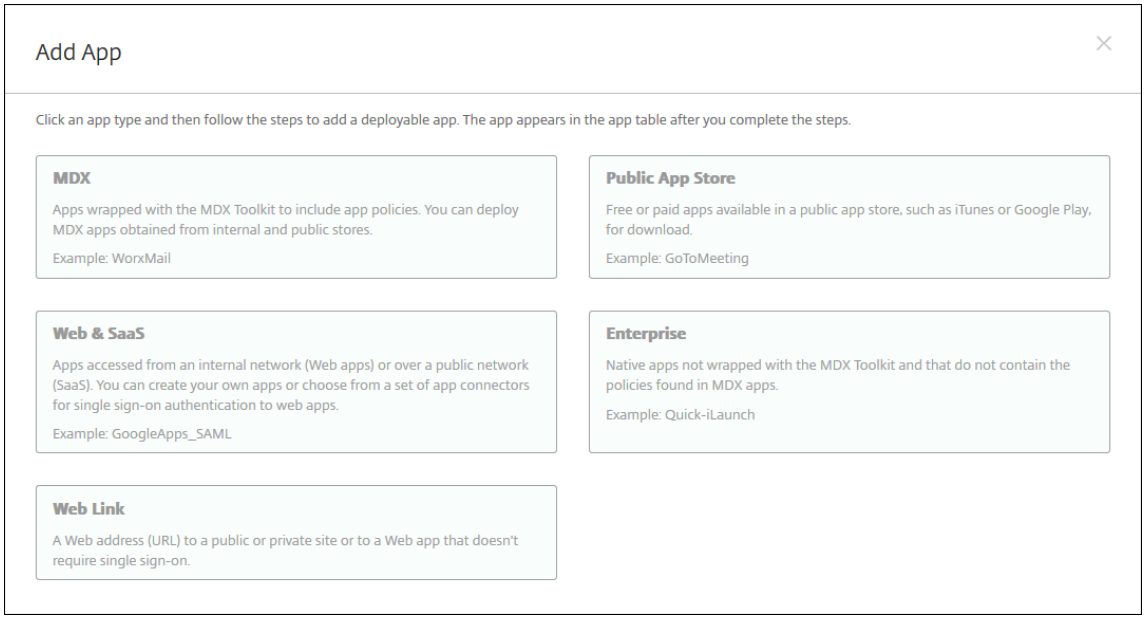
Sie können XenMobile kostenlose oder kostenpflichtige Apps, die in einem öffentlichen App Store (z. B. Apple App Store oder Google Play) verfügbar sind, hinzufügen.

Sie können Einstellungen zum Abrufen der Namen und Beschreibungen von Apps aus dem Apple App Store konfigurieren. Bei Abrufen der App-Informationen aus dem Store werden der vorhandene Name und die vorhandene Beschreibung in XenMobile überschrieben. Konfigurieren Sie die App-Informationen für Google Play Store manuell.

Wenn Sie eine kostenpflichtige App aus einem öffentlichen App-Store für Android Enterprise 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. Das Massenkaufabonnement für Android Enterprise vereinfacht für eine Organisation das Finden, Kaufen und Bereitstellen von Apps und anderer Daten in großer Zahl.

Konfigurieren von App-Informationen und Auswählen von Plattformen, auf denen App bereitgestellt werden soll:

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps > Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



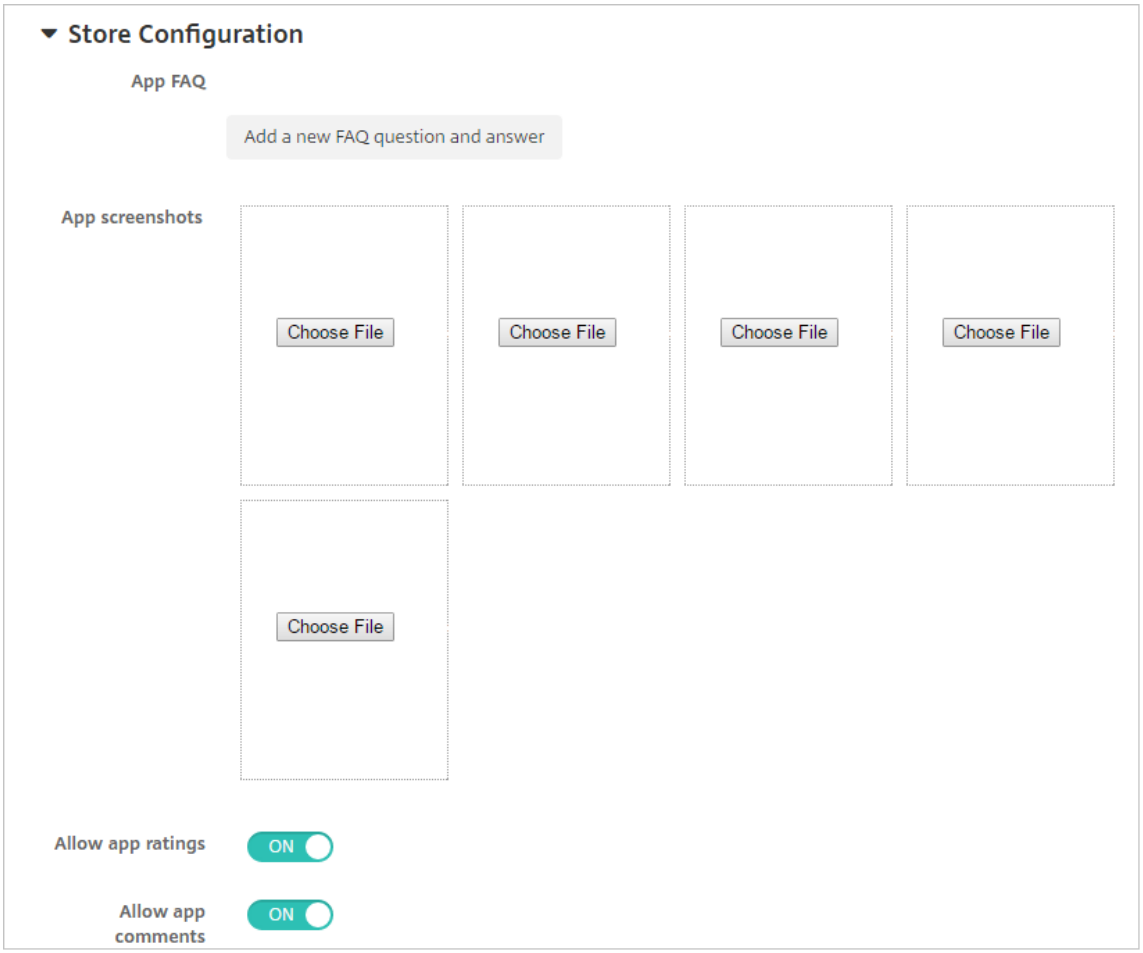
2. Klicken Sie auf **Öffentlicher App-Store**. Die Seite **App-Informationen** wird angezeigt.
3. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** 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 zu App-Kategorien finden Sie unter App-Kategorien.
4. Klicken Sie auf **Weiter**. Die Seite **Plattform** wird angezeigt.
5. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

Als Nächstes konfigurieren Sie die App-Einstellungen für jede Plattform. Siehe:

- Konfigurieren von App-Einstellungen für Google Play-Apps
- Apps aus dem verwalteten App-Store
- Konfigurieren der App-Einstellungen für iOS-Apps

Wenn Sie die Einstellungen für eine Plattform konfiguriert haben, legen Sie die Bereitstellungsregeln und die App-Storekonfiguration für die Plattform fest.

1. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Bereitstellungsregeln.
2. Erweitern Sie **Storekonfiguration**.



- **App FAQ:** Klicken Sie auf **Fügen Sie eine neue häufig gestellte Frage und deren Antwort hinzu**, um eine FAQ für die App zu erstellen.
- **App-Screenshots für Mobiltelefone/Tablets:** Fügen Sie Screenshots hinzu, die im App Store angezeigt werden.
- **App-Bewertungen zulassen:** Erlauben Sie Benutzern, die App im App Store zu bewerten.
- **App-Kommentare zulassen:** Erlauben Sie Benutzern, Kommentare zur App im App Store zu hinterlassen.

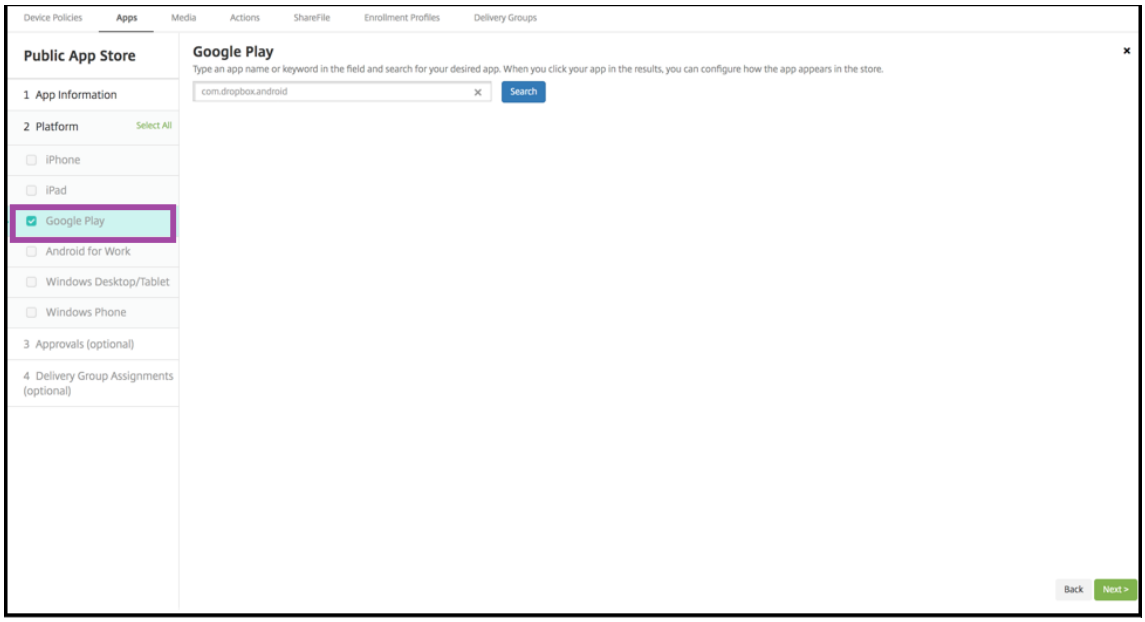
Konfigurieren von App-Einstellungen für Google Play-Apps

> **Hinweis:**
>
> Um alle Apps in Google Play über den verwalteten Google Play-Store zugänglich zu machen, verwenden Sie die XenMobile-Servereigenschaft für den **Zugriff auf den Verwalteten Google Play-Store**. Siehe Servereigenschaften. Wenn Sie diese Eigenschaft auf **Wahr** setzen, werden die Apps aus dem öffentlichen Google Play Store für alle Android Enterprise-Benutzer zugelassen. Mit der Einschränkungsrichtlinie können Sie dann den Zugriff auf diese Apps steuern.

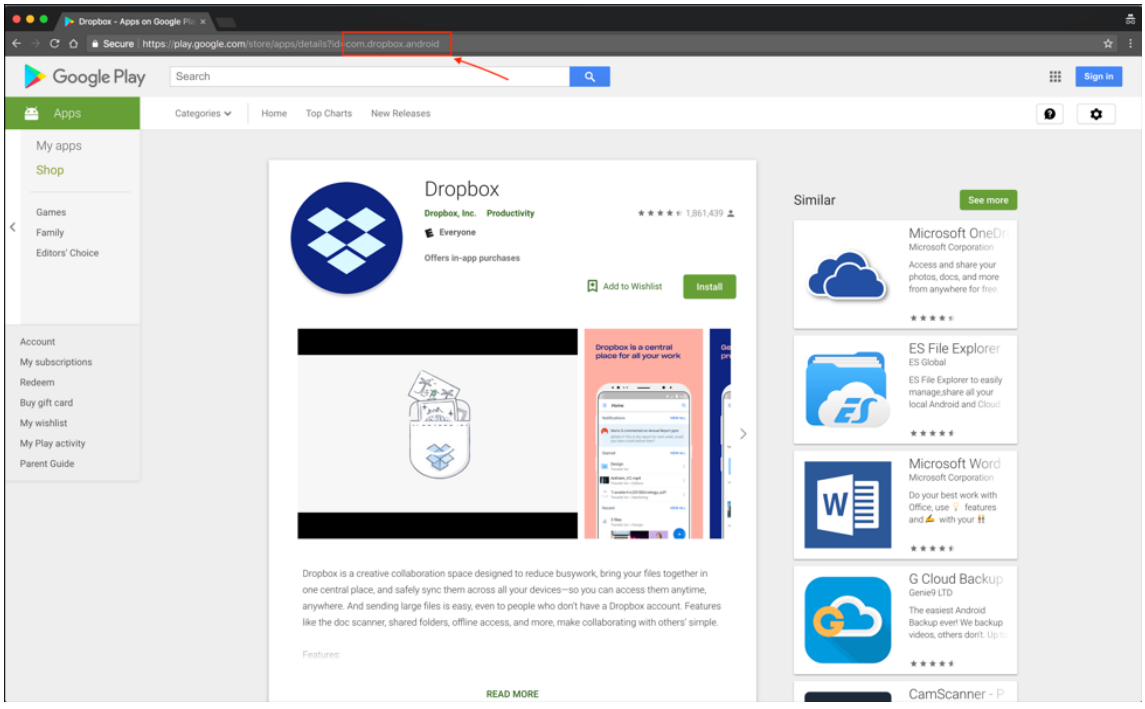
Das Konfigurieren von Einstellungen für Google Play Store-Apps erfordert andere Schritte als bei Apps

für andere Plattformen. Sie müssen die App-Informationen für Google Play Store manuell konfigurieren.

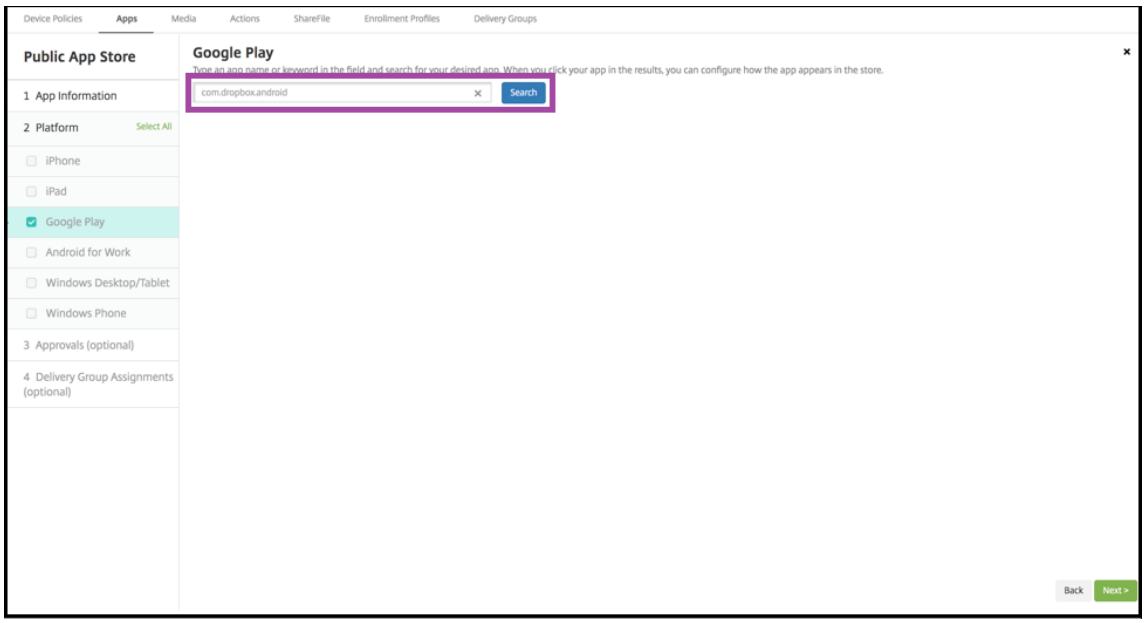
1. Stellen Sie sicher, dass **Google Play** unter **Plattformen** ausgewählt ist.



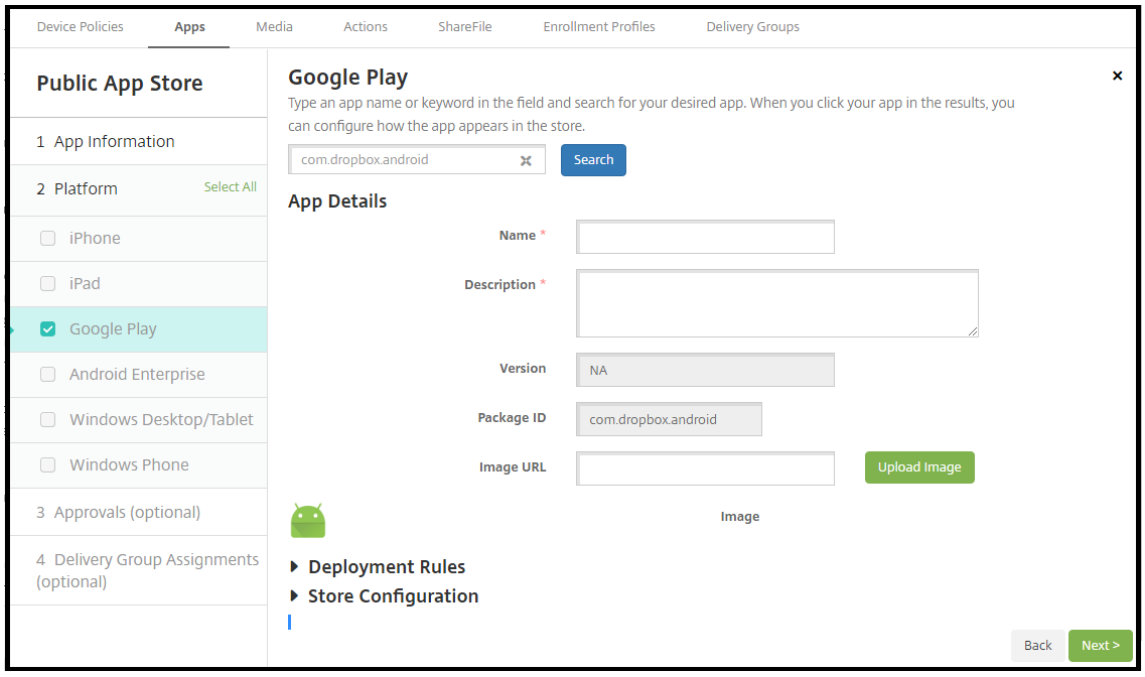
2. Rufen Sie Google Play auf. Kopieren Sie die Paket-ID aus Google Play. Die ID finden Sie in der URL der App.



3. Beim Hinzufügen einer App aus einem öffentlichen Store in der XenMobile Server-Konsole fügen Sie die Paket-ID in die Suchleiste ein. Klicken Sie auf **Search**.



4. Wenn die Paket-ID gültig ist, wird eine Benutzeroberfläche angezeigt, auf der Sie App-Details eingeben können.



5. Sie können die URL so konfigurieren, dass das Bild mit der App im Store angezeigt wird. Verwenden des Bilds aus dem Google Play Store:

   a) Rufen Sie Google Play Store auf. Klicken Sie mit der rechten Maustaste auf das App-Bild und kopieren Sie dessen Adresse.

   b) Fügen Sie die Bildadresse in das Feld **Bild-URL** ein.

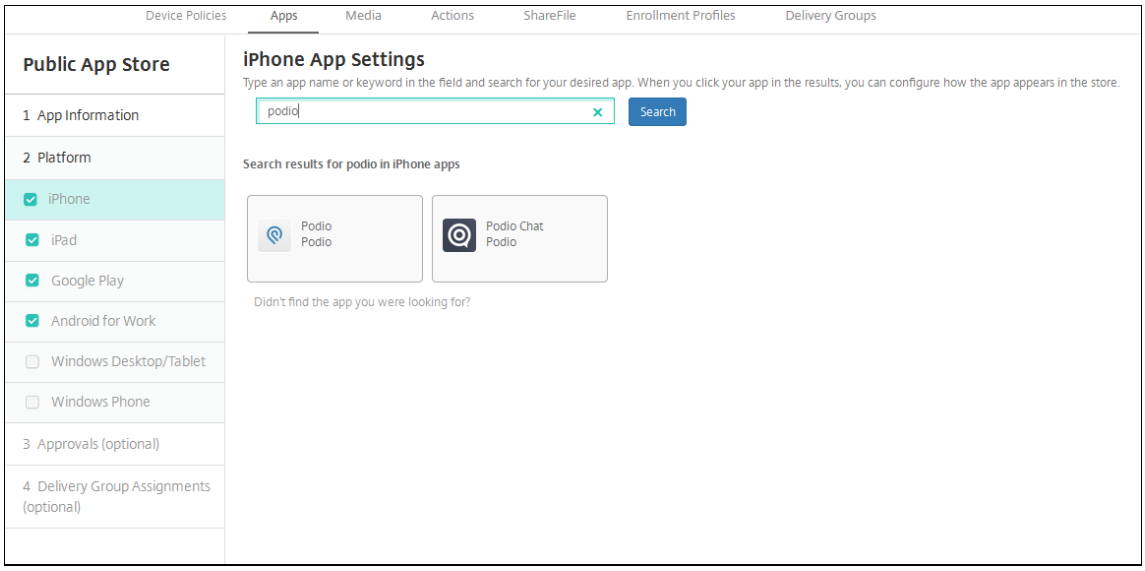
   c) Klicken Sie auf **Bild hochladen**. Das Bild wird neben **Bild** angezeigt.

Wenn Sie kein Bild konfigurieren, wird das generische Android-Bild mit der App angezeigt.

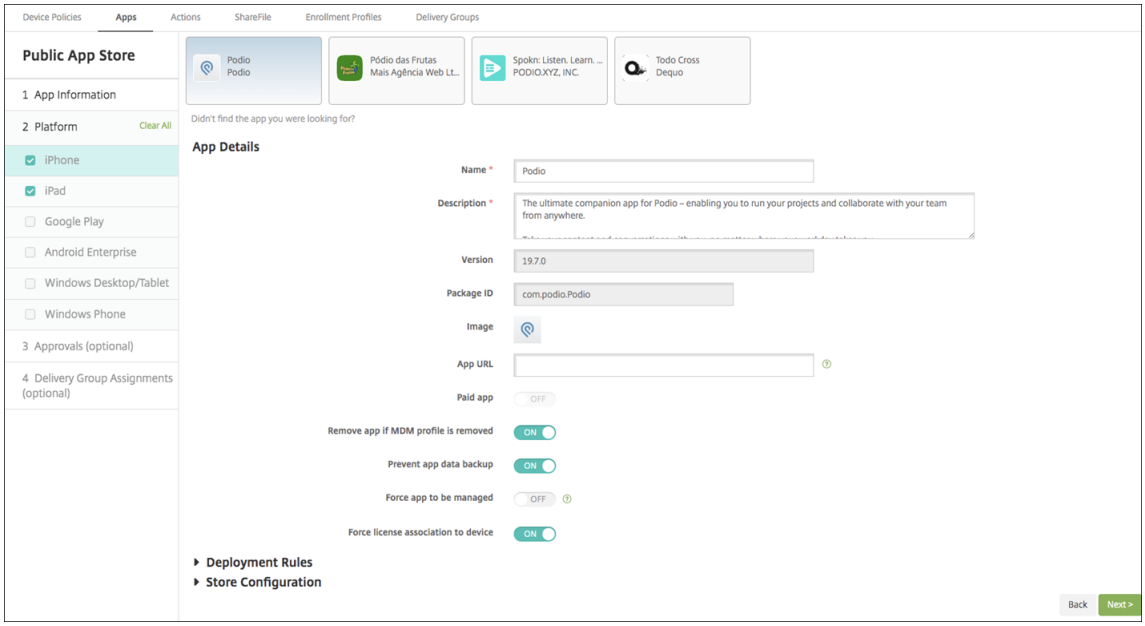
Konfigurieren der App-Einstellungen für iOS-Apps

1. Geben Sie den App-Namen in das Suchfeld ein und klicken Sie auf **Suchen**. Es werden die Apps angezeigt, die den Suchkriterien entsprechen. Es werden die Apps angezeigt, die den Suchkriterien entsprechen.

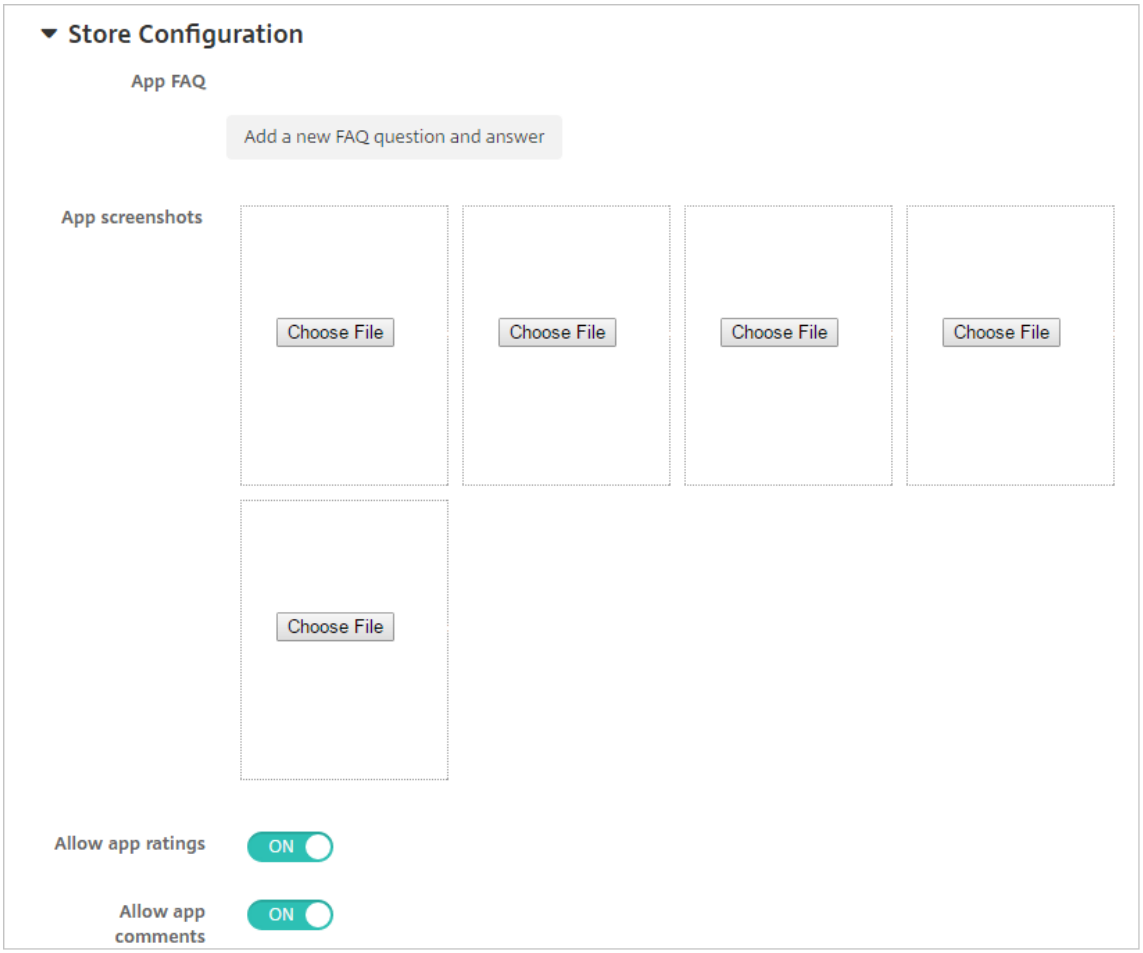
   Die folgende Abbildung zeigt das Ergebnis der Suche nach **podio** in Apps auf einem iPhone.



2. Klicken Sie auf die gewünschte App.
3. Die Felder im Bereich **App-Details** (Name, Beschreibung, Versionsnummer und zugeordnetes Bild) enthalten bereits Informationen zu der gewählten App.



4. Konfigurieren Sie folgende 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. Die Standardeinstellung ist **Ein**.
    - **App-Datenbackup verhindern:** Wählen Sie aus, ob die App Daten sichern können soll. Die Standardeinstellung ist **Ein**.
    - **Produktschiene:** Geben Sie an, welche Produktversion Sie auf Benutzergeräte übertragen möchten. Wenn Sie ein spezielles Testprodukt haben, können Sie dies auswählen und Ihren Benutzern zuweisen. Die Standardeinstellung ist **Produktion**.
    - **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. Die Standardeinstellung 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.
5. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Bereitstellungsregeln.
6. Erweitern Sie **Storekonfiguration**.



- **App FAQ:** Klicken Sie auf **Fügen Sie eine neue häufig gestellte Frage und deren Antwort hinzu**, um eine FAQ für die App zu erstellen.
- **App-Screenshots für Mobiltelefone/Tablets:** Fügen Sie Screenshots hinzu, die im App Store angezeigt werden.
- **App-Bewertungen zulassen:** Erlauben Sie Benutzern, die App im App Store zu bewerten.
- **App-Kommentare zulassen:** Erlauben Sie Benutzern, Kommentare zur App im App Store zu hinterlassen.

7. Für iPhone oder iPad erweitern Sie **Volume Purchase**.

   a) Anwenden einer Volume Purchase-Lizenz für die App in XenMobile: Klicken Sie in der Liste **Volume Purchase-Lizenz** auf **Volume Purchase-Lizenz hochladen**.

   b) Importieren Sie die Lizenz über das angezeigte Dialogfeld.

   Die Tabelle “Lizenzzuweisung” zeigt, wie viele der insgesamt verfügbaren Lizenzen für die App verwendet werden.

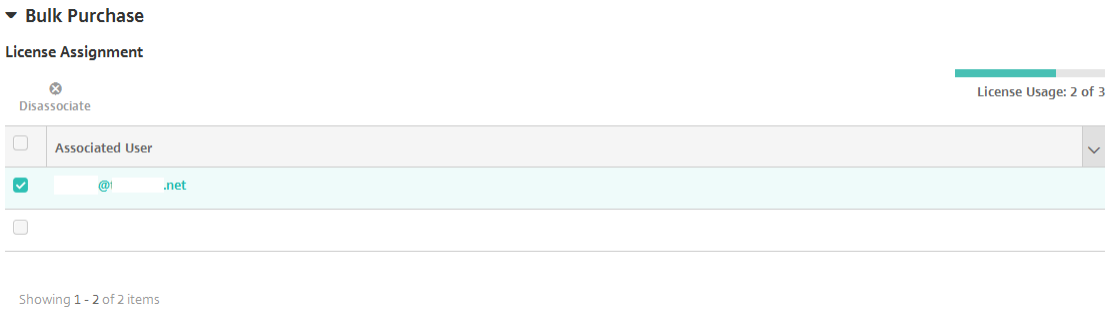
   Sie können die Zuordnung von Volume Purchase-Lizenzen für einen einzelnen Benutzer aufheben. Auf diese Weise wird die Lizenzzuweisung beendet und Lizenzen werden

freigegeben.

8. Für Android Enterprise erweitern Sie den Bereich **Massenkauf**.

   Die Tabelle “Lizenzzuweisung” zeigt, wie viele der insgesamt verfügbaren Lizenzen für die App verwendet werden.

   Sie können einen Benutzer auswählen und dann auf **Zuordnung aufheben** klicken, um die Lizenzzuweisung zu beenden und die 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.



9. Wenn Sie die Einstellungen für **Volume Purchase** oder für **Massenkauf** festgelegt haben, klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.

   Informationen zum Verwenden von Workflows für die Anforderung einer Genehmigung vor dem App-Zugriff durch Benutzer finden Sie unter Anwenden von Workflows. Wenn Sie keine Genehmigungsworkflows benötigen, fahren Sie mit dem nächsten Schritt fort.

10. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.

11. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, um nach einer Bereitstellungsgruppe zu suchen, oder wählen Sie eine oder mehrere Gruppen in der Liste aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

12. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

    - **Bereitstellen:** Wählen Sie aus, ob die App auf Geräten bereitgestellt werden soll. Die Standardeinstellung ist **Ein**.
    - **Bereitstellungszeitplan:** Wählen Sie aus, ob die App **Jetzt** oder **Später** bereitgestellt werden soll. Bei Auswahl von **Später** konfigurieren Sie ein Datum und eine Uhrzeit für die Bereitstellung der App. Die Standardeinstellung ist **Jetzt**.
    - **Bereitstellungsbedingung:** Wählen Sie **Bei jeder Verbindung**, um die App bei jeder Verbindung des Geräts bereitzustellen. Wählen Sie **Nur bei Fehler in der vorherigen Bereitstellung**, um die App bereitzustellen, wenn das Gerät die App zuvor nicht erhalten hat. Die Standardeinstellung ist **Bei jeder Verbindung**.

Die Option **Bereitstellen für immer aktive Verbindungen** gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.

Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

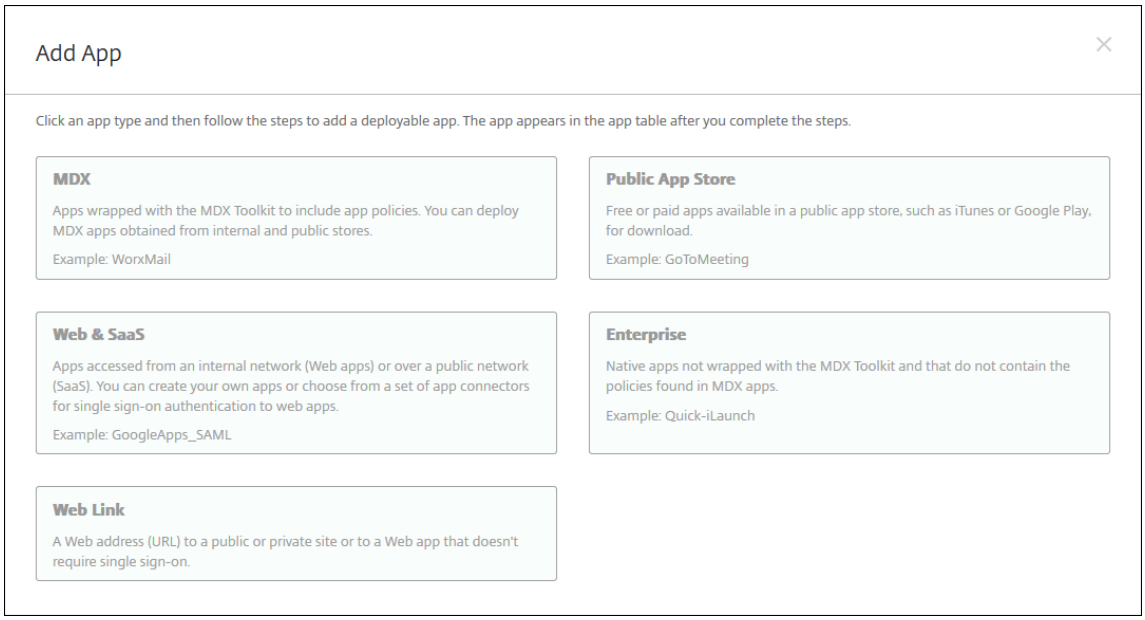
13. Klicken Sie auf **Speichern**.

Hinzufügen von Web- und SaaS-Apps

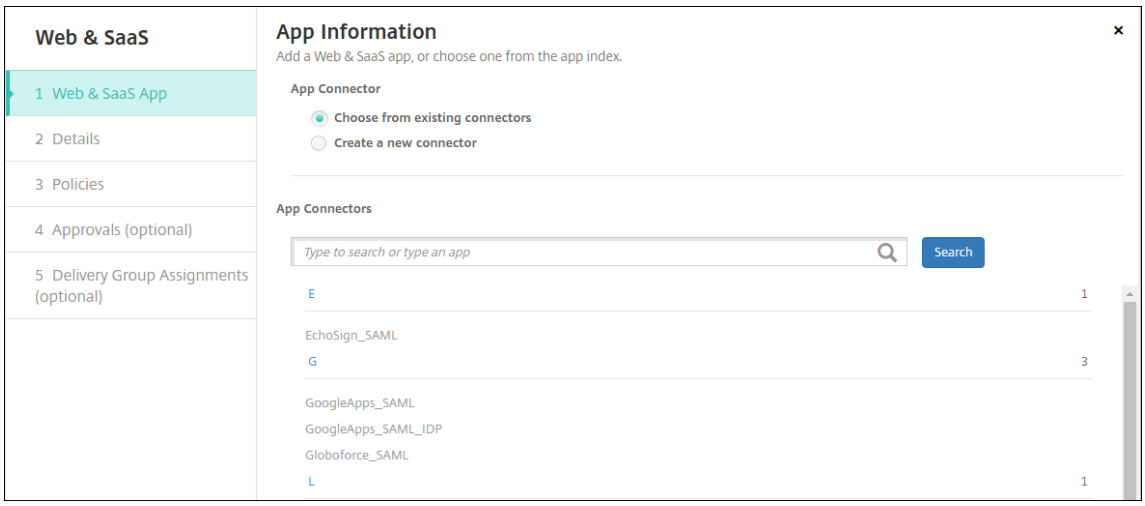
Mit der XenMobile-Konsole können Sie Benutzern SSO-Zugriff (Single Sign-On) auf Mobil-, Unternehmens-, Web- und SaaS-Apps gewähren. Zur Aktivierung von Apps für SSO können Sie Vorlagen für Anwendungsconnectors verwenden. Eine Liste der in XenMobile verfügbaren Connectortypen finden Sie unter Anwendungsconnectortypen. Sie können beim Hinzufügen einer Web- oder SaaS-App auch einen eigenen Connector in XenMobile erstellen.

Wenn eine App nur für SSO verfügbar ist, wird die App nach dem Speichern der Einstellungen auf der Registerkarte **Apps** in der XenMobile-Konsole angezeigt.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps > Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



2. Klicken Sie auf **Web & SaaS**. Die Seite **App-Informationen** wird angezeigt.



3. Konfigurieren Sie, wie nachfolgend beschrieben, einen vorhandenen oder neuen App-Connector.

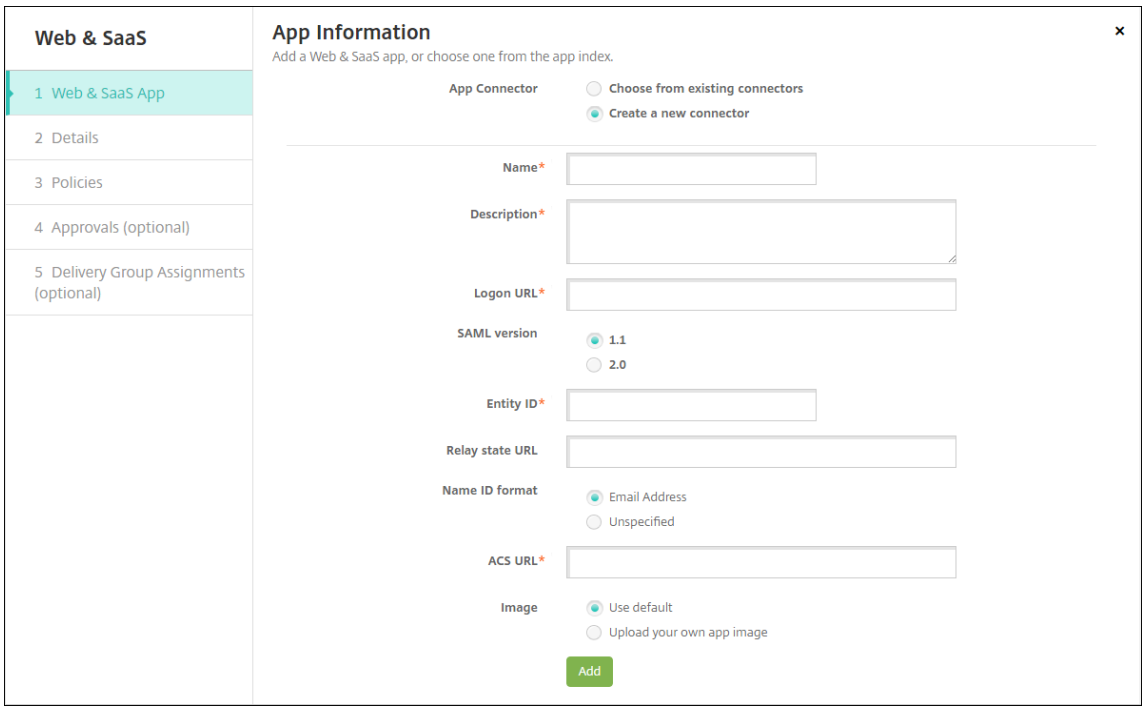
Konfigurieren eines vorhandenen App-Connectors

1. Auf der Seite **App-Informationen** ist **Vorhandenen Connector wählen** bereits ausgewählt (siehe vorherige Abbildung). Klicken Sie in der Liste **App-Connectors** auf den gewünschten Connector. Die Informationen zu dem App-Connector werden angezeigt.
2. 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:** Akzeptieren Sie die vorausgefüllte URL oder geben Sie die Webadresse der 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. Dieses Feld ist erforderlich.
   - **App wird im internen Netzwerk gehostet:** Wählen Sie, ob 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 Citrix Gateway erfolgen. Wenn Sie diese Option auf **EIN** festlegen, wird das VPN-Schlüsselwort der App hinzugefügt, sodass Benutzer eine Verbindung über Citrix Gateway herstellen können. Die Standardeinstellung 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 in der Liste auf die Aktion, die ausgeführt werden soll, wenn Benutzer keinen Zugriff auf die App mehr haben. Die Standardeinstellung ist **Konto deaktivieren**.
  - **Benutzernamenregel**
    - Führen für jede Benutzernamenregel, die Sie hinzufügen möchten, folgende Schritte aus:
      - **Benutzerattribute:** Klicken Sie in der Liste auf die Benutzerattribute, die Sie der Regel hinzufügen möchten.
      - **Länge (Zeichen):** Klicken Sie in der Liste auf die Anzahl der Zeichen des Benutzerattributs, 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. Die Standardeinstellung ist **8**.
- **Kennwortablauf**
  - **Gültigkeit (Tage):** Geben Sie die Anzahl Tage ein, die das Kennwort gültig sein soll. Gültig sind Werte zwischen **0 und 90**. Die Standardeinstellung ist 90.
  - **Kennwort nach Ablauf automatisch zurücksetzen:** Wählen Sie aus, ob Kennwörter nach Ablauf automatisch zurückgesetzt werden sollen. Die Standardeinstellung 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

1. Klicken Sie auf der Seite **App-Informationen** auf **Neuen Connector erstellen**. Die Felder zu dem App-Connector werden angezeigt.

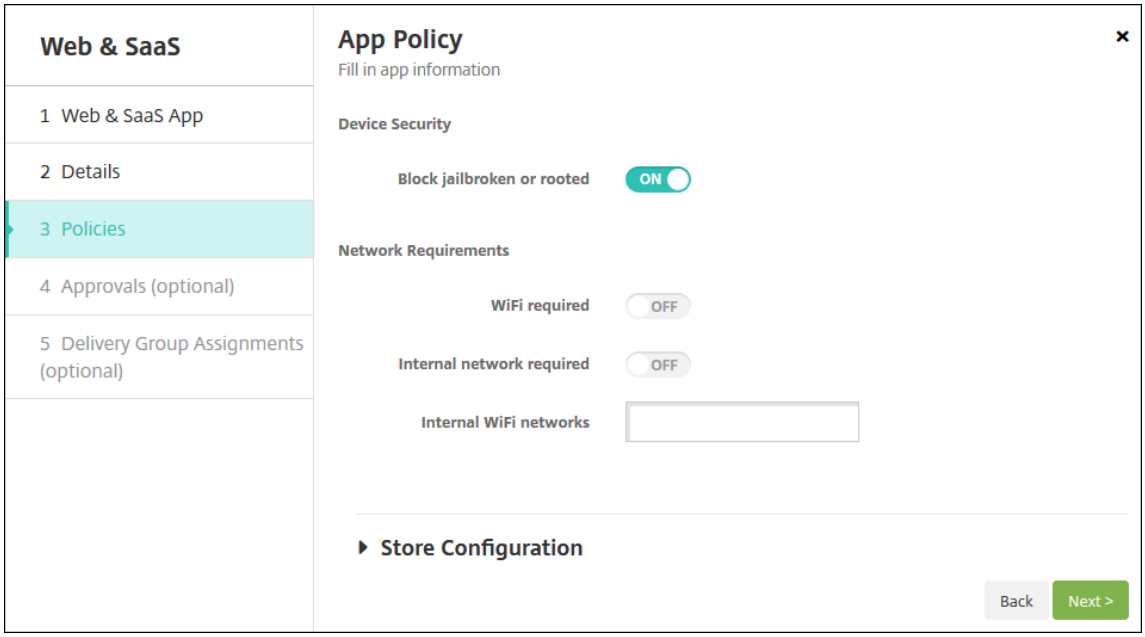


2. Konfigurieren Sie folgende Einstellungen:

   - **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, beispielsweise `https://www.example.com/logon`. Diese Angabe ist erforderlich.
   - **SAML-Version:** Wählen Sie **1.1** oder **2.0** aus. Die Standardeinstellung 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. Die Standardeinstellung ist “Standard verwenden”.
     - Zum Hochladen eines eigenen Bilds klicken Sie auf **Durchsuchen**, navigieren Sie zu dem Speicherort der Bilddatei und wählen Sie diese aus. Die Datei muss eine PNG-Datei sein. Sie können keine JPEG- oder GIF-Dateien hochladen. Eine

benutzerdefinierte Grafik kann später nicht mehr geändert werden.

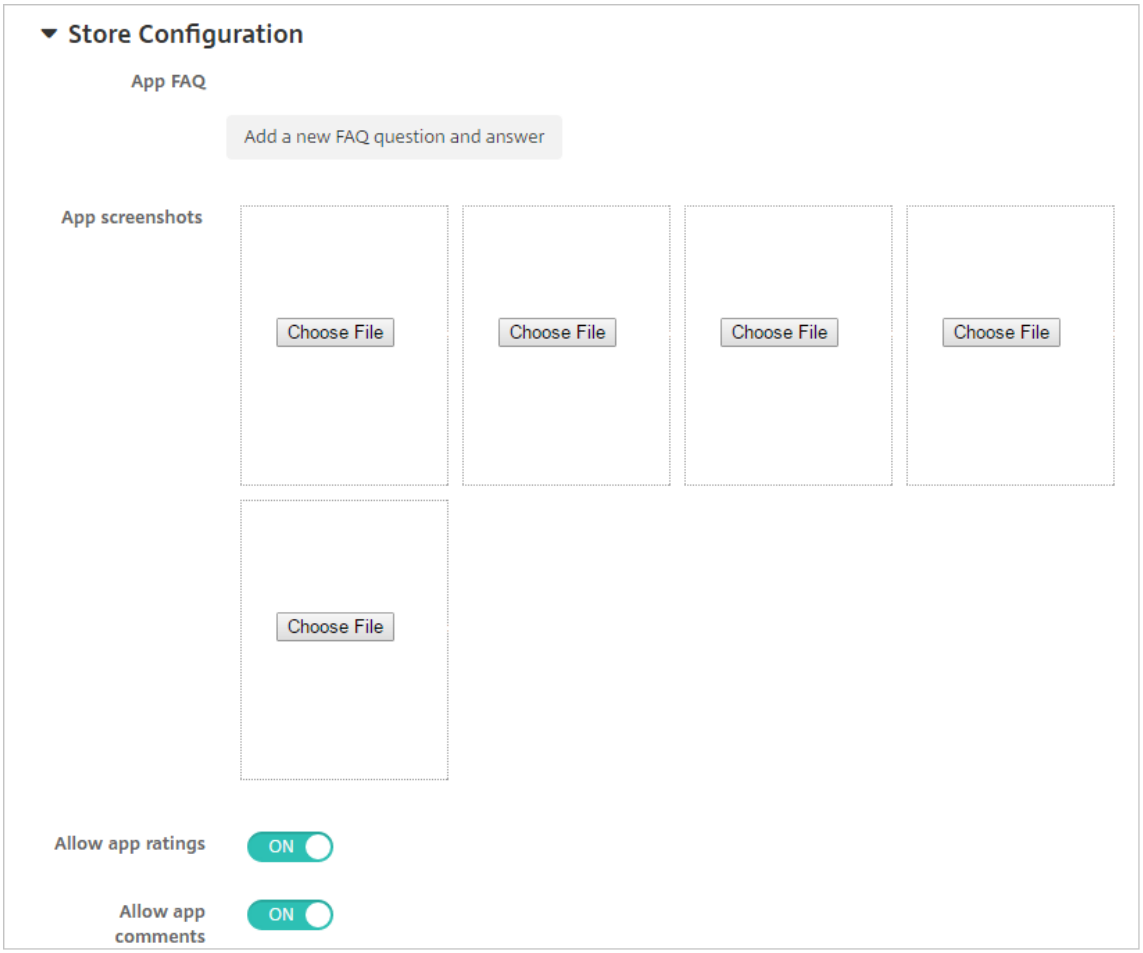
3. Wenn Sie fertig sind, klicken Sie auf **Hinzufügen**. Die Seite **Details** wird angezeigt.
4. Klicken Sie auf **Weiter**. Die Seite **App-Richtlinie** wird angezeigt.



5. Konfigurieren Sie folgende Einstellungen:

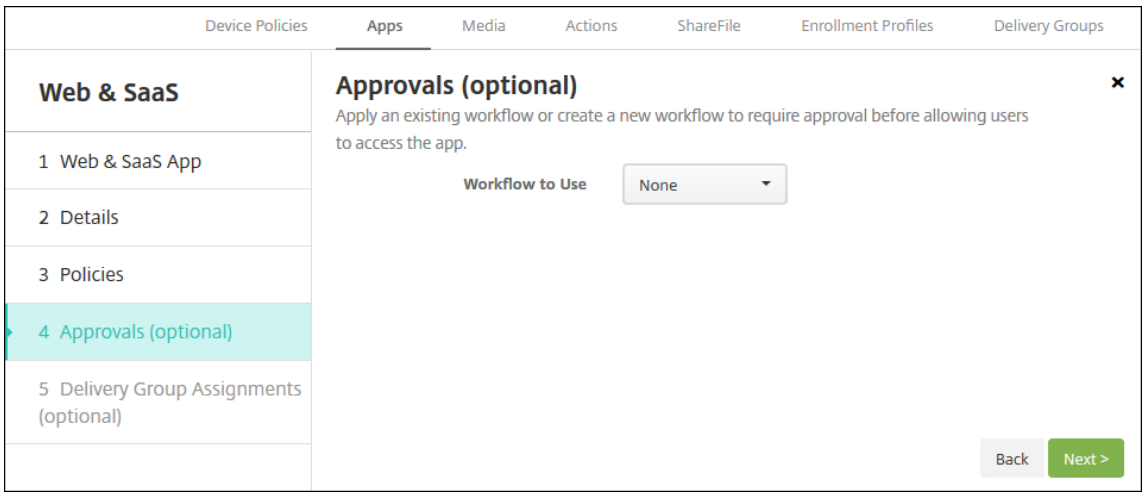
   - **Gerätesicherheit**
   - **Mit Jailbreak oder Root blockieren:** Wählen Sie aus, ob Geräte mit Jailbreak und gerootete Geräte vom Zugriff auf die App ausgeschlossen werden sollen. Die Standardeinstellung ist **Ein**.
   - **Netzwerkanforderungen**
   - **WiFi erforderlich:** Wählen Sie aus, ob zum Ausführen der App eine Wi-Fi-Verbindung erforderlich sein soll. Die Standardeinstellung ist **Aus**.
   - **Internes Netzwerk erforderlich:** Wählen Sie aus, ob zum Ausführen der App ein internes Netzwerk erforderlich sein soll. Die Standardeinstellung ist **Aus**.
   - **Interne WiFi-Netzwerke:** Wenn Sie **Wi-Fi erforderlich** aktiviert haben, geben Sie hier die internen Wi-Fi-Netzwerke an, die verwendet werden sollen.

6. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Bereitstellungsregeln.
7. Erweitern Sie **Storekonfiguration**.



- **App FAQ:** Klicken Sie auf **Fügen Sie eine neue häufig gestellte Frage und deren Antwort hinzu**, um eine FAQ für die App zu erstellen.
- **App-Screenshots für Mobiltelefone/Tablets:** Fügen Sie Screenshots hinzu, die im App Store angezeigt werden.
- **App-Bewertungen zulassen:** Erlauben Sie Benutzern, die App im App Store zu bewerten.
- **App-Kommentare zulassen:** Erlauben Sie Benutzern, Kommentare zur App im App Store zu hinterlassen.

8. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.



Informationen zum Verwenden von Workflows für die Anforderung einer Genehmigung vor dem App-Zugriff durch Benutzer finden Sie unter Anwenden von Workflows.

9. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.
10. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, um nach einer Bereitstellungsgruppe zu suchen bzw. eine oder mehrere Gruppen auszuwählen. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.
11. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:
    - **Bereitstellen:** Wählen Sie aus, ob die App auf Geräten bereitgestellt werden soll. Die Standardeinstellung ist **Ein**.
    - **Bereitstellungszeitplan:** Wählen Sie aus, ob die App **Jetzt** oder **Später** bereitgestellt werden soll. Bei Auswahl von **Später** konfigurieren Sie ein Datum und eine Uhrzeit für die Bereitstellung der App. Die Standardeinstellung ist **Jetzt**.
    - **Bereitstellungsbedingung:** Wählen Sie **Bei jeder Verbindung**, um die App bei jeder Verbindung des Geräts bereitzustellen. Wählen Sie **Nur bei Fehler in der vorherigen Bereitstellung**, um die App bereitzustellen, wenn das Gerät die App zuvor nicht erhalten hat. Die Standardeinstellung ist **Bei jeder Verbindung**.

    Die Option **Bereitstellen für immer aktive Verbindungen** gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.

    Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.
12. Klicken Sie auf **Speichern**.

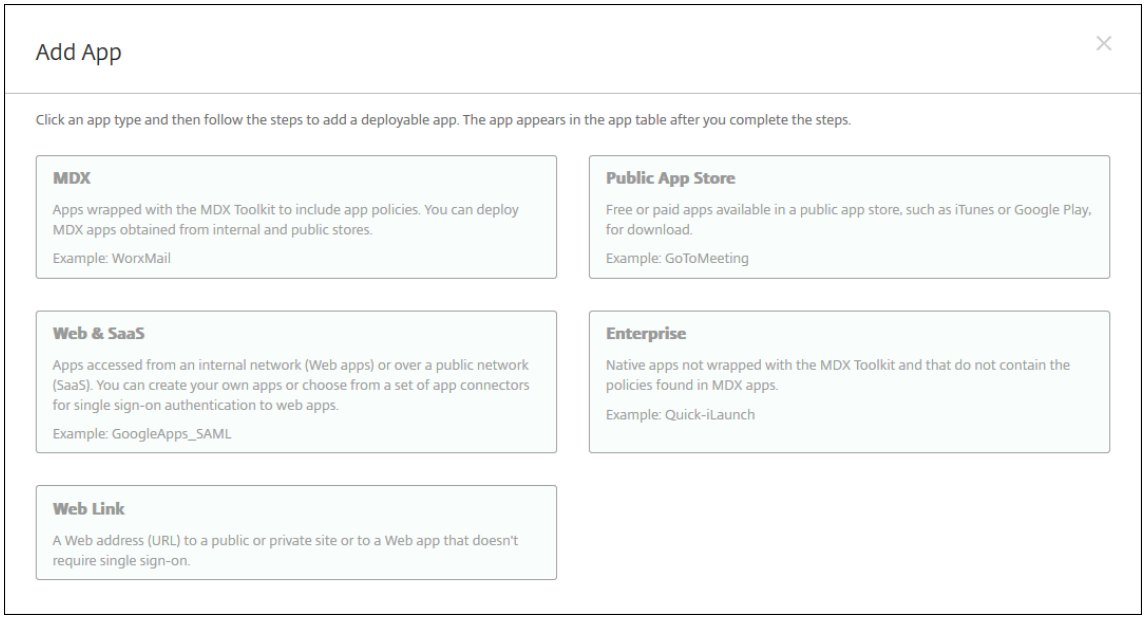
Hinzufügen einer Unternehmensapp

Enterprise-Apps in XenMobile stellen native Apps dar, die nicht mit dem MAM-SDK oder MDX Toolkit vorbereitet wurden. Diese Apps enthalten keine Richtlinien für MDX-Apps. Sie können Unternehmensapps mit der Registerkarte **Apps** der XenMobile-Konsole hochladen. Unternehmensapps unterstützen folgende Plattformen (und die entsprechenden Dateitypen):

- iOS (.ipa)
- Android (APK-Datei)
- Samsung Knox (APK-Datei)
- Android Enterprise (APK-Datei)
- Siehe auch: MDX-fähige private Apps

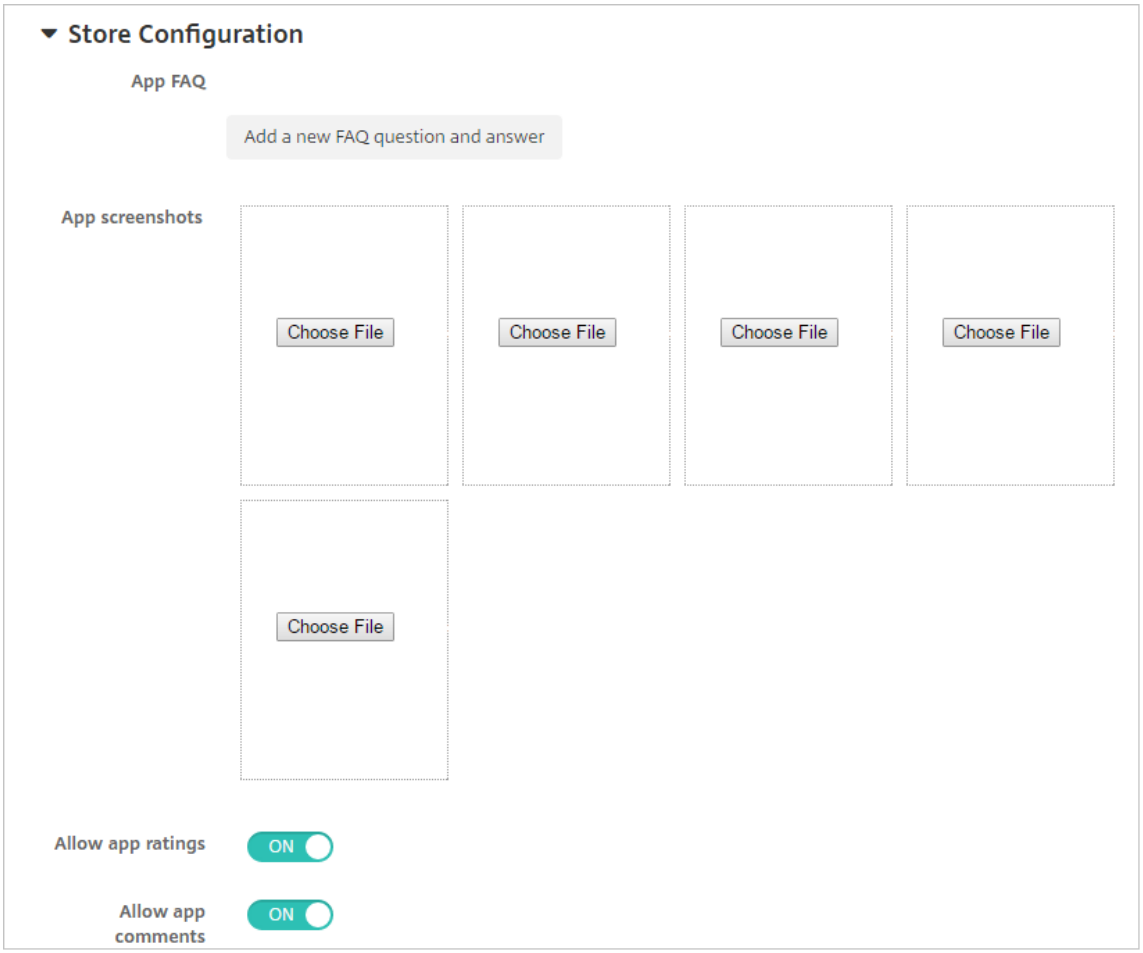
Das Hinzufügen von Apps aus dem Google Play Store als Unternehmensapps wird nicht unterstützt. Fügen Sie Apps aus dem Google Play Store stattdessen als Apps aus öffentlichen App-Stores hinzu. Siehe Hinzufügen von Apps aus einem öffentlichen App-Store.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps > Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



2. Klicken Sie auf **Enterprise**. Die Seite **App-Informationen** wird angezeigt.
3. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
    - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name” in der Tabelle “Apps” 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 zu App-Kategorien finden Sie unter App-Kategorien.

4. Klicken Sie auf **Weiter**. Die Seite **Plattform** wird angezeigt.
5. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.
6. Klicken Sie für jede ausgewählte Plattform auf **Hochladen**, navigieren Sie zum Speicherort der zu importierenden Datei und wählen Sie diese aus.
7. Klicken Sie auf **Weiter**. Die Seite mit den App-Informationen für die Plattform wird angezeigt.
8. 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 optional die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
   - **OS-Version (Maximum):** Geben Sie optional 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.
   - **Paket-ID:** Eindeutige Kennung Ihrer App.
   - **App entfernen, wenn MDM-Profil entfernt wird:** Wählen Sie aus, ob die App von Geräten entfernt werden soll, wenn das MDM-Profil entfernt wird. Die Standardeinstellung ist **Ein**.
   - **App-Datenbackup verhindern:** Wählen Sie aus, ob die App Daten sichern können soll. Die Standardeinstellung 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. Wenn sie akzeptieren, wird die App verwaltet.
9. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Bereitstellungsregeln.
10. Erweitern Sie **Storekonfiguration**.



- **App FAQ:** Klicken Sie auf **Fügen Sie eine neue häufig gestellte Frage und deren Antwort hinzu**, um eine FAQ für die App zu erstellen.
- **App-Screenshots für Mobiltelefone/Tablets:** Fügen Sie Screenshots hinzu, die im App Store angezeigt werden.
- **App-Bewertungen zulassen:** Erlauben Sie Benutzern, die App im App Store zu bewerten.
- **App-Kommentare zulassen:** Erlauben Sie Benutzern, Kommentare zur App im App Store zu hinterlassen.

11. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.

    Informationen zum Verwenden von Workflows für die Anforderung einer Genehmigung vor dem App-Zugriff durch Benutzer finden Sie unter Anwenden von Workflows. Wenn Sie keinen Genehmigungsworkflow benötigen, fahren Sie mit dem nächsten Schritt fort.

12. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.

13. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, um nach einer Bereitstellungsgruppe zu suchen, oder wählen Sie eine oder mehrere Gruppen in der Liste aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

14. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

    - **Bereitstellen:** Wählen Sie aus, ob die App auf Geräten bereitgestellt werden soll. Die Standardeinstellung ist **Ein**.
    - **Bereitstellungszeitplan:** Wählen Sie aus, ob die App **Jetzt** oder **Später** bereitgestellt werden soll. Bei Auswahl von **Später** konfigurieren Sie ein Datum und eine Uhrzeit für die Bereitstellung der App. Die Standardeinstellung ist **Jetzt**.
    - **Bereitstellungsbedingung:** Wählen Sie **Bei jeder Verbindung**, um die App bei jeder Verbindung des Geräts bereitzustellen. Wählen Sie **Nur bei Fehler in der vorherigen Bereitstellung**, um die App bereitzustellen, wenn das Gerät die App zuvor nicht erhalten hat. Die Standardeinstellung ist **Bei jeder Verbindung**.

    Die Option **Bereitstellen für immer aktive Verbindungen** gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.

    Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

15. Klicken Sie auf **Speichern**.

Hinzufügen von Weblinks

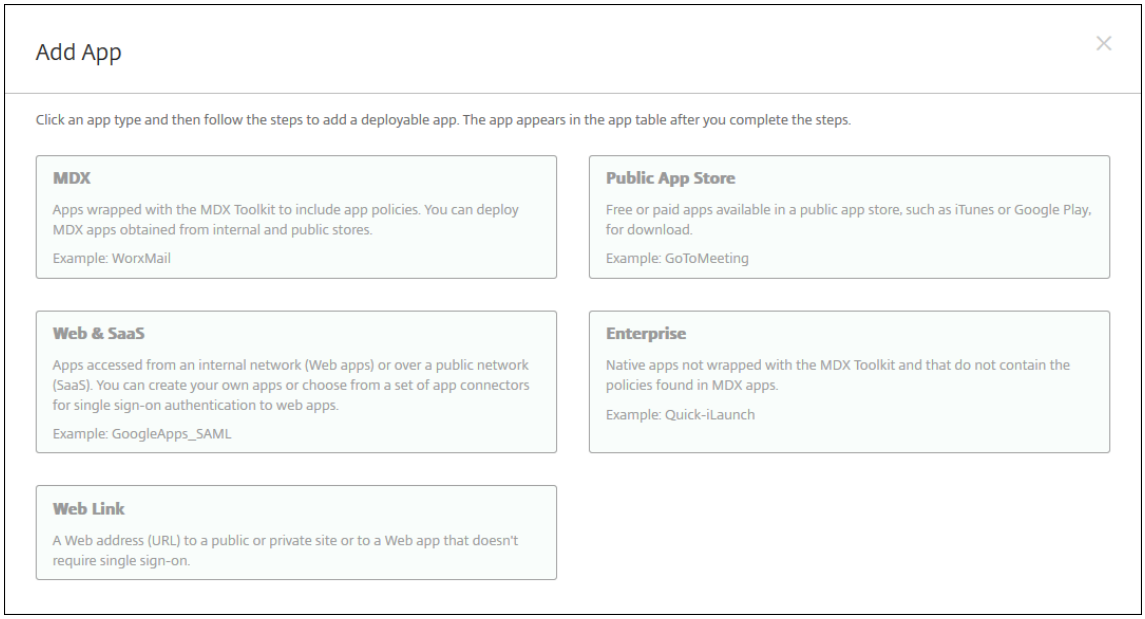
Ein Weblink ist die Webadresse einer Internet- oder Intranetsite. Er kann auch auf eine Web-App zeigen, für die kein SSO erforderlich ist. Wenn Sie die Konfiguration eines Weblinks abgeschlossen haben, wird dieser als Symbol im App-Store angezeigt. Der Link wird mit der Liste der verfügbaren Anwendungen und Desktops angezeigt, wenn Benutzer sich bei Secure Hub anmelden.

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 Tabelle **Apps** 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)

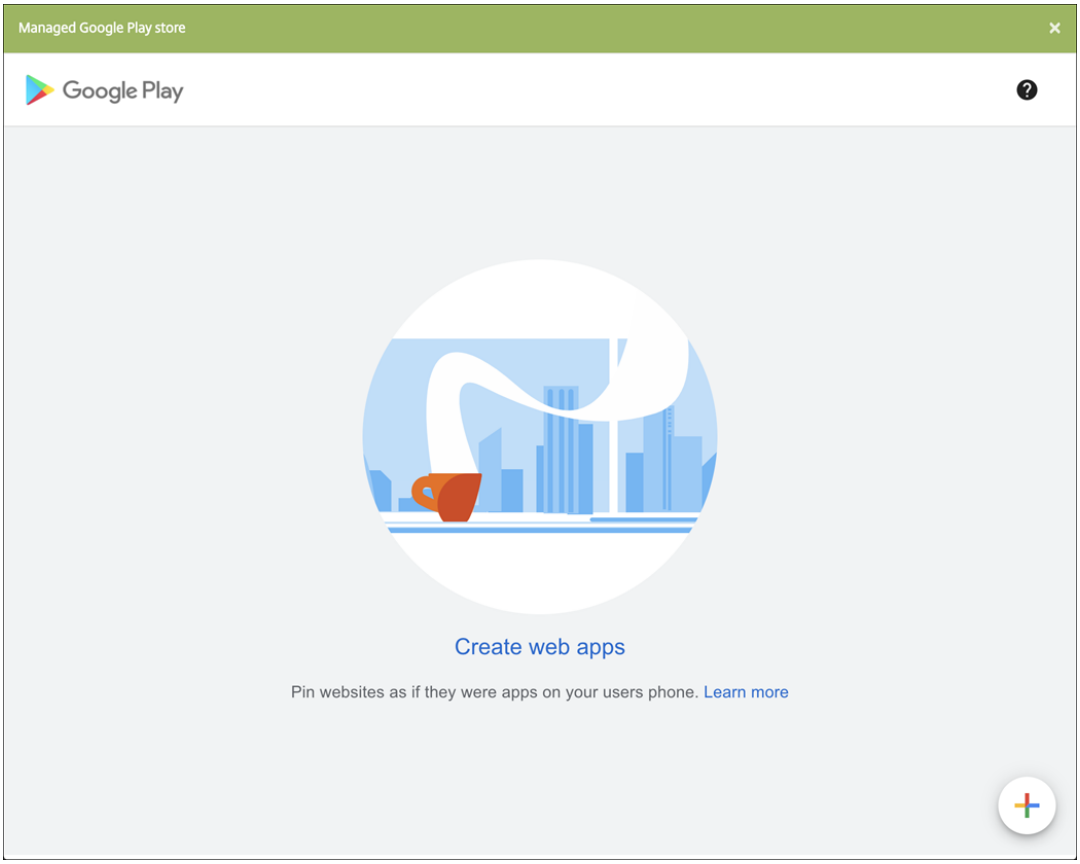
1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps > Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



2. Klicken Sie auf **Weblinks**. Die Seite **App-Informationen** wird angezeigt.
3. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:

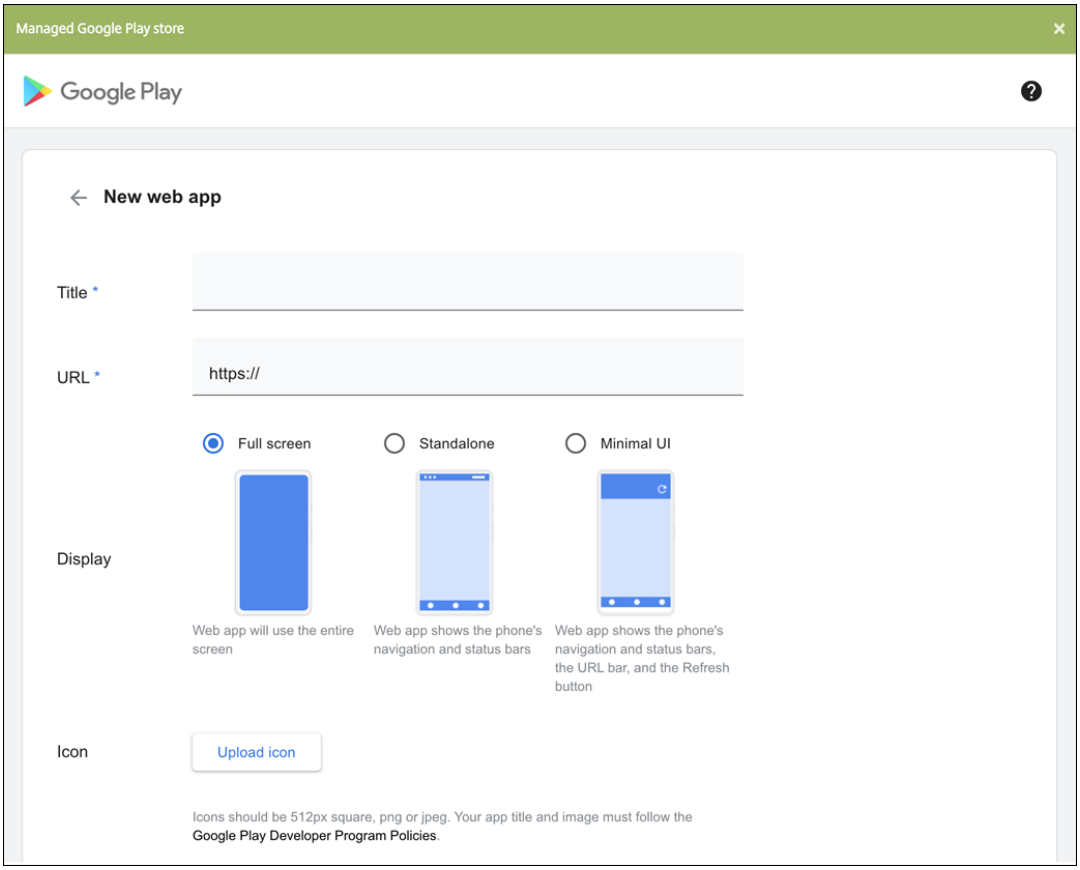
   Name: Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name” in der Tabelle “Apps” angezeigt.
   Beschreibung: Geben Sie optional eine Beschreibung der App ein.
   App-Kategorie: Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen möchten. Weitere Informationen zu App-Kategorien finden Sie unter App-Kategorien.
4. Klicken Sie auf **Weiter**. Die Seite **Plattform** wird angezeigt.
5. Wählen Sie unter **Plattformen** die Option **Andere Plattformen**, um eine Web-App für iOS und Android (Legacy-Geräteadministrator) hinzuzufügen, oder wählen Sie **Android Enterprise**. Deaktivieren Sie das Kontrollkästchen, das Sie nicht hinzufügen möchten.

   - Wenn Sie **Andere Plattformen** aktivieren, müssen Sie im nächsten Schritt die Einstellungen konfigurieren.
   - Bei Auswahl von **Android Enterprise** klicken Sie auf die Schaltfläche **Hochladen**, um den verwalteten Google Play Store zu öffnen. Sie müssen sich nicht für ein Entwicklerkonto registrieren, um eine Web-App zu veröffentlichen. Klicken Sie auf das **Plus**-Symbol in der unteren rechten Ecke, um fortzufahren.



Konfigurieren Sie folgende Einstellungen:

- **Title:** Geben Sie einen Namen für die Web-App ein.
- **URL:** Geben Sie die Webadresse für die App ein.
- **Display:** Wählen Sie aus, wie die Web-App auf Benutzergeräten angezeigt werden soll. Verfügbare Optionen sind **Vollbild**, **Eigenständig**und **Minimalistische Benutzeroberfläche**.
- **Icon:** Laden Sie Ihr eigenes Symbolbild für die Web-App hoch.



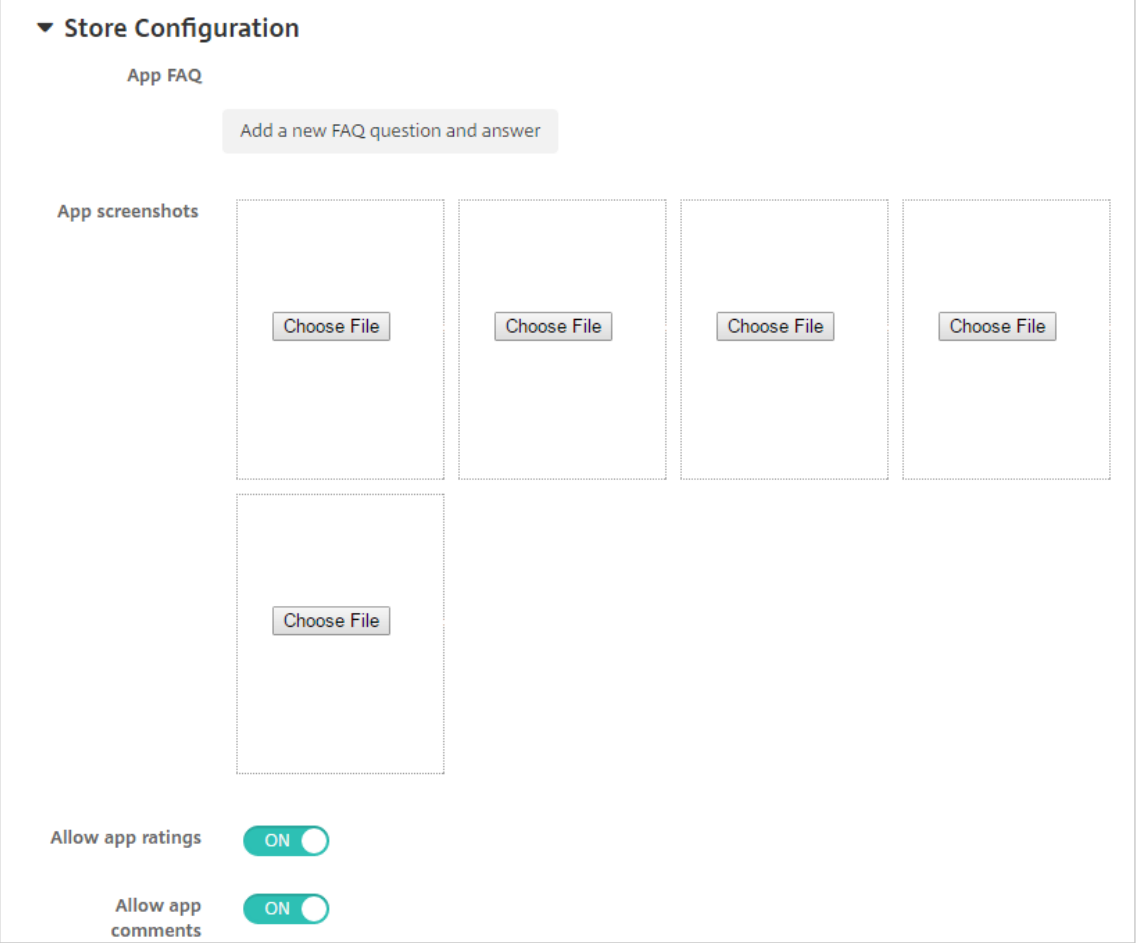
Wenn Sie fertig sind, klicken Sie auf **Erstellen**. Es kann bis zu 10 Minuten dauern, bis Ihre Web-App veröffentlicht wird.

6. Konfigurieren Sie für andere Plattformen als Android Enterprise 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:** Akzeptieren Sie die vorausgefüllte URL oder geben Sie die Webadresse der 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:** Wählen Sie, ob 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 Citrix Gateway erfolgen. Wenn Sie diese Option auf **EIN** festlegen, wird das VPN-Schlüsselwort der App hinzugefügt, sodass Benutzer eine Verbindung über Citrix Gateway herstellen können. Die Standardeinstellung 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. Die Standardeinstellung ist “Standard verwenden”.
  - Zum Hochladen eines eigenen Bilds klicken Sie auf **Durchsuchen**, navigieren Sie zu dem Speicherort der Bilddatei und wählen Sie diese aus. Die Datei muss eine PNG-Datei sein. Sie können keine JPEG- oder GIF-Dateien hochladen. Eine benutzerdefinierte Grafik kann später nicht mehr geändert werden.

7. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Bereitstellungsregeln.
8. Erweitern Sie **Storekonfiguration**.



- **App FAQ:** Klicken Sie auf **Fügen Sie eine neue häufig gestellte Frage und deren Antwort hinzu**, um eine FAQ für die App zu erstellen.
- **App-Screenshots für Mobiltelefone/Tablets:** Fügen Sie Screenshots hinzu, die im App Store angezeigt werden.
- **App-Bewertungen zulassen:** Erlauben Sie Benutzern, die App im App Store zu bewerten.
- **App-Kommentare zulassen:** Erlauben Sie Benutzern, Kommentare zur App im App Store zu hinterlassen.

9. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.
10. Nehmen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe vor, um nach einer Bereitstellungsgruppe zu suchen, oder wählen Sie eine oder mehrere Gruppen in der Liste aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.
11. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:
    - **Bereitstellen:** Wählen Sie aus, ob die App auf Geräten bereitgestellt werden soll. Die Standardeinstellung ist **Ein**.
    - **Bereitstellungszeitplan:** Wählen Sie aus, ob die App **Jetzt** oder **Später** bereitgestellt werden soll. Bei Auswahl von **Später** konfigurieren Sie ein Datum und eine Uhrzeit für die Bereitstellung der App. Die Standardeinstellung ist **Jetzt**.
    - **Bereitstellungsbedingung:** Wählen Sie **Bei jeder Verbindung**, um die App bei jeder Verbindung des Geräts bereitzustellen. Wählen Sie **Nur bei Fehler in der vorherigen Bereitstellung**, um die App bereitzustellen, wenn das Gerät die App zuvor nicht erhalten hat. Die Standardeinstellung ist **Bei jeder Verbindung**.

    Die Option **Bereitstellen für immer aktive Verbindungen** gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.

    Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.
12. Klicken Sie auf **Speichern**.

Aktivieren von Microsoft 365-Apps

Sie können den MDX-Container öffnen, um Secure Mail, Secure Web und Citrix Files 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.

Anwenden von Workflows

Konfigurieren Sie folgende Einstellungen zum Erstellen oder Zuweisen eines Workflows:

- **Verwendete Workflows:** Klicken Sie in der Liste auf einen Workflow oder klicken Sie auf **Neuen Workflow erstellen**. Die Standardeinstellung 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 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 **Search**, um das Suchergebnis einzuschränken.
  * Die Namen der Personen in der Liste **Selected additional required approvers** sind im Suchergebnis mit einem Häkchen gekennzeichnet. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Personen, die Sie entfernen möchten.

Branding für den App-Store und Citrix Secure Hub

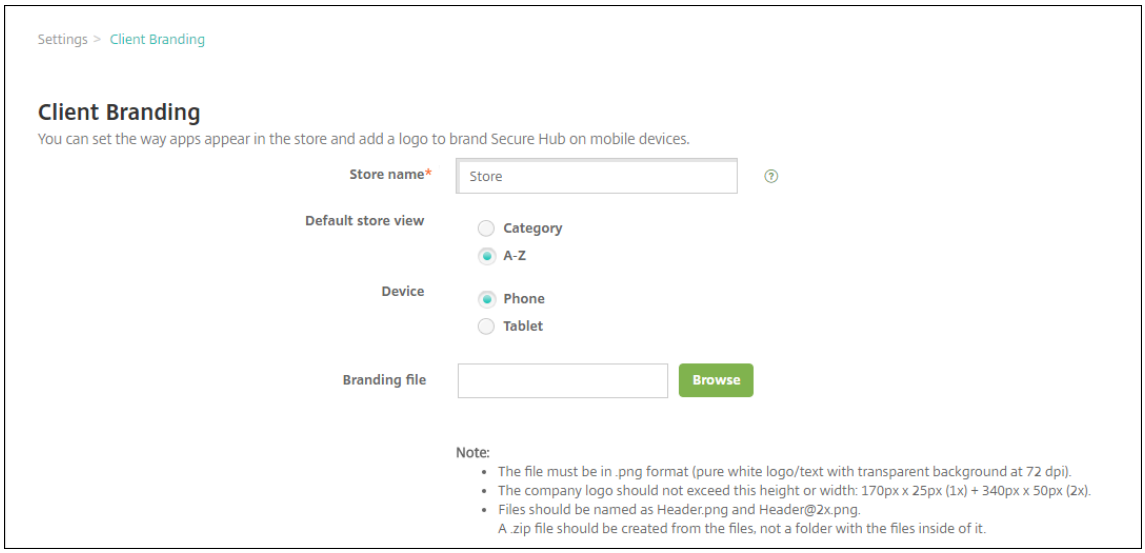
Sie können einstellen, wie Apps im Store angezeigt werden und ein Logo hinzufügen, um ein Branding für Secure Hub und den App-Store zu erstellen. Diese Branding-Features stehen für iOS- und Android-Geräte zur Verfügung.

Stellen Sie zunächst 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 Konsole von XenMobile Server rechts oben auf das Zahnradsymbol. 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.

     > **Wichtig:**
     >
     > Der Storename darf nur alphanumerische Zeichen enthalten.

   - **Standardstoreansicht:** Wählen Sie die Option **Kategorie** oder **A-Z** aus. Die Standardeinstellung ist **A-Z**.
   - **Gerät:** Wählen Sie **Telefon** oder **Tablet** aus. Die Standardeinstellung 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**.

App-Connectortypen

April 17, 2019

In der folgenden Tabelle finden Sie die Connectors und Connectortypen, die in XenMobile beim Hinzufügen einer Web- oder SaaS-App verfügbar sind. Sie können auch einen neuen Connector zu XenMobile hinzufügen, wenn Sie eine Web-oder SaaS-App hinzufügen.

Die Tabelle enthält Angaben dazu, ob ein Connector die Benutzerkontenverwaltung unterstützt, mit der neue Konten automatisch oder mit einem Workflow erstellt werden können.

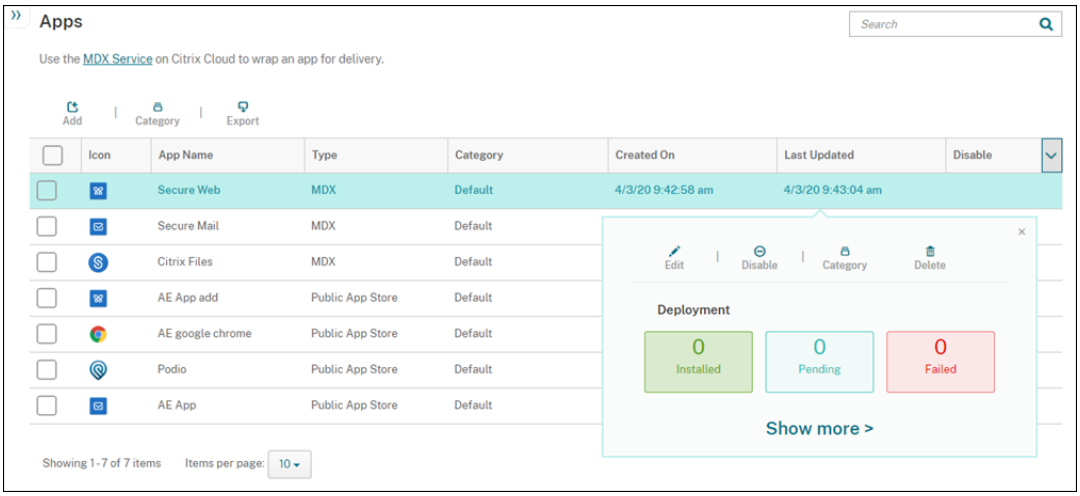
Connectorname	Single Sign-On SAML	Unterstützt Benutzerkontenverwaltung
EchoSign_SAML	J	J
Globoforce_SAML		**Hinweis:** Wenn Sie diesen Connector verwenden, müssen Sie “Benutzerverwaltung” für Provisioning aktivieren, um eine nahtlose SSO-Integration zu gewährleisten.
GoogleApps_SAML	J	J
GoogleApps_SAML_IDP	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

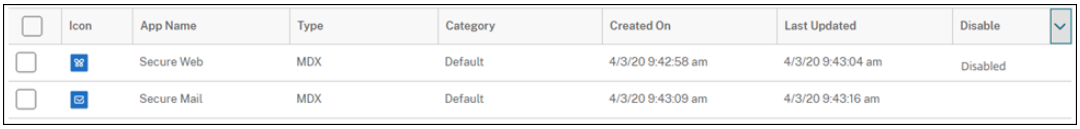
January 5, 2022

Zum Aktualisieren einer MDX- oder Unternehmensapp in XenMobile deaktivieren Sie diese in der XenMobile-Konsole und laden Sie die neue App-Version hoch. Sie brauchen öffentliche App-Store-Apps wie Citrix Secure Mail nicht zu deaktivieren.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Apps**. Die Seite **Apps** wird angezeigt.
2. Fahren Sie bei verwalteten Geräten (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:
   a) Aktivieren Sie in der Tabelle **Apps** das Kontrollkästchen neben der App oder klicken Sie auf die Zeile mit der zu aktualisierenden App.
   b) Klicken Sie in dem daraufhin angezeigten Menü auf **Deaktivieren**.



   c) Klicken Sie im Bestätigungsdialogfeld auf **Deaktivieren**. In der Spalte *Deaktivieren* der App wird nun **Deaktiviert** angezeigt.



> **Hinweis:**
>
> Benutzer können nach der Abmeldung keine Verbindung mit deaktivierten Apps mehr herstellen. Das Deaktivieren von Apps ist optional, es wird jedoch empfohlen, um Probleme bei der App-Funktionalität zu vermeiden. Beispielsweise kann ein

> Problem auftreten, wenn Benutzer einen Download der App anfordern, während Sie die neue Version hochladen.

3. Aktivieren Sie in der Tabelle **Apps** das Kontrollkästchen neben der App oder klicken Sie auf die Zeile mit der zu aktualisierenden App.
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 folgende 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:
   a) Wählen Sie die Datei aus, die Sie hochladen möchten, indem Sie auf **Upload** klicken und zur Datei navigieren. Die Anwendung wird in XenMobile hochgeladen.

      Wenn Sie eine App für Android Enterprise hochladen, wird ein verwaltetes Google Play-Fenster angezeigt. Laden Sie die neue Version der App hier hoch. Weitere Informationen finden Sie unter Verteilen von Android Enterprise-Apps.

   b) Falls gewünscht, können Sie die App-Details und Richtlinieneinstellungen für die Plattform ändern.

   c) Konfigurieren Sie, falls gewünscht, Bereitstellungsregeln und XenMobile Store-Konfigurationen. Informationen hierzu finden Sie unter Hinzufügen von Apps im Abschnitt “Hinzufügen von MDX-Apps”.
7. Klicken Sie auf **Speichern**. Die Seite **Apps** wird angezeigt.
8. Wenn Sie die App in Schritt 2 deaktiviert haben, führen Sie folgende Schritte aus:
   a) Klicken Sie in der Tabelle **Apps** auf die aktualisierte App und klicken Sie dann im angezeigten Menü auf **Aktivieren**.
   b) Klicken Sie in dem daraufhin angezeigten Bestätigungsdialogfeld auf **Aktivieren**. Die Benutzer können jetzt auf die App zugreifen und erhalten eine Benachrichtigung mit der Aufforderung, die App zu aktualisieren.

Citrix Launcher

January 5, 2022

Alternativen für Citrix Launcher

Citrix Launcher wird im August 2020 aus dem App Store entfernt. Anstelle von Citrix Launcher können Sie bereits verfügbare Features verwenden.

Provisioning dedizierter Geräte als Kiosk:

1. Fügen Sie eine RBAC-Rolle hinzu, mit der XenMobile-Administratoren dedizierte Geräte bei XenMobile registrieren können. Siehe Provisioning von dedizierten Android Enterprise-Geräten.
2. Erstellen Sie ein Registrierungsprofil mit dem **Registrierungstyp Vollständig verwaltet/Arbeitsprofil**. Siehe Erstellen eines Registrierungsprofils.
3. Erstellen Sie eine Kioskgeräterichtlinie, um eine App durch Aktivieren der Einstellung **LockTask-Modus** an den Gerätebildschirm anzuheften. Siehe Android Enterprise-Einstellungen.

Info zu Citrix Launcher

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. Citrix Launcher und die Launcher-Konfigurationsrichtlinie sind nicht mit Android Enterprise kompatibel.

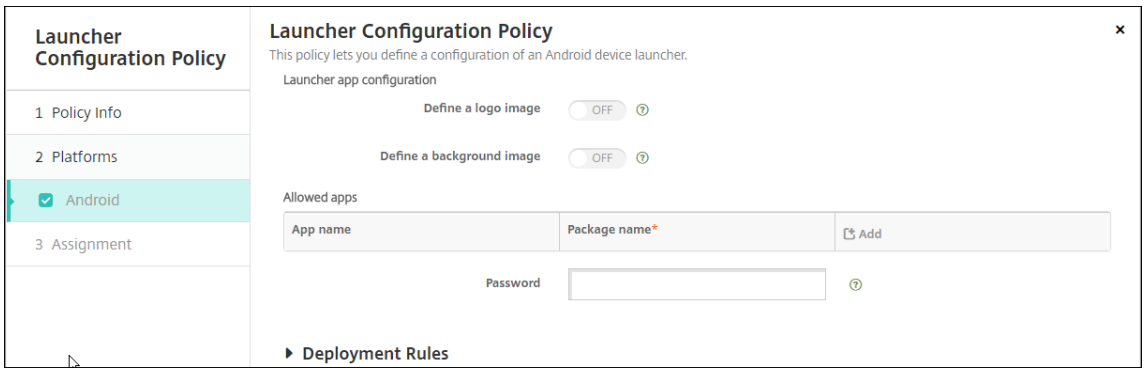
Mit der **Launcher-Konfigurationsrichtlinie**können Sie folgende Citrix Launcher-Features steuern:

- 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

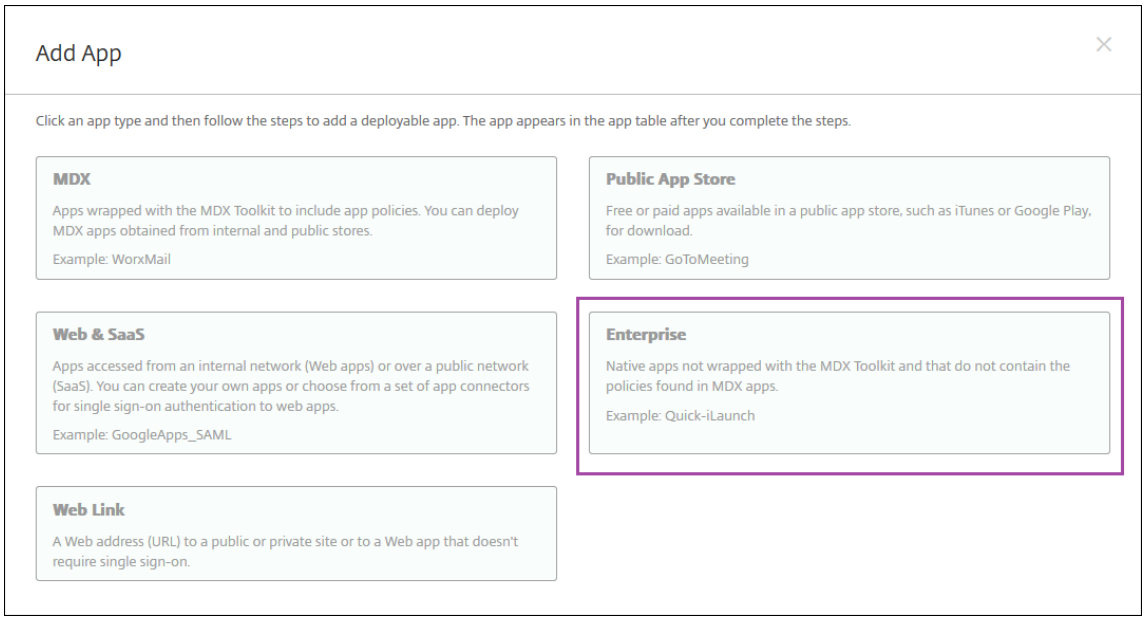
Mit Citrix Launcher können Sie diese Einschränkungen auf Geräteebene festlegen, gleichzeitig bietet Launcher den Benutzern integrierten Zugriff auf Geräteeinstellungen, wie z. B. für WiFi, Bluetooth und Gerätepasscode. Citrix Launcher ist nicht als zusätzliche Sicherheitsstufe gedacht.

Das Verfahren zum Bereitstellen von Citrix Launcher für Android-Geräte ist folgendes:

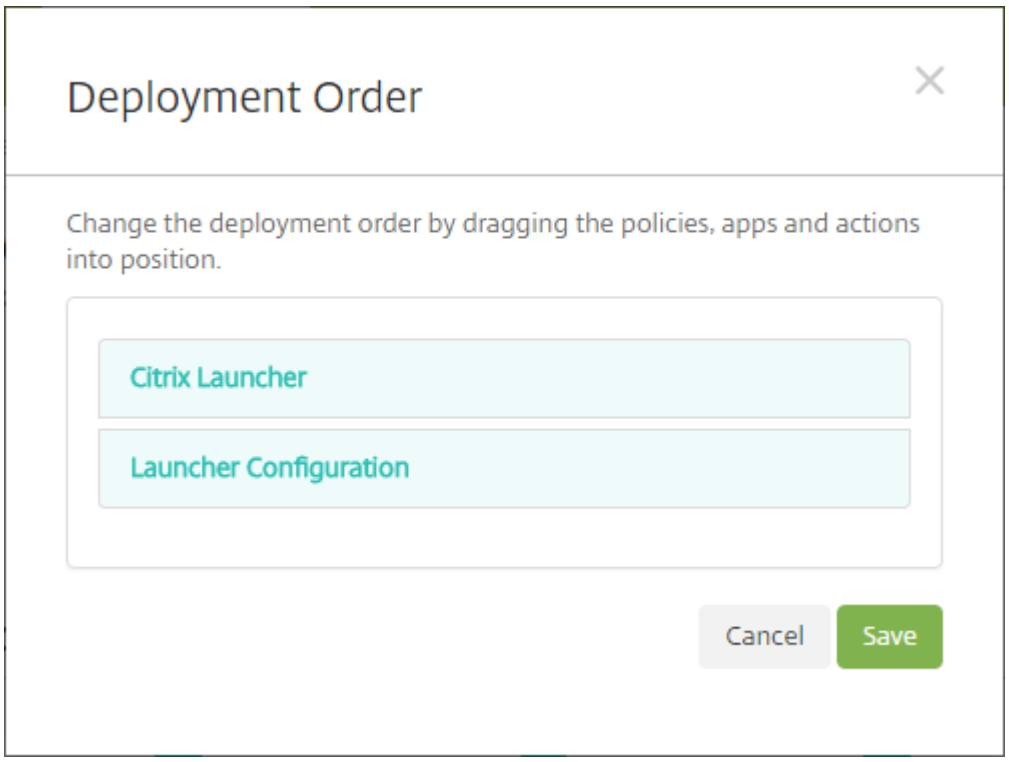
1. So laden Sie die Citrix Launcher App herunter: Wechseln Sie zu https://www.citrix.com/downloads. Suchen Sie nach **Citrix Launcher**. Der Dateiname lautet CitrixLauncher.apk. Die Datei kann ohne Umschließen in XenMobile hochgeladen werden.
2. Fügen Sie die **Launcher-Konfigurationsrichtlinie** hinzu. 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 als Unternehmensapp zu XenMobile hinzu. Klicken Sie unter **Konfigurieren > Apps** auf **Hinzufügen** und dann auf **Unternehmensanwendungen**. 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 stellen Sie sicher, dass die App **Citrix Launcher** vor der Richtlinie **Launcher-Konfiguration** steht.



Weitere Informationen finden Sie unter Bereitstellen von Ressourcen.

Apple Volume Purchase

January 5, 2022

Sie können die Lizenzierung von iOS-Apps über Apple iOS Volume Purchase verwalten. Die Volume Purchase-Lösung vereinfacht Suche, Erwerb und Verteilung von Apps und anderen Daten in großer Zahl.

Mit Volume Purchase können Sie XenMobile zur Verteilung von Apps aus dem öffentlichen App-Store verwenden.

- Volume Purchase wird für die MAM-Registrierung nicht unterstützt. Sie müssen Volume Purchase-Geräte in MDM oder MDM+MAM registrieren.
- Volume Purchase wird nicht für mobile Produktivitätsapps von Citrix unterstützt.
- Sie können XenMobile-Apps aus dem öffentlichen Store zwar mit Volume Purchase verteilen, die Bereitstellung ist jedoch nicht optimal. Verbesserungen an XenMobile und dem Secure Hub-Store sind erforderlich, um diese Einschränkungen zu beheben.
- Eine Liste der bekannten Probleme bei der Verteilung von XenMobile Apps aus dem öffentlichen Store über Volume Purchase finden Sie im Citrix Knowledge Center.

Mit Volume Purchase können Sie Apps direkt auf Ihre Geräte verteilen, oder Sie weisen Benutzern Inhalte über einlösbare Codes zu. Sie konfigurieren Einstellungen für iOS Volume Purchase in XenMobile.

XenMobile importiert Volume Purchase-Lizenzen in regelmäßigen Abständen erneut von Apple, um sicherzustellen, dass die Lizenzen alle Änderungen enthalten. Diese Änderungen umfassen das manuelle Löschen einer importierten App aus Volume Purchase. Standardmäßig aktualisiert XenMobile die Volume Purchase-Lizenzbasis mindestens alle 1440 Minuten (24 Stunden). Sie können das Volume Purchase-Basisintervall über die Servereigenschaft `VPP.baseline` ändern. Siehe Servereigenschaften.

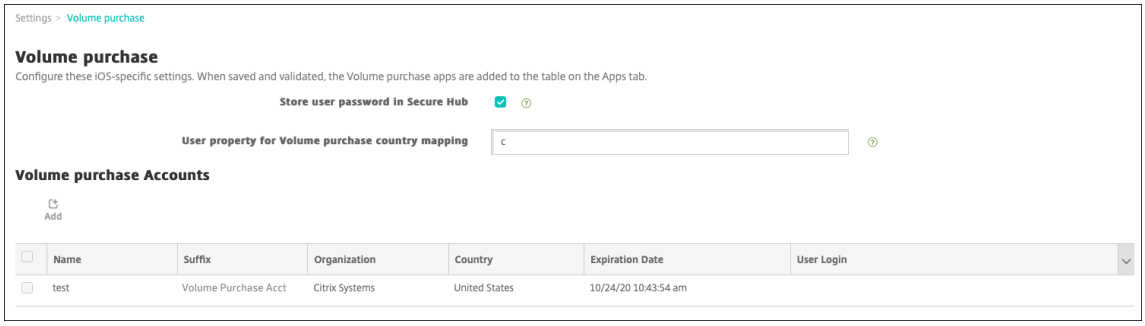
Die Einstellung **Automatische App-Updates** basiert ebenfalls auf der Servereigenschaft `VPP.baseline`, und Apps werden nach dem in dieser Eigenschaft festgelegten Zeitplan aktualisiert.

In diesem Artikel wird die Verwendung von Volume Purchase 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 Von Einlösecodes zur verwalteten Verteilung migrieren.

Informationen zum Erwerb von iOS-Volumenlizenzen (iOS Volume Purchase) finden Sie unter https://volume.itunes.apple.com/us/store. Zur Registrierung für Volume Purchase gehen Sie zu https://deploy.apple.com/qforms/open/register/index/avs. Um auf Ihren Volumenkauf-Shop in iTunes zuzugreifen, gehen Sie zu https://volume.itunes.apple.com/?l=en.

Wenn Sie die iOS Volume Purchase-Einstellungen in XenMobile gespeichert haben, werden die erworbenen Apps auf der Seite **Konfigurieren > Apps** in der XenMobile-Konsole angezeigt.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf **Volume Purchase**. Die Konfigurationsseite **Volume Purchase** 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 Volume Purchase-Länderzuordnung:** Geben Sie einen Code ein, um das Herunterladen aus landesspezifischen App-Stores zuzulassen.

Diese Zuweisung wird von XenMobile zur Auswahl des Eigenschaftenpools von Volume Purchase verwendet. Mit der Benutzereigenschaft “United States” können beispielsweise keine Apps heruntergeladen werden, wenn ihr Volume Purchase-Code für Deutschland gilt. Weitere Informationen über den Länderzuweisungscode erhalten Sie beim Volume Purchase-Administrator.

4. Klicken Sie für jedes Volume Purchase-Konto, das Sie hinzufügen möchten, auf **Hinzufügen**. Das Dialogfeld **Volume Purchase-Konto hinzufügen** wird angezeigt.
5. 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 **Volume Purchase**.

   - **Name:** Geben Sie einen Namen für das Volume Purchase-Konto ein.
   - **Suffix:** Geben Sie das Suffix ein, das mit dem Namen von Apps angezeigt werden soll, die über das Volume Purchase-Konto erworben wurden. Beispiel: Bei Eingabe von **VP** wird die App “Secure Mail” in der App-Liste als **Secure Mail - VP** angezeigt.
   - **Unternehmenstoken:** Kopieren Sie das von Apple erhaltene Volume Purchase-Diensttoken und fügen Sie es ein. Zum Anfordern des Tokens klicken Sie auf der Seite mit der **Kontoübersicht** im Apple Volume Purchase-Portal auf die Schaltfläche **Herunterladen** zum Erstellen und Herunterladen der Volume Purchase-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 Volume Purchase-Kontos ein, das für den Import von benutzerdefinierten B2B-Apps verwendet wird.
   - **Benutzerkennwort:** Geben Sie das Administratorkennwort für das Volume Purchase-Konto ein.
   - **Automatische App-Updates:** Bei Auswahl von **Ein** werden Volume Purchase-Apps automatisch aktualisiert, sobald ein Update im Apple Store vorliegt. Die Standardeinstellung ist **Aus**.
6. Klicken Sie auf **Speichern**, um das Dialogfeld zu schließen.
7. Klicken Sie auf **Speichern**, um die Volume Purchase-Konfiguration zu speichern.

   Es wird nun gemeldet, dass die Apps in XenMobile der Liste auf der Seite **Konfigurieren > Apps** hinzugefügt werden. Auf dieser Seite werden die Namen der Apps aus Ihrem Volume Purchase-Konto mit dem von Ihnen in der obigen Konfiguration angegebenen Suffix angezeigt.

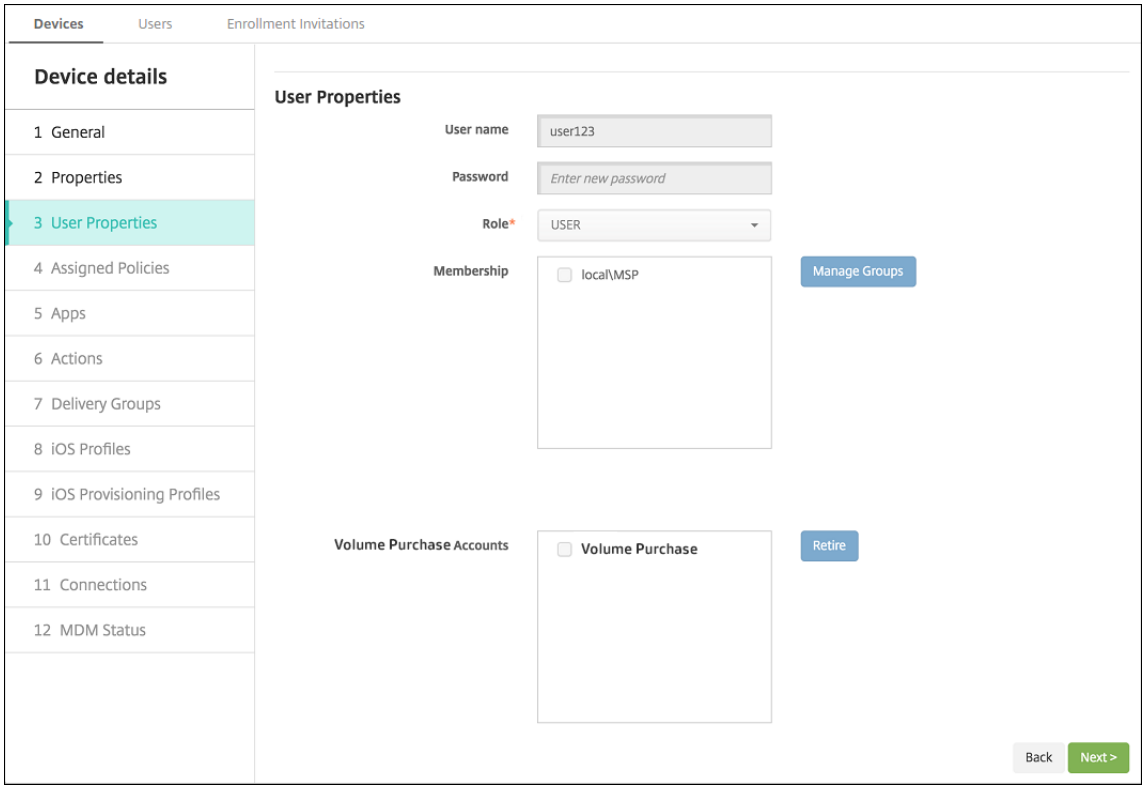
Sie können jetzt die Einstellungen für Volume Purchase-Apps konfigurieren und anschließend die Richtlinieneinstellungen für Bereitstellungsgruppen und Geräte für die Volume Purchase-Apps. Wenn Sie diese Konfiguration abgeschlossen haben, können Benutzer ihre Geräte registrieren. Die folgenden Hinweise sollten bei diesen Verfahren berücksichtigt werden.

- Beim Konfigurieren der Volume Purchase-App-Einstellungen (**Konfigurieren > Apps**) aktivieren Sie **Lizenzzuordnung zu Gerät erzwingen**. Ein Vorteil des Volume Purchase und Deployment Program von Apple für betreute Geräte: Apps können über XenMobile auf Geräteebene anstatt auf Benutzerebene zugewiesen werden. Es muss kein Gerät mit Apple-ID verwendet werden. Außerdem erhalten Benutzer keine Einladung zur Teilnahme an Apple Volume Purchase. Benutzer können die Apps zudem ohne Anmeldung bei ihrem iTunes-Konto herunterladen.

  Um die Volume Purchase-Informationen für diese App anzuzeigen, erweitern Sie **Volume Purchase**. In der Tabelle **Volume Purchase-Lizenzschlüssel** ist die Lizenz einem Gerät zugeordnet. Wenn der Benutzer das Token entfernt und es dann wieder importiert, wird anstelle der Seriennummer aufgrund von Apple-Datenschutzeinschränkungen der Hinweis **ausgeblendet** angezeigt.

  Um eine Lizenzzuweisung aufzuheben, klicken Sie auf die Zeile der Lizenz und dann auf **Zuweisung aufheben**.

  Wenn Sie Volume Purchase-Lizenzen Benutzern zuordnen, integriert XenMobile die Benutzer in Ihr Volume Purchase-Konto und ihre iTunes-ID wird dem Volume Purchase-Konto zugeordnet. 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 Apple Volume Purchase 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**. 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: Wenn die App von Volume Purchase per Push bereitgestellt wurde, wird sie auf Geräten automatisch aktualisiert. Führen Sie folgende Schritte aus, um ein Update für Secure Hub bereitzustellen, das keinem Benutzer, sondern einem Gerät zugewiesen wurde. Klicken Sie auf der Plattformseite unter **Konfigurieren > Apps** auf **Nach Updates suchen** und wenden Sie das Update an.

  XenMobile zeigt eine Lizenzablaufwarnung an, wenn Apple Volume Purchase abgelaufen ist.

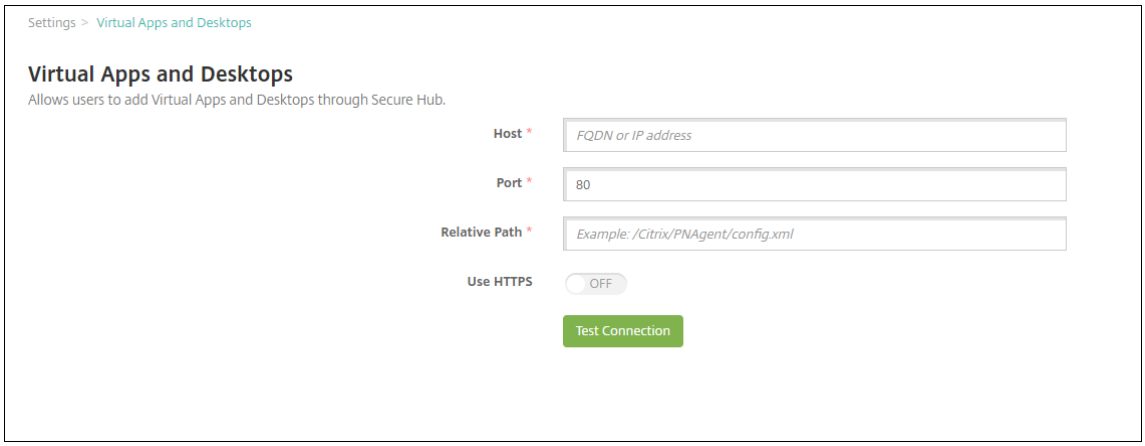
Virtuelle Apps und Desktops über Citrix Secure Hub

January 5, 2022

XenMobile kann Apps aus Virtual Apps and Desktops 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 **Virtual Apps and Desktops**. Die Seite **Virtual Apps and Desktops** wird angezeigt.



3. Konfigurieren Sie folgende 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 Standardeinstellung 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. Die Standardeinstellung ist **Aus**.
4. Klicken Sie auf **Verbindung testen**, um zu prüfen, ob XenMobile eine Verbindung mit dem angegebenen Virtual Apps and Desktops-Server herstellen kann.
5. Klicken Sie auf **Speichern**.

Verwenden von Citrix Content Collaboration mit XenMobile

January 5, 2022

XenMobile bietet zwei Optionen für die Integration in Citrix Content Collaboration: Citrix Files und Speicherzonenconnectors. Für die Integration in Citrix Files oder Speicherzonenconnectors ist XenMobile Enterprise Edition erforderlich.

Citrix Files

Wenn Sie über XenMobile Enterprise Edition verfügen, können Sie XenMobile zur Bereitstellung des Zugriffs auf das Citrix Files-Konto konfigurieren. Diese Konfiguration:

- Bietet mobilen Benutzern Zugriff auf alle Enterprise-Features, wie Dateifreigabe, Dateisynchronisierung und Speicherzonenconnectors.
- Kann Citrix Files mit Single Sign-On-Authentifizierung von XenMobile-App-Benutzern und umfassenden Zugriffssteuerungsrichtlinien bereitstellen.
- Bietet Citrix Files-Konfiguration, Servicelevel- und Lizenznutzungsüberwachung über die XenMobile-Konsole.

Weitere Informationen zur Konfiguration von XenMobile für Citrix Files finden Sie unter SAML für Single Sign-On mit Citrix Files.

Speicherzonenconnectors

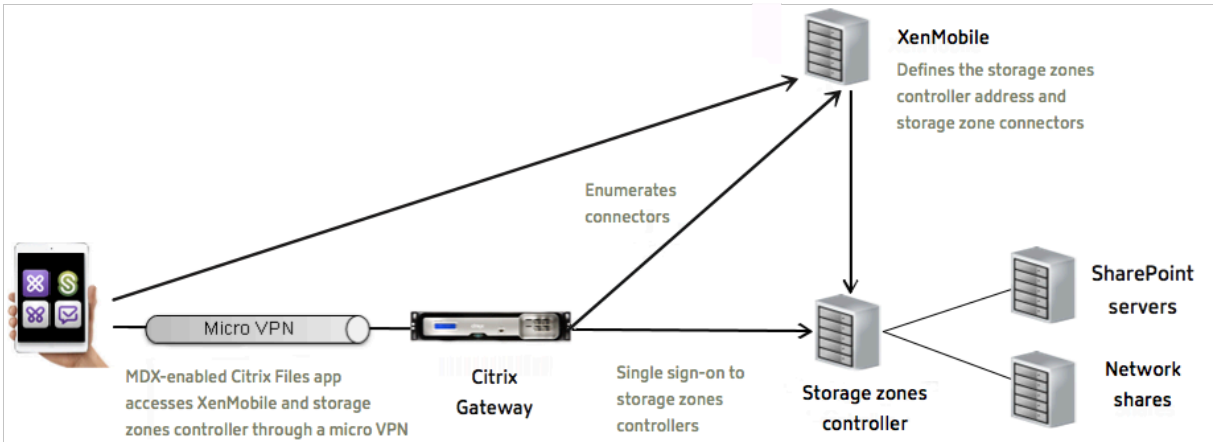
Sie können XenMobile so konfigurieren, dass der Zugriff auf Speicherzonenconnectors limitiert wird, die Sie über die XenMobile-Konsole erstellen. Diese Konfiguration:

- Bietet sicheren mobilen Zugriff auf vorhandene lokale Speicherrepositorys, wie SharePoint-Sites und Netzwerkdateifreigaben.
- Erfordert nicht, dass Sie eine Citrix Content Collaboration-Unterdomäne einrichten oder Citrix Files-Daten hosten.
- Bietet Benutzern mobilen Zugriff auf Daten über die mobilen Citrix Files-Produktivitätsapps für iOS und Android. Benutzer können Microsoft Office-Dokumente bearbeiten. Benutzer können darüber hinaus Adobe PDF-Dateien auf Mobilgeräten in der Vorschau anzeigen und mit Anmerkungen versehen.
- Entspricht den Sicherheitsbeschränkungen, die verhindern, dass Benutzerdaten außerhalb des Unternehmensnetzwerks gelangen.
- Bietet einfache Einrichtung von Speicherzonenconnectors über die XenMobile-Konsole. Wenn Sie zu einem späteren Zeitpunkt alle Citrix Files-Funktionen mit XenMobile verwenden möchten, können Sie die Konfiguration in der XenMobile-Konsole ändern.
- Erfordert XenMobile Enterprise Edition.

Bei einer Integration von XenMobile ausschließlich mit Speicherzonenconnectors gilt:

- Citrix Content Collaboration nutzt die Konfiguration mit Single Sign-On bei Citrix Gateway zur Authentifizierung bei einem Speicherzonencontroller.
- XenMobile authentifiziert nicht über SAML, da die Citrix Files-Steuerungsebene nicht verwendet wird.

Das folgende Diagramm zeigt die allgemeine Architektur für die Verwendung von XenMobile mit Speicherzonenconnectors.



Anforderungen

- Mindestversionen der Komponenten:
  - XenMobile Server 10.5 (on-premises)
  - ShareFile für iOS (MDX) 5.3
  - ShareFile für Android (MDX) 5.3
  - Speicherzonencontroller 5.0

    Dieser Artikel enthält Anweisungen zum Konfigurieren von Speicherzonencontroller 5.0.
- Stellen Sie sicher, dass der Server, auf dem der Speicherzonencontroller ausgeführt werden soll, die Systemanforderungen erfüllt. Informationen zu den Anforderungen finden Sie unter Systemanforderungen.

Die Systemanforderungen für Speicherzonen für Citrix Files-Daten und für eingeschränkte Speicherzonen gelten nicht für die ausschließliche Integration von XenMobile mit Speicherzonenconnectors.

XenMobile unterstützt keine Documentum-Connectors.

- Ausführen von PowerShell-Skripts:
  - Führen Sie die Skripts in der 32-Bit-Version (x86) von PowerShell aus.

Installationsaufgaben

Führen Sie folgende Aufgaben in der vorgegebenen Reihenfolge aus, um den Speicherzonencontroller zu installieren und einzurichten. Die Schrittfolge gilt nur für die Integration von XenMobile mit ausschließlich Speicherzonenconnectors: Einige dieser Artikel sind in der Dokumentation für den Speicherzonencontroller aufgeführt.

1. Konfigurieren von Citrix ADC für Speicherzonencontroller

   Sie können Citrix ADC als DMZ-Proxy für einen Speicherzonencontroller verwenden.
2. Installieren eines SSL-Zertifikats

Für einen Speicherzonencontroller, der als Host für Standardzonen eingesetzt wird, benötigen Sie ein SSL-Zertifikat. Für einen Speicherzonencontroller, der als Host für eingeschränkte Zonen eingesetzt wird und eine interne Adresse verwendet, benötigen Sie kein SSL-Zertifikat.

3. Vorbereiten des Servers

   Für Speicherzonenconnectors ist ein IIS- und ASP.NET-Setup erforderlich.

4. Installation des Speicherzonencontrollers
5. Vorbereiten des Speicherzonencontrollers für die ausschließliche Verwendung mit Speicherzonenconnectors
6. Festlegen eines Proxyservers für Speicherzonen

   Über die Speicherzonencontroller-Konsole können Sie einen Proxyserver für Speicherzonencontroller festlegen. Sie können einen Proxyserver auch mit anderen Methoden festlegen.

7. Konfiguration des Domänencontrollers, sodass er dem Speicherzonencontroller für die Delegierung vertraut

   Legen Sie fest, dass der Domänencontroller die NTLM- oder Kerberos-Authentifizierung auf Netzwerkfreigaben oder SharePoint-Sites unterstützt.

8. Anfügen eines sekundären Speicherzonencontrollers an eine Speicherzone

   Konfigurieren Sie eine Speicherzone mit hoher Verfügbarkeit durch Einbinden von mindestens zwei Speicherzonencontrollers.

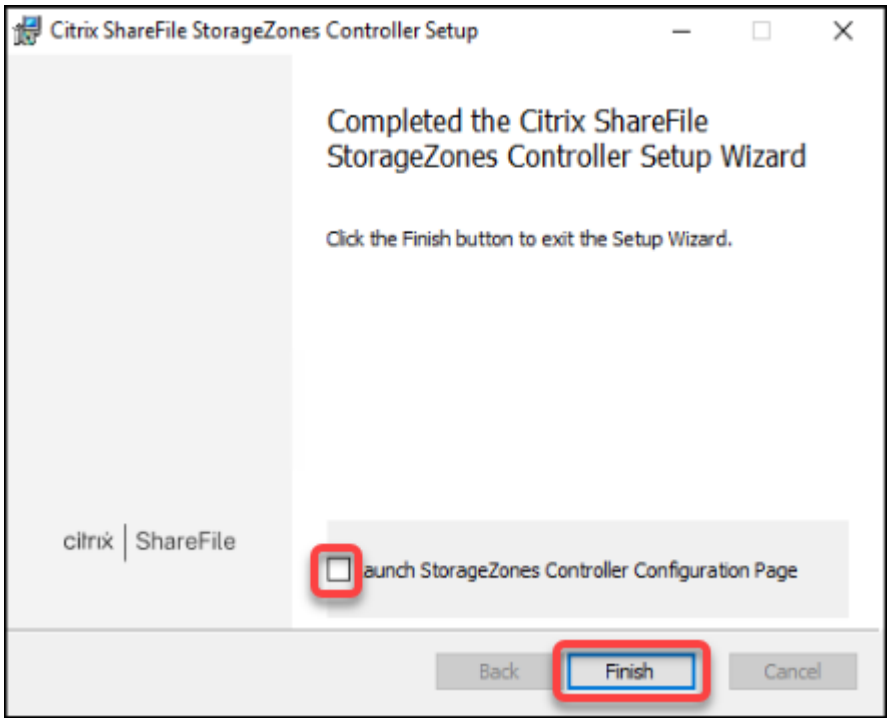
Installation des Speicherzonencontrollers

1. Führen Sie Download und Installation der Speicherzonencontroller-Software durch:
   a) Gehen Sie zu https://www.citrix.com/downloads. Suchen Sie nach **ShareFile** und laden Sie dann das neueste Installationsprogramm für den Speicherzonecontroller herunter.
   b) Durch Installation des Speicherzonencontrollers wechselt die Standardwebsite des Servers zum Installationspfad des Controllers. Aktivieren Sie **Anonyme Authentifizierung** auf der Standardwebsite.
2. Führen Sie StorageCenter.msi auf dem Server aus, auf dem Sie den Speicherzonencontroller installieren möchten.

   Der Speicherzonencontroller-Setupassistent wird gestartet.

3. Reagieren Sie auf die Eingabeaufforderungen:
   - Übernehmen Sie die Voreinstellungen auf der Seite **Zielordner**, wenn IIS (Internetinformationsdienste) am Standardspeicherort installiert ist. Ist dies nicht der Fall, navigieren Sie zum Installationsort von IIS.

- Nach Abschluss der Installation deaktivieren Sie das Kontrollkästchen zum **Start der Speicherzonencontroller-Konfigurationsseite** und klicken Sie auf **Fertig stellen**.



4. Wenn Sie dazu aufgefordert werden, starten Sie den Speicherzonencontroller neu.
5. Navigieren Sie zur Seite `https://localhost/`, um den Erfolg der Installation zu überprüfen. Bei erfolgreicher Installation wird das Citrix Files-Logo angezeigt.

   Wird das Citrix Files-Logo nicht angezeigt, löschen Sie den Browsercache und versuchen es noch einmal.

   > **Wichtig:**
   >
   > Wenn Sie den Speicherzonencontroller klonen möchten, erstellen Sie zunächst ein Datenträgerimage, bevor Sie mit der Konfiguration des Speicherzonencontrollers fortfahren.

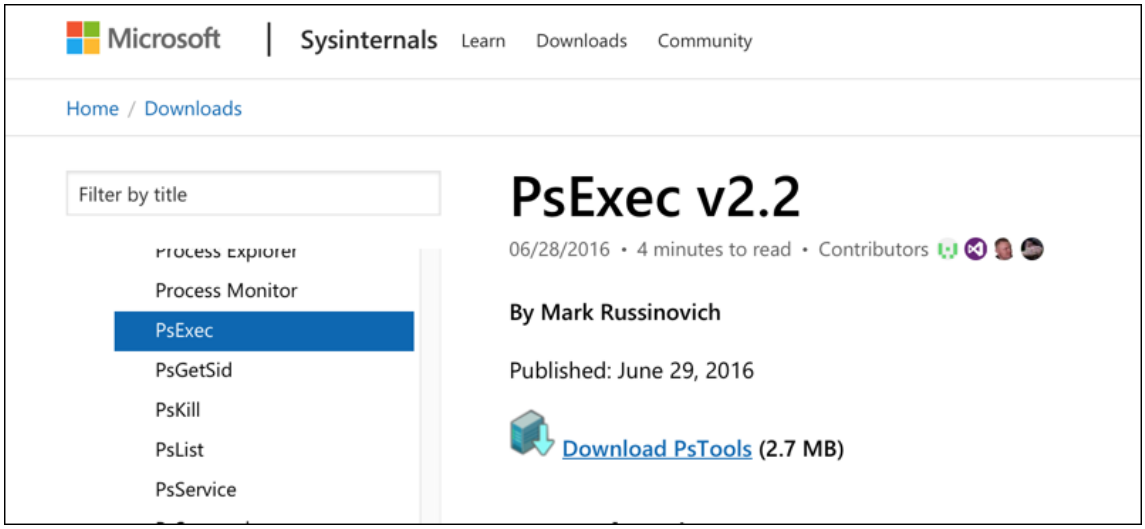
Vorbereiten des Speicherzonencontrollers für die ausschließliche Verwendung mit Speicherzonenconnectors

Bei der ausschließlichen Integration mit Speicherzonenconnectors verwenden Sie nicht die Verwaltungskonsole des Speicherzonencontrollers. Diese Schnittstelle erfordert ein Citrix Files-Administratorkonto, das für diese Lösung nicht notwendig ist. Durch Ausführen eines PowerShell-Skripts bereiten Sie den Speicherzonencontroller für den Einsatz ohne Citrix Files-Steuerungsebene vor. Das Skript führt folgende Schritte aus:

- Registrieren des aktuellen Speicherzonencontrollers als primären Speicherzonencontroller. Sie können später sekundäre Speicherzonencontroller zum primären Controller hinzufügen.

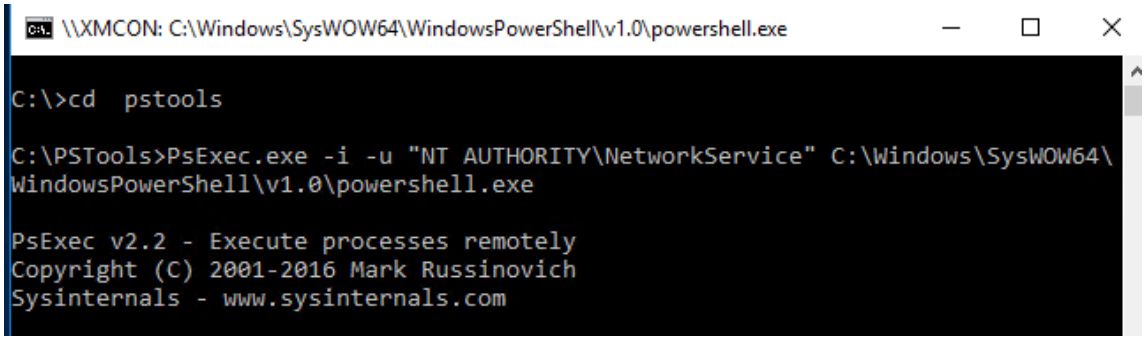
- Erstellen einer Zone und Festlegen der Passphrase.

1. Laden Sie vom StorageZone Controller-Server das Tool PsExec herunter: Navigieren Sie zu Microsoft Windows Sysinternals und klicken Sie auf **PsTools herunterladen**. Extrahieren Sie das Tool in das Stammverzeichnis von Laufwerk C.

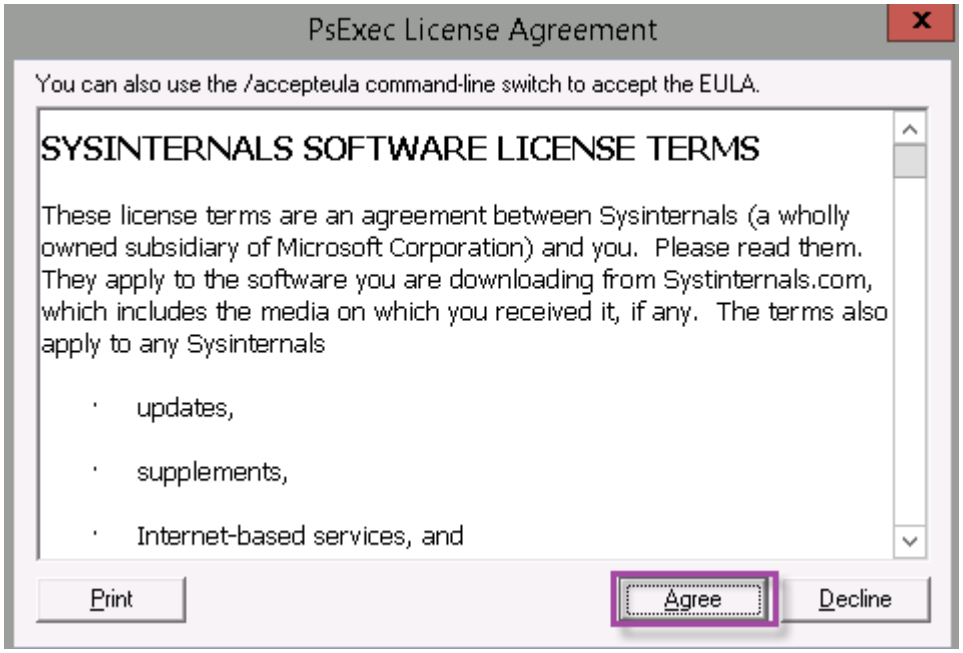


2. Führen Sie das Tool PsExec aus: Öffnen Sie die Eingabeaufforderung als Administrator und geben Sie Folgendes ein:

```
cd c:\pstools
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
<!--NeedCopy-->
```



3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Zustimmen**, um das Sysinternals-Tool auszuführen.



Ein PowerShell-Fenster wird geöffnet.

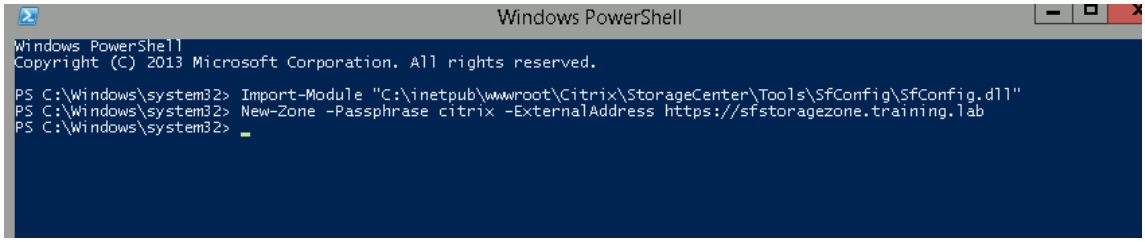
4. Geben Sie im PowerShell-Fenster Folgendes ein:

```
1 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll"
2 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
3 <!--NeedCopy-->
```

Wobei:

Passphrase: Passphrase, die Sie der Site zuweisen möchten. Machen Sie eine Notiz davon. Sie können die Passphrase nicht über den Controller wiederherstellen. Bei einem Verlust der Passphrase können Sie Speicherzonen nicht neu installieren, keine weiteren Speicherzonencontroller in die Speicherzone aufnehmen und die Speicherzone nach einem Serverausfall nicht wiederherstellen.

ExternalAddress: Dies ist der externe vollqualifizierte Domänenname des Speicherzonencontroller-Servers.



Der primäre Speicherzonencontroller ist nun einsatzbereit.

Führen Sie gegebenenfalls die folgende Konfiguration aus, bevor Sie sich bei XenMobile anmelden, um Speicherzonenconnectors zu erstellen:

Festlegen eines Proxyservers für Speicherzonen

Konfiguration des Domänencontrollers, sodass er dem Speicherzonencontroller für die Delegierung vertraut

Anfügen eines sekundären Speicherzonencontrollers an eine Speicherzone

Informationen zum Erstellen von Speicherzonenconnectoren finden Sie unter Definieren von Speicherzonencontroller-Verbindungen in XenMobile.

Anfügen eines sekundären Speicherzonencontrollers an eine Speicherzone

Konfigurieren Sie eine Speicherzone mit hoher Verfügbarkeit durch Einbinden von mindestens zwei Speicherzonencontrollers. Um einer Zone einen sekundären Speicherzonencontroller hinzuzufügen, installieren Sie den Speicherzonencontroller auf einem zweiten Server. Verbinden Sie diesen Controller dann mit der Zone des primären Controllers.

1. Öffnen Sie ein PowerShell-Fenster auf dem Speicherzonencontroller-Server, den Sie mit dem primären Server verbinden möchten.
2. Geben Sie im PowerShell-Fenster Folgendes ein:

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

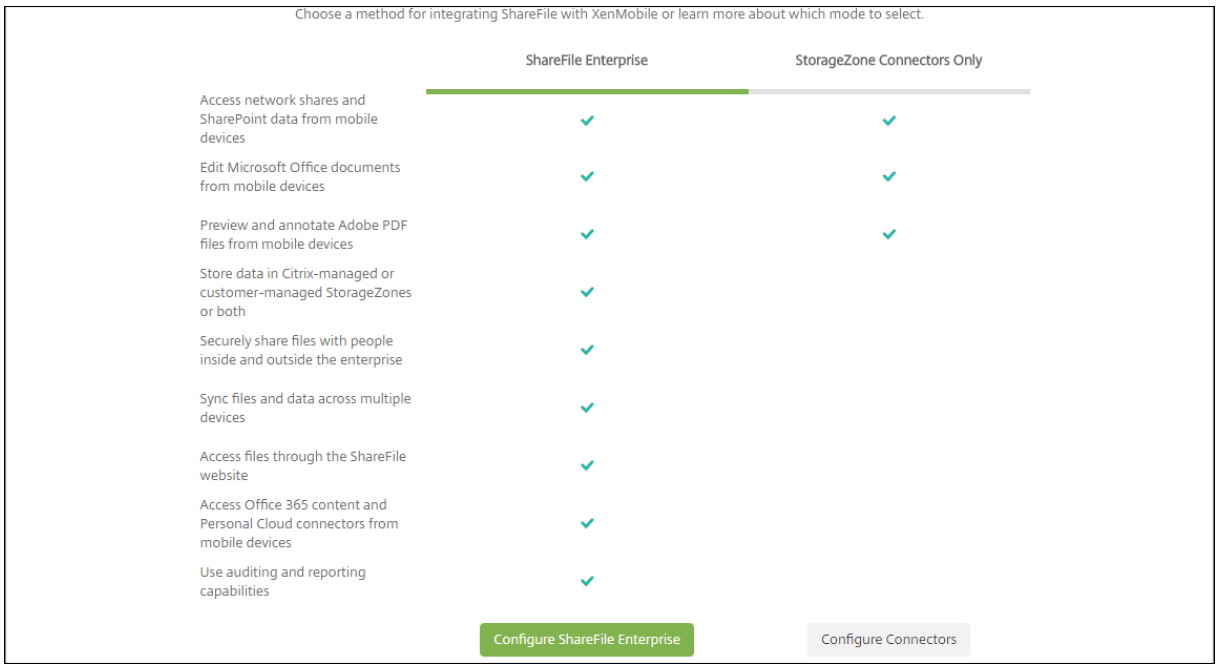
   Beispiel:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

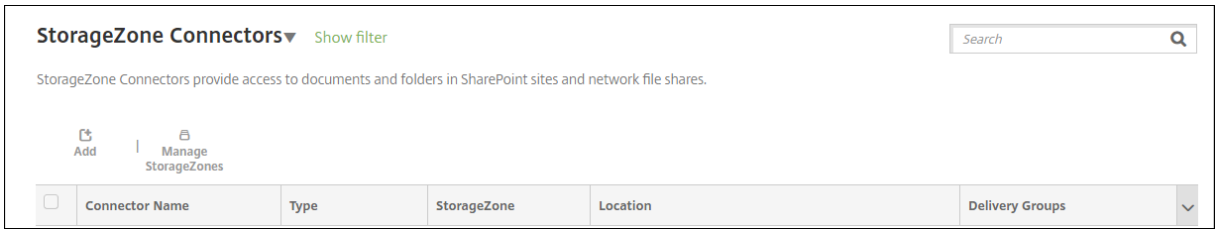
Definieren von Speicherzonencontroller-Verbindungen in XenMobile

Vor dem Hinzufügen von Speicherzonenconnectors konfigurieren Sie Verbindungsinformationen für jeden Speicherzonencontroller, der für Speicherzonenconnectors aktiviert ist. Sie können Speicherzonencontroller gemäß der Beschreibung in diesem Abschnitt oder beim Hinzufügen eines Connectors definieren.

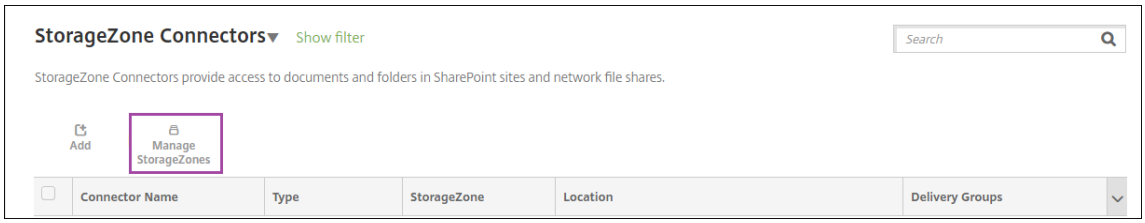
Beim ersten Aufrufen der Seite **Konfigurieren > ShareFile** werden dort die Unterschiede zwischen der Verwendung von XenMobile für Enterprise-Konten und Speicherzonenconnectors erläutert.



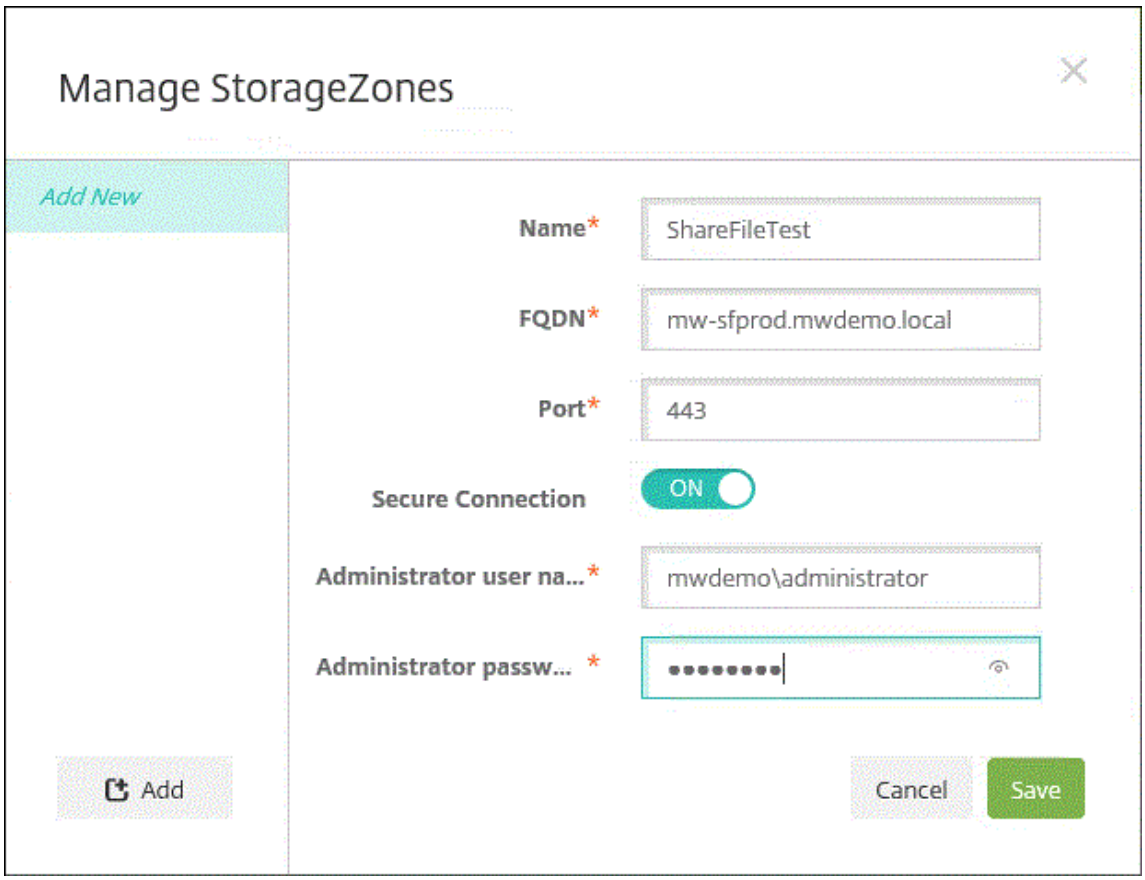
Klicken Sie auf **Connectors konfigurieren**, um mit den Konfigurationsschritten in diesem Artikel fortzufahren.



1. Klicken Sie unter **Konfigurieren > ShareFile** auf **StorageZones verwalten**.



2. Fügen Sie unter **StorageZones verwalten** die Verbindungsinformationen hinzu.



- **Name:** ein aussagekräftiger Name für die StorageZone, der zur Erkennung der StorageZone in XenMobile verwendet wird. Verwenden Sie kein Leerzeichen oder Sonderzeichen im Namen.
- **FQDN und Port:** der vollqualifizierte Domänenname und die Portnummer für den Speicherzonencontroller, der von XenMobile Server erreicht werden kann.
- **Sichere Verbindung:** Wenn Sie SSL für Verbindungen mit dem Speicherzonencontroller verwenden, wählen Sie die Standardeinstellung EIN. Wenn Sie SSL nicht für Verbindungen verwenden, ändern Sie diese Einstellung in AUS.
- **Administratorbenutzername** und **Administratorkennwort**: Benutzername (im Format "Domäne\Admin") und Kennwort des Dienstkontos des Administrators. Sie können auch ein Benutzerkonto mit Lese- und Schreibberechtigung für die Speicherzonencontroller verwenden.

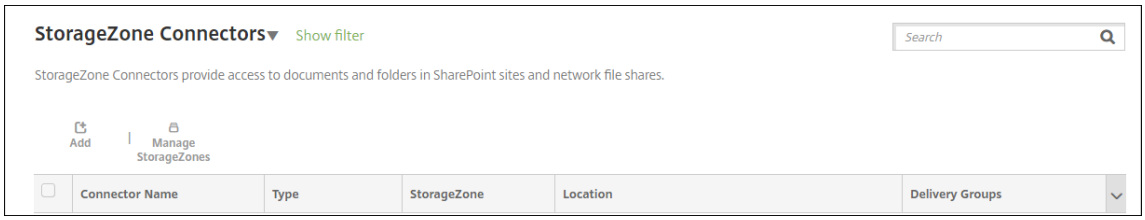
3. Klicken Sie auf **Speichern**.
4. Zum Testen der Verbindung stellen Sie sicher, dass XenMobile Server den vollqualifizierten Domänennamen des Speicherzonencontrollers auf Port 443 erreichen kann.
5. Klicken Sie zum Definieren einer weiteren Speicherzonencontroller-Verbindung unter **StorageZones verwalten** auf die Schaltfläche **Hinzufügen**.

   Zum Bearbeiten oder Löschen der Informationen für eine Speicherzonencontroller-Verbindung

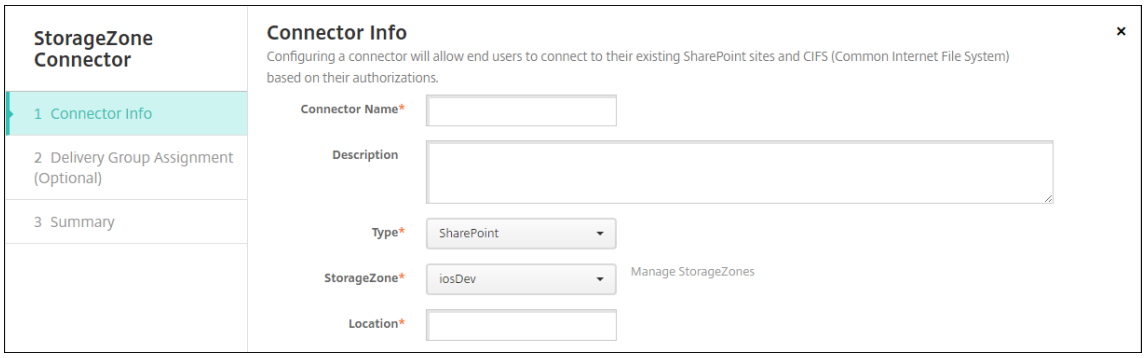
wählen Sie den Verbindungsnamen in **StorageZones verwalten** aus. Klicken Sie auf **Bearbeiten** oder **Löschen**.

Hinzufügen eines Speicherzonenconnectors in XenMobile

1. Gehen Sie zu **Konfigurieren > ShareFile** und klicken Sie dann auf **Hinzufügen**.

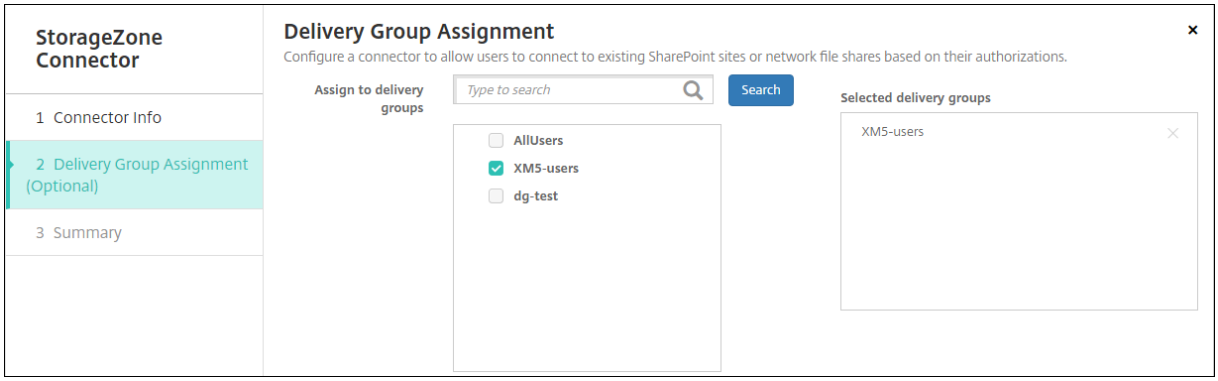


2. Konfigurieren Sie auf der Seite **Connectorinfo** die folgenden Einstellungen:



   - **Connectorname:** Name des Speicherzonenconnectors in XenMobile.
   - **Beschreibung:** optionale Anmerkungen zu diesem Connector.
   - **Typ:** Wählen Sie entweder **SharePoint** oder **Netzwerk** aus.
   - **StorageZone:** Wählen Sie die mit diesem Connector verbundene Speicherzone aus. Wenn die Speicherzone nicht aufgeführt wird, klicken Sie auf **StorageZones verwalten**, um den Speicherzonencontroller zu definieren.
   - **Speicherort:** Geben Sie für SharePoint die URL der SharePoint-Site auf Stammebene, der Site-Sammlung oder der Dokumentbibliothek im Format `https://sharepoint.company.com` an. Geben Sie für eine Netzwerkfreigabe den vollständig qualifizierten Domänennamen des UNC-Pfads (Uniform Naming Convention) im Format \\server\share an.

3. Weisen Sie den Connector auf der Seite **Bereitstellungsgruppenzuweisung** optional Bereitstellungsgruppen zu. Alternativ können Sie Connectors mithilfe von **Konfigurieren > Bereitstellungsgruppen** zu Bereitstellungsgruppen zuweisen.



1. Auf der Seite **Zusammenfassung** können Sie die konfigurierten Optionen überprüfen. Klicken Sie zum Anpassen der Konfiguration auf **Zurück**.
2. Klicken Sie auf **Speichern**, um den Connector zu speichern.
3. Testen Sie den Connector:

    a) Beim Umschließen der Citrix Files-Clients führen Sie folgende Schritte aus:

    - Legen Sie die Netzwerkzugriffsrichtlinie auf **Tunnel zum internen Netzwerk** fest.

    In diesem Betriebsmodus wird der gesamte Netzwerkverkehr, der vom Citrix Files-Client ausgeht, durch das MDX Framework von XenMobile abgefangen. Mit einem app-spezifischen Micro-VPN wird der Datenverkehr über Citrix Gateway umgeleitet.

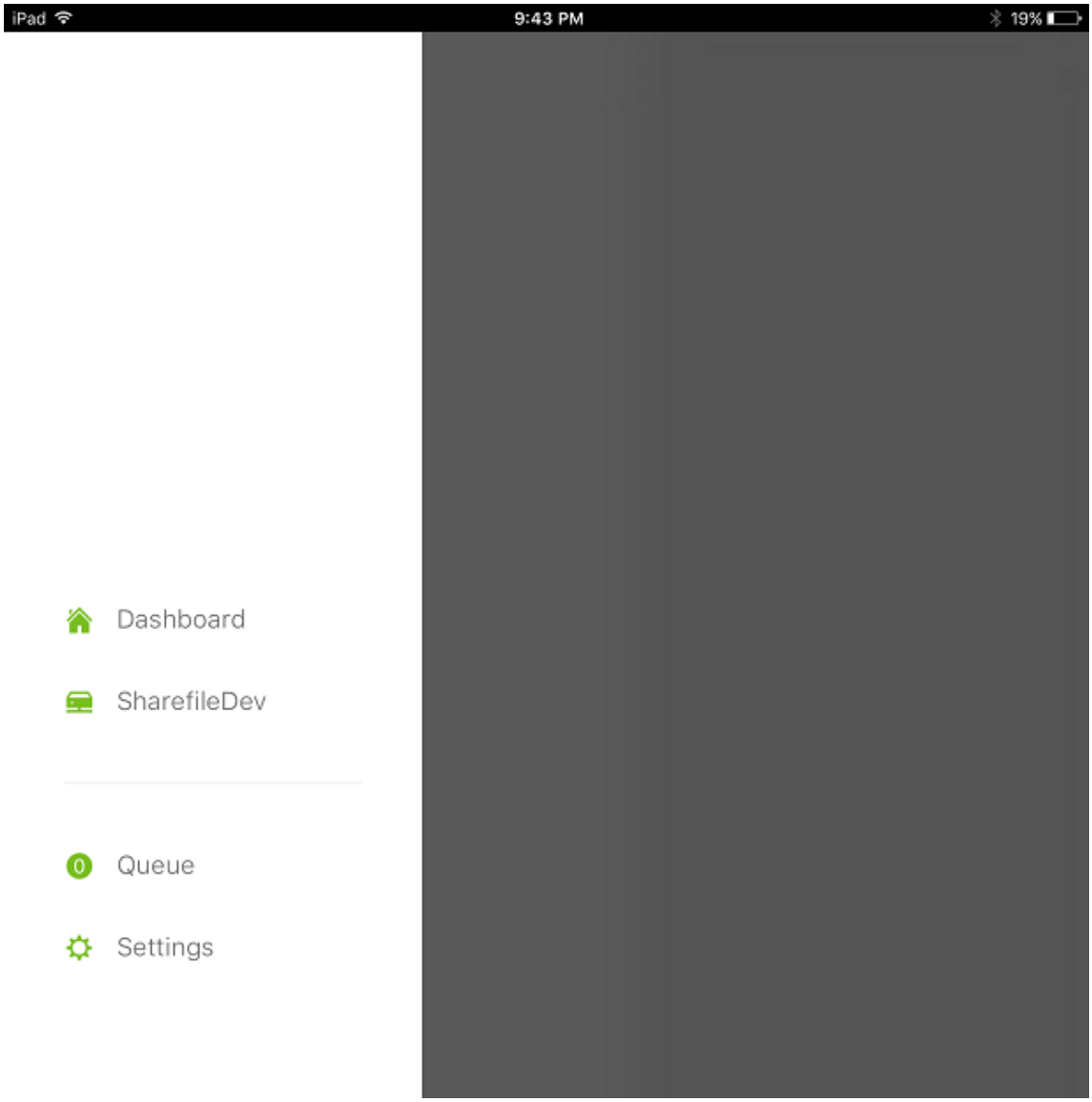
    - Legen Sie die Richtlinie “Bevorzugter VPN-Modus” auf **Tunnel - Web-SSO** fest.

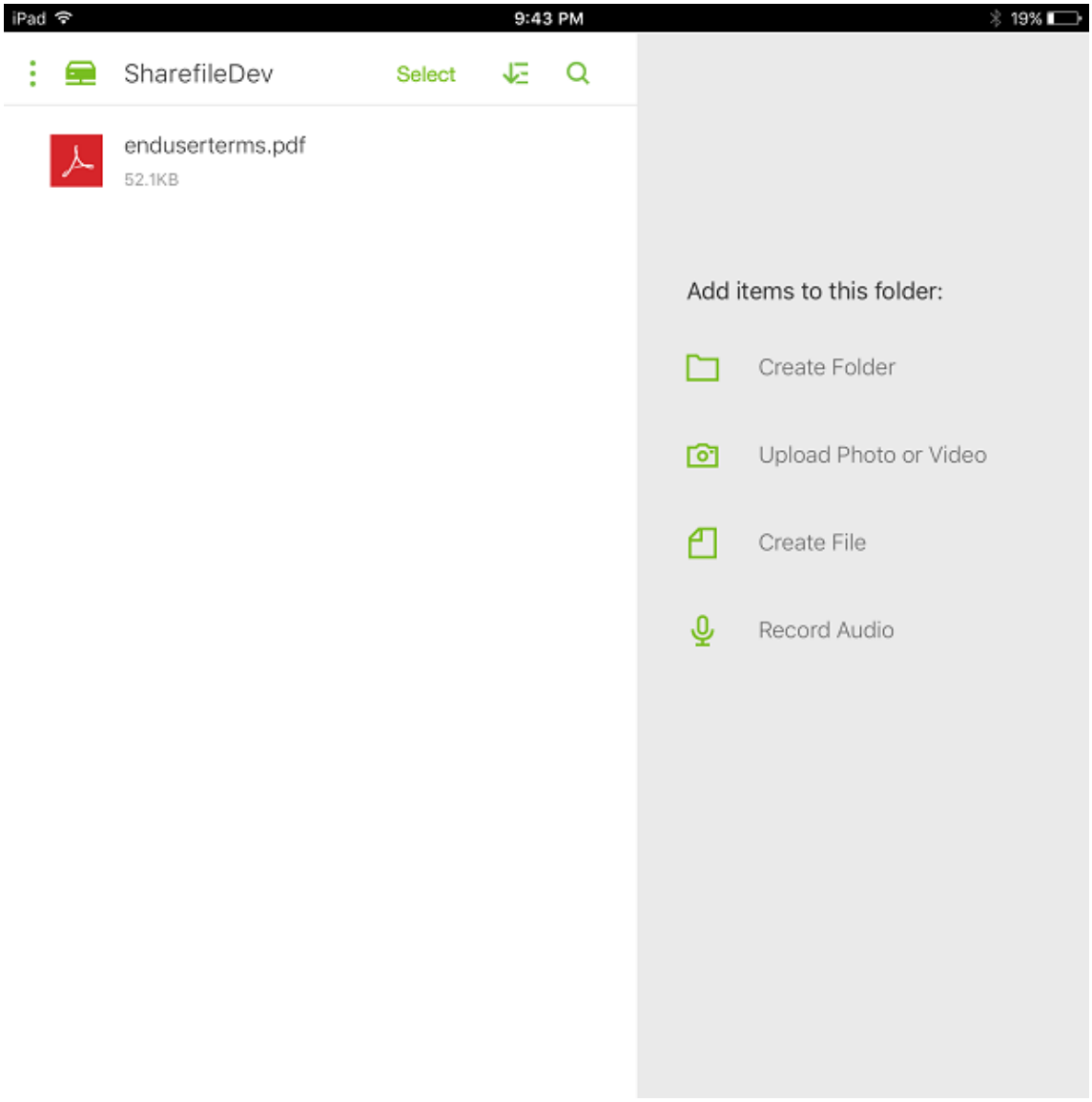
    In diesem Tunnelmodus beendet das MDX Framework den SSL/HTTP-Datenverkehr von einer MDX-App und initiiert für den Benutzer neue Verbindungen zu internen Verbindungen. Mit dieser Einstellung kann das MDX Framework Authentifizierungsaufforderungen von Webservern erkennen und darauf reagieren.

    b) Fügen Sie die Citrix Files-Clients zu XenMobile hinzu. Weitere Informationen finden Sie unter Integration und Bereitstellung von Citrix Files für Endpoint Management-Clients.

    c) Überprüfen Sie von einem unterstützten Gerät die Authentifizierung per Single Sign-On bei Citrix Files und Connectors.

In der folgenden Beispielen ist SharefileDev der Name eines Connectors.

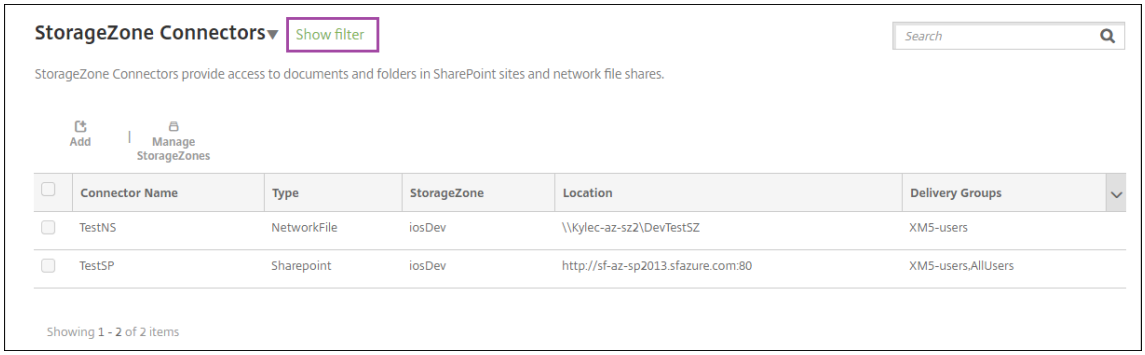




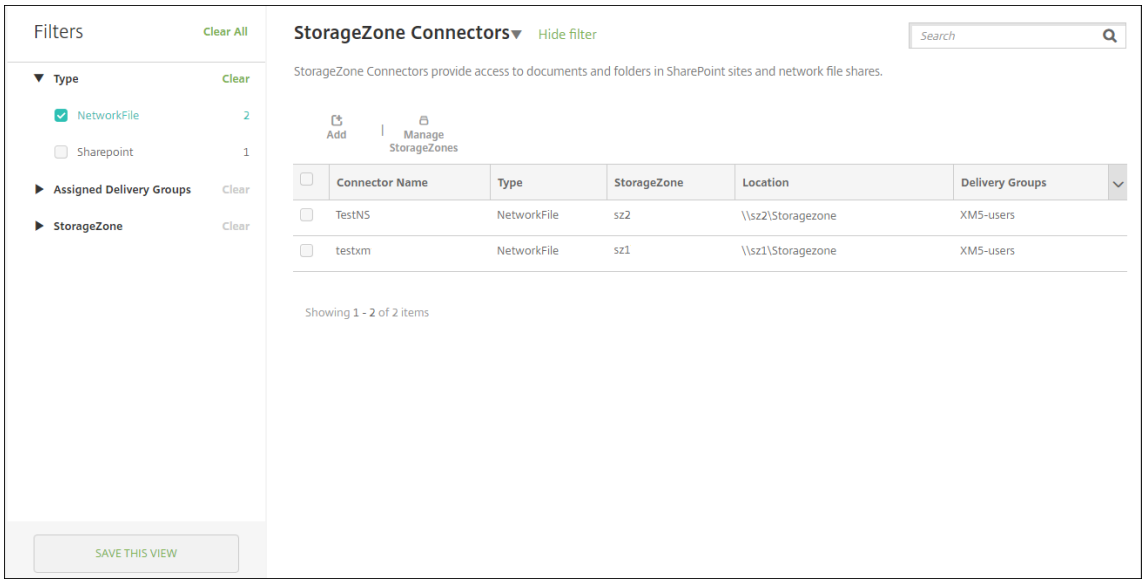
Filtern der Speicherzonenconnectors-Liste

Sie können die Liste der Speicherzonenconnectors nach Connector-Typ, zugewiesenen Bereitstellungsgruppen und Speicherzone filtern.

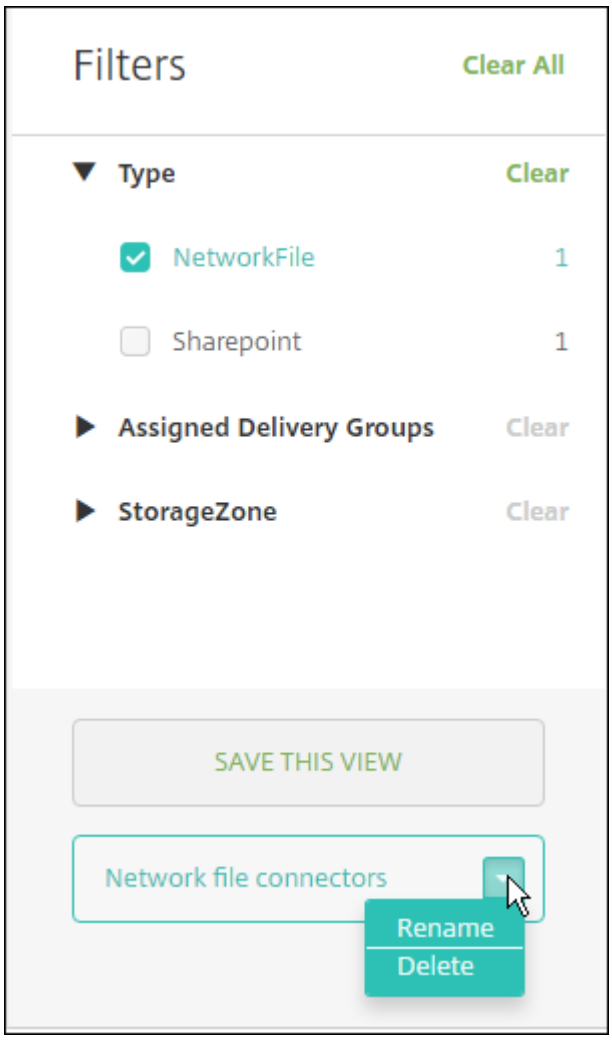
1. Wechseln Sie zu **Konfigurieren > ShareFile** und klicken Sie dann auf **Filter einblenden**.



2. Erweitern Sie die Filterüberschriften, um eine Auswahl zu treffen. Klicken Sie zum Speichern eines Filters auf **Diese Ansicht speichern**, geben Sie den Filternamen ein und klicken Sie auf **Speichern**.



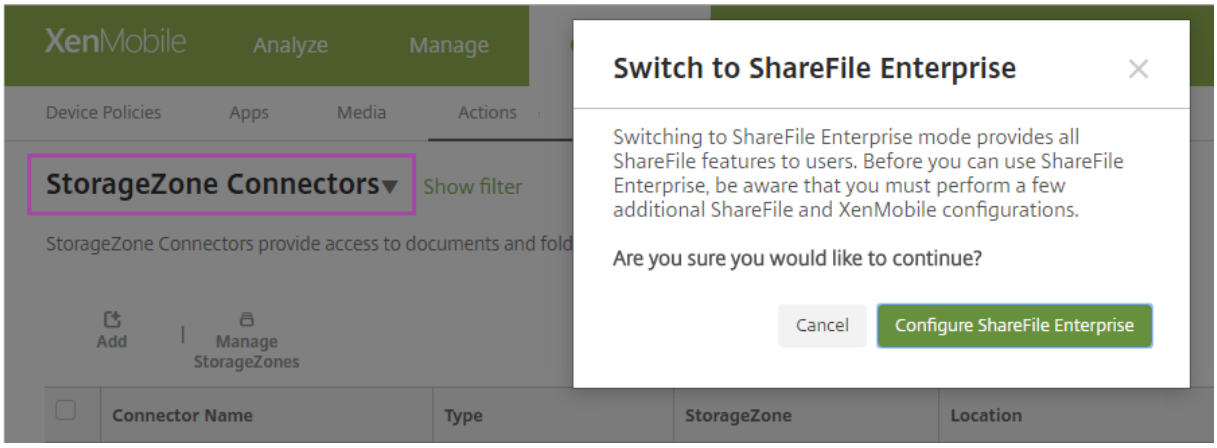
3. Klicken Sie zum Umbenennen oder Löschen eines Filters auf das Pfeilsymbol neben dem Filternamen.



Zu Citrix Files wechseln

Nach der Integration von Speicherzonenconnectors in XenMobile können Sie später zum gesamten Enterprise-Featuresatz wechseln. Die Verwendung des Citrix Files-Featuresatzes erfordert XenMobile Enterprise Edition. XenMobile behält die vorhandenen Integrationseinstellungen für Speicherzonenconnectors bei.

Wechseln Sie zu **Konfigurieren > ShareFile**, klicken Sie auf das Dropdownmenü **StorageZone Connectors** und klicken Sie dann auf **ShareFile Enterprise konfigurieren**.



Informationen zur Konfiguration von Citrix Files finden Sie unter SAML für Single Sign-On mit Citrix Files.

SmartAccess für HDX-Apps

January 5, 2022

Mit dieser Funktion können Sie den Zugriff auf HDX-Apps basierend auf den Geräteeigenschaften, den Benutzereigenschaften eines Geräts oder den auf einem Gerät installierten Anwendungen steuern. Mit dieser Funktion richten Sie automatisierte Aktionen ein, um das Gerät als nicht richtlinientreu zu markieren und diesem Gerät den Zugriff zu verweigern. HDX-Apps, die mit dieser Funktion verwendet werden, werden in Virtual Apps and Desktops anhand einer SmartAccess-Richtlinie konfiguriert, die nicht richtlinientreuen Geräten den Zugriff verweigert. XenMobile überträgt den Status des Geräts anhand eines signierten verschlüsselten Tags an StoreFront. StoreFront gewährt oder verweigert dann den Zugriff entsprechend der Zugriffssteuerungsrichtlinie der App.

Für die Verwendung dieses Features muss die Bereitstellung folgende Komponenten umfassen:

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 oder 3.8
- Mit XenMobile Server konfigurierte aggregierte HDX-Apps von einem StoreFront-Server
- XenMobile Server mit SAML-Zertifikat für das Signieren und Verschlüsseln von Tags. Das gleiche Zertifikat ohne privaten Schlüssel wird auf StoreFront-Server hochgeladen.

Um diese Funktion verwenden zu können, gehen Sie wie folgt vor:

- Konfigurieren Sie das XenMobile Server-Zertifikat für den StoreFront-Store.
- Konfigurieren Sie mindestens eine Virtual Apps and Desktops-Bereitstellungsgruppe mit der erforderlichen SmartAccess-Richtlinie
- Legen Sie die automatisierte Aktion in XenMobile fest.

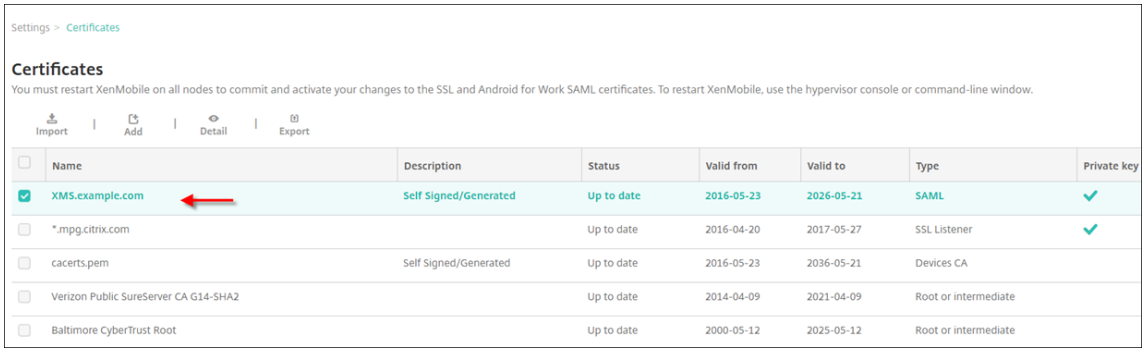
Exportieren und konfigurieren Sie das XenMobile-Serverzertifikat für den StoreFront-Store

SmartAccess verwendet signierte und verschlüsselte Tags für die Kommunikation zwischen XenMobile- und StoreFront-Servern. Um diese Kommunikation zu ermöglichen, fügen Sie das XenMobile Server-Zertifikat dem StoreFront-Store hinzu.

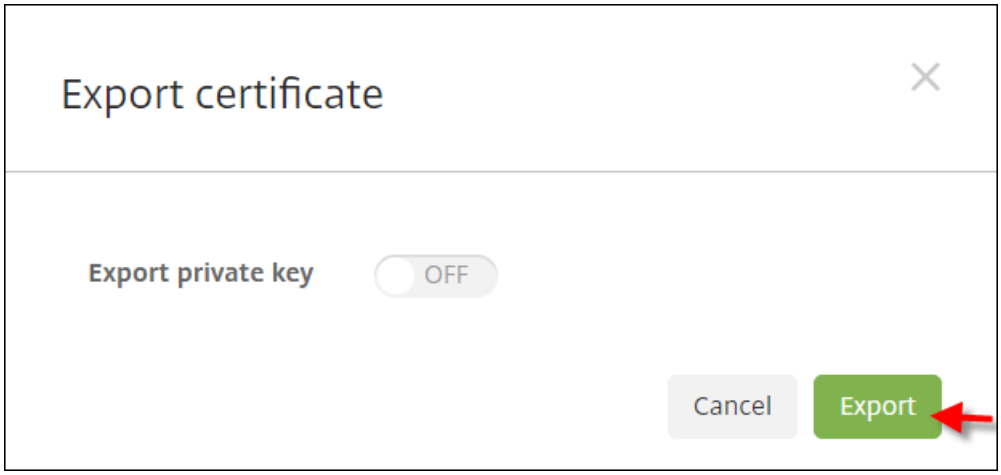
Weitere Informationen zur Integration von StoreFront in XenMobile, wenn für XenMobile die domänen- und zertifikatbasierte Authentifizierung konfiguriert ist, finden Sie im Support Knowledge Center.

Exportieren des SAML-Zertifikats von XenMobile Server

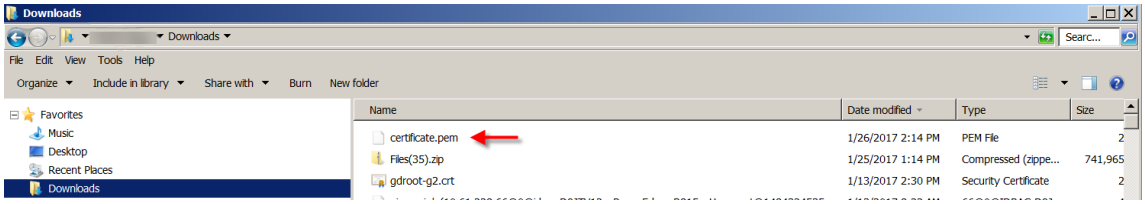
1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt. Klicken Sie auf **Zertifikate**.
2. Suchen Sie das SAML-Zertifikat für XenMobile Server.



3. Vergewissern Sie sich, dass **Privaten Schlüssel exportieren** auf **Aus** festgelegt ist. Klicken Sie auf **Exportieren**, um das Zertifikat in das Downloadverzeichnis zu exportieren.

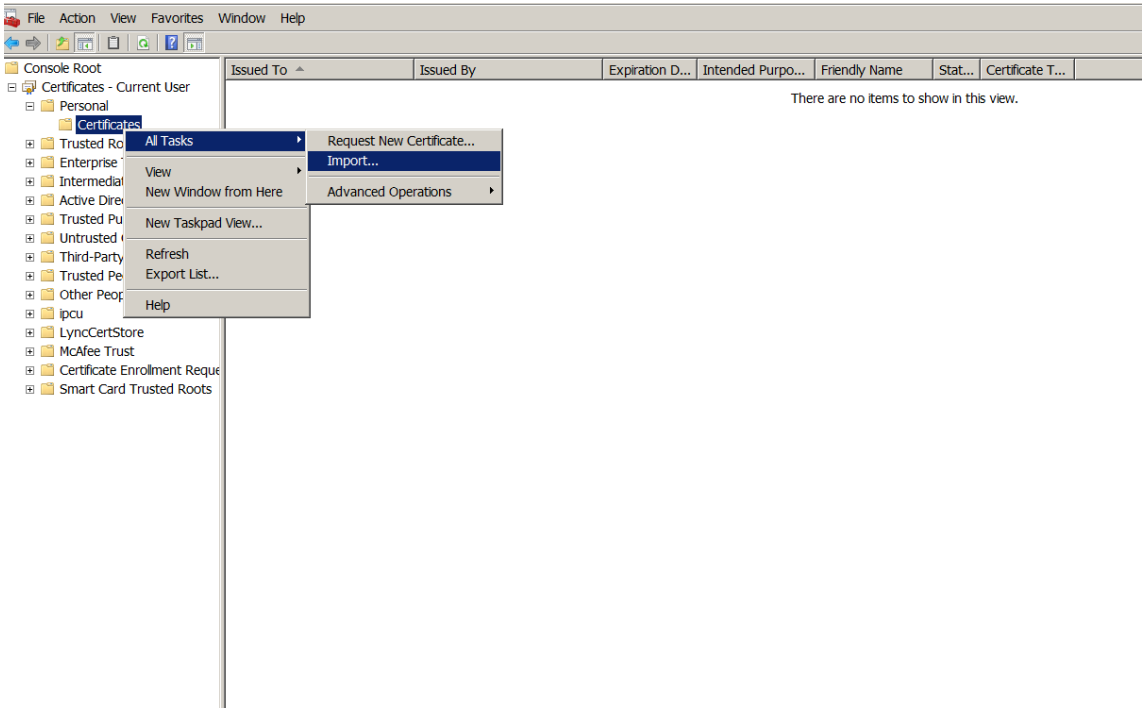


4. Suchen Sie das Zertifikat im Downloadverzeichnis. Das Zertifikat weist das PEM-Format auf.

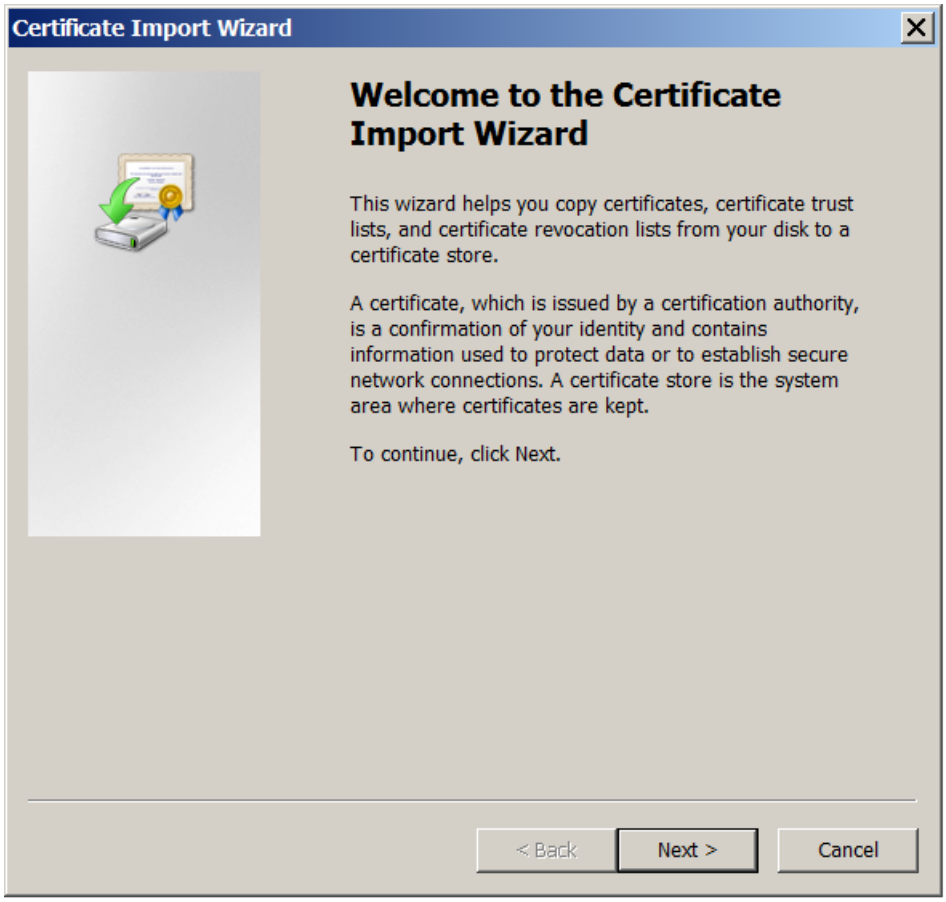


Konvertieren des Zertifikats von PEM in CER

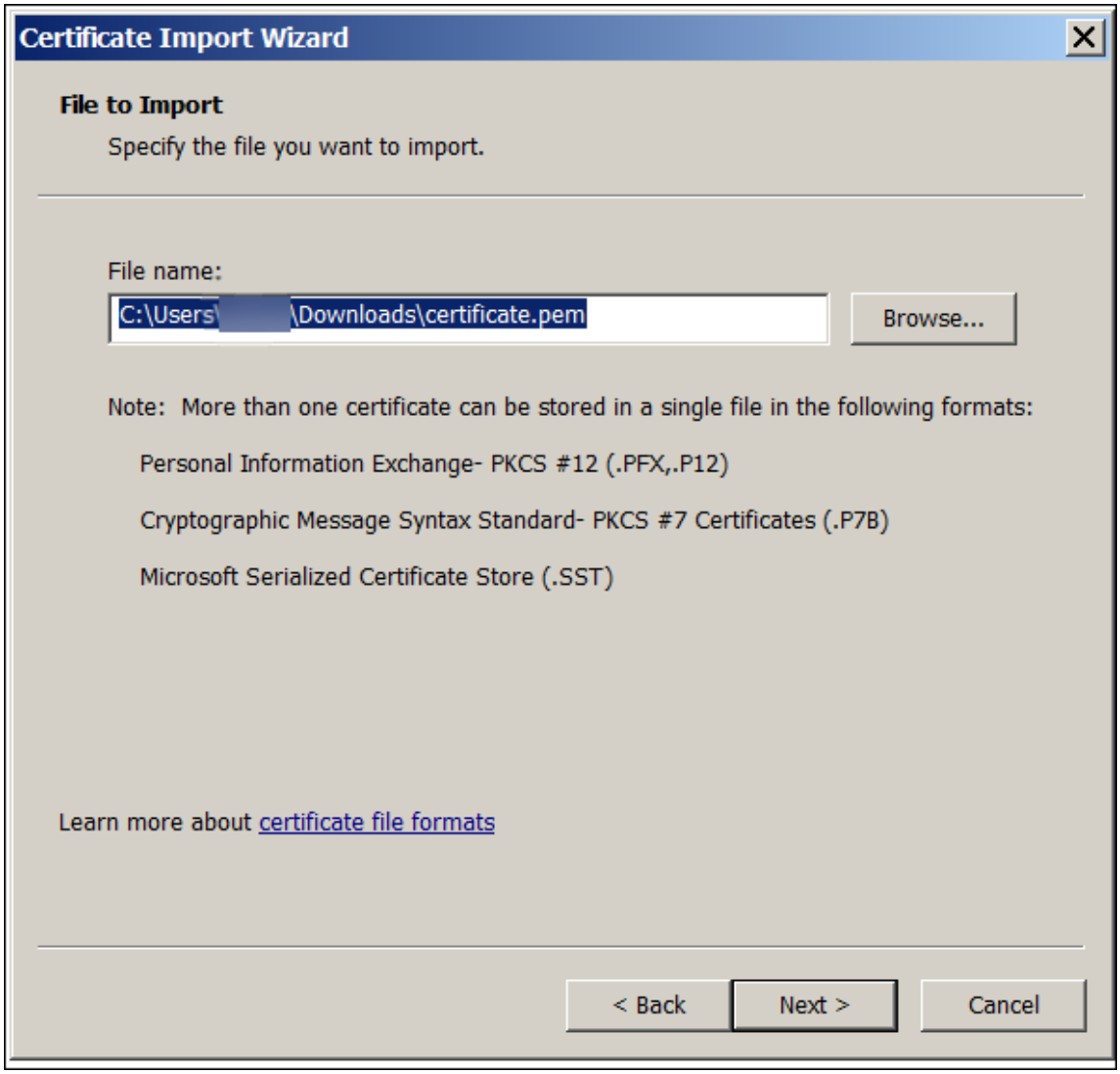
1. Öffnen Sie die Microsoft Management Console (MMC) und klicken Sie mit der rechten Maustaste auf **Zertifikate > Alle Aufgaben > Importieren**.



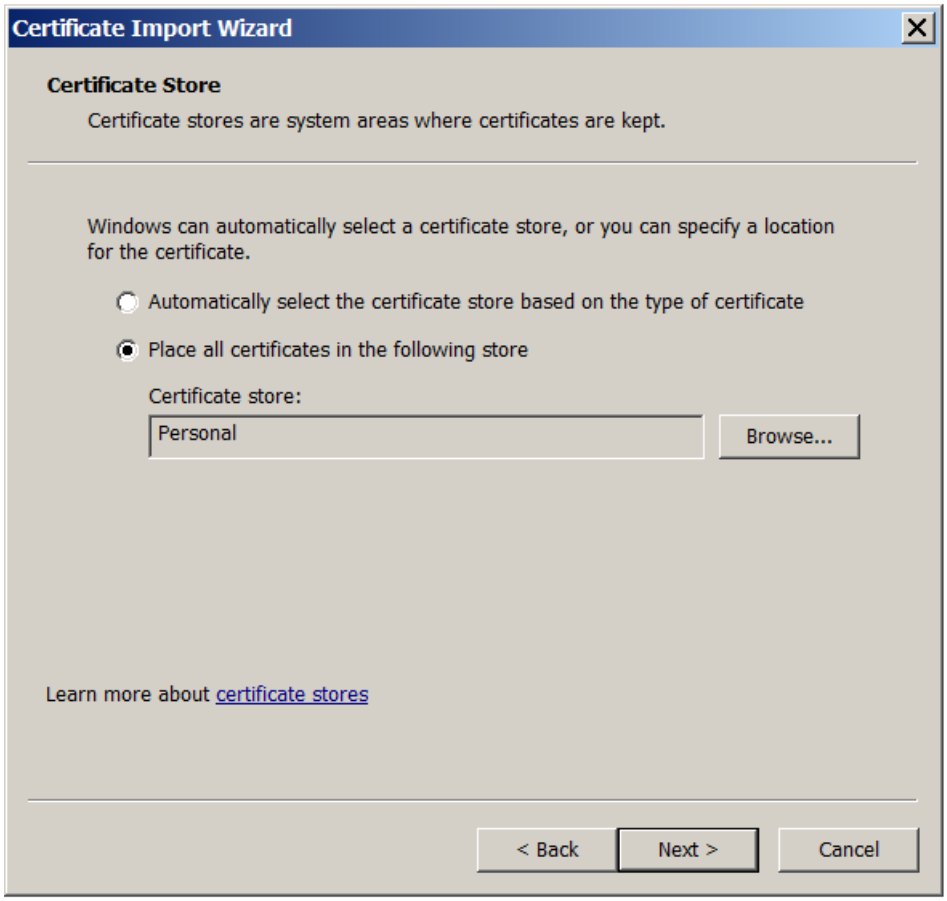
2. Wenn der Zertifikatimport-Assistent geöffnet wird, klicken Sie auf **Weiter**.



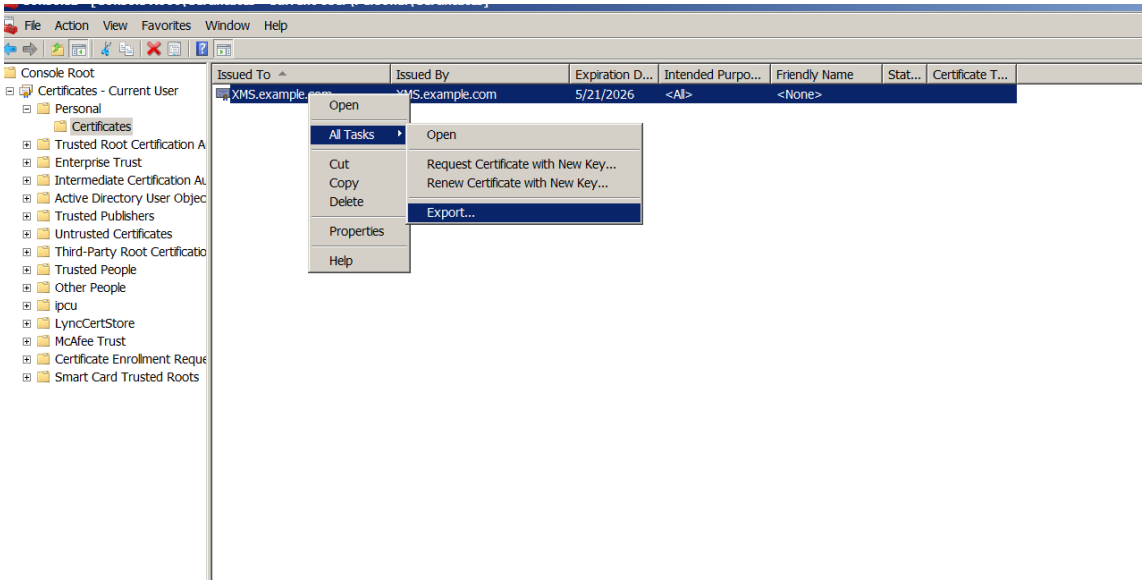
3. Navigieren Sie zum Zertifikat im Downloadverzeichnis.



4. Markieren Sie **Alle Zertifikate in folgendem Speicher speichern** und wählen Sie **Eigene Zertifikate** als Zertifikatspeicher. Klicken Sie auf **Weiter**.

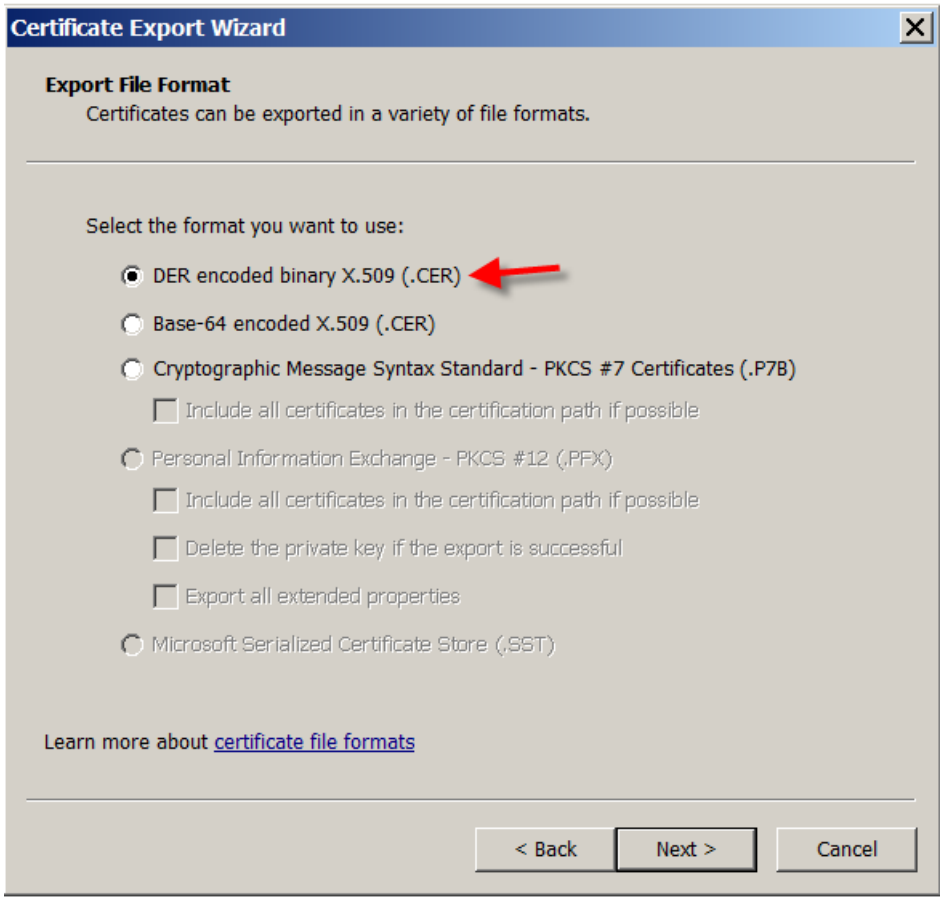


5. Überprüfen Sie Ihre Auswahl und klicken Sie auf **Fertig stellen**. Klicken Sie im Bestätigungsfenster auf **OK**.
6. Klicken Sie in der MMC mit der rechten Maustaste auf das Zertifikat und dann auf **Alle Aufgaben > Exportieren**.

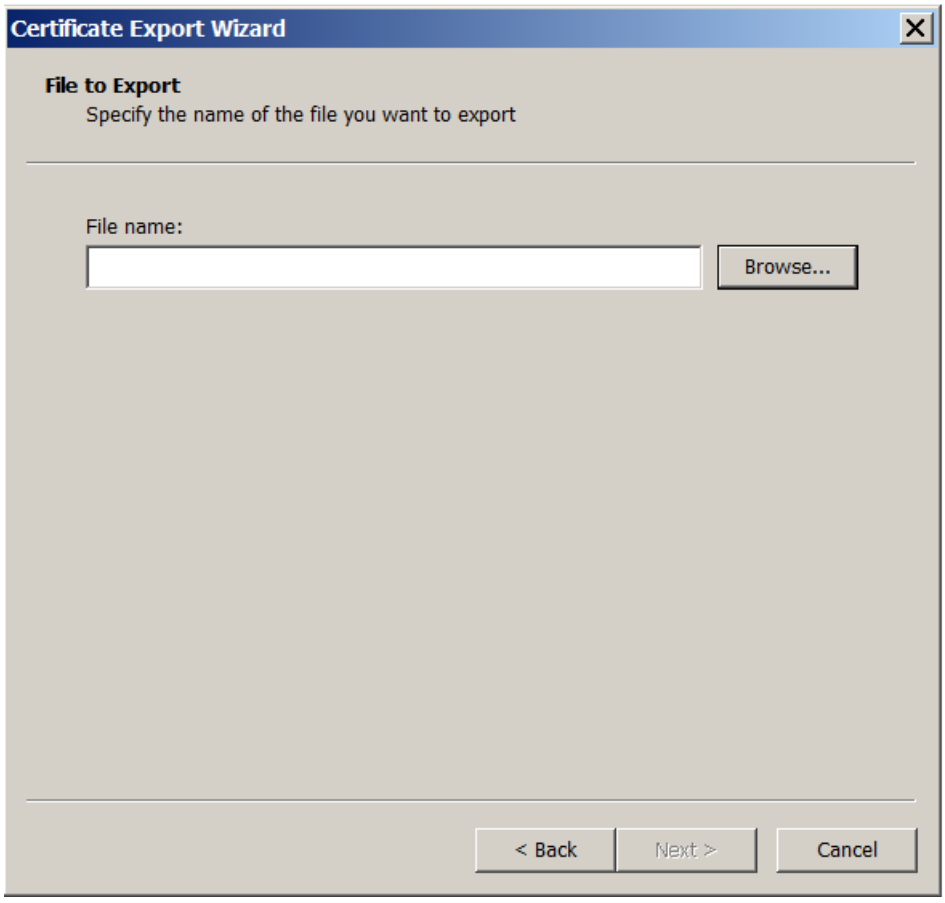


7. Wenn der Zertifikatexport-Assistent geöffnet wird, klicken Sie auf **Weiter**.

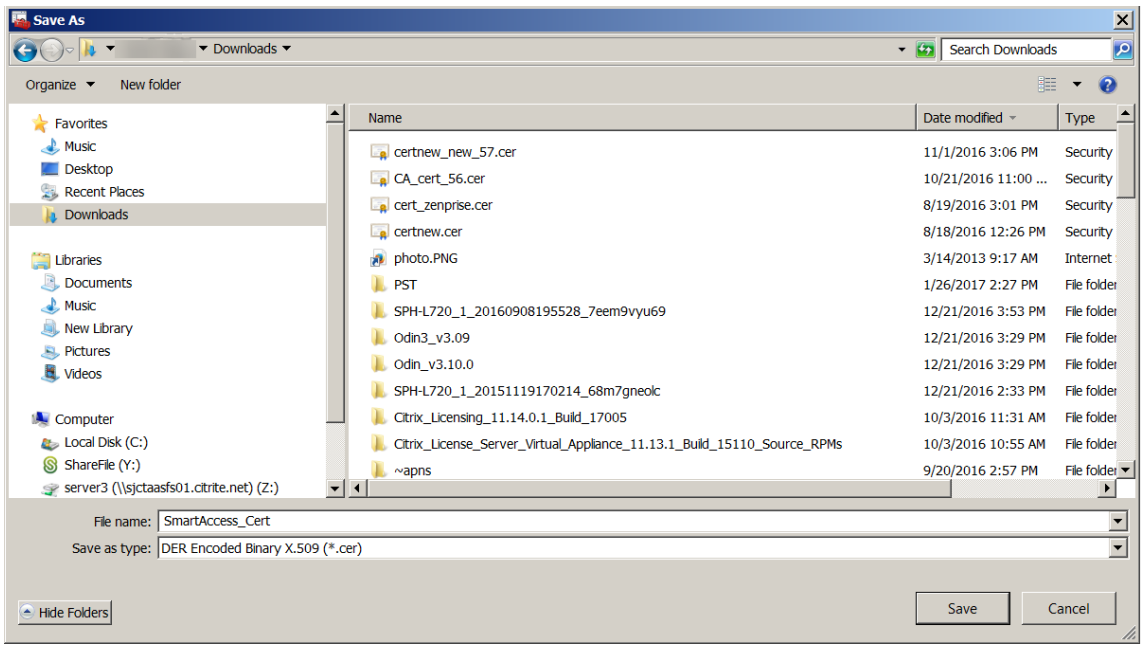
8. Wählen Sie das Format **DER-codiert-binär X.509 (.CER)**. Klicken Sie auf **Weiter**.



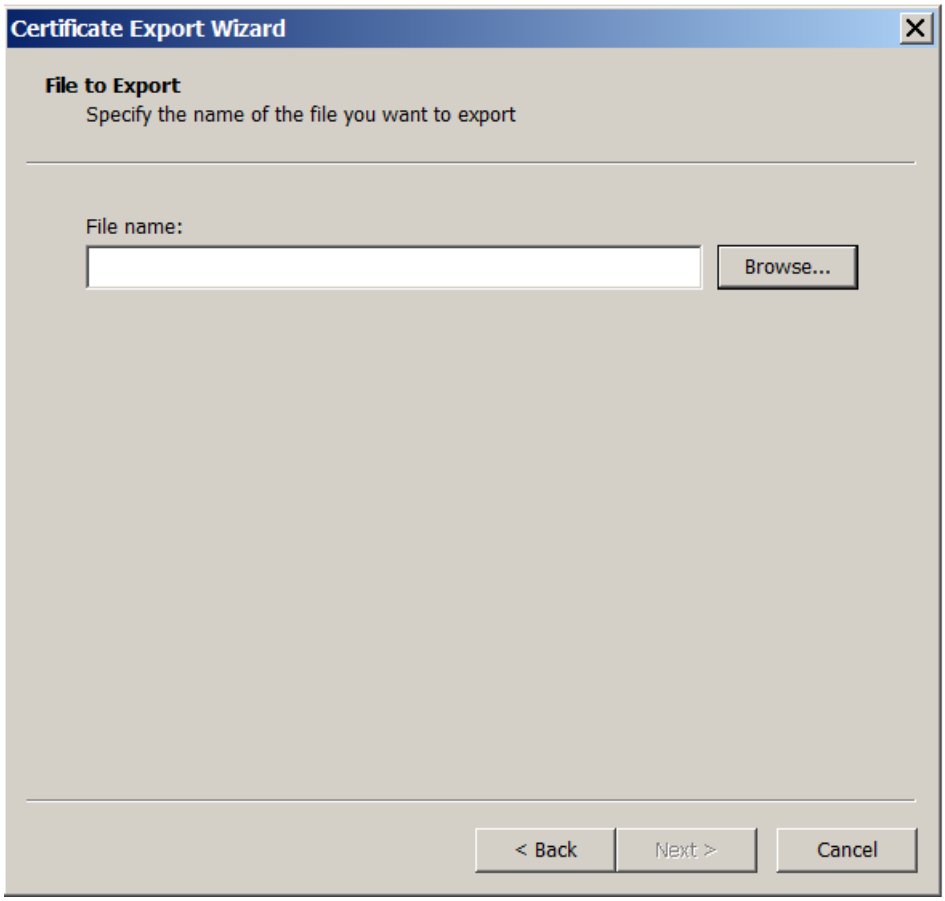
9. Navigieren Sie zu dem Zertifikat. Geben Sie einen Namen für das Zertifikat ein und klicken Sie auf **Weiter**.



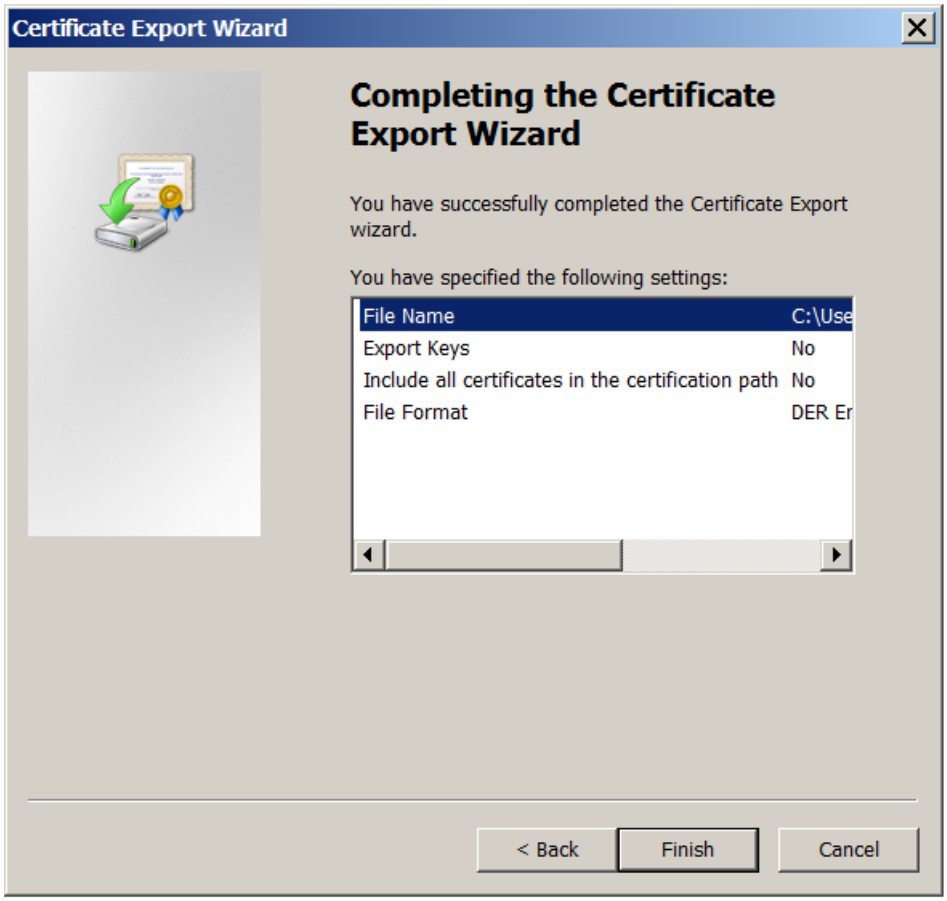
10. Speichern Sie das Zertifikat.



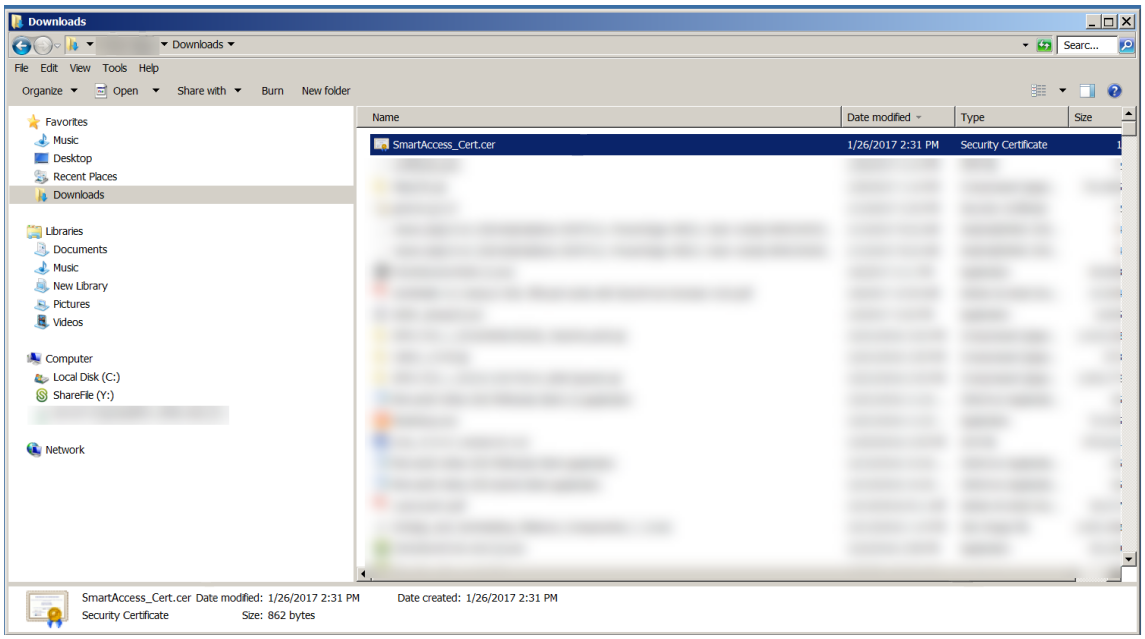
11. Navigieren Sie zu dem Zertifikat und klicken Sie auf **Weiter**.



12. Überprüfen Sie Ihre Auswahl und klicken Sie auf **Fertig stellen**. Klicken Sie im Bestätigungsfenster auf **OK**.

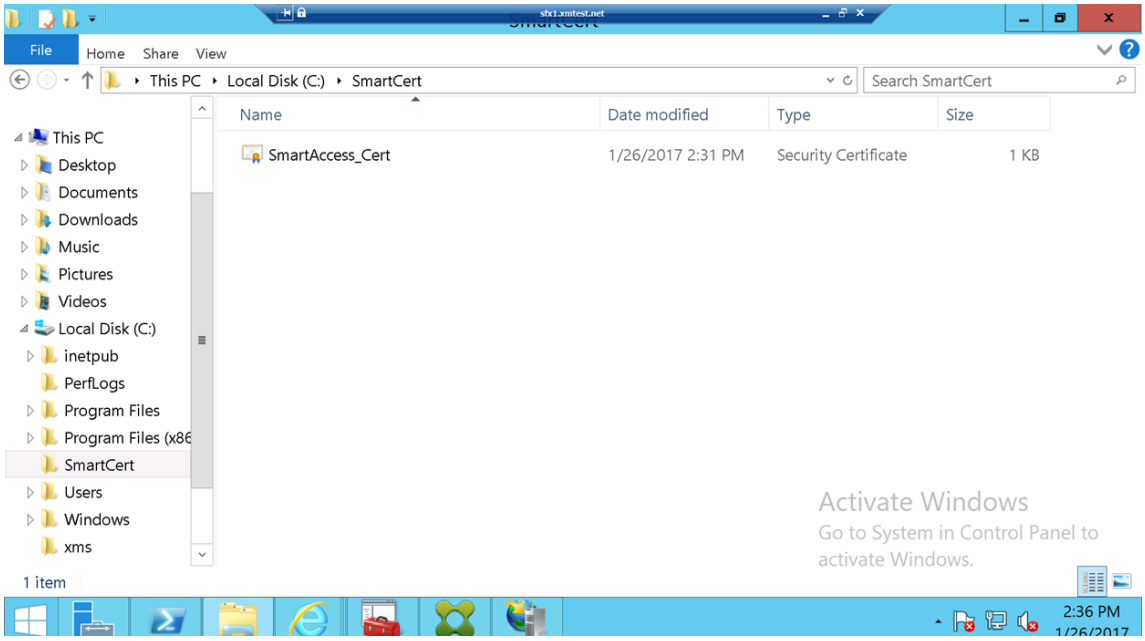


13. Suchen Sie das Zertifikat im Downloadverzeichnis. Beachten Sie, dass das Zertifikat im CER-Format vorliegt.



Kopieren Sie das Zertifikat auf den StoreFront-Server

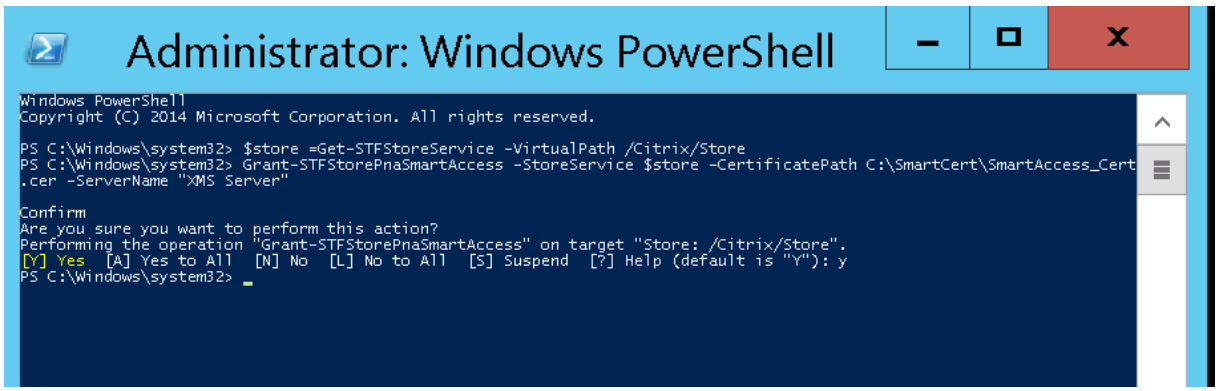
1. Erstellen Sie auf dem StoreFront-Server einen Ordner mit dem Namen **SmartCert**.
2. Kopieren Sie das Zertifikat in den Ordner **SmartCert**.



Konfigurieren des Zertifikats im StoreFront-Store

Führen Sie auf dem StoreFront-Server den folgenden PowerShell-Befehl aus, um das konvertierte XenMobile Server-Zertifikat im Store zu konfigurieren:

```
1    Grant-STFStorePnaSmartAccess -StoreService $store -
        CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
2  <!--NeedCopy-->
```



Wenn der StoreFront-Store vorhandene Zertifikate enthält, führen Sie folgenden PowerShell-Befehl aus, um sie zu widerrufen:


```
    Revoke-STFStorePnaSmartAccess  -StoreService $store  -All
<!--NeedCopy-->
```

Alternativ können Sie einen der folgenden PowerShell-Befehle auf dem StoreFront-Server ausführen, um vorhandene Zertifikate im StoreFront-Store zu widerrufen:

- Nach Name widerrufen:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -ServerName  "
       My XM Server"
<!--NeedCopy-->
```

- Nach Fingerabdruck widerrufen:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -
       CertificateThumbprint  "ReplaceWithThumbprint"
<!--NeedCopy-->
```

- Nach Serverobjekt widerrufen:

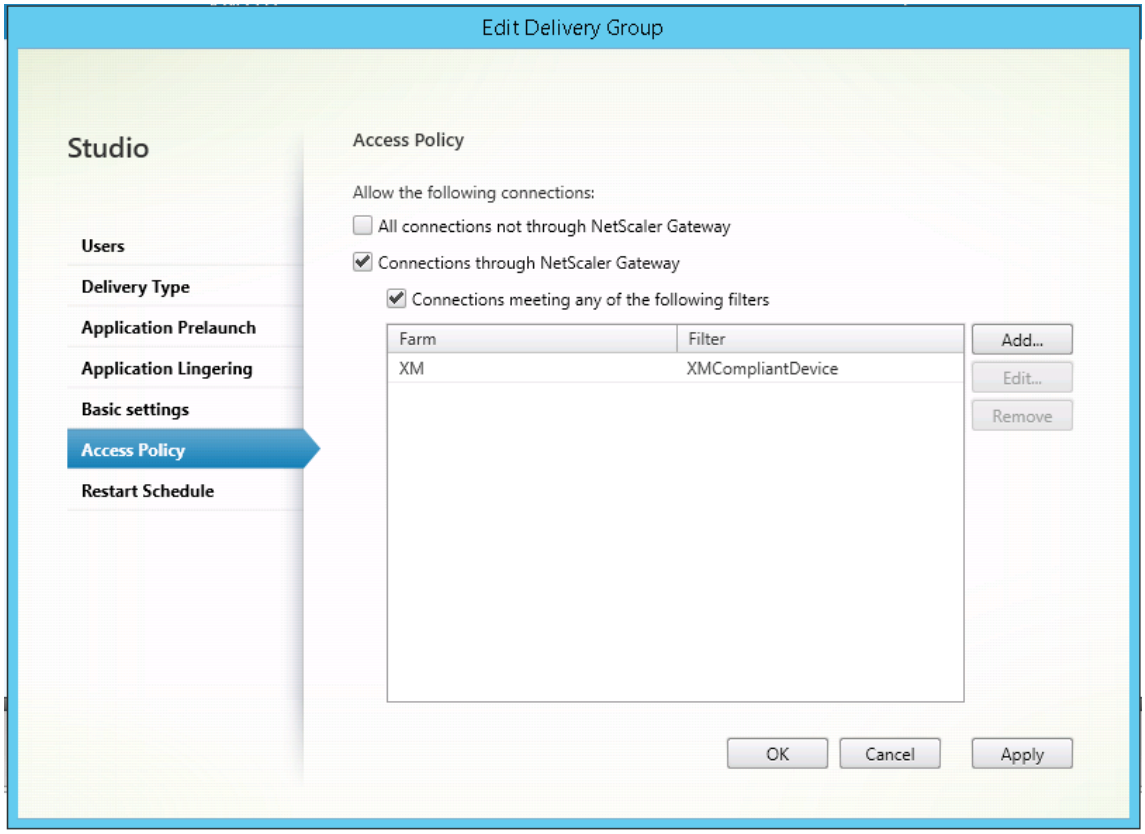
```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess  -StoreService $store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -SmartAccess
       $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

Konfigurieren der SmartAccess-Richtlinie für Virtual Apps and Desktops

Hinzufügen der erforderlichen SmartAccess-Richtlinie zur Bereitstellungsgruppe, die die HDX-App bereitstellt

1. Öffnen Sie auf dem Virtual Apps and Desktops-Server Citrix Studio.

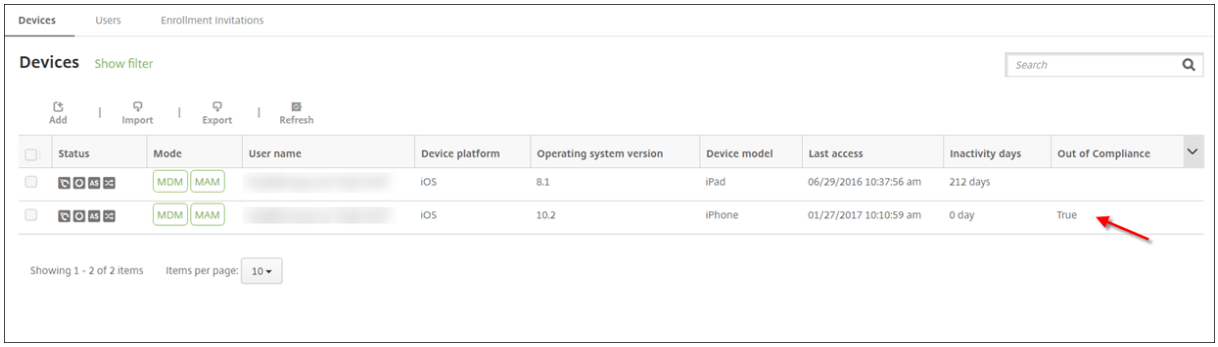
2. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
3. Wählen Sie eine Gruppe aus, die die App bzw. Apps bereitstellt und deren Zugriff Sie steuern möchten. Wählen Sie dann im Bereich **Aktion** die Option **Bereitstellungsgruppe bearbeiten** aus.
4. Wählen Sie auf der Seite **Zugriffsrichtlinie** die Optionen **Über NetScaler Gateway hergestellte Verbindungen** und **Verbindungen, auf die mindestens einer der folgenden Filter zutrifft** aus.
5. Klicken Sie auf **Hinzufügen**.
6. Fügen Sie eine Zugriffsrichtlinie hinzu, in der **Farm XM** und **Filter XMCompliantDevice** ist.



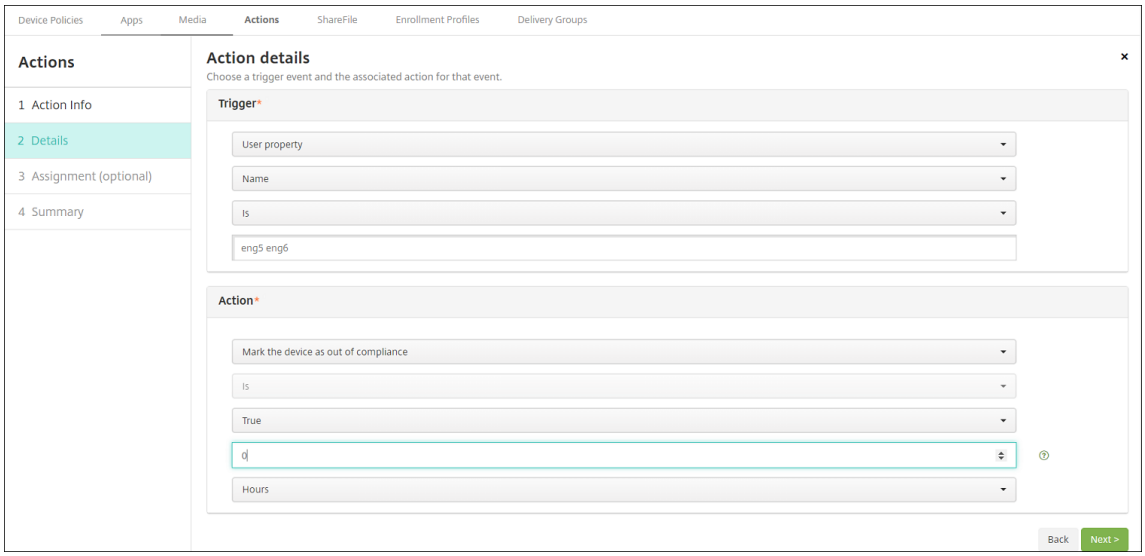
7. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Festlegen automatisierter Aktionen in XenMobile

Die SmartAccess-Richtlinie, die Sie in der Bereitstellungsgruppe für eine HDX-App festlegen, verweigert den Zugriff auf ein Gerät, wenn das Gerät nicht richtlinientreu ist. Verwenden Sie automatisierte Aktionen, um das Gerät als nicht richtlinientreu zu markieren.



1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Aktionen**. Die Seite **Aktionen** wird angezeigt.
2. Klicken Sie auf **Hinzufügen**, um eine Aktion hinzuzufügen. Die Seite **Aktionsinformationen** wird angezeigt.
3. Geben Sie auf der Seite **Aktionsinformationen** einen Namen und eine Beschreibung für die Aktion ein.
4. Klicken Sie auf **Weiter**. Die Seite **Aktionsdetails** wird angezeigt. Im folgenden Beispiel wird ein Auslöser erstellt, der Geräte sofort als nicht richtlinientreu markiert, wenn sie den Benutzereigenschaftsnamen **eng5** oder **eng6** aufweisen.



5. Wählen Sie in der Liste **Auslöser** die Option **Geräteeigenschaft**, **Benutzereigenschaft** oder **Name der installierten App** aus. SmartAccess unterstützt keine Ereignisauslöser.
6. Führen Sie in der Liste **Aktion** folgende Schritte aus:
   - Wählen Sie **Geräte als nicht richtlinientreu markieren**.
   - Wählen Sie **Ist**.
   - Wählen Sie **Wahr**.

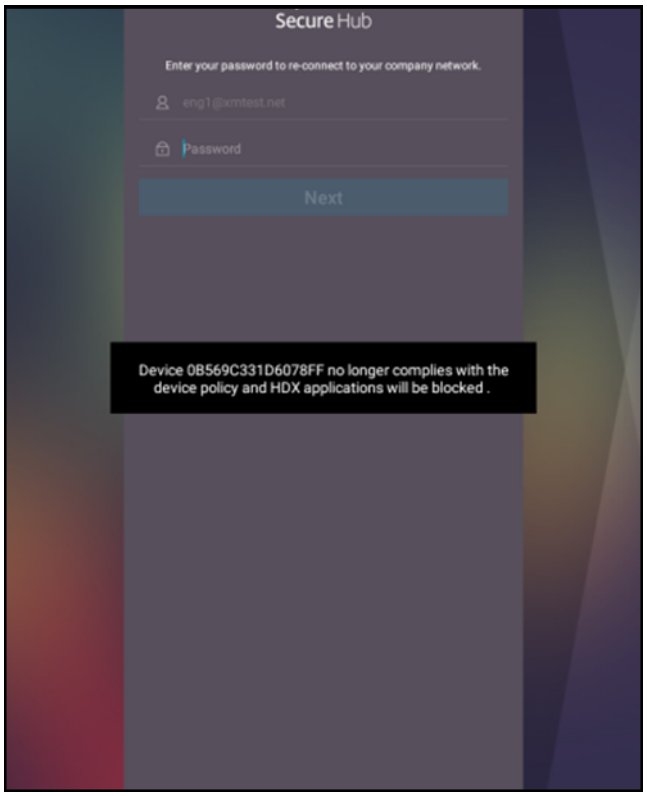
- Wenn das Gerät sofort bei Erfüllen der Auslösebedingung als nicht richtlinientreu markiert werden soll, legen Sie den Zeitrahmen auf **0** fest.

7. Wählen Sie die XenMobile-Bereitstellungsgruppe bzw. -gruppen aus, auf die diese Aktion angewendet werden soll.
8. Überprüfen Sie die Zusammenfassung der Aktion.
9. Klicken Sie auf **Weiter** und dann auf **Speichern**.

Wenn ein Gerät als nicht richtlinientreu markiert ist, werden die HDX-Apps nicht mehr im Secure Hub-Store angezeigt. Der Benutzer hat die Apps nicht mehr abonniert. Es wird keine Benachrichtigung an das Gerät gesendet, und nichts im Secure Hub-Store weist darauf hin, dass die HDX-Apps zuvor verfügbar waren.

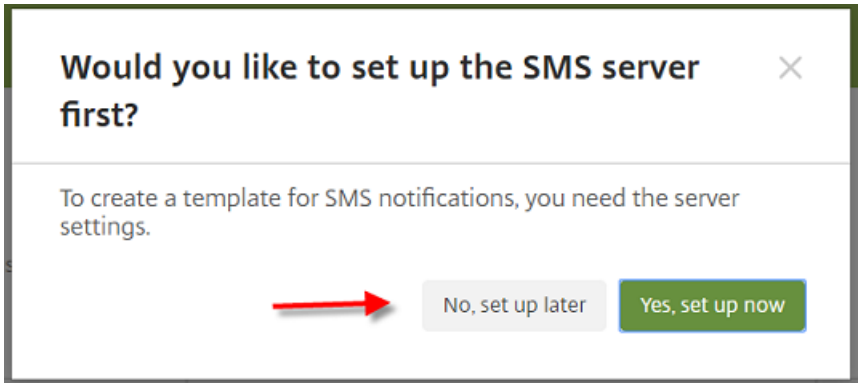
Wenn Sie möchten, dass Benutzer benachrichtigt werden, wenn ein Gerät als nicht richtlinientreu markiert wird, erstellen Sie eine Benachrichtigung und dann eine automatisierte Aktion zum Senden der Benachrichtigung.

In diesem Beispiel wird die folgende Benachrichtigung erstellt und gesendet, wenn ein Gerät als nicht richtlinientreu markiert wird: “Die Geräteseriennummer oder Telefonnummer erfüllt die Geräterichtlinie nicht mehr und HDX-Apps werden gesperrt.”

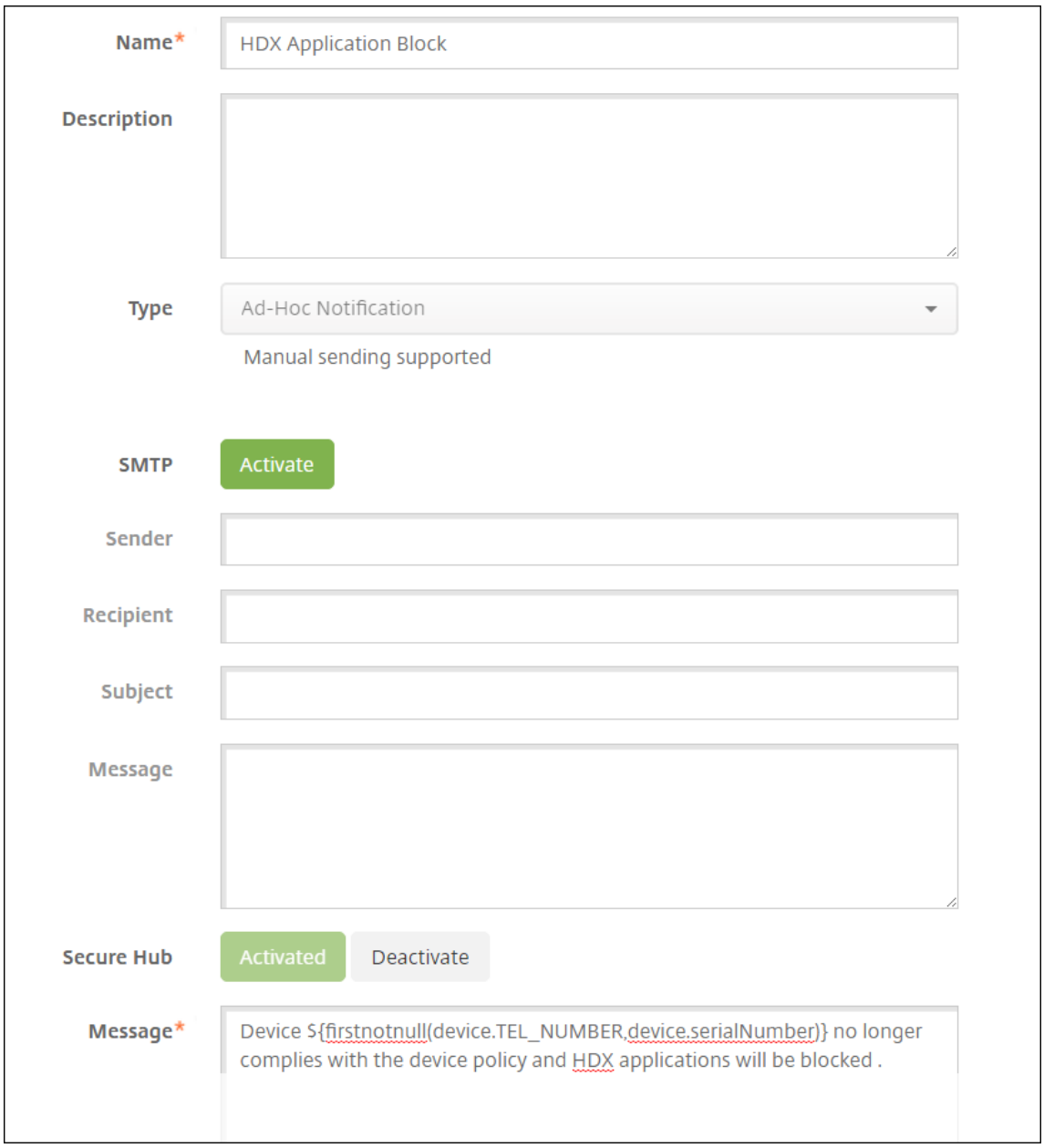


Erstellen der Benachrichtigung, die Benutzern angezeigt wird, wenn ein Gerät als nicht richtlinientreu markiert wird

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.
3. Klicken Sie auf **Hinzufügen**, um auf der Seite **Benachrichtigungsvorlagen** eine Vorlage hinzuzufügen.
4. Wenn Sie aufgefordert werden, zuerst den SMS-Server einzurichten, klicken Sie auf **Nein, später einrichten**.



5. Konfigurieren Sie folgende Einstellungen:
   - **Name:** HDX-Anwendungsblockierung
   - **Beschreibung:** Agent-Benachrichtigung, wenn das Gerät nicht richtlinientreu ist
   - **Typ:** Ad-Hoc-Benachrichtigung
   - **Secure Hub:** Aktiviert
   - **Nachricht:** Gerät ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} erfüllt die Geräterichtlinie nicht mehr und HDX-Apps werden gesperrt.

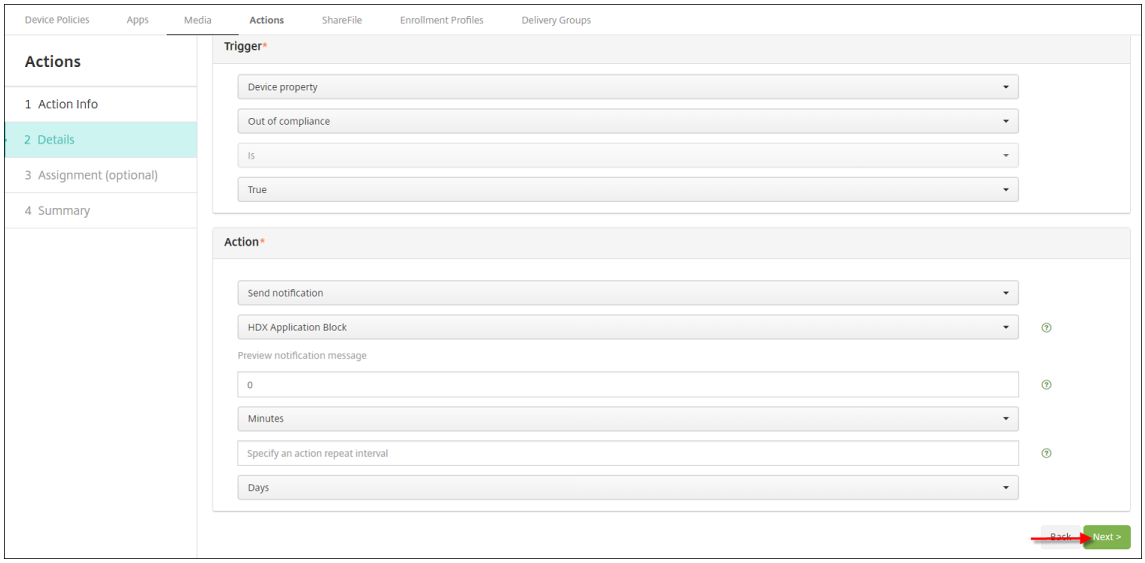


6. Klicken Sie auf **Speichern**.

Erstellen der Aktion, mit der die Benachrichtigung gesendet wird, wenn ein Gerät als nicht richtlinientreu markiert wird

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Aktionen**. Die Seite **Aktionen** wird angezeigt.
2. Klicken Sie auf **Hinzufügen**, um eine Aktion hinzuzufügen. Die Seite **Aktionsinformationen** wird angezeigt.

3. Geben Sie auf der Seite **Aktionsinformationen** einen Namen für die Aktion und optional eine Beschreibung ein.
    - **Name:** HDX blockiert Benachrichtigung
    - **Beschreibung:** HDX hat die Benachrichtigung gesperrt, weil das Gerät nicht richtlinientreu ist
4. Klicken Sie auf **Weiter**. Die Seite **Aktionsdetails** wird angezeigt.
5. In der Liste **Auslöser**:
    - Wählen Sie **Geräteeigenschaft** aus.
    - Wählen Sie **Nicht richtlinientreu**.
    - Wählen Sie **Ist**.
    - Wählen Sie **Wahr**.



6. Geben Sie in der Liste **Aktion** die Aktionen an, die ausgeführt werden, wenn die Auslösebedingung erfüllt ist:
    - Wählen Sie **Benachrichtigung senden** aus.
    - Wählen Sie die von Ihnen erstellte Benachrichtigung **HDX-Anwendungsblockierung**.
    - Wählen Sie **0**. Wenn der Wert auf 0 festgelegt ist, wird die Benachrichtigung sofort gesendet, sobald die Auslösebedingung erfüllt ist.
7. Wählen Sie die XenMobile-Bereitstellungsgruppe bzw. -gruppen aus, auf die diese Aktion angewendet werden soll. Wählen Sie in diesem Beispiel **AllUsers**.
8. Überprüfen Sie die Zusammenfassung der Aktion.
9. Klicken Sie auf **Weiter** und dann auf **Speichern**.

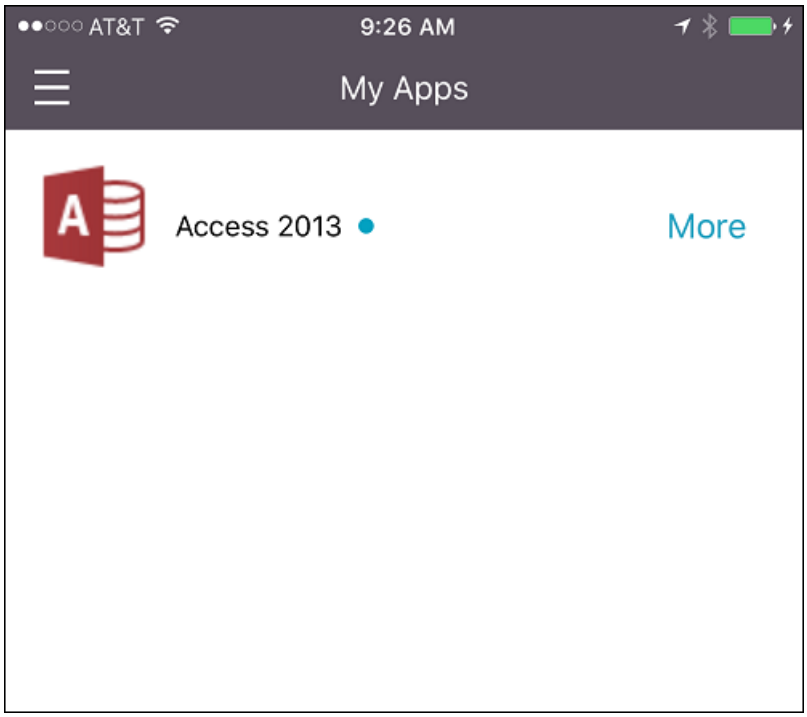
Details über das Festlegen von automatisierten Aktionen finden Sie unter Automatisierte Aktionen.

Zurückerhalten des Zugriffs auf HDX-Apps

Nachdem das Gerät wieder richtlinientreu ist, können Benutzer den Zugriff auf die HDX-Apps zurückerhalten:

1. Gehen Sie auf dem Gerät zu Secure Hub-Store, um die Apps im Store zu aktualisieren.
2. Gehen Sie zur App und tippen Sie auf **Hinzufügen** für die App.

Nach dem Hinzufügen der App wird sie unter “Eigene Apps” mit einem blauen Punkt angezeigt, da es sich um eine neu installierte App handelt.



Hinzufügen von Medien

December 14, 2020

Sie fügen Medien zu XenMobile hinzu, um sie auf Benutzergeräten zu verteilen. Mit XenMobile können Sie Apple-Bücher bereitstellen, die Sie über Apple Volume Purchase beschafft haben.

Nachdem Sie ein Volume Purchase-Konto in XenMobile eingerichtet haben, werden Ihre gekauften und kostenlosen Bücher unter **Konfigurieren > Medien** angezeigt. Über die Seiten unter **Medien** konfigurieren Sie Books für die Bereitstellung auf iOS-Geräten, indem Sie Bereitstellungsgruppen auswählen und Bereitstellungsregeln festlegen.

Wenn ein Benutzer das erste Mal ein Buch erhält und die Volume Purchase-Lizenz akzeptiert, werden bereitgestellte Bücher auf dem Gerät installiert. Die Bücher werden in Apple Books angezeigt. Sie kön-

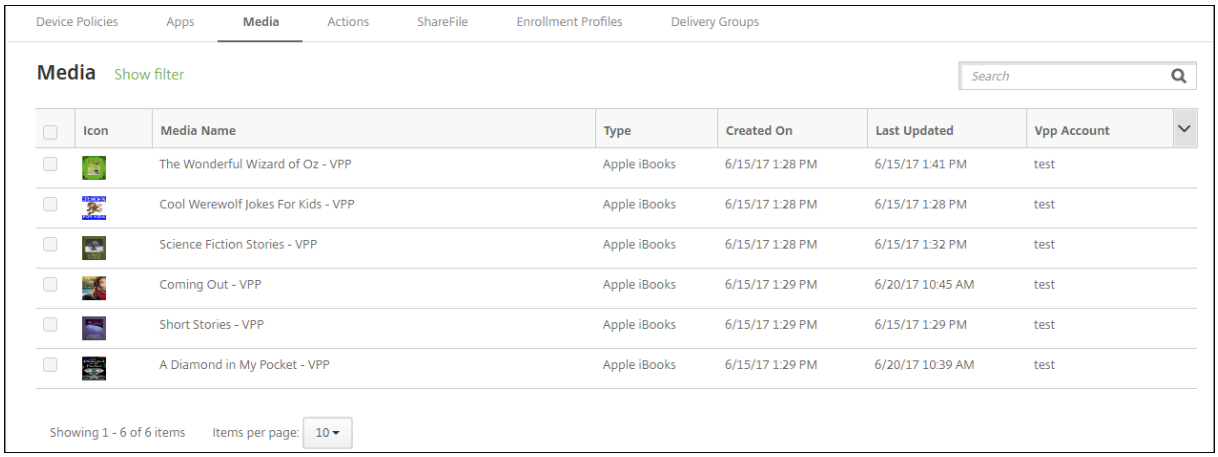
nen die Zuweisung zwischen Benutzer und Lizenz nicht aufheben und das Buch nicht vom Gerät entfernen. XenMobile installiert Bücher als erforderliche Medien. Wenn Benutzer ein installiertes Buch von dem Gerät löschen, bleibt es in Apple Books und kann von dort wieder heruntergeladen werden.

Voraussetzungen

- iOS-Geräte
- Konfigurieren Sie Apple Volume Purchase in XenMobile wie unter Apple Volume Purchase beschrieben.

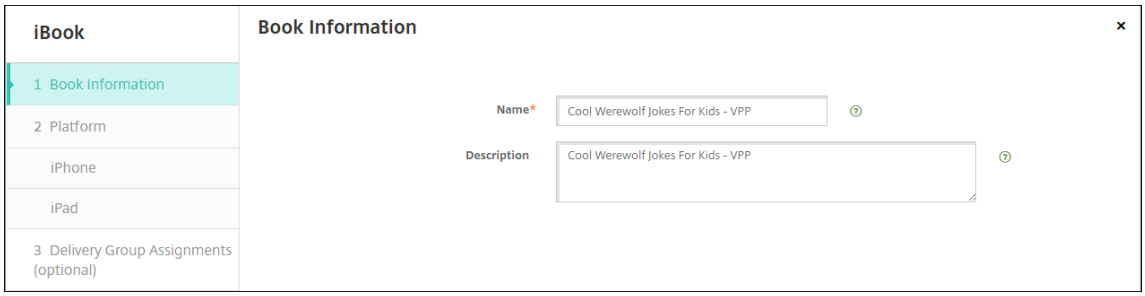
Konfigurieren von Büchern

Über Volume Purchase erworbene Bücher werden auf der Seite **Konfigurieren > Medien** angezeigt.



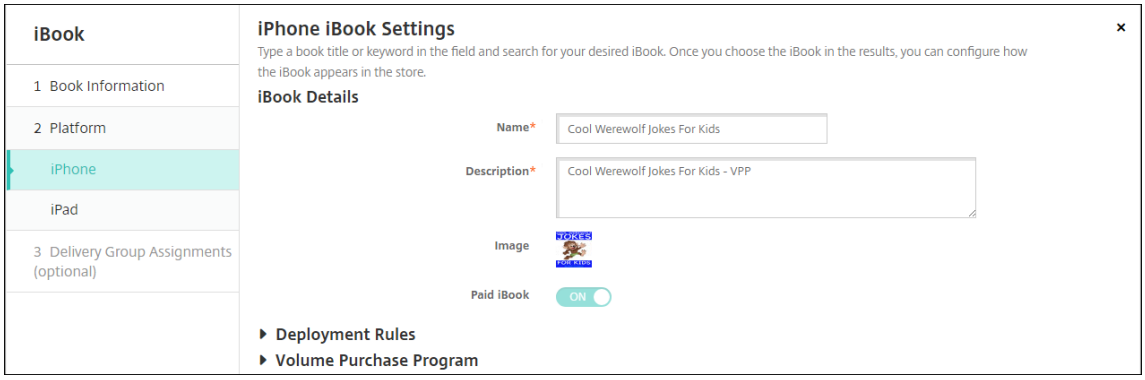
Konfigurieren eines Apple-Buchs für die Bereitstellung

1. Wählen Sie unter **Konfigurieren > Medien** ein Buch aus und klicken Sie auf **Bearbeiten**. Die Seite **Buchinformationen** wird angezeigt.

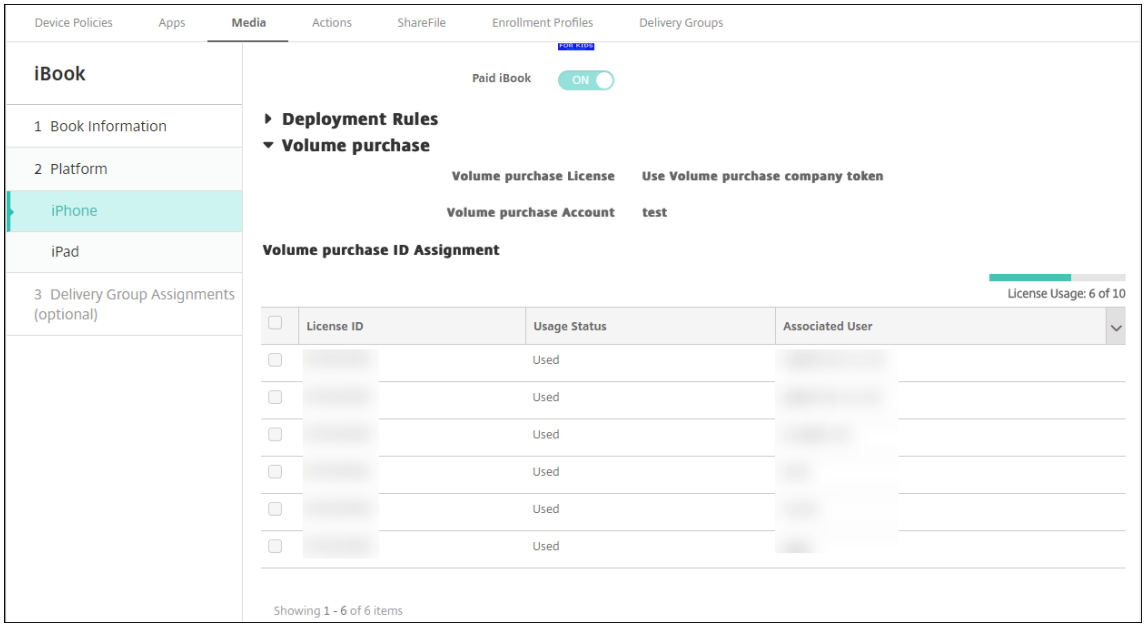


   Der **Name** und die **Beschreibung** werden nur in der XenMobile-Konsole und den Protokollen angezeigt.

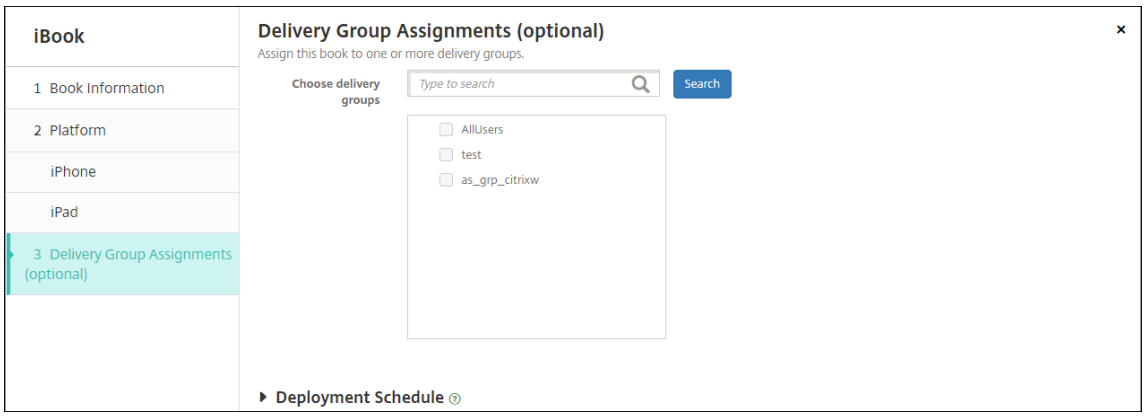
2. Auf den Seiten **iBook-Einstellungen für iPhone** und **iBook-Einstellungen iPad**: Sie können den Namen und die Beschreibung des Buchs optional ändern. Citrix empfiehlt jedoch, diese Einstellungen nicht zu ändern. Das Bild dient zur Information und kann nicht bearbeitet werden. **Bezahltes iBook:** zeigt an, dass ein Buch über Volume Purchase erworben wurde.



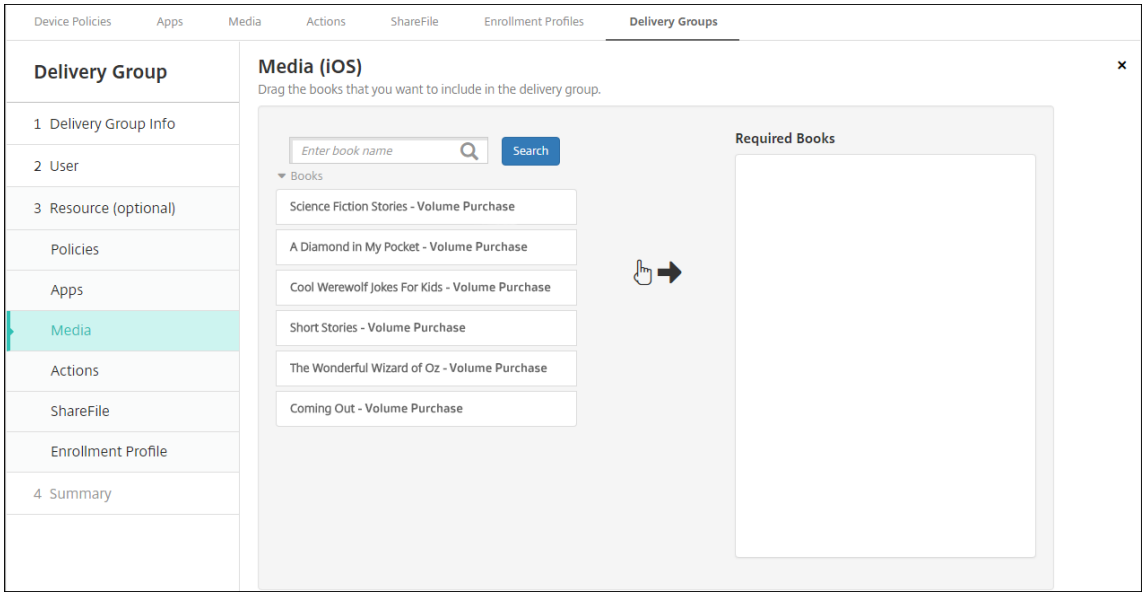
Sie können auch Volume Purchase-Informationen anzeigen oder Bereitstellungsregeln festlegen.



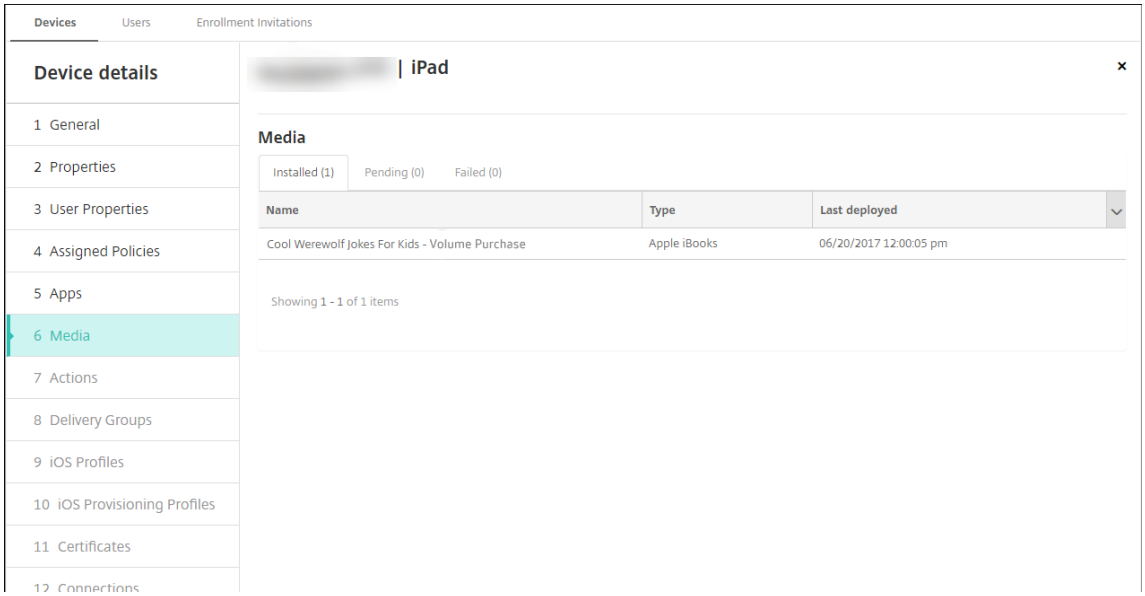
3. Optional können Sie das Buch Bereitstellungsgruppen zuordnen und einen Bereitstellungsplan festlegen.



Sie können Bücher Bereitstellungsgruppen auch über die Registerkarte **Medien** des Bereichs **Konfigurieren > Bereitstellungsgruppen** zuordnen. XenMobile unterstützt nur die Bereitstellung von erforderlichen Büchern.



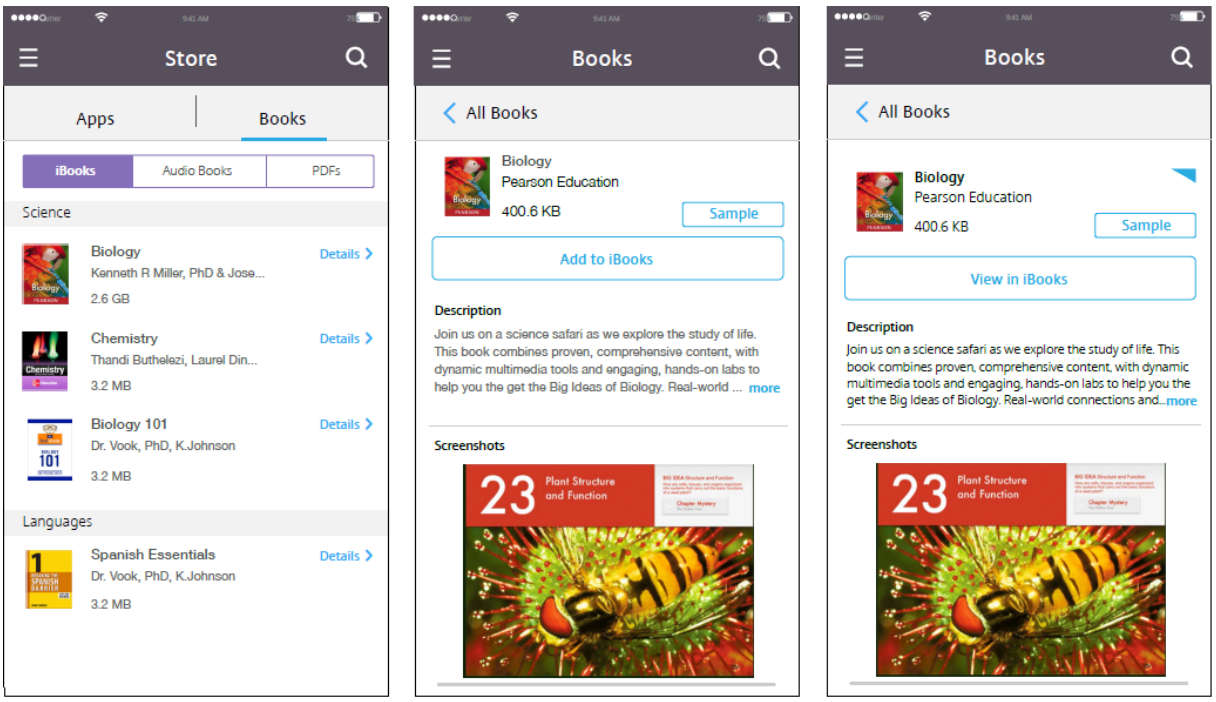
4. Verwenden Sie die Registerkarte **Medien** unter **Verwalten > Geräte**, um den Bereitstellungsstatus anzuzeigen.



Hinweis:

Wenn Sie auf der Seite **Konfigurieren > Medien** ein Buch auswählen und auf **Löschen** klicken, entfernt XenMobile das Buch aus der Liste. Wenn XenMobile jedoch das nächste Mal mit Apple Volume Purchase synchronisiert wird, erscheint das Buch wieder auf der Liste, sofern es nicht aus Apple Volume Purchase entfernt wurde. Das Löschen eines Buches aus der Liste entfernt das Buch nicht von den Geräten.

Bücher erscheinen auf Benutzergeräten wie im nachstehenden Beispiel gezeigt.



Bereitstellen von Ressourcen

January 5, 2022

Die Gerätekonfiguration und -verwaltung umfasst üblicherweise das Erstellen von Ressourcen (Richtlinien, Apps und Medien) 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 Folgendes beschrieben:

- Hinzufügen, Verwalten und Bereitstellen von Bereitstellungsgruppen
- Ändern der Bereitstellungsreihenfolge von Ressourcen in Bereitstellungsgruppen
- Festlegung der Bereitstellungsreihenfolge in XenMobile für Benutzer, die Mitglied mehrerer Bereitstellungsgruppen mit doppelten oder widersprüchlichen Richtlinien sind

Bereitstellungsgruppen sind Kategorien von Benutzern, für deren Geräte Sie Kombinationen aus Richtlinien, Apps, Medien 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 in einer Bereitstellungsgruppe wird eine Pushbenachrichtigung an alle Benutzer mit unterstützten iOS- und Windows-Geräten in der Bereitstellungsgruppe gesendet. Die Benutzer müssen zu der Bereitstellungsgruppe gehören, um eine Wiederverbindung mit XenMobile herstellen zu können. Sie können die Geräte neu auswerten und Richtlinien, Apps, Medien und Aktionen als Teil einer Bereitstellungsgruppe bereitstellen.

Android-Geräte: Besteht bereits eine Verbindung, erhalten die Benutzer die Ressourcen sofort. Ansonsten erhalten sie die Ressourcen basierend auf der Planungsrichtlinie beim nächsten Herstellen einer Verbindung.

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 gilt nur für Geräte in einer Bereitstellungsgruppe mit einem für die Geräteverwaltung (MDM) konfigurierten Registrierungsprofil.

Beim Ermitteln der Bereitstellungsreihenfolge wendet XenMobile Filter- und Steuerungskriterien für Ressourcen an, z. B. Bereitstellungsregeln und Bereitstellungszeitpläne. Ressourcen sind Richtlinien, Apps, Aktionen und Bereitstellungsgruppen. 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, Apps und Medien) 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, Medien 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 Richtlinien, Apps, Medien und Aktionen 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 Filter und Steuerungskriterien für die verschiedenen Objekt- und Ressourcentypen. Bereitstellungsregeln basieren auf Geräteeigenschaften.

Objekt/Ressource	Geräteplattform	Bereitstellungsregel	Bereitstellungszeitplan	Benutzer/Gruppen
Geräterichtlinie	J	J	J	-
App	J	J	J	-
Medien	J	J	J	-
Aktion	-	J	J	-
Bereitstellungsgru	-	J	-	J

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.

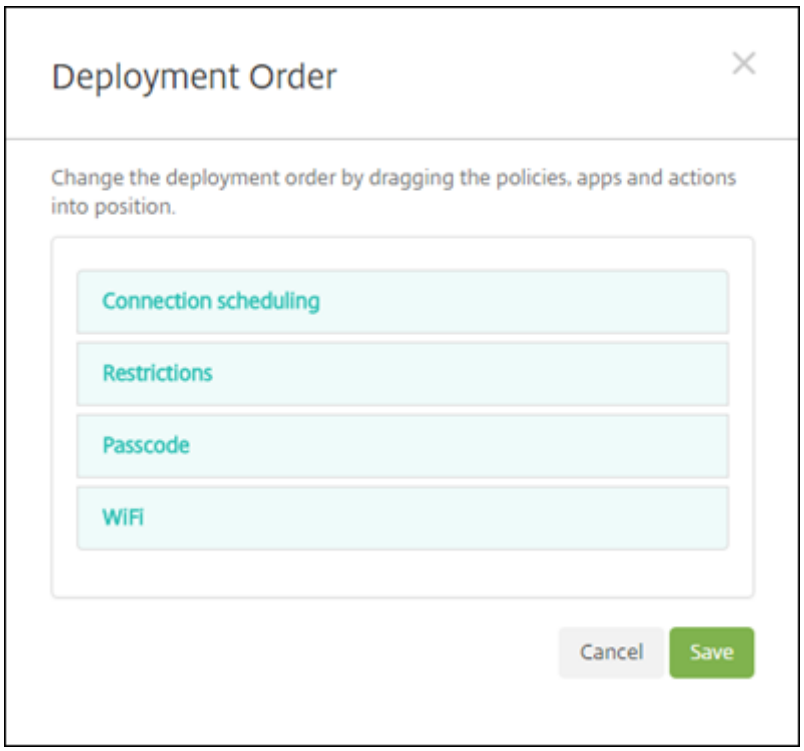
Berechnungsschritte

1. Ermitteln aller Bereitstellungsgruppen für einen bestimmten Benutzer, basierend auf den Filtern für Benutzer, Gruppen und Bereitstellungsregeln
2. Erstellen einer sortierten Liste aller Ressourcen (Richtlinien, Apps, Medien und Aktionen) in den ausgewählten Bereitstellungsgruppen. Die Liste basiert auf den Filtern für Geräteplattform, Bereitstellungsregeln und Bereitstellungszeitplan. Der Sortieralgorithmus ist wie folgt:
    a) Ressourcen von Bereitstellungsgruppen, die eine benutzerdefinierte Bereitstellungsreihenfolge haben, werden vor die von Bereitstellungsgruppen ohne Bereitstellungsreihenfolge gestellt. Die Begründung für diese Platzierung wird nach diesen Schritten beschrieben.
    b) Bei einem Gleichstand zwischen Bereitstellungsgruppen werden Ressourcen aus Bereitstellungsgruppen nach dem Bereitstellungsgruppennamen sortiert. Beispiel: Ressourcen von Bereitstellung Gruppe A werden vor denen aus Bereitstellungsgruppe B einsortiert.
    c) Wurde eine benutzerdefinierte Bereitstellungsreihenfolge für die Ressourcen in einer Bereitstellungsgruppe angegeben, muss sie beim Sortieren erhalten bleiben. Sonst die Ressourcen in der Bereitstellungsuppe nach Ressourcenname sortieren.
    d) Kommt dieselbe Ressource mehrmals vor, 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: Bei einer **nicht angegebenen** Ressourcenreihenfolge sind die Richtlinien **Wi-Fi** und **Passcode** enthalten.
- Bereitstellungsgruppe Kontomanager 2: Bei einer **angegebenen** Ressourcenreihenfolge sind die Richtlinien **Verbindungszeitplan**, **Einschränkungen**, **Passcode**, **Wi-Fi** enthalten. In diesem Fall sollten Sie die Richtlinie **Passcode** vor der Richtlinie **Wi-Fi** bereitstellen.



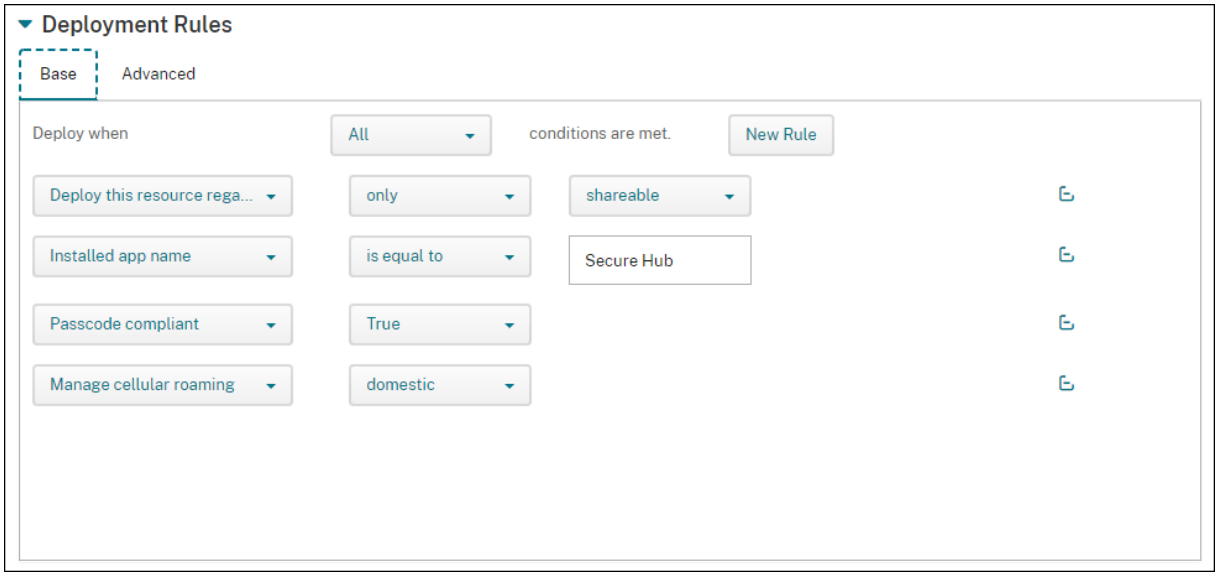
Wenn Bereitstellungsgruppen durch den Algorithmus nur nach Namen sortiert werden, führt XenMobile die Bereitstellung beginnend mit der Bereitstellungsgruppe “Kontomanager 1” in der Reihenfolge **Wi-Fi**, **Passcode**, **Verbindungszeitplan**, **Einschränkungen**. XenMobile ignoriert in diesem Fall **Passcode** und **Wi-Fi** (beides Duplikate) aus der Bereitstellungsgruppe “Kontomanager 2”.

Für die Gruppe “Kontomanager 2” gibt es jedoch eine vom Administrator festgelegte Bereitstellungsreihenfolge. Aus diesem Grund werden Ressourcen aus der Bereitstellungsgruppe “Kontomanager 2” von dem Algorithmus in der Liste höher platziert als die Ressourcen aus der anderen Bereitstellungsgruppe. Die Richtlinien werden daher von XenMobile in der folgenden Reihenfolge bereitgestellt: **Verbindungszeitplan**, **Einschränkungen**, **Passcode**, **Wi-Fi**. XenMobile ignoriert die Richtlinien **Wi-Fi** und **Passcode** aus der Bereitstellungsgruppe “Kontomanager 1”, da es sich um Duplikate handelt. Dieser Algorithmus wendet daher die vom XenMobile-Administrator festgelegte Reihenfolge an.

Bereitstellungsregeln

Konfigurieren Sie Bereitstellungsregeln, um Ressourcen nur dann bereitzustellen, wenn bestimmte Bedingungen erfüllt sind. Sie können einfache und erweiterte Bereitstellungsregeln konfigurieren.

Wenn Sie eine Bereitstellungsregel mit dem einfachen Editor hinzufügen, wählen Sie zuerst aus, wann die Ressource bereitgestellt werden soll.

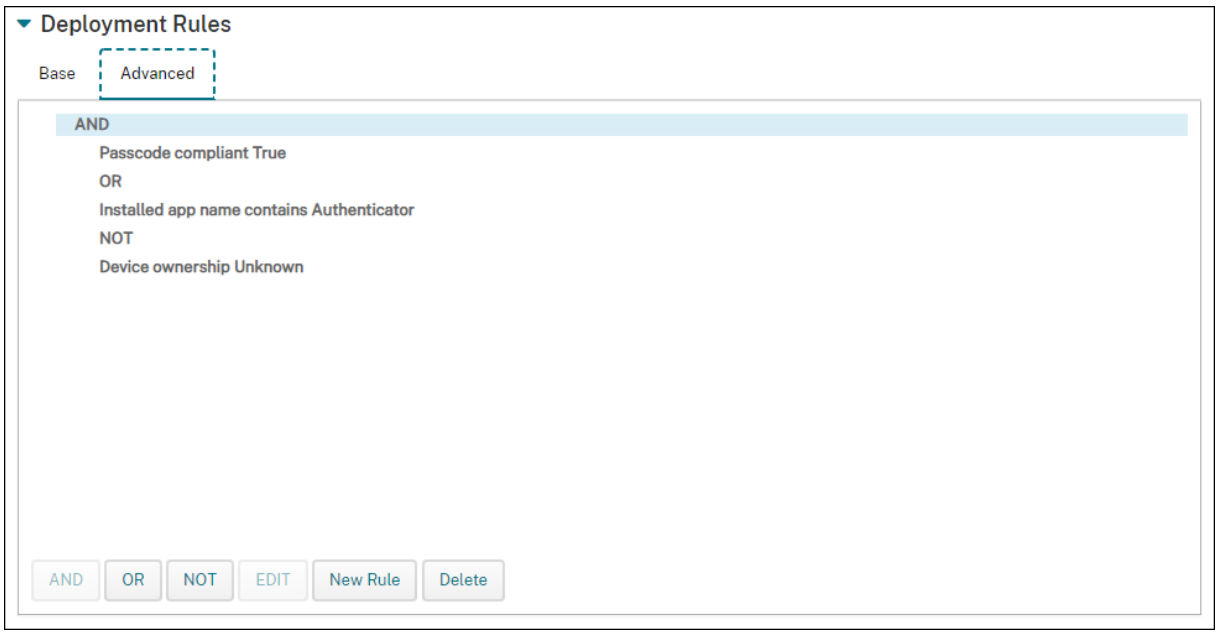


- **Alle:** Stellen Sie die Ressource bereit, wenn der Benutzer oder das Gerät alle von Ihnen konfigurierten Bedingungen erfüllt.
- **Beliebig:** Stellen Sie die Ressource bereit, wenn der Benutzer oder das Gerät mindestens eine der von Ihnen konfigurierten Bedingungen erfüllt.

Klicken Sie auf **Neue Regel**, um eine Bedingung hinzuzufügen. Die Regeln variieren je nach bereitgestellter Ressource und der Plattform, für die Sie die Ressource konfigurieren. Es gibt verschiedene Arten von Regeln. Je nach Auswahl können Sie die Ressource bereitstellen, wenn Folgendes gilt:

- Die ausgewählte Eigenschaft muss vorhanden bzw. darf nicht vorhanden sein.
- Die Eigenschaft stimmt mit dem von Ihnen eingegebenen Text genau überein, enthält den eingegebenen Text oder stimmt damit nicht überein.
- Das Gerät oder der Benutzer ist mit der von Ihnen ausgewählten Eigenschaft konform bzw. nicht konform.
- Die Geräte- oder Benutzereigenschaften stimmen mit der Bedingung überein, die Sie aus einer vordefinierten Liste auswählen.

Mit dem erweiterten Editor können Sie komplexere Bereitstellungsregeln erstellen. Es stehen mehr Regeln zur Auswahl, und Sie können verschiedene Boolesche Logikoperatoren kombinieren, wenn Sie eine erweiterte Regel erstellen.

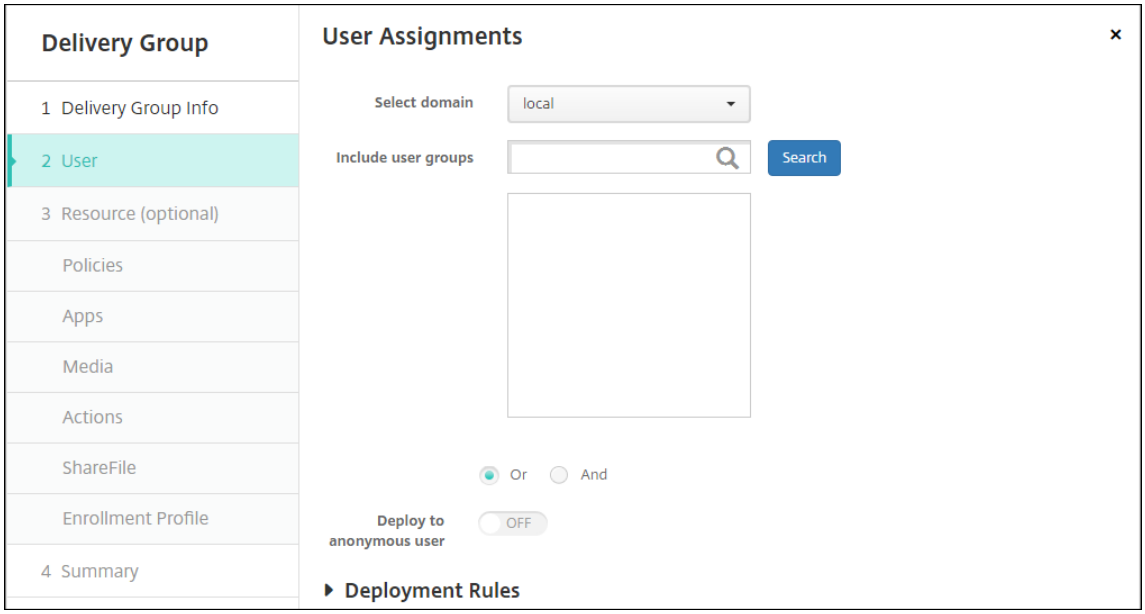


Hinzufügen einer Bereitstellungsgruppe

Citrix empfiehlt, erst die Bereitstellungsgruppen und dann die Geräterichtlinien und Registrierungsprofile zu erstellen.

1. Klicken Sie in der Konsole auf **Konfigurieren > Bereitstellungsgruppen**.
2. Klicken Sie auf der Seite **Bereitstellungsgruppen** auf **Hinzufügen**.
3. Geben Sie auf der Seite **Bereitstellungsgruppeninformationen** einen Namen und eine Beschreibung für die Bereitstellungsgruppe ein und klicken Sie dann auf **Weiter**.

   Wenn ein Benutzer zu mehreren Bereitstellungsgruppen mit unterschiedlichen Registrierungsprofilen gehört, bestimmt der Name der Bereitstellungsgruppe das verwendete Registrierungsprofil. XenMobile wählt die letzte Bereitstellungsgruppe in der alphabetisch geordneten Bereitstellungsgruppenliste aus. Weitere Informationen finden Sie unter Registrierungsprofile.
4. Geben Sie auf der Seite **Benutzerzuweisungen** an, wie die Zuweisungen der Bereitstellungsgruppe verwaltet werden sollen.



Wichtig:

Sie können die Einstellung **Benutzerzuweisungen verwalten** nach der Erstellung der Bereitstellungsgruppe nicht mehr ändern.

- **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 bereitgestellte 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. Nicht authentifizierte Benutzer sind Benutzer, bei denen keine Authentifizierung erfolgen konnte, denen aber dennoch eine Verbindung mit XenMobile gestattet wurde.

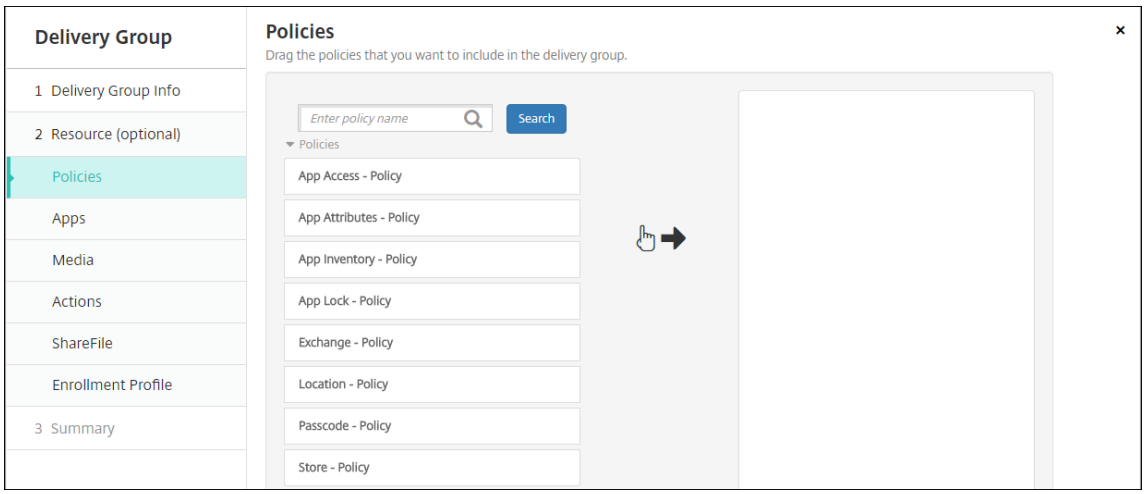
5. Konfigurieren Sie die Bereitstellungsregeln.
6. Klicken Sie auf **Weiter**. Die Seite **Ressourcen** für die Bereitstellungsgruppe wird angezeigt. Hier können Sie für die Bereitstellungsgruppe optional Richtlinien, Apps oder Aktionen hinzufügen. Zum Überspringen dieses Schritts klicken Sie unter **Bereitstellungsgruppe** auf **Zusammenfassung**, um eine Zusammenfassung der Bereitstellungsgruppenkonfiguration anzuzeigen.

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

Hinzufügen von Richtlinien

1. Führen Sie für jede Richtlinie, die Sie hinzufügen möchten, folgende Schritte aus:
   - Suchen Sie in der Liste der verfügbaren Richtlinien nach der hinzuzufügenden Richtlinie.
   - Alternative: Um die Liste der Richtlinien einzuschränken, geben Sie den Richtliniennamen vollständig oder teilweise im Suchfeld ein und klicken Sie dann auf **Suchen**.
   - Klicken Sie auf die Richtlinie und ziehen Sie sie in das Feld auf der rechten Seite.

   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

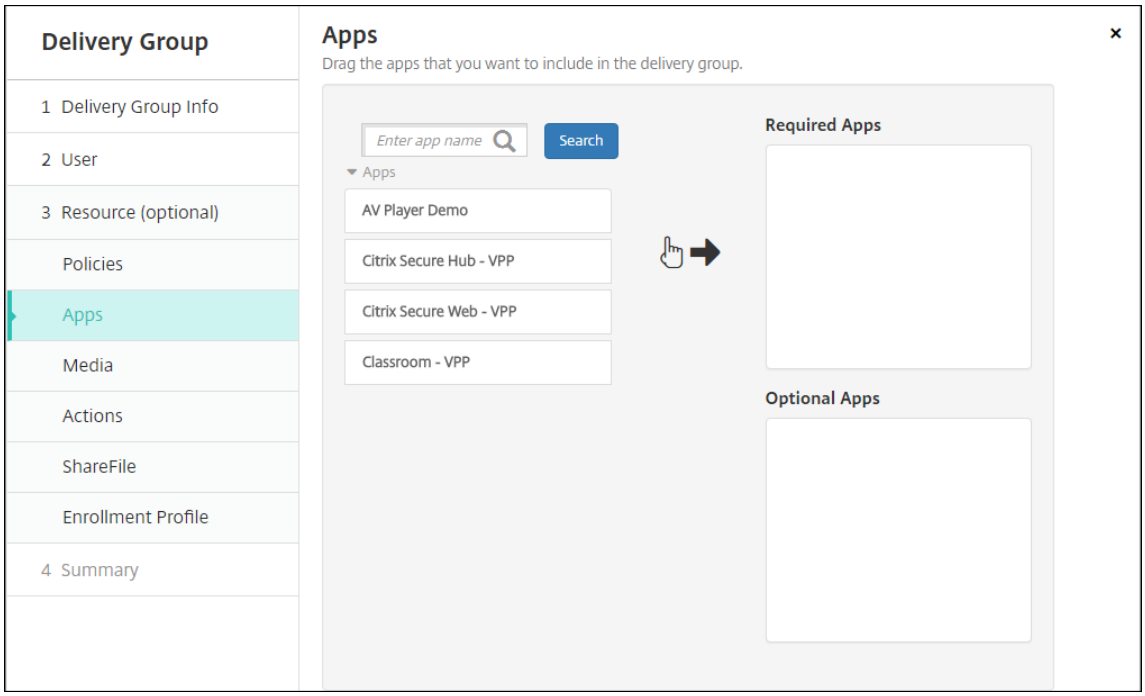
1. Führen Sie für jede hinzuzufügende App die folgenden Schritte durch:

   - 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 im 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**.

   Für als erforderlich markierte Apps können Benutzer u. a. in folgenden Situationen Updates schnell erhalten:

   - Sie laden eine neue App hoch und legen sie als erforderlich fest.
   - Sie legen eine vorhandene App als erforderlich fest.
   - Ein Benutzer löscht eine erforderliche App.
   - Es gibt ein Secure Hub-Update.

   Weitere Informationen zur erzwungenen Bereitstellung erforderlicher Apps und zur Aktivierung des Features finden Sie unter Erforderliche und optionale Apps.

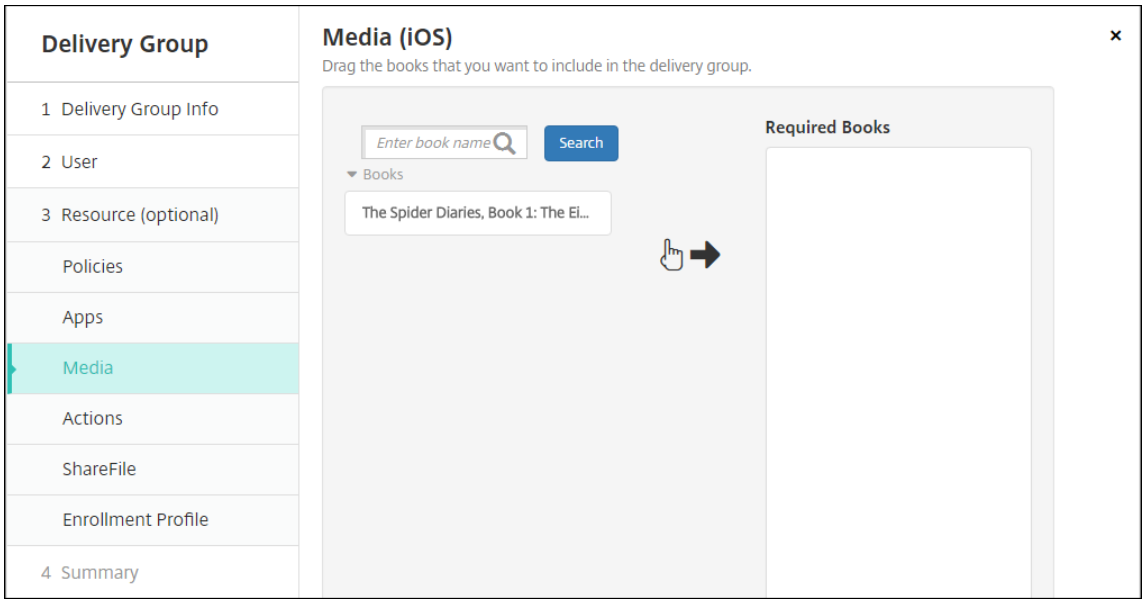


   Zum Entfernen einer App klicken Sie im rechten Feld auf das **X** neben deren Namen.

2. Klicken Sie auf **Weiter**. Die Seite **Medien** wird angezeigt.

Hinzufügen von Medien

1. Führen Sie für jedes gewünschte Medium folgende Schritte aus:
   - Suchen Sie das gewünschte Buch in der Liste der verfügbaren Bücher.
   - Alternative: Um die Liste der Bücher einzuschränken, geben Sie den Buchnamen vollständig oder teilweise im Suchfeld ein und klicken Sie dann auf **Suchen**.
   - Klicken Sie auf das Buch und ziehen Sie es in das Feld **Erforderliche Bücher**.



   Für als erforderlich markierte Bücher erhalten die Benutzer in folgenden Situationen unverzüglich Updates:

   - Sie laden ein neues Buch hoch und legen es als erforderlich fest.
   - Sie legen ein vorhandenes Buch als erforderlich fest.
   - Ein Benutzer löscht ein erforderliches Buch.
   - Es gibt ein Secure Hub-Update.

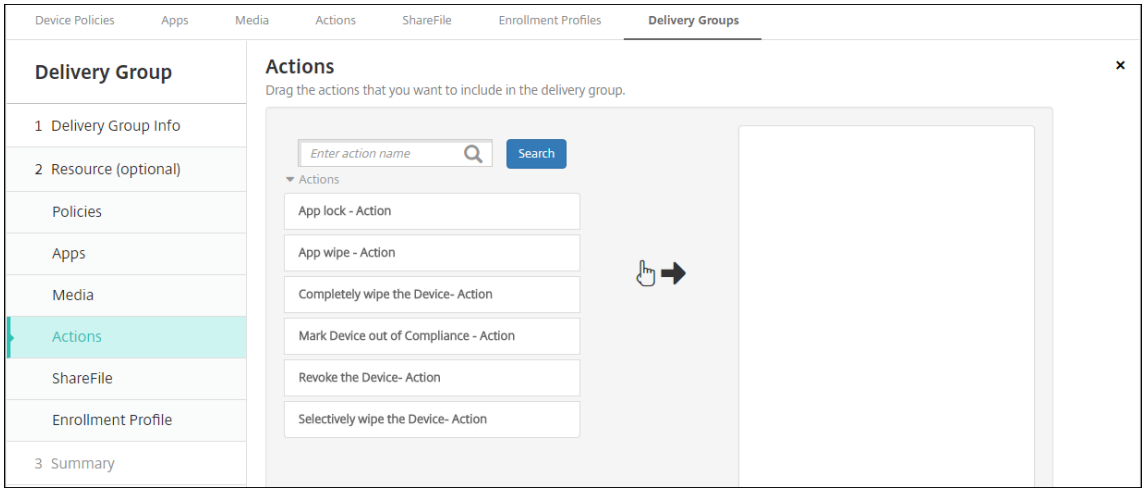
   Zum Entfernen eines Buchs klicken Sie im rechten Feld auf das **X** neben dessen Namen.

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 in der Liste der verfügbaren Aktionen nach der hinzuzufügenden Aktion.
   - Alternative: Um die Liste der Aktionen einzuschränken, geben Sie den Namen der Aktion vollständig oder teilweise im Suchfeld ein und klicken Sie dann auf **Suchen**.
   - Klicken Sie auf die Aktion und ziehen Sie sie in das Feld auf der rechten Seite.

Zum Entfernen einer Aktion klicken Sie im rechten Feld auf das **X** neben deren Namen.

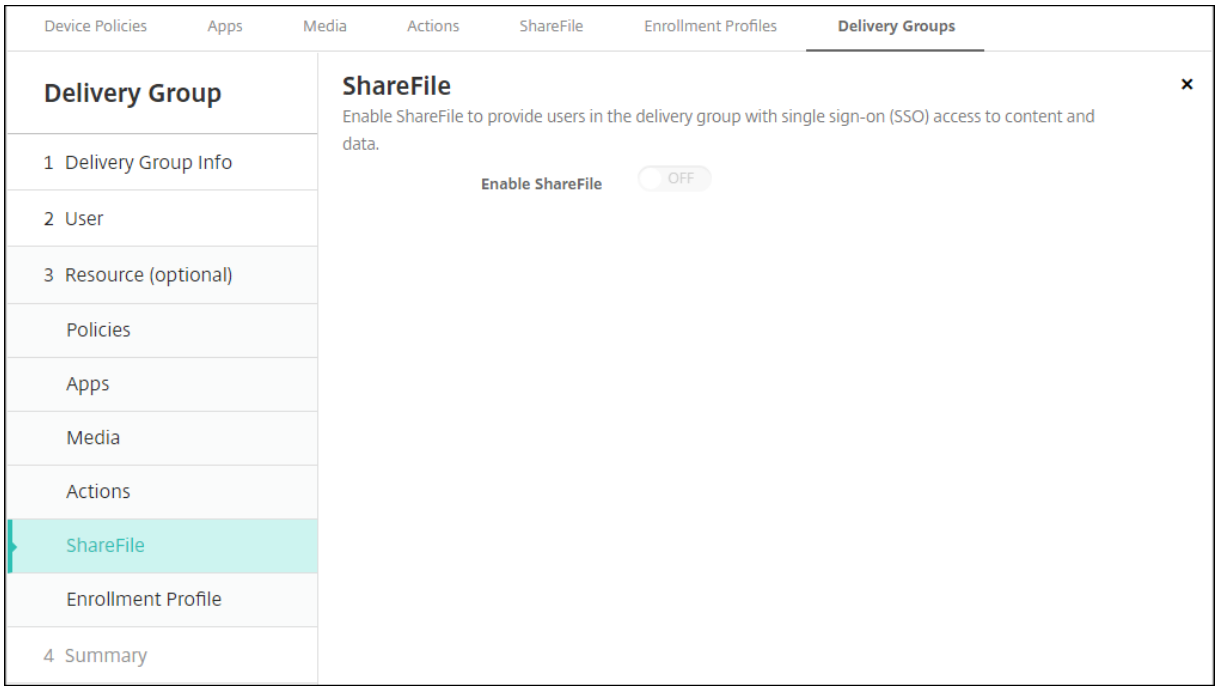


2. Klicken Sie auf **Weiter**. Die Seite **ShareFile** wird angezeigt.

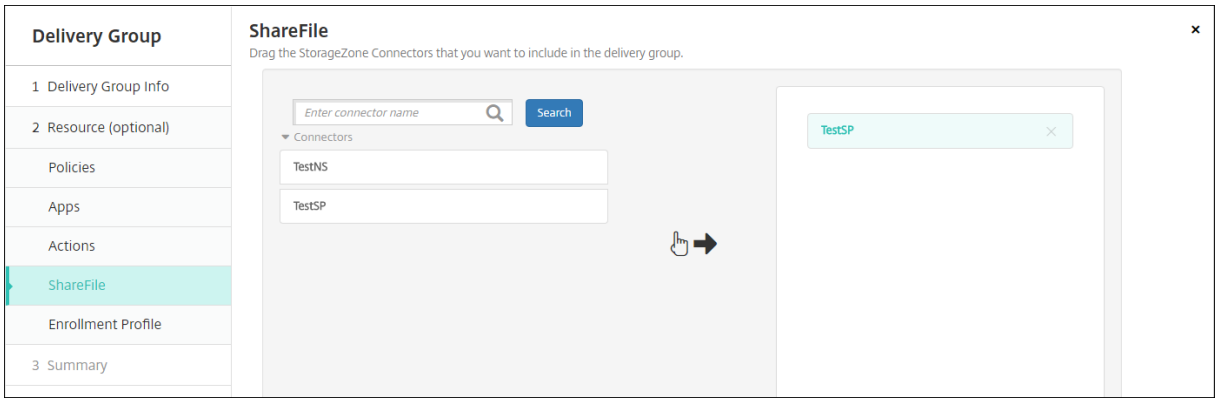
Anwenden der Content Collaboration-Konfiguration

Die Seite “Content Collaboration” unterscheidet sich je nachdem, ob Sie XenMobile (**Konfigurieren > ShareFile**) für Enterprise-Konten oder für Speicherzonen-Connectors konfiguriert haben.

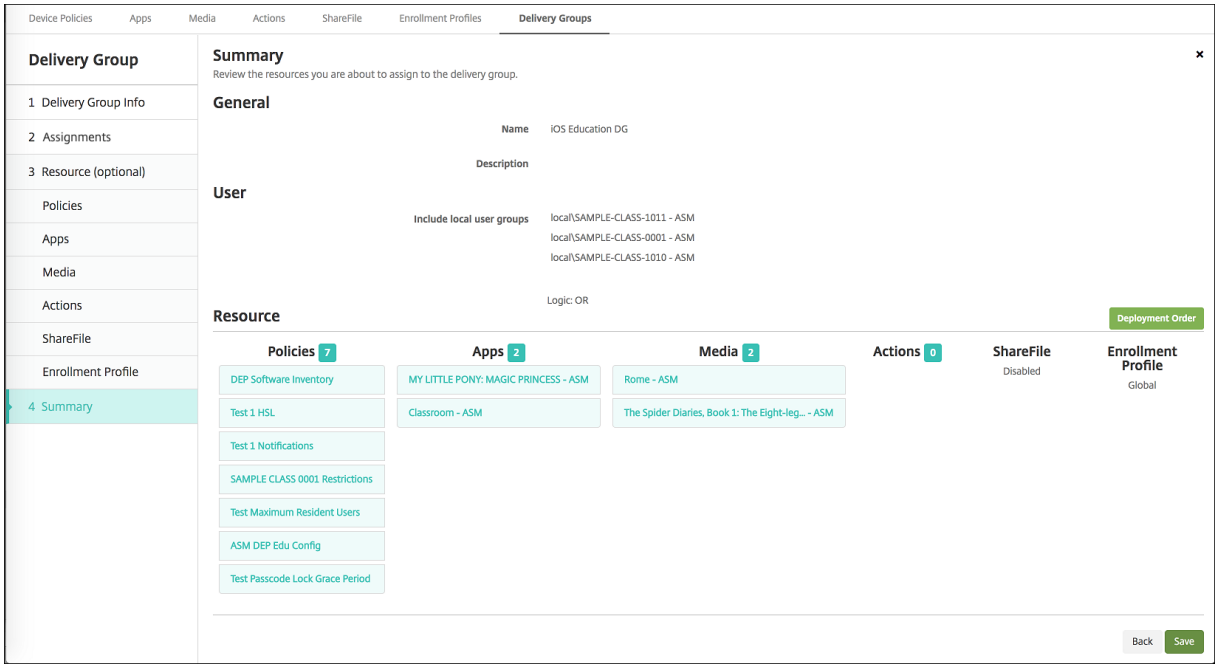
Wenn Sie Enterprise-Konten für XenMobile konfiguriert haben: Setzen Sie **ShareFile aktivieren** auf **EIN**, um den Bereitstellungsgruppen Single Sign-On-Zugriff auf Content Collaboration-Inhalte und -Daten zu gewähren.



Wenn Sie Speicherzonenconnectors für die Verwendung mit XenMobile konfiguriert haben, wählen Sie die Speicherzonenconnectors aus, die in die Bereitstellungsgruppe aufgenommen werden sollen.

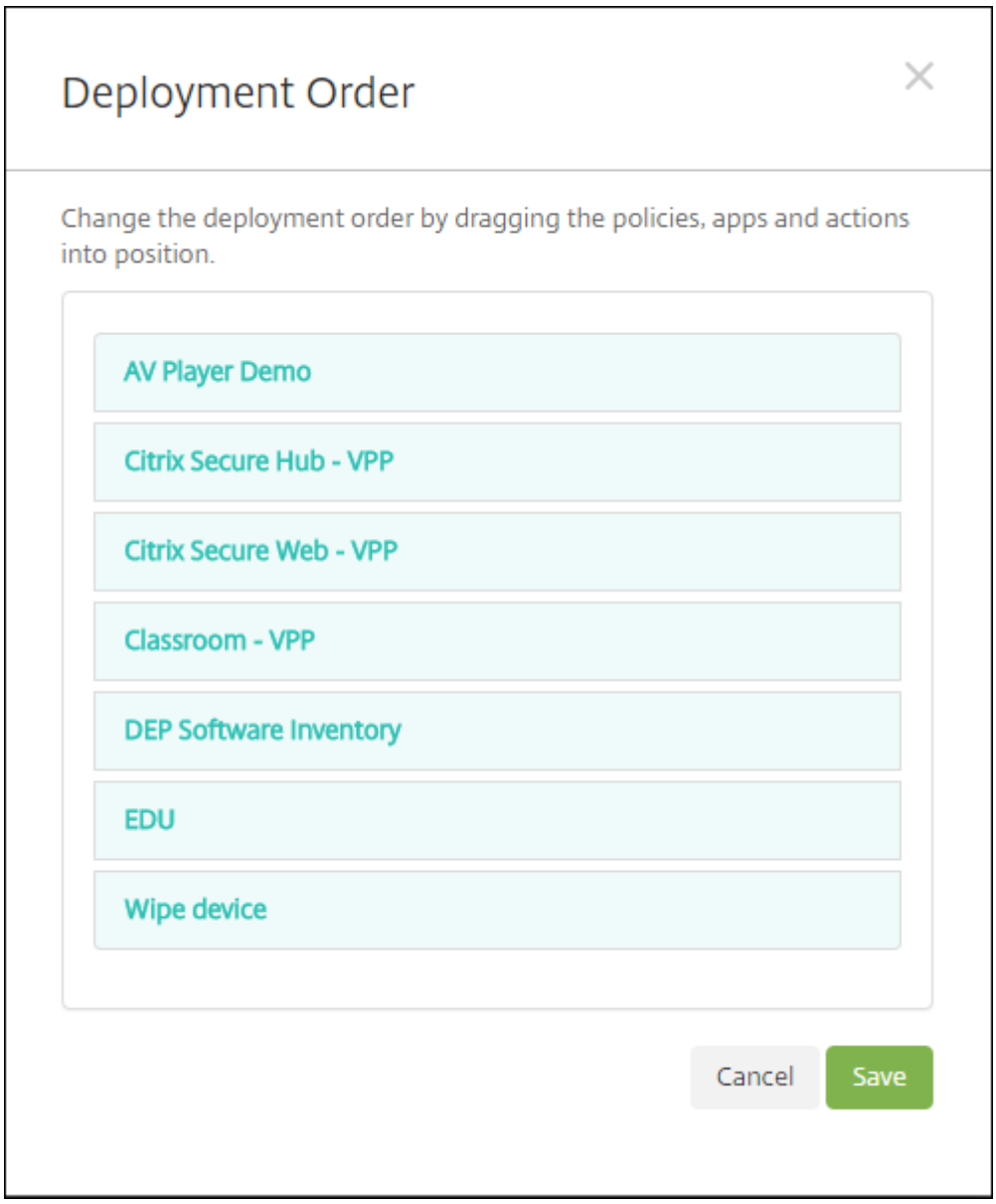


Überprüfen der konfigurierten Optionen und Ändern der Bereitstellungsreihenfolge



Auf der Seite **Zusammenfassung** können Sie die Optionen überprüfen, die Sie für die Bereitstellungsgruppe konfiguriert haben, und die Bereitstellungsreihenfolge der Ressourcen ändern. Auf der Seite "Zusammenfassung" werden die Ressourcen nach Kategorie angezeigt. Auf der Seite "Zusammenfassung" ist die Bereitstellungsreihenfolge nicht ersichtlich.

1. Klicken Sie auf **Zurück**, um zu vorherigen Seiten zurückzukehren und notwendige Änderungen an der Konfiguration zu machen.
2. Klicken Sie auf **Bereitstellungsreihenfolge**, um die Reihenfolge anzuzeigen und ggf. zu ändern. Das Dialogfeld **Bereitstellungsreihenfolge** wird angezeigt.



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

Bearbeiten einer Bereitstellungsgruppe

Sie können den Namen einer vorhandenen Bereitstellungsgruppe nicht ändern. Aktualisieren anderer Einstellungen: Wählen Sie unter **Konfigurieren > Bereitstellungsgruppen** die gewünschte Gruppe und klicken Sie auf **Bearbeiten**.

Aktivieren oder Deaktivieren der Bereitstellungsgruppe “AllUsers”

“AllUsers” ist die einzige Bereitstellungsgruppe, die Sie aktivieren oder deaktivieren können.

Wählen Sie auf der Seite **Bereitstellungsgruppen** die Bereitstellungsgruppe “AllUsers” aus, indem Sie auf das Kontrollkästchen neben **AllUsers** oder auf die Zeile mit “AllUsers” klicken. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Deaktivieren**, um die Bereitstellungsgruppe “AllUsers” zu deaktivieren. Dieser Befehl ist nur verfügbar, wenn “AllUsers” aktiviert ist (= Standardeinstellung). **Deaktiviert** wird unter der Überschrift **Deaktiviert** in der Tabelle der Bereitstellungsgruppen angezeigt.
- Klicken Sie auf **Aktivieren**, um die Bereitstellungsgruppe “AllUsers” zu aktivieren. Dieser Befehl ist nur verfügbar, wenn “AllUsers” deaktiviert ist. **Deaktiviert** wird unter der Überschrift **Deaktiviert** in der Tabelle der Bereitstellungsgruppen nicht mehr angezeigt.

Bereitstellen in Bereitstellungsgruppen

Das Bereitstellen in einer Bereitstellungsgruppe bedeutet, dass eine Pushbenachrichtigung an alle Benutzer mit iOS-, Windows Phone- und Windows Tablet-Geräte in der Bereitstellungsgruppe gesendet wird. Die Benutzer müssen zu der Bereitstellungsgruppe gehören, um eine Wiederverbindung mit XenMobile herstellen zu können. Auf diese Weise können Sie die Geräte neu auswerten und Apps, Richtlinien und Aktionen bereitstellen.

Benutzer anderer Geräteplattformen: Sind diese Geräte bereits mit XenMobile verbunden, erhalten die Benutzer die Ressourcen sofort. Ansonsten erhalten sie die Ressourcen basierend auf der Planungsrichtlinie beim nächsten Herstellen einer Verbindung.

Damit aktualisierte Apps in der Liste der verfügbaren Updates im XenMobile Store auf Android-Geräten angezeigt werden, stellen Sie auf den Geräten zunächst eine App-Bestandsrichtlinie bereit.

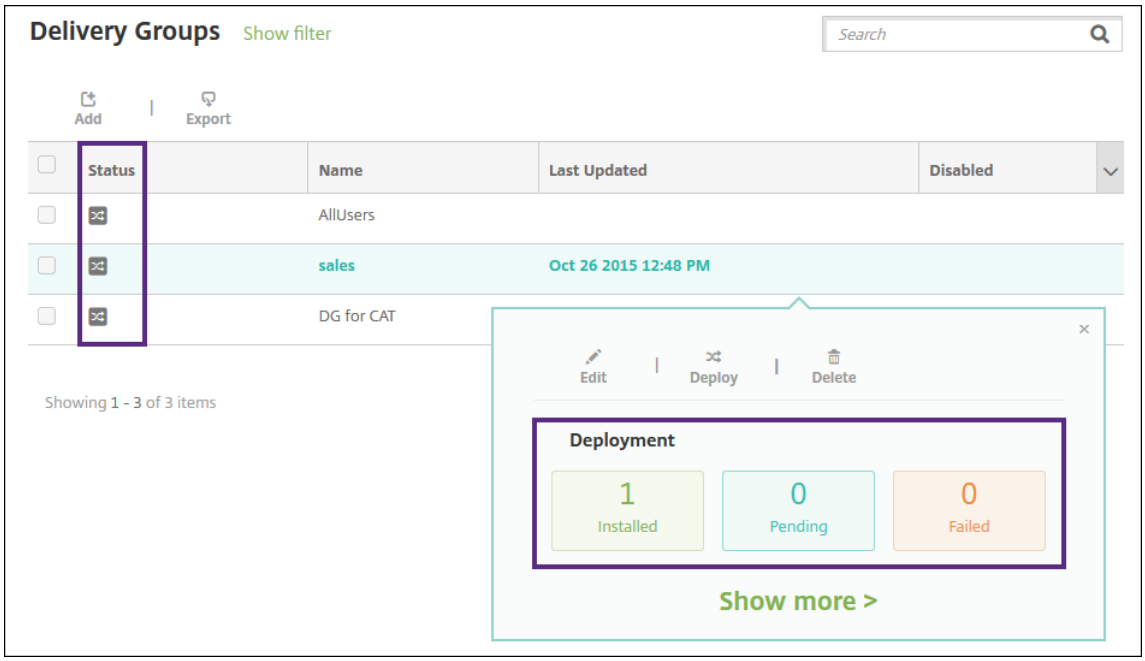
1. Führen Sie auf der Seite **Bereitstellungsgruppen** einen der folgenden Schritte aus:
    - Zur Bereitstellung für mehrere Bereitstellungsgruppen aktivieren Sie die Kontrollkästchen neben den gewünschten Gruppen.
    - Zur Bereitstellung für eine einzelne Bereitstellungsgruppe klicken Sie auf das Kontrollkästchen neben ihrem Namen oder auf die Zeile mit ihrem Namen.
2. Klicken Sie auf **Bereitstellen**.

    Der Befehl **Bereitstellen** wird je nach Auswahl der einzelnen Bereitstellungsgruppen oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

    Stellen Sie sich sicher, 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 die Zeile mit der Bereitstellungsgruppe, um eine Überlagerung einzublenden, in der der Status **Installiert**, **Ausstehend** oder **Fehlgeschlagen** angezeigt wird.



Löschen von Bereitstellungsgruppen

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.

   Der Befehl **Löschen** wird je nach Auswahl der einzelnen Bereitstellungsgruppen oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

> **Wichtig:**
>
> Sie können das Löschen nicht rückgängig machen.

3. Klicken Sie auf **Löschen**.

Exportieren der Bereitstellungsgruppentabelle

1. Klicken Sie auf die Schaltfläche **Exportieren** oberhalb der Tabelle **Bereitstellungsgruppen**. XenMobile extrahiert die Informationen in der Tabelle **Bereitstellungsgruppen** und konvertiert sie in eine CSV-Datei.
2. Öffnen oder speichern Sie die CSV-Datei mit dem bei Ihrem Browser üblichen Verfahren. Sie können den Vorgang auch abbrechen.

Makros

April 7, 2021

XenMobile bietet Makros zum Eintragen von Benutzer- und Geräteeigenschaften im Textfeld folgender Elemente:

- Richtlinien
- Benachrichtigungen
- Registrierungsvorlagen
- Automatisierte Aktionen
- Zertifikatsignieranforderungen für Anmeldeinformationsanbieter

XenMobile ersetzt die Makros durch die entsprechenden Benutzer- oder Systemwerte. Sie können beispielsweise den Postfachwert in einem Exchange-Profil für tausende Benutzer vorab eingeben.

Makrosyntax

Ein Makro kann folgendes Format haben:

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

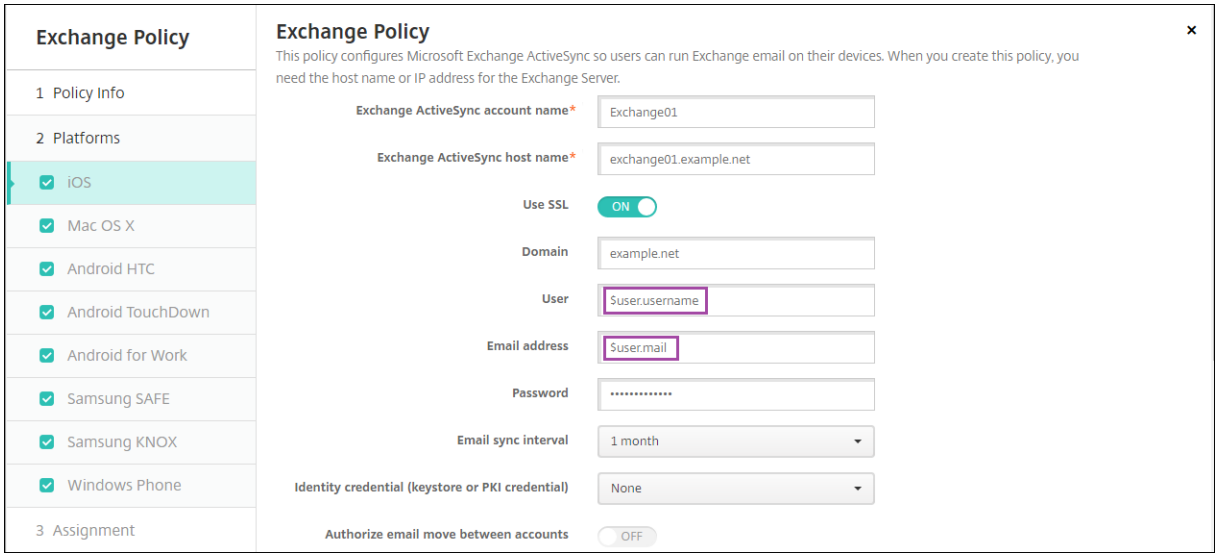
Umschließen Sie den gesamten Teil nach dem Dollarzeichen ($) mit geschweiften Klammern ({}).

- Qualifizierte Eigenschaftsnamen verweisen auf eine Benutzereigenschaft, eine Geräteeigenschaft oder eine benutzerdefinierte Eigenschaft.

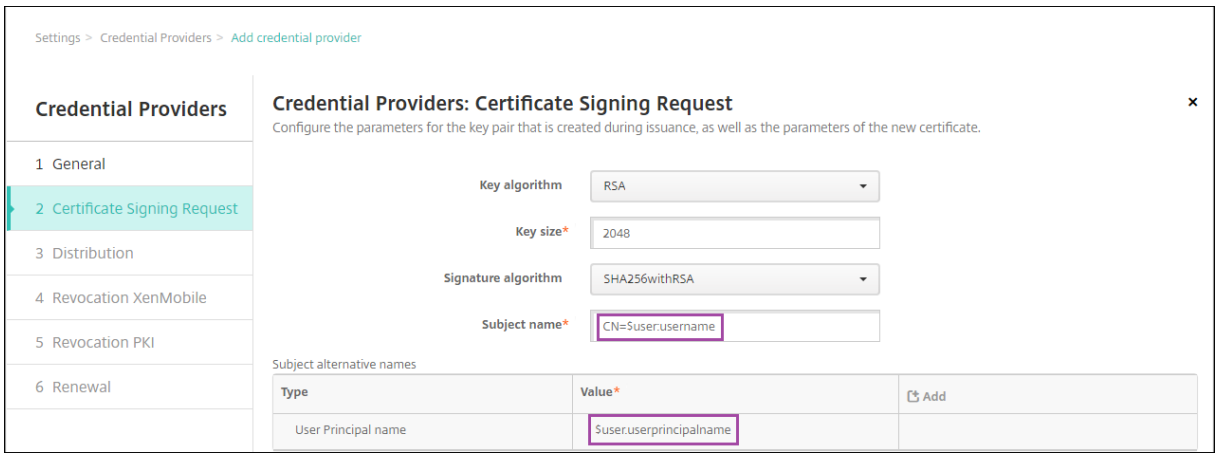
- Qualifizierte Eigenschaftsnamen bestehen aus einem Präfix gefolgt von dem eigentlichen Eigenschaftsnamen.
- Benutzereigenschaften haben die Form `${ user.[PROPERTYNAME] (prefix="user.")}`.
- Geräteeigenschaften haben die Form `${ device.[PROPERTYNAME] (prefix="device.") }`.
- Bei Eigenschaftennamen wird zwischen Groß- und Kleinschreibung unterschieden.
- Eine Funktion kann eine begrenzte Liste sein oder ein Link zu einer Drittanbieter-Referenz, die Funktionen definiert. Das folgende Makro für eine Benachrichtigung enthält die Funktion **firstnotnull**:

  Gerät `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` wurde gesperrt…
- Bei benutzerdefinierten (von Ihnen erstellten) Makros lautet das Präfix `${ custom }`. Sie können das Präfix auslassen.

Es folgt ein Beispiel des häufig verwendeten Makros `${ user.username }` zum Eintragen des Werts "Benutzername" im Textfeld einer Richtlinie. Das Makro ist nützlich beim Konfigurieren von Exchange ActiveSync-Profilen und anderen Profilen, die von mehreren Benutzern verwendet werden. Das folgende Beispiel zeigt, wie Makros in einer Exchange-Richtlinie verwendet werden. Das Makro für **Benutzer** ist **`${ user.username }`**. Das Makro für die **E-Mail-Adresse** ist **`${ user.mail }`**.

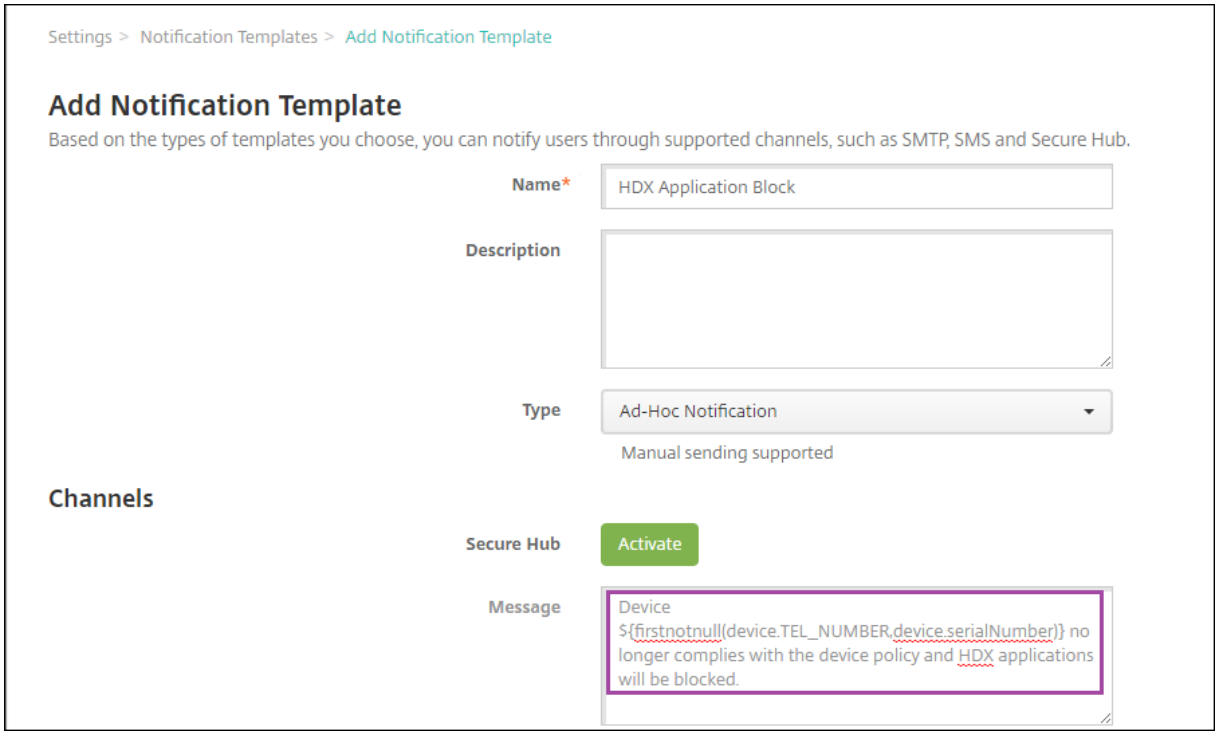


Das folgende Beispiel zeigt, wie Makros für eine Zertifikatsignieranforderung verwendet werden. Das Makro für **Antragstellername** ist **`CN=$user.username`**. Das Makro für den **Wert** von **Alternativer Antragstellername** ist **`$user.userprincipalname`**.



Das folgende Beispiel zeigt, wie Makros in einer Benachrichtigungsvorlage verwendet werden. Die Vorlage in dem Beispiel definiert die Nachricht, die an Benutzer gesendet wird, wenn HDX-Anwendungen aufgrund mangelnder Richtlinientreue des Geräts blockiert werden. Das Makro für **Meldung** ist:

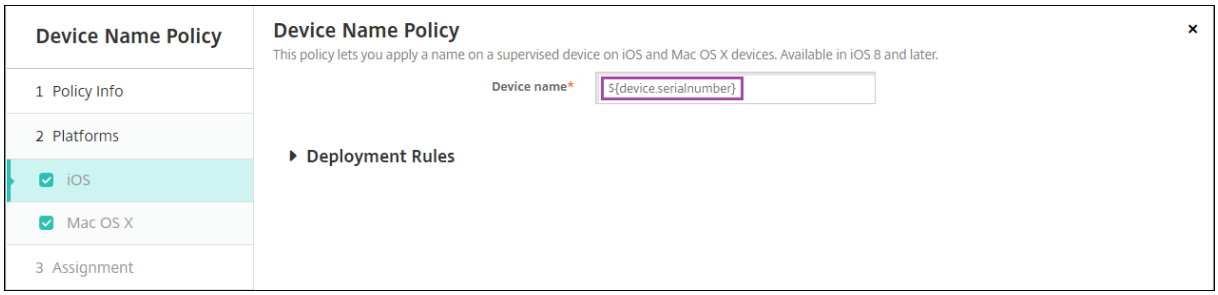
Gerät `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` erfüllt die Geräterichtlinie nicht mehr und HDX-Apps werden gesperrt.



Zum Aufrufen weiterer Beispiele für die Verwendung von Makros in Benachrichtigungen gehen Sie zu **Einstellungen > Benachrichtigungsvorlagen**, wählen Sie eine vordefinierte Vorlage und klicken Sie auf **Bearbeiten**.

Das folgende Beispiel zeigt ein Makro in der Geräterichtlinie “Gerätename”. Sie können das Makro,

eine Kombination aus Makros oder eine Kombination aus Makros und Text zur eindeutigen Benennung aller Geräte eingeben. Um beispielsweise als Gerätenamen die Seriennummer festzulegen, verwenden Sie `${ device.serialnumber }`. Verwenden Sie `${ device.serialnumber } ${ user.username }`, um den Benutzernamen in den Gerätenamen aufzunehmen. Die Geräterichtlinie “Gerätename” funktioniert auf betreuten iOS- und macOS-Geräten.



Makros für Standardbenachrichtigungsvorlagen

Folgende Makros können Sie in Standardbenachrichtigungsvorlagen verwenden:

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`
- `${ enrollment.url }`
- `${ enrollment.urls }`
- `${ enrollment.ios.url }`
- `${ enrollment.macos.url }`
- `${ enrollment.android.url }`
- `${ enrollment.ios.platform }`
- `${ enrollment.macos.platform }`
- `${ enrollment.android.platform }`
- `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${ firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${ outofcompliance.reason(smg_block)}`
- `${ outofcompliance.reason(whitelist_blacklist_apps_name)}`

> **Hinweis:**
>
> Die XenMobile Server-Konsole enthält im Englischen die Begriffe “Blacklist” und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

- `${ vpp.account }`
- `${ vpp.appname }`
- `${ vpp.url }`
- `${ zdmserver.hostPath } /enroll`

Makros für bestimmte Richtlinien

Bei der Geräterichtlinie für Gerätenamen (für iOS und macOS) können Sie folgende Makros für den **Gerätenamen** verwenden:

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

Bei der Webclip-Geräterichtlinie können Sie folgendes Makro für die **URL** verwenden:

- `${ webeas-url }`

Bei der Geräterichtlinie für Samsung MDM-Lizenzschlüssel können Sie dieses Makro für den **ELM-Lizenzschlüssel** verwenden:

- `${ elm.license.key }`

Makros zum Abrufen integrierter Geräteeigenschaften

Anzeigename	Makros
Geräte-ID	`$device.id`
Geräte-GUID	`$device.uniqueid`
Geräte-IMEI	`$device.imei`
OS-Familie	`$device.OSFamily`

Anzeigename	Makros
Seriennummer	`$device.serialNumber`

Makros für alle Geräteeigenschaften

Die folgende Liste enthält den Anzeigenamen, das Webelement und die Makros.

Konto vorübergehend gesperrt?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED

Code zum Umgehen der Aktivierungssperre

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE

Aktivierungssperre aktiviert

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED

Aktives iTunes-Konto

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

ActiveSync-Gerät ist MSP bekannt

- AS_DEVICE_KNOWN_BY_ZMSP
- ${device.AS_DEVICE_KNOWN_BY_ZMSP

ActiveSync-ID

- EXCHANGE_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_ID

Administrator deaktiviert

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED

AIK Present?

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT

Amazon MDM API verfügbar

- AMAZON_MDM

- ${device.AMAZON_MDM

Android Enterprise-Geräte-ID

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID

Android Enterprise-fähiges Gerät?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE

Android Enterprise-Installationstyp

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE

Status der Antispywaresignatur

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS

Antispywarestatus

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS

Status der Antivirenprogrammsignatur

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS

Antivirusstatus

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS

Code zum Umgehen der ASM-DEP-Aktivierungssperre

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE

Hinterlegter ASM-DEP-Schlüssel

- DEP_ESCROW_KEY
- ${device.DEP_ESCROW_KEY

Bestandskennzeichen

- ASSET_TAG
- ${device.ASSET_TAG

Automatisch auf Softwareupdates prüfen

- AutoCheckEnabled
- ${device.AutoCheckEnabled

Softwareupdates im Hintergrund automatisch herunterladen

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled

App-Updates automatisch installieren

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled

OS-Updates automatisch installieren

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled

Sicherheitsupdates automatisch installieren

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled

Status für automatische Updates

- AUTOUPDATE_STATUS
- ${device.AUTOUPDATE_STATUS

Verfügbarer RAM

- MEMORY_AVAILABLE
- ${device.MEMORY_AVAILABLE

Verfügbare Softwareupdates

- AVAILABLE_OS_UPDATE_HUMAN_READABLE
- ${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE

Verfügbarer Speicherplatz

- FREEDISK
- ${device.FREEDISK

Backupakku

- BACKUP_BATTERY_PERCENT
- ${device.BACKUP_BATTERY_PERCENT

Firmwareversion für Basisband

- MODEM_FIRMWARE_VERSION
- ${device.MODEM_FIRMWARE_VERSION

Akku wird geladen

- BATTERY_CHARGING_STATUS
- ${device.BATTERY_CHARGING_STATUS

Akku wird geladen

- BATTERY_CHARGING
- ${device.BATTERY_CHARGING

Verbleibender Akku

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING

Akkulaufzeit

- BATTERY_RUNTIME
- ${device.BATTERY_RUNTIME

Akkustatus

- BATTERY_STATUS
- ${device.BATTERY_STATUS

BES-Gerät ist MSP bekannt

- BES_DEVICE_KNOWN_BY_ZMSP
- ${device.BES_DEVICE_KNOWN_BY_ZMSP

BES-PIN

- BES_PIN
- ${device.BES_PIN

Agent-ID für BES-Server

- AGENT_ID
- ${device.AGENT_ID

BES-Servername

- BES_SERVER
- ${device.BES_SERVER

BES-Serverversion

- BES_VERSION
- ${device.BES_VERSION

BIOS-Info

- BIOS_INFO

- ${device.BIOS_INFO

BitLocker-Status

- WINDOWS_HAS_BIT_LOCKER_STATUS
- ${device.WINDOWS_HAS_BIT_LOCKER_STATUS

Bluetooth MAC-Adresse

- BLUETOOTH_MAC
- ${device.BLUETOOTH_MAC

Boot Debugging Enabled?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED

Boot Manager Rev List Version

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION

Code des Netzbetreibers

- CARRIER_CODE
- ${device.CARRIER_CODE

Version der Netzbetreibereinstellungen

- CARRIER_SETTINGS_VERSION
- ${device.CARRIER_SETTINGS_VERSION

Katalog-URL

- CatalogURL
- ${device.CatalogURL

Mobilnetzbreitengrad

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR

Mobilnetz - Kurs

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR

Mobilnetz - horizontale Genauigkeit

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR

Mobilnetzbreitengrad

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR

Mobilnetzlängengrad

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR

Mobilnetz - Geschwindigkeit

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR

Cellular-Technologie

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY

Mobilnetzzeitstempel

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR

Mobilnetz - vertikale Genauigkeit

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

Kennwort bei nächster Anmeldung ändern?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- ${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

Clienteräte-ID

- CLIENT_DEVICE_ID
- ${device.CLIENT_DEVICE_ID

Cloudbackup aktiviert

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED

Code Integrity Enabled?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED

Code Integrity Rev List Version

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION

Farbe

- COLOR
- ${device.COLOR

CPU-Taktfrequenz

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED

CPU-Typ

- CPU_TYPE
- ${device.CPU_TYPE}

Erstellungszeit

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- ${device.GOOGLE_AW_DIRECTORY_CREATION_TIME

Kritische Softwareupdates

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- ${device.AVAILABLE_OS_UPDATE_IS_CRITICAL

Aktuelles Betreibernetzwerk

- CARRIER
- ${device.CARRIER

Aktueller Ländercode für mobiles Gerät

- CURRENT_MCC
- ${device.CURRENT_MCC

Code für aktuelles mobiles Netzwerk

- CURRENT_MNC
- ${device.CURRENT_MNC

Datenroaming zugelassen

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED

Datum des letzten iCloud-Backups

- LAST_CLOUD_BACKUP_DATE
- ${device.LAST_CLOUD_BACKUP_DATE}

Standardkatalog

- IsDefaultCatalog

- ${device.IsDefaultCatalog

DEP-Kontoname

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- ${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME

DEP Policy

- WINDOWS_HAS_DEP_POLICY
- ${device.WINDOWS_HAS_DEP_POLICY

DEP-Profil zugewiesen

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME

DEP-Profil per Push bereitgestellt

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME

DEP-Profil entfernt

- PROFILE_REMOVE_TIME
- ${device.PROFILE_REMOVE_TIME

DEP-Registrierung durch

- DEVICE_ASSIGNED_BY
- ${device.DEVICE_ASSIGNED_BY

DEP-Registrierungsdatum

- DEVICE_ASSIGNED_DATE
- ${device.DEVICE_ASSIGNED_DATE

Beschreibung

- BESCHREIBUNG
- ${device.DESCRIPTION

Geräte-ID

- Activesyncid
- ${device.activesyncid

Gerätemodell

- SYSTEM_OEM
- ${device.SYSTEM_OEM

Gerätename

- DEVICE_NAME
- ${device.DEVICE_NAME

Gerätetyp

- DEVICE_TYPE
- ${device.DEVICE_TYPE

‘Nicht stören’ aktiviert

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB

ELAM Driver Loaded?

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED

Verschlüsselungscompliance

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE

ENROLLMENT_KEY_GENERATION_DATE

- ENROLLMENT_KEY_GENERATION_DATE
- ${device.ENROLLMENT_KEY_GENERATION_DATE

Unternehmens-ID

- ENTERPRISEID
- ${device.ENTERPRISEID

Externer Speicher 1: Verfügbarer Speicherplatz

- EXTERNAL_STORAGE1_FREE_SPACE
- ${device.EXTERNAL_STORAGE1_FREE_SPACE

Externer Speicher 1: Name

- EXTERNAL_STORAGE1_NAME
- ${device.EXTERNAL_STORAGE1_NAME

Externer Speicher 1: Gesamtspeicherplatz

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE

Externer Speicher 2: Verfügbarer Speicherplatz

- EXTERNAL_STORAGE2_FREE_SPACE
- ${device.EXTERNAL_STORAGE2_FREE_SPACE

Externer Speicher 2: Name

- EXTERNAL_STORAGE2_NAME
- ${device.EXTERNAL_STORAGE2_NAME

Externer Speicher 2: Gesamtspeicherplatz

- EXTERNAL_STORAGE2_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE

Externer Speicher verschlüsselt

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION

FileVault aktiviert

- IS_FILEVAULT_ENABLED
- ${device.IS_FILEVAULT_ENABLED

Firewallstatus

- DEVICE_FIREWALL_STATUS
- ${device.DEVICE_FIREWALL_STATUS

Firewallstatus

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS

Firmwareversion

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION

Erste Synchronisierung

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC

Google Directory - Alias

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS

Google Directory - Familienname

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME

Google Directory - Name

- GOOGLE_AW_DIRECTORY_NAME

- ${device.GOOGLE_AW_DIRECTORY_NAME}

Google Directory - primäre E-Mail

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

Google Directory - Benutzer-ID

- GOOGLE_AW_DIRECTORY_USER_ID
- ${device.GOOGLE_AW_DIRECTORY_USER_ID}

GPS-Höhe

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS

GPS - Kurs

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS

GPS - horizontale Genauigkeit

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS

GPS-Breitengrad

- GPS_LATITUDE_FROM_GPS
- ${device.GPS_LATITUDE_FROM_GPS

GPS-Längengrad

- GPS_LONGITUDE_FROM_GPS
- ${device.GPS_LONGITUDE_FROM_GPS

GPS - Geschwindigkeit

- GPS_SPEED_FROM_GPS
- ${device.GPS_SPEED_FROM_GPS

GPS-Zeitstempel

- GPS_TIMESTAMP_FROM_GPS
- ${device.GPS_TIMESTAMP_FROM_GPS

GPS - vertikale Genauigkeit

- GPS_VERTICAL_ACCURACY_FROM_GPS
- ${device.GPS_VERTICAL_ACCURACY_FROM_GPS

Hardwaregeräte-ID

- HW_DEVICE_ID
- ${device.HW_DEVICE_ID

Hardwareverschlüsselung

- HARDWARE_ENCRYPTION_CAPS
- ${device.HARDWARE_ENCRYPTION_CAPS

HAS_CONTAINER

- HAS_CONTAINER
- ${device.HAS_CONTAINER

Hash des aktuell angemeldeten iTunes-Storekontos

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH

Netzbetreiber für Heimnetzwerk

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK

Heimatländercode für mobiles Gerät

- SIM_MCC
- ${device.SIM_MCC

Code für mobiles Heimnetzwerk

- SIM_MNC
- ${device.SIM_MNC

ICCID

- ICCID
- ${device.ICCID

Identität

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY

IMEI/MEID-Nummer

- IMEI
- ${device.IMEI

IMSI

- SIM_ID
- ${device.SIM_ID

Interner Speicher verschlüsselt

- LOCAL_ENCRYPTION
- ${device.LOCAL_ENCRYPTION

IP-Standort

- IP_LOCATION
- ${device.IP_LOCATION

IPv4-Adresse

- IP_ADDRESSV4
- ${device.IP_ADDRESSV4

IPv6-Adresse

- IP_ADDRESSV6
- ${device.IP_ADDRESSV6

Issued At

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT

Jailbreak/Rooting

- ROOT_ACCESS
- ${device.ROOT_ACCESS

Kernel Debugging Enabled?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED

KIOSK-Modus

- IS_KIOSK
- ${device.IS_KIOSK

Letzte bekannte IP-Adresse

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR

Zeit der letzten Richtlinienaktualisierung

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME

Datum des letzten Scans

- PreviousScanDate

- ${device.PreviousScanDate

Ergebnis des letzten Scans

- PreviousScanResult
- ${device.PreviousScanResult

Letztes geplantes Softwareupdate

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME

Fehlermeldung für letztes geplantes Softwareupdate

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG

Status des letzten geplanten Softwareupdates

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS

Letzte Synchronisierung

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC

Ortungsdienst aktiviert

- DEVICE_LOCATOR
- ${device.DEVICE_LOCATOR

MAC-Adresse

- MAC_ADDRESS
- ${device.MAC_ADDRESS

Netzwerkverbindung per MAC-Adresse

- MAC_NETWORK_CONNECTION
- ${device.MAC_NETWORK_CONNECTION

MAC-Adresstyp

- MAC_ADDRESS_TYPE
- ${device.MAC_ADDRESS_TYPE

Postfachsetup

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- ${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP

Hauptakku

- MAIN_BATTERY_PERCENT
- ${device.MAIN_BATTERY_PERCENT

MDM-Modus ‘Verloren’ aktiviert

- IS_MDM_LOST_MODE_ENABLED
- ${device.IS_MDM_LOST_MODE_ENABLED

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- ${device.MDX_SHARED_ENCRYPTION_KEY

MEID

- MEID
- ${device.MEID

Mobiltelefonnummer

- TEL_NUMBER
- ${device.TEL_NUMBER

Modell-ID

- MODEL_ID
- ${device.MODEL_ID}

Modellnummer

- MODEL_NUMBER
- ${device.MODEL_NUMBER

Netzwerkadaptertyp

- NETWORK_ADAPTER_TYPE
- ${device.NETWORK_ADAPTER_TYPE

Betriebssystembuild

- SYSTEM_OS_BUILD
- ${device.SYSTEM_OS_BUILD

Edition des Betriebssystems

- OS_EDITION
- ${device.OS_EDITION

Betriebssystemsprache (Gebietsschema)

- SYSTEM_LANGUAGE
- ${device.SYSTEM_LANGUAGE

Betriebssystemversion

- SYSTEM_OS_VERSION
- ${device.SYSTEM_OS_VERSION

Adresse der Organisation

- ORGANIZATION_ADDRESS
- ${device.ORGANIZATION_ADDRESS

Geschäftliche E-Mail-Adresse

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL

Organization Magic

- ORGANIZATION_MAGIC
- ${device.ORGANIZATION_MAGIC

Name der Organisation

- ORGANIZATION_NAME
- ${device.ORGANIZATION_NAME

Telefonnummer der Organisation

- ORGANIZATION_PHONE
- ${device.ORGANIZATION_PHONE

Nicht richtlinientreu

- OUT_OF_COMPLIANCE
- ${device.OUT_OF_COMPLIANCE

Besitz von

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED

Passcode richtlinientreu

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT

Passcode richtlinientreu gemäß Konfiguration

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG

Passcode vorhanden

- PASSCODE_PRESENT

- ${device.PASSCODE_PRESENT

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0

Umkreisverletzung

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH

Periodische Prüfung

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck

Persönlicher Hotspot aktiviert

- PERSONAL_HOTSPOT_ENABLED
- ${device.PERSONAL_HOTSPOT_ENABLED

PIN-Code für Geofence

- PIN_CODE_FOR_GEO_FENCE
- ${device.PIN_CODE_FOR_GEO_FENCE

Plattform

- SYSTEM_PLATFORM
- ${device.SYSTEM_PLATFORM}

API-Level der Plattform

- API_LEVEL
- ${device.API_LEVEL

Richtlinienname

- POLICY_NAME
- ${device.POLICY_NAME

Primäre Telefonnummer

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER

Anbieter der primären SIM

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR

Primäre SIM-ICCID

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID

Primäre SIM, IMEI

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI

Primäre SIM, IMSI

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI

Primäre SIM, Roaming

- IDENTITY1_ROAMING
- ${device.IDENTITY1_ROAMING

Roamingcompliance für primäre SIM

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE

Produktname

- PRODUCT_NAME
- ${device.PRODUCT_NAME

Geräte-ID des Herausgebers

- PUBLISHER_DEVICE_ID
- ${device.PUBLISHER_DEVICE_ID

Reset Count

- WINDOWS_HAS_RESET_COUNT
- ${device.WINDOWS_HAS_RESET_COUNT

Restart Count

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT

Safe Mode aktiviert?

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE

Samsung KNOX API verfügbar

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX

Samsung KNOX API-Version

- SAMSUNG_KNOX_VERSION
- ${device.SAMSUNG_KNOX_VERSION

Samsung KNOX-Nachweis

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED

Aktualisierungsdatum für Samsung KNOX-Nachweis

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- ${device.SAMSUNG_KNOX_ATT_UPDATED_TIME

Samsung SAFE API verfügbar

- SAMSUNG_MDM
- ${device.SAMSUNG_MDM

Samsung SAFE API-Version

- SAMSUNG_MDM_VERSION
- ${device.SAMSUNG_MDM_VERSION

SBCP Hash

- WINDOWS_HAS_SBCP_HASH
- ${device.WINDOWS_HAS_SBCP_HASH

Bildschirm: Höhe

- SCREEN_HEIGHT
- ${device.SCREEN_HEIGHT

Bildschirm: Anzahl der Farben

- SCREEN_NB_COLORS
- ${device.SCREEN_NB_COLORS

Bildschirm: Größe

- SCREEN_SIZE
- ${device.SCREEN_SIZE

Bildschirm: Breite

- SCREEN_WIDTH
- ${device.SCREEN_WIDTH

Bildschirm: Auflösung X-Achse

- SCREEN_XDPI

- ${device.SCREEN_XDPI

Bildschirm: Auflösung Y-Achse

- SCREEN_YDPI
- ${device.SCREEN_YDPI

Sekundäre Telefonnummer

- IDENTITY2_PHONENUMBER
- ${device.IDENTITY2_PHONENUMBER

Anbieter der sekundären SIM

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR

Sekundäre SIM-ICCID

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID

Sekundäre SIM, IMEI

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI

Sekundäre SIM, IMSI

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI

Sekundäre SIM, Roaming

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING

Roamingcompliance für sekundäre SIM

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE

Secure Boot aktiviert?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED

Status von Secure Boot

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE

SecureContainer aktiviert

- DLP_ACTIVE
- ${device.DLP_ACTIVE

Sicherheitspatchebene

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL

Seriennummer

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER

SMS-fähig

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE

Betreut

- SUPERVISED
- ${device.SUPERVISED

Grund für vorübergehende Sperrung

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON

Manipulierter Status

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS

AGB

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS

Nutzungsbedingungen und Vereinbarung angenommen?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS

Testsignierung aktiviert?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED

Gesamt-RAM

- MEMORY
- ${device.MEMORY

Speicherplatz gesamt

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE

TPM-Version

- TPM_VERSION
- ${device.TPM_VERSION

UDID

- UDID
- ${device.UDID}

Status der Benutzerkontensteuerung

- UAC_STATUS
- ${device.UAC_STATUS

Benutzeragent

- USER_AGENT
- ${device.USER_AGENT

Benutzerdefiniert 1

- USER_DEFINED_1
- ${device.USER_DEFINED_1

Benutzerdefiniert 2

- USER_DEFINED_2
- ${device.USER_DEFINED_2

Benutzerdefiniert 3

- USER_DEFINED_3
- ${device.USER_DEFINED_3

Benutzersprache (Gebietsschema)

- USER_LANGUAGE
- ${device.USER_LANGUAGE

Anbieter

- VENDOR
- ${device.VENDOR

Sprachfähig

- IS_VOICE_CAPABLE

- ${device.IS_VOICE_CAPABLE

Sprachroaming zugelassen

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED

VSM aktiviert?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED

WiFi MAC-Adresse

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- ${device.WINDOWS_ENROLLMENT_KEY

WinPE Enabled?

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE

WNS-Benachrichtigungsstatus

- PROPERTY_WNS_PUSH_STATUS
- ${device.PROPERTY_WNS_PUSH_STATUS

URL für WNS-Benachrichtigung

- PROPERTY_WNS_PUSH_URL
- ${device.PROPERTY_WNS_PUSH_URL

Ablaufdatum der URL für WNS-Benachrichtigung

- PROPERTY_WNS_PUSH_URL_EXPIRY
- ${device.PROPERTY_WNS_PUSH_URL_EXPIRY

XenMobile-Agent-ID

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID

XenMobile-Agentrevision

- EW_REVISION
- ${device.EW_REVISION

XenMobile-Agentversion

- EW_VERSION
- ${device.EW_VERSION

Zebra API verfügbar

- ZEBRA_MDM
- ${device.ZEBRA_MDM

Zebra MXMF-Version

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION

Zebra Patch-Version

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

Makros zum Abrufen integrierter Benutzereigenschaften

Anzeigename	Makros
domainname (Domänenname; Standarddomäne)	`${ user.domainname }`
Loginname (Benutzername plus Domänenname)	`${ user.loginname }`
Benutzername (Loginname gegebenenfalls ohne Domäne)	`${ user.username }`

Makros für alle Benutzereigenschaften

Anzeigename	Webelement	Makros
Active Directory-Anmeldeversuchsfehler	badpwdcount	`${ user.badpwdcount }`
ActiveSync-Benutzer-E-Mail	asuseremail	`${ user.asuseremail }`
ASM-Datenquelle	asmpersonsource	`${ user.asmpersonsource }`
ASM-DEP-Kontoname	asmdepaccount	`${ user.asmdepaccount }`

Anzeigename	Webelement	Makros
ASM-verwaltete Apple-ID	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
ASM-Passcodetyp	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
ASM-Personen-ID	asmpersonid	${ user.asmpersonid }
ASM-Personenstatus	asmpersonstatus	${ user.asmpersonstatus }
ASM-Anrede	asmpersontitle	${ user.asmpersontitle }
ASM eindeutige Personen-ID	asmpersonuniqueid	${ user.asmpersonuniqueid }
ASM-Quellsystem-ID	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
ASM-Klassenstufe	asmpersongrade	${ user.asmpersongrade }
BES-Benutzer-E-Mail	besuseremail	${ user.besuseremail }
Firma	Firma	${ user.company }
Firmenname	companyname	${ user.companyname }
Land	c	${ user.c }
Abteilung	department	${ user.department }
Beschreibung	Beschreibung	${ user.description }
Deaktivierter Benutzer	disableduser	${ user.disableduser }
Anzeigename	Anzeigename	${ user.displayname }
Distinguished Name	distinguishedname	${ user.distinguishedname }
Domänenname	domainname	${ user.domainname }
E-Mail	mail	${ user.mail }
Vorname	givenname	${ user.givenname }

Anzeigename	Webelement	Makros
Adresse (privat)	homestreetaddress	${ user.homestreetaddress }
Stadt (privat)	homecity	${ user.homecity }
Land (privat)	homecountry	${ user.homecountry }
Fax (privat)	homefax	${ user.homefax }
Telefon (privat)	homephone	${ user.homephone }
Bundesland/Kanton (privat)	homestate	${ user.homestate }
Postleitzahl (privat)	homezip	${ user.homezip }
IP-Telefon	ipphone	${ user.ipphone }
Weitere Vornamen	middleinitial	${ user.middleinitial }
Weiterer Vorname	middlename	${ user.middlename }
Mobil	mobile	${ user.mobile }
Name	cn	${ user.cn }
Adresse (Büro)	physicaldeliveryofficename	${ user.physicaldeliveryofficename }
Stadt (Büro)	l	${ user.l }
Fax (Büro)	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
Bundesland/Kanton (Büro)	st	${ user.st }
Straße (Büro)	officestreetaddress	${ user.officestreetaddress }
Telefonnummer (Büro)	telephonenumber	${ user.telephonenumber }
Postleitzahl (Büro)	postalcode	${ user.postalcode }
Postfach	postofficebox	${ user.postofficebox }
Pager	pager	${ user.pager }
Primäre Gruppen-ID	primarygroupid	${ user.primarygroupid }

Anzeigename	Webelement	Makros
SAM-Konto	samaccountname	`${ user.samaccountname }`
Straße	streetaddress	`${ user.streetaddress }`
Nachname	sn	`${ user.sn }`
Titel	title	`${ user.title }`
Benutzeranmeldename	userprincipalname	`${ user.userprincipalname }`

Automatisierte Aktionen

January 5, 2022

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 über Auslöser die Auswirkungen auf den Geräten von Benutzern fest, wenn diese mit XenMobile verbunden sind. Wenn ein Ereignis ausgelöst wird, können Sie eine Nachricht mit einer Aufforderung zur Problembeseitigung an den betroffenen Benutzer senden, bevor Maßnahmen ergriffen werden.

Sie können folgende automatische Auswirkungen festlegen:

- Vollständige oder selektive Datenlöschung
- Einstufung von Geräten als nicht richtlinientreu
- Widerrufen von Geräten
- Senden einer Benachrichtigung an Benutzer mit der Aufforderung zur Problembehebung

Sie können Aktionen für App-Sperre und App löschen für den Nur-MAM-Modus konfigurieren.

> **Hinweis:**
>
> Sie können Benutzer nur benachrichtigen, wenn Sie in den XenMobile-Einstellungen Benachrichtigungsserver für SMTP und SMS konfiguriert haben, damit XenMobile Nachrichten senden kann. Weitere Informationen finden Sie unter Benachrichtigungen. Richten Sie, bevor Sie fortfahren, außerdem alle Benachrichtigungsvorlagen ein, die Sie verwenden möchten. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Benachrichtigungsvorlagen.

Beispielaktionen

Beispiele für die Verwendung automatisierter Aktionen:

Erstes Beispiel

- Sie möchten eine App (z. B. Words with Friends) erkennen, die Sie auf die Sperrliste gesetzt haben. Sie können einen Auslöser festlegen, durch den ein Benutzergerät als nicht richtlinientreu eingestuft wird, wenn die App "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 auch ein Limit für die Wartezeit auf die Reaktion der Benutzer festlegen. Nach Ablauf des Zeitlimits erfolgt eine definierte Aktion, beispielsweise das selektive Löschen des Geräts.

Zweites Beispiel

- Sie möchten überprüfen, ob Kunden die neueste Firmware verwenden, und den Zugriff auf Ressourcen blockieren, wenn Benutzer ihre Geräte aktualisieren müssen. Sie können einen Auslöser festlegen, durch den ein Benutzergerät als nicht richtlinientreu eingestuft wird, wenn nicht die neueste Version auf dem Gerät installiert ist. Sie verwenden automatisierte Aktionen, um Ressourcen zu blockieren und Kunden zu benachrichtigen.

Drittes Beispiel

- Ein Benutzergerät wird in einen nicht richtlinientreuen Zustand versetzt und der Benutzer behebt das Problem. Sie können eine Richtlinie zur Bereitstellung eines Pakets konfigurieren, das das Gerät in einen richtlinientreuen Zustand zurücksetzt.

Viertes Beispiel

- Sie möchten Benutzergeräte, die eine bestimmte Zeitlang inaktiv waren, als nicht richtlinientreu markieren. Sie können eine automatisierte Aktion für inaktive Geräte wie folgt erstellen:

  1. Gehen Sie in der XenMobile-Konsole zu **Einstellungen > Netzwerkzugriffssteuerung** und wählen Sie **Inaktive Geräte**. Weitere Informationen über die Einstellung **Inaktive Geräte** finden Sie unter Netzwerkzugriffssteuerung.
  2. Führen Sie die unter Hinzufügen und Verwalten von Aktionen beschriebenen Schritte aus, um eine Aktion hinzuzufügen. Der einzige Unterschied besteht in der Wahl folgender Konfiguration auf der Seite **Aktionsdetails**:
     - **Auslöser:** Wählen Sie **Geräteeigenschaft**, **Nicht richtlinientreu** und **Wahr**.
     - **Aktion**. Wählen Sie **Benachrichtigung senden** und dann eine unter **Benachrichtigungsvorlage** > **Einstellungen** erstellte Vorlage. Legen Sie die Verzögerung bis zum Ausführen der Aktion in Tagen, Stunden oder Minuten fest. Legen Sie das Intervall fest, in dem die Aktion wiederholt wird, bis der Benutzer reagiert.

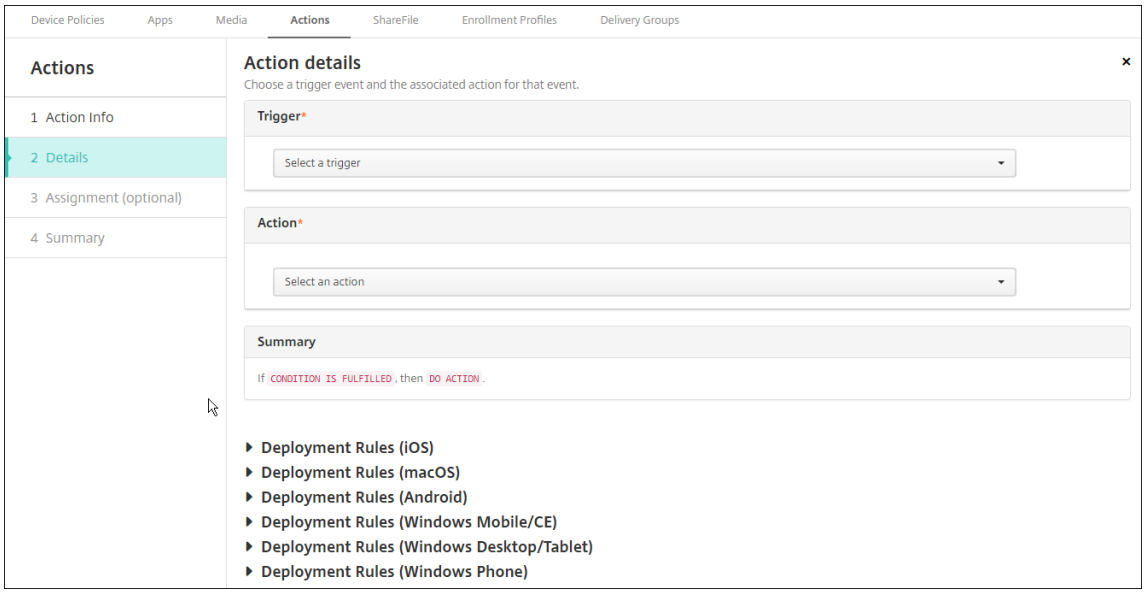
> **Tipp:**
>
> Zum Löschen inaktiver Geräte in großen Mengen verwenden Sie Public API for REST Services. Sie beschaffen zunächst manuell die IDs der inaktiven Geräte und führen dann die Lösch-API aus, um sie in einem Durchgang zu löschen.

Hinzufügen und Verwalten von Aktionen

Hinzufügen, Bearbeiten und Filtern von automatisierten Aktionen:

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 Aktion hinzuzufügen.
   - Wählen Sie eine vorhandene Aktion zum Bearbeiten oder Löschen aus. Klicken Sie auf die gewünschte Option.
3. Die Seite **Aktionsinformationen** wird angezeigt.
4. Konfigurieren Sie auf der Seite **Aktionsinformationen** die folgenden Informationen:
   - **Name:** Geben Sie einen Namen zur Identifizierung der Aktion ein. Diese Angabe ist erforderlich.
   - **Beschreibung:** Geben Sie eine Beschreibung dessen ein, was die Aktion bewirkt.
5. Klicken Sie auf **Weiter**. Die Seite **Aktionsdetails** wird angezeigt.

   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 vordefiniertes Ereignis.
   - **Geräteeigenschaft:** prüft mit MDM verwaltete Geräte auf ein Geräteattribut und reagiert darauf. Weitere Informationen finden Sie unter Namen und Werte von Geräteeigenschaften.
   - **Benutzereigenschaft:** reagiert auf ein Benutzerattribut, normalerweise aus Active Directory.
   - **Name der installierten App:** reagiert auf eine App, die gerade installiert wird. 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 App-Bestandsrichtlinien für Geräte.

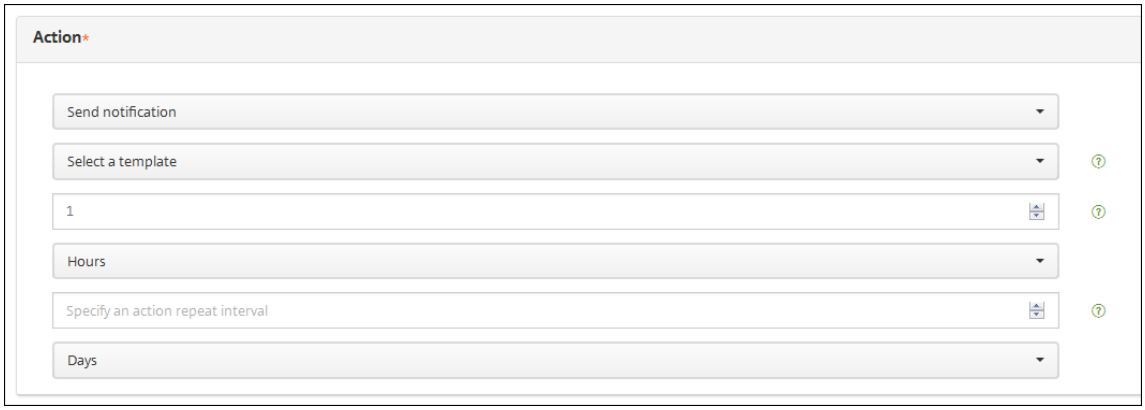
7. Klicken Sie in der nächsten Liste auf die Reaktion auf den Auslöser.

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. Definitionen der Aktionen, finden Sie unter Sicherheitsaktionen.

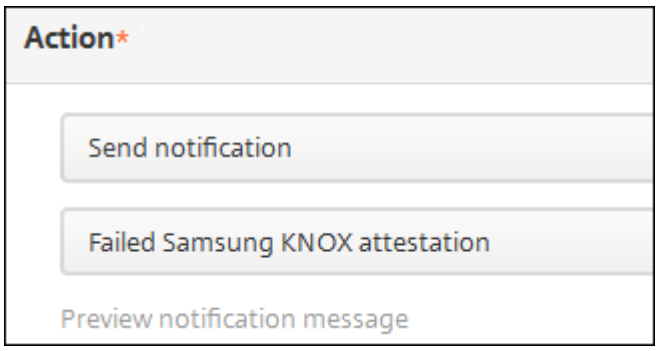
   Wenn Sie die Option **Benachrichtigung senden** auswählen, führen Sie die folgenden Schritte aus, um eine Benachrichtigungsaktion zu erstellen.

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**.

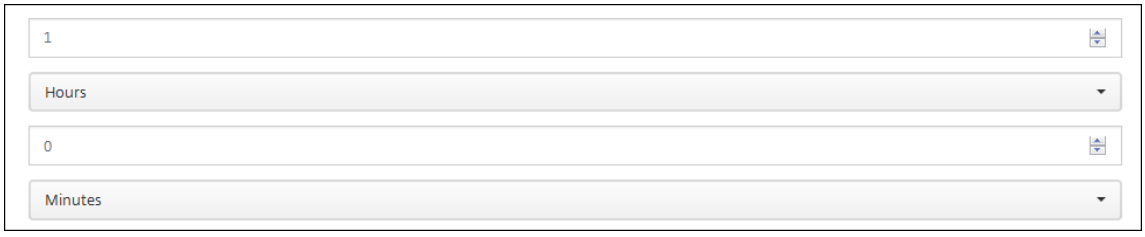
   Sie können Benutzer nur benachrichtigen, wenn Sie unter “Einstellungen” Benachrichtigungsserver für SMTP und SMS konfiguriert haben, damit XenMobile Nachrichten senden kann (siehe Benachrichtigungen). Richten Sie, bevor Sie fortfahren, außerdem alle Benachrichtigungsvorlagen ein, die Sie verwenden möchten. Weitere Informationen zum Einrichten von Benachrichtigungsvorlagen finden Sie unter Erstellen und Aktualisieren von Benachrichtigungsvorlagen.



Nach Auswahl der Vorlage können Sie diese in der Vorschau anzeigen, indem Sie auf **Vorschau für Benachrichtigung** klicken.



10. Legen Sie in den folgenden Feldern die Verzögerung bis zum Ausführen der Aktion in Tagen, Stunden oder Minuten fest. Legen Sie das Intervall fest, in dem die Aktion wiederholt wird, bis der Benutzer reagiert.



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 Bereitstellungsregeln. Allgemeine Informationen zum Konfigurieren der Bereitstellungsregeln finden Sie unter Bereitstellen von Ressourcen.

    Im vorliegenden Beispiel:

    - Der Gerätebesitz muss **BYOD** sein.
    - Die lokale Geräteverschlüsselung muss auf **True** festgelegt sein.
    - Das Gerät muss passcode-richtlinientreu sein.
    - Der MCC des Geräts kann nicht nur Andorra sein.

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 Gruppen in der Liste 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** wählen, sind keine weiteren Optionen erforderlich.
    - 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.

    Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

17. Klicken Sie auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt, auf der Sie die Konfiguration der Aktion prüfen können.

18. Klicken Sie auf **Speichern**, um die Aktion zu speichern.

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

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:

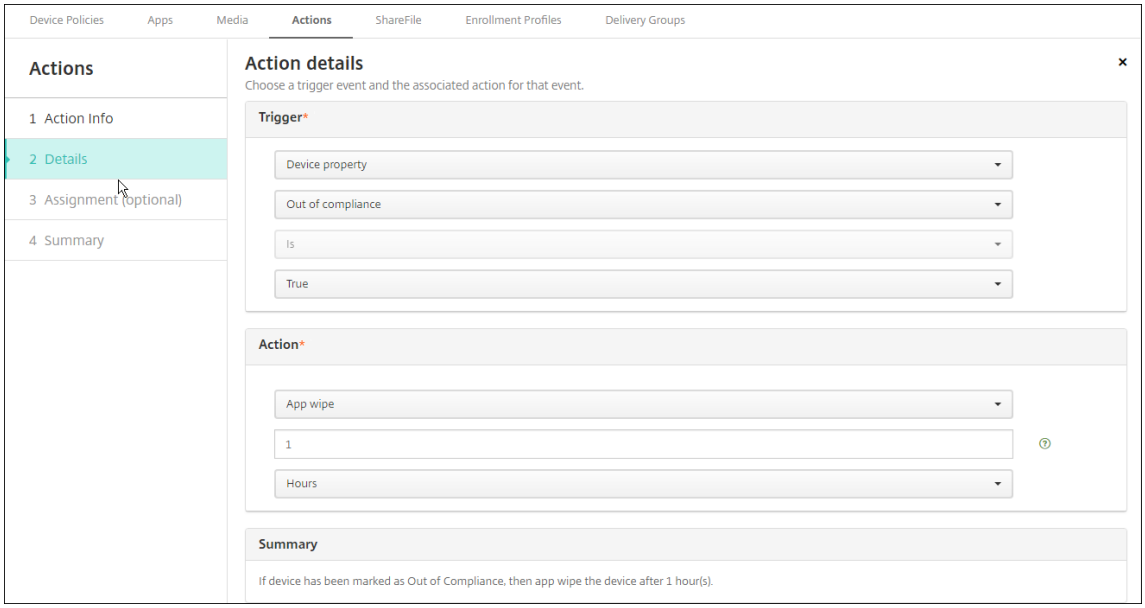
   Wenn der Auslösertyp **Ereignis** und der Wert nicht **Active Directory, deaktivierter Benutzer** ist, werden die Aktionen **App löschen** und **App sperren** nicht angezeigt.

   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 soll den Benutzern Zeit geben, ein Problem zu beheben, bevor die Aktion ausgeführt wird. Weitere Informationen zu den Aktionen zum Löschen und Sperren von Apps finden Sie unter Sicherheitsaktionen.

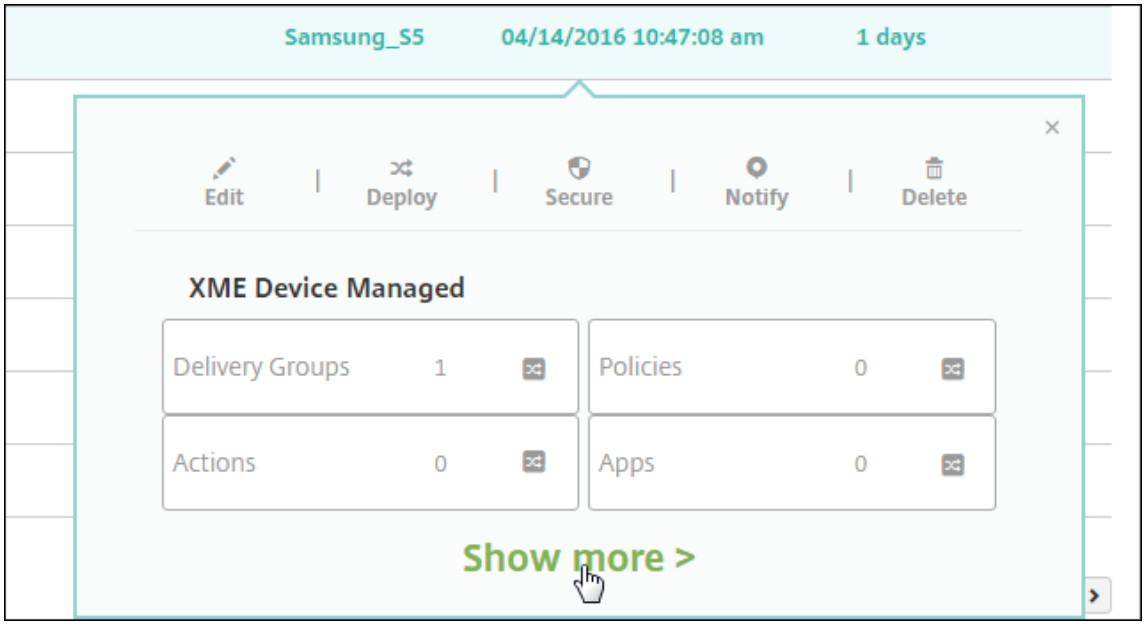
   > **Hinweis:**
   >
   > Wenn Sie den Auslöser auf **Ereignis** festlegen, wird als Wiederholungsintervall automatisch mindestens 1 Stunde festgelegt. Das Gerät muss eine Aktualisierung der Richtlinien zur Synchronisierung mit dem Server ausführen, damit Benachrichtigung empfangen werden. Normalerweise 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 1 Stunde vor der Ausführung der Aktion ist möglich, damit die Active Directory-Datenbank mit XenMobile synchronisiert werden kann.



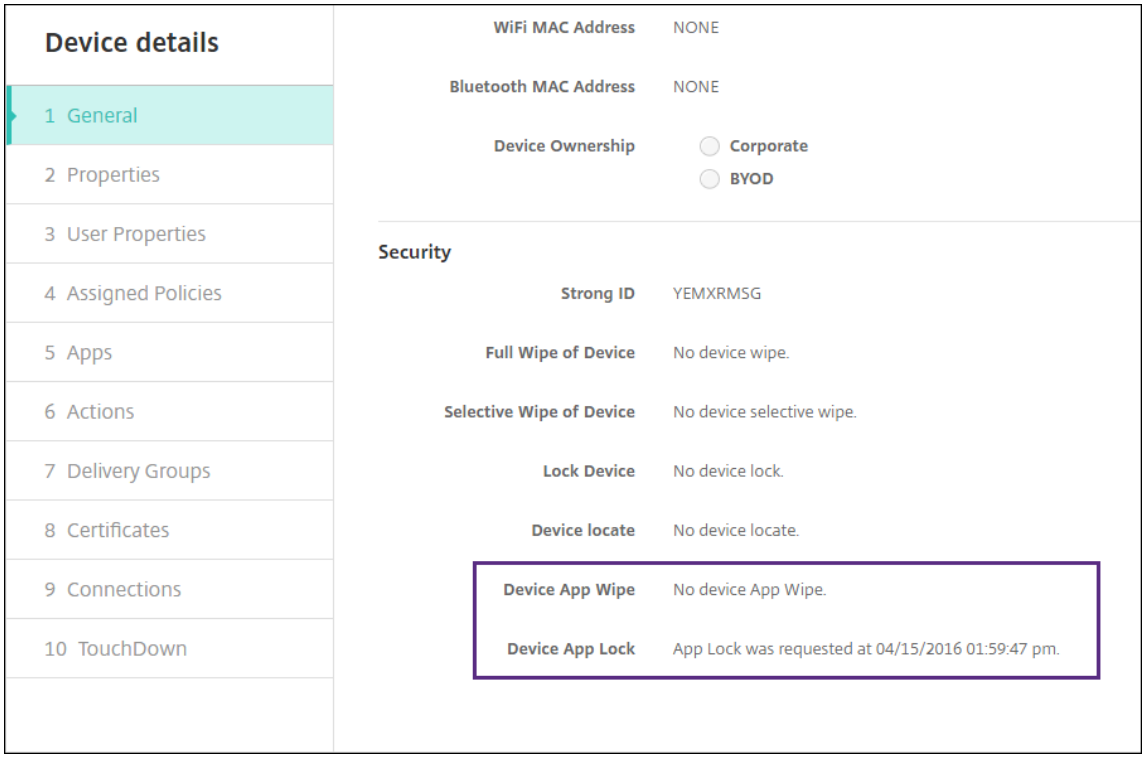
6. Konfigurieren Sie die Bereitstellungsregeln und klicken Sie auf **Weiter**.
7. Konfigurieren Sie die Zuweisungen für Bereitstellungsgruppen und einen Bereitstellungszeitplan, und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Speichern**.

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.



Nach einer Löschung wird der Benutzer aufgefordert, einen PIN-Code einzugeben. Wenn der Benutzer diesen Code vergessen hat, können Sie ihn in den Gerätedetails nachsehen.

Support und Überwachung

January 21, 2021

Nutzen Sie das XenMobile-Dashboard und die XenMobile-Supportseite zur Überwachung und zum Support von XenMobile Server. Auf der Seite “XenMobile Support” finden Sie Supportinformationen und -tools.

Bei einem on-premises XenMobile Server können Sie Aktionen auch über die Befehlszeilenschnittstelle von XenMobile ausführen. Einzelheiten finden Sie unter Optionen für die Befehlszeilenschnittstelle.

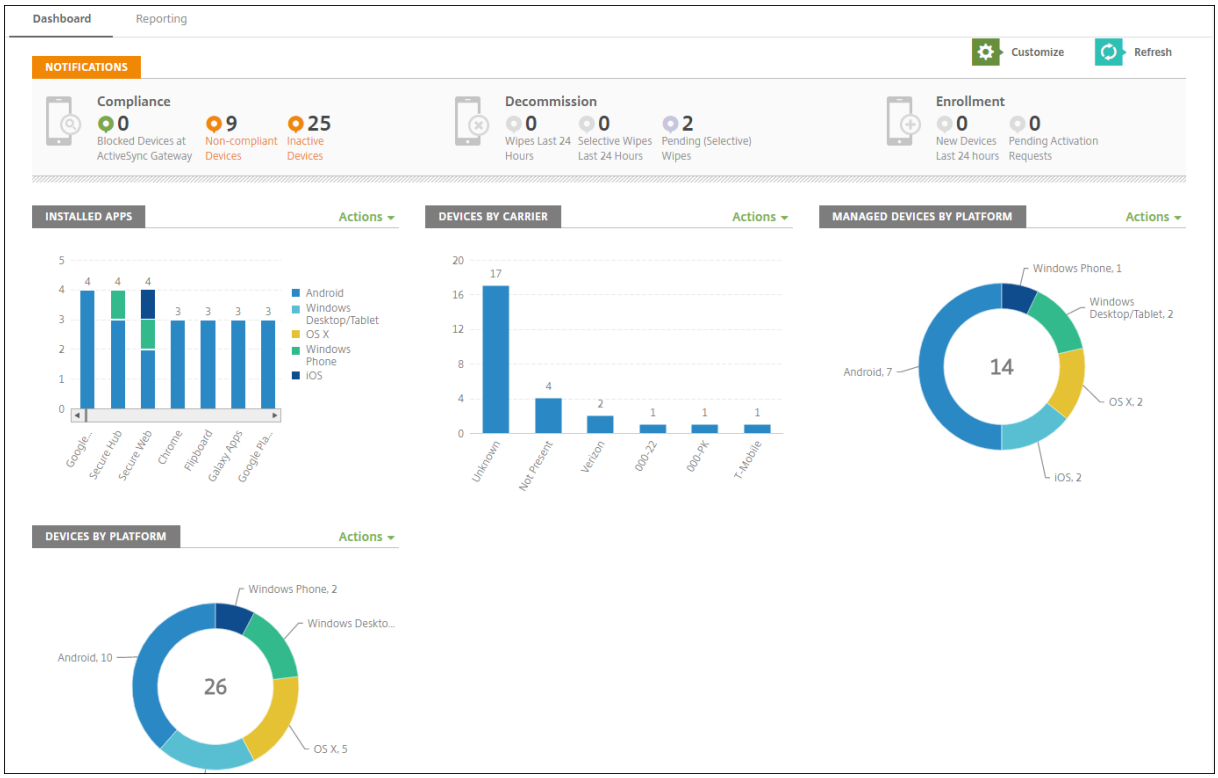
Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben.

Die Seite Problembehandlung und Support wird angezeigt.

Verwenden Sie die Seite **Support** von XenMobile für Folgendes:

- Diagnose
- Erstellen von Supportpaketen (nur für on-premises Installationen).
- Zugriff auf Links zur Citrix Produktdokumentation und Knowledge Center
- Zugriff auf Protokollvorgänge
- Erweiterte Konfigurationsoptionen
- Zugriff auf diverse Tools und Hilfsprogramme

Das Dashboard der XenMobile-Konsole ermöglicht die übersichtliche Anzeige von Informationen auf einen Blick. Mit diesen Informationen können Sie Probleme und erfolgreiche Aktionen schnell mit Widgets erfassen.



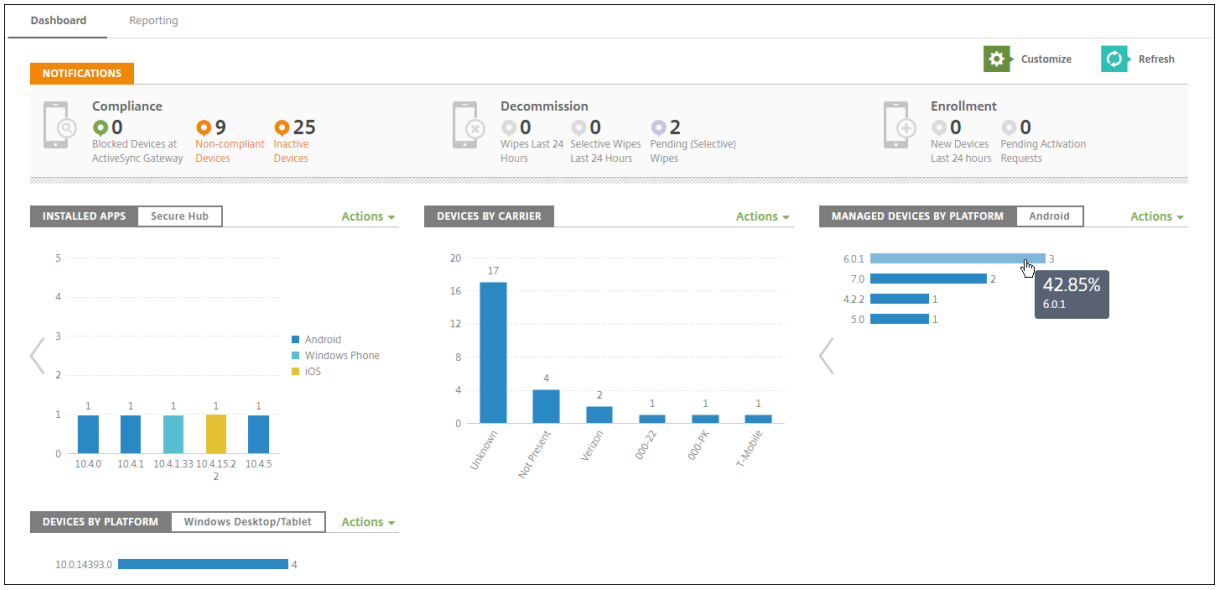
Das Dashboard ist normalerweise die erste Seite, die beim Anmelden bei der XenMobile-Konsole angezeigt wird. Um das Dashboard von anderer Stelle aus aufzurufen, klicken Sie auf **Analysieren**. Klicken Sie im Dashboard auf **Anpassen**, um das Seitenlayout und die angezeigten Widgets zu bearbeiten.

- **Meine Dashboards:** Sie können bis zu vier Dashboards speichern. Sie können diese Dashboards separat bearbeiten und jeweils durch Auswahl des gespeicherten Dashboards anzeigen.
- **Layoutstil:** In dieser Zeile können Sie auswählen, wie viele Widgets auf dem Dashboard angezeigt und wie sie angeordnet werden.
- **Widgetauswahl:** Legen Sie fest, welche Informationen auf dem Dashboard angezeigt werden.
  - **Benachrichtigungen:** Aktivieren Sie das Kontrollkästchen über den Ziffern auf der linken Seite, um eine Benachrichtigungsleiste über den Widgets hinzuzufügen. Diese Leiste zeigt

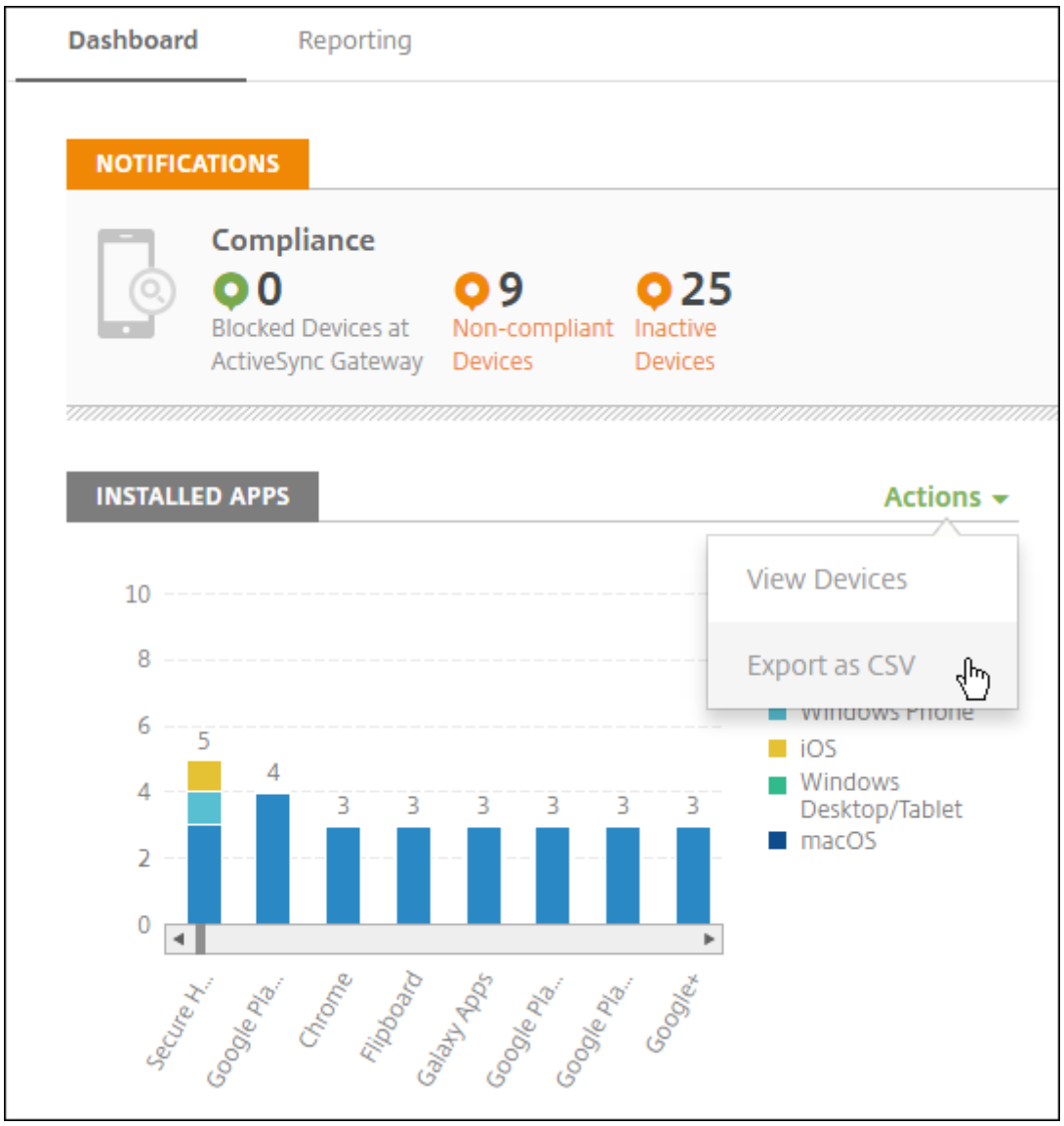
die Anzahl der richtlinientreuen Geräte, der inaktiven Geräte und der Geräte, die in den vergangenen 24 Stunden gelöscht oder registriert wurden.

- **Geräte nach Plattform:** Anzahl der verwalteten und nicht verwalteten Geräte pro Plattform.
- **Geräte nach Netzbetreiber:** Anzahl der verwalteten und nicht verwalteten Geräte pro Netzbetreiber. Klicken Sie auf die einzelnen Balken, um eine Aufschlüsselung nach Plattform anzuzeigen.
- **Verwaltete Geräte nach Plattform:** Anzahl der verwalteten Geräte pro Plattform.
- **Nicht verwaltete Geräte nach Plattform:** Anzahl der nicht verwalteten Geräte pro Plattform. Auf den Geräten in diesem Diagramm ist möglicherweise ein Agent installiert, ihre Privilegien wurden jedoch widerrufen oder sie wurden gelöscht.
- **Geräte nach ActiveSync-Gateway-Status:** Anzahl der Geräte gruppiert nach ActiveSync-Gateway-Status. Statusangaben werden unterteilt in "Blockiert", "Zugelassen" oder "Unbekannt". Mit einem Klick auf die einzelnen Balken können Sie die Angaben nach Plattform aufschlüsseln lassen.
- **Geräte nach Besitzer:** Anzahl der Geräte gruppiert nach Besitzerstatus. Statusangaben werden unterteilt in Unternehmens- oder Mitarbeiterbesitz oder Unbekannt.
- **Fehlerhafte Bereitstellungen von Bereitstellungsgruppen:** Gesamtzahl fehlgeschlagener Bereitstellungen pro Paket. Nur Pakete mit fehlgeschlagenen Bereitstellungen werden angezeigt.
- **Geräte nach Grund für das Blockieren:** Anzahl der Geräte, die von ActiveSync blockiert wurden.
- **Installierte Apps:** Geben Sie einen App-Namen für ein Diagramm mit App-Informationen ein.
- **Volume Purchas Apps-Lizenznutzung:** Zeigt statistische Angaben zur Nutzung von Lizenzen für Volumen Purchase Apps von Apple.

Mit jedem Widget können Sie auf einzelne Bestandteile klicken, um weitere Informationen zu erhalten.



Sie können die Informationen auch als CSV-Datei exportieren. Klicken Sie hierfür auf das Dropdown-Menü **Aktionen**.



Anonymisierung von Daten in Supportpaketen

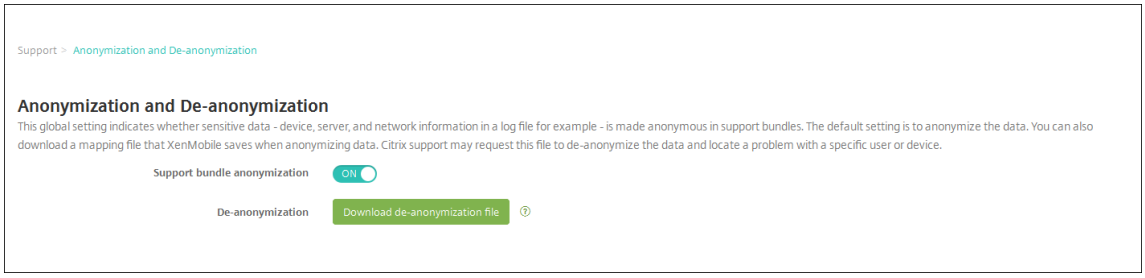
January 5, 2022

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

1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite

Support wird angezeigt.

2. Klicken Sie auf der Seite **Support** unter **Erweitert** auf **Anonymisierung und Deanonymisierung**. Die Seite **Anonymisierung und Deanonymisierung** wird angezeigt.



3. Wählen Sie unter **Supportpaketanonymisierung** aus, ob die Daten anonymisiert werden sollen. Die Standardeinstellung ist **Ein**.
4. Klicken Sie neben **Deanonymisierung** auf **Deanonymisierungsdatei herunterladen**, um die Zuordnungsdatei an den Citrix Support zu senden, wenn dieser spezifische Geräte- oder Benutzerinformationen zur Problemdiagnose benötigt.

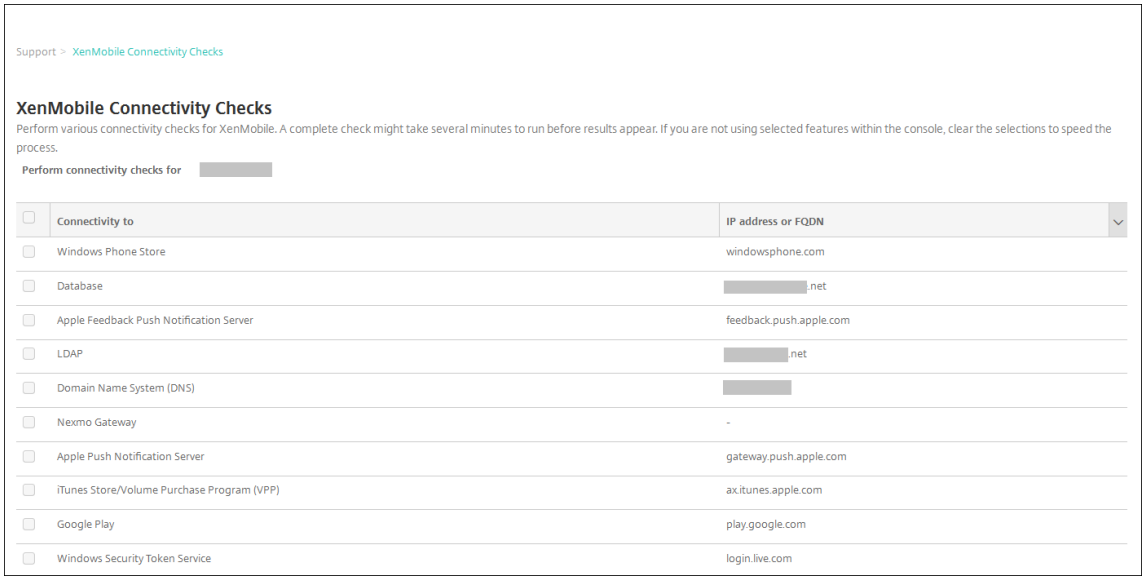
Konnektivitätsprüfungen

November 10, 2020

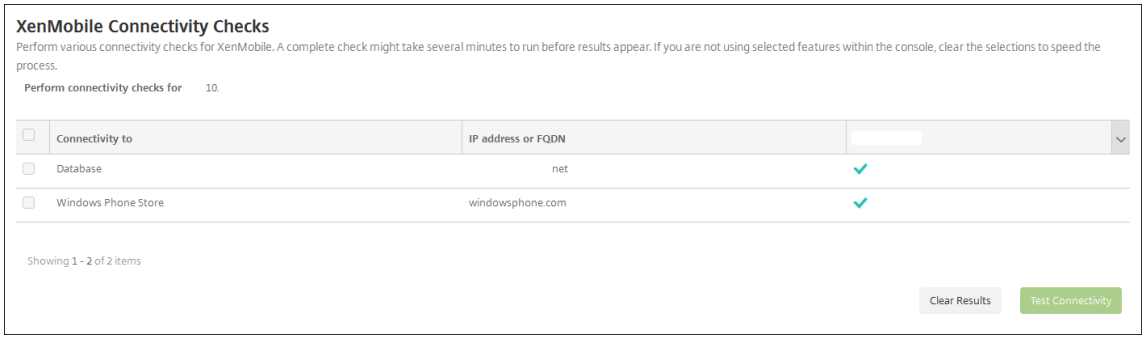
Über die Seite **Support** können Sie die Verbindung zwischen XenMobile und Citrix Gateway sowie XenMobile und anderen Servern und Speicherorten prüfen.

Prüfen von XenMobile-Verbindungen

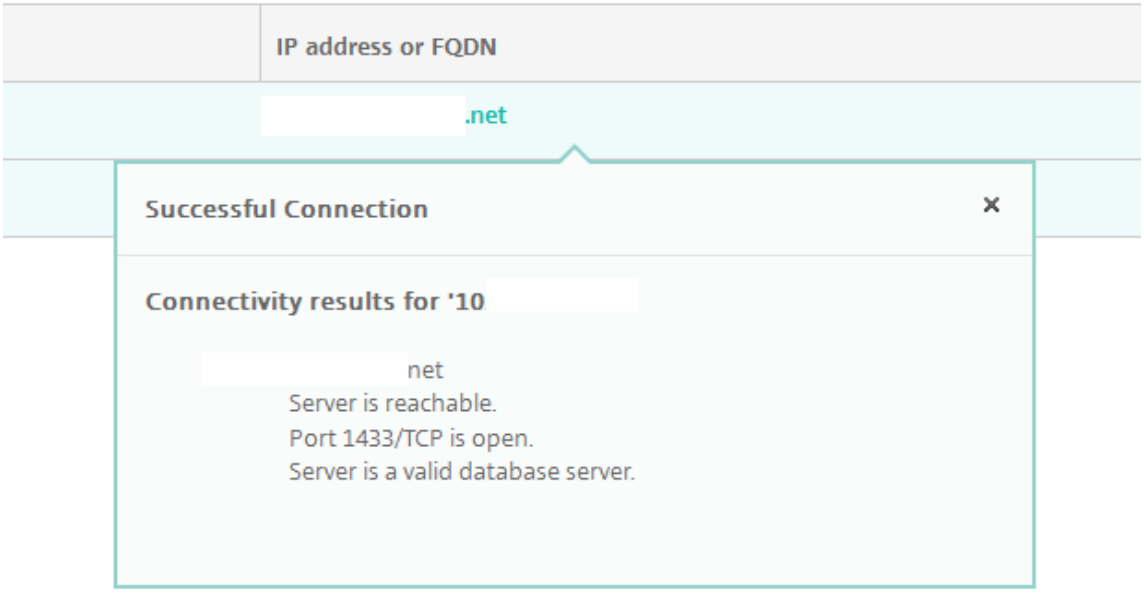
1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite **Support** wird angezeigt.
2. Klicken Sie unter **Diagnose** auf **XenMobile-Konnektivitätsprüfung**. Die Seite **XenMobile-Konnektivitätsprüfung** wird angezeigt. Wenn die XenMobile-Umgebung Clusterknoten enthält, werden alle Knoten angezeigt.



3. Wählen Sie die Server aus, deren Verbindung geprüft werden soll, und klicken Sie dann auf **Konnektivität testen**. Die Testergebnisseite wird angezeigt.

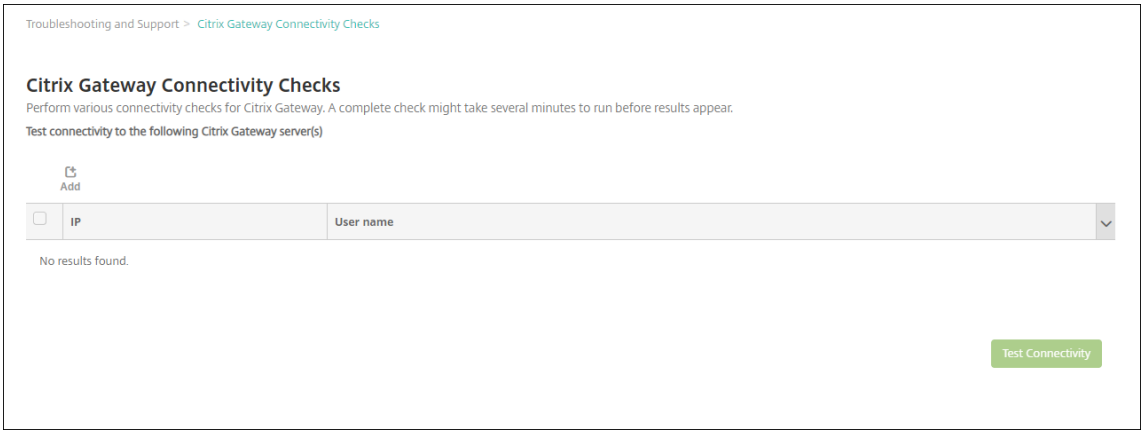


4. Wählen Sie einen Server in der Tabelle mit den Testergebnissen aus, um detaillierte Ergebnisse für den Server anzuzeigen.

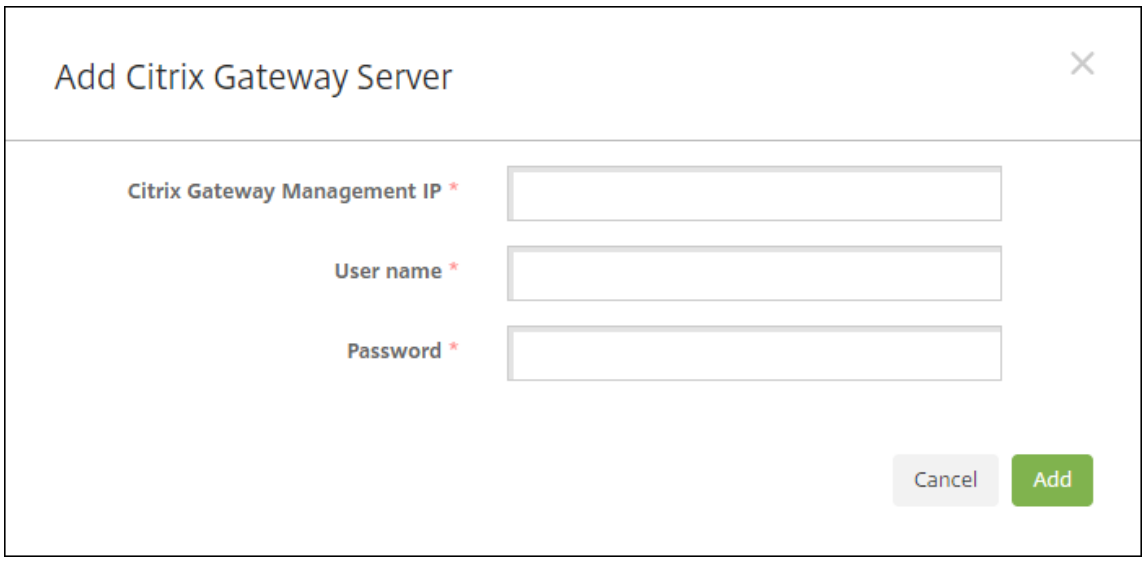


Prüfen von Citrix Gateway-Verbindungen

1. Klicken Sie auf der Seite **Support** unter **Diagnose** auf **Citrix Gateway-Konnektivitätsprüfung**. Die Seite **Citrix Gateway-Konnektivitätsprüfung** wird angezeigt. Die Tabelle ist leer, wenn Sie keine Citrix Gateway-Server hinzugefügt haben.



2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Citrix Gateway-Server hinzufügen** wird angezeigt.



3. Geben Sie unter **Citrix Gateway-Management-IP** die IP-Adresse des Servers mit Citrix Gateway ein, den Sie testen möchten.

   > **Hinweis:**
   >
   > Wenn Sie eine Konnektivitätsprüfung für einen Citrix Gateway-Server durchführen, der bereits hinzugefügt wurde, wird die IP-Adresse bereitgestellt.

4. Geben Sie die Administratoranmeldeinformationen für das Citrix Gateway ein.

   > **Hinweis:**
   >
   > Wenn Sie eine Konnektivitätsprüfung für einen Citrix Gateway-Server durchführen, der bereits hinzugefügt wurde, wird der Benutzername bereitgestellt.

5. Klicken Sie auf **Hinzufügen**. Das Citrix Gateway wird der Tabelle auf der Seite **Citrix Gateway-Konnektivitätsprüfung** hinzugefügt.
6. Wählen Sie den Citrix Gateway-Server aus und klicken Sie dann auf **Konnektivität testen**. 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.

Programm zur Verbesserung der Benutzerfreundlichkeit

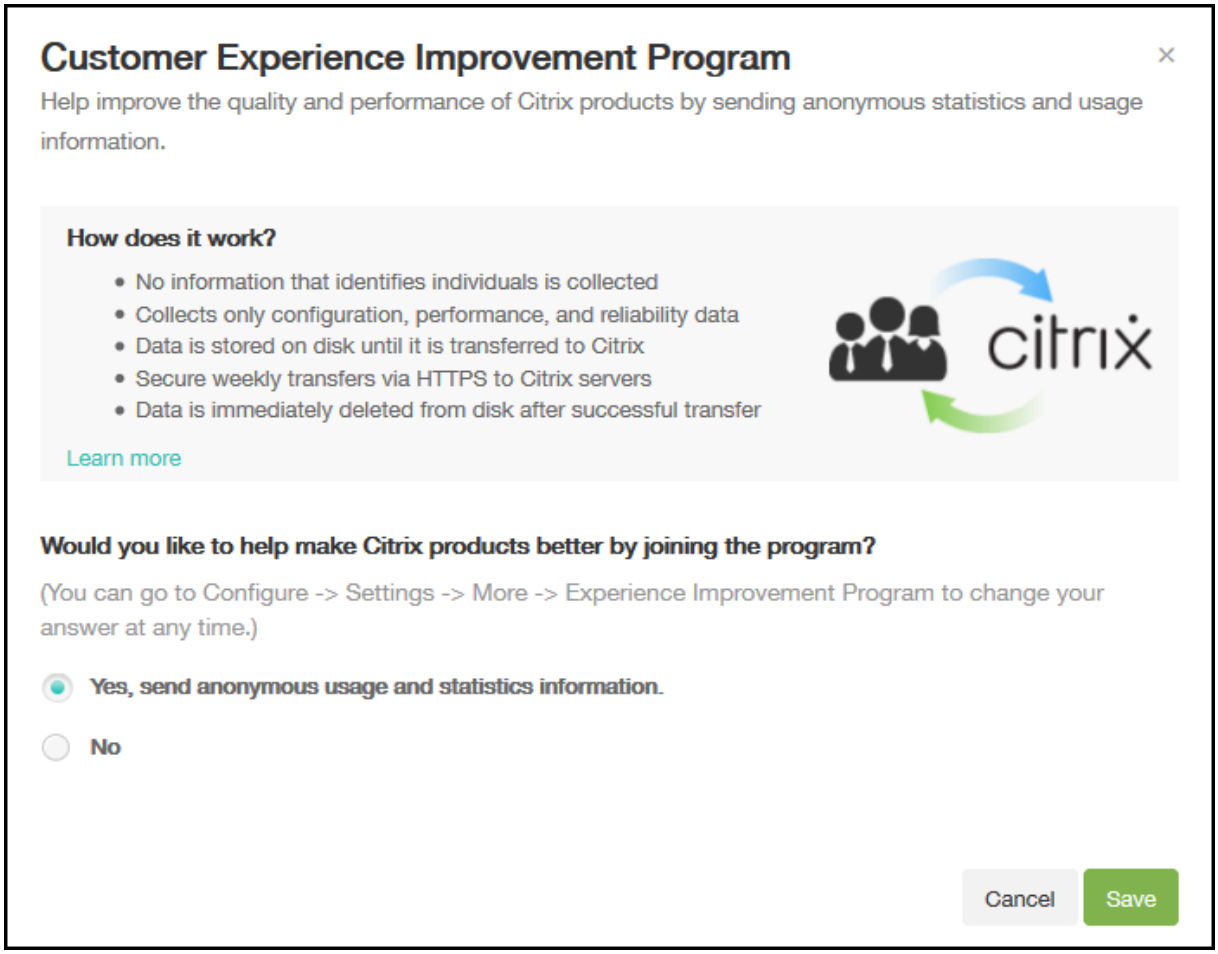
January 5, 2022

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 in der XenMobile-Konsole ändern. Weitere Informationen zum CEIP finden Sie unter Citrix Programm zur Verbesserung der Benutzerfreundlichkeit.

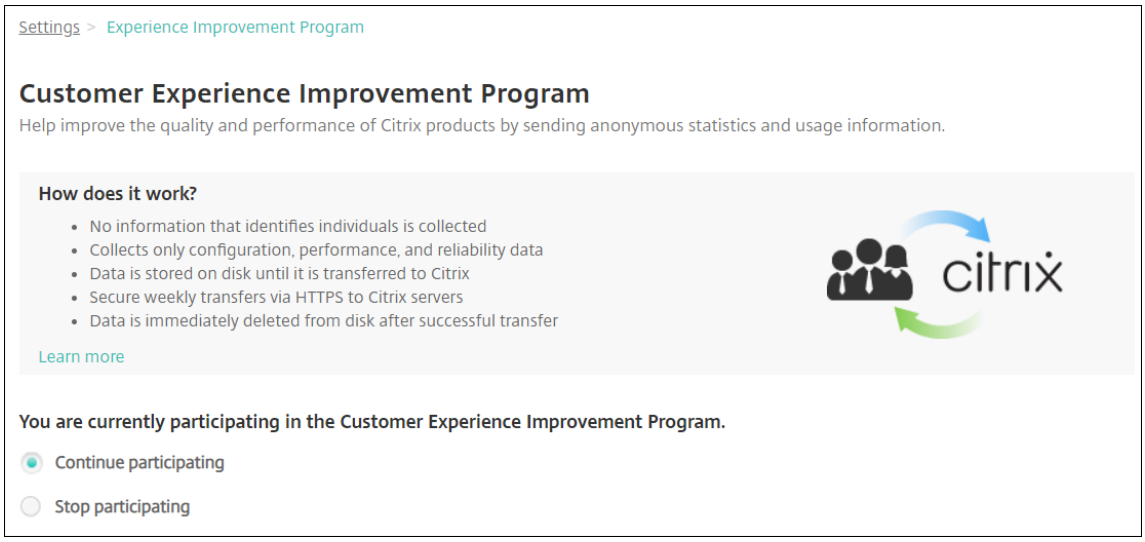
Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit

Bei der ersten Installation von XenMobile, oder wenn Sie ein Update durchführen, wird das folgende Dialogfeld mit einer Aufforderung zur Teilnahme angezeigt.



Ändern der Einstellung zur Teilnahme am CEIP

1. Zum Ändern der Einstellungen Ihrer Teilnahme am CEIP klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben, um die Seite **Einstellungen** zu öffnen.
2. Klicken Sie unter **Server** auf **Programm zur Verbesserung der Benutzerfreundlichkeit**. Die Seite **Programm zur Verbesserung der Benutzerfreundlichkeit** wird angezeigt. Wie die Seite genau aussieht, hängt davon ab, ob Sie zu dem Zeitpunkt am CEIP teilnehmen.



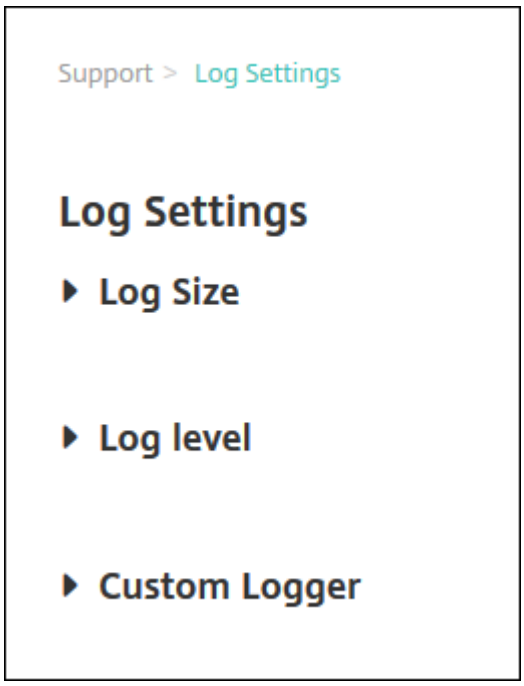
3. Wenn Sie aktuell am CEIP teilnehmen und die Teilnahme beenden möchten, klicken Sie auf **Nicht mehr** teilnehmen.
4. Wenn Sie aktuell nicht am CEIP teilnehmen und die Teilnahme beginnen möchten, klicken Sie auf **Teilnehmen**.
5. Klicken Sie auf **Speichern**.

Protokolle

May 24, 2019

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.

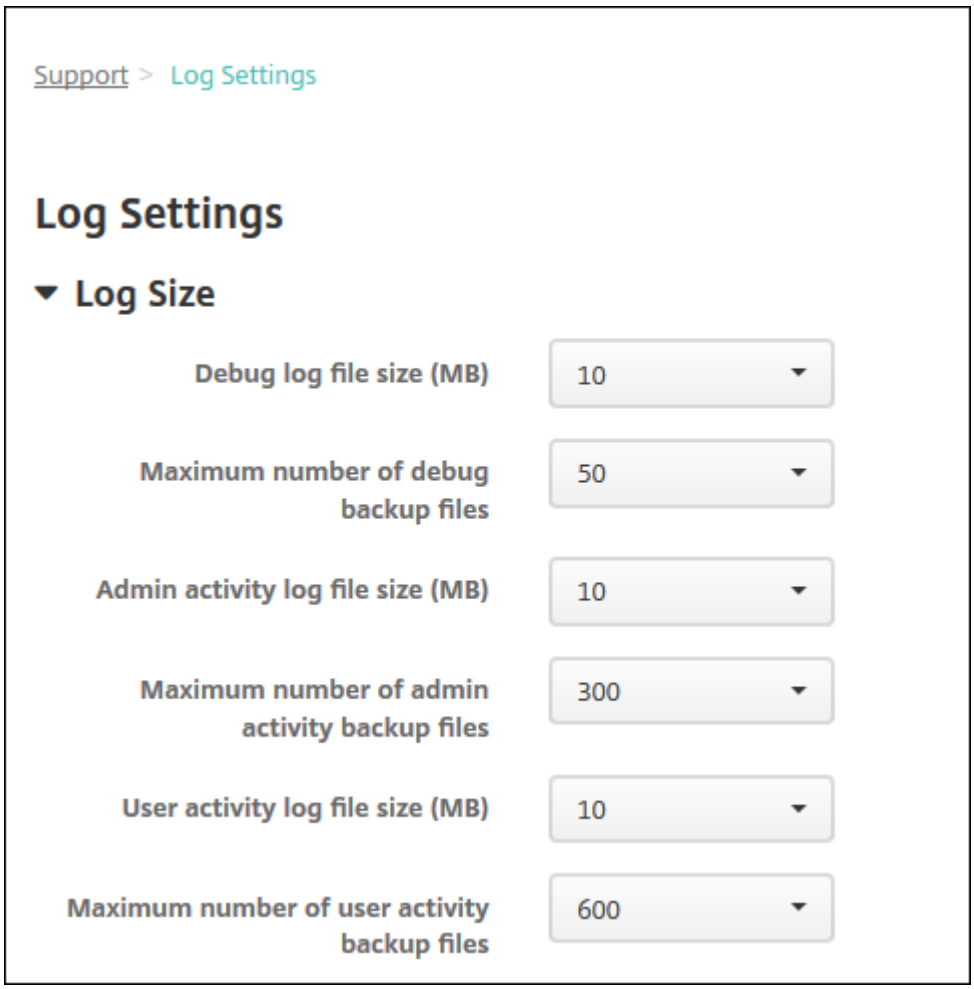


Auf der Seite **Protokolleinstellungen** können Sie folgende Einstellungen ändern:

- **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 auf der Seite **Protokolleinstellungen** die Option **Protokollgröße**.



2. Konfigurieren Sie folgende 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 Benutzeraktivitätsprotokoll-

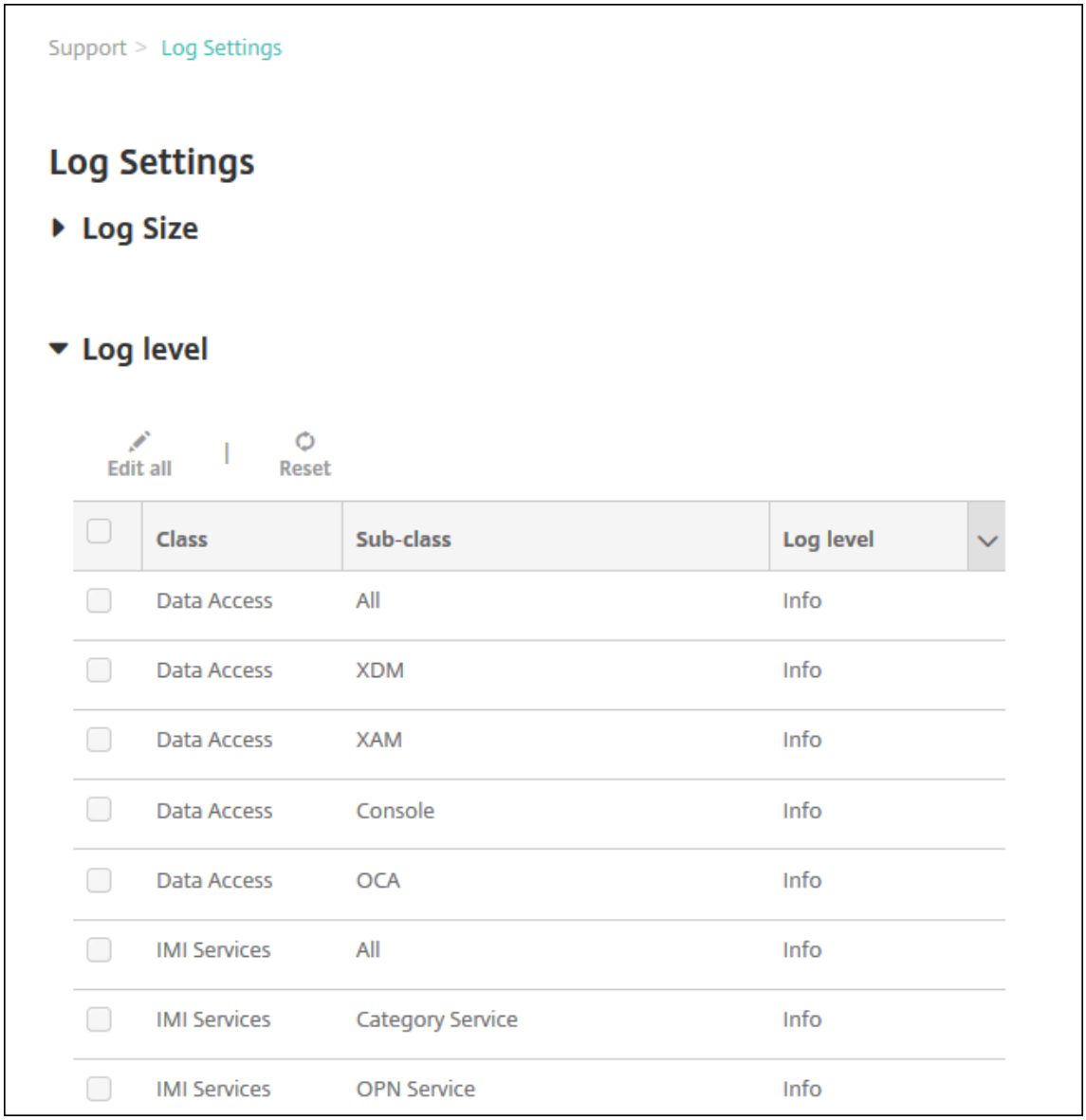
datei zu ändern. Die Standarddateigröße ist **10 MB**.

- **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.

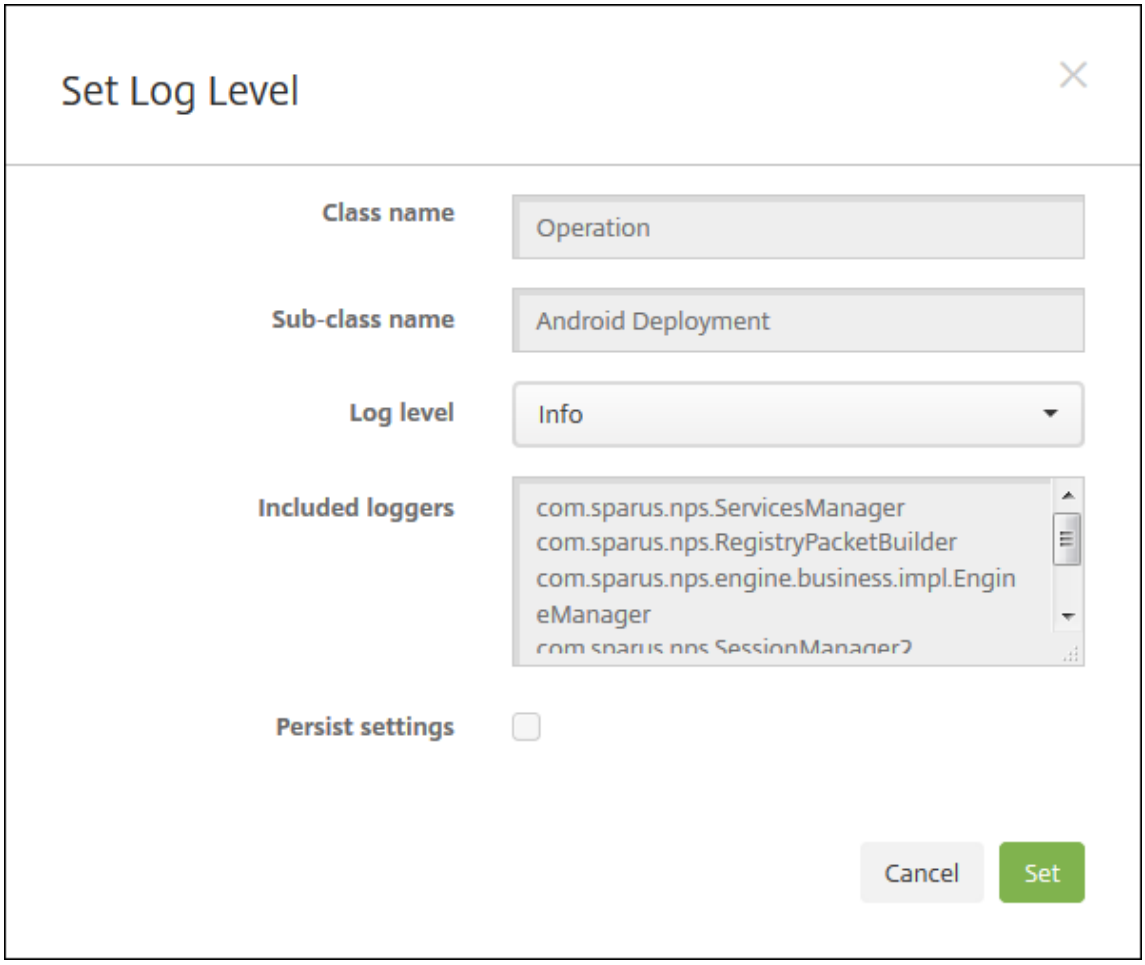
1. Erweitern Sie auf der Seite **Protokolleinstellungen** die Option **Protokollebene**. Die Tabelle mit allen Protokollklassen wird angezeigt.



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.

   Es wird das Dialogfeld **Protokollebene einstellen** angezeigt, in dem Sie die Protokollebene wählen und festlegen können, ob die Protokolleinstellungen beibehalten werden sollen, wenn Sie den XenMobile-Server neu starten.



- **Klassenname:** Wenn Sie die Auswahl für alle Klassen ändern, wird in diesem Feld “Alle” 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
  - Debuggen
  - Tracing
  - Aus
- **Enthaltene Protokollierung:** Wenn Sie die Protokollebene für alle Klassen ändern, ist dieses Feld leer, ansonsten wird der Name der aktuell konfigurierten Protokollierung für

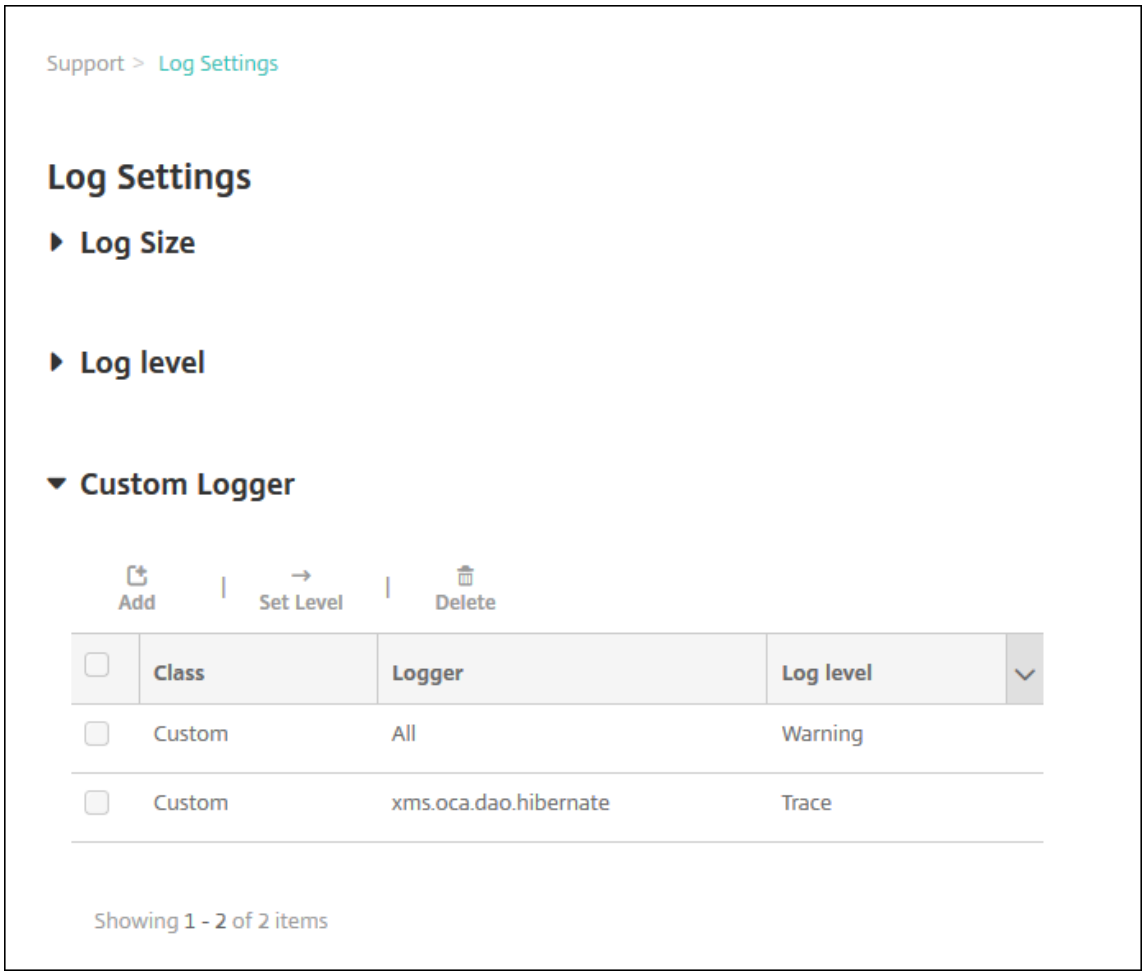
eine einzelne Klasse angezeigt. Das Feld kann nicht bearbeitet werden.

- **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.

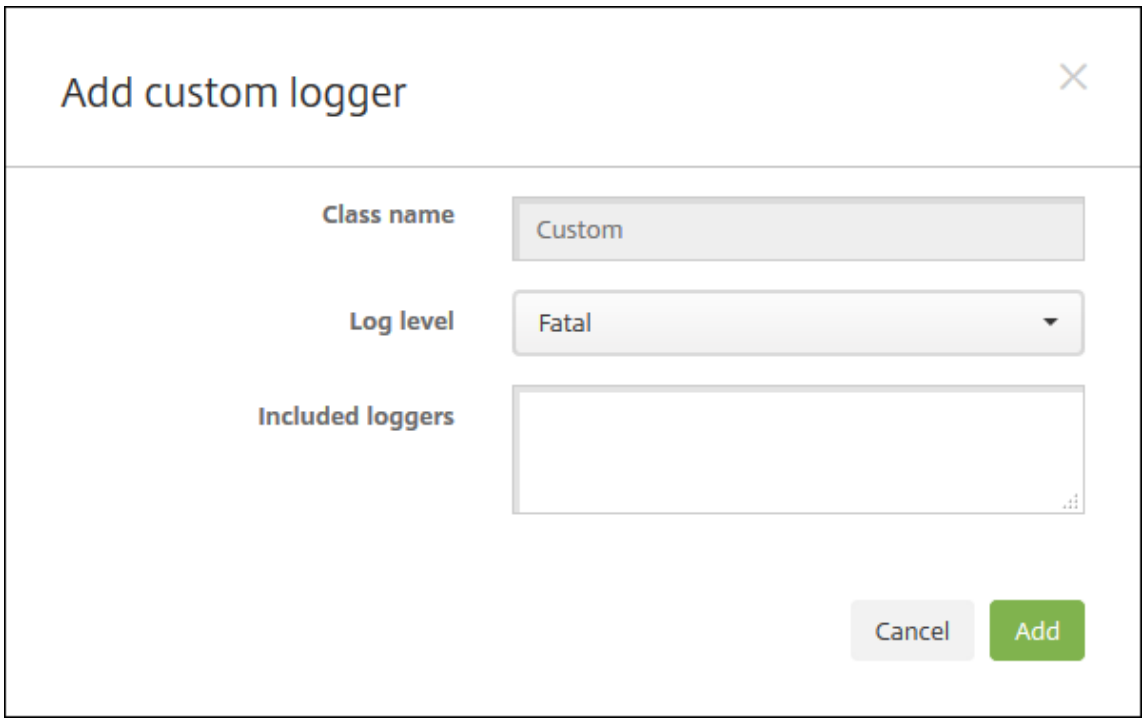
3. Klicken Sie auf **Festlegen**, um die Änderungen zu übernehmen.

Hinzufügen einer benutzerdefinierten Protokollierung

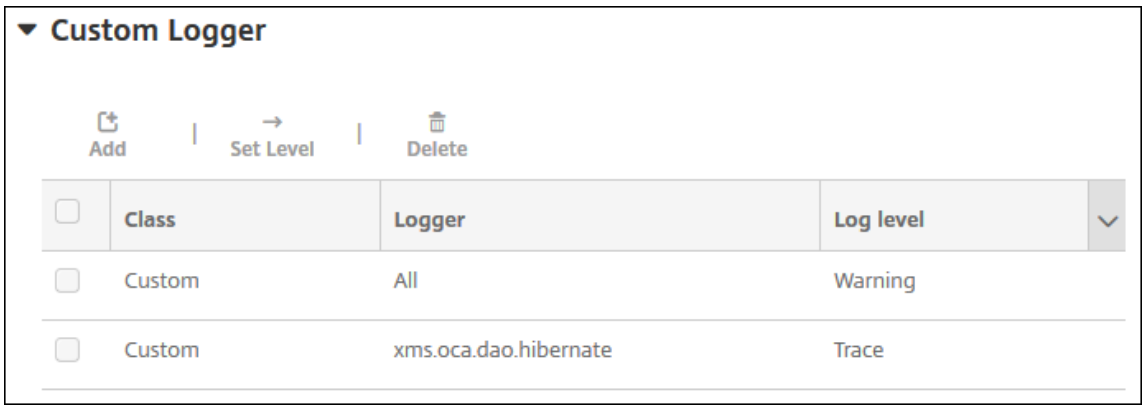
1. Erweitern Sie **Benutzerdefinierte Protokollierung** auf der Seite **Protokolleinstellungen**. Die Tabelle **Benutzerdefinierte Protokollierung** wird angezeigt. Wenn Sie noch keine benutzerdefinierte Protokollierung hinzugefügt haben, ist die Tabelle zunächst leer.



2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Benutzerdefinierte Protokollierung hinzufügen** wird angezeigt.



3. Konfigurieren Sie folgende Einstellungen:
   - **Klassenname:** In dem 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
     - Debuggen
     - Tracing
     - Aus
   - **Enthaltene Protokollierung:** Geben Sie die Protokollierungen ein, die Sie in die benutzerdefinierte Protokollierung aufnehmen 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.

Mobilfunkanbieter

January 5, 2022

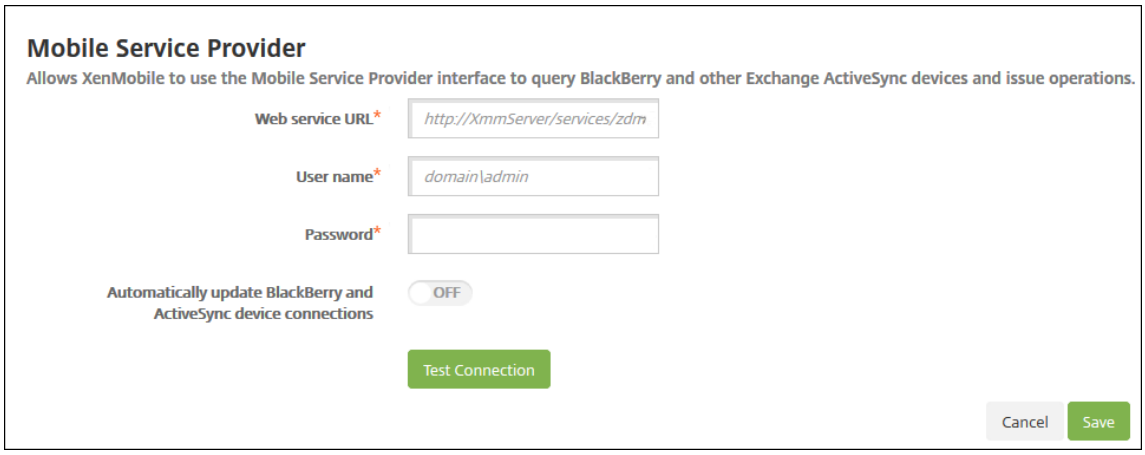
Sie können XenMobile für die Verwendung der Mobilfunkanbieter-Schnittstelle zum Abfragen von BlackBerry- und Exchange ActiveSync-Geräten und Auslösen von Vorgängen konfigurieren.

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 folgende Einstellungen:

   - **Webdienst-URL:** Geben Sie die URL des Webdiensts ein, z. B. `https://<XmmServer>/services/xdmservice`.
   - **Benutzername:** Geben Sie den Benutzernamen im Format “domain\admin” ein.
   - **Kennwort:** Geben Sie das Kennwort ein.
   - **Automatisch BlackBerry- und ActiveSync-Geräteverbindungen aktualisieren:** Wählen Sie aus, ob Geräteverbindungen automatisch aktualisiert werden sollen. Die Standardeinstellung ist **Aus**.
   - Klicken Sie auf **Verbindung testen**, um die Konnektivität zu prüfen.

4. Klicken Sie auf **Speichern**.

Berichte

August 10, 2020

XenMobile bietet die nachfolgend aufgeführten vordefinierten Berichte für die Analyse von App- und Gerätebereitstellungen. Jeder Bericht erscheint in Tabellen- und Diagrammform. Sie können die Tabellen nach Spalten sortieren. Sie können Elemente in den Diagrammen zum Aufrufen ausführlicher Informationen auswählen.

- **App-Bereitstellungsversuche insgesamt:** Liste bereitgestellter Apps, die Benutzer auf ihren Geräten zu installieren versucht haben
- **Apps nach Plattform**: Liste der Apps und App-Versionen sortiert nach Geräteplattform und -version
- **Apps nach Typ:** Liste der Apps sortiert nach Version, Typ und Kategorie

- **Geräteregistrierung:** Liste aller registrierten Geräte
- **Geräte & Apps:** Liste der Geräte, auf denen verwaltete Apps ausgeführt werden
- **Inaktive Geräte:** Liste der Geräte, die während der über die XenMobile Server-Eigenschaft "device.inactivity.days.threshold" festgelegten Zeitspanne nicht aktiv waren
- **Geräte mit Jailbreak/Rooting:** Liste der iOS-Geräte mit Jailbreak und der gerooteten Android-Geräte
- **AGB:** Benutzerliste mit Informationen dazu, ob die Benutzer die AGB akzeptiert oder abgelehnt haben Durch Auswählen von Diagrammbereichen können Sie weitere Details anzeigen.
- **Top 10 Apps:** Bereitstellung fehlgeschlagen: Liste mit bis zu 10 Apps, deren Bereitstellung fehlgeschlagen ist
- **Gesperrte Apps nach Geräten & Benutzer:** Liste der blockierten Apps, die Benutzer auf ihren Geräten haben

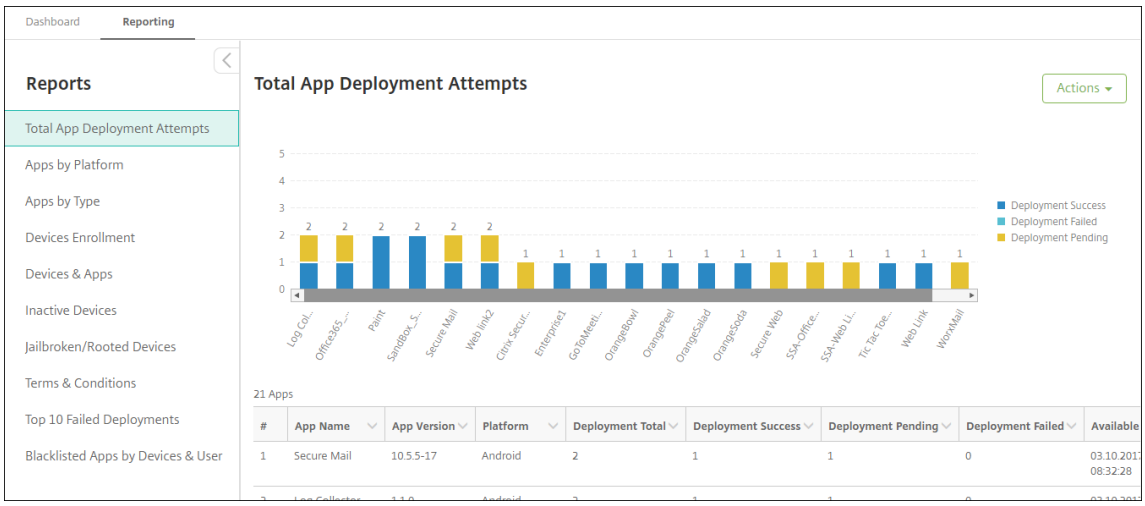
  > **Hinweis:**
  >
  > Die XenMobile Server-Konsole enthält im Englischen die Begriffe "Blacklist" und "Whitelist". Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

- **Nicht richtlinientreue Geräte:** Liste mit Geräten, die aufgrund bestimmter Kriterien (Jailbreak auf dem Gerät, ausgeführte OS-Version, fehlender Passcode auf Gerät) als nicht richtlinientreu einzustufen sind.

Sie können die Daten der Tabellen im CSV-Format exportieren und mit einem Programm wie Microsoft Excel öffnen. Sie können die Diagramme im PDF-Format exportieren.

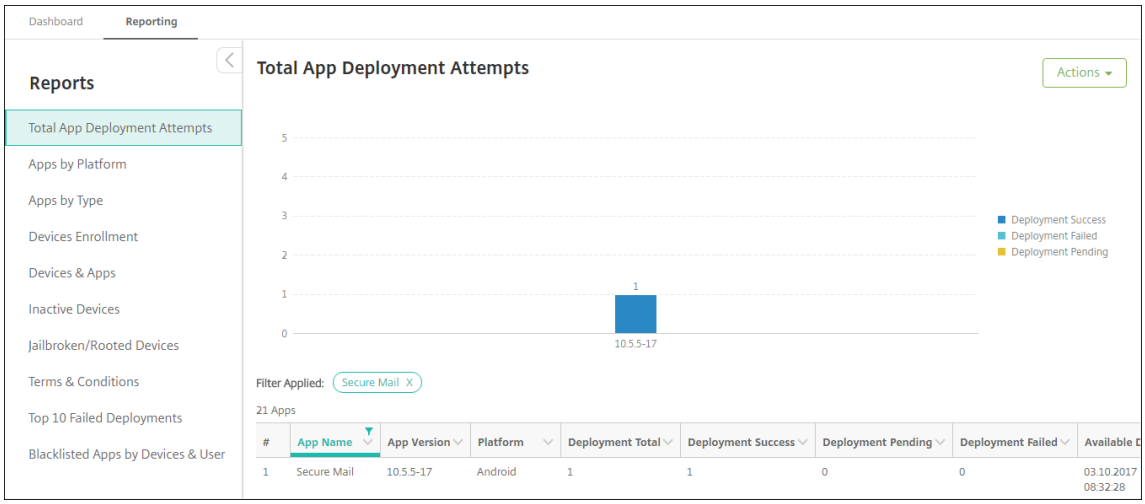
Erstellen eines Berichts

1. Klicken Sie in der XenMobile-Konsole auf **Analysieren > Berichterstellung**. Die Seite **Berichterstellung** wird angezeigt.
2. Klicken Sie auf den gewünschten Bericht.

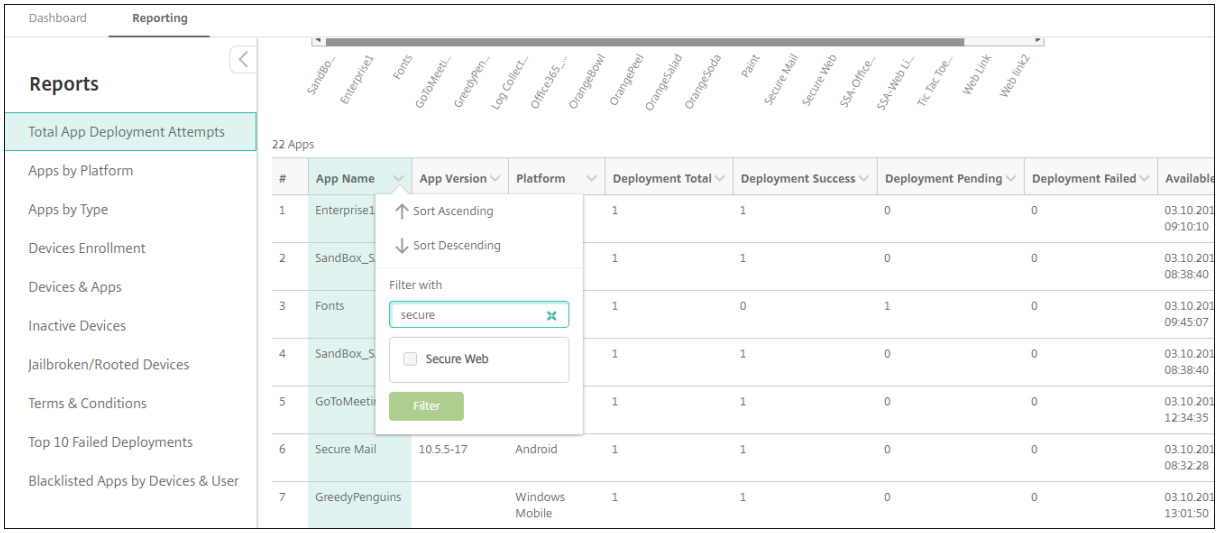


Anzeigen von Berichtdetails

1. Klicken Sie auf einzelne Bereiche des Diagramms, um weitere Details anzuzeigen.

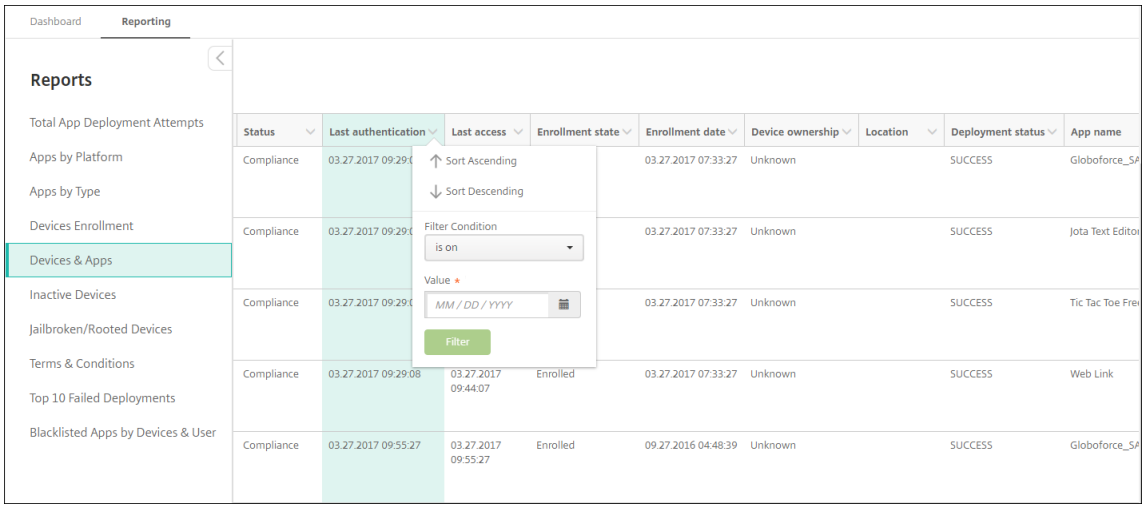


Zum Sortieren, Filtern oder Durchsuchen einer Tabellenspalte klicken Sie auf die Spaltenüberschrift

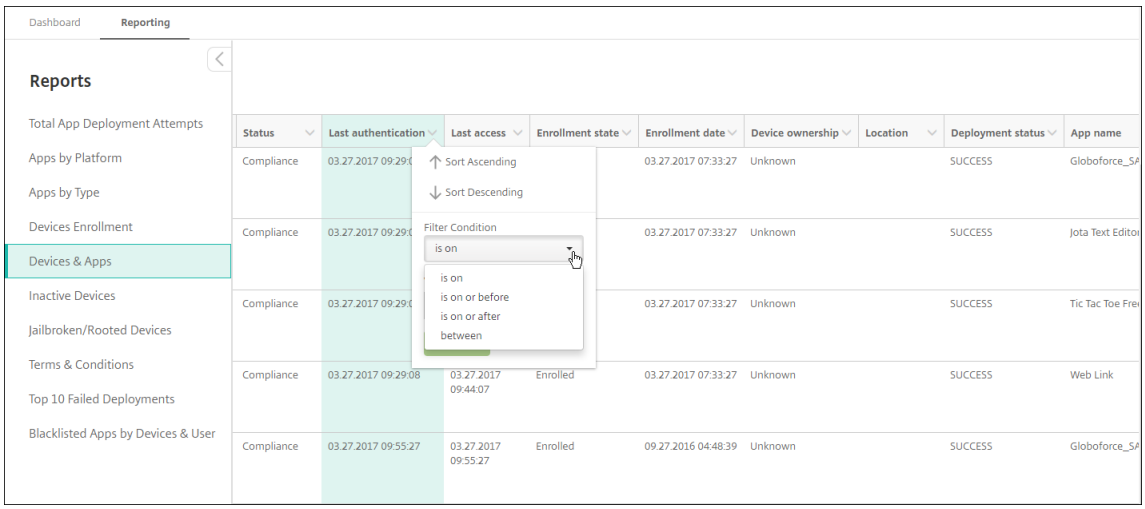


Filtern eines Berichts nach Datum

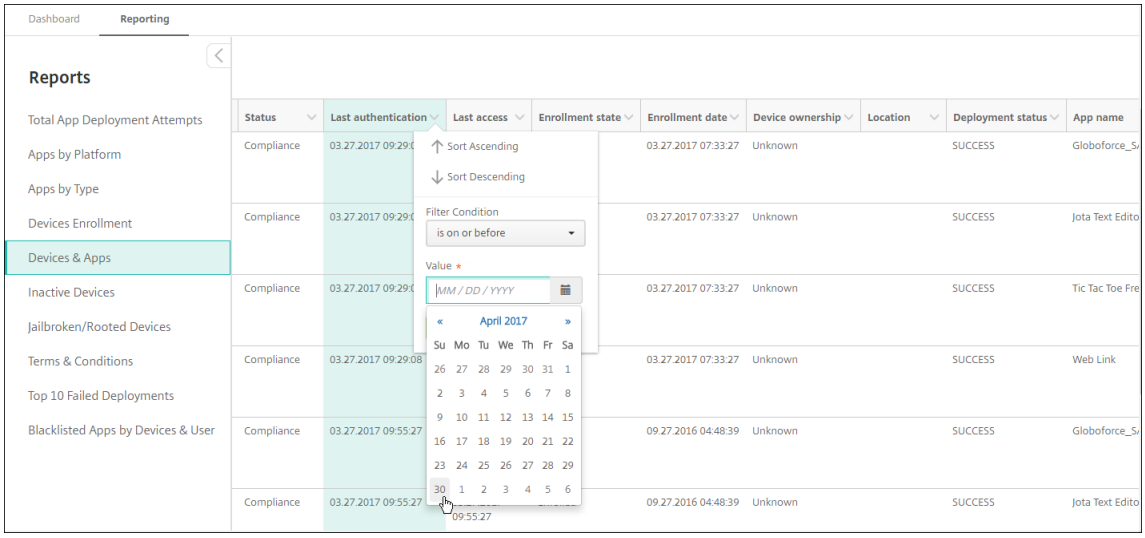
1. Klicken Sie auf eine Spaltenüberschrift, um die Filtereinstellungen anzuzeigen.



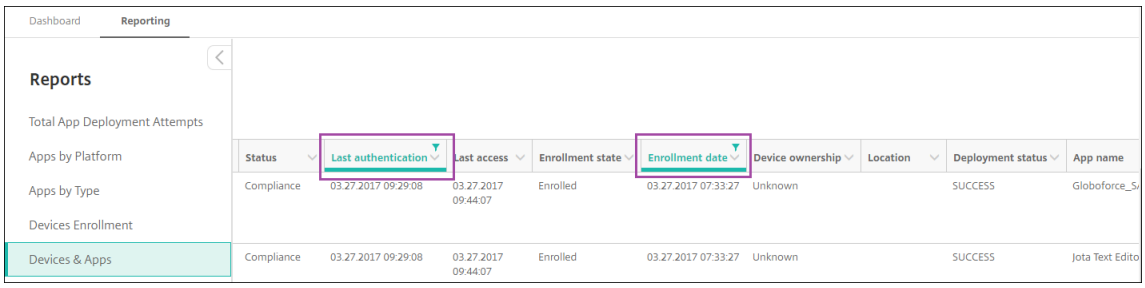
2. Wählen Sie über **Filterbedingung** aus, wie Sie die angezeigten Daten filtern möchten.



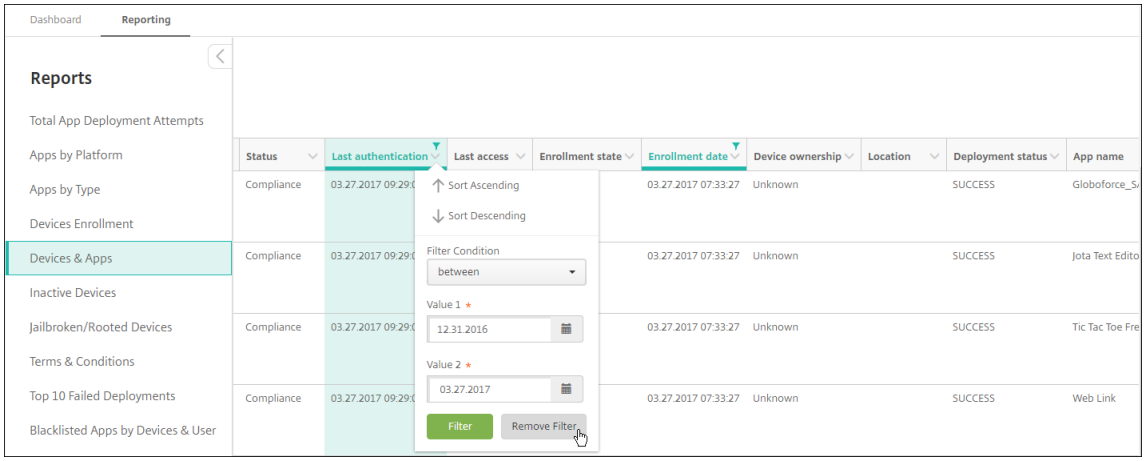
3. Verwenden Sie für Datumsangaben die Datumsauswahl.



4. Spalten mit Datumsfilter werden wie im folgenden Beispiel gezeigt angezeigt.

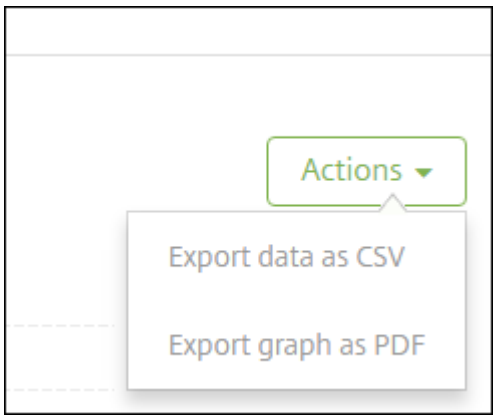


5. Um einen Filter zu entfernen, klicken Sie auf die Spaltenüberschrift und dann auf **Filter entfernen**.



Exportieren eines Diagramms oder einer Tabelle

- Um das Diagramm im PDF-Format exportieren möchten, klicken Sie auf **Aktion** und dann auf **Grafik als PDF-Datei exportieren**.
- Um die Tabellendaten im CSV-Format zu exportieren, klicken Sie auf **Aktion** und dann auf **Daten als CSV-Datei exportieren**.



> **Wichtig:**
>
> Benutzerdefinierte Berichte können zwar mit SQL Server erstellt werden, dies wird von Citrix jedoch nicht empfohlen. Citrix veröffentlicht das Schema nicht und kann das Schema ohne Benachrichtigung ändern. Wenn Sie diese Methode der Berichterstellung verwenden möchten, verwenden Sie für SQL-Abfragen ein Konto mit Nur-Lesezugriff. Beachten Sie, dass Abfragen mit mehreren JOIN-Operationen etwas dauern und sich auf die Leistung von XenMobile Server auswirken.

SNMP-Überwachung

January 5, 2022

Bei aktivierter SNMP-Überwachung in XenMobile Server können Überwachungssysteme Informationen zu Ihren XenMobile-Knoten abrufen. Abgefragt werden dabei Parameter wie Prozessorlast, Lastdurchschnitt, Speichernutzung und Konnektivität. Weitere Informationen zu SNMP v3, beispielsweise technische Daten zu Authentifizierung und Verschlüsselung, finden Sie in der offiziellen SNMP-Dokumentation für RFC 3414.

> **Hinweis:**
>
> SNMP v3-Überwachung wird von XenMobile Server 10.8 und höher unterstützt.

Sie können verschiedene Überwachungsanwendungen verwenden, die die SNMP-Überwachung unterstützen, z. B. SCOM. Informationen zum Konfigurieren von SCOM finden Sie in diesem Artikel im Citrix Support Knowledge Center.

Voraussetzungen

Konfigurieren Sie die folgenden TCP-Ports:

- **Port 161 (UDP):** wird für den SNMP-Datenverkehr mit UDP-Protokoll verwendet. Der SNMP-Manager ist die Quelle und XenMobile ist das Ziel.
- **Port 162 (UDP):** wird zum Senden von SNMP-Traps von XenMobile an den SNMP-Manager verwendet. XenMobile ist die Quelle und der SNMP-Manager ist das Ziel.

Weitere Informationen zur Konfiguration von XenMobile-Ports finden Sie unter Portanforderungen.

Das Architekturdiagramm einer On-Premises-Bereitstellung von XenMobile mit SNMP finden Sie unter Referenzarchitektur für On-Premises-Bereitstellungen.

Die allgemeine Schrittfolge zum Einrichten von SNMP ist wie folgt:

1. **Benutzer hinzufügen:** Die Benutzer erben die Berechtigung, Traps zu empfangen und XenMobile Server zu überwachen.
2. **SNMP-Manager für den Trap-Empfang hinzufügen:** Traps sind Warnungen, die von XenMobile generiert werden, wenn auf dem XenMobile-Knoten der benutzerdefinierte obere Schwellenwert überschritten wird.
3. **SNMP-Manager zur Interaktion mit XenMobile konfigurieren:** XenMobile Server verwendet bestimmte MIBs (Management Informationen Bases), um Vorgänge auszuführen. Die MIBs laden Sie in der XenMobile-Konsole über die Seite **Einstellungen > SNMP-Konfiguration** herunter. Importieren Sie die MIBs dann mit einem MIB-Importprogramm in den SNMP-Manager.

> **Hinweis:**
>
> Jeder SNMP-Manager hat ein eigenes MIB-Importprogramm.

4. **Traps aktivieren:** Sie aktivieren Traps in der XenMobile-Konsole und definieren die Intervalle und Schwellenwerte gemäß Ihrer Umgebung.
5. **Traps im SNMP-Manager eines Drittanbieters anzeigen:** Sie überprüfen Traps in dem SNMP-Manager. In einigen Managerprogrammen können Sie jedoch auch Benachrichtigungen außerhalb des Managers aktivieren. Diese Benachrichtigungen können dann zum Beispiel per E-Mail empfangen werden.

Sie können die folgenden Traps in XenMobile generieren.

Trapname: Prozessorlast

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.2.1.25.3.3.1.2
- **Beschreibung:** Überwacht die CPU-Last des Systems für das benutzerdefinierte Intervall. Falls die Last den benutzerdefinierten Schwellenwert übersteigt, generiert XenMobile den SNMP-Trap.

Trapname: Lastdurchschnitt für eine Minute

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.2021.10.1.5.1
- **Beschreibung:** Überwacht die durchschnittliche Systemlast eine Minute lang für das benutzerdefinierte Intervall. Falls der Lastdurchschnitt den benutzerdefinierten Schwellenwert übersteigt, generiert XenMobile den SNMP-Trap.

Trapname: Lastdurchschnitt für fünf Minuten

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.2021.10.1.5.2
- **Beschreibung:** Überwacht die durchschnittliche Systemlast fünf Minuten lang für das benutzerdefinierte Intervall. Falls der Lastdurchschnitt den benutzerdefinierten Schwellenwert übersteigt, generiert XenMobile den SNMP-Trap.

Trapname: Lastdurchschnitt für 15 Minuten

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.2021.10.1.5.3
- **Beschreibung:** Überwacht die durchschnittliche Systemlast 15 Minuten lang für jedes benutzerdefinierte Intervall. Falls der Lastdurchschnitt den benutzerdefinierten Schwellenwert übersteigt, generiert XenMobile den SNMP-Trap.

Trapname: Insgesamt verfügbarer Speicher

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.2021.4.11
- **Beschreibung:** Überwacht den verfügbaren Speicher für die benutzerdefinierten Intervalle. Falls der verfügbare Speicher den benutzerdefinierten Schwellenwert unterschreitet, generiert XenMobile den SNMP-Trap. Hinweis: Der Speicher umfasst den Arbeitsspeicher und den Auslagerungsspeicher (virtueller Speicher). Den gesamten Auslagerungsspeicher können Sie per

Abfrage mit SNMP-OID.1.3.6.1.4.1.2021.4.3 abrufen. Den verfügbaren Auslagerungsspeicher können Sie per Abfrage mit SNMP-OID.1.3.6.1.4.1.2021.4.4 abrufen.

Trapname: Insgesamt genutzter Speicherplatz

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.2021.9.1.9.1
- **Beschreibung:** Überwacht den Speicherplatz auf dem Systemdatenträger für jedes benutzerdefinierte Intervall. Falls der Datenträgerspeicher den benutzerdefinierten Schwellenwert übersteigt, generiert XenMobile den SNMP-Trap.

Trapname: Java Heap-Speicherauslastung

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.2.4.0
- **Beschreibung:** Überwacht die Auslastung des JVM-Heap (Java virtual machine) durch XenMobile für jedes benutzerdefinierte Intervall. Falls die Auslastung den benutzerdefinierten Schwellenwert übersteigt, generiert XenMobile den SNMP-Trap.

Trapname: Java Metaspace-Auslastung

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.2.5.0
- **Beschreibung:** Überwacht die Auslastung des Java-Metaspace durch XenMobile für jedes benutzerdefinierte Intervall. Falls die Auslastung den Schwellenwert übersteigt, generiert XenMobile den SNMP-Trap.

Trapname: LDAP-Konnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem LDAP-Server und dem XenMobile-Knoten für jedes benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: DNS-Konnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem DNS-Server und dem XenMobile-Knoten für jedes benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Google Store-Serverkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem Google Store-Server und dem XenMobile-Knoten für jedes benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Windows Phone Store-Konnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.4.0

- **Beschreibung:** Überwacht die Konnektivität zwischen dem Windows Phone Store-Server und dem XenMobile-Knoten für jedes benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Windows Tab Store-Konnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.5.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem Windows Tab Store-Server und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Windows-Sicherheitstoken-Serverkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem Windows-Sicherheitstoken-Server und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Windows-Benachrichtigungsserverkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem Windows-Benachrichtigungsserver und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: APNs-Serverkonnektivität (Apple Dienst für Push-Benachrichtigungen)

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **Beschreibung:** Überwacht die Konnektivität zwischen APNs und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Apple Feedback-Serverkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem Apple Feedback-Server und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Apple Store-Serverkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem Apple Store-Server und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: XenMobile-Datenbankserverkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.11.0

- **Beschreibung:** Überwacht die Konnektivität zwischen der XenMobile-Datenbank und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Firebase Cloud Messaging-Serverkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.12.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem Firebase Cloud Messaging-Server und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Citrix Lizenzserverkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem Citrix Lizenzserver und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Citrix Gateway-Konnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- **Beschreibung:** Überwacht die Konnektivität zwischen Citrix Gateway und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: XenMobile-Interknotenkonnektivität

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **Beschreibung:** Überwacht die Konnektivität zwischen den XenMobile-Clusterknoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

Trapname: Konnektivität des XenMobile Tomcat-Knotendiensts

- **Überwachungsobjekt-ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **Beschreibung:** Überwacht die Konnektivität zwischen dem XenMobile Tomcat-Knotendienst und den XenMobile-Knoten für das benutzerdefinierte Intervall. Falls die Verbindung fehlschlägt, generiert XenMobile den SNMP-Trap.

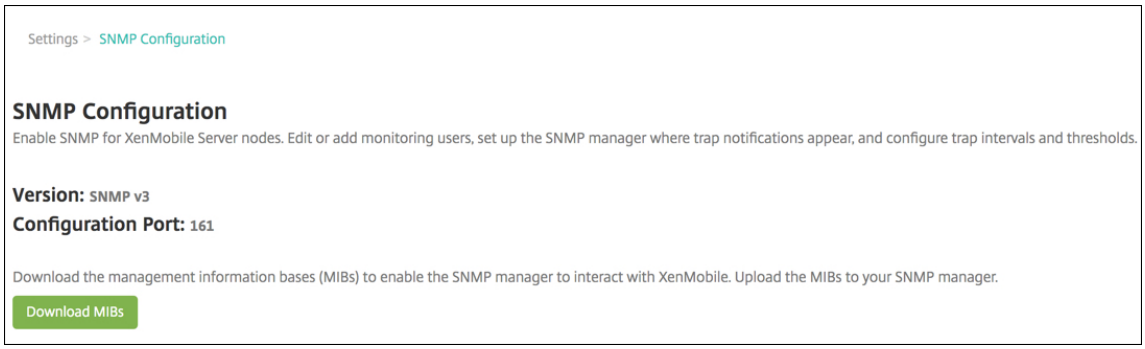
Berücksichtigen Sie bei der Konfiguration der SNMP-Schwellenwerte folgende Faktoren, um eine optimale Serverleistung zu gewährleisten:

- Häufigkeit der Anrufe
- zu erfassende Trap-Daten und Schwellenwertprüfungen
- der Kommunikationsmechanismus zwischen Knoten
- Häufigkeit der Konnektivitätsprüfungen
- Timeouts bei Fehler während der Prüfung

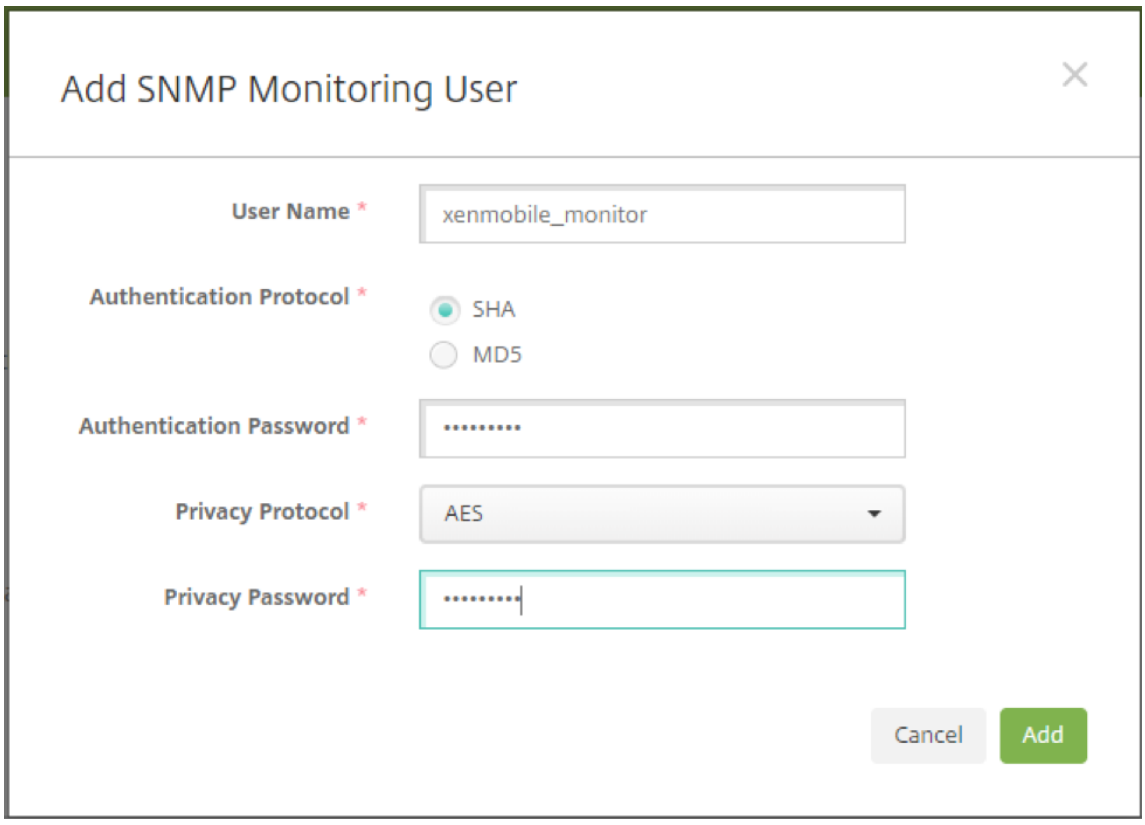
Hinzufügen von SNMP-Benutzern

SNMP-Benutzer interagieren mit SNMP-Managern und empfangen Traps.

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



3. Klicken Sie unter **SNMP-Überwachungsbenutzer** auf **Hinzufügen**.
4. Konfigurieren Sie im Dialogfeld **SNMP-Überwachungsbenutzer hinzufügen** folgende Einstellungen:



Benutzername: der bei der Anmeldung am SNMP-Manager verwendete Benutzername. Sie

können alphanumerische Zeichen, Unterstriche und Bindestriche im Benutzernamen verwenden, jedoch keine Leerzeichen oder anderen Sonderzeichen.

> **Hinweis:**
>
> Sie können den Benutzernamen “xmsmonitor” nicht hinzufügen, da XenMobile diesen Namen für interne Prozesse reserviert hat.

Authentifizierungsprotokoll:

- **SHA** (empfohlen)
- **MD5**

Authentifizierungskennwort: Geben Sie ein Kennwort einer Länge von 8 bis 18 Zeichen ein. Sie können alphanumerische Zeichen und Sonderzeichen verwenden.

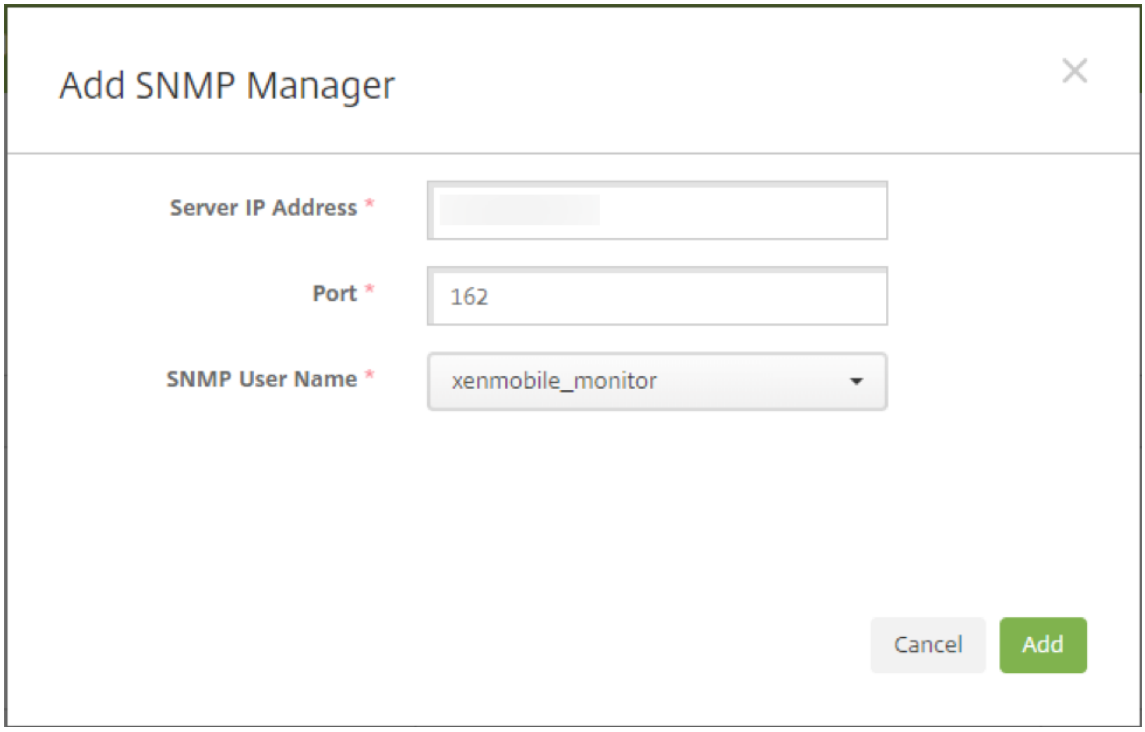
Datenschutzprotokoll:

- **DES**
- **AES-128** (empfohlen)

Datenschutzkennwort: Geben Sie ein Kennwort einer Länge von 8 bis 18 Zeichen ein. Sie können alphanumerische Zeichen und Sonderzeichen verwenden.

Hinzufügen eines SNMP-Managers

1. Klicken Sie unter **SNMP-Manager** auf **Hinzufügen**.
2. Konfigurieren Sie im Dialogfeld **SNMP-Manager hinzufügen** folgende Einstellungen:



Server-IP-Adresse: Geben Sie die IP-Adresse des SNMP-Managers ein.

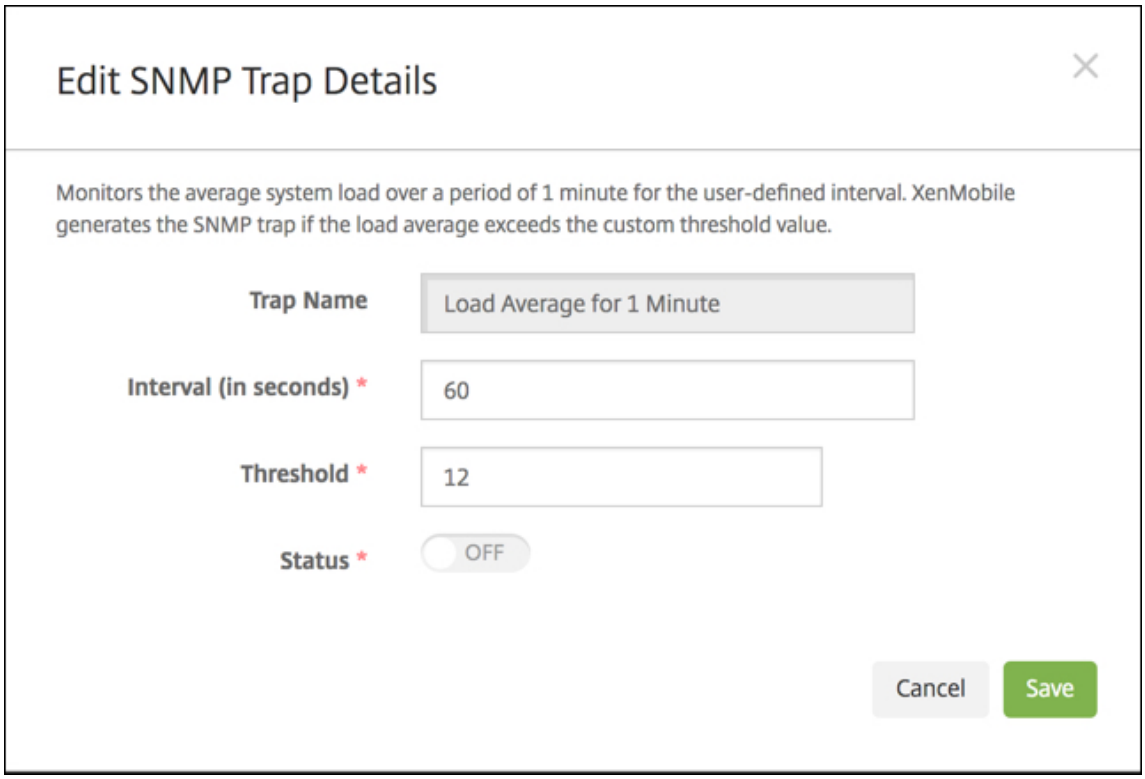
Port: Ändern Sie die Portnummer falls erforderlich. Die Standardeinstellung ist 162.

SNMP-Benutzername: Wählen Sie den Namen eines Benutzers mit Zugriff auf den Manager aus.

Aktivieren und Konfigurieren von SNMP-Traps

Nützliche Hinweise zum Bestimmen der geeigneten Trap-Einstellungen für Ihre Umgebung finden Sie unter Skalierbarkeit und Leistung. Um beispielsweise eine Minute lang den Lastdurchschnitt von XenMobile zu überwachen, können Sie die Option “Lastdurchschnitt für 1 Minute” aktivieren und einen Schwellenwert festlegen. Falls der einminütige Lastdurchschnitt von XenMobile Server den angegebenen Schwellenwert überschreitet, erhalten Sie einen Trap in den konfigurierten SNMP-Managern.

1. Zum Aktivieren einzelner Traps führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben dem Parameter und klicken Sie auf **Aktivieren**.
   - Zum Aktivieren aller Traps in der Liste aktivieren Sie das Kontrollkästchen oben im Dialogfeld und klicken Sie auf **Aktivieren**.
2. Um einen Trap zu bearbeiten, wählen Sie den Parameter aus und klicken Sie auf **Bearbeiten**.
3. Im Dialogfeld **SNMP-Trapdetails bearbeiten** können Sie die Schwellenwerte für einzelne Traps bearbeiten.



Trapname: der Name des Traps. Sie können dieses Feld nicht bearbeiten.

Intervall (in Sekunden): Der zulässige Bereich liegt zwischen 60 und 86400 (24 Stunden).

Schwellenwert: Sie können den Schwellenwert nur für folgende Traps ändern:

- Prozessorlast
- Lastdurchschnitt für 1 Minute
- Lastdurchschnitt für 5 Minuten
- Lastdurchschnitt für 15 Minuten
- Insgesamt verfügbarer Speicher
- Insgesamt genutzter Speicherplatz
- Java Heap-Speicherauslastung
- Java Metaspace-Auslastung

Status: Wählen Sie **Ein**, um die SNMP-Überwachung für den Trap zu aktivieren. Wählen Sie **Aus**, um die Überwachung zu deaktivieren.

Weitere Informationen zum Überwachen von XenMobile mithilfe von SNMP finden Sie in diesem Blogbeitrag .

Supportpakete

December 21, 2020

Erstellen Sie ein Supportpaket, um Citrix ein Problem zu melden oder um Hilfe bei der Problembehandlung zu erhalten. Laden Sie das Supportpaket dann hoch an Citrix Insight Services (CIS).

Standardmäßig enthält ein Supportpaket maximal 100 Backuparchive der folgenden Dateien. Die Standardgröße dieser Dateien ist 10 MB.

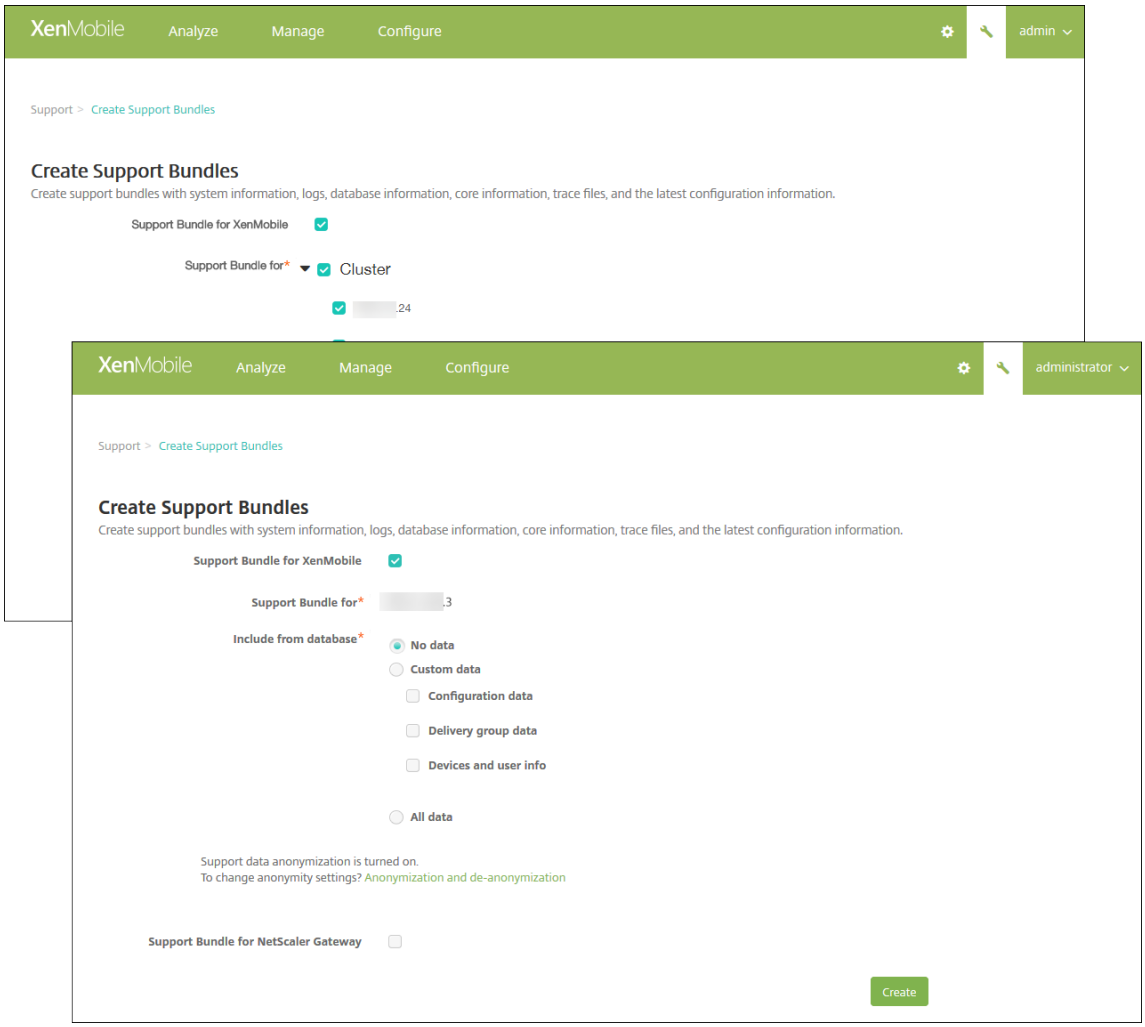
- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

Wenn das Supportpaket 100 archivierte Protokolldateien für jede dieser Kategorien enthält, wird per Dateirollover eine neue Protokolldatei erstellt. Wenn Sie eine niedrigere Höchstanzahl von Protokolldateien konfigurieren, löscht XenMobile die überflüssigen Protokolldateien für den Knoten sofort. Um die Anzahl der Protokolldateien zu konfigurieren, gehen Sie zu **Problembehandlung und Support > Protokolleinstellungen**.

Erstellen eines Supportpakets

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

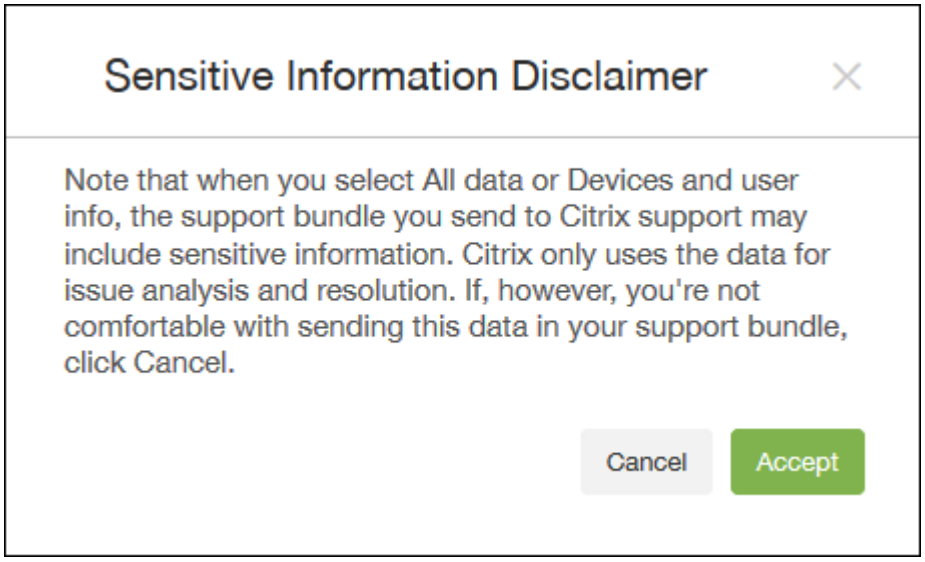
2. Klicken Sie auf der Seite **Support** auf **Supportpakete erstellen**. Die Seite **Supportpakete erstellen** wird angezeigt. Wenn die XenMobile-Umgebung Clusterknoten enthält, werden alle Knoten angezeigt.



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**. 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.

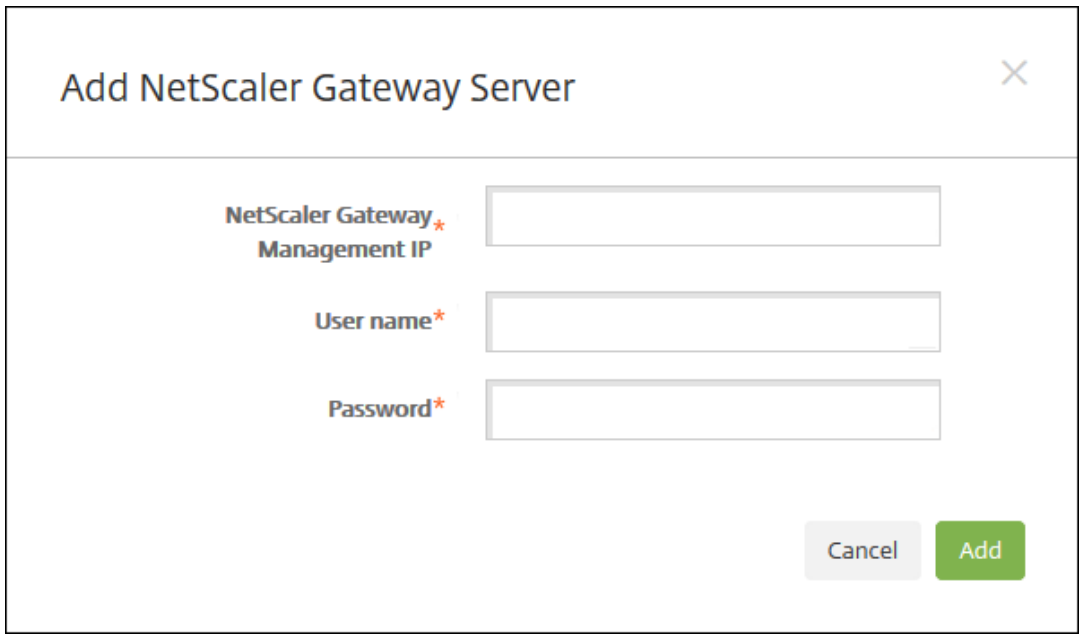


6. Die Option **Anonymisierung von Supportdaten** ist aktiviert gibt an, dass Daten in der Standardeinstellung anonymisiert werden. Dies bedeutet, dass vertrauliche Benutzer-, Server- und Netzwerkdaten in Supportpaketen anonymisiert werden.

   Sie können diese Einstellung über den Link **Anonymisierung und Deanonymisierung** ändern. Weitere Informationen finden Sie unter Anonymisierung von Daten in Supportpaketen.

7. Einschließen von Supportpaketen von Citrix Gateway: Aktivieren Sie das Kontrollkästchen **Supportpaket für Citrix Gateway** und führen Sie die folgenden Schritte aus:

   a) Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Citrix Gateway-Server hinzufügen** wird angezeigt.



b) Geben Sie unter **Citrix Gateway-Management-IP** die Citrix ADC-Verwaltungs-IP-Adresse für das Citrix Gateway ein, von dem Sie das Supportpaket beziehen möchten.

> **Hinweis:**
>
> Wenn Sie ein Paket von einem Citrix 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 Citrix Gateway ausgeführt wird.

> **Hinweis:**
>
> Wenn Sie ein Paket von einem Citrix Gateway-Server erstellen, der bereits hinzugefügt wurde, wird der Benutzername bereitgestellt.

8. Klicken Sie auf **Hinzufügen**. Das neue Citrix Gateway-Supportpaket wird der Tabelle hinzugefügt.
9. Wiederholen Sie Schritt 7 zum Hinzufügen weiterer Citrix Gateway-Supportpakete.
10. 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

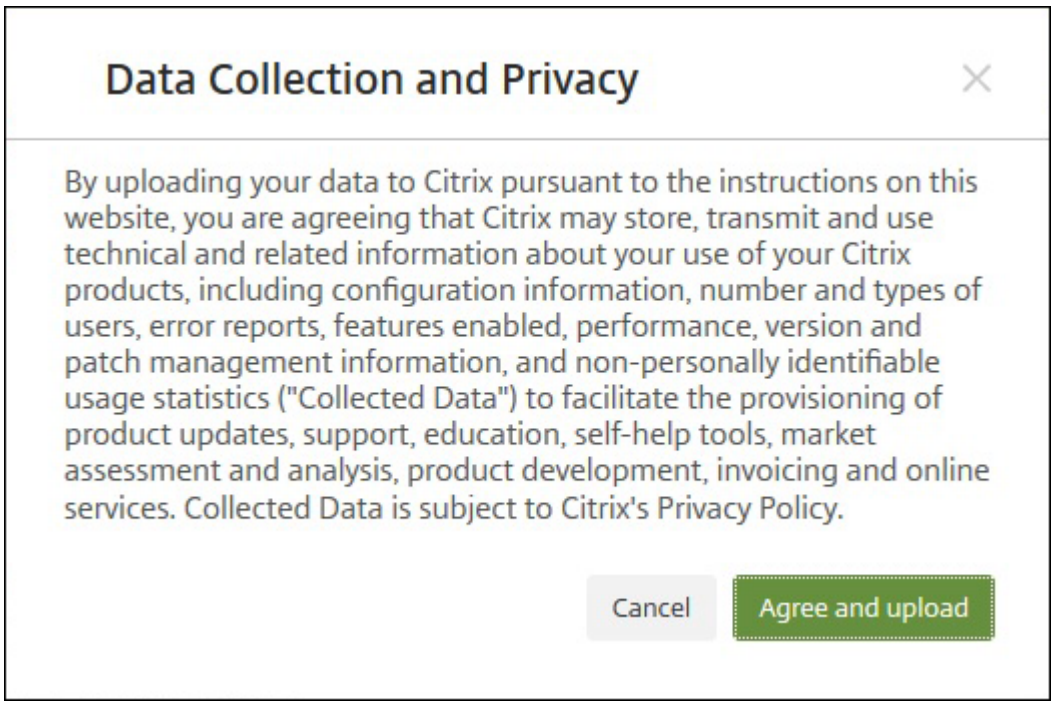
Nach dem Erstellen eines Supportpakets können Sie das Paket an Citrix Insight Services (CIS) hochladen oder auf Ihren Computer herunterladen.

Der Upload von XenMobile zu CIS erfolgt über eine ausgehende SSL-Verbindung. Öffnen Sie Port 443 für die CIS-Server-IP-Adresse (52.88.24.76, 52.88.118.220, 52.11.72.119). Wenn Sie einen Proxy für HTTPS-Datenverkehr verwenden, vergewissern Sie sich, dass er die IP-Adresse des CIS-Servers erreichen kann.

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 Serviceanforderung verbinden möchten, aktivieren Sie das Kontrollkästchen **Associate with SR#** und geben Sie in die beiden neu angezeigten Felder Folgendes ein:
   - Geben Sie für **SR#** die achtstellige Serviceanforderungsnummer ein, der Sie das Paket zuordnen möchten.
   - Geben Sie für **SR-Beschreibung** eine Beschreibung der Serviceanforderung 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 hochladen**. 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 Supportpakete erstellen auf Zu Client herunterladen. Das Paket wird auf Ihren Computer heruntergeladen.

Das Supportpaket enthält Dateien mit unterschiedlichem Wert für die Analyse. In der folgenden Tabelle finden Sie eine Liste der Dateien und ihren Analysezweck.

Dateiname	Typ	Beschreibung	Wert
DbDump.json	JSON Database Dump	Benutzer/Geräte/Anwer	Hoch
Garbage.html	HTML-Datei	Java Garbage Collector	Niedrig
MemoryInfo.html	HTML-Datei	Speicherauslastung - Java-bezogene Speichernutzung	Hoch
MultiNodeClusterInfo.html	HTML-Datei	Clusterkonfiguration	Hoch

Dateiname	Typ	Beschreibung	Wert
Patches.html	HTML-Datei	Patchinformationen. Better to xmspatches.txt	Hoch
pg_dump0.sql	PG Dump	Standard-Postgress-Instanzdump	Mittel
rt_db/*	DB Copy (redundant, eine binäre Darstellung von pg_dump0.sql)		Nicht zutreffend
sas_config/c3p0.properties	Eigenschaftendatei	C3P0 DB Config-Eigenschaften	Mittel
sas_config/catalina.pol	Richtliniendatei	Catalina-Richtlinien für Webserver - Dateien ändern sich nicht	Niedrig
sas_config/catalina.properties	Eigenschaftendatei	Webserver Catalina Eigenschaften - Dateien ändern sich nicht	Niedrig
sas_config/ew-config.properties	Eigenschaftendatei	Informationen zur Konfiguration des XM-Servers	Hoch
sas_config/ew-config-reloadable.properties	Eigenschaftendatei	Informationen zum Sicherheitsmodell	Hoch
sas_config/hazelcast.xr	XML-Datei	Hazelcast-Protokolle - wahrscheinlich nicht nützlich.	Niedrig
sas_config/pki.xml	XML-Datei	Könnte verwendet werden, um festzustellen, ob ein PKI-Server eines Drittanbieters verwendet wird.	Hoch
sas_config/push_servic	XML-Datei	Pushdienste - Dateien ändern sich nicht	Niedrig

Dateiname	Typ	Beschreibung	Wert
sas_config/server.xml	XML-Datei	Verschlüsselungsinformationen - Sicherheitsbezogen	Hoch
sas_config/sftu_config/	Eigenschaftendatei	AppC-Eigenschaften - Dateien ändern sich nicht	Niedrig
sas_config/sftu_config/catalina.policy	Richtliniendatei	Catalina-Richtlinien - Dateien ändern sich nicht	Niedrig
sas_config/sftu_config/	Eigenschaftendatei	Catalina Properties - Dateien ändern sich nicht	Niedrig
sas_config/sftu_config/logging.properties	Eigenschaftendatei	Eigenschaften für die Protokollierung - Dateien ändern sich nicht	Niedrig
sas_config/sftu_config/	XML-Datei	Verschlüsselungsinform - Sicherheitsbezogen	Hoch
sas_config/sftu_config/sxmc_migration.xml	XML-Datei	Informationen für die Migration	Hoch
sas_config/sftu_config/	XML-Datei	Einstellungen für Erstbenutzer	Hoch
sas_config/sftu_config/tomcat-users.xml	XML-Datei	TomCat Users - Dateien ändern sich nicht	Niedrig
sas_config/sftu_config/	XML-Datei	Web - Dateien ändern sich nicht	Niedrig
sas_config/sftu.properties	Eigenschaftendatei	Eigenschaften für SFTU Config	Hoch
sas_config/variables.xml	XML-Datei	Variablen - Dateien ändern sich nicht	Niedrig
sas_config/web.xml	XML-Datei	Webserver-bezogene Informationen	Mittel
sas_log/AdminAuditLog	Linux-Protokolldatei	Alle Änderungen an der Konfiguration	Hoch

Dateiname	Typ	Beschreibung	Wert
sas_log/create_sb_output.sh	Linux-Protokolldatei	Unterstützung für das Generieren von Befehlsausgaben	Niedrig
sas_log/DebugLogFile.l	Linux-Protokolldatei	Protokollierung aller Funktionen	Hoch
sas_log/HibernateStats.log	Linux-Protokolldatei	Hibernatestats-Protokoll	Niedrig
sas_log/kafka-consumer.log	Linux-Protokolldatei	Kafka-Protokoll	Niedrig
sas_log/kafka-server.log	Linux-Protokolldatei	Kafka-Protokoll	Niedrig
sas_log/kafka-topics.log	Linux-Protokolldatei	Kafka-Protokoll	Niedrig
sas_log/LPE.log	Linux-Protokolldatei	LPE-Protokoll	Niedrig
sas_log/migration.log	Linux-Protokolldatei	Ausgabe des Migrationsvorgangs	Mittel
sas_log/PlatformAuditLogFile.log	Linux-Protokolldatei	Backend-Auditebeneninformationen	Hoch
sas_log/PlatformDebug	Textdatei	Backendserver-bezogene Protokolle	Hoch
sas_log/postgres.log	Linux-Protokolldatei	PostGres-Protokolle	Mittel
sas_log/SFTU.log	Linux-Protokolldatei	SFTU-Protokoll	Mittel
sas_log/tc1/catalina.log	Linux-Protokolldatei	Catalina-Protokoll	Niedrig
sas_log/tc1/console	Linux-Protokolldatei	Konsole	Niedrig
sas_log/tc1/host-manager.log	Linux-Protokolldatei	Host Manager	Niedrig
sas_log/tc1/localhost.l	Linux-Protokolldatei	LocalHost	Niedrig
sas_log/updates.log	Linux-Protokolldatei	Ausgabe des Patchingvorgangs	Mittel
sas_log/UserAuditLogF	Linux-Protokolldatei	Benutzeraktionen	Hoch
sas_log/zookeeper.txt	Textdatei	Zookeeper-Protokoll	Niedrig
snmp/snmpd_etc_nets	Eigenschaftendatei	Eigenschaften der SNMP-Konfiguration	Niedrig

Dateiname	Typ	Beschreibung	Wert
snmp/snmpd_privileges.cfg	Eigenschaftendatei	Eigenschaften der SNMP-Konfiguration	Niedrig
sys_info/arp_entries.txt	Textdatei	ARP Entris im XMS-Server	Mittel
sys_info/chrony.txt	Textdatei	Chrony-Protokoll	Niedrig
sys_info/diskspace_usa	Textdatei	Speicherplatzbelegung	Hoch
sys_info/firewall_rules.txt	Textdatei	In XMS definierte Firewallregeln	Mittel
sys_info/interface_conf	Textdatei	Ausgabe von Systembefehlen	Mittel
sys_info/net_connections.txt	Textdatei	Ausgabe von Systembefehlen	Mittel
sys_info/root_account_	Textdatei	Ausgabe von Systembefehlen	Mittel
sys_info/routing_table.txt	Textdatei	Höchstwert	Hoch
sys_info/running_proce	Textdatei	Höchstwert	Hoch
sys_info/top.txt	Textdatei	Ausgabe von Systembefehlen	Mittel
ThreadDump.html	HTML-Datei	Nicht mehr verwendet.	Niedrig
ThreadDumpV2.html	HTML-Datei	Thread-Stack-Traces usw.	Mittel
var_log/auth.log	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
var_log/boot.log	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
var_log/btmp	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
var_log/daemon.log	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
var_log/kern.log	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel

Dateiname	Typ	Beschreibung	Wert
var_log/lastlog	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
var_log/mail.log	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
var_log/sys.log	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
var_log/user.log	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
var_log/wtmp	Linux-Protokolldatei	Protokoll für Betriebssystemebene	Mittel
version.txt	Textdatei	Version des XM-Servers	Mittel
XENMOBILE-<IP Address>-ConnectivityCheckResults.xml	XML-Datei	Ergebnisse der Konnektivitätsprüfung auf XMS-Servern	Mittel
xmspatches.txt	Textdatei	Patchinformationen.	Hoch

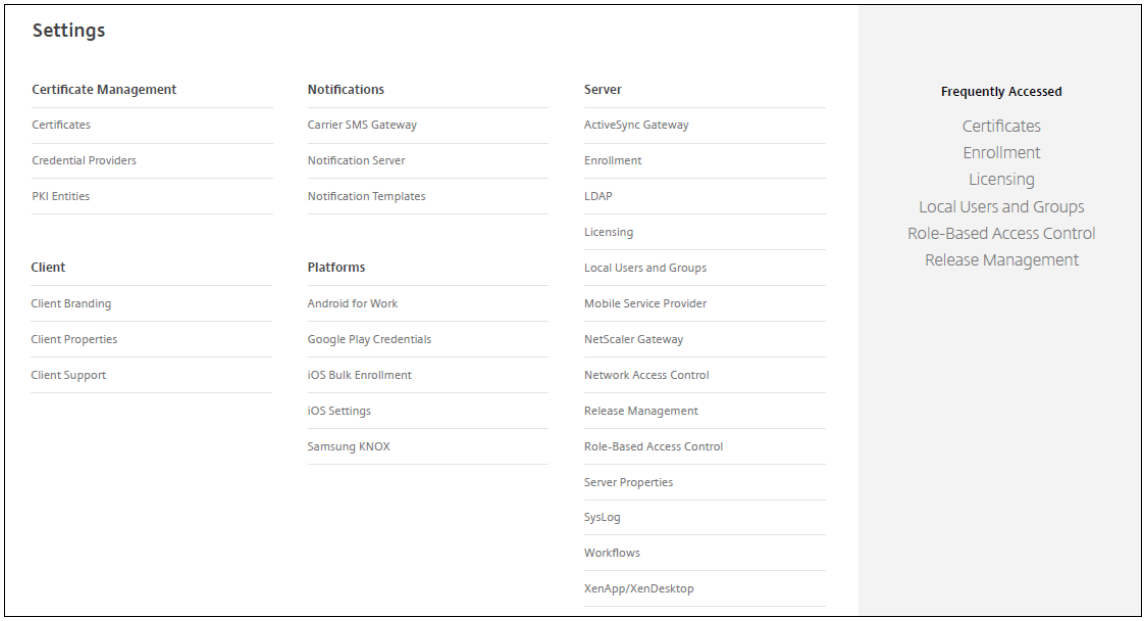
Supportoptionen und Remote Support

January 5, 2022

Sie können eine E-Mail-Adresse bereitstellen, unter der die Benutzer das Supportteam erreichen. Wenn Benutzer von ihrem Gerät aus Unterstützung anfordern, wird diese E-Mail-Adresse angezeigt.

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:
   - **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 (ShareFile heißt jetzt Citrix Content Collaboration). Wenn Sie “Protokolle in Citrix Content Collaboration speichern” aktivieren, werden die Protokolle direkt an Citrix Files 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, um zu verhindern, dass Protokolle eines Serverproblems 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**.

Remotesupport

> **Hinweis:**
>
> Remote Support ist ab dem 1. Januar 2019 für Neukunden nicht mehr verfügbar. Bestehende

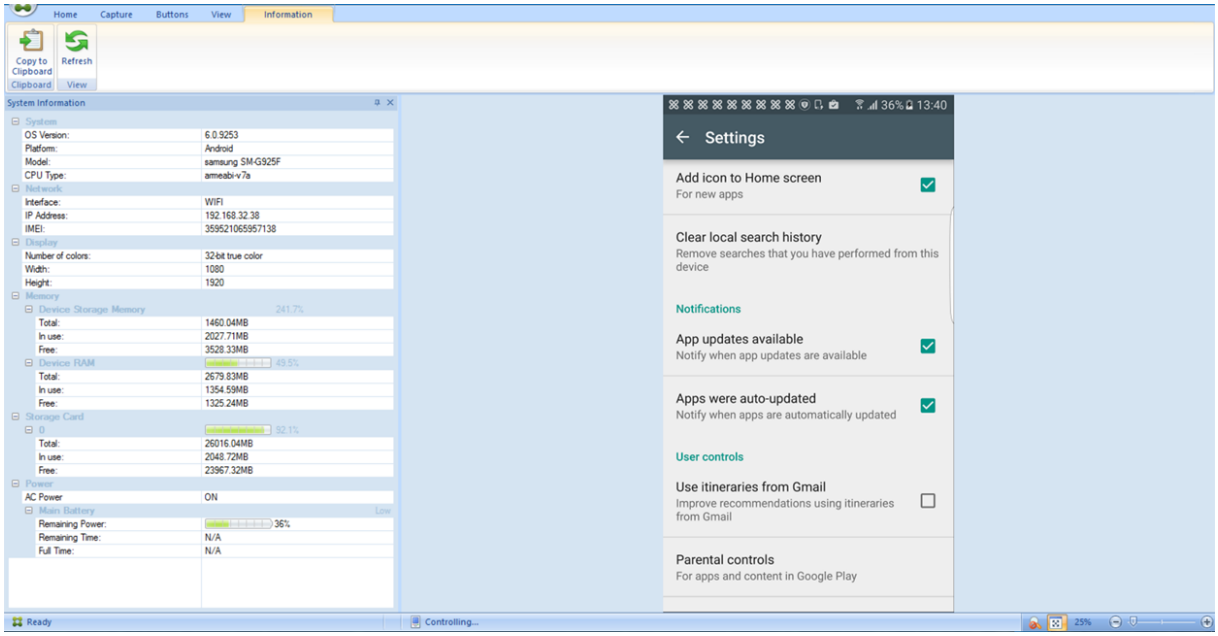
> Kunden können das Produkt weiterhin verwenden, Citrix stellt jedoch keine Neuerungen oder Fixes bereit.

Für on-premises XenMobile Server-Bereitstellungen: Durch Remotesupport können Helpdesk-Mitarbeiter die Fernsteuerung verwalteter Windows CE- und Android-Mobilgeräte übernehmen. Screencast wird nur auf Samsung Knox-Geräten unterstützt.

Remotesupport ist nicht für geclusterte on-premises XenMobile Server-Bereitstellungen verfügbar.

Während einer Remotesteuerungssitzung:

- Benutzern wird auf ihrem Mobilgerät durch ein Symbol angezeigt, dass eine Remotesteuerungssitzung aktiv ist.
- Remote Support-Mitarbeiter sehen das Remote Support-Anwendungsfenster und ein Remotesteuerungsfenster, das eine Darstellung des gesteuerten Geräts zeigt.



Remote Support bietet die folgenden Funktionen:

- Remoteanmeldung an dem Benutzergerät 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 oder Windows 11
- Microsoft Windows 8
- Microsoft Windows 7

Installieren von Remote Support über die Befehlszeile

Führen Sie den folgenden Befehl aus:

```
1 \*RemoteSupport\*.exe /S
```

RemoteSupport ist der Name des Installationsprogramms. Beispiel:

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

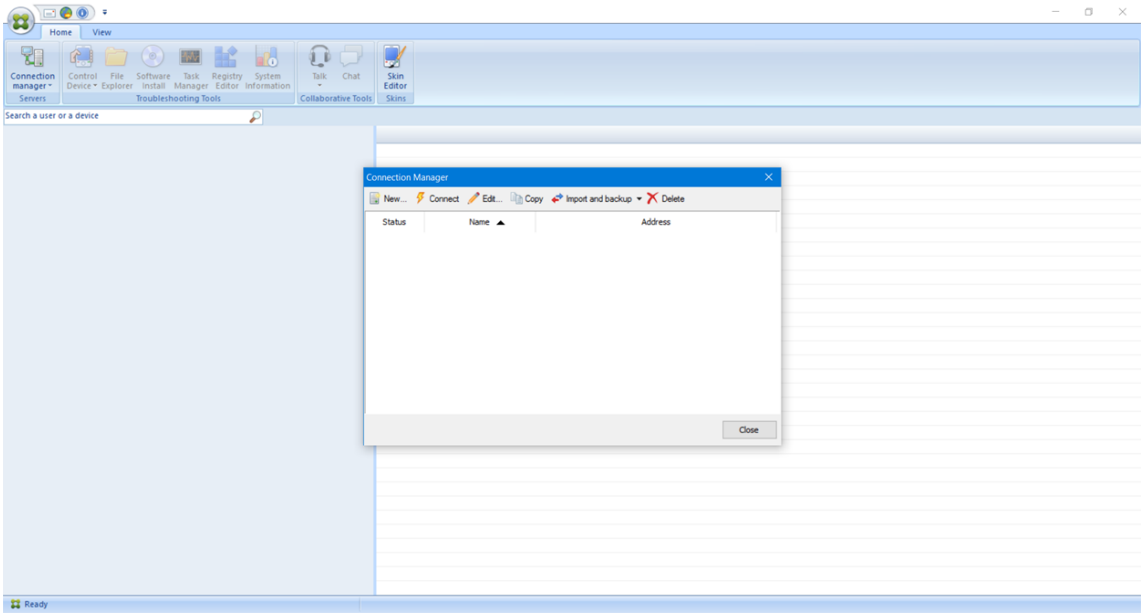
Beim Installieren der Remote Support-Software können Sie die folgenden Variablen verwenden:

- /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 unter **Configuration name** einen Namen für die Konfiguration ein.

   b) Geben Sie unter **Server IP address or name** die IP-Adresse oder den DNS-Namen des XenMobile-Servers ein.

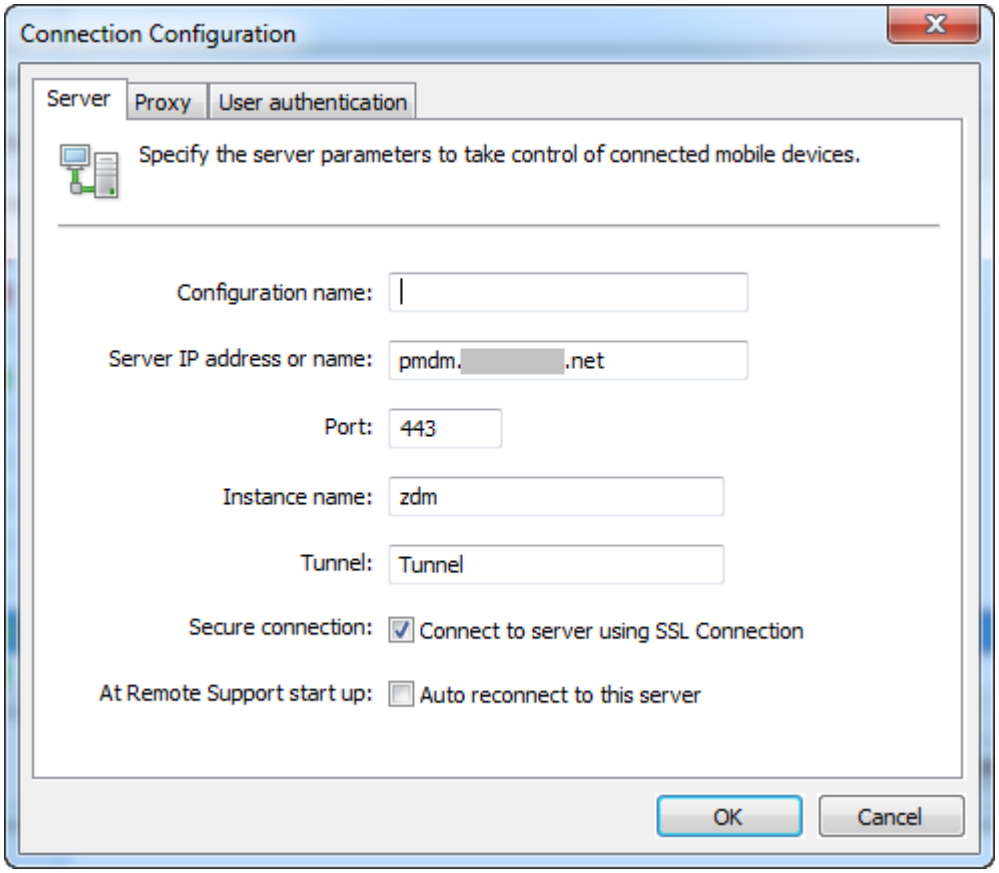
   c) Geben Sie unter **Port** eine TCP-Portnummer gemäß der Konfiguration von XenMobile-Server ein.

   d) Geben Sie unter **Instance name** einen Instanznamen ein, wenn XenMobile Teil einer Bereitstellung mit mehreren Mandanten ist.

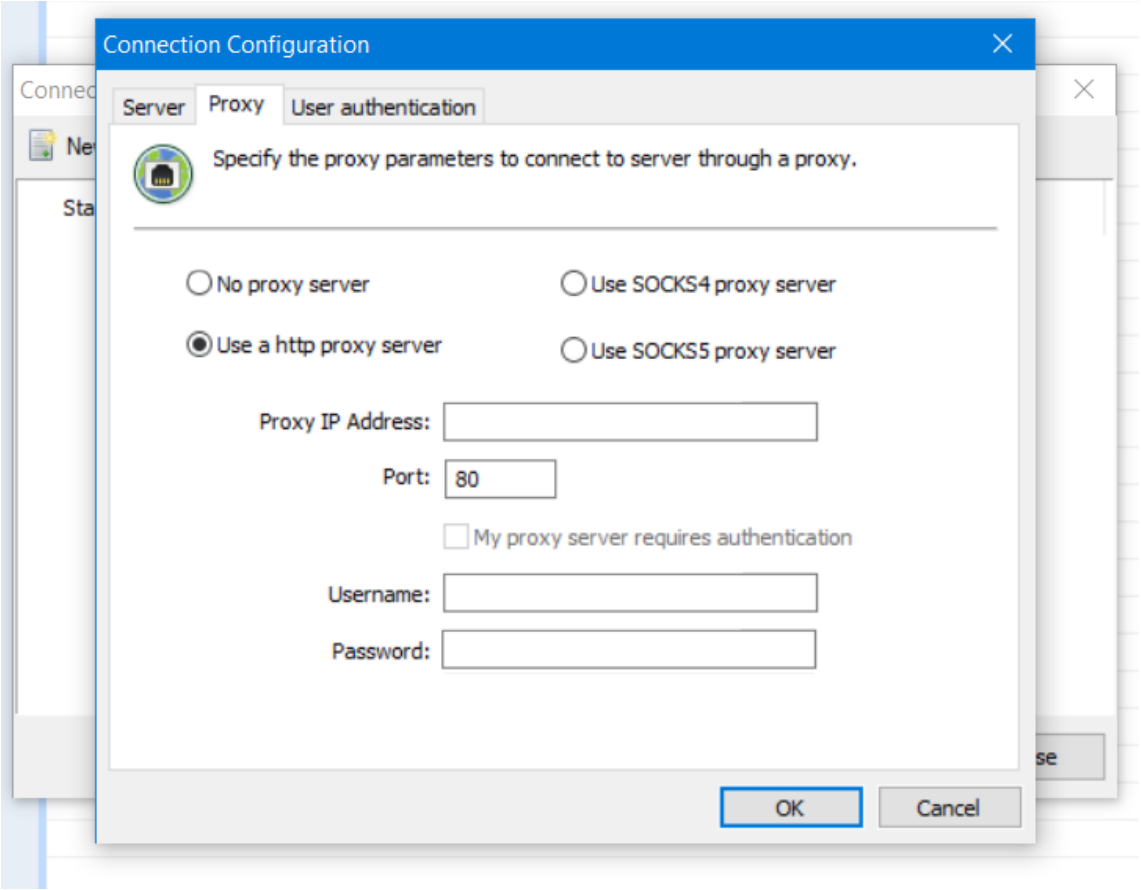
   e) Geben Sie unter **Tunnel** den Namen der Tunnelrichtlinie ein.

   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 für **Proxy IP Address** die IP-Adresse des Proxyservers ein.
    b) Geben Sie unter **Port** die Nummer des von dem Proxyserver verwendeten TCP-Ports ein.
    c) Aktivieren Sie das Kontrollkästchen **My proxy server requires authentication**, wenn der Proxyserver eine Authentifizierung erfordert, um Datenverkehr zuzulassen.
    d) Geben Sie unter **Username** den Benutzernamen für die Authentifizierung bei dem Proxyserver ein.
    e) Geben Sie unter **Password** das Kennwort für die Authentifizierung bei 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:** Anzeige von Diagnoseinformationen zum Gerät. Dazu gehören Systeminformationen, ausgeführte Prozesse, Task-Manager (Arbeitsspeicher und CPU-Nutzung), Inhalt des Ordners für installierte Software usw.
- **Premiumremotesupport:** Remotesteuerung des Gerätebildschirms. Sie können beispielsweise die Farben im Fenster steuern, eine VoIP-Sitzung zwischen Helpdesk und Benutzer einrichten und eine Chatsitzung zwischen Helpdesk und Benutzer erstellen.

Bei Premiumremotesupport 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**. Für die Plattform Samsung SAFE wird der ELM-Schlüssel bei der Registrierung bei XenMobile automatisch auf Samsung-Geräten bereitgestellt. Wählen Sie daher die Plattform Samsung SAFE nicht für diese Richtlinie aus. Weitere Informationen finden Sie unter Samsung MDM-Richtlinien für Geräte.

Informationen zum Konfigurieren der Richtlinie "Remotesupport" 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 XenMobile Server verbundenen Benutzer sind durch ein grünes Symbol gekennzeichnet.
2. Zum Anzeigen aller Benutzer, einschließlich der derzeit nicht verbundenen, klicken Sie auf **View** und wählen Sie **Non-connected devices**.
   Nicht verbundene Benutzer werden ohne grünes Symbol angezeigt.

Geräte mit einer Verbindung mit XenMobile Server, die keinem Benutzer zugewiesen sind, sind als anonym gekennzeichnet. (Die Zeichenfolge **Anonymous** wird in der Liste angezeigt.) Diese Geräte können genauso wie Geräte angemeldeter Benutzer gesteuert werden.

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

Syslog

November 10, 2020

Sie können XenMobile Server (nur lokal) 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

XenMobile verwendet den log4j-SyslogAppender zum Senden von syslog-Meldungen im RFC5424-Format. Die Daten in der syslog-Meldung sind reiner Text ohne ein bestimmtes Format.

Sie können anhand dieser Informationen die Ursache einer Warnung analysieren und ggf. Maßnahmen ergreifen.

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.
  - Debugprotokolle für XenMobile.

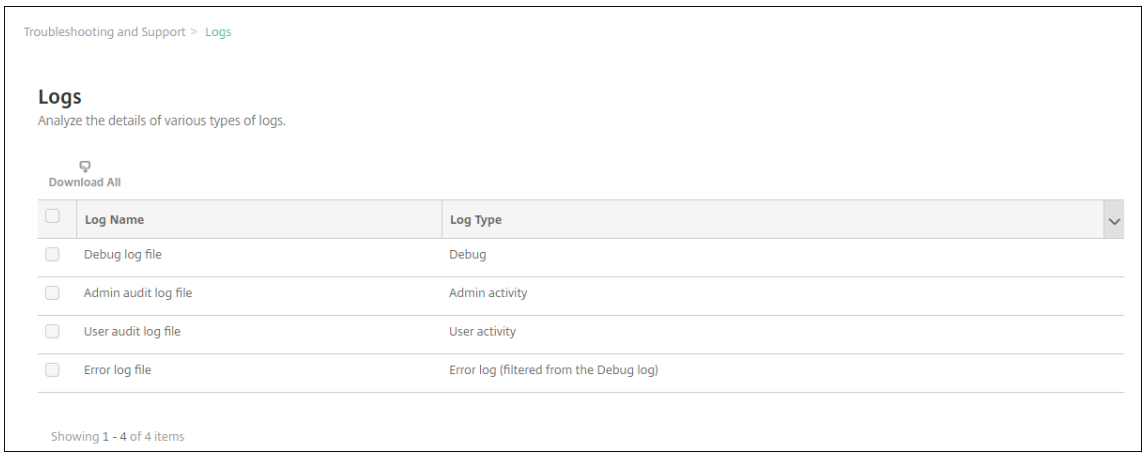
4. Klicken Sie auf **Speichern**.

Anzeigen von Protokolldateien in XenMobile

September 24, 2021

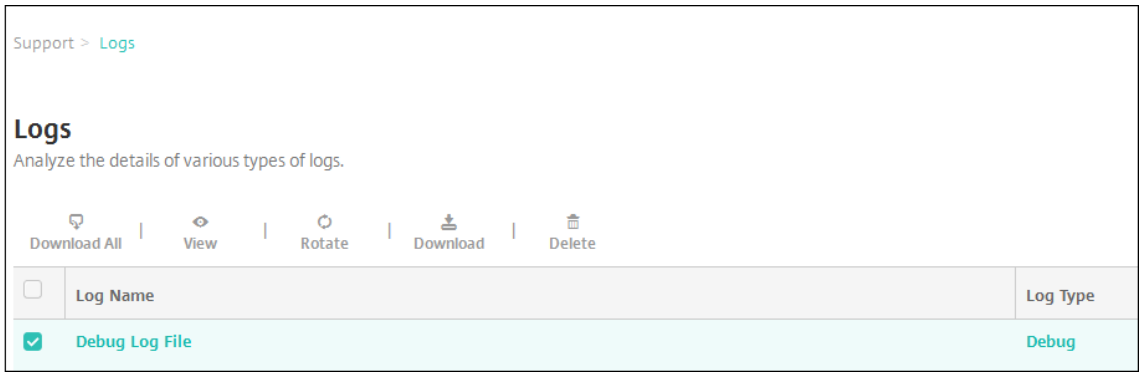
Für die Verwaltung mit XenMobile zeigen Sie Protokolle an, bearbeiten oder laden Sie sie herunter.

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 in der XenMobile-Konsole.
   - Benutzerüberwachungsprotokolle enthalten Informationen über konfigurierte Benutzer.
   - Fehlerprotokolldateien enthalten nur Fehlermeldungen, die aus dem Debugprotokoll gefiltert wurden.

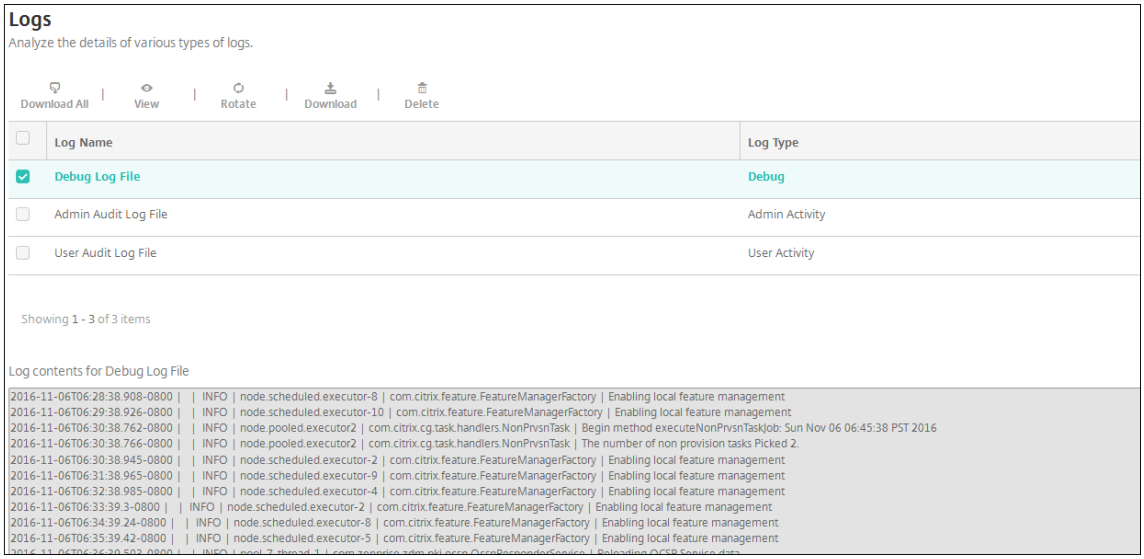
4. Verwenden Sie die Aktionen oberhalb der Tabelle zum Herunterladen aller oder einzelner Protokolle sowie zum Anzeigen, Archivieren und Löschen des ausgewählten Protokolls.



> **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-, Administrator-/Benutzerüberwachungs-, Serverprotokoll 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.



XenMobile Analyzer

January 5, 2022

XenMobile Analyzer ist ein cloudbasiertes Tool, mit dem Sie mit XenMobile zusammenhängende Konfigurationsprobleme 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.

Konfigurieren Sie das Tool, sodass es auf XenMobile Server verweist, und geben Sie Informationen wie Serverbereitstellungstyp, mobile Plattform, Authentifizierungstyp und die Anmeldeinformationen des Benutzers an. 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.

Hauptfeatures

- Sicherer, cloudbasierter Microservice zur Behandlung von mit XenMobile verbundenen Problemen
- Zielgenaue Empfehlungen zur Behebung von XenMobile-Konfigurationsproblemen
- Reduzierte Anzahl von Supportanrufen und schnellere Problembehandlung in XenMobile-Umgebungen
- Zero-Day-Support für Releases von XenMobile Server
- Planung täglicher oder wöchentlicher Systemdiagnosen
- Citrix ADC-Konfigurationsprüfung.

- Tests der Erreichbarkeit von Intranetsites für Secure Web.
- Prüfung des Autodiscovery-Diensts für Secure Mail
- Single Sign-On-Prüfungen (SSO) für Citrix Files.

Neue Features

- Der Citrix ADC-Konfigurationsbericht enthält einen Zähler mit der Anzahl der Empfehlungen. Die Empfehlungen basieren auf den grundlegenden Konfigurationsprüfungen eines spezifischen Citrix Gateway.
- Die Symbole auf der globalen Navigationsleiste der Seite mit den Testumgebungen wurden zur Verbesserung der Benutzererfahrung umgeordnet.

Im folgenden Video werden die Navigationsänderungen bei der Benutzeroberfläche gezeigt.

Citrix XenMobile Analyzer: neue Umgebungslisten-Benutzeroberfläche

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video wiederzugeben

> **Hinweis:**
>
> Das Video ist ohne Ton. Es wird am besten im Vollbildmodus abgespielt.

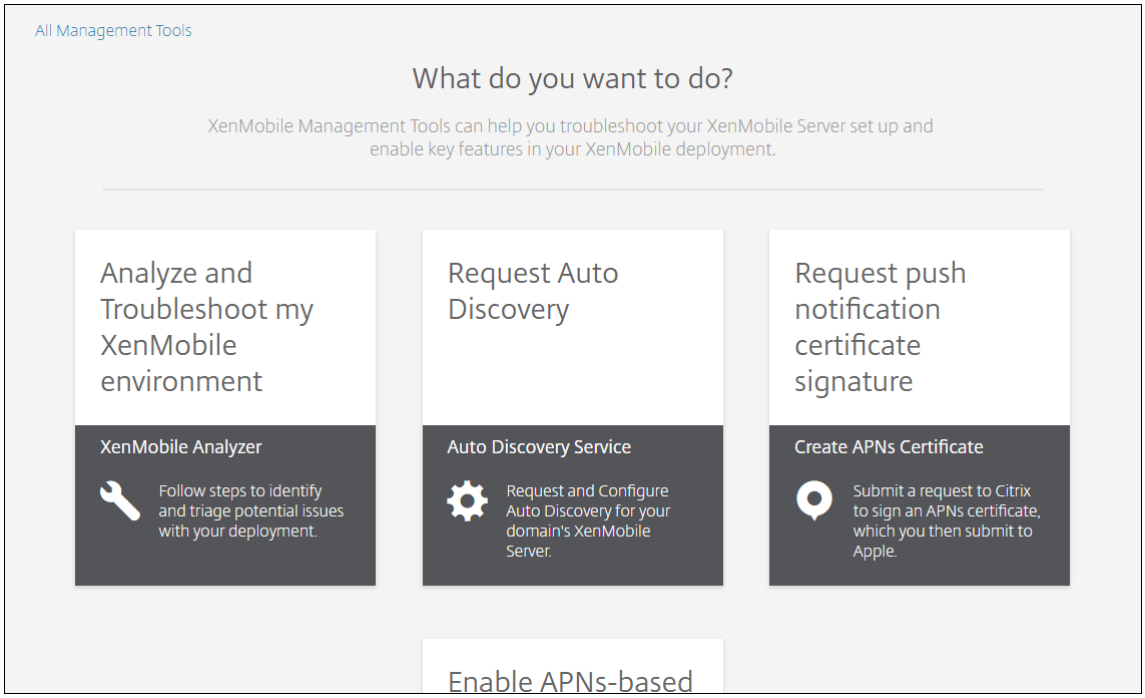
Zugriff auf XenMobile Analyzer und Programmstart

Voraussetzungen

Produkt	Unterstützte Version
XenMobile Server	10.1.0 und später
Citrix Gateway	10.5 und höher
Simulation der Clientregistrierung	iOS und Android

Rufen Sie XenMobile Analyzer mit einer der folgenden Methoden auf:

- Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol oben rechts, um die Seite **Problembehandlung und Support** anzuzeigen.
- Rufen Sie das Tool über https://tools.xm.cloud.com/ unter Verwendung Ihrer Citrix Anmeldeinformationen auf. Die XenMobile-Seite für Verwaltungstools wird geöffnet. Klicken Sie hier auf **Analyze and Troubleshoot my XenMobile Environment**, um XenMobile Analyzer zu starten.



XenMobile Analyzer bietet fünf Optionen, die Sie durch den Selektierungsvorgang führen. Dies reduziert die Anzahl an Supporttickets. Die Kosten können ebenfalls verringert werden.

Die folgenden Optionen stehen zur Auswahl:

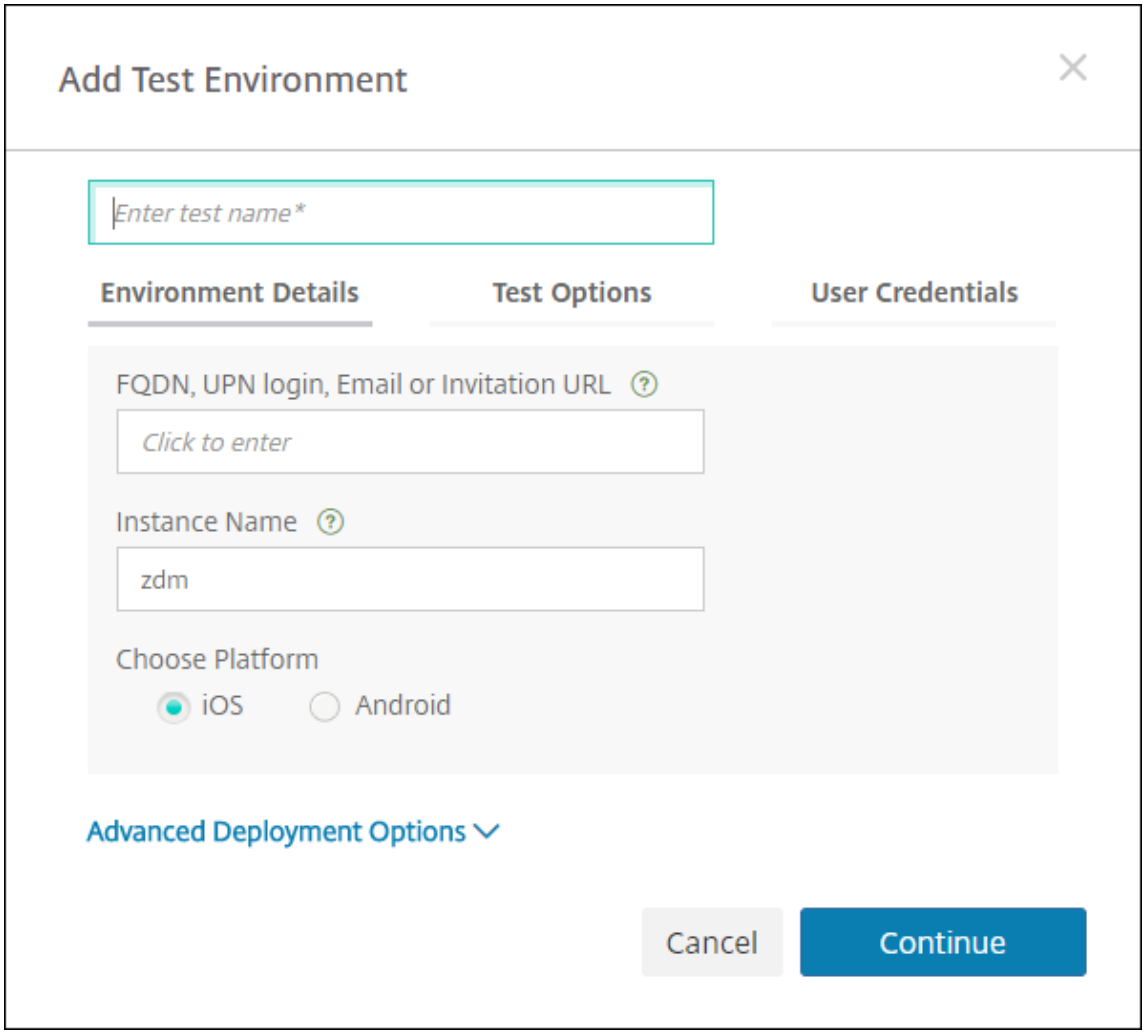
- **Environment Check:** In diesem Schritt richten Sie Tests ein, um das Setup auf Probleme zu prüfen. Der Schritt bietet auch Empfehlungen und Lösungen zu Problemen bei der Registrierung und Authentifizierung von Geräten und Benutzern.
- **Citrix ADC Check:** In diesem Schritt prüfen Sie, ob die Citrix ADC-Konfigurationen eine Bereitstellung von XenMobile zulassen.
- **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.
- **Server Connectivity Checks:** In diesem Schritt testen Sie die Konnektivität Ihrer Server.
- **Contact Citrix Support:** Wenn Sie immer noch Probleme haben, werden Sie in diesem Schritt zur Supportsite weitergeleitet, wo Sie einen Citrix Supportfall erstellen können.

In den folgenden Abschnitten werden die einzelnen Optionen detailliert erläutert.

Ausführen einer Umgebungsprüfung

1. Melden Sie sich bei XenMobile Analyzer an und klicken Sie auf **XenMobile Environment**.

2. Klicken Sie auf **Add Test Environment**.
3. Führen Sie im Dialogfeld **Add Test Environment** die folgenden Schritte aus:



a) Geben Sie einen eindeutigen Namen für den Test ein, damit Sie den Test zukünftig leicht identifizieren können.

b) Geben Sie unter **FQDN, UPN login, Email or URL Invitation** die Zugangsinformationen für den Server ein.

c) Wenn Sie eine benutzerdefinierte Instanz verwenden, geben Sie den Wert in **Instance Name** 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 Management (MDM)** zur Verfügung.

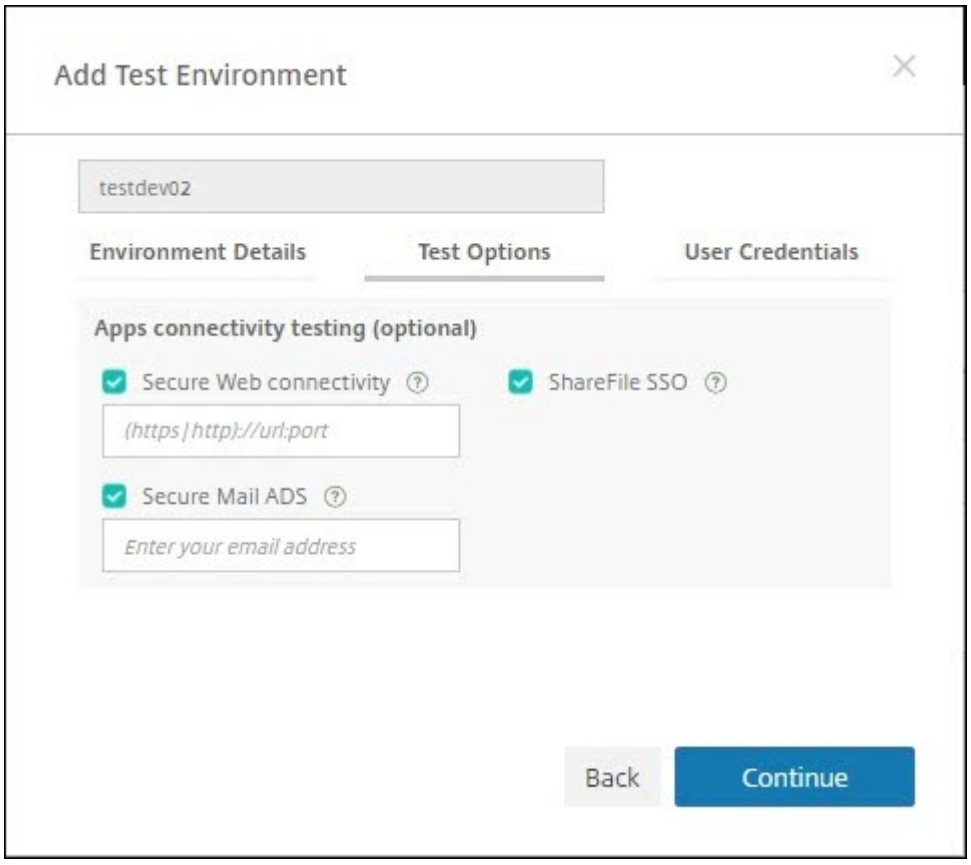
f) Klicken Sie auf **Weiter**.

4. Wählen Sie auf der Registerkarte **Test Options** einen oder mehrere der folgenden Tests und klicken Sie auf **Continue**.

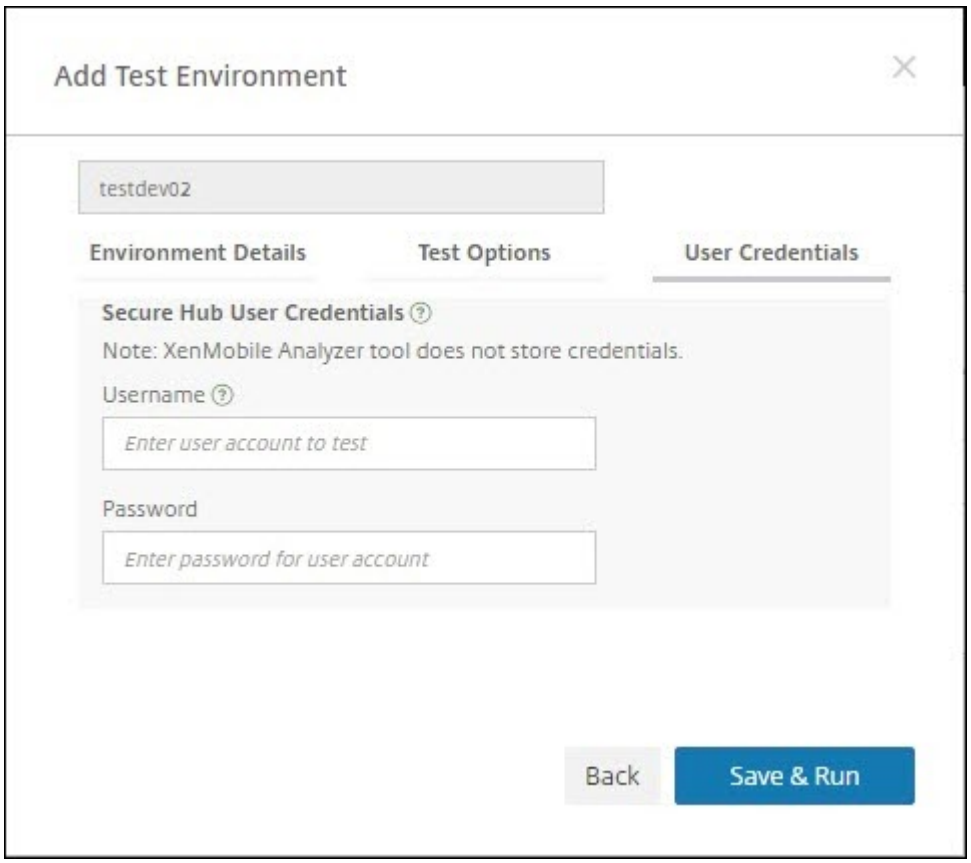
   a) **Secure Web Connectivity**. Geben Sie eine Intranet-URL an. Das Tool testet die Erreichbarkeit der URL. Dadurch werden mögliche Konnektivitätsprobleme in der Secure Web-App erkannt, die beim Versuch, Intranet-URLs zu erreichen, auftreten können.

   b) **Secure Mail ADS**: Geben Sie die E-Mail-Adresse eines Benutzers an. Mit dieser Adresse 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**: Wird dieser Test ausgewählt, testet XenMobile Analyzer auf eine erfolgreiche Citrix Files-DNS-Auflösung. Das Tool überprüft auch, ob Citrix Files Single Sign-on (SSO) mit den angegebenen Anmeldeinformationen kompatibel ist.



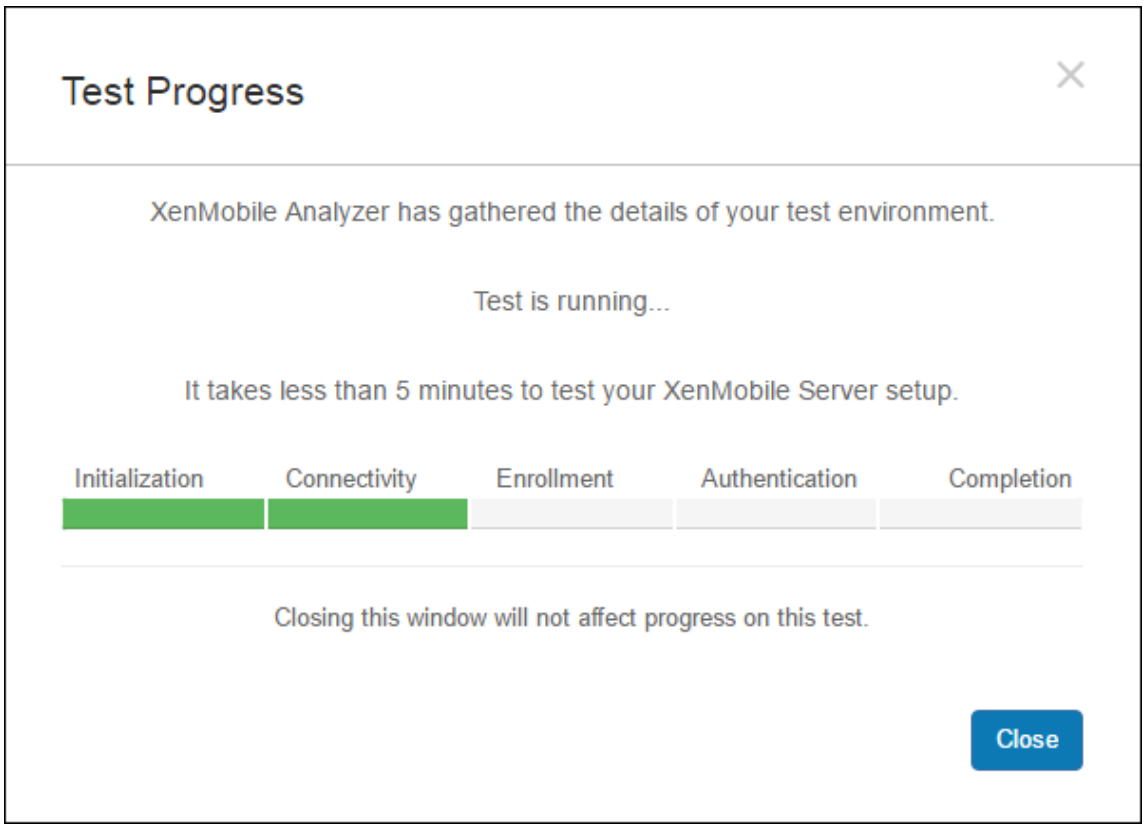
5. Abhängig von Ihrem Serversetup werden auf der Registerkarte **User Credentials** ggf. unterschiedliche Felder angezeigt. Mögliche Felder: **Username**, **Username and Password** oder **Username, Password** und **Enrollment PIN**.



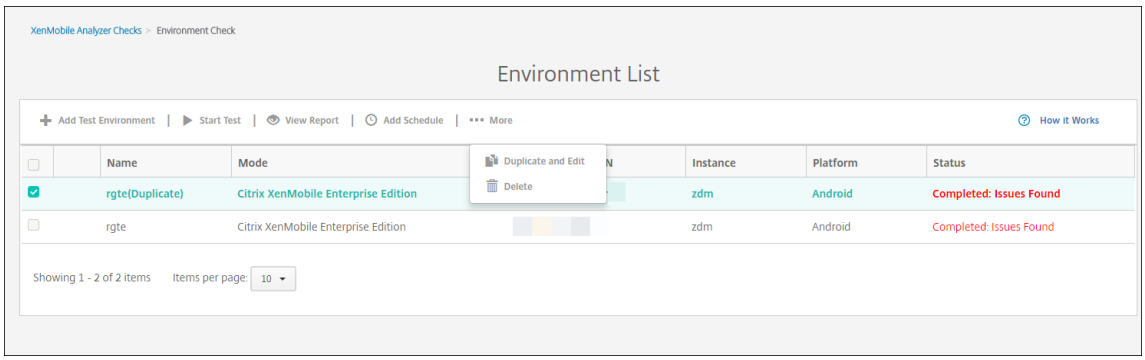
6. Klicken Sie auf **Save & Run**, um die Tests zu starten.

   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.



Nach dem Schließen des Statusdialogfelds kehren Sie zur Seite **Environments List** zurück.



Auf der Seite **Results** werden Testdetails, Empfehlungen und Ergebnisse angezeigt.

7. Klicken Sie auf das Symbol **View Report** zum Anzeigen der Testergebnisse.

   Wenn Empfehlungen mit Citrix Knowledge Base-Artikeln verknüpft sind, werden die Artikel auf dieser Seite aufgeführt.

8. Klicken Sie auf die Registerkarte **Results**, um die einzelnen Kategorien und Tests, die das Tool ausgeführt hat, sowie die Ergebnisse anzuzeigen.

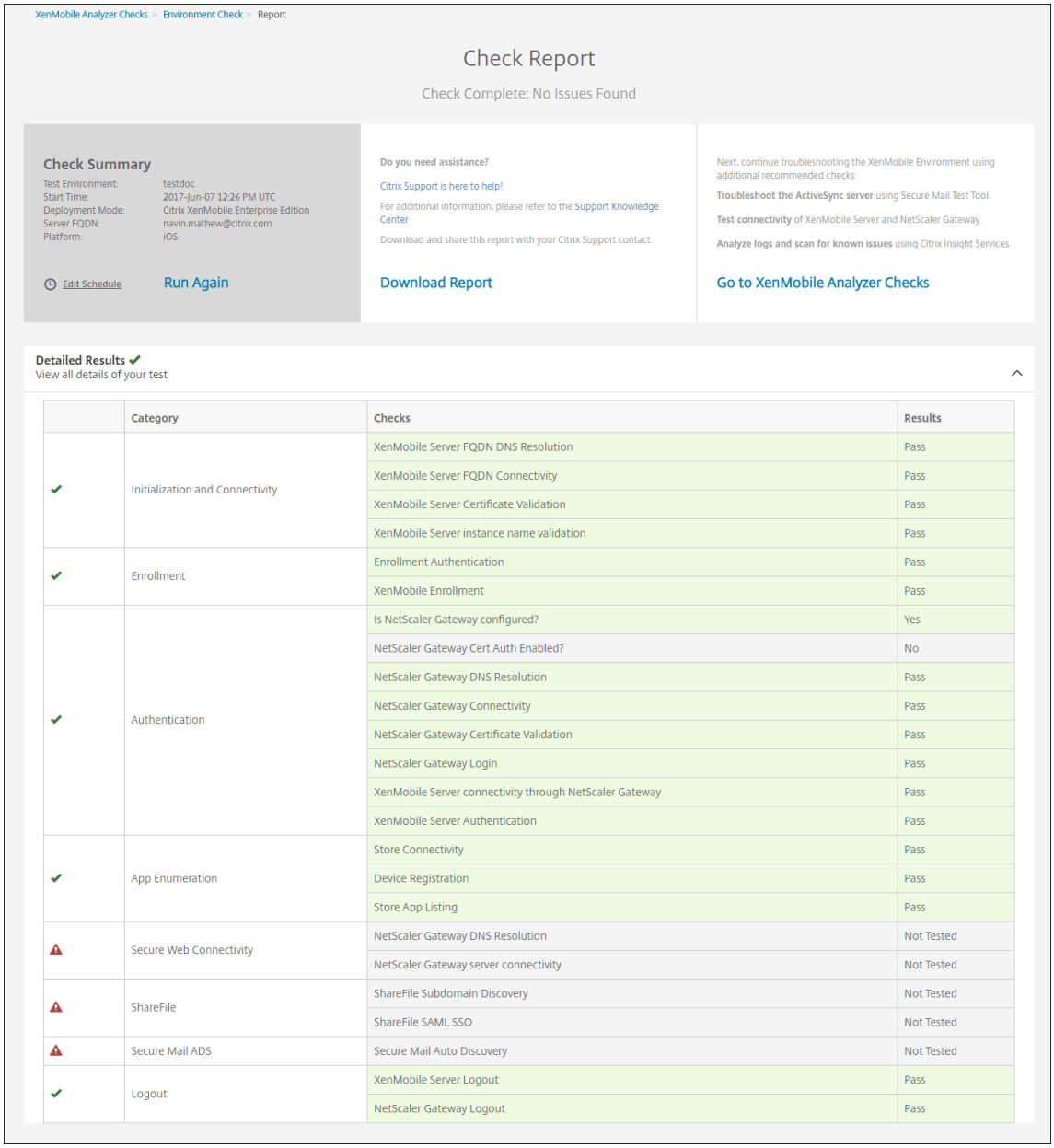
   a) Zum Herunterladen des Berichts klicken Sie auf **Download Report**.

   b) Wenn Sie zur Liste mit den Testumgebungen zurückkehren möchten, klicken Sie auf **Environment Check**.

c) Zum Wiederholen des Tests klicken Sie auf **Run Again**.

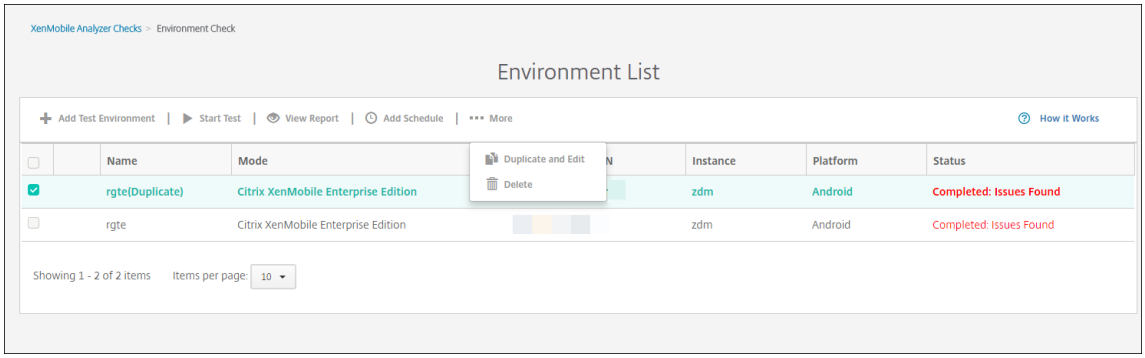
d) Wenn Sie einen anderen Test wiederholen möchten, wechseln Sie zu **Test Environments**, wählen Sie den Test aus und klicken Sie auf **Start Test**.

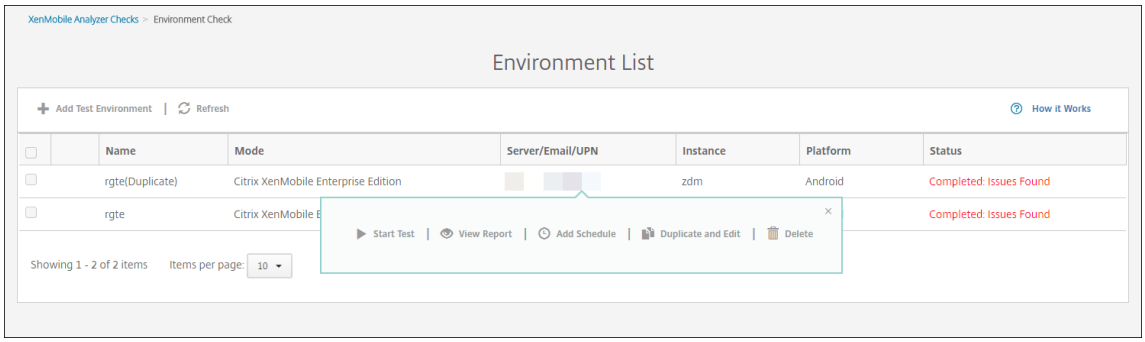
e) Um eine andere Option von XenMobile Analyzer auszuwählen, klicken Sie auf **Go To XenMobile Analyzer Checks**.

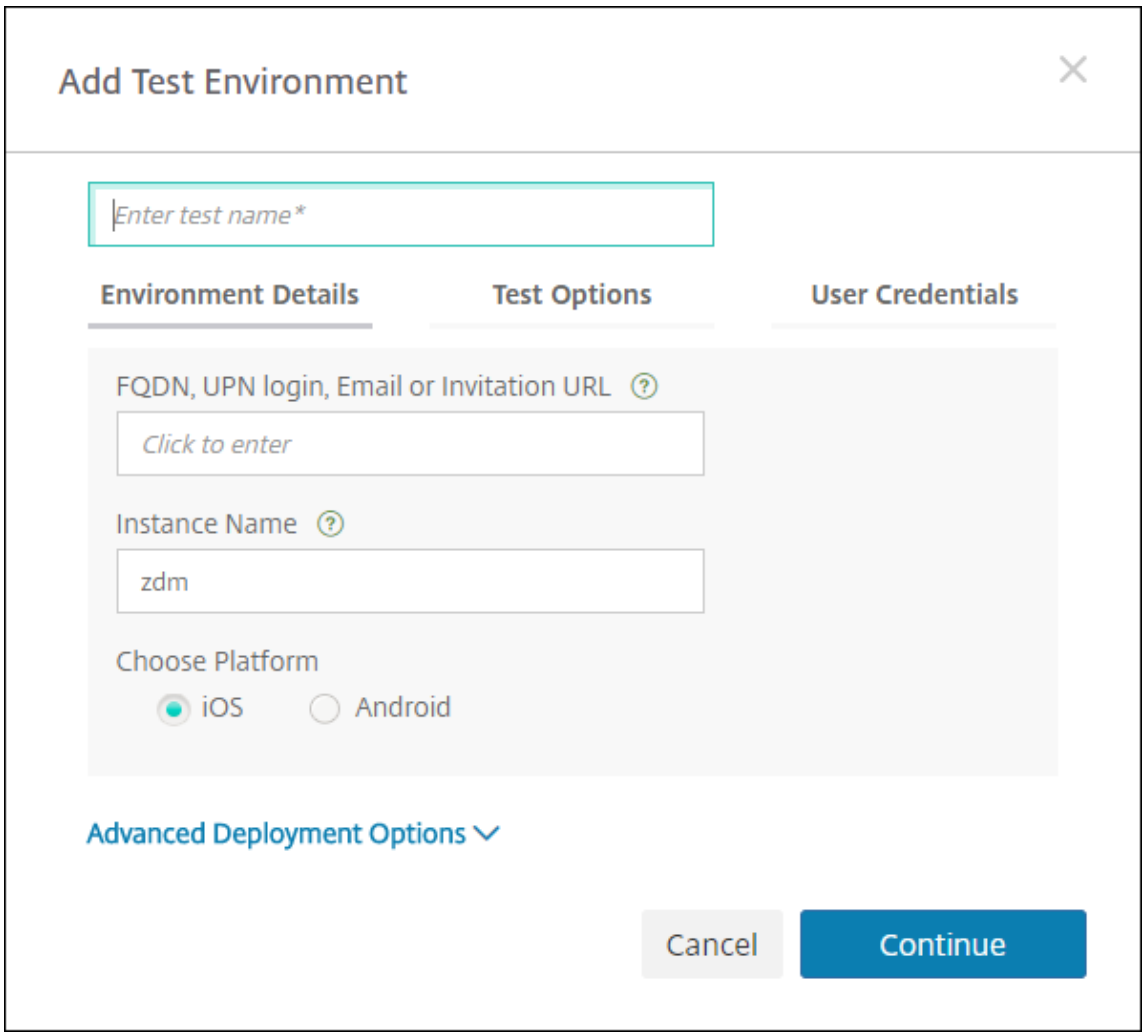


9. Sie können auf der Seite “Test Environments” Tests kopieren und bearbeiten. Wählen Sie hierfür einen Test aus, klicken Sie auf **More** und wählen Sie **Duplicate and Edit**.

   Es wird eine Kopie des ausgewählten Tests erstellt und das Dialogfeld “Add Test Environment” geöffnet, in dem Sie den neuen Test ändern können.



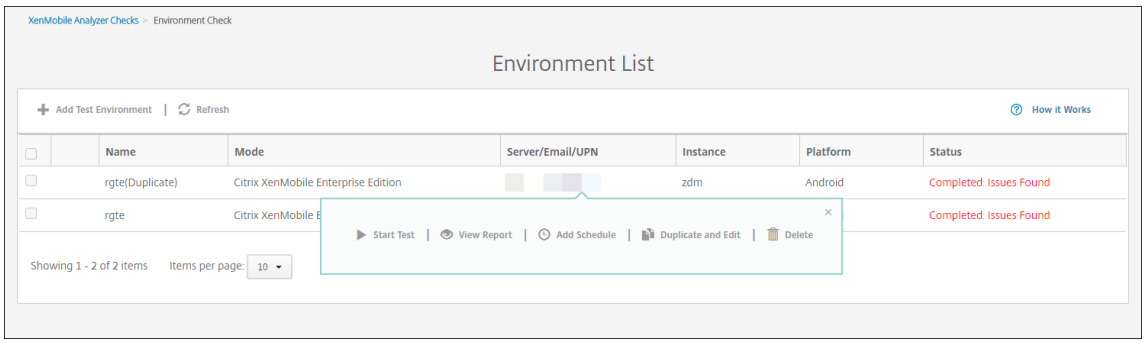




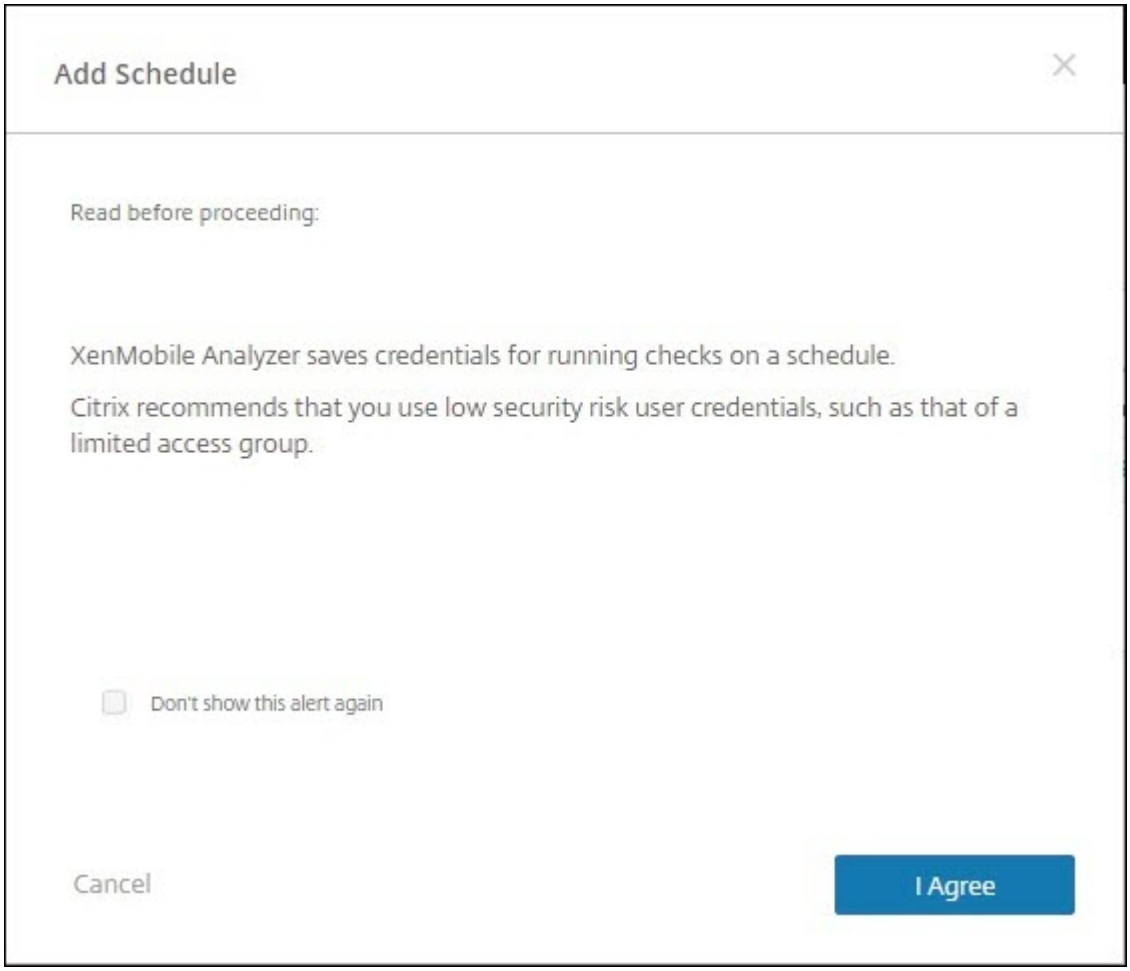
Erstellen eines Zeitplans für Umgebungsprüfungen

Tests können auch automatisch auf der Basis eines Zeitplans ausgeführt werden. Die Ergebnisse werden dann an eine konfigurierte Liste von Benutzern gesendet.

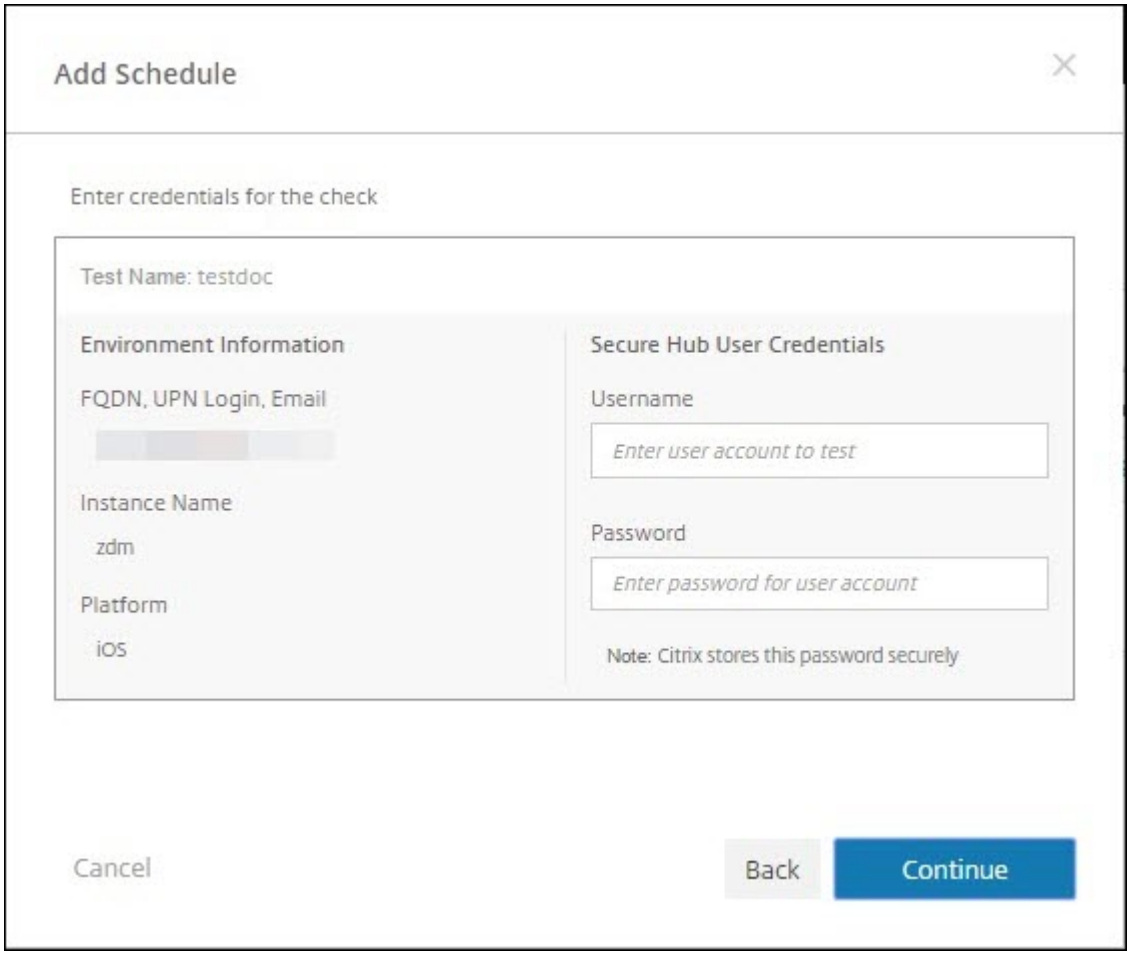
1. Wählen Sie auf der Seite **Environment List** die Umgebung aus, für die Sie einen Zeitplan einrichten möchten, und klicken Sie auf **Add Schedule**.



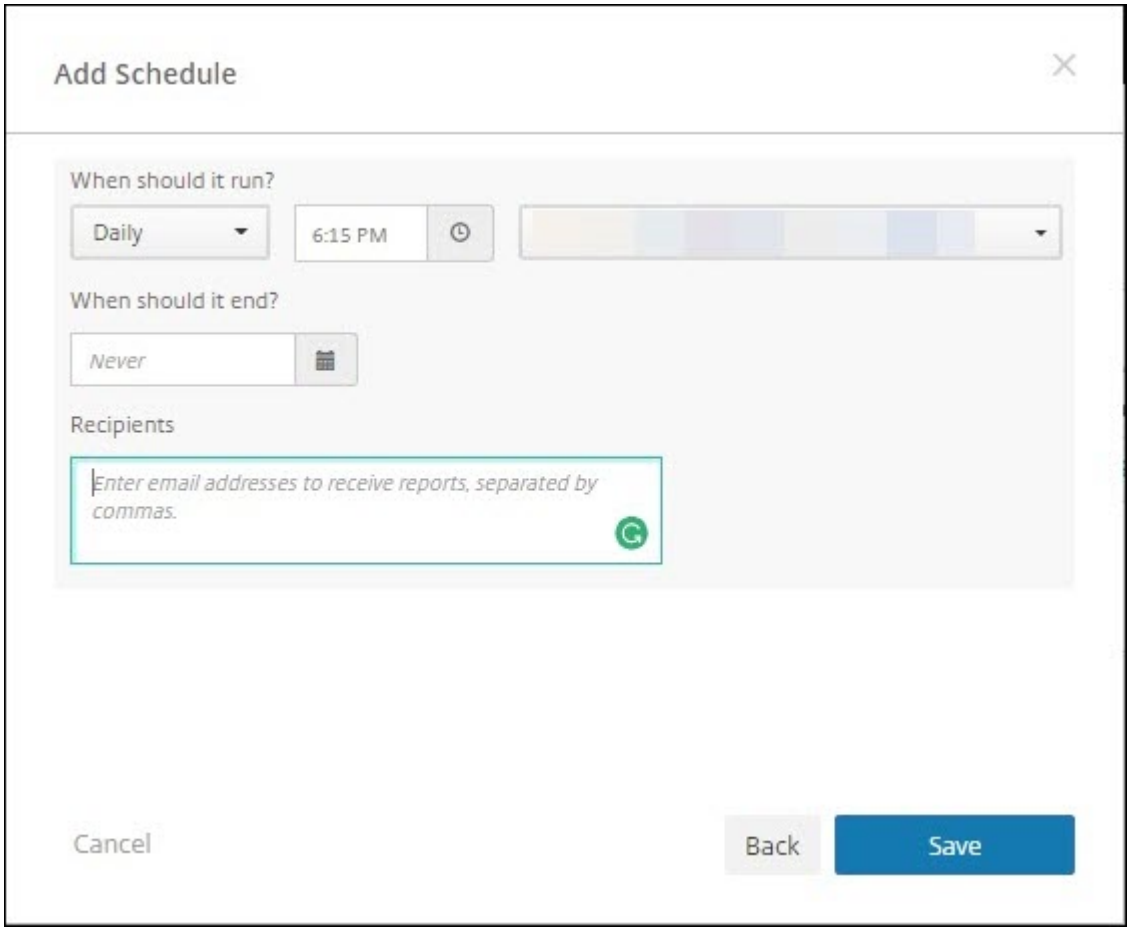
2. Im Fenster **Add Schedule** werden Sie in einer Warnmeldung darauf hingewiesen, dass die Anmeldeinformationen für das Ausführen geplanter Tests von XenMobile Analyzer gespeichert werden. Citrix empfiehlt, dass Sie zum Ausführen von geplanten Tests ein Konto mit eingeschränktem Zugriff verwenden. Klicken Sie zum Fortfahren auf **I Agree**.



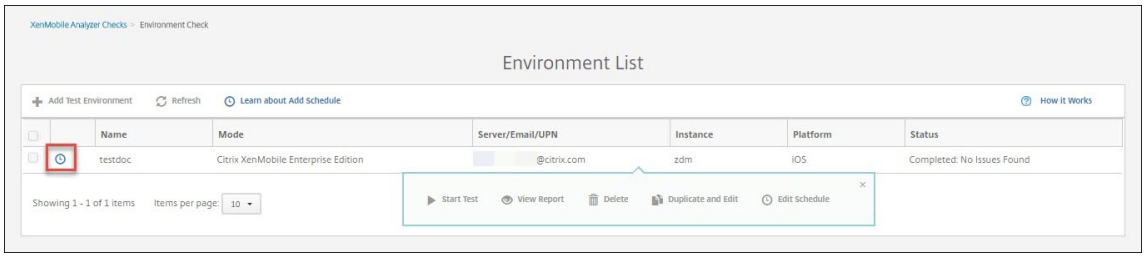
3. Geben Sie unter **Username** einen Benutzernamen und unter **Password** ein Kennwort für den Test ein.



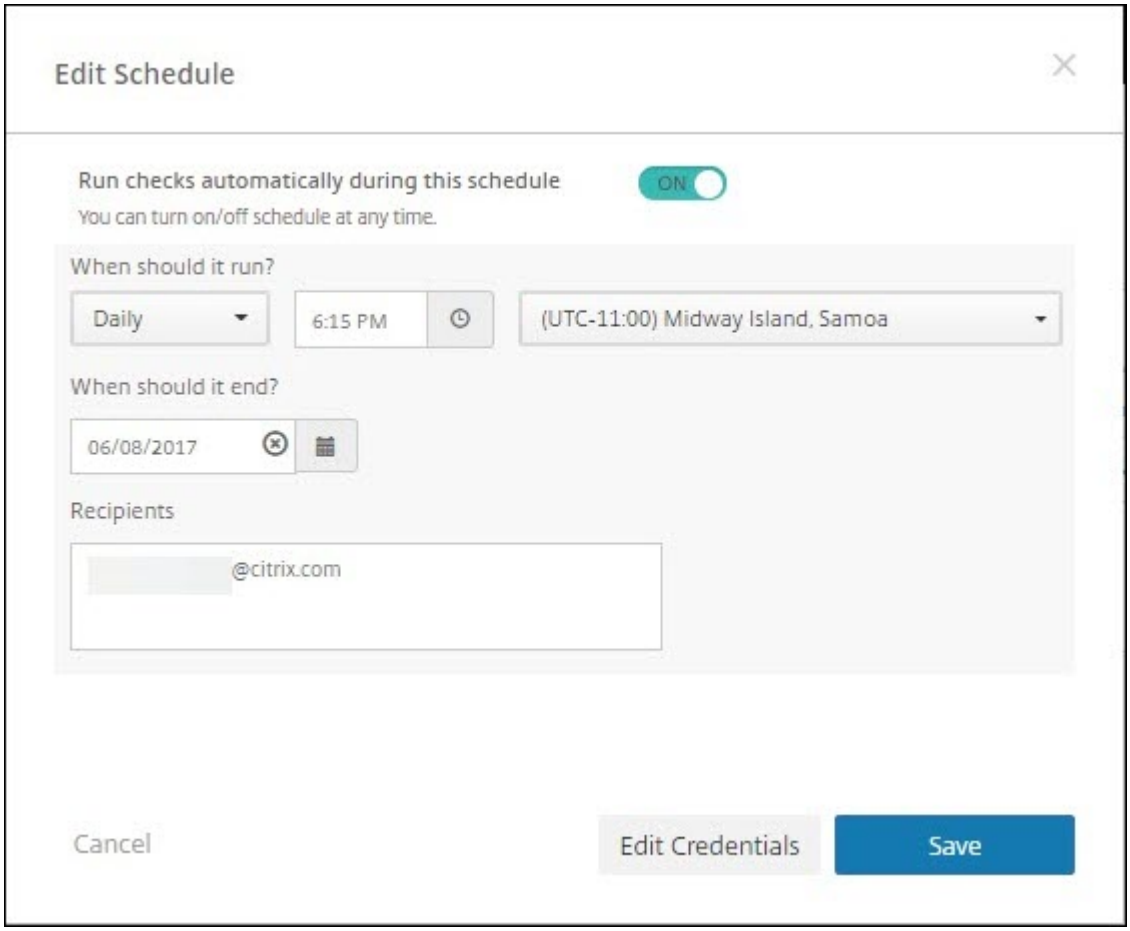
4. Konfigurieren Sie einen Zeitplan für den Test. In der Dropdown-Liste können Sie auswählen, ob der Test täglich (**Daily**) oder wöchentlich (**Weekly**) ausgeführt werden soll. Wählen Sie eine Uhrzeit und eine Zeitzone für den Test aus. Legen Sie mit der Datumsauswahl einen Endtermin für den Test fest oder lassen Sie das Feld frei, um den Test dauerhaft auszuführen. Geben Sie unter “Recipients” die E-Mail-Adressen der Berichtempfänger ein und trennen Sie diese durch Kommas. Klicken Sie auf **Speichern**.



5. Ein Uhrsymbol links neben dem Test gibt an, dass ein Zeitplan konfiguriert wurde. Markieren Sie den Test und klicken Sie auf **Edit Schedule**, um den Zeitpunkt des Tests zu ändern.



6. In diesem Fenster können Sie den Zeitpunkt ändern, zu dem der Test ausgeführt wird. Sie können den Test auch deaktivieren, indem Sie auf den Schalter oben im Dialogfeld klicken. Klicken Sie abschließend auf **Save**.



Ausführen weiterer Prüfungen zur Informationsgewinnung

Während Sie bei der Umgebungsprüfung mit XenMobile Analyzer direkt zum Ausführen von Tests interagieren, sind die übrigen Optionen rein informativ. Diese Optionen enthalten Informationen für andere Supporttools, mit denen Sie sicherstellen können, dass die XenMobile-Umgebung richtig eingerichtet ist.

- **Advanced Diagnostics:** Hiermit können Sie Informationen über Ihre Umgebung sammeln und an Citrix Insight Services weiterleiten. Das Tool analysiert Ihre Daten und erstellt einen personalisierten Bericht mit empfohlenen Lösungen.
- **Secure Mail Readiness:** Hiermit werden Sie durch das Herunterladen und Ausführen der XenMobile Exchange ActiveSync Test-Anwendung geführt. 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.
- **Server Connectivity Checks:** Hiermit können Sie die Verbindungen mit XenMobile-, Authentifizierungs- und Content Collaboration-Servern überprüfen.
- **Contact Citrix Support:** Wenn gar nichts hilft, können Sie ein Supportticket beim Citrix Support erstellen.

Bekannte Probleme

Im XenMobile Analyzer sind die nachfolgend aufgeführten Probleme bekannt:

- Bei den Tests der Secure Web-Konnektivität 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.

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.

REST APIs

January 5, 2022

> **Hinweis:**
>
> In diesem Artikel werden die REST APIs von XenMobile Server behandelt. Informationen zu den REST-APIs von Endpoint Management finden Sie unter REST APIs.

Mit der REST API für XenMobile 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 an der XenMobile-Konsole.

Eine umfassende, aktuelle Liste der verfügbaren APIs finden Sie in der PDF-Datei Public API for REST Services.

Erforderliche Berechtigungen für den Zugriff auf die REST API

Für den Zugriff auf die REST API ist eine der folgenden Berechtigungen erforderlich:

- Zugriffsberechtigung für öffentliche APIs, die bei der Konfiguration des rollenbasierten Zugriffs festgelegt wird Informationen 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.

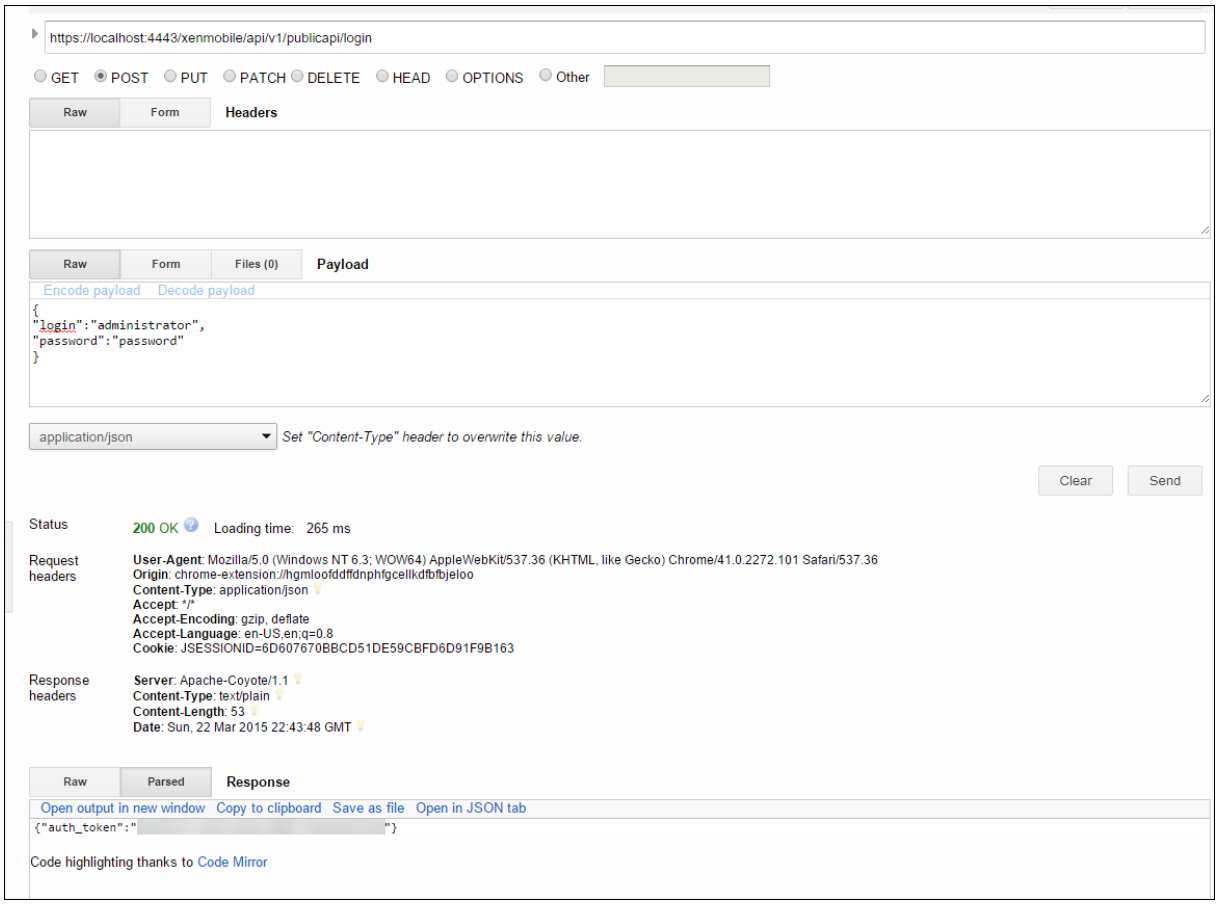
Anmeldung

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

Anforderung: `{ "login":"administrator", "password":"password"}`

Methodentyp: POST

Inhaltstyp: application/json



Verwandte Informationen

- XenMobile REST API

Endpoint Management Connector für Exchange ActiveSync

January 5, 2022

XenMobile Mail Manager heißt jetzt Endpoint Management Connector für Exchange ActiveSync. Weitere Informationen zum vereinheitlichten Citrix-Portfolio finden Sie im Citrix product name guide.

Der Connector erweitert die Funktionen von XenMobile auf folgenden Weise:

- 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.
- Löschen eines mobilen Geräts durch XenMobile auf der Basis des EAS-Status.
- Zugriff von XenMobile auf Informationen über Blackberry-Geräte, und Steuerungsvorgänge wie Löschen und Kennwort zurücksetzen.

Um ein Gerät basierend auf dem EAS-Status zu löschen, konfigurieren Sie eine automatisierte Aktion mit einem ActiveSync-Auslöser. Siehe Automatisierte Aktionen.

So laden Sie Endpoint Management Connector für Exchange ActiveSync herunter:

1. Gehen Sie zu https://www.citrix.com/downloads.
2. Navigieren Sie zu **Citrix Endpoint Management (und Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10 > Server Components**.
3. Klicken Sie auf der Kachel **Citrix Endpoint Management Connector für Exchange ActiveSync** auf **Download File**.

Neue Features

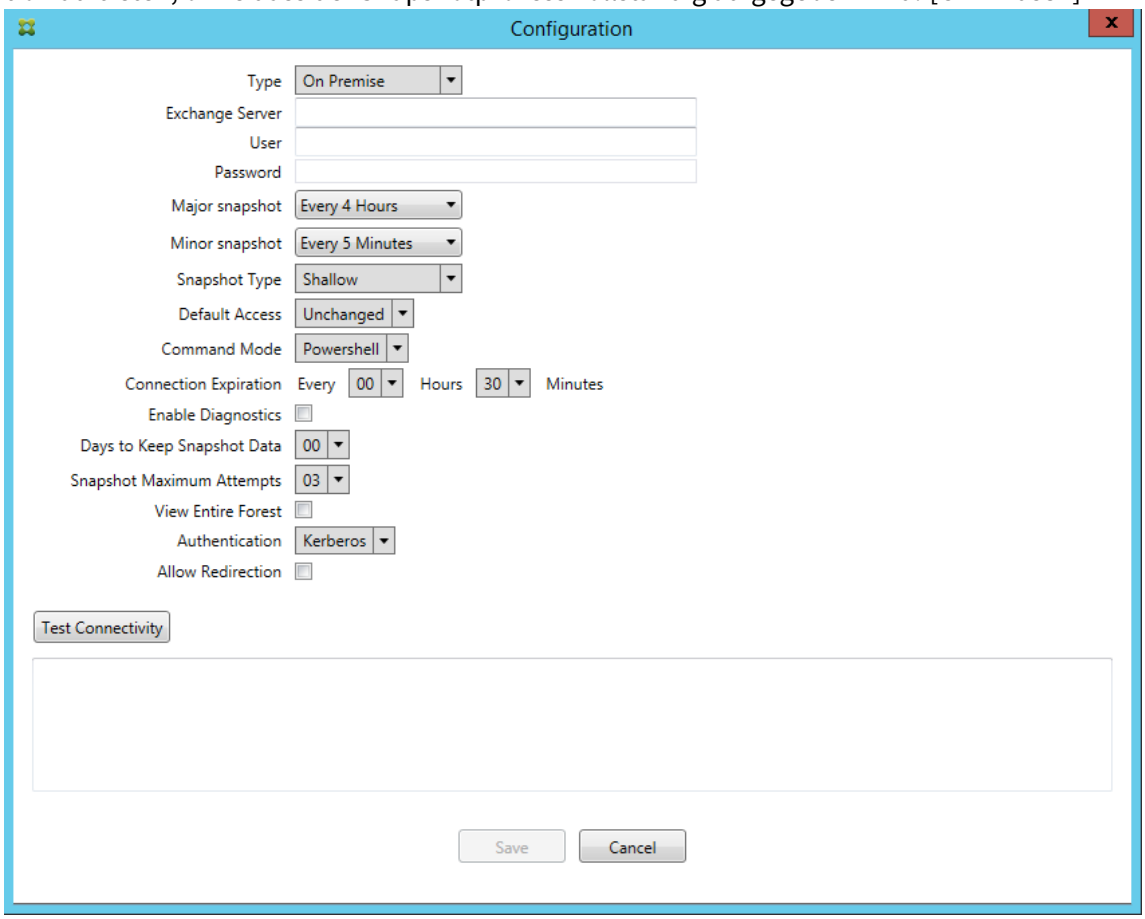
In den folgenden Abschnitten wird aufgeführt, was im Endpoint Management-Connector für Exchange ActiveSync (zuvor “XenMobile Mail Manager”) neu ist.

Neue Features in Version 10.1.10

Die folgenden Probleme wurden in Version 10.1.10 behoben:

- Kunden, bei denen häufig Netzwerkprobleme auftreten, können einen Snapshot möglicherweise nicht innerhalb der drei Versuche abschließen, die vorher verfügbar waren. Mit diesem Release kann ein Administrator die maximale Anzahl von Versuchen konfigurieren (1-10).

Dieser Fix ermöglicht, dass bei einem Snapshot mehrere Unterbrechungen in der Kommunikation auftreten, ohne dass der Snapshotprozess vollständig aufgegeben wird. [CXM-70837]



- In früheren Versionen wurde der Snapshottyp nicht in der Liste der Exchange-Konfigurationen angezeigt. Nun wird der Snapshottyp angezeigt. [CXM-70846]
- Die von PowerShell gemeldete PSRemotingTransport-Ausnahme weist darauf hin, dass die Exchange-Sitzung nicht mehr funktionsfähig ist. Der Status wird standardmäßig der Liste “Kritische Fehler” in der Konfigurationsdatei hinzugefügt. Wenn PSRemotingTransportException erkannt wird, wird die Verbindung zu einem fehlerhaft markiert für eine spätere Entfernung. Die nächste Kommunikation verwendet eine gültige Verbindung oder erstellt eine neue Verbindung. [XMHELP-2184, CXM-70836]
- Wenn eine Konfigurationsänderung gespeichert wird, ist es möglich, dass nicht alle zuvor konfigurierten internen Komponenten ordnungsgemäß entfernt werden, bevor die neue Konfiguration geladen wird. Dieses Problem kann zu unvorhersehbarem Verhalten führen. Das Verhalten hängt von der spezifischen Änderung ab und ob die Änderung mit der vorherigen Konfiguration in Konflikt steht. In dieser Version werden alle internen Komponenten entfernt, bevor die neue Konfiguration geladen wird. [XMHELP-2259, CXM-71388]

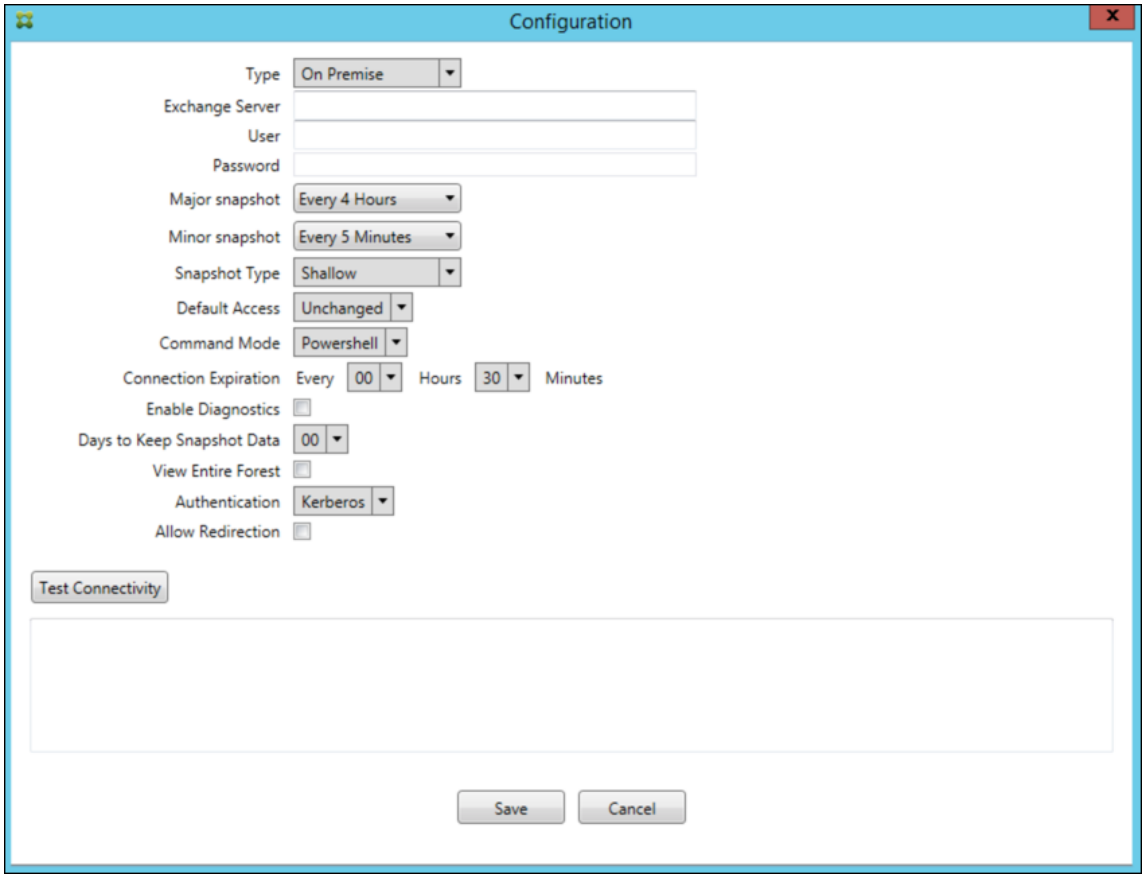
Was ist neu in früheren Releases

Im folgenden Abschnitt werden die Features und behobenen Probleme in früheren Versionen des Endpoint Management Connectors für Exchange ActiveSync aufgeführt.

Neue Features in Version 10.1.9

Die folgenden Probleme wurden in Version 10.1.9 behoben:

- Konfigurationsänderungen werden nun konsequenter umgesetzt. Sobald eine Konfigurationsänderung erkannt wird, wird jedes interne Subsystem gestoppt und jede aktive oder geplante Verarbeitung unterbrochen. Anschließend wird die neue Konfiguration geladen und die Subsysteme werden neu gestartet. Alle Zeitpläne und internen Infrastrukturelemente werden dann mit den neuen Einstellungen wiederhergestellt. Dies behebt ein bekanntes Problem in Version 10.1.8. [CXM-47709, CXM-61330]
- Während eines Upgrades wurde die vorhandene Datenbankkonfiguration nicht mit der neuen Konfigurationsdatei zusammengeführt. Die Datenbankkonfiguration wird nun in die aktualisierte Konfigurationsdatei integriert. [CXM-49326]
- In den Snapshot-bezogenen Diagnosedateien fehlten die Spaltenüberschriften. Die Kopfzeilen werden wiederhergestellt. [CXM-62680]
- Beim Upgrade von einer früheren Version wurden die Standardeinstellungen in der Konfigurationsdatei durch den entsprechenden Abschnitt in der bisher verwendeten Konfigurationsdatei überschrieben. Dadurch konnten Ergänzungen oder Verbesserungen dieses Abschnitts nach dem Upgrade nicht geladen werden. Ab dieser Version enthält der Abschnitt zu den Standardeinstellungen stets die neueste Konfiguration. [CXM-62681]
- Administratoren können nicht mehr auf bestimmte Optionen zugreifen, indem sie beim Ausführen der Anwendung die Umschalttaste drücken. Diese Optionen waren zuvor mit Citrix-Berechtigung verfügbar. Einige Optionen (z. B. Umleitung zulassen) sind jetzt vollständig verfügbar, während andere (z. B. das Erkennen von Reaktionsproblemen und die Zählkorrektur) nicht mehr unterstützt werden. [CXM-62767]



Neue Features in Version 10.1.8

Die folgenden Probleme wurden in Version 10.1.8 behoben:

- Es kann vorkommen, dass Exchange verhindert, dass der Citrix Endpoint Management Connector für Exchange ActiveSync zu häufig Befehle ausgibt. Dies passiert häufig bei Verbindungen mit Office 365. Die Drosselung führt dazu, dass der ActiveSync-Dienst pausiert, bevor er den nächsten Befehl sendet. In der Konsole zum Konfigurieren wird nun die verbleibende Zeit dieser Pause angezeigt. [CXM-48044]
- Wenn Änderungen an den Abschnitten “Watchdog” oder “SpecialistsDefaults” der Konfigurationsdatei (config.xml) vorgenommen werden, werden diese Änderungen nach einem Upgrade nicht in der Konfigurationsdatei übernommen. Bei diesem Release werden die Änderungen einwandfrei in die neue Konfigurationsdatei übernommen. [CXM-52523]
- Den an Google Analytics gesendeten Analysedaten wurden weitere Details (insbesondere in Bezug auf Snapshots) hinzugefügt. [CXM-56691]
- Das Exchange-Feature zum Testen der Verbindung versuchte nur einmal, die Verbindung zu initialisieren. Da Office 365-Verbindungen gedrosselt werden können, konnte ein Verbindungstest durch die Drosselung fehlschlagen. Der Citrix Endpoint Management Connector für Exchange ActiveSync versucht nun bis zu dreimal, eine Verbindung herzustellen. [CXM-58180]

- Um Richtlinien auf Exchange anzuwenden, muss der Citrix Endpoint Management Connector für Exchange ActiveSync einen **Set-CASMailbox**-Befehl kompilieren, der alle relevanten Geräte für jedes Postfach in zwei Listen (Zulassen und Blockieren) enthält. Wenn ein Gerät nicht in einer der Listen enthalten ist, kehrt Exchange zum Standardzugriffsstatus zurück. Wenn der Standardzugriffsstatus von dem gewünschten Status für ein Gerät abweicht, ist das Gerät nicht mehr richtlinientreu. Folglich verliert der Benutzer den Zugriff auf seine E-Mail, wenn der Exchange-Standardzugriffsstatus "blockiert" ist und der Status ansonsten "zugelassen" wäre. Umgekehrt kann einem Benutzer, dessen Zugriff auf E-Mail blockiert werden soll, der Zugriff gewährt werden. Der Citrix Endpoint Management Connector für Exchange ActiveSync stellt nun sicher, dass alle Geräte mit einem gültigen Sollstatus in jedem **Set- CASMailbox**-Befehl berücksichtigt werden. [CXM-61251]

Das folgende Problem ist in Version 10.1.8 bekannt:

Wenn ein Administrator Konfigurationsdaten in der Anwendung zum Konfigurieren ändert, während der Dienst eine lang andauernde Operation durchführt (z. B. Snapshot oder Richtlinienbewertung) kann der Dienst einen unbestimmten Zustand annehmen. Als mögliches Symptom werden Richtlinienänderungen evtl. nicht verarbeitet oder Snapshots nicht initiiert. Um den Dienst in einen funktionierenden Zustand zurückzuversetzen, muss er neu gestartet werden. Möglicherweise müssen Sie den Dienstprozess über den Windows-Dienstmanager beenden, bevor Sie den Dienst neu starten. [CXM-61330]

Neue Features in Version 10.1.7

- XenMobile Mail Manager heißt jetzt Endpoint Management Connector für Exchange ActiveSync.
- Die Option **Disable Pipelining** im Dialogfeld zur Exchange-Konfiguration ist jetzt veraltet. Sie können die gleiche Wirkung durch Konfiguration mehrerer Schritte für jeden Befehl in der Datei config.xml erzielen. [CXM-54593]

Die folgenden Probleme wurden in Version 10.1.7 behoben:

- Im Snapshotverlauf werden u. U. Fehlermeldungen mit wenig Kontext angezeigt. Jetzt ist Fehlermeldungen der Kontext ihres Auftretens vorangestellt. [CXM-49157]
- Für die XmmGoogleAnalytics-DLL gab es keine Dateiversion für das Release. [CXM-52518]
- Um die Diagnose zu verbessern, hat Citrix vor kurzem das Zeichenfolgenformat für eine Liste von Geräte-IDs geändert, die zum Festlegen eines Postfachs auf "Erlaubt/Gesperrt" verwendet werden. Bei Angabe von zu vielen Geräten wurde jedoch die maximale Zeichenfolgenlänge überschritten. Es wird jetzt eine interne Array-Datenstruktur verwendet. Diese Struktur hat keine Größenbeschränkung und formatiert außerdem die Daten für die Diagnose. [CXM-52610]
- Werden nicht mit Exchange synchronisierte Geräterichtlinien erkannt, können deren Befehle Geräte umfassen, die nicht zum entsprechenden Postfach gehören. Der Endpoint Management Connector für Exchange ActiveSync stellt jetzt sicher, dass Befehle an Exchange nur Geräte

darstellen, die zu den jeweiligen Postfächern gehören. [CXM-54842]
- In manchen Umgebungen ist eine Microsoft-Assembly nicht verfügbar. Die erforderliche Assembly wird jetzt zusammen mit der Anwendung installiert. [CXM-55439]
- Enthält der Distinguished Name eines Geräts oder Postfachs Leerzeichen zwischen dem Attributnamen und dem Gleichheitszeichen und/oder nach dem Gleichheitszeichen und vor dem Wert, ordnet der Endpoint Management Connector für Exchange ActiveSync das Gerät möglicherweise nicht seinem Postfach zu oder umgekehrt. Das kann dazu führen, dass Geräte und/oder Postfächer beim Snapshot-Abgleich abgelehnt werden. [CXM-56088]

> **Hinweis:**
>
> In den folgenden Abschnitten wird für den Endpoint Management Connector für Exchange ActiveSync (zuvor "XenMobile Mail Manager") der bisherige Name "XenMobile Mail Manager" verwendet. Der neue Name gilt ab Version 10.1.7.

Update in Version 10.1.6.20

Ein Update für Version 10.1.6 enthält folgenden Fix in Version 10.1.6.20:

- Werden nicht mit Exchange synchronisierte Geräterichtlinien erkannt, können deren Befehle Geräte umfassen, die nicht zum entsprechenden Postfach gehören. XenMobile Mail Manager stellt jetzt sicher, dass Befehle an Exchange nur Geräte darstellen, die zu den jeweiligen Postfächern gehören. [CXM-54842]

Neue Features in Version 10.1.6

Version 10.1.6 von XenMobile Mail Manager umfasst folgende Problemlösungen und Verbesserungen:

- Das Snapshot-Verlaufsfenster wird u. U. nicht mehr aktualisiert. Der Mechanismus zur Fensteraktualisierung wurde verbessert. [CXM-47983]
- Für partitionierte und nicht partitionierte Snapshots wurden zwei separate Modi und Codepfade verwendet. Da nicht partitionierte Snapshots partitionierten Snapshots entsprechen (mit einer Konfiguration mit einer einzelnen "*"-Partition) wurde der Modus mit nicht partitionierten Snapshots entfernt. Standardmodus sind jetzt Snapshots mit 36 Partitionen (0–9, A–). [CXM-49093]
- Im Fenster "Snapshot History" wurden Fehlermeldungen durch Statusmeldungen überschrieben. XenMobile Mail Manager bietet jetzt zwei Felder, damit Benutzer Status- und Fehlermeldungen gleichzeitig anzeigen können. [CXM-51942]
- Bei Verbindung mit Exchange Online (Office 365) erzeugten Snapshot-bezogene Abfragen evtl. ein unvollständiges Dataset. Dieses Problem konnte auftreten, wenn XenMobile Mail Manager ein Pipelineskript mit mehreren Befehlen ausführt. Der Upstreambefehl kann die Daten nicht schnell genug an den Downstreambefehl übergeben, der die Arbeit vorzeitig einstellt und un-

vollständige Daten liefert. XenMobile Mail Manager kann jetzt die Pipeline selbst nachahmen und die komplette Ausführung des Upstreambefehls abwarten, bevor der Downstreambefehl aufgerufen wird. Dadurch müssten alle Daten verarbeitet und erfasst werden. [CXM-52280]

- Trat ein nicht auflösbarer Fehler in einem Richtlinienaktualisierungsbefehl für Exchange auf, wurde der Befehl lange Zeit wiederholt an die Arbeitswarteschlange zurückgegeben. Dadurch wurde der Befehl viele Male an Exchange gesendet. In dieser Version von XenMobile Mail Manager wird ein Befehl, der zu einem Fehler führt, nur eine spezifische Anzahl von Malen an die Arbeitswarteschlange zurückgegeben. [CXM-52633]
- Wenn eine Richtlinienaktualisierung für ein bestimmtes Postfach das Zulassen oder Sperren aller Geräte beinhaltete, schlug der ausgegebene Befehl **Set-CASMailbox** fehl, weil die leere Liste in eine leere Zeichenfolge statt **NULL** konvertiert wurde. Jetzt werden die richtigen Daten gesendet. [CXM-53759]
- Bei der Verarbeitung eines neuen Geräts gab Exchange u. U. den Status eine Zeit lang (normalerweise 15 Minuten) mit “DeviceDiscovery” zurück. Der Status wurde von XenMobile Mail Manager nicht speziell behandelt. XenMobile Mail Manager behandelt jetzt den Status. Die Benutzer können jetzt die Geräte auf der Registerkarte “Überwachen” nach diesem Status filtern. [CXM-53840]
- XenMobile Mail Manager prüfte nicht, ob das Schreiben in die XenMobile Mail Manager-Datenbank möglich war. Bei begrenzten Berechtigungen war das Verhalten daher nicht vorhersagbar. XenMobile Mail Manager erfasst und validiert jetzt erforderliche Berechtigungen von der Datenbank. XenMobile Mail Manager weist jetzt bei Verbindungstests und beim Zeigen auf die Datenbankanzeige unten im Hauptfenster zum Konfigurieren durch eine Meldung auf begrenzte Berechtigungen hin. [CXM-54219]
- Workloadabhängig wird der XenMobile Mail Manager-Dienst u. U. nicht sofort gestoppt. Der Dienst scheint dann nicht mehr zu reagieren. Durch Verbesserungen können laufende Tasks jetzt unterbrochen werden, was ein ordnungsgemäßeres Beenden ermöglicht. [CXM-54282]

Neue Features in Version 10.1.5

Bei Version 10.1.5 von XenMobile Mail Manager wurden folgende Probleme behoben:

- Auf eine Drosselung der XenMobile Mail Manager-Aktivität durch Exchange wurde ausschließlich in den Protokollen hingewiesen. Bei der neuen Version wird beim Zeigen auf den aktiven Snapshot mit der Maus der Zustand “throttling” angezeigt. Während einer Drosselung von XenMobile Mail Manager kann außerdem kein größerer Snapshot gestartet werden, bis Exchange die Drosselung aufhebt. [CXM-49617]
- Wurde XenMobile Mail Manager während der Erstellung eines größeren Snapshots von Exchange gedrosselt wurde u. U. nicht genügend Zeit bis zum nächsten Snapshotversuch gewartet. Dies führte zu einer weiteren Drosselung und dem Fehlschlagen des Snapshots. XenMobile Mail Manager hält jetzt die von Exchange festgelegte Wartezeit zwischen Snap-

shotversuchen ein. [CXM-49618]

- Wenn die Diagnose aktiviert ist, enthielt die Befehlsdatei **Set-CasMailbox** Befehle, bei denen die Bindestriche vor den Eigenschaftsnamen fehlten. Dieses Problem trat nur in der Diagnosedatei, nicht aber in den an Exchange übergebenen Befehlen auf. Aufgrund des fehlenden Bindestrichs konnten Befehle nicht per Cut & Paste direkt in eine Powershell-Eingabeaufforderung zum Testen eingefügt werden. Die Bindestriche wurden jetzt hinzugefügt. [CXM-52520]
- Bei Postfachidentitäten des Formats "Nachname, Vorname" fügte Exchange vor dem Komma einen umgekehrten Schrägstrich ein, wenn Daten aus einer Abfrage zurückgegeben werden. Der Schrägstrich muss entfernt werden, wenn XenMobile Mail Manager unter Verwendung der Identität weitere Daten abfragt. [CXM-52635]

Bekannte Einschränkung

> **Hinweis:**
>
> Die folgende Einschränkung wurde mit Version 10.1.6 behoben.

Bei XenMobile Mail Manager ist eine Einschränkung bekannt, die dazu führen kann, dass Exchange-Befehle fehlschlagen. Zum Anwenden von Richtlinienänderungen auf Exchange wird der Befehl **Set_CASMailbox** von XenMobile Mail Manager ausgegeben. Dieser Befehl kann die Geräteliste zum Zulassen und die Geräteliste zum Blockieren umfassen. Der Befehl wird auf mit einem Postfach verknüpfte Geräte angewendet.

Die Listen sind durch die Microsoft-API auf jeweils 256 Zeichen beschränkt. Ist eine Liste länger, schlägt der Befehl vollständig fehl und keine der Richtlinien für die Geräte des Postfachs kann festgelegt werden. Der in den XenMobile Mail Manager-Protokollen gemeldete Fehler sieht in etwa wie folgt aus. Das Beispiel gilt für die gesperrte Liste.

"Message:'Cannot bind parameter 'ActiveSyncBlockedDeviceIDs' to the target. Exception setting "ActiveSyncBlockedDeviceIDs": "The length of the property is too long. The maximum length is 256 and the length of the value provided is …"

Die Länge von Geräte-IDs kann variieren, doch nach einer guten Grundregel überschreiten 10 oder mehr Geräte in einer Liste den Grenzwert. Es sind zwar nur selten so viele Geräte mit einem Postfach verknüpft, doch kann dies durchaus vorkommen. Bis XenMobile Mail Manager für die Verarbeitung eines solchen Szenarios verbessert ist, empfiehlt es sich, maximal 10 Geräte mit einem Benutzer und Postfach zu verknüpfen. [CXM-52633]

Neue Features in Version 10.1.4

Bei Version 10.1.4 von XenMobile Mail Manager wurden folgende Probleme behoben:

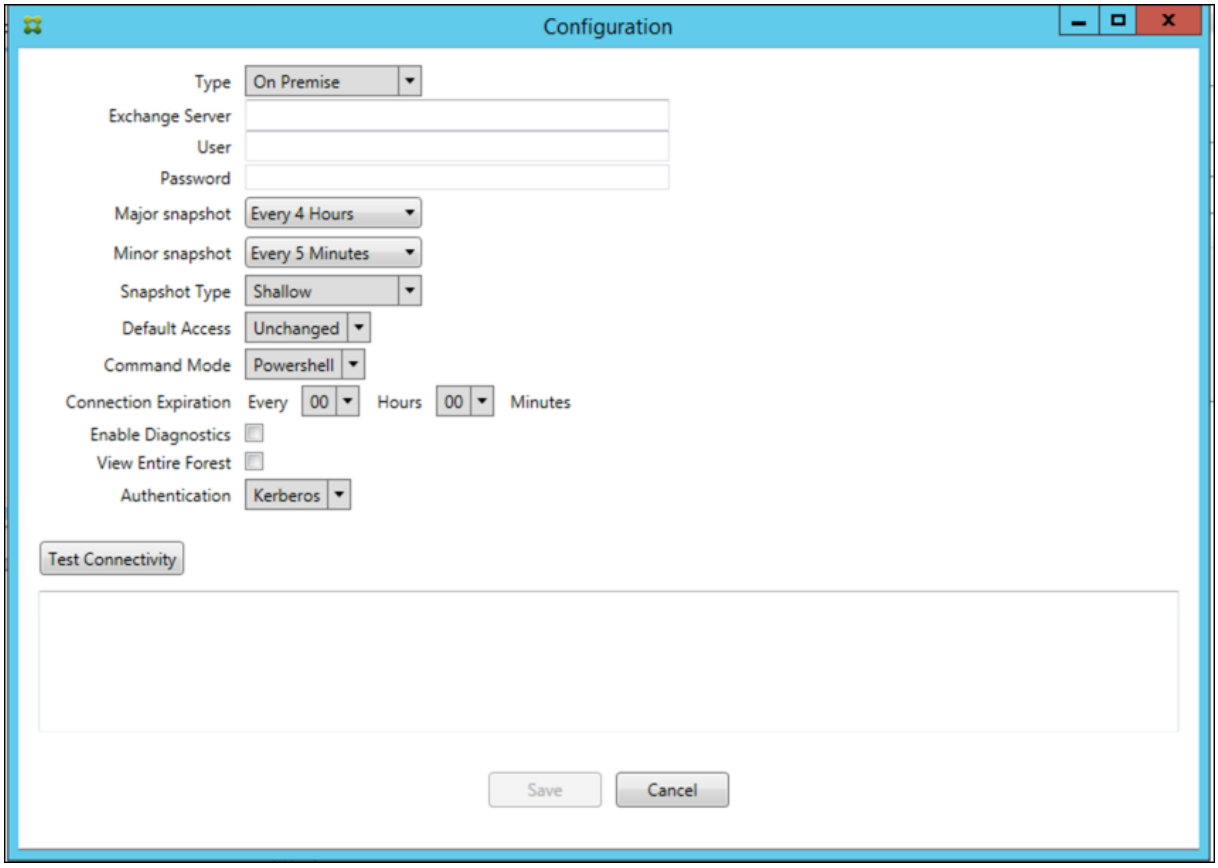
- Aufgrund der schwächer werdenden Sicherheit wird TLS 1.0 vom Payment Card Industry Security Standards Council abgelehnt. XenMobile Mail Manager unterstützt jetzt TLS 1.1 und 1.2.

[CXM-38573, CXM-32560]

- XenMobile Mail Manager umfasst eine neue Diagnosedatei. Wenn in der Exchange-Spezifikation **Diagnose aktivieren** ausgewählt wird, wird eine neue Snapshotverlaufsdatei generiert. Bei jedem Snapshotversuch wird der Datei eine Zeile mit dem Snapshotergebnis hinzugefügt. [CXM-49631]
- In der Commands-Diagnosedatei wurde die Liste der zulässigen und gesperrten Geräte für den Befehl **Set-CASMailbox** nicht angezeigt. Stattdessen wurde in der Datei der interne Klassenname für die zugehörigen Argumente angezeigt. XenMobile Mail Manager zeigt nun die Liste der Geräte-IDs in Form einer durch Kommas getrennten Liste. [CXM-50693]
- Beim Fehlschlagen einer Verbindung mit Exchange aufgrund einer fehlerhaften Spezifikation wurde fälschlicherweise gemeldet, dass alle Verbindungen in Verwendung seien. Es werden jetzt detailliertere Meldungen angezeigt, z. B. “All connections are inoperable”, “Connection pool is empty”, “All connections are throttled” und “No available connections”. [CXM-50783]
- Die Befehle Zulassen/Blockieren/Löschen wurden in Einzelfällen mehrfach im internen XenMobile Mail Manager-Cache hinzugefügt. Das Problem führt zu einer Verzögerung beim Senden des Befehls an Exchange. In XenMobile Mail Manager wird jetzt jeder Befehl nur einmal hinzugefügt. [CXM-51524]

Neue Features in Version 10.1.3

- **Unterstützung von Google Analytics:** Wir möchten wissen, wie Sie XenMobile Mail Manager verwenden, damit wir wissen, wo wir das Produkt verbessern können.
- **Einstellung zum Aktivieren der Diagnose:** Das Kontrollkästchen **Enable Diagnostic** wird im Dialogfeld **Configuration** der Konsole angezeigt.



Behobene Probleme in Version 10.1.3

- Im Fenster **Snapshot History** geben Zustands-QuickInfos nicht den tatsächlichen Zustand von Snapshots an. [CXM-5570]
  XenMobile Mail Manager kann zeitweise nicht in die Commands-Diagnosedatei schreiben. In diesem Fall wird der Befehlsverlauf nicht vollständig protokolliert. [CXM-49217]
- Wenn bei einer Verbindung ein Fehler auftritt, wird die Verbindung möglicherweise nicht als fehlerhaft markiert. Die Verbindung wird dann bei einem nachfolgenden Befehl ggf. verwendet, wodurch ein weiterer Fehler auftritt. [CXM-49495]
- Eine von Exchange Server kommende Drosselung kann eine Ausnahme in der Check Health-Routine auslösen. Verbindungen, bei denen ein Fehler aufgetreten ist oder die abgelaufen sind, werden dann evtl. nicht bereinigt. Außerdem stellt XenMobile Mail Manager möglicherweise keine Verbindungen her, bis die Drosselung endet. [CXM-49794].
- Bei Überschreiten der maximalen Sitzungsanzahl für Exchange meldet XenMobile Mail Manager fälschlicherweise den Fehler “Device Capture Failed”. Stattdessen müsste gemeldet werden, dass die beiden von XenMobile Mail Manager normalerweise für die Exchange-Kommunikation verwendeten Sitzungen in Verwendung sind. [CXM-49994]

Neue Features in Version 10.1.2

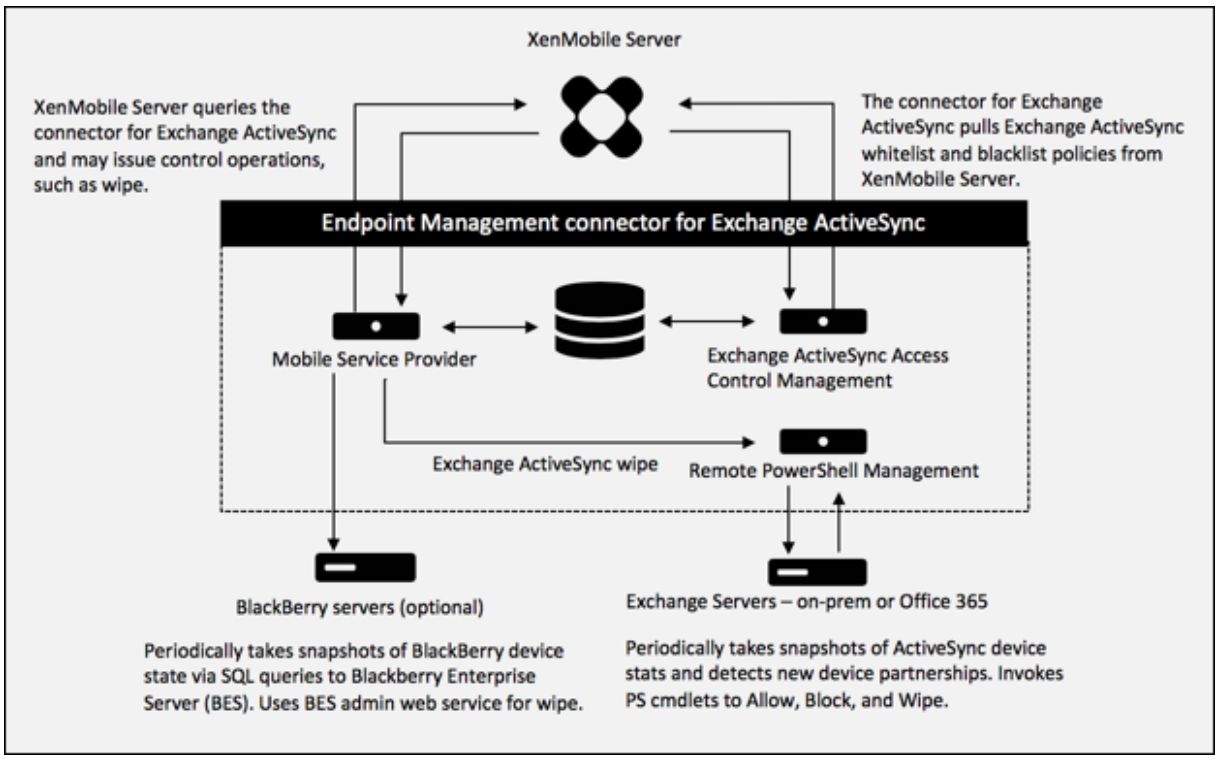
- **Verbesserte Verbindung mit Exchange:** XenMobile Mail Manager verwendet PowerShell-Sitzungen für die Kommunikation mit Exchange. Eine PowerShell-Sitzung kann – insbesondere bei Office 365 – nach einiger Zeit instabil werden, sodass Befehle nicht mehr ausgeführt werden. In XenMobile Mail Manager können jetzt Ablaufzeiträume für Verbindungen festgelegt werden. Wenn eine Verbindung abläuft, fährt XenMobile Mail Manager die PowerShell-Sitzung ordnungsgemäß herunter und erstellt eine neue. Dadurch sinkt die Wahrscheinlichkeit, dass PowerShell-Sitzungen instabil werden und Snapshotfehler auftreten.
- **Verbesserter Snapshot-Workflow:** Große Snapshots sind zeitaufwendig und prozessintensiv. Tritt während eines Snapshots ein Fehler auf, versucht XenMobile Mail Manager jetzt bis zu drei Mal, den Snapshot fertigzustellen. Die Wiederholungsversuche beginnen nicht beim Startpunkt. XenMobile Mail Manager fährt dort fort, wo der Vorgang unterbrochen wurde. Dies verbessert die allgemeine Snapshoterfolgsrate, da zeitweise Fehler während der Snapshoterstellung toleriert werden.
- **Verbesserte Diagnose**: Die Problembehandlung bei Snapshotvorgängen wird erleichtert durch drei neue Diagnosedateien, die optional während eines Snapshots generiert werden können. Mithilfe der Dateien lassen sich Probleme mit PowerShell-Befehlen, Postfächer, bei denen Informationen fehlen, und nicht mit einem Postfach verknüpfbare Geräte identifizieren. Anhand der Dateien können Administratoren fehlerhafte Daten in Exchange identifizieren.
- **Verbesserte Speichernutzung:** Die Speichernutzung durch XenMobile Mail Manager ist nun effizienter. Administratoren können festlegen, dass XenMobile Mail Manager automatisch neu und in einem sauberen Zustand gestartet wird.
- **Voraussetzung – Microsoft .NET Framework 4.6:** Microsoft .NET Framework ist jetzt in Version 4.6 erforderlich.

Behobene Probleme

- Fehler bei Aufforderung zur Eingabe von Anmeldeinformationen: Eine instabile Office 365-Sitzung führte häufig zu diesem Fehler. Das Problem wurde durch die verbesserte Verbindung mit Exchange behoben. (XMHELP-293, XMHELP-311, XMHELP-801)
- Ungenaue Postfach- und Gerätezahl: XenMobile Mail Manager besitzt einen verbesserten Algorithmus für die Zuordnung von Postfächern zu Geräten. Die verbesserte Diagnose hilft bei der Identifizierung von Postfächern und Geräten, für die XenMobile Mail Manager nicht zuständig ist. (XMHELP-623)
- Befehle zum Zulassen/Blockieren/Löschen nicht erkannt: Ein Fehler wurde behoben, durch den XenMobile Mail Manager-Befehle zum Zulassen/Blockieren/Löschen manchmal nicht erkannt wurden. (XMHELP-489)
- Speicherverwaltung: bessere Verwaltung und besserer Ausgleich für Speicher. (XMHELP-419)

Architektur

Die folgende Abbildung zeigt die Hauptkomponenten des Endpoint Management-Connectors für Exchange ActiveSync. Ein detailliertes Architekturdiagramm finden Sie unter Architektur.



Die drei Hauptkomponenten sind Folgende:

- **Exchange ActiveSync Access Control Management:** ruft eine Exchange ActiveSync-Richtlinie bei XenMobile ab und führt diese mit lokal definierten Richtlinien zusammen, um zu bestimmen, welche Exchange ActiveSync-Geräte Zugriff auf Exchange erhalten sollen. Lokale Richtlinien ermöglichen die Erweiterung der Richtlinienregeln für die Zugriffssteuerung auf der Basis von Active Directory-Gruppe, Benutzer, Gerätetyp oder Gerätebenutzer-Agent (im Allgemeinen die Version der mobilen Plattform).
- **Remote PowerShell Management:** verantwortlich für das Planen und Aufrufen von Remote-PowerShell-Befehlen für die Anwendung der über Exchange ActiveSync Access Control Management kompilierten Richtlinie. Erstellt in regelmäßigen Abständen einen Snapshot der Exchange ActiveSync-Datenbank zur Erkennung neuer oder geänderter Exchange ActiveSync-Geräte.
- **Mobile Service Provider:** bietet eine Webdienstschnittstelle, sodass XenMobile Exchange ActiveSync- und BlackBerry-Geräte abfragen und Vorgänge zu deren Steuerung, etwa die Löschung von Daten, ausgeben kann.

Systemanforderungen und Voraussetzungen

Für den Endpoint Management Connector für Exchange ActiveSync gelten die folgenden Mindestsystemanforderungen:

- Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2008 R2 Service Pack 1. Muss ein englischbasierter Server sein. Die Unterstützung für Windows Server 2008 R2 Service Pack 1 endet am 14. Januar 2020.
- Microsoft SQL Server 2016 Service Pack 2 oder SQL Server 2014 Service Pack 3.
- Microsoft .NET Framework 4.6.
- Blackberry Enterprise Service, Version 5 (optional).

Unterstützte Mindestversionen von Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 Service Pack 3 (Support endet am 14. Januar 2020)

Voraussetzungen

- 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 dem Endpoint Management Connector für Exchange ActiveSync und dem Remote-Computer mit Exchange Server geöffnet sein.
- **E-Mail-Clients auf Geräten:** Nicht alle E-Mail-Clients geben konstant dieselbe ActiveSync-ID für das Gerät zurück. Da der Endpoint Management Connector für Exchange ActiveSync 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 ordnungsgemäß:
  - Samsung-nativer E-Mail-Client
  - iOS-nativer E-Mail-Client
- **Exchange**: Anforderungen für lokale Computer mit Exchange:

  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 der Endpoint Management Connector für Exchange ActiveSync 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.
- Die Anmeldeinformationen zum Herstellen einer Remoteverbindung und Ausführen von Remotebefehlen müssen einem Benutzer entsprechen, der auf dem Remotecomputer Administratorrechte hat. Sie können diese Anforderung mit dem Befehl "Set-PSSessionConfiguration" umgehen. Eine Erläuterung dieses Befehls geht jedoch über den Rahmen des vorliegenden Dokuments hinaus. Weitere Informationen finden Sie im Microsoft-Artikel Informationen zu Sitzungskonfigurationen.
- 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 Drosselungsrichtlinien. 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 der Endpoint Management Connector für Exchange ActiveSync 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 Drosselungsrichtlinien 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.
- **Drosselungsrichtlinien:** Exchange hat zahlreiche Drosselungsrichtlinien. 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 der Endpoint Management Connector für Exchange ActiveSync 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 Drosselungsrichtlinien für die Remoteverwaltung per PowerShell.

Installation und Konfiguration

1. Klicken Sie auf die Datei XmmSetup.msi und folgen Sie den Anweisungen des Installers zum Installieren des Endpoint Management-Connectors für Exchange ActiveSync.
2. Lassen Sie auf dem letzten Bildschirm des Setupassistenten die Option **Launch the Configure utility** ausgewählt. Oder öffnen Sie den Endpoint Management Connector für Exchange ActiveSync über das Menü **Start**.
3. Konfigurieren Sie die folgenden Datenbankeigenschaften:

- Wählen Sie die Registerkarte **Configure > Database** aus.
- Geben Sie den Namen des SQL-Servers ein (standardmäßig “localhost”).
- Behalten Sie den Standarddatenbanknamen **CitrixXmm** bei.

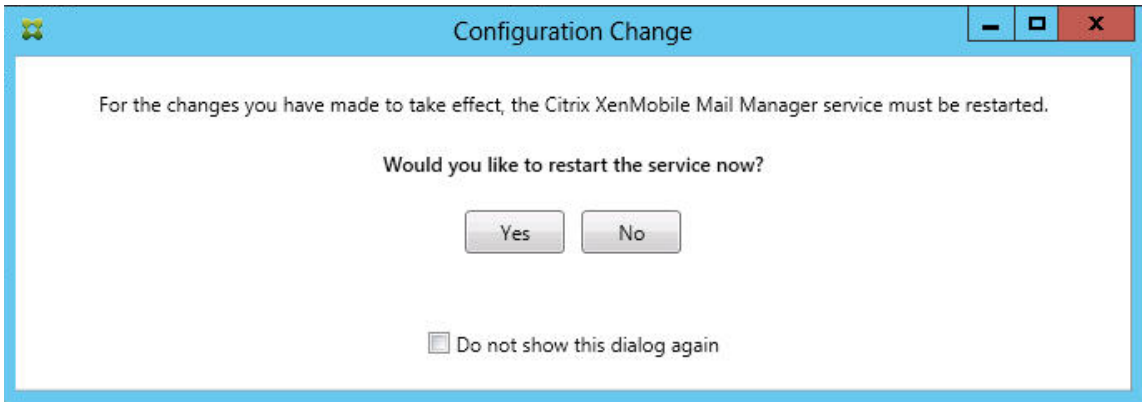
4. Wählen Sie einen der folgenden für SQL verwendeten Authentifizierungsmodi aus:

   - **SQL:** Geben Sie den Benutzernamen und das Kennwort eines gültigen SQL-Benutzers ein.
   - **Windows Integrated:** Wenn Sie diese Option auswählen, müssen die Anmeldeinformationen des Diensts des Endpoint Management-Connectors für Exchange ActiveSync in ein Windows-Konto geändert werden, das Zugriff auf den SQL-Server hat. Öffnen Sie hierfür **Systemsteuerung > Verwaltung > Dienste**. Klicken Sie mit der rechten Maustaste auf den Endpoint Management Connector für Exchange ActiveSync-Diensteintrag und klicken Sie dann auf die Registerkarte **Anmelden**.

   Wenn “Windows Integrated” auch für die BlackBerry-Datenbankverbindung ausgewählt wird, muss dem hier angegebenen Windows-Konto Zugriff auf die BlackBerry-Datenbank erteilt werden.

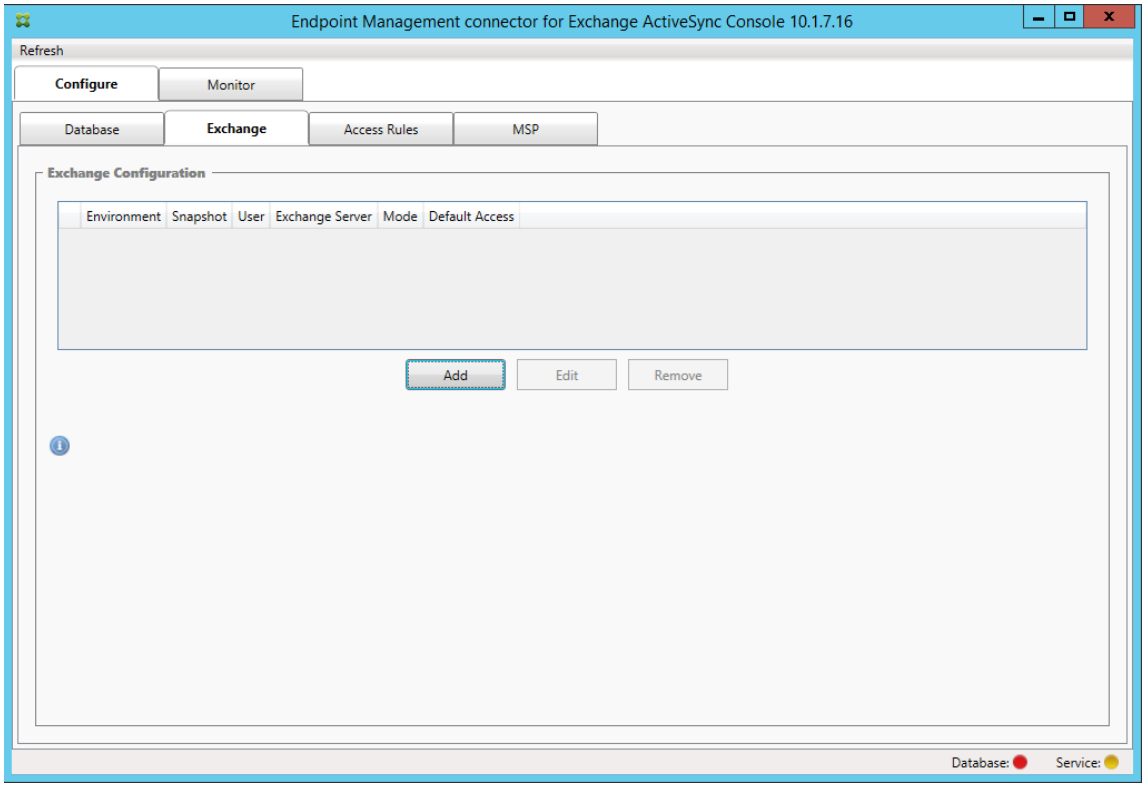
5. Klicken Sie auf **Test Connectivity**, um sicherzustellen, dass eine Verbindung zum SQL-Server hergestellt werden kann, und klicken Sie auf **Save**.

6. Eine Meldung fordert Sie zum Neustarten des Diensts auf. Klicken Sie auf **Ja**.



7. Konfigurieren Sie einen oder mehrere Exchange-Server:

   - Wenn Sie nur eine Exchange-Umgebung verwalten, konfigurieren Sie nur einen Server. Wenn Sie mehrere Exchange-Umgebungen verwalten, müssen Sie für jede einen eigenen Exchange Server-Computer festlegen.
   - Klicken Sie auf **Configure > Exchange** und dann auf **Add**.

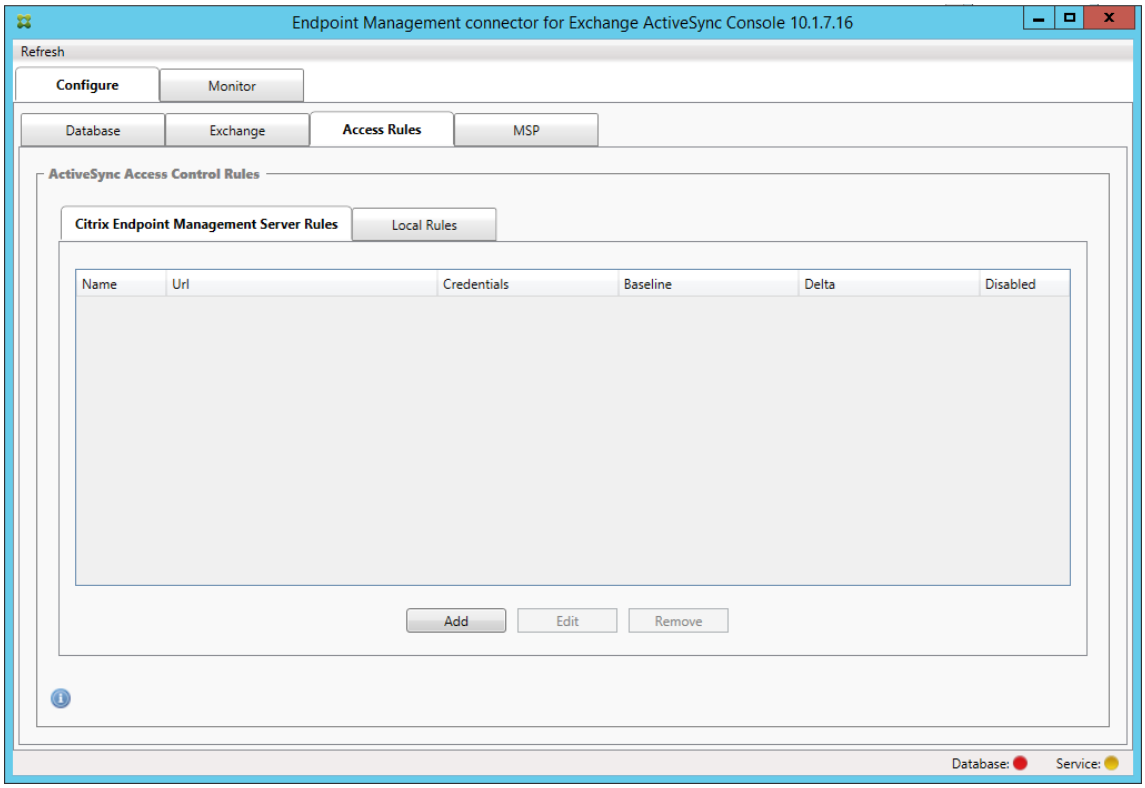


8. Wählen Sie den Typ der Exchange Server-Umgebung aus: **On Premise** oder **Office 365**.

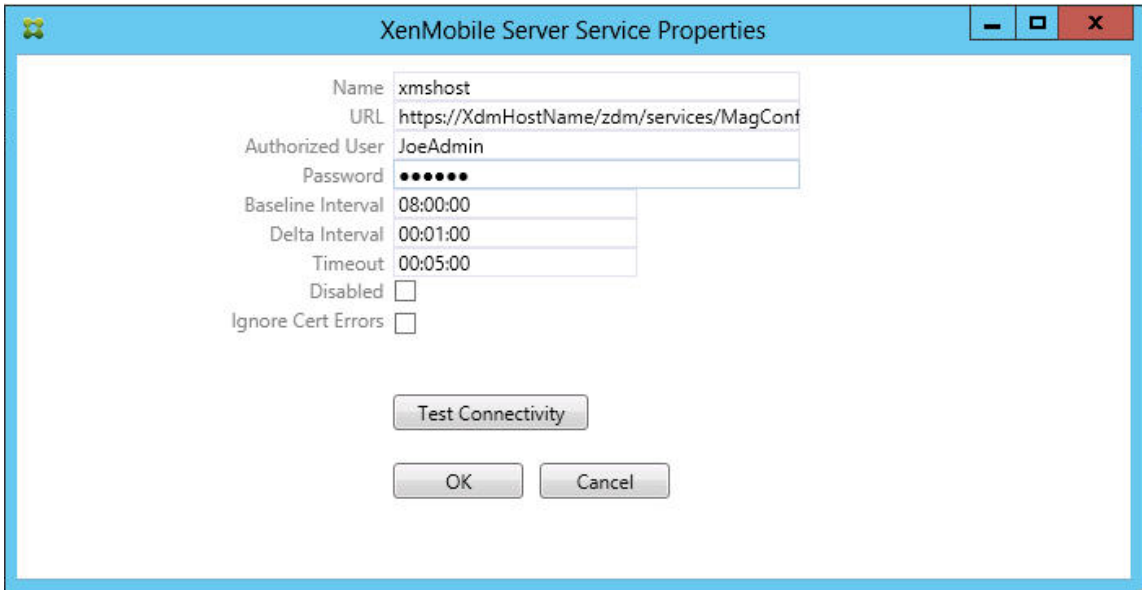
   - Wenn Sie **On Premise** auswählen, geben Sie den Namen des für Remote PowerShell-Befehle verwendeten Exchange Servers ein.
   - Geben Sie den **Benutzernamen** einer Windows-Identität ein, die die unter “Anforderungen” aufgeführten Berechtigungen auf dem Exchange Server-Computer hat, und geben Sie das zugehörige **Kennwort** ein.
   - Wählen Sie den Zeitplan zum Ausführen größerer Snapshots. Bei einem größeren Snapshot wird jede Exchange ActiveSync-Partnerschaft ermittelt.
   - Wählen Sie den Zeitplan zum Ausführen kleinerer Snapshots. Bei einem kleineren Snapshot werden neu erstellte Exchange ActiveSync-Partnerschaften ermittelt.
   - Wählen Sie den Snapshottyp: **Deep** oder **Shallow**. Flache Snapshots (Shallow) werden in der Regel viel schneller erstellt und reichen zur Ausführung aller Funktionen der Exchange ActiveSync-Zugriffssteuerung über den Endpoint Management Connector für Exchange ActiveSync aus. Tiefe Snapshots (Deep) brauchen länger und sind nur erforderlich, wenn Mobile Service Provider für ActiveSync aktiviert ist. Mit dieser Option kann XenMobile nicht verwaltete Geräte abfragen.
   - Wählen Sie den Standardzugriff aus: **Allow**, **Block** oder **Unchanged**. Durch die Einstellung wird gesteuert, wie Geräte behandelt werden, die keine der Kriterien von XenMobile-Regeln oder lokalen Regeln erfüllen. Wenn Sie **Allow** auswählen, ist der ActiveSync-Zugriff auf all diese Geräte zulässig. Wenn Sie **Block** auswählen, wird der Zugriff verweigert. Wenn Sie **Unchanged** auswählen, wird keine Änderung vorgenommen.

- Wählen Sie für “ActiveSync Command Mode” eine Option aus: **PowerShell** oder **Simulation**.
- Im **PowerShell**-Modus gibt der Endpoint Management Connector für Exchange ActiveSync die PowerShell-Befehle für die gewünschte Zugriffssteuerung aus. Im Simulationsmodus werden vom Endpoint Management Connector für Exchange ActiveSync 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.
- Legen Sie unter **Connection Expiration** die Lebensdauer für Verbindungen fest. Wenn eine Verbindung das vorgegebene Alter erreicht, wird sie als abgelaufen markiert und nicht wieder verwendet. Eine solchermaßen nicht mehr verwendete Verbindung wird vom Endpoint Management Connector für Exchange ActiveSync ordnungsgemäß getrennt. Wenn eine Verbindung wieder benötigt wird, wird eine neue Verbindung initialisiert, wenn keine verfügbar ist. Erfolgt keine Angabe, wird der Standardwert von 30 Minuten verwendet.
- Wählen Sie **View Entire Forest**, damit der Endpoint Management Connector für Exchange ActiveSync die gesamte Active Directory-Struktur in der Exchange-Umgebung anzeigt.
- Wählen Sie das Authentifizierungsprotokoll aus: **Kerberos** oder **Basic**. Der Endpoint Management Connector für Exchange ActiveSync unterstützt die Standardauthentifizierung für On-Premises-Bereitstellungen. Dadurch kann der Endpoint Management Connector für Exchange ActiveSync auch dann verwendet werden, wenn sein Server kein Mitglied der Domäne des Exchange-Servers ist.
- Klicken Sie auf **Test Connectivity**, um sicherzustellen, dass eine Verbindung zum Exchange-Server hergestellt werden kann, und klicken Sie auf **Save**.
- Eine Meldung fordert Sie zum Neustarten des Diensts auf. Klicken Sie auf **Ja**.

9. Konfigurieren Sie die Zugriffsregeln: Klicken Sie auf die Registerkarte **Configure > Access Rules**, klicken Sie auf die Registerkarte **XMS Rules** und dann auf **Add**.



10. Ändern Sie auf der Seite **XenMobile server Service Properties** die URL-Zeichenfolge so, dass sie auf XenMobile Server verweist. Wenn der Instanzname beispielsweise **zdm** lautet, geben Sie `https://<XdmHostName>/zdm/services/MagConfigService` ein. Ersetzen Sie **XdmHostName** in dem Beispiel durch die IP- oder DNS-Adresse des XenMobile-Servers.

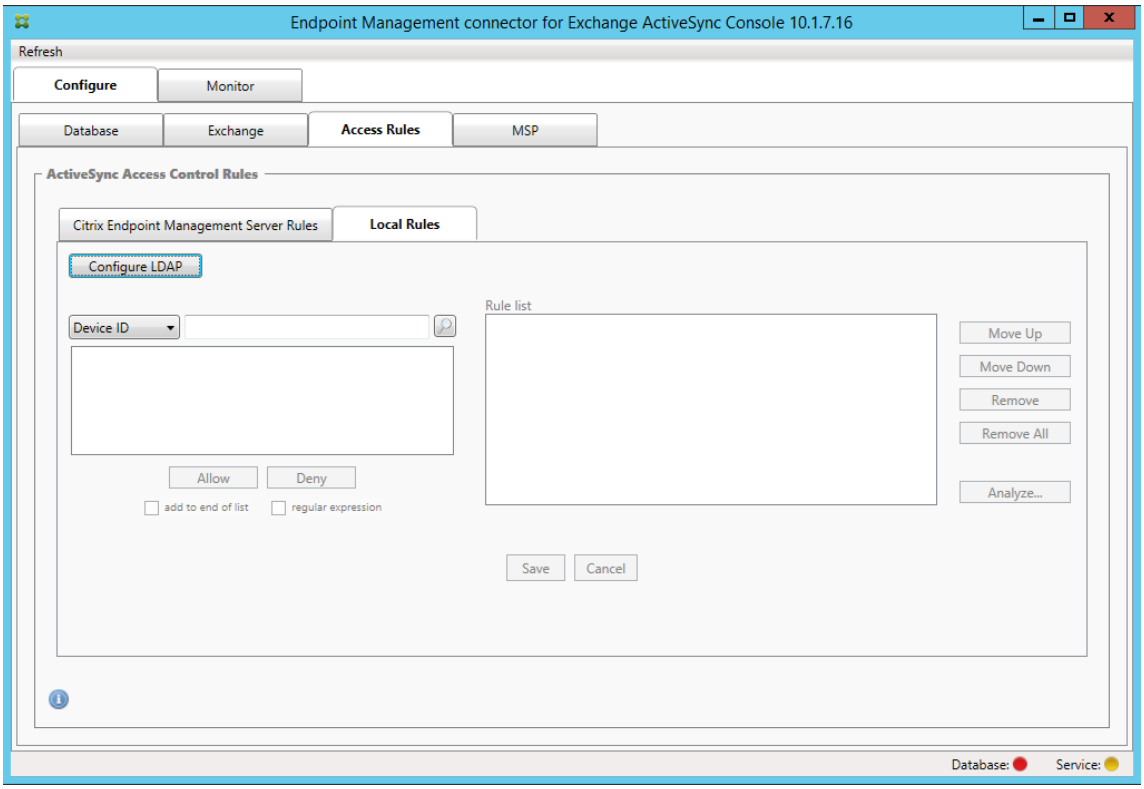


- Geben Sie einen berechtigten Serverbenutzer an.
- Geben Sie das Kennwort des Benutzers ein.
- Behalten Sie die Standardwerte für **Baseline Interval**, **Delta Interval** und **Timeout** bei.

- Klicken Sie auf **Test Connectivity**, um die Verbindung zu dem Server zu testen, und klicken Sie auf **OK**.

Wenn das Kontrollkästchen **Disabled** aktiviert ist, ruft der XenMobile Mail-Dienst keine Richtlinien von XenMobile ab.

11. Klicken Sie auf die Registerkarte **Local Rules**.



- 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.
- Geben Sie Text oder Textteile in das Textfeld ein. Klicken Sie optional auf die Schaltfläche “Query”, um die Entsprechungen für die Textteile anzuzeigen.

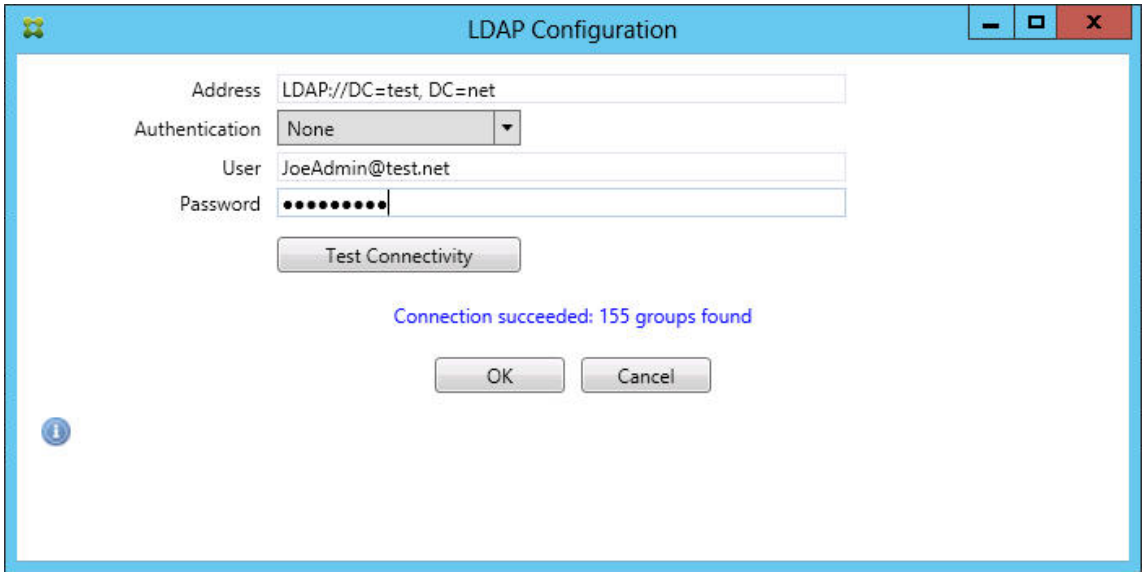
Bei allen Typen mit Ausnahme von Group verwendet das System die in einem Snapshot gefundenen Geräte. Wenn Sie gerade erst anfangen und noch keinen Snapshot erstellt haben, ist daher noch nichts verfügbar.

- Wählen Sie einen Textwert aus und klicken Sie auf **Allow** oder **Deny**, um ihn rechts zum Bereich **Rule List** hinzuzufügen. Sie können die Reihenfolge der Regeln ändern oder sie mithilfe der Schaltflächen rechts neben dem Bereich **Rule List** 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.

- Zum Durchführen einer Analyse der Regeln in der Liste auf mögliche Außerkraftsetzungen, Konflikte oder zusätzliche Konstrukte klicken Sie zunächst auf **Analyze** und dann auf **Save**.

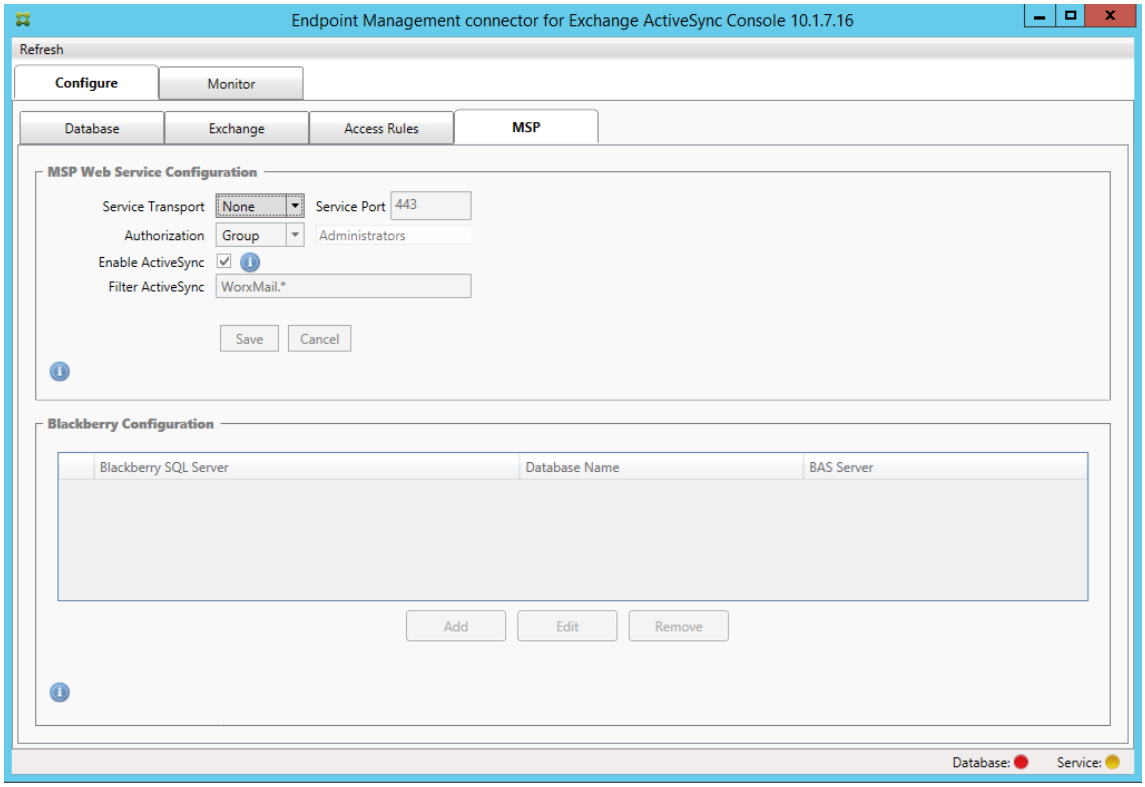
12. Wenn Sie lokale Regeln für Active Directory-Gruppen erstellen möchten, klicken Sie auf **Configure LDAP** und konfigurieren Sie die LDAP-Verbindungseigenschaften.



13. Konfigurieren des Mobile Service Provider-Diensts

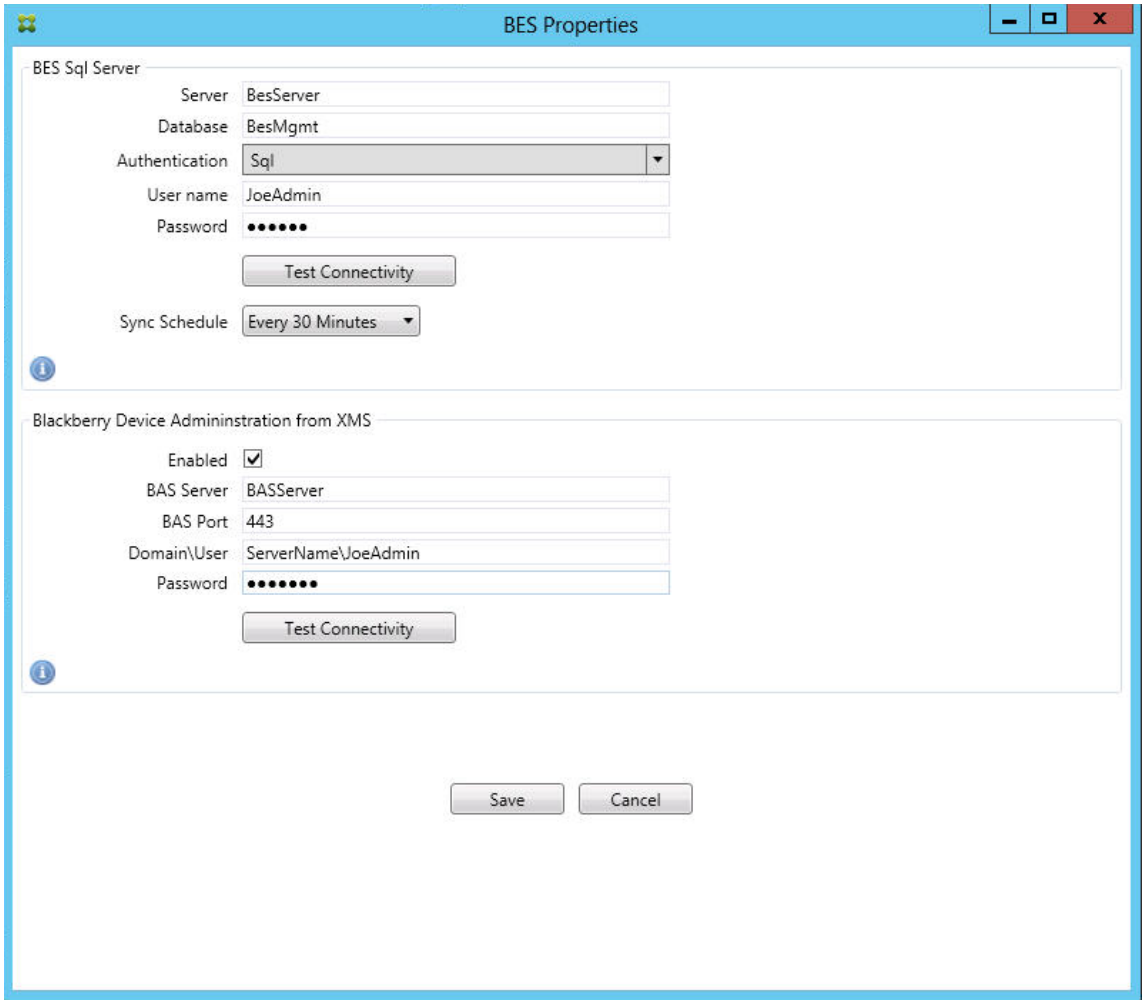
Mobile Service Provider ist optional. Der Dienst ist nur erforderlich, wenn auch XenMobile für die Verwendung der Mobile Service Provider-Schnittstelle zum Abfragen nicht verwalteter Geräte konfiguriert ist.

- Wählen Sie die Registerkarte **Configure > MSP**.



- Legen Sie den Diensttransporttyp für Mobile Service Provider auf **HTTP** oder **HTTPS** fest.
- Legen Sie unter **Service port** den Port (normalerweise 80 oder 443) für den Mobile Service Provider-Dienst fest. Wenn Sie Port 443 verwenden, muss an den Port in IIS ein SSL-Zertifikat gebunden sein.
- Legen Sie **Authorization Group** oder **User** fest. Dies ist die Gruppe bzw. der Benutzer, die bzw. der in XenMobile eine Verbindung mit dem Mobile Service Provider-Dienst herstellen kann.
- Legen Sie fest, ob ActiveSync-Abfragen aktiviert sein sollen. Wenn ActiveSync-Abfragen für XenMobile Server aktiviert werden, muss der Snapshottyp für den bzw. die Exchange Server auf **Deep** eingestellt werden. Diese Einstellung kann zu einer starken Leistungsminderung beim Erstellen von Snapshots führen.
- Standardmäßig werden ActiveSync-Geräte, die dem regelmäßigen Ausdruck “WorxMail.*” entsprechen, nicht an XenMobile gesendet. Zum Ändern dieses Verhaltens ändern Sie das Feld **Filter ActiveSync** nach Bedarf.
  Ein leeres Feld bedeutet, dass alle Geräte an XenMobile weitergeleitet werden.
- Klicken Sie auf **Speichern**.

14. Konfigurieren Sie optional eine oder mehrere Instanzen von BlackBerry Enterprise Server (BES): Klicken Sie auf **Add** und geben Sie den Servernamen des BES-SQL-Servers ein



- Geben Sie den Namen der BES-Verwaltungsdatenbank ein.
- Wählen Sie unter **Authentication** den Authentifizierungsmodus aus. Bei Auswahl von “Windows Integrated” wird das Dienstbenutzerkonto des Endpoint Management-Connectors für Exchange ActiveSync für die Verbindung mit dem BES SQL-Server verwendet. Wenn Sie für die Datenbankverbindung des Endpoint Management-Connectors für Exchange ActiveSync außerdem “Windows Integrated” auswählen, muss das hier angegebene Windows-Konto auch Zugriff auf die Datenbank des Endpoint Management-Connectors für Exchange ActiveSync erhalten.
- Wenn Sie **SQL authentication** auswählen, geben Sie den Benutzernamen und das Kennwort ein.
- Legen Sie unter **Sync Schedule** den Synchronisierungszeitplan fest. Nach diesem Zeitplan erfolgt eine regelmäßige Verbindung mit dem BES SQL-Server zur Prüfung auf Aktualisierungen an Geräten.
- Klicken Sie auf **Test Connectivity**, um die Verbindung mit dem SQL-Server zu prüfen. Wurde “Windows Integrated” ausgewählt, wird beim Test das Konto des aktuell angemeldeten Benutzers anstelle des Dienstkontos des Endpoint Management-

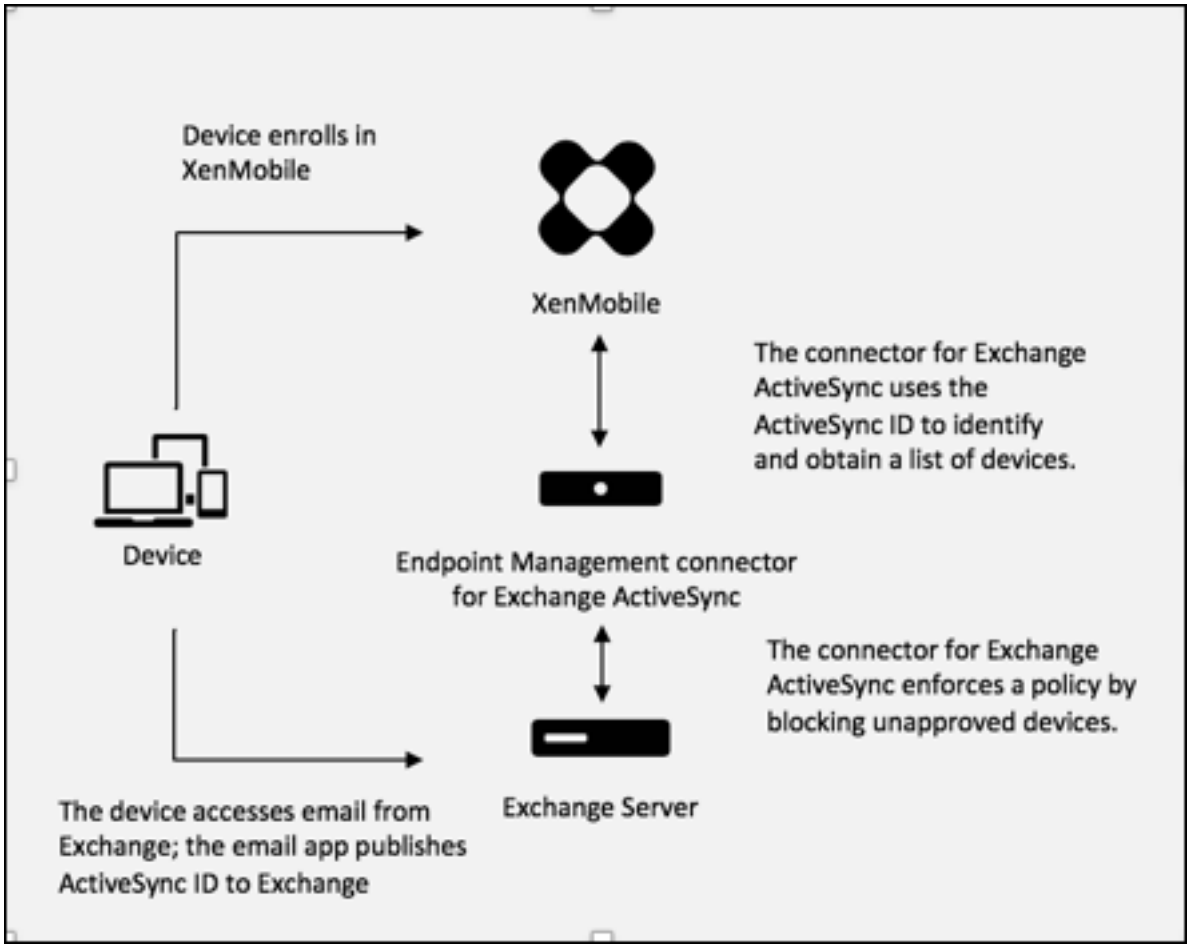
Connectors für Exchange ActiveSync verwendet und die SQL-Authentifizierung daher nicht richtig getestet.

- Wenn Sie Remotelöschen und Zurücksetzen des Kennworts auf BlackBerry-Geräten von XenMobile aus unterstützen möchten, aktivieren Sie das Kontrollkästchen **Enabled**.
- Geben Sie den vollqualifizierten Domänennamen (FQDN) für BES ein.
- Geben Sie den BES-Port ein, der für den Verwaltungswebdienst verwendet wird.
- Geben Sie den vollqualifizierten Benutzernamen und das Kennwort ein, das für den BES-Dienst erforderlich ist.
- Klicken Sie auf **Test Connectivity**, um die Verbindung mit BES zu testen.
- Klicken Sie auf **Speichern**.

Erzwingen von E-Mail-Richtlinien mit ActiveSync-IDs

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. Der Endpoint Management Connector für Exchange ActiveSync und XenMobile setzen eine solche E-Mail-Richtlinie zusammen durch. In XenMobile wird die Richtlinie für den Zugriff auf Unternehmens-E-Mail festgelegt und wenn ein nicht genehmigtes Gerät bei XenMobile registriert wird, erzwingt der Endpoint Management Connector für Exchange ActiveSync 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 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 der Endpoint Management Connector für Exchange ActiveSync ermitteln, ob ein bestimmtes Gerät auf Unternehmens-E-Mail zugreifen darf. Das Konzept wird in folgender Abbildung dargestellt:



Wenn XenMobile dem Endpoint Management Connector für Exchange ActiveSync eine ActiveSync-ID sendet, die sich von der von dem Gerät in Exchange veröffentlichten ID unterscheidet, kann der Connector nicht vorgeben, was mit dem Gerät geschehen 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.

Um sicherzustellen, dass die Unternehmensrichtlinien für den E-Mail-Zugriff ordnungsgemäß durchgesetzt werden, können Sie eine defensive Sicherheitsstrategie anwenden und den Endpoint Management Connector für Exchange ActiveSync so konfigurieren, dass E-Mails blockiert werden, indem Sie die statische Richtlinie standardmäßig auf “Verweigern” festlegen. Wenn ein Mitarbeiter einen anderen E-Mail-Client 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

Der Endpoint Management Connector für Exchange ActiveSync bietet eine regelbasierte Methode zur dynamischen Konfiguration der Zugriffssteuerung für Exchange ActiveSync-Geräte. Die Zugriffsregeln von Endpoint Management Connector für Exchange ActiveSync 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 **Speichern** klicken, gehen alle im Fenster gemachten Änderungen verloren, wenn Sie das Tool zum Konfigurieren schließen.

Der Endpoint Management Connector für Exchange ActiveSync bietet drei Regeltypen: lokale Regeln, XenMobile Server-Regeln (XDM-Regeln) und die Standardzugriffsregel.

Lokale Regeln: Diese haben die höchste Priorität, d. h. sobald eine lokale Regel auf ein Gerät zutrifft, wird die Regelauswertung eingestellt. Es werden weder die XenMobile Server-Regeln noch die Standardzugriffsregel konsultiert. Lokale Regeln werden in Bezug auf den Endpoint Management Connector für Exchange ActiveSync 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 regulären 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 regulären Ausdrücken hinzuzufügen. Wenn kein größerer Snapshot durchgeführt wurde, können Sie nur Regeln mit regulären Ausdrücken hinzufügen.

XenMobile Server-Regeln: XenMobile Server-Regeln sind Verweise auf einen externen XenMobile Server, der Regeln für verwaltete Geräte bereitstellt. 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 den Endpoint Management Connector für Exchange ActiveSync gesendet werden.

Standardzugriffsregel: Die Besonderheit der Standardzugriffsregel besteht darin, dass sie theoretisch auf jedes Gerät zutreffen kann und immer als letzte ausgewertet wird. Die Regel dient als

Auffangnetz für alle Geräte; trifft bei einem Gerät weder eine lokale noch eine XenMobile Server-Regel zu, wird der gewünschte Zugriffszustand durch die Standardzugriffsregel bestimmt.

- **Default Access – Allow:** Geräte, auf die weder eine lokale noch eine XenMobile Server-Regel zutrifft, werden alle zugelassen.
- **Default Access – Block:** Geräte, auf die weder eine lokale noch eine XenMobile Server-Regel zutrifft, werden alle blockiert.
- **Default Access – Unchanged:** Bei Geräten, auf die weder eine lokale noch eine XenMobile Server-Regel zutrifft, wird der Zugriffszustand vom Endpoint Management Connector für Exchange ActiveSync 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.

Regelauswertung

Für jedes Gerät, das Exchange dem Endpoint Management Connector für Exchange ActiveSync 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 Server-Regeln
- 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 Server-Regeln oder der Standardzugriffsregel. Das gleiche Prinzip gilt für die Regeln desselben Regeltyps. Beispiel: Treffen mehrere lokale Regeln auf ein Gerät zu, wird die Auswertung beendet, wenn die erste Übereinstimmung gefunden wird.

Der Endpoint Management Connector für Exchange ActiveSync 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 Kontext des Endpoint Management Connectors für Exchange ActiveSync funktionieren. In Exchange können Regeln dreierlei Ebenen konfiguriert werden: persönliche Ausnahmen, Geräteregeln und Organisationseinstellungen. Der Endpoint Management Connector für Exchange ActiveSync 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. Der

Endpoint Management Connector für Exchange ActiveSync übernimmt bei seiner Bereitstellung die Verwaltung der Ausnahmelistenfunktion in Exchange. Weitere Informationen finden Sie im Microsoft-Artikel Controlling Device Access.

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.

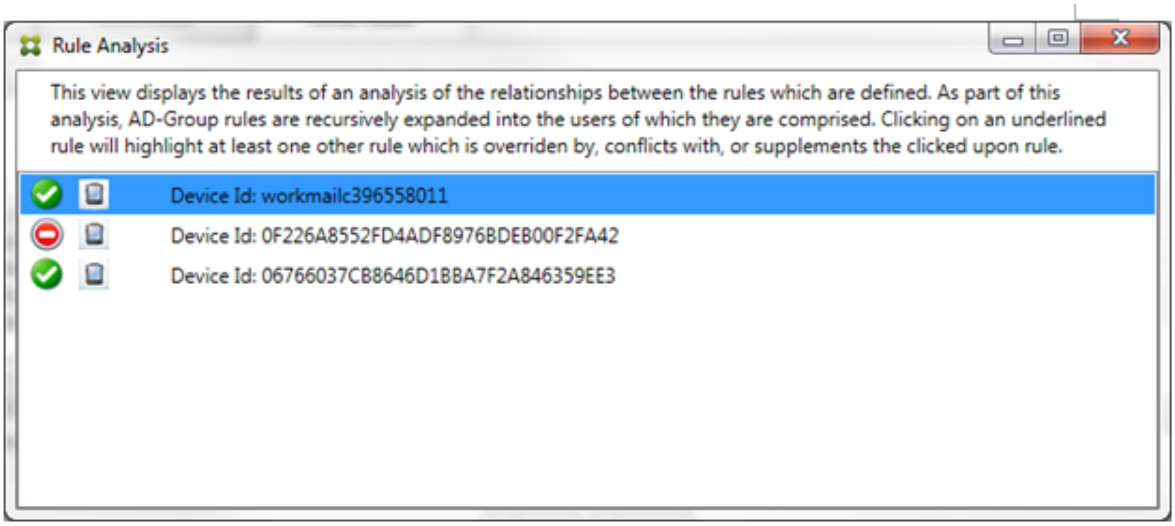
Terminologie der Regeln

- **Außerkraftsetzung:** Eine Außerkraftsetzung tritt auf, wenn mehrere Regeln auf ein Gerät zutreffen. Da Regeln nacheinander gemäß Priorität ausgewertet werden, werden zutreffende Regeln weiter unten in der Liste möglicherweise nie ausgewertet.
- **Konflikt:** 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 regulären Ausdrücken, folgt aus einem Konflikt grundsätzlich eine Außerkraftsetzung.
- **Ergänzung:** Eine Ergänzung liegt vor, wenn mehrere Regeln reguläre Ausdrücke enthalten und daher sichergestellt werden muss, dass die regulären Ausdrücke sich entweder zu einem einzigen zusammenfassen lassen, oder aber keine Funktionalität duplizieren. Eine Ergänzungsregel kann auch beim Zugriffszustand (Zulassen/Blockieren) einen Konflikt verursachen.
- **Primärregel:** 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.
- **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.

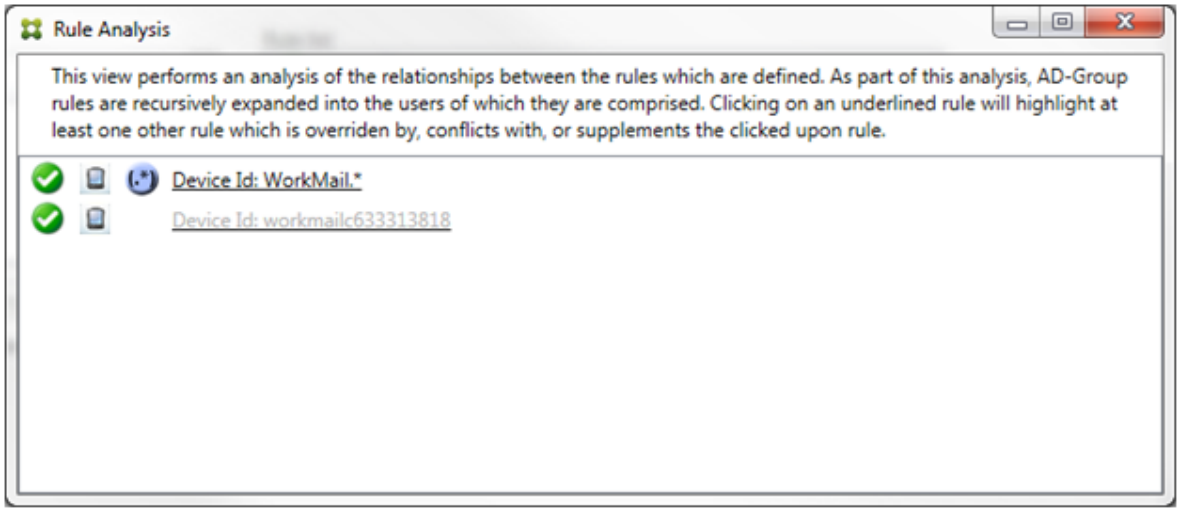
Darstellung des Regeltyps im Dialogfeld “Rule Analysis”

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.

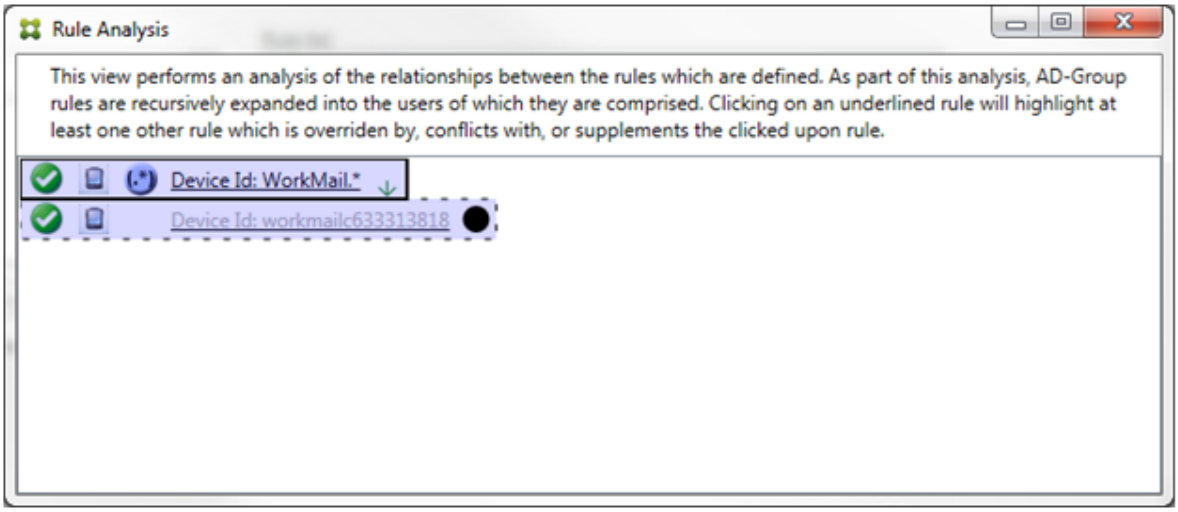
Im Fenster “Rule Analysis” ist ein Kontrollkästchen, bei dessen Aktivierung nur die Regeln angezeigt werden, die Konflikte, Überschreibungen, Redundanzen oder Ergänzungen sind.



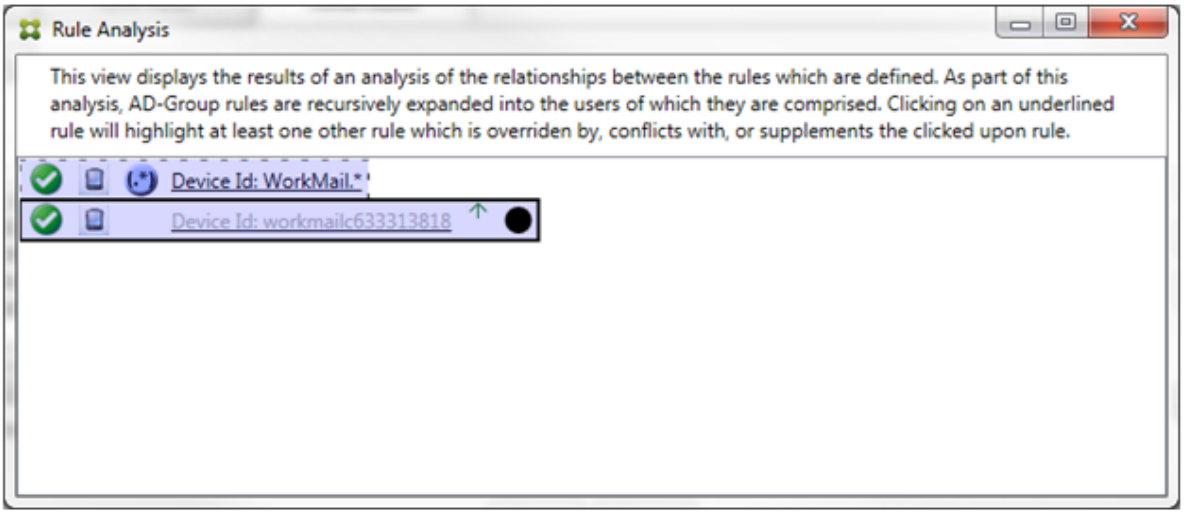
Wenn eine Außerkraftsetzung vorliegt, werden mindestens zwei Regeln unterstrichen dargestellt: die primäre Regel und die Nebenregel(n). Mindestens eine Nebenregel erscheint in einer helleren Schrift, um anzuzeigen, dass sie durch eine höhere Regel außer Kraft gesetzt wird. Sie können auf die außer Kraft 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:



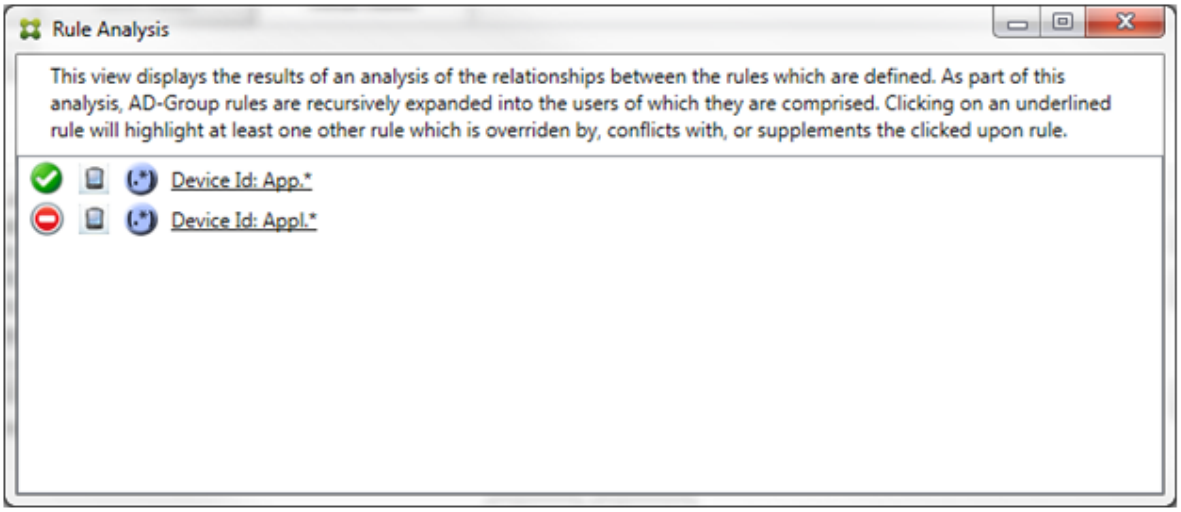
In diesem Beispiel ist die Regel mit regulären Ausdrücken `WorkMail.*` die primäre Regel (angezeigt durch den durchgehenden Rahmen) und die normale Regel `workmailc633313818` ist eine Nebenregel (angezeigt durch den gestrichelten Rahmen). Der schwarze Punkt neben der Nebenregel weist deutlich darauf hin, dass die Regel inaktiv ist (d. h. niemals ausgewertet wird), da ihr die Regel mit den regulären Ausdrücken voransteht und eine höhere Priorität hat. Nach dem Klicken auf die außer Kraft gesetzte Regel wird das Dialogfeld folgendermaßen angezeigt:



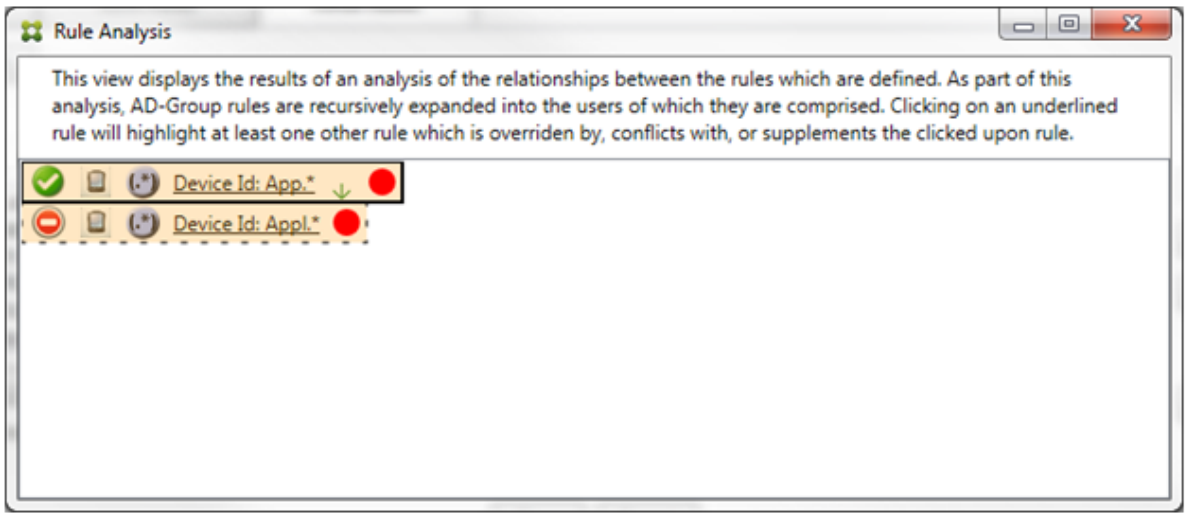
Im obigen Beispiel ist die Regel mit regulären Ausdrücken `WorkMail.*` die Nebenregel (angezeigt durch den gestrichelten Rahmen) und die normale Regel `workmailc633313818` ist eine primäre Regel (angezeigt durch den durchgehenden Rahmen). In diesem einfachen Beispiel ist der Unterschied nicht groß. Ein 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 gekennze-

ichnet. Ein reiner Konflikt ist nur möglich, wenn mindestens zwei Regeln mit regulären 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:

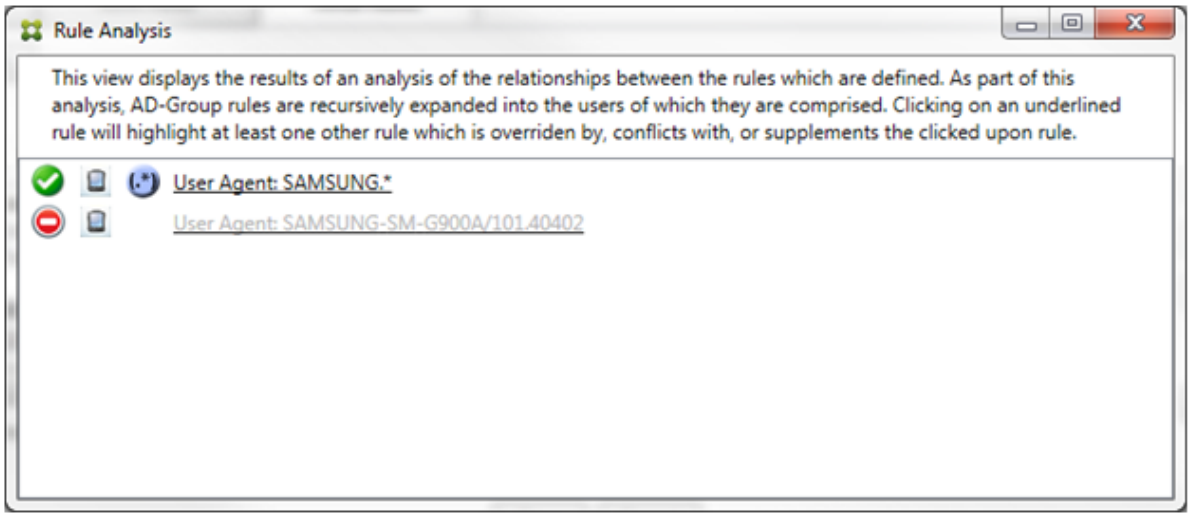


Eine Untersuchung der beiden Regeln mit regulären Ausdrücken ergibt, dass die erste alle Geräte, deren ID “App” enthält, zulässt und die zweite alle Geräte, deren ID “Appl” enthält, blockiert. Obwohl die zweite Regel alle Geräte, deren ID “Appl” enthält, blockiert, wird kein Gerät, auf das die Regel zutrifft, je blockiert, da die zulassende Regel eine höhere Priorität hat. Nach dem Klicken auf die erste Regel wird das Dialogfeld folgendermaßen angezeigt:



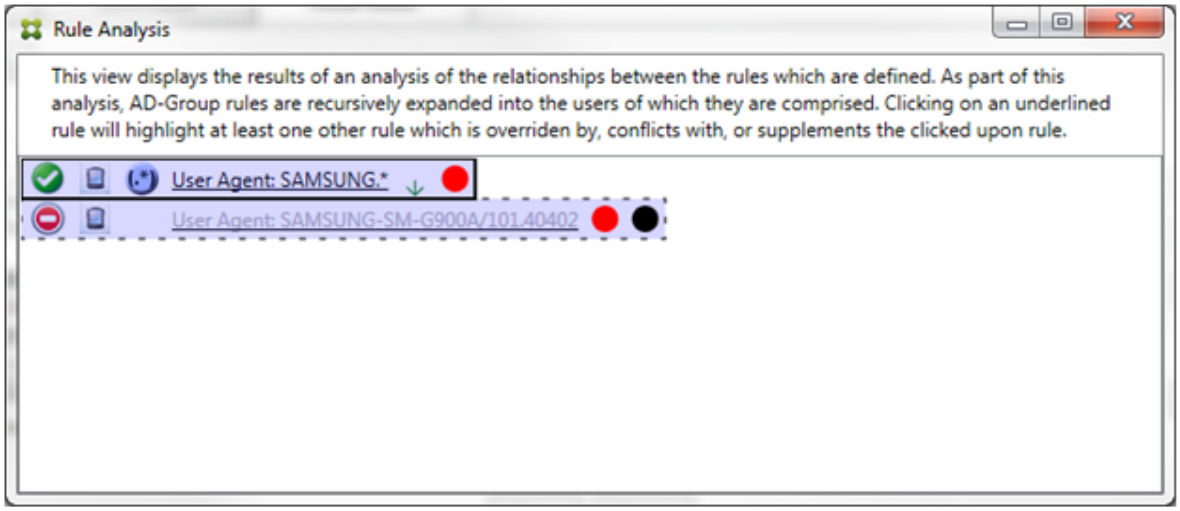
Im vorherigen Szenario wird sowohl die primäre Regel (mit dem regulären Ausdruck `App.*`) und die Nebenregel (mit dem regulären Ausdruck `Appl.*`) gelb markiert angezeigt. Dies ist ein einfacher optischer Warnhinweis auf den Umstand, dass mehrere Regeln mit regulärem Ausdruck für ein einzelnes Feld angewendet wurden, was eine Redundanz oder ein schwerwiegenderes Problem bedeuten kann.

In einem Szenario mit Konflikt und Außerkraftsetzung wird sowohl die primäre Regel (mit dem regulären Ausdruck `App.*`) und die Nebenregel (mit dem regulären Ausdruck `Appl.*`) gelb markiert angezeigt. Dies ist ein einfacher optischer Warnhinweis auf den Umstand, dass mehrere Regeln mit regulärem 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 regulären 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.

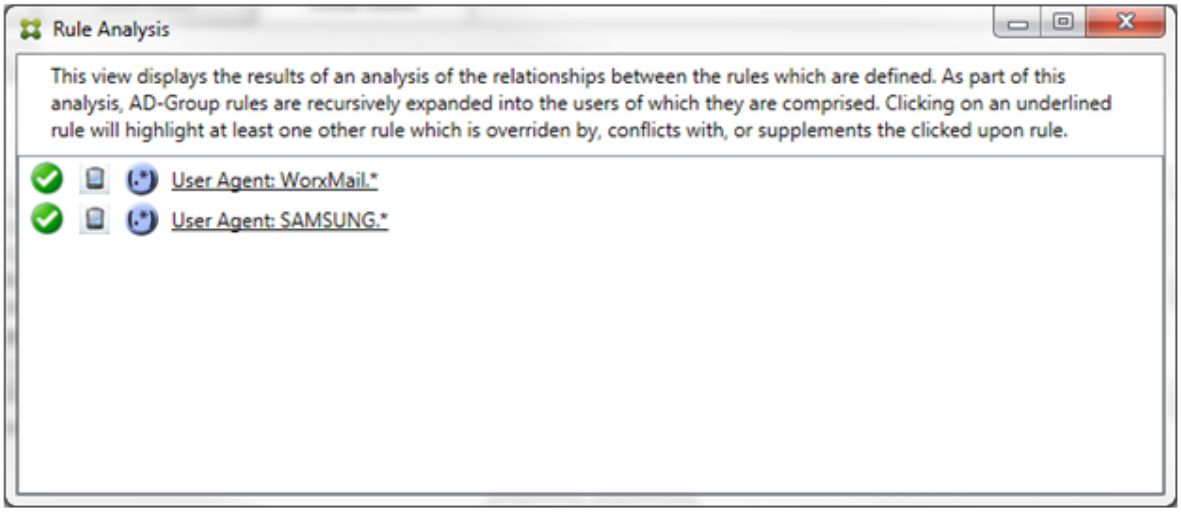
Nach dem Klicken auf die Regel mit dem regulären Ausdruck wird das Dialogfeld folgendermaßen angezeigt:



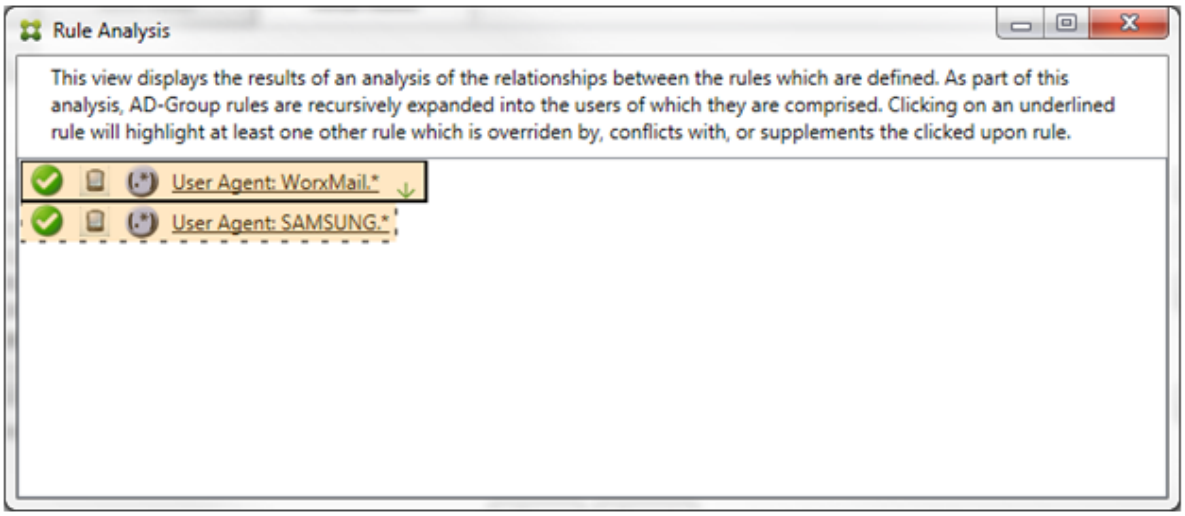
Die primäre Regel (mit dem regulären Ausdruck `SAMSUNG.*`) ist mit einem roten Punkt gekennzeichnet, um anzuzeigen, dass ihr Zugriffszustand im Widerspruch mit dem von mindestens einer

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. Ein schwarzer Punkt zeigt überdies an, 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 regulären Ausdrücken sein. Wenn Regeln einander ergänzen, werden sie durch eine gelbe Schattierung 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 regulären Ausdrücken sind, und beide auf das Feld “ActiveSync device ID” im Endpoint Management Connector für Exchange ActiveSync angewendet werden. Nach dem Klicken auf die erste Regel sieht das Dialogfeld folgendermaßen aus:



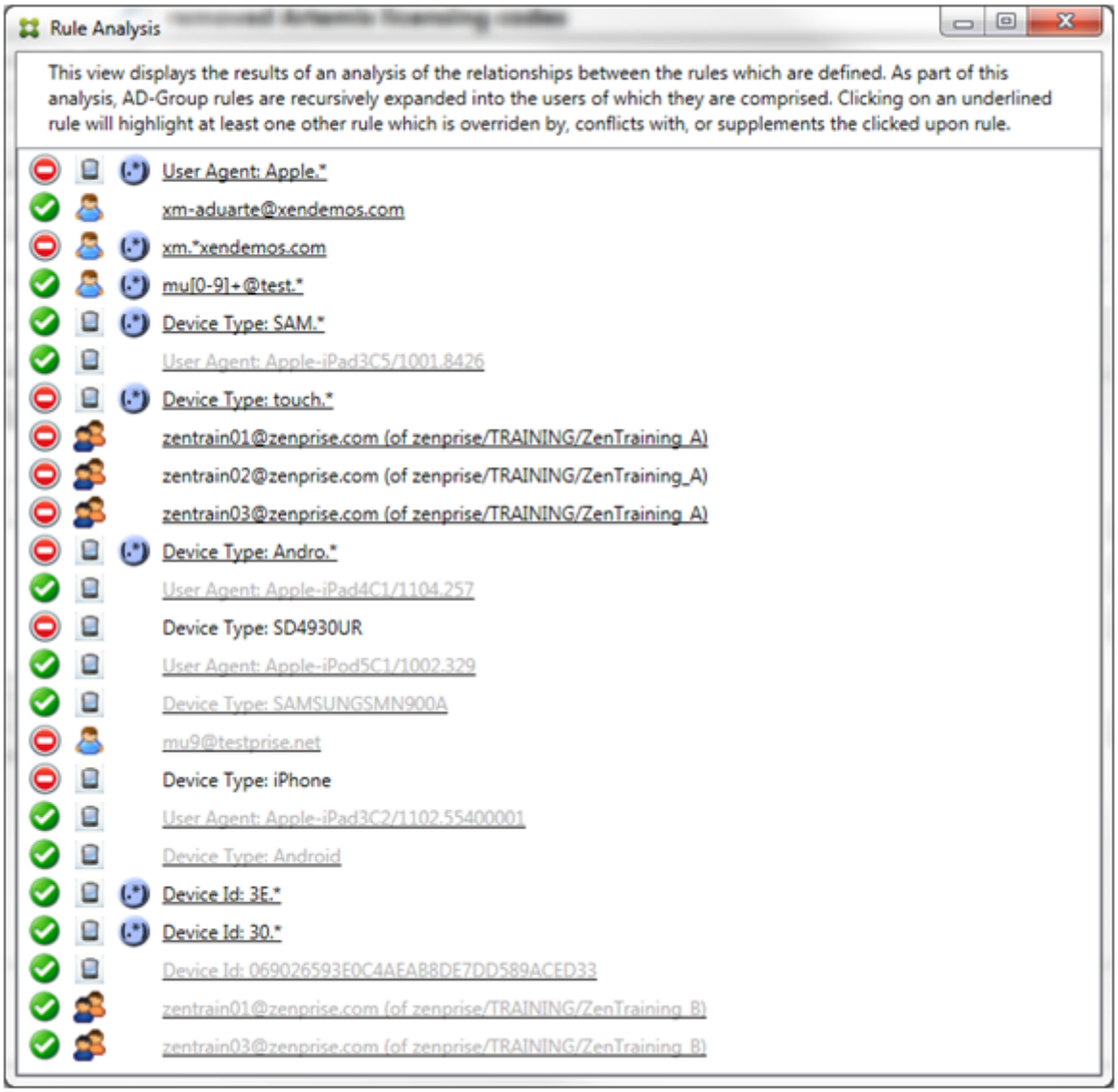
Die primäre Regel (mit dem regulären Ausdruck `WorkMail.*`) ist gelb hinterlegt, um anzuzeigen, dass es mindestens eine Nebenregel mit einem regulären Ausdruck gibt. Die Nebenregel (mit dem

regulären Ausdruck `SAMSUNG.*`) ist gelb hinterlegt, um anzuzeigen, dass sie und die primäre Regel als Regel mit einem regulären Ausdruck auf dasselbe Feld im Endpoint Management Connector für Exchange ActiveSync (ActiveSync device ID) angewendet werden. In diesem Fall ist dieses Feld die ActiveSync-Geräte-ID. Dabei überschneiden die regulären Ausdrücke einander möglicherweise. Sie müssen entscheiden, ob die regulären 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.

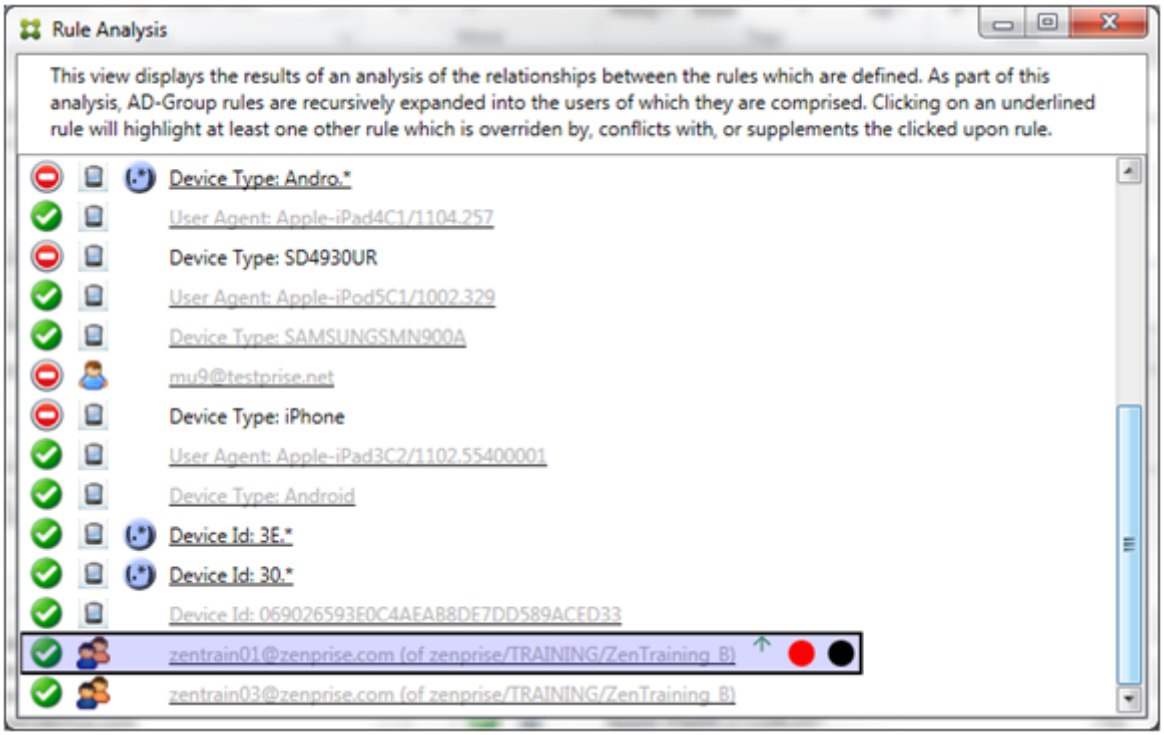
Die Liste enthält auch eine Reihe von Regeln mit regulären Ausdrücken, die durch das Symbol  gekennzeichnet sind.



Analysieren einer Außerkraftsetzung

Um zu sehen, welche Regeln eine bestimmte Regel außer Kraft setzen, klicken Sie auf die Regel.

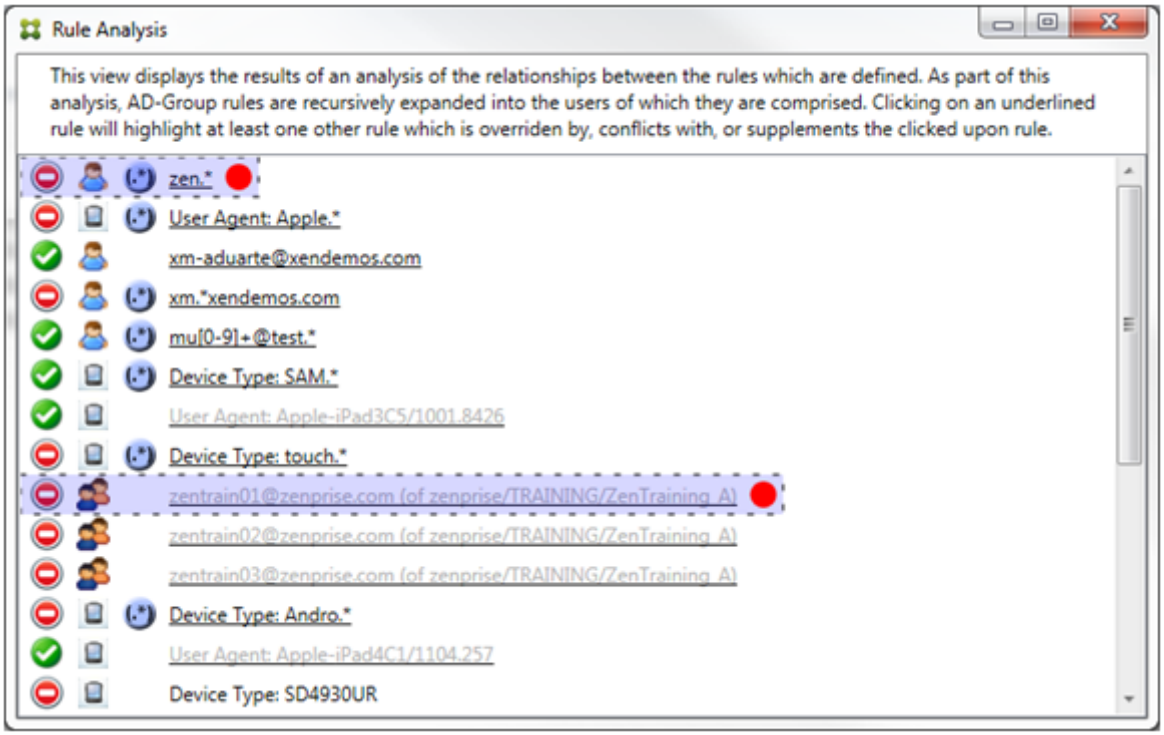
Beispiel 1: In diesem Beispiel wird untersucht, warum `zentrain01@zenprise.com` außer Kraft gesetzt wird.



Die primäre Regel (AD-Gruppenregel `zenprise/TRAINING/ZenTraining B`, bei der `zentrain01@zenprise.com` Mitglied ist) hat die folgenden Merkmale:

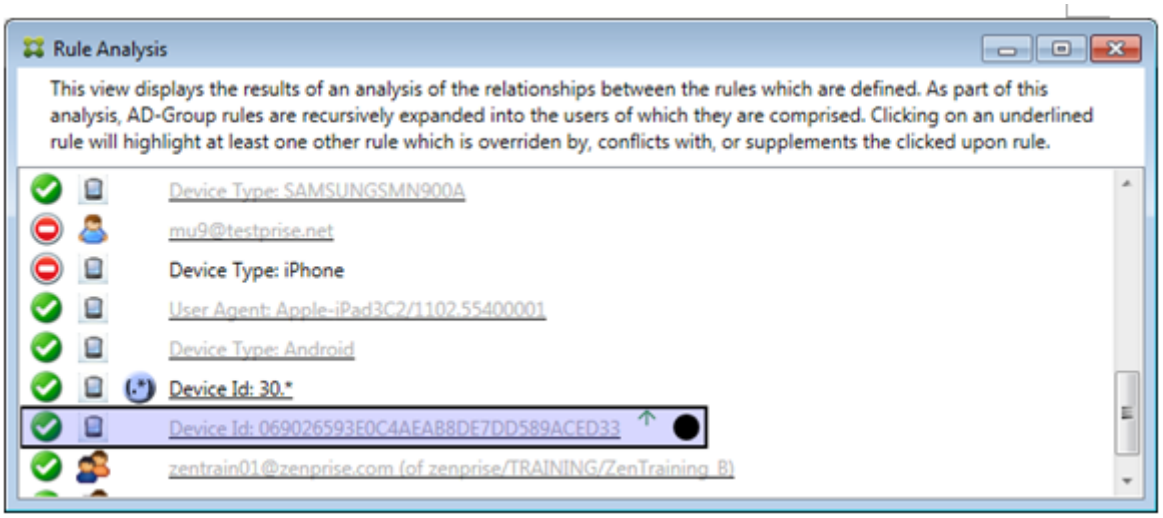
- Sie ist blau unterlegt und wird von einem durchgehenden Rahmen umgeben.
- Sie hat einen nach oben weisenden grünen Pfeil, was anzeigt, dass alle Nebenregeln weiter oben sind.
- Sie ist mit einem roten und einem schwarzen Punkt gekennzeichnet, um anzuzeigen, dass erstens mindestens eine Nebenregel einen 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:



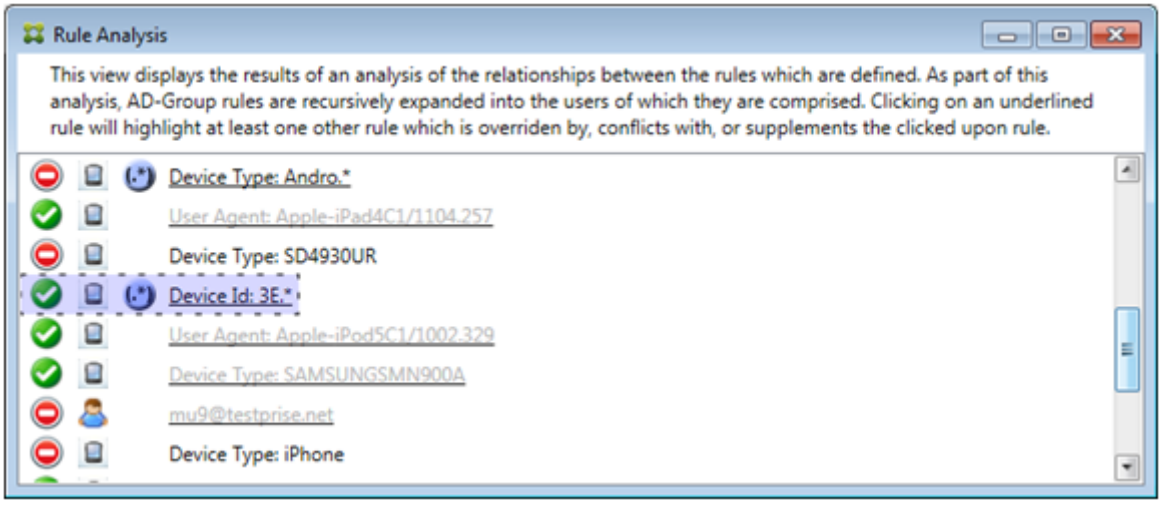
In diesem Fall gibt es zwei Nebenregeln, die die primäre Regel außer Kraft setzen: die Regel mit regulärem Ausdruck `zen.*` und die normale Regel `zentrain01@zenprise.com` (von `zenprise/TRAINING/ZenTraining A`). Bei der letzteren Nebenregel besteht das Problem darin, dass die Active Directory-Gruppenregel `ZenTraining A` den Benutzer `zentrain01@zenprise.com` enthält, die Active Directory-Gruppenregel `ZenTraining B` den Benutzer `zentrain01@zenprise.com` 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.

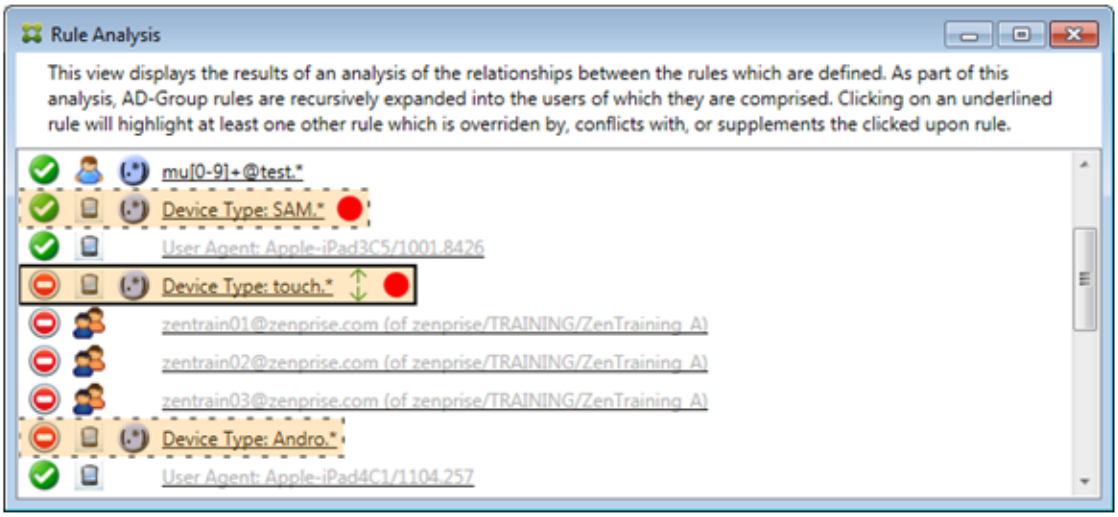


In diesem Fall wird die primäre Regel von einer einzigen Nebenregel außer Kraft gesetzt: der Regel mit der ActiveSync Geräte-ID und dem regulären Ausdruck `3E.*`. Da der reguläre Ausdruck `3E.*` auf `069026593E0C4AEAB8DE7DD589ACED33` zutrifft, würde die primäre Regel niemals ausgewertet.

Analysieren einer Ergänzung und eines Konflikts

In diesem Beispiel ist die primäre Regel die ActiveSync-Gerätetypregel mit dem regulären Ausdruck `touch.*` Sie hat folgende Merkmale:

- Sie ist von einem durchgehenden Rahmen umgeben und gelb hinterlegt, was anzeigt, dass mehrere Regeln mit regulären 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 regulären Ausdruck `SAM.*` und die ActiveSync-Gerätetypregel mit dem regulären Ausdruck `Andro.*`.
- Beide Nebenregeln sind von einem gestrichelten Rahmen umgeben, welcher anzeigt, dass es sich um Nebenregeln handelt.
- Beide Nebenregeln sind gelb hinterlegt, was anzeigt, dass sie auch auf das Regelfeld “ActiveSync device type” angewendet werden.
- In einem solchen Szenario sollten Sie sicherstellen, dass die Regeln mit regulären Ausdrücken nicht redundant sind.



Weitere Analyse von Regeln

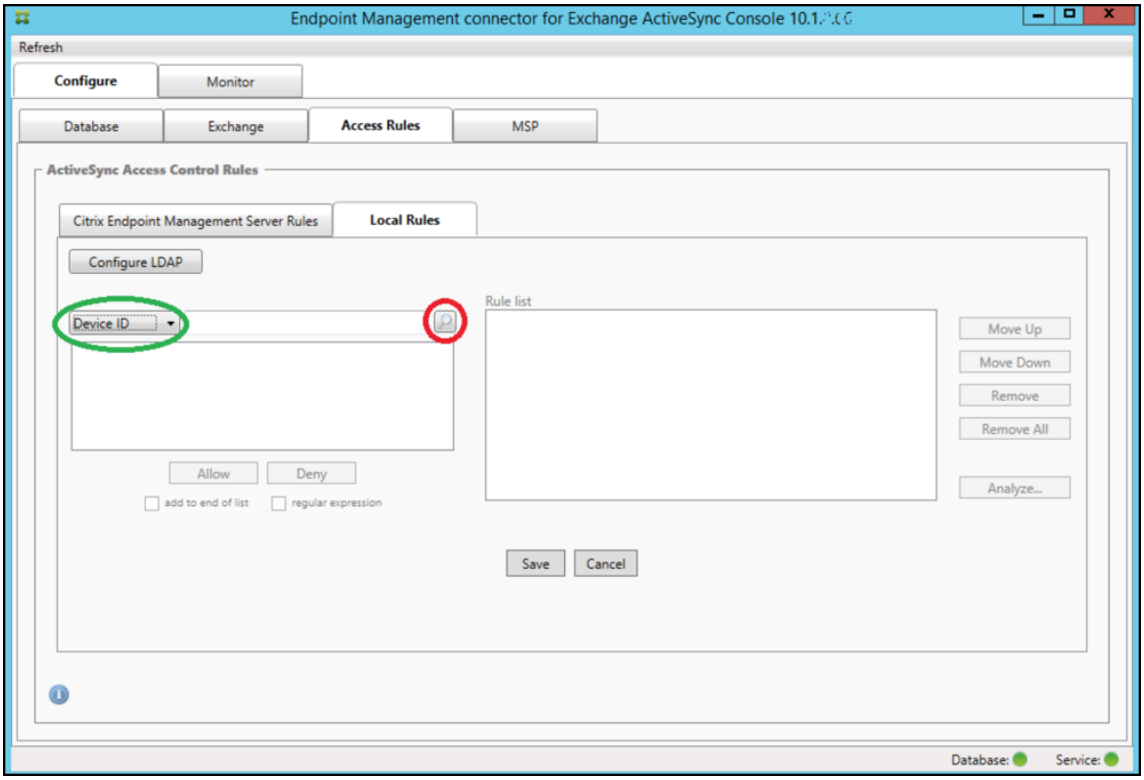
In diesem Beispiel wird demonstriert, dass Regelbeziehungen immer aus der Sicht der primären Regel dargestellt werden. Im vorherigen Beispiel wurde gezeigt, was ein Klick auf die Regel mit dem reg-

ulären Ausdruck für den Wert `touch.*` des Felds “device type” bewirkt. Wenn Sie auf die Nebenregel `Andro.*` klicken, werden andere Nebenregeln hervorgehoben.

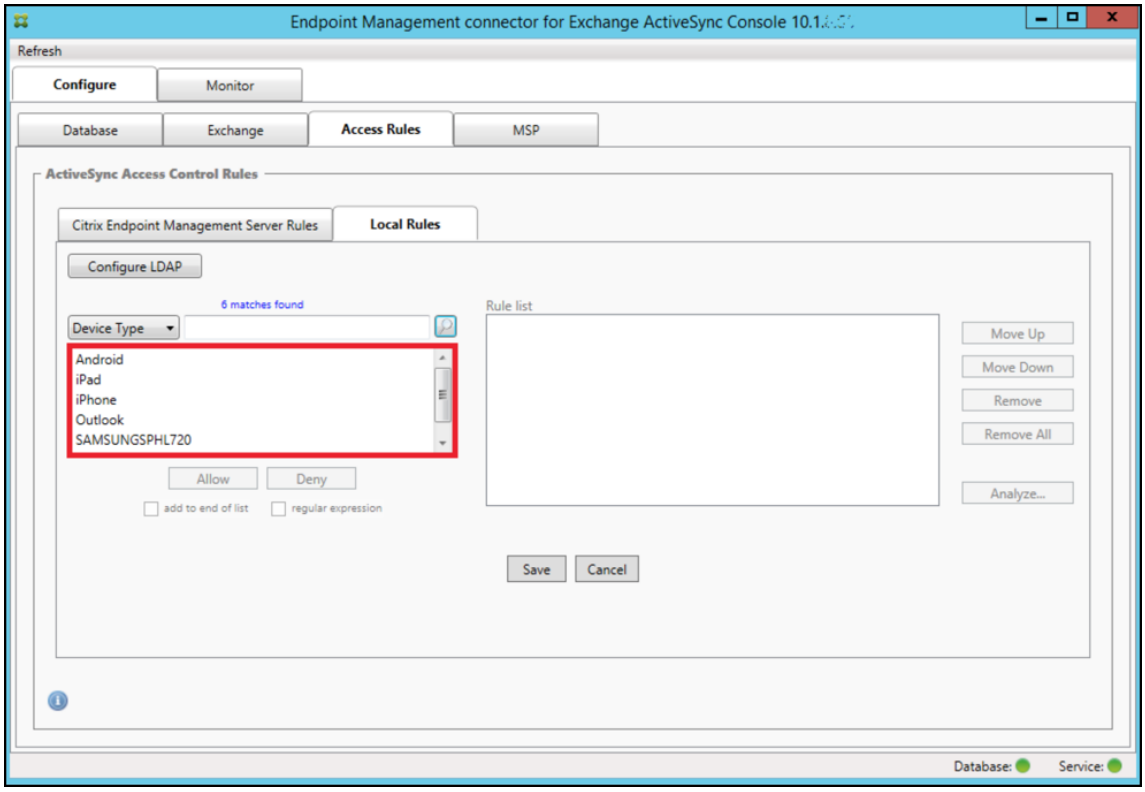
In diesem Beispiel wird eine außer Kraft gesetzte Regel, die Teil der Regelbeziehung ist, gezeigt. Diese Regel ist die normale ActiveSync-Gerätetypregel `Android`, die außer Kraft gesetzt ist (sichtbar an der helleren Schrift und dem schwarzen Punkt) und deren Zugriffszustand mit dem der primären ActiveSync-Gerätetypregel mit regulärem 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 regulärem Ausdruck `touch.*`) nicht mit dieser in Beziehung stand.

Konfigurieren einer lokalen Regel mit normalem Ausdruck

1. Klicken Sie auf die Registerkarte **Access Rules**.



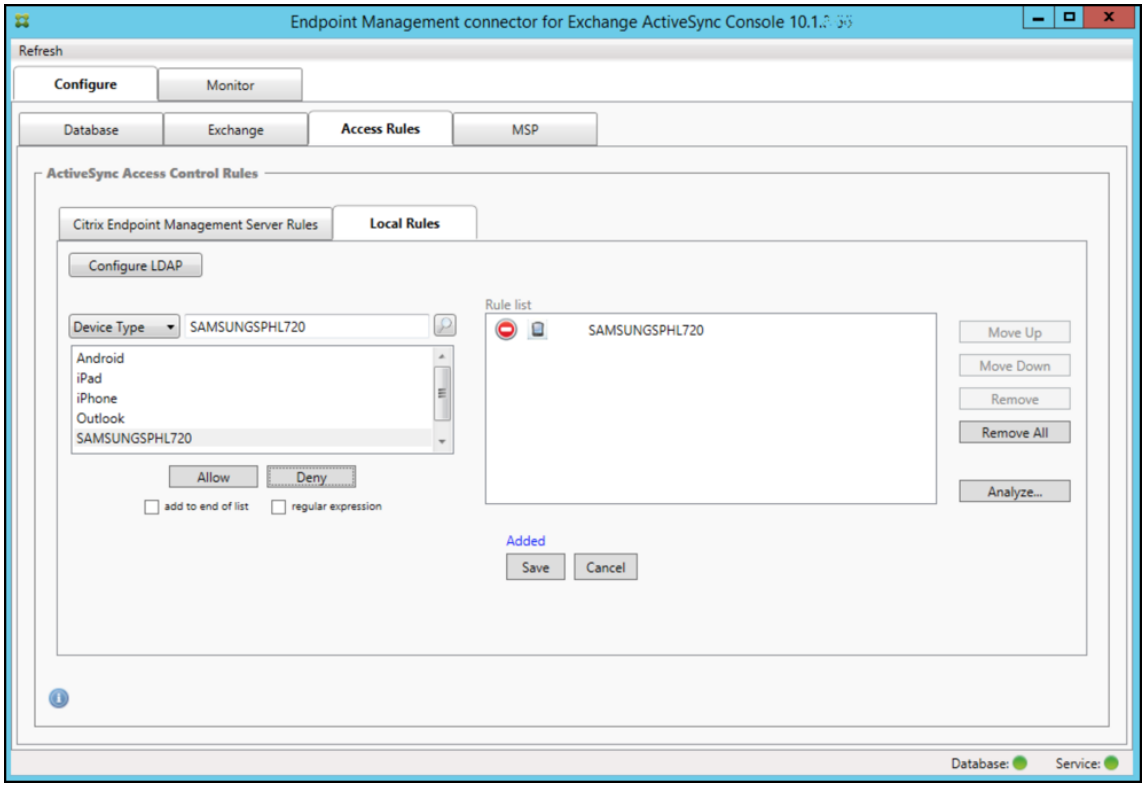
2. Wählen Sie in der Liste **Device ID** das Feld aus, für das Sie eine lokale Regel erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld **Gerätetyp** ausgewählt und die Auswahlmöglichkeiten werden unten im Listenfeld aufgeführt.



4. Klicken Sie auf eines der Elemente in der Ergebnisliste und anschließend auf eine der folgenden Optionen:

   - **Allow** konfiguriert Exchange so, dass ActiveSync-Datenverkehr für alle übereinstimmenden Geräte zugelassen wird.
   - **Deny** Allow konfiguriert Exchange so, dass ActiveSync-Datenverkehr für alle übereinstimmenden Geräte verweigert wird.

   In diesem Beispiel wird der Zugriff für alle Geräte des Typs SamsungSPhl720 verweigert.



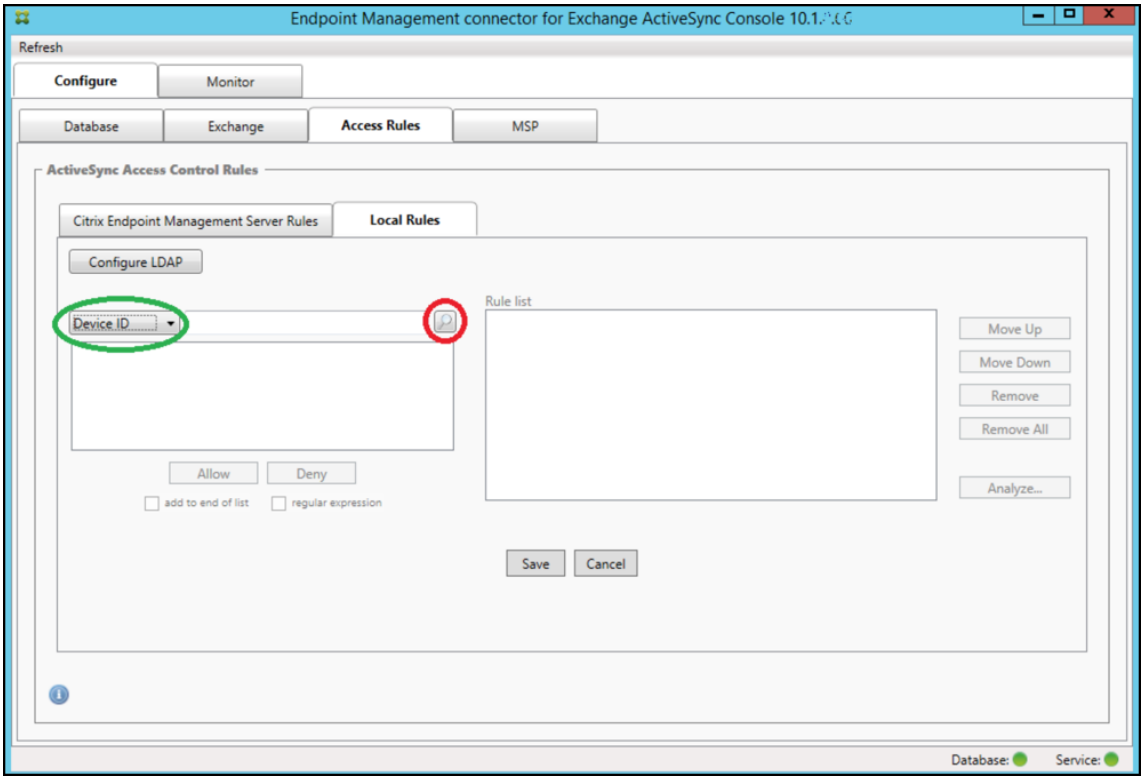
Hinzufügen eines regelmäßigen Ausdrucks

Lokale Regeln mit regulären Ausdrücken sind an dem Symbol  zu erkennen.

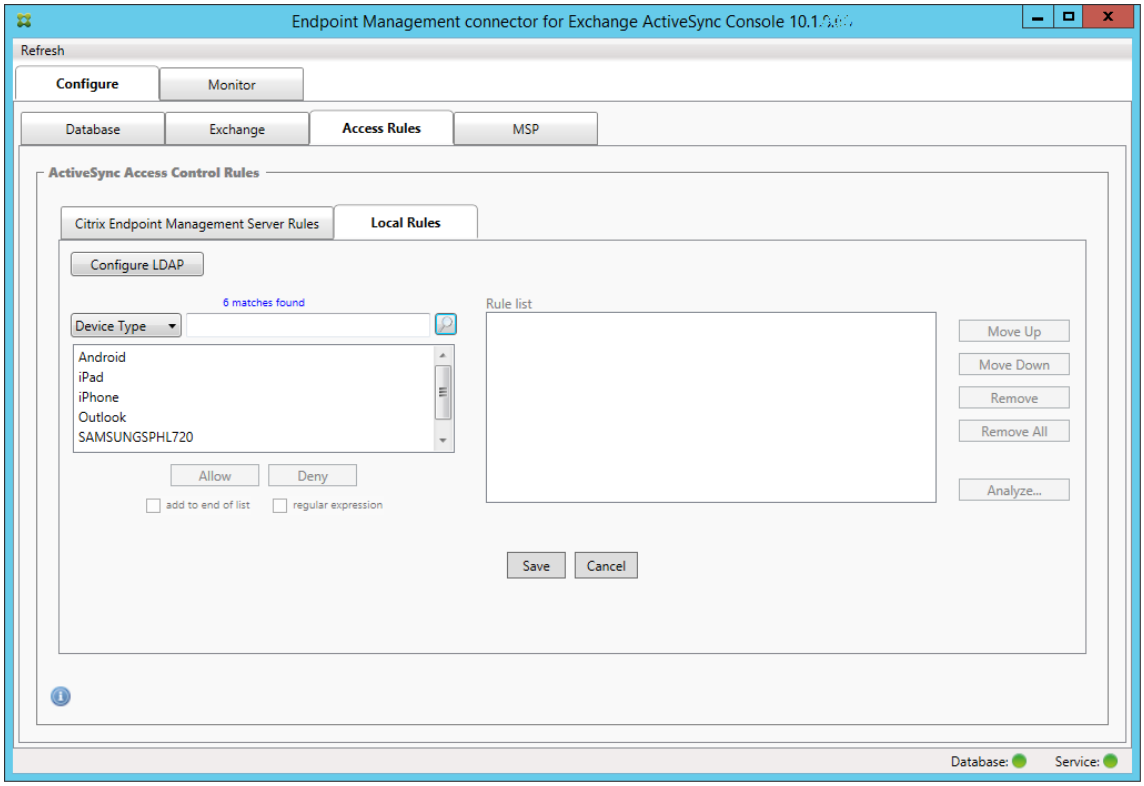
Zum Hinzufügen einer Regel mit regulärem Ausdruck können Sie entweder einen Wert aus der Ergebnisliste für ein spezifisches Feld als Grundlage verwenden (sofern bereits ein größerer Snapshot durchgeführt wurde) oder den regulären Ausdruck selbst eingeben.

Erstellen eines regulären Ausdrucks aus einem vorhandenen Feldwert

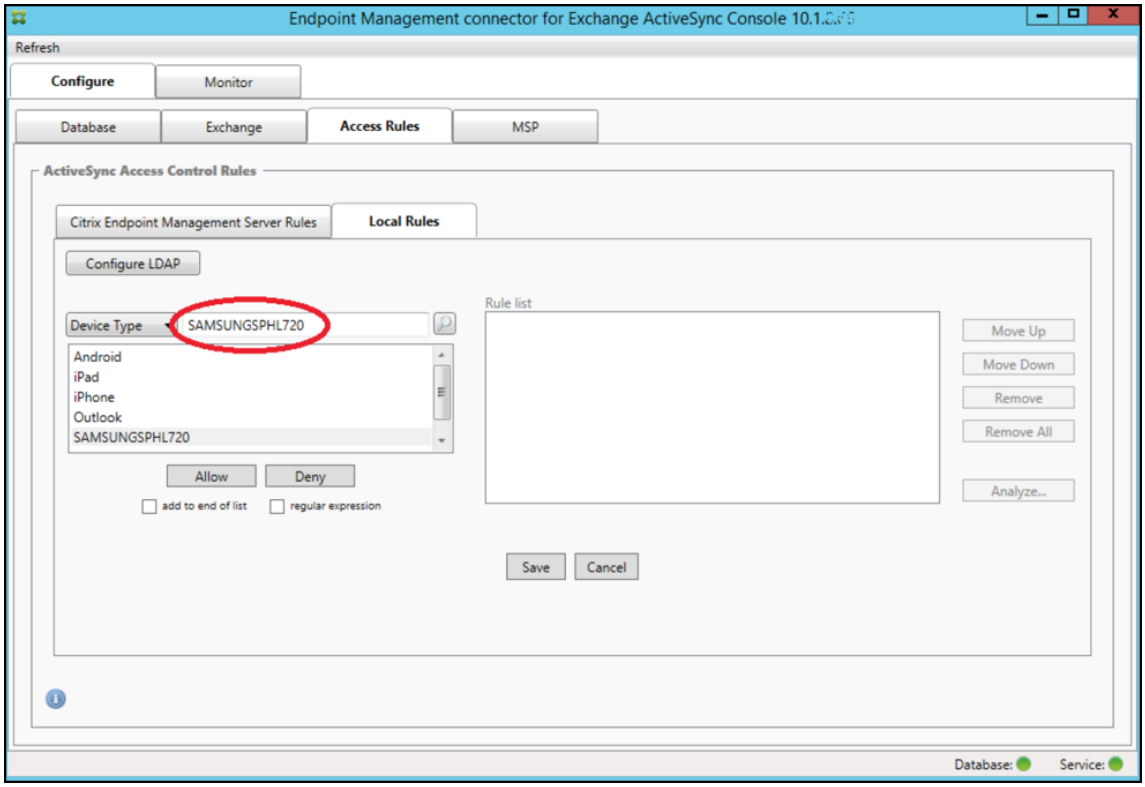
1. Klicken Sie auf die Registerkarte **Access Rules**.



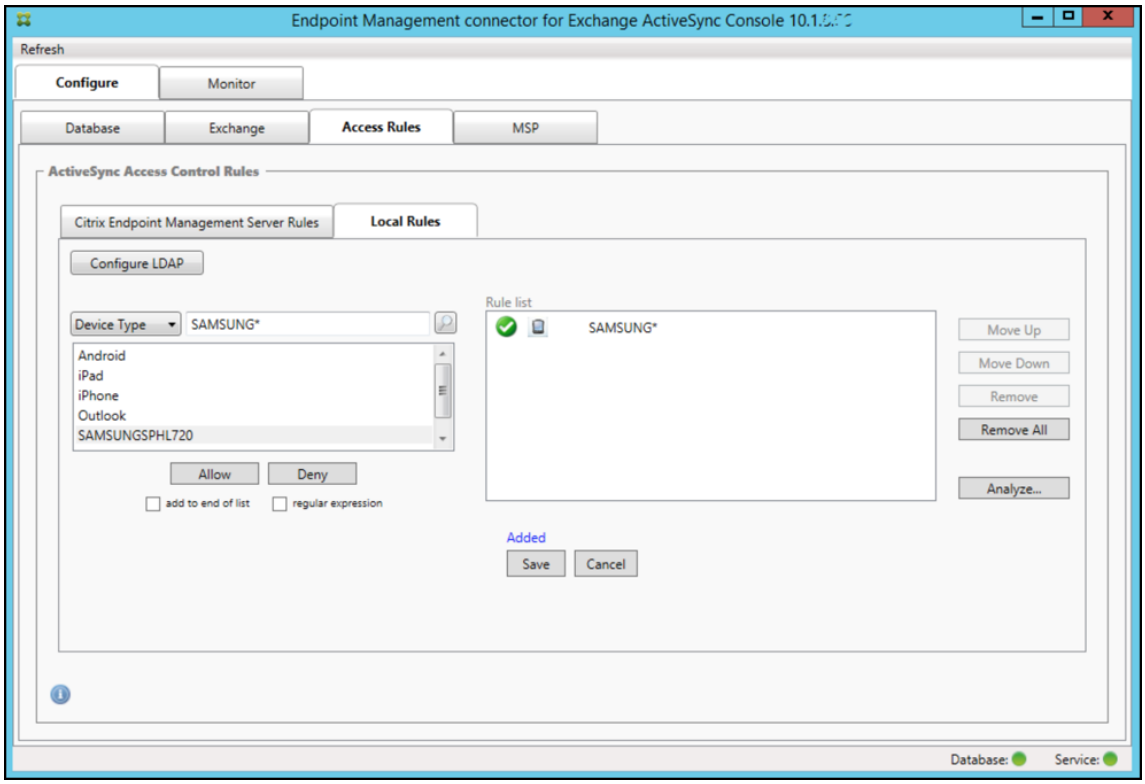
2. Wählen Sie in der Liste **Device ID** das Feld aus, für das Sie eine lokale Regel mit regulärem Ausdruck erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld **Gerätetyp** ausgewählt und die Auswahlmöglichkeiten werden unten im Listenfeld aufgeführt.



4. Klicken Sie auf einen der Einträge in der Ergebnisliste. In diesem Beispiel wurde **SAMSUNGSPHL720** ausgewählt und wird im Textfeld neben **Device Type** angezeigt.

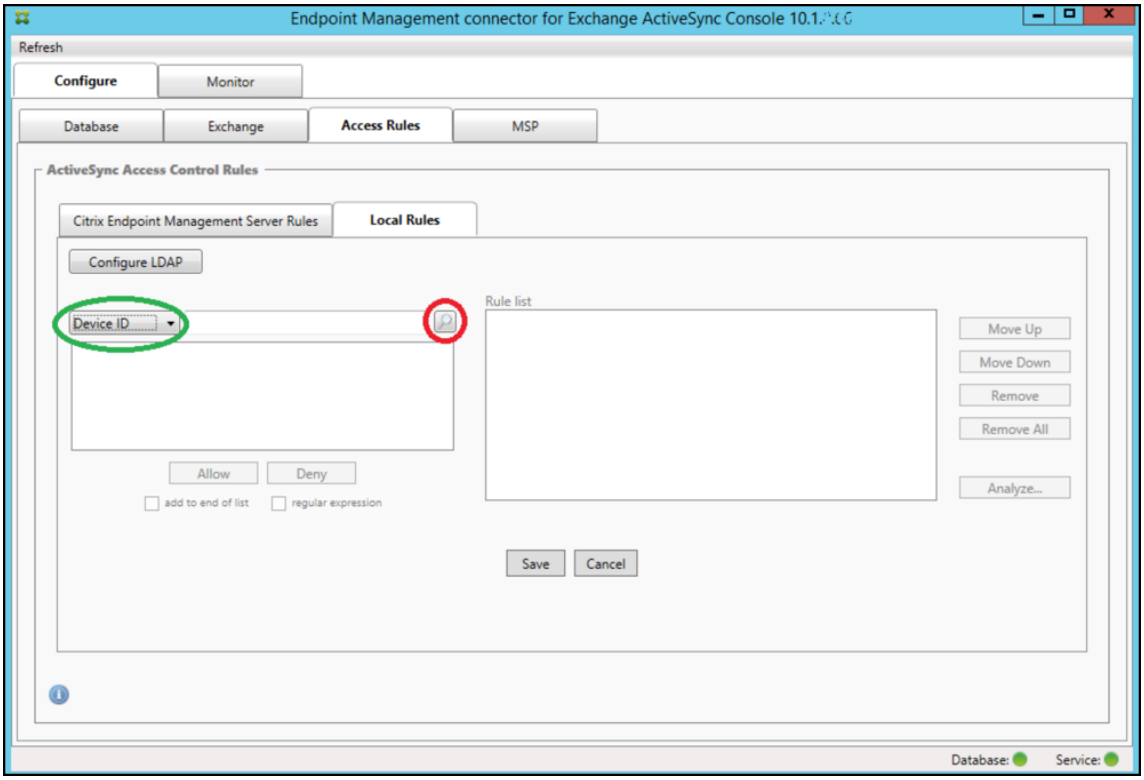


5. Um alle Gerätetypen zuzulassen, deren Gerätetypwert “Samsung” enthält, fügen Sie eine Regel mit regulärem Ausdruck hinzu, indem Sie die folgenden Schritte ausführen:
   a) Klicken Sie in das Textfeld des ausgewählten Elements.
   b) Ändern Sie den Text **SAMSUNGSPHL720** in **SAMSUNG.***.
   c) Stellen Sie sicher, dass das Kontrollkästchen “regular expression” aktiviert ist.
   d) Klicken Sie auf **Allow**.

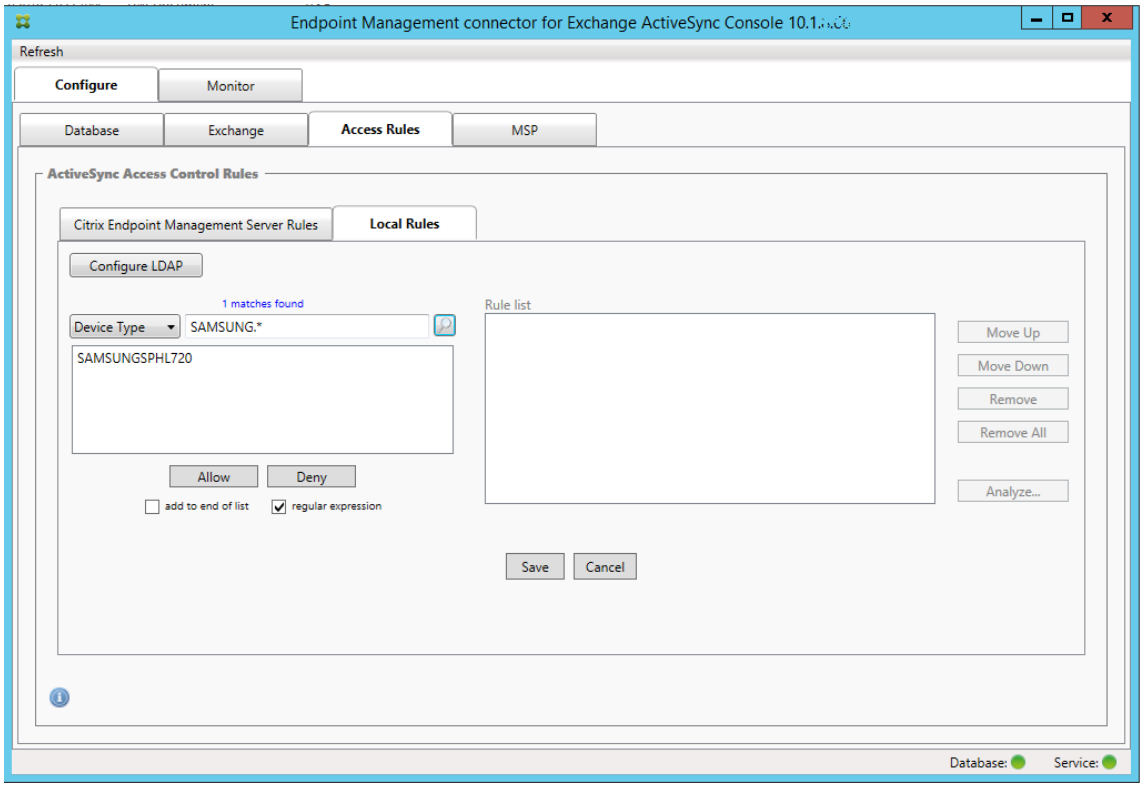


Erstellen einer Zugriffsregel

1. Klicken Sie auf die Registerkarte **Local Rules**.
2. Zur Eingabe des regulären Ausdrucks benötigen Sie die Liste “Device ID” und das Textfeld mit dem ausgewählten Element.



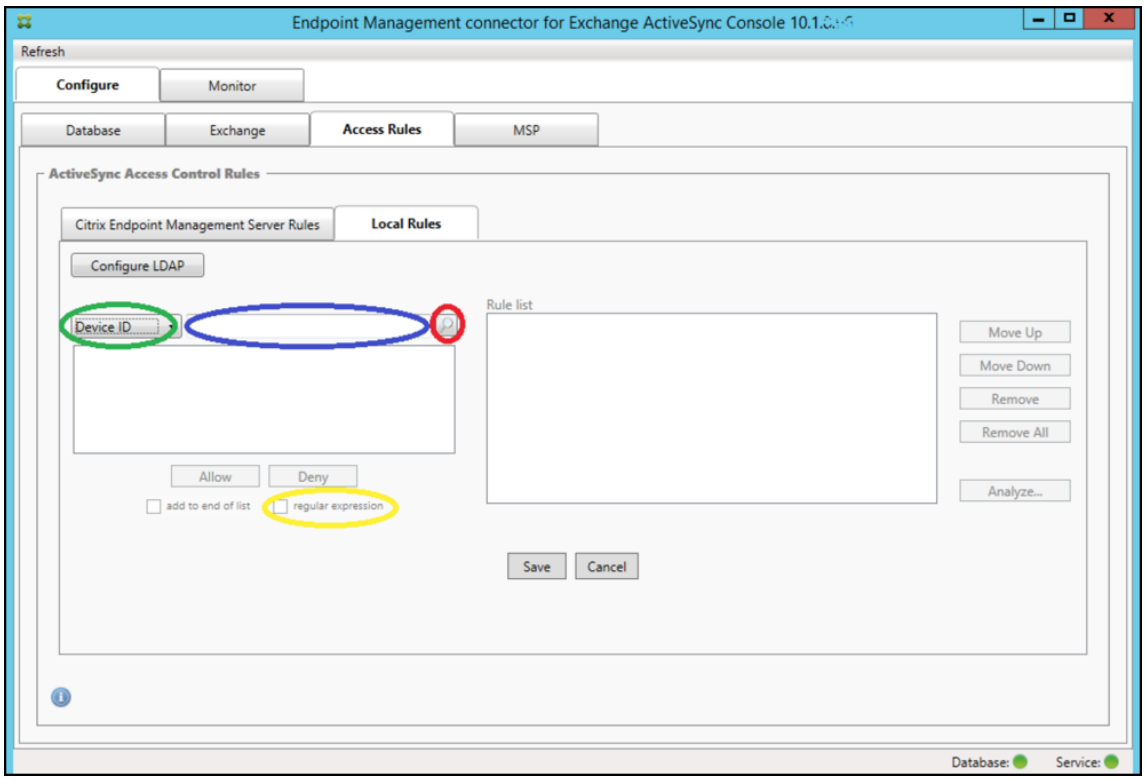
3. Wählen Sie das gewünschte Kriterienfeld aus. In diesem Beispiel ist dies Device Type.
4. Geben Sie den regulären Ausdruck ein. In diesem Beispiel ist dies `samsung.*`
5. Stellen Sie sicher, dass das Kontrollkästchen “regular expression” aktiviert ist, und klicken Sie auf **Allow** oder **Deny**. In diesem Beispiel ist die Auswahl **Allow**. Endergebnis:



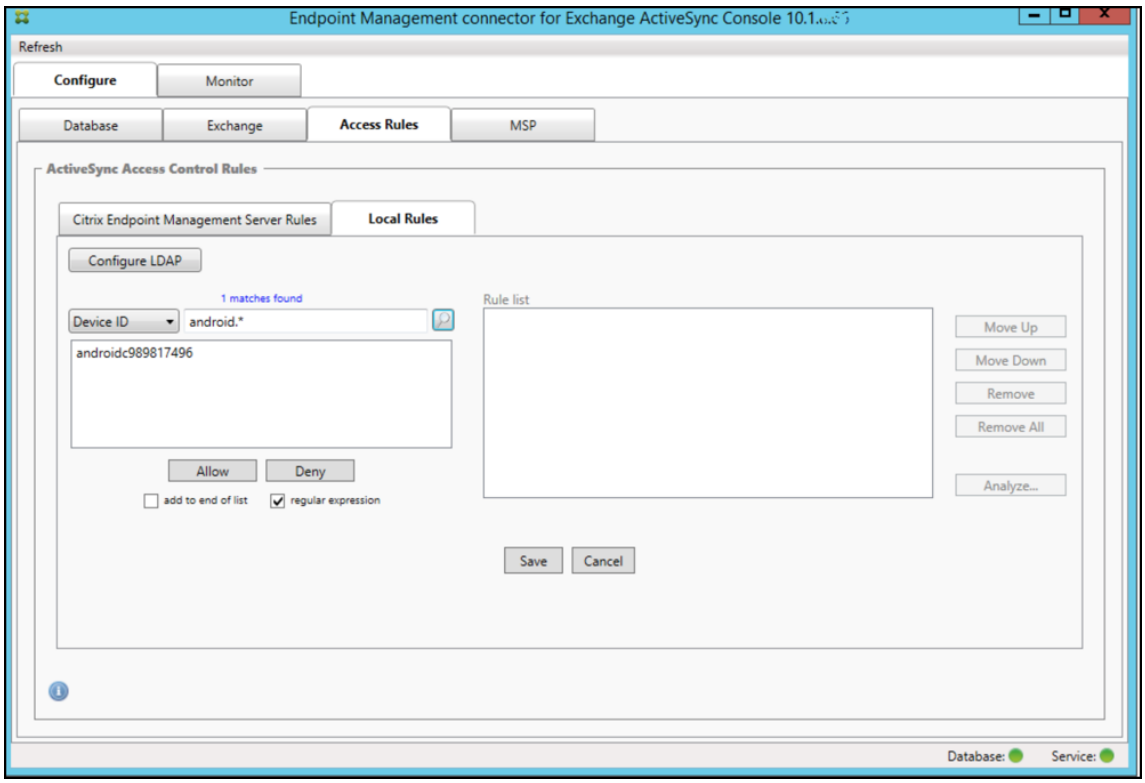
Suchen von Geräten

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 regulärer 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 als Kriterienfeld “Device ID” (= Standardeinstellung) ausgewählt ist.



3. Klicken Sie in das Textfeld des ausgewählten Elements (blau in der Abbildung oben) und geben Sie dann `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).

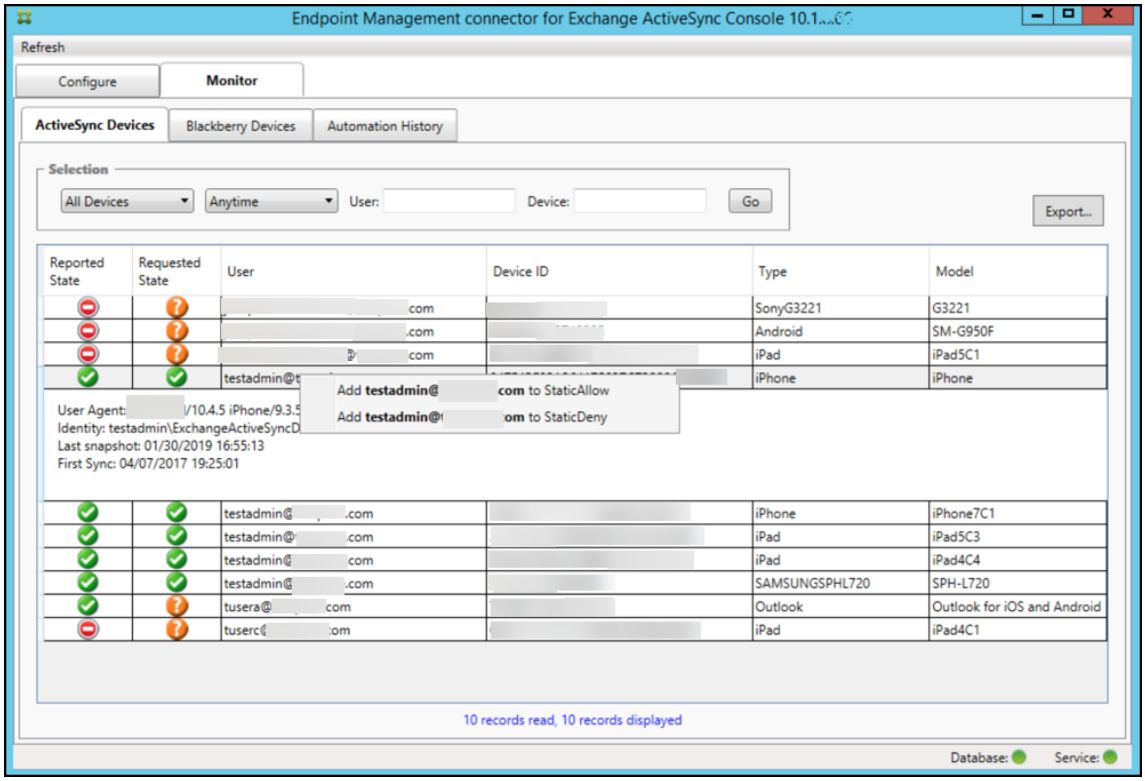


Hinzufügen eines einzelnen Benutzers, eines einzelnen Geräts oder eines einzelnen Gerätetyps zu einer statischen Regel

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 Zulassen oder Verweigern aus.

   Die folgende Abbildung zeigt die Allow-/Deny-Option für user1.



Geräteüberwachung

Die Registerkarte **Monitor** im Endpoint Management Connector für Exchange ActiveSync 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-Geräte**:
  - 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 klicken Sie darauf bei gedrückter Strg-Taste.
- **Blackberry-Geräte**
- **Automation History**

Auf der Registerkarte **Configure** wird der Verlauf aller Snapshots angezeigt. Unter “Snapshot history” wird angezeigt, 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

In folgender Protokolldatei des Endpoint Management-Connectors für Exchange ActiveSync werden Fehler und andere Betriebsinformationen aufgezeichnet: *Install Folder*\log\XmmWindowsService.log. Der Endpoint Management Connector für Exchange ActiveSync protokolliert außerdem wichtige Ereignisse im Windows-Ereignisprotokoll.

Ändern der Protokollierungsstufe

Der Endpoint Management Connector für Exchange ActiveSync enthält die folgenden Protokollierungsstufen: Error, Info, Warn, Debug und Trace.

> **Hinweis:**
>
> Auf jeder Stufe werden mehr Details (mehr Daten) als bei der vorherigen generiert. So bietet die Stufe “Error” die wenigsten und die Stufe “Trace” die meisten Details.

Führen Sie folgende Schritte aus, um die Protokollierungsstufe zu ändern:

1. Öffnen Sie unter C:\Programme\Citrix\Citrix Endpoint Management Connector die Datei nlog.config.
2. Ändern Sie im Abschnitt `<rules>` den Parameter *minilevel* in die gewünschte Protokollierungsstufe. Beispiel:

```
1      <rules>
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. Speichern Sie die Datei.

   Die Änderungen werden sofort wirksam. Sie müssen den Connector für Exchange ActiveSync nicht neu starten.

Häufige Fehler

Beispiele für verbreitete Fehler:

- Der Dienst des Endpoint Management-Connectors für Exchange ActiveSync wird nicht gestartet.

  Prüfen Sie die Protokolldatei und das Windows-Ereignisprotokoll auf Fehler. Typische Ursachen:

  - Der Dienst des Endpoint Management-Connectors für Exchange ActiveSync kann nicht auf den SQL Server zugreifen. 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 des Endpoint Management-Connectors für Exchange ActiveSync als zulässige SQL-Anmeldung konfiguriert sein. Standardmäßig ist das Konto des Diensts des Endpoint Management-Connectors für Exchange ActiveSync 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.

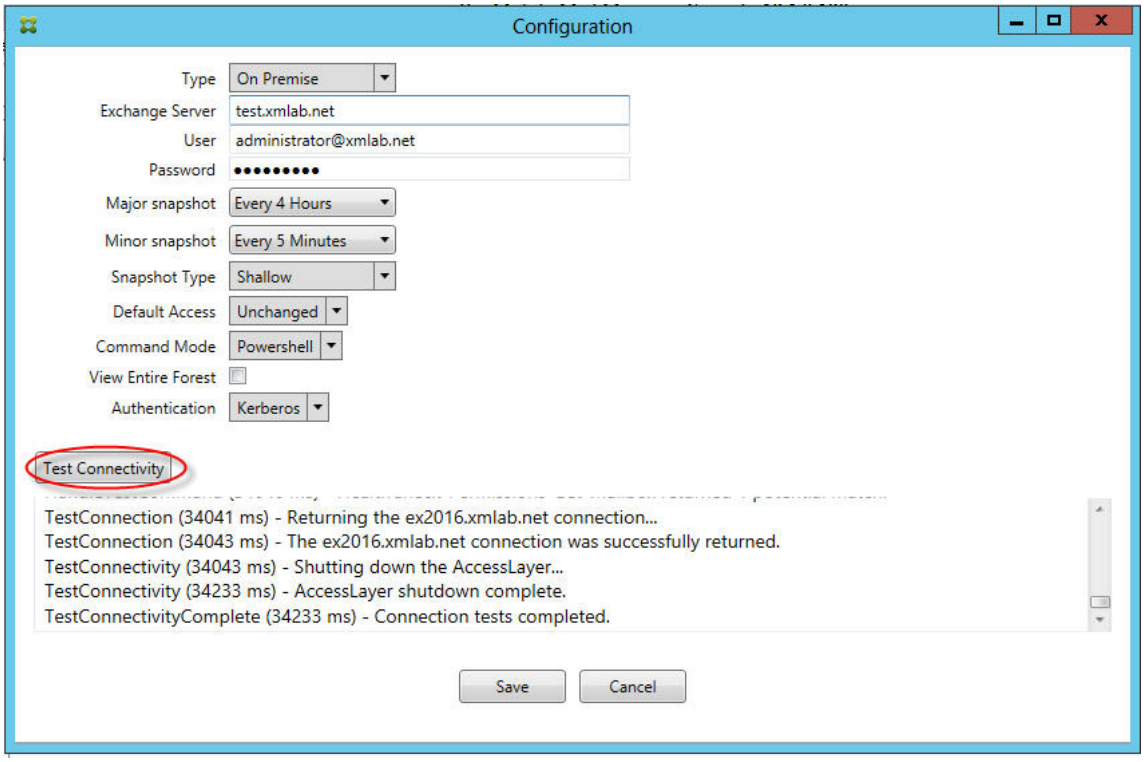
- XenMobile kann keine Verbindung mit dem Mobile Service Provider herstellen

  Stellen Sie auf der Registerkarte **Configure > MSP** der Konsole des Endpoint Management-Connectors für Exchange ActiveSync sicher, dass 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, finden Sie unter How to configure a port with an SSL certificate Anweisungen zur Installation von Zertifikaten.

  Der Endpoint Management Connector für Exchange ActiveSync enthält ein Hilfsprogramm zum Testen der Verbindung mit dem MSP-Dienst. Führen Sie das Programm *Install-Folder*\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 Server ausgehenden Webdienstanfragen. Wenn HTTPS konfiguriert ist, müssen Sie den Hostnamen des Servers (den im SSL-Zertifikat angegebenen Namen) verwenden.

  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.

Citrix Gateway Connector für Exchange ActiveSync

January 5, 2022

XenMobile Citrix ADC Connector ist jetzt der Citrix Gateway Connector für Exchange ActiveSync. Weitere Informationen zum vereinheitlichten Citrix-Portfolio finden Sie im Citrix product name guide.

Der Connector für Exchange ActiveSync bietet einen Authentifizierungsdienst auf Geräteebene für ActiveSync-Clients bei Citrix ADC, der als Reverseproxy für das Exchange ActiveSync-Protokoll fungiert. Die Autorisierung wird durch eine Kombination von Richtlinien, die Sie in XenMobile definieren, und lokal im Citrix Gateway Connector für Exchange ActiveSync definierten Regeln gesteuert.

Weitere Informationen finden Sie unter ActiveSync-Gateway.

Ein detailliertes Architekturdiagramm finden Sie unter Architektur.

Die aktuelle Version von Citrix Gateway Connector für Exchange ActiveSync ist Version 8.5.2.

Neue Features

In den folgenden Abschnitten wird aufgeführt, was in der aktuellen und früheren Versionen des Citrix Gateway-Connectors für Exchange ActiveSync (zuvor "XenMobile Citrix ADC Connector") neu ist.

Neue Features in Version 8.5.3

- Diese Version unterstützt die ActiveSync-Protokolle 16.0 und 16.1.
- Den an Google Analytics gesendeten Analysedaten wurden weitere Details (insbesondere in Bezug auf Snapshots) hinzugefügt. [CXM-52261]

Neue Features in Version 8.5.2

- XenMobile Citrix ADC Connector ist jetzt der Citrix Gateway Connector für Exchange ActiveSync.

Die folgenden Probleme wurden in diesem Release behoben:

- Wenn bei der Definition einer Richtlinienregel mehr als ein Kriterium verwendet wird und eines der Kriterien die Benutzer-ID betrifft, kann das folgende Problem auftreten: Wenn ein Benutzer mehrere Aliasse hat, werden die Aliasse bei der Anwendung der Regel auch nicht überprüft. [CXM-55355]

> **Hinweis:**
>
> Im folgenden "Neue Features"-Abschnitt wird für den Citrix Gateway Connector für Exchange ActiveSync der bisherige Name "XenMobile Citrix ADC Connector" verwendet. Der neue Name gilt ab Version 8.5.2.

Neue Features in Version 8.5.1.11

- **Geänderte Systemanforderungen:** Die aktuelle Version von Citrix ADC Connector erfordert Microsoft .NET Framework 4.5.
- **Unterstützung von Google Analytics:** Wir möchten wissen, wie Sie XenMobile Citrix ADC Connector verwenden, damit wir wissen, wo wir das Produkt verbessern können.
- **Unterstützung für TLS 1.1 und 1.2:** Aufgrund der schwächer werdenden Sicherheit wird TLS 1.0 vom Payment Card Industry Security Standards Council abgelehnt. XenMobile Citrix ADC Connector unterstützt jetzt TLS 1.1 und 1.2.

Citrix Gateway Connector für Exchange ActiveSync überwachen

Das Citrix Gateway Connector für Exchange ActiveSync-Konfigurationsprogramm bietet eine detaillierte Protokollierung, anhand derer Sie den gesamten von Secure Mobile Gateway zugelassenen bzw. blockierten Datenverkehr über den Exchange-Server überwachen können.

Auf der Registerkarte **Protokollierung** wird der Verlauf der von Citrix ADC zur Autorisierung an den Connector für Exchange ActiveSync weitergeleiteten ActiveSync-Anforderungen angezeigt.

Vergewissern Sie sich außerdem, dass der Webdienst des Citrix Gateway-Connectors für Exchange ActiveSync ausgeführt wird, indem Sie die folgende URL in einen Browser auf dem Connector-Server eingeben: `https://<host:port>/services/ActiveSync/Version`. Wird die Produktversion als Zeichenfolge zurückgegeben, wird der Webdienst ausgeführt.

Simulieren des ActiveSync-Datenverkehrs mit dem Citrix Gateway Connector für Exchange ActiveSync

Sie können den Citrix Gateway Connector für Exchange ActiveSync zum Simulieren des ActiveSync-Datenverkehrs gemäß Ihren Richtlinien verwenden. Klicken Sie im Connector-Konfigurationsprogramm auf die Registerkarte **Simulator**. Das Ergebnis zeigt, wie Ihre Richtlinien nach den von Ihnen konfigurierten Regeln angewendet werden.

Auswählen von Filtern für den Citrix Gateway Connector für Exchange ActiveSync

Citrix Gateway Connector für Exchange ActiveSync-Filter analysieren Geräte auf Verstöße gegen bestimmte Richtlinien oder Eigenschaften. Erfüllt ein Gerät die Kriterien, wird es in eine Geräteliste aufgenommen. Diese Geräteliste ist weder eine Liste zum Zulassen oder Blockieren. Es ist lediglich eine Liste der Geräte, die die Kriterien erfüllen. Die folgenden Filter stehen für den Connector in XenMobile zur Verfügung. Die Optionen für jeden Filter sind **Zulassen** oder **Verweigern**.

- **Anonyme Geräte:** dient zum Zulassen oder Blockieren von Geräten, die bei XenMobile registriert sind, bei denen die Identität des Benutzers jedoch unbekannt ist. Beispielsweise kann dies ein registrierter Benutzer sein, dessen Active Directory-Kennwort abgelaufen ist, oder ein Benutzer, der sich mit unbekannten Anmeldeinformationen registriert hat.
- **Samsung KNOX-Nachweisfehler:** Samsung-Geräte besitzen Funktionen für Sicherheit und Diagnose. Dieser Filter erteilt die Bestätigung, dass das Gerät für KNOX eingerichtet ist. Einzelheiten finden Sie unter Samsung Knox.
- **Unzulässige Apps:** Zulassen oder Blockieren von Geräten basierend auf Sperrlistenrichtlinien und dem Vorhandensein gesperrter Apps.
- **Implizit zulassen/verweigern:** erstellt eine Liste aller Geräte, die keines der anderen Filterkriterien erfüllen, und lässt den Zugriff zu bzw. blockiert ihn für diese Geräte. Die Option “Implizit zulassen/verweigern” stellt sicher, dass der Status des Citrix Gateway-Connectors für Exchange

ActiveSync für die Registerkarte “Geräte” aktiviert ist und der Connector-Status für die Geräte angezeigt wird. Die Option “Implizit zulassen/verweigern” steuert auch alle anderen Connector-Filter, die nicht ausgewählt wurden. Der Connector lehnt beispielsweise blockierte Apps ab, alle übrigen Filter werden jedoch zugelassen, da die Option “Implizit zulassen/verweigern” auf **Zulassen** festgelegt ist.

- **Inaktive Geräte:** erstellt eine Liste von Geräten, die innerhalb eines bestimmten Zeitraums nicht mit XenMobile kommuniziert haben. Solche Geräte werden als inaktiv eingestuft. Der Filter lässt die Geräte zu oder verweigert sie entsprechend.
- **Fehlende Pflicht-Apps:** Wenn sich ein Benutzer anmeldet, erhält er eine Liste der erforderlichen Apps, die installiert werden müssen. Der Filter für fehlende Plicht-Apps sucht Apps, die nicht mehr vorhanden sind (beispielsweise, weil sie vom Benutzer gelöscht wurden).
- **Nicht empfohlene Apps:** Wenn sich ein Benutzer anmeldet, erhält er eine Liste der Apps, deren Installation empfohlen wird. Der Filter für nicht empfohlene Apps überprüft das Gerät auf Apps, die nicht auf dieser Liste stehen.
- **Nicht richtlinientreues Kennwort:** erstellt eine Liste aller Geräte ohne Passcode.
- **Nicht richtlinientreue Geräte:** ermöglicht das Zulassen bzw. Blockieren von Geräten auf der Basis der Einhaltung firmeninterner IT-Richtlinien. Die Richtlinientreue ist eine willkürliche Einstellung, die durch die Geräteeigenschaft “Out of Compliance” definiert ist, einem booleschen Flag, das entweder **True** oder **False** sein kann. (Sie können diese Eigenschaft manuell unter Auswahl des Werts erstellen oder mit automatischen Aktionen auf einem Gerät, wenn das Gerät die Kriterien erfüllt bzw. nicht erfüllt.)
  - **Out of Compliance = True:** Wenn ein Gerät die Vorgaben und Richtliniendefinitionen der IT-Abteilung nicht erfüllt, wird das Gerät als nicht richtlinientreu eingestuft.
  - **Out of Compliance = False:** Wenn ein Gerät die Vorgaben und Richtliniendefinitionen der IT-Abteilung erfüllt, wird das Gerät als richtlinientreu eingestuft.
- **Widerrufenstatus:** erstellt eine Liste aller widerrufenen Geräte und lässt den Zugriff zu bzw. blockiert ihn auf der Basis des Gerätestatus.
- **Android-Geräte mit Rooting/iOS-Geräte mit Jailbreak:** erstellt eine Liste aller Geräte, die als gerootet markiert wurden, und lässt den Zugriff zu bzw. blockiert ihn auf der Basis des entsprechenden Gerätestatus.
- **Nicht verwaltete Geräte:** erstellt eine Liste aller Geräte in der XenMobile-Datenbank. Das Mobile Application Gateway muss im Modus “Blockieren” bereitgestellt werden.

Konfigurieren einer Verbindung zum Citrix Gateway Connector für Exchange ActiveSync

Der Citrix Gateway Connector für Exchange ActiveSync kommuniziert mit XenMobile und anderen Remote-Konfigurationsanbietern über sichere Webdienste.

1. Klicken Sie im Connector-Konfigurationsprogramm auf die Registerkarte **Config Providers** und

dann auf **Add**.

2. Geben Sie im Dialogfeld **Config Providers** unter **Name** den Benutzernamen eines Kontos mit Administratorrechten ein, das für die grundlegende HTTP-Autorisierung auf dem XenMobile Server verwendet wird.
3. Geben Sie unter **Url** die Webadresse des XenMobile-GCS (normalerweise im Format `https://<FQDN>/<instanceName>/services/<MagConfigService>`) ein. Bei dem Namen von *MagConfigService* wird die Groß-/Kleinschreibung unterschieden.
4. Geben Sie unter **Password** das Kennwort für die HTTP-Standardauthentifizierung beim XenMobile Server an.
5. Geben Sie unter **Managing Host** den Namen des Servers mit dem Citrix Gateway Connector für Exchange ActiveSync ein.
6. Geben Sie unter **Baseline Interval** das Intervall ein, in dem von Device Manager der aktualisierte Satz dynamischer Regeln abgerufen werden soll.
7. Geben Sie unter **Delta Interval** einen Zeitraum für den Abruf aktualisierter dynamischer Regeln ein.
8. Geben Sie unter **Request Timeout** das Timeoutintervall für die Serveranforderungen an.
9. Wählen Sie unter **Config Provider**, ob die Serverinstanz des Konfigurationsanbieters die Richtlinienkonfiguration bereitstellt.
10. Aktivieren Sie diese Option unter **Events Enabled**, wenn der Citrix Gateway Connector für Exchange ActiveSync die Blockierung eines Geräts an XenMobile melden soll. Die Option ist erforderlich, wenn Sie Regeln des Citrix Gateway-Connectors für Exchange ActiveSync in XenMobile für eine automatische Aktion verwenden.
11. Klicken Sie auf **Save** und dann auf **Test Connectivity**, um die Verbindung zwischen Gateway und Konfigurationsanbieter zu testen. Wenn die Verbindung fehlschlägt, überprüfen Sie, ob die lokalen Firewalleinstellungen die Verbindung gestatten, oder wenden Sie sich an den Administrator.
12. Wenn die Verbindung erfolgreich ist, deaktivieren Sie das Kontrollkästchen **Disabled** und klicken Sie auf **Save**.

Wenn Sie einen neuen Konfigurationsanbieter hinzufügen, erstellt der Citrix Gateway Connector für Exchange ActiveSync automatisch eine oder mehrere diesem Anbieter zugeordnete Richtlinien. Diese Richtlinien werden durch eine Vorlagendefinition im Abschnitt “NewPolicyTemplate” der Datei config\policyTemplates.xml festgelegt. Für jedes Policy-Element in diesem Abschnitt wird eine neue Richtlinie erstellt.

Policy-Elemente können hinzugefügt, entfernt oder modifiziert werden, wenn folgende Voraussetzungen erfüllt sind: Das Policy-Element entspricht der Schemadefinition und die Standard-Ersatzzeichenfolgen (in geschweiften Klammern) werden nicht geändert. Fügen Sie als Nächstes neue Gruppen für den Anbieter hinzu und aktualisieren Sie die Richtlinie zur Berücksichtigung der neuen Gruppen.

Importieren einer Richtlinie aus XenMobile

1. Klicken Sie im Konfigurationsprogramm des Citrix Gateway-Connectors für Exchange ActiveSync auf die Registerkarte **Config Providers** und dann auf **Add**.
2. Geben Sie im Dialogfeld **Config Providers** unter **Name** den Benutzernamen eines Kontos mit Administratorrechten ein, das für die grundlegende HTTP-Autorisierung auf dem XenMobile Server verwendet werden soll.
3. Geben Sie unter **Url** die Webadresse von XenMobile Gateway Configuration Service (normalerweise im Format `https://<xdmHost>/xdm/services/<MagConfigService>`) ein. Bei dem Namen von MagConfigService wird die Groß-/Kleinschreibung unterschieden.
4. Geben Sie unter **Password** das Kennwort für die HTTP-Standardauthentifizierung beim XenMobile Server an.
5. Klicken Sie auf **Test Connectivity**, um die Verbindung zwischen Gateway und Konfigurationsanbieter zu testen. Wenn die Verbindung fehlschlägt, überprüfen Sie, ob die lokalen Firewalleinstellungen die Verbindung gestatten, oder wenden Sie sich an den Administrator.
6. Wenn die Verbindung erfolgreich ist, deaktivieren Sie das Kontrollkästchen **Disabled** und klicken Sie auf **Save**.
7. Behalten Sie unter **Managing Host** den Standard-DNS-Namen des lokalen Hostcomputers bei. Diese Einstellung wird für die Koordination der Kommunikation mit XenMobile verwendet, wenn mehrere Forefront Threat Management Gateway-Server in einem Array konfiguriert sind.

   Nach dem Speichern der Einstellungen öffnen Sie Gateway Configuration Service.

Konfigurieren des Richtlinienmodus des Citrix Gateway-Connectors für Exchange ActiveSync

Der Citrix Gateway Connector für Exchange ActiveSync kann in folgenden sechs Modi ausgeführt werden:

- **Allow All**: In diesem Richtlinienmodus erhält der gesamte Datenverkehr, der den Citrix Gateway Connector für Exchange ActiveSync passiert, Zugriff. Es werden keine anderen Filterregeln verwendet.
- **Deny All**: In diesem Richtlinienmodus wird der gesamte Datenverkehr, der den Citrix Gateway Connector für Exchange ActiveSync passiert, blockiert. Es werden keine anderen Filterregeln verwendet.
- **Static Rules: Block Mode**: In diesem Richtlinienmodus werden statische Regeln mit einer impliziten Blockieren-Anweisung am Ende ausgeführt. Der Connector blockiert Geräte, die nicht über andere Filterregeln zugelassen werden.

- **Static Rules: Permit Mode**: In diesem Richtlinienmodus werden statische Regeln mit einer impliziten Zulassen-Anweisung am Ende ausgeführt. Geräte, die nicht über andere Filterregeln blockiert werden, werden von dem Connector zugelassen.
- **Static + ZDM Rules**: Block Mode: In diesem Richtlinienmodus werden statische Regeln und anschließend dynamische Regeln von XenMobile mit einer impliziten Blockieren-Anweisung am Ende ausgeführt. Geräte werden basierend auf Filtern und Device Manager-Regeln zugelassen oder blockiert. Alle Geräte, die keinem Filter und keiner Regel entsprechen, werden blockiert.
- **Static + ZDM Rules**: Permit Mode: In diesem Richtlinienmodus werden statische Regeln und anschließend dynamische Regeln von XenMobile mit einer impliziten Zulassen-Anweisung am Ende ausgeführt. Geräte werden basierend auf Filtern und XenMobile-Regeln zugelassen oder blockiert. Alle Geräte, die keinem Filter und keiner Regel entsprechen, werden zugelassen.

Das Ausführen dynamischer Regeln durch den Citrix Gateway Connector für Exchange ActiveSync-Prozess basiert auf eindeutigen ActiveSync-Kennungen von iOS- und Windows-Mobilgeräten, die von XenMobile empfangen werden. Bei Android-Geräten ist das Verhalten je nach Hersteller unterschiedlich, einige stellen ihre eindeutige ActiveSync-ID nicht einfach zur Verfügung. Ersatzweise sendet XenMobile für Android-Geräte die Benutzer-ID, damit eine Entscheidung über Zulassen und Blockieren getroffen werden kann. Hat ein Benutzer nur ein Android-Gerät, funktioniert die Zugriffssteuerung daher ordnungsgemäß. Hat ein Benutzer mehrere Android-Geräte, werden alle Geräte zugelassen, da Android-Geräte nicht einzeln unterschieden werden können. Sie können festlegen, dass diese Geräte vom Gateway nach ActiveSync-ID statisch blockiert werden, sofern sie bekannt sind. Sie können das Gateway auch so konfigurieren, dass Geräte nach Gerätetyp oder Benutzeragent blockiert werden.

Zum Festlegen des Richtlinienmodus führen Sie im Konfigurationsprogramm des SMG-Controllers folgende Schritte aus:

1. Klicken Sie auf die Registerkarte **Path Filters** und dann auf **Add**.
2. Wählen Sie im Dialogfeld **Path Properties** aus der Liste **Policy** einen Richtlinienmodus aus und klicken Sie auf **Save**.

Sie können Regeln auf der Registerkarte **Policies** des Konfigurationsprogramms prüfen. Die Regeln werden vom Citrix Gateway Connector für Exchange ActiveSync in der Reihenfolge von oben nach unten verarbeitet. Die Richtlinien zum Zulassen werden mit einem grünen Häkchen angezeigt. Die Richtlinien zum Verweigern werden mit einem durchgestrichenen roten Kreis angezeigt. Zum Aktualisieren der Anzeige der Regeln klicken Sie auf **Refresh**. Sie können die Reihenfolge der Regeln auch in der Datei config.xml ändern.

Zum Testen von Regeln klicken Sie auf die Registerkarte **Simulator**. Geben Sie Werte in den Feldern ein. Diese können auch aus den Protokollen bezogen werden. In einer Ergebnismeldung wird “Allow” oder “Block” angezeigt.

Konfigurieren von statischen Regeln

Geben Sie statische Regeln mit Werten ein, die von dem ISAPI-Filter der HTTP-Anforderungen der ActiveSync-Verbindung gelesen werden. Über statische Regeln kann der Citrix Gateway Connector für Exchange ActiveSync den Datenverkehr basierend auf folgenden Kriterien zulassen oder blockieren:

- **User:** Der Citrix Gateway Connector für Exchange ActiveSync verwendet die bei der Geräteregistrierung erfasste Struktur aus autorisiertem Benutzerwert und Namen. Dies ist normalerweise “domain\username” gemäß Verweis des Servers mit XenMobile, der mit Active Directory über LDAP verbunden ist. Auf der Registerkarte **Protokollierung** des Connector-Konfigurationsprogramms werden die durch den Connector gesendeten Werte angezeigt. Die Werte werden gesendet, wenn die Wertstruktur ermittelt werden muss oder wenn sie sich unterscheidet.
- **Deviceid (ActiveSyncID):** Wird auch als “ActiveSyncID” des verbundenen Geräts bezeichnet. Dieser Wert ist häufig auf der spezifischen Geräteeigenschaftenseite der XenMobile-Konsole. Er kann auch auf der Registerkarte Log des Konfigurationsprogramms für den Citrix Gateway Connector für Exchange ActiveSync ermittelt werden.
- **DeviceType:** Der Connector kann feststellen, ob es sich bei einem Gerät um ein iPhone, iPad oder einen anderen Gerätetyp handelt, und Geräte basierend auf diesem Kriterium blockieren oder zulassen. Wie bei anderen Werten kann Konfigurationsprogramm des Citrix Gateway-Connectors für Exchange ActiveSync alle verbundenen Gerätetypen, die für die ActiveSync-Verbindung verarbeitet werden, anzeigen.
- **UserAgent:** Enthält Informationen zu dem verwendeten ActiveSync-Client. Meist entspricht der Wert einem bestimmten Betriebssystem-Build-/Versionspaar für die Mobilgeräteplattform.

Das Connector-Konfigurationsprogramm, das auf dem Server ausgeführt wird, verwaltet immer die statischen Regeln.

1. Klicken Sie im Konfigurationsprogramm des Secure Mobile Gateway-Controllers auf die Registerkarte **Static Rules** und dann auf **Add**.
2. Legen Sie im Dialogfeld **Static Rule Properties** die Werte fest, die Sie als Kriterien verwenden möchten. Beispiel: Um einen Benutzer für den Zugriff zuzulassen, geben Sie dessen Benutzernamen ein (z. B. AllowedUser) und deaktivieren Sie dann das Kontrollkästchen **Disabled**.
3. Klicken Sie auf **Speichern**.

   Die statische Regel ist jetzt in Kraft. Zusätzlich können Sie reguläre Ausdrücke zum Definieren von Werten verwenden, Sie müssen jedoch den Regelverarbeitungsmodus in der Datei config.xml aktivieren.

Konfigurieren von dynamischen Regeln

Dynamische Regeln werden über Geräterichtlinien und -eigenschaften in XenMobile definiert und können einen dynamischen Citrix Gateway Connector für Exchange ActiveSync-Filter auslösen. Die Filter werden bei einem Verstoß gegen eine Richtlinie oder Eigenschaft ausgelöst. Die Connector-Filter analysieren Geräte auf Verstöße gegen bestimmte Richtlinien oder Eigenschaften. Erfüllt ein Gerät die Kriterien, wird es in eine Geräteliste aufgenommen. Diese Geräteliste ist weder eine Liste zum Zulassen oder zum Blockieren. Es ist lediglich eine Liste der Geräte, die die Kriterien erfüllen. Über die folgenden Konfigurationsoptionen können Sie mithilfe des Connectors festlegen, ob die Geräte in der Geräteliste zugelassen oder blockiert werden sollen.

> **Hinweis:**
>
> Sie müssen die XenMobile-Konsole verwenden, um dynamische Regeln zu konfigurieren.

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. Nur Android: Klicken Sie unter **Send Android domain users to ActiveSync Gateway** auf **YES**, um sicherzustellen, dass XenMobile Android-Geräteinformationen an das Secure Mobile Gateway sendet.

   Wenn diese Option aktiviert ist, sendet XenMobile Android-Geräteinformationen an den Citrix Gateway Connector für Exchange ActiveSync, wenn XenMobile keine ActiveSync-ID für den Android-Gerätebenutzer hat.

Konfigurieren benutzerdefinierter Richtlinien mithilfe der XML-Datei des Citrix Gateway-Connectors für Exchange ActiveSync

Sie können die grundlegenden Richtlinien der Standardkonfiguration auf der Registerkarte **Richtlinien** des Konfigurationsprogramms des Citrix Gateway Connectors für Exchange ActiveSync anzeigen. Zum Erstellen benutzerdefinierter Richtlinien können Sie die XML-Konfigurationsdatei des Connectors (config\config.xml) bearbeiten.

1. Suchen Sie in der Datei den Abschnitt **PolicyList** und fügen Sie diesem ein neues **Policy**-Element hinzu.
2. Wenn eine neue Gruppe erforderlich wird, z. B. eine zusätzliche statische Gruppe oder eine Gruppe für eine zusätzliche GCP, fügen Sie das neue **Group**-Element dem Abschnitt **GroupList** hinzu.

3. Falls gewünscht, können Sie die Reihenfolge der Gruppen in einer vorhandenen Richtlinie durch Umstellen der **GroupRef**-Elemente ändern.

Konfigurieren der XML-Datei des Citrix Gateway-Connectors für Exchange ActiveSync

Die Aktionen des Citrix Gateway-Connectors für Exchange ActiveSync werden über eine XML-Konfigurationsdatei vorgegeben. Unter anderem enthält die Datei die Dateigruppe und zugehörige Aktionen für den Filter bei der Auswertung von HTTP-Anforderungen. Standardmäßig heißt die Datei config.xml und ist im Verzeichnis \Programme\Citrix\XenMobile Citrix ADC Connector\config.

GroupRef-Knoten

Die GroupRef-Knoten definieren die logischen Gruppennamen. Die Standardwerte sind “AllowGroup” und “DenyGroup”.

> **Hinweis:**
>
> Die Reihenfolge der GroupRef-Knoten im GroupRefList-Knoten spielt eine Rolle.

Der ID-Wert eines GroupRef-Knotens identifiziert einen logischen Container bzw. eine Mitgliedersammlung, der bzw. die für die Zuordnung spezifischer Benutzerkonten oder Geräte verwendet wird. Die Action-Attribute geben an, wie ein Mitglied zu behandeln ist, das einer Regel in der Sammlung entspricht. Beispielsweise wird ein Benutzerkonto oder Gerät, das einer AllowGroup-Regel entspricht, zugelassen. Dies bedeutet, es erhält Zugriff auf den Exchange-Clientzugriffsserver. Ein Benutzerkonto oder Gerät, das einer DenyGroup-Regel entspricht, wird abgelehnt. Dies bedeutet, es erhält keinen Zugriff auf den Exchange-Clientzugriffsserver.

Entspricht ein bestimmtes Benutzerkonto/Gerät oder eine Konto-/Gerätekombination Regeln beider Gruppen, erfolgt die Behandlung gemäß einer Rangfolgenkonvention. Die Rangfolge entspricht der Reihenfolge der GroupRef-Knoten in der Datei config.xml von oben nach unten. Die GroupRef-Knoten werden nach Priorität gewichtet. Regeln für eine bestimmte Bedingung in der Allow-Gruppe haben immer Vorrang vor Regeln für die gleiche Bedingung in Deny-Gruppe.

Gruppenknoten

In der Datei config.xml sind außerdem Gruppenknoten definiert. Diese Knoten verknüpfen die logischen Container “AllowGroup” und “DenyGroup” mit externen XML-Dateien. Einträge in den externen Dateien bilden die Basis für die Filterregeln.

> **Hinweis:**
>
> In diesem Release werden nur externe XML-Dateien unterstützt.

In der Standardinstallation sind zwei XML-Dateien in der Konfiguration implementiert: allow.xml und deny.xml.

Konfigurieren des Citrix Gateway-Connectors für Exchange ActiveSync

Sie können den Citrix Gateway Connector für Exchange ActiveSync so konfigurieren, dass ActiveSync-Anforderungen basierend auf den folgenden Eigenschaften selektiv blockiert oder zugelassen werden: **ActiveSync Service ID**, **Device type**, **User Agent** (Geräte-OS), **Authorized user** und **ActiveSync Command**.

Die Standardkonfiguration unterstützt eine Kombination aus statischen und dynamischen Gruppen. Statische Gruppen werden mit dem Konfigurationsprogramm des Secure Mobile Gateway-Controllers verwaltet. Statische Gruppen können aus bekannten Gerätekategorien bestehen, z. B. alle Geräte mit einem bestimmten Benutzer-Agent.

Dynamische Gruppen werden von einer externen Quelle, dem Gateway-Konfigurationsanbieter, gepflegt. Der Citrix Gateway Connector für Exchange ActiveSync verbindet die Gruppen regelmäßig. XenMobile kann Gruppen zugelassener und blockierter Geräte und Benutzer in den Connector exportieren.

Dynamische Gruppen werden von einer externen Quelle, dem Gateway-Konfigurationsanbieter, gepflegt und regelmäßig von dem Citrix Gateway Connector für Exchange ActiveSync gesammelt. XenMobile kann Gruppen zugelassener und blockierter Geräte und Benutzer in den Connector exportieren.

Eine Richtlinie ist eine sortierte Liste von Gruppen, in der jeder Gruppe eine Aktion (zulassen oder blockieren) zugeordnet ist, und eine Liste der Gruppenmitglieder. Eine Richtlinie kann beliebig viele Gruppen enthalten. Die Reihenfolge der Gruppen in einer Richtlinie ist wichtig, weil bei einer Übereinstimmung die Aktion der Gruppe erfolgt und nachfolgende Gruppen nicht ausgewertet werden.

Mitglieder sind eine Methode für die Zuordnung der Eigenschaften einer Anforderung. Sie können einer einzelnen Eigenschaft (z. B. Geräte-ID) oder mehreren Eigenschaften entsprechen (z. B. Gerätetyp und Benutzer-Agent).

Auswählen eines Sicherheitsmodells für den Citrix Gateway Connector für Exchange ActiveSync

Die Implementierung eines Sicherheitsmodells ist für eine erfolgreiche Mobilgerätebereitstellung in Organisationen jeder Größe wichtig. Häufig wird eine Netzwerksteuerung mit Schutz oder Quarantäne verwendet, um den Zugriff auf Benutzer, Computer oder Geräte standardmäßig zuzulassen. Dieses Verfahren ist jedoch nicht immer ideal. In jeder Organisation werden bei der Verwaltung der IT-Sicherheit andere ggf. maßgeschneiderte Methoden zum Schutz von Mobilgeräten eingesetzt.

Die gleiche Logik gilt für die Sicherheit von Mobilgeräten. Angesichts der Vielzahl verschiedener Mobilgerätetypen, der großen Zahl Mobilgeräte pro Benutzer und der Vielfalt an Betriebssystemen und Apps ist das permissive Modell keine gute Wahl. In den meisten Organisationen ist das restriktive Modell die beste Wahl.

Citrix lässt bei der Integration des Citrix Gateway-Connectors für Exchange ActiveSync in XenMobile folgende Konfigurationsszenarios zu:

Permissives Modell (Zulassungsmodus)

Beim permissiven Sicherheitsmodell gilt, dass bei allem der Zugriff standardmäßig zugelassen ist. Nur durch Einsatz von Regeln und Filtern können Elemente blockiert und Beschränkungen angewendet werden. Das permissive Sicherheitsmodell ist für Organisationen geeignet, in denen keine strengen Sicherheitsvorschriften hinsichtlich der Mobilgeräte herrschen. Bei diesem Modell wird der Zugriff nur dann verweigert, wenn eine Richtlinienregel verletzt wurde.

Restriktives Modell (Blockierungsmodus)

Beim restriktiven Sicherheitsmodell gilt, dass bei nichts der Zugriff standardmäßig zugelassen ist. Alle Elemente werden bei der Sicherheitsprüfung gefiltert und untersucht. Der Zugriff wird blockiert, außer wenn die Regeln für die Zulassung des Zugriffs erfüllt werden. Das restriktive Sicherheitsmodell ist für Organisationen geeignet, in denen relativ strenge Sicherheitsvorschriften hinsichtlich der Mobilgeräte herrschen. Bei diesem Modell wird der Zugriff nur gewährt, wenn alle Regeln für das Zulassen des Zugriffs erfüllt werden.

Verwalten des Citrix Gateway-Connectors für Exchange ActiveSync

Sie können unter Einsatz des Citrix Gateway-Connectors für Exchange ActiveSync Zugriffsregeln erstellen. Mit diesen Regeln wird der Zugriff verwalteter Geräte auf ActiveSync-Verbindungsanforderungen zugelassen oder blockiert. Der Zugriff basiert auf Gerätestatus, App-Sperrlisten bzw. App-Positivlisten und anderen Vorgaben zur Richtlinientreue.

Mit dem Konfigurationsprogramm des Citrix Gateway-Connectors für Exchange ActiveSync können Sie dynamische und statische Regeln zum Erzwingen von Richtlinien für E-Mail erstellen, mit denen Benutzer, die die Richtlinien nicht einhalten, blockiert werden. Sie können außerdem die Verschlüsselung von E-Mail-Anlagen einrichten, sodass alle Anlagen, die über Exchange Server an verwaltete Geräte gesendet werden, verschlüsselt werden und nur von autorisierten Benutzern auf verwalteten Geräten angezeigt werden können.

Deinstallieren des Citrix Gateway-Connectors für Exchange ActiveSync

1. Führen Sie XncInstaller.exe als Administrator aus.
2. Folgen Sie den Anweisungen zum Durchführen der Deinstallation.

Installieren, Aktualisieren oder Deinstallieren des Citrix Gateway-Connectors für Exchange ActiveSync

1. Führen Sie XncInstaller.exe als Administrator aus, um den Connector zu installieren bzw. vorhandene Versionen zu aktualisieren oder zu deinstallieren.
2. Folgen Sie den angezeigten Anweisungen, um die Installation, das Upgrade oder die Deinstallation durchzuführen.

Nach der Installation des Connectors müssen Sie den XenMobile-Konfigurationsdienst und den Benachrichtigungsdienst manuell neu starten.

Installieren des Citrix Gateway-Connectors für Exchange ActiveSync

Sie installieren den Citrix Gateway Connector für Exchange ActiveSync auf einem eigenen Windows Server.

Die CPU-Last, die der Connector einem Server zuweist, hängt von der Anzahl der verwalteten Geräte ab. Bei hohen Gerätezahlen (über 50.000) müssen Sie möglicherweise mehrere Kerne bereitstellen, wenn Sie keine Clusterumgebung haben. Der Speicherbedarf des Connectors ist so gering, dass kein zusätzlicher Speicher erforderlich ist.

Systemanforderungen für den Citrix Gateway Connector für Exchange ActiveSync

Der Citrix Gateway Connector für Exchange ActiveSync kommuniziert mit Citrix ADC über eine auf dem Citrix ADC-Gerät konfigurierte SSL-Brücke. Über diese Brücke kann das Gerät sämtlichen sicheren Datenverkehr direkt an XenMobile übergeben. Der Connector erfordert die folgende Mindestsystemkonfiguration:

Komponente	Voraussetzung
Computer und Prozessor	Pentium III-Prozessor, 733 MHz oder schneller; empfohlen: Pentium III-Prozessor, 2.0 GHz oder schneller
Citrix ADC	Citrix ADC-Gerät mit Softwareversion 10
Speicher	1 GB
Festplatte	NTFS-formatierte lokale Partition mit 150 MB freiem Speicherplatz

Komponente	Voraussetzung
Betriebssystem	Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2008 R2 Service Pack 1. Muss ein englischbasierter Server sein. Die Unterstützung für Windows Server 2008 R2 Service Pack 1 endet am 14. Januar 2020.
Sonstige Geräte	Mit dem Hostbetriebssystem kompatibler Netzwerkadapter für die Kommunikation mit dem internen Netzwerk
Microsoft .NET Framework	Version 8.5.1.11 erfordert Microsoft .NET Framework 4.5.
Anzeigen	VGA-Monitor oder höher

Auf dem Hostcomputer für den Citrix Gateway-Connector für Exchange ActiveSync ist mindestens folgender freier Festplattenspeicher erforderlich:

- **Anwendung:** 10–15 MB (100 MB empfohlen)
- **Protokollierung:** 1 GB (20 GB empfohlen)

Informationen über die vom Citrix Gateway Connector für Exchange ActiveSync unterstützten Plattformen finden Sie unter Unterstützte Gerätebetriebssysteme.

Geräte-E-Mail-Clients

Nicht alle E-Mail-Clients geben konstant dieselbe ActiveSync-ID für das Gerät zurück. Da der Citrix Gateway Connector für Exchange ActiveSync 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 ordnungsgemäß:

- Samsung-nativer E-Mail-Client
- iOS-nativer E-Mail-Client

Bereitstellen des Citrix Gateway-Connectors für Exchange ActiveSync

Mit dem Citrix Gateway Connector für Exchange ActiveSync können Sie Citrix ADC als Proxy und für den Lastausgleich bei der Kommunikation zwischen XenMobile Server und mit XenMobile verwalteten Geräten verwenden. Der Connector kommuniziert in regelmäßigen Abständen mit XenMobile zur Synchronisierung von Richtlinien. Der Connector und XenMobile lassen sich zusammen oder separat in Clustern zusammenfassen. Ein Lastausgleich ist mit Citrix ADC möglich.

Komponenten des Citrix Gateway-Connectors für Exchange ActiveSync

- **Citrix Gateway-Connector für Exchange ActiveSync-Dienst:** Dieser Dienst bietet eine REST-Webdienstschnittstelle, die von Citrix ADC aufgerufen werden kann, um zu ermitteln, ob eine ActiveSync-Anforderung von einem Gerät autorisiert ist.
- **XenMobile-Konfigurationsdienst:** Dieser Dienst kommuniziert mit XenMobile zur Synchronisierung von XenMobile-Richtlinienänderungen mit dem Connector.
- **XenMobile-Benachrichtigungsdienst:** Dieser Dienst sendet Benachrichtigungen über unautorisierten Gerätezugriff an XenMobile. XenMobile kann dann die nötigen Schritte ergreifen und beispielsweise den Benutzer benachrichtigen, warum sein Gerät blockiert wurde.
- **Citrix Gateway Connector für Exchange ActiveSync-Konfigurationshilfsprogramm:** Mit dieser Anwendung kann der Administrator den Connector für konfigurieren und überwachen.

Einrichten von Überwachungsadressen für den Citrix Gateway Connector für Exchange ActiveSync

Führen Sie folgende Schritte aus, damit der Citrix Gateway Connector für Exchange ActiveSync Anforderungen von Citrix ADC zur Autorisierung von ActiveSync-Datenverkehr empfangen kann. Geben Sie den Port an, den der Connector auf Aufrufe des Citrix ADC-Webdiensts überwacht.

1. Wählen Sie im Menü **Start** das Konfigurationshilfsprogramm des Citrix Gateway-Connectors für Exchange ActiveSync aus.
2. Klicken Sie auf die Registerkarte **Web Service**, und geben Sie die zu überwachenden Adressen für den Connector-Webdienst ein. Sie können **HTTP** und/oder **HTTPS** auswählen. Residiert der Connector auf dem gleichen Server wie XenMobile, wählen Sie Ports aus, die keinen Konflikt mit denen von XenMobile auslösen.
3. Wenn die Werte konfiguriert sind, klicken Sie auf **Save** und dann auf **Start Service**, um den Webdienst zu starten.

Konfigurieren von Zugriffssteuerungsrichtlinien im Citrix Gateway Connector für Exchange ActiveSync

Zum Konfigurieren einer Zugriffssteuerungsrichtlinie für verwaltete Geräte gehen Sie folgendermaßen vor:

1. Klicken Sie im Konfigurationsprogramm des Citrix Gateway-Connectors für Exchange ActiveSync auf die Registerkarte **Path Filters**.
2. Wählen Sie die erste Zeile **Microsoft-Server-ActiveSync is for ActiveSync** und klicken Sie auf **Edit**.
3. Wählen Sie in der Liste **Policy** die gewünschte Richtlinie aus. Bei Richtlinien, die XenMobile-Richtlinien umfassen, wählen Sie **Static + ZDM: Permit Mode oder Static + ZDM: Block Mode**. Diese Richtlinien kombinieren lokale (statische) Regeln mit denen von XenMobile. Permit Mode

bedeutet, dass alle Geräte, die nicht explizit durch die Regeln identifiziert werden, Zugriff auf ActiveSync erhalten. Block Mode bedeutet, dass solche Geräte blockiert werden.

4. Klicken Sie nach dem Festlegen der Richtlinien auf **Save**.

Konfigurieren der Kommunikation mit XenMobile

Geben Sie Namen und Eigenschaften des XenMobile-Servers (= "Config Provider") an, den Sie mit dem Citrix Gateway Connector für Exchange ActiveSync und Citrix ADC verwenden möchten.

> **Hinweis:**
>
> Es wird davon ausgegangen, dass Sie XenMobile bereits installiert und konfiguriert haben.

1. Klicken Sie im Konfigurationsprogramm des Citrix Gateway-Connectors für Exchange ActiveSync auf die Registerkarte **Config Providers** und dann auf **Add**.
2. Geben Sie den Namen und die URL des XenMobile Servers ein, den Sie in der Bereitstellung verwenden. Wenn Sie mehrere XenMobile Server in einer Bereitstellung mit mehreren Mandanten haben, muss der Name für jede Serverinstanz eindeutig sein. Geben Sie unter **Name** beispielsweise **XMS** ein.
3. Geben Sie unter **Url** die Webadresse von XenMobile GlobalConfig Provider (normalerweise im Format `https://<FQDN>/<instanceName>/services/<MagConfigService>`) ein. Bei dem Namen von *MagConfigService* wird die Groß-/Kleinschreibung unterschieden.
4. Geben Sie unter **Password** das Kennwort für die HTTP-Standardauthentifizierung beim XenMobile-Webserver an.
5. Geben Sie unter **Managing Host** den Namen des Servers an, auf dem Sie den Citrix Gateway Connector für Exchange ActiveSync installiert haben.
6. Geben Sie unter **Baseline Interval** das Intervall ein, in dem von XenMobile der aktualisierte Satz dynamischer Regeln abgerufen werden soll.
7. Geben Sie unter **Request Timeout** das Timeoutintervall für die Serveranforderungen an.
8. Wählen Sie unter **Config Provider**, ob die Serverinstanz des Konfigurationsanbieters die Richtlinienkonfiguration bereitstellt.
9. Aktivieren Sie die Option unter **Events Enabled**, wenn Secure Mobile Gateway die Blockierung eines Geräts an XenMobile melden soll. Die Option ist erforderlich, wenn Sie Secure Mobile Gateway-Regeln in Device Manager für eine automatische Aktion verwenden.
10. Klicken Sie nach Abschluss der Konfiguration des Servers auf **Test Connectivity**, um die Verbindung mit XenMobile zu testen.
11. Wenn die Verbindung hergestellt wird, klicken Sie auf **Save**.

Bereitstellen des Citrix Gateway-Connectors für Exchange ActiveSync für Redundanz und Skalierbarkeit

Wenn Sie Ihre Bereitstellung des Citrix Gateway-Connectors für Exchange ActiveSync und von XenMobile skalieren möchten, installieren Sie Instanzen des Connectors auf mehreren Windows-Servern, die alle auf die gleiche XenMobile-Instanz verweisen, und führen Sie dann einen Lastausgleich der Server mit Citrix ADC aus.

Es gibt zwei Modi zur Konfiguration des Citrix Gateway-Connectors für Exchange ActiveSync:

- Im Modus ohne Freigabe kommuniziert jede Instanz des Citrix Gateway-Connectors für Exchange ActiveSync mit einem XenMobile-Server und speichert eine eigene Kopie der daraus resultierenden Richtlinie. Beispiel: In einem XenMobile-Servercluster können Sie eine Connector-Instanz auf jedem XenMobile-Server ausführen. Der Connector erhält dann Richtlinien von der lokalen XenMobile-Instanz.
- In Modus mit Freigabe wird ein Knoten mit dem Citrix Gateway Connector für Exchange ActiveSync als primärer Knoten festgelegt, der mit XenMobile kommuniziert. Die resultierende Konfiguration wird dann per Windows-Netzwerkfreigabe oder per Windows-Replikation (bzw. per Drittanbieter-Replikation) an die anderen Knoten weitergegeben.

Die Connector-Konfiguration (bestehend aus einigen XML-Dateien) ist in einem einzigen Ordner. Der Connector-Prozess erkennt Änderungen an jeder Datei in diesem Ordner und lädt die Konfiguration dann automatisch neu. Im Modus mit Freigabe gibt kein Failover für den primären Knoten. Bei einem Ausfall des primären Servers (z. B. durch Neustart) besteht jedoch einige Minuten lang Fehlertoleranz, da die letzte funktionsfähige Konfiguration im Connector-Prozess zwischengespeichert ist.

Erweiterte Konzepte

January 5, 2022

> **Hinweis:**
>
> In diesem Artikel werden erweiterte Konzepte von XenMobile Server behandelt. Weitere Informationen zu Endpoint Management finden Sie unter Erweiterte Konzepte.

Die Artikel zu erweiterten Konzepten bieten einen tieferen Einblick in die Produktdokumentation zu XenMobile. Behandelt werden Profitechniken, welche den Zeitaufwand für die Bereitstellung verringern sollen. In den Artikeln werden ggf. die Experten zitiert, die den Inhalt verfasst haben.

Entscheidungshilfen, Empfehlungen, Antworten auf allgemeine Fragen sowie Anwendungsfälle für XenMobile finden Sie im Bereitstellungshandbuch von XenMobile in diesem Abschnitt.

Foren für den Community-Support für XenMobile finden Sie unter Citrix Discussions.

Interaktion von lokal installiertem XenMobile mit Active Directory

January 5, 2022

Beitrag von Siddartha Vuppala

In diesem Artikel wird erläutert, auf welche Weise XenMobile Server mit Active Directory interagiert. Die Interaktion zwischen XenMobile Server und Active Directory erfolgt sowohl Inline als auch im Hintergrund. Die folgenden Abschnitte enthalten weitere Informationen zu Inline- und Hintergrundprozessen, die bei der Interaktion mit Active Directory ablaufen.

> **Hinweis:**
>
> Dieser Artikel bietet einen Überblick und beschreibt die Interaktionen nicht in jedem Detail. Weitere Informationen zum Konfigurieren von Active Directory und LDAP in der XenMobile-Konsole finden Sie unter Authentifizierung mit Domäne oder mit Domäne und Sicherheitstoken.

Inline-Interaktionen

Die Kommunikation zwischen XenMobile Server und Active Directory erfolgt über die vom Administrator konfigurierten LDAP-Einstellungen. Die Einstellungen dienen zum Abrufen von Informationen über Benutzer und Gruppen. Die folgenden Vorgänge führen zu einer Interaktion zwischen XenMobile Server und Active Directory.

1. **LDAP-Konfiguration.** Die Konfiguration von Active Directory führt selbst zu einer Interaktion mit Active Directory. XenMobile Server versucht, die Informationen durch ihre Authentifizierung mit Active Directory zu überprüfen. Dazu werden das Internetprotokoll, der Port und die Anmeldeinformationen des Dienstkontos verwendet. Eine erfolgreich durchgeführte Bind-Operation gibt an, dass die Verbindung fehlerfrei konfiguriert ist.
2. **Gruppenbasierte Interaktionen**
    a) Suche nach einer oder mehreren Gruppen während der Definition der rollenbasierten Zugriffssteuerung (RBAC) und der Bereitstellungsgruppe. Der XenMobile Server-Administrator gibt eine Suchtextzeichenfolge in der XenMobile-Konsole ein. XenMobile Server durchsucht die ausgewählte Domäne nach allen Gruppen, die die eingegebene Teilzeichenfolge enthalten. Anschließend ruft XenMobile Server für die bei der Suche identifizierten Gruppen die Attribute “objectGUID”, “sAMAccountName” und “Distinguished Name” ab.

        > **Hinweis:**
        >
        > Diese Informationen werden nicht in der Datenbank von XenMobile Server gespeichert.

b) Hinzufügen oder Aktualisieren der RBAC- und Bereitstellungsgruppendefinition. Der XenMobile Server-Administrator wählt die Active Directory-Gruppen aus, die bei der vorherigen Suche gefunden wurden, und fügt sie in die Bereitstellungsgruppendefinition ein. XenMobile Server durchsucht Active Directory nacheinander nach den angegebenen Gruppen. XenMobile Server sucht nach dem Attribut "objectGUID" und ruft ausgewählte Attribute ab, darunter Angaben zur Gruppenmitgliedschaft. Die Angaben zur Gruppenmitgliedschaft erleichtern die Bestimmung der Zugehörigkeit vorhandener Benutzer oder Gruppen in der XenMobile Server-Datenbank zur abgerufenen Gruppe. Änderungen an der Gruppenmitgliedschaft führen zu einer RBAC- und Bereitstellungsgruppenableitung, mit Auswirkung auf Berechtigungen der betroffenen Benutzer in der Gruppe.

> **Hinweis:**
>
> Eine geänderte Bereitstellungsgruppendefinition kann zur Folge haben, dass sich App- oder Richtlinienberechtigungen für die betroffenen Benutzer ändern.

c) **Einladungen mit Einmal-PIN (OTP-Einladungen):** Der XenMobile Server-Administrator wählt eine Gruppe aus der Liste der Active Directory-Gruppen in der XenMobile Server-Datenbank. Für diese Gruppe werden sämtliche Benutzer (direkte und indirekte Benutzer) aus Active Directory abgerufen. Dann werden OTP-Einladungen an die Benutzer gesendet, die im vorherigen Schritt identifiziert wurden.

> **Hinweis:**
>
> Die drei o. g. Interaktionen implizieren, dass gruppenbasierte Interaktionen durch Änderungen an der XenMobile Server-Konfiguration ausgelöst werden. Wird die Konfiguration nicht geändert, gibt es keine Interaktionen mit Active Directory. Weiterhin wird impliziert, dass die regelmäßige Aufzeichnung der gruppenseitigen Änderungen durch Hintergrundaufträge nicht erforderlich ist.

3. **Benutzerbasierte Interaktion:**

a) Benutzerauthentifizierung. Bei der Benutzerauthentifizierung kommt es zu zwei Interaktionen mit Active Directory:

- Authentifizierung des Benutzers mit den bereitgestellten Anmeldeinformationen.
- Hinzufügen oder Aktualisieren ausgewählter Benutzerattribute in der XenMobile Server-Datenbank, einschließlich "objectGUID", "Distinguished Name", "sAMAccountName" und direkter Gruppenmitgliedschaft. Änderungen an der Gruppenmitgliedschaft führen zu einer erneuten Evaluation der App-, Richtlinien- und Zugriffsberechtigungen.

Der Benutzer authentifiziert sich entweder über das Gerät oder über die XenMobile Server-Konsole. In beiden Szenarien folgt die Interaktion mit Active Directory demselben Muster.

b) Zugriff auf App-Store und Aktualisierung: Bei einer Aktualisierung des Stores werden auch

die Benutzerattribute aktualisiert, einschließlich direkter Gruppenmitgliedschaften. Diese Aktion ermöglicht eine erneute Evaluation von Benutzerberechtigungen.

c) Einchecken von Geräten. Administratoren können in der XenMobile-Konsole das regelmäßige Einchecken von Geräten konfigurieren. Bei jedem Einchecken eines Gerätes werden die entsprechenden Benutzerattribute einschließlich der direkten Gruppenmitgliedschaften aktualisiert. Dieses Einchecken ermöglicht eine erneute Evaluation der Benutzerberechtigungen.

d) OTP-Einladungen nach Gruppe: Der XenMobile Server-Administrator wählt eine Gruppe aus der Liste der Active Directory-Gruppen in der XenMobile Server-Datenbank. Benutzer, die Mitglied der Gruppe sind (entweder direkt oder indirekt über eine Verschachtelung), werden von Active Directory abgerufen und in der XenMobile Server-Datenbank gespeichert. Dann werden OTP-Einladungen an die Benutzer gesendet, die im vorherigen Schritt als Mitglied identifiziert wurden.

e) OTP-Einladungen nach Benutzer. Der Administrator gibt in der XenMobile-Konsole eine Suchtextzeichenfolge ein. XenMobile Server sendet eine Abfrage an Active Directory und erhält Benutzerdatensätze, die der eingegebenen Textzeichenfolge entsprechen. Der Administrator wählt dann den Benutzer aus, der eine OTP-Einladung erhalten soll. XenMobile Server ruft die Benutzerdetails aus Active Directory ab und aktualisiert diese Informationen in der Datenbank, bevor eine Einladung an den Benutzer gesendet wird.

Hintergrundinteraktionen

Eine Schlussfolgerung aus der Inlinekommunikation mit Active Directory ist, dass gruppenbasierte Interaktionen durch ausgewählte Änderungen an der XenMobile Server-Konfiguration ausgelöst werden. Wird die Konfiguration nicht geändert, gibt es keine Interaktionen mit Active Directory.

Für diese Interaktion sind Hintergrundaufträge erforderlich, die in regelmäßigen Abständen eine Synchronisierung mit Active Directory durchführen. Dabei werden Datensätze aktualisiert und relevante Änderungen an den Gruppen übernommen.

Die folgenden Hintergrundaufträge interagieren mit Active Directory.

1. **Gruppensynchronisierung:** Mit diesem Auftrag wird für jede untersuchte Gruppe eine separate Abfrage an Active Directory zu Änderungen an den Attributen “Distinguished Name” oder “sAMAccountName” gesendet. Die Suchabfrage an Active Directory verwendet die ObjectGUID der Gruppe, um die aktuellen Werte der Attribute “Distinguished Name” und “sAMAccountName” abzurufen. Die geänderten Werte für “Distinguished Name” oder “sAMAccountName” werden dann in der Datenbank aktualisiert.

> **Hinweis:**
>
> Informationen zu Gruppenmitgliedschaften von Benutzern werden mit diesem Auftrag nicht aktualisiert.

2. **Synchronisierung verschachtelter Gruppen:** Mit diesem Auftrag werden Änderungen an der Verschachtelungshierarchie der untersuchten Gruppen aktualisiert. XenMobile Server kann direkten und indirekten Mitgliedern einer Gruppe Berechtigungen zuweisen. Die direkte Mitgliedschaft der Benutzer wird bei benutzerbasierten Inline-Interaktionen aktualisiert. Dieser im Hintergrund ausgeführte Auftrag prüft indirekte Mitgliedschaften. Bei einer indirekten Mitgliedschaft ist ein Benutzer Mitglied einer Gruppe, die Mitglied der untersuchten Gruppe ist.

   Dieser Auftrag erstellt eine Liste der Active Directory-Gruppen aus der XenMobile Server-Datenbank. Diese Gruppen gehören entweder zur Bereitstellungsgruppen- oder RBAC-Definition. Für jede Gruppe in dieser Liste ruft XenMobile Server die Mitglieder der Gruppe ab. Die Liste mit Distinguished Names stellt Benutzer und Gruppen dar, die Mitglied einer Gruppe sind. XenMobile Server stellt eine weitere Abfrage an Active Directory, um nur die Benutzer zu erhalten, die Mitglied der gewünschten Gruppe sind. Der Unterschied zwischen beiden Listen stellt nur die Mitglieder dar, die Mitglied der Gruppe sind. Änderungen an Mitgliedsgruppen werden in der Datenbank aktualisiert. Dieser Vorgang wird für alle Gruppen in der Hierarchie wiederholt.

   Änderungen an einer Verschachtelung führen dazu, dass die Berechtigungen der betroffenen Benutzer angepasst werden.

3. **Prüfung auf deaktivierte Benutzer:** Dieser Auftrag wird nur ausgeführt, wenn der XenMobile-Administrator eine Aktion zur Prüfung auf deaktivierte Benutzer erstellt. Der Auftrag läuft im Rahmen einer Gruppensynchronisierung ab. Für jeden untersuchten Benutzer wird eine Abfrage an Active Directory gesendet, um zu prüfen, ob der Benutzer deaktiviert wurde.

Häufig gestellte Fragen

Wie häufig werden Hintergrundaufträge standardmäßig ausgeführt?

- Aufträge zur Gruppensynchronisierung starten alle fünf Stunden ab 02:00 Uhr Ortszeit.
- Aufträge zur Synchronisierung verschachtelter Gruppen werden einmal täglich um 00:00 Uhr Ortszeit ausgeführt.

Warum ist eine Gruppensynchronisierung erforderlich?

- Das Attribut “memberOf” im Datensatz eines Benutzers in Active Directory enthält eine Liste aller Gruppen, in denen der Benutzer ein direktes Mitglied ist. Wenn eine Gruppe aus einer Organisationseinheit in eine andere verschoben wird, stellt das Attribut “memberOf” den letzten Wert des “Distinguished Name” dar. In der XenMobile Server-Datenbank ist ebenfalls der zuletzt aktualisierte Wert gespeichert. Stimmen die “Distinguished Names” der Gruppe nicht überein,

kann dies dazu führen, dass der Benutzer den Zugriff auf die Bereitstellungsgruppe verliert. Der Benutzer kann zudem den Zugriff auf Apps und Richtlinien verlieren, die der Bereitstellungsgruppe zugeordnet sind.
- Der Hintergrundauftrag sorgt dafür, dass das Attribut "Distinguished Name" der Gruppe in der XenMobile Server-Datenbank aktualisiert wird, damit Berechtigungen von Benutzern erhalten bleiben.
- Synchronisierungsaufträge werden planmäßig alle fünf Stunden durchgeführt, da davon ausgegangen wird, dass Gruppenänderungen in Active Directory selten sind.

Kann eine Gruppensynchronisierung deaktiviert werden?

- Sie können Aufträge deaktivieren, wenn Sie wissen, dass die Gruppen nicht zwischen Organisationseinheiten wechseln.

Warum ist ein Hintergrundauftrag zur Verarbeitung verschachtelter Gruppen erforderlich?

- Änderungen an der Verschachtelung von Gruppen in Active Directory treten nicht täglich auf. Wird die Verschachtelungshierarchie der Gruppen geändert, wirkt sich dies auch auf die Berechtigungen der betroffenen Benutzer aus. Wenn eine Gruppe der Hierarchie hinzugefügt wird, erhalten die Benutzer in der Gruppe Anspruch auf die jeweiligen Rollen. Wenn eine Gruppe verschoben und damit aus der Verschachtelung entfernt wird, können Benutzer, die Mitglied der Gruppe sind, ihren Zugriff auf rollenbasierte Berechtigungen verlieren.
- Änderungen an der Verschachtelung werden bei der Aktualisierung des Benutzers nicht erfasst. Da Verschachtelungsänderungen nicht bedarfsgesteuert erfolgen können, werden diese Änderungen über einen Hintergrundauftrag erfasst.
- Änderungen an der Verschachtelung gelten als selten, sodass der Hintergrundauftrag, der dies kontrolliert, nur einmal am Tag ausgeführt wird.

Kann die Verarbeitung verschachtelter Gruppen deaktiviert werden?

- Sie können Aufträge deaktivieren, wenn Sie wissen, dass für die Gruppen keine Verschachtelungsänderungen auftreten.

Bereitstellung von XenMobile

November 9, 2020

Bei der Planung einer XenMobile-Bereitstellung sind zahlreiche Faktoren zu berücksichtigen:

- Welche Geräte sollen verwendet werden?
- Wie sollen die Geräte verwaltet werden?
- Wie stellen Sie sicher, dass Ihr Netzwerk sicher und gleichzeitig benutzerfreundlich ist?
- Welche Hardware benötigen Sie und wie soll sie gewartet werden?

Die Artikel in diesem Abschnitt sollen solche Fragen beantworten. Sie enthalten Anwendungsfälle und Empfehlungen zur Bereitstellung.

Beachten Sie, dass Richtlinien oder Empfehlungen unter Umständen nicht für alle Umgebungen oder Anwendungen gelten. Richten Sie in jedem Fall erst eine Testumgebung ein, bevor Sie eine XenMobile-Bereitstellung in der Praxis einsetzen.

In diesem Abschnitt werden folgende Bereiche erörtert:

- **Analyse:** gängige Anwendungsfälle und Aspekte bei der Planung der Bereitstellung .
- **Design & Konfiguration:** Empfehlungen zu Aufbau und Konfiguration der Umgebung.
- **Betrieb und Überwachung:** Maßnahmen für einen reibungslosen Betrieb der Umgebung.

Analyse

Wie bei jeder anderen Bereitstellung steht die Analyse der Anforderungen an erster Stelle. Welche Aufgaben soll XenMobile primär erfüllen? Müssen Sie jedes Gerät in der Umgebung oder nur die Apps verwalten? Vielleicht müssen Sie auch beides verwalten. Wie hoch sind die Sicherheitsanforderungen Ihrer XenMobile-Umgebung? Erörtern wir zunächst häufige Anwendungen und allgemeine Fragen, die bei der Planung der Bereitstellung zu berücksichtigen sind.

- Verwaltungsmodi
- Geräteanforderungen
- Sicherheit und Benutzererfahrung
- Apps
- Benutzergemeinschaften
- E-Mail-Strategie
- XenMobile-Integration
- Anforderungen von Umgebungen mit mehreren Sites

Design und Konfiguration

Nachdem Sie die Anforderungen an Ihre Bereitstellung analysiert haben, können Sie den Aufbau und die Konfiguration Ihrer Umgebung festlegen. Ein paar Dinge, die Sie planen müssen:

- Hardware für den Server
- Einrichten von Richtlinien für Apps und Geräte
- Registrierung der Benutzer

Dieser Abschnitt enthält Anwendungsfälle und Empfehlungen für jedes dieser Szenarien und mehr.

- Integration in Citrix ADC und Citrix Gateway
- SSO- und Proxy-Überlegungen für MDX-Apps
- Authentifizierung

- Referenzarchitektur für on-premises Bereitstellungen
- Servereigenschaften
- Richtlinien für Geräte und Apps
- Optionen der Benutzerregistrierung
- Optimieren von XenMobile-Prozessen

Betrieb und Überwachung

Nach der Inbetriebnahme der XenMobile-Umgebung gewährleistet eine effiziente Überwachung einen reibungslosen Betrieb. Im Abschnitt zur Überwachung wird erläutert, wo Sie die von XenMobile und seinen Komponenten generierten Protokolle und Meldungen finden und wie diese Protokolle zu lesen sind. Der Abschnitt enthält außerdem Anleitungen zur Problembehandlung, mit denen Sie die Zeit für ein Kundensupportfeedback reduzieren können.

- Bereitstellen und Entfernen von Apps
- Über das Dashboard steuerbare Vorgänge
- Unterstützung für die rollenbasierte Zugriffssteuerung in XenMobile
- Systemüberwachung
- Notfallwiederherstellung
- Citrix Support-Prozess

Verwaltungsmodi

January 5, 2022

Für jede XenMobile-Instanz (Einzelserver oder Cluster) können Sie auswählen, ob Geräte, Apps oder beides verwaltet werden sollen. In XenMobile gibt es folgende Verwaltungsmodi für Apps und Geräte:

- Mobilgeräteverwaltungsmodus (MDM-Modus)
- Mobilanwendungsverwaltungsmodus (MAM-Modus)
- MDM + MAM-Modus (Enterprise-Modus)

Mobilgeräteverwaltung (MDM-Modus)

> **Wichtig:**
>
> Wenn Sie den ursprünglich konfigurierten MDM-Modus in den ENT-Modus ändern, müssen Sie darauf achten, dass Sie die gleiche (Active Directory)-Authentifizierung verwenden. Die Änderung des Authentifizierungsmodus nach der Benutzerregistrierung wird in XenMobile nicht unterstützt. Weitere Informationen finden Sie unter Upgrade.

Mit MDM können Sie Mobileräte konfigurieren, schützen und betreuen. Mit MDM können Sie Geräte und Daten auf Geräten auf Systemebene schützen. Sie können Richtlinien, Aktionen und Sicherheitsfunktionen konfigurieren. Sie können beispielsweise ein Gerät selektiv löschen, wenn es verloren oder gestohlen wurde oder nicht mehr richtlinientreu ist. Die App-Verwaltung ist im MDM-Modus zwar nicht verfügbar, Sie können jedoch mobile Apps (z. B. aus öffentlichen App-Stores und Unternehmensapps) bereitstellen. Der MDM-Modus empfiehlt sich generell für folgende Szenarien:

- MDM ist eine Überlegung für unternehmenseigene Geräte, bei denen Verwaltungsrichtlinien auf Geräteebene oder Einschränkungen wie vollständiges oder selektives Löschen oder Geolocation erforderlich sind.
- Geräte müssen verwaltet werden, es sind jedoch keine MDX-Richtlinien (App-Containerization; Steuerung der App-Datenfreigabe, Micro-VPN usw.) erforderlich.
- E-Mail muss nur an die nativen E-Mail-Clients auf den Mobilgeräten übermittelt werden und Exchange ActiveSync oder Clientzugriffsserver steht bereits extern zur Verfügung. In diesem Fall können Sie mit MDM die E-Mail-Zustellung konfigurieren.
- Es werden native Enterprise-Apps (nicht-MDX), Apps aus öffentlichen App-Stores oder MDX-Apps aus öffentlichen Stores bereitgestellt. Es ist zu beachten, dass eine MDM-Lösung allein nicht unbedingt Datenlecks zwischen Apps auf Geräten verhindert. Datenlecks können beim Kopieren und Einfügen oder der Verwendung der Option “Speichern unter” in Office 365-Apps auftreten.

Mobilanwendungsverwaltung (MAM-Modus)

Im MAM-Modus werden App-Daten geschützt und Sie können die App-Datenfreigabe steuern. Außerdem können Sie im MAM-Modus Unternehmensdaten und -ressourcen getrennt von personenbezogenen Daten verwalten. Wenn XenMobile für den MAM-Modus konfiguriert ist, können Sie MDX-aktivierte mobile Apps für die Containerization und Steuerung auf App-Basis verwenden. Der MAM-Modus wird auch als “Nur-MAM-Modus” bezeichnet. Dieser Begriff unterscheidet diesen Modus vom Legacy-MAM-Modus.

Durch die Nutzung von MDX-Richtlinien können in XenMobile Netzwerkzugriff (z. B. Micro-VPN), App- und Geräteinteraktion, Datenverschlüsselung und App-Zugriff auf App-Ebene gesteuert werden.

Die Mobilanwendungsverwaltung eignet sich häufig für BYOD-Geräte, da Unternehmensdaten geschützt werden, obwohl die Geräte nicht verwaltet werden. MDX hat viele Nur-MAM-Richtlinien, die kein MDM-Steuerelement erfordern.

MAM unterstützt auch die mobilen Produktivitätsapps. Dies umfasst die sichere E-Mail-Zustellung an Citrix Secure Mail, die Datenfreigabe zwischen den geschützten mobilen Produktivitätsapps und die sichere Datenspeicherung in Citrix Files. Weitere Informationen finden Sie unter Mobile Produktivitätsapps.

Der MAM-Modus ist in folgenden Situationen häufig geeignet:

- Es werden mobile Apps (z. B. MDX-Apps) bereitgestellt, die auf App-Ebene verwaltet werden.
- Eine Geräteverwaltung auf Systemebene ist nicht erforderlich.

MDM + MAM (Enterprise-Modus)

MDM + MAM ("Enterprise-Modus") ist ein Hybridmodus, in dem alle Features der XenMobile Enterprise Mobility Management-Lösung zur Verfügung stehen. Im MDM + MAM-Modus von XenMobile können Sie die MDM- und die MAM-Features verwenden.

Sie können in XenMobile angeben, ob Benutzer die Geräteverwaltung abwählen können oder ob sie erzwungen wird. Diese Flexibilität ist für Umgebungen mit unterschiedlichen Anwendungsfällen nützlich. In einer solchen Umgebung kann die Verwaltung eines Geräts über MDM-Richtlinien für den Zugriff auf MAM-Ressourcen erforderlich sein.

Der MDM + MAM-Modus eignet sich für folgende Situationen:

- Es werden sowohl MDM als auch MAM benötigt. MDM ist für den Zugriff auf die MAM-Ressourcen erforderlich.
- In einigen Anwendungsfällen wird MDM benötigt, in anderen nicht.
- In einigen Anwendungsfällen wird MAM benötigt, in anderen nicht.

Den Verwaltungsmodus für XenMobile Server geben Sie über die Eigenschaft "Servermodus" an. Diese Einstellung wird in der XenMobile-Konsole konfiguriert. Es gibt die Modi MDM, MAM oder ENT (MDM + MAM).

Welche Verwaltungsmodi und Features zur Verfügung stehen, hängt von der lizenzierten XenMobile-Edition ab (siehe Tabelle unten).

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
MDM-Features	MDM-Features	MDM-Features
-	MAM-Features	MAM-Features
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	-	ShareConnect

-	-	Citrix Files

Verwaltungsmodi und Registrierungsprofile

Verwaltungsmodi und Registrierungsprofile arbeiten zusammen. Mit Registrierungsprofilen konfigurieren Sie Registrierungsoptionen zur Geräte- und App-Verwaltung für Android und iOS. Bei Android unterscheiden sich die für den MDM+MAM-Servermodus verfügbaren Registrierungsoptionen von denjenigen für den MDM-Modus. Weitere Informationen finden Sie unter Registrierungsprofile.

Geräteverwaltung und MDM-Registrierung

Eine XenMobile Enterprise-Umgebung kann unterschiedliche Anwendungsfälle enthalten, von denen einige eine Geräteverwaltung über MDM-Richtlinien für den Zugriff auf MAM-Ressourcen erfordern. Bevor Sie mobile Produktivitätsapps bereitstellen, sollten Sie Ihre Anwendungsfälle detailliert beurteilen und entscheiden, ob eine MDM-Registrierung erforderlich ist. Wenn Sie sich später für andere Anforderungen bei der MDM-Registrierung entscheiden, müssen die Benutzer in aller Regel ihre Geräte neu registrieren.

> **Hinweis:**
>
> Um anzugeben, ob die Benutzer eine MDM-Registrierung durchführen müssen, verwenden Sie die XenMobile Server-Eigenschaft **Registrierung erforderlich** in der XenMobile-Konsole (**Einstellungen > Servereigenschaften**). Diese globale Servereigenschaft gilt für alle Benutzer und Geräte der XenMobile-Instanz. Die Eigenschaft gilt nur im ENT-Modus von XenMobile Server.

Nachfolgend sind die Vor- und Nachteile (einschließlich Abhilfemöglichkeiten) des Erzwingens einer MDM-Registrierung in einer XenMobile-Bereitstellung im Enterprisemodus aufgeführt.

MDM-Registrierung optional

Vorteile:

- Die Benutzer können auf MAM-Ressourcen zugreifen, ohne ihre Geräte der MDM-Verwaltung zu unterstellen. Dies kann die Benutzerakzeptanz erhöhen.
- Möglichkeit, den Zugriff auf MAM-Ressourcen zu sichern, um Unternehmensdaten zu schützen.
- MDX-Richtlinien wie **App-Passode** können den App-Zugriff für jede MDX-App steuern.
- Die Konfiguration von Citrix ADC, XenMobile Server und App-basierten Timeouts sowie der Citrix PIN bieten eine zusätzliche Sicherheitsebene.

- MDM-Aktionen gelten zwar nicht für ein Gerät, es gibt jedoch MDX-Richtlinien zum Verweigern des MAM-Zugriffs. Die Verweigerung basierte auf Systemeinstellungen, etwa im Fall einer Erkennung von Jailbreak oder Rooting.
- Die Benutzer können bei der erstmaligen Verwendung wählen, ob sie ihr Gerät bei MDM registrieren möchten.

Nachteile:

- MAM-Ressourcen stehen für Geräte zur Verfügung, die nicht bei MDM registriert sind.
- MDM-Richtlinien und -Aktionen stehen nur für bei MDM registrierte Geräte zur Verfügung.

Abhilfemöglichkeiten:

- Die Benutzer müssen Unternehmensbestimmungen zustimmen, die sie bei fehlender Richtlinientreue haftbar machen. Administratoren überwachen nicht verwaltete Geräte.
- Anwendungszugriff und Sicherheit werden über App-Timer verwaltet. Kürzere Timeouts erhöhen die Sicherheit, können sich jedoch auf die Benutzererfahrung auswirken.
- Eine zweite XenMobile-Umgebung mit erzwungener MDM-Registrierung kann eingerichtet werden. Bedenken Sie hierbei den zusätzlichen Verwaltungs- und Ressourcenaufwand.

MDM-Registrierung erforderlich

Vorteile:

- Der Zugriff auf MAM-Ressourcen kann auf MDM-verwaltete Geräte beschränkt werden.
- MDM-Richtlinien und -Aktionen können nach Bedarf auf alle Geräte in der Umgebung angewendet werden.
- Die Benutzer können die Geräteregistrierung nicht umgehen.

Nachteile:

- Alle Benutzer müssen sich bei MDM registrieren.
- Dies kann die Akzeptanz bei Benutzern mindern, die eine Verwaltung ihrer eigenen Geräte durch das Unternehmen ablehnen.

Abhilfemöglichkeiten:

- Informieren Sie die Benutzer darüber, was genau durch XenMobile auf ihren Geräten verwaltet wird und auf welche Informationen die Administratoren zugreifen können.
- Sie können eine zweite XenMobile-Umgebung im MAM-Servermodus (“Nur-MAM-Modus”) für Geräte einrichten, für die keine MDM-Verwaltung benötigt wird. Bedenken Sie hierbei den zusätzlichen Verwaltungs- und Ressourcenaufwand.

MAM und Legacy-MAM-Modus

Mit XenMobile 10.3.5 wurde der Nur-MAM-Servermodus eingeführt. Zur Unterscheidung des älteren und des neuen MAM-Modus werden in der Dokumentation folgende Begriffe verwendet: Der neue Modus heißt “Nur-MAM-Modus” oder “MA”, der ältere MAM-Modus heißt “Legacy-MAM-Modus”.

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

Die Legacy-MAM-Funktionalität gilt, wenn für die Servermoduseigenschaft in XenMobile ENT eingestellt ist, und Benutzer sich gegen die Geräteverwaltung entscheiden. In diesem Fall werden die Geräte im MAM-Modus registriert. Für Benutzer, die sich gegen die MDM-Verwaltung entscheiden, bleibt die Legacy-MAM-Funktionalität erhalten.

> **Hinweis:**
>
> In früheren Versionen hatte das Einstellen der Servermoduseigenschaft auf MAM den gleichen Effekt wie die Einstellung ENT: Benutzer, die die MDM-Verwaltung ablehnen, erhalten die Legacy-MAM-Funktionalität.

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

Ihre Lizenzen sind für Edition	Geräte in diesem Modus registrieren	Servermodus festlegen auf
Enterprise/Advanced/MDM	MDM-Modus	MDM
Enterprise/Advanced	MAM-Modus (“Nur-MAM-Modus”)	MAM
Enterprise/Advanced	MDM+MAM-Modus	ENT (Benutzer, die die Geräteverwaltung ablehnen, verwenden den Legacy-MAM-Modus).

Der Nur-MAM-Modus unterstützt die folgenden Features, die bisher nur im ENT-Modus verfügbar waren. Diese Features sind nicht für Windows Phone verfügbar.

- **Zertifikatauthentifizierung:** Der Nur-MAM-Modus unterstützt die zertifikatbasierte Authentifizierung. Die Benutzer haben weiterhin Zugriff auf ihre Apps, selbst wenn ihr Active Directory-Kennwort abläuft. Wenn Sie die Zertifikatauthentifizierung für MAM-Geräte verwenden, müssen Sie das Citrix Gateway konfigurieren. In XenMobile ist unter **Einstellungen > Citrix Gateway** die Option “Benutzerzertifikat für Authentifizierung bereitstellen” standardmäßig

auf **Aus** festgelegt, sodass die Authentifizierung durch Benutzernamen und Kennwort erfolgt. Ändern Sie diese Einstellung in **Ein**, um die Zertifikatauthentifizierung zu aktivieren.

- **Selbsthilfeportal:** ermöglicht den Benutzern das Sperren und Löschen von Apps. Diese Aktionen können für alle Apps auf dem Gerät durchgeführt werden. Sie können unter **Konfigurieren > Aktionen** die Aktionen "App-Sperre" und "App löschen" konfigurieren.
- **Alle Registrierungssicherheitsmodi:** zum Beispiel "Hohe Sicherheit", "Einladungs-URL" und "Zweistufig"; die Konfiguration erfolgt unter **Verwalten > Registrierungseinladungen**.
- **Geräteregistrierungslimit für iOS- und Android-Geräte:** Die Servereigenschaft **Anzahl der Geräte pro Benutzer** wurde in den Bereich **Konfigurieren > Registrierungsprofile** verschoben und gilt jetzt für alle Servermodi.
- **Nur-MAM-APIs:** Für Geräte im Nur-MAM-Modus können Sie REST-Dienste mit einem beliebigen REST-Client und Dienste, die über die XenMobile-Konsole verfügbar gemacht werden, mit der XenMobile-REST-API aufrufen.
- Nur-MAM-APIs ermöglichen Folgendes:
  - Senden einer Einladungs-URL und Einmal-PIN
  - App-Sperr-/-Löschaktionen auf Geräten

In der Tabelle unten werden die Unterschiede zwischen Legacy-MAM- und Nur-MAM-Funktionalität aufgeführt.

Registrierungsszenarios und andere Features	Legacy-MAM (Servermodus ist ENT)	Ausschließlicher MAM-Modus (Servermodus ist MAM)
Zertifikatauthentifizierung	Nicht unterstützt	Unterstützt Für die Zertifikatauthentifizierung ist Citrix Gateway erforderlich.
Bereitstellungsanforderungen	XenMobile Server muss nicht direkt von Geräten aus zugänglich sein.	XenMobile Server muss nicht direkt von Geräten aus zugänglich sein.
Registrierungsoption	Verwenden des Citrix Gateway-FQDN oder, bei Verwendung des MDM-FQDN, Ablehnen der Registrierung	Verwenden des XenMobile Server-FQDN

Registrierungsmethoden*	Benutzername + Kennwort	Benutzername + Kennwort, Hohe Sicherheit, Einladungs-URL, Einladungs-URL + PIN, Einladungs-URL + Kennwort, Zweistufig, Benutzername + PIN
Apps sperren und löschen	Unterstützt	Unterstützt
Selbsthilfeportaloptionen zum Sperren und Löschen von Apps	Nicht unterstützt	Unterstützt
App-Löschen - Verhalten	Apps bleiben auf dem Gerät, sind aber nicht verwendbar. XenMobile löscht das Konto nur auf dem Client.	Apps bleiben auf dem Gerät, sind aber nicht verwendbar. XenMobile löscht das Konto nur auf dem Client.
Automatisierte Aktionen für ausschließliche MAM-Benutzer.	Mit Ereignissen, Geräteeigenschaften und Benutzereigenschaften verbundene Aktionen werden unterstützt. Automatisierte Aktionen für installierte Apps werden nicht unterstützt.	Unterstützt Aktionen auf der Basis von Ereignissen, Geräteeigenschaften, Benutzereigenschaften und Apps, einschließlich App-Löschung und App-Sperre.
Integrierte Aktion beim Löschen eines Active Directory-Benutzers	App-Löschen wird unterstützt.	App-Löschen wird unterstützt.
Registrierungslimit	Unterstützt, Konfiguration über ein Registrierungsprofil.	Unterstützt, Konfiguration über ein Registrierungsprofil.
Softwarebestand	Unterstützt XenMobile listet auf dem Gerät installierte Apps auf.	Nicht unterstützt

*__Benachrichtigungen:__ SMTP ist die einzige unterstützte Methode zum Senden von Registrierungseinladungen.

> **Wichtig:**
>
> Im Nur-MAM-Modus müssen zuvor registrierte Benutzer ihre Geräte erneut registrieren. Geben Sie Benutzern den vollqualifizierten Domänennamen (FQDN) für XenMobile Server, den sie für die Registrierung benötigen. Im Nur-MAM-Modus werden Geräte wie im ENT-Modus mit dem FQDN von XenMobile Server registriert. (Im Legacy-MAM-Modus werden Geräte unter Verwendung des Citrix Gateway-FQDN registriert.)

Geräteanforderungen

March 31, 2021

Überlegen Sie bei jeder Bereitstellung genau, welches Gerät Sie für das Rollout verwenden möchten. Zahlreiche Optionen stehen für die Plattformen iOS, Android und Windows zur Verfügung. Eine Liste der in XenMobile unterstützten Geräte finden Sie unter Unterstützte Geräteplattformen.

In einer BYOD-Umgebung mit Privatgeräten ist der gemeinsame Einsatz mehrerer unterstützter Plattformen möglich. Berücksichtigen Sie jedoch die im Artikel "Unterstützte Geräteplattformen" beschriebenen Einschränkungen, wenn Sie Benutzer darüber informieren, welche Geräte sie registrieren können. Selbst wenn Sie nur ein oder zwei Geräte in Ihrer Umgebung zulassen, funktioniert XenMobile etwas unterschiedlich auf iOS-, Android- und Windows-Geräten. Jede Plattform bietet ein anderes Funktionsspektrum.

Nicht alle App-Designs eignen sich zudem für Tablets und Smartphones. Testen Sie Apps, bevor Sie weitreichende Änderungen vollziehen, um sicherzustellen, dass die App sich auf dem geplanten Gerätebildschirm gut anzeigen lässt.

Ziehen Sie auch Registrierungsfaktoren in Erwägung. Apple und Google bieten Registrierungsprogramme für Unternehmen. Über das Apple-Bereitstellungsprogramm und Google Android Enterprise können Sie vorkonfigurierte Geräte erwerben, die sofort einsatzbereit sind.

Weitere Informationen zur Registrierung finden Sie unter Optionen der Benutzerregistrierung.

Sicherheit und Benutzererfahrung

September 24, 2021

Sicherheit ist für jede Organisation wichtig, Sie müssen jedoch ein Gleichgewicht zwischen Sicherheit und Benutzererfahrung finden. Sie könnten beispielweise eine hochsichere Umgebung haben, die Benutzer mühselig ist. Bei einer sehr benutzerfreundlichen Umgebung ist wiederum die Zugriffssteuerung nicht so streng. In den anderen Abschnitten dieses virtuellen Handbuchs werden Sicher-

heitsfeatures im Detail behandelt. Dieser Artikel enthält einen Überblick über allgemeine Sicherheitsanliegen und die in XenMobile verfügbaren Sicherheitsoptionen.

Wichtige Überlegungen für alle Anwendungsfälle:

- Möchten Sie bestimmte Apps, das gesamte Gerät oder beides schützen?
- Wie sollen sich die Benutzer authentifizieren? Möchten Sie LDAP, die zertifikatbasierte Authentifizierung oder beides zusammen verwenden?
- Wie sollen Benutzersitzungstimeouts behandelt werden? Beachten Sie, dass es für Hintergrunddienste, Citrix ADC und für den Offlinezugriff auf Apps unterschiedliche Timeouts gibt.
- Sollen die Benutzer einen Passcode auf Geräteebene und/oder auf App-Ebene einrichten? Wie viele Anmeldeversuche möchten Sie den Benutzern erlauben? Berücksichtigen Sie die Auswirkungen zusätzlicher über MAM implementierter Authentifizierungsanforderungen für die Apps auf die Benutzererfahrung.
- Welche weiteren Einschränkungen möchten Sie den Benutzern auferlegen? Sollen Benutzer auf Cloudservices wie Siri zugreifen? Was können die Benutzer mit den einzelnen von Ihnen zur Verfügung gestellten Apps tun und was nicht? Möchten Sie unternehmensweite Wi-Fi-Richtlinien bereitstellen, damit mobile Datenkontingente nicht im Büro verbraucht werden?

Gegenüberstellung: Apps und Gerät

Zu den ersten Überlegungen gehört diejenige, ob nur bestimmte Apps über die Mobilanwendungsverwaltung (MAM) geschützt werden sollen. Alternativ können komplette Geräte per Mobilgeräteverwaltung (MDM) verwaltet werden. Wenn Sie keine Steuerung auf Geräteebene benötigen, verwalten Sie meist nur die mobilen Apps, insbesondere wenn Sie BYOD-Geräte (Bring Your Own Device) zulassen.

Benutzer mit nicht von XenMobile verwalteten Geräten können Apps über den App-Store installieren. Anstelle einer Steuerung auf Gerätebasis, etwa der selektiven oder vollständigen Löschung der Daten auf einem Gerät, steuern Sie den Zugriff auf Apps über App-Richtlinien. Je nach Einstellung erfordern die Richtlinien, dass Geräte regelmäßig XenMobile abfragen, um sicherzustellen, dass Apps weiterhin zugelassen sind.

Mit MDM können Sie ein ganzes Gerät schützen und dabei auch einen Bestand von dessen Software aufstellen. Sie können die Registrierung von Geräten mit Jailbreak, Rooting oder nicht sicherer Software unterbinden. Eine so umfassende Kontrolle macht die Benutzer jedoch misstrauisch und kann dazu führen, dass weniger persönliche Geräte registriert werden.

Authentifizierung

Die Authentifizierung spielt für die Benutzererfahrung eine große Rolle. Wenn in Ihrer Organisation bereits Active Directory in Verwendung ist, bietet es die einfachste Möglichkeit für den Benutzerzugriff auf das System.

Ein wichtiger Aspekt der Benutzererfahrung bei der Authentifizierung sind Timeouts. In hochsicheren Umgebungen müssen sich Benutzer ggf. bei jedem Zugriff auf das System anmelden. Diese Option ist jedoch nicht für alle Organisationen geeignet. Beispielsweise ist es für die Benutzer u. U. mühselig, wenn sie sich jedes Mal, wenn sie in ihre E-Mail schauen möchten, anmelden müssen.

Benutzerentropie

Für zusätzliche Sicherheit können Sie ein Feature namens *Benutzerentropie* aktivieren. Citrix Secure Hub und einige weitere Apps verwenden häufig gemeinsame Daten wie Kennwörter, PINs und Zertifikate, um sicherzustellen, dass alles ordnungsgemäß funktioniert. Diese Informationen werden in einem generischen Tresor in Secure Hub gespeichert. Wenn Sie die Benutzerentropie über die Option **Encrypt Secrets** aktivieren, erstellt XenMobile einen neuen Tresor namens “UserEntropy”. XenMobile verschiebt die Informationen aus dem allgemeinen Tresor in den neuen Tresor. Damit Secure Hub bzw. andere Apps auf die Informationen zugreifen können, müssen die Benutzer ein Kennwort oder eine PIN eingeben.

Durch Aktivieren der Benutzerentropie wird an mehreren Stellen eine weitere Authentifizierungsebene hinzugefügt. Die Benutzer müssen dann jedes Mal, wenn eine App Zugriff auf gemeinsam genutzte Daten (einschließlich Zertifikate) im UserEntropy-Tresor benötigt, ein Kennwort oder eine PIN eingeben.

Weitere Informationen zur Benutzerentropie finden Sie unter Informationen zum MDX Toolkit in der Dokumentation zu XenMobile. Die Einstellungen zum Aktivieren der Benutzerentropie finden Sie in den Clienteigenschaften.

Richtlinien

MDX- und MDM-Richtlinien bieten große Flexibilität, sie können jedoch auch die Benutzer einschränken. Beispielsweise können Sie den Zugriff auf Cloudanwendungen wie Siri oder iCloud sperren, von denen aus sensible Daten an verschiedene Ziele gesendet werden könnten. Sie können eine Richtlinie einrichten, um den Zugriff auf diese Dienste zu sperren, eine solche Richtlinie kann aber unbeabsichtigte Konsequenzen haben. Das iOS-Tastaturmikrofon erfordert ebenfalls Cloudzugriff und Sie blockieren möglicherweise auch den Zugriff auf dieses Feature.

Apps

Das Enterprise Mobility Management (EMM) besteht aus dem Mobile Device Management (MDM) und dem Mobile Application Management (MAM). Mit MDM können Unternehmen Mobilgeräte schützen und steuern und MAM erleichtert die Bereitstellung und Verwaltung von Apps. Angesichts der Zunahme von BYOD wird häufig eine MAM-Lösung zur App-Bereitstellung, Softwarelizenzierung, Konfiguration und App-Lebenszyklusverwaltung implementiert.

Mit XenMobile können Sie diese Apps noch sicherer machen, indem Sie bestimmte MAM-Richtlinien und VPN-Einstellungen konfigurieren, um Datenlecks und andere Sicherheitsbedrohungen zu vermeiden. Mit XenMobile können Unternehmen flexibel eine der folgenden Lösungen bereitstellen:

- Nur-MAM-Umgebung
- Nur-MDM-Umgebung
- Einheitliche XenMobile Enterprise-Umgebung mit MDM- und MAM-Funktionen auf derselben Plattform

Zusätzlich zur App-Bereitstellung für Mobilgeräte ermöglicht XenMobile die App-Containerization per MDX-Technologie. MDX sichert Apps durch Verschlüsselung, separat von der Verschlüsselung auf Geräteebene, die von der Plattform bereitgestellt wird. Sie können die App löschen oder sperren. Die Apps unterliegen einer detaillierten richtlinienbasierten Steuerung. Unabhängige Softwarehersteller (ISV) können diese Steuerelemente über das Mobile Apps SDK anwenden.

In Unternehmensumgebungen verwenden Benutzer eine Reihe von mobilen Apps für ihre Arbeit. Dabei kann es sich um Apps aus einem öffentlichen App-Store, um unternehmensintern entwickelte Apps und native Apps handeln. In XenMobile werden Apps wie folgt kategorisiert:

Öffentliche Apps: Kostenlose oder kostenpflichtige Apps in einem öffentlichen App-Store, z. B. Apple App Store oder Google Play. Unternehmensexterne Hersteller bieten ihre Apps häufig in öffentlichen App-Stores an. Die Kunden können solche Apps direkt aus dem Internet herunterladen. Je nach Bedarf werden in einem Unternehmen u. U. zahlreiche öffentliche Apps in verwendet. Beispiele für solche Apps sind GoToMeeting, Salesforce und EpicCare.

Citrix unterstützt das direkte Herunterladen von App-Binärdateien aus öffentlichen App-Stores und das anschließende Umschließen mit dem MDX Toolkit zur Verteilung im Unternehmen nicht. Um Apps von Drittanbietern MDX-fähig zu machen, wenden Sie sich an den App-Anbieter, um die Binärdateien zu erhalten. Sie können die Binärdateien mit dem MDX Toolkit umschließen oder das MAM-SDK in die Binärdateien integrieren.

Intern entwickelte Apps: In vielen Unternehmen gibt es interne Entwickler, die Apps für spezifische Zwecke und zur unabhängigen Verteilung im Unternehmen entwickeln. In manchen Fällen haben Unternehmen auch Apps von ISV. Sie können solche Apps als native Apps bereitstellen oder mithilfe einer MAM-Lösung wie XenMobile eine Containerization durchführen. Beispielsweise kann eine Gesundheitsorganisation eine interne App erstellen, mit der Ärzte Patientendaten auf Mobilgeräten anzeigen können. Anschließend wird MAM-SDK in die App integriert oder die App wird mit MDM umschlossen, um die Patientendaten zu schützen und den VPN-Zugriff auf den Backendserver mit der Patientendatenbank zu ermöglichen.

Web- und SaaS-Apps: Apps, auf die über ein internes Netzwerk (Web-Apps) oder ein öffentliches Netzwerk (SaaS-Apps) zugegriffen wird. Mit XenMobile können Sie auch benutzerdefinierte Web- und SaaS-Apps unter Einsatz mehrerer App-Connectors erstellen. Die App-Connectors können das Single Sign-On (SSO) für bestehende Web-Apps vereinfachen. Weitere Informationen finden Sie unter

App-Connectortypen. Sie können beispielsweise Google Apps SAML für das SSO basierend auf SAML (Security Assertion Markup Language) für Google Apps verwenden.

Mobile Produktivitätsapps: von Citrix entwickelte Apps, die in der XenMobile-Lizenz enthalten sind. Weitere Informationen finden Sie unter Mobile Produktivitätsapps. Citrix bietet auch andere Citrix Ready-Apps an, die ISV mit dem Mobile Apps SDK entwickelt haben.

HDX-Apps: unter Windows gehostete Apps, die mit StoreFront veröffentlicht werden. In einer Citrix Virtual Apps and Desktops-Umgebung können Sie solche Apps in XenMobile integrieren, um sie registrierten Benutzern zur Verfügung zu stellen.

Die zugrunde liegende Konfiguration und Architektur hängt von der Art der Apps ab, die Sie mit XenMobile bereitstellen und verwalten möchten. Sollen beispielsweise mehrere Benutzergruppen mit unterschiedlichen Berechtigungsstufen eine App verwenden, benötigen Sie ggf. eigene Bereitstellungsgruppen, um zwei Versionen der App bereitzustellen. Darüber hinaus müssen Sie sicherstellen, dass sich die Benutzergruppenmitgliedschaft gegenseitig ausschließt, um Richtlinienkonflikte auf Benutzergeräten zu vermeiden.

Sie sollten ggf. auch die Lizenzierung von iOS-Apps über Apple Volume Purchase verwalten. Hierfür müssen Sie sich für Apple Volume Purchase registrieren und Volume Purchase-Einstellungen für XenMobile in der XenMobile-Konsole konfigurieren, um die Apps mit den Volume Purchase-Lizenzen zu verteilen. Bei vielen Anwendungsfällen muss die MAM-Strategie vor Implementierung der XenMobile-Umgebung bewertet und geplant werden. Die Planung Ihrer MAM-Strategie können Sie durch Aufstellung folgender Elemente beginnen:

App-Arten: Machen Sie eine Liste der verschiedenen App-Arten, die Sie unterstützen möchten, und teilen Sie sie in Kategorien ein. Beispiel: öffentliche Apps, native Apps, mobile Produktivitätsapps, Internet-Apps, interne Apps, ISV-Apps usw. Kategorisieren Sie die Apps auch nach Geräteplattform (z. B. iOS und Android). Die Kategorisierung hilft bei der Ausrichtung der XenMobile-Einstellungen für die einzelnen App-Typen. Manche Apps können beispielsweise nicht umschlossen werden oder benötigen für die Interaktion mit anderen Apps spezielle APIs, die über das Mobile Apps SDK aktiviert werden.

Netzwerkanforderungen: Konfigurieren Sie Apps mit bestimmten Netzwerkzugriffsanforderungen mit den entsprechenden Einstellungen. Beispielsweise erfordern bestimmte Apps möglicherweise Zugriff auf das interne Netzwerk über ein VPN. Andere Apps benötigen ggf. das Internet für das Zugriffsrouting über die DMZ. Damit solche Apps eine Verbindung mit dem gewünschten Netzwerk herstellen können, müssen Sie verschiedene Einstellungen entsprechend konfigurieren. Die Definition der Netzwerkanforderungen für die einzelnen Apps hilft Ihnen, Ihre Architekturentscheidungen frühzeitig zu treffen und verbessert so den gesamten Implementierungsprozess.

Sicherheitsanforderungen: Es ist unverzichtbar, die Sicherheitsanforderungen zu definieren, die für einzelne und/oder alle Apps gelten sollen. Diese Planung gewährleistet, dass Sie bei der Installation von XenMobile Server die richtigen Konfigurationen erstellen. Einstellungen wie MDX-Richtlinien

gelten zwar für einzelne Apps, Sitzungs- und Authentifizierungseinstellungen gelten jedoch für alle. Einige Apps haben möglicherweise besondere Anforderungen an Verschlüsselung, Containerization, Umschließen, Authentifizierung, Geofencing, Passcode oder Datenfreigabe, die Sie im Voraus umreißen können, um Ihre Bereitstellung zu vereinfachen.

Bereitstellungsvoraussetzungen: Über eine richtlinienbasierte Bereitstellung können Sie bei Bedarf dafür sorgen, dass nur berechtigte Benutzer die veröffentlichten Apps herunterladen können. Es kann beispielsweise sein, dass für bestimmte Apps eine oder mehrere der folgenden Bedingungen erfüllt sein müssen:

- Geräteplattformbasierte Verschlüsselung ist aktiviert
- Gerät wird verwaltet
- Gerät hat eine Mindestversion des Betriebssystems
- bestimmte Apps nur für Unternehmensbenutzer verfügbar

Außerdem können Sie festlegen, dass bestimmte Apps nur für Unternehmensbenutzer verfügbar sind. Stellen Sie solche Anforderungen im Voraus zusammen, damit Sie die entsprechenden Bereitstellungsregeln oder -aktionen konfigurieren können.

Lizenzanforderungen: Erstellen Sie eine Liste der Lizenzanforderungen für die Apps. Anhand dieser Liste können Sie die Lizenznutzung effektiv verwalten und entscheiden, ob Sie zur Vereinfachung der Lizenzierung bestimmte Features in XenMobile konfigurieren müssen. Wenn Sie beispielsweise eine kostenlose oder kostenpflichtige iOS-App bereitstellen, setzt Apple Lizenzanforderungen durch, indem Benutzer sich bei ihrem iTunes-Konto anmelden müssen. Sie können sich für Apple Volume Purchase registrieren, um solche Apps über XenMobile zu verteilen und zu verwalten. Über Volume Purchase können Benutzer die Apps ohne Anmeldung bei ihrem iTunes-Konto herunterladen. Außerdem müssen Tools wie Samsung SAFE und Samsung Knox spezielle Lizenzanforderungen erfüllen, bevor diese Funktionen bereitgestellt werden.

Anforderungen für Positiv- und Sperrlisten: Sie möchten wahrscheinlich das Installieren oder Verwenden mancher Apps unterbinden. Erstellen Sie eine Positivliste der Apps, mit denen ein Gerät seine Richtlinientreue verliert. Richten Sie anschließend Richtlinien ein, die ausgelöst werden, wenn ein Gerät nicht mehr richtlinientreu ist. Auf der anderen Seite kann die Verwendung einer App akzeptabel sein, die App jedoch aus einem bestimmten Grund unter die Sperrliste fallen. In dem Fall können Sie die App auf eine Positivliste setzen und angeben, dass sie akzeptabel ist, aber nicht benötigt wird. Bedenken Sie auch, dass auf neuen Geräten einige häufig verwendete Apps vorinstalliert sein können, die nicht Teil des Betriebssystems sind. Solche Apps könnten zu Konflikten mit Ihrer Sperrlistenstrategie führen.

Apps-Anwendungsfall

Eine Gesundheitsorganisation plant die Bereitstellung von XenMobile als MAM-Lösung für ihre mobilen Apps. Die Apps werden Benutzern mit Unternehmensgeräten und BYOD-Benutzern zur Verfü-

gung gestellt. Die IT entscheidet sich für die Bereitstellung und Verwaltung der folgenden Apps:

- **Mobile Produktivitätsapps:** iOS- und Android-Apps von Citrix.
- **Secure Mail:** E-Mail-, Kalender- und Kontakte-App.
- **Secure Web:** sicherer Webbrowser, der Zugriff auf das Internet und Intranetsites bietet.
- **Citrix Files:** App für den Zugriff auf geteilte Daten und zum Teilen, Synchronisieren und Bearbeiten von Dateien.

Öffentlicher App-Store

- **Secure Hub:** Client, der von allen Mobilgeräten zur Kommunikation mit XenMobile verwendet wird. Die IT überträgt über den Secure Hub-Client per Push Sicherheitseinstellungen, Konfigurationen und mobile Apps auf Mobilgeräte. Android- und iOS-Geräte registrieren sich über Secure Hub bei XenMobile.
- **Citrix Receiver:** mobile App, mit der Benutzer unter Virtual Apps and Desktops gehostete Apps auf Mobilgeräten öffnen können.
- **GoToMeeting:** Client für Online-Meetings, Desktopfreigabe und Videokonferenzen, mit dem Benutzer Besprechungen mit anderen Computerbenutzern, Kunden oder Kollegen über das Internet in Echtzeit abhalten können.
- **SalesForce1:** Mit Salesforce1 können Benutzer von Mobilgeräten aus auf Salesforce zugreifen. Die App vereint für Salesforce-Benutzer alle Chatter-, CRM- und benutzerdefinierten Apps sowie Geschäftsprozesse in einer einheitlichen Umgebung.
- **RSA SecurID:** softwarebasiertes Token für die zweistufige Authentifizierung.
- **EpicCare-Apps:** Apps für medizinisches Personal, mit denen sicher und mobil auf Patientendaten, Zeitpläne und Nachrichten zugegriffen werden kann.
  - **Haiku:** mobile App für iPhones und Android-Smartphones.
  - **Canto:** mobile App für iPads.
  - **Rover:** mobile Apps für iPhones und iPads.

HDX: Diese Apps werden über Citrix Virtual Apps and Desktops bereitgestellt.

- **Epic Hyperspace:** Epic-Client zur Verwaltung elektronischer Patientenakten.

ISV

- **Vocera:** HIPAA-kompatible Voice-over-IP- und Messaging-App, zur Nutzung der Vocera-Sprachtechnologie auf iPhones und Android-Smartphones.

Interne Apps

- **HCMail:** App zur Erstellung verschlüsselter Nachrichten, zum Durchsuchen von Adressbüchern auf internen Mailservern und zum Senden verschlüsselter Nachrichten über einen E-Mail-Client an Kontakte.

Interne Web-Apps

- **PatientRounding:** Web-App zur Erfassung von Patientendaten in verschiedenen Abteilungen.
- **Outlook Web Access:** ermöglicht den Zugriff auf E-Mails über einen Webbrowser.
- **SharePoint:** wird für die unternehmensweite Datei- und Datenfreigabe verwendet.

Die folgende Tabelle enthält die grundlegenden, für die MAM-Konfiguration erforderlichen Informationen.

App-Name	App-Typ	Mit MDX umschlossen	iOS	Android
Secure Mail	XenMobile App	Ab Version 10.4.1 nein	Ja	Ja
Secure Web	XenMobile App	Ab Version 10.4.1 nein	Ja	Ja
Citrix Files	XenMobile App	Ab Version 10.4.1 nein	Ja	Ja
Secure Hub	Öffentliche App	Nicht verfügbar	Ja	Ja
Citrix Receiver	Öffentliche App	Nicht verfügbar	Ja	Ja
GoToMeeting	Öffentliche App	Nicht verfügbar	Ja	Ja
SalesForce1	Öffentliche App	Nicht verfügbar	Ja	Ja
RSA SecurID	Öffentliche App	Nicht verfügbar	Ja	Ja
Epic Haiku	Öffentliche App	Nicht verfügbar	Ja	Ja
Epic Canto	Öffentliche App	Nicht verfügbar	Ja	Nein
Epic Rover	Öffentliche App	Nicht verfügbar	Ja	Nein
Epic Hyperspace	HDX-App	Nicht verfügbar	Ja	Ja
Vocera	ISV-App	Ja	Ja	Ja
HCMail	Interne App	Ja	Ja	Ja
PatientRounding	Web-App	Nicht verfügbar	Ja	Ja
Outlook Web Access	Web-App	Nicht verfügbar	Ja	Ja
SharePoint	Web-App	Nicht verfügbar	Ja	Ja

In den folgenden Tabellen sind spezifische Anforderungen aufgeführt, die Sie bei der Konfiguration

von MAM-Richtlinien in XenMobile konsultieren können.

App-Name	**VPN erforderlich**	**Interaktion**	**Interaktion**	**Geräteplattformbasierte Verschlüsselung**
		(mit Apps außerhalb des Containers)	**(von Apps außerhalb des Containers)**	
————	—	————————	————————	————
Secure Mail	J	Selektiv zugelassen	Zugelassen	Nicht erforderlich
Secure Web	J	Zugelassen	Zugelassen	Nicht erforderlich
Citrix Files	J	Zugelassen	Zugelassen	Nicht erforderlich
Secure Hub	J	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Citrix Receiver	J	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
GoToMeeting	N	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
SalesForce1	N	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
RSA SecurID	N	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Epic Haiku	J	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Epic Canto	J	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Epic Rover	J	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Epic Hyperspace	J	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Vocera	J	Blockiert	Blockiert	Nicht erforderlich
HCMail	J	Blockiert	Blockiert	Erforderlich
PatientRounding	J	Nicht zutreffend	Nicht zutreffend	Erforderlich
Outlook Web Access	J	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich
SharePoint	J	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich

App-Name	Proxy-Filter	Lizenzierung	Geofencing	Mobile Apps SDK	Mindestversion des Betriebssystems
Secure Mail	Erforderlich	Nicht zutreffend	Selektiv erforderlich	Nicht zutreffend	Erzwungen
Secure Web	Erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Erzwungen
Citrix Files	Erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Erzwungen
Secure Hub	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Citrix Receiver	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
GoToMeeting	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen

App-Name	Proxy-Filter	Lizenzierung	Geofencing	Mobile Apps SDK	Mindestversion des Betriebssystems
SalesForce1	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
RSA SecurID	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Epic Haiku	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Epic Canto	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Epic Rover	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Epic Hyperspace	Nicht erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Vocera	Erforderlich	Nicht zutreffend	Erforderlich	Erforderlich	Erzwungen
HCMail	Erforderlich	Nicht zutreffend	Erforderlich	Erforderlich	Erzwungen
PatientRoundir	Erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Outlook Web Access	Erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
SharePoint	Erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen

Benutzergemeinschaften

Jede Organisation besteht aus mehreren Benutzergemeinschaften, die unterschiedliche funktionelle Rollen besitzen. Diese Benutzergemeinschaften führen unterschiedliche Aufgaben und Bürofunktionen aus und nutzen diverse Ressourcen, die Sie über die Mobilgeräte bereitstellen. Manche Benutzer arbeiten von zu Hause oder an Remotestandorten und verwenden dabei die von Ihnen bereitgestellten Mobilgeräte. Andere Benutzer greifen über private Mobilgeräte auf Tools zu, für die bestimmte Regeln zur Sicherheitskonformität gelten.

Je mehr Benutzergemeinschaften mit Mobilgeräten arbeiten, desto bedeutender wird das Enterprise Mobility Management (EMM), um Datenverluste zu verhindern und Sicherheitsbeschränkungen

durchzusetzen. Im Interesse einer effizienten und differenzierten Mobilgeräteverwaltung können Sie Benutzergemeinschaften auch in Kategorien unterteilen. Dies vereinfacht die Zuordnung von Benutzern zu Ressourcen und stellt sicher, dass die richtigen Sicherheitsrichtlinien angewandt werden.

Das folgende Beispiel zeigt, wie Benutzergemeinschaften in einer US-Organisation im Gesundheitssektor für EMM klassifiziert werden.

Anwendungsfall Benutzergemeinschaften

Dieses Klinikunternehmen bietet technologische Ressourcen und Zugriffsrechte für verschiedene Benutzer, darunter angestellte, externe und ehrenamtliche Mitarbeiter. Die Organisation plant, die EMM-Lösung nur für Benutzer bereitzustellen, die nicht zur Geschäftsleitung gehören.

Die Benutzerrollen und -funktionen im Unternehmen können in folgende Untergruppen unterteilt werden: Klinik, Verwaltung, Extern. Einige Benutzer erhalten firmeneigene Mobilgeräte, während andere über Privatgeräte eingeschränkt Zugriff auf Unternehmensressourcen haben. Um Sicherheitsbeschränkungen angemessen umzusetzen und Datenlecks zu vermeiden, soll das IT-Team der Organisation jedes registrierte (Unternehmens- oder BYOD-)Gerät verwalten. Benutzer können zudem nur jeweils ein Gerät registrieren.

Der folgende Abschnitt bietet einen Überblick über die Rollen und Funktionen der einzelnen Untergruppen:

Klinik

- Pflegepersonal
- Mediziner (Ärzte, Chirurgen usw.)
- Fachärzte (Anästhesisten, Radiologen, Kardiologen, Onkologen usw.)
- Externe Mediziner (nicht angestellte Ärzte und Büromitarbeiter an Remotestandorten)
- Hausbesuchsdienste (Büropersonal und mobile Mitarbeiter, die arztbezogene Dienste für Hausbesuche bei Patienten durchführen)
- Forschungsspezialisten (Wissensarbeiter und Hauptbenutzer in sechs Forschungsinstituten, die in der klinischen Forschung tätig sind und medizinische Studien durchführen)
- Schulungen, Aus- und Weiterbildung (Pflegepersonal, Mediziner und Pädagogen)

Verwaltung

- Gemeinsam genutzte Dienste (Büromitarbeiter, die verschiedene Backoffice-Funktionen ausführen, z. B. Personalabteilung, Gehaltsabrechnung, Kreditorenbuchhaltung, Einkauf und Logistik usw.)

- Arztbezogene Dienste (Büromitarbeiter, die verschiedene Aufgaben im Bereich Gesundheitsmanagement und Administration ausüben und Geschäftsprozesslösungen für Anbieter bereitstellen. Dazu gehören Verwaltung und Geschäftsanalytik, Geschäftssysteme, Serviceangebote für Kunden und Patienten, Finanzwesen, Managed Care, Rentabilitätslösungen usw.)
- Supportdienste (Büromitarbeiter, die Funktionen in verschiedenen nichtklinischen Bereichen ausüben: Arbeitgeberleistungen, klinische Integration, Kommunikation, Vergütung, Gebäudemanagement, Technologiesysteme für die Personalabteilung, Informationsdienste, internes Audit und Prozessoptimierung usw.)
- Gemeinnützige Stiftungen (Büromitarbeiter und mobile Mitarbeiter, die verschiedene Funktionen im Rahmen philanthropischer Programme ausüben)

Auftragnehmer

- Hersteller und Vertriebspartner (Bereitstellung diverser nicht-klinischer Supportfunktionen vor Ort und remote über Site-to-Site-VPN)

Auf der Grundlage dieser Informationen hat die Organisation folgende Entitäten erstellt. Weitere Informationen zu Bereitstellungsgruppen in XenMobile finden Sie unter Bereitstellen von Ressourcen.

Active Directory-Organisationseinheiten (OUs) und -Gruppen

Für OU **=** XenMobile-Ressourcen:

- OU = Klinik; Gruppen =
  - XM - Pflegepersonal
  - XM - Mediziner
  - XM - Fachärzte
  - XM - Externe Mediziner
  - XM - Hausbesuchsdienste
  - XM - Forschungsspezialisten
  - XM - Schulungen, Aus- und Weiterbildung
- OU = Verwaltung; Gruppen =
  - XM - Gemeinsam genutzte Dienste
  - XM - Arztbezogene Dienste
  - XM - Supportdienste
  - XM - Gemeinnützige Stiftungen

Lokale XenMobile-Benutzer und -Gruppen

Für Gruppe = Auftragnehmer, Benutzer =

- Anbieter 1

- Anbieter 2
- Anbieter 3
- … Anbieter 10

XenMobile-Bereitstellungsgruppen

- Klinik - Pflegepersonal
- Klinik - Mediziner
- Klinik - Fachärzte
- Klinik - Externe Mediziner
- Klinik - Hausbesuchsdienste
- Klinik - Forschungsspezialisten
- Klinik - Schulungen, Aus- und Weiterbildung
- Verwaltung - Gemeinsam genutzte Dienste
- Verwaltung - Arztbezogene Dienste
- Verwaltung - Supportdienste
- Verwaltung - Gemeinnützige Stiftungen

Zuordnung von Bereitstellungsgruppe und Benutzergruppe

Active Directory-Gruppen	XenMobile-Bereitstellungsgruppen
XM - Pflegepersonal	Klinik - Pflegepersonal
XM - Mediziner	Klinik - Mediziner
XM - Fachärzte	Klinik - Fachärzte
XM - Externe Mediziner	Klinik - Externe Mediziner
XM - Hausbesuchsdienste	Klinik - Hausbesuchsdienste
XM - Forschungsspezialisten	Klinik - Forschungsspezialisten
XM - Schulungen, Aus- und Weiterbildung	Klinik - Schulungen, Aus- und Weiterbildung
XM - Gemeinsam genutzte Dienste	Verwaltung - Gemeinsam genutzte Dienste
XM - Arztbezogene Dienste	Verwaltung - Arztbezogene Dienste
XM - Supportdienste	Verwaltung - Supportdienste
XM - Gemeinnützige Stiftungen	Verwaltung - Gemeinnützige Stiftungen

Bereitstellungsgruppen und Ressourcenzuordnung

Die folgenden Tabellen zeigen, welche Ressourcen in diesem Anwendungsfall welcher Bereitstellungsgruppe zugeordnet sind. Die erste Tabelle zeigt die Zuweisungen für mobile Apps. Die zweite Tabelle zeigt die Zuweisung öffentlicher Apps, von HDX-Apps und von Geräteverwaltungsressourcen.

XenMobile-Bereitstellungsgruppe	Mobile Apps von Citrix	Öffentliche mobile Apps	Mobile HDX-Apps
Klinik - Pflegepersonal	X		
Klinik - Mediziner			
Klinik - Fachärzte			
Klinik - Externe Mediziner	X		
Klinik - Hausbesuchsdienste	X		
Klinik - Forschungsspezialisten	X		
Klinik - Schulungen, Aus- und Weiterbildung		X	X
Verwaltung - Gemeinsam genutzte Dienste		X	X
Verwaltung - Arztbezogene Dienste		X	X
Verwaltung - Supportdienste	X	X	X
Verwaltung - Gemeinnützige Stiftungen	X	X	X
Auftragnehmer	X	X	X

XenMobile Bereitstell	Öffentliche App: RSA SecurID	Öffentliche App: EpicCare Haiku	HDX-App: Epic Hyperspace	Passcoderi	Geräteeins	Automatisi Aktionen	Wi-Fi-Richtlinie
Klinik - Pflegepersonal							X
Klinik - Mediziner					X		
Klinik - Fachärzte							
Klinik - Externe Mediziner							
Klinik - Hausbesuchsdienste							
Klinik - Forschungsisten							
Klinik - Schulungen, Aus- und Weiterbildung		X	X				
Verwaltung - Gemeinsam genutzte Dienste		X	X				
Verwaltung - Arztbezogene Dienste		X	X				

Verwaltung - Support-dienste	X	X

Hinweise und Überlegungen

- XenMobile erstellt bei der Erstkonfiguration die Standardbereitstellungsgruppe “Alle Benutzer”. Wenn Sie diese Bereitstellungsgruppe nicht deaktivieren, sind alle Active Directory-Benutzer berechtigt, sich in XenMobile zu registrieren.
- XenMobile synchronisiert Active Directory-Benutzer und -Gruppen bei Bedarf über eine dynamische Verbindung mit dem LDAP-Server.
- Wenn ein Benutzer zu einer Gruppe gehört, die nicht in XenMobile zugeordnet ist, kann der Benutzer sich nicht registrieren. Wenn ein Benutzer Mitglieder mehrerer Gruppen ist, kategorisiert XenMobile den Benutzer nur als Mitglied der Gruppen, die in XenMobile zugeordnet sind.
- Für eine verbindliche MDM-Registrierung müssen Sie in der XenMobile-Konsole unter “Servereigenschaften” für die Option “Registrierung erforderlich” die Einstellung “Wahr” auswählen. Einzelheiten finden Sie unter Servereigenschaften.
- Sie können eine Benutzergruppe aus einer XenMobile-Bereitstellungsgruppe löschen, indem Sie den Eintrag in der SQL Server-Datenbank unter dbo.userlistgrps löschen.
  Achtung: Erstellen Sie ein Backup von XenMobile und der Datenbank, bevor Sie diese Aktion durchführen.

Geräteeigentümerschaft in XenMobile

Sie können Benutzer auch nach Eigentümer eines Benutzergeräts gruppieren. Es gibt unternehmenseigene Geräte und solche, die Benutzern gehören. Letztere werden auch als BYOD-Geräte (von “bring your own device”) bezeichnet. Sie können in zwei Bereichen der XenMobile-Konsole steuern, wie BYOD-Geräte eine Verbindung mit dem Netzwerk herstellen: in den Bereitstellungsregeln für jeden Ressourcentyp und über die XenMobile Server-Eigenschaften auf der Seite **Einstellungen**. Weitere Informationen zu Bereitstellungsregeln finden Sie in der Dokumentation zu XenMobile unter Konfigurieren von Bereitstellungsregeln. Weitere Informationen über Servereigenschaften finden Sie unter Servereigenschaften.

Sie können festlegen, dass alle BYOD-Benutzer die Verwaltung ihrer Geräte durch das Unternehmen akzeptieren müssen, bevor sie Zugriff auf Apps erhalten. Alternativ können Sie Benutzern auch ohne Verwaltung ihrer Geräte Zugriff auf Unternehmensapps erteilen.

Wenn Sie die Servereinstellung **wsapi.mdm.required.flag** auf **true** festlegen, werden alle BYOD-Geräte von XenMobile verwaltet und Benutzer, die eine Registrierung ablehnen, erhalten keinen

Zugriff auf Apps. Erwägen Sie das Festlegen von **wsapi.mdm.required.flag** auf **true** in Umgebungen, in denen neben einer hohen Sicherheit eine gute Benutzererfahrung bei der Registrierung der Geräte in XenMobile erforderlich ist.

Wenn Sie die Einstellung nicht ändern und die Standardeinstellung **false** für **wsapi.mdm.required.flag** übernehmen, können Benutzer die Registrierung ablehnen und dennoch ggf. mit ihrem Gerät auf Apps über den XenMobile Store zugreifen. Das Festlegen von **wsapi.mdm.required.flag** auf **false** eignet sich für Umgebungen, in denen juristische und datenschutzrechtliche Vorgaben keine Verwaltung von Geräten erfordern, sondern nur die Verwaltung von Unternehmensapps.

Benutzer mit nicht von XenMobile verwalteten Geräten können Apps über den XenMobile Store installieren. Anstelle einer Steuerung auf Gerätebasis, etwa der selektiven oder vollständigen Löschung der Daten auf einem Gerät, steuern Sie den Zugriff auf Apps über App-Richtlinien. Je nach Einstellung erfordern die Richtlinien, dass Geräte regelmäßig den XenMobile-Server abfragen, um sicherzustellen, dass Apps weiterhin zugelassen sind.

Sicherheitsanforderungen

Die Zahl der bei der Bereitstellung einer XenMobile-Umgebung zu beachtenden Sicherheitsaspekte kann schnell zu einer Herausforderung werden. Es gibt viele ineinandergreifende Elemente und Einstellungen. Um Ihnen die Auswahl eines akzeptablen Schutzniveaus zu erleichtern, macht Citrix Empfehlungen für hohe, höhere und höchste Sicherheit (siehe folgende Tabelle).

Bei der Wahl des Bereitstellungsmodus sind über die Sicherheit hinaus weitere Aspekte zu berücksichtigen. Sie müssen auch die Anforderungen des Anwendungsfalls bedenken und überlegen, ob Sie Sicherheitsbedenken ausräumen können.

Hoch: Die Verwendung dieser Einstellungen bietet die optimale Benutzererfahrung bei gleichzeitiger Gewährleistung einer einfachen, für die meisten Organisationen akzeptablen Sicherheitsstufe.

Höher: Diese Einstellungen bewirken ein ausgeglicheneres Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit.

Höchste: Die Einhaltung dieser Empfehlungen bietet ein hohes Maß an Sicherheit auf Kosten von Benutzerfreundlichkeit und Benutzerakzeptanz.

Bereitstellungsmodus – Sicherheitsüberlegungen

Die folgende Tabelle enthält die Bereitstellungsmodi für jede Sicherheitsstufe.

Hohe Sicherheit	Höhere Sicherheit	Höchste Sicherheit
MAM oder MDM	MDM+MAM	MDM+MAM, plus FIPS

Hinweise:

- Je nach Anwendungsfall kann eine Nur-MDM- oder Nur-MAM-Bereitstellung die Sicherheitsanforderungen erfüllen und eine gute Benutzererfahrung bieten.
- Wenn keine App-Containerization, kein Micro-VPN- und keine App-spezifischen Richtlinien erforderlich sind, reicht MDM zur Verwaltung und zum Schützen von Geräten aus.
- Für Anwendungsfälle wie BYOD, bei denen alle geschäftlichen und Sicherheitsanforderungen mit bloßer App-Containerization erfüllt werden können, empfiehlt Citrix den Nur-MAM-Modus.
- Für Umgebungen mit hoher Sicherheit (und vom Unternehmen gestellten Geräten) empfiehlt Citrix MDM+MAM zur Nutzung aller verfügbaren Sicherheitsfunktionen. Stellen Sie sicher, dass Sie die MDM-Registrierung erzwingen.
- FIPS-Optionen für Umgebungen mit höchsten Sicherheitsanforderungen, z. B. Regierungsbehörden.

Wenn Sie den FIPS-Modus aktivieren, müssen Sie SQL Server für die Verschlüsselung des SQL-Datenverkehrs konfigurieren.

Citrix ADC und Citrix Gateway – Sicherheitsüberlegungen

Die folgende Tabelle enthält Empfehlungen für Citrix ADC und Citrix Gateway für jede Sicherheitsstufe.

Hohe Sicherheit	Höhere Sicherheit	Höchste Sicherheit
Citrix ADC wird empfohlen. Citrix Gateway ist für MAM und ENT erforderlich und wird für MDM empfohlen.	Standardkonfiguration von Citrix ADC für XenMobile-Assistenten mit SSL-Brücke, wenn XenMobile in der DMZ ist. Oder SSL-Offload, sofern dies zur Erfüllung von Sicherheitsstandards erforderlich ist, wenn XenMobile Server im internen Netzwerk ist.	SSL-Offload mit End-to-End-Verschlüsselung

Hinweise:

- Bei MDM kann der XenMobile-Server nach Wahl über NAT, Drittanbieter-Proxys oder Load Balancer dem Internet ausgesetzt werden. Diese Konfiguration erfordert jedoch, dass der SSL-Datenverkehr auf dem XenMobile-Server endet, was ein Sicherheitsrisiko bedeutet.

- In Umgebungen mit hoher Sicherheit erfüllt oder übertrifft Citrix ADC mit der standardmäßigen XenMobile-Konfiguration normalerweise die Sicherheitsanforderungen.
- Für MDM-Umgebungen mit höchsten Sicherheitsanforderungen ermöglicht die SSL-Terminierung am Citrix ADC die Datenverkehrsprüfung am Umkreis und gewährleistet eine durchgängige SSL-Verschlüsselung.
- Optionen zum Definieren von SSL-/TLS-Verschlüsselungsverfahren.
- SSL FIPS Citrix ADC-Hardware ist ebenfalls verfügbar.
- Weitere Information finden Sie unter Integration in Citrix Gateway und Citrix ADC.

Registrierung – Sicherheitsüberlegungen

Die folgende Tabelle enthält Empfehlungen für Citrix ADC und Citrix Gateway für jede Sicherheitsstufe.

Hohe Sicherheit	Höhere Sicherheit	Höchste Sicherheit
Nur Active Directory-Gruppenmitgliedschaft. Bereitstellungsgruppe “Alle Benutzer” deaktiviert.	Sicherheitsmodus mit Registrierung nur auf Einladung. Nur Active Directory-Gruppenmitgliedschaft. Bereitstellungsgruppe “Alle Benutzer” deaktiviert.	Registrierungssicherheitsmodus mit Bindung an Geräte-ID. Nur Active Directory-Gruppenmitgliedschaft. Bereitstellungsgruppe “Alle Benutzer” deaktiviert.

Hinweise:

- Citrix empfiehlt generell, die Registrierung auf Benutzer in vordefinierten Active Directory-Gruppen zu beschränken. Hierfür muss die integrierte Bereitstellungsgruppe “Alle Benutzer” deaktiviert werden.
- Mit Registrierungseinladungen können Sie die Registrierung auf Benutzer beschränken, die eine Einladung erhalten haben. Registrierungseinladungen sind für Windows-Geräte nicht verfügbar.
- Sie können Registrierungseinladungen mit Einmal-PIN (OTP) als Lösung für die zweistufige Authentifizierung nutzen und vorgeben, wie viele Geräte jeder Benutzer registrieren kann. OTP-Einladungen sind für Windows-Geräte nicht verfügbar.

Überlegungen zur Sicherheit von Gerätepasscodes

Die folgende Tabelle enthält Empfehlungen für den Gerätepasscode für jede Sicherheitsstufe.

Hohe Sicherheit	Höhere Sicherheit	Höchste Sicherheit
Empfohlen. Für die Verschlüsselung auf Geräteebene ist hohe Sicherheit erforderlich. Über MDM erzwungen. Sie können hohe Sicherheit für Nur-MAM-Umgebungen über die MDX-Richtlinie “Verhalten für nicht richtlinientreue Geräte” erzwingen.	Über eine MDM, eine MDX-Richtlinie oder beides erzwungen.	Wird über eine MDM- und MDX-Richtlinie erzwungen. MDM-Richtlinie “Komplexer Passcode”.

Hinweise:

- Citrix empfiehlt die Verwendung eines Gerätepasscodes.
- Sie können die Verwendung von Gerätepasscodes über eine MDM-Richtlinie erzwingen.
- Sie können über eine MDX-Richtlinie festlegen, dass ein Gerätepasscode Voraussetzung für die Verwendung verwalteter Apps ist. Zum Beispiel für BYOD-Anwendungsfälle.
- Citrix empfiehlt, die Kombination von MDM- und MDX-Richtlinien zur größeren Sicherheit in MDM+MAM-Umgebungen.
- In Umgebungen mit höchsten Sicherheitsanforderungen können Sie Richtlinien für komplexe Passcodes konfigurieren und über MDM erzwingen. Sie können automatische Aktionen konfigurieren, um Administratoren zu benachrichtigen oder selektive/vollständige Gerätelöschungen zu veranlassen, wenn ein Gerät einer Passcoderichtlinie nicht entspricht.

Apps

January 5, 2022

Das Enterprise Mobility Management (EMM) besteht aus dem Mobile Device Management (MDM) und dem Mobile Application Management (MAM). Mit MDM können Unternehmen Mobilgeräte schützen und steuern und MAM erleichtert die Bereitstellung und Verwaltung von Apps. Zur Unterstützung der BYOD-Nutzung können Sie mit einer MAM-Lösung wie XenMobile in der Regel Folgendes erleichtern:

- Anwendungsbereitstellung
- Softwarelizenzierung
- Konfiguration

- Awendungslebenszyklus-Management

Sie können vorschreiben oder zulassen, dass Benutzer sich auch für die MDM-Verwaltung entscheiden können.

Mit XenMobile können Sie diese Apps noch sicherer machen, indem Sie bestimmte MAM-Richtlinien und VPN-Einstellungen konfigurieren, um Datenlecks und andere Sicherheitsbedrohungen zu vermeiden. Mit XenMobile können Unternehmen ihre Lösung flexibel in einer der folgenden Formen bereitstellen:

- Nur-MAM-Umgebung
- Nur-MDM-Umgebung
- Einheitliche XenMobile Enterprise-Umgebung mit MDM- und MAM-Funktionen

Zusätzlich zur App-Bereitstellung für Mobilgeräte ermöglicht XenMobile die App-Containerization per MDX-Technologie. Die Apps unterliegen einer detaillierten richtlinienbasierten Steuerung. Unabhängige Softwarehersteller (ISV) können diese Steuerelemente über das Mobile Apps SDK anwenden.

In Unternehmensumgebungen verwenden Benutzer eine Reihe von mobilen Apps für ihre Arbeit. Dabei kann es sich um Apps aus einem öffentlichen App-Store, um unternehmensintern entwickelte Apps oder native Apps handeln. In XenMobile werden Apps wie folgt kategorisiert:

- **Öffentliche Apps:** Kostenlose oder kostenpflichtige Apps in einem öffentlichen App-Store, z. B. Apple App Store oder Google Play. Unternehmensexterne Hersteller bieten ihre Apps häufig in öffentlichen App-Stores an. Die Kunden können solche Apps direkt aus dem Internet herunterladen. Je nach Bedarf werden in einem Unternehmen u. U. zahlreiche öffentliche Apps in verwendet. Beispiele für solche Apps sind GoToMeeting, Salesforce und EpicCare.
  - **Bei Verwendung des MAM-SDK:** Sie erhalten die App-Binärdateien von Ihrem App-Anbieter. Integrieren Sie dann das MAM-SDK in die App.
  - **Bei Verwendung des MDX Toolkit:** Citrix unterstützt nicht das direkte Herunterladen von App-Binärdateien aus öffentlichen App-Stores und das anschließende Umschließen mit dem MDX Toolkit zur Verteilung im Unternehmen. Um Apps von Drittanbietern zu umschließen, wenden Sie sich an den App-Anbieter, um die Binärdateien zu erhalten. Sie können dann die Binärdateien mit dem MDX Toolkit umschließen.
- **Intern entwickelte Apps:** In vielen Unternehmen gibt es interne Entwickler, die Apps für spezifische Zwecke und zur unabhängigen Verteilung im Unternehmen entwickeln. In manchen Fällen haben Unternehmen auch Apps von ISV. Sie können solche Apps als native Apps bereitstellen oder mithilfe einer MAM-Lösung wie XenMobile eine Containerization durchführen.

  Beispielsweise kann eine Gesundheitsorganisation eine interne App erstellen, mit der Ärzte Patientendaten auf Mobilgeräten anzeigen können. Die Organisation kann dann mit einem der

folgenden Verfahren die Patientendaten schützen und den VPN-Zugriff auf die Patientendatenbank ermöglichen.

  - MAM-SDK
  - MDX Toolkit

- **Web- und SaaS-Apps:** Apps, auf die über ein internes Netzwerk (Web-Apps) oder ein öffentliches Netzwerk (SaaS-Apps) zugegriffen wird. Mit XenMobile können Sie auch benutzerdefinierte Web- und SaaS-Apps unter Einsatz mehrerer App-Connectors erstellen. Die App-Connectors können das Single Sign-On (SSO) für bestehende Web-Apps vereinfachen. Weitere Informationen finden Sie unter App-Connectortypen. Sie können beispielsweise Google Apps SAML für das SSO basierend auf SAML (Security Assertion Markup Language) für Google Apps verwenden.
- **Mobile Produktivitätsapps:** Mobile Produktivitätsapps sind von Citrix entwickelte Apps, die in der XenMobile-Lizenz enthalten sind. Weitere Informationen finden Sie unter Mobile Produktivitätsapps. Citrix bietet auch andere Citrix Ready-Apps an, die ISV mit dem Mobile Apps SDK entwickelt haben.
- **HDX-Apps:** HDX-Apps sind unter Windows gehostete Apps, die mit StoreFront veröffentlicht werden. Wenn Sie Citrix Virtual Apps and Desktops und Citrix Workspace verwenden, stehen HDX-Apps für registrierte Benutzer zur Verfügung.

Die zugrunde liegende Konfiguration hängt von der Art der Apps ab, die Sie mit XenMobile bereitstellen und verwalten möchten. Beispiel: Mehrere Benutzergruppen mit unterschiedlichen Berechtigungsstufen sollen eine einzige App verwenden. In dem Fall können Sie separate Bereitstellungsgruppen erstellen, um zwei separate Versionen der App bereitzustellen. Darüber hinaus müssen Sie sicherstellen, dass sich die Benutzergruppenmitgliedschaft gegenseitig ausschließt, um Richtlinienkonflikte auf Benutzergeräten zu vermeiden.

Sie können die Lizenzierung von iOS-Apps auch über Apple Volume Purchase verwalten. Hierfür müssen Sie sich für das Volume Purchase-Programm registrieren und Volume Purchase-Einstellungen in der XenMobile-Konsole konfigurieren. Mit dieser Konfiguration können Sie die Apps mit den Volume Purchase-Lizenzen verteilen. Bei vielen Anwendungsfällen muss die MAM-Strategie vor Implementierung der XenMobile-Umgebung bewertet und geplant werden. Die Planung Ihrer MAM-Strategie können Sie durch Aufstellung folgender Elemente beginnen:

- **Arten von Apps:** Machen Sie eine Liste der Apps, die Sie unterstützen möchten, und kategorisieren Sie sie (öffentliche, native, interne Apps, Web- oder ISV-Apps). Kategorisieren Sie die Apps auch nach Geräteplattform (z. B. iOS und Android). Die Kategorisierung hilft bei der Definition der verschiedenen XenMobile-Einstellungen für die einzelnen App-Typen. Manche Apps benötigen beispielsweise für die Interaktion mit anderen Apps spezielle APIs, die über das Mobile Apps SDK aktiviert werden.
- **Netzwerkanforderungen:** Konfigurieren Sie die Einstellungen von Apps, für die bestimmte

Netzwerkzugriffsanforderungen gelten. Beispielsweise erfordern bestimmte Apps möglicherweise Zugriff auf das interne Netzwerk über ein VPN. Andere Apps benötigen ggf. das Internet für das Zugriffsrouting über die DMZ. Damit solche Apps eine Verbindung mit dem gewünschten Netzwerk herstellen können, müssen Sie verschiedene Einstellungen entsprechend konfigurieren. Die Definition der Netzwerkanforderungen für die einzelnen Apps hilft Ihnen, Ihre Architekturentscheidungen frühzeitig zu treffen und verbessert so den gesamten Implementierungsprozess.

- **Sicherheitsanforderungen:** Sie können Sicherheitsanforderungen definieren, die entweder für einzelne Apps oder für alle Apps gelten.
  - Einstellungen, z. B. die MDX-Richtlinien, gelten für einzelne Apps
  - Sitzungs- und Authentifizierungseinstellungen gelten für alle Apps
  - Einige Apps stellen möglicherweise besondere Anforderungen an Containerization, MDX, Authentifizierung, Geofencing, Passcode oder Datenfreigabe.

  Stellen Sie im Voraus eine Übersicht über diese Anforderungen zusammen, um Ihre Bereitstellung zu vereinfachen. Weitere Informationen zur Sicherheit in Endpoint Management finden Sie unter Sicherheit und Benutzererfahrung.

- **Bereitstellungsvoraussetzungen:** Über eine richtlinienbasierte Bereitstellung können Sie bei Bedarf dafür sorgen, dass nur berechtigte Benutzer die veröffentlichten Apps herunterladen können. Beispielsweise könnte für bestimmte Apps erforderlich sein, dass Geräte verwaltet werden oder auf den Geräten eine Mindestversion des Betriebssystems ausgeführt wird. Außerdem können Sie festlegen, dass bestimmte Apps nur für Unternehmensbenutzer verfügbar sind. Stellen Sie solche Anforderungen im Voraus zusammen, damit Sie die entsprechenden Bereitstellungsregeln oder -aktionen konfigurieren können.

- **Lizenzanforderungen:** Erstellen Sie eine Liste der Lizenzanforderungen für die Apps. Anhand dieser Liste können Sie die Lizenznutzung effektiv verwalten und entscheiden, ob Sie zur Vereinfachung der Lizenzierung bestimmte Features in XenMobile konfigurieren müssen. Wenn Sie beispielsweise eine kostenlose oder kostenpflichtige iOS-App bereitstellen, setzt Apple spezielle Lizenzanforderungen durch. Benutzer müssen sich dann bei ihrem Apple App Store-Konto anmelden.

  Wenn Sie sich bei Apple Volume Purchase registrieren, können Sie solche Apps über XenMobile verteilen und verwalten. Über Volume Purchase können Benutzer die Apps ohne Anmeldung bei ihrem Apple App Store-Konto herunterladen.

  Einige Plattformen wie Samsung SAFE und Samsung Knox stellen spezielle Lizenzanforderungen, die zu erfüllen sind, bevor diese Funktionen bereitgestellt werden.

- **Anforderungen für Positiv- und Sperrlisten:** Sie können Apps kennzeichnen, die von Benutzern nicht installiert oder verwendet werden sollen. Durch das Erstellen einer Sperrliste wird ein “nicht richtlinientreu”-Ereignis definiert. Sie können dann Richtlinien einrichten, die

ausgelöst werden, wenn das Ereignis eintritt. Auf der anderen Seite kann die Verwendung einer App akzeptabel sein, die App jedoch aus einem bestimmten Grund unter die Sperrliste fallen. In dem Fall können Sie die App auf eine Positivliste setzen und angeben, dass sie akzeptabel ist aber nicht benötigt wird. Bedenken Sie auch, dass auf neuen Geräten einige häufig verwendete Apps vorinstalliert sein können, die nicht Teil des Betriebssystems sind. Solche Apps können zu Konflikten mit Ihrer Sperrlistenstrategie führen.

Anwendungsfall

Eine Gesundheitsorganisation plant die Bereitstellung von XenMobile als MAM-Lösung für ihre mobilen Apps. Die Apps werden Benutzern mit Unternehmensgeräten und BYOD-Benutzern zur Verfügung gestellt. Die IT entscheidet sich für die Bereitstellung und Verwaltung der folgenden Apps:

Mobile Produktivitätsapps: iOS- und Android-Apps von Citrix. Weitere Informationen finden Sie unter Mobile Produktivitätsapps.

Citrix Secure Hub: Client, der von allen Mobilgeräten zur Kommunikation mit XenMobile verwendet wird. Sie übertragen über Secure Hub per Push Sicherheitseinstellungen, Konfigurationen und mobile Apps auf Mobilgeräte. Android- und iOS-Geräte registrieren sich über Secure Hub bei XenMobile.

Citrix Receiver: mobile App, mit der Benutzer unter Citrix Virtual Apps gehostete Apps auf Mobilgeräten öffnen können.

GoToMeeting: Client für Online-Meetings, Desktopfreigabe und Videokonferenzen, mit dem Benutzer Besprechungen mit anderen Computerbenutzern, Kunden oder Kollegen über das Internet in Echtzeit abhalten können.

SalesForce1: Mit Salesforce1 können Benutzer von Mobilgeräten aus auf Salesforce zugreifen. Die App vereint für Salesforce-Benutzer alle Chatter-, CRM- und benutzerdefinierten Apps sowie Geschäftsprozesse in einer einheitlichen Umgebung.

RSA SecurID: softwarebasiertes Token für die zweistufige Authentifizierung.

EpicCare-Apps: Apps für medizinisches Personal, mit denen sicher und mobil auf Patientendaten, Zeitpläne und Nachrichten zugegriffen werden kann.

Haiku: mobile App für iPhones und Android-Smartphones.

Canto: mobile App für iPads.

Rover: mobile Apps für iPhones und iPads.

HDX: HDX-Apps werden über Citrix Virtual Apps bereitgestellt.

- **Epic Hyperspace:** Epic-Client zur Verwaltung elektronischer Patientenakten.

ISV:

- **Vocera:** HIPAA-kompatible Voice-over-IP- und Messaging-App, zur Nutzung der Vocera-Sprachtechnologie auf iPhones und Android-Smartphones.

Interne Apps:

- **HCMail:** App zur Erstellung verschlüsselter Nachrichten, zum Durchsuchen von Adressbüchern auf internen Mailservern und zum Senden verschlüsselter Nachrichten über einen E-Mail-Client an Kontakte.

Interne Web-Apps:

- **PatientRounding:** Web-App zur Erfassung von Patientendaten in verschiedenen Abteilungen.
- **Outlook Web Access:** ermöglicht den Zugriff auf E-Mails über einen Webbrowser.
- **SharePoint:** wird für die unternehmensweite Datei- und Datenfreigabe verwendet.

Die folgende Tabelle enthält die grundlegenden, für die MAM-Konfiguration erforderlichen Informationen.

App-Name	App-Typ	Integration des MAM-SDK oder Umschließen mit MDX	iOS	Android
Secure Mail	XenMobile App	Ab Version 10.4.1 nein	Ja	Ja
Secure Web	XenMobile App	Ab Version 10.4.1 nein	Ja	Ja
Citrix Files	XenMobile App	Ab Version 10.4.1 nein	Ja	Ja
Secure Hub	Öffentliche App	Nicht zutreffend	Ja	Ja
Citrix Receiver	Öffentliche App	Nicht zutreffend	Ja	Ja
GoToMeeting	Öffentliche App	Nicht zutreffend	Ja	Ja
SalesForce1	Öffentliche App	Nicht zutreffend	Ja	Ja
RSA SecurID	Öffentliche App	Nicht zutreffend	Ja	Ja
Epic Haiku	Öffentliche App	Nicht zutreffend	Ja	Ja
Epic Canto	Öffentliche App	Nicht zutreffend	Ja	Nein
Epic Rover	Öffentliche App	Nicht zutreffend	Ja	Nein
Epic Hyperspace	HDX-App	Nicht zutreffend	Ja	Ja
Vocera	ISV-App	Ja	Ja	Ja

HCMail	Interne App	Ja	Ja	Ja
PatientRounding	Web-App	Nicht zutreffend	Ja	Ja
Outlook Web Access	Web-App	Nicht zutreffend	Ja	Ja
SharePoint	Web-App	Nicht zutreffend	Ja	Ja

In der folgenden Tabelle sind die spezifischen Anforderungen aufgeführt, die Sie bei der Konfiguration von MAM-Richtlinien in XenMobile konsultieren können.

App-Name	VPN erforderlich	Interaktion (mit Container-externen Apps)	Interaktion (von Container-externen Apps)	Proxy-Filter	Lizenzierung	Geofencing	Mobile Apps SDK	Mindestversion des Betriebssystems
Secure Mail	J	Selektiv zugelassen	Zugelasse	Erforderli	Nicht zutreffend	Selektiv erforderlich	Nicht zutreffend	Erzwungen
Secure Web	J	Zugelassen	Zugelassen	Erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Erzwungen
Citrix Files	J	Zugelasse	Zugelasse	Erforderli	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Erzwungen
Secure Hub	J	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Citrix Receiver	J	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen

App-Name	VPN erforderlich	Interaktion (mit Container-externen Apps)	Interaktion (von Container-externen Apps)	Proxy-Filter	Lizenzierung	Geofencing	Mobile Apps SDK	Mindestversion des Betriebssystems
GoToMeeting	Ng	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
SalesForc	N	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
RSA SecurID	N	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Epic Haiku	J	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Epic Canto	J	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Epic Rover	J	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Volume Purchase	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Epic Hyperspace	J	Nicht zutreffend	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Vocera	J	Blockiert	Blockiert	Erforderli	Nicht zutreffend	Erforderli	Erforderli	Erzwungen

App-Name	VPN erforderlich	Interaktion (mit Container-externen Apps)	Interaktion (von Container-externen Apps)	Proxy-Filter	Lizenzierung	Geofencing	Mobile Apps SDK	Mindestversion des Betriebssystems
HCMail	J	Blockiert	Blockiert	Erforderlich	Nicht zutreffend	Erforderlich	Erforderlich	Erzwungen
PatientRc	J	Nicht zutreffend	Nicht zutreffend	Erforderli	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
Outlook Web Access	J	Nicht zutreffend	Nicht zutreffend	Erforderlich	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen
SharePoi	J	Nicht zutreffend	Nicht zutreffend	Erforderli	Nicht zutreffend	Nicht erforderlich	Nicht zutreffend	Nicht erzwungen

Benutzergemeinschaften

November 9, 2020

Jede Organisation besteht aus mehreren Benutzergemeinschaften, die unterschiedliche funktionelle Rollen besitzen. Diese Benutzergemeinschaften führen unterschiedliche Aufgaben und Bürofunktionen aus und nutzen unterschiedliche Ressourcen, die Sie über mobile Benutzergeräte bereitstellen. Manche Benutzer arbeiten von zu Hause oder an Remotestandorten und verwenden dabei die von Ihnen bereitgestellten Mobilgeräte. Andere Benutzer greifen über private Mobilgeräte auf Tools zu, für die bestimmte Regeln zur Sicherheitskonformität gelten.

Je mehr Benutzergemeinschaften mit Mobilgeräten arbeiten, desto bedeutender wird das Enterprise Mobility Management (EMM), um Datenverluste zu verhindern und Sicherheitsbeschränkungen der Organisation durchzusetzen. Im Interesse einer effizienten und differenzierten Mobilgeräteverwaltung können Sie Benutzergemeinschaften auch in Kategorien unterteilen. Dies vereinfacht die Zuordnung von Benutzern zu Ressourcen und stellt sicher, dass die richtigen Sicherheitsrichtlinien ange-

wandt werden.

Das Kategorisieren von Benutzergemeinschaften kann folgende Komponenten umfassen:

- Active Directory-Organisationseinheiten (OUs) und -Gruppen

  Benutzer, die bestimmten Active Directory-Sicherheitsgruppen hinzugefügt wurden, können Richtlinien und Ressourcen (z. B. Apps) empfangen. Werden Benutzer aus einer Active Directory-Sicherheitsgruppe entfernt, können sie nicht mehr auf zuvor verfügbare XenMobile-Ressourcen zugreifen.

- Lokale XenMobile-Benutzer und -Gruppen

  Für Benutzer ohne Active Directory-Konto können Sie ein Konto als lokale XenMobile-Benutzer erstellen. Diese lokalen Benutzer können Sie dann zu Bereitstellungsgruppen hinzufügen und ihnen dieselben Ressourcen wie Active Directory-Benutzern bereitstellen.

- XenMobile-Bereitstellungsgruppen

  Wenn mehrere Benutzergruppen mit unterschiedlichen Berechtigungsstufen dieselbe App verwenden, müssen Sie eventuell separate Bereitstellungsgruppen erstellen. Mit separaten Bereitstellungsgruppen können Sie zwei Versionen einer App bereitstellen.

- Zuordnung von Bereitstellungsgruppe und Benutzergruppe

  Die Zuordnung von Bereitstellungsgruppe zu Active Directory-Gruppe kann entweder 1:1 oder 1:n erfolgen. Verwenden Sie eine Bereitstellungsgruppenzuordnung vom Typ 1:n, um grundlegende Richtlinien und Apps zuzuweisen. Verwenden Sie Bereitstellungsgruppenzuordnungen vom Typ 1:1, um funktionsspezifische Richtlinien und Apps zuzuweisen.

- Bereitstellungsgruppen und die Ressourcenzuordnung von Apps

  Weisen Sie jeder Bereitstellungsgruppe bestimmte Apps zu.

- Bereitstellungsgruppen und die Ressourcenzuordnung von MDM-Ressourcen

  Weisen Sie jeder Bereitstellungsgruppe Apps und bestimmte Geräteverwaltungsressourcen zu. Konfigurieren Sie beispielsweise eine Bereitstellungsgruppe mit einer Mischung aus folgenden Komponenten: verschiedene App-Typen (öffentlich, HDX usw.), bestimmte Apps pro App-Typ sowie Ressourcen wie Geräterichtlinien und automatisierte Aktionen.

Das folgende Beispiel zeigt, wie Benutzergemeinschaften in einer US-Organisation im Gesundheitssektor für EMM klassifiziert werden.

Anwendungsfall

Dieses Klinikunternehmen bietet technologische Ressourcen und Zugriffsrechte für verschiedene Benutzer, darunter angestellte, externe und ehrenamtliche Mitarbeiter. Die Organisation plant, die EMM-Lösung nur für Benutzer bereitzustellen, die nicht zur Geschäftsleitung gehören.

Die Benutzerrollen und -funktionen im Unternehmen können in folgende Untergruppen unterteilt werden: Klinik, Verwaltung, Extern. Einige Benutzer erhalten firmeneigene Mobilgeräte, während andere über Privatgeräte (per BYOD) eingeschränkt Zugriff auf Unternehmensressourcen haben. Um Sicherheitsbeschränkungen angemessen umzusetzen und Datenverluste zu vermeiden, soll das IT-Team der Organisation jedes registrierte Gerät verwalten. Benutzer können zudem nur jeweils ein Gerät registrieren.

Nachfolgend finden Sie einen Überblick über die Rollen und Funktionen der einzelnen Untergruppen.

Klinik

- Pflegepersonal
- Mediziner (Ärzte, Chirurgen usw.)
- Fachärzte (Ernährungsberater, Phlebologen, Anästhesisten, Radiologen, Kardiologen, Onkologen usw.)
- Externe Mediziner (nicht angestellte Ärzte und Büromitarbeiter an Remotestandorten)
- Hausbesuchsdienste (Büropersonal und mobile Mitarbeiter, die arztbezogene Dienste für Hausbesuche bei Patienten durchführen)
- Forschungsspezialisten (Wissensarbeiter und Hauptbenutzer in sechs Forschungsinstituten, die in der klinischen Forschung tätig sind und medizinische Studien durchführen)
- Schulungen, Aus- und Weiterbildung (Pflegepersonal, Mediziner und Pädagogen)

Verwaltung

- Gemeinsam genutzte Dienste (Büromitarbeiter, die verschiedene Backoffice-Funktionen ausführen, z. B. Personalabteilung, Gehaltsabrechnung, Kreditorenbuchhaltung, Einkauf und Logistik usw.)
- Arztbezogene Dienste (Büromitarbeiter, die verschiedene Aufgaben im Bereich Gesundheitsmanagement und Administration ausüben und Geschäftsprozesslösungen für Anbieter bereitstellen. Dazu gehören Verwaltung und Geschäftsanalytik, Geschäftssysteme, Serviceangebote für Kunden und Patienten, Finanzwesen, Managed Care, Rentabilitätslösungen usw.)
- Supportdienste (Büromitarbeiter, die Funktionen in verschiedenen nichtklinischen Bereichen ausüben: Arbeitgeberleistungen, klinische Integration, Kommunikation, Vergütung, Gebäudemanagement, Technologiesysteme für die Personalabteilung, Informationsdienste, internes Audit und Prozessoptimierung usw.)
- Gemeinnützige Stiftungen (Büromitarbeiter und mobile Mitarbeiter, die verschiedene Funktionen im Rahmen philanthropischer Programme ausüben)

Auftragnehmer

- Hersteller und Vertriebspartner (Bereitstellung diverser nicht-klinischer Supportfunktionen vor Ort und remote über Site-to-Site-VPN)

Auf der Grundlage dieser Informationen hat die Organisation folgende Entitäten erstellt. Weitere Informationen zu Bereitstellungsgruppen in XenMobile finden Sie in der Produktdokumentation zu XenMobile unter Bereitstellen von Ressourcen.

Active Directory-Organisationseinheiten (OUs) und -Gruppen

Für OU = XenMobile-Ressourcen

- OU = Klinik; Gruppen =
  - XM - Pflegepersonal
  - XM - Mediziner
  - XM - Fachärzte
  - XM - Externe Mediziner
  - XM - Hausbesuchsdienste
  - XM - Forschungsspezialisten
  - XM - Schulungen, Aus- und Weiterbildung
- OU = Verwaltung; Gruppen =
  - XM - Gemeinsam genutzte Dienste
  - XM - Arztbezogene Dienste
  - XM - Supportdienste
  - XM - Gemeinnützige Stiftungen

Lokale XenMobile-Benutzer und -Gruppen

Für Gruppe = Auftragnehmer, Benutzer =

- Anbieter 1
- Anbieter 2
- Anbieter 3
- … Anbieter 10

XenMobile-Bereitstellungsgruppen

- Klinik - Pflegepersonal
- Klinik - Mediziner
- Klinik - Fachärzte
- Klinik - Externe Mediziner

- Klinik - Hausbesuchsdienste
- Klinik - Forschungsspezialisten
- Klinik - Schulungen, Aus- und Weiterbildung
- Verwaltung - Gemeinsam genutzte Dienste
- Verwaltung - Arztbezogene Dienste
- Verwaltung - Supportdienste
- Verwaltung - Gemeinnützige Stiftungen

Zuordnung von Bereitstellungsgruppe und Benutzergruppe

Active Directory-Gruppen	XenMobile-Bereitstellungsgruppen
XM - Pflegepersonal	Klinik - Pflegepersonal
XM - Mediziner	Klinik - Mediziner
XM - Fachärzte	Klinik - Fachärzte
XM - Externe Mediziner	Klinik - Externe Mediziner
XM - Hausbesuchsdienste	Klinik - Hausbesuchsdienste
XM - Forschungsspezialisten	Klinik - Forschungsspezialisten
XM - Schulungen, Aus- und Weiterbildung	Klinik - Schulungen, Aus- und Weiterbildung
XM - Gemeinsam genutzte Dienste	Verwaltung - Gemeinsam genutzte Dienste
XM - Arztbezogene Dienste	Verwaltung - Arztbezogene Dienste
XM - Supportdienste	Verwaltung - Supportdienste
XM - Gemeinnützige Stiftungen	Verwaltung - Gemeinnützige Stiftungen

Bereitstellungsgruppen und die Ressourcenzuordnung von Apps

	Secure Mail	Secure Web	ShareFil	Receiver	SalesFor	RSA SecurID	EpicCare Haiku	Epic Hyperspace
Klinik - Pflegepersonal	X	X	X					

Klinik - Mediziner						
Klinik - Fachärzte						
Klinik - Externe Mediziner	X		X			
Klinik - Hausbesuchsdienste	X		X			
Klinik - Forschunisten	X		X			
Klinik - Schulungen, Aus- und Weiterbildung					X	X
Verwaltu - Gemeinsam genutzte Dienste					X	X
Verwaltung - Arztbezogene Dienste					X	X

Verwaltu - Sup- portdi- enste	X	X				X	X
Verwaltung - Gemein- nützige Stiftun- gen	X	X				X	X
Auftragne	X	X	X	X		X	X

Bereitstellungsgruppen und die Ressourcenzuordnung von MDM-Ressourcen

	MDM: Pass-coderichtlinie	MDM: Geräteein-schränkungen	MDM: Automatisierte Aktionen	WiFi-Richtlinie
Klinik - Pflegepersonal				X
Klinik - Mediziner		X		
Klinik - Fachärzte				
Klinik - Externe Mediziner				
Klinik - Hausbe-suchsdienste				
Klinik - Forschungsspezialisten				

Klinik - Schulungen, Aus- und Weiterbildung		
Verwaltung - Gemeinsam genutzte Dienste		
Verwaltung - Arztbezogene Dienste		
Verwaltung - Supportdienste		
Verwaltung - Gemeinnützige Stiftungen		
Auftragnehmer		X

Hinweise und Überlegungen

- XenMobile erstellt bei der Erstkonfiguration die Standardbereitstellungsgruppe “Alle Benutzer”. Wenn Sie diese Bereitstellungsgruppe nicht deaktivieren, sind alle Active Directory-Benutzer berechtigt, sich in XenMobile zu registrieren.
- XenMobile synchronisiert Active Directory-Benutzer und -Gruppen bei Bedarf über eine dynamische Verbindung mit dem LDAP-Server.
- Wenn ein Benutzer zu einer Gruppe gehört, die nicht in XenMobile zugeordnet ist, kann der Benutzer sich nicht registrieren. Wenn ein Benutzer Mitglieder mehrerer Gruppen ist, kategorisiert XenMobile den Benutzer nur als Mitglied der Gruppen, die in XenMobile zugeordnet sind.
- Für eine verbindliche MDM-Registrierung wählen Sie in der XenMobile-Konsole unter **Servereigenschaften** für die Option **Registrierung erforderlich** die Einstellung **Wahr**. Einzelheiten finden Sie unter Servereigenschaften.
- Zum Löschen einer Benutzergruppe aus einer XenMobile-Bereitstellungsgruppe löschen Sie den Eintrag in der SQL Server-Datenbank unter dbo.userlistgrps.

> **Achtung:**
>
> Erstellen Sie ein Backup von XenMobile und der Datenbank, bevor Sie diese Aktion durchführen.

Geräteeigentümerschaft in XenMobile

Sie können Benutzer auch nach dem Eigentümer eines Benutzergeräts gruppieren. Es gibt unternehmenseigene Geräte und solche, die Benutzern gehören. Letztere werden auch als BYOD-Geräte (von "bring your own device") bezeichnet. Sie können in zwei Bereichen der XenMobile-Konsole steuern, wie BYOD-Geräte eine Verbindung mit dem Netzwerk herstellen: unter "Bereitstellungsregeln" und über die XenMobile Server-Eigenschaften auf der Seite **Einstellungen**. Weitere Informationen zu Bereitstellungsregeln finden Sie in der Dokumentation zu XenMobile unter Bereitstellen von Ressourcen. Weitere Informationen über Servereigenschaften finden Sie in diesem Handbuch unter Servereigenschaften.

Beim Definieren der Servereigenschaften können Sie festlegen, dass alle BYOD-Benutzer die Verwaltung ihrer Geräte durch das Unternehmen akzeptieren müssen, bevor sie Zugriff auf Apps erhalten. Alternativ können Sie Benutzern auch ohne Verwaltung ihrer Geräte Zugriff auf Unternehmensapps erteilen.

Wenn Sie die Servereigenschaft **wsapi.mdm.required.flag** auf **true** festlegen, werden alle BYOD-Geräte von XenMobile verwaltet und Benutzer, die eine Registrierung ablehnen, erhalten keinen Zugriff auf Apps. Das Festlegen von **wsapi.mdm.required.flag** auf **true** sollte in Umgebungen erwogen werden, in denen neben einer hohen Sicherheit eine gute Benutzererfahrung bei der Geräteregistrierung erforderlich ist.

Wenn Sie die Einstellung nicht ändern und die Standardeinstellung **false** für **wsapi.mdm.required.flag** übernehmen, können Benutzer die Registrierung ablehnen. Sie können dennoch mit ihren Geräten über den XenMobile Store auf Apps zugreifen. Das Festlegen von **wsapi.mdm.required.flag** auf **false** eignet sich für Umgebungen, in denen juristische und datenschutzrechtliche Vorgaben keine Verwaltung von Geräten erfordern, sondern nur die Verwaltung von Unternehmensapps.

Benutzer mit nicht von XenMobile verwalteten Geräten können Apps über den XenMobile Store installieren. Anstelle einer Steuerung auf Gerätebasis, etwa der selektiven oder vollständigen Löschung der Daten auf einem Gerät, steuern Sie den Zugriff auf Apps über App-Richtlinien. Einige Richtlinieneinstellungen erfordern, dass Geräte regelmäßig XenMobile Server abfragen, um sicherzustellen, dass Apps weiterhin zugelassen sind.

E-Mail-Strategie

January 5, 2022

Der sichere Zugriff auf E-Mail über Mobilgeräte gehört zu den wichtigsten Bereichen des Mobilitätsmanagements in Unternehmen. Die Entscheidung über die richtige E-Mail-Strategie ist oft eines der Hauptkriterien beim XenMobile-Designs. XenMobile bietet Optionen für unterschiedliche Anwendungsfälle basierend auf Sicherheit, Benutzererfahrung und Anforderungen im Hinblick auf die Integration. In diesem Artikel wird der gängige Prozess zur Wahl des Designs einschließlich Überlegungen bei der Auswahl der richtigen Lösung, vom Client bis zum E-Mail-Verkehr, behandelt.

Auswählen der E-Mail-Clients

Die Auswahl des oder der Clients steht in der Regel bei der Entwicklung der E-Mail-Strategie an oberster Stelle. Es stehen mehrere Clients zur Auswahl: Citrix Secure Mail, systemeigene Clients von Mobilbetriebssystemen und Clients von Drittanbietern aus öffentlichen App-Stores. Je nach Anforderungen genügt evtl. ein einzelner (Standard-) Client oder es ist eine Kombination von Clients erforderlich.

Die folgende Tabelle enthält Kriterien, die bei den verschiedenen Clientoptionen zu berücksichtigen sind:

Thema	Secure Mail	Systemeigene Clients (z. B. iOS Mail)	Drittanbieterclients
XenMobile-Mindestedition	Erweitert	MDM	MDM
Konfiguration	Über eine MDX-Richtlinie konfigurierte Exchange-Kontoprofile.	Über eine MDM-Richtlinie konfigurierte Exchange-Kontoprofile. Android-Unterstützung beschränkt auf: SAFE/KNOX und Android Enterprise. Alle anderen Clients gelten als Drittanbieterclients.	Erfordert im Allgemeinen manuelle Konfiguration durch Benutzer.

Sicherheit	Höchste, designinhärente Sicherheit. Verwendet MDX-Richtlinien mit zusätzlichen Datenverschlüsselungsstufen. Secure Mail ist eine vollständig verwaltete App (per MDX-Richtlinie). Zusätzliche Authentifizierungsstufe per Citrix-PIN.	Je nach Anbieter/App-Features. Bietet höhere Sicherheit. Verwendet Geräteverschlüsselungseinstellungen (ohne Sicherheit über MDX-Richtlinien). Erfordert Authentifizierung auf Geräteebene für den Zugriff auf die App	Je nach Anbieter/App-Features. Bietet hohe Sicherheit.
Integration	Ermöglicht standardmäßig die Interaktion mit verwalteten Apps (MDX). Öffnen von Internet-URLs mit Citrix Secure Web. Speichern und Anhängen von Dateien aus Citrix Files. Direkte Teilnahme und Einwahl bei GoToMeeting.	Kann standardmäßig nur mit anderen nicht verwalteten Apps (ohne MDX) interagieren.	Kann standardmäßig nur mit anderen nicht verwalteten Apps (ohne MDX) interagieren.

Bereitstellung/Lizenzierung	Direkte Pushbereitstellung von Secure Mail über MDM aus öffentlichen App-Stores. In XenMobile Advanced und Enterprise enthalten.	Client-App im Betriebssystem der Plattform enthalten. Keine zusätzliche Lizenzierung erforderlich.	Pushbereitstellung über MDM als Unternehmensapp oder direkt aus öffentlichen App-Stores. Lizenzierungsmodell/-kosten je nach App-Anbieter.
Support	Support aus einer Hand für Client- und EMM-Lösung (Citrix). Integrierte Support-Kontaktinformationen in Secure Hub, Funktionen zur Protokollierung des App-Debuggings. Nur ein Client muss betreut werden.	Support je nach Hersteller (Apple/Google). Je nach Geräteplattform müssen ggf. verschiedene Clients betreut werden.	Support je nach Hersteller. Support eines Clients, vorausgesetzt, dieser wird von allen verwalteten Geräteplattformen unterstützt.

Überlegungen zu E-Mail-Verkehr und Filterung

In diesem Abschnitt werden die drei Hauptszenarien sowie Designüberlegungen für den E-Mail-(ActiveSync-)Verkehr im Zusammenhang mit XenMobile erläutert.

Szenario 1: offenes Exchange

In Umgebungen, die externe Clients unterstützen, sind die Exchange ActiveSync-Dienste häufig mit dem Internet verbunden. Mobile ActiveSync-Clients stellen über diese externe Route Verbindungen durch einen Reverseproxy (z. B. Citrix ADC) oder einen Edgeserver her. Diese Option ist zur Verwendung systemeigener E-Mail-Clients oder solcher von Drittanbietern erforderlich, wodurch diese Clients zur bevorzugten Wahl für dieses Szenario werden. Es ist zwar nicht üblich, doch Sie können in diesem Szenario auch den Secure Mail-Client verwenden. Dadurch können Sie die Sicherheitsfunktionen der MDX-Richtlinien und der App-Verwaltung nutzen.

Szenario 2: Tunneling über Citrix ADC (Micro-VPN und STA)

Dieses Szenario ist Standard bei Verwendung des Secure Mail-Clients aufgrund von dessen Micro-VPN-Funktionen. Der Secure Mail-Client stellt über Citrix Gateway eine sichere Verbindung mit ActiveSync her. Im Wesentlichen ist Secure Mail hier der Client, der aus dem internen Netzwerk eine direkte Verbindung mit ActiveSync herstellt. Citrix Kunden verwenden Secure Mail häufig als bevorzugten mobilen ActiveSync-Client. Auf diese Weise soll vermieden werden, dass ActiveSync-Dienste über einen Exchange Server im Internet offengelegt werden, wie dies in Szenario 1 der Fall wäre.

Nur MAM-SDK-fähige Apps oder Apps, die mit MDX umschlossen wurden, können die Micro-VPN-Funktion verwenden. Dieses Szenario gilt nicht für native Clients, wenn Sie das MDX-Verfahren zum Umschließen verwenden. Es ist zwar evtl. möglich, Clients von Drittanbietern mit dem MDX Toolkit zu umschließen, dies ist jedoch nicht üblich. Die Verwendung von VPN-Clients auf Geräteebene für das Tunneling für systemeigene Clients oder Clients von Drittanbietern hat sich als umständlich und nicht praktikabel erwiesen.

Szenario 3: in der Cloud gehosteter Exchange-Dienst

In der Cloud gehostete Exchange-Dienste wie Microsoft Office 365 erfreuen sich zunehmender Beliebtheit. Im Kontext von XenMobile kann dieses Szenario mit Szenario 1 gleichgesetzt werden, da der ActiveSync-Dienst offen gegenüber dem Internet ist. In diesem Fall diktieren die Anforderungen des Cloudservice-Anbieters die Entscheidungen im Hinblick auf Clients. Es werden im Allgemeinen die meisten ActiveSync-Clients unterstützt, z. B. Secure Mail oder andere systemeigene oder Drittanbieterclients.

XenMobile bietet bei diesem Szenario in drei Bereichen Vorteile:

- Clients mit MDX-Richtlinien und App-Verwaltung mit Secure Mail
- Clientkonfiguration unter Verwendung einer MDM-Richtlinie bei unterstützten systemeigenen E-Mail-Clients
- ActiveSync-Filteroptionen mit Einsatz des Endpoint Management Connectors für Exchange ActiveSync

Filtern des E-Mail-Verkehrs

Wie bei den meisten mit dem Internet verbundenen Diensten müssen Sie die Route schützen und eine Filterung für den autorisierten Zugriff bereitstellen. XenMobile umfasst zwei speziell für ActiveSync-Filterfunktionen für systemeigene und Clients von Drittanbietern entwickelte Komponenten: Citrix Gateway Connector für Exchange ActiveSync und Endpoint Management Connector für Exchange ActiveSync.

Citrix Gateway Connector für Exchange ActiveSync

Citrix Gateway Connector für Exchange ActiveSync ermöglicht eine ActiveSync-Filterung im Umkreis, wobei Citrix ADC als Proxy für den ActiveSync-Datenverkehr agiert. Dies bedeutet, dass die Filterkomponente im Pfad des E-Mail-Datenverkehrs ist und E-Mails beim Erreichen oder Verlassen der Umgebung abfängt. Der Citrix Gateway Connector für Exchange ActiveSync fungiert als Vermittler zwischen Citrix ADC und dem XenMobile-Server. Wenn ein Gerät über den virtuellen ActiveSync-Server auf dem Citrix ADC mit Exchange kommuniziert, führt der Citrix ADC einen HTTP-Callout an den Connector für den Exchange ActiveSync-Dienst aus. Der Dienst überprüft dann den Gerätestatus bei XenMobile. Je nach Gerätestatus weist der Connector für Exchange ActiveSync dann Citrix ADC an, die Verbindung zuzulassen oder zu verweigern. Sie können auch statische Regeln konfigurieren, um den Zugriff basierend auf Benutzer, Agent und Gerätetyp oder Geräte-ID zu filtern.

Dadurch können Exchange ActiveSync-Dienste dem Internet mit einer zusätzlichen Sicherheitsebene zur Verhinderung eines unbefugten Zugriffs ausgesetzt werden. Es sind folgende Punkte zu berücksichtigen:

- Windows-Server: Der Connector für Exchange ActiveSync erfordert einen Windows-Server.
- Filterregeln: Der Connector für Exchange ActiveSync filtert nach Gerätestatus und -informationen und nicht nach Benutzerinformationen. Sie können zwar statische Regeln zur Filterung nach Benutzer-ID konfigurieren, es gibt jedoch keine Optionen beispielsweise zum Filtern nach Active Directory-Gruppenmitgliedschaft. Wenn eine Filterung nach Active Directory-Gruppen erforderlich ist, können Sie stattdessen den Endpoint Management Connector für Exchange ActiveSync verwenden.
- Citrix ADC-Skalierbarkeit: Angesichts der Notwendigkeit, den ActiveSync-Datenverkehr über Citrix ADC als Proxy zu leiten, ist die richtige Dimensionierung der Citrix ADC-Instanz entscheidend, um die zusätzliche Workload aller ActiveSync-SSL-Verbindungen zu bewältigen.
- Integrated Caching bei Citrix ADC: Die Konfiguration des Connectors für Exchange ActiveSync auf dem Citrix ADC verwendet Integrated Caching zum Zwischenspeichern der Antworten des Connectors. Daher muss Citrix ADC keine Anforderung für jede ActiveSync-Transaktion in einer bestimmten Sitzung an den Citrix Gateway Connector für Exchange ActiveSync senden. Diese Konfiguration ist auch entscheidend für eine angemessene Leistung und Skalierung. Integrated Caching ist mit der Citrix ADC Platinum Edition verfügbar, für Enterprise Editions wird eine separate Lizenz angeboten.
- Benutzerdefinierte Filterrichtlinien: Sie müssen ggf. eigene Citrix ADC-Richtlinien erstellen, um bestimmte ActiveSync-Clients außerhalb der standardmäßigen systemeigenen Mobilclients einzuschränken. Diese Konfiguration erfordert Kenntnisse in den Bereichen ActiveSync-HTTP-Anforderungen und Erstellung von Citrix ADC-Responderrichtlinien.
- Secure Mail-Clients: Secure Mail hat Micro-VPN-Funktionen, die das Filtern am Umkreis überflüssig machen. Der Secure Mail-Client wird im Allgemeinen als interner (vertrauenswürdiger) ActiveSync-Client behandelt, wenn er über Citrix Gateway verbunden ist. Werden sowohl sys-

temeigene Clients und Drittanbieter-Clients (mit dem Connector für Exchange ActiveSync) als auch Secure Mail-Clients verwendet, empfiehlt Citrix, den Secure Mail-Datenverkehr nicht über den für den Connector für Exchange ActiveSync verwendeten virtuellen Citrix ADC-Server zu leiten. Sie können den Datenverkehr über DNS leiten und Auswirkungen der Connector für Exchange ActiveSync-Richtlinie auf die Secure Mail-Clients verhindern.

Ein Diagramm des Citrix Gateway-Connectors für Exchange ActiveSync in einer XenMobile-Bereitstellung finden Sie unter Referenzarchitektur für On-Premises-Bereitstellungen.

Endpoint Management Connector für Exchange ActiveSync

Endpoint Management Connector für Exchange ActiveSync ist eine XenMobile-Komponente, die eine ActiveSync-Filterung auf der Exchange-Dienstebene ermöglicht. Die Filterung erfolgt erst, wenn die E-Mail den Exchange-Dienst erreicht, und nicht sobald sie in die XenMobile-Umgebung gelangt. Mail Manager verwendet PowerShell, um bei Exchange ActiveSync Gerätepartnerschaftsinformationen abzufragen und den Zugriff über Gerätequarantäneaktionen zu steuern. Dadurch werden Geräte basierend auf den Regelkriterien des Endpoint Management Connectors für Exchange ActiveSync unter Quarantäne gestellt, bzw. aus dieser befreit. Ähnlich wie der Citrix Gateway Connector für Exchange ActiveSync überprüft der Endpoint Management Connector für Exchange ActiveSync den Gerätestatus mit XenMobile, um den Zugriff basierend auf der Gerätecompliance zu filtern. Sie können auch statische Regeln konfigurieren, um den Zugriff basierend auf Gerätetyp, Geräte-ID, Agentversion und Active Directory-Gruppenmitgliedschaft zu filtern.

Diese Lösung erfordert nicht die Verwendung von Citrix ADC. Sie können den Endpoint Management Connector für Exchange ActiveSync ohne Änderungen am Routing des ActiveSync-Datenverkehrs bereitstellen. Es sind folgende Punkte zu berücksichtigen:

- Windows-Server: Der Endpoint Management Connector für Exchange ActiveSync erfordert einen Windows-Server.
- Filterregelsatz: Wie der Citrix Gateway Connector für Exchange ActiveSync umfasst der Endpoint Management Connector für Exchange ActiveSync Filterregeln zur Bewertung des Gerätezustands. Darüber hinaus unterstützt der Endpoint Management Connector für Exchange ActiveSync auch statische Regeln zum Filtern nach Active Directory-Gruppenmitgliedschaft.
- Exchange-Integration: Der Endpoint Management Connector für Exchange ActiveSync benötigt direkten Zugriff auf den Exchange-Clientzugriffsserver (CAS), auf dem die ActiveSync-Rolle und die Steuerung der Gerätequarantäne gehostet werden. Diese Anforderung kann abhängig von der Umgebungsarchitektur und der Sicherheitslage eine Herausforderung darstellen. Diese technische Anforderung muss auf jeden Fall im Vorfeld bewertet werden.
- Andere ActiveSync-Clients: Da der Endpoint Management Connector für Exchange ActiveSync auf der ActiveSync-Dienstebene filtert, sollten Sie andere ActiveSync-Clients außerhalb der

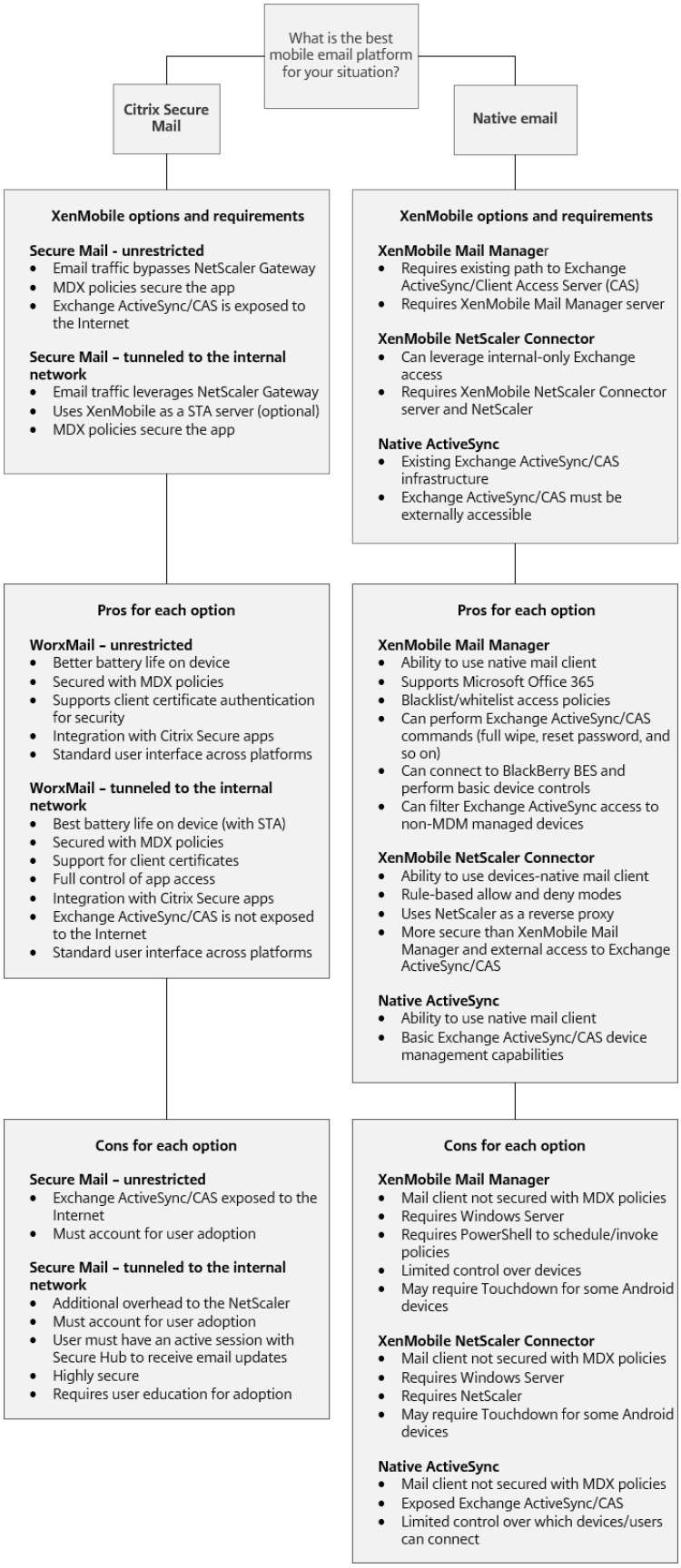
XenMobile-Umgebung berücksichtigen. Sie können statische Regeln für den Endpoint Management Connector für Exchange ActiveSync konfigurieren, um unbeabsichtigte Auswirkungen auf andere ActiveSync-Clients zu vermeiden.

- Erweiterte Exchange-Funktionen: Durch die direkte Integration in Exchange ActiveSync bietet der Endpoint Management Connector für Exchange ActiveSync die Möglichkeit, über XenMobile eine Exchange ActiveSync-Löschung auf einem Mobilgerät durchzuführen. Mit dem Endpoint Management Connector für Exchange ActiveSync kann XenMobile außerdem auf Blackberry-Geräteinformationen zugreifen und andere Steuerungsvorgänge durchführen.

Ein Diagramm des Endpoint Management-Connectors für Exchange ActiveSync in einer XenMobile-Bereitstellung finden Sie unter Referenzarchitektur für On-Premises-Bereitstellungen.

Entscheidungsbaum zur Wahl der E-Mail-Plattform

Die folgende Abbildung bietet einen Überblick über die Vor- und Nachteile der Verwendung systemeigener Lösungen und von Secure Mail in einer XenMobile-Bereitstellung. Für jede Option gibt es spezifische XenMobile-Optionen und -Anforderungen, für den Zugriff auf Server, Netzwerk- und Datenbank. Die Vor- und Nachteile umfassen Aspekte im Hinblick auf Sicherheit, Richtlinien und Benutzeroberfläche.



XenMobile-Integration

January 5, 2022

In diesem Artikel werden die Punkte beschrieben, die bei der Planung der Integration von XenMobile in ein Netzwerk und bestehende Lösungen berücksichtigt werden müssen. Falls Sie beispielsweise Citrix ADC bereits für Virtual Apps and Desktops verwenden:

- Sollten Sie die vorhandene Citrix ADC-Instanz oder eine neue, dedizierte Instanz verwenden?
- Möchten Sie die mit StoreFront veröffentlichten HDX-Apps in XenMobile integrieren?
- Planen Sie die Verwendung von Citrix Files mit XenMobile?
- Haben Sie eine Network Access Control-Lösung, die Sie in XenMobile integrieren möchten?
- Stellen Sie Webproxys für den gesamten von Ihrem Netzwerk ausgehenden Datenverkehr bereit?

Citrix ADC und Citrix Gateway

Citrix Gateway ist für XenMobile im ENT- und MAM-Modus obligatorisch. Citrix Gateway bietet einen Micro-VPN-Pfad für den Zugriff auf alle Unternehmensressourcen und unterstützt eine starke Multifaktorauthentifizierung. Der Citrix ADC-Lastausgleich ist für alle XenMobile Server-Gerätemodi in folgenden Fällen erforderlich:

- Sie haben mehrere XenMobile-Server.
- XenMobile Server ist in der DMZ oder dem internen Netzwerk (d. h. der Datenverkehr fließt von den Geräten an Citrix ADC und dann an XenMobile).

Sie können vorhandene Citrix ADC-Instanzen verwenden oder neue für XenMobile einrichten. In den folgenden Abschnitten werden die Vor- und Nachteile der Verwendung vorhandener und neuer Citrix ADC-Instanzen aufgeführt.

Gemeinsames Citrix ADC MPX mit einer virtuellen für XenMobile erstellten Citrix Gateway-IP

Vorteile:

- Verwendung einer Citrix ADC-Instanz für alle Citrix Remoteverbindungen: Citrix Virtual Apps and Desktops, vollständiges/clientloses VPN.
- Verwendung der bestehenden Citrix ADC-Konfigurationen, z. B. für die Zertifikatauthentifizierung und den Zugriff auf Dienste wie DNS, LDAP und NTP.
- Verwendung einer einzelnen Citrix ADC-Plattformlizenz.

Nachteile:

- Die Skalierungsplanung ist schwieriger, wenn zwei unterschiedliche Anwendungsfälle auf demselben Citrix ADC bewältigt werden.

- In Einzelfällen wird eine bestimmte Citrix ADC-Version für einen Citrix Virtual Apps and Desktops-Anwendungsfall benötigt. Bei der benötigten Version können Probleme im Zusammenhang mit XenMobile vorliegen. Umgekehrt können bei XenMobile Probleme im Zusammenhang mit der Citrix ADC-Version vorliegen.
- Ist ein Citrix Gateway vorhanden, können Sie den Citrix ADC für XenMobile-Assistenten kein zweites Mal ausführen, um die Citrix ADC-Konfiguration für XenMobile zu erstellen.
- Auf Citrix ADC installierte Benutzerzugriffslizenzen, die für die VPN-Konnektivität erforderlich sind, werden gepoolt (außer bei Verwendung von Platinum-Lizenzen für Citrix Gateway 11.1 oder höher). Da diese Lizenzen für alle virtuellen Citrix ADC-Server verfügbar sind, können andere Dienste als XenMobile sie verbrauchen.

Dedizierte Citrix ADC VPX-/MPX-Instanz

Vorteile:

Citrix empfiehlt die Verwendung einer dedizierten Citrix ADC-Instanz.

- Einfachere Skalierungsplanung und Trennung des XenMobile-Datenverkehrs von einer möglicherweise bereits mit eingeschränkten Ressourcen laufenden Citrix ADC-Instanz.
- Keine Probleme, wenn XenMobile und Citrix Virtual Apps and Desktops unterschiedliche Citrix ADC-Softwareversionen erfordern. Normalerweise empfiehlt sich die Verwendung der neuesten kompatiblen Citrix ADC-Version für XenMobile.
- Konfiguration von Citrix ADC für XenMobile über den integrierten Citrix ADC für XenMobile-Assistenten möglich.
- Virtuelle und physische Trennung von Diensten.
- Die für XenMobile erforderlichen Benutzerzugriffslizenzen sind nur für XenMobile-Dienste auf dem Citrix ADC verfügbar (außer bei Nutzung einer Platinum-Lizenz für Citrix Gateway 11.1 oder höher).

Nachteile:

- Erfordert die Einrichtung zusätzlicher Dienste auf Citrix ADC für die XenMobile-Konfiguration.
- Erfordert eine zusätzliche Citrix ADC-Plattformlizenz. Lizenzierung jeder Citrix ADC-Instanz für Citrix Gateway.

Informationen darüber, was bei der Integration von Citrix Gateway und Citrix ADC in den einzelnen XenMobile-Servermodi zu beachten ist, finden Sie unter Integration mit Citrix ADC und Citrix Gateway.

StoreFront

In Citrix Virtual Apps and Desktops-Umgebungen können HDX-Anwendungen mithilfe von StoreFront in XenMobile integriert werden. Für die Integration von HDX-Apps in XenMobile gilt Folgendes:

- Die Apps stehen Benutzern zur Verfügung, die bei XenMobile registriert sind.

- Die Apps werden zusammen mit anderen Apps im XenMobile-Store angezeigt.
- XenMobile verwendet die ältere PNAgent-Site (Dienste) in StoreFront.
- Ist Citrix Receiver auf einem Gerät installiert, wird es von HDX-Apps verwendet.

Bei StoreFront gilt die Beschränkung auf eine Services-Site pro StoreFront-Instanz. Angenommen, Sie haben mehrere Stores und möchten sie von anderen Produktionsverwendungen trennen. In diesem Fall empfiehlt Citrix, die Verwendung einer neuen StoreFront-Instanz und -Services-Site für XenMobile in Betracht zu ziehen.

Es sind u. a. folgende Punkte zu berücksichtigen:

- Gibt es für StoreFront andere Authentifizierungsanforderungen? Die StoreFront Services-Site erfordert Active Directory-Anmeldeinformationen für die Anmeldung. Bei ausschließlicher Verwendung der zertifikatbasierten Authentifizierung können Anwendungen nicht über XenMobile unter Verwendung desselben Citrix Gateways aufgelistet werden.
- Sollten Sie den gleichen Store verwenden oder einen neuen erstellen?
- Sollten Sie den gleichen oder einen anderen StoreFront-Server verwenden?

In den folgenden Abschnitten werden die Vor- und Nachteile der Verwendung eigener oder gemeinsamer StoreFront-Instanzen für Receiver und mobile Produktivitätsapps aufgeführt.

Integration der bestehenden StoreFront-Instanz in XenMobile Server

Vorteile:

- Gleicher Store: XenMobile erfordert keine zusätzliche Konfiguration von StoreFront, vorausgesetzt es wird dieselbe Citrix ADC-VIP für den HDX-Zugriff verwendet. Angenommen, Sie entscheiden sich für die Verwendung desselben Stores und möchten den Citrix Receiver-Zugriff auf eine neue Citrix ADC-VIP umleiten. Fügen Sie in diesem Fall StoreFront die entsprechende Citrix Gateway-Konfiguration hinzu.
- Gleicher StoreFront-Server: Verwendung der bestehenden StoreFront-Installation und -Konfiguration.

Nachteile:

- Gleicher Store: Jede Änderung der StoreFront-Konfiguration zur Bewältigung von Citrix Virtual Apps and Desktops-Workloads kann sich negativ auf XenMobile auswirken.
- Gleicher StoreFront-Server: In großen Umgebungen müssen Sie die zusätzliche Belastung des PNAgent durch XenMobile für die App-Auflistung und den Start berücksichtigen.

Verwenden einer neuen, dedizierten StoreFront-Instanz zur Integration in XenMobile Server

Vorteile:

- Neuer Store: Konfigurationsänderungen am StoreFront-Store für XenMobile dürften keine Auswirkungen auf Citrix Virtual Apps and Desktops-Workloads haben.
- Neuer StoreFront-Server: Änderungen an der Serverkonfiguration sollten sich nicht auf den Virtual Apps and Desktops-Workflow auswirken. Darüber hinaus sollte die XenMobile-externe Belastung des PNAgent für App-Auflistung und Start die Skalierbarkeit nicht beeinträchtigen.

Nachteile:

- Neuer Store: StoreFront-Store-Konfiguration.
- Neuer StoreFront-Server: erfordert eine neue StoreFront-Installation und -Konfiguration.

Weitere Informationen finden Sie unter Virtual Apps and Desktops über Citrix Secure Hub in der Dokumentation zu XenMobile.

Citrix Content Collaboration und Citrix Files

Citrix Files ermöglicht Benutzern von jedem Gerät aus den Zugriff auf all ihre Daten und deren Synchronisierung. Über Citrix Files können die Benutzer Daten mit Personen innerhalb und außerhalb der Organisation sicher teilen. Bei Integration von Citrix Content Collaboration in XenMobile Advanced Edition oder XenMobile Enterprise Edition ermöglicht XenMobile für Citrix Files Folgendes:

- Single-Sign-On-Authentifizierung für XenMobile App-Benutzer.
- Active Directory-basierte Benutzerkontobereitstellung.
- Umfassende Richtlinien zur Zugriffssteuerung.

Mobile Benutzer können alle Funktionen des Enterprise-Kontos verwenden.

Alternativ können Sie XenMobile für die ausschließliche Integration in Speicherzonenconnectors konfigurieren. Über Speicherzonenconnectors bietet Citrix Files Zugriff auf folgende Inhalte:

- Dokumente und Ordner
- Netzwerkdateifreigaben
- In SharePoint-Sites: Sitesammlungen und Dokumentbibliotheken.

Verbundene Dateifreigaben können die gleichen Basisnetzlaufwerke enthalten wie Citrix Virtual Apps and Desktops-Umgebungen. Die Konfiguration der Integration in Citrix Files oder Speicherzonenconnectors erfolgt über die XenMobile-Konsole. Weitere Informationen finden Sie unter Citrix Files mit XenMobile.

In den folgenden Abschnitten werden die Fragen aufgeführt, die Sie sich im Hinblick auf den Einsatz von Citrix Files stellen sollten.

Integration mit Citrix Files oder nur mit Speicherzonenconnectors

Relevanten Fragen:

- Müssen Daten in von Citrix verwalteten Speicherzonen gespeichert werden?
- Sollen die Benutzer Dateien freigeben und synchronisieren können?
- Sollen die Benutzer Zugriff auf Dateien auf der Citrix Files-Website erhalten? Sollen die Benutzer mit Mobilgeräten auf Office 365-Inhalte und Connectors für die persönliche Cloud zugreifen können?

Designentscheidung:

- Wenn die Antwort auf eine dieser Fragen "Ja" lautet, wählen Sie die Integration in Citrix Files.
- Eine ausschließliche Integration mit Speicherzonenconnectors bietet iOS-Benutzern sicheren mobilen Zugriff auf bestehende lokale Speicherrepositorys, wie z. B. SharePoint-Sites und Netzwerkdateifreigaben. In dieser Konfiguration müssen Sie keine Content Collaboration-Unterdomäne einrichten, Benutzer für Citrix Files bereitstellen oder Citrix Files-Daten hosten. Die Verwendung von Speicherzonenconnectors mit XenMobile entspricht den Sicherheitsbeschränkungen, die verhindern, dass Benutzerdaten außerhalb des Unternehmensnetzwerks gelangen.

Standort des Speicherzonencontroller-Servers

Relevanten Fragen:

- Benötigen Sie on-premises Speicher oder Features wie Speicherzonenconnectors?
- Wo befinden sich bei Verwendung von on-premises Citrix Files-Features die Speicherzonencontroller im Netzwerk?

Designentscheidung:

- Entscheiden Sie, wo Sie die Speicherzonencontroller ansiedeln: in der Citrix Files-Cloud, on-premises in einem Einmandanten-Speichersystem oder im unterstützten Cloudspeicher eines Drittanbieters.
- Speicherzonencontroller benötigen Internetzugriff für die Kommunikation mit der Citrix Files-Steuerungsebene. Es gibt verschiedene Verbindungsmöglichkeiten, einschließlich direktem Zugriff, NAT/PAT- und Proxykonfigurationen.

Speicherzonenconnectors

Relevanten Fragen:

- Welches sind die CIFS-Freigabepfade?
- Welches sind die SharePoint-URLs?

Designentscheidung:

- Ermitteln Sie, ob on-premises Speicherzonencontroller für den Zugriff auf diese Orte erforderlich sind.

- Aufgrund der Kommunikation zwischen Speicherzonenconnectors und internen Ressourcen wie Repositorys, CIFS-Freigaben und SharePoint empfiehlt Citrix, Speicherzonencontroller im internen Netzwerk hinter DMZ-Firewalls und mit vorgeschaltetem Citrix ADC anzusiedeln.

SAML-Integration in XenMobile Enterprise

Relevanten Fragen:

- Ist eine Active Directory-Authentifizierung für Citrix Files erforderlich?
- Erfordert die erstmalige Verwendung der Citrix Files-App für XenMobile Single Sign-on?
- Gibt es in der aktuellen Umgebung einen Standard-IdP?
- Wie viele Domänen werden für SAML benötigt?
- Gibt es mehrere E-Mail-Aliasse für Active Directory-Benutzer?
- Sind Active Directory-Domänenmigrationen im Gang oder in Kürze geplant?

Designentscheidung:

In XenMobile Enterprise-Umgebungen kann SAML als Authentifizierungsmechanismus für Citrix Files verwendet werden. Authentifizierungsoptionen:

- Verwendung von XenMobile Server als Identitätsanbieter (IdP) für SAML

Diese Option kann eine hervorragende Benutzererfahrung bieten, sie automatisiert die Erstellung von Citrix Files-Konten und sie ermöglicht die Nutzung von Singe Sign-On-Features für mobile Apps.

- XenMobile Server ist für diesen Prozess optimiert: Es ist keine Active Directory-Synchronisierung erforderlich.
- Verwenden des Citrix Files-Benutzerverwaltungstools für die Benutzerbereitstellung
- Verwenden eines unterstützten Drittanbieter-IdPs für SAML

Wenn Sie einen unterstützten IdP haben und keine Single Sign-On-Features für mobile Apps benötigen, ist diese Option möglicherweise am besten geeignet. Auch sie erfordert die Verwendung des Citrix Files-Benutzerverwaltungstools für die Kontobereitstellung.

IdP-Lösungen von Drittanbietern wie ADFS bieten möglicherweise auf dem Windows-Client Single Sign-On-Features. Bewerten Sie die Anwendungsfälle vor Auswahl des SAML-Identitätsanbieters für Citrix Files.

Um beiden Anwendungsfällen zu genügen, können Sie ADFS und XenMobile als dualen IdP konfigurieren.

Mobile Apps

Relevanten Fragen:

- Welche mobile Citrix Files-App (öffentlich, MDM, MDX) möchten Sie verwenden?

Designentscheidung:

- Sie verteilen mobile Produktivitätsapps über den App-Store von Apple und Google Play. Mit der öffentlichen App Store-Verteilung erhalten Sie umschlossene Apps von der Citrix Downloadseite.
- Bei niedriger Sicherheitsstufe (ohne erforderliche Containerization) ist die öffentliche Citrix Files-App möglicherweise ungeeignet. In einer Nur-MDM-Umgebung können Sie die MDM-Version der Citrix Files-App über XenMobile im MDM-Modus bereitstellen.
- Weitere Informationen finden Sie unter Apps und Citrix Files für XenMobile.

Sicherheit, Richtlinien und Zugriffssteuerung

Relevanten Fragen:

- Welche Einschränkungen benötigen Sie für Desktop-, Internet- und mobile Benutzer?
- Welche Standardeinstellungen für die Zugriffssteuerung sollen für Benutzer gelten?
- Welche Dateispeicherrichtlinie möchten Sie verwenden?

Designentscheidung:

- Mit Citrix Files können Sie die Berechtigungen von Mitarbeitern und die Gerätesicherheit verwalten. Weitere Informationen finden Sie unter Mitarbeiterberechtigungen und Verwalten von Geräten und Apps.
- Einige Citrix Files-Einstellungen zur Gerätesicherheit steuern dieselben Features wie MDX-Richtlinien. In diesen Fällen haben die XenMobile-Richtlinien Vorrang gefolgt von der Citrix Files-Einstellung. Beispiel: Wenn Sie externe Apps in Citrix Files deaktivieren, in XenMobile jedoch aktivieren, werden die externen Apps in Citrix Files deaktiviert. Sie können die Apps so konfigurieren, dass XenMobile keine(n) PIN/Passcode anfordert, die Citrix Files-App jedoch schon.

Standard-Speicherzonen oder eingeschränkte Speicherzonen

Relevanten Fragen:

- Benötigen Sie eingeschränkte Speicherzonen?

Designentscheidung:

- Eine Standard-Speicherzone ist für nicht-vertrauliche Daten gedacht und ermöglicht Mitarbeitern das Freigeben von Daten für Personen, die keine Mitarbeiter sind. Diese Option unterstützt Workflows, bei denen Daten außerhalb Ihrer Domäne freigegeben werden.
- Eine eingeschränkte Speicherzone schützt vertrauliche Daten: Nur authentifizierte Domänenbenutzer haben Zugriff auf die in dieser Zone gespeicherten Daten.

Webproxys

Wahrscheinlichstes Szenario für die Leitung des XenMobile-Datenverkehrs über einen HTTP(S)-/SOCKS-Proxy: Wenn das Subnetz mit dem XenMobile-Server keinen ausgehenden Internetzugriff auf die erforderlichen Apple-, Google- oder Microsoft-IP-Adressen hat. Sie können in XenMobile Proxyservereinstellungen angeben, um den gesamten Internetdatenverkehr an den Proxyserver zu leiten. Weitere Informationen finden Sie unter Aktivieren von Proxyservern.

Die folgende Tabelle enthält die Vor- und Nachteile der gebräuchlichsten Proxykonfigurationen für XenMobile.

Option	Vorteile	Nachteile
HTTP(S)-/SOCKS-Proxy mit XenMobile-Server	Wenn Richtlinien keine ausgehenden Internetverbindungen vom Subnetz mit dem XenMobile-Server zulassen, können Sie einen HTTP(S)- oder SOCKS-Proxy für die Internetverbindung konfigurieren.	Fällt der Proxyserver aus, wird die Verbindung mit APNs (iOS) bzw. Firebase Cloud Messaging (Android) getrennt. Es sind dann keine Gerätebenachrichtigungen für iOS- und Android-Geräte möglich.
HTTP(S)-Proxy mit Secure Web	Sie können den HTTP-/HTTPS-Datenverkehr überwachen, um sicherzustellen, dass die Internetaktivität Ihren Standards entspricht.	Bei dieser Konfiguration muss der gesamte Internetdatenverkehr von Secure Web per Tunnel zurück ins Unternehmensnetzwerk geleitet werden, bevor die Daten wieder ins Internet übertragen werden. Wenn das Surfen durch die Internetverbindung einschränkt ist, kann diese Konfiguration die Surfleistung beeinträchtigen.

Die Konfiguration des Citrix ADC-Sitzungsprofils für Split-Tunneling wirkt sich wie folgt auf den Datenverkehr aus.

Wenn Citrix ADC-Split-Tunneling **deaktiviert** ist:

- Wenn die MDX-**Netzwerkzugriffsrichtlinie** auf **Tunnel zum internen Netzwerk** festgelegt ist, muss der gesamte Datenverkehr den Micro VPN- oder Clientless VPN (cVPN)-Tunnel zurück zum Citrix Gateway verwenden.
- Konfigurieren Sie die Citrix ADC-Datenverkehrsrichtlinien/-profile für den Proxyserver und binden Sie sie an die virtuelle IP-Adresse von Citrix Gateway.

> **Wichtig:**
>
> Schließen Sie auf jeden Fall cVPN-Datenverkehr von Secure Hub von dem Proxy aus.

- Weitere Informationen finden Sie unter XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode.

Wenn **Citrix ADC-Split-Tunneling aktiviert** ist:

- Wenn für Apps die MDX-**Netzwerkzugriffsrichtlinie** auf **Tunnel zum internen Netzwerk** festgelegt ist, versuchen die Apps zunächst, die Webressource direkt zu beziehen. Ist die Webressource nicht öffentlich verfügbar, verwenden die Apps Citrix Gateway.
- Konfigurieren Sie die Citrix ADC-Datenverkehrsrichtlinien/-profile für den Proxyserver. Binden Sie sie dann an die virtuelle IP-Adresse von Citrix Gateway.

> **Wichtig:**
>
> Schließen Sie auf jeden Fall cVPN-Datenverkehr von Secure Hub von dem Proxy aus.

Die Citrix ADC-Sitzungsprofilkonfiguration für **Split DNS** (unter **Client experience**) funktioniert ähnlich wie Split-Tunneling.

Wenn **Split DNS** aktiviert und auf **Both** festgelegt ist, gilt Folgendes:

- Der Client versucht, den FQDN lokal aufzulösen, und greift bei einem Fehler auf Citrix ADC zur DNS-Auflösung zurück.

Wenn **Split DNS** auf **Remote** festgelegt ist, gilt Folgendes:

- Es findet ausschließlich eine DNS-Auflösung durch Citrix ADC statt.

Wenn **Split DNS** auf **Local** festgelegt ist, gilt Folgendes:

- Der Client versucht, den FQDN lokal aufzulösen. Citrix ADC wird nicht für die DNS-Auflösung verwendet.

Zugriffssteuerung

Unternehmen können mobile Geräte innerhalb und außerhalb von Netzwerken verwalten. Enterprise Mobility Management-Lösungen wie XenMobile eignen sich hervorragend zur Bereitstellung

von Sicherheit und zur Steuerung von mobilen Geräten unabhängig vom Standort. In Kombination mit einer NAC-Lösung (Network Access Control) erhalten Sie jedoch QoS und eine gezieltere Steuerung für Geräte innerhalb Ihres Netzwerks. Mit dieser Kombination reicht die Bewertung der Gerätesicherheit durch XenMobile in Ihre NAC-Lösung hinein. Die NAC-Lösung kann dann anhand der XenMobile-Sicherheitsbewertung Authentifizierungsentscheidungen vereinfachen und bewältigen.

Sie können NAC-Richtlinien mit jeder der folgenden Lösungen durchsetzen:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix übernimmt keine Gewährleistung für die Integration anderer NAC-Lösungen.

Vorteile einer NAC-Integration in XenMobile:

- Mehr Sicherheit, Compliance und Steuerung für alle Endpunkte im Unternehmensnetzwerk.
- Eine NAC-Lösung ermöglicht Folgendes:
  - Erkennen von Geräten in dem Moment, in dem diese versuchen, eine Verbindung mit dem Netzwerk herzustellen.
  - Abfragen der Geräteattribute von XenMobile.
  - Entscheidung über Zulassen, Blockieren, Einschränken oder Umleiten der Geräte auf der Basis der abgefragten Geräteinformationen. Die Entscheidung hängt von den von Ihnen festgelegten Sicherheitsrichtlinien.
- Eine NAC-Lösung bietet IT-Administratoren eine Übersicht über nicht verwaltete und nicht richtlinientreue Geräte.

Eine Beschreibung der von XenMobile unterstützten NAC-Richtlinientreuefilter und eine Konfigurationsübersicht finden Sie unter Netzwerkzugriffssteuerung (NAC).

Anforderungen von Umgebungen mit mehreren Sites

January 5, 2022

Sie können XenMobile-Bereitstellungen mit mehreren Sites für hohe Verfügbarkeit und die Notfallwiederherstellung einrichten. Dieser Artikel bietet einen Überblick über die Modelle für hohe Verfügbarkeit und Notfallwiederherstellung in XenMobile.

Hohe Verfügbarkeit

- Bei XenMobile-Clusterknoten erfolgt der Lastausgleich über Citrix ADC. Weitere Informationen finden Sie unter Konfigurieren von Clustering
- XenMobile-Serverknoten werden in einer Aktiv/Aktiv-Konfiguration ausgeführt.

- Bei Kapazitätsbedarf werden weitere XenMobile-Serverknoten einem Hochverfügbarkeitscluster hinzugefügt. Ein Knoten kann bis zu etwa 8.500 Benutzergeräte bedienen (siehe Skalierbarkeit und Leistung).
- Citrix empfiehlt die Konfiguration von “n + 1” XenMobile-Servern: ein Server für jeweils 8.500 Benutzergeräte und ein zusätzlicher Server für Redundanz.
- Citrix empfiehlt alle Citrix ADC-Instanzen nach Möglichkeit für hohe Verfügbarkeit zu konfigurieren, damit Konfigurationen mit einem zweiten Citrix ADC synchronisiert werden können.
- Standardmäßig wird ein Citrix ADC-Hochverfügbarkeitspaar in einer Aktiv/Passiv-Konfiguration ausgeführt.

Eine typische XenMobile-Bereitstellung mit hoher Verfügbarkeit umfasst in der Regel Folgendes:

- Zwei Citrix ADC-Instanzen (VPX oder MPX). Bei Einsatz der Citrix ADC-SDX-Plattform ist ebenfalls hohe Verfügbarkeit in Betracht zu ziehen.
- Mindestens zwei XenMobile-Server mit identischen Datenbankeinstellungen.

Notfallwiederherstellung

Sie können XenMobile für die Notfallwiederherstellung mit zwei Datencentern – einem aktiven und einem passiven – konfigurieren. Mit Citrix ADC und Global Server Load Balancing (GSLB) wird ein Aktive/aktiv-Datenpfad erstellt, sodass die Benutzererfahrung der einer Aktiv/aktiv-Einrichtung entspricht.

Für die Notfallwiederherstellung umfasst eine XenMobile-Bereitstellung Folgendes:

- Zwei Datencenter, von denen jedes mindestens eine Citrix ADC-Instanz, die XenMobile-Server und SQL Server-Datenbanken enthält.
- Ein GSLB-Server, der den Datenverkehr zu den Datencentern leitet. Der GSLB-Server ist sowohl für die XenMobile-Registrierungs-URL als auch für die Citrix Gateway-URL für den Datenverkehr zur Site konfiguriert.
- Wenn Sie Citrix Gateway mit dem Citrix ADC für XenMobile-Assistenten konfigurieren, wird GSLB standardmäßig nicht für die Auflösung des Datenverkehrs über den XenMobile-Registrierungsserver und Citrix Gateway zum MAM-Lastausgleichsserver aktiviert. Daher sind zusätzliche Schritte erforderlich. Weitere Informationen zur Vorbereitung und Durchführung dieser Schritte finden Sie unter Notfallwiederherstellung.
- Geclusterte SQL Server von AlwaysOn-Verfügbarkeitsgruppen.
- Die Latenz zwischen XenMobile-Servern und SQL Server muss unter 5 ms liegen.

> **Hinweis:**
>
> Die in diesem Dokument beschriebenen Methoden zur Notfallwiederherstellung bieten nur eine automatische Notfallwiederherstellung für die Zugriffsebene. Sie müssen alle XenMobile-Serverknoten und die SQL Server-Datenbank in der Failoversite manuell starten, damit Geräte

> eine Verbindung mit dem XenMobile-Server herstellen können.

Integration in Citrix Gateway und Citrix ADC

January 5, 2022

Bei Integration in XenMobile bietet Citrix Gateway für MAM-Geräte einen Authentifizierungsmechanismus für den Remotezugriff auf das interne Netzwerk. Durch die Integration können mobile Produktivitätsapps über ein Micro-VPN auf Unternehmensserver im Intranet zugreifen. Das Micro-VPN wird von den Apps auf dem Mobilgerät zu Citrix Gateway erstellt. Citrix Gateway bietet einen Micro-VPN-Pfad für den Zugriff auf alle Unternehmensressourcen und unterstützt eine starke Multifaktorauthentifizierung.

Der Citrix ADC-Lastausgleich ist für alle XenMobile Server-Gerätemodi in folgenden Fällen erforderlich:

- Sie haben mehrere XenMobile-Server.
- XenMobile Server ist in der DMZ oder dem internen Netzwerk (d. h. der Datenverkehr fließt von den Geräten an Citrix ADC und dann an XenMobile).

Integrationsanforderungen nach XenMobile Server-Modus

Die Integrationsanforderungen für Citrix Gateway und Citrix ADC unterscheiden sich je nach den XenMobile-Servermodus (MAM, MDM oder ENT).

MAM

Mit XenMobile Server im MAM-Modus gilt Folgendes:

- **Citrix Gateway** ist erforderlich. Citrix Gateway bietet einen Micro-VPN-Pfad für den Zugriff auf alle Unternehmensressourcen und unterstützt eine starke Multifaktorauthentifizierung.
- **Citrix ADC** wird für den Lastausgleich empfohlen.

  Citrix empfiehlt die Bereitstellung von XenMobile in einer Konfiguration mit hoher Verfügbarkeit, für die ein Load Balancer vor XenMobile erforderlich ist. Weitere Informationen finden Sie unter MAM und Legacy-MAM-Modus.

MDM

Für XenMobile Server im MDM-Modus gilt Folgendes:

- Citrix Gateway ist nicht erforderlich. Für MDM-Bereitstellungen empfiehlt Citrix die Verwendung von Citrix Gateway für VPNs für Mobilgeräte.

- Citrix ADC wird für die Gewährleistung der Sicherheit und für den Lastausgleich empfohlen.

  Citrix empfiehlt die Bereitstellung einer Citrix ADC-Appliance vor XenMobile Server zur Gewährleistung der Sicherheit und zum Lastausgleich. Bei Standardbereitstellungen mit XenMobile in der DMZ empfiehlt Citrix den Citrix ADC für XenMobile-Assistenten und den XenMobile Server-Lastausgleich im SSL-Brückenmodus. Bei Bereitstellungen mit folgenden Eigenschaften kommt auch SSL-Offload in Betracht:

  - Der XenMobile-Server ist nicht in der DMZ, sondern im internen Netzwerk
  - Das Sicherheitsteam benötigt eine Konfiguration mit SSL-Bridge

  Citrix rät davon ab, den XenMobile-Server über NAT, Drittanbieter-Proxys oder Load Balancer für MDM dem Internet auszusetzen. Diese Konfigurationen stellen ein Sicherheitsrisiko dar, selbst wenn der SSL-Datenverkehr auf dem XenMobile-Server endet (SSL-Bridge).

  In Umgebungen mit hoher Sicherheit erfüllt oder übertrifft Citrix ADC mit der standardmäßigen XenMobile-Konfiguration die Sicherheitsanforderungen.

  In MDM-Umgebungen mit höchsten Sicherheitsanforderungen bietet die SSL-Terminierung am Citrix ADC die Möglichkeit, den Datenverkehr am Umkreis zu untersuchen und gewährleistet gleichzeitig eine Ende-zu-Ende-SSL-Verschlüsselung. Weitere Informationen finden Sie unter Sicherheitsanforderungen. Citrix ADC bietet Optionen zum Definieren von SSL-/TLS-Verschlüsselungsverfahren und SSL FIPS Citrix ADC-Hardware.

ENT (MAM+MDM)

Für XenMobile Server im ENT-Modus gilt Folgendes:

- Citrix Gateway ist erforderlich. Citrix Gateway bietet einen Micro-VPN-Pfad für den Zugriff auf alle Unternehmensressourcen und unterstützt eine starke Multifaktorauthentifizierung.

  Wenn XenMobile Server im ENT-Modus betrieben wird und ein Benutzer die MDM-Registrierung ablehnt, wird sein Gerät im Legacy-MAM-Modus betrieben. Im Legacy-MAM-Modus werden Geräte unter Verwendung des Citrix Gateway-FQDN registriert. Weitere Informationen finden Sie unter MAM und Legacy-MAM-Modus.

- Citrix ADC wird für den Lastausgleich empfohlen. Weitere Informationen finden Sie weiter oben zu Citrix ADC unter “MDM”.

> **Wichtig:**
>
> Bei der erstmaligen Registrierung erfolgt die Authentifizierung für den Datenverkehr von Benutzergeräten auf dem XenMobile-Server, unabhängig davon, ob Sie virtuelle Lastausgleichsserver für SSL-Offload oder SSL-Brücke konfiguriert haben.

Designentscheidungen

Nachfolgend finden Sie eine Zusammenfassung der zahlreichen Designentscheidungen, die bei der Planung einer Citrix Gateway-Integration in XenMobile getroffen werden müssen.

Lizenzierung und Edition

Entscheidungsdetails:

- Welche Edition von Citrix ADC möchten Sie verwenden?
- Haben Sie Plattformlizenzen auf Citrix ADC angewendet?
- Wenn Sie MAM-Funktionalität benötigen, haben Sie die universelle Lizenz für Citrix ADC angewendet?

Designhilfe:

Stellen Sie sicher, dass Sie die richtigen Lizenzen auf das Citrix Gateway anwenden. Wenn Sie Citrix Gateway Connector für Exchange ActiveSync verwenden, ist möglicherweise integriertes Zwischenspeichern erforderlich. Daher muss die korrekte Citrix ADC-Edition vorliegen.

Zum Aktivieren von Citrix ADC-Features gelten folgende Lizenzanforderungen:

- XenMobile-MDM-Lastausgleich erfordert mindestens eine Standardplattformlizenz für Citrix ADC.
- Content Collaboration-Lastausgleich mit Speicherzonencontroller erfordert mindestens eine Standardplattformlizenz für Citrix ADC.
- Die XenMobile Enterprise-Edition enthält die erforderlichen universellen Citrix Gateway-Lizenzen für MAM.
- Exchange-Lastausgleich erfordert eine Platinum- oder Enterprise-Plattformlizenz für Citrix ADC sowie eine zusätzliche Integrated Caching-Lizenz.

Citrix ADC-Version für XenMobile

Entscheidungsdetails:

- Welche Citrix ADC-Version wird in der XenMobile-Umgebung ausgeführt?
- Benötigen Sie eine separate Instanz?

Designhilfe:

Citrix empfiehlt die Verwendung einer dedizierten Citrix ADC-Instanz für den virtuellen Citrix Gateway-Server. Stellen Sie sicher, dass Citrix ADC-Version und -Build in der für die XenMobile-Umgebung geltenden Mindestversion vorliegen. Normalerweise empfiehlt sich die Verwendung der neuesten kompatiblen Citrix ADC-Version für XenMobile. Wenn ein Upgrade von Citrix Gateway die vorhandene Umgebung beeinträchtigen würde, ist möglicherweise eine zweite, dedizierte Instanz für XenMobile die geeignete Lösung.

Wenn Sie eine Citrix ADC-Instanz für XenMobile und eine andere App, die VPN-Verbindungen verwendet, nutzen möchten, stellen Sie sicher, dass Sie genügend VPN-Lizenzen für beides haben. Hinweis: Eine Test- und eine Produktionsumgebung für XenMobile können keine Citrix ADC-Instanz gemeinsam nutzen.

Zertifikate

Entscheidungsdetails:

- Benötigen Sie ein höheres Maß an Sicherheit für Registrierungen und den Zugriff auf die XenMobile-Umgebung?
- Ist LDAP keine Option?

Designhilfe:

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. Sie können Zertifikate mit LDAP für die zweistufige Authentifizierung verwenden und so ohne RSA-Server ein höheres Maß an Sicherheit gewährleisten.

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 für die Authentifizierung bei der XenMobile-Umgebung verwendet wird, und stellt dieses bereit.

XenMobile unterstützt Zertifikatsperrlisten (CRL) nur für Drittanbieterzertifizierungsstellen. Wenn Sie eine Microsoft-Zertifizierungsstelle konfiguriert haben, wird in XenMobile zum Verwalten der Zertifikatsperre Citrix ADC verwendet. Bedenken Sie beim Konfigurieren der Clientzertifikatauthentifizierung, ob Sie die Citrix ADC-Einstellung für Zertifikatsperrlisten (CRL) **Enable CRL Auto Refresh** konfigurieren müssen. Dadurch wird sichergestellt, dass Benutzer von bei MAM registrierten Geräten keine Authentifizierung mit einem existierenden Zertifikat am Gerät durchführen können. XenMobile stellt ein neues Zertifikat aus, da es Benutzer nicht daran hindert, ein Benutzerzertifikat zu generieren, wenn eines gesperrt wird. Diese Einstellung erhöht die Sicherheit von PKI-Entitäten, wenn über die Zertifikatsperrliste auf abgelaufene PKI-Entitäten geprüft wird.

Netzwerktopologie

Entscheidungsdetails:

- Welche Citrix ADC-Topologie ist erforderlich?

Designhilfe:

Citrix empfiehlt die Verwendung einer Citrix ADC-Instanz für XenMobile. Allerdings ist ein Datenfluss vom internen Netzwerk an die DMZ vielleicht unerwünscht. In diesem Fall sollten Sie eine zusätzliche Citrix ADC-Instanz einrichten. Verwenden Sie eine Citrix ADC-Instanz für interne Benutzer und eine für externe Benutzer. Wenn Benutzer zwischen dem internen und externen Netzwerk wechseln, werden durch das Zwischenspeichern von DNS-Datensätzen evtl. mehr Secure Hub-Anmeldeaufforderungen erzeugt.

XenMobile unterstützt Citrix Gateway-Double-Hop nicht.

Dedizierte oder gemeinsam genutzt Citrix Gateway-VIPs

Entscheidungsdetails:

- Verwenden Sie zurzeit Citrix Gateway für Virtual Apps and Desktops?
- Soll XenMobile das gleiche Citrix Gateway wie Virtual Apps and Desktops nutzen?
- Welche Authentifizierungsanforderungen gelten für beide Datenströme?

Designhilfe:

Wenn Ihre Citrix Umgebung sowohl XenMobile als auch Citrix Virtual Apps and Desktops enthält, können Sie für beides dieselbe Citrix ADC-Instanz und denselben virtuellen Citrix Gateway-Server verwenden. Aufgrund möglicher Versionskonflikte und der Umgebungsisolierung werden eine dedizierte Citrix ADC-Instanz und ein dediziertes Citrix Gateway für jede XenMobile-Umgebung empfohlen. Ist eine dedizierte Citrix ADC-Instanz nicht möglich, empfiehlt Citrix, einen dedizierten virtuellen Citrix Gateway-Server zu verwenden, um die Datenströme für Secure Hub zu trennen. Diese Konfiguration ist die Alternative zu einem von XenMobile und Virtual Apps and Desktops gemeinsam genutzten virtuellen Server.

Wenn Sie die LDAP-Authentifizierung verwenden, ist eine Authentifizierung von Receiver und Secure Hub bei demselben Citrix Gateway problemlos möglich. Bei Verwendung der zertifikatbasierten Authentifizierung überträgt XenMobile ein Zertifikat in den MDX-Container und Secure Hub verwendet das Zertifikat zur Authentifizierung beim Citrix Gateway. Receiver ist von Secure Hub getrennt und kann für die Authentifizierung bei demselben Citrix Gateway nicht dasselbe Zertifikat verwenden.

Mit folgendem Workaround können Sie denselben FQDN für zwei Citrix Gateway-VIPs verwenden:

- Erstellen Sie zwei Citrix Gateway-VIPs mit derselben IP-Adresse. Die VIP für Secure Hub verwendet den Standardport 443 und die VIP für Citrix Virtual Apps and Desktops (= Receiver-Bereitstellung) den Port 444.
- Ein FQDN wird dann in die gleiche IP-Adresse aufgelöst.
- Für diesen Workaround konfigurieren Sie StoreFront so, dass eine ICA-Datei für Port 444 anstelle des Standardports 443 zurückgegeben wird. Der Workaround erfordert keine Eingabe einer Portnummer durch die Benutzer.

Citrix Gateway-Timeouts

Entscheidungsdetails:

- Wie möchten Sie die Citrix Gateway-Timeouts für den XenMobile-Datenverkehr konfigurieren?

Designhilfe:

Citrix Gateway enthält die Einstellungen “Session time-out” und “Forced time-out”. Weitere Informationen finden Sie unter Empfohlene Konfigurationen. Beachten Sie, dass es für Hintergrunddienste, Citrix ADC und für den Offlinezugriff auf Anwendungen unterschiedliche Timeoutwerte gibt.

IP-Adresse des XenMobile Load Balancers für MAM

Entscheidungsdetails:

- Verwenden Sie interne oder externe IP-Adressen für virtuelle IP-Adressen?

Designhilfe:

In Umgebungen, in denen öffentliche IP-Adressen als Citrix Gateway-VIP verwendet werden können, führt eine solche Zuweisung der XenMobile Load Balancer-VIP zu Fehlern bei der Registrierung.

Stellen Sie sicher, dass für die Load Balancer-VIP eine interne IP-Adresse verwendet wird, um Registrierungsfehler zu vermeiden. Die virtuelle IP-Adresse muss dem Standard RFC 1918 für private IP-Adressen entsprechen. Wenn Sie für diesen virtuellen Server keine private IP-Adresse verwenden, kann Citrix ADC XenMobile Server bei der Authentifizierung nicht kontaktieren. Einzelheiten finden Sie unter https://support.citrix.com/article/CTX200430.

MDM-Lastausgleichsmechanismus

Entscheidungsdetails:

- Wie erfolgt der Lastausgleich zwischen den XenMobile-Servern durch Citrix Gateway?

Designhilfe:

Verwenden Sie SSL-Brücke, wenn XenMobile in der DMZ ist. Verwenden Sie SSL-Offload, sofern dies zur Erfüllung von Sicherheitsstandards erforderlich ist, wenn XenMobile im internen Netzwerk ist.

- Bei einem XenMobile-Lastausgleich mit Citrix ADC-VIPs im SSL-Brückenmodus fließt der Internetdatenverkehr direkt an XenMobile Server, wo die Verbindungen enden. Der SSL-Brückenmodus ist im Hinblick auf Einrichtung und Problembehandlung am einfachsten.
- Bei einem XenMobile Server-Lastausgleich mit Citrix ADC-VIPs im SSL-Offload-Modus fließt der Internetdatenverkehr direkt an Citrix ADC, wo die Verbindungen enden. Es werden dann neue Sitzungen von Citrix ADC zu XenMobile Server eingerichtet. Der SSL-Offload-Modus ist bei Einrichtung und Problembehandlung etwas komplexer.

Dienstport für MDM-Lastausgleich mit SSL-Offload

Entscheidungsdetails:

- Wenn Sie den SSL-Offload-Modus für den Lastausgleich verwenden, welchen Port verwendet der Back-End-Dienst?

Designhilfe:

Wählen Sie für den SSL-Offload Port 80 oder 8443:

- Verwenden Sie Port 80 an XenMobile Server für echtes Offloading.
- End-to-End-Verschlüsselung, d. h. eine erneute Verschlüsselung des Datenverkehrs, wird nicht unterstützt. Weitere Informationen finden Sie in dem Citrix Support-Artikel Supported Architectures Between NetScaler and XenMobile Server.

Registrierungs-FQDN

Entscheidungsdetails:

- Welcher FQDN soll für die Registrierung und die XenMobile-Instanz/Lastausgleichs-VIP verwendet werden?

Designhilfe:

Für die Konfiguration des ersten XenMobile-Servers in einem Cluster müssen Sie den XenMobile-Server-FQDN eingeben. Dieser FQDN muss der MDM-VIP-URL und der internen MAM-LB-VIP-URL entsprechen. (Ein interner Citrix ADC-Adressdatensatz löst die MAM-LB-VIP auf.) Weitere Informationen finden Sie weiter unten unter “Registrierungs-FQDN für die einzelnen Verwaltungsmodi”.

Außerdem müssen Sie das gleiche Zertifikat verwenden wie Folgendes:

- XenMobile SSL-Listenerzertifikat
- Internes MAM-LB-VIP-Zertifikat
- MDM-VIP-Zertifikat (bei Verwendung von SSL-Offload für MDM-VIP)

> **Wichtig:**
>
> Nachdem Sie den Registrierungs-FQDN konfiguriert haben, können Sie ihn nicht mehr ändern. Ein neuer Registrierungs-FQDN erfordert eine neue SQL Server-Datenbank und die Neuerstellung von XenMobile Server.

Secure Web-Datenverkehr

Entscheidungsdetails:

- Soll Secure Web auf das interne Webbrowsing beschränkt werden?
- Soll Secure Web für das interne und das externe Webbrowsing aktiviert werden?

Designhilfe:

Wenn Sie Secure Web nur für das interne Webbrowsing verwenden, bereitet das Konfigurieren von Citrix Gateway keine Probleme. Secure Web muss alle internen Sites standardmäßig erreichen. Möglicherweise müssen Sie Firewalls und Proxyserver konfigurieren.

Wenn Sie Secure Web für das interne und das externe Browsing verwenden möchten, müssen Sie für die SNIP ausgehenden Internetzugriff aktivieren. Geräte, die (mit dem MDX-Container) registriert wurden, werden in der Regel als Erweiterung des Unternehmensnetzwerks angesehen. Daher ist es normalerweise erwünscht, dass Secure Web-Verbindungen zu Citrix ADC zurückgehen und über einen Proxyserver in das Internet führen. Standardmäßig verwendet Secure Web pro Anwendung einen VPN-Tunnel zurück zum internen Netzwerk für den gesamten Netzwerkzugriff. Citrix ADC verwendet Split-Tunnel-Einstellungen.

Eine Beschreibung von Secure Web-Verbindungen finden Sie unter Konfigurieren von Benutzerverbindungen.

Pushbenachrichtigungen für Secure Mail

Entscheidungsdetails:

- Möchten Sie Pushbenachrichtigungen verwenden?

Designhilfe für iOS:

Ihre Citrix Gateway-Konfiguration kann eine STA enthalten, wobei Split-Tunneling deaktiviert ist. Das Citrix Gateway muss Datenverkehr von Secure Mail zu den für Secure Mail-Pushbenachrichtigungen für iOS angegebenen Citrix Listenerdienst-URLs zulassen.

Designhilfe für Android:

Steuern Sie mit Firebase Cloud Messaging (FCM), wie und wann Android-Geräte eine Verbindung zu XenMobile herstellen. Wenn FCM konfiguriert ist, lösen Sicherheitsaktionen oder Bereitstellungsbefehle eine Pushbenachrichtigung an Secure Hub aus, sodass der Benutzer aufgefordert wird, eine erneute Verbindung mit XenMobile Server herzustellen.

HDX-STAs

Entscheidungsdetails:

- Welche STAs sollte man bei Integration des Zugriffs auf HDX-Anwendungen verwenden?

Designhilfe:

HDX STAs müssen mit den STAs in StoreFront übereinstimmen und für die Virtual Apps and Desktops-Farm gültig sein.

Citrix Files und Citrix Content Collaboration

Entscheidungsdetails:

- Möchten Sie Speicherzonencontroller in der Umgebung verwenden?
- Welche Citrix Files-VIP-URL möchten Sie verwenden?

Designhilfe:

Wenn die Umgebung Speicherzonencontroller enthält, müssen Sie Folgendes korrekt konfigurieren:

- Citrix Files Switch-VIP (zur Kommunikation zwischen Citrix Files-Steuerungsebene und Speicherzonencontroller-Servern)
- Citrix Files-Lastausgleichs-VIPs
- Alle erforderlichen Richtlinien und Profile

Weitere Informationen finden Sie in der Dokumentation für den Speicherzonencontroller.

SAML-Identitätsanbieter

Entscheidungsdetails:

- Wenn für Citrix Files SAML erforderlich ist, soll XenMobile als SAML-Identitätsanbieter verwendet werden?

Designhilfe:

Die empfohlene bewährte Methode ist die Integration von Citrix Files in XenMobile Advanced Edition oder XenMobile Enterprise Edition – eine einfachere Alternative zur Konfiguration eines SAML-basierten Verbunds. Wenn Sie Citrix Files mit diesen XenMobile-Editionen verwenden, stellt XenMobile für Citrix Files Folgendes bereit:

- Authentifizierung per Single Sign-On (SSO) für Benutzer mobiler Produktivitätsapps
- Active Directory-basiertes Benutzerkontoprovisioning.
- Umfassende Richtlinien zur Zugriffssteuerung

Mit der XenMobile-Konsole können Sie Citrix Files konfigurieren sowie Servicelevel und Lizenznutzung überwachen.

Es gibt zwei Arten von Citrix Files-Clients: Citrix Files für XenMobile-Clients (“umschlossenes Citrix Files”) und mobile Citrix Files-Clients (“nicht umschlossenes Citrix Files”). Die Unterschiede werden unter Unterschiede zwischen Citrix Files für XenMobile-Clients und mobilen Citrix Files-Clients erläutert.

Sie können XenMobile und Citrix Content Collaboration so konfigurieren, dass Sie mit SAML per SSO auf Folgendes zugreifen können:

- Mobile Citrix Files-Apps

- Nicht umschlossene Citrix Files-Clients, z. B. die Website, das Outlook-Plug-in oder Synchronisierungsclients

Zur Verwendung von XenMobile als SAML-IdP für Citrix Files stellen Sie sicher, dass die richtigen Konfigurationen vorhanden sind. Weitere Informationen finden Sie unter SAML für SSO bei Citrix Files.

Direkte ShareConnect-Verbindungen

Entscheidungsdetails:

- Müssen Benutzer von einem Computer oder Mobilgerät mit ShareConnect direkt auf einen Hostcomputer zugreifen?

Designhilfe:

Mit ShareConnect können Benutzer sichere Verbindungen von iPads sowie Android-Tablets und -Telefonen mit ihren Computern herstellen und auf Dateien und Anwendungen zugreifen. Bei direkten Verbindungen bietet XenMobile über Citrix Gateway sicheren Benutzerzugriff auf Ressourcen außerhalb des lokalen Netzwerks. Informationen zur Konfiguration finden Sie unter ShareConnect.

Registrierungs-FQDN für jeden Verwaltungsmodus

Verwaltungsmodus	Registrierungs-FQDN
Enterprise (MDM + MAM) mit verbindlicher MDM-Registrierung	FQDN des XenMobile-Servers
Enterprise (MDM + MAM) mit optionaler MDM-Registrierung	FQDN des XenMobile-Servers oder Citrix Gateways
Nur MDM	FQDN des XenMobile-Servers
Nur-MAM (Legacy)	Citrix Gateway-FQDN
Nur MAM	FQDN des XenMobile-Servers

Zusammenfassung der Bereitstellung

Citrix empfiehlt die Verwendung des Assistenten für Citrix ADC für XenMobile zur Gewährleistung einer ordnungsgemäßen Konfiguration. Sie können den Assistenten nur einmal verwenden. Wenn Sie mehrere XenMobile-Instanzen haben (z. B. für die Test-, die Entwicklungs- und die Produktionsumgebung), müssen Sie Citrix ADC für die zusätzlichen Umgebungen manuell konfigurieren. Bei einer funktionierenden Umgebung notieren Sie sich die Einstellungen, bevor Sie Citrix ADC manuell für XenMobile konfigurieren.

Die wichtigste Entscheidung, die Sie bei Verwendung des Assistenten treffen, ist die Wahl zwischen HTTPS und HTTP für die Kommunikation mit dem XenMobile-Server. HTTPS bietet eine sichere Back-End-Kommunikation, da der Datenverkehr zwischen Citrix ADC und XenMobile verschlüsselt wird. Die erneute Verschlüsselung hat allerdings Auswirkungen auf die Leistung von XenMobile Server. HTTP bietet die bessere XenMobile Server-Leistung. Der Datenverkehr zwischen Citrix ADC und XenMobile ist nicht verschlüsselt. Die folgenden Tabellen enthalten die erforderlichen HTTP- und HTTPS-Ports für Citrix ADC und XenMobile Server.

HTTPS

Citrix empfiehlt normalerweise die Verwendung einer SSL-Brücke für Citrix ADC in Konfigurationen mit virtuellem MDM-Server. Bei Verwendung von SSL-Offload für Citrix ADC mit virtuellen MDM-Servern unterstützt XenMobile nur Port 80 als Back-End-Dienst.

Verwaltungsmodus	Citrix ADC-Lastausgleichsmetho	SSL-Neuverschlüsselung	XenMobile-Serverport
MDM	SSL-Brücke	Nicht zutreffend	443, 8443
MAM	SSL-Offload	Aktiviert	8443
Enterprise	MDM: SSL-Brücke	Nicht zutreffend	443, 8443
Enterprise	MAM: SSL-Offload	Aktiviert	8443

HTTP

Verwaltungsmodus	Citrix ADC-Lastausgleichsmetho	SSL-Neuverschlüsselung	XenMobile-Serverport
MDM	SSL-Offload	Nicht unterstützt	80
MAM	SSL-Offload	Aktiviert	8443
Enterprise	MDM: SSL-Offload	Nicht unterstützt	80
Enterprise	MAM: SSL-Offload	Aktiviert	8443

Diagramme von Citrix Gateway in XenMobile-Bereitstellungen finden Sie in unter Referenzarchitektur für On-Premises-Bereitstellungen.

SSO- und Proxy-Überlegungen für MDX-Apps

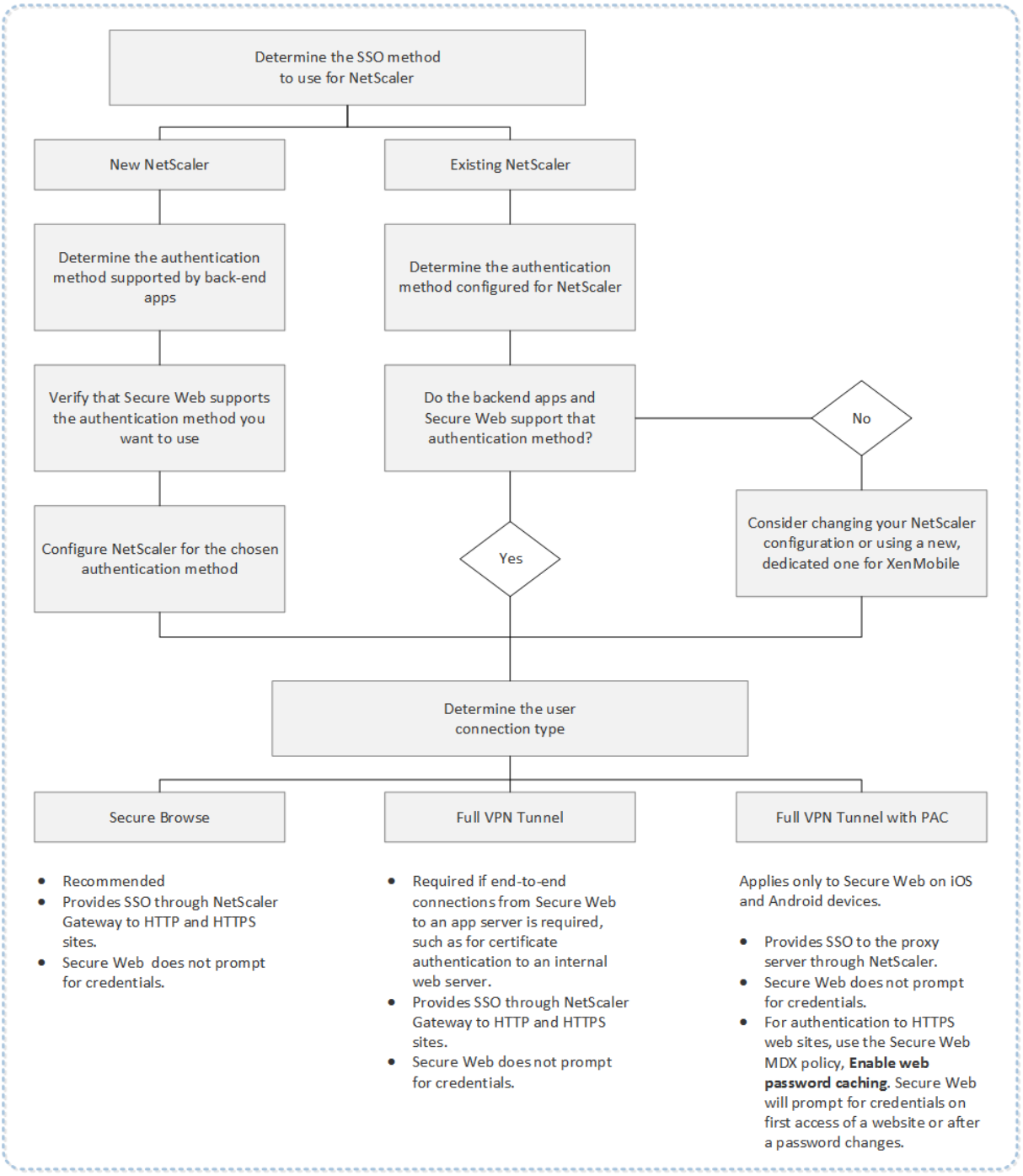
January 5, 2022

Durch die XenMobile-Integration mit Citrix ADC können Sie Benutzern Single Sign-On (SSO) für alle Backend-HTTP- und -HTTPS-Ressourcen bereitstellen. Je nach Ihren SSO-Authentifizierungsanforderungen können Sie zwei Arten der Benutzerverbindung für eine MDX-App konfigurieren:

- Secure Browse (eine Variante des clientlosen VPNs)
- Vollständiger VPN-Tunnel

Bietet Citrix ADC nicht die bestgeeignete SSO-Methode für Ihre Umgebung, können Sie eine MDX-App mit richtlinienbasiertem lokalem Kennwortcaching einrichten. In diesem Artikel werden die verschiedenen SSO- und Proxyoptionen erläutert, wobei der Schwerpunkt auf Secure Web liegt. Die Konzepte gelten für weitere MDX-Apps.

Das folgende Flussdiagramm stellt die Entscheidungsfindung bei der Wahl der SSO- und Benutzerverbindungen zusammen.



Citrix ADC-Authentifizierungsmethoden

Dieser Abschnitt enthält allgemeine Informationen zu den von Citrix ADC unterstützten Authentifizierungsmethoden.

SAML-Authentifizierung

Wenn Sie Citrix ADC für Security Assertion Markup Language (SAML) konfigurieren, können die Benutzer eine Verbindung mit Web-Apps herstellen, die SAML für Single Sign-On unterstützen. Citrix Gateway unterstützt Single Sign-On per Identitätsanbieter (IdP) für SAML-Web-Apps.

Erforderliche Konfiguration:

- Konfigurieren von SAML-SSO im Citrix ADC-Traffic-Profil.
- Konfigurieren des SAML-IdP für den angeforderten Dienst.

NTLM-Authentifizierung

Wenn SSO bei Web-Apps im Sitzungsprofil aktiviert ist, führt Citrix ADC die NTLM-Authentifizierung automatisch durch.

Erforderliche Konfiguration:

- Aktivieren von SSO im Citrix ADC-Session- oder Traffic-Profil.

Kerberos-Identitätswechsel

XenMobile unterstützt Kerberos nur für Secure Web. Wenn Sie Citrix ADC für Kerberos SSO konfigurieren, verwendet Citrix ADC das Identitätswechselverfahren, wenn ein Benutzerkennwort für Citrix ADC verfügbar ist. Das bedeutet, dass Citrix ADC die Benutzeranmeldeinformationen verwendet, um das für den Zugriff auf Dienste wie Secure Web erforderliche Ticket zu erhalten.

Erforderliche Konfiguration:

- Konfigurieren der Citrix ADC-Sitzungsrichtlinie “Worx”, sodass sie den Kerberos-Bereich der Verbindung identifizieren kann.
- Konfigurieren eines Kontos zur eingeschränkten Kerberos-Delegierung (KCD) auf Citrix ADC. Konfigurieren Sie dieses Konto ohne Kennwort und binden Sie es an eine Traffic-Richtlinie im XenMobile-Gateway.
- Einzelheiten zu dieser und weiteren Konfigurationen finden Sie im Citrix Blog unter WorxWeb and Kerberos Impersonation SSO.

Eingeschränkte Kerberos-Delegierung

XenMobile unterstützt Kerberos nur für Secure Web. Wenn Sie Citrix ADC für Kerberos SSO konfigurieren, verwendet Citrix ADC die eingeschränkte Delegierung, wenn kein Benutzerkennwort für Citrix ADC verfügbar ist.

Bei der eingeschränkten Delegierung verwendet Citrix ADC ein spezifisches Administratorkonto für den Abruf von Tickets für Benutzer und Dienste.

Erforderliche Konfiguration:

- Konfigurieren von je einem Konto für die eingeschränkte Kerberos-Delegierung (KCD) in Active Directory (mit den erforderlichen Berechtigungen) und auf Citrix ADC.
- Aktivieren von SSO im Citrix ADC-Traffic-Profil.
- Konfigurieren Sie die Backend-Website für die Kerberos-Authentifizierung.

Formularbasierte Authentifizierung

Wenn Sie Citrix ADC für formularbasiertes Single Sign-On konfigurieren, können sich die Benutzer einmal anmelden und dann auf alle geschützten Apps im Netzwerk zuzugreifen. Diese Authentifizierungsmethode gilt für Apps, für die Secure Browse oder ein vollständiges VPN verwendet wird.

Erforderliche Konfiguration:

- Konfigurieren von formularbasiertem SSO im Citrix ADC-Traffic-Profil.

Digest-HTTP-Authentifizierung

Wenn SSO bei Web-Apps im Sitzungsprofil aktiviert ist, führt Citrix ADC die Digest-HTTP-Authentifizierung automatisch durch. Diese Authentifizierungsmethode gilt für Apps, für die Secure Browse oder ein vollständiges VPN verwendet wird.

Erforderliche Konfiguration:

- Aktivieren von SSO im Citrix ADC-Session- oder Traffic-Profil.

Einfache HTTP-Authentifizierung

Wenn SSO bei Web-Apps im Sitzungsprofil aktiviert ist, führt Citrix ADC die einfache HTTP-Authentifizierung automatisch durch. Diese Authentifizierungsmethode gilt für Apps, für die Secure Browse oder ein vollständiges VPN verwendet wird.

Erforderliche Konfiguration:

- Aktivieren von SSO im Citrix ADC-Session- oder Traffic-Profil.

Secure Browse, vollständiger VPN-Tunnel oder vollständiger VPN-Tunnel mit PAC

In den folgenden Abschnitten werden die Benutzerverbindungsarten von Secure Web beschrieben. Weitere Informationen finden Sie in der Citrix-Dokumentation im Artikel zu Secure Web unter Konfigurieren von Benutzerverbindungen.

Vollständiger VPN-Tunnel

Verbindungen, die einen Tunnel zum internen Netzwerk benötigen, können einen vollständigen VPN-Tunnel verwenden. Verwenden Sie die Secure Web-Richtlinie “Bevorzugter VPN-Modus” zum Konfigurieren des vollständigen VPN-Tunnels. Citrix empfiehlt die Einstellung “Vollständiger VPN-Tunnel” für Verbindungen, die Clientzertifikate oder End-To-End-SSL für Ressourcen im internen Netzwerk einsetzen. Vollständiger VPN-Tunnel unterstützt beliebige Protokolle über TCP. Sie können einen vollständigen VPN-Tunnel für Windows-, Mac-, iOS- und Android-Geräte verwenden.

Bei Verwendung eines vollständigen VPN-Tunnels genießt Citrix ADC keine Transparenz in HTTPS-Sitzungen.

Secure Browse

Verbindungen, die einen Tunnel zum internen Netzwerk benötigen, können eine Variante eines clientlosen VPNs (Secure Browse) verwenden. Secure Browse ist die Standardkonfiguration für die Secure Web-Richtlinie **Bevorzugter VPN-Modus**. Citrix empfiehlt Secure Browse für Verbindungen, die Single Sign-On (SSO) erfordern.

Bei Verwendung von Secure Browse unterteilt Citrix ADC die HTTPS-Sitzung in zwei Teile:

- Client zum Citrix ADC
- Citrix ADC zum Back-End-Ressourcenserver.

Auf diese Weise genießt Citrix ADC volle Transparenz in allen Transaktionen zwischen dem Client und dem Server und kann SSO bereitstellen.

Sie können auch Proxyserver für Secure Web konfigurieren, wenn der Secure Browse-Modus aktiviert ist. Weitere Informationen finden Sie in dem Blog XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

Vollständiger VPN-Tunnel mit PAC

Sie können eine PAC-Datei (Proxy Automatic Configuration) mit einem vollständigen VPN-Tunnel für Secure Web auf iOS- und Android-Geräten verwenden. XenMobile unterstützt die von Citrix ADC bereitgestellte Proxyauthentifizierung. Eine PAC-Datei enthält Regeln, die festlegen, wie Webbrowser einen Proxy für den Zugriff auf eine URL auswählen. Mit Regeln in einer PAC-Datei kann die Handhabung von internen und externen Sites festgelegt werden. Secure Web analysiert die Regeln in der PAC-Datei und sendet die Proxyserverinformationen an Citrix Gateway. Citrix Gateway sieht weder PAC-Datei noch Proxyserver.

Für die Authentifizierung bei HTTPS-Websites ermöglicht die Secure Web-MDX-Richtlinie **Webkennwortcaching aktivieren**, dass Secure Web Authentifizierungen durchführen und Single Sign-On beim Proxyserver über MDX bereitstellen kann.

Split-Tunneling in Citrix ADC

Bei der Planung der SSO- und Proxykonfiguration müssen Sie auch überlegen, ob Sie Split-Tunneling in Citrix ADC verwenden möchten. Citrix empfiehlt, Split-Tunneling in Citrix ADC nur zu verwenden, wenn es erforderlich ist. In diesem Abschnitt finden Sie einen Überblick über die Funktionsweise von Split-Tunneling: Citrix ADC ermittelt den Datenverkehrspfad anhand seiner Routingtabelle. Wenn Split-Tunneling in Citrix ADC aktiviert ist, unterscheidet Secure Hub internen (geschützten) Netzwerkverkehr und Internetverkehr. Secure Hub unterscheidet anhand des DNS-Suffixes und der Intranetanwendungen. Secure Hub leitet dann nur den internen Datenverkehr durch den VPN-Tunnel. Ist Split-Tunneling in Citrix ADC deaktiviert, wird der gesamte Datenverkehr durch den VPN-Tunnel geleitet.

- Wenn Sie aus Sicherheitsgründen den gesamten Datenverkehr überwachen möchten, deaktivieren Sie Split-Tunneling in Citrix ADC. Der gesamte Datenverkehr fließt dann durch den VPN-Tunnel.
- Wenn Sie einen vollständigen VPN-Tunnel mit PAC verwenden, müssen Sie Split-Tunneling in Citrix Gateway deaktivieren. Falls Sie bei aktiviertem Split-Tunneling eine PAC-Datei konfigurieren, setzen die Regeln der PAC-Datei die Split-Tunneling-Regeln in Citrix ADC außer Kraft. Ein in einer Traffic-Richtlinie konfigurierter Proxyserver setzt keine Split-Tunneling-Regeln in Citrix ADC außer Kraft.

Die Richtlinie **Netzwerkzugriff** ist für Secure Web standardmäßig auf **Tunnel zum internen Netzwerk** festgelegt. Bei dieser Konfiguration verwenden MDX-Apps die Split-Tunneling-Einstellungen von Citrix ADC. Bei einigen anderen mobilen Produktivitätsapps gibt es eine andere Standardeinstellung für die Richtlinie **Netzwerkzugriff**.

Citrix Gateway bietet auch einen Modus mit Reverse-Split-Tunneling und Micro-VPN. In diesem Modus kann eine Ausschlussliste mit IP-Adressen verwendet werden, die nicht an Citrix ADC getunnelt werden. Stattdessen wird die Internetverbindung des Geräts verwendet. Weitere Informationen über Reverse-Split-Tunneling finden Sie in der Citrix Gateway-Dokumentation.

XenMobile bietet eine **Ausschlussliste für Reverse-Split-Tunneling**. Wenn bestimmte Websites keinen Tunnel durch Citrix Gateway verwenden sollen, fügen Sie eine durch Kommas getrennte Liste mit vollqualifizierten Domänennamen (FQDN) oder DNS-Suffixen hinzu, die stattdessen eine Verbindung über das LAN herstellen. Diese Liste wird nur im Secure Browse-Modus verwendet, wenn Citrix Gateway für Reverse-Split-Tunneling konfiguriert ist.

Authentifizierung

January 5, 2022

Bei einer XenMobile-Bereitstellung sind bei der Konfiguration der Authentifizierung verschiedene Faktoren zu berücksichtigen. Diese werden in diesem Abschnitt eingehend erläutert und es wird insbesondere auf Folgendes eingegangen:

- Die wichtigsten MDX-Richtlinien, XenMobile-Clienteigenschaften und Citrix Gateway-Einstellungen, die mit der Authentifizierung verbunden sind.
- Die Interaktion dieser Richtlinien, Clienteigenschaften und Einstellungen miteinander.
- Die Vor- und Nachteile jeder Auswahl.

Der Artikel enthält auch drei empfohlene Konfigurationsbeispiele, mit denen die Sicherheit erhöht werden kann.

Im Allgemeinen geht eine verstärkte Sicherheit zu Lasten der Benutzererfahrung, da Benutzer sich häufiger authentifizieren müssen. Wie Sie hier einen Ausgleich schaffen, hängt ab von den Anforderungen und Prioritäten Ihrer Organisation. Die drei empfohlenen Konfigurationen verdeutlichen das Zusammenspiel der verfügbaren Authentifizierungsmaßnahmen und zeigen, wie Sie Ihre eigene XenMobile-Umgebung am besten bereitstellen.

Authentifizierungsmodi

Onlineauthentifizierung: ermöglicht Benutzern den Zugriff auf das XenMobile-Netzwerk. Eine Internetverbindung ist hierfür erforderlich.

Offlineauthentifizierung: wird auf dem Gerät ausgeführt. Benutzer entsperren den Tresor und erhalten Offlinezugriff auf heruntergeladene E-Mails, zwischengespeicherte Websites, Notizen und andere Elemente.

Methoden der Authentifizierung

Einstufig

LDAP: Sie können in XenMobile eine Verbindung mit einem oder mehreren LDAP-kompatiblen Verzeichnissen, z. B. Active Directory, herstellen. Dies ist eine häufig verwendete Methode, um in Unternehmensumgebungen einen Single Sign-On (SSO) mit einmaliger Anmeldung bereitzustellen. Bei Authentifizierung mit Citrix-PIN mit Active Directory-Kennwortzwischenspeicherung können Sie den Benutzerkomfort mit LDAP verbessern und gleichzeitig die Sicherheit durch Registrierung mit komplexem Kennwort, Kennwortablauf und Kontosperrung gewährleisten.

Weitere Informationen finden Sie unter Domäne oder Domäne plus STA.

Clientzertifikat: XenMobile ermöglicht die Integration mit branchenüblichen Zertifizierungsstellen zur Verwendung von Zertifikaten als einzige Methode für eine Online-Authentifizierung. XenMobile bietet dieses Zertifikat nach der Benutzerregistrierung, wofür entweder ein Einmalkennwort, eine Einladungs-URL oder die LDAP-Anmeldeinformationen erforderlich sind. Bei Verwendung

eines Clientzertifikats als primäre Authentifizierungsmethode ist in Umgebungen, die nur ein Clientzertifikat verwenden, eine Citrix-PIN erforderlich, um die Sicherheit des Gerätezertifikats zu gewährleisten.

XenMobile unterstützt Zertifikatsperrlisten (CRL) nur für Drittanbieterzertifizierungsstellen. Wenn Sie eine Microsoft-Zertifizierungsstelle konfiguriert haben, wird in XenMobile zum Verwalten der Zertifikatsperre Citrix ADC verwendet. Bedenken Sie beim Konfigurieren der Clientzertifikatauthentifizierung, ob Sie die Citrix ADC-Einstellung für Zertifikatsperrlisten (CRL) 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.

Bereitstellungsdiagramme für eine zertifikatbasierte Authentifizierung für Benutzer oder die Ausstellung von Gerätezertifikaten über die Zertifizierungsstelle (ZS) Ihres Unternehmens finden Sie unter Referenzarchitektur für on-premises Bereitstellungen.

Zweistufig

LDAP + Clientzertifikat: 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 Citrix ADC. Die Verwendung von LDAP und Clientzertifikat bietet Sicherheit durch etwas, das Benutzer wissen (ihr Active Directory-Kennwort) und etwas, das sie haben (Clientzertifikate auf ihrem Gerät). Secure Mail (und einige andere mobilen Produktivitätsapps) bieten eine intuitive Benutzererfahrung mit automatischer Konfiguration und Clientzertifikatauthentifizierung, bereitgestellt in einer ordnungsgemäß konfigurierten Exchange-Clientzugriffsserverumgebung. Die optimale Benutzerfreundlichkeit erreichen Sie, wenn Sie diese Option mit der Citrix-PIN und der Active Directory-Kennwortzwischenspeicherung kombinieren.

LDAP + Token: Diese Konfiguration ermöglicht die Standardkonfiguration mit LDAP-Anmeldeinformationen und einem Einmalkennwort unter Verwendung des RADIUS-Protokolls. Die optimale Benutzerfreundlichkeit erreichen Sie, wenn Sie diese Option mit der Citrix-PIN und der Active Directory-Kennwortzwischenspeicherung kombinieren.

Wichtige Richtlinien, Einstellungen und Clienteigenschaften für die Authentifizierung

Die folgenden Richtlinien, Einstellungen und Clienteigenschaften sind für die folgenden drei empfohlenen Konfigurationen von Bedeutung:

MDX-Richtlinien

App-Passcode: Bei der Einstellung **Ein** ist nach einem bestimmten Zeitraum der Inaktivität zum Starten bzw. Fortsetzen der App eine Citrix-PIN oder ein Passcode erforderlich. Die Standardeinstellung ist **Ein**.

Sie konfigurieren den Inaktivitätstimer für alle Apps, indem Sie in der XenMobile-Konsole auf der Registerkarte **Einstellungen** unter **Clienteigenschaften** den Wert INACTIVITY_TIMER in Minuten festlegen. Der Standardwert ist 15 Minuten. Setzen Sie den Wert auf Null, um den Inaktivitätstimer zu deaktivieren, damit eine Eingabeaufforderung für PIN oder Passcode nur beim Start der App angezeigt wird.

> **Hinweis:**
>
> Wenn Sie für die Richtlinie "Verschlüsselungsschlüssel" den Wert "Sicherer Offlinezugriff" auswählen, wird diese Richtlinie automatisch aktiviert.

Onlinesitzung erforderlich: Bei der Einstellung **Ein** muss der Benutzer mit dem Unternehmensnetzwerk verbunden sein und eine aktive Sitzung haben, um auf die App auf dem Gerät zugreifen zu können. Bei Auswahl der Einstellung **Aus** ist für einen Zugriff auf die App auf dem Gerät keine aktive Sitzung erforderlich. Die Standardeinstellung ist **Aus**.

Maximale Offlinezeit (Stunden): legt die maximale Zeit fest, die eine App ausgeführt werden kann, ohne dass der App-Anspruch und die Aktualisierungsrichtlinien von XenMobile neu bestätigt werden müssen. Wenn Sie die maximale Offlinezeit festlegen, ruft die App neue Richtlinien für MDX-Apps von XenMobile ab, ohne dass dies Benutzern Unterbrechungen verursacht, wenn Secure Hub für iOS einen gültigen Citrix Gateway-Token hat. Wenn Secure Hub keinen gültigen Citrix ADC-Token hat, müssen Benutzer sich über Secure Hub authentifizieren, damit App-Richtlinien aktualisiert werden. Der Citrix ADC-Token kann durch Citrix Gateway-Sitzungsinaktivität oder eine erzwungene Sitzungstimeoutrichtlinie ungültig werden. Benutzer können die App jedoch weiter verwenden, wenn sie sich wieder bei Secure Hub anmelden.

Benutzer werden 30, 15 und 5 Minuten vor Ablauf dieser Zeit daran erinnert, sich anzumelden. Nach Ablauf der Zeit wird die App gesperrt, bis sich Benutzer anmelden. Der Standardwert ist **72 Stunden (3 Tage)**. Der Mindestzeitraum ist 1 Stunde.

> **Hinweis:**
>
> Beachten Sie, dass in einem Szenario, bei dem Benutzer häufig unterwegs sind und auch internationales Roaming verwenden, die Standardeinstellung von 72 Stunden (3 Tagen) zu kurz sein kann.

Ticketablauf für Hintergrunddienste: die Zeitspanne, die ein Netzwerkdienstticket im Hintergrund gültig bleibt. Wenn Secure Mail über Citrix Gateway die Verbindung mit einem Exchange-Server herstellt, auf dem ActiveSync ausgeführt wird, gibt XenMobile ein Token aus, das Secure Mail für die Verbindung mit dem internen Exchange-Server verwendet. Diese Eigenschaft bestimmt, wie lange

Secure Mail den Token verwenden kann, ohne einen neuen Token für die Authentifizierung und die Verbindung zum Exchange Server zu benötigen. Wenn das Zeitlimit abläuft, müssen Benutzer sich neu anmelden, damit ein neues Token generiert wird. Die Standardeinstellung ist **168 Stunden (7 Tage)**. Nach Ablauf des Zeitlimits werden keine weiteren E-Mail-Benachrichtigungen gesendet.

Kulanzzeitraum bis Onlinesitzung erforderlich: legt fest, wie viele Minuten ein Benutzer die App offline verwenden kann, bevor die Richtlinie "Onlinesitzung erforderlich" die weitere Verwendung verhindert (bis die Onlinesitzung validiert ist). Der Standardwert ist 0 (kein Kulanzzeitraum).

Informationen zur Authentifizierungsrichtlinien finden Sie hier:

- Bei Verwendung des MAM-SDK: Überblick über das MAM-SDK
- Wenn Sie das MDX Toolkit verwenden: MDX-Richtlinien für iOS und MDX-Richtlinien für Android.

XenMobile-Clienteigenschaften

> **Hinweis:**
>
> Clienteigenschaften sind eine globale Einstellung und gelten für alle Geräte, die mit XenMobile verbunden sind.

Citrix-PIN: Durch Aktivieren der Citrix-PIN ermöglichen Sie Benutzern eine einfache Anmeldung. Mit der PIN müssen Benutzer andere Anmeldeinformationen, z. B. ihren Active Directory-Benutzernamen und ihr Kennwort, nicht wiederholt eingeben. Konfigurieren Sie die Citrix-PIN als eigenständige Option zur Authentifizierung im Offlinemodus, oder kombinieren Sie die PIN mit der Active Directory-Kennwortzwischenspeicherung, um den Authentifizierungsprozess zu vereinfachen. Sie konfigurieren die Citrix PIN in der XenMobile-Konsole unter **Einstellungen > Client > Clienteigenschaften**.

Es folgt eine Zusammenfassung der wichtigsten Eigenschaften. Weitere Informationen finden Sie unter Clienteigenschaften.

ENABLE_PASSCODE_AUTH

Anzeigename: Enable Citrix PIN Authentication

Über diesen Schlüssel 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. Aktivieren Sie diese Einstellung, wenn **ENABLE_PASSWORD_CACHING** aktiviert ist oder wenn XenMobile die Zertifikatauthentifizierung verwendet.

Mögliche Werte: true oder **false**

Standardwert: false

ENABLE_PASSWORD_CACHING

Anzeigename: Enable User Password Caching

Über diesen Schlüssel können Sie die lokale Zwischenspeicherung des Active Directory-Kennworts auf dem Mobilgerät zulassen. Wenn Sie diesen Schlüssel auf “true” setzen, werden die Benutzer aufgefordert, eine Citrix-PIN oder einen Citrix Passcode festzulegen. Der Schlüssel ENABLE_PASSCODE_AUTH muss auf “true” festgelegt werden, wenn Sie diesen Schlüssel auf **true** festlegen.

Mögliche Werte: true oder **false**

Standardwert: false

PASSCODE_STRENGTH

Anzeigename: PIN Strength Requirement

Dieser Schlüssel 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** oder **Strong**

Standardwert: Medium

INACTIVITY_TIMER

Anzeigename: Inactivity Timer

Dieser Schlüssel definiert die Zeitdauer (in Minuten), die Geräte inaktiv sein dürfen, bevor Benutzer zur Eingabe von Citrix-PIN bzw. Citrix Passcode aufgefordert werden, wenn sie auf eine App zugreifen möchten. Zum Aktivieren dieser Einstellung für eine MDX-App müssen Sie die Einstellung “App-Passcode” auf **Ein** festlegen. Wenn “App Passcode” auf **Aus** festgelegt ist, werden die Benutzer für eine vollständige Authentifizierung an 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. Der Standardwert ist 15 Minuten.

ENABLE_TOUCH_ID_AUTH

Anzeigename: Enable Touch ID Authentication

Ermöglicht die Verwendung des Fingerabdrucklesegeräts (nur iOS) zur Offlineauthentifizierung. Die Onlineauthentifizierung erfordert weiterhin die primäre Authentifizierungsmethode.

ENCRYPT_SECRETS_USING_PASSCODE

Anzeigename: Encrypt secrets using Passcode

Mit diesem Schlüssel können vertrauliche Daten auf Mobilgeräten in einem Geheimtresor statt in einem plattformbasierten systemeigenen Speicher (z. B. iOS-Schlüsselbund) gespeichert werden. Der Konfigurationsschlüssel ermöglicht eine starke Verschlüsselung von Schlüsselartefakten und erzeugt zudem Benutzerentropie (eine vom Benutzer generierte zufällige PIN, die nur dem Benutzer bekannt ist).

Mögliche Werte: true oder **false**

Standardwert: false

Citrix ADC-Einstellungen

Session time-out: Wenn Sie diese Einstellung aktivieren, wird die Sitzung von Citrix Gateway getrennt, wenn Citrix ADC im angegebenen Zeitraum keine Netzwerkaktivität erkennt. Die Einstellung wird für Benutzer durchgesetzt, die eine Verbindung mit dem Citrix Gateway Plug-in, Citrix Receiver, Secure Hub oder über einen Webbrowser herstellen. Der Standardwert ist **1440 Minuten**. Wenn Sie diesen Wert auf Null setzen, wird die Einstellung deaktiviert.

Forced time-out: Mit dieser Einstellung trennt Citrix Gateway die Sitzung nach Ablauf der Timeoutfrist, unabhängig von den aktuellen Aktivitäten des Benutzers. Benutzer haben keine Möglichkeit, diese Trennung nach Ablauf der Timeoutfrist zu vermeiden. Die Einstellung wird für Benutzer durchgesetzt, die eine Verbindung mit dem Citrix Gateway Plug-in, Citrix Receiver, Secure Hub oder über einen Webbrowser herstellen. Bei Verwendung von STA, einem speziellen Citrix ADC-Modus in Secure Mail, wird die Einstellung "Forced Time-out" nicht auf Secure Mail-Sitzungen angewendet. Der Standardwert ist **1440 Minuten**. Wenn Sie diesen Wert leer lassen, wird die Einstellung deaktiviert.

Weitere Informationen zu den Timeouteinstellungen in Citrix Gateway finden Sie in der Citrix ADC-Dokumentation.

Weitere Informationen zu den Szenarios, bei denen Benutzer zur Authentifizierung bei XenMobile durch Eingabe der Anmeldeinformationen auf ihrem Gerät aufgefordert werden, finden Sie unter Szenarios für Authentifizierungsaufforderungen.

Standardkonfigurationseinstellungen

Bei diesen Einstellungen handelt es sich um die Standardwerte, die bereitgestellt werden von:

- NetScaler für XenMobile-Assistent
- MAM-SDK oder MDX Toolkit
- XenMobile-Konsole

Einstellung	Ort der Einstellung	Standardeinstellung
Session time-out	Citrix Gateway	1440 Minuten
Force time-out	Citrix Gateway	1440 Minuten
Maximale Offlinezeit	MDX-Richtlinien	72 Stunden
Ticketablauf für Hintergrunddienste	MDX-Richtlinien	168 Stunden (7 Tage)

Einstellung	Ort der Einstellung	Standardeinstellung
Onlinesitzung erforderlich	MDX-Richtlinien	Aus
Kulanzzeitraum bis Onlinesitzung erforderlich	MDX-Richtlinien	0
App-Passcode	MDX-Richtlinien	Ein
Encrypt secrets using passcode	XenMobile-Clienteigenschaften	false
Enable Citrix-PIN Authentication	XenMobile-Clienteigenschaften	false
PIN Strength Requirement	XenMobile-Clienteigenschaften	Mittel
PIN Type	XenMobile-Clienteigenschaften	Numerisch
Enable User Password Caching	XenMobile-Clienteigenschaften	false
Inactivity Timer	XenMobile-Clienteigenschaften	15
Enable Touch ID Authentication	XenMobile-Clienteigenschaften	false

Empfohlene Konfigurationen

Der folgende Abschnitt enthält Beispiele für drei XenMobile-Konfigurationen. Die Beispiele reichen von niedrigster Sicherheit und optimaler Benutzererfahrung bis hin zu höchster Sicherheit bei eingeschränktem Benutzerkomfort. Die Beispiele sind als Referenzpunkte gedacht, anhand derer Sie bestimmen können, wo Sie die eigene Konfiguration auf der Skala platzieren möchten. Beachten Sie, dass möglicherweise auch andere Einstellungen angepasst werden müssen, wenn Sie diese Einstellungen ändern. Beispielsweise sollte die maximale Offlinezeit stets niedriger sein als das Sitzungstimeout.

Höchste Sicherheit

Diese Konfiguration bietet die höchste Sicherheit, jedoch verbunden mit beträchtlichen Einschränkungen bei der Benutzerfreundlichkeit.

Einstellung	Ort der Einstellung	Empfohlene Einstellung	Auswirkungen
Session time-out	Citrix Gateway	1440	Benutzer geben ihre Anmeldeinformationen in Secure Hub nur bei erforderlicher Onlineauthentifizierung ein – alle 24 Stunden.
Force time-out	Citrix Gateway	1440	Obligatorische Onlineauthentifizierung alle 24 Stunden. Aktivität verlängert nicht die Sitzungsdauer.
Maximale Offlinezeit	MDX-Richtlinien	23	Richtlinienaktualisierung jeden Tag erforderlich.
Ticketablauf für Hintergrunddienste	MDX-Richtlinien	72 Stunden	Das STA-Timeout ermöglicht längere Sitzungen ohne Sitzungstoken von Citrix Gateway. In Secure Mail verhindert ein STA-Timeout, das länger ist als das Sitzungstimeout, dass E-Mail-Benachrichtigungen ohne Aufforderung beendet werden, wenn Benutzer die App nicht vor Ablauf der Sitzung öffnen.

Onlinesitzung erforderlich	MDX-Richtlinien	Aus	Gewährleistet eine gültige Netzwerkverbindung und Citrix Gateway-Sitzung zur Verwendung von Apps.
Kulanzzeitraum bis Onlinesitzung erforderlich	MDX-Richtlinien	0	Kein Kulanzzeitraum (bei aktivierter Option “Onlinesitzung erforderlich”).
App-Passcode	MDX-Richtlinien	Ein	Passcode für Anwendung erforderlich.
Encrypt secrets using passcode	XenMobile-Clienteigenschaften	true	Tresor wird durch einen von der Benutzerentropie abgeleiteten Schlüssel geschützt.
Enable Citrix-PIN Authentication	XenMobile-Clienteigenschaften	true	Citrix-PIN zur vereinfachten Benutzerauthen-tifizierung aktivieren.
PIN Strength Requirement	XenMobile-Clienteigenschaften	Gut	Hohe Anforderungen an die Kennwortkom-plexität.
PIN Type	XenMobile-Clienteigenschaften	Alphanumerisch	PIN ist eine alphanumerische Sequenz.

Enable Password Caching	XenMobile-Clienteigenschaften	false	Das Active Directory-Kennwort wird nicht zwischengespeichert, und die Citrix-PIN wird für Offlineauthentifizierungen verwendet.
Inactivity Timer	XenMobile-Clienteigenschaften	15	Aufforderung zur Offlineauthentifizierung anzeigen, wenn Benutzer keine MDX-Apps oder Secure Hub im festgelegten Zeitraum verwendet.
Enable Touch ID Authentication	XenMobile-Clienteigenschaften	false	Deaktiviert die Offlineauthentifizierung per Touch ID in iOS.

Höhere Sicherheit

Diese Konfiguration liegt im Mittelfeld und umfasst eine häufigere Authentifizierung von Benutzern (alle 3 Tage anstatt alle 7) und strengere Sicherheitsmaßnahmen. Die erhöhte Anzahl an Authentifizierungen führt häufiger zur Containersperre, was die Datensicherheit gewährleistet, wenn Geräte nicht verwendet werden.

Einstellung	Ort der Einstellung	Empfohlene Einstellung	Auswirkungen
Session time-out	Citrix Gateway	4320	Benutzer geben ihre Anmeldeinformationen in Secure Hub nur bei erforderlicher Onlineauthentifizierung ein – alle 3 Tage.

Force time-out	Citrix Gateway	Kein Wert	Sitzungen werden bei Aktivität verlängert.
Maximale Offlinezeit	MDX-Richtlinien	71	Erfordert alle 3 Tage eine Richtlinienaktualisierung. Die Differenz von einer Stunde ermöglicht die Aktualisierung vor dem Sitzungstimeout.
Ticketablauf für Hintergrunddienste	MDX-Richtlinien	168 Stunden	Das STA-Timeout ermöglicht längere Sitzungen ohne Sitzungstoken von Citrix Gateway. In Secure Mail verhindert ein STA-Timeout, das länger ist als das Sitzungstimeout, dass E-Mail-Benachrichtigungen ohne Aufforderung beendet werden, wenn Benutzer die App nicht vor Ablauf der Sitzung öffnen.
Onlinesitzung erforderlich	MDX-Richtlinien	Aus	Gewährleistet eine gültige Netzwerkverbindung und Citrix Gateway-Sitzung zur Verwendung von Apps.

Kulanzzeitraum bis Onlinesitzung erforderlich	MDX-Richtlinien	0	Kein Kulanzzeitraum (bei aktivierter Option “Onlinesitzung erforderlich”).
App-Passcode	MDX-Richtlinien	Ein	Passcode für Anwendung erforderlich.
Encrypt secrets using passcode	XenMobile-Clienteigenschaften	false	Keine Benutzerentropie zum Verschlüsseln des Tresors erforderlich.
Enable Citrix-PIN Authentication	XenMobile-Clienteigenschaften	true	Citrix-PIN zur vereinfachten Benutzerauthen-tifizierung aktivieren.
PIN Strength Requirement	XenMobile-Clienteigenschaften	Mittel	Erzwingt Kennwörter mittlerer Komplexität.
PIN Type	XenMobile-Clienteigenschaften	Numerisch	PIN ist eine numerische Sequenz.
Enable Password Caching	XenMobile-Clienteigenschaften	true	Die Benutzer-PIN speichert und schützt das Active Directory-Kennwort.
Inactivity Timer	XenMobile-Clienteigenschaften	30	Aufforderung zur Of-flineauthentifizierung anzeigen, wenn Benutzer keine MDX-Apps oder Secure Hub im festgelegten Zeitraum verwendet.

Enable Touch ID Authentication	XenMobile-Clienteigenschaften	true	Aktiviert Touch ID für Anwendungsfälle mit Offlineauthentifizierung in iOS.

Hohe Sicherheit

Diese Konfiguration ist am benutzerfreundlichsten und bietet ein Mindestmaß an Sicherheit.

Einstellung	Ort der Einstellung	Empfohlene Einstellung	Auswirkungen
Session time-out	Citrix Gateway	10080	Benutzer geben ihre Anmeldeinformationen in Secure Hub nur bei erforderlicher Onlineauthentifizierung ein – alle 7 Tage.
Force time-out	Citrix Gateway	Kein Wert	Sitzungen werden bei Aktivität verlängert.
Maximale Offlinezeit	MDX-Richtlinien	167	Erfordert eine wöchentliche Richtlinienaktualisierung (alle 7 Tage). Die Differenz von einer Stunde ermöglicht die Aktualisierung vor dem Sitzungstimeout.

Ticketablauf für Hintergrunddienste	MDX-Richtlinien	240	Das STA-Timeout ermöglicht längere Sitzungen ohne Sitzungstoken von Citrix Gateway. In Secure Mail verhindert ein STA-Timeout, das länger ist als das Sitzungstimeout, dass E-Mail-Benachrichtigungen ohne Aufforderung beendet werden, wenn Benutzer die App nicht vor Ablauf der Sitzung öffnen.
Onlinesitzung erforderlich	MDX-Richtlinien	Aus	Gewährleistet eine gültige Netzwerkverbindung und Citrix Gateway-Sitzung zur Verwendung von Apps.
Kulanzzeitraum bis Onlinesitzung erforderlich	MDX-Richtlinien	0	Kein Kulanzzeitraum (bei aktivierter Option “Onlinesitzung erforderlich”).
App-Passcode	MDX-Richtlinien	Ein	Passcode für Anwendung erforderlich.
Encrypt secrets using passcode	XenMobile-Clienteigenschaften	false	Keine Benutzerentropie zum Verschlüsseln des Tresors erforderlich.

Enable Citrix-PIN Authentication	XenMobile-Clienteigenschaften	true	Citrix-PIN zur vereinfachten Benutzerauthentifizierung aktivieren.
PIN Strength Requirement	XenMobile-Clienteigenschaften	Niedrig	Keine Anforderungen an die Kennwortkomplexität.
PIN Type	XenMobile-Clienteigenschaften	Numerisch	PIN ist eine numerische Sequenz.
Enable Password Caching	XenMobile-Clienteigenschaften	true	Die Benutzer-PIN speichert und schützt das Active Directory-Kennwort.
Inactivity Timer	XenMobile-Clienteigenschaften	90	Aufforderung zur Offlineauthentifizierung anzeigen, wenn Benutzer keine MDX-Apps oder Secure Hub im festgelegten Zeitraum verwendet.
Enable Touch ID Authentication	XenMobile-Clienteigenschaften	true	Aktiviert Touch ID für Anwendungsfälle mit Offlineauthentifizierung in iOS.

Verwenden der verstärkten Authentifizierung

Einige Apps erfordern unter Umständen eine erweiterte Authentifizierung (z. B. sekundäre Authentifizierungsfaktoren wie einen Token oder aggressive Sitzungstimeouts). Sie können diese Authentifizierungsmethode über eine MDX-Richtlinie steuern. Dieses Verfahren erfordert einen eigenen virtuellen Server (auf demselben oder einem separaten Citrix ADC-Gerät) zur Steuerung der Authentifizierungsmethoden.

Einstellung	Ort der Einstellung	Empfohlene Einstellung	Auswirkungen
Alternatives Citrix Gateway	MDX-Richtlinien	Erfordert FQDN und Port des sekundären Citrix ADC-Geräts.	Ermöglicht eine erweiterte Authentifizierung, die durch die Authentifizierungs- und Sitzungsrichtlinien des sekundären Citrix ADC-Geräts gesteuert wird.

Öffnet ein Benutzer eine App, die sich an der alternativen Citrix Gateway-Instanz anmeldet, verwenden alle übrigen Apps diese Citrix Gateway-Instanz zur Kommunikation mit dem internen Netzwerk. Die Sitzung wechselt nur dann zurück zur Citrix Gateway-Instanz mit geringerer Sicherheit, wenn bei der Citrix Gateway-Instanz mit erhöhter Sicherheit ein Sitzungstimeout auftritt.

Erforderliche Verwendung einer Onlinesitzung

Für bestimmte Anwendungen wie Secure Web möchten Sie eventuell sicherstellen, dass Benutzer eine App nur dann ausführen, wenn sie eine authentifizierte Sitzung verwenden und wenn das Gerät mit einem Netzwerk verbunden ist. Diese Richtlinie erzwingt diese Option und ermöglicht einen Kulanzzeitraum, damit Benutzer ihre Arbeit beenden können.

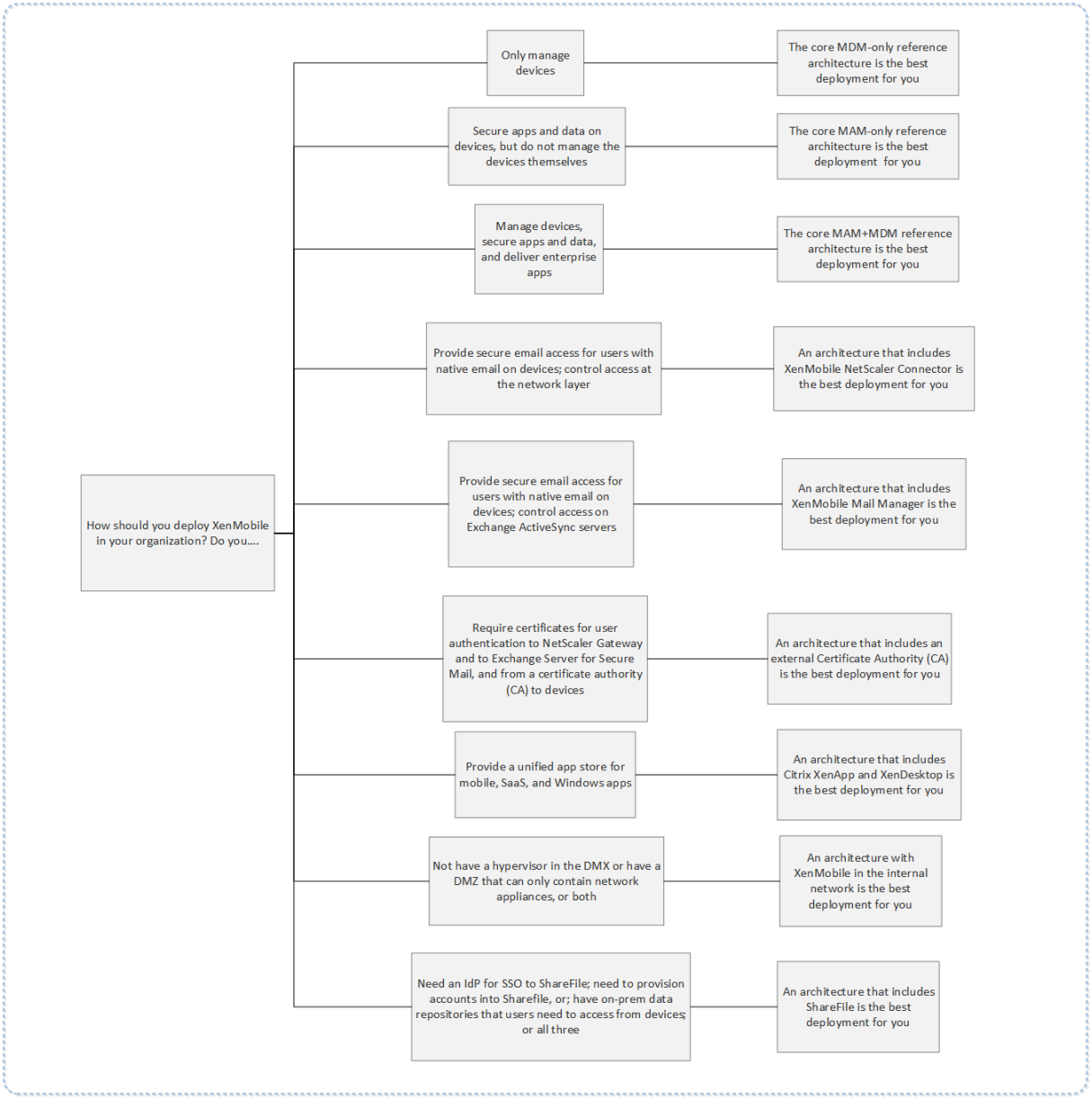
Einstellung	Ort der Einstellung	Empfohlene Einstellung	Auswirkungen
Onlinesitzung erforderlich	MDX-Richtlinien	Ein	Gewährleistet, dass das Gerät online ist und einen gültigen Authentifizierungstoken hat.
Kulanzzeitraum bis Onlinesitzung erforderlich	MDX-Richtlinien	15	Gewährt einen Kulanzzeitraum von 15 Minuten, bevor der Benutzer die Apps nicht mehr verwenden kann.

Referenzarchitektur für On-Premises-Bereitstellungen

January 5, 2022

Die Abbildungen in diesem Artikel zeigen die Referenzarchitekturen für eine On-Premises-Bereitstellung von XenMobile. Die Bereitstellungsszenarios umfassen Nur-MDM-, Nur-MAM- und MDM+MAM als Kernarchitektur sowie solche mit Komponenten wie SNMP-Manager Citrix Gateway Connector für Exchange ActiveSync, Endpoint Management Connector für Exchange ActiveSync und Citrix Virtual Apps and Desktops. Die Abbildungen zeigen die für XenMobile mindestens erforderlichen Komponenten.

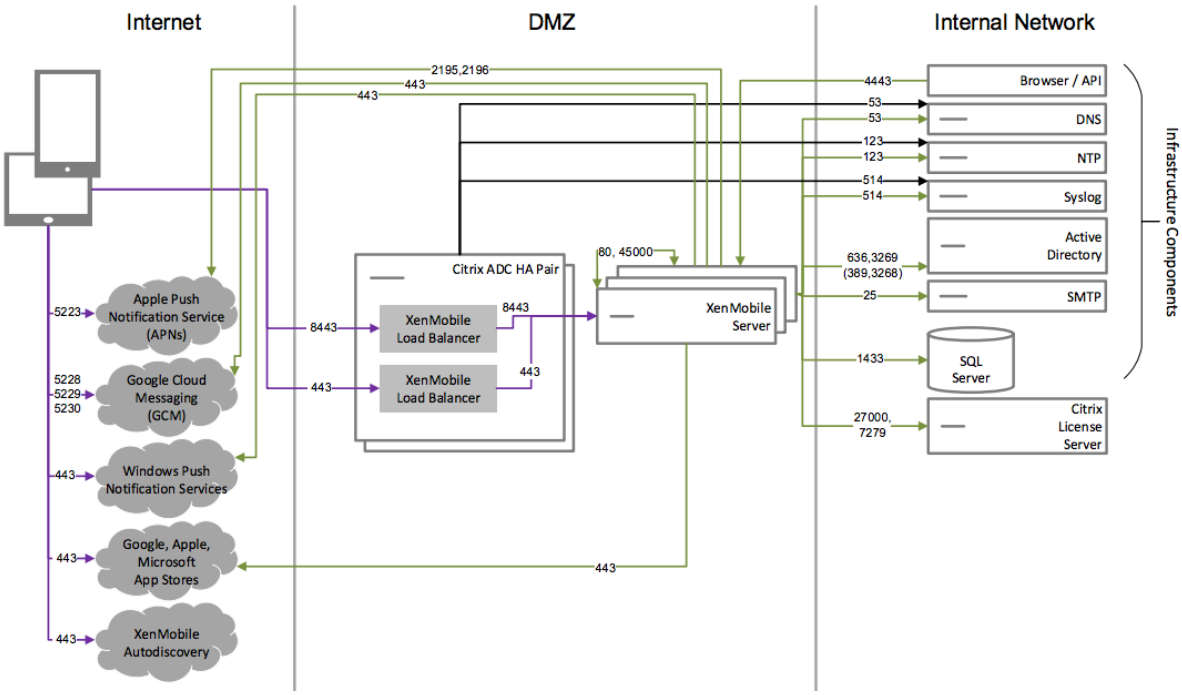
Verwenden Sie das Diagramm als allgemeine Richtlinie für Ihre Bereitstellungsplanung.



Die Nummern an den Verbindungen stehen für die Ports, die geöffnet werden müssen, damit die Verbindung zwischen den Komponenten möglich ist. Eine vollständige Liste der Ports finden Sie unter Portanforderungen in der Dokumentation zu XenMobile.

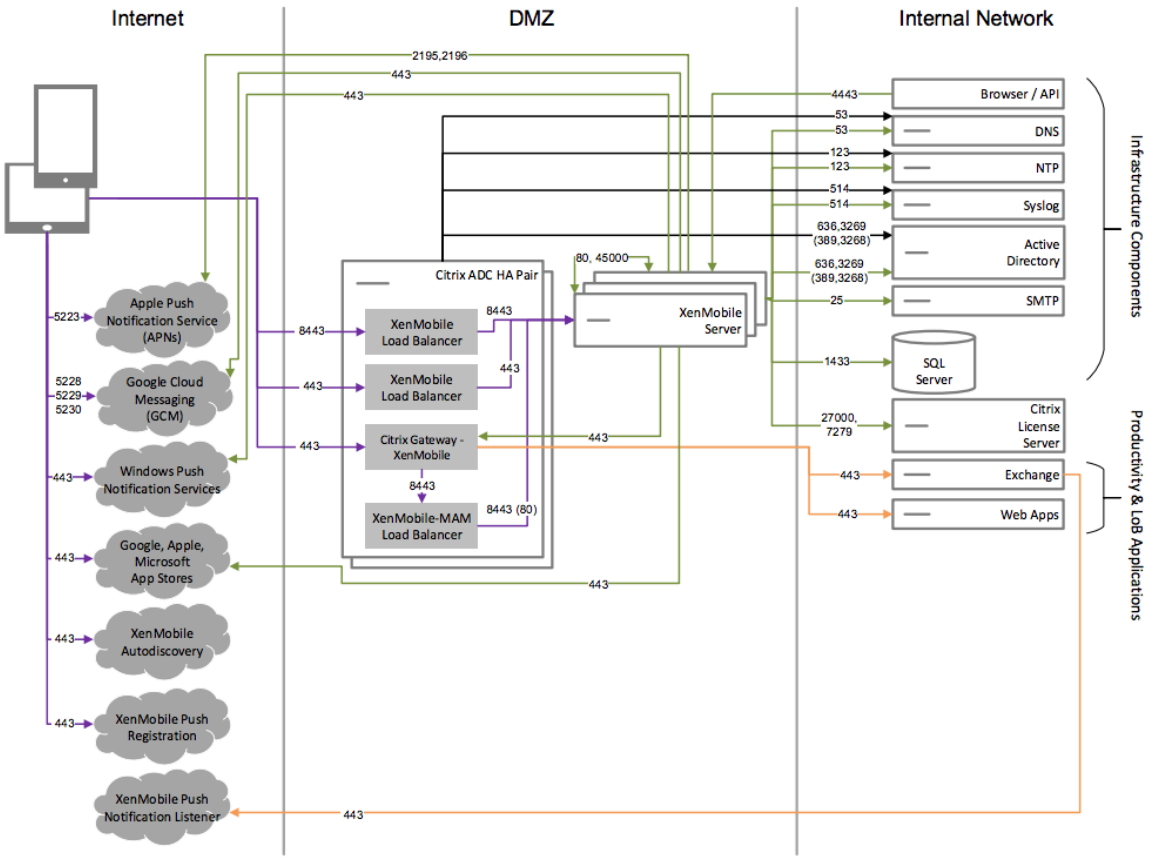
Referenzarchitektur für Nur-MDM-Bereitstellungen

Stellen Sie diese Architektur bereit, wenn Sie planen, nur die MDM-Features von XenMobile zu verwenden. Beispielsweise müssen Sie vom Unternehmen bereitgestellte Geräte per MDM verwalten, um Richtlinien und Apps bereitzustellen, Assetinventare abzurufen und Aktionen wie Löschvorgänge auf Geräten auszuführen.



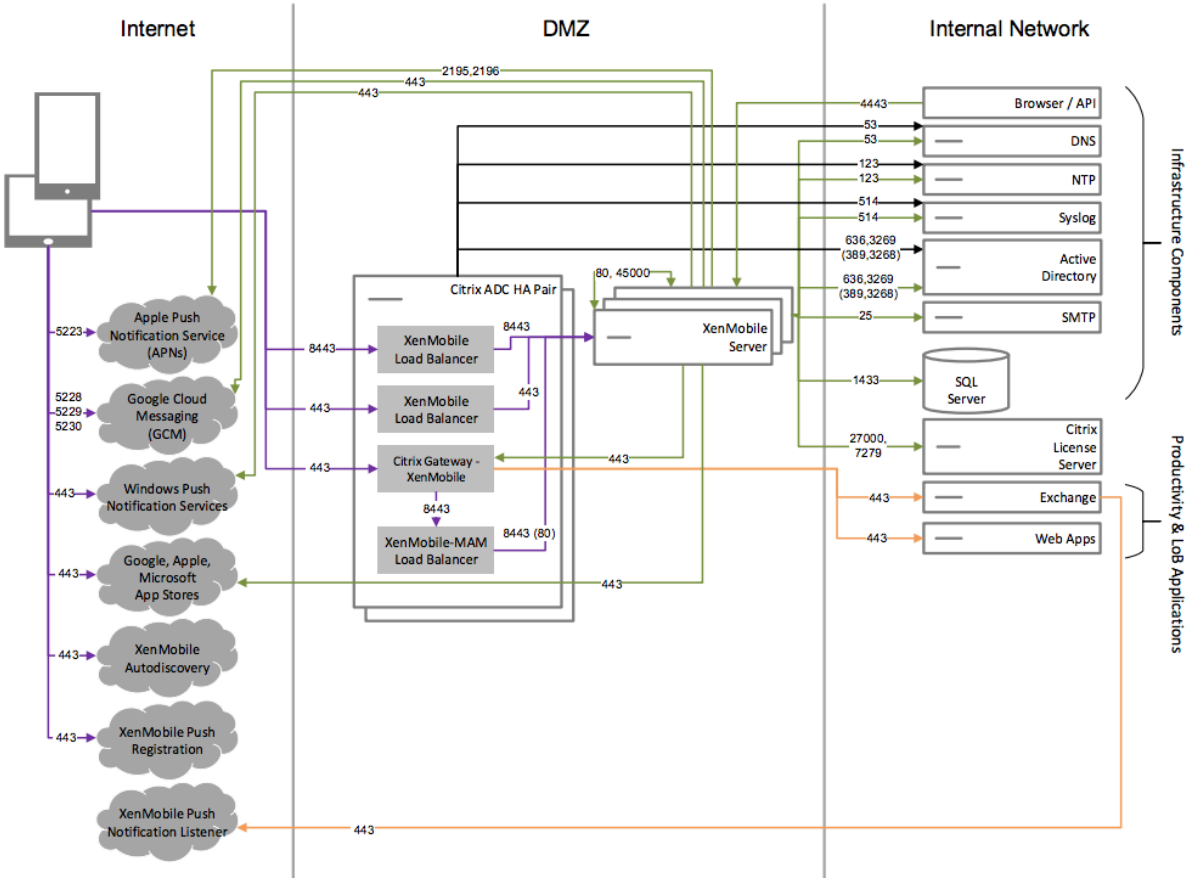
Referenzarchitektur für Nur-MAM-Bereitstellungen

Stellen Sie diese Architektur bereit, wenn Sie planen, nur die MAM-Features von XenMobile zu verwenden und Geräte den MDM-Modus nicht erfordern. 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 für die Mobilgeräteverwaltung (MDM) registriert sein.



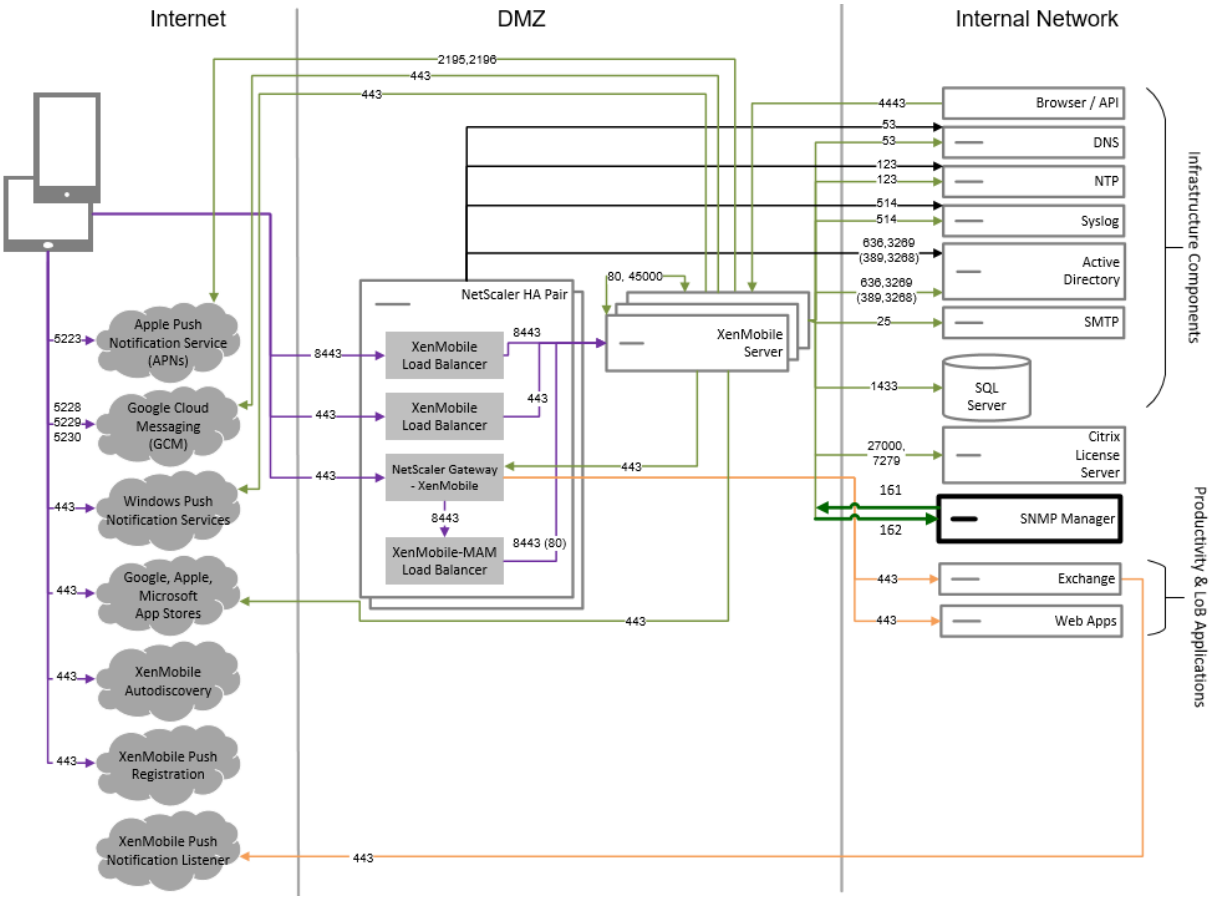
Referenzarchitektur für MAM+MDM-Bereitstellungen

Stellen Sie diese Architektur bereit, wenn Sie die MDM- und die MAM-Features von XenMobile verwenden. Beispielsweise können Sie vom Unternehmen bereitgestellte Geräte per MDM verwalten, Richtlinien und Apps bereitzustellen, Assetinventare abrufen und Daten von Geräten löschen. Zudem können Sie mobile Unternehmens-Apps bereitstellen, Apps sperren und die Daten auf Benutzergeräten löschen.



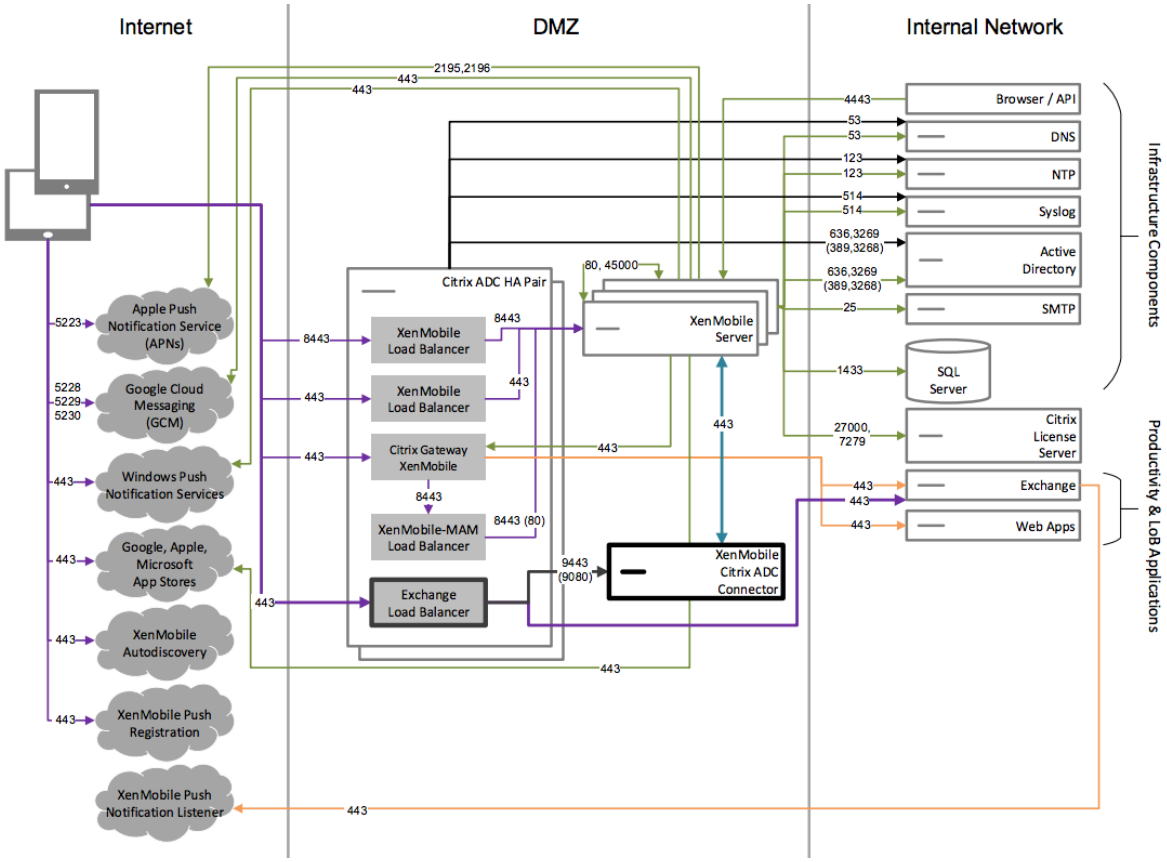
Referenzarchitektur mit SNMP

Stellen Sie diese Architektur bereit, wenn Sie die SNMP-Überwachung mit XenMobile aktivieren möchten. Damit können Überwachungssysteme beispielsweise Informationen zu Ihren XenMobile-Knoten abrufen. Weitere Informationen finden Sie unter SNMP-Überwachung.



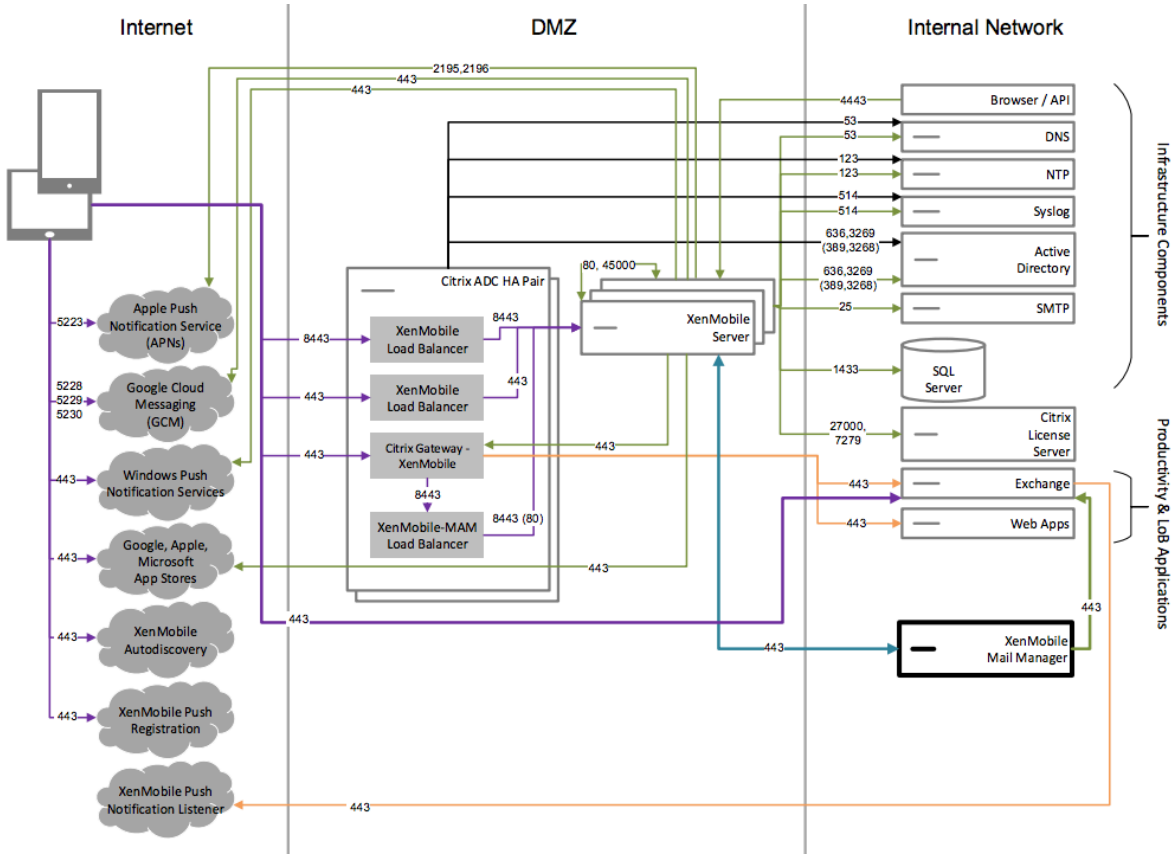
Referenzarchitektur mit Citrix Gateway Connector für Exchange ActiveSync

Stellen Sie diese Architektur bereit, wenn Sie den Citrix Gateway Connector für Exchange ActiveSync mit XenMobile verwenden möchten. Damit können Sie beispielsweise Benutzern, die native mobile E-Mail-Apps verwenden, einen sicheren Zugriff auf ihre E-Mail ermöglichen. Solche Benutzer können ihre native App weiterverwenden oder Sie können für eine allmähliche Umstellung auf Citrix Secure Mail sorgen. Die Zugriffssteuerung muss in der Netzwerkschicht erfolgen, bevor der Datenverkehr die Exchange Active Sync-Server erreicht. Das Diagramm zeigt den Connector für Exchange ActiveSync zwar in einer MDM+MAM-Architektur, Sie können ihn aber genauso auch in einer Nur-MDM-Architektur bereitstellen.



Referenzarchitektur mit Endpoint Management Connector für Exchange ActiveSync

Stellen Sie diese Architektur bereit, wenn Sie den Endpoint Management Connector für Exchange ActiveSync mit XenMobile verwenden möchten. Beispielsweise, wenn Sie Benutzern, die native mobile E-Mail-Apps verwenden, sicheren E-Mail-Zugriff gewähren möchten. Solche Benutzer können ihre native App weiterverwenden oder Sie können für eine allmähliche Umstellung auf Secure Mail sorgen. Die Zugriffssteuerung ist auf den Exchange ActiveSync-Servern möglich. Das Diagramm zeigt den Endpoint Management Connector für Exchange ActiveSync zwar in einer MDM+MAM-Architektur, Sie können ihn aber genauso auch in einer Nur-MDM-Architektur bereitstellen.

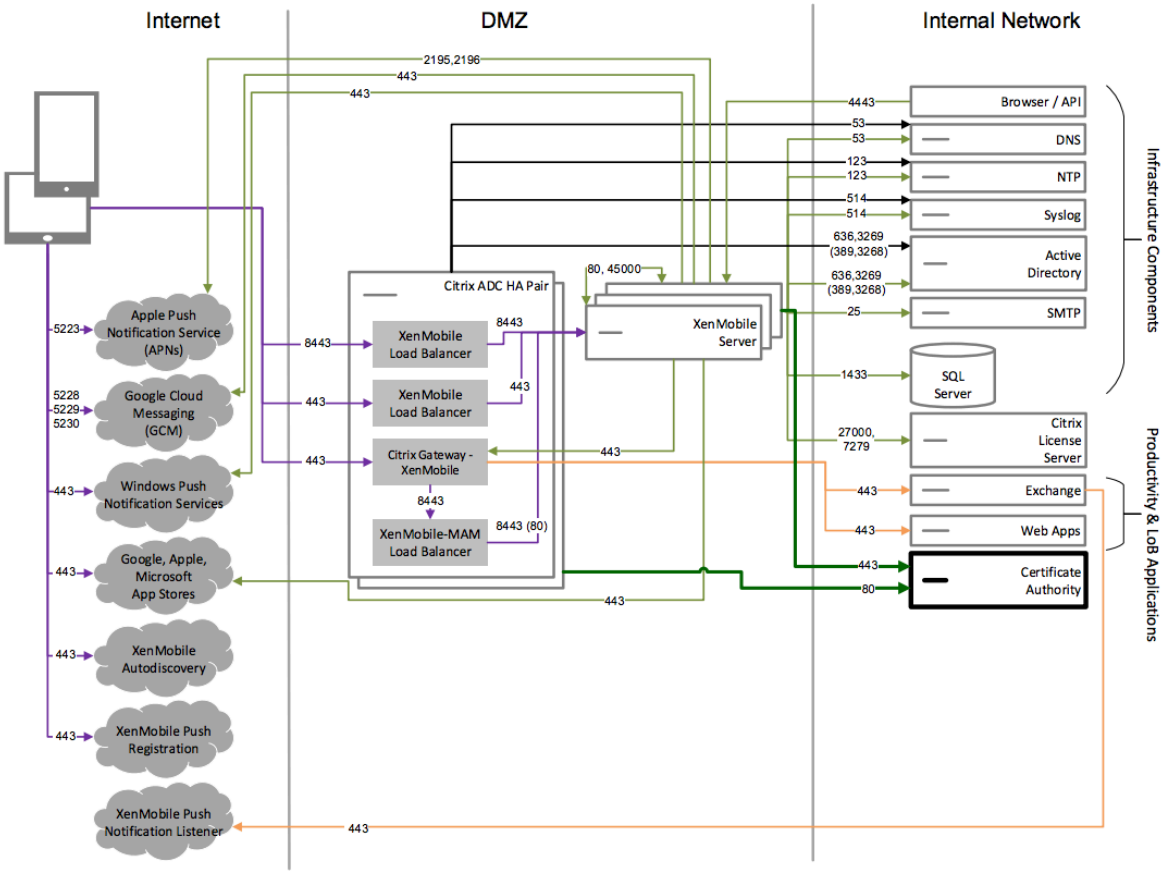


Referenzarchitektur mit externer Zertifizierungsstelle

Eine Bereitstellung mit externer Zertifizierungsstelle wird empfohlen, wenn mindestens eine der folgenden Anforderungen erfüllt werden muss:

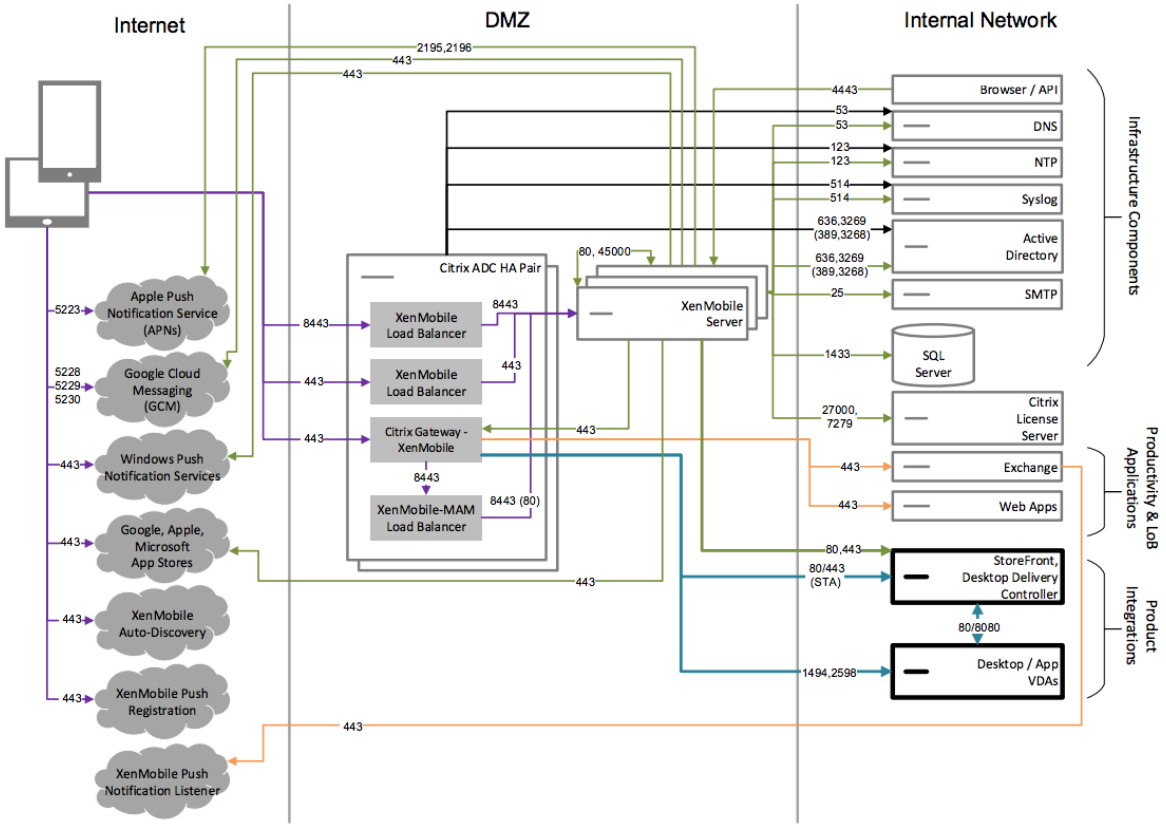
- Sie benötigen Benutzerzertifikate für die Benutzerauthentifizierung bei Citrix Gateway (für den Intranetzugang).
- Zur Authentifizierung von Secure Mail-Benutzern bei Exchange Server soll ein Benutzerzertifikat verwendet werden.
- Sie müssen Zertifikate, die von Ihrer Unternehmenszertifizierungsstelle ausgestellt wurden, an mobile Geräte für den Wi-Fi-Zugriff senden.

Das Diagramm zeigt die externe Zertifizierungsstelle zwar in einer MDM+MAM-Architektur, Sie können sie aber genauso auch in einer Nur-MDM- oder Nur-MAM-Architektur bereitstellen.



Referenzarchitektur mit Virtual Apps and Desktops

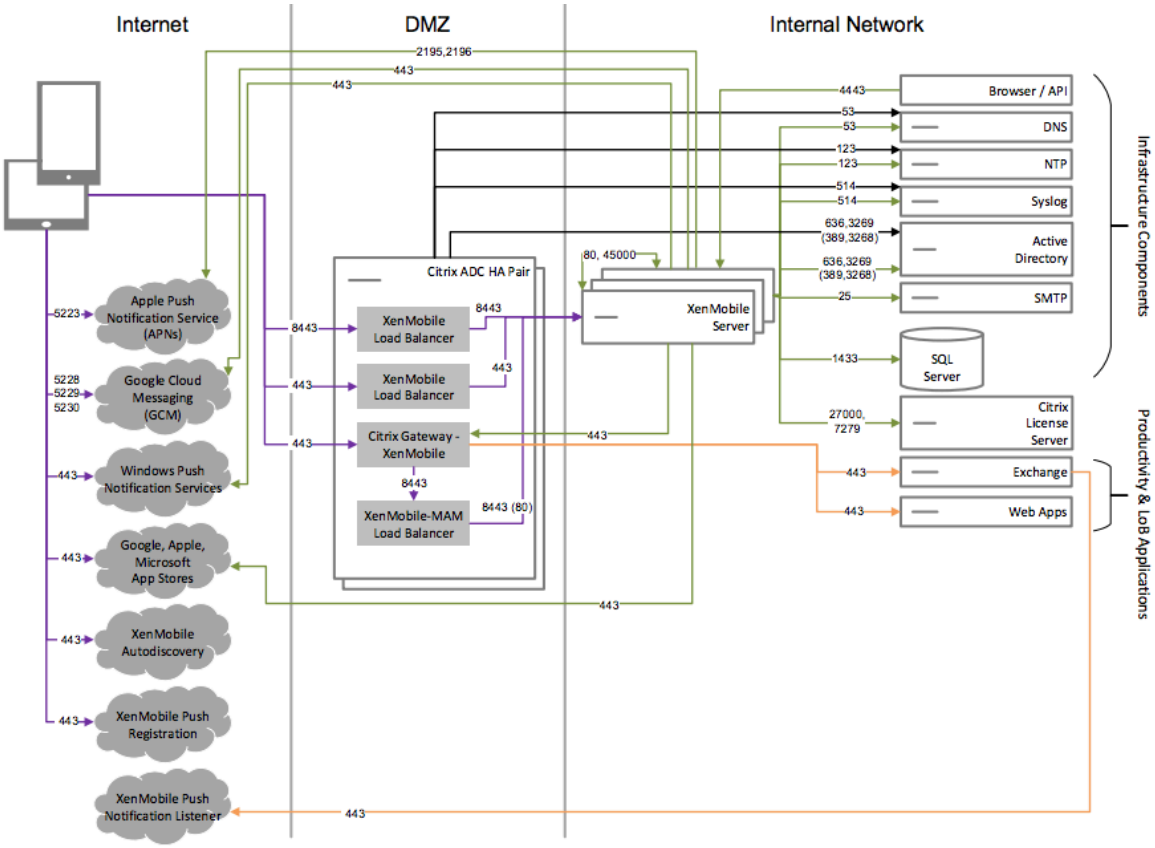
Stellen Sie diese Architektur bereit, wenn Sie Citrix Virtual Apps and Desktops in XenMobile integrieren möchten. Dies ist beispielsweise der Fall, wenn Sie mobilen Benutzern einen einheitlichen App-Store für Anwendungen aller Art (Mobile, SaaS, Windows) bereitstellen möchten. Das Diagramm zeigt zwar virtuelle Desktops, die in einer MDM+MAM-Architektur bereitgestellt sind, Sie können solche Desktops aber auch in einer Nur-MAM-Architektur bereitstellen.



Referenzarchitektur mit XenMobile im internen Netzwerk

Wenn für Sie eine der folgenden Bedingungen zutrifft, können Sie XenMobile im internen Netzwerk bereitstellen.

- Sie haben keinen Hypervisor in der DMZ bzw. ein Hypervisor ist dort nicht zugelassen.
- Ihre DMZ darf nur Netzwerkgeräte enthalten.
- Ihre Sicherheitsanforderungen erfordern die Verwendung von SSL-Offload.



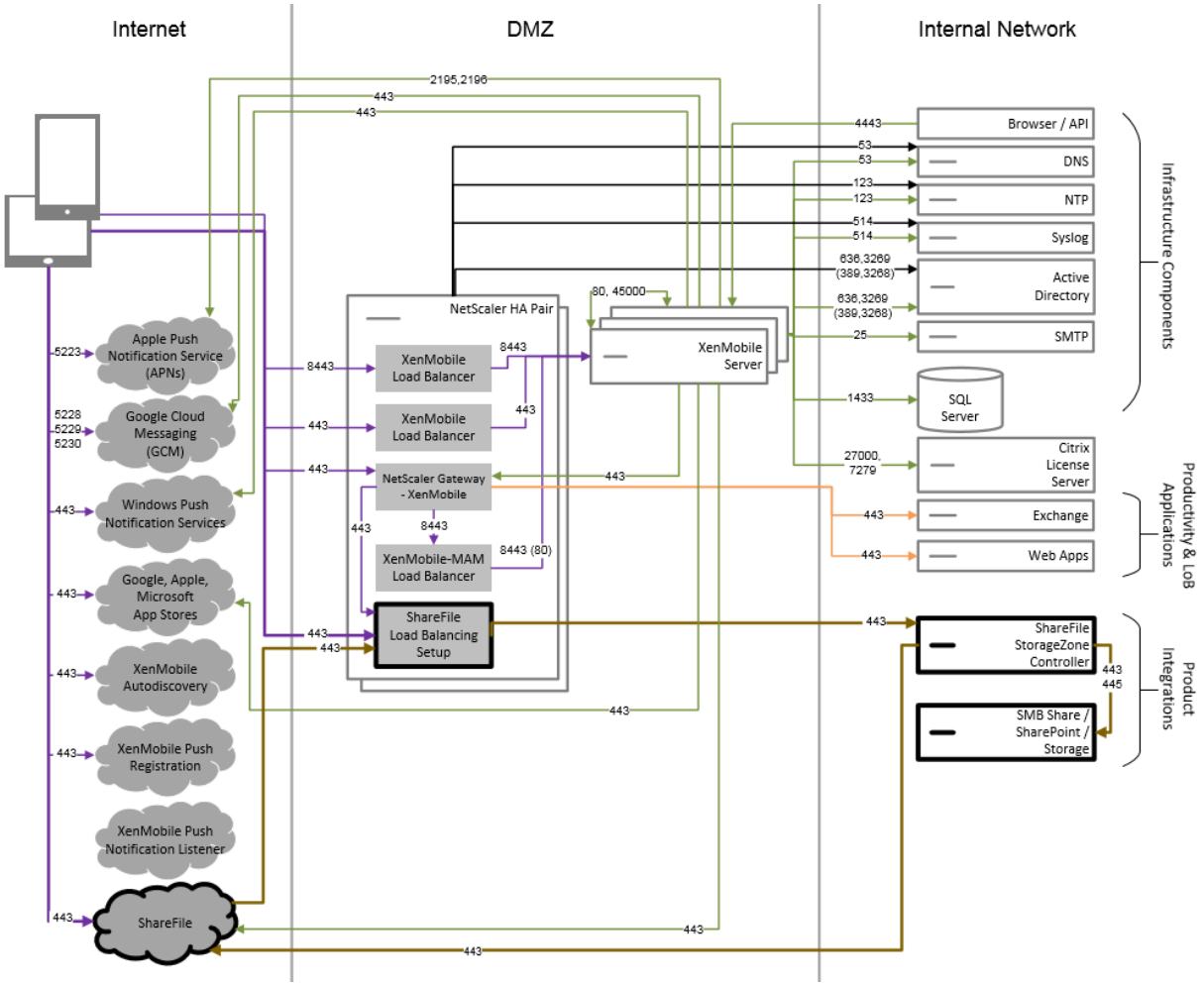
Referenzarchitektur mit Citrix Content Collaboration

Stellen Sie diese Architektur bereit, wenn Sie Citrix Files oder nur Speicherzonenconnectors in XenMobile integrieren möchten. Die Citrix Files-Integration eignet sich zur Erfüllung folgender Anforderungen:

- Sie benötigen einen IDP für das Single Sign-On (SSO) bei ShareFile.com.
- Sie müssen Konten in ShareFile.com bereitstellen.
- Sie haben On-Premises-Datenrepositorys, auf die von mobilen Geräten aus zugegriffen werden muss.

Eine ausschließliche Integration in Speicherzonenconnectors bietet den Benutzern sicheren mobilen Zugriff auf bestehende lokale Speicherrepositorys, wie z. B. SharePoint-Sites und Netzwerkdateifreigaben. In dieser Konfiguration müssen Sie keine Citrix Content Collaboration-Unterdomäne einrichten, Benutzer für Citrix Files bereitstellen oder Citrix Files-Daten hosten.

Das Diagramm zeigt Citrix Files zwar in einer MDM+MAM-Architektur, Sie können es aber genauso auch in einer Nur-MAM-Architektur bereitstellen.



Servereigenschaften

January 5, 2022

Servereigenschaften sind global und gelten für alle Vorgänge, Benutzer und Geräte einer XenMobile-Instanz. Citrix empfiehlt, die in diesem Artikel behandelten Servereigenschaften für Ihre Umgebung zu bewerten. Setzen Sie sich mit Citrix in Verbindung, bevor Sie andere Servereigenschaften ändern.

Bei Änderung einiger Servereigenschaften ist ein Neustart jedes XenMobile-Serverknotens erforderlich. XenMobile benachrichtigt Sie, wenn ein Neustart erforderlich ist.

Einige Servereigenschaften verbessern die Leistung und Stabilität. Informationen finden Sie unter Optimieren von XenMobile-Prozessen.

Bereitstellen von Legacy-Android-Apps auf Android Enterprise-Geräten: Wenn für `afw.allow.legacy.apps` die Einstellung **`true`** festgelegt wurde, erhalten Android Enterprise-Geräte sowohl

Legacy-Android-Apps als auch Android Enterprise-Apps. Wenn die Einstellung **false** festgelegt wurde, erhalten Android Enterprise-Geräte nur Android Enterprise-Apps. Der Standardwert ist **true**.

Dateinamenerweiterungen für die Dateirichtlinie zulassen: Konfigurieren Sie `file.extension.whitelist` mit einer durch Trennzeichen getrennten Liste von Dateitypen, die Administratoren unter Verwendung der Dateirichtlinie hochladen können. Die folgenden Dateitypen können nicht hochgeladen werden, selbst wenn Sie sie dieser Positivliste hinzufügen:

- CAB
- APPX
- IPA
- APK
- XAP
- MDX
- .exe

Der Standardwert ist `7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,mscr,pl,py,rb,sh,tcl,txt,htm,html,doc,docx,rtf,xap`.

Zugriff auf alle Apps im verwalteten Google Play Store. Bei Einstellung auf **true** macht XenMobile alle Apps aus dem öffentlichen Google Play Store über den verwalteten Google Play Store zugänglich. Wenn Sie diese Eigenschaft auf **true** setzen, werden die Apps aus dem öffentlichen Google Play Store für alle Android Enterprise-Benutzer zugelassen. Mit der Geräteeinschränkungsrichtlinie können Administratoren dann den Zugriff auf diese Apps steuern. Die Standardeinstellung ist **false**.

Registrierung von Android Enterprise-Arbeitsprofil auf unternehmenseigenen Geräten. Wenn für `afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled` die Einstellung **true** festgelegt wurde, können Geräte mit Android 11 oder höher im Modus "Arbeitsprofil auf unternehmenseigenen Geräten" (WPCOD) registriert werden. Die Änderungen für diesen Registrierungsmodus werden in der XenMobile Server-Konsole übernommen. Wenn die Einstellung **false** festgelegt wurde, sind keine WPCOD-Einstellungen verfügbar. Der Standardwert ist **true**.

Zusätzliche Einstellungen zu Android Enterprise-Einschränkungen. Wenn für die Eigenschaft `afw.restriction.policy.v2` der Wert **true** festgelegt wurde, sind die folgenden Einschränkungseinstellungen für Android Enterprise-Geräte verfügbar:

- App-Deinstallation zulassen
- Bluetooth-Freigabe zulassen

Weitere Informationen zu diesen Einstellungen finden Sie unter Geräteeinschränkungsrichtlinie.

Android Enterprise-Einschränkungen für COPE-Geräte. Legen Sie für `afw.restriction.cope` den Wert **true** fest, um die Einstellung **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil bzw. Arbeitsprofil auf unternehmenseigenen Geräten anwenden** in der Einschränkungsrichtlinie zu aktivieren. Der Standardwert ist **true**. Weitere Informationen zu dieser Einstellung finden Sie unter Geräteeinschränkungsrichtlinie.

Allow hostnames for iOS App Store links: Eigenschaft `ios.app.store.allowed.hostnames` ist eine Liste zulässiger Hostnamen, die beim Hochladen öffentlicher App Store-Apps auf den Server mithilfe der öffentlichen APIs verwendet wird. Wenn Sie öffentliche App Store-Apps statt eines Uploads über den Server mithilfe der öffentlichen APIs hochladen möchten, konfigurieren Sie diese Eigenschaft. Der Standardwert ist `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com`.

Alternativer APNs-Port. Sie können Port 2197 anstelle von Port 443 zum Senden und Empfangen von APNs-Benachrichtigungen von `api.push.apple.com` verwenden. Der Port verwendet die HTTP/2-basierte APNs-Anbieter-API. Legen Sie für die Eigenschaft `apns.http2.alternate.port.enabled` den Wert **`true`** fest, um Port 2197 zu verwenden. Der Standardwert der Servereigenschaft `apns.http2.alternate.port.enabled` ist **`false`**.

Kennwortvalidierung aktivieren, um lokale Benutzer mit schwachen Kennwörtern zu verhindern. Wenn für `enable.password.strength.validation` der Wert **`true`** festgelegt wurde, können Sie keine lokalen Benutzer mit einem schwachen Kennwort hinzufügen. Wurde der Wert **`false`** festgelegt, können Sie mit der öffentlichen API lokale Benutzer mit einem schwachen Kennwort erstellen. Der Standardwert ist **`true`**.

Registrierung für Android- und iOS-Geräte mit Rooting/Jailbreak blockieren: Wenn diese Eigenschaft auf **`true`** festgelegt wird, blockiert XenMobile die Registrierung von Android-Geräten mit Rooting und von iOS-Geräten mit Jailbreak. Die Standardeinstellung ist **`true`**. Die empfohlene Einstellung **`true`** gilt für alle Sicherheitsstufen.

Registrierung erforderlich: `wsapi.mdm.required.flag` Gilt nur im XenMobile Server-Modus ENT und gibt an, ob die Benutzer eine Registrierung bei MDM durchführen müssen. Die Eigenschaft gilt für alle Benutzer und Geräte der XenMobile-Instanz. Eine erforderliche Registrierung erhöht die Sicherheit der Anwendung. Diese Entscheidung hängt jedoch davon ab, ob Sie MDM verwenden möchten. Standardmäßig wird die Registrierung nicht erzwungen.

Wenn Sie die Einstellung auf **`false`** festlegen, können Benutzer die Registrierung ablehnen und dennoch ggf. mit ihrem Gerät auf Apps über den XenMobile Store zugreifen. Wenn die Eigenschaft auf **`true`** festgelegt wird, wird allen Benutzern, die die Registrierung ablehnen, der Zugriff auf Apps verweigert.

Wenn Sie diese Eigenschaft nach der Benutzerregistrierung ändern, müssen sich die Benutzer erneut registrieren.

Informationen darüber, wann eine MDM-Registrierung erforderlich ist, finden Sie unter Geräteverwaltung und MDM-Registrierung.

Enable multimode enrollment: Mit der Eigenschaft `enable.multimode.xms` können Sie Registrierungsprofile auf einem XenMobile-Server erstellen, der die Registrierungseinstellungen für die Geräte- und die App-Verwaltung für Android- und iOS-Geräte steuert. Darüber hinaus ermöglicht das neu erweiterte Registrierungsprofil-Feature die Registrierung dedizierter Android-Geräte und die

Registrierung von Android- und iOS-Geräten im Nur-MAM-Modus. Wenn die Eigenschaft auf **false** festgelegt ist, sind diese Registrierungsoptionen beim Einrichten von Registrierungsprofilen nicht verfügbar. Der Standardwert ist **true**. Geräte, die registriert werden, während die Eigenschaft auf **true** festgelegt ist, funktionieren weiter, wenn Sie die Einstellung in **false** ändern.

Enable the Self-Help Portal: Wenn `shp.console.enable` auf **false** festgelegt ist, ist kein Zugriff auf das Selbsthilfeportal möglich. Wenn Benutzer das Portal über Port 443 aufrufen, wird ein Fehler 404 angezeigt. Benutzer, die über Port 4443 zum Portal navigieren, erhalten die Meldung "Zugriff verweigert". Bei Auswahl von **true** erfolgt der Zugriff auf das Selbsthilfeportal über Port 443. Die Standardeinstellung ist **false**.

Local user account lockout limit: Mit der Einschränkungsrichtlinie können Sie ein Anmeldeversuchslimit für Active Directory-Benutzer festlegen. Mit dem Schlüssel `local.user.account.lockout.limit` ist dies auch für lokale Benutzerkonten möglich. Wenn ein Benutzer die von Ihnen vorgegebene Anzahl Anmeldeversuche unternommen hat, kann er es erst nach Ablauf einer Zeitspanne erneut versuchen. Die Länge der Zeitspanne konfigurieren Sie über die Eigenschaft **Local user account lockout time**. Der Standardwert ist `6`.

Local user account lockout time: Mit der Eigenschaft `local.user.account.lockout.time` können Sie eine Anzahl von Minuten festlegen, die vergehen müssen, bevor ein gesperrtes lokales Benutzerkonto erneut versuchen kann, sich anzumelden. Der Standardwert ist `30` Minuten.

Maximum size of file upload restriction enabled: Aktivieren Sie die Beschränkung der maximalen Dateigröße für Uploads `max.file.size.upload.restriction` auf **true**. Wenn Sie diese Einschränkung aktivieren, konfigurieren Sie die maximale Dateigröße mit `max.file.size.upload.allowed`. Der Standardwert dieser Eigenschaft ist **true**.

Maximum size of file upload allowed: Mit `max.file.size.upload.allowed` können Sie eine maximale Dateigröße für Uploads angeben. Beispielwerte: `500 B`, `1 KB`, `1 MB`, `1 MiB`, `1 G` oder `1 GiB`. Der Standardwert ist `5 MB`.

Inaktivitätstimeout in Minuten: Die Zeitdauer in Minuten, nach welcher XenMobile einen inaktiven Benutzer abmeldet, der auf die XenMobile-Konsole über die öffentliche XenMobile Server-API oder eine Drittanbieter-App zugegriffen hat. Ein Timeout von `0` bedeutet, dass inaktive Benutzer angemeldet bleiben. Für Apps von Drittanbietern, die auf die API zugreifen, ist es in der Regel erforderlich, dass der Benutzer angemeldet bleibt. Die Standardeinstellung ist `5`.

Registrierung für iOS-Geräteverwaltung: Stammzertifizierungsstelle ggf. installieren: Der aktuelle Registrierungsworkflow von Apple erfordert, dass Benutzer die MDM-Profile manuell installieren. Der Workflow gilt nicht für die MDM-Registrierung für in Apple Business Manager und Apple School Manager zugewiesene Server. Bei der manuellen MDM-Registrierung erhalten iOS-Gerätebenutzer jedoch nur die MDM-Gerätezertifikataufforderung während der Registrierung.

Zur Verbesserung der Benutzererfahrung bei der manuellen Registrierung empfiehlt Citrix, die Servereigenschaft `ios.mdm.enrollment.installRootCaIfRequired` in **false** zu ändern. Der

Standardwert ist **`true`**. Mit der Änderung wird während der MDM-Registrierung ein Safari-Fenster geöffnet, um die Profilinstallation für die Benutzer zu vereinfachen.

VPP-Baselineintervall: Die Eigenschaft `vpp.baseline` legt das Mindestintervall fest, in dem XenMobile den Import von Volume Purchase-Lizenzen von Apple wiederholt. Durch Aktualisierung der Lizenzinformationen wird sichergestellt, dass in XenMobile alle Änderungen widergespiegelt werden, beispielsweise das manuelle Löschen einer importierten App aus Volume Purchase. Standardmäßig aktualisiert XenMobile die Volume Purchase-Lizenzbasis mindestens alle `1440` Minuten.

Wenn Sie zahlreiche Volume Purchase-Lizenzen installiert haben (beispielsweise über 50.000), empfiehlt Citrix die Verlängerung des Basisintervalls, um den Mehraufwand zu verringern, der beim Importieren von Lizenzen entsteht. Wenn Sie davon ausgehen, dass Apple häufig Änderungen an den Volume Purchase-Lizenzen vornimmt, rät Citrix dazu, den Wert zu verringern, damit XenMobile fortlaufend mit den Änderungen aktualisiert wird. Das Mindestintervall zwischen zwei Basiswerten beträgt 60 Minuten. Da der Cron Job alle 60 Minuten ausgeführt wird, kann das Intervall zwischen Basiswerten auf bis zu 119 Minuten steigen, wenn das Volume Purchase-Basisintervall auf 60 Minuten festgelegt ist.

Maximales Inaktivitätsintervall (in Minuten) für das XenMobile MDM-Selbsthilfeportal: Dieser Eigenschaftsname spiegelt ältere XenMobile-Versionen wider. Die Eigenschaft steuert das maximale Inaktivitätsintervall der XenMobile-Konsole. Das Intervall ist die Zeit in Minuten, nach der ein inaktiver Benutzer von der XenMobile-Konsole abgemeldet wird. Ein Timeoutwert von 0 bedeutet, dass ein inaktiver Benutzer angemeldet bleibt. Die Standardeinstellung ist `30`.

Richtlinien für Geräte und Apps

January 5, 2022

XenMobile Geräte- und App-Richtlinien ermöglichen einen optimierten Ausgleich mehrerer Faktoren. Dazu gehören beispielsweise:

- Unternehmenssicherheit
- Schutz der Daten und Anlagen von Unternehmen
- Schutz von Benutzerdaten
- Produktive und positive Benutzererfahrung

Der optimale Ausgleich dieser Faktoren kann variieren. Stark regulierte Organisationen, beispielsweise im Finanzsektor, benötigen strengere Sicherheitsmechanismen als andere Branchen, z. B. Bildung und Einzelhandel, wo es vor allem auf die Produktivität der Benutzer ankommt.

Durch zentrale Steuerung und Konfiguration von Richtlinien auf der Grundlage von Identität, Geräten, Standort und Verbindungstyp des Benutzers können Sie die missbräuchliche Nutzung von Unternehmensinhalten wirksam einschränken. Falls ein Gerät verloren oder gestohlen wird,

können Sie Unternehmensanwendungen und -daten remote deaktivieren, sperren oder löschen. Das Gesamtergebnis ist eine Lösung, mit der die Zufriedenheit und Produktivität der Mitarbeiter erhöht wird, während Sicherheit und administrative Steuerung ebenfalls gewährleistet sind.

Der Hauptschwerpunkt dieses Artikels liegt auf den zahlreichen Geräte- und App-Richtlinien, die in Verbindung mit der Sicherheit konfiguriert werden können.

Richtlinien zur Einschränkung von Sicherheitsrisiken

XenMobile Geräte- und App-Richtlinien berücksichtigen zahlreiche Situationen, die ein Sicherheitsrisiko darstellen können. Dazu gehören beispielsweise:

- Benutzer versuchen, über nicht vertrauenswürdige Geräte oder an unsicheren Standorten auf Apps und Daten zuzugreifen.
- Benutzer senden Daten von Gerät zu Gerät.
- Ein nicht autorisierter Benutzer will auf Daten zugreifen.
- Benutzer, die ihr Privatgerät für die Arbeit verwendet haben (BYOD), verlassen die Firma.
- Ein Benutzer verliert ein Gerät.
- Benutzer benötigen jederzeit einen sicheren Netzwerkzugriff.
- Benutzer benutzen ein verwaltetes Privatgerät, und Sie müssen Firmendaten von persönlichen Daten trennen.
- Die Benutzeranmeldeinformationen müssen nach Inaktivität eines Geräts überprüft werden.
- Benutzer kopieren vertrauliche Inhalte über die Zwischenablage in nicht geschützte E-Mail-Systeme.
- Benutzer empfangen E-Mail-Anlagen oder Weblinks mit vertraulichen Daten auf einem Gerät, auf dem Privat- und Firmenkonten angelegt sind.

Diese Situationen verweisen auf zwei Hauptbereiche, die beim Schutz von Firmendaten Probleme verursachen können:

- Datenspeicherung
- Datenübertragung

Schutz ruhender Daten durch XenMobile

Daten, die auf mobilen Geräten gespeichert sind, werden auch ruhende Daten genannt. XenMobile verwendet die von den iOS- und Android-Plattformen bereitgestellte Geräteverschlüsselung. XenMobile ergänzt die plattformbasierte Verschlüsselung um Features, wie z. B. die Complianceprüfung, die über das Citrix MAM SDK verfügbar sind.

Die MAM-Funktionen in XenMobile bieten Sicherheit und Verwaltungsfunktionen für alle mobilen Produktivitätsapps, MDX-aktivierten Apps und zugehörige Daten.

Das SDK für mobile Apps ermöglicht die Bereitstellung von Apps über XenMobile mit der Citrix MDX-App-Containertechnologie. Die Containertechnologie trennt auf den Geräten der Benutzer Unternehmens-Apps und -Daten von persönlichen Apps und -Daten. Durch die Trennung der Daten können Sie benutzerdefinierte Apps, Drittanbieter-Apps oder mobile BYO-Apps durch umfassende richtlinienbasierte Steuerelemente sichern.

XenMobile enthält auch Verschlüsselung auf App-Ebene. XenMobile verschlüsselt die in einer MDX-aktivierten App gespeicherten Daten separat und ohne erforderlichen Passcode des Gerätes. Sie müssen das Gerät auch nicht verwalten, um die Richtlinie umsetzen zu können.

Richtlinien und das Mobile Apps SDK ermöglichen Folgendes:

- Geschäftliche und private Apps und Daten werden separat in einem sicheren mobilen Container gespeichert.
- Sichere Apps durch Verschlüsselung und andere Technologien zum Verhindern von Datenverlust bei mobilen Daten.

MDX-Richtlinien bieten zahlreiche Steuerungsmöglichkeiten. Sie können die nahtlose Integration zwischen Apps aktivieren, die MAM-SDK-fähig oder MDX-umschlossen sind und gleichzeitig die gesamte Kommunikation steuern. Auf diese Weise können Sie Richtlinien erzwingen und beispielsweise sicherstellen, dass nur MAM-SDK-fähige Apps oder Apps, die mit MDX umschlossen wurden, auf Daten zugreifen können.

Neben der Steuerung von Geräte- und App-Richtlinien lassen sich ruhende Daten am besten über eine Verschlüsselung schützen. XenMobile fügt eine Verschlüsselungsebene für alle Daten ein, die in einer MDX-aktivierten App gespeichert sind. Dadurch erhalten Sie die Kontrolle über Richtlinien zur Verschlüsselung öffentlicher oder privater Dateien und zu Ausnahmen für die Verschlüsselung. Das Mobile Apps SDK verwendet FIPS 140-2-konforme AES-256-Bit-Verschlüsselung mit Schlüsseln, die in einem geschützten Citrix Geheimtresor gespeichert sind.

Schutz von Daten im Übertragungsprozess durch XenMobile

Daten, die zwischen Mobilgeräten des Benutzers und dem internen Netzwerk übertragen werden, heißen auch Daten im Übertragungsprozess. MDX-App-Container ermöglichen einen anwendungsspezifischen VPN-Zugriff auf Ihr internes Netzwerk über Citrix Gateway.

Betrachten Sie die Situation, in der Mitarbeiter von einem Mobilgerät aus auf die folgenden Ressourcen im sicheren Unternehmensnetzwerk zugreifen möchten:

- Der Unternehmens-E-Mail-Server
- Eine SSL-fähige Webanwendung, die im Unternehmensintranet gehostet wird
- Auf einem Dateiserver oder Microsoft SharePoint gespeicherte Dokumente

MDX ermöglicht den Zugriff auf diese Unternehmensressourcen von mobilen Geräten über ein anwendungsspezifisches Micro-VPN. Jedes Gerät nutzt einen eigenen Micro-VPN-Tunnel.

Für die Micro-VPN-Funktionalität ist kein geräteübergreifendes VPN erforderlich, welches die Sicherheit auf nicht vertrauenswürdigen Mobilgeräten einschränken kann. Das interne Netzwerk ist keiner Schadsoftware und keinen Angriffen ausgesetzt, die das gesamte Unternehmenssystem infizieren könnten. Geschäftliche und private mobile Apps können nebeneinander auf dem Gerät existieren.

Um eine noch höhere Sicherheitsstufe anzubieten, können Sie für MDX-aktivierte Apps eine Richtlinie mit Alternativem Citrix Gateway konfigurieren. Diese legt die Authentifizierung und Micro-VPN-Sitzungen für eine App fest. Sie können ein Alternatives Citrix Gateway mit der Richtlinie "Onlinesitzung erforderlich" verwenden, um eine erneute Authentifizierung von Apps bei dem spezifischen Gateway zu erzwingen. Solche Gateways haben normalerweise unterschiedliche (höhere Sicherheit) Authentifizierungsanforderungen und Datenverwaltungsrichtlinien.

Neben Sicherheitsfeatures bietet das Micro-VPN-Feature Komprimierungsalgorithmen und andere Techniken zur Datenoptimierung. Komprimierungsalgorithmen stellen sicher, dass:

- nur die Mindestmenge an Daten übertragen wird
- die Übertragung in der schnellstmöglichen Zeit erfolgt. Die Geschwindigkeit verbessert die Benutzererfahrung und ist ein wichtiger Erfolgsfaktor bei der Akzeptanz mobiler Geräte.

Überprüfen Sie Ihre Geräterichtlinien in regelmäßigen Abständen, zum Beispiel in folgenden Situationen:

- Wenn eine neue Version von XenMobile neue oder aktualisierte Richtlinien aufgrund veröffentlichter Gerätebetriebssystemupdates enthält
- Beim Hinzufügen eines Gerätetyps:

  Obwohl viele Richtlinien für alle Geräte gelten, gibt es für jedes Gerät einen betriebssystemspezifischen Richtliniensatz. Daher gibt es möglicherweise Unterschiede zwischen iOS-, Android- und Windows-Geräten und sogar zwischen Android-Geräten verschiedener Hersteller.
- Sie möchten XenMobile mit unternehmens- oder branchenspezifischen Änderungen synchronisieren, beispielsweise mit neuen Konformitätsanforderungen oder Sicherheitsrichtlinien im Unternehmen.
- Eine neue Version des MAM-SDKs enthält neue oder aktualisierte Richtlinien.
- Sie möchten eine App hinzufügen oder aktualisieren.
- Zum Integrieren neuer Workflows für Ihre Benutzer aufgrund neuer Apps oder Anforderungen.

Szenarios für App-Richtlinien und Anwendungsfälle

Sie können zwar auswählen, welche Apps über Secure Hub verfügbar sind, vielleicht möchten Sie aber auch die Interaktion dieser Apps mit XenMobile definieren. Verwenden Sie App-Richtlinien:

- Wenn Sie möchten, dass sich Benutzer nach einem bestimmten Zeitraum authentifizieren.

- Wenn Sie Benutzern Offlinezugriff auf ihre Daten gewähren möchten.

Die folgenden Abschnitte enthalten einige der Richtlinien und Einsatzbeispiele.

- Eine Liste aller Drittanbieterrichtlinien, die Sie mit dem MAM-SDK in Ihre iOS- und Android-App integrieren können, finden Sie unter Überblick über das MAM-SDK.
- Eine Liste aller MDX-Richtlinien pro Plattform finden Sie unter MDX-Richtlinien.

Authentifizierungsrichtlinien

- **Gerätepasscode**

  Verwendungszweck dieser Richtlinie: Aktivieren Sie die Passcoderichtlinie für Geräte, um festzulegen, dass ein Benutzer nur dann auf eine MDX-App zugreifen kann, wenn das Gerät einen aktivierten Passcode hat. Dieses Feature gewährleistet die Verwendung der iOS-Verschlüsselung auf Geräteebene.

  Benutzerbeispiel: Bei Aktivieren dieser Richtlinie müssen Benutzer einen Passcode auf ihrem iOS-Gerät festlegen, bevor sie auf die MDX-App zugreifen können.

- **App-Passcode**

  Verwendungszweck dieser Richtlinie: Aktivieren Sie die Richtlinie für App-Passcodes, damit Benutzer in Secure Hub aufgefordert werden, sich bei der verwalteten App zu authentifizieren, bevor sie die App öffnen und auf Daten zugreifen können. Benutzer können sich über ihr Active Directory-Kennwort, die Citrix PIN oder die iOS Touch ID authentifizieren, je nachdem, was Sie in den XenMobile Server-Einstellungen unter “Clienteigenschaften” konfigurieren. Sie können unter “Clienteigenschaften” einen Inaktivitätstimer festlegen, damit Secure Hub bei andauernder Nutzung Benutzer erst nach Ablauf des Timers zur erneuten Authentifizierung bei der verwalteten App auffordert.

  Der App-Passcode unterscheidet sich vom Gerätepasscode, da beim Übertragen einer Gerätepasscode-Richtlinie an ein Gerät der Benutzer von Secure Hub aufgefordert wird, einen Passcode oder eine PIN zu konfigurieren. Diese müssen sie dann entsperren, bevor sie Zugriff auf ihr Gerät erhalten, entweder beim Einschalten des Geräts oder bei Ablauf des Inaktivitätstimers. Weitere Informationen finden Sie unter Authentifizierung in XenMobile.

  Benutzerbeispiel: Beim Öffnen von Citrix Secure Web auf dem Gerät müssen Benutzer nach Ablauf des Inaktivitätszeitraums ihre Citrix-PIN eingeben, bevor sie Websites durchsuchen können.

- **Onlinesitzung erforderlich**

  Verwendungszweck dieser Richtlinie: Wenn eine Anwendung Zugriff auf eine Web-App (einen Webdienst) benötigt, aktivieren Sie diese Richtlinie. Benutzer werden dann in XenMobile aufgefordert, eine Verbindung mit dem Unternehmensnetzwerk herzustellen oder eine Sitzung zu aktivieren, bevor sie die App verwenden.

Benutzerbeispiel: Wenn Benutzer eine MDX-App öffnen, für die die Richtlinie mit erforderlicher Onlinesitzung aktiviert ist, können sie die App erst dann verwenden, wenn sie über Wi-Fi oder ein Mobilnetz mit dem Netzwerk verbunden sind.

- **Maximale Offlinezeit**

  Verwendungszweck dieser Richtlinie: Verwenden Sie diese Richtlinie, um sicherzustellen, dass Benutzer eine Anwendung nicht für längere Zeit offline ausführen können, ohne den App-Anspruch zu bestätigen und die Richtlinien von XenMobile zu aktualisieren.

  Benutzerbeispiel: Wenn Sie eine MDX-App mit maximaler Offlinezeit konfigurieren, kann der Benutzer die App bis zum Ablauf des Offlinetimers offline verwenden. Anschließend muss der Benutzer sich per Mobilnetz oder Wi-Fi-Dienst mit dem Netzwerk verbinden und sich auf Aufforderung erneut authentifizieren.

Weitere Zugriffsrichtlinien

- **Kulanzzeitraum für App-Update (Stunden)**

  Verwendungszweck dieser Richtlinie: Der Kulanzzeitraum für App-Updates ist die Zeitdauer, vor deren Ablauf Benutzer eine App aktualisieren müssen, deren neue Version im XenMobile Store veröffentlicht wurde. Ist die Zeit abgelaufen, müssen Benutzer die App aktualisieren, bevor sie Zugriff auf die Daten in der App erhalten. Berücksichtigen Sie beim Festlegen dieses Werts die Anforderungen Ihrer mobilen Mitarbeiter, insbesondere von Benutzern, die aufgrund von Auslandsreisen längere Zeit offline sind.

  Benutzerbeispiel: Sie laden eine neue Version von Secure Mail in den XenMobile Store und definieren einen Kulanzzeitraum für das App-Update von 6 Stunden. Alle Benutzer von Secure Mail werden in einer Meldung aufgefordert, ihre Secure Mail-App innerhalb von 6 Stunden zu aktualisieren. Nach Ablauf der 6 Stunden werden Benutzer von Secure Hub zum XenMobile Store weitergeleitet.

- **Aktives Abfrageintervall (Minuten)**

  Verwendungszweck der Richtlinie: Das aktive Abfrageintervall ist der Zeitraum, in dem XenMobile prüft, wann für eine App notwendige Sicherheitsaktionen wie App sperren und App löschen durchzuführen sind.

  Benutzerbeispiel: Wenn Sie die Richtlinie für das aktive Abfrageintervall auf 60 Minuten festlegen und dann den Befehl zur App-Sperre von XenMobile an das Gerät senden, erfolgt die Sperre innerhalb von 60 Minuten nach der letzten Abfrage.

Richtlinien für nicht richtlinientreue Geräte

Wenn ein Gerät unter die Mindestanforderungen für die Compliance fällt, können Sie mit der Richtlinie "Verhalten für nicht richtlinientreue Geräte" wählen, welche Aktion ausgeführt wird. Informationen hierzu finden Sie unter Verhalten für nicht richtlinientreue Geräte.

App-Interaktionsrichtlinien

Verwendungszweck dieser Richtlinien: Verwenden Sie App-Interaktionsrichtlinien, um den Daten- und Dokumentenfluss von MDX-Apps zu anderen Apps auf dem Gerät zu steuern. Beispielsweise können Sie verhindern, dass Benutzer Daten in ihre persönlichen Apps außerhalb des Container verschieben oder externe Daten in die Apps im Container einfügen.

Benutzerbeispiel: Sie wählen für eine App-Interaktionsrichtlinie die Einstellung "Eingeschränkt", sodass Benutzer Texte zwar von Secure Mail in Secure Web, nicht jedoch in ihren persönlichen Safari- oder Chrome-Browser außerhalb des Containers kopieren können. Darüber hinaus können Benutzer Dokumentanlagen aus Secure Mail zwar in Citrix Files oder Quick Edit öffnen, jedoch nicht in ihren persönlichen Dateianzeige-Apps, die außerhalb des Containers sind.

App-Einschränkungsrichtlinien

Verwendungszweck dieser Richtlinien: Mit App-Einschränkungsrichtlinien legen Sie fest, auf welche Features Benutzer aus einer geöffneten MDX-App heraus zugreifen können. Dies ist hilfreich, um schädliche Aktivitäten zu verhindern, während die App ausgeführt wird. Die App-Einschränkungsrichtlinien von iOS und Android unterscheiden sich leicht. In iOS können Sie beispielsweise den Zugriff auf iCloud blockieren, während die MDX-App ausgeführt wird. In Android können Sie NFC blockieren, während die MDX-App ausgeführt wird.

Benutzerbeispiel: Wenn Sie die App-Einschränkungsrichtlinie zum Blockieren des Diktierfunktion auf iOS in einer MDX-App aktivieren, können Benutzer diese Funktion nicht auf der iOS-Tastatur verwenden, während die MDX-App ausgeführt wird. Diktierte Daten können damit nicht an den unsicheren Cloud-Diktierdienst eines Drittanbieters weitergegeben werden. Wenn Benutzer ihre persönliche App außerhalb des Containers öffnen, können sie die Diktierfunktion weiterhin für ihre persönliche Kommunikation nutzen.

Richtlinien für den App-Netzwerkzugriff

Verwendungszweck dieser Richtlinien: Mit den Richtlinien für den App-Netzwerkzugriff ermöglichen Sie den Zugriff aus einer MDX-App im Container auf dem Gerät auf Daten in Ihrem Unternehmensnetzwerk. Verwenden Sie für die Netzwerkzugriffsrichtlinie die Option **Tunnel zum internen Netzwerk**, um ein automatisiertes Micro-VPN von der MDX-App über Citrix ADC zu einem Backend-Webdienst oder -Datenspeicher einzurichten.

Benutzerbeispiel: Wenn ein Benutzer eine MDX-App mit aktivierter Tunnelfunktion öffnet (z. B. Secure Web), wird der Browser geöffnet und eine Intranetsite gestartet, ohne dass der Benutzer ein VPN starten muss. Die Secure Web-App greift automatisch über das Micro-VPN auf die Intranetsite zu.

Richtlinien für App-Geolocation/-Geofencing

Verwendungszweck dieser Richtlinien: Mit diesen Richtlinien steuern Sie App-Geolocation/-Geofencing und legen Einstellungen wie Längengrad von Mittelpunkt, Breitengrad von Mittelpunkt und Radius fest. Die Richtlinien beschränken den Zugriff auf Daten in MDX-Apps auf einen bestimmten geografischen Bereich. Die Richtlinien definieren einen geografischen Bereich durch einen Radius mit Koordinaten für Längen- und Breitengrad. Wenn ein Benutzer versucht, eine App außerhalb des definierten Radius zu verwenden, bleibt die App gesperrt und der Benutzer hat keinen Zugriff auf die App-Daten.

Benutzerbeispiel: Ein Benutzer kann auf Daten zu Fusionen und Übernahmen zugreifen, während er sich im Büro befindet. Sobald er seinen Bürostandort verlässt, hat er keinen Zugriff auf diese vertraulichen Daten.

Secure Mail-App-Richtlinien

- **Hintergrundnetzwerkdienste**

  Verwendungszweck dieser Richtlinie: Hintergrundnetzwerkdienste in Secure Mail verwenden Secure Ticket Authority (STA), eine Art SOCKS5-Proxy, um über Citrix Gateway eine Verbindung herzustellen. STA unterstützt längere Verbindungen und bietet eine bessere Akkulaufzeit im Vergleich zu Micro-VPN. STA ist daher ideal für E-Mail-Programme, die eine ständige Verbindung benötigen. Citrix empfiehlt, dass Sie diese Einstellungen für Secure Mail konfigurieren. Der Citrix ADC für XenMobile-Assistent richtet STA für Secure Mail automatisch ein.

  Benutzerbeispiel: Wenn STA nicht aktiviert ist, werden Android-Benutzer beim Öffnen von Secure Mail aufgefordert, ein VPN zu öffnen, das dann auf dem Gerät geöffnet bleibt. Wenn STA aktiviert ist, wird beim Öffnen von Secure Mail durch Android-Benutzer sofort eine Verbindung hergestellt und es ist kein VPN erforderlich.

- **Standardsynchronisierungsintervall**

  Verwendungszweck dieser Richtlinie: Mit dieser Einstellung wird die Standardanzahl von Tagen festgelegt, für die eine E-Mail-Synchronisierung mit Secure Mail erfolgt, wenn ein Benutzer das erste Mal auf Secure Mail zugreift. Bedenken Sie, dass die Synchronisierung aller E-Mails der vergangenen 2 Wochen länger dauert als nur für 3 Tage, und dass dies zu einem längeren Setup für den Benutzer führt.

Benutzerbeispiel: Bei einem Standardsynchronisierungsintervall von 3 Tagen findet ein Benutzer nach dem ersten Einrichten von Secure Mail alle E-Mails im Posteingang, die er in den vergangenen 3 Tagen erhalten hat. Wenn ein Benutzer E-Mails anzeigen möchte, die älter als 3 Tage sind, kann er eine Suche durchführen. Secure Mail zeigt dann auch ältere E-Mails an, die auf dem Server gespeichert sind. Nach der Installation von Secure Mail kann jeder Benutzer diese Einstellung an seine Anforderungen anpassen.

Geräterichtlinien und Anwendungsverhalten

Geräterichtlinien (gelegentlich auch als MDM-Richtlinien bezeichnet) legen fest, wie XenMobile mit Geräten interagiert. Obwohl viele Richtlinien für alle Geräte gelten, gibt es für jedes Gerät einen betriebssystemspezifischen Richtliniensatz. Die folgende Liste enthält einige dieser Geräterichtlinien und erläutert, wie sie verwendet werden. Eine Liste aller Geräterichtlinien finden Sie unter Geräterichtlinien.

- **App-Bestandsrichtlinie**

  Verwendungszweck dieser Richtlinie: Stellen Sie die App-Bestandsrichtlinie auf einem Gerät bereit, um sämtliche vom Benutzer installierten Apps anzuzeigen. Wenn Sie die App-Bestandsrichtlinie nicht bereitstellen, können Sie nur die vom Benutzer aus dem XenMobile Store installierten Apps anzeigen, nicht jedoch persönlich installierte Apps. Sie müssen diese Richtlinie verwenden, wenn Sie bestimmte Apps auf Unternehmensgeräten blockieren möchten.

  Benutzerbeispiel: Benutzer mit einem MDM-verwalteten Gerät können diese Funktion nicht deaktivieren. Die persönlich installierten Anwendungen des Benutzers sind für XenMobile-Administratoren sichtbar.

- **App-Sperre**

  Verwendungszweck dieser Richtlinie: Mit der App-Sperre können Sie Apps in Android sperren oder zulassen. Durch Zulassen von Apps können Sie beispielsweise ein Kioskgerät konfigurieren. Normalerweise stellen Sie die Richtlinie mit App-Sperre nur auf Unternehmensgeräten bereit, da sie einschränkt, welche Apps von Benutzern installiert werden können. Sie können ein Kennwort festlegen, mit dem Benutzer die Sperre außer Kraft setzen und auf blockierte Apps zugreifen können.

  Benutzerbeispiel: Sie möchten eine App-Sperr-Richtlinie bereitstellen, um die “Angry Birds”-App zu blockieren. Benutzer können “Angry Birds” dann zwar von Google Play herunterladen und installieren, beim Öffnen der App erhalten sie jedoch eine Nachricht, dass die App vom Administrator blockiert wurde.

- **Verbindungszeitplanrichtlinie**

Verwendungszweck dieser Richtlinie: Sie müssen die Verbindungszeitplanrichtlinie verwenden, damit Windows Mobile-Geräte für Funktionen wie MDM-Verwaltung, App-Push und Richtlinienbereitstellung eine Verbindung mit XenMobile Server herstellen können. Für Android-, Android Enterprise- und Chrome OS-Geräte verwenden Sie stattdessen Google Firebase Cloud Messaging (FCM), um eine Verbindung zu XenMobile Server herzustellen. Es gibt folgende Verbindungszeitplanoptionen:

- **Immer:** Die Verbindung bleibt jederzeit bestehen. Citrix empfiehlt diese Option zur Gewährleistung der optimalen Sicherheit. Wenn Sie **Immer** wählen, sollten Sie auch die Richtlinie für Verbindungstimer verwenden, um sicherzustellen, dass durch die Verbindung nicht der Akku entladen wird. Wenn Sie die Verbindung aufrechterhalten, können Sie Sicherheitsbefehle, wie Löschen und Sperren, bei Bedarf per Push auf dem Gerät bereitstellen. Aktivieren Sie unter "Bereitstellungszeitplan" auch die Option **Bereitstellen für immer aktive Verbindungen** für jede Richtlinie, die Sie auf dem Gerät bereitstellen.
- **Nie:** Die Verbindung muss manuell hergestellt werden. 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 Richtlinie auf dem Gerät, wenn das Gerät das nächste Mal eine Verbindung herstellt.
- **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.

Benutzerbeispiel: Sie möchten eine Passcoderichtlinie auf registrierten Geräten bereitstellen. Die Zeitplanrichtlinie gewährleistet, dass die Geräte sich in regelmäßigen Abständen erneut mit dem Server verbinden, um die neue Richtlinie abzufragen.

- **Anmeldeinformationen**

  Verwendungszweck dieser Richtlinie: Diese Richtlinie wird oft zusammen mit einer Wi-Fi-Richtlinie verwendet. Sie ermöglicht es Ihnen, Authentifizierungszertifikate bereitzustellen, die für die Authentifizierung bei internen Ressourcen benötigt werden, die eine Zertifikatauthentifizierung erfordern.

  Benutzerbeispiel: Sie stellen eine Wi-Fi-Richtlinie bereit, um ein Drahtlosnetzwerk auf dem Gerät zu konfigurieren. Das Wi-Fi-Netzwerk erfordert ein Zertifikat für die Authentifizierung. Die Anmeldeinformationsrichtlinie stellt ein Zertifikat bereit, das dann im Schlüsselspeicher des Be-

triebssystems gespeichert wird. Benutzer können das Zertifikat dann beim Verbindungsaufbau mit der internen Ressource auswählen.

- **Exchange-Richtlinie**

  Verwendungszweck dieser Richtlinie: XenMobile bietet zwei Optionen zum Bereitstellen von E-Mail mit Microsoft Exchange ActiveSync.

  - **Secure Mail-App:** Versand von E-Mails mit der Secure Mail-App, die Sie über den öffentlichen App-Store oder XenMobile Store verteilen.
  - **Systemeigene E-Mail-App:** Mit der Exchange-Richtlinie können Sie ActiveSync-E-Mail für den systemeigenen E-Mail-Client auf dem Gerät aktivieren. Mit der Exchange-Richtlinie für systemeigene E-Mail können Sie mit Makros die Benutzerdaten aus den Active Directory-Attributen übernehmen, z. B. ${user.username} für den Benutzernamen und ${user.domain} für die Benutzerdomäne.

  Benutzerbeispiel: Beim Bereitstellen der Exchange-Richtlinie senden Sie Exchange Server-Informationen an das Gerät. Der Benutzer wird dann von Secure Hub zur Authentifizierung aufgefordert, und die E-Mail-Synchronisierung wird gestartet.

- **Standort-/Ortungsrichtlinie**

  Verwendungszweck dieser Richtlinie: Mit dieser Richtlinie können Sie den Standort von Geräten auf einer Karte abrufen, vorausgesetzt auf dem Gerät ist GPS für Secure Hub aktiviert. Wenn Sie nach dem Bereitstellen der Richtlinie einen Ortungsbefehl vom XenMobile-Server senden, antwortet das Gerät mit den Standortkoordinaten.

  Benutzerbeispiel: Wenn Sie die Standort-/Ortungsrichtlinie bereitstellen und GPS auf dem Gerät aktiviert ist, können Benutzer sich bei Verlust ihres Geräts beim XenMobile-Selbsthilfeportal anmelden und mit der Option “Orten” den Standort des Geräts auf einer Karte anzeigen. Beachten Sie, dass der Benutzer festlegt, ob er die Verwendung von Positionsdiensten in Secure Hub zulässt. Sie können den Einsatz von Positionsdiensten nicht erzwingen, wenn Benutzer ein Gerät selbst registrieren. Die Auswirkung dieser Richtlinie auf die Akkulaufzeit ist ebenfalls zu berücksichtigen.

- **Passcoderichtlinie**

  Verwendungszweck dieser Richtlinie: 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.

  Benutzerbeispiel: Beim Bereitstellen einer Passcoderichtlinie auf einem verwalteten Gerät wird der Benutzer von Secure Hub aufgefordert, einen Passcode oder eine PIN zu konfigurieren. Diese müssen sie dann entsperren, bevor sie Zugriff auf ihr Gerät erhalten, entweder beim Einschalten des Geräts oder nach Ablauf des Inaktivitätstimers.

- **Profilentfernungsrichtlinie**

  Verwendungszweck dieser Richtlinie: Sie stellen eine Richtlinie für eine Gruppe von Benutzern bereit und müssen später die Richtlinie aus einer Untergruppe der Benutzer entfernen. Sie können die Richtlinie für ausgewählte Benutzer entfernen, indem Sie eine Profilentfernungsrichtlinie erstellen und über die Bereitstellungsregeln die Profilentfernungsrichtlinie nur für bestimmte Benutzernamen anwenden.

  Benutzerbeispiel: Das Bereitstellen einer Profilentfernungsrichtlinie auf Benutzergeräten fällt Benutzern u. U. überhaupt nicht auf. Wird mit der Profilentfernungsrichtlinie beispielsweise die Einschränkung entfernt, die bislang den Einsatz der Gerätekamera verhinderte, merkt der Benutzer nicht, dass die Kamera jetzt verwendet werden kann. Überlegen Sie, ob Sie Benutzer informieren, wenn Änderungen sich auf ihre Benutzererfahrung auswirken.

- **Einschränkungsrichtlinie**

  Verwendungszweck dieser Richtlinie: Über die Einschränkungsrichtlinie können Sie Features und Funktionalität auf verwalteten Geräten auf vielfältige Weise sperren und steuern. Sie können hunderte von Einschränkungsoptionen für unterstützte Geräte aktivieren, vom Deaktivieren der Kamera oder des Mikrofons auf einem Gerät bis zum Durchsetzen von Roamingregeln und dem Steuern des Zugriffs auf Drittanbieterdienste, wie App-Stores.

  Benutzerbeispiel: Wenn Sie eine Einschränkung auf einem iOS-Gerät bereitstellen, können Benutzer u. U. nicht auf iCloud oder den Apple App Store zugreifen.

- **AGB-Richtlinie**

  Verwendungszweck dieser Richtlinie: Sie müssen möglicherweise Benutzer auf rechtliche Auswirkungen hinweisen, die sich aus der Verwaltung ihres Geräts ergeben. Darüber hinaus sollten Sie Benutzer informieren, welche Sicherheitsrisiken mit dem Bereitstellen von Unternehmensdaten auf dem Gerät verbunden sind. Das benutzerdefinierte Dokument mit den AGB ermöglicht Ihnen die Veröffentlichung von Regeln und Hinweisen, bevor der Benutzer sich registriert.

  Benutzerbeispiel: Ein Benutzer sieht die AGB-Informationen während der Registrierung. Wenn er die Bedingungen nicht akzeptiert, wird die Registrierung beendet und er erhält keinen Zugriff auf Unternehmensdaten. Sie können Berichte für Personal- und Rechtsabteilung oder das Compliance-Team generieren, um anzuzeigen, wer die Nutzungsbedingungen akzeptiert oder abgelehnt hat.

- **VPN-Richtlinie**

  Verwendungszweck dieser Richtlinie: Mit der VPN-Richtlinie gewähren Sie Zugriff auf Backend-Systeme mit älterer VPN-Gatewaytechnologie. Die Richtlinie unterstützt eine Reihe von VPN-Anbietern, einschließlich Cisco AnyConnect, Juniper sowie Citrix VPN. Die Richtlinie

kann auch mit einer Zertifizierungsstelle verbunden werden und VPN bei Bedarf aktivieren, falls das VPN-Gateway diese Option unterstützt.

Benutzerbeispiel: Bei aktivierter VPN-Richtlinie öffnet das Gerät eines Benutzers eine VPN-Verbindung, wenn der Benutzer auf eine interne Domäne zugreift.

- **Webclip-Richtlinie**

  Verwendungszweck dieser Richtlinie: Mit dieser Richtlinie können Sie auf Geräten ein Symbol bereitstellen, das direkten Zugriff auf eine Website ermöglicht. Ein Webclip enthält einen Link zu einer Website und kann ein benutzerdefiniertes Symbol umfassen. Auf einem Gerät sieht ein Webclip wie ein App-Symbol aus.

  Benutzerbeispiel: Ein Benutzer kann durch Klicken auf ein Webclip-Symbol eine Website mit Diensten öffnen, auf die er zugreifen muss. Der Einsatz eines Weblinks ist benutzerfreundlicher, als eine Browserapp zu öffnen und eine Linkadresse einzugeben.

- **Wi-Fi-Richtlinie**

  Verwendungszweck dieser Richtlinie: Mit der Wi-Fi-Richtlinie können Sie auf einem verwalteten Gerät Wi-Fi-Netzwerkangaben wie SSID, Authentifizierungs- und Konfigurationsdaten bereitstellen.

  Benutzerbeispiel: Wenn Sie die Wi-Fi-Richtlinie bereitstellen, verbindet sich das Gerät automatisch mit dem Wi-Fi-Netzwerk und authentifiziert den Benutzer, der damit Zugriff auf das Netzwerk erhält.

- **Richtlinie zu Windows Information Protection (WIP)**

  Verwendungszweck dieser Richtlinie: Verwenden Sie die Windows Information Protection (WIP)-Richtlinie zum Schutz von Unternehmensdaten vor Verlust. Sie können angeben, welche Apps Windows Information Protection erfordern, und eine Erzwingungsstufe festlegen. Sie können beispielsweise jede unangemessene Datenfreigabe blockieren, vor einer unangemessenen Datenfreigabe warnen und Benutzern ermöglichen, die Richtlinie außer Kraft zu setzen. Sie können WIP im Hintergrund ausführen und unangemessene Datenfreigaben zulassen und protokollieren.

  Benutzerbeispiel: Sie möchten die WIP-Richtlinie so konfigurieren, dass eine unangemessene Datenfreigabe blockiert wird. Wenn ein Benutzer eine geschützte Datei kopiert oder an einem nicht geschützten Speicherort speichert, wird diese oder eine ähnliche Meldung angezeigt: Geschützte Arbeitsinhalte können nicht an diesem Ort abgelegt werden.

- **XenMobile Store-Richtlinie**

  Verwendungszweck dieser Richtlinie: Der XenMobile-Store ist ein einheitlicher App-Store, in dem Administratoren alle Unternehmensressourcen wie Apps und Daten veröffentlichen können, die von Benutzern benötigt werden. Ein Administrator kann Folgendes hinzufügen:

- Web-Apps, SaaS-Apps, MAM-SDK-fähige Apps, oder mit MDX umschlossene Apps
- Mobile Produktivitätsapps von Citrix
- Native mobile Apps wie IPA- oder APK-Dateien
- Apps aus dem Apple App Store und von Google Play
- Weblinks
- Mit Citrix StoreFront veröffentlichte Citrix Virtual Apps

Benutzerbeispiel: Nachdem ein Benutzer seine Geräte bei XenMobile registriert hat, kann er über Citrix Secure Hub auf den XenMobile Store zugreifen und alle für ihn verfügbaren Unternehmens-Apps und -Dienste anzeigen. Benutzer können Apps per Mausklick installieren, auf Daten zugreifen, Apps bewerten und App-Updates aus dem XenMobile Store herunterladen.

Optionen der Benutzerregistrierung

September 24, 2021

Es gibt mehrere Verfahren, mit denen Benutzer ihre Geräte bei XenMobile registrieren können. Bevor Sie Einzelheiten überlegen, entscheiden Sie, welche Geräte Sie bei MDM+MAM, MDM oder MAM registrieren möchten. Weitere Informationen über diese Verwaltungsmodi finden Sie unter Verwaltungsmodi.

Auf der höchsten Stufe gibt es vier Registrierungsoptionen:

- **Registrierungseinladung:** Senden Sie Benutzern eine Registrierungseinladung oder eine Einladungs-URL. Registrierungseinladungen und -URLs sind für Windows-Geräte nicht verfügbar.
- **Selbsthilfeportal:** Richten Sie ein Portal ein, über das Benutzer Secure Hub herunterladen und ihre Geräte registrieren oder sich selbst eine Registrierungseinladung senden können.
- **Manuelle Registrierung:** Informieren Sie Benutzer per E-Mail, Handbuch oder auf anderem Wege, dass das System bereit für die Registrierung ist. Benutzer laden dann Secure Hub herunter und registrieren ihre Geräte manuell.
- **Unternehmen:** Weitere Optionen für die Geräteregistrierung sind das Deployment Program von Apple sowie Android Enterprise von Google. Über jedes dieser Programme können Sie vorkonfigurierte Geräte erwerben, die sofort einsatzbereit sind. Weitere Informationen finden Sie in den Artikeln zum Apple-Bereitstellungsprogramm im Apple-Support und der Dokumentation zu Google Android Enterprise auf der Android Enterprise-Website.

Registrierungseinladung

Sie können per E-Mail eine Registrierungseinladung an Benutzer mit iOS- und macOS-Geräten, Android Enterprise-Geräten und Android-Legacygeräten senden. Registrierungseinladungen und -URLs

sind für Windows-Geräte nicht verfügbar.

Sie können auch einen Installationslink über SMTP oder SMS an Benutzer mit iOS-, macOS-, Android- oder Windows-Geräten senden. Weitere Informationen finden Sie unter Registrieren von Geräten.

Wenn Sie Registrierungseinladungen verwenden, können Sie:

- die Registrierungssicherheitsmodi **Einladungs-URL**, **Einladungs-URL + PIN** oder **Einladungs-URL + Kennwort** auswählen.
- die Modi in beliebiger Kombination verwenden.
- die Modi auf der Seite **Einstellungen** aktivieren oder deaktivieren.

Weitere Informationen zu jedem Registrierungssicherheitsmodus finden Sie unter Konfigurieren von Registrierungssicherheitsmodi.

Einladungen erfüllen viele Zwecke. Ihre häufigste Verwendung besteht darin, Benutzer zu benachrichtigen, dass das System verfügbar ist und sie sich registrieren können. Einladungs-URLs sind eindeutig. Nachdem ein Benutzer eine Einladungs-URL verwendet hat, ist die URL nicht mehr verfügbar. Nutzen Sie diese Eigenschaft zur Einschränkung der Benutzer oder Geräte, die sich im System registrieren.

Beim Konfigurieren eines Registrierungsprofils können Sie die Anzahl der Geräte steuern, die bestimmte Benutzer registrieren können, basierend auf Active Directory-Gruppen. Beispielsweise könnten Sie für die Finanzabteilung nur ein Gerät pro Benutzer zulassen.

Berücksichtigen Sie zusätzlich entstehende Kosten und mögliche Risiken bestimmter Registrierungsoptionen. Der Versand von Einladungen per SMS erfordert beispielsweise zusätzliche Infrastruktur. Weitere Informationen zu dieser Option finden Sie unter Benachrichtigungen.

Wenn Sie Registrierungseinladungen per E-Mail senden möchten, müssen Sie außerdem sicherstellen, dass die Benutzer außerhalb von Secure Hub auf ihre E-Mails zugreifen können. Verwenden Sie gegebenenfalls den Registrierungssicherheitsmodus mit Einmalkennwort (OTP) als Alternative zu Active Directory-Kennwörtern für die MDM-Registrierung.

Selbsthilfeportal

Die Benutzer können eine Registrierungseinladung über das Selbsthilfeportal anfordern. Weitere Informationen über das Einrichten des Selbsthilfeportals finden Sie unter Konfigurieren von Registrierungssicherheitsmodi.

Manuelle Registrierung

Bei einer manuellen Registrierung verbinden sich Benutzer über Autodiscovery oder über Eingabe der Serverinformationen mit XenMobile. Bei Verwendung von AutoDiscovery benötigen Benutzer

für die Anmeldung nur ihre E-Mail-Adresse oder die Active Directory-Anmeldeinformationen im UPN-Format (Benutzerprinzipalname). Ohne AutoDiscovery müssen sie die Serveradresse und ihre Active Directory-Anmeldeinformationen eingeben. Weitere Informationen zum Einrichten von AutoDiscovery finden Sie unter XenMobile AutoDiscovery Service.

Es gibt mehrere Möglichkeiten, die manuelle Registrierung einfacher zu gestalten. Sie können eine Anleitung erstellen und diese an Benutzer verteilen, damit sie sich selbst registrieren. Sie können Ihre IT-Abteilung beauftragen, Benutzergruppen in bestimmten Zeitfenstern manuell zu registrieren. Sie können jede andere Methode verwenden, bei der Benutzer ihre Anmelde- und/oder Serverinformationen eingeben müssen.

Onboarding von Benutzern

Nach dem Einrichten Ihrer Umgebung müssen Sie festlegen, wie Sie Benutzer in die Umgebung aufnehmen. Weiter oben wurden bereits die einzelnen Sicherheitsmodi für die Benutzerregistrierung erläutert. In diesem Abschnitt wird beschrieben, wie Sie Benutzer erreichen können.

Offene Registrierung vs. Selektive Einladung

Beim Onboarding von Benutzern können Sie die Registrierung über zwei grundlegende Methoden zulassen:

- Offene Registrierung. Standardmäßig kann sich jeder Benutzer mit LDAP-Anmeldeinformationen und den XenMobile-Umgebungsinformationen registrieren.
- Eingeschränkte Registrierung. Sie können die Anzahl der Benutzer einschränken, indem sich nur eingeladene Benutzer registrieren können. Sie können auch die offene Registrierung nach Active Directory-Gruppe einschränken.

Bei Verwendung einer Einladung können Sie auch die Anzahl der Geräte beschränken, die ein Benutzer registrieren kann. In den meisten Situationen ist eine offene Registrierung zulässig, es sind jedoch folgende Punkte zu berücksichtigen:

- Für MAM können Sie die Registrierung problemlos über die Active Directory-Gruppenmitgliedschaft beschränken.
- Für MDM können Sie die Registrierung nur einschränken, indem Sie auf Basis der Active Directory-Gruppenmitgliedschaft die Anzahl der Geräte beschränken, die registriert werden können. Wenn Sie nur Unternehmensgeräte in Ihrer Umgebung zulassen, ist diese Einschränkung in der Regel unerheblich. Die Methode könnte sich jedoch für BYOD-Arbeitsbereiche eignen, wo Sie die Anzahl der Geräte in Ihrer Umgebung einschränken möchten.

Die selektive Einladung wird in der Regel seltener verwendet, da sie mehr Aufwand erfordert als eine offene Registrierung. Damit Benutzer ihre Geräte in Ihrer Umgebung registrieren können, müssen

Sie an jeden Benutzer eine separate Einladung senden. Hinweise zum Senden von Registrierungseinladungen finden Sie unter Senden von Registrierungseinladungen.

Es ist zwar möglich, Einladungen mithilfe von Active Directory-Gruppen zu bündeln, dies muss jedoch gestaffelt erfolgen.

Erster Kontakt mit Benutzern

Nachdem Sie sich für die offene Registrierung bzw. selektive Einladung entschieden und Ihre Umgebung entsprechend eingerichtet haben, müssen Sie Benutzer über ihre Registrierungsoptionen informieren.

Beim selektiven Einladungsverfahren sind E-Mail- und SMS-Nachrichten Teil des Verfahrens. Auch bei der offenen Registrierung können Sie E-Mails über die XenMobile-Konsole senden. Weitere Einzelheiten finden Sie unter Senden von Registrierungseinladungen.

Bedenken Sie in beiden Fällen, dass Sie für E-Mails einen SMTP-Server benötigen. Für Textnachrichten benötigen Sie einen SMS-Server. Ein solcher Server kann zusätzliche Kosten verursachen, die bei der Entscheidung zu berücksichtigen sind. Sie sollten vor der Wahl eines Verfahrens bedenken, auf welche Weise neue Benutzer auf Informationen wie E-Mail zugreifen. Wenn alle Benutzer über XenMobile auf ihre E-Mail zugreifen, ist das Senden einer Einladung per E-Mail problematisch.

Sie können für eine offene Registrierungsumgebung die Benachrichtigungen auch auf andere Weise außerhalb von XenMobile senden. Achten Sie bei dieser Option darauf, alle relevanten Informationen einzubeziehen. Teilen Sie den Benutzern mit, wo sie die Secure Hub App erhalten und welche Methode für die Registrierung verwendet werden soll. Wenn Sie die Discovery deaktiviert haben, müssen Sie den Benutzern auch die XenMobile-Serveradresse mitteilen. Weitere Informationen zu AutoDiscovery finden Sie unter XenMobile AutoDiscovery Service.

Optimieren von XenMobile-Prozessen

January 5, 2022

Die Leistung und Stabilität von XenMobile-Prozessen basiert auf vielen Einstellungen in XenMobile und wird durch die Konfiguration von Citrix ADC und der SQL Server-Datenbank beeinflusst. In diesem Artikel werden die Einstellungen beschrieben, die für eine Optimierung von XenMobile am häufigsten zu konfigurieren sind. Citrix empfiehlt, dass Sie jede der im Artikel beschriebenen Einstellungen überprüfen, bevor Sie XenMobile bereitstellen.

> **Wichtig:**
>
> In diesen Richtlinien wird davon ausgegangen, dass CPU und Arbeitsspeicher des XenMobile-

> Servers für die Anzahl der Geräte angemessen sind. Weitere Informationen zur Skalierbarkeit finden Sie unter Skalierbarkeit und Leistung.

Die folgenden Servereigenschaften gelten global für alle Vorgänge, Benutzer und Geräte einer XenMobile-Instanz. Bei Änderung einiger Servereigenschaften ist ein Neustart jedes XenMobile-Serverknotens erforderlich. XenMobile benachrichtigt Sie, wenn ein Neustart erforderlich ist.

Diese Richtlinien zur Optimierung gelten für geclusterte und nicht geclusterte Umgebungen.

hibernate.c3p0.idle_test_period

Diese XenMobile Server-Eigenschaft ist ein benutzerdefinierter Schlüssel, mit dem die Leerlaufzeit (in Sekunden) festgelegt wird, bevor eine Verbindung automatisch überprüft wird. Konfigurieren Sie den Schlüssel wie im Folgenden beschrieben. Die Standardeinstellung ist **30**.

- Schlüssel: **Benutzerdefinierter Schlüssel**
- Schlüssel: **hibernate.c3p0. idle_test_period**
- Wert: **120**
- Anzeigename: **hibernate.c3p0. idle_test_period**
- Beschreibung: **Leerlaufzeit vor Ruhezustand**

hibernate.c3p0.max_size

Dieser benutzerdefinierte Schlüssel legt fest, wie viele Verbindungen zur SQL Server-Datenbank von XenMobile maximal geöffnet werden können. XenMobile verwendet den für diesen benutzerdefinierten Schlüssel eingegebenen Wert als Obergrenze. Die Verbindungen werden nur bei Bedarf geöffnet. Wählen Sie Ihre Einstellungen je nach Kapazität des Datenbankservers.

Berücksichtigen Sie die folgende Gleichung in einer Clusterkonfiguration. Ihre c3p0-Verbindung multipliziert mit der Anzahl der Knoten entspricht der tatsächlichen Höchstanzahl an Verbindungen zur SQL Server-Datenbank, die XenMobile öffnen kann.

Wird dieser Wert in geclusterten und nicht geclusterten Konfigurationen mit zu kleinem SQL Server zu hoch angesetzt, kann dies bei Spitzenlast zu Problemen führen. Ein zu niedrig eingestellter Wert bedeutet, dass verfügbare SQL-Ressourcen möglicherweise ungenutzt bleiben.

Konfigurieren Sie den Schlüssel wie im Folgenden beschrieben. Der Standardwert ist **1000**.

- Schlüssel: **hibernate.c3p0.max_size**
- Wert: **1000**
- Anzeigename: **hibernate.c3p0.max_size**
- Beschreibung: DB-Verbindungen mit SQL

hibernate.c3p0.min_size

Dieser benutzerdefinierte Schlüssel legt fest, wie viele Verbindungen zur SQL Server-Datenbank von XenMobile mindestens geöffnet werden. Konfigurieren Sie den Schlüssel wie im Folgenden beschrieben. Der Standardwert ist **100**.

- Schlüssel: **hibernate.c3p0.min_size**
- Wert: **100**
- Anzeigename: **hibernate.c3p0.min_size**
- Beschreibung: DB-Verbindungen mit SQL

hibernate.c3p0.timeout

Dieser benutzerdefinierte Schlüssel definiert den Wert für Leerlauftimeouts. Bei einem Datenbankcluster mit Failover empfiehlt Citrix, diesen benutzerdefinierten Schlüssel hinzuzufügen und einzurichten, um Leerlauftimeouts zu reduzieren. Die Standardeinstellung ist **120**.

- Schlüssel: **Benutzerdefinierter Schlüssel**
- Schlüssel: **hibernate.c3p0.timeout**
- Wert: **120**
- Anzeigename: **hibernate.c3p0.timeout**
- Beschreibung: Timeout bei Datenbankleerlauf

Taktintervall der Pushdienste

Diese Einstellung legt fest, wie häufig ein iOS-Gerät prüft, ob zwischenzeitlich eine APNs-Benachrichtigung nicht zugestellt wurde. Eine Erhöhung der APNs-Taktfrequenz kann die Datenbankkommunikation optimieren. Ein zu hoher Wert kann die Arbeitslast unnötig erhöhen. Diese Einstellung gilt nur für iOS-Geräte. Die Standardeinstellung ist **20** Stunden.

Bei sehr vielen iOS-Geräten in Ihrer Umgebung kann das Taktintervall zu einer unnötigen Erhöhung der Arbeitslast führen. Sicherheitsaktionen wie Selektives Löschen, Sperren und Vollständiges Löschen agieren unabhängig vom Heartbeat: Wenn diese Aktionen ausgeführt werden, wird eine APNs-Benachrichtigung an das Gerät gesendet. Dieser Wert legt fest, wie schnell eine Richtlinie nach Änderungen an einer Active Directory-Gruppenmitgliedschaft aktualisiert wird. Daher ist es oft sinnvoll, einen Wert zwischen 12 und 20 Stunden zu verwenden, um die Last zu reduzieren.

iOS MDM APNs - Verbindungspoolgröße

Ein zu kleiner APNs-Verbindungpool kann sich negativ auf die APNs-Aktivität auswirken, wenn Sie mehr als 100 Geräte verwenden. Auftretende Leistungsprobleme können eine langsame Bereitstellung von Apps und Richtlinien auf Geräten und eine verzögerte Geräteregistrierung sein. Die Standardeinstellung ist **1**. Wir empfehlen, diesen Wert für etwa alle 400 Geräte um 1 zu erhöhen.

auth.ldap.connect.timeout

Bei einer langsamen LDAP-Antwort empfiehlt Citrix das Hinzufügen von Servereigenschaften für den folgenden benutzerdefinierten Schlüssel.

- Schlüssel: **Benutzerdefinierter Schlüssel**
- Schlüssel: **auth.ldap.connect.timeout**
- Wert: **60000**
- Anzeigename: **auth.ldap.connect.timeout**
- Beschreibung: **Zeitlimit für LDAP-Verbindung**

auth.ldap.read.timeout

Bei einer langsamen LDAP-Antwort empfiehlt Citrix das Hinzufügen von Servereigenschaften für den folgenden benutzerdefinierten Schlüssel.

- Schlüssel: **Benutzerdefinierter Schlüssel**
- Schlüssel: **auth.ldap.read.timeout**
- Wert: **60000**
- Anzeigename: **auth.ldap.read.timeout**
- Beschreibung: **LDAP-Lesezeitlimit**

Weitere Serveroptimierungen

Servereigenschaft	Standardeinstellung	Gründe für ein Ändern dieser Einstellung
Hintergrundbereitstellung	1440 Minuten	Die Häufigkeit der Hintergrundbereitstellung von Richtlinien, in Minuten. Gilt nur für immer aktive Verbindungen bei Android-Geräten. Eine häufigere Bereitstellung von Richtlinien verringert die Serverlast. Die empfohlene Einstellung ist **1440** (24 Stunden).

Hardwareinventur im Hintergrund	1440 Minuten	Die Häufigkeit von Hardwareinventuren im Hintergrund, in Minuten. Gilt nur für immer aktive Verbindungen bei Android-Geräten. Ein häufigeres Durchführen von Hardwareinventuren verringert die Serverlast. Die empfohlene Einstellung ist **1440** (24 Stunden).
Intervall zur Suche nach gelöschten Active Directory-Benutzern	15 Minuten	Die standardmäßige Synchronisierungszeit für Active Directory ist **15** Minuten. Der Wert **0** deaktiviert in XenMobile die Suche nach gelöschten Active Directory-Benutzern. Die empfohlene Einstellung ist **15** Minuten.
MaxNumberOfWorker	3	Zahl der beim Importieren eine großen Anzahl von Volume Purchase-Lizenzen verwendeten Threads. Der Standardwert ist **3**. Ist eine weitere Optimierung erforderlich, können Sie die Zahl der Threads erhöhen. Bei einer größeren Anzahl von Threads (z. B. 6) führt ein Volume Purchase-Import jedoch zu einer hohen CPU-Auslastung.

Überprüfen von Deadlocks in einer SQL-Datenbank und Löschen von Verlaufsdaten

Bei vorhandenen Deadlocks führen Sie die folgende Abfrage aus, um die Deadlocks anzuzeigen. Anschließend kann ein Datenbankadministrator oder Microsoft SQL-Teammitglied die Informationen bestätigen.

SQL-Abfrage

```
SELECT

db.name DB_Service,

tl.request_session_id,

wt.blocking_session_id,

OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,

tl.resource_type,

h1.TEXT AS RequestingText,

h2.TEXT AS BlockingTest,

tl.request_mode

FROM sys.dm_tran_locks AS tl

INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id

INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
    resource_address

INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
    resource_associated_entity_id

INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
    request_session_id

INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
    blocking_session_id

CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1

```



```
CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2

GO
<!--NeedCopy-->
```

Bereinigen der Datenbank

> **Wichtig:**
>
> Sichern Sie Ihre Datenbank, bevor Sie Änderungen an Tabellen vornehmen.

1. Führen Sie die folgende Abfrage aus, um die Verlaufsdaten zu überprüfen.

```
select COUNT(\*) as total_record from dbo.EWDEPLOY_HISTO;
select COUNT(\*) as total_record from dbo.EWSESS;
select COUNT(*) as total_record from dbo.EWAUDIT;
<!--NeedCopy-->
```

2. Löschen Sie die Daten aus den vorangegangenen drei Tabellen.

> **Hinweis:**
>
> Unter Umständen sehen Sie keine Verlaufsdaten in einer Tabelle. Überspringen Sie in diesem Fall die TRUNCATE-Abfrage für diese spezielle Tabelle.

```
truncate TABLE dbo.EWDEPLOY_HISTO;
truncate TABLE dbo.EWSESS;
truncate TABLE dbo.EWAUDIT;
<!--NeedCopy-->
```

3. Entsperren Sie die SELECT-Abfragen, die durch die Deadlocks blockiert wurden. Dieser Schritt behebt alle weiteren Deadlocks.

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT
   ON WITH ROLLBACK IMMEDIATE
<!--NeedCopy-->
```

4. Standardmäßig erfolgt die Datenbankbereinigung alle sieben Tage für aufzubewahrende Sitzungs- und Auditprotokolldaten, deren Datenmenge bei vielen Benutzern hoch ist. Ändern Sie den Bereinigungswert in 1 oder 2 Tage. Ändern Sie die Servereigenschaften wie folgt:

```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
zdm.dbcleanup.auditRetentionTimeInDays=1 day
<!--NeedCopy-->
```


Verwaiste Einträge in der KEYSTORE-Tabelle bereinigen

Wenn XenMobile-Knoten eine schlechte Leistung zeigen, überprüfen Sie, ob die KEYSTORE-Tabelle zu groß ist. XenMobile speichert Registrierungszertifikate in den Tabellen ENROLLMENT_CERTIFICATE und KEYSTORE. Wenn Sie Geräte löschen oder neu registrieren, werden die Zertifikate in der Tabelle ENROLLMENT_CERTIFICATE gelöscht. Einträge in der KEYSTORE-Tabelle bleiben erhalten, was zu Leistungsproblemen führen kann. Führen Sie das folgende Verfahren aus, um die verwaisten Einträge aus der KEYSTORE-Tabelle zu löschen.

> **Wichtig:**
>
> Sichern Sie Ihre Datenbank, bevor Sie Änderungen an Tabellen vornehmen.

1. Führen Sie die folgende Abfrage aus, um die Verlaufsdaten zu überprüfen.

```
select COUNT(*) from KEYSTORE
<!--NeedCopy-->
```

2. Suchen Sie mit der folgenden Abfrage nach verwaisten Einträgen in der KEYSTORE-Tabelle.

```
WITH cte(KEYSTORE_ID)
AS (SELECT KEYSTORE_ID
    FROM ENROLLMENT_CERTIFICATE
    UNION
    SELECT CA_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT CLIENT_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT KEYSTORE_ID
    FROM SAML_SERVICE_PROVIDER
    UNION
    SELECT KEYSTORE_ID
    FROM SERVER_CERTIFICATE)
SELECT keystore.id
FROM keystore
    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
WHERE KEYSTORE_ID IS NULL;
<!--NeedCopy-->
```

3. Löschen Sie die verwaisten Einträge mit der folgenden Abfrage.

```
WITH cte(KEYSTORE_ID)
    AS (SELECT KEYSTORE_ID
        FROM ENROLLMENT_CERTIFICATE
```



```
        UNION
        SELECT CA_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT CLIENT_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT KEYSTORE_ID
        FROM SAML_SERVICE_PROVIDER
        UNION
        SELECT KEYSTORE_ID
        FROM SERVER_CERTIFICATE)
    DELETE FROM keystore
    WHERE id IN
    (
        SELECT keystore.id
        FROM keystore
            LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
        WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
    );
<!--NeedCopy-->
```

4. Fügen Sie der KEYSTORE-Tabelle einen Index hinzu, um die Sucheffizienz zu verbessern.

```
DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;
CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
    ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
    DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
<!--NeedCopy-->
```

Bereitstellen und Entfernen von Apps

January 5, 2022

Bei der App-Bereitstellung dreht sich alles um die App-Lebenszyklusverwaltung, d. h. um das Vorbereiten, Konfigurieren, Bereitstellen und Verwalten mobiler Apps in einer XenMobile-Umgebung. In einigen Fällen kann das Entwickeln oder Modifizieren von App-Code Teil des Bereitstellungsprozesses sein. XenMobile bietet verschiedene Tools und Prozesse für die App-Bereitstellung.

Bevor Sie den vorliegenden Artikel zur App-Bereitstellung lesen, empfehlen wir die Lektüre der folgenden Artikel:

- Apps — Benutzergemeinschaften

Wenn Sie eruiert haben, welche Art von Apps Ihr Unternehmen bereitstellen möchte, können Sie einen Prozess für die Lebenszyklusverwaltung umreißen.

Berücksichtigen Sie beim Aufstellen des Bereitstellungsprozesses die folgenden Punkte:

- **App-Profilerstellung:** Ihre Organisation beginnt möglicherweise mit einer begrenzten Anzahl von Apps. Die Zahl der Apps kann mit zunehmender Akzeptanz unter den Benutzern und einem Wachstum Ihrer Umgebung schnell steigen. Definieren Sie von Anfang an bestimmte App-Profile, um die App-Bereitstellung so einfach wie möglich zu gestalten. Über die App-Profilerstellung können Sie Apps in aus nichttechnischer Sicht logische Gruppen einteilen. Sie können beispielsweise App-Profile basierend auf den folgenden Faktoren erstellen:
  - Version: App-Version für die Nachverfolgung
  - Instanzen: mehrere Instanzen, die für unterschiedliche Benutzergruppen bereitgestellt werden, z. B. mit unterschiedlichen Zugriffsebenen
  - Plattform: iOS, Android oder Windows
  - Zielgruppe: Standardbenutzer, Abteilungen, C-Level-Führungskräfte
  - Besitz: Abteilung, der die App gehört
  - Typ: MDX, öffentlich, Web und SaaS oder Weblinks
  - Upgrade-Zyklus: wie oft die App aktualisiert wird
  - Lizenzierung: Lizenzanforderungen und Eigentumsrechte
  - MAM-SDK- oder MDX-Richtlinien: zur Anwendung von MDX-Funktionen auf Ihre mobilen Apps
  - Netzwerkzugriff: Art des Zugriffs, z. B. Secure Browse oder vollständiges VPN

    > **Hinweis:**
    > "Tunnel - Web-SSO" steht in den Einstellungen für Secure Browse. Das Verhalten ist dasselbe.

Beispiel:

Faktor	Secure Mail	E-Mail	Intern	Epic Rover
Version	10.1	10.1	X.x	X.x
Instanz	VIP	Ärzte	Klinik	Klinik
Plattform	iOS	iOS	iOS	iOS
Zielbenutzer	VIP-Benutzer	Ärzte	Klinische Benutzer	Klinische Benutzer
Besitz	IT	IT	IT	IT
Typ	MDX	MDX	Nativ	Öffentlich
Upgradezyklus	Vierteljährlich	Vierteljährlich	Jährlich	Nicht zutreffend

Faktor	Secure Mail	E-Mail	Intern	Epic Rover
Lizenzierung	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Volume Purchase
MDX-Richtlinien	Ja	Ja	Ja	Nein
Netzwerkzugriff	VPN	VPN	VPN	Öffentlich

- **App-Versionsverwaltung:** Die Pflege der App-Versionen ist ein wesentlicher Bestandteil des Bereitstellungsprozesses. Die Versionsverwaltung ist für Benutzer transparent. Sie erhalten nur Benachrichtigungen, wenn eine neue App-Version zum Download bereitsteht. Aus Ihrer Sicht ist das Überprüfen und Testen jeder App-Version in einer Umgebung außerhalb der Produktion ebenfalls wichtig, um eine Beeinträchtigung der Produktionssite zu vermeiden.

  Es ist auch wichtig zu bewerten, ob ein bestimmtes Upgrade erforderlich ist. Es gibt in der Regel zwei Arten von App-Upgrades: Eine sind kleinere Upgrades, etwa zur Korrektur eines Fehlers. Die zweite sind Hauptreleases mit umfassenderen Änderungen und Verbesserungen. In beiden Fällen sollten Sie die Versionshinweise sorgfältig lesen, um zu entscheiden, ob das Upgrade erforderlich ist.

- **App-Entwicklung:** Beim Integrieren des MAM-SDK in die von Ihnen entwickelten mobilen Apps wenden Sie MDX-Funktionen auf diese Apps an. Siehe Überblick über das MAM-SDK.

  Das MAM-SDK ersetzt das MDX Toolkit, das ab März 2022 veraltet ist. Informationen zum Umschließen von Apps finden Sie unter MDX Toolkit. Die App-Bereitstellung unterscheidet sich bei umschlossenen Apps von der Bereitstellung standardmäßiger, nicht umschlossener Apps.

- **App-Sicherheit:** Im Rahmen der Bereitstellung definieren Sie die Sicherheitsanforderungen für einzelne Apps oder App-Profile. Sie können Sicherheitsanforderungen bestimmten MDM- oder MAM-Richtlinien zuordnen, bevor Sie Apps bereitstellen. Diese Art der Planung vereinfacht und beschleunigt die App-Bereitstellung. Beispiel:

  - Sie stellen bestimmte Apps auf unterschiedliche Weise bereit.
  - Sie möchten die Architektur der XenMobile-Umgebung ändern. Die Änderungen hängen von der Art der für die Apps benötigten Sicherheitskonformität ab. Beispielsweise kann es wünschenswert sein, dass eine Business Intelligence-App nur auf verschlüsselten Geräten verwendet werden kann. Eine andere App erfordert möglicherweise Ende-zu-Ende-SSL-Verschlüsselung oder Geofencing.

- **Bereitstellungsart:** In XenMobile können Sie Apps als MDM- oder MAM-Apps bereitstellen. MDM-Apps werden im XenMobile Store angezeigt. Über diesen Store können Sie Benutzern öffentliche oder native Apps bequem bereitstellen. Die einzige von Ihnen verwaltete MDM-App-Steuerung ist die Erzwingung von Einschränkungen auf Geräteebene. Im MAM-Modus haben

Sie jedoch die vollständige Kontrolle über die App-Bereitstellung und die Apps selbst. Die Bereitstellung von Apps per MAM ist normalerweise besser geeignet.

- **Anwendungswartung:**
  - Führen Sie ein Anfangsaudit durch: Halten Sie die App-Versionen in Ihrer Produktionsumgebung sowie den letzten Upgradezyklus fest. Notieren Sie außerdem Features oder Fehlerbehebungen, für die ein Upgrade erforderlich war.
  - Legen Sie die Basislinien fest: Führen Sie eine Liste der letzten stabilen Version jeder App, um diese bei etwaigen Problemen nach einem Upgrade als Fallback zu verwenden. Entwickeln Sie außerdem einen Rollbackplan. Testen Sie App-Upgrades in einer Testumgebung, bevor Sie sie in der Produktion bereitstellen. Stellen Sie Upgrades nach Möglichkeit zunächst einer begrenzten Zahl von Benutzern in der Produktion und erst anschließend für alle Benutzer bereit.
  - Abonnieren Sie Citrix Benachrichtigungen über Softwareupdates und Benachrichtigungen von Drittanbietern. Es ist wichtig, über neue App-Versionen informiert zu bleiben. Es gibt ggf. ein EAR Build (Early Access Release) für Tests.
  - Entwickeln Sie eine Strategie zum Benachrichtigen von Benutzern über das Verfügbarwerden von App-Upgrades. Bereiten Sie Benutzer vor der Bereitstellung mit Schulungen vor. Sie können mehrere Benachrichtigungen senden, bevor Sie Apps aktualisieren. Je nach App sind E-Mail-Benachrichtigungen oder Onlinebenachrichtigungen möglicherweise die bessere Benachrichtigungsmethode.

Das App-Lebenszyklusmanagement repräsentiert den abgeschlossenen Lebenszyklus einer App von der ersten Bereitstellung bis zu ihrer Ausmusterung. Der Lebenszyklus von Apps besteht aus folgenden Phasen:

1. Anforderungen für die Spezifikation: Geschäftsszenario und Benutzeranforderungen
2. Entwicklung: Überprüfen der App auf Anforderungstauglichkeit.
3. Testen: Identifizieren von Testbenutzern, Problemen und Fehlern
4. Bereitstellung: Bereitstellen der App für die Benutzer in der Produktion
5. Wartung: Updaten der App-Version. Stellen Sie die App vor einem Update in der Produktionsumgebung in einer Testumgebung bereit.

Lebenszyklusbeispiel: Secure Mail

1. Anforderungen für die Spezifikation: Sie benötigen eine sichere E-Mail-App mit Containern, die MDX-Sicherheitsrichtlinien unterstützt.
2. Entwicklung: Überprüfen der App auf Anforderungstauglichkeit. Es muss möglich sein, MDX-Richtlinien auf die App anzuwenden.
3. Testen: Weisen Sie Secure Mail einer Gruppe von Testbenutzern zu und stellen Sie die entsprechende MDX-Datei über XenMobile Server bereit. Die Testbenutzer testen den rei-

bungslosen E-Mail-Empfang und -Versand und den Zugriff auf Kalender und Kontakte. Die Testbenutzer melden Probleme und identifizieren Fehler. Basierend auf dem Feedback der Testbenutzer optimieren Sie die Secure Mail-Konfiguration für den Einsatz in der Produktion.

4. Bereitstellung: Nach Abschluss der Testphase weisen Sie Secure Mail Produktionsbenutzern zu und stellen die entsprechende MDX-Datei über XenMobile bereit.
5. Wartung: Ein neues Update für Secure Mail ist verfügbar. Sie laden die neue MDX-Datei von Citrix Downloads herunter und ersetzen durch sie die MDX-Datei in XenMobile Server. Sie weisen die Benutzer an, das Update durchzuführen. Hinweis: Citrix empfiehlt, diesen Prozess in einer Testumgebung zu testen. Laden Sie die App dann in eine XenMobile-Produktionsumgebung hoch und stellen Sie sie für die Benutzer bereit.

Weitere Informationen finden Sie unter Umschließen von mobilen iOS-Apps und Umschließen von mobilen Android-Apps in der XenMobile-Dokumentation.

Über das Dashboard steuerbare Vorgänge

January 21, 2021

Das Dashboard der XenMobile-Konsole ermöglicht die übersichtliche Anzeige von Informationen auf einen Blick. Mit diesen Informationen können Sie Probleme und erfolgreiche Aktionen schnell mit Widgets erfassen.

Das Dashboard ist normalerweise der erste Bildschirm, der beim Anmelden an der XenMobile-Konsole angezeigt wird. Um das Dashboard von anderer Stelle aus aufzurufen, klicken Sie auf **Analysieren**. Klicken Sie im Dashboard auf **Anpassen**, um das Seitenlayout und die angezeigten Widgets zu bearbeiten.

- **Meine Dashboards:** Sie können bis zu vier Dashboards speichern. Sie können diese Dashboards separat bearbeiten und jeweils durch Auswahl des gespeicherten Dashboards anzeigen.
- **Layoutstil:** In dieser Zeile können Sie auswählen, wie viele Widgets auf dem Dashboard angezeigt und wie sie angeordnet werden.
- **Widgetauswahl:** Legen Sie fest, welche Informationen auf dem Dashboard angezeigt werden.
  - **Benachrichtigungen:** Aktivieren Sie das Kontrollkästchen über den Ziffern auf der linken Seite, um eine Benachrichtigungsleiste über den Widgets hinzuzufügen. Diese Leiste zeigt die Anzahl der richtlinientreuen Geräte, der inaktiven Geräte und der Geräte, die in den vergangenen 24 Stunden gelöscht oder registriert wurden.
  - **Geräte nach Plattform:** Anzahl der verwalteten und nicht verwalteten Geräte pro Plattform.
  - **Geräte nach Netzbetreiber:** Anzahl der verwalteten und nicht verwalteten Geräte pro Netzbetreiber. Klicken Sie auf die einzelnen Balken, um eine Aufschlüsselung nach Plattform anzuzeigen.

- **Verwaltete Geräte nach Plattform:** Anzahl der verwalteten Geräte pro Plattform.
- **Nicht verwaltete Geräte nach Plattform:** Anzahl der nicht verwalteten Geräte pro Plattform. Auf den Geräten in diesem Diagramm ist möglicherweise ein Agent installiert, ihre Privilegien wurden jedoch widerrufen oder sie wurden gelöscht.
- **Geräte nach ActiveSync-Gateway-Status:** Anzahl der Geräte gruppiert nach ActiveSync-Gateway-Status. Statusangaben werden unterteilt in "Blockiert", "Zugelassen" oder "Unbekannt". Mit einem Klick auf die einzelnen Balken können Sie die Angaben nach Plattform aufschlüsseln lassen.
- **Geräte nach Besitzer:** Anzahl der Geräte gruppiert nach Besitzerstatus. Statusangaben werden unterteilt in Unternehmens- oder Mitarbeiterbesitz oder Unbekannt.
- **Fehlerhafte Bereitstellungen von Bereitstellungsgruppen:** Gesamtzahl fehlgeschlagener Bereitstellungen pro Paket. Nur Pakete mit fehlgeschlagenen Bereitstellungen werden angezeigt.
- **Geräte nach Grund für das Blockieren:** Anzahl der Geräte, die von ActiveSync blockiert wurden.
- **Installierte Apps:** Mit diesem Widget können Sie bei Eingabe eines App-Namens ein Diagramm mit Informationen zur App anzeigen.
- **Volume Purchas Apps-Lizenznutzung:** Zeigt statistische Angaben zur Nutzung von Lizenzen für Volumen Purchase Apps von Apple.

Anwendungsfälle

Im Folgenden finden Sie einige Beispiele für die zahlreichen Einsatzmöglichkeiten für Dashboard-Widgets zum Überwachen Ihrer Umgebung.

- Sie haben mobile Produktivitätsapps bereitgestellt und erhalten Supporttickets für Fälle, in denen diese nicht installiert werden können. Verwenden Sie die Widgets **Nicht richtlinientreue Geräte** und **Installierte Apps**, um die Geräte anzuzeigen, auf denen mobile Produktivitätsapps nicht installiert sind.
- Sie möchten inaktive Geräte überwachen, sodass Sie die Geräte aus Ihrer Umgebung entfernen und Lizenzen zurückfordern können. Verwenden Sie das Widget **Inaktive Geräte**, um diese nachzuverfolgen.
- Sie erhalten Supporttickets für Daten, die nicht ordnungsgemäß synchronisiert werden. Sie können mithilfe der Widgets **Geräte nach ActiveSync-Gateway-Status** und **Geräte nach Grund für das Blockieren** feststellen, ob ein Problem mit ActiveSync zu tun hat.

Berichterstellung

Nach Einrichtung der Umgebung und Registrierung der Benutzer können Sie Berichte ausführen, um mehr über Ihre Bereitstellung zu erfahren. XenMobile enthält eine Reihe von Berichten, anhand

derer Sie sich über die Geräte in Ihrer Umgebung informieren können. Einzelheiten finden Sie unter Berichte.

> **Wichtig:**
>
> 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.

Unterstützung für die rollenbasierte Zugriffssteuerung in XenMobile

January 5, 2022

In XenMobile wird der Benutzer- und Gruppenzugriff auf XenMobile-Systemfunktionen (z. B. XenMobile-Konsole, Remotesupport, öffentliche API) über die rollenbasierte Zugriffssteuerung (RBAC) beschränkt. In diesem Artikel werden die in XenMobile integrierten Rollen und Überlegungen zur Wahl eines XenMobile-Supportmodells, für das RBAC verwendet wird, beschrieben.

> **Hinweis:**
>
> Remote Support ist ab dem 1. Januar 2019 für Neukunden nicht mehr verfügbar. Bestehende Kunden können das Produkt weiterhin verwenden, Citrix stellt jedoch keine Neuerungen oder Fixes bereit.

Integrierte Rollen

Sie können den Zugriff für die folgenden integrierten Rollen ändern und Rollen hinzufügen. Informationen zum vollständigen Satz von Zugriffs- und Featureberechtigungen der Rollen und zu deren Standardeinstellung finden Sie in Role-Based Access Control Defaults (Download) in der XenMobile-Dokumentation. Eine Definition der einzelnen Features finden Sie unter Konfigurieren von Rollen mit RBAC in der XenMobile-Dokumentation.

Administratorrolle

Standardzugriff:

- Vollzugriff auf das System mit Ausnahme des Remotesupports.
- Standardmäßig können Administratoren einige Supportaufgaben ausführen, z. B. Verbindungsprüfungen oder Supportpaketerstellung.

Überlegungen:

- Benötigen einige oder alle Administratoren Zugriff auf den Remotesupport? Wenn dies der Fall ist, können Sie die Administratorrolle bearbeiten oder Administratorrollen hinzufügen.
- Zum weiteren Einschränken des Zugriffs für einige Administratoren oder Administratorgruppen fügen Sie Rollen basierend auf Admin-Vorlage hinzu und bearbeiten Sie die Berechtigungen.

Geräteprovisioning

Standardzugriff:

- Zugriff auf die XenMobile-Konsole für die grundlegende Verwaltung von Windows CE-Geräten: Hinzufügen, Ändern und Entfernen von Geräten, Verwenden der Seite "Einstellungen".

Überlegungen:

- Gilt nur für Windows CE-Geräte.

Support

Standardzugriff:

- Zugriff auf Remotesupport.

Überlegungen:

- Für on-premises XenMobile Server-Bereitstellungen: Durch Remotesupport können Helpdesk-Mitarbeiter die Fernsteuerung verwalteter Windows CE- und Android-Mobilgeräte übernehmen. Screencast wird nur auf Samsung KNOX-Geräten unterstützt.
- Remotesupport ist nicht für geclusterte on-premises XenMobile Server-Bereitstellungen verfügbar.

Benutzer

Standardzugriff:

- Eingeschränkter Zugriff auf die XenMobile-Konsole: Gerätefunktionen (z. B. Löschen, Sperren/Entsperren von Geräten, Sperren/Entsperren von Containern, Ortung und Festlegen geografischer Einschränkungen, Anrufen von Geräten, Zurücksetzen des Containerkennworts), Hinzufügen, Entfernen und Senden von Registrierungseinladungen.

Überlegungen:

- Mit der Benutzerrolle können Sie Benutzern die Selbsthilfe ermöglichen.
- Um gemeinsam genutzte Geräte zu unterstützen, erstellen Sie eine Benutzerrolle für die Registrierung gemeinsam genutzter Geräte.

Überlegungen zum XenMobile-Supportmodell

Sie können sehr unterschiedliche Supportmodelle verwenden und bei Bedarf Level 1 und 2 an Drittanbieter übergeben, während Ihre Mitarbeiter Level 3 und 4 handhaben. Unabhängig von der Verteilung der Supportaufgaben sollten Sie die in diesem Abschnitt für Ihre spezifische XenMobile-Bereitstellung und Ihren spezifischen Benutzerstamm aufgeführten Überlegungen berücksichtigen.

Haben Benutzer unternehmenseigene oder BYO-Geräte?
Die wichtigste Frage für den Support ist die, wem die Benutzergeräte in der XenMobile-Umgebung gehören. Wenn die Benutzer firmeneigene Geräte verwenden, können Sie sich evtl. durch Angebot einer niedrigeren Supportstufe eine Möglichkeit der Gerätesperrung schaffen. In diesem Fall helfen Sie den Benutzern möglicherweise über einen Helpdesk bei der Verwendung der Geräte und bei Problemen. Überlegen Sie abhängig von der Art der betreuten Geräte, wie Sie die Rollen zum RBAC-Geräteprovisioning und für den Support für Ihren Helpdesk verwenden.

Wenn die Benutzer BYOD-Geräte verwenden, wird von ihnen möglicherweise erwartet, dass sie eigene Supportquellen finden. In diesem Fall hat Ihr Support eher administrative, auf XenMobile-spezifische Probleme konzentrierte Aufgaben.

Was ist Ihr Supportmodell für Desktops?
Überlegen Sie, ob Ihr Desktop-Supportmodell für andere unternehmenseigene Geräte geeignet ist. Können Sie dieselbe Supportorganisation nutzen? Welche zusätzliche Schulung ist erforderlich?

Sollen Benutzer Zugriff auf das XenMobile-Selbsthilfeportal erhalten?
Über **Einstellungen > Registrierung** können Sie das Selbsthilfeportal für einen Registrierungssicherheitsmodus aktivieren. Im Selbsthilfeportal generieren Benutzer nach der Anmeldung Registrierungslinks, mit denen sie ihre Geräte registrieren können. Alternativ können sie eine Registrierungseinladung an das eigene E-Mail-Konto senden. Siehe Konfigurieren von Registrierungssicherheitsmodi.

Systemüberwachung

January 5, 2022

Zur Gewährleistung einer optimalen Verfügbarkeit für App-Zugriff und Konnektivität sollten Sie die folgenden Kernkomponenten in der XenMobile-Umgebung überwachen.

XenMobile Server

Der XenMobile-Server generiert und speichert lokal Protokolle, die Sie auf einen Systemprotokollserver (Syslog-Server) exportieren können. Sie können Protokolleinstellungen für

Größenbeschränkungen oder Protokollebenen konfigurieren und benutzerdefinierte Protokollfunktionen zum Filtern bestimmter Ereignisse erstellen. Die XenMobile-Serverprotokolle können Sie jederzeit über die XenMobile-Konsole anzeigen. Sie können den Protokollinhalt außerdem über den Syslog-Server auf Ihre Splunk-Protokollserver in der Produktion exportieren.

Nachfolgend werden die verschiedenen Arten von Protokolldateien in XenMobile beschrieben.

Debugprotokoll: enthält Debuginformationen zu zentralen Webdiensten von XenMobile mit Fehlermeldungen und serverbezogenen Aktionen.

Meldungsformat:

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <
log message>
```

- <id> ist ein eindeutiger Bezeichner wie “sessionID”.
- <log message> ist die von der Anwendung erhaltene Meldung.

Administratorüberwachungsprotokolle: enthalten Auditinformationen über Aktivitäten in der XenMobile-Konsole.

> **Hinweis:**
>
> Dasselbe Format wird für das Administrator- und das Benutzerüberwachungsprotokoll verwendet.

Meldungsformat:

Mit Ausnahme von Datums- und Zeitstempel sind alle Attribute optional. Optionale Felder werden in der Meldung durch “ “ gekennzeichnet.

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

In der folgenden Tabelle werden die möglichen Überwachungsprotokollereignisse aufgeführt:

Ereignismeldungen im Administratorüberwachungsprotokoll	Status
Login	success/failure
Logout	success/failure
Get admin	success/failure
Update admin	success/failure
Get application	success/failure
Add application	success/failure

Ereignismeldungen im Administratorüberwachungsprotokoll	Status
Update application	success/failure
Delete application	success/failure
Bind application	success/failure
Unbind application	success/failure
Disable application	success/failure
Enable application	success/failure
Get category	success/failure
Add category	success/failure
Update category	success/failure
Delete category	success/failure
Add certificate	success/failure
Delete certificate	success/failure
Active certificate	success/failure
CSR certificate	success/failure
Export certificate	success/failure
Delete certificate chain	success/failure
Add certificate chain	success/failure
Get connector	success/failure
Add connector	success/failure
Delete connector	success/failure
Update connector	success/failure
Get device	success/failure
Lock device	success/failure
Unlock device	success/failure
Wipe device	success/failure
Unwipe device	success/failure
Delete device	success/failure
Get role	success/failure

Ereignismeldungen im Administratorüberwachungsprotokoll	Status
Add role	success/failure
Update role	success/failure
Delete role	success/failure
Bind role	success/failure
Unbind role	success/failure
Update config settings	success/failure
Update workflow email	success/failure
Add workflow	success/failure
Delete workflow	success/failure
Add Active Directory	success/failure
Update Active Directory	success/failure
Add masteruserlist	success/failure
Update masteruserlist	success/failure
Update DNS	success/failure
Update Network	success/failure
Update log server	success/failure
Transfer log from log server	success/failure
Update syslog	success/failure
Update receiver updates	success/failure
Update time server	success/failure
Update trust	success/failure
Add service record	success/failure
Update service record	success/failure
Update receiver email	success/failure
Upload patch	success/failure
Import snapshot	success/failure
Fetch app store app details	success/failure
Update MDM	success/failure

Ereignismeldungen im Administratorüberwachungsprotokoll	Status
Delete MDM	success/failure
Add HDX	success/failure
Update HDX	success/failure
Delete HDX	success/failure
Add Branding	success/failure
Delete Branding	success/failure
Update SSL offload	success/failure
Add account property	success/failure
Delete account property	success/failure
Update account property	success/failure
Add beacon	success/failure

Benutzerüberwachungsprotokoll: enthält Informationen zu Benutzeraktivitäten auf registrierten Geräten.

> **Hinweis:**
>
> Dasselbe Format wird für das Benutzer- und das Administratorüberwachungsprotokoll verwendet.

Meldungsformat:

Mit Ausnahme von Datums- und Zeitstempel sind alle Attribute optional. Optionale Felder werden in der Meldung durch “ “ gekennzeichnet. Zum Beispiel:

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

In der folgenden Tabelle werden die möglichen Überwachungsprotokollereignisse aufgeführt:

Ereignismeldungen im Benutzerüberwachungsprotokoll	Status
Login	success/failure
Session time-out	success/failure
Subscribe	success/failure

Ereignismeldungen im Benutzerüberwachungsprotokoll	Status
Unsubscribe	success/failure
Pre-launch	success/failure
AGEE SSO	success/failure
SAML Token for Citrix Files	success/failure
Device registration	success/failure
Device check	lock/wipe
Device update	success/failure
Token refresh	success/failure
Secret saved	success/failure
Secret retrieved	success/failure
User initiated change password	success/failure
Mobile client download	success/failure
Logout	success/failure
Discovery Service	success/failure
Endpoint Service	success/failure

MDM-Funktionen	Status
REGHIVE	success/failure
Cab inventory	success/failure
Cab	success/failure
Cab auto install	success/failure
Cab shell install	success/failure
Cab create folder	success/failure
Cab file get	success/failure
File create folder	success/failure
File get	success/failure
File sent	success/failure
Script create folder	success/failure

MDM-Funktionen	Status
Script get	success/failure
Script sent	success/failure
Script shell execution	success/failure
Script auto execution	success/failure
APK inventory	success/failure
APK	success/failure
APK shell install	success/failure
APK auto install	success/failure
APK create folder	success/failure
APK file get	success/failure
APK App	success/failure
EXT App	success/failure
List get	success/failure
List sent	success/failure
Locate device	success/failure
CFG	success/failure
Unlock	success/failure
SharePoint wipe	success/failure
SharePoint Configuration	success/failure
Remove profile	success/failure
Remove application	success/failure
Remove unmanaged application	success/failure
Remove unmanaged profile	success/failure
IPA App	success/failure
EXT App	success/failure
Apply redemption code	success/failure
Apply settings	success/failure
Enable tracking device	success/failure
App management policy	success/failure

MDM-Funktionen	Status
SD card wipe	success/failure
Encrypted email attachment	success/failure
Branding	success/failure
Secure browser	success/failure
Container browser	success/failure
Container unlock	success/failure
Container password reset	success/failure
AG client auth creds	success/failure

Citrix ADC überwacht auch den Status des XenMobile-Webdiensts, der mit intelligenten Überwachungstestern konfiguriert ist, um HTTP-Anforderungen an jeden Knoten im XenMobile-Servercluster zu simulieren. Die Tester ermitteln, ob der Dienst online ist und antworten dann basierend auf der empfangenen Antwort. Antwortet ein Knoten nicht wie erwartet, markiert Citrix ADC den Server als inaktiv. Darüber hinaus entfernt Citrix ADC den Knoten aus dem Lastausgleichspool und protokolliert das Ereignis für die Generierung von Warnungen über die Citrix ADC-Überwachungslösung.

Sie können die virtuellen XenMobile-Maschinen auch mithilfe der normalen Hypervisortools überwachen und relevante Warnungen zu CPU-, RAM- und Speicherauslastungskennzahlen generieren.

SQL Server und SQL-Datenbank

Die Leistung von SQL Server und SQL-Datenbank wirkt sich direkt auf XenMobile-Dienste aus. Die XenMobile-Instanz benötigt jederzeit Zugriff auf die Datenbank und geht bei einem Ausfall der SQL-Infrastruktur offline (z. B. reagiert sie nicht mehr). Die XenMobile-Konsole funktioniert nach dem Auftreten von Speicherplatzproblemen bei SQL Server möglicherweise noch eine Weile weiter. Um eine maximale Verfügbarkeit der Datenbank und eine angemessene Leistung für die XenMobile-Workload zu gewährleisten, sollten Sie den Status von SQL Server proaktiv überwachen. Weitere Informationen zur Überwachung Ihrer SQL Server finden Sie unter Monitoring and Tuning for Performance Overview. Darüber hinaus sollten Sie die Ressourcenzuweisung für CPU, RAM und Speicher bei einem Wachstum Ihrer XenMobile-Umgebung anpassen, damit Service Level Agreements weiter erfüllt werden.

Citrix ADC

Mit Citrix ADC können Sie Kennzahlen im internen Speicher protokollieren oder Protokolle an einen externen Protokollserver senden. Sie können außerdem den Syslog-Server konfigurieren, damit Citrix ADC-Protokkolle auf Ihre Splunk-Protokollserver in der Produktion exportiert werden. Die folgenden Protokollebenen sind in Citrix ADC verfügbar:

- Notfall
- Warnung
- Kritisch
- Fehler
- Warnung
- Information

Die Protokolldateien werden im Citrix ADC-Speicher im Verzeichnis /var/log/ns.log unter dem Namen "newnslog" gespeichert. In Citrix ADC wird das Rollover und die Komprimierung der Dateien mit dem GZIP-Algorithmus durchgeführt. Die Dateinamen lauten "newnslog.xx.gz", wobei xx eine laufende Nummer ist.

Citrix ADC unterstützt auch SNMP-Traps und Warnungen als Überwachungsoption. Eine Liste der SNMP-Traps finden Sie unter SNMP-Überwachung.

Notfallwiederherstellung

January 5, 2022

Sie können XenMobile-Bereitstellungen mit mehreren Sites für die Notfallwiederherstellung und einer Aktiv-Passive-Failoverstrategie einrichten.

Die hier vorgestellte Strategie zur Notfallwiederherstellung umfasst Folgendes:

- Eine aktive XenMobile-Site im Datencenter eines geografischen Standorts, die von allen Benutzer des Unternehmens weltweit genutzt wird. Dies ist die "primäre Site".
- Eine zweite XenMobile-Site im Datencenter eines zweiten geografischen Standorts, der "Notfallwiederherstellungssite". Die Notfallwiederherstellungssite bietet aktiv-passives Sitefailover, wenn das Datencenter der primären Site ausfällt. Die primäre Site umfasst XenMobile, die SQL-Datenbank und die Citrix ADC-Infrastruktur zur Erleichterung des Failovers und damit die Benutzer bei einem Ausfall der Verbindung mit der primären Site Zugriff auf XenMobile haben.

Die XenMobile-Server der Notfallwiederherstellungssite sind im Normalbetrieb offline und werden nur online geschaltet, wenn ein vollständiges Sitefailover von der primären Site zur Notfallwiederherstellungssite erforderlich ist. Die SQL-Server der Notfallwiederherstellungssite müssen aktiv und verbindungsbereit sein, bevor Sie die XenMobile-Server der Site starten.

Diese Notfallwiederherstellungsstrategie basiert auf einem manuellen Failover der Citrix ADC-Zugriffsebene mittels DNS-Änderungen für das Routing von MDM- und MAM-Verbindungen zur Notfallwiederherstellungssite bei einem Ausfall.

> **Hinweis:**
>
> Die Verwendung dieser Architektur erfordert einen Prozess für asynchrone Sicherungen der Datenbanken sowie eine Methode zur Gewährleistung der hohen Verfügbarkeit der SQL-Infrastruktur.

Prozess der Notfallwiederherstellung

1. Zum Testen des Failovers zur Notfallwiederherstellung fahren Sie die XenMobile-Server der primären Site herunter, um einen Siteausfall zu simulieren.
2. Ändern Sie die öffentlichen DNS-Einträge der XenMobile-Server sodass sie auf die externen IP-Adressen der Notfallwiederherstellungssite verweisen.
3. Ändern Sie den internen DNS-Eintrag für den SQL-Server sodass er auf die IP-Adresse des SQL-Servers der Notfallwiederherstellungssite verweist.
4. Schalten Sie die XenMobile-SQL-Datenbanken der Notfallwiederherstellungssite online. Stellen Sie sicher, dass SQL-Server und -Datenbank aktiv sind und Verbindungen von den lokalen XenMobile-Servern bedienen können.
5. Fahren Sie die XenMobile-Server der Notfallwiederherstellungssite hoch.

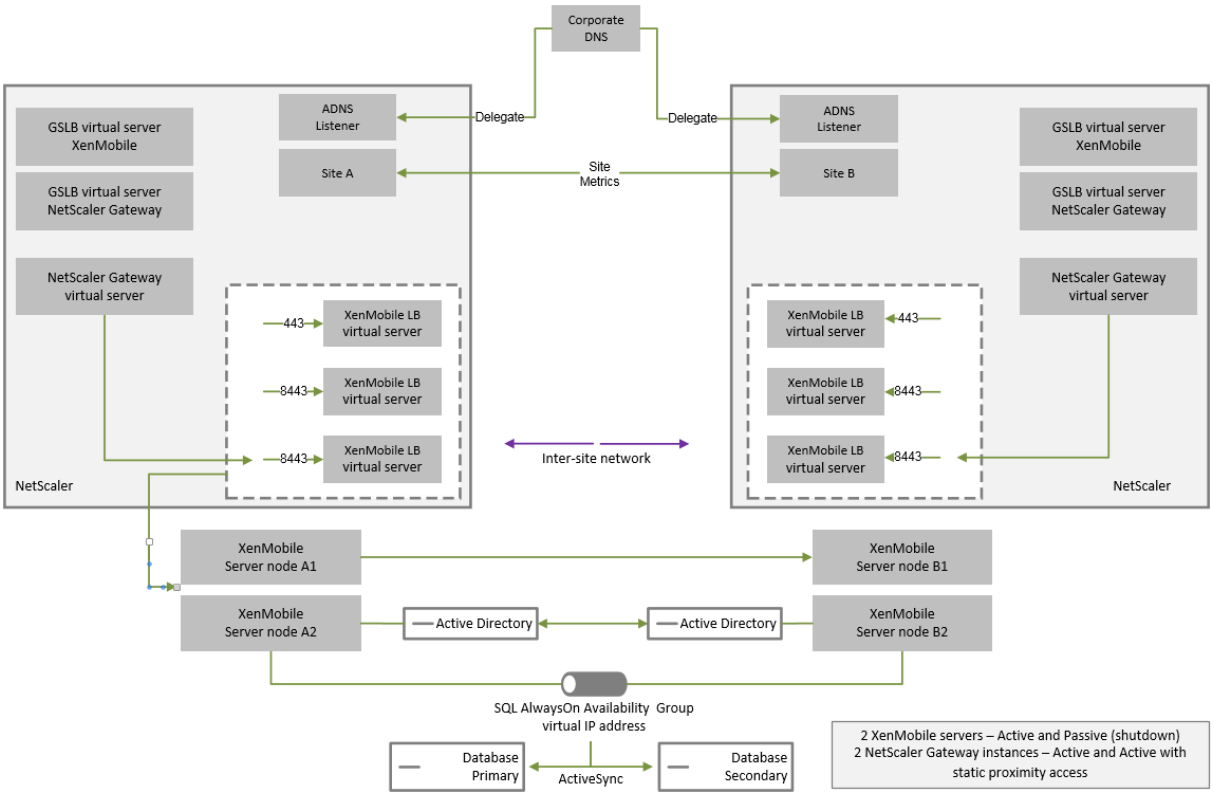
XenMobile Server-Updates

Führen Sie die nachfolgend aufgeführten Schritte bei jedem Update von XenMobile mit Patches und Releases aus, damit der Code der Server der primären Site und der Notfallwiederherstellungssite einheitlich bleibt.

1. Stellen Sie sicher, dass die XenMobile-Server der primären Site aktualisiert wurden.
2. Stellen Sie sicher, dass der DNS-Eintrag des SQL-Servers in die aktive SQL-Server-Datenbank der primären Site aufgelöst wird.
3. Schalten Sie die XenMobile-Server der Notfallwiederherstellungssite online. Die Server stellen nur während des Upgrades eine Verbindung über das WAN zur Datenbank der primären Site her.
4. Wenden Sie die erforderlichen Patches und Updates auf alle XenMobile-Server der Notfallwiederherstellungssite an.
5. Starten Sie die XenMobile-Server neu und vergewissern Sie sich, dass das Upgrade erfolgreich war.

Diagramm der Referenzarchitektur für die Notfallwiederherstellung

Das folgende Diagramm zeigt eine Referenzarchitektur zur Notfallwiederherstellung bei XenMobile.



GSLB für die Notfallwiederherstellung

Ein Schlüsselelement dieser Architektur ist die Verwendung von Global Server Load Balancing (GSLB), um den Datenverkehr zum richtigen Datencenter zu leiten.

Standardmäßig aktiviert der Citrix ADC für XenMobile-Assistent in Citrix Gateway GSLB nicht für die Notfallwiederherstellung. Daher müssen Sie zusätzliche Schritte ausführen.

Funktionsweise von GSLB

GSLB ist im Prinzip eine Art DNS. Teilnehmende Citrix ADC-Geräte agieren als autorisierende DNS-Server und lösen DNS-Einträge in die richtige IP-Adresse auf (normalerweise in die VIP, die Datenverkehr empfangen soll). Das Citrix ADC-Gerät überprüft den Systemzustand, bevor es auf eine DNS-Abfrage reagiert, die den Datenverkehr zu diesem System leitet.

Nach der Auflösung für einen Datensatz ist die Aufgabe des GSLB erledigt. Der Client kommuniziert direkt mit der VIP des Ziels. Das Verhalten des DNS-Clients spielt eine wichtige Rolle dafür, wie und wann ein Datensatz abläuft. Dies übersteigt die Grenzen des Citrix ADC-Systems. Daher unterliegt GSLB denselben Einschränkungen wie die DNS-Namensauflösung. Bei Clients werden Antworten im Cache abgelegt. Ein Lastenausgleich ist somit nicht so schnell wie der herkömmliche Lastenausgleich.

Die Aufgabe der GSLB-Konfiguration auf dem Citrix ADC, einschließlich Sites, Diensten und Monitoren, ist die korrekte DNS-Namensauflösung.

Die eigentliche Konfiguration für das Veröffentlichen von Servern (in diesem Szenario die vom Citrix ADC für XenMobile-Assistenten erstellte Konfiguration) ist nicht vom GSLB betroffen. GSLB ist ein eigener Dienst auf dem Citrix ADC.

Herausforderungen bei der Delegierung von Domänen bei Verwendung von GSLB für XenMobile

Der Citrix ADC für XenMobile-Assistent konfiguriert Citrix Gateway für XenMobile. Der Assistent generiert drei virtuelle Lastausgleichsserver und einen virtuellen Citrix Gateway-Server.

Zwei der virtuellen Lastausgleichsserver verarbeiten den MDM-Datenverkehr an Port 443 und 8443. Citrix Gateway empfängt MAM-Datenverkehr und leitet ihn an den dritten Server, den virtuellen MAM-Lastausgleichsserver an Port 8443 weiter. Der gesamte Datenverkehr zum virtuellen MAM-Lastausgleichsserver wird über Citrix Gateway übertragen.

Der virtuelle MAM-Lastausgleichsserver erfordert dasselbe SSL-Zertifikat wie die XenMobile-Server und verwendet den gleichen FQDN wie für die Registrierung von Geräten. Der MAM-Lastausgleichsserver verwendet auch denselben Port (8443) wie einer der MDM-Lastenausgleichsserver. Damit der Datenverkehr aufgelöst werden kann, erstellt der Citrix ADC für XenMobile-Assistent einen lokalen DNS-Eintrag in Citrix Gateway. Der DNS-Eintrag entspricht dem zum Registrieren von Geräten verwendeten FQDN.

Diese Konfiguration ist wirksam, wenn die XenMobile-Server-URL keine GSLB-Domänen-URL ist. Wenn eine GSLB-Domänen-URL als URL des XenMobile-Servers verwendet wird – was für die Notfallwiederherstellung erforderlich ist – verhindert der lokale DNS-Eintrag, dass Citrix Gateway Datenverkehr an die MDM-Lastausgleichsserver auflöst.

Verwenden der CNAME-Methode für die GSLB-Notfallwiederherstellung

Zur Bewältigung der Herausforderungen der vom Citrix ADC für XenMobile-Assistenten erstellten Standardkonfiguration können Sie in der übergeordneten Domäne einen CNAME-Eintrag für den FQDN des XenMobile-Servers erstellen (`company.com`) und auf einen Datensatz in der delegierten Unterzone verweisen (`gslb.company.com`), für die der Citrix ADC zuständig ist. Dies ermöglicht die Erstellung des statischen DNS-A-Eintrags für die MAM-Lastausgleichs-VIP, die zum Auflösen des Datenverkehrs benötigt wird.

1. Erstellen Sie im externen DNS einen CNAME für den FQDN des XenMobile-Servers, der auf den GSLB-Domänen-FQDN von Citrix ADC-GSLB verweist. Sie benötigen zwei GSLB-Domänen: eine für MDM-Verkehr und eine weitere für MAM-Verkehr (Citrix Gateway).

   Beispiel:


```
CNAME = xms.company.com IN CNAME xms.gslb.comany.com
```

2. Erstellen Sie in der Citrix Gateway-Instanz jeder Site einen virtuellen GSLB-Server mit einem FQDN, auf den der CNAME-Eintrag verweist.

   Beispiel:

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   Wenn Sie Citrix Gateway mit dem Citrix ADC für XenMobile-Assistenten bereitstellen, verwenden Sie beim Konfigurieren des MAM-Lastenausgleichsservers die URL des XenMobile-Servers. Dabei wird ein statischer DNS-A-Eintrag für die URL des XenMobile-Servers erstellt.

3. Führen Sie Tests mit Clients aus, die sich unter Einsatz der URL des XenMobile-Servers (`xms.company.com`) bei Secure Hub registrieren.

   In diesem Beispiel werden die folgenden FQDNs verwendet:

   - `xms.company.com` ist die URL, die vom MDM-Datenverkehr und von Geräten bei der Registrierung verwendet wird und die im vorliegenden Beispiel mit dem Citrix ADC für XenMobile-Assistenten konfiguriert wird.
   - `xms.gslb.company.com` ist der FQDN der GSLB-Domäne für den XenMobile-Server.

Citrix Support-Prozesse

January 5, 2022

Wenden Sie sich an den Technischen Support von Citrix, um Hilfe bei Problemen mit Citrix Produkten zu erhalten. Die Gruppe bietet Lösungen und Workarounds und arbeitet Hand in Hand mit erfahrenen Entwicklerteams.

Citrix Consulting Services oder Citrix Education Services bieten Produktschulungen und Empfehlungen zur Nutzung, Konfiguration und Installation von Produkten sowie zur Planung und Architektur von Umgebungen.

Citrix Consulting unterstützt Sie bei der Planung und Umsetzung von Citrix Projekten, zum Beispiel mit Machbarkeitsstudien und Infrastrukturprüfungen, einer Analyse der wirtschaftlichen Folgen und der Designanforderungen, der Prüfung und Integration des Architekturdesigns und einer anschließenden Prozessentwicklung.

Citrix Education bietet ausgezeichnete Schulungs- und Zertifizierungsprogramme zur Citrix Virtualisierung sowie zu Cloudanwendungen und Netzwerktechnologien.

Citrix empfiehlt, dass Sie zunächst die Selbsthilferessourcen von Citrix ausschöpfen, bevor Sie einen Supportfall erstellen. Zur Verfügung stehen Artikel und Mitteilungen von Citrix IT-Fachleuten, die Produktdokumentation mit Citrix Lösungen und Technologien und andere Infoseiten mit dem Neuesten

aus der Führungsetage sowie von Produktteams und Technikexperten. Besuchen Sie das Knowledge Center, die Produktdokumentation und die Blogs.

Sie können sich auch an Diskussionsforen beteiligen, wo Sie praxisorientierte Antworten von anderen Kunden erhalten, in Benutzergruppen oder Interessengruppen Ideen, Meinungen, technische Informationen und bewährte Verfahren diskutieren können oder die Citrix Supporttechniker erreichen, die in den sozialen Netzwerken die Citrix Supportsites betreiben. Besuchen Sie die Supportforen und die Website der Citrix Community.

Ebenfalls zur Verfügung stehen Schulungen und Zertifizierungskurse, mit denen Sie Ihre Kenntnisse weiter vertiefen können. Weitere Informationen finden Sie unter Citrix Education.

Citrix Insight Services ist eine praktische Onlineplattform zur Problembehandlung und Integritätsprüfung für Ihre Citrix Umgebung. Verfügbar für XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor und Citrix Gateway. Weitere Informationen finden Sie unter Analysetool.

Um den technischen Support zu erreichen, können Sie telefonisch oder per Internet einen Supportfall erstellen. Nutzen Sie bei leichten oder mittelschweren Problemen das Internet, während sich bei Problemen mit hohem Schweregrad ein Anruf empfiehlt. Hinweise zur Kontaktaufnahme bei Problemen mit XenMobile finden Sie unter How to Contact Support.

Wenn Sie einen erfahrenen Spezialisten als ständigen Ansprechpartner wünschen, kann Citrix Services Ihnen einen Technical Relationship Manager vermitteln. Weitere Informationen zu den Angeboten und Vorteilen von Citrix Services finden Sie im Worldwide Support Services Guide.

Senden von Registrierungseinladungen an Gruppen in XenMobile

September 24, 2021

Beitrag von John Bartel III

In XenMobile Server können Sie Registrierungseinladungen an Gruppen und verschachtelte Gruppen senden. Registrierungseinladungen sind für Windows-Geräte nicht verfügbar.

Beim Einrichten der Gruppeneinladung können Sie eine oder mehrere Geräteplattformen angeben. Sie können Geräte auch kennzeichnen, um beispielsweise zwischen Unternehmensgeräten und Privatgeräten zu unterscheiden. Legen Sie anschließend den Authentifizierungstyp für Benutzergeräte fest.

> **Hinweis:**
>
> Wenn Sie benutzerdefinierte Benachrichtigungsvorlagen verwenden möchten, müssen Sie diese vor dem Konfigurieren der Registrierungssicherheitsmodi erstellen. Weitere Informationen über Benachrichtigungsvorlagen finden Sie unter Erstellen und Aktualisieren von

> Benachrichtigungsvorlagen.

Weitere Informationen zur Grundkonfiguration von Benutzerkonten, Rollen, Registrierungssicherheitsmodi und Einladungen finden Sie unter Benutzerkonten, Rollen und Registrierung.

Allgemeine Schritte

1. Gehen Sie in der XenMobile-Konsole zu **Verwalten > Registrierungseinladungen**.
2. Klicken Sie links oben im Bildschirm auf **Hinzufügen** und klicken Sie auf **Einladung hinzufügen**.
3. Klicken Sie im Menü **Empfänger** auf **Gruppe**.

   Dadurch können Sie eine oder mehrere Plattformen auswählen. Wenn Sie diverse Betriebssysteme im Unternehmen verwenden, wählen Sie alle Plattformen. Löschen Sie die Plattformauswahl nur dann, wenn Sie sicher sind, dass kein Benutzer eine bestimmte Plattform verwendet.
4. Sie können Geräte während der Einladung mit Tags kennzeichnen. Wählen Sie **Unternehmen** oder **Mitarbeiter**.

   Das Verwenden von Tags erleichtert das Trennen von Unternehmens- und Privatgeräten.
5. Wählen Sie in der Liste **Domäne** die Domäne, in der sich die Gruppe befindet.
6. Wählen Sie in der Liste **Gruppe** die Active Directory-Gruppe, an die Sie die Einladungen senden möchten.
7. Unter **Registrierungsmodus** können Sie den bevorzugten Authentifizierungssicherheitstyp für Benutzer festlegen.

   - Benutzername + Kennwort
   - Hohe Sicherheit
   - Einladungs-URL
   - Einladungs-URL + PIN
   - Einladungs-URL + Kennwort
   - Zweistufig
   - Benutzername + PIN

   > **Hinweis:**
   >
   > Um Registrierungseinladungen zu senden, können Sie nur die Registrierungsicherheitsmodi **Einladungs-URL**, **Einladungs-URL + PIN** oder **Einladungs-URL + Kennwort** verwenden. Für Geräte, die mit **Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** registriert werden, müssen Benutzer ihre Anmeldeinformationen manuell in Secure Hub eingeben.

8. Wählen Sie für die Vorlagen **Agentdownload**, **Registrierungs-URL**, **Registrierungs-PIN** und **Registrierungsbestätigung** die benutzerdefinierte Benachrichtigungsvorlage aus, die Sie im Voraus erstellt haben. Alternativ können Sie auch die angezeigte Standardvorlage verwenden.

   Wenn Sie benutzerdefinierte Benachrichtigungsvorlagen verwenden möchten, müssen Sie diese vor dem Konfigurieren der Registrierungssicherheitsmodi erstellen. Weitere Informationen zu Benachrichtigungsvorlagen finden Sie unter Benachrichtigungen.

   Verwenden Sie für diese Benachrichtigungsvorlagen den konfigurierten SMTP-Server in XenMobile. Legen Sie die SMTP-Einstellungen fest, bevor Sie fortfahren.

   > **Hinweis:**
   >
   > Die Optionen **Ablauf nach** und **Versuche maximal** ändern sich je nach gewähltem **Registrierungsmodus**. Sie können diese Optionen nicht ändern.

9. Setzen Sie **Einladung senden** auf “Ein” und klicken Sie auf **Speichern und senden**, um den Vorgang abzuschließen.

Unterstützung für verschachtelte Gruppen

Sie können verschachtelte Gruppen verwenden, um Einladungen zu senden. Normalerweise werden verschachtelte Gruppen in großen Umgebungen verwendet, in denen Gruppen mit ähnlichen Berechtigungen miteinander verbunden sind.

Navigieren Sie zu **Einstellungen > LDAP** und aktivieren Sie die Option **Verschachtelte Gruppen unterstützen**.

Problembehandlung und bekannte Einschränkungen

Problem: Einladungen werden an Benutzer gesendet, obwohl diese aus einer Active Directory-Gruppe entfernt wurden.

Lösung: Je nach Größe Ihrer Active Directory-Umgebung kann es bis zu sechs Stunden dauern, bis Änderungen auf alle Server verteilt wurden. Wenn ein Benutzer oder eine verschachtelte Gruppe erst vor kurzem entfernt wurde, kann XenMobile diese Benutzer weiterhin als Teil der Gruppe betrachten.

Es empfiehlt sich daher, bis zu sechs Stunden zu warten, bevor Sie eine neue Gruppeneinladung an die Gruppe senden.

Konfigurieren eines on-premises DHA-Servers zum Nachweis der Geräteintegrität

January 5, 2022

Beitrag von Sanket Mishra

Sie können Device Health Attestation (DHA) für Windows 10- und Windows 11-Mobilgeräte über einen On-Premises-Windows-Server aktivieren. Um DHA on-premises zu aktivieren, konfigurieren Sie zunächst einen DHA-Server.

Nach dem Konfigurieren des DHA-Servers erstellen Sie eine XenMobile Server-Richtlinie, um den DHA-Dienst on-premises zu aktivieren. Informationen zum Erstellen dieser Richtlinie finden Sie unter Geräterichtlinie für Device Health Attestation.

Voraussetzungen für einen DHA-Server

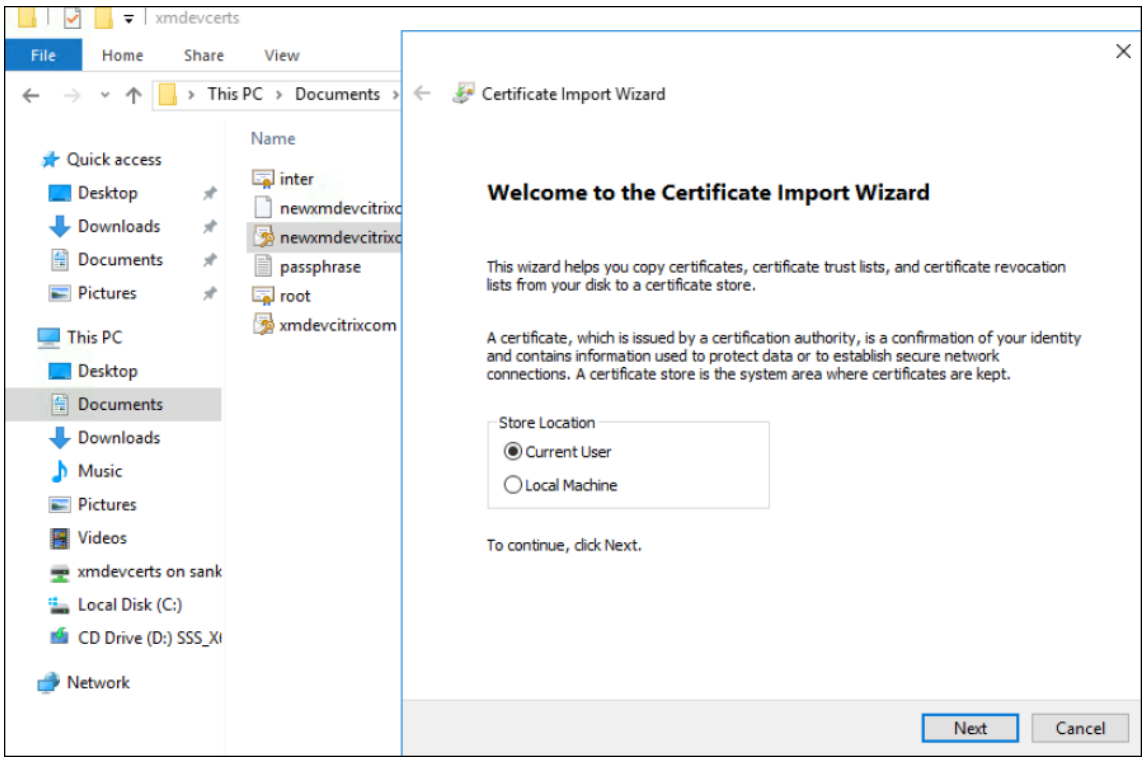
- Ein Server mit Windows Server Technical Preview 5 oder höher, installiert mit Installationsoption Desktop Experience.
- Ein oder mehrere Clientgeräte mit Windows 10 und Windows 11. Auf diesen Geräten muss TPM 1.2 oder 2.0 mit der aktuellen Version von Windows installiert sein.
- Folgende Zertifikate:
  - **DHA-SSL-Zertifikat.** Ein x.509-SSL-Zertifikat in einer Kette mit einem vertrauenswürdigen Unternehmensstammzertifikat mit exportierbarem privatem Schlüssel. Dieses Zertifikat schützt die DHA-Datenkommunikation in der Übertragung, darunter die Kommunikation von Server zu Server (DHA-Service und MDM-Server) und von Server zu Client (DHA-Service und ein Windows 10- oder Windows 11-Gerät).
  - **DHA-Signaturzertifikat.** Ein x.509-Zertifikat in einer Kette mit einem vertrauenswürdigen Unternehmensstammzertifikat mit exportierbarem privatem Schlüssel. Der DHA-Service verwendet dieses Zertifikat für die digitale Signatur.
  - **DHA-Verschlüsselungszertifikat.** Ein x.509-Zertifikat in einer Kette mit einem vertrauenswürdigen Unternehmensstammzertifikat mit exportierbarem privatem Schlüssel. Der DHA-Service verwendet dieses Zertifikat auch für die Verschlüsselung.
- Wählen Sie eines der folgenden Verfahren für die Zertifikatüberprüfung:
  - **EKCert.** Der EKCert-Überprüfungsmodus wurde für Geräte in Organisationen optimiert, die nicht mit dem Internet verbunden sind. Geräte, die sich mit einem DHA-Dienst im EKCert-Überprüfungsmodus verbinden, haben keinen Direktzugriff auf das Internet.
  - **AIKCert.** Der AIKCert-Überprüfungsmodus wurde für Betriebsumgebungen optimiert, die Zugriff auf das Internet haben. Geräte, die sich mit einem DHA-Dienst im AIKCert-Überprüfungsmodus verbinden, benötigen Direktzugriff auf das Internet und können ein AIK-Zertifikat von Microsoft erhalten.

Hinzufügen der DHA-Serverrolle zum Windows-Server

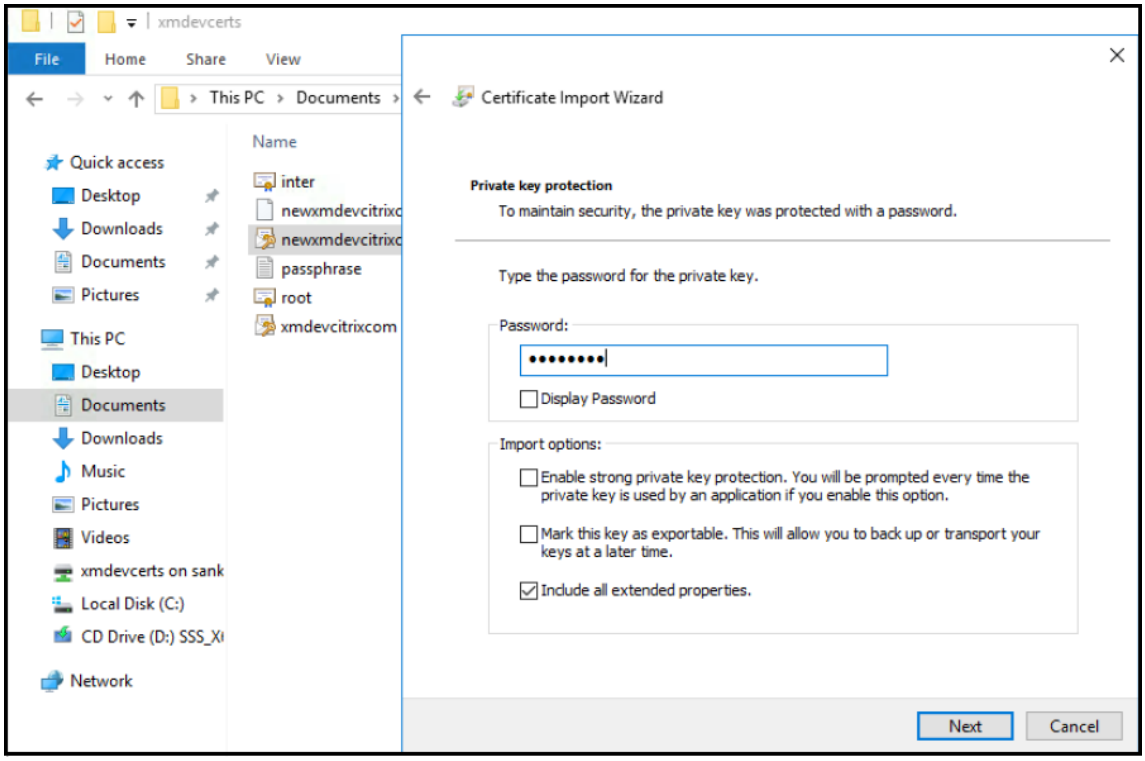
1. Klicken Sie im Windows-Server (falls der Server-Manager noch nicht geöffnet ist) auf **Start** und dann auf **Server-Manager**.
2. Klicken Sie auf **Rollen und Features hinzufügen**.
3. Klicken Sie auf der Seite **Vorbereitung** auf **Weiter**.
4. Klicken Sie auf der Seite **Installationstyp wählen** auf **Rollenbasierte oder featurebasierte Installation** und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite **Zielserver auswählen** auf **Einen Server aus dem Serverpool auswählen**, wählen Sie den Server aus und klicken Sie auf **Weiter**.
6. Aktivieren Sie auf der Seite **Serverrolle auswählen** das Kontrollkästchen für Device Health Attestation.
7. Optional: Klicken Sie auf **Features hinzufügen**, um weitere erforderliche Rollendienste und Features zu installieren.
8. Klicken Sie auf **Weiter**.
9. Klicken Sie auf der Seite **Feature auswählen** auf **Weiter**.
10. Klicken Sie auf der Seite **Rolle "Webserver" (IIS)** auf **Weiter**.
11. Klicken Sie auf der Seite **Rollendienste auswählen** auf **Weiter**.
12. Klicken Sie auf der Seite **Device Health Attestation Service** auf **Weiter**.
13. Klicken Sie auf der Seite **Installationsauswahl bestätigen** auf **Installieren**.
14. Nach Abschluss der Installation klicken Sie auf **Schließen**.

Hinzufügen des SSL-Zertifikats zum Zertifikatspeicher des Servers

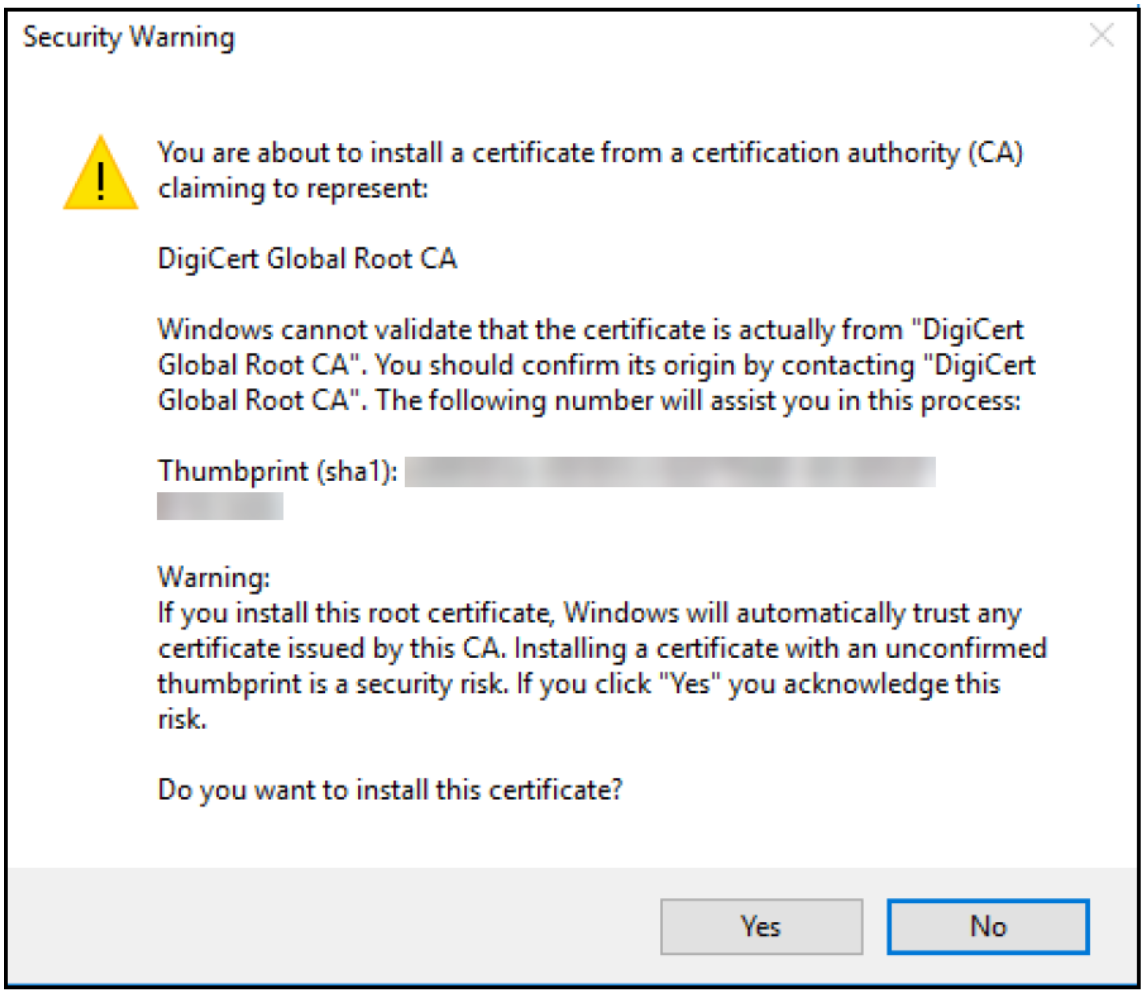
1. Gehen Sie zur SSL-Zertifikatsdatei und wählen Sie sie aus.
2. Wählen Sie **Aktueller Benutzer** als Speicherort aus und klicken Sie auf **Weiter**.



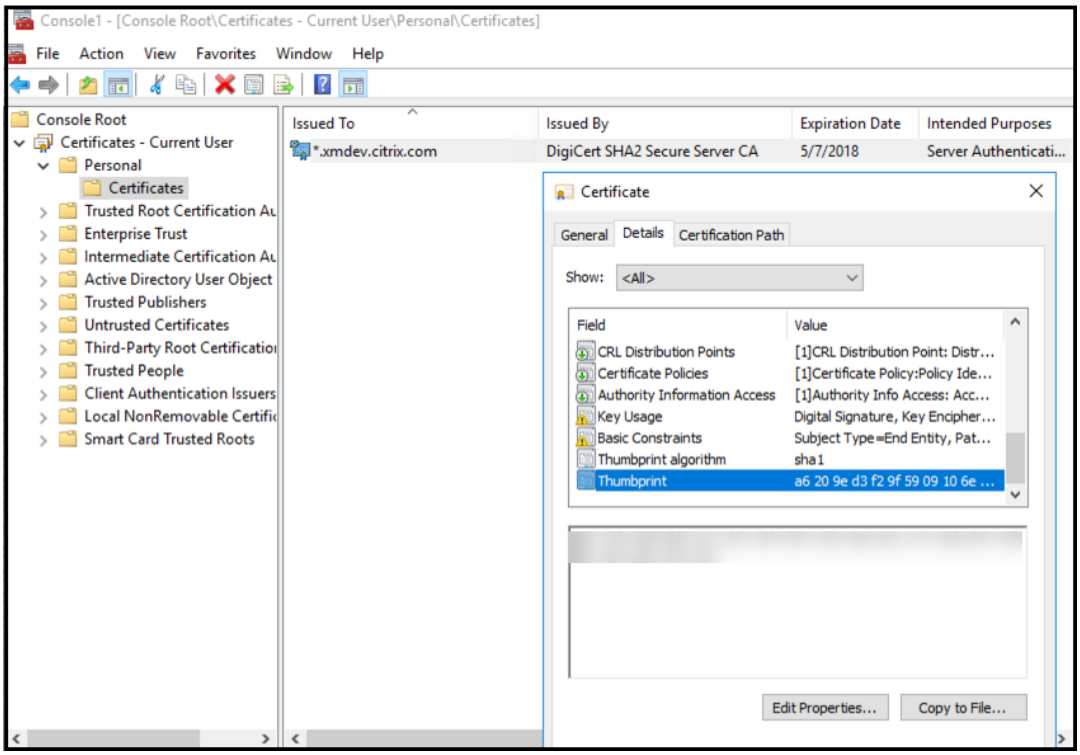
3. Geben Sie das Kennwort für den privaten Schlüssel ein.
4. Stellen Sie sicher, dass die Importoption **Alle erweiterten Eigenschaften mit einbeziehen** ausgewählt ist. Klicken Sie auf **Weiter**.



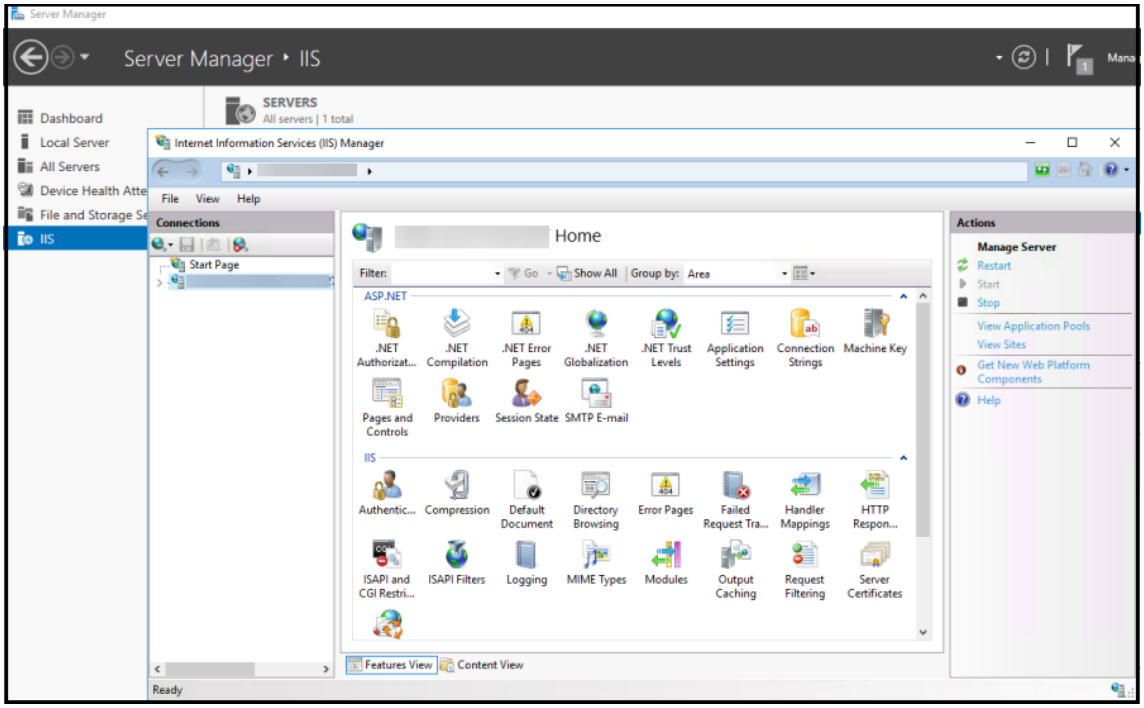
5. Wenn dieses Fenster angezeigt wird, klicken Sie auf **Ja**.



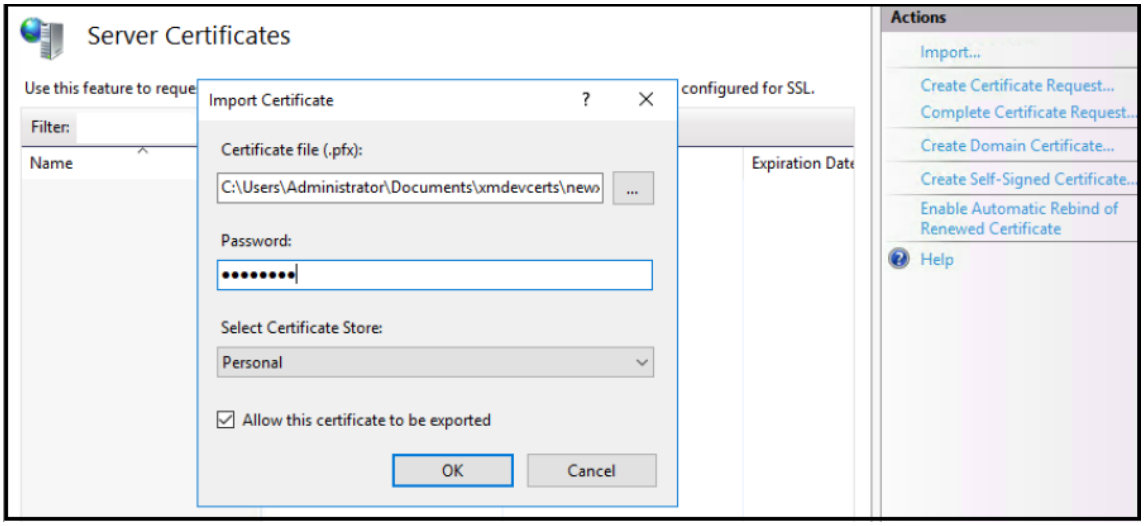
6. Bestätigen Sie, dass das Zertifikat installiert ist:
    a) Öffnen Sie ein Eingabeaufforderungsfenster.
    b) Geben Sie **mmc** ein und drücken Sie die Eingabetaste. Zur Anzeige der Zertifikate im Speicher der lokalen Maschine müssen Sie die Administratorrolle haben.
    c) Klicken Sie im Menü “Datei” auf **Snap-In hinzufügen/entfernen**.
    d) Klicken Sie auf **Hinzufügen**.
    e) Wählen Sie im Dialogfeld “Eigenständiges Snap-In hinzufügen” die Option **Zertifikate**.
    f) Klicken Sie auf **Hinzufügen**.
    g) Wählen Sie im Dialogfeld “Zertifikat-Snap-In” die Option **Eigenes Benutzerkonto** aus. (Wenn Sie als Dienstkontoinhaber angemeldet sind, wählen Sie **Dienstkonto**.)
    h) Klicken Sie im Dialogfeld “Computer auswählen” auf **Fertig stellen**.



7. Navigieren Sie zu **Server-Manager > IIS** und wählen Sie das Symbol **Serverzertifikate** aus.

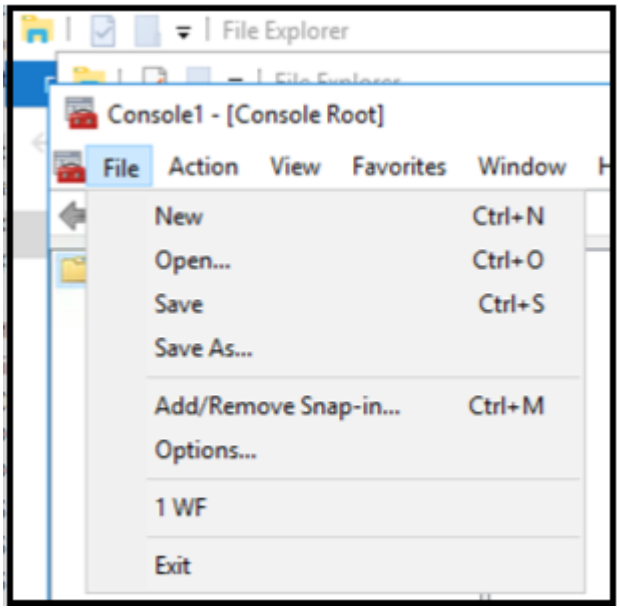


8. Wählen Sie im Menü “Aktion” den Befehl **Importieren...**, um das SSL-Zertifikat zu importieren.

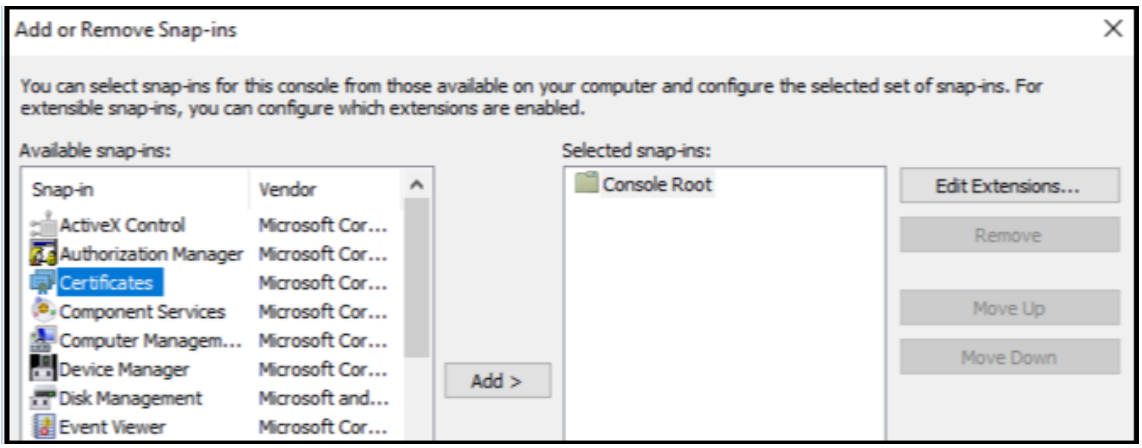


Abrufen und Speichern des Zertifikatfingerabdrucks

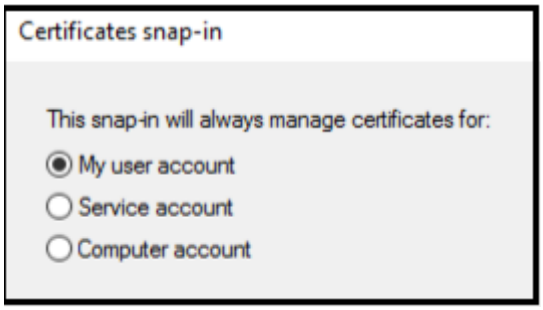
1. Geben Sie in der Suchleiste des Datei-Explorers **mmc** ein.
2. Klicken Sie im Fenster “Konsolenstamm” auf **Datei > Snap-In hinzufügen/entfernen...**.



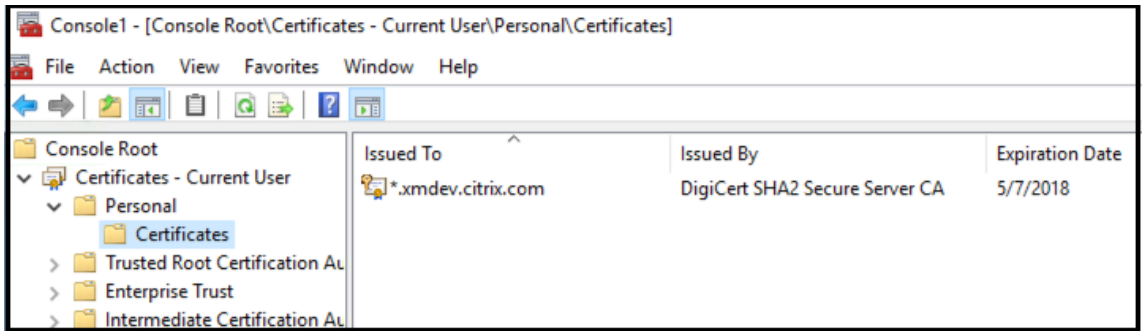
3. Wählen Sie das Zertifikat in der Liste der verfügbaren Snap-Ins aus und fügen Sie es den ausgewählten Snap-Ins hinzu.



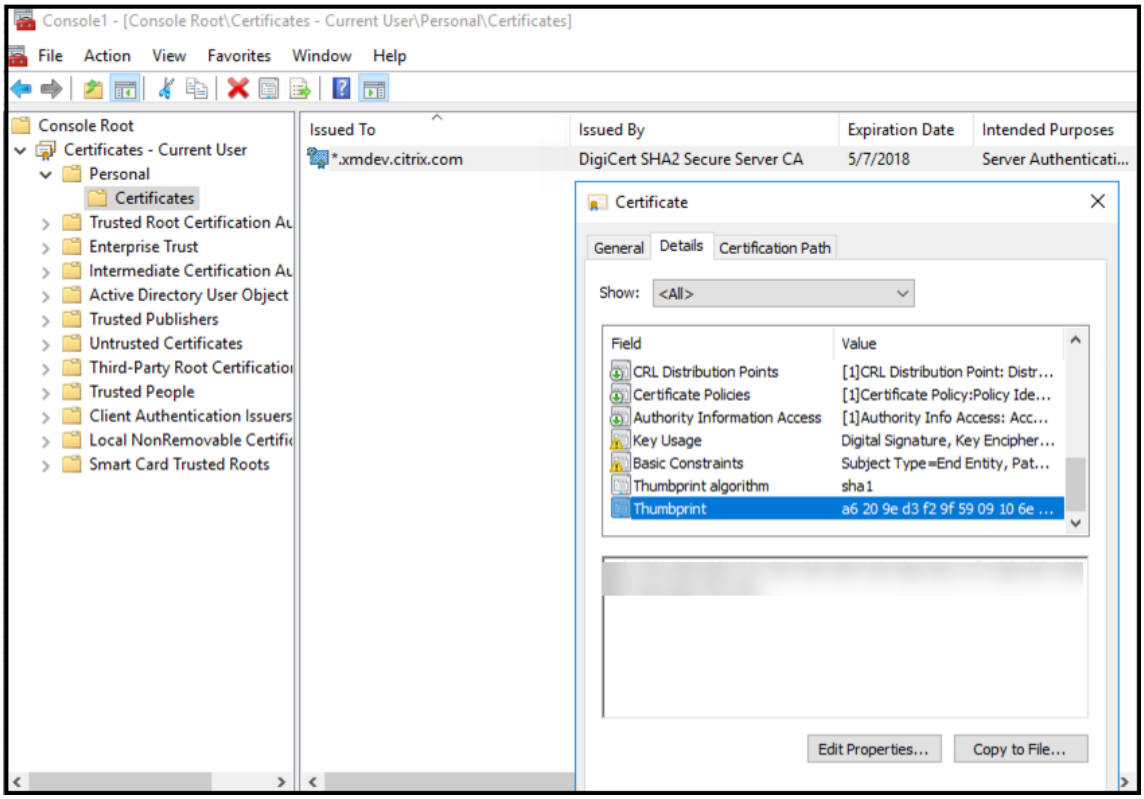
4. Wählen Sie **Eigenes Benutzerkonto**.



5. Wählen Sie das Zertifikat aus und klicken Sie auf **OK**.



6. Doppelklicken Sie auf das Zertifikat und wählen Sie die Registerkarte **Details**. Führen Sie einen Bildlauf nach unten durch, um den Fingerabdruck des Zertifikats anzuzeigen.



7. Kopieren Sie den Fingerabdruck in eine Datei. Entfernen Sie die Leerstellen, wenn Sie den Fingerabdruck in PowerShell-Befehlen verwenden.

Installieren der Signatur- und Verschlüsselungszertifikate

Mit folgenden PowerShell-Befehlen können Sie die Signatur- und Verschlüsselungszertifikate auf dem Windows-Server installieren:

Ersetzen Sie den Platzhalter “ReplaceWithThumbprint” und schließen Sie ihn wie gezeigt in Anführungszeichen ein.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
   $keyname icacls $keypath /grant IIS_IUSRS`:R
<!--NeedCopy-->
```


Extrahieren des TPM-Stammzertifikats und Installieren des Pakets vertrauenswürdiger Zertifikate

Führen Sie folgende Befehle auf dem Windows-Server aus:

```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
<!--NeedCopy-->
```

Konfigurieren des DHA-Diensts

Führen Sie folgenden Befehl auf dem Windows-Server aus, um den DHA-Dienst zu konfigurieren.

Ersetzen Sie den Platzhalter “ReplaceWithThumbprint”.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
    ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
    ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
<!--NeedCopy-->
```

Führen Sie folgende Befehle auf dem Windows-Server aus, um die Richtlinie “Zertifikatskette” für den DHA-Dienst einzurichten:

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
<!--NeedCopy-->
```

Reagieren Sie auf die Eingabeaufforderungen wie folgt:

```
  Confirm

```



```
Are you sure you want to perform this action?

Performing the operation "Install-DeviceHealthAttestation" on
   target "WIN-N27D1FKCEBT".

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
   Help (default is "Y"): A

Adding SSL binding to website 'Default Web Site'.

Add SSL binding?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

Add application pool?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding web application 'DeviceHealthAttestation' to website '
   Default Web Site'.

Add web application?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding firewall rule 'Device Health Attestation Service' to allow
   inbound connections on port(s) '443'.

Add firewall rule?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Setting initial configuration for Device Health Attestation Service
   .

Set initial configuration?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Registering User Access Logging.

Register User Access Logging?

```



```
43      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
44  <!--NeedCopy-->
```

Überprüfen der Konfiguration

Um zu prüfen, ob das Zertifikat “DHASActiveSigningCertificate” aktiviert wurde, führen Sie folgenden Befehl auf dem Server aus:

```
Get-DHASActiveSigningCertificate
```

Wenn das Zertifikat aktiv ist, werden der Zertifikatstyp (Signatur) und der Fingerabdruck angezeigt.

Um zu prüfen, ob das Zertifikat “DHASActiveSigningCertificate” aktiviert wurde, führen Sie folgende Befehle auf dem Server aus

Ersetzen Sie den Platzhalter “ReplaceWithThumbprint” und schließen Sie ihn wie gezeigt in Anführungszeichen ein.

```
1  Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
       -Force
2
3  Get-DHASActiveEncryptionCertificate
4  <!--NeedCopy-->
```

Wenn das Zertifikat aktiv ist, wird der Fingerabdruck angezeigt.

Rufen Sie zum Durchführen einer letzten Prüfung diese URL auf:

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate
/v1
```

Wenn der DHA-Dienst ausgeführt wird, wird “Methode unzulässig” angezeigt.

Konfigurieren der zertifikatbasierten Authentifizierung mit EWS für Secure Mail-Pushbenachrichtigungen

January 5, 2022

Beitrag von Vijay Kumar Kunchakuri

Damit Pushbenachrichtigungen für Secure Mail funktionieren, müssen Sie Exchange Server für die zertifikatbasierte Authentifizierung konfigurieren. Dies ist vor allem dann erforderlich, wenn Secure Hub mit zertifikatbasierter Authentifizierung bei XenMobile registriert ist.

Sie müssen das virtuelle Verzeichnis für Active Sync und Exchange Web Services (EWS) auf dem Exchange-Mailserver mit zertifikatbasierter Authentifizierung konfigurieren.

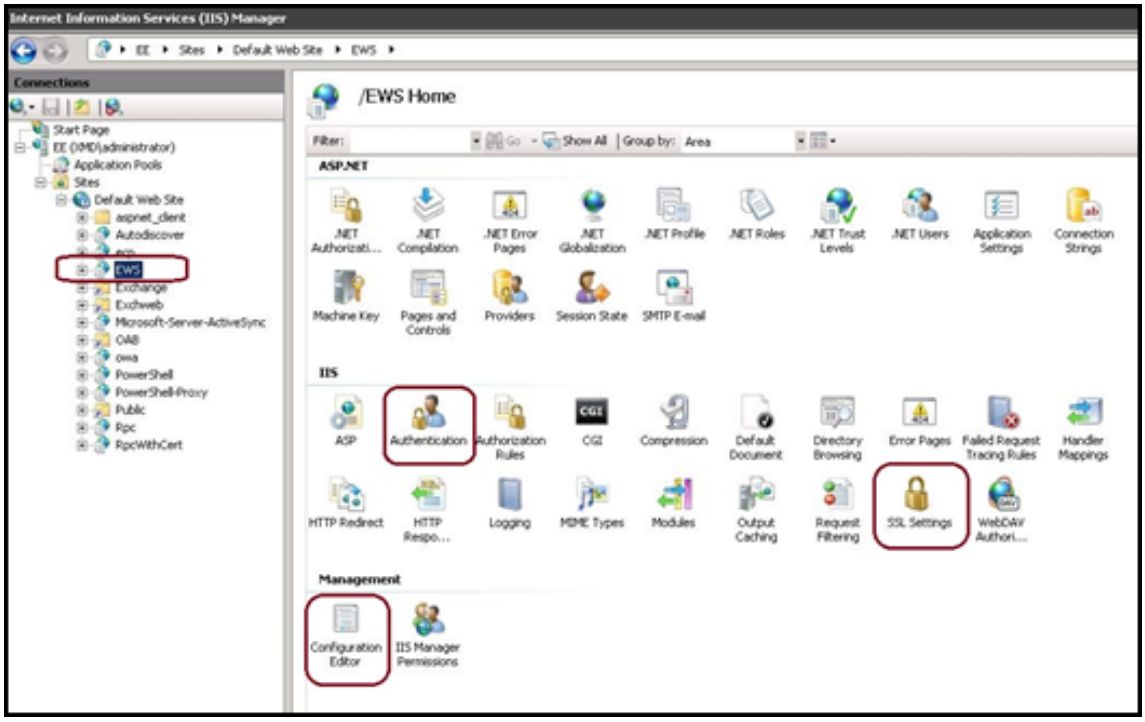
Wenn Sie diese Konfigurationen nicht durchführen, schlägt das Abonnement für Secure Mail-Pushbenachrichtigungen fehl und der Badge in Secure Mail wird nicht aktualisiert.

In diesem Artikel wird die Schrittfolge zum Konfigurieren der zertifikatbasierten Authentifizierung beschrieben. Diese Konfigurationen betreffen speziell das virtuelle EWS-Verzeichnis auf Exchange Server.

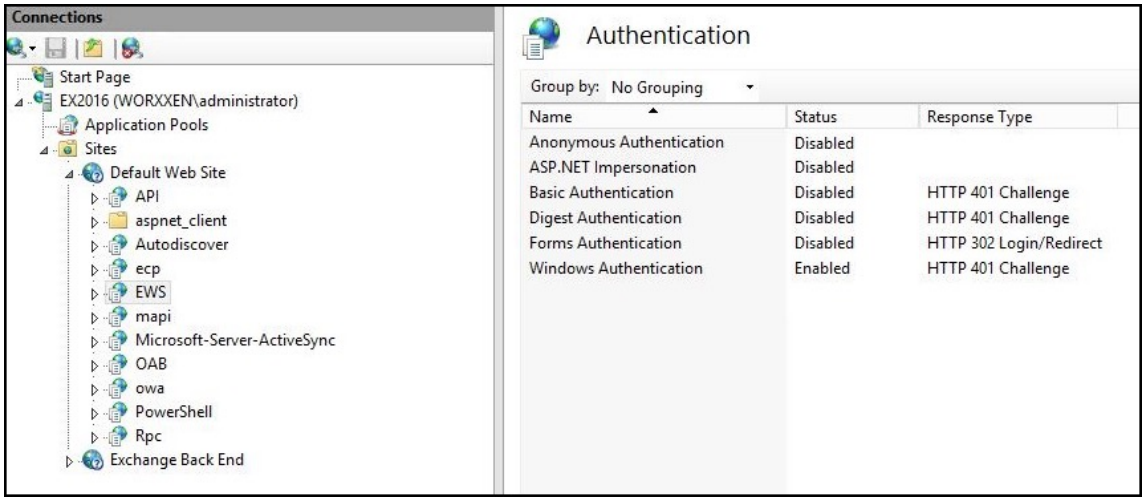
Führen Sie zu Beginn der Konfiguration zunächst folgende Schritte aus:

1. Melden Sie sich an allen Servern an, auf denen das virtuelle EWS-Verzeichnis installiert ist.
2. Öffnen Sie IIS-Manager.
3. Klicken Sie unter **Standardwebsite** auf das virtuelle EWS-Verzeichnis.

   Die Snap-Ins für Authentifizierung, SSL-Einstellungen und Konfigurationseditor sind auf der rechten Seite von IIS-Manager.



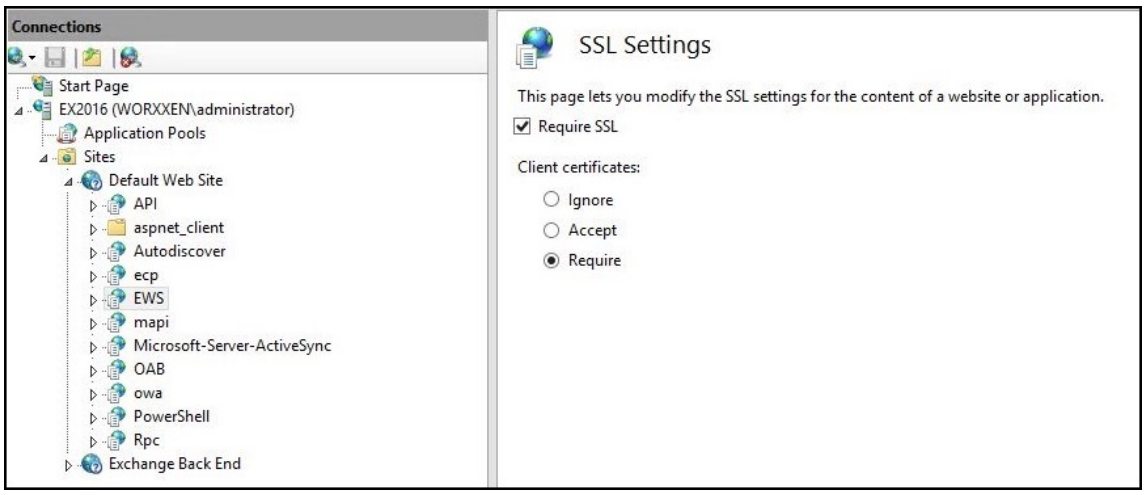
4. Stellen Sie sicher, dass die Einstellungen zur **Authentifizierung** für EWS wie in der folgenden Abbildung konfiguriert sind.



5. Konfigurieren Sie die **SSL-Einstellungen** für das virtuelle EWS-Verzeichnis.

   a) Aktivieren Sie das Kontrollkästchen **SSL erforderlich**.

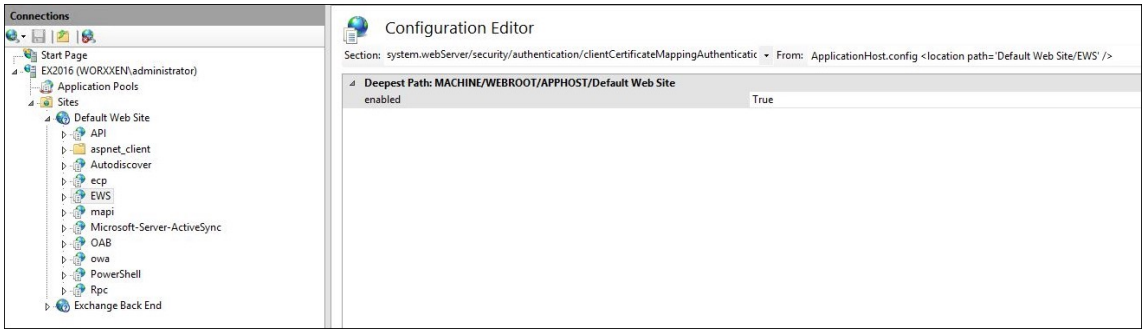
   b) Klicken Sie unter **Clientzertifikate** auf **Erfordern**. Sie können auch **Akzeptieren** auswählen, falls andere EWS-Mail-Clients sich mit Benutzernamen und Kennwort zur Authentifizierung und für den Verbindungsaufbau mit Exchange Server anmelden.



6. Klicken Sie auf **Konfigurationseditor** und gehen Sie in der Dropdownliste **Abschnitt** zum folgenden Abschnitt:

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Setzen Sie **Aktiviert** auf **Wahr**.

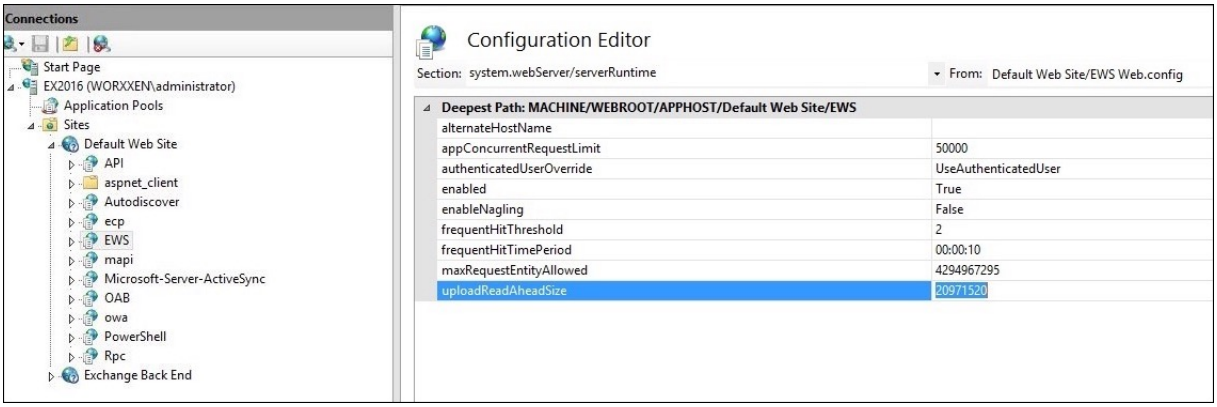


8. Klicken Sie auf **Konfigurationseditor** und gehen Sie in der Dropdownliste **Abschnitt** zum folgenden Abschnitt:
    - **system.webServer/serverRuntime**
9. Wählen Sie für **uploadReadAheadSize** den Wert **10485760** (10 MB), **20971520** (20 MB) oder den für Ihre Organisation erforderlichen Wert.

> **Wichtig:**
>
> Wenn Sie diesen Wert nicht korrekt festlegen, kann die zertifikatbasierte Authentifizierung beim Abonnieren von EWS-Pushbenachrichtigungen fehlschlagen, und es wird der Fehlercode 413 angezeigt.
>
> Legen Sie diesen Wert nicht auf **0** fest.

Weitere Informationen finden Sie in den Ressourcen folgender Drittanbieter:

- Microsoft IIS server runtime
- Butsch Client Management Blog



Weitere Informationen zur Problembehandlung in Secure Mail bei Problemen mit iOS-Pushbenachrichtigungen finden Sie in diesem Artikel im Citrix Support Knowledge Center.

Verwandte Informationen

Pushbenachrichtigungen für Secure Mail für iOS

Integrieren von XenMobile-Mobilgeräteverwaltung (MDM) mit der Cisco Identity Services Engine (ISE)

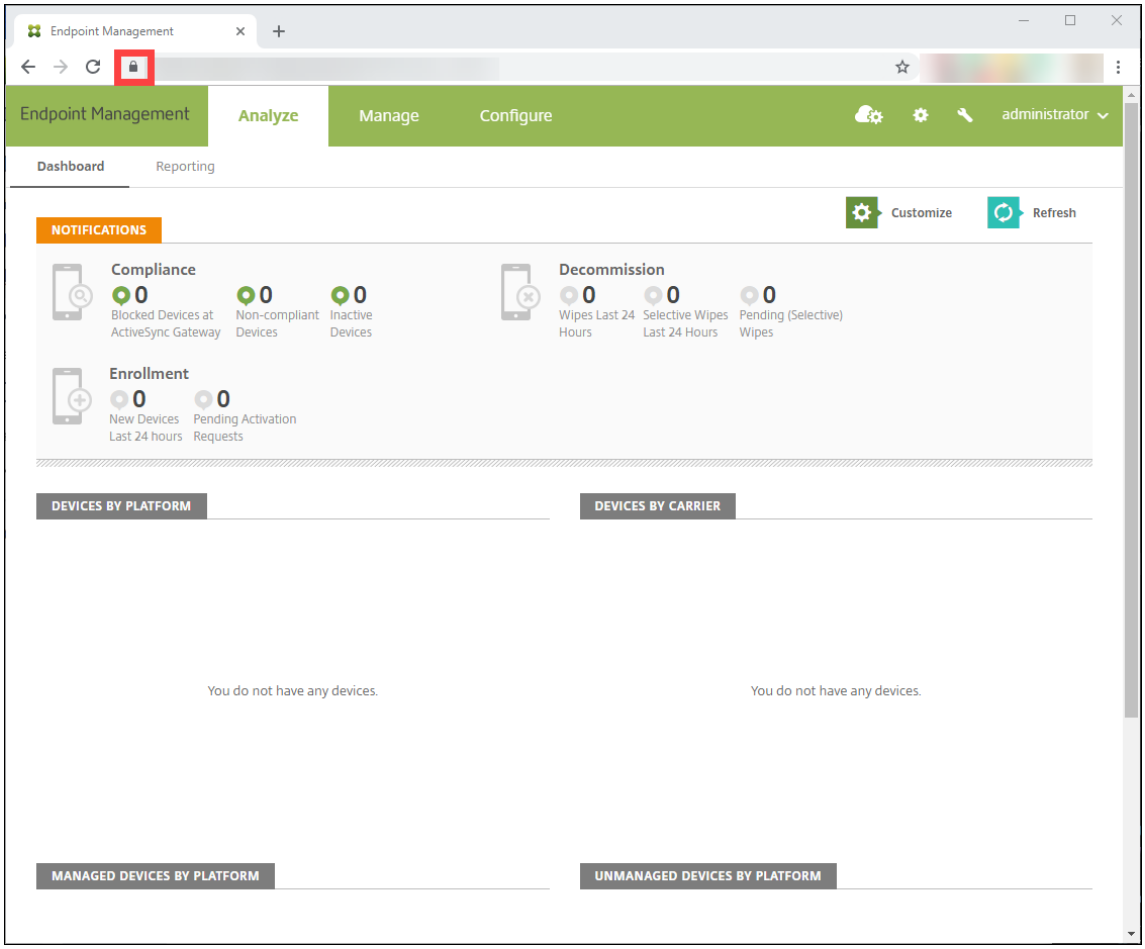
August 10, 2020

Beitrag von John Bartel III

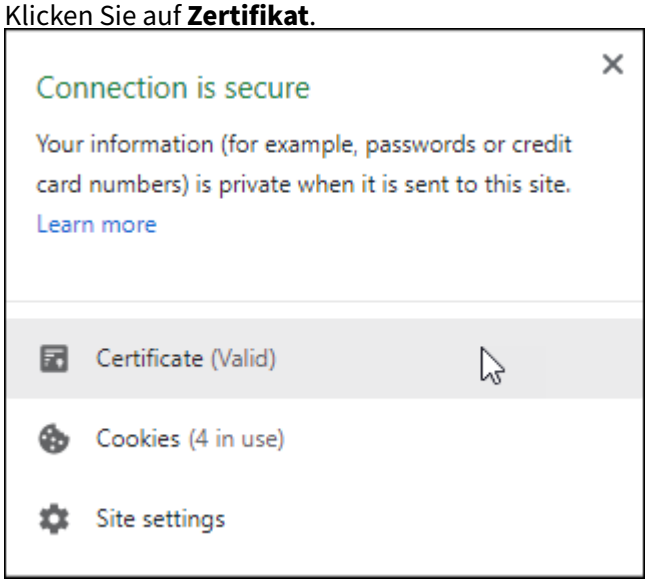
Cisco ISE wird verwendet, um mobile Geräte am Arbeitsplatz bereitzustellen, zu sichern, zu überwachen, zu integrieren und zu verwalten. Die auf das mobile Gerät heruntergeladene Software steuert die Verteilung von Anwendungen und Patches und steuert Daten und Konfiguration auf dem Endpunkt. XenMobile kann mit Cisco ISE integriert werden, um nicht konforme und nicht verwaltete Geräte auf der Cisco ISE-Konsole zu verwalten. Mit XenMobile können Sie auch den Zugriff auf Unternehmensdienste selektiv zulassen, verweigern oder in Quarantäne stellen.

Um die Integration mit XenMobile einzurichten, erstellen Sie ein lokales Dienstkonto auf dem XenMobile Server mit der Administrator-RBAC-Rolle. Diese Rolle ermöglicht dem Cisco ISE den Zugriff auf die XenMobile API. ISE muss dem XenMobile Zertifikat vertrauen. Um dieses Zertifikat herunterzuladen, öffnen Sie einen Webbrowser, navigieren Sie zur Server-URL und melden Sie sich an.

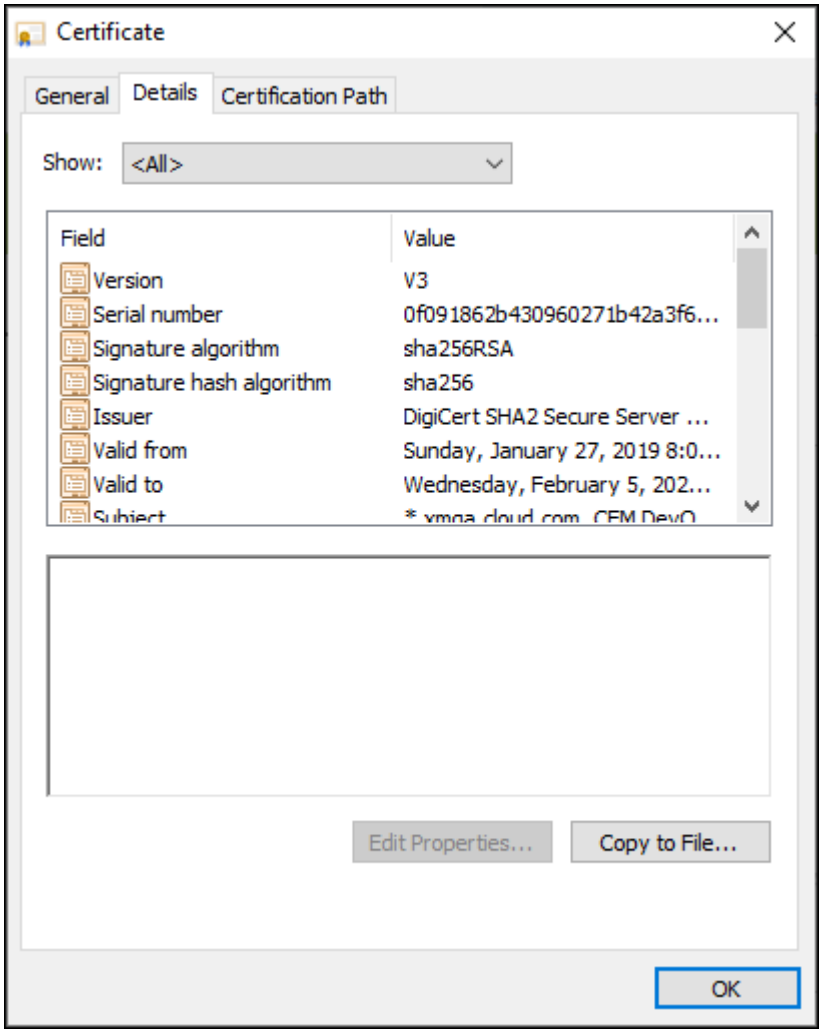
1. Klicken Sie nach der Anmeldung auf die Sperre neben der URL in der Adressleiste.



2. Klicken Sie auf **Zertifikat**.



3. Wählen Sie die Registerkarte **Details** und klicken Sie auf **In Datei kopieren**.



4. Folgen Sie dem Assistenten, um das Zertifikat lokal zu speichern.
5. Melden Sie sich an der Cisco ISE-Konsole an und importieren Sie das heruntergeladene XenMobile-Zertifikat. Importieren Sie das Zertifikat in den “Trusted Certificate Store” von Cisco ISE. Dieser Import ist notwendig, damit Cisco ISE der Kommunikation mit dem XenMobile Server vertraut.
    a) Navigieren Sie zu **Administration > System > Certificates > Certificate Management > Trusted Certificates**. Klicken Sie auf **Importieren**.
    b) Geben Sie dem Zertifikat einen Namen und aktivieren Sie die Kontrollkästchen **Trust for authentication within ISE** und **Trust for authentication of Cisco Services**.
6. Fügen Sie XenMobile als externes MDM in Cisco ISE hinzu.
    a) Navigieren Sie zu **Administration > Network Resource > External MDM**. Klicken Sie auf **Add**, und füllen Sie Folgendes aus:
        - **Serverhost:** Ihr XenMobile FQDN
        - **Port:** 443
        - **Instanzname:** Der Instanzname von XenMobile Server. Der Instanzname ist in den

meisten Bereitstellungen standardmäßig “zdm”.

- **Benutzername:** Geben Sie den Namen des Benutzers ein, den Sie für diese Aufgabe erstellt haben. Der Benutzer sollte ein lokales Administratorkonto in der ursprünglichen Admin-RBAC-Gruppe sein.
- **Kennwort:** Das Kennwort für den Benutzer, den Sie gerade hinzugefügt haben.
- Überprüfen Sie, wo es **Aktivieren** heißt.

7. Wenn der Test erfolgreich ist, klicken Sie auf **Submit**.

Weitere Informationen zu Cisco ISE finden Sie in der Cisco-Dokumentation.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States