Citrix Endpoint Management

Contents

Citrix Endpoint Management

March 11, 2024

Citrix Endpoint Management ist eine Lösung für die Verwaltung von Endpunkten, die Funktionen für die Mobilgeräteverwaltung (MDM) und die Mobilanwendungsverwaltung (MAM) bietet. Mit Citrix Endpoint Management verwalten Sie Geräte- und App-Richtlinien und stellen Apps für Benutzer bereit. Ihre Geschäftsinformationen bleiben durch strenge Sicherheit für Identitäten, Geräte, Apps, Daten und Netzwerke geschützt.

Verantwortungsbereiche von Citrix bzw. des Kunden

Citrix Cloud Operations übernimmt verschiedene Infrastruktur- und Überwachungsaufgaben. So können Sie sich auf die Benutzererfahrung und die Verwaltung von Geräten, Apps und Richtlinien konzentrieren.

Verantwortung von Citrix:

- Citrix Endpoint Management-Serverknoten
- Anfängliche Integration und Konfiguration von NetScaler Gateway (Service- oder On-Premises-Version)
- NetScaler Gateway Load Balancer
- Datenbank
- Konfiguration der Cloud Connector-Software
- SAML-Authentifizierungsintegration für ShareFile
- Citrix Endpoint Management-Siteüberwachung: Instanz, Datenbank, Unternehmenskonnektivität (LDAP), VPN-Tunnel (falls vorhanden), öffentliches SSL-Zertifikat, Citrix Endpoint Management-Lizenzierung

Verantwortung des Kunden:

- Verwaltung und Aktualisierung von NetScaler Gateway (On-Premises-Version)
- Maschinen, auf denen Cloud Connectors und Gateway Connector (für Citrix Gateway Service) installiert sind
- LDAP/Active Directory
- DNS
- ShareFile: Anfängliche ShareFile-Konfiguration, On-premises-Installation von Speicherzonencontrollers, Citrix Files-Updates
- Citrix Endpoint Management-Konfiguration: Geräte, Richtlinien, Apps, Bereitstellungsgruppen, Aktionen und Clientzertifikate

Integration mit Microsoft Endpoint Manager

Citrix Endpoint Management kann mit Microsoft Endpoint Manager (MEM) integriert werden. Durch diese Integration können Microsoft Intune-fähige Apps wie Microsoft Edge Browser die Vorteile von Citrix Endpoint Management Micro-VPN nutzen. Die Integration ermöglicht Folgendes:

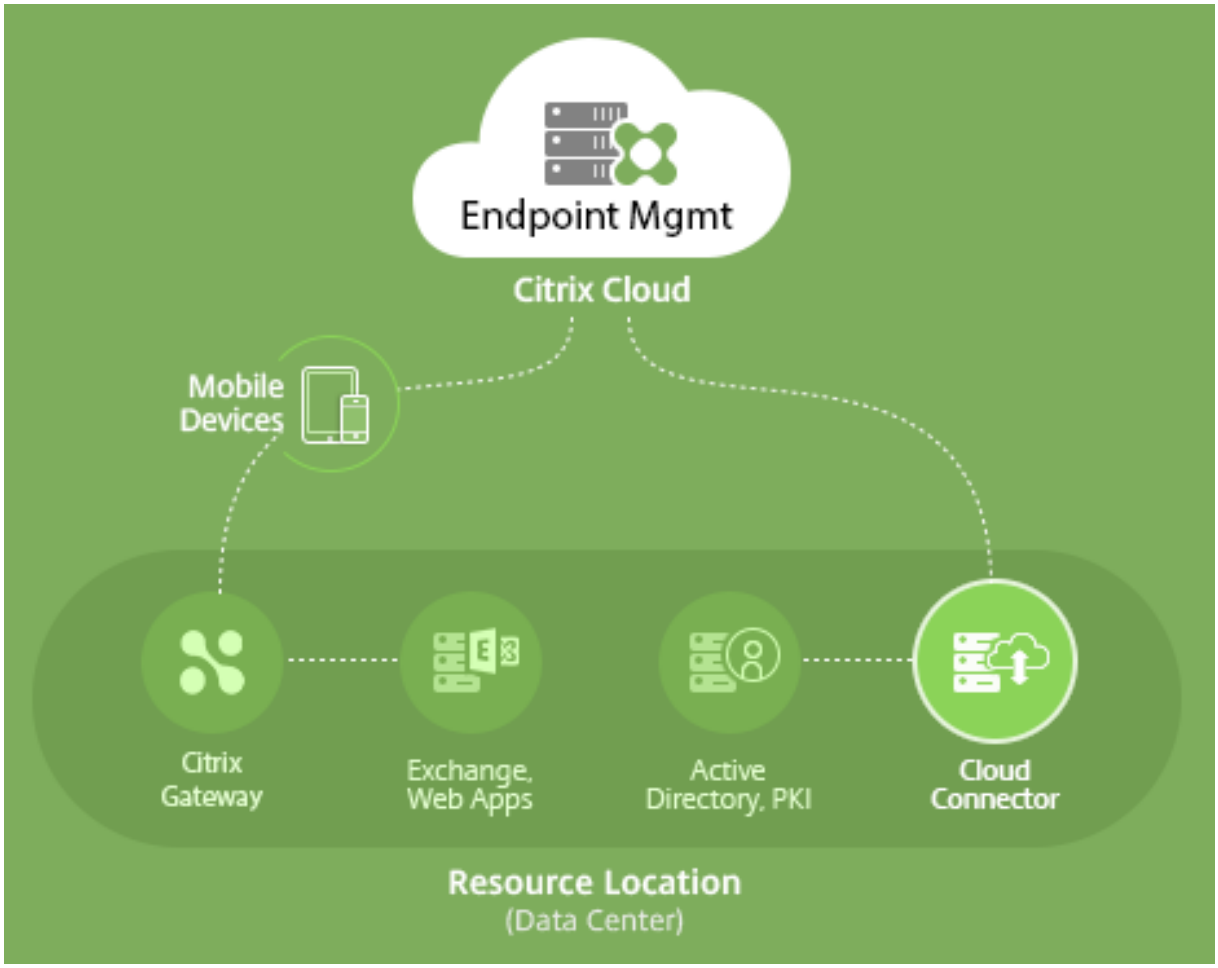
- Secure Office 365-Anwendungen mit bedingtem Zugriff und Azure AD. Weitere Informationen finden Sie unter Integration in bedingten Azure AD-Zugriff.
- Sie können Ihre Branchenanwendungen mit Intune und Citrix umschließen, um Micro-VPN-Funktionen in einem Intune-Container zur Mobilanwendungsverwaltung (MAM) bereitzustellen.
- Sie können Office 365-Apps, branchenspezifische Apps und Citrix Secure Mail in einem einzigen Container verwalten und bereitstellen. Diese Verwaltungsmethode bietet ultimative Sicherheit und Produktivität. Beispiel:
  - Blockieren einzelner Geräte oder Betriebssysteme
  - Anpassen von ActiveSync-Richtlinien basierend auf Geräten, Benutzern oder Benutzergruppen
  - Quarantäne auf Geräteebene
  - Überwachen einzelner Verbindungen oder Geräte
  - Vermeiden von Sicherheitsrisiken durch zwischengespeicherte Anmeldeinformationen und Daten

Verwenden Sie Citrix Endpoint Management MDM+MAM oder Intune MDM zum Verwalten von Geräten. Weitere Informationen finden Sie unter Integration von Citrix Endpoint Management mit Microsoft Endpoint Manager.

Cloud Connector und Ressourcenstandorte

Die Verbindung mit Citrix Endpoint Management stellen Sie über den Cloud Connector her. Der Cloud Connector dient als Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten. Mit Cloud Connector kann die Cloud ohne komplexe Netzwerk- oder Infrastrukturkonfiguration (VPNs, IPsec-Tunnel o. Ä.) verwaltet werden.

Ressourcenstandorte enthalten die Ressourcen zum Bereitstellen von Services für Ihre Abonnenten. Ressourcenstandorte für Citrix Endpoint Management sind Ihre NetScaler Gateway-, LDAP-, DNS- und PKI-Server.



Weitere Informationen zum Cloud Connector und zu Ressourcenstandorten finden Sie unter Info über Citrix Endpoint Management.

Erste Schritte mit Citrix Endpoint Management

> **Tipp:**
>
> XenMobile Migration Service
>
> Wenn Sie die On-Premises-Version von XenMobile Server verwenden, hilft Ihnen unser XenMobile Migration Service beim Start in Citrix 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.
>
> Weitere Informationen zu unserem Migrationsservice finden Sie unter 3 reasons to move to Citrix Endpoint Management service.

> Informationen dazu, warum eine Migration auf Citrix Endpoint Management sich lohnt und wie sie durchgeführt wird, finden Sie im Kurskatalog des CEM Migration Service und in der Anleitung zum Citrix Endpoint Management (CEM) Migration Service.

Wenn Sie Citrix Endpoint Management testen oder erwerben, bietet das Citrix Endpoint Management Operations-Team eine fortlaufende Onboardinghilfe. Das Team bleibt außerdem mit Ihnen in Verbindung, um sicherzustellen, dass die Kerndienste von Citrix Endpoint Management ordnungsgemäß ausgeführt und konfiguriert werden. Diese Abbildung zeigt die Onboardingschritte.

Wenden Sie sich an einen Citrix Vertriebsmitarbeiter, um sich für ein Citrix-Konto zu registrieren und eine Citrix Endpoint Management-Testversion anzufordern. Wenn Sie zum Fortfahren bereit sind, rufen Sie https://onboarding.cloud.com auf.

Einen kurzen Überblick über das Onboarding und die Konfiguration von Citrix Endpoint Management bietet dieses Video.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Benötigen Sie weitere Informationen vor dem Start? Verwenden Sie diese Ressourcen:

Citrix Endpoint Management-Dokumentation: Bietet die vollständige Citrix Endpoint Management-Dokumentation, vom Onboarding über die Erstkonfiguration bis zur erweiterten Konfiguration. Ein Artikel beschreibt neue Features und Fixes. Citrix benachrichtigt Sie, wenn dieser Artikel für eine neue Version verfügbar ist.

Citrix Endpoint Management Onboarding Handbook: enthält alle Informationen, die Sie für ein reibungsloses Onboarding und Aktivieren von Citrix Endpoint Management benötigen. In diesem Dokument können Sie Änderungen für interne Prozesse aufzeichnen und Ihre allgemeinen und funktionellen Designs dokumentieren.

Citrix Endpoint Management-Bereitstellungsdokumentation: Bei der Planung einer Citrix Endpoint Management-Bereitstellung müssen viele Punkte berücksichtigt werden. Das Handbuch enthält Empfehlungen, häufige Fragen und Anwendungsfälle für Ihre Citrix Endpoint Management-Umgebung.

SalesIQ: weitere Ressourcen für Citrix Partner.

Nächste Schritte

Informationen zum Onboarding-Prozess von Citrix Endpoint Management finden Sie unter Onboarding und Einrichten von Ressourcen.

Nachdem Sie das Onboarding abgeschlossen haben, siehe Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen

Ankündigung für das Einstellen der Unterstützung

Vorankündigungen zu Features von Citrix Endpoint Management, die schrittweise ausgemustert werden, finden Sie unter Einstellung von Features und Plattformen.

Citrix Endpoint Management-Support

Informationen zum Zugriff auf entsprechende Informationen und Tools in der Citrix Endpoint Management-Konsole finden Sie unter Überwachen und Support.

Updates für Citrix Endpoint Management werden ca. alle zwei Wochen veröffentlicht. Der Prozess ist für die Kunden transparent. Erste Updates werden nur auf interne Sites von Citrix angewendet und erst danach schrittweise auf Kundenumgebungen. Durch diese schrittweise Bereitstellung von Updates wird die Produktqualität sichergestellt und die Verfügbarkeit maximiert.

Citrix Endpoint Management-Kunden erhalten Updates und Mitteilungen direkt vom Citrix Endpoint Management Cloud Operations-Team. Über diese Updates werden Sie bezüglich neuer Features, bekannter Probleme, behobener Probleme usw. auf dem Laufenden gehalten.

Das Citrix Cloud Operations-Team wartet die Citrix Endpoint Management-Umgebungen mit den neuesten Patches von Citrix Endpoint Management. Zum Abrufen von Patches oder Fixes, die vor einem Rolling Patch erforderlich sind, wenden Sie sich an den technischen Support von Citrix.

Wenn Sie Probleme mit der Umgebung haben, wenden Sie sich an den technischen Citrix Support oder das für Sie zuständige Citrix Team. Solche Probleme können z. B. die Registrierung von mobilen Geräten, der Zugriff auf die Citrix Endpoint Management-Konsole oder Citrix Secure Mail-Probleme sein.

Wenn Sie eine Integration oder Änderungen an NetScaler Gateway in der Cloud oder Citrix Endpoint Management benötigen, senden Sie eine Anfrage über den technischen Support von Citrix.

Beispiele solcher Änderungen:

- Citrix Files-Integration mit NetScaler Gateway in der Cloud
- Änderung des Typs der NetScaler Gateway-Authentifizierung
- Überprüfen der Verbindung mit Datencenterressourcen des Kunden

- Änderung der Split-Tunneling-Konfiguration für ein Micro-VPN
- Neustarten von Citrix Endpoint Management-Komponenten im Anschluss an einige Konfigurationsänderungen auf dem Server

Servicelevelziele

Citrix Endpoint Management verwendet bewährte Methoden der Branche, um eine Cloudskalierung und einen hohen Grad an Serviceverfügbarkeit zu erreichen.

Ausführliche Informationen zur Verpflichtung von Citrix bezüglich Verfügbarkeit von Citrix Cloud-Diensten finden Sie unter Servicelevelziele.

Was ist neu

June 25, 2024

Das Ziel von Citrix ist es, Citrix Endpoint Management-Kunden neue Features und Produktupdates unverzüglich zur Verfügung zu stellen. Neue Releases bieten größeren Wert, daher gibt es keinen Grund, Updates zu verzögern.

- Updates für Citrix Endpoint Management werden ca. alle zwei Wochen veröffentlicht.
- Diese Updates bewirken keinerlei Ausfallzeit für Ihre Instanz oder Gerätebenutzer.
- Nicht jede Version umfasst neue Features, einige Updates enthalten Fixes und Leistungsverbesserungen.

Der Prozess ist für die Kunden transparent. Erste Updates werden zunächst nur auf interne Sites von Citrix angewendet und anschließend nach und nach auf Kundenumgebungen. Durch diese schrittweise Bereitstellung von Updates wird die Produktqualität sichergestellt und die Verfügbarkeit maximiert.

Sie erhalten zudem Citrix Endpoint Management-Updates und Mitteilungen direkt vom Citrix Endpoint Management Cloud Operations-Team. Über diese Updates werden Sie bezüglich neuer Features, bekannter Probleme, behobener Probleme usw. auf dem Laufenden gehalten.

Weitere Informationen zur Clouddimensionierung und Serviceverfügbarkeit bieten die Servicelevelziele für Citrix Endpoint Management. Informationen zu Serviceunterbrechungen und geplanten Wartungsmaßnahmen finden Sie im Dienstzustandsdashboard.

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 Citrix Endpoint Management-Integrationen mit NetScaler Gateway. Citrix Endpoint Management unterstützt weiterhin die Classic-Richtlinien. Es sind keine Maßnahmen erforderlich.

Vor dem Upgrade von Endpunkten auf iOS 14.5

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

- Aktualisieren Sie Citrix Secure Mail und Citrix Secure Web auf Version 21.2.X oder höher. Siehe Durchführen eines Upgrades von MDX- oder Unternehmensapps.
- Bei Verwendung des MDX Toolkit umschließen Sie alle iOS-Apps von Drittanbietern mit dem MDX Toolkit 21.3.X oder höher und aktualisieren die Apps dann in der Citrix Endpoint Management-Konsole. Die neueste Version des MDX Toolkit finden Sie auf der Downloadseite.

Vor dem Upgrade eines on-premises Citrix ADC auf 13.0-64.35+

Wenn Sie bei verwendeter On-Premises-Version von Citrix ADC ein Upgrade auf Version 13.0–64.35+ planen, führen Sie zunächst den unter Bekannte Probleme in Citrix Endpoint Management 20.10.1 beschriebenen Workaround durch.

Citrix Endpoint Management 24.4.0

- **Neue Geräterichtlinie für Knox Platform for Enterprise Key hinzugefügt:** Eine neue Geräterichtlinie **Knox Platform for Enterprise Key** wurde hinzugefügt. Diese Richtlinie ermöglicht es Ihnen, die erforderlichen Samsung Knox Platform for Enterprise (KPE)-Lizenzinformationen bereitzustellen und die KPE-Lizenzen zu verwenden, um die Sicherheit Ihres Samsung-Geräts zu erhöhen. Weitere Informationen finden Sie unter Geräterichtlinie "Knox Platform for Enterprise".
- **Mindestversion des Betriebssystems erzwingen, um die Einrichtung der automatischen Registrierung abzuschließen:** Mit iOS 17 können MDMs jetzt eine Mindestbetriebssystemversion bei der Registrierung von Geräten erzwingen, wenn sie die automatische Geräteregistrierung verwenden. Weitere Informationen finden Sie unter Schritt 3 unter Konto zu Citrix Endpoint Management hinzufügen.

- **Unterstützung von "Return to Service"in iOS 17:** Mit der Funktion "Return to Service" kann der MDM-Server einen Löschbefehl mit WLAN-Details und einem Standard-MDM-Registrierungsprofil an das Benutzergerät senden. Das Gerät löscht dann automatisch alle Benutzerdaten, stellt eine Verbindung zum angegebenen WLAN-Netzwerk her und registriert sich mithilfe des bereitgestellten Registrierungsprofils erneut beim MDM-Server.
- **Unterstützung von Samsung Enhanced Attestation v3:** Samsung Enhanced Attestation v3 verbessert die CEM-Sicherheitsfunktionen auf Samsung Knox-Geräten. Weitere Informationen finden Sie unter Samsung Knox Enhanced Attestation.
- **Sortieren und Filtern bei der Geräteregistrierung modernisieren:** Die Listenansichten in CEM sind derzeit schwer zu navigieren und weniger benutzerfreundlich. Indem die Filter- und Sortieroptionen in die Spaltenüberschriften verschoben werden, können Kunden diese Funktionen problemlos kombinieren, wodurch es viel einfacher und intuitiver wird, die benötigten Daten zu finden.
- **Unterstützung für die sofortige Installation von Betriebssystemupdates für iOS-Geräte:** In der Geräterichtlinie "Betriebssystemaktualisierung"wurde in den Betriebssystemaktualisierungsoptionen für iOS ein neues Optionsfeld mit dem Namen **schnell wie möglich installieren** hinzugefügt. Mit dieser Funktion können Sie die zuvor heruntergeladenen Betriebssystemupdates sofort für iOS-Geräte installieren. Weitere Informationen finden Sie unter Geräterichtlinie für Betriebssystemupdates für iOS.
- **Automatischen Always-On-VPN-Verbindungsneustart verbessern:** Eine neue verwaltete Konfigurationseinstellung **Always On VPN (optional)** wurde zur Citrix Secure Access-App hinzugefügt, die auf "true"gesetzt werden muss, damit diese Erweiterung zuverlässig für Always-On-VPN-Profile funktioniert. Weitere Informationen finden Sie unter Citrix SSO-Protokolls für Android konfigurieren und Eine von Android Enterprise verwaltete Konfiguration für Citrix SSO erstellen.

Behobene Probleme in CEM 24.4.0

- Unternehmensapps melden nach dem Upgrade auf iOS-Geräten möglicherweise eine falsche Versionsnummer. [CXM-112711]
- Registrierte iOS-Geräte werden aufgefordert, UPN auf Secure Hub einzugeben. [CXM-114316]

Citrix Endpoint Management 24.1.0

In dieser Version wurden durch das Beheben verschiedener Probleme die allgemeine Leistung und Stabilität verbessert. Es wurden keine neuen Features hinzugefügt.

Citrix Endpoint Management 23.12.0

Ein neues obligatorisches Feld "Domäne"wurde in den 802.1x-Einstellungen für Android hinzugefügt: Auf der Seite mit den **Netzwerkrichtlinieneinstellungen für die Android Enterprise-Plattform** wurde ein neues Feld **Domäne** für den Authentifizierungstyp **802.1x EAP** hinzugefügt. Weitere Informationen finden Sie unter 802.1x-Einstellungen für Android.

Derzeit bekannte Probleme

Bekannte Probleme in Citrix Endpoint Management 22.6.0

Die Auswahl aller drei Protokolltypen (**Debug**, **Administratorüberwachung**, **Benutzerüberwachung**) zum Herunterladen unter **Problembehandlung und Support > Protokolle** funktioniert zeitweise nicht. Es werden nur Debugprotokolle heruntergeladen. Als Workaround können Sie jedes Protokoll separat herunterladen oder Ihren Browser im Inkognitomodus öffnen, um alle Protokolle herunterzuladen, indem Sie alle drei Kontrollkästchen markieren. [CXM-105334]

Beim Erstellen eines Weblinks in Android Enterprise tritt ein Fehler auf, wenn Sie versuchen, die App mit einem Symbol zu speichern. Dieser Fehler ist ein Problem der Google-Dienste. Speichern Sie als Workaround die App, ohne ein Symbol hochzuladen. [CXM-105395]

Samsung Knox/SAFE-Richtlinien sind auch nach eingestellter Unterstützung auf registrierten Geräten aktiv und können nicht deaktiviert oder konfiguriert werden. Als Workaround heben Sie die Registrierung des Geräts auf und registrieren es erneut. [CXM-104303]

Bekannte Probleme in Citrix Endpoint Management 22.4.0

Bei der Suche nach einem registrierten Active Directory-Benutzer auf der Registerkarte **Überwachung** werden keine registrierten Geräte für den Benutzer angezeigt. Sie können weiterhin Richtlinien und Apps anzeigen, die dem Benutzer zugewiesen sind, und alle Sicherheitsaktionen unter **Verwalten > Geräte** ausführen. Sowohl iOS- als auch Android-registrierte Geräte sind betroffen. [CXM-104283]

Private Apps können aufgrund eines Problems in den Google-Diensten nicht mit Android Enterprise veröffentlicht werden. Wir werden unsere Dokumentation aktualisieren, sobald das Problem gelöst ist. [CXM-103690]

Bekannte Probleme in Citrix Endpoint Management 21.12.0

Nach der Migration auf Citrix Cloud-basierte RBAC erhalten Administratorbenutzer mit Vollzugriff in Citrix Cloud auch Vollzugriffsberechtigung in CEM, selbst wenn sie vor der Migration über

benutzerdefinierte Berechtigungen verfügten. Als Workaround können Sie die Administratorberechtigungen auf der Seite "Identitäts- und Zugriffsverwaltung"in der Citrix Cloud mit dem gewünschten Zugriff aktualisieren. [CXM-102765]

Kunden, die das Onboarding vor 2018 durchgeführt haben, haben lokalen Administratorzugriff auf die Konsole. CEM-Administratorbenutzer mit Berechtigungen zum Hinzufügen oder Bearbeiten lokaler Benutzer können auch lokale Benutzer in Citrix Cloud hinzufügen oder bearbeiten. Zu diesen Berechtigungen gehört das Ändern der Kennwörter lokaler Benutzer. Um dieses Problem zu beheben, können Sie den Support anrufen, um den direkten lokalen Administratorzugriff auf die Konsole zu blockieren, sodass nur Citrix Cloud-Administratorzugriff gewährt wird. [CXM-102780]

Bekannte Probleme in Citrix Endpoint Management 21.11.0

Unternehmensapps können auf iOS-Geräten, die nur in MAM registriert sind, nicht installiert werden. [CXM-101852]

Wenn der CEM-Server auf Version 21.11.0 aktualisiert wurde, kann die Android Enterprise-Richtlinie **Verwaltete Apps automatisch aktualisieren** nicht auf Geräte angewendet werden. Dieser Richtlinienfehler wirkt sich auf App-Aktualisierungen auf dem Gerät aus. Als Problemumgehung kann ein Administrator die Richtlinie bearbeiten und speichern, um die Standardwerte zu aktualisieren. [CXM-102446]

Bekannte Probleme in Citrix Endpoint Management 21.10.0

Die VPN-Geräterichtlinie funktioniert auf verwalteten Windows 11-Geräten nicht ordnungsgemäß. Wir haben dieses Problem an Microsoft gemeldet und arbeiten gemeinsam an einer Lösung. Über die Fortschritte werden wir informieren.

Bekannte Probleme in Citrix Endpoint Management 21.9.1

Auf Android-Geräten, die im Modus "Arbeitsprofil auf unternehmenseigenen Geräten"registriert sind, erhalten Benutzer möglicherweise die Fehlermeldung, dass sie Apps nicht in ihrem persönlichen Profil installieren oder suchen können. Aktualisieren Sie in diesem Fall die Google Play Store-App und versuchen Sie es erneut. [CXM-100678]

Bekannte Probleme in Citrix Endpoint Management 21.5.0

Benutzer können sich bei Azure Active Directory (AAD) nicht authentifizieren, wenn:

1. Sie ihr Gerät mit AAD-Anmeldeinformationen bei Citrix Endpoint Management registrieren.

2. Sie eine Office 365-App starten und die AAD-Registrierung abschließen.
3. Sie das Konto aus der Microsoft Authenticator-App entfernen.
4. Sie eine Office 365-App starten und sich abmelden.

Als Workaround heben Sie die Registrierung des Geräts bei Citrix Endpoint Management auf und registrieren Sie es neu. [CXM-90235]

Bekannte Probleme in Citrix Endpoint Management 21.4.0

Eine erneute Registrierung von iOS-Geräten schlägt fehl, wenn es sich bei dem Benutzer, der die Registrierung versucht, nicht um den Azure Active Directory-Benutzer handelt, der ursprünglich für das Gerät registriert war. Heben Sie als Workaround vor einer erneuten Registrierung die Registrierung des ursprünglichen Benutzers in der Microsoft Authenticator-App auf dem Gerät auf. [CXM-90218]

Bekannte Probleme in Citrix Endpoint Management 21.2.0

Beim Hinzufügen von Citrix Secure Web als MDX-App für Android Enterprise kann verwaltetes Google Play die App nicht über die App-ID finden. Wenn Sie anstelle der App-ID nach "Citrix Secure Web" suchen, findet Google Play die App gefunden. Das Problem basiert auf einem Google-Fehler. [CXM-91991]

Beim Importieren des SSL-Listenerzertifikats kann ein Fehler auftreten. Verpacken Sie den Zertifikat-Schlüsselspeicher neu, und verwenden Sie hierfür die Schrittfolge in CTX-297153. [XMHELP-3346]

Bekannte Probleme in Citrix Endpoint Management 20.10.1

Wenn Sie ein Upgrade von on-premises Citrix ADC auf 13.0-64.35 oder höher ausführen und Citrix Endpoint Management nicht Workspace-fähig ist, schlagen der Single Sign-On bei Citrix Files oder die ShareFile-Domänen-URL fehl. Der Benutzer kann sich nicht anmelden. Dieser Fehler tritt nur in Browsern mit der Option **Mitarbeiteranmeldung** auf.

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

```
set vpn parameter SSO ON

bind vpn vs <vsName> -portalTheme X1
```

Weitere Informationen:

- Citrix ADC Release
- 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]

Bekannte Probleme in Citrix Endpoint Management 20.2.1

Nachdem Sie ShareFile in der Citrix Endpoint Management-Konsole mit einer ShareFile-URL konfiguriert haben, führt das Klicken auf die Schaltfläche **Verbindung testen** zu einem Fehler. Deaktivieren Sie zur Problemlösung die Multifaktorauthentifizierung für ShareFile. Weitere Informationen zu diesem Problem und dem Workaround finden Sie auf dieser Supportseite. [CXM-79240]

Bekannte Probleme in Citrix Endpoint Management 20.1.0

Wenn Sie in Citrix Cloud Benutzer zu einer Bibliothek hinzufügen, erhalten Sie in Citrix Endpoint Management eine Bestätigung, obwohl die Benutzer nicht hinzugefügt wurden. [CXM-73726]

Bekannte Probleme in Citrix Endpoint Management 19.11.0

MDX- und öffentliche Apps können nicht von der Konsole gelöscht werden. Als Workaround wählen Sie die App aus, die Sie löschen möchten, und klicken Sie dann auf **Bearbeiten**. Deaktivieren Sie **Android Enterprise** und wählen Sie eine beliebige andere Plattform aus der Plattformliste aus. Speichern Sie die App. Anschließend können Sie die App löschen. [CXM-74468]

Bekannte Probleme in Citrix Endpoint Management 19.5.0

Beim Registrieren eines Citrix Ready Workspace Hub-Geräts muss die Ethernet-MAC-Adresse (eth0) in der Positivliste definiert werden, sonst schlägt die Registrierung fehl. [CXM-43141]

Bekannte Probleme in Citrix Endpoint Management 19.4.1

Beim Durchlaufen der Optionen in der Windows-GPO-Geräterichtlinie mit der Tabulatortaste werden Optionsfelder und Kontrollkästchen übersprungen. [CXM-58277]

Bekannte Probleme in Citrix Endpoint Management 19.2.1

Wenn Sie die Registrierung eines Android Enterprise-Unternehmens durch Löschen über die Google Admin-Konsole aufheben, kann das Unternehmen möglicherweise nicht neu registriert werden. Verwenden Sie immer die Citrix Endpoint Management-Konsole, um die Registrierung eines Android

Enterprise-Unternehmens aufzuheben, wie unter Registrierung für Android Enterprise-Unternehmen aufheben beschrieben. Google Workspace-Kunden folgen den Anweisungen unter Registrierung für Android Enterprise-Unternehmen aufheben. [CXM-62709] [CXM-62950]

Bekannte Probleme in Citrix Endpoint Management 19.2.0

Wenn Sie beim Erstellen einer öffentlichen Store-App in Citrix Endpoint Management 10.18.3 auf der Seite "App-Einstellungen"für iPad auf **Zurück** klicken, ohne nach Apps zu suchen, und dann auf **Weiter** klicken, tritt das folgende Problem auf. Die Navigationsschaltflächen reagieren nicht und ermöglichen keine App-Suche. Das Problem tritt bei der Erstellung öffentlicher Store-Apps für iOS oder Android auf. [CXM-46820]

Bekannte Probleme in Citrix Endpoint Management 10.19.1

Nachdem Sie den Registrierungsvorgang auf der Seite **Einstellungen > Android Enterprise** abgeschlossen haben, wird folgende Fehlermeldung angezeigt: `A configuration error occurred. Please try again`. Wenn Sie die Fehlermeldung schließen, wird Ihre Android Enterprise-Konfiguration gespeichert, die Einstellung für **Android Enterprise aktivieren** ist jedoch **Aus**. Reduzieren Sie die Anzahl der App-Kategorien auf maximal 30, um dieses Problem zu umgehen. [CXM-60899]

Bekannte Probleme in Citrix Endpoint Management 10.18.5

Wenn eine Chrome-App als erforderliche App für Chrome OS-Geräte konfiguriert war, mussten sich Benutzer u. U. abmelden und erneut anmelden, um die App zu installieren. Es handelte sich hierbei um den Google-Bug 76022819. [CXM-48060]

Bekannte Probleme in Citrix Endpoint Management 10.18.3

Nach dem Löschen eines Citrix Cloud-Administrators, der ein Gerät registriert hat: Citrix Endpoint Management aktualisiert die Benutzerrolle in der Citrix Endpoint Management-Konsole erst, nachdem der Administrator sich neu über die Citrix Secure Hub-App oder das Selbsthilfeportal angemeldet hat. [CXM-45730]

Bekannte Probleme in Citrix Endpoint Management 10.7.4

Wenn Sie Citrix Endpoint Management für Single Sign-On (SSO) über den Citrix-Identitätsanbieter mit Azure Active Directory konfigurieren und ein Citrix Endpoint Management-Administrator oder -Benutzer an den **Anmeldebildschirm von Azure Active Directory** weitergeleitet wird, wird dort die

Meldung “Sign-in page for Citrix Secure Hub”angezeigt. Die richtige Meldung lautet “Sign-in page for Citrix Endpoint Management console.”[CXM-42309]

Hinweise zu Drittanbietern

April 23, 2020

Citrix Endpoint Management enthält ggf. Software von Drittanbietern, die gemäß den im folgenden Dokument aufgeführten Bestimmungen lizenziert ist:

Citrix Endpoint Management: Hinweise zu Drittanbietern

Einstellung von Features und Plattformen

June 25, 2024

Die Ankündigungen in diesem Artikel bieten Ihnen frühzeitige Informationen über Features von Citrix Endpoint Management, die ausgemustert werden, sodass Sie rechtzeitig Geschäftsentscheidungen treffen können. 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 Produktlebenszyklussupport finden Sie unter Product Lifecycle Support Policy.

> **Wichtig:**
>
> Vielen Dank, dass Sie das Citrix Endpoint Management Analyzer Tool verwenden. Wir wissen das zu schätzen. Aufgrund unserer hohen Releasefrequenz ist dieses Tool nicht länger erforderlich. Der Service wird daher von Citrix am 31. März 2023 eingestellt. Verwenden Sie stattdessen die Konnektivitätsprüfungen, die in der Citrix Endpoint Management-Konsole oder in Citrix NetScaler Gateway verfügbar sind. Weitere Informationen finden Sie unter Konnektivitätsprüfungen.

Veraltete und entfernte Produkte und Features

Die in der folgenden Liste aufgeführten Features von Citrix Endpoint Management sind veraltet oder wurden entfernt:

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 Citrix Endpoint Management 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
Citrix Endpoint Management Government	Die Unterstützung für Citrix Endpoint Management Government wurde eingestellt.	Januar 2022	Juli 2022	Citrix Endpoint Management Standard-Edition
SafetyNet Attestation API	Android SafetyNet-Nachweis wird gemäß Ankündigung von Google nicht mehr unterstützt.	Juli 2023	November 2023	Play Integrity API
Chrome OS	Unterstützung für Chrome OS wurde eingestellt.	Juli 2022	Mai 2023	Keine Alternative
tvOS	Unterstützung für tvOS wird eingestellt.	Juli 2022	Mai 2023	Keine Alternative
Windows Information Protection (WIP)	Unterstützung für Windows Information Protection ist laut der Ankündigung von Microsoft veraltet.	August 2022	Oktober 2022	Keine Alternative

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Citrix Endpoint Management Analyzer	Die Unterstützung für das Citrix Endpoint Management Analyzer-Tool läuft aus.	Juli 2022	Ziel: 31. März 2023	Keine Alternative
Workspace Hub-Geräteverwaltung	Die Unterstützung für Citrix Ready Workspace Hub-Geräte läuft aus.	Januar 2022	Juni 2022	Keine Alternative
Microsoft Store für Unternehmen	Unterstützung für Microsoft Store für Unternehmen wurde eingestellt. Microsoft unterstützt diese Plattform nicht mehr. Weitere Informationen finden Sie in der Microsoft-Dokumentation.	Juli 2021	Ziel: März 2023	Keine Alternative
Samsung SAFE	Unterstützung für Samsung SAFE wurde eingestellt.	Januar 2022	Juni 2022	Verwenden Sie Android Enterprise.
Benutzerdefiniertes XML für Zebra	Unterstützung für benutzerdefiniertes XML auf Zebra-Geräten wurde eingestellt.	Januar 2022	Juni 2022	Verwenden Sie die verwaltete Android Enterprise-Konfiguration.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
PKI-Identitäten: Generic, Symantec PKI, DigiCert und Entrust	Die Unterstützung für Generic-, DigiCert Managed- und Entrust Adapter-PKI-Entitäten läuft aus.	Juni 2021	Januar 2022	Keine Alternative
Android für Workspace	Unterstützung für Android for Workspace ist veraltet	Januar 2022	April 2022	Keine Alternative
SMS-Gateway des Netzbetreibers	Einstellung der Unterstützung für Nexmo SMS-Gateway-Benachrichtigungen	Januar 2022	April 2022	Verwenden von SMTP-Serverbenachrichtigungen
Mobilfunkanbieter	Einstellung der Unterstützung für Mobilfunkanbieterschnittstelle zum Abfragen von Blackberry- und anderen Exchange ActiveSync-Geräten und Auslösen von Vorgängen	Januar 2022	April 2022	Keine Alternative

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
MDX Toolkit	Einstellung der Unterstützung für das MDX Toolkit zugunsten des MAM-SDK. In der Übergangsphase können Sie mit MDX umschlossene und MAM SDK-Apps verwenden.	März 2020	Juli 2023	Verwenden Sie zur weiteren Verwaltung Ihrer Unternehmen-sanwendungen das MAM SDK.
RBAC-Rolle - Registrierung für gemeinsam genutzte Geräte und Registrierung für COSU-Geräte	Einstellung der Unterstützung für vordefinierte Einstellungen für die rollenbasierte Zugriffssteuerung (RBAC) für “Registrierung für gemeinsam genutzte Geräte” und “Registrierung für COSU-Geräte”.	Juli 2021	Dezember 2021	Konfigurieren Sie iOS-Geräte über Apple School Manager oder Apple Business Manager. Konfigurieren Sie (dedizierte) COSU-Geräte mit Android über Registrierungsprofile.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
“Automatische Verbindung mit Wi-Fi Sense-Hotspots zulassen”für Windows-Geräte.	Entfernen Sie die Unterstützung für die Einschränkung “Automatische Verbindung mit Wi-Fi Sense-Hotspots zulassen”für Windows 10-Geräte. Dieses Feature wird von Windows 10 nicht mehr unterstützt. Informationen hierzu finden Sie in der Dokumentation von Microsoft.	Oktober 2021	Februar 2022	Keine Alternative
MDX: alternativer Gatewayserver	Einstellung der Unterstützung für die verstärkte Authentifizierung für iOS- und Android-Geräte.	März 2020	September 2021	Keine Alternative
MDX: Micro-VPN (Volltunnelmodus)	Veraltet: vollständiger VPN-Tunnel für iOS- und Android-Geräte.	März 2020	September 2021	Verwenden Sie den MAM SDK Web SSO-Modus oder erstellen Sie eine Pro-App-VPN-Richtlinie mit dem Verbindungstyp “Citrix SSO”.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
MDX: PAC-Dateiunterstützung	Unterstützung für PAC-Datei (Proxy Automatic Configuration) mit einem vollständigen VPN-Tunnel für iOS- und Android-Geräte eingestellt.	März 2020	September 2021	Verwenden Sie NetScaler 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	September 2021	Verwenden Sie für Android Enterprise gemeinsam genutzte Geräte, die als dedizierte Geräte registriert sind. Verwenden Sie für iOS Apple School Manager oder GroundControl.
Android - Sony	Die Android-Unterstützung auf Sony-Geräten und in Sony-spezifischen Richtlinien läuft ab.	Januar 2021	Februar 2022	Verwenden Sie Android Enterprise.
Android - HTC	Die Android-Unterstützung auf HTC-Geräten und in HTC-spezifischen Richtlinien läuft ab.	Januar 2021	Februar 2022	Verwenden Sie Android Enterprise.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Android - Amazon	Die Android-Unterstützung für Amazon-Geräte und Amazon-spezifische Richtlinien läuft ab.	Januar 2021	Februar 2022	Verwenden Sie Android Enterprise.
Knox Mobile Enrollment (Legacy-Geräteadmin)	Unterstützung für Knox Mobile Enrollment (KME) im Legacy-Geräteadmin-Modus für alle Android-Versionen läuft aus.	1. Mai 2021	September 2021	Verwenden Sie KME für die Registrierung im Android Enterprise-Modus. Android Enterprise wird von Android 8, 9, 10, 11 unterstützt.
Registrierungsmodus “Hochsicherheit”	Das Generieren von Registrierungseinladungen mit dem Registrierungssicherheitsmodus **Hohe Sicherheit** ist veraltet.	Juli 2021	Februar 2022	Eine Liste der unterstützten Registrierungssicherheitsmodi finden Sie unter Registrierungseinladungen.
Abgeleitete Anmeldeinformationen	Die Unterstützung für abgeleitete Anmeldeinformationen und die Citrix Derived Credential Manager-App läuft aus.	März 2021	Dezember 2021	Unter iOS finden Sie eine Liste der für iOS unterstützten Authentifizierungstypen.

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	März 2021	Verwenden Sie stattdessen Port 443. Siehe Netzwerk- und Firewall-Anforderungen.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
MDX Service	Einstellung der Unterstützung für MDX Service zugunsten des MAM-SDK. In der Übergangsphase können Sie sowohl mit dem MDX Toolkit umschlossene Apps als auch MAM SDK-Apps verwenden.	März 2020	September 2021	Verwenden Sie zum Umschließen von Unternehmen-sapps weiterhin das MDX Toolkit.
Einrichten der Registrierungsein-ladung im Selbsthilfeportal	Das Generieren von Registrierungsein-ladungen durch Benutzer im Selbsthilfeportal wird nicht mehr unterstützt.	Juli 2021	Juli 2021	Wenden Sie sich an Ihren Administrator, um Registrierung-seinladungen in der Citrix Endpoint Management-Konsole zu generieren.
Einrichten von Registrierungsein-ladungen	Unterstützung für Verwendung einer Geräte-IMEI, Seriennummer oder UDID zum Generieren einer Registrierungsein-ladung läuft aus.	April 2021	Juli 2021	Wenn Sie eine Registrierungsein-ladung erstellen, konfigurieren Sie die verfügbaren Einstellungen unter **Verwalten > Registrierung-seinladungen** in der Citrix Endpoint Management-Konsole.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Signaturalgorithmen für zertifikatbasierte Authentifizierung (Nicht-FIPS und schwache Verschlüsselungsverfahren)	Die Unterstützung für folgende Signaturalgorithmen ist veraltet: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRSA, RIPEMD128withRSA, RIPEMD256withRSA.	Mai 2020	Juni 2021	Wenn Sie in der Citrix Endpoint Management-Konsole eine Zertifikatsignieranforderung für einen Anmeldeinformationsanbieter erstellen (**Einstellungen > Anmeldeinformationsanbieter > Zertifikatsignieranforderung**), wählen Sie ein stärkeres Verschlüsselungsverfahren.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Mobile Apps und Workspace-Apps von Citrix für Android 7.x und iOS 12.x	Veraltet: Unterstützung für Citrix Secure Hub, Citrix Secure Mail, Citrix Secure Web und Citrix Workspace-App für Android 7.x und iOS 12.x.	April 2021	Juni 2021	Verwenden Sie mindestens die aktuelle Version und die Vorversion jeder gängigen Betriebssystemplattform. Ältere Geräte bleiben registriert. Legacygeräte werden jedoch nicht von Citrix getestet und erhalten keinen technischen Support.
Unterstützung für RSA-Softwaretoken in Android	Die Unterstützung für das direkte Importieren von RSA-Softtoken in Citrix 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 NetScaler Gateway-Authentifizierung verwenden.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Internet Explorer 11	Die Unterstützung von Internet Explorer für die Citrix Endpoint Management-Konsole läuft aus.	Januar 2021	Januar 2021	Verwenden Sie die neueste Version folgender Webbrowser: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Gateway-Konfigurationsprüfung in Citrix Endpoint Management Analyzer	Die Unterstützung der Gateway-Konfigurationsprüfung läuft aus.	November 2020	November 2020	Prüfen Sie mit Citrix Insight Services in Analyzer, ob Ihre Citrix ADC-Konfigurationen bereit sind, Citrix Endpoint Management bereitzustellen.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Apps, die auf Android Enterprise-Geräten für den Modus “Legacygeräteverwaltung” 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.
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
Android TouchDown	DigiCert hat die Unterstützung für Android TouchDown eingestellt. Citrix hat die Seite zur Android TouchDown-Plattform aus der Exchange-Geräterichtlinie entfernt.	Juli 2018	November 2020	Empfehlung: Verwenden Sie Citrix Secure Mail.
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.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
MDX-Verschlüsselung	Das MDX-Verschlüsselungsfeature in der Citrix Endpoint Management-Konsole ist veraltet.	Oktober 2019	September 2020	Aktivieren Sie die iOS- oder Android-Plattformverschlüsselung über unsere Verschlüsselungsverwaltung mit zusätzlicher Compliance-Überprüfung. Sie müssen die Migration weg von der MDX-Verschlüsselung bis Juli 2020 testen und planen.
Windows Mobile/CE	Die Unterstützung für Windows Mobile/CE-Geräte läuft aus.	April 2018	September 2020	Verwenden Sie Desktops und Laptops mit Windows 10.
Samsung SEAMS-Container	Unterstützung für den Samsung SEAMS-Container läuft aus.	Juni 2020	August 2020	Verwenden Sie Android Enterprise.
Remotesupport	Der Remotesupportclient ist veraltet.	Januar 2019	August 2020	Keine Alternative

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 Citrix Secure Hub, Citrix Secure Mail, Citrix 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 Betriebssystemplattform. Ältere Geräte bleiben registriert. Legacygeräte werden jedoch nicht von Citrix getestet und erhalten keinen technischen Support.
Citrix Secure Hub Network Extensions für iOS	Veraltet: Network Extension-Framework zur Anpassung der Netzwerkfeatures für iOS-Geräte. Citrix Secure Hub Release 20.3.0	October 2018	März 2020	Keine Alternative
API-Anmeldung mit lokalen Konten	Administratoren können sich nicht länger mit einem lokalen Konto an der REST-API anmelden.	Oktober 2020		Administratoren können sich mit einem Citrix Cloud-Konto anmelden. Siehe REST-API.

Element	Beschreibung	Einstellung der Unterstützung angekündigt	Entfernt	Alternative
Selbstsignierte SSL-Zertifikate (Secure Sockets Layer)	Die Unterstützung für selbstsignierte SSL-Zertifikate ist für alle Geräteplattformen veraltet.	Mai 2020		Ersetzen Sie Ihr vorhandenes selbst signiertes Zertifikat durch ein vertrauenswürdiges SSL-Zertifikat einer etablierten Zertifizierungsstelle (ZS).

Systemanforderungen

March 11, 2024

Während Sie darauf warten, dass Citrix das Provisioning von Citrix Endpoint Management durchführt, bereiten Sie Ihre Citrix Endpoint Management-Bereitstellung vor, indem Sie den Cloud Connector installieren. Citrix hostet zwar Ihre Citrix Endpoint Management-Lösung, für die Kommunikation und Ports ist jedoch etwas Setup erforderlich. Bei diesem Setup wird die Citrix Endpoint Management-Infrastruktur mit Unternehmensdiensten wie Active Directory verbunden.

Anforderungen für Cloud Connector

Citrix verwendet Cloud Connector, um die Citrix Endpoint Management-Architektur in Ihre vorhandene Infrastruktur zu integrieren. Cloud Connector integriert folgende Ressourcenstandorte über Port 443 in den Citrix Endpoint Management: LDAP, PKI Server, interne DNS-Abfragen und Citrix Workspace-Enumeration.

- Mindestens zwei dedizierte Windows Server-Maschinen, die zu Ihrer Active Directory-Domäne gehören. Dies können physikalische oder virtuelle Maschinen sein. Die Maschine, auf der Sie den Connector installieren, muss mit der UTC-Zeit synchronisiert sein, um eine korrekte Installation und einen fehlerfreien Betrieb zu gewährleisten. Eine vollständige Liste der aktuellen

Anforderungen finden Sie in den Bereitstellungsmaterialien, die Sie von Ihrem Citrix Account-Team erhalten.

Der Onboarding-Assistent führt Sie durch die Installation des Cloud Connectors auf diesen Maschinen.

- Weitere Informationen zu Plattformsystemanforderungen finden Sie unter Citrix Cloud Connector.

Unterstützte Funktionsebenen von Active Directory

Der Citrix Cloud Connector unterstützt die folgenden Funktionsebenen für Active Directory-Gesamtstrukturen und -Domänen für eine Verwendung mit Citrix Endpoint Management:

Funktionsebene	Domänenfunktionsebene	Unterstützte Domänencontroller
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019
Windows Server 2016	Windows Server 2019	Windows Server 2019
Windows Server 2019	Windows Server 2019	Windows Server 2019

> **Hinweis:**
>
> Windows Server 2012 R2, 2012 und 2008 R2 werden nicht mehr unterstützt, da sie das Ende des Lebenszyklus erreicht haben. Weitere Informationen finden Sie in der Dokumentation zum Lebenszyklus von Microsoft-Produkten.

Anforderungen für NetScaler Gateway

Citrix Endpoint Management erfordert für folgende Szenarios, dass NetScaler Gateway an Ihrem Ressourcenstandort installiert ist:

- Sie benötigen ein Micro-VPN, damit branchenspezifische Apps auf interne Netzwerkressourcen zugreifen können. Die Apps sind mit der Citrix MDX-Technologie umschlossen. Das Micro-VPN muss über NetScaler Gateway eine Verbindung zu internen Backend-Infrastrukturen herstellen.
- Sie planen, mobile Produktivitätsapps von Citrix wie Citrix Secure Mail zu verwenden.
- Sie planen, Citrix Endpoint Management mit Microsoft Endpoint Manager zu integrieren.

Anforderungen:

- Domänenauthentifizierung (LDAP)

- NetScaler Gateway 12.1 oder höher mit einer Plattform-/universellen Lizenz

Weitere Informationen finden Sie unter Lizenzierung.

- Öffentliches SSL-Zertifikat

Weiter Informationen finden Sie unter Erstellen und Verwenden von SSL-Zertifikaten auf einem Citrix ADC-Gerät.

- Nicht verwendete, öffentliche IP-Adresse für den virtuellen NetScaler Gateway-Server
- Öffentlich auflösbarer FQDN für den virtuellen NetScaler Gateway-Server
- Zwischen- und Stammzertifikat für cloudgehostetes Citrix Endpoint Management (im Skriptpaket enthalten)
- Nicht verwendete, interne, private IP-Adresse für den Proxy-Load Balancer
- Informationen zu Portanforderungen finden Sie weiter unten unter Portanforderungen für NetScaler Gateway.
- Integration von Citrix Endpoint Management in Microsoft Endpoint Manager
- Bereitstellen der Citrix ADC VPX-Instanz unter Microsoft Azure

Weitere Informationen zu NetScaler Gateway-Anforderungen finden Sie in den Bereitstellungsmaterialien, die Sie von Ihrem Citrix Account-Team erhalten.

Informationen zu den Android Enterprise-Anforderungen finden Sie im Abschnitt Android Enterprise.

Anforderungen für Citrix Files

Die Citrix Files-Dienste zur Dateisynchronisierung und -freigabe sind im Citrix Endpoint Management Premium Service-Angebot enthalten. Der Speicherzonencontroller erweitert den Cloudspeicher von Citrix Files SaaS (Software as a Service) durch privaten Datenspeicher für Ihr Citrix Files-Konto.

Anforderungen an den Speicherzonencontroller:

- Eine dedizierte physische oder virtuelle Maschine
- Windows Server 2012 R2 (Datacenter, Standard oder Essentials), Windows Server 2016, Windows Server 2019 oder Windows Server 2022
- 2 vCPUs
- 4 GB RAM
- 50 GB Festplattenspeicherplatz
- Serverrollen für den Webserver (IIS):
  - Anwendungsentwicklung: ASP. NET 4.5.2

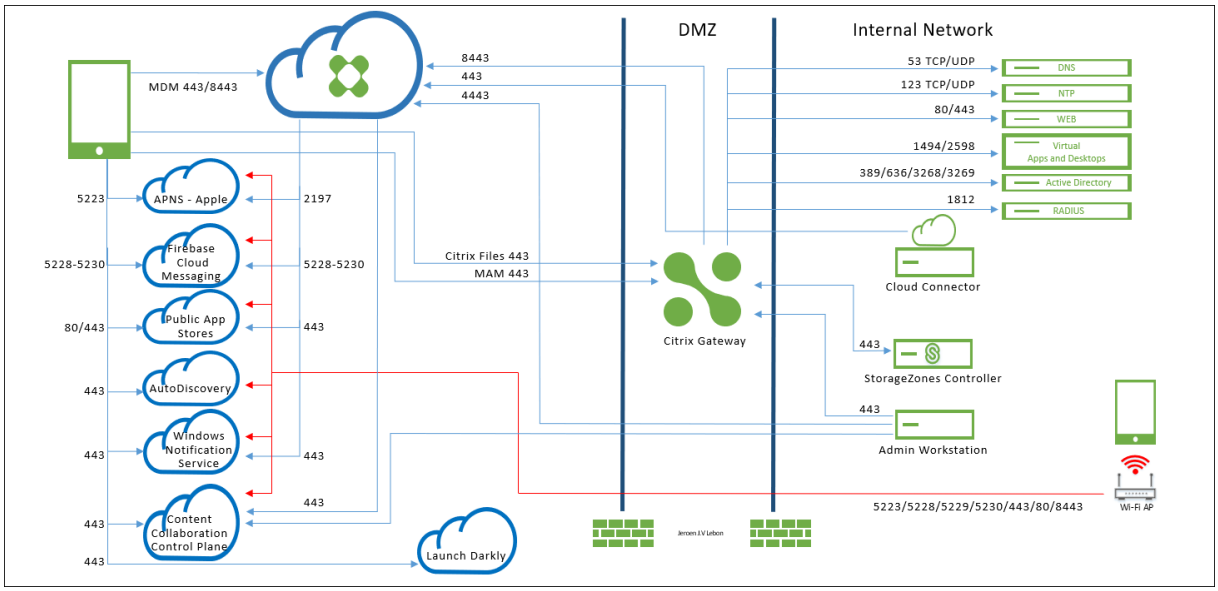
- Sicherheit: Basic-Authentifizierung
- Sicherheit: Windows-Authentifizierung

Plattformanforderungen für Citrix Files

- Der Citrix Files-Installer erfordert Administratorrechte auf dem Windows Server
- Administratorbenutzername für Citrix Files

Portanforderungen

Damit Geräte und Apps mit Citrix Endpoint Management kommunizieren können, öffnen Sie bestimmte Ports in den Firewalls. Das folgende Diagramm zeigt den Datenfluss für Citrix Endpoint Management.



Nachfolgend sind die Ports aufgeführt, die Sie öffnen müssen. Informationen zu den von mobilen Produktivitätsapps verwendeten URLs finden Sie unter Verwalten von Featureflags.

Portanforderungen für NetScaler Gateway

Öffnen Sie folgende Ports, damit Benutzer über NetScaler Gateway Verbindungen von Citrix Secure Hub und Citrix Workspace mit diesen Komponenten herstellen können:

- Citrix Endpoint Management
- StoreFront
- Andere interne Netzwerkressourcen, z. B. Intranet-Websites

Weitere Informationen zu NetScaler Gateway finden Sie unter Configuring Settings for Your Citrix Endpoint Management Environment in der NetScaler Gateway-Dokumentation. Informationen

zu IP-Adressen finden Sie unter So verwendet NetScaler Gateway IP-Adressen in der NetScaler Gateway-Dokumentation.

TCP-Port	Beschreibung	Quelle	Ziel
53 (TCP und UDP)	Wird für DNS-Verbindungen verwendet.	NetScaler Gateway-SNIP	DNS-Server
80/443	NetScaler Gateway leitet die Micro-VPN-Verbindung mit der internen Netzwerksressource durch die zweite Firewall.	NetScaler Gateway-SNIP	Intranet-Websites
123 (TCP und UDP)	Wird für Network Time Protocol-Dienste (NTP) verwendet.	NetScaler Gateway-SNIP	NTP-Server
389	Wird für unsichere LDAP-Verbindungen verwendet.	NetScaler Gateway-NSIP (oder, wenn Sie einen Load Balancer verwenden, SNIP)	LDAP-Authentifizierungsserver oder Microsoft-Active Directory
443	Wird für Verbindungen zu StoreFront von Citrix Workspace zu Citrix Virtual Apps and Desktops verwendet.	Internet	NetScaler Gateway
443	Wird für Verbindungen mit Citrix Endpoint Management zur Bereitstellung von Web-, Mobil- und SaaS-Apps verwendet.	Internet	NetScaler Gateway

TCP-Port	Beschreibung	Quelle	Ziel
443	Wird für die Cloud Connector-Kommunikation verwendet –LDAP-, DNS-, PKI- und Citrix Workspace-Enumeration	Cloud Connector-Server	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.blob.core.windows.net/, https://*.servicebus.windows.net
443	Für den Zugriff auf das Selbsthilfeportal von Citrix Endpoint Management (sofern aktiviert) über den Browser.	Zugriffspunkt (Browser)	Citrix Endpoint Management (https://<sitename>/zdm/shp)
636	Wird für sichere LDAP-Verbindungen verwendet.	NetScaler Gateway-NSIP (oder, wenn Sie einen Load Balancer verwenden, SNIP)	LDAP-Authentifizierungsserver oder Active Directory
1494	Wird für ICA-Verbindungen mit Windows-basierten Anwendungen im internen Netzwerk verwendet. Citrix empfiehlt, diesen Port geöffnet zu lassen.	NetScaler Gateway-SNIP	Citrix Virtual Apps and Desktops
1812	Wird für RADIUS-Verbindungen verwendet.	NetScaler Gateway-NSIP	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.	NetScaler Gateway-SNIP	Citrix Virtual Apps and Desktops
3269	Wird für sichere LDAP-Verbindungen mit dem globalen Microsoft-Katalog verwendet.	NetScaler Gateway-NSIP (oder, wenn Sie einen Load Balancer verwenden, SNIP)	LDAP-Authentifizierungsserver oder Active Directory
4443	Wird von Administratoren für den Zugriff auf die Citrix Endpoint Management-Konsole über einen Browser verwendet.	Zugriffspunkt (Browser)	Citrix Endpoint Management
8443	Wird für die Registrierung, App-Store und die Mobilanwendungsverwaltung (MAM) verwendet.	NetScaler Gateway-SNIP	Citrix Endpoint Management
8443	STA-Port (Secure Ticket Authority) für das Citrix Secure Mail-Authentifizierungstoken	NetScaler Gateway-SNIP	Citrix Endpoint Management

Netzwerk- und Firewall-Anforderungen

Damit Geräte und Apps mit Citrix Endpoint Management kommunizieren können, öffnen Sie bestimmte Ports in den Firewalls. Diese Ports sind in den folgenden Tabellen aufgelistet.

Öffnen der Ports vom internen Netzwerk zu Citrix Cloud:

TCP-Port	Quell-IP	Beschreibung	Ziel	Ziel-IP
443		Cloud Connector	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.sharefile.com, https://cwsproduction.blob.core.windows.net/downloads, https://*.servicebus.windows.net	
443		Verwaltungskonsole	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.citrix.com, https://cwsproduction.blob.core.windows.net/downloads	

TCP-Port	Quell-IP	Beschreibung	Ziel	Ziel-IP
443		Zugriff auf das Selbsthilfeportal von Citrix Endpoint Management über einen Browser (bei aktiviertem Portal)	Citrix Endpoint Management	
4443		Citrix Endpoint Management-Konsolenzugriff über einen Browser	Citrix Endpoint Management	

Öffnen der Ports vom Internet zur DMZ:

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
443	Citrix Endpoint Management-Clientgerät		NetScaler Gateway-IP	
443	Citrix Endpoint Management-Clientgerät		NetScaler Gateway VIP	
443	Öffentliche IP für Citrix Files	CTX208318	NetScaler Gateway VIP	

Öffnen der Ports von der DMZ zum internen Netzwerk:

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
389 oder 636	NetScaler Gateway-NSIP		Active Directory-IP	
53 (UDP)	NetScaler Gateway-NSIP		DNS-Server-IP	

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
443	NetScaler Gateway-SNIP		Exchange (EAS) Server-IP	
443	NetScaler Gateway-SNIP		Interne Web-Apps/Webdienste	
443	NetScaler Gateway-SNIP		Speicherzonencontroller-IP	

Öffnen der Ports vom internen Netzwerk zur DMZ:

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
443	Administrator-Client		NetScaler Gateway-NSIP	

Öffnen der Ports vom internen Netzwerk zum Internet:

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
443	Exchange (EAS) Server-IP		Citrix Endpoint Management Push-Benachrichtigungslistener (1)	
443	Speicherzonencontroller-IP		Citrix Files-Steuerungsebene	CTX208318

(1)us-east-1.mailboxlistener.xm.citrix.com, eu-west-1.mailboxlistener.xm.citrix.com, ap-southeast-1.mailboxlistener.xm.citrix.com

Öffnen der Ports vom Wi-Fi des Unternehmens zum Internet:

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
8443 / 443	Citrix Endpoint Management-Clientgerät		Citrix Endpoint Management	

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
5223	Citrix Endpoint Management-Clientgerät		APNS-Server von Apple	17.0.0.0/8
5228	Citrix Endpoint Management-Clientgerät		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5229	Citrix Endpoint Management-Clientgerät		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5230	Citrix Endpoint Management-Clientgerät		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
443	Citrix Endpoint Management-Clientgerät		Firebase Cloud Messaging	fcm.googleapis.com
443	Citrix Endpoint Management-Clientgerät		Windows-Pushbenachrichtigungsdienst	*.notify.windows.com
443 / 80	Citrix Endpoint Management-Clientgerät		Apple iTunes App-Store	ax.apps.apple.com, *.mzstatic.com, vpp.itunes.apple.com

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
443 / 80	Citrix Endpoint Management-Clientgerät		Google Play	play.google.com, android.clients.google.com, android.l.google.com, android.com, google-analytics.com
443 / 80	Citrix Endpoint Management-Clientgerät		Microsoft App-Store	login.live.com, *.notify.windows.com
443	Citrix Endpoint Management-Clientgerät		Citrix Endpoint Management Autodiscoverydienst für iOS und Android	discovery.cem.cloud.us
443	Citrix Endpoint Management-Clientgerät		Citrix Endpoint Management AutoDiscovery Service für Windows	enterpriseenrollment.mycompany.com, discovery.cem.cloud.us
443	Speicherzonencontroller-IP		Citrix Files-Steuerungsebene	CTX208318
443	Citrix Endpoint Management-Clientgerät		Google Mobile Management, Google APIs, Google Play Store APIs	*.googleapis.com

TCP-Port	Beschreibung	Quell-IP	Ziel	Ziel-IP
443	Citrix Endpoint Management-Clientgerät		Konnektivitätsüberprüfungen für CloudDPC-Versionen vor 470. Für die ab Android N-MR1 durchgeführte Android-Konnektivitätsprüfung muss `https://www.google.com/generate_204` erreichbar sein oder das vorliegende Wi-Fi-Netzwerk auf eine erreichbare PAC-Datei verweisen.	`connectivitycheck.android.com`, `www.google.com`

Portanforderungen für die Verbindung mit dem AutoDiscovery Service

Diese Portkonfiguration gewährleistet, dass Android-Geräte mit Citrix Secure Hub für Android über das interne Netzwerk auf den Citrix Endpoint Management AutoDiscovery Service (ADS) zugreifen können. Der Zugriff auf den ADS ist zum Herunterladen von Sicherheitsupdates wichtig, die über diesen Dienst zur Verfügung gestellt werden.

> **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, müssen Sie folgende Voraussetzungen erfüllen:

- **Sammeln von Citrix Endpoint Management-Server- und NetScaler Gateway-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, um Zertifikatpinning zu aktivieren:** Bei diesem Prozess müssen Sie Ihre Zertifikate angeben.

Zertifikatpinning erfordert, dass Geräte vor der Registrierung eine Verbindung mit ADS herstellen. Damit wird sichergestellt, dass Citrix Secure Hub über die aktuellen Sicherheitsinformationen verfügt. Für eine Registrierung in Citrix 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 Citrix Secure Hub für Android/iOS möglich ist, öffnen Sie Port 443 für den folgenden FQDN:

FQDN	Port	IP- und Port-Nutzung
`discovery.cem.cloud.us`	443	Citrix Secure Hub – ADS-Kommunikation über CloudFront

Weitere Informationen zu unterstützten IP-Adressen finden Sie unter Cloud-based storage centers from AWS.

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.

App-Anforderungen

Citrix Endpoint Management unterstützt das Hinzufügen und Verwalten von bis zu 300 Apps. Wenn Sie dieses Limit überschreiten, wird das System instabil.

Citrix Endpoint Management-Kompatibilität

March 11, 2024

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 Juli 2023. Um die Verwaltung Ihrer Unternehmensapps fortzusetzen, müssen Sie das MAM-SDK integrieren.

- Mobile Produktivitätsapps

In diesem Artikel werden die Versionen der unterstützten Citrix Endpoint Management-Komponenten, die integriert werden können, zusammengefasst.

Die aktuellen Versionen von Citrix Secure Hub, MDX Toolkit und der mobilen Produktivitätsapps sind mit der aktuellen sowie den vorherigen beiden Versionen von Citrix Endpoint Management kompatibel.

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 Citrix Secure Hub erforderlich. Die beiden Vorgängerversionen der Apps sind mit der aktuellen Version von Citrix 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

Das MDX Toolkit erreicht das Ende des Lebenszyklus (EOL) im Juli 2023. 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 Citrix Endpoint Management-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

June 25, 2024

Dieser Artikel behandelt für Enterprise Mobility Management unterstützte Geräte mit Citrix Endpoint Management. Aufgrund von Plattformeinschränkungen und Sicherheitsfeatures werden von Citrix Endpoint Management nicht alle Funktionen auf allen Plattformen unterstützt:

Die neuesten Versionen der mobilen Produktivitätsapps finden Sie unter Unterstützung für mobile Produktivitätsapps.

> **Hinweis:**
>
> - Citrix unterstützt die aktuelle Version und die Vorversion jeder gängigen Betriebssystemplattform. Einige Features von Citrix Endpoint Management funktionieren nicht auf älteren Plattformen. Ankündigungen zu veralteten Funktionen finden Sie unter Einstellung von Features und Plattformen.
> - Citrix Endpoint Management unterstützt die Geräteverwaltung für Windows x86- und ARM-Geräte.

Liste der unterstützten Betriebssysteme

Citrix Endpoint Management unterstützt die folgenden Betriebssysteme:

- **Android:** 10.x, 11.x, 12.x, 13.x, 14.x

  Citrix empfiehlt ein Upgrade auf Android 10 und höher, bevor Sie Android Enterprise verwenden. Weitere Informationen finden Sie unter Überlegungen zu Android.

- **iOS:** 13.x, 14.x, 15.x, 16.x, 17.x

  Citrix Endpoint Management und Citrix Mobile Apps unterstützen derzeit nicht alle neuen Features, die für iOS 14.x, iOS 15.x, iOS 16.x und iOS 17.x verfügbar sind.

- **iPadOS:** 13.x, 14.x, 15.x, 16.x, 17.x

  Citrix Endpoint Management und Citrix Mobile Apps unterstützen derzeit nicht alle neuen Features von iPadOS 14.x, iPadOS 15.x, iPadOS 16.x und iPadOS 17.x.

- **macOS:** 11.x, 12.x, 13.x, 14.x

  Citrix Endpoint Management und Citrix Mobile Apps unterstützen derzeit nicht alle neuen Features, die für macOS 11, macOS 12, macOS 13 und macOS 14 verfügbar sind.

- **Windows 10- und Windows 11-Desktops und -Tablets:** (Nur MDM)

  - Windows 10 Professional und Windows 11 Professional
  - Windows 10 Enterprise und Windows 11 Enterprise
  - Windows 10 Education und Windows 11 Education
  - Windows IoT Enterprise

  Weitere Informationen zum Supportangebot für ein bestimmtes Betriebssystem finden Sie in der Microsoft-Dokumentation.

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. Lesen Sie auch diesen Citrix-Blog.

- Google stellt Device Administration APIs ein, was sich auf Geräte mit Android 10+ auswirkt. Die Registrierung von Android 10+-Geräten im Legacy-Geräteverwaltungsmodus schlägt fehl. Citrix unterstützt nicht die Registrierung von Android-Geräten im Geräteverwaltungsmodus.
- Citrix empfiehlt, Android Enterprise für Android-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.
- Lesen Sie auch diesen Citrix-Blog.

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 einen SAN enthalten, der dem Hostnamen entspricht.

Sprachunterstützung

December 1, 2023

Die mobilen Produktivitätsapps von Citrix und die Citrix Endpoint Management-Konsole wurden für andere Sprachen als Englisch angepasst. 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 Citrix Endpoint Management unterstützten Sprachen.

Citrix Endpoint Management-Konsole und das Selbsthilfeportal

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

Mobile Produktivitätsapps von Citrix

Ein X bedeutet, dass die App in der jeweiligen Sprache verfügbar ist.

iOS und Android

Sprache	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Japanisch	X	X	X	X	X	X
Vereinfachtes Chinesisch	X	X	X	X	X	X
Traditionelles Chinesisch	X	X	X	X	X	X
Französisch	X	X	X	X	X	X

Sprache	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Deutsch	X	X	X	X	X	X
Spanisch	X	X	X	X	X	X
Koreanisch	X	X	X	X	X	X
Portugiesisch	X	X	X	X	X	X
Niederländisch	X	X	X	X	X	X
Italienisch	X	X	X	X	X	X
Dänisch	X	X	X	X	X	X
Schwedisch	X	X	X	X	X	X
Hebräisch	X	X	X	X	X	Nur iOS
Arabisch	X	X	X	X	X	X
Russisch	X	X	X	X	X	X
Türkisch	X	X	Nur Android	-	-	-
Polnisch	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
Citrix Secure Hub	X	X
Citrix Secure Mail	X	X
Citrix Secure Web	X	X
QuickEdit	X	X

FIPS 140-2-Compliance

March 11, 2024

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.

Für alle kryptographischen Vorgänge an ruhenden und in der Übertragung befindlichen Daten unter iOS werden FIPS-validierte kryptographische Module verwendet. Unter Android werden für alle kryptographischen Vorgänge mit ruhenden Daten FIPS-validierte kryptographische Module von Citrix oder die kryptographischen Module der Plattform, die vom Gerätehersteller stammen, verwendet. 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 für Citrix Endpoint Management 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 NetScaler Gateway.

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

Citrix Endpoint Management

March 11, 2024

Citrix Endpoint Management ist eine Lösung zur einheitlichen Endpunktverwaltung (Unified Endpoint Management, UEM), die alle Apps und Endpunkte in einer einzigen Ansicht anzeigt und damit die Sicherheit und Produktivität steigert. Einen Überblick über UEM finden Sie in der technischen Kurzbeschreibung Citrix Endpoint Management in der Citrix Tech Zone.

Citrix Endpoint Management bietet Mobile Device Management (MDM) und Mobile App Management (MAM).

Die MDM-Funktionen von Citrix Endpoint Management bieten folgende Möglichkeiten:

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

Die MAM-Funktionen von Citrix Endpoint Management bieten folgende Möglichkeiten:

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

Eine Kombination aus MDM- und MAM-Funktionen bietet folgende Möglichkeiten:

- Verwalten eines vom Unternehmen bereitgestellten Geräts mithilfe von MDM
- Bereitstellen von Geräterichtlinien und Apps
- Abrufen eines Bestandsverzeichnisses
- Geräte löschen
- Bereitstellen mobiler Unternehmensapps
- Sperren von Apps und Löschen der Daten auf Geräten

In der folgenden Tabelle werden die für MDM, MAM und MDM+MAM unterstützten Citrix Endpoint Management-Features aufgeführt.

Feature (nach Plattform)	MDM (1)	MAM (2)	MDM+MAM
Android Enterprise:			
Unterstützung für die Geräteregistrierung	Ja	Ja	Ja
Unterstützung für die Domänenauthen-tifizierung	Ja	Nein	Ja
Unterstützung für die Authentifizierung mit Domäne und Sicherheitstoken	Nein	Nein	Ja
Unterstützung für die Clientzertifikatauthen-tifizierung	Nein	Ja	Ja

Feature (nach Plattform)	MDM (1)	MAM (2)	MDM+MAM
Unterstützung für die Clientzertifikatauthentifizierung plus Authentifizierung mit Domäne	Nein	Nein	Ja
Unterstützung für die Clientzertifikatauthentifizierung und für die Authentifizierung mit Sicherheitstoken	Nein	Nein	Ja
Unterstützung für Azure AD-Identitätsanbieter	Ja	Nein	Ja
Unterstützung für Okta-Identitätsanbieter	Ja	Nein	Ja
Single Sign-On bei nativen SaaS-Anwendungen	Ja	Nein	Ja
Unterstützung von Citrix Netzwerk für die Inhaltsübermittlung für Unternehmensapp	Ja	Ja	Ja
Unterstützung von Citrix Netzwerk für die Inhaltsübermittlung für MDX-App	Ja	Ja	Ja
Unterstützung gemeinsam genutzter Geräte durch Provisioning dedizierter Android Enterprise-Geräte (COSU-Geräte)	Ja	Nein	Ja
Android (Legacy):			
Unterstützung für die Geräteregistrierung	Ja	Ja	Ja

Feature (nach Plattform)	MDM (1)	MAM (2)	MDM+MAM
Unterstützung für die Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken	Nein	Nein	Ja
Unterstützung für die Clientzertifikatauthentifizierung	Nein	Ja	Ja
Unterstützung für die Clientzertifikatauthentifizierung plus Authentifizierung mit Domäne	Nein	Nein	Ja
Unterstützung für die Clientzertifikatauthentifizierung und für die Authentifizierung mit Sicherheitstoken	Nein	Nein	Ja
Unterstützung für Azure AD und Citrix-Identitätsanbieter	Ja	Nein	Ja
Unterstützung für Okta-Identitätsanbieter	Ja	Nein	Ja
Single Sign-On bei nativen SaaS-Anwendungen	Ja	Nein	Ja
Unterstützung von Citrix Netzwerk für die Inhaltsübermittlung für Unternehmensapp	Ja	Ja	Ja
Unterstützung von Citrix Netzwerk für die Inhaltsübermittlung für MDX-App	Ja	Ja	Ja
Chrome:			

Feature (nach Plattform)	MDM (1)	MAM (2)	MDM+MAM
Unterstützung für die Geräteregistrierung	Ja	Nein	Ja
Unterstützung für Authentifizierung mit Benutzernamen und Kennwort	Ja	Nein	Ja
iOS:			
Unterstützung für die Geräteregistrierung	Ja	Ja	Ja
Unterstützung für die Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken	Nein	Nein	Ja
Unterstützung für die Clientzertifikatauthen-tifizierung	Nein	Ja	Ja
Unterstützung für die Clientzertifikatauthen-tifizierung plus Authentifizierung mit Domäne	Nein	Nein	Ja
Unterstützung für Azure AD und Citrix-Identitätsanbieter	Ja	Nein	Ja
Unterstützung für Okta-Identitätsanbieter	Ja	Nein	Ja
Single Sign-On bei nativen SaaS-Anwendungen	Ja	Nein	Ja
Unterstützung von Citrix Netzwerk für die Inhaltsübermittlung für Unternehmensapp	Ja	Ja	Ja

Feature (nach Plattform)	MDM (1)	MAM (2)	MDM+MAM
Unterstützung von Citrix Netzwerk für die Inhaltsübermittlung für MDX-App	Ja	Ja	Ja
Integration von Apple Bildung	Ja	Nein	Ja
macOS:			
Unterstützung für die Geräteregistrierung	Ja	Nein	Nein
Unterstützung für Domäne oder Domäne plus Einmalkennwort	Ja	Nein	Nein
Unterstützung für Einladungs-URL + Einmalkennwort	Ja	Nein	Nein
Windows:			
Unterstützung für die Geräteregistrierung	Ja	Nein	Nein
Automatische Registrierung von Windows 10- und Windows 11-Geräten mit der Citrix Workspace-App	Ja	Nein	Nein
Unterstützung für die Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken	Ja	Nein	Nein
Unterstützung für die Clientzertifikatauthen-tifizierung	Ja	Nein	Nein

Feature (nach Plattform)	MDM (1)	MAM (2)	MDM+MAM
Unterstützung für die Clientzertifikatauthen-tifizierung plus Authentifizierung mit Domäne	Ja	Nein	Nein
Verbundauthentifizierung über Azure AD oder Citrix-Identitätsanbieter	Ja	Nein	Nein
Unterstützung von Citrix Netzwerk für die Inhaltsübermittlung für Unternehmensapp	Ja	Nein	Nein
Integration von Workspace Environment Management (3)	Ja	Nein	Nein

> **Hinweise:**
>
> (1) Die Bereitstellungsreihenfolge gilt nur für Geräte in einer Bereitstellungsgruppe mit einem für MDM konfigurierten Registrierungsprofil.
>
> (2) Die MAM-Registrierung erfordert NetScaler Gateway.
>
> (3) Die Integration von Workspace Environment Management (WEM) ermöglicht den Zugriff auf MDM-Features auf vielfältigen Windows-Betriebssystemen.

Weitere Informationen finden Sie unter Verwaltungsmodi.

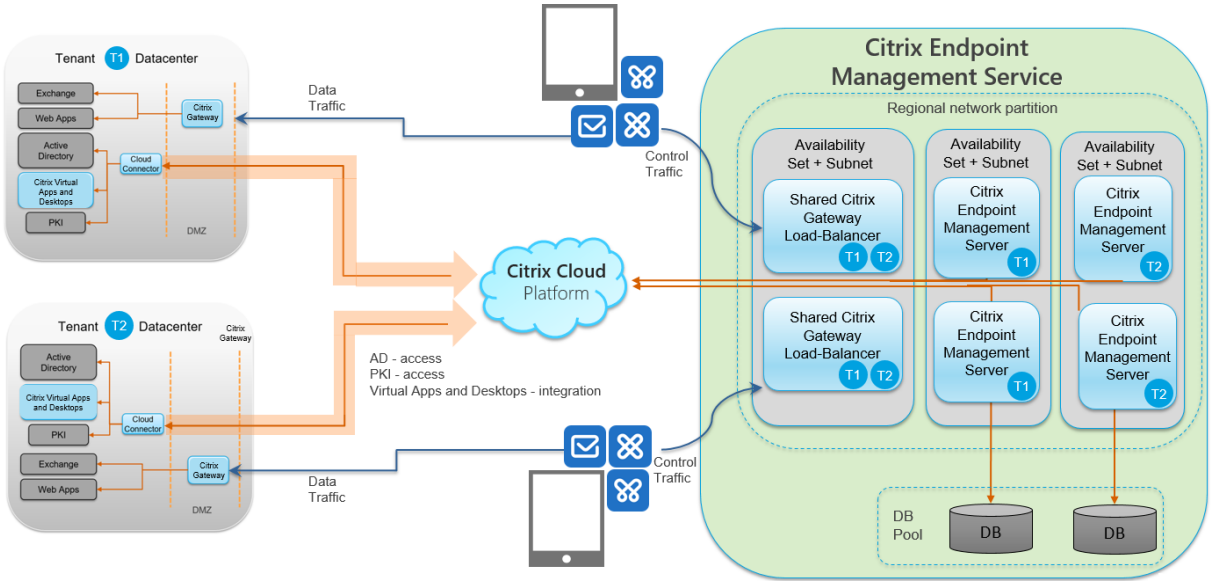
Architektur

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

- NetScaler Gateway ermöglicht Benutzern Remotezugriff auf mobile Apps und überwacht Benutzergerätetypen.

- In Citrix Endpoint Management können Sie diese Apps und Geräte verwalten.

Das folgende Diagramm zeigt eine allgemeine Übersicht über die Architektur einer Citrix Endpoint Management-Cloudbereitstellung und ihre Integration in das Datencenter:



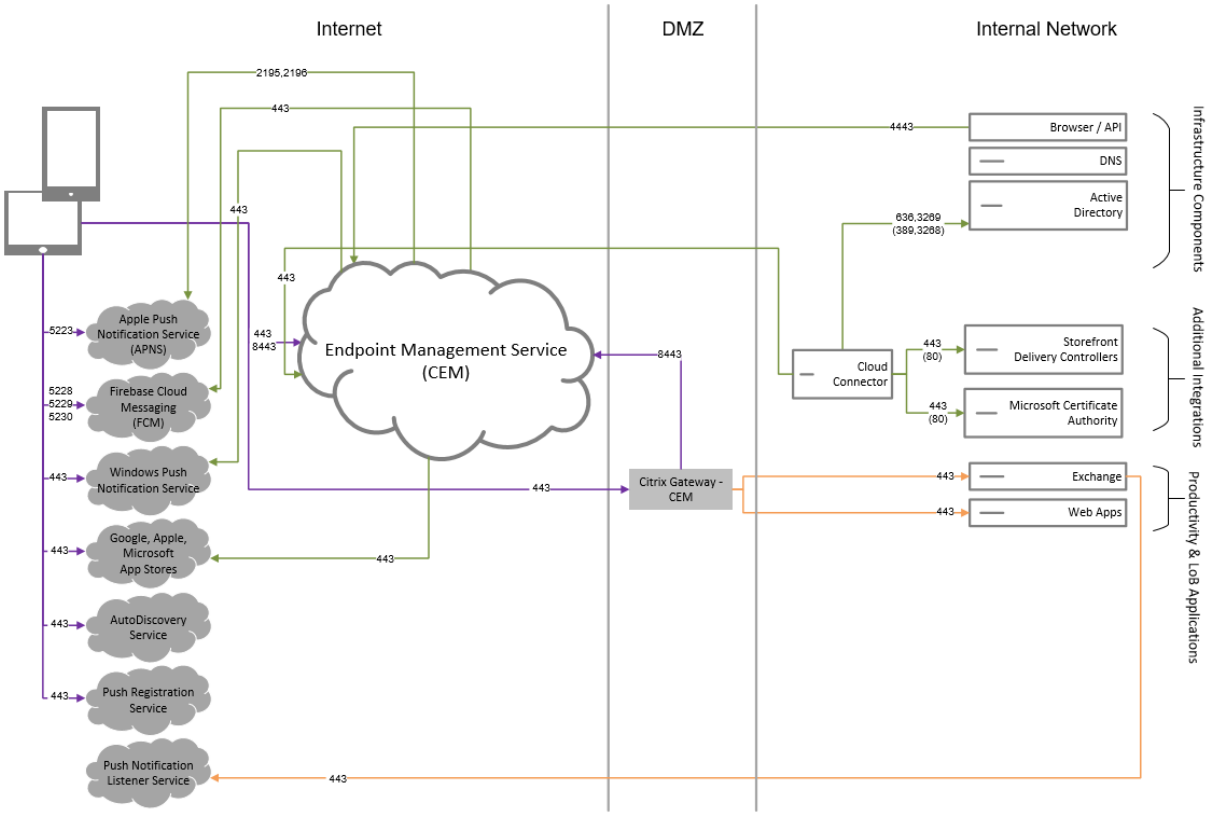
Die folgenden Unterabschnitte enthalten Referenzarchitekturdiagramme für:

- Citrix Endpoint Management
- Optionale Komponenten wie eine externe Zertifizierungsstelle, einen Citrix Endpoint Management-Connector für Exchange ActiveSync und einen Datenfluss mit Citrix Endpoint Management MDM+MAM und Intune MAM.

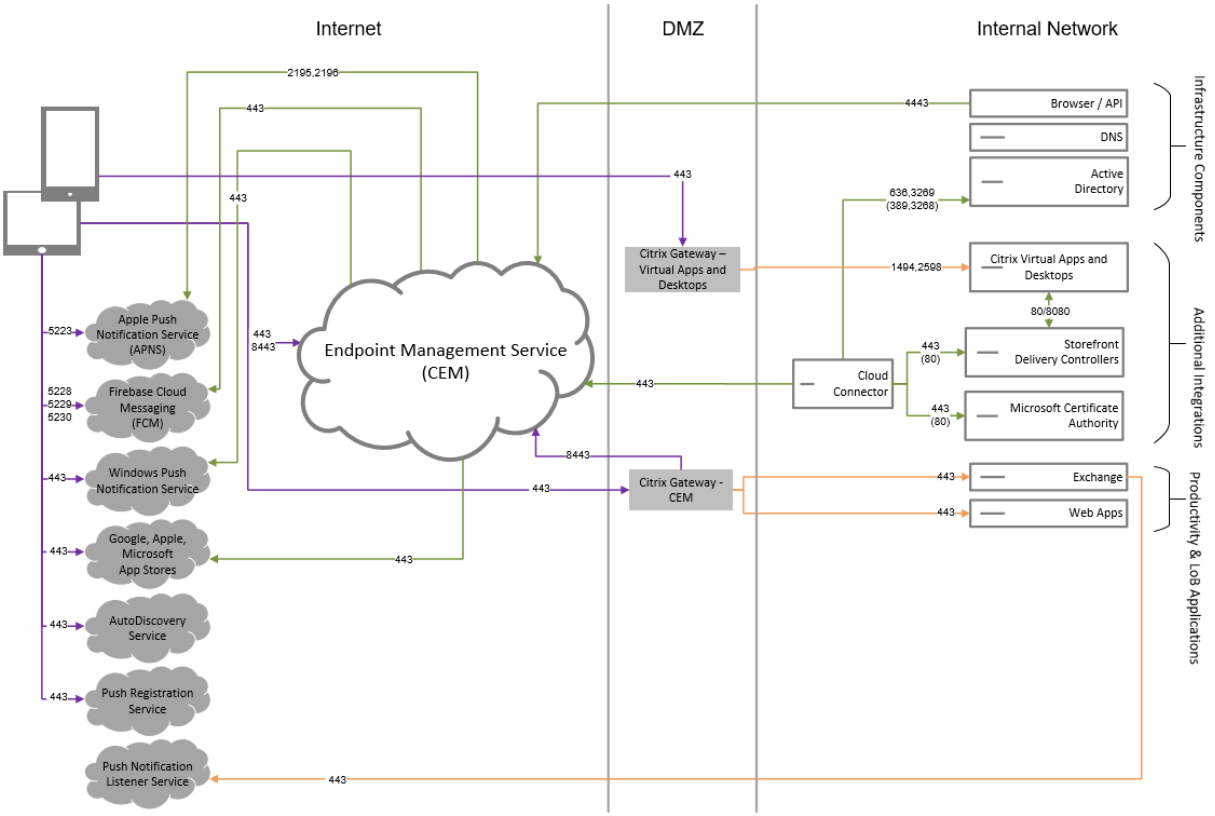
Weitere Informationen zu den Anforderungen für Citrix ADC und NetScaler Gateway finden Sie in der Citrix Produktdokumentation unter https://docs.citrix.com/.

Referenzarchitektur mit Kernstruktur

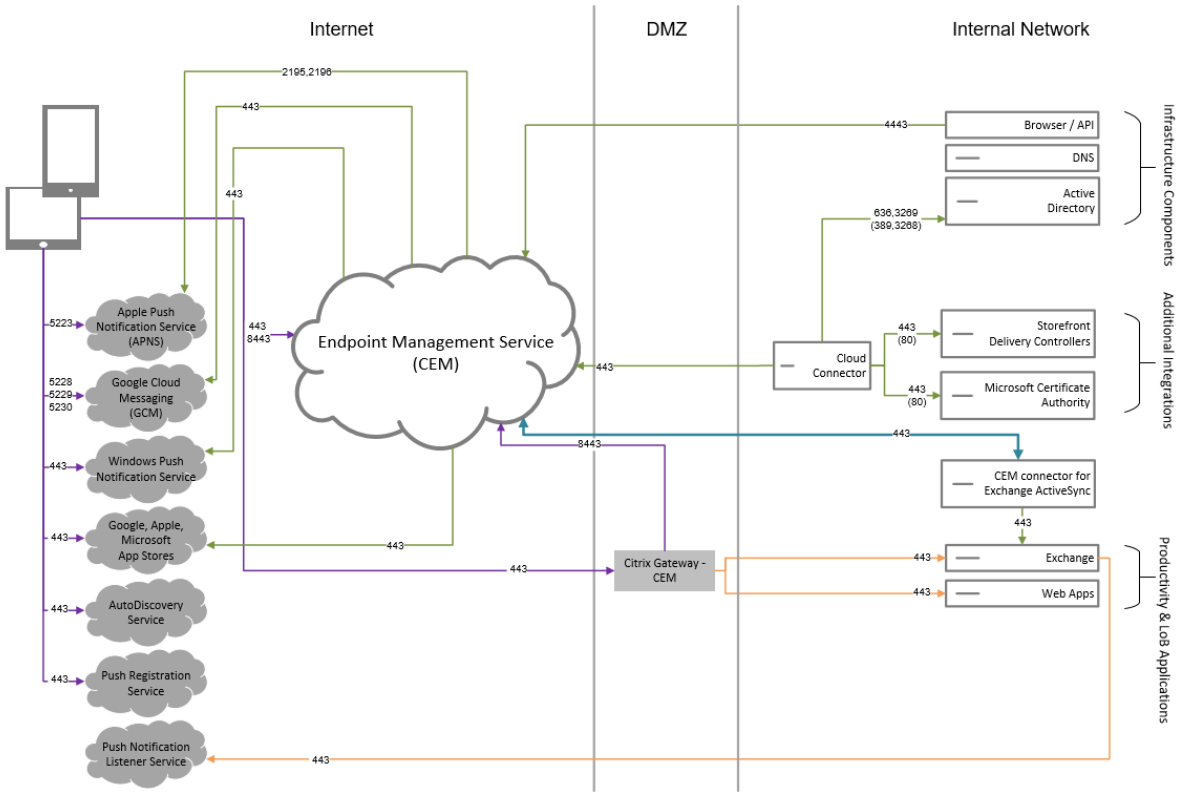
Informationen zu den Portanforderungen finden Sie unter Systemanforderungen.



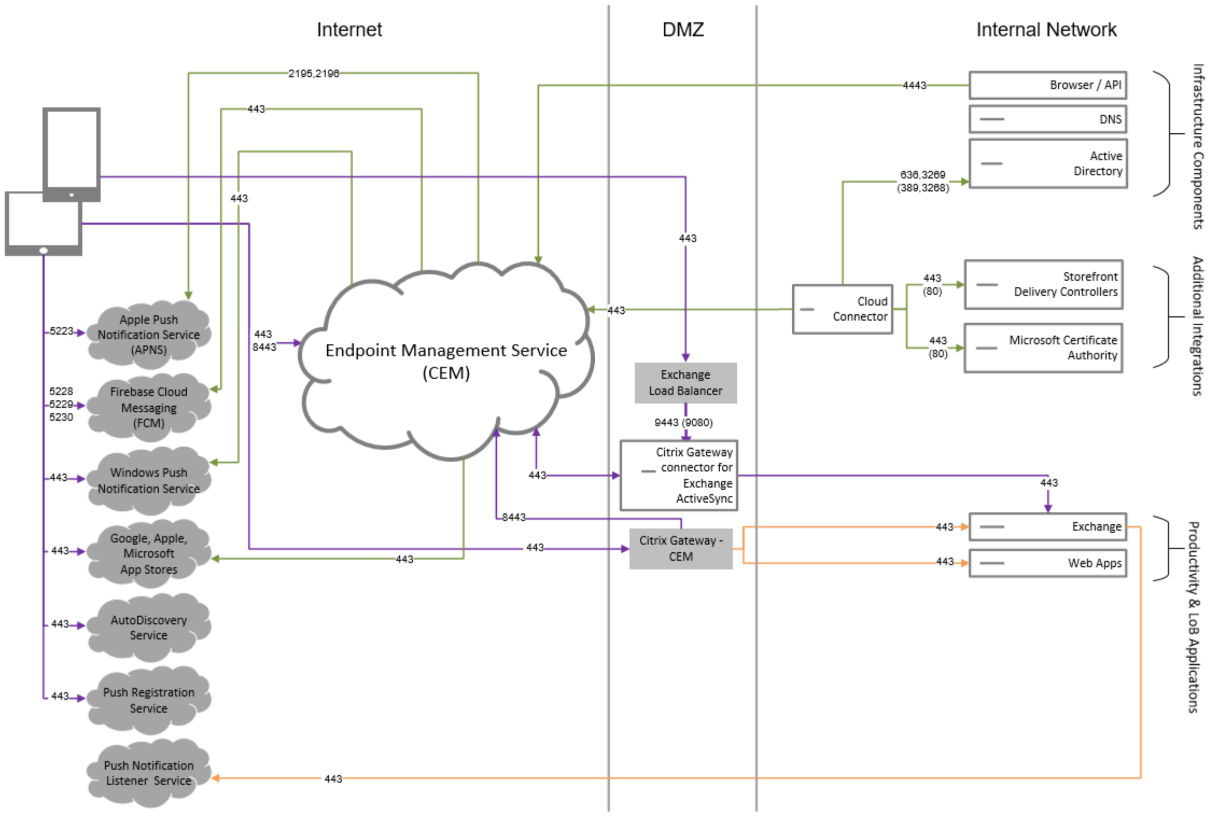
Referenzarchitektur mit Citrix Virtual Apps and Desktops



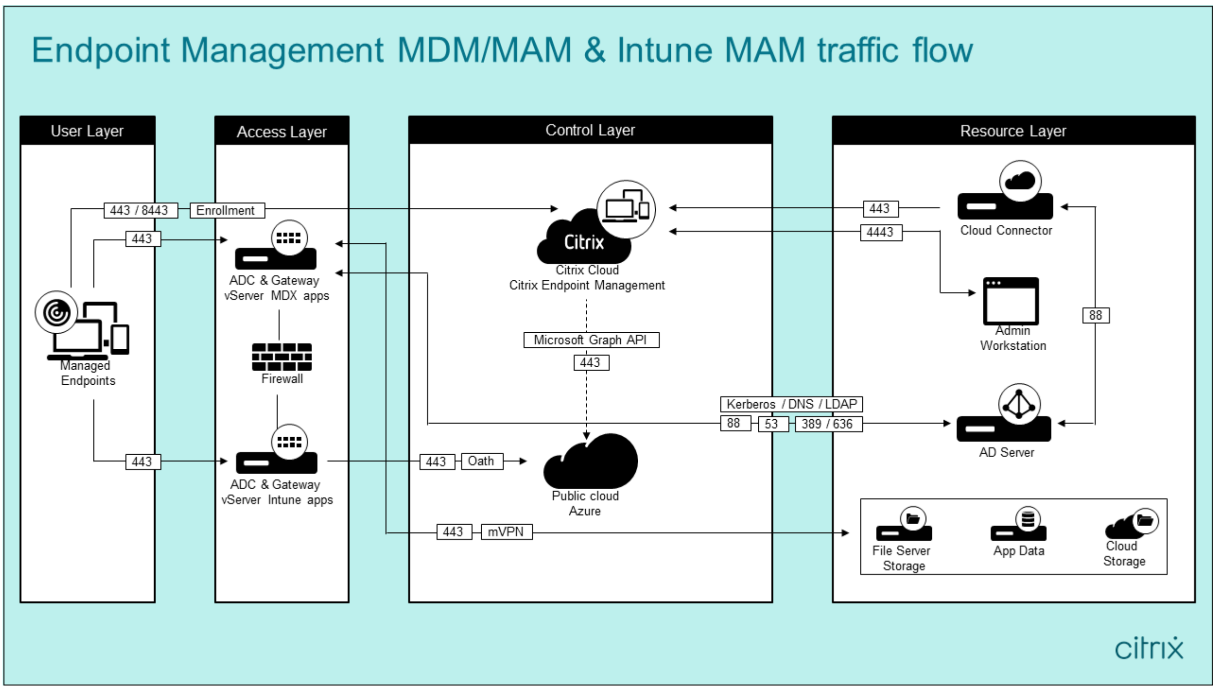
Referenzarchitektur mit Citrix Endpoint Management Connector für Exchange ActiveSync



Referenzarchitektur mit NetScaler Gateway Connector für Exchange ActiveSync



Referenzarchitektur mit Citrix Endpoint Management MDM+MAM und Intune MAM



Ressourcenstandorte

Platzieren Sie Ressourcenstandorte dort, wo sie die Unternehmensanforderungen am besten erfüllen. Beispiele: in einer öffentlichen Cloud, einer Zweigstelle, einer privaten Cloud oder in einem Datencenter. Faktoren für die Standortwahl:

- die Nähe zu Abonnenten
- die Nähe zu Daten
- Anforderungen an die Skalierbarkeit
- Sicherheitsattribute

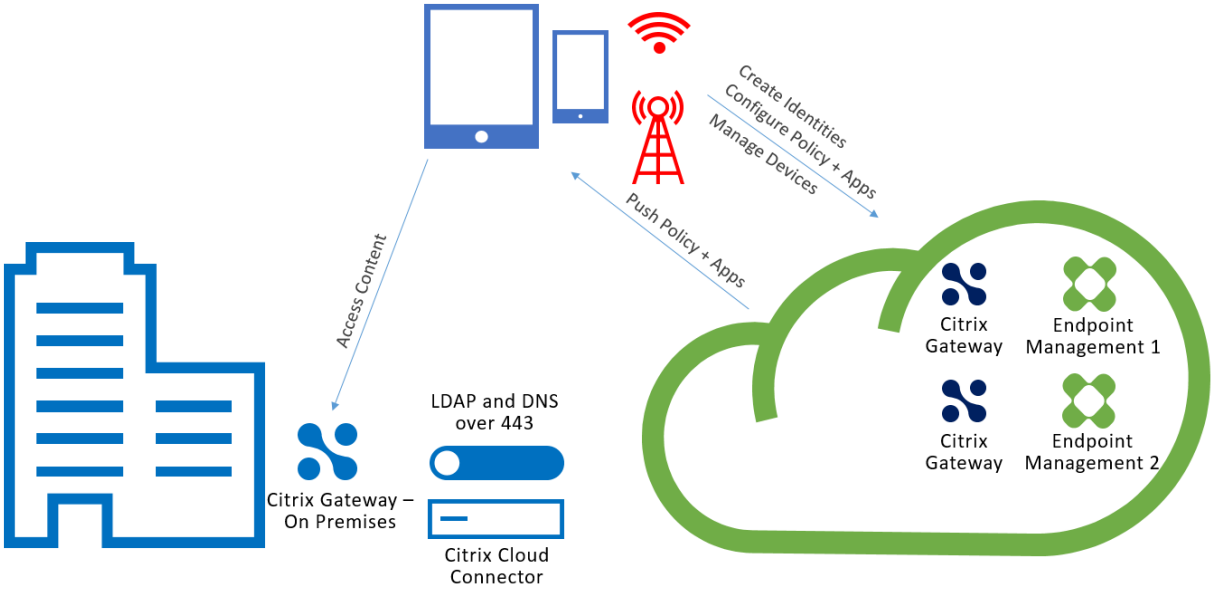
Sie können beliebig viele Ressourcenstandorte erstellen. Beispiel:

- Sie erstellen einen Ressourcenstandort im Datencenter für den Firmenhauptsitz, basierend auf Abonnenten und Anwendungen, die in Datennähe sein müssen.
- Sie fügen einen separaten Ressourcenstandort für die globalen Benutzer in einer öffentlichen Cloud hinzu. Alternativ können Sie separate Ressourcenstandorte in Geschäftsstellen erstellen, um die Anwendungen bereitzustellen, die in der Nähe der Filialmitarbeiter sein sollten.
- Sie fügen einen weiteren Ressourcenstandort in einem anderen Netzwerk hinzu, der eingeschränkte Anwendungen bereitstellt. Dies schränkt die Sichtbarkeit für andere Ressourcen und Abonnenten ein, ohne die anderen Ressourcenstandorte anpassen zu müssen.

Cloud Connector

Der Cloud Connector authentifiziert und verschlüsselt die gesamte Kommunikation zwischen Citrix Cloud und Ihren Ressourcen. Der Cloud Connector ist für den Zugriff auf folgende Dienste erforderlich: LDAP, IdPs, PKI-Server, interne DNS-Abfragen, Citrix Virtual Apps, NetScaler Gateway, Citrix Workspace und Microsoft Endpoint Manager.

Das folgende Diagramm zeigt den Datenfluss für Cloud Connector.



Der Cloud Connector stellt Verbindungen zu Citrix Cloud her. Der Cloud Connector akzeptiert keine eingehenden Verbindungen.

Cloud Connector ist nur während der Geräteregistrierung unter Last. Weitere Informationen finden Sie unter Überlegungen zur Skalierung und Größe für Cloud Connectors.

Eine Lösung mit integrierter Mobilanwendungsverwaltung (MAM) benötigt ein Micro-VPN, das über ein on-premises NetScaler Gateway bereitgestellt wird. Für dieses Szenario gilt:

- Die folgenden Komponenten befinden sich in Ihrem Datencenter:
  - Cloud Connector
  - NetScaler Gateway
  - Ihre Server für Exchange, Web-Apps, Active Directory und die PKI
- Mobilgeräte kommunizieren mit Citrix Endpoint Management und Ihrem on-premises NetScaler Gateway.

Citrix Endpoint Management-Komponenten

Citrix Endpoint Management-Konsole. Sie verwenden die Citrix Endpoint Management-Konsole zum Konfigurieren von Citrix Endpoint Management. Informationen zur Verwendung der Citrix Endpoint Management-Konsole finden Sie in den Artikeln unter Citrix Endpoint Management. Citrix benachrichtigt Sie, wenn die Artikel "Neue Features"für Citrix Endpoint Management bei Veröffentlichung eines neuen Releases aktualisiert werden.

Beachten Sie folgende Unterschiede zwischen Citrix Endpoint Management und on-premises Versionen:

- Der Remotesupportclient ist für Citrix Endpoint Management nicht verfügbar.
- Citrix unterstützt keine Syslog-Integration in Citrix Endpoint Management mit einem lokalen Syslog-Server. Sie können die Protokolle von der Seite **Problembehandlung und Support** in der Citrix Endpoint Management-Konsole herunterladen. Klicken Sie hierfür auf **Alle herunterladen**.

MAM-SDK. Das MDX Toolkit erreicht das Ende des Lebenszyklus (EOL) im Juli 2023. 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.

Mobile Produktivitätsapps. Die von Citrix entwickelten mobile Produktivitätsapps bieten innerhalb der Citrix Endpoint Management-Umgebung Produktivitäts- und Kommunikationstools. Ihre Unternehmensrichtlinien sichern diese Apps. Weitere Informationen finden Sie unter Mobile Produktivitätsapps.

Citrix Endpoint Management Connector für Exchange ActiveSync. Der Citrix Endpoint Management Connector für Exchange ActiveSync bietet Benutzern, die native mobile E-Mail-Apps verwenden, einen sicheren Zugriff auf ihre E-Mail. Der Connector für Exchange ActiveSync ermöglicht eine ActiveSync-Filterung auf der Exchange-Dienstebene. Das Resultat ist, dass die Filterung erst dann erfolgt, wenn die E-Mail den Exchange-Dienst erreicht, und nicht sobald sie in die Citrix Endpoint Management-Umgebung gelangt. NetScaler Gateway ist für den Connector nicht erforderlich. Sie können den Connector ohne Änderungen am Routing des ActiveSync-Datenverkehrs bereitstellen. Weitere Informationen finden Sie unter Citrix Endpoint Management Connector für Exchange ActiveSync.

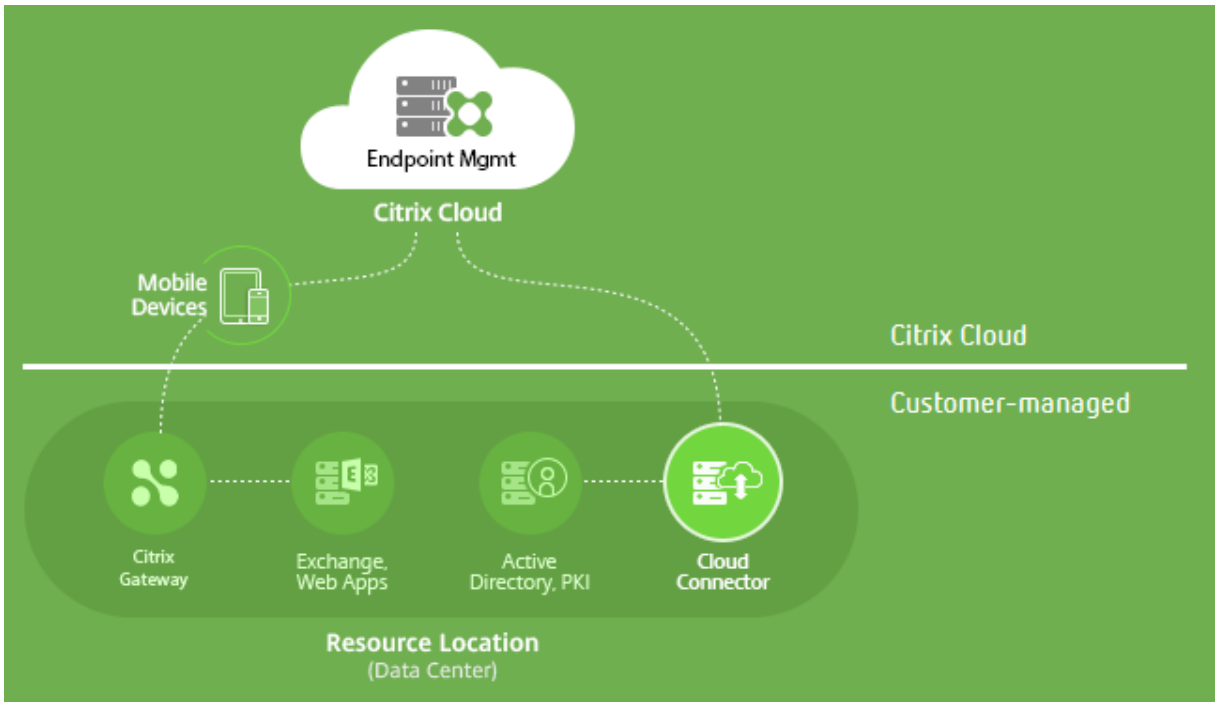
NetScaler Gateway Connector für Exchange ActiveSync. Der NetScaler Gateway Connector für Exchange ActiveSync bietet Benutzern, die native mobile E-Mail-Apps verwenden, einen sicheren Zugriff auf ihre E-Mail. Der Connector für Exchange ActiveSync bietet ActiveSync-Filterung am Umkreis. Die Filterung verwendet NetScaler Gateway als Proxy für ActiveSync-Datenverkehr. Dies bedeutet, dass die Filterkomponente im Pfad des E-Mail-Datenverkehrs ist und E-Mails beim Erreichen oder Verlassen der Umgebung abfängt. Der Connector für Exchange ActiveSync fungiert als Vermittler zwischen NetScaler Gateway und Citrix Endpoint Management. Weitere Informationen finden Sie unter NetScaler Gateway Connector für Exchange ActiveSync.

Citrix Endpoint Management –Technische Sicherheit

Citrix Cloud verwaltet die Steuerungsebene für Citrix Endpoint Management-Umgebungen. Die Steuerungsebene umfasst den Citrix Endpoint Management-Server, den Citrix ADC-Load Balancer

und eine Einmandanten-Datenbank. Der Cloudservice kann über den Citrix Cloud Connector in ein Kunden-Datencenter integriert werden. Citrix Endpoint Management-Kunden, die Cloud Connector verwenden, verwalten NetScaler Gateway normalerweise in ihren Datencentern.

Die folgende Abbildung zeigt den Service und seine Sicherheitsgrenzen.



Die Informationen in diesem Abschnitt:

- bieten eine Einführung in die Sicherheitsfunktionen von Citrix Cloud.
- enthalten eine Erläuterung der Aufgabenverteilung für den Schutz der Citrix Cloud-Bereitstellung zwischen Citrix und Kunden.
- sind keine Konfigurations- oder Verwaltungsanleitung für Citrix Cloud oder zugehörige Komponenten oder Services.

Informationen zur Technologie, die in Citrix Endpoint Management zur Bereitstellung umfassender End-to-End-Sicherheit verwendet wird, finden Sie unter Security and Productivity for the Mobile Enterprise.

Datenfluss

Die Steuerungsebene hat einen eingeschränkten Lesezugriff auf Benutzer- und Gruppenobjekte. Diese Objekte befinden sich in Ihrem Verzeichnis, im DNS und in ähnlichen Diensten. Die Steuerungsebene greift auf diese Dienste über Citrix Cloud Connector und sichere HTTPS-Verbindungen zu.

Unternehmensdaten, etwa E-Mail-, Intranet- und Web-App-Datenverkehr, werden über NetScaler Gateway direkt zwischen Gerät und Anwendungsservern übertragen. NetScaler Gateway wird im Datencenter des Kunden bereitgestellt.

Datenisolierung

In der Steuerungsebene werden die zur Verwaltung von Benutzergeräten und mobilen Apps benötigten Metadaten gespeichert. Der Service selbst besteht aus einer Mischung aus Multimandanten- und Einmandanten-Komponenten. Die Kundenmetadaten werden jedoch gemäß der Servicearchitektur für jeden Mandanten separat gespeichert und mithilfe eindeutiger Anmeldeinformationen geschützt.

Handhabung von Anmeldeinformationen

Der Service verarbeitet die folgenden Arten von Anmeldeinformationen:

- **Benutzeranmeldeinformationen:** Diese werden über eine HTTPS-Verbindung vom Gerät an die Steuerungsebene übertragen. Die Steuerungsebene prüft die Anmeldeinformationen über eine sichere Verbindung gegen ein Kundenverzeichnis.
- **Administratoranmeldeinformationen:** Administratoren authentifizieren sich bei Citrix Cloud mit dem Anmeldesystem von Citrix Online. Dabei wird ein signiertes JSON Web Token (JWT) zur einmaligen Benutzung generiert, das dem Administrator Zugriff auf den Service gewährt.
- **Active Directory-Anmeldeinformationen:** Die Steuerungsebene erfordert Binde-Anmeldeinformationen, um Benutzermetadaten aus Active Directory zu lesen. Die Anmeldeinformationen werden mit AES-256 verschlüsselt und in einer Mandantendatenbank gespeichert.

Überlegungen zur Bereitstellung

Beachten Sie die in der Dokumentation beschriebenen bewährten Methoden für die Bereitstellung von NetScaler Gateway in Ihren Umgebungen.

Weitere Ressourcen

Kunden wird empfohlen, Sicherheitsbulletins zu lesen, die sich auf ihre Citrix Produkte beziehen. Informationen zu neuen und aktualisierten Sicherheitsbulletins finden Sie in den Sicherheitsbulletins von Citrix. Überlegen Sie auch, in Ihren Warnungseinstellungen anzugeben, dass Sie Benachrichtigungen erhalten möchten.

Weitere Informationen zur Sicherheit finden Sie in den folgenden Ressourcen:

- Citrix-Sicherheitssite: https://www.citrix.com/security
- Citrix Cloud-Dokumentation: Leitfaden zur sicheren Bereitstellung für die Citrix Cloud-Plattform
- Leitfaden zur sicheren Bereitstellung von Citrix ADC

Integration mit Mobile Threat Defense-Software

Mit Mobile Threat Defense (MTD)-Software können Sie weitreichende Cyberangriffe gegen mobile Geräte des Unternehmens erkennen, analysieren und leichter abwehren. Durch eine Kombination aus MTD und UEM (Unified Citrix Endpoint Management) erhöhen Sie Sicherheit und Transparenz in Ihrem Unternehmen.

Citrix Endpoint Management nutzt die Bedrohungsdaten der MTD-Software für Folgendes:

- Schutz vor Malware, Phishing, Netzwerkangriffen und Man-in-the-Middle-Angriffen
- Überprüfen der Richtlinientreue von Geräten
- Bestimmen von Risikostufen
- Schutz Ihrer Apps, Daten, Geräte und des mobilen Netzwerks durch richtlinienbasierte Aktionen

Citrix Endpoint Management kann mit folgenden MTD-Anbietern integriert werden:

- Check Point
- Lookout
- Wandera
- Zimperium

Weitere Informationen oder eine Demoversion erhalten Sie von unseren MTD-Partnern oder Ihrem Citrix-Vertriebsmitarbeiter.

Integration von Citrix Endpoint Management in Microsoft Endpoint Manager

March 11, 2024

Durch die Integration von Citrix Endpoint Management mit Microsoft Endpoint Manager (MEM) können Microsoft Intune-fähige Apps (z. B. Microsoft Edge Browser) die Vorteile von Citrix Endpoint Management Micro-VPN nutzen.

Wenden Sie sich an das Citrix Cloud Operations-Team, um die **Integration zu aktivieren**.

Dieses Release unterstützt die folgenden Anwendungsfälle:

- Intune MAM mit Citrix Endpoint Management MDM+MAM.

  Dieser Artikel erläutert den Anwendungsfall Intune MAM + Citrix Endpoint Management MDM+MAM. Nachdem Sie Citrix als MDM-Anbieter hinzugefügt haben, konfigurieren Sie mit Intune verwaltete Apps für die Bereitstellung auf Geräten.

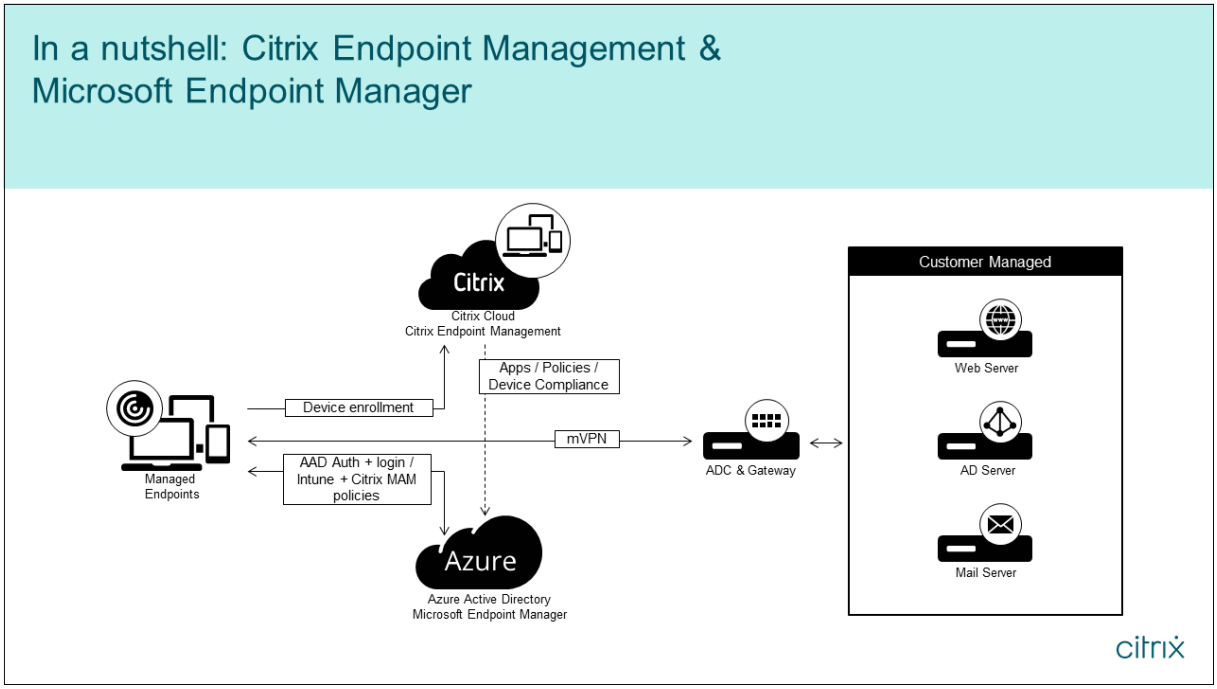
  > **Wichtig:**
  >
  > In diesem Anwendungsfall unterstützt Citrix Secure Mail die Integration mit Intune nicht. Citrix Secure Mail funktioniert nur bei im MDX-Modus registrierten Geräten.

- Intune MAM und Citrix Endpoint Management MDM.
- Intune MAM.
- Intune MAM und Intune MDM. Citrix Secure Mail für iOS unterstützt Single Sign-On für diesen Anwendungsfall.

Eine einfache grafische Anleitung zum Einrichten der Citrix Endpoint Management-Integration mit MEM finden Sie unter Erste Schritte.

Weitere Informationen zur Integration in den bedingten Azure AD-Zugriff finden Sie unter Integration in bedingten Azure AD-Zugriff.

Die folgende Abbildung bietet einen Überblick über die Integration von Citrix Endpoint Management mit Microsoft Endpoint Manager.



Systemanforderungen

MDX-fähig

- MAM SDK

  Oder

- MDX Toolkit

Microsoft

- Azure Active Directory-Zugriff (mit Mandantenadministratorberechtigung)
- Intune-fähiger Mandant

Firewallregel

- Firewallregel, die DNS- und SSL-Datenverkehr von einer NetScaler Gateway-Subnetz-IP an `*.manage.microsoft.com`, `https://login.microsoftonline.com` und `https://graph.windows.net` zulässt (Port 53 und 443)

Voraussetzungen

- **Microsoft Edge-Browser:** Das Mobile Apps SDK ist in die Microsoft Edge-Browser-App für iOS und Android integriert. Weitere Informationen zu Microsoft Edge finden Sie in der Dokumentation zu Microsoft Edge.
- **Citrix Cloud-Konto:** Wenden Sie sich an einen Citrix Vertriebsmitarbeiter, um sich für ein Citrix-Konto zu registrieren und eine Citrix Endpoint Management-Testversion anzufordern. Wenn Sie zum Fortfahren bereit sind, rufen Sie https://onboarding.cloud.com auf. Weitere Informationen zum Anfordern eines Citrix Cloud-Kontos finden Sie unter Bei Citrix Cloud registrieren.

  > **Hinweis:**
  >
  > Die von Ihnen angegebene E-Mail-Adresse darf nicht mit Azure AD verknüpft sein. Sie können einen beliebigen kostenlosen E-Mail-Service nutzen.

- **APNs-Zertifikate für iOS:** Konfigurieren Sie APNs-Zertifikate für iOS. Weitere Informationen zum Einrichten solcher Zertifikate finden Sie in dem Citrix Blogbeitrag Creating and Importing APNs Certificates.

- **Azure AD-Synchronisierung:** Richten Sie die Synchronisierung zwischen Azure AD und dem On-Premises-Active Directory ein. Installieren Sie das Tool zur AD-Synchronisierung nicht auf dem Domänencontroller. Weitere Informationen zum Einrichten dieser Synchronisierung finden Sie in der Microsoft-Dokumentation zu Azure Active Directory.

Konfigurieren von NetScaler Gateway

Wenn Sie eine neue Bereitstellung von Citrix Endpoint Management einrichten, installieren Sie eines der folgenden NetScaler Gateway-Geräte:

- NetScaler Gateway VPX, Serie 3000 oder höher
- NetScaler Gateway MPX oder dedizierte SDX-Instanz

Verwenden von NetScaler Gateway mit der Citrix Endpoint Management-Integration mit MEM:

- Konfigurieren Sie NetScaler Gateway mit einer Managementoberfläche und einer Subnetz-IP-Adresse.
- Verwenden Sie TLS 1.2 für die gesamte Kommunikation zwischen Client und Server. Hinweise zum Konfigurieren von TLS 1.2 für NetScaler Gateway finden Sie unter CTX247095.

Wenn Sie die Citrix Endpoint Management-Integration mit MEM mit einer MDM+MAM-Bereitstellung von Citrix Endpoint Management verwenden, konfigurieren Sie zwei Citrix Gateways. Der Datenverkehr der MDX-App wird über das eine NetScaler Gateway geleitet. Der Datenverkehr der Intune-App wird über das andere NetScaler Gateway geleitet. Konfigurieren Sie:

- Zwei öffentliche IP-Adressen.
- Optional eine IP-Adresse mit Netzwerkadressübersetzung.
- Zwei DNS-Namen. Beispiel: `https://mam.company.com`.
- Zwei öffentliche SSL-Zertifikate. Konfigurieren Sie Zertifikate, die dem reservierten öffentlichen DNS-Namen entsprechen, oder verwenden Sie Zertifikate mit Platzhalterzeichen.
- Ein MAM-Load Balancer mit einer internen, nicht routbaren IP-Adresse nach RFC 1918.
- Ein LDAP/Active Directory-Dienstkonto.

Zustimmung zu delegierten Berechtigungsaufforderungen

Verwaltete Apps, bei denen Benutzer sich authentifizieren müssen, fordern Anwendungsberechtigungen an, die von Microsoft Graph bereitgestellt werden. Bei einer Zustimmung erhalten die Apps Zugriff auf erforderliche Ressourcen und APIs. Einige Apps erfordern die Zustimmung des globalen Administrators für Microsoft Azure AD. Für solche delegierten Berechtigungen muss der globale Administrator Citrix Cloud die Berechtigung erteilen, Token anzufordern. Die Token aktivieren dann die nachfolgend aufgeführten Berechtigungen. Weitere Informationen finden Sie unter Microsoft Graph permissions reference.

- **Anmelden und Benutzerprofil lesen:** Diese Berechtigung ermöglicht es Benutzern, sich anzumelden und eine Verbindung mit Azure AD herzustellen. Citrix kann die Benutzeranmeldeinformationen nicht sehen.
- **Grundlegende Profile aller Benutzer lesen:** Die App liest Profileigenschaften für die Benutzer in der Organisation. Zu den Eigenschaften gehören Anzeigename, Vor- und Nachname, E-Mail-Adresse und das Foto von Benutzern in der Organisation.
- **Alle Gruppen lesen:** Mit dieser Berechtigung können Azure AD-Gruppen für die Zuweisung von Apps und Richtlinien festgelegt werden.
- **Als angemeldeter Benutzer auf das Verzeichnis zugreifen:** Diese Berechtigung überprüft das Intune-Abonnement und aktiviert die NetScaler Gateway- und VPN-Konfiguration.
- **Lesen und Schreiben für Microsoft Intune-Apps.:** Die App hat Lese-/Schreibrechte für Folgendes:
  - Von Microsoft verwaltete Eigenschaften
  - Gruppenzuweisungen und App-Status
  - App-Konfigurationen
  - App-Schutzrichtlinien

Während der NetScaler Gateway-Konfiguration muss der globale Administrator für Azure AD zudem Folgendes ausführen:

- Genehmigen des Active Directory, das für das Micro-VPN ausgewählt wurde. Der globale Administrator muss außerdem einen Clientschlüssel erstellen, der von NetScaler Gateway für die Kommunikation mit Azure AD und Intune verwendet wird.
- Er darf nicht die Rolle des Citrix Administrators haben. Der Citrix Administrator weist stattdessen Benutzern mit entsprechenden Administratorberechtigungen für Intune-Anwendungen Azure AD-Konten zu. Der Intune-Administrator übernimmt dann die Rolle eines Citrix Cloud-Administrators, um Intune in Citrix Cloud zu verwalten.

> **Hinweis:**
>
> Citrix verwendet das Kennwort des globalen Intune-Administrators nur während der Einrichtung und leitet die Authentifizierung an Microsoft weiter. Citrix hat keinen Zugriff auf das Kennwort.

Konfigurieren der Citrix Endpoint Management-Integration mit MEM

1. Melden Sie sich bei der Citrix Cloud-Site an und fordern Sie eine Testversion von Citrix Endpoint Management an.

2. Ein Vertriebsingenieur vereinbart mit Ihnen ein Onboarding-Meeting. Teilen Sie mit, dass Sie Citrix Endpoint Management mit MEM integrieren möchten. Wenn Ihre Anforderung genehmigt wurde, klicken Sie auf **Verwalten**.
3. Von hier können Sie auf das Zahnrad in der oberen rechten Ecke Ihrer Website klicken oder auf **Site konfigurieren**.
4. Folgen Sie dem Link im ersten Schritt zur Seite **Identitäts- und Zugriffsverwaltung**.
5. Klicken Sie auf **Verbinden**, um eine Verbindung mit Ihrem Azure AD herzustellen.
6. Geben Sie eine eindeutige Anmelde-URL ein, die der Azure AD-Administrator zur Anmeldung verwendet, und klicken Sie auf **Bestätigen**.
7. Fügen Sie ein globales Azure AD-Administratorkonto hinzu und akzeptieren Sie die Berechtigungsanforderung.
8. Vergewissern Sie sich, dass Ihre Azure AD-Instanz erfolgreich eine Verbindung herstellen kann. Eine erfolgreiche Verbindung ist daran zu erkennen, dass der Text **Nicht verbunden** zu **Aktiviert** wechselt.
9. Klicken Sie auf die Registerkarte **Administratoren** und fügen Sie den Azure AD Intune-Administrator als Citrix Cloud-Administrator hinzu. Wählen Sie im Dropdownmenü entweder Azure AD oder Citrix Identität aus und suchen Sie nach dem Benutzernamen, den Sie hinzufügen möchten. Klicken Sie auf **Einladen**, gewähren Sie dem Benutzer **Vollzugriff** oder **Benutzerdefinierten Zugriff**, und klicken Sie auf **Einladung senden**.

   > **Hinweis:**
   >
   > Für den **benutzerdefinierten Zugriff** in Citrix Endpoint Management sind folgende Regeln erforderlich: Bibliothek und Citrix Endpoint Management.

   Der Azure AD Intune-Administrator erhält dadurch eine E-Mail-Einladung zum Erstellen eines Kennworts und zur Anmeldung bei Citrix Cloud. Vor der Anmeldung des Administrators müssen Sie sich von allen anderen Konten abmelden.

   Der Azure AD Intune-Administrator muss die verbleibenden Schritte in diesem Verfahren ausführen.
10. Nach der Anmeldung mit dem neuen Konto klicken Sie unter **Citrix Endpoint Management** auf **Verwalten**. Wenn Sie alles richtig konfigurieren, wird auf der Seite angezeigt, dass der Azure AD-Administrator angemeldet und das Intune-Abonnement gültig ist.

Konfigurieren von NetScaler Gateway für Micro-VPN

Zur Verwendung von Micro-VPN in Intune müssen Sie NetScaler Gateway für die Authentifizierung bei Azure AD konfigurieren. Ein vorhandener virtueller NetScaler Gateway-Server kann in diesem Anwen-

dungsfall nicht verwendet werden.

Konfigurieren Sie Azure AD zunächst zur Synchronisierung mit dem On-Premises-Active Directory. Dieser Schritt ist erforderlich, um eine einwandfreie Authentifizierung zwischen Intune und NetScaler Gateway sicherzustellen.

1. Klicken Sie in der Citrix Cloud-Konsole unter **Citrix Endpoint Management** auf **Verwalten**.
2. Klicken Sie neben **Micro-VPN** auf **Micro-VPN konfigurieren**.
3. Geben Sie einen Namen für den Micro-VPN-Dienst und die externe URL für das NetScaler Gateway ein und klicken Sie auf **Weiter**.

   Das Skript konfiguriert NetScaler Gateway zur Unterstützung von Azure AD und der Intune-Apps.
4. Klicken Sie auf **Script herunterladen**. Die ZIP-Datei enthält eine Readme-Datei mit Anweisungen zum Implementieren des Skripts. Sie können an dieser Stelle zwar speichern und beenden, das Micro-VPN wird jedoch erst eingerichtet, wenn Sie das Skript auf dem NetScaler Gateway ausführen.

   > **Hinweis:**
   >
   > Wird nach der NetScaler Gateway-Konfiguration ein anderer OAuth-Status als COMPLETE angezeigt, konsultieren Sie den Abschnitt "Problembehandlung".

Konfigurieren der Geräteverwaltung

Wenn Sie außer Apps auch Geräte verwalten möchten, wählen Sie eine Methode zur Geräteverwaltung aus. Sie können Citrix Endpoint Management MDM+MAM oder Intune MDM verwenden.

> **Hinweis:**
>
> Die Standardeinstellung ist Intune MDM. Informationen zur Verwendung von Intune als MDM-Anbieter finden Sie in der Microsoft Intune-Dokumentation.

1. Klicken Sie in der Citrix Cloud-Konsole im Bereich zur Citrix Endpoint Management-Integration mit MEM auf **Verwalten**. Klicken Sie neben **Geräteverwaltung - optional** auf **MDM konfigurieren**.
2. Geben Sie einen eindeutigen Sitenamen ein, wählen Sie die für Sie nächstgelegene Cloudregion und fordern Sie eine **Site** an. Sie erhalten eine E-Mail, wenn Ihre Site fertig ist.
3. Klicken Sie auf **OK**, um die Information zu schließen. Wählen Sie einen Active Directory-Ort zur Verknüpfung mit Ihrer Site oder erstellen Sie einen Ressourcenstandort und klicken Sie auf **Weiter**.
4. Klicken Sie auf **Cloud Connector herunterladen** und folgen Sie den angezeigten Anweisungen, um den Cloud Connector zu installieren. Klicken Sie nach der Installation auf **Verbindung testen**, um die Verbindung zwischen Citrix Cloud und dem Cloud Connector zu überprüfen.

5. Klicken Sie abschließend auf **Speichern & Beenden**. Der Ressourcenstandort wird angezeigt. Wenn Sie auf **Fertig stellen** klicken, gelangen Sie zurück zum Einstellungsbildschirm.
6. Sie können nun von Ihrer Sitekachel aus auf die Citrix Endpoint Management-Konsole zugreifen. Von hier aus können Sie MDM-Verwaltungsaufgaben ausführen und Geräterichtlinien zuweisen. Weitere Informationen zu Geräterichtlinien finden Sie unter Geräterichtlinien.

Konfigurieren der Bereitstellung von mit Intune verwalteten Apps auf Geräten

Das Bereitstellen von mit Intune verwalteten Apps umfasst folgende Schritte:

- Hinzufügen der Apps zur Citrix Cloud-Bibliothek
- Erstellen von Citrix Endpoint Management-Geräterichtlinien zur Datenflusssteuerung
- Erstellen einer Bereitstellungsgruppe für die Apps und Richtlinien

Hinzufügen von Microsoft Intune-Apps zur Citrix Cloud-Bibliothek

Führen Sie Folgendes für jede App aus, die Sie hinzufügen möchten:

1. Klicken Sie in der Citrix Cloud-Konsole auf das Menüsymbol und dann auf **Bibliothek**.
2. Klicken Sie rechts oben auf das Pluszeichen und dann auf **Mobile App hinzufügen**.
3. Wenn Sie Android Enterprise in der Citrix Endpoint Management-Konsole konfiguriert haben, wählen Sie unter **Wählen Sie eine Anwendung** die Option **Microsoft Intune-Apps**. Wählen Sie eine App-Vorlage zum Anpassen aus oder klicken Sie auf **Upload my own App**.

   Citrix stellt App-Vorlagen bereit, zu denen jeweils ein Satz vorkonfigurierter Standardrichtlinien gehört. Für von Kunden hochgeladene Apps gelten folgende Richtlinien:

   - **MDX-Dateien:** Enthält MAM-SDK-fähige Apps oder Apps, die mit MDX umschlossen wurden, zum Beispiel:
     - Intune App-Schutzrichtlinien und standardmäßige MDX-Richtlinien im Paket
     - Öffentliche Store-Apps, z. B. Intune App-Schutzrichtlinien und standardmäßige MDX-Richtlinien, die der Paket-ID entsprechen
   - **IPA-Dateien:** Intune-App-Schutzrichtlinien.
   - **APK-Dateien:** Intune-App-Schutzrichtlinien.

   > **Hinweis:**
   >
   > Wenn eine App nicht mit Intune umschlossen ist, werden keine Intune-App-Schutzrichtlinien angewendet.

4. Klicken Sie auf **Upload my own App** und laden Sie Ihre mit MDX bzw. Intune umschlossene Datei hoch.
5. Geben Sie einen Namen und eine Beschreibung für die App ein, wählen Sie aus, ob die App optional oder erforderlich sein soll, und klicken Sie auf **Weiter**.
6. Konfigurieren Sie die Anwendungseinstellungen. Die folgenden Konfigurationen ermöglichen den Datentransfer zwischen Citrix Endpoint Management- und Intune-Containern.

    - **Allow apps to receive data from other app:** Wählen Sie **Policy managed apps**.
    - **Allow app to transfer data to other apps:** Wählen Sie **All apps**.
    - **Restrict cut, copy, paste with other apps:** Wählen Sie **Policy managed apps**.

7. Konfigurieren Sie die Speicherrepositorys für gespeicherte Daten. Wählen Sie unter **Select which storage services corporate data can be saved to** die Option **LocalStorage**.
8. Optional: Legen Sie Data Relocation-, Access- und PIN-Richtlinien für die App fest. Klicken Sie auf **Weiter**.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

    Die App-Konfiguration kann einige Minuten dauern. Wenn sie abgeschlossen ist, wird gemeldet, dass die App in der Bibliothek veröffentlicht wurde.
10. Um der App Benutzergruppen zuzuweisen, klicken Sie auf **Benutzer zuweisen**.
11. Suchen Sie über das Suchfeld nach Benutzergruppen und klicken Sie auf diese, um sie hinzuzufügen. Sie können keine einzelnen Benutzer hinzufügen.
12. Wenn Sie alle Gruppen hinzugefügt haben, klicken Sie auf das X, um das Fenster zu schließen.

    Beim Hinzufügen von Benutzergruppen kann ein Fehler auftreten. Das ist der Fall, wenn die Benutzergruppe nicht mit dem lokalen Active Directory synchronisiert wurde.

Hinzufügen von Android Enterprise-Apps zur Citrix Cloud-Bibliothek

Um Android Enterprise-Apps zur Bibliothek in Citrix Cloud hinzuzufügen und Intune-App-Schutzrichtlinien festzulegen, konfigurieren Sie Ihre Cloudumgebung wie folgt:

- Verbinden Sie Citrix Cloud mit Ihrem Azure Active Directory-Konto (AAD-Konto). Siehe Verbinden von Azure Active Directory mit Citrix Cloud.
- Konfigurieren Sie LDAP und Cloud Connector in Citrix Endpoint Management.
- Richten Sie Android Enterprise in Citrix Endpoint Management ein. Stellen Sie sicher, dass sich Android Enterprise-Geräte bei MDM+MAM registrieren. Informationen zum Einrichten von Android Enterprise finden Sie unter Android Enterprise.

Nach diesem Verfahren werden Android Enterprise-Apps gleichzeitig zur Citrix Endpoint Management-Konsole und zur Intune-Konsole hinzugefügt. Führen Sie für jede hinzuzufügende Android Enterprise-App folgende Schritte aus:

1. Klicken Sie in der Citrix Cloud-Konsole auf das Menüsymbol und dann auf **Bibliothek**.
2. Klicken Sie rechts oben auf das Pluszeichen und dann auf **Mobile App hinzufügen**.
3. Wählen Sie unter **Wählen Sie eine Anwendung** die Option **Android Enterprise-Apps**.
4. Suchen Sie eine App und genehmigen Sie sie im Fenster des Managed Google Play Store. Klicken Sie nach dem Schließen des Google-Fensters auf **Weiter**.
5. Fügen Sie Anwendungsdetails hinzu und klicken Sie auf **Weiter**.
6. Wenn Sie eine mobile Produktivitätsapp von Citrix gesucht und ausgewählt haben, können Sie Micro-VPN-Richtlinien konfigurieren. Nachdem Sie diese Richtlinien konfiguriert haben, klicken Sie auf **Weiter**.
7. Konfigurieren Sie Intune-App-Schutzrichtlinien. Klicken Sie auf **Weiter**.
8. Konfigurieren Sie die Anwendungseinstellungen. Die folgenden Konfigurationen ermöglichen den Datentransfer zwischen Citrix Endpoint Management- und Intune-Containern.
    - **Allow apps to receive data from other app:** Wählen Sie **Policy managed apps**.
    - **Allow app to transfer data to other apps:** Wählen Sie **All apps**.
    - **Restrict cut, copy, paste with other apps:** Wählen Sie **Policy managed apps**.
9. Konfigurieren Sie die Speicherrepositorys für gespeicherte Daten. Wählen Sie unter **Select which storage services corporate data can be saved to** die Option **LocalStorage**.
10. Optional: Legen Sie Data Relocation-, Access- und PIN-Richtlinien für die App fest. Klicken Sie auf **Weiter**.
11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

    Die App-Konfiguration kann einige Minuten dauern. Wenn sie abgeschlossen ist, wird gemeldet, dass die App in der Bibliothek veröffentlicht wurde. Die App ist in den Citrix Endpoint Management- und Intune-Konsolen verfügbar. In der Citrix Endpoint Management-Konsole ist die App Teil einer neuen Bereitstellungsgruppe und wird als App aus einem öffentlichen App-Store identifiziert.
12. Um der App Benutzergruppen zuzuweisen, klicken Sie auf **Benutzer zuweisen**.
13. Suchen Sie über das Suchfeld nach Benutzergruppen und klicken Sie auf diese, um sie hinzuzufügen. Sie können keine einzelnen Benutzer hinzufügen.
14. Wenn Sie alle Gruppen hinzugefügt haben, klicken Sie auf das X, um das Fenster zu schließen.

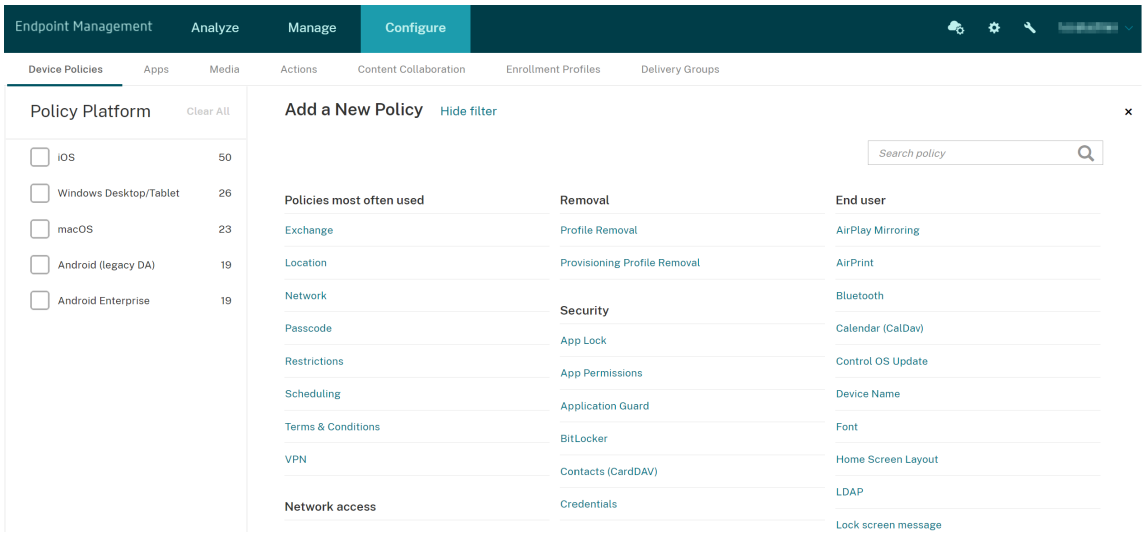
    Beim Hinzufügen von Benutzergruppen kann ein Fehler auftreten. Das ist der Fall, wenn die Benutzergruppe nicht mit dem lokalen Active Directory synchronisiert wurde.

Steuerung des Datentransfertyps zwischen verwalteten Apps

Mit Citrix Endpoint Management-Geräterichtlinien können Sie festlegen, welche Daten zwischen verwalteten Apps in den Citrix Endpoint Management- oder Intune-Containern übertragen werden können. Sie können eine Einschränkungsrichtlinie konfigurieren, sodass nur Daten mit dem Tag "corporate"zugelassen werden. Konfigurieren Sie eine App-Konfigurationsrichtlinie, um Datentags hinzuzufügen.

Konfigurieren der Geräteeinschränkungsrichtlinie:

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Geräterichtlinien**.
2. Klicken Sie auf der Seite **Geräterichtlinien** auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.



3. Klicken Sie in der Liste der Richtlinien auf **Einschränkungen**.
4. Geben Sie auf der Seite **Richtlinieninformationen** einen Namen und (optional) eine Beschreibung für die Richtlinie ein. Klicken Sie auf **Weiter**.
5. Um eine Geräterichtlinie für iOS-Apps zu erstellen, wählen Sie im Bereich **Plattformen** die Option **iOS**.
6. Wählen Sie unter **Sicherheit - Zulassen** für die Option **Dokumente von verwalteten Apps in nicht verwalteten Apps** die Einstellung **Aus**. Bei Auswahl von **Aus** werden auch **Nicht verwaltete Apps lesen verwaltete Kontakte** und **Verwaltete Apps schreiben nicht verwaltete Kontakte** auf **Aus** gesetzt. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Weiter**, bis die Schaltfläche **Speichern** angezeigt wird. Klicken Sie auf **Speichern**.

Konfigurieren Sie für jede App die Geräterichtlinie für die App-Konfiguration:

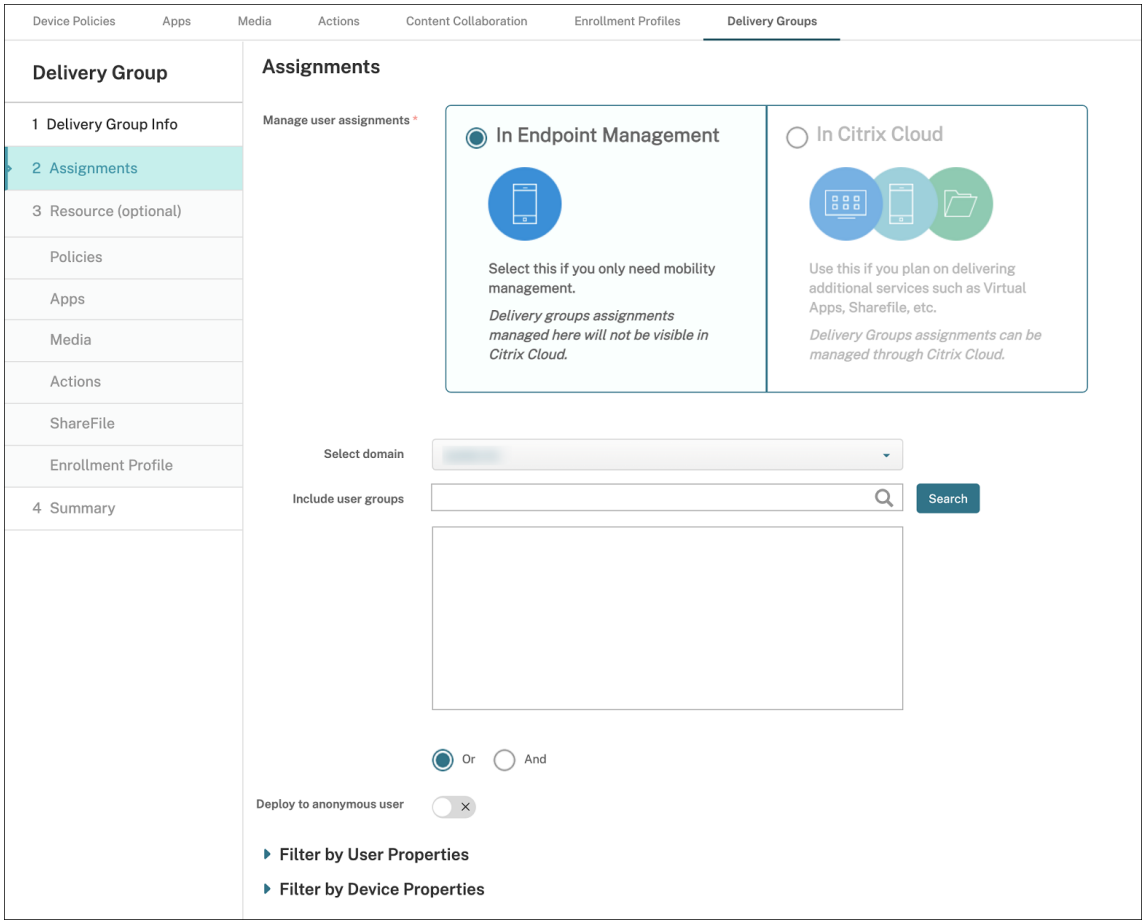
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Geräterichtlinien**.
2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.
3. Klicken Sie in der Liste der Richtlinien auf **App-Konfiguration**.
4. Geben Sie auf der Seite **Richtlinieninformationen** einen Namen und (optional) eine Beschreibung für die Richtlinie ein. Klicken Sie auf **Weiter**.
5. Um eine Geräterichtlinie für eine iOS-App zu erstellen, wählen Sie im Bereich **Plattformen** die Option **iOS**.
6. Wählen Sie den Bezeichner für die zu konfigurierende App aus.
7. Fügen Sie für iOS-Apps den folgenden Text zum **Wörterbuchinhalt** hinzu:

```
<dict>
    <key>IntuneMAMUPN</key>
    <string>${
 user.userprincipalname }
 </string>
</dict>
<!--NeedCopy-->
```

8. Klicken Sie auf **Wörterbuch prüfen**.
9. Klicken Sie auf **Weiter**.
10. Klicken Sie auf **Speichern**.

Konfigurieren von Bereitstellungsgruppen für Apps und Geräterichtlinien

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Bereitstellungsgruppen**.
2. Klicken Sie auf der Seite **Bereitstellungsgruppen** auf **Hinzufügen**. Die Seite **Bereitstellungsgruppeninformationen** wird angezeigt.
3. Geben Sie auf der Seite **Bereitstellungsgruppeninformationen** einen Namen und (optional) eine Beschreibung für die Bereitstellungsgruppe ein. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Zuweisungen** an, wie die Bereitstellungsgruppe bereitgestellt werden soll: Wählen Sie **In Citrix Endpoint Management** oder **In Citrix Cloud**.



5. Bei Auswahl von **In Citrix Endpoint Management**:

   - **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.

6. Klicken Sie auf **Weiter**.
7. Ziehen Sie auf der Seite **Richtlinien** die Einschränkungsrichtlinie und die App-Konfigurationsrichtlinie, die Sie erstellt haben, von links nach rechts. Klicken Sie auf **Weiter**.
8. Ziehen Sie auf der Seite **Apps** die Apps, die Sie bereitstellen möchten, von der linken Seite auf **Erforderliche Apps** oder **Optionale Apps**. Klicken Sie auf **Weiter**.
9. Konfigurieren Sie optional die Einstellungen auf den Seiten **Medien**, **Aktionen** und **Registrierungsprofil**. Oder übernehmen Sie auf jeder Seite die Standardwerte und klicken Sie auf **Weiter**.
10. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen für die Bereitstellungsgruppe und klicken Sie auf **Speichern**, um die Bereitstellungsgruppe zu erstellen.

Wählen Sie beim Veröffentlichen der App in der Intune-Konsole die Option **Verwaltung der App erzwingen**. Benutzer auf nicht betreuten Geräten werden aufgefordert, die Verwaltung der App zuzulassen. Wenn Benutzer die Eingabeaufforderung akzeptieren, wird die App auf dem Gerät verwaltet. Wenn Benutzer die Aufforderung ablehnen, ist die App auf dem Gerät nicht verfügbar.

Konfigurieren von Citrix Secure Mail

Citrix Secure Mail unterstützt jetzt verschiedene Konfigurationen. Sie können Citrix Secure Mail in einem Intune-MAM-Container umschließen, der mit einem On-Premises-Exchange Server verbunden ist. Sie können Citrix Secure Mail mit gehosteten Exchange- oder mit Office 365-Postfächern verbinden. Dieses Release unterstützt jedoch keine zertifikatbasierte Authentifizierung. Verwenden Sie stattdessen LDAP.

> **Wichtig:**
>
> Um Citrix Secure Mail im MDX-Modus zu verwenden, müssen Sie Citrix Endpoint Management MDM+MAM verwenden.

Citrix Secure Mail stellt außerdem automatisch die Benutzernamen bereit. Hierfür müssen Sie zunächst die folgenden benutzerdefinierten Richtlinien konfigurieren:

1. Wechseln Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Servereigenschaften** und klicken Sie dann auf **Hinzufügen**.
2. Klicken Sie in der Liste auf **Benutzerdefinierter Schlüssel** und geben Sie im Feld **Schlüssel** `xms.store.idpuser_attrs` ein.
3. Legen Sie den Wert auf **true** fest und geben Sie dann unter **Anzeigename** `xms.store.idpuser_attrs` ein. Klicken Sie auf **Speichern**.
4. Klicken Sie auf **Clienteigenschaften** und dann auf **Hinzufügen**.
5. Wählen Sie **Benutzerdefinierter Schlüssel** und geben Sie **SEND_LDAP_ATTRIBUTES** im Feld **Schlüssel** ein.
6. Geben Sie `userPrincipalName=${ user.userprincipalname } ,email=${ user.mail } ,displayname=${ user.displayname } ,sAMAccountName=${ user.samaccountname } ,aadupn=${ user.id_token.upn } ,aadtid=${ user.id_token.tid }` im Feld **Wert** ein. Geben Sie eine Beschreibung ein und klicken Sie auf **Speichern**.

   Die folgenden Schritte gelten nur für iOS-Geräte.
7. Gehen Sie zu **Konfigurieren > Geräterichtlinien** klicken Sie auf “Hinzufügen”und wählen die Richtlinie **App-Konfiguration**.
8. Geben Sie einen Richtliniennamen ein und klicken Sie auf **Weiter**.

   Klicken Sie in der Liste “ID”auf **Hinzufügen**. Geben Sie im angezeigten Textfeld die Paket-ID Ihrer Citrix Secure Mail-App ein.
9. Geben Sie im Feld **Wörterbuchinhalt** Folgendes ein:

```
<dict>

<key>XenMobileUserAttributes</key>

<dict>

<key>userPrincipalName</key>

<string>${
 user.userprincipalname }
 </string>

<key>email</key>

<string>${
 user.mail }
 </string>

<key>displayname</key>

```



```
<string>${
 user.displayname }
 </string>

<key>sAMAccountName</key>

<string>${
 user.samaccountname }
 </string>

<key>aadupn</key>

<string>${
 user.id_token.upn }
 </string>

<key>aadtid</key>

<string>${
 user.id_token.tid }
 </string>

</dict>

<key>IntuneMAMUPN</key>

<string>${
 user.id_token.upn }
 </string>

</dict>
```

10. Deaktivieren Sie das Kontrollkästchen **Windows Desktop/Tablet** und klicken Sie dann auf **Weiter**.
11. Wählen Sie die Benutzergruppen aus, für die die Richtlinie bereitgestellt werden soll, und klicken Sie dann auf **Speichern**.

Problembehandlung

Allgemeine Probleme

Problem: Beim Öffnen einer App wird folgende Fehlermeldung angezeigt: App-Richtlinie erforderlich.

Lösung: Fügen Sie Richtlinie der Microsoft Graph-API hinzu.

Problem: Es liegen Richtlinienkonflikte vor.

Lösung: Pro App ist nur eine Richtlinie zulässig.

Problem: Die App kann keine Verbindung zu internen Ressourcen herstellen.

Lösung: Stellen Sie sicher, dass die richtigen Firewallports geöffnet sind, korrigieren Sie ggf. die Mandanten-ID usw.

NetScaler Gateway-Probleme

In der folgenden Tabelle werden häufige Probleme mit der NetScaler Gateway-Konfiguration sowie Lösungen aufgeführt. Zur Problembehandlung aktivieren Sie weitere Protokolle und überprüfen diese, wie folgt:

1. Führen Sie an der Befehlszeilenschnittstelle den folgenden Befehl aus: `set audit syslogParams -logLevel ALL`
2. Überprüfen Sie die Protokolle über die Shell mit `tail -f /var/log/ns.log`.

Problem	Lösung
Die für die Konfiguration der Gateway-App in Azure erforderlichen Berechtigungen sind nicht verfügbar.	Überprüfen Sie, ob eine Intune-Lizenz verfügbar ist. Versuchen Sie eine Verwendung des Portals manage.windowsazure.com, um zu prüfen, ob die Berechtigung hinzugefügt werden kann. Wenden Sie sich an den Microsoft-Support, wenn das Problem weiterhin besteht.
NetScaler Gateway kann `login.microsoftonline.com` und `graph.windows.net` nicht erreichen.	Überprüfen Sie in der NS-Shell, ob Sie die folgende Microsoft-Website erreichen können: `curl -v -k https://login.microsoftonline.com`. Überprüfen Sie dann, ob DNS auf dem NetScaler Gateway konfiguriert ist und ob die Firewalleinstellungen korrekt sind (falls DNS-Anforderungen die Firewall passieren).
Ein Fehler erscheint in ns.log nachdem Sie OAuthAction konfiguriert haben.	Überprüfen Sie, ob die Intune-Lizenzierung aktiviert ist und die Azure Gateway-App über die richtigen Berechtigungen verfügt.
Der Befehl “OAuthAction”zeigt den OAuth-Status nicht als abgeschlossen an.	Überprüfen Sie die DNS-Einstellungen und Berechtigungen für die Azure Gateway-App.
Auf dem Android- bzw. iOS-Gerät wird die Zweifaktor-Authentifizierungsaufforderung nicht angezeigt.	Überprüfen Sie, ob das Zweifaktor-Geräte-ID-LogonSchema an den virtuellen Authentifizierungsserver gebunden ist.

OAuth-Fehlerbedingung und -status

Status	Fehlerbedingung
COMPLETE	Erfolg
AADFORGRAPH	Ungültiger Schlüssel, URL nicht aufgelöst, Verbindungstimeout
MDMINFO	*manage.microsoft.com ausgefallen oder nicht erreichbar
GRAPH	Graph-Endpunkt nicht erreichbar
CERTFETCH	Kommunikation mit Token Endpoint: `https://login.microsoftonline.com` wegen eines DNS-Fehlers nicht möglich. Um diese Konfiguration zu überprüfen, gehen Sie zur Shell und geben Sie `curl https://login.microsoftonline.com` ein. Der Befehl muss validieren.

Einschränkungen

Folgende Einschränkungen gelten bei der Verwendung von MEM mit Citrix Endpoint Management.

- Wenn Sie Apps mit Citrix und Intune zur Unterstützung von Micro-VPN bereitstellen: Wenn Benutzer ihren Benutzername und ihr Kennwort für den Zugriff auf Digest-Sites eingeben, erscheint ein Fehler, obwohl die Anmeldeinformationen gültig sind. [CXM-25227]
- Nach dem Ändern von **Split-Tunneling** von **Ein** in **Aus** und Warten auf das Ablaufen der aktuellen Gateway-Sitzung wird externer Datenverkehr direkt und ohne Leitung über NetScaler Gateway gesendet, bis der Benutzer eine interne Site im Modus “vollständiges VPN”startet. [CXM-34922]
- Nach dem Ändern der Öffnen-in-Richtlinie von **Nur verwaltete Apps** in **Alle Apps** können Benutzer Dokumente erst dann in nicht verwalteten Apps öffnen, wenn sie Citrix Secure Mail geschlossen und neu gestartet haben. [CXM-34990]
- Wenn im Modus “vollständiges VPN”Split-Tunneling auf **Ein** festgelegt ist und Split DNS von lokal zu remote wechselt, können interne Sites nicht geladen werden. [CXM-35168]

Bekannte Probleme

Wenn die mVPN-Richtlinie **HTTP/HTTPS-Umleitung (mit SSO) aktivieren** deaktiviert ist, funktioniert Citrix Secure Mail nicht. [CXM-58886]

Probleme mit Drittanbieterprodukten

Wenn ein Benutzer in Citrix Secure Mail für Android auf **Neues Ereignis erstellen**tippt, wird die Seite zum Erstellen von Ereignissen nicht angezeigt. [CXM-23917]

Wenn Sie Citrix Secure Mail für iOS mit Citrix und Intune zur Unterstützung von Micro-VPN bereitstellen, wird die App-Richtlinie, die den Citrix Secure Mail-Bildschirm überlagert, wenn Benutzer die App in den Hintergrund verschieben, nicht erzwungen. [CXM-25032]

Onboarding und Einrichten von Ressourcen

March 11, 2024

Wenn Sie Citrix, Citrix Cloud oder Citrix Endpoint Management das erste Mal verwenden, führt Sie in dieser Artikel durch das Onboarding. Erfahren Sie mehr über den Workflow und die Details, die Sie benötigen, um loszulegen.

- **Wo fange ich an?**
  - Wenn Sie kein Citrix Endpoint Management-Abonnement erworben haben, finden Sie weitere Informationen unter Für neue Citrix-Kunden.
  - Wenn Sie ein Citrix Endpoint Management-Abonnement erworben haben, fahren Sie mit Wenn die Schaltfläche "Verwalten"verfügbar ist fort.
  - Wenn Ihre Citrix Endpoint Management-Site bereitgestellt ist, fahren Sie mit Konfigurieren der Authentifizierung fort.
- **Ist die Konfigurationsreihenfolge wichtig?** Dieser Artikel folgt einer empfohlenen Konfigurationsreihenfolge. Sie können in einer anderen Reihenfolge arbeiten. In der Citrix Endpoint Management-Konsole erfahren Sie, ob Voraussetzungen fehlen, z. B. durch Meldungen wie "Einrichten nach dem Provisioning".
- **Was mache ich nach dem Onboarding?** Nachdem Sie das Onboarding und die Ressourcenkonfiguration wie in diesem Artikel beschrieben abgeschlossen haben, setzen Sie Ihre Konfiguration in der Citrix Endpoint Management-Konsole fort. Informationen zu den nächsten Schritten finden Sie unter Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen.

Für neue Citrix-Kunden

Für Citrix Cloud-Kunden, die Citrix Endpoint Management das erste Mal verwenden:

Wenn Sie bereits ein Citrix Endpoint Management-Abonnement erworben haben, fahren Sie mit Wenn die Schaltfläche "Verwalten"verfügbar ist fort.

Wenn Sie noch kein Citrix Cloud-Konto eingerichtet haben, lesen Sie Bei Citrix Cloud registrieren.

Wenn Sie bereits ein Citrix Cloud-Konto eingerichtet haben, Citrix Endpoint Management aber noch nicht erworben haben, fordern Sie eine Servicedemo an.

1. Verwenden Sie Ihre Citrix Cloud-Administratoranmeldeinformationen, um sich bei Ihrem Citrix Cloud-Konto anzumelden. Die Citrix Cloud-Homepage wird angezeigt.

   Alle Citrix Cloud-Administratorkonten werden wie folgt erstellt:

   - Citrix Cloud-Administratoren sind standardmäßig auch Citrix Endpoint Management-Administratoren.
   - Citrix Cloud-Administratoren, die mit Kundenzugriff erstellt wurden, müssen Citrix Endpoint Management ausgewählt haben, damit sie Citrix Endpoint Management verwalten können.

2. Suchen Sie auf der Citrix Cloud-Homepage die Kachel für den Citrix Endpoint Management Service aus und klicken Sie auf **Demo anfordern**.
3. Füllen Sie das Formular zum Anfordern einer Demoversion aus und senden Sie es ab. Die Schaltfläche auf der Kachel für den Citrix Endpoint Management Service ändert sich in **Demo angefordert**.

Wenn Sie vor der Bearbeitung der Anforderung auf die Kachel für den Citrix Endpoint Management Service klicken, werden Sie aufgefordert, sich an Ihren Vertriebsmitarbeiter oder Partner zu wenden. Ein Citrix-Vertriebsmitarbeiter kann weitere Informationen und Details über den Service geben.

Bereiten Sie sich während der Wartezeit auf die Citrix Endpoint Management-Bereitstellung vor, indem Sie den Artikel Systemanforderungen lesen. Citrix hostet zwar Ihre Citrix Endpoint Management-Lösung, es gelten jedoch einige Anforderungen an Kommunikation und Ports.

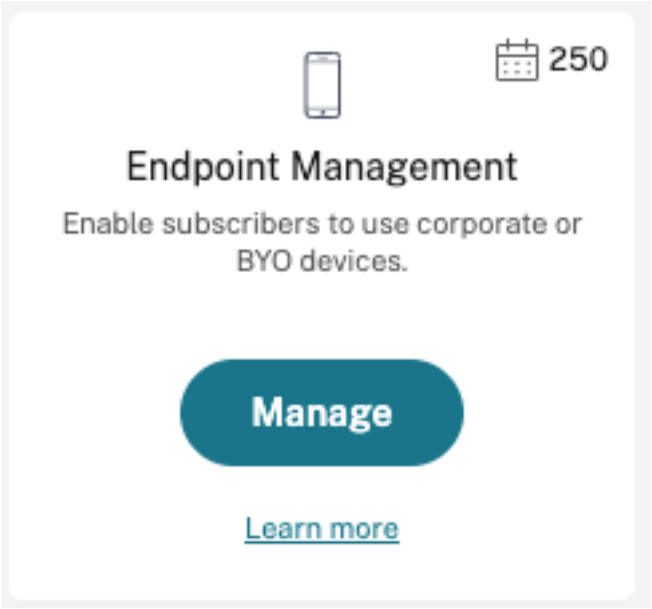
Fahren Sie mit dem nächsten Abschnitt fort.

Wenn die Schaltfläche “Verwalten”verfügbar ist

In diesem Video wird das Onboarding erläutert:

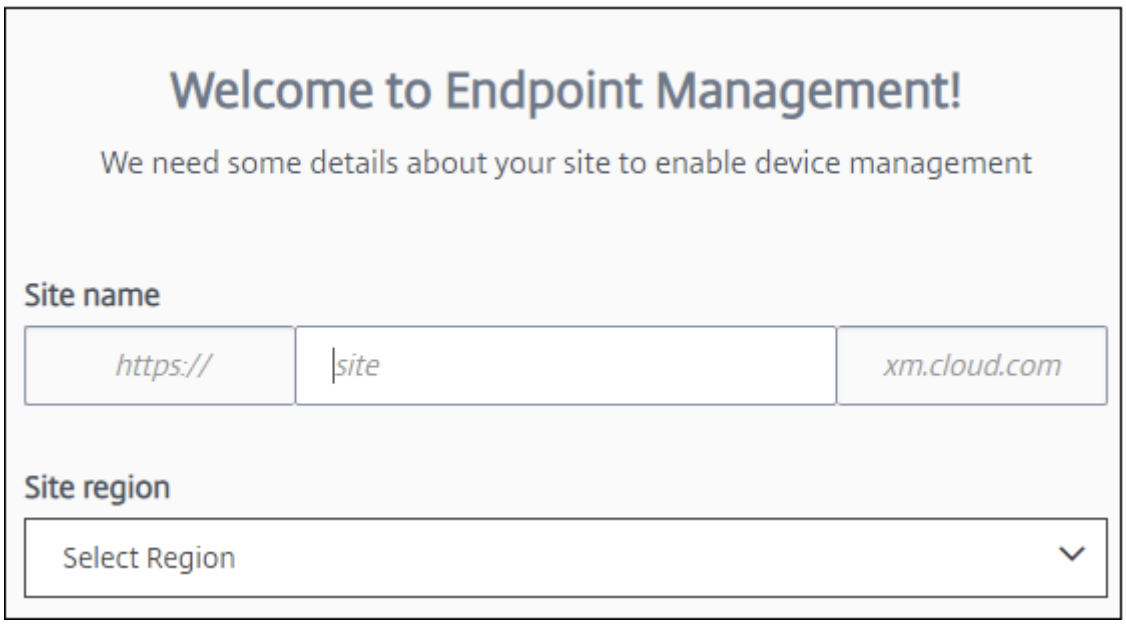
Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Wenn Ihr Citrix Endpoint Management Service verfügbar ist, ändert sich die Schaltfläche auf der Kachel für den Citrix Endpoint Management Service in **Verwalten**.



Mit dem Einrichten beginnen:

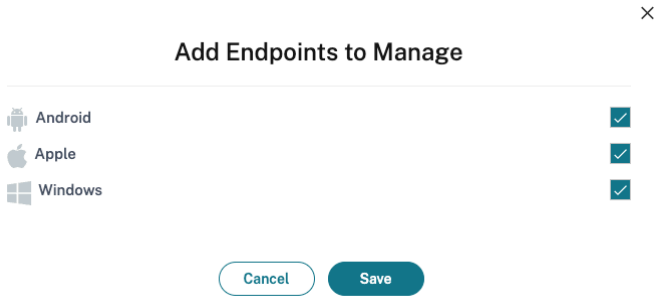
1. Melden Sie sich mit Ihren Citrix Cloud-Administratoranmeldeinformationen bei Ihrem Citrix Cloud-Konto an.
2. Klicken Sie auf der Citrix Endpoint Management-Kachel auf **Verwalten**, um die Citrix Endpoint Management-Konsole zu öffnen.
3. Geben Sie Ihren Websitenamen ein und wählen Sie eine Region aus. Wählen Sie dann **Speichern und Fortfahren**.



> **Hinweis:**
>
> Wenden Sie sich an den Citrix Support-Mitarbeiter, um eine IP-Positivliste anzufordern.

Die Citrix Endpoint Management-Konsole wird dann geöffnet und es wird eine Meldung angezeigt, die darauf hinweist, dass während des laufenden Provisioning der Suite einige Citrix Endpoint Management-Funktionen gesperrt sind.

1. Klicken Sie im **Begrüßungsbildschirm** auf **Setup starten**.
2. Wählen Sie die Endpunkte aus, die Sie verwalten möchten, und klicken Sie auf **Speichern**. Sie können Endpunkte jederzeit hinzufügen oder löschen, um sie in der Konsole ein- oder auszublenden. Das Ein- und Ausblenden von Endpunkten wirkt sich nicht auf Ihre Konfiguration aus.



Wir senden Ihnen eine E-Mail, wenn das Provisioning abgeschlossen ist.

Ressourcencenter


Klicken Sie auf das **Ressourcencenter-Symbol**, um Anleitungsvideos zu sehen, ohne die Konsole zu verlassen.

Während des Provisionings

Während wir das Provisioning von Citrix Endpoint Management durchführen, können Sie mit der Konfiguration beginnen.

Konfigurieren von Ressourcenstandorten

Sie benötigen Ressourcenstandorte, bevor Sie Lightweight Directory Access Protocol (LDAP)-Verbindungen für Citrix Endpoint Management konfigurieren können. Ressourcenstandorte enthalten die Ressourcen zum Bereitstellen von Cloudservices für Ihre Abonnenten. Sie benötigen

einen Ressourcenstandort pro Domäne. Weitere Informationen finden Sie im Citrix Cloud-Artikel zu Ressourcenstandorten.

Bereiten Sie sich während der Wartezeit auf die Citrix Endpoint Management-Bereitstellung vor, indem Sie den Artikel Systemanforderungen lesen. Citrix hostet zwar Ihre Citrix Endpoint Management-Lösung, es gelten jedoch einige Anforderungen an Kommunikation und Ports. Bei diesem Setup wird die Citrix Endpoint Management-Infrastruktur mit Unternehmensdiensten wie Active Directory verbunden. Die Informationen, die Sie bereitstellen müssen, sind im Onboarding Handbook unter "Citrix Endpoint Management Trial Sales Engineer engagement"aufgeführt

Nachdem Sie die Genehmigung zum Zugriff auf die Testversion erhalten haben, ändert sich die Schaltfläche **Citrix Endpoint Management** in **Verwalten**. Klicken Sie auf **Verwalten**, um die Citrix Endpoint Management-Konsole zu öffnen.

Authentifizierung konfigurieren

Nachdem die Site bereitgestellt wurde, können Sie mit der Konfiguration fortfahren. Es wird empfohlen, einen cloudgehosteten Identitätsanbieter (IdP) oder Lightweight Directory Access Protocol (LDAP) für den Import von Gruppen, Benutzerkonten und zugehörigen Eigenschaften einzurichten.

Konfigurieren von IdP

Citrix Endpoint Management unterstützt die Authentifizierung mit Identitätsanbietern wie Azure Active Directory, Okta und On-Premises-NetScaler Gateway.

Konfigurieren eines IdP in Citrix Cloud und Einrichten für Citrix Endpoint Management:

- Authentifizierung mit Azure Active Directory über Citrix Cloud
- Authentifizierung mit Okta über Citrix Cloud
- Authentifizierung mit einem On-Premises-NetScaler Gateway über Citrix Cloud

Konfigurieren von LDAP

Sie können eine Verbindung in Citrix Endpoint Management zu einem oder mehreren LDAP-kompatiblen Verzeichnissen für die domänenbasierte Authentifizierung konfigurieren. Citrix Endpoint Management unterstützt Gruppen, die in LDAP verschachtelt sind. Verschachtelte Gruppen werden täglich um 12 Uhr Ortszeit synchronisiert.

Im Rahmen der Konfiguration von LDAP müssen Sie mindestens einen Cloud Connector installieren.

Für einen schnellen Überblick sehen Sie sich dieses Video an.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Einrichten von LDAP:

1. Scrollen Sie auf der Seite **Einstellungen** zur **LDAP**-Kachel und klicken Sie dann auf **Einrichten**.
2. Folgen Sie den Anweisungen auf dem Bildschirm, um einen Cloud Connector herunterzuladen und zu installieren. Cloud Connectors sind für die Kommunikation zwischen Citrix Cloud und Ihren Ressourcen erforderlich. Weitere Informationen finden Sie unter Citrix Cloud Connector.

Wenn Sie LDAP konfiguriert haben und Azure AD oder Okta als Identitätsanbieter hinzufügen, synchronisiert Citrix Endpoint Management IdP-spezifische Informationen für Ihre Active Directory-Gruppen in der Citrix Endpoint Management-Datenbank. Diese Konfiguration wirkt sich nicht auf vorhandene Bereitstellungsgruppen und Benutzerregistrierungen aus. Sie können jedoch danach keine LDAP-Einstellungen in Citrix Endpoint Management hinzufügen. Weitere Informationen finden Sie unter Identitätsanbieter-Authentifizierung.

Wenn Sie die Einstellungen **Domänenalias** und **Benutzersuche nach** nach der Registrierung ändern, müssen Benutzer sich neu registrieren. Weitere Informationen zur LDAP-Konfiguration finden Sie unter Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken.

Nach dem Einrichten von LDAP können Sie mit der Authentifizierungskonfiguration fortfahren oder eine bestimmte Plattform einrichten.

Konfigurieren von NetScaler Gateway

Bei Integration in Citrix Endpoint Management bietet NetScaler Gateway Remotezugriff von Geräten auf das interne Netzwerk und interne Ressourcen.

Citrix Endpoint Management erfordert NetScaler Gateway für folgende Szenarios:

- Sie benötigen ein Micro-VPN, damit branchenspezifische Apps auf interne Netzwerkressourcen zugreifen können. Die Apps sind mit der Citrix MDX-Technologie umschlossen. Das Micro-VPN muss über NetScaler Gateway eine Verbindung zu internen Backend-Infrastrukturen herstellen.
- Sie möchten Citrix Endpoint Management zum Verwalten von Apps verwenden (MAM oder MDM+MAM). NetScaler Gateway ist nicht erforderlich, um nur Geräte zu verwalten (MDM).
- Sie planen, Citrix Endpoint Management mit Microsoft Endpoint Manager zu integrieren. (Erfordert ein on-premises NetScaler Gateway.)

Für einen schnellen Überblick sehen Sie sich dieses Video an.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Die folgende Tabelle enthält alle Features, die von on-premises NetScaler Gateway-Lösungen unterstützt werden.

Unterstützte Features	NetScaler Gateway (on-premises)
Citrix Secure Mail (STA)*	Ja
Tunnel mit Web-SSO (Web-Single Sign-On)	Ja
Vollständiges VPN (nicht für mobile Citrix Produktivitätsapps für iOS verfügbar)	Ja
Pro-App-VPN	Ja
Mobiles Single Sign-On (Zugriffssteuerung)	no
Hohe Verfügbarkeit	Ja**
Multi-POP-Bereitstellung	Ja***
Proxyunterstützung	Ja
Split-Tunneling	Ja
Split-DNS	Ja

* Konfiguration mit Citrix Cloud STA-Dienst (Secure Ticket Authority)

** On-Premises-Konfiguration

*** Konfiguration mit Global Server Load Balancing

Anwendungsfälle für NetScaler Gateway (On-Premises-Version)

Verwenden Sie in folgenden Situationen Citrix Endpoint Management mit mindestens einer on-premises NetScaler Gateway-Appliance:

- Sie benötigen Funktionen mit Pro-App-VPN.
- Sie benötigen einen vollständigen Tunnel, Split-Tunneling, Reverse-Split-Tunneling oder Split DNS. Wir empfehlen die Einstellung "Vollständiger VPN-Tunnel"für Verbindungen, die Clientzertifikate oder End-To-End-SSL für Ressourcen im internen Netzwerk einsetzen.
- Sie verwenden die Citrix Endpoint Management-Integration mit Microsoft Endpoint Manager.

Um ein on-premises NetScaler Gateway zu verwenden, ist ein erheblicher Konfigurations- und Wartungsaufwand erforderlich. Nachdem Sie LDAP und NetScaler Gateway in der Citrix Endpoint Management-Konsole konfiguriert haben, exportieren Sie ein Skript von dieser Konsole. Anschließend führen Sie das Skript in NetScaler Gateway aus.

1. Scrollen Sie auf der Seite **Einstellungen** zur **NetScaler Gateway**-Kachel und klicken Sie auf **Setup starten**.
2. Wählen Sie **NetScaler Gateway (on-premises)** als Typ aus.

3. Folgen Sie den Anweisungen auf dem Bildschirm. Weitere Informationen finden Sie unter Konfigurieren eines on-premises NetScaler Gateway für Citrix Endpoint Management.

Konfigurieren des Benachrichtigungsservers

Zum Senden von Benachrichtigungen müssen Sie ein Gateway und einen Benachrichtigungsserver konfigurieren. Ein Benachrichtigungsserver stellt die Konnektivität sicher und ermöglicht die Kommunikation zwischen Endbenutzern und dem Administrator. Informationen zum Einrichten eines Benachrichtigungsservers in Citrix Endpoint Management finden Sie unter Benachrichtigungen.

Konfigurieren eines APNs-Zertifikats für Apple-Geräte

Citrix Endpoint Management erfordert ein APNs (Apple Dienst für Pushbenachrichtigungen)-Zertifikat von Apple, um Apple-Geräte zu registrieren und zu verwalten. Citrix Endpoint Management erfordert außerdem ein APNs-Zertifikat, wenn Sie Pushbenachrichtigungen für Citrix Secure Mail für Apple verwenden möchten. Informationen zu Citrix Endpoint Management und APNs finden Sie unter Pushbenachrichtigungen für Citrix Secure Mail für iOS.

Um ein Zertifikat von Apple zu erhalten, benötigen Sie eine Apple-ID und ein Entwicklerkonto. Informationen finden Sie unter Apple Developer Program.

Für einen schnellen Überblick sehen Sie sich dieses Video an.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Konfigurieren von APNs mit einer Citrix-Zertifikatsignieranforderung:

1. Erweitern Sie auf der Seite **Einstellungen** die Kachel **Apple**.
2. Klicken Sie auf der Kachel **APNs-Zertifikat** auf **Einrichten** und folgen Sie dann den Anweisungen auf dem Bildschirm.

Weitere Informationen finden Sie unter Zertifikate und Authentifizierung.

Konfigurieren von Android Enterprise

Citrix Endpoint Management ist vollständig konfiguriert, wenn Sie Bereitstellungsgruppen erstellt und ihnen Benutzer über die Cloud-Bibliothek zugewiesen haben. Von diesem Zeitpunkt an findet die Citrix Endpoint Management-Verwaltung in der Citrix Cloud statt. Die kombinierte Schnittstelle vereinfacht den Wechsel zwischen Citrix Cloud und Citrix Endpoint Management.

Sie können Android Enterprise für Citrix Endpoint Management mit Google Play oder Google Workspace einrichten.

1. **Wenn Ihre Organisation Google Workspace nicht verwendet:** Mit verwaltetem Google Play können Sie Citrix als Ihren EMM-Anbieter registrieren. 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 die von Ihnen zur Verfügung gestellten Firmen-Apps installieren und verwenden. 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. Mit dieser Konfiguration können Sie verschiedene Unternehmen verwenden, um separate Gruppen von Geräten und Apps zu verwalten.

2. **Wenn Ihre Organisation bereits Google Workspace verwendet, um Benutzern Zugriff auf Google-Apps zu ermöglichen:** Mit Google Workspace können Sie Citrix als EMM registrieren. Wenn Ihre Organisation Google Workspace verwendet, besitzt sie eine Unternehmens-ID und Google-Konten für Benutzer. Um Citrix Endpoint Management mit Google Workspace zu verwenden, führen Sie eine Synchronisierung mit Ihrem LDAP-Verzeichnis durch und rufen Google-Kontoinformationen über die Google Directory-API ab.

   Dieser Unternehmenstyp ist an eine vorhandene Domäne gebunden. Daher kann jede Domäne nur ein Unternehmen erstellen. Um ein Gerät bei Citrix Endpoint Management zu registrieren, muss sich jeder Benutzer manuell mit dem vorhandenen Google-Konto anmelden. Über dieses Konto können Benutzer auf verwaltetes Google Play zugreifen und die übrigen Google-Dienste nutzen, die von Ihrem Google Workspace-Tarif bereitgestellt werden.

Für einen schnellen Überblick sehen Sie sich dieses Video an.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Erste Schritte:

1. Erweitern Sie auf der Seite **Einstellungen** die Kachel **Android**.
2. Klicken Sie auf der Kachel **Android Enterprise** auf **Einrichten**.
3. Wählen Sie **Google Play** oder **G Suite** aus, je nachdem, wie Sie Benutzern Zugriff auf Google-Anwendungen gewähren.
   Wenn Sie zuvor die Android Enterprise Plattform mit Google Play konfiguriert haben, führt Sie die Benutzeroberfläche zum Google Play Store, um sich neu zu registrieren. Klicken Sie auf **Neu registrieren**, kehren Sie zur CEM-Konsole zurück und aktualisieren Sie die Seite.
4. Folgen Sie den Anweisungen auf dem Bildschirm.

Siehe:

- Erstellen eines Android Enterprise-Kontos

Konfigurieren von Firebase Cloud Messaging

Citrix empfiehlt, dass Sie mit Firebase Cloud Messaging (FCM) steuern, wie und wann Android-Geräte eine Verbindung zu Citrix Endpoint Management herstellen. Citrix Endpoint Management sendet 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 dem Citrix Endpoint Management-Server herzustellen. Siehe Firebase Cloud Messaging.

Integration mit Microsoft Endpoint Manager

Durch die Integration von Citrix Endpoint Management mit Microsoft Endpoint Manager können Microsoft Intune-fähige Apps (z. B. Microsoft Edge Browser) die Vorteile von Citrix Endpoint Management Micro-VPN nutzen.

Bei einer Citrix Endpoint Management-Integration mit MEM können unternehmenseigene branchenspezifische Apps außerdem mit Intune und Citrix umschlossen werden. Das Umschließen von Apps bietet Micro-VPN-Funktionen in einem Intune Mobile App Management (MAM)-Container. Das Micro-VPN von Citrix Endpoint Management ermöglicht Apps den Zugang zu lokalen Ressourcen. Sie können Office 365-Apps, branchenspezifische Apps und Citrix Secure Mail in einem einzigen Container verwalten und bereitstellen. Ein einziger Container bietet ultimative Sicherheit und Produktivität.

- Citrix Cloud-Administratoren sind standardmäßig auch Citrix Endpoint Management-Administratoren.
- Citrix Cloud-Administratoren, die mit Kundenzugriff erstellt wurden, müssen Citrix Endpoint Management ausgewählt haben, damit sie Citrix Endpoint Management verwalten können.

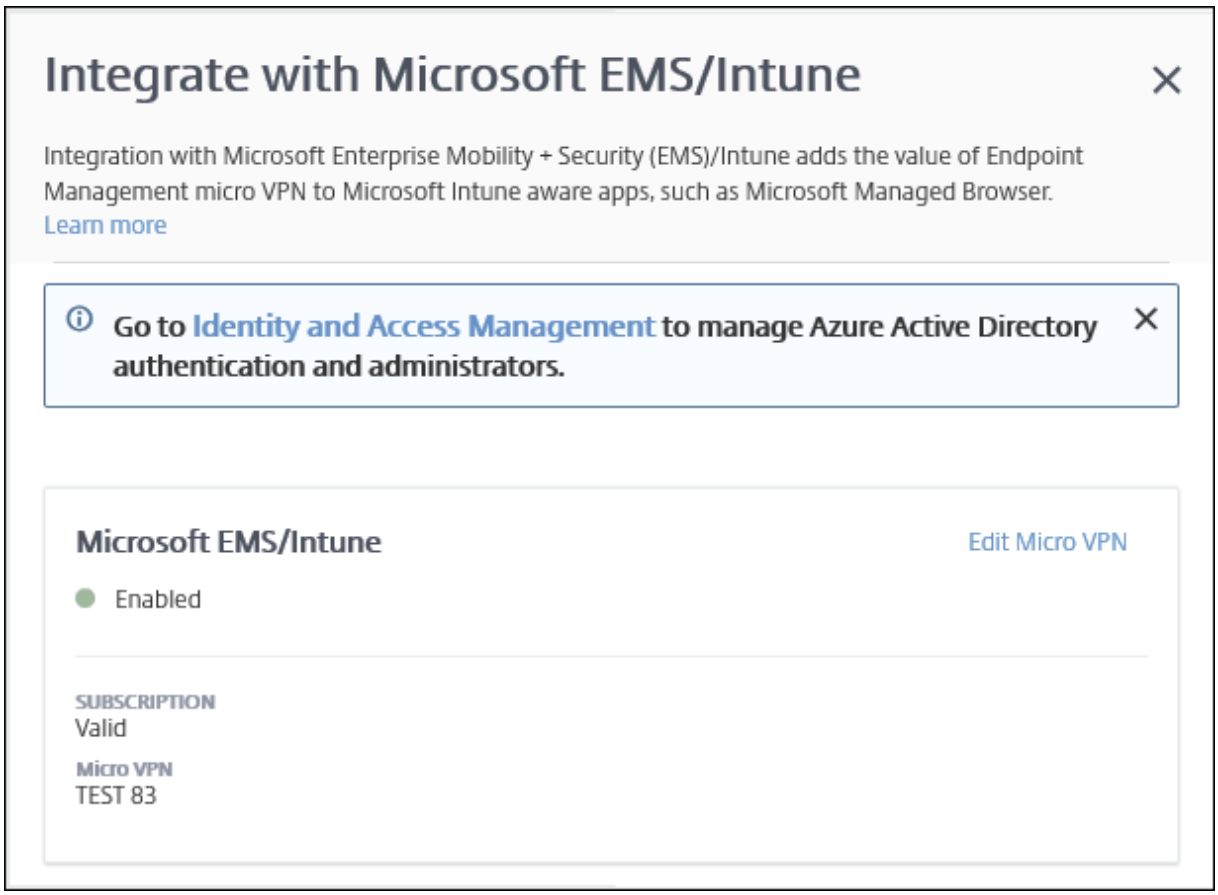
In der Citrix Endpoint Management-Konsole können Sie nur die Rolle und Mitgliedschaft eines Benutzers ändern. Um jederzeit eine Rolle zu ändern, greifen Sie über das Citrix Cloud-Dashboard auf die Citrix Endpoint Management-Konsole zu. Wechseln Sie zur Registerkarte **Verwalten** und klicken Sie auf **Benutzer**. Wählen Sie einen bestimmten Benutzer aus und klicken Sie auf **Bearbeiten**, um die Rolle zu ändern. Weitere Informationen finden Sie unter Rollen mit RBAC konfigurieren.

Informationen zur Integration mit MEM finden Sie unter Integration von Citrix Endpoint Management mit Microsoft Endpoint Manager.

Nachdem Sie die Konfiguration in Citrix Cloud abgeschlossen haben, kehren Sie wie folgt zur Citrix Endpoint Management-Konsole zurück: Gehen Sie zur **Citrix Cloud-Homepage** und klicken Sie dann auf der Kachel **Citrix Endpoint Management** auf **Verwalten**. Anschließend können Sie überprüfen, ob Sie sich mit Ihrem Azure Active Directory-Konto bei Citrix Endpoint Management angemeldet haben.

1. Scrollen Sie auf der Seite **Einstellungen** zur Kachel **Integration mit Microsoft EMS/Intune**.

2. Klicken Sie auf **Weitere Informationen**. Die Benutzeroberfläche zeigt an, ob Sie die Verbindung erfolgreich aktiviert haben.

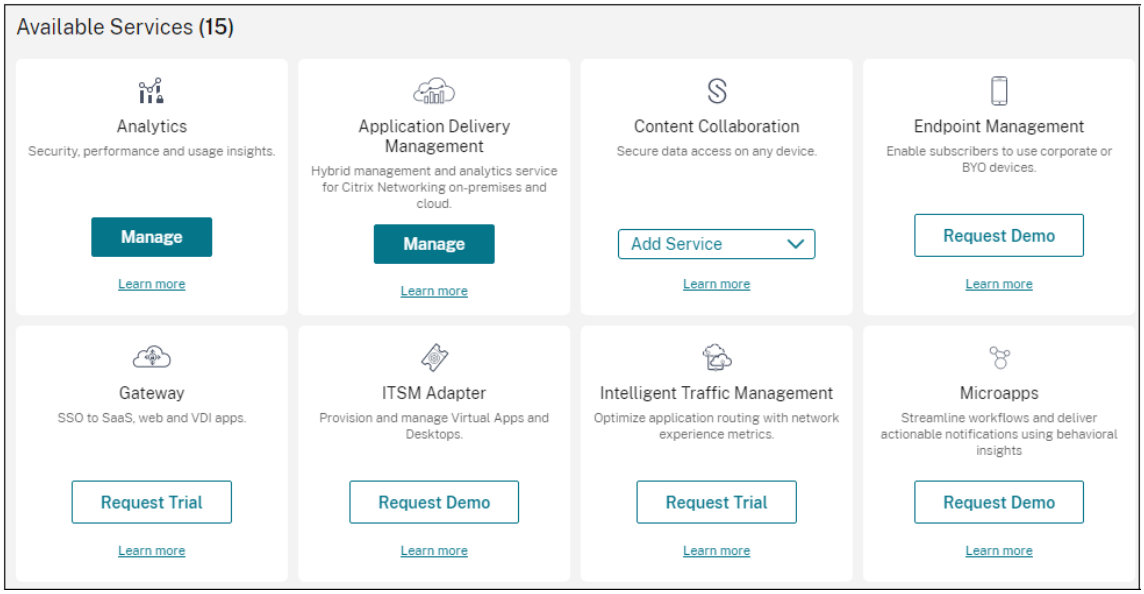


In der Citrix Cloud-Konsole können Sie auch Benutzernamen oder Kennwörter ändern und lokale Benutzer löschen oder bearbeiten. Siehe Identitäts- und Zugriffsverwaltung.

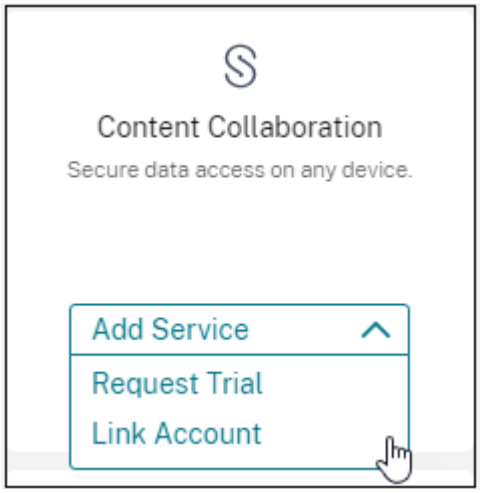
Verknüpfen eines ShareFile-Kontos mit Citrix Cloud

Wenn Sie ein ShareFile-Konto haben, das bereits bestand, bevor Sie sich bei Citrix Cloud registriert haben, müssen Sie dieses Konto mit Citrix Cloud verknüpfen. Um das Konto verknüpfen zu können, muss Ihre E-Mail-Adresse Administrator des ShareFile-Kontos sein. Wenn Sie bereit sind, fortzufahren, navigieren Sie zu https://onboarding.cloud.com.

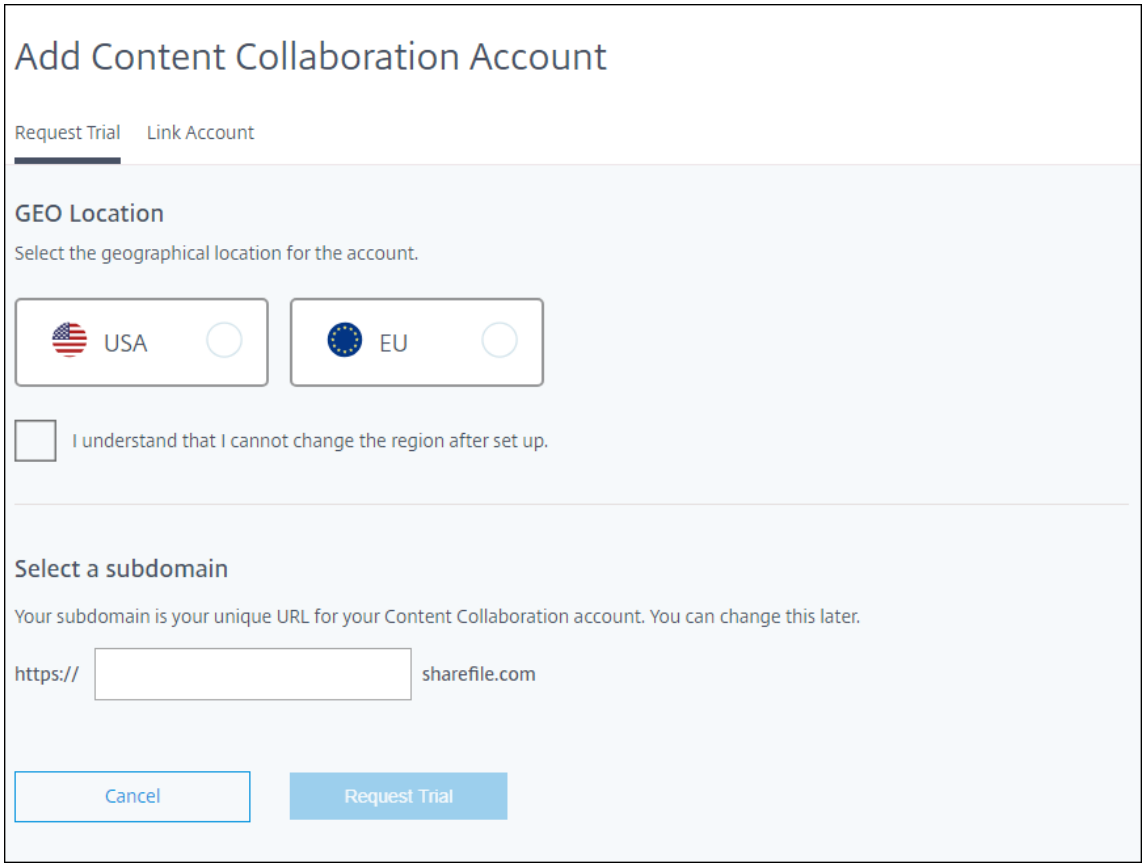
1. Nach der Anmeldung wird ein Bildschirm angezeigt, der in etwa so aussieht:



2. Wählen Sie in der **ShareFile**-Kachel **Konto verknüpfen**.



3. Wenn Citrix Ihr ShareFile-Konto bestätigt hat, wird die folgende Seite angezeigt:



4. Klicken Sie auf **Konto verknüpfen**, um den Vorgang abzuschließen. Sie können Ihr ShareFile-Konto dann sofort von Citrix Cloud aus verwalten.

Überlegungen zur Skalierung und Größe für Cloud Connectors

December 1, 2023

Wenn Sie Citrix Endpoint Management auf Dimensionierung und Skalierbarkeit prüfen, sollten Sie die Konfiguration der Cloud Connectors an Ihre spezifischen Anforderungen anpassen und testen. Cloud Connector ist nur während der Geräteregistrierung unter Last. Zu knapp dimensionierte Maschinen können sich negativ auf die Systemleistung auswirken.

Citrix benötigt zwei Cloud Connectors pro Ressourcenstandort. Installieren Sie Cloud Connector auf einem dedizierten Server, der nicht von anderen Komponenten oder Produkten genutzt wird. In unseren Tests wurden Cloud Connectors in Hochverfügbarkeitsgruppen bereitgestellt (**ohne Lastausgleich**).

Testkonfiguration

- Zwei dedizierte Windows Server 2019, 2 vCPU, 4 GB Arbeitsspeicher
- Registrierung von Android- und iOS-Geräten in MDM+MAM, bei gleichmäßiger Verteilung über einen Zeitraum von 8 Stunden
- Citrix Endpoint Management-Konfiguration mit 125 registrierten Geräten pro Stunde pro 1000 Geräte
  - 1000 Geräte (125 Geräteregistrierungen pro Stunde)
  - 5000 Geräte (625 Geräteregistrierungen pro Stunde)
  - 10.000 Geräte (1250 Geräteregistrierungen pro Stunde)
  - 20.000 Geräte (2500 Geräteregistrierungen pro Stunde)

Testergebnisse

Cloud Connector	1000 Geräte	5000 Geräte	10.000 Geräte	20.000 Geräte
Mittlere CPU	2 %	2 %	4 %	4 %
Max. CPU	8 %	8 %	10 %	11 %
Mittlerer Speicher	73 %	73 %	75 %	75 %
Max. Speicher	76 %	76 %	76 %	79 %

Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen

March 11, 2024

> **Wichtig:**
>
> Bevor Sie fortfahren, müssen Sie alle Schritte ausführen, die unter Onboarding und Einrichten von Ressourcen beschrieben werden.
>
> Halten Sie Ihre Benutzer über bevorstehende Änderungen auf dem Laufenden. Siehe Welcome to your Citrix User Adoption Kit.

Citrix Endpoint Management unterstützt verschiedene Registrierungsoptionen. In diesem Artikel wird das Basissetup beschrieben, das für die Registrierung aller unterstützten Geräte erforderlich ist. Die folgende Abbildung fasst die Grundschritte für das Setup zusammen.

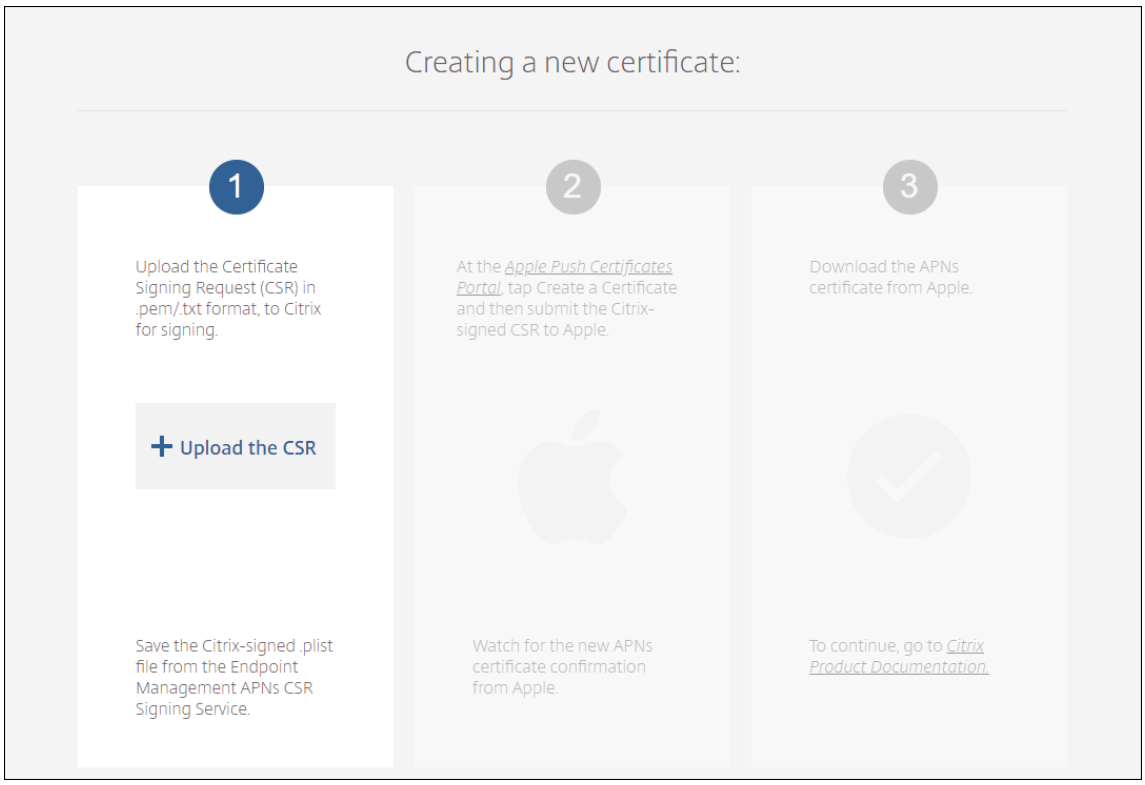
Eine Liste der unterstützten Geräte finden Sie unter Unterstützte Gerätebetriebssysteme.

Einrichten eines APNs-Zertifikats für iOS-Geräte

> **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 20.1.0 unterstützt Citrix Endpoint Management 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.

Citrix Endpoint Management erfordert ein APNs (Apple Dienst für Pushbenachrichtigungen)-Zertifikat von Apple, um iOS-Geräte zu registrieren und zu verwalten. Citrix Endpoint Management erfordert außerdem ein APNs-Zertifikat für Citrix Secure Mail für iOS-Pushbenachrichtigungen.

- Um ein Zertifikat von Apple zu erhalten, benötigen Sie eine Apple-ID und ein Entwicklerkonto. Informationen finden Sie unter Apple Developer Program.
- Um ein APNs-Zertifikat zu erhalten und in Citrix Endpoint Management zu importieren, siehe APNs-Zertifikate.



- Weitere Informationen zu Citrix Endpoint Management und APNs finden Sie unter Pushbenachrichtigungen für Citrix Secure Mail für iOS.

Einrichten von Firebase Cloud Messaging (FCM) für Android-Geräte

Firebase Cloud Messaging (FCM) steuert, wie und wann Android-Geräte eine Verbindung zum Citrix Endpoint Management-Dienst herstellen. Sicherheitsaktionen oder Bereitstellungsbefehle lösen eine Pushbenachrichtigung aus. Die Benachrichtigung fordert Benutzer auf, sich neu mit Citrix Endpoint Management zu verbinden.

- Für das FCM-Setup müssen Sie Ihr Google-Konto konfigurieren. Zum Erstellen von Google Play-Anmeldeinformationen siehe Manage your developer account information. Sie verwenden auch Google Play zum Hinzufügen, Erwerben und Genehmigen von Apps für die Bereitstellung in dem Android Enterprise-Workspace von Geräten. Über Google Play können Sie private Android-Apps, öffentliche Apps und solche von Drittanbietern bereitstellen.
- Zum Einrichten von FCM, siehe Firebase Cloud Messaging.

Einrichten von Citrix Endpoint Management AutoDiscovery Service

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 Citrix Endpoint Management-Bereitstellungen.

Der Autodiscoverydienst bietet folgende Vorteile:

- Benutzer können ihre Geräte mit den Anmeldeinformationen für das Unternehmensnetzwerk registrieren.
- Benutzer müssen keine Details zur Citrix Endpoint Management-Serveradresse 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 Citrix Endpoint Management verwendet wird. Wenden Sie sich an den Citrix Support, um das Zertifikatpinning für Ihre Citrix Endpoint Management-Sites zu konfigurieren. Informationen über das Zertifikatpinning finden Sie unter Zertifikatpinning.

Für den Zugriff auf den Autodiscoverydienst gehen Sie zu https://adsui.cloud.com (Unternehmen).

Voraussetzungen

- Der neue Autodiscoverydienst in Citrix Cloud erfordert die neueste Version von Citrix Secure Hub:
  - Für iOS: Citrix Secure Hub Version 21.6.0 oder höher
  - Für Android: Citrix Secure Hub Version 21.8.5 oder höher

    Bei Geräten mit früheren Versionen von Citrix 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.

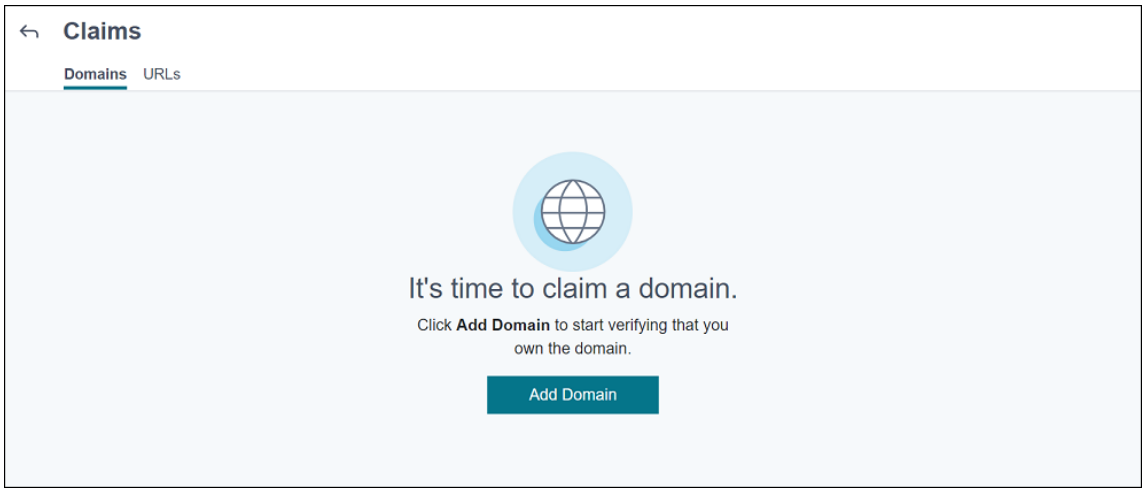
  Citrix hat alle vorhandenen AutoDiscovery-Datensätze ohne Betriebsunterbrechung in Citrix Cloud migriert. Die migrierten Datensätze werden nicht automatisch in der neuen Konsole angezeigt. Sie müssen Domänen im neuen AutoDiscovery-Dienst zurückfordern, um die Inhaberschaft nachzuweisen. Weitere Informationen finden Sie unter CTX312339.
- Bevor Sie den Autodiscoverydienst für Ihre Citrix Endpoint Management-Bereitstellungen verwenden, müssen Sie Ihre Domäne verifizieren und beanspruchen. Sie können bis zu 10 Domä-

nen 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.

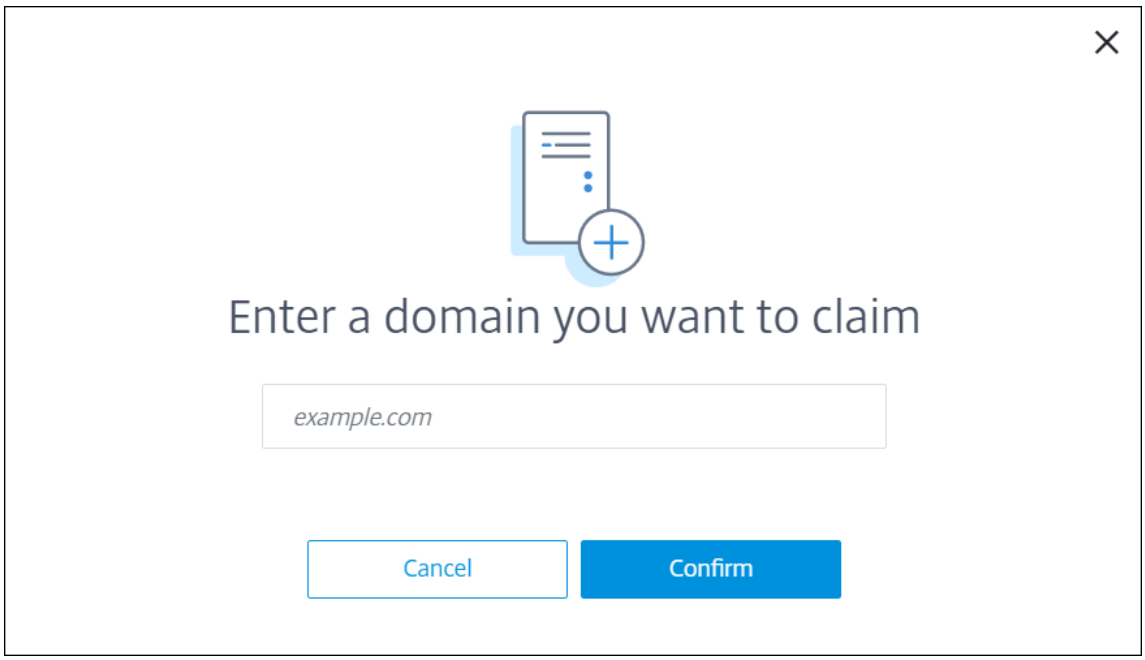
- Verwenden Sie die Einstellung MAM-Port anstelle von NetScaler Gateway-FQDN, um MAM-Datenverkehr an Ihr Datencenter zu leiten. Wenn Sie einen vollqualifizierten Domänennamen zusammen mit dem Port von NetScaler Gateway eingeben, verwendet das Clientgerät die Konfiguration aus der Einstellung **MAM-Port**.
- Wenn ein Werbeblocker das Öffnen der Site verhindert, müssen Sie ihn für die gesamte Website deaktivieren.

Beanspruchen einer Domäne

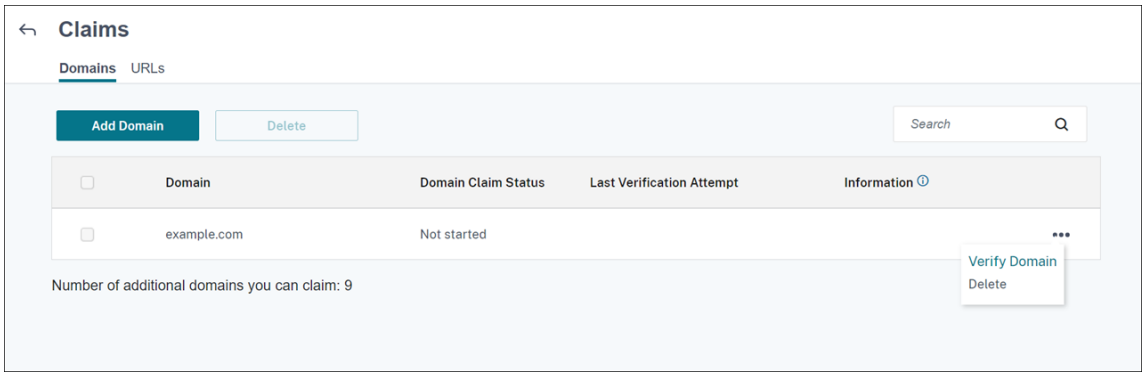
1. Klicken Sie auf der Registerkarte **Ansprüche > Domänen** auf **Domäne hinzufügen**.



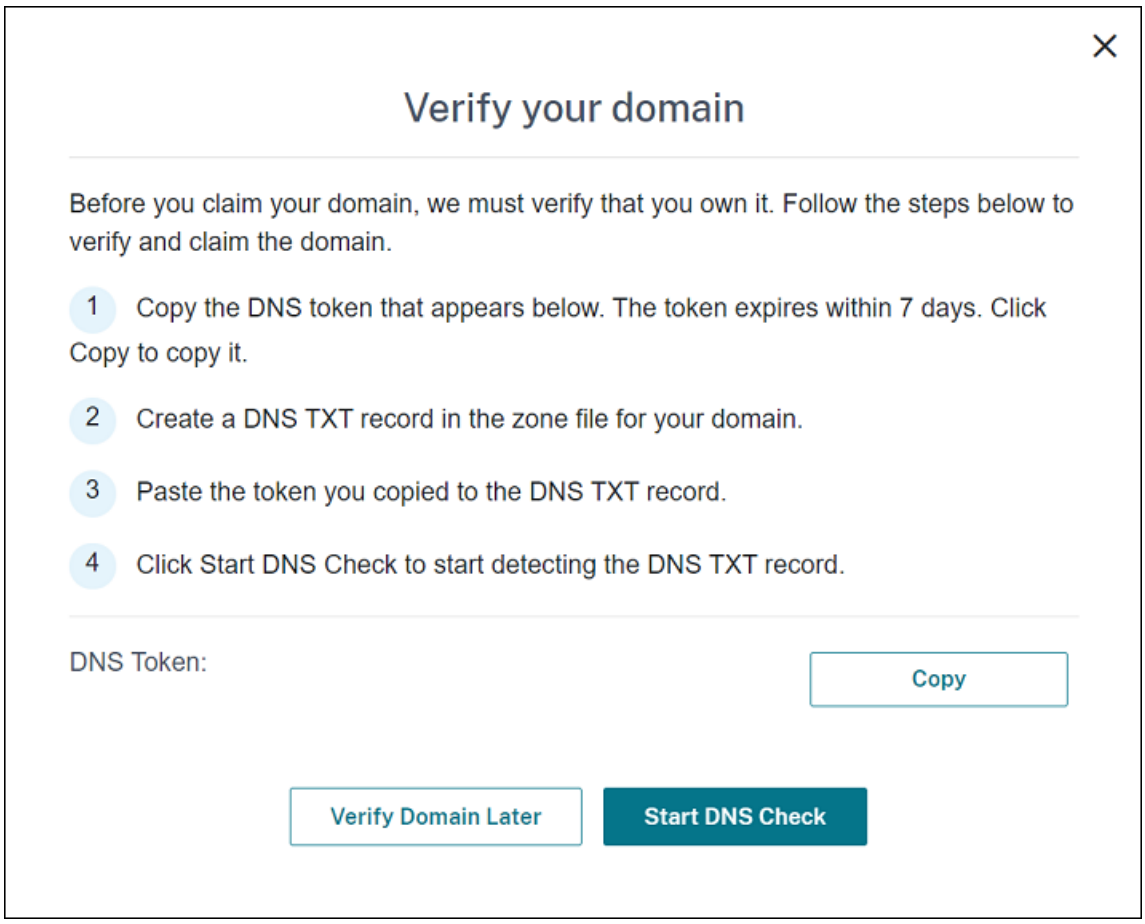
2. Geben Sie im angezeigten Dialogfeld den Domänennamen Ihrer Citrix Endpoint Management-Umgebung ein und klicken Sie auf **Bestätigen**. Ihre Domäne wird unter **Ansprüche > Domänen** angezeigt.



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.



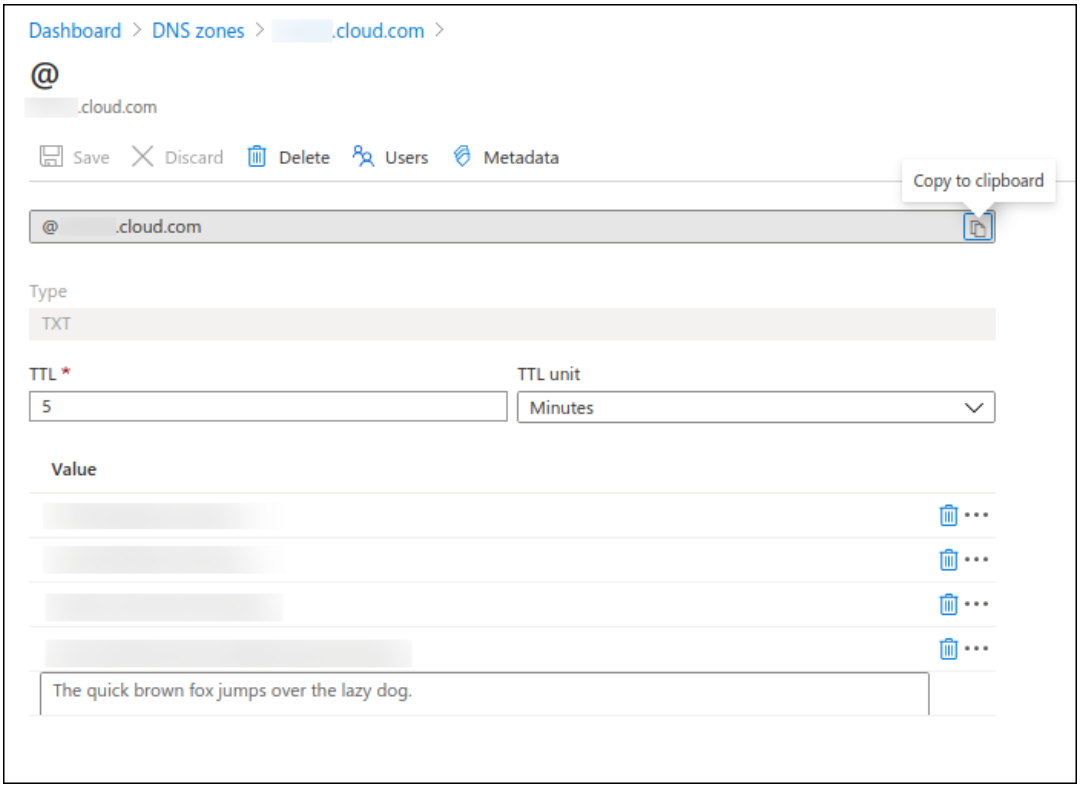
4. Folgen Sie auf der Seite **Überprüfen Ihrer Domäne** den Anweisungen, um zu verifizieren, dass Sie die Domäne besitzen.



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 Autodiscovery-dienst ein. Klicken Sie auf die Auslassungspunkte (…) der hinzugefügten Domäne und dann auf die Option zum **Hinzufügen von Citrix 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 Citrix Endpoint Management:** Geben Sie den vollqualifizierten Domänennamen des Citrix Endpoint Management-Servers ein. Beispiel: `example.xm.cloud.com`. Diese Einstellung wird für MDM- und MAM-Datenverkehr verwendet.
   - **NetScaler Gateway-FQDN:** Geben Sie den vollqualifizierten Domänennamen von NetScaler 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 **NetScaler Gateway-FQDN** verwenden, um MAM-Datenverkehr zu steuern. Wenn Sie einen vollqualifizierten Domänennamen zusammen mit dem Port von NetScaler Gateway eingeben, verwendet das Clientgerät die Konfiguration aus der Einstellung **MAM-Port**.

- **Instanzname:** Geben Sie den Instanznamen des Citrix Endpoint Management-Servers ein, den Sie zuvor konfiguriert haben. Wenn Sie sich bezüglich Ihres Instanznamens nicht sicher sind, übernehmen Sie den Standardwert **zdm**.
- **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:

- Bereitstellen der Details des Citrix Endpoint Management-Servers.
- Anweisen des Geräts, ein gültiges Zertifikat von Citrix Endpoint Management 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.

Integration in bedingten Azure AD-Zugriff

Sie können Citrix Endpoint Management so konfigurieren, dass Unterstützung für bedingten Azure AD-Zugriff auf Office 365-Anwendungen angewendet wird. Mit diesem Feature können Sie die Zero-Trust-Methode für Gerätebenutzer bei der Bereitstellung von Office 365-Anwendungen bereitstellen. Sie können den Gerätestatus, die Risikobewertung, den Standort und den Geräteschutz verwenden, um automatisierte Aktionen anzuwenden und den Zugriff auf die Office 365-Anwendungen auf verwalteten Android Enterprise- und iOS-Geräten zu definieren.

Um die Compliance von Azure AD-Geräten durchzusetzen, müssen Sie Richtlinien für bedingten Zugriff für einzelne Office 365-Anwendungen konfigurieren. Sie können den Benutzerzugriff auf bestimmte Office 365-Anwendungen auf nicht verwalteten und nicht richtlinientreuen Geräten einschränken und den Zugriff auf einzelne Anwendungen nur auf verwalteten und richtlinientreuen Geräten zulassen.

Voraussetzungen

- Für diese Integration müssen Sie über ein gültiges Azure AD Premium-Abonnement verfügen, einschließlich Intune- und Microsoft Office 365-Lizenzen.
- Citrix Secure Hub Version 21.4.0 und höher
- Konfigurieren Sie Azure AD als Identitätsanbieter (IdP) in Citrix Cloud und legen Sie dann Citrix-Identität als IdP-Typ für Citrix Endpoint Management fest. Weitere Informationen finden Sie unter Authentifizierung mit Azure Active Directory über Citrix Cloud.
- Akzeptieren Sie die Citrix Mehrmandanten-AAD-Anwendung, damit mobile Anwendungen sich bei der AAD-Client-App authentifizieren können. Nur erforderlich, wenn der globale Azure-Administrator für**Benutzer können Anwendungen registrieren** den Wert **Nein** festgelegt hat. Konfigurieren Sie diese Einstellung im Azure-Portal unter **Azure Active Directory > Benutzer > Benutzereinstellungen**. Informationen zur Zustimmung finden Sie unter Konfigurieren von Citrix Endpoint Management für Azure AD-Compliancеverwaltung.
- Installieren Sie die Microsoft Authenticator-Anwendung auf dem Gerät, bevor Sie den Registrierungsprozess für Azure AD-Geräte starten.

- Konfigurieren Sie für die Android Enterprise-Plattform eine Webbrowser-App als erforderliche App für den öffentlichen Store.
- Deaktivieren Sie die Einstellung **Sicherheitsstandards** in der Azure AD-Konsole. Wenn Sie die Azure AD-Konfiguration starten, ersetzen Sie Sicherheitsstandards durch genauere Richtlinien für den bedingten Azure AD-Zugriff. Weitere Informationen zu Sicherheitsstandards finden Sie in der Dokumentation von Microsoft.

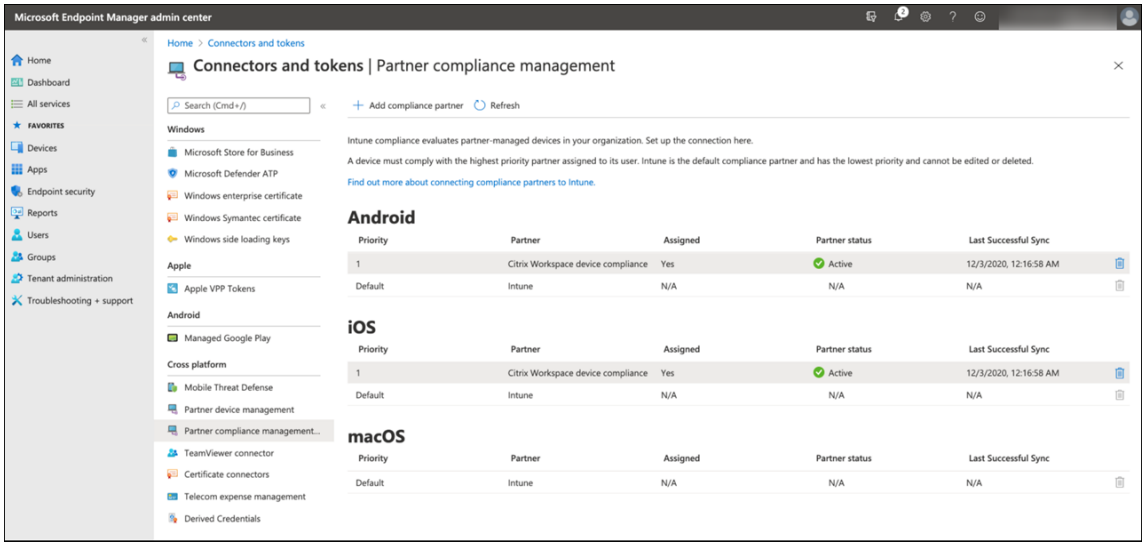
Konfigurieren der Gerätecompliance durch Richtlinien für bedingten Azure AD-Zugriff

Die allgemeinen Schritte zur Konfiguration der Gerätecompliance durch Richtlinien für bedingten Azure AD-Zugriff lauten wie folgt:

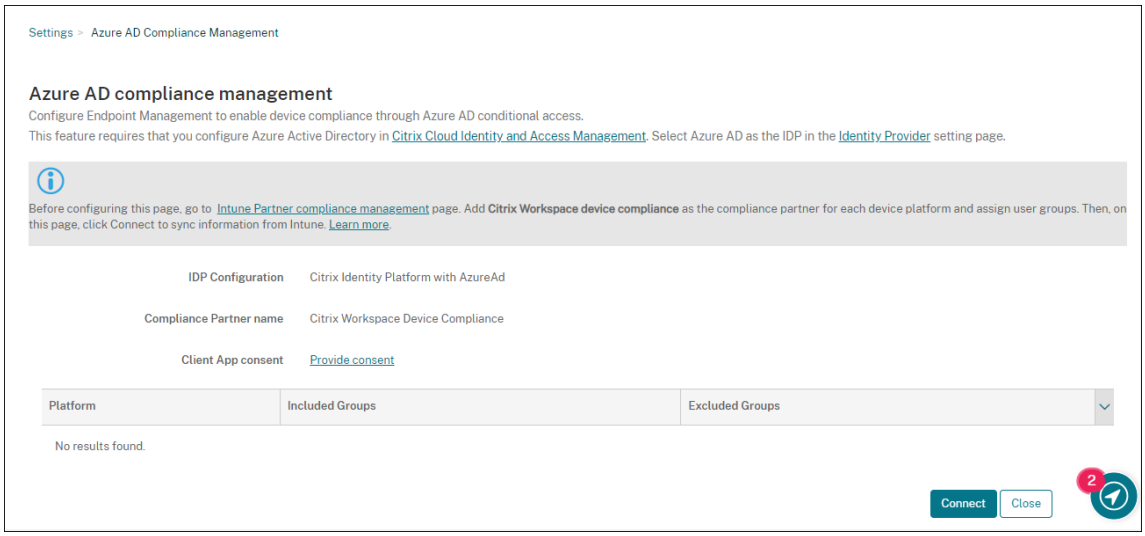
1. **Citrix Endpoint Management-Konfiguration:**
    - Fügen Sie im Microsoft Endpoint Manager Admin Center **Citrix Workspace-Gerätecompliance** als Compliancepartner für jede Geräteplattform hinzu und weisen Sie Benutzergruppen zu.
    - Synchronisieren Sie in Citrix Endpoint Management Informationen aus dem Microsoft Endpoint Manager Admin Center.
2. **Azure AD-Konfiguration:** Legen Sie im Azure AD-Portal Richtlinien für bedingten Zugriff für einzelne Office 365-Apps fest.
3. **Citrix Endpoint Management-Konfiguration:** Nachdem Sie Richtlinien für bedingten Zugriff für Office 365-Apps konfiguriert haben, fügen Sie die Microsoft Authenticator-App und Office 365-Apps als Apps im öffentlichen App Store in Citrix Endpoint Management hinzu. Weisen Sie diese öffentlichen Apps der Bereitstellungsgruppe zu und legen Sie sie als erforderliche Apps fest.

Konfigurieren von Citrix Endpoint Management für Azure AD-Complianceverwaltung

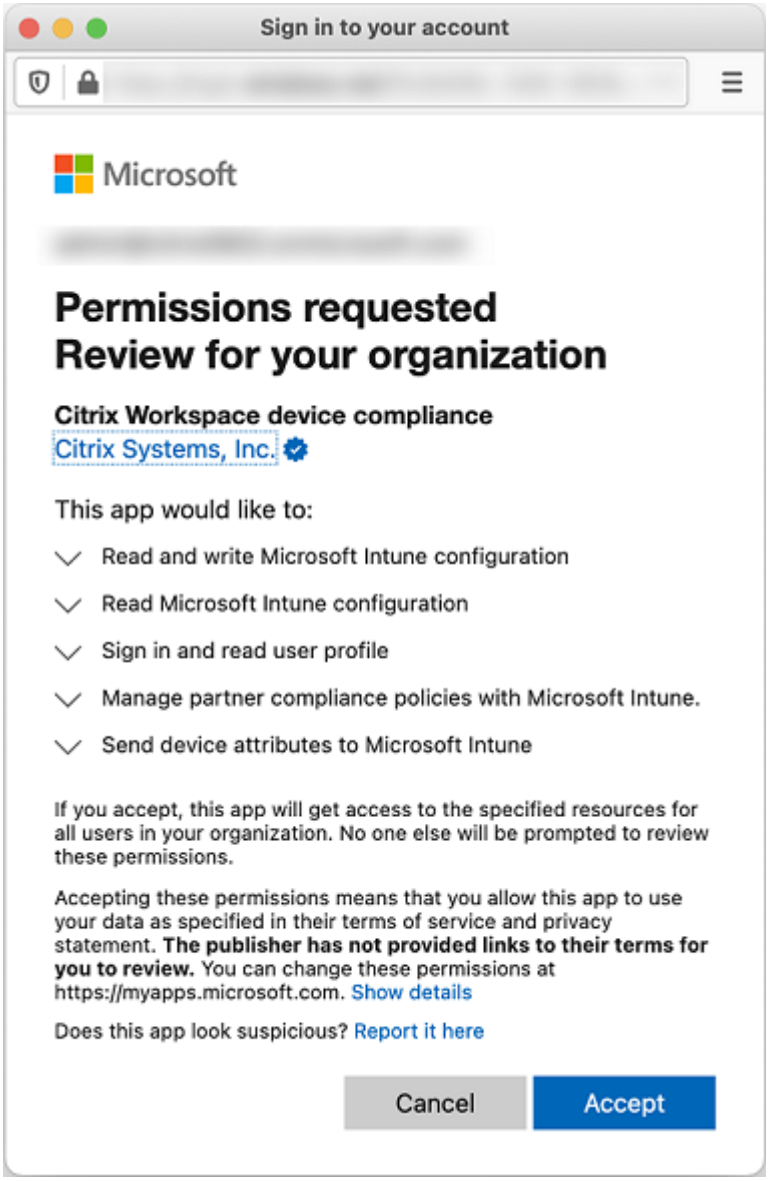
1. Melden Sie sich im Microsoft Endpoint Manager Admin Center an und navigieren Sie zu **Mandantenverwaltung > Connectors und Token > Gerätecomplianceverwaltung**. Klicken Sie auf **Compliancepartner hinzufügen** und wählen Sie **Citrix Workspace-Gerätecompliance** als Compliancepartner für jede Geräteplattform aus. Weisen Sie dann Benutzergruppen zu.



2. Gehen Sie in Citrix Endpoint Management zu **Einstellungen > Azure AD-Complianceverwaltung**.
3. Legen Sie optional die globale Zustimmung fest, damit Benutzer nicht auf jedem Gerät ihre Zustimmung geben müssen. Klicken Sie neben **Zustimmung zur Client-App** auf **Zustimmen**. Geben Sie Ihre globalen Azure AD-Administratoranmeldeinformationen ein und folgen Sie den Anweisungen, um die globale Zustimmung für die Client-Apps zu geben.
4. Klicken Sie auf **Verbinden**, um Informationen aus dem Microsoft Endpoint Manager Admin Center zu synchronisieren



In einem Dialogfeld werden Sie aufgefordert, die Berechtigungen für diese Konfiguration zu akzeptieren. Klicken Sie auf **Akzeptieren**. Nach Abschluss der Konfiguration werden synchronisierte Geräteplattformen in der Liste angezeigt.



Konfigurieren von Richtlinien für bedingten Zugriff in Azure AD

Konfigurieren Sie im Azure AD-Portal Richtlinien für bedingten Zugriff für Office 365-Apps, um die Gerätecompliance durchzusetzen. Gehen Sie zu **Geräte > Bedingter Zugriff > Richtlinien > Neue Richtlinie**. Informationen hierzu finden Sie in der Dokumentation von Microsoft.

So konfigurieren Sie die Gerätecompliance für mit Intune verwaltete Apps:

- Konfigurieren der Bereitstellung von mit Intune verwalteten Apps auf Geräten
- Genehmigte Client-Apps erforderlich
- App-Schutzrichtlinie und genehmigte Client-App für Cloud-App-Zugriff erforderlich

Konfigurieren von Apps in Citrix Endpoint Management

Nachdem Sie Richtlinien für bedingten Zugriff für Office 365-Apps konfiguriert haben, fügen Sie die Microsoft Authenticator-App und Office 365-Apps als Apps im öffentlichen App Store in Citrix Endpoint Management hinzu. Weisen Sie diese öffentlichen Apps der Bereitstellungsgruppe zu und legen Sie sie als erforderliche Apps fest. Weitere Informationen finden Sie unter Hinzufügen von Apps aus einem öffentlichen App-Store.

Workflow für Benutzerauthentifizierung

1. Ein neuer Benutzer muss ein Gerät mit Azure AD-Anmeldeinformationen bei Citrix Endpoint Management registrieren. Benutzer, die sich zuvor mit Azure AD-Anmeldeinformationen registriert haben, müssen ihre Geräte nicht erneut registrieren.
2. Citrix Endpoint Management überträgt Microsoft Authenticator und konfigurierte Office 365-Apps per Push als erforderliche Apps auf ein Gerät. Wenn Sie eine Webbrowser-App als erforderliche App im öffentlichen Store für die Android-Plattform konfiguriert haben, überträgt Citrix Endpoint Management sie ebenfalls per Push auf das Benutzergerät.
3. Alle über Citrix Endpoint Management verwalteten Apps werden von Citrix Secure Hub automatisch installiert und angezeigt.
4. Wenn ein Benutzer versucht, sich bei einer verfügbaren Office 365-App anzumelden, fordert das Gerät den Benutzer auf, auf den Link zur **Azure AD-Registrierung** zu tippen, um den Registrierungsprozess zu starten.
5. Nachdem der Benutzer auf den Registrierungslink geklickt hat, wird die Microsoft Authenticator-App geöffnet. Der Benutzer gibt Azure AD-Anmeldeinformationen ein und stimmt den Bedingungen für die Geräteregistrierung zu. Dann wird die Microsoft Authenticator-App geschlossen und Citrix Secure Hub wird wieder geöffnet.
6. Citrix Secure Hub zeigt eine Meldung an, die besagt, dass die Azure AD-Geräteregistrierung abgeschlossen ist. Der Benutzer kann jetzt Microsoft-Apps verwenden, um auf seine Cloudressourcen zuzugreifen.

   Nach Abschluss der Registrierung kennzeichnet Azure AD das Gerät in der Konsole als verwaltet und richtlinientreu.

Standard-Geräterichtlinien und mobile Produktivitätsapps

Bei einer Erstverwendung von Citrix Endpoint Management ab Version 19.5.0 oder höher sind einige Geräterichtlinien und mobile Produktivitätsapps bereits vorab konfiguriert. Mit dieser Konfiguration haben Sie folgende Möglichkeiten:

- Sofortige Bereitstellung grundlegender Funktionen auf Geräten
- Start mit den empfohlenen Grundkonfigurationen für einen sicheren Workspace

Für die Plattformen Android, Android Enterprise, iOS, macOS und Windows Desktop/Tablet enthält Ihre Site folgende vorkonfigurierte Geräterichtlinien:

- **Passcode-Geräterichtlinie:** Die Passcode-Geräterichtlinie ist auf **Ein** gesetzt und alle Passcode-Standardeinstellungen sind aktiviert.
- **App-Bestandsrichtlinie für Geräte:** Die App-Bestandsrichtlinie für Geräte ist auf **Ein** gesetzt.
- **Geräteeinschränkungsrichtlinie:** Die Geräteeinschränkungsrichtlinie ist auf **Ein** gesetzt und alle Standardeinstellungen zu Einschränkungen sind aktiviert.

Diese Richtlinien befinden sich in der Bereitstellungsgruppe **AllUsers**, die alle Active Directory- und lokalen Benutzer enthält. Es wird empfohlen, die Bereitstellungsgruppe "AllUsers"nur für erste Tests zu verwenden. Erstellen Sie anschließend Ihre Bereitstellungsgruppen und deaktivieren Sie die Bereitstellungsgruppe "AllUsers". Sie können die vorkonfigurierten Geräterichtlinien und Apps in Ihren Bereitstellungsgruppen wiederverwenden.

Alle Citrix Endpoint Management-Geräterichtlinien werden unter Geräterichtlinien dokumentiert. Dieser Artikel enthält Informationen zum Bearbeiten von Geräterichtlinien über die Konsole. Informationen zu häufig verwendeten Geräterichtlinien finden Sie unter Geräterichtlinien und Anwendungsverhalten.

Für die Plattformen iOS und Android enthält Ihre Site folgende vorkonfigurierte mobile Produktivitätsapps:

- **Citrix Secure Mail**
- **Citrix Secure Web**
- **Citrix Files**

Diese Apps sind in der Bereitstellungsgruppe **AllUsers**.

Weitere Informationen finden Sie unter Mobile Produktivitätsapps.

Fortsetzen der Citrix Endpoint Management-Konfiguration

Nachdem Sie das Basissetup für die Geräteregistrierung abgeschlossen haben, hängt die Konfiguration von Citrix Endpoint Management stark von Ihrem Anwendungsfall ab. Beispiel:

- Was sind Ihre Sicherheitsanforderungen und wie möchten Sie diese Anforderungen mit der Benutzererfahrung in Einklang bringen?
- Welche Geräteplattformen unterstützen Sie?
- Besitzen Benutzer die Geräte oder verwenden sie unternehmenseigene Geräte?

- Welche Geräterichtlinien möchten Sie auf Geräte übertragen?
- Welche Arten von Apps stellen Sie Benutzern zur Verfügung?

Dieser Abschnitt hilft, durch die zahlreichen Konfigurationsentscheidungen zu navigieren, indem Sie auf die entsprechenden Artikeln in dieser Dokumentation geführt werden.

Wenn Sie die Konfiguration auf Websites von Drittanbietern abschließen, notieren Sie die Informationen und ihren Speicherort zur Referenz beim Konfigurieren der Einstellungen in der Citrix Endpoint Management-Konsole.

- Sicherheit und Authentifizierung. Citrix Endpoint Management verwendet Zertifikate, um sichere Verbindungen zu erstellen und Benutzer zu authentifizieren. Citrix stellt Platzhalterzertifikate für Ihre Citrix Endpoint Management-Instanz bereit.
  - Eine Besprechung der Authentifizierungskomponenten und der empfohlenen Konfigurationen nach Sicherheitsstufe finden Sie unter "Erweiterte Konzepte"im Artikel Authentifizierung. Siehe auch Sicherheit und Benutzererfahrung.
  - Eine Übersicht über die Authentifizierungskomponenten, die während der Citrix Endpoint Management-Vorgänge verwendet werden, finden Sie unter Zertifikate und Authentifizierung.
  - Sie können unter den folgenden Authentifizierungstypen wählen. Die Konfiguration der Authentifizierung umfasst Aufgaben in den Konsolen von Citrix Endpoint Management und NetScaler Gateway.
    - Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken
    - Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne
  - Um Zertifikate an Benutzer zu übermitteln, konfigurieren Sie:
    - PKI-Entitäten
    - Anmeldeinformationsanbieter
  - Registrierungssicherheitsmodi für Geräte. Registrierungssicherheitsmodi für Geräte geben die Arten der Anmeldeinformationen an und verwenden Registrierungsschritte, die die Benutzer für die Registrierung ihrer Geräte bei Citrix Endpoint Management benötigen. Weitere Informationen finden Sie unter Registrierungssicherheitsmodi konfigurieren.
  - Informationen zur Authentifizierung von Benutzern mit Azure Active Directory-Anmeldeinformationen finden Sie unter Authentifizierung mit Azure Active Directory über Citrix Cloud.
- Geräteregistrierung
  - Für die Registrierung einer großen Anzahl von Geräten stehen Programme zur Verfügung:
    - Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm

    * Massenregistrierung von Apple-Geräten
    * Massenregistrierung von Windows-Geräten
  - Erstellen Sie für die Registrierung von Android-Geräten ein Android Enterprise-Administratorkonto. Siehe Android Enterprise. Oder siehe Kunden mit Legacy Android Enterprise für Google Workspace.
  - Sie können Registrierungseinladungen verwenden oder Benachrichtigungen für die Registrierung senden.
    * Registrierungseinladungen.
    * Benachrichtigungen.
  - Weitere Informationen zur Registrierung finden Sie unter Geräteverwaltung und Artikeln unter diesem Knoten.

- Geräterichtlinien und -verwaltung
  - Geräterichtlinien (MDM). Alle Citrix Endpoint Management-Geräterichtlinien werden unter Geräterichtlinien dokumentiert. Informationen zu häufig verwendeten Geräterichtlinien finden Sie unter Geräterichtlinien und Anwendungsverhalten.
  - Clienteigenschaften. Clienteigenschaften enthalten Informationen, die direkt in Citrix Secure Hub auf den Geräten der Benutzer bereitgestellt werden. Siehe Clienteigenschaften und Citrix Endpoint Management-Clienteigenschaften.
  - Bereitstellungsgruppen. Ein Beispiel für einen Anwendungsfall für Bereitstellungsgruppen finden Sie unter Benutzergemeinschaften und Hinzufügen einer Bereitstellungsgruppe.

- Vorbereiten von Apps für die Bereitstellung
  - Informationen zu den von Citrix Endpoint Management unterstützten Apps finden Sie unter Apps hinzufügen.
  - Sie können die Lizenzierung von iOS-Apps über Apple Volume Purchase verwalten. Weitere Informationen finden Sie unter Apple Volume Purchase.
  - Mit Citrix Endpoint Management können Sie iBooks bereitstellen, die Sie über Apple Volume Purchase beschafft haben. Siehe Hinzufügen von Medien.
  - Citrix bietet mobile Produktivitätsapps, einschließlich Citrix Secure Mail und Citrix Secure Web. Siehe Mobile Produktivitätsapps.
  - Als Alternative zu Citrix Secure Mail können Sie native E-Mails an Geräte senden. Siehe:
    * E-Mail-Strategie
    * Citrix Endpoint Management Connector für Exchange ActiveSync

    - NetScaler Gateway Connector für Exchange ActiveSync

  - Informationen zum sicheren Übertragen von Daten und Dokumenten an Microsoft Office 365-Apps finden Sie unter Zulassen der sicheren Interaktion mit Office 365-Apps und Office-Geräterichtlinie.
  - Allgemeine Informationen zu App-Richtlinien finden Sie unter Szenarios für App-Richtlinien und Anwendungsfälle.
  - Das MDX Toolkit ist eine Technologie zum Umschließen von Apps, mit denen Unternehmensapps für die sichere Bereitstellung mit Citrix Endpoint Management vorbereitet werden. Das MAM-SDK ersetzt das MDX Toolkit. Das MDX Toolkit erreicht das Ende des Lebenszyklus (EOL) im Juli 2023.

    Weitere Informationen zum MAM-SDK finden Sie unter Überblick über das MAM-SDK.
  - Weitere Informationen zu Apps finden Sie in anderen Artikeln unter Apps hinzufügen.

- Mit der rollenbasierten Zugriffssteuerung (RBAC) in Citrix Endpoint Management können Sie Benutzern und Gruppen vordefinierte Rollen bzw. Berechtigungssätze zuweisen. Diese Berechtigungen steuern den Zugriff der Benutzer auf Systemfunktionen. Informationen finden Sie unter Rollen mit RBAC konfigurieren.
- Sie können in Citrix Endpoint Management mit automatisierten Aktionen eine Reaktion auf Ereignisse, bestimmte Einstellungen oder das Vorhandensein von Apps auf Benutzergeräten festlegen. Informationen finden Sie unter Automatisierte Aktionen.

Zertifikate und Authentifizierung

March 11, 2024

Mehrere Komponenten spielen für die Authentifizierung bei Citrix Endpoint Management-Operationen eine Rolle:

- **Citrix Endpoint Management:** Auf dem Citrix Endpoint Management-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. Clienteigenschaften in Citrix Endpoint Management ermöglichen es Ihnen, die Citrix-PIN-Authentifizierung zu aktivieren und die Komplexität sowie den Ablauf der PIN zu konfigurieren.

- **NetScaler Gateway:** NetScaler Gateway ermöglicht Terminierung für Micro-VPN-SSL-Sitzungen. NetScaler Gateway bietet zudem Sicherheit bei der Datenübertragung im Netzwerk und ermöglicht das Definieren der Authentifizierungserfahrung beim Zugriff auf Apps durch Benutzer.
- **Citrix Secure Hub:** Citrix Secure Hub und Citrix Endpoint Management Server wirken bei der Registrierung zusammen. Citrix Secure Hub ist auf Geräten die Entität, die mit NetScaler Gateway kommuniziert: Wenn eine Sitzung abläuft, erhält Citrix Secure Hub ein Authentifizierungsticket von NetScaler Gateway 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 Citrix Secure Hub-Artikel zum Zertifikatpinning.

  Citrix Secure Hub moderiert zudem den MDX-Sicherheitscontainer durch Übertragen von Richtlinien, Erstellen einer Sitzung mit NetScaler Gateway bei einem App-Timeout und durch Festlegen des MDX-Timeouts und der Benutzererfahrung. Außerdem ist Citrix Secure Hub für die Erkennung von Jailbreaks, Geolocation-Prüfungen und alle von Ihnen angewendeten Richtlinien verantwortlich.
- **MDX-Richtlinien:** MDX-Richtlinien erstellen den Datentresor auf Geräten. MDX-Richtlinien leiten Micro-VPN-Verbindungen zurück zu NetScaler Gateway und erzwingen Einschränkungen für den Offlinemodus sowie die Einhaltung von Clientrichtlinien (z. B. Timeouts).

Citrix Endpoint Management authentifiziert Benutzer mit den folgenden Authentifizierungsmethoden für ihre Ressourcen:

- Mobilgeräteverwaltung (MDM)
  - Cloudgehostete Identitätsanbieter (IdPs)
  - Lightweight Directory Access Protocol (LDAP)
    - Einladungs-URL + PIN
    - Zweistufige Authentifizierung
- Mobilanwendungsverwaltung (MAM)
  - LDAP
  - Zertifikat
  - MAM-Authentifizierung mit Sicherheitstoken erfordert NetScaler Gateway.

Informationen zu weiteren Konfigurationsdetails finden Sie in den folgenden Artikeln:

- Zertifikate hochladen, aktualisieren und erneuern
- NetScaler Gateway und Citrix Endpoint Management
- Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken
- Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne
- PKI-Entitäten

- Anmeldeinformationsanbieter
- APN-Zertifikate
- SAML für Single Sign-On mit Citrix Files
- Authentifizierung mit Azure Active Directory über Citrix Cloud
- Authentifizierung mit Okta über Citrix Cloud
- Authentifizierung mit einem On-Premises-NetScaler Gateway über Citrix Cloud
- Senden eines Zertifikats an Geräte zur Authentifizierung am Wi-Fi-Server: Netzwerkgerät-erichtlinie
- Senden eines eindeutigen Zertifikats, das nicht für die Authentifizierung verwendet wird, z. B. des Zertifikats einer internen Stammzertifizierungsstelle, oder einer bestimmten Richtlinie: Anmeldeinformationsrichtlinie

Zertifikate

Citrix Endpoint Management generiert bei der Installation ein selbstsigniertes SSL-Zertifikat (Secure Socket Layer) zum Sichern der Kommunikation mit dem Server. Ersetzen Sie das SSL-Zertifikat durch ein vertrauenswürdiges SSL-Zertifikat von einer allgemein bekannten Zertifizierungsstelle.

Citrix Endpoint Management 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 Citrix Endpoint Management-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 Citrix Endpoint Management müssen Sie ein Zertifikat von Apple für den Apple Dienst für Push-Benachrichtigungen (APNs) erstellen und einrichten. Anweisungen finden Sie unter APNs-Zertifikate.

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

Citrix Endpoint Management-Komponenten	Zertifikatformat	Erforderlicher Zertifikattyp
NetScaler Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Stamm (NetScaler Gateway konvertiert PFX automatisch in PEM).
Citrix Endpoint Management	.p12 (.pfx auf Windows-basierten Computern)	SSL, SAML, APNs (Citrix Endpoint Management generiert während des Installationsprozesses auch eine vollständige PKI.) **Wichtig:** Citrix Endpoint Management 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 Citrix Endpoint Management importieren.
StoreFront	PFX (PKCS #12)	SSL, Stamm

Citrix Endpoint Management unterstützt Clientzertifikate einer Bitlänge von 4096 und 2048.

Für NetScaler Gateway und Citrix Endpoint Management empfiehlt sich das Abrufen von Serverzertifikaten einer öffentlichen Zertifizierungsstelle, z. B. Verisign, DigiCert oder Thawte. Sie können eine Zertifikatsignieranforderung (CSR) mit dem NetScaler Gateway- oder dem Citrix Endpoint Management-Konfigurationsprogramm erstellen. Übermitteln Sie die CSR dann zum Signieren an die Zertifizierungsstelle. Wenn die Zertifizierungsstelle das signierte Zertifikat zurückgesendet hat, können Sie es unter NetScaler Gateway oder Citrix Endpoint Management 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 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.

LDAP-Authentifizierung

Citrix Endpoint Management unterstützt die domänenbasierte Authentifizierung für ein oder mehrere Lightweight Directory Access Protocol-konforme Verzeichnisse. LDAP ist ein Softwareprotokoll, das Zugriff auf Informationen über Gruppen, Benutzerkonten und zugehörige Eigenschaften bietet. Weitere Informationen finden Sie unter Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken.

Authentifizierung von Identitätsanbietern

Sie können einen Identitätsanbieter (IdP) über Citrix Cloud zum Registrieren und Verwalten von Benutzergeräten konfigurieren.

Unterstützte Anwendungsfälle für IdPs:

- Azure Active Directory über Citrix Cloud
  - Workspace-Integration ist optional
  - NetScaler Gateway, konfiguriert für die zertifikatbasierte Authentifizierung
  - Android Enterprise (Preview. Unterstützt BYOD, vollständig verwaltete Geräte und erweiterte Registrierungsprofile)
  - iOS für die MDM+MAM- und MDM-Registrierung
  - iOS und macOS für die Apple Business Manager-Registrierung
  - Legacy-Android (DA)

  Features für die automatische Registrierung (z. B. Apple School Manager) werden derzeit nicht unterstützt.
- Okta über Citrix Cloud
  - Workspace-Integration ist optional
  - NetScaler Gateway, konfiguriert für die zertifikatbasierte Authentifizierung
  - Android Enterprise (Preview. Unterstützt BYOD, vollständig verwaltete Geräte und erweiterte Registrierungsprofile)
  - iOS für die MDM+MAM- und MDM-Registrierung
  - iOS und macOS für die Apple Business Manager-Registrierung
  - Legacy-Android (DA)

  Features für die automatische Registrierung (z. B. Apple School Manager) werden derzeit nicht unterstützt.

- On-Premises-NetScaler Gateway über Citrix Cloud
  - NetScaler Gateway, konfiguriert für die zertifikatbasierte Authentifizierung
  - Android Enterprise (Preview. Unterstützt BYOD, vollständig verwaltete Geräte und erweiterte Registrierungsprofile)
  - iOS für die MDM+MAM- und MDM-Registrierung
  - Legacy-Android (DA)
    Features für die automatische Registrierung (z. B. Apple-Bereitstellungsprogramm) werden derzeit nicht unterstützt.

Zertifikate hochladen, aktualisieren und erneuern

June 25, 2024

Wir empfehlen, dass Sie die für Ihre Citrix Endpoint Management-Bereitstellung benötigten Zertifikate auflisten. Überwachen Sie anhand der Liste Ablaufdatum und Kennwörter der Zertifikate. Dieser Artikel enthält Informationen zur Verwaltung von Zertifikaten während deren gesamter Nutzungszeit.

Ihre Umgebung kann die folgenden Zertifikate enthalten:

- Citrix Endpoint Management-Server
  - SSL-Zertifikat für MDM-FQDN (erforderlich, wenn Sie von XenMobile Server zu Citrix Endpoint Management migriert haben. Andernfalls verwaltet Citrix dieses Zertifikat.)
  - SAML-Zertifikat (für 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
  - PKI-Benutzerzertifikat für die Verbindung mit der PKI (erforderlich, wenn eine zertifikatbasierte Authentifizierung erforderlich ist)
- MDX Toolkit
  - Apple Developer-Zertifikat
  - Apple-Provisioningprofil (pro Anwendung)
  - APNs-Zertifikat von Apple (zur Verwendung für Citrix Secure Mail)
  - Android-Schlüsselspeicherdatei

  Das MAM-SDK umschließt Apps nicht und erfordert daher kein Zertifikat.
- NetScaler Gateway
  - 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

> **Hinweis:**
>
> Das Clientgerät muss über das erforderliche Stamm-/Zwischenzertifikat verfügen, um eine Vertrauensstellung mit der Zertifizierungsstelle herzustellen, die das Serverzertifikat ausgestellt hat. Andernfalls wird möglicherweise der SSL-Fehler 61 angezeigt. Problemlösung:
>
> 1. Wählen Sie die vom SSL-Zertifikatanbieter ausgestellte SSL-Stamm-/Zwischenzertifikatdatei (CRT oder CER), oder laden Sie sie herunter. Das Stamm-/Zwischen-/Serverzertifikat ist normalerweise im Zertifikatspaket, das vom SSL-Dienstanbieter bereitgestellt wird.
> 2. Installieren Sie das Stamm-/Zwischenzertifikat auf dem Clientgerät.
> 3. Wenn ein Antivirenprogramm auf dem Clientgerät installiert ist, muss das Programm das Zertifikat für vertrauenswürdig halten.

Hochladen von Zertifikaten

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 Kriterien erfüllt. Beispiel: Sie konfigurieren die Integration von Citrix Endpoint Management in Ihrer Microsoft-Zertifizierungsstelle. Die Verbindung mit der Microsoft-Zertifizierungsstelle erfordert eine Authentifizierung mit einem Clientzertifikat.

Citrix Endpoint Management hat evtl. den privaten Schlüssel für ein bestimmtes Zertifikat nicht. Analog erfordert Citrix Endpoint Management möglicherweise keinen privaten Schlüssel für hochgeladene Zertifikate.

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.

Sie haben zwei Optionen zum Hochladen von Zertifikaten:

- Einzelupload auf die Konsole.
- Massenupload mit der REST-API. Die Option ist nur für iOS-Geräte verfügbar.

Beim Hochladen von Zertifikaten in die Konsole haben Sie folgende Möglichkeiten:

- Importieren eines Schlüsselspeichers. Anschließend geben Sie im Schlüsselspeicherrepository an, welchen Eintrag Sie installieren möchten (es sei denn, Sie laden ein PKCS #12-Zertifikat hoch).

- Importieren eines Zertifikats.

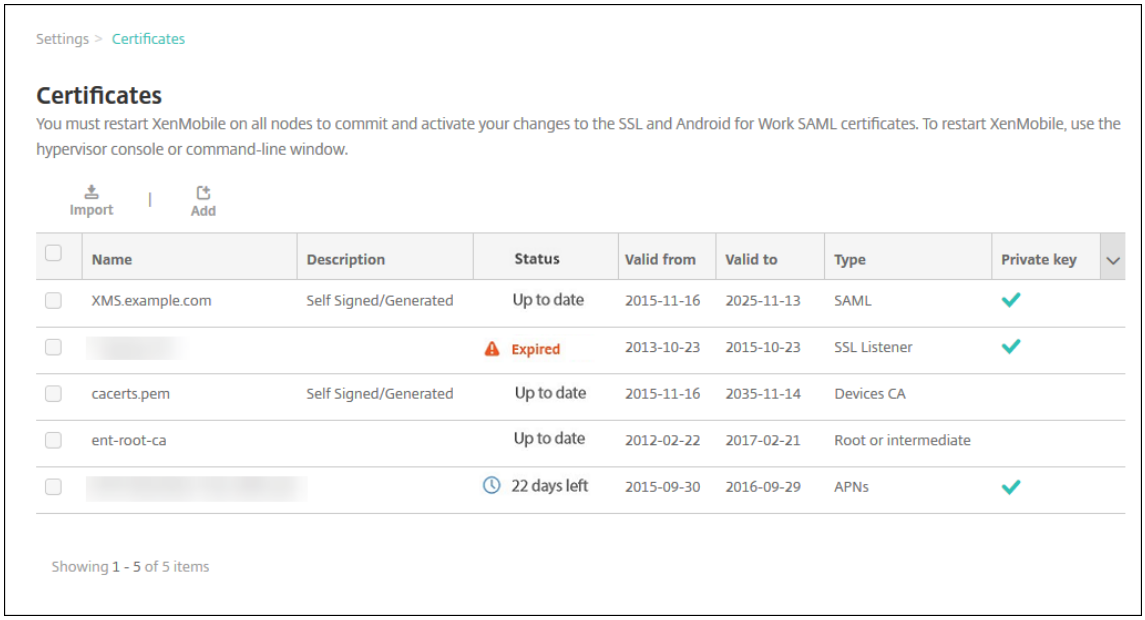
Sie können das ZS-Zertifikat (ohne privaten Schlüssel) hochladen, das von der Zertifizierungsstelle zum Signieren von Zertifikatsanforderungen verwendet wird. Sie können auch ein SSL-Clientzertifikat (mit privatem Schlüssel) für die Clientauthentifizierung hochladen.

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 Citrix Endpoint Management den privaten Schlüssel hat.

Importieren eines Schlüsselspeichers

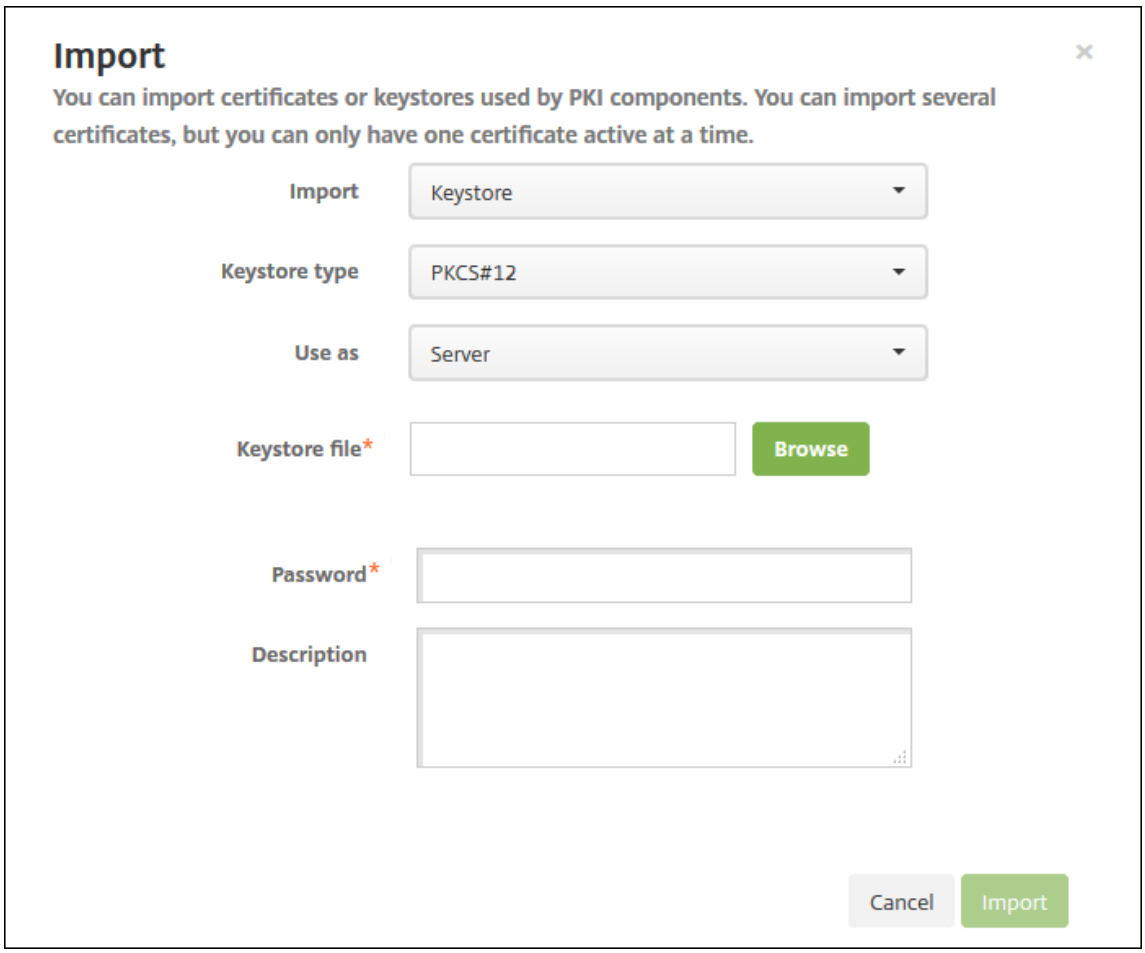
Ein Schlüsselspeicher ist ein Repository von Sicherheitszertifikaten. Schlüsselspeicher können konstruktionsbedingt viele Einträge enthalten. Beim Laden aus einem Schlüsselspeicher müssen Sie das Alias des gewünschten Eintrags angeben. Wenn Sie kein Alias angeben, wird der erste Eintrag aus dem Speicher 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 Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Mit der Suchleiste können Sie die Einstellung **Zertifikate** suchen und öffnen.



2. Klicken Sie auf **Importieren**. Das Dialogfeld **Importieren** wird angezeigt.
3. Konfigurieren Sie folgende Einstellungen:

    - **Importieren:** Wählen Sie **Schlüsselspeicher**.



- **Keystore-Typ:** Klicken Sie in der Dropdownliste auf **PKCS #12**.
- **Verwenden als:** Wählen Sie in der Liste aus, wie Sie das Zertifikat verwenden möchten. Es gibt folgende Optionen:
  - **Server:** Serverzertifikate werden funktional von Citrix Endpoint Management verwendet. Sie laden Serverzertifikate in die Citrix Endpoint Management-Webkonsole hoch. Zu diesen Zertifikaten gehören 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:** APN-Zertifikate von Apple ermöglichen die Mobilgeräteverwaltung über das Apple Push-Netzwerk.
  - **SSL-Listener:** Der Secure Sockets Layer-Listener benachrichtigt Citrix Endpoint Management über SSL-Kryptografieaktivitäten.
- **Schlüsselspeicherdatei:** Navigieren Sie zu dem Schlüsselspeicher, den Sie importieren

möchten. Der Schlüsselspeicher ist eine P12- oder PFX-Datei. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**.
- **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.

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

Importieren eines Zertifikats

Beim Importieren eines Zertifikats versucht Citrix Endpoint Management die Erstellung einer Zertifikatkette aus der Eingabe. Citrix Endpoint Management importiert alle Zertifikate in dieser Kette, um jeweils einen Serverzertifikateintrag für jedes Zertifikat zu erstellen. Dies funktioniert nur, wenn die Zertifikate in der Datei oder dem Schlüsselspeichereintrag tatsächlich eine Kette bilden, Jedes folgende Zertifikat in der Kette muss Aussteller des vorherigen Zertifikats sein.

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 Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Mit der Suchleiste können Sie die Einstellung **Zertifikate** suchen und öffnen.
2. Klicken Sie auf der Seite **Zertifikate** auf **Importieren**. Das Dialogfeld **Importieren** wird angezeigt. Konfigurieren Sie Folgendes:

    - **Importieren:** Klicken Sie auf **Zertifikat**.
    - **Verwenden als:** Wählen Sie aus, wie Sie das Zertifikat verwenden möchten. Es gibt folgende Optionen:
        - **Server:** Serverzertifikate werden funktional von Citrix Endpoint Management verwendet. Sie laden Serverzertifikate in die Citrix Endpoint Management-Webkonsole hoch. Zu diesen Zertifikaten gehören 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 Citrix Endpoint Management über SSL-Kryptografieaktivitäten.
    - **Zertifikatimport:** Navigieren Sie zu dem Zertifikat, das Sie importieren möchten. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**.

- **Datei für privaten Schlüssel:** 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. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**.
- **Beschreibung:** Geben Sie optional eine Beschreibung für das Zertifikat ein, um es von anderen Zertifikaten unterscheiden zu können.

3. Klicken Sie auf **Importieren**. Das Zertifikat wird der Zertifikattabelle hinzugefügt.

Massenupload von Zertifikaten mit der REST-API Manchmal ist das Hochladen einzelner Zertifikate nacheinander nicht sinnvoll. Führen Sie in diesen Fällen einen Massenupload mit der REST-API durch. 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:

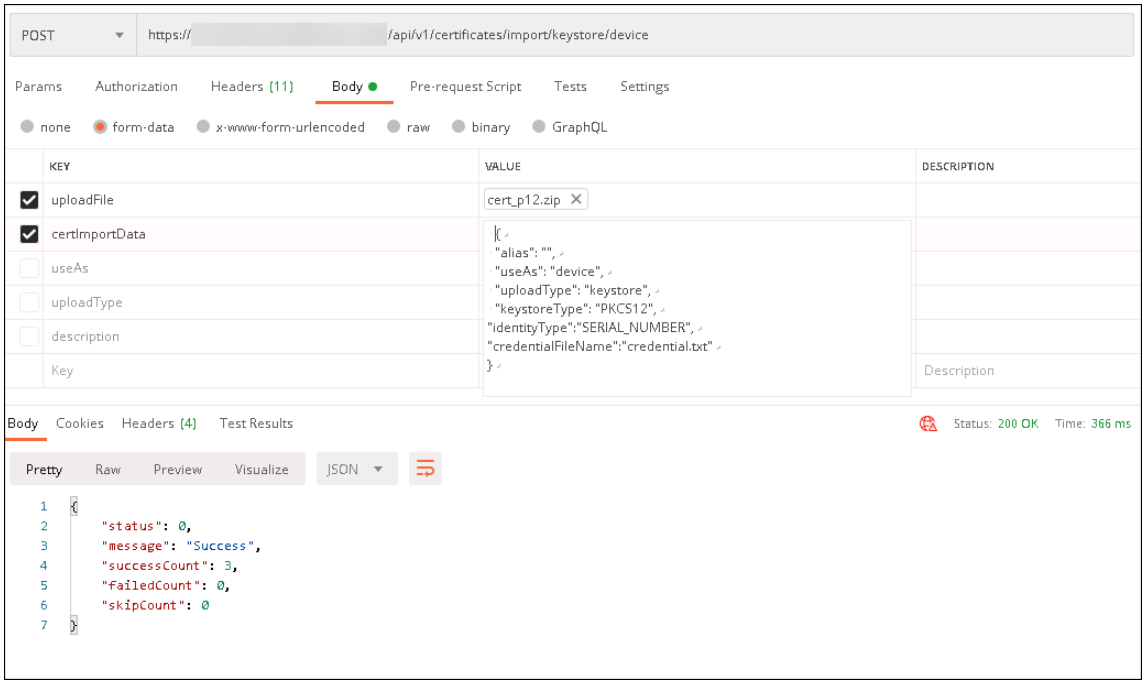
```
A12BC3D4EFGH.p12=password1!
A12BC3D4EFIJ.p12=password2@
A12BC3D4EFKL.p12=password3#
<!--NeedCopy-->
```

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 Citrix Endpoint Management an und rufen Sie ein Authentifizierungstoken ab.
5. Importieren Sie Ihre Zertifikate und stellen Sie sicher, dass Sie Folgendes in den Nachrichtentext einfügen:

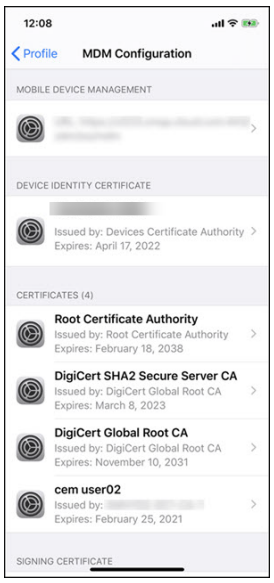
```
{

    "alias": "",
    "useAs": "device",
    "uploadType": "keystore",
    "keystoreType": "PKCS12",
    "identityType":"SERIAL_NUMBER",        # identity type can be
       "SERIAL_NUMBER","IMEI","MEID"
```

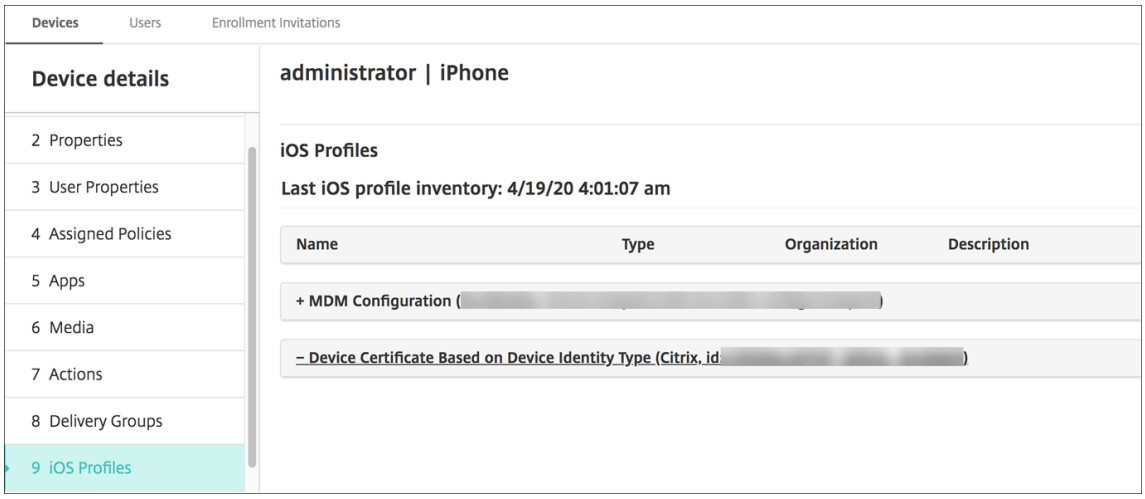


```
    "credentialFileName":"credential.txt"    # The credential file
        name in .zip
}

<!--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 Citrix Endpoint Management-Konsole überprüfen.



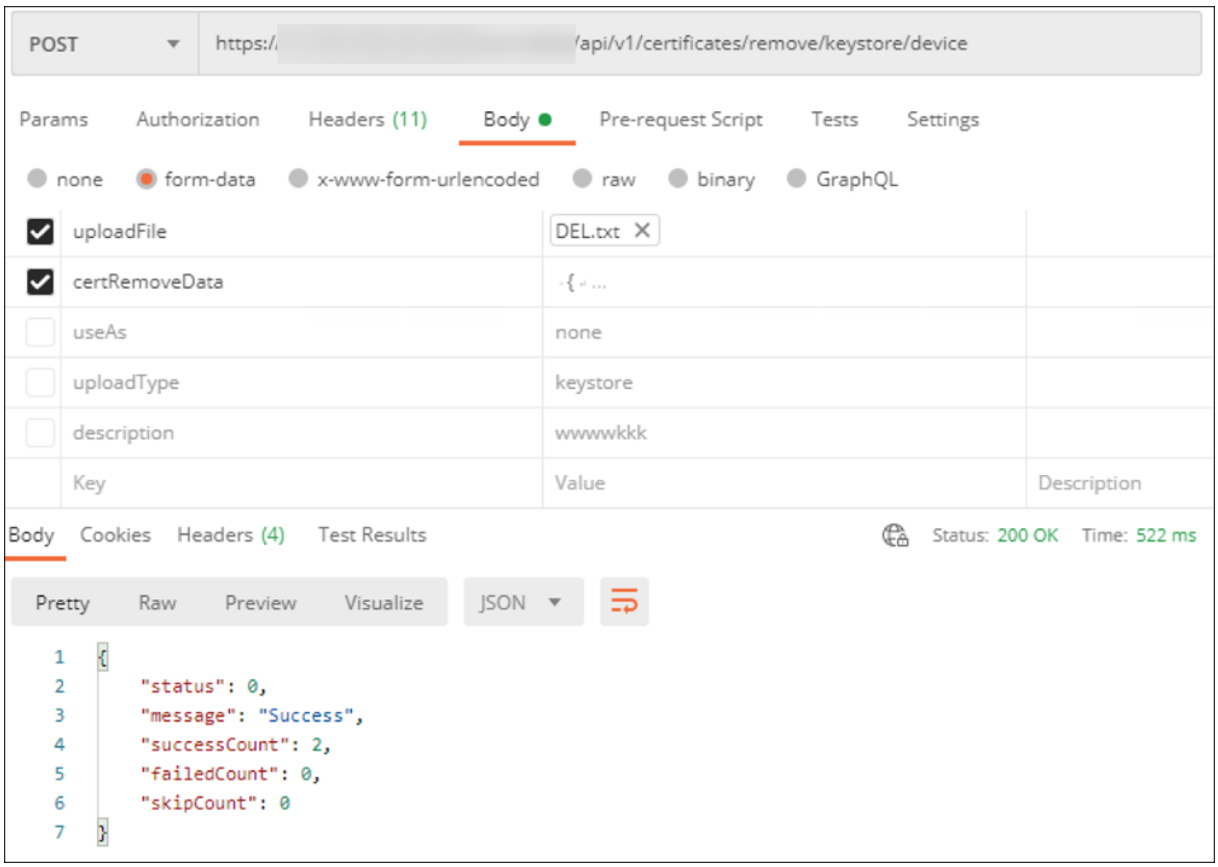


Sie können auch eine Massenlöschung von Zertifikaten ausführen, indem Sie eine Textdatei mit dem Wert von `device_identity_value` für jedes zu löschende Zertifikat erstellen. Rufen Sie in der REST API die Lösch-API auf und verwenden Sie die folgende Anforderung, wobei Sie `device_identity_value` durch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

```
```
{

    "identityType"="device_identity_value"
 }

<!--NeedCopy--> ```
```

 
```



Aktualisieren eines Zertifikats

In Citrix Endpoint Management 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 folgende Aktionen ausführen:

- Sie ersetzen den vorhandenen Eintrag.
- Sie löschen den Eintrag.

Nachdem Sie ein neues Zertifikat hochgeladen haben, können Sie das alte Zertifikat nicht löschen. Wenn Sie die Einstellung "PKI-Entitäten"konfigurieren, sind beide Zertifikate im Menü **SSL-Clientzertifikat** vorhanden. Das neuere Zertifikat steht weiter unten in der Liste als das alte Zertifikat.

Aktualisieren von Zertifikaten

1. Führen Sie die Schritte unter Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne aus, um ein Ersatzzertifikat zu erstellen.

> **Wichtig:**
>
> Verwenden Sie die Option nicht, um ein Zertifikat mit dem vorhandenen privaten Schlüssel zu erstellen. Wenn Sie ein Zertifikat zum Aktualisieren eines ablaufenden Zertifikats erstellen, muss der private Schlüssel ebenfalls neu sein.

2. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Mit der Suchleiste können Sie die Einstellung **Zertifikate** suchen und öffnen.
3. 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.

Um ein APNs-Zertifikat zu aktualisieren, führen Sie die Schritte zum Erstellen eines Zertifikats aus und rufen dann das Apple Push Certificates Portal auf. Weitere Informationen finden Sie unter Erneuern eines APNs-Zertifikats.

Ist NetScaler Gateway für SSL-Offload eingerichtet, stellen Sie beim Generieren eines neuen Zertifikats sicher, dass Sie den Load Balancer mit der neuen cacert.perm aktualisieren.

> **Hinweis:**
>
> Wenn Sie von on-premises XenMobile zu Citrix Endpoint Management migriert haben und Ihr Zertifikat aktualisieren, wenden Sie sich nach Abschluss der vorherigen Schritte an den Citrix Support. Sie müssen ihnen eine Kopie des neuen Zertifikats (im PFX-Format), einschließlich des Zertifikatskennworts, zur Verfügung stellen. Der Citrix Support aktualisiert Cloud-NetScaler und startet die Mandantenknoten neu, um den Zertifikatsupdateprozess abzuschließen.

Aktualisieren einer PKI-Dienstzertifizierungsstelle

Sie können anfordern, dass Citrix Cloud Operations die internen PKI-Zertifizierungsstellen in Ihrer Citrix Endpoint Management-Bereitstellung aktualisiert oder neu generiert. Öffnen Sie einen Technischer Support-Fall für diese Anfragen.

```
When the new CAs are available, Cloud Operations lets you know that you
    can proceed with renewing the device certificates for your users.
```

Verlängern von Gerätezertifikaten

Wenn ein Zertifikat auf einem Gerät abläuft, wird es ungültig. Sie können dann keine weiteren sicheren Transaktionen in Ihrer Umgebung ausführen und haben keinen Zugriff mehr auf Citrix Endpoint Management-Ressourcen. Die Zertifizierungsstelle (ZS) fordert Sie vor dem Ablaufdatum

zur Verlängerung des SSL-Zertifikats auf. Führen Sie die zuvor beschriebenen Schritte aus, um das Zertifikat zu aktualisieren, und erneuern Sie dann das Zertifikat auf registrierten Geräten.

Für unterstützte iOS-, macOS- und Android-Geräte können Sie die Zertifikatsverlängerung über die Sicherheitsaktion "Zertifikatserneuerung"einleiten. Sie erneuern Gerätezertifikate über die Citrix Endpoint Management-Konsole oder die öffentliche REST API. Registrierte Windows-Geräte müssen von den Benutzern erneut registriert werden, damit sie eine neue Gerätezertifizierungsstelle erhalten.

Wenn Geräte das nächste Mal eine Verbindung zu Citrix Endpoint Management herstellen, gibt der Citrix Endpoint Management-Server neue Gerätezertifikate basierend auf der neuen Zertifizierungsstelle aus.

Erneuern der Gerätezertifikate über die Konsole

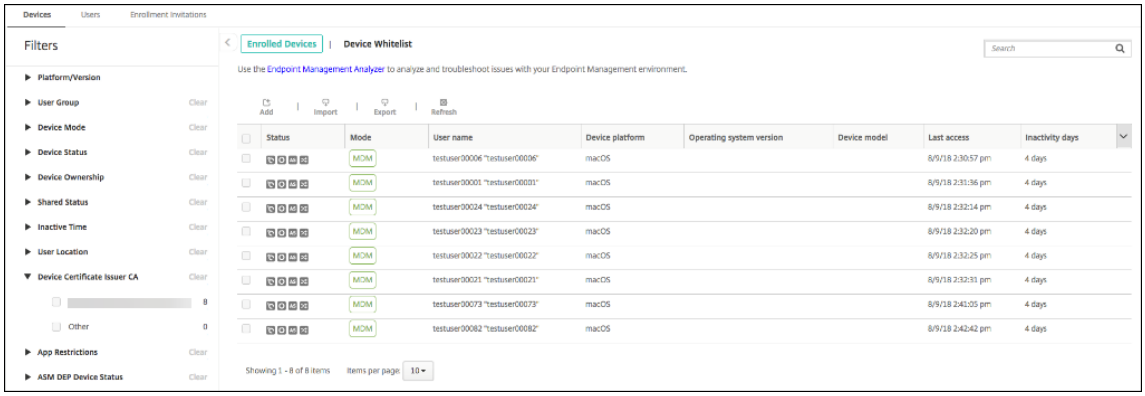
1. Gehen Sie zu **Verwalten > Geräte** und wählen Sie die Geräte aus, für die Sie Gerätezertifikate erneuern möchten.
2. Klicken Sie auf **Sichern** und klicken Sie dann auf **Zertifikaterneuerung**.

   Registrierte Geräte funktionieren weiterhin ohne Unterbrechung. Citrix Endpoint Management gibt ein Gerätezertifikat aus, wenn ein Gerät eine Verbindung zum Server herstellt.

Abfragen der Geräte, die in einer bestimmten Zertifizierungsstellengruppe für Gerätezertifikate sind:

1. Erweitern Sie unter **Verwalten > Geräte** den Bereich **Filter**.
2. Erweitern Sie im Bereich **Filter** die Option **Ausstellende ZS für Gerätezertifikat** und wählen Sie dann die ausstellende ZS, die Sie erneuern möchten.

In der Gerätetabelle werden die Geräte für die ausgewählten ausstellenden Zertifizierungsstellen angezeigt.



Erneuern der Gerätezertifikate über die REST API

Citrix Endpoint Management verwendet intern folgende Zertifizierungsstellen für PKI: Stamm-ZS, Geräte-ZS und Server-ZS. Diese Zertifizierungsstellen sind eine logische Gruppe und haben einen Gruppennamen. Während des Citrix Endpoint Management-Provisioning generiert der Server drei Zertifizierungsstellen und gibt ihnen den Gruppennamen "Standard".

Die Zertifizierungsstelle stellt die folgenden APIs zum Verwalten und Erneuern der Gerätezertifikate bereit. Registrierte Geräte funktionieren weiterhin ohne Unterbrechung. Citrix Endpoint Management gibt ein Gerätezertifikat aus, wenn ein Gerät eine Verbindung zum Server herstellt. Weitere Informationen finden Sie im PDF-Dokument Public API for REST Services.

- Liefert eine Liste von Geräten, die noch die alte ZS verwenden (siehe Abschnitt 3.16.2 im PDF-Dokument "Public API for REST Services").
- Gerätezertifikat erneuern (siehe Abschnitt 3.16.58)
- Alle ZS-Gruppen abrufen (siehe Abschnitt 3.23.1)

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 Citrix Secure Mail-Pushbenachrichtigungen. Außerdem können Sie keine weiteren Pushbenachrichtigungen für Ihre Apps senden.

APNs-Zertifikat für die Verwaltung von iOS-Geräten

Zum Registrieren und Verwalten von iOS-Geräten bei bzw. mit Citrix Endpoint Management müssen Sie ein APNs-Zertifikat von Apple erstellen und einrichten. Wenn das Zertifikat abläuft, können die

Benutzer keine Registrierung bei Citrix Endpoint Management 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:

```
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.

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

Thank You,

Apple Push Notification Service
<!--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 MDX 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 Citrix Endpoint Management-Serverzertifikate gültig sind, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Citrix Endpoint Management-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.

NetScaler Gateway

Weitere Informationen zur Handhabung des Zertifikatablaufs beim NetScaler Gateway finden Sie unter How to handle certificate expiry on NetScaler im Knowledge Center des Citrix Supports.

Ein abgelaufenes NetScaler Gateway-Zertifikat hindert Benutzer daran, Geräte zu registrieren und auf den Store zuzugreifen. Das abgelaufene Zertifikat verhindert außerdem, dass Benutzer bei der Verwendung von Citrix 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 NetScaler Gateway-Zertifikate zu überwachen. Das Center benachrichtigt Sie zudem, wenn ein Zertifikatablauf ansteht. Die Tools helfen bei der Überwachung der folgenden NetScaler Gateway-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

NetScaler Gateway und Citrix Endpoint Management

June 25, 2024

Bei Integration in Citrix Endpoint Management bietet NetScaler Gateway Remotezugriff von Geräten auf das interne Netzwerk und interne Ressourcen. Citrix Endpoint Management erstellt ein Micro-VPN von den Apps auf dem Gerät zu NetScaler Gateway.

Sie können den Citrix Gateway Service (Preview) oder ein on-premises NetScaler Gateway verwenden. Einen Überblick über diese beiden NetScaler Gateway-Lösungen finden Sie unter Konfigurieren eines NetScaler Gateway für Citrix Endpoint Management.

Konfigurieren der Authentifizierung für den Remotezugriff von Geräten auf das interne Netzwerk

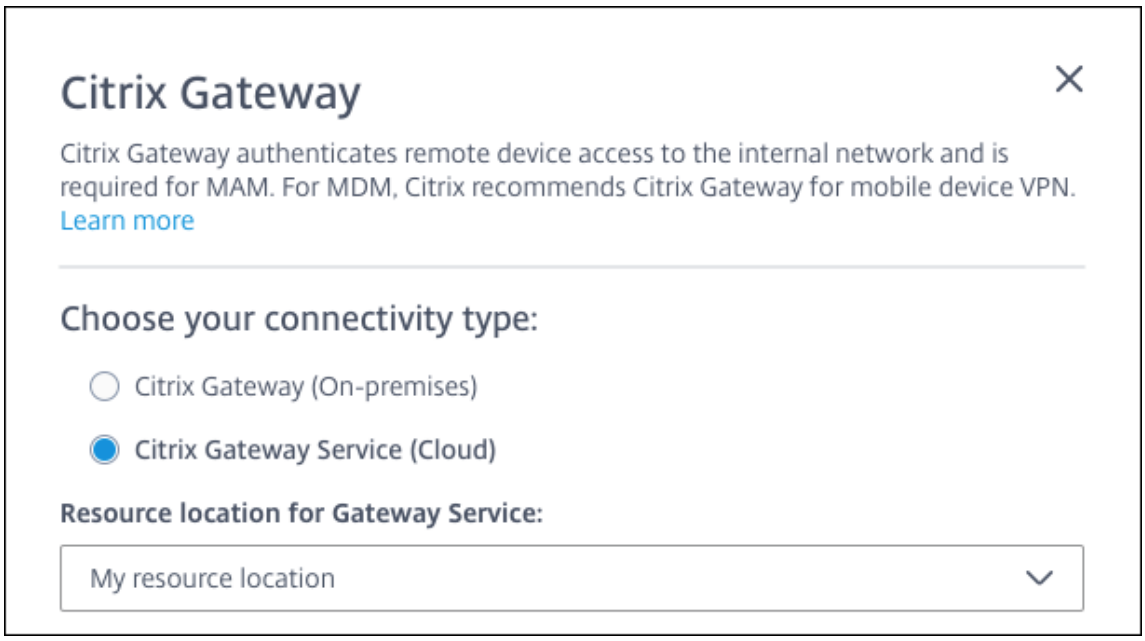
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Server** auf **NetScaler Gateway**. Die Seite **NetScaler Gateway** wird angezeigt. In dem folgenden Beispiel ist eine NetScaler Gateway-Instanz 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 Citrix Endpoint Management das Authentifizierungszertifikat zusammen mit Citrix Secure Hub verwenden soll. Mit einem gemeinsam genutzten Zertifikats kann NetScaler Gateway die Clientzertifikatauthentifizierung verarbeiten. Die Standardeinstellung ist **Aus**.
   - **Anmeldeinformationsanbieter:** Klicken Sie in der Dropdownliste auf den Namen des Anmeldeinformationsanbieters. Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.
4. Klicken Sie auf **Speichern**.

Hinzufügen einer Citrix Gateway Service-Instanz (Preview)

Nach dem Speichern der Authentifizierungseinstellungen fügen Sie Citrix Endpoint Management eine NetScaler Gateway-Instanz hinzu.

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Scrollen Sie auf der Seite **Einstellungen** zur NetScaler Gateway-Kachel und klicken Sie auf **Setup starten**. Die Seite **NetScaler Gateway** wird angezeigt.
3. Wählen Sie **Citrix Gateway Service (Cloud)** und geben Sie den Ressourcenstandort für den Gateway Service an.



- **Ressourcenstandort für Gateway Service:** ist erforderlich, wenn Sie Citrix Secure Mail verwenden. Legen Sie den Ressourcenstandort für den STA-Dienst fest. Der Ressourcenstandort muss ein konfiguriertes NetScaler Gateway enthalten. Wenn Sie später einen für den Gateway Service konfigurierten Ressourcenstandort entfernen möchten, aktualisieren Sie diese Einstellung.

Nachdem Sie diese Einstellungen vorgegeben haben, klicken Sie auf **Verbinden**, um die Verbindung herzustellen. Das neue NetScaler Gateway wird hinzugefügt. Die Kachel **Citrix Gateway Service(Cloud)** wird nun auf der Seite **Einstellungen** angezeigt. Um eine Instanz zu bearbeiten, klicken Sie auf **Weitere Informationen**. Wenn am ausgewählten Ressourcenstandort keine Gateway Connectors verfügbar sind, klicken Sie auf **Gateway Connector hinzufügen**. Folgen Sie den angezeigten Anweisungen, um Gateway Connectors zu installieren. Sie können Gateway Connectors auch später hinzufügen.

4. Klicken Sie auf **Skript speichern und exportieren**.

   - **Skript speichern und exportieren**. Klicken Sie auf die Schaltfläche, um Ihre Einstellungen zu speichern und ein Konfigurationspaket zu exportieren. Sie können ein Skript aus dem Paket in NetScaler Gateway hochladen, um es mit Citrix Endpoint Management-Einstellungen zu konfigurieren. Weitere Informationen finden Sie im Anschluss an diese Schritte unter "Konfigurieren eines NetScaler Gateway für Citrix Endpoint Management".

Sie haben damit ein NetScaler Gateway hinzugefügt. Die Kachel **NetScaler Gateway** wird nun auf der Seite **Einstellungen** angezeigt. Um eine Instanz zu bearbeiten, klicken Sie auf **Weitere Informationen**.

Konfigurieren eines on-premises NetScaler Gateway für Citrix Endpoint Management

Zum Konfigurieren eines lokalen NetScaler Gateway für Citrix Endpoint Management führen Sie die in den nachfolgenden Abschnitten erläuterten allgemeinen Schritte aus.

1. Vergewissern Sie sich, dass Ihre Umgebung die Voraussetzungen erfüllt.
2. Exportieren Sie das Skriptpaket aus der Citrix Endpoint Management-Konsole.
3. Extrahieren Sie die Dateien aus dem Paket. Wenn Sie nur klassische Richtlinien im NetScaler Gateway verwenden und Citrix ADC 13.0 oder früher ausführen, verwenden Sie das Skript mit "Classic"im Dateinamen. Wenn Sie erweiterte Richtlinien verwenden oder Citrix ADC 13.1 oder höher ausführen, verwenden Sie das Skript mit "Advanced"im Dateinamen.
4. Führen Sie das Skript auf dem NetScaler Gateway aus. Aktuelle und detaillierte Anweisungen finden Sie in der Readmedatei des Skripts.
5. Testen Sie die Konfiguration.

Mit dem Skript werden die folgenden, für Citrix Endpoint Management erforderlichen NetScaler Gateway-Einstellungen konfiguriert:

- Virtuelle NetScaler Gateway-Server für MDM und MAM
- Sitzungsrichtlinien für virtuelle NetScaler Gateway-Server
- Citrix Endpoint Management-Serverdetails
- Proxy-Load-Balancer für die Zertifikatüberprüfung
- Authentifizierungsrichtlinien und Aktionen für den virtuellen NetScaler 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 NetScaler Gateway
- Andere Bindungen: Dienstrichtlinie, ZS-Zertifikat

Mit dem Skript wird folgende Konfiguration nicht erstellt:

- Exchange-Lastausgleich
- Citrix Files-Lastausgleich
- ICA-Proxykonfiguration
- SSL-Offload

Voraussetzungen für die Verwendung der Skripts zur NetScaler Gateway-Konfiguration

Anforderungen für Citrix Endpoint Management:

- Konfigurieren Sie LDAP und das NetScaler Gateway in Citrix Endpoint Management, bevor Sie das Skriptpaket exportieren. Wenn Sie Einstellungen ändern, exportieren Sie das Skriptpaket erneut.

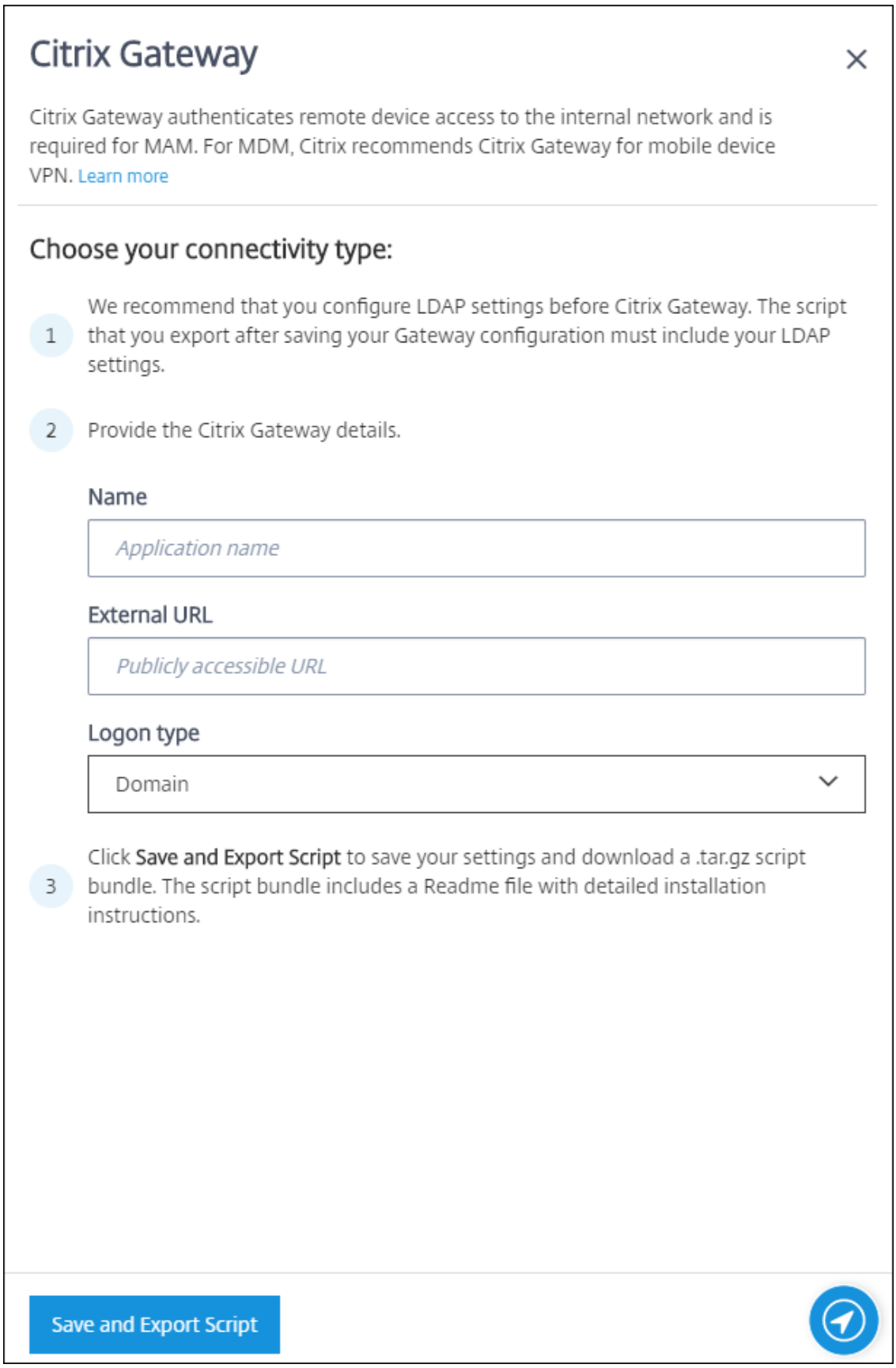
Anforderungen für NetScaler Gateway:

- Wenn Sie die zertifikatbasierte Authentifizierung am NetScaler Gateway verwenden, müssen Sie SSL-Zertifikate auf einem Citrix ADC-Gerät erstellen. Siehe Erstellen und Verwenden von SSL-Zertifikaten auf einem Citrix ADC-Gerät.
- NetScaler Gateway (mindestens Version 11.0 Build 70.12).
- NetScaler Gateway-IP-Adresse ist konfiguriert und verfügt über Konnektivität mit dem LDAP-Server (es sei denn, für LDAP ist ein Lastausgleich eingerichtet).
- NetScaler Gateway-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.
- NetScaler Gateway ist per Plattform-/Universell- oder Testlizenz lizenziert. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX126049.

Export des Skriptpakets aus Citrix Endpoint Management

Nach dem Speichern der Authentifizierungseinstellungen fügen Sie Citrix Endpoint Management eine NetScaler Gateway-Instanz hinzu.

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Scrollen Sie auf der Seite **Einstellungen** zur NetScaler Gateway-Kachel und klicken Sie auf **Setup starten**. Die Seite **NetScaler Gateway** wird angezeigt.
3. Wählen Sie **NetScaler Gateway (on-premises)** und konfigurieren Sie diese Einstellungen:



- **Name:** Geben Sie einen Namen für die NetScaler Gateway-Instanz ein.
- **Externe URL:** Geben Sie die öffentlich zugängliche URL für NetScaler Gateway ein. Beispiel: `https://receiver.com`.
- **Anmeldetyp:** Wählen Sie einen Anmeldetyp. Zur Auswahl stehen **Domäne**, **Nur Sicherheitstoken**, **Domäne und Sicherheitstoken**, **Zertifikat**, **Zertifikat und Domäne** und **Zertifikat und Sicherheitstoken**. Die Standardeinstellung ist **Domäne**.

Wenn Sie mehrere Domänen haben, verwenden Sie **Zertifikat und Domäne**. Weitere Informationen finden Sie unter Konfigurieren der Authentifizierung für mehrere Domänen.

Die zertifikatbasierte Authentifizierung über NetScaler Gateway erfordert zusätzliche Konfiguration. Beispielsweise müssen Sie Ihr Stammzertifizierungsstellenzertifikat auf das Citrix ADC-Gerät hochladen. Siehe Erstellen und Verwenden von SSL-Zertifikaten auf einem Citrix ADC-Gerät.

Weitere Informationen finden Sie unter Authentifizierung im Bereitstellungshandbuch.

4. Klicken Sie auf **Skript speichern und exportieren**.

   - **Skript speichern und exportieren**. Klicken Sie auf die Schaltfläche, um Ihre Einstellungen zu speichern und ein Konfigurationspaket zu exportieren. Sie können ein Skript aus dem Paket in NetScaler Gateway hochladen, um es mit Citrix Endpoint Management-Einstellungen zu konfigurieren. Weitere Informationen finden Sie im Anschluss an diese Schritte unter "Konfigurieren eines NetScaler Gateway für Citrix Endpoint Management".

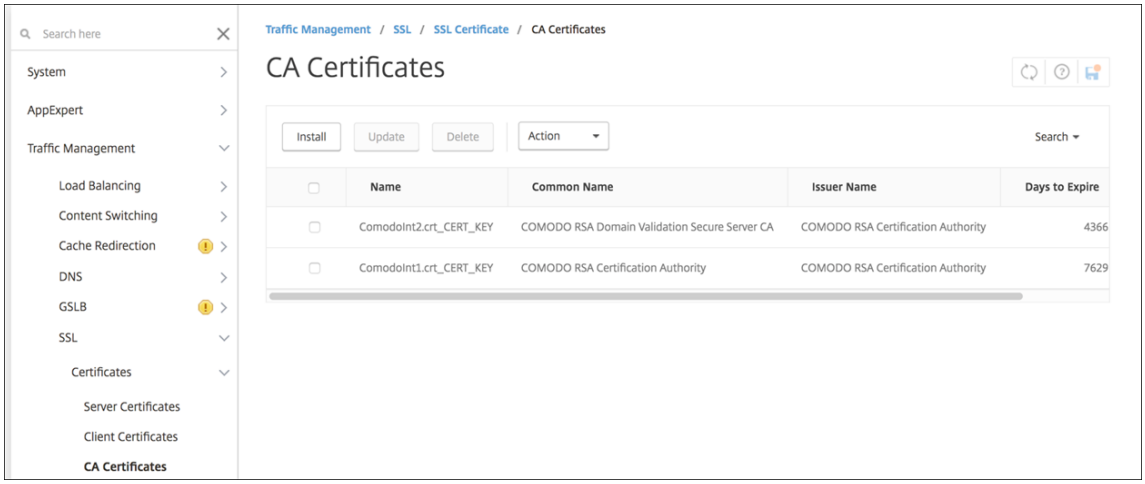
   Sie haben damit ein NetScaler Gateway hinzugefügt. Die Kachel **NetScaler Gateway** wird nun auf der Seite **Einstellungen** angezeigt. Um eine Instanz zu bearbeiten, klicken Sie auf **Weitere Informationen**.

Installieren des Skripts in der Umgebung

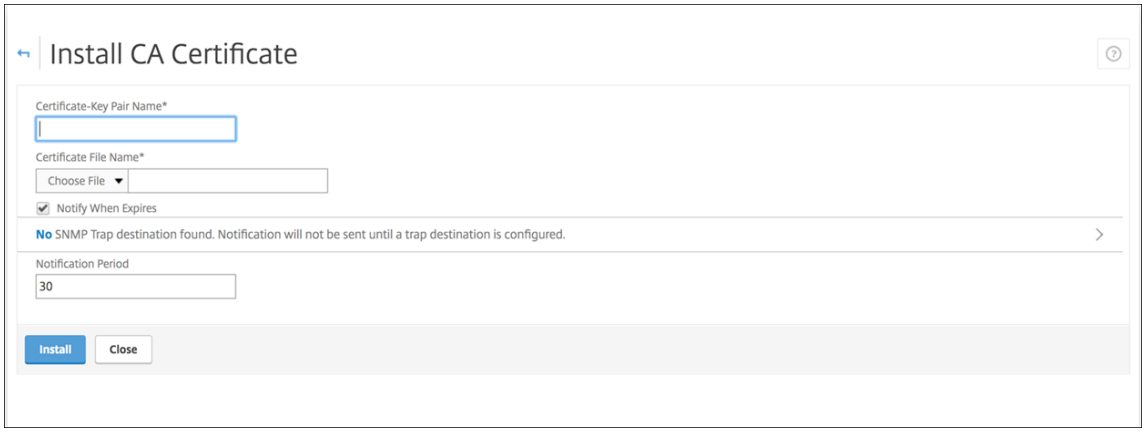
Das Skriptpaket enthält Folgendes:

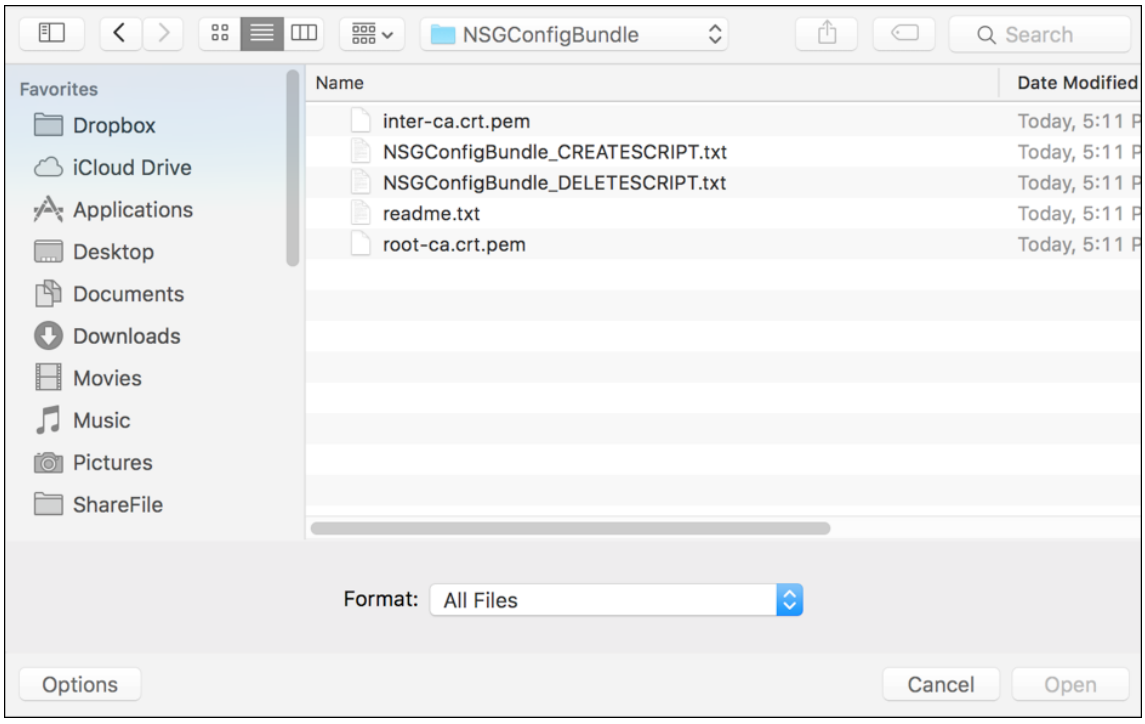
- Infodatei mit detaillierten Anweisungen
- Skripts mit den NetScaler-CLI-Befehlen zum Konfigurieren der erforderlichen Komponenten in NetScaler
- Öffentliches Stamm-ZS-Zertifikat und Zwischenzertifikat
- Skripts mit den NetScaler-CLI-Befehlen zum Entfernen der NetScaler-Konfiguration

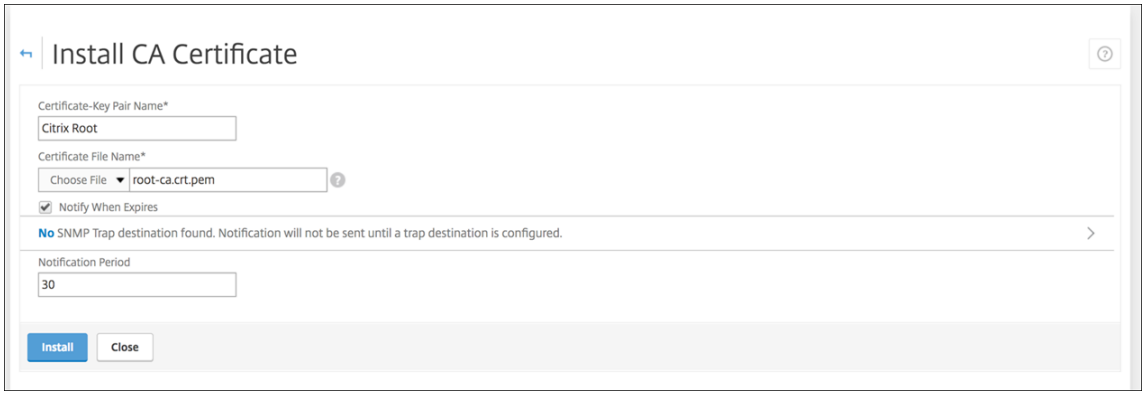
1. Laden Sie die Zertifikatdateien aus dem Skriptpaket auf das Citrix ADC-Gerät hoch und installieren Sie sie im Verzeichnis /nsconfig/ssl/. Siehe Erstellen und Verwenden von SSL-Zertifikaten auf einem Citrix ADC-Gerät.

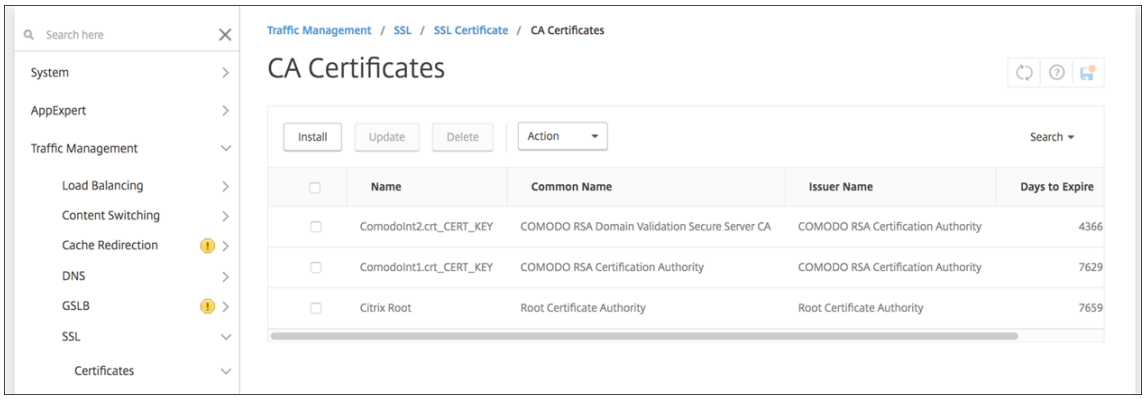


Die folgenden Beispiele zeigen, wie das Stammzertifikat installiert wird.









Installieren Sie auf jeden Fall sowohl das Stammzertifikat als auch das Zwischenzertifikat.

2. Bearbeiten Sie das Skript (ConfigureCitrixGatewayScript_Classic.txt oder ConfigureCitrixGatewayScript_Advanced.txt), indem Sie alle Platzhalter durch Details Ihrer Umgebung ersetzen.

```
#Important Note: Please update the following placeholders with valid values:
# <NSG_IP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a NAT.
# <PROXY_LB_VIP> -- Virtual IP Address to be assigned to the proxy load-balancer configured on the NetScaler. This IP address must be a private address.
# <LDAP_SVC_USERNAME> -- LDAP Service Account Username.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <SERVER_CERT_NAME> -- Name of the server certificate file on the NetScaler. This certificate is bound to the NetScaler Gateway virtual server.
```

3. Führen Sie das bearbeitete Skript in der NetScaler-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/OfflineNSGConfigtBundle_CREATESCRIPT.txt"
```



```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

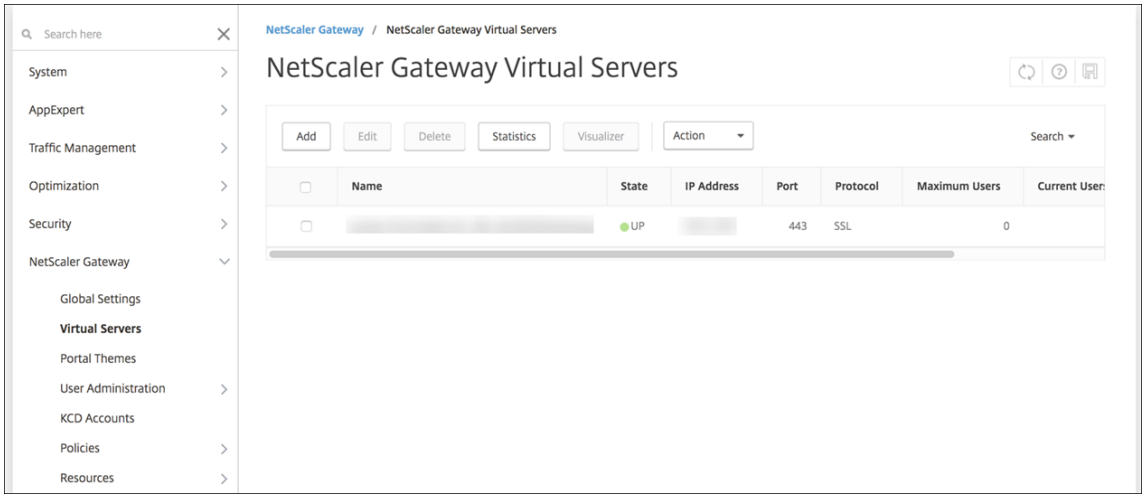
Nach Abschluss der Skriptausführung werden die folgenden Zeilen angezeigt:

```
exec: save ns config
 Done
 Done
root@ns#
```

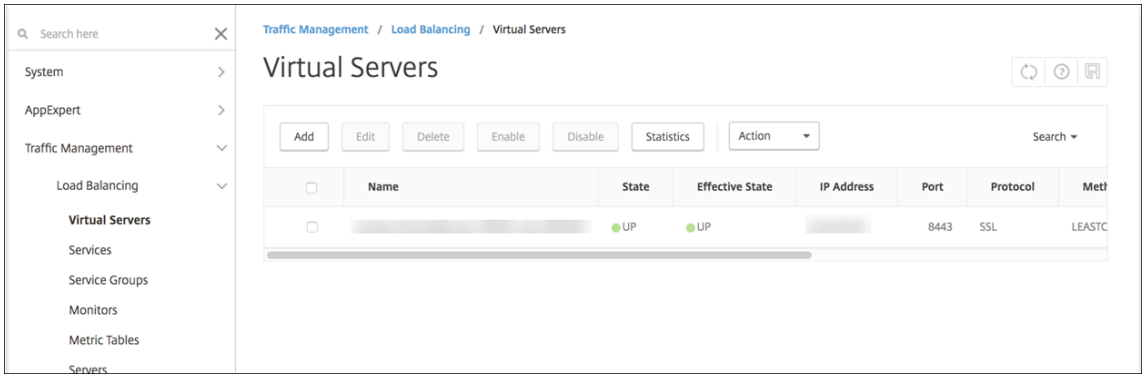
Testen der Konfiguration

Führen Sie zum Überprüfen der Konfiguration folgende Schritte aus:

1. Überprüfen Sie, ob für den virtuellen NetScaler 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 NetScaler Gateway-URL her und versuchen Sie, sich zu authentifizieren. Wenn die Authentifizierung gelingt, werden Sie an einen HTTP-404-Fehler (nicht gefunden) weitergeleitet.
4. Registrieren Sie ein Gerät für MDM und MAM.

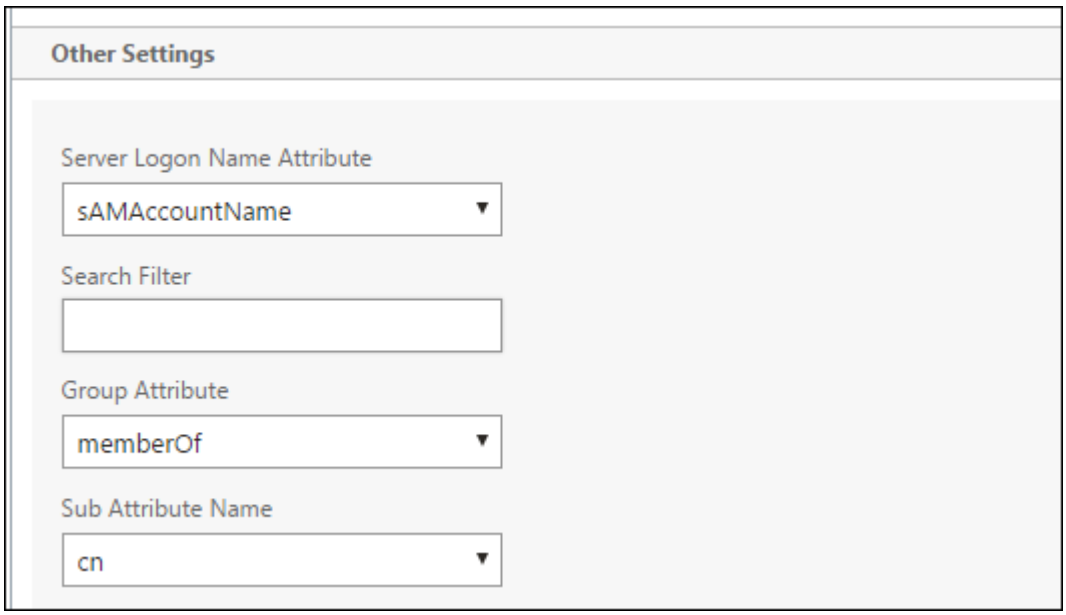
Konfigurieren der Authentifizierung für mehrere Domänen

Wenn Sie mehrere Citrix Endpoint Management-Instanzen haben (z. B. für die Test-, die Entwicklungs- und die Produktionsumgebung), müssen Sie NetScaler Gateway für die zusätzlichen Umgebungen manuell konfigurieren. (Sie können den NetScaler für XenMobile-Assistenten nur einmal ausführen.)

Konfigurieren von NetScaler Gateway

Führen Sie zum Konfigurieren von NetScaler Gateway-Authentifizierungsrichtlinien und einer Sitzungsrichtlinie für eine Umgebung mit mehreren Domänen folgende Schritte aus:

1. Erweitern Sie im Konfigurationsprogramm für NetScaler Gateway auf der Registerkarte **Configuration** die Optionen **NetScaler 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 angegebene Attribut. Sie geben es beim Konfigurieren von LDAP-Einstellungen in der Citrix Endpoint Management-Konsole an.

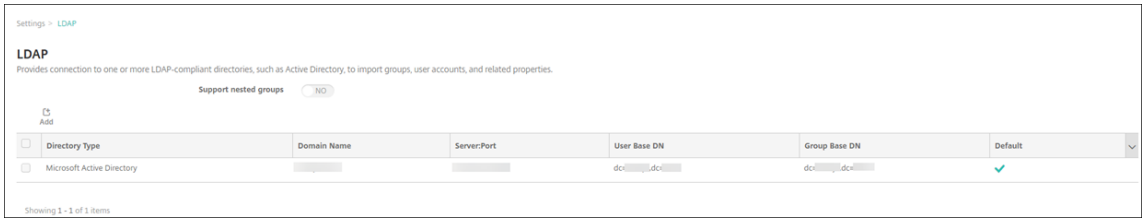


4. Wiederholen Sie diese Schritte für jede LDAP-Richtlinie. Für jede Domäne ist eine separate LDAP-Richtlinie erforderlich.
5. Geben Sie in der an den virtuellen NetScaler Gateway-Server gebundenen Sitzungsrichtlinie zu **Edit session profile > Published Applications**. Stellen Sie sicher, dass **Single Sign-On Domain** leer ist.

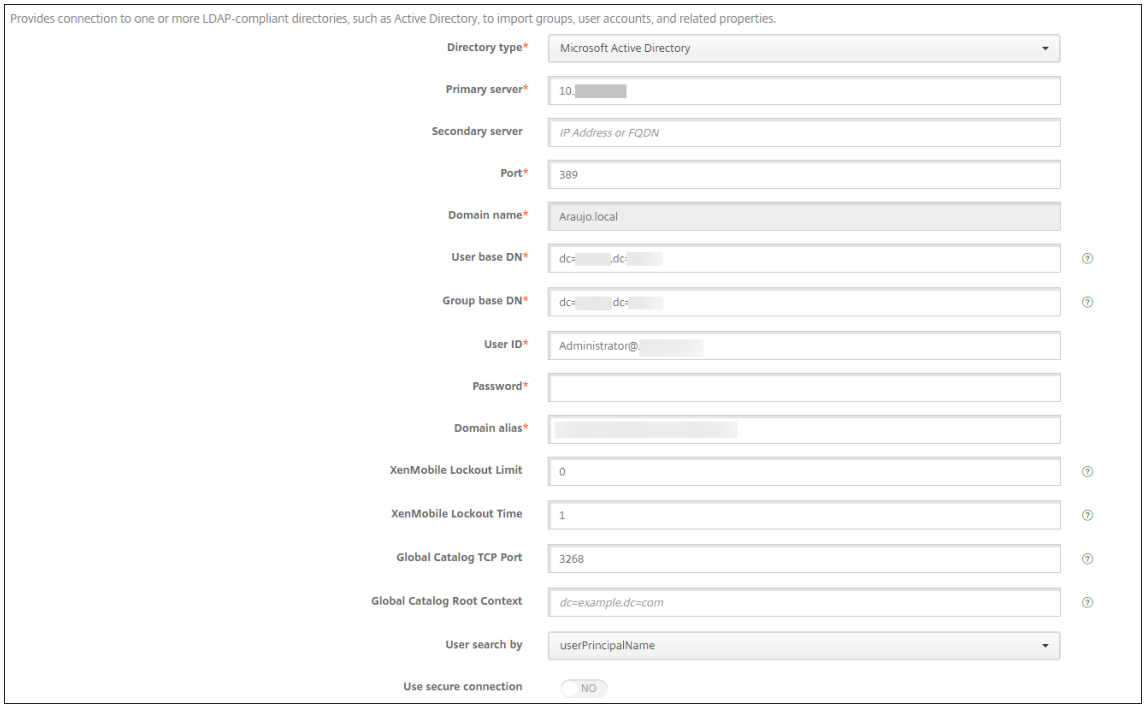
Citrix Endpoint Management-Konfiguration

Konfigurieren von Citrix Endpoint Management-LDAP für eine Umgebung mit mehreren Domänen:

1. Gehen Sie in der Citrix Endpoint Management-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: domäne1.com,domäne2.com,domäne3.com
   - Stellen Sie sicher, dass die Angabe im Feld **Benutzersuche nach** mit der Angabe unter **Server Logon Name Attribute** in der LDAP-Richtlinie von NetScaler Gateway übereinstimmt.



Verwerfen eingehender Verbindungsanforderungen an bestimmte URLs

Wenn NetScaler Gateway in Ihrer Umgebung für SSL-Offload konfiguriert ist, soll das Gateway möglicherweise eingehende Verbindungsanforderungen für bestimmte URLs verwerfen. Wenn Sie diese zusätzliche Sicherheit wünschen, wenden Sie sich an Citrix Cloud Operations und fordern Sie an, dass Ihre IP-Adresse für Ihre On-Premises-Rechenzentren zugelassen wird.

Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken

June 25, 2024

Citrix Endpoint Management unterstützt die domänenbasierte Authentifizierung mit einem oder mehreren Lightweight Directory Access Protocol-konformen Verzeichnissen. Sie konfigurieren eine Verbindung in Citrix Endpoint Management mit einem oder mehreren Verzeichnissen. Citrix Endpoint Management verwendet dann die LDAP-Konfiguration für den Import von Gruppen, Benutzerkonten und zugehörigen Eigenschaften.

> **Wichtig:**
>
> Der Authentifizierungsmodus kann nicht von einem Authentifizierungsmodustyp in einen anderen Authentifizierungsmodus geändert werden, nachdem Benutzer die Geräte bei Citrix End-

> point Management registriert haben. Beispielsweise können Sie den Authentifizierungsmodus nicht von **Domänenauthentifizierung** in **Domäne + Zertifikat** ändern, nachdem Benutzer sich registriert haben.

Info über LDAP

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.

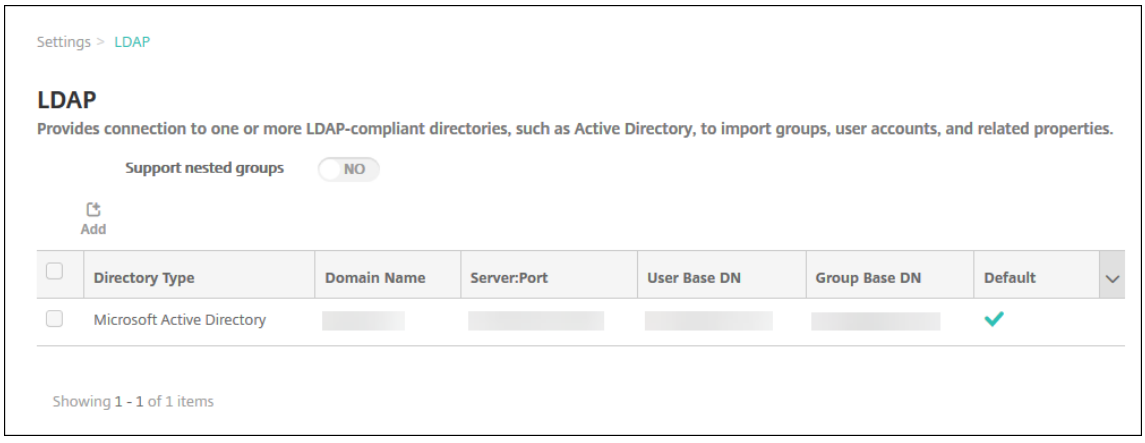
LDAP wird häufig zur Bereitstellung von Single Sign-On (SSO) für Benutzer eingesetzt, bei dem ein Kennwort (pro Benutzer) für mehrere Dienste verwendet wird. Mit Single Sign-On melden sich die Benutzer einmal bei der Unternehmenswebsite an und erhalten so authentifizierten Zugriff auf das Unternehmensintranet.

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.

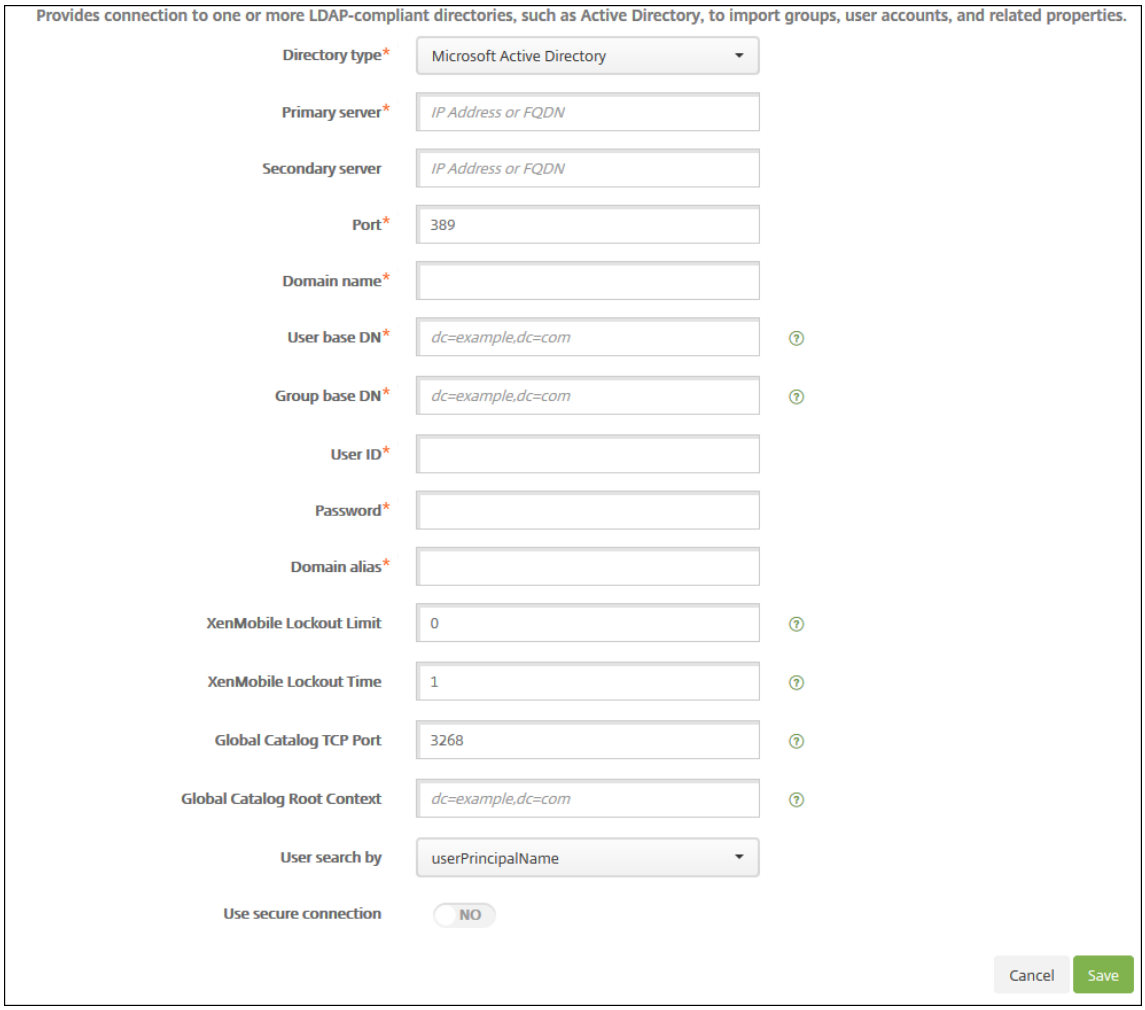
Konfigurieren oder Bearbeiten von LDAP-Verbindungen in Citrix Endpoint Management

Normalerweise konfigurieren Sie LDAP-Verbindungen beim Onboarding in Citrix Endpoint Management, wie unter Konfigurieren von LDAP beschrieben. Wenn die Bildschirme im Abschnitt beim Onboarding noch nicht verfügbar waren, verwenden Sie die Informationen in diesem Abschnitt, um LDAP-Verbindungen hinzuzufügen.

1. Gehen Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > LDAP**.
2. Klicken Sie unter **Server** auf **LDAP**. Die Seite **LDAP** wird angezeigt.



3. Klicken Sie auf der **LDAP**-Seite auf **Hinzufügen** oder **Bearbeiten**. Die Seite **LDAP hinzufügen** oder **LDAP bearbeiten** wird angezeigt.



4. Konfigurieren Sie folgende Einstellungen:

   - **Verzeichnistyp:** Klicken Sie in der Dropdownliste auf den entsprechenden 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.
- **Citrix Endpoint Management-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 Citrix Endpoint Management ausgesperrt. Die Standardeinstellung ist **0**.

  Sie können auch ein Sperrlimit festlegen, das unter dem Wert in Ihrer LDAP-Sperrrichtlinie liegt. So können Sie eine Benutzersperre verhindern, wenn Citrix Endpoint Management nicht beim LDAP-Server authentifiziert werden kann. Wenn die LDAP-Sperrrichtlinie beispielsweise bei 5 Versuchen liegt, konfigurieren Sie dieses Sperrlimit auf **4** oder niedriger.
- **Citrix Endpoint Management-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. Der Standardwert ist **1**.
- **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:** Wählen Sie ein Format für Benutzernamen oder Benutzer-ID aus, das Citrix Endpoint Management für die Suche nach Benutzern in diesem Verzeichnis verwendet werden soll. Benutzer geben dann bei der Registrierung ihren Benutzernamen

oder ihre Benutzer-ID in diesem Format ein. Wenn Sie die Einstellung **Benutzersuche nach** nach der Registrierung ändern, müssen sich Benutzer neu registrieren.

Wenn Sie **userPrincipalName** wählen, geben Benutzer einen Benutzerprinzipalnamen (UPN) in folgendem Format ein:

- `*username*@*domain*`

Bei Auswahl von **sAMAccountName** geben Benutzer einen SAM-Namen (Secure Account Manager) in einem der folgenden Formate ein:

- `*username*@*domain*`
- `*domain\username*`

- **Sichere Verbindung verwenden:** Wählen Sie aus, ob sichere Verbindungen verwendet werden sollen. Die Standardeinstellung ist **NEIN**.

5. Klicken Sie auf **Speichern**.

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 mit Domäne und Sicherheitstoken

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

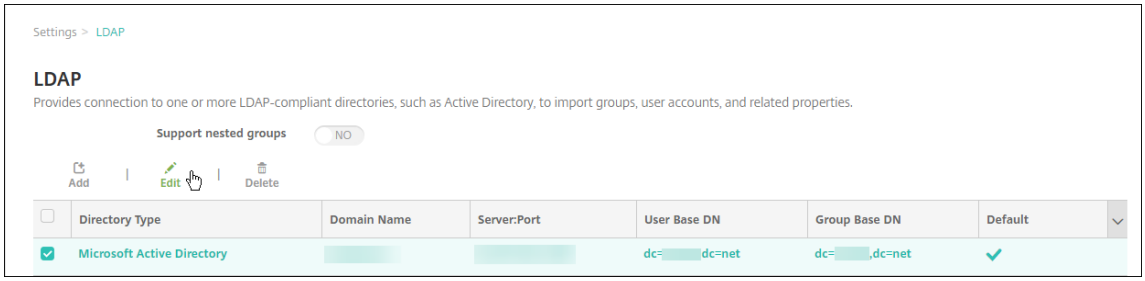
Die optimale Benutzerfreundlichkeit erreichen Sie, wenn Sie diese Konfiguration mit der Citrix-PIN und der Active Directory-Kennwortzwischenspeicherung kombinieren. Die Benutzer müssen dann ihre LDAP-Benutzernamen und -Kennwörter nicht wiederholt eingeben. Die Benutzer geben Benutzernamen und Kennwörter für die Registrierung sowie bei Kennwortablauf und Kontosperrung ein.

Konfigurieren von LDAP-Einstellungen

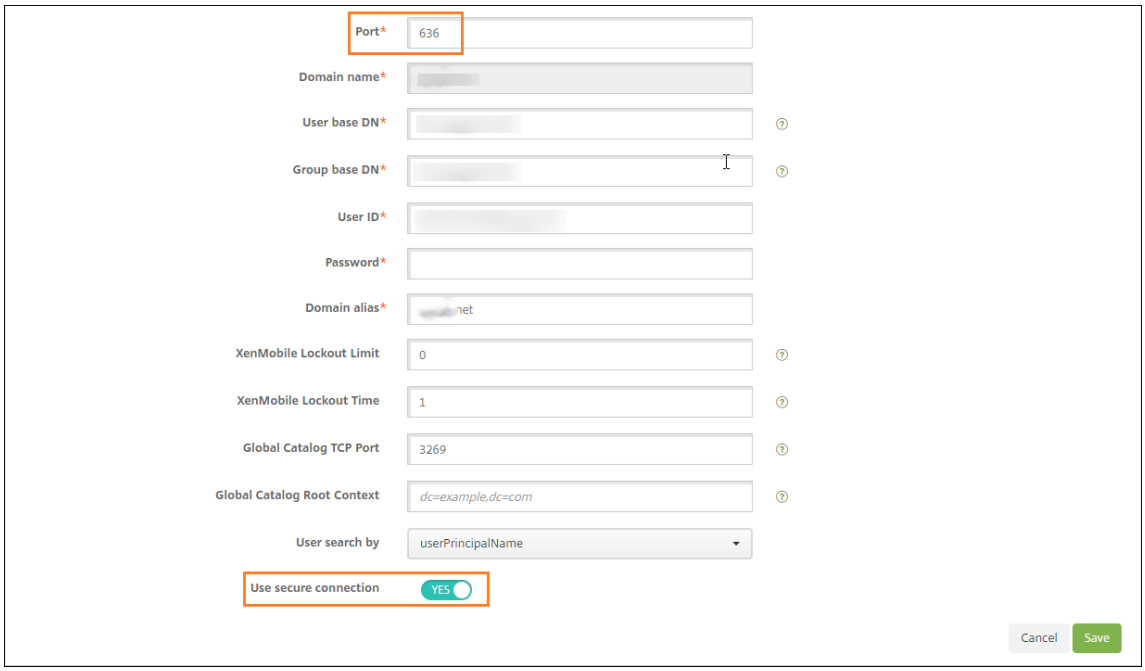
Wenn Sie LDAP für die Authentifizierung verwenden möchten, müssen Sie ein SSL-Zertifikat von einer Zertifizierungsstelle in Citrix Endpoint Management installieren. Weitere Informationen finden Sie

unter Hochladen von Zertifikaten.

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 NetScaler Gateway-Einstellungen

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

1. Klicken unter **Einstellungen** auf **NetScaler Gateway**.
2. Wählen Sie das NetScaler 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 NetScaler Gateway für die Authentifizierung mit Domäne und Sicherheitstoken

Konfigurieren Sie NetScaler Gateway-Sitzungsprofile und Richtlinien für die virtuellen Server, die mit Citrix Endpoint Management verwendet werden. Weitere Informationen finden Sie in der Dokumentation zu NetScaler Gateway.

Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne

June 25, 2024

Standardmäßig ist Citrix Endpoint Management für die Authentifizierung per Benutzernamen und Kennwort konfiguriert. Als zusätzliche Sicherheitsstufe für die Registrierung bei und den Zugriff auf die Citrix Endpoint Management-Umgebung ist die zertifikatbasierte Authentifizierung in Betracht zu ziehen. In der Citrix Endpoint Management-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 NetScaler Gateway 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 Citrix Endpoint Management registriert haben.

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

Sie können die in Citrix Endpoint Management erforderliche Konfiguration mit dem NetScaler für XenMobile-Assistenten durchführen, wenn Sie die NetScaler Gateway-Authentifizierung per Zertifikat oder per Zertifikat und Domäne verwenden. Sie können den NetScaler 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 Citrix Endpoint Management for Certificate and Security Token Authentication.

Die Clientzertifikatauthentifizierung ist für Geräte verfügbar, die bei MAM und MDM+MAM registriert sind. Zum Verwenden von Clientzertifikatauthentifizierung auf solchen Geräten müssen Sie den Microsoft-Server, Citrix Endpoint Management und dann NetScaler Gateway konfigurieren. Folgen Sie den in diesem Artikel beschriebenen allgemeinen Schritten.

Auf dem Microsoft-Server:

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

In Citrix Endpoint Management:

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

Informationen über die NetScaler Gateway-Konfiguration finden Sie in folgenden Artikeln der Citrix ADC-Dokumentation:

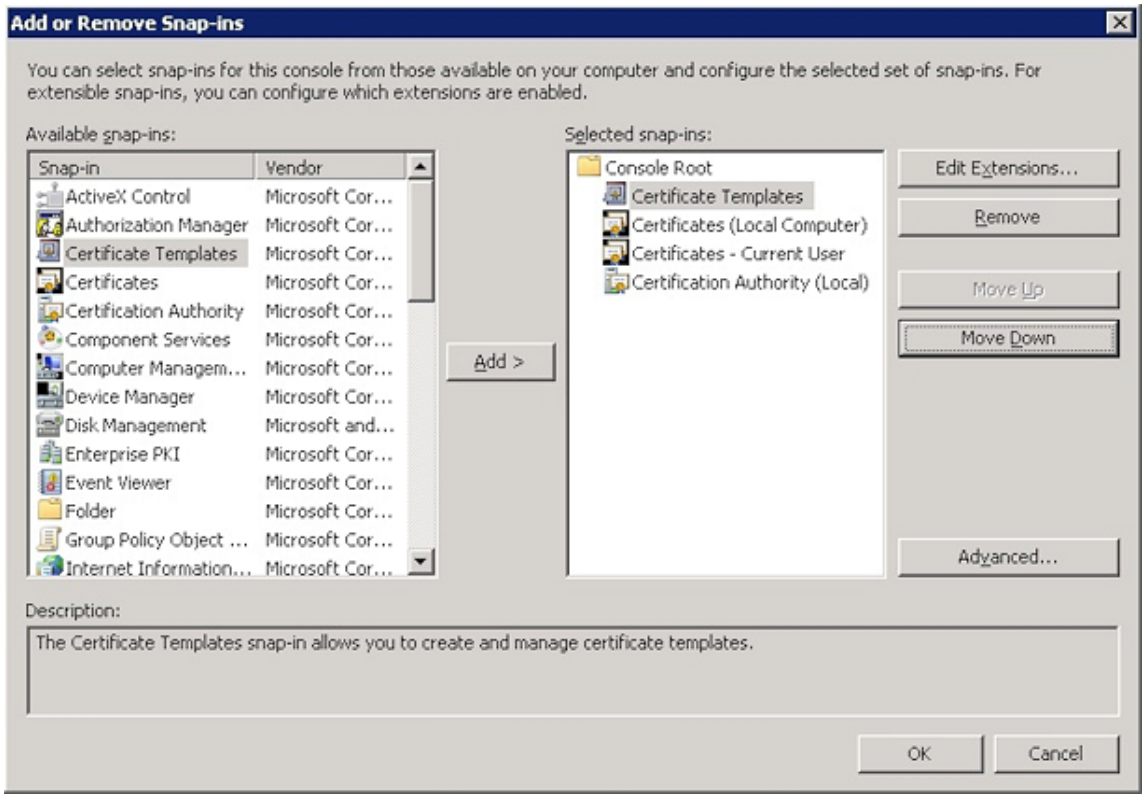
- Clientauthentifizierung
- SSL-Profilinfrastruktur
- Konfigurieren und Binden einer Richtlinie für die Clientzertifikatauthentifizierung

Voraussetzungen

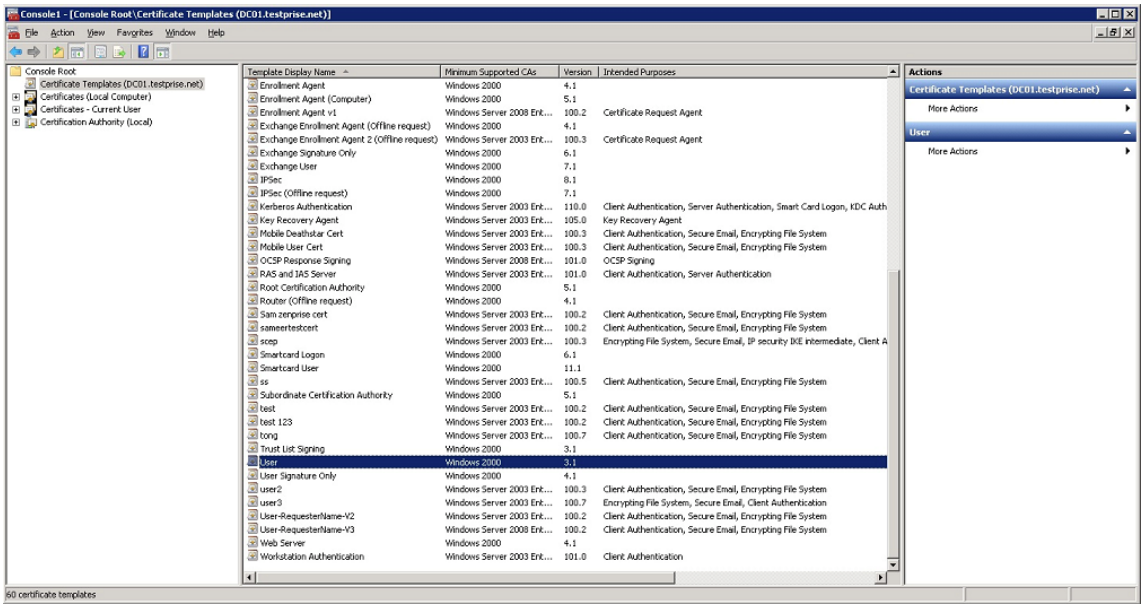
- Vermeiden Sie beim Erstellen einer Microsoft-Zertifikatdiensteentitätsvorlage die Verwendung von Sonderzeichen. Verwenden in Vorlagennamen beispielsweise nicht folgende Zeichen: **:** `! $ ()# % + * ~ ? | { } []`
- Informationen zum Konfigurieren der zertifikatbasierten Authentifizierung für Exchange ActiveSync finden Sie in der Microsoft-Dokumentation zu Exchange Server. 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 Stamm- und Zwischenzertifikate haben. Ansonsten schlägt die zertifikatbasierte Authentifizierung beim Einrichten des Postfachs in Citrix Secure Mail fehl. In der Exchange-IIS-Konsole müssen Sie folgende Schritte ausführen:
  - Fügen Sie die Website für die Citrix Endpoint Management-Verwendung mit Exchange hinzu und binden Sie das Webserverzertifikat.
  - 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

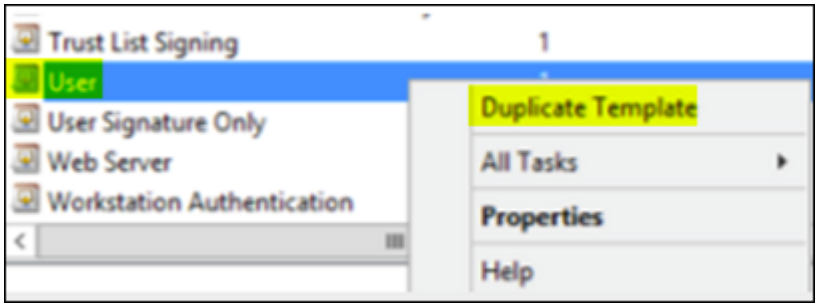
1. Öffnen Sie die Konsole und klicken Sie auf **Snap-In hinzufügen/entfernen**.
2. Fügen Sie die folgenden Snap-Ins hinzu:
   - Zertifikatvorlagen
   - Zertifikate (lokaler Computer)
   - Zertifikate –aktueller Benutzer
   - Zertifizierungsstelle (lokal)



3. Erweitern Sie **Zertifikatvorlagen**.



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



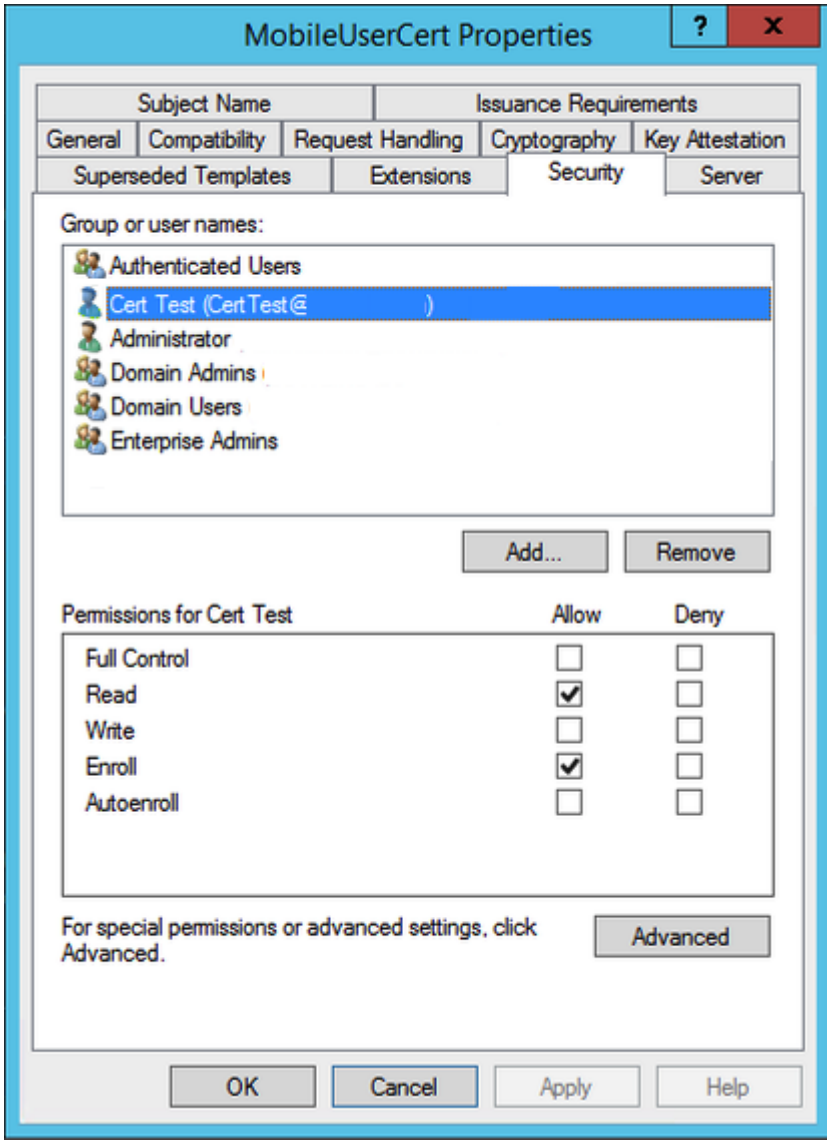
5. Geben Sie den Anzeigenamen der Vorlage an.

   > **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.

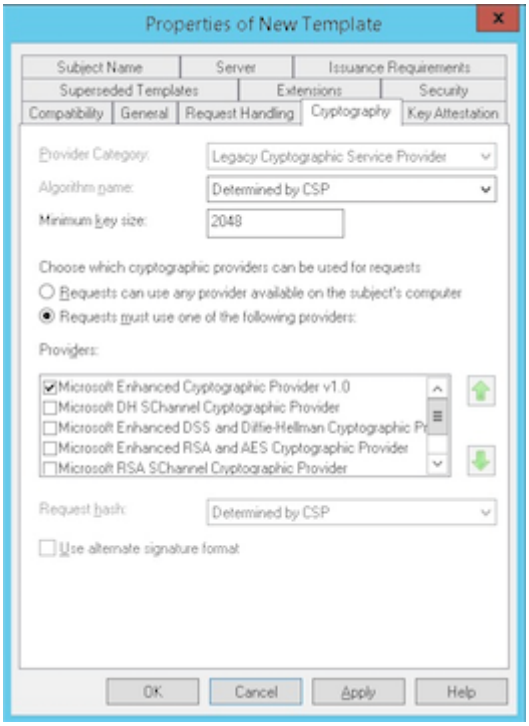
6. Wählen Sie als Vorlagentyp **Windows 2003 Server**. Wählen Sie in Windows 2012 R2-Server unter **Kompatibilität** die Option **Zertifizierungsstelle** und legen Sie als Empfänger **Windows 2003** fest.
7. Klicken Sie unter **Sicherheit** auf **Hinzufügen** und wählen Sie dann das AD-Benutzerkonto aus, das Citrix Endpoint Management zum Generieren von Zertifikaten verwendet.

   > **Wichtig:**
   >
   > Fügen Sie hier nur den Dienstkontobenutzer hinzu. Fügen Sie nur die Berechtigung **Registrieren** für dieses AD-Benutzerkonto hinzu.

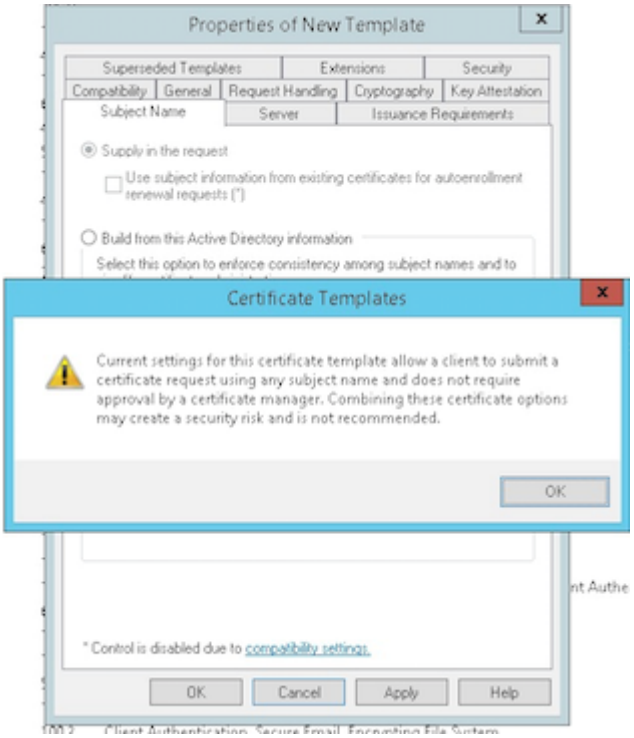
   Wie später in diesem Artikel beschrieben, erstellen Sie mit dem Dienstkonto ein PFX-Benutzerzertifikat. Weitere Informationen finden Sie unter Erstellen eines PFX-Zertifikats vom ZS-Server.



8. Geben Sie unter **Kryptografie** die Schlüsselgröße an. Sie geben die Schlüsselgröße später bei der Citrix Endpoint Management-Konfiguration ein.

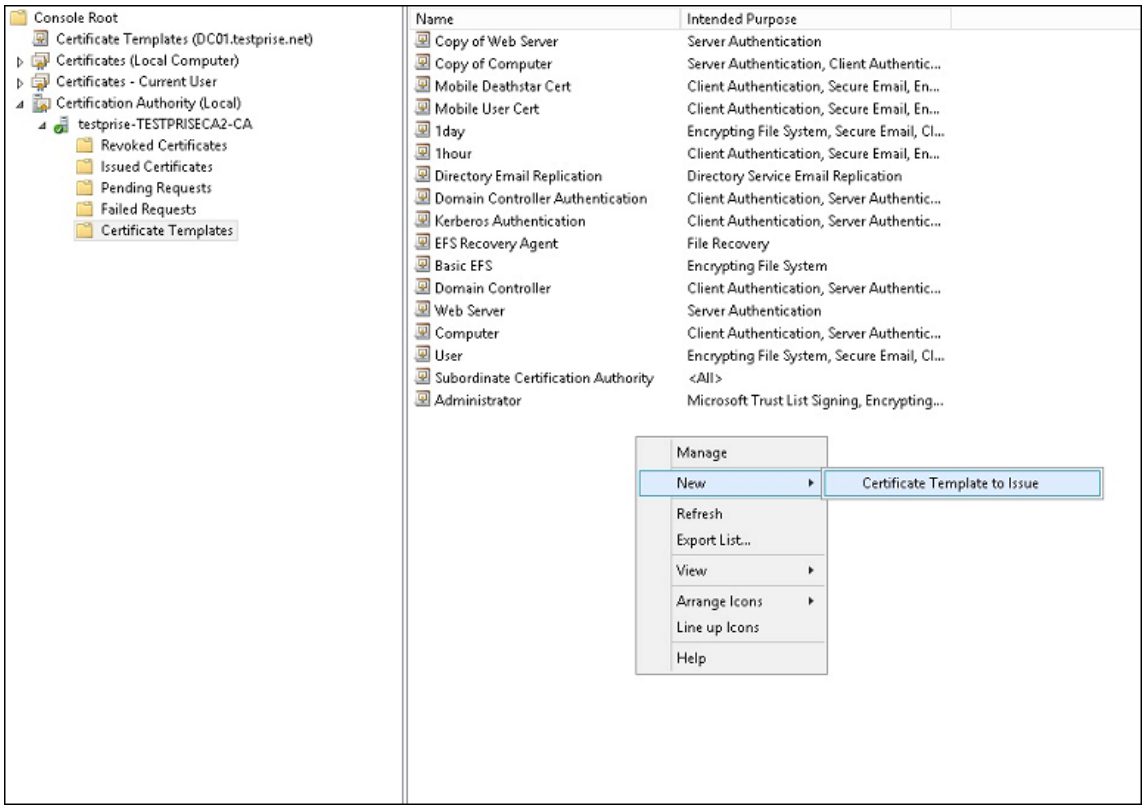


9. Wählen Sie unter **Antragstellername** die Option **Informationen werden in der Anforderung angegeben** aus. Wenden Sie die Änderungen an und speichern Sie.

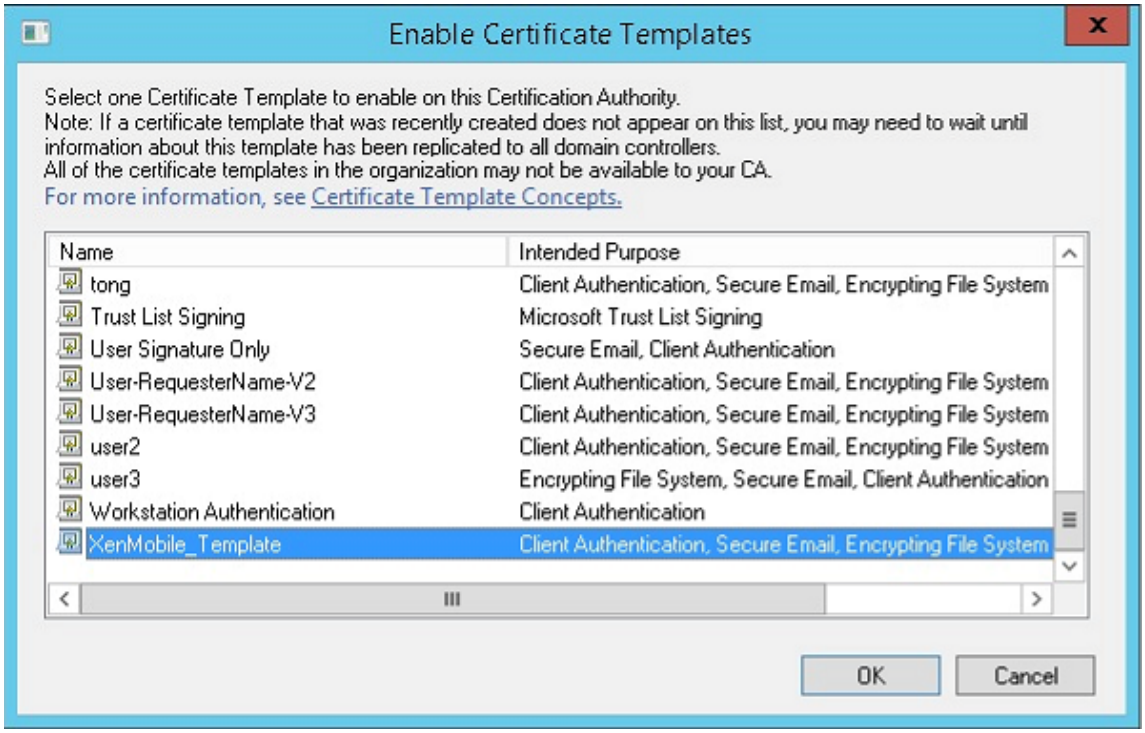


Hinzufügen der Vorlage zur Zertifizierungsstelle

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**.

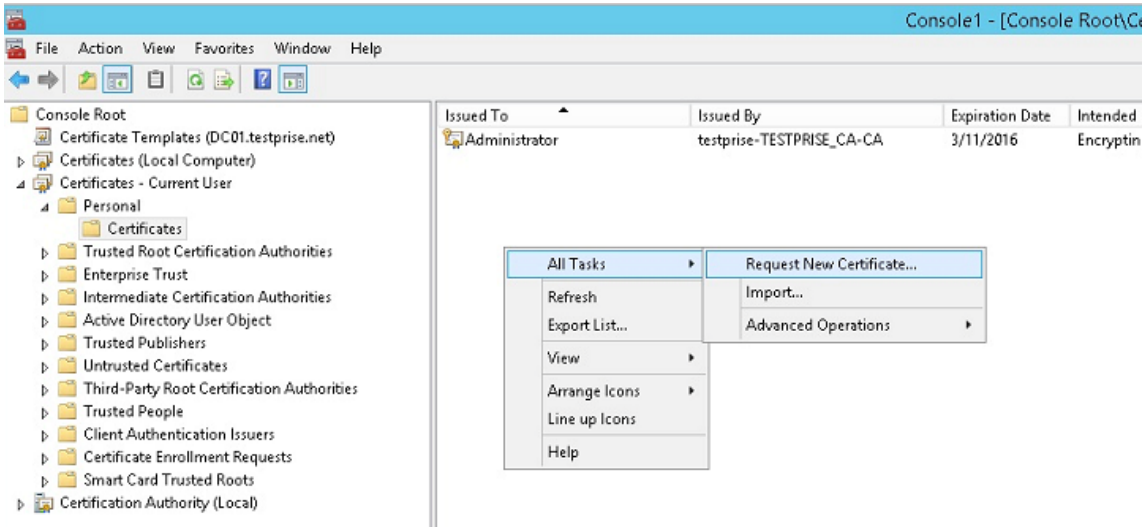


3. Wählen Sie die im vorherigen Schritt erstellte Vorlage und klicken Sie auf **OK**, um sie der **Zertifizierungsstelle** hinzuzufügen.

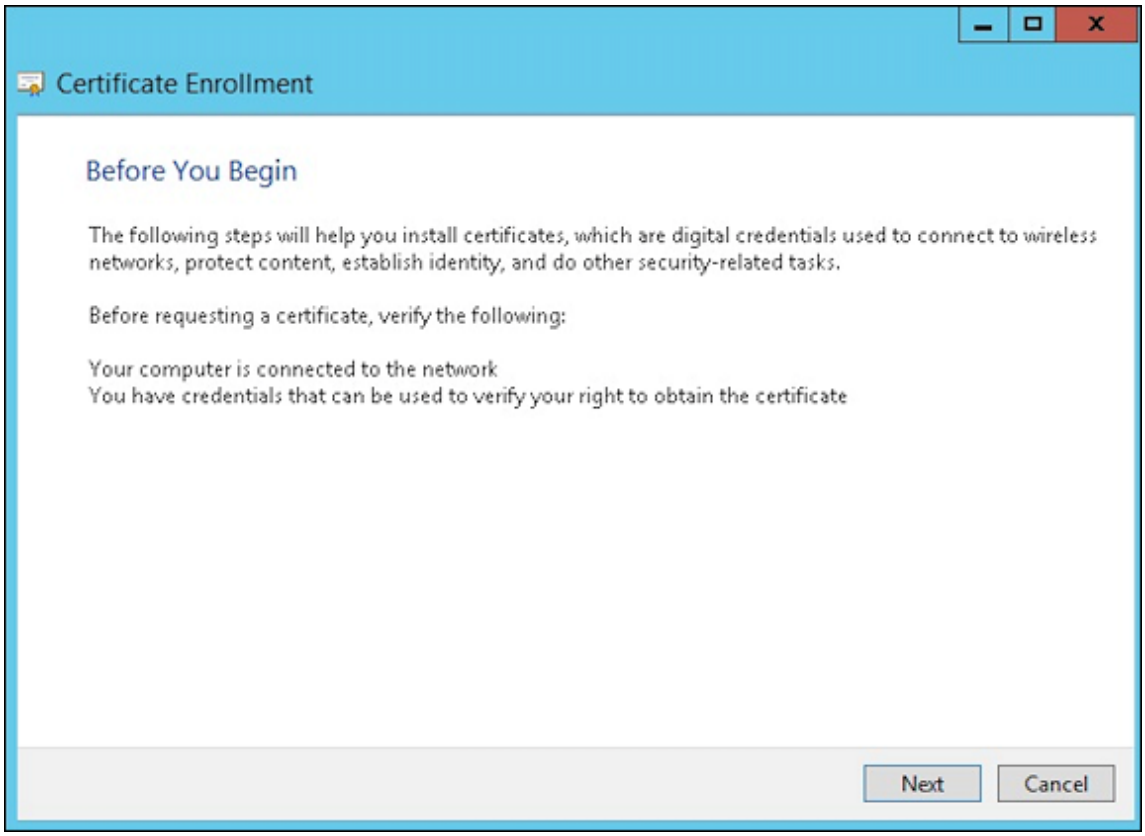


Erstellen eines PFX-Zertifikats vom ZS-Server

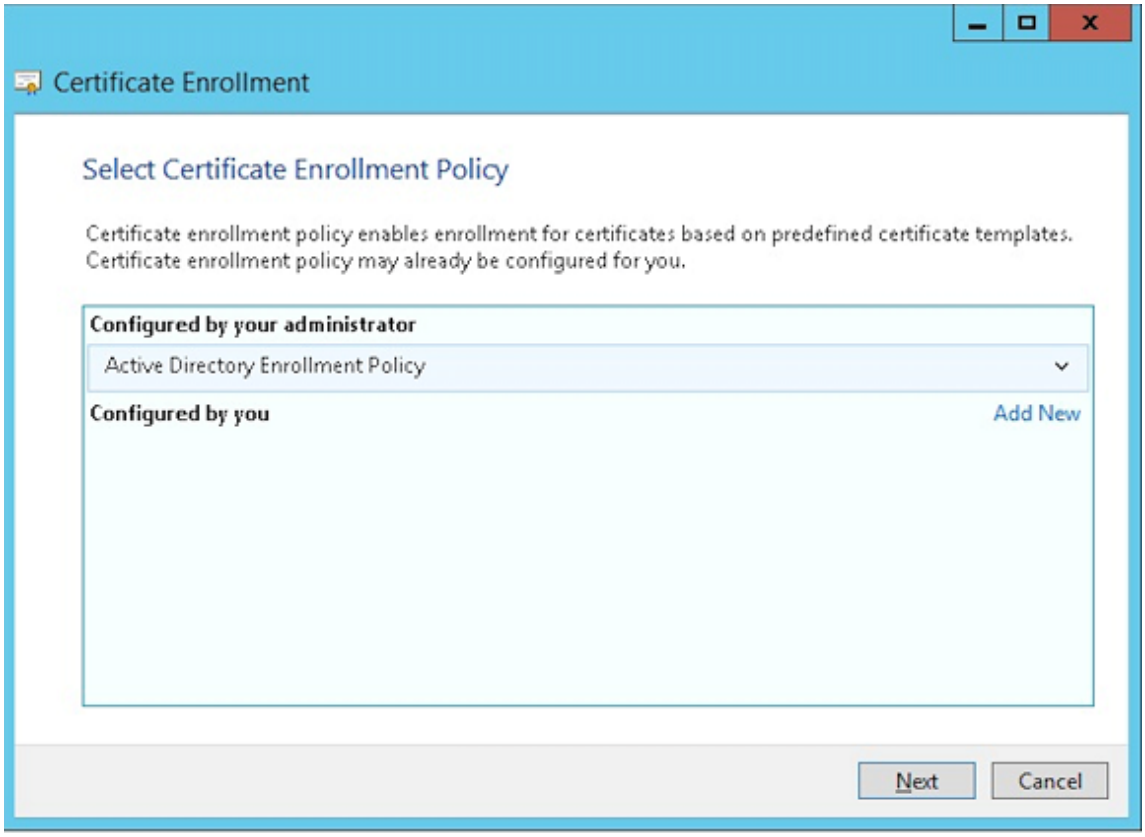
1. Erstellen Sie mit dem Dienstkonto, mit dem Sie sich angemeldet haben, ein PFX-Benutzerzertifikat. Diese PFX-Datei wird in Citrix Endpoint Management hochgeladen, um ein Benutzerzertifikat im Namen der Benutzer anzufordern, die ihre Geräte registrieren.
2. Erweitern Sie **Zertifikate** unter **Aktueller Benutzer**.
3. Klicken Sie mit der rechten Maustaste in den rechten Bereich und klicken Sie auf **Neues Zertifikat anfordern**.



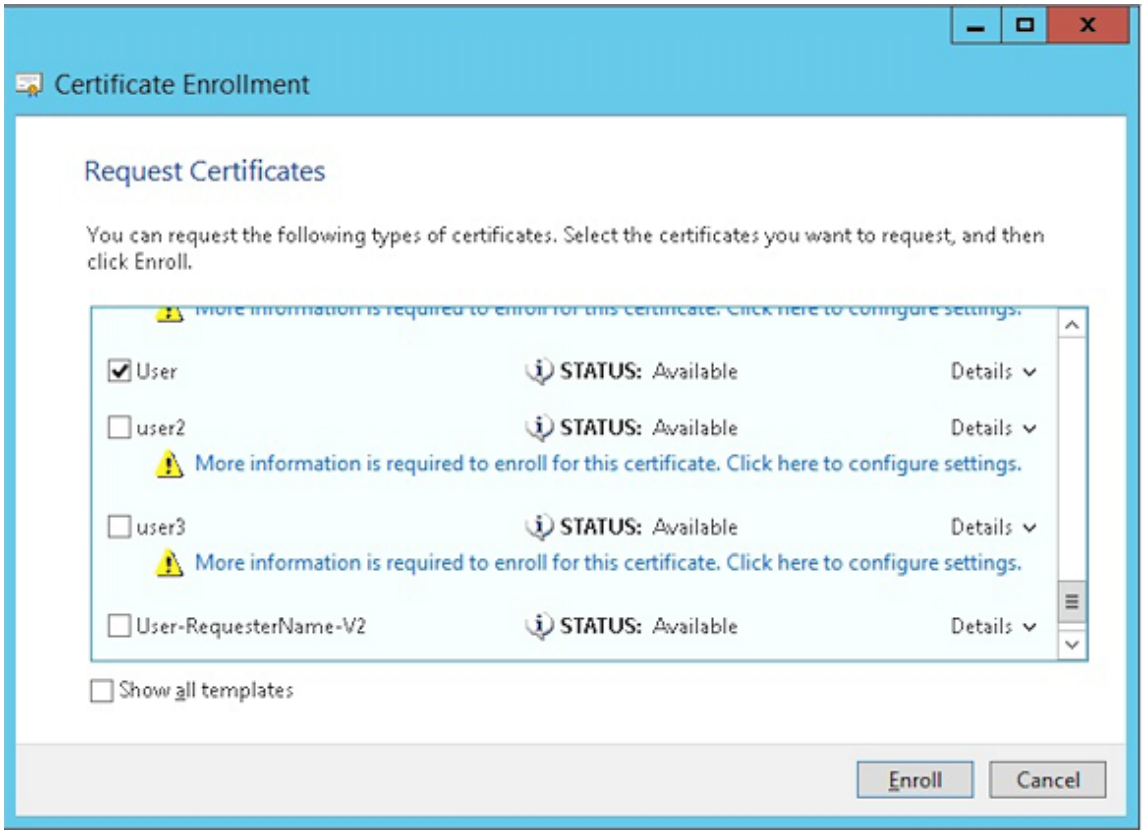
4. Der Bildschirm **Zertifikatregistrierung** wird angezeigt. Klicken Sie auf **Weiter**.



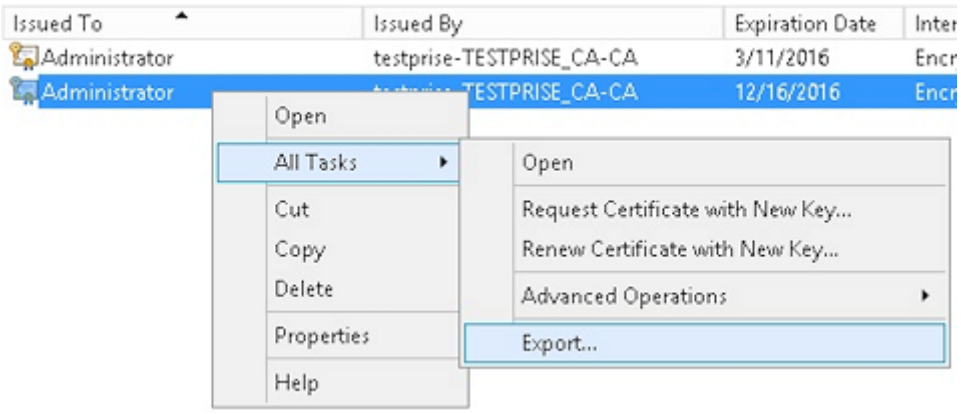
5. Wählen Sie **Active Directory-Registrierungsrichtlinie** und klicken Sie auf **Weiter**.



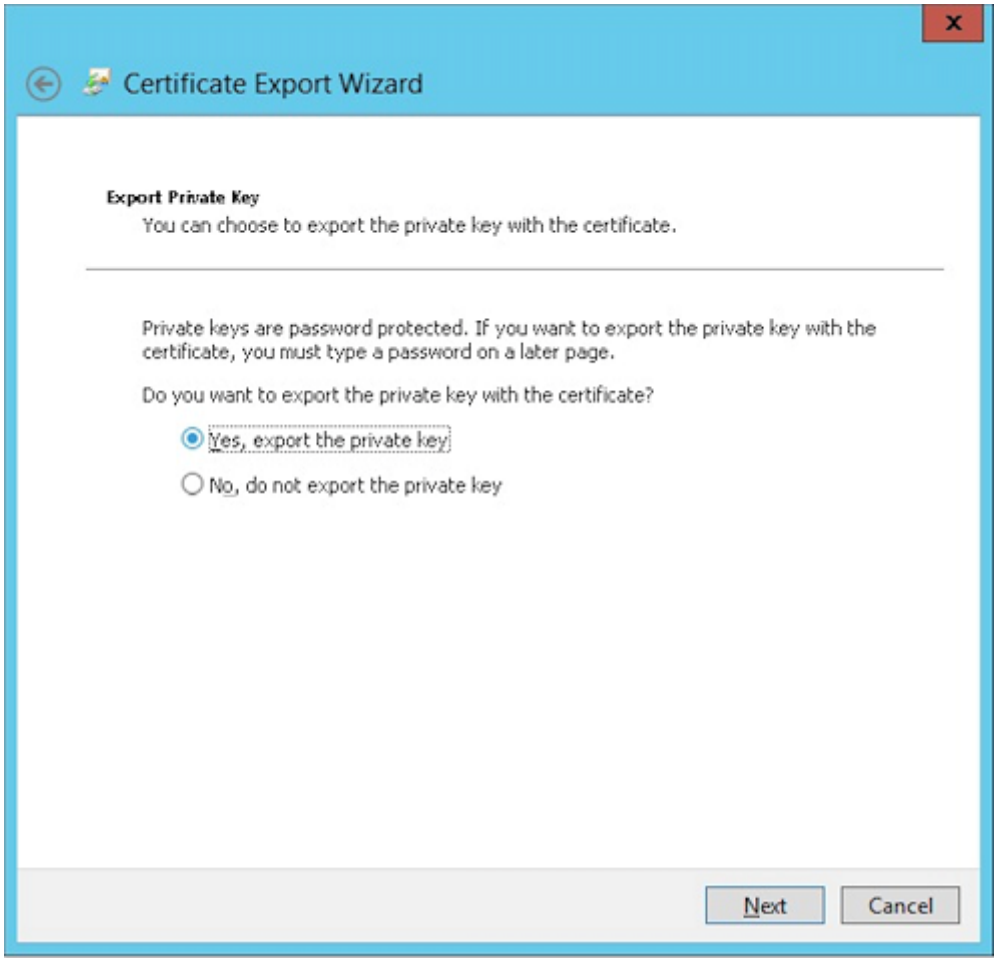
6. Wählen Sie die Vorlage **Benutzer** und klicken Sie auf **Registrieren**.



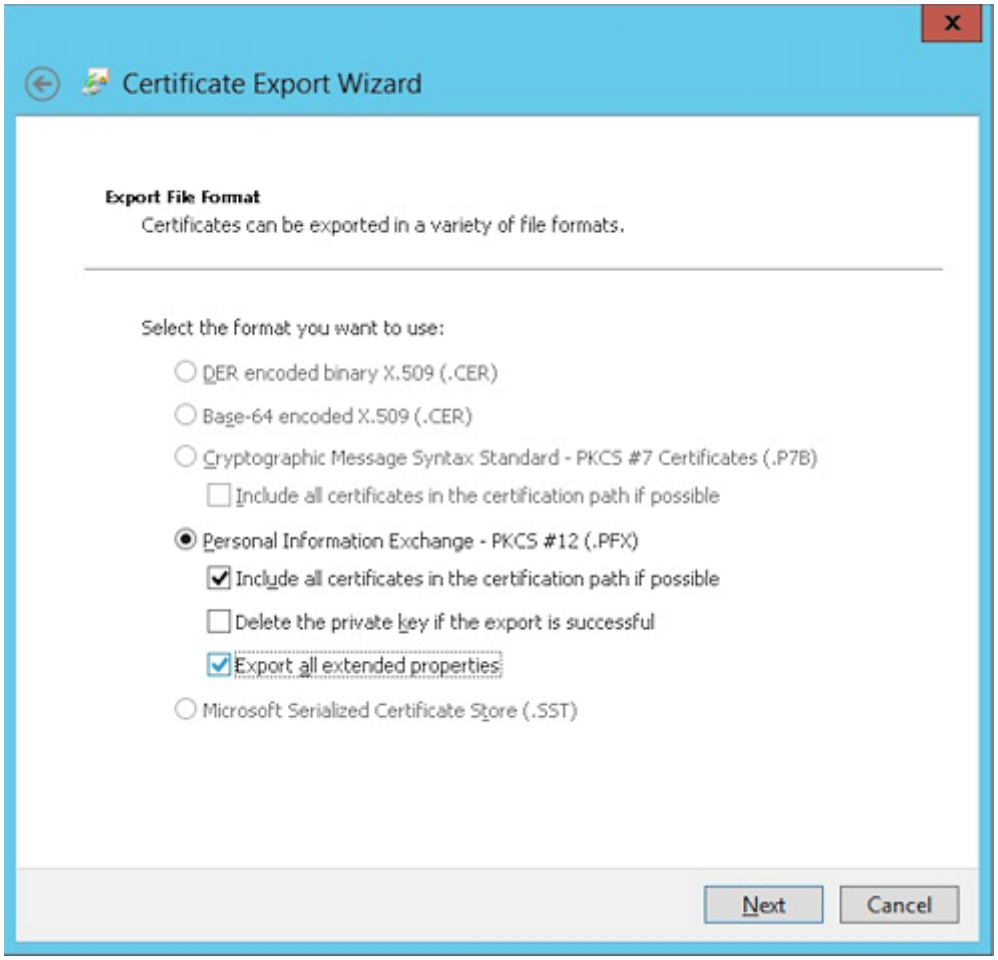
7. Exportieren Sie die PFX-Datei, die Sie im vorherigen Schritt erstellt haben.



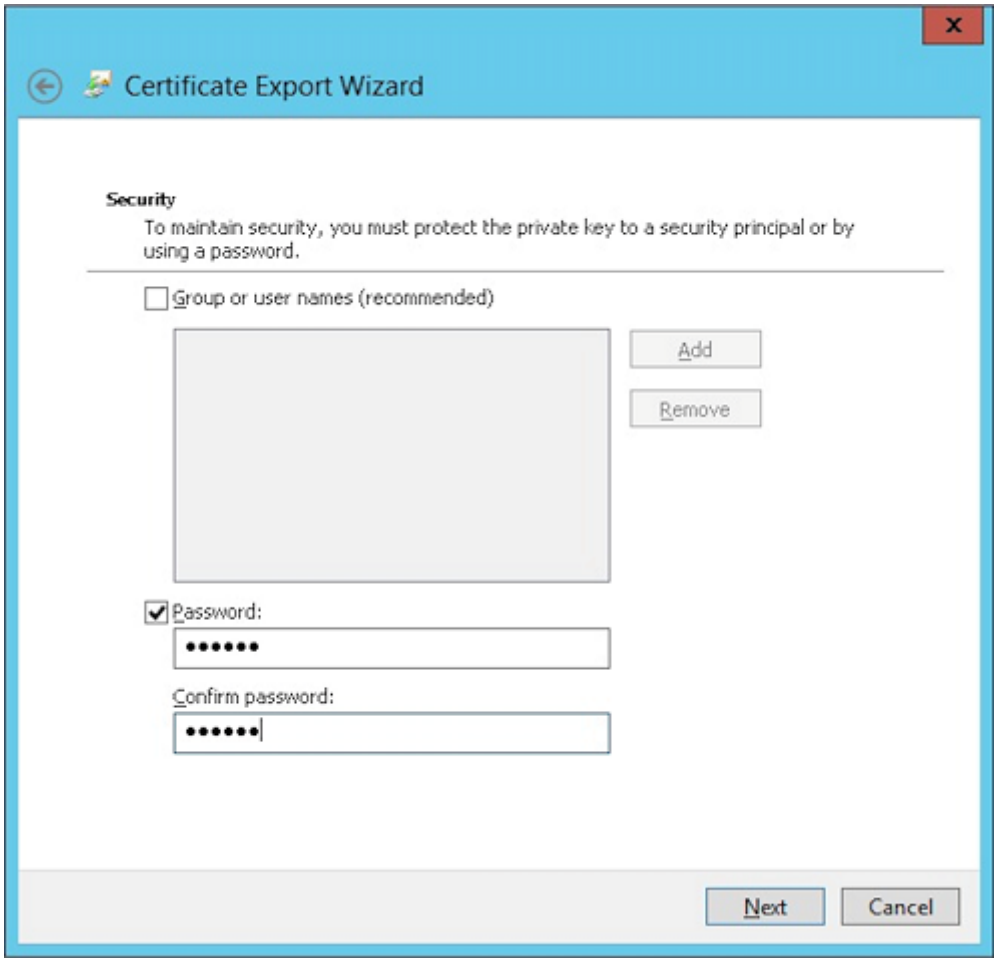
8. Klicken Sie auf **Ja, privaten Schlüssel exportieren**.



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



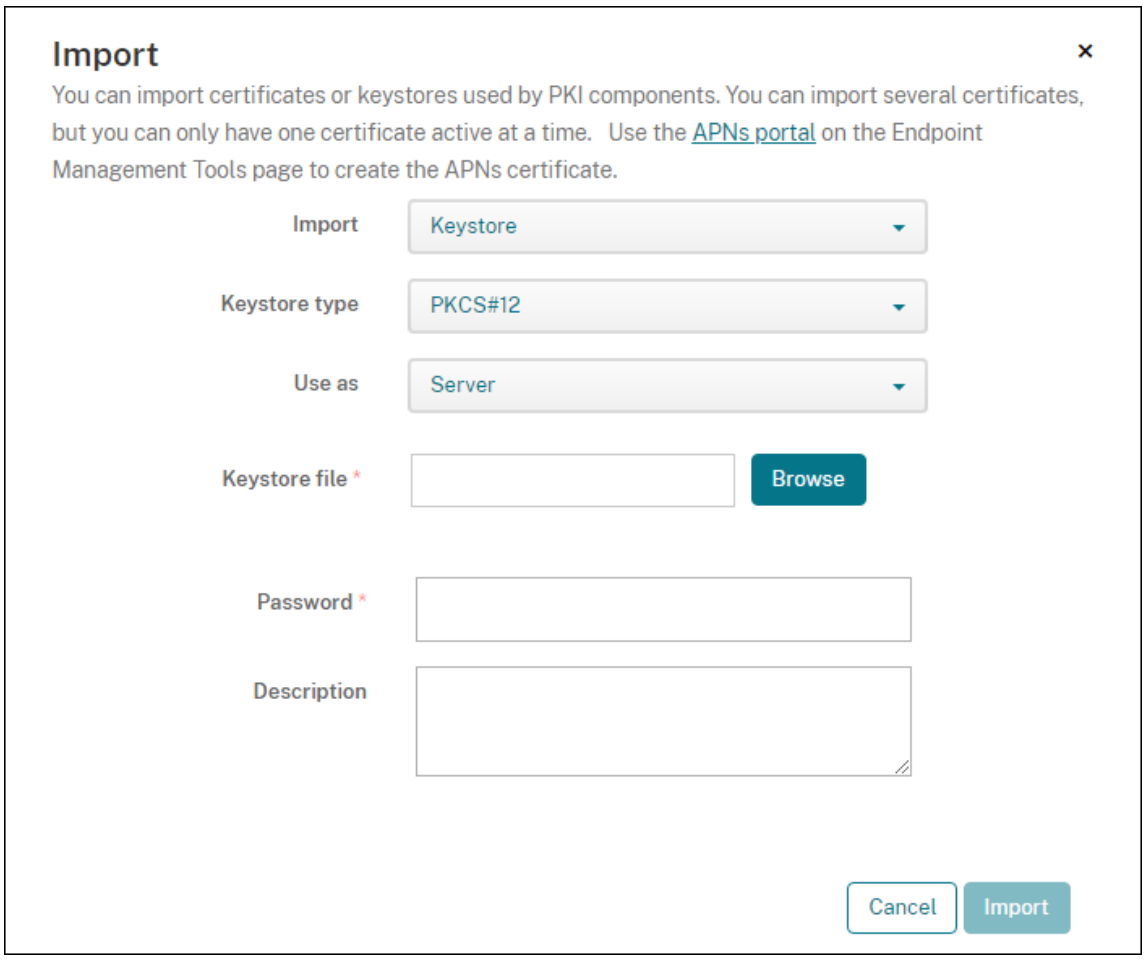
10. Legen Sie ein Kennwort für den Upload des Zertifikats in Citrix Endpoint Management fest.



11. Speichern Sie das Zertifikat auf Ihrer Festplatte.

Hochladen des Zertifikat in Citrix Endpoint Management

1. Klicken Sie in der Citrix Endpoint Management-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.

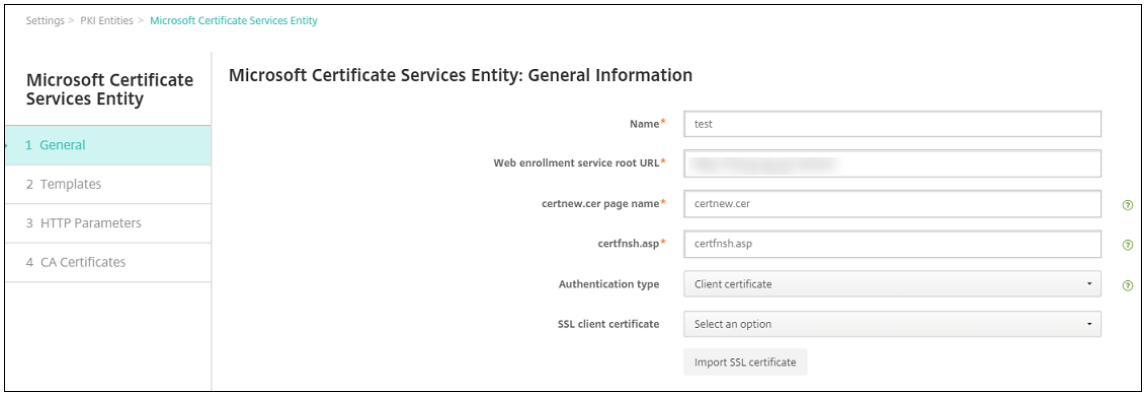


4. Klicken Sie auf **Importieren**.
5. Prüfen Sie, ob das Zertifikat richtig installiert wurde. Ein richtig installiertes Zertifikat wird als Benutzerzertifikat angezeigt.

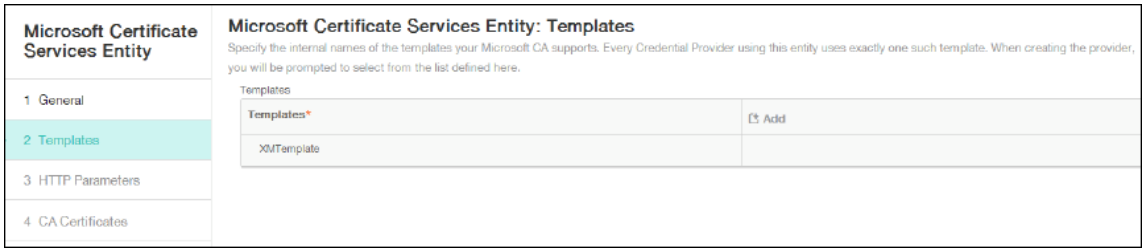
Erstellen der PKI-Entität für die zertifikatbasierte Authentifizierung

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)

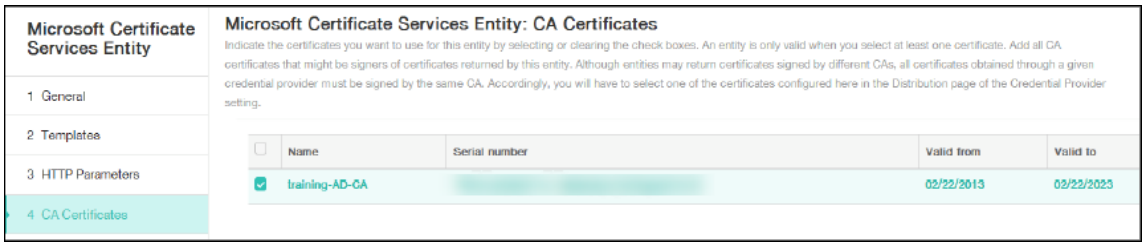
- **Authentifizierungstyp:** Clientzertifikat
- **SSL-Clientzertifikat:** Wählen Sie das Benutzerzertifikat aus, das zum Ausstellen des Citrix Endpoint Management-Clientzertifikats verwendet werden soll. Wenn kein Zertifikat vorhanden ist, folgen Sie dem Verfahren im vorherigen Abschnitt, um Zertifikate hochzuladen.



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 Citrix Endpoint Management-Clientzertifikat importiert wurde.



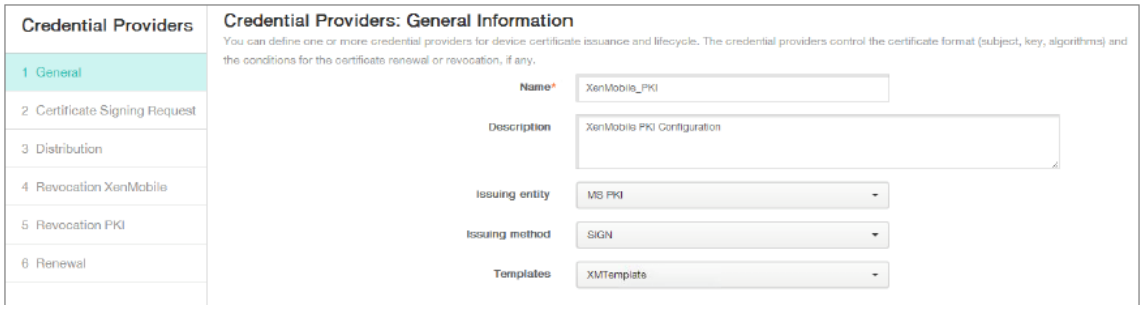
7. Klicken Sie auf **Speichern**.

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.

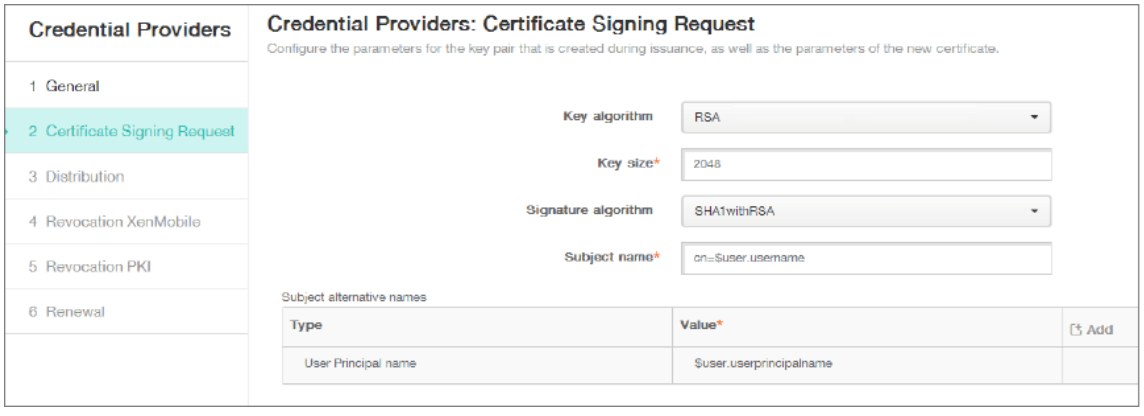


4. Klicken Sie auf **Zertifikatsignieranforderung** und geben Sie die folgenden Parameter ein:

    - **Schlüsselalgorithmus:** RSA
    - **Schlüsselgröße:** 2048
    - **Signaturalgorithmus:** SHA256withRSA
    - **Antragsstellername:** `cn=$user.username`

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

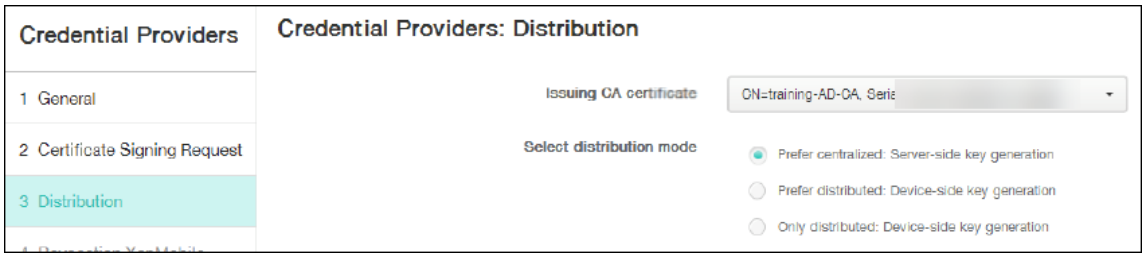
    - **Typ:** Benutzerprinzipalname
    - **Wert:** `$user.userprincipalname`



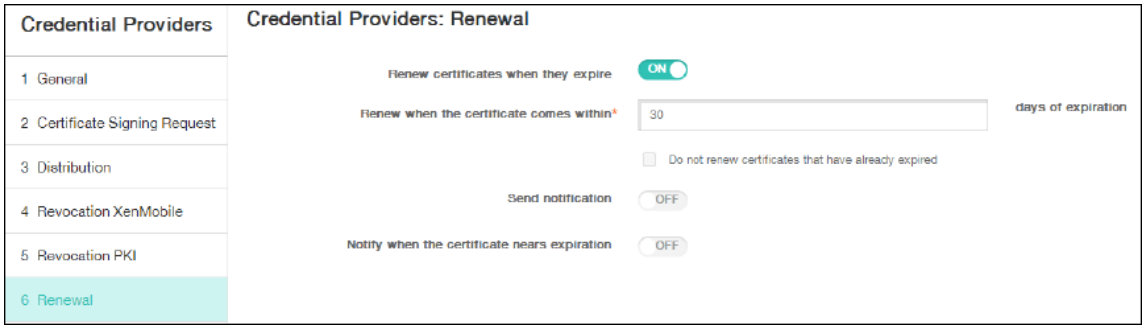
5. Klicken Sie auf **Verteilung** und geben Sie die folgenden Parameter ein:

    - **Zertifikat der ausstellenden ZS:** Wählen Sie die ausstellende Zertifizierungsstelle, die das Citrix Endpoint Management-Clientzertifikat signiert hat.

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



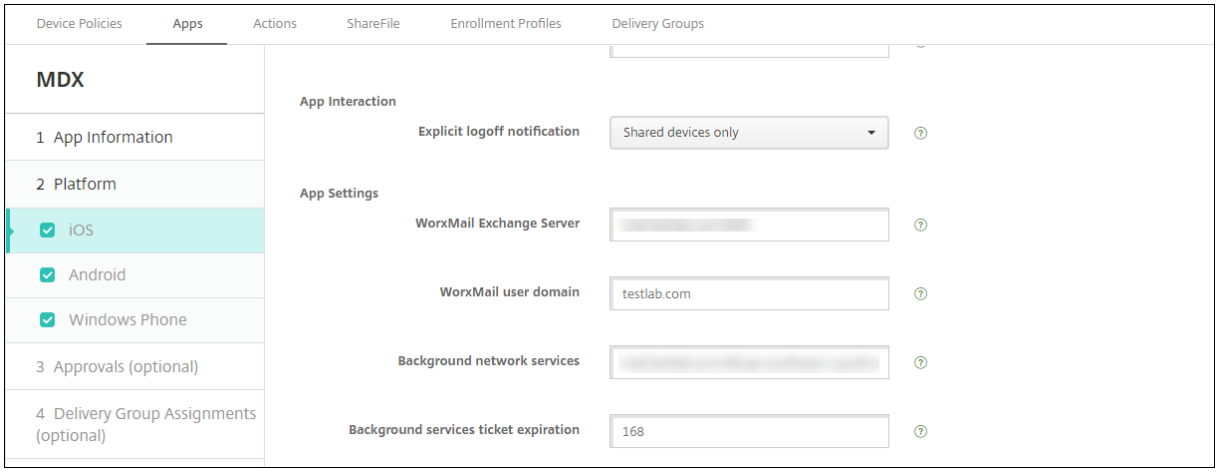
6. Legen Sie für die zwei folgenden Abschnitte **Citrix Endpoint Management-Sperrung** und **PKI-Sperrung** die Parameter nach Bedarf fest. In diesem Beispiel werden beide Optionen übersprungen.
7. Klicken Sie auf **Verlängerung**.
8. Aktivieren Sie **Zertifikate erneuern, wenn sie ablaufen**.
9. Behalten Sie für alle anderen Einstellungen die Standardwerte bei oder ändern Sie sie nach Bedarf.



10. Klicken Sie auf **Speichern**.

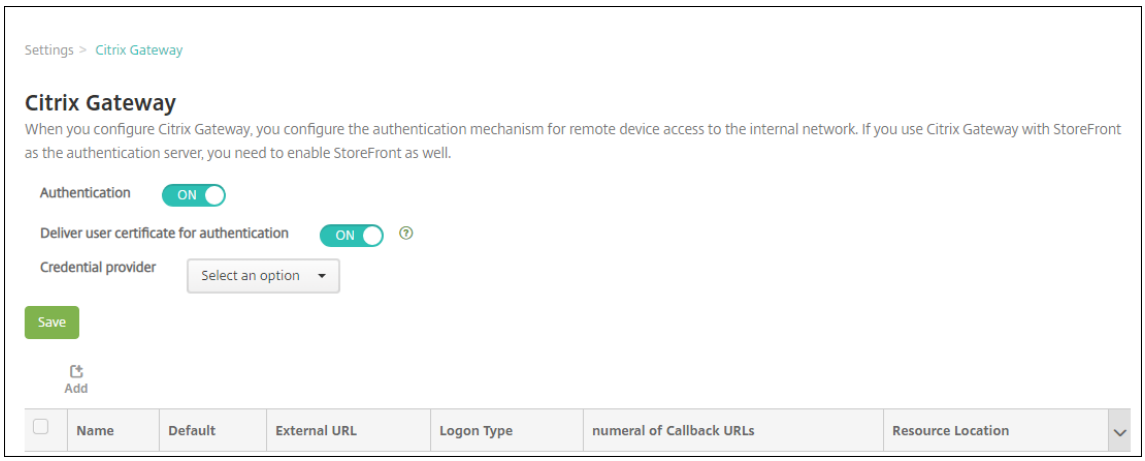
Konfigurieren von Citrix Secure Mail für die zertifikatbasierte Authentifizierung

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

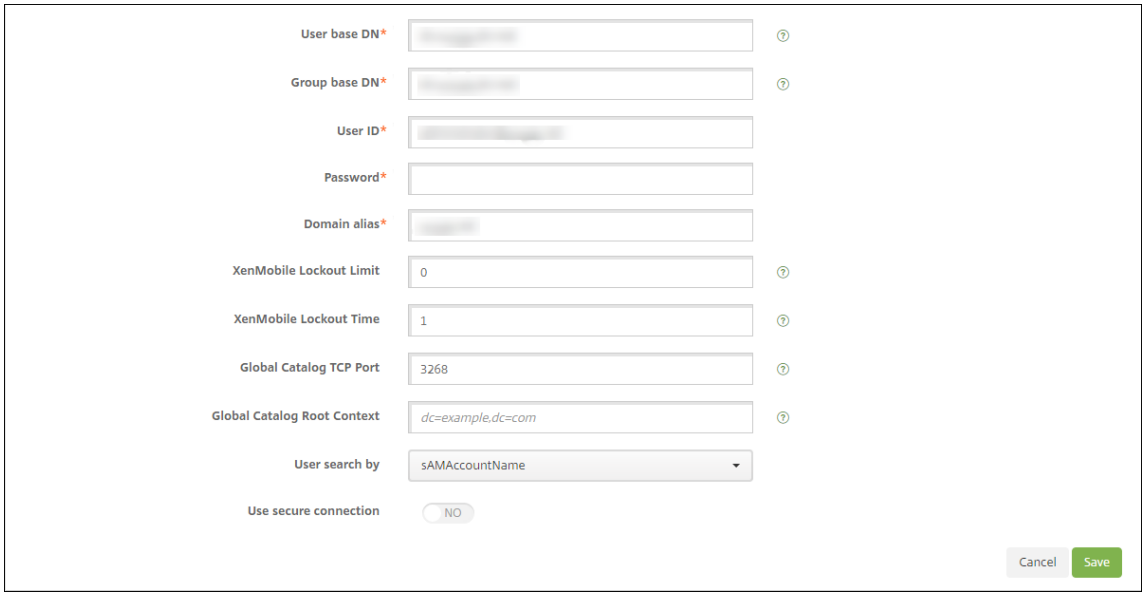


Konfigurieren der NetScaler Gateway-Zertifikatbereitstellung in Citrix Endpoint Management

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Server** auf **NetScaler Gateway**.
3. Wenn NetScaler Gateway noch nicht hinzugefügt wurde, klicken Sie auf **Hinzufügen** und legen Sie folgende Einstellungen fest:
   - **Name:** Ein aussagekräftiger Namen für die Appliance.
   - **Alias:** Ein optionaler Alias für die Appliance.
   - **Externe URL:** `https://YourCitrixGatewayURL`
   - **Anmeldetyp:** Wählen Sie **Zertifikat und Domäne**.
   - **Kennwort erforderlich:** Aus
   - **Als Standard festlegen:** Ein
4. Wählen Sie für **Authentifizierung** und **Benutzerzertifikat für Authentifizierung bereitstellen** die Einstellung **Ein**.



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 Citrix Endpoint Management 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.

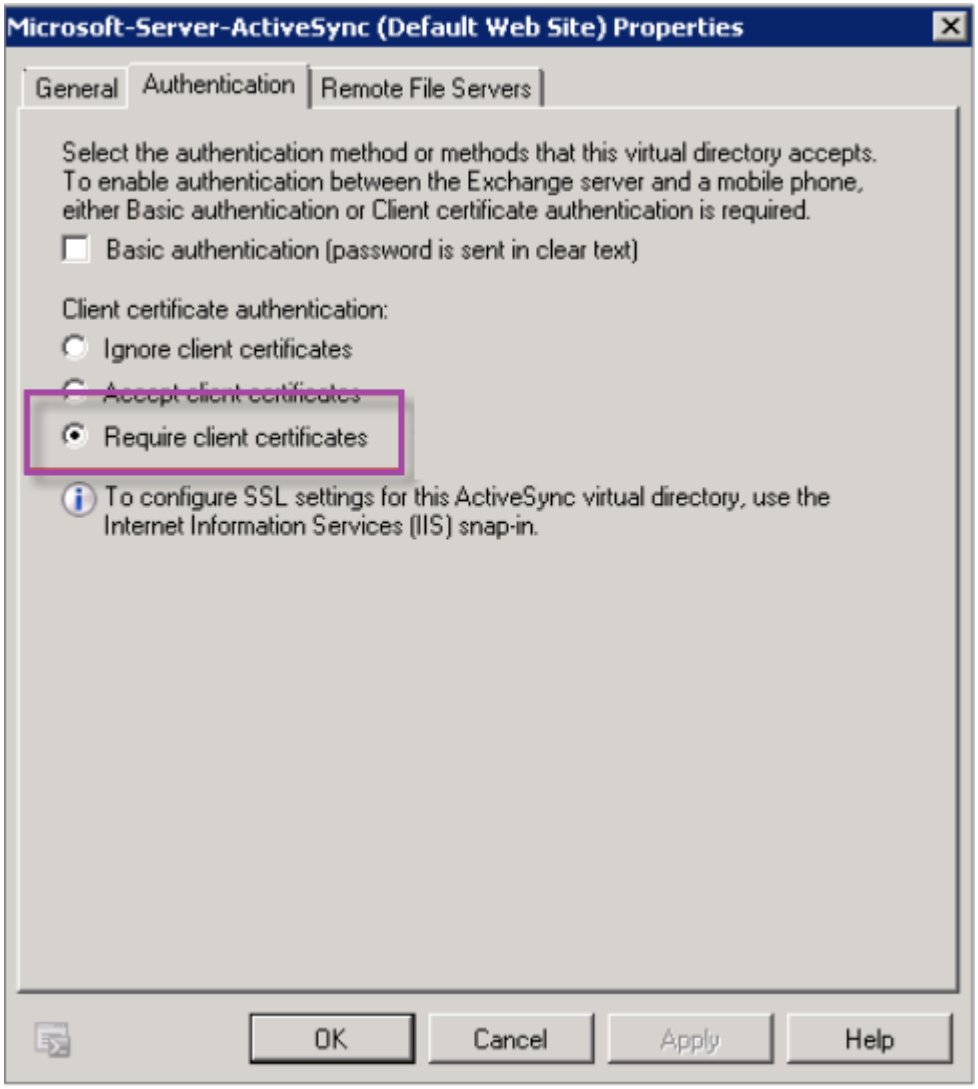
Problembehandlung bei der Clientzertifikatkonfiguration

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

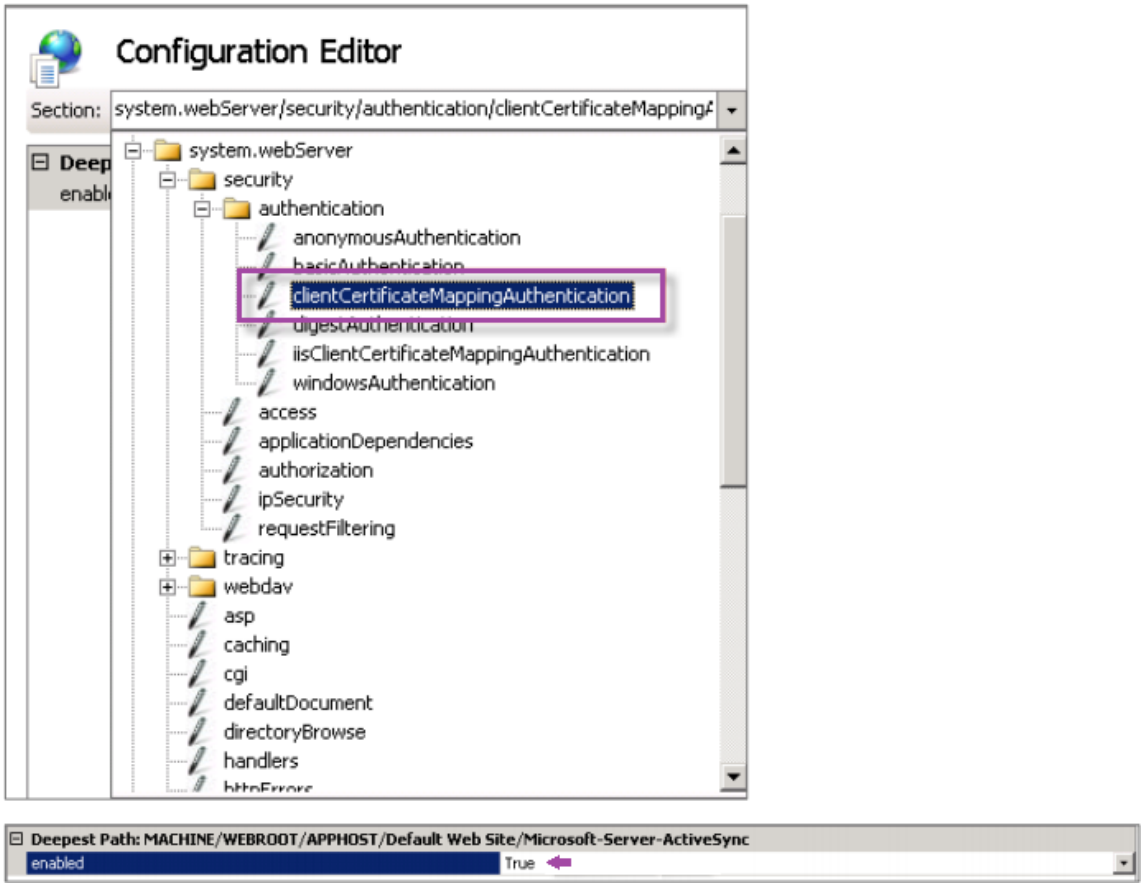
1. Der Benutzer registriert sein mobiles Gerät.
2. Citrix Endpoint Management fordert den Benutzer auf, eine Citrix-PIN zu erstellen.
3. Der Benutzer wird an den App-Store weitergeleitet.
4. Wenn Benutzer Citrix Secure Mail starten, fordert Citrix Endpoint Management sie nicht auf, die Benutzeranmeldeinformationen einzugeben, um das Postfach zu konfigurieren. Stattdessen fordert Citrix Secure Mail das Clientzertifikat aus Citrix Secure Hub an und sendet es zur Authentifizierung an Microsoft Exchange Server. Wenn Citrix Endpoint Management beim Starten von Citrix Secure Mail durch die Benutzer die Eingabe von Anmeldeinformationen anfordert, prüfen Sie die Konfiguration.

Wenn die Benutzer Citrix 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 NetScaler Gateway-Einstellungen in der Citrix Endpoint Management-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 Citrix Endpoint Management-Konsole zu **Verwalten > Geräte** und wählen Sie das Gerät.
2. Klicken Sie auf **Bearbeiten** oder **Mehr anzeigen**.
3. Navigieren Sie zum Bereich **Bereitstellungsgruppen** und suchen Sie folgenden Eintrag:

   NetScaler Gateway-Anmeldeinformationen: Requested credential, CertId=

Überprüfen, ob die Clientzertifikataushandlung aktiviert wurde

1. Führen Sie 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=23498dfsdfhaf98rhkjqf98
    appid={ 123asd456jd-a12b-3c45-d678-123456lkjhgf } certstorename=
   ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWit
   =Disable UsageCheck=Enable clientcertnegotiation=Enable
   ```

Wenn Sie über Citrix Endpoint Management 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 Citrix Secure Mail nicht unter Windows Phone 8.1 installiert werden kann, überprüfen Sie Folgendes:

- Der Anwendungsregistrierungstoken (.AETX) wird mit Citrix Endpoint Management über die Unternehmenshubrichtlinie bereitgestellt.
- Der Anwendungsregistrierungstoken wurde mit dem gleichen Enterprise-Zertifikat des Zertifikatanbieters erstellt, das zum Umschließen und zum Signieren von den Apps Citrix Secure Mail und Citrix Secure Hub verwendet wird.
- Zum Signieren und Umschließen von Citrix Secure Hub, Citrix Secure Mail und Anwendungsregistrierungstoken wird die gleiche Aussteller-ID verwendet.

PKI-Entitäten

June 25, 2024

Eine Citrix Endpoint Management-PKI-Entität ist eine Komponente, die PKI-Vorgänge (Ausstellung, Sperrung und Statusinformationen) durchführt. Dies sind interne oder externe Komponenten von Citrix Endpoint Management. Interne Komponenten werden als eigenverwaltet bezeichnet. Externe Komponenten sind Teil Ihrer Unternehmensinfrastruktur.

Citrix Endpoint Management unterstützt folgende Arten von PKI-Entitäten:

- Microsoft Zertifikatdienste
- Eigenverwaltete CAs

Citrix Endpoint Management unterstützt die folgenden Zertifizierungsstellenserver:

- Windows Server 2016
- Windows Server 2019

> **Hinweis:**
>
> Windows Server 2012 R2, 2012 und 2008 R2 werden nicht mehr unterstützt, da sie das Ende des Lebenszyklus erreicht haben. Weitere Informationen finden Sie in der Dokumentation zum Lebenszyklus von Microsoft-Produkten.

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 Citrix Endpoint Management 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 Citrix Endpoint Management 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: `! : $ ( )# % + * ~ ? | { } [ ]`

Microsoft Zertifikatdienste

Citrix Endpoint Management interagiert mit Microsoft Zertifikatdiensten über seine Schnittstelle zur Webregistrierung. Citrix Endpoint Management unterstützt nur das Ausstellen neuer Zertifikate über diese Schnittstelle. Wenn die Microsoft-ZS ein NetScaler Gateway-Benutzerzertifikat erstellt, unterstützt NetScaler Gateway Verlängerung und Sperrung für diese Zertifikate.

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

Hinzufügen einer Microsoft-Zertifikatdiensteentität

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben und dann auf **PKI-Entitäten**.
2. Klicken Sie auf der Seite **PKI-Entitäten** auf **Hinzufügen**.

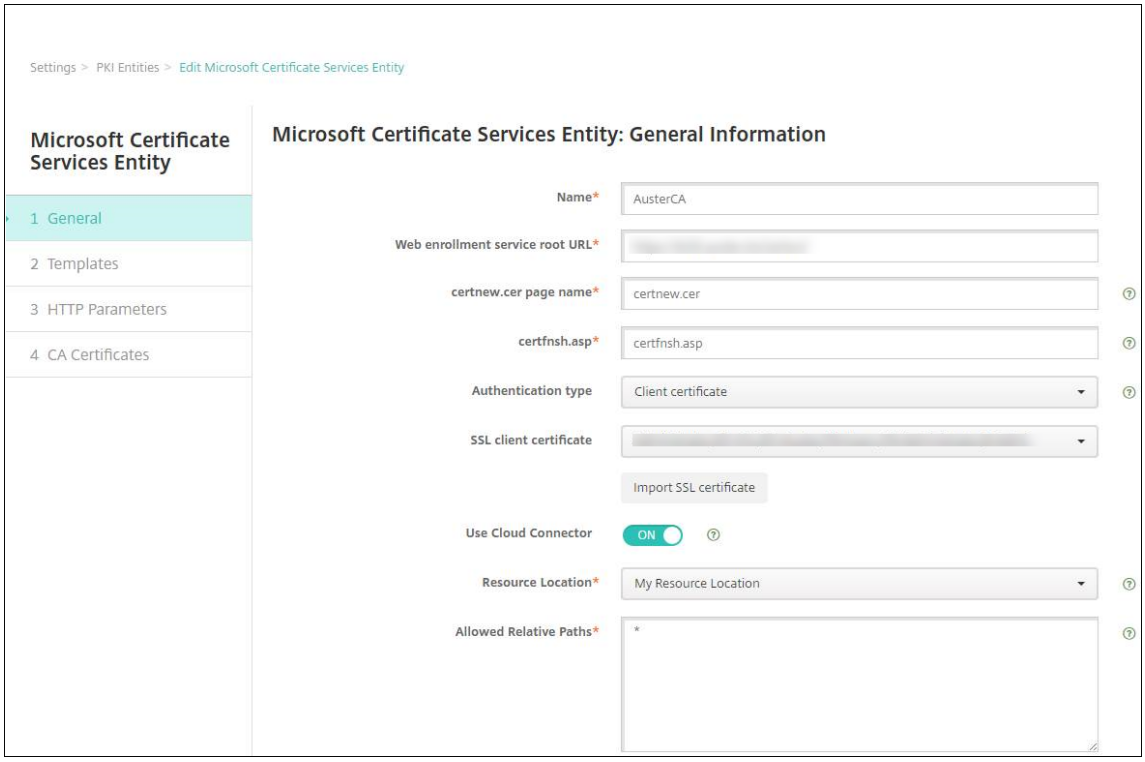
   Ein Menü der PKI-Entitätstypen wird angezeigt.
3. Klicken Sie auf **Microsoft Zertifikatdiensteentität**.

   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://192.0.0.1/certsrv/`. Die URL kann 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.
- **Cloud Connector verwenden:** Wählen Sie **Ein**, um Cloud Connector für Verbindungen mit dem PKI-Server zu verwenden. Geben Sie dann einen **Ressourcenstandort** und **Zulässige relative Pfade** für die Verbindung an.
  - **Ressourcenstandort:** Treffen Sie Ihre Auswahl unter den unter Citrix Cloud Connector definierten Ressourcenstandorten.
  - **Zulässige relative Pfade:** die relativen Pfade, die für den angegebenen Ressourcenstandort zulässig sind. Geben Sie einen Pfad pro Zeile an. Sie können das Sternchen (*) als Platzhalter verwenden.

    Angenommen, der Ressourcenstandort ist `https://www.ServiceRoot/certsrv`. Um Zugriff auf alle URLs in diesem Pfad zu gewähren, geben Sie `/*` in **Zulässige relative Pfade** ein.



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 die Microsoft Zertifikatdienste-Vorlage finden Sie in der Microsoft-Dokumentation zu Ihrer Windows Server-Version. In Citrix Endpoint Management gelten außer den unter Zertifikate aufgeführten Regeln für Zertifikatformate keine weiteren Anforderungen für die von Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management die Signierer der Zertifikate angeben, die das System über diese Entität erhält. Wenn das ZS-Zertifikat erneuert wurde, aktualisieren Sie es in Citrix Endpoint Management. Citrix Endpoint Management 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.

NetScaler Gateway-Zertifikatsperrliste

Citrix Endpoint Management unterstützt Zertifikatsperrlisten (CRL) nur für Drittanbieterzertifizierungsstellen. Wenn Sie eine Microsoft-Zertifizierungsstelle konfiguriert haben, wird in Citrix

Endpoint Management zum Verwalten der Zertifikatsperre NetScaler Gateway verwendet.

Bedenken Sie beim Konfigurieren der Clientzertifikatauthentifizierung, ob Sie die NetScaler Gateway-Einstellung für Zertifikatsperrlisten (CRL) **Enable CRL Auto Refresh** konfigurieren müssen. Dadurch wird sichergestellt, dass Benutzer von Geräten im ausschließlichen MAM-Modus keine Authentifizierung mit einem existierenden Zertifikat am Gerät durchführen können.

Citrix Endpoint Management 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 Citrix Endpoint Management ein Zertifizierungsstellenzertifikat mit zugehörigem privatem Schlüssel angeben. Citrix Endpoint Management 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. Nur wenn die OCSP-Unterstützung aktiviert wird, fügt die Zertifizierungsstelle den von ihr ausgestellten Zertifikaten die Erweiterung `id-pe-authorityInfoAccess` hinzu. Die Erweiterung verweist auf die Citrix Endpoint Management-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`.

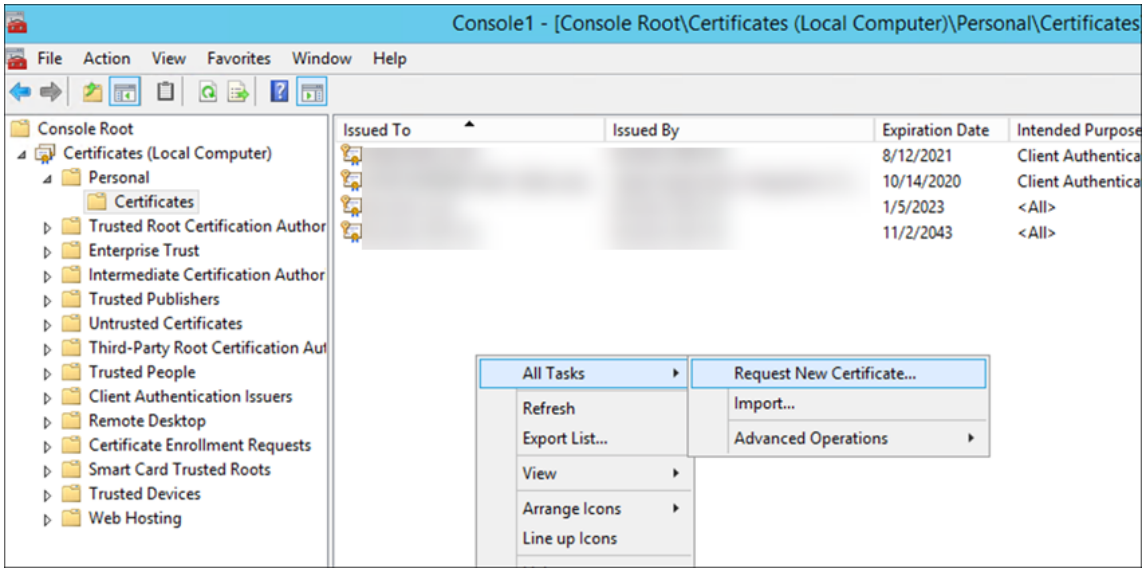
Der OCSP-Responder-Dienst von Citrix Endpoint Management unterstützt einfache OCSP-Antworten und folgende Hashalgorithmen in Anforderungen:

- SHA-256
- SHA-384
- SHA-512

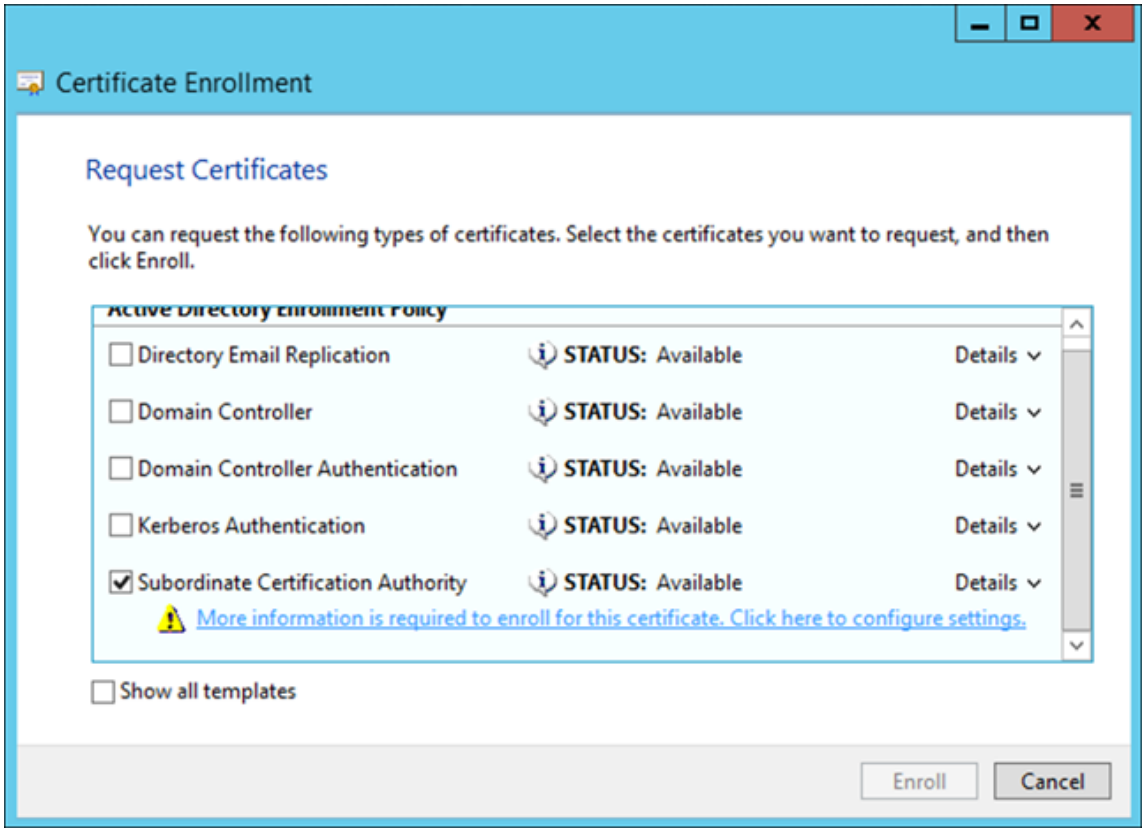
Antworten werden mit SHA-256 und dem Signaturzertifikat-Schlüsselalgorithmus (DSA, RSA oder ECDSA) signiert.

Generieren und Importieren eines Zertifikats für Ihre Zertifizierungsstelle

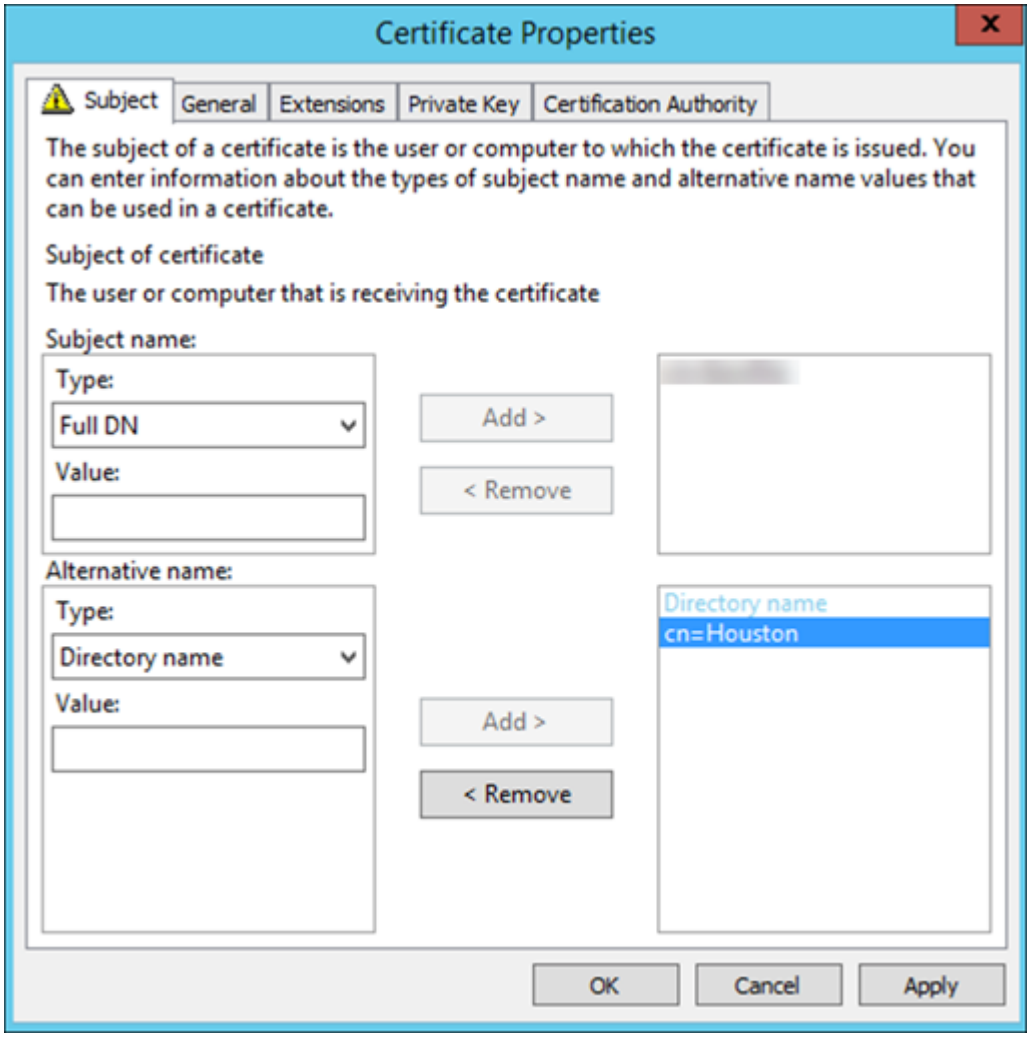
1. Öffnen Sie auf Ihrem Server Microsoft Management Console (MMC) mit dem lokalen Systemkonto und öffnen Sie das Snap-In "Zertifikate". Klicken Sie mit der rechten Maustaste in den rechten Bereich und dann auf **Alle Aufgaben > Neues Zertifikat anfordern**.



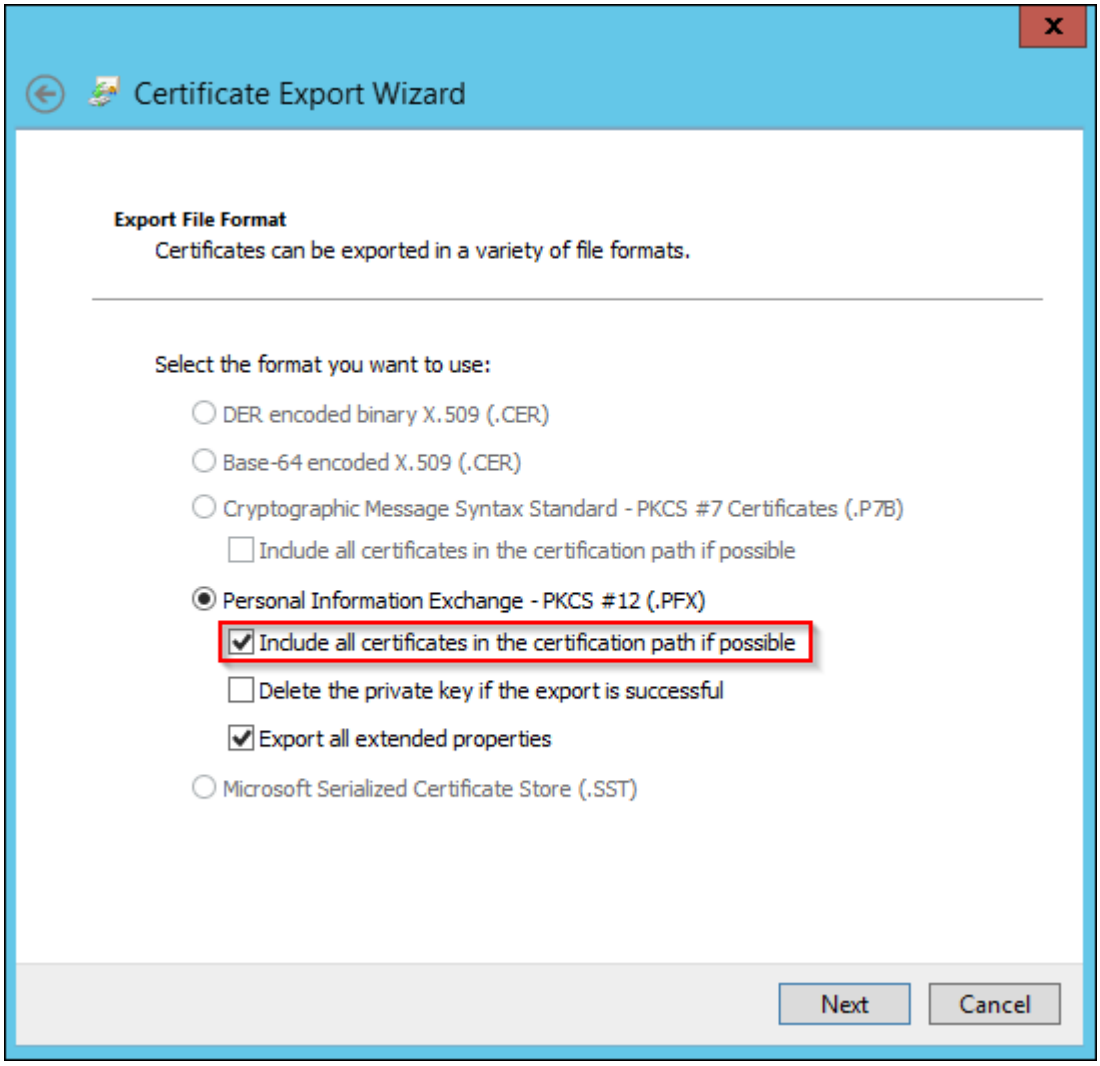
2. Klicken Sie in dem nun geöffneten Assistenten zweimal auf **Weiter**. Wählen Sie in der Liste **Zertifikate anfordern** die Option **Untergeordnete Zertifizierungsstelle** und klicken Sie auf den Link **Weitere Informationen**.



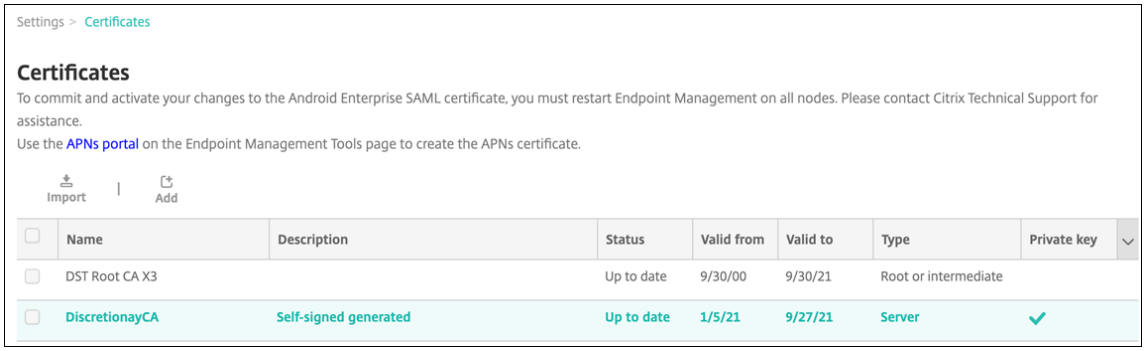
3. Geben Sie einen **Antragstellernamen** und einen **Alternativen Namen** ein. Klicken Sie auf **OK**.



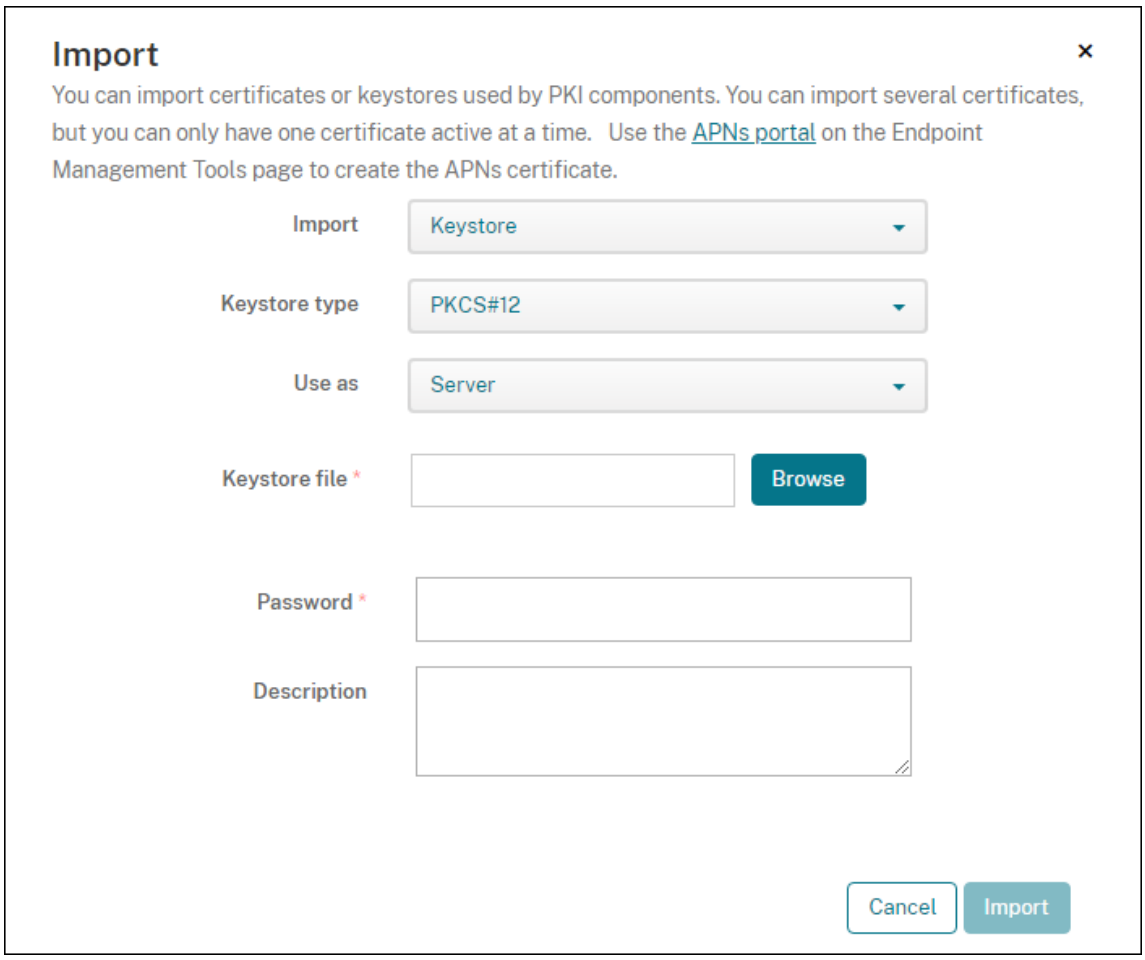
4. Klicken Sie auf **Registrieren**und dann auf **Fertig stellen**.
5. Klicken Sie in MMC mit der rechten Maustaste auf das von Ihnen erstellte Zertifikat. Klicken Sie auf **Alle Aufgaben > Exportieren**. Exportieren Sie das Zertifikat als PFX-Datei mit einem privaten Schlüssel. Wählen Sie die Option **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen**.



6. Gehen Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Zertifikate**.



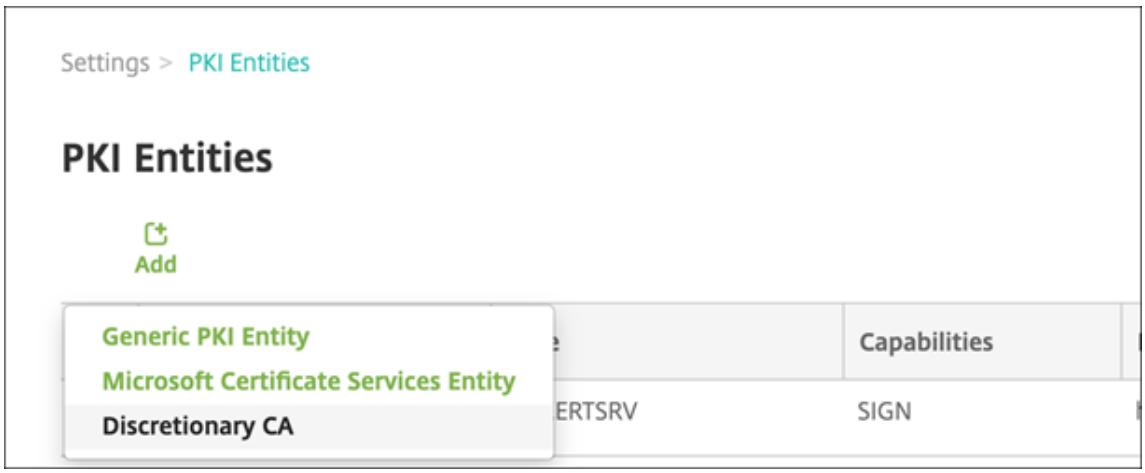
7. Klicken Sie auf **Importieren**. Suchen Sie in dem nun geöffneten Fenster die Dateien für das Zertifikat und den privaten Schlüssel, die Sie zuvor exportiert haben.



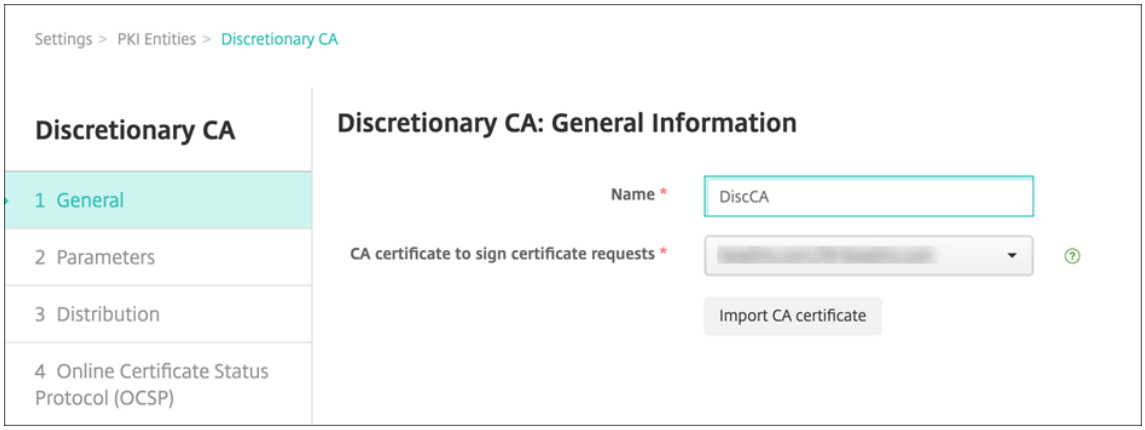
8. Klicken Sie auf **Importieren**. Das Zertifikat wird der Tabelle hinzugefügt.

Hinzufügen von eigenverwalteten Zertifizierungsstellen

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben und dann auf **Mehr > PKI-Entitäten**.
2. Klicken Sie auf der Seite **PKI-Entitäten** auf **Hinzufügen**.



3. Klicken Sie auf **Eigenverwaltete ZS**.

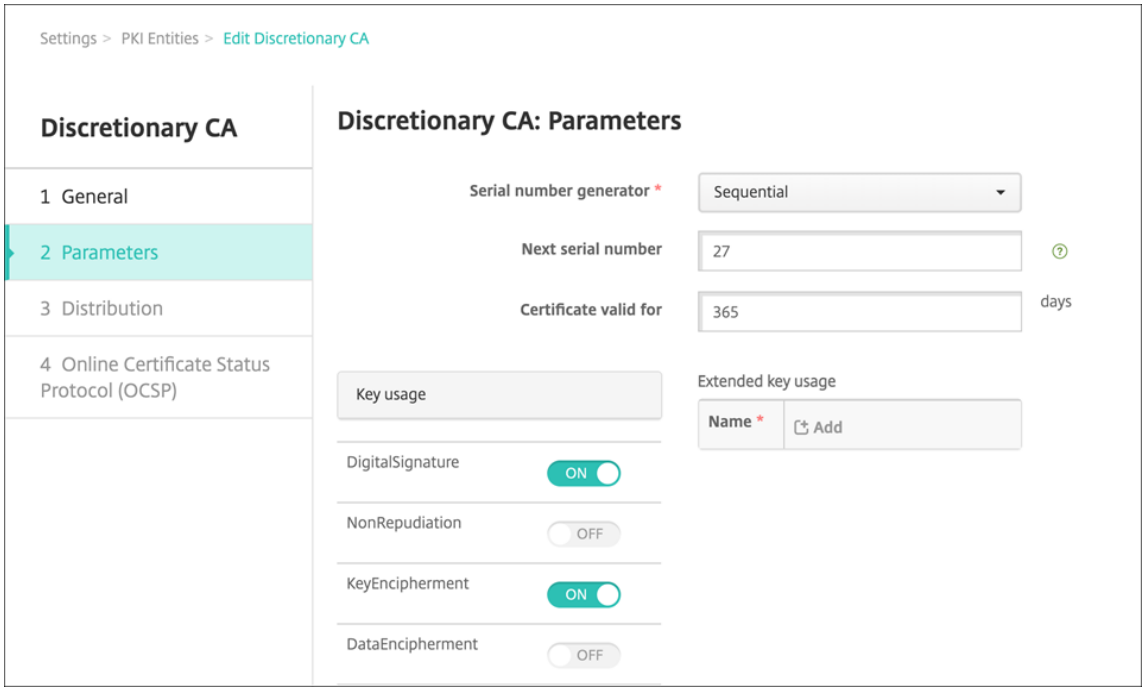


4. Führen Sie auf der Seite **Eigenverwaltete ZS: Allgemeine Informationen** folgende Schritte aus:

   - **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 Citrix Endpoint Management hochgeladenen Zertifizierungsstellenzertifikaten mit privatem Schlüssel generiert.

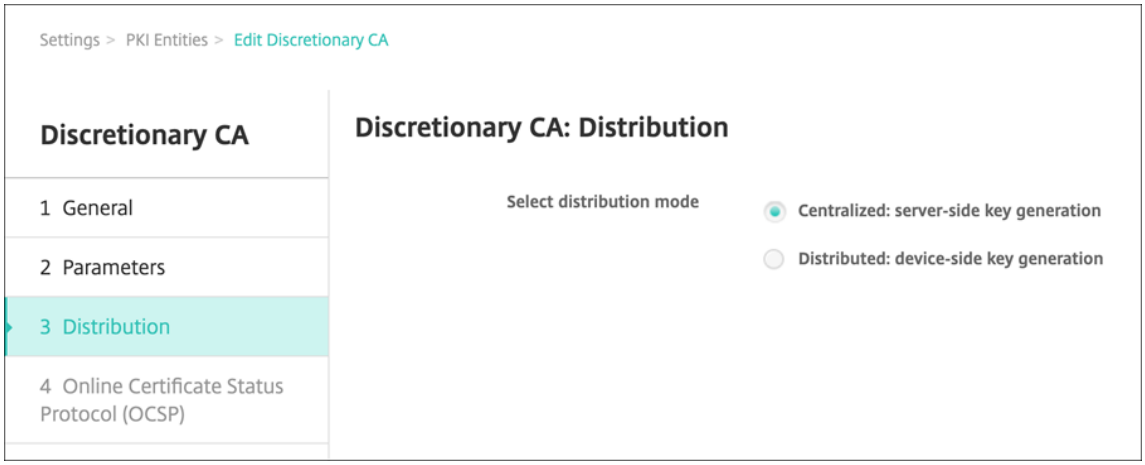
5. Klicken Sie auf **Weiter**.



6. Konfigurieren Sie auf der Seite **Eigenverwaltete ZS: Parameter** Folgendes:

   - **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**.

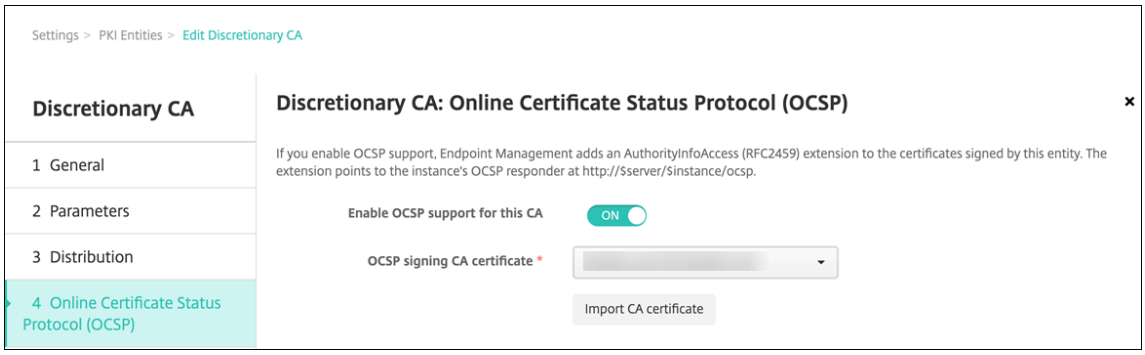
7. Klicken Sie auf **Weiter**.



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**.



10. Konfigurieren Sie auf der Seite **Eigenverwaltete ZS: Online Certificate Status Protocol (OCSP)** Folgendes:

    - 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 Citrix Endpoint Management

hochgeladenen Zertifizierungsstellenzertifikaten generiert.

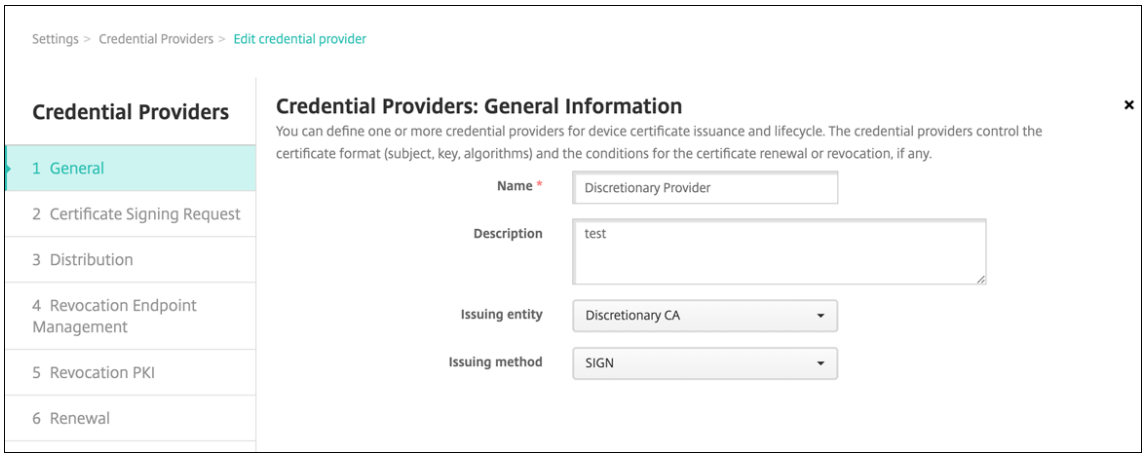
Bei Aktivierung des Features kann Citrix ADC den Status von Zertifikaten überprüfen. Citrix empfiehlt, dass Sie dieses Feature aktivieren.

11. Klicken Sie auf **Speichern**.

    Die eigenverwaltete ZS wird in der Tabelle der PKI-Entitäten angezeigt.

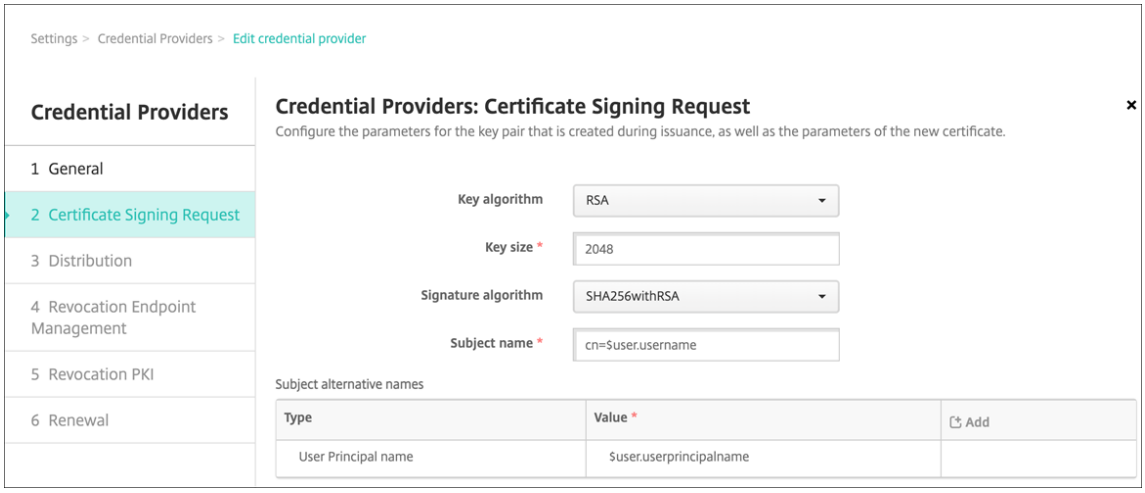
Konfigurieren eines Anmeldeinformationsanbieters

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Anmeldeinformationsanbieter** und klicken Sie auf **Hinzufügen**.
2. Führen Sie auf der Seite **Anmeldeinformationsanbieter: 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 Citrix Endpoint Management-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:** Wählen Sie **Eigenverwaltete ZS**.
   - **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**.

3. Klicken Sie auf **Weiter**. Konfigurieren Sie auf der Seite **Anmeldeinformationsanbieter: Zertifikatsignieranforderung** die folgenden Einstellungen gemäß Ihrer Zertifikatkonfiguration:



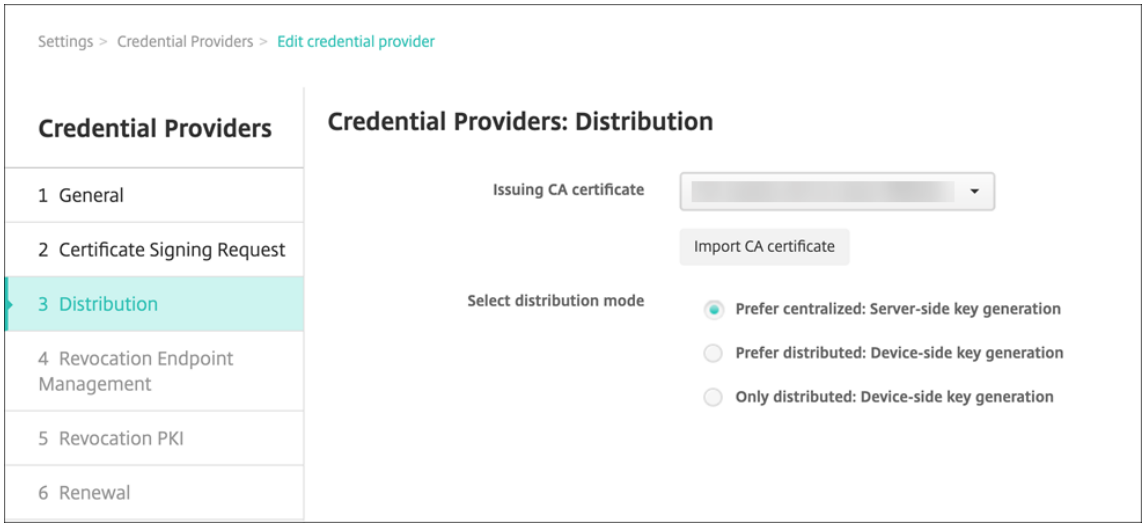
- **Schlüsselalgorithmus:** Wählen Sie den Schlüsselalgorithmus für das neue Schlüsselpaar. Verfügbare Werte sind **RSA**, **DSA** und **ECDSA**.
- **Schlüsselgröße:** Geben Sie die Länge des Schlüsselpaars in Bit ein. Dieses Feld ist erforderlich. Citrix empfiehlt die Verwendung von **2048** Bits.
- **Signaturalgorithmus:** Klicken Sie auf einen Wert für das neue Zertifikat. Welche Werte zulässig sind, hängt vom Schlüsselalgorithmus ab. Citrix empfiehlt **SHA256withRSA**.
- **Antragstellername:** erforderlich. Geben Sie den Distinguished Name des Antragstellers für das neue Zertifikat ein. Verwenden Sie `CN=${ user.username }` für den Benutzernamen oder `CN=${ user.samaccountname }`, um sAMAccountName zu verwenden.
- 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.

  Fügen Sie Folgendes hinzu:

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

  Wie beim Antragstellernamen können Sie im Wertfeld Citrix Endpoint Management-Makros verwenden.

4. Klicken Sie auf **Weiter**. Konfigurieren Sie auf der Seite **Anbieter für Anmeldeinformationen: Verteilung** Folgendes:

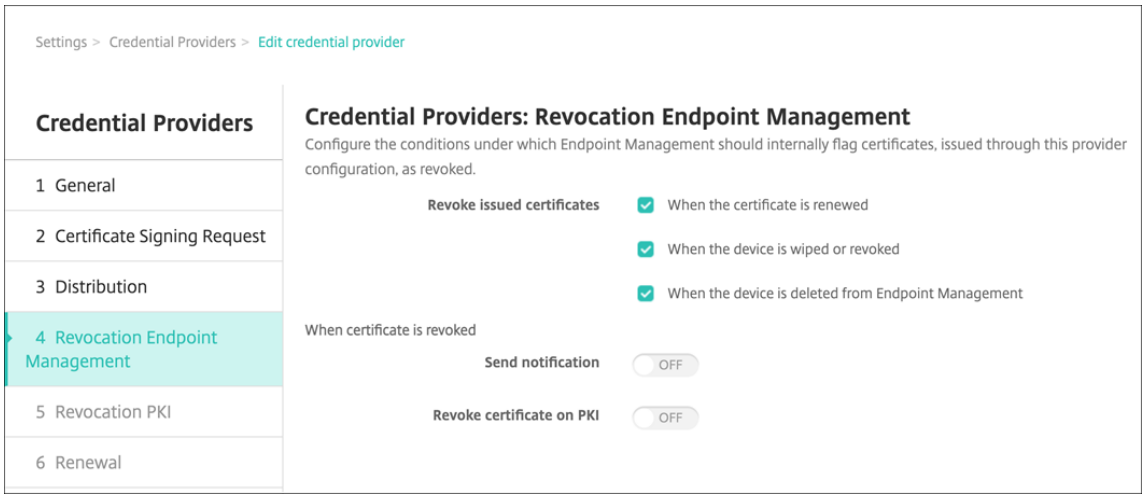


- **Zertifikat der ausstellenden ZS:** Wählen Sie das zuvor hinzugefügte Zertifikat der eigenverwalteten ZS aus.
- **Verteilungsmodus wählen**: Wählen Sie eine der folgenden Methoden zum Generieren und Verteilen von Schlüsseln aus:
  - **Bevorzugt zentralisiert: Schlüssel serverseitig generieren:** Citrix empfiehlt diese Option. Sie unterstützt alle von Citrix Endpoint Management unterstützten Plattformen und ist erforderlich, wenn die NetScaler Gateway-Authentifizierung verwendet wird. Die privaten Schlüssel werden auf dem Server generiert und gespeichert und auf die Benutzergeräte verteilt.
  - **Bevorzugt verteilt: Schlüssel geräteseitig generieren** Die privaten Schlüssel werden auf den Benutzergeräten generiert und gespeichert. Beim verteilten Modus wird SCEP verwendet und es ist ein RA-Verschlüsselungszertifikat mit KeyUsage “keyEncryption”sowie ein RA-Signaturzertifikat mit KeyUsage “digitalSignature”erforderlich. Das gleiche Zertifikat kann für Verschlüsselung und Signieren verwendet werden.
  - **Nur verteilt: Schlüssel geräteseitig generieren:** Diese Option funktioniert wie **Bevorzugt verteilt: Schlüssel geräteseitig generieren**, doch 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.

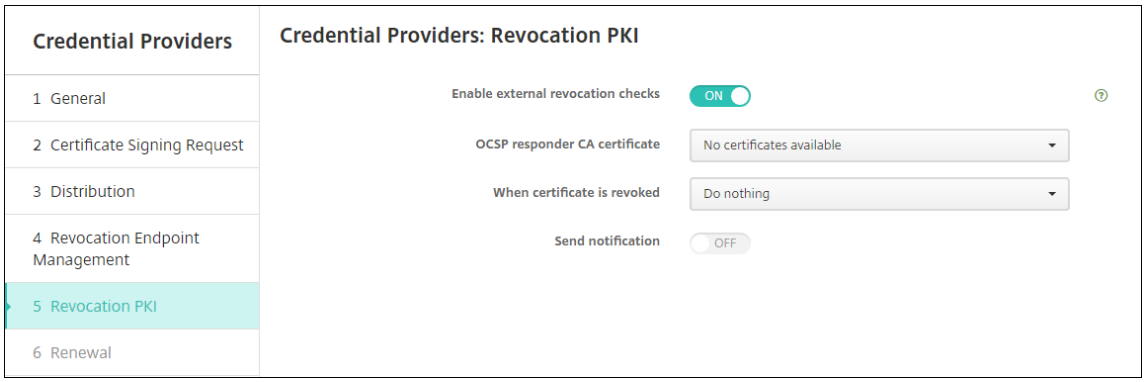
5. Klicken Sie auf **Weiter**. Konfigurieren Sie auf der Seite **Anmeldeinformationsanbieter: Citrix Endpoint Management-Sperrung** die Bedingungen, unter denen Citrix Endpoint Management-Zertifikate, die über diese Anbieterkonfiguration ausgestellt wurden, intern als gesperrt kennze-

ichnet. Konfigurieren Sie Folgendes:



- Wählen Sie für **Ausgestellte Zertifikate widerrufen** eine der Optionen zur Angabe des Zeitpunkts aus, an dem Zertifikate gesperrt werden sollen.
- Soll Citrix Endpoint Management eine Benachrichtigung bei Sperrung des Zertifikats senden, legen Sie für **Benachrichtigung senden** die Einstellung **Ein** fest und wählen Sie eine Benachrichtigungsvorlage aus.
- **Zertifikat in PKI widerrufen** funktioniert nicht, wenn Sie Citrix Endpoint Management als eigenverwaltete PKI verwenden.

6. Klicken Sie auf **Weiter**. Legen Sie auf der Seite **Anmeldeinformationsanbieter: PKI-Sperrung** fest, welche Aktionen in der PKI auszuführen sind, wenn das Zertifikat gesperrt wird. Darüber hinaus können Sie eine Benachrichtigung einrichten. Konfigurieren Sie Folgendes:



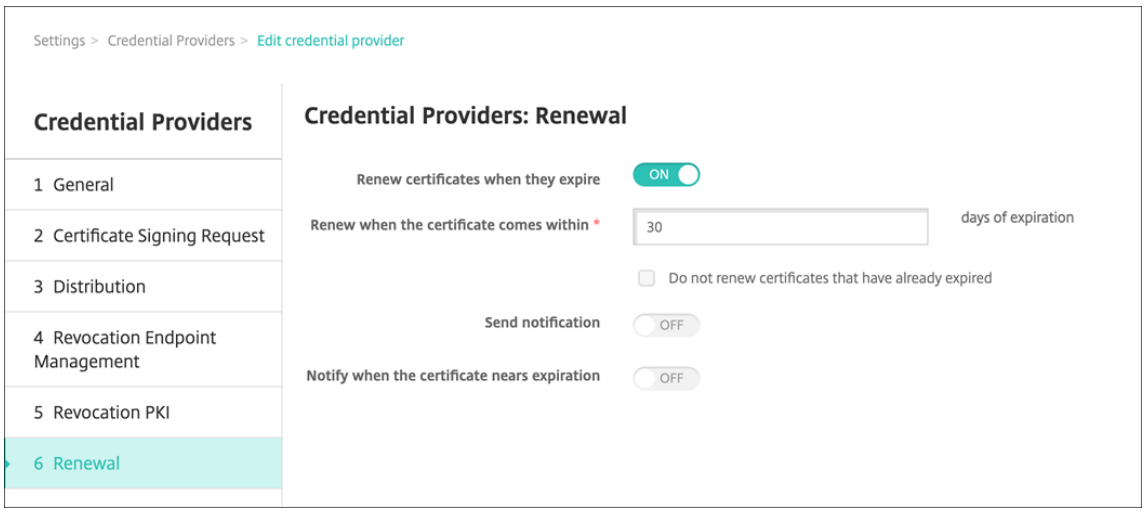
- **Prüfen der externen Zertifikatsperre aktivieren:** Legen Sie diese Einstellung auf **Ein** fest. Zusätzliche Felder für die Sperrung werden angezeigt.
- Wählen Sie in der Liste **OCSP Responder für ZS-Zertifikat** den Distinguished Name (DN) des Zertifikatantragstellers.

Sie können Citrix Endpoint Management-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 Citrix Endpoint Management 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.

7. Klicken Sie auf **Weiter**. Konfigurieren Sie auf der Seite **Anbieter für Anmeldeinformationen: Verlängerung** Folgendes:



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. Citrix Endpoint Management erneuert keine Zertifikate, nachdem sie intern gesperrt wurden.

Wenn Citrix Endpoint Management eine Benachrichtigung bei Verlängerung des Zertifikats senden soll, legen Sie **Benachrichtigung senden** auf **Ein** fest. Wenn Citrix Endpoint Management 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.

8. Klicken Sie auf **Speichern**.

Anmeldeinformationsanbieter

June 25, 2024

Anmeldeinformationsanbieter sind die Zertifikatkonfigurationen, die Sie in den verschiedenen Teilen des Citrix Endpoint Management-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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 oder Wiederherstellung: Zum Beispiel CSR-Parameter (Certificate Signing Request), wie Schlüsselgröße, Schlüsselalgorithmus und Zertifikatserweiterungen.
- Die Art und Weise, in der Zertifikate auf Geräten bereitgestellt werden.
- Zwar werden alle Zertifikate bei Beenden der Verwaltungsbeziehung in Citrix Endpoint Management 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 Citrix Endpoint Management an die Back-End-PKI (Public Key-Infrastruktur) gesendet werden. Das bedeutet, dass die Zertifikatsperrung in Citrix Endpoint Management eine Zertifikatssperrung in der PKI verursachen kann.
- Verlängerungseinstellungen: Zertifikate, die über einen bestimmten Anmeldeinformationsanbieter erworben wurden, können automatisch verlängert 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.

Methode der Zertifikatausstellung

Sie können ein Zertifikat durch Signieren erhalten, dies wird als Ausstellungsmethode bezeichnet.

Bei dieser Methode werden ein privater Schlüssel und eine Zertifikatsignieranforderung (CSR) erstellt und die CSR zum Signieren an eine Zertifizierungsstelle (ZS) übermittelt. Citrix Endpoint Management unterstützt die Signiermethode sowohl für MS-Zertifikatdiensteentitäten als auch eigenverwaltete Zertifizierungsstellen.

Ein Anmeldeinformationsanbieter verwendet die Signiermethode für die Zertifikatausstellung.

Zertifikatbereitstellung

Es gibt zwei Arten der Zertifikatbereitstellung in Citrix Endpoint Management: 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 Citrix Endpoint Management bei Verwendung des SCEP-Protokolls als Delegate (erweiterte Registrierungsstelle) für die tatsächliche Zertifizierungsstelle fungiert. Citrix Endpoint Management muss dem Client nachweisen, dass die Berechtigung hierzu vorliegt. Diese Berechtigung ist durch das Hochladen der o. g. Zertifikate für Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management:

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 Tablet	Nein	Nein

Kontext	SCEP unterstützt	SCEP erforderlich
Konfiguration von Windows Tablet	Nein, mit Ausnahme der Netzwerkgeräterichtlinie, die für 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 Citrix Endpoint Management gepflegten Zertifikatstatus aus. Citrix Endpoint Management 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.
- **Externally propagated revocation:** Also known as Revocation Citrix Endpoint Management, this type of revocation applies to certificates got from an external PKI. Das Zertifikat wird in der PKI gesperrt, wenn es unter den in der Konfiguration des Anmeldeinformationsanbieters festgelegten Bedingungen intern von Citrix Endpoint Management gesperrt wird.
- **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 Citrix Endpoint Management diesen bei der PKI ab. Ist das Zertifikat gesperrt, wird es von Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management, 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, Citrix Endpoint Management-interne Entitäten sind interne Entitäten. Die Ausstellungsmethode bei eigenverwalteten Zertifizierungsstellen ist immer "sign". Das bedeutet, dass bei jeder Ausstellung von Citrix Endpoint Management 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, gehört die Microsoft-Zertifizierungsstelle.

1. Klicken Sie in der Citrix Endpoint Management-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 Citrix Endpoint Management-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 En-

tität 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. Dieses Feld ist erforderlich.

     Die zulässigen Werte sind abhängig vom Schlüsseltyp. Die maximale Länge für DSA-Schlüssel beträgt beispielsweise 2048 Bit. To avoid false negatives, which depend on the underlying hardware and software, Citrix Endpoint Management doesn't enforce key sizes. 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`

     For example, for client certificate authentication, use these settings:

     - **Key algorithm:** RSA
     - **Key size:** 2048
     - **Signature algorithm:** SHA256withRSA
     - **Subject name:** `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 Citrix Endpoint Management-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 Citrix Endpoint Management unterstützten Plattformen und ist erforderlich, wenn die NetScaler Gateway-Authentifizierung verwendet wird. Die privaten Schlüssel werden auf dem Server generiert und gespeichert und auf die Benutzergeräte verteilt.
     - **Bevorzugt verteilt: Schlüssel geräteseitig generieren** Die privaten Schlüssel werden auf den Benutzergeräten generiert und gespeichert. Beim verteilten Modus wird SCEP verwendet und es ist ein RA-Verschlüsselungszertifikat mit KeyUsage “keyEncryption”sowie ein RA-Signaturzertifikat mit KeyUsage “digitalSignature”erforderlich. Das gleiche Zertifikat kann für Verschlüsselung und Signieren verwendet werden.
     - **Nur verteilt: Schlüssel geräteseitig generieren:** Diese Option funktioniert wie “Bevorzugt verteilt: Schlüssel geräteseitig generieren”, doch da sie anstelle einer Bevorzugung eine Ausschließlichkeit definiert, steht keine Option zur Verfügung, wenn die geräteseitige Schlüsselgenerierung fehlschlägt oder nicht verfügbar ist.

   Wenn Sie **Bevorzugt verteilt: Schlüssel geräteseitig generieren** oder **Nur verteilt: Schlüssel geräteseitig generieren** ausgewählt haben, klicken Sie auf das gewünschte RA-Signaturzertifikat und das RA-Verschlüsselungszertifikat. Das gleiche Zertifikat kann für beides verwendet werden. Es werden neue Felder für diese Zertifikate eingeblendet.

8. Klicken Sie auf **Weiter**.

Die Seite **Anbieter für Anmeldeinformationen: Citrix Endpoint Management-Sperrung** wird angezeigt. Auf dieser Seite konfigurieren Sie die Bedingungen, unter denen Citrix Endpoint Management Zertifikate, die über diese Anbieterkonfiguration ausgestellt wurden, intern als gesperrt kennzeichnet.

9. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: Citrix Endpoint Management-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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 Entitäten mit Sperrfunktion. Wenn das Zertifikat von Citrix Endpoint Management gesperrt wird, wird ein Sperraufruf an die in der Liste "Entität"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 Citrix Endpoint Management-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 Citrix Endpoint Management 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 Citrix Endpoint Management für folgende Aufgaben konfigurieren:

    - 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. Citrix Endpoint Management erneuert keine Zertifikate, nachdem sie intern gesperrt wurden.

    Wenn Citrix Endpoint Management eine Benachrichtigung bei Verlängerung des Zertifikats senden soll, legen Sie **Benachrichtigung senden** auf **Ein** fest. Wenn Citrix Endpoint Management 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.

APN-Zertifikate

June 25, 2024

Zum Registrieren und Verwalten von Apple-Geräten mit Citrix Endpoint Management müssen Sie ein Zertifikat von Apple für den Apple-Dienst für Push-Benachrichtigungen (Apple Push Notification service, APNs) einrichten. Das Zertifikat ermöglicht die Mobilgeräteverwaltung über das Apple Push-Netzwerk.

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 OpenSSL

Schritt 2: Signieren der Zertifikatsignieranforderung in Citrix Endpoint Management 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 Citrix Endpoint Management

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 re-enrollment.
> - 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. Sie können beispielsweise den vollqualifizierten Domänennamen (FQDN) Ihres Citrix Endpoint Management-Servers eingeben, z. B. `www.domain.com`. 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 OpenSSL

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
   9  Locality Name (eg, city) []:RWC
   10 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.

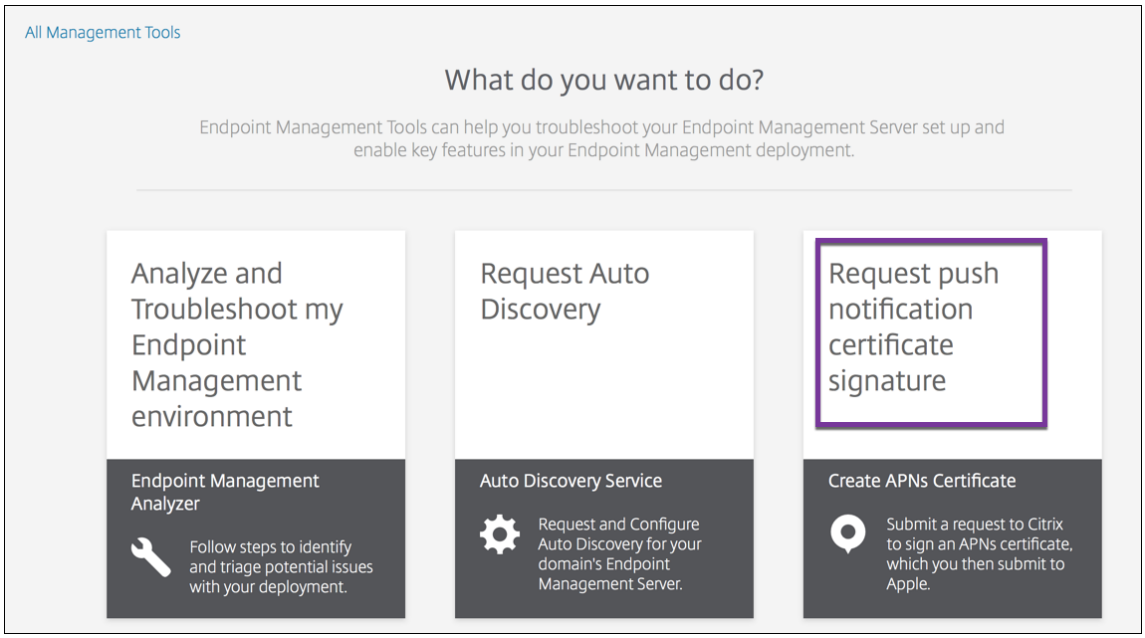
```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
<!--NeedCopy-->
```

4. Um fortzufahren, signieren Sie die Zertifikatsignieranforderung wie im nächsten Abschnitt beschrieben.

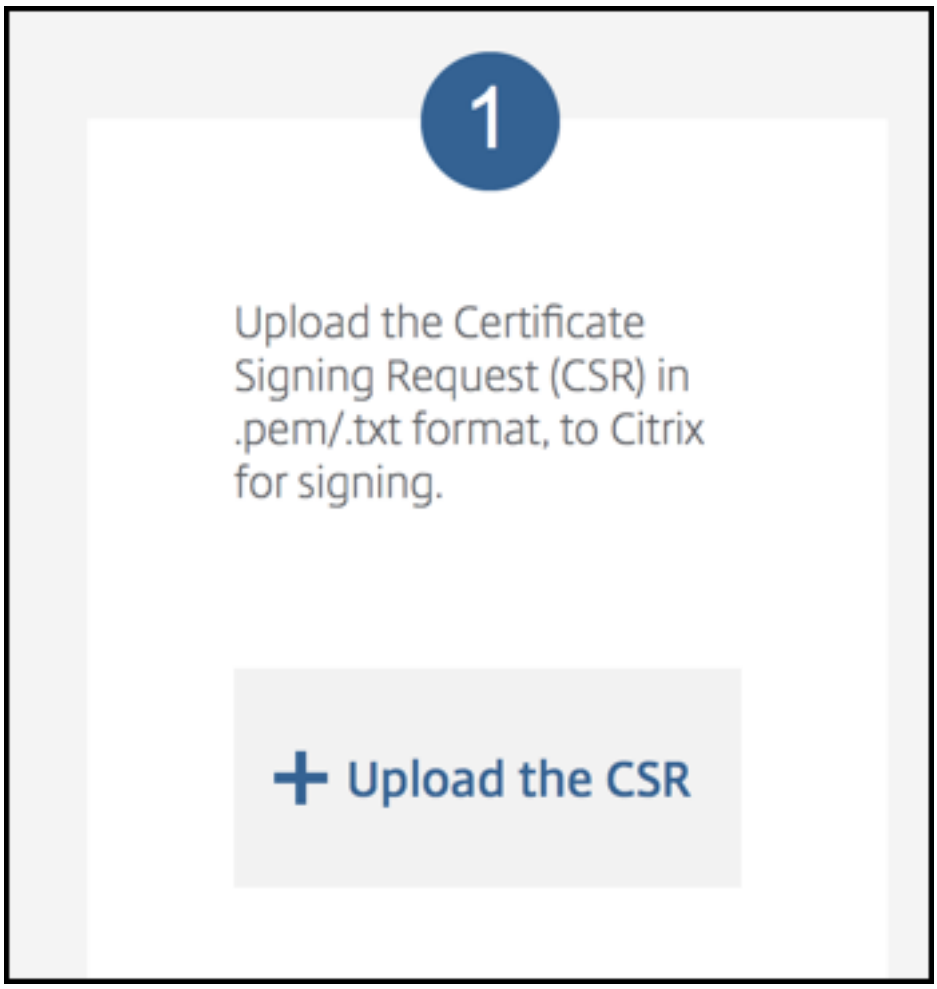
Signieren der Zertifikatsignieranforderung

Um ein Zertifikat mit Citrix Endpoint Management zu verwenden, müssen Sie es zum Signieren an Citrix übermitteln. Citrix signiert die Zertifikatsignieranforderung mit seinem Zertifikat für die Mobilgeräteverwaltung und sendet die signierte Datei im Format `.plist` zurück.

1. Wechseln Sie in Ihrem Browser zu der Website Citrix 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.

> **Wichtig:**
>
> Das Zertifikat muss im PEM/TXT-Format vorliegen. Ändern Sie bei Bedarf die Dateinamenerweiterung des Zertifikats in .pem oder .txt, indem Sie mit der rechten Maustaste klicken und die Datei umbenennen.

4. Klicken Sie auf der Seite **Citrix 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 Citrix Endpoint Management importieren müssen.

> **Hinweis:**
>
> Es gibt Berichte über Probleme mit der Anmeldung beim Apple Push Portal. Alternativ können Sie sich beim Apple Developer Portal anmelden. 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 Citrix Endpoint Management. 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 im Citrix Endpoint Management-Server verwendet werden.
8. Um fortzufahren, siehe Importieren eines APNs-Zertifikats in Citrix Endpoint Management.

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 Citrix Endpoint Management zu importieren.

7. Kopieren Sie die PFX-Zertifikatdatei auf den Server, auf dem Citrix Endpoint Management installiert werden soll.
8. Um fortzufahren, siehe Importieren eines APNs-Zertifikats in Citrix Endpoint Management.

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 Citrix Endpoint Management hochladen.
3. Notieren Sie den Speicherort der PFX-Zertifikatsdatei. Kopieren Sie dann die Datei auf den Citrix Endpoint Management-Server, damit Sie sie mit der Konsole hochladen können.
4. Um fortzufahren, importieren Sie ein APNs-Zertifikat in Citrix Endpoint Management, wie im nächsten Abschnitt beschrieben.

Importieren eines APNs-Zertifikats in Citrix Endpoint Management

Nachdem Sie das neue APNs-Zertifikat erhalten haben, importieren Sie es in Citrix Endpoint Management –entweder als erstes Zertifikat oder als Ersatz für ein bestehendes Zertifikat.

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **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 Citrix Endpoint Management 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.

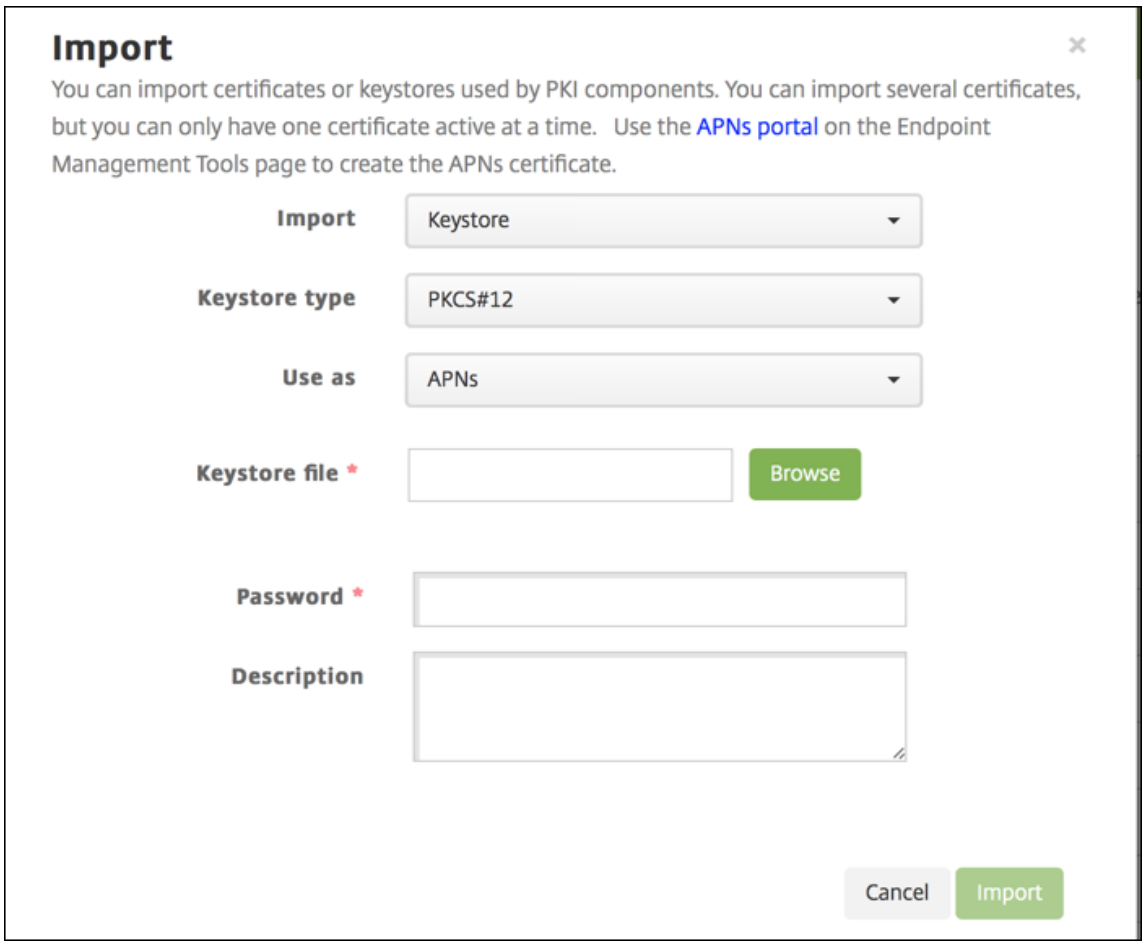
Um herauszufinden, wann Ihr APNs-Zertifikat abläuft, klicken Sie in der Citrix Endpoint Management-Konsole auf **Einstellungen > Zertifikate**. Widerrufen Sie das Zertifikat nicht, falls es abläuft.

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. Rufen Sie im Browser die Citrix Endpoint Management Tools auf. 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 Citrix Endpoint Management-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**.

Citrix Endpoint Management 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

March 11, 2024

Citrix Endpoint Management und ShareFile 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 anmelden, werden zur Benutzerauthentifizierung und zum Abrufen eines SAML-Token an Citrix Secure Hub weitergeleitet. Nach einer erfolgreichen Authentifizierung sendet die mobile Citrix Files-App das SAML-Token an ShareFile. Nach der Erstanmeldung können Benutzer über SSO auf die mobile Citrix Files-App zugreifen. Sie können außerdem Dokumente aus ShareFile an E-Mails in Citrix 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 Citrix Endpoint Management umgeleitet. Citrix Endpoint Management authentifiziert die Benutzer, die dann einen SAML-Token erhalten, der an ShareFile gesendet wird. Nach der ersten Anmeldung können Benutzer auf Citrix Files-Clients über SSO ohne erneute Anmeldung zugreifen.

Um Citrix Endpoint Management als SAML-Identity-Provider (IdP) für ShareFile zu verwenden, müssen Sie Citrix Endpoint Management für Enterprise-Konten konfigurieren, wie in diesem Artikel beschrieben. Alternativ können Sie Citrix Endpoint Management für die ausschließliche Verwendung mit Speicherzonenconnectors konfigurieren. Weitere Informationen finden Sie unter ShareFile mit Citrix Endpoint Management.

Ein detailliertes Architekturdiagramm finden Sie unter Architektur.

Voraussetzungen

Damit Sie Single Sign-On für Citrix Endpoint Management und Citrix Files-Apps konfigurieren können, müssen die folgenden Voraussetzungen erfüllt sein:

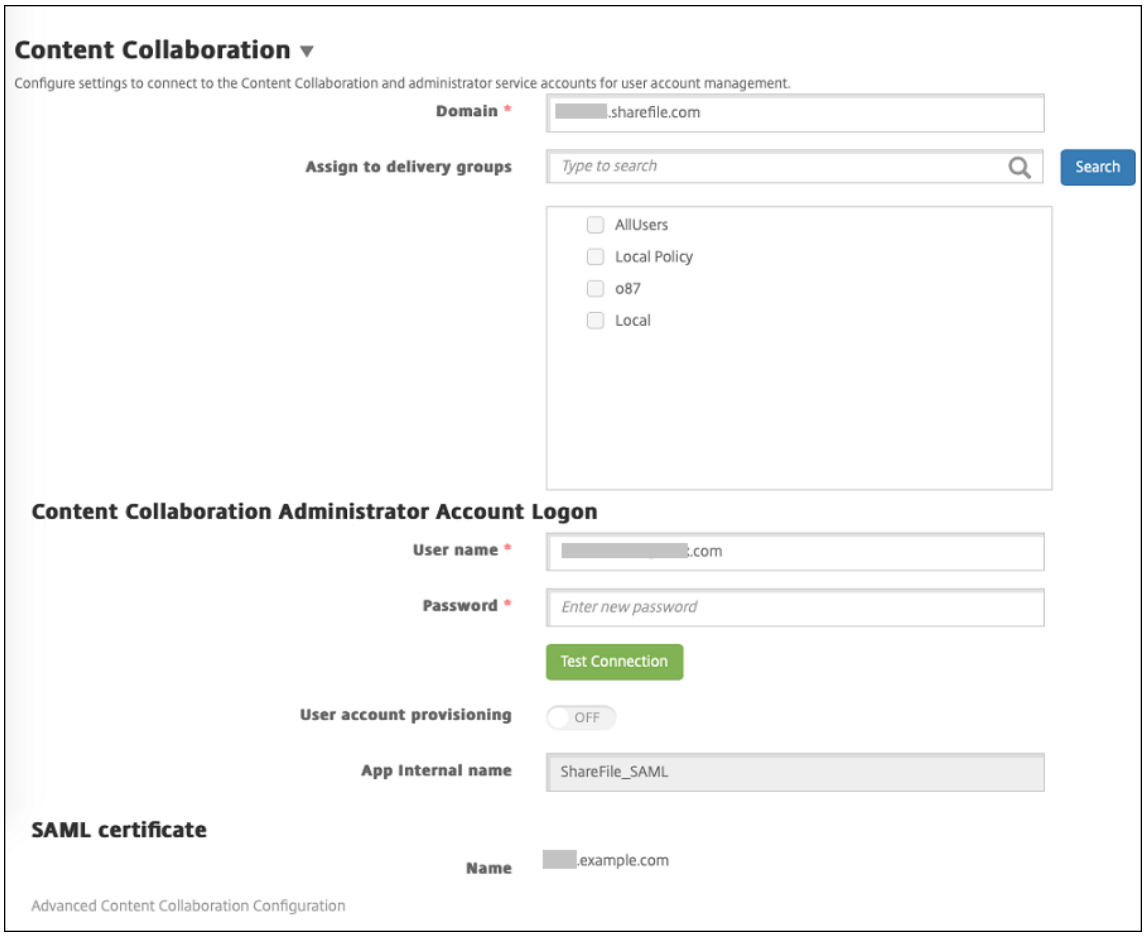
- Das MAM-SDK oder eine kompatible Version des MDX Toolkits (für mobile Citrix Files-Apps).

  Weitere Informationen finden Sie unter Citrix Endpoint Management-Kompatibilität.
- Eine kompatible Version mobiler Citrix Files-Apps und Citrix Secure Hub.
- ShareFile-Administratorkonto
- Überprüfte Konnektivität zwischen Citrix Endpoint Management und ShareFile.

ShareFile-Zugriff konfigurieren

Vor der Einrichtung von SAML für ShareFile geben Sie die ShareFile-Zugriffsinformationen wie folgt an:

1. Klicken Sie in der Citrix Endpoint Management-Webkonsole auf **Konfigurieren > ShareFile**. Die Konfigurationsseite **ShareFile** wird angezeigt.



2. Konfigurieren Sie folgende Einstellungen:

   - **Domäne:** Geben Sie den Namen der ShareFile-Unterdomäne ein. Beispiel: `example.sharefile.com`.
   - **Bereitstellungsgruppen zuweisen:** Suchen Sie nach Bereitstellungsgruppen, die SSO mit ShareFile verwenden sollen, oder wählen Sie sie aus.
   - **Anmeldung beim ShareFile-Administratorkonto**
   - **Benutzername:** Geben Sie den Benutzernamen des ShareFile-Administrators ein. Dieses Benutzerkonto muss über Administratorrechte verfügen.
   - **Kennwort:** Geben Sie das Kennwort des ShareFile-Administrators ein.
   - **Benutzerkontoprovisioning:** Lassen Sie diese Einstellung deaktiviert. Verwendung des

ShareFile User Management Tools für die Benutzerbereitstellung Siehe Provision user accounts and distribution groups.

3. Sie können über die Schaltfläche **Verbindung testen** prüfen, ob Benutzername und Kennwort des ShareFile-Administratorkontos für das angegebene ShareFile-Konto authentifiziert werden.
4. Klicken Sie auf **Speichern**.
   - Citrix Endpoint Management synchronisiert mit ShareFile und aktualisiert die ShareFile-Einstellungen **ShareFile-Aussteller/Entitäts-ID** und **Anmelde-URL**.
   - 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 benötigen NetScaler Gateway nicht für die Single Sign-On-Konfiguration von Citrix Files-Apps, die mit dem MAM-SDK vorbereitet wurden. 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 NetScaler Gateway für andere Citrix Files-Clients.

So konfigurieren Sie SAML für umschlossene Citrix Files MDX-Apps:

1. Laden Sie die ShareFile für Citrix Endpoint Management-Clients herunter. Siehe Citrix.com-Downloads.
2. Bereiten Sie die mobile Citrix Files-App mit dem MAM-SDK vor. Weitere Informationen finden Sie unter Überblick über das MAM-SDK.
3. Laden Sie in der Citrix Endpoint Management-Konsole die vorbereitete mobile Citrix Files-App hoch. Weitere Informationen zum Hochladen von MDX-Apps finden Sie unter Hinzufügen einer MDX-App zu Citrix Endpoint Management.
4. Überprüfen Sie die SAML-Einstellungen: Melden Sie sich bei ShareFile mit den Anmeldeinformationen des Administrators an, die Sie vorher angegeben haben.
5. Vergewissern Sie sich, dass ShareFile und Citrix Endpoint Management für dieselbe Zeitzone konfiguriert sind. Stellen Sie sicher, dass in Citrix Endpoint Management 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 Citrix Secure Hub auf dem Benutzergerät.

2. Laden Sie die mobile Citrix Files-App aus dem App-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 Citrix Secure Mail

1. Installieren und konfigurieren Sie Citrix Secure Hub gegebenenfalls auf dem Benutzergerät.
2. Laden Sie Citrix Secure Mail aus dem App-Store herunter und installieren und konfigurieren Sie das Programm.
3. Öffnen Sie ein neues E-Mail-Formular und tippen Sie auf **Von ShareFile anfügen**. Die zum Anfügen verfügbaren Dateien werden ohne Anforderung von Benutzernamen und Kennwort angezeigt.

Konfigurieren von NetScaler Gateway für andere Citrix Files-Clients

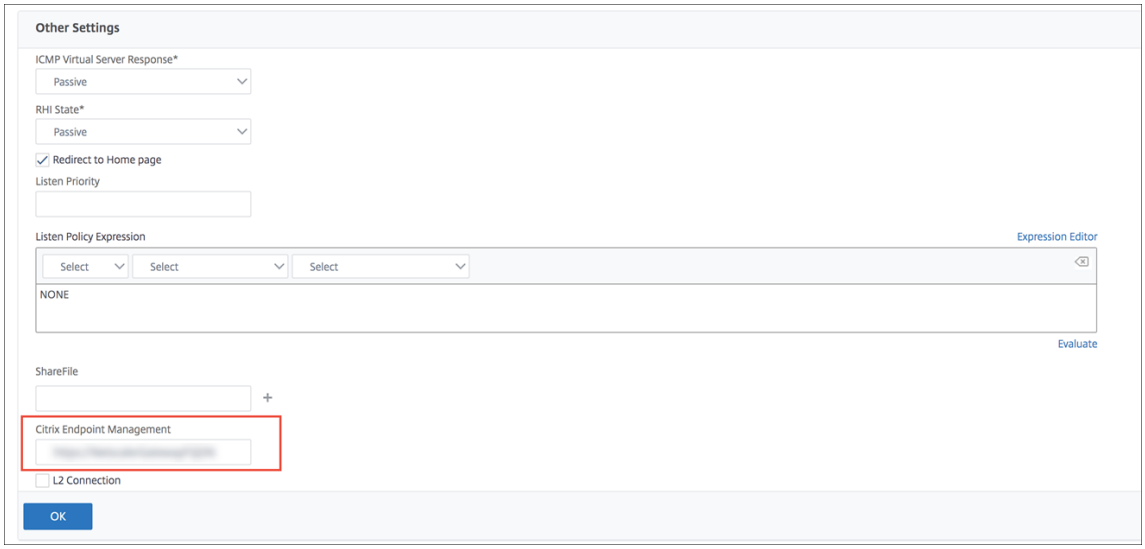
Zum Konfigurieren des Zugriffs für nicht umschlossene Citrix Files-Clients (z. B. Website, Outlook-Plug-In oder Synchronisierungsclients) konfigurieren Sie NetScaler Gateway folgendermaßen, damit es die Verwendung von Citrix Endpoint Management als SAML-Identitätsanbieter unterstützt:

- Deaktivieren Sie die Homepageumleitung.
- Erstellen Sie eine Citrix Files-Sitzungsrichtlinie und ein Profil.
- Konfigurieren Sie Richtlinien auf dem virtuellen NetScaler 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 NetScaler Gateway-Server, der für Citrix Endpoint Management-Anmeldungen verwendet wird. Navigieren Sie in NetScaler Gateway zu **Other Settings** und deaktivieren Sie das Kontrollkästchen **Redirect to Home Page**.



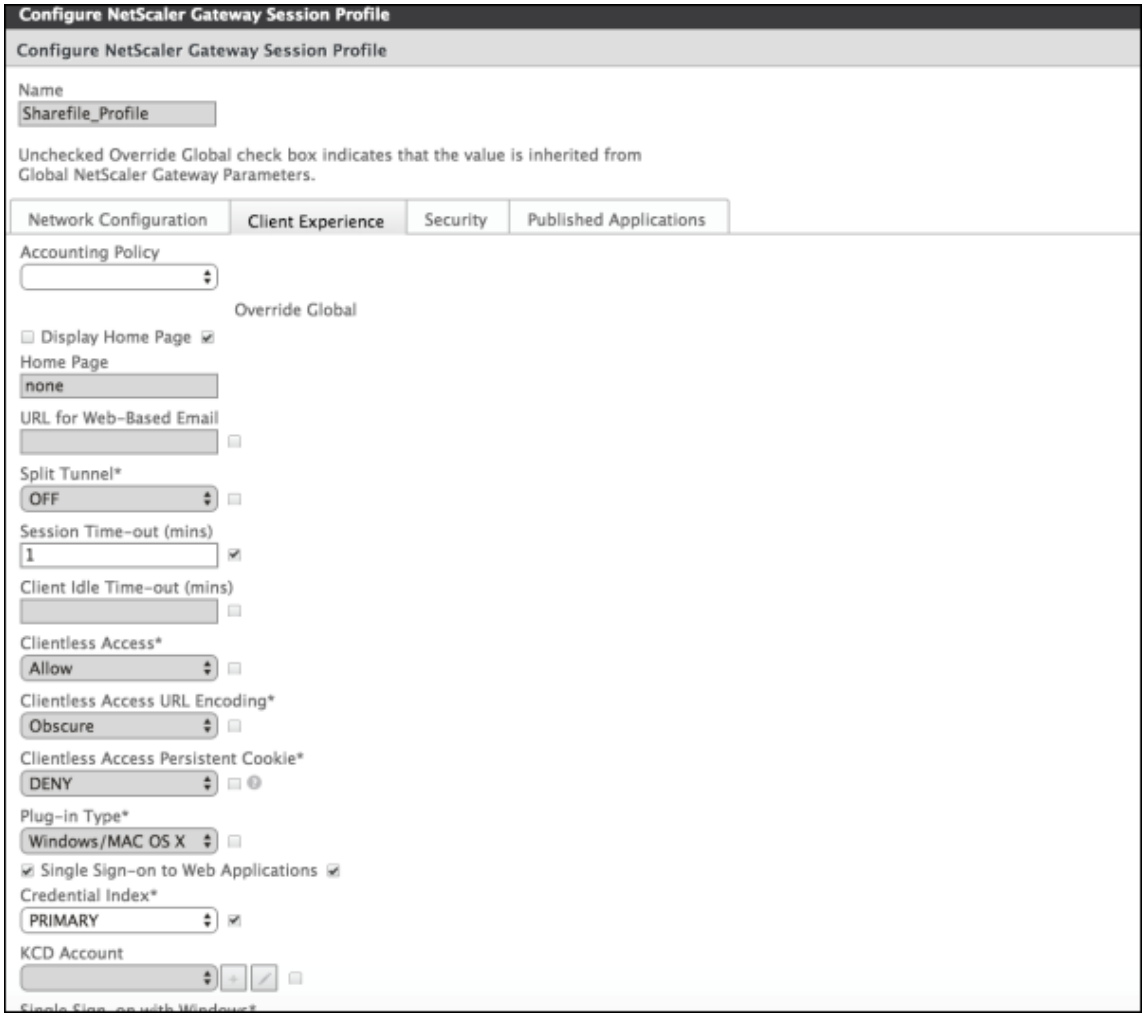
2. Geben Sie unter **ShareFile** den internen Namen des Citrix Endpoint Management-Servers und die Portnummer ein.
3. Geben Sie unter **Citrix Endpoint Management** Ihre Citrix Endpoint Management-URL ein.

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

Erstellen einer Citrix Files-Sitzungsrichtlinie und eines Anforderungsprofils

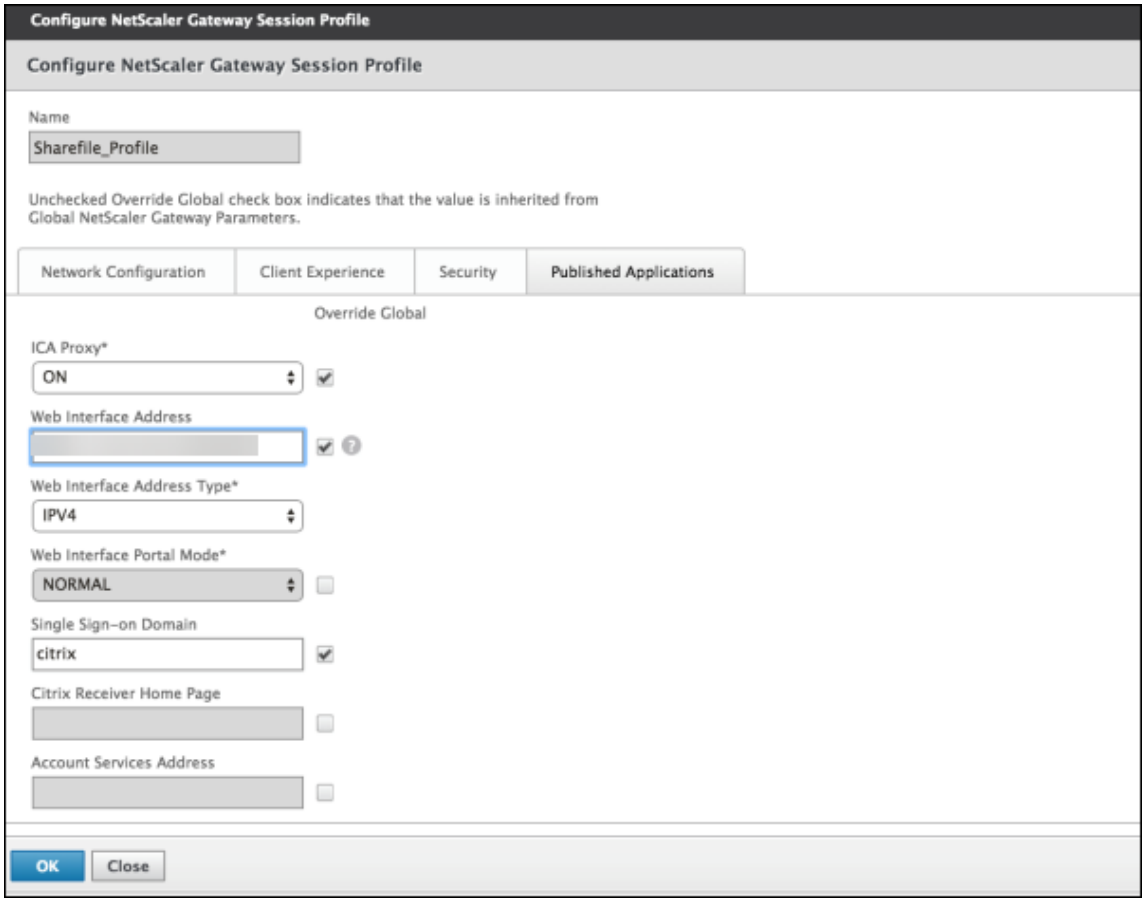
Konfigurieren Sie die folgenden Einstellungen zum Erstellen einer Citrix Files-Sitzungsrichtlinie und eines Anforderungsprofils:

1. Klicken Sie im Konfigurationsprogramm für NetScaler Gateway im linken Navigationsbereich auf **NetScaler 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 NetScaler Gateway Session Profile** wird angezeigt.



Konfigurieren Sie folgende Einstellungen:

- **Name:** Geben Sie **ShareFile_Profile** ein.
- Klicken Sie auf die Registerkarte **Client Experience** und konfigurieren Sie die folgenden Einstellungen:
  - **Home Page:** Geben Sie **none** ein.
  - **Session Time-out (mins):** Geben Sie **1** ein.
  - **Single Sign-on to Web Applications:** Wählen Sie diese Einstellung aus.
  - **Credential Index:** Klicken Sie auf **PRIMARY**.
- Klicken Sie auf die Registerkarte **Published Applications**.

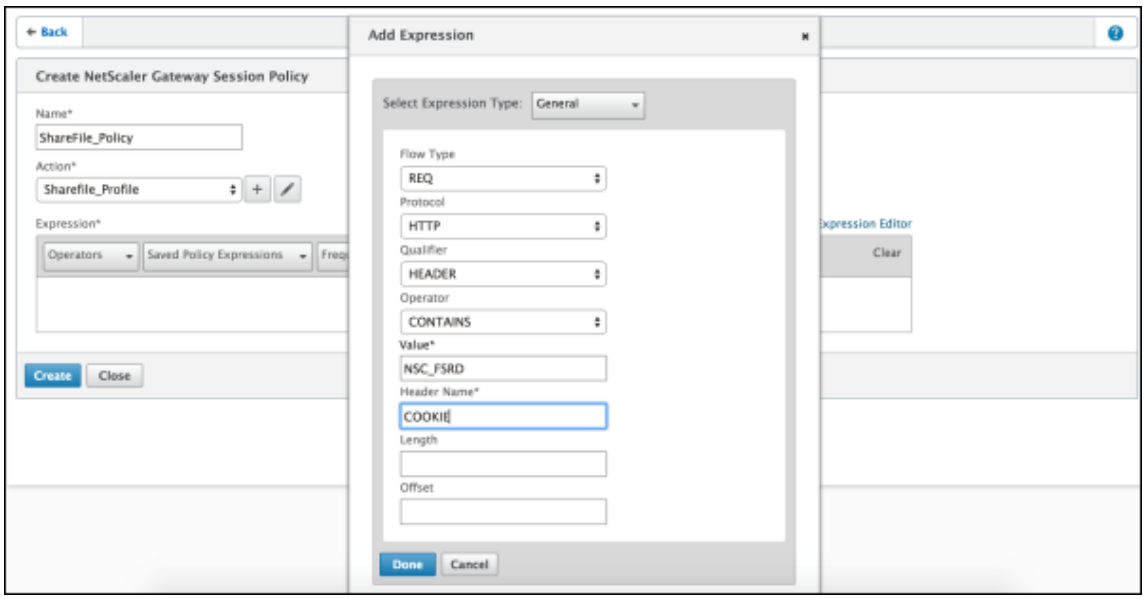


Konfigurieren Sie folgende Einstellungen:

- **ICA Proxy:** Klicken Sie auf **On**.
- **Web Interface Address:** Geben Sie die URL des Citrix Endpoint Management-Servers ein.
- **Single Sign-on Domain:** Geben Sie den Namen Ihrer Active Directory-Domäne ein.

  Beim Konfigurieren des NetScaler Gateway-Sitzungsprofils muss das Domänensuffix für **Single Sign-on Domain** mit dem in LDAP festgelegten Citrix Endpoint Management-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.

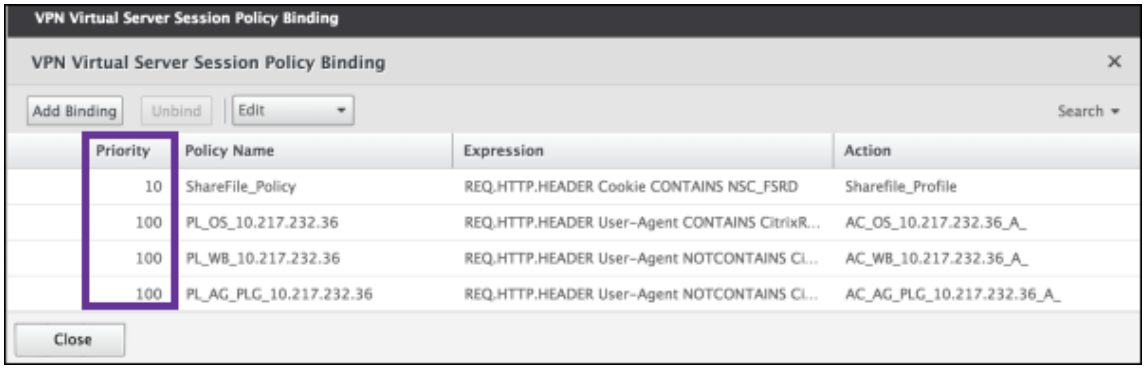
7. Klicken Sie auf **Create** und dann auf **Close**.

Konfigurieren von Richtlinien auf dem virtuellen NetScaler Gateway-Server

Konfigurieren Sie die folgenden Einstellungen auf dem virtuellen NetScaler Gateway-Server.

1. Klicken Sie im Konfigurationsprogramm für NetScaler Gateway im linken Navigationsbereich auf **NetScaler Gateway > Virtual Servers**.
2. Klicken Sie im Bereich **Details** auf den virtuellen NetScaler Gateway-Server.
3. Klicken Sie auf **Bearbeiten**.
4. Klicken Sie auf **Configured policies > Session policies** und dann auf **Add binding**.

5. Wählen Sie **ShareFile_Policy** aus.
6. Bearbeiten Sie die automatisch generierte Prioritätszahl unter **Priority** für die ausgewählte Richtlinie so, dass sie die höchste Priorität (die niedrigste Zahl) vor allen anderen aufgeführten Richtlinien hat. Beispiel:



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

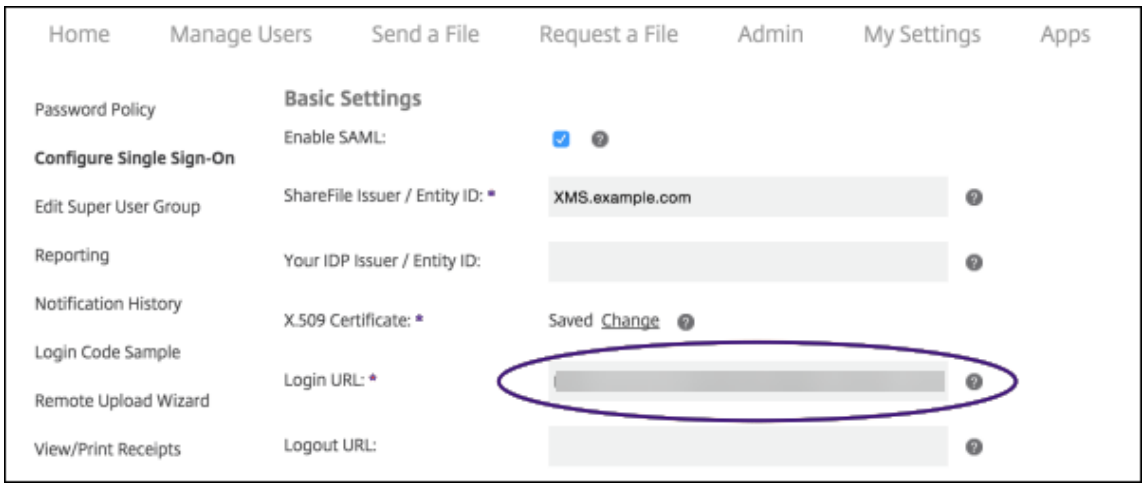
Ändern der SSO-Einstellungen für Citrix Files.com

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 ShareFile-Einstellungen in Citrix Endpoint Management ändern
>
> Daher müssen Sie die Anmelde-URL auf der Citrix Files-Website dem neuen App-Namen entsprechend aktualisieren.

1. Melden Sie sich bei Ihrem ShareFile-Konto (`https://<subdomain>.sharefile.com`) als ShareFile-Administrator an.
2. Klicken Sie im ShareFile-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 NetScaler Gateway-Servers plus **/cginfra/https/** vor dem FQDN des Citrix Endpoint Management-Servers und **8443** hinter dem FQDN des Citrix Endpoint Management-Servers 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`

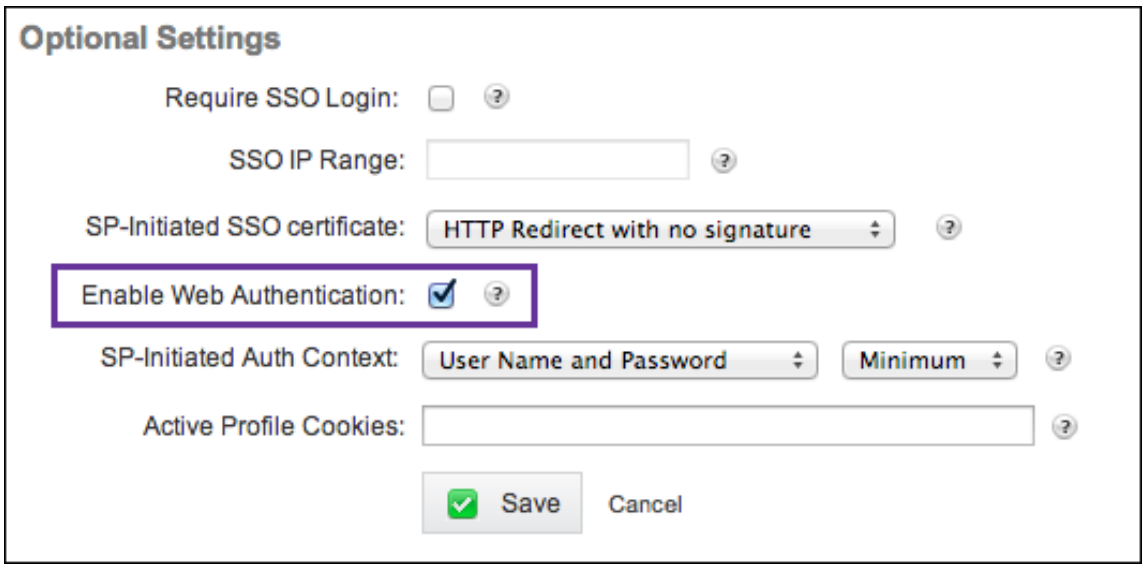
- Ändern Sie den Parameter `&app=ShareFile_SAML_SP` in den internen Citrix Files-App-Namen. Der interne Name lautet standardmäßig `ShareFile_SAML`. Jedes Mal, wenn Sie die Konfiguration ändern, wird eine Zahl an den internen Namen angehängt (`ShareFile_SAML_2`, `ShareFile_SAML_3` usw.). Sie können den **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 NetScaler Gateway-Anmeldungsformular umgeleitet. Erfolgt keine Umleitung, überprüfen Sie die oben aufgeführten Konfigurationseinstellungen.

2. Geben Sie die Anmeldeinformationen ein, die Sie für die NetScaler Gateway- bzw. Citrix Endpoint Management-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.

Authentifizierung mit Azure Active Directory über Citrix Cloud

June 25, 2024

Citrix Endpoint Management unterstützt die Authentifizierung mit Azure Active Directory (Azure AD)-Anmeldeinformationen über Citrix Cloud. Diese Authentifizierungsmethode steht nur Benutzern zur Verfügung, die sich über Citrix Secure Hub bei MDM registrieren.

Um Citrix Secure Hub mit MDM+MAM zu verwenden, konfigurieren Sie Citrix Endpoint Management zur Verwendung von NetScaler Gateway für die MAM-Registrierung. Weitere Informationen finden Sie unter NetScaler Gateway und Citrix Endpoint Management.

Citrix Endpoint Management verwendet die Citrix-Identität, einen Service von Citrix Cloud, für den Verbindungsaufbau mit Azure Active Directory. Citrix empfiehlt, dass Sie den Citrix-Identitätsanbieter und keine direkte Verbindung mit Azure Active Directory verwenden.

Citrix Endpoint Management unterstützt die Authentifizierung mit Azure AD für die folgenden Plattformen:

- iOS- und macOS-Geräte, die nicht im Apple Business Manager oder Apple School Manager registriert sind
- iOS- und macOS-Geräte, die im Apple Business Manager registriert sind
- Android Enterprise-Geräte (Preview) im BYOD- und vollständig verwalteten Modus

Für die Authentifizierung mit Azure AD über Citrix Cloud gelten folgende Einschränkungen:

- Nicht für lokale Citrix Endpoint Management-Konten verfügbar.
- Unterstützt keine Authentifizierung mit Azure AD für Registrierungseinladungen. Wenn Sie eine Registrierungseinladung mit einer Registrierungs-URL senden, authentifizieren sich die Benutzer über LDAP anstelle von Azure AD.

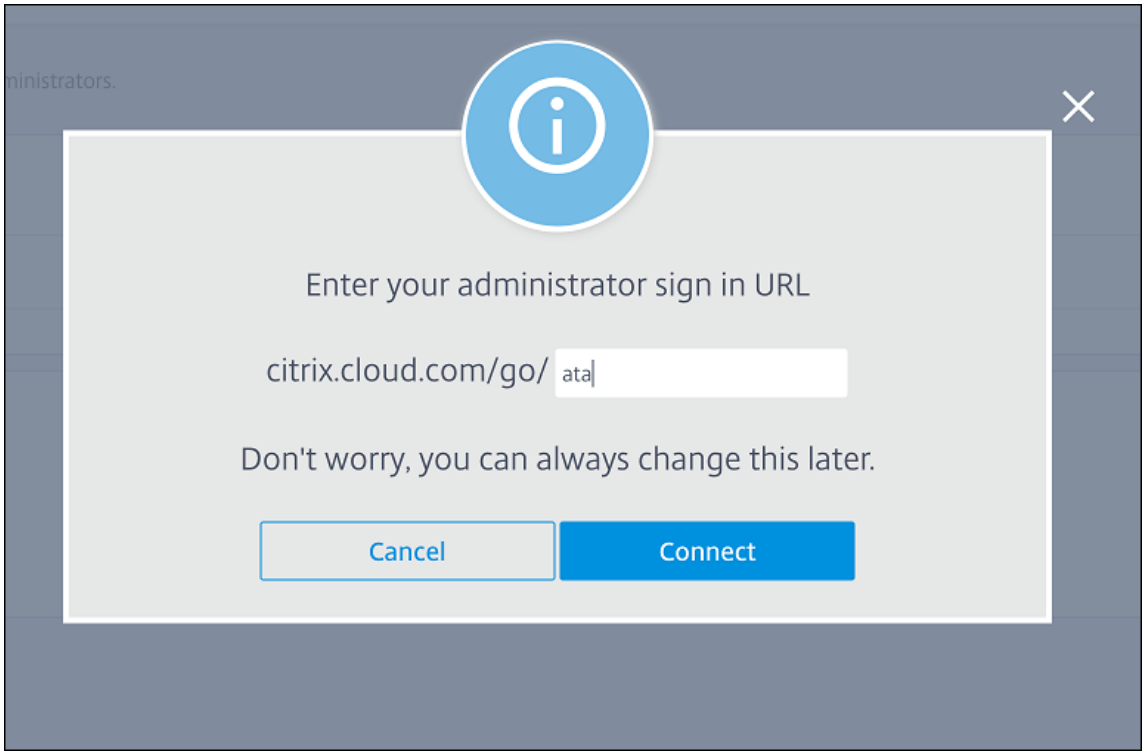
Voraussetzungen

- Azure Active Directory-Benutzeranmeldeinformationen
- Benutzergruppen in Active Directory müssen mit den Benutzergruppen in Azure Active Directory übereinstimmen.
- Benutzernamen und E-Mail-Adressen in Active Directory müssen mit den Benutzernamen und E-Mail-Adressen im Azure Active Directory übereinstimmen.
- Citrix Cloud-Konto mit installiertem Citrix Cloud Connector für die Synchronisierung der Verzeichnisdienste
- NetScaler Gateway. Citrix empfiehlt, dass Sie entweder die zertifikatsbasierte Authentifizierung oder Azure AD für eine komplette Single Sign-On-Erfahrung aktivieren. Wenn Sie die LDAP-Authentifizierung für das NetScaler Gateway für die MAM-Registrierung verwenden, erhalten Endbenutzer bei der Registrierung zwei Authentifizierungsanforderungen. Weitere Informationen finden Sie unter Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne.
- Legen Sie in Registrierungsprofilen für Android Enterprise die Option **Benutzer dürfen Geräteverwaltung ablehnen** auf **Aus** fest. Wenn Benutzer die Geräteverwaltung ablehnen, können sie sich bei der Authentifizierung nicht mit einem Identitätsanbieter registrieren. Weitere Informationen finden Sie unter Registrierungssicherheit.

Konfigurieren von Azure Active Directory als Identitätsanbieter (IdP) in Citrix Cloud

Um diesen Dienst für die Verwendung mit Citrix Secure Hub einzurichten, konfigurieren Sie Azure Active Directory in Citrix Cloud.

1. Melden Sie sich unter https://citrix.cloud.com an Ihrem Citrix Cloud-Konto an.
2. Stellen Sie im Citrix Cloud-Menü auf der Seite **Identitäts- und Zugriffsverwaltung** eine Verbindung mit Azure Active Directory her.
3. Geben Sie Ihre Administrator-Anmelde-URL ein und klicken Sie auf **Verbinden**.



4. Nach der Anmeldung wird Ihr Azure Active Directory-Konto mit Citrix Cloud verbunden. Auf der Seite **Identitäts- und Zugriffsverwaltung > Authentifizierung** sehen Sie, mit welchen Konten Sie sich bei den Citrix Cloud- und Azure AD-Konten anmelden.
5. Um die Authentifizierung mit Azure AD für Benutzer zu aktivieren, die sich über Citrix Secure Hub registrieren, wählen Sie unter **Workspacekonfiguration > Authentifizierung** die Option **Azure Active Directory**. Nach Abschluss der Konfiguration können Sie Benutzergeräte über Citrix Secure Hub registrieren.

Konfigurieren der Citrix-Identität als IdP-Typ für Citrix Endpoint Management

Diese Konfiguration gilt nur für Benutzer, die sich über Citrix Secure Hub registrieren. Nach dem Konfigurieren von Azure Active Directory in Citrix Cloud konfigurieren Sie Citrix Endpoint Management

wie nachfolgend beschrieben.

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Identitätsanbieter (IdP)** und klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie auf der Seite **Identitätsanbieter (IdP)** folgende Einstellungen:
   - **IdP-Name:** Geben Sie einen eindeutigen Namen für die IdP-Verbindung ein, die Sie erstellen.
   - **IdP-Typ:** Wählen Sie **Citrix-Identitätsplattform**.
   - **Auth-Domäne:** Wählen Sie **Azure Active Directory**. Diese Domäne entspricht der Identitätsanbieterdomäne auf der Seite **Workspacekonfiguration > Authentifizierung** in Citrix Cloud.
3. Klicken Sie auf **Weiter**. Konfigurieren Sie folgende Einstellungen auf der Seite **IdP-Anspruchsverwendung**:
   - **Benutzer-ID-Typ:** Dieses Feld ist standardmäßig auf **userPrincipalName** festgelegt. Stellen Sie sicher, dass Sie alle Benutzer im on-premises Active Directory und in Azure Active Directory mit derselben ID konfigurieren. Citrix Endpoint Management verwendet diese ID, um Benutzer im Identitätsanbieter den on-premises Active Directory-Benutzern zuzuordnen.
   - **Benutzer-ID-Zeichenfolge:** Dieses Feld wird automatisch ausgefüllt.
4. Klicken Sie auf **Weiter**, lesen Sie die **Zusammenfassung** und klicken Sie auf **Speichern**.

   Benutzer von Citrix Secure Hub, der Citrix Endpoint Management-Konsole und des Selbsthilfeportals können sich jetzt mit ihren Azure Active Directory-Anmeldeinformationen anmelden. Domänengebundene Citrix Secure Hub-Benutzer können sich über Citrix Secure Hub mit ihren Azure AD-Anmeldeinformationen anmelden. Citrix Secure Hub verwendet die Clientzertifikat-Authentifizierung für MAM-Geräte.

Verfahren zur Authentifizierung in Citrix Secure Hub

Citrix Endpoint Management verwendet das folgende Verfahren, um Benutzer mit Azure AD als Identitätsanbieter auf Geräten zu authentifizieren, die über Citrix Secure Hub registriert sind:

1. Ein Benutzer startet Citrix Secure Hub.
2. Die Authentifizierungsanforderung wird von Citrix Secure Hub an die Citrix-Identität und von dort an Azure Active Directory geleitet.
3. Der Benutzer gibt den Benutzernamen und das Kennwort für Azure Active Directory ein.
4. Azure Active Directory überprüft den Benutzer und sendet einen Code an die Citrix-Identität.
5. Die Citrix-Identität sendet den Code an Citrix Secure Hub, von wo er an den Citrix Endpoint Management-Server weitergeleitet wird.

6. Citrix Endpoint Management fordert mit dem Code und dem geheimen Schlüssel einen ID-Token an und überprüft die Benutzerinformationen im ID-Token. Citrix Endpoint Management gibt eine Sitzungs-ID zurück.

Authentifizierung mit Azure Active Directory über NetScaler Gateway für die MAM-Registrierung

June 25, 2024

Citrix Endpoint Management unterstützt die Authentifizierung mit Azure Active Directory (Azure AD)-Anmeldeinformationen über NetScaler Gateway. Diese Authentifizierungsmethode ist nur für Benutzer verfügbar, die sich über Citrix Secure Hub bei MAM registrieren.

Voraussetzungen

Um Citrix Endpoint Management so zu konfigurieren, dass Azure AD über NetScaler Gateway als Identitätsanbieter (IdP) für Geräte verwendet wird, die mit MAM registriert wurden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Konfigurieren Sie Citrix Endpoint Management mit Azure AD über Citrix Cloud als Identitätsanbieter für Geräte, die mit MDM registriert sind. Weitere Informationen zur Konfiguration von Azure AD für MDM finden Sie unter Authentifizierung mit Azure Active Directory über Citrix Cloud.
- Verbinden Sie Azure AD mit Citrix Cloud. Weitere Informationen finden Sie unter Verbinden von Azure Active Directory mit Citrix Cloud.
- Aktivieren Sie je nach Plattform die folgenden entsprechenden Featureflags:
  - iOS:
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android:
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

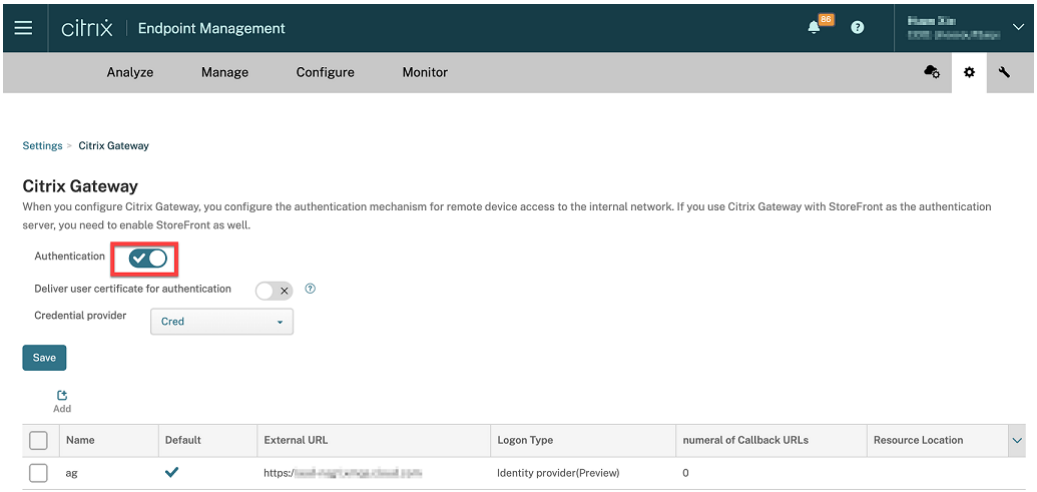
  > **Hinweis:**
  >
  > Um das entsprechende Featureflag in Ihrer Umgebung zu aktivieren, füllen Sie das Podio-Formular aus.

- Für Android aktivieren Sie **Android Enterprise**.

> **Hinweis:**
>
> Dieses Feature wurde unter dem Legacymodus “Android Device Administrator”(DA) nicht getestet oder überprüft. Dieser Modus wird nicht unterstützt.

Azure AD für MAM als Identitätsanbieter konfigurieren

1. Konfigurieren Sie NetScaler Gateway in Citrix Endpoint Management wie folgt:
   a) Melden Sie sich an der Citrix Endpoint Management-Konsole an und klicken Sie dann auf das Symbol **Einstellungen** .
   b) Klicken Sie unter **Server** auf **NetScaler Gateway**.
   c) Aktivieren Sie die Umschalttaste **Authentifizierung**.



   d) Stellen Sie sicher, dass der **Anmeldetyp** des Gateways *Identitätsanbieter* ist.
   e) Klicken Sie auf **Speichern**.
2. Konfigurieren Sie Azure AD als SAML-Identitätsanbieter mit Azure AD als SAML IdP konfigurieren.
3. Konfigurieren Sie NetScaler ADC als SAML-Dienstanbieter mit der erweiterten Richtlinie mithilfe der Anleitungen unter NetScaler ADC als SAML SP konfigurieren.
4. Erstellen Sie einen virtuellen AAA-Server mit So richten Sie einen virtuellen Authentifizierungsserver über die GUI ein.
5. Konfigurieren Sie den virtuellen AAA-Server mit Konfigurieren des virtuellen Authentifizierungsservers.
6. Erstellen und konfigurieren Sie das Authentifizierungsprofil mithilfe von Authentifizierungsprofilen.

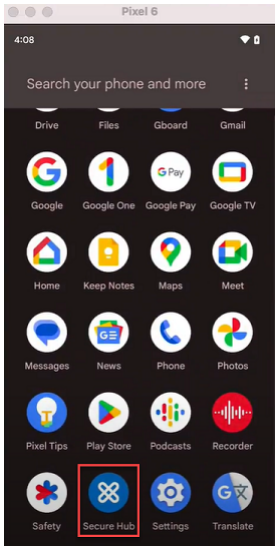
7. Verbinden Sie das Authentifizierungsprofil mit dem virtuellen Gateway-Server und speichern Sie alle Konfigurationen.

Jetzt wird Azure AD als Identitätsanbieter für mit MAM registrierte Geräte hinzugefügt und Sie können sie mit Azure AD authentifizieren.

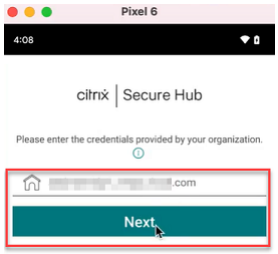
Erwartetes Verhalten

Das folgende Beispiel verwendet ein Android-Gerät:

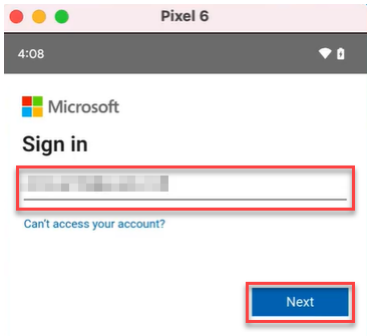
1. Öffnen Sie auf Ihrem Mobilgerät die Citrix Secure Hub-App.



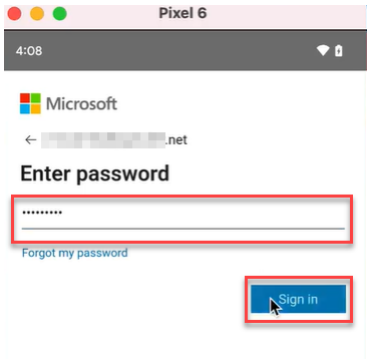
2. Geben Sie die erforderlichen Berechtigungen an.
3. Geben Sie auf der Anmeldeseite die von Ihrer Organisation bereitgestellten Anmeldeinformationen ein und tippen Sie dann auf **Weiter**.



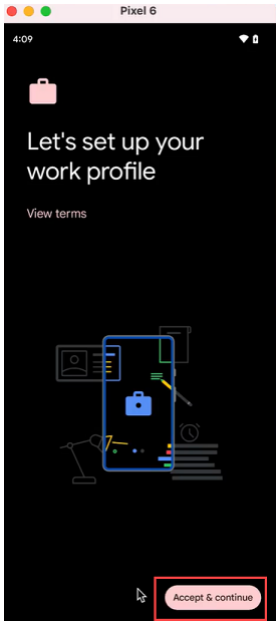
   Sie werden zur Microsoft-Anmeldeseite weitergeleitet.
4. Geben Sie auf der Microsoft-Anmeldeseite Ihre E-Mail-Adresse ein und tippen Sie dann auf **Weiter**.



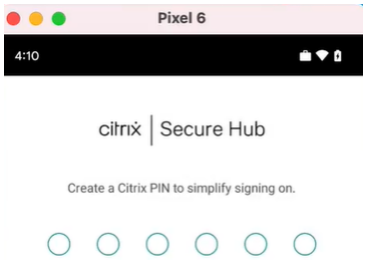
5. Geben Sie das Kennwort ein und tippen Sie dann auf **Anmelden**.



6. Tippen Sie auf der Seite **Let's set up your work profile** auf **Accept & continue**.



7. Erstellen Sie die PIN für die Citrix Secure Hub-App und bestätigen Sie diese.



Sie werden zur Citrix Secure Hub-Homepage weitergeleitet.

Authentifizierung mit Okta über Citrix Cloud

June 25, 2024

Citrix Endpoint Management unterstützt die Authentifizierung mit Okta-Anmeldeinformationen über Citrix Cloud. 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 Okta-Anmeldeinformationen über Citrix Cloud authentifizieren. Um Citrix Secure Hub mit MDM+MAM zu verwenden, konfigurieren Sie Citrix Endpoint Management zur Verwendung von NetScaler Gateway für die MAM-Registrierung. Weitere Informationen finden Sie unter NetScaler Gateway und Citrix Endpoint Management.

Citrix Endpoint Management verwendet den Citrix Cloud-Service Citrix Identität für den Verbindungsaufbau mit Okta. Citrix empfiehlt, dass Sie den Citrix-Identitätsanbieter und keine direkte Verbindung mit Okta verwenden.

Citrix Endpoint Management unterstützt die Authentifizierung bei Okta für die folgenden Plattformen:

- iOS- und macOS-Geräte, die nicht im Apple Business Manager oder Apple School Manager registriert sind
- iOS- und macOS-Geräte, die im Apple Business Manager registriert sind
- Android Enterprise-Geräte (Preview) im BYOD- und vollständig verwalteten Modus

Für die Authentifizierung bei Okta über Citrix Cloud gelten folgende Einschränkungen:

- Nicht für lokale Citrix Endpoint Management-Konten verfügbar.
- Unterstützt keine Authentifizierung mit Okta für Registrierungseinladungen. Wenn Sie eine Registrierungseinladung mit einer Registrierungs-URL senden, authentifizieren sich die Benutzer über LDAP anstelle von Okta.

Voraussetzungen

- Okta-Benutzeranmeldeinformationen
- Benutzergruppen in Active Directory müssen mit den Benutzergruppen in Okta übereinstimmen.
- Benutzernamen und E-Mail-Adressen im Active Directory müssen mit den Benutzernamen und E-Mail-Adressen bei Okta übereinstimmen.
- Citrix Cloud-Konto mit installiertem Citrix Cloud Connector für die Synchronisierung der Verzeichnisdienste
- NetScaler Gateway. Citrix empfiehlt die Aktivierung der zertifikatbasierten Authentifizierung für die komplette Single-Sign-On-Erfahrung. Wenn Sie die LDAP-Authentifizierung für das NetScaler Gateway für die MAM-Registrierung verwenden, erhalten Endbenutzer bei der Registrierung zwei Authentifizierungsanforderungen. Weitere Informationen finden Sie unter Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne.
- Legen Sie in Registrierungsprofilen für Android Enterprise die Option **Benutzer dürfen Geräteverwaltung ablehnen** auf **Aus** fest. Wenn Benutzer die Geräteverwaltung ablehnen, können sie sich bei der Authentifizierung nicht mit einem Identitätsanbieter registrieren. Weitere Informationen finden Sie unter Registrierungssicherheit.

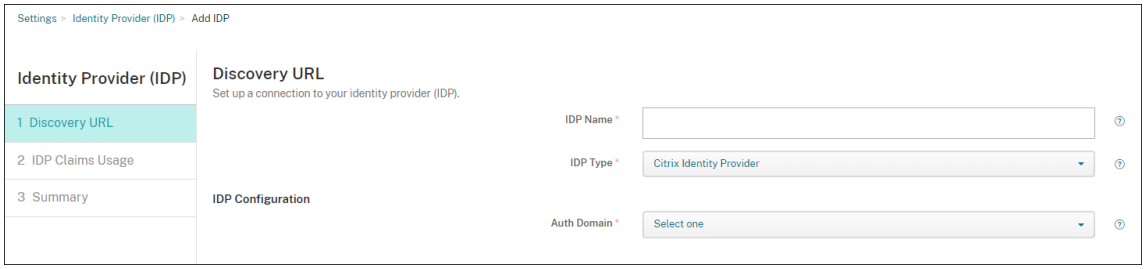
Konfigurieren von Okta als Identitätsanbieter in Citrix Cloud

Informationen zum Konfigurieren von Okta in Citrix Cloud finden Sie unter Verbinden von Okta als Identitätsanbieter mit Citrix Cloud.

Konfigurieren der Citrix-Identität als IdP-Typ für Citrix Endpoint Management

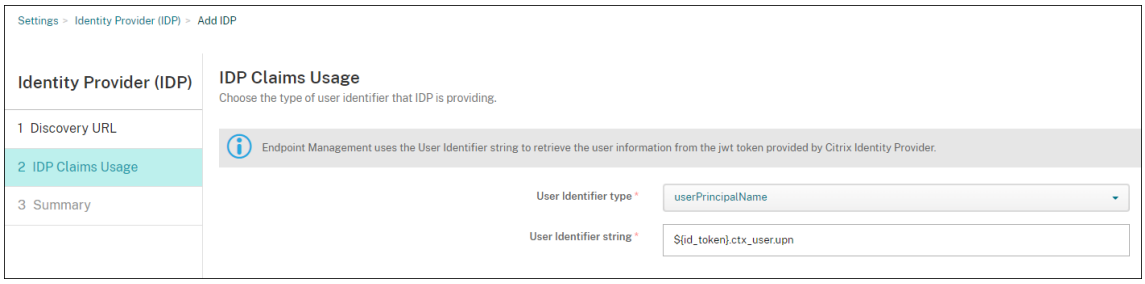
Diese Konfiguration gilt nur für Benutzer, die sich über Citrix Secure Hub registrieren. Nach dem Konfigurieren von Azure Active Directory in Citrix Cloud konfigurieren Sie Citrix Endpoint Management wie nachfolgend beschrieben:

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Identitätsanbieter (IdP)** und klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie auf der Seite **Identitätsanbieter (IdP)** folgende Einstellungen:



- **IdP-Name:** Geben Sie einen eindeutigen Namen für die IdP-Verbindung ein, die Sie erstellen.
- **IdP-Typ:** Wählen Sie **Citrix-Identitätsanbieter**.
- **Auth-Domäne:** Wählen Sie die Citrix Cloud-Domäne. Angaben zu Ihrer Domäne finden Sie bei Bedarf in Citrix Cloud auf der Seite **Identitäts- und Zugriffsverwaltung > Authentifizierung**.

3. Klicken Sie auf **Weiter**. Konfigurieren Sie folgende Einstellungen auf der Seite **IdP-Anspruchsverwendung**:



- **Benutzer-ID-Typ:** Dieses Feld ist auf **userPrincipalName** festgelegt. Stellen Sie sicher, dass Sie alle Benutzer im on-premises Active Directory und in Okta mit derselben ID konfigurieren. Citrix Endpoint Management verwendet diese ID, um Benutzer im Identitätsanbieter den on-premises Active Directory-Benutzern zuzuordnen.
- **Benutzer-ID-Zeichenfolge:** Dieses Feld wird automatisch ausgefüllt.

Nach dieser Konfiguration können domänengebundene Citrix Secure Hub-Benutzer sich über Citrix Secure Hub mit ihren Okta-Anmeldeinformationen anmelden. Citrix Secure Hub verwendet die Clientzertifikat-Authentifizierung für MAM-Geräte.

Verfahren zur Authentifizierung in Citrix Secure Hub

Citrix Endpoint Management verwendet das folgende Verfahren, um Benutzer mit Okta als Identitätsanbieter auf Geräten zu authentifizieren, die über Citrix Secure Hub registriert sind:

1. Ein Benutzer startet Citrix Secure Hub.
2. Die Authentifizierungsanforderung wird von Citrix Secure Hub an die Citrix-Identität und von dort an Okta geleitet.
3. Der Benutzer gibt den Benutzernamen und das Kennwort ein.
4. Okta überprüft den Benutzer und sendet einen Code an die Citrix-Identität.
5. Die Citrix-Identität sendet den Code an Citrix Secure Hub, von wo er an den Citrix Endpoint Management-Server weitergeleitet wird.
6. Citrix Endpoint Management fordert mit dem Code und dem geheimen Schlüssel einen ID-Token an und überprüft die Benutzerinformationen im ID-Token. Citrix Endpoint Management gibt eine Sitzungs-ID zurück.

Authentifizierung mit Okta über NetScaler Gateway für die MAM-Registrierung

June 25, 2024

Citrix Endpoint Management unterstützt die Authentifizierung mit Okta-Anmeldeinformationen über NetScaler Gateway. Diese Authentifizierungsmethode ist nur für Benutzer verfügbar, die sich über Citrix Secure Hub bei MAM registrieren.

Voraussetzungen

Um Citrix Endpoint Management so zu konfigurieren, dass Okta über NetScaler Gateway als Identitätsanbieter (IdP) für Geräte verwendet wird, die mit MAM registriert wurden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Konfigurieren Sie Citrix Endpoint Management mit Okta über Citrix Cloud als Identitätsanbieter für Geräte, die mit MDM registriert sind. Weitere Informationen zur Konfiguration von Okta für MDM finden Sie unter Authentifizierung mit Okta über Citrix Cloud.
- Aktivieren Sie je nach Plattform die folgenden entsprechenden Featureflags:
  - iOS:
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android:
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

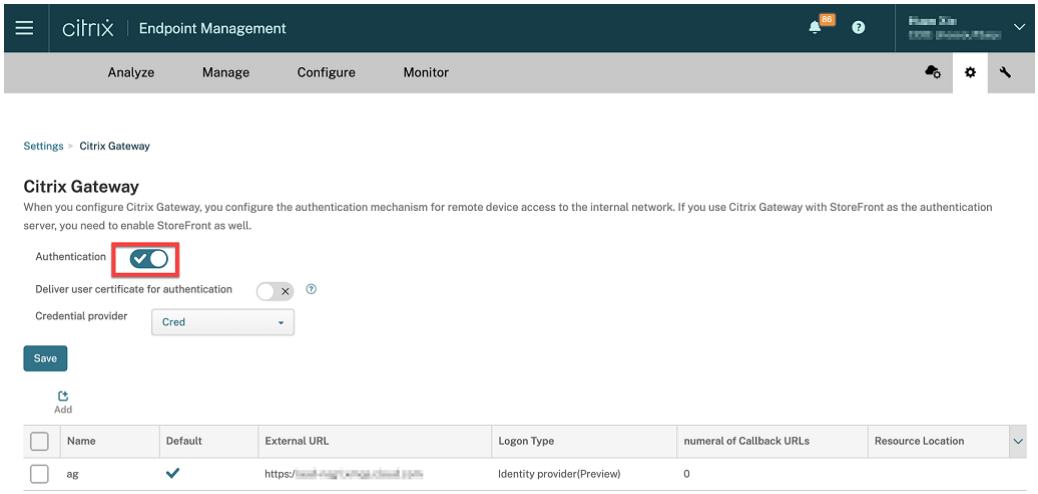
> **Hinweis:**
>
> Um das entsprechende Featureflag in Ihrer Umgebung zu aktivieren, füllen Sie das Podio-Formular aus.

- Laden Sie die neueste Version von Citrix Secure Hub herunter und installieren Sie sie.
- Stellen Sie sicher, dass der Okta-Dienst für Ihre Organisation verfügbar ist und die entsprechenden Benutzer und Gruppen erstellt oder in Okta importiert wurden.

NetScaler Gateway in Citrix Endpoint Management konfigurieren

1. Melden Sie sich an der Citrix Endpoint Management-Konsole an und klicken Sie dann auf das Symbol **Einstellungen** .

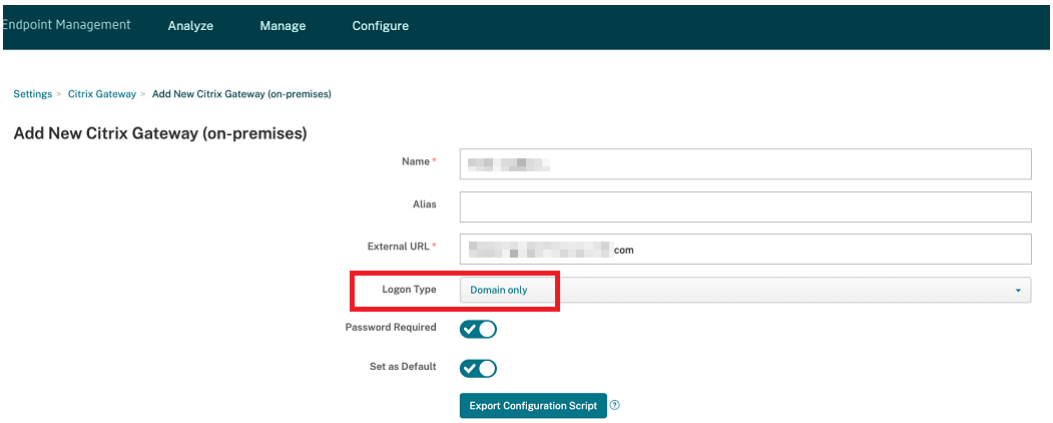
2. Klicken Sie unter **Server** auf **NetScaler Gateway**.
3. Aktivieren Sie die Umschalttaste **Authentifizierung**.



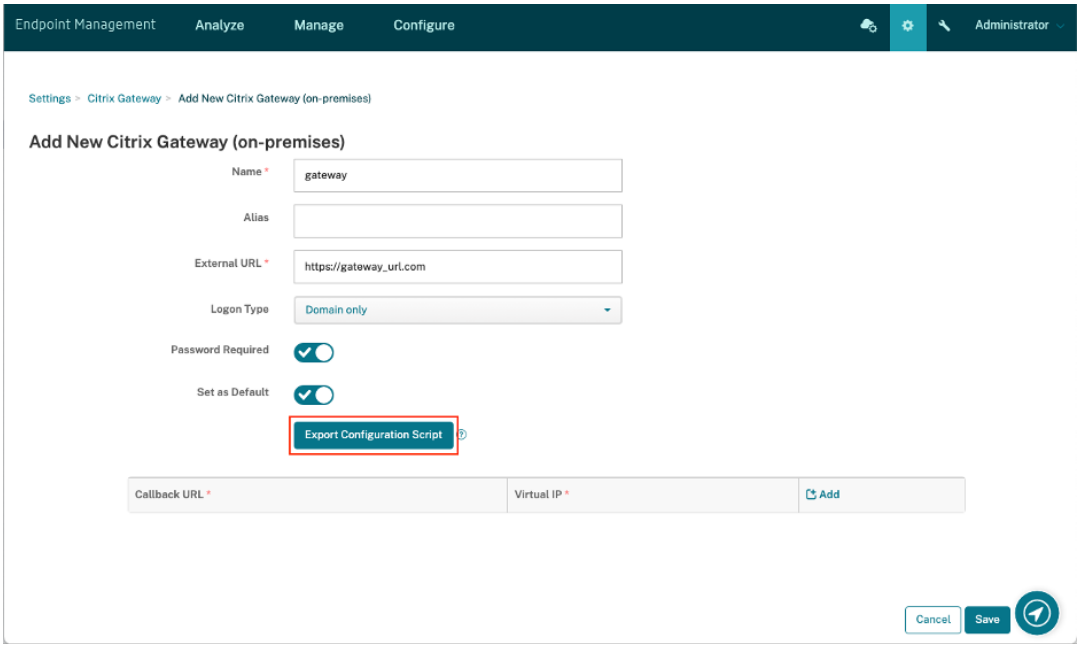
4. Stellen Sie sicher, dass der **Anmeldetyp** des Gateways *Identitätsanbieter* ist.
5. Klicken Sie auf **Speichern**.

On-Premises NetScaler Gateway vorbereiten

1. Wenn Sie kein on-premises NetScaler Gateway für Citrix Endpoint Management konfiguriert haben, führen Sie die folgenden Schritte aus:
   a) Klicken Sie in der Citrix Endpoint Management-Konsole auf das Symbol **Einstellungen** .
   b) Klicken Sie unter **Server** auf **NetScaler Gateway**.
   c) Klicken Sie auf **Bearbeiten**.
   d) Klicken Sie auf das Dropdownmenü **Anmeldetyp** und wählen Sie *Nur Domäne*.

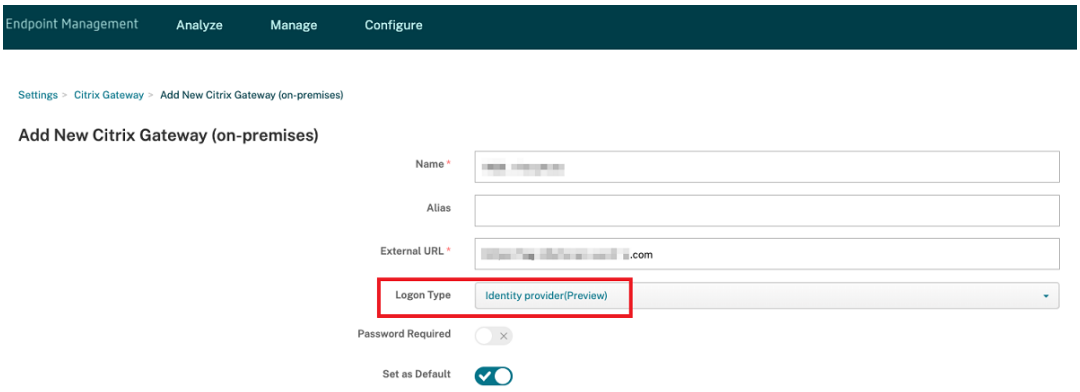


e) Klicken Sie auf **Konfigurationsskript exportieren**.



Das **Konfigurationsscript** wird heruntergeladen.

f) Klicken Sie auf das Dropdownmenü **Anmeldetyp** und wählen Sie *Identitätsanbieter*.



g) Klicken Sie auf **Speichern**.

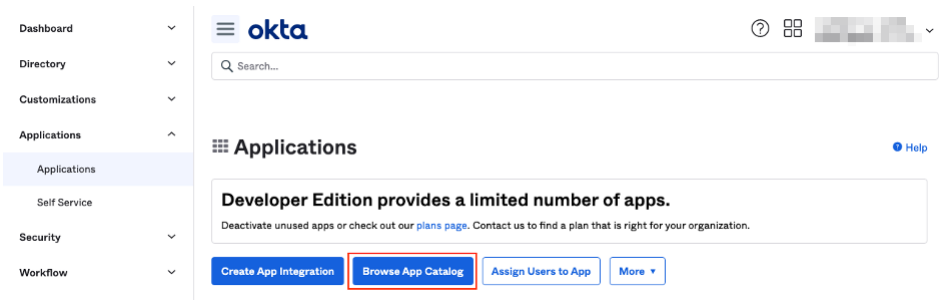
h) Öffnen Sie die heruntergeladene ZIP-Datei und extrahieren Sie die Dateien.

i) Führen Sie die Skripts in den extrahierten TXT-Dateien aus, um das on-premises NetScaler Gateway vorzubereiten.

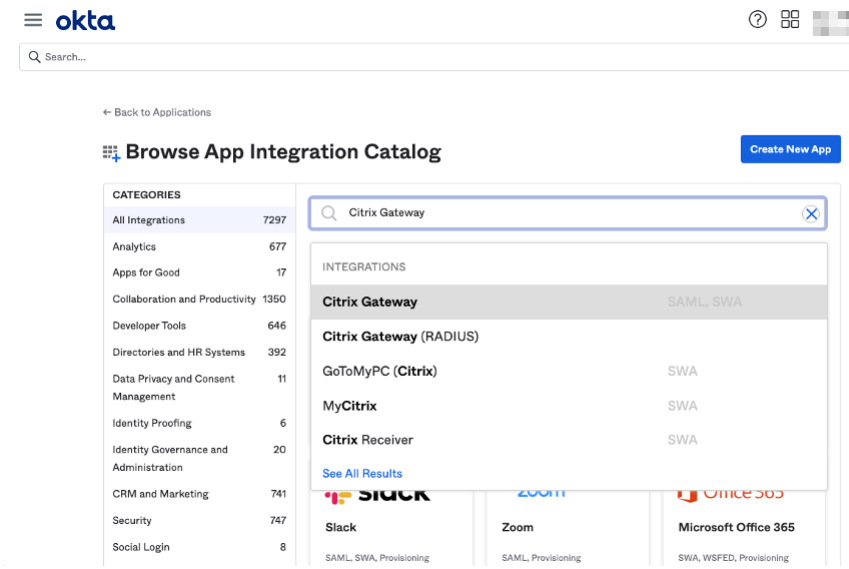
2. Melden Sie sich an der Citrix ADC-Verwaltungskonsole an und navigieren Sie dann zu **NetScaler Gateway** > **Virtuelle Server**.
3. Klicken Sie auf das Gateway, das für Ihre Citrix Endpoint Management-Einrichtung relevant ist.
4. Heben Sie die Bindung aller vorhandenen Authentifizierungsrichtlinien auf dem on-premises NetScaler Gateway auf.

Okta konfigurieren

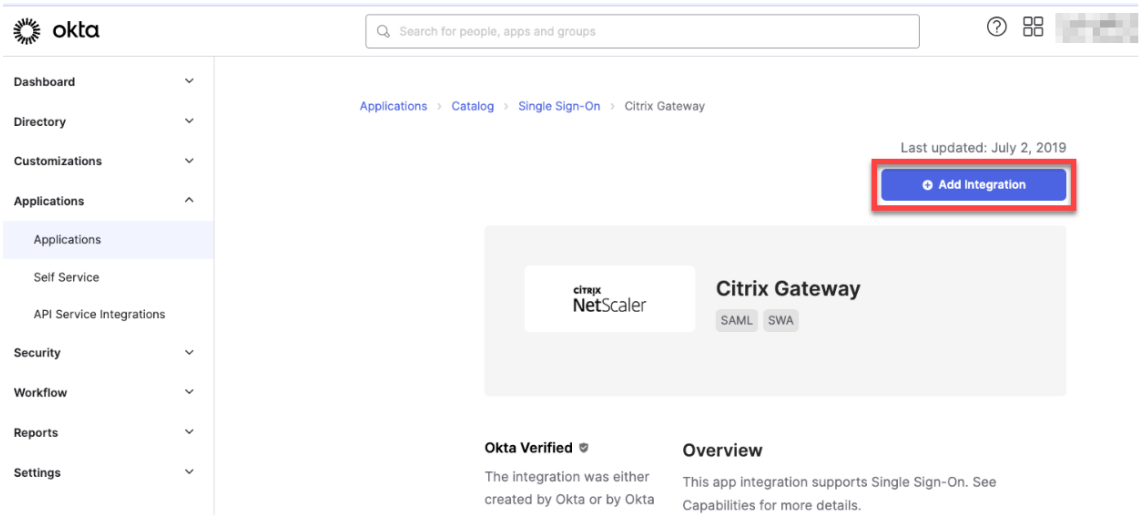
1. Melden Sie sich bei Okta als Administrator an.
2. Klicken Sie auf **Applications** > **Applications** > **Browse App Catalog**.



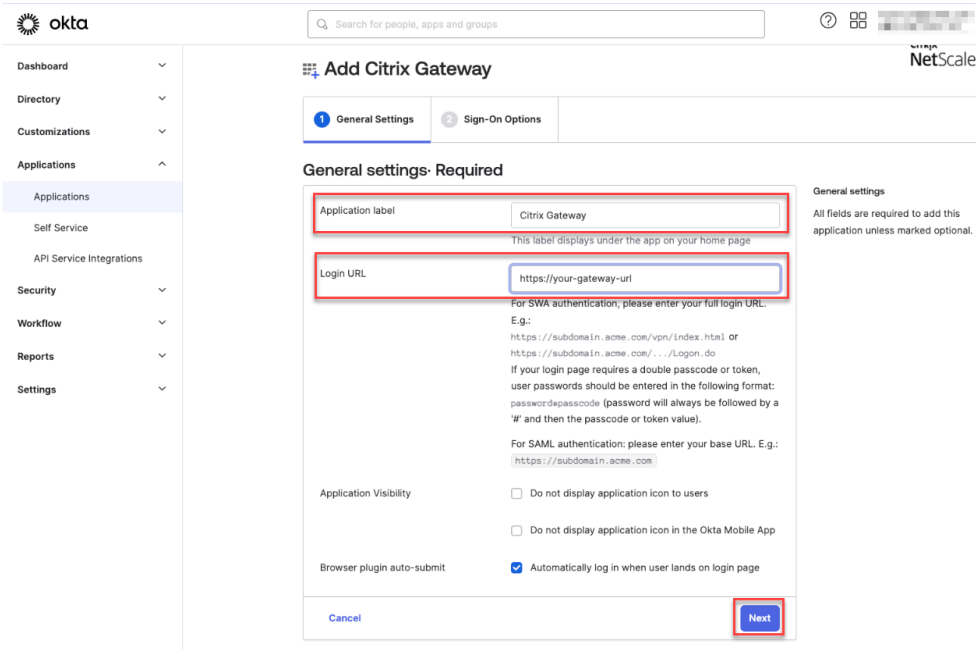
3. Geben Sie **NetScaler Gateway** in die Suchleiste unter **Browse App Integration Catalog** ein und wählen Sie dann **NetScaler Gateway (SAML, SWA)**.



4. Klicken Sie auf **Add Integration**.

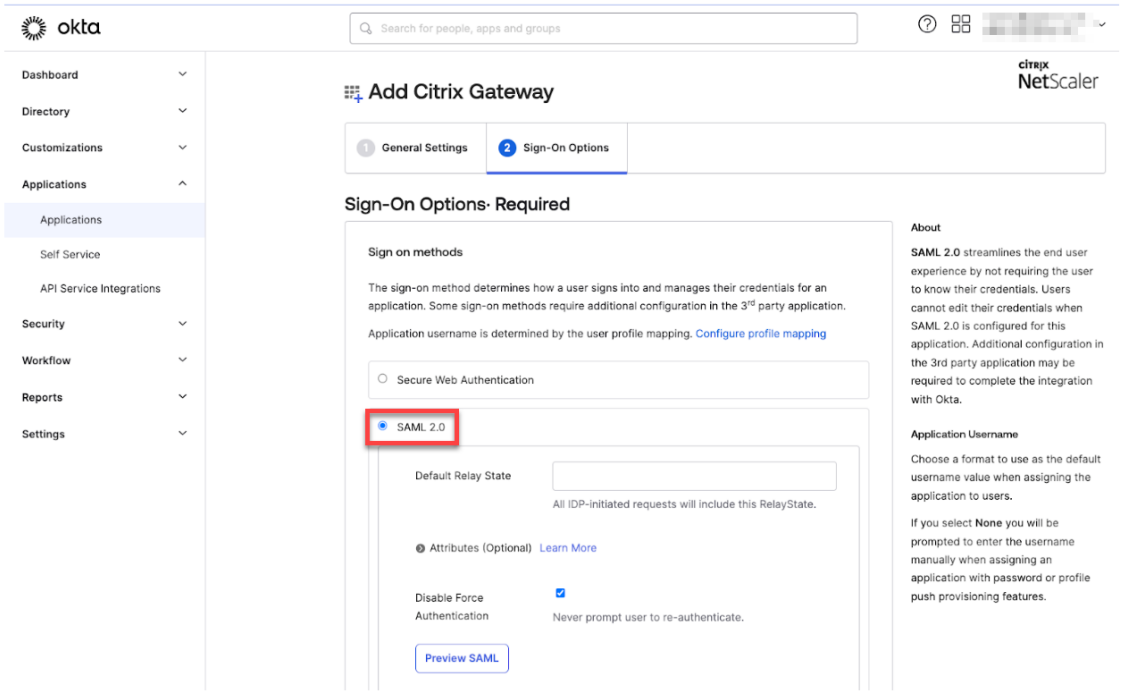


5. Geben Sie den entsprechenden Namen in das Feld **Application label** ein.
6. Geben Sie die URL des virtuellen Gateway-Servers in das Feld **Login URL** ein und klicken Sie dann auf **Next**.

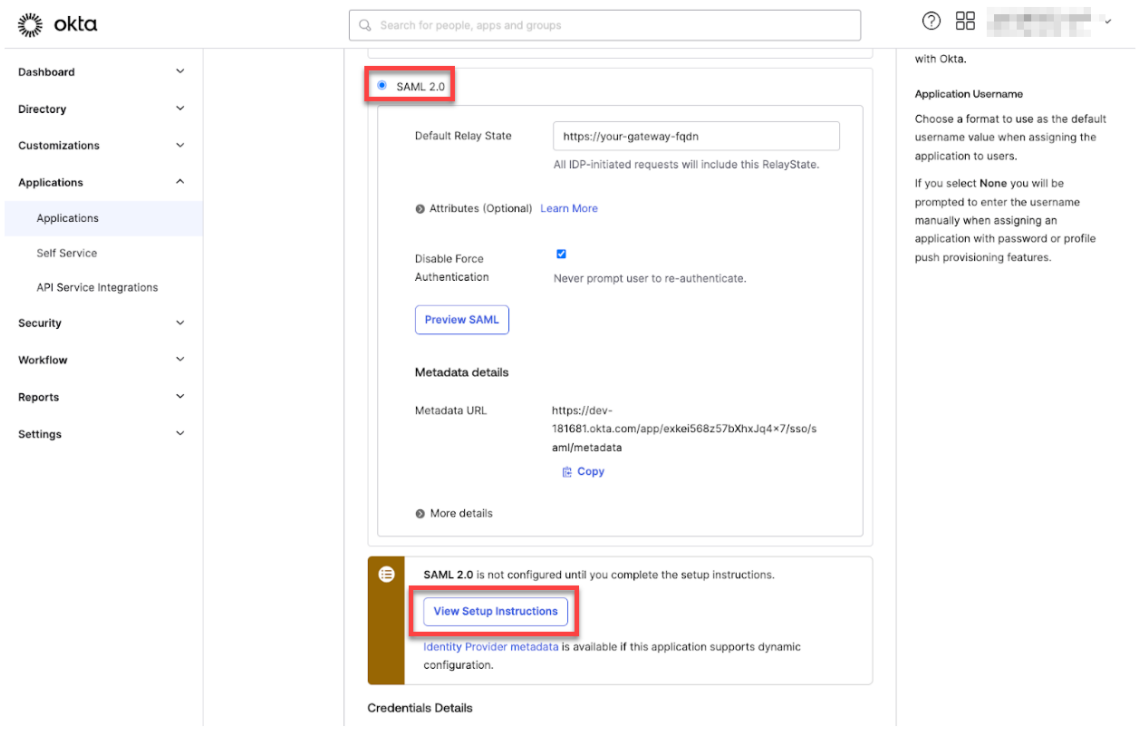


> **Hinweis:**
>
> Die im Feld **Login URL** eingegebene URL muss mit der NetScaler Gateway-URL für Citrix Endpoint Management-Einstellungen übereinstimmen.

7. Wählen Sie unter **Sign-On Options Required** > **Sign on methods** die Option **SAML 2.0**.



8. Klicken Sie auf **View Setup Instructions** und folgen Sie den Anweisungen auf der Seite, um die SAML-Richtlinie in der Citrix On-Premises-Gateway-Administratorkonsole zu erstellen.



Hinweis:

- Nach der Installation des Zertifizierungsstellenzertifikats bei der Konfiguration von NetScaler Gateway, Version 11.1 oder höher, erstellen Sie eine SAML-Aktion. Um eine SAML-Aktion zu erstellen, navigieren Sie zu **Security** > **AAA - Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **Actions** > **SAML Actions**. Klicken Sie auf **Add** und geben Sie die Informationen ein, die auf der vorhergehenden Seite angegeben sind. Folgen Sie nicht der auf der Seite angegebenen Navigation, d. h. **Netscaler Gateway** > **Policies** > **Authentication** > **SAML** > **Servers**.
- Folgen Sie auch nicht den angegebenen Schritten zum Erstellen einer SAML-Richtlinie, da diese Schritte die klassische Richtlinie verwenden. Wir verwenden jetzt die erweiterte Richtlinie. Führen Sie den folgenden Schritt 9 aus, um eine SAML-Richtlinie mit einer erweiterten Richtlinie zu erstellen.

9. Erstellen Sie eine entsprechende SAML-Richtlinie für die SAML-Aktion, und binden Sie die Richtlinie wie folgt an den virtuellen Authentifizierungsserver:

   a) Navigieren Sie zu **Security** > **AAA-Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** und klicken Sie auf **Add**.

   b) Geben Sie auf der Seite “Create Authentication Policy”die folgenden Details an:

      - **Name** - Geben Sie einen Namen für die SAML-Richtlinie an.
      - **Action Type** - Wählen Sie *SAML* als Authentifizierungsaktionstyp aus.

- **Action** - Wählen Sie das SAML-Serverprofil aus, an das die SAML-Richtlinie gebunden werden soll.
- **Expression** - Zeigt den Namen der Regel oder des Ausdrucks an, den die SAML-Richtlinie verwendet, um zu bestimmen, ob sich der Benutzer beim SAML-Server authentifizieren muss. Legen Sie im Textfeld den Wert **rule** = `true` fest, damit die SAML-Richtlinie wirksam wird und die entsprechende SAML-Aktion ausgeführt wird.

c) Binden Sie die SAML-Richtlinie an den virtuellen VPN-Server und verknüpfen Sie den virtuellen VPN-Server mit dem virtuellen Authentifizierungsserver über ein Authentifizierungsprofil. Weitere Informationen zum Bindungsvorgang finden Sie unter Authentifizierungsrichtlinie binden.

10. Erstellen Sie einen virtuellen AAA-Server mit So richten Sie einen virtuellen Authentifizierungsserver über die GUI ein.
11. Konfigurieren Sie den virtuellen AAA-Server mit Konfigurieren des virtuellen Authentifizierungsservers.
12. Erstellen und konfigurieren Sie das Authentifizierungsprofil mithilfe von Authentifizierungsprofilen.
13. Verbinden Sie das Authentifizierungsprofil mit dem virtuellen Gateway-Server und speichern Sie alle Konfigurationen.
14. Nachdem Sie die SAML-Richtlinie in der Administratorkonsole des Citrix on-premises-Gateways erstellt haben, klicken Sie auf “Done”.

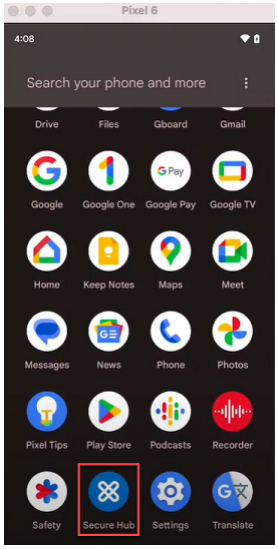
    Jetzt müssen Sie in der Lage sein, zwei Anwendungen für die Citrix Endpoint Management-Integration zu sehen, eine Webanwendung für Citrix Cloud und eine SAML-Anwendung für die Citrix Endpoint Management MAM-Authentifizierung.
15. Weisen Sie der soeben erstellten SAML-Anwendung die entsprechenden Benutzer und Gruppen zu.

Jetzt wird Okta als Identitätsanbieter für mit MAM registrierte Geräte hinzugefügt, und Sie können sie mit Okta authentifizieren.

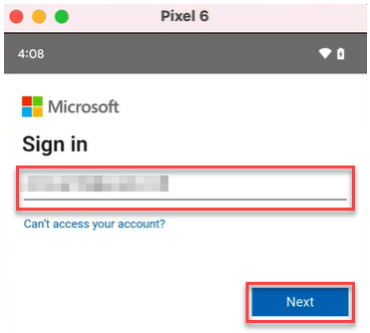
Erwartetes Verhalten

Das folgende Beispiel verwendet ein Android-Gerät:

1. Öffnen Sie auf Ihrem Mobilgerät die Citrix Secure Hub-App.

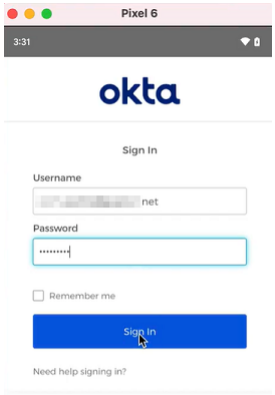


2. Geben Sie die erforderlichen Berechtigungen an.
3. Geben Sie auf der Anmeldeseite die von Ihrer Organisation bereitgestellten Anmeldeinformationen ein und tippen Sie dann auf **Weiter**.

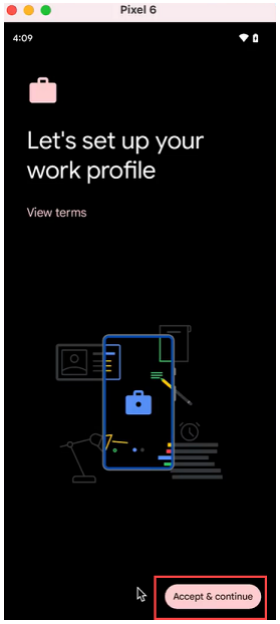


Sie werden zur Okta-Anmeldeseite weitergeleitet.

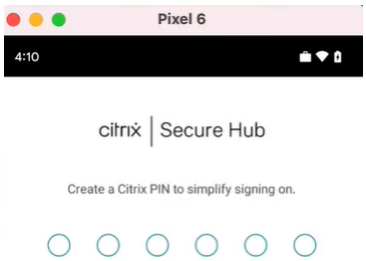
4. Geben Sie auf der Okta-Anmeldeseite Ihre Anmeldeinformationen ein und tippen Sie dann auf **Anmelden**.



5. Tippen Sie auf der Seite **Let's set up your work profile** auf **Accept & continue**.



6. Erstellen Sie die PIN für die Citrix Secure Hub-App und bestätigen Sie diese.



Sie werden zur Citrix Secure Hub-Homepage weitergeleitet.

Authentifizierung mit einem On-Premises-NetScaler Gateway über Citrix Cloud

June 25, 2024

Citrix Endpoint Management unterstützt die Authentifizierung mit einem On-Premises-NetScaler Gateway über Citrix Cloud. 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 den Anmeldeinformationen eines On-Premises-NetScaler Gateway über Citrix Cloud authentifizieren. Um Citrix Secure Hub mit MDM+MAM zu verwenden, konfigurieren Sie Citrix Endpoint Management zur Verwendung von NetScaler Gateway für die MAM-Registrierung. Weitere Informationen finden Sie unter NetScaler Gateway und Citrix

Endpoint Management.

Citrix Endpoint Management unterstützt die Authentifizierung mit einem On-Premises-NetScaler Gateway über Citrix Cloud für die folgenden Plattformen:

- iOS-Geräte
- Android Enterprise-Geräte im BYOD- und vollständig verwalteten Modus

> **Hinweis:**
>
> Citrix Endpoint Management unterstützt keine Authentifizierung mit On-Premises-NetScaler Gateway über Citrix Cloud für Registrierungseinladungen. Wenn Sie Benutzern eine Registrierungseinladung mit einer Registrierungs-URL senden, authentifizieren sie sich über LDAP anstelle eines On-Premises-NetScaler Gateway als Identitätsanbieter.

Citrix empfiehlt die Aktivierung der zertifikatbasierten Authentifizierung für die komplette Single-Sign-On-Erfahrung. Wenn Sie die LDAP-Authentifizierung für das NetScaler Gateway für die MAM-Registrierung verwenden, erhalten Endbenutzer bei der Registrierung zwei Authentifizierungsanforderungen. Weitere Informationen finden Sie unter Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne.

Voraussetzungen

- NetScaler Gateway. Citrix empfiehlt die Aktivierung der zertifikatbasierten Authentifizierung für die komplette Single-Sign-On-Erfahrung. Wenn Sie die LDAP-Authentifizierung für das NetScaler Gateway für die MAM-Registrierung verwenden, erhalten Endbenutzer bei der Registrierung zwei Authentifizierungsanforderungen. Weitere Informationen finden Sie unter Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne.
- Citrix Cloud-Konto mit installiertem Citrix Cloud Connector für die Synchronisierung der Verzeichnisdienste
- Citrix Secure Hub 20.5.0 und höher.

Konfigurieren von NetScaler Gateway als Identitätsanbieter in Citrix Cloud

Informationen zum Einrichten der NetScaler Gateway-Authentifizierung in Citrix Cloud finden Sie unter Verbinden eines on-premises NetScaler Gateway als Identitätsanbieter mit Citrix Cloud.

Konfigurieren des Citrix-Identitätsanbieters als IdP-Typ für Citrix Endpoint Management

Diese Konfiguration gilt nur für Benutzer, die sich über Citrix Secure Hub registrieren. Nach dem Konfigurieren von NetScaler Gateway in Citrix Cloud konfigurieren Sie Citrix Endpoint Management wie

nachfolgend beschrieben.

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Identitätsanbieter (IdP)** und klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie auf der Seite **Identitätsanbieter (IdP)** folgende Einstellungen:

   - **IdP-Name:** Geben Sie einen eindeutigen Namen für die IdP-Verbindung ein, die Sie erstellen.
   - **IdP-Typ:** Wählen Sie **Citrix-Identitätsanbieter**.
   - **Auth-Domäne:** Wählen Sie **NetScaler Gateway**. Diese Domäne entspricht Ihrer Identitätsanbieterdomäne auf der Seite **Workspacekonfiguration > Authentifizierung** in Citrix Cloud.

3. Klicken Sie auf **Weiter**. Konfigurieren Sie folgende Einstellungen auf der Seite **IdP-Anspruchsverwendung**:

   - **Benutzer-ID-Typ:** Dieses Feld ist standardmäßig auf **userPrincipalName** festgelegt.
   - **Benutzer-ID-Zeichenfolge:** Dieses Feld wird automatisch ausgefüllt.

4. Klicken Sie auf **Weiter**, lesen Sie die **Zusammenfassung** und klicken Sie auf **Speichern**.

   Sie können jetzt Benutzergeräte über Citrix Secure Hub mit einem On-Premises-NetScaler Gateway als Identitätsanbieter registrieren.

Verfahren zur Authentifizierung in Citrix Secure Hub

Citrix Endpoint Management verwendet das folgende Verfahren, um Benutzer mit einem On-Premises-NetScaler Gateway als Identitätsanbieter auf Geräten zu authentifizieren, die über Citrix Secure Hub registriert sind:

1. Ein Benutzer startet Citrix Secure Hub.
2. Die Authentifizierungsanforderung wird von Citrix Secure Hub an die Citrix-Identität und von dort an das On-Premises-NetScaler Gateway geleitet.
3. Der Benutzer gibt den Benutzernamen und das Kennwort ein.
4. Ein On-Premises-NetScaler Gateway validiert den Benutzer und sendet einen Code an die Citrix-Identität.
5. Die Citrix-Identität sendet den Code an Citrix Secure Hub, von wo er an den Citrix Endpoint Management-Server weitergeleitet wird.
6. Citrix Endpoint Management fordert mit dem Code und dem geheimen Schlüssel einen ID-Token an und überprüft die Benutzerinformationen im ID-Token. Citrix Endpoint Management gibt eine Sitzungs-ID zurück.

nFactor-Authentifizierung

June 26, 2024

Mit der nFactor-Authentifizierung können Sie alle derzeit mit NetScaler möglichen Authentifizierungsmodi verwenden, wenn Sie Citrix Secure Hub verwenden. Sie erhöht die Sicherheit einer Anwendung, da Benutzer mehrere Identifikationsnachweise bereitstellen müssen, um Zugriff zu erhalten. Weitere Informationen zur nFactor-Authentifizierung finden Sie unter nFactor-Authentifizierung.

Weitere Informationen zu den verschiedenen Authentifizierungs- und Autorisierungsmethoden und deren Konfiguration finden Sie außerdem unter Authentifizierung und Autorisierung.

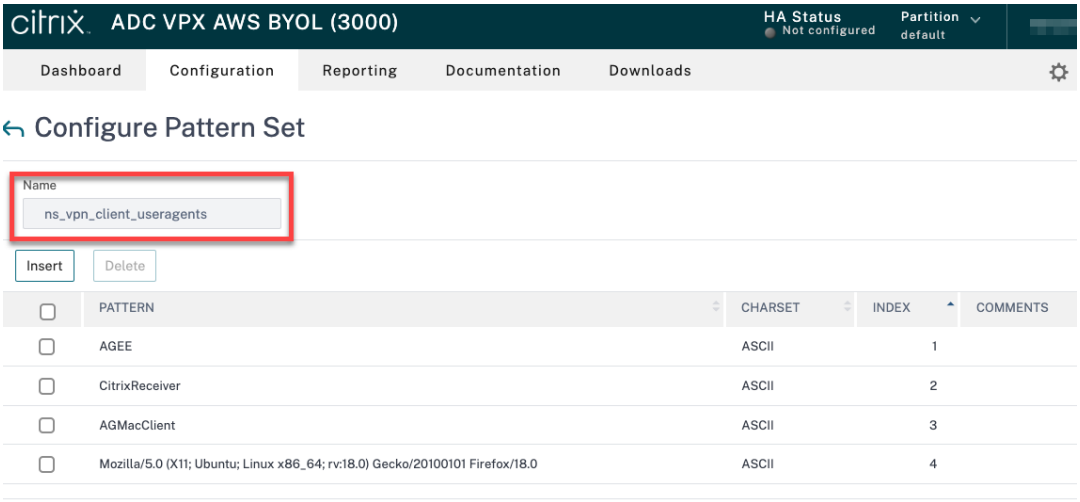
Citrix Endpoint Management unterstützt die folgenden Authentifizierungstypen mit nFactor-Authentifizierung:

- Lokal
- Lightweight Directory Access Protocol (LDAP)
- RADIUS
- SAML
- Clientzertifikatauthentifizierung

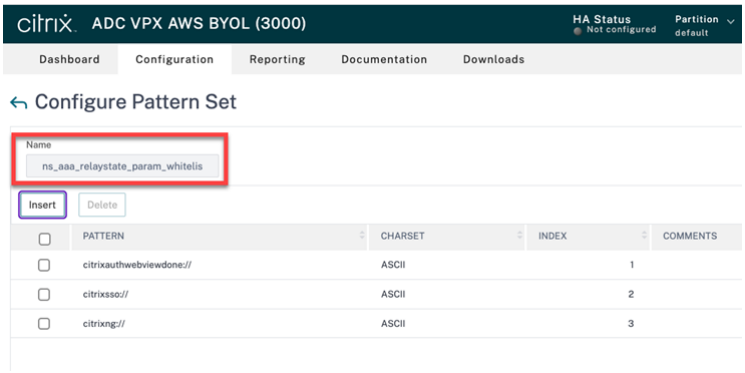
Voraussetzungen

Um Citrix Endpoint Management für die Verwendung der nFactor-Authentifizierung zu konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Stellen Sie sicher, dass Sie NetScaler 13.0 oder höher verwenden.
- Stellen Sie sicher, dass Sie in NetScaler die folgenden Mustersatzeinstellungen für Ihre Android- und iOS-Geräte konfiguriert haben:
  - Ns_vpn_client_useragents



– Ns_aaa_relaystate_param_whitelist



- Stellen Sie sicher, dass Sie die neueste Version von Citrix Secure Hub von Apple oder Google Play installiert haben.
- Stellen Sie sicher, dass Sie die Richtlinie “Erweiterte Authentifizierung”im NetScaler Gateway verwenden.
- Stellen Sie sicher, dass Sie die Clienteigenschaft **ENABLE_MAM_NFACTOR_SSO** für on-premises und für Cloud auf **True** festlegen. Weitere Informationen zur Eigenschaft **ENABLE_MAM_NFACTOR_SSO** finden Sie unter Referenz der Clienteigenschaften.

> **Hinweis:**
>
> Wenn die Clienteigenschaft **Enable nFactor SSO** auf **False** festgelegt ist, müssen Sie sicherstellen, dass die klassischen Authentifizierungsrichtlinien an das NetScaler Gateway gebunden sind.

nFactor-Authentifizierung konfigurieren

Konfigurieren Sie die nFactor-Authentifizierung für Citrix Endpoint Management je nachdem, wie Ihr NetScaler Gateway eingerichtet ist:

- Citrix Endpoint Management ist bereits mit dem NetScaler Gateway mit der klassischen Authentifizierungsrichtlinie eingerichtet. Weitere Informationen finden Sie unter Klassische Richtlinie im vorhandenen NetScaler Gateway auf die Richtlinie für erweiterte Authentifizierung aktualisieren.
- Einrichtung von Citrix Endpoint Management mit dem NetScaler Gateway mithilfe der Richtlinie für erweiterte Authentifizierung. Weitere Informationen finden Sie unter NetScaler Gateway-Setup mithilfe der Richtlinie für erweiterte Authentifizierung konfigurieren.

Klassische Richtlinie im vorhandenen NetScaler Gateway auf die Richtlinie für erweiterte Authentifizierung aktualisieren

Wenn Ihr Citrix Endpoint Management bereits mit der klassischen Authentifizierungsrichtlinie im NetScaler Gateway eingerichtet ist, müssen Sie die klassische Authentifizierungsrichtlinie mit einer der folgenden Methoden auf die erweiterte Authentifizierungsrichtlinie aktualisieren:

- Erstellen Sie eine neue erweiterte Authentifizierungsrichtlinie und ändern Sie die Gatewaykonfiguration, sodass die erweiterte Authentifizierungsrichtlinie verwendet wird. Weitere Informationen finden Sie unter Authentifizierungsrichtlinien.
- Aktualisieren Sie die klassische Authentifizierungsrichtlinie auf die erweiterte Authentifizierungsrichtlinie. Weitere Informationen finden Sie unter Richtlinienausdrücke mit dem NSPEPI-Tool konvertieren.

NetScaler Gateway-Setup mithilfe der Richtlinie für erweiterte Authentifizierung konfigurieren

Informationen zum Konfigurieren der nFactor-Authentifizierung für Citrix Endpoint Management im NetScaler Gateway mithilfe der erweiterten Authentifizierungsrichtlinie finden Sie unter nFactor-Authentifizierung konfigurieren.

> **Hinweis:**
>
> - Sie können den entsprechenden Authentifizierungstyp aus den unterstützten Authentifizierungstypen auswählen.
> - Wenn Sie den SAML-Authentifizierungstyp verwenden, können Sie SAML mit dem MAM-IdP mithilfe einer der folgenden Methoden konfigurieren:
>   - Informationen zur Konfiguration mit Azure Active Directory finden Sie unter Au-

> thentifizierung mit Azure Active Directory über NetScaler Gateway für die MAM-Registrierung.
> - Informationen zur Konfiguration mit Okta finden Sie unter Authentifizierung mit Okta über NetScaler Gateway für die MAM-Registrierung.

Benutzerkonten, Rollen und Registrierung

March 11, 2024

Sie führen Benutzerkonfigurationsaufgaben in der Citrix Endpoint Management-Konsole auf der Registerkarte **Verwalten** und der Seite **Einstellungen** durch. Sofern nicht anders angegeben, finden Sie in diesem Artikel die Schritte für die folgenden Aufgaben.

- Registrierungssicherheitsmodus und Registrierungseinladungen
  - Unter **Einstellungen > Registrierung** können Sie bis zu sieben Registrierungssicherheitsmodi konfigurieren und auch Registrierungseinladungen versenden. Jeder Registrierungssicherheitsmodus hat eine eigene Sicherheitsstufe und eigene Verfahren zum Registrieren von Geräten.
- 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 Rollen mit RBAC konfigurieren.
  - 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 zwei verschiedene Kanäle konfigurieren: Citrix Secure Hub oder SMTP. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Benachrichtigungsvorlagen.
- Benutzerkonten und Gruppen:
  - Unter **Verwalten > Benutzer** können Sie manuell lokale Benutzerkonten hinzufügen oder eine CSV-Provisioningdatei verwenden, um die Konten zu importieren und lokale Gruppen zu verwalten. Die meisten Citrix Endpoint Management-Bereitstellungen stellen jedoch eine Verbindung zu LDAP her, um Benutzer- und Gruppeninformationen abzurufen. In folgenden Anwendungsfällen ist es möglicherweise besser, Benutzerkonten lokal zu erstellen:

    * In Umgebungen wie dem Einzelhandel, in denen Geräte gemeinsam genutzt werden und nicht dediziert für einzelne Benutzer sind.
    * Wenn Sie ein nicht unterstütztes Verzeichnis wie Novell eDirectory verwenden.
  - Unter **Einstellungen > Workflows** verwenden Sie die Workflows, um das Erstellen und Entfernen von Benutzerkonten zu verwalten.

Informationen zu Benutzerkonten

Ein Citrix Endpoint Management-Benutzerkonto ist entweder für einen lokalen, Active Directory- oder Cloudbenutzer.

- **Cloudbenutzer:** Ein Cloudbenutzer ist ein spezielles Benutzerkonto, das Citrix Cloud erstellt, wenn Ihrem Citrix Cloud-Kundenkonto ein Administrator hinzugefügt wird. Ein Cloudbenutzerkonto verwendet denselben Benutzernamen wie das Administratorkonto in Citrix Cloud und als Standard die Administratorrolle. Das Cloudbenutzerkonto bietet Single Sign-On und führt andere Verwaltungsfunktionen aus.

  Informationen zum Hinzufügen von Administratoren zu einem Citrix Cloud-Konto finden Sie unter Einladen neuer Administratoren.

Für Cloudbenutzer gilt:

- Sie können die Rollen und Eigenschaften von Cloudbenutzern über die Citrix Cloud-Konsole ändern. Siehe Verwalten von Citrix Cloud-Administratoren.
- Informationen zum Ändern des Kennworts finden Sie unter Administratoren.
- Um einen Cloudbenutzer zu löschen, gehen Sie in Citrix Cloud zu **Identitäts- und Zugriffsverwaltung > Administratoren**. Klicken Sie auf die drei Punkte (…) am Ende der Benutzerzeile und wählen Sie **Administrator löschen**.
- Sie können Cloudbenutzer nicht zu einer lokalen Gruppe hinzufügen.

Registrierungssicherheitsmodi konfigurieren

Sie konfigurieren einen Registrierungssicherheitsmodus für Geräte, um eine Sicherheitsstufe und eine Benachrichtigungsvorlage für die Geräteregistrierung bei Citrix Endpoint Management anzugeben.

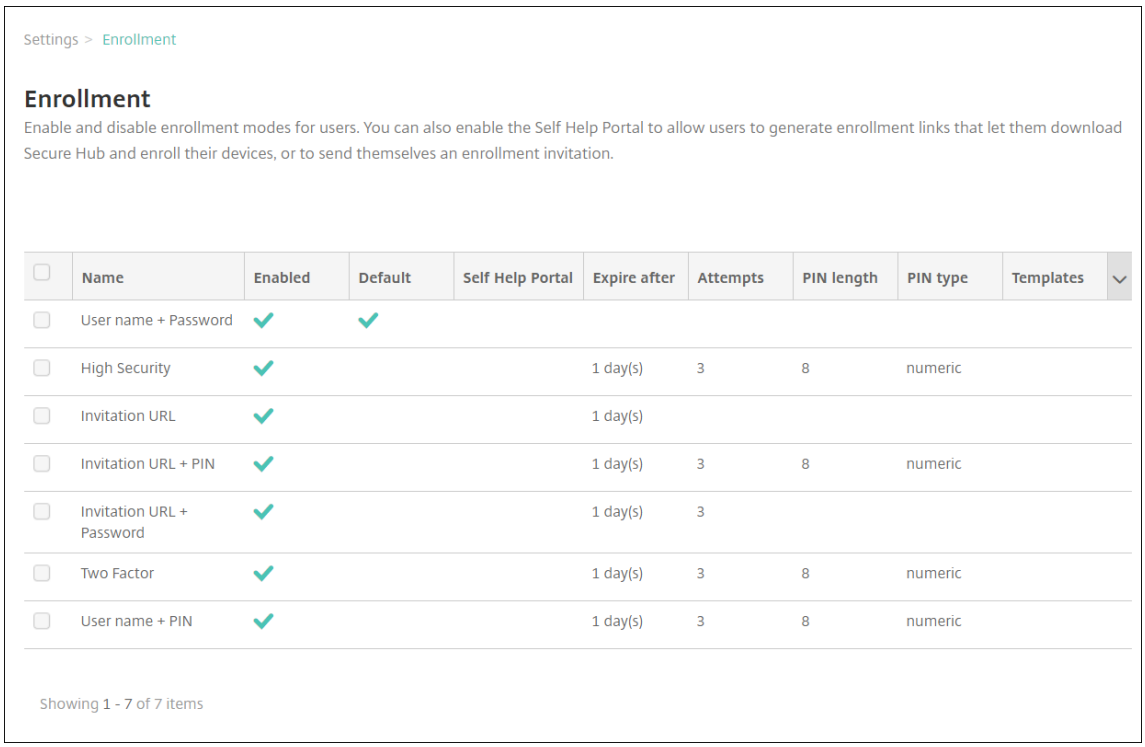
Citrix Endpoint Management bietet sechs Registrierungssicherheitsmodi mit verschiedenen Sicherheitsstufen und Schritten, die die Benutzer zum Registrieren von Geräten ausführen müssen. Konfigurieren Sie Registrierungssicherheitsmodi in der Citrix Endpoint Management-Konsole auf der Seite **Einstellungen > Registrierungseinladungen**. Weitere Informationen finden Sie unter 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 Citrix Endpoint Management-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 mit allen verfügbaren Registrierungssicherheitsmodi. Standardmäßig sind alle Registrierungssicherheitsmodi aktiviert.
3. Wählen Sie einen Registrierungssicherheitsmodus in der Liste zur Bearbeitung aus. Stellen Sie dann den Modus als Standard ein oder deaktivieren Sie den Modus.

   Aktivieren Sie das Kontrollkästchen neben einem Registrierungssicherheitsmodus, um das Optionsmenü anzuzeigen. Sie können auch an eine andere Stelle in der Liste klicken, um das Menü mit den Optionen rechts daneben anzuzeigen.

   > **Tipp:**
   >
   > Beim Bearbeiten des Registrierungssicherheitsmodus können Sie einen Zeitraum angeben, nach dessen Ablauf die Benutzer ihre Geräte nicht mehr registrieren können. Weitere Informationen finden Sie unter Bearbeiten eines Registrierungssicherheitsmodus in diesem Artikel. Der Wert wird auf den Seiten zur Konfiguration der Registrierungseinladung für Benutzer und Gruppen angezeigt.



Je nach Plattform stehen folgende Registrierungssicherheitsmodi zur Auswahl:

- Benutzername + Kennwort
- Einladungs-URL
- Einladungs-URL + PIN
- Einladungs-URL + Kennwort
- Zwei Faktoren
- Benutzername + PIN

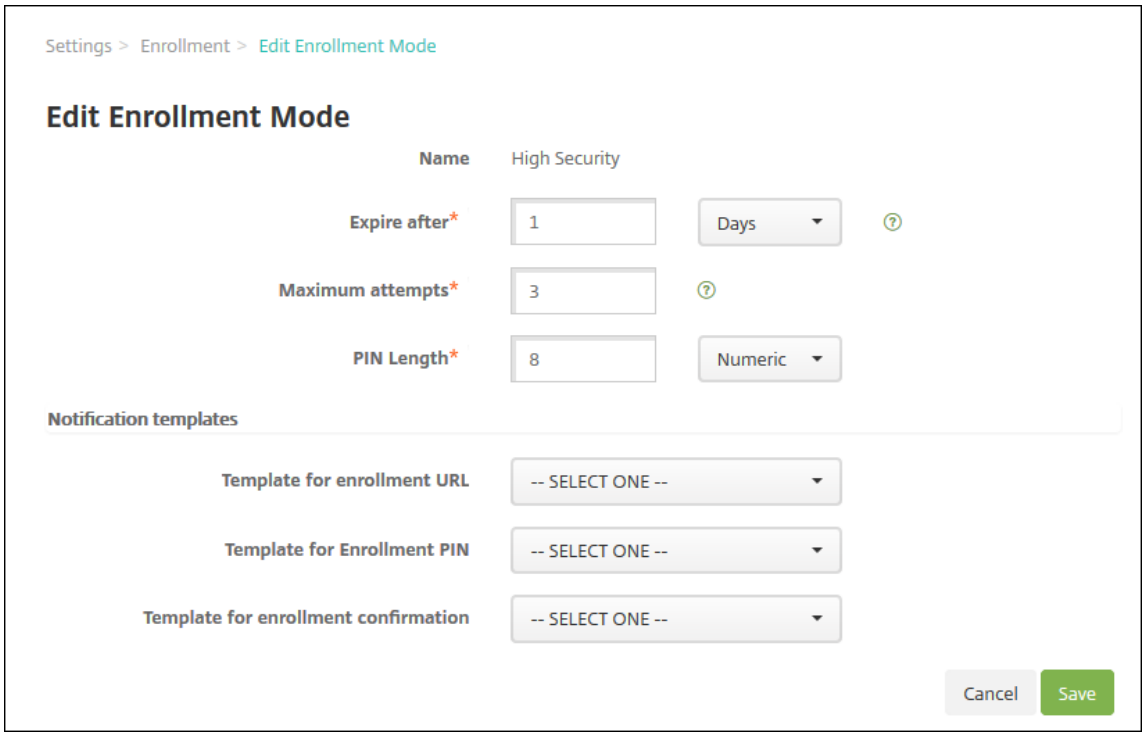
Hinweise zu plattformspezifischen Registrierungssicherheitsmodi finden Sie unter Registrierungssicherheitsmodi nach Plattform.

Sie können die Registrierung über Registrierungseinladungen auf bestimmte Benutzer oder Gruppen beschränken. 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 Citrix Secure Hub eingeben.

Als zweistufige Authentifizierungslösung 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. Abhängig von dem ausgewählten Modus werden ggf. andere Optionen angezeigt.



2. Ändern Sie nach Bedarf die folgenden Informationen:

   - **Ablauf nach:** Geben Sie einen Zeitraum ein, nach dem die Benutzer ihre Geräte nicht mehr registrieren können. Dieser Wert wird auf den Seiten zur Konfiguration der Registrierungseinladung für Benutzer und Gruppen angezeigt.

     Geben Sie **0** ein, wenn die Einladung nicht ablaufen soll.

   - **Tage:** Klicken Sie in der Dropdownliste 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 Dropdownliste auf **Numerisch** oder **Alphanumerisch**, um die Art der PIN festzulegen.

- **Benachrichtigungsvorlagen:**
  - **Vorlage für Registrierungs-URL:** Wählen Sie in der Dropdownliste eine Vorlage für die Registrierungs-URL aus. Die Vorlage für Registrierungseinladungen sendet beispielsweise eine E-Mail an Benutzer. Weitere Informationen über Benachrichtigungsvorlagen finden Sie unter Erstellen oder Aktualisieren von Benachrichtigungsvorlagen.
  - **Vorlage für Registrierungs-PIN:** Wählen Sie in der Dropdownliste eine Vorlage für die Registrierungs-PIN aus.
  - **Vorlage für Registrierungsbestätigung:** Wählen Sie in der Dropdownliste eine Vorlage für die Benachrichtigung der Benutzer über eine erfolgreiche Registrierung aus.

3. Klicken Sie auf **Speichern**.

Festlegen eines Registrierungssicherheitsmodus als Standard

Der standardmäßige Registrierungssicherheitsmodus wird für alle Geräteregistrierungsanforderungen verwendet, es sei denn, Sie wählen einen anderen Registrierungssicherheitsmodus aus. Wenn kein Registrierungssicherheitsmodus als Standard festgelegt ist, müssen Sie für jede Geräteregistrierung eine eigene Registrierungsanforderung erstellen.

1. Wenn der Registrierungssicherheitsmodus, den Sie als Standard verwenden möchten, nicht aktiviert ist, wählen Sie ihn aus und klicken Sie auf **Aktivieren**. Sie können nur **Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** als Standard festlegen.
2. Wählen Sie den Registrierungssicherheitsmodus aus und 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.

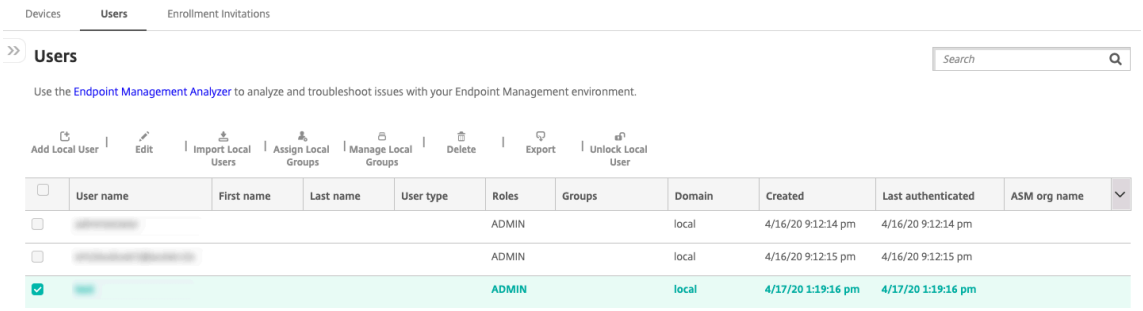
2. Klicken Sie auf **Deaktivieren**. Der Registrierungssicherheitsmodus ist nicht mehr aktiviert.

Erstellen, Bearbeiten, Entsperren und Löschen lokaler Benutzerkonten

Sie können lokale Benutzerkonten in Citrix Endpoint Management manuell hinzufügen oder mit einer Provisioningdatei importieren. Eine Anleitung zum Importieren von Benutzerkonten aus einer Provisioningdatei finden Sie unter Importieren von Benutzerkonten.

Alle Citrix Cloud-Administratoren werden als Citrix Endpoint Management-Administratoren erstellt. Wenn Sie einen Citrix Cloud-Administrator mit benutzerdefiniertem Zugriff erstellen, stellen Sie sicher, dass der Zugriff Citrix Endpoint Management umfasst. Weitere Informationen zum Hinzufügen von Citrix Cloud-Administratoren finden Sie unter Hinzufügen von Administratoren.

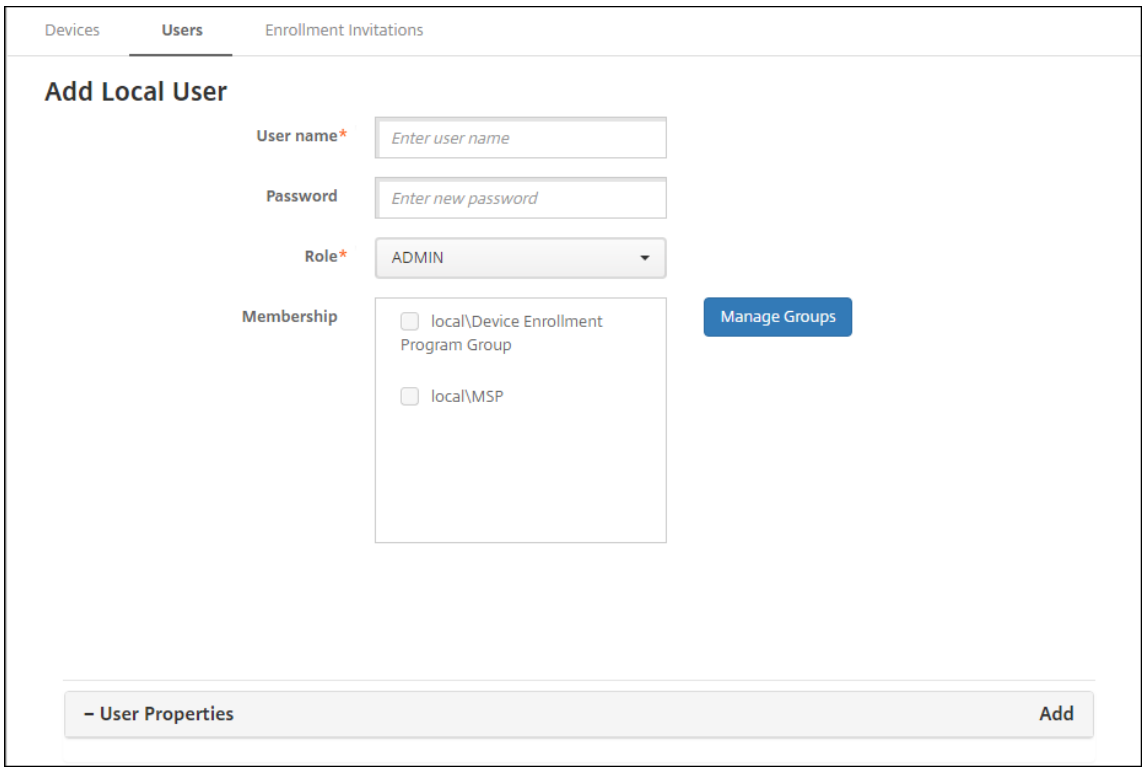
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Verwalten > Benutzer**. Die Seite **Benutzer** wird angezeigt.



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 können Folgendes enthalten: Leerzeichen, Großbuchstaben und Kleinbuchstaben.
   - **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 Dropdownliste auf die Rolle des Benutzers. Weitere Informationen über Rollen finden Sie unter Rollen mit RBAC konfigurieren. Mögliche Optionen:
     - ADMIN
     - DEVICE_PROVISIONING
     - SUPPORT
     - USER
   - **Mitgliedschaft:** Klicken Sie in der Dropdownliste auf die Gruppe bzw. 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 Dropdownliste 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**.

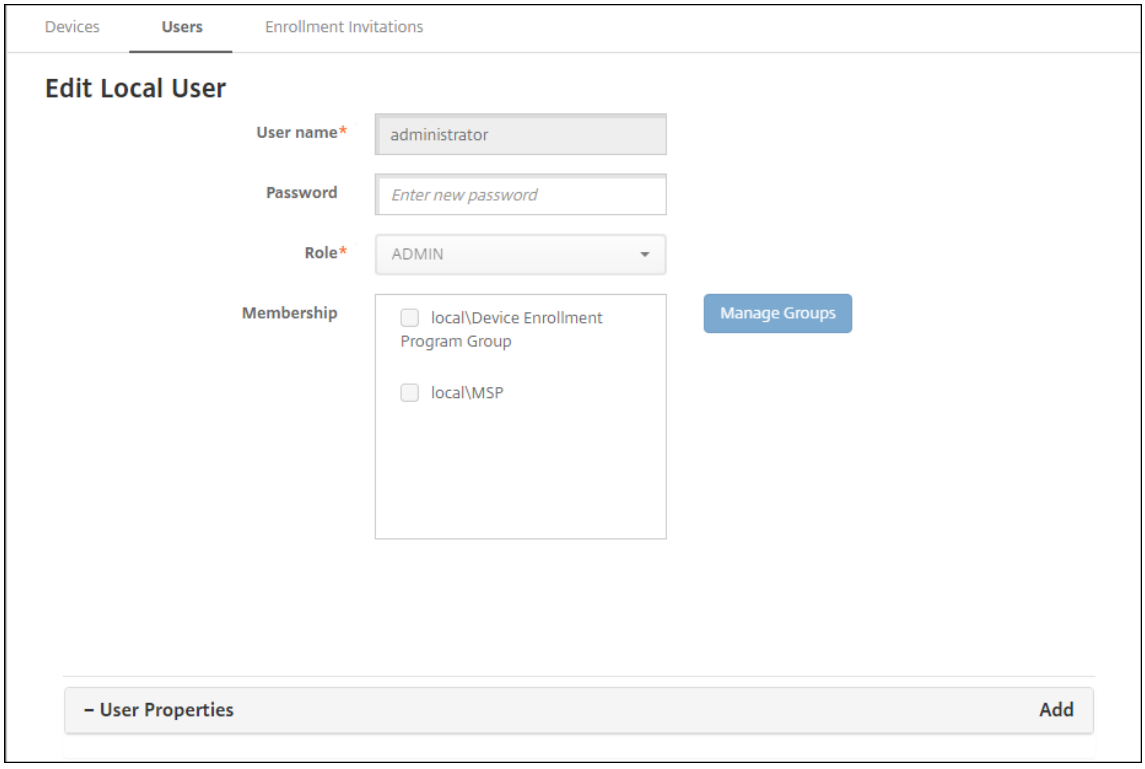
  Zum Löschen einer vorhandenen Benutzereigenschaft zeigen Sie auf deren Zeile und klicken Sie auf das **X** auf der rechten Seite. Die Eigenschaft wird sofort gelöscht.

  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**. Nachdem Sie einen Benutzer erstellt haben, bleibt das Feld **Benutzertyp** für ein lokales Benutzerkonto leer.

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 Dropdownliste auf die Rolle des Benutzers.
- **Mitgliedschaft:** Klicken Sie in der Dropdownliste 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 Dropdownliste 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

Ein lokales Benutzerkonto wird entsprechend diesen Servereigenschaften gesperrt:

- `local.user.account.lockout.time`
- `local.user.account.lockout.limit`

  Weitere Informationen finden Sie unter Servereigenschaften –Definitionen.

Wenn ein lokales Benutzerkonto gesperrt wird, können Sie es über die Citrix Endpoint Management-Konsole entsperren.

1. Wählen Sie auf der Seite **Benutzer** in der Liste das Benutzerkonto aus.
2. Klicken Sie auf **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.

Sie können einen Active Directory-Benutzer nicht über die Citrix Endpoint Management-Konsole entsperren. Ein gesperrter Active Directory-Benutzer muss sich an den Active Directory-Helpdesk wenden, um das Kennwort zurücksetzen 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.

2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt.
3. 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**.

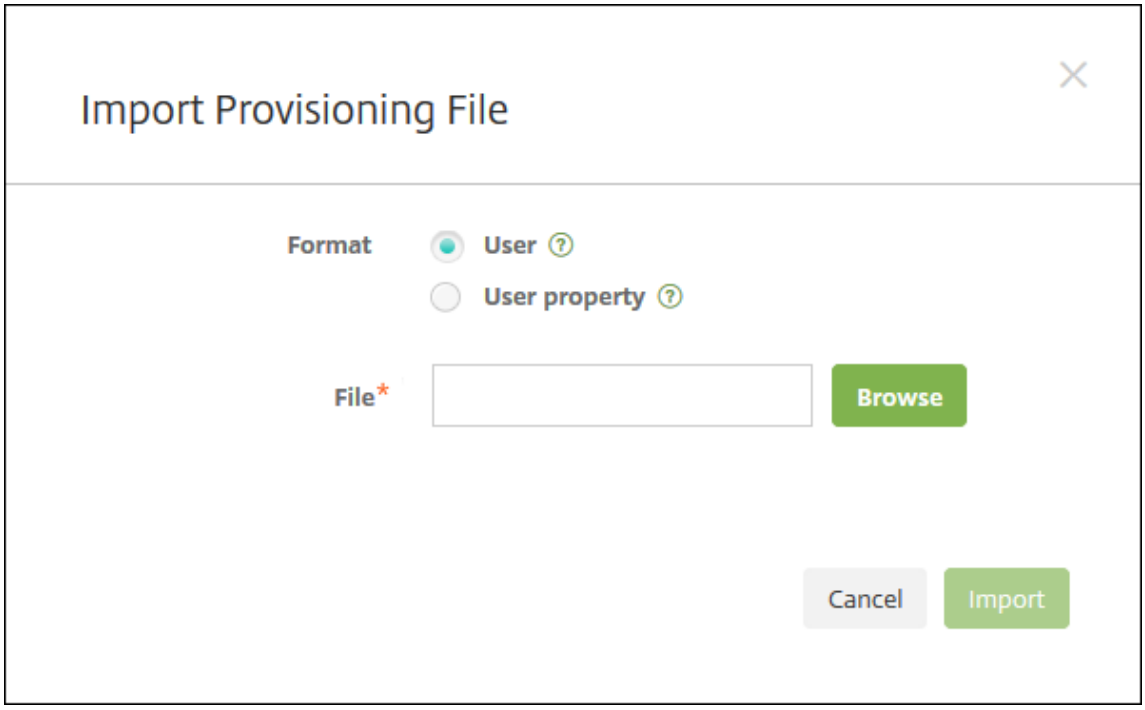
Importieren von Benutzerkonten

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. Geben Sie beispielsweise `username@domain` an. Wenn der erstellte oder importierte lokale Benutzer für eine verwaltete Domäne in Citrix Endpoint Management vorgesehen ist, kann der Benutzer sich nicht mit den entsprechenden LDAP-Anmeldeinformationen registrieren.
> - Beim Importieren von Benutzerkonten in das interne Benutzerverzeichnis von Citrix Endpoint Management deaktivieren Sie die Standarddomäne, um den Importvorgang zu beschleunigen. Beachten Sie, dass die Deaktivierung der Domäne sich auf Registrierungen auswirkt. Aktivieren Sie die Standarddomäne wieder, nachdem der Import interner Benutzer abgeschlossen ist.
> - 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 Citrix Endpoint Management durch.

1. Klicken Sie in der Citrix Endpoint Management-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 erstellen und sie zum Importieren von Benutzerkonten und Eigenschaften in Citrix Endpoint Management verwenden. Verwenden Sie eines der folgenden Formate für eine Provisioningdatei:

- **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 folgender Form in der Provisioningdatei ein: **propertyV;test;1;2**.
> - 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 eine Gruppenhierarchie 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:** Active Directory.test.net

Beispiel für Benutzerattribut-Provisioninginhalt Der Eintrag `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` bedeutet:

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

- **Name:** prop 2
- **Wert:** prop2 value

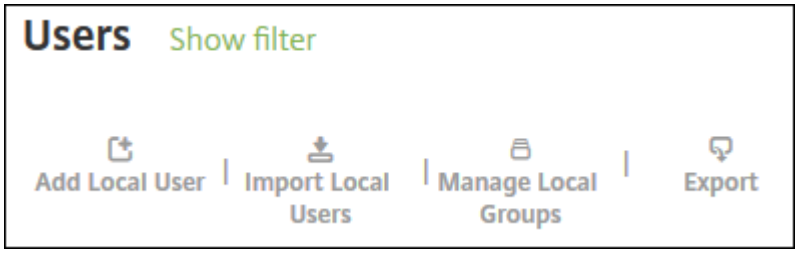
Hinzufügen und Entfernen von Gruppen

Gruppen werden im Dialogfeld **Gruppen verwalten** in der Citrix Endpoint Management-Konsole auf folgenden Seiten verwaltet: **Benutzer**, **Lokalen Benutzer hinzufügen** oder **Lokalen Benutzer bearbeiten**. Es gibt keinen spezifischen Befehl zum Bearbeiten von Gruppen.

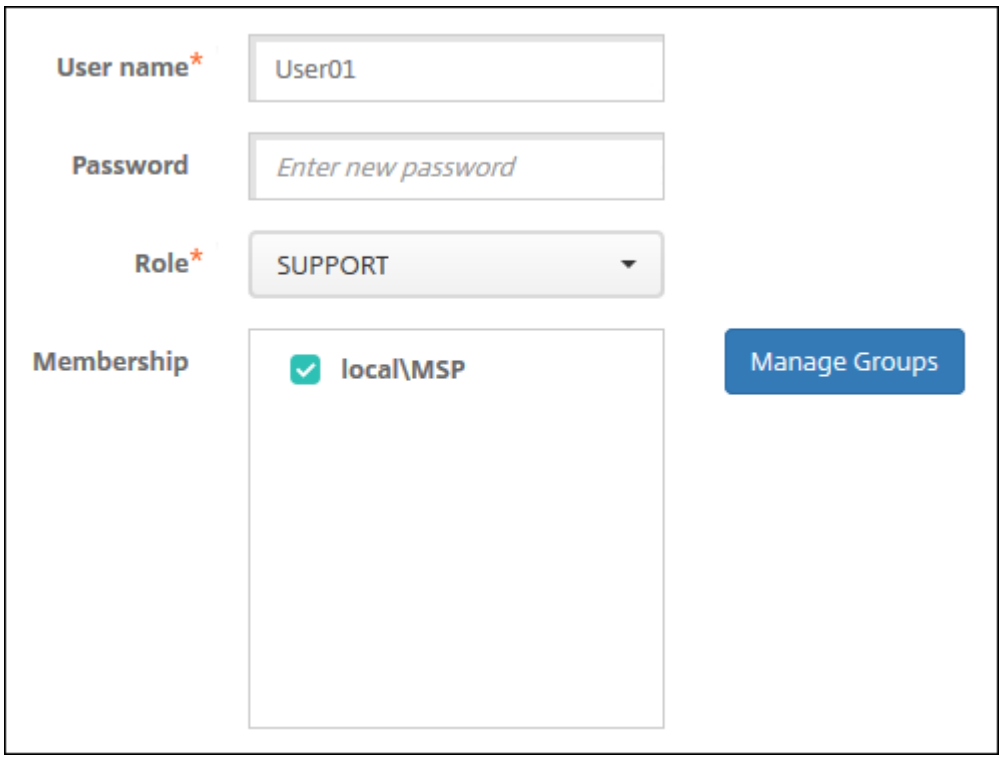
Hinzufügen einer lokalen Gruppe

1. Führen Sie einen der folgenden Schritte aus:

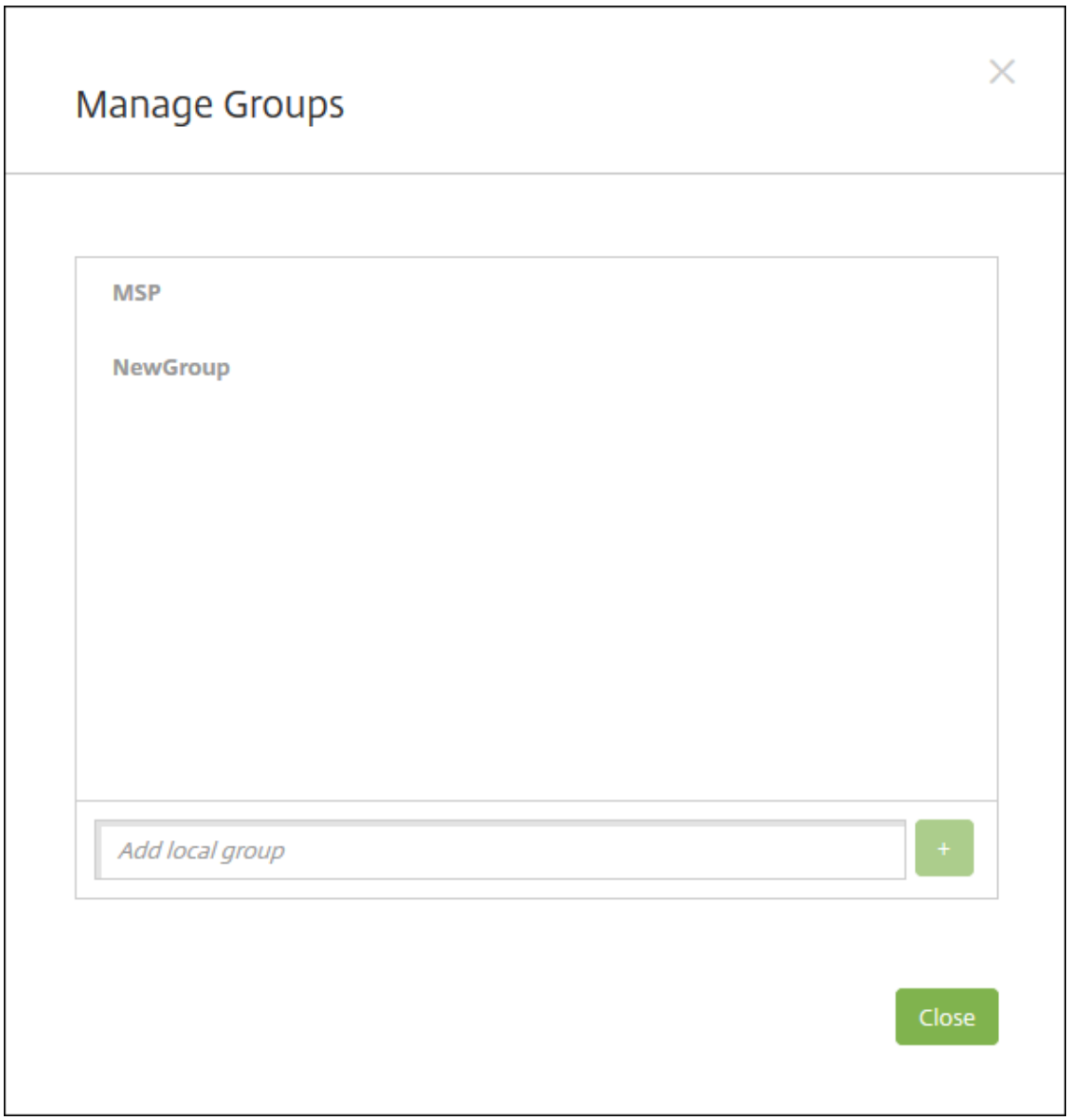
   - Klicken Sie auf der Seite **Benutzer** auf **Lokale Gruppen** verwalten.



   - 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

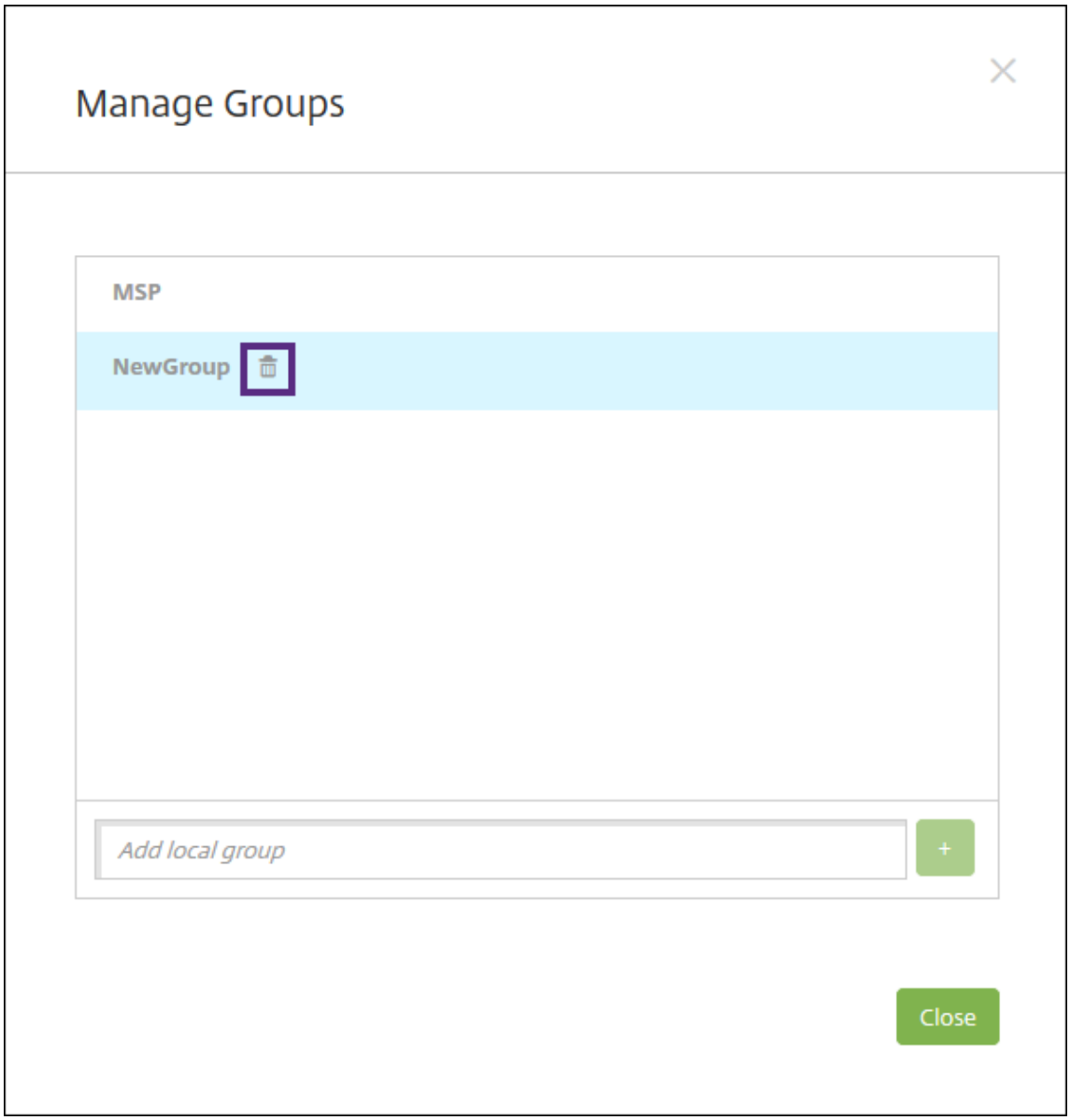
Das Entfernen einer Gruppe hat keine Auswirkungen auf die Benutzerkonten. Stattdessen wird beim Entfernen einer Gruppe nur die Zuordnung der Benutzer zu dieser Gruppe aufgehoben. Die Benutzer verlieren zudem den Zugriff auf Apps und Profile, die über Bereitstellungsgruppen bereitgestellt werden, die der gelöschten Gruppe zugeordnet sind. Alle anderen Gruppenzuordnungen bleiben jedoch erhalten. 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. Bevor Sie einen Workflow erstellen, ermitteln Sie die Personen in Ihrer Organisation, die zum Genehmigen von Benutzerkontenanforderungen berechtigt sind. Anschließend können Sie mit der Workflowvorlage Benutzerkontenanforderungen erstellen und genehmigen.

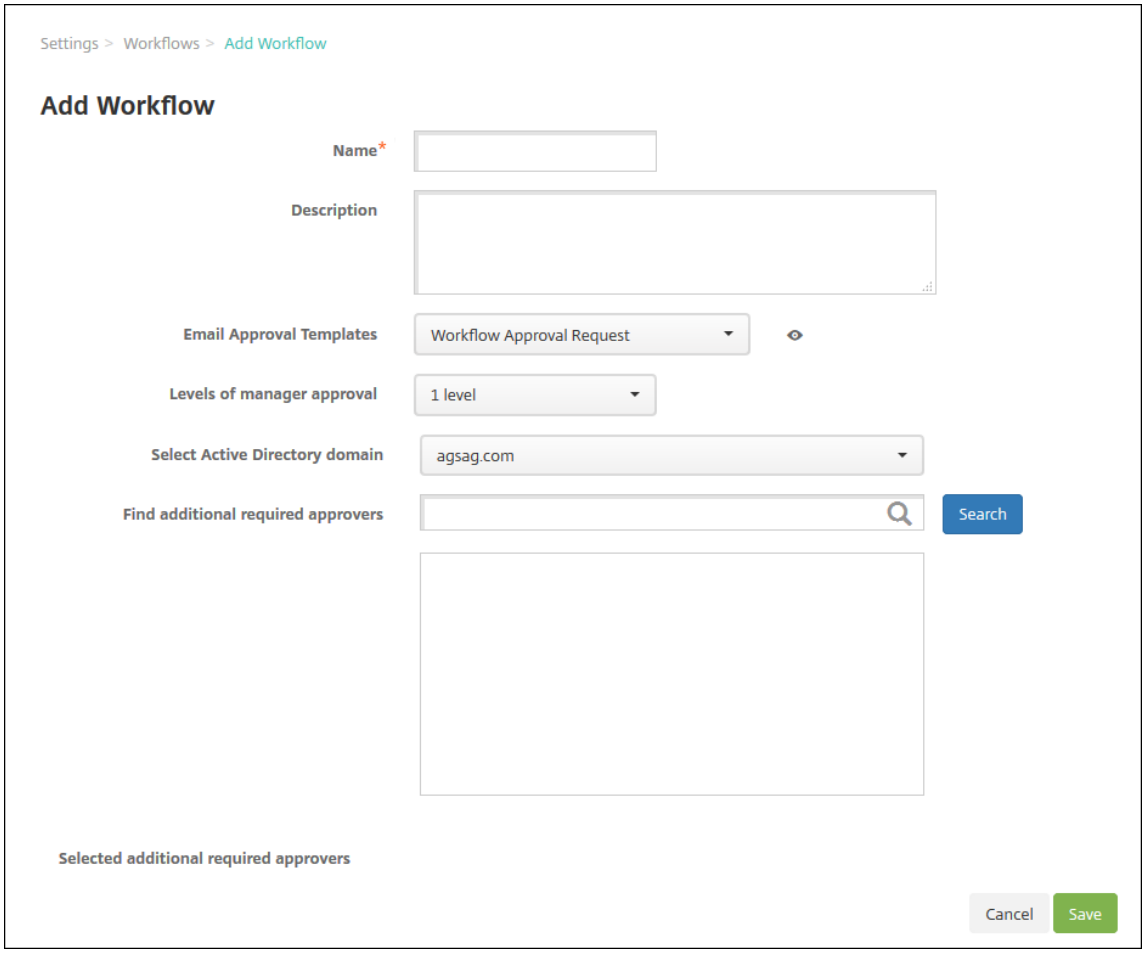
Beim ersten Einrichten von Citrix Endpoint Management konfigurieren Sie Einstellungen für Workflow-E-Mails. Diese müssen festgelegt werden, bevor Sie Workflows verwenden können. Sie können die Einstellungen für Workflow-E-Mails jederzeit ändern. Diese Einstellungen umfassen E-Mail-Server, Port, E-Mail-Adresse und Angaben dazu, ob die Anforderung zum Erstellen des Benutzerkontos genehmigt werden muss.

Workflows können in Citrix Endpoint Management an zwei Stellen konfiguriert werden:

- Auf der Seite **Einstellungen > Workflows** in der Citrix Endpoint Management-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 Apps hinzufügen.

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 Citrix Endpoint Management 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 Citrix Endpoint Management-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 Citrix Endpoint Management-Konsole im Bereich **Benachrichtigungsvorlagen** unter **Einstellungen**. Wenn Sie auf das Augensymbol rechts neben dem Feld klicken, wird eine Vorschau der Vorlage angezeigt, die Sie konfigurieren.
   - **Ebenen für Managergenehmigung:** Wählen Sie in der Liste die Anzahl der Managergenehmigungsebenen für den Workflow aus. Der Standardwert ist **1 Ebene**. Mögliche Optionen:
     - Nicht erforderlich
     - 1 Ebene
     - 2 Ebenen
     - 3 Ebenen
   - **Active Directory-Domäne wählen:** Wählen Sie in der Liste die für den Workflow zu 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

March 11, 2024

Registrierungsprofile legen Folgendes fest:

- Registrierungsoptionen zur Geräteverwaltung für Android-, iOS- und Windows-Geräte.
- 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 Citrix Endpoint Management-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)
- Automatische Registrierung von Windows 10- und Windows 11-Geräten über die Citrix Workspace-App für Windows (Preview)

Wenn Ihre Site nur MDM verwendet und Sie MAM hinzufügen möchten, müssen Sie ein NetScaler Gateway konfigurieren. Weitere Informationen finden Sie unter Anforderungen für NetScaler Gateway.

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 Verwaltungsmodus und den Gerätebesitzermodus an. Beispiel: Unternehmenseigenes Gerät, vollständig verwaltet mit Arbeitsprofil, und BYOD-Arbeitsprofil.

  Neue Geräte registrieren sich standardmäßig bei Android Enterprise. Sie können Geräte nach Bedarf im Legacymodus (Android-Geräteadministrator) verwalten. Neue Geräte werden standardmäßig auch bei der App-Verwaltung registriert.

  Weitere Informationen zum Festlegen der Sicherheitsstufe und zum Registrierungsverfahren finden Sie unter Benutzerkonten, Rollen und Registrierung.

- **iOS:** Sie geben den Geräteverwaltungstyp an: **Apple-Benutzerregistrierung**, **Apple-Geräteregistrierung** oder **Geräte nicht verwalten**. Der Modus **Apple-Benutzerregistrierung** ist als öffentliche Preview verfügbar. Wenden Sie sich an das Supportteam, um dieses Feature zu aktivieren.

  Wenn Sie die Apple-Benutzerregistrierung auswählen, können Sie eine benutzerdefinierte Domäne für verwaltete Apple-IDs verwenden und diese Domäne konfigurieren.

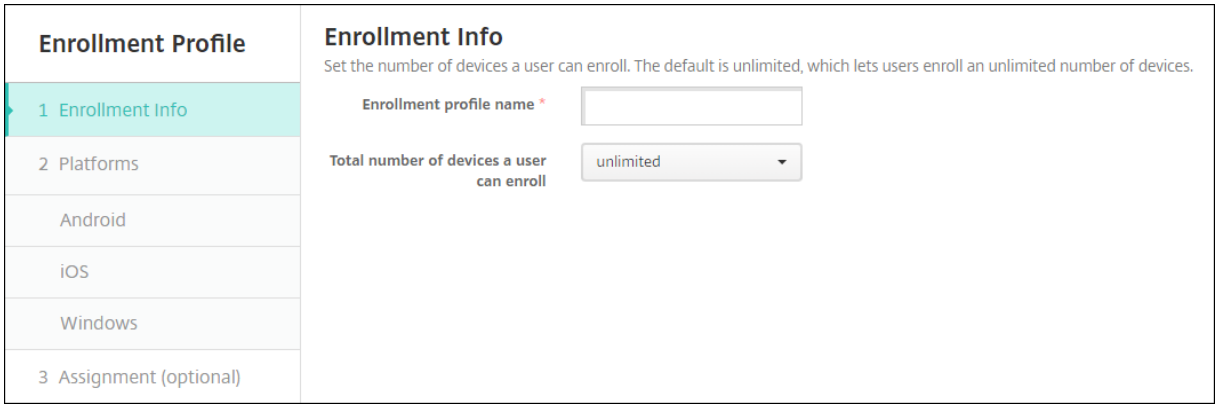
  Neue Geräte registrieren sich standardmäßig bei der Apple-Geräteverwaltung. Neue Geräte werden standardmäßig auch bei der App-Verwaltung registriert.

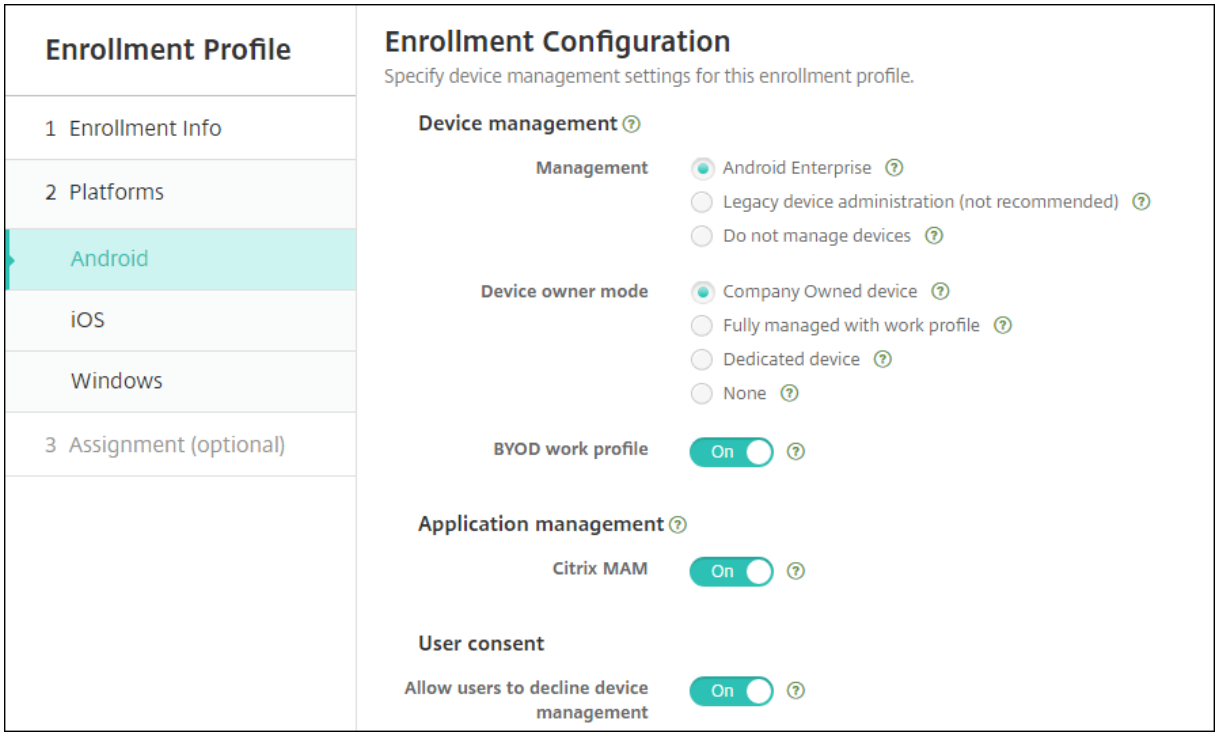
- **Windows 10 und Windows 11:** Sie geben an, ob die Citrix Geräteverwaltung für Windows verwendet werden soll. Neue Geräte registrieren sich standardmäßig bei der Geräteverwaltung.

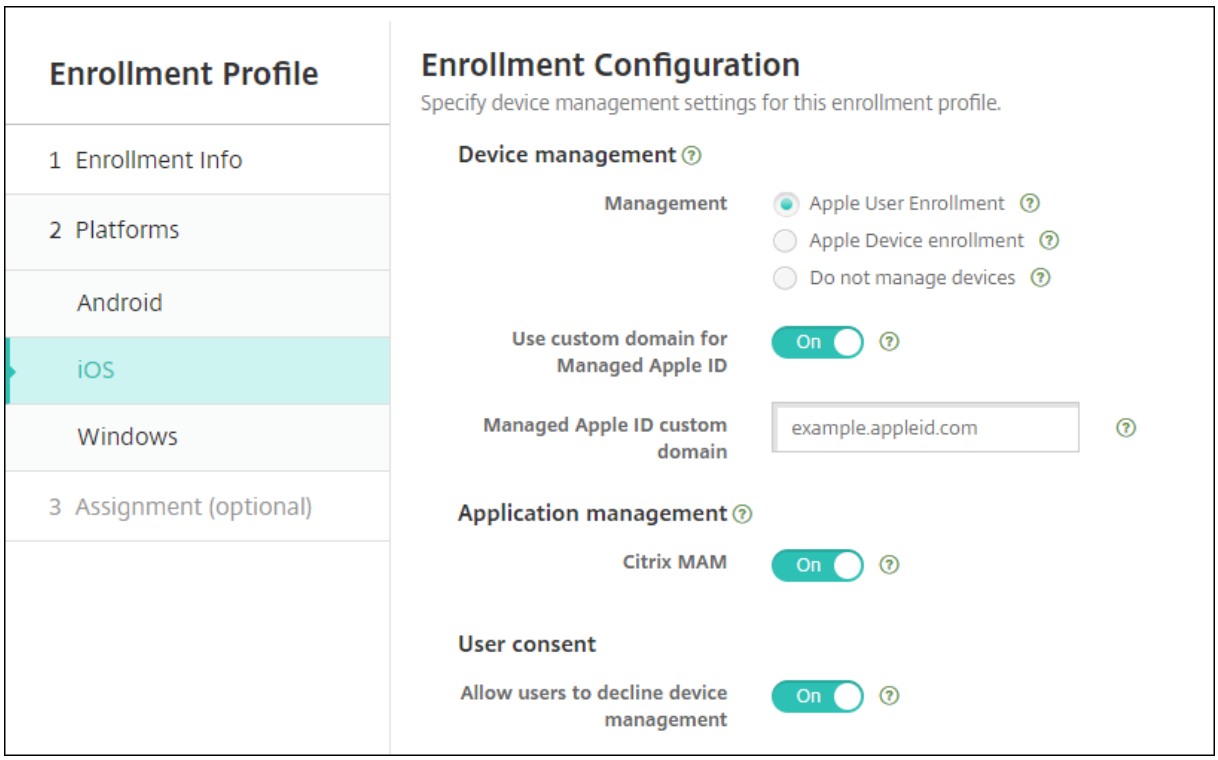
Globales Registrierungsprofil

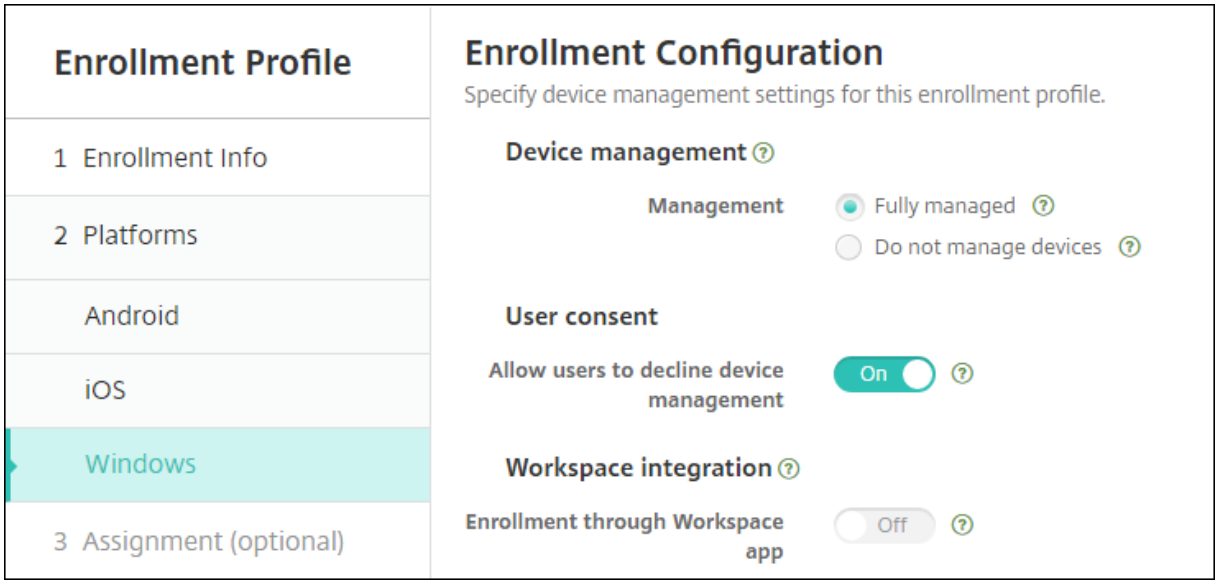
Das Standardregistrierungsprofil heißt “Global”. Das Profil “Global”eignet sich für Testzwecke, wenn noch keine spezifischen Registrierungsprofile erstellt wurden.

In Citrix Endpoint Management 20.2.1 und höher besitzt das globale Registrierungsprofil vordefinierte Einstellungen. Die folgenden Screenshots zeigen die Standardeinstellungen des globalen Registrierungsprofils. Nur-MAM-Bereitstellungen zeigen eine Teilmenge dieser Optionen an.









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. Citrix Endpoint Management 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 Citrix Endpoint Management 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:
  - Downgrade der Konfiguration eines Geräts von MDM+MAM- auf MAM- oder MDM-Registrierung. Eine Herabstufung ist möglich, wenn Sie ein Registrierungsprofil aktualisieren oder ein Gerät in eine andere Bereitstellungsgruppe verschieben.

  - Hinzufügen von MAM zu einem Registrierungsprofil, das für MDM konfiguriert ist.
  - 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

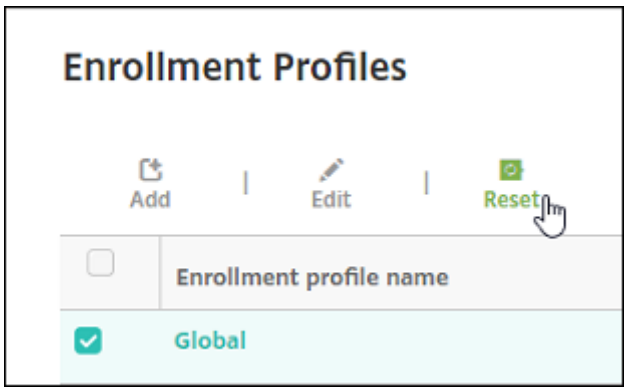
1. Gehen Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Registrierungsprofile**.
2. Geben Sie auf der Seite **Registrierungsinfo** einen aussagekräftigen Namen für das Registrierungsprofil ein. Standardmäßig können Benutzer beliebig viele Geräte registrieren. Wählen Sie einen Wert, wenn Sie die Anzahl der Geräte pro Benutzer begrenzen möchten. Das Limit gilt für die Summe aller in MAM oder MDM verwalteten Android-, iOS- und Windows-Geräte eines Benutzers.
3. Füllen Sie die Plattformseiten aus. Informationen zu plattformspezifischen Registrierungseinstellungen finden Sie unter:

   - Android Enterprise: Registrierungsprofile erstellen
   - iOS: Unterstützte Registrierungsmethoden
   - Windows Desktop/Tablet: Unterstützte Registrierungsmethoden

4. Fügen Sie auf der Seite **Zuweisungen** 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. Citrix Endpoint Management 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.



Benachrichtigungen

June 25, 2024

Sie können Benachrichtigungen in Citrix Endpoint Management 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 auf einem Gerät Jailbreak oder Rooting durchgeführt wurde

Details zu automatisierten Aktionen finden Sie unter Automatisierte Aktionen.

Zum Senden von Benachrichtigungen mit Citrix Endpoint Management müssen Sie ein Gateway und einen Benachrichtigungsserver konfigurieren. Sie können in Citrix Endpoint Management einen Benachrichtigungsserver einrichten, um SMTP-Server zu konfigurieren. Diese Server senden E-Mail-Benachrichtigungen an Benutzer. Sie können Benachrichtigungen zum Senden von Nachrichten über SMTP verwenden.

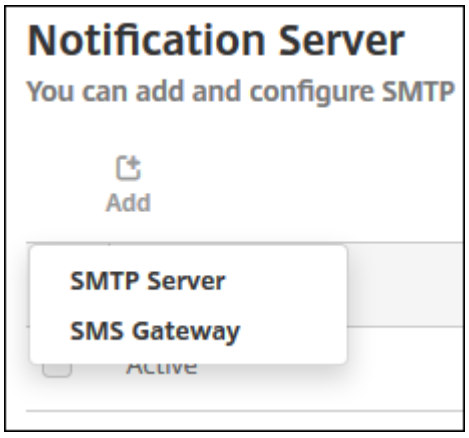
- SMTP ist ein verbindungsorientiertes, textbasiertes Protokoll, über das ein E-Mail-Absender mit einem E-Mail-Empfänger kommuniziert. Der E-Mail-Absender gibt Befehlszeichenfolgen aus und liefert die erforderlichen Daten (in der Regel über eine TCP-Verbindung). SMTP-Sitzungen bestehen aus Befehlen von einem SMTP-Client (der Person, die die Nachricht sendet) und den entsprechenden Antworten vom SMTP-Server.

Voraussetzungen

- 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 nur einen aktiven SMTP-Server verwenden. Dieser Kommunikationskanal erlaubt nur eine aktive Konfiguration.
- Öffnen Sie Port 25 über Citrix Endpoint Management in der DMZ, um zum SMTP-Server im internen Netzwerk zurückzuverweisen. Auf diese Weise kann Citrix Endpoint Management Benachrichtigungen erfolgreich senden.

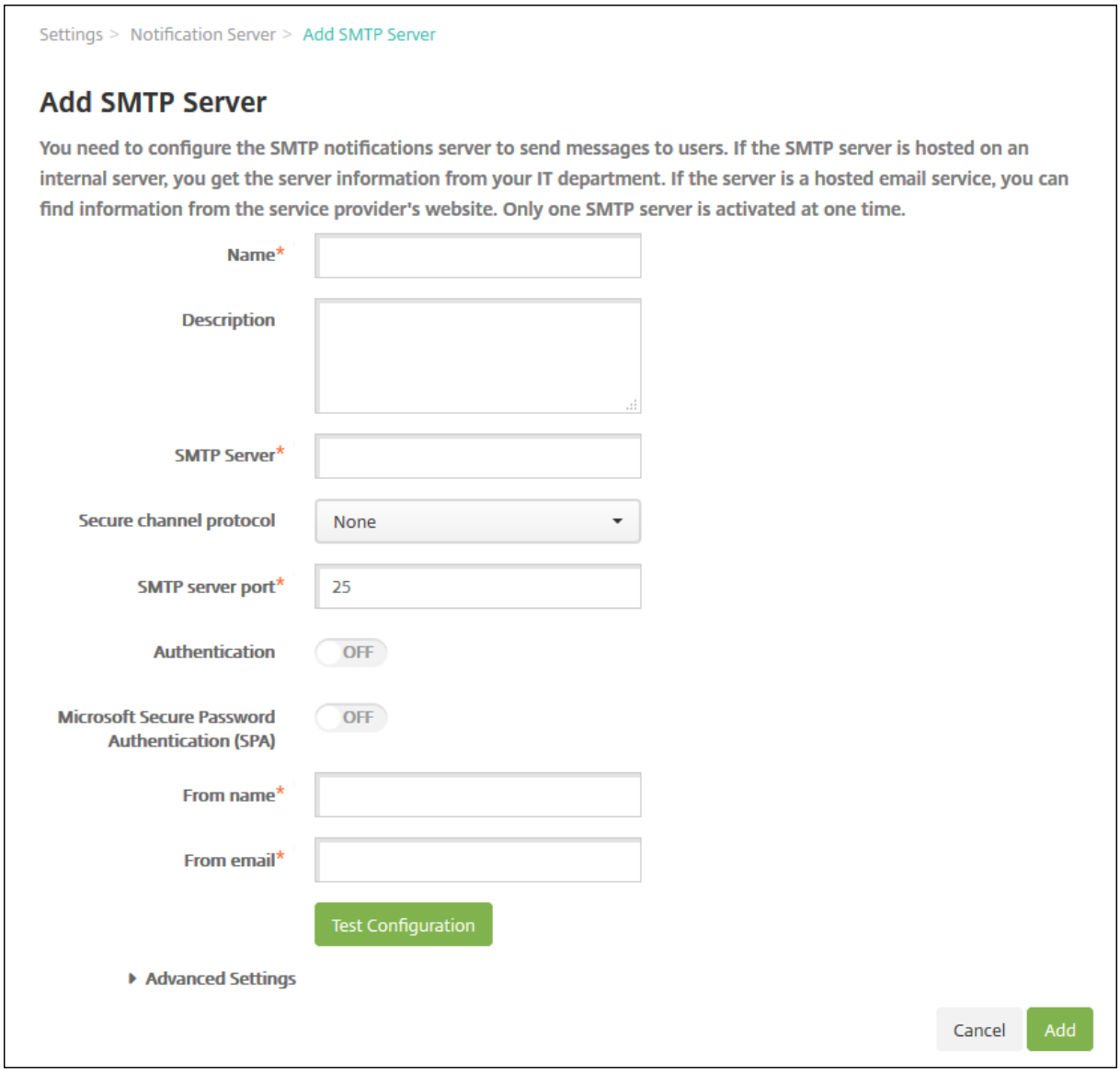
Konfigurieren eines SMTP-Servers

1. Klicken Sie in der Citrix Endpoint Management-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 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.

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. Geben Sie einen vollqualifizierten Domänennamen (FQDN) oder eine IP-Adresse ein.
   - **Secure Channel-Protokoll:** Klicken Sie in der Dropdownliste 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 dieser Port auf 25 eingestellt. Wenn SMTP-Verbindungen SSL verwenden, legen Sie den

Port auf 465 fest.

- **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. Verringern Sie diesen Wert allerdings nicht zu drastisch, um zu vermeiden, dass mehr Nachrichten aufgrund von Zeitüberschreitungen nicht gesendet werden. 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**.

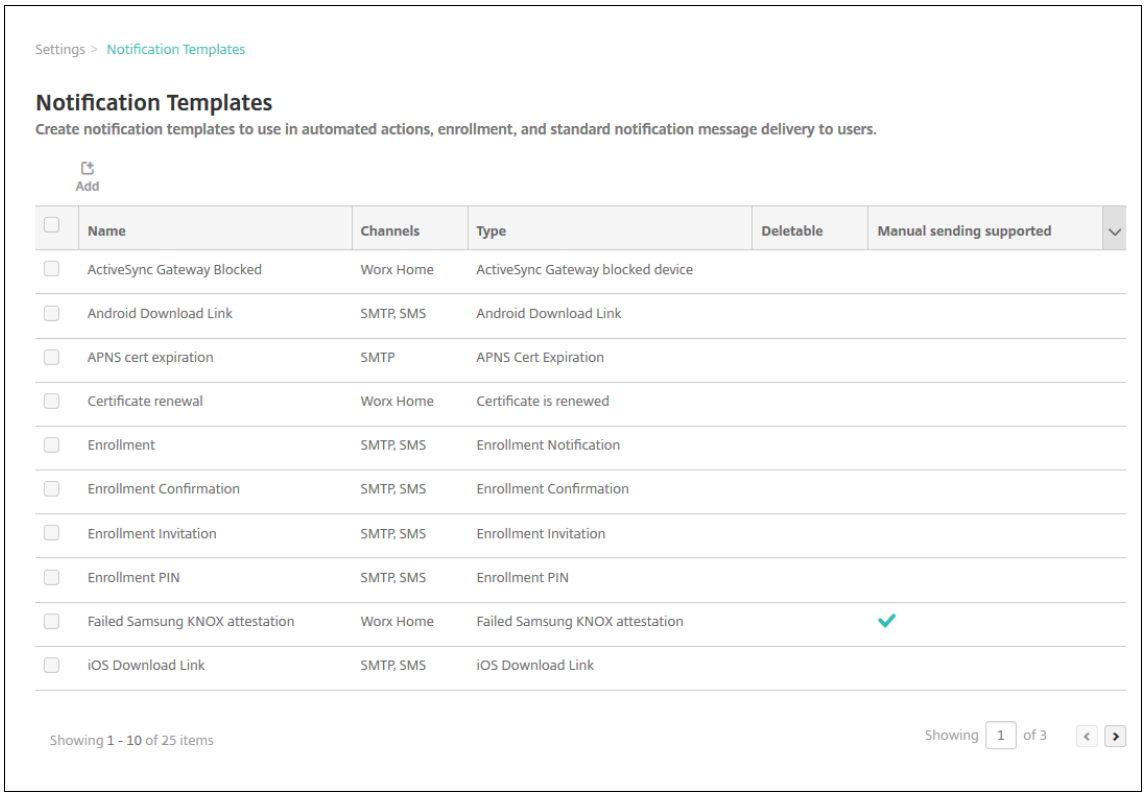
Benachrichtigungsvorlagen erstellen und aktualisieren

Sie können Benachrichtigungsvorlagen in Citrix Endpoint Management erstellen oder aktualisieren, die für automatisierte Aktionen, bei der Registrierung und für Standardbenachrichtigungen an Benutzer verwendet werden. Sie können Benachrichtigungsvorlagen zum Senden von Nachrichten über zwei verschiedene Kanäle konfigurieren: Citrix Secure Hub oder SMTP.

Citrix Endpoint Management enthält viele vordefinierte Benachrichtigungsvorlagen. Diese sind auf die diversen Ereignisse ausgelegt, auf die Citrix Endpoint Management automatisch für jedes Gerät im System reagiert.

> **Hinweis:**
>
> Für die Verwendung von SMTP als Kanal für den Versand von Benachrichtigungen müssen Sie den Kanal vor dem Aktivieren zunächst einrichten. Citrix Endpoint Management fordert Sie beim Hinzufügen von Benachrichtigungsvorlagen zum Einrichten der Kanäle auf, wenn dies nicht bereits geschehen ist.

1. Klicken Sie in der Citrix Endpoint Management-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 SMTP-Server eingerichtet ist, wird eine Meldung bezüglich der Verwendung von SMTP-Benachrichtigungen angezeigt. Sie können wählen, ob Sie den SMTP-Server sofort oder später einrichten möchten.

   Wenn Sie sich für eine sofortige Einrichtung des 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 den SMTP-Server später einrichten, können Sie die Kanäle beim Hinzufügen oder Bearbeiten einer Benachrichtigungsvorlage nicht aktivieren. Die Kanäle stehen demnach nicht zum Senden von Benutzerbenachrichtigungen zur Verfügung.

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 Dropdownliste 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 keine Vorlage dieses Typs hinzufügen.

   > **Hinweis:**
   >
   > Unterhalb bestimmter Vorlagentypen wird "Manuelles Senden wird unterstützt"angezeigt. Diese Vorlagentypen sind in der Liste **Benachrichtigungen** im **Dashboard** und auf der Seite **Geräte** verfügbar. Von dort aus können Sie die Benachrichtigung manuell an Benutzer senden. Manuelles Senden ist bei Vorlagen, bei denen für das Betreffs- oder Nachrichtenfeld die folgenden Makros verwendet werden, über keinen Kanal möglich:

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

     > **Hinweis:**
     >
     > Die Citrix Endpoint Management-Konsole enthält im Englischen die Begriffe "Blacklist"und "Whitelist". Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

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 **Citrix Secure Hub** auswählen, erhalten nur iOS- und Android-Geräte Benachrichtigungen. Diese werden im Infobereich des Geräts angezeigt.
   - Wenn Sie **SMTP**auswählen, erhalten Benutzer, die sich mit ihrer E-Mail-Adresse registriert haben, die Nachricht.

   Citrix 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 Citrix 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 weitere Empfänger (z. B. einen Unternehmensadministrator) hinzufügen, indem Sie deren Adressen in diesem Feld eintragen. Verwenden Sie Semikola (;), um Makros und weitere Adressen voneinander zu trennen. Zum Senden von Ad-hoc-Benachrichtigungen können Sie Empfänger 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. Dieses Feld 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.

4. Klicken Sie auf **Hinzufügen**. Wenn alle Kanäle richtig konfiguriert sind, werden sie in dieser Reihenfolge auf der Seite **Benachrichtigungsvorlagen** angezeigt: SMTP und Citrix Secure Hub. Falsch konfigurierte Kanäle werden nach den richtig konfigurierten Kanälen angezeigt.

Bearbeiten einer Benachrichtigungsvorlage

1. Wählen Sie eine Benachrichtigungsvorlage aus. Die Bearbeitungsseite für diese Vorlage wird angezeigt. Sie können die Vorlage mit Ausnahme des Felds **Typ** bearbeiten 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.

Konfigurieren von Rollen mit RBAC

June 25, 2024

Mit der rollenbasierten Zugriffssteuerung (RBAC) in Citrix Endpoint Management können Sie Benutzern und Gruppen Rollen zuweisen. Rollen sind Berechtigungssätze, die den Zugriff von Benutzern auf Systemfunktionen steuern.

Citrix Endpoint Management enthält die folgenden Standardbenutzerrollen. Sie können die Standardrollen als Vorlagen verwenden und anpassen, um ihre eigenen Benutzerrollen zu erstellen.

- **Administrator:** gewährt vollen Zugriff auf das System.
- **Benutzer:** ermöglicht Benutzern die Registrierung von Geräten und den Zugriff auf das Selbsthilfeportal.

Mit dem RBAC-Feature in Citrix Endpoint Management ist Folgendes möglich:

- Erstellen und Bearbeiten von Benutzerrollen
- Zuweisen von Rollen zu lokalen Benutzergruppen und Active Directory-Gruppen
- Zuweisen von Rollen zu Administratoren in Citrix Cloud über **Identitäts- und Zugriffsverwaltung > Administratoren**. Weitere Informationen finden Sie unter Hinzufügen von Rollen zu Citrix Cloud-Administratoren.

Verwenden der RBAC-Features

Sie können lokalen Benutzern, Cloudadministratoren (in Citrix Cloud) und lokalen Benutzergruppen und Active Directory-Gruppen Rollen zuweisen.

- **Lokale Benutzer:** Weisen Sie lokalen Benutzern Rollen über **Verwalten > Benutzer** zu. Sie können lokalen Benutzern nur eine Rolle zuweisen. Um die Rollen zu ändern, können Sie das

Benutzerkonto manuell bearbeiten. Sie können auch eine Gruppe für lokale Benutzer erstellen und dieser eine Rolle zuweisen.

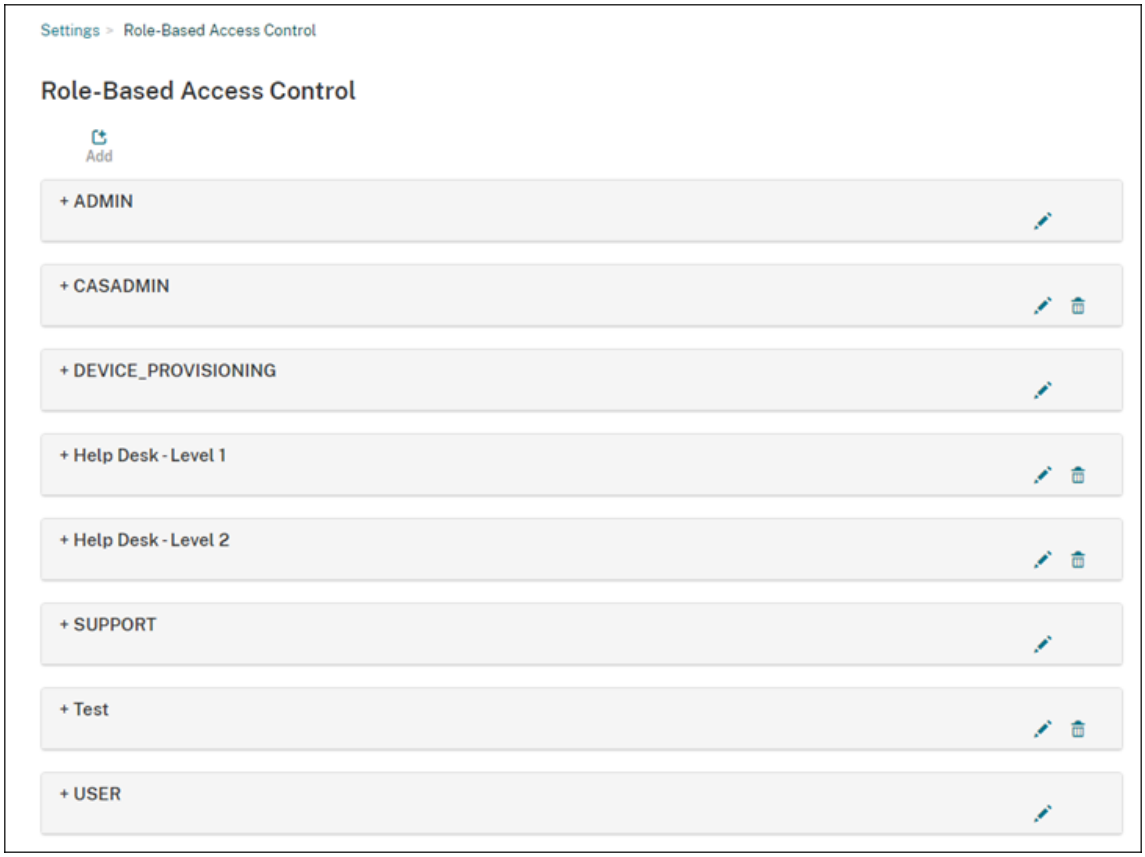
- **Cloudadministratoren:** Ein Cloudadministrator ist ein spezielles Benutzerkonto, das Citrix Cloud erstellt, wenn Ihrem Citrix Cloud-Kundenkonto ein Administrator hinzugefügt wird. Ein Cloudadministratorkonto verwendet denselben Benutzernamen wie das Administratorkonto in Citrix Cloud. Erstellen Sie RBAC-Rollen in der Citrix Endpoint Management-Konsole und weisen Sie diesen Benutzern Rollen über **Identitäts- und Zugriffsverwaltung > Administratoren** in Citrix Cloud zu.
- **Active Directory Gruppen:** Alle Benutzer in einer Active Directory-Gruppe haben die gleichen Berechtigungen. 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. Ein Benutzer, der beiden Gruppen angehört, kann Geräte von Managern und Mitarbeitern suchen und eine Datenlöschung darauf durchführen. Wenn ein Benutzer zu Gruppen mit widersprüchlichen Berechtigungen gehört, haben die zulässigen Berechtigungen Vorrang.

Weitere Informationen finden Sie unter Informationen zu Benutzerkonten.

Erstellen oder Bearbeiten von Rollen

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben, um auf die Seite **Einstellungen** zuzugreifen.
2. Klicken Sie auf **Rollenbasierte Zugriffssteuerung**. Auf der Seite **Rollenbasierte Zugriffssteuerung** werden die Standardbenutzerrollen und alle von Ihnen hinzugefügten Rollen angezeigt.

   Klicken Sie auf das Pluszeichen (+) neben einer Rolle, um alle Berechtigungen für diese Rolle anzuzeigen.



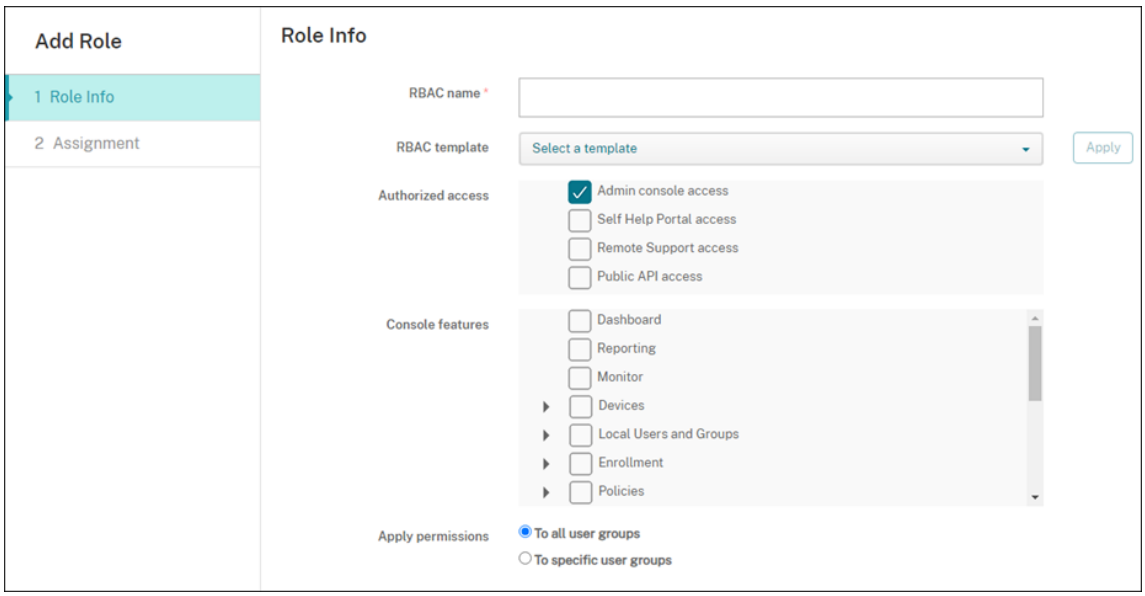
3. Klicken Sie zum Hinzufügen einer Rolle auf **Hinzufügen**. Zum Bearbeiten einer vorhandenen Rolle klicken Sie auf das Stiftsymbol rechts neben der Rolle.

   > **Hinweis:**
   >
   > Sie können eine Rolle löschen, indem Sie auf das Papierkorbsymbol rechts neben einer von Ihnen definierten Rolle klicken. Sie können die Standardbenutzerrollen nicht löschen.

4. Geben Sie auf der Seite **Rolle hinzufügen** die folgenden Informationen ein:

   - **RBAC-Name:** Geben Sie einen aussagekräftigen Namen für die neue Benutzerrolle ein. Sie können den Namen einer vorhandenen Rolle nicht ändern.
   - **RBAC-Vorlage:** Wählen Sie optional eine Vorlage als Ausgangsbasis für die neue Rolle aus. (Beim Bearbeiten einer Rolle können Sie keine Vorlagen auswählen oder ändern.) RBAC-Vorlagen sind die Standardbenutzerrollen, die den Zugriff auf Systemfunktionen definieren.

   Klicken Sie auf **Übernehmen**, damit die Kontrollkästchen **Autorisierter Zugriff** und **Konsolenfeatures** aufgefüllt werden. Citrix Endpoint Management füllt diese Felder mit den vordefinierten Zugriffs- und Featureberechtigungen für die ausgewählte Vorlage aus.



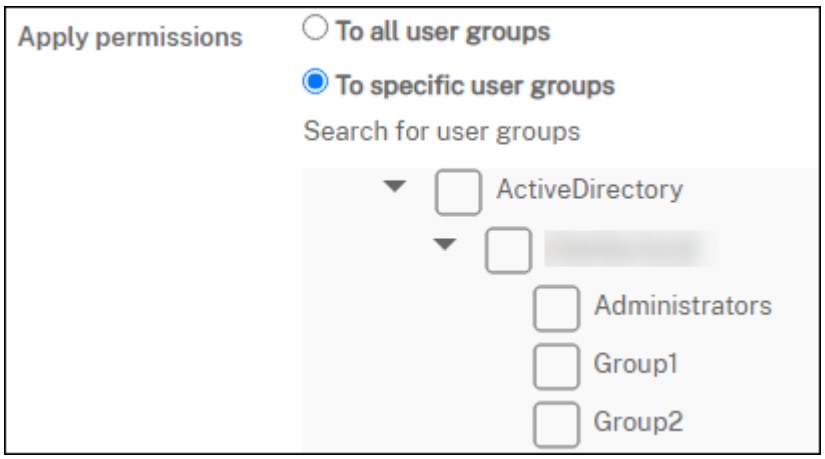
5. Zum Anpassen der Rolle aktivieren bzw. deaktivieren Sie die Kontrollkästchen unter **Autorisierter Zugriff** und **Konsolenfeatures**.

   Klicken Sie auf das Dreieck neben einem Konsolenfeature, um die spezifischen Berechtigungen für dieses Feature anzuzeigen und auszuwählen. Beim Klicken auf das oberste Kontrollkästchen werden die einzelnen Berechtigungen nicht ausgewählt. Wählen Sie einzelne Optionen aus, nachdem Sie die Berechtigung auf der obersten Ebene erweitert haben.

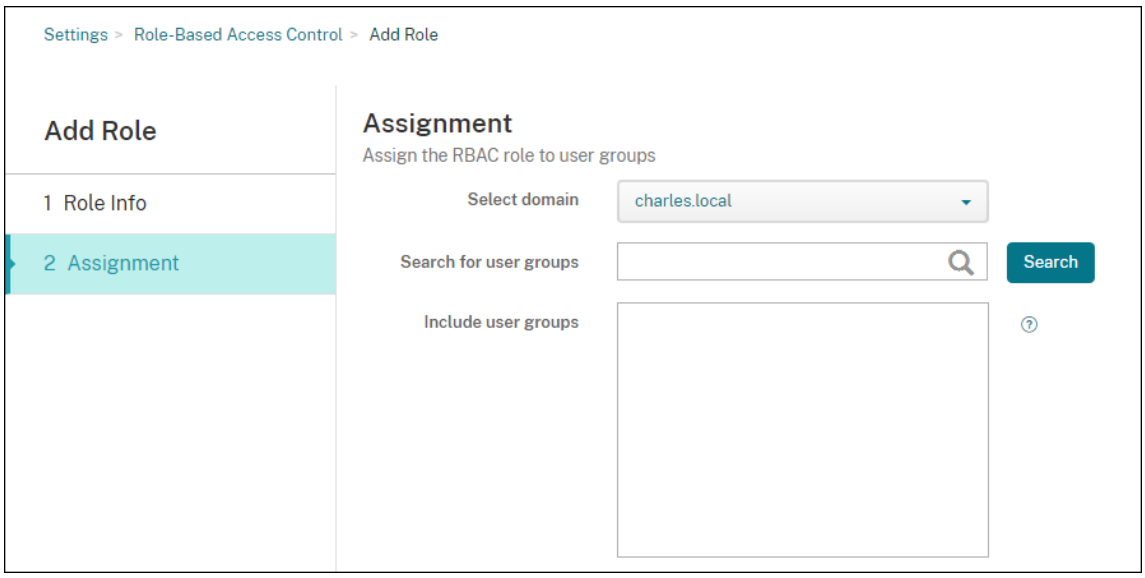
6. **Berechtigungen anwenden:** Klicken Sie auf **Auf bestimmte Benutzergruppen**, um Berechtigungen auf die von Ihnen ausgewählten Gruppen anzuwenden.

   Beispiel: Ein RBAC-Administrator verfügt über Berechtigungen für die Benutzergruppe “ActiveDirectory”:

   - Der Administrator kann nur auf Informationen für Benutzer zugreifen, die in der Gruppe “ActiveDirectory”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** und geben Sie die folgenden Informationen zum Zuweisen der Rolle zu Benutzergruppen ein.



   - **Domäne auswählen:** Wählen Sie eine Domäne aus der Liste aus.
   - **Nach Benutzergruppen suchen:** Klicken Sie auf **Suchen**, um eine Liste aller verfügbaren Gruppen anzuzeigen. Geben Sie den Gruppennamen vollständig oder teilweise ein, um die Suche einzugrenzen.
   - **Benutzergruppen einschließen:** Wählen Sie in der nun angezeigten Liste die Benutzergruppen aus, denen Sie die Rolle zuweisen möchten.

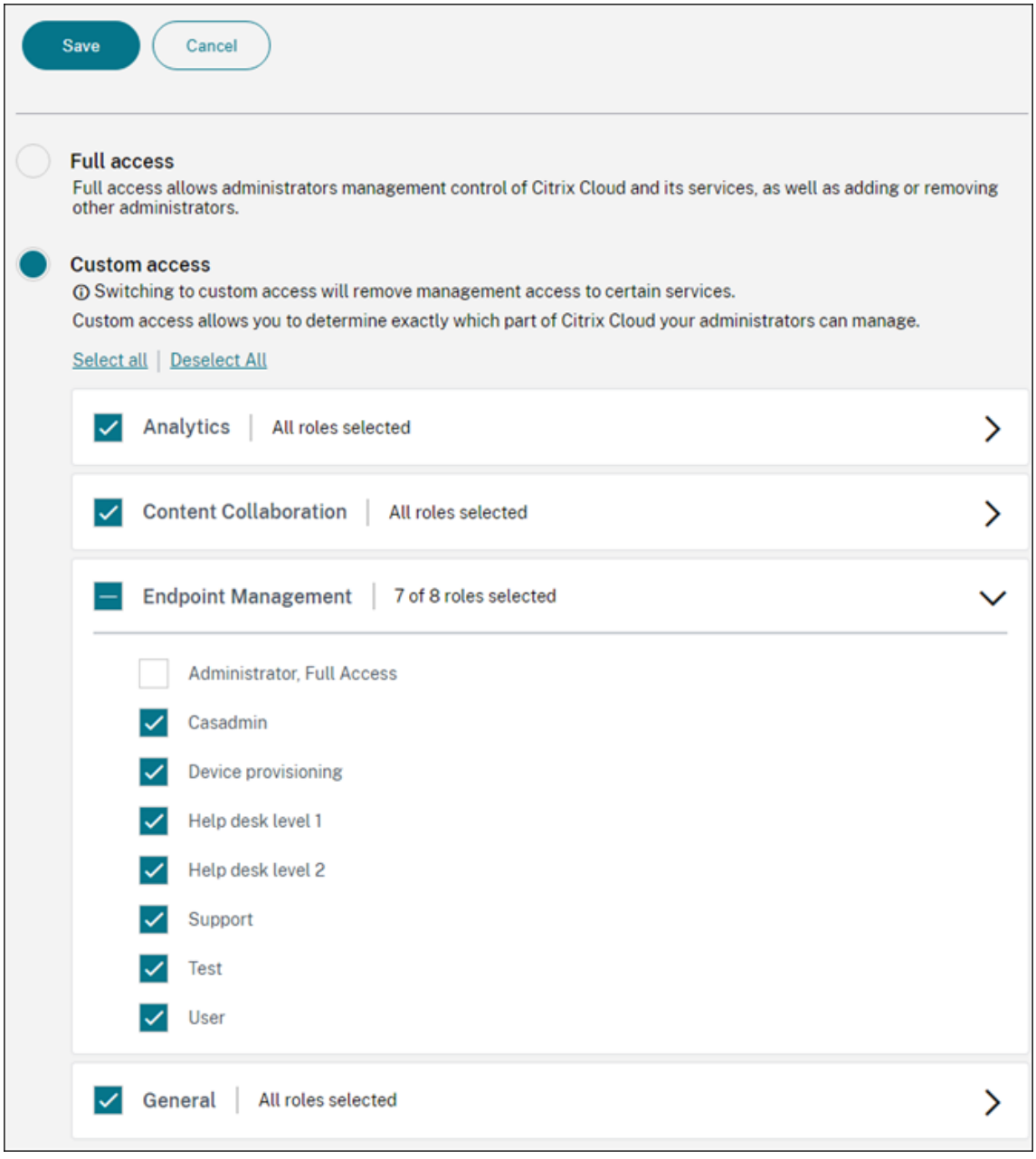
8. Klicken Sie auf **Speichern**.

Hinzufügen von Rollen zu Citrix Cloud-Administratoren

Anstatt über die Citrix Endpoint Management-Konsole können Sie RBAC-Rollen auch über die Citrix Cloud-Konsole Ihren Citrix Cloud-Administratoren zuzuweisen.

1. Navigieren Sie in der Citrix Cloud-Konsole zu **Identitäts- und Zugriffsverwaltung > Administratoren**.
2. Wählen Sie einen Identitätsanbieter und geben Sie eine E-Mail-Adresse ein, um einen Administrator hinzuzufügen. Klicken Sie auf **Einladen**.

   Klicken Sie am Ende einer bestehenden Administratorzeile auf die drei Punkte **...**, um die Berechtigungen zu bearbeiten.
3. Klicken Sie auf **Benutzerdefinierter Zugriff**. Wenn Sie dem Administrator Berechtigungen zuweisen, können Sie die in der Citrix Endpoint Management-Konsole erstellten RBAC-Rollen auswählen.



4. Klicken Sie auf **Einladung senden**, um eine Einladung an einen neuen Administrator zu senden, oder klicken Sie auf **Speichern**, um die Bearbeitung des Administrators abzuschließen.

Vordefinierte Rollen

Jeder vordefinierten RBAC-Rolle sind bestimmte Zugriffs- und Featureberechtigungen zugewiesen. In den folgenden Tabellen werden die einzelnen Berechtigungen für die Administratorrolle und die Benutzerrolle beschrieben. Sie können die vordefinierten Rollen nicht löschen oder bearbeiten.

- Eine vollständige Liste der Standardberechtigungen für jede integrierte Rolle finden Sie unter Role-Based Access Control Defaults.
- Weitere Informationen zu den Citrix Endpoint Management-Benutzerkonten finden Sie unter Informationen zu Benutzerkonten.

> **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 Citrix Endpoint Management-System zu bearbeiten.

Administratorrolle

Die vordefinierte Administratorrolle ermöglicht spezifischen Zugriff in Citrix Endpoint Management. Standardmäßig sind **Autorisierter Zugriff** (außer Selbsthilfeportal), **Konsolenfeatures** und **Berechtigungen anwenden** aktiviert.

Sie können die Rolle für lokale Benutzer, denen die Administratorrolle zugewiesen ist, über **Verwalten > Benutzer** ändern. Verwenden Sie für Cloudbenutzer mit Administratorrolle die Citrix Cloud-Konsole, um die Rolle zu ändern. Standardmäßig haben Cloud- und lokale Benutzer mit Administratorrolle Vollzugriff.

Autorisierter Zugriff für Administratoren

Zugriff über Administratorkonsole	Administratoren haben Zugriff auf alle Features der Citrix Endpoint Management-Konsole.

Zugriff auf das Selbsthilfeportal	Standardmäßig können Administratoren nicht auf das Selbsthilfeportal zugreifen. (Benutzer mit der Benutzerrolle können nur auf das Selbsthilfeportal zugreifen.)
Remotesupportzugriff	Administratoren haben Zugriff auf das Remotesupport-Feature.
Zugriff über öffentliche API	Mit der öffentlichen API für Administratoren können Aktionen, die in der Citrix Endpoint Management-Konsole verfügbar sind, programmatisch durchgeführt werden. Ein Beispiel für solche Aktionen ist das Verwalten von Zertifikaten, Apps, Geräten, Bereitstellungsgruppen und lokalen Benutzern.

Konsolenfeatures für Administratoren	Administratoren haben uneingeschränkten Zugriff auf die Citrix Endpoint Management-Konsole.

Dashboard	Das **Dashboard** ist die erste Seite, die Administratoren nach der Anmeldung an der Citrix Endpoint Management-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 bei Citrix Endpoint Management eingeladen werden.
Richtlinien	Die Seite **Verwalten > Geräterichtlinien** dient zur Verwaltung von Geräterichtlinien wie VPN und Netzwerk.
App	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.
Bereitstellungsgruppe	Auf der Seite **Konfigurieren > Bereitstellungsgruppen** verwalten Sie Bereitstellungsgruppen und die ihnen zugeordneten Ressourcen.
Registrierungsprofil	Auf der Seite **Konfigurieren > Registrierungsprofile** legen Sie fest, wie die Benutzer ihre Geräte registrieren können.
Alexa for Business	Auf der Seite **Einstellungen** verwalten Sie Ihre Alexa for Business-Profile.
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 Citrix 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.

Geräteeinschränkungen für Administratoren 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.
Einschränkung 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. Einschließlich: Gerät orten, Gerätetracking.
Gerät sperren	Remotesperren eines Geräts, sodass es nicht verwendet werden kann.
Gerät entsperren	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 aktivieren	Speichern eines Umgehungscodes auf einem betreuten iOS-Gerät bei aktivierter Aktivierungssperre. Zum Löschen der Daten auf dem Gerät verwenden Sie diesen Code, um die Aktivierungssperre automatisch aufzuheben.

Residente Benutzer abrufen	Liste der Benutzer, die auf dem aktuellen Gerät aktive Konten haben. Diese Aktion erzwingt eine Synchronisierung zwischen Gerät und Citrix Endpoint Management-Konsole.
Residenten Benutzer abmelden	Abmelden des aktuellen Benutzers erzwingen.
Residenten Benutzer löschen	Die aktuelle Sitzung für einen bestimmten Benutzer löschen. Der Benutzer kann sich erneut anmelden.
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 Citrix Endpoint Management-Konsole.
Auf Gerät bereitstellen	Senden von Apps, Benachrichtigungen, Einschränkungen und anderen Ressourcen 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 Citrix Endpoint Management.
Geräte importieren	Importieren einer Gerätegruppe aus einer Datei in Citrix Endpoint Management.
Gerätetabelle exportieren	Sammeln von Geräteinformationen auf der Geräteseite und Exportieren in eine CSV-Datei.
Gerät widerrufen	Verhindern der Verbindung zwischen einem Gerät und Citrix Endpoint Management.
App-Sperre	Verhindern des Zugriffs auf alle Apps auf einem Gerät. Unter Android verhindert diese Einschränkung, dass sich Benutzer bei Citrix Endpoint Management anmelden können. Unter iOS können Benutzer sich anmelden, jedoch nicht auf Apps zugreifen.

Apps löschen	Diese Einschränkung löscht auf Android-Geräten das Citrix Endpoint Management-Konto der Benutzer. Auf iOS-Geräten wird mit dieser Einschränkung der Verschlüsselungsschlüssel gelöscht, den Benutzer für den Zugriff auf Citrix Endpoint Management-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	Auf der Seite **Verwalten > Geräte** können Sie betreute Geräte in den Modus “Verloren” versetzen, damit das betreute Gerät mit dem Sperrbildschirm gesperrt wird. Sie können das Gerät dann orten, wenn das Gerät verloren oder gestohlen wurde.
Modus ‘Verloren’deaktivieren	Auf der Seite **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”auf Geräten bereitstellen.
Gerät herunterfahren	Herunterfahren von iOS-Geräten über die Citrix Endpoint Management-Konsole.
Gerät neu starten	Neustarten von iOS-Geräten über die Citrix Endpoint Management-Konsole.
Geräteregistrierungszertifikat erneuern	ZS-Zertifikat für Gerät erneuern

Lokale Benutzer und Gruppen Administratoren verwalten auf der Seite **Verwalten > Benutzer** in Citrix Endpoint Management 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 Citrix Endpoint Management.

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 Citrix Endpoint Management.
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 Citrix Endpoint Management.
Kategorie hinzufügen/löschen	Hinzufügen oder Löschen einer Kategorie für die Anzeige von Apps im App-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 aus einem öffentlichen App-Store oder einer Volume Purchase-Lizenz.

App-Store- oder Unternehmensbücher hinzufügen/löschen
Öffentliche bzw. Unternehmensbücher Bereitstellungsgruppe zuweisen
App-Store- oder Unternehmensbücher bearbeiten

Aktion

Aktion hinzufügen/löschen	Hinzufügen oder Entfernen einer Aktion, die über einen Auslöser und die zugehörige Antwort definiert wird. Ein Auslöser ist ein Ereignis, eine Geräte- oder Benutzereigenschaft oder der Name der installierten App.
Aktion bearbeiten	Ändern einer Aktion, die über einen Auslöser und die zugehörige Antwort definiert wird. Ein Auslöser ist ein Ereignis, eine Geräte- oder Benutzereigenschaft oder der Name der installierten App.
Aktion 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

Alexa for Business Verwalten von Alexa for Business-Profilen.

Räume hinzufügen/löschen/bearbeiten
Raumprofile hinzufügen/löschen/bearbeiten
Skillgruppen hinzufügen/löschen/bearbeiten

Einstellungen für Administratoren Administratoren konfigurieren diverse Einstellungen auf der Seite **Einstellungen**.

RBAC	RBAC-Zuweisung. **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 Citrix Endpoint Management-System zu bearbeiten.
LDAP	Verwalten LDAP-kompatibler Verzeichnisse, z. B. von Active Directory, zum Importieren von Gruppen, Benutzerkonten und zugehörigen Eigenschaften.
Registrierung	Aktivieren von Registrierungssicherheitsmodi für Benutzer und das Selbsthilfeportal.
Releasemanagement	Anzeigen des aktuell installierten Release. Inklusive Releasemanagementupdate.
Zertifikate	APNs-Zertifikat bearbeiten
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 und -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 App-Store. Hinzufügen eines benutzerdefinierten Logos für den App-Store oder Citrix Secure Hub.
SMS-Gateway des Netzbetreibers	Einrichten von Netzbetreiber-SMS-Gateways zum Konfigurieren von Benachrichtigungen, die Citrix Endpoint Management durch SMS-Gateways 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.
Google Chrome	Konfigurieren von Citrix Endpoint Management für die Kommunikation mit Ihrem Google Workspace-Konto.
Apple-Bereitstellungsprogramm	Hinzufügen eines Apple-Bereitstellungsprogramm-Kontos zu Citrix Endpoint Management.
Apple Configurator-Geräteregistrierung	Konfigurieren von Apple Configurator-Einstellungen in der Citrix Endpoint Management-Konsole.
iOS-/Volume Purchase-Einstellungen	Hinzufügen von Apple Volume Purchase-Konten.
NetScaler Gateway	Konfigurieren der NetScaler Gateway-Einstellungen (jetzt NetScaler Gateway) in Citrix Endpoint Management.
Netzwerkzugriffssteuerung (NAC)	Festlegen der Bedingungen zum Einordnen von Geräten als nicht richtlinientreu, sodass diese Geräte keinen Zugriff auf das Netzwerk haben

Servereigenschaften	Hinzufügen und Ändern von Servereigenschaften. Erfordert einen Neustart von Citrix Endpoint Management auf allen Knoten.
Virtual Apps and Desktops	Zulassen, dass Benutzer Citrix Virtual Apps and Desktops über die Citrix Workspace-App hinzuzufügen.
Citrix Files	Citrix Endpoint Management mit Enterprise-Konten: Konfigurieren Sie Einstellungen für Verbindungen mit dem ShareFile-Konto und dem Administratordienstkonto, um Benutzerkonten zu verwalten. Eine Citrix Files-Domäne und Administratoranmeldeinformationen sind erforderlich. Citrix Endpoint Management mit Speicherzonenconnectors: Konfigurieren Sie Citrix Endpoint Management zum Verweisen auf Netzwerkfreigaben und SharePoint-Speicherorte, die in Speicherzonenconnectors definiert sind.
Android Enterprise	Konfigurieren der Android Enterprise-Servereinstellungen.
Identitätsanbieter (IdP)	Konfigurieren eines Identitätsanbieters.
Citrix Endpoint Management Tools	Zugriff auf die Citrix Endpoint Management Tools-Seite.
Windows-Massenregistrierung	Einstellungen für Windows-Massenregistrierung konfigurieren

Support Administratoren können verschiedene Supportaufgaben ausführen.

NetScaler Gateway-Konnektivitätsprüfung	Durchführen diverser Verbindungsprüfungen für NetScaler Gateway nach IP-Adresse. Erfordert Benutzernamen und Kennwort.

Citrix Endpoint Management-Konnektivitätsprüfung	Durchführen von Konnektivitätsprüfungen für bestimmte Citrix Endpoint Management-Features, z. B. Datenbank, DNS und Google-Abonnement.
Citrix Produktdokumentation	Zugriff auf die öffentliche Citrix Endpoint Management-Dokumentationssite.
Citrix Knowledge Center	Rufen Sie die Citrix Support-Website auf, um nach Artikeln der Knowledge Base zu suchen.
Protokolle	Protokolldateien anzeigen und herunterladen
Makros	Auffüllen der Benutzer- oder Geräteeigenschaftsdaten im Textfeld eines Profils, einer Richtlinie, 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.
PKI-Konfiguration	Importieren und Exportieren von PKI-Konfigurationsinformationen.
Hilfsprogramm für APNs-Signierung	Senden einer Anforderung für ein APNs-Signaturzertifikat und Hochladen eines Citrix Secure Mail-APNs-Zertifikats für iOS.
Citrix Insight Services	Hochladen von Protokollen an Citrix Insight Services (CIS) für Hilfe bei verschiedenen Problemen.
NetScaler Gateway Connector für Exchange ActiveSync - Gerätestatus	Statusabfrage für ein Gerät in Citrix Endpoint Management. Der Status wird dann an den Connector für Exchange ActiveSync gesendet. Die Abfrage basiert auf der Geräte-ID in ActiveSync.

Gruppenzugriff einschränken Administratoren können auf alle Benutzergruppen Berechtigungen anwenden.

Konsolenfeatures für das Geräteprovisioning Benutzer mit der Geräteprovisioningrolle haben den folgenden eingeschränkten Zugriff auf die Citrix Endpoint Management-Konsole. Standardmäßig

sind die folgenden Features aktiviert.

Geräteeinschränkungen

Gerät bearbeiten	Ändern der Einstellungen auf dem Gerät.
Gerät hinzufügen/löschen	Hinzufügen oder Löschen von Geräten in Citrix Endpoint Management.

Einstellungen für das Geräteprovisioning Geräteprovisioningbenutzer können auf die Seite **Einstellungen** zugreifen, jedoch keine Features konfigurieren.

Benutzerrolle

Benutzer mit der Benutzerrolle haben den folgenden eingeschränkten Zugriff auf Citrix Endpoint Management.

Autorisierter Zugriff für Benutzer

Selbsthilfeportal	Benutzern nur Zugriff auf das Selbsthilfeportal in Citrix Endpoint Management geben.

Konsolenfeatures für Benutzer Benutzer haben den folgenden eingeschränkten Zugriff auf die Citrix Endpoint Management-Konsole.

Beschränkter Zugriff für Benutzer auf dem Gerät

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.
Gerät sperren	Remotesperren eines Geräts, sodass es nicht verwendet werden kann.
Gerät entsperren	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 aktivieren	Speichern eines Umgehungscodes auf einem betreuten iOS-Gerät bei aktivierter Aktivierungssperre. Zum Löschen der Daten auf dem Gerät verwenden Sie diesen Code, um die Aktivierungssperre automatisch aufzuheben.
Residente Benutzer abrufen	Liste der Benutzer, die auf dem aktuellen Gerät aktive Konten haben. Diese Aktion erzwingt eine Synchronisierung zwischen Gerät und Citrix Endpoint Management-Konsole.
Residenten Benutzer abmelden	Abmelden des aktuellen Benutzers erzwingen.
Residenten Benutzer löschen	Die aktuelle Sitzung für einen bestimmten Benutzer löschen. Der Benutzer kann sich erneut anmelden.
Gerät klingeln lassen	Remoteauslösen des Klingeltons auf einem Windows-Gerät in voller Lautstärke für 5 Minuten.
Gerät neu starten	Neustarten von Windows-Geräten.
App-Sperre	Verhindern des Zugriffs auf alle Apps auf einem Gerät. Auf Android-Geräten können Benutzer sich nicht bei Citrix Endpoint Management anmelden. Unter iOS können Benutzer sich anmelden, jedoch nicht auf Apps zugreifen.

Apps löschen	Diese Einschränkung löscht auf Android-Geräten das Citrix Endpoint Management-Konto der Benutzer. Auf iOS-Geräten wird mit dieser Einschränkung der Verschlüsselungsschlüssel gelöscht, den Benutzer für den Zugriff auf Citrix Endpoint Management-Features benötigen.
Softwarebestand anzeigen	Anzeigen einer Liste der auf einem Gerät installierten Software.

Registrierungsbeschränkungen für Benutzer

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 für alle Rollen einschränken Für die Standardrollen ist diese Berechtigung standardmäßig festgelegt. Sie kann auf alle Benutzergruppen angewendet werden. Sie können die Rolle nicht bearbeiten.

Lizenzen

December 1, 2023

Informationen zur Citrix-Lizenznutzung finden Sie unter:

- Überwachen von Lizenzen und aktiver Nutzung für Cloud Services
- Überwachen von Lizenzen und aktiver Nutzung für Citrix Endpoint Management

Geräteverwaltung

June 25, 2024

Citrix Endpoint Management kann verschiedenste Gerätetypen in einer einzigen Verwaltungskonsole bereitstellen, verwalten, sichern und inventarisieren.

- Verwenden Sie einen einheitlichen Satz an Geräterichtlinien, um unterstützte Geräte zu verwalten. So können Sie die pro Plattform verfügbaren Geräterichtlinien anzeigen:

  1. Wechseln Sie zur Citrix Endpoint Management-Konsole, und navigieren Sie zu **Konfigurieren > Geräterichtlinien**.
  2. Klicken Sie auf **Hinzufügen** und wählen Sie die Plattformen aus, die Sie anzeigen möchten.

     Weitere Informationen finden Sie unter Filtern der Liste hinzugefügter Geräterichtlinien.

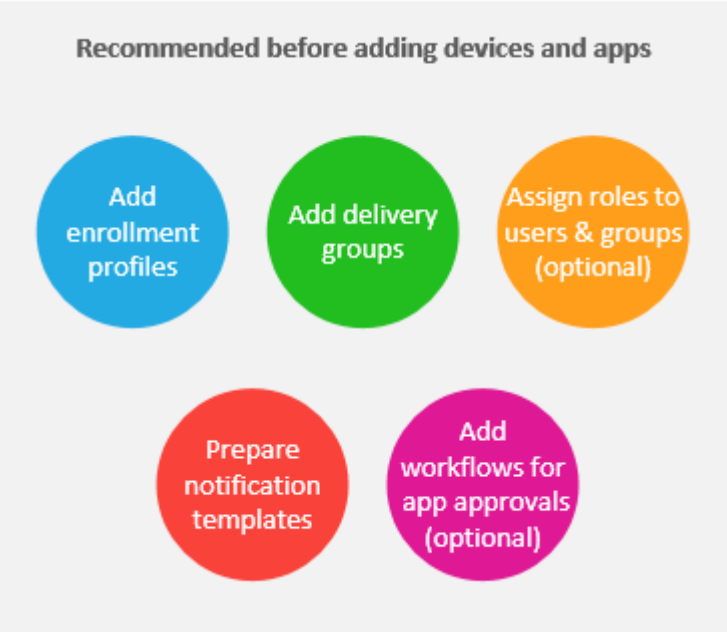
- Schützen Sie Ihre Geschäftsinformationen durch strenge Sicherheit für Identitäten, unternehmenseigene und private Geräte, Apps, Daten und Netzwerke. Definieren Sie die Benutzeridentitäten, die für die Authentifizierung bei Geräten zu verwenden sind. Konfigurieren Sie, wie geschäftliche und persönliche Daten auf Geräten getrennt werden.
- Stellen Sie beliebige Apps für Endbenutzer bereit, unabhängig vom Gerät oder Betriebssystem. Schützen Sie Ihre Informationen auf App-Ebene und sorgen Sie für eine unternehmensgerechte Mobilanwendungsverwaltung.
- Verwenden Sie Provisioning- und Konfigurationssteuerelemente zum Einrichten von Geräten. Dazu gehören die Geräteregistrierung, Zugriffsberechtigungen und das Anwenden von Richtlinien.
- Erstellen Sie eine benutzerdefinierte Sicherheitsgrundlage mit auslösbaren Aktionen mithilfe von Sicherheits- und Compliance-Steuerelementen. Sperren, löschen oder melden Sie beispielsweise jedes Gerät, das gegen definierte Definitionen zur Gerätecompliance verstößt.
- Verwenden Sie OS-Update-Steuerelemente, um Betriebssystemaktualisierungen zu verhindern oder zu erzwingen. Dieses Feature ist entscheidend, um Datenverluste aufgrund von Sicherheitslücken im Betriebssystem zu verhindern.

Artikel zu jeder unterstützten Plattform finden Sie im Inhaltsverzeichnis unter "Geräteverwaltung". Die dort aufgeführten Artikel enthalten spezifische Angaben zu den einzelnen Geräteplattformen. Allgemeine Geräteverwaltungsaufgaben werden im Folgenden in diesem Artikel beschrieben.

Arbeitsabläufe bei der Geräteverwaltung

Die Workflow-Diagramme in diesem Abschnitt enthalten eine empfohlene Abfolge von Aufgaben zur Geräteverwaltung.

1. **Empfohlene Voraussetzungen für das Hinzufügen von Geräten und Apps:** Wenn Sie folgende Schritte im Voraus durchführen, können Sie anschließend Geräte und Apps ohne Unterbrechung konfigurieren.



   Siehe:

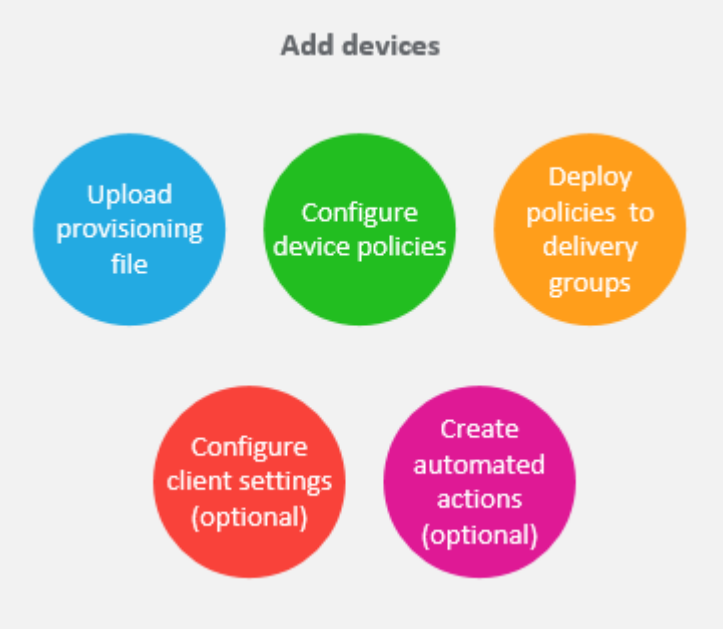
   Ressourcen bereitstellen

   Rollen mit RBAC konfigurieren

   Benachrichtigungsvorlagen erstellen und aktualisieren

   Erstellen und Verwalten von Workflows

2. **Geräte hinzufügen:**



Siehe:

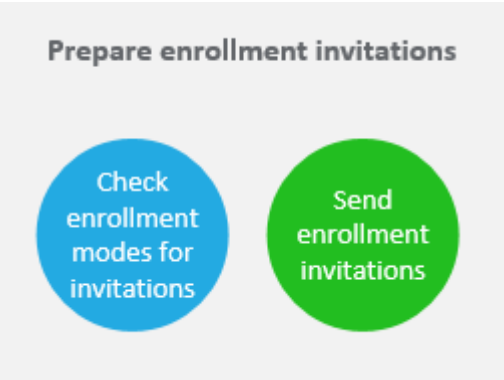
Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen

Geräterichtlinien

In Bereitstellungsgruppen bereitstellen

Automatisierte Aktionen

3. **Vorbereiten von Registrierungseinladungen:** Sie können eine Registrierungseinladung an Benutzer mit iOS-, iPadOS- und macOS-Geräten, Android Enterprise-Geräten und Android-Legacygeräten senden. Führen Sie folgende Schritte aus, wenn Sie Registrierungseinladungen verwenden möchten.



Siehe:

Registrierungssicherheitsmodi konfigurieren

Benachrichtigung an Geräte senden

4. **Apps hinzufügen:**

   Siehe:

   MAM SDK

   Apps hinzufügen

   Info zu App-Kategorien

   Workflows anwenden

   In Bereitstellungsgruppen bereitstellen

5. **Fortlaufende Geräte- und App-Verwaltung:** Neben der Verwendung des Citrix Endpoint Management-Dashboards empfehlen wir Ihnen, für jede Version das Kapitel Neue Features zu lesen. "Neue Features"enthält Informationen zu erforderlichen Aktionen, z. B. zum Konfigurieren neuer Geräterichtlinien.

Siehe:

Überwachen und unterstützen

Berichte

Sicherheitsaktionen

Neue Features

Geräterichtlinien

Registrierungseinladungen

Für die sichere Remoteverwaltung von Benutzergeräten registrieren Sie diese bei Citrix Endpoint Management. Die Citrix Endpoint Management-Clientsoftware wird auf dem Benutzergerät installiert und die Identität des Benutzers wird authentifiziert. Anschließend werden Citrix Endpoint Management und das Benutzerprofil installiert. Informationen zur Registrierung von Geräten mit unterstützten Plattformen finden Sie in den Artikeln zu Geräten im vorliegenden Abschnitt.

In der Citrix Endpoint Management-Konsole

- Sie können eine Registrierungseinladung an Benutzer mit iOS-, iPadOS- und macOS-Geräten, Android Enterprise-Geräten und Android-Legacygeräten senden. Registrierungseinladungen sind für Windows-Geräte nicht verfügbar.
- Sie können eine Einladungs-URL an Benutzer mit iOS- und iPadOS-Geräten, Android Enterprise-Geräten und Android-Legacygeräten senden. Einladungs-URLs sind für Windows-Geräte nicht verfügbar.

Registrierungseinladungen werden wie folgt gesendet:

- Active Directory-Benutzer mit einer in Active Directory verzeichneten E-Mail-Adresse erhalten die Einladung. Lokale Benutzer erhalten die Einladung über die in den Benutzereigenschaften angegebene E-Mail-Adresse.

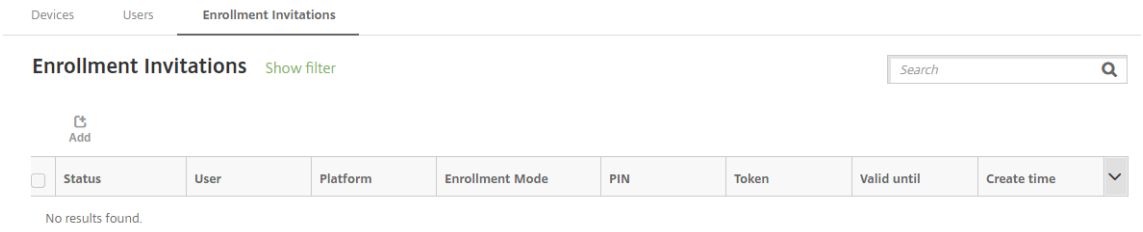
Nach der Registrierung werden die betreffenden **Geräte unter Verwalten > Geräte** als verwaltet angezeigt. Der Status der Einladungs-URL wird als **Angenommen** angezeigt.

Voraussetzungen

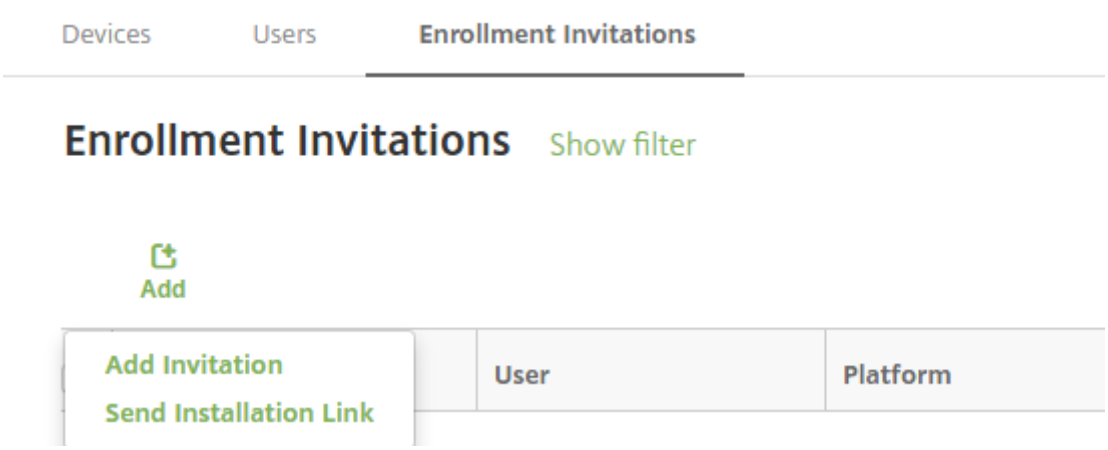
- LDAP konfiguriert
- Bei Verwendung lokaler Gruppen und Benutzer:
  - Eine oder mehrere lokale Gruppen
  - Lokale Benutzer, die lokalen Gruppen zugewiesen sind
  - Bereitstellungsgruppen, die lokalen Gruppen zugeordnet sind
- Bei Verwendung von Active Directory:
  - Bereitstellungsgruppen, die Active Directory-Gruppen zugeordnet sind

Erstellen von Registrierungseinladungen

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Verwalten > Registrierungseinladungen**. Die Seite **Registrierungseinladungen** wird angezeigt.



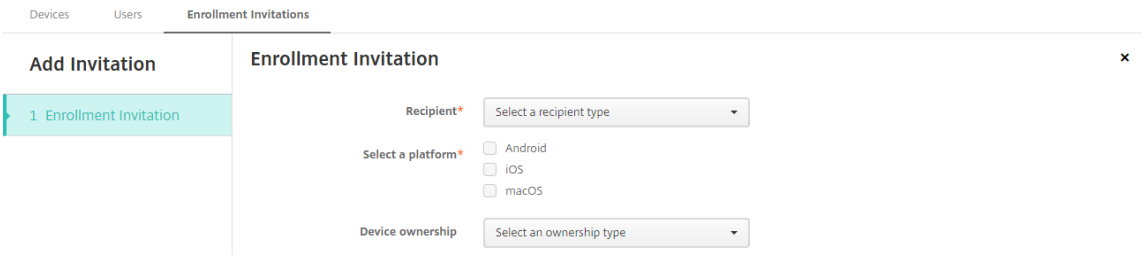
2. Klicken Sie auf **Hinzufügen**. Ein Menü mit Registrierungsoptionen wird eingeblendet.



- 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 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.



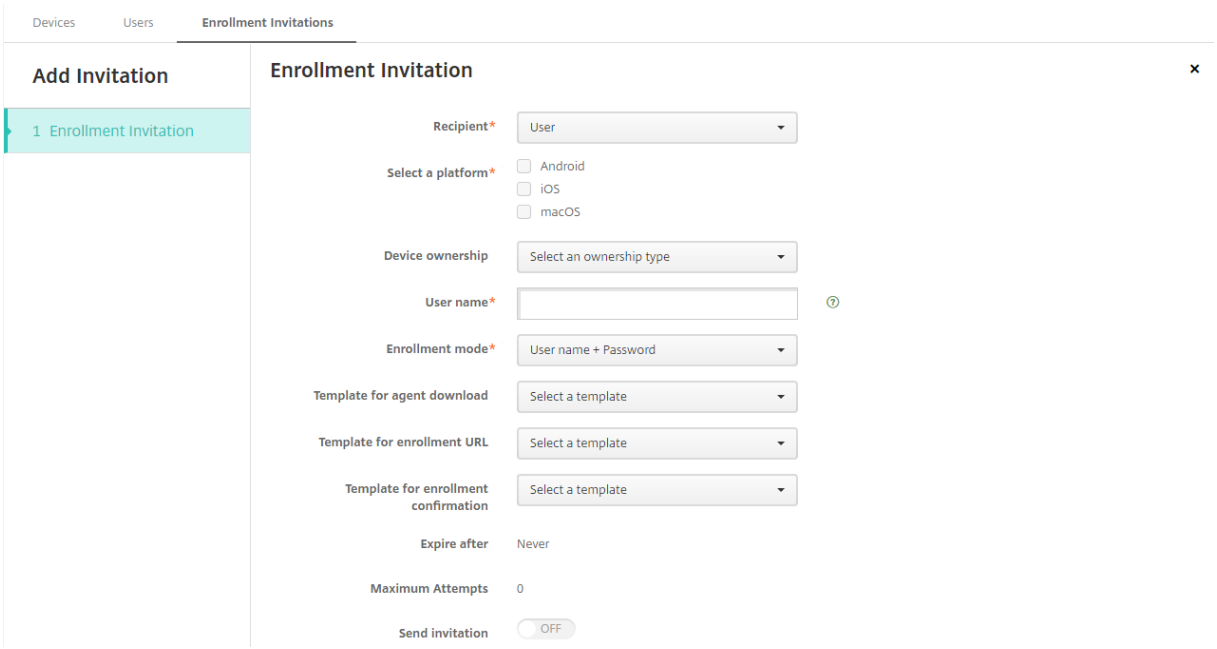
4. Konfigurieren Sie folgende Einstellungen:

   - **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**.
   - **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 in Citrix Endpoint Management als lokaler oder Active Directory-Benutzer vorliegen. Legen Sie bei lokalen Benutzern die E-Mail-Eigenschaft fest, damit Benachrichtigungen an die Benutzer gesendet werden können. Bei Active Directory-Benutzern muss LDAP konfiguriert sein.
    - **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**
        - **Einladungs-URL**
        - **Einladungs-URL + PIN**
        - **Einladungs-URL + Kennwort**
        - **Zweistufig**
        - **Benutzername + PIN**

    Die Unterstützung für den Registrierungsmodus **Hohe Sicherheit** läuft aus. Um Registrierungseinladungen zu senden, können Sie nur die Registrierungsicherheitsmodi **Einladungs-URL**,

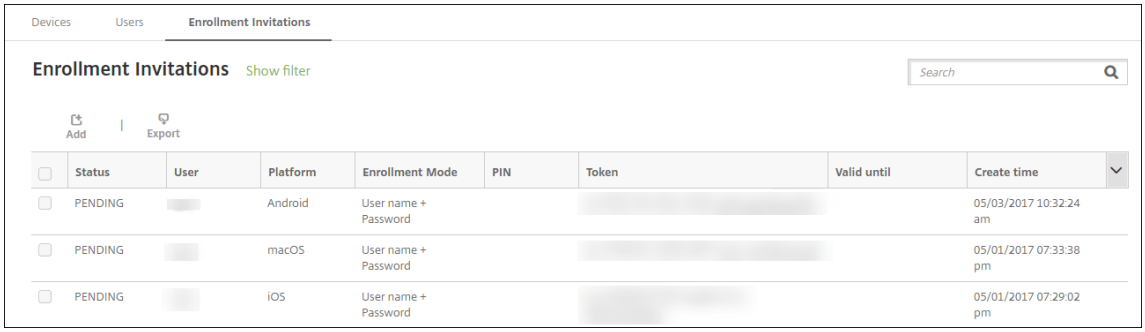
Einladungs-URL + PIN oder **Einladungs-URL + Kennwort** verwenden. Für Geräte, die mit **Benutzername + Kennwort**, **Zweistufig** oder **Benutzername + PIN** registriert werden, müssen Benutzer Citrix Secure Hub herunterladen und ihre Anmeldeinformationen manuell eingeben.

Weitere Informationen finden Sie unter Registrierungssicherheitsmodi nach Plattform. 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. Klicken Sie auf **Registrierungs-PIN**.

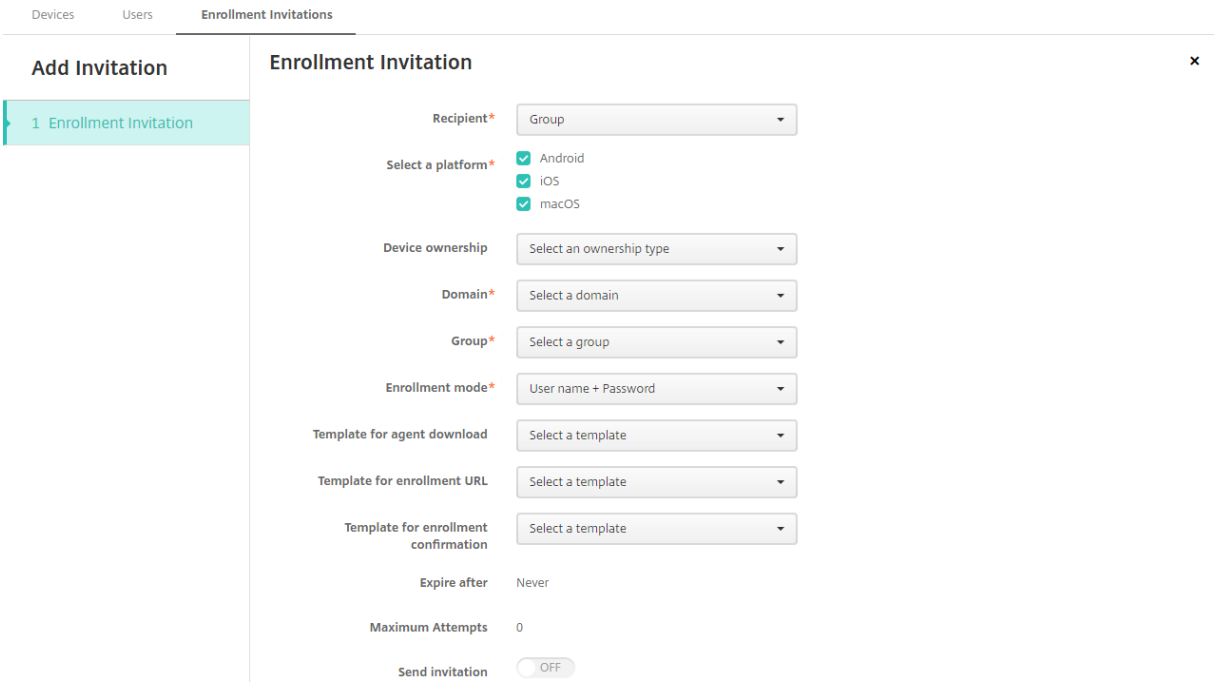
- **Vorlage für Agentdownload:** Wählen Sie die Downloadlinkvorlage **Downloadlink**. Diese Vorlage ist für alle unterstützten Plattformen vorgesehen.
- **Vorlage für Registrierungs-URL:** Wählen Sie **Registrierungseinladung**.
- **Vorlage für Registrierungsbestätigung:** Wählen Sie **Registrierungsbestätigung**.
- **Ablauf nach:** Dieses Feld wird ausgefüllt, wenn Sie den Registrierungssicherheitsmodus konfigurieren. Es gibt an, wann die Registrierung abläuft. Weitere Informationen zum Konfigurieren von Registrierungssicherheitsmodi finden Sie unter Registrierungssicherheitsmodi konfigurieren.
- **Versuche maximal:** Dieser Wert wird festgelegt, wenn Sie den Registrierungssicherheitsmodus konfigurieren. Er gibt an, wie oft der Registrierungsprozess maximal durchgeführt wird.
- **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. Citrix Endpoint Management ruft die Benutzerliste aus Active Directory ab. Die Liste enthält Benutzer, deren Namen Sonderzeichen enthalten.
   - **Registrierungsmodus:** Wählen Sie die gewünschte Registrierungsmethode. Die Standardeinstellung ist **Benutzername + Kennwort**. Einige der folgenden Optionen stehen nicht für alle Plattformen zur Verfügung:
     - **Benutzername + Kennwort**
     - **Einladungs-URL**
     - **Einladungs-URL + PIN**
     - **Einladungs-URL + Kennwort**
     - **Zweistufig**
     - **Benutzername + PIN**

   Die Unterstützung für den Registrierungsmodus **Hohe Sicherheit** läuft aus. 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

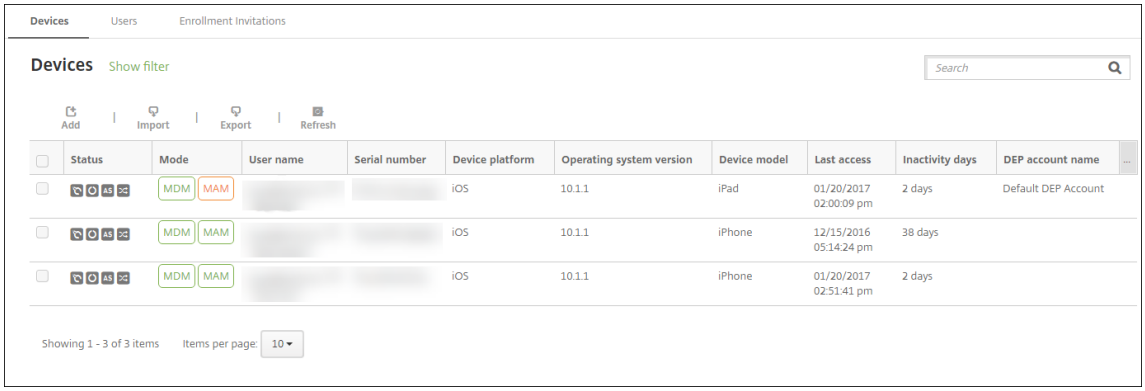
Benutzer Citrix Secure Hub herunterladen und ihre Anmeldeinformationen manuell eingeben.

Es werden nur die Registrierungssicherheitsmodi angezeigt, die für die ausgewählten Plattformen zulässig sind. Weitere Informationen finden Sie unter Registrierungssicherheitsmodi nach Plattform.

> **Hinweis:**
>
> Wenn Sie einen Registrierungssicherheitsmodus mit PIN auswählen, wird das Feld **Vorlage für Registrierungs-PIN** eingeblendet. Klicken Sie auf **Registrierungs-PIN**.

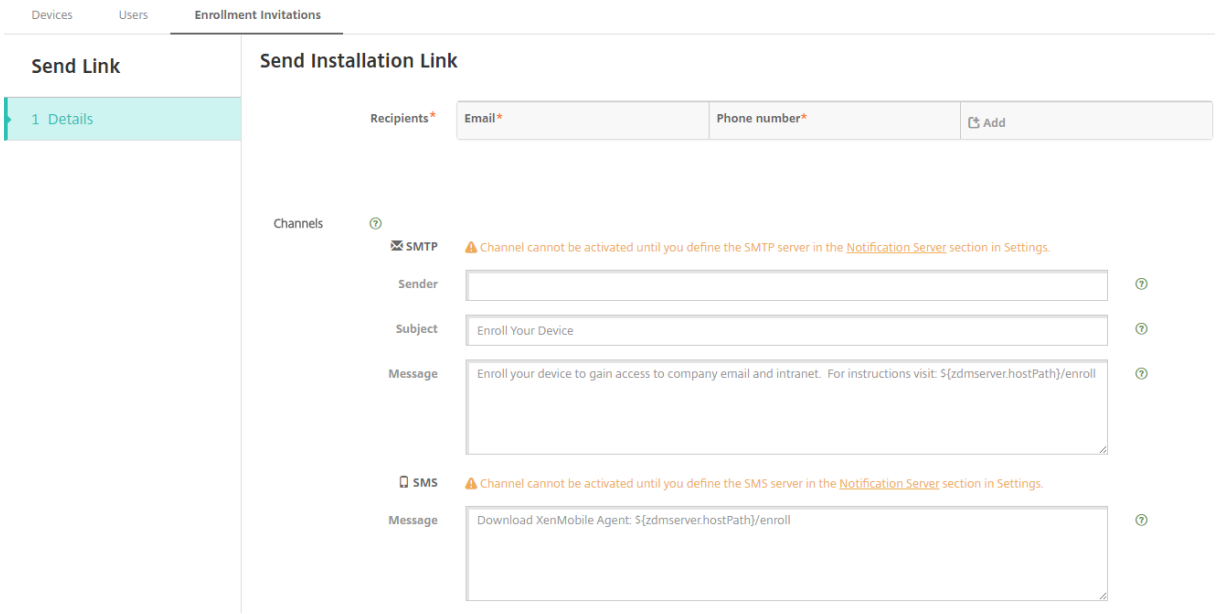
- **Vorlage für Agentdownload:** Wählen Sie die Downloadlinkvorlage **Downloadlink**. Diese Vorlage ist für alle unterstützten Plattformen vorgesehen.
- **Vorlage für Registrierungs-URL:** Wählen Sie **Registrierungseinladung**.
- **Vorlage für Registrierungsbestätigung:** Wählen Sie **Registrierungsbestätigung**.
- **Ablauf nach:** Dieses Feld wird ausgefüllt, wenn Sie den Registrierungssicherheitsmodus konfigurieren. Es gibt an, wann die Registrierung abläuft. Weitere Informationen zum Konfigurieren von Registrierungssicherheitsmodi finden Sie unter Registrierungssicherheitsmodi konfigurieren.
- **Versuche maximal:** Dieser Wert wird festgelegt, wenn Sie den Registrierungssicherheitsmodus konfigurieren. Er gibt an, wie oft der Registrierungsprozess maximal durchgeführt wird.
- **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) auf dem Benachrichtigungsserver über die Seite **Einstellungen** konfigurieren. Details finden Sie unter Benachrichtigungen.



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. Dieses Feld ist erforderlich.
     - **Telefonnummer:** Geben Sie die Telefonnummer des Empfängers ein. Dieses Feld ist erforderlich.

     > **Hinweis:**
     >
     > Zum Löschen eines Empfängers zeigen Sie auf dessen Zeile und klicken dann 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. Klicken Sie dann 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** 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".

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@domainname.com` angezeigt. Die Benutzer müssen den Teil `@domainname.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-Registrierungssicherheit auf NetScaler Gateway	Unterstützung verschiedener Verwaltungsmodi	Unterstützung verschiedener Registrierungsprofile	Android (Legacy)	Android Enterprise	iOS (Benutzerregistrierungsmodus)	iOS	macOS	Windows
Azure AD und Okta als Identitätsanbieter über Citrix Cloud	Clientzertifikat	MDM+MAM oder MDM	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Benutzername + Kennwort	LDAP, LDAP + Clientzertifikat, nur Clientzertifikat	MDM+MAM, MDM oder MAM (Nur-MAM-Modus unterstützt keine Clientzertifikate auf NetScaler Gateway)	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Einladungs-URL	Clientzertifikat	MDM+MAM oder MDM	Ja	Ja	Ja	Nein	Ja	Nein	Nein
Einladungs-URL + PIN	Clientzertifikat	MDM+MAM oder MDM	Ja	Ja	Ja	Nein	Ja	Nein	Nein

MDM-Registrierungssicherheitsmodus	MAM-Registrierungssicherheitsmodus auf NetScaler Gateway	Unterstützung verschiedener Registrierungsmodi	Android (Legacy)	Android Enterprise	iOS (Benutzerregistrierungsmodus)	iOS	macOS	Windows
Einladungs-URL + Kennwort	LDAP, LDAP + Clientzertifikat, nur Clientzertifikat	MDM+MAM oder MDM	Ja	Ja	Ja	Nein	Ja	Nein	Nein
Zweistufige Authentifizierung (Benutzername + Kennwort + PIN)	LDAP, LDAP + Clientzertifikat, nur Clientzertifikat	MDM+MAM oder MDM	Ja	Ja	Ja	Nein	Ja	Ja	Nein
Benutzername + PIN	Clientzertifikat	MDM+MAM 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 Citrix Secure Hub geöffnet. Der Benutzer gibt einen Benutzernamen und ein Kennwort ein, um sein Gerät bei Citrix Endpoint Management zu registrieren.
- **Einladungs-URL**
  - Sendet Benutzern eine Benachrichtigung mit einer Registrierungs-URL. Klickt der Benutzer auf die URL, wird Citrix Secure Hub geöffnet. Der Name des Citrix Endpoint Management-Servers und die Schaltfläche **Ja, registrieren** werden eingeblendet. Der

Benutzer tippt auf **Ja, registrieren**, um das Gerät bei Citrix Endpoint Management 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 Citrix Secure Hub bei Citrix Endpoint Management 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 Citrix Secure Hub geöffnet. Der Name des Citrix Endpoint Management-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 Citrix Secure Hub geöffnet. Es werden der Name des Citrix Endpoint Management-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 Citrix Secure Hub. Wenn Citrix Secure Hub geöffnet wird, wird der Benutzer zur Eingabe eines Benutzernamens und Kennworts aufgefordert, um sein Gerät bei Citrix Endpoint Management 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 bei Citrix Endpoint Management 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 bei Citrix Endpoint Management 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. Informationen zur Registrierung von Windows-Geräten finden Sie unter Windows-Geräte.

Sicherheitsaktionen

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 Citrix Endpoint Management anmelden. Unter iOS können Benutzer sich anmelden, jedoch nicht auf Apps zugreifen.

- **App löschen:** Entfernt das Benutzerkonto aus Citrix 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 registriert sind.
- **Zertifikaterneuerung:**Für unterstützte iOS-, macOS- und Android-Geräte können Sie die Zertifikaterneuerung über die Sicherheitsaktion "Zertifikaterneuerung"starten. Wenn Geräte das nächste Mal eine Verbindung zu Citrix Endpoint Management herstellen, gibt der Citrix Endpoint Management-Server neue Gerätezertifikate basierend auf der neuen Zertifizierungsstelle aus.
- **Einschränkungen deaktivieren:** Dieser Befehl ermöglicht auf betreuten iOS-Geräten das Deaktivieren des vom Benutzer festgelegten Einschränkungskennworts und der Einschränkungseinstellungen durch Citrix Endpoint Management.
- **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 Citrix Endpoint Management 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. Citrix Secure Hub meldet den Standort regelmäßig, wenn das Gerät läuft.
- **Vollständig löschen:** löscht sofort alle Daten und Apps von Geräten, einschließlich Speicherkarten. Gelöschte Geräte bleiben zu Auditzwecken in der Geräteliste auf der Seite **Verwalten > Geräte**. Sie können ein gelöschtes Gerät aus der Geräteliste entfernen.
  - 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 und iPadOS 12-Geräte (Mindestversion): Wenn Sie die vollständige Löschung bestätigen, können Sie entscheiden, ob Sie den Mobilfunktarif auf dem Gerät beibehalten.

Für iOS 11.3-Geräte (Mindestversion): Wenn Sie die vollständige Löschung bestätigen, verhindern Sie, dass iOS-Geräte ein Proximity Setup durchführen. Bei der Einrichtung eines neuen iOS-Geräts können die Benutzer normalerweise ein bereits konfiguriertes iOS-Gerät nutzen. Sie können das Proximity Setup für Geräte blockieren, die von Citrix Endpoint Management verwaltet und gelöscht wurden.

  - 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 Citrix Endpoint Management sie beim Senden des Befehls **Orten** noch einmal 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 der Befehl nur erfolgreich, wenn die Geräte im MDM-Modus “Verloren”sind.

- **Sperren:** Sperrt ein Gerät remote. Eine Sperre ist nützlich, wenn ein Gerät gestohlen wurde und gesperrt werden muss. Citrix Endpoint Management 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 Citrix Endpoint Management-Konsole zu entsperren.
- **Sperren und Kennwort zurücksetzen:** Sperrt Geräte remote und setzt den Passcode zurück.

  - Nicht unterstützt für Geräte, die:
    * bei Android Enterprise im Arbeitsprofilmodus registriert sind und

        * auf denen Android-Versionen vor Android 7.0 läuft
    - Auf in Android Enterprise im Arbeitsprofilmodus registrierten Geräten mit Android 7.0 oder höher tritt Folgendes auf:
        * Der Passcode sperrt das Arbeitsprofil. Das Gerät ist nicht gesperrt.
        * Wenn kein Passcode gesendet wird oder der gesendete Passcode nicht den Anforderungen entspricht und das Arbeitsprofil keinen Passcode hat, wird das Gerät gesperrt.
        * Wenn kein Passcode gesendet wird oder der gesendete Passcode nicht den Anforderungen entspricht, das Arbeitsprofil aber bereits einen Passcode hat, 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. Auf Windows-Tablets und -PCs wird eine Meldung über den ausstehenden Neustart angezeigt. Der Neustart erfolgt nach fünf Minuten.
- **AirPlay-Synchronisierung anfordern/AirPlay-Synchronisierung beenden:** startet bzw. beendet die AirPlay-Synchronisierung auf betreuten iOS-Geräten.
- **Neu starten/Herunterfahren:** startet betreute Geräte sofort bzw. fährt sie sofort herunter.
- **Widerrufen:** Verhindert die Verbindung zwischen Geräten und Citrix Endpoint Management.
- **Sperren/Autorisieren:** 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.
- **Persönlichen Wiederherstellungsschlüssel rotieren:** Wenn Sie die FileVault-Geräterichtlinie aktiviert haben, generiert diese Aktion einen neuen persönlichen Wiederherstellungsschlüssel und ersetzt damit den alten Schlüssel. Sie können die Anforderung abbrechen, solange sie anstehend ist. Klicken Sie hierzu auf **Rotieren des persönlichen Wiederherstellungsschlüssels abbrechen**.
- **Selektiv löschen:** löscht alle Unternehmensdaten und -Apps von Geräten, private Daten und Apps bleiben erhalten. Verwenden Sie nach einer selektiven Löschung die Aktion **Autorisieren** zum erneuten Genehmigen eines Geräts, damit es wieder registriert werden kann. Gelöschte Geräte bleiben zu Auditzwecken in der Geräteliste auf der Seite **Verwalten > Geräte**. Sie können ein gelöschtes Gerät aus der Geräteliste entfernen.
    - 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 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.

- **Entsperren:** löscht den Passcode, der beim Sperren an das Gerät gesendet wurde. Dieser Befehl öffnet das Gerät nicht.

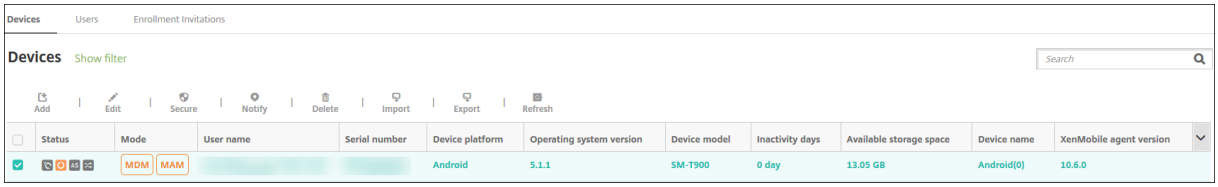
Auf der Seite **Verwalten > Geräte** werden unter **Gerätedetails** außerdem Sicherheitseigenschaften aufgeführt. Dazu gehören Starke ID, Gerätesperrung, Umgehen der Aktivierungssperre und weitere plattformspezifische Informationen. Das Feld **Gerät vollständig löschen** enthält den Benutzer-PIN-Code. Der Benutzer muss den Code eingeben, anschließend erfolgt die Löschung. Wenn der Benutzer den Code vergessen hat, können Sie ihn hier nachsehen.

Sie können einige Aktionen automatisieren. Weitere Informationen hierzu finden Sie unter Automatisierte Aktionen.

Entfernen von Geräten aus der Citrix Endpoint Management-Konsole

> **Wichtig:**
>
> Wenn Sie ein Gerät aus der Citrix Endpoint Management-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 Citrix Endpoint Management-Konsole navigieren Sie zu **Verwalten > Geräte**, wählen Sie ein verwaltetes Gerät und klicken Sie auf **Löschen**.



Durchführen einer selektiven Löschung

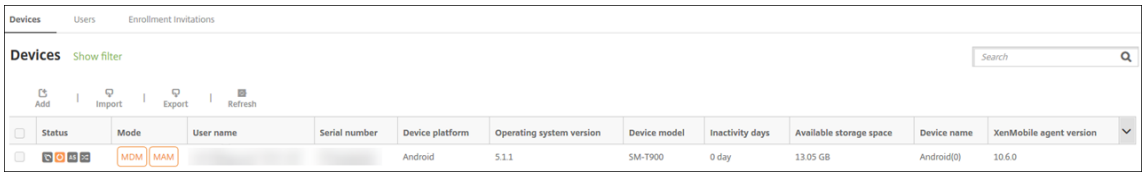
1. Navigieren Sie zu **Verwalten > Geräte**, wählen Sie ein verwaltetes Gerät aus und klicken Sie auf **Sicherheit**.
2. Klicken Sie unter **Sicherheitsaktionen** auf **Selektiv löschen**.
3. Android-Geräte: Klicken Sie nach der Datenlöschung auf **Sicherheitsaktionen** > **Widerrufen**, um das Gerät 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 Citrix Endpoint Management-Konsole gelöscht. Mit der öffentlichen REST-API von Citrix 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.

Apps löschen und Löschen rückgängig machen

1. Gehen Sie zu **Verwalten > Geräte**. Wählen Sie ein Gerät aus.
2. Apps löschen
   - Klicken Sie auf **Sicherheit > Apps löschen**. Ein Dialogfeld mit der folgenden Meldung wird angezeigt: **Möchten Sie wirklich die Apps von diesem Gerät löschen?** Klicken Sie auf **Apps löschen**.
3. Löschen der Apps rückgängig machen
   - Klicken Sie auf **Sicherheit > Löschen der Apps rückgängig machen**. Ein Dialogfeld mit der folgenden Meldung wird angezeigt: **Möchten Sie wirklich das Löschen der Apps von diesem Gerät rückgängig machen?** Klicken Sie auf **Löschen der Apps vom Gerät rückgängig machen**.
4. Registrieren Sie das Gerät erneut als derselbe Benutzer im gleichen Modus.
5. Starten Sie eine MDX-App auf der Seite **Eigene Apps**.
6. Starten Sie Citrix Secure Hub.

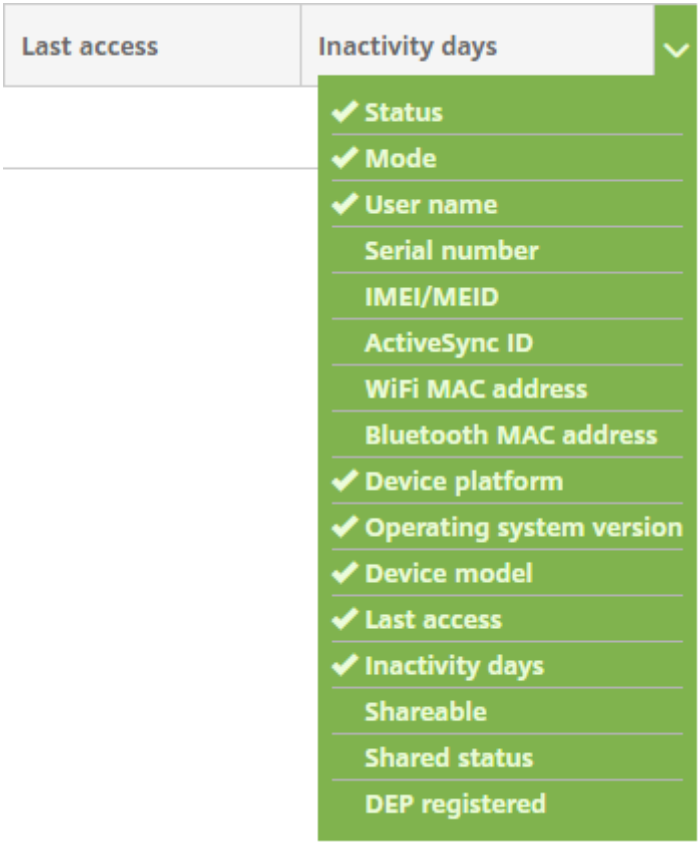
Informationen über Geräte abrufen

In der Citrix Endpoint Management-Datenbank wird eine Liste der Mobilgeräte gespeichert. Sie können der Citrix Endpoint Management-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 **Verwalten > Geräte** der Citrix Endpoint Management-Konsole werden alle Geräte mit folgenden Informationen aufgelistet:

- **Status** (Symbole, die angeben, ob ein Jailbreak vorliegt, ob das Gerät verwaltet wird, ob das ActiveSync-Gateway verfügbar ist und welchen Bereitstellungszustand das Gerät aufweist)
- **Modus:** Gibt den Gerätemodus an, z. B. MDM oder MDM+MAM.
- Weitere Informationen, z. B. **Benutzername**, **Geräteplattform**, **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.



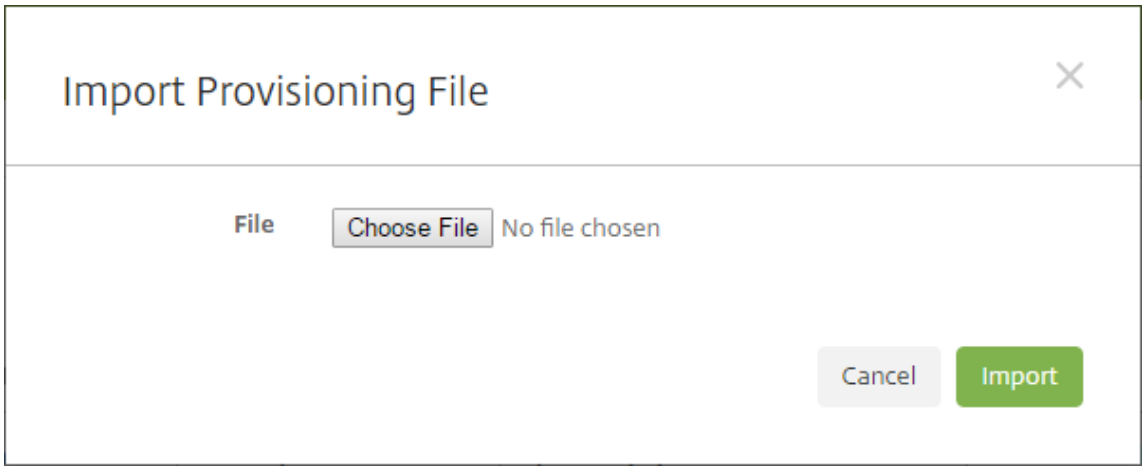
Sie können Geräte manuell hinzufügen, Geräte aus einer Geräteprovisioningdatei importieren, Gerätedetails bearbeiten, die Active Directory-Benutzereigenschaften anpassen, Sicherheitsaktionen durchführen und Benachrichtigungen an Geräte senden. Sie können auch alle Gerätedaten aus der Tabelle in eine 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 Citrix Endpoint Management berücksichtigt.

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.

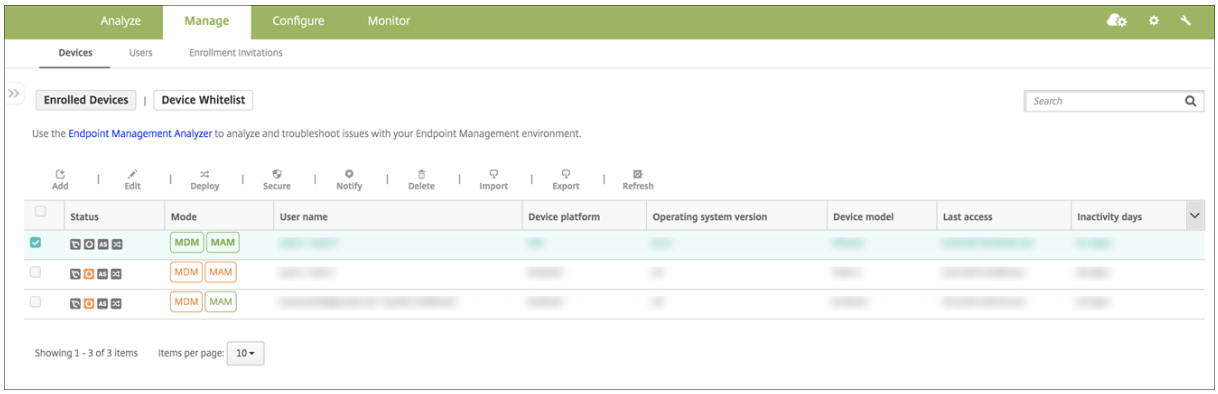
1. Gehen Sie zu **Verwalten > Geräte** und klicken Sie auf **Importieren**. Das Dialogfeld **Provisioningdatei importieren** wird angezeigt.



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 Informationen über Geräte abrufen.

Auf Gerät bereitstellen

Sie können erzwingen, dass ein oder mehrere Geräte eine Verbindung mit Citrix Endpoint Management herstellen. Die ausgewählten Geräte erhalten dann sofort Ressourcen, anstatt auf den nächsten geplanten Check-in zu warten.

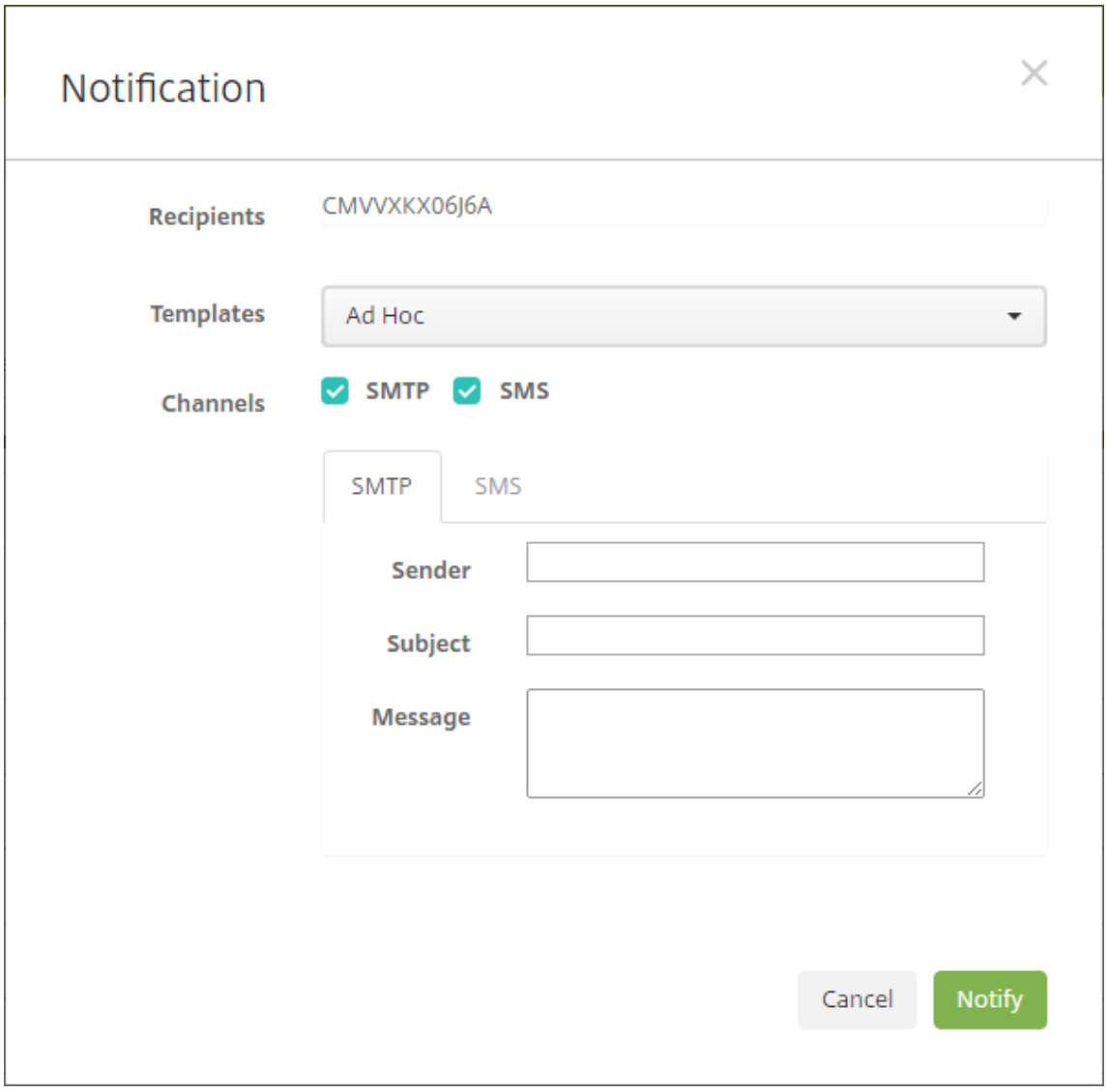


1. Navigieren Sie zu **Verwalten > Geräte**, wählen Sie ein mit MDM oder MDM+MAM verwaltetes Gerät und klicken Sie auf **Bereitstellen**.
2. Klicken Sie im Dialogfeld auf **Bereitstellen**, um die Aktion zu bestätigen.

Benachrichtigung an Geräte senden

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 Dropdownliste 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. Die Standardeinstellung ist **SMTP**. 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**. Citrix Endpoint Management 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.

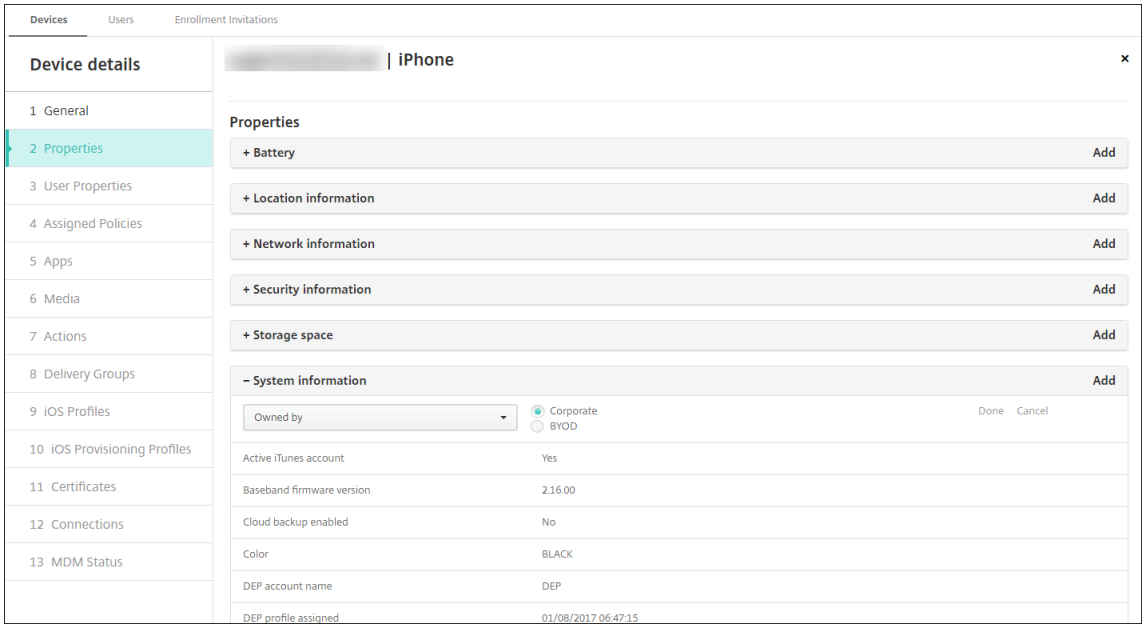
Geräte manuell per Tag kennzeichnen

Sie können Geräte in Citrix Endpoint Management 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 Citrix Endpoint Management-Konsole eine Eigenschaft hinzu.
2. Fügen Sie die Eigenschaft **Besitz von** hinzu und wählen Sie entweder **Unternehmen** oder **BYOD** (Privatgerät).



Anpassen von Active Directory-Benutzerattributen

Sie können Active Directory-Benutzerattribute anpassen, um festzulegen, auf welche Attribute Citrix Endpoint Management zum Erstellen eines Benutzerkontos zugreifen kann.

Um die Liste der Attribute anzuzeigen, fügen Sie die Servereigenschaft `optional.user.identity.attributes` als benutzerdefinierten Schlüssel unter **Einstellungen > Servereigenschaften**hinzu. Im Feld **Wert** können Sie die optionalen Active Directory-Benutzerattribute entfernen und später wiederherstellen, die Citrix Endpoint Management standardmäßig bereitstellt. Weitere Informationen finden Sie unter Servereigenschaften.

Wenn Sie die Liste der Standardwerte bearbeitet und die Änderungen gespeichert haben, können Sie die aktualisierten Active Directory-Benutzerattribute unter **Verwalten > Geräte > Benutzereigenschaften** anzeigen. Die Citrix Endpoint Management-Konsole wird beim nächsten geplanten Einchecken des Geräts aktualisiert oder wenn sich der Benutzer am Gerät anmeldet. Wenn Sie einen Tippfehler machen oder einen nicht unterstützten Wert hinzufügen, ignoriert Citrix Endpoint Management Ihre Änderungen.

Das Entfernen der optionalen Active Directory-Benutzerattribute kann sich auf die folgenden Funktionen auswirken:

- **Provisioning des Benutzerkontos:** Wenn Sie die Werte für den Vor- und Nachnamen entfernen, kann Citrix Endpoint Management das Benutzerkonto nicht für ShareFile und Salesforce bereitstellen.
- **Anmeldungseinladungen:** Wenn Sie die E-Mail- oder Mobiltelefondaten des Benutzers entfernen, kann dieser keine Registrierungseinladung empfangen.

- **Gerätebenachrichtigungen:** Wenn Sie die E-Mail-Daten des Benutzers entfernen, kann dieser keine Benachrichtigungen über SMTP empfangen.
- **Single Sign-On bei Citrix Secure Mail:** Wenn Sie den Anzeigenamen entfernen, kann sich der Benutzer nicht per Single Sign-On bei Citrix Secure Mail anmelden.
- **Benutzereigenschaft und Bereitstellungsregeln:** Wenn Sie eines der optionalen Attribute entfernen, die Sie zum Konfigurieren der Benutzereigenschaft und der Bereitstellungsregeln verwenden, kann dies Auswirkungen auf vorhandene Konfigurationen haben.
- **Aktionen:** Wenn Sie eines der optionalen Attribute entfernen, die Sie zum Festlegen einer automatisierten Aktion unter **Konfigurieren > Aktionen**verwenden, kann dies Auswirkungen auf vorhandene Konfigurationen haben.
- **Benutzerdefinierte Berichte:** Wenn Sie eines der optionalen Attribute entfernen, die Sie in benutzerdefinierten Berichten verwenden, kann dies Auswirkungen auf vorhandene Konfigurationen haben.

Gerätesuche

Zur schnellen Suche enthält der Standardsuchbereich die folgenden Geräteeigenschaften:

- Seriennummer
- IMEI
- WiFi MAC-Adresse
- Bluetooth MAC-Adresse
- Active Sync ID
- Benutzername

Sie können den Suchbereich über eine neue Servereigenschaft konfigurieren, **include.device.properties.during.s** die standardmäßig auf **false** gesetzt ist. Um alle Geräteeigenschaften in eine Gerätesuche einzubeziehen, gehen Sie zu **Einstellungen > Servereigenschaften** und ändern Sie die Einstellung in **true**.

Geräte-Provisioningdateiformate

Viele Mobilfunkanbieter und Mobilgerätehersteller geben Listen autorisierter Mobilgeräte heraus. Sie können diese Listen verwenden, statt lange Mobilgerätelisten manuell einzugeben. Citrix Endpoint Management unterstützt ein für alle unterstützten Gerätetypen (Android, iOS und Windows) geeignetes Importdateiformat.

Eine manuell erstellte Provisioningdatei 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:

```
`1050BF3F5173010816100655105903915244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F5173010816100655105903925244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F5173010816100655105903935244201625379903;iOS;test;
4050BF3F5173010816100655105903935;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

Jede Zeile der Datei enthält ein Gerät. Der erste Eintrag in dem Beispiel bedeutet Folgendes:

- SerialNumber: 1050BF3F5173010816100655105903915
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- PropertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

Alexa for Business

June 25, 2024

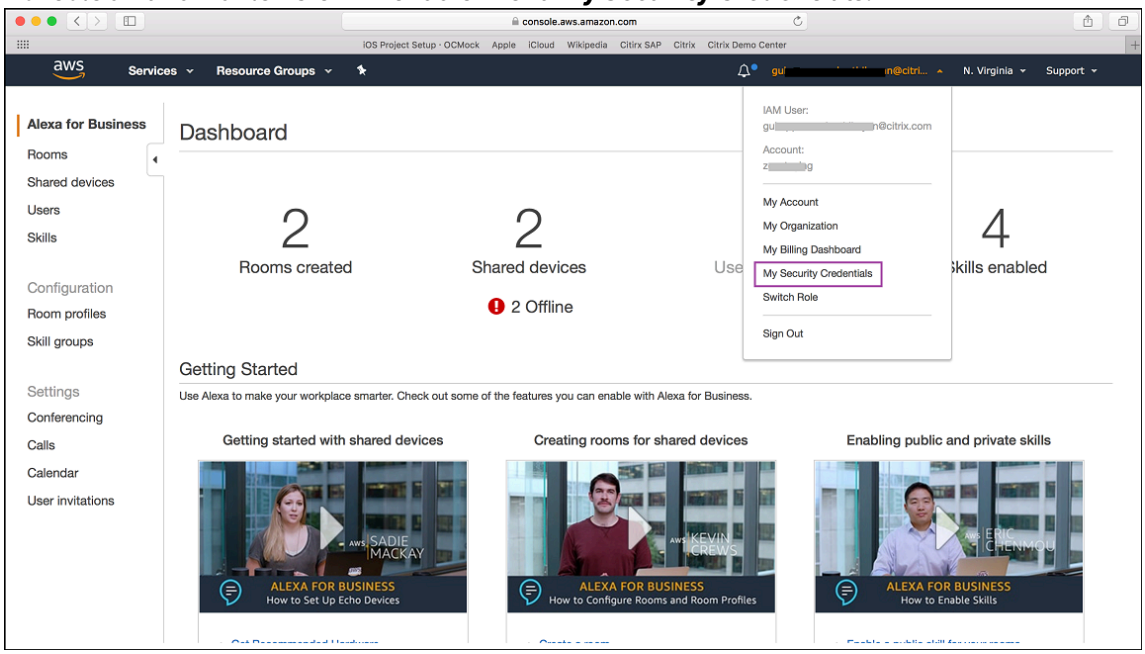
Mit dem Alexa for Business-Dienst von Amazon Web Services (AWS) können Sie eine große Anzahl von Alexa-fähigen Geräten für geschäftliche Zwecke verwalten, beispielsweise für die Unterstützung

von Konferenzräumen. Mit Citrix Endpoint Management können Sie diese Geräte in der Citrix Endpoint Management-Konsole konfigurieren und verwalten. Citrix Endpoint Management stellt Richtlinien nicht direkt auf Alexa-Geräten bereit. Stattdessen aktualisiert Citrix Endpoint Management AWS-Dienste und AWS stellt die Konfigurationen auf Alexa-Geräten bereit.

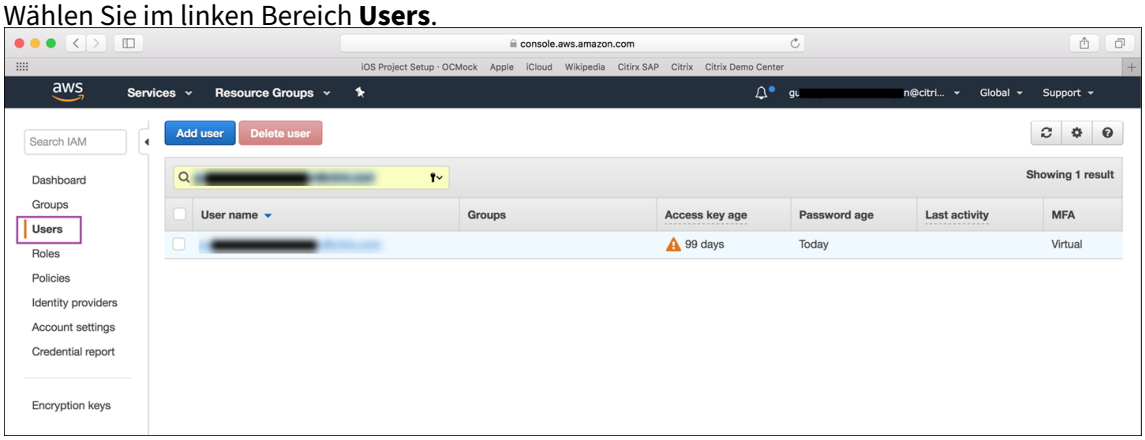
Informationen zur Verwendung von Alexa for Business finden Sie unter Alexa for Business Administration Guide.

Authentifizieren Sie Ihr AWS-Konto bei Citrix Endpoint Management

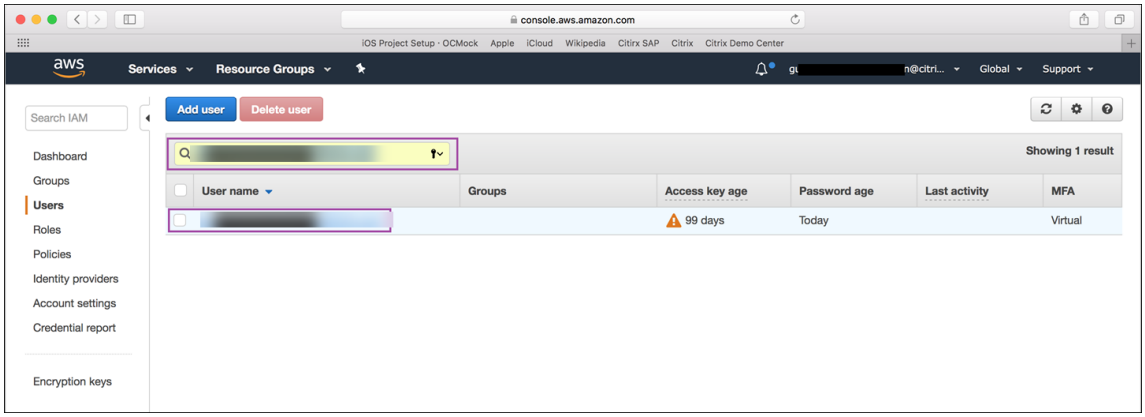
1. Zum Abrufen der Anmeldeinformationen Ihres AWS-Kontos melden Sie sich bei der AWS-Konsole an und wählen Sie im Benutzermenü **My Security Credentials**.



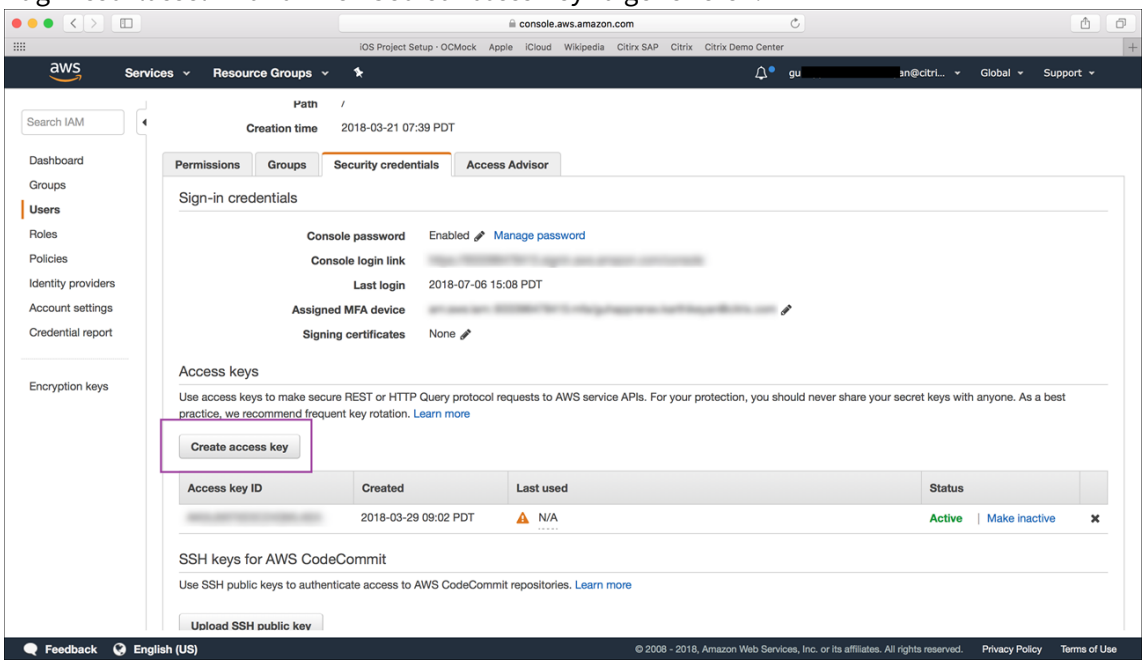
2. Wählen Sie im linken Bereich **Users**.



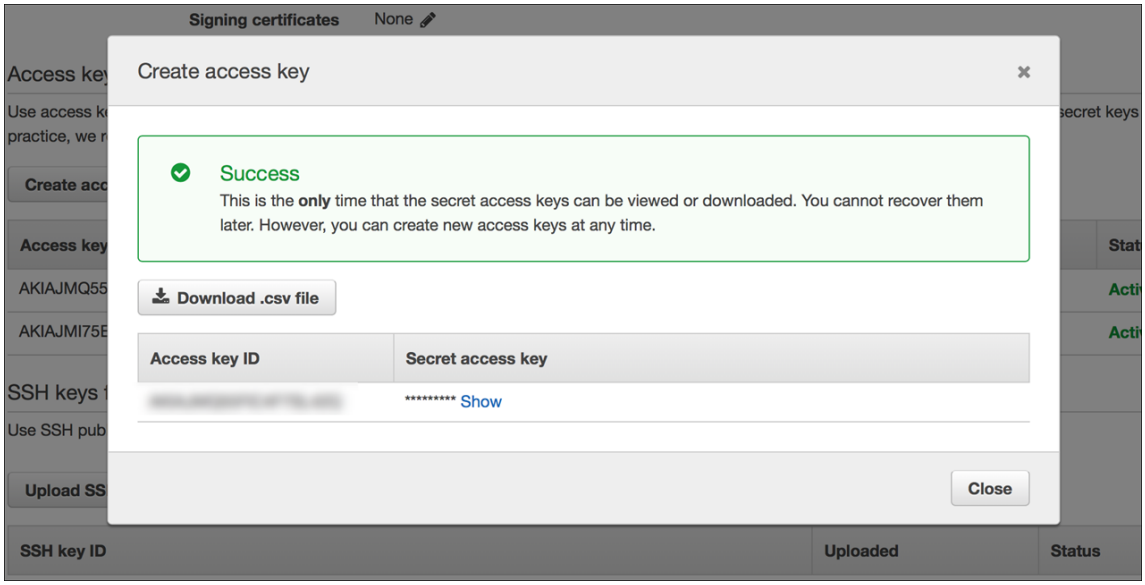
3. Suchen Sie Ihren Benutzernamen und wählen Sie ihn aus.



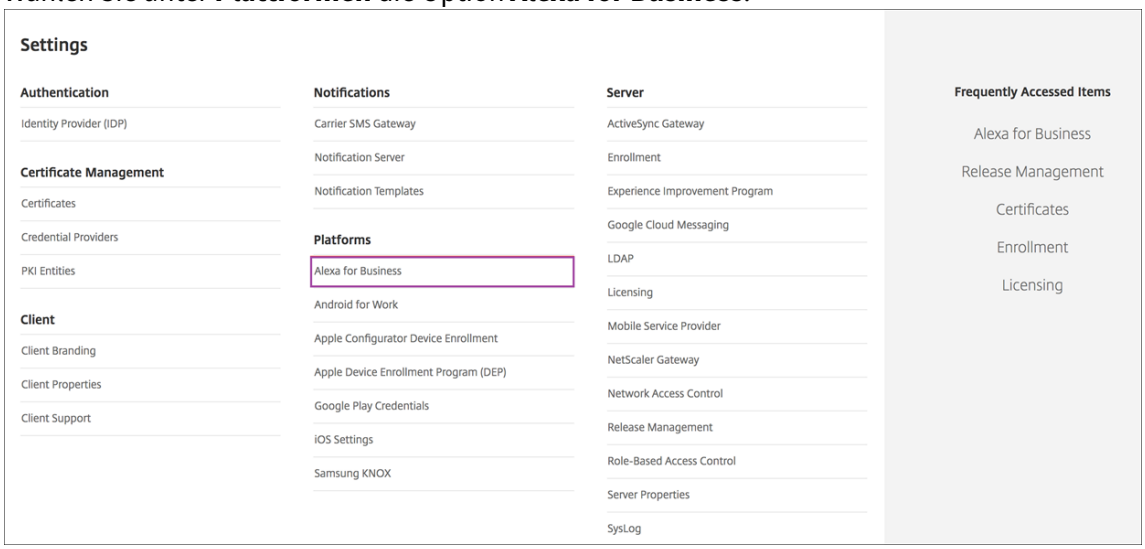
4. Klicken Sie auf der Registerkarte **Security Credentials** auf **Create access key**, um Ihre Zugriffsschlüssel-ID und Ihren Secret Access Key zu generieren.



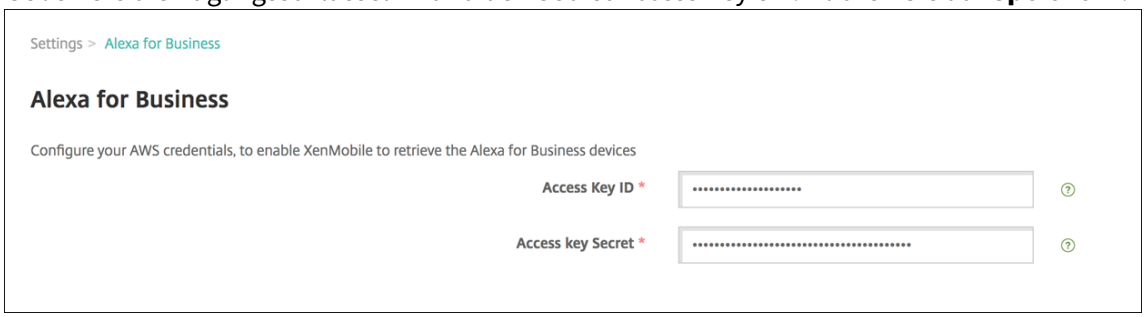
5. Laden Sie die Zugangsschlüssel-ID und den Secret Access Key herunter. Speichern oder notieren Sie beide.



6. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol, um die **Einstellungen** aufzurufen.
7. Wählen Sie unter **Plattformen** die Option **Alexa for Business**.



8. Geben Sie die Zugangsschlüssel-ID und den Secret Access Key ein. Klicken Sie auf **Speichern**.



Alexa for Business in Citrix Endpoint Management konfigurieren

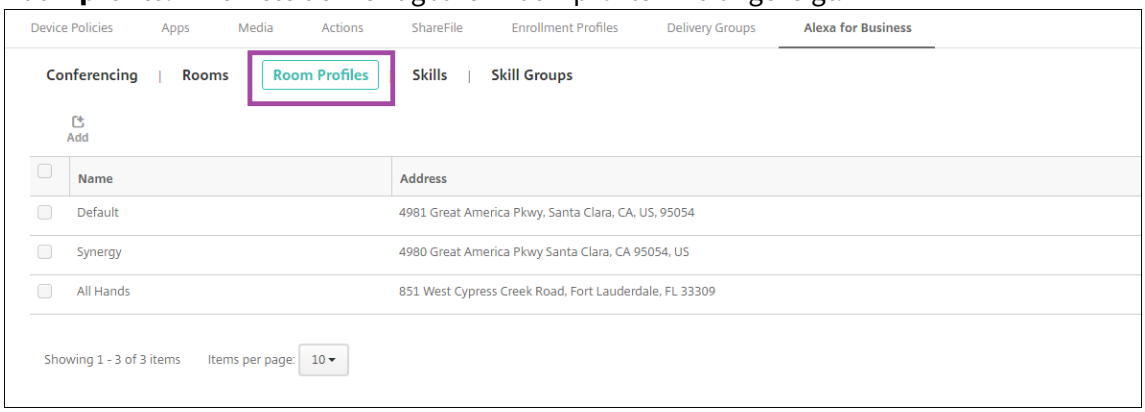
Mit Citrix Endpoint Management können Sie Folgendes konfigurieren:

- Raumprofile mit Einstellungen, die Sie auf Räume anwenden, die über Alexa-Geräte verfügen
- Räume zur Repräsentation der physischen Räume, in denen sich die Geräte befinden
- Skillgruppen zur Zuweisung zu Räumen oder Geräten
- Skills aus dem Alexa-Skills-Shop, die Skillgruppen hinzugefügt werden können
- Konferenzfeatures, mit denen Sie einen Konferenzanbieter auswählen und steuern können, wie Benutzer Besprechungen in Ihren Räumen planen und an ihnen teilnehmen

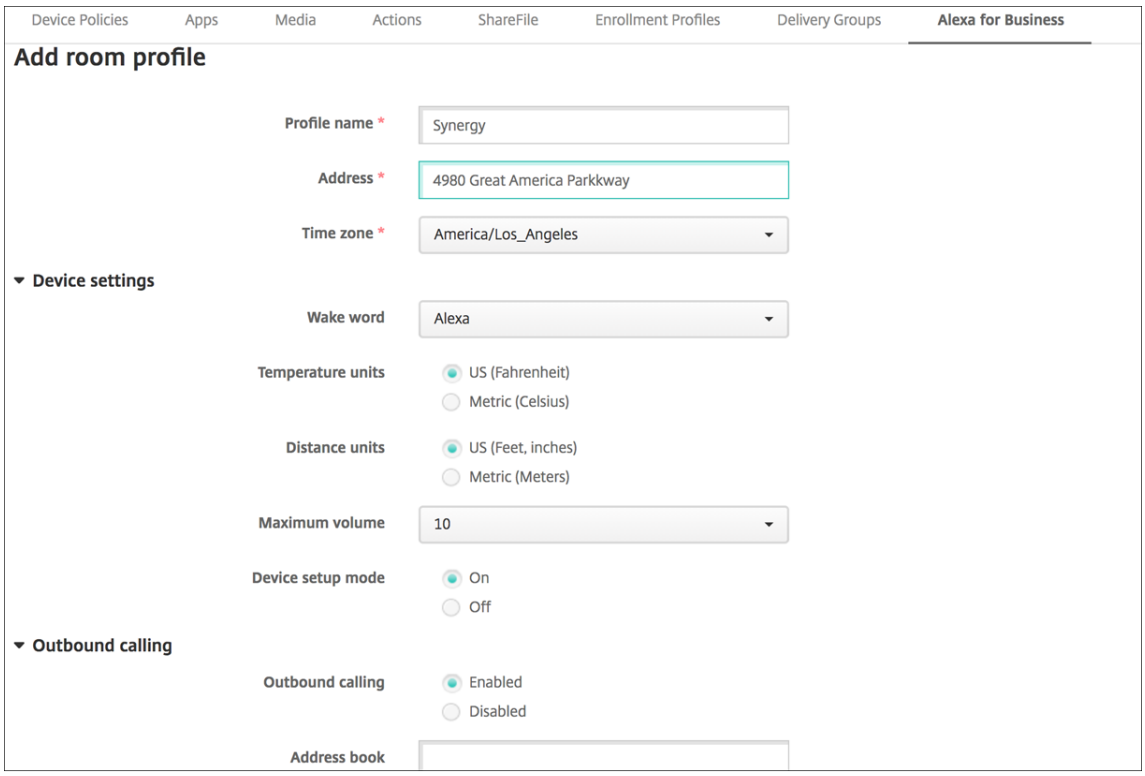
Raumprofile konfigurieren

Ein Raumprofil ist eine Konfiguration zur Anwendung auf Räume, in denen sich Alexa-Geräte befinden. Sie können Raumprofile hinzufügen, bearbeiten und löschen.

1. Wählen Sie in der Citrix Endpoint Management-Konsole **Konfigurieren > Alexa for Business > Raumprofile**. Eine Liste der verfügbaren Raumprofile wird angezeigt.



2. Zum Hinzufügen eines Raumprofils klicken Sie auf **Hinzufügen**. Um ein Raumprofil zu bearbeiten, wählen es aus und klicken Sie auf **Bearbeiten**.
3. Geben Sie die Raumprofileinstellungen ein:



- **Profilname:** Geben Sie einen Profilnamen ein.
- **Adresse:** Geben Sie die Adresse des Gebäudes ein, in dem sich die Räume mit den Alexa-Geräten befinden.
- **Zeitzone:** Wählen Sie die Zeitzone des Orts.
- **Aktivierungswort:** Wählen Sie das Aktivierungswort zum Ansprechen der Alexa-Geräte.
- **Temperatureinheiten:** Wählen Sie die Einheiten aus, in denen Alexa-Geräte die Temperatur angeben.
- **Längeneinheiten:** Wählen Sie die Einheiten aus, in denen Alexa-Geräte die Länge angeben.
- **Maximale Lautstärke:** Wählen Sie die maximale Lautstärke für Alexa.
- **Gerätesetupmodus:** Legen Sie fest, ob Alexa-Geräte durch Erzwingen des Gerätesetupmodus neu konfiguriert werden können.
- **Ausgehende Anrufe**: Aktivieren oder deaktivieren Sie die Anruffunktion von Alexa-Geräten.
- **Adressbuch:** Richten Sie die Adressbuchkonfiguration für Alexa-Geräte ein.

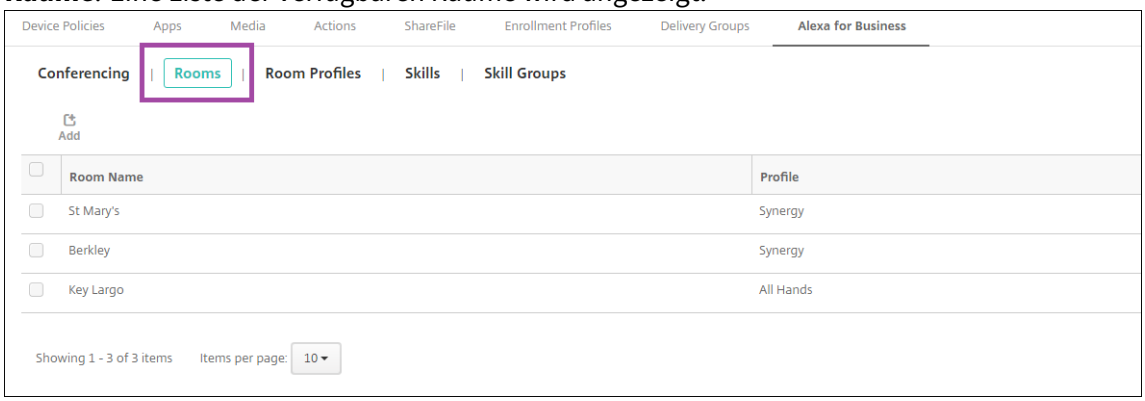
4. Klicken Sie auf **Speichern**.

Räume konfigurieren

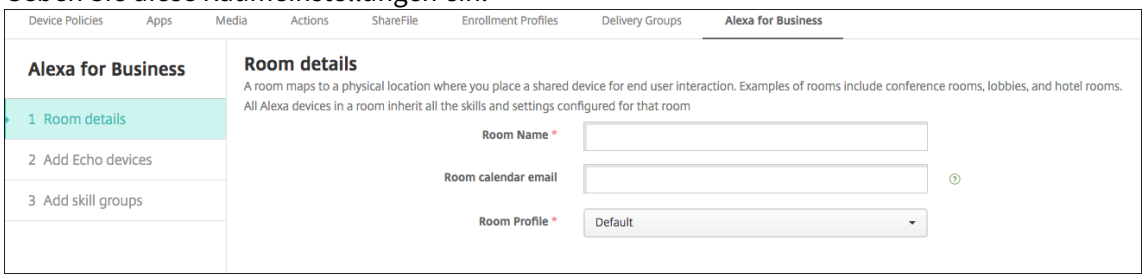
In der Citrix Endpoint Management-Konsole konfigurierte Räume repräsentieren die physischen Räume eines Gebäudes (Besprechungsräume usw.). Beim Konfigurieren eines Raums weisen

Sie diesem ein Alexa-Gerät zu und fügen dem Gerät eine Skillgruppe hinzu. Sie können Räume hinzufügen, bearbeiten und löschen.

1. Wählen Sie in der Citrix Endpoint Management-Konsole **Konfigurieren > Alexa for Business > Räume**. Eine Liste der verfügbaren Räume wird angezeigt.

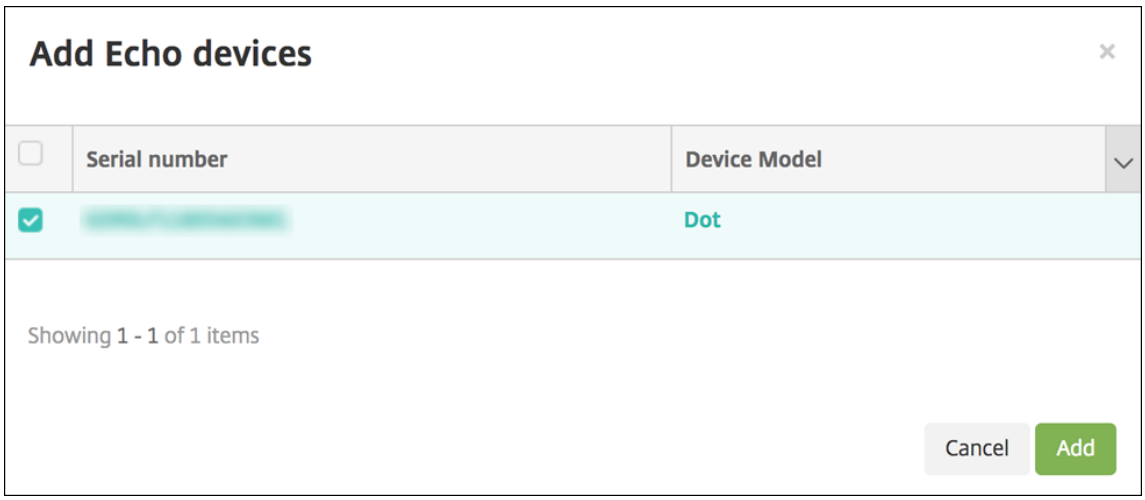


2. Zum Hinzufügen eines Raums klicken Sie auf **Hinzufügen**. Um einen Raum zu bearbeiten, wählen ihn aus und klicken Sie auf **Bearbeiten**.
3. Geben Sie diese Raumeinstellungen ein:

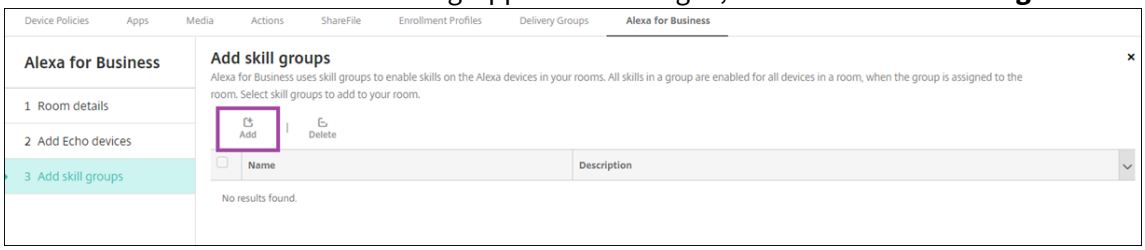


   - **Raumname:** Geben Sie den Namen des Konferenzraums, des Besprechungszimmers oder eines anderen Raums ein.
   - **Raumkalender-E-Mail-Adresse:** Geben Sie die E-Mail-Adresse des Raumkalenders ein.
   - **Raumprofil:** Wählen Sie den Namen der Raumprofilkonfiguration für den Raum.

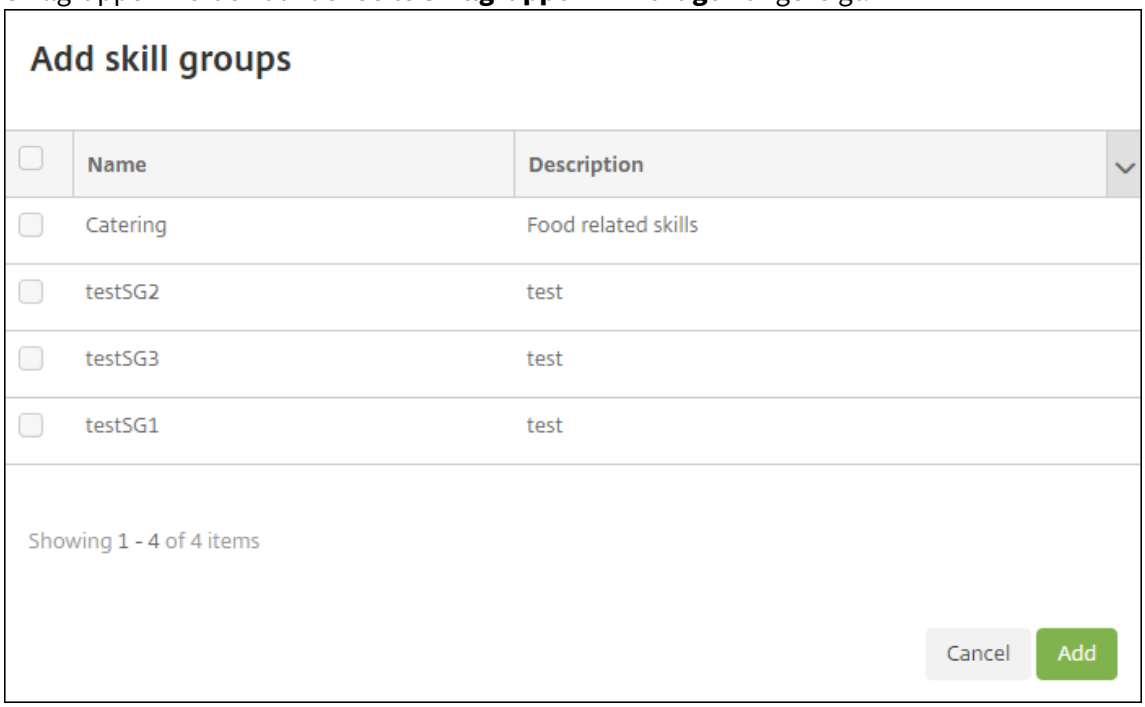
4. Klicken Sie auf **Weiter**.
5. Um ein Alexa-Gerät mit dem Raum zu verknüpfen, klicken Sie auf **Hinzufügen**.
6. Wählen Sie ein Gerät aus und klicken Sie auf **Hinzufügen**. Das ausgewählte Gerät wird auf der Seite **Echo-Geräte hinzufügen** angezeigt.



7. Klicken Sie auf **Weiter**.
8. Um den Alexa-Geräten im Raum Skillgruppen hinzuzufügen, klicken Sie auf **Hinzufügen**.



9. Wählen Sie die gewünschten Skillgruppen aus. Klicken Sie auf **Hinzufügen**. Die ausgewählten Skillgruppen werden auf der Seite **Skillgruppen hinzufügen** angezeigt.

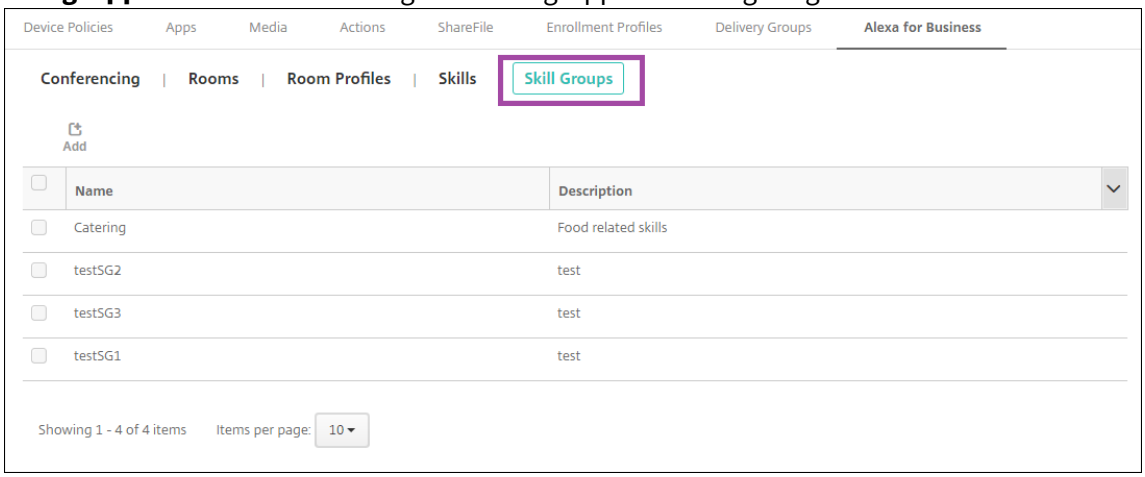


10. Klicken Sie auf **Speichern**.

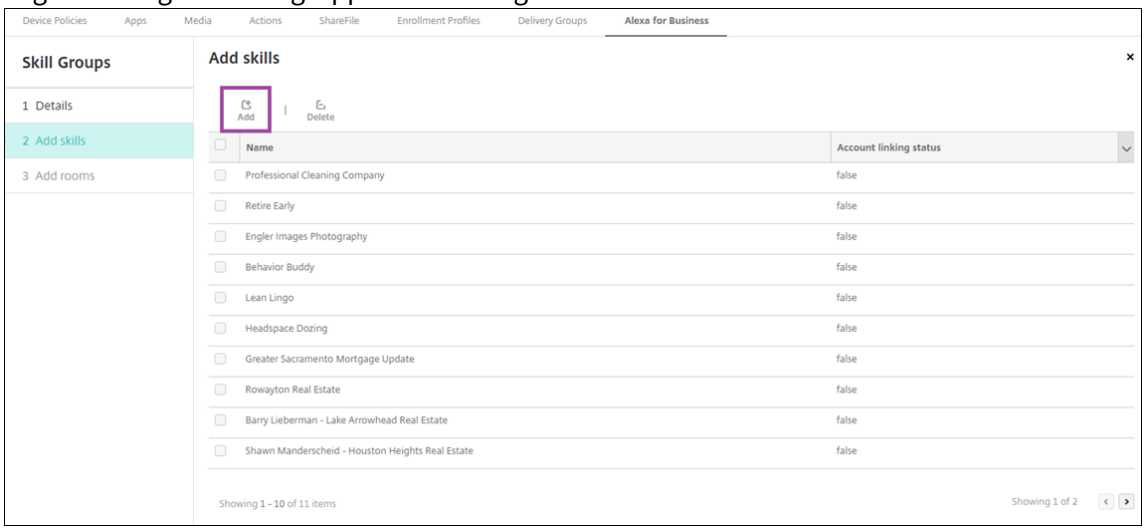
Skillgruppen konfigurieren

Skillgruppen sind Sammlungen von Skills, die auf einen Raum angewendet werden können. Sie können eine Skillgruppe erstellen und sie dann einem Raum zuweisen. Durch Skills können Sie ein Alexa-Gerät beispielsweise zum Beginnen von Online-Meetings oder zur Durchsicht einer Tagesordnung verwenden. Sie können Skillgruppen hinzufügen, bearbeiten und löschen.

1. Wählen Sie in der Citrix Endpoint Management-Konsole **Konfigurieren > Alexa for Business > Skillgruppe**. Eine Liste der verfügbaren Skillgruppen wird angezeigt.

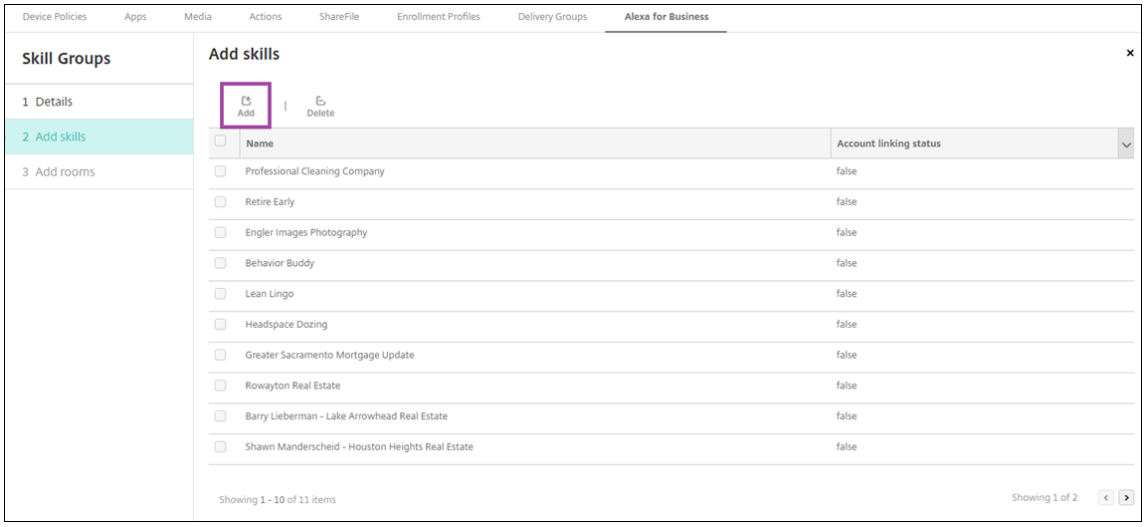


2. Um eine Skillgruppe hinzuzufügen, klicken Sie auf **Hinzufügen**. Zum Bearbeiten einer Skillgruppe wählen Sie diese aus und klicken Sie auf **Bearbeiten**.
3. Legen Sie folgende Skillgruppeneinstellungen fest:

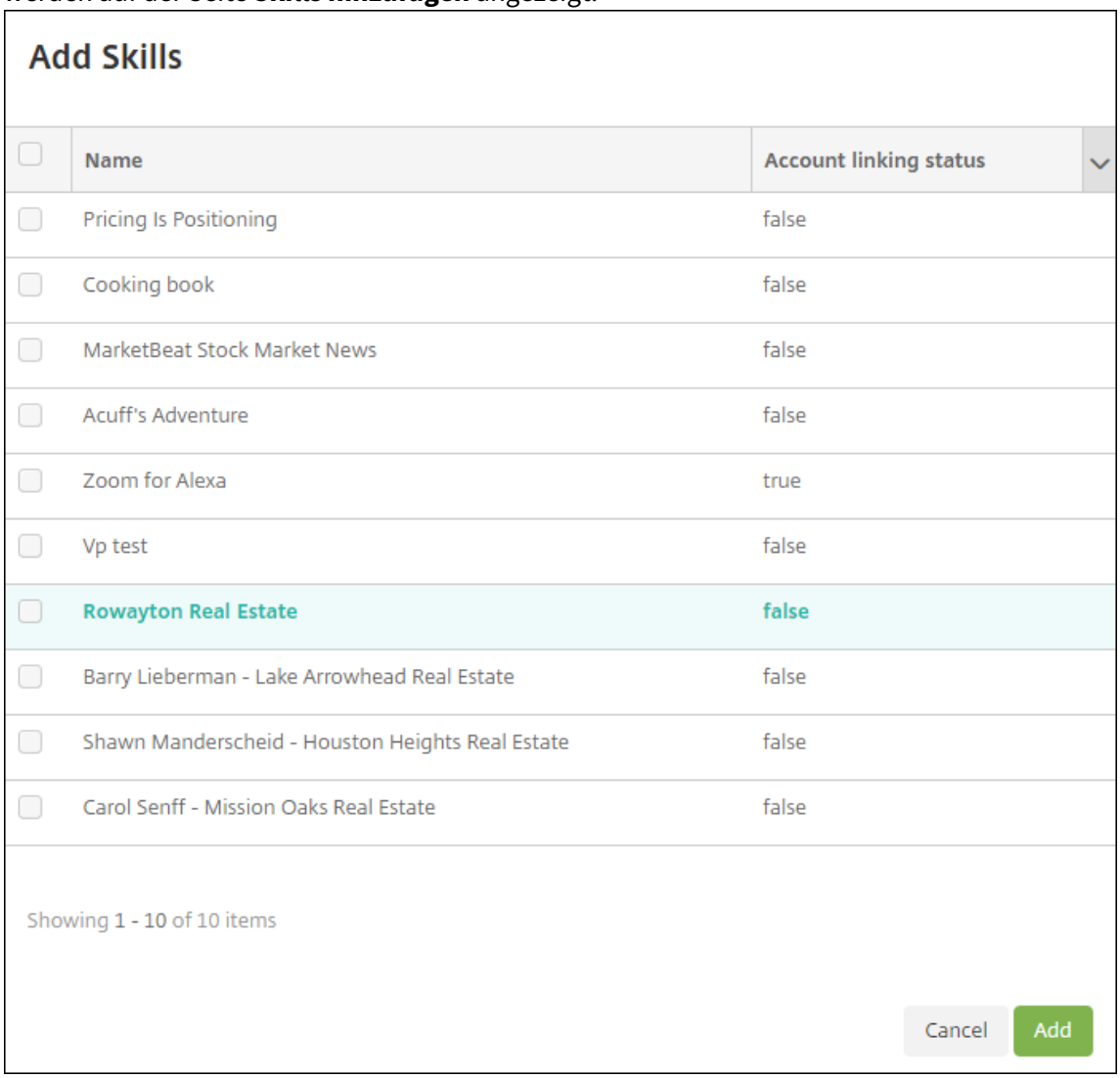


   - **Name:** Geben Sie den Namen der Skillgruppe ein.
   - **Beschreibung:** Geben Sie eine kurze Beschreibung der Skillgruppe ein.

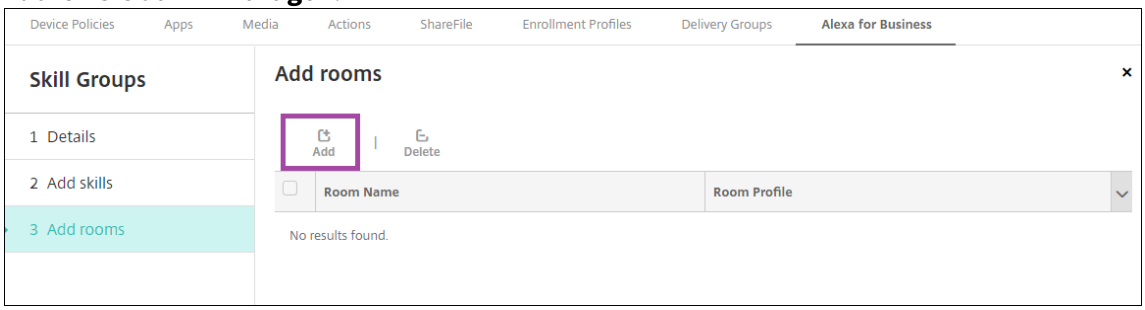
4. Klicken Sie auf **Weiter**.
5. Klicken Sie zum Hinzufügen von Skills zu der Skillgruppe auf **Hinzufügen**.



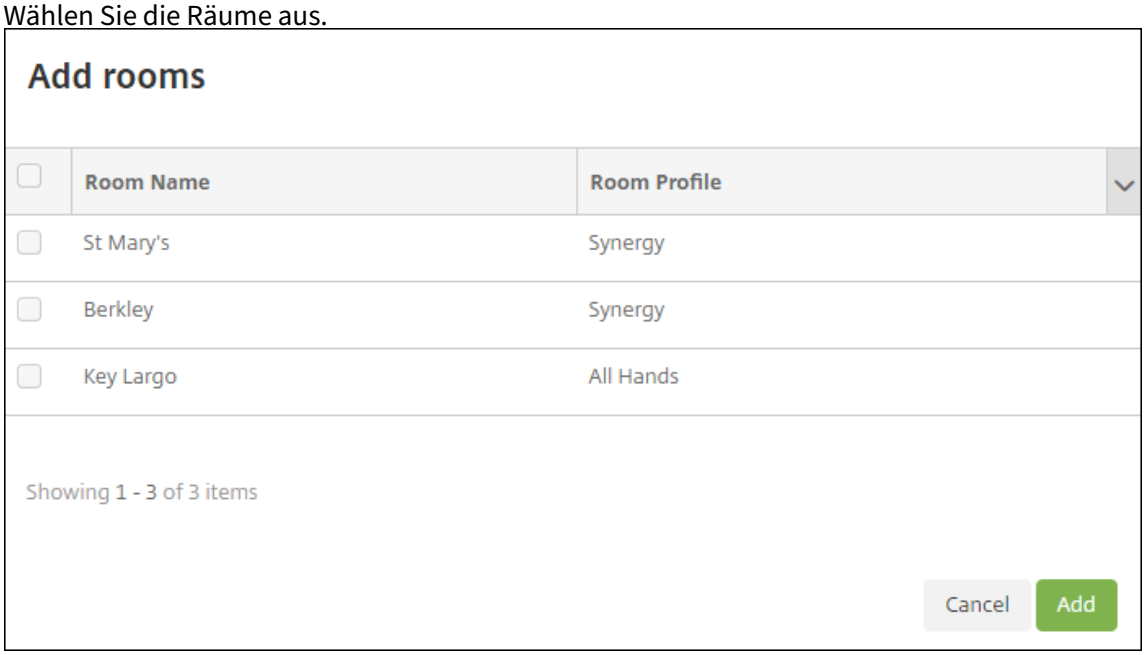
6. Wählen Sie die gewünschten Skills und klicken Sie auf **Hinzufügen**. Die ausgewählten Skills werden auf der Seite **Skills hinzufügen** angezeigt.



7. Um die Skillgruppe den Alexa-Geräten in den von Ihnen angegebenen Räumen hinzuzufügen, klicken Sie auf **Hinzufügen**.



8. Wählen Sie die Räume aus.



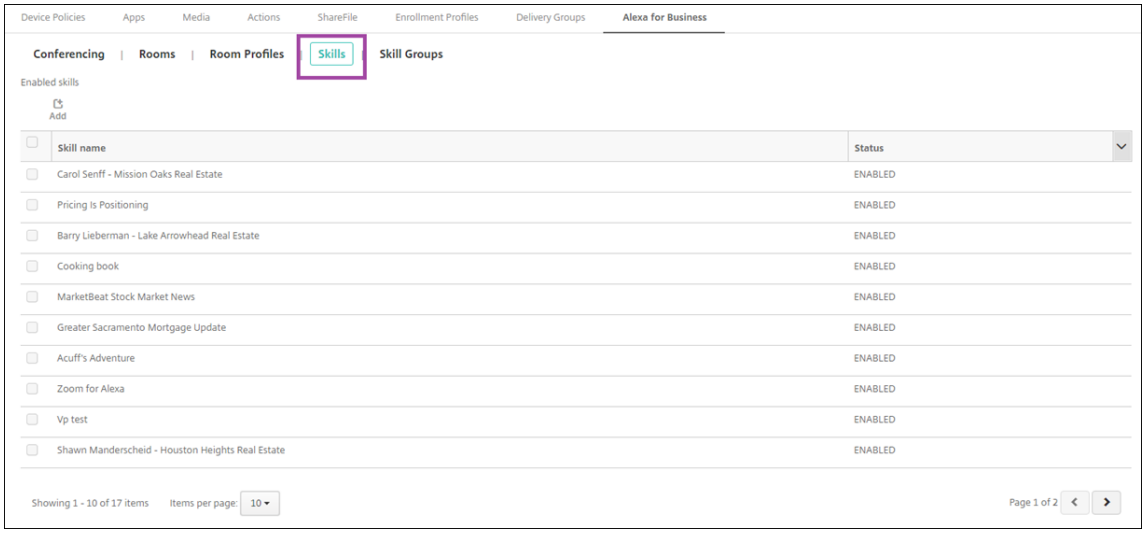
9. Klicken Sie auf **Speichern**.

Skills für Skillgruppen bereitstellen

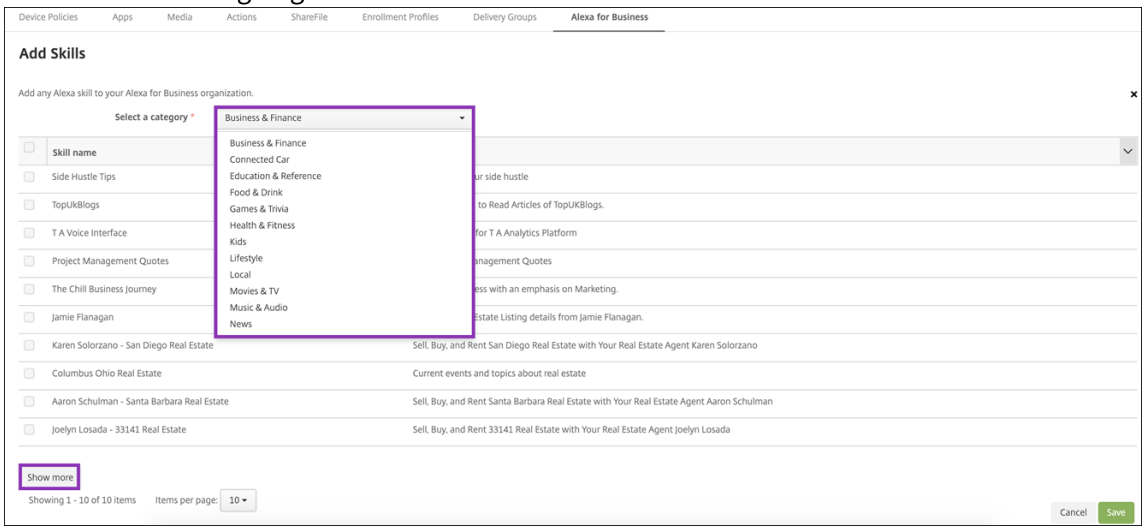
Sie konfigurieren die Liste der verfügbaren Alexa-Skills, die Skillgruppen hinzugefügt werden können, in Ihrer Alexa for Business-Organisation. Es handelt sich um Skills aus dem öffentlichen Alexa-Skills-Shop oder private Skills, die für Ihre Organisation veröffentlicht wurden.

Skills zu Ihrer Organisation hinzufügen

1. Wählen Sie in der Citrix Endpoint Management-Konsole **Konfigurieren > Alexa for Business > Skills**. Die Liste der aktivierten Skills wird angezeigt.



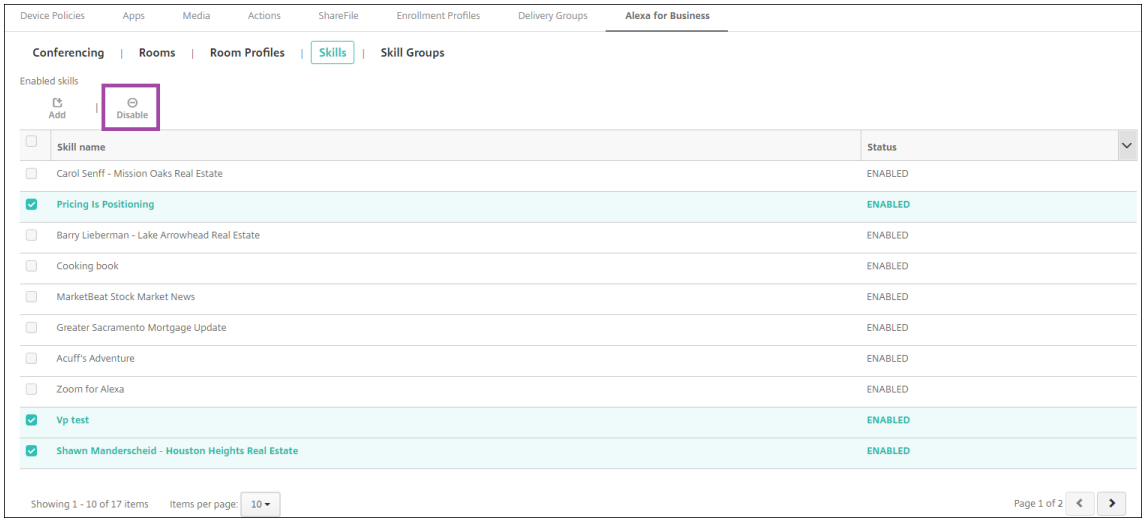
2. Um Skills hinzuzufügen, klicken Sie auf **Hinzufügen**.
3. Um weitere Alexa-Skills anzuzeigen, wählen Sie eine Kategorie aus und klicken Sie auf **Mehr anzeigen**. Mit **Mehr anzeigen** wird die Liste der Skills, die Sie Ihrer Organisation hinzufügen können, um bis zu zehn weitere Skills erweitert. Durch Klicken auf **Mehr anzeigen** werden weitere Skills hinzugefügt.



4. Wählen Sie die Skills aus, die Sie Ihrer Organisation hinzufügen möchten.
5. Klicken Sie auf **Speichern**.

Skills aus der Organisation entfernen

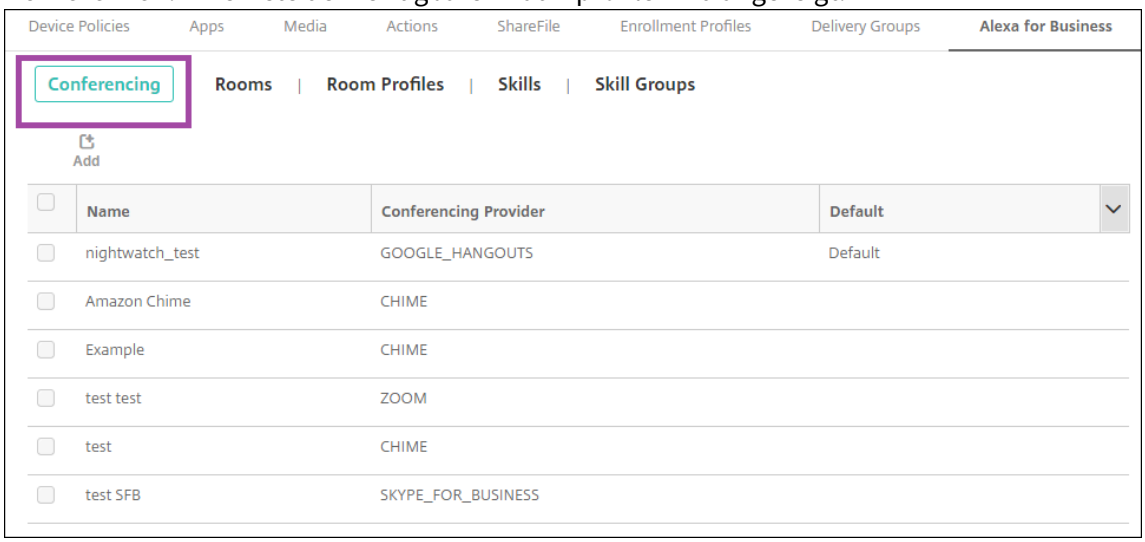
1. Wählen Sie in der Citrix Endpoint Management-Konsole **Konfigurieren > Alexa for Business > Skills**. Die Liste der aktivierten Skills wird angezeigt.
2. Wählen Sie die Skills aus, die Sie aus Ihrer Organisation entfernen möchten.
3. Klicken Sie auf **Deaktivieren**.



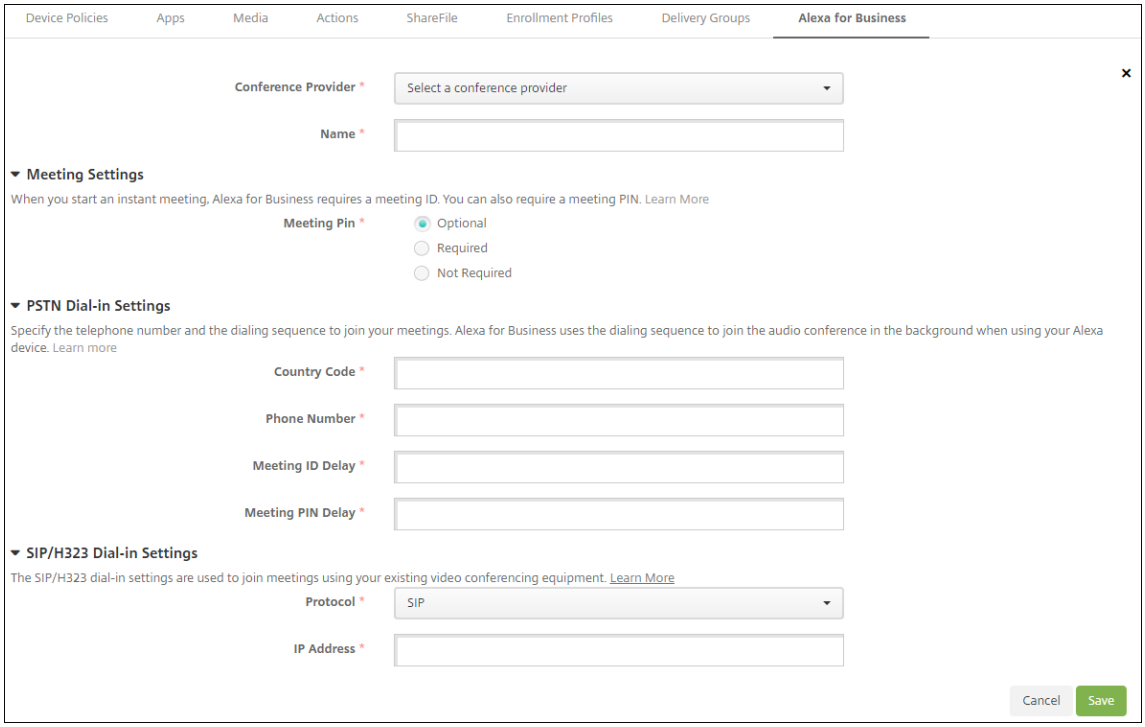
Konferenzen konfigurieren

Mit Konferenzfeatures können Sie Konferenzanbieter wie Google Hangouts oder Amazon Chime konfigurieren, die steuern, wie Benutzer Konferenzen in Räumen mit Alexa-Geräten beitreten. Sie können Konferenzanbieter hinzufügen, bearbeiten und löschen. Sie können auch einen Standard-Konferenzanbieter festlegen.

1. Wählen Sie in der Citrix Endpoint Management-Konsole **Konfigurieren > Alexa for Business > Konferenzen**. Eine Liste der verfügbaren Raumprofile wird angezeigt.



2. Um einen Konferenzanbieter hinzuzufügen, klicken Sie auf **Hinzufügen**. Um einen Konferenzanbieter zu bearbeiten, wählen das entsprechende Raumprofil aus und klicken Sie auf **Bearbeiten**.
3. Geben Sie die Raumprofileinstellungen ein:



- **Konferenzanbieter:** Wählen Sie einen Konferenzanbieter aus der Liste aus.
- **Name:** Geben Sie einen Namen für den Konferenzanbieter ein.
- **Besprechungs-PIN:** Geben Sie an, ob eine PIN für die Teilnahme an Besprechungen erforderlich sein soll.
- **PSTN-Einwahleinstellungen**
  - **Ländercode:** Geben Sie den Ländercode ein.
  - **Telefonnummer:** Geben Sie die Telefonnummer ein.
  - **Besprechungs-ID-Verzögerung:** Geben Sie die Zeit in Sekunden ein, bis die Besprechungs-ID gesendet wird.
  - **Besprechungs-PIN-Verzögerung:** Geben Sie die Zeit in Sekunden ein, bis die PIN gesendet wird.
- **SIP/H323-Einwahleinstellungen:** Diese Einstellungen werden verwendet, um an Besprechungen unter Verwendung vorhandener Videokonferenzgeräte teilzunehmen.
  - **Protokoll:** Wählen Sie ein Protokoll aus.
  - **IP-Adresse:** Geben Sie die IP-Adresse ein.

4. Klicken Sie auf **Speichern**.

Wenn Sie mehrere Konferenzanbieter konfigurieren, legen Sie den Standardanbieter fest.

1. Wählen Sie in der Citrix Endpoint Management-Konsole **Konfigurieren > Alexa for Business > Konferenzen**. Eine Liste der verfügbaren Raumprofile wird angezeigt.
2. Wählen Sie den Konferenzanbieter aus, den Sie als Standard festlegen möchten.
3. Klicken Sie auf **Als Standard festlegen**.

Geräteverwaltung zu Android Enterprise migrieren

June 25, 2024

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.

Citrix Endpoint Management 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.

Wir empfehlen Ihnen auch den Citrix Tech Zone-Artikel Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management, der weitere Informationen bietet.

Auswirkungen der nicht mehr unterstützten Geräteverwaltung

Die Device Administration-APIs sind veraltet und werden ab 2. November 2020 von Google nicht mehr unterstützt. Nach unserem Upgrade von Citrix Secure Hub auf die Android API-Stufe 29 werden diese APIs auf Geräten mit Android 10+ nicht mehr funktionieren.

- **Kamera deaktivieren:** Steuert den Zugriff auf Gerätekameras.
- **Keyguard-Funktionen**: Steuert Funktionen für die Gerätesperre, darunter Biometrie und Muster.
- **Kennwortablauf:** Zwingt Benutzer, ihr Kennwort nach einem konfigurierbaren Zeitraum zu ändern.
- **Kennwort beschränken:** Legt restriktive Kennwortanforderungen fest.

Anforderungen und Empfehlungen

- Wenn Sie ein Gerät auf Android 10+ aktualisieren können, müssen Sie dieses Gerät in Android Enterprise registrieren.
  - Sie müssen Android 11-Geräte bei Android Enterprise registrieren.

  - Ab September 2020 gilt für Android 10-Geräte: Citrix unterstützt nicht Neuregistrierungen oder Wiederregistrierungen von Geräten in den Geräteverwaltungsmodus. Bereits registrierte Geräte funktionieren weiter bis zum 2. November 2020, wie im vorangegangenen Abschnitt erwähnt.

- Für Geräte mit Android 9 oder niedriger unterstützen wir weiterhin den Modus "Legacygeräteverwaltung". Wir empfehlen jedoch einen zeitnahen Wechsel dieser Geräte zu Android Enterprise.
- Für neue oder vorhandene Geräte, die im Citrix Nur-MAM-Modus registriert sind, ist keine Aktion erforderlich. Die veralteten Google APIs haben keine Auswirkungen auf Geräte im Nur-MAM-Modus. Angesichts der Umstellung auf die Plattformverschlüsselung empfehlen wir jedoch dringend, vom Nur-MAM-Modus in den Arbeitsprofilmodus (BYOD) in Android Enterprise zu wechseln. Der Arbeitsprofilmodus bietet MAM-Funktionalität, aber in einem Container auf dem Gerät.

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 Citrix Endpoint Management: 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 Citrix Endpoint Management-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
  - OS-Version
- 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 Workspace-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 Apps hinzufügen.

- 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 Citrix Endpoint Management.
- Option 2: Veröffentlichen Sie die App aus Citrix Endpoint Management als Unternehmensapp. Veröffentlichen Sie die APK in Citrix Endpoint Management und wählen Sie die Plattform **Android Enterprise** für die MDX-Datei.

Migration der Citrix Geräterichtlinien

Wenn Richtlinien für die Plattformen **Android (Legacy-Geräteadmin)** und **Android Enterprise** verfügbar sind, bearbeiten Sie die Richtlinie und wählen als Plattform **Android Enterprise** aus.

- Berücksichtigen Sie bei Android Enterprise die Geräteregistrierungsmethode. Einige Richtlinienoptionen sind nur für Geräte im Arbeitsprofilmodus oder im vollständig verwalteten Modus verfügbar. Siehe Konfigurieren von App- und Geräterichtlinien für Android Enterprise.
- Wenn Sie die Exchange-Geräterichtlinie für Legacy-Geräteadmin-Geräte verwenden, erstellen Sie stattdessen eine Geräterichtlinie für verwaltete Konfigurationen, um E-Mail-Einstellungen zu konfigurieren.
- Fügen Sie der Richtlinie eine Bereitstellungsregel hinzu, um sicherzustellen, dass eine Richtlinie auf die beabsichtigten Geräte angewendet wird (Android Enterprise bzw. Legacy-Geräteadmin). Verwenden Sie beispielsweise für die Plattform “Legacy-Geräteadmin”diese Bereitstellungsregel:

```
Limit by known device property name Android Enterprise
Enabled Device? Isn't equal to true
<!--NeedCopy-->
```

Diese Bereitstellungsregel prüft, ob das Gerät NICHT für Android Enterprise aktiviert ist, und stellt die Richtlinie zusammen mit den Apps auf Geräten bereit, die für Legacy-Geräteadmin aktiviert sind.

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 Citrix Endpoint Management.

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

June 25, 2024

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 unternehmenseigene und private Android-Arbeitsgeräte (BYOD) mit Citrix Endpoint Management.

- 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 von Google über Android Enterprise-Funktionen finden Sie unter Android Enterprise Management.

Ressourcen:

- Eine Liste mit Begriffen und Definitionen für Android Enterprise finden Sie im Google Android Enterprise-Entwicklerhandbuch unter Android Enterprise terminology. Diese Liste wird von Google häufig aktualisiert.
- Eine Liste der Android-Betriebssysteme mit Unterstützung für Citrix Endpoint Management 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.
- Informationen zum Bereitstellen von Android Enterprise finden Sie unter Ressourcen bereitstellen.

Erste Schritte mit Android Enterprise

> **Wichtig:**
>
> Der Geräteverwaltungsmodus wird nicht mehr unterstützt. Wenn Benutzer Geräte im Geräteverwaltungsmodus verwenden, lesen Sie Migration von der Geräteverwaltung zu Android Enterprise. Nach der Migration Ihrer Geräte auf Android Enterprise richten Sie Android Enterprise-Geräte wie folgt ein.

Einmalige Einrichtung

1. Erstellen Sie ein verwaltetes Google Play-Konto.

   Siehe Verwaltetes Google Play mit Citrix Endpoint Management verwenden und Anforderungen.
2. Binden Sie Ihr Google Play-Konto in Citrix Endpoint Management ein.

   Siehe Verbinden von Citrix Endpoint Management mit Google Play.
3. Planen Sie, wie Sie die Geräte verwalten möchten.

   Siehe Szenarien und Profile für die Gerätebereitstellung.
4. Planen Sie die Registrierungssicherheit für Benutzergeräte.

   Siehe Registrierungssicherheit.

5. Bereiten Sie die Bereitstellung von MDX-fähigen Apps vor.

   Verwenden Sie das MAM-SDK, um Apps zu entwickeln. Wenn Sie noch nicht zum Wechsel auf das neue SDK bereit sind, können Sie die Apps auch mit dem befehlszeilenbasierten MDX Toolkit umschließen.

   Siehe Überblick über das MAM-SDK.

Sie sind jetzt bereit, Ihre Android Enterprise-Geräte mit App- und Geräterichtlinien, Registrierungsprofilen und Apps zu konfigurieren. Im folgenden Abschnitt finden Sie die zugehörigen Anleitungen dafür.

Geräte konfigurieren

1. Erstellen Sie Bereitstellungsgruppen.

   Legen Sie fest, welcher Benutzer zu welchem Zeitpunkt Zugriff auf welche Ressourcen erhält. Siehe Ressourcen bereitstellen.

   Für die Plattform "Legacy-Geräteadmin"veröffentlichte Apps werden von Citrix nicht länger auf Geräten bereitgestellt, die in Android Enterprise registriert sind. 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. Siehe Auslaufende Features.

2. Fügen Sie Apps hinzu. Sie können die Apps in Google Play direkt über die Citrix Endpoint Management-Konsole genehmigen.

   Weitere Informationen finden Sie im Google-Supportartikel Manage apps in your organization.

3. Erstellen Sie Registrierungsprofile.

   Legen Sie Registrierungsoptionen für die Geräte- und App-Verwaltung fest. Siehe Szenarien und Profile für die Gerätebereitstellung und Erstellen von Registrierungsprofilen.

   - Wenn Sie einem Android-Gerätebenutzer eine Android Enterprise-App aus dem öffentlichen App-Store bereitstellen, wird dieser Benutzer automatisch bei Android Enterprise registriert.
   - Mit der Zero-Touch-Registrierung können Sie festlegen, dass Geräte beim ersten Einschalten automatisch registriert werden. Siehe Zero-Touch-Registrierung.

4. Konfigurieren Sie App- und Geräterichtlinien.

   Berücksichtigen Sie hierbei sowohl die Unternehmenssicherheit als auch Datenschutz und Benutzererfahrung. Siehe Konfigurieren von App- und Geräterichtlinien für Android Enterprise.

5. Verteilen Sie Apps.

   Sie verwenden verwaltetes Google Play zum Hinzufügen, Erwerben und Genehmigen von Apps für die Bereitstellung in dem Android Enterprise-Workspace von Geräten. Nutzer können nur Apps aus verwaltetem Google Play installieren, die Sie ihnen zur Verfügung stellen.

   Siehe:

   - Android Enterprise-Apps verteilen
   - Richtlinie für verwaltete Konfigurationen
   - Richtlinie für App-Berechtigungen

6. Konfigurieren Sie Sicherheitsaktionen, um die Richtlinientreue zu gewährleisten und zu überwachen.

   Weitere Informationen finden Sie unter Sicherheitsaktionen.

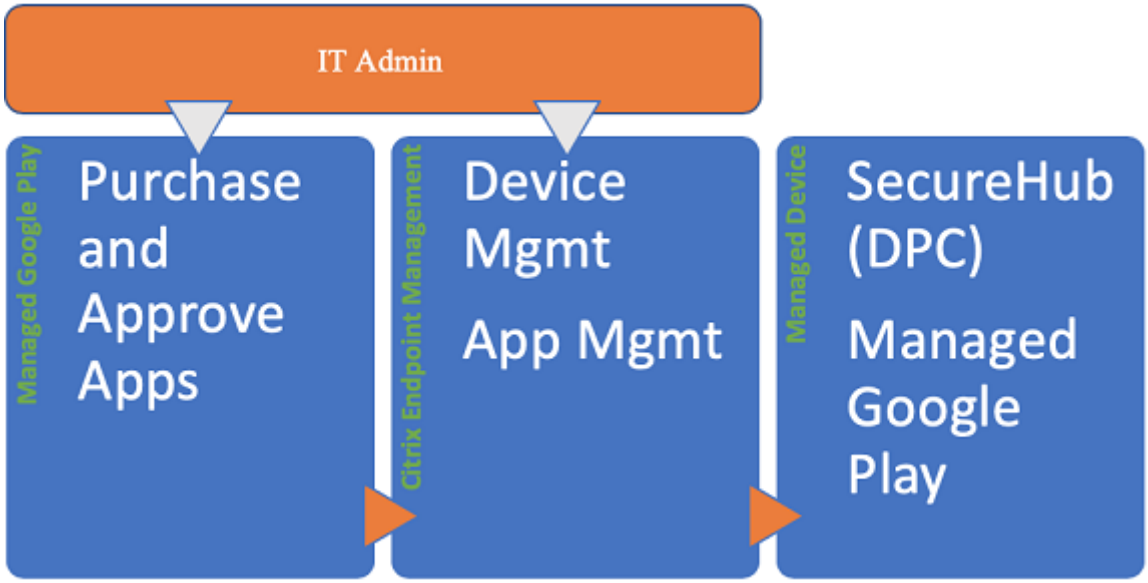
Verwaltetes Google Play mit Citrix Endpoint Management verwenden

Wenn Sie Citrix Endpoint Management 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 Citrix Endpoint Management mit Android Enterprise integrieren, besteht die Komplettlösung aus folgenden Komponenten:

- **Citrix Endpoint Management:** EMM-Lösung von Citrix. Citrix Endpoint Management ist die einheitliche Endpunktverwaltung für einen sicheren digitalen Workspace. Citrix Endpoint Management bietet IT-Administratoren die Möglichkeit, Geräte und Apps für ihre Organisationen zu verwalten.
- **Citrix Secure Hub:** DPC-App von Citrix. Citrix Secure Hub ist das Launchpad für Citrix Endpoint Management. Citrix Secure Hub ermöglicht das Durchsetzen von Richtlinien auf dem Gerät.
- **Verwaltetes Google Play:** Googles Plattform für Unternehmensapps, die mit Citrix Endpoint Management 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.



> **Hinweis:**
>
> Sie können Citrix über verwaltetes Google Play oder über Google Workspace (ehemals G Suite) 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.

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. Durch Einrichten mehrerer Unternehmen können Sie separate Gruppen von Geräten und Apps verwalten.

Für Citrix Endpoint Management-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 instal-

lieren, die Sie ihnen zur Verfügung stellen.

Szenarien und Profile für die Gerätebereitstellung

Gerätebereitstellungsszenarios legen 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. Arbeitsprofile und persönliche Profile werden auf Betriebssystemebene getrennt. Weitere Informationen zu Arbeitsprofilen finden Sie unter Was ist ein Arbeitsprofil?.

> **Wichtig:**
>
> Beim Update von Android Enterprise-Geräten auf Android 11 migriert Google alle Geräte mit der Einstellung "Vollständig verwaltet mit Arbeitsprofil"zu einem neuartigen Arbeitsprofil mit verbesserter Sicherheit. Der neue Registrierungsmodus heißt "Arbeitsprofil auf unternehmenseigenem Gerät". Weitere Informationen finden Sie unter Changes ahead for Android Enterprise's Fully Managed with Work Profile.
> Informationen zu Android 12-Geräten finden Sie unter Security and privacy enhancements for work profile.

Geräteverwaltung	Anwendungsfälle	Arbeitsprofil	Persönliches Profil	Hinweise
Unternehmenseigene Geräte (vollständig verwaltet)	Unternehmenseigene Geräte, die nur für den geschäftlichen Einsatz bestimmt sind	Nein	Nein	Nur für neue oder auf die Werkseinstellungen zurückgesetzte Geräte. Siehe Provisioning vollständig verwalteter Geräte mit Android Enterprise.

Geräteverwaltung	Anwendungsfälle	Arbeitsprofil	Persönliches Profil	Hinweise
Vollständig verwaltet mit Arbeitsprofil / Arbeitsprofil auf unternehmen-seigenem Gerät	Unternehmenseigene 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 Gerätebesitzer-modus und der zweite das Arbeitsprofil im Profilbesitzer-modus verwaltet. Sie können separate Richtlinien für Gerät und Arbeitsprofil festlegen.	Siehe Provisioning vollständig verwalteter Android Enterprise-Geräte mit Arbeitsprofil oder Arbeitsprofil auf unternehmen-seigenem Gerät.
Dedizierte Geräte*	Unternehmenseigene Geräte, die für einen einzigen Anwendungsfall konfiguriert sind, z. B. digitale Werbetechnik oder Ticketdruck	Nein	Nein	Siehe Provisioning von dedizierten Android Enterprise-Geräten.

BYOD-Arbeitsprofil**	Private Geräte, die bei der Arbeitsprofilverwaltung registriert sind (auch "Profilbesitzermodus")	Ja	Ja. Der DPC verwaltet nur das Arbeitsprofil, nicht das gesamte Gerät.	Diese Geräte müssen nicht neu oder auf die Werkseinstellungen zurückgesetzt sein. Siehe Provisioning von Arbeitsprofilgeräten mit Android Enterprise.

* 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 appbezogen.

** Zebra-Geräte können in Citrix Endpoint Management nicht als Geräte im BYOD-Arbeitsprofilmodus verwendet werden. Citrix Endpoint Management unterstützt Zebra-Geräte als vollständig verwaltete Geräte mit Android Enterprise.

Registrierungssicherheit

Registrierungsprofile bestimmen, ob Android-Geräte bei MAM, MDM oder MDM+MAM registriert werden, wobei im letzteren Modus die Benutzer ggf. MDM abwählen können.

Weitere Informationen zum Festlegen der Sicherheitsstufe und zum Registrierungsverfahren finden Sie unter Benutzerkonten, Rollen und Registrierung.

Citrix Endpoint Management unterstützt die folgenden Authentifizierungsverfahren für bei MDM oder MDM+MAM registrierte Android-Geräte. Weitere Informationen finden Sie in den folgenden Artikeln:

- Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken
- Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne
- Identitätsanbieter:
  - Authentifizierung mit Azure Active Directory über Citrix Cloud (Preview)
  - Authentifizierung mit Okta über Citrix Cloud (Preview)

Eine 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:

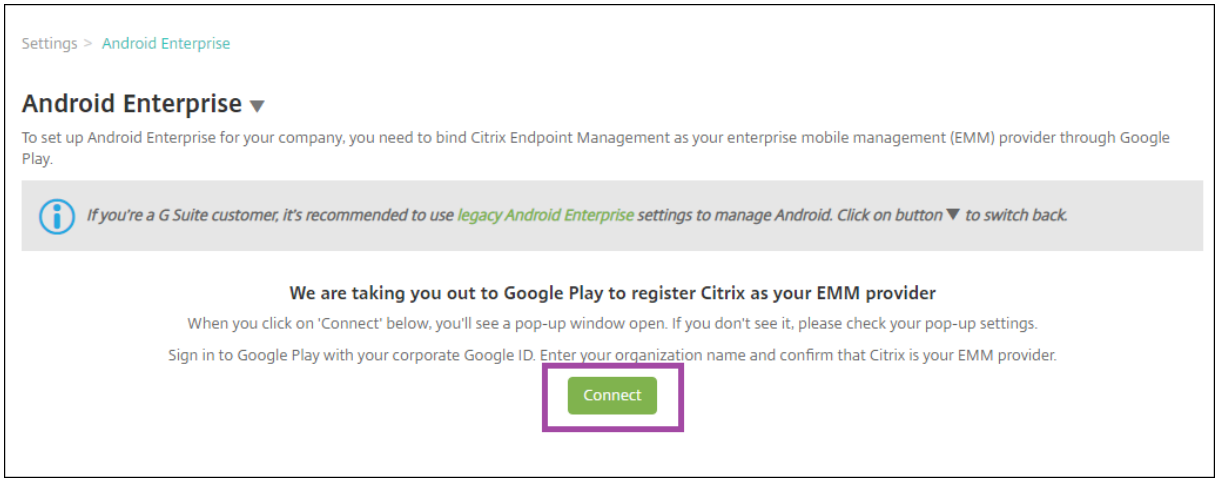
- Konten und Anmeldeinformationen:
  - Ein Google-Unternehmenskonto zum Einrichten von Android Enterprise mit verwaltetem Google Play
  - Ein Citrix-Kundenkonto zum Download der aktuellen MDX-Dateien
- Firebase Cloud Messaging (FCM) und eine Verbindungszeitplanrichtlinie für Geräte sind für Citrix Endpoint Management konfiguriert. Weitere Informationen finden Sie unter Firebase Cloud Messaging und Verbindungszeitplanrichtlinie für Geräte.

Verbinden von Citrix Endpoint Management mit Google Play

Um Android Enterprise für Ihre Organisation einzurichten, registrieren Sie Citrix über verwaltetes Google Play als EMM-Anbieter. Damit wird verwaltetes Google Play mit Citrix Endpoint Management verbunden und ein Unternehmen für Android Enterprise in Citrix Endpoint Management erstellt.

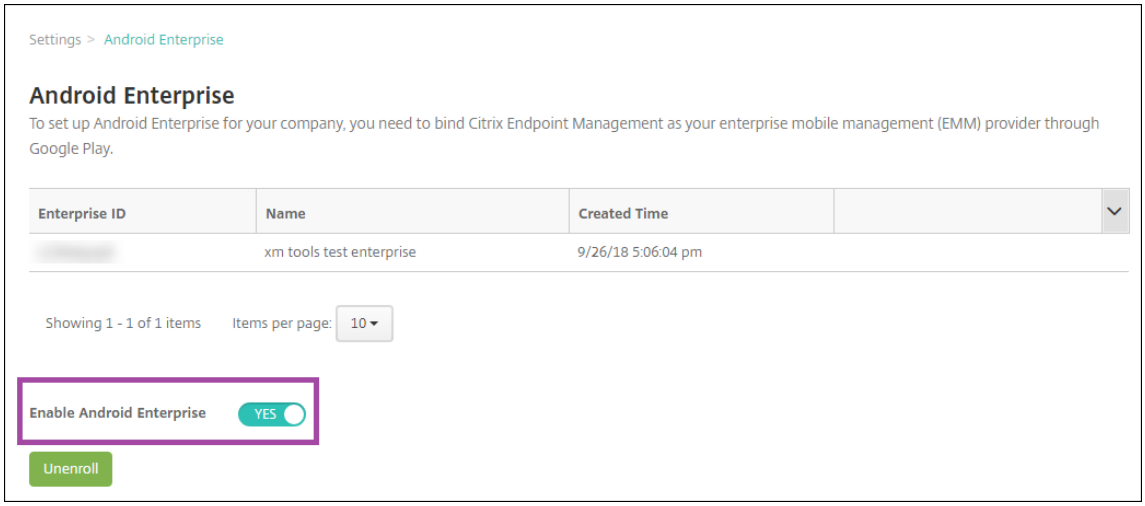
Sie benötigen ein Google-Unternehmenskonto, um sich bei Google Play anzumelden.

1. Wechseln Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Android Enterprise**.
2. Klicken Sie auf **Verbinden**. Google Play wird geöffnet.

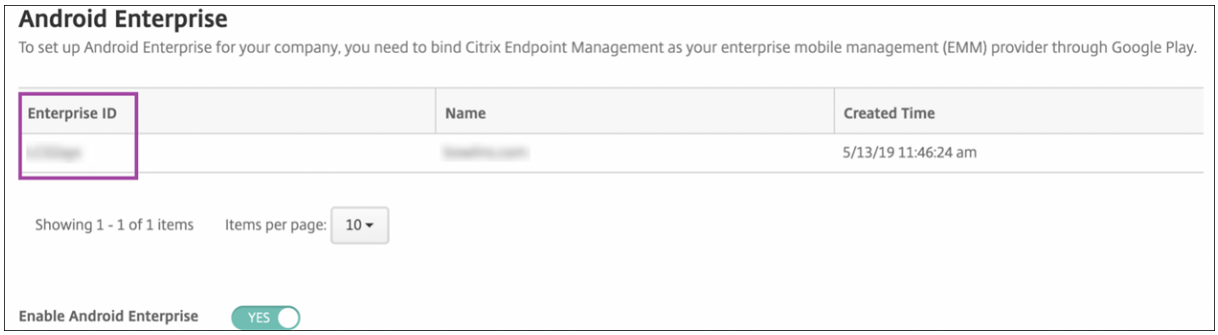


1. Melden Sie sich mit den Anmeldeinformationen für Ihr Google-Unternehmenskonto bei Google Play an. Geben Sie den Namen Ihrer Organisation ein und bestätigen Sie, dass Citrix Ihr EMM-Anbieter ist.

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 Citrix Endpoint Management-Konsole angezeigt.



Ihre Umgebung ist mit Google verbunden und kann die Geräte verwalten. Sie können nun Apps für Benutzer bereitstellen.

Citrix Endpoint Management 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 zum Bereitstellen dieser App-Typen für Benutzer finden Sie unter Verteilen von Android Enterprise-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.

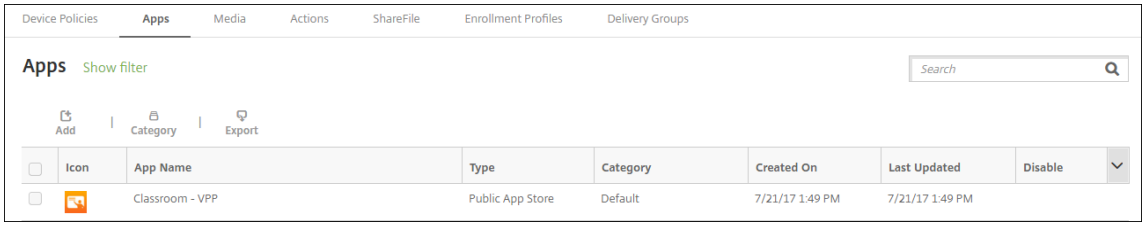
Die veröffentlichten Apps sind für Geräte verfügbar, die in Ihrem Android Enterprise-Unternehmen registriert sind.

> **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.

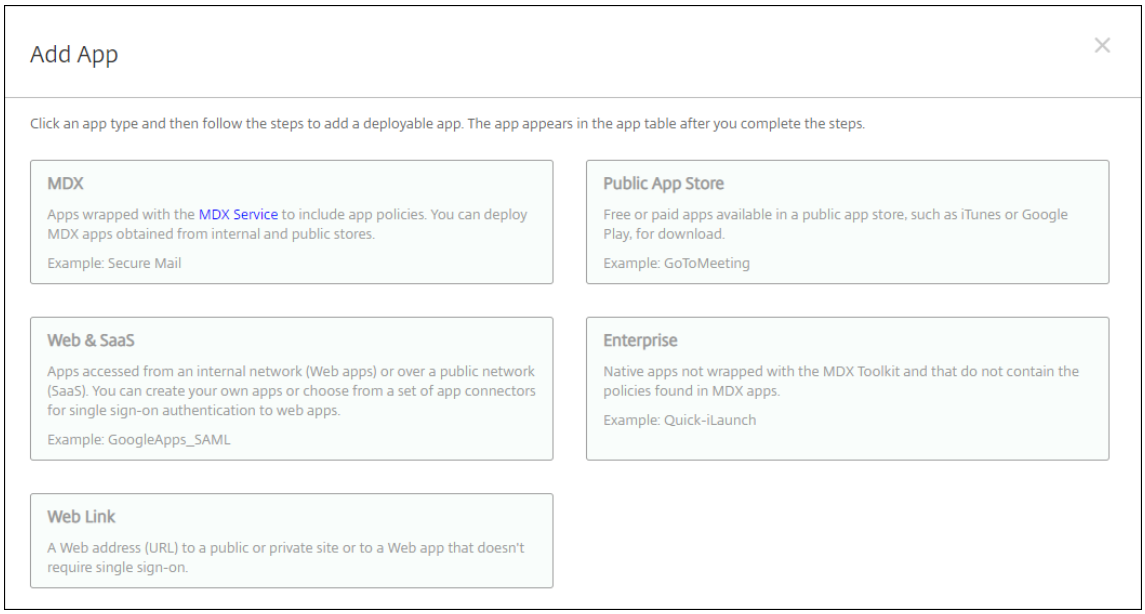
Konfigurieren von Apps als MDX-Apps

Gehen Sie zum Konfigurieren einer Citrix Produktivitätsapp als MDX-App für Android Enterprise folgendermaßen vor:

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps**. Die Seite **Apps** wird angezeigt.

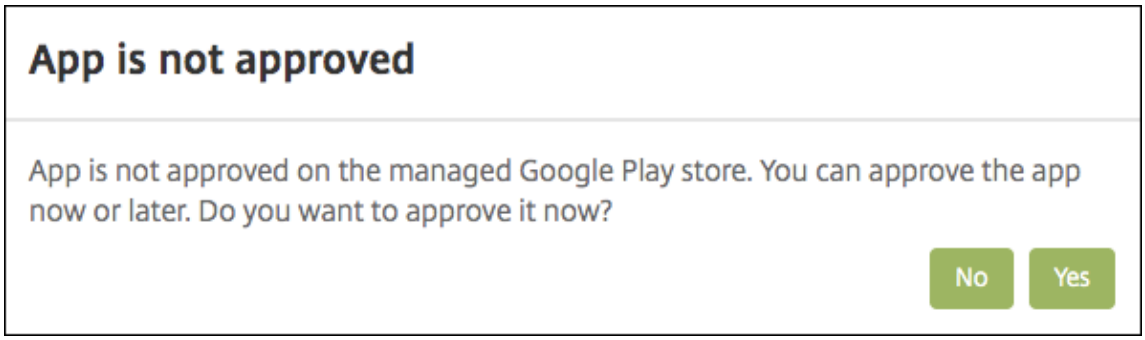


2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

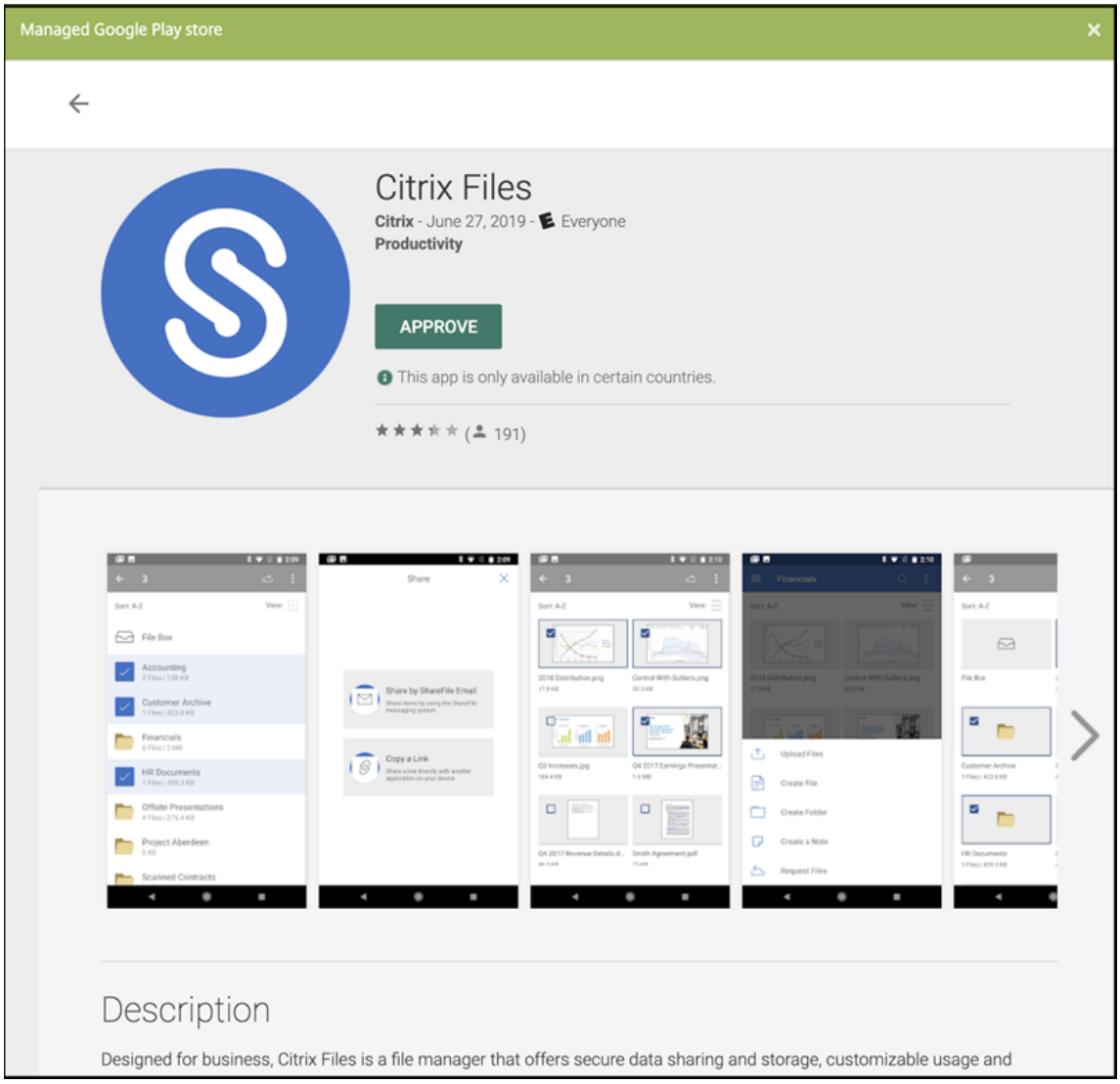


3. Klicken Sie auf **MDX**. Die Seite **App-Informationen** wird angezeigt.

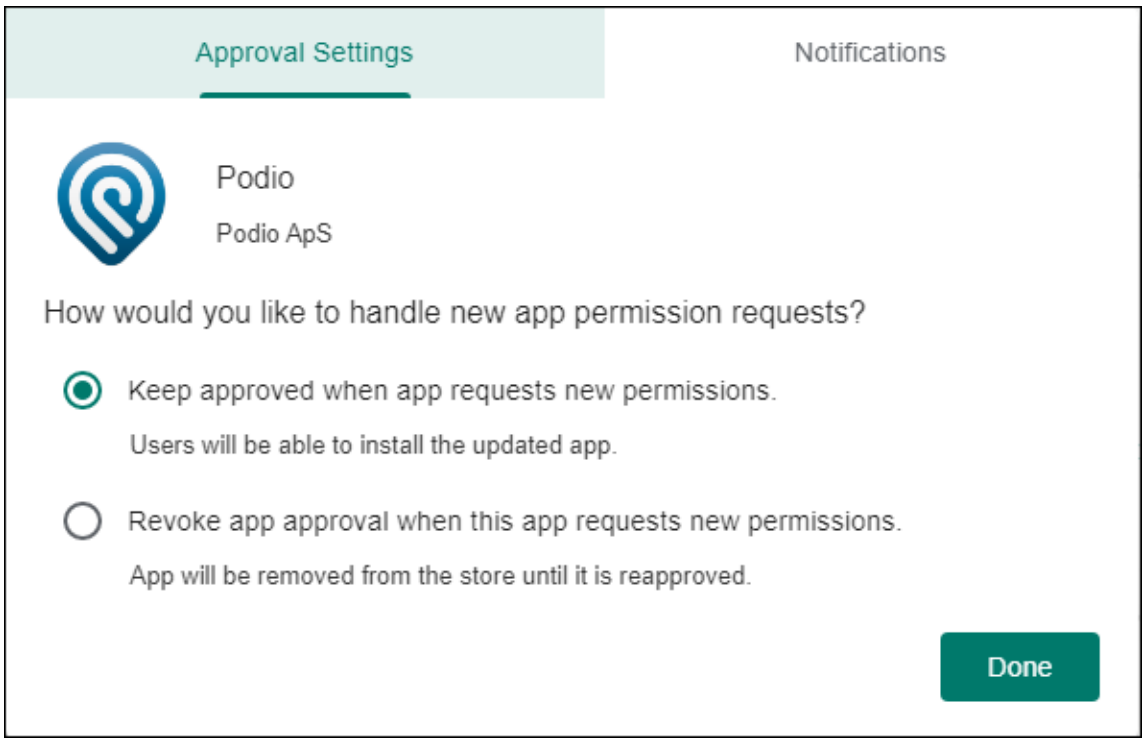
4. Wählen Sie links **Android Enterprise** als Plattform aus.
5. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
    - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** angezeigt.
    - **Beschreibung:** 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 Citrix Endpoint Management-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:

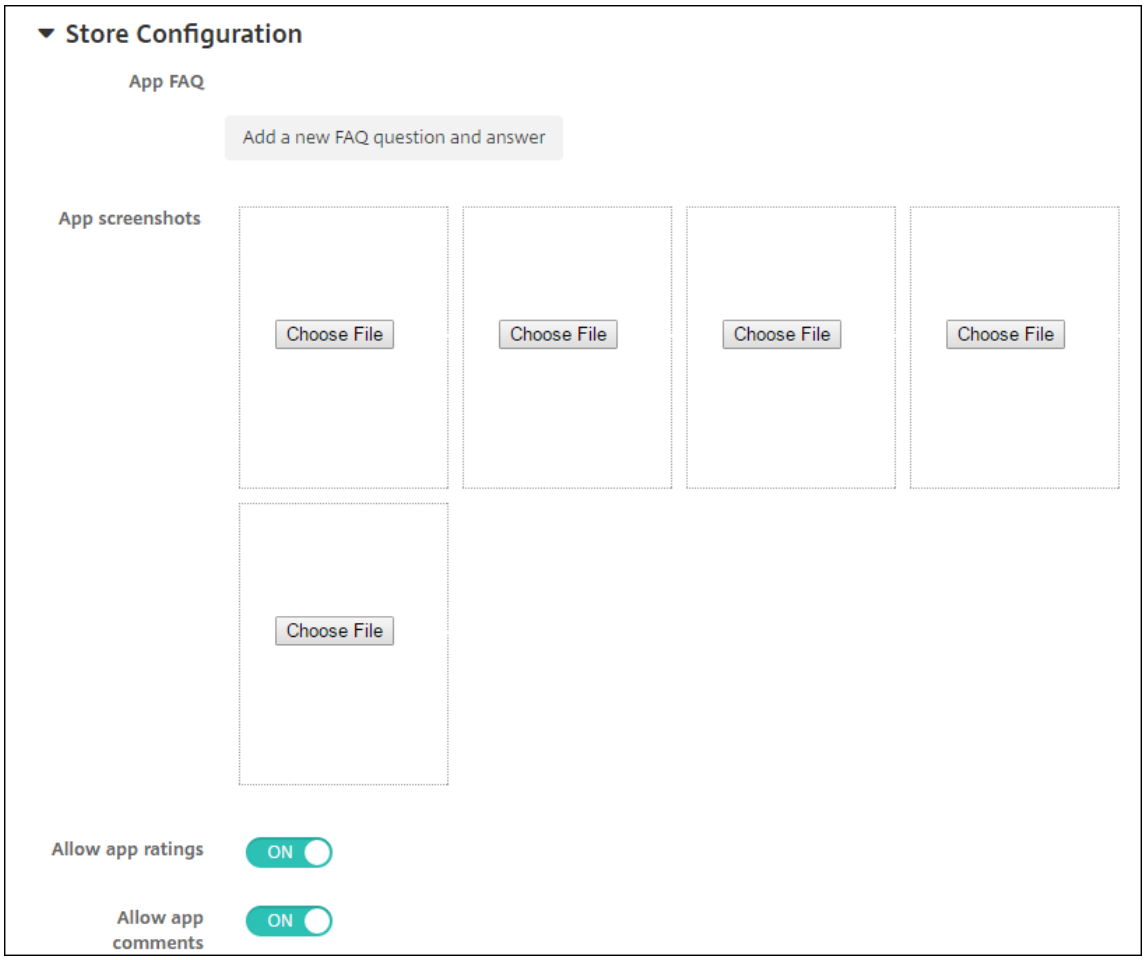
    - **Dateiname:** Geben Sie den Dateinamen der App ein.
    - **App-Beschreibung:** Geben Sie eine Beschreibung für die App ein.
    - **Produktschiene:** Geben Sie an, welche Produktversion Sie auf Benutzergeräte übertragen möchten. Wenn Sie ein spezielles Testprodukt haben, können Sie dies auswählen 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 Ressourcen bereitstellen.

15. Erweitern Sie **Storekonfiguration**. Diese Einstellung gilt nicht für Android Enterprise-Apps, die

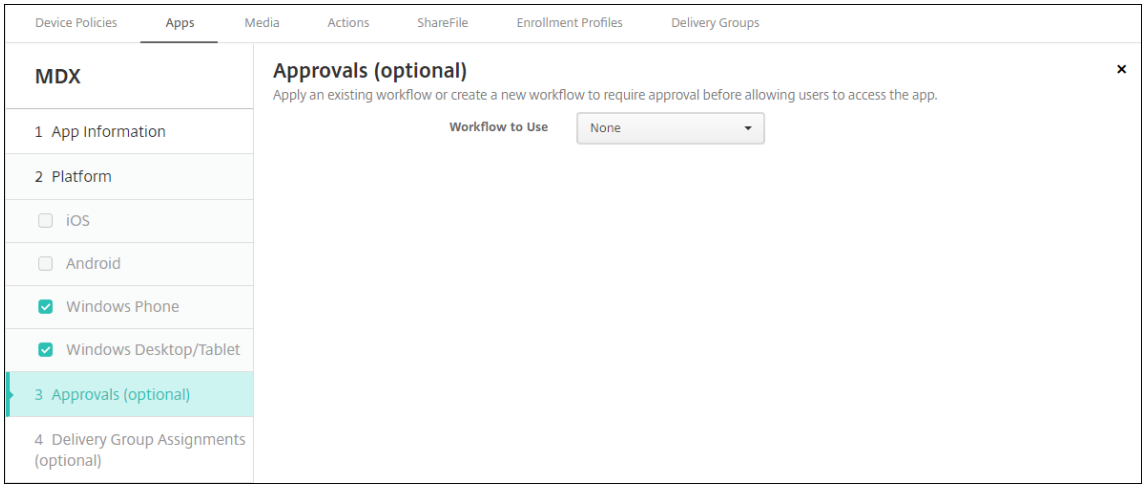
nur im verwalteten Google Play angezeigt werden.



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.

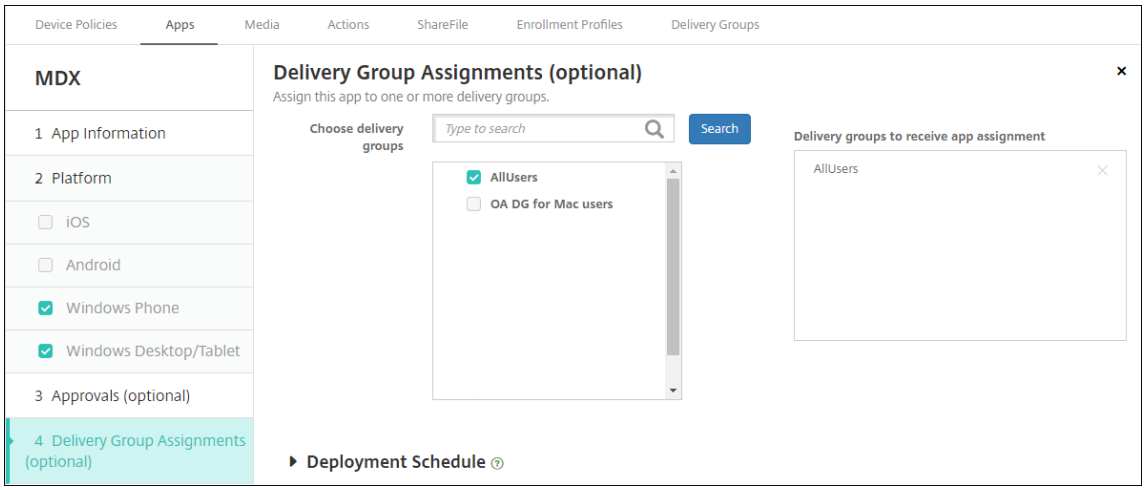
Konfigurieren Sie folgende Einstellungen zum Erstellen oder Zuweisen eines Workflows:

- **Verwendete Workflows:** Klicken Sie in der Dropdownliste 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 Erstellen und Verwalten 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 Kunden Citrix Endpoint Management in einer Version ab 10.18.19 verwenden. Wir empfehlen diese Verbindungen nicht für Kunden, die Citrix Endpoint Management in einer Version vor 10.18.19 verwenden.

  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 für jede mobile Produktivitätsapp.

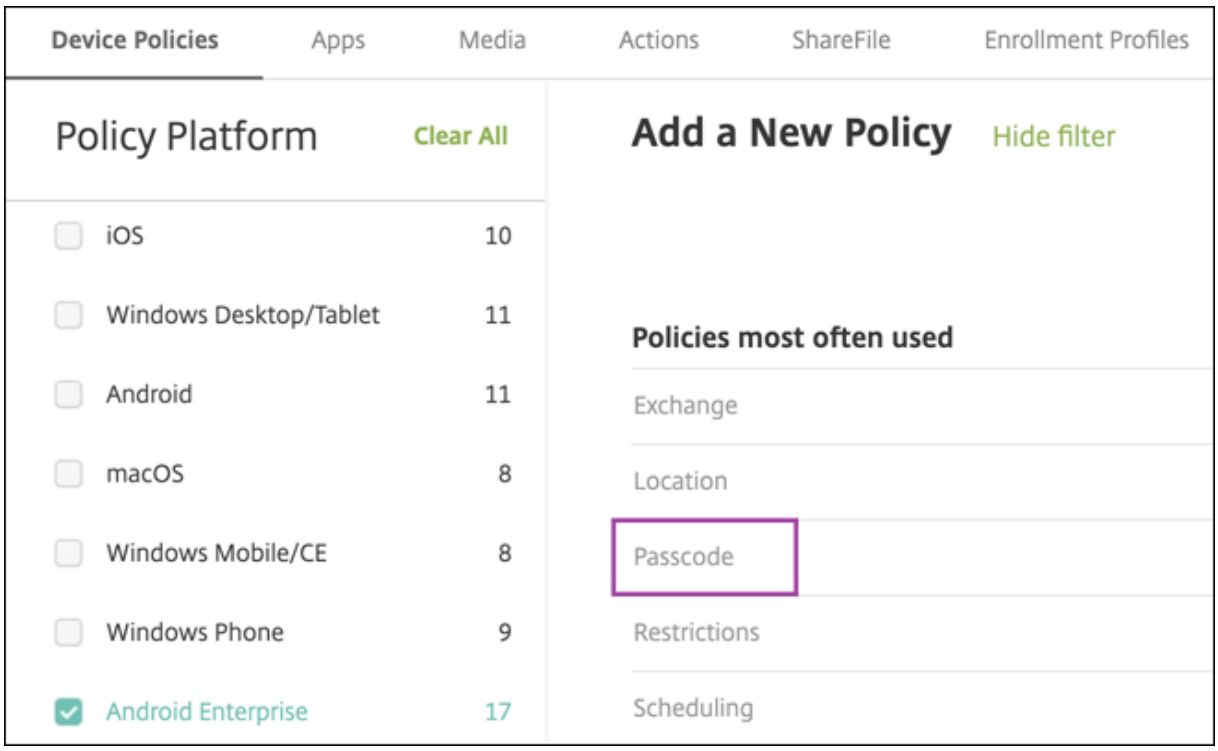
Konfigurieren der Richtlinie für die Sicherheitsabfrage

Die Geräterichtlinie für Citrix Endpoint Management-Passcode konfiguriert Sicherheitsabfrageregeln. Die Abfragen werden angezeigt, wenn Benutzer auf ihre Geräte oder auf 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.

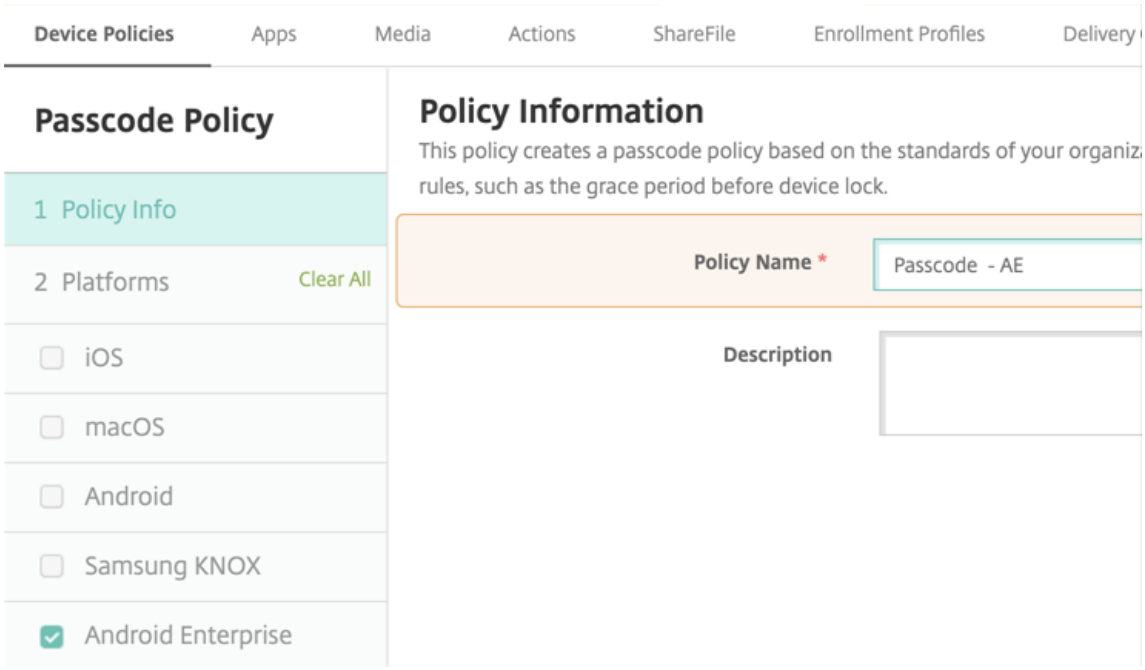
- Wenn in Ihrer Android Enterprise-Bereitstellung auch BYOD-Geräte enthalten sind, konfigurieren Sie die Passcoderichtlinie für das Arbeitsprofil.
- Wenn Ihre Bereitstellung vollständig verwaltete, firmeneigene Geräte umfasst, konfigurieren Sie die Passcoderichtlinie für das Gerät selbst.
- Wenn Ihre Bereitstellung beide Gerätetypen umfasst, konfigurieren Sie beide Arten von Passcoderichtlinien.

Konfigurieren der Passcoderichtlinie:

1. Klicken Sie in der Citrix Endpoint Management-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 verfüg-

baren 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 Citrix Endpoint Management-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
- Dedizierte Geräte
- Vollständig verwaltete Geräte mit Arbeitsprofil / Arbeitsprofil auf unternehmenseigenem Gerät

Sie können jedes dieser Android Enterprise-Registrierungsprofile auch so konfigurieren, dass BYOD-Android-Geräte als Arbeitsprofilgeräte registriert werden.

Wenn Android Enterprise für Ihre Citrix Endpoint Management-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 private Android-Arbeitsgeräte (BYOD) als Arbeitsprofil auf unternehmenseigenem Gerät.

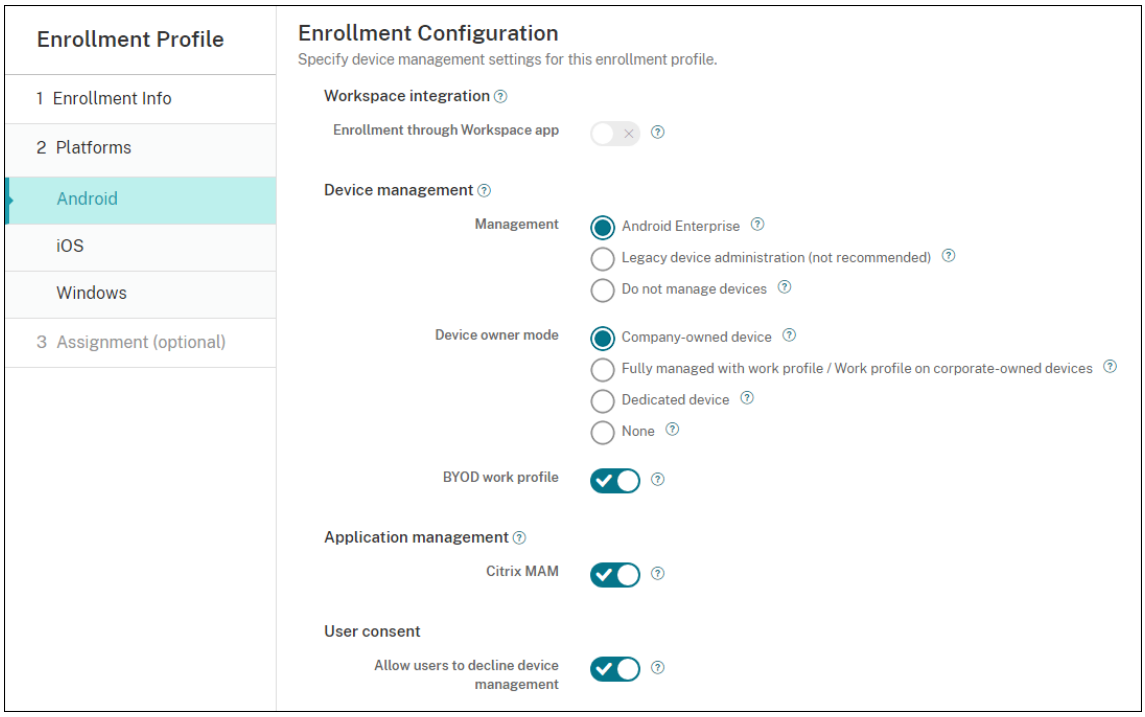
Wenn Sie Registrierungsprofile erstellen, weisen Sie ihnen Bereitstellungsgruppen zu. Wenn ein Benutzer zu mehreren Bereitstellungsgruppen mit unterschiedlichen Registrierungsprofilen gehört, bestimmt der Name der Bereitstellungsgruppe das verwendete Registrierungsprofil. Citrix Endpoint Management wählt die letzte Bereitstellungsgruppe in der alphabetisch geordneten Bereitstellungsgruppenliste aus. Weitere Informationen finden Sie unter Registrierungsprofile.

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 Citrix Endpoint Management-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. Legen Sie **BYOD-Arbeitsprofil** auf **Aus** fest, um die Registrierung auf vollständig verwaltete Geräte zu beschränken. Die Standardeinstellung ist **Ein**.
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.

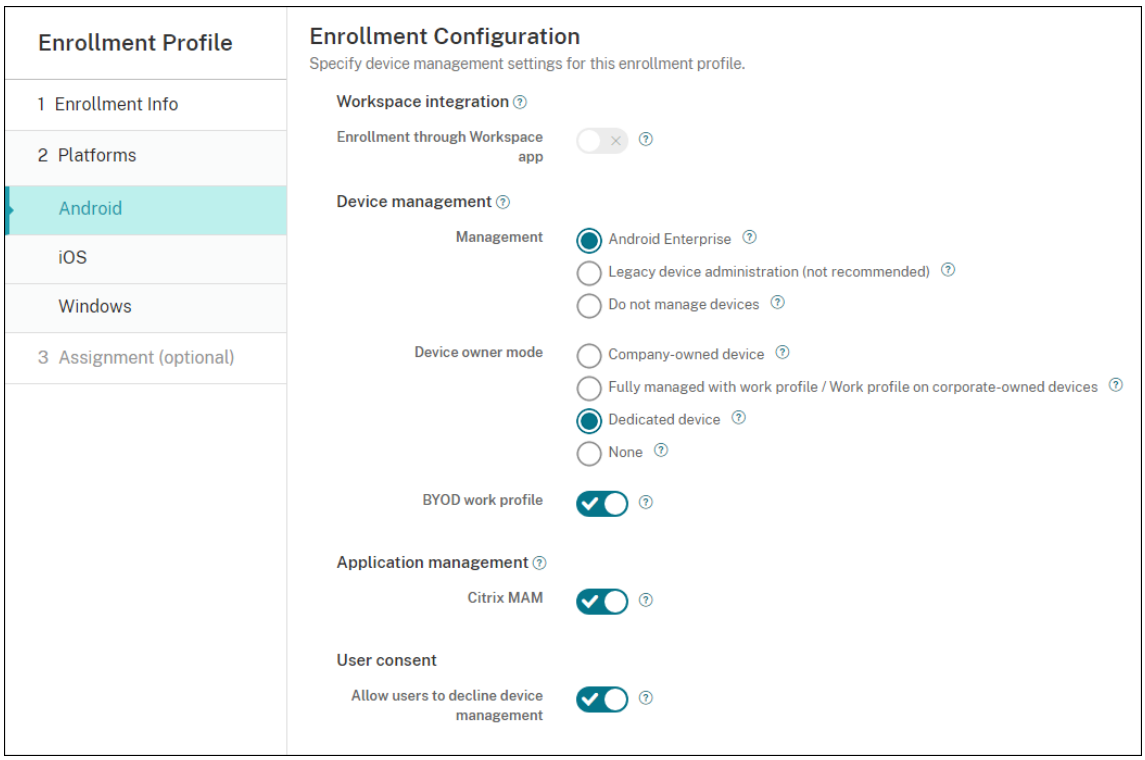
11. Wählen Sie die Bereitstellungsgruppe(n) mit den Administratoren, die voll verwaltete Geräte mit Arbeitsprofil registrieren sollen. Klicken Sie auf **Speichern**.

    Die Seite "Registrierungsprofil"wird mit dem von Ihnen hinzugefügten Profil angezeigt.

Hinzufügen eines Registrierungsprofil für dedizierte Geräte

Wenn Ihre Citrix Endpoint Management-Bereitstellung dedizierte Geräte enthält, können zahlreiche dedizierte Geräte durch einen oder mehrere Citrix Endpoint Management-Administratoren registriert werden. 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 Citrix Endpoint Management-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 die Anzahl der Geräte, die Mitglieder mit diesem Profil registrieren können, auf **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.



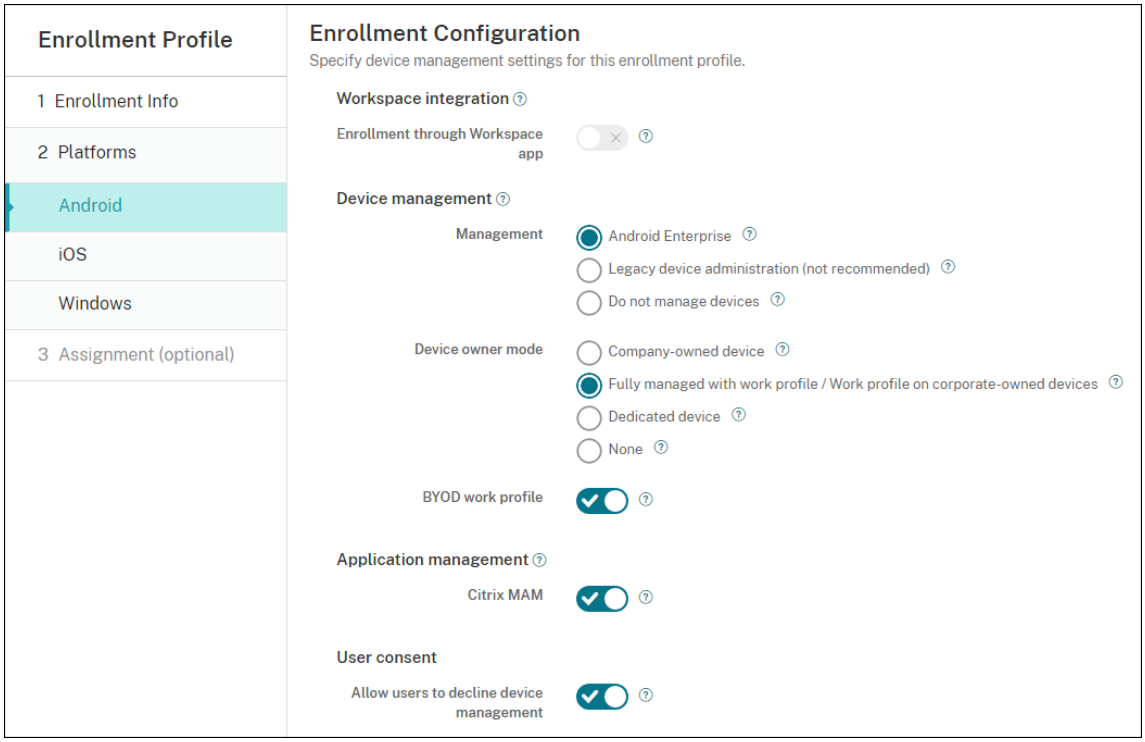
6. Mit **BYOD-Arbeitsprofil** können Sie das Registrierungsprofil so konfigurieren, dass BYOD-Geräte als Arbeitsprofilgeräte registriert werden. Neue Geräte und Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, werden als dedizierte Geräte registriert. Legen Sie **BYOD-Arbeitsprofil** auf **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 / Arbeitsprofil auf unternehmenseigenem Gerät

1. Gehen Sie in der Citrix Endpoint Management-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 bzw. Arbeitsprofil auf unternehmenseigenen Geräten** 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

Der Geräteadministratormodus für die Geräteverwaltung ist veraltet und wurde von Google eingestellt. 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 Citrix Endpoint Management-Bereitstellung aktiviert ist, werden alle neu registrierten oder wieder 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 Citrix Endpoint Management weiterhin in diesem Modus verwaltet.

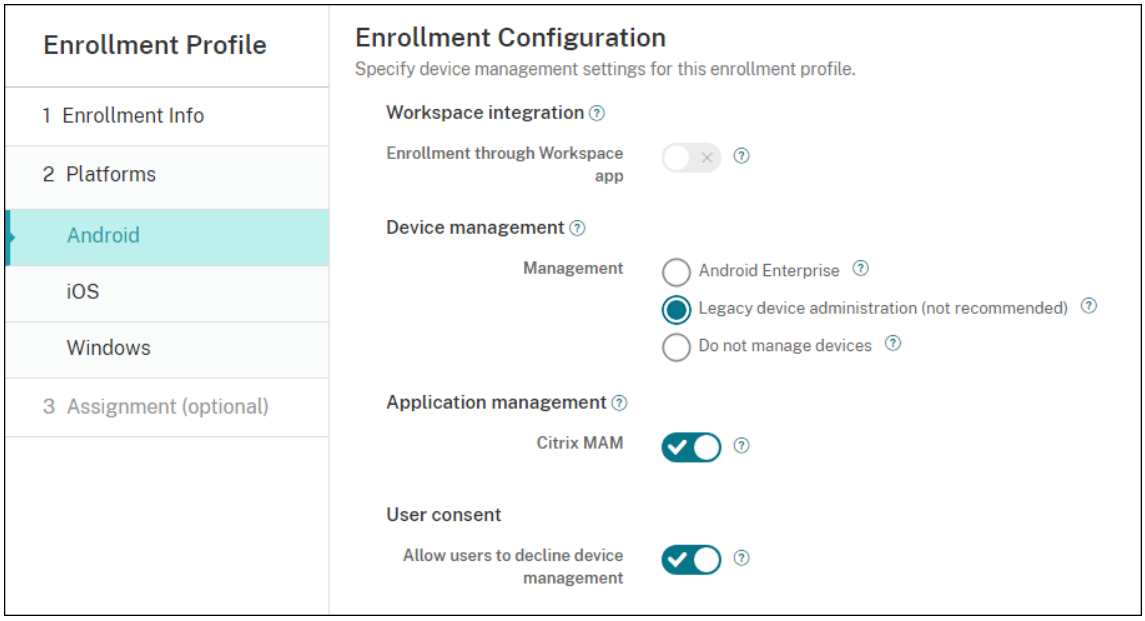
Erstellen Sie ein Registrierungsprofil für Legacygeräte, um bei der Neuregistrierung dieser Android-Geräte den Geräteadministratormodus zu verwenden.

Erstellen eines Registrierungsprofils für Legacygeräte:

1. Gehen Sie in der Citrix Endpoint Management-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 Legacygeräte weiterhin im Geräteadministratormodus zu verwalten, müssen Sie sie mit diesem Profil registrieren oder erneut registrieren. Sie registrieren Geräteadministratorgeräte ähnlich wie Arbeitsprofilgeräte, indem Benutzer Citrix 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 Citrix Endpoint Management. Die Benutzer laden Citrix 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 Citrix 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 Citrix Endpoint Management verwaltet und lädt Citrix 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 9.0 oder höher unterstützt. Siehe Zero-Touch-Registrierung.

- **Google-Konten:** Benutzer geben die Anmeldeinformationen für ihr Google-Konto ein, um das Provisioning zu starten. Diese Option gilt für Unternehmen, die Google Workspace verwenden.

Registrierung von Geräten mit dem Citrix DPC-ID-Token

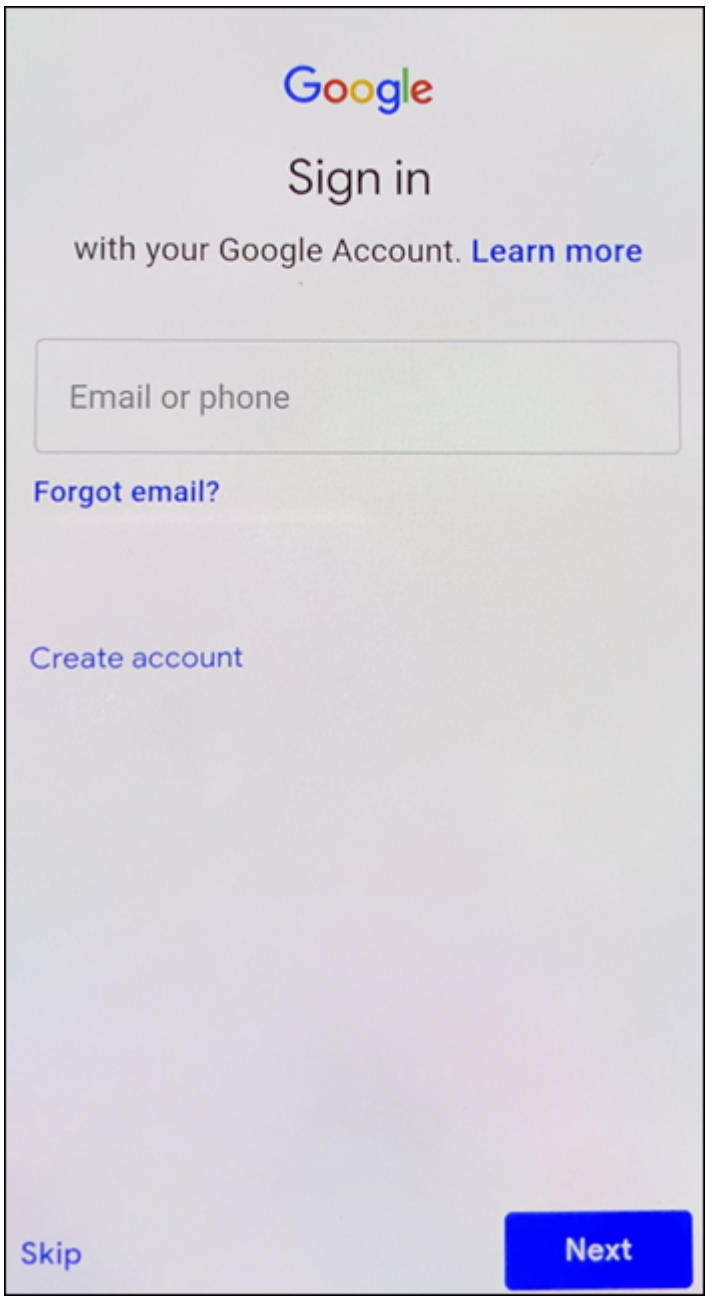
Benutzer geben `afw#xenmobile` ein, nachdem sie ein neues oder auf die Werkseinstellungen zurückgesetztes Gerät für die Ersteinrichtung eingeschaltet haben und aufgefordert wurden, ein Google-Konto einzugeben. Mit dieser Aktion wird Citrix Secure Hub heruntergeladen und installiert. Die Benutzer folgen anschließend den Anweisungen in Citrix Secure Hub zum Abschließen der Registrierung.

Systemanforderungen

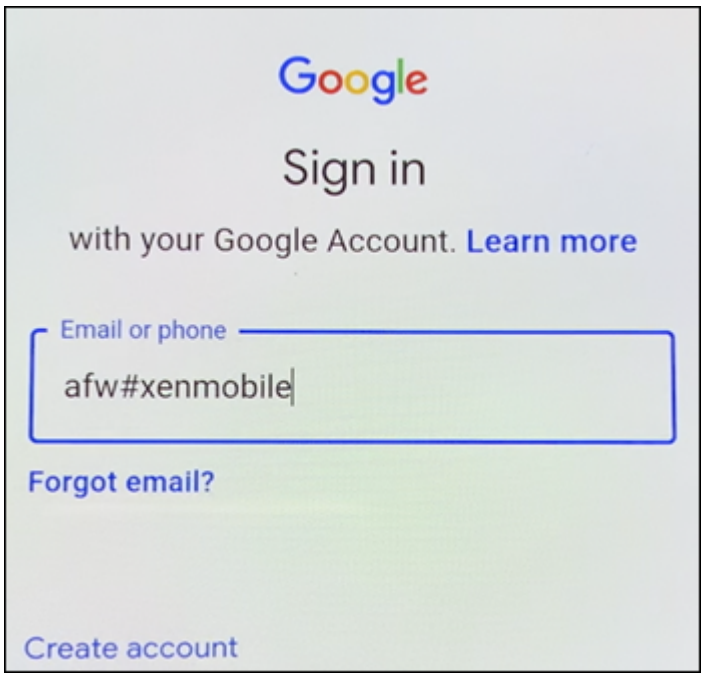
- Wird auf allen Android-Geräten mit Android-OS unterstützt.

Gerät registrieren

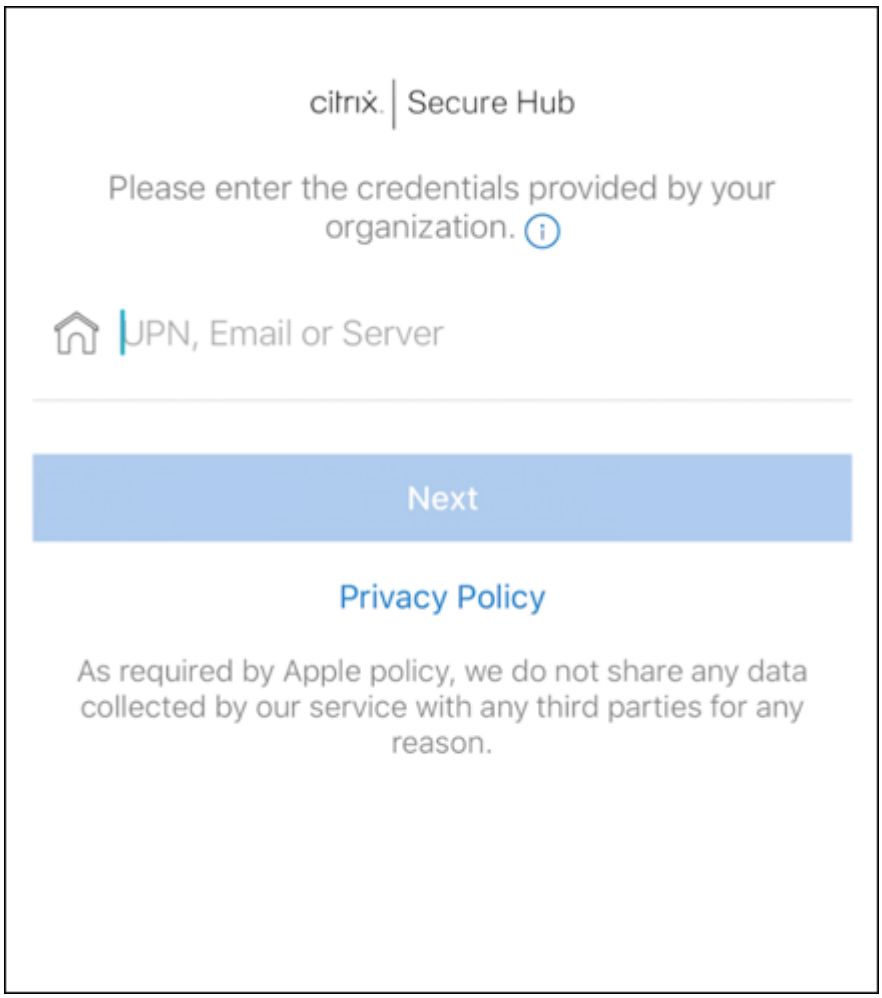
1. Schalten Sie ein neues oder auf die Werkseinstellungen zurückgesetztes Gerät ein.
2. Die Ersteinrichtung des Geräts wird geladen und der Benutzer wird aufgefordert, ein Google-Konto einzugeben. Falls das Gerät den Startbildschirm lädt, überprüfen Sie, ob in der Benachrichtigungsleiste die Benachrichtigung **Finish Setup** angezeigt wird.



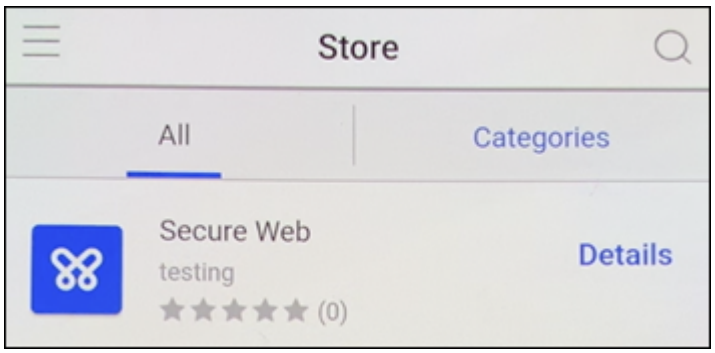
3. Geben Sie `afw#xenmobile` im Feld **Email oder phone** ein.



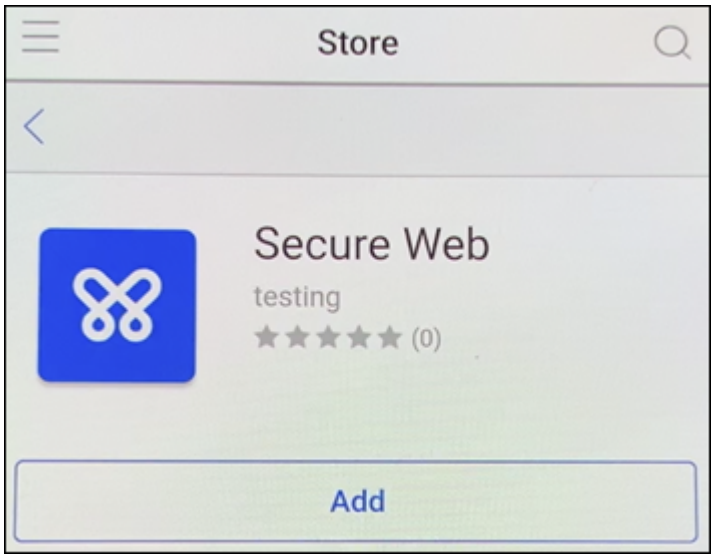
4. Tippen Sie im Android Enterprise-Bildschirm auf **Install**, um Citrix Secure Hub zu installieren.
5. Tippen Sie im Citrix Secure Hub-Installationsbildschirm auf **Install**.
6. Tippen Sie für alle App-Berechtigungsanforderungen auf **Allow**.
7. Tippen Sie auf **Accept & Continue**, um Citrix Secure Hub zu installieren und das Gerät damit zu verwalten.
8. Citrix 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**.



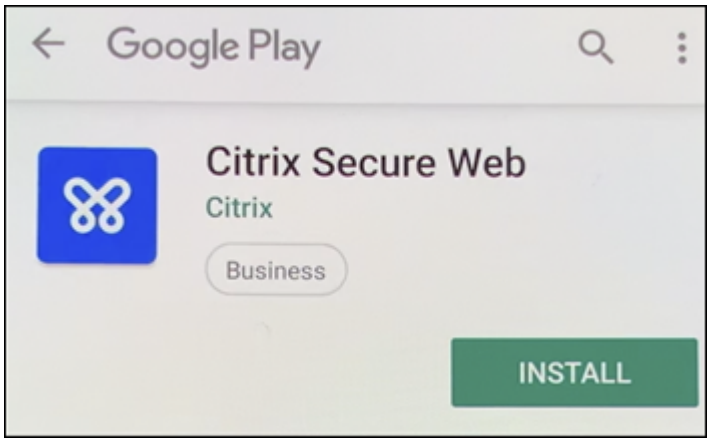
9. In der Standardkonfiguration für Citrix Endpoint Management können Benutzer auswählen, ob sie MAM oder MDM+MAM verwenden. Wenn die Aufforderung angezeigt wird, tippen Sie auf **Ja, Registrieren**, um MDM+MAM auszuwählen.
10. Geben Sie die E-Mail-Adresse und das Kennwort des Benutzers ein und tippen 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 Citrix Secure Hub. Tippen Sie auf **Apps aus dem Store hinzufügen**.
14. Tippen Sie zum Hinzufügen von Citrix Secure Web auf **Citrix Secure Web**.



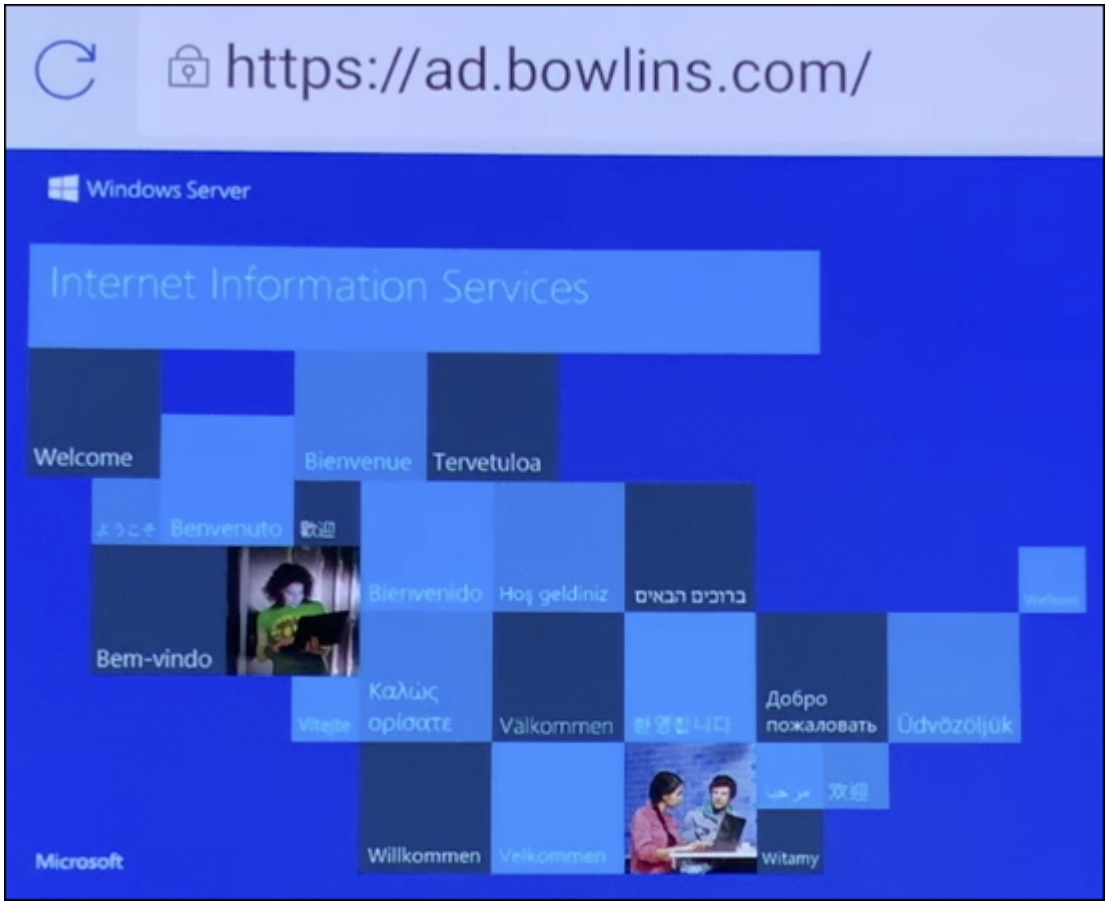
15. Tippen Sie auf **Hinzufügen**.



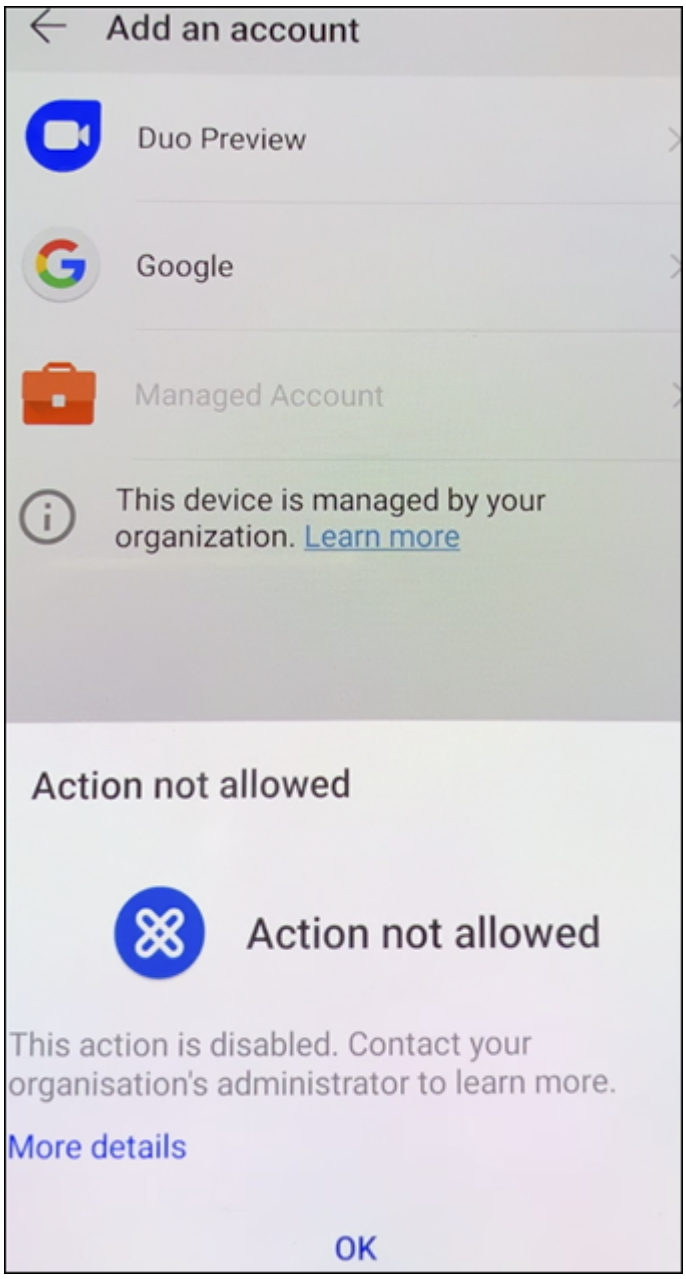
16. Citrix Secure Hub leitet den Benutzer zum Google Play Store, um Citrix Secure Web zu installieren. Tippen Sie auf **Installieren**.



17. Tippen Sie nach der Installation von Citrix 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 Citrix Endpoint Management Provisioning Tool ausgeführt wird.

Systemanforderungen und Voraussetzungen

- Unterstützte Android-Geräte.

- Ein neues oder auf die Werkseinstellungen zurückgesetztes Gerät mit NFC-Funktion, das für Android Enterprise als vollständig verwaltetes Gerät bereitgestellt wurde. Weitere Informationen finden Sie im Abschnitt Provisioning vollständig verwalteter Geräte mit Android Enterprise.
- Ein Gerät mit NFC-Funktion, auf dem das konfigurierte Provisioning Tool ausgeführt wird. Das Provisioning Tool ist in Citrix Secure Hub und auf der Citrix Downloadseite verfügbar.

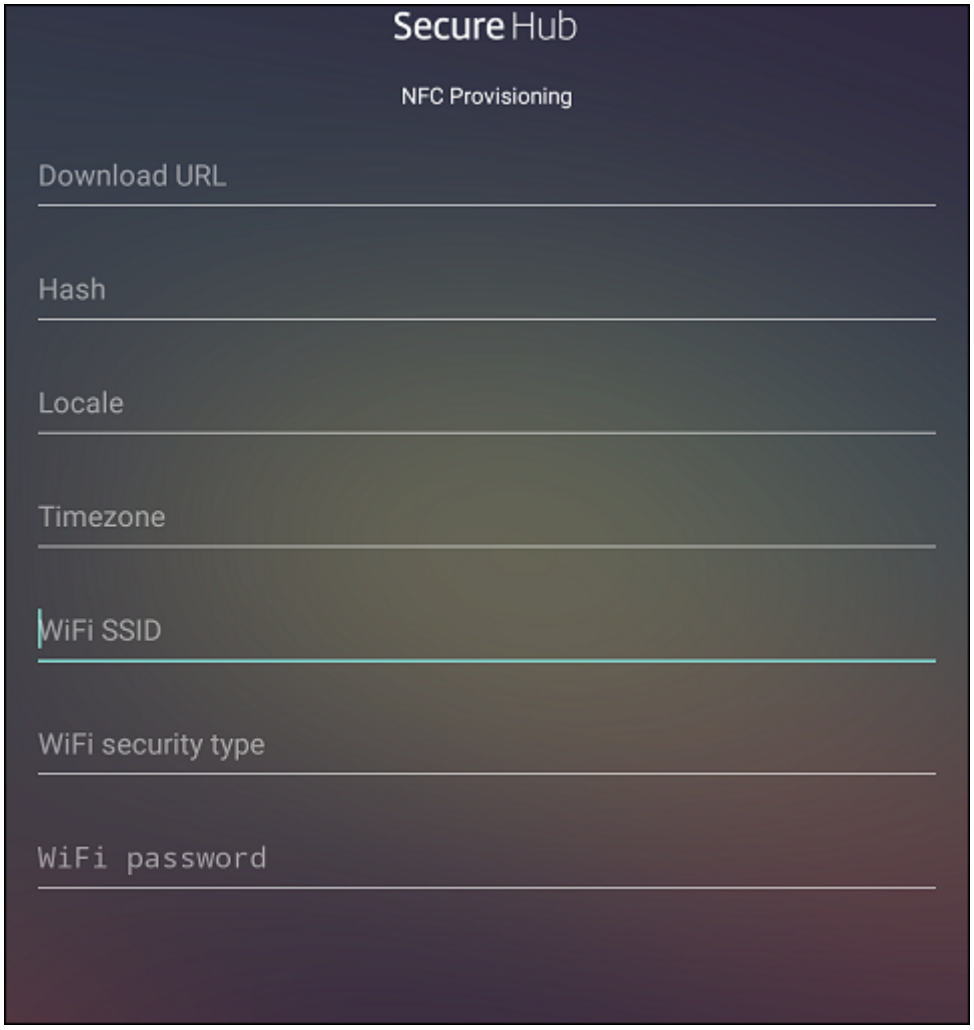
Auf jedem Gerät kann nur ein Android Enterprise-Profil installiert sein. In diesem Fall ist dies das Profil für den verwalteten Citrix Secure Hub. Sobald Sie eine zweite DPC-App hinzufügen, wird der installierte Citrix Secure Hub entfernt.

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 Citrix Secure Hub).
- Intranet-/Internetspeicherort, von dem das Gerät die DPC-App herunterlädt.
- SHA-256-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 Citrix Secure Hub mit Administratoreinstellungen verwendet. Wenn Sie keine Werte für Zeitzone und Speicherort eingeben, konfiguriert Android sie automatisch auf dem neuen Gerät.

Citrix Endpoint Management Provisioning Tool konfigurieren 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 eingeben oder die Felder mithilfe einer Textdatei ausfüllen. Nachfolgend wird beschrieben, wie Sie die Textdatei mit den Beschreibungen für jedes Feld konfigurieren. Die App speichert die eingegebenen Informationen nicht. Erstellen Sie daher eine Textdatei zur Aufbewahrung der Informationen.

Provisioning Tool mit einer Textdatei konfigurieren 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=<SHA-256 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 den Datenbanknamen des Gebiets/Standorts ein. Geben Sie beispielsweise **America/Los_Angeles** für “Pacific Time”ein. Wenn Sie keinen Namen eingeben, wird die Zeitzone automatisch eingefügt.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

Keine Eingabe ist erforderlich, da der Wert in der App als Citrix 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=ga50TwdCmfdJ72LGR
\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=ga50TwdCmfdJ72LGR
\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
```

Citrix Secure Hub-Prüfsumme abrufen Die Citrix Secure Hub-Prüfsumme ist ein konstanter Wert: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. Um eine APK-Datei für Citrix Secure Hub herunterzuladen, verwenden Sie den folgenden Google Play-Link: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

App-Prüfsumme abrufen 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_S` 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.

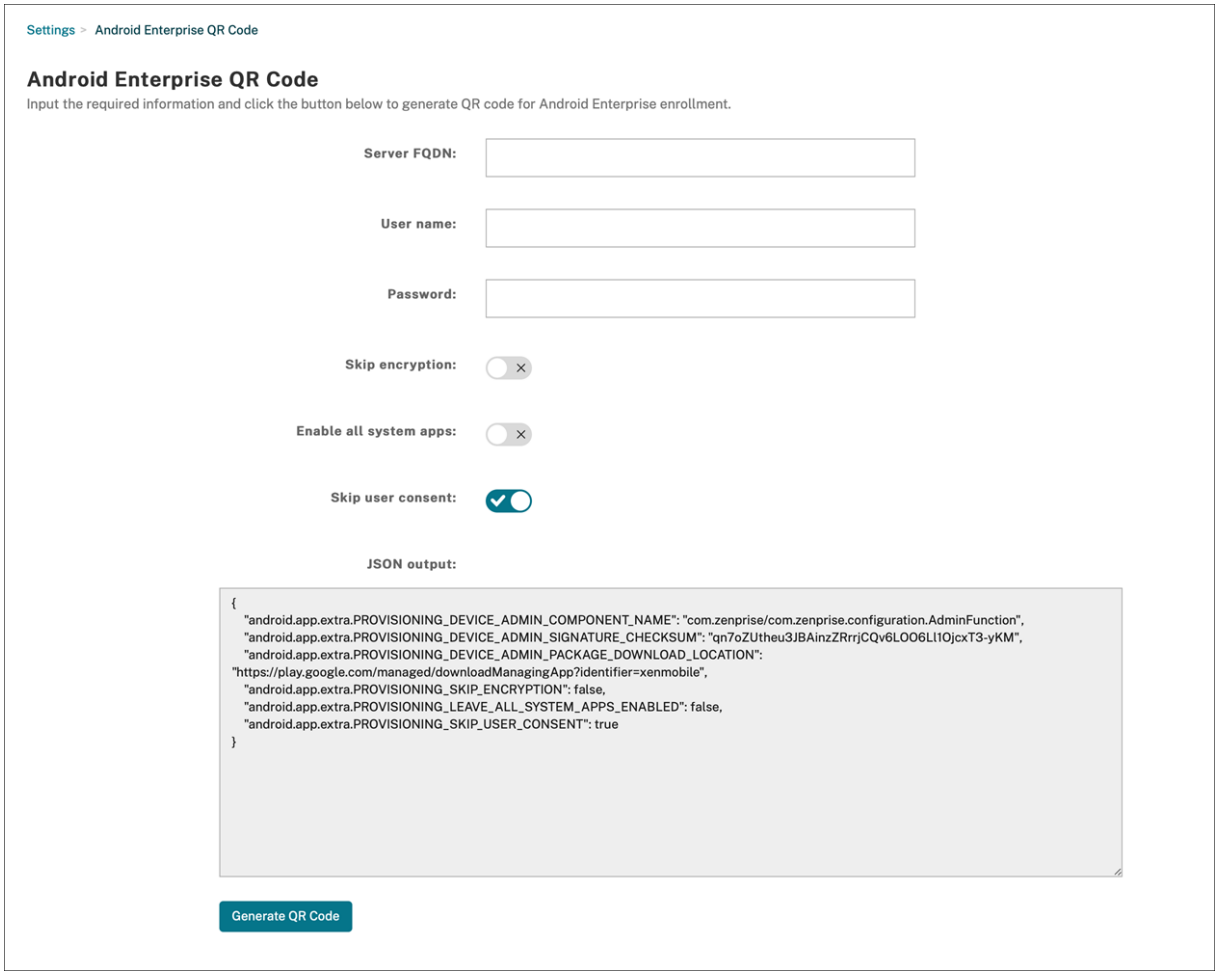
- Butter Knife von Jake Wharton unter Apache-Lizenz 2.0

Registrieren von Geräten per QR-Code

Benutzer können ein vollständig verwaltetes Gerät per QR-Code registrieren, den Sie für sie generieren.

Systemanforderungen Android-Geräte mit Android 7.0 oder höher.

Erstellen eines QR-Codes Sie generieren einen QR-Code, indem Sie die Registrierungsinformationen nach Bedarf festlegen. Nachdem Sie einen QR-Code generiert haben, speichern Sie ihn lokal. Er wird nicht in Citrix Endpoint Management gespeichert.



1. Navigieren Sie zu **Einstellungen > Android Enterprise QR-Code**.
2. Falls erforderlich, geben Sie die folgenden Registrierungsinformationen ein:

    - **Server-FQDN:** Geben Sie den Server-FQDN für Citrix Endpoint Management ein (z. B. `example.cem.cloud.com`). Das Feld ist optional. Wenn Sie es unausgefüllt lassen, müssen Benutzer die Information bei der Registrierung eingeben.
    - **Benutzername:** Geben Sie den Benutzernamen für die Registrierung ein. Wir empfehlen, dieses Feld leer zu lassen, wenn Sie den QR-Code an mehrere Benutzer verteilen möchten. Das Konfigurieren eines QR-Codes mit Benutzernamen und Kennwort ist nützlich, um Kioskgeräte zu registrieren. Wenn Sie das Feld unausgefüllt lassen, müssen Benutzer die Information bei der Registrierung eingeben.
    - **Kennwort:** Geben Sie das zugeordnete Kennwort für den eingegebenen Benutzernamen ein. Wenn Sie das Feld unausgefüllt lassen, müssen Benutzer die Information bei der Registrierung eingeben.
    - **Verschlüsselung überspringen:** Bei Auswahl von **Ein** wird das Gerät bei der Registrierung nicht verschlüsselt. Die Standardeinstellung ist **Aus**.
    - **Alle System-Apps aktivieren:** Die Einstellung **Ein** ermöglicht den Zugriff auf alle System-

Apps auf dem Gerät. Die Standardeinstellung ist **Aus**.

- **Einwilligung des Benutzers überspringen:** Bei Auswahl von **Aus** können Benutzer die Geräteverwaltung ablehnen. Die Standardeinstellung ist **Aus**.

Im Feld **JSON-Ausgabe** wird der JSON-Inhalt angezeigt, der mit den von Ihnen angegebenen Informationen übereinstimmt.

3. Bearbeiten Sie den JSON-Inhalt im Feld **JSON-Ausgabe**, um weitere Registrierungsinformationen hinzuzufügen.
4. Klicken Sie auf **QR-Code generieren**. Der QR-Code wird rechts von der JSON-Ausgabe angezeigt.
5. Klicken Sie mit der rechten Maustaste auf den QR-Code, um ihn zu speichern.
6. Senden Sie das Bild zur Geräteregistrierung an die Benutzer.

Ein auf die Werkseinstellungen zurückgesetztes Gerät scannt den QR-Code, um als vollständig verwaltetes Gerät registriert zu werden.

Gerät registrieren 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 kann der Speicherort im QR-Code für den Download von Citrix Secure Hub aufgerufen werden.

   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 Citrix Secure Hub vom Speicherort im QR-Code herunter, validiert die Signatur des Signaturzertifikats, installiert Citrix 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 Citrix Endpoint Management registriert. Die dem Gerät zugewiesene Konfiguration definiert den automatischen Registrierungsprozess.

Systemanforderungen

- Unterstützung für Zero-Touch-Registrierung beginnt mit Android 9.0.

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 Citrix Endpoint Management-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-->
```

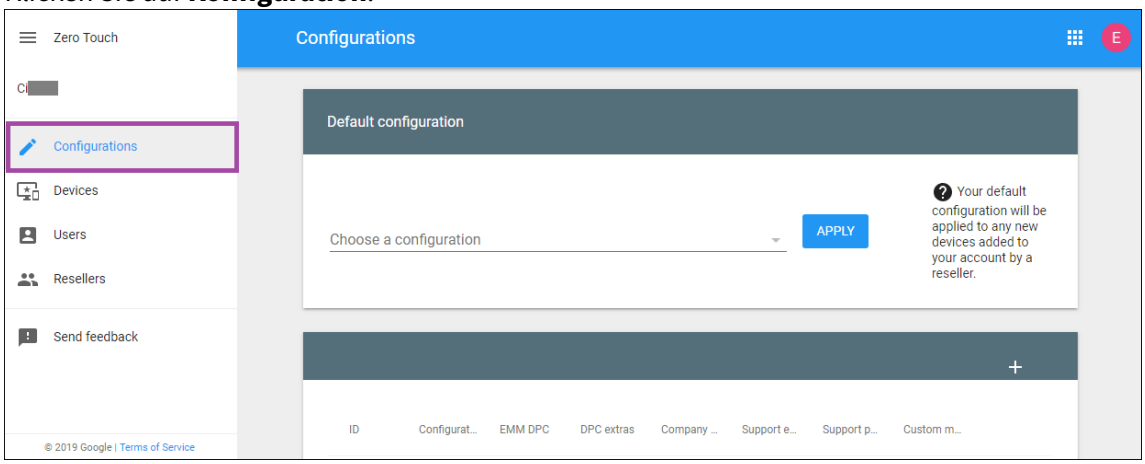
Mit einem optionalen JSON-Objekt mit zusätzlichen Parametern können Sie Ihre Konfiguration weiter anpassen. Im folgenden Beispiel sind der Citrix Endpoint Management-Server festgelegt sowie der Benutzername und das Kennwort, mit denen Geräte sich in dieser Konfiguration am Server anmelden.


```
    {

        "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
          {

              "serverURL":"URL",
              "xm_username":"username",
              "xm_password":"password"
           }

             }

<!--NeedCopy-->
```

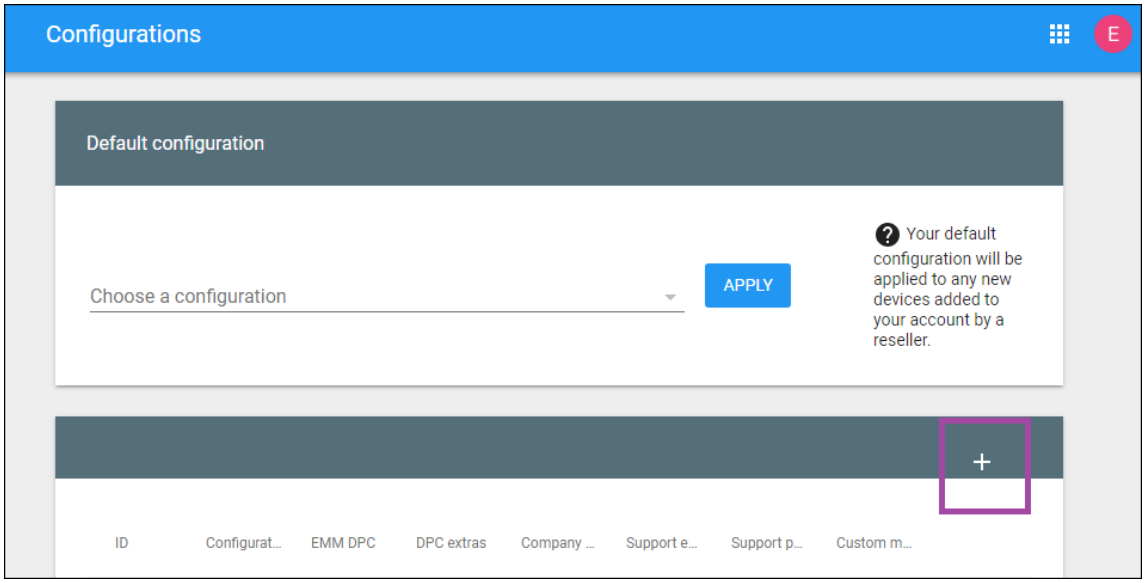
Wichtig:

Um Geräte im Modus “Arbeitsprofil auf unternehmenseigenem Gerät”zu registrieren, ergänzen Sie das benutzerdefinierte JSON unter `PROVISIONING_ADMIN_EXTRAS_BUNDLE` um `{ "desiredProvisioningMode": "managedProfile"}`.

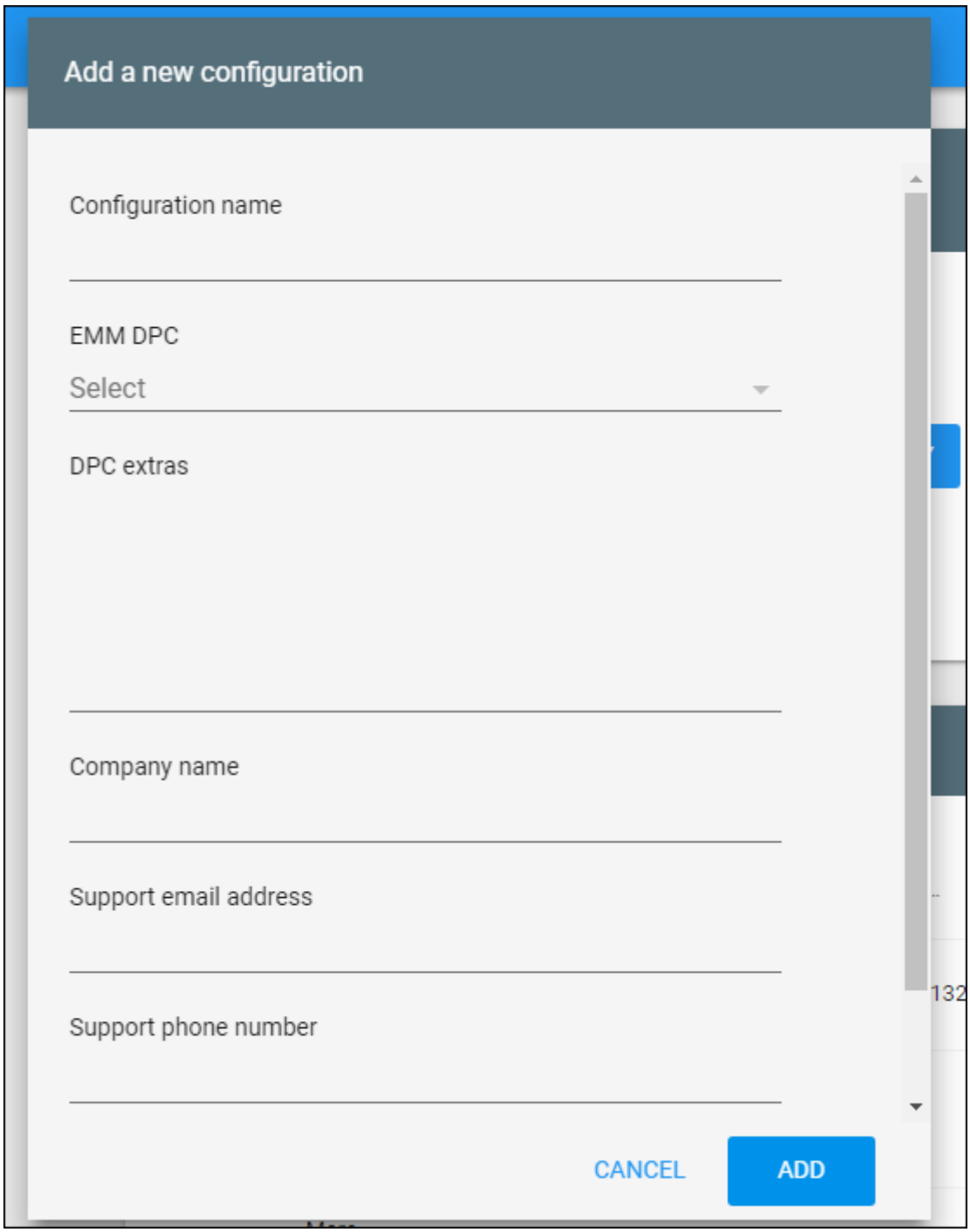
1. Navigieren Sie zum Android-Portal für die Zero-Touch-Registrierung unter https://partner.android.com/zerotouch. Melden Sie sich mit den Kontoinformationen an, die Sie vom Vertriebspartner Ihres Zero-Touch-Geräts erhalten haben.
2. Klicken Sie auf **Konfiguration**.



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

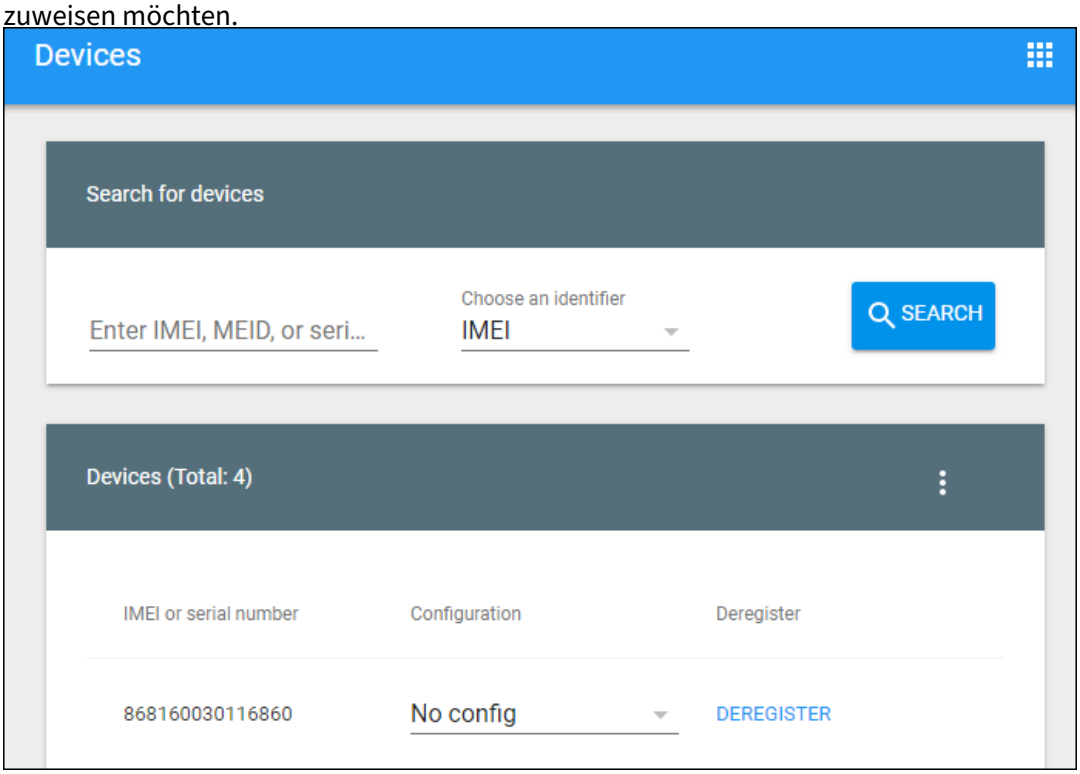
Benutzern ein. Diese Adresse wird vor dem Provisioning auf Ihren Android Enterprise-Geräten mit Zero-Touch-Registrierung angezeigt.

- **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 **Update**.

Über eine CSV-Datei können Sie eine Konfiguration auf mehrere Geräte anwenden.

Informationen zum Anwenden einer Konfiguration auf mehrere Geräte finden Sie unter Zero-Touch-Registrierung für IT-Administratoren. Dieses Android Enterprise-Hilfethema enthält weitere Informa-

tionen, wie Sie Konfigurationen verwalten und auf Geräte anwenden.

Provisioning von dedizierten Geräten mit Android Enterprise

Dedizierte Android Enterprise-Geräte sind vollständig verwaltete Einzweckgeräte. Sie beschränken diese Geräte 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 Citrix Endpoint Management-Administratoren hinzu, denen Sie die Registrierung von dedizierten Geräten bei Citrix Endpoint Management gestatten möchten. Siehe Registrierungsprofile erstellen.
- Um einem dedizierten Gerät den Zugriff auf Apps zu ermöglichen, fügen Sie diese zur Positivliste hinzu.
- 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. Citrix Secure Hub- und Google Play-Dienste stehen standardmäßig auf der Positivliste.

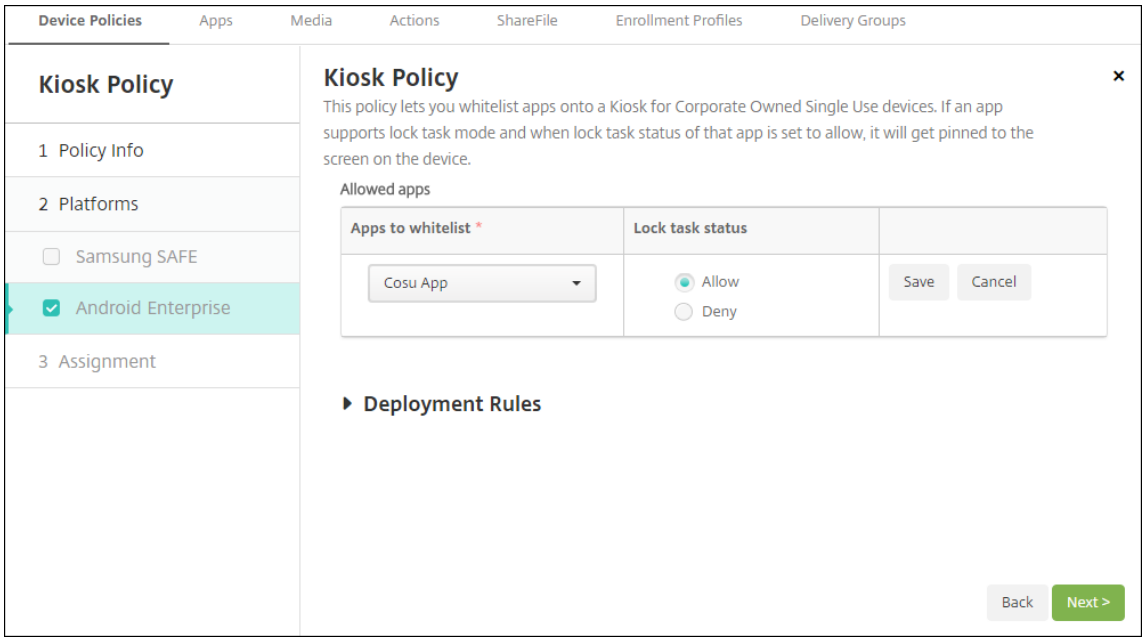
Hinzufügen der Kioskrichtlinie

1. Klicken Sie in der Citrix Endpoint Management-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.

Provisioning vollständig verwalteter Android Enterprise-Geräte mit Arbeitsprofil oder Arbeitsprofil auf unternehmenseigenem Gerät

Geräte mit Android 9.0-10.x werden als "vollständig verwaltet mit Arbeitsprofil"registriert. Ab Android 11 werden Geräte als "Arbeitsprofil auf unternehmenseigenem Gerät"registriert. Alle diese Geräte sind firmeneigene Geräte, die für geschäftliche und private Zwecke genutzt werden. Ihre Organisation verwaltet das gesamte Gerät. Sie können einige Richtlinien auf das Gerät und andere Richtlinien auf das Arbeitsprofil anwenden.

In der Citrix Endpoint Management-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 9.0 unterstützt.

Gerät registrieren

Neue Geräte und Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, werden als vollständig verwaltete Geräte mit Arbeitsprofil registriert. Diese Geräte verwenden die Registrierungsmethoden für vollständig verwaltete Geräte, wie unter Provisioning vollständig verwalteter Geräte in Android Enterprise beschrieben. Geräte mit Android 11 können als "Arbeitsprofil auf unternehmenseigenem Gerät"registriert werden, mithilfe der dort beschriebenen Verfahren per QR-Code bzw. Zero-Touch-Registrierung.

> **Wichtig:**
>
> Wenn Sie Geräte im Modus "Arbeitsprofil auf unternehmenseigenem Gerät"per QR-Code registrieren, sollten Sie der JSON-Ausgabe oberhalb des Felds `serverURL` Folgendes hinzufügen:
> `"desiredProvisioningMode": "managedProfile",`

JSON output

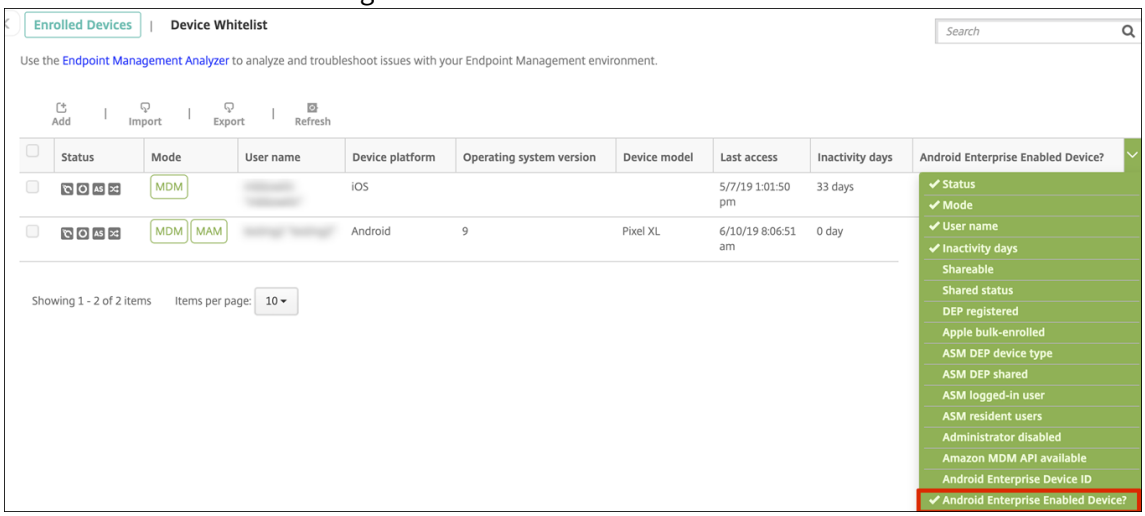

```
{
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
    "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
    "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
    "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
        "desiredProvisioningMode": "managedProfile",
        "serverURL": "https://testServer.xmqa.cloud.com",
        "username": "username",
        "password": "password"
    }
```


Geräte, die nicht neu oder auf die Werkseinstellungen zurückgesetzt sind, werden als Arbeitsprofilgeräte registriert, wie unter Provisioning von Arbeitsprofilgeräten mit Android Enterprise beschrieben.

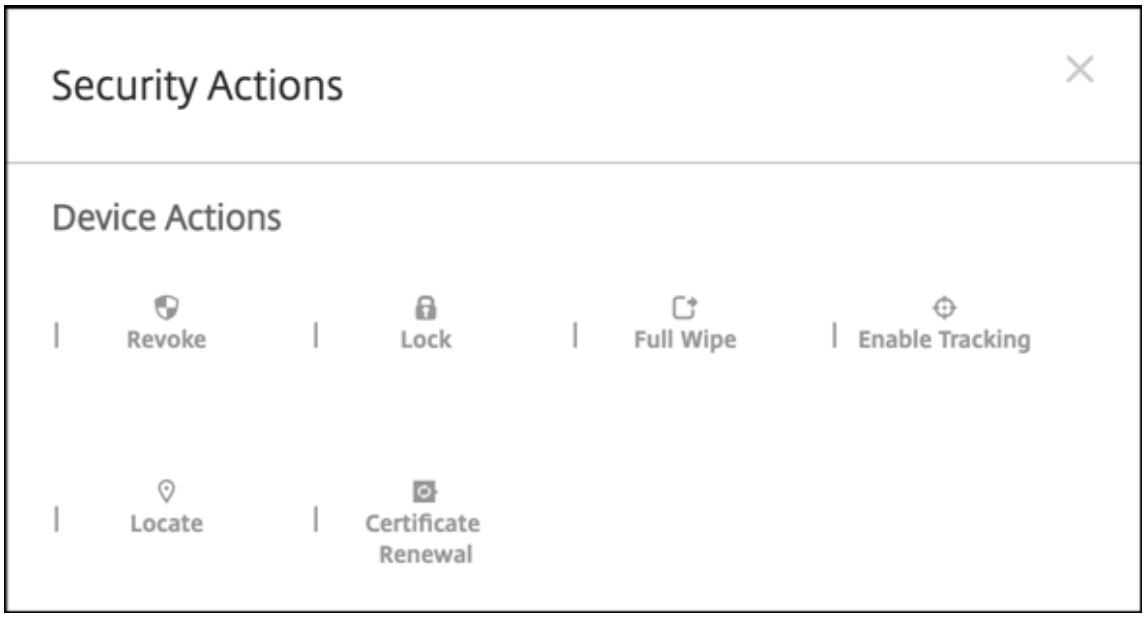
Anzeige von Android Enterprise-Geräten in der Citrix Endpoint Management-Konsole

Anzeige von vollständig verwalteten Android Enterprise-Geräten, dedizierten Geräten und vollständig verwalteten Geräten mit Arbeitsprofil:

1. Gehen Sie in der Citrix Endpoint Management-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:

- **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.

Geräterichtlinien

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 Enterprise.

	App-Berechtigungen	App-Bestand	App-Deinstallation
	Verwaltete Apps automatisch aktualisieren	Verbindungszeitplan	Anmeldeinformationen
	Benutzerdefiniertes XML	Citrix Endpoint Management-Optionen	Dateien
	Keyguard-Verwaltung	Kiosk	Launcher-Konfiguration
	Standort	Verwaltete Konfigurationen	Netzwerk
	OS-Update	Passcode	Einschränkungen

Geräterichtlinien für vollständig verwaltete Geräte mit Arbeitsprofil (COPE-Geräte)

Bei vollständig verwalteten Geräten mit Arbeitsprofil können Sie mithilfe von Geräterichtlinien separate Einstellungen auf das gesamte Gerät bzw. das Arbeitsprofil anwenden. Mit separaten Geräterichtlinien können Sie bei vollständig verwalteten Geräterichtlinien mit Arbeitsprofil Einstellungen nur auf das gesamte Gerät oder auf das Arbeitsprofil anwenden. Bei Geräten, die im Modus "Arbeitsprofil auf unternehmenseigenem Gerät"registriert sind, gelten die Richtlinien nur für das Arbeitsprofil und nicht für das gesamte Gerät.

Richtlinie	Gilt für
App-Berechtigungen	Arbeitsprofil
App-Bestand	Arbeitsprofil
App-Deinstallation	Arbeitsprofil

Richtlinie	Gilt für
Verwaltete Apps automatisch aktualisieren	Arbeitsprofil
Verbindungszeitplan	Arbeitsprofil
Anmeldeinformationen	Arbeitsprofil
Benutzerdefiniertes XML	–
Citrix Endpoint Management-Optionen	Arbeitsprofil
Dateien	Arbeitsprofil
Keyguard-Verwaltung	Gerät und Arbeitsprofil
Kiosk	–
Launcher-Konfiguration	Gerät und Arbeitsprofil
Standort	Gerät (nur Standortmodus)
Verwaltete Konfigurationen	Arbeitsprofil
Netzwerk	Gerät
OS-Update	–
Passcode	Gerät und Arbeitsprofil
Einschränkungen	Geräte- und Arbeitsprofil (separate Richtlinien für Gerät und Arbeitsprofil erstellen)
VPN	–

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.

Sicherheitsaktion	Arbeitsprofil	Vollständig verwaltet
Zertifikaterneuerung	Ja	Ja
Vollständig löschen	Ja (nach selektivem Löschen)	Ja
Orten	Ja	Ja

Sicherheitsaktion	Arbeitsprofil	Vollständig verwaltet
Sperren	Ja	Ja
Lock and Reset Password	Nein	Ja
Notify (Ring)	Ja	Ja
Widerrufen	Ja	Ja
Selektiv löschen	Ja	Ja

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 9.0 gilt Folgendes:
  - Die Aktion “Sperren und Kennwort zurücksetzen”wird nicht unterstützt.
- Auf Arbeitsprofilgeräten mit Android 9.0 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).

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 Citrix Endpoint

> Management-Konsole aktualisieren.

Nachdem die Registrierung des Android Enterprise-Unternehmens aufgehoben wurde:

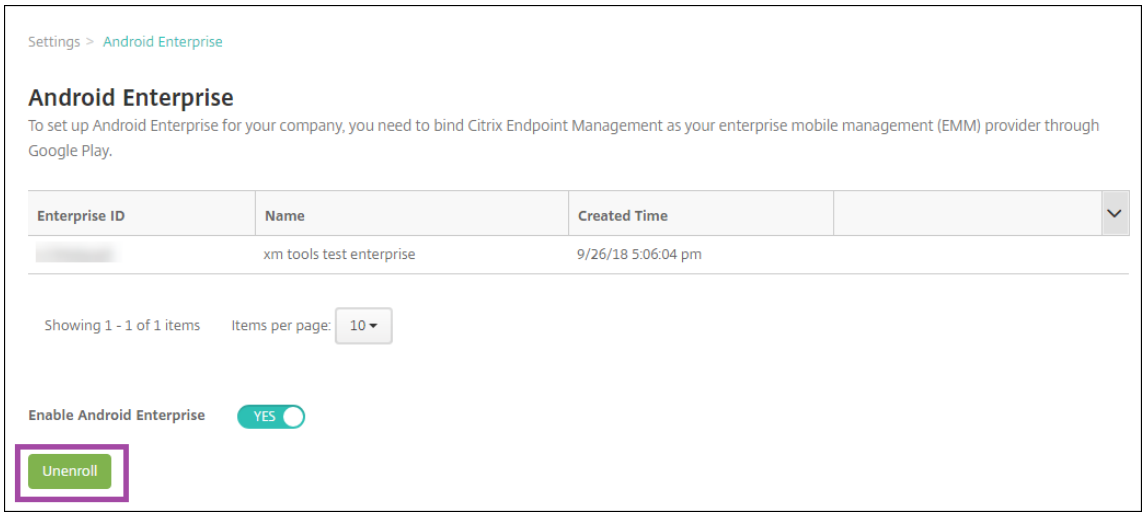
- Für Geräte und Benutzer, die über das Unternehmen registriert sind, wurden die Android Enterprise-Apps auf die Standardeinstellung zurückgesetzt. Zuvor angewendete Richtlinien für verwaltete Konfigurationen haben keine Wirkung mehr auf Vorgänge.
- Citrix Endpoint Management verwaltet Geräte, die über 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 Konfigurationen anwenden. 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 für Android Enterprise-Unternehmen mit der Citrix Endpoint Management-Serverkonsole und den Citrix Endpoint Management Tools auf.

Wenn Sie diese Aufgabe ausführen, wird in Citrix Endpoint Management ein Tools-Popupfenster geöffnet. Stellen Sie darum zunächst sicher, dass Popupfenster im Browser geöffnet werden können. In einigen Browsern (z. B. Google Chrome) müssen Sie die Popupblockierung deaktivieren und die Adresse der Citrix Endpoint Management-Site der Positivliste des Popupblockers hinzufügen.

Registrierung für Android Enterprise-Unternehmen aufheben:

1. Klicken Sie in der Citrix Endpoint Management-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**.



Android Enterprise-Apps verteilen

June 25, 2024

Citrix Endpoint Management verwaltet die auf Geräten bereitgestellten Apps. Sie können folgende Arten von Android Enterprise-Apps organisieren und bereitstellen.

- **Verwaltete App Store-Apps:** Dies sind kostenlose 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 Citrix Endpoint Management-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 Citrix Endpoint Management-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 Citrix Endpoint Management-Konsole wechseln, ist der App-Besitzer unterschiedlich. In diesem Fall müssen Sie Ihre Apps an beiden Standorten verwalten. 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 Apps hinzufügen. 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

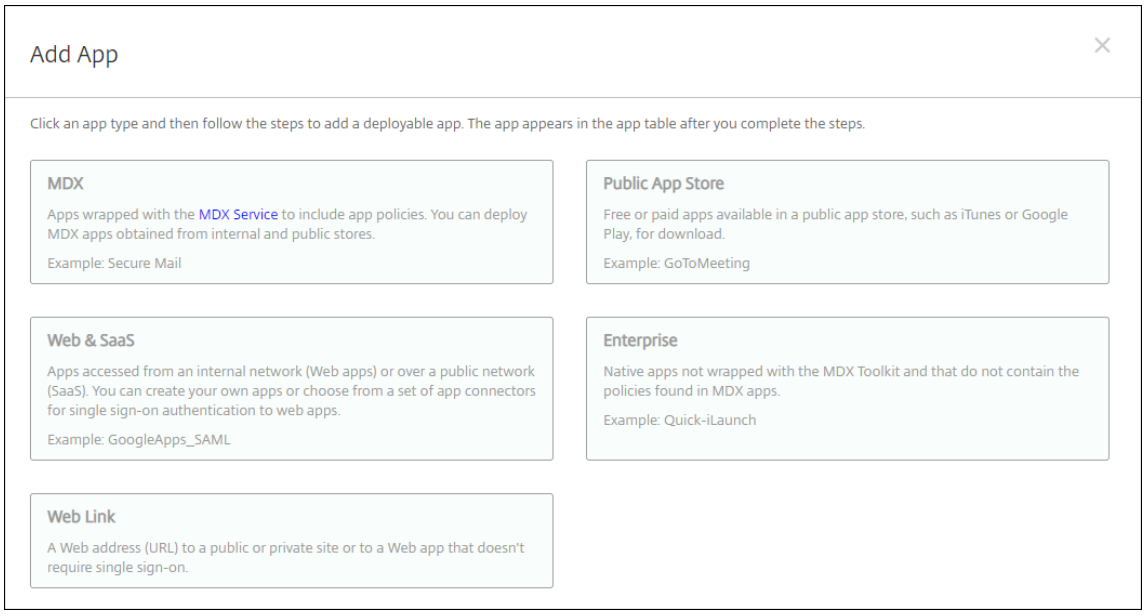
Verwaltete App Store-Apps

Sie können kostenlose Apps aus dem verwalteten Google Play Store in Citrix Endpoint Management hinzufügen.

> **Hinweis:**
>
> Um alle Apps in Google Play über den verwalteten Google Play-Store zugänglich zu machen, verwenden 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

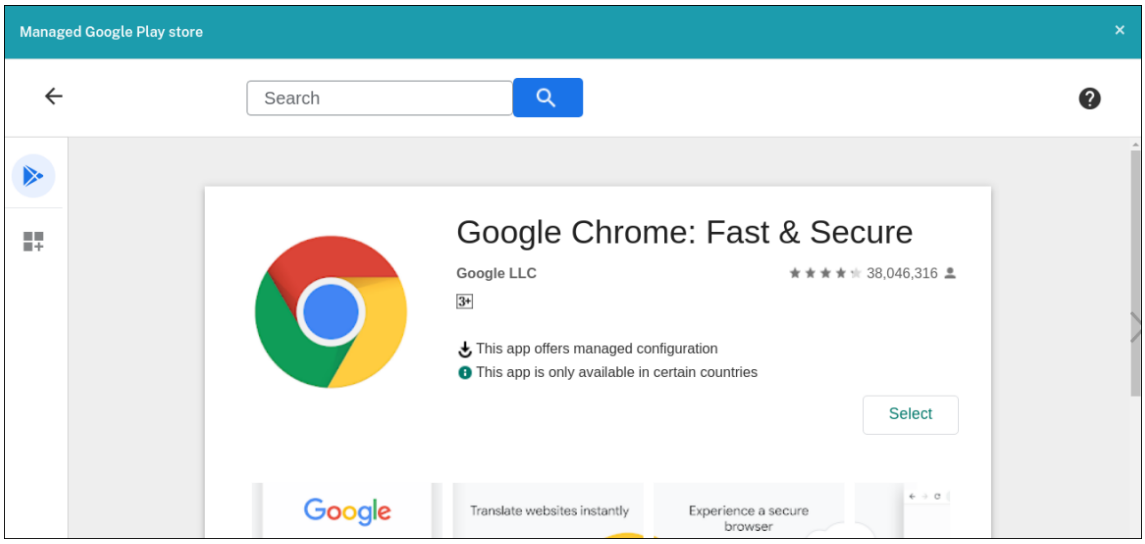
1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **Öffentlicher App-Store**.



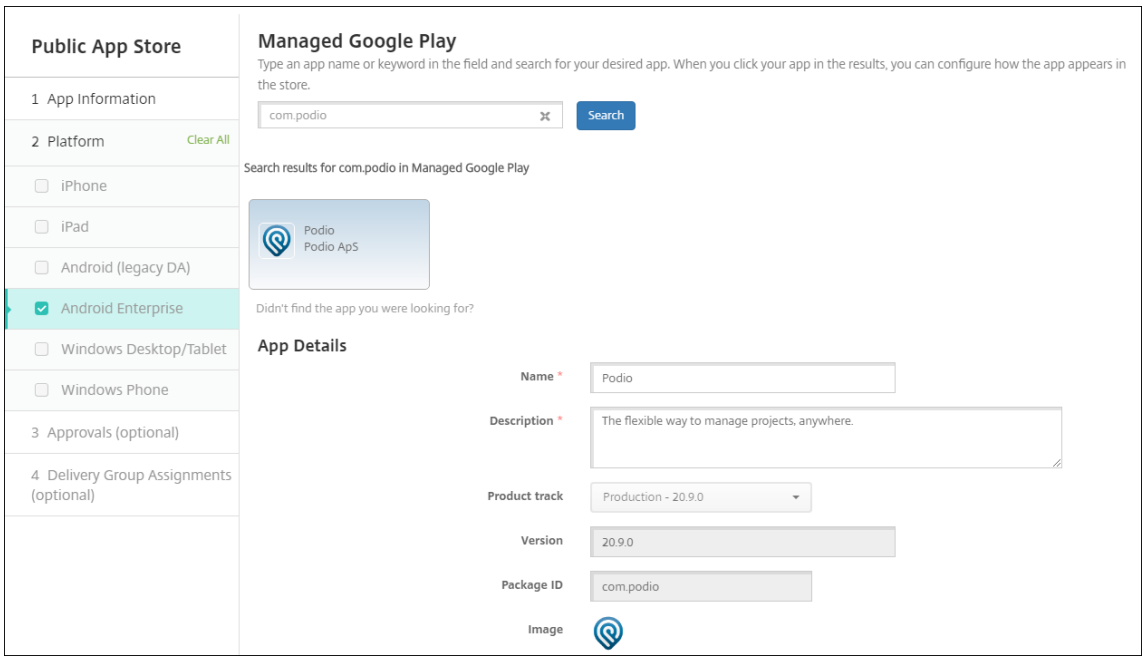
3. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** angezeigt.

- **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.

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 **Auswählen**.



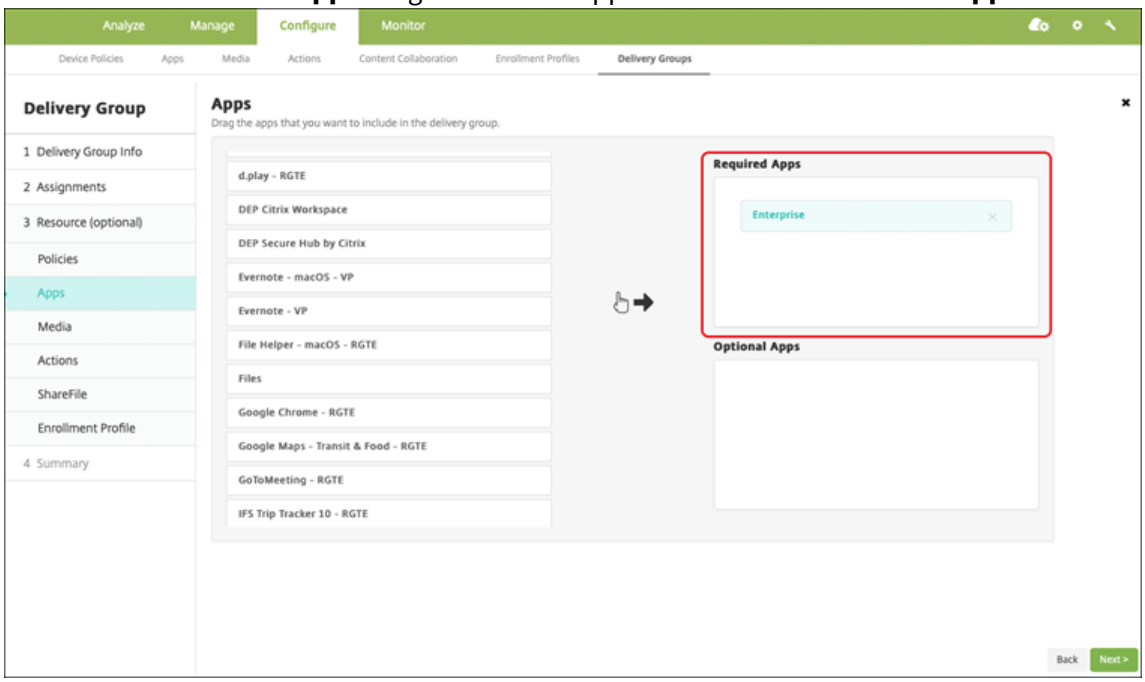
7. Klicken Sie erneut auf **Auswählen**.
8. Klicken Sie auf das App-Symbol und konfigurieren Sie **Name** und **Beschreibung** der App.



9. Weisen Sie der App beliebige Bereitstellungsgruppen zu und klicken Sie auf **Speichern**. Informationen finden Sie unter Ressourcen bereitstellen.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen** und wählen Sie die von Ihnen konfigurierte Bereitstellungsgruppe aus. Klicken Sie auf **Bearbeiten**.
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 zu Citrix Endpoint Management 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:

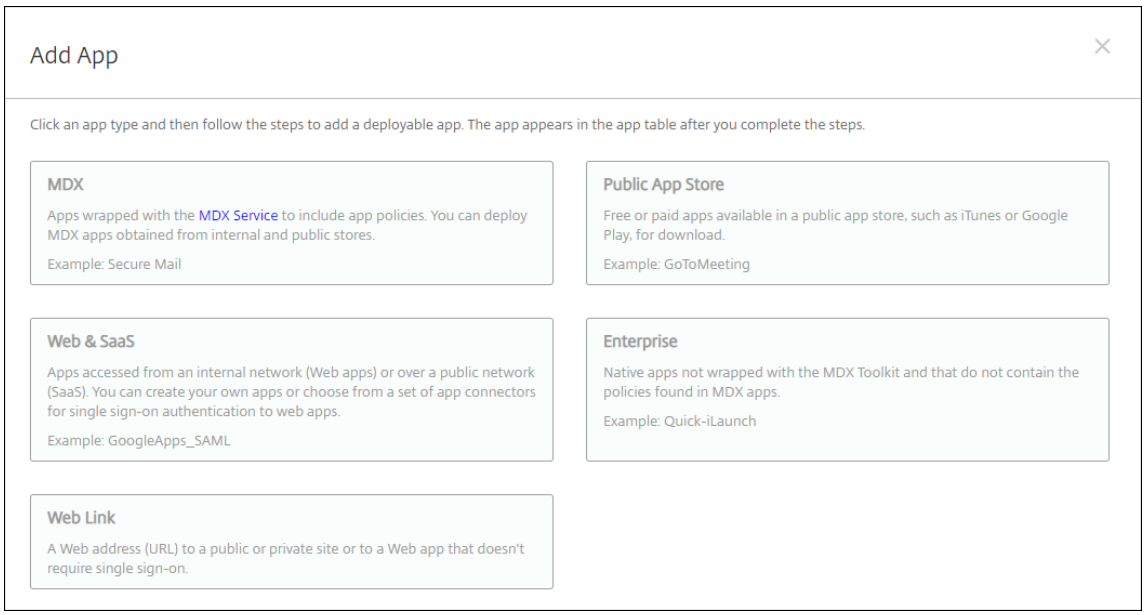
- Überblick über das MAM-SDK
- MDX-Richtlinien auf einen Blick

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 Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

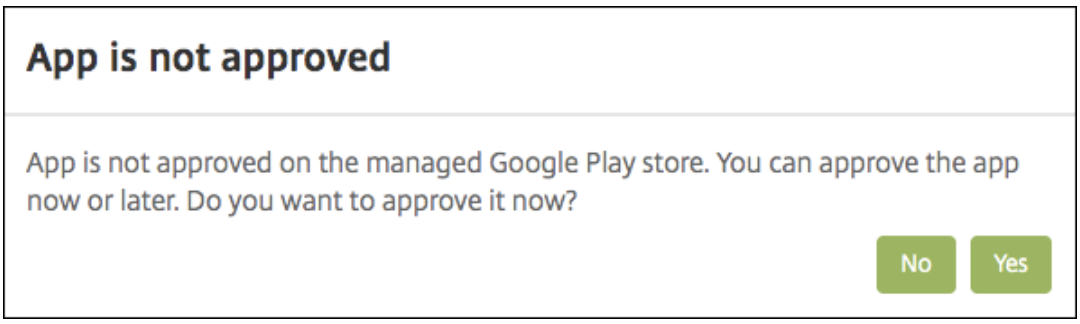


3. Klicken Sie auf **MDX**. Die Seite **App-Informationen** für MDX wird angezeigt. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:

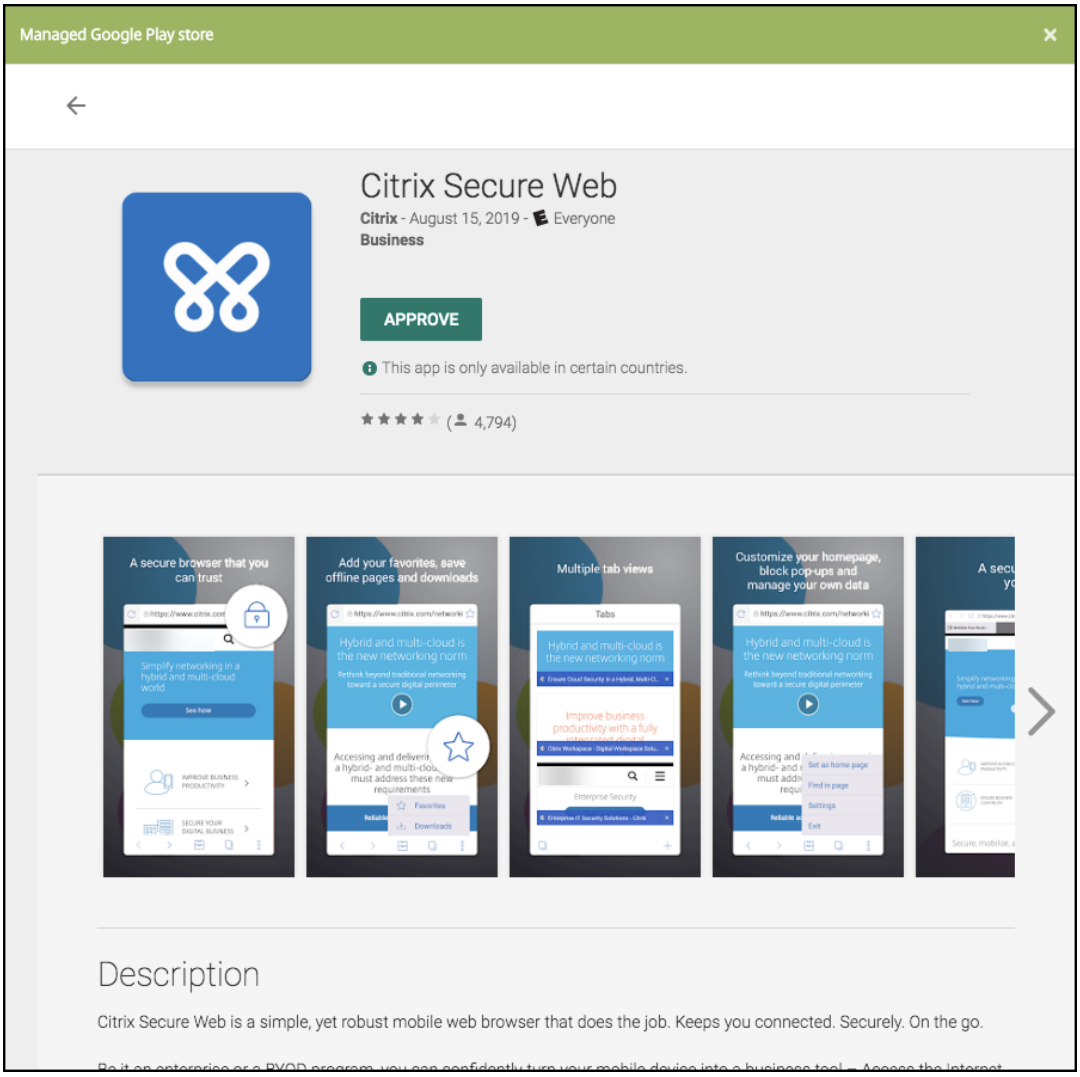
- **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** angezeigt.
- **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.

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-Stores erfordert. Klicken Sie auf **Ja**, um die Anwendung zu genehmigen, ohne die Citrix Endpoint Management-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 aus dem verwalteten Google Play Store ein.
   - **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

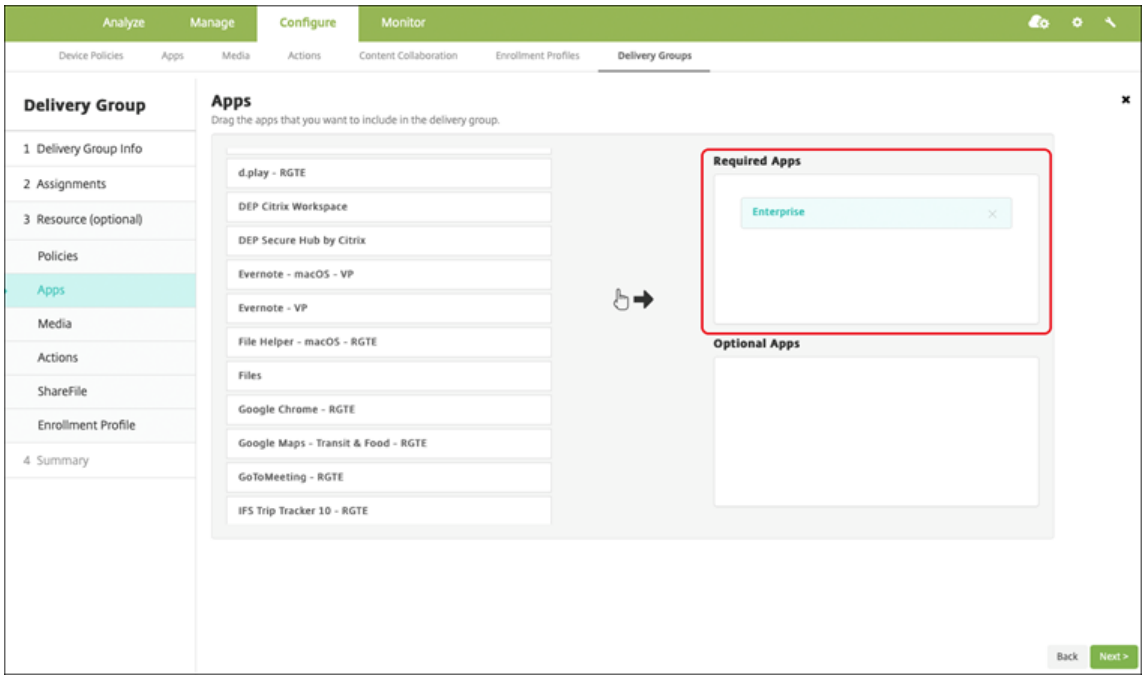
bieten Optionen für Richtlinienbereiche wie Authentifizierung, Gerätesicherheit und App-Einschränkungen. In der Konsole kann eine QuickInfo mit einer Beschreibung der Richtlinien angezeigt werden. Informationen über die für die einzelnen Geräteplattformen verfügbaren App-Richtlinien finden Sie hier:

- 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 Ressourcen bereitstellen.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen** und wählen Sie die von Ihnen konfigurierte Bereitstellungsgruppe aus. Klicken Sie auf **Bearbeiten**.
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.

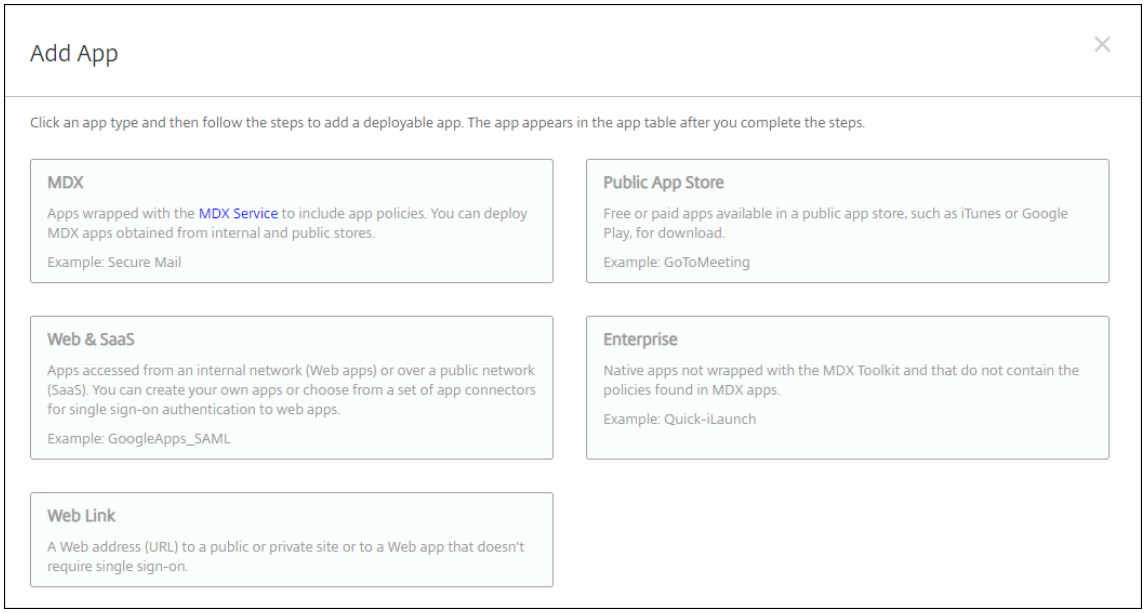
Sehen Sie sich dieses Video an, um mehr zu erfahren:

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 Citrix Endpoint Management-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 Citrix Endpoint Management-Konsole als Unternehmensapp hinzu. Führen Sie hierfür die folgenden Schritte aus:

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

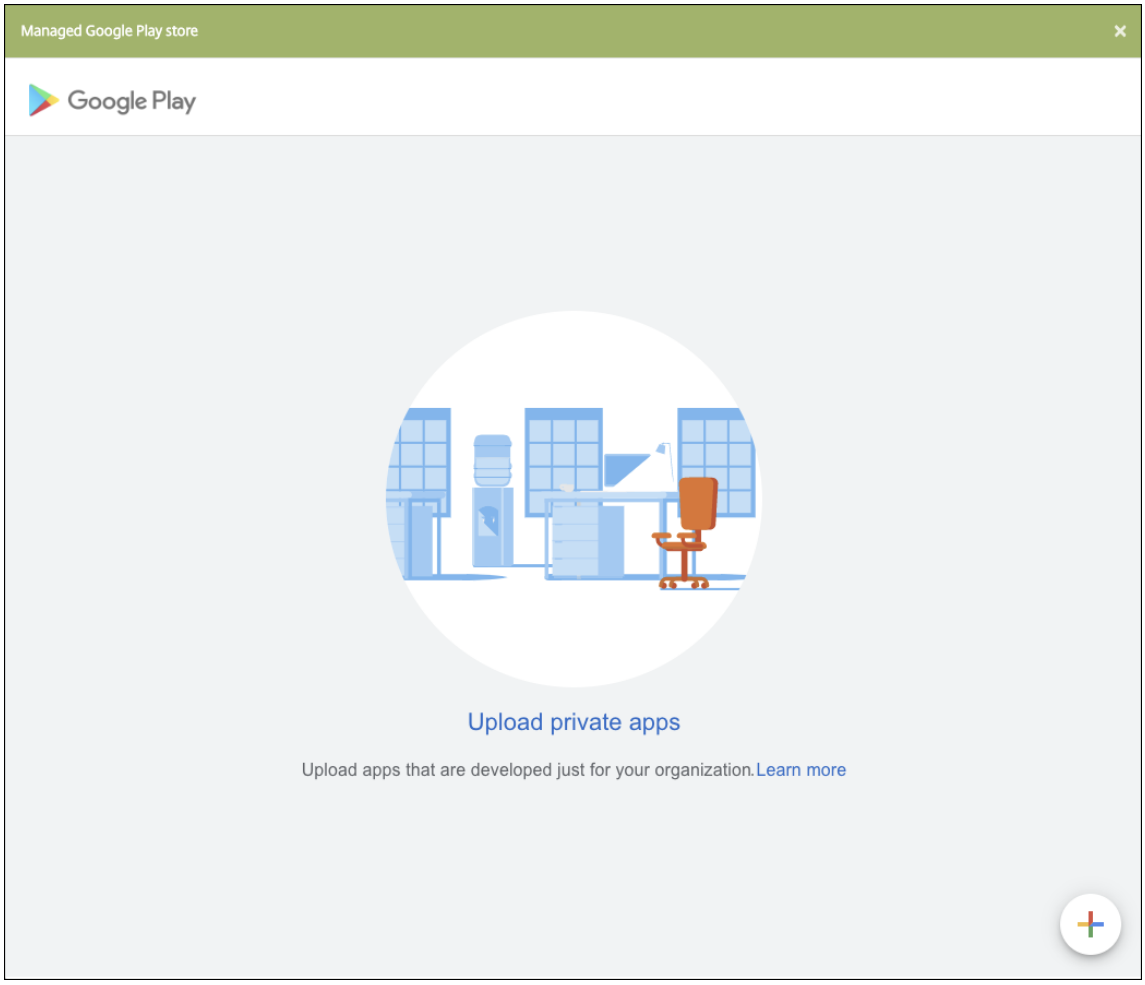


2. Klicken Sie auf **Enterprise**. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:

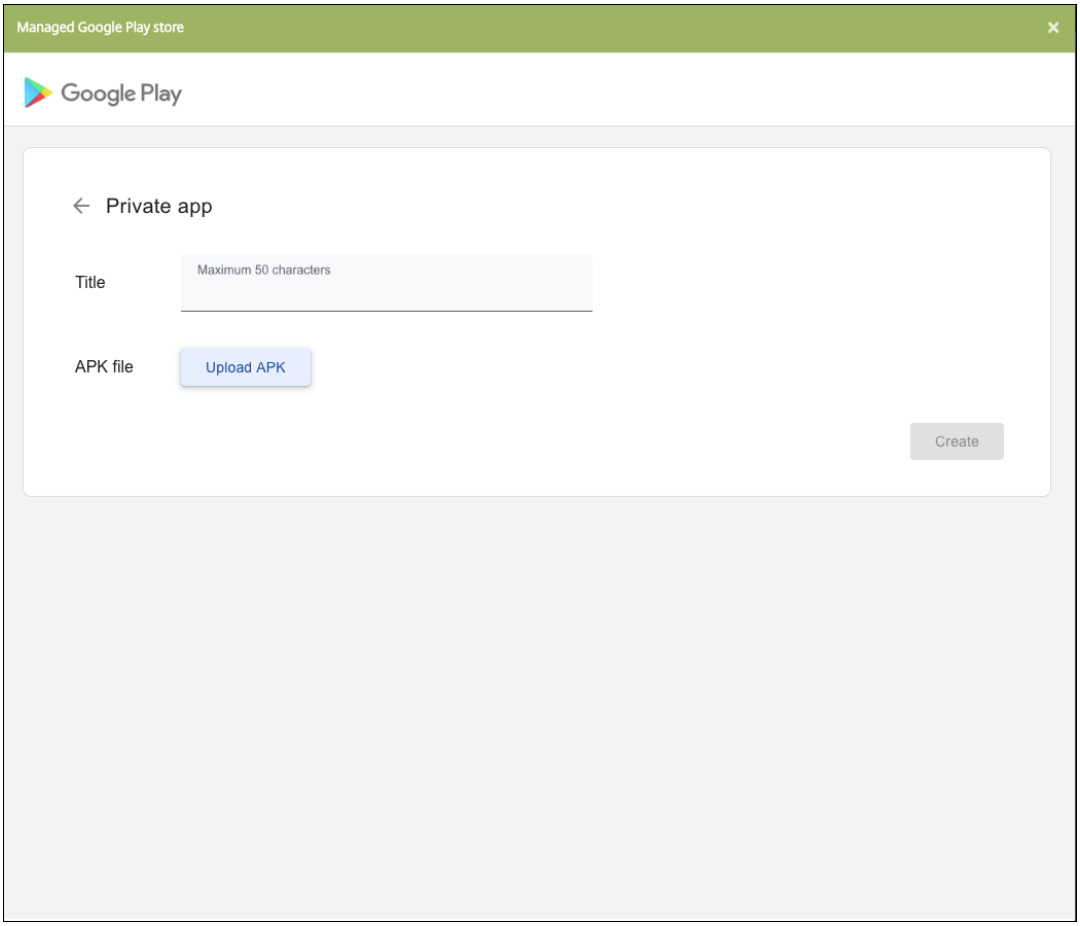
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name”in der Tabelle “Apps”angezeigt.
   - **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.

3. Wählen Sie als Plattform **Android Enterprise**.

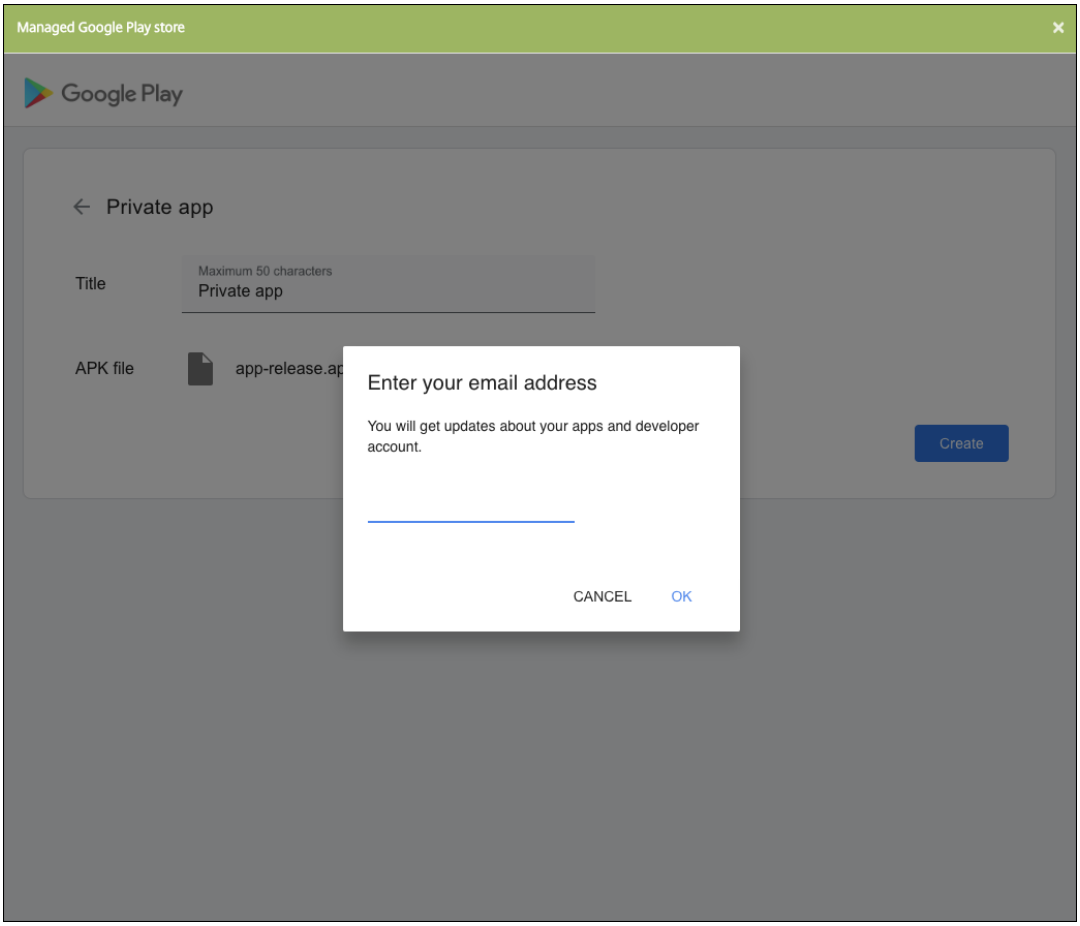
4. Die Schaltfläche **Upload** öffnet den verwalteten Google Play Store. Sie müssen sich nicht für ein Entwicklerkonto registrieren, um eine private App zu veröffentlichen. Klicken Sie auf das **Plus-Symbol** in der unteren rechten Ecke, um fortzufahren.



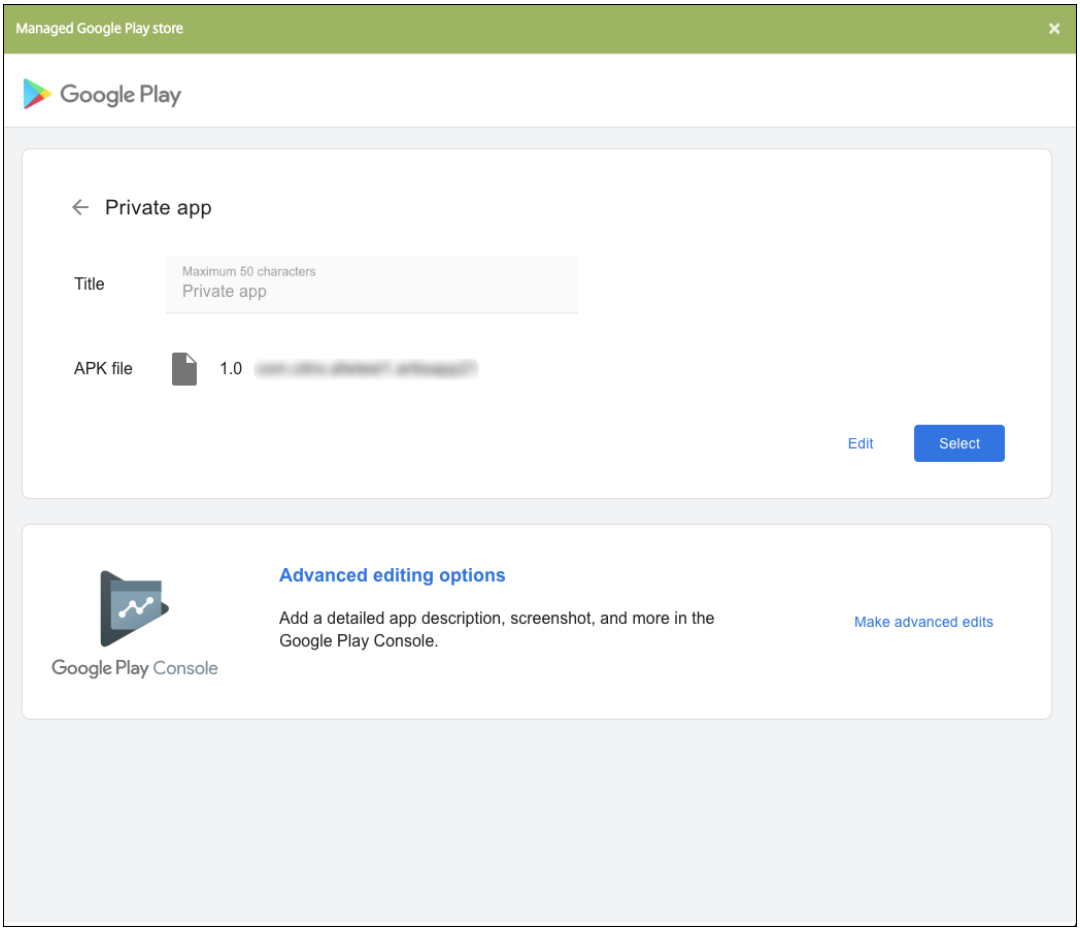
a) Geben Sie den Namen für Ihre App ein und laden Sie die APK-Datei hoch. Wenn Sie fertig sind, klicken Sie auf **Erstellen**. Es kann bis zu 10 Minuten dauern, bis Ihre private App veröffentlicht wird.



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.



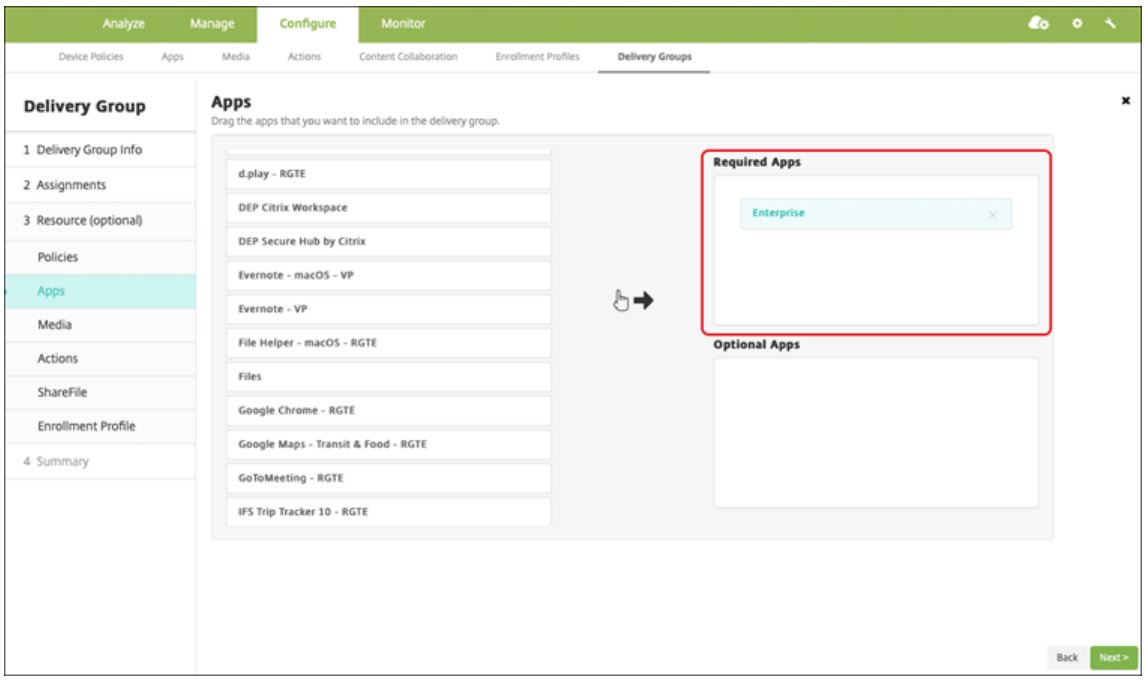
5. Klicken Sie auf **Weiter**. Die Seite mit den App-Informationen für die Plattform wird angezeigt.
6. Konfigurieren Sie die Einstellungen für die Plattform, z. B.:

   - **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 Ressourcen bereitstellen.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen** und wählen Sie die von Ihnen konfigurierte Bereitstellungsgruppe aus. Klicken Sie auf **Bearbeiten**.
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 Citrix Endpoint Management-Konsole hinzu.
    - Hosten und veröffentlichen Sie die Apps im verwalteten Google Play Store.
    - Fügen Sie die App der Citrix Endpoint Management-Konsole als Unternehmensapp hinzu.
3. Fügen Sie die MDX-Datei zu Citrix Endpoint Management 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 Citrix Endpoint Management finden Sie in den folgenden Abschnitten.

Vorbereiten einer Android Enterprise-App

Wenn Sie eine Android Enterprise-App erstellen, beachten Sie die Hinweise von Google unter Best practices for private apps.

Nachdem Sie eine 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 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-->
```

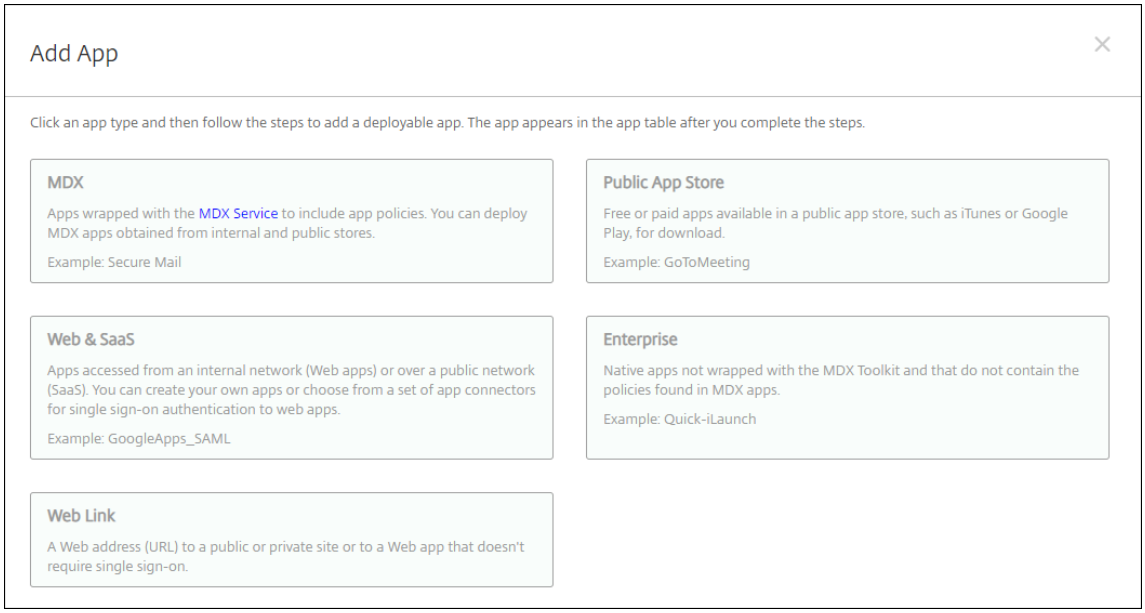
3. Umschließen Sie die App mit dem MDX Toolkit. Informationen zur Verwendung des MDX Toolkits finden Sie unter Umschließen von mobilen Android-Apps.

   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 Citrix Endpoint Management-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 Citrix Endpoint Management-Konsole als Unternehmensapp hinzu. Führen Sie hierfür die folgenden Schritte aus:

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps**. Die Seite **Apps** wird geöffnet.
2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

 
```

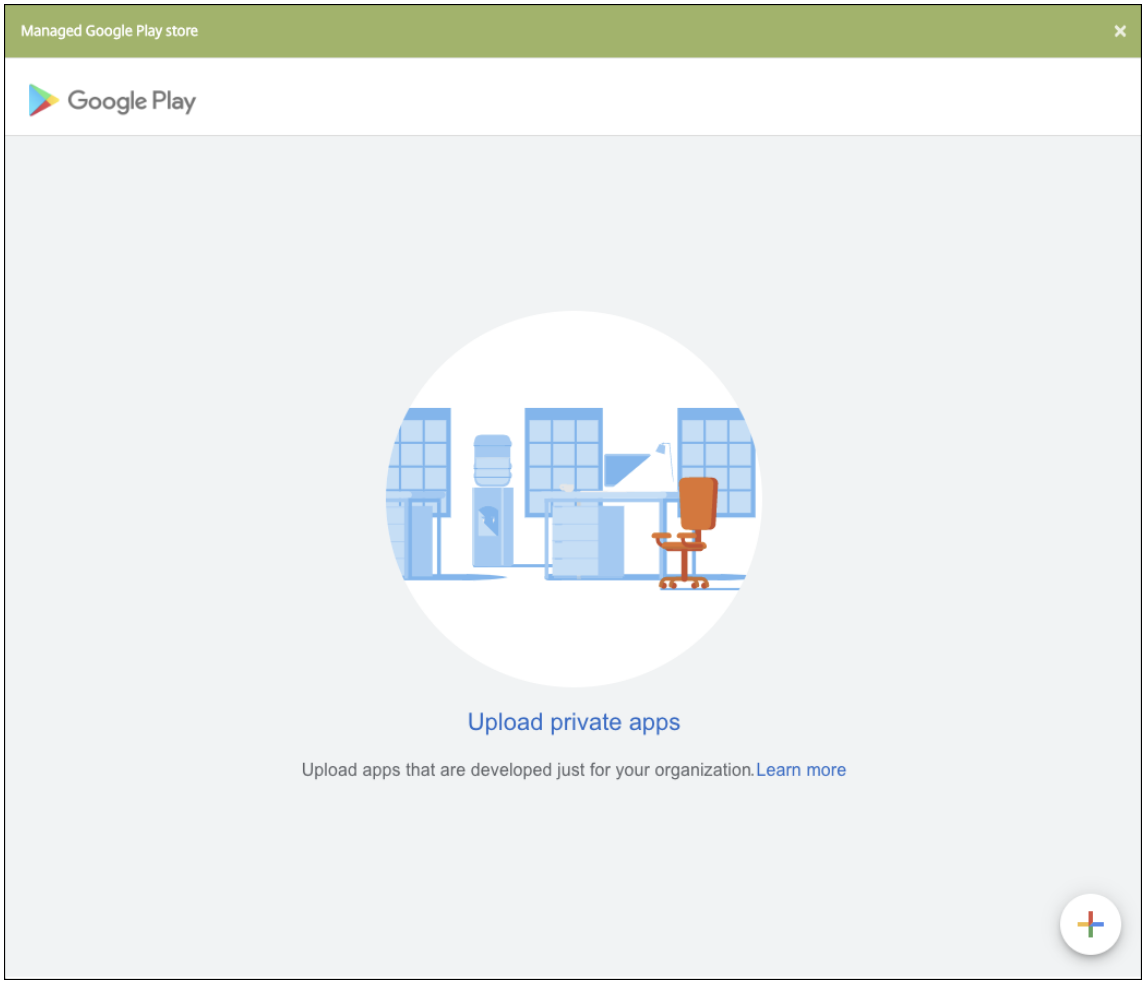


3. Klicken Sie auf **Enterprise**. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:

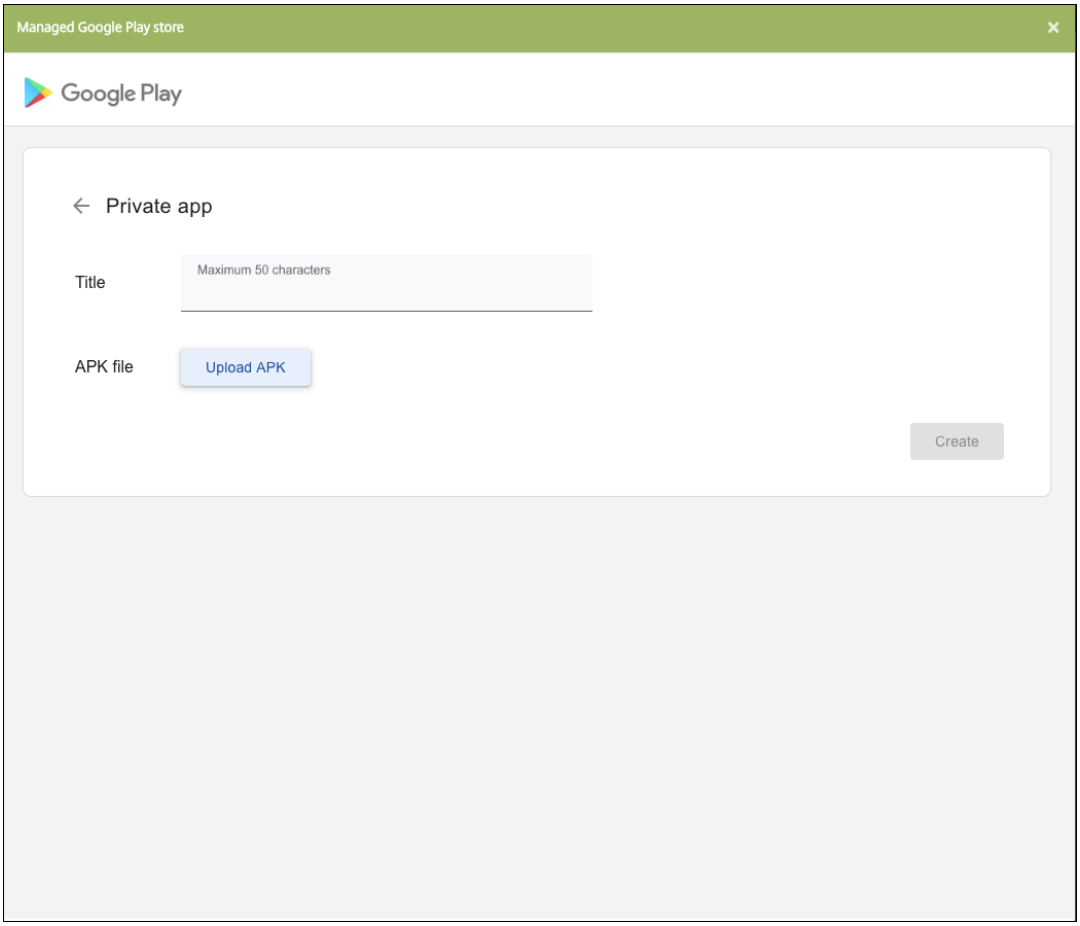
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name”in der Tabelle “Apps”angezeigt.
   - **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.

4. Wählen Sie als Plattform **Android Enterprise**.

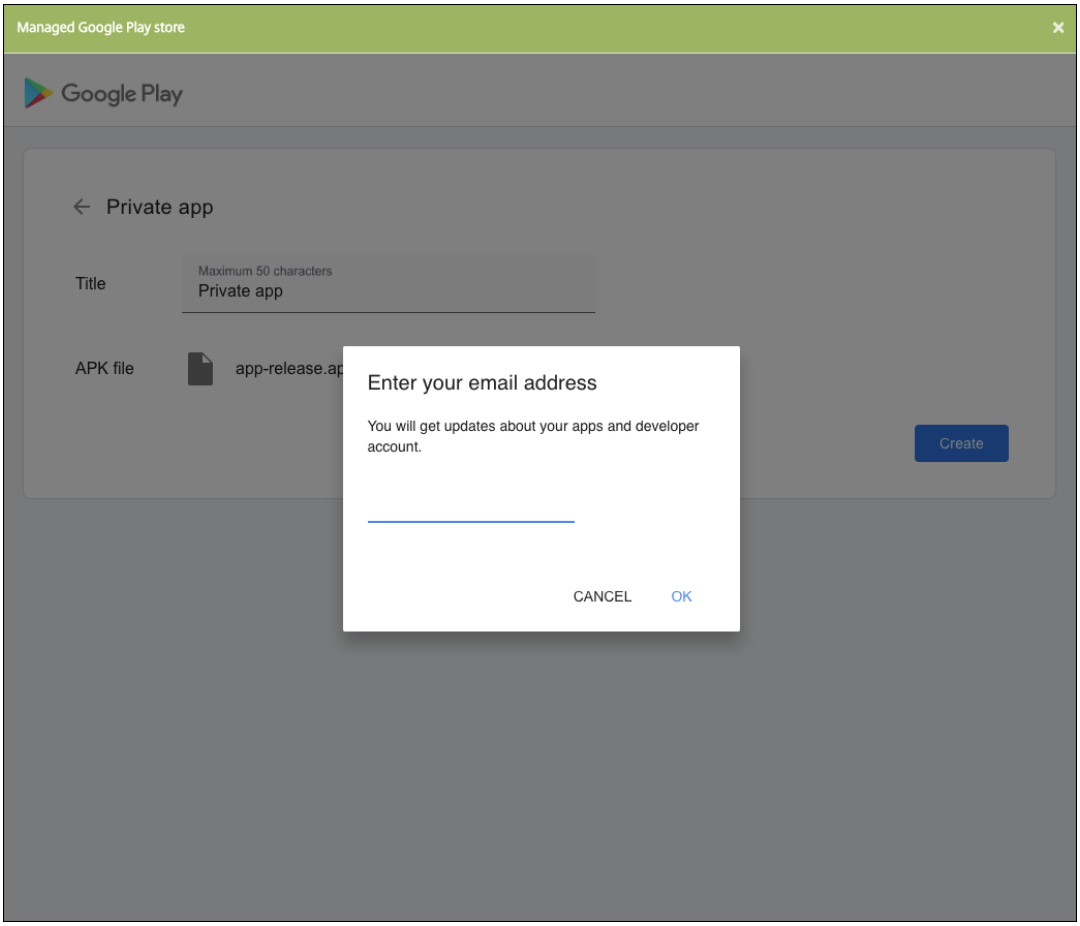
5. Die Schaltfläche **Upload** öffnet den verwalteten Google Play Store. Sie müssen sich nicht für ein Entwicklerkonto registrieren, um eine private App zu veröffentlichen. Klicken Sie auf das **Plus-Symbol** in der unteren rechten Ecke, um fortzufahren.



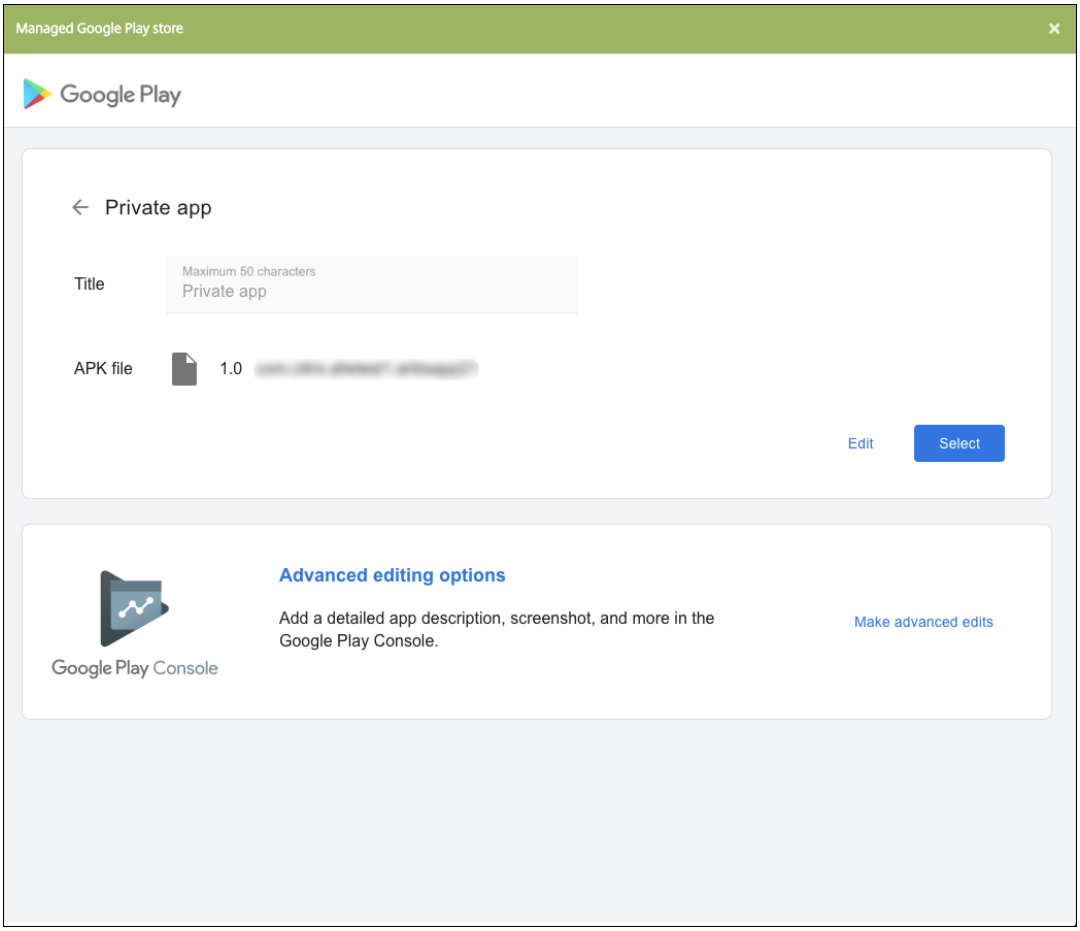
a) Geben Sie den Namen für Ihre App ein und laden Sie die APK-Datei hoch. Wenn Sie fertig sind, klicken Sie auf **Erstellen**. Es kann bis zu 10 Minuten dauern, bis Ihre private App veröffentlicht wird.



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:**Eindeutiger Bezeichner 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 **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

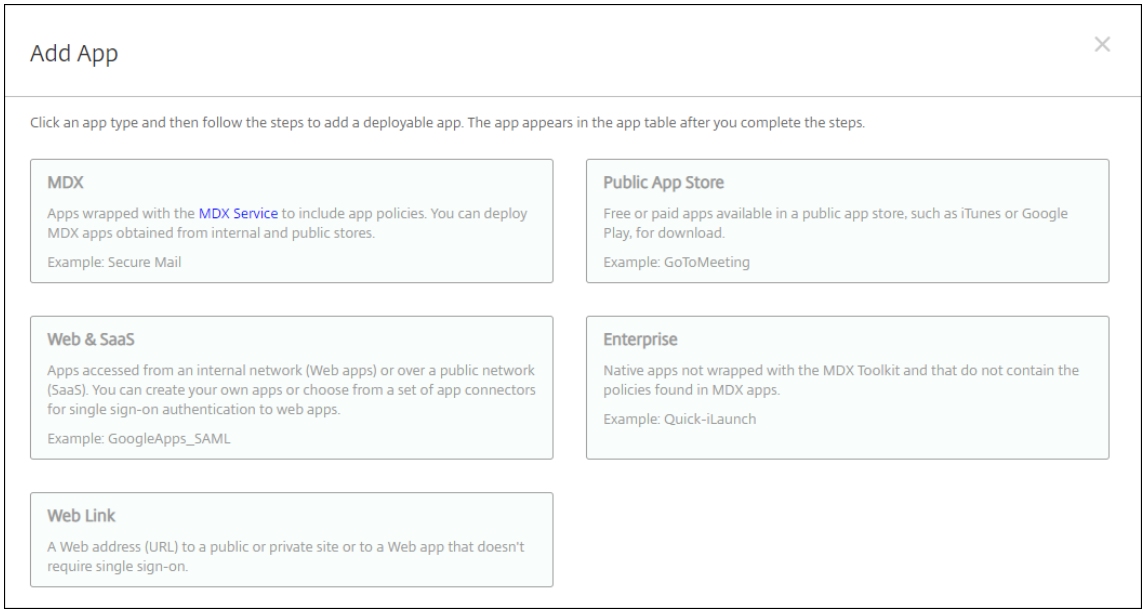
Wenn Sie die Store-URL beim Umschließen der App nicht kennen, fügen Sie sie jetzt hinzu.

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 Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.



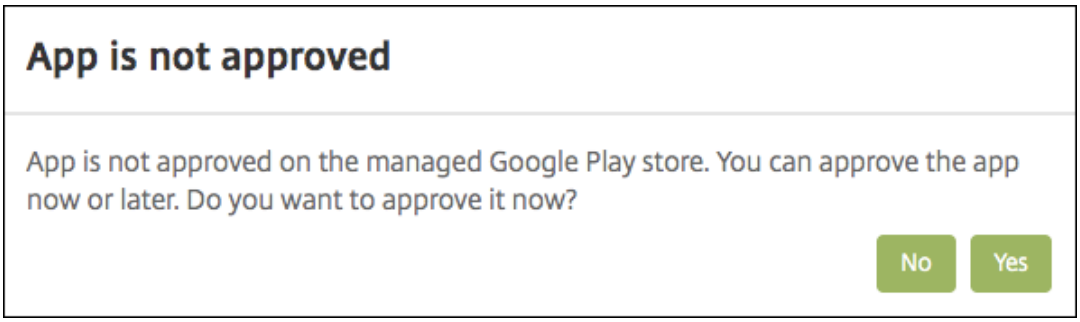
2. Klicken Sie auf **MDX**. Die Seite **App-Informationen** für MDX wird angezeigt. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:

   - **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.

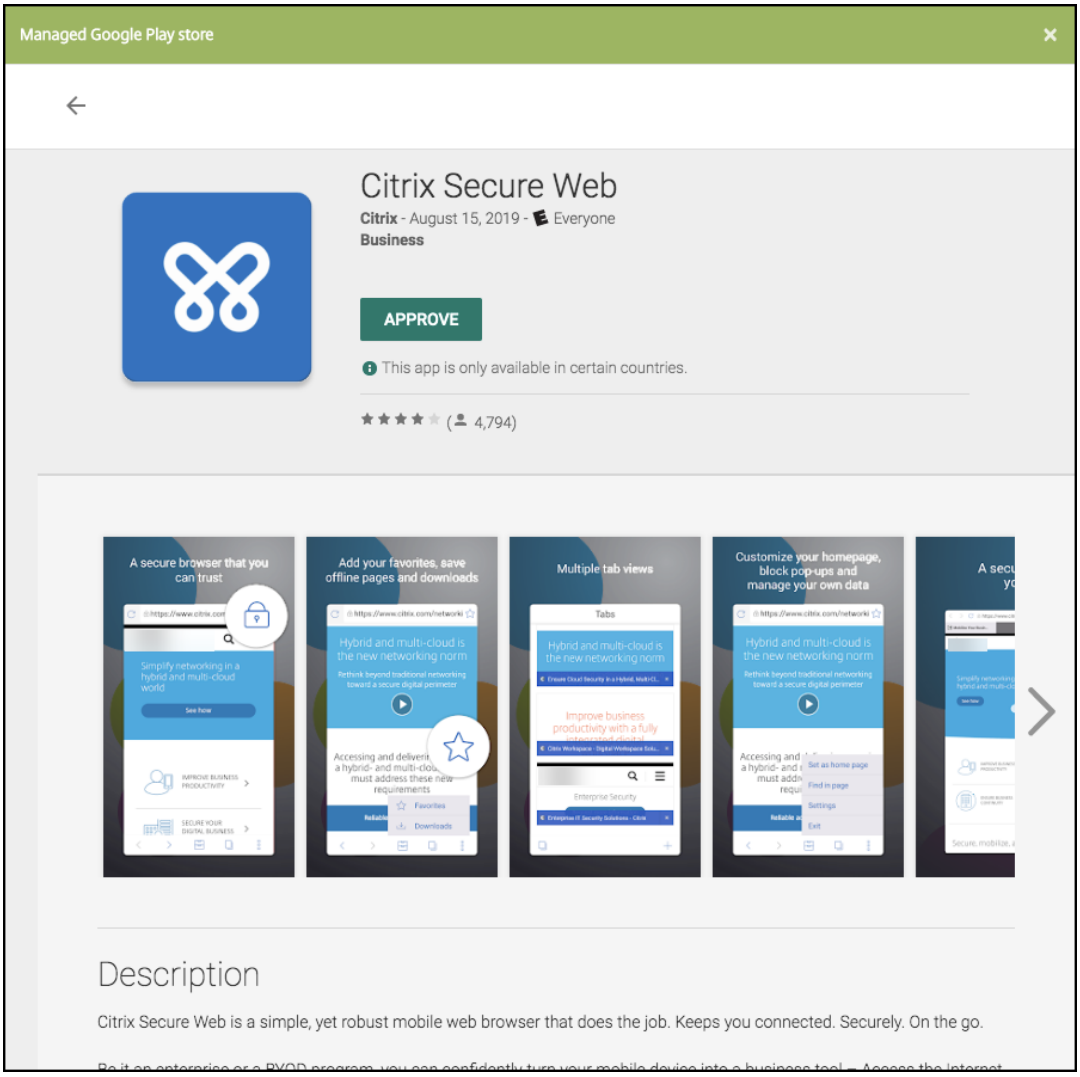
3. Wählen Sie als Plattform **Android Enterprise**.

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-Stores erfordert. Klicken Sie auf **Ja**, um die Anwendung zu genehmigen, ohne die Citrix Endpoint Management-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 aus dem verwalteten Google Play Store ein.
   - **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 iOS-Geräte
   - Ist nicht verfügbar für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version ab 10.18.19 verwenden
   - Wird nicht empfohlen für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version vor 10.18.19 verwenden

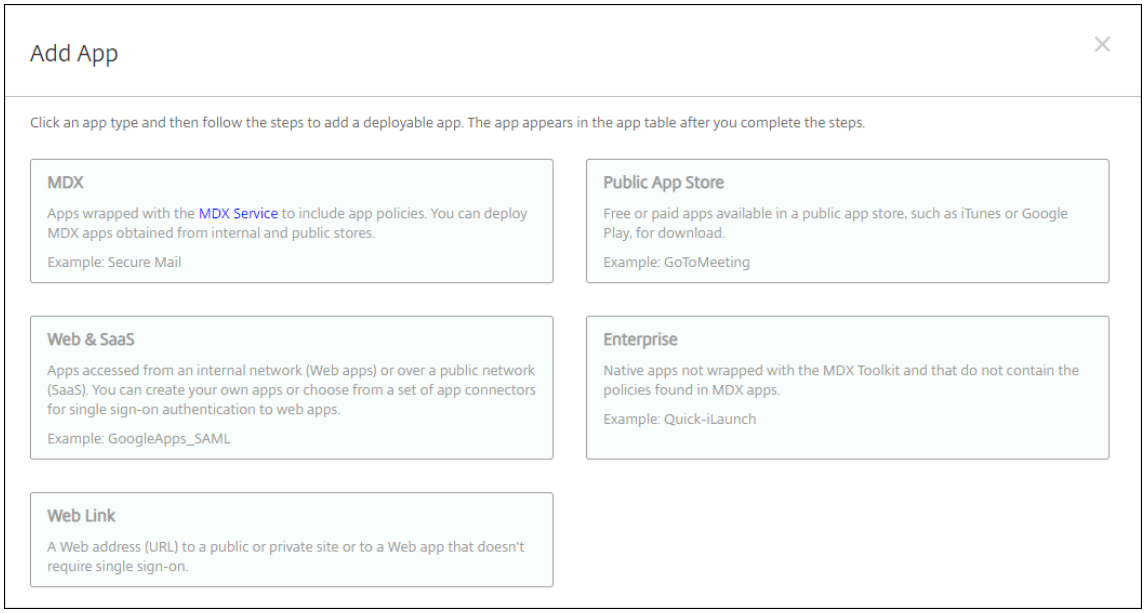
   Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.

8. Weisen Sie der App beliebige Bereitstellungsgruppen zu und klicken Sie auf **Speichern**. Informationen finden Sie unter Ressourcen bereitstellen.

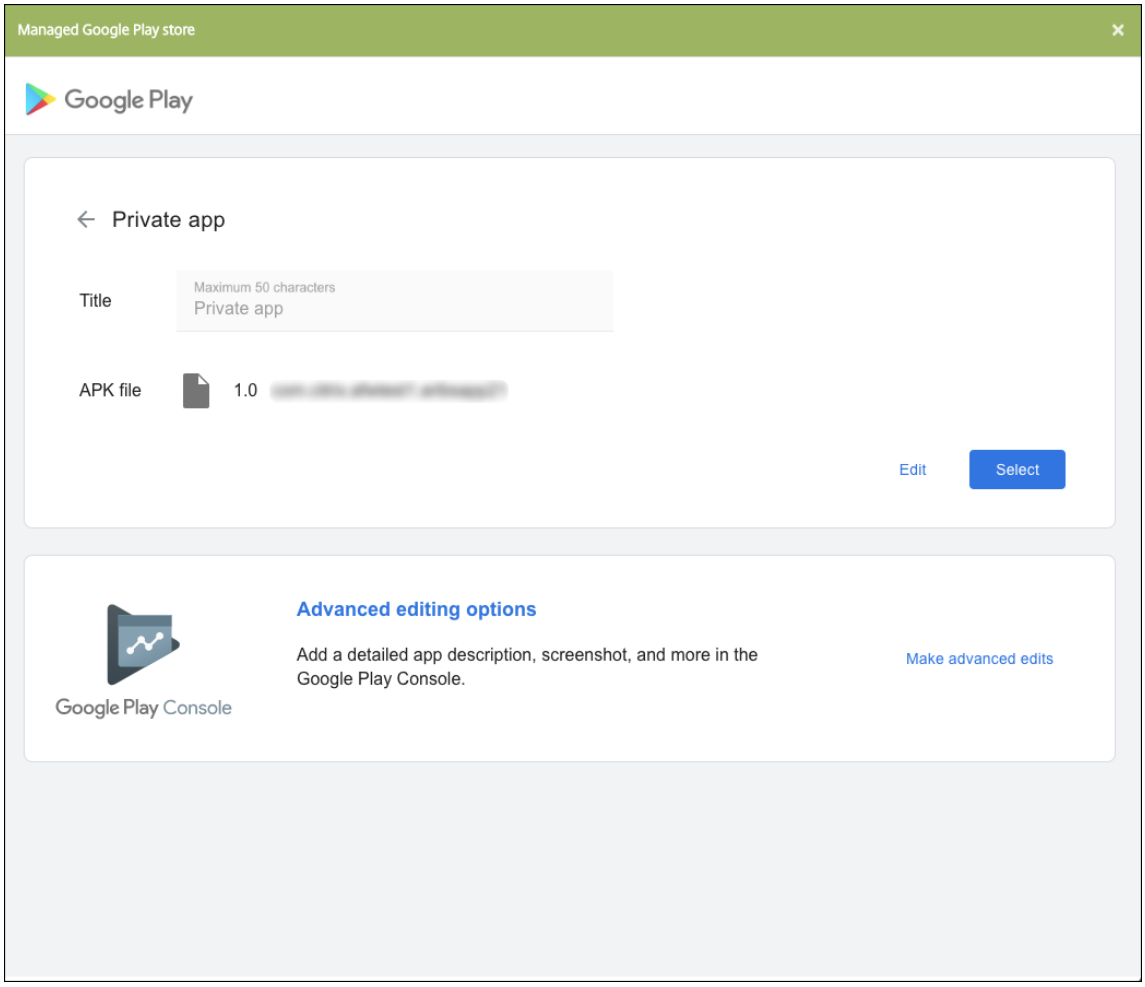
Aktualisieren der App

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 Citrix Endpoint Management-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.
5. Wählen Sie als Plattform **Android Enterprise**.
6. Klicken Sie auf **Weiter**. Die Seite **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)

June 25, 2024

Kunden mit Google Workspace müssen die Legacy Android Enterprise-Einstellungen zum Konfigurieren von Legacy Android Enterprise verwenden. G Suite wurde von Google in Google Workspace umbenannt.

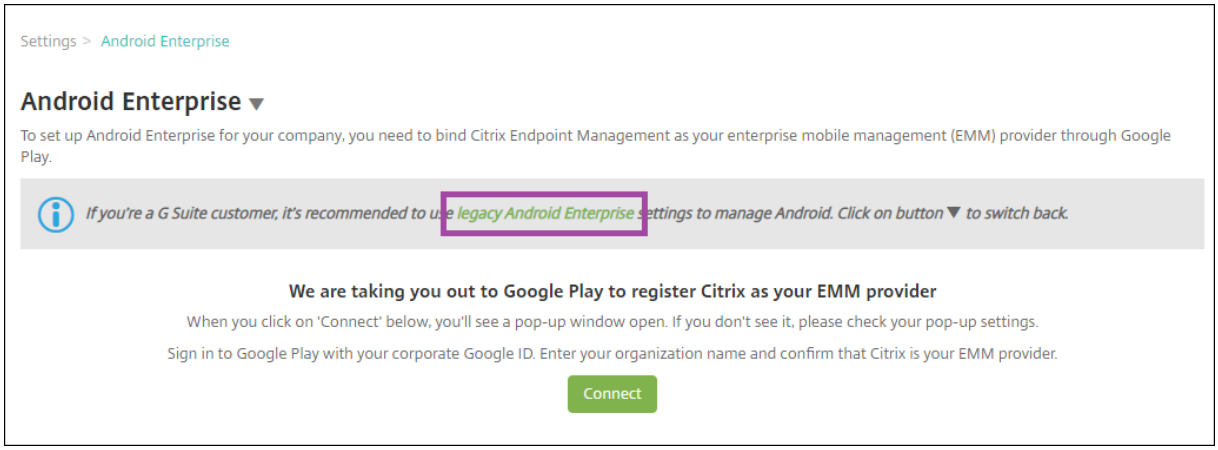
Wenn Ihre Organisation bereits Google Workspace verwendet, um Benutzern Zugriff auf Google-Apps zu ermöglichen, können Sie mit Google Workspace Citrix als EMM registrieren. Wenn Ihre Organisation Google Workspace verwendet, besitzt sie eine Unternehmens-ID und Google-Konten für

Benutzer. Um Citrix Endpoint Management mit Google Workspace zu verwenden, führen Sie eine Synchronisierung mit Ihrem LDAP-Verzeichnis durch und rufen Google-Kontoinformationen über die Google Directory-API ab. Da dieser Unternehmenstyp an eine vorhandene Domäne gebunden ist, kann jede Domäne nur ein Unternehmen erstellen. Um ein Gerät bei Citrix Endpoint Management zu registrieren, muss sich jeder Benutzer manuell mit dem vorhandenen Google-Konto anmelden. Über dieses Konto können sie auf verwaltetes Google Play zugreifen und die übrigen Google-Dienste nutzen, die von Ihrem Google Workspace-Plan bereitgestellt werden.

Anforderungen für Legacy Android Enterprise:

- Öffentlich zugängliche Domäne
- Google-Administratorkonto
- Android-Geräte mit Unterstützung für verwaltete Profile
- Ein Google-Konto, für das Google Play installiert wurde
- Arbeitsprofil auf den Geräten eingerichtet

To start configuring the legacy Android Enterprise, click **legacy Android Enterprise** in the **Android Enterprise** page in Citrix Endpoint Management Settings.



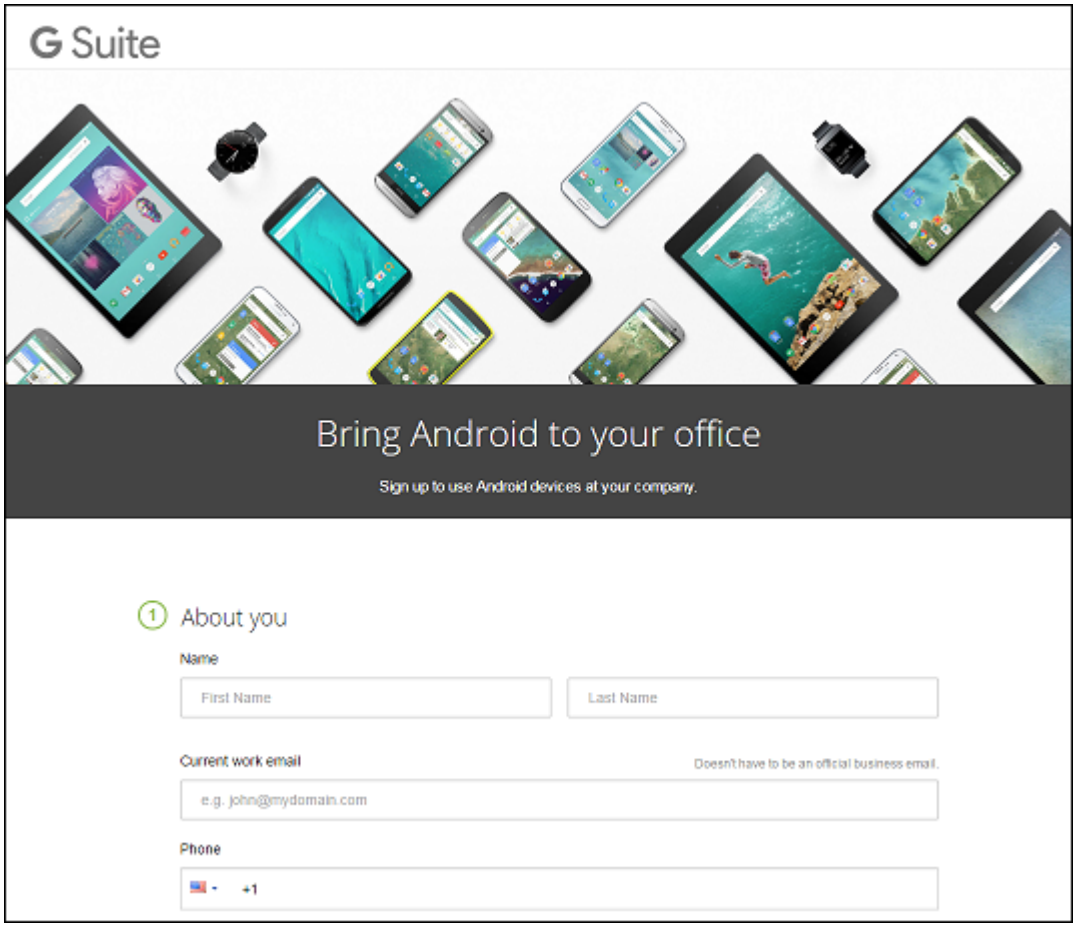
Erstellen eines Android Enterprise-Kontos

Bevor Sie ein Android Enterprise-Konto einrichten können, müssen Sie Ihren Domainnamen bei Google bestätigen.

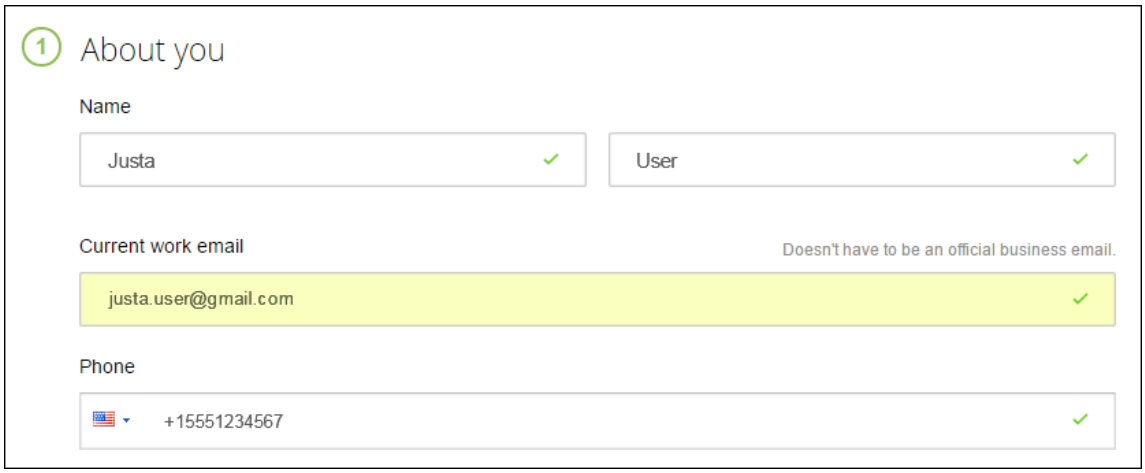
Wenn Ihr Domänenname bei Google bereits verifiziert wurde, können Sie mit dem Schritt Einrichten eines Android Enterprise-Dienstkontos und Download eines Android Enterprise-Zertifikats fortfahren.

1. Navigieren Sie zu https://gsuite.google.com/signup/basic/welcome.

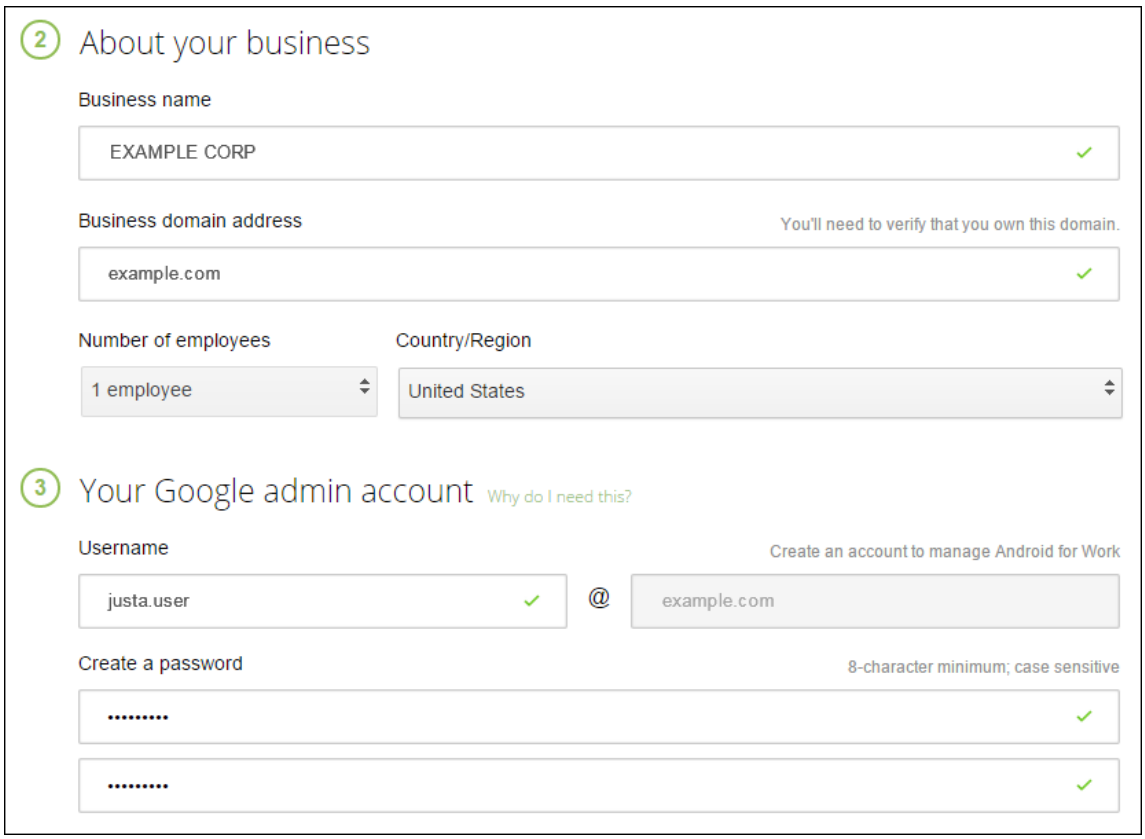
   Auf der nachfolgend gezeigten Seite geben Sie die Administrator- und Unternehmensinformationen ein.



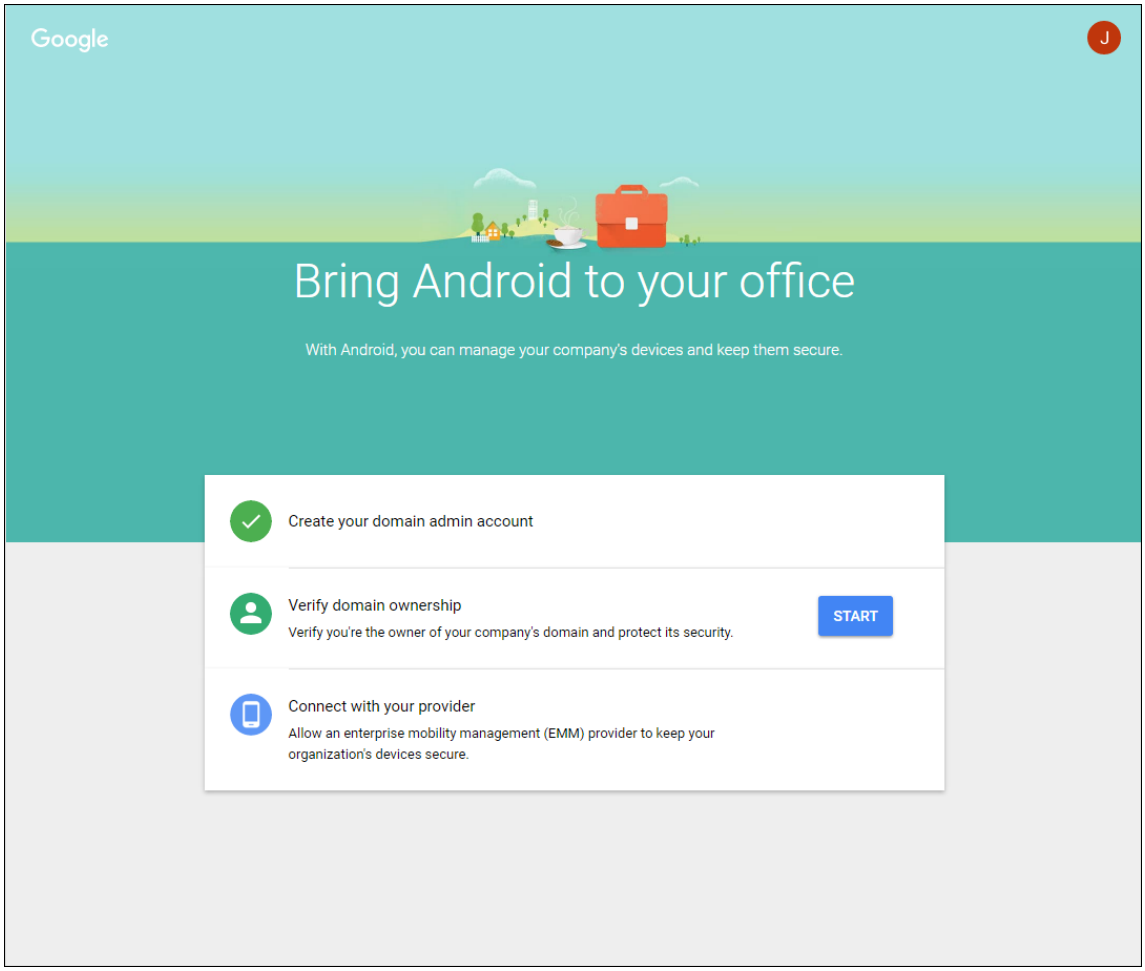
2. Geben Sie Ihre Administratorinformationen ein.



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

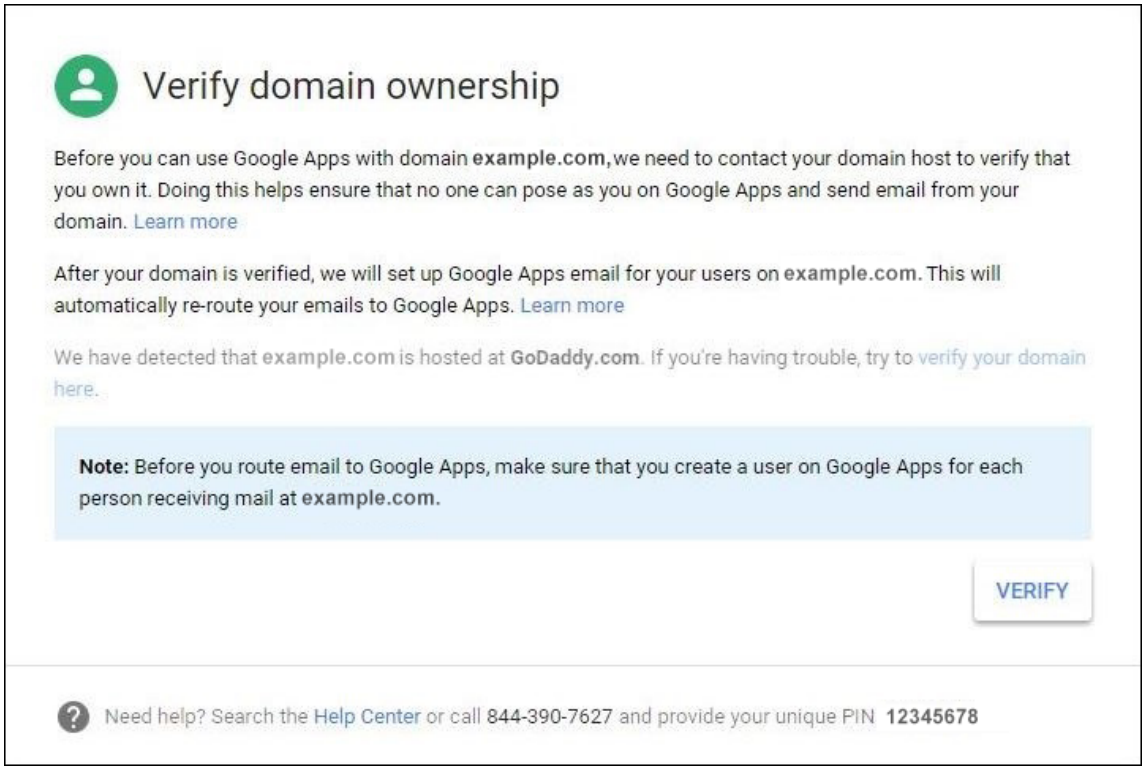
Zur Verifizierung Ihrer Domäne durch Google gibt es folgende Methoden:

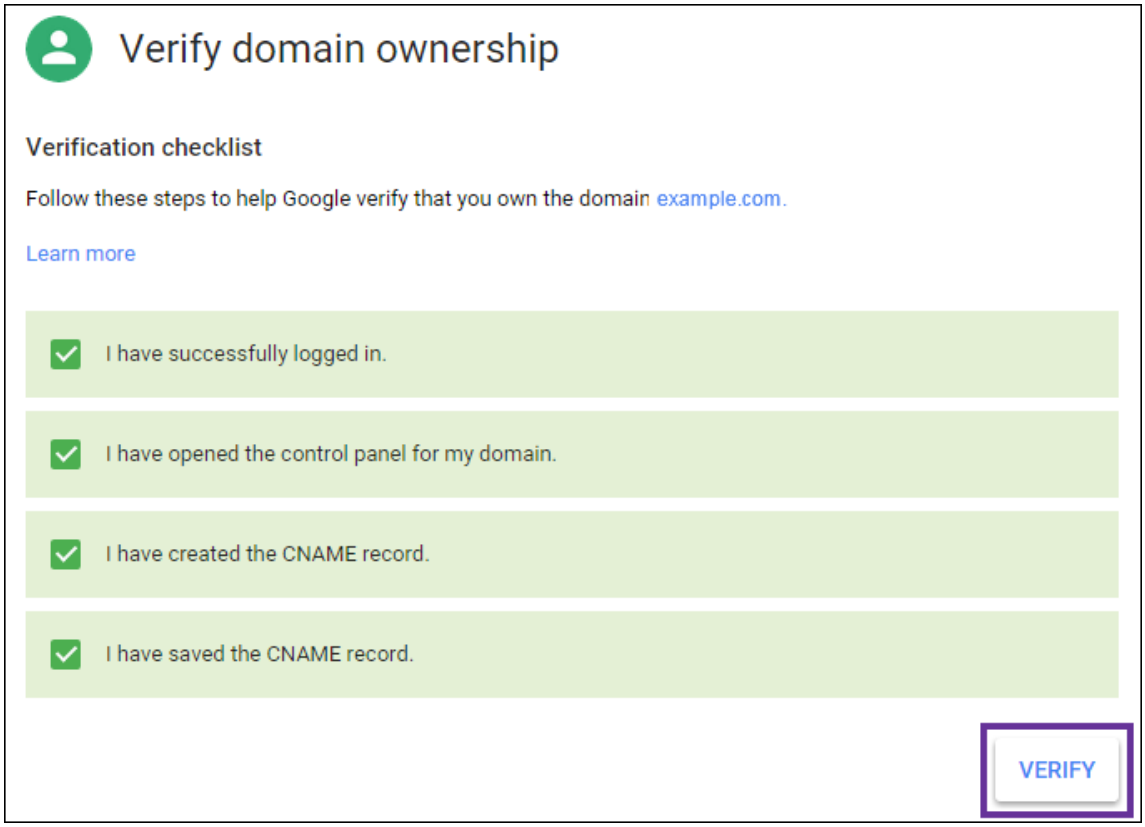
- Hinzufügen eines TXT- oder CNAME-Datensatzes zu der Website Ihres Domänenhosts.
- Hochladen einer HTML-Datei auf den Webserver Ihrer Domäne.
- Hinzufügen eines `<meta>`-Tags zu Ihrer Homepage. Google empfiehlt die Verwendung der ersten Methode. Die Schritte zum Überprüfen Ihrer Domäneneigentümerschaft 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.

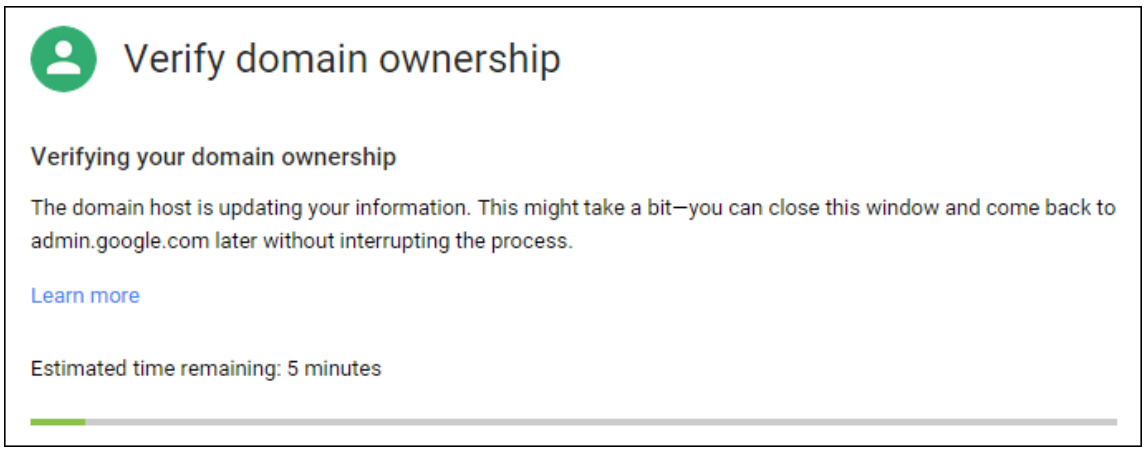
   Die Seite **Verify domain ownership** wird angezeigt. Folgen Sie den angezeigten Anweisungen zum Überprüfen Ihrer Domäne.

2. Klicken Sie auf **Verify**.

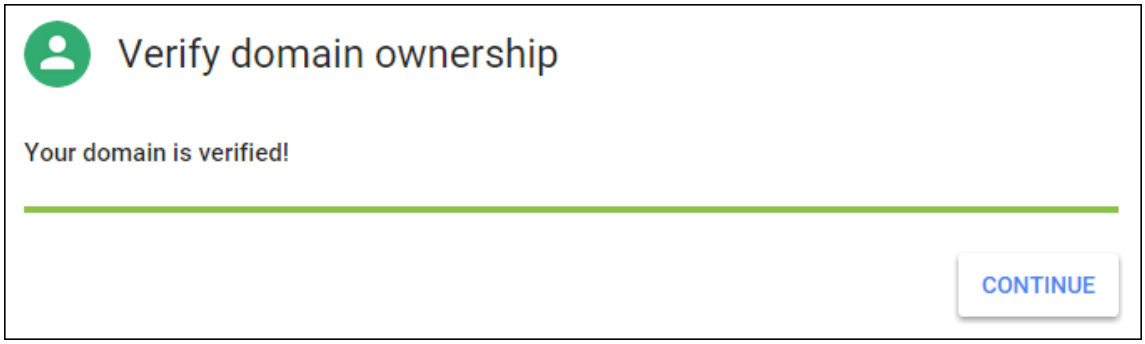




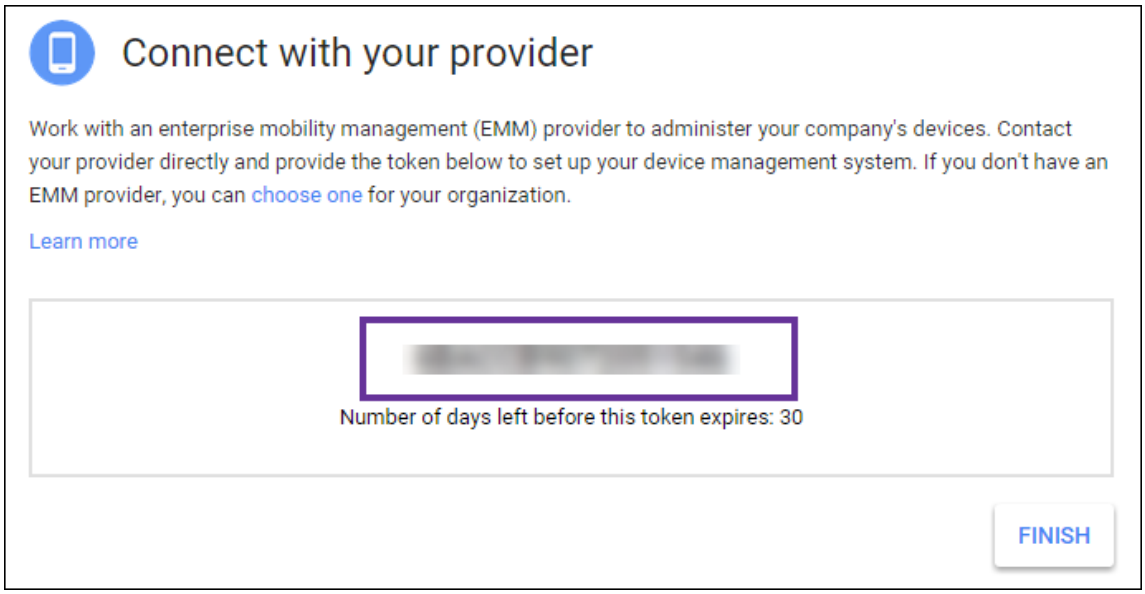
3. Google überprüft die Eigentümerschaft der Domäne.



4. Nach einer erfolgreichen Überprüfung wird die folgende Seite angezeigt. Klicken Sie auf **Continue**.



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

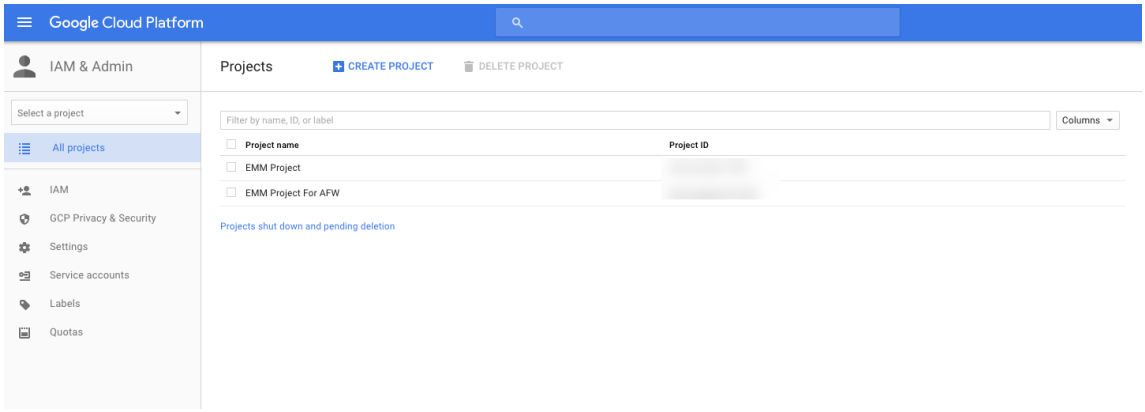
Seite mit der Meldung angezeigt, dass Ihre Domäne erfolgreich verifiziert wurde.

Nach dem Erstellen eines Android Enterprise-Dienstkontos können Sie sich bei der Google Admin-Konsole anmelden und die Einstellungen Ihrer Mobilitätsverwaltung festlegen.

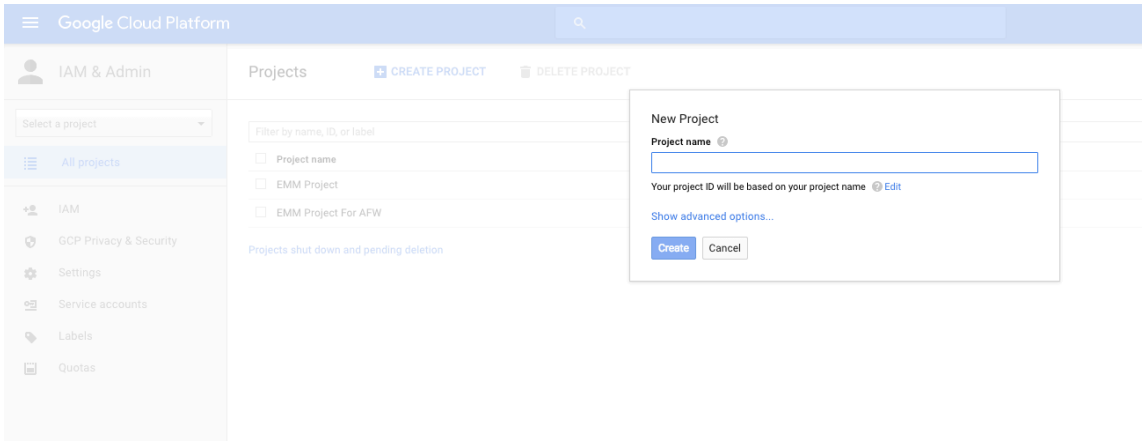
Einrichten eines Android Enterprise-Dienstkontos und Herunterladen eines Android Enterprise-Zertifikats

Damit Citrix Endpoint Management 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 Citrix Endpoint Management und den Google-Diensten für Android verwendet. Weitere Informationen zum verwendeten Authentifizierungsprotokoll finden Sie unter https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

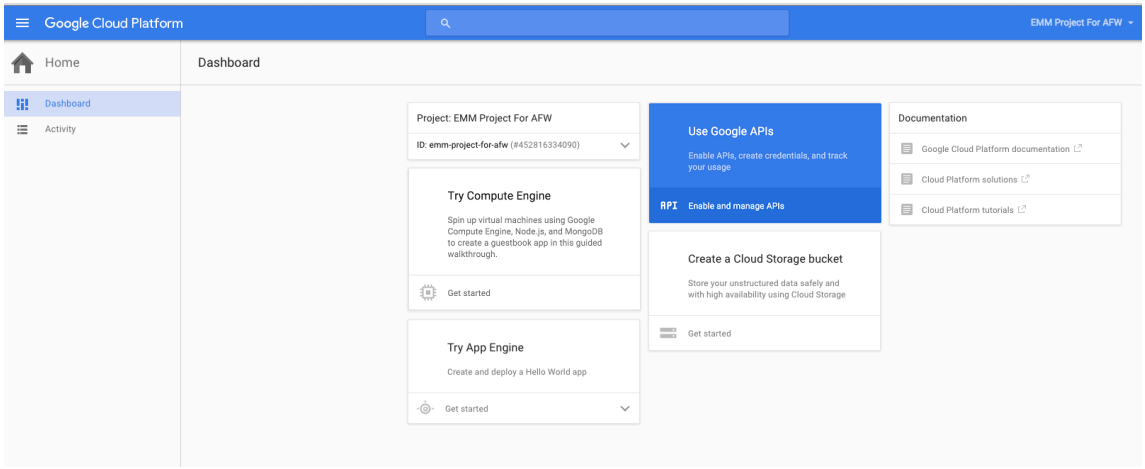
1. Rufen Sie in einem Webbrowser https://console.cloud.google.com/project auf und melden Sie sich mit Ihren Anmeldeinformationen als Google-Administrator an.
2. Klicken Sie in der Liste **Projects** auf **Create project**.



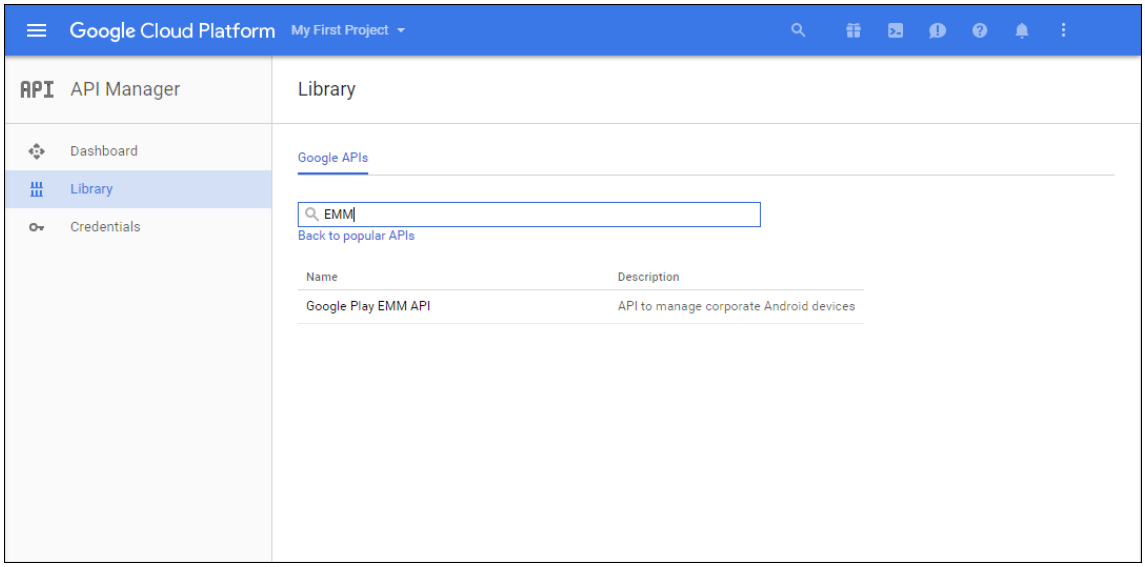
3. Geben Sie unter **Project name** einen Namen für das Projekt ein.



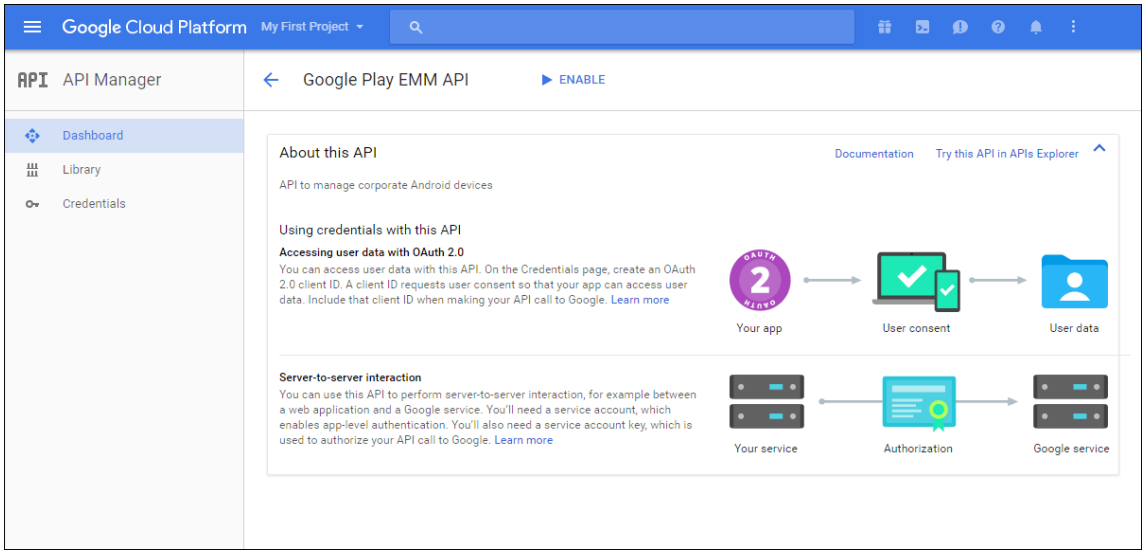
4. Klicken Sie im Dashboard auf **Use Google APIs**.



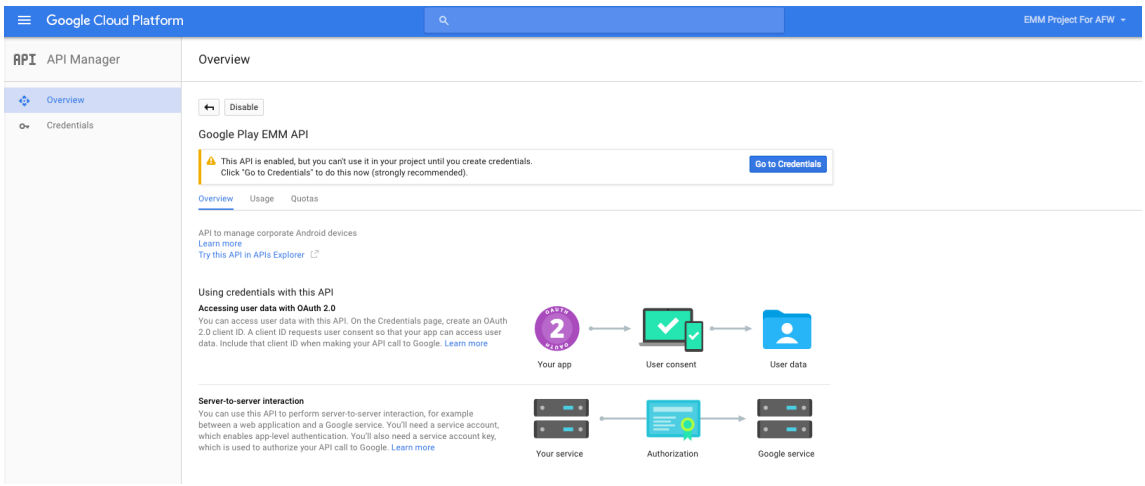
5. Klicken Sie auf **Library** geben Sie für **Search** den Text **EMM** ein und klicken Sie auf das Suchergebnis.



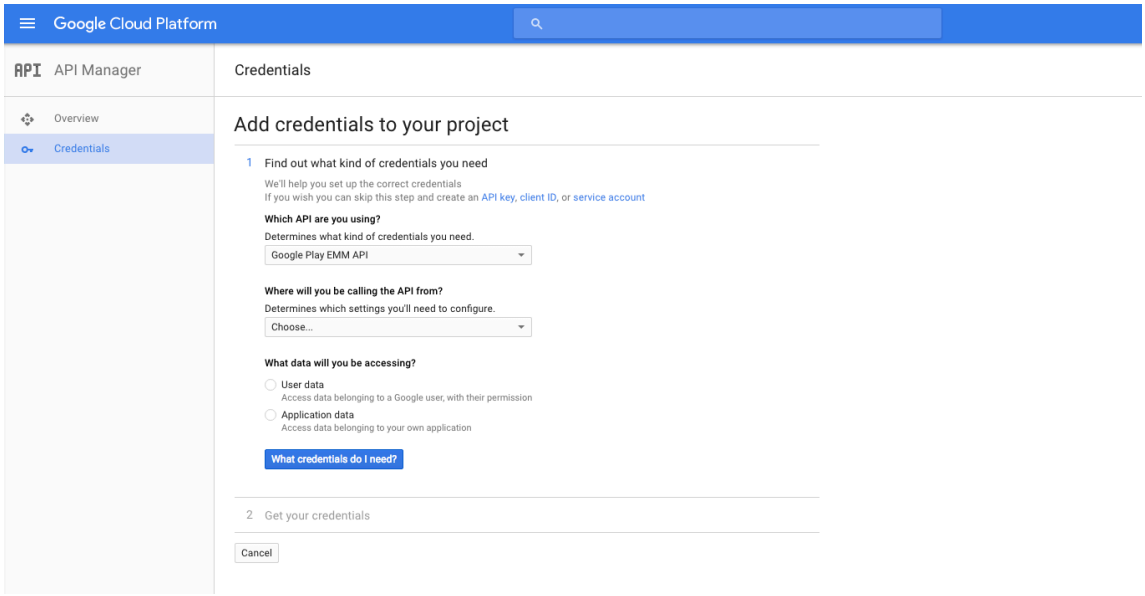
6. Klicken Sie auf der Seite **Overview** auf **Enable**.



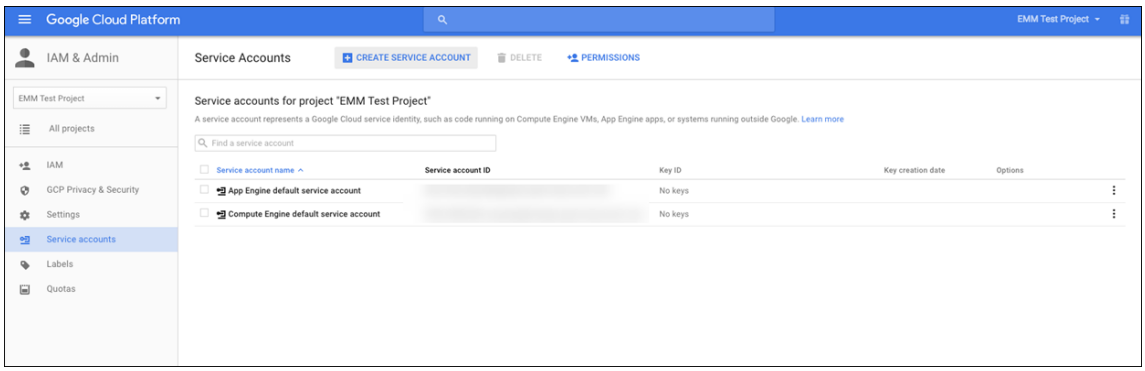
7. Klicken Sie neben **Google Play EMM API** auf **Go to Credentials**.



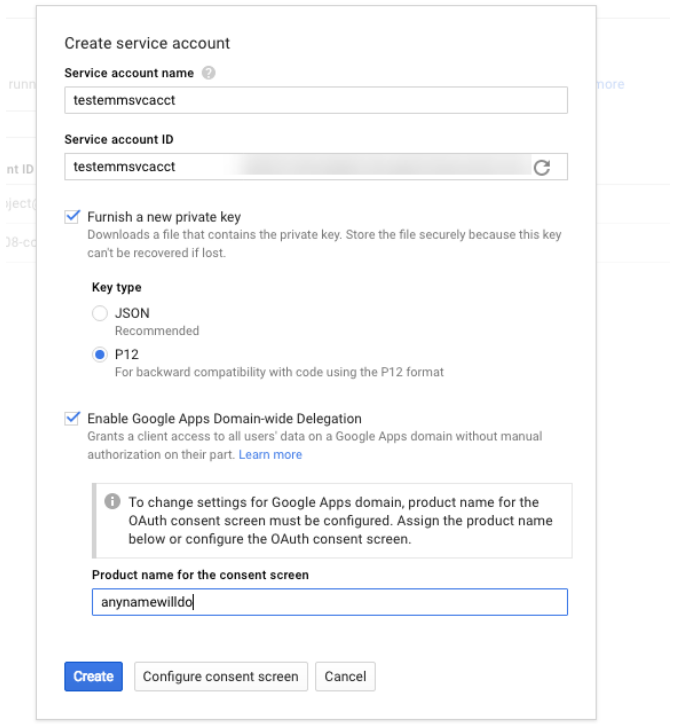
8. Klicken Sie in der Liste **Add credentials to our project** unter Schritt 1 auf **service account**.



9. Klicken Sie auf der Seite **Service Accounts** auf **Create Service Account**.

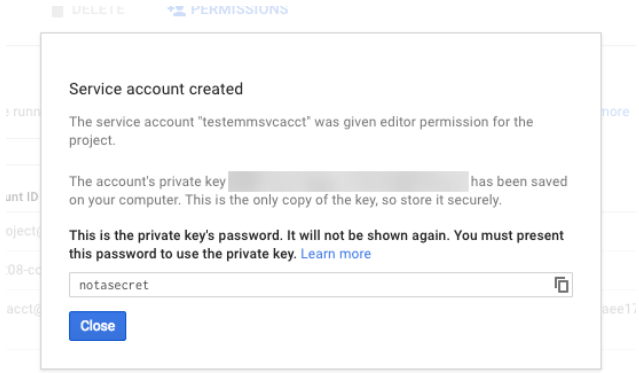


10. Geben Sie unter **Create service account** einen Namen für das Konto ein und aktivieren Sie das Kontrollkästchen **Furnish a new private key**. Klicken Sie auf **P12**, aktivieren Sie das Kontrollkästchen **Enable Google Apps Domain-wide Delegation** und klicken Sie auf **Create**.

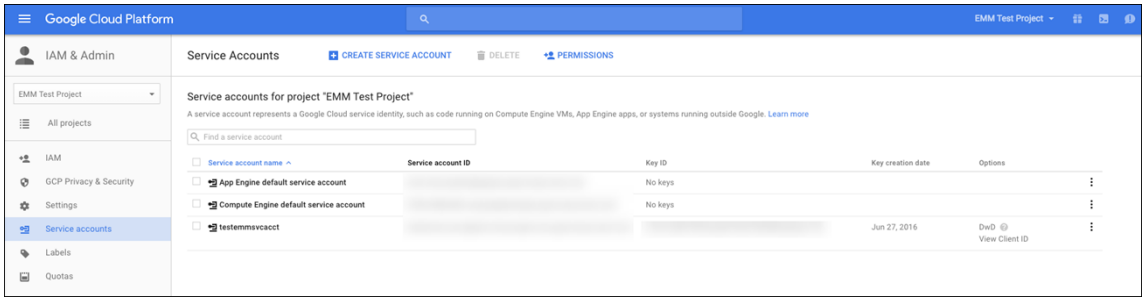


Die Zertifikatdatei (P12-Datei) wird auf Ihren Computer heruntergeladen. Speichern Sie das Zertifikat an einem sicheren Ort.

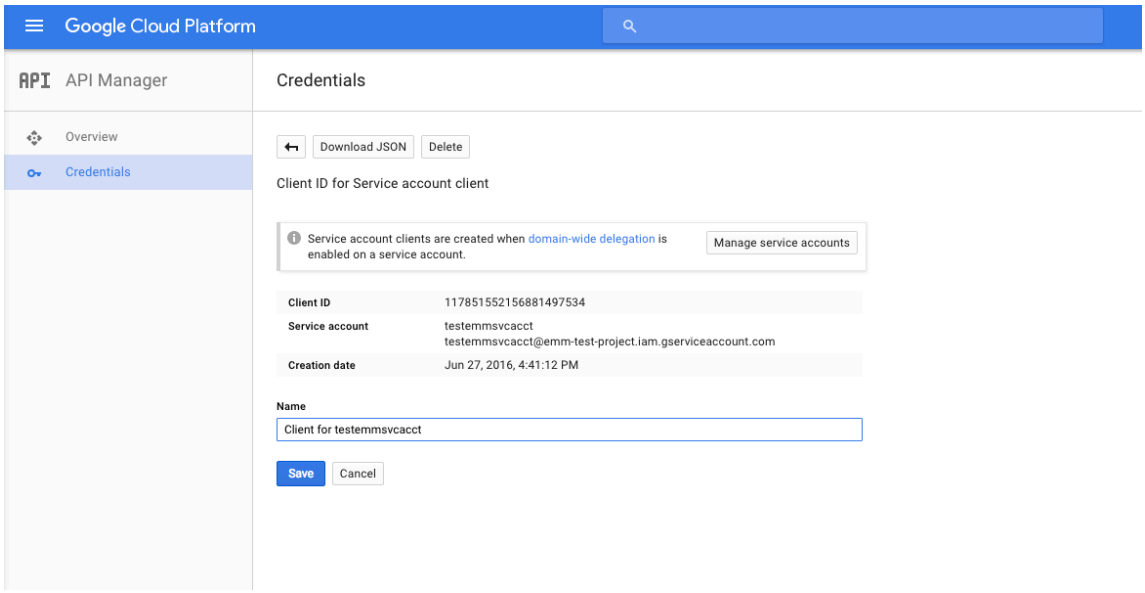
11. Klicken Sie auf der Seite **Service account created** auf **Close**.



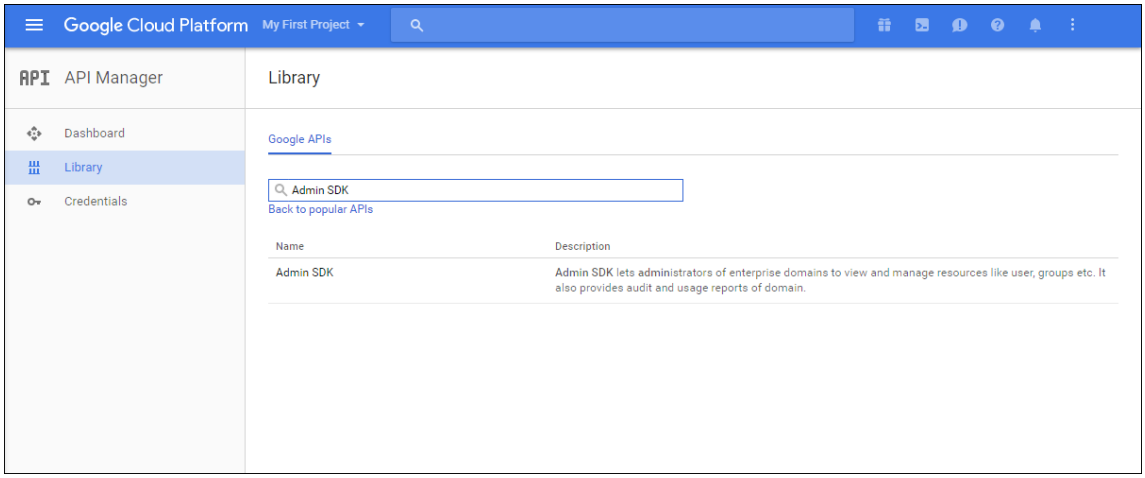
12. Klicken Sie unter **Permissions** auf **Service accounts** und dann unter **Options** für Ihr Dienstkonto auf **View Client ID**.



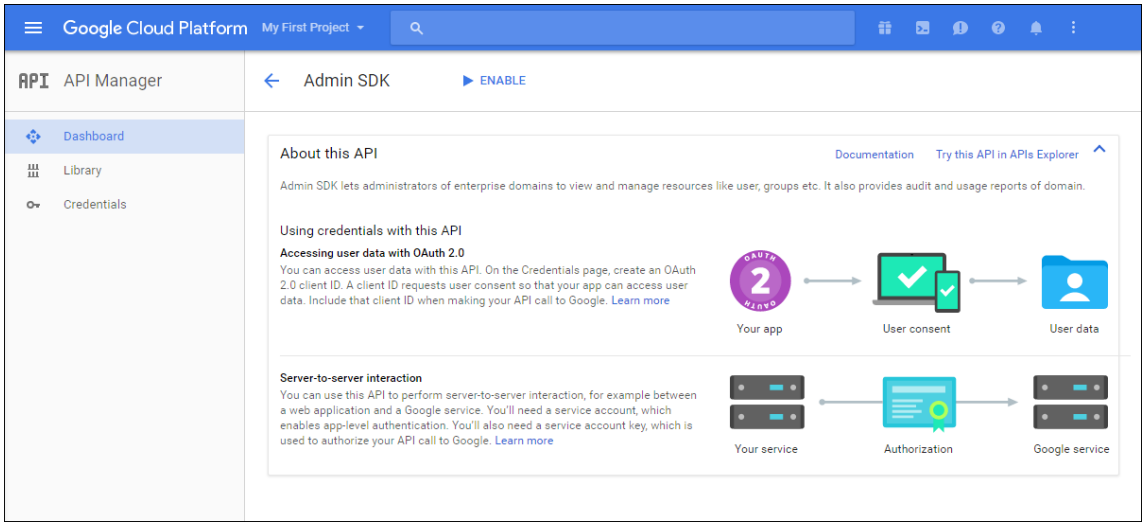
13. Die für die Kontoautorisierung auf der Google Admin-Konsole erforderlichen Informationen werden angezeigt. Kopieren Sie die **Client ID** und die **Service account ID** an einen Speicherort, an dem Sie die Informationen später abrufen können. Sie müssen diese Informationen mit dem Domänennamen an den Citrix Support senden, damit sie auf eine Positivliste gesetzt werden.



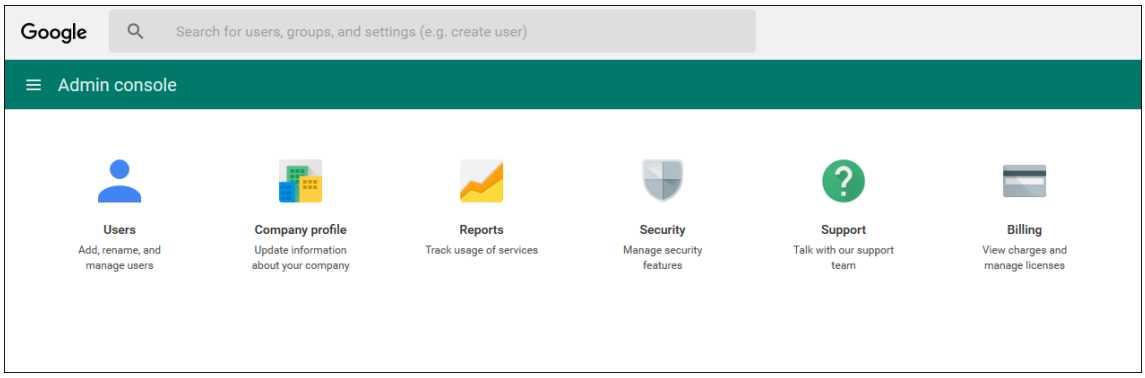
14. Suchen Sie auf der Seite **Library** den Eintrag **Admin SDK** und klicken Sie auf das Suchergebnis.



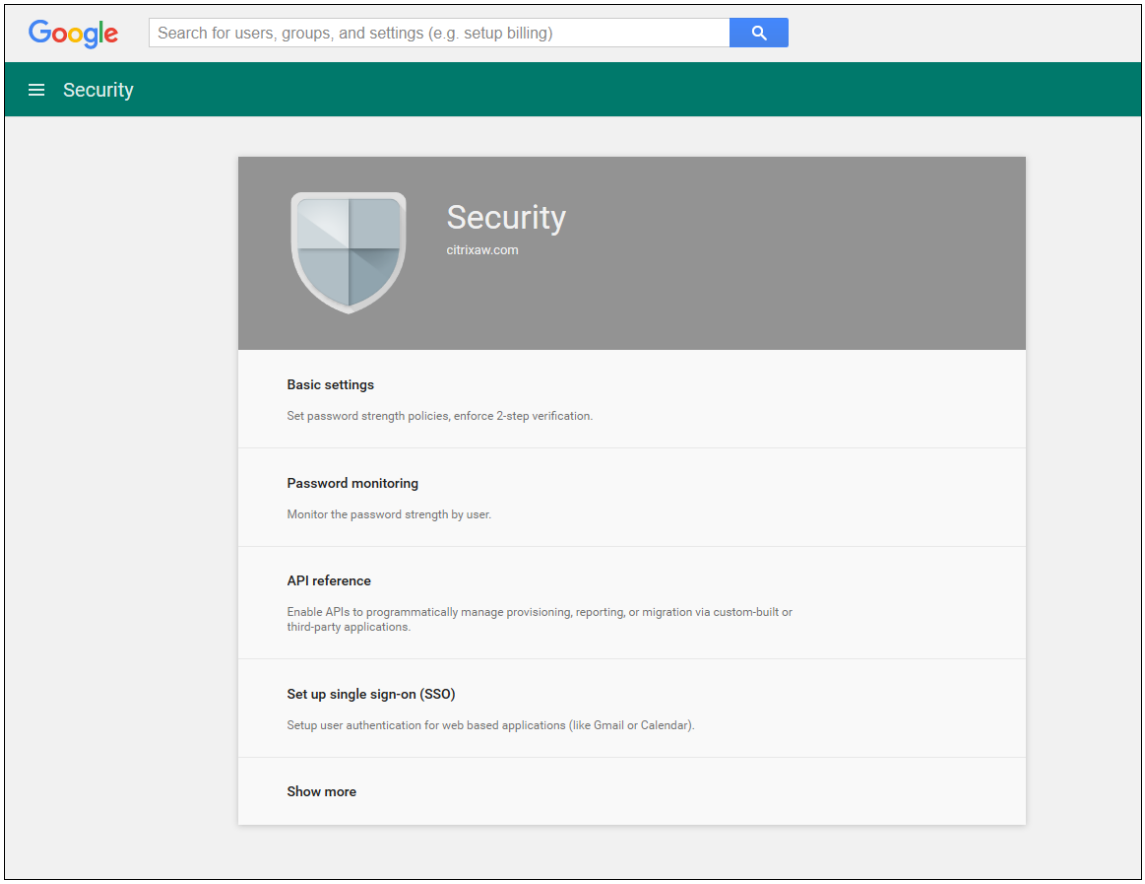
15. Klicken Sie auf der Seite **Overview** auf **Enable**.

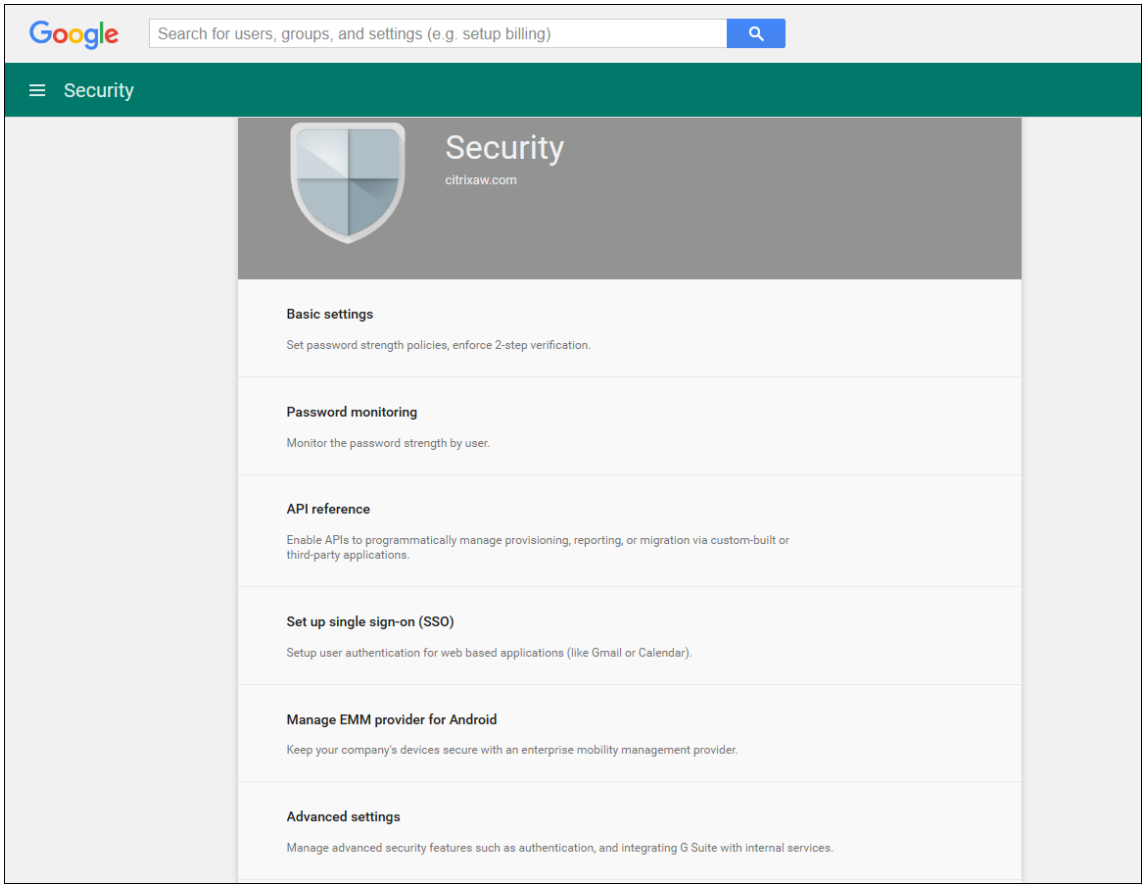


16. Öffnen Sie die Google Admin-Konsole für Ihre Domäne und klicken Sie auf **Security**.

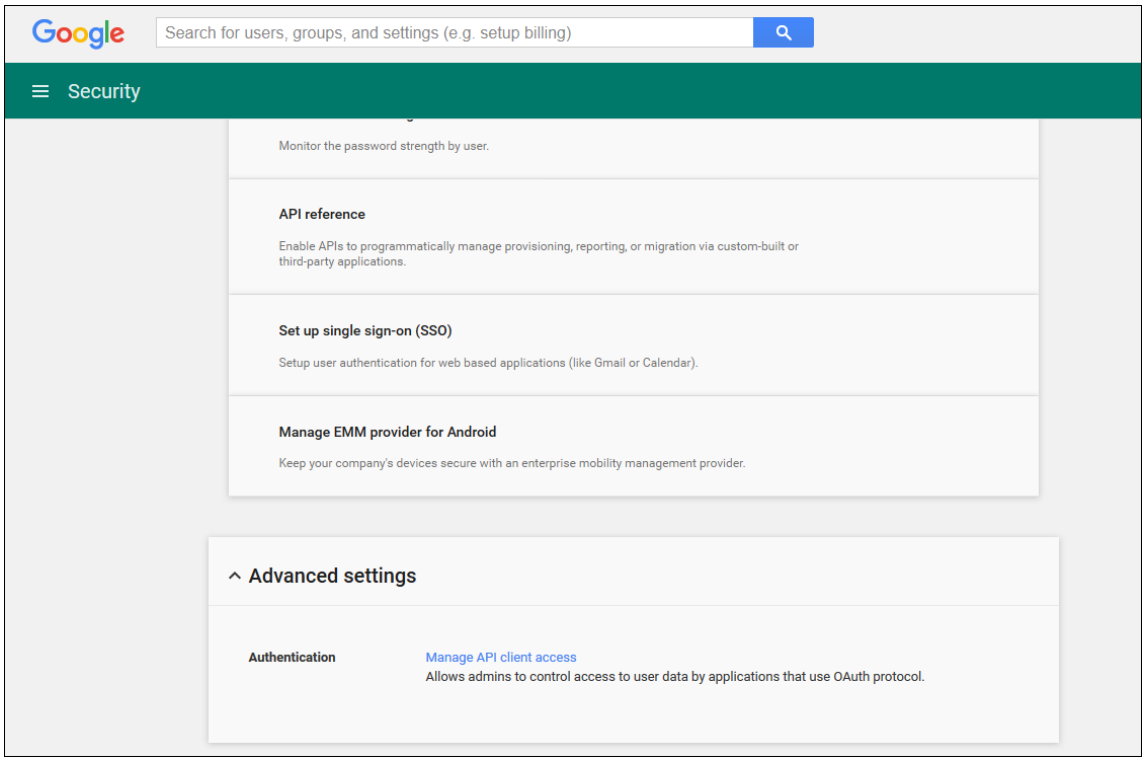


17. Klicken Sie auf der Seite **Settings** auf **Show more** und dann auf **Advanced settings**.

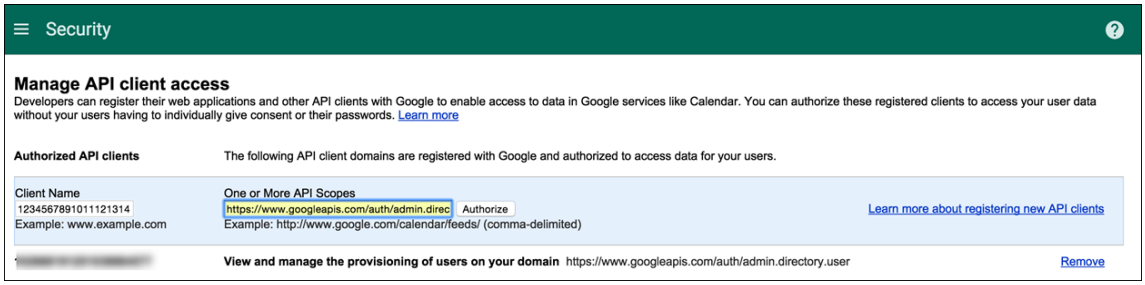




18. Klicken Sie auf **Manage API client access**.



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**.



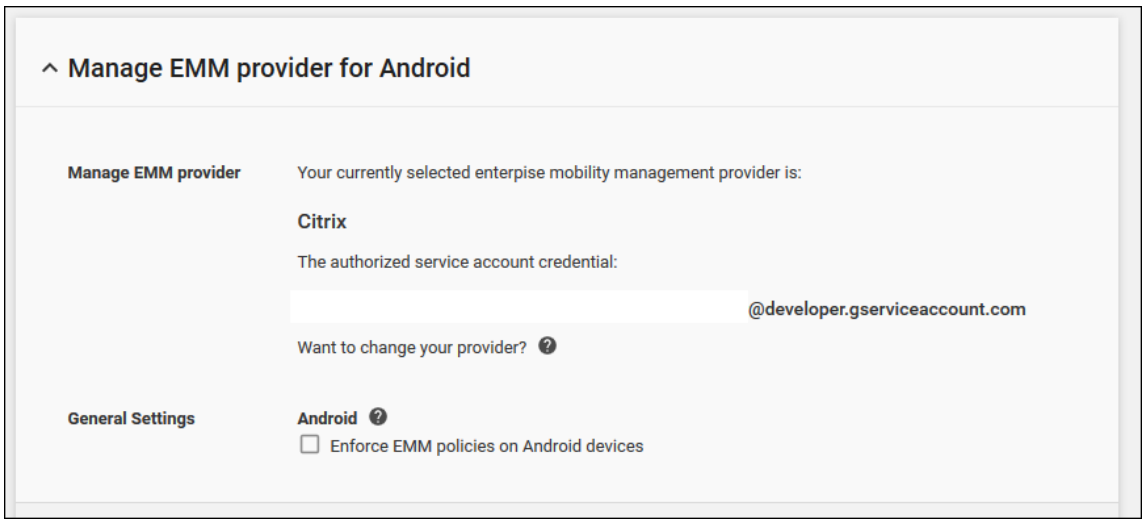
Binden an EMM

Bevor Sie Android-Geräte mit Citrix Endpoint Management verwalten können, müssen Sie dem technischen Support von Citrix den Namen Ihrer Domäne, das Dienstkonto und den Bindungstoken senden. Citrix bindet den Token dann an Citrix Endpoint Management 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.

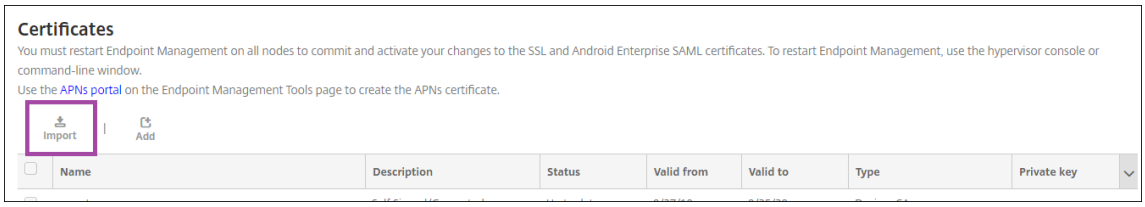
   Nach der Prüfung der Tokenbindung können Sie Citrix Endpoint Management zum Verwalten der Android-Geräte verwenden. Importieren Sie das P12-Zertifikat, das Sie in Schritt 14 erstellt haben. Richten Sie den Android Enterprise-Server ein, aktivieren Sie das SAML-basierte Single Sign-On und definieren Sie mindestens eine Android Enterprise-Richtlinie.



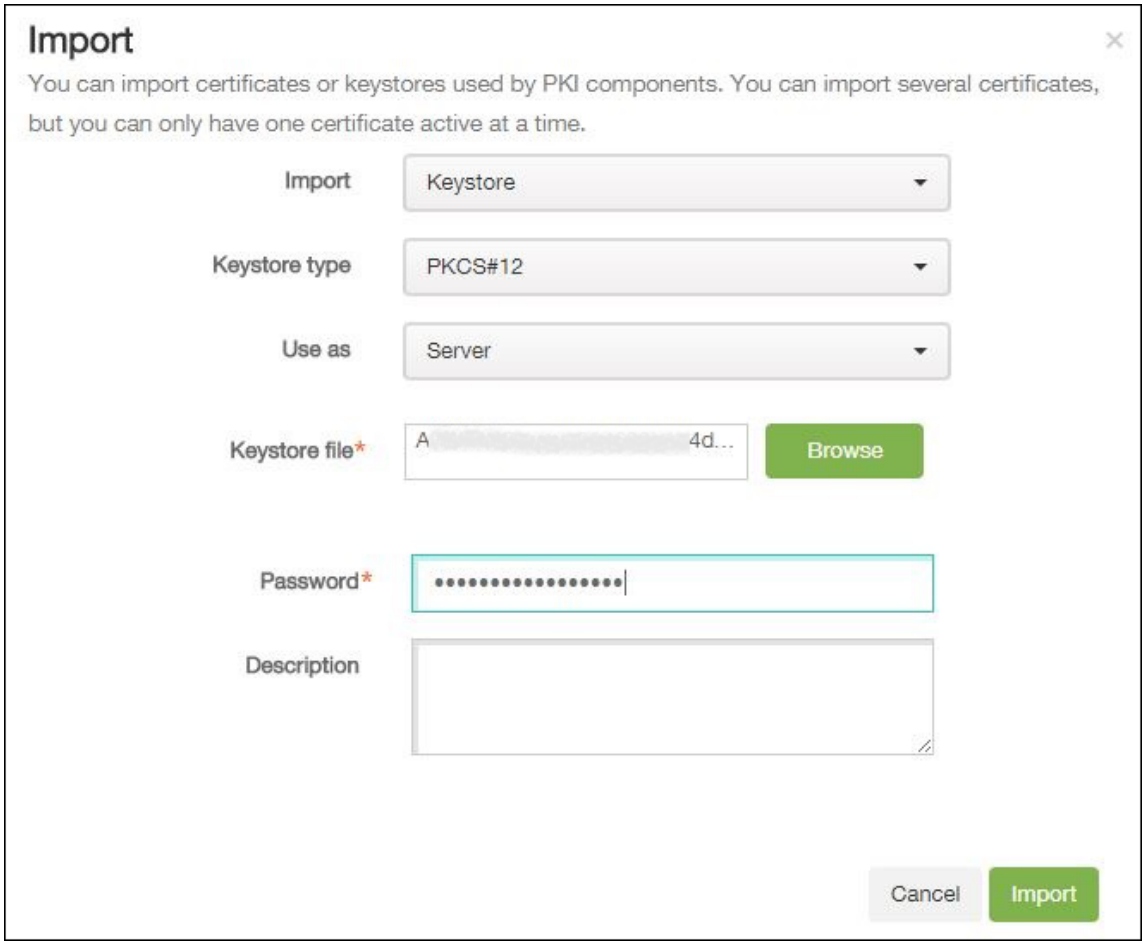
Importieren des P12-Zertifikats

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

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben, um die Seite **Einstellungen** zu öffnen, und klicken Sie dann auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.



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



Konfigurieren Sie die folgenden Einstellungen:

- **Import:** Klicken Sie in der Dropdownliste auf **Keystore**.
- **Keystore-Typ:** Klicken Sie in der Dropdownliste auf **PKCS #12**.
- **Verwenden als:** Klicken Sie in der Dropdownliste auf **Server**.
- **Schlüsselspeicherdatei:** Klicken Sie auf **Durchsuchen** und navigieren Sie zu dem P12-Zertifikat.
- **Kennwort**: Geben Sie das Kennwort für das Zertifikat ein. Dies ist das Kennwort für den privaten Schlüssel, das Sie beim Einrichten Ihres Android Enterprise-Kontos erstellt haben.
- **Beschreibung:** Geben Sie optional eine Beschreibung des Zertifikats ein.

3. Klicken Sie auf **Importieren**.

Einrichten der Android Enterprise-Servereinstellungen

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

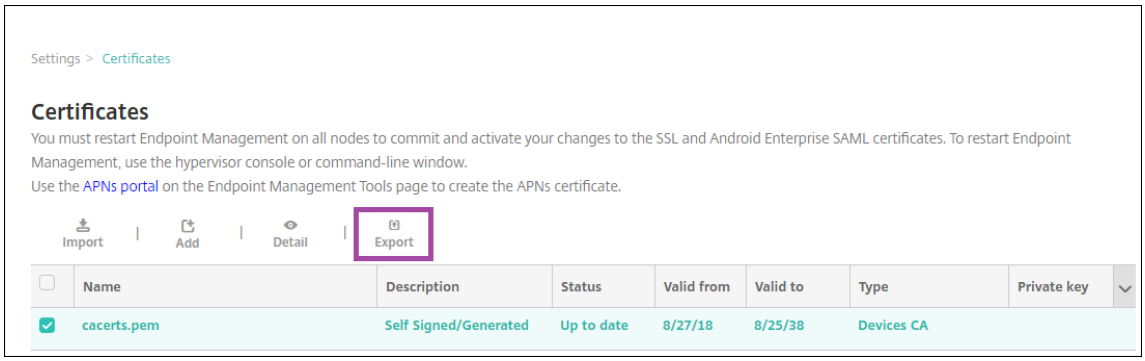
2. Wählen Sie unter **Plattformen** die Option **Android Enterprise**. Die Seite **Android Enterprise** wird angezeigt.

Konfigurieren Sie die folgenden Einstellungen und klicken Sie dann auf **Speichern**.

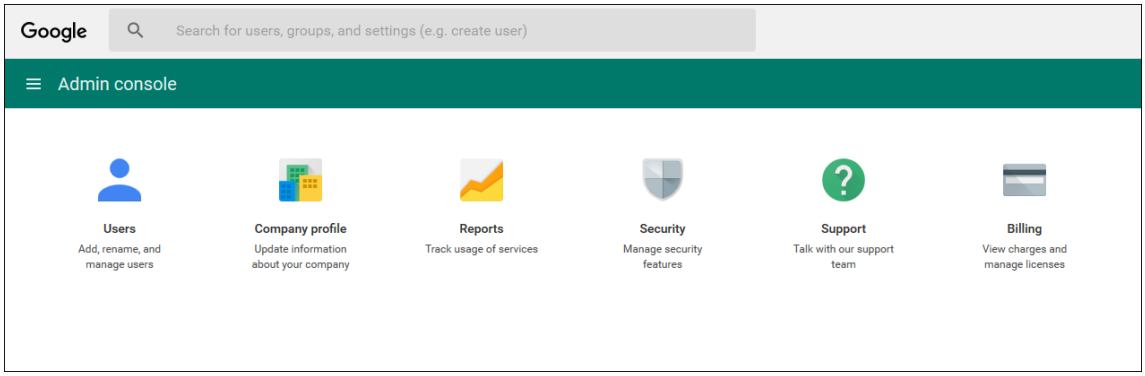
- **Domänenname:** Geben Sie den Namen der Android Enterprise-Domäne ein, z. B. domain.com.
- **Domänenadministratorkonto:** Geben Sie Ihren Domänenadministrator-Benutzernamen ein, z. B. das für das Google Developer Portal verwendete E-Mail-Konto.
- **Dienstkonto-ID:** Geben Sie die ID Ihres Dienstkontos 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

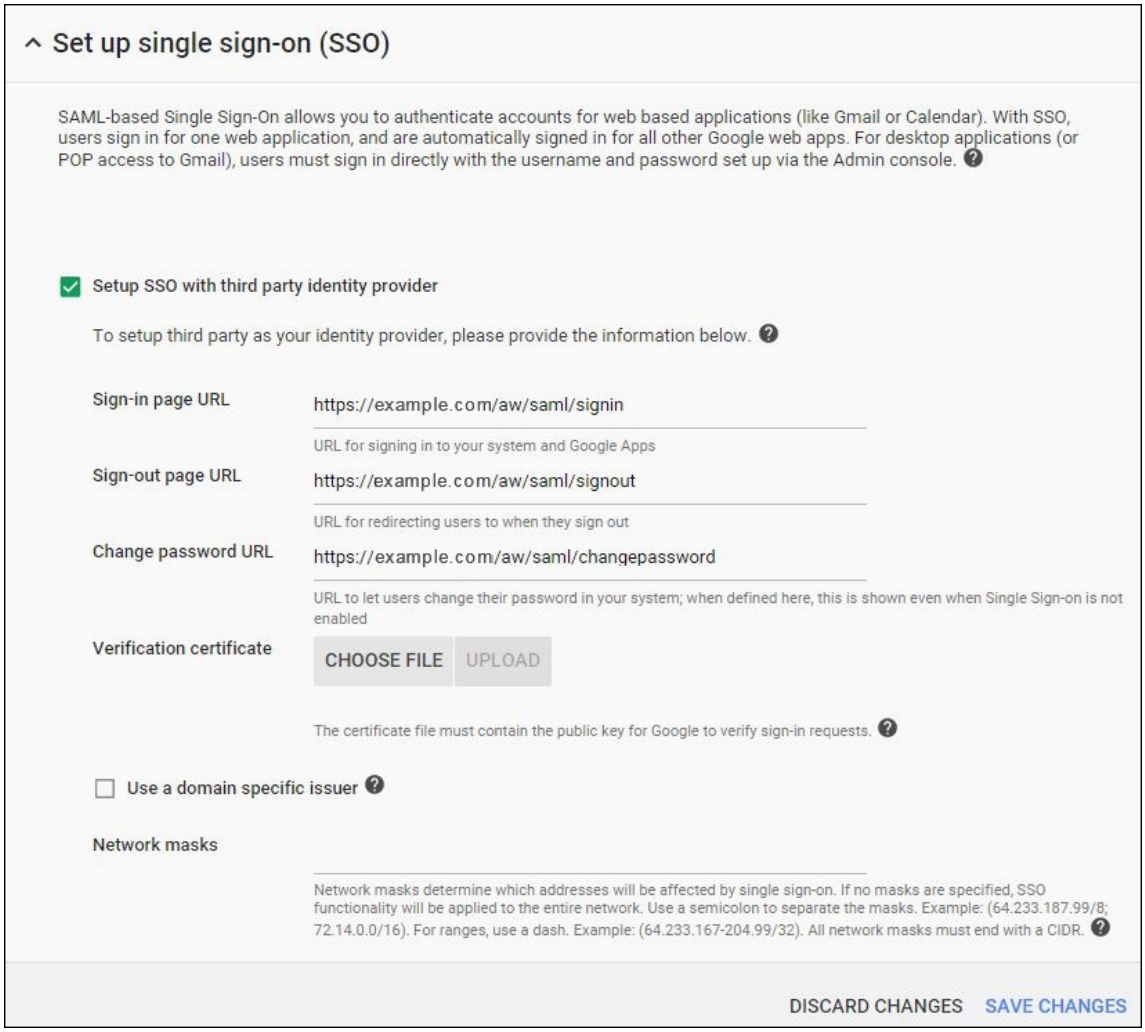
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.



3. Klicken Sie in der Liste der Zertifikate auf das SAML-Zertifikat.
4. Klicken Sie auf **Exportieren** und speichern Sie das Zertifikat auf Ihrem Computer.
5. Melden Sie sich beim Google-Verwaltungsportal mit Ihren Android Enterprise-Administratoranmeldeinforma an. Informationen zum Zugriff auf das Portal finden Sie unter Google-Verwaltungsportal.
6. Klicken Sie auf **Sicherheit**.



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

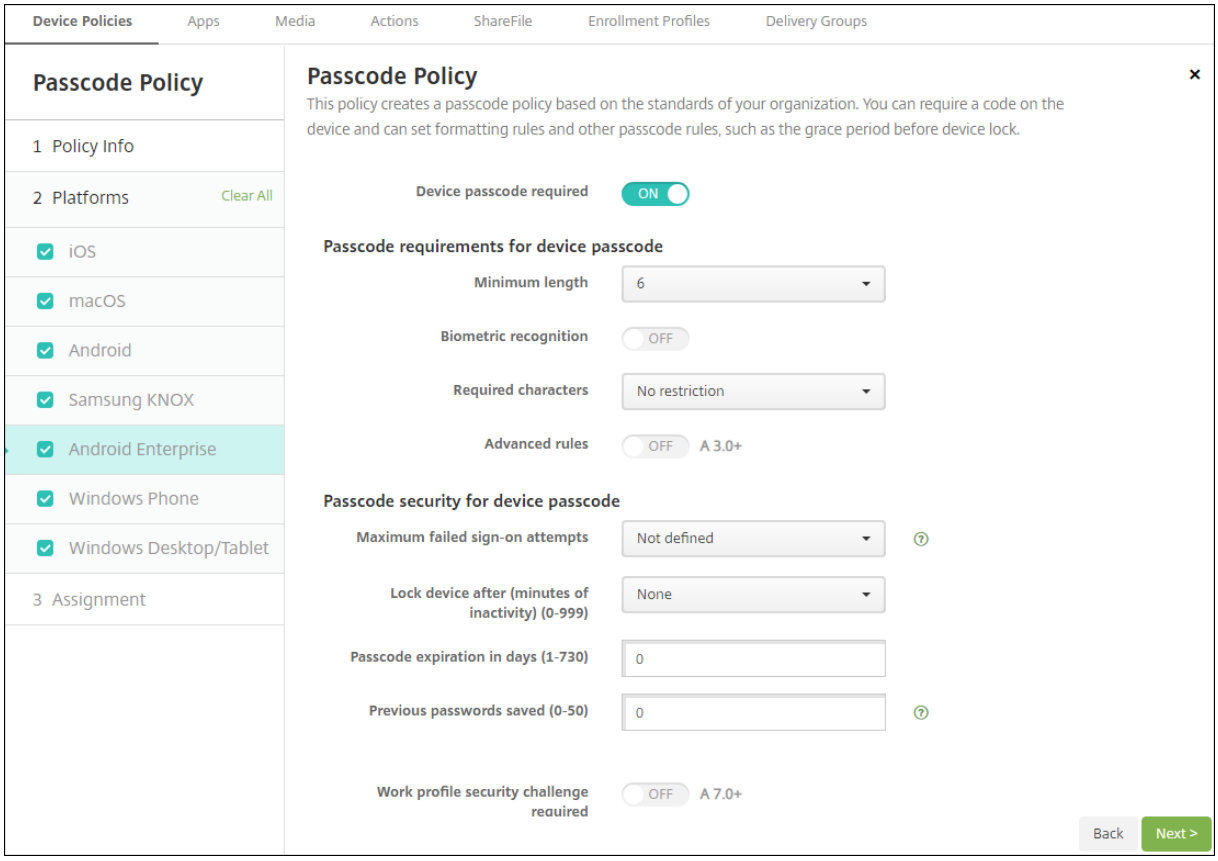


- **Sign-in page URL:** Geben Sie die URL der Seite an, über die Benutzer sich bei Ihrem System und Google Apps anmelden. Beispiel: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **Sign-out page URL:** Geben Sie die URL an, an die die Benutzer weitergeleitet werden, wenn sie sich abmelden. Beispiel: `https://<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 Citrix Endpoint Management exportierten SAML-Zertifikat.

8. 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. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren** und dann auf **Geräterichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie 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 Citrix Endpoint Management 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 Citrix Endpoint Management-Webkonsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Wählen Sie unter **Plattformen** die Option **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 eines Google Workspace-Partnerzugriffs für Citrix Endpoint Management

Einige Citrix Endpoint Management-Features für Chrome verwenden Google-Partner-APIs für die Kommunikation zwischen Citrix Endpoint Management und Ihrer Google Workspace-Domäne. Beispielsweise benötigt Citrix Endpoint Management 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 Citrix Endpoint Management-Konsole ein und konfigurieren anschließend Ihr Google Workspace-Konto.

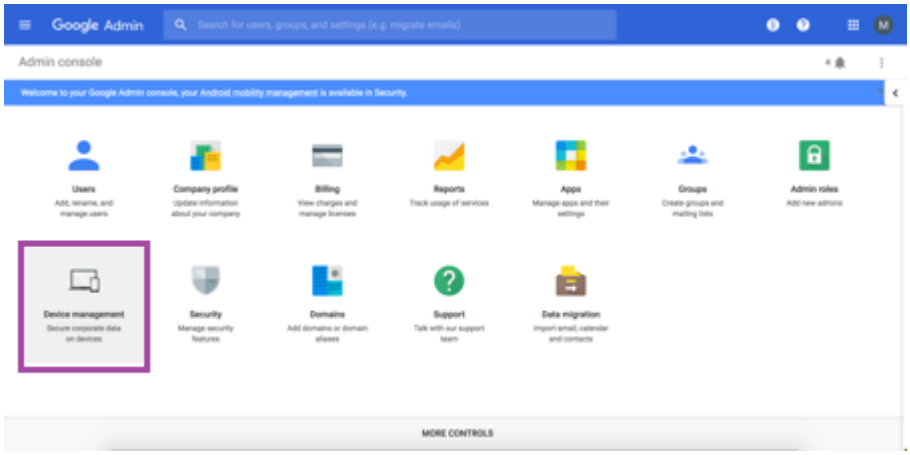
Einrichten der Google Workspace-Domäne in Citrix Endpoint Management

Um die Kommunikation zwischen Citrix Endpoint Management und den APIs in Ihrer Google Workspace-Domäne zu aktivieren, gehen Sie zu **Einstellungen > Google Chrome-Konfiguration** und konfigurieren Sie die Einstellungen.

- **Google Workspace-Domäne:** Die Google Workspace-Domäne mit den von Citrix Endpoint Management benötigten APIs.
- **Google Workspace-Administratorkonto:** Das Administratorkonto für Ihre Google Workspace-Domäne.
- **Google Workspace-Client-ID:** Die Client-ID für Citrix. Konfigurieren Sie mit diesem Wert den Partnerzugriff für Ihre Google Workspace-Domäne.
- **Google Workspace-Unternehmens-ID:** Die Unternehmens-ID für Ihr Konto mit den Angaben Ihres Google Enterprise-Kontos.

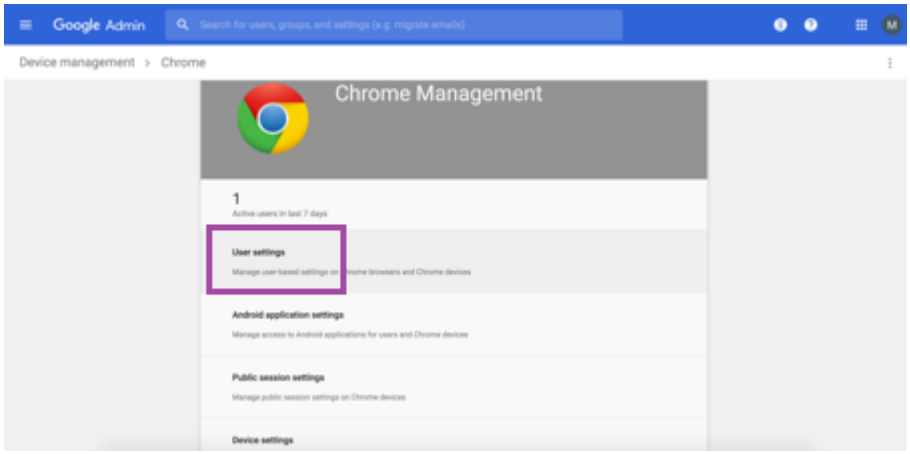
Aktivieren des Partnerzugriffs für Geräte und Benutzer in Ihrer Google Workspace-Domäne

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**.

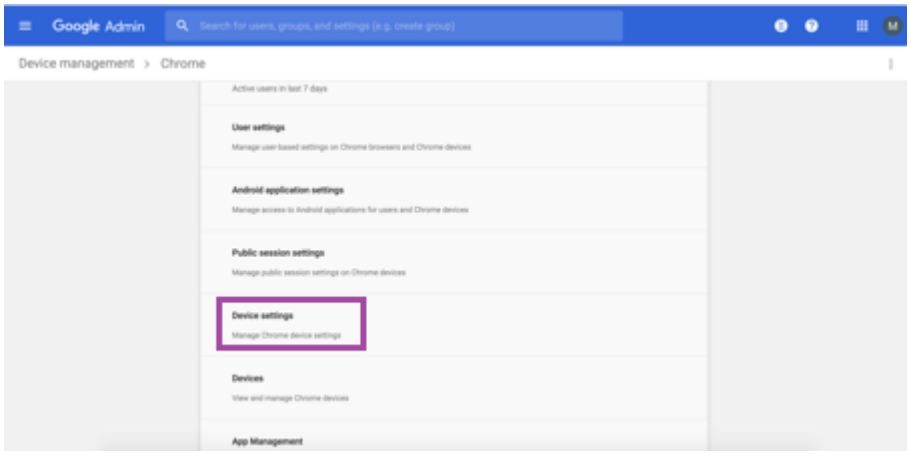


5. Suchen Sie nach **Chrome Management - Partner Access**.

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.

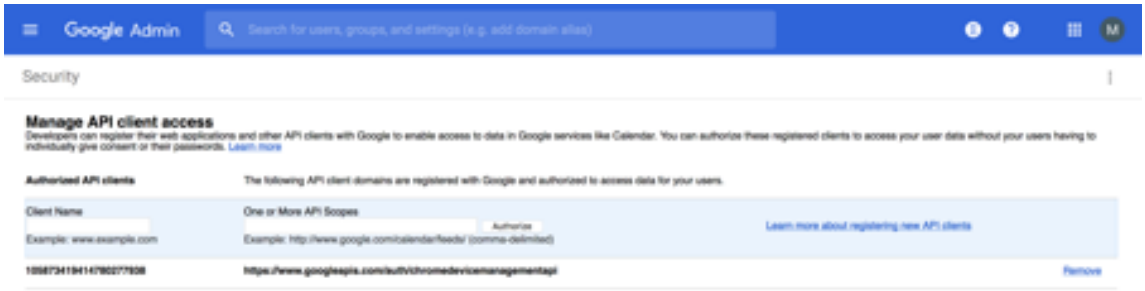
8. Klicken Sie auf der Chrome-Verwaltungsseite auf **Device Settings**.



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 Citrix Endpoint Management-Konsole zu **Einstellungen > Google Chrome-Konfiguration** und kopieren Sie den Wert für G Suite 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, hängt das akzeptierte Format davon ab, ob im Citrix Endpoint Management-Server der Benutzerprinzipalname (UPN) oder der SAM-Kontoname für die Benutzersuche konfiguriert ist.

Wenn die Benutzer in Citrix Endpoint Management über den UPN gesucht werden, müssen sie einen UPN in diesem Format eingeben:

- *username@domain*

Wenn die Benutzer in Citrix Endpoint Management über SAM gesucht werden, müssen sie die SAM in einem dieser Formate eingeben:

- *username@domain*
- *domain\username*

Bestimmen des konfigurierten Benutzernamentyps im Citrix Endpoint Management-Server:

1. Klicken Sie in der Citrix Endpoint Management-Konsole 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 Citrix Endpoint Management für UPN konfiguriert.
    - If it is set to **sAMAccountName**, the Citrix Endpoint Management server is set for SAM.

Registrierung für Android Enterprise-Unternehmen aufheben

Sie können die Registrierung für Android Enterprise-Unternehmen mit der Citrix Endpoint Management-Serverkonsole und den Citrix Endpoint Management Tools aufheben.

Wenn Sie diese Aufgabe ausführen, öffnet Citrix Endpoint Management ein Popupfenster für Citrix Endpoint Management Tools. Bevor Sie beginnen, sollten Sie sicherstellen, dass Citrix Endpoint Management im verwendeten Browser die Berechtigung hat, Popupfenster zu öffnen. In einigen Browsern (z. B. Google Chrome) müssen Sie die Popupblockierung deaktivieren und die Adresse der Citrix Endpoint Management-Site der Positivliste des Popupblockers hinzufügen.

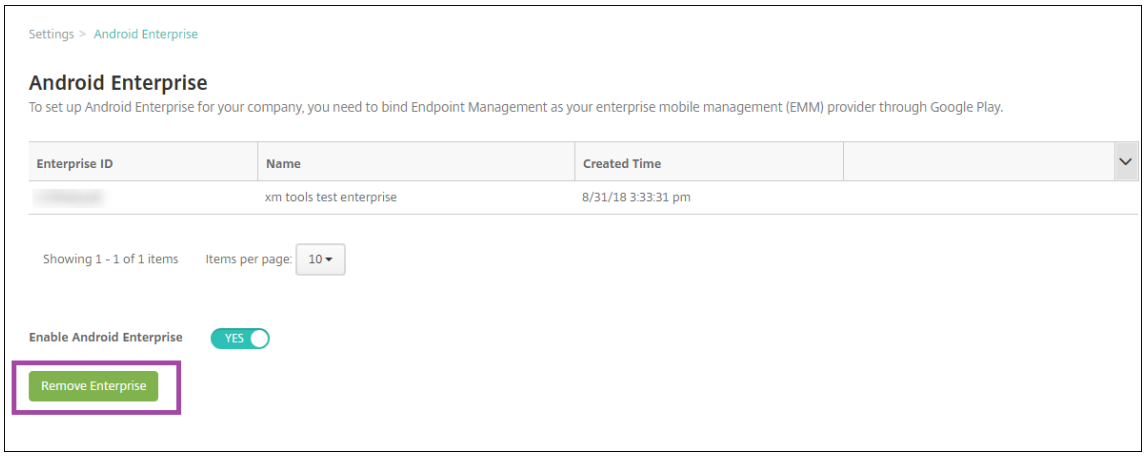
> **Warnung:**
>
> Nachdem die Registrierung eines Unternehmens aufgehoben wurde, werden Android Enterprise-Apps auf Geräten, die bereits registriert wurden, auf die Standardeinstellungen zurückgesetzt. Die Geräte werden nicht mehr von Google verwaltet. Für die Neuregistrierung in einem Android Enterprise-Unternehmen ist möglicherweise eine weitere Konfiguration erforderlich, um die vorherige Funktionalität wiederherzustellen.

Nachdem die Registrierung des Android Enterprise-Unternehmens aufgehoben wurde:

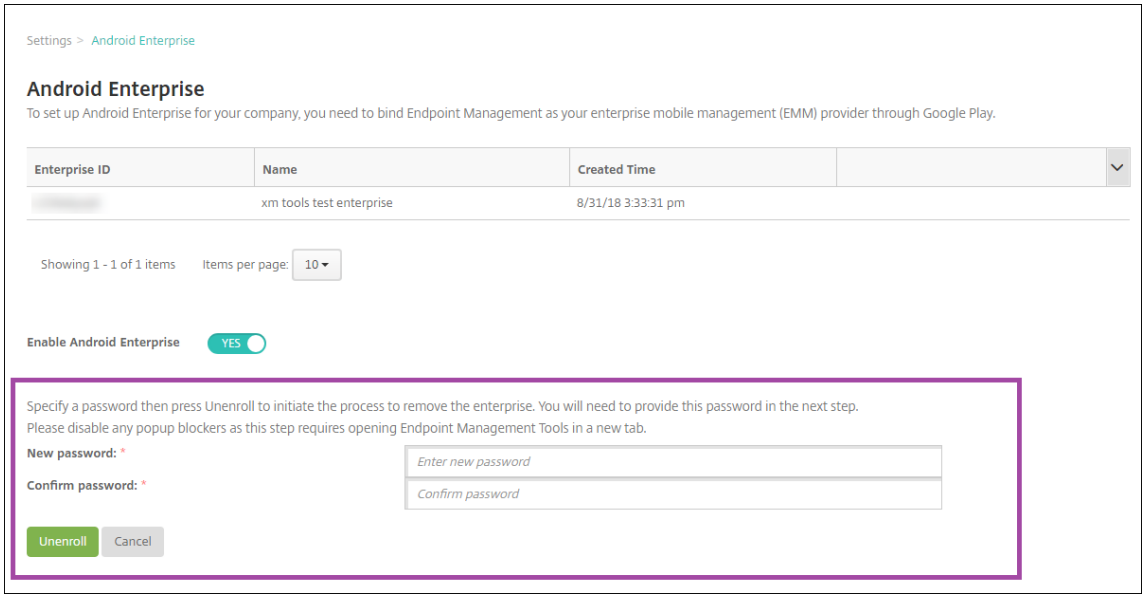
- Für Geräte und Benutzer, die über das Unternehmen registriert sind, wurden die Android Enterprise-Apps auf die Standardeinstellung zurückgesetzt. Zuvor angewendete App-Berechtigungen und Richtlinien für verwaltete Konfigurationen haben keine Wirkung mehr auf Vorgänge.
- Über das Unternehmen registrierte Geräte werden zwar von Citrix Endpoint Management verwaltet, sind jedoch aus der Perspektive von Google nicht verwaltet. Es können keine neuen Android Enterprise-Apps hinzugefügt werden. App-Berechtigungen oder Richtlinien für verwaltete Konfigurationen können nicht angewendet werden. 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:

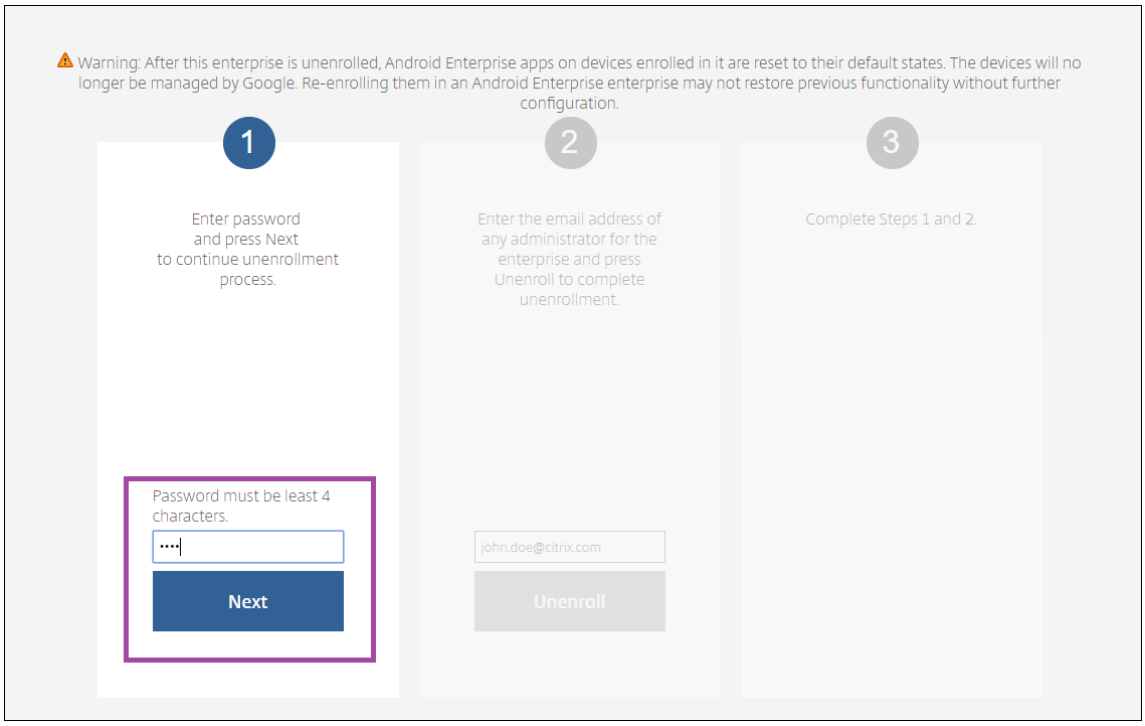
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite Einstellungen wird angezeigt.
2. Klicken Sie auf der Seite “Einstellungen”auf **Android Enterprise**.
3. Klicken Sie auf **Unternehmen entfernen**.



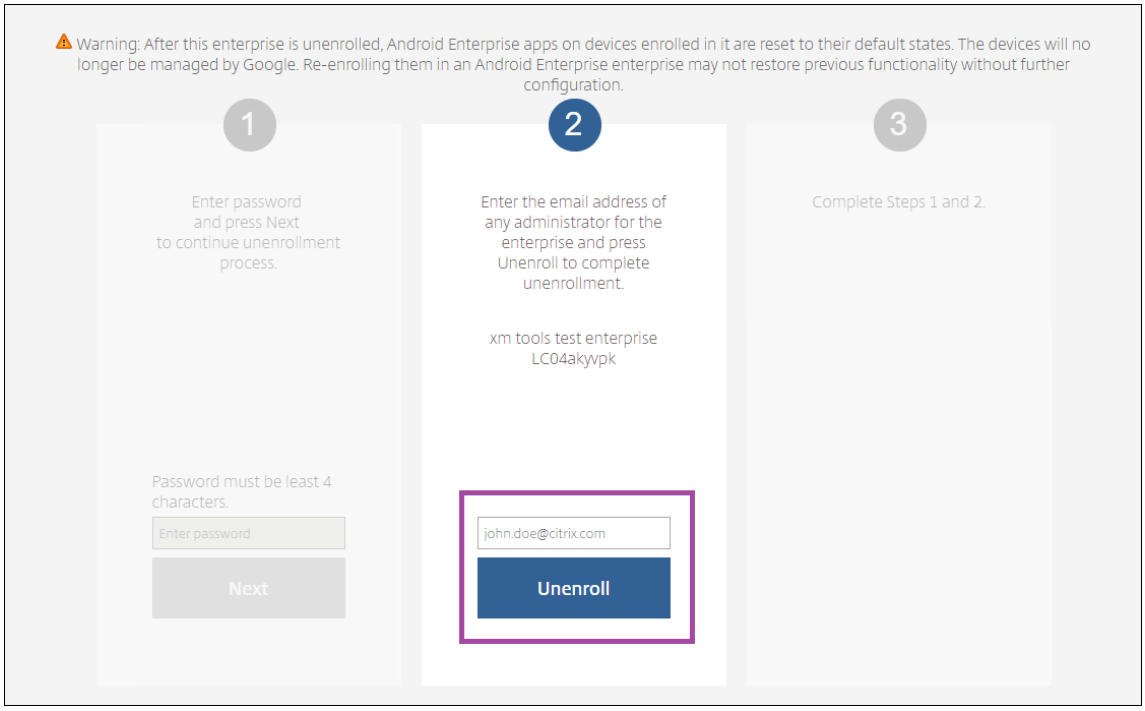
4. Geben Sie ein Kennwort an. Dies ist für den nächsten Schritt erforderlich, um das Aufheben der Registrierung abzuschließen. Klicken Sie dann auf **Registrierung aufheben**.



5. Wenn die Citrix Endpoint Management 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 Citrix Endpoint Management durch folgende Verfahren registriert werden:

- **afw#xenmobile:** Bei dieser Registrierungsmethode gibt der Benutzer beim Einrichten des Geräts die Zeichen `afw#xenmobile` ein. Der Token identifiziert das Gerät als von Citrix Endpoint Management verwaltet und lädt Citrix 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 Citrix Secure Hub heruntergeladen und installiert. Die Benutzer folgen anschließend den Anweisungen in Citrix Secure Hub zum Abschließen der Registrierung.

Diese Registrierungsmethode wird für die meisten Kunden empfohlen, da die aktuelle Citrix Secure Hub-Version aus Google Play heruntergeladen wird. Im Gegensatz zu anderen Registrierungsmethoden wird Citrix Secure Hub nicht zum Herunterladen vom Citrix Endpoint Management-Server bereitgestellt.

Voraussetzungen:

- Wird auf allen Android-Geräten mit Android-OS 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://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.

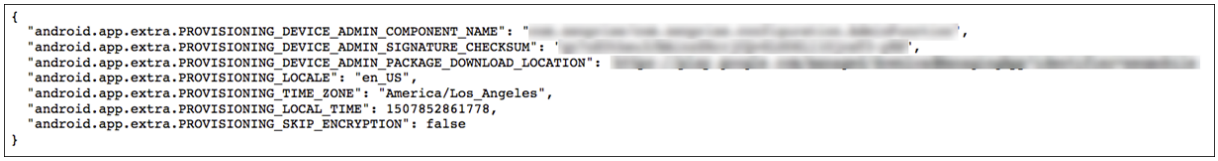
  Geben Sie den Datenbanknamen des Gebiets/Standorts ein. Geben Sie beispielsweise **America/Los_Angeles** für "Pacific Time"ein. Wenn Sie keinen Namen eingeben, wird die Zeitzone automatisch eingefügt.

- **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:



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 in einen QR-Code.

Der QR-Code wird von einem auf Werkseinstellungen zurückgesetzten Gerät gescannt, um das Gerät als vollständig verwaltetes Gerät zu registrieren.

Gerät registrieren

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 Citrix 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 Citrix Secure Hub vom Speicherort im QR-Code herunter, validiert die Signatur des Signaturzertifikats, installiert Citrix Secure Hub und legt die App als Gerätebesitzer fest.

Weitere Informationen zum Bereitstellen von Geräten per QR-Code finden Sie in der Google API-Dokumentation für Android-EMM-Entwickler.

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 Citrix Endpoint Management Provisioning Tool ausgeführt wird.

Voraussetzungen:

- Unterstützte Android-Geräte
- Citrix Endpoint Management, aktiviert für Android Enterprise
- 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 Citrix Secure Hub 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 Citrix Endpoint Management ist Citrix Secure Hub die EMM-App. Nur ein Profil ist pro Gerät zulässig. Wenn Sie versuchen, eine zweite EMM-App hinzuzufügen, wird die erste entfernt.

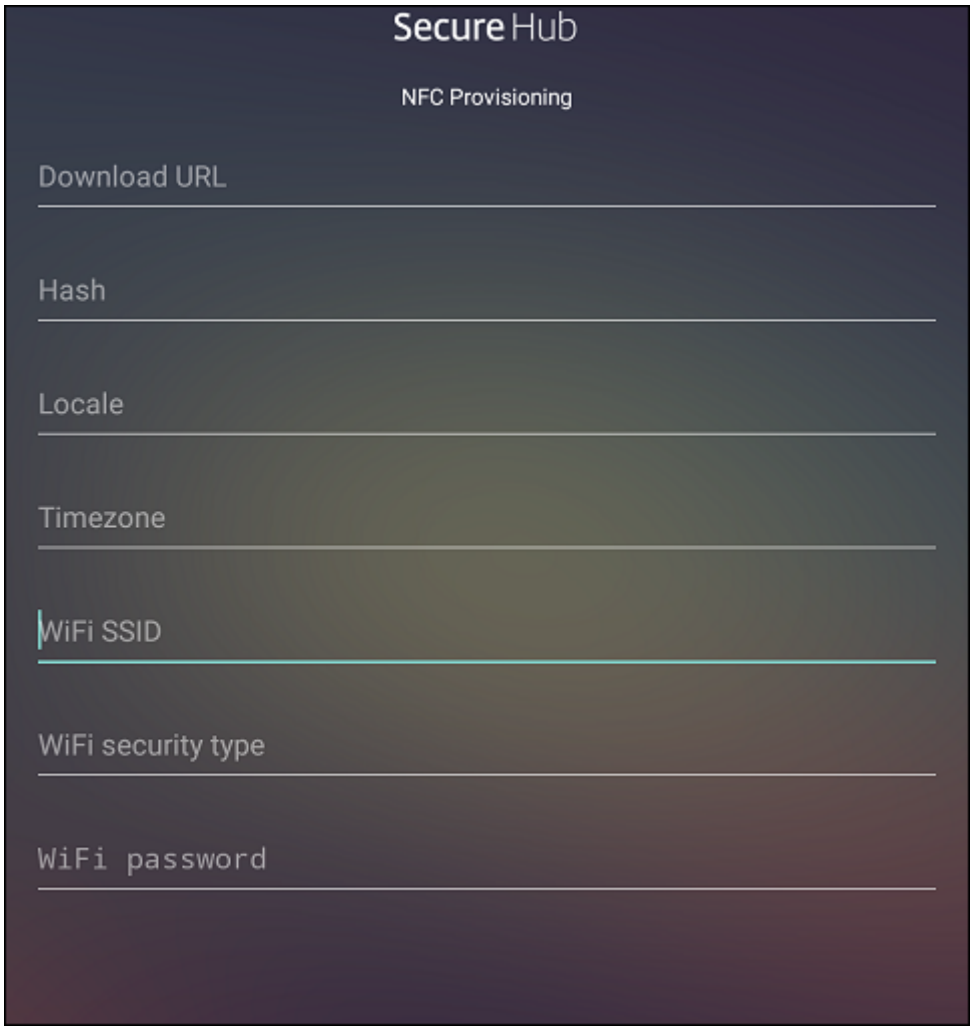
Per NFC übertragene Daten Für das Provisioning eines auf Werkseinstellungen zurückgesetzten Geräts müssen Sie die folgenden Daten per NFC senden, damit Android Enterprise initialisiert wird:

- Paketname der EMM-Anbieter-App, die als Gerätebesitzer fungiert (in diesem Fall Citrix Secure Hub).
- Intranet-/Internetspeicherort, von dem das Gerät die EMM-Anbieter-App herunterlädt.
- SHA-256-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 Citrix Secure Hub mit Administratoreinstellungen verwendet. Wenn Sie keine Werte für Zeitzone und Speicherort eingeben, konfiguriert Android sie automatisch auf dem neuen Gerät.

Citrix Endpoint Management Provisioning Tool konfigurieren 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.



You can type data into the required fields or populate them via a text file. 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.

Provisioning Tool mit einer Textdatei konfigurieren 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=<SHA-256 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 den Datenbanknamen des Gebiets/Standorts ein. Geben Sie beispielsweise **America/Los_Angeles** für "Pacific Time"ein. Wenn Sie keinen Namen eingeben, wird die Zeitzone automatisch eingefügt.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

Keine Eingabe ist erforderlich, da der Wert in der App als Citrix 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=ga50TwdCmfdJ72LGR
\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=ga50TwdCmfdJ72LGR
\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
```

Citrix Secure Hub-Prüfsumme abrufen Die Citrix Secure Hub-Prüfsumme ist ein konstanter Wert: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. Um eine APK-Datei für Citrix Secure Hub herunterzuladen, verwenden Sie den folgenden Google Play-Link: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

App-Prüfsumme abrufen 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_S` 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 Support Library

  Weitere Informationen finden Sie im Handbuch "Support Library Features Guide"in der Dokumentation für Android-Entwickler.

- 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 von Arbeitsprofilgeräten ähnelt der Android-Registrierung in Citrix Endpoint

Management. Die Benutzer laden Citrix Secure Hub aus Google Play herunter und registrieren ihre Geräte.

Standardmäßig sind die Einstellungen USB-Debugging und Unbekannte Quellen auf einem Gerät deaktiviert, wenn es bei Android Enterprise als Gerät mit Arbeitsprofil registriert ist.

> **Tipp:**
>
> Beim Registrieren von Geräten als Arbeitsprofilgerät in Android Enterprise wechseln Sie stets zu Google Play. Aktivieren Sie dort Citrix Secure Hub, das dann im persönlichen Profil des Benutzers angezeigt wird.

Android OS

June 25, 2024

> **Hinweis:**
>
> Dieser Artikel gilt nicht für Geräte, die mit Android Enterprise verwaltet werden. Weitere Informationen zu diesen Geräten finden Sie in anderen Artikeln in diesem Abschnitt.

Citrix Endpoint Management unterstützt auch Android-Geräte, die nicht über ein Android- oder Samsung Enterprise-Programm verwaltet werden. Zum Steuern, wie und wann Android-Geräte eine Verbindung zum Citrix Endpoint Management-Dienst herstellen, verwenden Sie Firebase Cloud Messaging (FCM). Weitere Informationen finden Sie unter Firebase Cloud Messaging.

Registrierungsprofile bestimmen, ob Android-Geräte bei MAM, MDM oder MDM+MAM registriert werden, wobei im letzteren Modus die Benutzer ggf. MDM abwählen können. Citrix Endpoint Management unterstützt die folgenden Authentifizierungstypen für Android-Geräte in MDM+MAM. Weitere Informationen finden Sie in den folgenden Artikeln:

- Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken
- Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne
- Identitätsanbieter:
  - Authentifizierung mit Azure Active Directory über Citrix Cloud
  - Authentifizierung mit Okta über Citrix Cloud

Eine weitere, selten verwendete Authentifizierungsmethode ist das Clientzertifikat plus Sicherheitstoken. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX215200.

Die Android-Geräteverwaltung wird generell folgendermaßen begonnen:

1. Durchführen des Onboarding-Prozesses. Weitere Informationen finden Sie unter Onboarding und Einrichten von Ressourcen und Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen.
2. Auswahl und Konfigurieren der Registrierungsmethode. Weitere Informationen finden Sie unter Unterstützte Registrierungsmethoden.
3. Konfigurieren von Android-Geräterichtlinien.
4. Registrieren von Android Enterprise-Geräten.
5. Einrichten von Sicherheitsaktionen für Apps und Geräte. Weitere Informationen finden Sie unter Sicherheitsaktionen.

Informationen zu unterstützten Betriebssystemen finden Sie unter Unterstützte Gerätebetriebssysteme.

Unterstützte Registrierungsmethoden

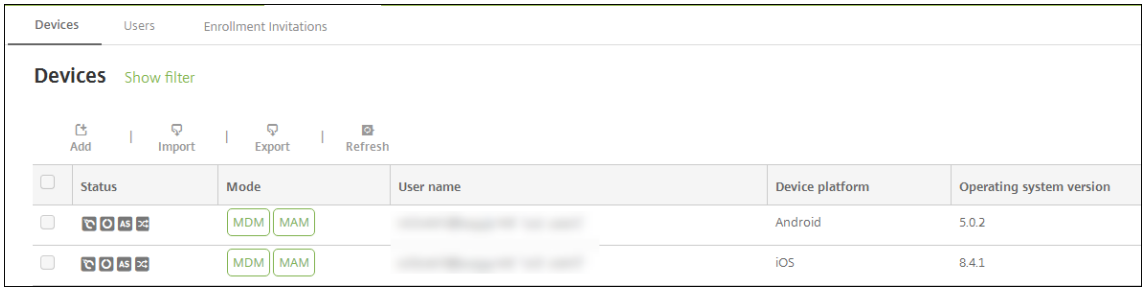
In der folgenden Tabelle werden die Registrierungsmethoden aufgelistet, die Citrix Endpoint Management für Android-Geräte unterstützt:

Methode	Unterstützt
Massenregistrierung	Nein
Manuelle Registrierung	Ja
Registrierungseinladungen	Ja

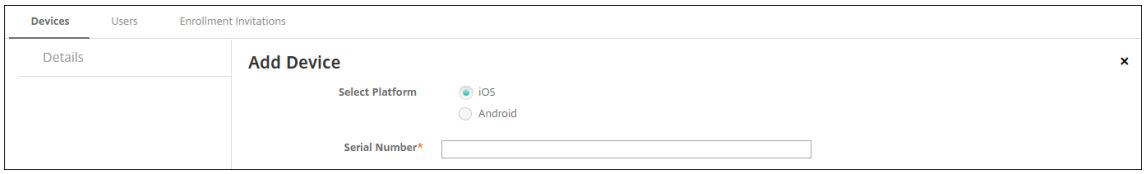
Manuelles Hinzufügen eines Android-Geräts

Führen Sie folgende Schritte aus, um ein Android- oder iOS-Gerät manuell hinzuzufügen (beispielsweise zu Testzwecken).

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.



2. Klicken Sie auf **Hinzufügen**. Die Seite **Gerät hinzufügen** wird angezeigt.



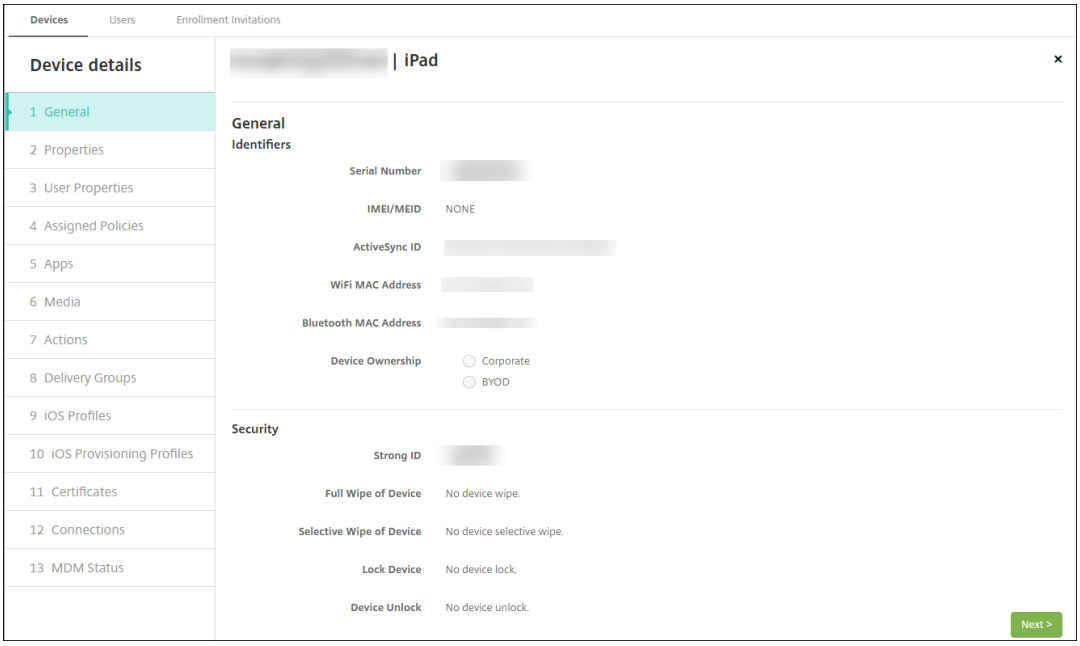
3. Konfigurieren Sie folgende Einstellungen:

   - **Plattform wählen:** Klicken Sie auf **Android**.
   - **Seriennummer:** Geben Sie die Seriennummer des Geräts ein.
   - **IMEI/MEID:** Geben Sie optional die IMEI/MEID 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 Citrix Endpoint Management 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. Citrix Endpoint Management löscht das Element sofort.

7. Die verbleibenden Abschnitte mit **Gerätedetails** enthalten zusammenfassende Informationen zu dem Gerät.

   - **Benutzereigenschaften:** Zeigt RBAC-Rollen, Gruppenmitgliedschaften, verwaltete Google Play-Konten und Eigenschaften des Benutzers an. Auf dieser Seite können Sie ein

verwaltetes Google Play-Konto deaktivieren.

- **Zugewiesene Richtlinien:** zeigt die Anzahl der bereitgestellten, ausstehenden und fehlgeschlagenen Richtlinien an. Für die einzelnen Richtlinien werden Name, Typ und letzte Bereitstellung angezeigt. Ermöglicht das Zurücksetzen des Bereitstellungsstatus auf "Ausstehend"und die erneute Bereitstellung der vom Benutzer entfernten Richtlinien.
- **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 Android-Geräterichtlinien

Verwenden Sie diese Richtlinien, um die Interaktion von Citrix Endpoint Management mit Geräten zu konfigurieren, auf denen Android ausgeführt wird. In dieser Tabelle werden alle für Android-Geräte verfügbaren Geräterichtlinien aufgeführt.

[APN](/de-de/citrix-endpoint-management/policies/apn-policy.html#android-settings)	[App-

Zugriff](/de-de/citrix-endpoint-management/policies/app-access-policy.html) |[App-Bestand](/de-de/citrix-endpoint-management/policies/app-inventory-policy.html) |
|[App-Sperre](/de-de/citrix-endpoint-management/policies/app-lock-policy.html#android-legacy-da-settings) |[App-Deinstallation](/de-de/citrix-endpoint-management/policies/app-uninstall-policy.html) |[Anmeldeinformationen](/de-de/citrix-endpoint-management/policies/credentials-policy.html#android-settings) |
|[Citrix Endpoint Management-Optionen](/de-de/citrix-endpoint-management/policies/options-policy.html) |[Citrix Endpoint Management-Deinstallation](/de-de/citrix-endpoint-management/policies/uninstall
policy.html) |[Dateien](/de-de/citrix-endpoint-management/policies/files-policy.html) |
|[Launcher-Konfiguration](/de-de/citrix-endpoint-management/policies/launcher-configuration-policy.html) |[Standort](/de-de/citrix-endpoint-management/policies/location-policy.html#android-legacy-da-settings) |[Netzwerk](/de-de/citrix-endpoint-management/policies/network-policy.html#android-legacy-da-settings)|
|[Passcode](/de-de/citrix-endpoint-management/policies/passcode-policy.html#android-legacy-da-settings) |[Einschränkungen](/de-de/citrix-endpoint-management/policies/restrictions-policy.html#android-settings) |[Planung](/de-de/citrix-endpoint-management/policies/connection-scheduling-policy.html)
|
|[Store](/de-de/citrix-endpoint-management/policies/store-policy.html) |[AGB](/de-de/citrix-endpoint-management/policies/terms-and-conditions-policy.html) |[Tunnel](/de-de/citrix-endpoint-management/policies/tunnel-policy.html)|
|VPN |Webclip |

Registrieren von Android-Geräten

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 Citrix Secure Hub installiert ist, tippen Sie auf **Öffnen**.
4. Akzeptieren Sie bei Geräten mit Android ab Version 6.0 die erforderlichen Berechtigungen:
    - Citrix Secure Hub kann Anrufe tätigen und verwalten (erforderlich)
    - Citrix Secure Hub den Zugriff auf Fotos, Medien und Dateien auf Ihrem Gerät zulassen (erforderlich)
    - Citrix Secure Hub Zugriff auf den Gerätestandort gestatten (optional)
5. Geben Sie Ihre geschäftlichen Anmeldeinformationen ein, z. B. den Namen des Citrix Endpoint Management-Servers, Ihren Benutzerprinzipalnamen oder Ihre E-Mail-Adresse. Klicken Sie dann auf **Weiter**.

6. Wählen Sie, wie Sie das Gerät registrieren möchten:
   - Für die Registrierung bei MDM+MAM tippen Sie auf **Ja, registrieren**.
   - Zur Registrierung bei MAM tippen Sie auf **Nein**.
7. Tippen Sie im Bildschirm **Geräteadministrator aktivieren** auf **Aktivieren**.
8. Geben Sie Ihr geschäftliches Kennwort ein und tippen Sie dann auf **Anmelden**.
9. Je nachdem, wie Citrix Endpoint Management konfiguriert ist, werden Sie möglicherweise aufgefordert, eine Citrix-PIN zu erstellen. Mit dieser PIN können Sie sich bei Citrix Secure Hub und anderen Citrix Endpoint Management-aktivierten Apps wie Citrix Secure Mail und Citrix Files anmelden. Sie müssen die Citrix-PIN zweimal eingeben. Geben Sie im Bildschirm **Citrix-PIN erstellen** eine PIN ein.
10. Geben Sie die PIN erneut ein. Citrix Secure Hub wird geöffnet. Sie können nun auf den App-Store zugreifen und Apps für die Installation auf dem Android-Gerät anzeigen.
11. Wenn Sie Citrix Endpoint Management 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 Citrix Endpoint Management konfigurieren, auf dem Gerät bereitgestellt. Tippen Sie auf **Installieren**, um die App zu installieren.

Aufheben der Registrierung eines Android-Geräts auf und erneute Registrierung

Benutzer können über Citrix Secure Hub die Registrierung aufheben. Wenn Benutzer die Registrierung mit dem folgenden Verfahren aufheben, wird das Gerät weiterhin im Gerätebestand der Citrix Endpoint Management-Konsole angezeigt. Aktionen können jedoch nicht auf dem Gerät ausgeführt werden. Sie können beispielsweise das Gerät nicht verfolgen oder die Gerätekonformität überwachen.

1. Öffnen Sie die Citrix 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 im Fenster **Konto löschen?** auf **Ja, löschen**.
   Citrix Secure Hub hebt die Registrierung des Geräts auf. Folgen Sie dann den Anweisungen auf dem Bildschirm, um das Gerät erneut zu registrieren.

Sicherheitsaktionen

Android unterstützt die folgenden Sicherheitsaktionen. Eine Beschreibung der einzelnen Sicherheitsaktionen finden Sie unter Sicherheitsaktionen.

App-Sperre	Apps löschen	Zertifikaterneuerung
Vollständig löschen	Orten	Sperren
Lock and Reset Password	Benachrichtigen	Widerrufen
Selektiv löschen		

> **Hinweis:**
>
> Bei Geräten mit Android 6.0 und höher muss der Benutzer zur Verwendung der Sicherheitsaktion Orten bei der Registrierung eine Standortberechtigung erteilt haben. Der Benutzer kann das Erteilen der Berechtigung ablehnen. Wenn der Benutzer die Berechtigung bei der Registrierung nicht erteilt hat, fordert Citrix Endpoint Management sie beim Senden des Befehls Orten noch einmal an.

Firebase Cloud Messaging

December 1, 2023

> **Hinweis:**
>
> Firebase Cloud Messaging (FCM) war zuvor als Google Cloud Messaging (GCM) bekannt. Bei einigen Beschriftungen und Meldungen für die Citrix Endpoint Management-Konsole wird GCM-Terminologie verwendet.

Citrix empfiehlt, dass Sie mit Firebase Cloud Messaging (FCM) steuern, wie und wann Android-Geräte eine Verbindung zu Citrix Endpoint Management herstellen. Ist Citrix Endpoint Management 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 dem Citrix Endpoint Management-Server herzustellen.

Wenn ein Gerät nach Abschluss der in diesem Artikel beschriebenen Konfigurationsschritte eingecheckt wird, wird es beim FCM-Dienst in Citrix Endpoint Management registriert. Über diese Verbindung können Citrix Endpoint Management-Dienst und Ihr Gerät mittels FCM nahezu in Echtzeit miteinander kommunizieren. Die FCM-Registrierung funktioniert bei neuen und zuvor registrierten Geräten.

Wenn Citrix Endpoint Management 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 Citrix Secure Hub-Client
- Anmeldeinformationen für Google Developer-Konto
- Google Play auf FCM-aktivierten Android-Geräten installiert

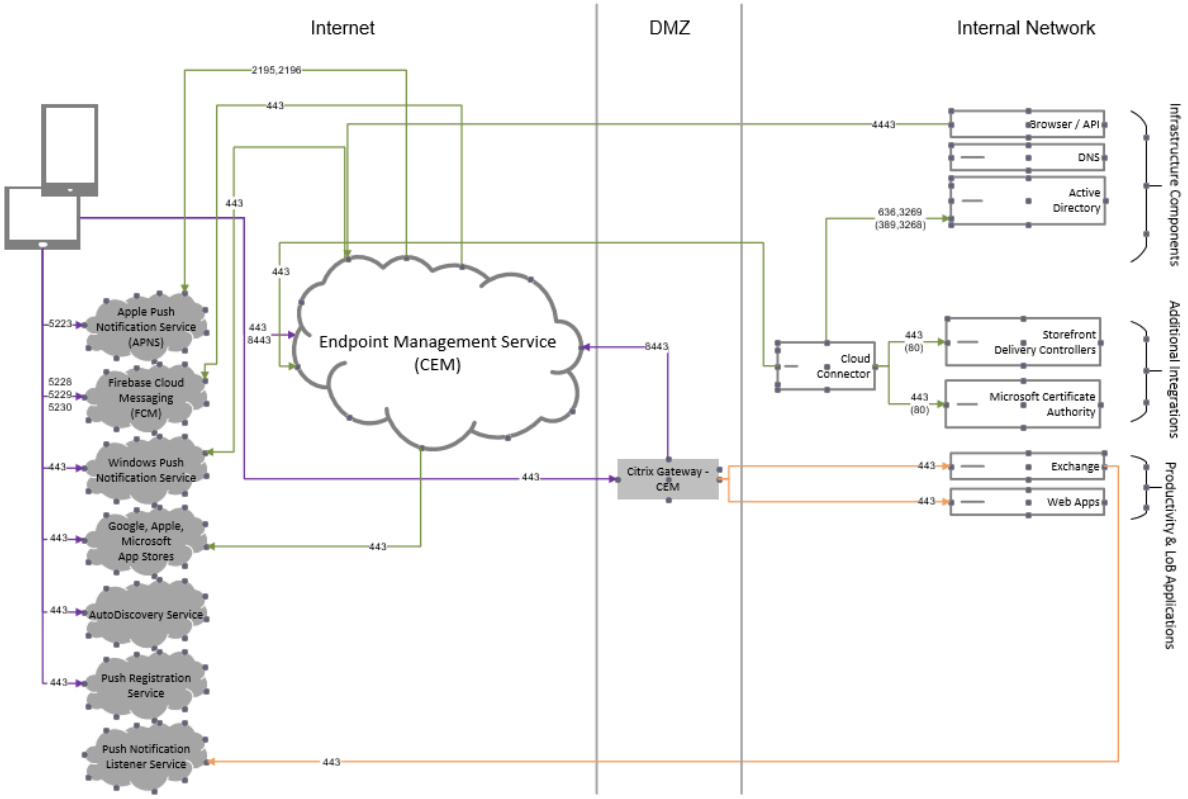
Firewallports

- Öffnen Sie Port 443 in Citrix Endpoint Management 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 eine 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.

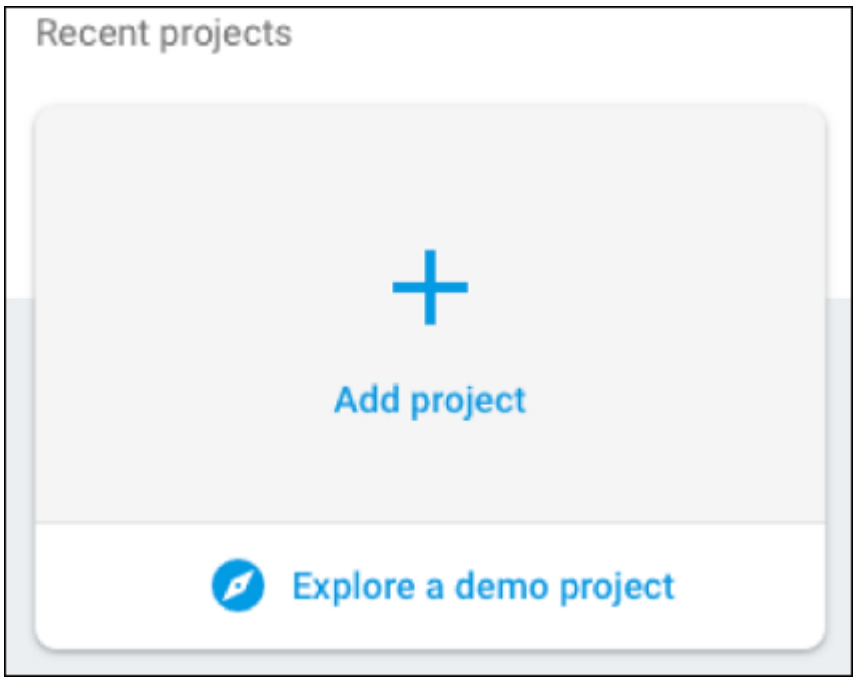


Konfigurieren Ihres Google-Kontos für FCM

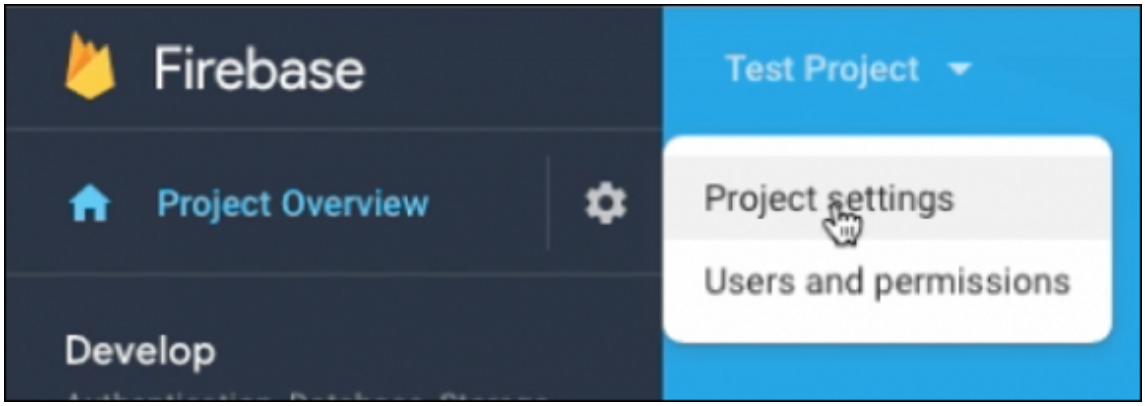
1. Melden Sie sich bei der folgenden URL mit den Anmeldeinformationen für Ihr Google Developer-Konto an:

   https://console.firebase.google.com/

2. Klicken Sie auf **Add project**.



3. Klicken Sie nach dem Erstellen des Projekts auf **Project settings**.



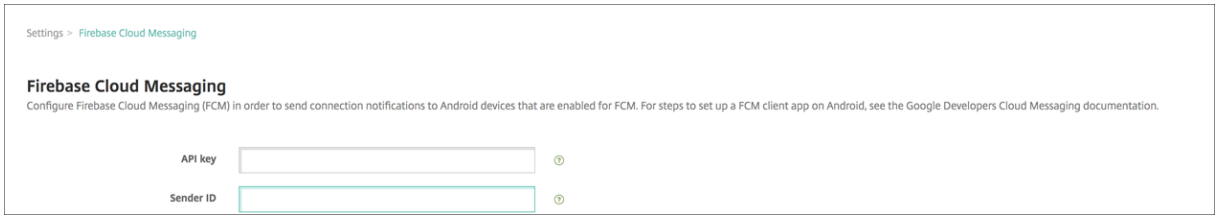
4. Klicken Sie auf die Registerkarte **Cloud Messaging** . Stellen Sie sicher, dass die Firebase Cloud Messaging API aktiviert ist, und klicken Sie auf **Manage Service Accounts**.
5. Kopieren Sie die Werte aus den Feldern **Key** und **OAuth 2 Client ID**. Wenn kein Schlüssel aufgeführt ist, klicken Sie auf das Ellipis unter **Aktionen**, um einen neuen Schlüssel hinzuzufügen.

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 Citrix Endpoint Management für FCM

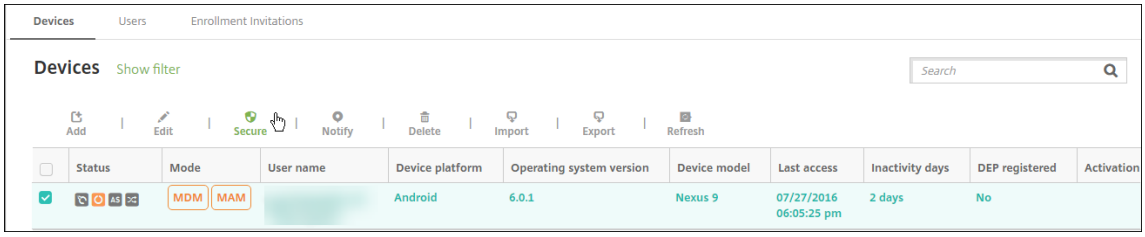
Gehen Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Firebase Cloud Messaging**.

- Bearbeiten Sie den **API-Schlüssel** und geben Sie den Firebase Cloud Messaging-**Schlüssel** ein, den Sie im letzten Schritt der Konfiguration von Firebase Cloud Messaging kopiert haben.
- Bearbeiten Sie die **Absender-ID** und geben Sie den Wert **OAuth 2 Client ID** ein, die Sie im vorherigen Vorgang kopiert haben.

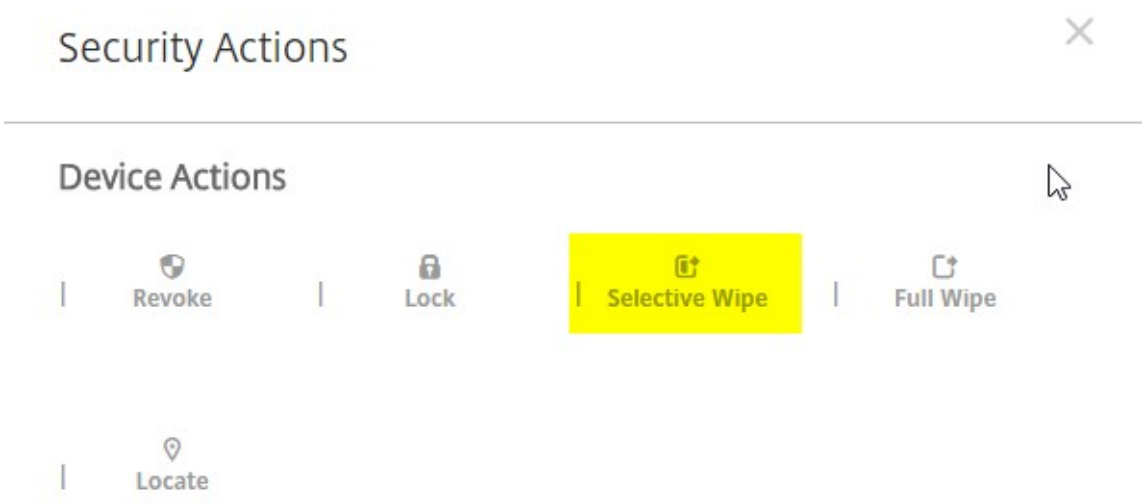


Testen der Konfiguration

1. Registrieren Sie ein Android-Gerät.
2. Lassen Sie das Gerät eine Zeit lang inaktiv, sodass die Verbindung mit Citrix Endpoint Management getrennt wird.
3. Klicken Sie in der Citrix Endpoint Management-Konsole 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.

Android SafetyNet

June 25, 2024

Sie können das Android SafetyNet-Features verwenden, um die Kompatibilität und Sicherheit von Android-Geräten zu bewerten, auf denen Citrix Secure Hub installiert ist. Android SafetyNet ist für MAM-Bereitstellungen nicht verfügbar.

Wenn diese Funktion aktiviert ist, prüft die SafetyNet Attestation API die Software- und Hardwareinformationen auf einem Gerät, um ein Profil dieses Geräts zu erstellen. Die API sucht dann in einer Liste von Gerätemodellen, die den Android-Kompatibilitätstest bestanden haben, nach demselben Profil. Die API verwendet diese Informationen außerdem, um zu ermitteln, ob Citrix Secure Hub von einer unbekannten Quelle geändert wurde.

Wenn die Android SafetyNet-Funktion aktiviert ist, sendet Citrix Secure Hub die SafetyNet Attestation API-Anfrage an die Google Play-Dienste und das Ergebnis wird an Citrix Endpoint Management zurückgemeldet. Citrix Endpoint Management aktualisiert dann die Geräteinformationen mit den Attestierungsergebnissen. Sie können automatisierte Aktionen festlegen, die die Ergebnisse verwenden, um Aktionen auf dem Gerät auszulösen.

Weitere Informationen zur Funktionsweise der SafetyNet Attestation API finden Sie in der Dokumentation für Android-Entwickler.

Schätzen der Anzahl der benötigten SafetyNet Attestation API-Anforderungen

SafetyNet Attestation API-Anforderungen werden gesendet:

- Wenn ein Gerät bei Citrix Endpoint Management registriert wird
- Wenn eine Citrix Secure Hub-Onlineauthentifizierung stattfindet

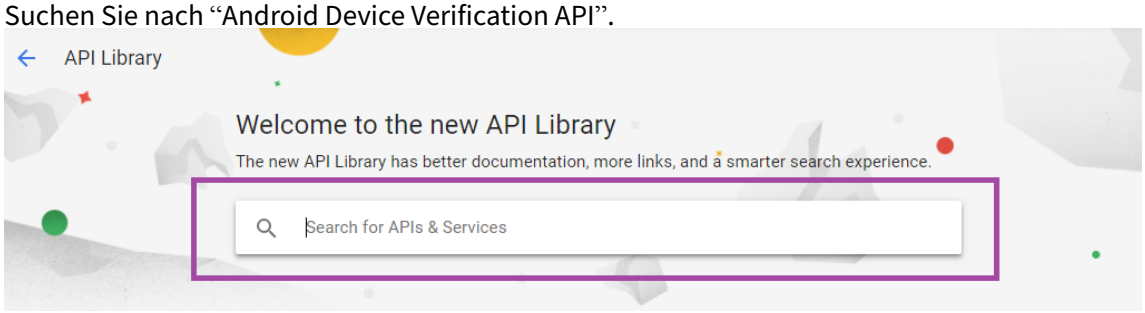
  Die Onlineauthentifizierung findet statt, wenn eine Serversitzung abläuft oder wenn ein Benutzer sich vom Server abmeldet und sich dann wieder anmeldet. Citrix Secure Hub fordert den Benutzer auf, Anmeldeinformationen zur Authentifizierung beim Server einzugeben.
- Wenn ein Gerät neu gestartet wird
- Nach einem bestimmten Zeitintervall, das Sie konfigurieren, zwischen 24 und 1.000 Stunden.

Wenn Ihre Citrix Endpoint Management-Bereitstellung mehr als 10.000 Anforderungen pro Tag benötigt, Füllen Sie dieses Anfragequotenformular aus.

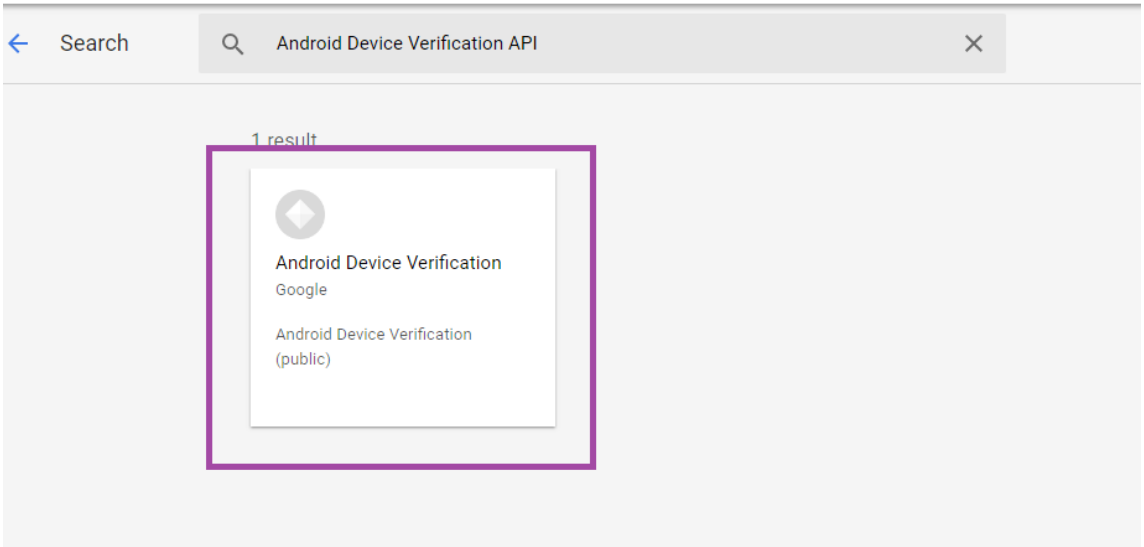
Abrufen des SafetyNet-API-Schlüssels

Um Android SafetyNet in Citrix Endpoint Management zu aktivieren, benötigen Sie den **SafetyNet-API**-Schlüssel.

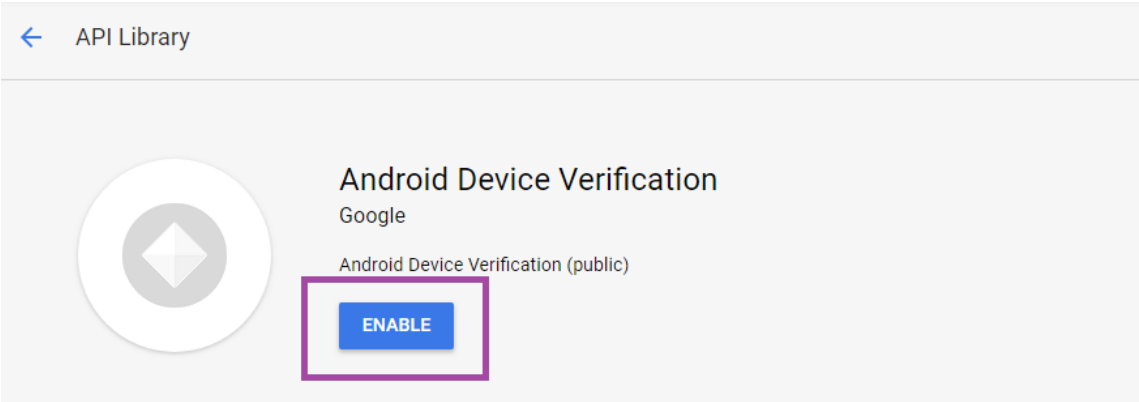
1. Melden Sie sich mit einem Google-Administratorkonto an der Google API-Konsole an.
2. Gehe zur Seite “Library”.
3. Suchen Sie nach “Android Device Verification API”.



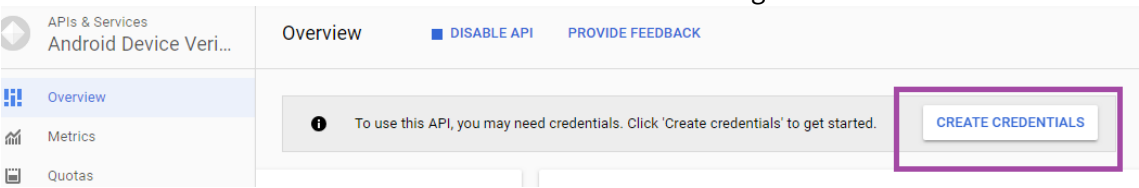
4. Klicken Sie auf **Android Device Verification API**.



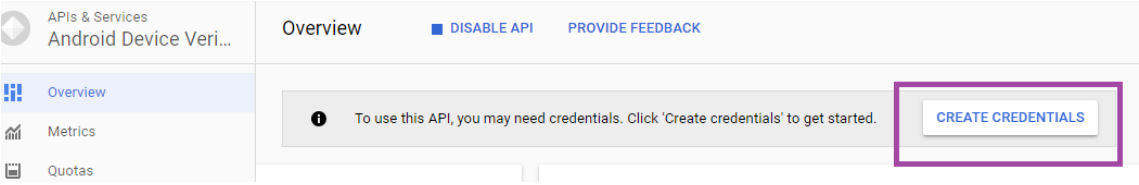
5. Wenn die API noch nicht aktiviert ist, klicken Sie auf **Enable**.



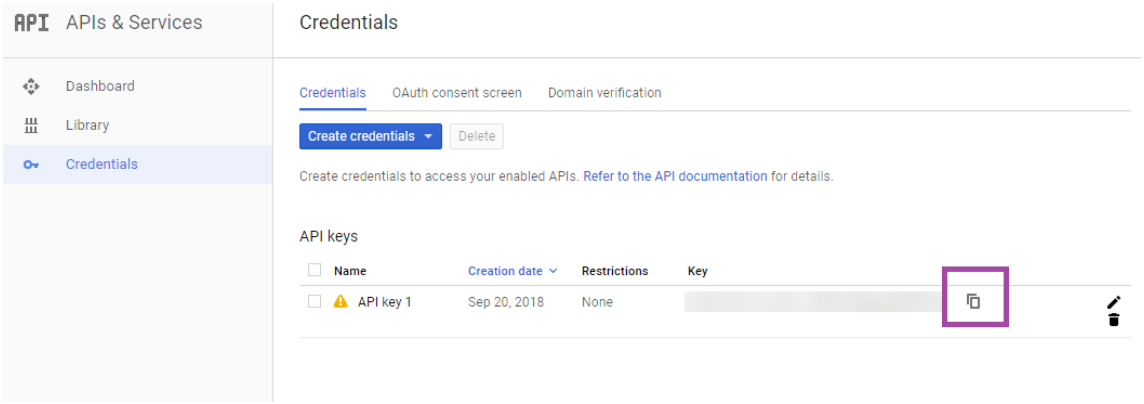
6. Klicken Sie auf **Verwalten**.
7. Klicken Sie auf **Create Credentials** um einen API-Schlüssel zu generieren.



8. Wählen Sie **Android Device Verification** und klicken Sie auf **What credentials to I need**. Klicken Sie dann auf **Done**.



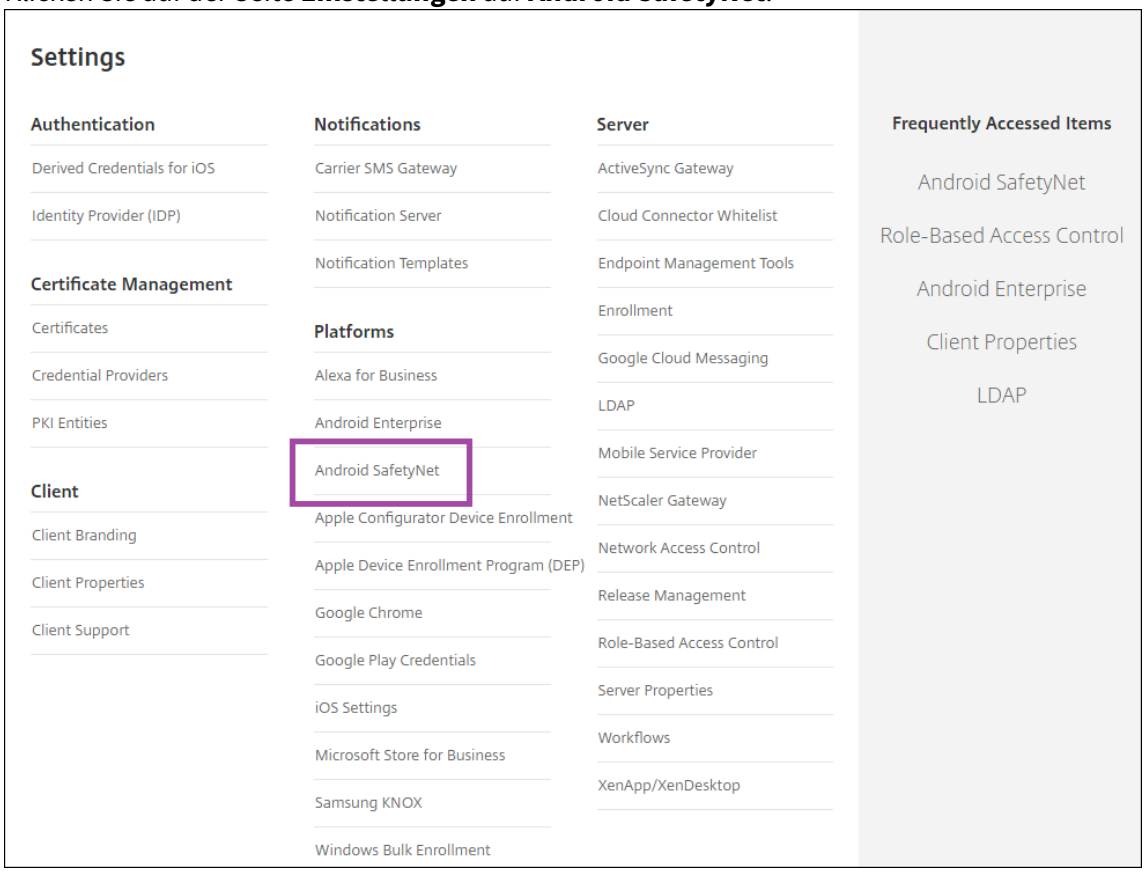
9. Klicken Sie auf der Seite **Credentials** auf das Kopierensymbol neben dem Schlüssel, um den Schlüssel zu kopieren.



10. Speichern Sie den Schlüssel, damit Sie ihn in der Citrix Endpoint Management-Konsole einfügen können, wenn Sie Android SafetyNet aktivieren.

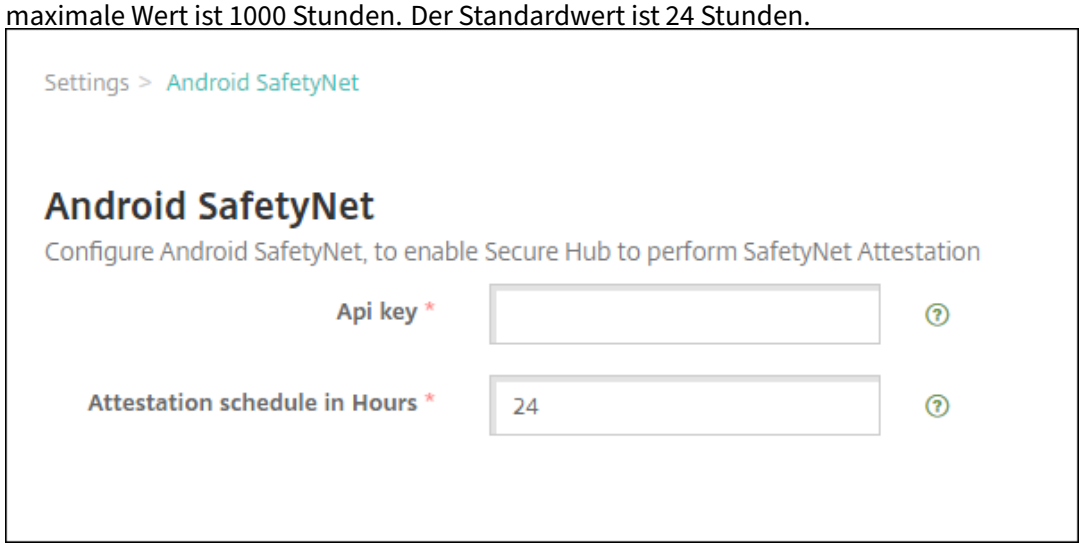
Aktivieren von Android SafetyNet

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf der Seite **Einstellungen** auf **Android SafetyNet**.



3. Konfigurieren Sie folgende Einstellungen:

- **API-Schlüssel**. Fügen Sie den SafetyNet-API-Schlüssel ein, den Sie über die Google-API-Konsole erhalten haben.
- **Nachweiszeitplan in Stunden**. Geben Sie das Intervall an, in dem die SafetyNet Attestation API Ihre Android-Geräte auswertet (in Stunden). Der Mindestwert ist 24 Stunden. Der maximale Wert ist 1000 Stunden. Der Standardwert ist 24 Stunden.

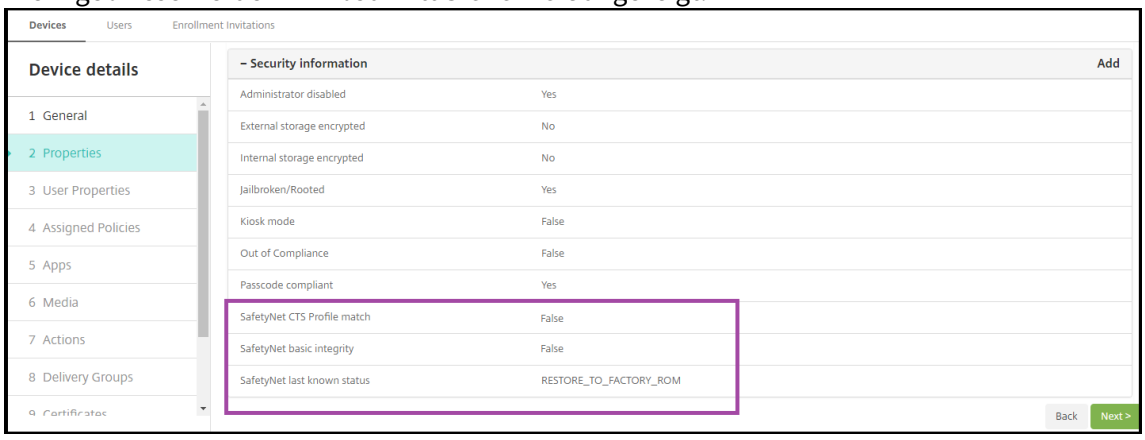


4. Klicken Sie auf **Speichern**.

Anzeigen der Android SafetyNet-Ergebnisse

Um die Ergebnisse der SafetyNet Attestation API für ein Gerät anzuzeigen:

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Verwalten > Geräte**.
2. Wählen Sie Android-Geräte aus, um die Ergebnisse der SafetyNet Attestation API anzuzeigen. Klicken Sie dann auf **Mehr anzeigen**.
3. Wählen Sie auf der Seite **Gerätedetails** die Option **Eigenschaften**.
4. Die Ergebnisse werden im Abschnitt **Sicherheit** angezeigt.



Die SafetyNet Attestation API gibt für jedes Gerät diese Statusmeldungen zurück:

- **SafetyNet CTS-Profilübereinstimmung:** Ist dieser Wert **Wahr**, hat das Gerät ein Profil, das mit einem übereinstimmt, das Android Compatibility Test Suite (CTS) bestanden hat. Ist der Wert **Falsch**, hat das Gerät kein Profil, das mit einem Profile übereinstimmt, das Android CTS bestanden hat.
- **SafetyNet-Basisintegrität:** Ist dieser Wert **Wahr**, hat die SafetyNet Attestation API keinen Nachweis gefunden, dass Citrix Secure Hub auf dem Gerät von einer unbekannten Quelle verändert wurde. Ist dieser Wert **Falsch**, wurde Citrix Secure Hub auf dem Gerät von einer unbekannten Quelle verändert.
- **Letzter bekannter Status von SafetyNet:** Dieser Wert zeigt den letzten bekannten SafetyNet-Status auf dem Gerät:
  - **Erfolg:** Die SafetyNet Attestation API hat keinen Nachweis gefunden, dass Citrix Secure Hub auf dem Gerät von einer unbekannten Quelle verändert wurde.
  - **LOCK_BOOTLOADER:** The user must lock the bootloader of the device. Citrix Secure Hub auf dem Gerät wurde von einer unbekannten Quelle geändert.
  - **RESTORE_TO_FACTORY_ROM:** Der Benutzer sollte das Gerät in einem sauberen Factory-ROM wiederherstellen. Citrix Secure Hub auf dem Gerät wurde von einer unbekannten Quelle geändert.

Play Integrity API

June 25, 2024

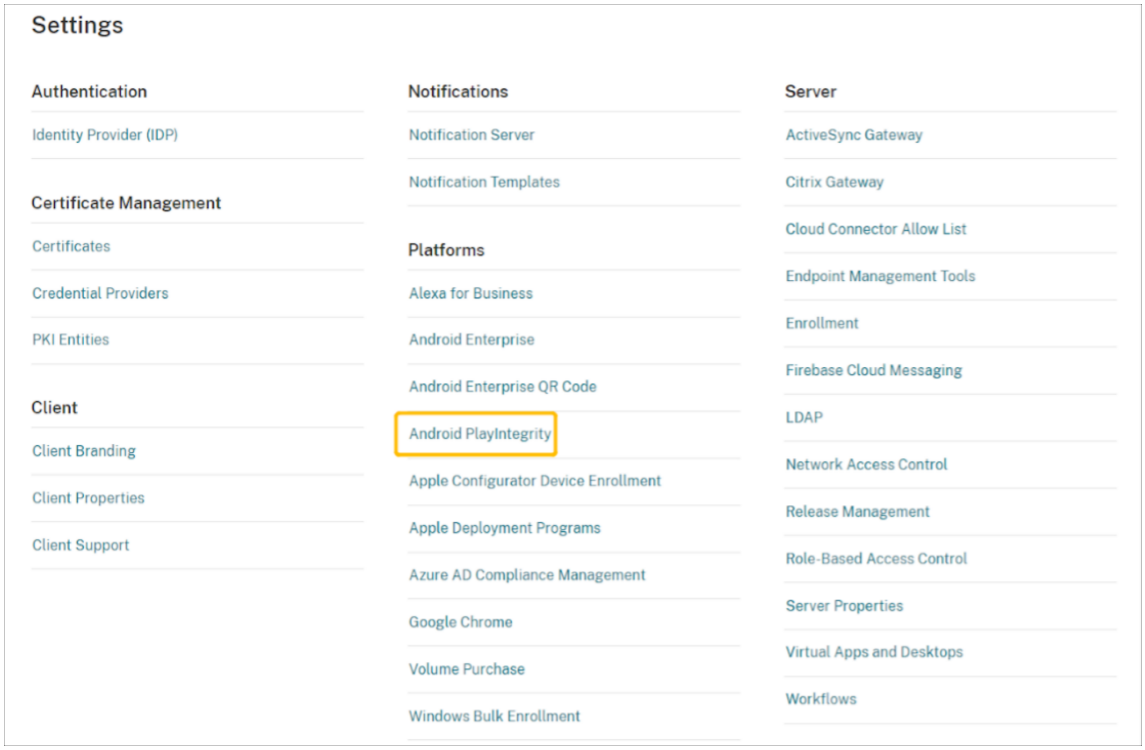
Die Play Integrity API schützt Ihre Apps und Spiele vor potenziell riskanten und betrügerischen Interaktionen, wie Cheaten und unbefugtem Zugriff, sodass Sie mit geeigneten Maßnahmen reagieren können, um Angriffe zu verhindern und Missbrauch zu reduzieren. Weitere Informationen finden Sie unter Play Integrity API.

Play Integrity API aktivieren

Gehen Sie wie folgt vor, um zur Play Integrity API zu wechseln.

1. Aktivieren Sie die *afw.safetynet.attestation.api*. Featureflag für veraltete Versionen für den angegebenen Citrix Endpoint Management-Server.

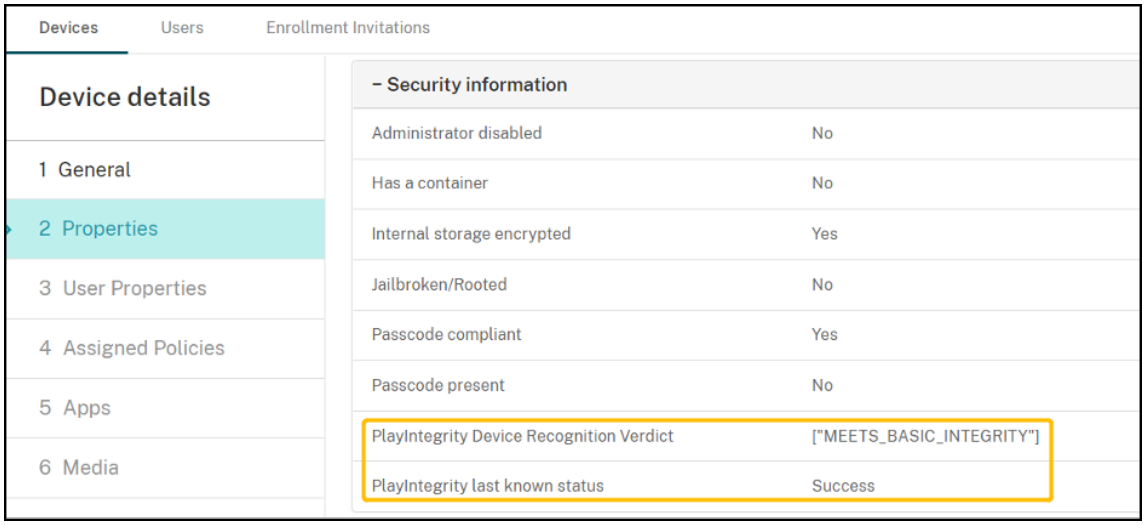
2. Wählen Sie in der Citrix Endpoint Management-Konsole auf der Seite **Einstellungen** die Option **Android PlayIntegrity** aus.



3. Geben Sie im Nachweiszeitplan einen Wert in das Feld “Stunden”ein. Dies ist die Intervallzeit, in der die PlayIntegrity Attestation API Ihr Gerät überprüft. Der Mindestwert ist 24 Stunden und der Höchstwert ist 1000 Stunden. Der Standardwert ist 24 Stunden. Klicken Sie auf **Speichern**.
4. Führen Sie ein Upgrade auf Citrix Secure Hub Android Version 23.7.0 durch. Melden Sie sich von Ihrem Gerät ab und melden Sie sich bei Citrix Secure Hub an, um den Nachweis per Play Integrity API auszulösen.

Ergebnisse des Play Integrity API-Nachweises anzeigen und analysieren

1. Gehen Sie in der Citrix Endpoint Management-Konsole zu **Verwalten > Geräte**.
2. Wählen Sie das Gerät aus, für das Sie die Play Integrity API-Nachweisergebnisse sehen möchten. Klicken Sie auf **Mehr anzeigen**.
3. Wählen Sie auf der Registerkarte **Geräte** die Option **Eigenschaften** aus. Die Ergebnisse werden im Abschnitt **Sicherheitsinformationen** angezeigt.



4. Der Play Integrity API-Nachweis gibt die folgenden Status zurück:

   - Wenn das Feld **PlayIntegrity - Geräteerkennungsbewertung**den Text **MEETS_BASIC_INTEGRITY** enthält, erfüllt Citrix Secure Hub, das auf dem Gerät ausgeführt wird, zumindest die grundlegende Systemintegrität.
   - Wenn das Feld **PlayIntegrity - Geräteerkennungsbewertung** nicht **MEETS_BASIC_INTEGRITY** enthält, bedeutet das, dass Citrix Secure Hub auf dem Gerät möglicherweise auf einer unbekannten Version von Android ausgeführt wird, einen entsperrten Bootloader hat oder möglicherweise nicht vom Hersteller zertifiziert wurde.
   - Wenn **Letzter bekannter Status von PlayIntegrity** den Status **Erfolg** aufweist, wurde der PlayIntegrity API-Nachweis erfolgreich ausgeführt.
   - Wenn **Letzter bekannter Status von PlayIntegrity** den Status **Fehler** aufweist, ist das Ausführen des PlayIntegrity API-Nachweises fehlgeschlagen.

> **Hinweis:**
>
> Der Administrator kann das Featureflag, das Ihnen die Nutzung von SafetyNet ermöglicht, vor der endgültigen Deaktivierung von SafetyNet Attestation (Ende November 2023) löschen.

Einschränkungen

1. Neu registrierte unternehmenseigene Einzweckgeräte (COSU-Geräte) und Geräte mit Gerätebesitzerprofil werden als nicht richtlinientreu gekennzeichnet, auch wenn die Geräte richtlinientreu sind.

   Die Play Integrity API gibt beim ersten Nachweis während der Gerätebesitzer-Registrierung einen leeren Wert zurück, wodurch das Gerät nicht richtlinientreu erscheint. Diese Einschränkung ist ein bekanntes Problem von Google. DPC Support Lib 20230418 wurde veröffentlicht, um dieses Problem zu beheben.

Das Update ist ab der Version 23.9.0 verfügbar. Verwenden Sie bis dahin diesen Workaround:

- Löschen Sie das Featureflag und verwenden Sie weiterhin die SafetyNet API, um die SafetyNet Attestation API weiterhin zu verwenden.
- Melden Sie sich ab und erneut an, um nach der Registrierung einen Nachweis auszulösen. Sie können auch auf den nächsten regelmäßigen Nachweis warten, der standardmäßig alle 24 Stunden erfolgt.

Dieses Problem tritt nur bei der Registrierung auf. Die Play Integrity API funktioniert nach der Registrierung einwandfrei.

2. Neu registrierte WPCOD-Geräte werden als nicht richtlinientreu markiert, auch wenn die Geräte richtlinientreu sind. Google überprüft dieses Problem.

Samsung

June 25, 2024

Samsung bietet mehrere mit Citrix Endpoint Management kompatible Lösungen.

Zum Steuern, wie und wann Android-Geräte eine Verbindung zum Citrix Endpoint Management-Dienst herstellen, verwenden Sie Firebase Cloud Messaging (FCM). Weitere Informationen finden Sie unter Firebase Cloud Messaging.

Registrierungsprofile bestimmen, ob Android-Geräte bei MAM, MDM oder MDM+MAM registriert werden, wobei im letzteren Modus die Benutzer ggf. MDM abwählen können. Citrix Endpoint Management unterstützt die folgenden Authentifizierungstypen für in MDM+MAM registrierte Android-Geräte. Weitere Informationen finden Sie in den folgenden Artikeln:

- Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken
- Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne
- Identitätsanbieter:
  - Authentifizierung mit Azure Active Directory über Citrix Cloud
  - Authentifizierung mit Okta über Citrix Cloud

Eine weitere, selten verwendete Authentifizierungsmethode ist das Clientzertifikat plus Sicherheitstoken. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX215200.

Die Android-Geräteverwaltung wird generell folgendermaßen begonnen:

1. Durchführen des Onboarding-Prozesses. Weitere Informationen finden Sie unter Onboarding und Einrichten von Ressourcen und Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen.

2. Auswahl und Konfigurieren der Registrierungsmethode. Weitere Informationen finden Sie unter Unterstützte Registrierungsmethoden.
3. Bereitstellen der Samsung-Lizenzschlüssel.
4. Konfigurieren der Samsung-Geräterichtlinien.
5. Einrichten von Sicherheitsaktionen für Apps und Geräte. Weitere Informationen finden Sie unter Sicherheitsaktionen.

Informationen zu unterstützten Betriebssystemen finden Sie unter Unterstützte Gerätebetriebssysteme.

Unterstützte Registrierungsmethoden

In der folgenden Tabelle werden die Registrierungsmethoden aufgelistet, die Citrix Endpoint Management für Android-Geräte unterstützt:

Methode	Unterstützt
Manuelle Registrierung	Ja
Registrierungseinladungen	Ja

Informationen zur Registrierung finden Sie unter Registrieren von Android-Geräten.

Bereitstellen der Samsung-Lizenzschlüssel

Samsung bietet ELM-Schlüssel (Enterprise License Management). Sie kaufen Samsung-Lizenzen von Samsung.

Konfigurieren der Samsung-Geräterichtlinien

Geräterichtlinien:

[App-Einschränkungen](/de-de/citrix-endpoint-management/policies/app-restrictions-policy.html)	[App-Deinstallation](/de-de/citrix-endpoint-management/policies/app-uninstall-policy.html)	[Browser](/de-de/citrix-endpoint-management/policies/browser-policy.html)

|[Apps in Samsung Container kopieren](/de-de/citrix-endpoint-management/policies/copy-apps-to-samsung-container-policy.html) |[Exchange](/de-de/citrix-endpoint-management/policies/exchange-policy.html) |[Passcode](/de-de/citrix-endpoint-management/policies/passcode-policy.html)|
| Einschränkungen | VPN|

Sicherheitsaktionen

Android unterstützt die folgenden Sicherheitsaktionen. Eine Beschreibung der einzelnen Sicherheitsaktionen finden Sie unter Sicherheitsaktionen.

App-Sperre	Apps löschen	Zertifikaterneuerung
Vollständig löschen	Orten	Sperren
Lock and Reset Password	Benachrichtigen	Widerrufen
Selektiv löschen		

> **Hinweis:**
>
> Bei Geräten mit Android 6.0 und höher muss der Benutzer zur Verwendung der Sicherheitsaktion **Orten** bei der Registrierung eine Standortberechtigung erteilt haben. Der Benutzer kann das Erteilen der Berechtigungen ablehnen. Wenn der Benutzer die Berechtigung bei der Registrierung nicht erteilt hat, fordert Citrix Endpoint Management sie beim Senden des Ortungsbefehls noch einmal an.

Netzwerkzugriffssteuerung (NAC)

June 25, 2024

Sie können mit Ihrer NAC-Lösung (Network Access Control) die Bewertung der Gerätesicherheit durch Citrix Endpoint Management für Android- und Apple-Geräte erweitern. Die NAC-Lösung vereinfacht und bewältigt anhand der Citrix Endpoint Management-Sicherheitsbewertung Authentifizierungsentscheidungen. Nach dem Konfigurieren des NAC-Geräts werden die in Citrix Endpoint Management konfigurierten Geräterichtlinien und NAC-Filter erzwungen.

Die Verwendung von Citrix Endpoint Management mit einer NAC-Lösung ermöglicht QoS und eine gezieltere Steuerung für Geräte innerhalb Ihres Netzwerks. Eine Zusammenfassung der Vorteile einer Integration von NAC mit Citrix Endpoint Management finden Sie unter Zugriffssteuerung.

Citrix unterstützt die folgenden Lösungen für die Integration mit Citrix Endpoint Management:

- NetScaler Gateway
- ForeScout

Citrix übernimmt keine Gewährleistung für die Integration anderer NAC-Lösungen.

Bei vorhandenem NAC-Gerät in Ihrem Netzwerk:

- Citrix Endpoint Management unterstützt NAC als Endpunktsicherheitsfeature für Geräte mit iOS, Android Enterprise und Android.
- Sie können Filter in Citrix Endpoint Management aktivieren, um Geräte anhand von Regeln oder Eigenschaften als (nicht) richtlinientreu für NAC festzulegen. Beispiel:
  - Wenn ein verwaltetes Gerät in Citrix Endpoint Management nicht die vorgegebenen Kriterien erfüllt, wird das Gerät in Citrix Endpoint Management als nicht richtlinientreu eingestuft. Ein NAC-Gerät blockiert dann nicht richtlinientreue Geräte in Ihrem Netzwerk.
  - Wenn auf einem verwalteten Gerät in Citrix Endpoint Management 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 NetScaler Gateway für NAC verwenden, können Sie durch Aktivieren von Split-Tunneling verhindern, dass das NetScaler Gateway Plug-In unnötigen Netzwerkverkehr an NetScaler Gateway sendet. Weitere Informationen zum Split-Tunneling finden Sie unter Konfigurieren von Split-Tunneling.

Unterstützte NAC-Richtlinientreuefilter

Citrix Endpoint Management unterstützt die folgenden NAC-Richtlinientreuefilter:

Anonyme Geräte: Prüft, ob ein Gerät im anonymen Modus ist. Diese Prüfung ist verfügbar, wenn Citrix Endpoint Management bei einer Wiederverbindung den Benutzer des Geräts nicht erneut authentifizieren kann.

Unzulässige Apps: Prüft, ob ein Gerät unzulässige Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind. Weitere 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 in der Regel von automatisierten Aktionen geändert oder von Drittanbietern, die Citrix Endpoint Management-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 von Citrix Endpoint Management verwaltet 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 Citrix Endpoint Management 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 Citrix Endpoint Management
3. Konfigurieren einer NAC-Lösung:

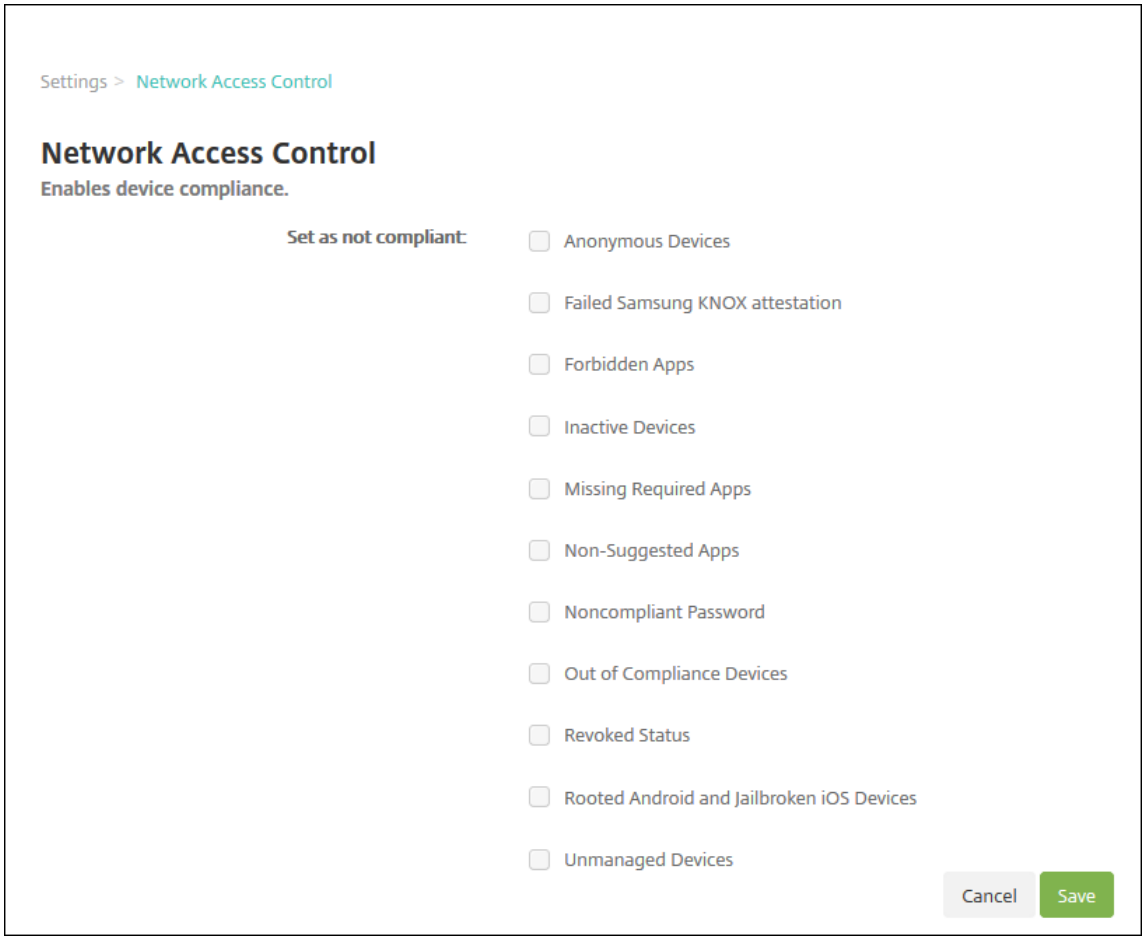
- NetScaler Gateway, beschrieben unter Aktualisieren der NetScaler Gateway-Richtlinien zur Unterstützung von NAC

  Erfordert Installation von Citrix SSO auf Geräten. Siehe NetScaler Gateway-Clients.

- ForeScout: Siehe ForeScout-Dokumentation.

Aktivieren von NAC-Filtern in Citrix Endpoint Management

1. Gehen Sie in der Citrix Endpoint Management-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 NetScaler 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 NetScaler Gateway mit einem der folgenden Merkmale aktualisiert:

- In Citrix Endpoint Management integriert.
- Oder für VPN eingerichtet, nicht Teil der Citrix Endpoint Management-Umgebung und kann Citrix Endpoint Management erreichen.

Führen Sie auf dem virtuellen VPN-Server in einem Konsolenfenster die nachfolgend aufgeführten Schritte aus. Die hier gezeigten FQDNs und 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_EndpointManagement -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_EndpointManagement -authnProfile xm_nac_prof
   ```

8. Überprüfen Sie die Verbindung von NetScaler Gateway zu einem Gerät, indem Sie Folgendes eingeben:

   ```
   curl -v -k https://<Endpoint Management_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 Citrix Endpoint Management. 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 Citrix Endpoint Management, indem Sie Folgendes eingeben: In diesem Beispiel lautet die Citrix Endpoint Management-IP-Adresse `10.207.87.82` und der FQDN ist `example.em.cloud.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.cloud.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\")"
    ```

    Bei Erfolg ist die Ausgabe für Citrix Endpoint Management-NAC `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 Citrix 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
    ```

iOS

June 25, 2024

Zum Verwalten von iOS-Geräten mit Citrix Endpoint Management 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. die Mobilgeräteverwaltung (MDM) abwählen können. Citrix Endpoint Management unterstützt die folgenden Authentifizierungstypen für iOS-Geräte in MDM+MAM. Weitere Informationen finden Sie in den folgenden Artikeln:

- Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken
- Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne
- Identitätsanbieter:
  - Authentifizierung mit Azure Active Directory über Citrix Cloud
  - Authentifizierung mit Okta über Citrix Cloud

> **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 Zertifikate hochladen.

Die iOS-Geräteverwaltung kann über folgendes Standardverfahren gestartet werden:

1. Durchführen des Onboarding-Prozesses. Weitere Informationen finden Sie unter Onboarding und Einrichten von Ressourcen und Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen.
2. Auswahl und Konfigurieren der Registrierungsmethode. Weitere Informationen finden Sie unter Unterstützte Registrierungsmethoden.
3. Konfigurieren von iOS-Geräterichtlinien.
4. Registrieren von iOS-Geräten.
5. Einrichten von Sicherheitsaktionen für Apps und Geräte. Weitere Informationen finden Sie unter Sicherheitsaktionen.

Informationen zu unterstützten Betriebssystemen finden Sie unter Unterstützte Gerätebetriebssysteme.

Kompatibilität mit iOS 14

Citrix Endpoint Management 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. Wählen Sie eine der folgenden Registrierungseinstellungen:

- **Apple-Benutzerregistrierung:** Bietet bei BYOD-Geräten ein Gleichgewicht zwischen Schutz von persönlichen Daten und Sicherheit für Unternehmensdaten. Dieser Registrierungsmodus ist als öffentliche Preview verfügbar. Wenden Sie sich an das Supportteam, um dieses Feature zu aktivieren.
- **Apple-Geräteregistrierung:** Für betreute iOS-Geräte mit separaten persönlichen und Unternehmensprofilen auf dem Gerät.
- **Geräte nicht verwalten:** Schließen Sie diese Geräte von MDM aus, wenn Sie nur Apps verwalten möchten.

Weitere Informationen zum Erstellen von Registrierungsprofilen finden Sie unter Registrierungsprofile.

Citrix Endpoint Management unterstützt die folgenden Registrierungsmethoden für iOS-Geräte:

Methode	Unterstützt
Apple Business Manager	Ja
Apple School Manager	Ja
Apple Configurator	Ja
Manuelle Registrierung	Ja
Registrierungseinladungen	Ja

Die Apple-Bereitstellungsprogramme umfassen Apple Business Manager (ABM) für Unternehmensorganisationen und Apple School Manager (ASM) für Bildungseinrichtungen. Weitere Informationen finden Sie unter Bereitstellen von Geräten über die Apple-Bereitstellungsprogramme.

Apple School Manager ist ein Apple-Bereitstellungsprogramm für Bildungseinrichtungen. Weitere Informationen finden Sie unter Integration von Apple Bildung-Features.

Verwenden Sie die Apple-Bereitstellungsprogramme für die Massenregistrierung von iOS-, iPadOS- und macOS-Geräten. Sie können diese Geräte direkt bei Apple, einem autorisierten Apple-Vertriebspartner oder einem Netzbetreiber erwerben. 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.

Verwaltete Apple-IDs

Die Benutzerregistrierung ist eng in verwaltete Apple-IDs integriert. Sie können eine verwaltete Apple-ID manuell mit ABM/ASM oder dynamisch mit Azure Active Directory (AAD) erstellen.

Erstellen Sie für die Authentifizierung ohne Verbund verwaltete Apple-IDs mit ABM/ASM, um ein Konto hinzuzufügen. Informationen zum Hinzufügen eines Kontos in ABM/ASM finden Sie in der Dokumentation von Apple unter `https://support.apple.com/guide/apple-business-manager/welcome/web` und für ASM unter `https://support.apple.com/guide/apple-school-manager/welcome/web`. Wir empfehlen Folgendes, um zusätzliche Schritte zu vermeiden, wenn Benutzer sich registrieren:

- Verwenden Sie beim Erstellen einer verwalteten Apple-ID eine E-Mail-Adresse, die der geschäftlichen E-Mail-Adresse entspricht.
- Legen Sie für die Benutzerrolle **Staff** fest.
- Veranlassen Sie die Benutzer, ihr Kennwort manuell zu ändern, bevor sie sich registrieren. Teilen Sie den Benutzern mit, dass empfohlen wird, dasselbe Kennwort zu verwenden wie für das Unternehmenskonto.

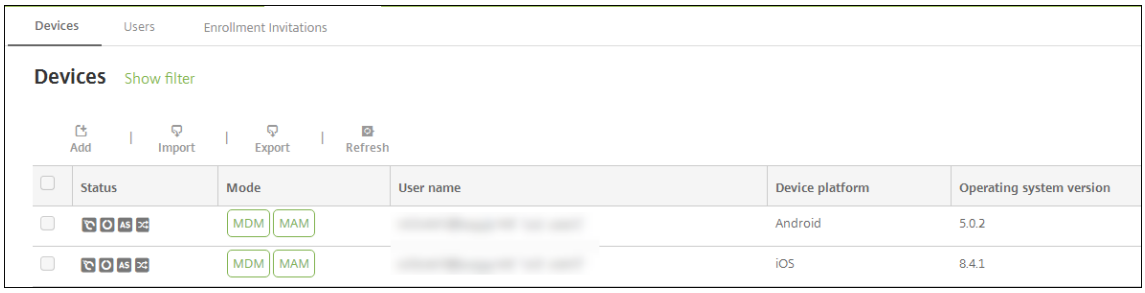
Zum dynamischen Erstellen verwalteter Apple-IDs konfigurieren Sie Citrix Cloud für die Verwendung von AAD als Identitätsanbieter. Weitere Informationen zum Konfigurieren von Citrix Cloud für die Verwendung von AAD finden Sie unter Authentifizierung mit Azure Active Directory über Citrix Cloud. Konfigurieren Sie außerdem die Verbundauthentifizierung in ABM/ASM. Weitere Informationen zum Konfigurieren der Verbundauthentifizierung in ABM oder ASM finden Sie im Apple Business Manager-Benutzerhandbuch oder im Apple School Manager-Benutzerhandbuch.

Wenn Sie verwaltete Apple-IDs manuell erstellen, können Sie eine benutzerdefinierte Domäne statt der Standarddomäne konfigurieren. Die von Ihnen konfigurierte benutzerdefinierte Domäne ersetzt die vorhandene Domäne. Beispiel: Ihre geschäftlichen E-Mail-Adressen haben das Format `first.last@company.com`, Sie möchten jedoch stattdessen `mycompany.website.com` als Domäne für die verwaltete Apple-ID verwenden. Beim Erstellen der verwalteten Apple-ID in ABM/ASM ergibt sich die E-Mail-Adresse `first.last@mycompany.website.com`.

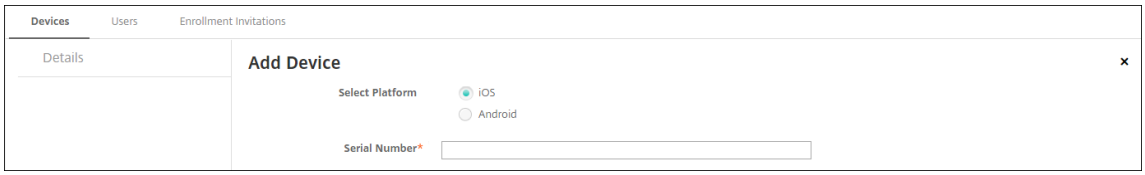
Manuelles Hinzufügen eines iOS-Geräts

Führen Sie folgende Schritte aus, um ein iOS-Gerät manuell hinzuzufügen (beispielsweise zu Testzwecken).

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.



2. Klicken Sie auf **Hinzufügen**. Die Seite **Gerät hinzufügen** wird angezeigt.



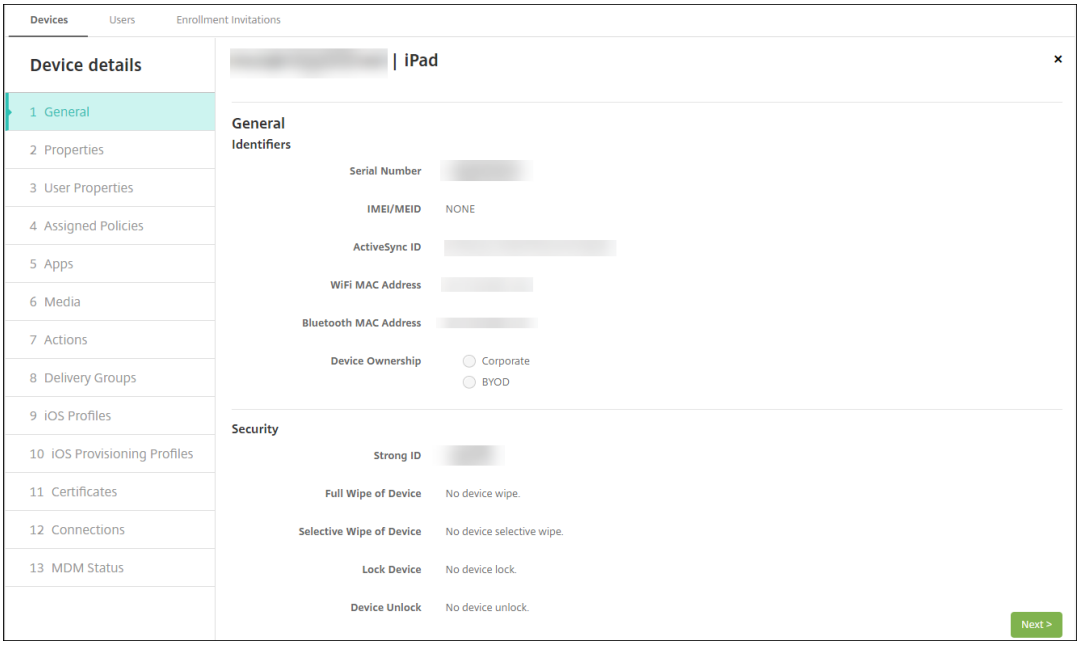
3. Konfigurieren Sie folgende Einstellungen:

   - **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 Citrix Endpoint Management 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. Citrix Endpoint Management löscht das Element sofort.

7. Die verbleibenden Abschnitte mit **Gerätedetails** enthalten Zusammenfassungen 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 bereitgestellten, ausstehenden und fehlgeschlagenen Richtlinien an. Für die einzelnen Richtlinien werden Name, Typ und letzte Bereitstellung angezeigt. Ermöglicht das Zurücksetzen des Bereitstellungsstatus auf "Ausstehend"und die erneute Bereitstellung der vom Benutzer entfernten Richtlinien.
- **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 die Interaktion von Citrix Endpoint Management mit Geräten zu konfigurieren, auf denen iOS oder iPadOS ausgeführt wird. In dieser Tabelle sind alle für iOS- und iPadOS-Geräte verfügbaren Geräterichtlinien aufgeführt.

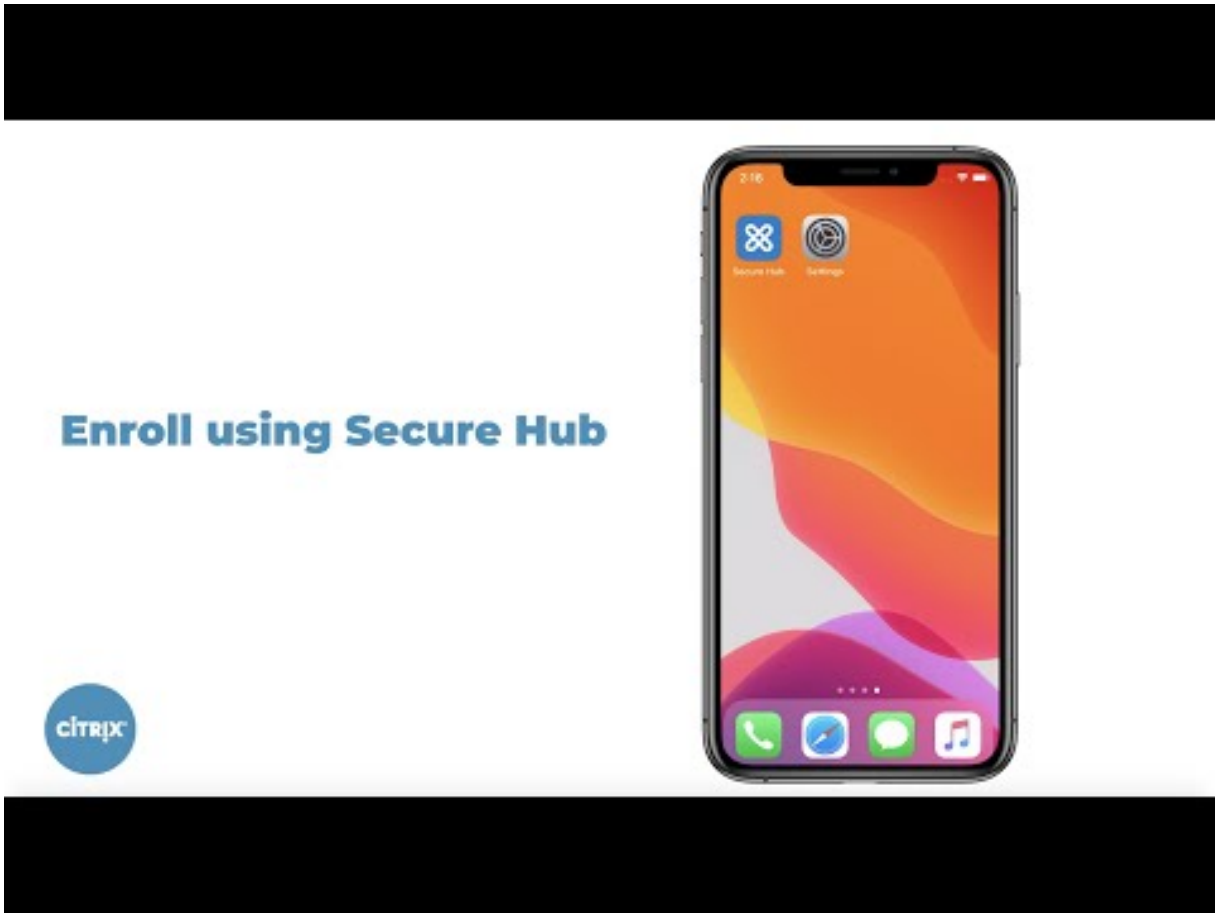
[AirPlay-Synchronisierung](/de-de/citrix-endpoint-management/policies/airplay-mirroring-ios-policy.html)	[AirPrint](/de-de/citrix-endpoint-management/policies/airprint-ios-policy.html)

|[APN](/de-de/citrix-endpoint-management/policies/apn-policy.html#ios-settings) |
|[App-Zugriff](/de-de/citrix-endpoint-management/policies/app-access-policy.html) |[App-Attribute](/de-de/citrix-endpoint-management/policies/app-attributes-policy.html) |[App-Konfiguration](/de-de/citrix-endpoint-management/policies/app-configuration-policy.html#ios-settings) |
|[App-Bestand](/de-de/citrix-endpoint-management/policies/app-inventory-policy.html) |[App-Sperre](/de-de/citrix-endpoint-management/policies/app-lock-policy.html#ios-settings) |[App-Deinstallation](/de-de/citrix-endpoint-management/policies/app-uninstall-policy.html#ios-and-macos-settings) |
|[App-Benachrichtigungen](/de-de/citrix-endpoint-management/policies/apps-notifications-policy.html) |[Bluetooth](/de-de/citrix-endpoint-management/policies/bluetooth-policy.html)
|[Kalender (CalDAV)](/de-de/citrix-endpoint-management/policies/calendar-caldav-ios-policy.html)
|[Mobiltelefon](/de-de/citrix-endpoint-management/policies/cellular-policy.html) |[Kontakte (CardDAV)](/de-de/citrix-endpoint-management/policies/contacts-carddav-ios-policy.html)
|[Anmeldeinformationen](/de-de/citrix-endpoint-management/policies/credentials-policy.html#ios-settings)
|[Gerätename](/de-de/citrix-endpoint-management/policies/device-name-policy.html) |[Bildungseinrichtung - Konfiguration](/de-de/citrix-endpoint-management/policies/education-configuration-policy.html)
|[Exchange](/de-de/citrix-endpoint-management/policies/exchange-policy.html#ios-settings)
|[Schriftart](/de-de/citrix-endpoint-management/policies/font-policy.html) |[Layout für Homebildschirm](/de-de/citrix-endpoint-management/policies/home-screen-layout-policy.html)
|[Importieren von iOS- und macOS-Profilen](/de-de/citrix-endpoint-management/policies/import-ios-mac-os-x-profile-policy.html)
|[LDAP](/de-de/citrix-endpoint-management/policies/ldap-policy.html) |[Standort](/de-de/citrix-endpoint-management/policies/location-policy.html) |[Meldung auf Sperrbildschirm](/de-de/citrix-endpoint-management/policies/lock-screen-message-policy.html)
|[Mail](/de-de/citrix-endpoint-management/policies/mail-policy.html) |[Verwaltete Domänen](/de-de/citrix-endpoint-management/policies/managed-domains-policy.html) |[Maximale Anzahl residenter Benutzer](/de-de/citrix-endpoint-management/policies/maximum-resident-users-policy.html)
|[MDM-Optionen](/de-de/citrix-endpoint-management/policies/mdm-options-policy.html) |[Netzwerk](/de-de/citrix-endpoint-management/policies/network-policy.html#ios-settings)|[Netzwerknutzung](/de-de/citrix-endpoint-management/policies/network-usage-policy.html)
|[Informationen zum Unternehmen](/de-de/citrix-endpoint-management/policies/organization-info-policy.html) |[OS-Update](/de-de/citrix-endpoint-management/policies/control-os-updates.html#ios-settings) |[Passcode](/de-de/citrix-endpoint-management/policies/passcode-policy.html#ios-settings)
|[Passcodesperre - Kulanzzeitraum](/de-de/citrix-endpoint-management/policies/passcode-lock-grace-period.html) |[Persönlicher Hotspot](/de-de/citrix-endpoint-management/policies/personal-hotspot-policy.html) |[Profilentfernung](/de-de/citrix-endpoint-management/policies/profile-

removal-policy.html)
|[Provisioningprofil](/de-de/citrix-endpoint-management/policies/provisioning-profile-policy.html)
|[Entfernen des Provisioningprofils](/de-de/citrix-endpoint-management/policies/provisioning-profile-removal-policy.html) |[Proxy](/de-de/citrix-endpoint-management/policies/proxy-policy.html)
|[Einschränkungen](/de-de/citrix-endpoint-management/policies/restrictions-policy.html#ios-settings) |[Roaming](/de-de/citrix-endpoint-management/policies/roaming-policy.html) |[SCEP](/de-de/citrix-endpoint-management/policies/scep-policy.html)
|[SSO-Konto](/de-de/citrix-endpoint-management/policies/sso-account-policy.html) |[Store](/de-de/citrix-endpoint-management/policies/store-policy.html) |[Abonnierte Kalender](/de-de/citrix-endpoint-management/policies/subscribed-calendars-policy.html)
|[AGB](/de-de/citrix-endpoint-management/policies/terms-and-conditions-policy.html) |[VPN](/de-de/citrix-endpoint-management/policies/vpn-policy.html#ios-settings) |[Wallpaper](/de-de/citrix-endpoint-management/policies/wallpaper-policy.html)
|Webinhaltsfilter |Webclip | | |

Registrieren von iOS-Geräten

Dieser Abschnitt zeigt, wie Benutzer iOS-Geräte (12.2 oder höher) in Citrix Endpoint Management registrieren. Weitere Informationen zur iOS-Registrierung finden Sie in folgendem Video:

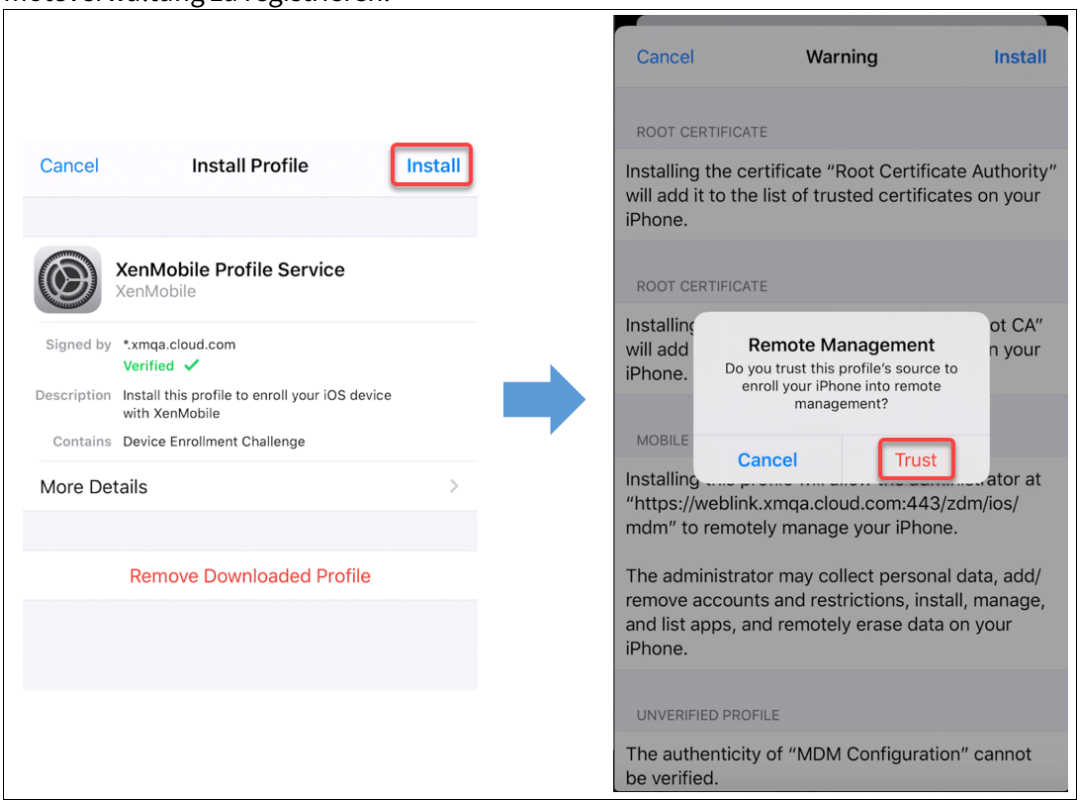


1. Rufen Sie auf dem iOS-Gerät den Apple-Store auf, laden Sie die Citrix Secure Hub-App herunter und tippen Sie auf die App.
2. Wenn Sie aufgefordert werden, die App zu installieren, tippen Sie auf **Weiter** und dann auf **Installieren**.
3. Wenn Citrix Secure Hub installiert ist, tippen Sie auf **Öffnen**.
4. Geben Sie Ihre geschäftlichen Anmeldeinformationen ein, z. B. den Namen des Citrix Endpoint Management-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 Citrix Endpoint Management 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 in den Geräteeinstellungen das XenMobile-Profil.

    - 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 Citrix 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

Die Geräteregistrierung für iOS unterstützt die folgenden Sicherheitsaktionen. Eine Beschreibung der einzelnen Sicherheitsaktionen finden Sie unter Sicherheitsaktionen.

- Aktivierungssperre umgehen
- App-Sperre
- Apps löschen
- ASM-Aktivierungssperre
- Zertifikaterneuerung
- Einschränkungen deaktivieren
- Modus "Verloren"aktivieren/deaktivieren

- Tracking aktivieren/deaktivieren
- Vollständig löschen
- Orten
- Sperren
- Klingeln
- AirPlay-Synchronisierung anfordern/beenden
- Neustart/Herunterfahren
- Wiederrufen/Autorisieren
- Selektiv löschen
- Entsperren

Die Benutzerregistrierung für iOS unterstützt die folgenden Sicherheitsaktionen:

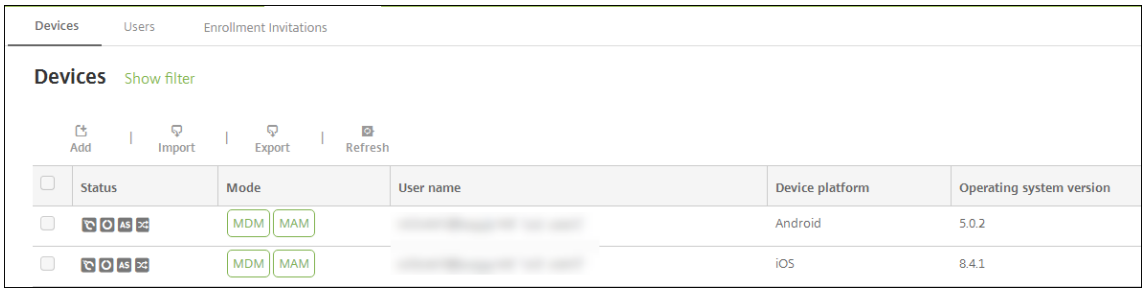
- Widerrufen
- Sperren
- Selektiv löschen
- Zertifikaterneuerung

Sperren von iOS-Geräten

Sie können ein verlorenes iOS-Gerät sperren und eine entsprechende Nachricht und Telefonnummer auf dem Sperrbildschirm anzeigen lassen.

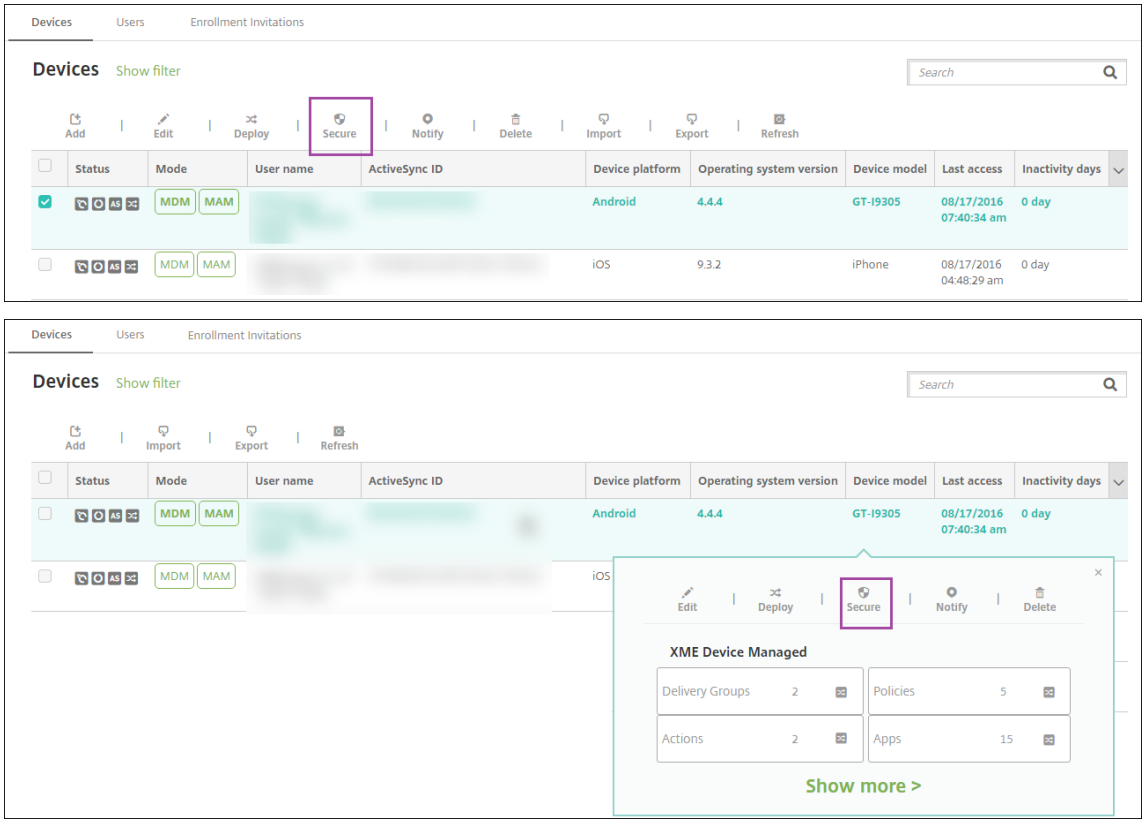
Zum Anzeigen einer Nachricht und Telefonnummer auf einem gesperrten Gerät muss die Richtlinie Passcode in der Citrix Endpoint Management-Konsole auf **wahr** festgelegt werden. Alternativ können Benutzer den Passcode auf dem Gerät auch manuell aktivieren.

1. Klicken Sie auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.

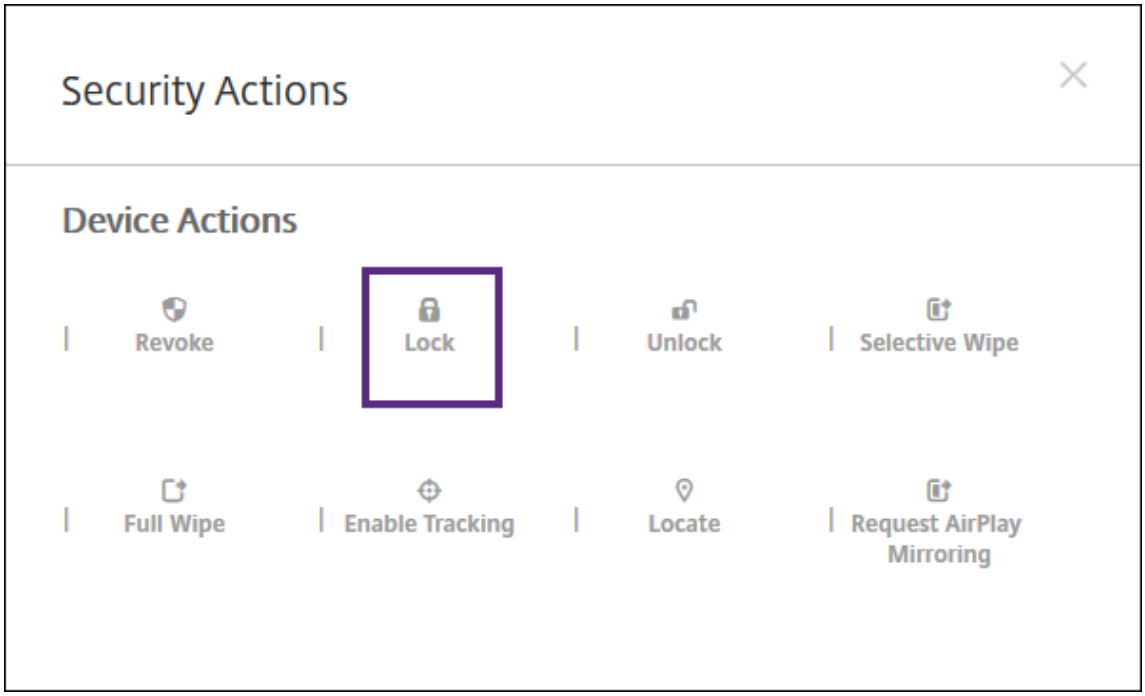


2. Wählen Sie das iOS-Gerät aus, das Sie sperren möchten.

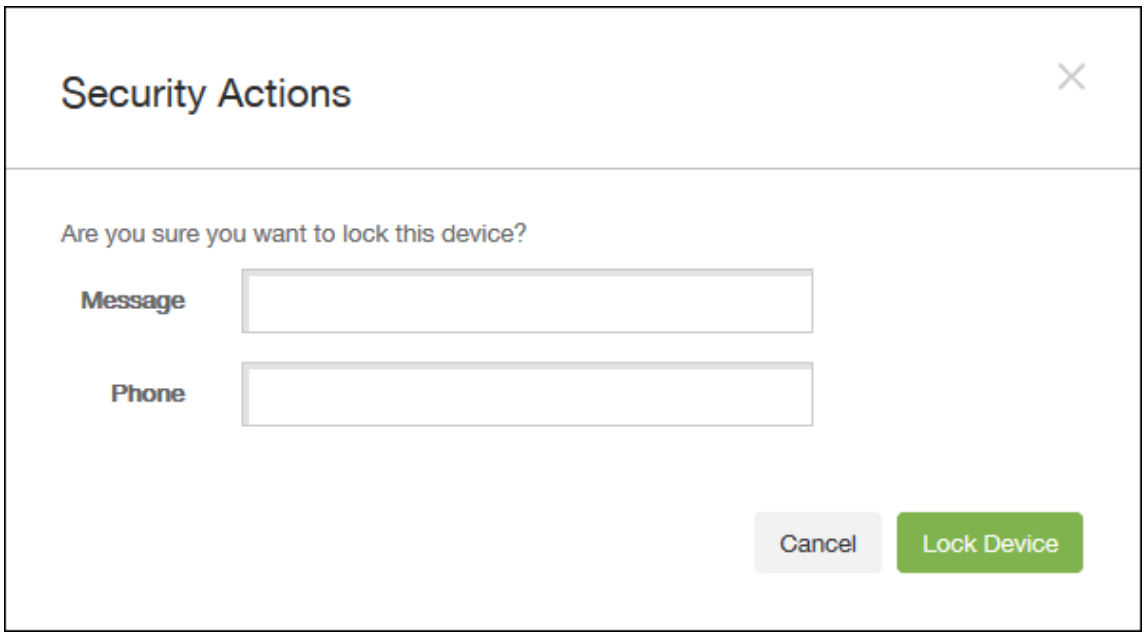
   Aktivieren Sie das Kontrollkästchen neben einem Gerät, um das Menü mit den Optionen oberhalb der Liste anzuzeigen. Klicken Sie an eine andere Stelle in der Liste, um das Menü mit den Optionen rechts daneben anzuzeigen.



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.

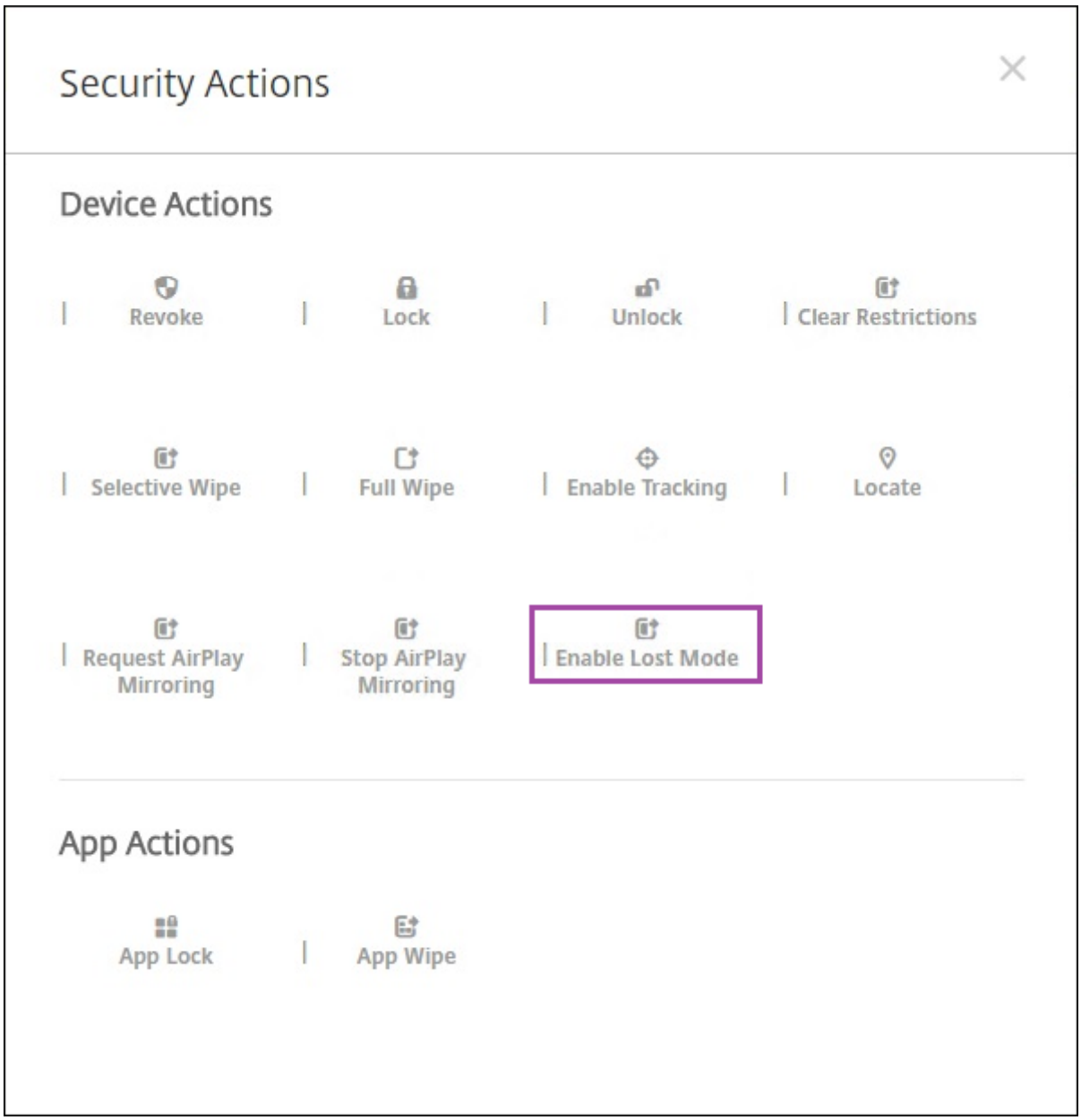
6. Klicken Sie auf **Gerät sperren**.

Versetzen von iOS-Geräten in den Modus "Verloren"

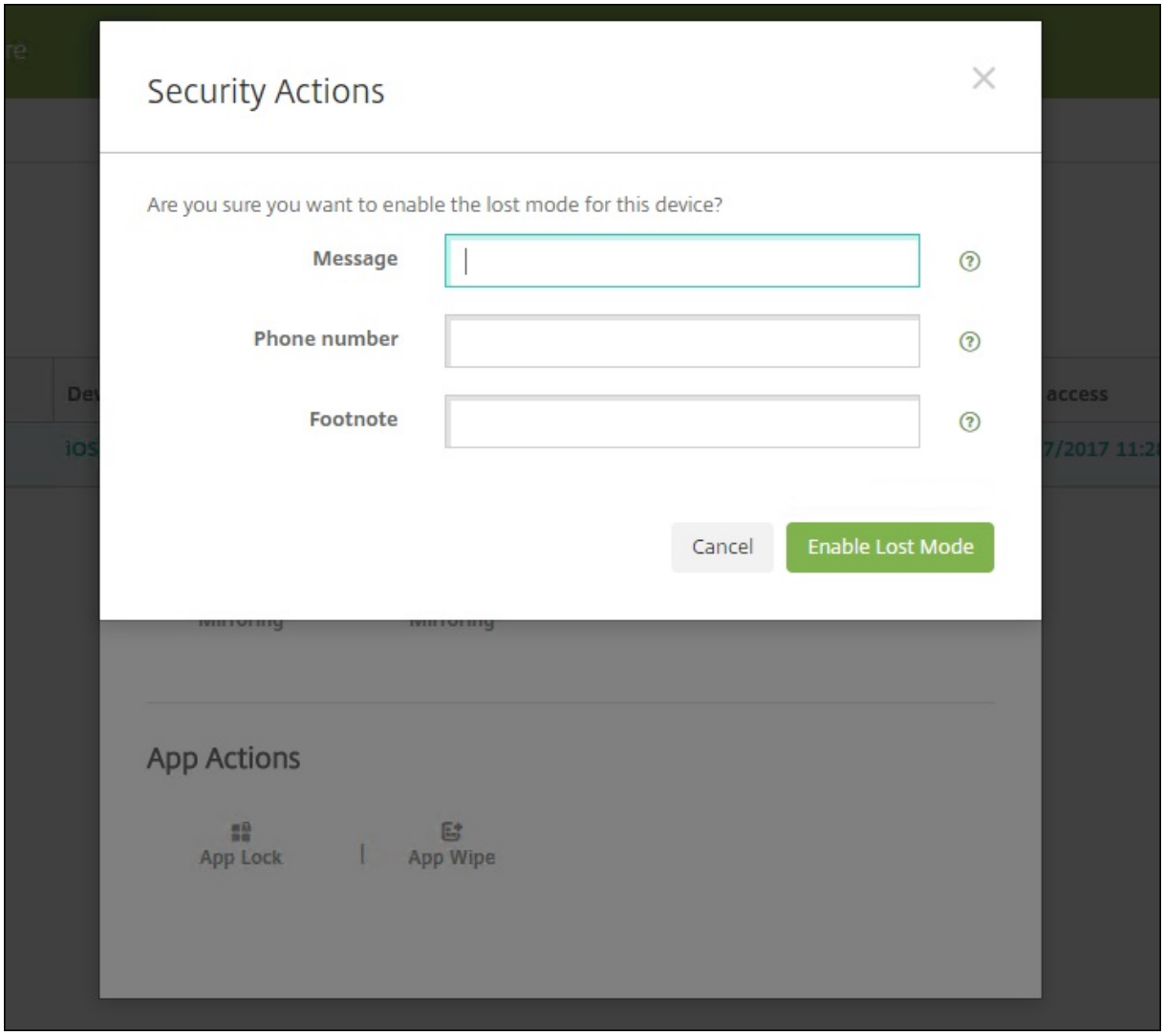
Die Geräteeigenschaft "Citrix Endpoint Management-Modus 'Verloren'"versetzt iOS-Geräte in den Modus "Verloren". Im Gegensatz zum von Apple verwalteten Modus "Verloren"muss ein Benutzer beim Modus "Verloren"in Citrix Endpoint Management keine der folgenden Aktionen ausführen, um sein Gerät zu suchen: Konfigurieren der Einstellung **Find My iPhone/iPad** oder Aktivieren der Ortungsdienste für Citrix Secure Hub.

Im Citrix Endpoint Management-Modus "Verloren"kann ein Gerät nur über Citrix Endpoint Management entsperrt werden. (Wenn Sie hingegen das Citrix Endpoint Management-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**.

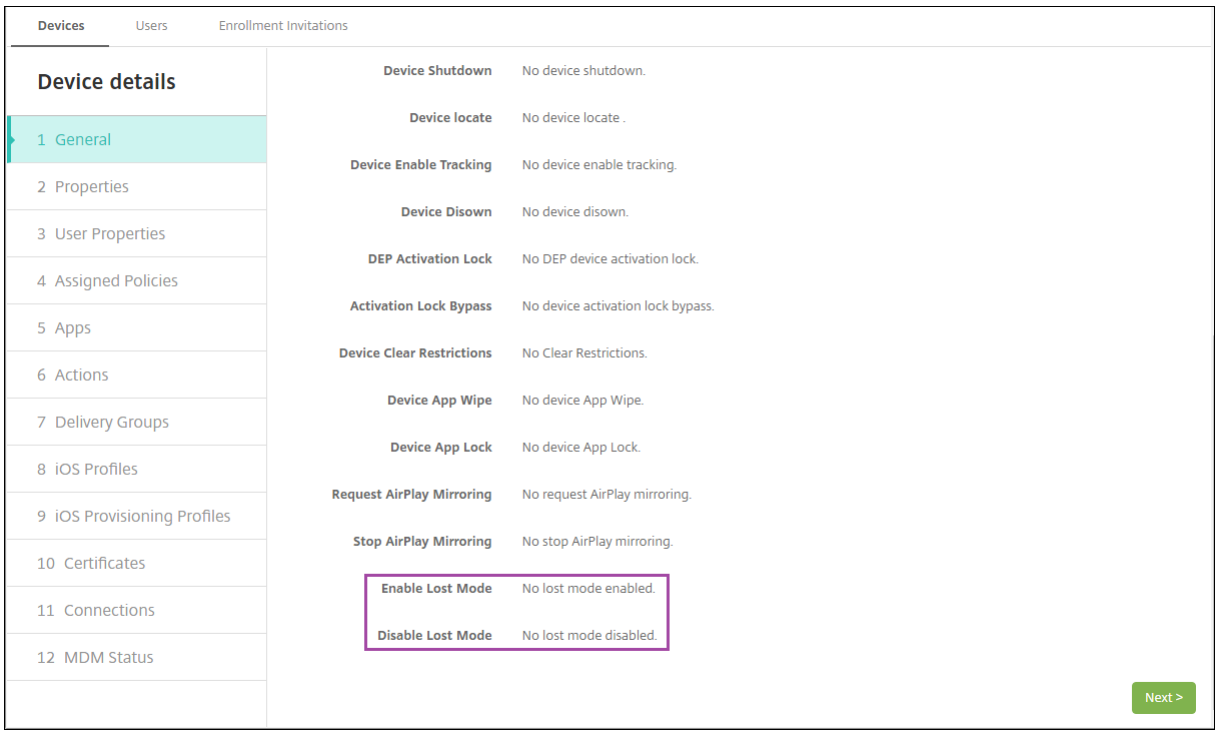


Wenn Sie auf **Modus 'Verloren' aktivieren** klicken, geben Sie die Informationen ein, die auf dem Gerät angezeigt werden sollen, wenn es im Modus "Verloren" ist.

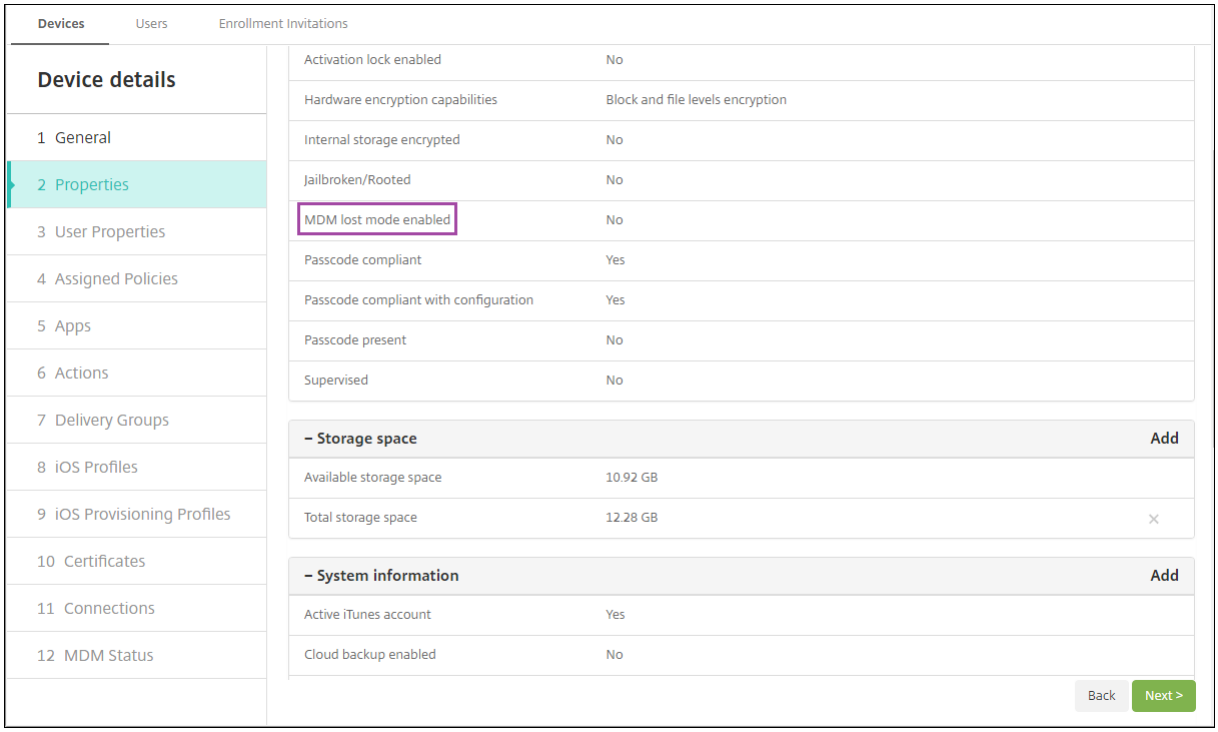


Verwenden Sie eine der folgenden Methoden, um den Status des Modus “Verloren”zu überprüfen:

- Überprüfen Sie im Fenster **Sicherheitsaktionen**, ob die Schaltfläche auf **Modus ‘Verloren’ deaktivieren** festgelegt 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 Citrix Endpoint Management-Modus "Verloren"auf iOS-Geräten aktivieren, ändert sich die Citrix Endpoint Management-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 Aktivieren der Aktivierungssperre müssen Sie die Citrix Endpoint Management-Geräterichtlinie "MDM-Optionen"konfigurieren und bereitstellen. Sie können dann ein Gerät über die Citrix Endpoint Management-Konsole ohne die Apple-Anmeldeinformationen des Benutzers verwalten. Um die erforderliche Eingabe der Apple-Anmeldeinformationen bei einer Aktivierungssperre zu umgehen, geben Sie die Sicherheitsaktion "Aktivierungssperre umgehen"auf der Citrix Endpoint Management-Konsole ein.

Nehmen wir folgendes Beispiel: Ein Benutzer bringt ein verlorenes Telefon zurück oder möchte ein Gerät vor oder nach einem vollständigen Löschen einrichten. Wenn das Telefon zur Eingabe der Anmeldeinformationen für das Apple App Store-Konto auffordert, umgehen Sie diesen Schritt, indem Sie 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 Citrix Endpoint Management 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 Citrix Endpoint Management löschen. Sie oder der Benutzer können sich direkt an den Apple-Support wenden, um das Gerät entsperren zu lassen.
- Während einer Hardwareinventur ruft Citrix Endpoint Management den Code zum Umgehen der Aktivierungssperre von einem Gerät ab. Wenn ein Umgehungscode verfügbar ist, wird er vom Gerät an Citrix Endpoint Management gesendet. Um den Umgehungscode dann vom Gerät zu entfernen, aktivieren Sie auf der Citrix Endpoint Management-Konsole die Sicherheitsaktion "Aktivierungssperre umgehen". Damit haben Citrix Endpoint Management 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 durch eine der folgenden Methoden entsperren:
  - Geben Sie auf dem Gerät manuell die Anmeldeinformationen des iCloud-Kontos ein.
  - Lassen Sie das Feld "Benutzername"leer und geben Sie den Umgehungscode im Feld "Kennwort"ein. 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

June 25, 2024

Zum Verwalten von macOS-Geräten mit Citrix Endpoint Management 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.

Citrix Endpoint Management registriert macOS-Geräte in MDM. Citrix Endpoint Management 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 Zertifikate hochladen.

Die macOS-Geräteverwaltung kann über folgendes Standardverfahren gestartet werden:

1. Durchführen des Onboarding-Prozesses. Weitere Informationen finden Sie unter Onboarding und Einrichten von Ressourcen und Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen.
2. Auswahl und Konfigurieren der Registrierungsmethode. Weitere Informationen finden Sie unter Unterstützte Registrierungsmethoden.
3. Konfigurieren der macOS-Geräterichtlinien.
4. Registrieren der macOS-Geräte.
5. 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 Citrix Endpoint Management 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 es zum Registrieren und Verwalten von Geräten in Citrix Endpoint Management zu verwenden. Das Programm wird für iOS-, macOS- und Apple TV-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-, macOS- und Apple TV-Geräten verwenden. Sie können diese Geräte direkt bei Apple, einem autorisierten Apple-Vertriebspartner oder einem Netzbetreiber erwerben.

Konfigurieren der macOS-Geräterichtlinien

Verwenden Sie diese Richtlinien, um die Interaktion von Citrix Endpoint Management mit Geräten zu konfigurieren, auf denen macOS ausgeführt wird. In dieser Tabelle werden alle für macOS-Geräte verfügbaren Geräterichtlinien aufgeführt.

AirPlay-Synchronisierung	App-Bestand	App-Deinstallation
Kalender (CalDAV)	Kontakte (CardDAV)	Anmeldeinformationen
Gerätename	Exchange	FileVault
Firewall	Schriftart	Importieren von iOS- und macOS-Profilen
LDAP	Mail	Netzwerk
OS-Update	Passcode	Profilentfernung
Einschränkungen	SCEP	VPN
Webclip		

Registrieren der macOS-Geräte

Citrix Endpoint Management bietet zwei Registrierungsmethoden für Geräte, auf denen macOS ausgeführt wird. Beide Methoden ermöglichen macOS-Benutzern die Registrierung per Funk direkt über das Gerät.

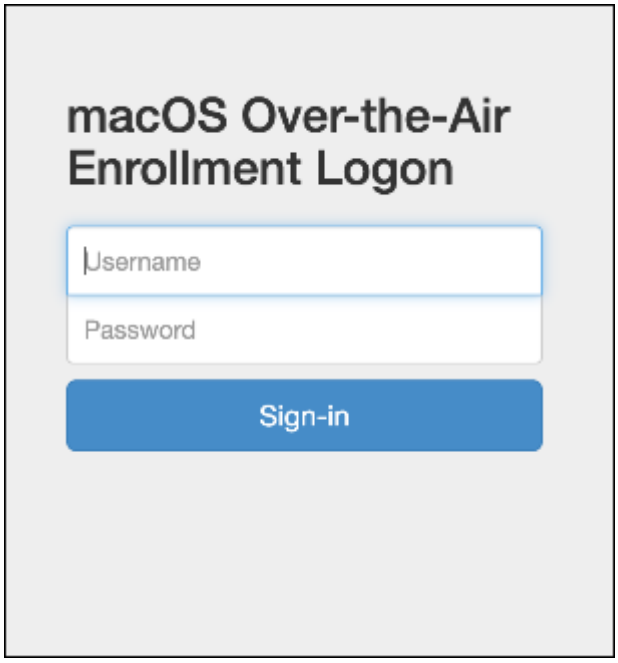
- **Senden einer Registrierungseinladung:** Bei dieser Registrierungsmethode können Sie jeden der folgenden Registrierungssicherheitsmodi für macOS-Geräte festlegen:
  - Benutzername + Kennwort
  - Benutzername + PIN
  - Zweistufige Authentifizierung

  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. Weitere Informationen finden Sie unter Registrierungseinladungen.
2. Wenn ein Benutzer die Einladung erhält und auf den Link klickt, wird in Safari folgende Seite angezeigt: Der Benutzername wird von Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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.

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 Citrix Endpoint Management genauso verwalten wie Mobilgeräte.

Sicherheitsaktionen

macOS unterstützt die folgenden Sicherheitsaktionen. Eine Beschreibung der einzelnen Sicherheitsaktionen finden Sie unter Sicherheitsaktionen.

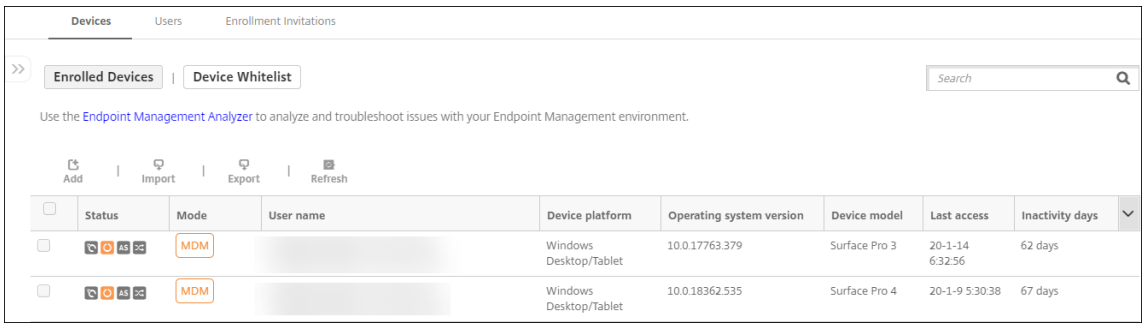
Widerrufen	Sperren	Selektiv löschen
Vollständig löschen	Zertifikaterneuerung	Persönlichen Wiederherstellungsschlüssel rotieren

Sperren von macOS-Geräten

Sie können verlorene macOS-Geräte auch remote sperren. Citrix Endpoint Management 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 Citrix Endpoint Management-Konsole zu entsperren.

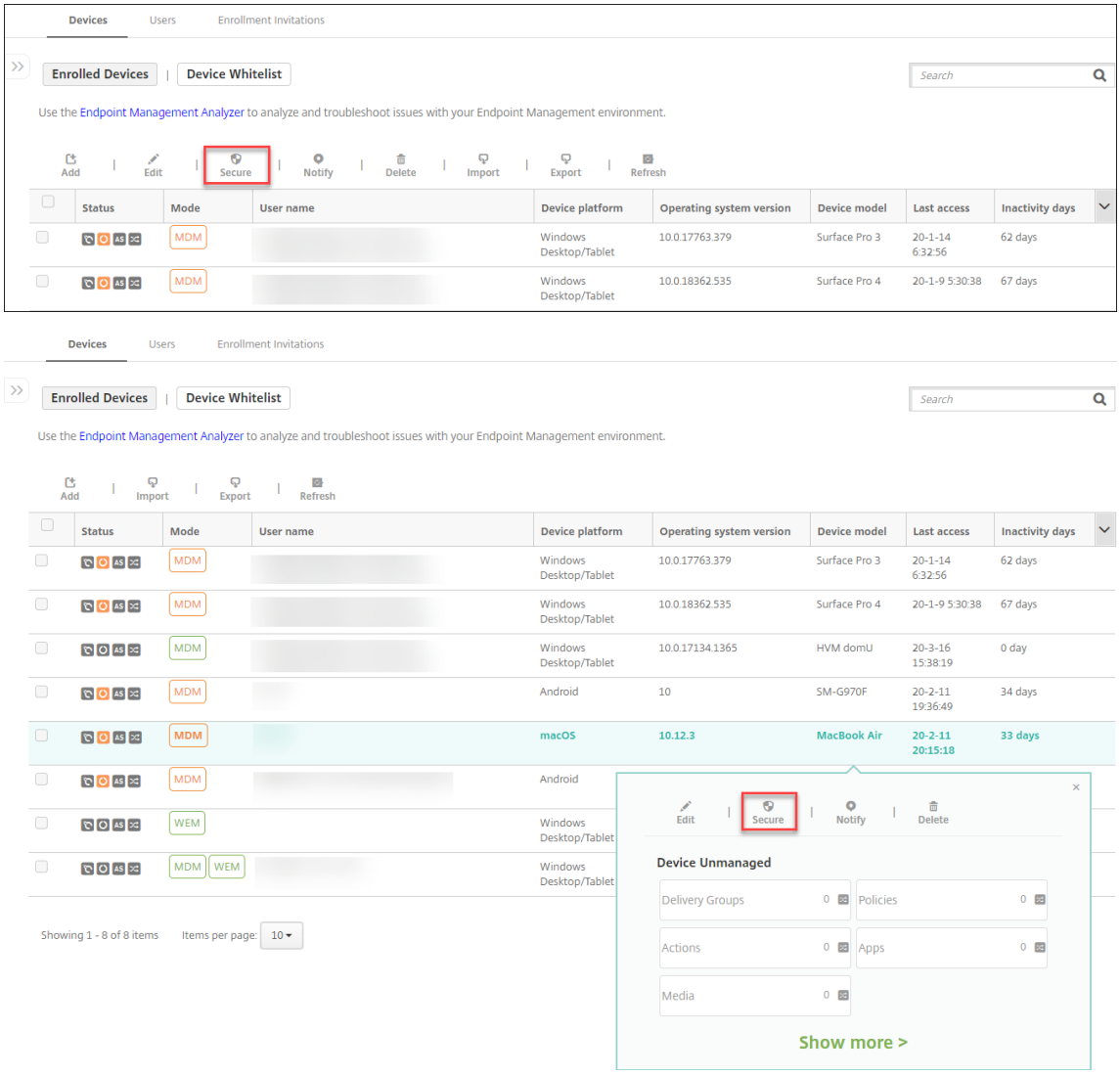
Mit der Geräterichtlinie Passcode können Sie weitere Einstellungen konfigurieren, die mit dem PIN-Code verknüpft sind. Weitere Informationen finden Sie unter macOS-Einstellungen.

1. Klicken Sie auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.



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

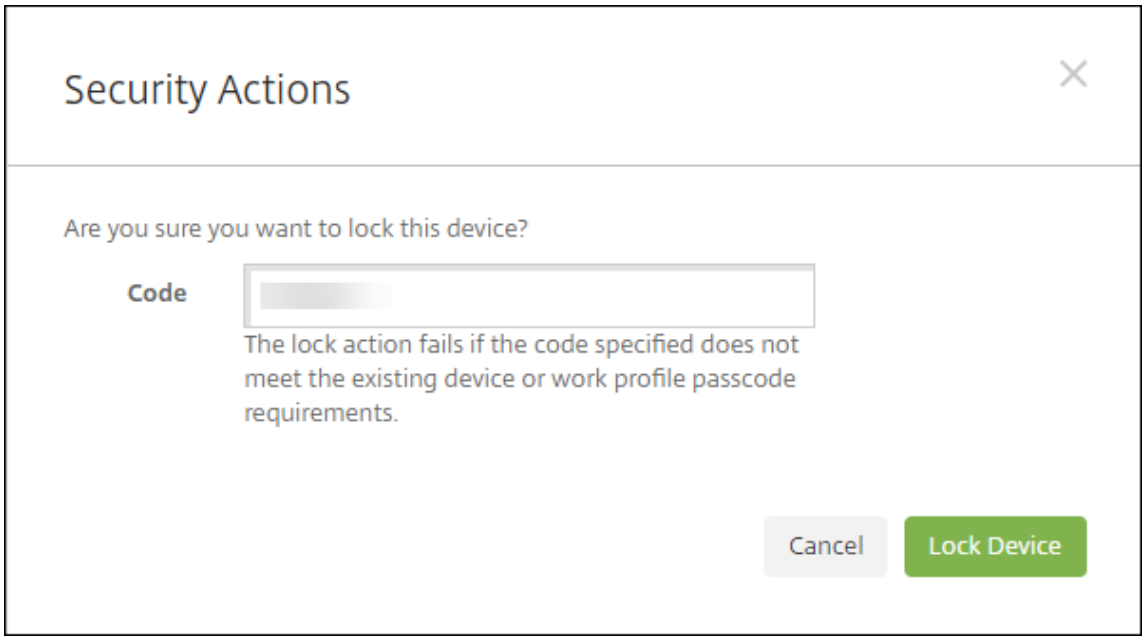
   Aktivieren Sie das Kontrollkästchen neben einem Gerät, um das Menü mit den Optionen oberhalb der Liste anzuzeigen. Sie können auch auf ein aufgelistetes Element klicken, um das Menü mit den Optionen rechts daneben anzuzeigen.



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 Citrix Endpoint Management generierten Codes können Sie auch einen Passcode festlegen. Die Sperraktion schlägt fehl, wenn der angegebene Code nicht den Passcodean-

> forderungen des Geräts oder vorhandenen Arbeitsprofils entspricht.

Bootstraptoken

Mit einem Bootstraptoken können Konten das macOS-Attribut "SecureToken"erhalten, wenn Sie sich bei einem macOS-Gerät anmelden. SecureToken wird von einem vertrauenswürdigen Konto auf ein anderes übertragen. Konten mit SecureToken können kryptografische Vorgänge auf dem Gerät ausführen. Ohne den Bootstraptoken müssen Sie Konten über komplexe Workflows auf dem Gerät erstellen, bevor Sie einzelne Benutzerkonten hinzufügen können.

Citrix Endpoint Management unterstützt das Hinterlegen von Bootstraptoken für macOS-Geräte, die über das Apple-Bereitstellungsprogramm registriert sind. Registrieren Sie über das Apple-Bereitstellungsprogramm die macOS-Geräte, die Sie direkt bei Apple, einem autorisierten Apple-Wiederverkäufer oder einem Netzbetreiber erworben haben. Informationen zum Registrieren beim Apple-Bereitstellungsprogramm finden Sie unter Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm.

Bootstraptoken werden während der Einrichtung durch den Setupassistenten generiert. Sie werden speziell beim Erstellen lokaler Benutzerkonten generiert. Der Setupassistent wird ausgeführt, wenn Benutzer das Gerät zum ersten Mal starten. Die Token werden in der Citrix Endpoint Management-Datenbank gespeichert und sind für Sie und Endbenutzer nicht sichtbar. Wenn Sie Geräte aus der Citrix Endpoint Management-Site löschen, werden die Token ebenfalls gelöscht. Durch ein Zurücksetzen auf die Werkseinstellungen werden sie nicht gelöscht.

Voraussetzungen:

- macOS 11.0 oder höher
- macOS-Geräte mit Apple T2-Sicherheitschip
- macOS-Geräte, die über das Apple-Bereitstellungsprogramm registriert sind

Durch das Hinterlegen von Bootstraptoken bei Citrix Endpoint Management können Remote-Konten für FileVault aktiviert werden und das FileVault-Volume entsperren. Weitere Informationen zu FileVault finden Sie unter FileVault-Geräterichtlinie.

Geräte über die Apple-Bereitstellungsprogramme bereitstellen

June 25, 2024

Mit den Apple-Bereitstellungsprogrammen (ADPs) können Sie Apple-Geräte vor der Übergabe an Benutzer automatisch in Citrix Endpoint Management registrieren, ohne auf die Geräte zugreifen zu müssen. Nachdem ein Benutzer das Gerät auspackt und einschaltet, registriert es sich automatisch

bei Citrix Endpoint Management, und alle Verwaltungseinstellungen, Apps und Bücher sind für ihn bereit.

Die ADPs umfassen Apple Business Manager (ABM) für Unternehmensorganisationen und Apple School Manager (ASM) für Bildungseinrichtungen. ABM und ASM sind für iOS-, iPadOS- und macOS-Geräte verfügbar. Weitere Informationen zur Berechtigung von Geräten finden Sie im Apple Business Manager-Benutzerhandbuch und im Apple School Manager-Benutzerhandbuch.

> **Hinweis:**
>
> ABM und ASM kombinieren das vorherige Programm zur Geräteregistrierung (DEP) und das Programm für Volumenlizenzen (VPP) von Apple.

Dieser Artikel erläutert das allgemeine Bereitstellungsverfahren mit ABM oder ASM:

1. Bei ABM oder ASM registrieren
2. ABM- oder ASM-Konto mit Citrix Endpoint Management verbinden
3. Geräte bestellen
4. Geräte Citrix Endpoint Management zuweisen
5. Volumenkauf von Inhalten und Synchronisieren mit Citrix Endpoint Management
6. Bereitstellungsregeln von Geräterichtlinien und Apps konfigurieren
7. Bereitstellungsgruppen hinzufügen, die Benutzer und ihnen zugewiesene Ressourcen enthalten

Nachdem Sie diesen Bereitstellungsprozess abgeschlossen haben, sind die Geräte einsatzbereit und können für eine automatisierte Geräteregistrierung aktiviert werden.

Voraussetzungen

Öffnen Sie die erforderlichen Ports für die Verbindung zwischen Citrix Endpoint Management und Apple. Weitere Informationen finden Sie unter Portanforderungen.

Bei ABM oder ASM registrieren

Um Geräte in Apple bereitzustellen, registrieren Sie sich bei ABM oder ASM.

ABM und ASM sind nur für Organisationen und nicht für Einzelpersonen verfügbar. Sie müssen zahlreiche Unternehmensdetails angeben, um ein Konto zu erstellen. Es kann eine Weile dauern, bis angeforderte Kontogenehmigungen vorliegen.

Registrierung bei ABM

Zum Registrieren bei ABM 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 ABM, um ein Konto zu erstellen.

Registrierung bei ASM

Zum Erstellen eines ASM-Kontos gehen Sie zu Apple School Manager und folgen den Anweisungen zur Registrierung. 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 eines ASM-Benutzerkontos 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. Informationen zum Hinzufügen von Dienstplandaten zu ASM finden Sie in der oben erwähnten Benutzerdokumentation zu Apple School Manager.
- Sie können das Format der verwalteten Apple-ID für Ihre Institution anpassen (siehe oben erwähnte Benutzerdokumentation zu Apple School Manager).

  > **Wichtig:**
  >
  > Ändern Sie keine verwalteten Apple-IDs, nachdem Sie ASM-Informationen in Citrix Endpoint Management importiert haben.

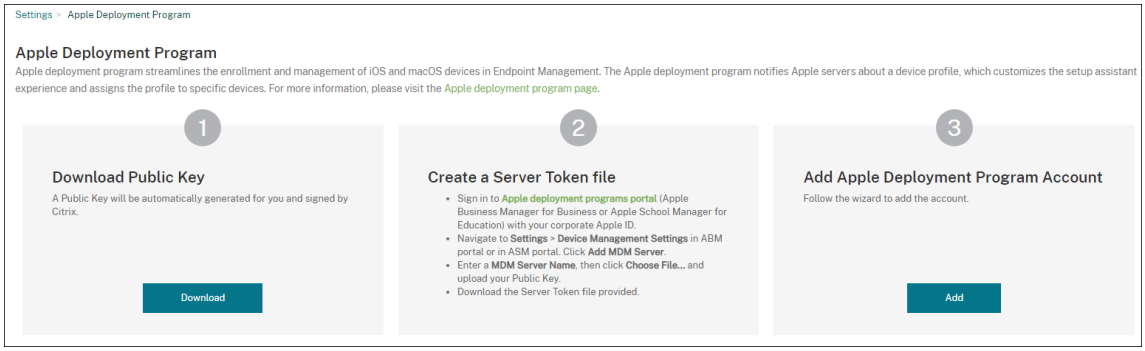
- Wenn Sie Geräte über Wiederverkäufer oder Netzbetreiber erworben haben, verknüpfen Sie die Geräte mit ASM. Informationen finden Sie in der oben erwähnten Benutzerdokumentation zu Apple School Manager.

ABM- oder ASM-Konto mit Citrix Endpoint Management verbinden

Nachdem Sie Ihr ABM- oder ASM-Konto erstellt haben, verbinden Sie es mit Ihrer Citrix Endpoint Management-Serverbereitstellung.

Schritt 1. Laden Sie einen öffentlichen Schlüssel vom Citrix Endpoint Management-Server herunter

1. Gehen Sie in der Citrix Endpoint Management-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 oder Apple School 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 Citrix Endpoint Management-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 Citrix Endpoint Management heruntergeladen haben, und speichern Sie die Änderungen.
5. Klicken Sie auf **Download Token**, um die Servertokendatei auf Ihren Computer herunterzuladen.

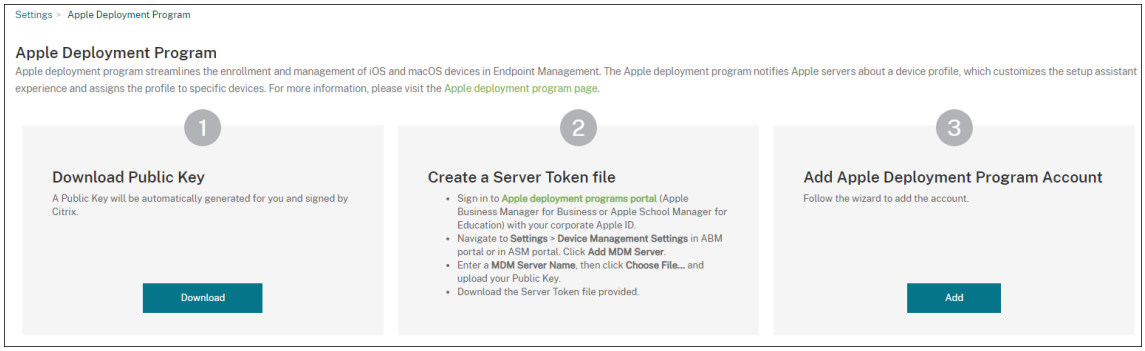
   Sie laden die Servertokendatei hoch, wenn Sie das ABM- oder ASM-Konto zu Citrix Endpoint Management hinzufügen. Nach dem Import der Tokendatei werden Ihre Tokeninformationen in der Citrix Endpoint Management-Konsole angezeigt.
6. Klicken Sie unter **Default Device Assignment** auf **Change**. Wählen Sie aus, wie Sie Geräte zuweisen möchten, und geben Sie die angeforderten Informationen ein. Weitere Informationen finden Sie im Apple Business Manager-Benutzerhandbuch oder im Apple School Manager-Benutzerhandbuch.

Schritt 3: Hinzufügen Ihres Kontos zu Citrix Endpoint Management

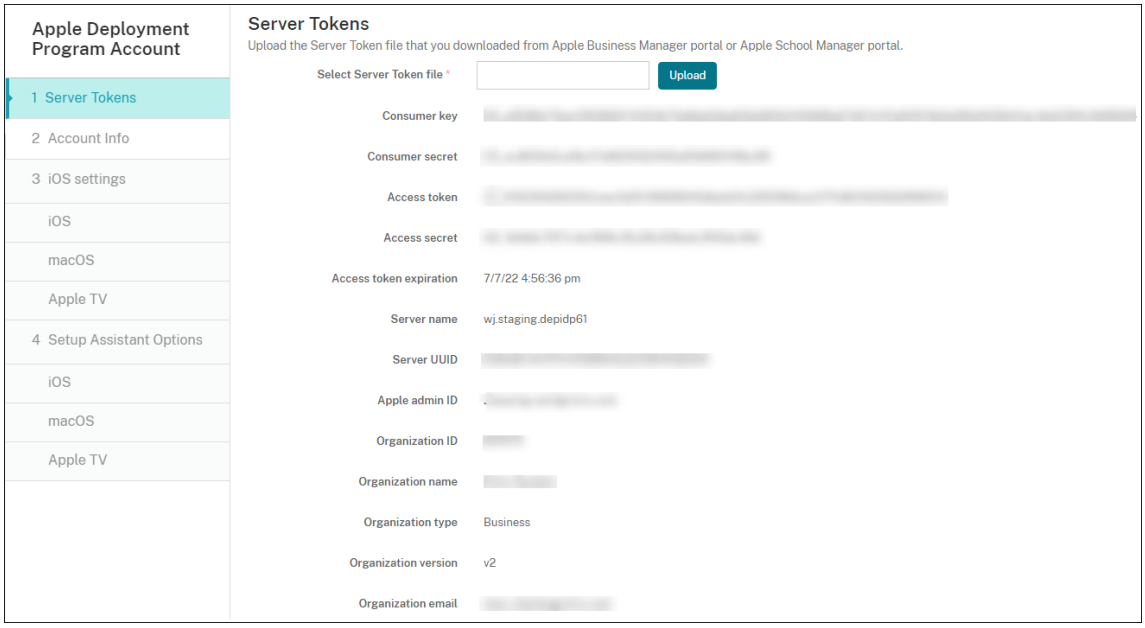
Sie können mehrere ABM- oder ASM-Konten zu Citrix Endpoint Management hinzufügen. Dieses Feature ermöglicht die Verwendung verschiedener Registrierungseinstellungen sowie verschiedener Optionen im Setupassistenten je nach Land, Abteilung usw. Anschließend verknüpfen Sie die ABM- oder ASM-Konten mit verschiedenen Geräterichtlinien.

Sie können beispielsweise alle ABM- oder ASM-Konten aus verschiedenen Ländern auf einem Citrix Endpoint Management-Server zentralisieren, um dort alle ABM- oder ASM-Geräte zu importieren und zu überwachen. Sie passen zunächst die Registrierungseinstellungen und Setupassistentenoptionen nach Abteilung, Organisationshierarchie oder einer anderen Struktur an. Anschließend konfigurieren Sie Richtlinien für eine unternehmensweit geeignete Funktionalität und helfen Benutzern, geeignete Unterstützung zu erhalten.

1. Rufen Sie in der Citrix Endpoint Management-Konsole **Einstellungen > Apple-Bereitstellungsprogramm** auf und klicken Sie unter **Konto für Apple-Bereitstellungsprogramm hinzufügen** auf **Hinzufügen**.

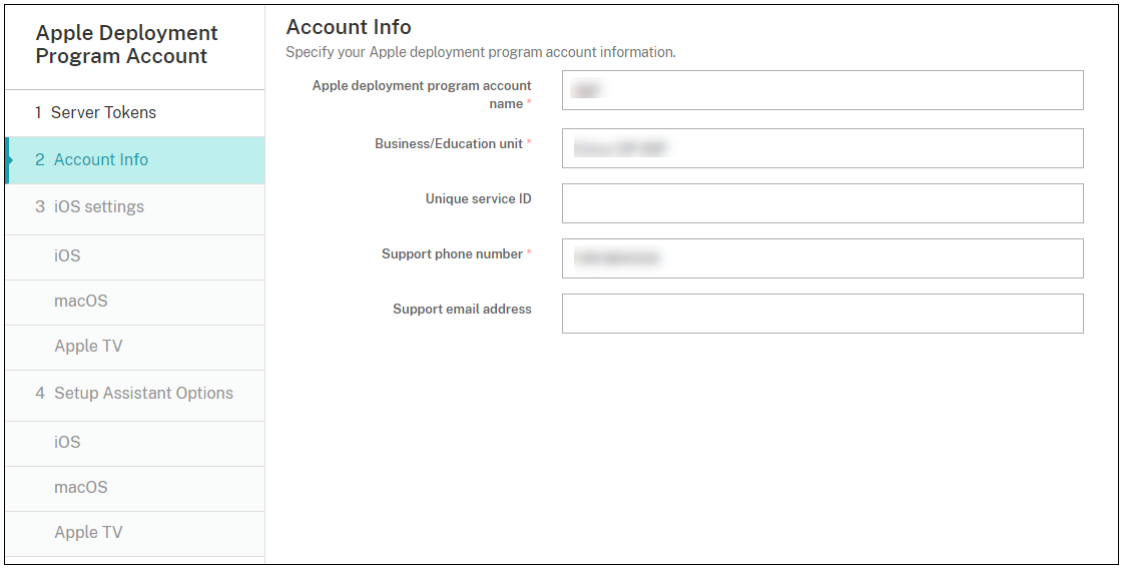


2. Geben Sie auf der Seite **Servertoken** die Servertokendatei ein und klicken Sie dann auf **Hochladen**.



Die Informationen zum Servertoken werden angezeigt.

3. Geben Sie auf der Seite **Kontoinformationen** folgende Einstellungen an:

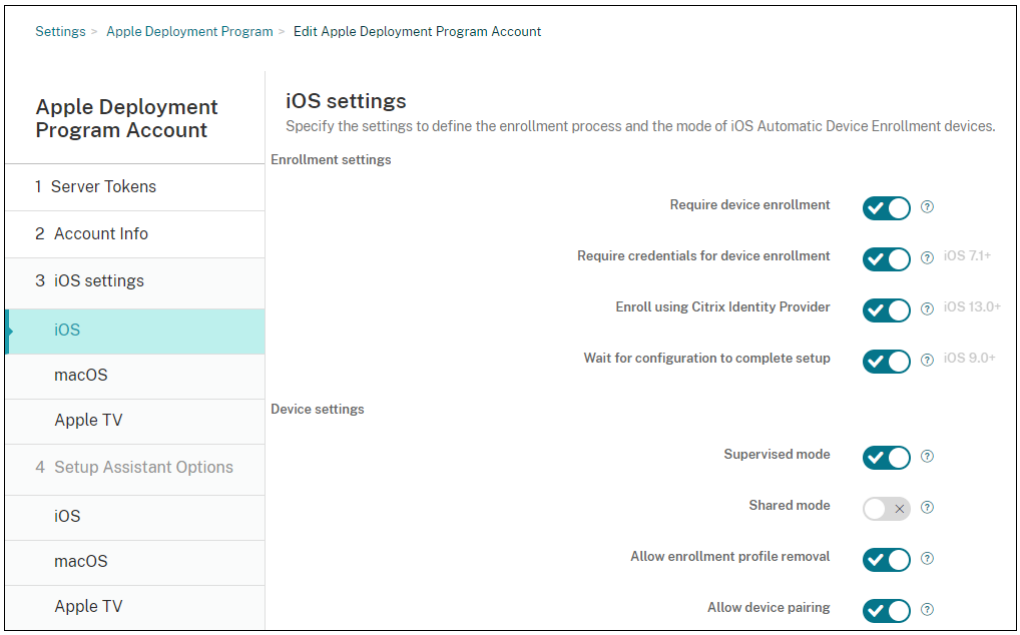


- **Name des Kontos für Apple-Bereitstellungsprogramm:** Ein aussagekräftiger eindeutiger Name für dieses ADP-Konto, der angibt, wie Ihre ADP-Konten organisiert werden, z. B. nach Land oder nach Organisationshierarchie.
- **Geschäftseinheit:** Die Unternehmenseinheit oder Abteilung, der das Gerät zugewiesen ist. Dieses Feld 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. Dieses Feld ist erforderlich.

- **E-Mail-Adresse vom Support:** Eine optionale E-Mail-Adresse des Supports, die Benutzern zur Verfügung steht.
- **Suffix der Bildungseinrichtung:** Für ASM-Konten. Geben Sie das Suffix ein, das Geräten zugewiesen ist, die über dieses Konto registriert sind.

4. Geben Sie unter **iOS-Einstellungen** die folgenden Einstellungen an:



Registrierungseinstellungen:

- **Geräteregistrierung erforderlich:** Wählen Sie aus, ob Benutzer Geräte registrieren müssen. Die Standardeinstellung ist **Ein**.
- **Anmeldeinformationen für Geräteregistrierung erforderlich:** Wählen Sie aus, ob Benutzer bei der ABM- und ASM-Registrierung ihre Anmeldeinformationen eingeben müssen. Wir empfehlen, dass alle Benutzer während der Geräteregistrierung ihre Anmeldeinformationen eingeben müssen, damit nur autorisierte Benutzer Geräte registrieren können. Die Standardeinstellung ist **Ein**.

  Wenn Sie ABM oder ASM vor dem ersten Einrichten aktivieren und diese Option nicht auswählen, erstellt Citrix Endpoint Management die ABM- oder ASM-Komponenten. Dabei werden Komponenten wie Benutzer, Citrix Secure Hub, Softwarebestand und Bereitstellungsgruppe erstellt. Wenn Sie diese Option auswählen, werden die Komponenten nicht von Citrix Endpoint Management erstellt. Wenn Sie später die Option deaktivieren, können Benutzer, die ihre Anmeldeinformationen nicht eingegeben haben, die ABM- oder ASM-Registrierung nicht ausführen, da diese Komponenten nicht vorhanden sind. Zum Hinzufügen von ABM- oder ASM-Komponenten deaktivieren und reaktivieren Sie in diesem Fall das ABM- oder ASM-Konto.

- **Mit dem Citrix-Identitätsanbieter registrieren:** Wählen Sie, ob Sie zur Registrierung den Citrix-Identitätsanbieter verwenden. Diese Einstellung ist nur für ABM-Konten verfügbar. Bei Auswahl der Einstellung **Ein** registrieren sich ADP-fähige iOS-Geräte nur mithilfe des Citrix-Identitätsanbieters. Die Standardeinstellung ist **Aus**.

  Um die Einstellung zu aktivieren, müssen Sie zuerst den Citrix-Identitätsanbieter als Ihren Identitätsanbieter konfigurieren. Gehen Sie zu **Einstellungen > Identitätsanbieter (IdP)**, klicken Sie auf **Hinzufügen**und wählen Sie **Citrix-Identitätsanbieter**.

  Bei Auswahl der Einstellung **Ein** ist Folgendes zu beachten:

  - Sie können die entsprechende Konfiguration des Citrix-Identitätsanbieters auf der Seite **Einstellungen > Identitätsanbieter (IdP)** nicht löschen.
  - Wenn Sie die entsprechende Konfiguration des Citrix-Identitätsanbieters bearbeiten, können Sie nicht zu einem anderen Identitätsanbieter wechseln.

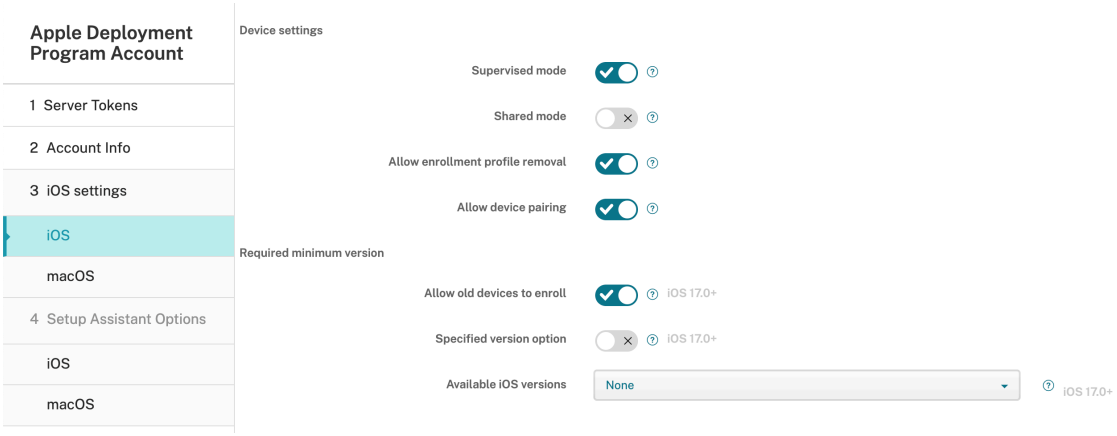
- **Abschluss der Konfiguration abwarten:** Wählen Sie aus, ob Geräte im Setupassistentenmodus verbleiben müssen, bis alle erforderlichen MDM-Ressourcen auf den Geräten bereitgestellt wurden. Diese Einstellung ist nur für Geräte im betreuten Modus verfügbar. Die Standardeinstellung ist **Aus**.
- Laut 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 ist auf **Ein** festgelegt, wenn Sie Apple Configurator zum Verwalten von registrierten Geräten verwenden oder wenn **Abschluss der Konfiguration abwarten** aktiviert ist. Die Standardeinstellung ist **Ein**. Informationen, wie Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Bereitstellen von Geräten mit Apple Configurator 2.
- **Entfernen des Registrierungsprofils zulassen:** Wählen Sie aus, ob auf Geräten ein Profil verwendet werden darf, das remote entfernt werden kann. Die Standardeinstellung ist **Aus**.
- **Koppeln von Geräten zulassen:** Wählen Sie aus, ob registrierte Geräte mit Apple Music und dem Apple Configurator verwaltet werden dürfen. Die Standardeinstellung ist **Aus**.

Erforderliche Mindestversion



- **Registrierung alter Geräte zulassen:** Wenn diese Option aktiviert ist, können Geräte registriert werden, auch wenn sie nicht auf die aktuell erforderliche Mindestversion aktualisiert werden konnten. Die Standardeinstellung ist Ein. Diese Option ist nur für iOS 17.0 und höher verfügbar.
- **Option für angegebene Version:** Ob der Administrator die angegebene Version manuell eingeben darf. Die Standardeinstellung ist **Aus**. Diese Option ist nur für iOS 17.0 und höher verfügbar.
- **Verfügbare iOS-Versionen:** Sie können die verfügbaren iOS-Versionen aus der Liste auswählen. Wenn das Gerät über eine niedrigere iOS-Version als die aktuelle Version verfügt, wird der Aktualisierungsvorgang auf dem Gerät gestartet. Wenn die Version in der Zukunft abläuft, wird eine Mindestversion der verfügbaren Versionsliste verwendet. Die Standardeinstellung ist "Keine", sie wird nicht wirksam, wenn sie auf "Keine"gesetzt ist. Diese Option ist nur für iOS 17.0 und höher verfügbar.
- **Angegebene Version:** Wenn das Gerät eine niedrigere iOS-Version als die aktuelle Version hat, wird der Aktualisierungsvorgang auf dem Gerät gestartet. Wenn die Version in der Zukunft abläuft, wird eine Mindestversion der verfügbaren Versionsliste verwendet. Geben Sie die richtige Versionsnummer ein, da sonst unbekannte Fehler auftreten können.

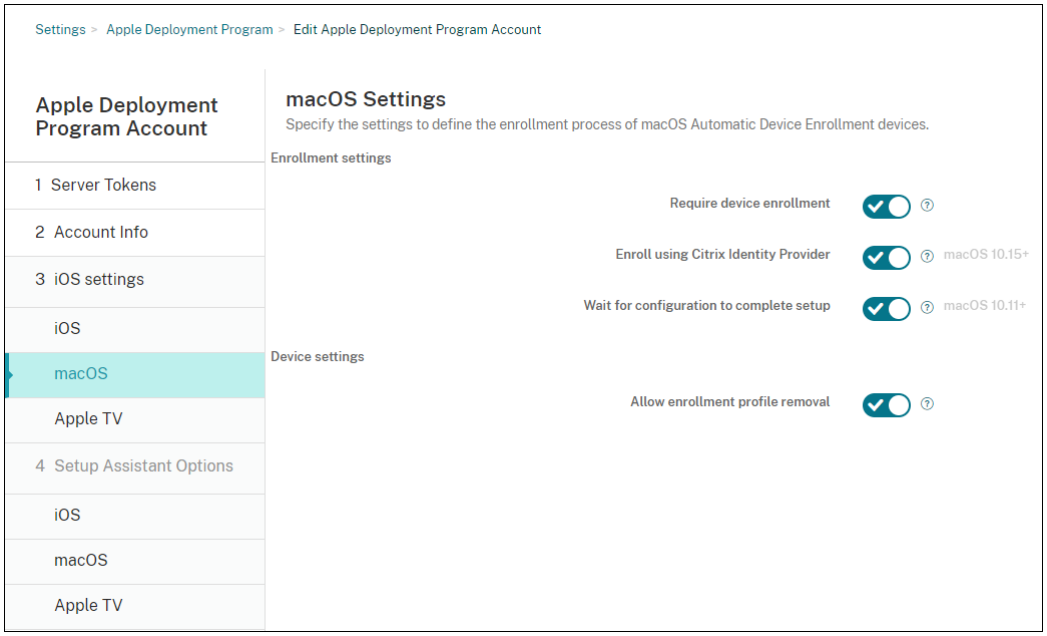
Überwachungsidentitäten

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- oder ASM-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 **Ein**.
- **Mit dem Citrix-Identitätsanbieter registrieren:** Wählen Sie, ob Sie zur Registrierung den Citrix-Identitätsanbieter verwenden. Diese Einstellung ist nur für ABM-Konten verfügbar. Bei Auswahl der Einstellung **Ein** registrieren sich ADP-fähige macOS-Geräte nur mithilfe des Citrix-Identitätsanbieters. Die Standardeinstellung ist **Aus**.

  Um die Einstellung zu aktivieren, müssen Sie zuerst den Citrix-Identitätsanbieter als Ihren Identitätsanbieter konfigurieren. Gehen Sie zu **Einstellungen > Identitätsanbieter (IdP)**, klicken Sie auf **Hinzufügen**und wählen Sie **Citrix-Identitätsanbieter**.

  Bei Auswahl der Einstellung **Ein** ist Folgendes zu beachten:

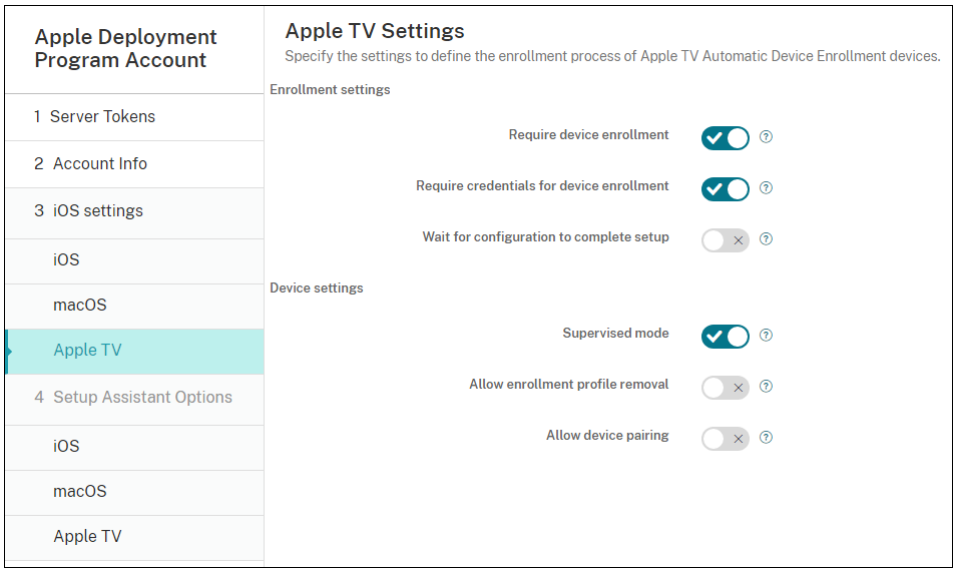
  - Sie können die entsprechende Konfiguration des Citrix-Identitätsanbieters auf der Seite **Einstellungen > Identitätsanbieter (IdP)** nicht löschen.
  - Wenn Sie die entsprechende Konfiguration des Citrix-Identitätsanbieters bearbeiten, können Sie nicht zu einem anderen Identitätsanbieter wechseln.
- **Abschluss der Konfiguration abwarten:** Bei Auswahl von **Ein** 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 **Aus**.

Geräteeinstellungen:

- **Entfernen des Registrierungsprofils zulassen:** Wählen Sie aus, ob auf Geräten ein Profil verwendet werden darf, das remote entfernt werden kann. Die Standardeinstellung ist **Aus**.

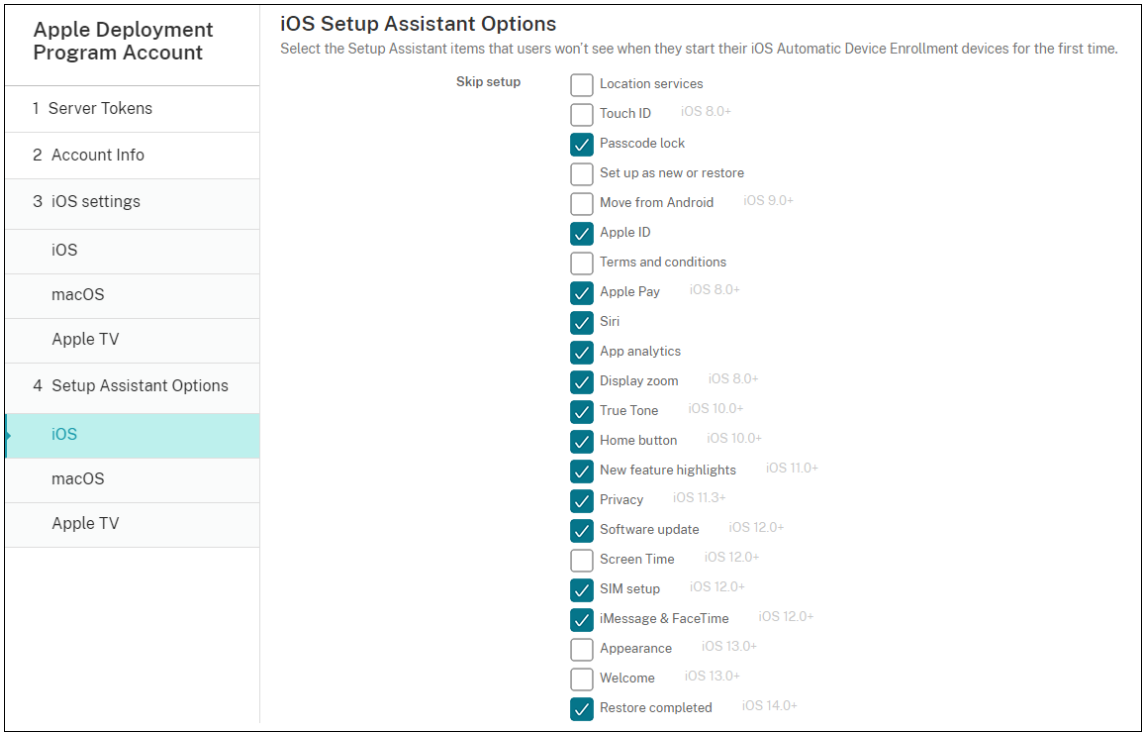
6. Legen Sie unter **Apple TV-Einstellungen** folgende Einstellungen fest:

   - **Geräteregistrierung erforderlich:** Verhindert, dass Benutzer die Registrierung überspringen.
   - **Anmeldeinformationen für Geräteregistrierung erforderlich:** Bei der Registrierung müssen die Anmeldeinformationen eingegeben werden. Wenn diese Einstellung deaktiviert ist, werden Apple TV-Geräte unter Verwendung des Device Enrollment Program-Standardbenutzerkontos registriert.
   - **Abschluss der Konfiguration abwarten:** Das Gerät wartet im **Setupassistenten**, bis alle Ressourcen bereitgestellt sind.
   - **Betreuter Modus:** Der Administrator kann beim Konfigurieren von Einschränkungen zusätzliche Funktionen nutzen.
   - **Entfernen des Registrierungsprofils zulassen:** Ermöglicht Benutzern das Entfernen der Registrierungsprofile.
   - **Koppeln von Geräten zulassen:** Ermöglicht, dass Geräte, die über das Device Enrollment Program registriert wurden, mit Apple-Tools wie Apple App Store und Apple Configurator verwaltet werden.



7. Wählen Sie unter **Optionen des iOS-Setupassistenten** die Schritte aus, die beim ersten Gerätestart durch Benutzer übersprungen werden sollen. 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.

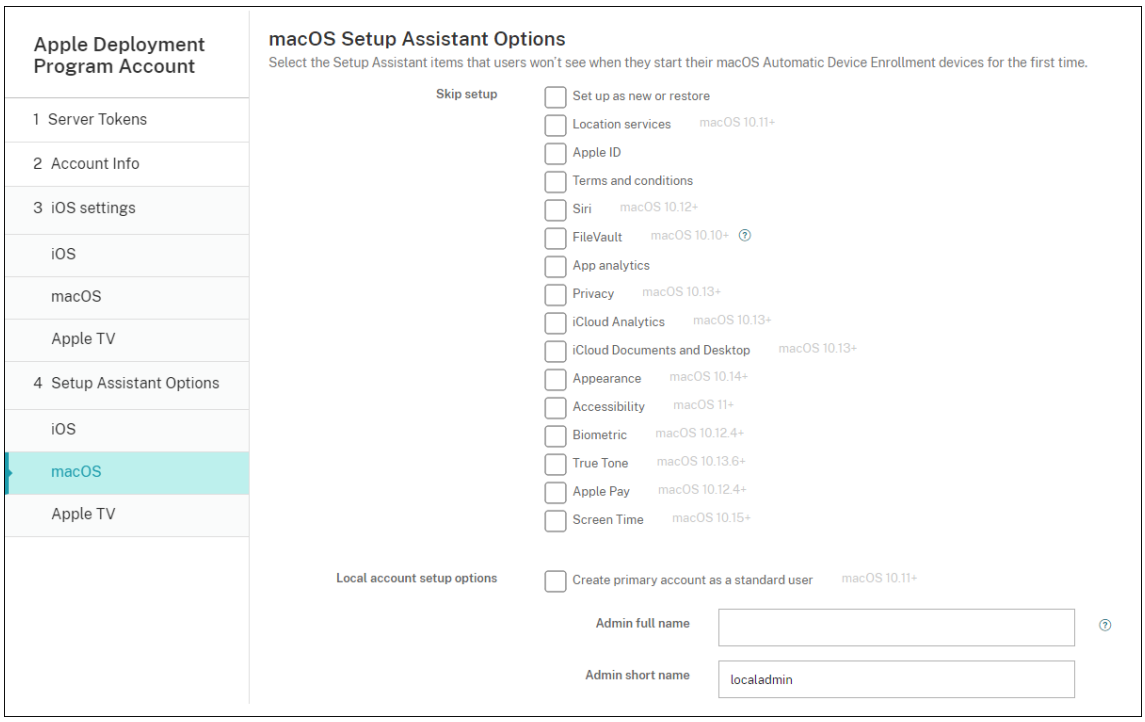


- **Ortungsdienste:** Verhindert, dass Benutzer den Ortungsdienst auf dem Gerät einrichten.
- **Touch ID:** Verhindert, dass Benutzer Touch ID oder Face ID auf iOS-Geräten einrichten.
- **Passcodesperre:** Verhindert, dass Benutzer einen Passcode für das Gerät einrichten. Wenn kein Passcode existiert, 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.
- **App Store:** Verhindert, dass Benutzer den App-Store einrichten. Für iOS 11.1 und höher.

Das Konto wird unter **Einstellungen > Apple-Bereitstellungsprogramm** angezeigt.

8. 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. Citrix Endpoint Management 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 Nutzungsstatistiken 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.
- **Bildschirmzeit:** Verhindert, dass Benutzer die Bildschirmzeit aktivieren. Für macOS 10.15 und höher.
- **App Store:** Verhindert, dass Benutzer den App-Store einrichten. Für macOS 11.1 und höher.
- **Mit Apple Watch entsperren:** Verhindert, dass Benutzer ihren Mac mit einer Apple Watch entsperren. Für macOS 12 und höher:
- **Setupoptionen für lokales Konto:** Geben Sie die Einstellungen zum Erstellen eines Kontos auf dem Gerät an. Citrix Endpoint Management erstellt zuerst das lokale Administratorkonto mit den hier angegebenen Informationen. Wenn Benutzer ihr Gerät aktivieren, wird ein Benutzerkonto als primäres Konto erstellt. Über die Option **Erstellen Sie ein primäres Konto als Standardbenutzer** wird festgelegt, ob das primäre Konto über Administratorrechte verfügt.

> **Wichtig:**
>
> Sie können **Erstellen Sie ein primäres Konto als Standardbenutzer** erst auswählen,

> nachdem Sie auf der Seite **macOS-Einstellungen** für **Abschluss der Konfiguration abwarten** die Einstellung **Ein** gewählt haben.

- **Erstellen Sie ein primäres Konto als Standardbenutzer:** Wenn diese Option aktiviert ist, erstellt Citrix Endpoint Management den Benutzer mit Standardberechtigungen und gewährt ihm keine Administratorrechte auf dem Gerät. Überspringen Sie diese Option, wenn Sie dem Benutzer Administratorrechte auf dem Gerät gewähren möchten. Die Option ist standardmäßig nicht aktiviert.
- **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 Citrix Endpoint Management erstellte Administratorkonto auszublenden.

Um die Sicherheit zu erhöhen, prüft Citrix Endpoint Management, ob das Kennwort des Administratorkontos täglich rotiert werden soll. Standardmäßig wird das Kennwort in Citrix Endpoint Management alle 7 Tage gewechselt. Diese Standardeinstellung können Sie in der Servereigenschaft `mac.dep.admin.passwd.rotate` ändern. Weitere Informationen finden Sie unter Servereigenschaften.

Um Stärke und Sicherheit des Kennworts zu erhöhen, müssen Kennwörter in Citrix Endpoint Management folgende Vorgaben erfüllen:

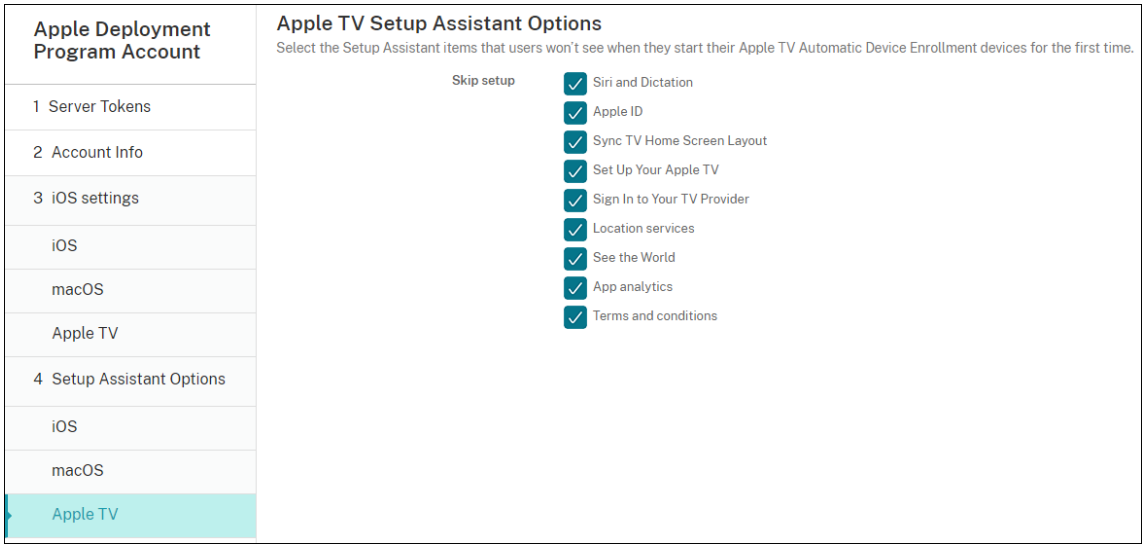
- 12 Zeichen lang
- 3 Großbuchstaben
- 3 Kleinbuchstaben
- 3 Ziffern
- 3 Sonderzeichen: `! \@ \\# \$ % \\^ \* ? + = -`

Um das vorherige Kennwort, das aktuelle Kennwort und den Kennwortänderungsstatus für ein Gerät anzuzeigen, gehen Sie zu **Verwalten > Geräte**. Klicken Sie auf dieses Gerät, klicken Sie auf **Mehr anzeigen** und rufen Sie die Seite **Gerätedetails > Allgemein** auf. Im Abschnitt **Sicherheit** wird Folgendes angezeigt:

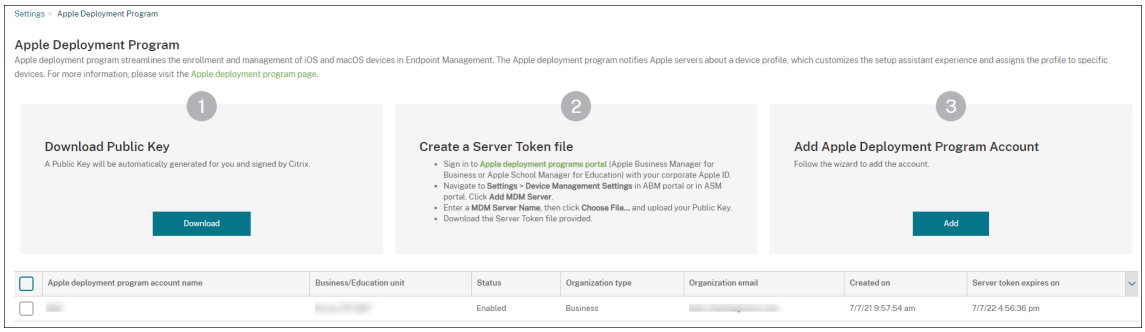
- **Vorheriges Administratorkennwort:** Hier können Sie das vorherige Kennwort anzeigen. Citrix Endpoint Management zeigt nur das letzte Kennwort. Klicken Sie auf **Kennwort anzeigen**, um das Kennwort zu sehen.

- **Aktuelles Administratorkennwort:** Hier können Sie das aktuelle Kennwort anzeigen.
- **Administratorkennwort ändern:** Hier können Sie den Kennwortänderungsstatus anzeigen. Je nach vorliegendem Status werden folgende Informationen angezeigt:
  - Die Kennwortänderung wurde angefordert: <spezieller Zeitwert>.
  - Das Kennwort wurde geändert: <bestimmter Zeitwert>.
  - Versuche, das Kennwort zu ändern, schlugen fehl: <bestimmter Zeitwert>.
  - Das Kennwort wurde noch nicht geändert.

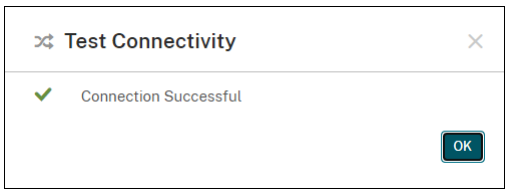
9. Wählen Sie unter **Optionen des Apple TV-Setupassistenten** die Schritte aus, die Benutzer beim ersten Gerätestart überspringen. Alle Optionen sind standardmäßig deaktiviert. Speichern Sie die Änderung.



10. Das Konto wird unter **Einstellungen > Apple-Bereitstellungsprogramm** angezeigt. Zum Testen der Verbindung zwischen Citrix Endpoint Management und Apple wählen Sie das Konto aus und klicken auf **Konnektivität testen**.



Eine Statusmeldung wird angezeigt.



Geräte bestellen

Sie können Geräte direkt über die folgenden Kanäle bestellen:

- Apple Teilen Sie dem Verkäufer Ihre Apple-Kundennummern mit.
- Autorisierter Apple-Vertriebspartner oder Netzbetreiber. Teilen Sie dem Verkäufer Ihre Organisations-ID mit und fragen Sie nach seiner Wiederverkäufer-ID.

Weitere Informationen zum Verwalten von Geräteverkäufern finden Sie im Apple Business Manager-Benutzerhandbuch und im Apple School Manager-Benutzerhandbuch.

Nach dem Versand Ihrer Bestellung werden die erworbenen Apple-Geräte Ihrem ABM- oder ASM-Konto hinzugefügt.

Geräte Citrix Endpoint Management zuweisen

Suchen Sie im ABM- oder ASM-Portal nach einer Bestellnummer und weisen Sie damit die bestellten Geräte Citrix Endpoint Management zu. iPhone-, iPad-, iPod touch- und Apple TV-Geräte können Sie auch mit Apple Configurator 2 zu ABM oder ASM hinzufügen, unabhängig davon, wo die Geräte gekauft wurden.

Weitere Informationen finden Sie im Apple Business Manager-Benutzerhandbuch oder im Apple School Manager-Benutzerhandbuch.

Volumenkauf von Inhalten und Synchronisierung mit Citrix Endpoint Management

Mit ABM und ASM können Sie Volumenlizenzen für Apps und Bücher über ein einziges Unternehmenskonto erwerben, verteilen und verwalten. Führen Sie die folgenden Schritte aus, um Citrix Endpoint Management mit ABM oder ASM zu verknüpfen und die Lizenzinformationen für die Verteilung abzurufen:

1. Kaufen Sie im ABM- oder ASM-Portal öffentliche Apps und Bücher unter **Apps and Books** bzw. unter **Custom Apps** benutzerdefinierte Apps, die für Ihr Citrix Endpoint Management entwickelt wurden.

2. Laden Sie im ABM- oder ASM-Portal den Inhaltstoken für Ihr Citrix Endpoint Management herunter.

   Weitere Informationen zu Schritt 1 und 2 finden Sie im Apple Business Manager-Benutzerhandbuch oder im Apple School Manager-Benutzerhandbuch.

3. Erstellen Sie in der Citrix Endpoint Management-Konsole ein Volume Purchase-Konto, das auf dem heruntergeladenen Inhaltstoken basiert.

   Weitere Informationen finden Sie unter Hinzufügen von Apps über Apple Volume Purchase.

   Nach dem Erstellen des Volume Purchase-Kontos werden Ihre erworbenen Apps und Bücher unter **Verwalten** > **Apps** angezeigt, während die Geräte, die Sie dem Citrix Endpoint Management-Server zugewiesen haben, unter **Verwalten > Geräte** erscheinen.

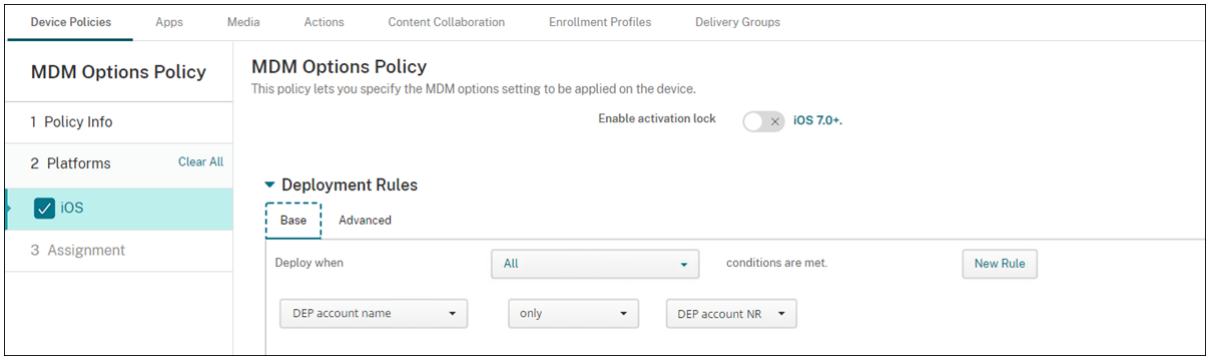
Bereitstellungsregeln von Geräterichtlinien und Apps konfigurieren

Beim Konfigurieren von Geräterichtlinien und Apps können Sie ABM- oder ASM-Konten mit verschiedenen Apps und Geräterichtlinien verknüpfen.

1. Erweitern Sie auf den Seiten **Konfigurieren > Geräterichtlinien** und **Konfigurieren > Apps** die Option **Bereitstellungsregeln**.
2. Legen Sie fest, dass eine Richtlinie oder App für ein bestimmtes ABM-Konto oder für alle ABM-Konten mit Ausnahme des ausgewählten Kontos bereitgestellt wird.

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 Citrix Endpoint Management 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.



Massenregistrierung von Apple-Geräten

March 11, 2024

Sie können iOS-, iPadOS- und macOS-Geräte in großer Zahl bei Citrix Endpoint Management auf zwei Arten registrieren.

- Verwenden Sie die Apple-Bereitstellungsprogramme (ADP), um Apple-Geräte zu registrieren, die Sie direkt bei Apple, einem autorisierten Apple-Wiederverkäufer oder einem Netzbetreiber erworben haben.

  Weitere Informationen zum Bereitstellen von ADP-fähigen Geräten finden Sie unter Bereitstellen von Geräten über die Apple-Bereitstellungsprogramme. In diesem Artikel wird beschrieben, wie Benutzer ADP-fähige Geräte registrieren bzw. erneut registrieren.

- Verwenden Sie Apple Configurator 2 zum Registrieren von iOS-Geräten, unabhängig davon, ob Sie sie direkt bei Apple erworben haben.

In diesem Artikel wird beschrieben, wie Sie Geräte mit Apple Configurator 2 in großen Mengen bereitstellen.

Informationen zur Massenregistrierung

Die ADPs umfassen Apple Business Manager (ABM) für Unternehmen und Apple School Manager (ASM) für Bildungseinrichtungen. Die Massenregistrierung über die Features der ADPs umfasst die folgenden Schritte:

- Die Geräte müssen nicht vorbereitet werden.
- Nachdem Sie die Bereitstellungseinstellungen in Citrix Endpoint Management abgeschlossen haben, können Sie die Geräte an Benutzer aushändigen, die sie sofort verwenden können.
- Sie können den Einrichtungsprozess für Benutzer vereinfachen, indem Sie einige Schritte im Setupassistenten eliminieren.
- Weitere Informationen zum Einrichten von ABM und ASM finden Sie in der Dokumentation zu Apple Business Manager und Apple School Manager.

Die Massenregistrierung über Apple Configurator 2-Features umfasst folgende Schritte:

- Sie schließen iOS-Geräte an einen Mac mit macOS 10.7.2 oder höher und der Apple Configurator 2-App an. Sie bereiten die iOS-Geräte vor und konfigurieren Richtlinien über Apple Configurator 2.
- Geräte werden während des Setups automatisch bei Citrix Endpoint Management registriert. Nach Abschluss des Setups überträgt Citrix Endpoint Management Richtlinien, Apps und andere Ressourcen an Geräte. Sie können dann mit dem Verwalten der Geräte beginnen.

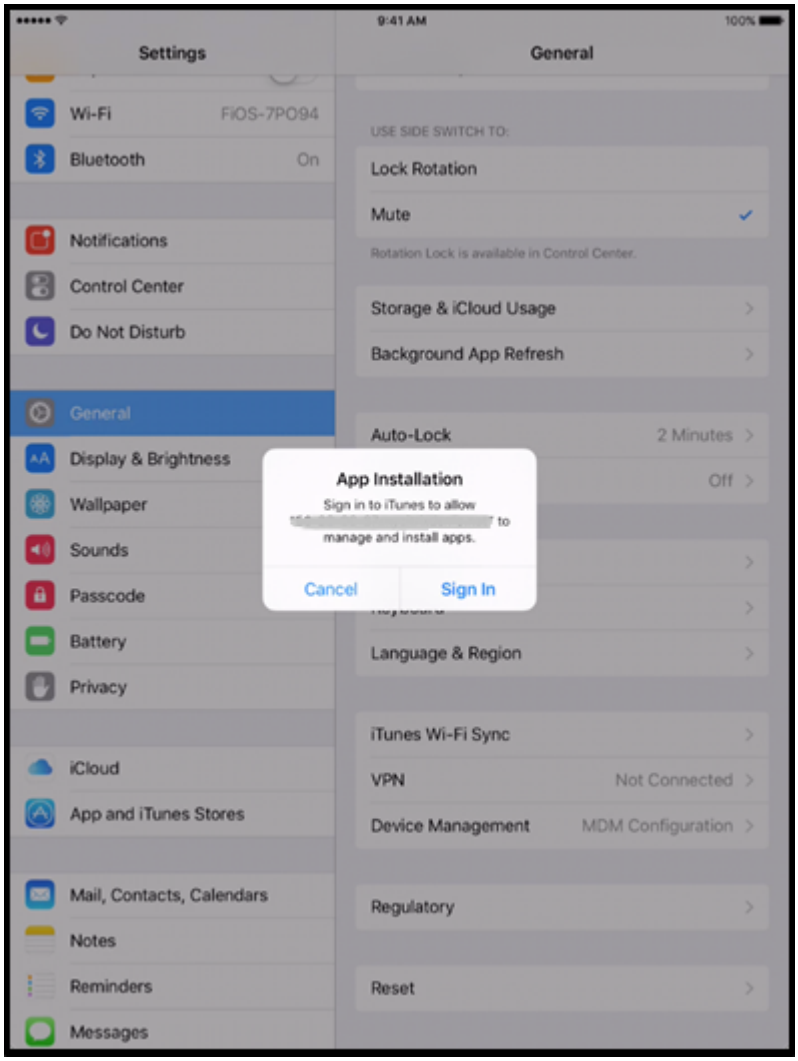
- Weitere Informationen über die Verwendung von Apple Configurator 2 finden Sie in der Apple Configurator-Hilfe.

Registrieren von ADP-fähigen Geräten durch Benutzer

Benutzer registrieren ihre Geräte wie folgt bei Citrix Endpoint Management:

1. Benutzer starten ihr Gerät.
2. Citrix Endpoint Management stellt die ADP-Einstellungen, die Sie unter **Einstellungen > Apple-Bereitstellungsprogramme** konfiguriert haben, auf dem Gerät bereit.
3. Benutzer konfigurieren die anfänglichen Einstellungen auf ihrem Gerät.
4. Das Gerät startet automatisch die Citrix Endpoint Management-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 Citrix Endpoint Management für die Bereitstellung der Citrix 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 Citrix Secure Hub und geben ihre Anmeldeinformationen ein. Entsprechend der Richtlinie müssen Benutzer unter Umständen eine Citrix-PIN erstellen und verifizieren.

   Citrix Endpoint Management stellt dem Gerät alle verbleibenden notwendigen Apps zur Verfügung.

Erneute Registrierung der ADP-fähigen Geräte

ADP-fähige Geräte werden über eine Bedingung zum Zurücksetzen auf die Werkseinstellungen registriert. Um ein ADP-fähiges Gerät erneut zu registrieren, müssen Sie zunächst sämtliche Daten löschen, um die Registrierung des Geräts aufzuheben. Verfahren:

1. Wählen Sie das Gerät auf der Seite **Verwalten > Geräte** aus.
2. Klicken Sie auf **Sicherheit**.
3. Klicken Sie auf **Vollständig löschen**, um die Registrierung des Geräts aufzuheben und es auf die Werkseinstellungen zurückzusetzen.

4. Starten Sie das Gerät.

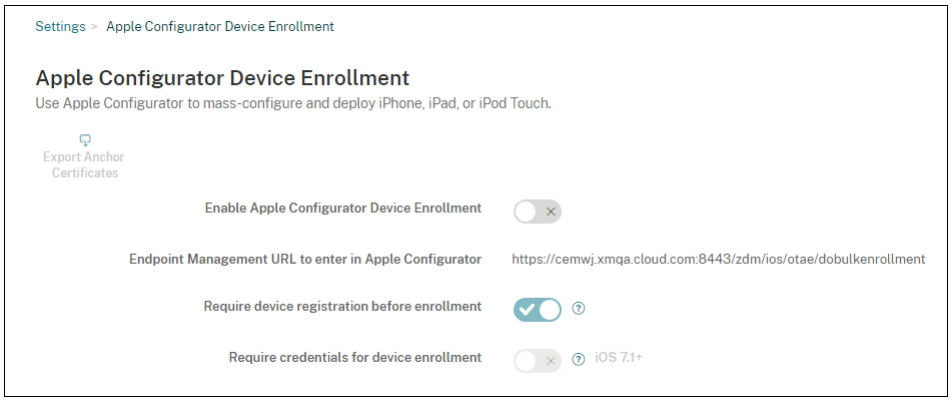
> **Wichtig:**
>
> Verwenden Sie nicht **Selektives Löschen**, um die Registrierung eines ADP-fähigen Geräts aufzuheben, da das Gerät für die ADP-Registrierung auf die Werkseinstellungen zurückgesetzt werden muss.

Bereitstellen von Geräten mit Apple Configurator 2

Mit Apple Configurator 2 können Sie eine große Anzahl von Geräten mit Einstellungen, Apps und Daten bereitstellen und diese Geräte in Citrix Endpoint Management registrieren.

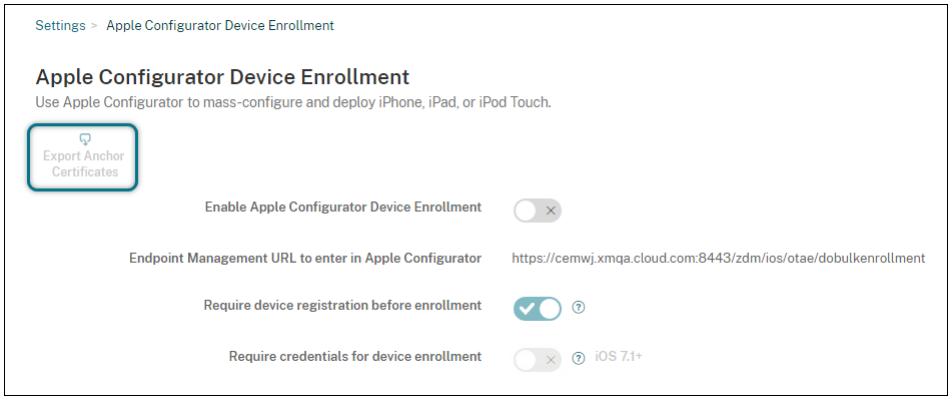
Schritt 1: Konfigurieren von Einstellungen in Citrix Endpoint Management

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Apple Configurator-Geräteregistrierung**.



2. Wählen Sie für **Apple Configurator - Geräteregistrierung aktivieren** die Einstellung **Ja**.
3. Kopieren Sie die Einstellung für die **Registrierungs-URL zum Eingeben in Apple Configurator** und fügen Sie diese URL beim Konfigurieren der Einstellungen in Apple Configurator 2 ein. Diese Einstellung liefert die URL für den Citrix Endpoint Management-Server, der mit Apple kommuniziert. Die Registrierungs-URL entspricht dem vollqualifizierten Domänennamen (z. B. `mdm.server.url.com`) oder der IP-Adresse des Citrix Endpoint Management-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 Citrix Endpoint Management 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. Die Standardeinstellung ist **Nein**.

> **Hinweis:**
>
> Wenn der Citrix Endpoint Management-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. Bereiten Sie einen Mac mit macOS 10.7.2 oder höher vor, auf dem Apple Configurator 2 installiert ist.
2. Schließen Sie Apple-Geräte über ein Apple Dock Connector-auf-USB-Kabel am Mac an. 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 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 Citrix Endpoint Management-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.

Hinzufügen von Geräten zu ABM oder ASM mit Apple Configurator 2

iPhone-, iPad- und Apple TV-Geräte können Sie auch mit Apple Configurator 2 zu Ihrem ABM- oder ASM-Konto hinzufügen, unabhängig davon, wo die Geräte gekauft wurden.
Hinzugefügte Geräte werden im Abschnitt **Geräte** angezeigt. Diese Geräte enthalten keine Registrierungseinstellungen mehr, die über Apple Configurator 2 zugewiesen wurden. Weitere Informationen finden Sie im Apple Business Manager-Benutzerhandbuch oder im Apple School Manager-Benutzerhandbuch.

Erneuern des ADP-Tokens

Wenn Ihr ADP-Token abläuft, zeigt Citrix Endpoint Management eine Lizenzablaufwarnung an. Ersetzen Sie den Token von ASM oder ABM.

Schritt 1. Laden Sie einen öffentlichen Schlüssel vom Citrix Endpoint Management-Server herunter

1. Gehen Sie in der Citrix Endpoint Management-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 ABM an, um den Token herunterzuladen.
2. Öffnen Sie **Einstellungen** und wählen Sie den Server aus, von dem Sie ein Token benötigen. Klicken Sie auf **Bearbeiten**.
3. Laden Sie unter **MDM Server Settings** den neuen öffentlichen Schlüssel hoch, den Sie von Citrix Endpoint Management heruntergeladen haben, und speichern Sie die Änderungen.
4. Klicken Sie auf **Token herunterladen**, um den neuen Token herunterzuladen.

Schritt 3: Hochladen einer Servertokendatei in Citrix Endpoint Management

1. Gehen Sie in Citrix Endpoint Management 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.

Integration von Apple Bildung-Features

June 25, 2024

Sie können Citrix Endpoint Management für die Mobilgeräteverwaltung (MDM) in einer Umgebung mit Apple Bildung verwenden. Citrix Endpoint Management unterstützt Apple School Manager (ASM) und die Classroom-App für iPad. Mit der Citrix Endpoint Management-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 Citrix Endpoint Management, eine verwaltete Apple-ID mit einem neuen Kennwort und erforderliche Volume Purchase-Apps sowie iBooks.

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.

Apple School Manager

Führen Sie diesen allgemeinen Schritte aus, um Citrix Endpoint Management in ASM zu integrieren.

1. Erstellen Sie ein Konto für Ihre Institution in ASM, um Ihre Institution bei ASM zu registrieren.
2. Konfigurieren Sie ein Education Volume Purchase-Konto für Apple School Manager.
3. Fügen Sie Kennwörter für Apple School Manager-Benutzer hinzu.
4. Fügen Sie Citrix Endpoint Management Ressourcen und Bereitstellungsgruppen hinzu.
5. Testen Sie die Registrierung von Geräten der Benutzer
6. Stellen Sie Lehrkräften und Lernenden vorkonfigurierte Geräte bereit.
7. Lehrkräfte, Lernende und Unterrichtsdate verwalten
8. Wenn ein Gerät verloren geht oder gestohlen wird, können Sie das Gerät sperren und orten.

Informationen zum Registrieren bei ASM und zum Verbinden Ihres Kontos mit Citrix Endpoint Management finden Sie unter Bereitstellen von Geräten über das Apple-Bereitstellungsprogramm.

Voraussetzungen

- NetScaler Gateway
- Für MDM+MAM konfiguriertes Registrierungsprofil
- Apple iPad 3. Generation (Mindestversion) oder iPad Mini mit iOS 9.3 (Mindestversion)

> **Hinweis:**
>
> Citrix Endpoint Management validiert ASM-Benutzerkonten nicht anhand von LDAP oder Active Directory. Sie können Citrix Endpoint Management 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) Citrix Secure Mail und Citrix 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 NetScaler Gateway-Authentifizierung unterstützt keine lokalen Benutzer (nur Active Directory-Benutzer). Aus diesem Grund stellt Citrix Endpoint Management nur erforderliche Volume Purchase-Apps und -iBooks auf den Geräten von Lehrkräften und Lernenden bereit.

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, Weblinks teilen und öffnen und den Bildschirm von Lernenden auf Apple TV anzeigen.

Classroom steht im App-Store kostenlos zur Verfügung. Sie laden die App in die Citrix Endpoint Management-Konsole hoch. Anschließend konfigurieren Sie die App mit der Geräterichtlinie “Bildungseinrichtung - Konfiguration”die Sie auf den Geräten der Lehrkräfte bereitstellen.

Weitere Informationen zum Bereitstellen der Classroom-App finden Sie unter Verteilen von Apple-Apps.

Weitere Informationen zu den Anforderungen, der Einrichtung und den Funktionen von Classroom-Apps finden Sie im Classroom-Benutzerhandbuch auf der Apple-Supportseite.

Hinzufügen von Kennwörtern für Apple School Manager-Benutzer

Nachdem Sie ein ASM-Konto hinzugefügt haben, importiert Citrix Endpoint Management Klassen und Benutzer aus ASM. Citrix Endpoint Management behandelt Klassen als lokale Gruppen, daher werden

Sie in der Konsole als “Gruppe”angezeigt. Wenn eine Klasse in ASM einen Gruppennamen hat, weist Citrix Endpoint Management der Klasse den Gruppennamen zu. Andernfalls verwendet Citrix Endpoint Management die Quellsystem-ID als Gruppennamen. Citrix Endpoint Management verwendet den Kursnamen nicht als Klassennamen, da Kursnamen im ASM nicht eindeutig sind.

Citrix Endpoint Management 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 Citrix Endpoint Management keinen Verzeichnisserver, um diese neuen Benutzer zu authentifizieren.

ASM sendet keine temporären Benutzerkennwörter an Citrix Endpoint Management. Sie können sie aus einer CSV-Datei importieren oder manuell hinzufügen. Gehen Sie zum Importieren temporärer Benutzerkennwörter folgendermaßen vor:

1. Öffnen 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 Citrix Endpoint Management 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!`

   Ort:

   Benutzer: `user@appleid.citrix.com`

   Vorname: `Firstname`

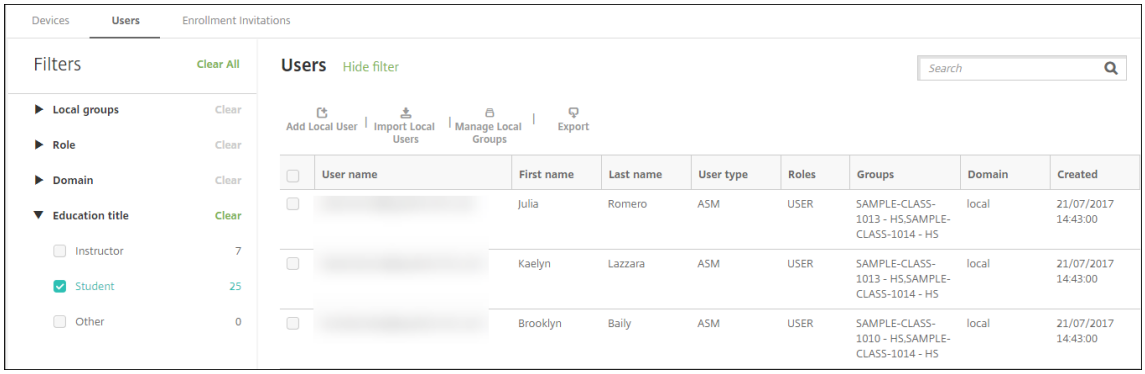
   Weiterer Vorname: `Middle`

   Nachname: `Lastname`

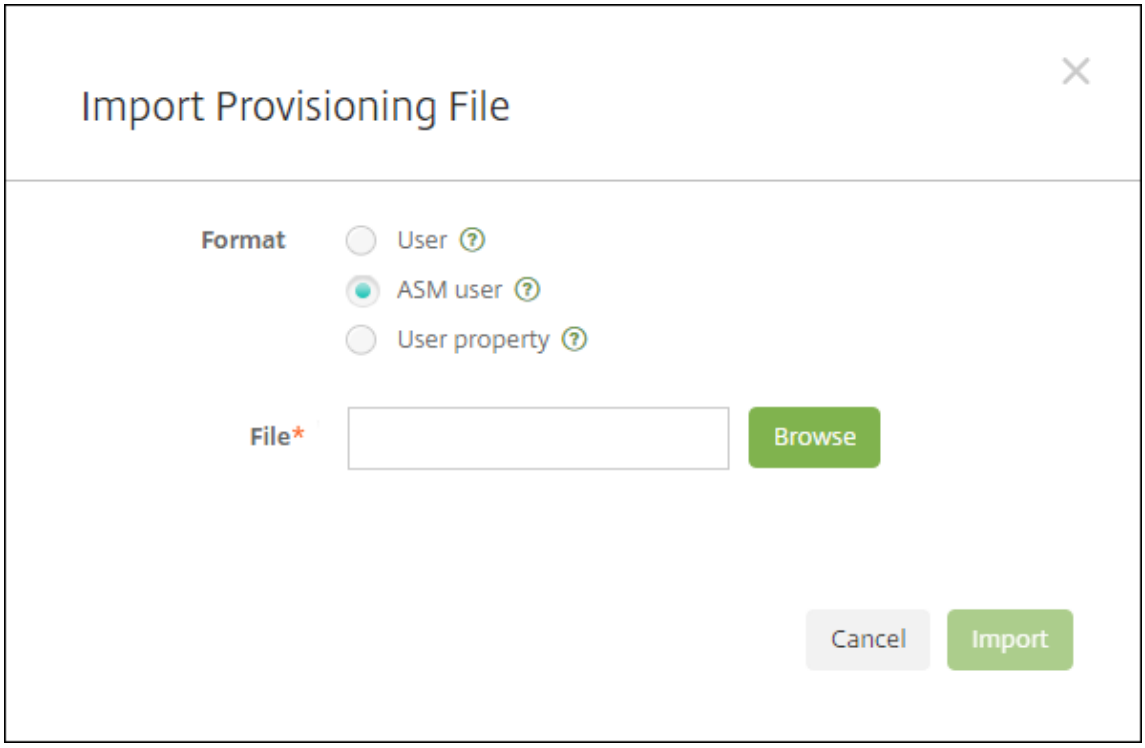
   Kennwort: `Password123!`
3. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Verwalten > Benutzer**. Die Seite **Benutzer** wird angezeigt.

   Das Beispiel der Seite **Verwalten > Benutzer** zeigt eine Liste der Benutzer, die aus ASM importiert wurde. In der Liste **Benutzer**:

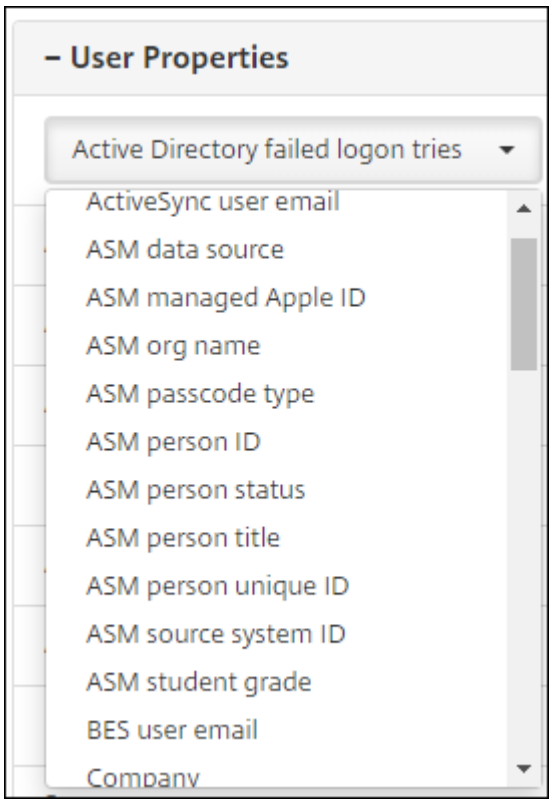
   - **Benutzername** enthält die verwaltete Apple-ID.
   - Der Benutzertyp ist **ASM**, d. h. das Konto stammt aus ASM.
   - Unter **Gruppen** werden die Klassen angezeigt.



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. Citrix Endpoint Management erfordert eine verwaltete Apple-ID für die Authentifizierung.
- **ASM-Organisationsname:** Name, den Sie dem Konto in Citrix Endpoint Management 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).

Hinzufügen von Ressourcen und Bereitstellungsgruppen zu Citrix Endpoint Management

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:

  Citrix Endpoint Management erfordert, dass Sie Volume Purchase-Apps für Bildungsbenutzer als erforderliche Apps bereitstellen. Die Bereitstellung solcher Volume Purchase-Apps als optional wird nicht von Citrix Endpoint Management unterstützt.

  Wenn Sie Apple Classroom verwenden, stellen Sie die App nur für Geräte von Lehrkräften bereit.

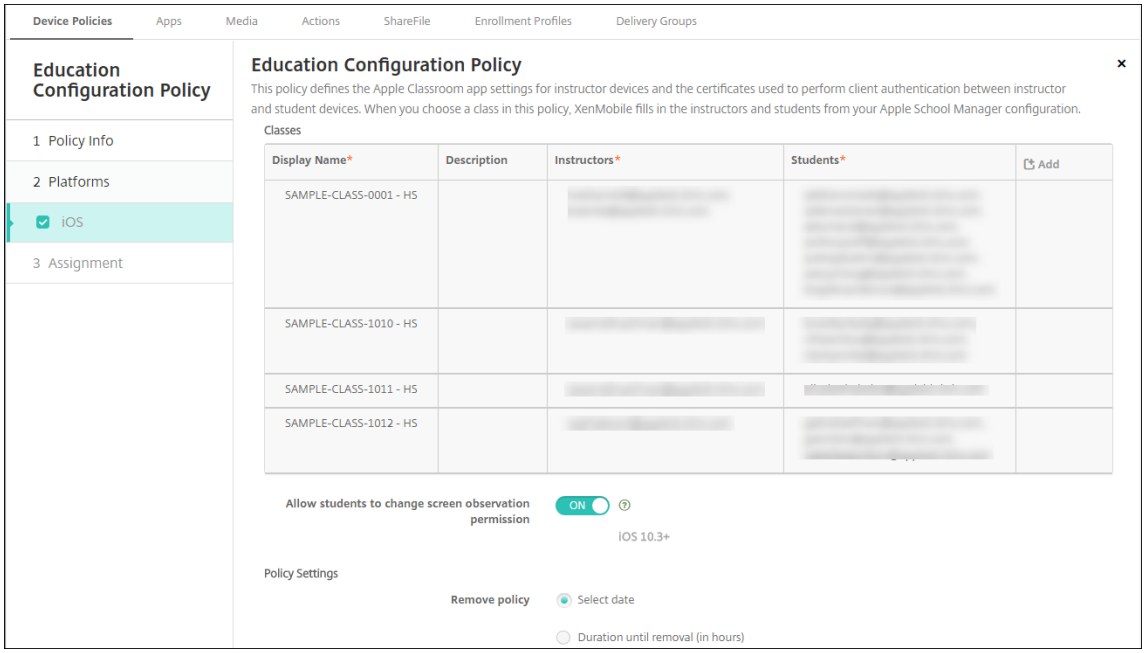
  Stellen Sie alle anderen Apps bereit, die Sie Lehrkräften oder Lernenden zur Verfügung stellen möchten. Bei dieser Lösung wird Citrix Secure Hub nicht verwendet und muss daher nicht für Lehrkräfte oder Lernende bereitgestellt werden.

- Volume Purchase-iBooks:

  Wenn Citrix Endpoint Management eine Verbindung mit Ihrem ASM-Konto hergestellt hat, werden Ihre gekauften iBooks in der Citrix Endpoint Management-Konsole unter **Konfigurieren > Medien** angezeigt. Der auf der Seite aufgelisteten iBooks können Bereitstellungsgruppen hinzugefügt werden. Citrix Endpoint Management 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 Citrix Endpoint Management-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".

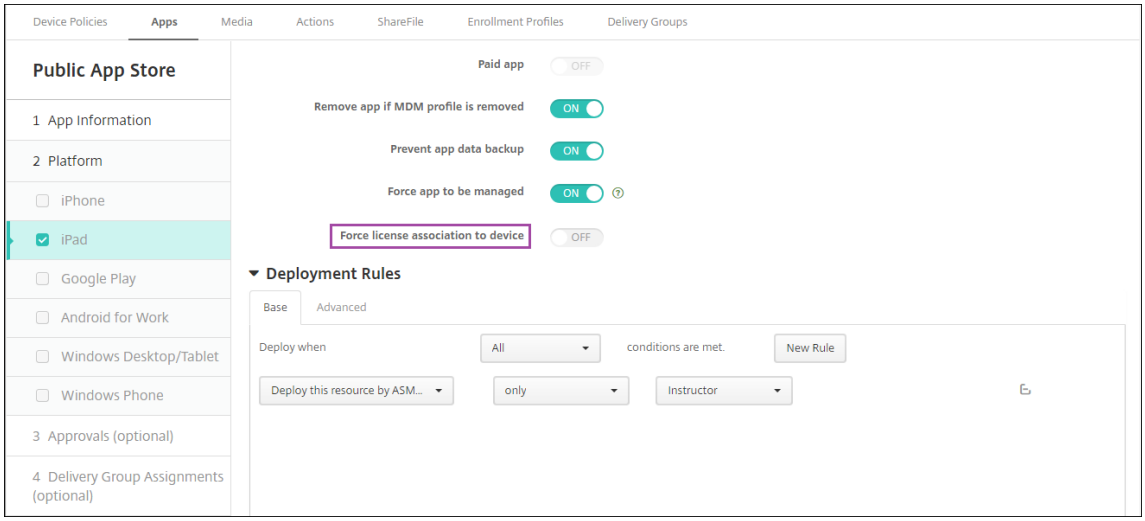


Informationen zu Geräterichtlinien finden Sie unter Geräterichtlinien und in den Artikeln zu den einzelnen Richtlinien.

2. Konfigurieren Sie Apps (**Konfigurieren > Apps**) und iBooks (**Konfigurieren > Media**).

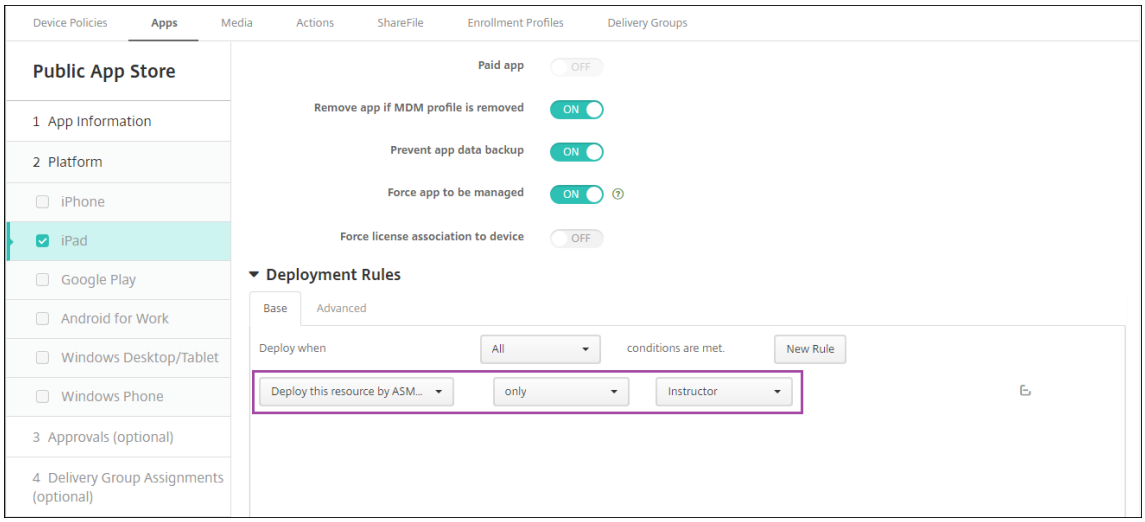
   - Standardmäßig weist Citrix Endpoint Management Apps und iBooks auf Benutzerebene zu. Bei der ersten Bereitstellung erhalten Lehrkräfte und Lernende eine Aufforderung zur Registrierung bei ASM. Nach Annahme der Einladung erhalten die Nutzer ihre ASM-Apps und iBooks bei der nächsten Bereitstellung (innerhalb 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 am Volume Purchase Program.



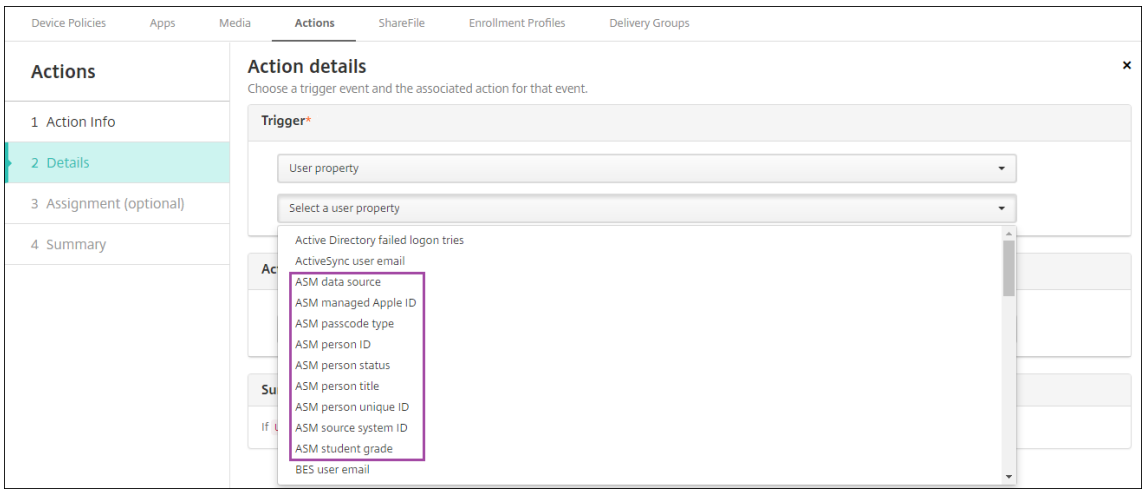
- Um eine App nur für Lehrkräfte bereitzustellen, wählen Sie eine Bereitstellungsgruppe aus, die nur Lehrkräfte umfasst, oder verwenden Sie die folgende Bereitstellungsregel:

```
Deploy this resource by ASM device type
only
Instructor
<!--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).

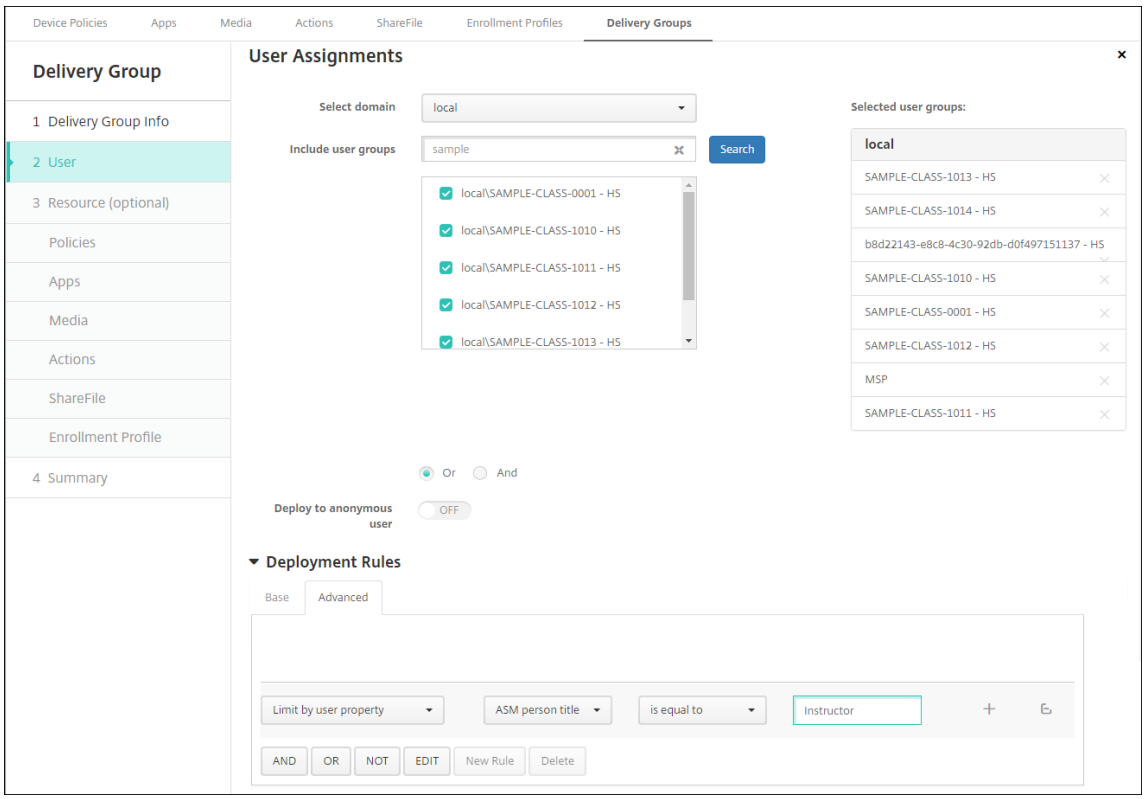


Zum Erstellen einer Aktion gehen Sie zu **Konfigurieren > Aktionen**. Informationen zum Konfigurieren von Aktionen finden Sie unter Automatisierte Aktionen.

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.

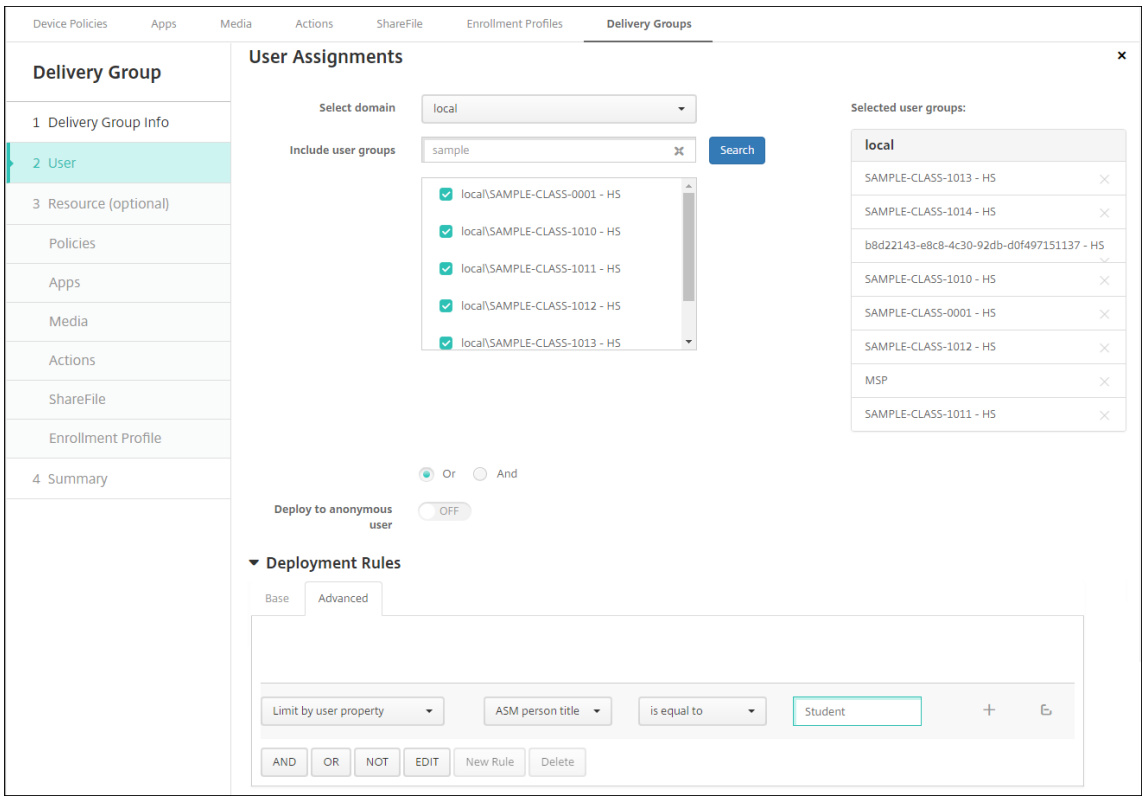
   Die folgenden Benutzerzuweisungen gelten beispielsweise für Lehrkräfte. Die Bereitstellungsregel lautet:

```
Limit by user property
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```

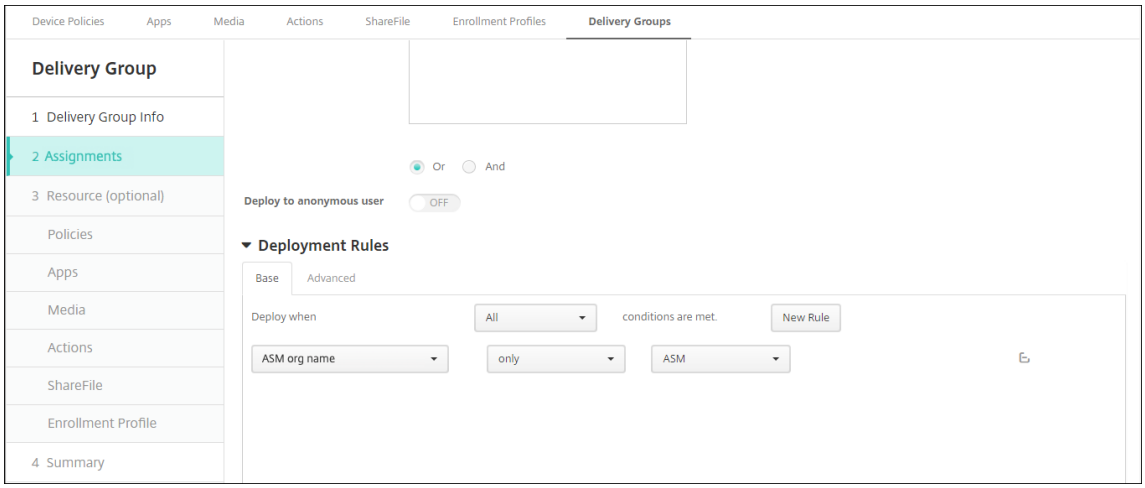



Die folgenden Benutzerzuweisungen gelten für Lernende. Die Bereitstellungsregel lautet:

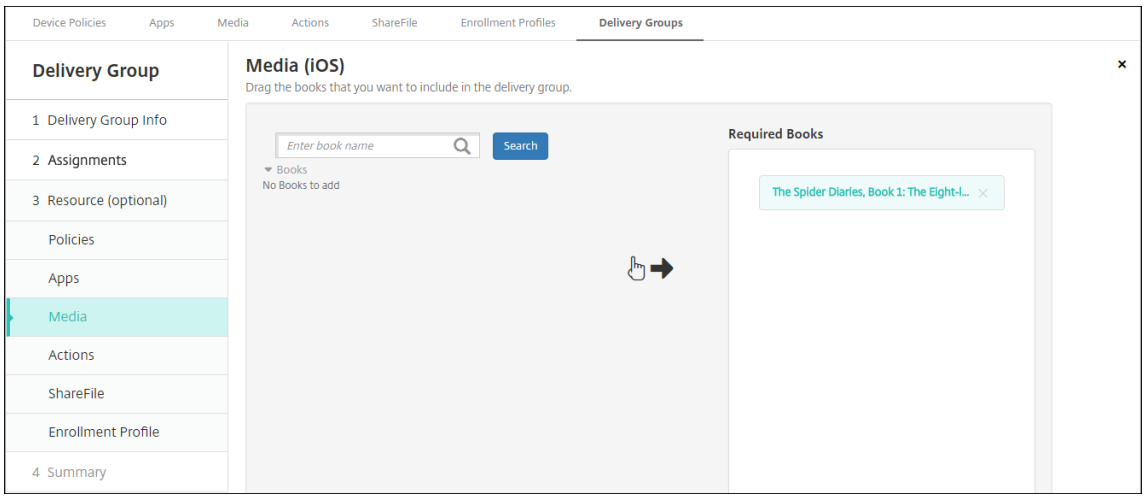
```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

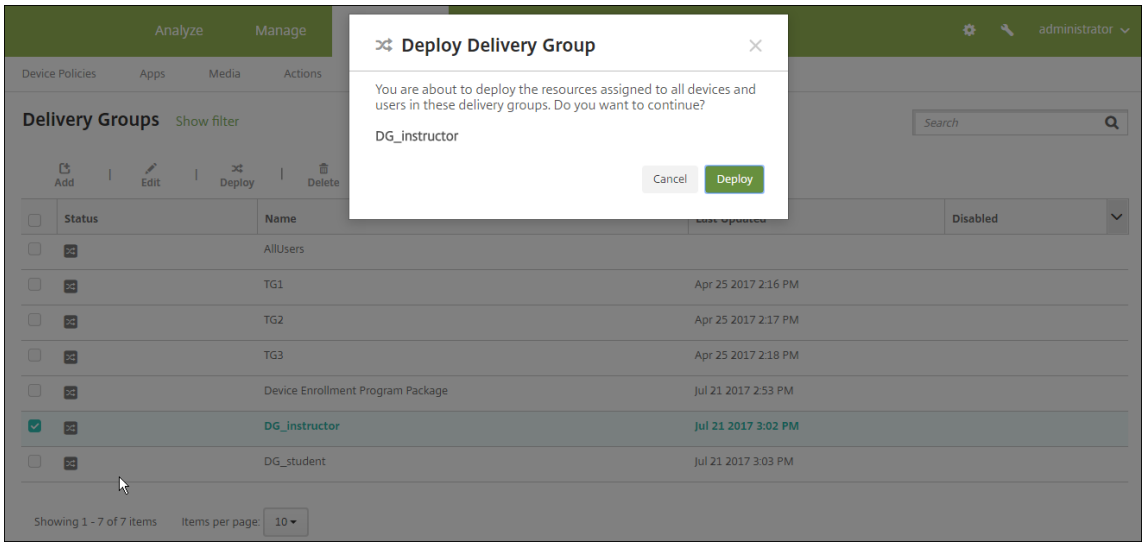
Sie können Bereitstellungsgruppen auch nach einer auf dem ASM-Organisationsnamen basierenden Bereitstellungsregel filtern.



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 Ressourcen bereitstellen in den Abschnitten "Bereitstellungsgruppe bearbeiten"und "In Bereitstellungsgruppen bereitstellen".

Testen der Registrierung von Geräten der Benutzer

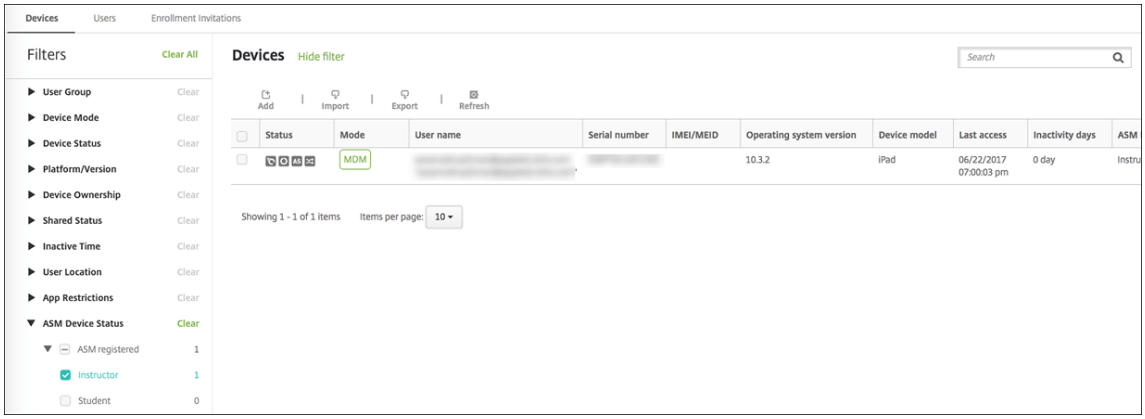
Sie können Geräte von Lehrkräften und Lernenden mit einer der folgenden Methoden registrieren:

- Eine Verwaltungskraft kann die Geräte mithilfe des Benutzerkennworts registrieren, das Sie in der Citrix Endpoint Management-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 Citrix Endpoint Management Geräterichtlinien, Apps und Medien an die Geräte.

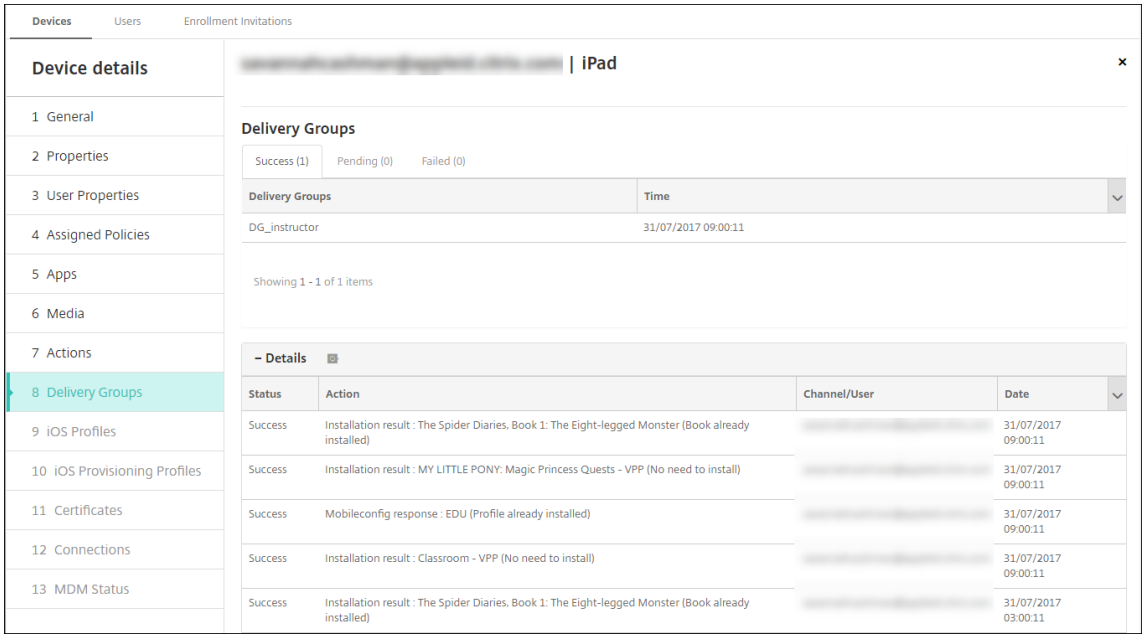
Verwenden Sie zum Testen der Registrierung Apple-Bereitstellungsprogrammgeräte, die mit ASM verknüpft sind.

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.



Geräte verteilen

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:

- Citrix Endpoint Management-Kennwort für die Registrierung
- Temporäres ASM-Kennwort für die verwaltete Apple-ID

Für die Benutzer läuft die Inbetriebnahme folgendermaßen ab:

1. Wenn Benutzer ein Gerät nach der Rücksetzung auf die Werkseinstellungen zum ersten Mal starten, werden sie von Citrix Endpoint Management im Registrierungsbildschirm zum Registrieren des Geräts aufgefordert.
2. Benutzer geben das Kennwort für die verwaltete Apple-ID an sowie das Kennwort für die Authentifizierung bei Citrix Endpoint Management.
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 Citrix Endpoint Management 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).

Lehrkräfte, Lernende und Unterrichtsdate verwalten

Beim Verwalten von Lehrkräften, Lernenden und Unterrichtsdaten ist Folgendes zu beachten:

- Ändern Sie keine verwalteten Apple-IDs, nachdem Sie ASM-Informationen in Citrix Endpoint Management importiert haben. Auch Citrix Endpoint Management verwendet ASM-Benutzer-IDs zum Identifizieren 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.

- Wenn Sie eine Lehrkraft für eine Klasse nach dem Bereitstellen der Geräterichtlinie "Bildung - Konfiguration"ändern, vergewissern Sie sich, dass die Richtlinie in der Citrix Endpoint Management-Konsole aktualisiert wird, und stellen Sie sie dann erneut bereit.
- Wenn Sie die Benutzereigenschaften im ASM-Portal aktualisieren, aktualisiert Citrix Endpoint Management diese Eigenschaften auch in der Konsole. Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management-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 Citrix Endpoint Management diesen Benutzer nach einem Abruf auch aus der Citrix Endpoint Management-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.

Verlorenes oder gestohlenes Gerät verwalten

Der Apple-Service Find My iPhone/iPad enthält ein Feature zur Aktivierungssperre. Die Aktivierungssperre verhindert, dass nicht autorisierte Benutzer ein verlorenes oder gestohlenes

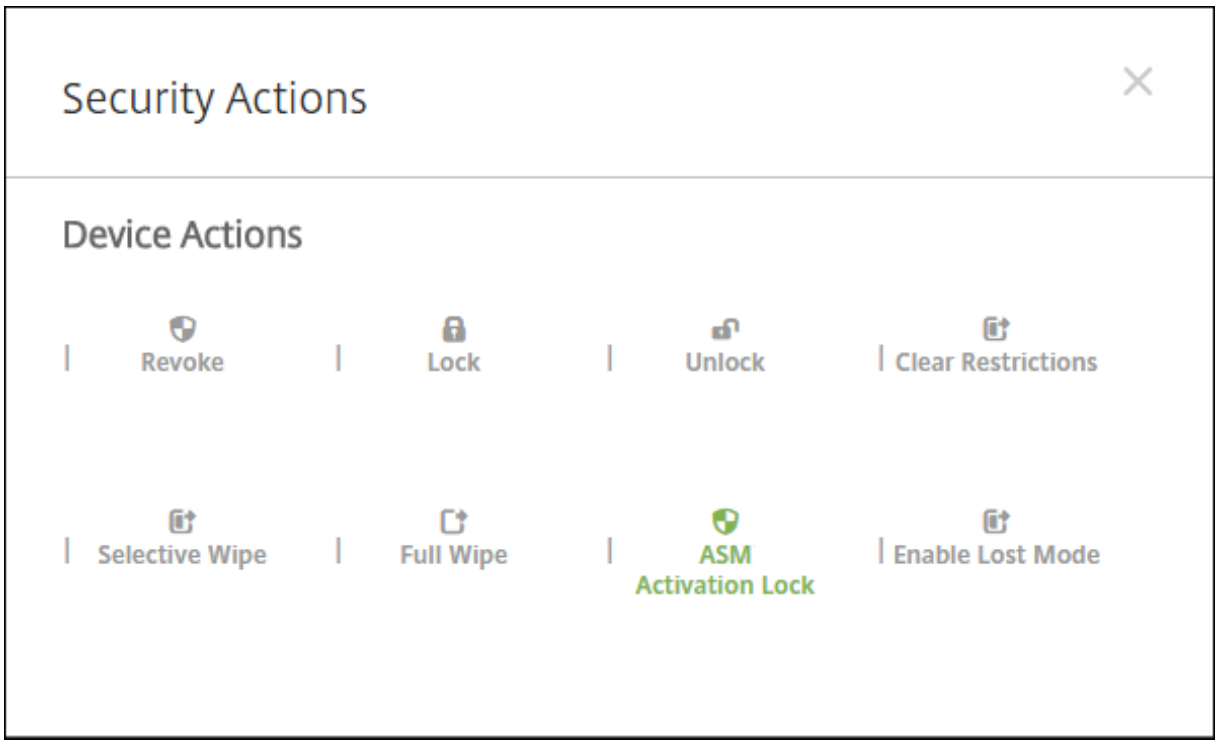
Gerät, das beim Apple-Bereitstellungsprogramm registriert ist, verwenden oder verkaufen.

Citrix Endpoint Management enthält die Sicherheitsaktion **ASM-Aktivierungssperre**, mit der Sie einen Sperrcode an Geräte senden, die mit dem ASM-Apple-Bereitstellungsprogramm registriert sind.

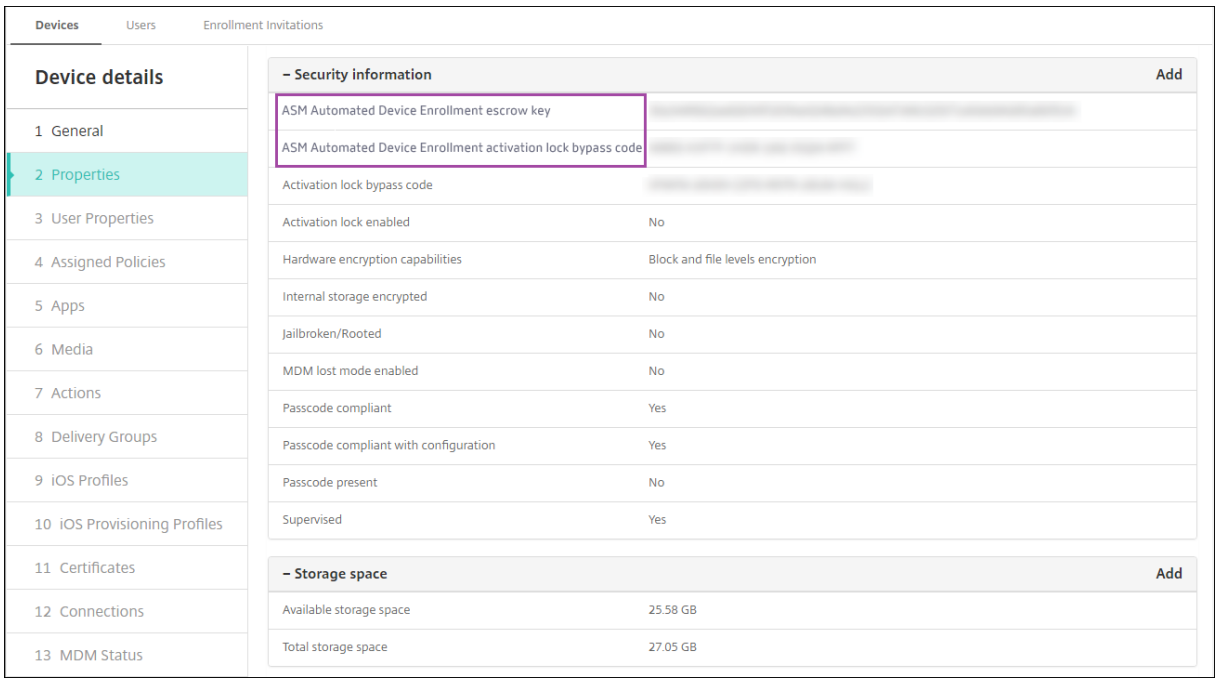
Wenn Sie die Sicherheitsaktion **ASM-Aktivierungssperre** verwenden, kann Citrix Endpoint Management Geräte orten, ohne dass der Find My iPhone/iPad-Service vom Benutzer aktiviert werden muss. Wenn ein ASM-Gerät auf die Werkseinstellungen zurückgesetzt wurde oder alle Daten auf dem Gerät gelöscht wurden, 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 die Anmeldung auch leer lassen und den Code zum Umgehen der **ASM-Aktivierungssperre** als Kennwort eingeben. Diese Informationen stehen auf der Registerkarte **Eigenschaften** unter **Gerätedetails** zur Verfügung.

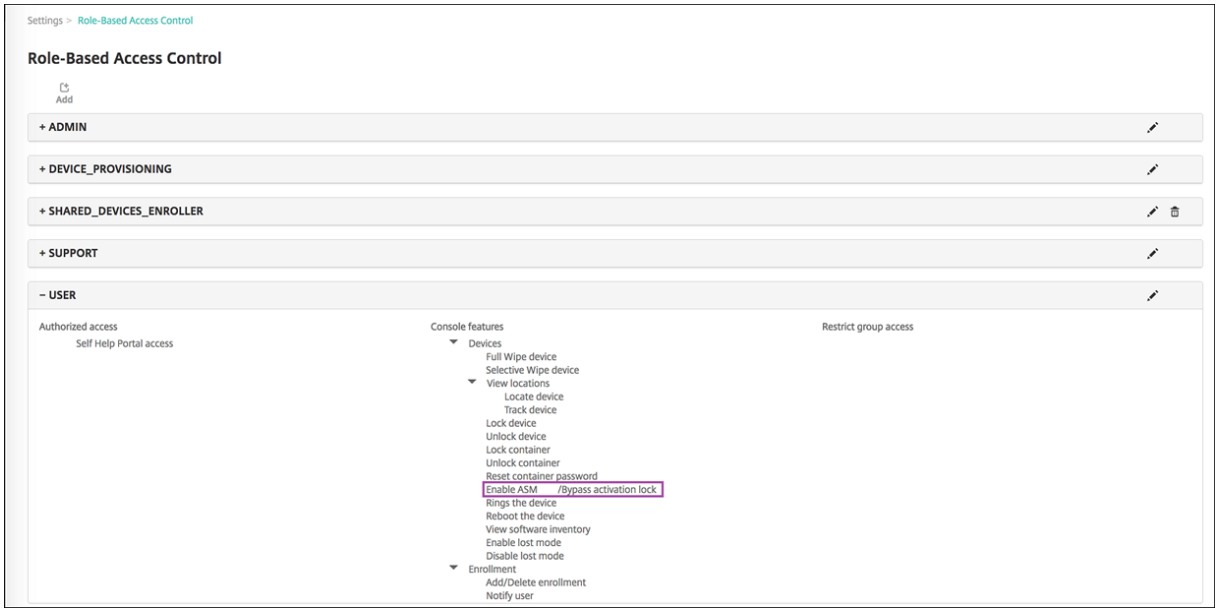
Um die Aktivierungssperre festzulegen, wählen Sie unter **Verwalten > Geräte** das Gerät aus, klicken Sie auf **Sicherheit** und dann auf **ASM-Aktivierungssperre**.



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**.



Geteilte iPads

June 25, 2024

Das Feature für geteilte iPads ermöglicht es mehreren Benutzern, ein iPad zu verwenden. Die Be-

nutzererfahrungen können personalisiert werden, obwohl die Geräte gemeinsam genutzt werden. Sie können geteilte iPads für Bildungs- oder Geschäftszwecke verwenden. Apple School Manager (ASM) unterstützt zusätzlich zu den Rollen, die Apple Business Manager (ABM) unterstützt, die Rollen des Kursleiters und der Schüler.

Voraussetzungen für geteilte iPads

- Apple School Manager oder Apple Business Manager
- Citrix Endpoint Management
- Beliebiges iPad Pro, iPad 5. Generation, iPad Air 2 oder später und iPad mini 4 oder später
- Mindestens 32 GB Speicherplatz
- Betreute Geräte

Konfigurieren von geteilten iPads

Mehrere Lernende bzw. Mitarbeiter können ein iPad für verschiedene Zwecke teilen.

Sie oder die Gerätebesitzer registrieren geteilte iPads und stellen dann Geräterichtlinien, Apps und Medien auf den Geräten bereit. Die Benutzer 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.

Citrix Endpoint Management verwendet zwei Kommunikationskanäle für geteilte iPads: den Systemkanal für den Gerätebesitzer (Lehrkraft bzw. Vorgesetzter) und den Benutzerkanal für den aktuellen Benutzer (Lernender bzw. Mitarbeiter). Citrix Endpoint Management verwendet diese Kanäle, um die entsprechenden MDM-Befehle für die von Apple unterstützten Ressourcen zu senden.

Über den Systemkanal bereitgestellte Ressourcen:

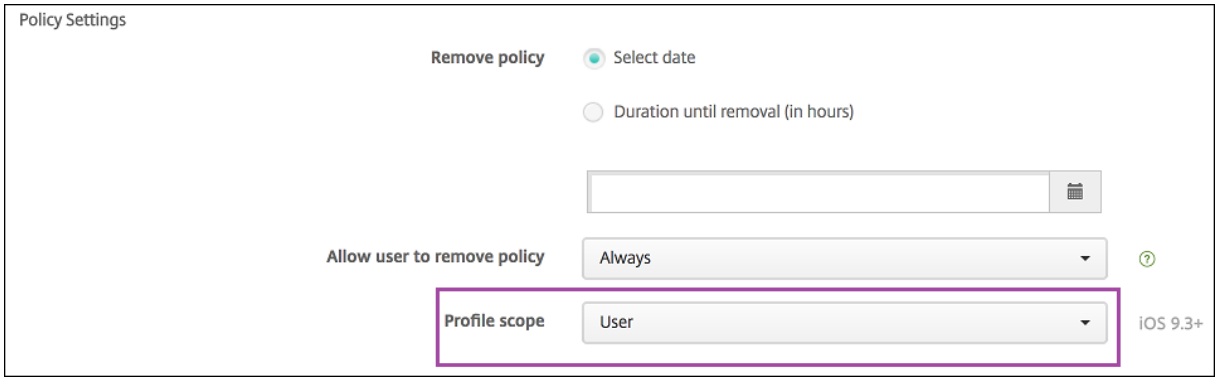
- Geräterichtlinien, z. B. Bildungseinrichtung - Konfiguration, Meldung auf Sperrbildschirm, maximale Anzahl residenter Benutzerund Passcodesperre - Kulanzzeitraum
- Gerätebasierte Volume Purchase-Apps
  Apple unterstützt auf geteilten iPads weder Unternehmensapps noch benutzerbasierte Volume Purchase-Apps. 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, Layout für Homebildschirm, Einschränkungen und Webclip.

  Citrix Endpoint Management 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 Gerätebesitzern vorkonfigurierte und betreute iPads zur Verfügung. Diese Personen verteilen die Geräte dann an Lernende bzw. Mitarbeiter. Wenn Sie keine vorinstallierten iPads verteilen, müssen Sie den Gerätebesitzern ihr Citrix Endpoint Management-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 Citrix Endpoint Management-Konsole ASM- bzw. ABM-Konten mit aktiviertem **Freigabemodus** hinzu (**Einstellungen > Apple-Bereitstellungsprogramm**). Weitere Informationen finden Sie weiter unten unter "Verwalten von Konten für geteilte iPads".
2. Sie fügen in Citrix Endpoint Management die erforderlichen Geräterichtlinien, Apps und Medien gemäß den Informationen in diesem Abschnitt hinzu. Sie weisen die Ressourcen Bereitstellungsgruppen zu.
3. Sie bitten die Gerätebesitzer, auf den geteilten iPads eine Rücksetzung auf die Werkseinstellungen durchzuführen. Der Remoteverwaltungsbildschirm für die Registrierung wird angezeigt.
4. Die Gerätebesitzer registrieren die geteilten iPads.
   Citrix Endpoint Management stellt konfigurierte Ressourcen für jedes registrierte, geteilte iPad bereit. Nach einem automatischen Neustart können die Gerätebesitzer die Geräte mit Benutzern teilen. Eine Anmeldeseite wird auf dem iPad angezeigt.

5. Ein Gerätebenutzer gibt seine Managed Apple-ID und sein temporäres ASM-Kennwort ein. Es erfolgt die Authentifizierung des iPads bei ASM und der Benutzer wird aufgefordert, ein ASM-Kennwort zu erstellen. Bei der nächsten Anmeldung auf dem geteilten iPad gibt der Benutzer das neue ASM-Kennwort ein.
6. Es kann sich dann ein weiterer Benutzer, der das iPad ebenfalls verwendet, unter Wiederholung des vorigen Schritts anmelden.

Verwalten von Konten für geteilte iPads

Wenn Sie Citrix Endpoint Management bereits für Apple Bildung oder Apple für Unternehmen verwenden, haben Sie in Citrix Endpoint Management ein für nicht geteilte Geräte (z. B. Geräte der Lehrkräfte) konfiguriertes ASM-Konto. Sie können dasselbe ASM-/ABM-Konto und denselben Citrix Endpoint Management-Server parallel für geteilte und nicht geteilte Geräte verwenden.

Einteilen geteilter iPads in Gerätegruppen

In ASM/ABM 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 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 Citrix Endpoint Management-Konsole mehrere ASM/ABM-Konten erstellen, importieren Sie automatisch Gruppen geteilter iPads:

- 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:

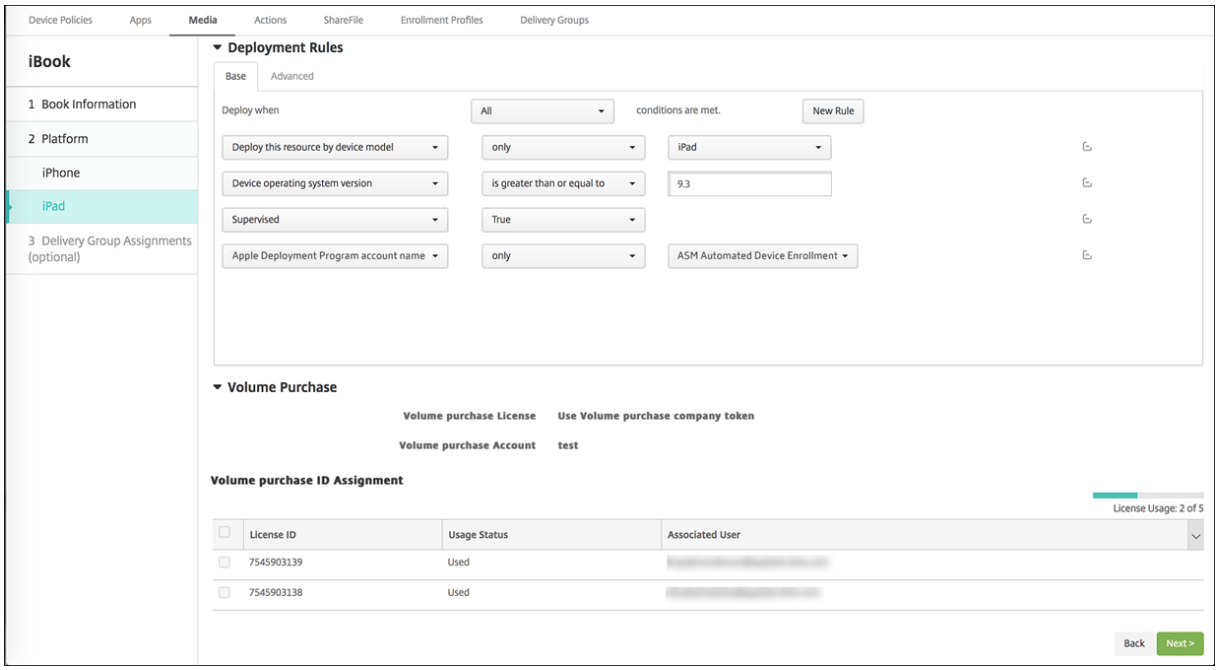
- Ein ASM/ABM-Konto pro Gerätegruppe, für das folgende Einstellungen aktiviert sind:
  - **Geräteregistrierung erforderlich**
  - **Betreuter Modus**
  - **Freigabemodus**
- Verwenden Sie für alle ASM-Konten einer Bildungseinrichtung das gleiche **Suffix der Bildungseinrichtung**.

Apps für geteilte iPads

Geteilte iPads unterstützen die Zuweisung von gerätebasierten Volume Purchase-Apps. Vor dem Bereitstellen einer App auf einem geteilten iPad sendet Citrix Endpoint Management 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 Citrix Endpoint Management eine Anforderung an den Apple Volume Purchase-Server, um Benutzern 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:

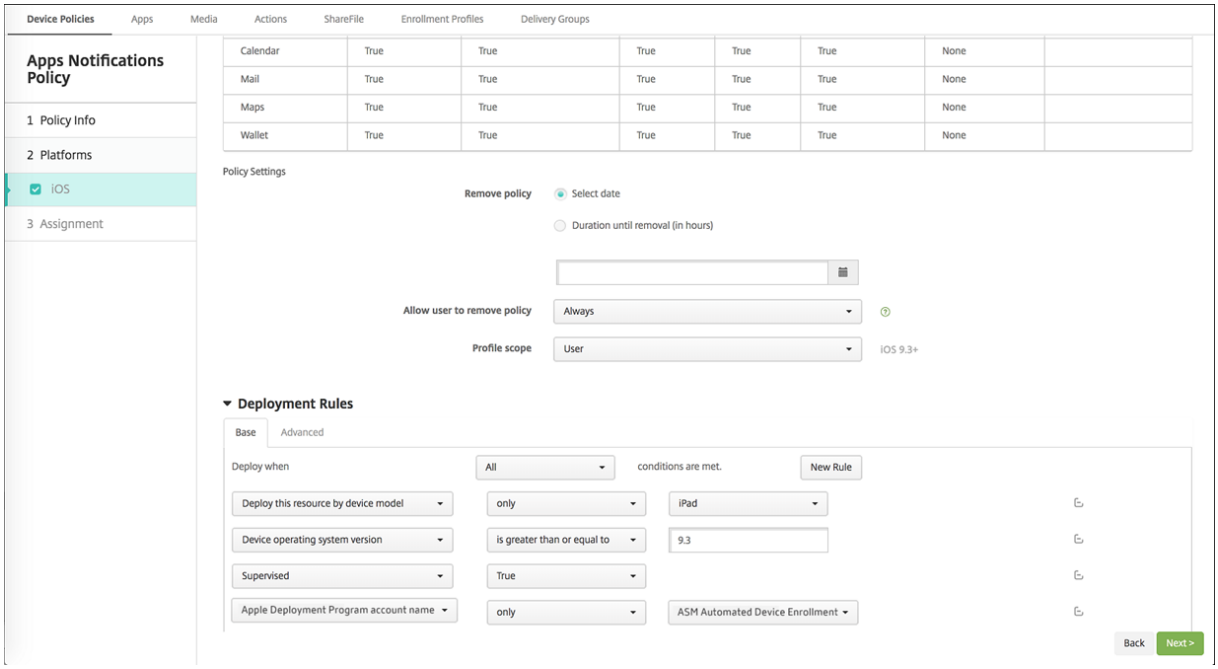

```
Apple Deployment Program account name
Only
Device Group 1 account

<!--NeedCopy-->
```

- Legen Sie für das Konto der Gerätegruppe 2 folgende Bereitstellungsregel fest:

```
Apple Deployment Program account name
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 Gerätebesitzern (für nicht geteilte iPads) bereitstellen möchten, filtern Sie die Ressourcen anhand des ASM-Teilen-Status mit folgenden Bereitstellungsregeln:

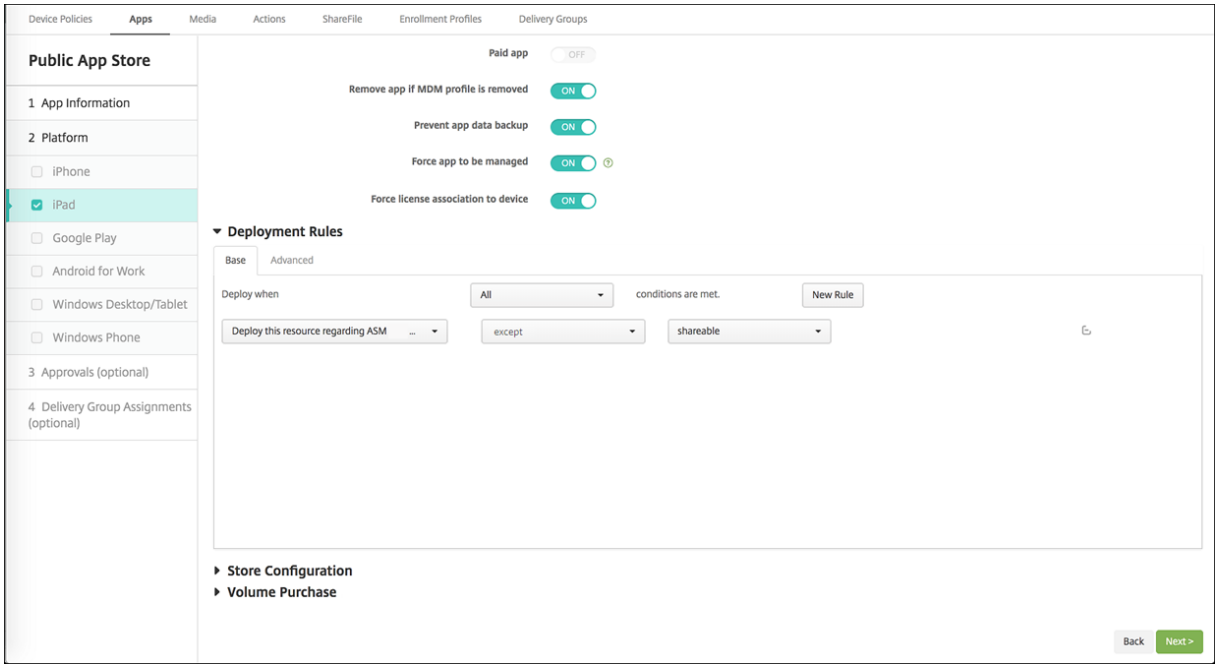
```
Deploy this resource regarding ASM/ABM shared mode
only
unshared

```



```
<!--NeedCopy-->
```

Oder:

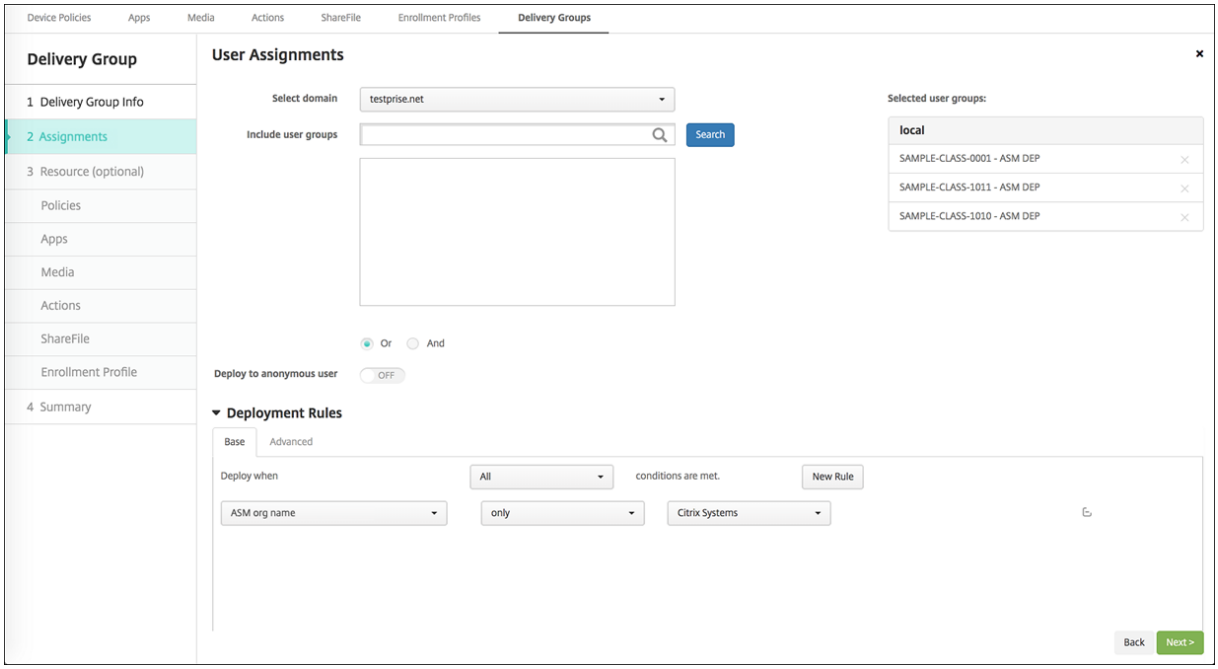
```
Deploy this resource regarding ASM/ABM shared mode
except
shareable

<!--NeedCopy-->
```



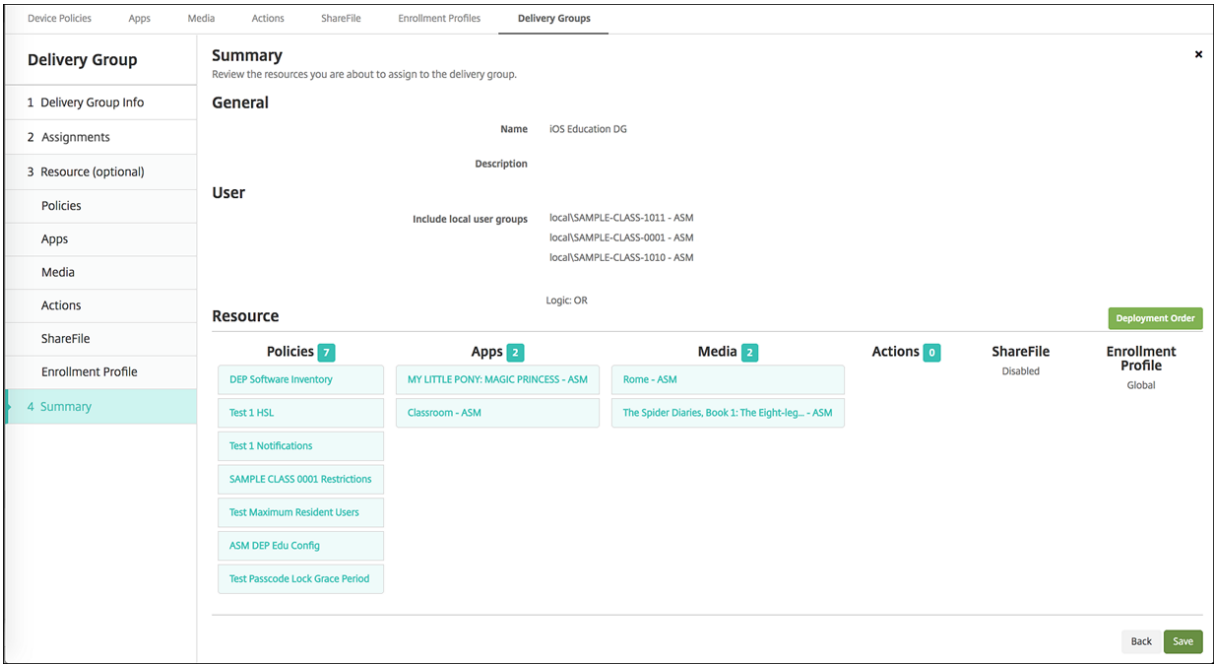
Bereitstellungsgruppen für geteilte iPads

Für die Gerätegruppe:

- Konfigurieren Sie eine Bereitstellungsgruppe. Weisen Sie für Lehrkräfte alle in der Richtlinie “Bildung - Konfiguration”definierten Klassen zu.



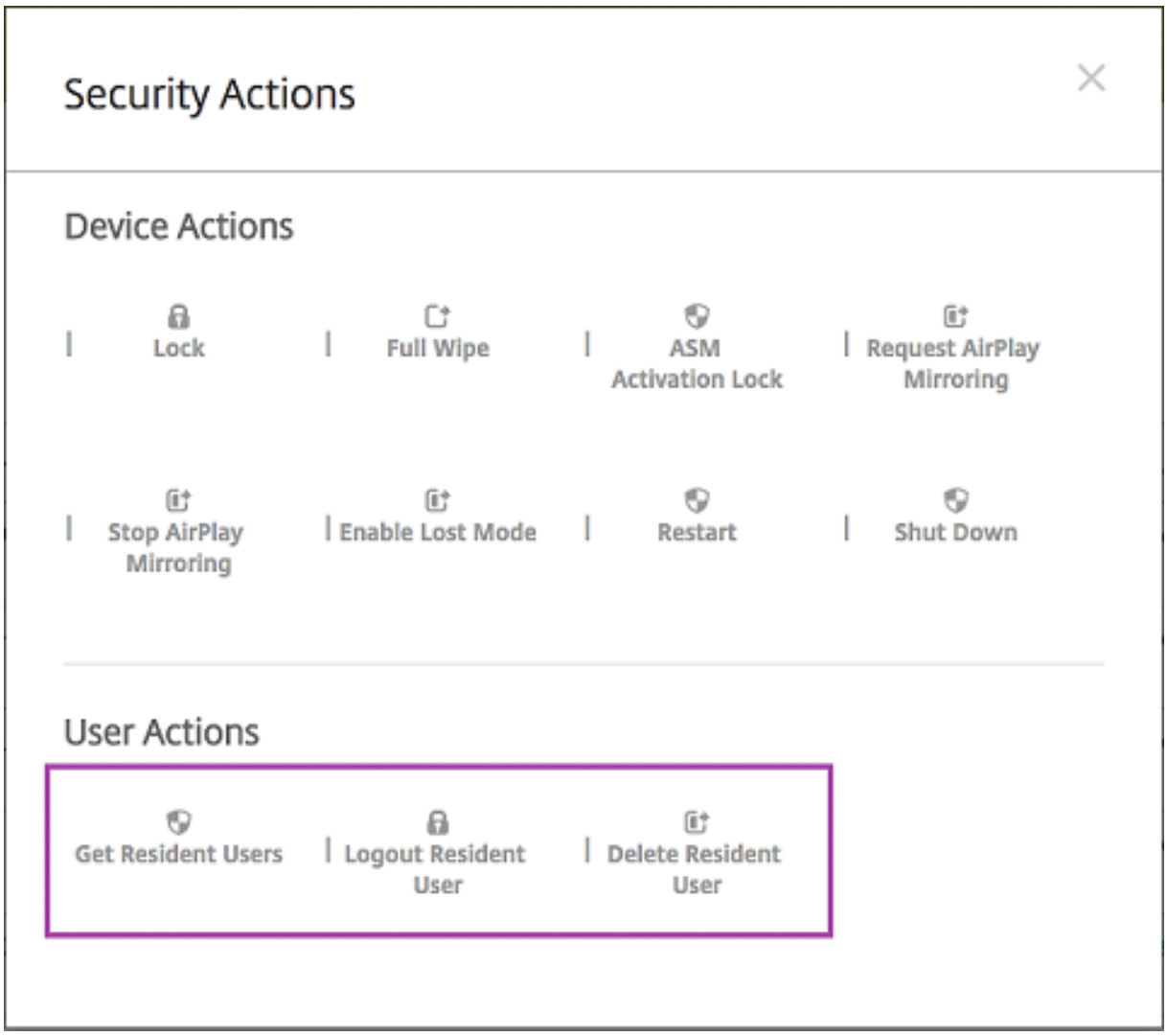
- Die Bereitstellungsgruppe muss folgende MDM-Ressourcen enthalten:
  - Geräterichtlinien:
    - Bildungseinrichtung - Konfiguration (für ASM)
    - Meldung auf Sperrbildschirm
    - App-Benachrichtigungen
    - Layout für Homebildschirm
    - Einschränkungen
    - Maximale Anzahl residenter Benutzer
    - Passcodesperre - Kulanzzeitraum
  - Erforderliche Volume Purchase-Apps
  - Erforderliche Volume Purchase-iBooks



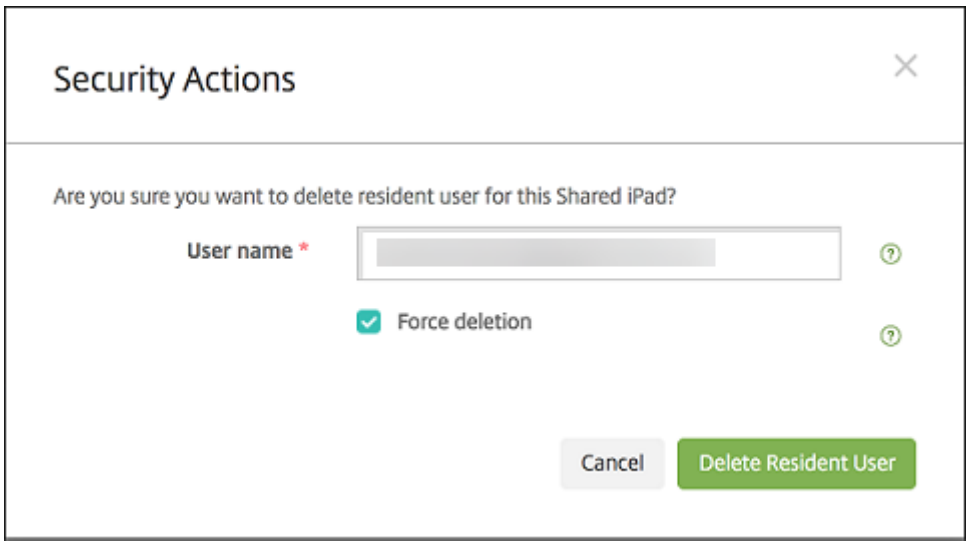
Sicherheitsaktionen für geteilte iPads

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 Citrix Endpoint Management-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.
- **Alle Benutzer löschen:** Löscht alle Benutzer auf dem Gerät.



Nachdem Sie auf **Residenten Benutzer löschen** geklickt haben, können Sie den Benutzernamen angeben.

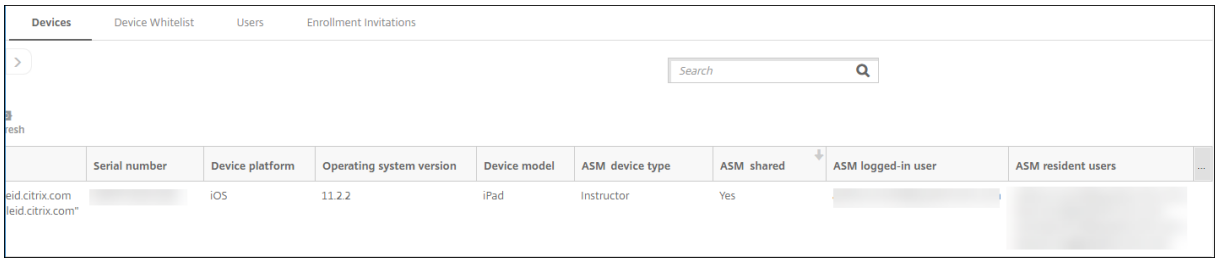


Ergebnisse von Sicherheitsaktionen werden auf den Seiten **Verwalten > Geräte > Allgemein** und **Verwalten > Geräte > Bereitstellungsgruppen** angezeigt.

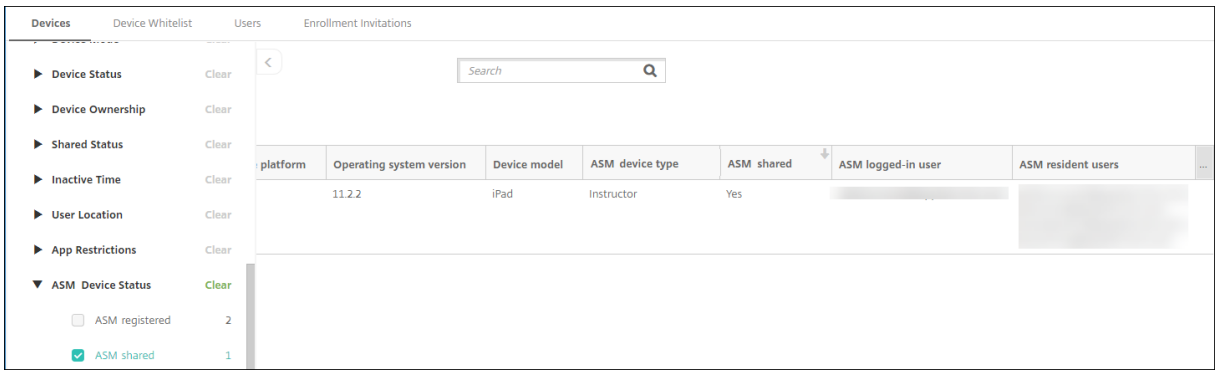
Aufrufen von Informationen über geteilte iPads

Informationen über geteilte iPads finden Sie auf der Seite **Verwalten > Geräte**.

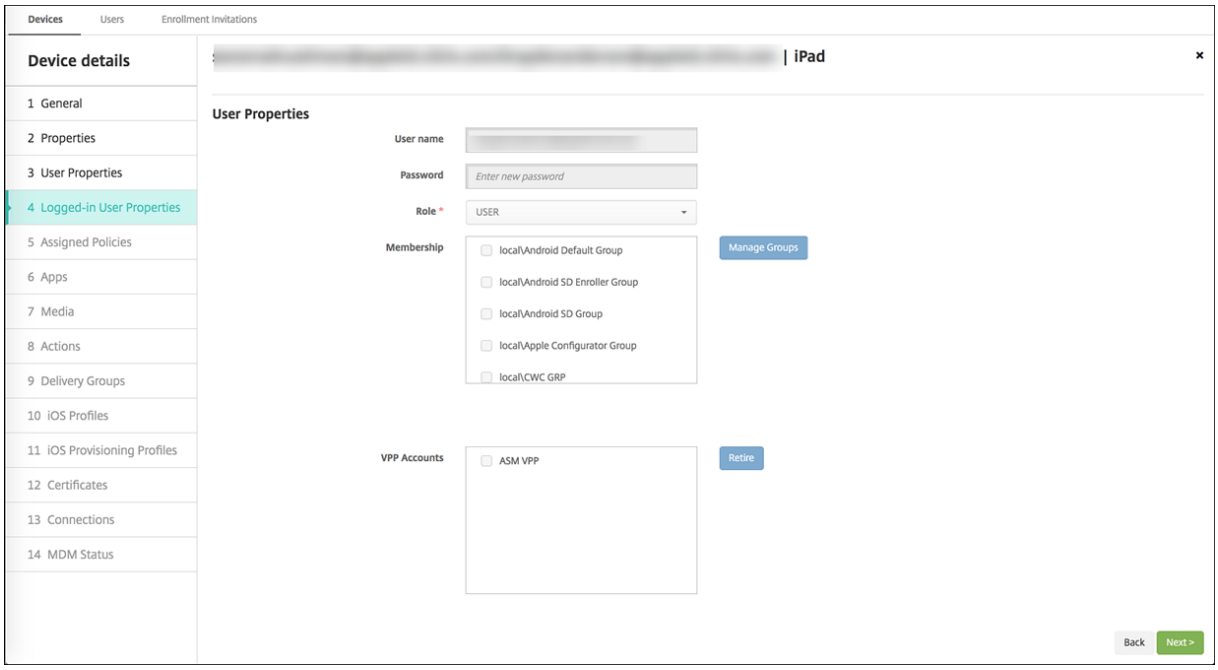
- Es stehen folgende Informationen zur Verfügung:
  - Ob ein Gerät geteilt wird (**ASM/ABM-Freigabe**)
  - Wer bei dem geteilten Gerät angemeldet ist (**Angemeldeter ASM/ABM-Benutzer**)
  - Alle Benutzer, die dem geteilten Gerät zugewiesen sind (**Residente ASM/ABM-Benutzer**)

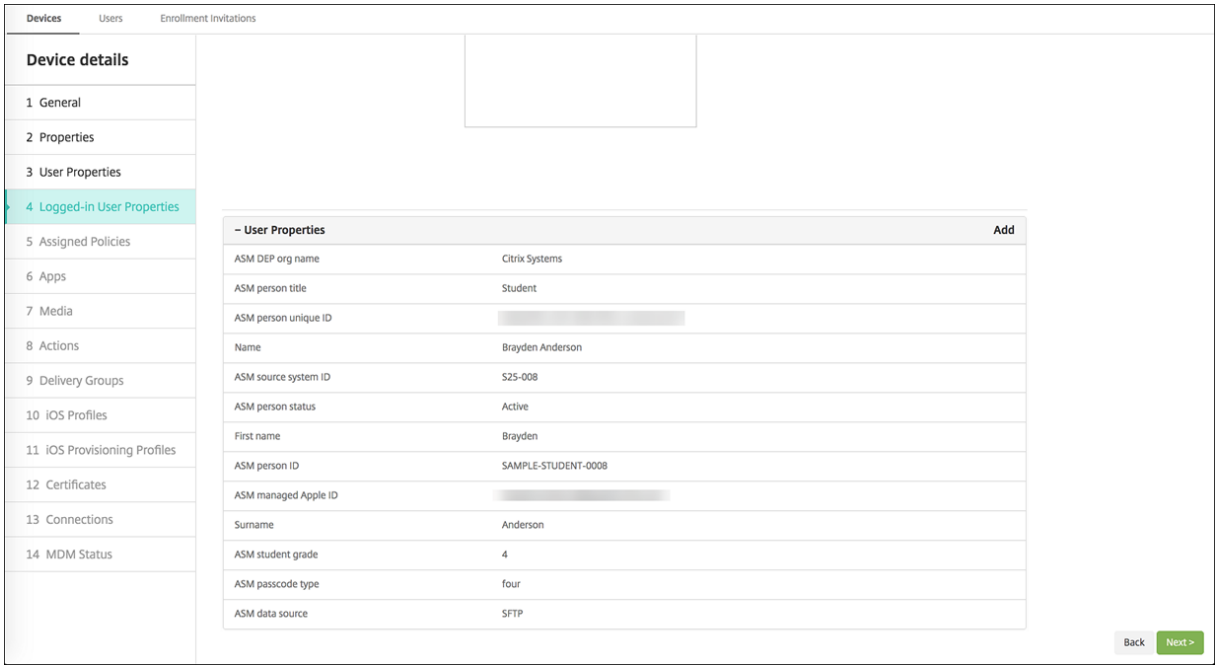


- Sie können die Geräteliste nach ihrem **ASM/ABM-Gerätestatus** filtern:

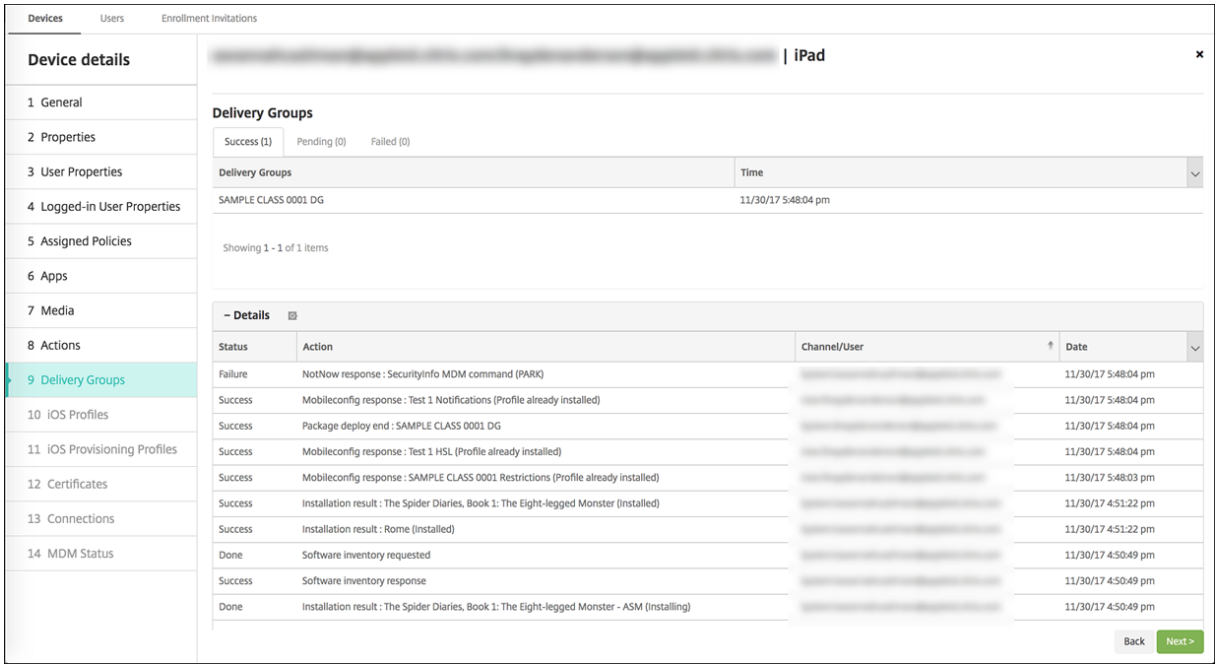


- Sie können Details zu dem bei einem geteilten iPad angemeldeten Benutzer auf der Seite **Verwalten > Geräte > Angemeldeter Benutzer - Eigenschaften** anzeigen.



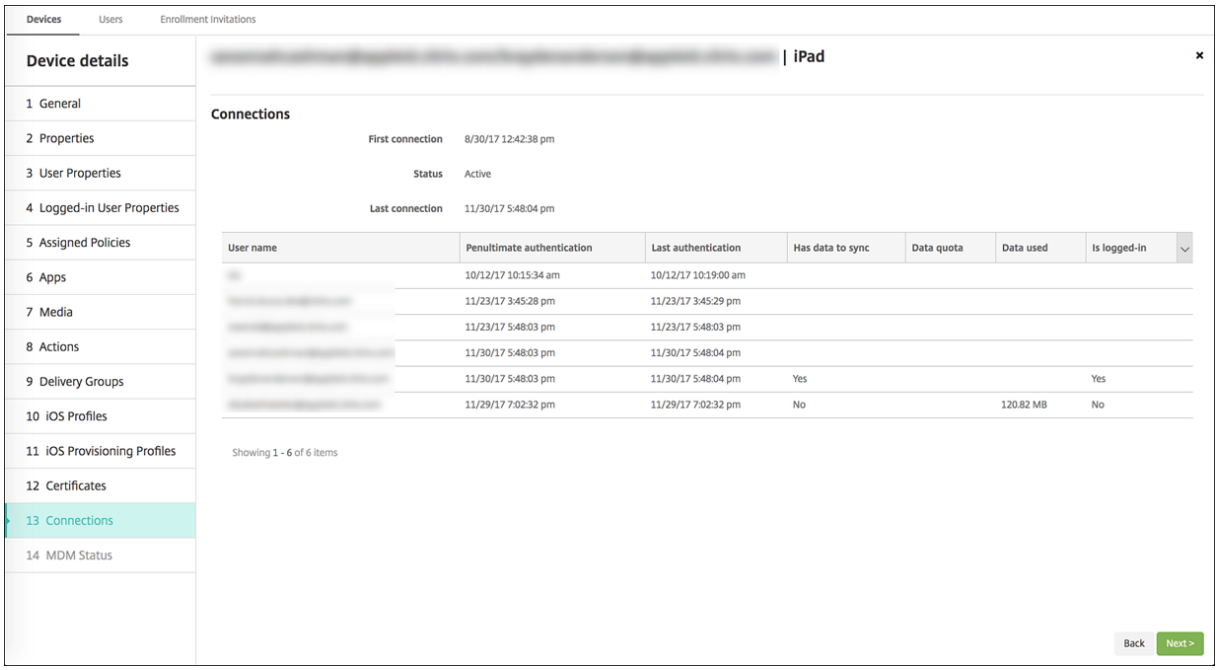


- Informationen zu dem für die Bereitstellung von Ressourcen für Gerätebesitzer und Benutzer in einer Bereitstellungsgruppe verwendeten Kanal finden Sie auf der Seite **Verwalten > Geräte > Bereitstellungsgruppen**. In der Spalte **Kanal/Benutzer** werden der Typ (**System** oder **Benutzer**) und der Empfänger angezeigt.

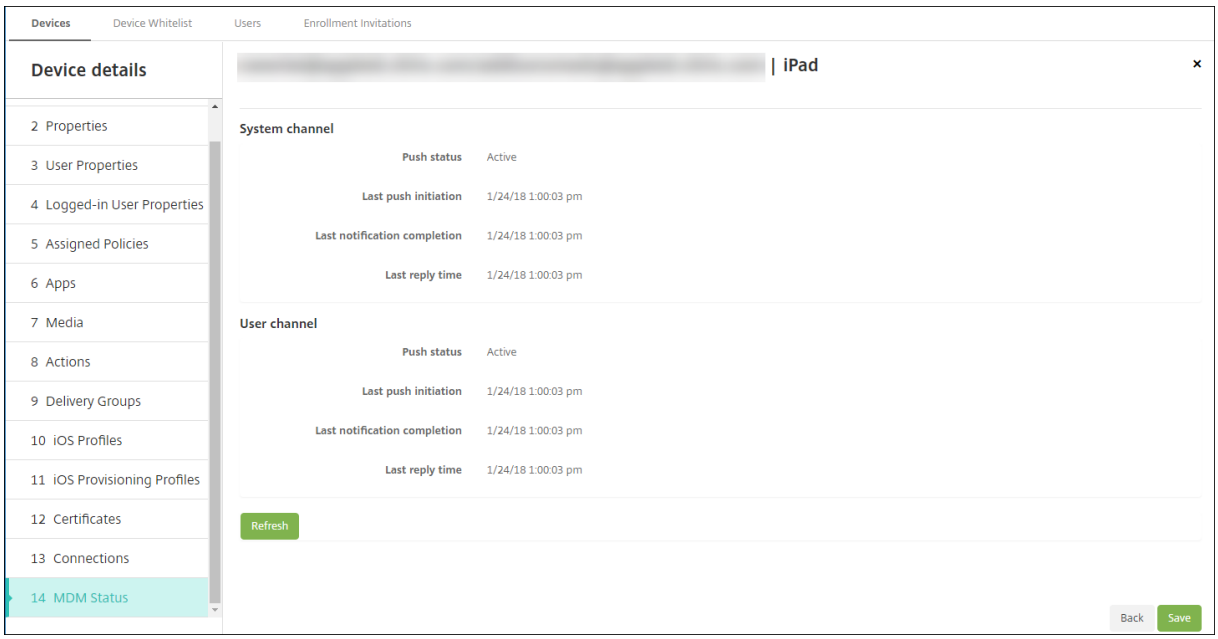


- Es stehen folgende Informationen zu residenten Benutzern zur Verfügung:
  - **Zu synchronisierende Daten vorhanden:** Gibt an, ob Daten des Benutzers zur Synchronisierung mit der Cloud vorhanden sind.

- **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.



Apple-Apps verteilen

June 25, 2024

Citrix Endpoint Management verwaltet die auf Geräten bereitgestellten Apps. 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 Apps hinzufügen.

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 Apps hinzufügen. 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 Citrix Endpoint Management:** 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 Citrix Endpoint Management:** 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 Citrix Endpoint Management:** 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 Citrix Endpoint Management:** Gehen Sie zu **Konfigurieren > Apps**, konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In Citrix Endpoint Management:** 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 Citrix Endpoint Management:** 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 Citrix Endpoint Management:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.
MDX-Apps	Nicht zutreffend	**In Citrix Endpoint Management:** 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 Citrix Endpoint Management:** 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
Über Apple Volume Purchase verteilte MDX-Apps	Registrieren Sie sich in einem Apple-Bereitstellungsprogramm **In Citrix Endpoint Management:** 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 Citrix Endpoint Management:** Gehen Sie zu **Konfigurieren > Apps**, konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In Citrix Endpoint Management:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.
Benutzerdefinierte Apps	Registrieren Sie sich in einem Apple-Bereitstellungsprogramm **In Citrix Endpoint Management:** 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 Citrix Endpoint Management:** Gehen Sie zu **Konfigurieren > Apps**, konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In Citrix Endpoint Management:** 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-Bereitstellungsprogramm. **In Citrix Endpoint Management:** 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 Citrix Endpoint Management:** Gehen Sie zu **Konfigurieren > Apps** und laden Sie die MDX-Datei hoch. Konfigurieren Sie die Apps und weisen Sie sie Bereitstellungsgruppen zu.	**In Citrix Endpoint Management:** Konfigurieren Sie Apps und stellen Sie sie mit Bereitstellungsgruppen bereit.

Apps aus öffentlichem App-Store

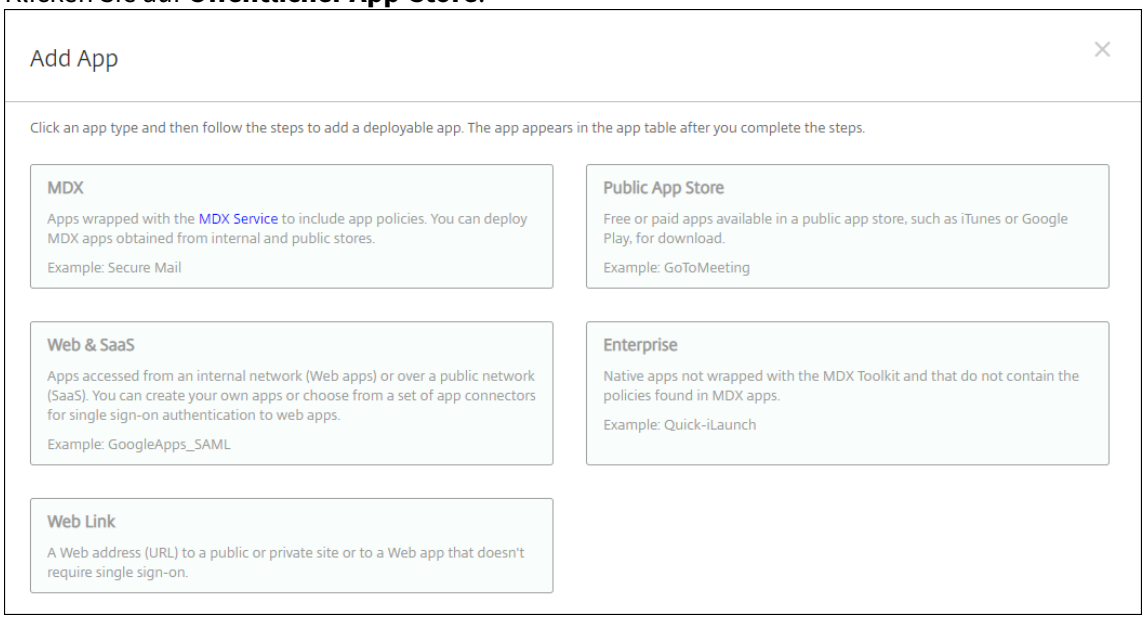
Sie können kostenlose und kostenpflichtige Apps aus dem App-Store zu Citrix Endpoint Management hinzufügen.

Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Nein
Verfügbar auf	iOS/iPadOS

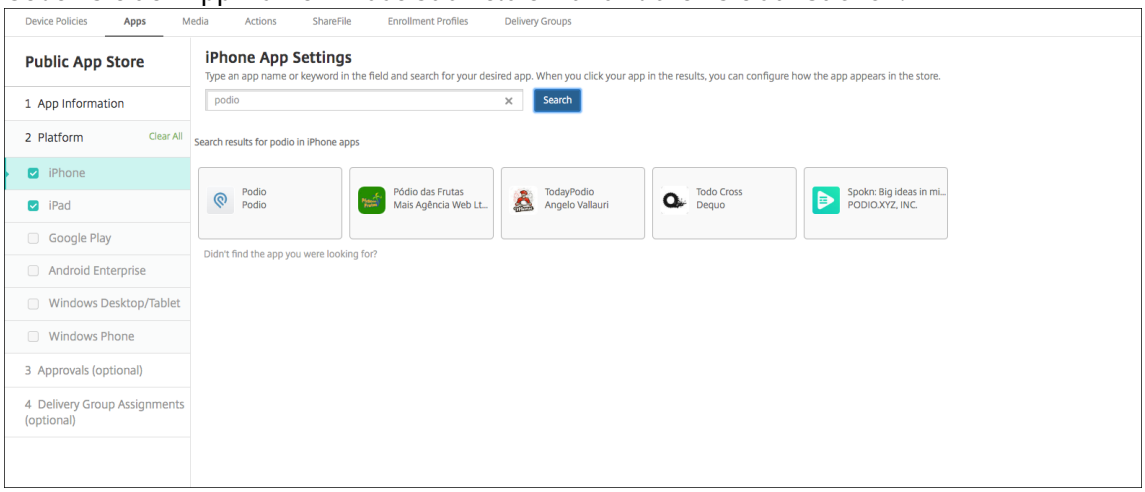
Schritt 1: Hinzufügen und Konfigurieren von Apps

1. Navigieren Sie in der Citrix Endpoint Management-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**.

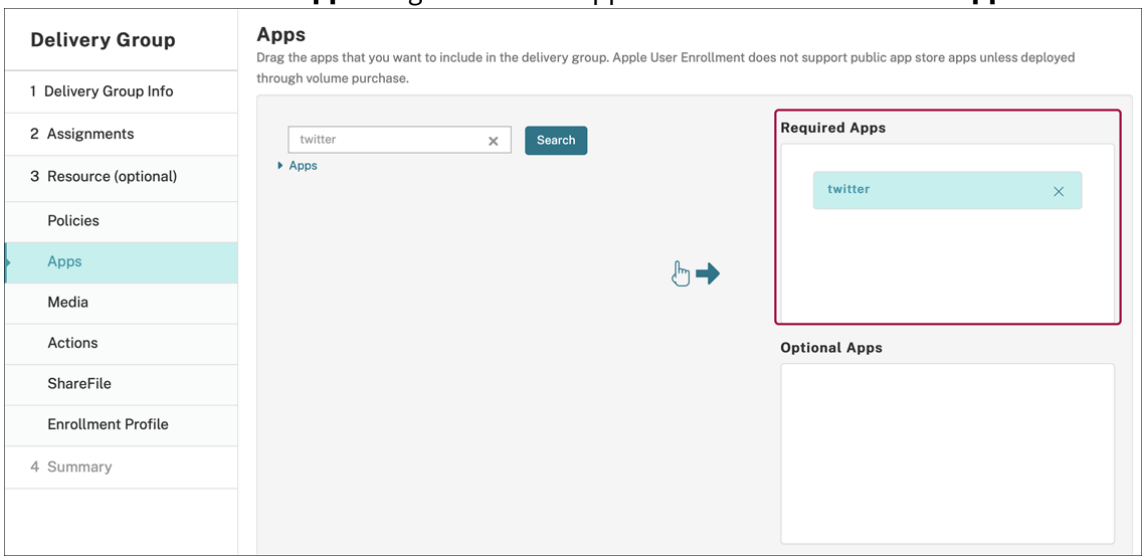


5. Es werden die Apps angezeigt, die den Suchkriterien entsprechen. Klicken Sie auf die gewünschte App.
6. Weisen Sie der App eine Bereitstellungsgruppe zu und klicken Sie auf **Speichern**.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der Citrix Endpoint Management-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** und klicken Sie auf **Hinzufügen**.

6. Ziehen Sie im Abschnitt **Apps** die gewünschten Apps in das Feld **Erforderliche Apps**.



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 Citrix Endpoint Management 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 Citrix Endpoint Management. 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. Wenn für eine App die Einstellung **Verwaltung der App erzwingen** aktiviert ist, wird sie ohne Aufforderung des Benutzers aktualisiert. Das Update erfolgt unabhängig davon, ob die App erforderlich oder optional ist.

   Um die Einstellungen **Verwaltung der App erzwingen** und **Automatische App-Updates** zu verwenden, aktivieren Sie die Servereigenschaft `apple.app.force.managed`. Siehe Servereigenschaften.

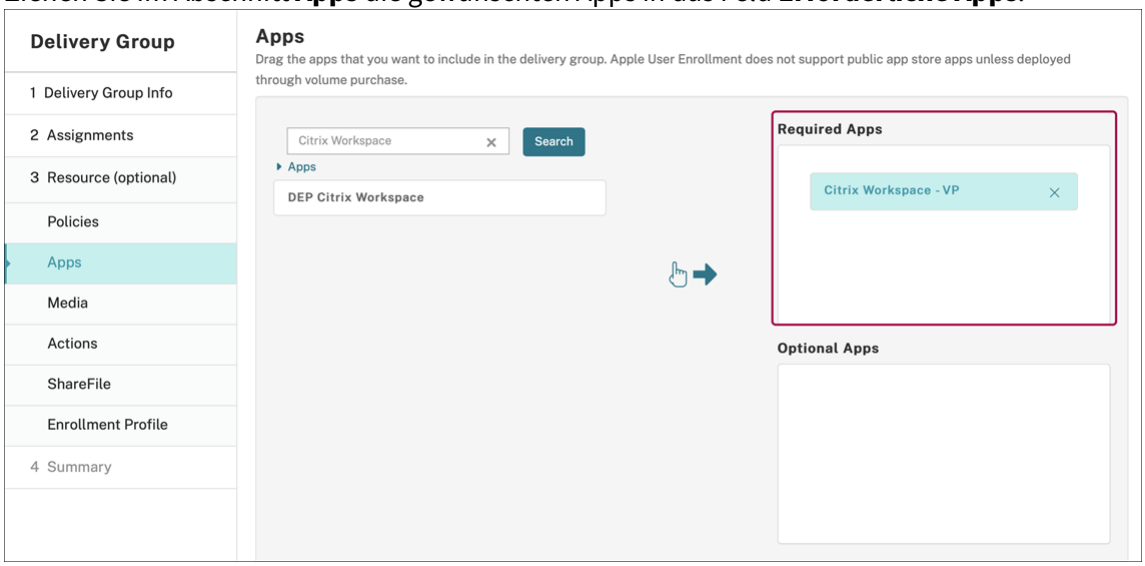
Schritt 2: Abrufen von Apps und Lizenzen von Apple

Erwerben Sie Apps in Ihrem ABM/ASM-Konto. Sie können Apps in Apple Books (nur für iOS/iPadOS) oder im Apple App Store erwerben. Denken Sie daran, dass Sie alle Apps kaufen müssen, auch wenn diese kostenlos sind. Sobald Sie Lizenzen in ABM/ASM erworben haben, zeigt Citrix Endpoint Management die App automatisch an.

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 Citrix Endpoint Management-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** und klicken Sie auf **Hinzufügen**.
7. Ziehen Sie im Abschnitt **Apps** die gewünschten Apps in das Feld **Erforderliche Apps**.



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.

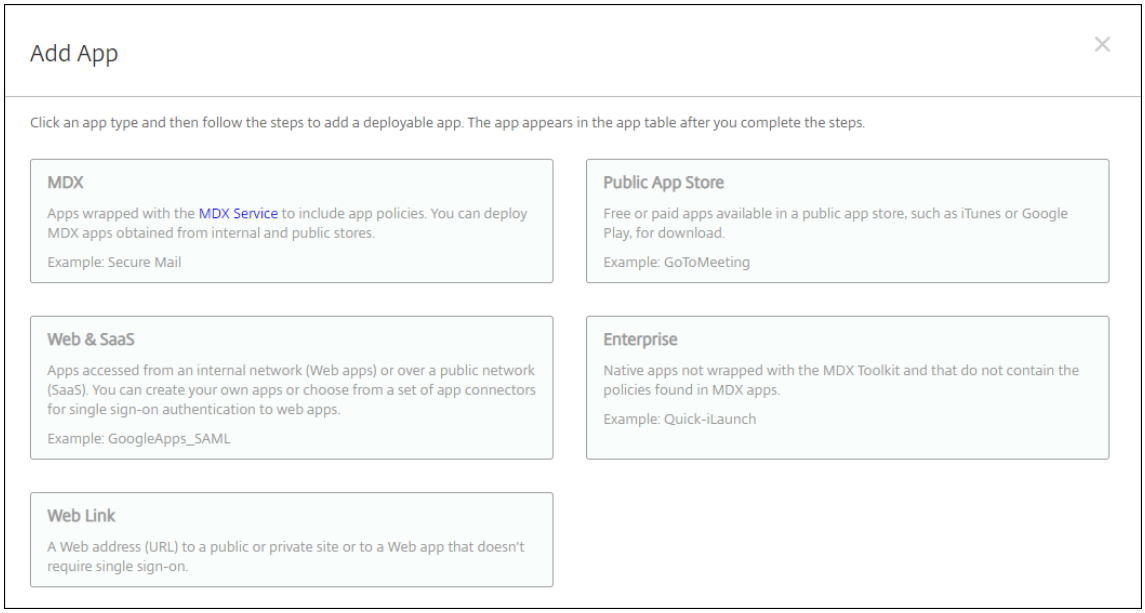
Unternehmensapps

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
Betriebssystem	iOS/iPadOS/macOS

Schritt 1: Hinzufügen und Konfigurieren von Apps

1. Navigieren Sie in der Citrix Endpoint Management-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.

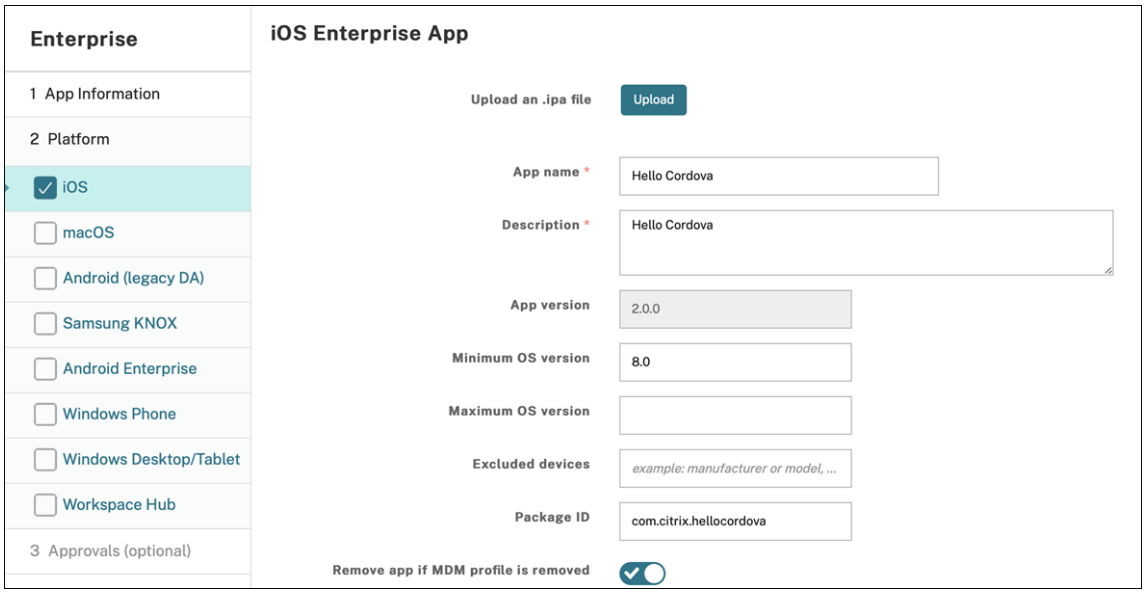
4. Klicken Sie auf **Weiter**. Die Seite **Plattform** wird angezeigt.
5. Wählen Sie als Plattform **iPhone**, **iPad** oder **macOS**.
6. Hochladen der IPA-Datei (iOS/iPadOS) bzw. der PKG-Datei (macOS)
7. Klicken Sie auf **Weiter**. Die Seite mit den **App-Details** wird angezeigt.
8. Konfigurieren 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**, wenn Benutzer nicht betreuter Geräte aufgefordert werden sollen, die Verwaltung der App zuzulassen. Wenn sie akzeptieren, wird die App verwaltet. Wenn für eine App die Einstellung **Verwaltung der App erzwingen** aktiviert ist, wird sie ohne Aufforderung des Benutzers aktualisiert. Das Update erfolgt unabhängig davon, ob die App erforderlich oder optional ist. (nur iOS/iPadOS)

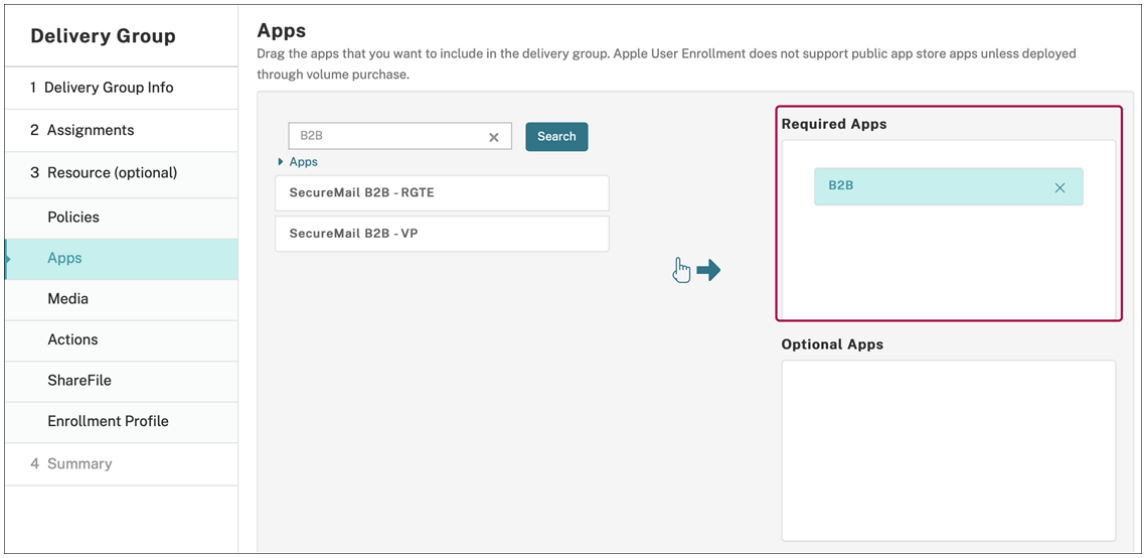
Um die Einstellungen **Verwaltung der App erzwingen** und **Automatische App-Updates** zu verwenden, aktivieren Sie die Servereigenschaft `apple.app.force.managed`. Siehe Servereigenschaften.



9. Weisen Sie der App eine Bereitstellungsgruppe zu und klicken Sie auf **Speichern**.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Bereitstellungsgruppen**. Wählen Sie die zu konfigurierende Bereitstellungsgruppe aus und klicken Sie auf die Seite **Apps**.
2. Ziehen Sie die gewünschten Apps in das Feld **Erforderliche Apps**.



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

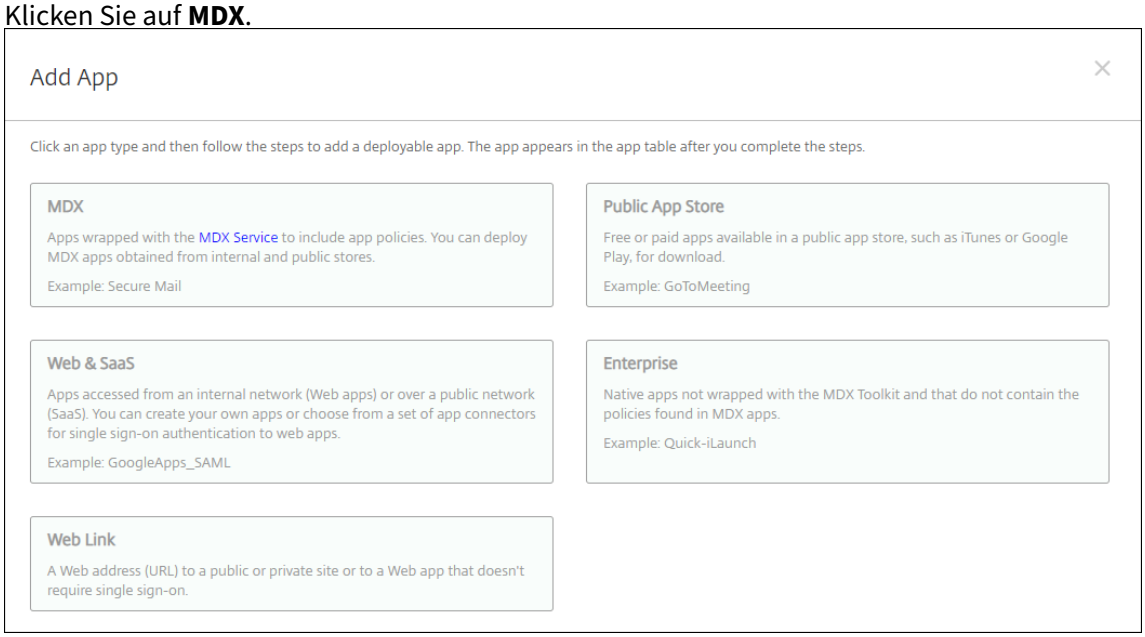
Um MDX-bezogene Richtlinien und Sicherheitsfunktionen zu verwenden, fügen Sie MAM-SDK-fähige Apps oder Apps, die mit MDX umschlossen wurden, hinzu. Sie können MDX-Apps mit oder ohne Volume Purchase bereitstellen.

Verfügbarkeit des Features	
Gerätebetreuung erforderlich	Nein
Benutzerregistrierung möglich	Ja
Verfügbar unter	iOS/iPadOS

Um die MDX-Version einer App aus dem öffentlichen App-Store hinzuzufügen, führen Sie zunächst die Schritte unter Apps aus öffentlichem App-Store und dann die Schritte in diesem Abschnitt aus.

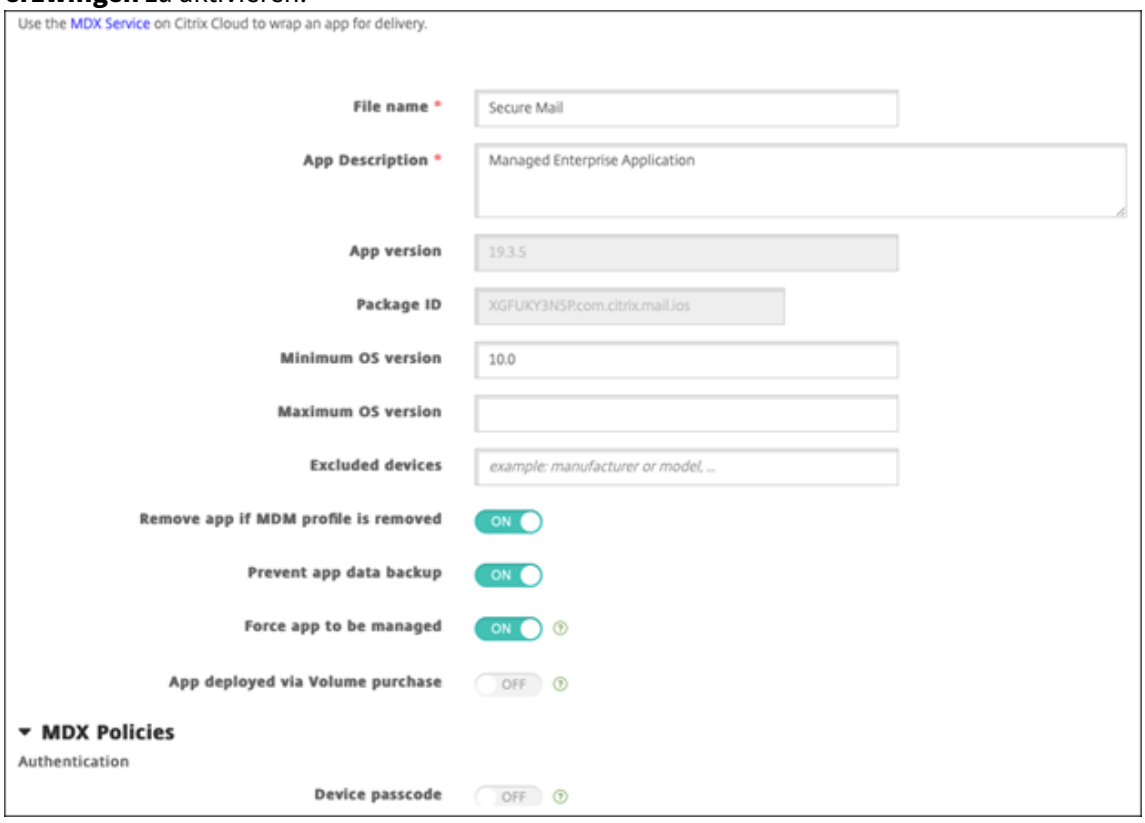
Schritt 1: Hinzufügen und Konfigurieren von Apps

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **MDX**.

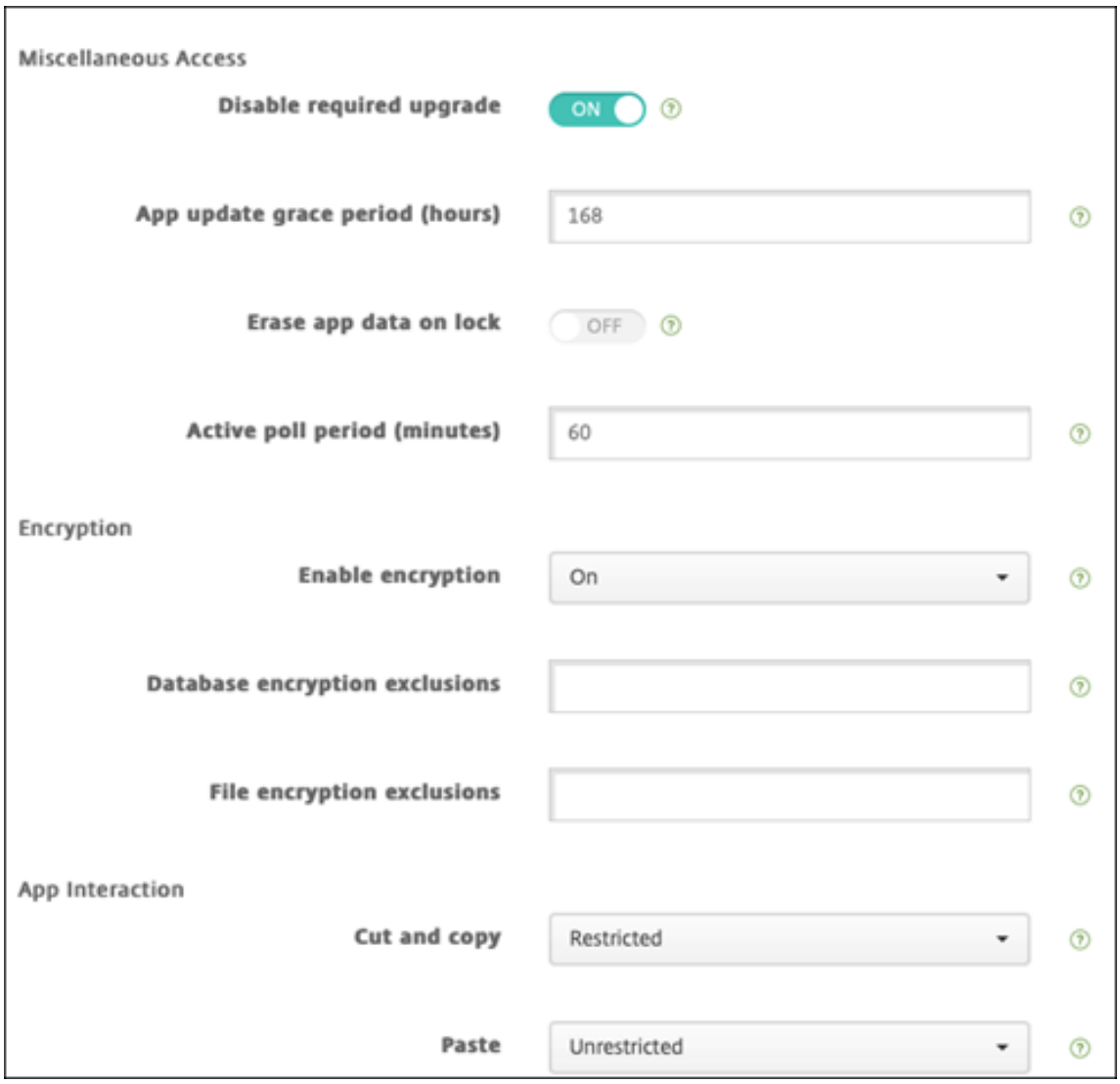


3. Wählen Sie als Plattform **iPhone** oder **iPad**.
4. Laden Sie die MDX-Datei hoch.
5. Konfigurieren Sie die App-Details. Wählen Sie für **App wird per Volume Purchase bereitgestellt** die Einstellung **Aus**. Citrix empfiehlt außerdem, das Feature **Verwaltung der App**

erzwingen zu aktivieren.



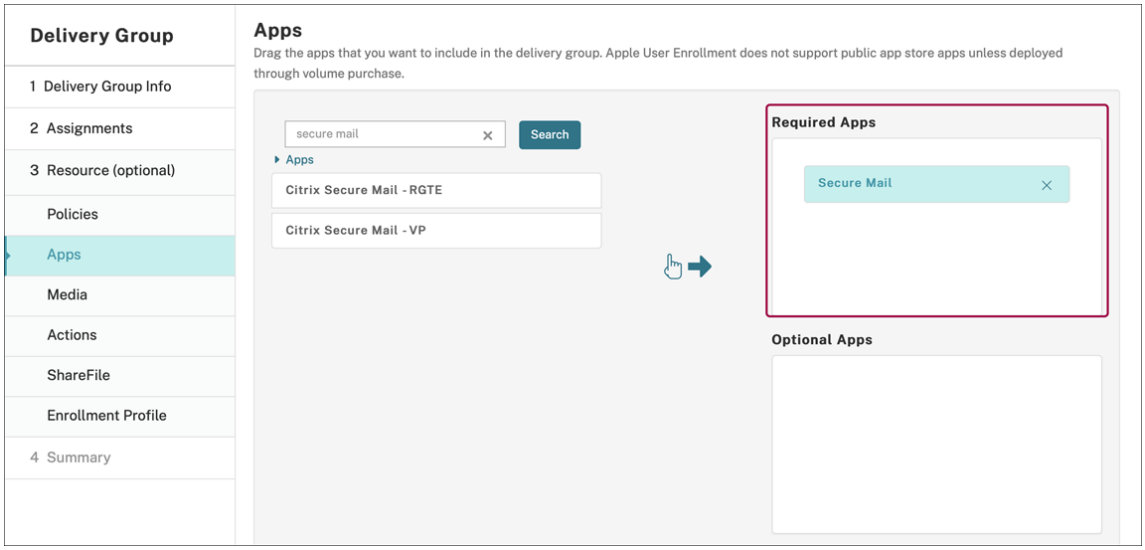
6. Konfigurieren Sie die MDX-Richtlinien. Wählen Sie für **Erforderliches Upgrade deaktivieren** die Einstellung **Ein**.



7. Weisen Sie der App eine Bereitstellungsgruppe zu und klicken Sie auf **Speichern**.

Schritt 2: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Bereitstellungsgruppen** und klicken Sie auf **Hinzufügen**.
2. Ziehen Sie im Abschnitt **Apps** die gewünschten Apps in das Feld **Erforderliche Apps**.



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.

Über Apple Volume Purchase verteilte MDX-Apps

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 Citrix Endpoint Management. 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. Wenn für eine App die Einstellung **Verwaltung der App erzwingen** aktiviert ist, wird sie ohne Aufforderung des Benutzers aktualisiert. Das Update erfolgt unabhängig davon, ob die App erforderlich oder optional ist.

   Um die Einstellungen **Verwaltung der App erzwingen** und **Automatische App-Updates** zu verwenden, aktivieren Sie die Servereigenschaft `apple.app.force.managed`. Siehe Servereigenschaften.

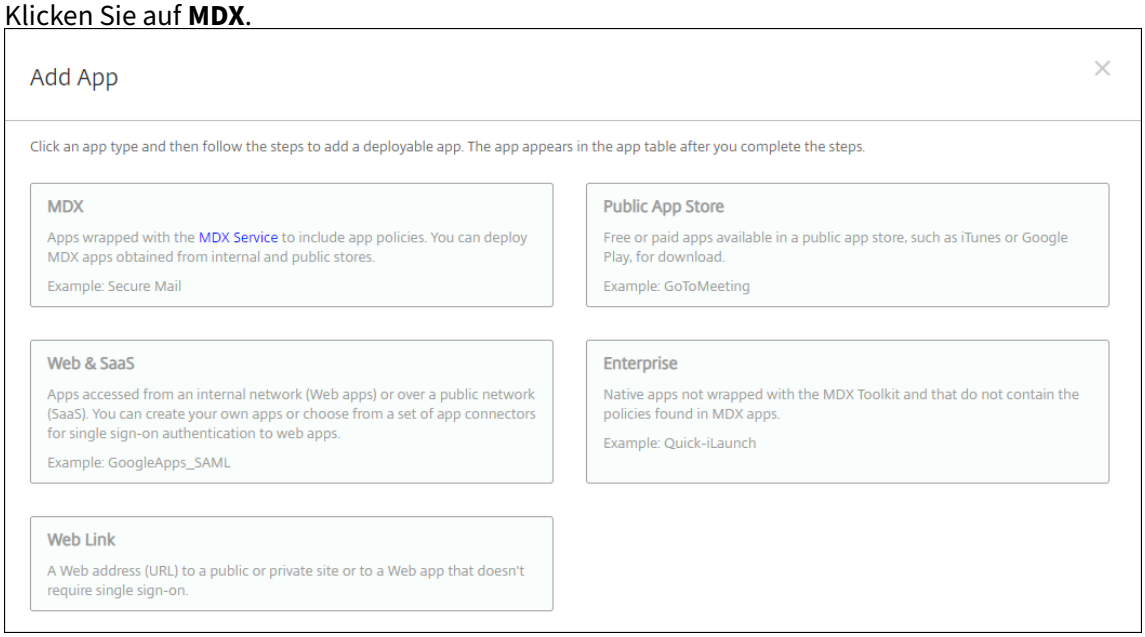
Schritt 2: Abrufen von Apps und Lizenzen von Apple

Erwerben Sie Apps in Ihrem ABM/ASM-Konto. Sie können Apps in Apple Books (nur für iOS/iPadOS) oder im Apple App Store erwerben. Denken Sie daran, dass Sie alle Apps kaufen müssen, auch wenn diese kostenlos sind. Sobald Sie Lizenzen in ABM/ASM erworben haben, zeigt Citrix Endpoint Management die App automatisch an.

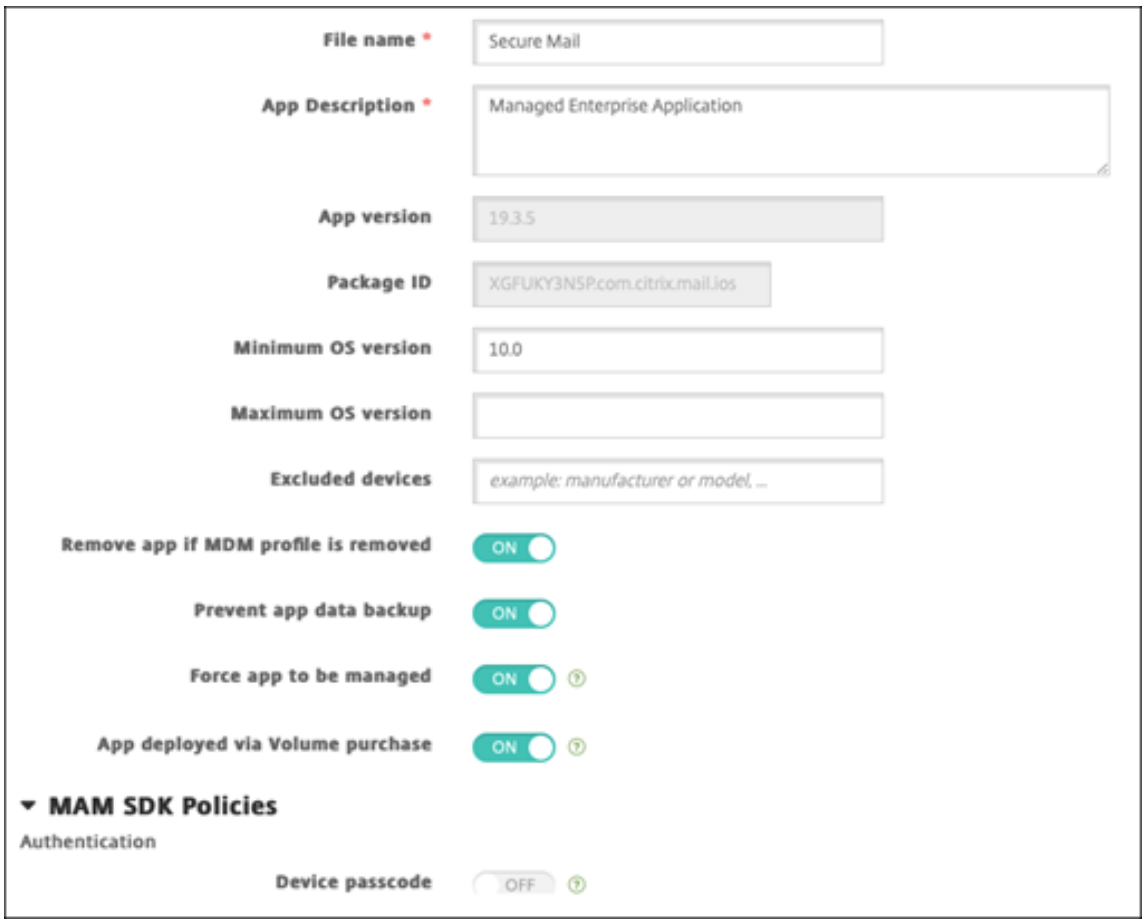
Informationen dazu, wie Sie Apps in Ihrem Unternehmen zur Verfügung stellen, finden Sie in der Dokumentation von Apple.

Schritt 3: Hinzufügen und Konfigurieren von Apps

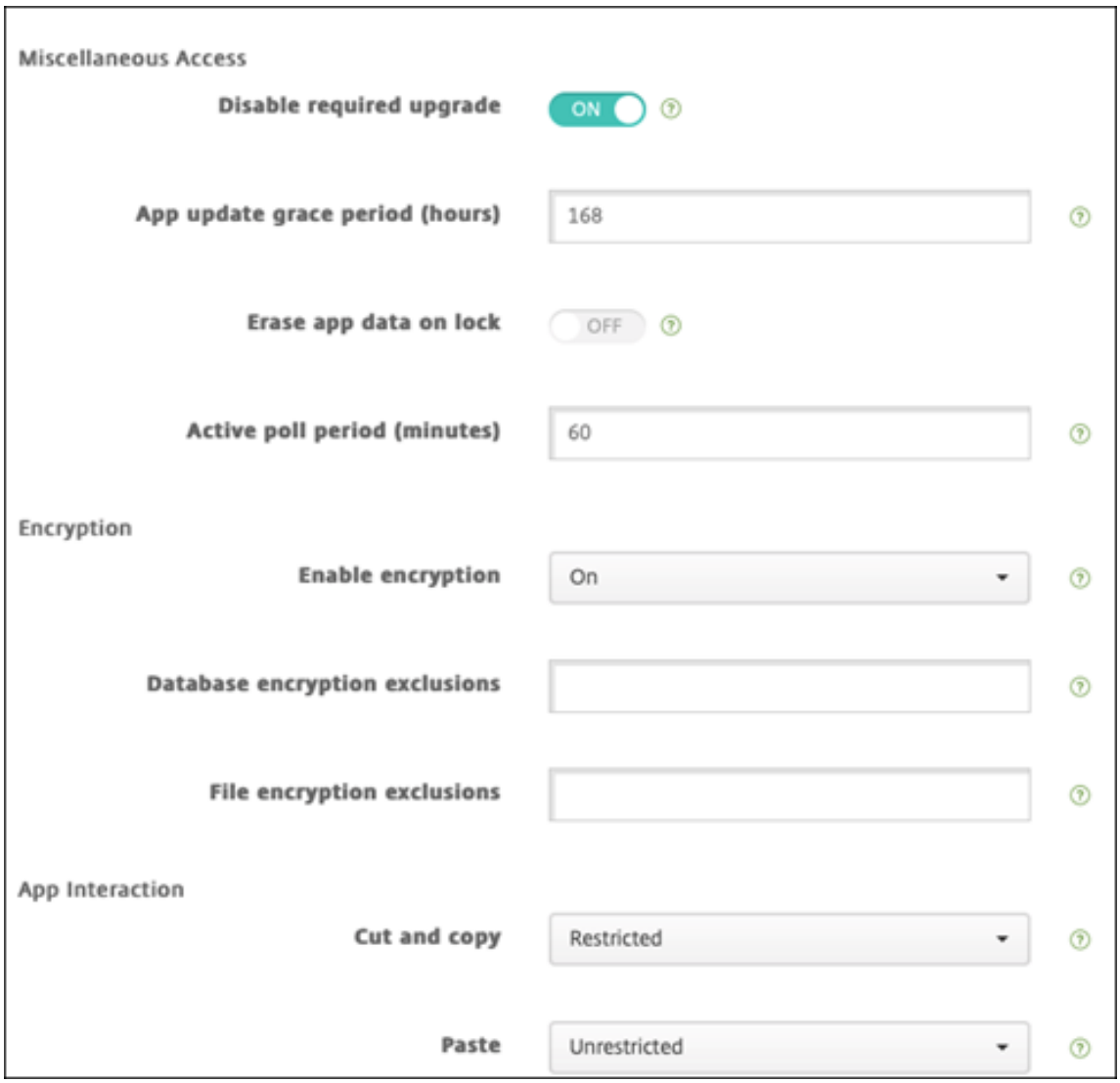
1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **MDX**.



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**.

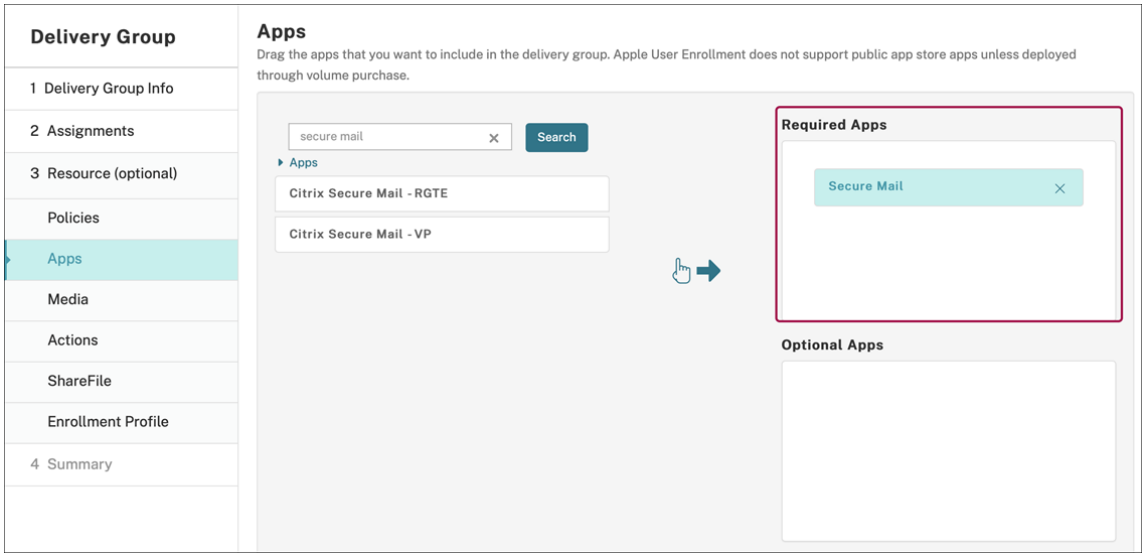


7. Weisen Sie der App eine Bereitstellungsgruppe für jede Plattform zu und klicken Sie auf **Speichern**.

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 4: Konfigurieren der App-Bereitstellung

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Bereitstellungsgruppen** und klicken Sie auf **Hinzufügen**.
2. Ziehen Sie im Abschnitt **Apps** die gewünschten MDX-Apps in das Feld **Erforderliche Apps**.



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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management.

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 Citrix Endpoint Management. 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. Wenn für eine App die Einstellung **Verwaltung der App erzwingen** aktiviert ist, wird sie ohne Aufforderung des Benutzers aktualisiert. Das Update erfolgt unabhängig davon, ob die App erforderlich oder optional ist.

Um die Einstellungen **Verwaltung der App erzwingen** und **Automatische App-Updates** zu verwenden, aktivieren Sie die Servereigenschaft `apple.app.force.managed`. Siehe Servereigenschaften.

Schritt 2: Konfigurieren von Apps in ABM

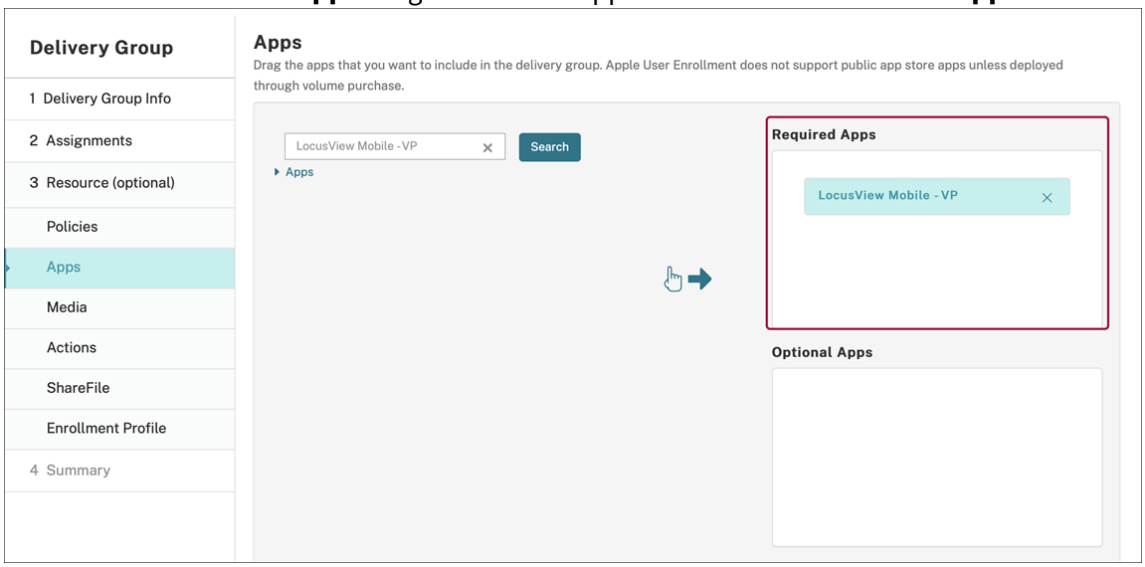
Fügen Sie Apps in Ihrem ABM-Konto hinzu. Sie können eigene benutzerdefinierte Apps hochladen und verteilen oder Lizenzen für benutzerdefinierte Apps anderer Organisationen erwerben. Weitere Informationen zum Hinzufügen und Aktivieren benutzerdefinierter Apps in ABM finden Sie in der Dokumentation von Apple.

Schritt 3: Hinzufügen und Konfigurieren von Apps in Citrix Endpoint Management

1. Navigieren Sie in der Citrix Endpoint Management-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 **Bearbeiten**.
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 Citrix Endpoint Management-Konsole zu **Konfigurieren > Bereitstellungsgruppen** und klicken Sie auf **Hinzufügen**.
2. Ziehen Sie im Abschnitt **Apps** die gewünschten Apps in das Feld **Erforderliche Apps**.



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 Citrix Endpoint Management.

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 Citrix Endpoint Management. 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. Wenn für eine App die Einstellung **Verwaltung der App erzwingen** aktiviert ist, wird sie ohne Aufforderung des Benutzers aktualisiert. Das Update erfolgt unabhängig davon, ob die App erforderlich oder optional ist.

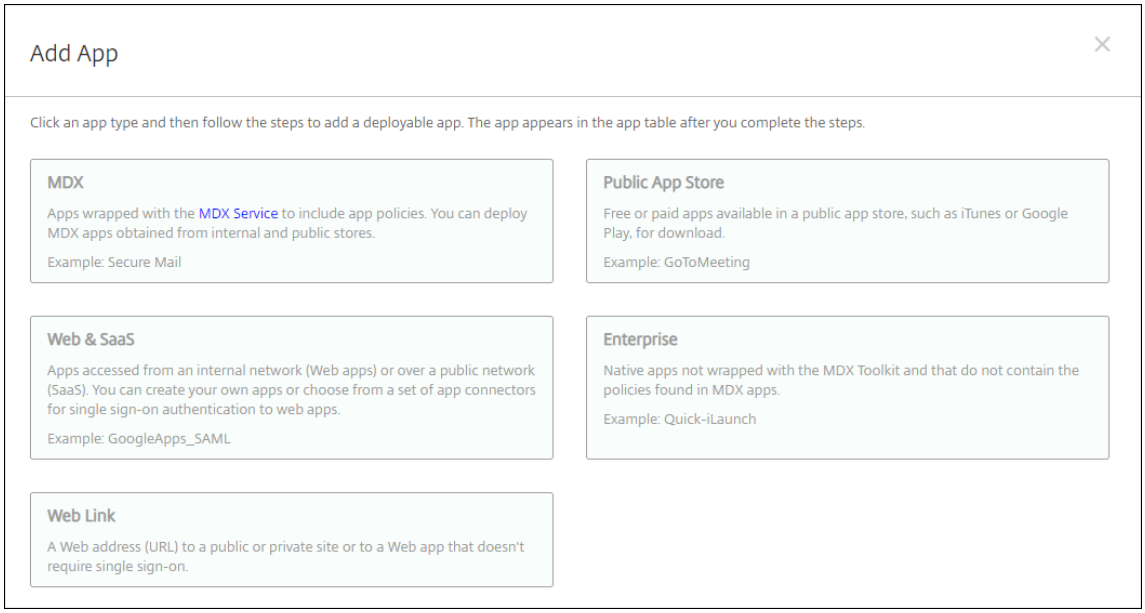
   Um die Einstellungen **Verwaltung der App erzwingen** und **Automatische App-Updates** zu verwenden, aktivieren Sie die Servereigenschaft `apple.app.force.managed`. Siehe Servereigenschaften.

Schritt 2: Konfigurieren von Apps in ABM

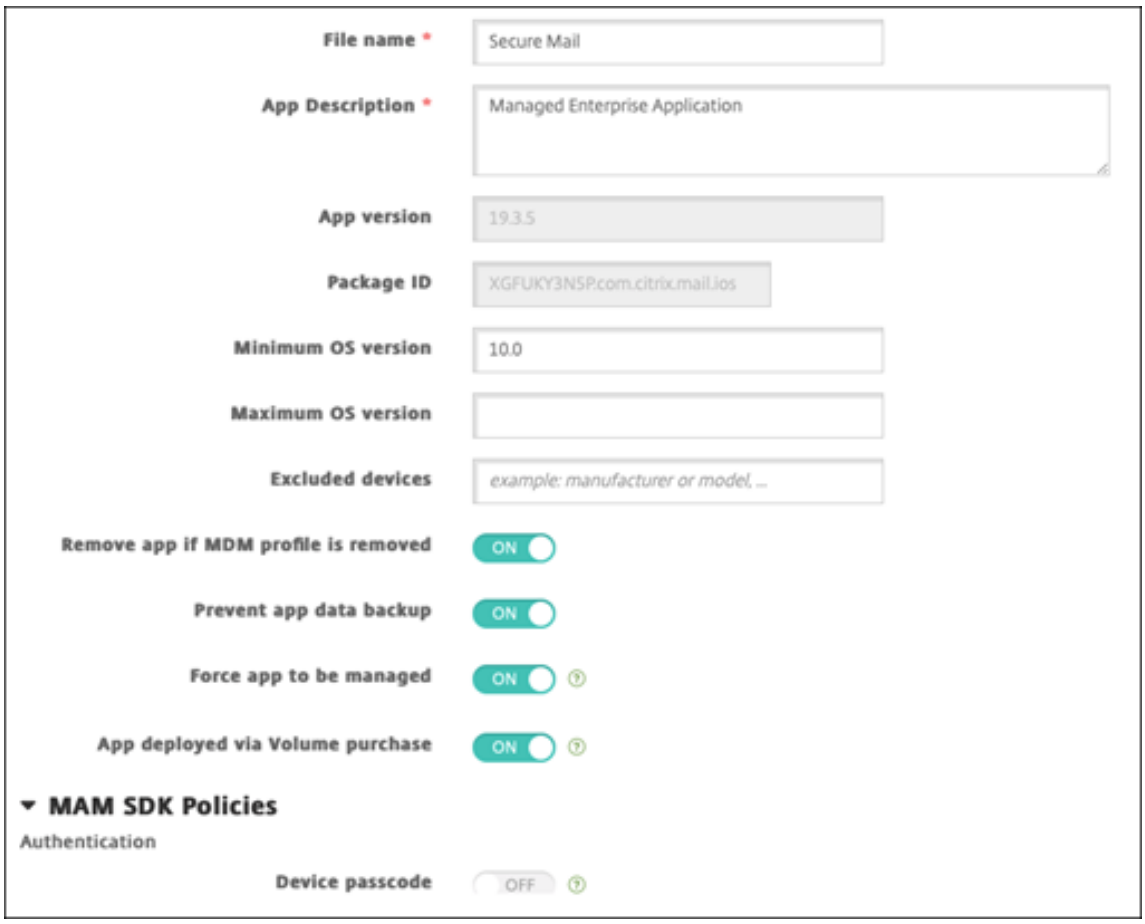
Fügen Sie Apps in Ihrem ABM-Konto hinzu. Sie können eigene benutzerdefinierte Apps hochladen und verteilen oder Lizenzen für benutzerdefinierte Apps anderer Organisationen erwerben. Weitere Informationen zum Hinzufügen und Aktivieren benutzerdefinierter Apps in ABM finden Sie in der Dokumentation von Apple.

Schritt 3: Hinzufügen und Konfigurieren von Apps in Citrix Endpoint Management

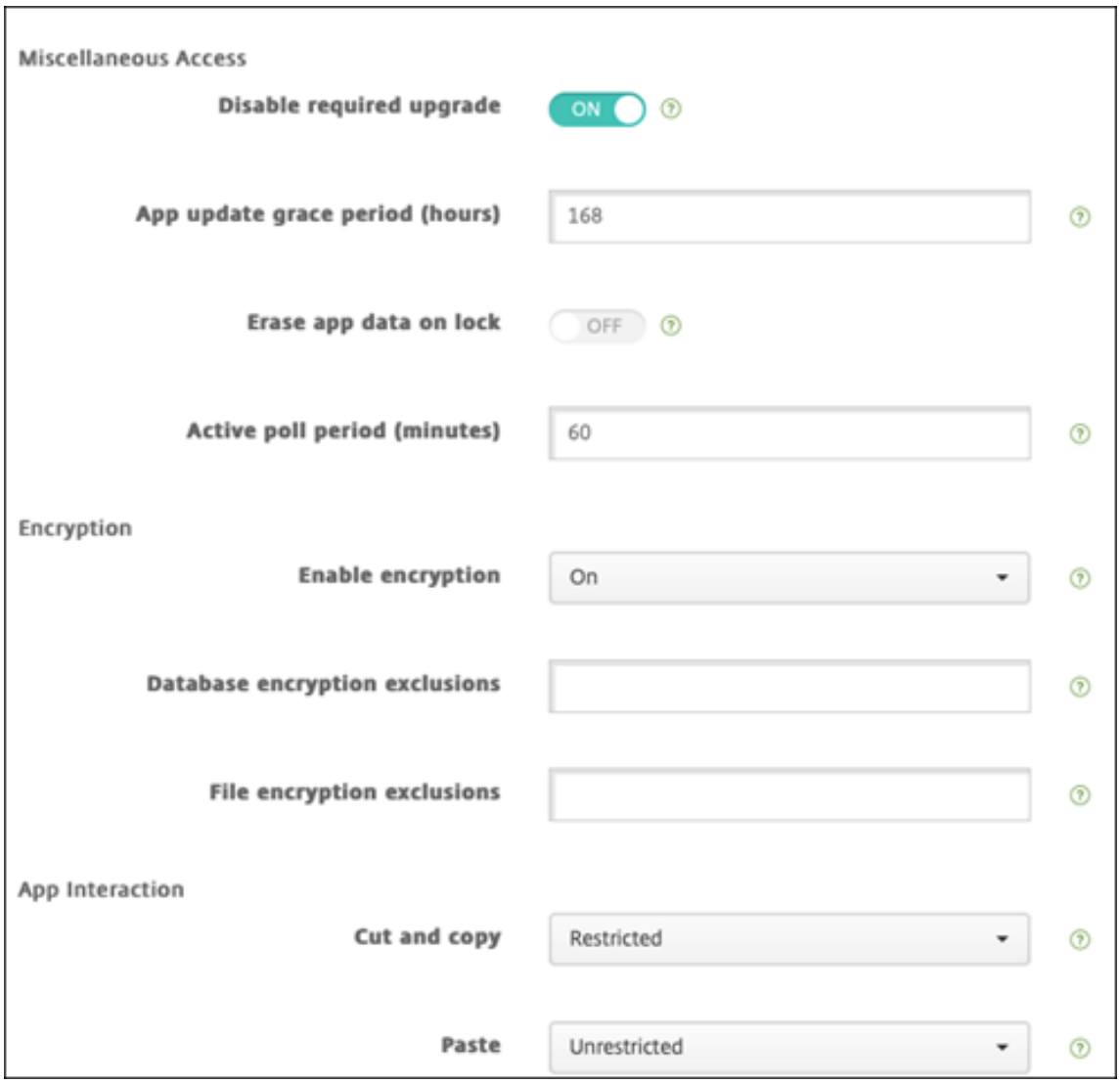
1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Apps**. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf **MDX**.



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**.

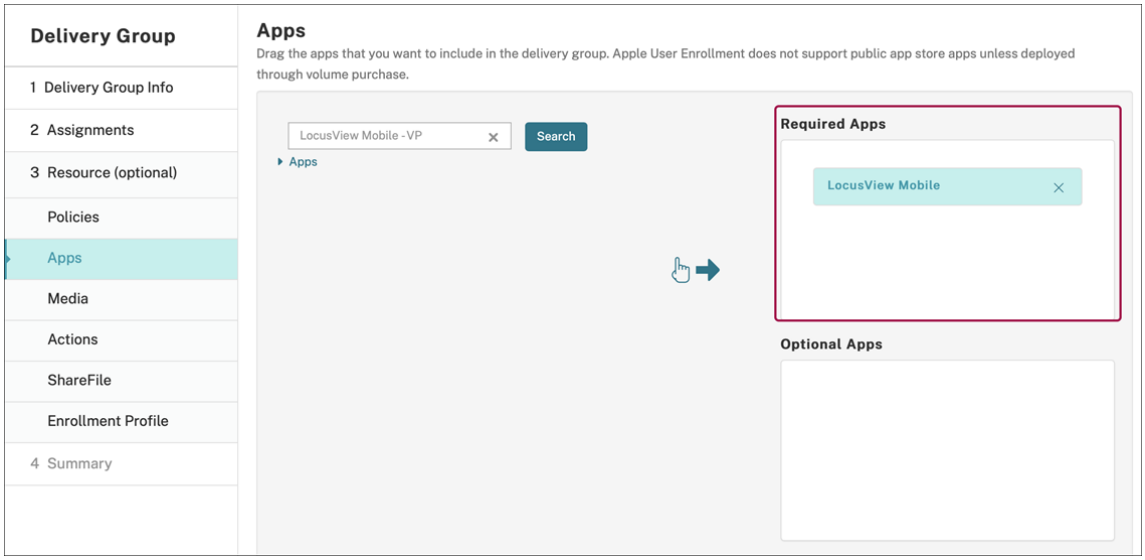


7. Weisen Sie der App eine Bereitstellungsgruppe zu und klicken Sie auf **Speichern**.

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 Citrix Endpoint Management-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 **Bearbeiten**.
3. Wählen Sie die Bereitstellungsgruppen aus, an die die App auf jeder Plattform verteilt werden soll. Klicken Sie auf **Speichern**.
4. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen** und klicken Sie auf **Hinzufügen**.
5. Ziehen Sie im Abschnitt **Apps** die gewünschten MDX-Apps in das Feld **Erforderliche Apps**.



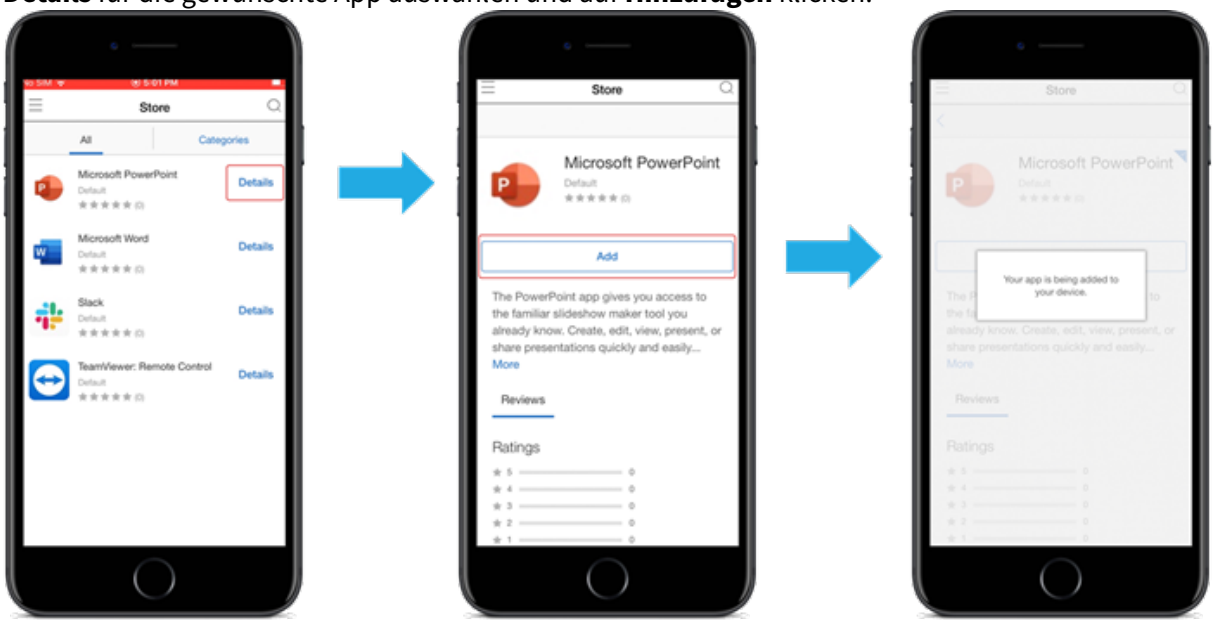
6. Gehen Sie zurück zu **Konfigurieren > Bereitstellungsgruppen**.
7. Wählen Sie die gewünschte Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellen**.
8. Benutzer erhalten eine Anforderung zum Bereitstellen von Apps. Apps werden im Hintergrund installiert, nachdem sie akzeptiert wurden.

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 Citrix Secure Hub starten.

Zu Installation optionaler Apps müssen Benutzer Citrix Secure Hub starten, den **Store** aufrufen, die **Details** für die gewünschte App auswählen und auf **Hinzufügen** klicken.



Netzwerkzugriffssteuerung (NAC)

June 25, 2024

Sie können mit Ihrer NAC-Lösung (Network Access Control) die Bewertung der Gerätesicherheit durch Citrix Endpoint Management für Android- und Apple-Geräte erweitern. Die NAC-Lösung vereinfacht und bewältigt anhand der Citrix Endpoint Management-Sicherheitsbewertung Authentifizierungsentscheidungen. Nach dem Konfigurieren des NAC-Geräts werden die in Citrix Endpoint Management konfigurierten Geräterichtlinien und NAC-Filter erzwungen.

Die Verwendung von Citrix Endpoint Management mit einer NAC-Lösung ermöglicht QoS und eine gezieltere Steuerung für Geräte innerhalb Ihres Netzwerks. Eine Zusammenfassung der Vorteile einer Integration von NAC mit Citrix Endpoint Management finden Sie unter Zugriffssteuerung.

Citrix unterstützt die folgenden Lösungen für die Integration mit Citrix Endpoint Management:

- NetScaler Gateway
- ForeScout

Citrix übernimmt keine Gewährleistung für die Integration anderer NAC-Lösungen.

Bei vorhandenem NAC-Gerät in Ihrem Netzwerk:

- Citrix Endpoint Management unterstützt NAC als Endpunktsicherheitsfeature für Geräte mit iOS, Android Enterprise und Android.
- Sie können Filter in Citrix Endpoint Management aktivieren, um Geräte anhand von Regeln oder Eigenschaften als (nicht) richtlinientreu für NAC festzulegen. Beispiel:
  - Wenn ein verwaltetes Gerät in Citrix Endpoint Management nicht die vorgegebenen Kriterien erfüllt, wird das Gerät in Citrix Endpoint Management als nicht richtlinientreu eingestuft. Ein NAC-Gerät blockiert dann nicht richtlinientreue Geräte in Ihrem Netzwerk.
  - Wenn auf einem verwalteten Gerät in Citrix Endpoint Management 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 NetScaler Gateway für NAC verwenden, können Sie durch Aktivieren von Split-Tunneling verhindern, dass das NetScaler Gateway Plug-In unnötigen Netzwerkverkehr an NetScaler Gateway sendet. Weitere Informationen zum Split-Tunneling finden Sie unter Konfigurieren von Split-Tunneling.

Unterstützte NAC-Richtlinientreuefilter

Citrix Endpoint Management unterstützt die folgenden NAC-Richtlinientreuefilter:

Anonyme Geräte: Prüft, ob ein Gerät im anonymen Modus ist. Diese Prüfung ist verfügbar, wenn Citrix Endpoint Management bei einer Wiederverbindung den Benutzer des Geräts nicht erneut authentifizieren kann.

Unzulässige Apps: Prüft, ob ein Gerät unzulässige Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind. Weitere 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 in der Regel von automatisierten Aktionen geändert oder von Drittanbietern, die Citrix Endpoint Management-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 von Citrix Endpoint Management verwaltet 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 Citrix Endpoint Management 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 Citrix Endpoint Management
3. Konfigurieren einer NAC-Lösung:

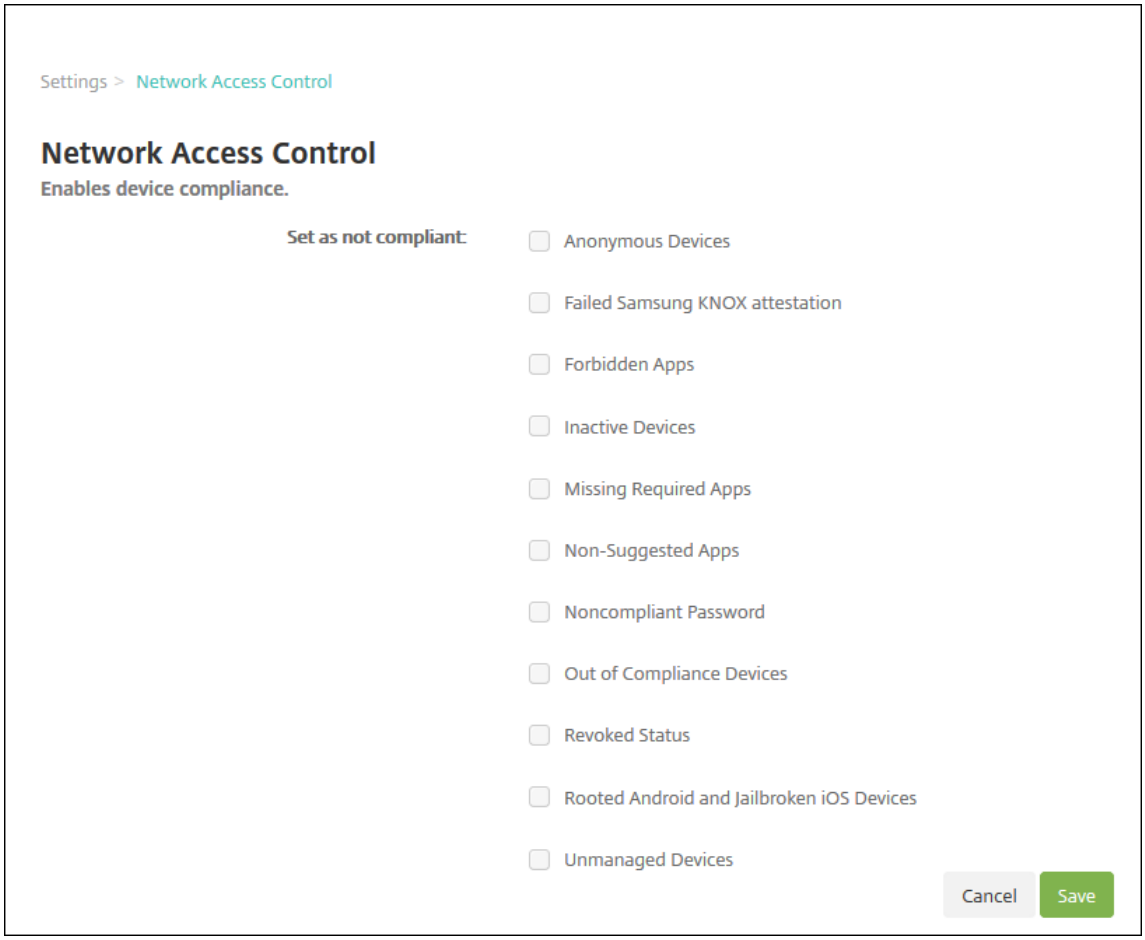
   - NetScaler Gateway, beschrieben unter Aktualisieren der NetScaler Gateway-Richtlinien zur Unterstützung von NAC

Erfordert Installation von Citrix SSO auf Geräten. Siehe NetScaler Gateway-Clients.

- ForeScout: Siehe ForeScout-Dokumentation.

Aktivieren von NAC-Filtern in Citrix Endpoint Management

1. Gehen Sie in der Citrix Endpoint Management-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 NetScaler 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 NetScaler Gateway mit einem der folgenden Merkmale aktualisiert:

- In Citrix Endpoint Management integriert.
- Oder für VPN eingerichtet, nicht Teil der Citrix Endpoint Management-Umgebung und kann Citrix Endpoint Management erreichen.

Führen Sie auf dem virtuellen VPN-Server in einem Konsolenfenster die nachfolgend aufgeführten Schritte aus. Die hier gezeigten FQDNs und 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_EndpointManagement -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_EndpointManagement -authnProfile xm_nac_prof
   ```

8. Überprüfen Sie die Verbindung von NetScaler Gateway zu einem Gerät, indem Sie Folgendes eingeben:

   ```
   curl -v -k https://<Endpoint Management_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 Citrix Endpoint Management. 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 Citrix Endpoint Management, indem Sie Folgendes eingeben: In diesem Beispiel lautet die Citrix Endpoint Management-IP-Adresse `10.207.87.82` und der FQDN ist `example.em.cloud.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.cloud.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\")"
    ```

    Bei Erfolg ist die Ausgabe für Citrix Endpoint Management-NAC `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 Citrix 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
    ```

Windows-Desktop-/Tablet

June 25, 2024

Citrix Endpoint Management registriert Windows 10- und Windows 11-Geräte bei MDM. Citrix Endpoint Management unterstützt die folgenden Authentifizierungstypen für bei MDM registrierte Windows 10- und Windows 11-Geräte:

- Domänenbasierte Authentifizierung
  - Active Directory
  - Azure Active Directory
- Identitätsanbieter:
  - Azure Active Directory
  - Citrix-Identitätsanbieter

Weitere Informationen zu den unterstützten Authentifizierungstypen finden Sie unter Zertifikate und Authentifizierung.

Die Verwaltung von Windows 10- oder Windows 11-Geräten kann über folgendes Standardverfahren gestartet werden:

1. Durchführen des Onboarding-Prozesses. Weitere Informationen finden Sie unter Onboarding und Einrichten von Ressourcen und Vorbereitung zum Registrieren von Geräten und Bereitstellen von Ressourcen.

   Wenn Sie Windows-Geräte über den Autodiscoverydienst registrieren möchten, müssen Sie den Citrix Autodiscoverydienst konfigurieren. Unterstützung hierfür erhalten Sie beim technischen Support von Citrix. Weitere Informationen finden Sie unter Anfordern von Autodiscovery für Windows-Geräte.

2. Auswahl und Konfigurieren der Registrierungsmethode. Weitere Informationen finden Sie unter Unterstützte Registrierungsmethoden.
3. Konfigurieren der Geräterichtlinien für Windows-Desktops/-Tablets.
4. Registrieren von Windows 10- und Windows 11-Geräten durch Benutzer.
5. Einrichten von Sicherheitsaktionen für Apps und Geräte. Weitere Informationen finden Sie unter Sicherheitsaktionen.

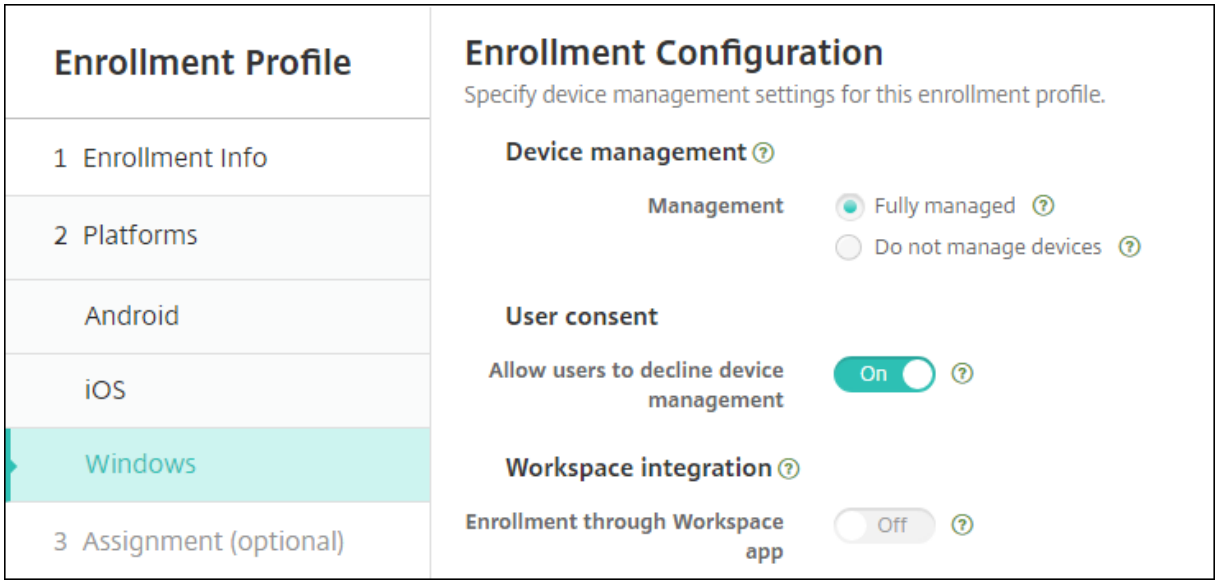
Informationen zu unterstützten Betriebssystemen finden Sie unter Unterstützte Gerätebetriebssysteme.

Unterstützte Registrierungsmethoden

Über Registrierungsprofile legen Sie fest, wie Windows 10- und Windows 11-Geräte verwaltet werden. Zwei Optionen stehen zur Verfügung.

- Vollständig verwaltet (MDM-Registrierung)
- Ohne Geräteverwaltung (keine MDM-Registrierung)

Um Registrierungseinstellungen für Windows 10- und Windows 11-Geräte zu konfigurieren, gehen Sie zu **Konfigurieren > Registrierungsprofile > Windows**. Weitere Informationen über Registrierungsprofile finden Sie unter Registrierungsprofile.



In der folgenden Tabelle werden die Registrierungsmethoden aufgelistet, die Citrix Endpoint Management für Windows 10- und Windows 11-Geräte unterstützt:

Methode	Unterstützt
Registrierung über Azure Active Directory	Ja
Registrierung über den Autodiscoverydienst	Ja
Windows-Massenregistrierung	Ja
Manuelle Registrierung	Ja
Registrierungseinladungen	Nein

> **Hinweis:**
>
> - Für die manuelle Registrierung müssen Benutzer den vollqualifizierten Domänennamen (FQDN) des Citrix Endpoint Management-Servers eingeben. Die manuelle Registrierung wird von uns nicht empfohlen. Verwenden Sie stattdessen andere Methoden, um den Registrierungsprozess für Benutzer zu vereinfachen.
> - Sie können keine Registrierungseinladungen an Windows-Geräte senden. Benutzer von Windows-Geräten registrieren diese direkt über das Gerät.

Konfigurieren der Geräterichtlinien für Windows-Desktops/-Tablets

Verwenden Sie diese Richtlinien, um die Interaktion von Citrix Endpoint Management mit Geräten zu konfigurieren, auf denen Windows 10 oder Windows 11 ausgeführt wird. In dieser Tabelle werden alle für Windows-Desktops/-Tablets verfügbaren Geräterichtlinien aufgeführt.

—	—	—
[App-Konfiguration](/de-de/citrix-endpoint-management/policies/app-configuration-policy.html#windows-desktoptablet-settings)	[App-Bestand](/de-de/citrix-endpoint-management/policies/app-inventory-policy.html)	[App-Sperre](/de-de/citrix-endpoint-management/policies/app-lock-policy.html#windows-desktop-and-tablet-settings)
[App-Deinstallation](/de-de/citrix-endpoint-management/policies/app-uninstall-policy.html)	[Application Guard](/de-de/citrix-endpoint-management/policies/application-guard-policy.html)	[BitLocker](/de-de/citrix-endpoint-management/policies/bitlocker-policy.html#windows-desktop-and-tablet-settings)
[Anmeldeinformationen](/de-de/citrix-endpoint-management/policies/credentials-policy.html#windows-desktoptablet-settings)	[Benutzerdefiniertes XML](/de-de/citrix-endpoint-management/policies/custom-xml-policy.html)	[Defender](/de-de/citrix-endpoint-management/policies/defender-policy.html)
[Device Guard](/de-de/citrix-endpoint-management/policies/device-guard-policy.html)	[Device Health Attestation](/de-de/citrix-endpoint-management/policies/device-health-attestation-policy.html)	[Exchange](/de-de/citrix-endpoint-management/policies/exchange-policy.html#windows-desktoptablet-settings)
[Firewall](/de-de/citrix-endpoint-management/policies/firewall-device-policy.html#windows-desktop-and-tablet-settings)	[Kiosk](/de-de/citrix-endpoint-management/policies/kiosk-policy.html#windows-desktop-and-tablet-settings)	[Netzwerk](/de-de/citrix-endpoint-management/policies/network-policy.html#windows-desktoptablet-settings)
[Office](/de-de/citrix-endpoint-management/policies/office-policy.html)	[OS-Update](/de-de/citrix-endpoint-management/policies/control-os-updates.html#windows-desktop-and-tablet-settings)	[Passcode](/de-de/citrix-endpoint-management/policies/passcode-policy.html#windows-desktoptablet-settings)
[Einschränkungen](/de-de/citrix-endpoint-management/policies/restrictions-policy.html#windows-desktoptablet-settings)	[Store](/de-de/citrix-endpoint-management/policies/store-policy.html)	[AGB](/de-de/citrix-endpoint-management/policies/terms-and-conditions-policy.html#windows-tablet-settings)
[VPN](/de-de/citrix-endpoint-management/policies/vpn-policy.html#windows-desktoptablet-settings)	[Webclip](/de-de/citrix-endpoint-management/policies/webclip-policy.html#windows-desktoptablet-settings)	[Windows Agent](/de-de/citrix-endpoint-management/policies/windows-agent-policy.html)
Windows-GPO-Konfiguration	Windows Hello for Business

Registrierung von Windows 10- und Windows 11-Geräten über Azure Active Directory

> **Wichtig:**

> Bevor Benutzer sich registrieren können, müssen Sie Azure Active Directory (AD)-Einstellungen in Azure konfigurieren und dann Citrix Endpoint Management konfigurieren. Weitere Informationen finden Sie unter Verbinden von Citrix Endpoint Management und Azure AD.

Windows 10- und Windows 11-Geräte können mit Microsoft Azure als Active Directory-Verbundauthentifizierung registriert werden. Für diese Registrierung ist ein Azure AD Premium-Abonnement erforderlich.

Mit den folgenden Verfahren können Sie Windows 10- und Windows 11-Geräte in Microsoft Azure AD einbinden:

- Für unternehmenseigene Geräte:
  - Führen Sie die MDM-Registrierung durch, wenn Sie das Gerät beim ersten Einschalten in Azure AD einbinden. In diesem Szenario schließen Benutzer die Registrierung wie in diesem Artikel beschrieben ab: https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-joined-devices-frx.

    Für Windows-Geräte, die Sie auf diese Weise registrieren, können Sie Windows AutoPilot zum Einrichten und Vorkonfigurieren der Geräte verwenden. Weitere Informationen finden Sie unter Einrichten und Konfigurieren von Geräten mit Windows AutoPilot.
  - Führen Sie die MDM-Registrierung durch, wenn Sie das Gerät über die Windows-Seite **Einstellungen** nach dem Konfigurieren in Azure AD einbinden. In diesem Szenario schließen Benutzer die Registrierung wie unter MDM-Registrierung beim Einbinden in Azure AD nach der Gerätekonfiguration beschrieben ab.
- Für persönliche Geräte (BYOD oder mobile Geräte):
  - Führen Sie die MDM-Registrierung beim Registrieren in Azure AD durch, während Sie das Microsoft-Arbeitskonto zu Windows hinzufügen. In diesem Szenario schließen Benutzer die Registrierung wie unter MDM-Registrierung beim Registrieren in Azure AD beschrieben ab.

MDM-Registrierung beim Einbinden in Azure AD nach der Gerätekonfiguration

1. Navigieren Sie auf einem Gerät im Startmenü zu **Einstellungen > Konten > Arbeitsplatz oder Schule** und klicken Sie auf **Verbinden**.
2. Klicken Sie unter **Geschäfts-, Schul- oder Unikonto einrichten** unter **Alternative Aktionen** auf **Dieses Gerät in Azure Active Directory einbinden**.
3. Geben Sie die Azure AD-Anmeldeinformationen ein und klicken Sie auf **Anmelden**.
4. Akzeptieren Sie die Nutzungsbedingungen der Organisation.

- Wenn Benutzer auf **Ablehnen** klicken, wird das Gerät weder in Azure AD eingebunden noch in Citrix Endpoint Management registriert.

5. Klicken Sie auf **Beitreten**, um mit dem Registrierungsvorgang fortzufahren.
6. Klicken Sie auf **Fertig**, um die Registrierung abzuschließen.

MDM-Registrierung beim Registrieren in Azure AD

1. Navigieren Sie auf einem Gerät im Startmenü zu **Einstellungen > Konten > Arbeitsplatz oder Schule** und klicken Sie auf **Verbinden**.
2. Geben Sie im Dialogfeld **Geschäfts-, Schul- oder Unikonto einrichten** die Azure AD-Anmeldeinformationen ein und klicken Sie auf **Anmelden**.
3. Akzeptieren Sie die Nutzungsbedingungen der Organisation. Das Gerät wird in Azure AD und bei Citrix Endpoint Management registriert.

   - Wenn Benutzer auf **Ablehnen** klicken, wird das Gerät zwar in Azure AD registriert, aber nicht in Citrix Endpoint Management. Es gibt keine **Info**-Schaltfläche zum Konto.

4. Klicken Sie auf **Beitreten**, um mit der Registrierung fortzufahren.
5. Klicken Sie auf **Fertig**, um die Registrierung abzuschließen.

Registrieren von Windows-Geräten über den Autodiscoverydienst

Wenden Sie sich an den technischen Support von Citrix, um den Autodiscoverydienst für Windows-Geräte zu konfigurieren. Weitere Informationen finden Sie unter Anfordern von Autodiscovery für Windows-Geräte.

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

Benutzer führen die folgenden Schritte aus, um die Registrierung abzuschließen:

1. Navigieren Sie auf einem Gerät im Startmenü zu **Einstellungen > Konten > Zugriff auf Geschäfts-, Schul- oder Unikonto** und klicken Sie auf **Nur bei Geräteverwaltung registrieren**.
2. Geben Sie im Dialogfeld **Geschäfts-, Schul- oder Unikonto einrichten** eine E-Mail-Adresse des Unternehmens ein und klicken Sie auf **Weiter**.

   Zur Registrierung als lokaler Benutzer geben Sie eine nicht vorhandene E-Mail-Adresse mit dem richtigen Domänennamen (z. B. `foo\@mydomain.com`) ein. Damit können Benutzer eine

bekannte Microsoft-Einschränkung umgehen, durch die die integrierte Geräteverwaltung unter Windows die Registrierung durchführt. Geben Sie im Dialogfeld **Mit einem Dienst verbinden** den Benutzernamen und das Kennwort des lokalen Benutzers ein. Das Gerät sucht dann einen Citrix Endpoint Management-Server und startet die Registrierung.

3. Geben Sie die Anmeldeinformationen ein und klicken Sie auf **Weiter**.
4. Stimmen Sie im Dialogfeld **Nutzungsbedingungen** der Verwaltung Ihres Geräts zu und tippen Sie auf **Annehmen**.

Das Registrieren von domänengebundenen Windows-Geräten über den Autodiscoverydienst schlägt fehl, wenn die Domänenrichtlinie die MDM-Registrierung deaktiviert. Benutzer können stattdessen eine der folgenden Methoden verwenden:

- Entfernen Sie die Geräte aus der Domäne, registrieren Sie sie und binden Sie sie erneut ein.
- Geben Sie den vollqualifizierten Domänennamen des Citrix Endpoint Management-Servers ein, um fortzufahren.

Windows-Massenregistrierung

Per Windows-Massenregistrierung können Sie viele Geräte für die Verwaltung durch einen MDM-Server ohne Reimaging der Geräte einrichten. Sie können das Provisioningpaket für die Massenregistrierung von Windows 10- und Windows 11-Desktops/-Tablets verwenden. Weitere Informationen finden Sie unter Massenregistrierung von Windows-Geräten.

Sicherheitsaktionen

Windows 10- und Windows 11-Geräte unterstützen die folgenden Sicherheitsaktionen. Eine Beschreibung der einzelnen Sicherheitsaktionen finden Sie unter Sicherheitsaktionen.

Orten	Sperren	Neustart
Widerrufen	Selektiv löschen	Löschen

Verbinden von Citrix Endpoint Management und Azure AD

Windows 10- und Windows 11-Geräte können sich in Azure registrieren. Benutzer, die in Azure AD erstellt wurden, können auf diese Geräte zugreifen. Citrix Endpoint Management wird in Microsoft Azure als MDM-Dienst bereitgestellt. Durch das Verbinden von Citrix Endpoint Management und Azure

AD können Benutzer ihre Geräte automatisch bei Citrix Endpoint Management registrieren, wenn sie sie in Azure AD registrieren.

Führen Sie die folgenden Schritte aus, um Citrix Endpoint Management mit Azure AD zu verbinden:

1. Navigieren Sie im Azure-Portal zu **Azure Active Directory > Mobilität (MDM und MAM) > Anwendung hinzufügen** und klicken Sie auf **Lokale MDM-Anwendung**.
2. Geben Sie einen Namen für die Anwendung ein und klicken Sie auf **Hinzufügen**.
3. (Optional) Azure erlaubt keine unverifizierten Domänen (z. B. cloud.com) für die IdP-Konfiguration. Wenn Ihr Citrix Endpoint Management-Registrierungs-FQDN cloud.com enthält, wenden Sie sich an den Citrix Support und geben Sie den TXT-Datensatz aus Azure an. Der Citrix Support überprüft die Unterdomäne, und Sie können dann mit der Konfiguration fortfahren. Wenn Ihr FQDN in Ihrer eigenen Domäne ist, können Sie ihn wie üblich in Azure überprüfen.
4. Wählen Sie die von Ihnen erstellte Anwendung aus, konfigurieren Sie folgende Einstellungen und klicken Sie auf **Speichern**.

    - **MDM-Benutzerbereich**. Wählen Sie **Alle**.
    - **URL für MDM-Nutzungsbedingungen**. Geben Sie sie im Format `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou` ein.
    - **URL für MDM-Ermittlung**. Geben Sie sie im Format `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe` ein.

5. Klicken Sie auf **Lokale MDM-Anwendungseinstellungen**.

    - Geben Sie im Bereich **Eigenschaften** die **App-ID-URI** im Format `https://< Citrix Endpoint Management Enrollment FQDN>:8443` ein. Diese App-ID-URI ist eine eindeutige ID, die Sie in keiner anderen App wiederverwenden können.
    - Wählen Sie im Bereich **Erforderliche Berechtigungen** die Optionen **Microsoft Graph** und **Windows Azure Active Directory** aus.
    - Erstellen Sie im Bereich **Schlüssel** den Authentifizierungsschlüssel. Klicken Sie auf **Speichern**, um den Schlüsselwert anzuzeigen. Der Schlüsselwert wird nur einmal angezeigt. Speichern Sie den Schlüssel für die spätere Verwendung. Sie benötigen den Schlüssel in Schritt 7.

6. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Identitätsanbieter (IdP)** und klicken Sie auf **Hinzufügen**.
7. Konfigurieren Sie auf der Seite **Discovery-URL** folgende Einstellungen und klicken Sie auf **Weiter**.

    - **IdP-Name**. Geben Sie einen eindeutigen Namen für die IdP-Verbindung ein, die Sie erstellen.

- **IdP-Typ**. Wählen Sie **Azure Active Directory**.
- **Mandanten-ID**. Die **Verzeichnis-ID** in Azure. Sie sehen sie, wenn Sie in Azure zu **Azure Active Directory > Eigenschaften** navigieren.

8. Konfigurieren Sie auf der Seite **Info über Windows MDM** folgende Einstellungen und klicken Sie auf **Weiter**.

   - **App-ID-URI**. Der APP-ID-URI-Wert, den Sie in Azure eingegeben haben.
   - **Client-ID**. Die Anwendungs-ID, die Sie in Azure im Bereich **Eigenschaften** sehen.
   - **Schlüssel**. Der Schlüsselwert, den Sie im vorherigen Schritt 4 erstellt und gespeichert haben.

9. Konfigurieren Sie folgende Einstellungen auf der Seite **IdP-Anspruchsverwendung** und klicken Sie auf "Weiter".

   - **Benutzer-ID-Typ**. Wählen Sie **userPrincipalName**.
   - **Benutzer-ID-Zeichenfolge**. Geben Sie `${ id_token } .upn` ein.

10. Klicken Sie auf **Speichern**.
11. Fügen Sie einen Azure AD-Benutzer als lokalen Benutzer hinzu und weisen Sie ihn einer lokalen Benutzergruppe zu.
12. Erstellen Sie eine Geräterichtlinie für Nutzungsbedingungen und eine Bereitstellungsgruppe, die diese lokale Benutzergruppe enthält.

Geräteverwaltung bei Integration mit Workspace Environment Management

Nur mit Workspace Environment Management (WEM) sind MDM-Bereitstellungen nicht möglich. Mit Citrix Endpoint Management allein können Sie nur Windows 10- und Windows 11-Geräte verwalten. Durch die Integration beider Managementtools können Sie mit WEM auf MDM-Features zugreifen und mit Citrix Endpoint Management ein breiteres Spektrum an Windows-Betriebssystemen verwalten. Die Verwaltung erfolgt über die Konfiguration von Windows-Gruppenrichtlinienobjekten. Derzeit importieren Administratoren eine ADMX-Datei in Citrix Endpoint Management und übertragen sie auf Windows 10- und Windows 11-Desktops und -Tablets, um bestimmte Anwendungen zu konfigurieren. Mit der Geräterichtlinie zur Windows-GPO-Konfiguration können Sie Gruppenrichtlinienobjekte konfigurieren und Änderungen an den WEM-Dienst übertragen. Der WEM-Agent wendet dann die Gruppenrichtlinienobjekte auf Geräte und ihre Apps an.

Die Mobilgeräteverwaltung (MDM) ist keine Voraussetzung für die WEM-Integration. Sie können GPO-Konfigurationen auf jedes von WEM unterstützte Gerät übertragen, selbst wenn Citrix Endpoint Management das Gerät nicht nativ unterstützt.

Eine Liste der unterstützten Geräte finden Sie unter Betriebssystemanforderungen.

Geräte, die die Geräterichtlinie zur Windows-GPO-Konfiguration empfangen, werden im neuen Citrix Endpoint Management-Modus "WEM"ausgeführt. Unter **Verwalten > Geräte** wird in der Liste registrierter Geräte in der Spalte **Modus** für WEM-verwaltete Geräte **WEM** angezeigt.

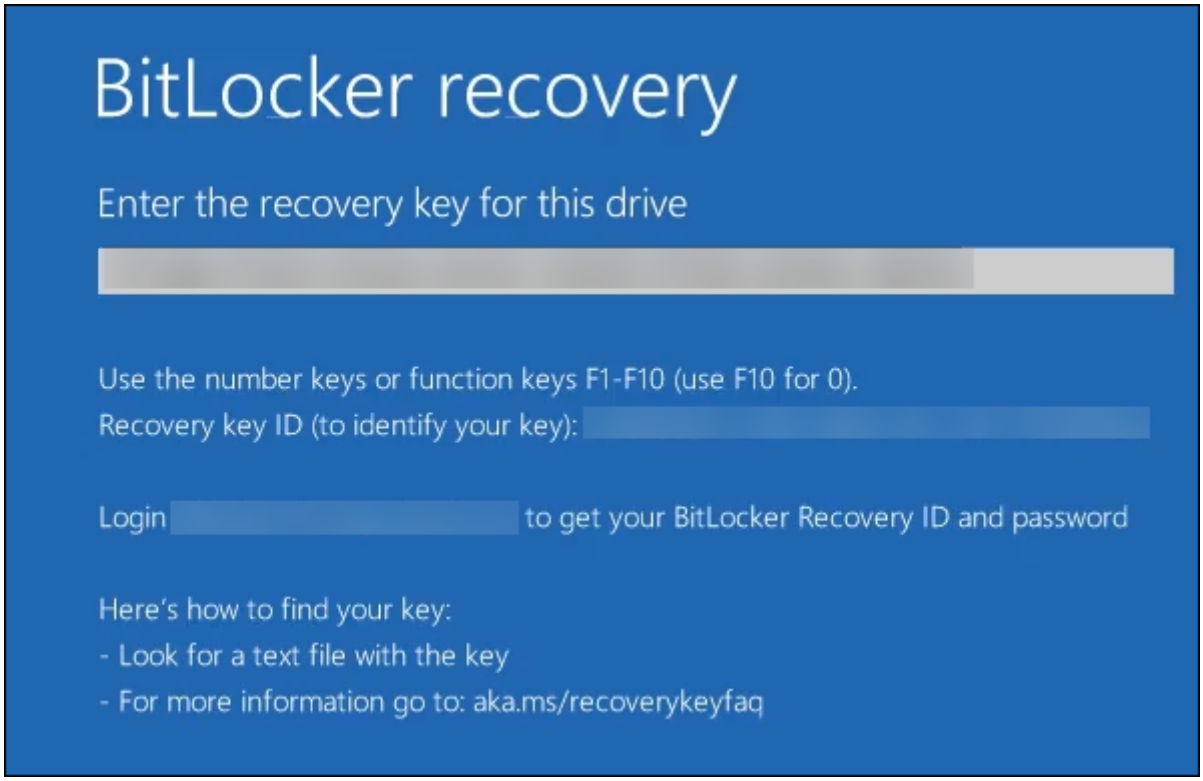
Weitere Informationen finden Sie unter Geräterichtlinie "Windows-GPO-Konfiguration".

BitLocker-Wiederherstellungsschlüssel

Das Verschlüsseln von Datenträgern mit BitLocker ist ein nützliches Sicherheitsfeature. Das Entsperren eines Geräts kann allerdings schwierig werden, wenn ein Benutzer seinen BitLocker-Wiederherstellungsschlüssel verliert. Citrix Endpoint Management kann jetzt automatisch und sicher BitLocker-Wiederherstellungsschlüssel für Benutzer speichern. Die Benutzer können ihren BitLocker-Wiederherstellungsschlüssel im Selbsthilfeportal finden. Aktivieren und Finden des BitLocker-Wiederherstellungsschlüssels:

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Servereigenschaften**.
2. Suchen Sie `shp` und aktivieren Sie das Feature `shp.console.enable`. Stellen Sie sicher, dass `enable.new.shp` deaktiviert bleibt. Weitere Informationen zum Aktivieren des Selbsthilfeportals finden Sie unter Registrierungssicherheitsmodi konfigurieren.
3. Gehen Sie zu **Konfigurieren > Geräterichtlinien**. Suchen Sie die BitLocker-Richtlinie oder erstellen Sie eine und aktivieren Sie die Einstellung **BitLocker-Wiederherstellungsbackup auf Citrix Endpoint Management**.

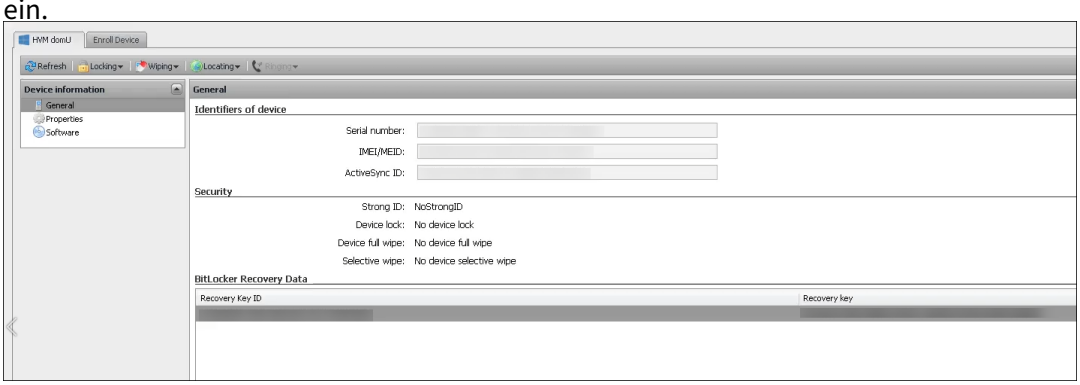
Beim Entsperren ihres Geräts sehen Endbenutzer eine Meldung, in der sie aufgefordert werden, ihren Schlüssel einzugeben. Die Meldung enthält auch die ID des Wiederherstellungsschlüssels.



Die Benutzer können ihren BitLocker-Wiederherstellungsschlüssel im Selbsthilfeportal finden.

1. Dort rufen sie unter **Allgemein** die Option **BitLocker-Wiederherstellungsdaten** auf.

    - **Wiederherstellungsschlüssel-ID:** ID des BitLocker-Wiederherstellungsschlüssels, der zum Verschlüsseln des Datenträgers verwendet wurde. Diese ID muss mit der in der vorherigen Meldung angegebenen Schlüssel-ID übereinstimmen.
    - **Wiederherstellungsschlüssel:** Schlüssel, den der Benutzer eingeben muss, um seinen Datenträger zu entsperren. Geben Sie diesen Schlüssel an der Entsperrungsaufforderung ein.



Weitere Informationen finden Sie unter BitLocker-Geräterichtlinie.

Massenregistrierung von Windows-Geräten

June 25, 2024

Citrix Endpoint Management unterstützt die Massenregistrierung von Desktop- und Tablet-Geräten mit Windows 10 und Windows 11. Dadurch können Sie viele Geräte für die Verwaltung durch Citrix Endpoint Management ohne Reimaging der Geräte einrichten. Sie verwenden das Provisioningpaket für die Massenregistrierung.

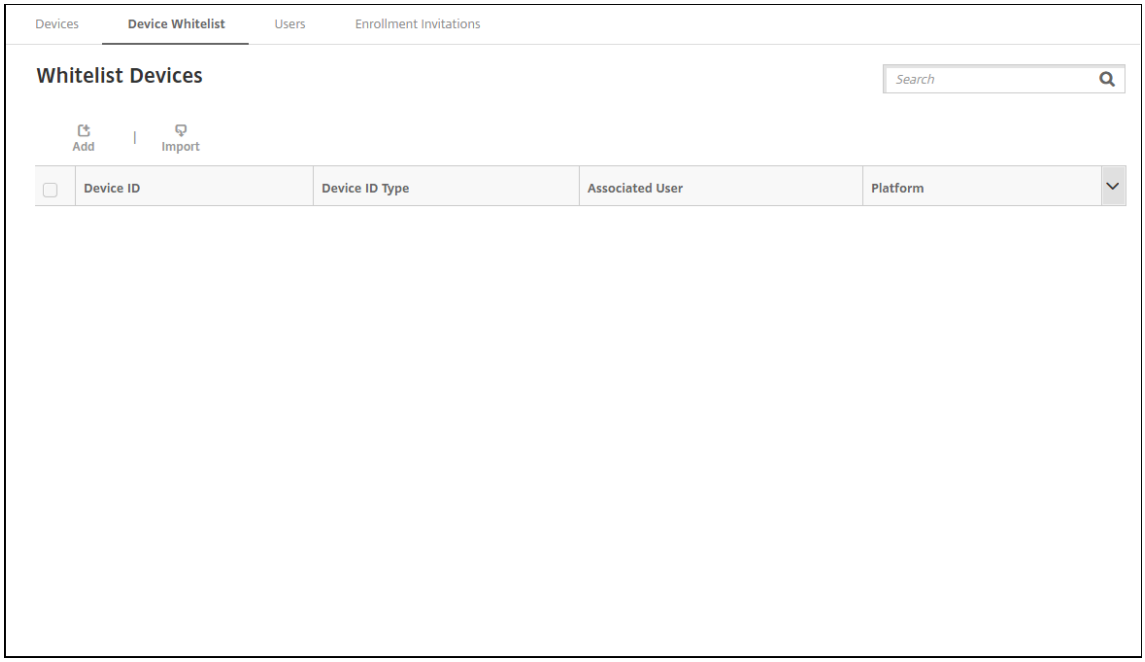
Dies ist ein allgemeiner Workflow für die Massenregistrierung von Windows 10- und Windows 11-Geräten:

1. Weisen Sie Geräte zu. Sie können Geräte einzeln oder gemeinsam zuweisen.
2. Konfigurieren Sie die Massenregistrierung.
3. Erstellen Sie ein Provisioningpaket und wenden Sie dieses Paket pro Gerät an.

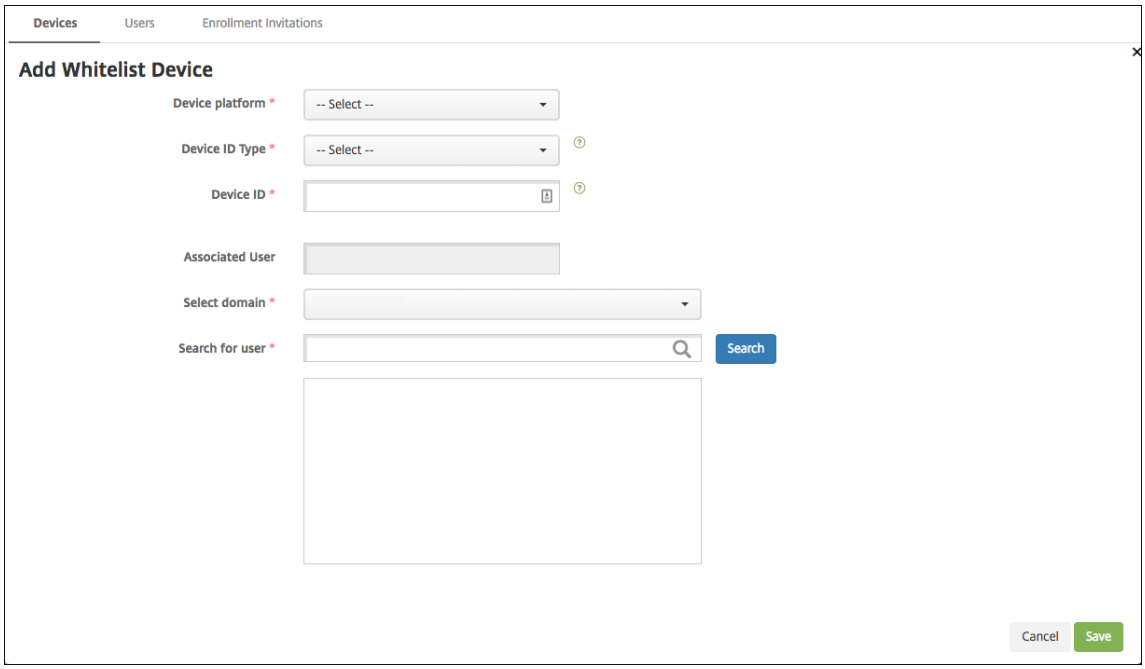
Stellen Sie vor der Massenregistrierung sicher, dass Sie jedes Gerät dem richtigen Benutzer zugewiesen haben. Führen Sie die Zuweisung durch, indem Sie die Geräte einzeln oder gemeinsam hinzufügen.

Zuweisen einzelner Geräte

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Verwalten** > **Geräte** > **Gerätepositivliste**.



2. Um jedes Gerät einzeln hinzuzufügen, klicken Sie auf **Hinzufügen**.



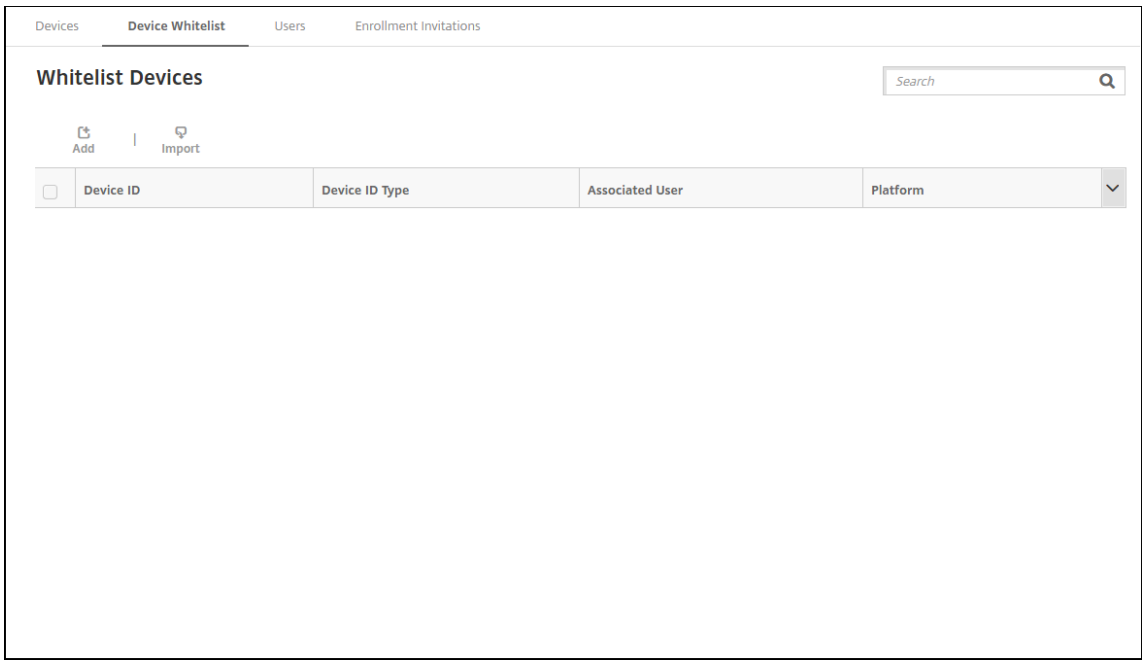
3. Geben Sie die folgenden Informationen ein:

   - **Geräteplattform:** Wählen Sie **Windows**.
   - **Geräte-ID-Typ:** Wählen Sie eine ID aus, die das Gerät identifiziert. Citrix Endpoint Management unterstützt **Hardware-ID** und **Gerätename** für Windows-Geräte.
   - **Geräte-ID:** Geben Sie die ID ein, die dem Typ entspricht, den Sie zuvor für das Gerät ausgewählt haben.
   - **Zugeordneter Benutzer:** Zeigt den Benutzer an, der diesem Gerät zugeordnet ist. Dieses Feld wird automatisch mit dem ausgewählten Benutzer gefüllt.
   - **Domäne auswählen:** Wählen Sie die Domäne, in der Sie nach einem zugeordneten Benutzer suchen möchten.
   - **Nach Benutzer suchen** Geben Sie den vollständigen Benutzernamen oder ein Teil davon in dieses Feld ein und klicken Sie auf **Suchen** um einen Benutzer zu finden, der diesem Gerät zugeordnet werden soll.

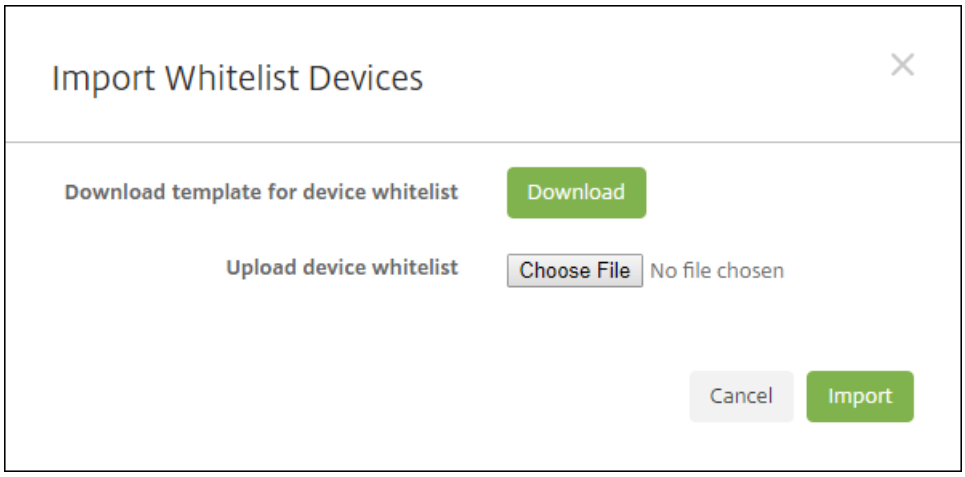
4. Klicken Sie auf **Speichern**.

Große Mengen an Geräten hinzufügen

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Verwalten > Geräte > Gerätepositivliste**.



2. Klicken Sie auf **Importieren**.

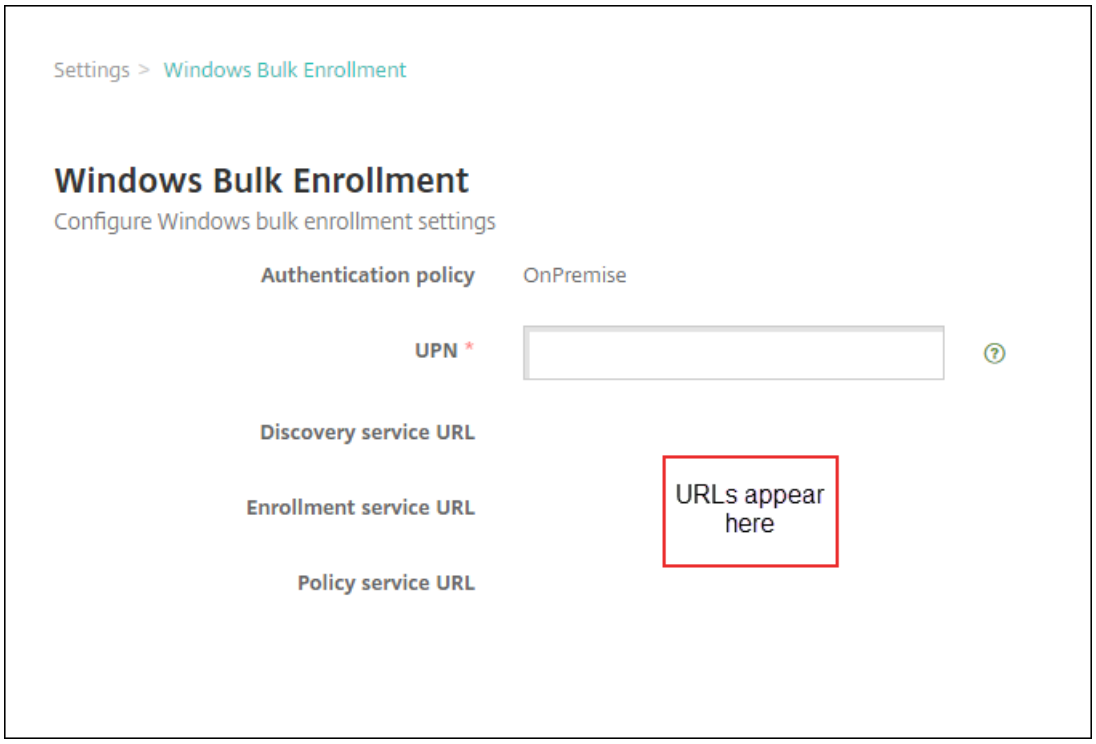


3. Klicken Sie auf **Herunterladen**, um eine Vorlage (Kalkulationstabelle) für die Positivliste für Geräte herunterzuladen. Füllen Sie die Kalkulationstabelle aus und laden Sie sie mit **Datei auswählen** und **Importieren** hoch.

Konfigurieren der Massenregistrierung

1. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Windows-Massenregistrierung**.
2. Geben Sie im Feld **UPN** einen Benutzernamen ein, der für die Bereitstellung aller Geräte verwendet werden soll. Der UPN muss ein gültiger Benutzer in Citrix Endpoint Management sein, der

über die Registrierungsberechtigungen verfügt. Sie können einen UPN angeben, der sich vom zuvor ausgewählten zugeordneten Benutzer unterscheidet.



Sie benötigen die URLs, wenn Sie ein Provisioningpaket im Windows Configuration Designer erstellen.

3. Klicken Sie auf **Speichern**.

Erstellen und Anwenden eines Provisioningpakets

Laden Sie für das Massenprovisioning von Geräten Windows Configuration Designer aus dem Microsoft-Store herunter. Windows Configuration Designer erstellt die Provisioningpakete für das Geräteimaging. Sie können Citrix Endpoint Management-Einstellungen für die Massenregistrierung in die Pakete einschließen, damit die Geräte automatisch bei Citrix Endpoint Management registriert werden.

Weitere Informationen zur Verwendung eines Provisioningpakets finden Sie unter https://docs.microsoft.com/en-us/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool. Führen Sie die Schritte aus, die dort im Abschnitt *Erstellen und Anwenden eines Bereitstellungspakets für die lokale Authentifizierung* beschrieben sind. Führen Sie diese Schritte aus, um die folgenden Konfigurationseinstellungen für die Massenregistrierung in Citrix Endpoint Management festzulegen und das Paket auf jedes Gerät anzuwenden.

- **Discoverydienst-URL**.

- **Registrierungsdienst-URL**.
- **Richtliniendienst-URL**.
- **Geheimnis**. Kennwort des UPN. Bislang haben Sie den Benutzernamen in das Feld "UPN" eingegeben.

Massenregistrierung von Geräten beim ersten Einschalten

Citrix Endpoint Management unterstützt die Massenregistrierung von Windows-Geräten beim ersten Einschalten. Folgen Sie den nachstehenden Schritten zur Einrichtung und Durchführung einer Massenregistrierung:

1. Verwenden Sie die Citrix Endpoint Management-Konsole, um Geräte (einzeln oder gemeinsam) hinzuzufügen und die Massenregistrierung zu konfigurieren. Weitere Informationen finden Sie unter Große Mengen an Geräten hinzufügen und Konfigurieren der Massenregistrierung.
2. Erstellen Sie ein Provisioningpaket, wie unter Erstellen und Anwenden eines Provisioningpakets beschrieben.

   > **Hinweis:**
   >
   > Beim Erstellen eines Provisioningpakets müssen Sie den Gerätenamen für jedes Gerät konfigurieren. Navigieren Sie dazu im Windows Configuration Designer zu **Laufzeiteinstellungen > Konten > Computerkonto > Computername** und legen Sie den Namen des Geräts fest. Der angegebene Gerätename muss mit dem Namen übereinstimmen, den Sie beim Importieren der Geräte über die Positivliste verwendet haben.

3. Speichern Sie das Provisioningpaket auf einem USB-Stick.
4. Schließen Sie den USB-Stick im Zielgerät an, wenn der Benutzer das Gerät zum ersten Mal einschaltet.

   Das Windows-Gerät erkennt automatisch das Provisioningpaket (.ppkg) auf dem USB-Stick. Detaillierte Anweisungen finden Sie in der Microsoft-Dokumentation zum Anwenden eines Provisioningpakets bei der Ersteinrichtung.

Das Gerät registriert sich automatisch bei Citrix Endpoint Management.

Auf Geräten mit Windows 10 (ab Version 2004) oder Windows 11 können Sie den Registrierungsprozess vereinfachen, indem Sie nur ein Provisioningpaket erstellen. Dieses Paket kann dann auf alle Geräte angewendet werden. Sie müssen dann kein Provisioningpaket für jedes Gerät erstellen.

Führen Sie beim Erstellen eines Provisioningpakets die folgenden Schritte aus, um den Registrierungsprozess zu vereinfachen:

1. Navigieren Sie im Windows Configuration Designer zu **Laufzeiteinstellungen > Konten > Computerkonto > Computername**.

2. Geben Sie im Feld **Computername** die folgende Zeichenfolge als Teil des Gerätenamens ein: `%SERIAL%`. Beispiel: `Surface-%SERIAL%`. Die Zeichenfolge wird auf die BIOS-Seriennummer jedes Geräts erweitert.

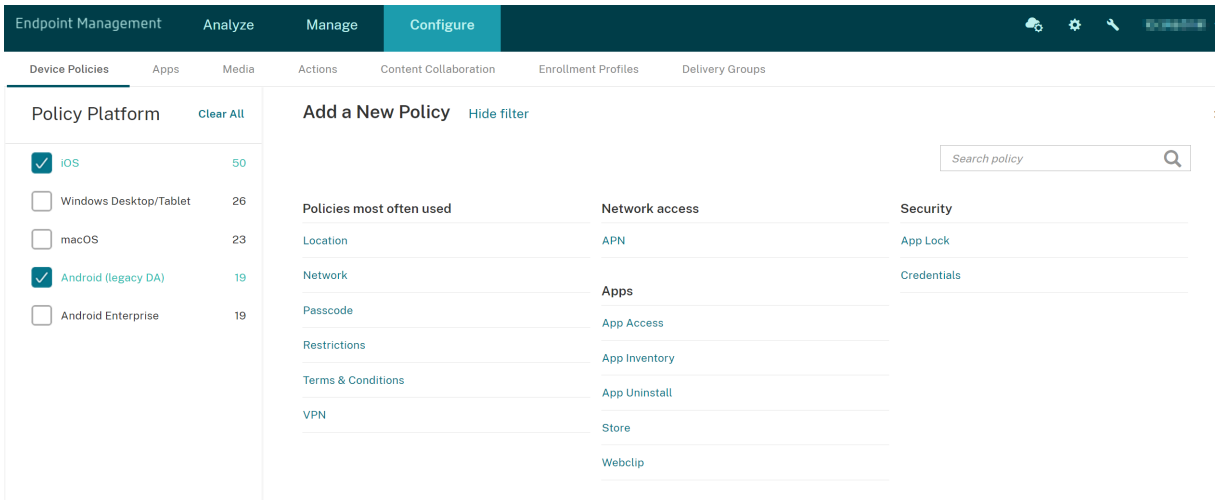
Geräterichtlinien

June 25, 2024

Durch Erstellen von Richtlinien können Sie konfigurieren, wie Citrix Endpoint Management 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.

Anzeige der pro Plattform verfügbaren Richtlinien:

1. Klicken Sie in der Citrix Endpoint Management-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.



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 folgenden Regeln beim Konfigurieren der Citrix Endpoint Management-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.

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

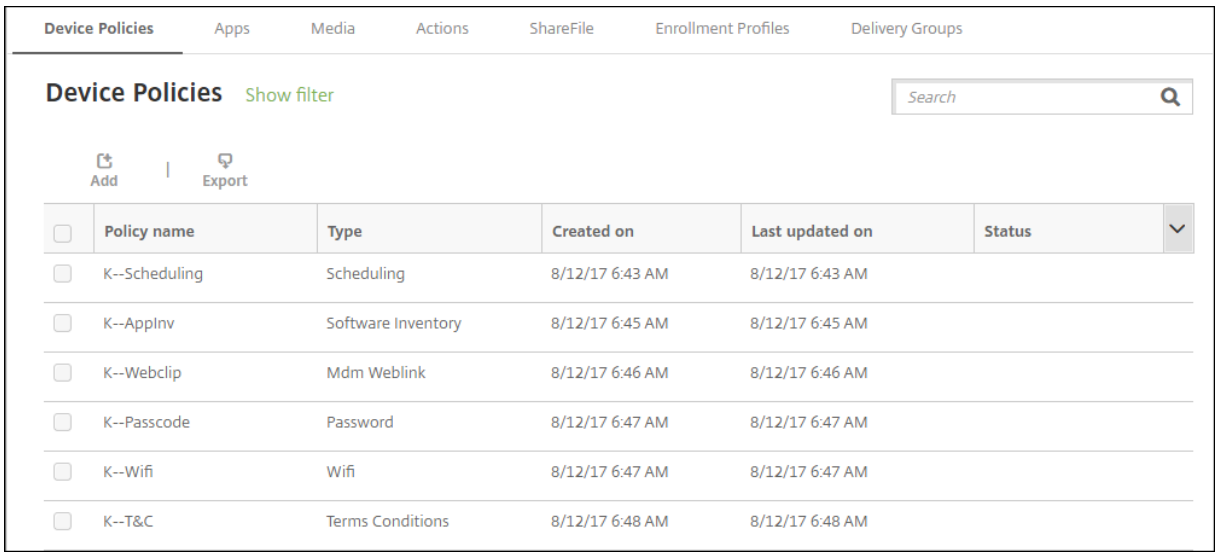
Das Erstellen einer Geräterichtlinie besteht im Wesentlichen aus folgenden Schritten:

1. Benennen und Beschreiben der Richtlinie

   > **Wichtig:**
   >
   > Verwenden Sie keinen Schrägstrich (/) in einem Richtliniennamen. Dieser kann einen Fehler verursachen, wenn Sie die Richtlinie später bearbeiten.

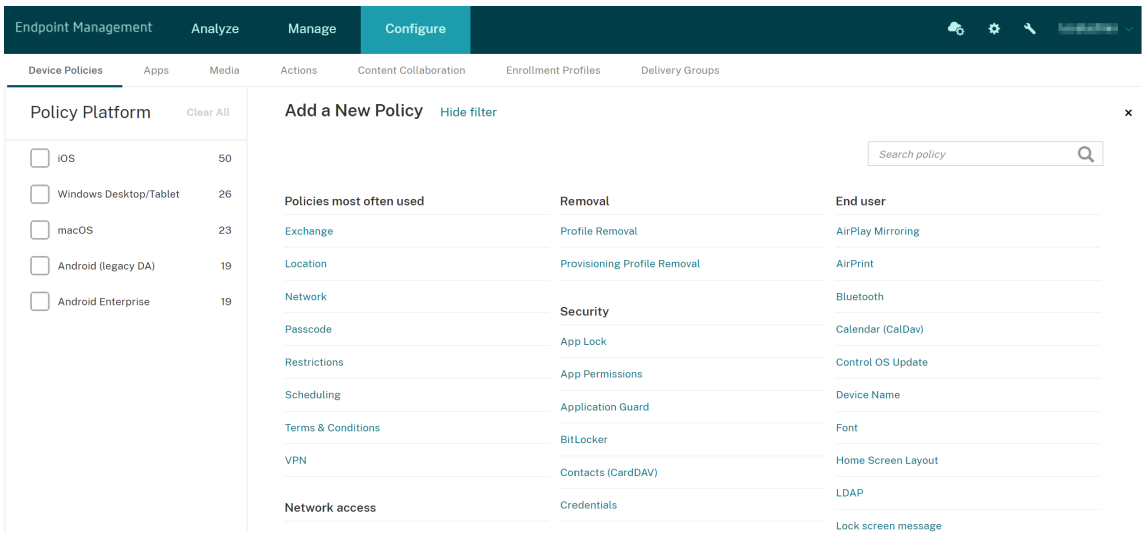
2. Konfigurieren der Richtlinie für eine oder mehrere Plattformen
3. Erstellen von Bereitstellungsregeln (optional)
4. Zuweisen der Richtlinie zu Bereitstellungsgruppen
5. Konfigurieren des Bereitstellungszeitplans (optional)

Zum Erstellen und Verwalten der Geräterichtlinien gehen Sie zu **Konfigurieren > Geräterichtlinien**.

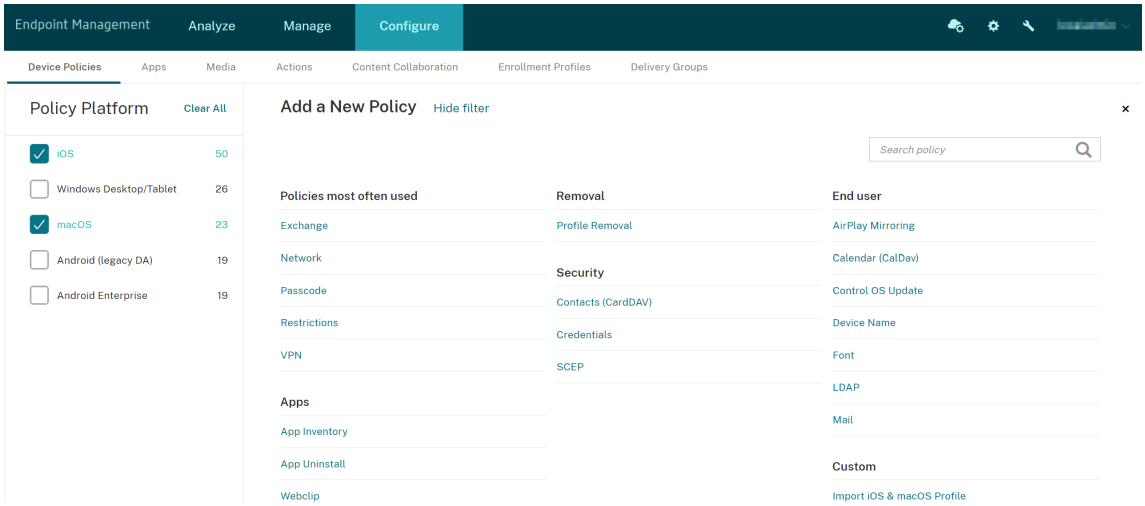


Hinzufügen einer Richtlinie

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 Ressourcen bereitstellen.

1. Erweitern Sie auf einer Plattformseite **Bereitstellungsregeln** und konfigurieren Sie folgende Einstellungen. Standardmäßig wird die Registerkarte **Basis** angezeigt.

    - Wählen Sie in den Listen die gewünschten Optionen aus, um die Bedingungen für die Bereitstellung festzulegen. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardoption ist auf **Alle**festgelegt.
    - 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.

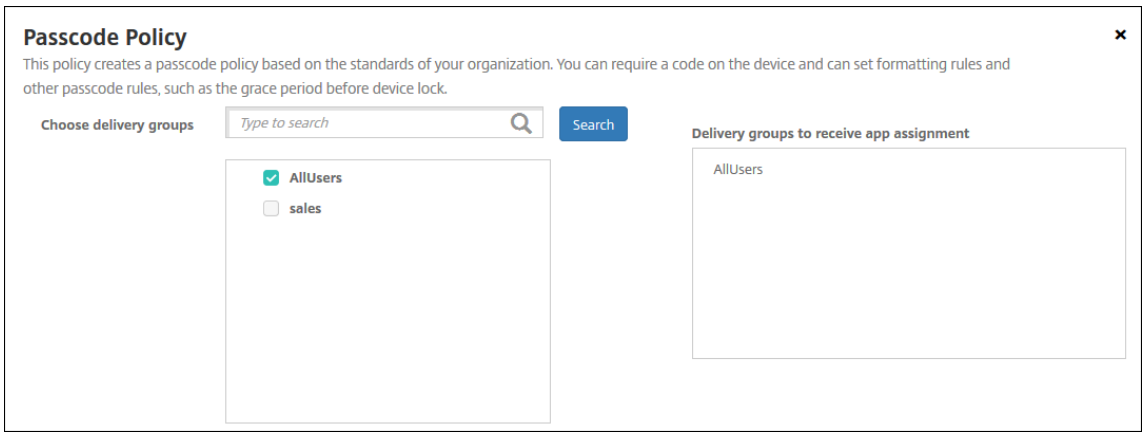
    - Klicken Sie auf **UND**, **ODER** oder **NICHT**.
    - Wählen Sie in den Listen die Bedingungen aus, die der Regel hinzugefügt werden sollen. Klicken Sie anschließend rechts auf das Pluszeichen (**+**), um die Bedingung zur Regel hinzuzufügen.

      Sie können jederzeit eine Bedingung auswählen und dann auf **BEARBEITEN** oder **Löschen** klicken.
    - 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.

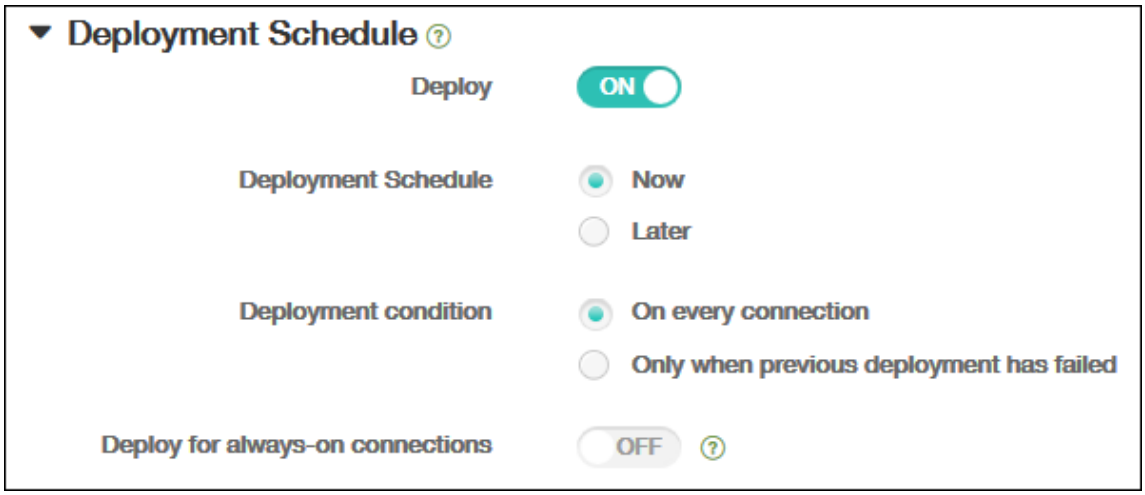


6. Erweitern Sie auf der Seite **Zuweisung** die Option **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

   - 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
     > - Ist nicht verfügbar für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version ab 10.18.19 verwenden
     > - Wird nicht empfohlen für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version vor 10.18.19 verwenden
     >
     > Der konfigurierte Bereitstellungszeitplan ist für alle Plattformen gleich. Alle von Ih-

> nen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**.



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 "Citrix Endpoint Management-Deinstallation". Weitere Informationen finden Sie unter Citrix Endpoint Management-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

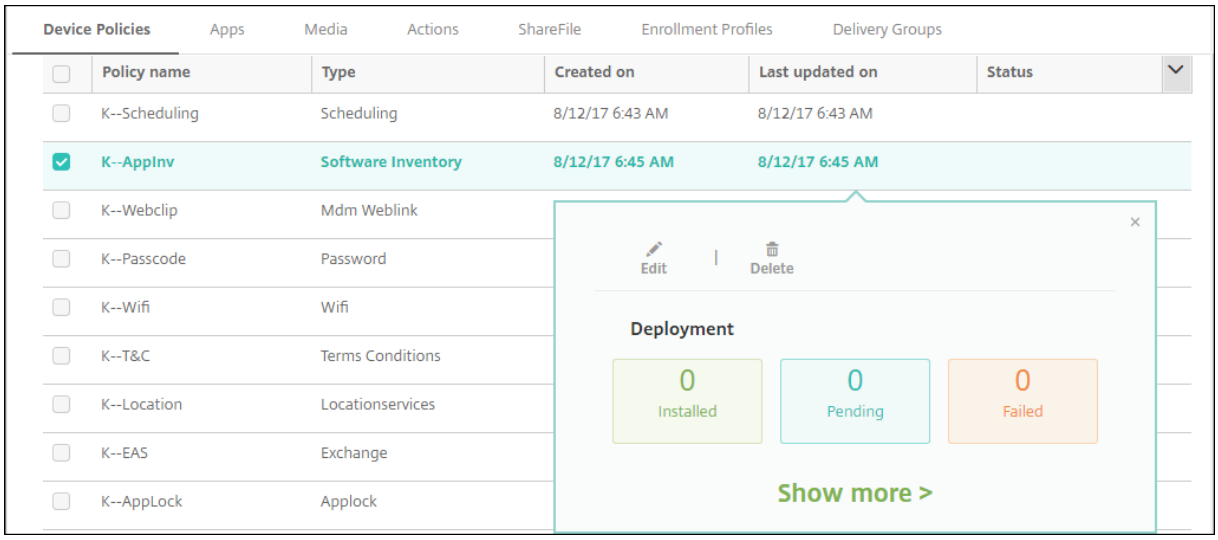
  Sie können eine Geräterichtlinie nicht direkt von einem Windows Desktop oder Tablet entfernen. Verwenden Sie stattdessen eine der folgenden Methoden:

  - 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.

Bearbeiten einer Geräterichtlinie

Zum Bearbeiten einer Richtlinie aktivieren Sie das Kontrollkästchen neben der Richtlinie. Das Menü der Optionen wird dann oberhalb der Richtlinienliste angezeigt. Oder klicken Sie auf eine Richtlinie in der Liste, um weitere Steuerelemente anzuzeigen.



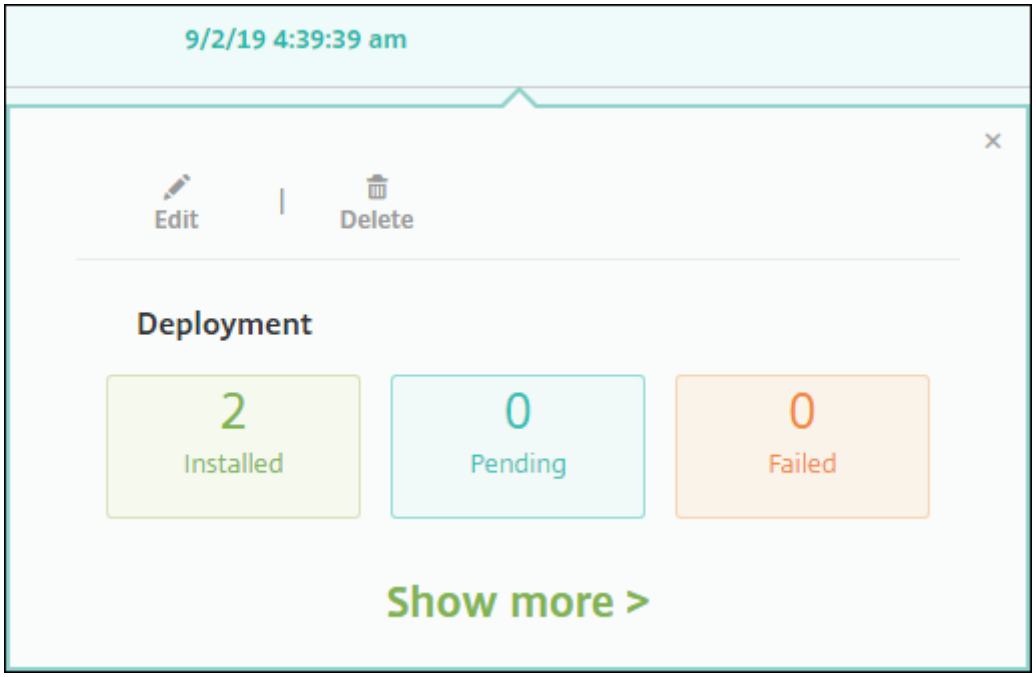
Um Details zur Richtlinie anzuzeigen, klicken Sie auf **Mehr anzeigen**.

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

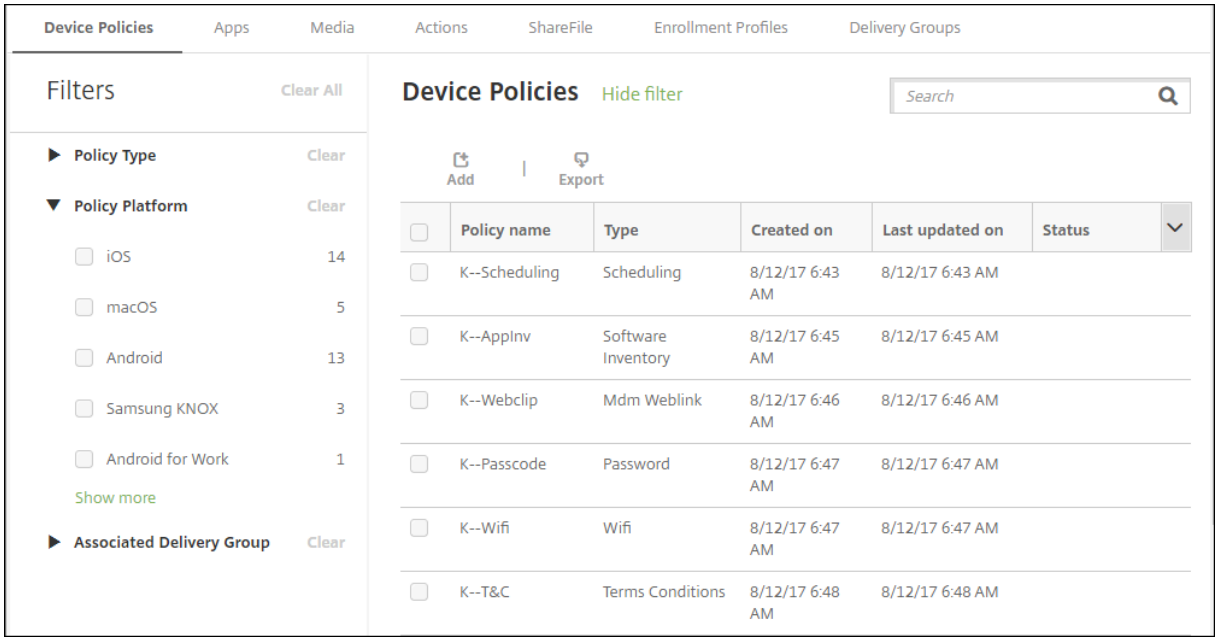
Klicken Sie auf der Seite **Konfigurieren > Geräterichtlinien** auf eine Richtlinienzeile, um den Bereitstellungsstatus zu überprüfen.



Bei ausstehender Bereitstellung einer Richtlinie können Benutzer die Richtlinie über Citrix 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. Apple TV oder einen Mac-Computer) zu iOS-Geräten hinzu. Sie können Geräte auch zu einer Positivliste für betreute Geräte hinzufügen. 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.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
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.
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. Auf Tablets oder Desktops mit Windows 10 können Sie wahlweise auch Schlüssel/Wert-Paare bereitstellen.
App-Bestand	Hiermit können Sie einen Bestand der Apps auf verwalteten Geräten abrufen. Citrix Endpoint Management 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.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
App-Sperre	Hiermit definieren Sie eine Liste von Apps, die Benutzer auf iOS- oder bestimmten Android-Geräten ausführen oder nicht ausführen können. Ermöglicht das Umwandeln eines iPads in einen Kiosk.
App-Berechtigungen	Hiermit können Sie konfigurieren, was geschieht, wenn Android Enterprise-Apps in Firmenprofilen Berechtigungsanfragen erhalten, die von Google als "gefährlich"eingestuft werden.
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.
Application Guard	Diese Richtlinie gibt (nur für den Microsoft Edge-Browser) die Windows Defender Application Guard-Einstellungen an. Die Einstellungen steuern, ob externer Inhalt auf Unternehmenssites blockiert werden soll.
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.
Bluetooth	Hiermit können Sie Bluetooth auf iOS-Geräten aktivieren oder deaktivieren.
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.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Cellular	Hiermit werden mobile Netzwerkeinstellungen konfiguriert.
Verbindungszeitplan	Diese Richtlinie ist für Android-Geräte erforderlich, damit sie für MDM-Verwaltung, App-Push und Richtlinienbereitstellung erneut eine Verbindung mit Citrix Endpoint Management herstellen. Wenn Sie diese Richtlinie nicht an Geräte senden und Google FCM nicht aktiviert haben, kann das Gerät keine Verbindung mit dem Server herstellen.
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.
Anmeldeinformationen	Ermöglicht eine in die Public Key-Infrastruktur in Citrix Endpoint Management 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 Aktivierung von Gerätefeatures, die Gerätekonfiguration und die Fehlerverwaltung anpassen.
Defender	Hiermit werden Windows Defender-Einstellungen für Windows 10 und Windows 11 für Desktop und Tablet konfiguriert.
Device Guard	Hiermit werden Sicherheitsfunktionen wie “Sicherer Start”, eine UEFI-Sperre und eine Virtualisierung aktiviert.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
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 Citrix Endpoint Management gesendet wird. Basierend auf dem Inhalt des Health Attestation-Zertifikats kann Citrix Endpoint Management 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. Unterstützt für iOS-/iPadOS-Geräte.
Citrix Endpoint Management-Optionen	Hiermit konfigurieren Sie das Citrix Secure Hub-Verhalten für Verbindungen zwischen Citrix Endpoint Management und Android-Geräten.
Citrix Endpoint Management-Deinstallation	Hiermit können Sie Citrix Endpoint Management von Android-Geräten deinstallieren. Wenn diese Richtlinie bereitgestellt wird, entfernt sie Citrix Endpoint Management von allen Geräten in der Bereitstellungsgruppe.
Exchange	Hiermit aktivieren Sie ActiveSync-E-Mail für den systemeigenen E-Mail-Client auf dem Gerät.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Dateien	Hiermit fügen Sie Citrix Endpoint Management 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.
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. Citrix Endpoint Management bietet keine Unterstützung für Schriftsammlungen (.ttc, .otc).
Layout für Homebildschirm	Gibt das Layout von Apps und Ordnern für den iOS-Homebildschirm auf betreuten iOS-Geräten an.
Importieren von iOS- und macOS-Profilen	Hiermit importieren Sie XML-Dateien für die Konfiguration von iOS- und macOS-Geräten in Citrix Endpoint Management. Die Datei enthält Gerätesicherheitsrichtlinien und -einschränkungen, die Sie mit Apple Configurator vorbereitet haben.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
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.
Schlüssel für Knox Platform for Enterprise	Ermöglicht es Ihnen, die erforderlichen Samsung Knox Platform for Enterprise-(KPE)-Lizenzinformationen bereitzustellen.
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 Citrix Secure Hub aktiviert. Nach dem Bereitstellen dieser Richtlinie auf dem Gerät können Sie einen Ortungsbefehl von Citrix Endpoint Management senden. Das Gerät antwortet dann mit den Standortkoordinaten. Citrix Endpoint Management unterstützt auch Richtlinien zum Geofencing und Gerätetracking.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Meldung auf Sperrbildschirm	Hiermit kann für das Anmeldefenster geteilter iPads und den Sperrbildschirm betreuter iOS-Geräte eine Meldung festgelegt werden, die bei Geräteverlust angezeigt wird.
E-Mail	Hiermit wird ein E-Mail-Konto auf iOS- oder macOS-Geräten konfiguriert.
Verwaltete Konfigurationen	Hiermit können Sie verschiedene App-Konfigurationsoptionen und App-Einschränkungen für Android Enterprise-Geräte steuern.
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 können Sie mithilfe von URLs oder Unterdomänen festlegen, wie Benutzer Dokumente, Anlagen und über den Browser heruntergeladene Objekte öffnen können.
Maximale Anzahl residenter Benutzer	Gibt die maximale Anzahl von Benutzern für ein geteiltes iPad an. Unterstützt für iOS- und iPadOS-Geräte.
MDM-Optionen	Hiermit wird die Aktivierungssperre des Features “Mein iPhone/iPad suchen”auf betreuten iOS-Geräten verwaltet.
Netzwerk	Diese Richtlinie ermöglicht Administratoren das Bereitstellen von Wi-Fi-Routerdetails auf verwalteten Geräten. Die Routerdetails umfassen die SSID sowie Authentifizierungs- und Konfigurationsdaten.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Netzwerknutzung	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 Citrix Endpoint Management auf den Geräten der Benutzer bereitstellen.
Office	Stellen Sie Microsoft Office-Apps auf jedem Gerät mit Windows 10 (Version 1709 oder höher) oder Windows 11 bereit.
Informationen zum Unternehmen	Hiermit geben Sie die Unternehmensinformationen für Warnmeldungen an, die von Citrix Endpoint Management auf iOS-Geräten bereitgestellt werden.
OS-Update	Hiermit werden aktuelle Betriebssystemupdates auf unterstützten und betreuten Geräten bereitgestellt.
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.
Passcodesperre - Kulanzzeitraum	Gibt die Zeitdauer in Minuten an, die der Bildschirm eines geteilten iPads gesperrt bleibt, bevor der Benutzer zum Entsperren einen Passcode eingeben muss. Unterstützt für iOS- und iPadOS-Geräte.
Persönlicher Hotspot	Hiermit können Benutzer sich auch dann mit dem Internet verbinden, wenn sie nicht in Reichweite eines Wi-Fi-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 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 iOS-Geräte festlegen. Sie können nur eine globale HTTP-Proxyrichtlinie pro Gerät bereitstellen.
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-Geräten das Sprach- und Datenroaming zugelassen wird. Bei deaktiviertem Sprachroaming wird das Datenroaming ebenfalls automatisch deaktiviert.
Samsung MDM-Lizenzschlüssel	Gibt den integrierten Samsung Enterprise License Management (ELM)-Schlüssel an, den Sie auf einem Gerät bereitstellen müssen. Citrix Endpoint Management unterstützt zudem den Dienst Samsung E-FOTA (Enterprise Firmware-Over-The-Air).

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 Citrix Endpoint Management verbundenen PKI an das Gerät übermitteln. Erstellen Sie dazu eine PKI-Entität und einen PKI-Anbieter im verteilten Modus.
Single Sign-On-Konto	Hiermit erstellen Sie Single Sign-On-Konten (SSO), damit Benutzer nach einmaliger Anmeldung auf Citrix Endpoint Management und interne Unternehmensressourcen zugreifen können. Sie müssen keine Anmeldeinformationen auf dem Gerät speichern. Die Unternehmensanmeldeinformationen eines SSO-Kontos werden von Citrix Endpoint Management 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.
Store	Hiermit geben Sie an, ob ein Webclip des App Store auf dem Homebildschirm von Benutzergeräten angezeigt wird.
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 Citrix Endpoint Management registrieren, müssen sie die Nutzungsbestimmungen akzeptieren, damit sie ihr Gerät registrieren können. Lehnen sie die Nutzungsbedingungen ab, wird die Registrierung abgebrochen.
Tunnel	Hiermit werden Proxyparameter zwischen der Clientkomponente beliebiger Mobilgeräte-Apps und der App-Serverkomponente definiert.
VPN	Diese Richtlinie ermöglicht den Zugriff auf Back-End-Systeme, die Legacy-VPN-Gatewaytechnologie verwenden. Die VPN-Gateway-Verbindungsinformationen ermöglichen die Bereitstellung auf Geräten. Citrix Endpoint Management 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.
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.
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 eigene Symbole für die Webclips angeben. Bei Windows-Tablets sind nur eine Beschriftung und eine URL erforderlich.

Name der Geräterichtlinie	Beschreibung der Geräterichtlinie
Webinhaltsfilter	Hiermit werden Webinhalte auf iOS-Geräten gefiltert. Citrix Endpoint Management verwendet die automatische Filterfunktion von Apple in Verbindung mit Ihren Sperr- und Positivlisten für Websites. Nur verfügbar für betreute iOS-Geräte.
Windows Agent	Aktivieren Sie diese Richtlinie, um hochgeladene PowerShell-Skripts auf Windows-Desktops und -Tablets auszuführen.
Windows-GPO-Konfiguration	Konfigurieren Sie Gruppenrichtlinienobjekte (GPOs) für alle Windows-Geräte, die von Citrix Workspace Environment Management unterstützt werden.
Windows Hello for Business	Aktiviert das Windows-Feature, damit Benutzer Windows Hello for Business auf ihrem Gerät bereitstellen können. Mit dieser Richtlinie können Sie auch Passcodebeschränkungen und andere Sicherheitsfunktionen konfigurieren.

Geräterichtlinien nach Plattform

Richtlinie	iOS	macOS	Android Enterprise	Android (Legacy-Geräteadmin)	Windows-Desktops und -Tablets	Sonstiges
Geräterichtlinie für die AirPlay-Synchronisierung	X	X				
AirPrint-Geräterichtlinie	X					
APN-Geräterichtlinie	X			X		
App-Zugriffsrichtlinie für Geräte	X			X		

Richtlinie	iOS	macOS	Android Enterprise	Android (Legacy-Geräteadmin)	Windows-Desktops und -Tablets	Sonstiges
Geräterichtlinie für App-Attribute	X					
App-Konfigurationsrichtlinie für Geräte	X				X	
App-Bestandsrichtlinie für Geräte	X	X	X	X	X	
Geräterichtlinie zum Sperren von Apps	X			X	X	
Geräterichtlinie für App-Berechtigungen			X			
App-Deinstallationsrichtlinie	X	X	X	X		
Einschränkungsrichtlinie für die App-Deinstallation						X
Application Guard-Richtlinie					X	
Geräterichtlinie für App-Benachrichtigungen	X					
Verwaltete Apps automatisch aktualisieren			X			
BitLocker-Geräterichtlinie					X	
Bluetooth-Geräterichtlinie	X					

Richtlinie	iOS	macOS	Android Enterprise	Android (Legacy-Geräteadmin)	Windows-Desktops und -Tablets	Sonstiges
Browserrichtlinie für Geräte						X
Kalenderrichtlinie	X	X				
Mobilfunkgerätericht linie	X					
Verbindungszeitplanrichtlinie für Geräte			X	X		
Geräterichtlinie für Kontakte (CardDAV)	X	X				
Richtlinie zum Kopieren von Apps in den Samsung-Container						X
Anmeldeinformationsrichtlinie	X	X	X	X	X	
Benutzerdefinierte XML-Geräterichtlinie			X		X	
Defender-Geräterichtlinie					X	
Device Guard-Richtlinie					X	
Integritätsnachweisrichtlinie für Geräte					X	
Richtlinien für Gerätenamen	X	X				
Geräterichtlinie “Bildung - Konfiguration”	X					

Richtlinie	iOS	macOS	Android Enterprise	Android (Legacy-Geräteadmin)	Windows-Desktops und -Tablets	Sonstiges
Citrix Endpoint Management-Optionsrichtlinie für Geräte			X	X		
Citrix Endpoint Management-Deinstallationsrichtlinie				X		
Exchange-Geräterichtlinie	X	X	X	X	X	
Dateirichtlinie			X	X		
FileVault-Geräterichtlinie		X				
Firewallrichtlinie		X			X	
Geräterichtlinie für Schriftarten	X	X				
Geräterichtlinie für Home-bildschirm-layout	X					
Geräterichtlinie “Gerätekon-figuration im-portieren”						X
Richtlinie zum Importieren von iOS- und macOS-Profilen	X	X				

Richtlinie	iOS	macOS	Android Enterprise	Android (Legacy-Geräteadmin)	Windows-Desktops und -Tablets	Sonstiges
Geräterichtlinie für die Keyguard-Verwaltung			X			
Kioskgeräterichtlinie			X		X	
Launcher-Konfigurationsrichtlinie			X	X		
LDAP-Geräterichtlinie	X	X				
Standortrichtlinie für Geräte	X		X	X		
Geräterichtlinie “Meldung auf Sperrbildschirm”	X					
E-Mail-Geräterichtlinie	X	X				
Geräterichtlinie für verwaltete Konfigurationen			X			
Geräterichtlinie für verwaltete Domänen	X					
Geräterichtlinie für die maximale Anzahl residenter Benutzer	X					

Richtlinie	iOS	macOS	Android Enterprise	Android (Legacy-Geräteadmin)	Windows-Desktops und -Tablets	Sonstiges
MDM-Optionsrichtlinien für Geräte	X					
Netzwerkgerätrichtlinie	X		X	X		
Richtlinie für die Netzwerkauslastung	X					
Office-Geräterichtlinie					X	
Geräterichtlinie für Unternehmensinformationen	X					
Geräterichtlinie für OS-Updates	X	X	X		X	
Passcode-Geräterichtlinie	X	X	X	X	X	
Passcodesperre - Kulanzzeitraumrichtlinie	X					
Richtlinien für persönliche Hotspots	X					
Geräterichtlinie für Profilentfernung	X	X				
Provisioningprofilrichtlinie	X					

Richtlinie	iOS	macOS	Android Enterprise	Android (Legacy-Geräteadmin)	Windows-Desktops und -Tablets	Sonstiges
Richtlinie zum Entfernen von Provisioningprofilen	X					
Proxy-Geräterichtlinie	X					
Geräteeinschränkungsrichtlinie	X	X		X	X	
Roamingrichtlinie	X					
Geräterichtlinie für Samsung MDM-Lizenzschlüssel			X			
SCEP-Geräterichtlinie	X	X				
Richtlinien für Siri und die Diktierfunktion	X					
SSO-Kontorichtlinie	X					
Speicherverschlüsselungsrichtlinie für Geräte						
Store-Geräterichtlinie	X			X	X	
Richtlinie für abonnierte Kalender	X					
AGB-Geräterichtlinie	X			X	X	
Geräterichtlinie für Tunnel				X		

Richtlinie	iOS	macOS	Android Enterprise	Android (Legacy-Geräteadmin)	Windows-Desktops und -Tablets	Sonstiges
VPN-Geräterichtlinie	X	X		X	X	
Hintergrundbild-Geräterichtlinie	X					
Webclip-Geräterichtlinie	X	X		X	X	
Geräterichtlinie für Webinhaltsfilter	X					
Windows Agent-Geräterichtlinie					X	
Geräterichtlinie “Windows-GPO-Konfiguration”					X	
Geräterichtlinie für Windows Hello for Business					X	

Geräterichtlinie für die AirPlay-Synchronisierung

December 1, 2023

Mit dem Apple AirPlay-Feature kann Inhalt drahtlos von einem iOS-Gerät über Apple TV auf einen Fernseher gestreamt oder die Anzeige auf dem Gerät auf einem Fernseher oder einem Mac-Computer gespiegelt werden.

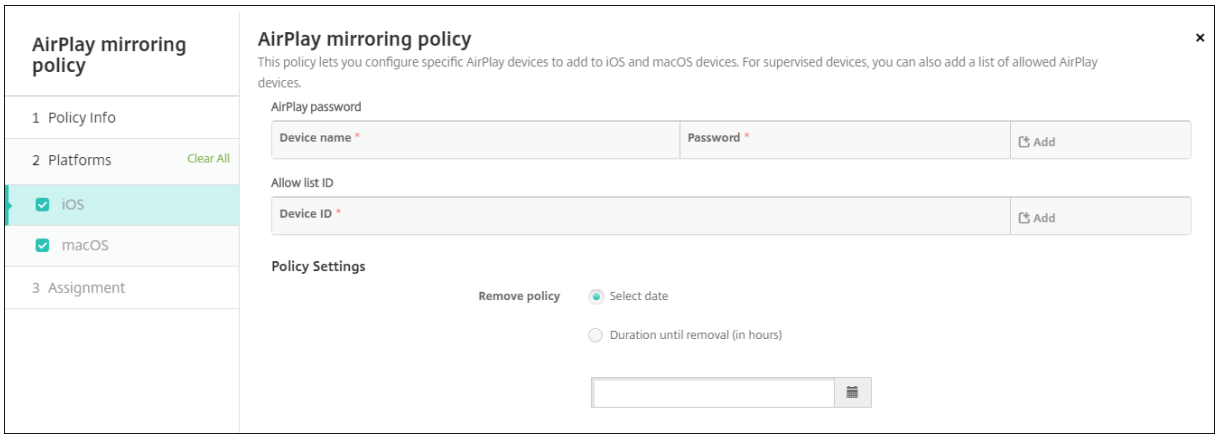
Sie können in Citrix Endpoint Management eine Geräterichtlinie zum Hinzufügen spezifischer AirPlay-Geräte (z. B. Apple TV oder einen anderen Mac-Computer) einrichten und iOS-Geräten hinzufügen. Zudem können Sie Geräte zu einer Positivliste betreuter Geräte hinzufügen, sodass Benutzer nur diese

AirPlay-Geräte verwenden können. Informationen, wie Sie Geräte in den betreuten Modus versetzen, finden Sie unter Bereitstellen von Geräten mit Apple Configurator 2.

> **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 Gerätерichtlinien.

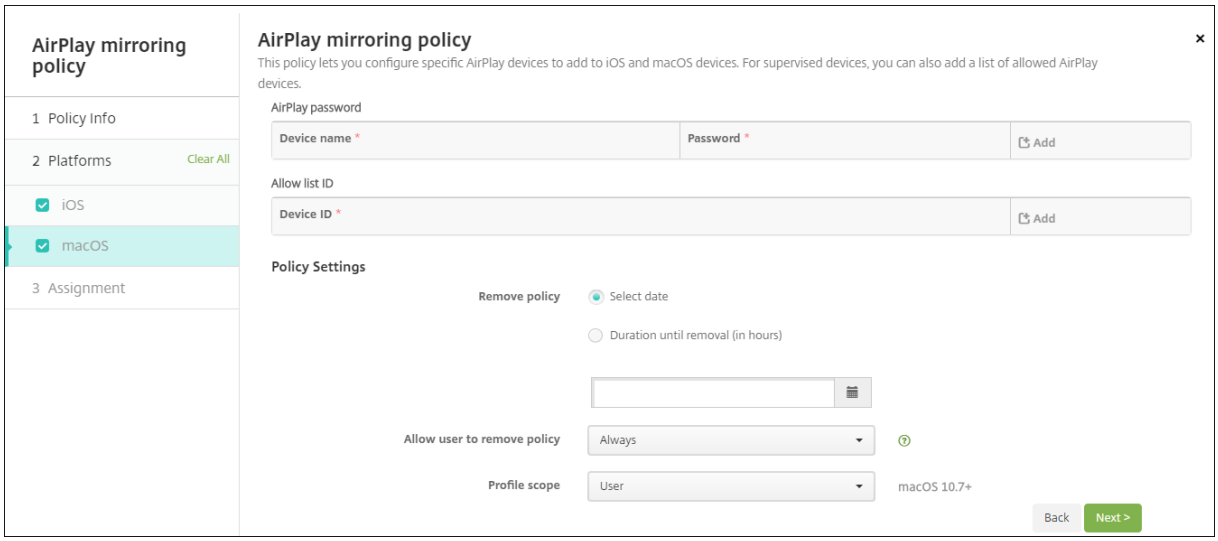
iOS-Einstellungen



- **AirPlay-Kennwort:** Für jedes Gerät, das Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Gerätename:** 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.

macOS-Einstellungen



- **AirPlay-Kennwort:** Für jedes Gerät, das Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Gerätename:** 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

December 10, 2021

Mit der AirPrint-Geräterichtlinie 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.

> **Hinweis:**
>
> Um die AirPrint-Geräterichtlinie zu konfigurieren, benötigen Sie die IP-Adresse und den Ressourcenpfad jedes Druckers.

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 `_ipps.tcp`. Beispiel: `printers/Canon_MG5300_series` oder `printers/Xerox_Phaser_7600`.

- **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 verfügbar ab iOS 6.0.

Geräterichtlinie für App-Berechtigungen

June 25, 2024

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 folgende Berechtigungen als "gefährlich":

- Berechtigungen, die App-Zugriff auf Daten oder Ressourcen geben, die private Benutzerinformationen betreffen.
- Oder solche, die potenzielle Auswirkungen auf die gespeicherten Daten des Benutzers oder den Betrieb anderer Apps haben. Beispielsweise ist die Möglichkeit, Benutzerkontakte zu lesen, eine gefährliche Berechtigung.

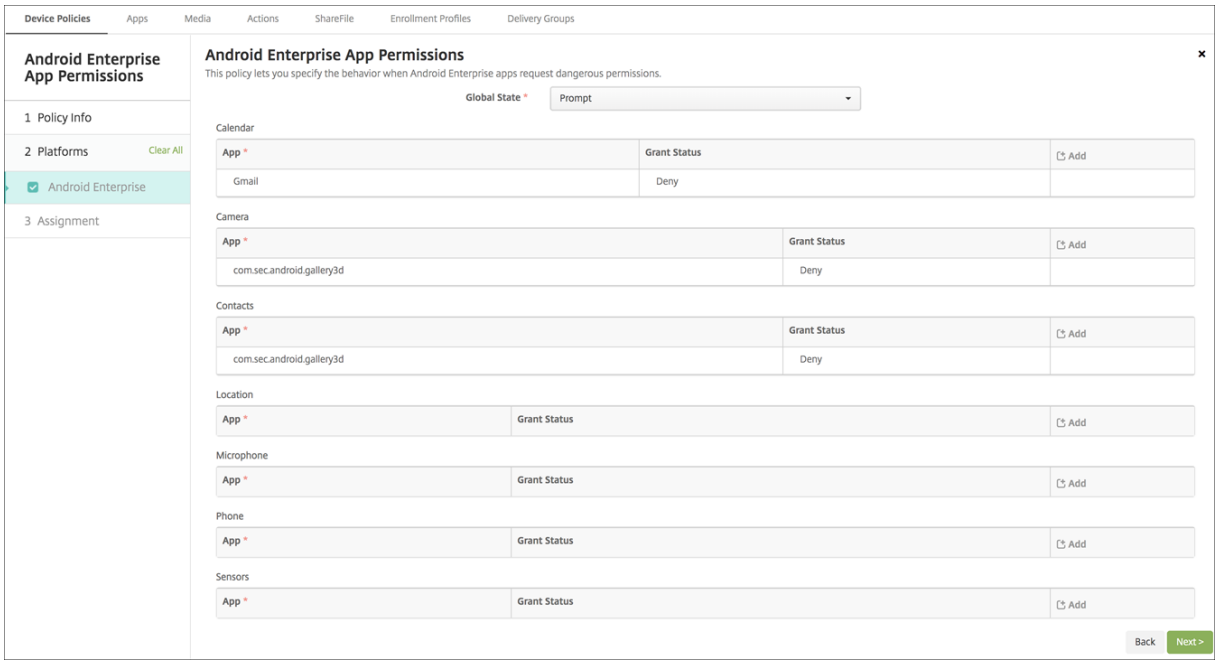
Sie können den Umgang mit Anforderungen für gefährliche Berechtigungen durch Konfigurieren eines globalen Status global steuern. Den Bereich für diese Konfiguration bilden die Android Enterprise-Apps in Arbeitsprofilen. Außerdem können Sie für jede App das Verhalten für einzelne Berechtigungsgruppen (gemäß Google-Definition) festlegen. Diese individuell festgelegten Einstellungen haben Vorrang vor dem globalen Status.

Weitere Informationen zur Google-Definition von Berechtigungsgruppen finden Sie im Android Developers Guide.

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 Gerätерichtlinien.

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**.

- Legen Sie für jede Berechtigungsgruppe und für jede App ein individuelles Verhalten fest. Um das Verhalten für eine Berechtigungsgruppe zu konfigurieren: Klicken Sie auf **Hinzufügen**. Wählen Sie 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 "Gewährungsstatus"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.

  > **Hinweis:**
  >
  > Für Geräte, die im **Profilbesitzermodus** registriert sind, gilt die Berechtigung **Gewähren** für Kamera, Standort, Mikrofon und Sensor nicht, wenn das Betriebssystem des Geräts Android 12 oder höher ist.

- **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 der App und "Gewährungsstatus"auf **Speichern**.
- Um der Berechtigungsgruppe weitere Apps hinzuzufügen, klicken Sie erneut auf **Hinzufügen** und wiederholen Sie die Schrittfolge.
- Nachdem Sie für die Berechtigungsgruppen **Gewährungsstatus** eingestellt haben, klicken Sie auf **Weiter**.

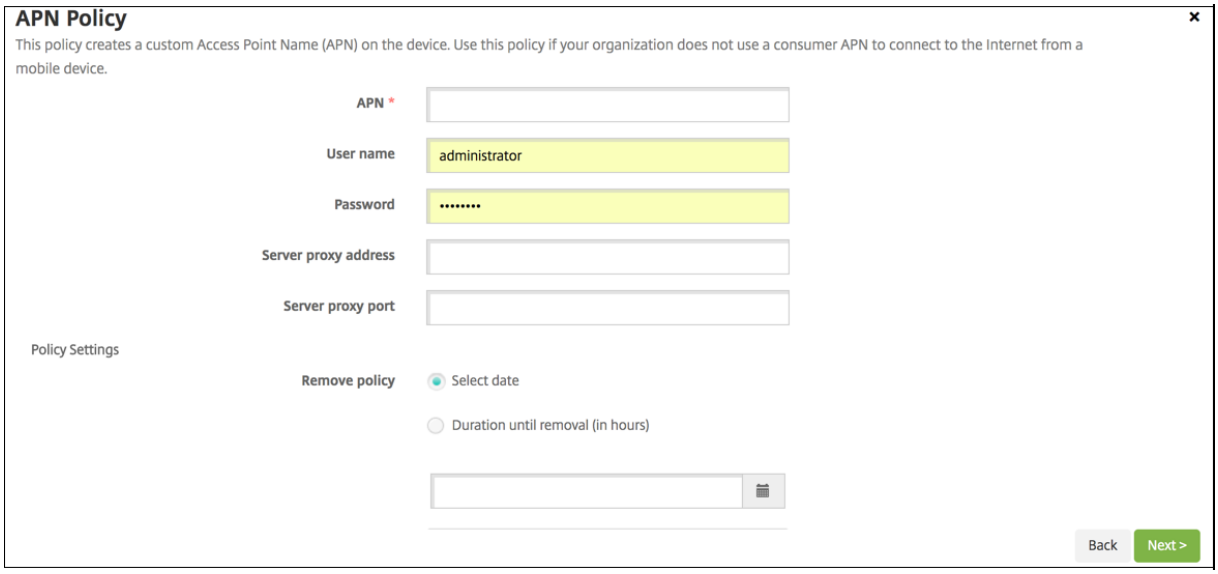
APN-Geräterichtlinie

December 10, 2021

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

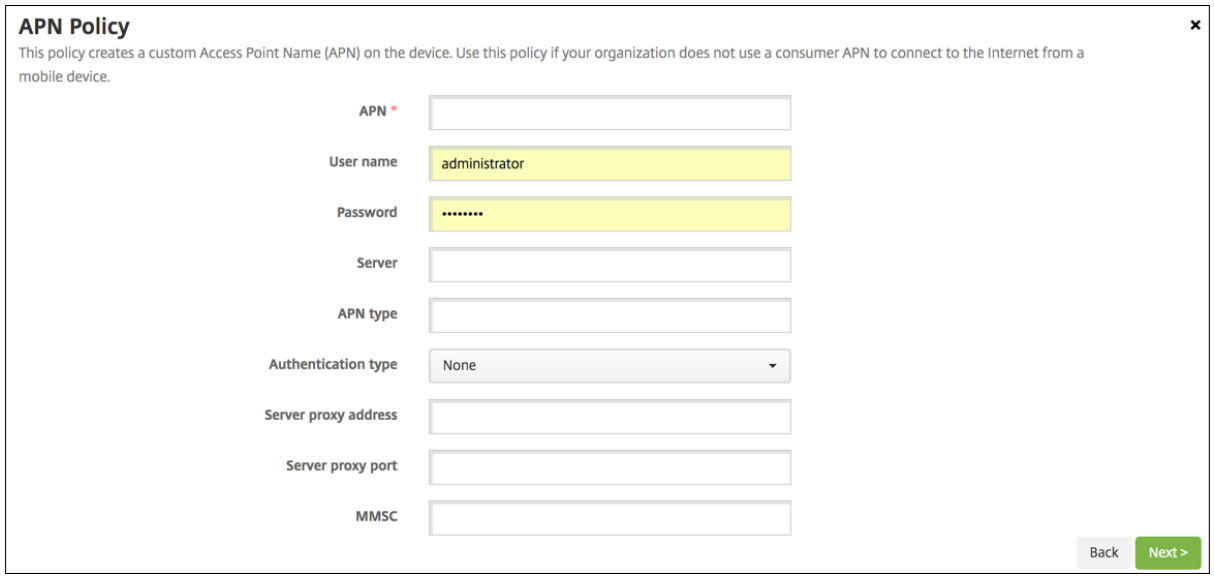
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



- **APN:** Geben Sie den Namen des Zugriffspunkts ein. Der Name muss mit einem akzeptierten iOS-Zugriffspunkt übereinstimmen, sonst funktioniert die Richtlinie nicht.
- **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. Die Portnummer 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.
  - Bei Auswahl von **Kennwort erforderlich** geben Sie das Kennwort 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 verfügbar ab iOS 6.0.

Android-Einstellungen



- **APN:** Geben Sie den Namen des Zugriffspunkts ein. Der Name muss mit einem akzeptierten Android-Zugriffspunkt übereinstimmen, sonst funktioniert die Richtlinie nicht.
- **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 ist.
- **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 wird selten verwendet.
  - `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. Der Port ist erforderlich, wenn Sie eine Serverproxyadresse eingegeben haben.
- **MMSC:** Die vom Netzbetreiber angegebene Adresse des MMS Gateway Servers.
- **MMS-Proxyadresse:** Die Adresse des Multimedia-Messaging-Dienstservers für MMS. MMS ist der Nachfolger von SMS und eignet sich für das Senden größerer Nachrichten mit Multimedia-inhalten z. B. Bilder oder Videos. Diese Server benötigen bestimmte Protokolle (z. B. MM1,… MM11).
- **MMS-Port:** Der Port des MMS-Proxyservers.

App-Zugriffsrichtlinie für Geräte

June 25, 2024

Mit der App-Zugriffsrichtlinie für Geräte können Sie eine Liste von Apps definieren, die installiert werden müssen, installiert werden können oder nicht installiert werden dürfen. Wenn die Apps auf einem Gerät dieser Richtlinie widersprechen, kennzeichnet Citrix Endpoint Management das Gerät als nicht richtlinientreu. Sie können dann eine automatisierte Aktion erstellen, wie darauf reagiert werden soll.

> **Wichtig:**
>
> Die App-Zugriffsrichtlinie für Geräte hindert einen Benutzer nicht daran, eine verbotene App zu installieren oder eine erforderliche App zu deinstallieren.

Sie können in einem Arbeitsgang nur eine Zugriffsrichtlinie konfigurieren. Jede App-Zugriffsrichtlinie enthält eine Liste erforderlicher, empfohlener oder verbotener Apps, jedoch keine Mischung aus verschiedenen Listen. Wählen Sie beim Erstellen einer Richtlinie für jeden Listentyp einen aussagekräftigen Namen, damit Sie wissen, welche Richtlinie für welche Liste von Apps gilt.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren** > **Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Einstellungen für iOS und Android (Legacy-Geräteadmin)

- **Zugriffsrichtlinie:** Wählen Sie den Listentyp aus, der für diese Richtlinie konfiguriert werden soll.
  - **Erforderlich:** Die App muss auf dem Gerät vorhanden sein. Ist die App nicht vorhanden, wird das Gerät als nicht richtlinientreu markiert. **Erforderlich** ist die Standardoption.

  - **Verboten:** Die App darf auf dem Gerät nicht vorhanden sein. Ist die App vorhanden, wird das Gerät als nicht richtlinientreu markiert.

- Hinzufügen einer oder mehrerer Apps zur Liste:

  1. Klicken Sie auf **Hinzufügen** und konfigurieren Sie Folgendes:
     - **App-Name:** Geben Sie einen App-Namen ein.
     - **App-ID:** Geben Sie optional eine App-ID ein.
  2. Klicken Sie auf **Speichern**.
  3. Wiederholen Sie diese Schritte für jede App, die Sie hinzufügen möchten.

Konfigurieren automatisierter Aktionen gemäß App-Zugriffsrichtlinie

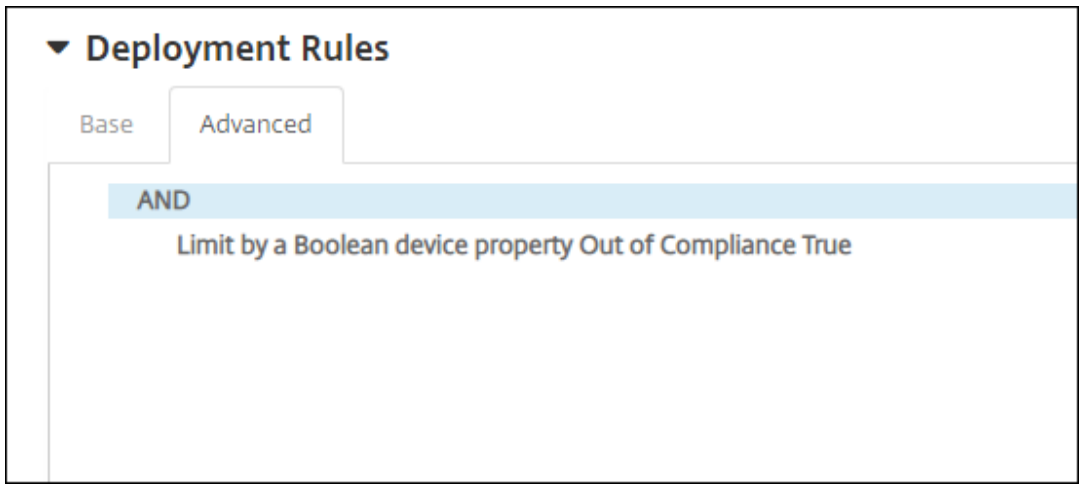
1. Fügen Sie eine App-Zugriffsrichtlinie hinzu, um Apps als erforderlich oder verboten festzulegen.
2. Konfigurieren Sie zwei automatisierte Aktionen basierend darauf, ob die betreffenden Apps erforderlich oder verboten sind:

   - Erforderlich
     - Markieren Sie ein Gerät als nicht richtlinientreu, wenn eine erforderliche App auf dem Gerät nicht vorhanden ist.
     - Markieren Sie ein Gerät als richtlinientreu, wenn die erforderliche App installiert ist.
   - Verboten
     - Markieren Sie ein Gerät als nicht richtlinientreu, wenn eine verbotene App auf dem Gerät vorhanden ist.
     - Markieren Sie ein Gerät als richtlinientreu, wenn die verbotene App nicht mehr installiert ist.

       Details über das Festlegen von automatisierten Aktionen finden Sie unter Automatisierte Aktionen.

3. Erstellen Sie eine Einschränkungsrichtlinie mit den Einstellungen, die Sie auf nicht richtlinientreuen Geräten implementieren möchten.

   a) Fügen Sie als Teil der Einschränkungsrichtlinie eine erweiterte Bereitstellungsregel mit den Optionen **Durch eine boolesche Geräteeigenschaft beschränken**, **Nicht richtlinientreu** und **Wahr** hinzu. Weitere Informationen finden Sie unter Geräteeinschränkungsrichtlinie.



4. Erstellen Sie eine Profilentfernungsrichtlinie, um die Einschränkungsrichtlinie zu entfernen, sobald das Gerät erneut richtlinientreu ist.
5. Fügen Sie eine erweiterte Bereitstellungsregel mit den Optionen **Durch eine boolesche Geräteeigenschaft beschränken**, **Nicht richtlinientreu** und **Wahr** hinzu. Siehe Geräterichtlinie für Profilentfernung.

Geräterichtlinie für App-Attribute

December 1, 2023

Mit der Geräterichtlinie für **App-Attribute** können Sie Attribute für Apps auf iOS-Geräten angeben. Durch Konfigurieren einer derartigen Richtlinie können Sie Folgendes erreichen:

- Zuweisen von Pro-App-VPNs zu Apps.
- Verhindern einer Deinstallation unternehmenskritischer Apps durch Benutzer. Gilt für iOS 14 und höher.
- Wenn das Feature "Zugeordnete Domänen"aktiviert ist, definieren Sie zugeordnete Domänen, die Apps hinzugefügt werden sollen. Gilt für iOS 13 und höher.

  Weitere Informationen finden Sie unter Zugeordnete Domänen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

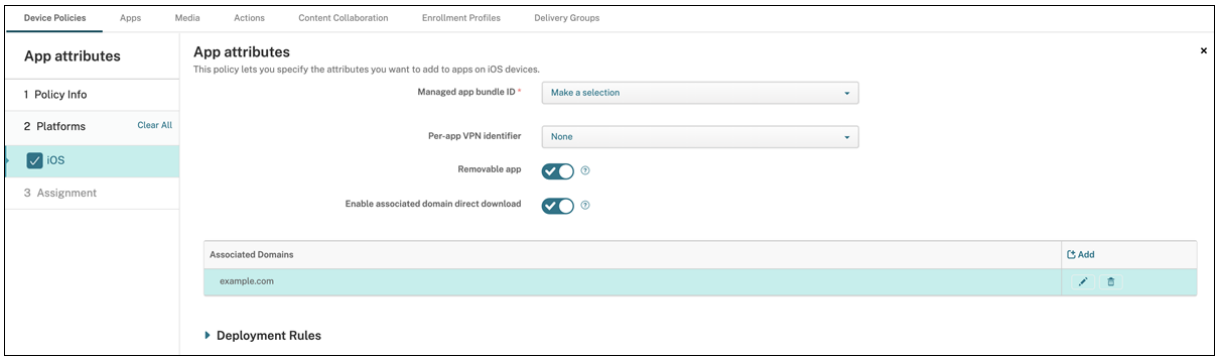
Zugeordnete Domänen

Zugeordnete Domänen ermöglichen eine sichere Zuordnung von Domänen zu Apps. Sie können dann Anmeldeinformationen freigeben oder Features in ihrer App über Ihre Websites bereitstellen. Wenn

dieses Feature aktiviert ist, können Sie beispielsweise Daten und Anmeldeinformationen zwischen Apps und Websites in Ihrer Organisation freigeben.

Weitere Informationen zum Aktivieren dieses Features finden Sie unter Supporting Associated Domains auf der Apple-Website.

iOS-Einstellungen



- **Paket-ID für verwaltete App:** Zum Angeben einer App gibt es folgende Methoden:
  - Wählen Sie die App-Paket-ID aus. Die Optionen sind erst verfügbar, wenn Sie die Geräterichtlinie **App-Bestand** aktivieren. Sie listet den App-Bestand auf verwalteten Geräten auf.
  - Wählen Sie **Hinzufügen** und geben Sie die App-Paket-ID ein.
    Informationen zum Ermitteln einer App-Paket-ID finden Sie unter Suche der Paket-ID für eine App im App Store.
- **ID für Pro-App-VPN:** (Optional) Wählen Sie ein Pro-App-VPN für diese App. Die Optionen umfassen die Pro-App-VPN-Verbindungen, die Sie auf der Seite **Geräterichtlinien > VPN-Richtlinie** konfiguriert haben.
  Weitere Informationen finden Sie unter Pro-App-VPN-Zugriff konfigurieren.
- **Entfernbare App:** (Optional) Geben Sie an, ob eine verwaltete App von Benutzern entfernt werden darf. Um zu verhindern, dass Benutzer die App deinstallieren, wählen Sie für diese Option die Einstellung **Aus**. Die Standardeinstellung ist **Ein**.
- **Direkten Download für zugeordnete Domäne aktivieren:** (Optional) Die Standardeinstellung ist **Ein**, d. h. die App führt die Überprüfung der beanspruchten Sitezuordnung direkt in der Domäne und nicht auf den Apple-Servern durch. Wählen Sie die Einstellung **Ein** nur für Domänen, die keinen Zugriff auf das Internet haben.
- **Zugeordnete Domänen:** (Optional) Zum Hinzufügen einer zugeordneten Domäne für die App klicken Sie auf **Hinzufügen** und geben dann den vollqualifizierten Domänennamen (FQDN) ein.

Suche der Paket-ID für eine App im App Store

1. Suchen Sie die App im App Store und kopieren Sie die Nummer am Ende der URL. Für die Citrix Workspace-App ist die App-ID beispielsweise die Ziffernfolge 363501921.
2. Wechseln Sie zu `https://itunes.apple.com/lookup?id=` und fügen Sie diese Nummer nach der URL ein. Eine TXT-Datei wird automatisch auf Ihren Computer heruntergeladen.
3. Suchen Sie in der TXT-Datei nach `bundleId` und erfassen Sie die Paket-ID der App. Die Paket-ID für die Citrix Workspace-App ist beispielsweise `com.citrix.ReceiveriPad`.

App-Konfigurationsrichtlinie für Geräte

June 25, 2024

Sie können Apps, die eine verwaltete Konfiguration unterstützen, remote konfigurieren, indem Sie Folgendes bereitstellen:

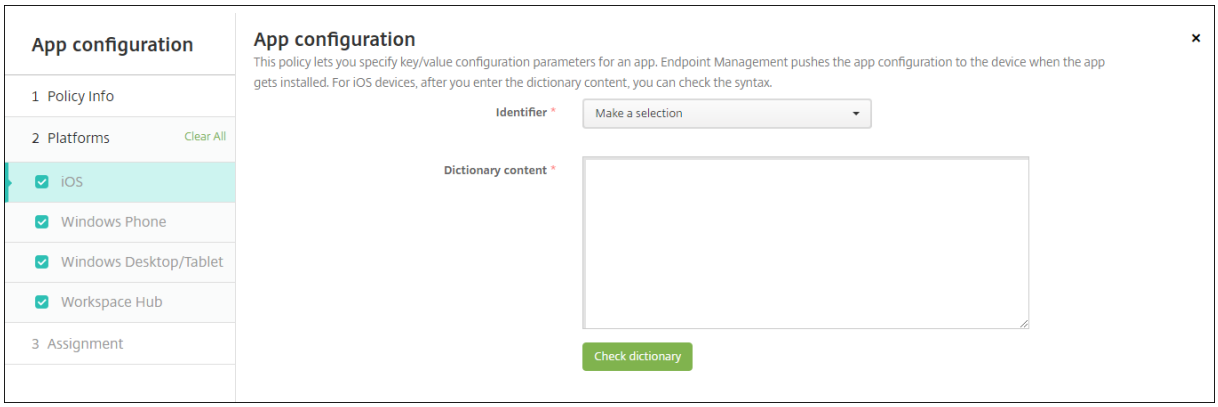
- Eine XML-Konfigurationsdatei (eine sogenannte Eigenschaftenliste oder `.plist`) auf iOS-Geräten
- Schlüssel/Wert-Paare auf Tablets, Desktops oder Telefonen mit Windows 10 oder Windows 11

Die Konfiguration legt mehrere Einstellungen und Verhaltensweisen der App fest. Citrix Endpoint Management 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.

> **Hinweis:**
>
> Die App-Konfigurationsvariablen werden von den jeweiligen Anwendungseigentümern definiert.
> App-Konfigurationsvariablen für Chrome werden beispielsweise von Chrome verwaltet und gepflegt. Weitere Informationen finden Sie unter App-Konfigurationsvariablen für Chrome.

iOS-Einstellungen



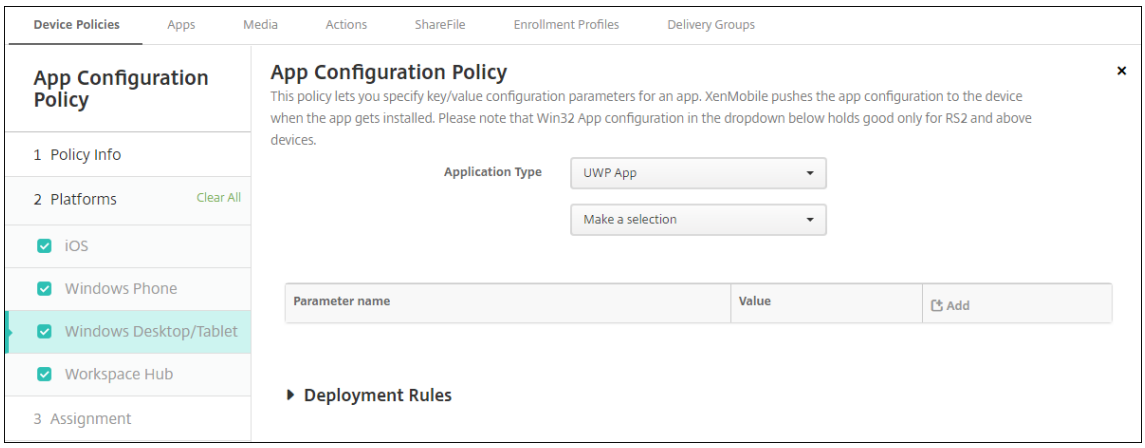
- **Bezeichner:** Klicken Sie in der Dropdownliste auf die gewünschte App oder auf **Hinzufügen**, um der Liste eine App hinzuzufügen.
  - Wenn Sie auf **Hinzufügen** klicken, geben Sie den App-Bezeichner in dem nun eingeblendeten Feld ein.
- **Wörterbuchinhalt:** Geben Sie die Konfigurationsinformationen der XML-Eigenschaftenliste (`.plist`) ein, bzw. kopieren Sie sie und fügen Sie ein.
- Klicken Sie auf **Wörterbuch prüfen**. Citrix Endpoint Management 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 Desktop/Tablet-Einstellungen

Sie können UWP-Apps (Universelle Windows-Plattform) oder Win 32-Apps konfigurieren. Konfigurieren Sie Win 32-Apps, um Microsoft ADMX-Richtlinieneinstellungen (Microsoft Administrative Template) zu importieren.

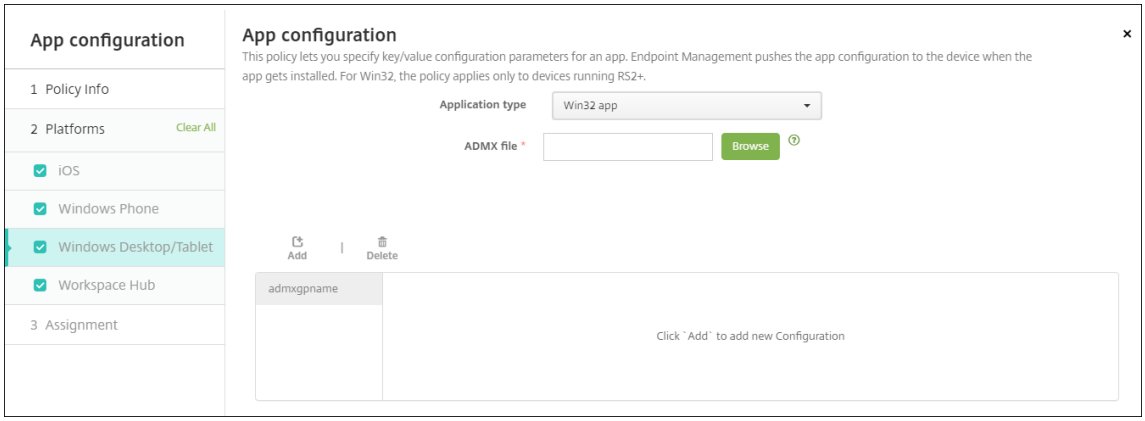
> **Hinweis:**
>
> Die Geräterichtlinie “App-Konfiguration”unterstützt externe ADMX-Dateien für Drittanbieteranwendungen wie Office. Nicht unterstützt werden Microsoft ADMX-Vorlagen für Windows, die im Betriebssystem als Gruppenrichtlinien unter `%SystemRoot%\PolicyDefinitions<!--NeedCopy-->` zur Verfügung gestellt werden.

- Bei Auswahl von **UWP-App**: Klicken Sie in der Liste **Auswählen** auf die App, die Sie konfigurieren möchten, oder auf **Hinzufügen**, um der Liste eine App hinzuzufügen.

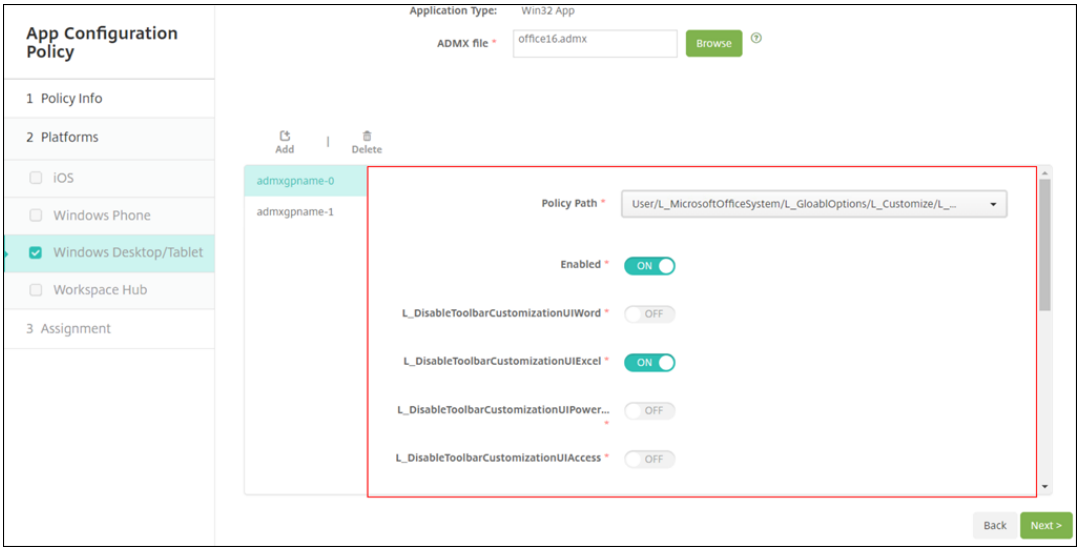


- Wenn Sie auf **Hinzufügen** geklickt haben, geben Sie den Paketfamiliennamen in dem nun eingeblendeten Feld ein.
- Für jeden Konfigurationsparameter, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Parametername:** Geben Sie den Schlüsselnamen 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.

- Bei Auswahl von **Win32-App**: Klicken Sie auf **Durchsuchen** und navigieren Sie zur ADMX-Datei, die Sie zum Konfigurieren der Richtlinie verwenden möchten.



- Klicken Sie auf **Hinzufügen**. Die Konfigurationsoptionen aus der ADMX-Datei werden rechts auf der Seite angezeigt.



- Wählen Sie einen Richtlinienpfad. Wenn Sie denselben Pfad mehrfach verwenden, wird die Konfiguration der aktuellen Version durchgesetzt.
- Legen Sie **Aktivieren** auf **Ein** fest.
- Geben Sie erforderliche Listenelementwerte als Schlüssel/Wert-Paare ein. Trennen Sie die einzelnen Schlüssel/Wert-Paare sowie Wert und Schlüssel innerhalb eines Paares mit der Textzeichenfolge **&#xF000**.
- Bei Elementwerten, die eine Dezimalzahl enthalten, sind möglicherweise nur Werte innerhalb eines bestimmten Bereichs zulässig.

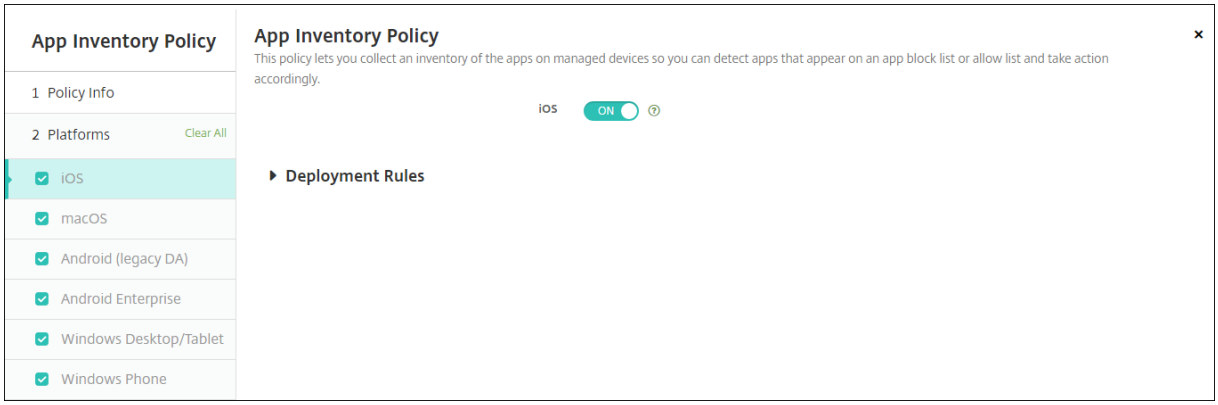
App-Bestandsrichtlinie für Geräte

June 25, 2024

Mit der App-Bestandsrichtlinie können Sie einen Bestand der Apps auf verwalteten Geräten abrufen. Citrix Endpoint Management 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. Verwenden Sie eine App-Zugriffsrichtlinie, um Positiv- oder Sperrlisten zu definieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS, macOS, Android (Legacy-Geräteadmin), Android Enterprise und Windows Desktop/Tablet



- Behalten Sie für jede ausgewählte Plattform den Standardwert bei oder klicken Sie auf **Aus**. Die Standardeinstellung ist **Ein**.

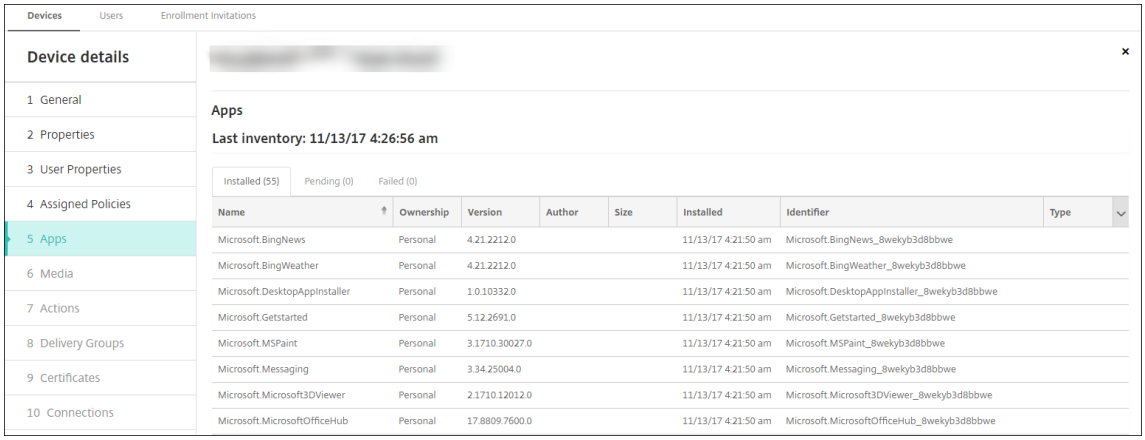
Bestandsaufnahme und Löschen von `Win32`-Apps

Sie können festlegen, ob die `Win32`-Apps auf Benutzergeräten Ihrer Geräterichtlinie für den App-Zugriff entsprechen. Zur Anzeige aller `Win32`-Apps auf verwalteten Desktop- und Tablet-Geräten mit Windows 10 und Windows 11:

1. Navigieren Sie zu **Konfigurieren > Geräterichtlinien** und fügen Sie für die Plattform **Windows Desktop/Tablet** eine App-Bestandsrichtlinie hinzu. Stellen Sie die Richtlinie bereit.
2. Gehen Sie zu **Verwalten > Geräte**, wählen Sie das gewünschte Windows 10- und Windows 11-Gerät aus, klicken Sie auf **Bearbeiten** und klicken Sie auf die Registerkarte **Apps**.

   Die Ergebnisse der Bestandsaufnahme werden angezeigt.

   > **Hinweis:**
   >
   > Wenn Sie ein Windows 11-Gerät konfigurieren, müssen Sie bis zu 24 Stunden auf genaue Ergebnisse der Bestandsaufnahme warten, wie von Microsoft vorgesehen.



3. Vergleichen Sie den App-Bestand mit der App-Zugriffsrichtlinie. Wenn gesperrte Apps auf dem Gerät installiert sind, können Sie diese vom Gerät löschen.

Probleme beim Installieren und Deinstallieren von Apps aufgrund eines fehlerhaften Produktcodes

Wenn eine `Win32`-App mit dem falschen Produktcode konfiguriert wurde, wird die App zwar installiert, der App-Status wird jedoch nicht von Microsoft an Citrix Endpoint Management übermittelt. Dies bewirkt Folgendes:

- Die App kann nicht mit der Geräterichtlinie zur App-Deinstallation deinstalliert werden.
- Citrix Endpoint Management stellt die App weiterhin bereit, da eine Bestätigung der App-Installation nicht erhalten wurde. Bei jeder Bereitstellung generiert das Gerät einen Fehlercode, da die App bereits installiert ist. Der unter **Verwalten > Gerät > Details zu Bereitstellungsgruppe** angezeigte Fehler lautet: `Msi Application received: Reporting: AppPush id:7z1701-x64.msi: Command execution failed -2147023293`

Korrektur des Produktcodes

1. Entfernen Sie die App manuell vom Gerät.
2. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Konfigurieren > Apps** und korrigieren Sie den Produktcode für die `Win32`-App.
3. Stellen Sie die `Win32`-App bereit.

Application Guard-Richtlinie

June 25, 2024

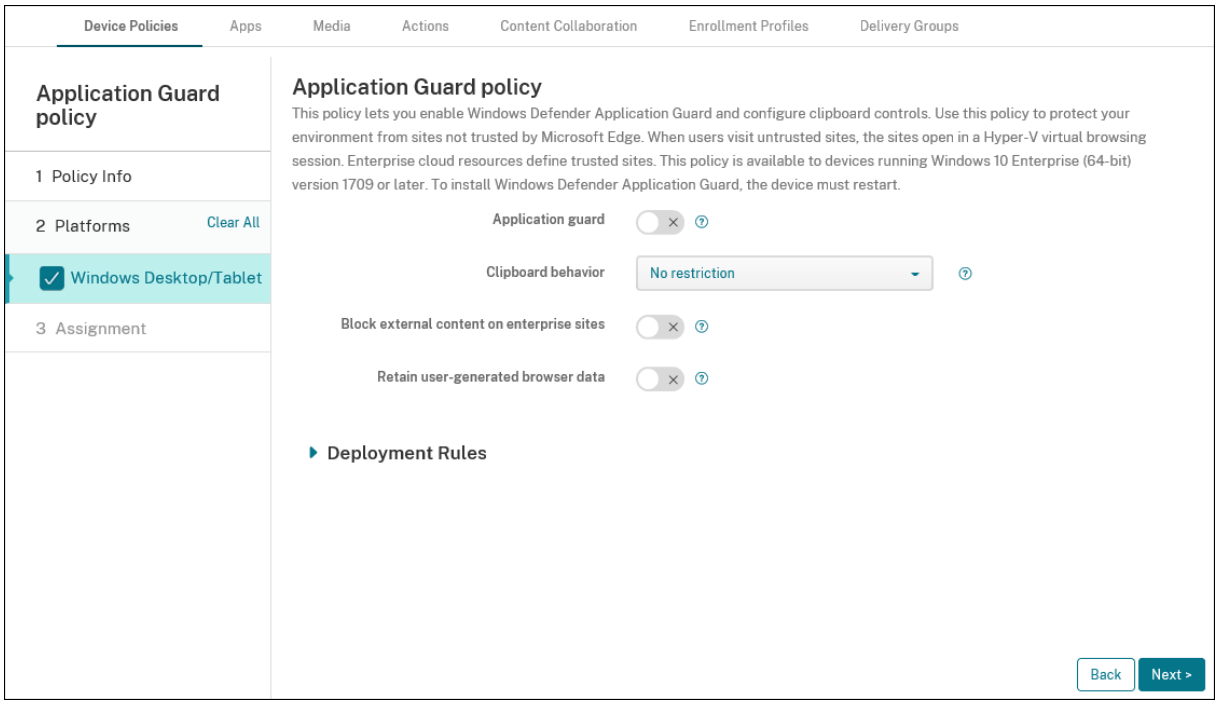
Über die Application Guard-Richtlinie werden Windows Defender Application Guard-Einstellungen festgelegt. Dazu gehören die Aktivierung/Deaktivierung von Application Guard und Steuerelementen für das Verhalten der Zwischenablage.

Windows Defender Application Guard schützt Ihre Umgebung vor Websites, die von Ihrer Organisation nicht als vertrauenswürdig definiert wurden. Wenn Benutzer Websites besuchen, die nicht in der isolierten Netzwerkgrenze aufgelistet sind, werden die Websites in einer virtuellen Browsersitzung in Hyper-V geöffnet. Vertrauenswürdige Sites werden durch Unternehmenscloudressourcen definiert.

Anforderungen

- Geräte mit Windows 10 Enterprise (64 Bit) oder Windows 11 Enterprise (64 Bit). Für die Installation von Windows Defender Application Guard ist ein Neustart des Geräts erforderlich.
- Microsoft Edge-Browser

Windows Desktop-/Tablet-Einstellungen



- **Application Guard:** Hiermit wird Application Guard aktiviert. Die Standardeinstellung ist **Aus**.
  - **Enterprise-Cloudressourcen:** Eine durch Kommas getrennte Liste von Unternehmenscloud-domänen.

- **Verhalten der Zwischenablage:** Steuert, ob und in welche Richtung Inhalte kopiert und eingefügt werden können. Die folgenden Optionen stehen zur Auswahl:
  - **Nicht konfiguriert**
  - **Kopieren und Einfügen nur vom Browser zum PC zulassen:** Benutzer können Inhalte nur vom Browser auf den PC kopieren und einfügen.
  - **Kopieren und Einfügen nur vom PC zum Browser zulassen:** Benutzer können Inhalte nur vom PC zum Browser kopieren und einfügen.
  - **Kopieren und Einfügen zwischen PC und Browser zulassen:** Benutzer können Inhalte frei zwischen PC und Browser kopieren und einfügen.
  - **Kopieren und Einfügen zwischen PC und Browser blockieren:** Benutzer können keine Inhalte zwischen PC und Browser kopieren und einfügen.
- **Inhalt der Zwischenablage:** Steuert, welche Inhalte von Benutzern kopiert und eingefügt werden können. Die folgenden Optionen stehen zur Auswahl:
  - **Keine Einschränkung**
  - **Kopieren von Text zulassen:** Benutzer können nur Text kopieren.
  - **Kopieren von Bildern zulassen:** Benutzer können nur Bilder kopieren.
  - **Kopieren von Text und Bildern zulassen:** Benutzer können Text und Bilder kopieren.
- **Externen Inhalt auf Unternehmenswebsites blockieren:** Mit **Ein** verhindert Windows Defender Application Guard, dass Inhalte von nicht genehmigten Sites auf Unternehmenssites geladen werden. Die Standardeinstellung ist **Aus**.
- **Benutzergenerierte Browserdaten beibehalten:** Mit **Ein** können Benutzerdaten gespeichert werden, die während einer virtuellen Browsersitzung von Application Guard erstellt wurden. Diese Daten umfassen Elemente wie Kennwörter, Favoriten und Cookies. Die Standardeinstellung ist **Aus**.

Geräterichtlinie zum Sperren von Apps

June 25, 2024

Die Geräterichtlinie zum Sperren von Apps definiert eine Liste von Apps, die:

- Auf Geräten ausgeführt werden dürfen.
- Auf Geräten blockiert werden.

Die genaue Funktionsweise der Richtlinie unterscheidet sich bei jeder unterstützten Plattform. Auf einem iOS-Gerät können Sie beispielsweise nicht mehrere Apps blockieren.

Auf iOS-Geräten können Sie auch nur eine iOS-App pro Richtlinie auswählen. Benutzer können ihr Gerät dann nur zum Ausführen einer einzigen App verwenden. Außer den Optionen, die ausdrücklich zulässig sind, wenn die Geräterichtlinie für die App-Sperre erzwungen wird, können sie keine anderen Aktivitäten auf dem Gerät ausführen.

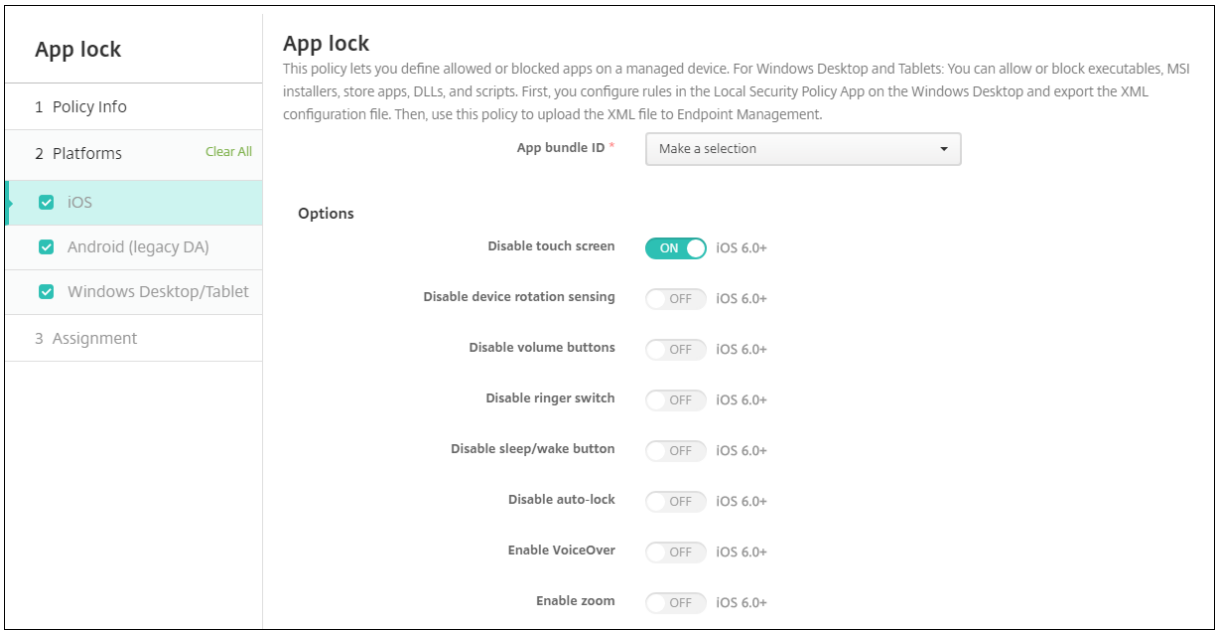
Außerdem müssen die iOS-Geräte beaufsichtigt werden, um die App-Sperrrichtlinien durchzusetzen.

Die Geräterichtlinie funktioniert auf den meisten Android L- und M-Geräten, jedoch nicht auf Android N- oder neueren Geräten. Dies liegt daran, dass Google die erforderliche API nicht mehr bereitstellt.

Für verwaltete Windows-Desktops und -Tablets können Sie eine Geräterichtlinie für die App-Sperre erstellen, in der zugelassene und gesperrte Apps aufgelistet sind. Sie können ausführbare Dateien, MSI-Installationsprogramme, Store-Apps, DLLs und Skripts zulassen oder sperren.

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 Dropdownliste auf die App, auf die die Richtlinie angewendet werden soll, oder klicken Sie 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:** 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
  - Sprachsteuerung aktivieren

- **Benutzeraktivierte Optionen:** Der Standardwert aller Optionen ist **AUS**.
  - Anpassen von VoiceOver zulassen
  - Anpassen von Zoom zulassen
  - Anpassen von Farbumkehrung zulassen
  - Anpassen von AssistiveTouch zulassen
  - Anpassen der Sprachsteuerung 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 verfügbar ab iOS 6.0.

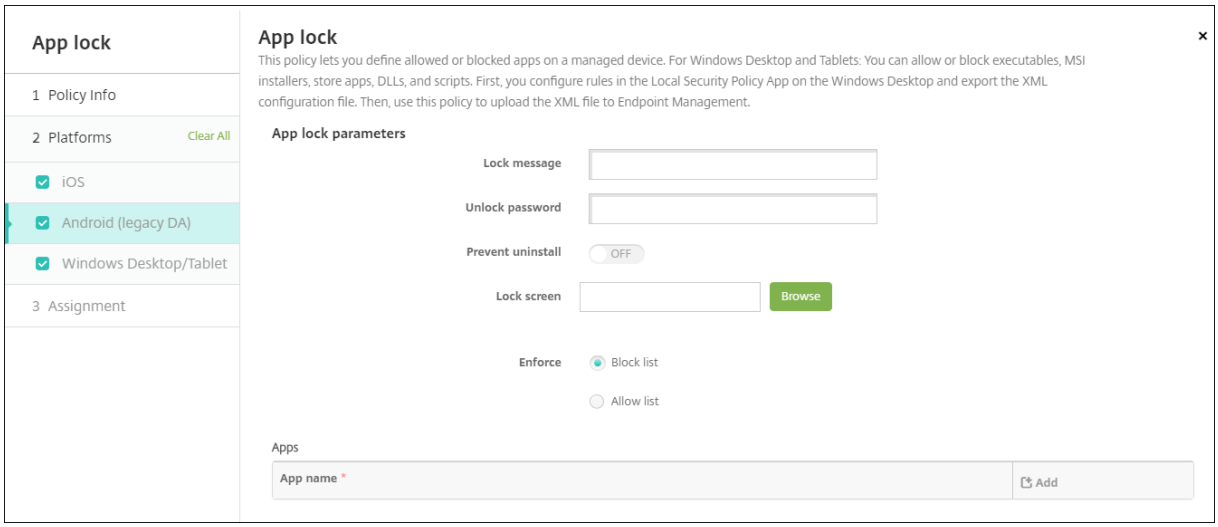
Konfigurieren eines iPads als Kiosk

Sie können die Geräterichtlinie für die App-Sperre verwenden, um ein betreutes iPad als Kiosk auszuführen. Apple bezeichnet diese Funktion als Einzelappmodus. Weitere Informationen zu diesem Feature finden Sie in der Dokumentation von Apple. Stellen Sie sicher, dass Sie die auszuführende App vor der Richtlinie bereitstellen.

1. Navigieren Sie zu **Konfigurieren > Geräterichtlinien** und klicken Sie auf **Hinzufügen**.
2. Wählen Sie die Richtlinie **App-Sperre**.
3. Geben Sie einen **Richtliniennamen** und optional eine **Beschreibung** ein.
4. Wählen Sie nur die **iOS-Plattform** aus.
5. Wählen Sie unter **App-Paket-ID** die App aus, die auf dem iPad ausgeführt werden soll.
6. Konfigurieren Sie die gewünschten Optionen, wie zuvor beschrieben, und speichern Sie die Richtlinie.
7. Fügen Sie die Richtlinie derselben Bereitstellungsgruppe wie Ihr iPad hinzu, und stellen Sie die Richtlinie bereit.

Einstellungen für Android (Legacy-Geräteadministrator)

> **Hinweis:**
>
> Sie können die App für Android-Einstellungen nicht über die Geräterichtlinie zum Sperren von Apps blockieren.

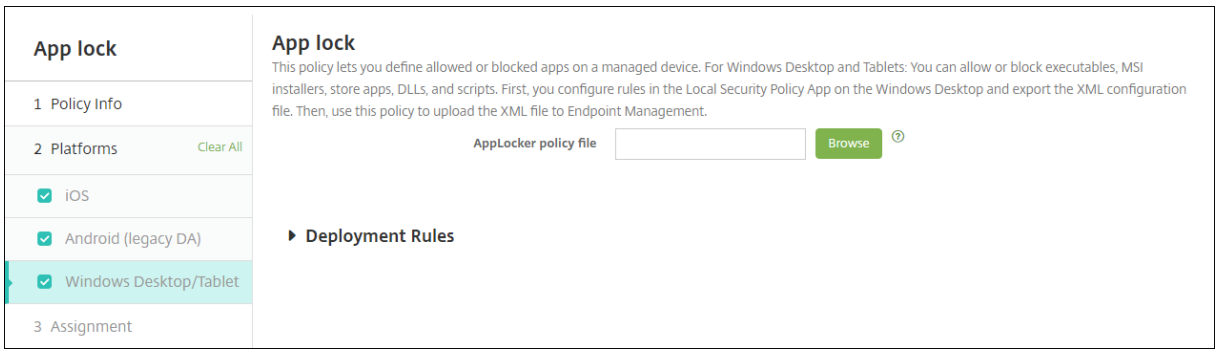


- **Parameter für App-Sperre**
  - **Sperrmeldung:** Geben Sie eine Meldung ein, die angezeigt wird, wenn ein Benutzer versucht, eine gesperrte App zu öffnen.
  - **Entsperrkennwort:** Geben Sie das Kennwort zum Entsperren der App ein.
  - **Deinstallation verhindern:** Wählen Sie aus, ob eine Deinstallation 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 Apps aufzulisten, die auf Geräten nicht ausgeführt werden dürfen. Klicken Sie auf **Positivliste**, um Apps aufzulisten, die auf Geräten

ausgeführt werden dürfen.

- **Apps:** Klicken Sie auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name:** Klicken Sie in der Dropdownliste auf den Namen der App, die Sie zur Positivliste oder Sperrliste hinzufügen möchten. Alternativ können Sie auf **Hinzufügen** klicken, um eine App in die Liste aufzunehmen.
  - 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.

Windows Desktop-/Tablet-Einstellungen



Voraussetzungen für die App-Sperre

- Konfigurieren Sie Regeln im Editor für lokale Sicherheitsrichtlinien auf einem Windows 10- oder Windows 11-Desktop.
- Exportieren Sie die Richtlinien-XML-Datei. Citrix empfiehlt die Erstellung von Standardregeln in Windows, um eine Sperrung der Standardkonfiguration und Probleme auf Geräten zu verhindern.
- Laden Sie die XML-Datei anschließend über die Geräterichtlinie zum Sperren von Apps in Citrix Endpoint Management hoch. Weitere Informationen zum Erstellen von Regeln finden Sie in diesem Microsoft-Artikel: https://docs.microsoft.com/en-us/windows/security/threat-protection/applocker/applocker-overview

Konfigurieren und Exportieren der Richtlinien-XML-Datei aus Windows

> **Wichtig:**
>
> Verwenden Sie beim Konfigurieren der Richtlinien-XML-Datei über den Windows-Richtlinieneditor den Modus "Nur überwachen".

1. Starten Sie auf dem Windows-Computer den **Editor für lokale Sicherheitsrichtlinien**. Klicken Sie auf **Start**, geben Sie **Lokale Sicherheitsrichtlinie** ein und klicken Sie dann auf **Lokale Sicherheitsrichtlinie**.
2. Erweitern Sie in der Konsolenstruktur **Anwendungssteuerungsrichtlinien**.
3. Klicken Sie auf **AppLocker** und klicken Sie dann im mittleren Bereich auf **Regelerzwingung konfigurieren**.
4. Wählen Sie **Konfiguriert** und dann **Regeln erzwingen**. Wenn Sie eine Regel aktivieren, ist **Regeln erzwingen** die Standardeinstellung.
5. Klicken Sie mit der rechten Maustaste auf **AppLocker**, klicken Sie auf **Richtlinie exportieren** und speichern Sie die XML-Datei.

> **Hinweis:**
>
> Sie können **Regeln für ausführbare Dateien**, **Windows Installer-Regeln**, **Skriptregeln** und **App-Paketregeln** erstellen. Klicken Sie dazu mit der rechten Maustaste auf den jeweiligen Ordner und dann auf **Neue Regel erstellen**.

Importieren der XML-Richtliniendatei in Citrix Endpoint Management

Erstellen Sie eine App-Sperrrichtlinie. Klicken Sie neben der Einstellung der **App-Sperrrichtliniendatei** auf **Durchsuchen**, und navigieren Sie zur XML-Datei.

Beenden der Anwendung einer App-Sperrrichtlinie

Nach dem Bereitstellen einer App-Sperrrichtlinie in Citrix Endpoint Management: Wenn die App-Sperrrichtlinie nicht mehr angewendet werden soll, erstellen Sie eine leere XML-Datei. Erstellen Sie anschließend eine weitere App-Sperrrichtlinie, laden Sie die Datei hoch und stellen Sie die Richtlinie bereit. Geräte, für die eine App-Sperre aktiviert ist, sind nicht betroffen. Geräte, die die Richtlinie zum ersten Mal erhalten, verfügen nicht über die App-Sperrrichtlinie.

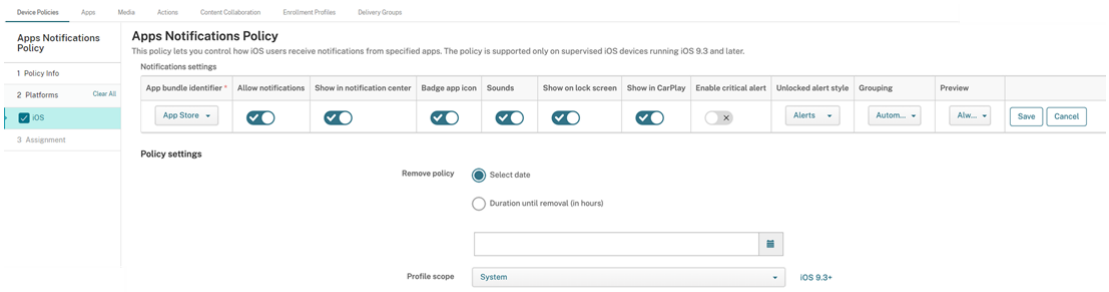
Geräterichtlinie für App-Benachrichtigungen

June 25, 2024

Mit der App-Benachrichtigungsrichtlinie können Sie steuern, wie iOS-Benutzer Benachrichtigungen von bestimmten Apps erhalten. Die Richtlinie wird nur für betreute iOS-Geräte mit iOS 9.3 oder höher unterstützt.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Gerätерichtlinien.

iOS-Einstellungen



- **App-Paket-ID:** Geben Sie die App an, deren Benachrichtigungseinstellungen Sie verwalten möchten:
  - Wählen Sie die App-Paket-ID aus. Die Optionen sind erst verfügbar, wenn Sie die Geräterichtlinie **App-Bestand** aktivieren. Sie listet den App-Bestand auf verwalteten Geräten auf.
  - Wählen Sie **Hinzufügen** und geben Sie die App-Paket-ID ein.
    Informationen zum Ermitteln einer App-Paket-ID finden Sie unter Suche der Paket-ID für eine App im App Store.
- **Benachrichtigungen zulassen:** Wählen Sie **Ein**, um Benachrichtigungen zuzulassen.
- **In Mitteilungszentrale anzeigen:** Wählen Sie **Ein**, um Benachrichtigungen in der Mitteilungszentrale der Benutzergeräte 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**, um Benachrichtigungen in Apple CarPlay anzuzeigen. Gilt für iOS 12 und höher. Die Standardeinstellung ist **Ein**.
- **Kritische Warnung aktivieren:** Wählen Sie **Ein**, damit eine App eine Benachrichtigung als kritisch markieren und damit die Einstellungen für “Nicht stören”und “Klingel”ignorieren kann. Gilt für iOS 12 und höher. Die Standardeinstellung ist **Aus**.
- **Hinweisstil (entsperrt):** Wählen Sie **Keine**, **Banner** oder **Warnungen**, um das Erscheinungsbild von Hinweisen bei entsperrtem Gerät zu konfigurieren.

- **Vorschau:** Wählen Sie aus, wie eine Benachrichtigungsvorschau für die App angezeigt wird. Gilt für iOS 14 und höher.
  - **Immer:** Eine Benachrichtigungsvorschau wird angezeigt, wenn das Gerät gesperrt oder entsperrt ist.
  - **Wenn entsperrt:** Eine Benachrichtigungsvorschau wird nur angezeigt, wenn das Gerät entsperrt ist.
  - **Nie:** Um die Benachrichtigungsvorschauen auf dem Gerät zu löschen.
- **Gruppierung:** Wählen Sie aus, wie App-Benachrichtigungen auf dem Gerät gruppiert werden. Gilt für Geräte mit iOS 12 und höher.
  - **Automatisch:** Die App legt fest, wie Benachrichtigungen gruppiert werden.
  - **Nach App:** Benachrichtigungen werden nach App gruppiert.
  - **Aus:** Das Gruppieren von Benachrichtigungen wird für die App deaktiviert. Geräte zeigen alle Benachrichtigungen nacheinander an.
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Folgende Optionen sind verfügbar:
    - **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. Gilt für iOS 6.0 oder höher.
  - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob diese Richtlinie für einen **Benutzer** oder ein ganzes **System** gilt. Die Standardeinstellung ist **Benutzer**. Gilt für iOS 9.3 und höher.

App-Deinstallationsrichtlinie

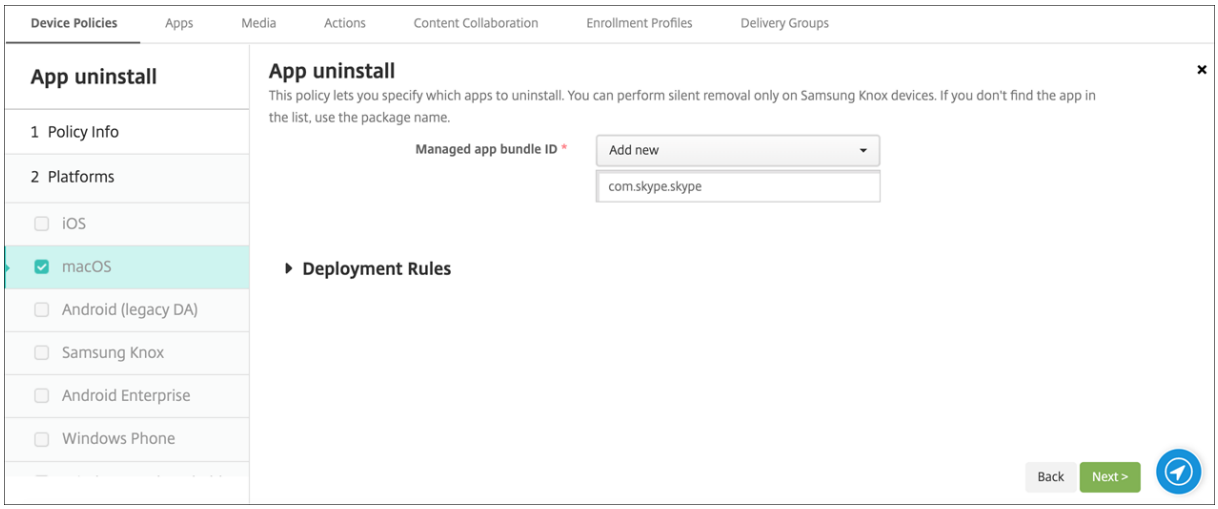
June 25, 2024

Mit der App-Deinstallationsrichtlinie können Sie Apps von Benutzergeräten entfernen. Sie entfernen eine App beispielsweise, wenn Sie sie nicht mehr unterstützen oder durch eine ähnliche App eines anderen Anbieters ersetzen möchten.

Wenn diese Richtlinie auf Benutzergeräten bereitgestellt wird, werden Benutzer aufgefordert, die App zu deinstallieren. Anschließend wird die App entfernt.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS- und macOS-Einstellungen



- **Paket-ID für verwaltete App:** Wählen Sie in der Liste eine vorhandene verwaltete App oder **Hinzufügen** aus. Wenn keine Apps für diese Plattform konfiguriert sind, ist die Liste leer und Sie müssen eine neue verwaltete App hinzufügen. Wenn Sie **Hinzufügen** auswählen, wird ein Feld zur Eingabe eines Namens für die verwaltete App angezeigt. Verfügbar für iOS 5.0 und höher und macOS 11.0 und höher.

Einstellungen für Android (Legacy-Geräteadmin), Android Enterprise und Windows Desktop/Tablet

- **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 Dropdownliste 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.

Aktivieren Sie für Android Enterprise-Apps auch die App-Bestandsrichtlinie. Siehe App-Bestandsrichtlinie für Geräte.

Automatische Deinstallation einer Unternehmensapp nach Installation der entsprechenden App aus dem öffentlichen App-Store

Sie können Citrix Endpoint Management so konfigurieren, dass die Unternehmensversion von Citrix-Apps bei der Installation der Version aus dem öffentlichen App-Store entfernt wird. Durch dieses Fea-

ture wird verhindert, 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 Citrix Endpoint Management, ältere Apps bei der Installation der neuen Version von Benutzergeräten zu entfernen. Dieses Feature ist nur für verwaltete iOS-Geräte verfügbar, die mit einem Citrix Endpoint Management-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 Citrix Endpoint Management 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

June 25, 2024

Sie können vorgeben, welche Apps Benutzer von einem Amazon-Gerät deinstallieren dürfen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Amazon-Einstellungen

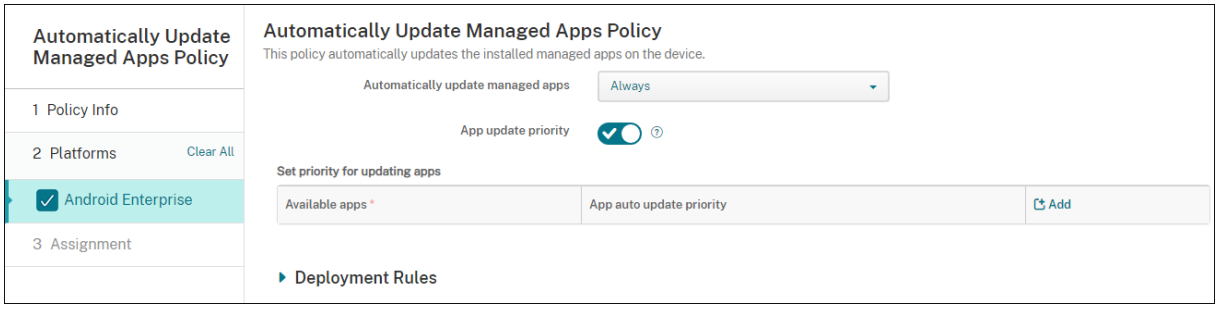
- **Einstellungen zum Einschränken der App-Deinstallation:** Klicken Sie für jede Regel, die Sie hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name:** Klicken Sie in der Dropdownliste auf eine App oder auf **Neu hinzufügen**, um eine App hinzuzufügen.
  - **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

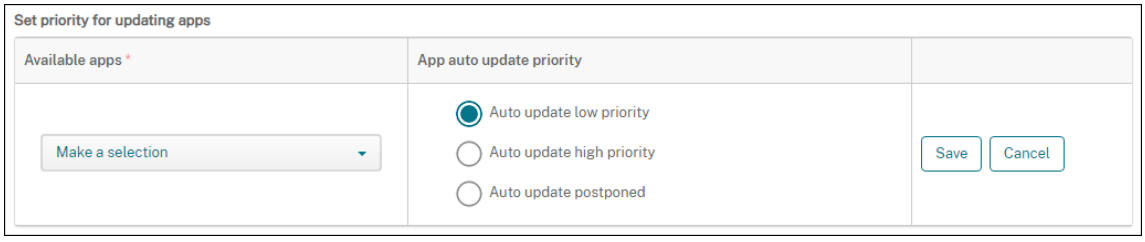
May 3, 2022

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.



- **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.
- **App-Updatepriorität:** Bei Auswahl von **Ein** können Sie für jede verwaltete App eine Updateprioritätsstufe konfigurieren.
- **Priorität für die Aktualisierung von Apps festlegen:** Klicken Sie auf **Hinzufügen**, um die Updatepriorität für eine App zu konfigurieren.



  - **Verfügbare Apps:** Wählen Sie im Menü eine App aus, für die Sie eine Updatepriorität konfigurieren möchten.

- **Priorität für automatische App-Updates:** Wählen Sie eine Option für die Updatepriorität aus:
  * **Autom. Update mit niedriger Priorität:** Die App wird aktualisiert, wenn das Gerät lädt, nicht aktiv genutzt wird und mit einem Netzwerk ohne Datenlimit verbunden ist.
  * **Autom. Update mit hoher Priorität:** Die App wird so bald wie möglich und ohne Einschränkungen aktualisiert.
  * **Autom. Update verschoben:** Die App wird bis zu 90 Tage lang nicht automatisch aktualisiert, nachdem eine neue Version verfügbar ist. Nach 90 Tagen wird die App automatisch mit niedriger Priorität aktualisiert. Nach dem App-Update wird die App für weitere 90 Tage nicht automatisch aktualisiert. Der Benutzer kann die App jederzeit manuell aktualisieren.
- Klicken Sie abschließend auf **Save**. Um eine Konfiguration zu bearbeiten, klicken Sie auf das Bleistiftsymbol. Um eine Konfiguration zu löschen, klicken Sie auf den Papierkorb.

BitLocker-Geräterichtlinie

December 1, 2023

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 Citrix Endpoint Management konfigurieren Sie die Einstellungen im BitLocker-Assistenten auf Windows 10- und Windows 11-Geräten. Auf einem Gerät mit aktiviertem BitLocker kann der Benutzer beispielsweise Folgendes auswählen:

- Art und Weise der Entsperrung seines Laufwerks beim Start
- Art und Weise der Sicherung des Wiederherstellungsschlüssels
- Art und Weise der Entsperrung eines Festplattenlaufwerks

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.

- ein verschlüsselter BitLocker-Wiederherstellungsschlüssel sicher gespeichert werden soll, auf den Benutzer im Fall des Verlusts zugreifen können. Den Schlüssel finden sie im Selbsthilfeportal.

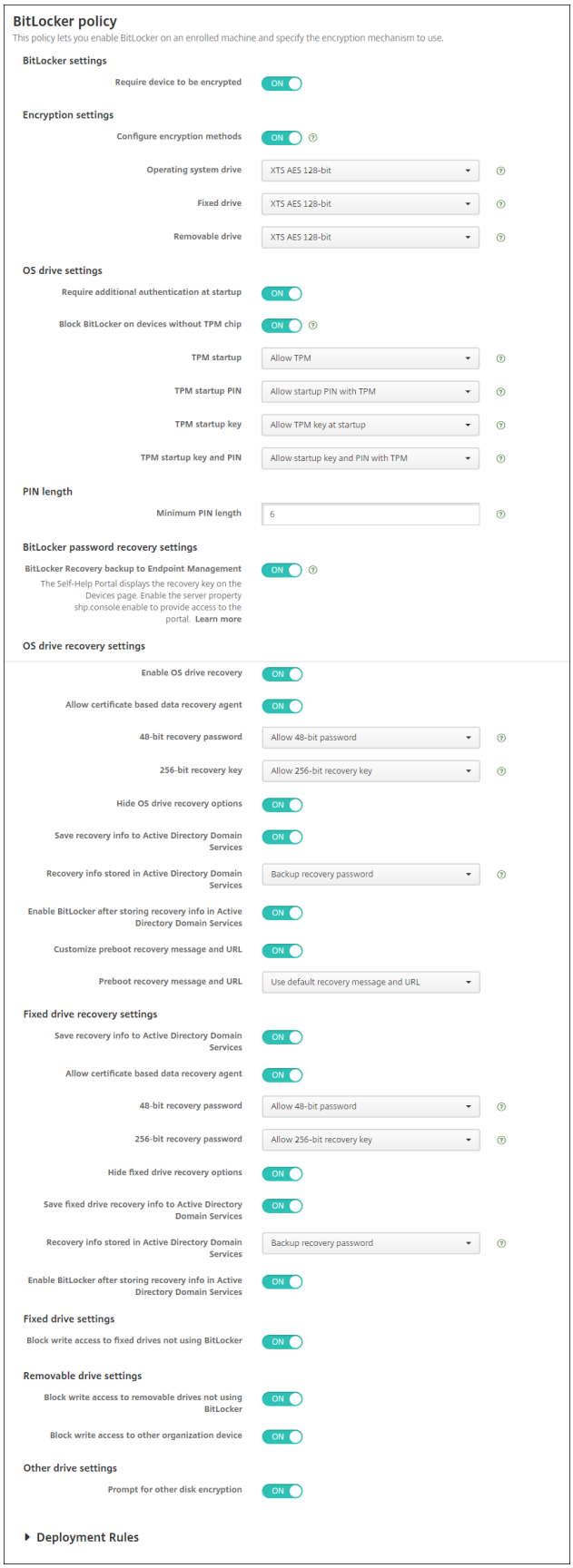
> Hinweis
>
> Nachdem die BitLocker-Verschlüsselung auf einem Gerät gestartet wurde, können Sie die BitLocker-Einstellungen auf dem Gerät nicht mehr ändern, indem Sie eine aktualisierte BitLocker-Geräterichtlinie bereitstellen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Anforderungen

- Die BitLocker-Geräterichtlinie erfordert Windows 10 Enterprise oder Windows 11 Enterprise Edition.
- Bereiten Sie vor der Bereitstellung der BitLocker-Geräterichtlinie Ihre Umgebung für die Verwendung von BitLocker vor. Ausführliche Informationen von Microsoft, darunter zu Systemanforderungen und zum Einrichten von BitLocker, finden Sie in den Artikeln unter BitLocker.

Windows Desktop-/Tablet-Einstellungen



- **BitLocker-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**.
- **Verschlüsselungseinstellungen**
  - **Verschlüsselungsmethoden konfigurieren:** legt die Verschlüsselungsmethoden für spezifische Laufwerktypen fest. Bei Auswahl von **Aus** fordert der BitLocker-Assistent den Gerätebenutzer 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**.
- **OS-Laufwerkseinstellungen**
  - **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 gesonderten 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. Andernfalls wechselt das Gerät in den Wiederherstellungsmodus.

- **PIN-Länge**
  - **PIN-Mindestlänge:** die Mindestlänge der TPM-Start-PIN. Der Standardwert ist **6**.
- **BitLocker-Kennwortwiederherstellungseinstellungen**
  - **BitLocker-Wiederherstellungsbackup auf Citrix Endpoint Management:** Wenn diese Option aktiviert ist, können Benutzer, die ihre Geräte entsperren müssen, ihren BitLocker-Wiederherstellungsschlüssel im Selbsthilfeportal finden. Der Citrix Endpoint Management-Administrator kann den BitLocker-Wiederherstellungsschlüssel von Benutzern nicht sehen. Weitere Informationen zum Anzeigen des BitLocker-Wiederherstellungsschlüssels finden Sie unter BitLocker-Wiederherstellungsschlüssel.
- **Einstellungen für OS-Laufwerkswiederherstellung:** konfiguriert die Wiederherstellungsoptionen für Benutzer eines mit BitLocker verschlüsselten OS-Laufwerks.
  - **OS-Laufwerkswiederherstellung aktivieren:** 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:** 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. Die Standardeinstellung ist **48-Bit-Kennwort zulassen**.
- **256-Bit-Wiederherstellungsschlüssel:** 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**.
- **Wiederherstellungsinformationen in den Active Directory-Domänendiensten speichern:** gibt an, ob die Wiederherstellungsoptionen in Active Directory-Domänendiensten gespeichert werden sollen. Die Standardeinstellung ist **Aus**.
- **Wiederherstellungsinformationen in den Active Directory-Domänendiensten gespeichert:** gibt an, ob das BitLocker-Wiederherstellungskennwort bzw. das Wiederherstellungskennwort und Schlüsselpaket in Active Directory-Domänendiensten gespeichert werden sollen. Das Speichern des Schlüsselpakets unterstützt die Wiederherstellung von Daten von einem physisch beschädigten Laufwerk. Standardwert ist **Wiederherstellungskennwort sichern**.
- **Aktivieren Sie BitLocker nach dem Speichern der Wiederherstellungsinformationen in den Active Directory-Domänendiensten:** gibt an, ob Benutzer daran gehindert werden sollen, BitLocker zu aktivieren, wenn ihr Gerät nicht mit der Domäne verbunden ist und das Backup 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**.
- **Wiederherstellungsmeldung und -URL vor dem Start:** 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**, **Benutzerdefinierte Wiederherstellungs-URL verwenden** und **Citrix Endpoint Management-Wiederherstellungsnachricht und -URL verwenden**. Bei Auswahl von **Aus** werden die Standardwiederherstellungsmeldung und -URL angezeigt. Die Standardeinstellung ist **Aus**.

- **Einstellungen für Festplattenlaufwerkswiederherstellung:** 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**.
- **Festplattenlaufwerkseinstellungen**
  - **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**.
- **Wechseldatenträgereinstellungen**
- **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**.
- **Schreibzugriff auf andere Unternehmensgeräte blockieren:** Wenn diese Option auf **Ein** festgelegt ist, haben Benutzer keinen Schreibzugriff auf andere Geräte in der Organisation (z. B. Netzlaufwerke).
- **Andere Laufwerkseinstellungen**
- **Eingabeaufforderung für andere Festplattenverschlüsselung:** ermöglicht das Deaktivieren der Warnungsaufforderung für andere Datenträgerverschlüsselungen auf Geräten. Die Standardeinstellung ist **Aus**.

Bluetooth-Geräterichtlinie

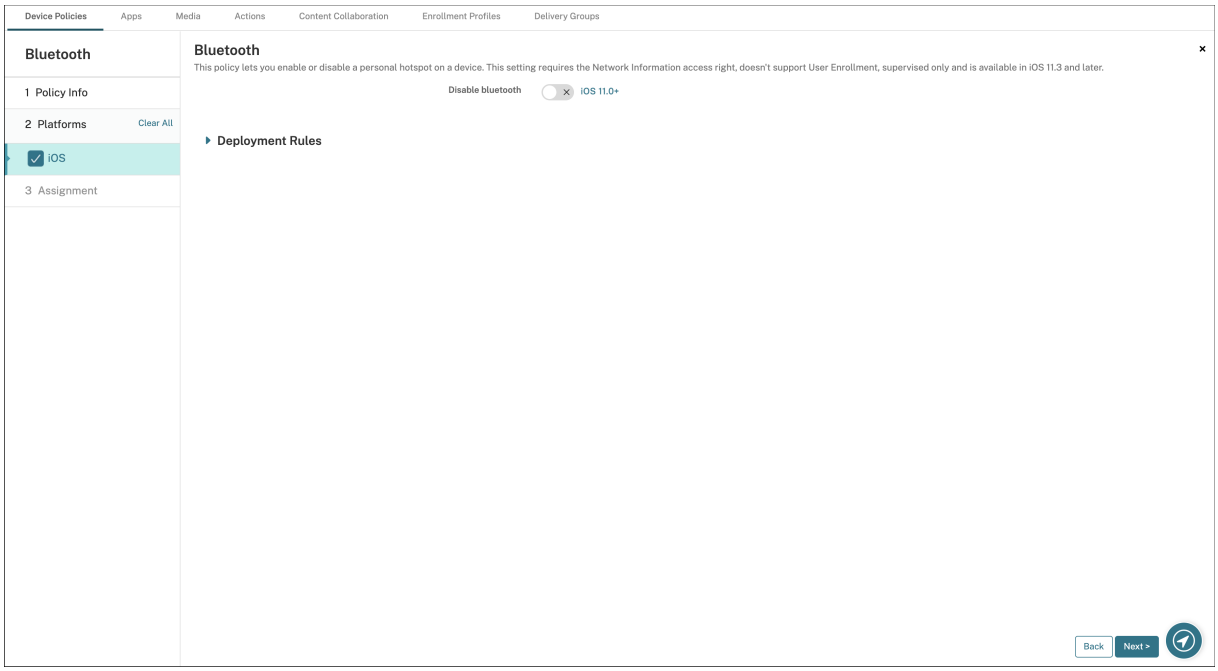
December 10, 2021

Sie können auf betreuten iOS-Geräten eine Bluetooth-Richtlinie konfigurieren, um Bluetooth zu aktivieren oder zu deaktivieren.

Für diese Einstellung ist das Zugriffsrecht für Netzwerkinformationen erforderlich. Die Benutzerregistrierung wird nicht unterstützt und die Einstellung ist ab iOS 11.3 verfügbar.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



- **Bluetooth deaktivieren:** Ermöglicht das Deaktivieren oder Aktivieren von Bluetooth auf dem betreuten Gerät.

Kalenderrichtlinie

December 1, 2023

Sie können in Citrix Endpoint Management 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. Dieses Feld ist erforderlich.

- **Hostname:** Geben Sie die Adresse des CalDAV-Servers ein. Dieses Feld ist erforderlich.
- **Port:** Geben Sie den Port für die Verbindung mit dem CalDAV-Server ein. Dieses Feld 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. Dieses Feld 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 verfügbar ab iOS 6.0.

macOS-Einstellungen

- **Kontobeschreibung:** Geben Sie eine Kontobeschreibung ein. Dieses Feld ist erforderlich.
- **Hostname:** Geben Sie die Adresse des CalDAV-Servers ein. Dieses Feld ist erforderlich.
- **Port:** Geben Sie den Port für die Verbindung mit dem CalDAV-Server ein. Dieses Feld 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. Dieses Feld 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

June 25, 2024

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

Sie können Makros in Feldern ohne Zeichenfolgen, z. B. **Proxyserverport**, verwenden.

Beispielsweise können Sie ein Makro wie `${ device.xyz }` oder `${ setting.xyz }` verwenden, das in eine Ganzzahl erweitert wird. Sie können die Makros auch in einer XML-Datei zu Gerätekonfiguration verwenden, die Sie mit der Geräterichtlinie **iOS- und macOS-Profilimport** in Citrix Endpoint Management importieren.

- **APN anfügen**
  - **Name:** Name für die Konfiguration.
  - **Authentifizierungstyp:** Klicken Sie in der Dropdownliste 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 Dropdownliste 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.

Verbindungszeitplanrichtlinie für Geräte

June 25, 2024

> **Wichtig:**
>
> Citrix empfiehlt, dass Sie Firebase Cloud Messaging (FCM) verwenden, um die Verbindung von Android- und Android Enterprise-Geräten mit Citrix Endpoint Management 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 Citrix Endpoint Management herstellen. Wenn Sie FCM verwenden, müssen Sie auch eine Richtlinie für die Verbindungszeitplanung erstellen.

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.

Android- und Android Enterprise-Einstellungen

- **Geräte müssen Verbindung herstellen:** Klicken Sie auf die Option, die Sie für diesen Zeitplan festlegen möchten.

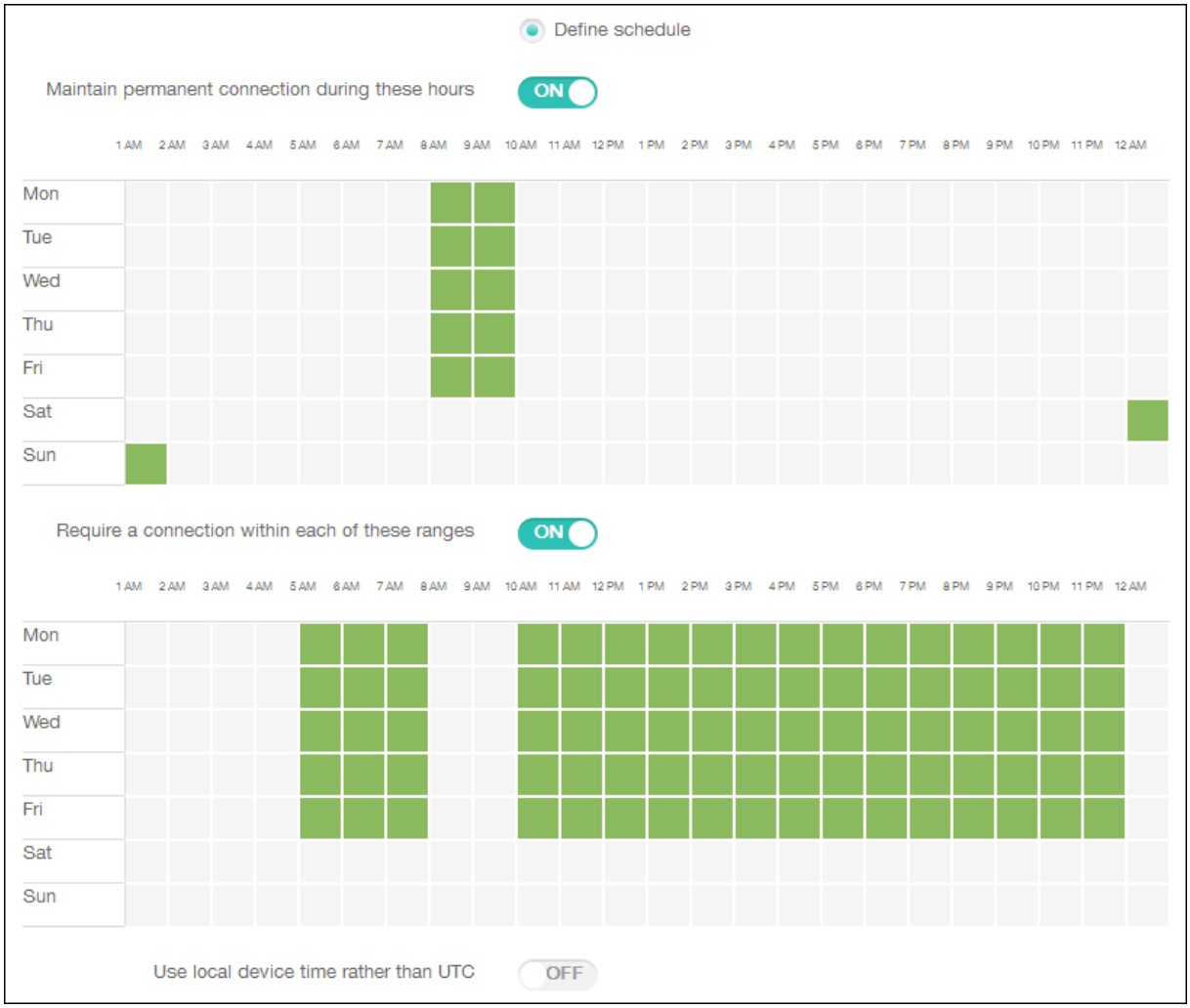
- **Nie:** Die Verbindung muss manuell hergestellt werden. Die Benutzer müssen die Verbindung mit Citrix Endpoint Management auf ihrem Gerät herstellen. Citrix empfiehlt, diese Option nicht für Produktionsumgebungen zu verwenden, da sie die Bereitstellung von Sicherheitsrichtlinien auf Geräten verhindert, sodass Benutzer nie neue Apps und Richtlinien erhalten. Die Option **Nie** ist standardmäßig aktiviert.
- **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 Citrix Endpoint Management 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 Standard- und Mindestwert ist **120**.
- **Zeitplan festlegen:** Citrix Endpoint Management versucht nach einer Netzwerkverbindungsunterbrechung eine Wiederherstellung der Verbindung zwischen Benutzergerät und Citrix Endpoint Management-Server. Citrix Endpoint Management überwacht die Verbindung durch regelmäßige Übertragung von Kontrollpaketen in dem von Ihnen festgelegten Zeitrahmen. Informationen zum Einrichten eines Verbindungszeitrahmens finden Sie unter "Verbindungszeitrahmen definieren".
  - **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.

Verbindungszeitrahmen definieren

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 entspricht einer Stunde. Wenn Sie beispielsweise eine Verbindung zwischen 8:00 und 9:00 Uhr an jedem Werktag wünschen, klicken Sie für jeden Werktag auf das Quadrat zwischen 8:00 und 9:00 Uhr.

Die beiden Zeitachsen in der folgenden Abbildung bewirken Folgendes:

- Eine stehende Verbindung zwischen 8:00 Uhr und 10:00 Uhr an jedem Werktag.
- Eine stehende Verbindung zwischen 1:00 Uhr und 2:00 Uhr am Sonntag.
- Mindestens eine Verbindung an jedem Werktag zwischen 5:00 und 8:00 Uhr oder zwischen 10:00 Uhr und 00:00 Uhr.



Geräterichtlinie für Kontakte (CardDAV)

December 1, 2023

Sie können in Citrix Endpoint Management 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. Dieses Feld ist erforderlich.

- **Hostname:** Geben Sie die Adresse des CardDAV-Servers ein. Dieses Feld ist erforderlich.
- **Port:** Geben Sie den Port für die Verbindung mit dem CardDAV-Server ein. Dieses Feld 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. Dieses Feld 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.

macOS-Einstellungen

- **Kontobeschreibung:** Geben Sie eine Kontobeschreibung ein. Dieses Feld ist erforderlich.
- **Hostname:** Geben Sie die Adresse des CardDAV-Servers ein. Dieses Feld ist erforderlich.
- **Port:** Geben Sie den Port für die Verbindung mit dem CardDAV-Server ein. Dieses Feld 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. Dieses Feld 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.

Benutzerdefinierte XML-Geräterichtlinie

June 25, 2024

Sie können benutzerdefinierte XML-Richtlinien in Citrix Endpoint Management erstellen, um die folgenden Features auf unterstützten Windows-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 DM protocol support.

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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Desktop/Tablet-Einstellungen

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 Citrix Endpoint Management 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.

Einrichten und Konfigurieren von Geräten mit Windows AutoPilot

Windows AutoPilot ist eine Sammlung von Technologien, mit denen neue Geräte eingerichtet, vorkonfiguriert und betriebsbereit gemacht werden können. Sie können Windows AutoPilot verwenden, um Geräte zurückzusetzen, für neue Zwecke zu verwenden oder wiederherzustellen. AutoPilot kann dazu beitragen, die aktuelle Bereitstellung Ihres Betriebssystems zu vereinfachen. AutoPilot reduziert diese Aufgabe auf eine Reihe einfacher Einstellungen und Vorgänge, mit denen Ihre Geräte im Handumdrehen einsatzbereit sind.

In diesem Video finden Sie einen kurzen Überblick über die Verwendung von Windows AutoPilot mit Citrix Endpoint Management.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Voraussetzungen

- Das Firmenbranding ist im Azure Active Directory-Portal konfiguriert.
- Das Unternehmen hat ein Azure AD-Premium P1- oder P2-Abonnement.
- Konfigurieren Sie Azure Active Directory als IdP-Typ für Citrix Endpoint Management. Navigieren Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Identitätsanbieter (IdP)**.
- Netzwerkverbindung zu Clouddiensten, die von Windows AutoPilot verwendet werden.
- Windows 10, Professional, Enterprise oder Education (Version 1703 oder höher) oder Windows 11, Professional, Enterprise oder Education ist auf den Geräten vorinstalliert.
- Geräte haben Internetzugriff.

Weitere Informationen zum Konfigurieren von Voraussetzungen finden Sie in der Microsoft Windows-Dokumentation zu AutoPilot: https://docs.microsoft.com.

Konfigurieren der automatischen Windows-Neubereitstellung in Citrix Endpoint Management für AutoPilot-Geräte

1. Führen Sie folgende Schritte aus, um unter "Benutzerdefinierte XML-Geräterichtlinie"eine benutzerdefinierte XML-Richtlinie hinzuzufügen. Fügen Sie unter **XML-Inhalt** Folgendes hinzu:

```
<Add>
<CmdID>_cmdid_</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
   DisableAutomaticReDeploymentCredentials</LocURI>
</Target>
<Meta>
<Format xmlns="syncml:metinf">int</Format>
</Meta>
<Data>0</Data>
</Item>
</Add>

<!--NeedCopy-->
```

2. Geben Sie im Windows-Sperrbildschirm den Tastaturbefehl **STRG + Windows-Taste + R** ein.
3. Melden Sie sich mit einem Azure Active Directory-Konto an.
4. Das Gerät überprüft, ob der Benutzer über die notwendigen Berechtigungen zum erneuten Bereitstellen des Geräts verfügt. Anschließend erfolgt die erneute Bereitstellung des Geräts.
5. Nach der Aktualisierung des Geräts mit der AutoPilot-Konfiguration kann sich der Benutzer am neu konfigurierten Gerät anmelden.

Bereitstellen eines Einzel-App-Kiosks auf Windows 11-Geräten

> **Hinweis:**
>
> Windows 11-Geräte unterstützen nur den Einzel-App-Kioskmodus.

Kopieren Sie im Textfeld **XML-Inhalt** das folgende XML-Skript, fügen Sie es ein und ersetzen Sie dann die folgenden Zeichenfolgen durch Ihre Einstellungen:

- `your_username_here`(zwei Instanzen): Benutzername, den Sie auf dem Gerät erstellen möchten. Behalten Sie für beide Instanzen dieselben Einstellungen bei.
- `your password_here`: Kennwort für den Benutzer.
- `your_UWP_app_id_here`: AUMID für die UMP-App, die Sie auf dem Gerät bereitstellen möchten.

XML-Skript:


```
<Add>
    <CmdID>_cmdid_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/Accounts/Users/
               your_username_here/Password</LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data>your_password_here</Data>
    </Item>
</Add>
<Replace>
    <CmdID>_cmdid_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/AssignedAccess/Configuration</
               LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data><![CDATA[<AssignedAccessConfiguration
        xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config"
        xmlns:rs5="http://schemas.microsoft.com/AssignedAccess/201810/
           config">
            <Profiles>
                <Profile Id="{
 AFF9DA33-AE89-4039-B646-3A5706E92957 }
 ">
                    <KioskModeApp AppUserModelId="your_UWP_app_id_here"
                       />
                </Profile>
            </Profiles>
            <Configs>
                <Config>
                    <Account>your_username_here</Account>
                    <DefaultProfile Id="{
 AFF9DA33-AE89-4039-B646-3A5706E92957 }
 "/>
                </Config>
            </Configs>
        </AssignedAccessConfiguration>]]></Data>
    </Item>
</Replace>
<!--NeedCopy-->
```

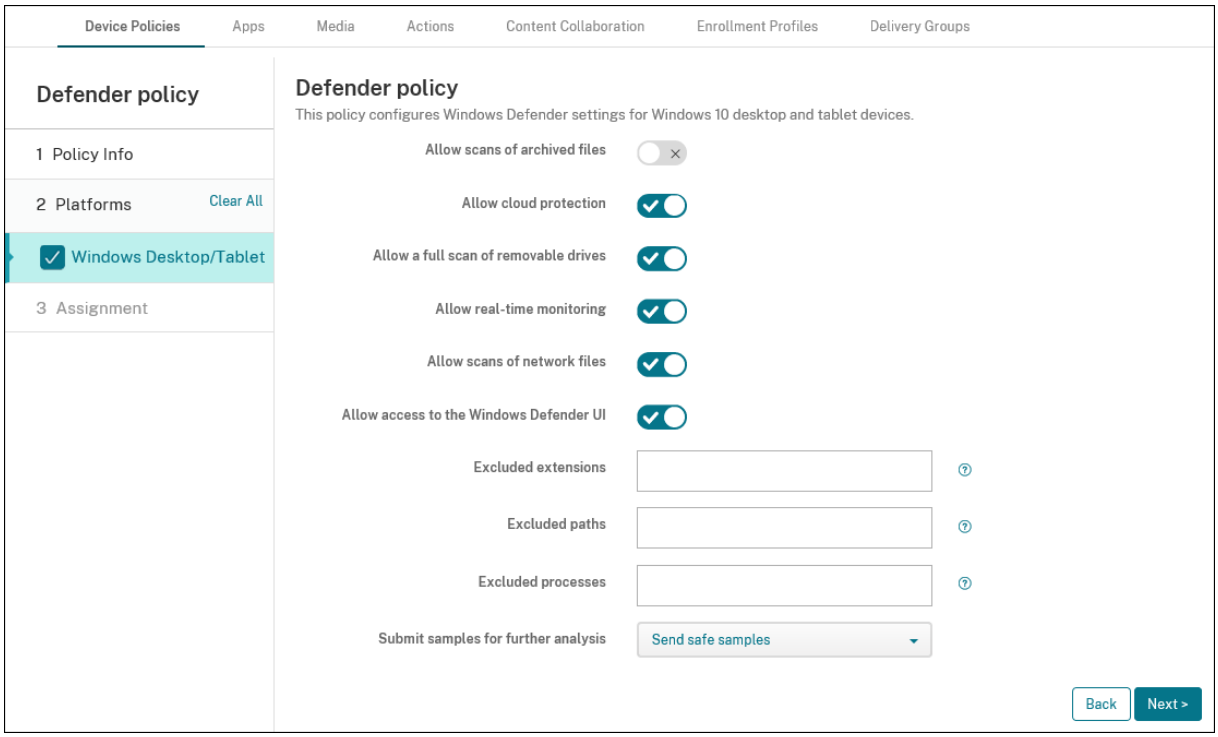

Defender-Geräterichtlinie

December 1, 2023

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 Citrix Endpoint Management-Geräterichtlinie "Defender"verwenden, um die Microsoft Defender-Richtlinie für Desktops und Tablets mit Windows 10 und Windows 11 zu konfigurieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Desktop-/Tablet-Einstellungen



- **Scannen archivierter Dateien zulassen:** Ermöglicht oder blockiert das Scannen archivierter Dateien durch Defender. Die Standardeinstellung ist **Aus**.
- **Cloud-Schutz zulassen:** Ermöglicht oder blockiert das Senden von Informationen über Malware-Aktivitäten an Microsoft durch Defender. Die Standardeinstellung ist **Ein**.
- **Vollständigen Scan von Wechsellaufwerken zulassen:** Ermöglicht oder blockiert das Scannen von Wechseldatenträgern (z. B. USB-Sticks) durch Defender. Die Standardeinstellung ist **Ein**.
- **Echtzeitüberwachung zulassen:** Die Standardeinstellung ist **Ein**.

- **Scannen von Netzwerkdateien zulassen:** Ermöglicht oder blockiert das Scannen von Netzwerkdateien durch Defender. Die Standardeinstellung ist **Ein**.
- **Zugriff auf die Benutzeroberfläche von Windows Defender zulassen:** 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`.
- **Beispiele zur weiteren Analyse senden:** Steuert das Senden von Microsoft-Dateien zur weiteren Analyse auf Schadsoftware. Optionen: **Immer auffordern**, **Sichere Proben senden**, **Nie senden**, **Alle Proben senden**. Die Standardeinstellung lautet **Sichere Proben senden**.

Device Guard-Richtlinie

June 25, 2024

Device Guard ist ein Sicherheitsfeature, das unter Windows 10 und Windows 11 zur Verfügung steht. Dieses Feature ermöglicht virtualisierungsbasierte Sicherheit, indem es über den **Windows-Hypervisor** Sicherheitsdienste auf dem Gerät unterstützt. Über die Device Guard-Geräterichtlinie können Sie Sicherheitsfunktionen wie "Sicherer Start", eine UEFI-Sperre und eine Virtualisierung aktivieren.

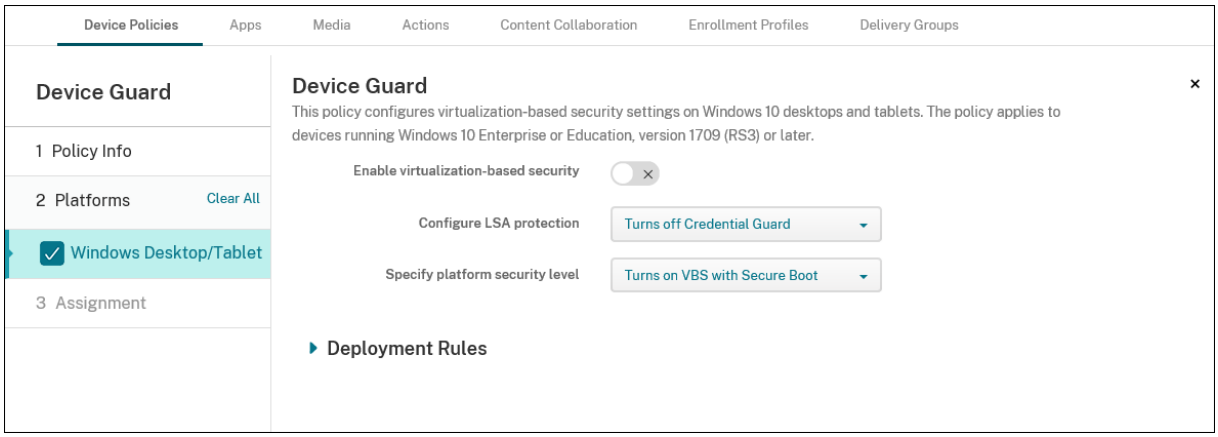
Voraussetzungen

- Desktops und Tablets mit Windows 10 und Windows 11 und einer Enterprise- oder Education-Lizenz
- In Windows aktiviertes Device Guard-Feature

  Weitere Informationen zum Device Guard finden Sie unter https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Gerätерichtlinien.

Windows Desktop-/Tablet-Einstellungen



- **Virtualisierungsbasierte Sicherheit aktivieren:** Deaktivieren oder aktivieren Sie die virtualisierungsbasierten Sicherheitsfunktionen. Die virtualisierungsbasierte Sicherheit stellt Sicherheitsdienste über den Windows-Hypervisor bereit.
- **LSA-Schutz konfigurieren:** Ermöglicht das Konfigurieren von Credential Guard. Mit dieser Einstellung können Benutzer Credential Guard aktivieren, eine virtualisierungsbasierte Sicherheitsfunktion, mit der Anmeldeinformationen beim nächsten Neustart besser geschützt sind. Optionen sind **Deaktiviert Credential Guard**, **Aktiviert Credential Guard mit UEFI-Sperre** und **Aktiviert Credential Guard ohne UEFI-Sperre**. Die Standardeinstellung ist **Deaktiviert Credential Guard**.
- **Plattformsicherheitsstufe angeben:** Hier können Sie die Plattformsicherheitsstufe beim nächsten Neustart angeben. Verfügbare Optionen sind **Aktiviert VBS mit Secure Boot** und **Aktiviert VBS mit Secure Boot und direktem Speicherzugriff**. Die Standardeinstellung ist **Aktiviert VBS mit Secure Boot**.

Citrix Endpoint Management überprüft, ob die virtualisierungsbasierten Sicherheitseinstellungen des Geräts mit den Einstellungen auf dem Server übereinstimmen. Wenn die Sicherheitseinstellungen übereinstimmen, stellt Citrix Endpoint Management die Richtlinie nicht auf dem Gerät bereit. Wenn die Sicherheitseinstellungen nicht übereinstimmen, wird die Richtlinie von Citrix Endpoint Management bereitgestellt.

Integritätsnachweisrichtlinie für Geräte

December 1, 2023

In Citrix Endpoint Management können Sie festlegen, dass Windows 10- und Windows 11-Geräte ihren Integritätsstatus melden müssen. Dazu senden die Geräte 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 Citrix Endpoint Management gesendet wird. Citrix Endpoint Management löst anhand des Zertifikats für den Integritätsnachweis von Ihnen eingerichtete automatische Aktionen aus.

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.

Sie können DHA über Microsoft Cloud oder einen lokalen Windows-DHA-Server wie folgt konfigurieren:

- Microsoft Cloud: Fügen Sie eine DHA-Richtlinie hinzu und konfigurieren Sie sie gemäß der Anleitung im vorliegenden Artikel.
- Lokaler Windows-DHA-Server: Konfigurieren Sie einen DHA-Server. Fügen Sie dann eine DHA-Richtlinie hinzu und konfigurieren Sie sie gemäß der Anleitung im vorliegenden Artikel.

  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.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Desktop/Tablet-Einstellungen

Bei Konfiguration von DHA mit Microsoft Cloud

- **Device Health Attestation aktivieren:** Wählen Sie aus, ob ein Integritätsnachweis erforderlich sein soll. Die Standardeinstellung ist **Aus**.

Bei Konfiguration von DHA mit einem lokalen Windows-DHA-Server

- **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.

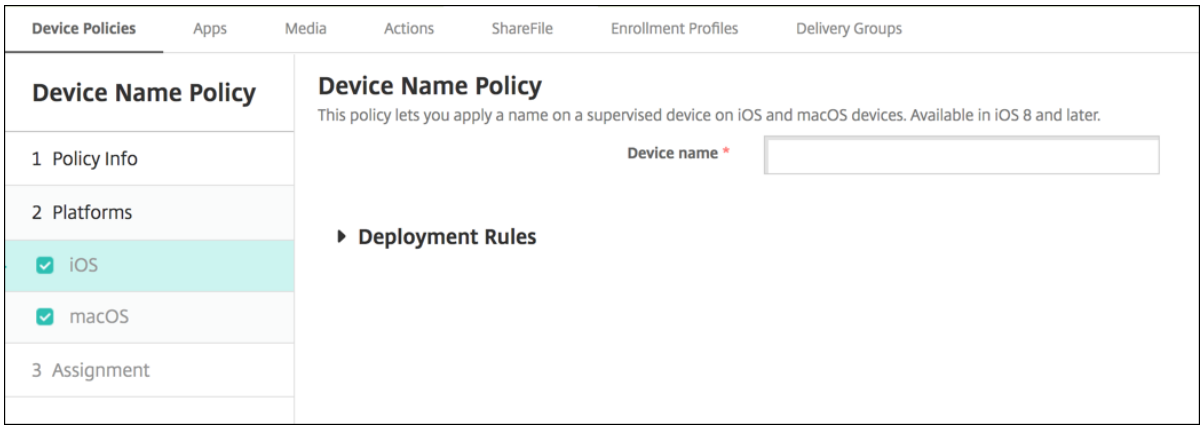
Richtlinien für Gerätenamen

December 1, 2023

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 Citrix Endpoint Management.

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 die Apple-ID des Benutzers in den Gerätenamen aufzunehmen.

Geräterichtlinie “Bildung - Konfiguration”

December 1, 2023

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

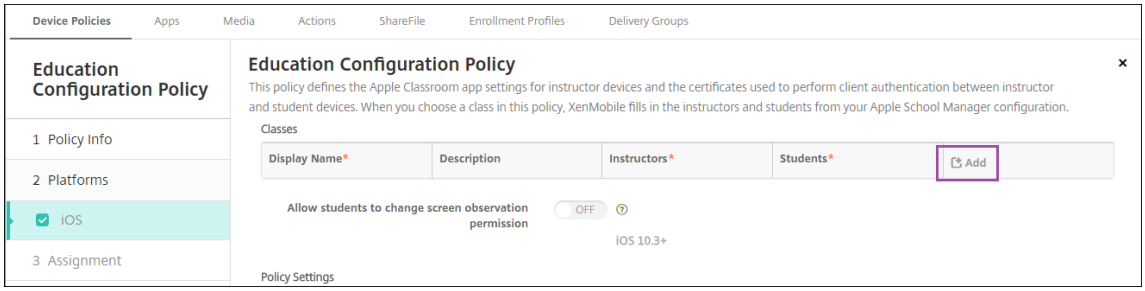
Die Richtlinie zur Konfiguration von Apple Bildung wird für iOS-Geräte (iPadOS) unterstützt.

Wenn Sie in dieser Richtlinie eine Klasse auswählen, werden in der Citrix Endpoint Management-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.

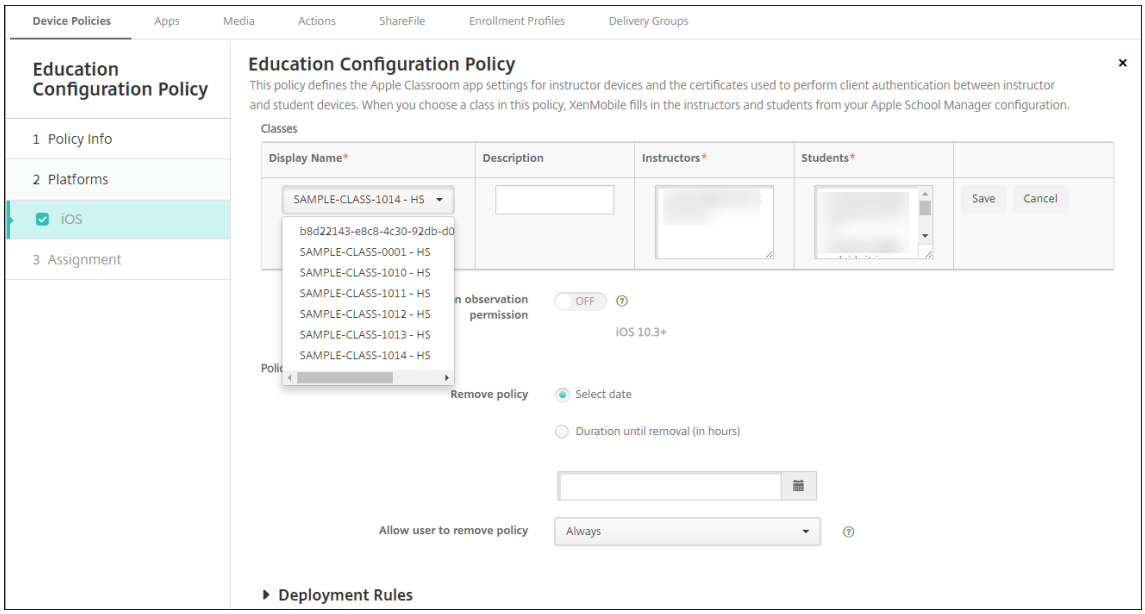
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

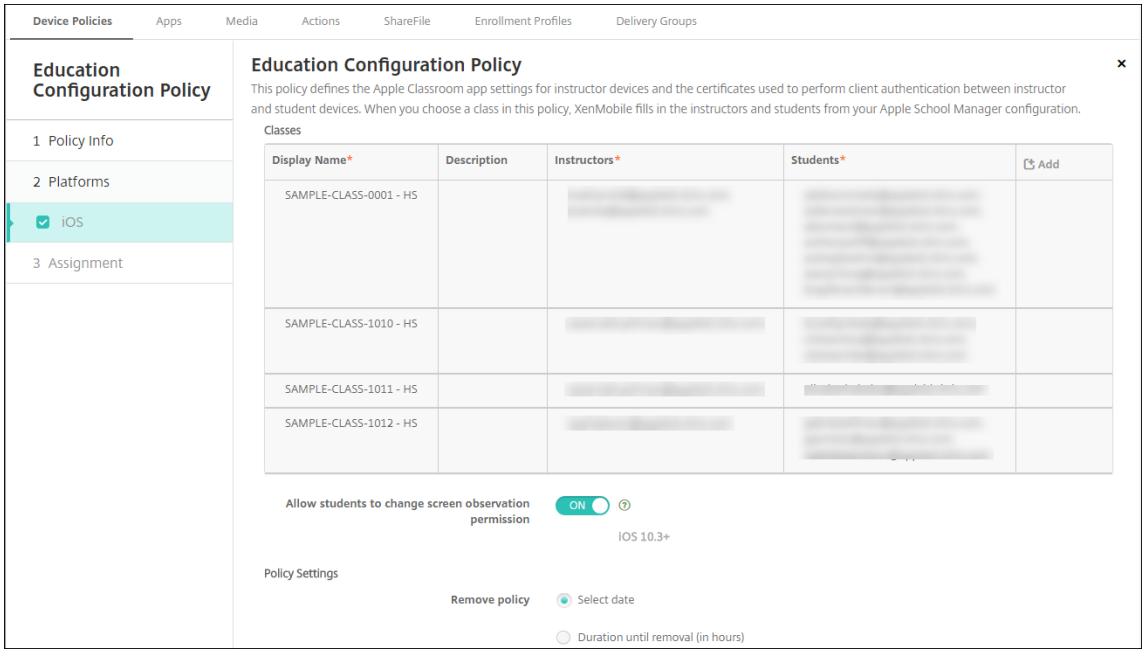
- **Klassen:** Um eine Klasse hinzuzufügen, klicken Sie auf **Hinzufügen**.



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 Citrix Endpoint Management automatisch eingetragen. Fügen Sie weitere Klassen hinzu.

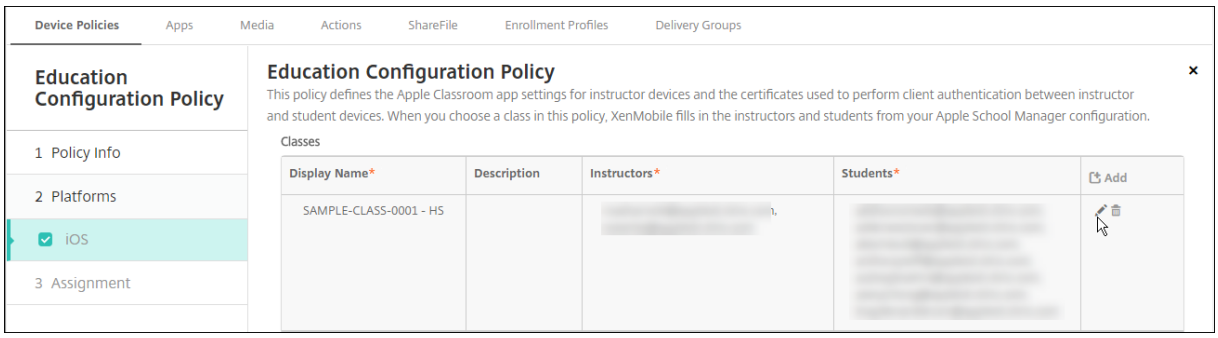


- **Schüler dürfen Berechtigung für Bildschirmansicht ändern:** Wenn diese Option auf **Ein** festgelegt wird, können Lernende in verwalteten Klassen wählen, ob sie der Lehrkraft das Betrachten des Bildschirms auf ihren Geräten gestatten möchten. Die Standardeinstellung ist **Aus**.
- **Richtlinieneinstellungen**
  - **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 Citrix Endpoint Management 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.

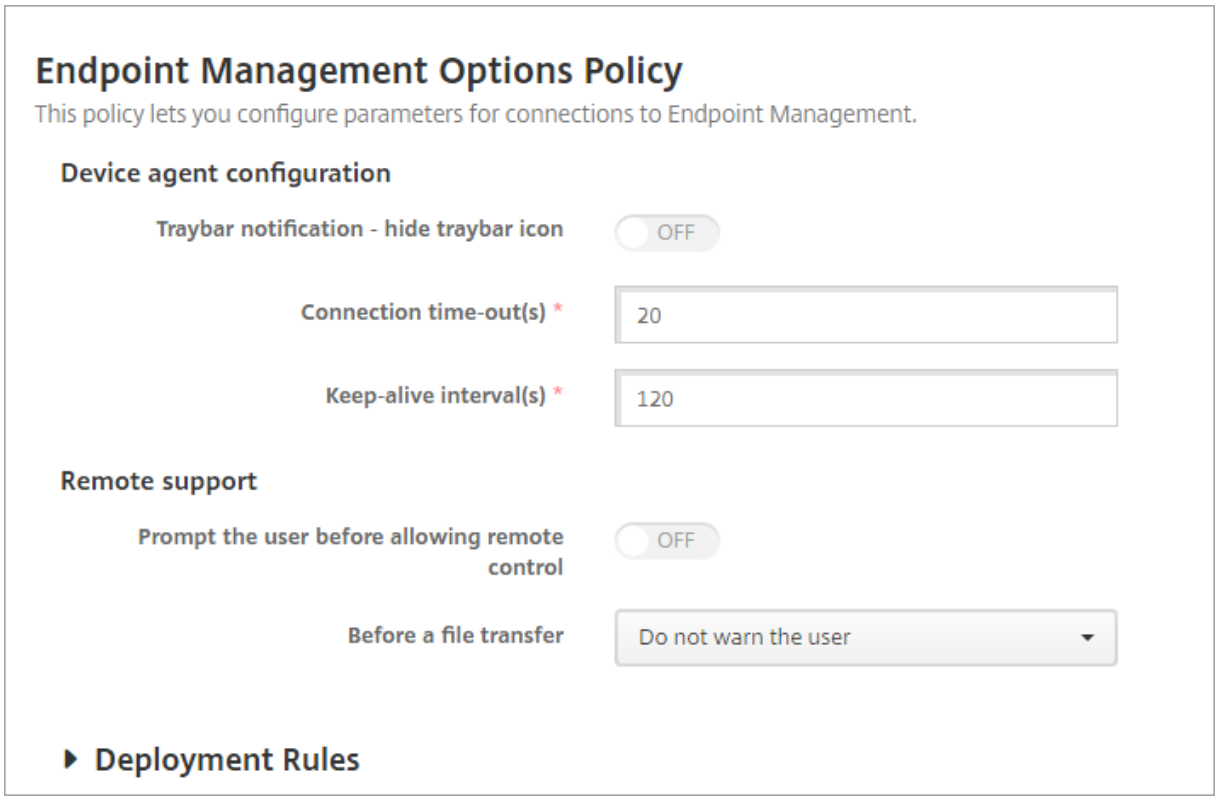
Endpoint Management-Optionsrichtlinie für Geräte

June 25, 2024

Sie fügen eine Endpoint Management-Optionsrichtlinie hinzu, um das Citrix Secure Hub-Verhalten für Verbindungen zwischen Citrix Endpoint Management und Android-Geräten zu konfigurieren.

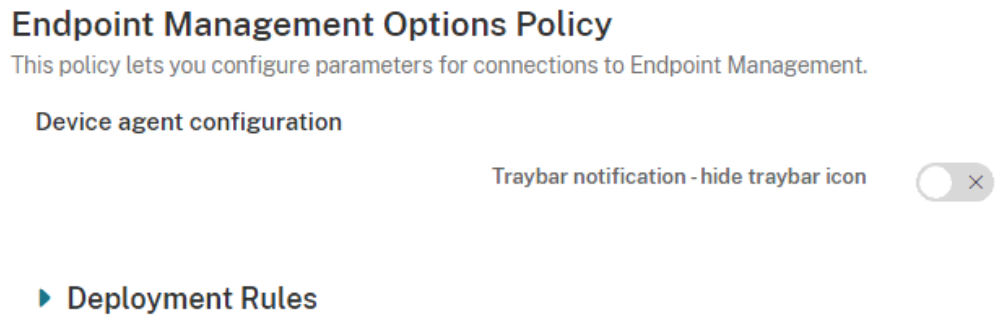
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

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-Intervalle:** 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 Dropdownliste 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**.

> **Hinweis:**
>
> Wenn Sie den VPN-Dienst für Geräte aktivieren möchten, die auf Android Enterprise ausgeführt werden, können Sie die Option **Always-On-VPN aktivieren** in der **VPN-Geräterichtlinie** aktivieren. Wenn Sie in einer früheren Version die Option **Always-On-VPN aktivieren** in der Geräterichtlinie **Endpoint Management-Optionen** bereits aktiviert haben, stellen Sie sicher, dass Sie sie erneut in der **VPN-Geräterichtlinie** aktivieren.

Citrix Endpoint Management-Deinstallationsrichtlinie

December 1, 2023

Sie können in Citrix Endpoint Management eine Geräterichtlinie einrichten, mit der Citrix Endpoint Management von Android-Geräten deinstalliert wird. Wenn diese Richtlinie bereitgestellt wird, entfernt sie Citrix Endpoint Management von allen Geräten in der Bereitstellungsgruppe.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android-Einstellungen

- **Citrix Endpoint Management von Geräten deinstallieren:** Wählen Sie aus, ob Citrix Endpoint Management von allen Geräten deinstalliert werden soll, für die Sie die Richtlinie bereitstellen. Die Standardeinstellung ist **Aus**.

Exchange-Geräterichtlinie

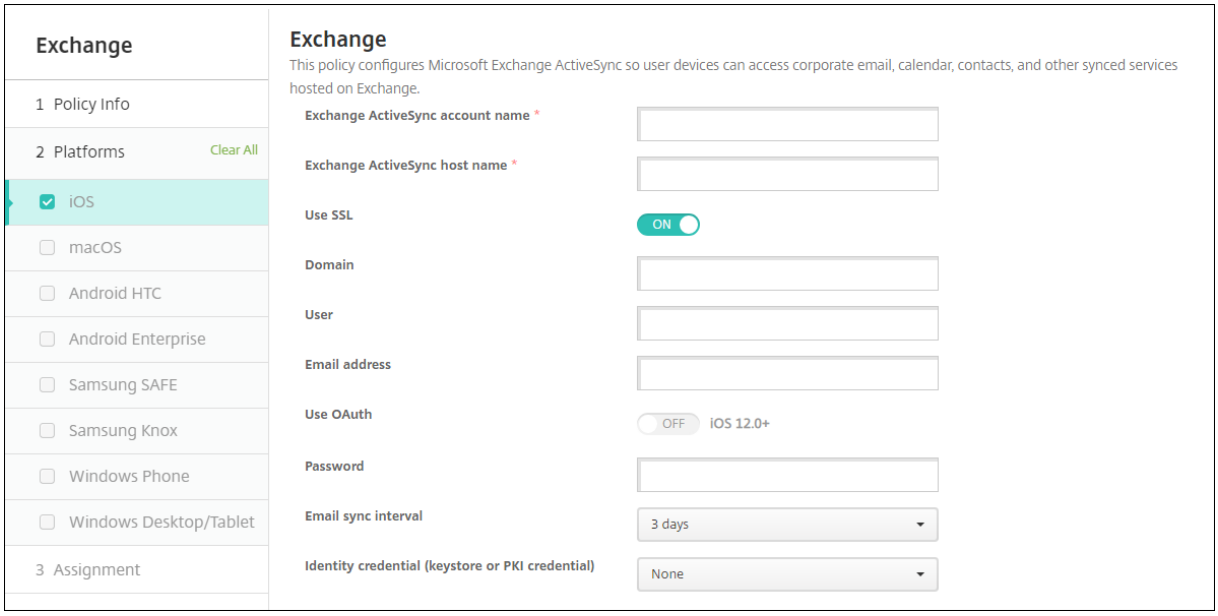
June 25, 2024

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. 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 im 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 Citrix Endpoint Management 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 an, ob Benutzer
  - E-Mail von diesem Konto in ein anderes Konto verschieben
  - E-Mail von einem anderen Konto aus weiterleiten
  - oder 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**.
- **Verhindern, dass Benutzer aktuelle Adressen synchronisieren:** Wählen Sie aus, ob eine Synchronisierung zuletzt verwendeter Adressen durch die Benutzer verhindert werden soll. Die Standardeinstellung ist **Aus**.

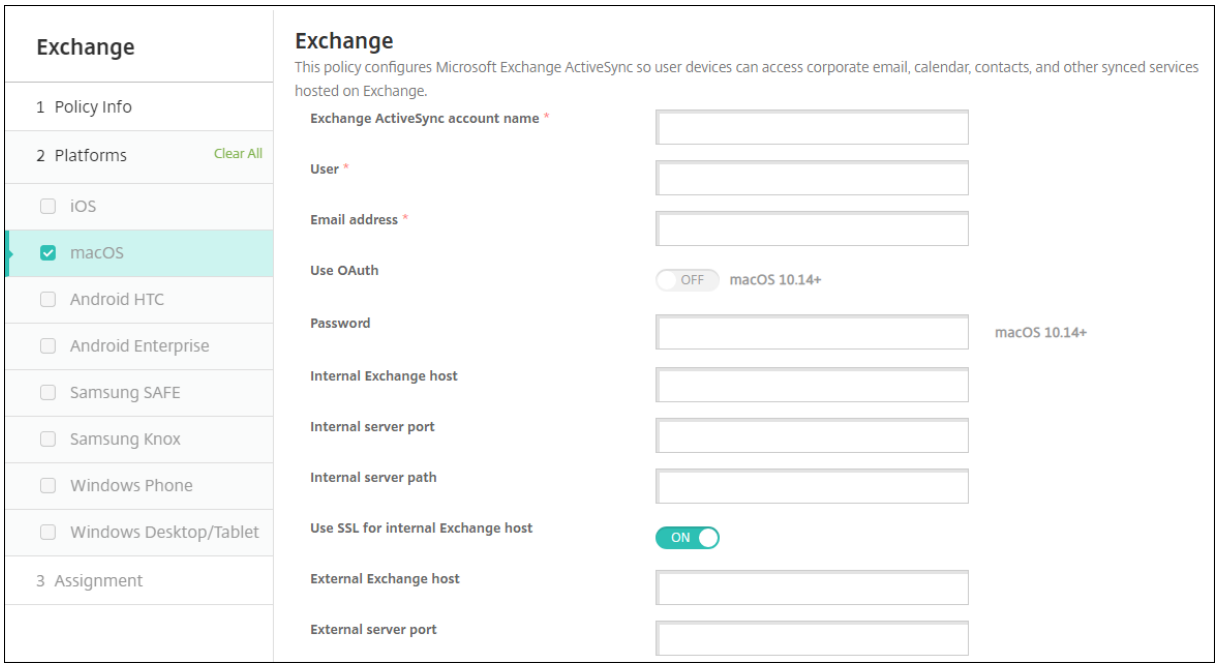
- **Mail Drop zulassen:** Wählen Sie aus, ob das Konto Mail Drop verwenden darf. Die Standardeinstellung ist **Aus**.
- **S/MIME-Signatur aktivieren:** Wählen Sie, ob dieses Konto S/MIME-Signaturen unterstützt. Die Standardeinstellung ist **Ein**. Wenn Sie **Ein** wählen, werden folgende Felder eingeblendet.
  - **Anmeldeinformationen für Signieridentität:** Wählen Sie die Anmeldeinformationen für die Signatur aus.
  - **Benutzer darf S/MIME-Signatur überschreiben:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Signatur in den Einstellungen ihrer Geräte aktivieren und deaktivieren. Die Standardeinstellung ist **Aus**. Diese Option gilt für iOS 12.0 und höher.
  - **Benutzer darf die UUID des S/MIME-Signaturzertifikats überschreiben:** 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**.
  - **Benutzer darf S/MIME-Verschlüsselung überschreiben:** 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.
  - **Benutzer darf die UUID des S/MIME-Verschlüsselungszertifikats überschreiben:** Wenn Sie **Ein** wählen, können Benutzer die S/MIME-Verschlüsselungsidentität und Verschlüsselung in den Einstellungen ihrer 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.

Synchronisierte Exchange-Dienste

Über die Einstellungen “Synchronisierte Exchange-Dienste”können Sie auswählen, ob die folgenden Features synchronisiert werden sollen:

- Kalender
- Kontakte
- E-Mail
- Hinweise
- Erinnerungen

macOS-Einstellungen



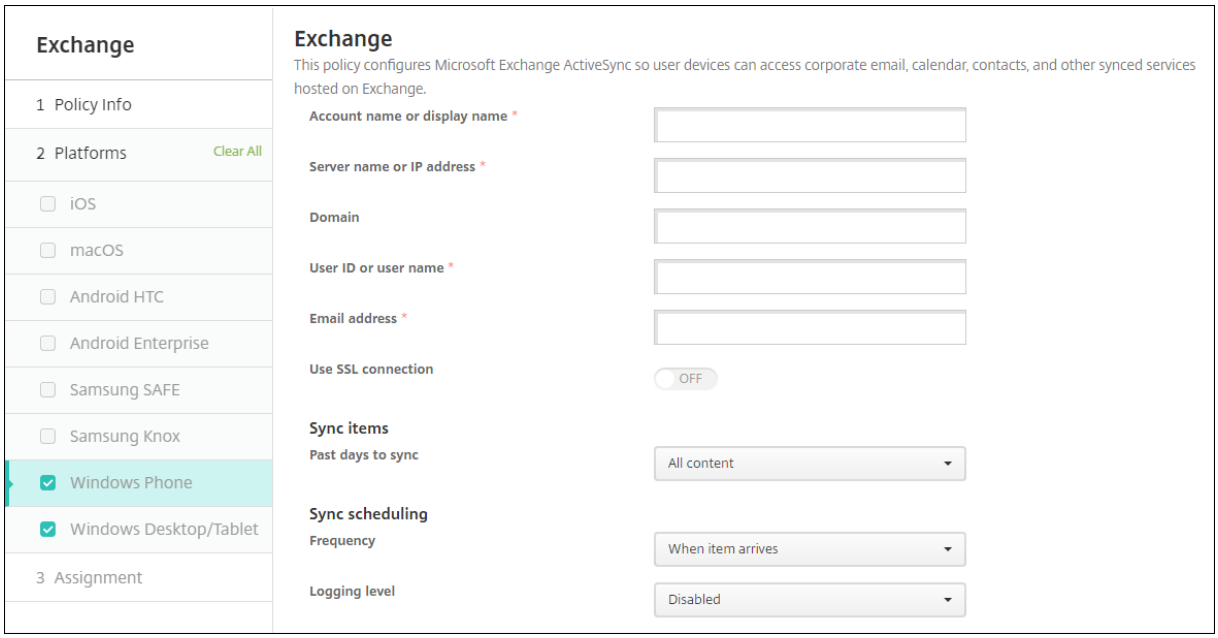
- **Exchange ActiveSync-Kontoname:** Geben Sie die Beschreibung des E-Mail-Kontos ein, die auf den Geräten angezeigt werden soll.
- **Benutzer:** Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro `$user.username` verwenden, um die Benutzernamen automatisch zu suchen.
- **E-Mail-Adresse:** Geben Sie die vollständige E-Mail-Adresse ein. Sie können in diesem Feld das Systemmakro `$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.

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 Dropdownliste 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 Dropdownliste auf **Deaktiviert**, **Einfach** oder **Erweitert**, um festzulegen, wie detailliert Exchange-Aktivitäten protokolliert werden sollen. Die Standardeinstellung ist **Deaktiviert**.

Dateirichtlinie

November 3, 2022

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)

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.
- **Zielordner:** Wählen Sie in der Liste den Speicherort für die hochgeladene Datei aus oder klicken Sie auf **Hinzufügen**, um einen Speicherort auszuwählen. Wählen Sie das Makro `%Flash Storage%\` oder `%XenMobile Storage%\`, um den Speicherort der hochgeladenen Datei anzugeben. Damit wird der jeweilige Speicherort auf jedem Gerät erweitert.

  - %XenMobile Storage%\ wird auf Android/data/com.zenprise/ im internen Speicherverzeichnis erweitert.
  - In Android 9.0 und früher wird die Datei mit %Flash Storage%\ im externen Speicherverzeichnis gespeichert.
  - Ab Android 10.0 wird die Datei mit %Flash Storage%\ im Ordner **Downloads** des internen Speicherverzeichnisses gespeichert.
  - In Android 11.0 und höher kann %XenMobile Storage%\ nicht mehr angewendet werden aufgrund von Google-Einschränkungen, die den Zugriff auf den Zielstandort begrenzen.

- **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**.

> **Wichtig:**
>
> Die Geräterichtlinie "Dateien"unterstützt das Hinzufügen von Skripts auf Android Enterprise nicht mehr. Wenn eine vorhandene Richtlinie ein Skript enthält, wird bei der Auswahl der Richtlinie eine Fehlermeldung angezeigt und Sie können die Richtlinie erneut hinzufügen, um das Problem zu beheben.

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. 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 Speicherort auszuwählen. Wählen Sie das Makro %Flash Storage%\ oder %XenMobile Storage%\, um den Speicherort der hochgeladenen Datei anzugeben. Damit wird der jeweilige Speicherort auf jedem Gerät erweitert.
  - %XenMobile Storage%\ wird auf Android/data/com.zenprise/ im internen Speicherverzeichnis erweitert.
  - In Android 9.0 und früher wird die Datei mit %Flash Storage%\ im externen Speicherverzeichnis gespeichert.

  - Ab Android 10.0 wird die Datei mit `%Flash Storage%\` im Ordner **Downloads** des internen Speicherverzeichnisses gespeichert.
  - In Android 11.0 und höher kann `%XenMobile Storage%\` nicht mehr angewendet werden aufgrund von Google-Einschränkungen, die den Zugriff auf den Zielstandort begrenzen.

- **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**.

FileVault-Geräterichtlinie

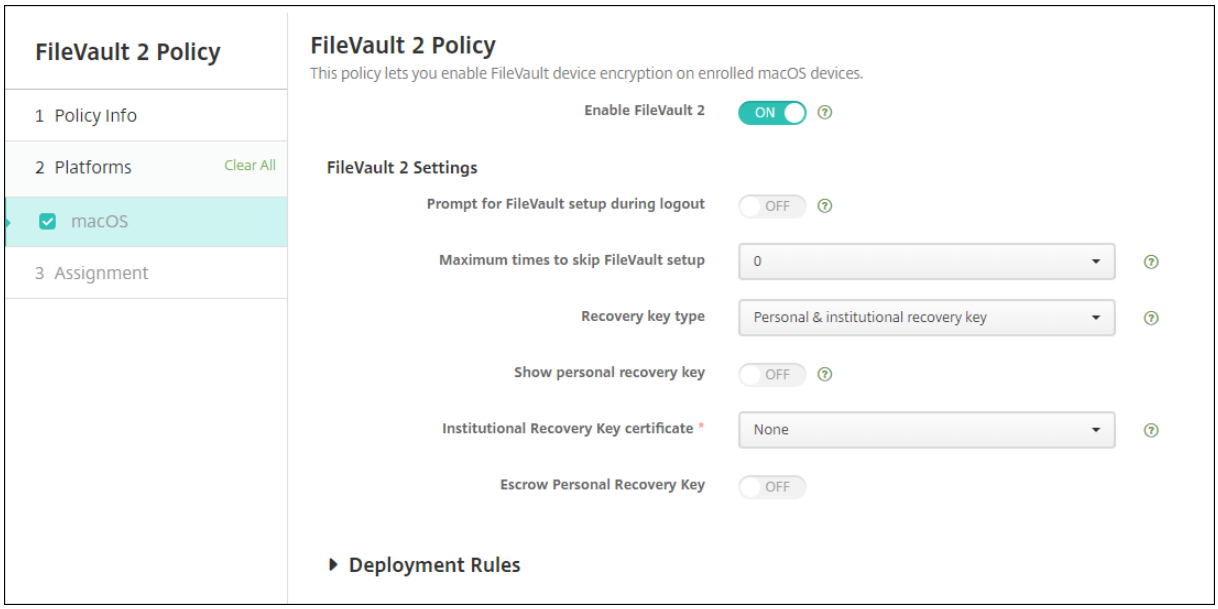
December 1, 2023

Die macOS-FileVault-Datenträgerverschlüsselung (FileVault 2) schützt das Systemvolume durch Verschlüsselung der Inhalte. Bei einem macOS-Gerät, auf dem FileVault 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.

Diese Geräterichtlinie aktiviert Bildschirme zur FileVault-Benutzereinrichtung und konfiguriert Einstellungen wie z. B. den Wiederherstellungsschlüssel. Weitere Informationen zu FileVault finden Sie auf der Apple-Supportsite.

Zum Hinzufügen der FileVault-Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**.

macOS-Einstellungen



- **FileVault aktivieren:** 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** erhalten Benutzer zwar keine Aufforderung, FileVault zu aktivieren, können FileVault aber trotzdem selbst aktivieren.
- **Beim Abmelden zur Einrichtung von FileVault auffordern:** Wenn **Ein** aktiviert ist, werden die Benutzer beim Abmelden dazu aufgefordert, FileVault zu aktivieren.
- **Male, die das Einrichten von FileVault übersprungen werden darf:** maximale Zahl der Male, die der Benutzer die FileVault-Einrichtung überspringen kann. Wird die Höchstzahl erreicht, muss der Benutzer FileVault einrichten, um sich anmelden zu können. Bei der Einstellung **0** muss der Benutzer FileVault beim ersten Anmeldeversuch aktivieren. Die Standardeinstellung ist **0**.
- **Typ des Wiederherstellungsschlüssels:** Vergisst ein Benutzer sein Kennwort, kann er einen Wiederherstellungsschlüssel eingeben, um die Festplatte zu entsperren und das Kennwort zurückzusetzen. Optionen für Wiederherstellungsschlüssel:
  - **Persönlicher Wiederherstellungsschlüssel:** Ein persönlicher Wiederherstellungsschlüssel ist für den Benutzer eindeutig. Bei der FileVault-Einrichtung wählt der Benutzer aus, ob ein Wiederherstellungsschlüssel erstellt werden soll oder ob sein iCloud-Konto die Festplatte entsperren soll. Um den Wiederherstellungsschlüssel dem Benutzer nach Abschluss der FileVault-Installation anzuzeigen, aktivieren Sie **Persönlichen Wiederherstellungsschlüssel anzeigen**. Anhand der Anzeige des Schlüssels kann der Benutzer diesen für die

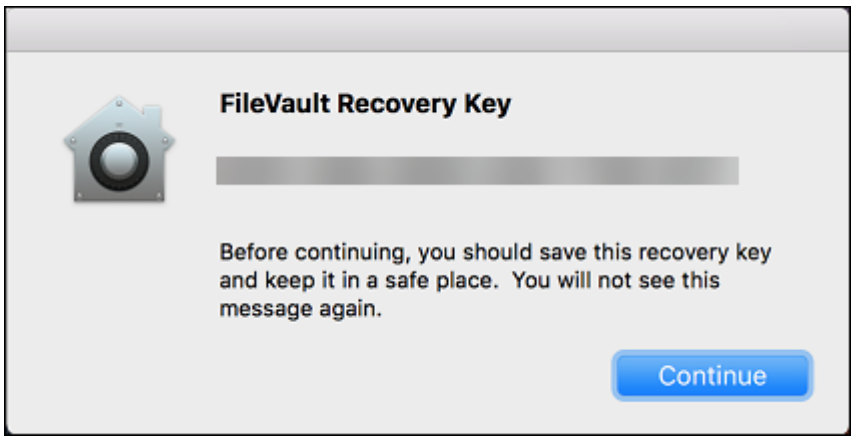
künftige Verwendung notieren. Damit Benutzer ihren Schlüssel bei Verlust nachschlagen können, aktivieren Sie **Hinterlegter persönlicher Wiederherstellungsschlüssel**.

Sie können persönliche Wiederherstellungsschlüssel durch Sicherheitsaktionen rotieren. Weitere Hinweise zum Archivieren persönlicher Wiederherstellungsschlüssel finden Sie unter Sicherheitsaktionen.

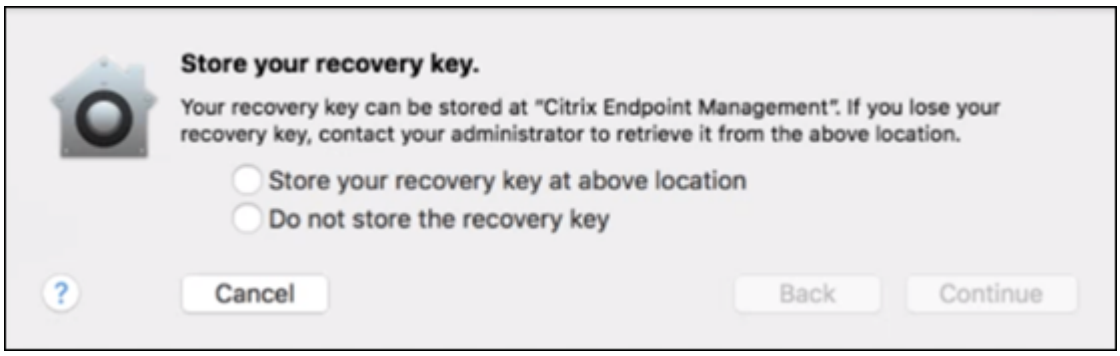
Informationen zur Verwaltung von Wiederherstellungsschlüsseln finden Sie auf der Apple-Supportsite.

- **Institutioneller Wiederherstellungsschlüssel:** Sie können einen institutionellen Wiederherstellungsschlüssel (Hauptschlüssel) und ein FileVault-Zertifikat erstellen, mit deren Hilfe Sie Benutzergeräte entsperren können. Weitere Informationen finden Sie auf der Apple-Supportsite. Verwenden Sie Citrix Endpoint Management, um das FileVault-Zertifikat auf Geräten bereitstellen. Informationen hierzu finden Sie unter Zertifikate und Authentifizierung.
- **Persönlicher und institutioneller Wiederherstellungsschlüssel:** Wenn Sie beide Arten von Wiederherstellungsschlüsseln aktivieren, müssen Sie Benutzergeräte nur entsperren, wenn ein Benutzer seinen persönlichen Wiederherstellungsschlüssel verliert.

- **Zertifikat für den institutionellen Wiederherstellungsschlüssel:** Wenn Sie als **Typ des Wiederherstellungsschlüssels** die Option **Institutioneller Wiederherstellungsschlüssel** oder **Persönlicher & institutioneller Wiederherstellungsschlüssel** auswählen, wählen Sie das Zertifikat für den Schlüssel aus.
- **Persönlichen Wiederherstellungsschlüssel anzeigen:** Bei der Einstellung **Ein** wird auf dem Benutzergerät der persönliche Wiederherstellungsschlüssel nach dem Aktivieren von FileVault angezeigt. Die Standardeinstellung ist **Aus**.

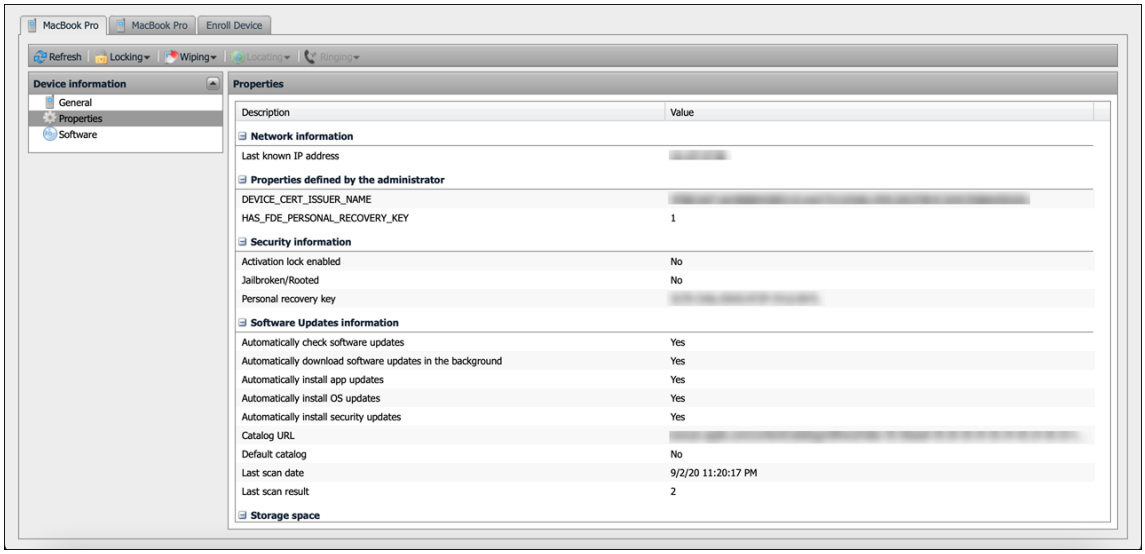


- **Hinterlegter persönlicher Wiederherstellungsschlüssel:** Wenn diese Option aktiviert ist, können Benutzer mit Citrix Endpoint Management für jedes Gerät eine Kopie ihres persönlichen Wiederherstellungsschlüssels speichern.



Um von Citrix Endpoint Management aus auf den Schlüssel zuzugreifen, gehen Sie zu **Verwalten > Geräte**, wählen Sie das macOS-Gerät aus und klicken Sie auf **Bearbeiten**. Gehen Sie dann zu **Gerätedetails > Allgemein** und suchen Sie den **persönlichen Wiederherstellungsschlüssel**.

Damit Benutzer ihren Wiederherstellungsschlüssel im Selbsthilfe-Portal anzeigen können, aktivieren Sie die Einstellungen **Hinterlegter persönlicher Wiederherstellungsschlüssel** und **Persönlichen Wiederherstellungsschlüssel anzeigen**. Der Schlüssel wird im Selbsthilfeportal auf der Seite **Eigenschaften** unter **Sicherheitsinformationen** angezeigt. Weitere Informationen zum Selbsthilfeportal finden Sie unter Selbsthilfeportal.



Sie können die Einstellung **Hinterlegter persönlicher Wiederherstellungsschlüssel** auch dann aktivieren, wenn Sie die Einstellung **FileVault aktivieren** nicht aktivieren. Bei deaktivierter Einstellung **FileVault aktivieren** können Benutzer FileVault weiterhin selbst aktivieren. Aktivieren Sie in diesem Fall **Hinterlegter persönlicher Wiederherstellungsschlüssel**, damit Benutzer eine Kopie ihres Schlüssels mit Citrix Endpoint Management aufbewahren können.

Wenn ein Benutzer FileVault vor der Registrierung des Geräts in Citrix Endpoint Management aktiviert, wird der Wiederherstellungsschlüssel nicht von Citrix Endpoint Management gespeichert. Das Gerät wird in der Konsole als FileVault-aktiviert angezeigt.

Firewallrichtlinie

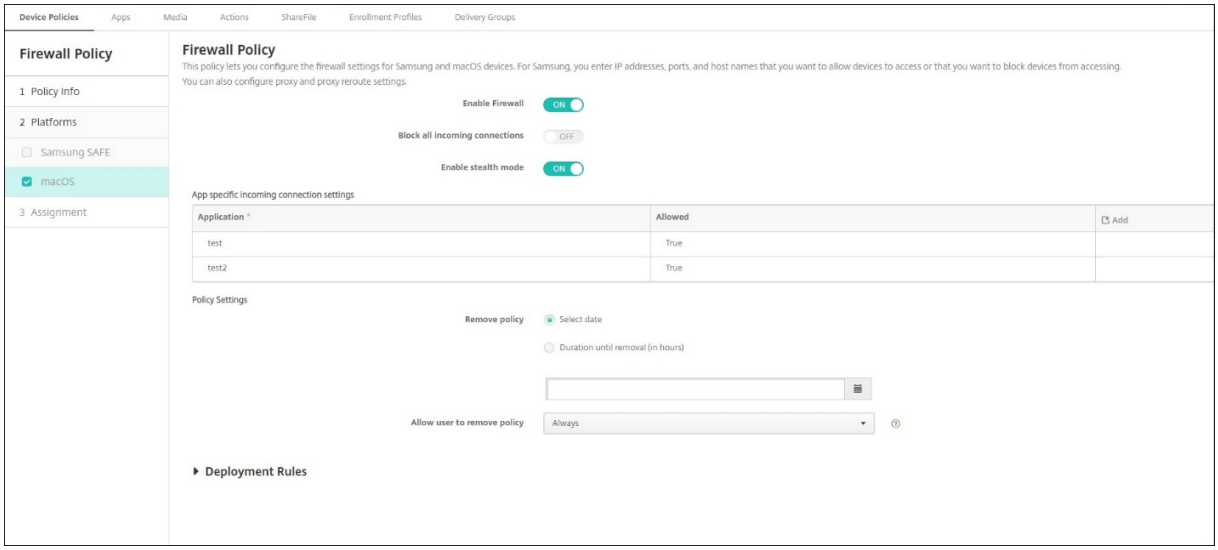
July 7, 2022

Mit dieser Richtlinie können Sie Firewall-Einstellungen für Samsung-, macOS- und Windows-Geräte konfigurieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

macOS-Einstellungen

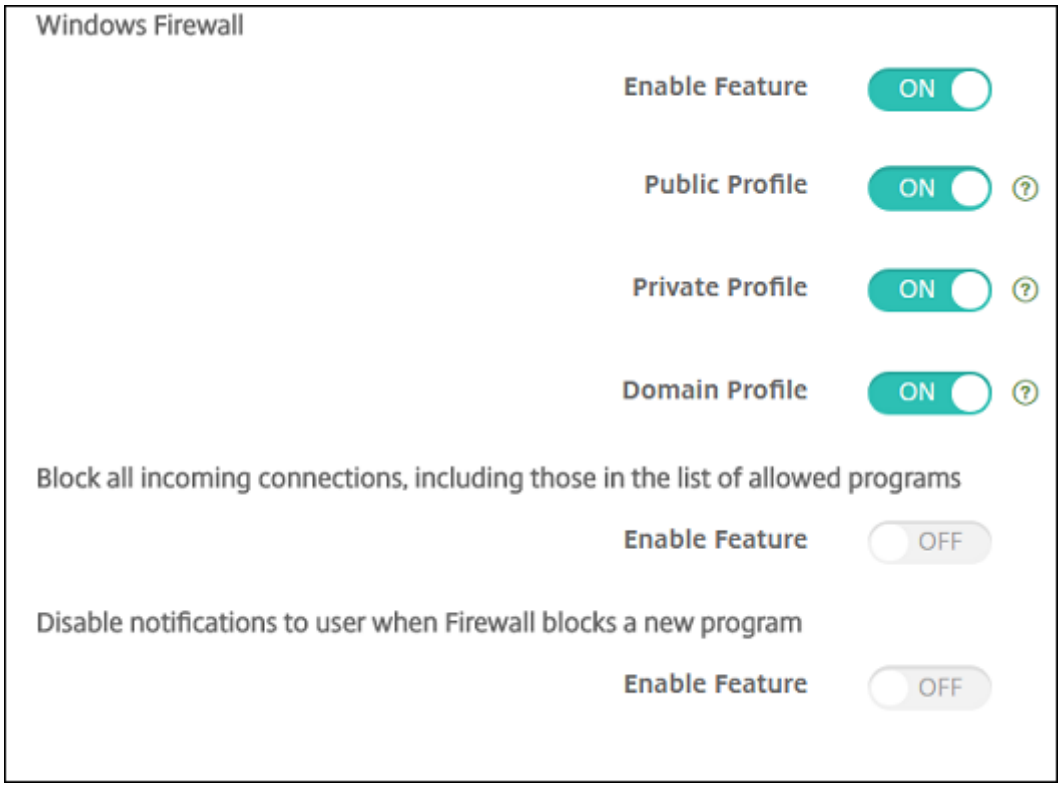
Erfordert macOS 10.12 und höher.



- **Firewall aktivieren:** Legen Sie diese Option auf **Ein** fest, um die Firewall zu aktivieren.
- **Alle eingehende Verbindungen blockieren:** Wenn diese Option auf **Ein** festgelegt ist, werden alle eingehenden Verbindungen blockiert, mit Ausnahme der Verbindungen, die für grundlegende Dienste erforderlich sind.
- **Geschützten Modus aktivieren:** Im geschützten Modus werden Zugriffsversuche aus dem Netzwerk durch Testanwendungen mit ICMP, wie Ping, nicht vom Gerät beantwortet oder anerkannt. Legen Sie diese Option auf **Ein** fest, um den geschützten Modus zu aktivieren.
- **Einstellungen für App-spezifische eingehende Verbindungen:** Um den Verbindungsempfang für bestimmte Apps zuzulassen, fügen Sie die Apps hinzu und legen für **Zugelassen** den Wert **True** fest.

Windows-Desktop-/Tablet-Einstellungen

Erfordert auf Windows Desktop- und Tablet-Geräten Windows 10 (Version 1709 oder höher) oder Windows 11.



- **Feature aktivieren:** steuert den ein- und ausgehenden Datenverkehr auf Computern, auf denen diese Richtlinie bereitgestellt ist. Die Standardeinstellung ist **Ein**.
- **Öffentliches Profil:** steuert die Windows-Firewall, wenn Computer mit einem nicht vertrauenswürdigen Netzwerk im öffentlichen Raum verbunden sind, beispielsweise im Flughafen oder im Café. Die Standardeinstellung ist **Ein**.
- **Privates Profil:** steuert die Windows-Firewall, wenn Computer mit einem vertrauenswürdigen Netzwerk verbunden sind, beispielsweise dem Heimnetzwerk. Die Standardeinstellung ist **Ein**.
- **Domänenprofil:** steuert die Windows-Firewall, wenn Computer mit einem Domänennetzwerk verbunden sind, zum Beispiel am Arbeitsplatz. Die Standardeinstellung ist **Ein**.
- **Alle eingehenden Verbindungen blockieren, einschließlich der zulässigen Programme:** Die Standardeinstellung ist **Aus**.
- **Benachrichtigungen für Benutzer deaktivieren, wenn Firewall neues Programm blockiert:** Die Standardeinstellung ist **Aus**.

Geräterichtlinie für Schriftarten

December 1, 2023

Sie können in Citrix Endpoint Management eine Geräterichtlinie einrichten, mit der zusätzliche Schriftarten auf iOS- und macOS-Geräten hinzugefügt werden. Schriftarten müssen im Format TrueType (`.ttf`) oder OpenType (`.oft`) vorliegen. Schriftartsammlungen (`.ttc` oder `.otc`) werden nicht unterstützt.

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:** Zur Auswahl der Schriftartdatei, die auf den Geräten hinzugefügt werden soll, klicken Sie 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.

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:** Zur Auswahl der Schriftartdatei, die auf den Geräten hinzugefügt werden soll, klicken Sie 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.

Geräterichtlinie für Homebildschirmlayout

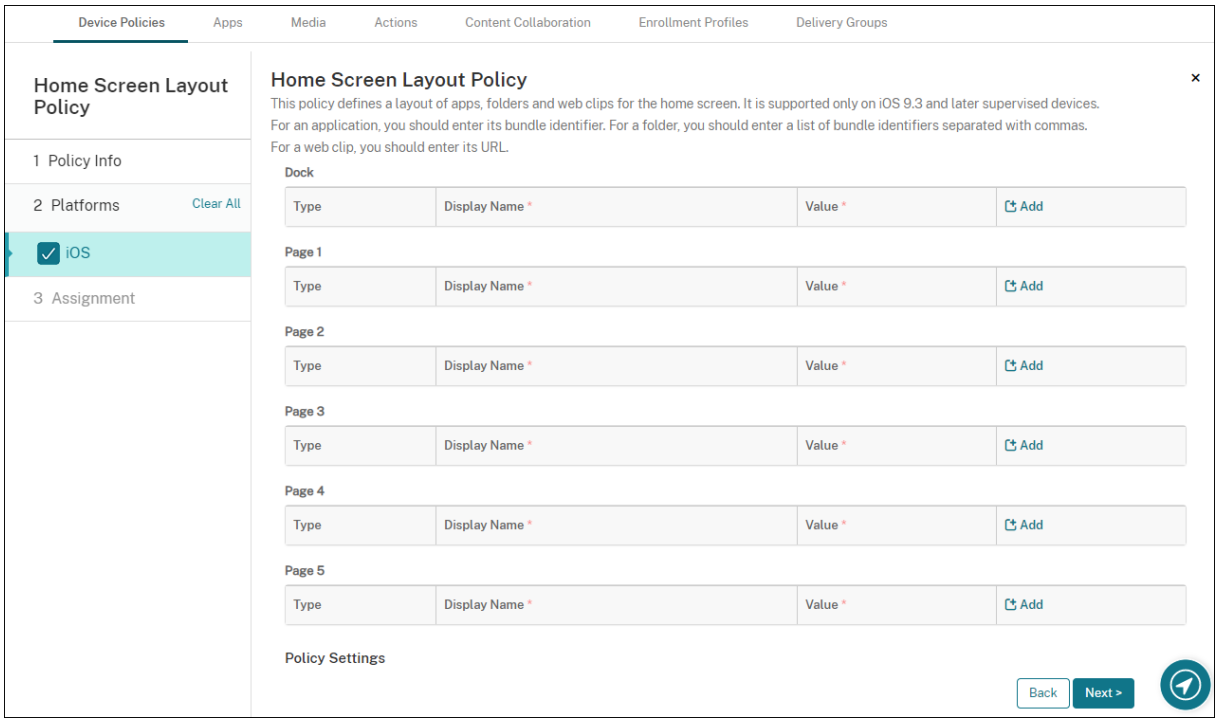
June 25, 2024

Die Geräterichtlinie **Layout für Homebildschirm** ermöglicht das Festlegen des Layouts für Apps und Ordner auf dem iOS-Homebildschirm.

> **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 Citrix Endpoint Management-Richtlinie oder den Apple Configurator definieren.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

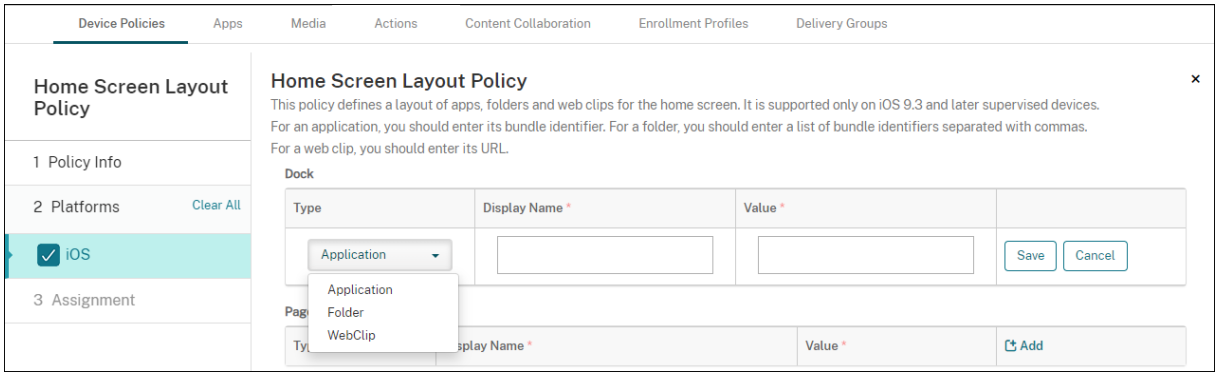
iOS-Einstellungen



- Klicken Sie für jeden der Bildschirmbereiche, die Sie konfigurieren möchten (wie **Dock** oder **Seite 1**) auf **Hinzufügen**.
- **Typ:** Wählen Sie **Anwendung**, **Ordner** oder **Web-Clip**.

  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.
  - **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

June 25, 2024

Sie können XML-Dateien für die Konfiguration von iOS- und macOS-Geräten in Citrix Endpoint Management importieren. Die Datei enthält Gerätesicherheitsrichtlinien und -einschränkungen, die Sie mit Apple Configurator 2 oder Profile Creator vorbereitet haben. Die XML-Konfigurationsdatei kann Makros enthalten. Weitere Informationen finden Sie unter Makros.

Anwendungsfälle

Importieren Sie die folgenden Konfigurationen, die außerhalb von Citrix Endpoint Management für macOS-Geräte mit Profile Creator erstellt wurden:

- **System Policy Control:** Diese Richtlinie kennzeichnet Apps, die von zertifizierten Apple-Entwicklern signiert wurden, und ermöglicht Benutzern den Download verifizierter Apps aus dem Mac App Store.

  Beachten Sie beim Konfigurieren der Richtlinie:

  - Wählen Sie **Enable Gatekeeper**, damit Benutzer nur verifizierte und vertrauenswürdige Software ausführen können.
  - Wählen Sie **Allow Identified Developers**, damit Benutzer nur Apps installieren, die von zertifizierten Apple-Entwicklern signiert sind.

- **Privacy Preferences Policy Control:** Mit dieser Richtlinie können Sie den Zugriff auf bestimmte Dateien oder Features, z. B. Ortungsdienste, Kamerafunktion und Screenshot, anwendungsübergreifend gewähren oder einschränken.

  Konfigurieren Sie die Einstellungen, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter Einstellungen für Payload in der Richtliniensteuerung in der Systemeinstellung "Sicherheit".

- **Kernel Extensions Policy:** Mit dieser Richtlinie können Benutzer App-Erweiterungen installieren, die die systemeigenen Funktionen des Betriebssystems erweitern. Kernel-Erweiterungen werden auf Kernelebene ausgeführt.

  Konfigurieren Sie die Einstellungen, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter Einstellungen der Payload "Richtlinie für Kernel-Erweiterung".

- **Ethernet Settings Policy:** Mit dieser Richtlinie können Sie die Ethernet-Netzwerkverbindung verwalten.

  Konfigurieren Sie die Einstellungen, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter Ethernet-Einstellungen.

Verwenden Sie den Apple Configurator 2 oder Profile Creator, um die folgenden Richtlinien für macOS- und iOS-Geräte zu konfigurieren:

- **Wi-Fi Policy:** Mit dieser Richtlinie können Sie verwalten, wie Benutzer ihre Geräte mit einem Wi-Fi-Netzwerk verbinden.

  Beachten Sie beim Konfigurieren der Richtlinie:

  - Fügen Sie die Ziel-SSID ganz oben in der Prioritätsliste hinzu.

  - Wählen Sie den Verbindungsmodus, der vom Benutzer beim Verbinden mit dem Netzwerk genutzt werden soll. Bei Auswahl von **System** wird der Benutzer mit den Systemanmeldeinformationen authentifiziert. Bei Auswahl von **Anmeldefenster** wird der Benutzer mit den Anmeldeinformationen authentifiziert, die im Anmeldefenster eingegeben wurden.

  Weitere Informationen finden Sie unter Wi-Fi-Einstellungen.

- **Restrictions Policy:** Mit dieser Richtlinie wird die Verwendung bestimmter Features auf Benutzergeräten erlaubt oder beschränkt.

  Konfigurieren Sie die Einstellungen, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter Einschränkungen –Übersicht.

- **VPN Policy:** Diese Richtlinie ermöglicht eine verschlüsselte Verbindung mit privaten Netzwerken auf Geräteebene.

  Konfigurieren Sie die Einstellungen, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter VPN –Übersicht.

Erstellen eines Konfigurationsprofils mit Apple Configurator 2

1. Installieren Sie Apple Configurator 2 aus dem Apple App Store.
2. Starten Sie Apple Configurator 2 und gehen Sie zu **File > New Profile**. Ein neues Konfigurationsfenster wird angezeigt.
3. Geben Sie im Einstellungsbereich **General** einen Namen und eine ID für Ihr Profil ein und fügen Sie zusätzliche Payloadoptionen hinzu.
4. Wählen Sie im linken Bereich eine Payload aus, klicken Sie auf **Configure** und geben Sie die Einstellungen ein. Signieren Sie Ihr Profil nicht, da signierte Profile nicht unterstützt werden.

   Um mehrere Payloads in einem Profil hinzuzufügen, wählen Sie eine Payload aus und klicken rechts oben auf die Schaltfläche **Add Payload**.
5. Gehen Sie zu **File > Save**, wählen Sie einen Namen und Speicherort für die XML-Datei aus und klicken Sie auf **Save**.

Erstellen eines Konfigurationsprofils mit Profile Creator

1. Installieren Sie Profile Creator von GitHub.
2. Starten Sie Profile Creator und gehen Sie zu **File > New**. Ein neues Konfigurationsfenster wird angezeigt.
3. Geben Sie im Einstellungsbereich **General** einen Namen und eine Beschreibung für Ihr Profil ein und fügen Sie zusätzliche Payloadoptionen hinzu.

- Empfehlung: Wählen Sie **Prevent users from removing this profile**.
- Wählen Sie für **Payload Scope** die Option **System** oder **User**.

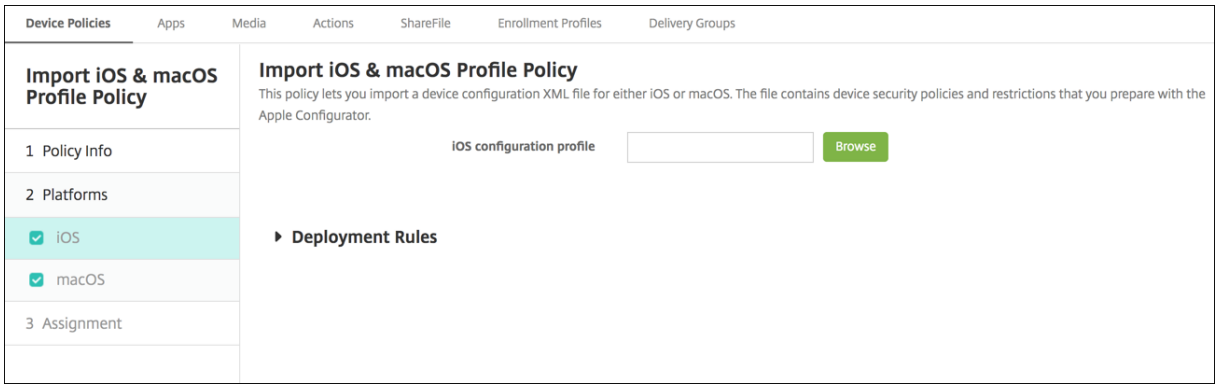
4. Wählen Sie im linken Bereich die Richtlinie aus, konfigurieren Sie die Einstellungen und klicken Sie dann rechts oben auf **Add**.

   Um mehrere Richtlinien in einem Profil zu konfigurieren, wählen Sie eine Richtlinie aus und klicken dann auf die Schaltfläche **Add**.

5. Gehen Sie zu **File > Export**, wählen Sie einen Namen und Speicherort für die XML-Datei aus und klicken Sie auf **Save**.

Um in der Citrix Endpoint Management-Konsole eine Konfigurationsdatei für die Geräterichtlinie des iOS- und macOS-Profils zu importieren, 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.

Geräterichtlinie für die Keyguard-Verwaltung

June 25, 2024

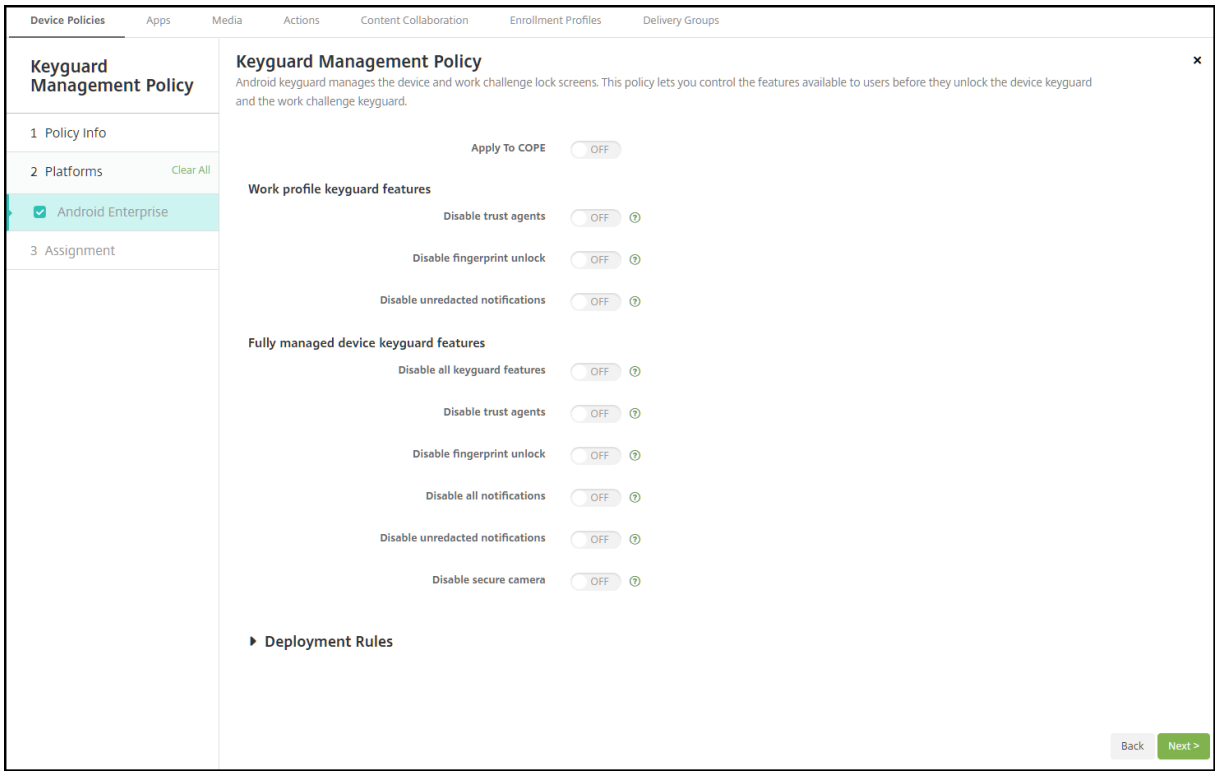
Android Keyguard verwaltet die Sperrbildschirme für Gerät und Arbeitsprofil. Mit dieser Richtlinie können Sie Funktionen für den Android Enterprise Arbeitsprofil-Keyguard und erweiterte Funktionen für den Geräte-Keyguard steuern. Sie können Folgendes steuern:

- 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. Diese Geräte wurden früher als COPE-Geräte (Unternehmenseigentum, vom Benutzer verwaltet) bezeichnet. 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.

Sehen Sie sich dieses Video an, um mehr zu erfahren:

Android Enterprise-Einstellungen



- **Auf COPE 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 **Aus** ist das Entsperren per Fingerabdruck auf sicheren Keyguard-Displays verfügbar, wenn eine Sicherheitsabfrage im Arbeitsprofil festgelegt ist. Mit **Ein** ist das Entsperren per Fingerabdruck im Arbeitsprofil deaktiviert. 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 deaktivierten Features der biometrischen Authentifizierung sind 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

June 25, 2024

Mit der Kioskrichtlinie können Sie Geräte auf den Kioskmodus und ausführbare Apps beschränken. Citrix Endpoint Management 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.

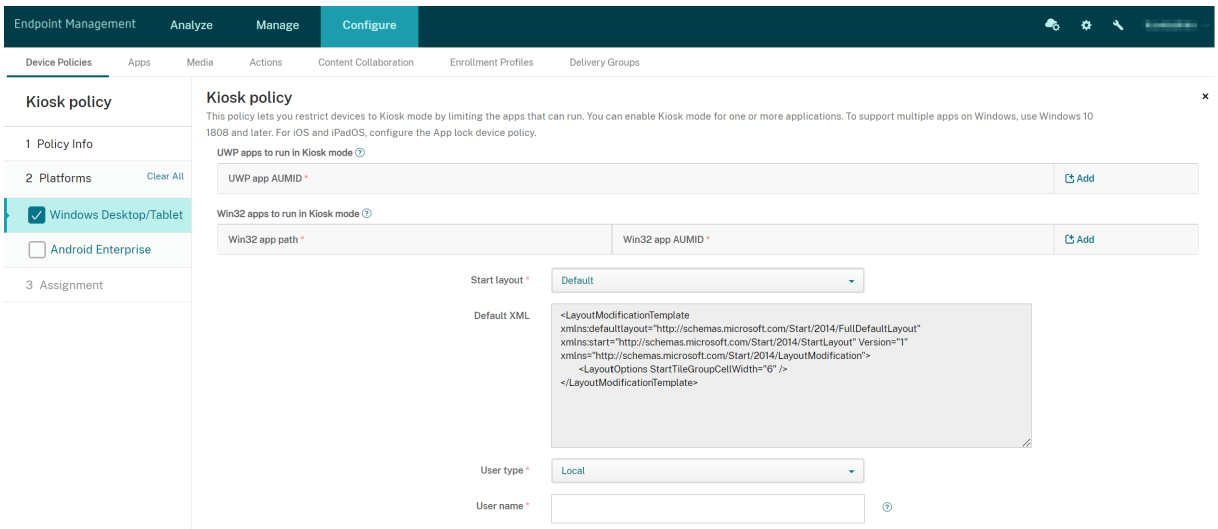
Zum Einrichten von iPads für die Ausführung im Kioskmodus verwenden Sie die Geräterichtlinie zum Sperren von Apps. Informationen zum Einrichten von iPads als Kiosks finden Sie unter Konfigurieren eines iPads als Kiosk. Sie können ein iPad auch so konfigurieren, dass nur eine einzige Website geöffnet wird. Weitere Informationen finden Sie in der Webclip-Richtlinie.

Windows Desktop-/Tablet-Einstellungen

Für Windows-Desktops und -Tablets gilt die Kioskrichtlinie nur für lokale Benutzer und für Benutzer, die in Azure AD registriert sind.

Eine oder mehrere Apps können im Kioskmodus auf Windows- Desktops und -Tablets ausgeführt werden.

> **Hinweis:**
>
> Die Kioskgeräterichtlinie gilt nur für Windows 10-Geräte.
> Um einen Einzel-App-Kiosk auf Windows 11-Geräten bereitzustellen, können Sie die Geräterichtlinie "Benutzerdefiniertes XML"verwenden, um unser XML-Skript für die Geräte bereitzustellen. Weitere Informationen finden Sie unter Bereitstellen eines Einzel-App-Kiosks auf Windows 11-Geräten.



- **UWP App AUMID:** Klicken Sie auf **Hinzufügen**, wählen Sie die UWP-App (Universelle Windows-Plattform) und geben Sie die Anwendungsbenutzermodell-ID (AUMID) für jede UWP-App ein. Geben Sie zum Beispiel die folgende AUMID ein:
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Win32 App Path** und **Win32 App AUMID**: Klicken Sie auf **Hinzufügen**, wählen Sie die Windows-Desktop-App (`Win32`) und geben Sie Pfad und AUMID für jede `Win32`-App ein. Geben Sie zum Beispiel den folgenden Pfad samt AUMID ein:
  - `%windir%\system32\mspaint.exe` oder `C:\Windows\System32\mspaint.exe`
  - `{ 1AC14E77-02E7-4E5D-B744-2EB1AE5198B7 } \mspaint.exe`
- **Startlayout:** Nur der standardmäßige Startbildschirm ist für Apps verfügbar.

- **Standard-XML:** Nur das standardmäßige XML-Skript ist verfügbar.
- **Benutzertyp auswählen:** Geben Sie den Benutzertyp an, der die Kioskrichtlinie empfangen soll. Ihre Optionen:
  - **Lokal:** Citrix Endpoint Management erstellt einen Benutzer für das Zielgerät oder fügt einen vorhandenen Benutzer hinzu.
  - **Azure AD:** Citrix Endpoint Management fügt Benutzer hinzu, die in Azure AD registriert sind.
- **Benutzername:** Geben Sie den Benutzernamen ein, der die Kioskrichtlinie empfangen soll.
  - Um einen lokalen Benutzernamen auf dem Zielgerät zu erstellen, geben Sie den Namen ein. Stellen Sie sicher, dass Ihr lokaler Benutzername nicht über die Domäne verfügt. Wenn Sie einen vorhandenen Namen eingeben, erstellt Citrix Endpoint Management keinen Benutzer und ändert nicht das aktuelle Kennwort.
  - Zum Hinzufügen eines Azure AD-Benutzers geben Sie den Namen im Format `azuread\user` ein. `user` kann dabei der **Name** oder der **Benutzername** sein, der beim Erstellen eines Benutzers in Azure AD eingegeben wurde. Der zugewiesene Benutzer kann kein Azure AD-Administrator sein.
- **Kennwort:** Es gibt keine Kennwortkonfiguration für Azure AD-Benutzer. Geben Sie das Kennwort nur für den lokalen Benutzernamen ein.
- **Taskleiste anzeigen:** Aktivieren Sie die Taskleiste, damit Benutzer Anwendungen leicht anzeigen und verwalten können. Die Standardeinstellung ist **Aus**.
- Klicken Sie auf **Weiter** und speichern Sie die Änderungen.

Für eine UWP-App, die Sie im Kioskmodus zulassen möchten, müssen Sie die AUMID bereitstellen. Um eine Liste der AUMIDs für alle Microsoft Store-Apps abzurufen, die für den aktuellen Gerätebenutzer installiert sind, führen Sie den folgenden PowerShell-Befehl aus.

```
$installedapps = get-AppxPackage

$aumidList = @()
foreach ($app in $installedapps)
{

    foreach ($id in (Get-AppxPackageManifest $app).package.applications
        .application.id)
    {

        $aumidList += $app.packagefamilyname + "!"+ $id
     }

 }


$aumidList
```



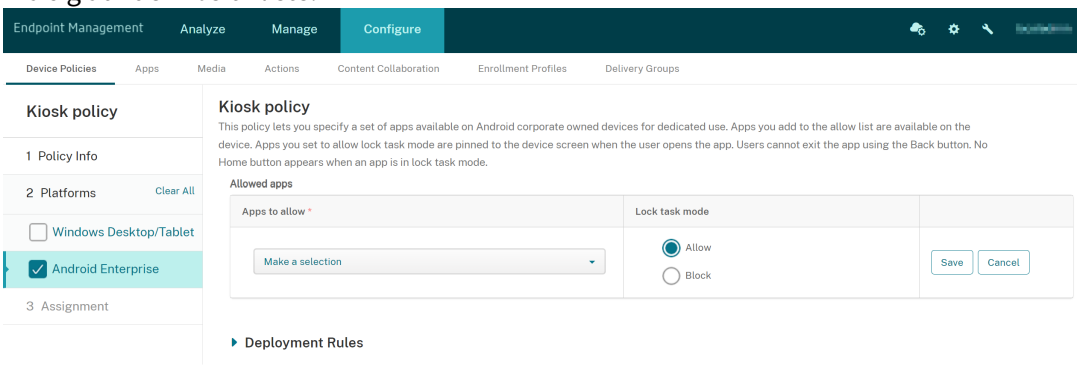
```
<!--NeedCopy-->
```

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.

Um eine App zuzulassen, klicken Sie auf **Hinzufügen**. Sie können der Positivliste mehrere Apps hinzufügen. Weitere Informationen finden Sie unter Android Enterprise.

- **Zulässige Apps:** 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 zugelassenen App in die Liste einzugeben.
  - Wählen Sie die App aus der Liste aus. Die Liste enthält Apps, die in Citrix Endpoint Management hochgeladen wurden. Citrix 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 **Blockieren**, um festzulegen, dass die App nicht angeheftet werden soll. 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.

Knox Platform for Enterprise Key-Geräterichtlinie

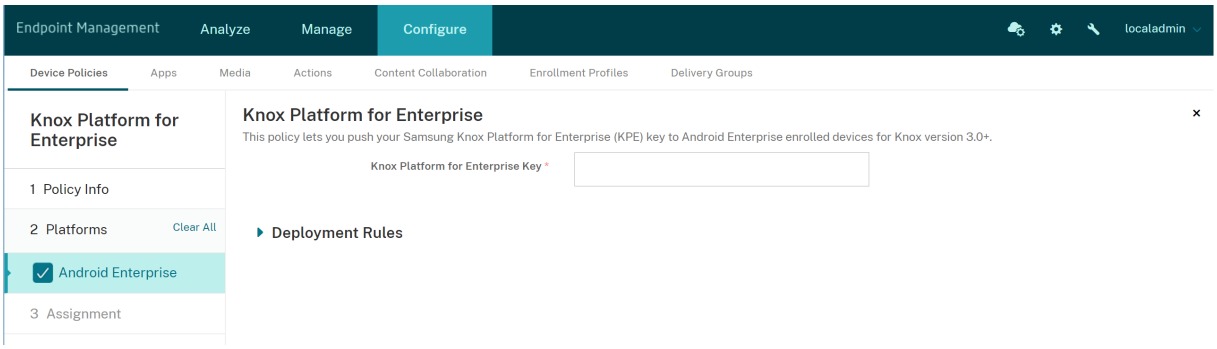
June 25, 2024

Diese Richtlinie ermöglicht es Ihnen, die erforderlichen Samsung Knox Platform for Enterprise-(KPE)-Lizenzinformationen bereitzustellen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren** > **Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android Enterprise-Einstellungen

Diese Richtlinie enthält die erforderlichen Lizenzinformationen für Samsung Knox Platform for Enterprise (KPE). Für Android 12 oder früher müssen Sie eine KPE Premium-Lizenz beantragen, um die Knox-Premium-Funktionen nutzen zu können. Für Android 13 oder höher wird standardmäßig eine KPE Premium-Lizenz bereitgestellt.



Knox Platform for Enterprise Key: Geben Sie den Samsung Knox Platform for Enterprise-(KPE)-Schlüssel ein, den Sie auf das Android Enterprise-Gerät übertragen möchten. Beantragen Sie einen KPE-Lizenzschlüssel unter Samsung Knox Platform for Enterprise-(KPE)-Schlüssel.

Launcher-Konfigurationsrichtlinie

December 1, 2023

Mit Citrix Launcher können Sie die Benutzererfahrung für über Citrix Endpoint Management bereitgestellte Android Enterprise-Geräte und Android-Legacygeräte anpassen.

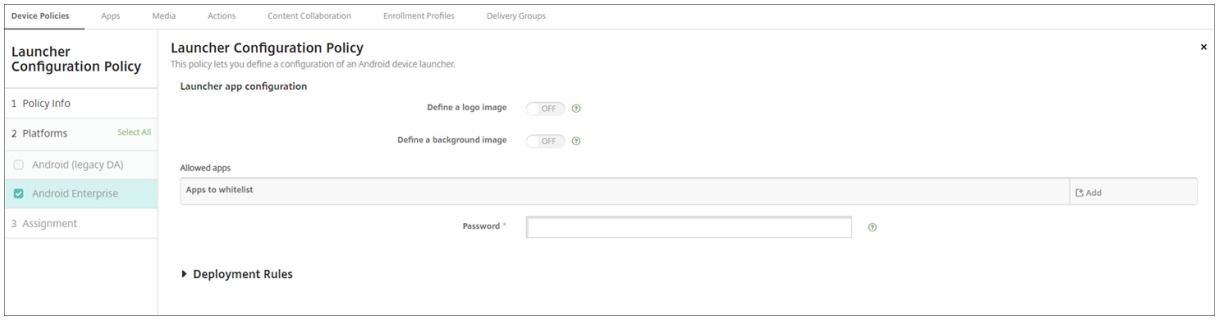
Mit einer Launcher-Konfigurationsrichtlinie steuern Sie folgende Citrix Launcher-Features:

- Verwalten von Android Enterprise-Geräten und Android-Legacygeräten, sodass Benutzer nur auf von Ihnen festgelegte Apps zugreifen können
- Optionale Angabe eines benutzerdefinierten Logos als Citrix Launcher-Symbol sowie eines benutzerdefinierten Hintergrundbilds für Citrix Launcher
- Festlegen eines Kennworts, das Benutzer zum Beenden von Launcher eingeben müssen

Citrix Launcher ist nicht als zusätzliche Sicherheitsstufe gedacht.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Android Enterprise- und Android-Einstellungen



- **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

December 1, 2023

Sie erstellen eine LDAP-Richtlinie für iOS-Geräte in Citrix Endpoint Management, 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. Dieses Feld 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. Dieses Feld 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. Dieses Feld 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.

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. Dieses Feld 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. Dieses Feld 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. Dieses Feld 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.

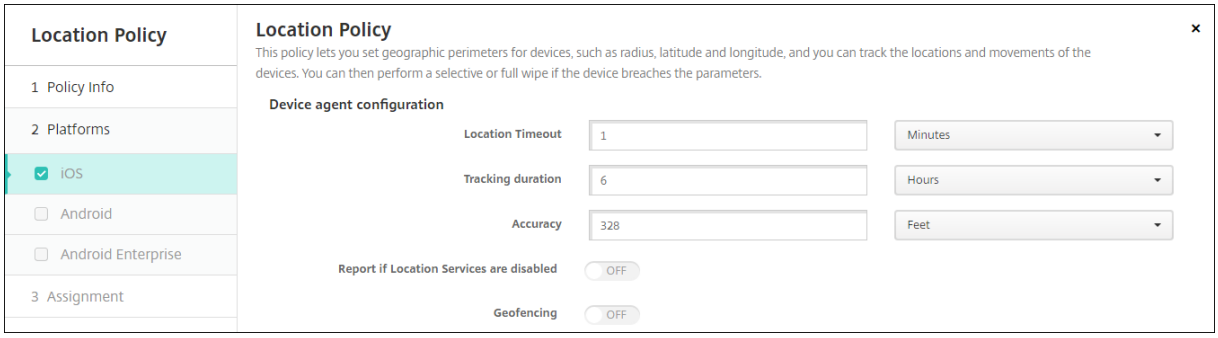
Standortrichtlinie für Geräte

June 25, 2024

Mit einer Standortrichtlinie legen Sie in Citrix Endpoint Management geografische Grenzen fest. Wenn ein Benutzer den durch die Grenze (*Geofence*) festgelegten Bereich verlässt, kann Citrix Endpoint Management 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.

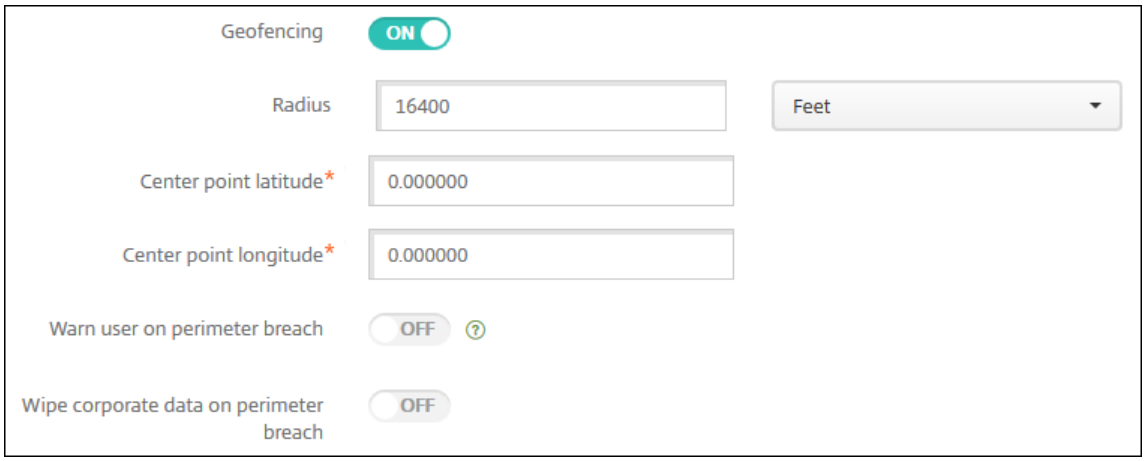
Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen



- **Standorttimeout:** Geben Sie eine Ziffer ein und klicken Sie auf **Sekunden** oder **Minuten**, um festzulegen, wie häufig Citrix Endpoint Management den Gerätestandort abrufen soll. Gültige Werte sind 60-900 Sekunden oder 1-15 Minuten. Die Standardeinstellung ist **1 Minute**.

- **Trackingdauer:** Geben Sie eine Ziffer ein und klicken Sie auf **Stunden** oder **Minuten**, um festzulegen, wie lange Citrix Endpoint Management das Gerät verfolgen soll. Gültige Werte sind 1–10 Stunden oder 10–600 Minuten. Der Standardwert ist **6 Stunden**.
- **Genauigkeit:** Geben Sie eine Ziffer ein und klicken Sie auf **Meter**, **Fuß** oder **Yards**, um festzulegen, wie nahe am Gerät Citrix Endpoint Management das Gerät verfolgen soll. Gültige Werte sind 10–5000 Meter (30–15000 Fuß, 10–5000 Yard). Die Standardeinstellung ist **100 Meter** (**328 Fuß**).
- **Deaktivierte Ortungsdienste melden:** Wählen Sie, ob das Gerät einen Bericht an Citrix Endpoint Management senden soll, wenn der Benutzer das GPS deaktiviert. Die Standardeinstellung ist **Aus**.
- **Geofencing**



Bei Auswahl von Geofencing konfigurieren Sie die folgenden Einstellungen:

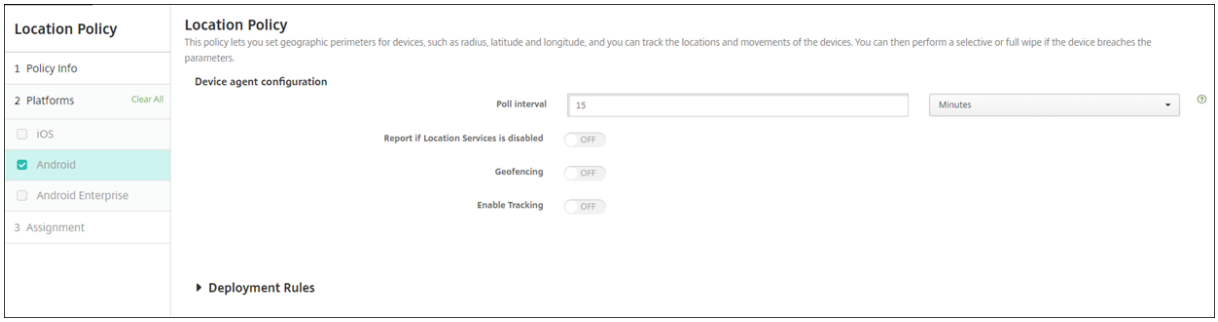
- **Radius:** Geben Sie zur Messung des Radius eine Ziffer ein und klicken Sie auf die zu verwendenden Einheiten. Die Standardeinstellung ist **5000 Meter** (**16400 Fuß**). Gültige Werte für den Radius:
  - 164-16400 Fuß
  - 50-50000 Meter
  - 54-54680 Yard
  - 1–31 Meilen
- **Breitengrad von Mittelpunkt:** 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 Citrix Endpoint Management erforderlich.

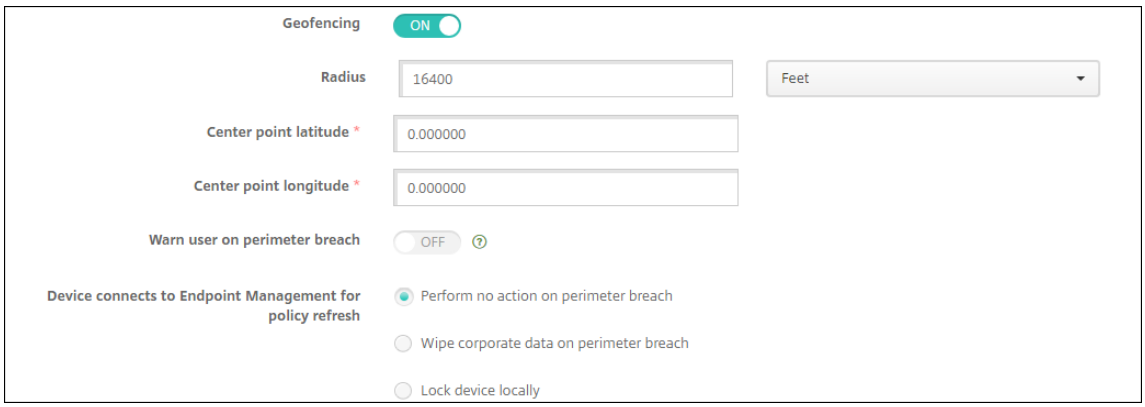
- **Bei Umkreisverletzung Unternehmensdaten löschen:** Wählen Sie aus, ob auf den Geräten bei Verlassen des Bereichs eine Datenlöschung erfolgen soll. Die Standardeinstellung ist **Aus**. Wenn Sie diese Option aktivieren, wird das Feld **Verzögerung beim lokalen Löschen** angezeigt.
  - Geben Sie eine Ziffer ein und klicken Sie 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 Citrix Endpoint Management eine selektive Datenlöschung auf ihrem Gerät durchführt. Die Standardeinstellung ist **0 Sekunden**.

Einstellungen für Android (Legacy-Geräteadministrator)

Die Android-Standortverfolgung erfordert Android ab Version 9.



- **Abrufintervall:** Geben Sie eine Ziffer ein und klicken Sie auf **Minuten**, **Stunden** oder **Tage**, um festzulegen, wie häufig Citrix Endpoint Management den Gerätestandort abrufen soll. Gültige Werte sind 15-1440 Minuten, 1-24 Stunden oder eine beliebige Anzahl an Tagen. Der Standardwert ist **15 Minuten**.
- **Deaktivierte Ortungsdienste melden:** Wählen Sie, ob das Gerät einen Bericht an Citrix Endpoint Management senden soll, wenn der Benutzer das GPS deaktiviert. 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 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.
- **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 Citrix Endpoint Management erforderlich.
- **Gerät mit Citrix Endpoint Management 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 festzule-

gen. Durch die Verzögerung haben Benutzer die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor Citrix Endpoint Management eine selektive Datenlöschung auf ihrem Gerät durchführt. Die Standardeinstellung ist **0 Sekunden**.

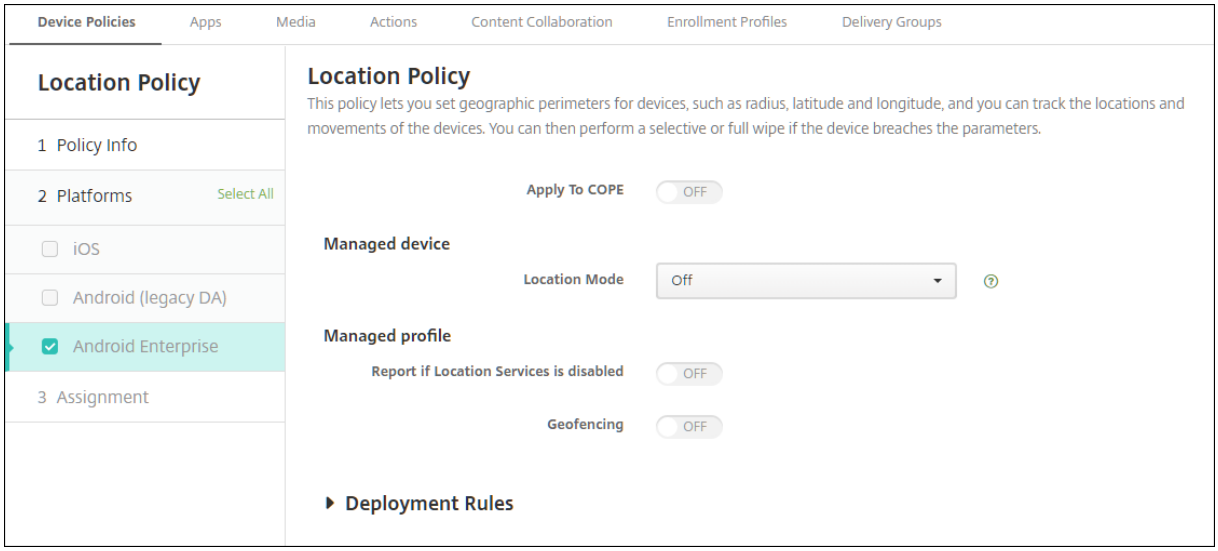
- **Gerät lokal sperren:** Sperren Sie die Geräte der Benutzer nach einer bestimmten Zeit. Wenn Sie diese Option aktivieren, wird das Feld **Verzögerung beim Sperren** angezeigt.
  - Geben Sie eine Ziffer ein und klicken Sie auf **Sekunden** oder **Minuten**, um die Dauer der Verzögerung bis zum Sperren der Geräte festzulegen. Durch die Verzögerung haben Benutzer die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor Citrix Endpoint Management die Geräte sperrt. Die Standardeinstellung ist **0 Sekunden**.

- **Tracking aktivieren:** Wählen Sie aus, ob das Gerät den Benutzerstandort verfolgt. Die Standardeinstellung ist **Aus**.

Android Enterprise-Einstellungen

Damit die Android-Standortverfolgung funktioniert, müssen die folgenden Anforderungen erfüllt sein:

- Android 9 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

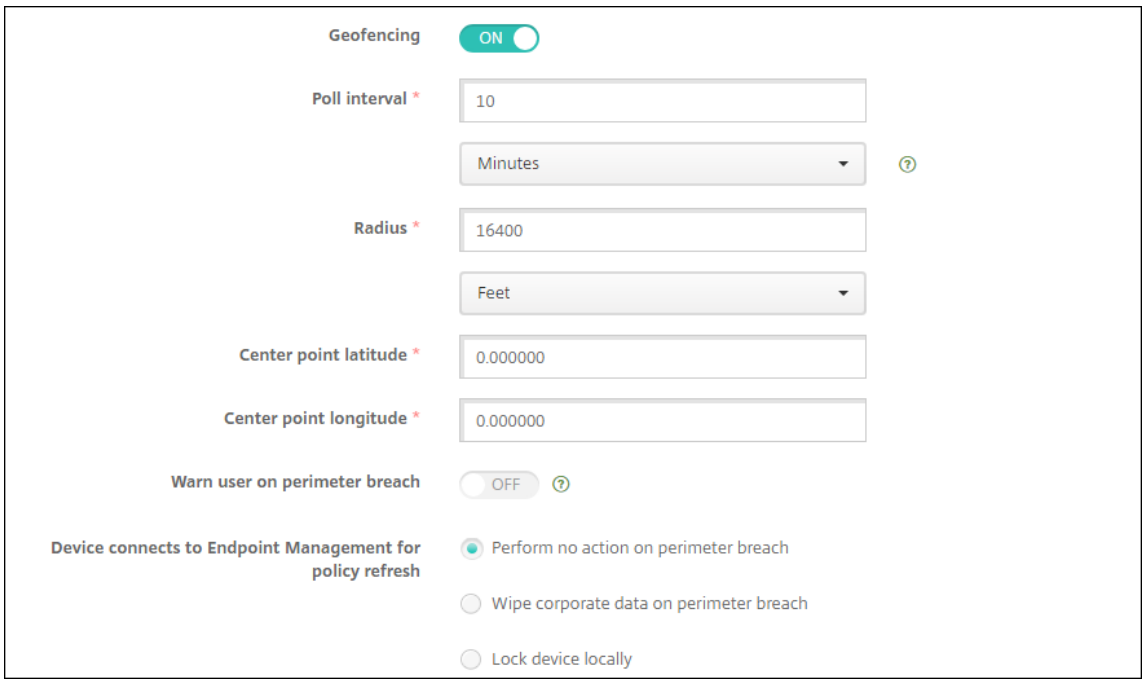
Für vollständig verwaltete Geräte mit Arbeitsprofil (ehemals COPE-Geräte genannt) ist nur die Einstellung "Standortmodus"verfügbar.

- **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 das Arbeitsprofil:
  - **Deaktivierte Ortungsdienste melden:** Wählen Sie, ob das Gerät einen Bericht an Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management erforderlich.
- **Gerät mit Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management die Geräte sperrt. Die Standardeinstellung ist **0 Sekunden**.

Arbeitsprofil

- **Deaktivierte Ortungsdienste melden:** Wählen Sie, ob das Gerät einen Bericht an Citrix Endpoint Management senden soll, wenn der Benutzer das GPS deaktiviert. Die Standardeinstellung ist **Aus**.
- **Geofencing:** Siehe Einstellungen unter Verwaltetes Gerät.

Geräterichtlinie "Meldung auf Sperrbildschirm"

June 25, 2024

Mit der Geräterichtlinie **Meldung auf Sperrbildschirm** können Sie Meldungen festlegen, die beim Verlust folgender iOS-Geräte angezeigt werden:

- Im Anmeldefenster freigegebener iPads
- Auf dem Sperrbildschirm überwachter iOS-Geräte

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Bestandskennzeicheninfo für das Gerät:** das Bestandskennzeichen für das Gerät. Da lange Zeichenfolgen auf Apple-Geräten abgeschnitten werden, sollten Sie die Zeichenfolge vor einer Bereitstellung in der Produktion unbedingt testen. Die zulässige Länge der Zeichenfolge hängt vom Apple-Gerätemodell und den Apple-Einstellungen ab, die sich ändern können.
- **Fußnote für Anmeldefenster und Sperrbildschirm:** Informationen, die eine Rückgabe des Geräts ermöglichen, zum Beispiel eine Adresse oder andere Kontaktinformationen. Beispiel: "Bei Verlust bitte abgeben bei…". Da lange Zeichenfolgen auf Apple-Geräten abgeschnitten werden, sollten Sie die Zeichenfolge vor einer Bereitstellung in der Produktion unbedingt testen. Die zulässige Länge der Zeichenfolge hängt vom Apple-Gerätemodell und den Apple-Einstellungen ab, die sich ändern können.
- **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.

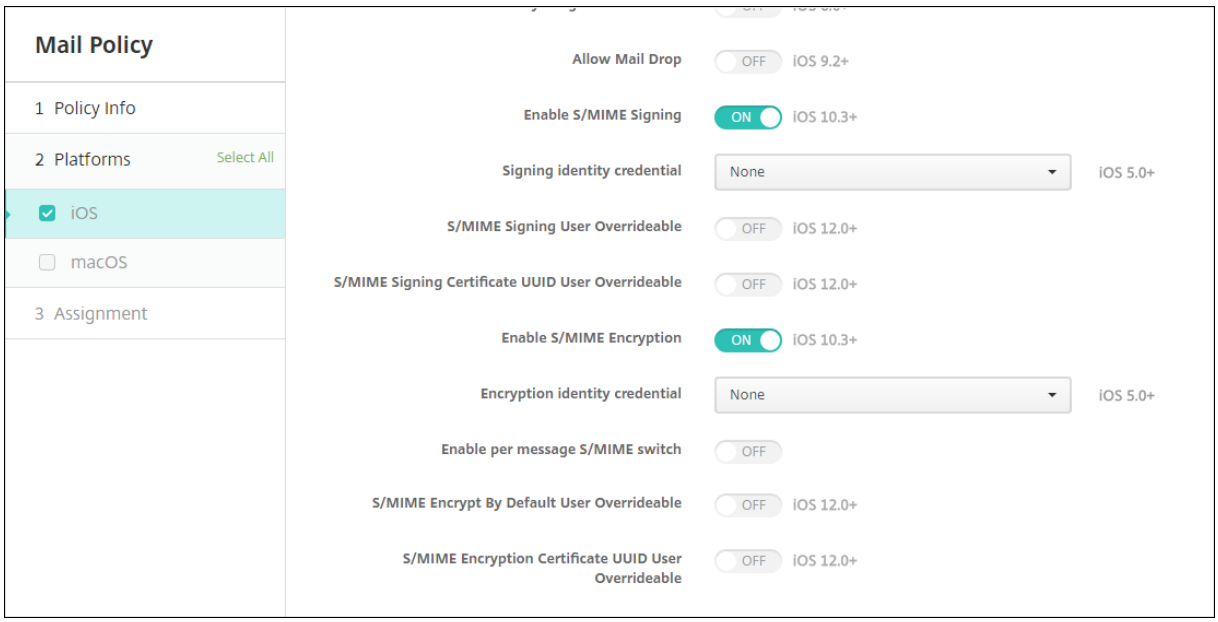
E-Mail-Geräterichtlinie

June 25, 2024

Sie können in Citrix Endpoint Management 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. Dieses Feld 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. Dieses Feld ist erforderlich.
- **Anzeigename für Benutzer:** Geben Sie den vollständigen Benutzernamen zur Anzeige in Nachrichten usw. an. Dieses Feld ist erforderlich.
- **E-Mail-Adresse:** Geben Sie die vollständige E-Mail-Adresse für das Konto ein. Dieses Feld 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. Dieses Feld ist erforderlich.
  - **Port des E-Mail-Servers:** Geben Sie die Portnummer des Servers für eingehende E-Mails ein. Die Standardeinstellung ist **143**. Dieses Feld 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. Dieses Feld 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. Dieses Feld 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. Dieses Feld 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 an, ob Benutzer
    * E-Mail von diesem Konto in ein anderes Konto verschieben
    * E-Mail von einem anderen Konto aus weiterleiten
    * oder 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)** legen Sie fest, dass die Richtlinie später 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. Nur für macOS verfügbar.
  - **Profilbereich:** Wählen Sie aus, ob die Richtlinie pro **Benutzer** oder für das gesamte **System** angewendet wird (nur für macOS).

Richtlinie für verwaltete Konfigurationen

June 25, 2024

Mit der Richtlinie für verwaltete Konfigurationen können Sie verschiedene App-Konfigurationsoptionen

und App-Einschränkungen steuern. Sie erstellen diese Richtlinie für jede Android Enterprise-App, die Sie steuern möchten.

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 Citrix Endpoint Management-Makro. Weitere Informationen finden Sie unter Remote configuration overview(auf der Android-Entwicklerwebsite) und Makros.

Die App-Konfigurationseinstellungen können folgende Elemente umfassen:

- E-Mail-App-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.

> **Hinweis:**
>
> Citrix SSO für Android heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation, um diese Namensänderung widerzuspiegeln.

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.
- Fügen Sie Android Enterprise-Apps in Citrix Endpoint Management hinzu. Weitere Informationen finden Sie unter Hinzufügen von Apps in Citrix Endpoint Management.

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 Android Enterprise zu erstellen, müssen Sie zusätzlich zur Konfiguration der Geräterichtlinie für verwaltete Konfigurationen weitere Schritte ausführen. Außerdem müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- On-Premises NetScaler 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 NetScaler Gateway.

Einschränkungen

Die folgenden Einschränkungen gelten für Pro-App-VPNs auf Android 11+-Geräten in einer Android Enterprise-Umgebung verwenden, aufgrund von Paketsichtbarkeitsbeschränkungen, die in Android 11 eingeführt wurden:

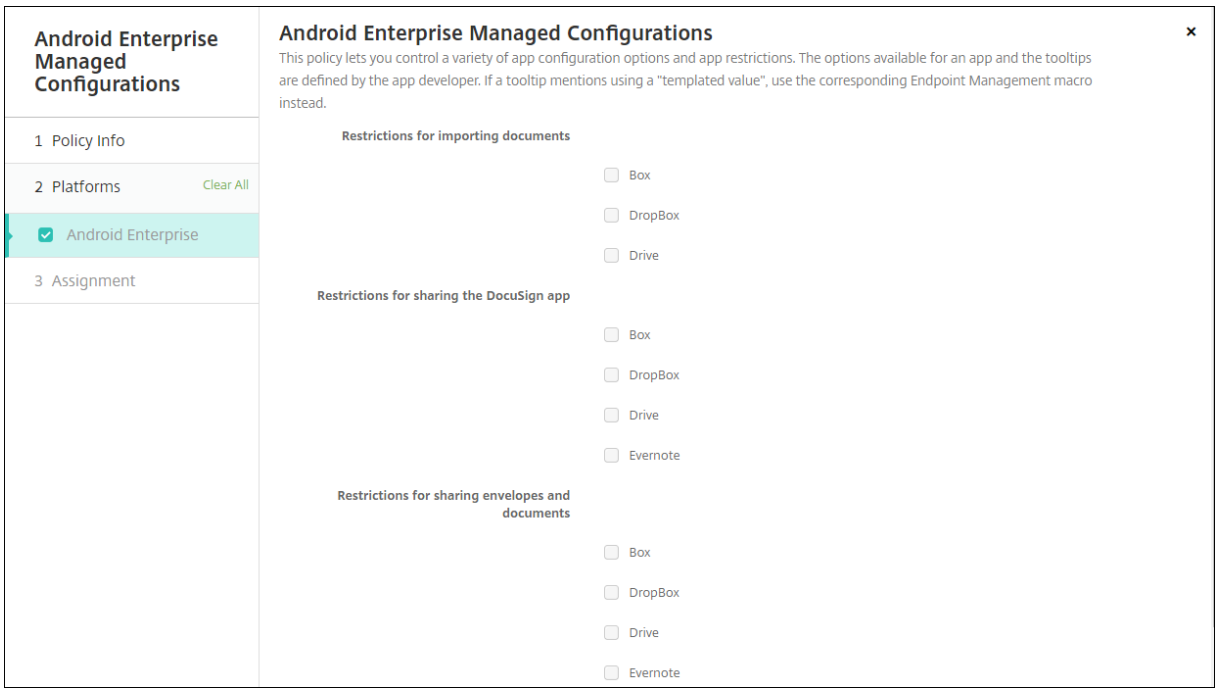
- Wenn eine App aus der Liste der erlaubten/verweigerten Apps nach VPN-Sitzungsstart auf einem Gerät bereitgestellt wird, muss der Benutzer die VPN-Sitzung neu starten, damit der App-Datenverkehr durch die VPN-Sitzung geleitet werden kann.
- Wenn ein Pro-App-VPN über eine Always-On-VPN-Sitzung verwendet wird, muss der Benutzer nach der Installation einer neuen App auf dem Gerät das Arbeitsprofil oder das Gerät neu starten, damit der App-Datenverkehr durch die VPN-Sitzung geleitet werden kann.

> **Hinweis:**
>
> Diese Einschränkungen gelten nicht bei Verwendung von Citrix SSO für Android 23.8.1 oder höher. Weitere Informationen finden Sie unter Automatic restart of Always On VPN.

Android Enterprise-Einstellungen

Nachdem Sie eine Richtlinie für verwaltete Konfigurationen hinzugefügt haben, werden Sie zur Auswahl einer App aufgefordert. Wenn Citrix Endpoint Management keine Android Enterprise-Apps hinzugefügt wurden, können Sie nicht fortfahren.

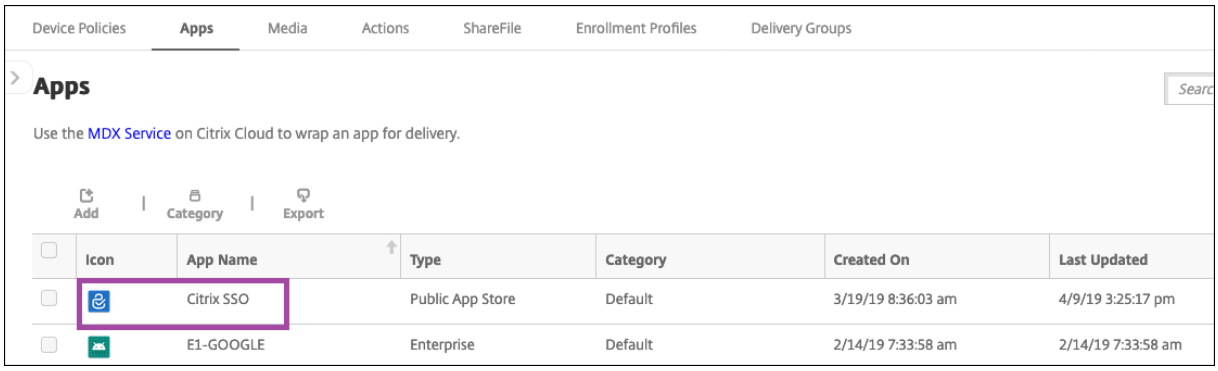
Nachdem Sie eine App ausgewählt haben, konfigurieren Sie die Richtlinieneinstellungen. Die Einstellungen sind App-spezifisch.



Konfigurieren von VPN-Profilen für Android Enterprise

Stellen Sie VPN-Profile auf Android Enterprise-Geräten mit der Citrix SSO-App und der Geräterichtlinie für verwaltete Konfigurationen bereit.

Fügen Sie zunächst Citrix SSO als Google Play Store-App zur Citrix Endpoint Management-Konsole hinzu (siehe Hinzufügen von Apps aus einem öffentlichen App-Store).



Sehen Sie sich dieses Video an, um mehr zu erfahren:

Erstellen einer verwalteten Android Enterprise-Konfiguration für Citrix SSO

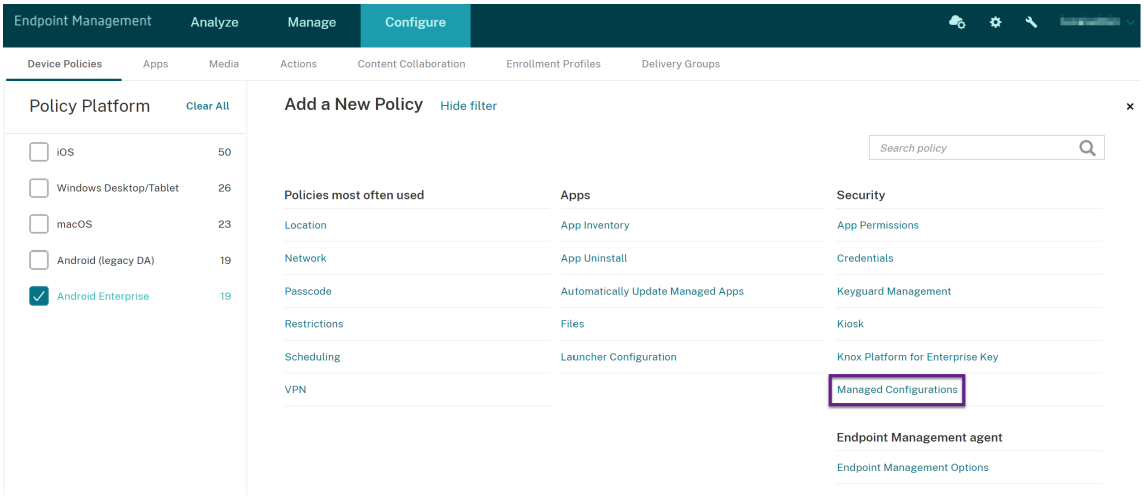
Konfigurieren Sie zum Erstellen von VPN-Profilen die Geräterichtlinie für verwaltete Konfigurationen für Citrix SSO. Geräte mit installierter Citrix SSO-App und bereitgestellter Richtlinie können auf die von Ihnen erstellten VPN-Profile zugreifen.

Unter folgenden Bedingungen verwendet Citrix Endpoint Management das Benutzerzertifikat im Geräteschlüsselspeicher:

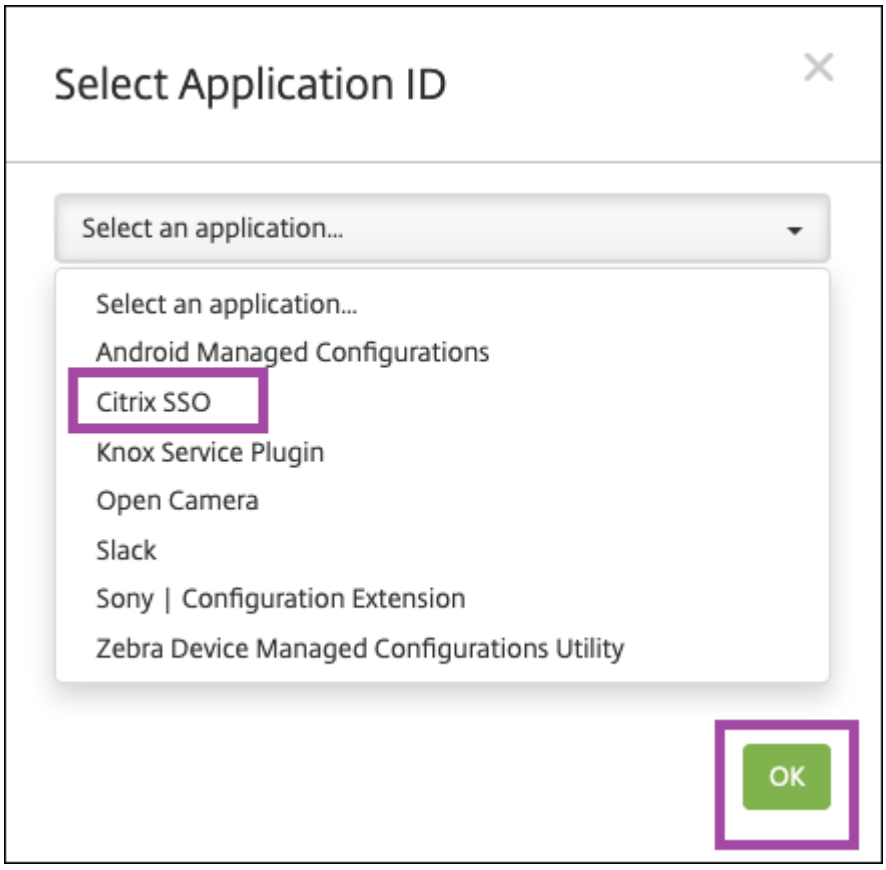
- NetScaler Gateway ist für die zertifikatbasierte Authentifizierung konfiguriert.
- **Benutzerzertifikat für Authentifizierung bereitstellen** ist in Citrix Endpoint Management auf der Seite **Einstellungen > NetScaler Gateway** aktiviert.

Sie benötigen Ihren NetScaler Gateway-FQDN und -Port.

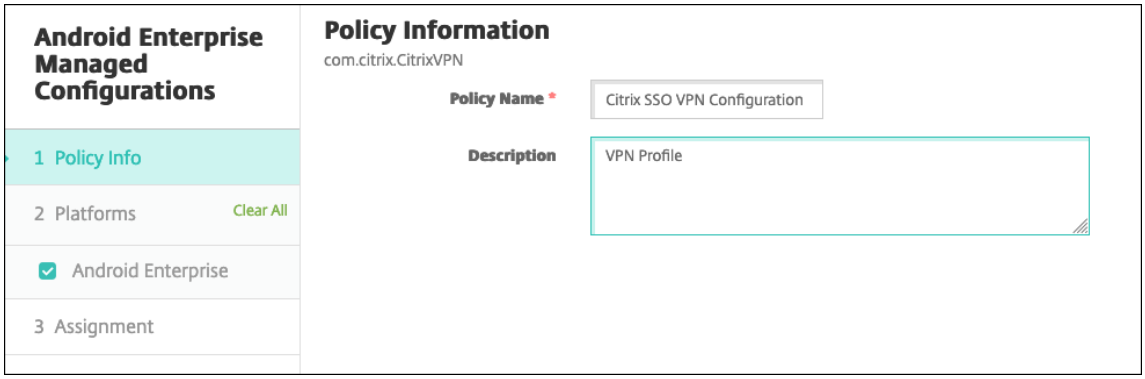
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Geräterichtlinien**. Klicken Sie auf **Hinzufügen**.
2. Wählen Sie **Android Enterprise**. Klicken Sie auf **Verwaltete Konfigurationen**.



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**.



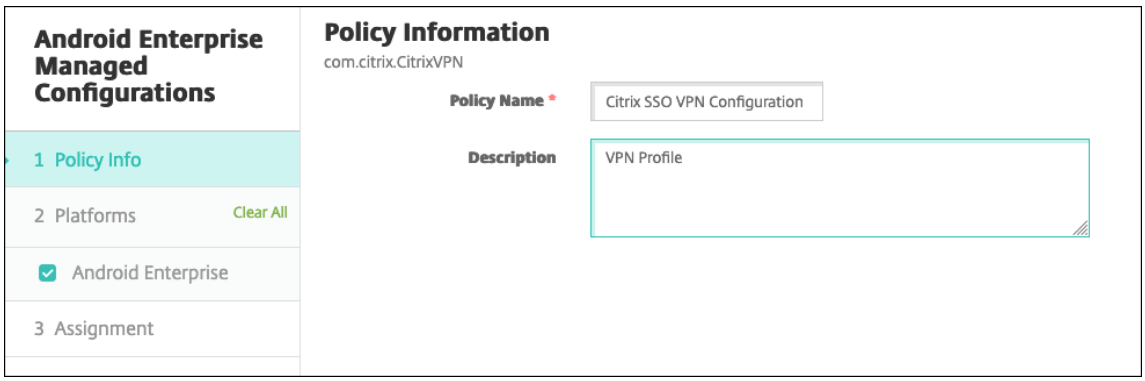
5. Konfigurieren Sie VPN-Profilparameter.

   - **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 NetScaler Gateway-FQDN ein. Geben Sie auch den NetScaler 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 NetScaler Gateway verwenden. Sie können für dieses Feld auch das Citrix Endpoint Management-Makro {user.username} verwenden. (Siehe Makros.) Wenn Sie keinen Benutzernamen angeben, werden Benutzer beim Herstellen einer Verbindung mit NetScaler Gateway aufgefordert, einen Benutzernamen anzugeben.
   - **Kennwort (optional):** Geben Sie das Kennwort an, das Endbenutzer für die Authentifizierung beim NetScaler Gateway verwenden. Wenn Sie kein Kennwort angeben, werden Benutzer beim Herstellen einer Verbindung mit NetScaler Gateway aufgefordert, ein Kennwort anzugeben.
   - **Zertifikatalias (optional):** Geben Sie einen 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.
   - **Angeheftete Gateway-Zertifikate (optional):** JSON-Objekt, das die angehefteten Zertifikate für NetScaler Gateway beschreibt. Beispielwert: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`. Weitere Informationen finden Sie unter NetScaler Gateway certificate pinning with Android Citrix SSO.
   - **Pro-App-VPN-Typ (optional):** Wenn Sie mit Pro-App-VPN beschränken, welche Apps das

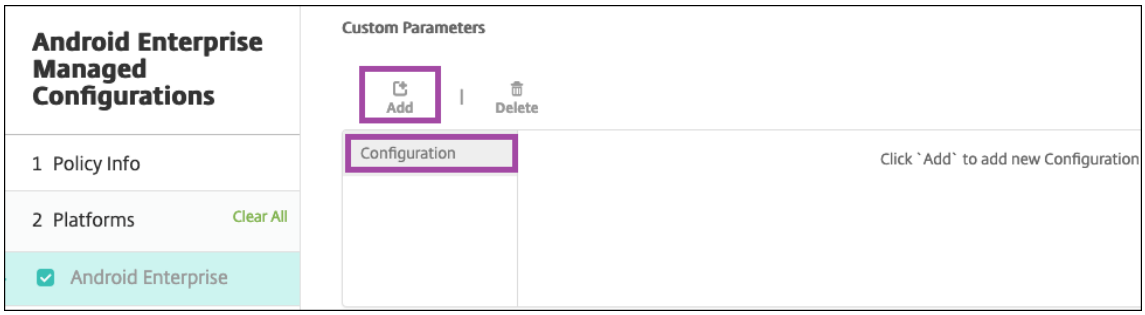
VPN verwenden, können Sie diese Einstellung konfigurieren. Bei Auswahl von **Zulassen** wird der Netzwerkdatenverkehr für die in der **App-Liste für Pro-App-VPN** aufgeführten App-Paketnamen über das VPN geleitet. Der Netzwerkverkehr aller anderen Apps wird nicht über das VPN geleitet. Bei Auswahl von **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 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.
- **Always On VPN (optional):** Dieses Attribut gibt an, ob das VPN-Profil als Always-On-VPN-Profil konfiguriert ist. Wenn der Wert auf **true** gesetzt ist, bedeutet dies, dass das VPN-Profil ein Always-On-VPN-Profil ist. Der Standardwert ist **False**. Diese Eigenschaft kann nur dem Haupt-VPN-Profil zugewiesen werden. Die Aktivierung dieser Eigenschaft ist unerlässlich, um das zuverlässige Funktionieren von Always On VPN sicherzustellen.
- **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:** Diese Einstellung ist in den folgenden Szenarios auf "Aus"gesetzt:
  - Sie verwenden ein selbstsigniertes Zertifikat für NetScaler Gateway
  - Das Stammzertifikat für die Zertifizierungsstelle, die das NetScaler Gateway-Zertifikat ausstellt, ist nicht in der Liste der Systemzertifizierungsstellen aufgeführt.

  Bei der Einstellung "Ein"wird das NetScaler Gateway-Zertifikat vom Android-Betriebssystem überprüft. Wenn die Validierung fehlschlägt, wird die Verbindung nicht zugelassen. Der Standardwert ist Ein.

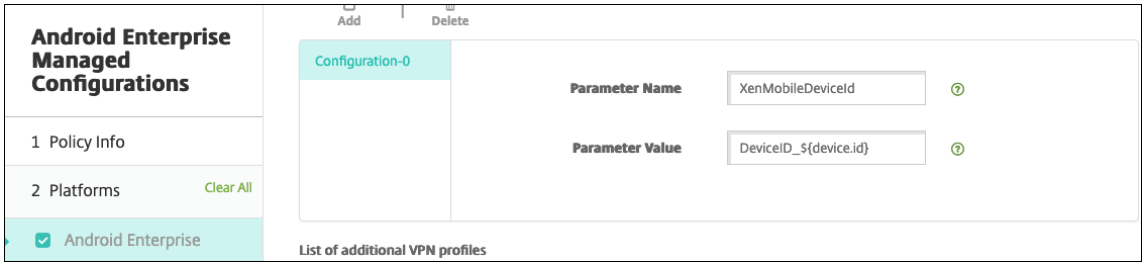


6. Optional können Sie benutzerdefinierte Parameter erstellen. Die benutzerdefinierten Parameter **XenMobileDeviceId** und **UserAgent** werden unterstützt. Wählen Sie die aktuelle VPN-Konfiguration und klicken Sie auf **Hinzufügen**.



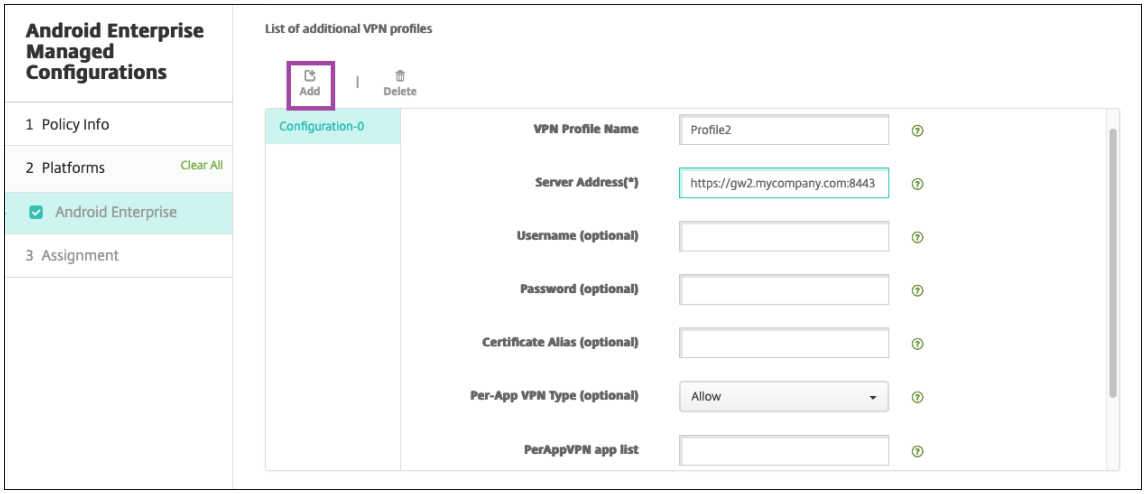
Parametername	Beschreibung	Wert
XenMobileDeviceId	Dies ist die Geräte-ID, die für die Netzwerkzugriffsprüfung basierend auf der Geräteregistrierung in Citrix Endpoint Management verwendet wird. Wenn das Gerät von Citrix Endpoint Management registriert und verwaltet wird, wird die VPN-Verbindung zugelassen. Andernfalls schlägt die Authentifizierung bei der VPN-Einrichtung fehl.	Damit der Registrierungs- und Verwaltungsstatus von Geräten in Citrix Endpoint Management bestimmt werden kann, wird der Wert für XenMobileDeviceID auf `DeviceID_${ device.id }` festgelegt.

Parametername	Beschreibung	Wert
UserAgent	Dieser Text wird zur zusätzlichen Prüfung von NetScaler Gateway an den User-Agent-HTTP-Header angehängt. Der Wert dieses Textes wird während der Kommunikation mit NetScaler Gateway von der Citrix SSO-App an den User-Agent-HTTP-Header angehängt.	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.
EnableDebugLogging	Debug-Protokollierung in der Citrix SSO-App aktivieren, um VPN-Verbindungsprobleme bei Always-On-VPN zu beheben. Sie können es in einer beliebigen verwalteten VPN-Konfiguration aktivieren. Die Debug-Protokollierung wird wirksam, wenn die verwalteten Konfigurationen verarbeitet werden.	**True**: Aktiviert die Debug-Protokollierung. Standardwert: **False**



Zum Erstellen eines weiteren benutzerdefinierten Parameters klicken Sie erneut auf **Hinzufügen**.

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.

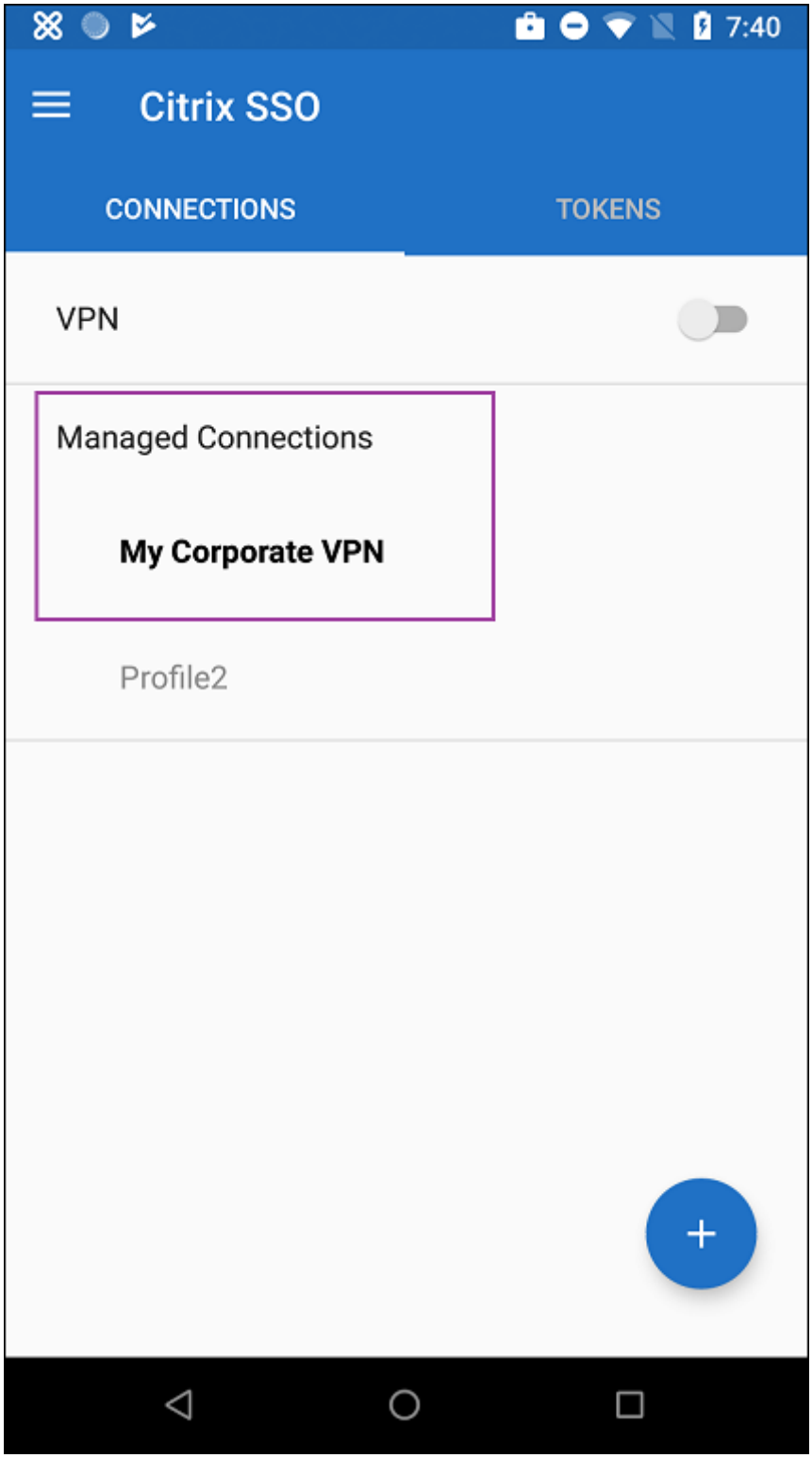
Zum Aktivieren von Always-On für die konfigurierten VPN-Profile, setzen Sie die Citrix Endpoint Management-Optionsrichtlinie für Geräte.

> **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 verwalteten 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.

Citrix Endpoint Management 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.

Wir unterstützen derzeit die folgenden Zebra-Geräte:

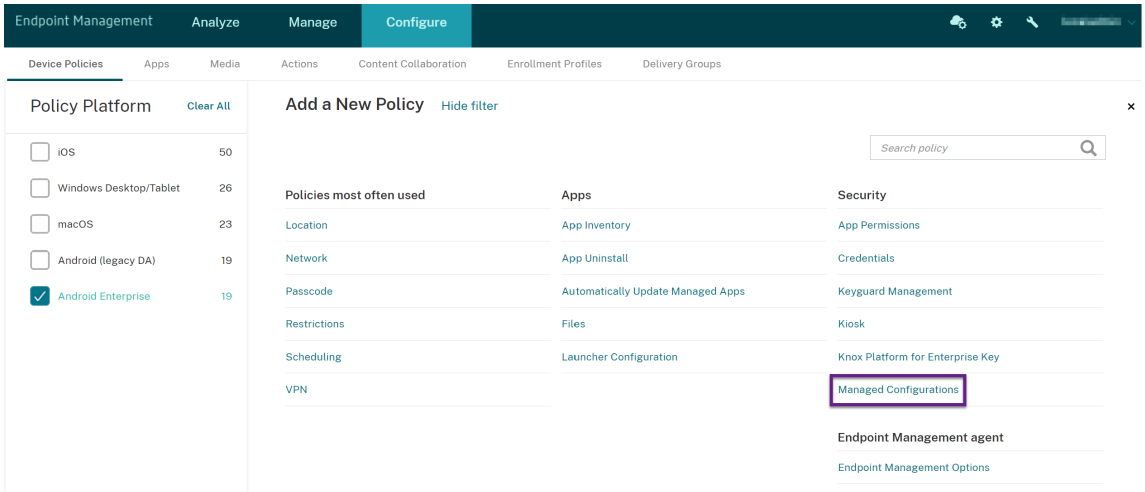
- EC50, EC55, ET56
- TC52x, TC52x-HC
- TC52ax, TC52ax-HC
- TC57x

Fügen Sie zunächst Zebra OEMConfig in der Citrix Endpoint Management-Konsole als Google Play Store-App 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 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 Citrix Endpoint Management-Konsole auf **Konfigurieren > Geräterichtlinien**. Klicken Sie auf **Hinzufügen**.
2. Wählen Sie **Android Enterprise**. Klicken Sie auf **Verwaltete 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** (12-Stunden-Format) oder **24** (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**.

Geräterichtlinie für verwaltete Domänen

September 20, 2021

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 iOS-Geräte geben Sie Folgendes an:

- URLs oder Unterdomänen, die steuern, wie Benutzer Dokumente, Anlagen und über Browser heruntergeladene Objekte öffnen können.
- URLs, für die Benutzer Kennwörter in Safari speichern können.

Die Schrittfolge, mit der Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Bereitstellen von Geräten mit Apple Configurator 2.

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`.

Format	Beschreibung
`\*.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.

Geräterichtlinie für die maximale Anzahl residenter Benutzer

December 1, 2023

Die Richtlinie "Maximale Anzahl residenter Benutzer"gilt für gemeinsam genutzte iOS/iPadOS-Geräte. Weitere Informationen über gemeinsam genutzte iPads finden Sie unter Integration von Apple Bildung-Features.

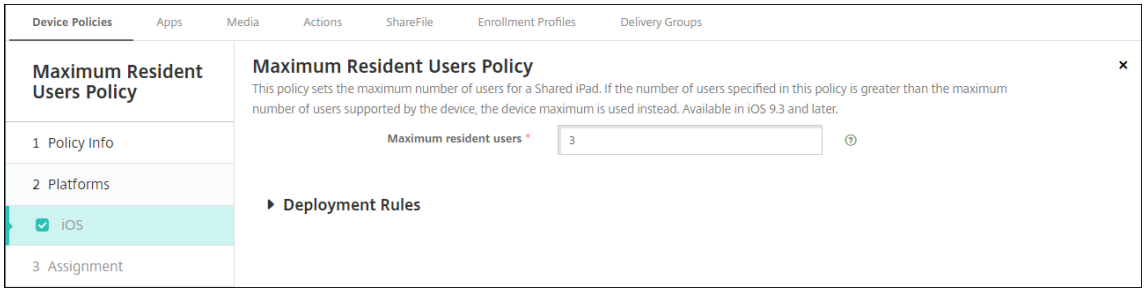
Diese Richtlinie muss bereitgestellt werden, wenn sich das iPad in der Phase "Warten auf Konfiguration"des Setupassistenten befindet. Apple gestattet die Bereitstellung dieser Richtlinie nicht, nachdem geteilte iPads registriert wurden.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Maximale Anzahl residenter Benutzer:** die maximale Anzahl von Benutzern für ein geteiltes iPad. Übersteigt die in dieser Richtlinie angegebene Anzahl Benutzer die maximale, von dem Gerät unterstützte Anzahl, verwendet Citrix Endpoint Management die maximal von dem Gerät unterstützte Anzahl. Der Standardwert ist **5** Benutzer.

  Apple empfiehlt, die maximale Anzahl residenter Benutzer möglichst niedrig zu wählen. Durch einen niedrigen Wert wird die Menge an iPad-Speicher für die einzelnen Benutzer maximiert. Außerdem ist dann weniger Kommunikation mit iCloud erforderlich und die Anmeldung erfolgt schneller. Informationen zur Verteilung von Speicher auf geteilten iPads durch Apple finden Sie unter https://developer.apple.com/education/shared-ipad/.



MDM-Optionsrichtlinien für Geräte

December 1, 2023

Mit der MDM-Richtlinie wird die Aktivierungssperre des Features "Mein iPhone/iPad suchen"auf betreuten iOS-Geräten verwaltet. Die Schrittfolge, mit der Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Bereitstellen von Geräten mit Apple Configurator 2.

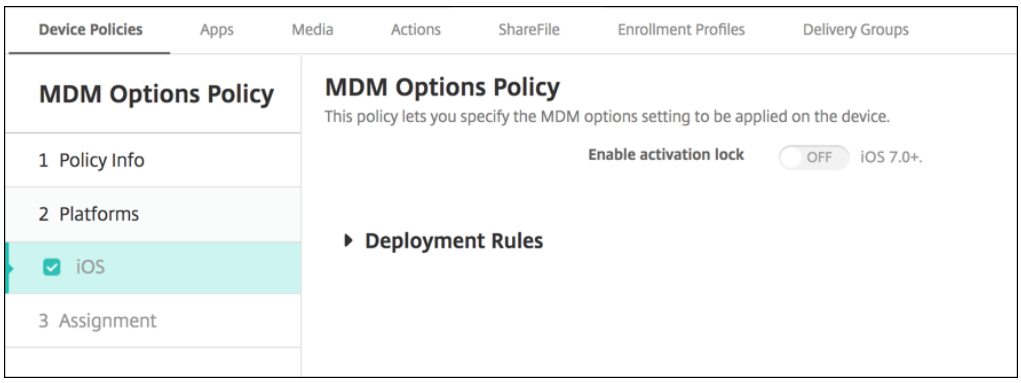
Die Aktivierungssperre ist ein Feature von "Mein iPhone/iPad suchen", mit dem das Reaktivieren von verlorenen oder gestohlenen betreuten Geräten verhindert wird. Die Aktivierungssperre erfordert die Eingabe der Apple-ID und des Benutzerkennworts, bevor ein beliebiger Benutzer "Mein iPhone/iPad suchen"deaktivieren, 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 Aktivieren der Aktivierungssperre müssen Sie die Citrix Endpoint Management-Geräterichtlinie "MDM-Optionen"konfigurieren und bereitstellen. Sie können dann ein Gerät über die Citrix Endpoint Management-Konsole ohne die Apple-Anmeldeinformationen des Benutzers verwalten. Um die erforderliche Eingabe der Apple-Anmeldeinformationen bei einer Aktivierungssperre zu umgehen, geben Sie die Sicherheitsaktion "Aktivierungssperre umgehen"auf der Citrix Endpoint Management-Konsole ein.

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 auf der Citrix Endpoint Management-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 unter Umgehen einer iOS-Aktivierungssperre.

Netzwerkgeräterichtlinie

June 25, 2024

Mit der Netzwerkrichtlinie können Sie festlegen, wie Benutzergeräte mit Wi-Fi-Netzwerken verbunden werden. Definieren Sie hierzu Folgendes:

- Netzwerknamen und -typen
- Authentifizierungs- und Sicherheitsrichtlinien
- Verwendung des Proxyservers
- Andere Wi-Fi-Details

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

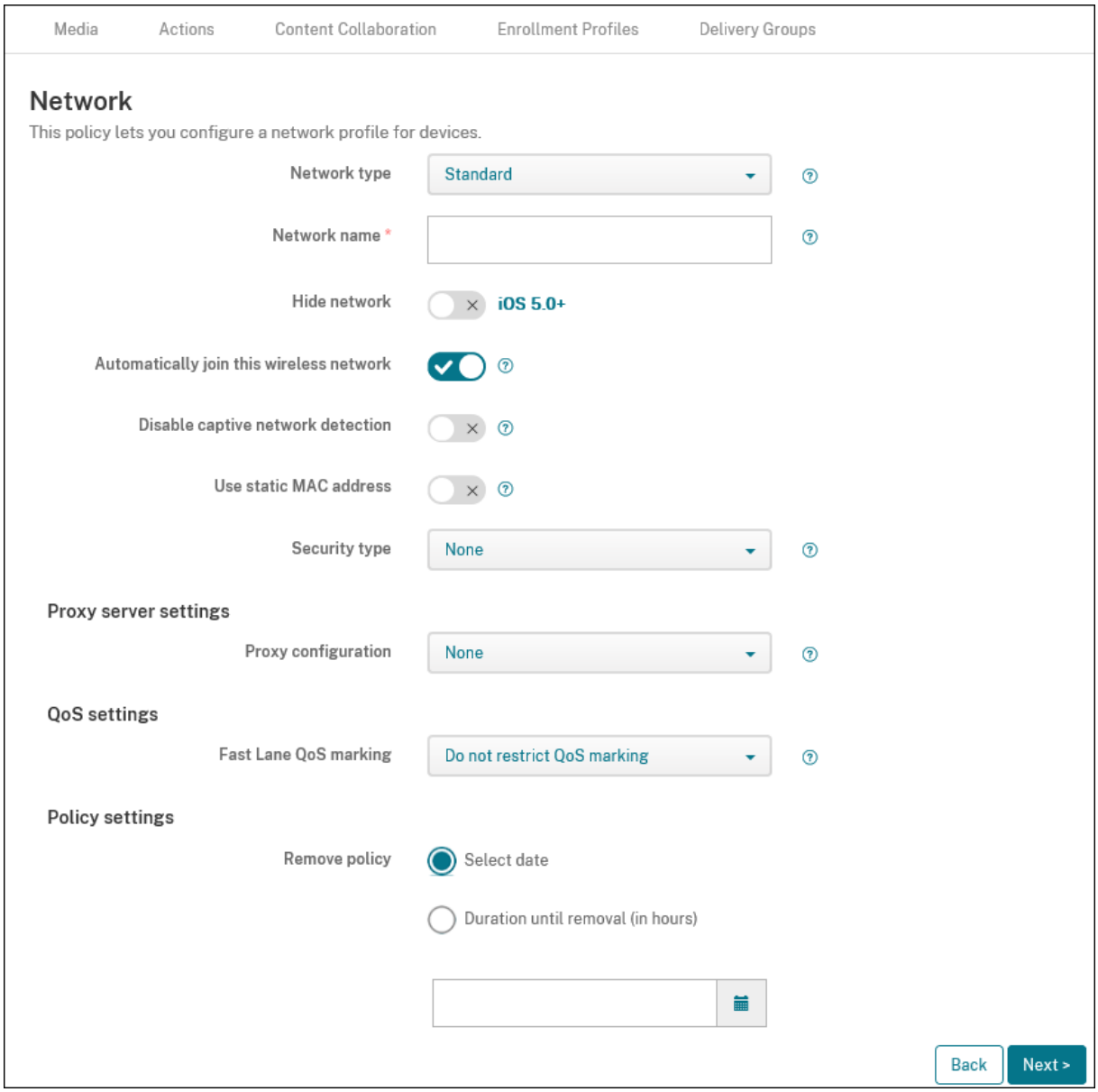
Voraussetzungen

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**.
- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **Automatisch mit diesem Drahtlosnetzwerk verbinden:** Wählen Sie aus, ob ein Gerät dem Netzwerk automatisch beitreten soll. Wenn ein Gerät mit einem anderen Netzwerk verbunden ist, tritt es diesem Netzwerk nicht bei. Der Benutzer muss die Verbindung zum vorherigen Net-

zwerk trennen, bevor das Gerät automatisch eine Verbindung herstellt. Die Standardeinstellung ist **Ein**.

- **Erkennung von Captive-Netzwerk deaktivieren:** Der Assistent für Captive-Netzwerke unterstützt Benutzer beim Zugriff auf Abonnement- oder Wi-Fi-Hotspot-Netzwerke. Sie finden diese Netzwerke meist in Cafés, Hotels und an anderen öffentlichen Orten. Bei Auswahl von **Ein** können Geräte weiterhin eine Verbindung zu Captive-Netzwerken herstellen, der Benutzer muss jedoch einen Browser öffnen und sich manuell anmelden. Die Standardeinstellung ist **Aus**.
- **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/WPA3 Personal
  - Beliebig (Persönlich)
  - WEP (Unternehmen)
  - WPA/WPA2/WPA3 Enterprise: Konfigurieren Sie in der aktuellen Version von Windows 10 das Simple Certificate Enrollment Protocol (SCEP), um WPA-2 Enterprise zu verwenden. Citrix Endpoint Management kann das Zertifikat dann an die Geräte zur Authentifizierung am Wi-Fi-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.
- **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**.

- **Fast Lane-QoS-Kennzeichnung:** Wenn Sie die QoS-Kennzeichnung für ein Wi-Fi-Netzwerk, das Cisco Fast Lane QoS unterstützt, nicht einschränken, können alle Apps L2- und L3-Kennzeichnung verwenden. Wenn Sie die QoS-Kennzeichnung einschränken, müssen Sie die Apps angeben, die L2- und L3-Kennzeichnung verwenden dürfen.

    - **QoS-Kennzeichnung aktivieren:** Wenn Sie die QoS-Kennzeichnung einschränken, wird sie mit dieser Einstellung vollständig deaktiviert oder nur für bestimmte Apps zugelassen. Bei Auswahl von **Aus** deaktivieren Sie die QoS-Kennzeichnung vollständig. Bei Auswahl von **Ein** konfigurieren Sie eine Liste der Apps, die die QoS-Kennzeichnung verwenden können. Die Standardeinstellung ist **Ein**.
    - **Apple Audio-/Video-Anrufe zulassen:** Legen Sie fest, ob Apps für Audio- und Videoanrufe die QoS-Kennzeichnung verwenden dürfen. Bei Auswahl von **Aus** kann dies die Qualität von Video- und Audioanrufen beeinträchtigen.
    - **Bestimmte Apps zulassen:** Fügen Sie der Liste eine App-Paket-ID hinzu, damit die App die QoS-Kennzeichnung verwenden kann.

- **Einstellungen für Hotspot 2.0**

    - **Angezeigter Operatorname:** Der vom Hotspot-Gerät gesendete Anzeigename. Benutzer sehen diesen Namen in der Liste der verfügbaren Wi-Fi-Netzwerke.
    - **Domänenname:** Der für die Wi-Fi-Hotspot 2.0-Aushandlung verwendete Domänenname.
    - **Verbindung zu Roamingpartnernetzwerken zulassen:** Bei Auswahl von **Ein** können Geräte außerhalb ihres Heimnetzwerks eine Verbindung mit Partnernetzwerken herstellen.
    - **Organisations-ID für Roaming Consortium (OI):** Fügen Sie eine Liste der Organisations-IDs hinzu, auf die das Gerät zugreifen kann. Organisations-IDs für Roaming Consortium gehören zu einer Organisation mit gemeinsamen Authentifizierungsmethoden. Wenn der

von Ihnen konfigurierte Hotspot nicht verfügbar ist, stellt das Gerät eine Verbindung mit einer hier aufgeführten Organisations-ID für Roaming Consortium her.
  - **NAI-Bereichsnamen (Network Access Identifier):** Konfigurieren Sie eine Liste von Bereichsnamen, die verwendet werden, um Benutzer in einem Roaming-Netzwerk zu identifizieren. Der NAI-Name wird in der Form `user@realm` übertragen.
  - **MCCs (Mobile Country Codes) und MNCs (Mobile Network Configurations):** Ein Mobile Country Code besteht aus drei Ziffern, die das Land eines Netzwerks identifizieren. Der Mobile Network Code besteht aus zwei oder drei eindeutigen Ziffern. Bei gemeinsamer Verwendung können MCC/MNC einen Mobilfunknetzbetreiber oder Mobilfunkanbieter eindeutig identifizieren.

- **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. Nicht verfügbar für iOS.

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), WPA3 (Unternehmen), Beliebig (Unternehmen) für iOS

Wenn Sie einen dieser Sicherheitstypen auswählen, werden **EAP**-Einstellungen nach den **QoS-Einstellungen** angezeigt.

> **Wichtig:**
>
> Wenn Sie den Sicherheitstyp **WPA2 (Unternehmen)** auswählen, müssen Sie mindestens ein EAP-Protokoll zulassen.

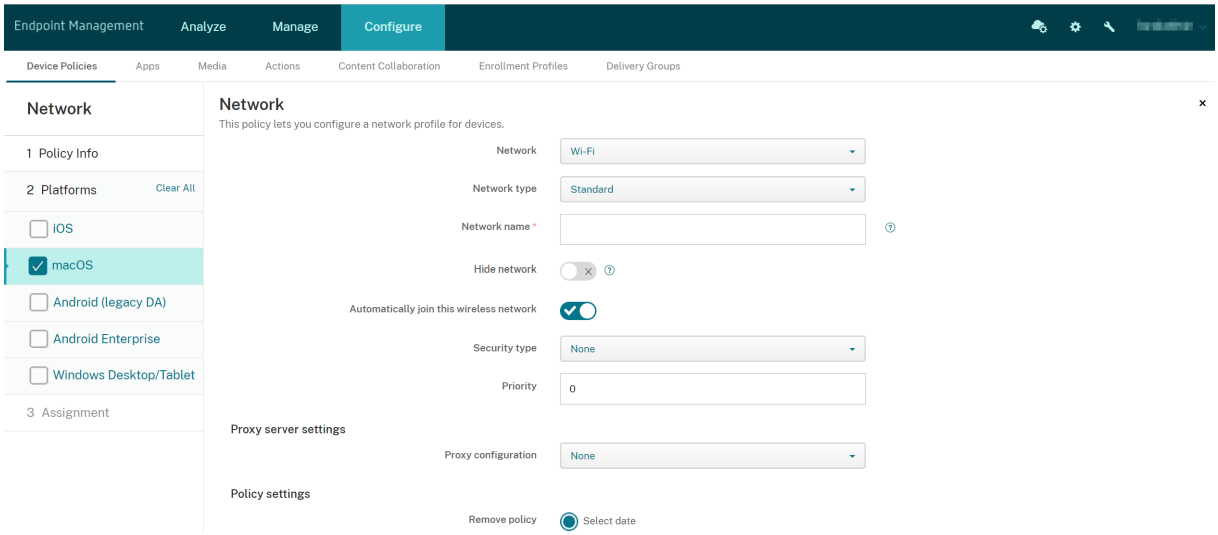
- **Zulässige EAP-Protokolle:** Aktivieren Sie die EAP-Typen, die unterstützt werden sollen, und konfigurieren Sie dann die zugehörigen Einstellungen. Die Standardeinstellung ist für alle verfügbaren EAP-Typen **Aus**.
- **Interne Authentifizierung (TTLS):** *nur erforderlich, wenn Sie TTLS aktivieren.* Wählen Sie in der Liste die gewünschte interne Authentifizierungsmethode aus. Optionen: **PAP**, **CHAP**, **MSCHAP** und **MSCHAPv2**. Der Standardwert ist **MSCHAPv2**.
- **EAP-FAST mit PAC:** 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.
    * Wenn Sie **Provisioning-PAC** wählen, müssen Sie auch angeben, ob ein anonymer TLS-Handshake zwischen dem Endbenutzerclient und Citrix Endpoint Management 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):** 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 "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 für den 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**.

macOS-Einstellungen



- **Netzwerk:** Wählen Sie in der Liste die Netzwerkoption aus, die Sie verwenden möchten. Die Standardeinstellung ist **Wi-Fi**.
  - Wi-Fi
  - Globales Ethernet
  - Erstes aktives Ethernet
  - Zweites aktives Ethernet
  - Drittes aktives Ethernet
  - Erstes Ethernet
  - Zweites Ethernet
  - Drittes Ethernet
- **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**.

- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **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.
- **Priorität:** Geben Sie bei mehreren Netzwerken eine Ziffer ein, um die Priorität der Netzwerkverbindung zu definieren. Das Gerät stellt zuerst eine Verbindung mit dem Netzwerk mit der niedrigsten Prioritätsziffer her. Negative Zahlen sind zulässig. Die Standardeinstellung ist **0**.
- **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**.

- **Einstellungen für Hotspot 2.0**
  - **Angezeigter Operatorname:** Der vom Hotspot-Gerät gesendete Anzeigename. Benutzer sehen diesen Namen in der Liste der verfügbaren Wi-Fi-Netzwerke.
  - **Domänenname:** Der für die Wi-Fi-Hotspot 2.0-Aushandlung verwendete Domänenname.
  - **Verbindung zu Roamingpartnernetzwerken zulassen:** Bei Auswahl von **Ein** können Geräte außerhalb ihres Heimnetzwerks eine Verbindung mit Partnernetzwerken herstellen.
  - **Organisations-ID für Roaming Consortium (OI):** Fügen Sie eine Liste der Organisations-IDs hinzu, auf die das Gerät zugreifen kann. Organisations-IDs für Roaming Consortium gehören zu einer Organisation mit gemeinsamen Authentifizierungsmethoden. Wenn der von Ihnen konfigurierte Hotspot nicht verfügbar ist, stellt das Gerät eine Verbindung mit einer hier aufgeführten Organisations-ID für Roaming Consortium her.
  - **NAI-Bereichsnamen (Network Access Identifier):** Konfigurieren Sie eine Liste von Bereichsnamen, die verwendet werden, um Benutzer in einem Roaming-Netzwerk zu identifizieren. Der NAI-Name wird in der Form `user@realm` übertragen.
  - **MCCs (Mobile Country Codes) und MNCs (Mobile Network Configurations):** Ein Mobile Country Code besteht aus drei Ziffern, die das Land eines Netzwerks identifizieren. Der Mobile Network Code besteht aus zwei oder drei eindeutigen Ziffern. Bei gemeinsamer Verwendung können MCC/MNC einen Mobilfunknetzbetreiber oder Mobilfunkanbieter eindeutig identifizieren.

- **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.

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

- **Verbindungsmodus:** Wählen Sie bei Auswahl von **Ein** den Verbindungsmodus, der vom Benutzer beim Verbinden mit dem Netzwerk genutzt werden soll. Die Standardeinstellung ist **Aus**.
  - **System:** Bei Auswahl dieser Option wird der Benutzer mit den Systemanmeldeinformationen authentifiziert. Die Option ist standardmäßig deaktiviert.
  - **Anmeldefenster:** Wenn diese Option markiert ist, wird der Benutzer mit den Anmeldeinformationen authentifiziert, die im Anmeldefenster eingegeben wurden. Die Option ist standardmäßig deaktiviert.

Wenn Sie einen dieser Sicherheitstypen auswählen, werden **EAP**-Einstellungen nach den **QoS-Einstellungen** angezeigt.

> **Wichtig:**
>
> Wenn Sie den Sicherheitstyp **WPA2 (Unternehmen)** auswählen, müssen Sie mindestens ein EAP-Protokoll zulassen.

- **Zulässige EAP-Protokolle:** 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**.
- **EAP-FAST mit PAC:** 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.
    - Wenn Sie **Provisioning-PAC** wählen, müssen Sie auch angeben, ob ein anonymer TLS-Handshake zwischen dem Endbenutzerclient und Citrix Endpoint Management zulässig ist.
      - **Anonymes PAC-Provisioning**
- **Authentifizierung:**

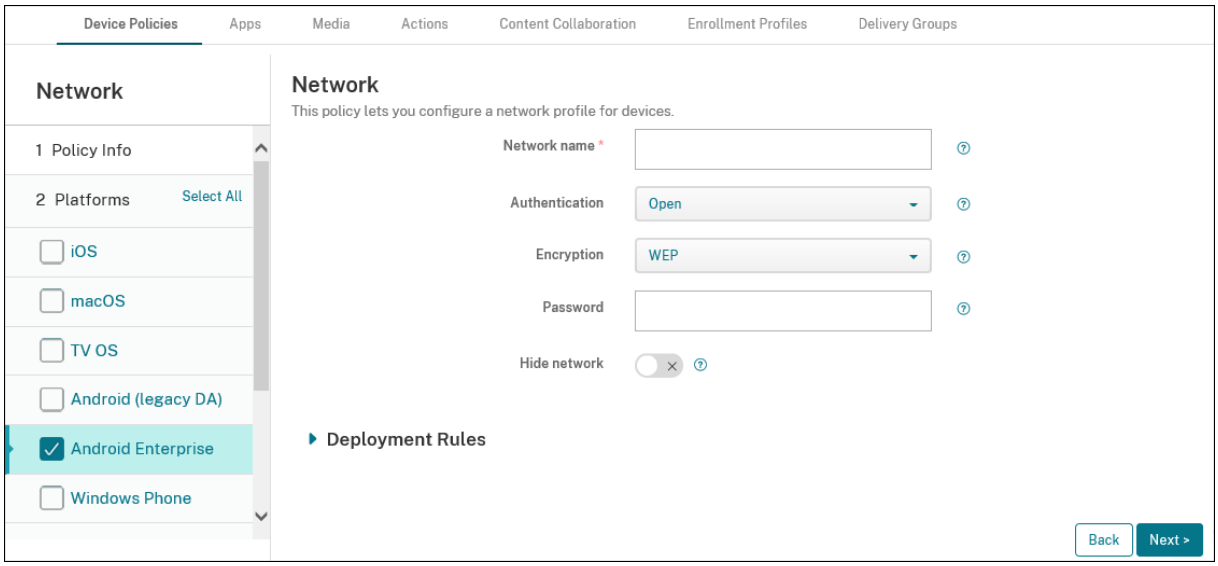
  - **Active Directory-Authentifizierung verwenden:** Wählen Sie aus, ob die Active Directory-Authentifizierung aktiviert werden soll. Für macOS 10.7 und höher verfügbar. Führen Sie die folgenden Schritte aus, um diese Option zur Verfügung zu stellen:
    * Legen Sie **PEAP** als EAP-Protokoll fest.
    * Wählen Sie für "Gültigkeitsbereich für Profil"die Option **System**. Sie können diese Einstellungsoption nur verwenden, wenn Sie die Richtlinie auf das gesamte System anwenden.
  - **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):** 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 "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 für den 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**.

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. Der Standardwert ist **Offen**.

Einstellung für Offen/Freigegeben für Android Enterprise

- **Verschlüsselung:** Wählen Sie in der Liste entweder **Deaktiviert** oder **WEP** aus. Die Standardeinstellung ist **WEP**.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

Einstellungen für WPA, WPA-PSK, WPA2, WPA2-PSK für Android Enterprise

- **Verschlüsselung:** Wählen Sie in der Liste entweder **TKIP** oder **AES**. Der Standardwert ist **TKIP**.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

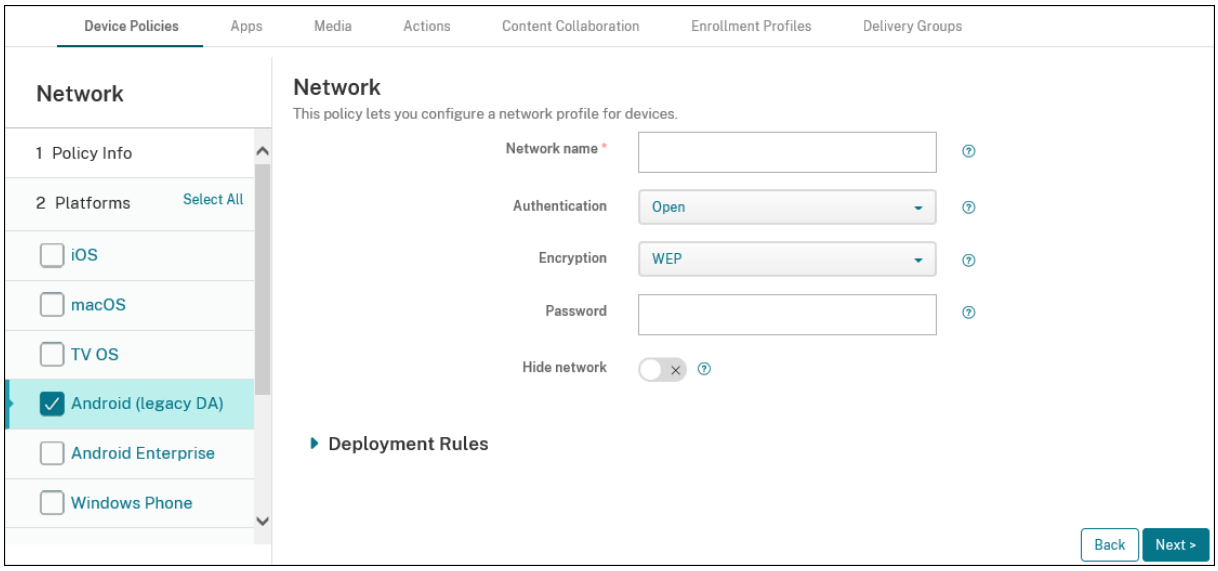
802.1x-Einstellungen für Android Enterprise

- **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 "Anonym"erhöhen und somit die Anzeige des Benutzernamens vermeiden.
- **ZS-Zertifikat:** Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
- **Domäne:** Geben Sie den erforderlichen Domänennamen ein. Weitere Informationen finden Sie unter Domäne.

  > **Hinweis:**
  >
  > Wenn Sie die Wi-Fi-Richtlinie auf Geräten mit Android 13 oder höher konfigurieren, müssen die Felder **Zertifizierungsstellenzertifikat** und **Domäne** aktualisiert werden. Wenn sie nicht aktualisiert werden, schlägt die Konfiguration fehl.

- **Identitätsanmeldeinformationen:** Klicken Sie in der Liste auf die Identitätsanmeldeinformationen, die verwendet werden sollen. Die Standardeinstellung ist **Ohne**.
- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

Einstellungen für Android (Legacy-Geräteadministrator)



- **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 (nur Android Enterprise)
  - WPA (nur Android Enterprise)
  - WPA-PSK (nur Android Enterprise)
  - 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.
- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

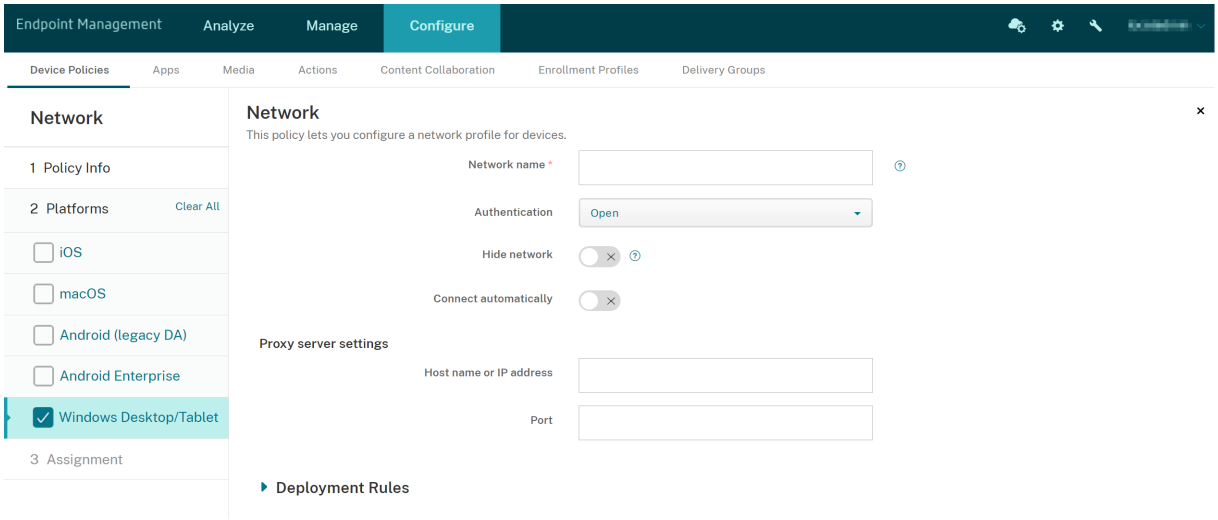
Einstellungen für WPA, WPA-PSK, WPA2, WPA2-PSK für Android

- **Verschlüsselung:** Wählen Sie in der Liste entweder **TKIP** oder **AES**. Der Standardwert ist **TKIP**.
- **Kennwort:** Geben Sie ein optionales Kennwort ein.
- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

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 "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**.
- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

Windows Desktop/Tablet-Einstellungen



- **Netzwerkname:** Die SSID, die in der Liste der verfügbaren Netzwerke angezeigt wird.
- **Authentifizierung:** Klicken Sie in der Dropdownliste auf den Sicherheitstyp, den Sie für die WLAN-Verbindung verwenden möchten.

  - Offen
  - WPA (Persönlich)
  - WPA-2 (Persönlich)
  - WPA (Unternehmen)
  - WPA-2 (Unternehmen): Konfigurieren Sie in der aktuellen Version von Windows 10 SCEP, um WPA-2 Enterprise zu verwenden. Nach der SCEP-Konfiguration kann Citrix Endpoint Management das Zertifikat an Geräte senden, zur Authentifizierung am Wi-Fi-Server. 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

- **Netzwerk ausblenden:** 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**.
- **Gemeinsamer Schlüssel:** Geben Sie den Verschlüsselungsschlüssel für die ausgewählte Methode an.
- **Netzwerk ausblenden:** 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**.
- **Netzwerk ausblenden:** Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
- **Automatisch verbinden:** Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

- **SCEP aktivieren?:** Wählen Sie aus, ob das Zertifikat auf den Benutzergeräten über SCEP bereitgestellt werden soll.
- **Anmeldeinformationsanbieter für SCEP:** Wählen Sie in der Liste die Anmeldeinformationsanbieter für SCEP aus. Die Standardeinstellung ist **Ohne**.

Richtlinie für die Netzwerkauslastung

December 1, 2023

Sie können Netzwerkauslastungsregeln festlegen, um vorzugeben, wie Netzwerke (z. B. mobile Datennetzwerke) von iOS-Geräten verwendet werden. Die Regeln gelten für verwaltete Apps und festgelegte SIMs. Verwaltete Apps sind Apps, die Sie über Citrix Endpoint Management auf den Geräten der Benutzer bereitstellen. Dazu gehören keine Apps, die Benutzer ohne Citrix Endpoint Management direkt auf ihre Geräte heruntergeladen haben. Sie enthalten auch keine Apps, die bereits auf den Geräten installiert waren, als die Geräte bei Citrix Endpoint Management registriert wurden. Diese Richtlinie gilt für SIMs für iOS 13-Geräte. Sie können App-Regeln, SIM-Regeln oder beides konfigurieren. SIM-Regeln gelten für alle verwalteten Apps auf diesem Gerät.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Anwendungsregeln**
  - **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 konfigurieren Sie Folgendes:
    - **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.
- **SIM-Regeln**
  - **SIM-Wi-Fi-Assistenzrichtlinie:** Beim Aktivieren von **Von schlechtem Wi-Fi wechseln** wechselt die SIM-Wi-Fi-Assistenzrichtlinie bei schlechter WLAN-Verbindung schneller zu

Mobilfunkverbindungen. Diese Einstellung kann die mobile Datennutzung erhöhen und die Akkulaufzeit beeinträchtigen.

- **SIM-ICCIDs:** Klicken Sie für jede SIM, die Sie der Liste hinzufügen möchten, auf **Hinzufügen**, und konfigurieren Sie Folgendes:
  * **ICCID:** Geben Sie die 19- oder 20-stellige Nummer für die hinzuzufügende SIM-Karte ein.

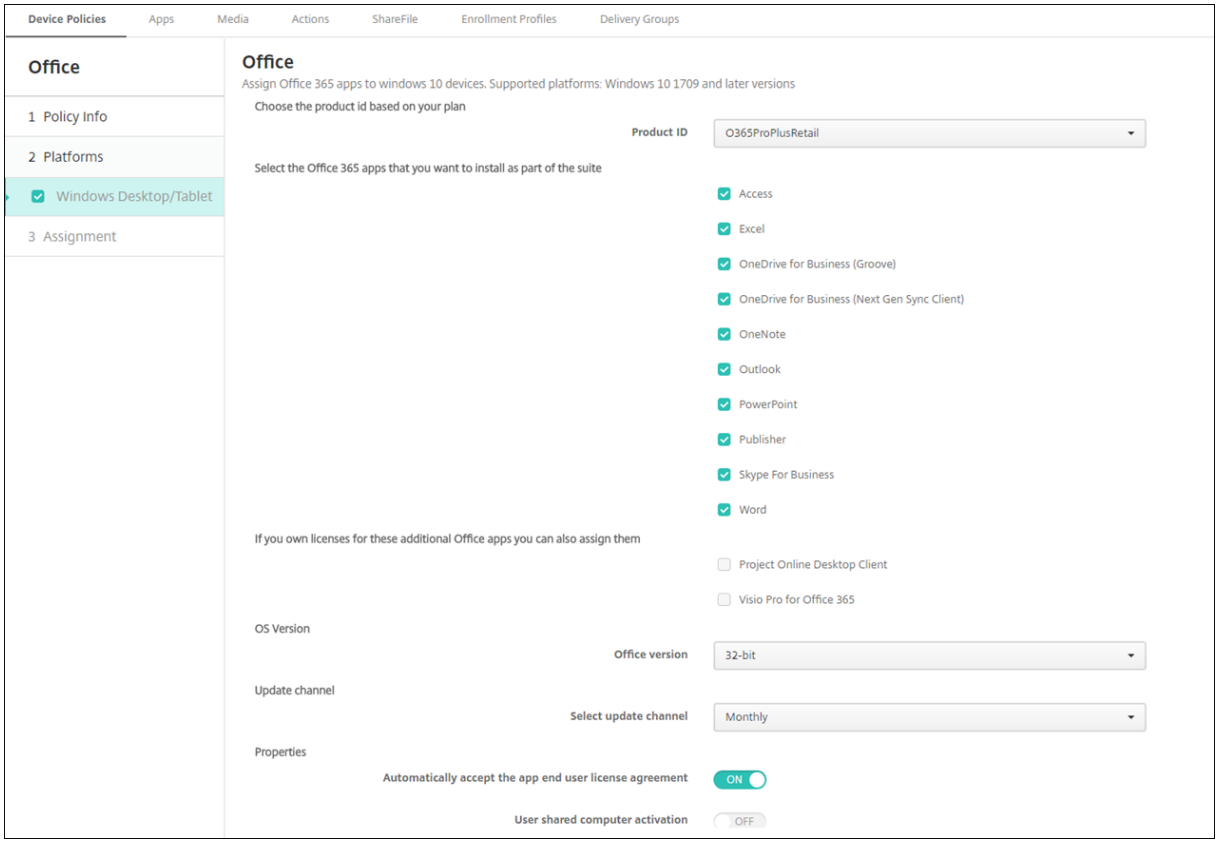
Office-Geräterichtlinie

December 1, 2023

Citrix Endpoint Management ermöglicht die Bereitstellung von Microsoft Office 365-Produkten über den Office-Konfigurationsdienstanbieter (Office CSP). Durch Konfigurieren der Office-Geräterichtlinie können Sie Microsoft Office-Anwendungen auf jedem Gerät mit Windows 10 (Version 1709 oder höher) oder Windows 11 bereitstellen.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Desktop/Tablet-Einstellungen



- **Produkt-ID:** Wählen Sie eine Produkt-ID basierend auf Ihrem Office 365-Plan. Die Optionen sind **O365ProPlusRetail, O365BusinessRetail** oder **O365SmallBusPremRetail**.
- **Office 365-Apps:** Wählen Sie die Office 365-Apps aus, die bereitgestellt werden sollen. Standardmäßig sind alle Apps ausgewählt.
- **Zusätzliche Office-Apps:** Wenn Sie Lizenzen für **Project Online-Desktopclient** oder **Visio Pro für Office 365** haben, können Sie diese Apps für die Installation auswählen.
- **Office-Version:** Wählen Sie, ob die **32-Bit**- oder **64-Bit**-Version von Office installiert werden soll.
- **Updatekanal:** Wählen Sie, wie oft Updates durchgeführt werden sollen. Optionen sind **Monatlich**, **Monatlich (Ziel)**, **Halbjährlich** oder **Halbjährlich (Ziel)**.
- **Eigenschaften:**
  - **Lizenzvereinbarung der App automatisch akzeptieren:** Wählen Sie **Ein** oder **Aus**. Die Standardeinstellung ist **Ein**.
  - **Für Benutzer freigegebenen Computer aktivieren:** Wählen Sie, ob der Computer freigegeben ist oder nicht. Optionen sind **Ein** oder **Aus**. Die Standardeinstellung ist **Aus**.
- **Office-Sprache:** Office wird automatisch in allen Sprachen installiert, die Windows bereits installiert hat. Sie können zusätzliche Sprachen zur Installation auswählen.

Geräterichtlinie für Unternehmensinformationen

December 1, 2023

Über die Richtlinie "Informationen zur Organisation"legen Sie die Unternehmensinformationen für Warnmeldungen fest, die von Citrix Endpoint Management an iOS-Geräte gesendet werden.

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 Citrix Endpoint Management 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.

Geräterichtlinie für OS-Updates

June 25, 2024

Mit der Geräterichtlinie "OS-Update"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 im Apple-Bereitstellungsprogramm registrierte macOS-Geräte, auf denen macOS 10.11.5 und höher ausgeführt wird.

> **Hinweis:**
>
> Apple beschränkt Betriebssystemupdates derzeit auf Hauptversionen. Administratoren dürfen keine Nebenversionen aktualisieren. Weitere Informationen finden Sie in der Dokumentation von Apple.

- Die aktuellen Betriebssystemupdates auf betreuten Desktop- und Tablet-Geräten mit Windows 10 oder Windows 11.

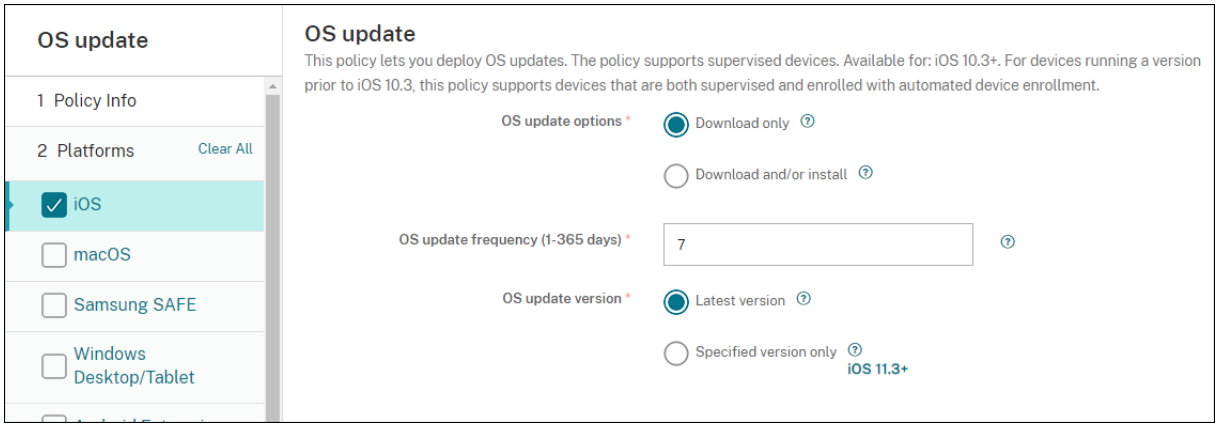
  Sie können über die Richtlinie für Betriebssystemupdates auch Einstellungen für die Übermittlungsoptimierung für Desktops und Tablets mit Windows 10 (Version 1607 oder höher) oder Windows 11 verwalten. Die Übermittlungsoptimierung ist ein Peer-to-Peer-Clientupdatedienst von Microsoft für Windows 10- und Windows 11-Updates. Zweck der Übermittlungsoptimierung ist die Reduzierung der bei Updates verwendeten Bandbreite. Die Reduzierung der Bandbreite wird erreicht, indem der Downloadtask auf mehrere Geräte verteilt wird. Weitere Informationen finden Sie im Microsoft-Artikel Configure Delivery Optimization for Windows 10 updates.

- Die aktuellen Betriebssystemupdates auf verwalteten Android Enterprise-Geräten (Android 7.0 und höher).

> **Wichtig:**
>
> Mit der Richtlinie für OS-Updates können Sie Updates nicht vollständig deaktivieren. Erstellen Sie eine Einschränkungsrichtlinie, um Updates bis zu 90 Tage zu verzögern. Siehe Geräteeinschränkungsrichtlinie.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

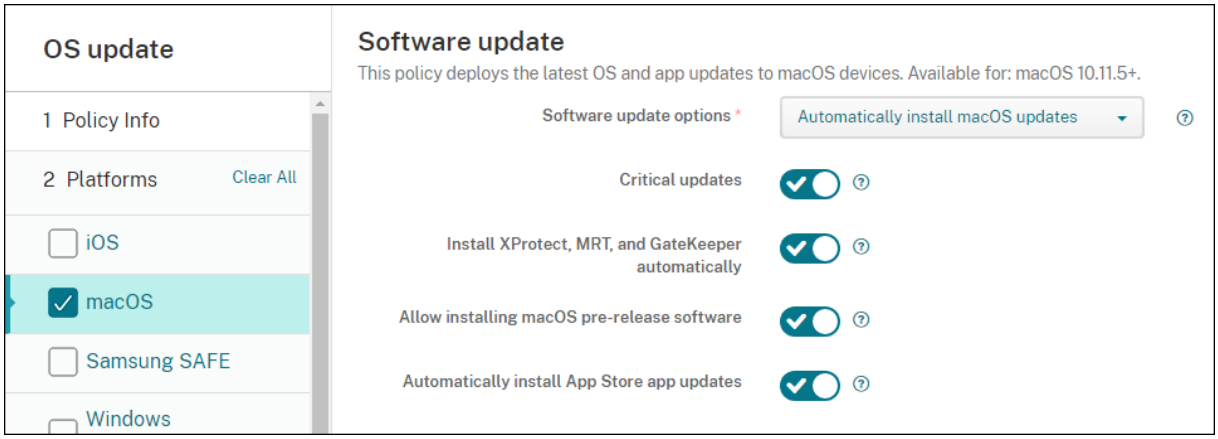


Die folgenden Einstellungen gelten für betreute iOS-Geräte.

- **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 Citrix Endpoint Management das Gerätebetriebssystem überprüft und aktualisiert. Die Standardeinstellung ist **7** Tage.
- **OS-Updateversion:** legt die Version zum Aktualisieren betreuter iOS-Geräte fest. Die Standardeinstellung ist **Aktuelle Version**.
  - **Aktuelle Version:** Wählen Sie diese Option für ein Update auf die neueste Betriebssystemversion.
  - **Bestimmte:** Wählen Sie diese Option für ein Update auf eine bestimmte Betriebssystemversion und geben Sie dann die Versionsnummer ein.

macOS-Einstellungen



- **Softwareupdateoptionen:** Legt fest, wie macOS-Geräte Updates suchen und installieren. Zur Auswahl stehen folgende Optionen:
  - **macOS-Updates automatisch installieren:** Updates werden automatisch heruntergeladen und installiert.
  - **Neue Updates herunterladen, wenn verfügbar:** Updates werden heruntergeladen und müssen manuell installiert werden.
  - **Nach Updates suchen:** Updates werden angezeigt, aber nicht automatisch heruntergeladen oder installiert.
  - **Nicht nach Updates suchen:** Neue Updates werden nicht angezeigt und nicht automatisch heruntergeladen oder installiert. Benutzer können Updates jedoch weiterhin manuell installieren.
- **Wichtige Updates:** Wichtige macOS-Updates können automatisch installiert werden.
- **Updates für xProtect, MRT und GateKeeper automatisch installieren:** macOS-Geräte können Updates für Sicherheitssoftware automatisch installieren.
- **Installieren von macOS-Vorabversionen zulassen:** Benutzer können Vorabversionen von macOS-Software installieren.

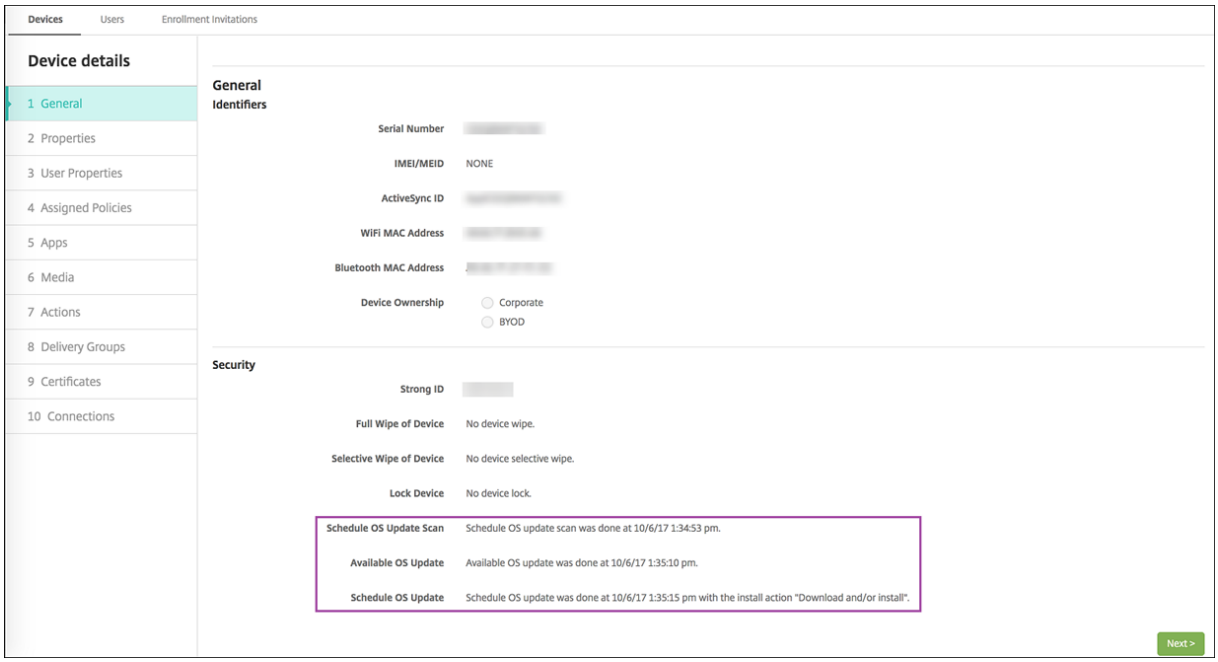
- **App-Updates für App Store automatisch installieren:** App Store-Apps können automatisch aktualisiert werden.

Statusabfragen für iOS- und macOS-Update-Aktionen

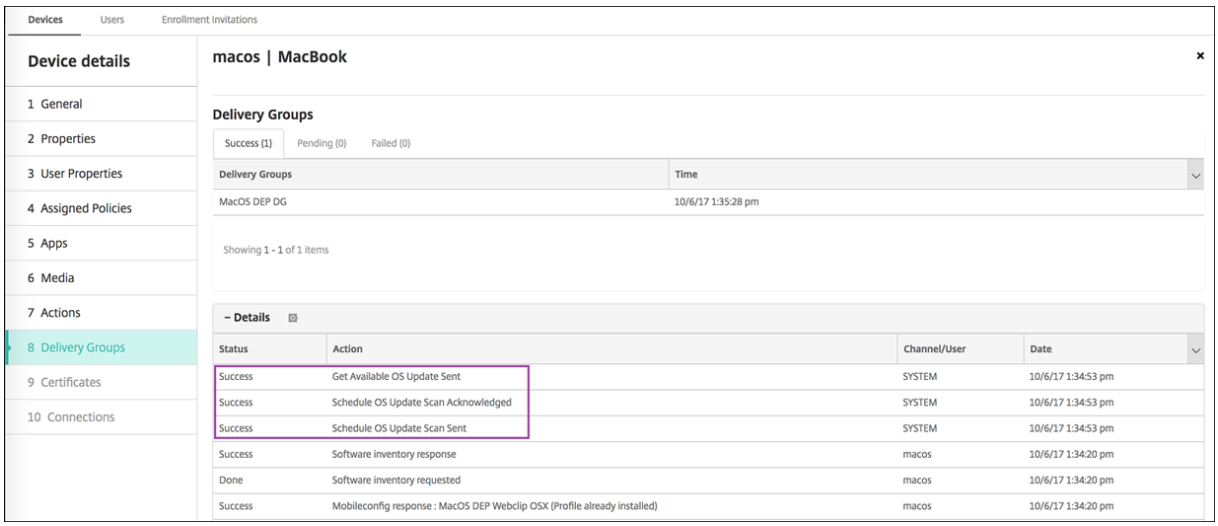
Auf Geräten mit iOS und macOS wird die Richtlinie "OS-Updates steuern"nicht von Citrix Endpoint Management bereitgestellt. Stattdessen sendet Citrix Endpoint Management über die Richtlinie folgende MDM-Befehle an Geräte:

- 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.

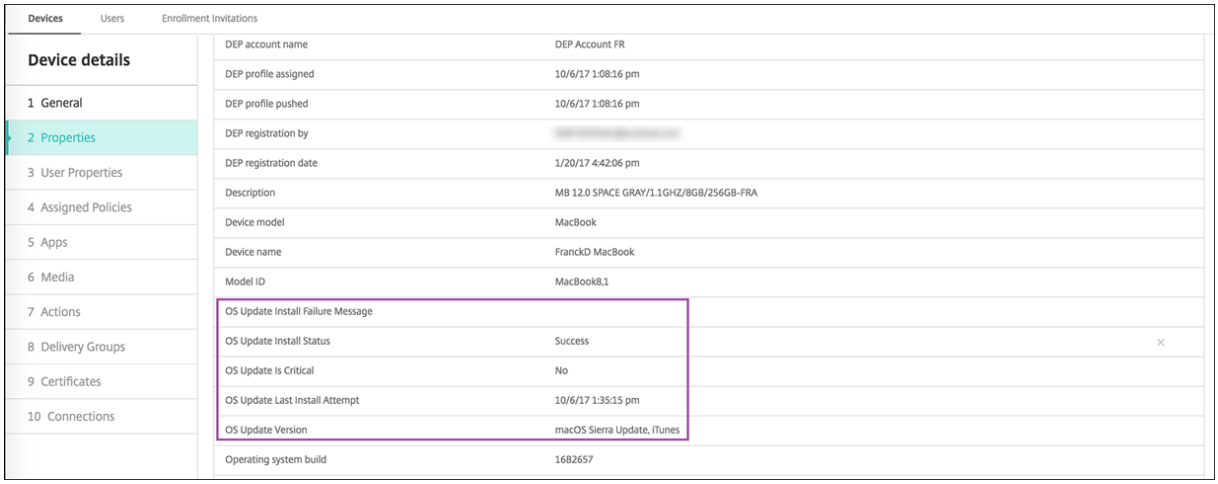
Auf der Seite **Verwalten > Geräte > Gerätedetails** wird der Status geplanter und verfügbarer OS-Updatescans und geplanter macOS- und App-Updates angezeigt.

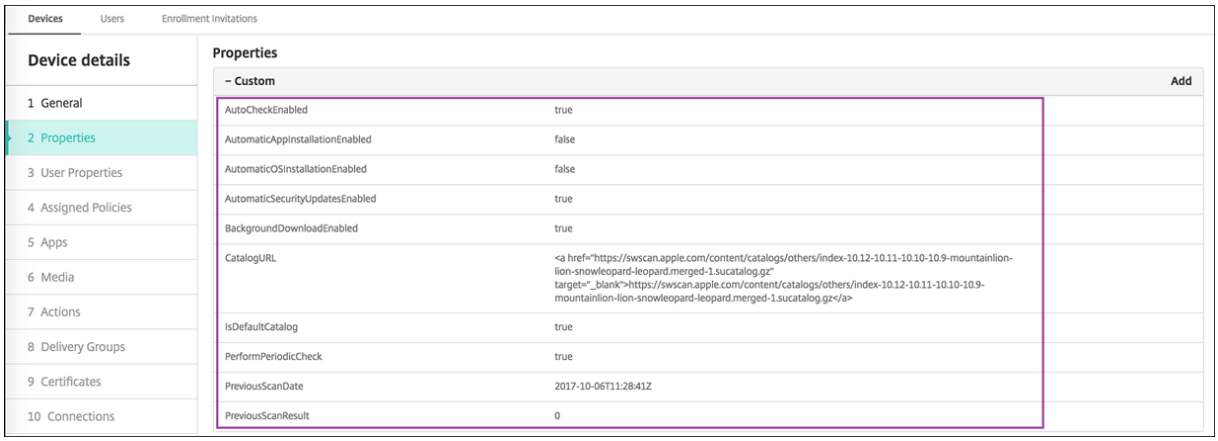


Weitere Informationen zum Status der Updateaktionen finden Sie auf der Seite **Verwalten > Geräte > Gerätedetails (Bereitstellungsgruppen)**.

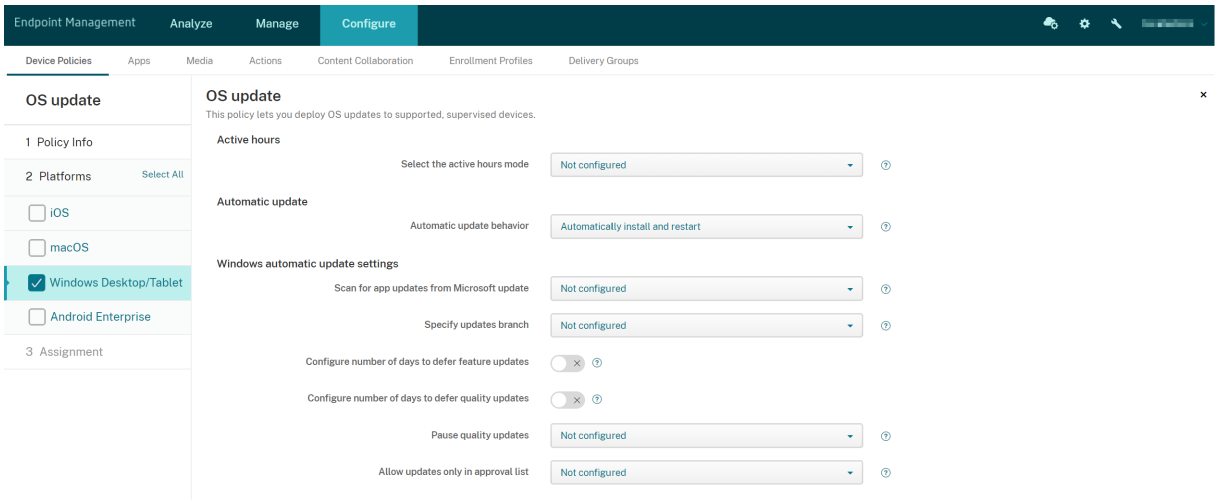


Weitere Informationen, z. B. verfügbare Betriebssystemupdates und Angaben zum letzten Installationsversuch, finden Sie auf der Seite **Verwalten > Geräte > Gerätedetails (Eigenschaften)**.





Windows Desktop-/Tablet-Einstellungen



- **Modus für Nutzungszeit auswählen:** Wählen Sie einen Modus zum Festlegen der Nutzungszeit für die Durchführung von Betriebssystemupdates. Die Nutzungszeit kann als Zeitraum in Stunden oder durch Angabe der Start- und Endzeit konfiguriert werden. Nach Auswahl des Modus werden weitere Einstellungen angezeigt: **Zeitraum für Nutzungszeit angeben** oder **Beginn der Nutzungszeit** und **Ende der Nutzungszeit**. Bei Auswahl von **Nicht konfiguriert** können Betriebssystemupdates jederzeit durchgeführt werden. Der Standardwert ist **Nicht konfiguriert**.
- **Verhalten bei automatischen Updates:** Konfiguriert das Download-, Installations- und Neustartverhalten des Windows Update-Diensts auf Benutzergeräten. Standardeinstellung ist **Autom. Installation und Neustart**.
  - **Benutzer vor dem Download des Updates benachrichtigen:** Windows benachrichtigt die Benutzer, wenn Updates verfügbar sind. Updates werden nicht automatisch heruntergeladen und installiert. Benutzer müssen die Download- und Installationsaktionen starten.
  - **Autom. Installation und Benachrichtigung, um den Geräteneustart zu planen:** In Netzwerken ohne Datenlimit lädt Windows Updates automatisch herunter. Windows installiert Updates während der automatischen Wartung, wenn das Gerät nicht verwendet wird und nicht im Akkubetrieb läuft. Wenn die automatische Wartung zwei Tage lang keine Updates installieren kann, installiert Windows Update die Updates sofort. Wenn die Installation einen Neustart erfordert, fordert Windows den Benutzer auf, die Neustartzeit zu planen. Der Benutzer kann den Neustart für einen Zeitraum von bis zu sieben Tagen planen. Nach sieben Tagen erzwingt Windows das Neustarten des Geräts. Wenn Benutzer den Zeitpunkt des Neustarts selbst wählen können, wird das Risiko versehentlicher Datenverluste durch Apps reduziert, die beim Neustart nicht ordnungsgemäß heruntergefahren werden.
  - **Autom. Installation und Neustart:** Dies ist die Standardeinstellung. In Netzwerken ohne

Datenlimit lädt Windows Updates automatisch herunter. Windows installiert Updates während der automatischen Wartung, wenn das Gerät nicht verwendet wird und nicht im Akkubetrieb läuft. Wenn die automatische Wartung zwei Tage lang keine Updates installieren kann, installiert Windows Update die Updates sofort. Wenn die Installation einen Neustart erfordert, startet Windows das Gerät automatisch neu, wenn es inaktiv ist.

  - **Autom. Installation und Neustart zu einem bestimmten Zeitpunkt:** Wenn Sie diese Option auswählen, werden weitere Einstellungen angezeigt, sodass Sie Tag und Uhrzeit angeben können. Die Standardeinstellung ist täglich um 3:00 Uhr. Die automatische Installation erfolgt zur angegebenen Zeit und der Geräteneustart 15 Minuten später. Wenn Windows zum Neustart bereit ist kann ein zu diesem Zeitpunkt angemeldeter Benutzer den 15-minütigen Countdown unterbrechen, um den Neustart zu verzögern.
  - **Autom. Installation und Neustart ohne Endbenutzerbeteiligung:** In Netzwerken ohne Datenlimit lädt Windows Updates automatisch herunter. Windows installiert Updates während der automatischen Wartung, wenn das Gerät nicht verwendet wird und nicht im Akkubetrieb läuft. Wenn die automatische Wartung zwei Tage lang keine Updates installieren kann, installiert Windows Update die Updates sofort. Wenn die Installation einen Neustart erfordert, startet Windows das Gerät automatisch neu, wenn es inaktiv ist. Mit dieser Option wird auch das Benutzer-Bedienpanel auf schreibgeschützt festgelegt.
  - **Automatische Updates deaktivieren:** deaktiviert die automatischen Windows-Updates auf dem Gerät.

- **Auf App-Updates von Microsoft Update scannen:** gibt an, ob Windows Updates für andere Microsoft-Apps vom Microsoft Update-Dienst akzeptiert. Der Standardwert ist **Nicht konfiguriert**.

  - **Nicht konfiguriert:** Verwenden Sie diese Einstellung, wenn Sie das Verhalten nicht konfigurieren möchten. Windows ändert die zugehörige Benutzeroberfläche auf Benutzergeräten nicht. Die Benutzer können Updates für andere Microsoft-Apps akzeptieren oder ablehnen.
  - **Ja:** Windows ermöglicht die Installation von App-Updates über den Windows Update-Dienst. Die Einstellung auf dem Benutzergerät ist inaktiv, sodass der Benutzer sie nicht ändern kann.
  - **Nein:** Windows ermöglicht die Installation von App-Updates über den Windows Update-Dienst nicht. Die Einstellung auf dem Benutzergerät ist inaktiv, sodass der Benutzer sie nicht ändern kann.

- **Updates-Branch angeben:** gibt an, welcher Windows Update-Branch für Updates verwendet werden soll. Der Standardwert ist **Nicht konfiguriert**.

  - **Nicht konfiguriert:** Verwenden Sie diese Einstellung, wenn Sie das Verhalten nicht konfigurieren möchten. Windows ändert die zugehörige Benutzeroberfläche auf Benutzergeräten nicht. Die Benutzer können einen Windows Update-Branch auswählen.

  - **Current Branch:** Windows empfängt Updates vom Current Branch. Die Einstellung auf dem Benutzergerät ist inaktiv, sodass der Benutzer sie nicht ändern kann.
  - **Current Branch for Business:** Windows empfängt Updates vom Current Business Branch. Die Einstellung auf dem Benutzergerät ist inaktiv, sodass der Benutzer sie nicht ändern kann.

- **Anzahl der Tage konfigurieren, die Featureupdates zurückgestellt werden können:** Mit **Ein** werden Featureupdates von Windows um die angegebene Anzahl von Tagen verzögert und der Benutzer kann die Einstellung nicht ändern. Wenn **Aus**, kann der Benutzer den Zeitraum der Verschiebung von Featureupdates ändern. Die Standardeinstellung ist **Aus**.
- **Anzahl der Tage konfigurieren, die Qualitätsupdates zurückgestellt werden können:** Mit **Ein** werden Qualitätsupdates von Windows um die angegebene Anzahl von Tagen verzögert und der Benutzer kann die Einstellung nicht ändern. Wenn **Aus**, kann der Benutzer den Zeitraum der Verschiebung von Qualitätsupdates ändern. Die Standardeinstellung ist **Aus**.
- **Qualitätsupdates zurückstellen:** gibt an, ob Qualitätsupdates 35 Tage lang zurückgestellt werden sollen. Der Standardwert ist **Nicht konfiguriert**.

  - **Nicht konfiguriert:** Verwenden Sie diese Einstellung, wenn Sie das Verhalten nicht konfigurieren möchten. Windows ändert die zugehörige Benutzeroberfläche auf Benutzergeräten nicht. Die Benutzer können Qualitätsupdates für 35 Tage zurückstellen.
  - **Ja:** Windows stellt die Installation von Qualitätsupdates aus dem Windows Update-Dienst 35 Tage zurück. Die Einstellung auf dem Benutzergerät ist inaktiv, sodass der Benutzer sie nicht ändern kann.
  - **Nein:** Windows stellt die Installation von Qualitätsupdates aus dem Windows Update-Dienst nicht zurück. Die Einstellung auf dem Benutzergerät ist inaktiv, sodass der Benutzer sie nicht ändern kann.

- **Nur Updates entsprechend Genehmigungsliste zulassen:** gibt an, ob nur die Updates installiert werden sollen, die von einem MDM-Server genehmigt wurden. Citrix Endpoint Management unterstützt nicht, eine Liste genehmigter Updates zu konfigurieren. Der Standardwert ist **Nicht konfiguriert**.

  - **Nicht konfiguriert:** Verwenden Sie diese Einstellung, wenn Sie das Verhalten nicht konfigurieren möchten. Windows ändert die zugehörige Benutzeroberfläche auf Benutzergeräten nicht. Die Benutzer können auswählen, welche Updates zulässig sind.
  - **Ja, nur genehmigte Updates installieren:** Es werden nur genehmigte Updates installiert.
  - **Nein, alle anwendbaren Updates installieren:** ermöglicht die Installation aller anwendbaren Updates.

- **Internen Updateserver verwenden:** gibt an, ob Updates über den Windows Update-Dienst oder einen internen Updateserver über Windows Server Update Services (WSUS) abgerufen werden sollen. Bei Auswahl von **Aus** wird der Windows Update-Dienst verwendet. Bei Auswahl von

Ein stellen Geräte eine Verbindung zum angegebenen WSUS-Server her, um Updates zu erhalten. Die Standardeinstellung ist **Aus**.

  - **Updates akzeptieren, die von anderen Entitäten als Microsoft signiert sind:** gibt an, ob Updates akzeptiert werden sollen, die von Drittanbieterentitäten signiert wurden. Das Feature erfordert, dass das Gerät dem Drittanbieterzertifikat vertraut. Die Standardeinstellung ist **Aus**.
  - **Verbindung zum Microsoft Updatedienst zulassen:** Ermöglicht eine regelmäßige Verbindung zwischen Windows Update auf dem Gerät und dem Microsoft Updatedienst, selbst wenn das Gerät so konfiguriert ist, dass Updates von einem WSUS-Server abgerufen werden. Die Standardeinstellung ist **Ein**.
  - **WSUS-Server:** Geben Sie die Server-URL für den WSUS-Server ein.
  - **Alternativer Intranetserver zum Hosten von Updates:** Geben Sie die URL eines alternativen Intranetservers zum Hosten von Updates und Empfang von Berichtsinformationen an.

- **Übermittlungsoptimierung konfigurieren:** gibt an, ob die Übermittlungsoptimierung für Windows 10- und Windows 11-Updates verwendet werden soll. Die Standardeinstellung ist **Aus**.
- **Cachegröße:** die maximale Größe des Cache für die Übermittlungsoptimierung. Ein Wert von **0** bedeutet eine unbegrenzte Cachegröße. Die Standardeinstellung ist **10** GB.
- **VPN-Peercaching zulassen:** gibt an, ob Geräte, die über VPN mit dem Domänennetzwerk verbunden sind, am Peercaching teilnehmen können. Mit **Ein** können Geräte über ein VPN oder das Unternehmensdomänennetzwerk Updatedaten von anderen Geräten im Domänennetzwerk herunterladen oder auf diese hochladen. Die Standardeinstellung ist **Aus**.
- **Downloadmethode:** Die Downloadmethode, die von der Übermittlungsoptimierung zum Download von Windows-Updates, Apps und App-Updates verwendet werden kann. Standardeinstellung ist **HTTP kombiniert mit Peering hinter der gleichen NA**. Optionen:

  - **Nur HTTP, kein Peering:** deaktiviert das Peercaching, ermöglicht jedoch den Download von Inhalten von Windows Update-Servern oder WSUS-Servern (Windows Server Update Services) per Übermittlungsoptimierung.
  - **HTTP kombiniert mit Peering hinter der gleichen NAT:** ermöglicht das Peersharing im gleichen Netzwerk. Der Übermittlungsoptimierungs-Clouddienst sucht andere Clients, die unter Verwendung derselben öffentlichen IP-Adresse wie der Zielclient eine Verbindung mit dem Internet herstellen. Diese Clients versuchen dann, eine Verbindung mit anderen Peers im selben Netzwerk unter Verwendung der privaten Subnetz-IP herzustellen.
  - **HTTP kombiniert mit Peering in einer privaten Gruppe:** wählt automatisch eine Gruppe basierend auf der Site der Active Directory-Domänendienste (AD DS) des Geräts oder der Domäne, in der das Gerät authentifiziert ist. Das Peering erfolgt in internen Subnetzen

zwischen Geräten, die zu derselben Gruppe gehören, einschließlich solchen in Remotebüros.
  - **HTTP kombiniert mit Internetpeering:** aktiviert Internetpeerquellen für die Übermittlungsoptimierung.
  - **Einfacher Downloadmodus ohne Peering:** deaktiviert den Übermittlungsoptimierungs-Clouddienst. Die Übermittlungsoptimierung wechselt automatisch in diesen Modus, wenn der Übermittlungsoptimierungs-Clouddienst nicht verfügbar oder nicht erreichbar ist oder wenn die Größe der Inhaltsdatei unter 10 MB liegt. In diesem Modus bietet die Übermittlungsoptimierung einen zuverlässigen Download ohne Peercaching.
  - **Keine Übermittlungsoptimierung, sondern BITS verwenden:** ermöglicht Clients die Verwendung von BranchCache. Weitere Informationen finden Sie in dem Microsoft-Artikel BranchCache.

- **Max. Downloadbandbreite:** die maximale Downloadbandbreite in KBit/s. Der Standardwert ist **0** und bewirkt eine dynamische Anpassung der Bandbreite.
- **Prozentsatz der maximalen Downloadbandbreite:** die maximale Downloadbandbreite, die von der Übermittlungsoptimierung für alle gleichzeitig ablaufenden Downloadaktivitäten genutzt werden kann. Der Wert ist ein Prozentsatz der verfügbaren Downloadbandbreite. Der Standardwert ist **0** und bewirkt eine dynamische Anpassung.
- **Max. Uploadbandbreite:** die maximale Uploadbandbreite in KBit/s. Die Standardeinstellung ist **0**. Ein Wert von **0** bedeutet eine unbegrenzte Bandbreite.
- **Obergrenze für monatliche Upload-Daten:** die maximale Datenmenge (in GB), die die Übermittlungsoptimierung in jedem Kalendermonat auf Internetpeers hochladen kann. Die Standardeinstellung ist 20 GB. Ein Wert von **0** bedeutet unbegrenzte monatliche Uploads.

Genehmigte Updates für Windows Desktop- und Tablet-Geräte in Citrix Endpoint Management

Sie können festlegen, dass nur genehmigte Updates installiert werden. Citrix Endpoint Management behandelt die Updates wie folgt:

- Sicherheitsupdates wie Windows Defender-Definitionen werden von Citrix Endpoint Management automatisch genehmigt und bei der nächsten Synchronisierung installiert.
- Bei allen übrigen Updates sendet Citrix Endpoint Management erst nach Ihrer Genehmigung einen Installationsbefehl an das Gerät.

Voraussetzungen

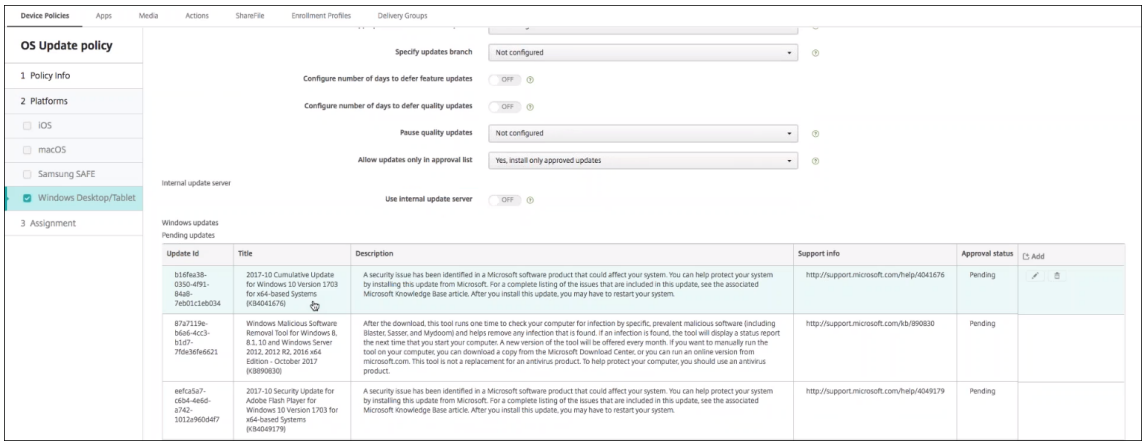
- Sie müssen das Microsoft-Stammzertifikat als Serverzertifikat auf den Citrix Endpoint Management-Server hochladen.
- Informationen zum Importieren eines Serverzertifikats finden Sie unter Zertifikate und Authentifizierung im Abschnitt “Importieren eines Zertifikats”.

Ausschließliche Installation von genehmigten Updates

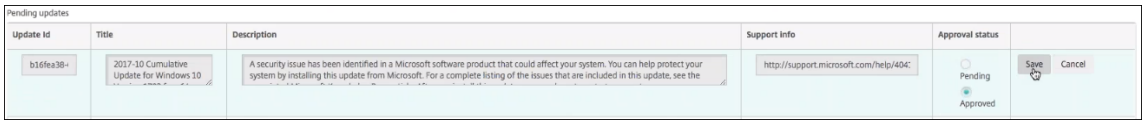
1. Navigieren Sie zu **Konfigurieren > Geräterichtlinien** und öffnen Sie die Richtlinie "OS-Updates".
2. Ändern Sie die Einstellung **Nur Updates entsprechend Genehmigungsliste zulassen** in **Ja, nur genehmigte Updates installieren**.

Genehmigen eines Updates

1. Führen Sie in der Geräterichtlinie "OS-Updates"einen Bildlauf nach unten zur Tabelle **Updates verfügbar** durch. Citrix Endpoint Management ruft die in der Tabelle aufgeführten Updates von den Geräten ab.
2. Suchen Sie nach Updates mit einem **Genehmigungsstatus** von **Ausstehend**.
3. Klicken Sie in die Zeile für das zu genehmigende Update und klicken Sie auf das Symbol "Bearbeiten"für diese Zeile (in der Spalte **Hinzufügen**).

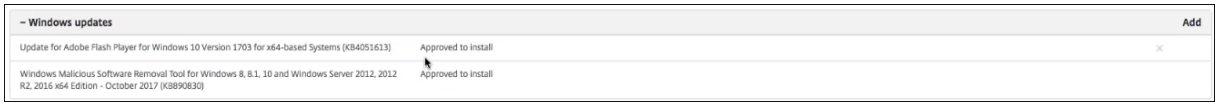


4. Klicken Sie zum Genehmigen des Updates auf **Genehmigt** und klicken Sie auf **Speichern**.



> **Hinweis:**
>
> Obwohl die Tabelle "Updates verfügbar"auch Befehle zum Hinzufügen und Löschen enthält, bewirken diese Befehle keine Änderungen an der Citrix Endpoint Management-Datenbank. Das Bearbeiten des Genehmigungsstatus ist die einzige verfügbare Aktion für ausstehende Updates.

Zur Anzeige des Windows-Updatestatus für ein Gerät gehen Sie zu **Verwalten > Geräte > Eigenschaften**.



Bei Veröffentlichung eines Updates wird in der ersten Spalte die **Update-ID** mit Status (Erfolg oder Fehler) angezeigt. Sie können einen Bericht oder eine automatisierte Aktion für Geräte mit fehlgeschlagenem Update erstellen. Datum und Uhrzeit der Veröffentlichung werden ebenfalls angezeigt.

Funktionsweise von Updates für erste und nachfolgende Bereitstellungen Die Geräterichtlinie "OS-Update"wirkt sich bei der ersten Bereitstellung anders aus als bei einer Bereitstellung, nachdem Geräte Updates erhalten.

- Damit Citrix Endpoint Management Update-Abfragen an Geräte sendet, müssen Sie einer Bereitstellungsgruppe mindestens eine Gruppenrichtlinie "OS-Update"zuweisen.

  Citrix Endpoint Management überprüft ein Gerät während einer MDM-Synchronisierung auf installierbare Updates.

- Nach der ersten Bereitstellung der Geräterichtlinie "OS-Update"ist die Liste der Windows-Updates leer, da noch keine Gerätedaten abgefragt wurden.

- Sobald Geräte in der zugewiesenen Bereitstellungsgruppe Updates melden, werden diese Updates von Citrix Endpoint Management in der Datenbank gespeichert. Zum Genehmigen von gemeldeten Updates bearbeiten Sie erneut die Richtlinie.

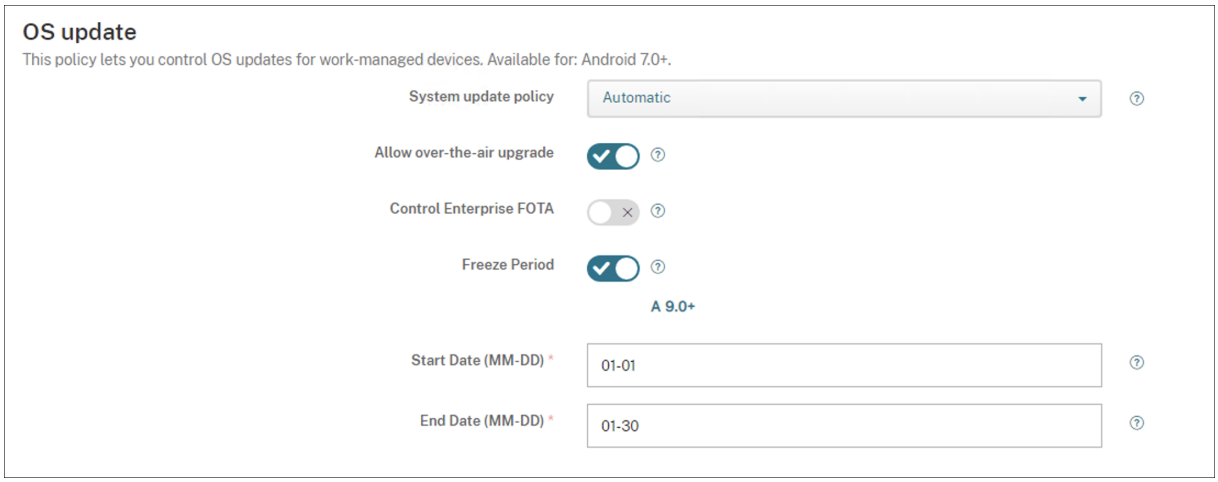
  Die Update-Genehmigung gilt nur für die derzeit bearbeitete Richtlinie. Updates, die in einer Richtlinie genehmigt wurden, werden in anderen Richtlinien nicht als genehmigt angezeigt. Bei der nächsten Gerätesynchronisierung sendet Citrix Endpoint Management eine Bestätigung an das Gerät, dass das Update genehmigt ist.

- Für eine zweite Geräterichtlinie vom Typ "OS-Update"enthält die Updateliste alle in der Citrix Endpoint Management-Datenbank gespeicherten Updates. Genehmigen Sie Updates für jede Richtlinie.

  Bei jeder Gerätesynchronisierung fragt Citrix Endpoint Management den Status genehmigter Updates ab, bis das Gerät die Installation des Updates bestätigt. Ist nach der Installation ein Neustart des Geräts erforderlich, prüft Citrix Endpoint Management den Updatestatus, bis das Gerät den Abschluss der Installation meldet.

- Die auf der Seite zur Richtlinienkonfiguration angezeigten Updates werden von Citrix Endpoint Management nicht nach Bereitstellungsgruppe oder Gerät beschränkt. Alle von den Geräten gemeldeten Updates werden in der Liste angezeigt.

Android Enterprise-Einstellungen



- **Systemupdate:** Diese Richtlinie legt fest, wann Systemupdates durchgeführt werden.
  - **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.
  - **Standard:** Legt die Aktualisierungsrichtlinie auf die Standardeinstellung des Systems fest.
- **Drahtloses Upgrade zulassen:** Wenn diese Option deaktiviert ist, können Benutzergeräte keine drahtlosen Softwareupdates empfangen. Die Standardeinstellung ist **Ein**.
- **Freeze Period:** Mit **Ein** werden OS-Updates in dem Datumsbereich, der für die Updaterichtlinien **Automatisch**, **Verschieben** und **Im Wartungsfenster** angegeben ist, nicht auf dem Gerät installiert. Für ein Gerät kann jeweils nur eine "Freeze Period"festgelegt werden. Die Dauer der "Freeze Period"darf 90 Tage nicht überschreiten.
  - **Startdatum/Enddatum:** Der Datumsbereich, in dem OS-Updates nicht installiert werden, wenn **Freeze Period** aktiviert ist.
- **Freeze Period:** Mit **Ein** werden OS-Updates in dem Datumsbereich, der für die Updaterichtlinien **Automatisch**, **Verschieben** und **Im Wartungsfenster** angegeben ist, nicht auf dem Gerät installiert. Für ein Gerät kann jeweils nur eine "Freeze Period"festgelegt werden. Die Dauer der "Freeze Period"darf 90 Tage nicht überschreiten.
  - **Startdatum/Enddatum:** Der Datumsbereich, in dem OS-Updates nicht installiert werden, wenn **Freeze Period** aktiviert ist.

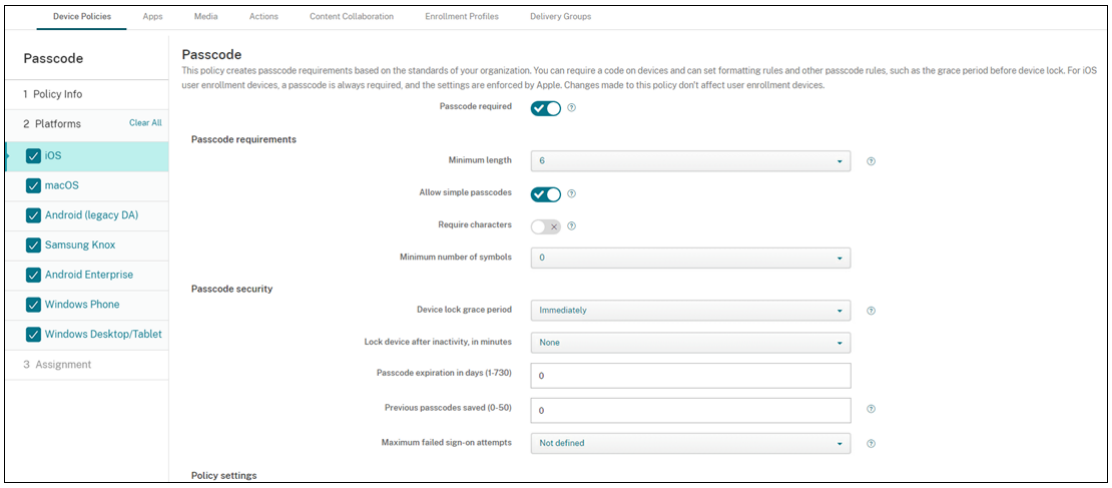
Passcode-Geräterichtlinie

June 25, 2024

Erstellen Sie Passcoderichtlinien in Citrix Endpoint Management gemäß den Standards Ihres Unternehmens. Sie können festlegen, dass Passcodes auf den Geräten der Benutzer eingegeben werden müssen, und verschiedene Formate und Passcoderegeln vorgeben. Erstellen Sie Richtlinien für iOS, macOS, Android, Android Enterprise und Windows Desktop/Tablet. 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 Dropdownliste auf die Mindestlänge für den Passcode. Die Standardeinstellung 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**

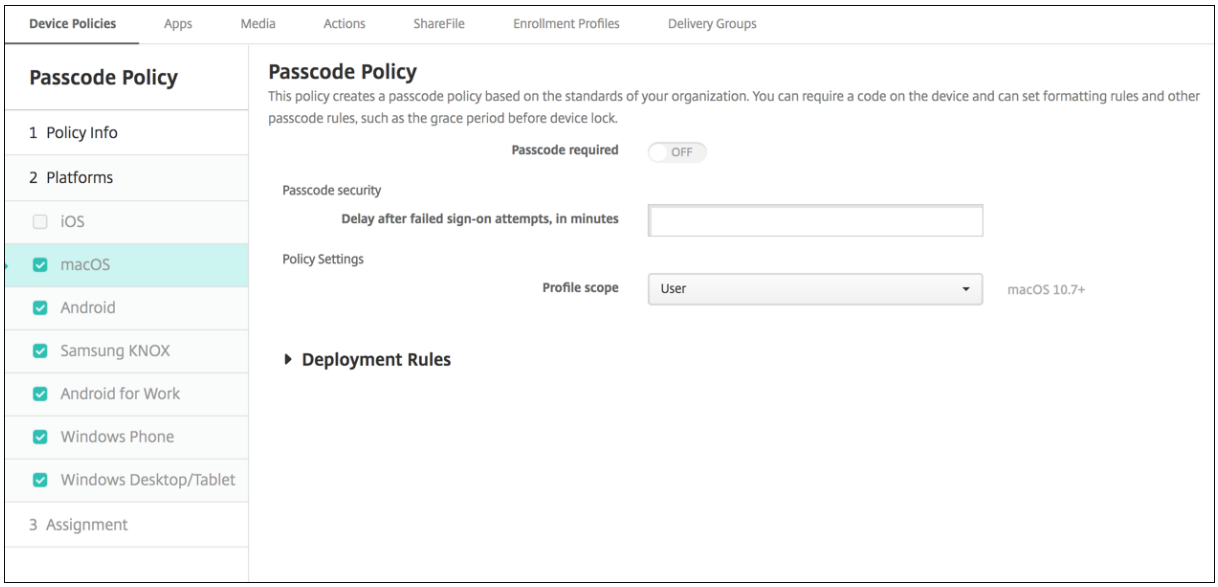
  - **Kulanzzeitraum für Gerätesperre:** Klicken Sie in der Liste auf die Zeitdauer, innerhalb derer die Benutzer einen Passcode zum Entsperren eines gesperrten Geräts eingeben müssen. Der Standardwert ist **Sofort**.
  - **Gerät bei Inaktivität sperren:** Geben Sie im Feld ein, wie lange ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Wert kann zwischen 1 und 15 Minuten sein. Setzen Sie den Wert auf **Ohne**, um die Richtlinie zu deaktivieren. 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 möglicher fehlgeschlagener Anmeldeversuche.
    * Bei Auswahl einer Zahl über 6 wird nach dem sechsten Versuch eine zeitliche Verzögerung zwischen Versuchen erzwungen. Diese Verzögerung wird mit jedem weiteren erfolglosen Anmeldeversuch etwas länger. Nach dem letzten Versuch werden alle Daten und Einstellungen sicher gelöscht.
    * Bei Auswahl einer Zahl bis 6 wird das Gerät ohne zeitliche Verzögerung gelöscht.
    * Bei Auswahl von **Nicht definiert** wird nach dem 6. Anmeldeversuch eine ansteigende Verzögerung zwischen Versuchen erzwungen, das Gerät wird jedoch nicht gelöscht.

    Die Standardeinstellung ist **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.

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 **Passcode erforderlich** deaktiviert ist, 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 Dropdownliste auf die Mindestlänge für den Passcode. Die Standardeinstellung 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:** 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 bei Inaktivität sperren:** Klicken Sie in der Liste auf den Zeitraum, den ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Wert kann zwischen 1 und 5 Minuten liegen. Setzen Sie den Wert auf **Ohne**, um die Richtlinie zu deaktivieren. 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 möglicher fehlgeschlagener Anmeldeversuche.
  * Bei Auswahl einer Zahl über 6 wird nach dem sechsten Versuch eine zeitliche Verzögerung zwischen Versuchen erzwungen. Diese Verzögerung wird mit jedem weiteren erfolglosen Anmeldeversuch etwas länger. Nach dem letzten Versuch wird das Gerät gesperrt.
  * Bei Auswahl einer Zahl bis 6 wird das Gerät ohne zeitliche Verzögerung gesperrt.
  * Bei Auswahl von **Nicht definiert** wird nach dem 6. Anmeldeversuch eine ansteigende Verzögerung zwischen Versuchen erzwungen, das Gerät wird jedoch nicht gesperrt.

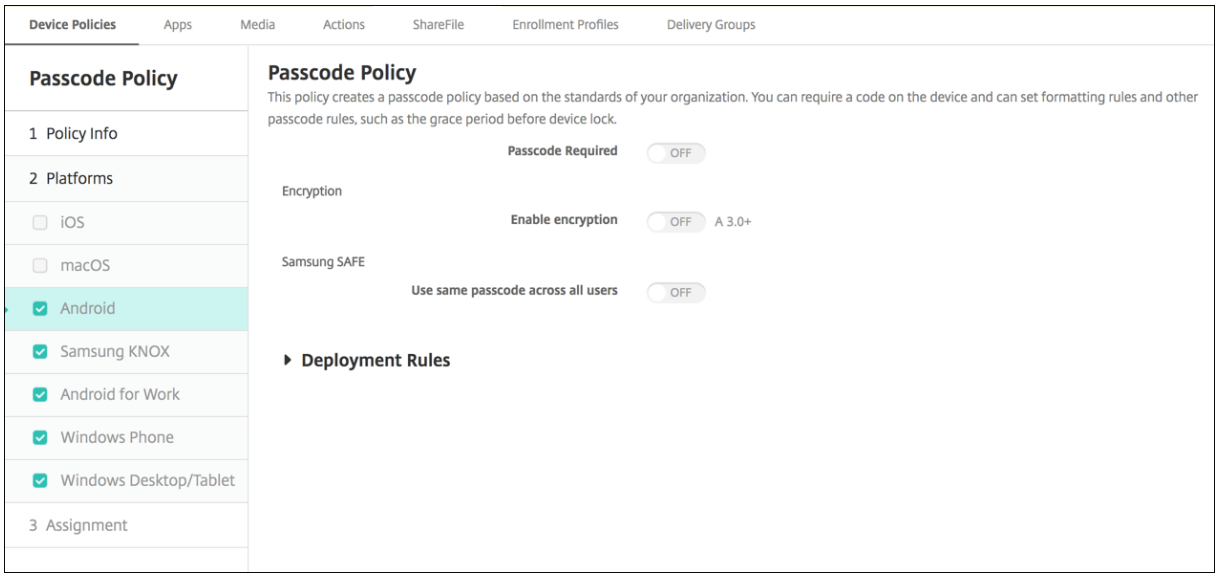
  Die Standardeinstellung ist **Nicht definiert**.
- **Verzögerung (in Minuten) nach fehlgeschlagenen Anmeldeversuchen:** Geben Sie ein, wie lange ein Benutzer warten musst, bevor das Anmeldefenster erneut erscheint, wenn die maximale Anzahl fehlgeschlagener Versuche erreicht wurde.
- **Passcodezurücksetzung erzwingen:** Bei Auswahl von **Aus** müssen Benutzer ihren Passcode bei der nächsten Authentifizierung nicht zurücksetzen, nachdem ihr Gerät diese Richtlinie erhalten hat. 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.

Einstellungen für Android (Legacy-Geräteadministrator)



> **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 und Passcodeverschlüsselung konfigurieren können.
- **Passcodeanforderungen**
  - **Mindestlänge:** Klicken Sie in der Dropdownliste auf die Mindestlänge für den Passcode. Die Standardeinstellung 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. Die Standardeinstellung ist **Aus**.

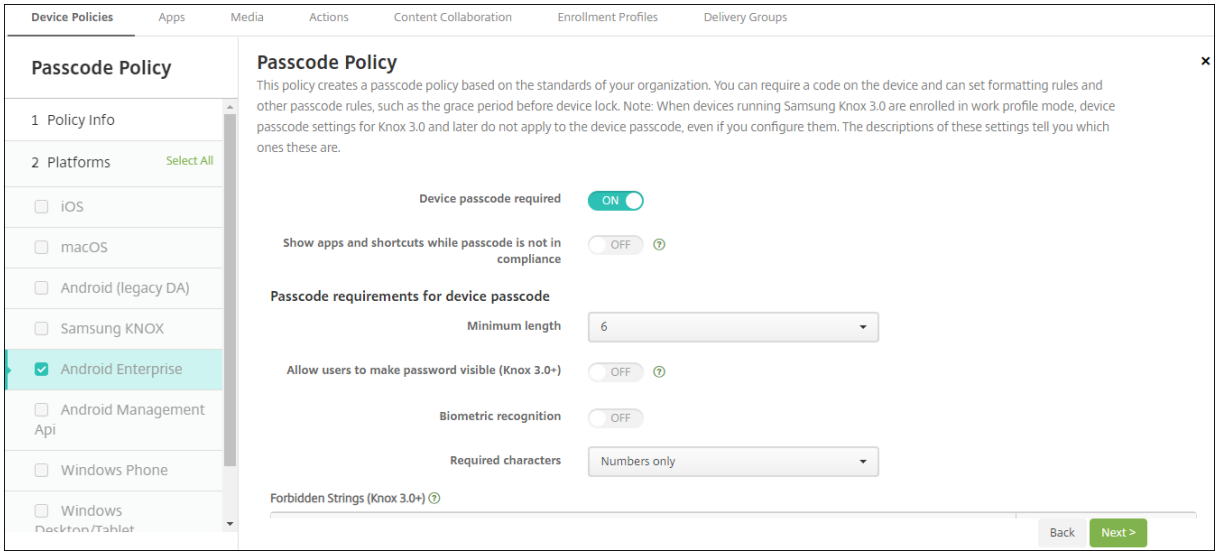
  - Wenn Sie **Erweiterte Regeln** aktivieren, wählen Sie aus den folgenden Listen die Mindestzahl der Zeichen des jeweiligen Typs aus, die der Passcode enthalten muss:
    * **Symbole:** Mindestanzahl der Symbole.
    * **Buchstaben:** Mindestanzahl der Buchstaben.
    * **Kleinbuchstaben:** Mindestanzahl der Kleinbuchstaben.
    * **Großbuchstaben:** Mindestanzahl der Großbuchstaben.
    * **Ziffern oder Symbole:** Mindestanzahl der Ziffern oder Symbole.
    * **Ziffern:** Mindestanzahl der Ziffern.

- **Passcodesicherheit**
  - **Gerät bei Inaktivität sperren:** 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 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 bis zum Abschluss der Verschlüsselung am Stromnetz angeschlossen sein. Der Vorgang kann eine Stunde oder länger dauern. 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.

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.

- **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. Die Standardeinstellung ist 6.
  - **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**.
  - **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 für ein Zeichen:** 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.

- **Passcodekomplexität für Gerätepasscode (Android 12+):**
  - **Passcodekomplexität anwenden:** Erfordert ein Kennwort mit einer Komplexitätsstufe, die von der Plattform und nicht von einer benutzerdefinierten Kennwortanforderung definiert wird. Nur für Geräte mit Android 12+ und Citrix Secure Hub 22.9 und höher.
  - **Komplexitätsgrad:** Vordefinierte Ebenen der Kennwortkomplexität.
    - **Ohne:** Kein Kennwort erforderlich.
    - **Niedrig:** Das Kennwort kann Folgendes sein:
      - Ein Muster

        - Eine PIN mit mindestens vier Ziffern
    * **Mittel:** Das Kennwort kann Folgendes sein:
        - Eine PIN mit mindestens vier Ziffern ohne Sequenzen, die sich wiederholen (4444) oder geordnet sind (1234)
        - Alphabetisch mit mindestens vier Zeichen
        - Alphanumerisch mit mindestens vier Zeichen
    * **Hoch:** Das Kennwort kann Folgendes sein:
        - Eine PIN mit mindestens acht Ziffern ohne Sequenzen, die sich wiederholen (4444) oder geordnet sind (1234)
        - Alphabetisch mit mindestens sechs Zeichen
        - Alphanumerisch mit mindestens sechs Zeichen

        > **Hinweis:**
        > Für BYOD-Geräte mit Android 12 und höher sind Passcodeeinstellungen wie "Mindestlänge", "Erforderliche Zeichen", "Biometrische Erkennung" und "Erweiterte Regeln"nicht anwendbar. Verwenden Sie stattdessen Passcodekomplexität.

- **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 bei Inaktivität sperren:** Legt die Anzahl der Minuten fest, die ein Gerät inaktiv sein darf, bevor es gesperrt wird. Setzen Sie den Wert auf 0, um die Richtlinie zu deaktivieren.
    - **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.
- **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.

- **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**.
- **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 für ein Zeichen:** 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.

- **Passcodekomplexität für die Sicherheitsabfrage im Arbeitsprofil (Android 12+):**
  - **Passcodekomplexität anwenden:** Erfordert ein Kennwort mit einer Komplexitätsstufe,

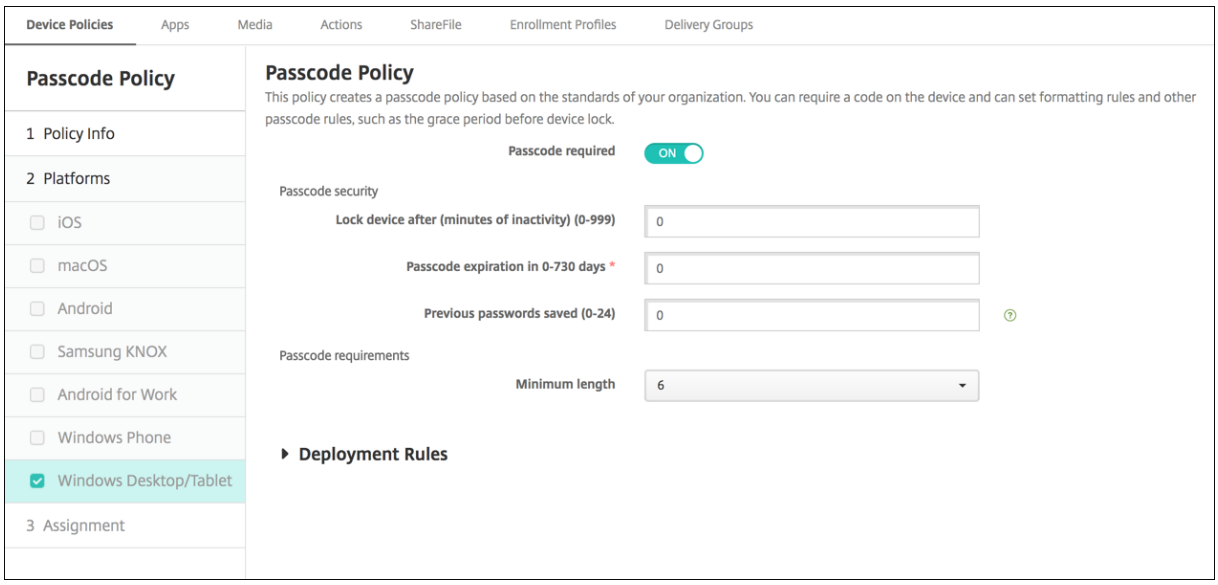
die von der Plattform und nicht von einer benutzerdefinierten Kennwortanforderung definiert wird. Nur für Geräte mit Android 12+ und Citrix Secure Hub 22.9 und höher.

- **Komplexitätsgrad:** Vordefinierte Ebenen der Kennwortkomplexität.
  - **Ohne:** Kein Kennwort erforderlich.
  - **Niedrig:** Das Kennwort kann Folgendes sein:
    - Ein Muster
    - Eine PIN mit mindestens vier Ziffern
  - **Mittel:** Das Kennwort kann Folgendes sein:
    - Eine PIN mit mindestens vier Ziffern ohne Sequenzen, die sich wiederholen (4444) oder geordnet sind (1234)
    - Alphabetisch mit mindestens vier Zeichen
    - Alphanumerisch mit mindestens vier Zeichen
  - **Hoch:** Das Kennwort kann Folgendes sein:
    - Eine PIN mit mindestens acht Ziffern ohne Sequenzen, die sich wiederholen (4444) oder geordnet sind (1234)
    - Alphabetisch mit mindestens sechs Zeichen
    - Alphanumerisch mit mindestens sechs Zeichen

      > **Hinweis:**
      > Wenn Sie Passcodekomplexität für ein Arbeitsprofil aktivieren, müssen Sie sie auch für das Gerät aktivieren.

- **Passcodesicherheit für die Sicherheitsabfrage für Arbeitsprofil**
  - **Container nach fehlgeschlagenen Anmeldeversuchen löschen:** Legt die Anzahl fehlgeschlagener Anmeldeversuche fest, nach deren Ablauf das Arbeitsprofil samt Daten vom Gerät gelöscht wird. Benutzer müssen das Arbeitsprofil nach dem Löschen neu initialisieren. Die Standardeinstellung ist **Nicht definiert**.
  - **Container bei Inaktivität sperren:** Legt die Anzahl der Minuten fest, die ein Gerät inaktiv sein darf, bevor das Arbeitsprofil gesperrt wird. Der Wert kann zwischen 0 und 999 Minuten liegen. Setzen Sie den Wert auf 0, um die Richtlinie zu deaktivieren.
  - **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.

Windows Desktop/Tablet-Einstellungen



- **Passcode erforderlich:** Deaktivieren Sie diese Option, wenn für Windows Desktop/Tablet-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.
- **Passcodesicherheit**
  - **Gerät bei Inaktivität sperren:** Geben Sie die Anzahl der Minuten ein, die ein Gerät inaktiv sein darf, bevor es gesperrt wird. Die Standardeinstellung ist **0**.
  - **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.
  - **Vorherige Kennwörter speichern (0-24):** Geben Sie an, wie viele verwendete Passcodes gespeichert werden sollen. Die Benutzer können keinen gespeicherten Passcode wiederverwenden. Gültige Werte sind 1-24. Geben Sie eine Zahl zwischen 1 und 24 in diesem Feld ein. Die Standardeinstellung ist **0**.
- **Passcodeanforderungen**
  - **Mindestlänge:** Klicken Sie in der Dropdownliste auf die Mindestlänge für den Passcode. Die Standardeinstellung ist **6**.

Passcodesperre - Kulanzzeitraumrichtlinie

December 10, 2021

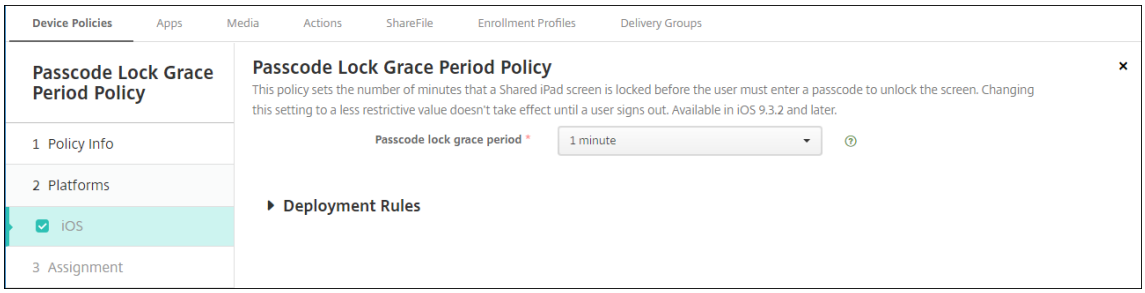
Die Richtlinie “Passcodesperre - Kulanzzeitraum”gilt für gemeinsam genutzte iOS/iPadOS-Geräte. Weitere Informationen über gemeinsam genutzte iPads finden Sie unter Integration von Apple Bildung-Features.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-Einstellungen

- **Passcodesperre - Kulanzzeitraum:** die Zeitdauer in Minuten, die der Bildschirm eines geteilten iPads gesperrt bleibt, bevor der Benutzer zum Entsperren einen Passcode eingeben muss. Die Änderung dieser Einstellung auf einen weniger restriktiven Wert wird erst wirksam, wenn sich ein Benutzer abmeldet. Der Standardwert ist **Sofort**.

  Standardmäßig werden geteilte iPads nach zwei Minuten Inaktivität automatisch gesperrt.



Richtlinien für persönliche Hotspots

May 28, 2021

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 Wi-Fi-Netzwerks sind.

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.

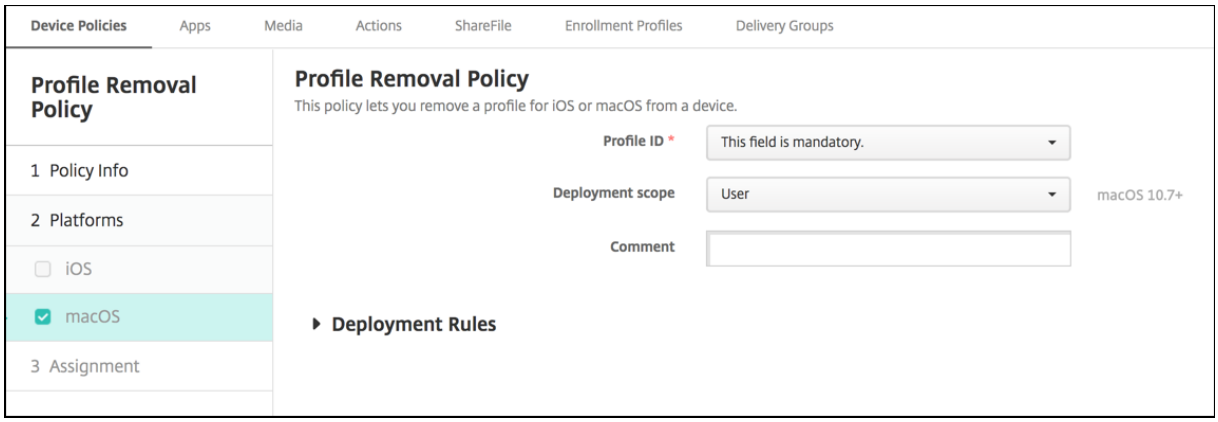
Geräterichtlinie für Profilentfernung

June 25, 2024

Sie können eine Richtlinie zum Entfernen von App-Profilen in Citrix Endpoint Management 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.

macOS-Einstellungen



- **Profil-ID:** Klicken Sie in der Dropdownliste auf die App-Profil-ID. Dieses Feld ist erforderlich.
- **Umfang der Bereitstellung:** Klicken Sie in der Dropdownliste 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

December 1, 2023

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 Citrix Endpoint Management 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

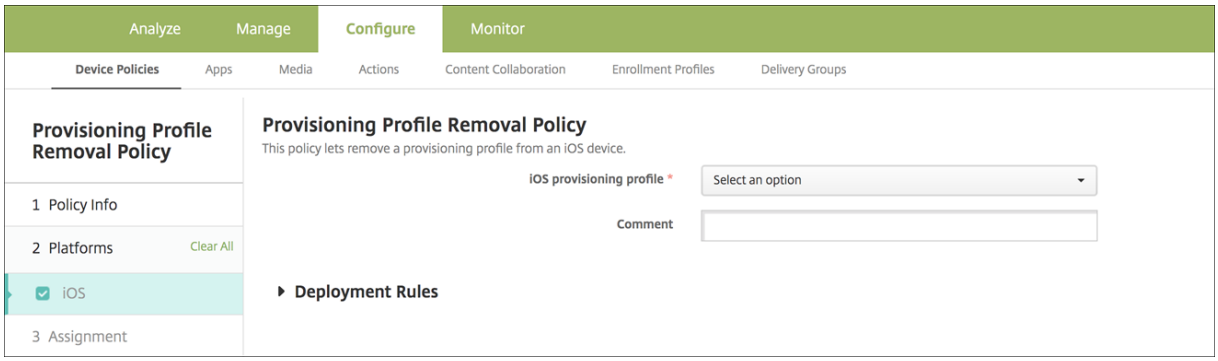
June 25, 2024

Mit einem Provisioningprofil können Sie iOS-Apps auf Benutzergeräten verteilen. Apps müssen mit einem Provisioningprofil signiert sein, damit sie auf einem iOS-Gerät ausgeführt werden können. Weitere Informationen finden Sie unter Provisioningprofilrichtlinie.

Mit der Richtlinie zum Entfernen von Provisioningprofilen können Sie ältere Provisioningprofile entfernen oder austauschen.

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 Dropdownliste auf das Provisioningprofil, das Sie entfernen möchten.
- **Kommentar:** Geben Sie optional einen Kommentar ein.

Proxy-Geräterichtlinie

June 25, 2024

Über die Proxy-Richtlinie legen Sie globale HTTP-Proxy-Einstellungen für unterstützte iOS-Geräte 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. Weitere Informationen finden Sie unter Bereitstellen von Geräten mit Apple Configurator 2 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. Dieses Feld ist erforderlich.
    * **Port für den Proxyserver:** Geben Sie die Portnummer des Proxyservers ein. Dieses Feld 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**.

- **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.

Geräteeinschränkungsrichtlinie

June 25, 2024

> **Hinweis:**
>
> Wenn ein Upgrade neue Einstellungen für die Einschränkungsrichtlinie enthält, müssen Sie die Richtlinie bearbeiten und speichern. Citrix Endpoint Management stellt eine aktualisierte Einschränkungsrichtlinie erst bereit, wenn Sie sie gespeichert haben.

Die Geräterichtlinie für Einschränkungen lässt bestimmte Features oder Funktionen wie z. B. die Kamera auf Benutzergeräten zu oder schränkt sie ein. Sie können Sicherheitsrichtlinien sowie Beschränkungen für Medieninhalte einstellen. Sie können auch einschränken, welche Apps 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.

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 ihrem Gerät verwenden. Bei Auswahl von **Aus** können Benutzer die Kamera auf ihrem Gerät nicht verwenden.
- **Screenshots:** Bei Auswahl von **Ein** können Benutzer Screenshots auf ihrem Gerät erstellen. Bei Auswahl von **Aus** können Benutzer keine Screenshots auf ihrem Gerät erstellen.

Wenn sowohl die Geräteeinschränkungsrichtlinie als auch die Kioskgeräterichtlinie konfiguriert ist, hat die Geräteeinschränkungsrichtlinie Vorrang.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

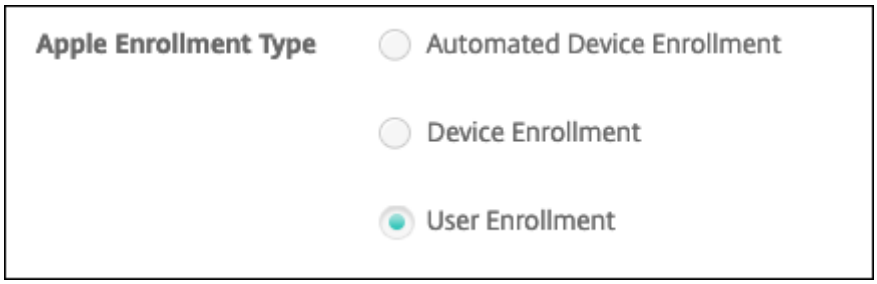
iOS-Einstellungen

Einige Einstellungen der iOS-Einschränkungsrichtlinie gelten nur für bestimmte iOS-Versionen, wie hier und auf der Seite zur Einschränkungsrichtlinie der Citrix Endpoint Management-Konsole beschrieben ist.

Diese Einstellungen gelten, wenn das Gerät im Benutzer-Registrierungsmodus, im nicht betreuten Modus (vollständiges MDM) oder im betreuten Modus registriert ist. Die folgende Tabelle enthält die Registrierungsmodi für jede Einstellung für iOS 13 und höher.

- **Automatisierte Geräteregistrierung:** Betreute Geräte. Das sind Geräte, die per Massenregistrierung registriert werden.
- **Geräteregistrierung:** Nicht betreute Geräte. Diese Geräte werden einzeln und im nicht betreuten Modus (vollständiges MDM) registriert.
- **Benutzerregistrierung:** Geräte, auf denen nur bestimmte Benutzer verwaltet werden. Weitere Informationen zur Benutzerregistrierung finden Sie in der Dokumentation von Apple.

Einstellungen der iOS-Einschränkungsrichtlinie können gelten, wenn das Gerät im Benutzer-Registrierungsmodus oder im nicht betreuten Modus (vollständiges MDM) 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 Citrix Endpoint Management registriert, gelten die Einstellungen für das Gerät.
- Wenn sich ein nicht betreutes Gerät mit iOS 13+ bei Citrix Endpoint Management registriert, gelten die Einstellungen nicht für das Gerät.
- Wenn ein Gerät mit iOS 12 (oder niedriger), das bereits bei Citrix Endpoint Management 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 Bereitstellen von Geräten mit Apple Configurator 2.

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Hardwaresteuerelemente zulassen			
Kamera	Nein	Ja	Ja
FaceTime	Nein	Nein	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
Temporäre Sitzung für geteiltes iPad zulassen	Nein	Nein	Ja
Sprachwahl	Nein	Ja	Ja
Siri	Ja	Ja	Ja
Zulassen, während Gerät gesperrt ist	Ja	Ja	Ja
Siri-Obszönitätenfilter	Nein	Nein	Ja
Apps installieren	Nein	Nein	Ja
Globale Hintergrundabfrage beim Roaming zulassen	Nein	Ja	Ja
Apps zulassen			
Apple App-Store	Nein	Nein	Ja
In-App-Käufe	Nein	Ja	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Apple App Store-Kennwort für Käufe erforderlich	Nein	Ja	Ja
Safari	Nein	Nein	Ja
Automatisch ausfüllen	Nein	Nein	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	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
Freigeben von verwalteten Dokumenten mit AirDrop	Ja	Ja	Ja
Sicherheit - Zulassen			

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Nicht vertrauenswürdige SSL-Zertifikate akzeptieren	Nein	Ja	Ja
Automatisches Update für Zertifikatvertrauensstellungsoptionen	Nein	Ja	Ja
Verwaltete Zwischenablage erforderlich	Ja	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 Diagnoseinformationen an Apple	Ja	Ja	Ja
Touch ID zum Entsperren von Gerät	Nein	Ja	Ja
Automatisches Entsperren	Nein	Ja	Ja
Wallet-Benachrichtigungen bei Sperre	Nein	Ja	Ja
Übergabe	Nein	Ja	Ja
iCloud-Synchronisierung für verwaltete Apps	Ja	Ja	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
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
Personalisierte Werbung von Apple zulassen	Nein	Ja	Ja
Einstellungen nur für Betreute Geräte - Zulassen			
eSIM-Änderung zulassen	Nein	Nein	Ja
Alle Inhalte und Einstellungen löschen	Nein	Nein	Ja
Bildschirmzeit	Nein	Nein	Ja
Podcasts	Nein	Nein	Ja
Installation von Konfigurationsprofilen	Nein	Nein	Ja
Touch ID- und Face ID-Änderung	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
Hintergrundbildänderung	Nein	Nein	Ja
Automatischer Download von Apps	Nein	Nein	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
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	Ja
Freunde hinzufügen	Nein	Nein	Ja
Multiplayer-Gaming	Nein	Nein	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
Netzlaufwerksverbindungen zulassen	Nein	Nein	Ja
USB-Geräteverbindungen zulassen	Nein	Nein	Ja
“Mein Gerät finden” zulassen	Nein	Nein	Ja
Einstellungen für Freundesuche zulassen	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

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
QuickPath-Tastatur zulassen	Nein	Nein	Ja
Definition nachschlagen	Nein	Nein	Ja
Einzelne App-Paket-ID			
Nachrichten	Nein	Nein	Ja
Apple Music	Nein	Nein	Ja
Apple Music	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
Ändern, ob WLAN ein- oder ausgeschaltet ist	Nein	Nein	Ja
Nur Wi-Fi-Netzwerken beitreten, die von einer Netzwerkrichtlinie 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

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Automatische Teilnahme an Klassen der Classroom-App ohne Aufforderung	Nein	Nein	Ja
AirPrint zulassen	Nein	Nein	Ja
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
Hinzufügen von VPN-Konfigurationen	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

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Authentifizierung vor automatischem Ausfüllen erzwingen	Nein	Nein	Ja
Automatisches Datum und Uhrzeit erzwingen	Nein	Nein	Ja
Kennwörter autom. ausfüllen	Nein	Nein	Ja
Kennwortanforderung bei Geräten in der Nähe	Nein	Nein	Ja
Kennwort teilen	Nein	Nein	Ja
Persönliche Hotspot-Änderung zulassen	Nein	Nein	Ja
Booten zur Wiederherstellung durch ein nicht gekoppeltes Gerät zulassen	Nein	Nein	Ja
Schnelle Sicherheitsmaßnahme installieren	Nein	Nein	Ja
Schnelle Sicherheitsmaßnahme entfernen	Nein	Nein	Ja
E-Mail-Datenschutz zulassen	Nein	Nein	Ja
NFC	Nein	Nein	Ja
App-Clips zulassen	Nein	Nein	Ja
Sicherheit - Auf Sperrbildschirm anzeigen			
Kontrollzentrum	Ja	Ja	Ja
Benachrichtigung	Ja	Ja	Ja
Heuteansicht	Ja	Ja	Ja

Einstellung	Benutzerregistrierung	Unbetreut	Betreut
Medieninhalte - Zulassen			
Anstößige Musik, Podcasts und iTunes U-Inhalte	Nein	Nein	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 Lernende 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.
  - **Temporäre Sitzung für geteiltes iPad zulassen:** Verhindert den Zugriff auf temporäre Sitzungen auf geteilten iPads.

  - **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**

  - **Apple App Store:** Zugriff auf den Apple App Store zulassen. Für betreute iOS-Geräte.
  - **In-App-Käufe:** Zulassen, dass Benutzer In-App-Käufe machen.
    * **Apple App Store-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.
  - **Verwaltete Zwischenablage erforderlich:** Für Kopieren und Einfügen können die gleichen Einschränkungen gelten wie für **Dokumente von verwalteten Apps in nicht verwalteten Apps** und **Dokumente von nicht verwalteten Apps in verwalteten Apps**. Konfigurieren Sie beispielsweise Folgendes:
    * **Verwaltete Zwischenablage erforderlich** Ein
    * **Dokumente von verwalteten Apps in nicht verwalteten Apps:** Aus
    * **Dokumente von nicht verwalteten Apps in verwalteten Apps:** Ein
      Nach dem Bereitstellen der Richtlinie auf iOS-Geräten können Benutzer keine Daten aus verwalteten Apps in nicht verwaltete Apps kopieren und einfügen, sie können jedoch Daten aus nicht verwalteten Apps in verwaltete Apps kopieren und einfügen.
  - **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 oder Face ID zum Entsperren von Gerät:** Entsperren von Geräten per Touch ID oder Face ID zulassen.
- **Automatisches Entsperren:** Wenn diese Option auf **Aus** festgelegt ist, kann der Benutzer die Apple Watch nicht verwenden, um ein gekoppeltes iPhone zu entsperren. Die Standardeinstellung ist **Ein**. Verfügbar für iOS 14.5 oder höher.
- **Wallet-Benachrichtigungen bei Sperre:** Anzeige von Wallet-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.
- **Personalisierte Werbung von Apple zulassen:** Wenn die Option auf **Aus** festgelegt ist, werden die Daten der Benutzer von der Apple-Werbeplattform nicht zur Bereitstellung personalisierter Werbung verwendet. Die Standardeinstellung ist **Ein**. Verfügbar für iOS 14.0 oder höher.

- **Einstellungen nur für Betreute Geräte - Zulassen**

  Diese Einstellungen gelten nur für überwachte Geräte. Die Schrittfolge, mit der Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Bereitstellen von Geräten mit Apple Configurator 2.

- **eSIM-Änderung zulassen:** Benutzer können die eSIM-Einstellungen auf ihrem Gerät ändern.
- **Alle Inhalte und Einstellungen löschen:** Löschen aller Inhalte und Einstellungen von den Geräten zulassen.
- **Bildschirmzeit:** Benutzer können die Bildschirmzeit aktivieren.
- **Podcasts:** Download und Synchronisierung von Podcasts zulassen.
- **Installation von Konfigurationsprofilen:** Installation eines anderen Konfigurationsprofils als des von Ihnen bereitgestellten zulassen.
- **Touch ID- und Face ID-Änderung:** Benutzer können ihre Touch ID oder Face ID ändern oder löschen.
- **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.
- **Netzlaufwerksverbindungen zulassen:** Verhindert die Verbindung mit Netzlaufwerken in der App "Files".
- **USB-Geräteverbindungen zulassen:** Verhindert das Verbinden mit angeschlossenen USB-Geräten in der App "Files".
- **"Mein Gerät finden"zulassen:** Deaktiviert die Option **Mein Gerät finden** in der App "Wo ist?".
- **Einstellungen für Freundesuche zulassen:** Deaktiviert die Option **Meine Freunde suchen** in der App "Wo ist?".
- **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.
- **Apple Music:** Verwendung von Apple Music 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**.
- **Ändern, ob WLAN ein- oder ausgeschaltet ist:** Verhindert, dass Wi-Fi in den Einstellungen oder im Kontrollzentrum aktiviert oder deaktiviert wird. Das Aktivieren des Flugzeugmodus'hat ebenfalls keine Wirkung. Diese Einschränkung verhindert nicht die Auswahl eines bestimmten Wi-Fi-Netzwerks.
- **Nur Wi-Fi-Netzwerken beitreten, die von einer Netzwerkrichtlinie installiert wurden:** optional. 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. Diese Einstellung 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. Die Richtlinie für OS-Updates enthält weitere Einstellungen, die steuern, wie oft Geräte Updates empfangen. Weitere Informationen finden Sie unter Geräterichtlinie für OS-Updates.
- **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.
- **Authentifizierung vor automatischem Ausfüllen erzwingen:** Benutzer müssen sich authentifizieren, bevor sie das automatische Ausfüllen verwenden können.

- **Automatisches Datum und Uhrzeit erzwingen:** Ermöglicht, Datum und Uhrzeit auf betreuten Geräten automatisch einzustellen. Mit **Ein** können Gerätebenutzer die Option **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.
- **Persönliche Hotspot-Änderung zulassen:** Verhindert, dass Benutzer die persönlichen Hotspot-Einstellungen ändern.
- **Booten zur Wiederherstellung durch ein nicht gekoppeltes Gerät zulassen:** Wen diese Option auf **Ein** festgelegt ist, können Geräte von einem nicht gekoppelten Gerät zur Wiederherstellung gestartet werden. Die Standardeinstellung ist **Aus**. Verfügbar für iOS 14.5 oder höher.
- **Schnelle Sicherheitsreaktion installieren:** Wenn diese Option auf **Aus** festgelegt ist, wird die Installation von schnellen Sicherheitsreaktionen verhindert. Die Standardeinstellung ist **Ein**.
- **Schnelle Sicherheitsreaktion entfernen:** Wenn diese Option auf **Aus** festgelegt ist, wird das Entfernen schneller Sicherheitsreaktionen verhindert. Die Standardeinstellung ist **Ein**.
- **E-Mail-Datenschutz zulassen:** Wenn diese Option auf **Aus** festgelegt ist, wird der E-Mail-Datenschutz auf dem Gerät deaktiviert. Die Standardeinstellung ist **Ein**. Verfügbar für iOS 15.2 oder höher.
- **NFC:** Wenn die Option auf **Aus** festgelegt ist, wird NFC deaktiviert. Die Standardeinstellung ist **Ein**. Verfügbar für iOS 14.2 oder höher.
- **App-Clips zulassen**: Wenn die Option auf **Aus** festgelegt ist, kann ein Benutzer keine App-Clips hinzufügen, und alle vorhandenen App-Clips auf dem Gerät werden entfernt. Die Standardeinstellung ist **Ein**. Verfügbar für iOS 14.0 oder höher.

- **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.

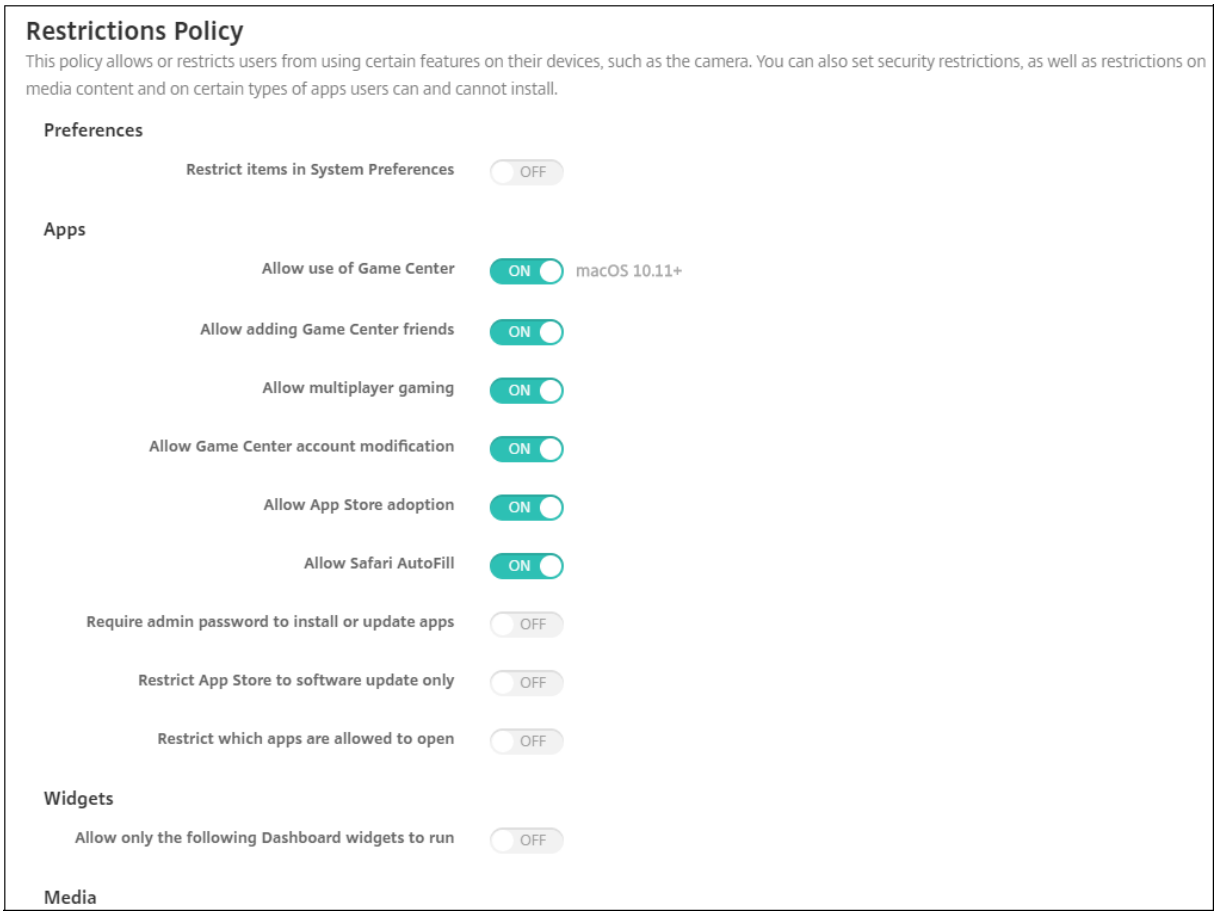
- **Medieninhalte - Zulassen**

  - **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



Einstellung	Unbetreut	Betreut
Apps		
Game Center zulassen	Nein	Ja
Hinzufügen von Game Center-Freunden zulassen	Nein	Ja
Multiplayer-Gaming zulassen	Nein	Ja
Game Center-Kontoänderung zulassen	Ja	Ja
Übernahme in App Store zulassen	Ja	Ja
Autom. ausfüllen in Safari zulassen	Nein	Ja
Admin-Kennwort zum Installieren oder Aktualisieren von Apps erforderlich	Ja	Ja

Einstellung	Unbetreut	Betreut
App Store auf Softwareupdates beschränken	Ja	Ja
Öffnen von Apps beschränken	Ja	Ja
Medien		
AirDrop zulassen	Nein	Ja
Funktionalität		
Desktopbild sperren	Nein	Ja
Verwendung der Kamera zulassen	Nein	Ja
Apple Music zulassen	Nein	Ja
Spotlight-Vorschläge zulassen	Ja	Ja
LookUp zulassen	Ja	Ja
iCloud-Kennwort für lokale Konten verwenden	Ja	Ja
iCloud-Dokumente & -Daten zulassen	Ja	Ja
iCloud-Desktop und -Dokumente zulassen	Nein	Ja
Synchronisieren des iCloud-Schlüsselbunds zulassen	Nein	Ja
iCloud-Mail zulassen	Ja	Ja
iCloud-Kontakte zulassen	Ja	Ja
iCloud-Kalender zulassen	Ja	Ja
iCloud-Erinnerungen zulassen	Ja	Ja
iCloud-Lesezeichen zulassen	Ja	Ja
iCloud-Notizen zulassen	Ja	Ja
iCloud-Fotos zulassen	Ja	Ja
Automatisches Entsperren zulassen	Ja	Ja
Entsperren des Macs durch Touch ID zulassen	Ja	Ja
Verzögerte Softwareupdates erzwingen	Nein	Ja

Einstellung	Unbetreut	Betreut
Kennwörter autom. ausfüllen	Nein	Ja
Kennwortanforderung bei Geräten in der Nähe	Nein	Ja
Kennwort teilen	Ja	Ja

- **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
      · Allgemein
      · Bedienungshilfen
      · App Store
      · Softwareupdate
      · Bluetooth
      · CDs & DVDs
      · Datum und 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
- Freigabe
- 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**. Verwenden Sie für mobile Produktivitätsapps von Citrix die ID aus dem Feld **Paket-**

ID, wenn Sie die App hinzufügen. Wiederholen Sie diesen Schritt für jede App, die gestartet werden darf.

* **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:** Bei Auswahl von **Ein** können Benutzer nur die in dieser Einstellung konfigurierten Dashboard-Widgets ausführen. 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, Standorten usw. mit nahegelegenen iOS-Geräten zulassen.
- **Freigabe**
  - **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-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**

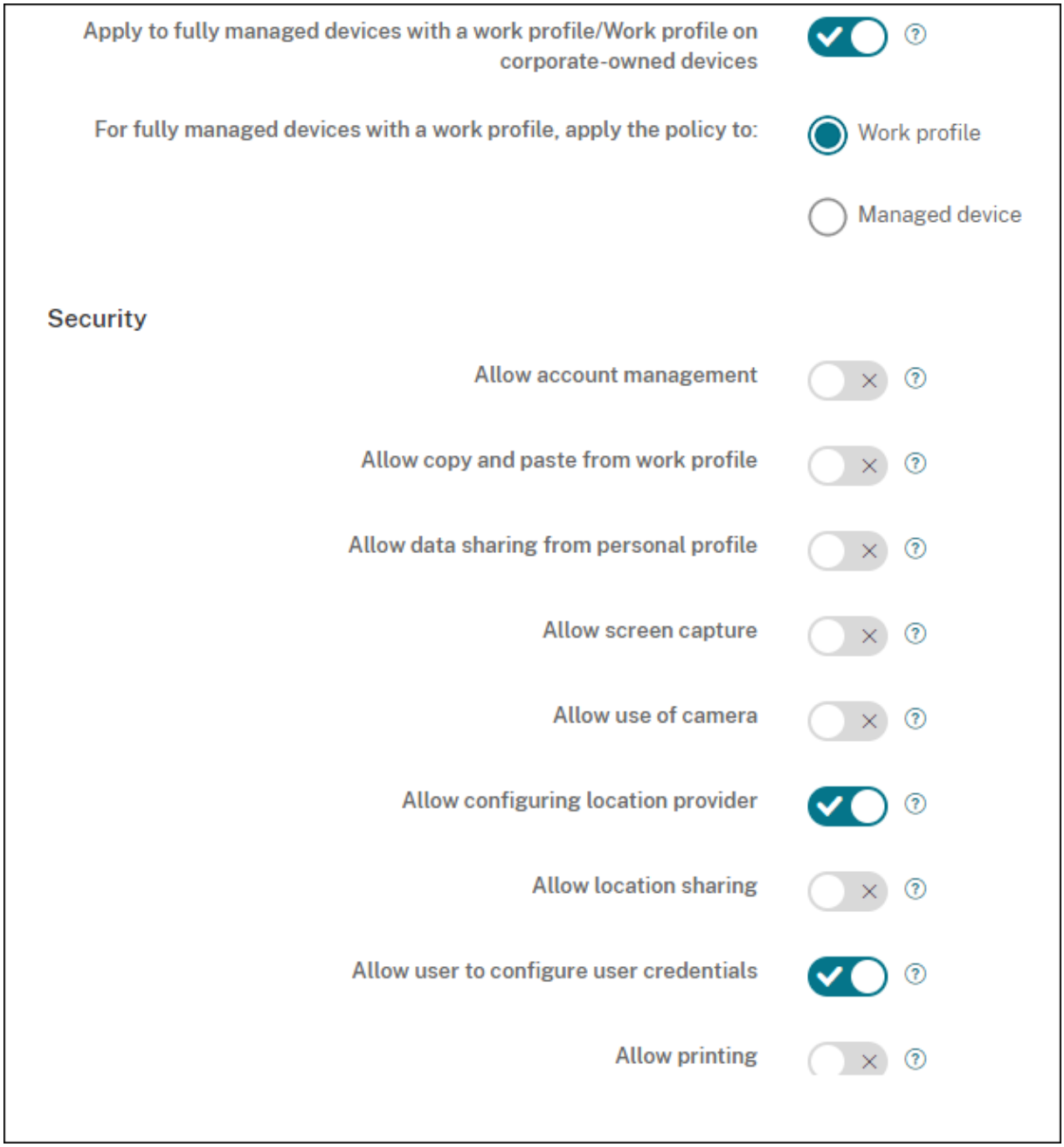
  - **Desktopbild sperren:** Wählen Sie aus, ob Benutzern das Ändern des Desktopbilds gestattet werden soll. Die Standardeinstellung ist **Aus**, d. h. Benutzer können das Desktopbild ändern.
  - **Verwendung der Kamera zulassen:** Wählen Sie aus, ob Benutzern die Verwendung der Kamera auf Macs gestattet 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 Benutzer Spotlight-Vorschläge für die Suche auf ihrem Mac und aus Internet und dem App-Store verwenden dürfen. 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 Look Up 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 **Ein**, d. h. die Benutzer können nicht von ihren Macs 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. Die Richtlinie für OS-Updates enthält weitere Einstellungen, die steuern, wie oft Geräte Updates empfangen. Weitere Informationen finden Sie unter Geräterichtlinie für OS-Updates.
- **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. Der Standardwert ist **Ein**. (macOS 10.14 und höher)
- **Kennwortanforderung bei Geräten in der Nähe:** Optional. Wenn die Option deaktiviert ist, fordern Benutzergeräte keine Kennwörter von Geräten in der Nähe an. Der Standardwert ist **Ein**. (macOS 10.14 und höher)
- **Kennwort teilen:** Optional. Wenn diese Option deaktiviert ist, können Benutzer ihre Kennwörter nicht per AirDrop teilen. Der Standardwert ist **Ein**. (macOS 10.14 und höher)

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 9.0-10.x als vollständig verwaltetes Gerät mit

einem Arbeitsprofil registriert. Geräte ab Android 11 werden als Arbeitsprofil auf unternehmenseigenem 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, funktionieren die folgenden Einschränkungen nicht:

- Backupdienst zulassen
- System-Apps aktivieren
- 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.

Sehen Sie sich dieses Video an, um mehr zu erfahren:

- **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. Diese Geräte werden auch als COPE-Geräte (Unternehmenseigentum, vom Benutzer verwaltet) bezeichnet. 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 folgenden Einstellungen:

- **Sicherheit**
  - **Kontoverwaltung zulassen:** Ermöglicht die Kontenverwaltung im Arbeitsprofil und auf verwalteten Geräten. Die Standardeinstellung ist **Aus**.
  - **Kopieren und Einfügen aus dem Arbeitsprofil zulassen:** Bei der Einstellung **Ein** können Benutzer Daten aus Apps im Arbeitsprofil kopieren und in Apps im persönlichen Profil einfügen. Die Standardeinstellung ist **Aus**.

- **Datenfreigabe aus dem persönlichen Profil zulassen:** Bei der Einstellung **Ein** können Benutzer Dateien und Daten aus Apps im persönlichen Profil kopieren und in Apps im Arbeitsprofil einfügen sowie freigeben. 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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**.
  - **Nicht-Google Play-Apps für alle Profile zulassen:** Bei der Einstellung **Ein** können Benutzer Apps aus anderen Stores als Google Play für alle Profile des Geräts installieren. 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**.

- **BYOD-Arbeitsprofil**

  - **Verbundene Apps aktivieren:** Wenn diese Option aktiviert ist, können Benutzer Apps auswählen, die über Arbeitsprofile und private Profile hinweg kommunizieren können und

dabei sowohl Firmendaten als auch persönliche Daten verwenden. Klicken Sie nach der Aktivierung auf **Hinzufügen**, wählen Sie die gewünschten Apps aus und klicken Sie dann auf **Speichern**. Zur Aktivierung dieses Features ist ein Arbeitsprofil erforderlich. Die Standardeinstellung ist **Aus**.

- **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 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.
  - **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 Keyguard das Gerät sperrt:** Wird diese Einstellung auf **Ein** festgelegt, deaktiviert sie die Tastatursperre 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.
- **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: Vollständig verwaltetes Gerät**

  - **Sperrprüfung aktivieren:** Prüfung auf gesperrte Zertifikate aktivieren. Die Standardeinstellung ist **Aus**.

Wenn **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil bzw. Arbeitsprofil auf unternehmenseigenen Geräten 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 Citrix Endpoint Management 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 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 Citrix Endpoint Management 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**.

- **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: Vollständig verwaltetes Gerät**

  - **Sperrprüfung aktivieren:** Prüfung auf gesperrte Zertifikate aktivieren. Die Standardeinstellung ist **Aus**.

Wenn **Auf vollständig verwaltete Geräte mit einem Arbeitsprofil bzw. Arbeitsprofil auf unternehmenseigenen Geräten anwenden** aktiviert ist und für **Richtlinie bei vollständig verwalteten Geräten mit einem Arbeitsprofil anwenden auf:** die Einstellung **Verwaltetes Gerät** gewählt ist, konfigurieren Sie die folgenden 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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**.

• **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.
- **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**.
- **Schutz beim Zurücksetzen auf die Werkseinstellungen zulassen:** Bei der Einstellung **Ein** muss der Benutzer beim Zurücksetzen des Geräts per Wiederherstellungsmodus die Anmeldeinformationen für das Konto angeben, das sich vor dem Zurücksetzen auf dem Gerät befand. Benutzer können auch die Gerätesperre bereitstellen, wenn sie vor dem

Zurücksetzen eingestellt wurde. Bei der Einstellung **Aus** ist nach dem Zurücksetzen keine Authentifizierung erforderlich. 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 Keyguard das Gerät sperrt:** Wird diese Einstellung auf **Ein** festgelegt, deaktiviert sie die Tastatursperre 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 Verbindun-

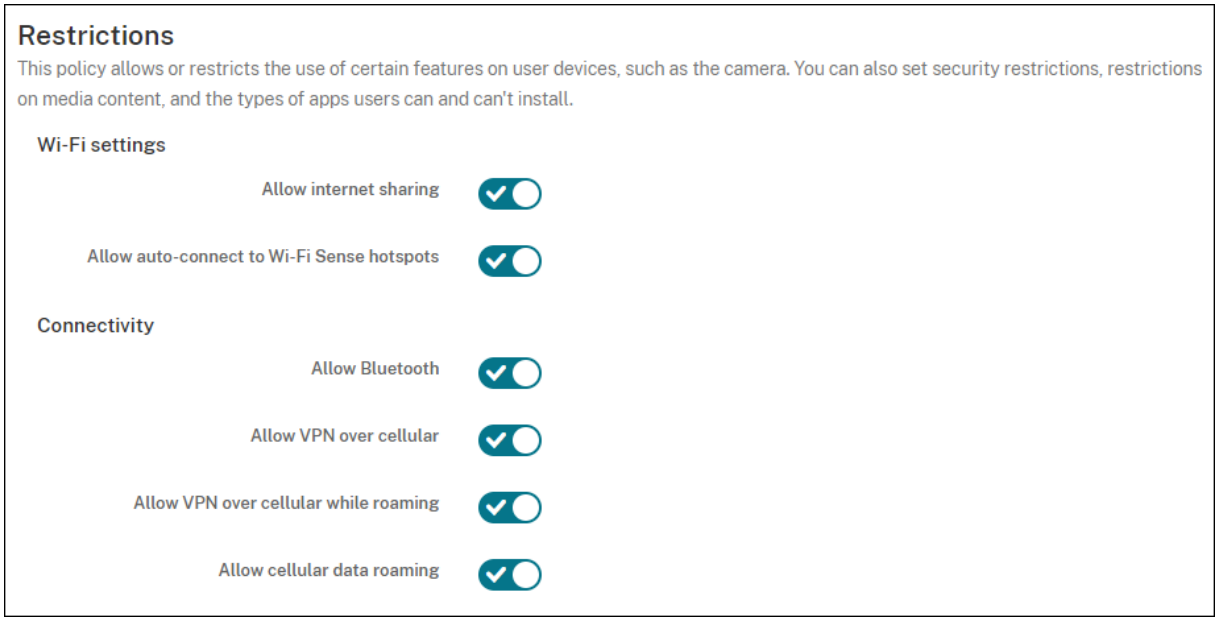
gen zu verwenden (MDM 4.0 oder höher). Die Standardeinstellung ist **Ein**.

- **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: Vollständig verwaltetes Gerät**

  - **Sperrprüfung aktivieren:** Prüfung auf gesperrte Zertifikate aktivieren. Die Standardeinstellung ist **Aus**.

Windows Desktop/Tablet-Einstellungen



- **WiFi-Einstellungen**

  - **Internetfreigabe zulassen:** gemeinsame Verwendung der Internetverbindung eines Geräts mit anderen Geräten durch Nutzung des Geräts als Wi-Fi-Hotspot zulassen.

- **Konnektivität**

  - **Bluetooth zulassen:** Verbindungen von Geräten über Bluetooth zulassen.
  - **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.
  - **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.

- **System**

  - **Speicherkarte zulassen:** Verwendung einer Speicherkarte durch Geräte zulassen.
  - **Telemetrie:** Klicken Sie in der Dropdownliste 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**.
  - **App-Zugriff auf Positionsdienst zulassen:** App-Zugriff auf 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.

- **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:** Zulassen, dass die Registrierung eines Geräts bei Citrix Endpoint Management MDM manuell aufgehoben werden kann.
  - **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.

  - **Popupbenachrichtigungen auf dem Sperrbildschirm zulassen:** Popup-Benachrichtigungen auf dem Sperrbildschirm zulassen. Nur für Windows Desktop/Tablet.

- **Apps**

  - **Automatische Updates aus dem App Store zulassen:** Automatische Aktualisierung von Apps aus dem App Store zulassen. Nur für Windows Desktop/Tablet.

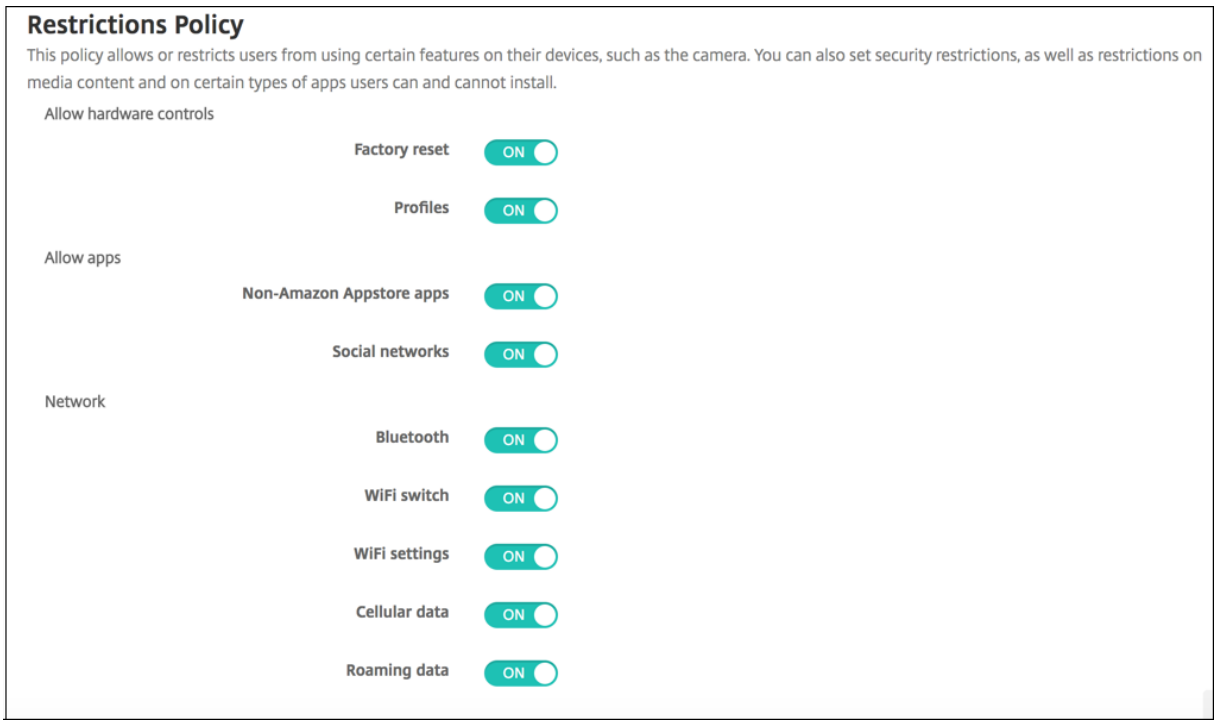
- **Datenschutz:** nur für Windows Desktop/Tablet.

  - **Eingabepersonalisierung zulassen:** Ausführen der Eingabepersonalisierung zulassen. Dieser Dienst verbessert die Eingabevorhersage (zum Beispiel für Stift und Bildschirmtastatur) je nach Eingabe des Benutzers.

- **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.
  - **Wi-Fi-Switch:** Wechseln des Wi-Fi-Verbindungszustands durch Apps zulassen.
  - **Wi-Fi-Einstellungen:** Ändern der Wi-Fi-Einstellungen zulassen.
  - **Mobile Netzwerke konfigurieren:** Ermöglicht Benutzern die Verwendung ihrer Mobilfunkdatenverbindung.
  - **Roamingdaten:** Verwendung mobiler Daten beim Roaming zulassen.
  - **Ortungsdienste:** GPS-Verwendung zulassen.
- **USB-Aktionen:**
  - **Debugging:** USB-Verbindungen mit einem Computer für das Debugging zulassen.

Roamingrichtlinie

December 1, 2023

Sie können in Citrix Endpoint Management eine Geräterichtlinie einrichten, um vorzugeben, ob Sprach- und Datenroaming auf unterstützten iOS-Geräten zugelassen wird. Wird Sprachroaming deaktiviert, dann wird Datenroaming automatisch auch deaktiviert.

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 Standardeinstellung ist **Aus**, Sprachroaming ist also zugelassen.
- **Datenroaming deaktivieren:** Wählen Sie aus, ob das Datenroaming deaktiviert werden soll. Diese Option ist nur verfügbar, wenn Sprachroaming aktiviert ist. Die Standardeinstellung ist **Aus**, Datenroaming ist also zugelassen.

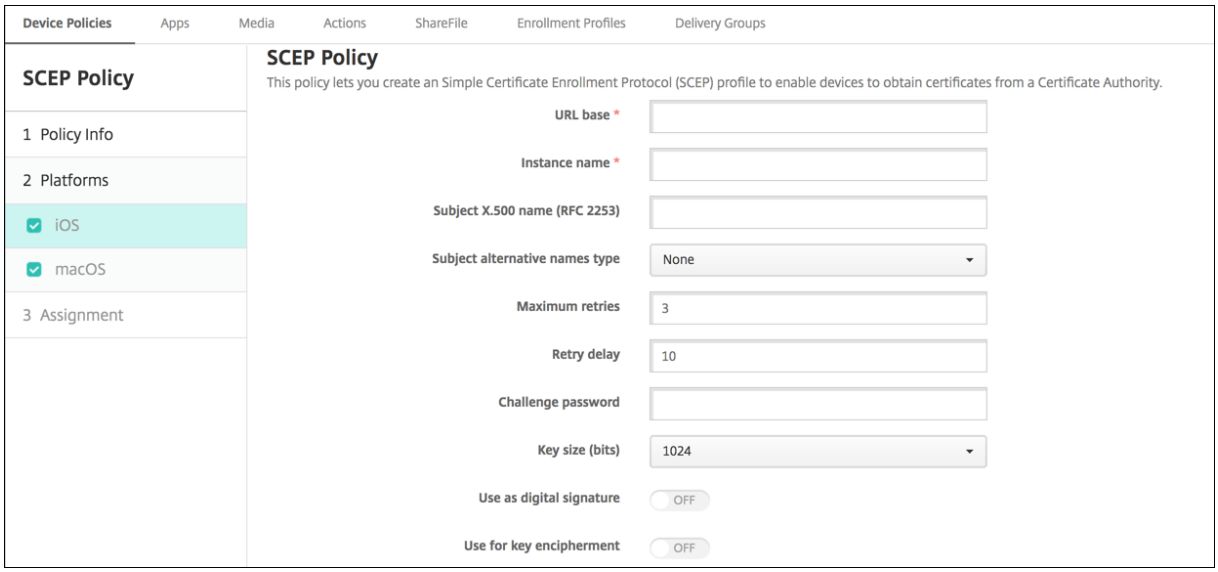
SCEP-Geräterichtlinie

December 1, 2023

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. Um Zertifikate mit SCEP von einer mit Citrix Endpoint Management verbundenen PKI auf Geräten bereitzustellen, 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.

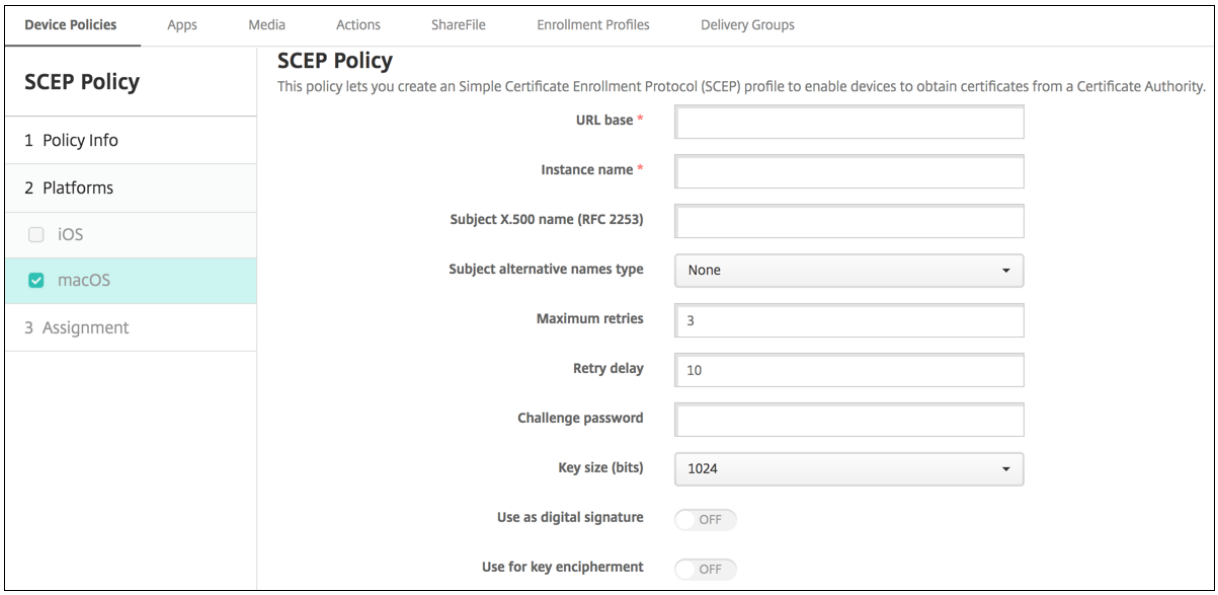
iOS-Einstellungen



- **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 wiederverwendet werden soll, verwenden Sie HTTPS, um das Kennwort zu schützen. 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`. Dies wird übersetzt in `[ [ ["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:** Wählen Sie einen alternativen Namenstyp. Ein optional verwendeter, alternativer Namenstyp kann die von der Zertifizierungsstelle für die Ausstellung eines Zertifikats angeforderten Werte bereitstellen. 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:** Wählen Sie, ob das Zertifikat als digitale Signatur verwendet werden soll. Der SCEP-Server überprüft die Verwendung des Zertifikats als digitale Signatur, bevor der Hash mit dem öffentlichen Schlüssel entschlüsselt wird.
- **Für Schlüsselchiffrierung verwenden:** Wählen Sie, ob das Zertifikat für die Schlüsselchiffrierung verwendet werden soll. Ein Server prüft zunächst, ob das vom Client bereitgestellte Zertifikat für die Schlüsselverschlüsselung zulässig ist. Anschließend verwendet der Server den öffentlichen Schlüssel in einem Zertifikat, um zu überprüfen, ob ein Datenelement mit dem privaten Schlüssel verschlüsselt wurde. Sonst kann die Spiegelung nicht durchgeführt werden.
- **SHA-256-Fingerabdruck (hexadezimale Zeichenfolge):** Wenn Ihre Zertifizierungsstelle HTTP verwendet, geben Sie hier den Fingerabdruck des ZS-Zertifikats an. Mit dem Fingerabdruck bestätigt das Gerät die Authentizität der Antwort der Zertifizierungsstelle bei der Registrierung. Sie können einen SHA-256-Fingerabdruck bereitstellen 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 wiederverwendet werden soll, verwenden Sie HTTPS, um das Kennwort zu schützen. 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`. Dies wird übersetzt in `[ [ ["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:** Wählen Sie einen alternativen Namenstyp. Ein optional verwendeter, alternativer Namenstyp kann die von der Zertifizierungsstelle für die Ausstellung eines Zertifikats angeforderten Werte bereitstellen. 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:** Wählen Sie, ob das Zertifikat als digitale Signatur verwendet werden soll. Der SCEP-Server überprüft die Verwendung des Zertifikats als digitale Signatur, bevor der Hash mit dem öffentlichen Schlüssel entschlüsselt wird.
- **Für Schlüsselchiffrierung verwenden:** Wählen Sie, ob das Zertifikat für die Schlüsselchiffrierung verwendet werden soll. Ein Server prüft zunächst, ob das vom Client bereitgestellte Zertifikat für die Schlüsselverschlüsselung zulässig ist. Anschließend verwendet der Server den öffentlichen Schlüssel in einem Zertifikat, um zu überprüfen, ob ein Datenelement mit dem privaten Schlüssel verschlüsselt wurde. Sonst kann die Spiegelung nicht durchgeführt werden.
- **SHA-256-Fingerabdruck (hexadezimale Zeichenfolge):** Wenn Ihre Zertifizierungsstelle HTTP verwendet, geben Sie hier den Fingerabdruck des ZS-Zertifikats an. Mit dem Fingerabdruck bestätigt das Gerät die Authentizität der Antwort der Zertifizierungsstelle bei der Registrierung. Sie können einen SHA-256-Fingerabdruck bereitstellen 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.

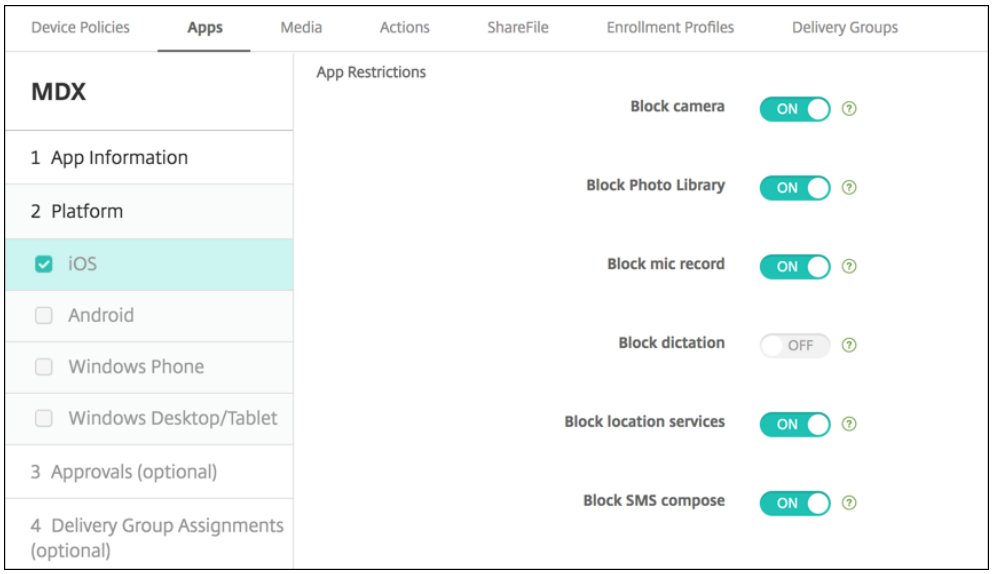
Richtlinien für Siri und die Diktierfunktion

December 1, 2023

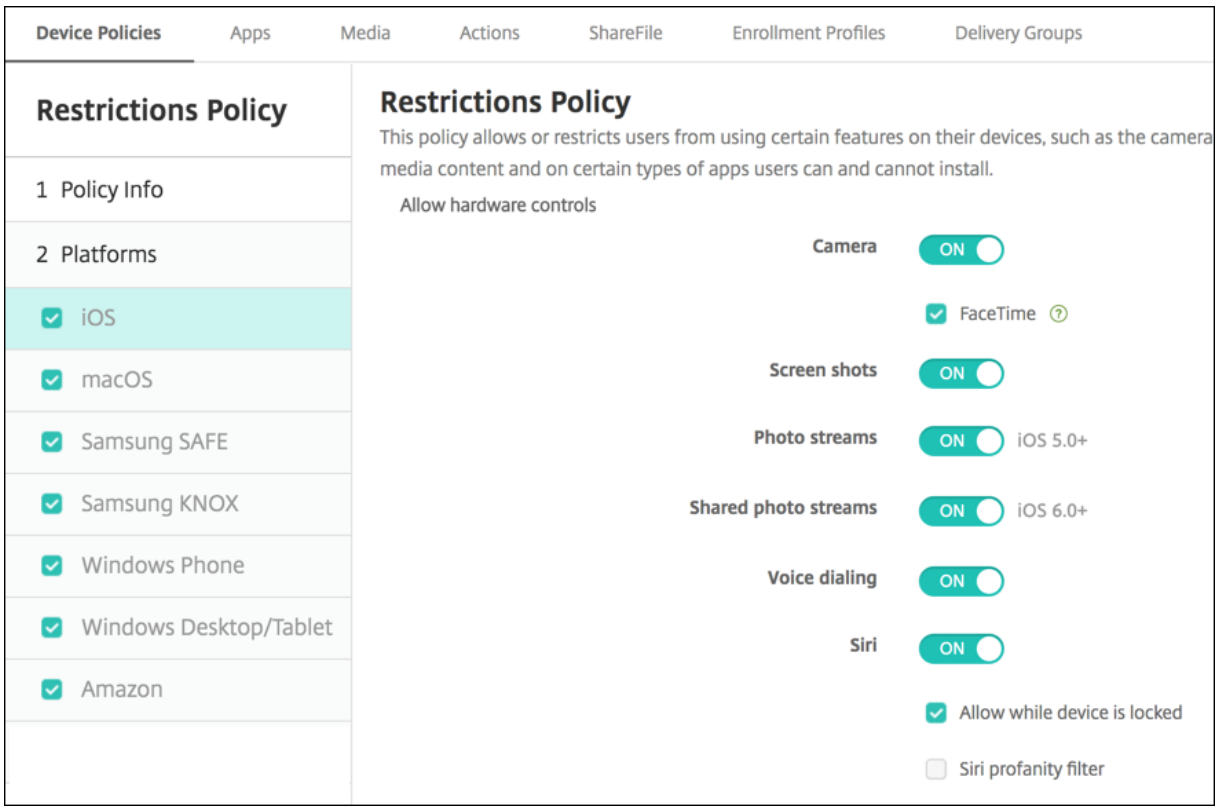
Wenn Benutzer auf einem iOS-Gerät Siri eine Frage stellen oder Text diktieren, werden die Sprachdaten von Apple zur Verbesserung von Siri gesammelt. Die Sprachdaten werden über die cloudbasierten Dienste von Apple gesendet und verlassen somit den sicheren Citrix Endpoint Management-Container. Diktierter Text verbleibt dagegen im Container.

Über Citrix Endpoint Management 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 Citrix Endpoint Management-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.
- Die Apple-Datenschutzrichtlinie können Sie auf jedem iOS-Gerät über **Einstellungen > Allgemein > Tastaturen** und Tippen auf den Link unter **Diktierfunktion aktivieren** aufrufen.

SSO-Kontorichtlinie

June 25, 2024

Mit der SSO-Kontorichtlinie können Sie Single Sign-On-Konten in Citrix Endpoint Management erstellen. Mit solchen Konten können die Benutzer nach einmaliger Anmeldung auf Citrix Endpoint Management und interne Unternehmensressourcen von unterschiedlichen Apps aus zugreifen. 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.

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. Dieses Feld ist erforderlich.
- **Kerberos-Prinzipalname:** Geben Sie den Kerberos-Prinzipalnamen ein. Dieses Feld ist erforderlich.
- **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen):** Klicken Sie in der Dropdownliste 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). Dieses Feld 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. Beispiel: `https://shopping.apple.com` ist gültig, `https://*.apple.com` nicht.

    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.
- **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.

Store-Geräterichtlinie

December 1, 2023

Sie können in Citrix Endpoint Management eine Richtlinie erstellen, mit der Sie angeben, ob auf dem Homebildschirm von Geräten ein App-Store-Webclip angezeigt werden soll.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

iOS-, Android- und Windows-Desktop/-Tableteinstellungen

Legen Sie für jede Plattform, die Sie konfigurieren, fest, ob ein App-Store-Webclip auf den Geräten angezeigt werden soll. Die Standardeinstellung ist **Ein**.

Richtlinie für abonnierte Kalender

December 1, 2023

Sie können in Citrix Endpoint Management 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 auf der Apple-Supportsite unter “Downloads”.

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. Dieses Feld ist erforderlich.
- **URL:** Geben Sie die Kalender-URL ein. Sie können eine `webcal://`-URL oder einen `https://`-Link zu einer iCalendar-Datei (.ics) eingeben. Dieses Feld ist erforderlich.
- **Benutzername:** Geben Sie den Anmeldenamen des Benutzers ein. Dieses Feld 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

December 1, 2023

Sie erstellen Geräterichtlinien mit Nutzungsbestimmungen in Citrix Endpoint Management, wenn die Benutzer die unternehmensspezifischen Richtlinien für Verbindungen mit dem Unternehmensnetzwerk akzeptieren sollen. Wenn Benutzer ihr Gerät bei Citrix Endpoint Management 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**.

> **Hinweis:**
>
> Die Allgemeinen Geschäftsbedingungen werden nicht angezeigt, wenn ein iOS-Gerät über das Device Enrolment Program (DEP) registriert wurde.

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**.

Geräterichtlinie für Tunnel

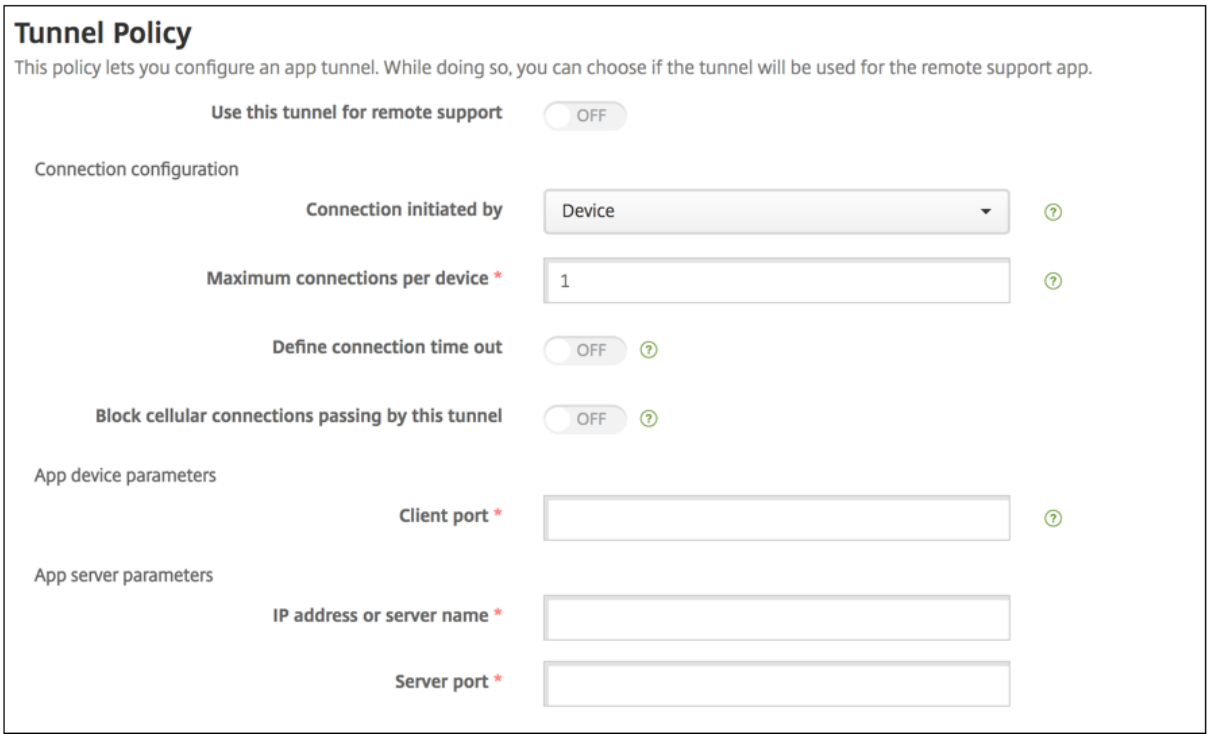
June 25, 2024

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 die Tunnelrichtlinie für Android-Geräte konfigurieren.

Jeglicher App-Datenverkehr, der über einen in dieser Richtlinie definierten Tunnel gesendet wird, durchläuft zunächst Citrix Endpoint Management, 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



- **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. Wi-Fi- und USB-Verbindungen werden nicht blockiert.
- **Clientport:** Geben Sie die Nummer des Clientports ein. Normalerweise ist diese mit der des Serverports identisch.
- **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.

VPN-Geräterichtlinie

June 25, 2024

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.

> **Hinweis:**
>
> Citrix SSO für Android und iOS heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation, um diese Namensänderung widerzuspiegeln.

Anforderungen für Pro-App-VPNs

Sie konfigurieren die Pro-App-VPN-Funktion für die folgenden Plattformen über VPN-Richtlinien:

- iOS
- macOS
- Android (Legacy-Geräteadmin)

Mit der Geräterichtlinie für verwaltete Konfigurationen können Sie VPN-Profile für Android Enterprise konfigurieren.

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.	

Plattform	Verbindungstyp	Anmerkung
Android (Legacy-Geräteadmin)	Citrix SSO	

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 NetScaler Gateway
- Die folgenden Anwendungen sind auf dem Gerät installiert:
  - Citrix SSO
  - Citrix Secure Hub

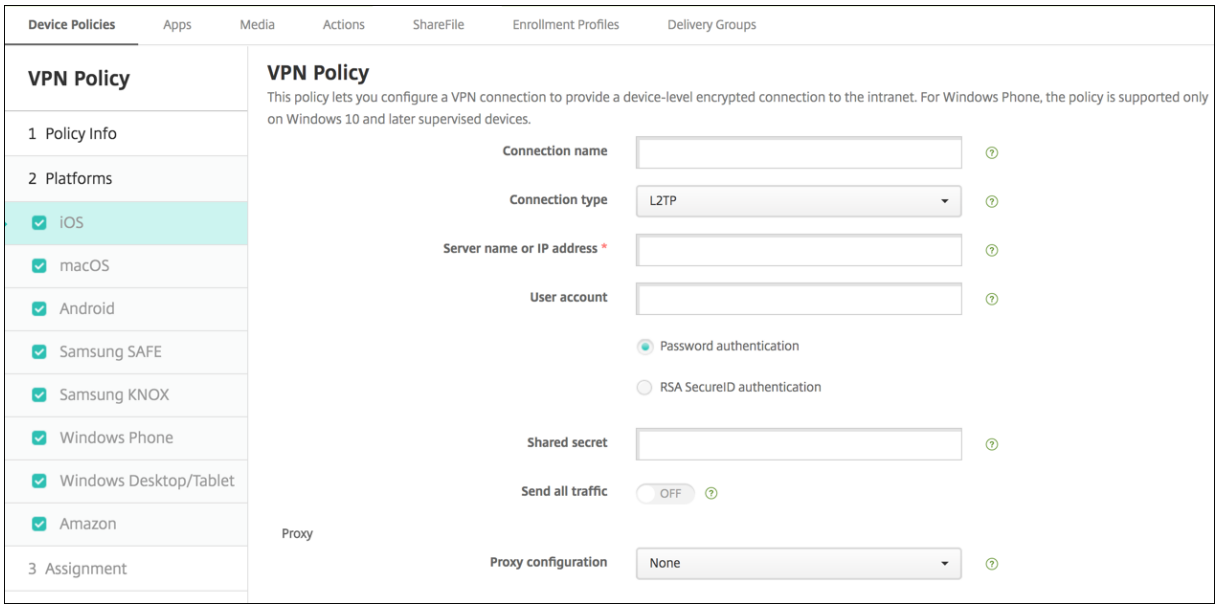
Ein allgemeiner Workflow zur Konfiguration eines Pro-App-VPN für iOS- und Android-Geräte mit der Citrix SSO-App ist wie folgt:

1. Konfigurieren Sie eine VPN-Geräterichtlinie wie in diesem Artikel beschrieben.
   - Informationen zu iOS finden Sie unter Citrix SSO-Protokoll für iOS konfigurieren. 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 Pro-App-VPN-Zugriff konfigurieren.
     - Wenn Sie für **Authentifizierungstyp für Verbindung** die Option **Zertifikat** auswählen, müssen Sie zuerst die zertifikatbasierte Authentifizierung für Citrix Endpoint Management konfigurieren. Siehe Authentifizierung mit Clientzertifikat oder Zertifikat und Domäne.
   - Informationen zu Android (Legacy-Geräteadmin) finden Sie unter Citrix SSO-Protokoll für Android konfigurieren.
     - Wenn Sie für **Authentifizierungstyp für Verbindung** die Option **Zertifikat** oder **Kennwort und Zertifikat** auswählen, müssen Sie zuerst die zertifikatbasierte Authentifizierung für Citrix 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 NetScaler Gateway.

iOS-Einstellungen

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 mit den folgenden Einstellungen hinzu:
    - **Verbindungstyp: Citrix SSO**
    - **Pro-App-VPN aktivieren: Ein**
    - **Anbietertyp: Paketttunnel**
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.

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.
- **Alle Netzwerke einschließen:** Wählen Sie aus, ob alle Netzwerke diese Verbindung verwenden dürfen. Die Standardeinstellung ist **Aus**.
- **Lokale Netzwerke ausschließen:** Wählen Sie aus, ob lokale Netzwerke von der Verwendung der Verbindung ausgeschlossen werden sollen. Die Standardeinstellung ist **Aus**.

- **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. Dieses Feld ist erforderlich.
- **Remote-ID:** Geben Sie den FQDN oder die IP-Adresse des VPN-Servers ein. Dieses Feld 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. 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.
- **Fallback aktivieren:** Wenn diese Einstellung aktiviert wird, kann Wi-Fi Assist-fähiger Datenverkehr, der ein VPN erfordert, durch einen Mobilfunktunnel übertragen werden. Die Standardeinstellung ist **Aus**.
- **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. Damit 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 Standardroute 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. Der Standardwert ist **SHA-256**.
  - **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.

- **Pro-App-VPN:** Konfigurieren Sie diese Einstellungen für IKEv2-Verbindungstypen.
  - **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 im Apple-Store 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.
  - **user agent:** Ordnet dieser Geräterichtlinie alle NetScaler 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-secure-client/id1135064690 hoch, fügen Sie die App zu Citrix Endpoint Management 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.
- **Alle Netzwerke einschließen:** Wählen Sie aus, ob alle Netzwerke diese Verbindung verwenden dürfen. Die Standardeinstellung ist **Aus**.
- **Lokale Netzwerke ausschließen:** Wählen Sie aus, ob lokale Netzwerke von der Verwendung der Verbindung ausgeschlossen werden sollen. Die Standardeinstellung ist **Aus**.
- **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 dem **Parameternamen** 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:** Starten Sie bedingungslos eine VPN-Verbindung.
    - **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 jeden DNS-Server, der 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 die IP-Adresse des DNS-Servers ein. Dieser Server kann außerhalb der aktuellen Netzwerkkonfiguration des Geräts residieren. 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** unterhalb von **XML-Inhalt** angezeigt. Wenn sie nicht gültig ist, wird 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. Dieses Feld ist erforderlich.
      - **Port für den Proxyserver:** Geben Sie die Portnummer des Proxyservers ein. Dieses Feld 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. Dieses Feld ist erforderlich.

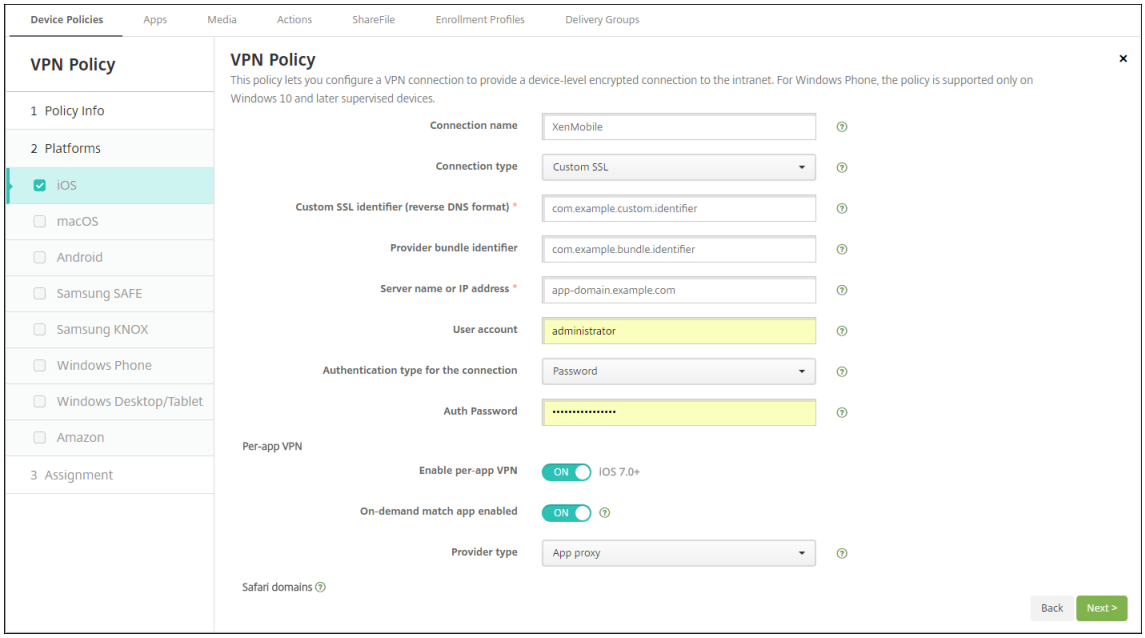
- **Richtlinieneinstellungen**
  - **Richtlinie entfernen:** Wählen Sie eine Methode, um das Entfernen von Richtlinien zu planen. Verfügbare Optionen sind **Datum auswählen** und **Zeit bis zum Entfernen (in Stunden)**
    - **Datum auswählen:** Klicken Sie auf den Kalender, um das Datum für das Entfernen 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.

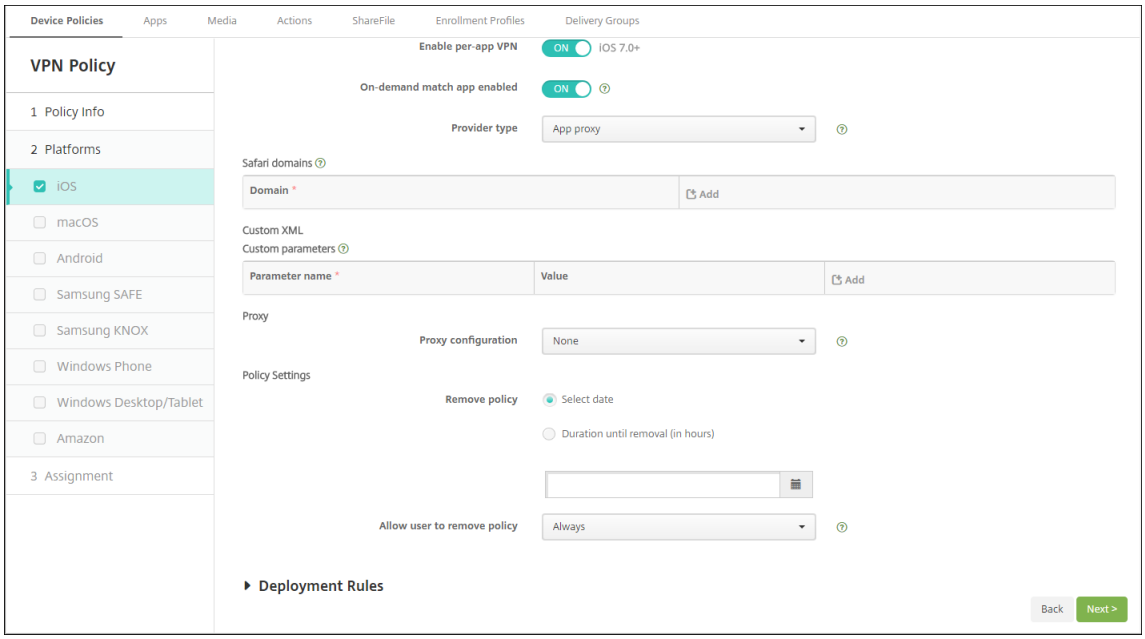
Pro-App-VPN-Zugriff konfigurieren

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.

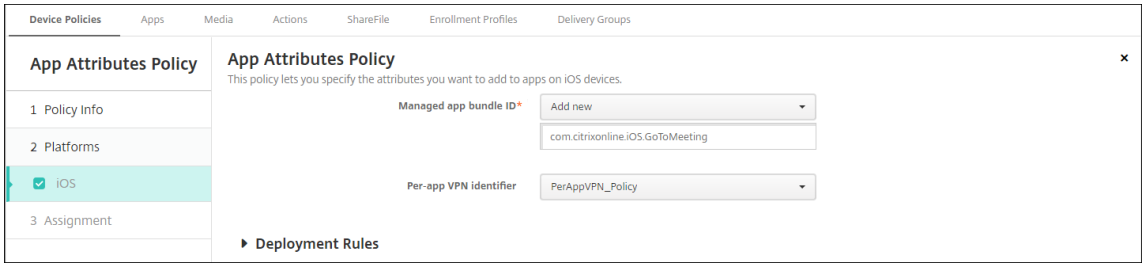
Pro-App-VPN-Zugriff konfigurieren:

1. Erstellen Sie unter **Konfigurieren > Geräterichtlinien** eine VPN-Richtlinie. Beispiel:

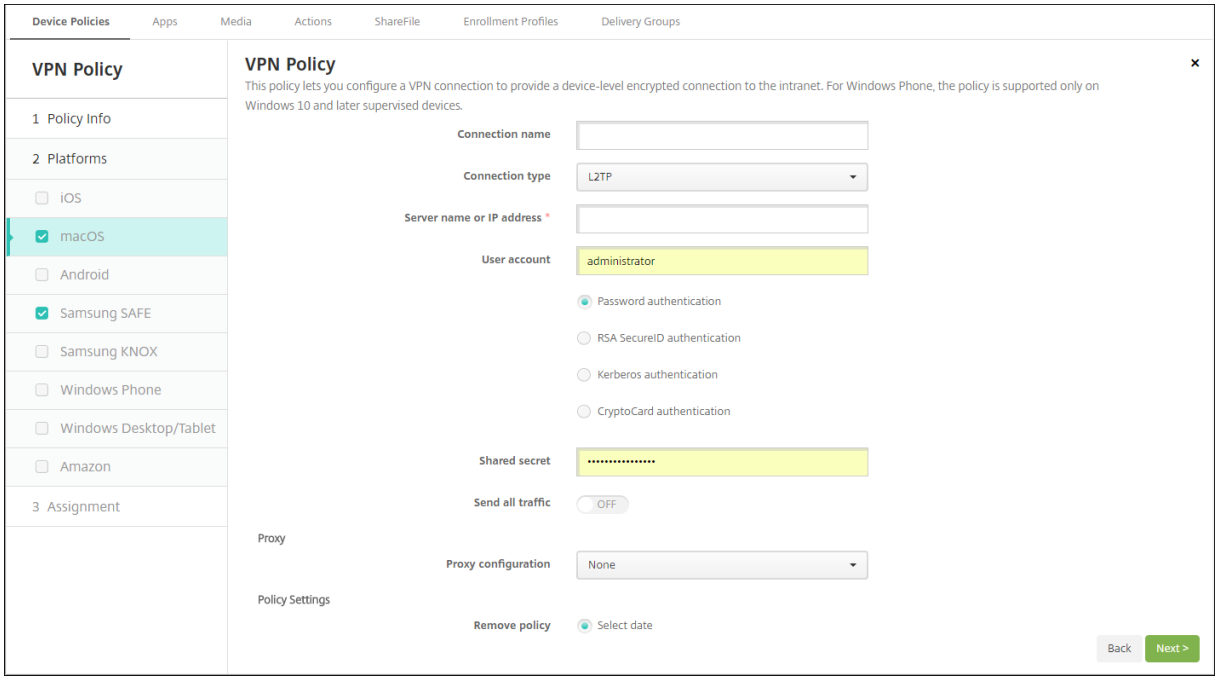




2. Erstellen Sie unter **Konfigurieren > Geräterichtlinien** eine Geräterichtlinie für App-Attribute, um der Pro-VNP-Richtlinie eine App zuzuordnen. Wählen Sie für **ID für VPN-Zugriff pro App** den Namen der in Schritt 1 erstellten VPN-Richtlinie. Wählen Sie für **Paket-ID für verwaltete App** eine Option aus der App-Liste oder geben Sie die Paket-ID ein. (Wenn Sie eine iOS-App-Bestandsrichtlinie bereitstellen, enthält die Liste Apps.)



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 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 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 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 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 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 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 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 benutzerdefinierten SSL-Protokolls für macOS

- **Benutzerdefinierte SSL-ID (Reverse DNS-Format):** Geben Sie den SSL-Bezeichner im Reverse DNS-Format ein. Dieses Feld ist erforderlich.
- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein. Dieses Feld 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 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.
- **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 die Domänen, die bei der Suche anhand der Domänenliste von Geräten als Treffer in Betracht gezogen werden sollen, 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 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 jeden DNS-Server, der 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 die IP-Adresse des DNS-Servers ein, den Sie hinzufügen möchten. Dieser Server kann außerhalb der aktuellen Netzwerkkonfiguration des Geräts residieren. 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** unterhalb von **XML-Inhalt** angezeigt. Wenn sie nicht gültig ist, wird 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**.

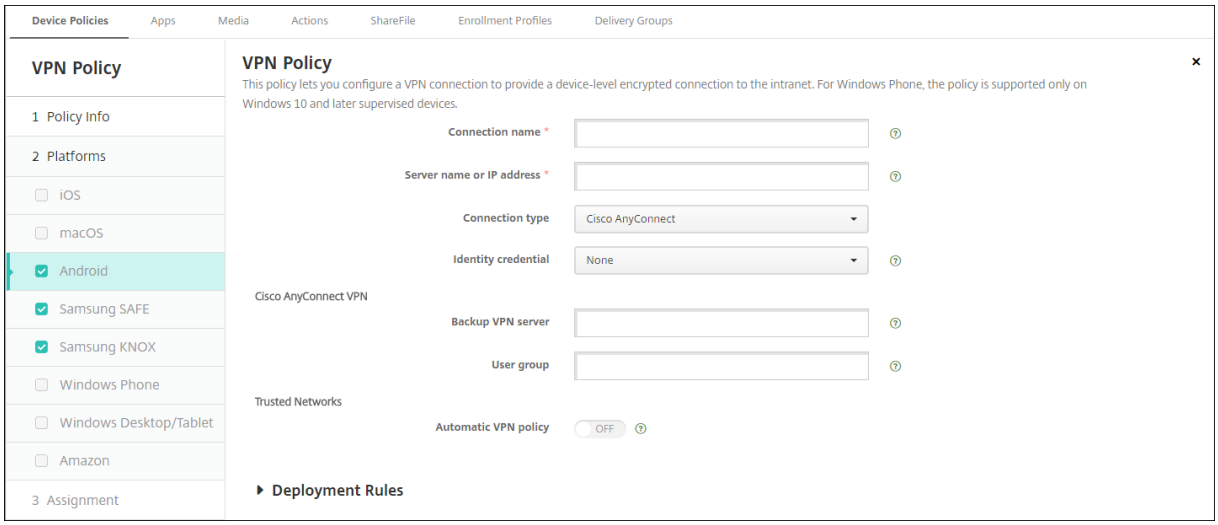
  * Bei Auswahl von **Manuell** konfigurieren Sie die folgenden Einstellungen:
    · **Hostname oder IP-Adresse des Proxyservers:** Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein. Dieses Feld ist erforderlich.
    · **Port für den Proxyserver:** Geben Sie die Portnummer des Proxyservers ein. Dieses Feld 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. Dieses Feld ist erforderlich.

- **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.

Einstellungen für Android (Legacy-Geräteadministrator)



Konfigurieren des Cisco AnyConnect VPN-Protokolls für Android

- **Verbindungsname:** Geben Sie einen Namen für die Cisco AnyConnect VPN-Verbindung ein. Dieses Feld ist erforderlich.
- **Servername oder IP-Adresse:** Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein. Dieses Feld 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. Dieses Feld ist erforderlich.

- **Servername oder IP-Adresse:** Geben Sie den FQDN oder die IP-Adresse des NetScaler 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 Apps, die auf der Positivliste stehen, 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.
  - **Anwendungsliste:** Die Apps auf einer Positivliste oder Sperrliste. 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. Citrix Endpoint Management unterstützt folgende Parameter für Citrix VPN:
  - **DisableUserProfiles:** Optional. Geben Sie zum Aktivieren des Parameters für **Wert Yes** ein. Ist die Option aktiviert, werden von Citrix Endpoint Management 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.
  - **IsAlwaysOnVpn:** Optional. Diese Eigenschaft bestimmt, ob das VPN-Profil ein Always-ON-VPN-Profil ist oder nicht. Auf **Ja** gesetzt, um anzugeben, dass das VPN-Profil ein Always-On-VPN-Profil ist. Die Standardeinstellung ist **Nein**. Nur bei einem VPN-Profil kann diese Eigenschaft auf **Ja** gesetzt werden, damit Always On VPN zuverlässig funktioniert.

Konfigurieren von VPNs zur Unterstützung von NAC

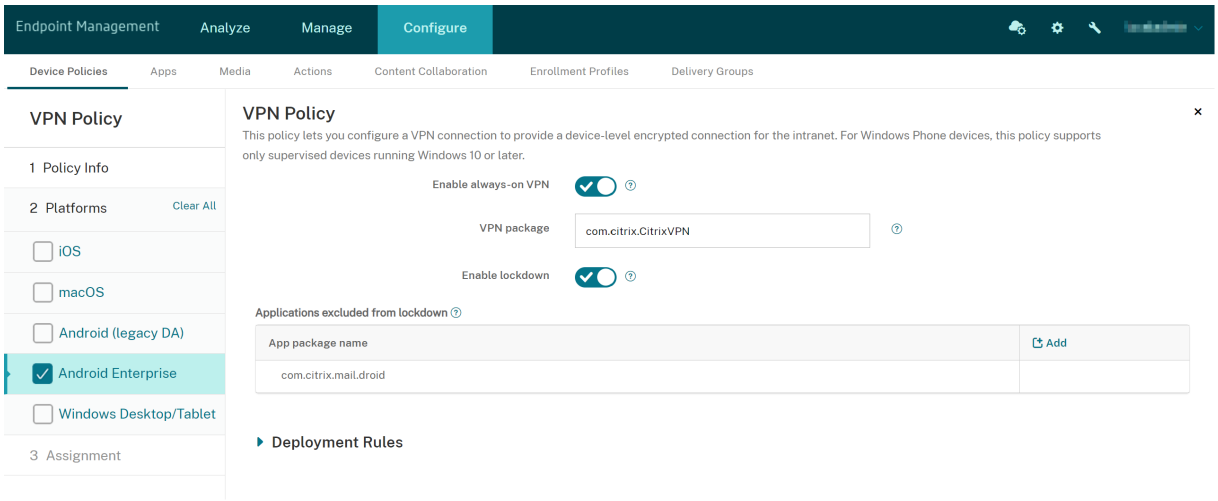
1. Verwenden Sie für die Konfiguration des NAC-Filters als **Verbindungstyp** die Option **Benutzerdefiniertes SSL**.
2. Geben Sie für **Verbindungsname** die Option **VPN** an.
3. Klicken Sie unter **Benutzerdefiniertes XML** auf **Hinzufügen** und führen Sie folgende Schritte aus:

    - **Parametername:** Geben Sie **XenMobileDeviceId** ein. Dies ist die Geräte-ID, die für die Netzwerkzugriffsprüfung basierend auf der Geräteregistrierung in Citrix Endpoint Management verwendet wird. Wenn das Gerät von Citrix Endpoint Management 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.

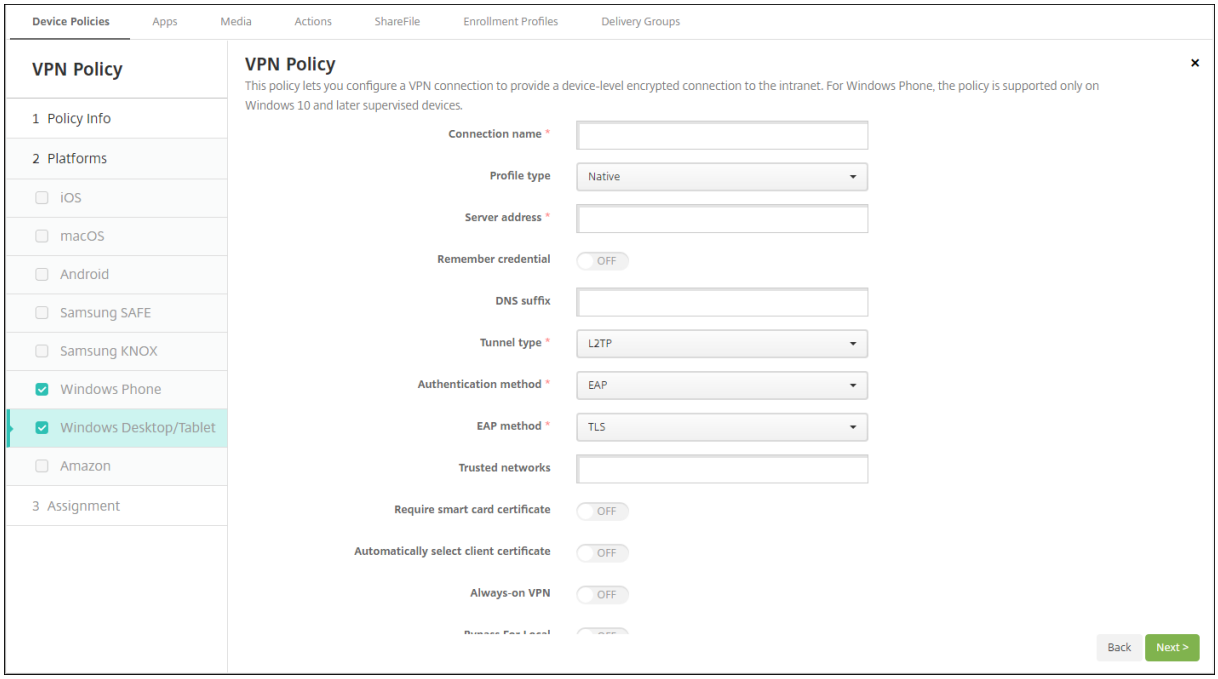
Android Enterprise-Einstellungen



- **Always-On-VPN aktivieren:** Wählen Sie aus, ob das Always-On-VPN aktiviert werden soll. Die Standardeinstellung ist **Aus**. Wenn diese Option aktiviert ist, bleibt die VPN-Verbindung bestehen, bis der Benutzer sie manuell trennt.

- **VPN-Paket:** Geben Sie den Paketnamen der VPN-App ein, die von den Geräten verwendet wird.
- **Sperrung aktivieren:** Wenn diese Option deaktiviert ist, kann keine App ohne VPN-Verbindung auf das Netzwerk zugreifen. Wenn die Option aktiviert ist, können die Apps, die Sie in der folgenden Einstellung konfigurieren, auf das Netzwerk zugreifen, selbst wenn keine VPN-Verbindung besteht. Verfügbar für Geräte mit Android 10 und höher.
- **Von der Sperrung ausgeschlossene Anwendungen:** Klicken Sie auf **Hinzufügen**, um die Paketnamen der Apps einzugeben, die die Sperrung umgehen sollen.

Windows Desktop/Tablet-Einstellungen



- **Verbindungsname:** Geben Sie einen Namen für die Verbindung ein. Dieses Feld 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. Dieses Feld 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:** Verwenden Sie das Challenge Handshake Authentication-Protokoll 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.

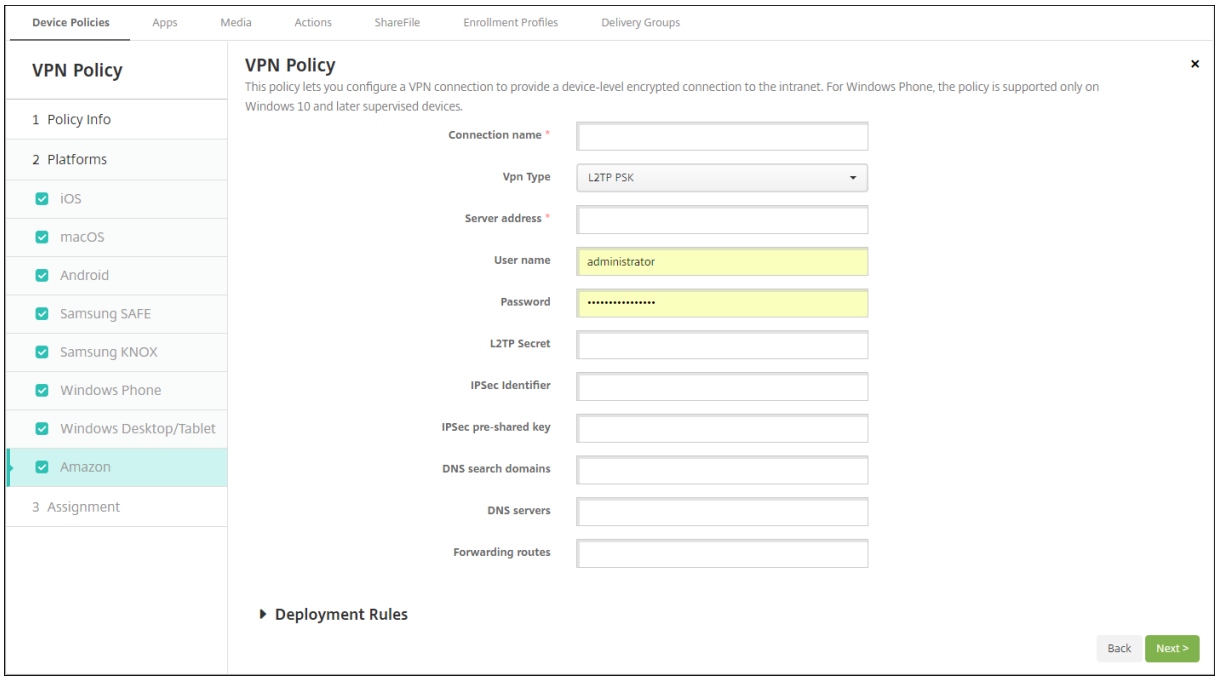
- **Konfigurieren des Plug-In-Profils:** Die nachfolgenden Einstellungen gelten für VPN-Plug-Ins aus dem Windows-Store, die auf Geräten installiert sind.

  - **Serveradresse:** Geben Sie den FQDN oder die IP-Adresse des VPN-Servers ein. Dieses Feld 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 9, 2021

Die Hintergrundbild-Geräterichtlinie ermöglicht das Hinzufügen einer PNG- oder JPG-Datei, um Hintergrundbilder auf dem Sperr- und Homebildschirm oder auf beiden festzulegen. Diese Richtlinie ist nur für betreute Geräte verfügbar. Zum Verwenden verschiedener Bilder auf iPads und iPhones müssen Sie unterschiedliche Richtlinien erstellen und den entsprechenden Benutzern bereitstellen.

In der folgenden Tabelle werden die von Apple empfohlenen Bildgrößen für iOS-Geräte aufgeführt.

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

June 25, 2024

Sie können Webinhalte auf iOS-Geräten filtern, indem Sie die automatische Filterfunktion von Apple verwenden, für die Sie bestimmte Websites zu Positivlisten oder Sperrlisten hinzufügen. Die Geräterichtlinie für Webinhalte gilt nur für iOS-Geräte im betreuten Modus. Informationen, wie Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Bereitstellen von Geräten mit Apple Configurator 2.

> **Hinweis:**
>
> - Android-Geräte unterstützen keine Webinhaltsfilter.
> - Ab iOS-Version 16.5 und höher erkennt die Geräterichtlinie für den Web Content Filter `https://localhost` in der Positivliste nicht mehr. Dies führt dazu, dass einige Apps nicht mehr reagieren. Auch das Hinzufügen einer Ableitung der URL wie `http://localhost:`, `http://localhost:*` usw. zur Positivliste löst das Problem nicht.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren** > **Geräterichtlinien**. Weitere Informationen finden Sie unter Gerätерichtlinien.

iOS-Einstellungen

- **Filtertyp:** Klicken Sie in der Dropdownliste 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 `https://` bzw. `https://` beginnen.
    * Klicken Sie auf **Speichern**, um die Website der Positivliste hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
  - **Blockierte 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 `https://` bzw. `https://` beginnen.
    * Klicken Sie auf **Speichern**, um die Website der Sperrliste hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Positivliste für Lesezeichen erstellen**
  - **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 Citrix Secure Hub-Store zu ermöglichen, fügen Sie die URL von Citrix Endpoint Management der Liste **URL** hinzu. Die URL muss mit `https://` bzw. `https://` beginnen. Dieses Feld 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 Dropdownliste 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

June 25, 2024

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**. Diese Option wird für geteilte iPads nicht unterstützt.
- **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. Durch diese Einstellung können Sie auch festlegen, dass ein iPad nur eine einzige Website öffnet. Zum Einrichten von iPads für die Ausführung im Kioskmodus können Sie alternativ auch die Geräterichtlinie zum Sperren von Apps verwenden. Weitere Informationen finden Sie unter Konfigurieren eines iPads als Kiosk. 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.
    - **Gültigkeitsbereich für Profil:** Wählen Sie aus, ob die Richtlinie für einen Benutzer oder ein ganzes System gilt. Der Standardwert ist **System**. Nur für Geräte ab iOS 9.3 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.
- **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.

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.

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.

Windows Agent-Geräterichtlinie

June 25, 2024

Über die Windows Agent-Geräterichtlinie können Sie PowerShell-Skripts auf verwalteten Windows-Desktops und -Tablets ausführen. Sie können auf Skriptdateien verweisen, die in Citrix Endpoint Management als Unternehmensapp und auf andere Server, die Skripts hosten, hochgeladen wurden. Informationen zum Hinzufügen von Unternehmensapps finden Sie unter Apps hinzufügen.

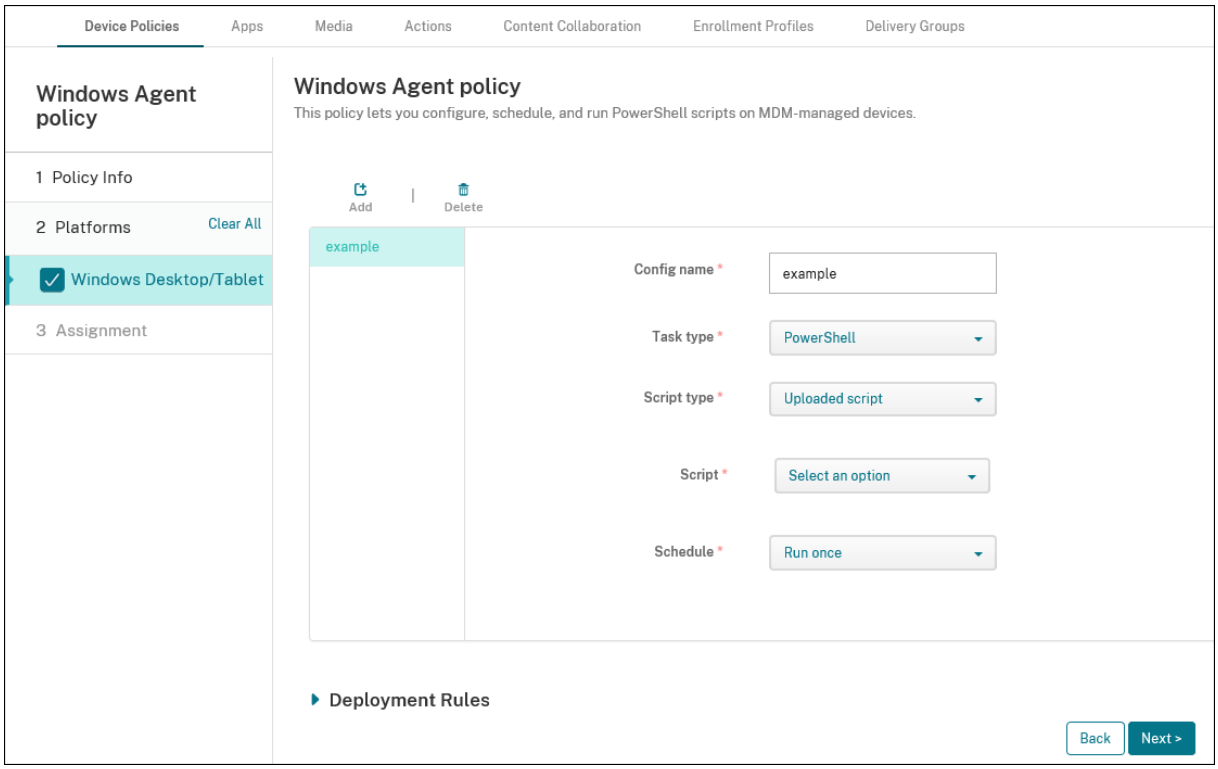
Alle Skripte werden unter dem privilegierten Status ausgeführt. Sie müssen Skripte nicht als Administrator ausführen.

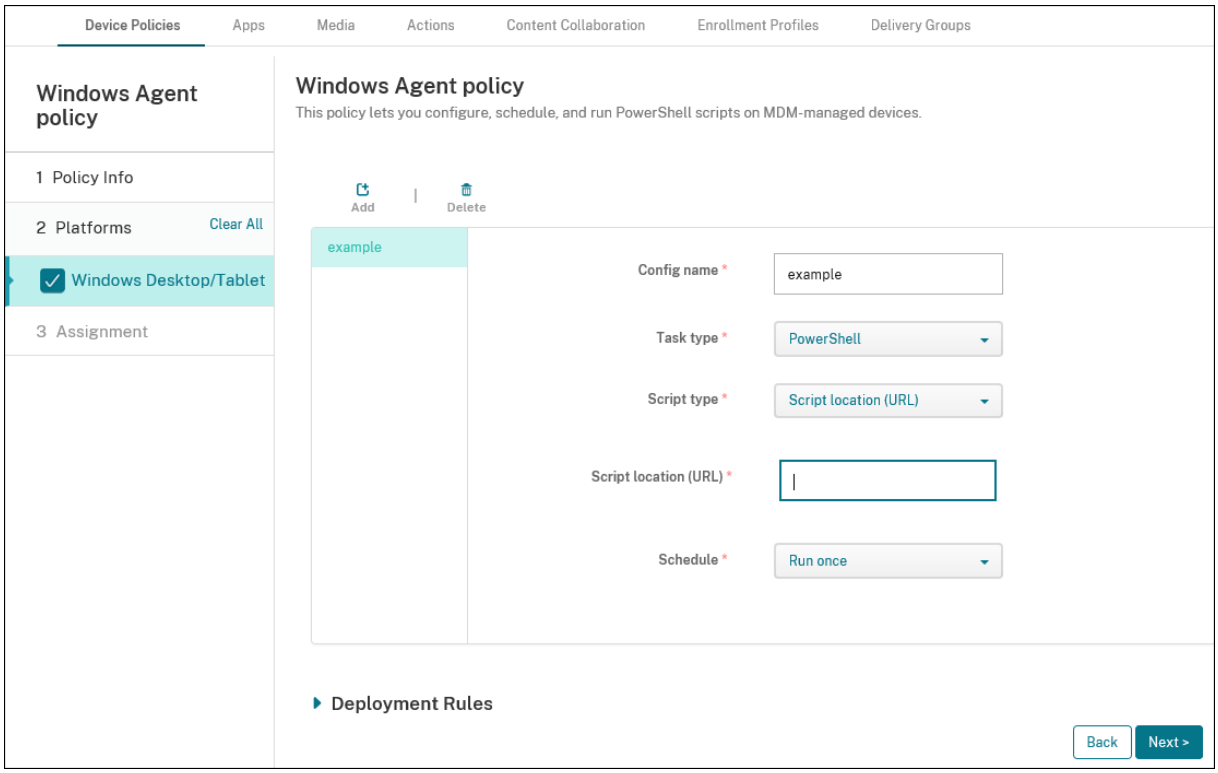
Sie können dann eine automatisierte Aktion basierend auf den von einem Skript zurückgegebenen Werten konfigurieren. Beispielsweise können Sie ein Skript ausführen, das einen Registrierungsschlüssel überwacht und ein Ergebnis zurückgibt. Basierend auf dem zurückgegebenen Ergebnis wird eine automatisierte Aktion ausgeführt. Diese Aktion gewährt oder verweigert den Zugriff auf eine App, markiert das Gerät als nicht richtlinientreu oder hat andere Auswirkungen.

Sie können diese Richtlinie auch zum Bereitstellen benutzerdefinierter MSI-Installationsprogramme verwenden, indem Sie ein PowerShell-Skript konfigurieren, das auf eine MSI-Datei und eine MST-Datei verweist.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows Desktop-/Tablet-Einstellungen





- **Konfigurationsname:** Geben Sie einen aussagekräftigen Namen für die Konfiguration ein.

- **Aufgabentyp:** Wählen Sie **PowerShell**.
- **Skripttyp:** Wählen Sie **Hochgeladenes Skript** für Skripts, die Sie in Citrix Endpoint Management hochgeladen haben, oder wählen Sie **Skriptspeicherort (URL)** für Skripts, die extern gehostet werden. Weitere Informationen zum Hochladen eines Skripts in Citrix Endpoint Management finden Sie unter Hinzufügen von Win32-Apps als Unternehmensapps.
  - **Skript auswählen:** Für **Hochgeladenes Skript** wählen Sie das auszuführende Skript aus.
  - **Skriptspeicherort (URL):** Für **Skriptspeicherort (URL)** geben Sie den Speicherort des auszuführenden Skripts ein. Diese URL muss das Skript als Nutzlast bereitstellen. Citrix Endpoint Management unterstützt keine URLs, die Scripts als JavaScript-Download bereitstellen. Das Skript muss auch öffentlich verfügbar sein.
- **Zeitplan:** Wählen Sie **Einmal ausführen**, um das ausgewählte Skript einmal auszuführen, oder **Regelmäßig ausführen**, um das Skript regelmäßig auszuführen.
  - **Alle X Stunden ausführen:** Geben Sie die Anzahl der Stunden zwischen zwei Skriptläufen ein.

Um den Status eines Skripts zu überprüfen, gehen Sie in der Konsole zu **Verwalten > Geräte**. Wählen Sie das Gerät aus, auf dem Sie den Skriptstatus prüfen möchten, und klicken Sie auf **Bearbeiten**. Unter **Eigenschaften** können Sie den Status Ihrer Skripts überprüfen, indem Sie unter **Windows Agent** auf **Download** klicken.

Bereitstellen eines PowerShell-Skripts zum Auslösen einer automatisierten Aktion

1. Erstellen Sie ein PowerShell-Skript zum Überwachen eines Registrierungsschlüssels. Das folgende PowerShell-Skript überprüft, ob die Firewall aktiviert ist.

```
$body = @{
  }

$firewallEnabled = Get-ItemPropertyValue HKLM:\SYSTEM\
   CurrentControlSet\Services\SharedAccess\Parameters\
   FirewallPolicy\StandardProfile -Name EnableFirewall
if($firewallEnabled -eq 1){

$body["firewallEnabled"]="true"
 }
  else {

$body["firewallEnabled"]="false"
 }

$body | ConvertTo-Json -Depth 10
<!--NeedCopy-->
```


Das Skript gibt einen der folgenden Werte zurück:

```
{

    "firewallEnabled":  "true"
 }

<!--NeedCopy-->
```

Oder

```
{

    "firewallEnabled":  "false"
 }

<!--NeedCopy-->
```

2. Laden Sie das Skript als Unternehmensapp in die Citrix Endpoint Management- Konsole hoch oder hosten Sie es an einer zugänglichen URL.
3. Konfigurieren Sie die Windows Agent-Geräterichtlinie, die im vorliegenden Artikel beschrieben ist. Stellen Sie sicher, dass das Skript zur sofortigen Ausführung konfiguriert ist.
4. Prüfen Sie nach Ausführung des Skripts den Skriptstatus.
   a) Gehen Sie in der Konsole zu **Verwalten > Geräte**.
   b) Wählen Sie das Gerät zum Prüfen des Skriptstatus und klicken Sie auf **Bearbeiten**.
   c) Klicken Sie unter der Überschrift **Windows Agent** auf **Herunterladen**.
5. Konfigurieren Sie eine automatisierte Aktion basierend auf dem empfangenen Status. Weitere Informationen zum Konfigurieren automatisierter Aktionen finden Sie unter Erstellen einer automatisierten Aktion basierend auf einem Ergebnis der Windows Agent-Geräterichtlinie. In diesem Abschnitt werden die für das Beispielskript und die Windows Agent-Geräterichtlinie erstellten automatisierten Aktionen aufgeführt.

Geräterichtlinie “Windows-GPO-Konfiguration”

December 1, 2023

Die Geräterichtlinie “Windows-GPO-Konfiguration”ermöglicht Folgendes:

- Nutzen Sie die Citrix Endpoint Management-Konsole, um Gruppenrichtlinienobjekte (GPOs) zu importieren und auf Windows 10- und Windows 11-Geräten bereitzustellen.
- Konfigurieren Sie Gruppenrichtlinienobjekte für alle Windows-Geräte, die von Citrix Workspace Environment Management unterstützt werden.

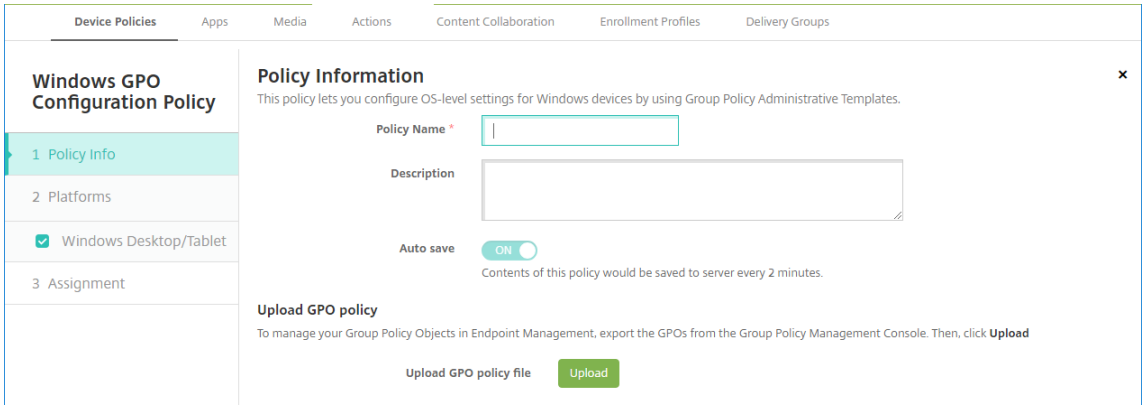
- Konfigurieren Sie Gruppenrichtlinienobjekte auf Geräte- und Benutzerebene.

Importieren von Gruppenrichtlinienobjekten für die Bereitstellung auf Windows 10- und Windows 11-Geräten

Anstatt Gruppenrichtlinienobjekte von einen AD-Administrator per Gruppenrichtlinien-Verwaltungskonsole verwalten zu lassen, können Sie GPOs auch über die Citrix Endpoint Management-Konsole importieren und bereitstellen.

Erstellen eines Backups Ihrer Gruppenrichtlinienobjekte in Citrix Endpoint Management:

1. Bitten Sie Ihren AD-Administrator, die Gruppenrichtlinienobjekte aus der Gruppenrichtlinien-Verwaltungskonsole zu exportieren und Ihnen die Dateien bereitzustellen.
2. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Geräterichtlinien** und erstellen Sie die Richtlinie **Windows-GPO-Konfiguration**.
3. Klicken Sie auf **Upload**, suchen Sie die Datei und klicken Sie auf **Öffnen**, um die Datei zu importieren.



   Informationen zum Konfigurieren von Gruppenrichtlinienobjekten finden Sie im Artikel Windows-Desktop-/Tablet-Einstellungen.

Konfigurieren von Gruppenrichtlinienobjekten für die Bereitstellung in Citrix Workspace Environment Management

Mit der Geräterichtlinie für die Windows-GPO-Konfiguration können Sie Gruppenrichtlinienobjekte (GPOs) für alle Windows-Geräte konfigurieren, die von Citrix Workspace Environment Management (WEM) unterstützt werden. Citrix Endpoint Management überträgt die Richtlinien an den Citrix WEM-Dienst. Der WEM-Dienst wendet dann über den WEM-Agent auf den Geräten die Gruppenrichtlinienobjekte auf Geräte und ihre Apps an.

Informationen zum Installieren des Workspace Environment Management-Agents finden Sie unter Installation und Konfiguration.

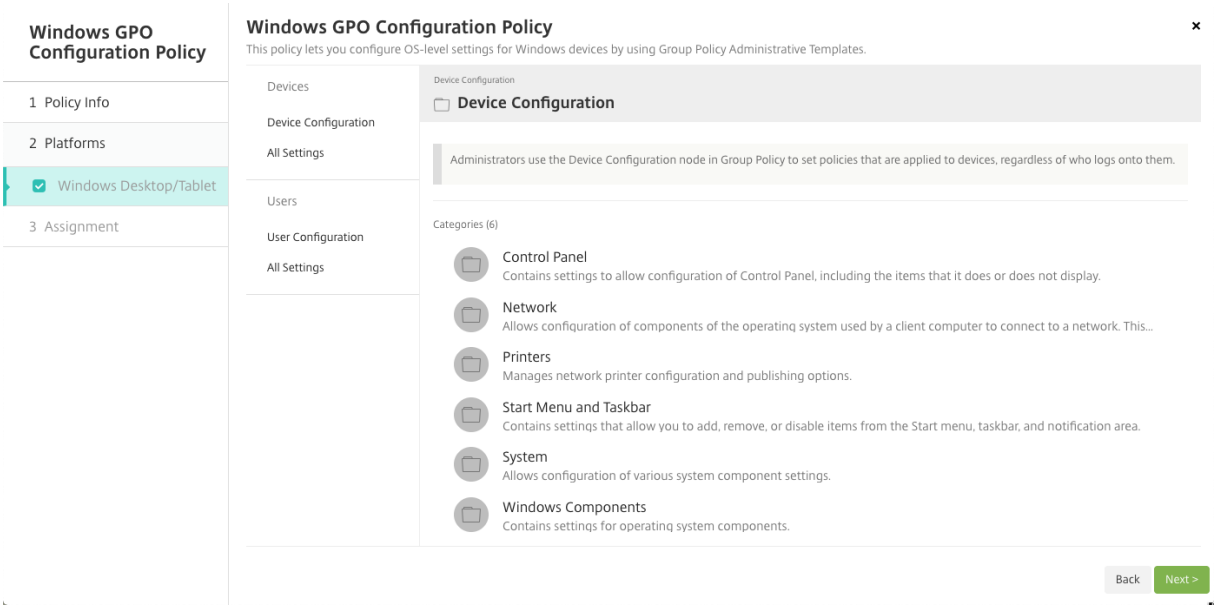
Diese Richtlinie verwendet nur ADMX-Dateien von Windows. Wenn Sie die ADMX-Datei eines Drittanbieters hochladen möchten, verwenden Sie die App-Konfigurationsrichtlinie. Weitere Informationen zum Hochladen von ADMX-Dateien von Drittanbietern finden Sie unter App-Konfigurationsrichtlinie.

- Sie können GPO-Konfigurationen auf jedes von WEM unterstützte Gerät übertragen, selbst wenn Citrix Endpoint Management das Gerät nicht nativ unterstützt. Eine Liste der unterstützten Geräte finden Sie unter Betriebssystemanforderungen.
- Für diese Richtlinie muss auf dem Gerät ein WEM-Agent installiert und konfiguriert sein. Ein MDM- oder MAM-Registrierung der Geräte ist nicht erforderlich.
- Citrix Endpoint Management überträgt die GPO-Einstellungen über den WEM-Kanal. (Das Übertragen von Einstellungen auf Geräteebene über den MDM-Kanal wird von Microsoft nicht unterstützt.) Geräte, die die Geräterichtlinie zur Windows-GPO-Konfiguration empfangen, werden im Citrix Endpoint Management-Modus WEM ausgeführt. Unter **Verwalten > Geräte** wird in der Liste registrierter Geräte in der Spalte **Modus** für WEM-verwaltete Geräte **WEM** angezeigt.

Zum Hinzufügen oder Konfigurieren dieser Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Weitere Informationen finden Sie unter Geräterichtlinien.

Windows-Desktop-/Tablet-Einstellungen

Mit dieser Richtlinie können Sie Gruppenrichtlinienobjekte auf Geräte- und Benutzerebene konfigurieren.



Wählen und konfigurieren Sie das Windows-Gruppenrichtlinienobjekt für die Bereitstellung auf Ihren Windows-Geräten. Sie können die **Gerätekonfiguration** und die **Benutzerkonfiguration** ändern. Richtlinien werden in einer Baumstruktur aufgelistet. Klicken Sie auf **Alle Einstellungen**, um jede Einstellung anzuzeigen. Informationen zu den Einstellungen finden Sie im GPO-Referenzblatt, das bei Microsoft zum Download bereitsteht.

Zum Konfigurieren einer Einstellung müssen Sie sie zunächst aktivieren. Während der Konfiguration speichert Citrix Endpoint Management die Änderungen automatisch, damit diese Einstellungen beibehalten werden. Wenn Sie die Seite vor dem Speichern einer Einstellung verlassen, wird in einer Meldung angezeigt, dass nicht gespeicherte Änderungen vorliegen.

Wenn eine Einstellung zwei Optionen hat, werden zwei Optionsfelder angezeigt. Bei mehr als zwei Optionen wird ein Menü angezeigt.

> **Hinweis:**
>
> Um zu überprüfen, welche Einstellungen Sie konfiguriert haben, führen Sie folgende Schritte aus.
>
> 1. Öffnen Sie in der Citrix Endpoint Management-Konsole unter **Windows-GPO-Konfiguration** die zu bearbeitende Richtlinie.
> 2. Wählen Sie unter **Geräte** oder **Benutzer** die Option **Alle Einstellungen** aus.
> 3. Sortieren Sie die Tabelle nach **Status** (in aufsteigender Reihenfolge). Alle nicht konfigurierten Richtlinien haben den Status **Nicht konfiguriert**. Die von Ihnen konfigurierten Richtlinien werden oben aufgeführt.

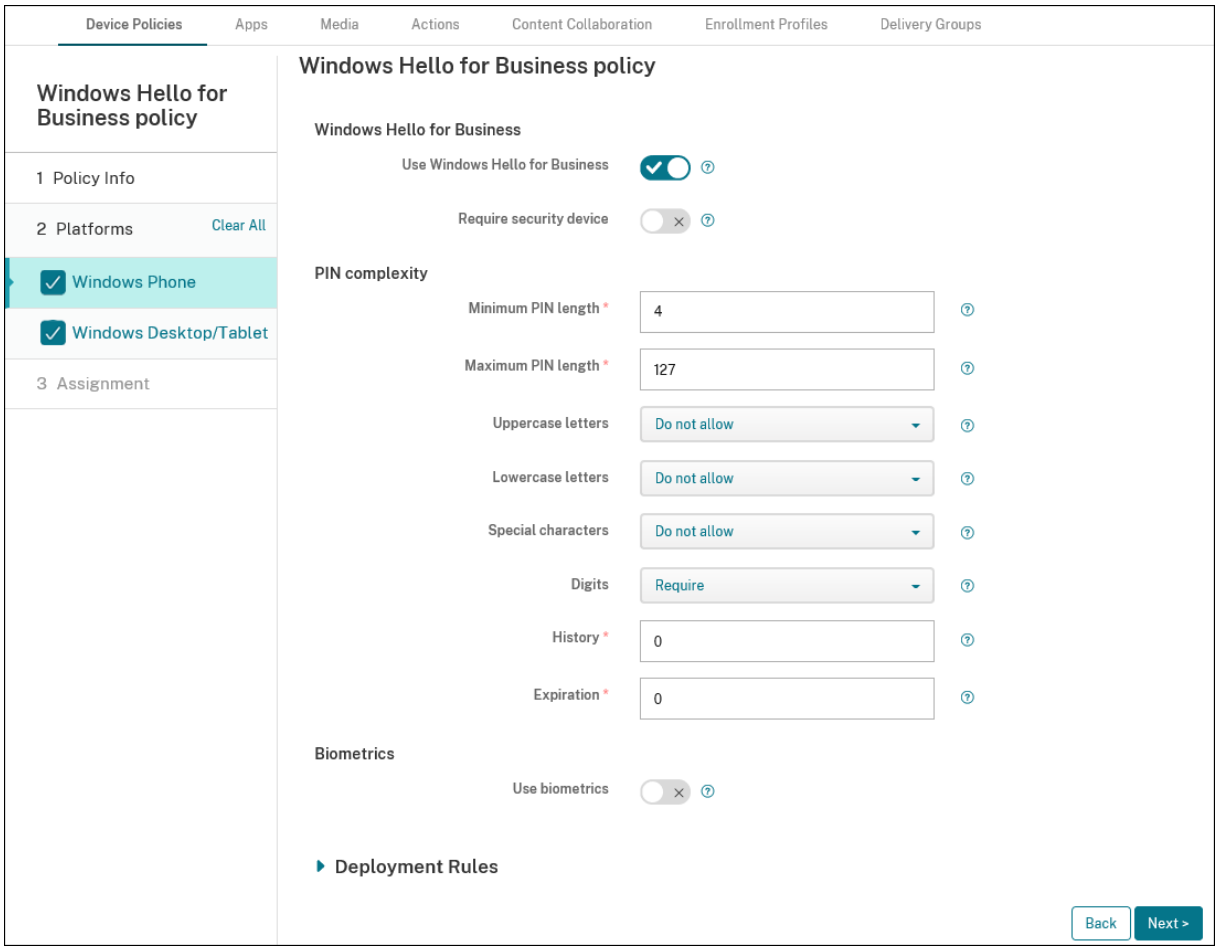
Geräterichtlinie für Windows Hello for Business

June 25, 2024

Mit Windows Hello for Business können sich Benutzer mit ihrem Active Directory- oder Azure Active Directory-Kontos an Windows-Geräten anmelden. Sie verwenden die Geräterichtlinie **Windows Hello for Business**, um die Funktion zu aktivieren, damit Benutzer Windows Hello for Business auf ihrem Gerät bereitstellen können. Mit dieser Richtlinie können Sie auch Passcodebeschränkungen und andere Sicherheitsfunktionen konfigurieren.

Zum Hinzufügen der **Windows Hello for Business**-Richtlinie gehen Sie zu **Konfigurieren > Geräterichtlinien**. Konfigurieren Sie folgende Einstellungen:

Windows Desktop/Tablet-Einstellungen



- **Windows Hello for Business verwenden:** Aktivieren Sie das Feature, damit Benutzer Windows Hello for Business auf ihrem Gerät bereitstellen können.
- **Sicherheitsgerät erforderlich:** Benutzer brauchen ein Trusted Platform Module (TPM), um sich anzumelden.
- **Minimale/Maximale PIN-Länge:** Minimale und maximale Länge für Benutzer-PINs. **PIN-Mindestlänge** ist standardmäßig **4**. **Maximale PIN-Länge** ist standardmäßig **127**.
- **Großbuchstaben**, **Kleinbuchstaben**, **Sonderzeichen**: Wählen Sie für jeden Zeichentyp **Zulassen**, **Erforderlich** oder **Nicht zulassen**. Standardwert ist **Nicht zulassen**.
- **Ziffern:** Wählen Sie **Zulassen**, **Erforderlich** oder **Nicht zulassen**. Standardwert ist **Erforderlich**.
- **Verlauf:** Die Anzahl der früheren PINs, die Benutzer nicht wiederverwenden können. Der Standardwert ist **0**. Dies bedeutet, dass Benutzer alle PINs wiederverwenden können.
- **Ablauf:** Die Anzahl der Tage, bevor ein Benutzer die PIN ändern muss. Der Standardwert ist **0**, was bedeutet, dass PINs nicht ablaufen.
- **Biometrie verwenden:** Benutzeranmeldung mit Biometrie statt PINs zulassen.

Apps hinzufügen

June 25, 2024

Das Hinzufügen von Apps zu Citrix Endpoint Management bietet Funktionen für die Mobilanwendungsverwaltung (MAM). Citrix Endpoint Management unterstützt Sie bei der Anwendungsbereitstellung, Softwarelizenzierung, Konfiguration und Anwendungslebenszyklusverwaltung.

Einige App-Typen müssen zunächst MDX-fähig gemacht werden, bevor Apps an Benutzergeräte verteilt werden können. Eine Einführung in MDX finden Sie unter Citrix Endpoint Management-Komponenten 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 Auslaufende Features.
- 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 Citrix Endpoint Management-Konsole umfasst folgende Schritte:

- Konfigurieren von App-Einstellungen
- Einteilen von Apps in Kategorien, um sie in Citrix 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:

- Android Enterprise-Apps verteilen
- Apple-Apps verteilen

> **Wichtig:**
>
> Citrix Endpoint Management unterstützt das Hinzufügen und Verwalten von bis zu 300 Apps. Wenn Sie dieses Limit überschreiten, wird das System instabil.

App-Typen und Features

In der folgenden Tabelle sind alle App-Typen aufgeführt, die Sie mit Citrix Endpoint Management 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 Citrix Endpoint Management hinzu.	Eine MDX-App hinzufügen
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 Citrix Endpoint Management hinzu.	Apps aus einem öffentlichen App-Store hinzufügen
Web und SaaS	Ihr internes Netzwerk (Web-Apps) oder ein öffentliches Netzwerk (SaaS).	Citrix Endpoint Management 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 Citrix Endpoint Management-Servern.	Fügen Sie die Apps zu Citrix Endpoint Management hinzu.	Unternehmensapp hinzufügen
Weblink	Internet-Webadressen, Intranet-Webadressen oder Web-Apps, für die kein Single Sign-On erforderlich ist.	Konfigurieren Sie Weblinks in Citrix Endpoint Management.	Weblink hinzufügen

Berücksichtigen Sie bei der Planung der App-Verteilung die folgenden Features:

- Automatische Installationen
- Erforderliche und optionale Apps
- Info zu App-Kategorien
- Bereitstellen von Unternehmensapps über das Citrix CDN
- Aktivieren von Microsoft 365-Apps
- Workflows anwenden
- Branding für den App-Store und Citrix Secure Hub
- Citrix Virtual Apps and Desktops über den App-Store

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. Weitere Informationen 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-Lizenzzugangscodes 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 Citrix Secure Hub starten.

Für als erforderlich markierte Apps können Benutzer u. a. in folgenden Situationen Updates schnell erhalten:

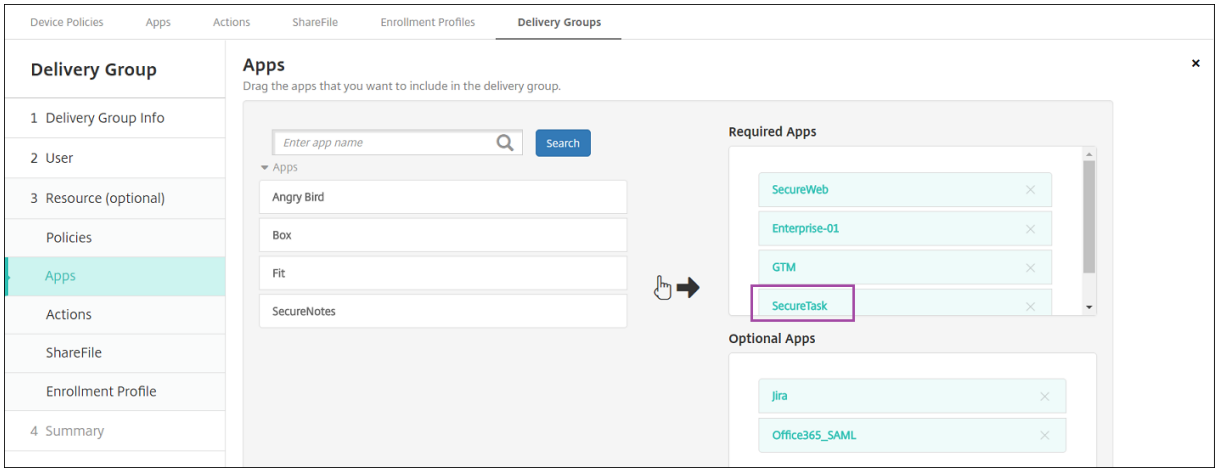
- Sie laden eine neue App hoch und legen sie als erforderlich fest.
- Sie legen eine vorhandene App als erforderlich fest.
- Ein Benutzer löscht eine erforderliche App.
- Es gibt ein Citrix Secure Hub-Update.

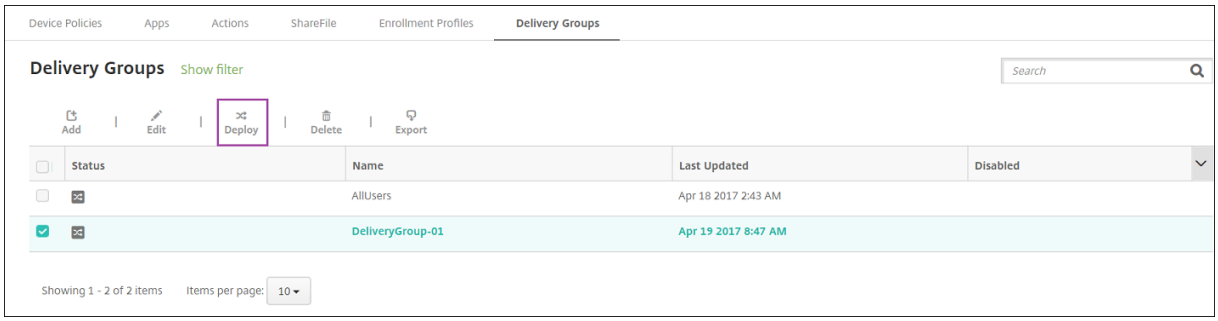
Voraussetzungen für die erzwungene Bereitstellung erforderlicher Apps

- Citrix Secure Hub 10.5.15 für iOS und 10.5.20 für Android (Mindestversionen)
- MAM-SDK oder MDX Toolkit 10.6 (Mindestversion)
- Nach dem Upgrade von Citrix Endpoint Management und Citrix Secure Hub müssen sich Benutzer mit registrierten Geräten abmelden und dann bei Citrix Secure Hub anmelden, um die erforderlichen App-Bereitstellungsupdates zu erhalten.

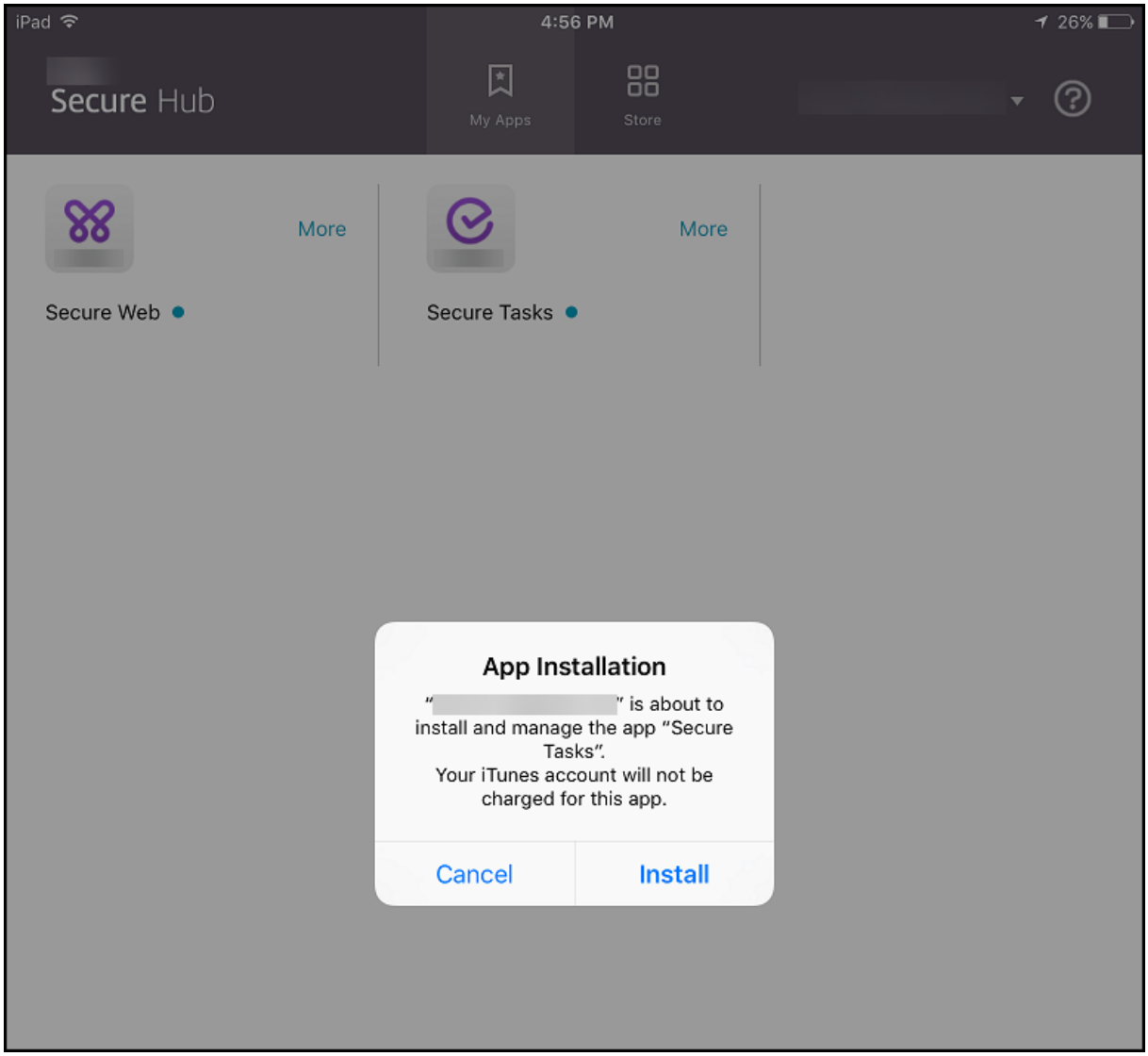
Beispiele

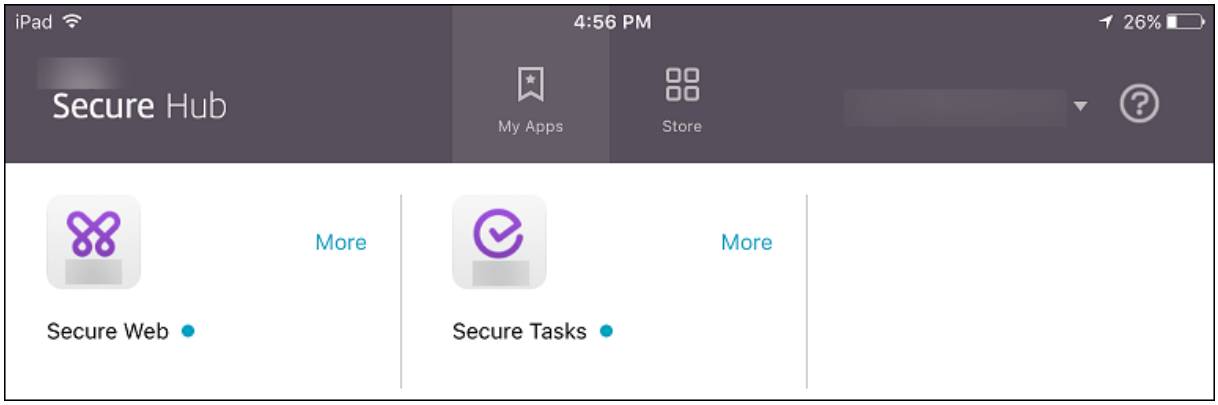
Das folgende Beispiel zeigt die Reihenfolge beim Hinzufügen der App "Secure Tasks"zu einer Bereitstellungsgruppe und dem Bereitstellen der Bereitstellungsgruppe.





Nach der Bereitstellung von Secure Tasks auf dem Gerät eines Benutzers wird dieser von Citrix 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 auch bei konfigurierter MDX-Richtlinie mit

> Kulanzzeitraum für App-Upgrades und wenn der Benutzer die App später aktualisieren möchte.

iOS-Workflow für erforderliche Unternehmensapps und Apps aus dem öffentlichen Store

1. Stellen Sie die mobile Produktivitätsapp bei der ersten Registrierung bereit. Die erforderliche App wird im Gerät installiert.
2. Aktualisieren Sie die App in der Citrix Endpoint Management-Konsole.
3. Verwenden Sie die Citrix Endpoint Management-Konsole, um erforderliche Apps bereitzustellen.
4. Die App auf dem Homebildschirm wird aktualisiert. Bei Apps aus dem öffentlichen Store wird das Upgrade automatisch gestartet. Benutzer erhalten 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 mobile Produktivitätsapp bei der ersten Registrierung bereit. Die erforderliche App wird im Gerät installiert.
2. Verwenden Sie die Citrix Endpoint Management-Konsole, um erforderliche Apps bereitzustellen.
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 mobile Produktivitätsapp bei der ersten Registrierung bereit. Die erforderliche App wird im Gerät installiert.
2. Aktualisieren Sie die App in der Citrix Endpoint Management-Konsole.
3. Verwenden Sie die Citrix Endpoint Management-Konsole, um erforderliche Apps bereitzustellen. Alternativ können Sie auch den Citrix 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

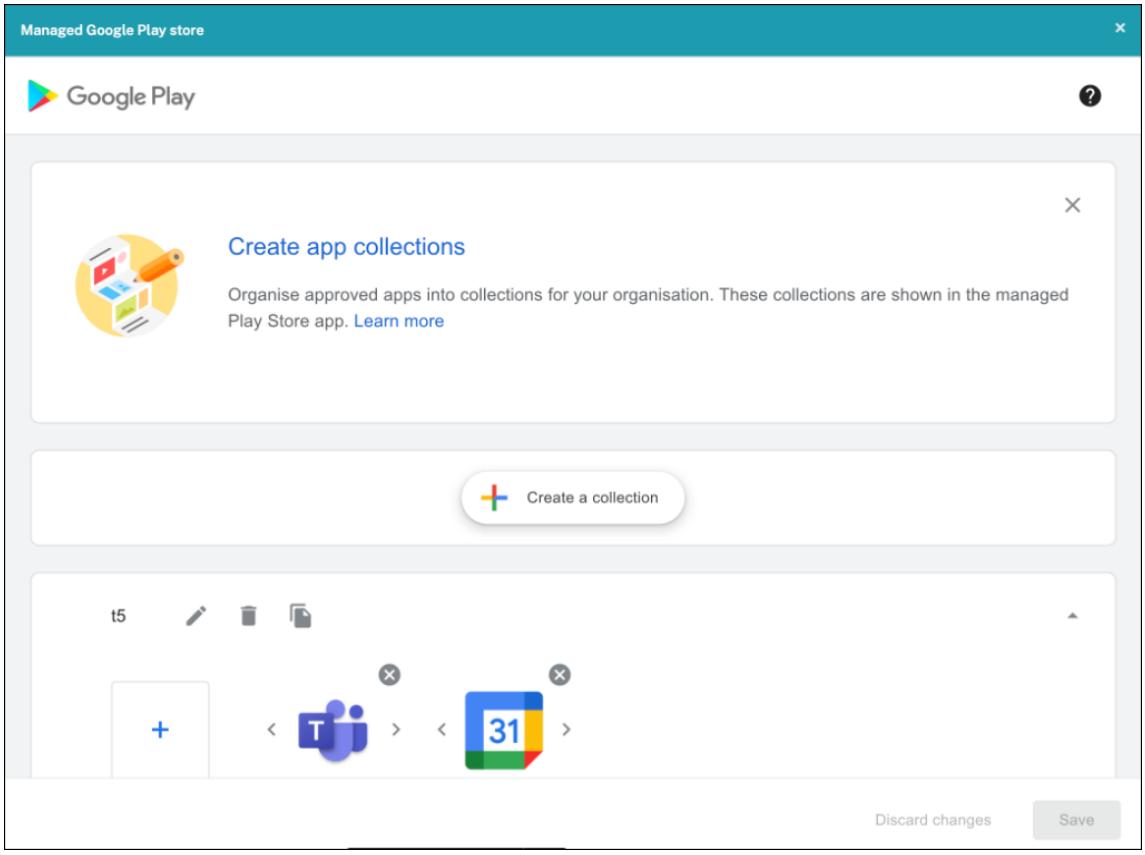
Sie können Benutzern gestatten, eine App zu deinstallieren, die als erforderlich konfiguriert ist. Gehen Sie zu **Konfigurieren> Bereitstellungsgruppen** und verschieben Sie die App aus **Erforderliche Apps** in **Optionale Apps**.

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.

Organisieren von Apps (Android Enterprise)

Wenn Benutzer sich bei Citrix Secure Hub anmelden, erhalten sie eine Liste der Apps, Weblinks und Stores, die Sie in Citrix Endpoint Management konfiguriert haben. In Android Enterprise können Sie diese Apps in Sammlungen organisieren, damit Benutzer nur auf bestimmte Apps, Stores oder Weblinks zugreifen können. Beispiel: Sie erstellen eine Sammlung “Finanzen”und fügen der Sammlung dann nur Apps hinzu, die für den Bereich Finanzen relevant sind. Ebenso können Sie eine Sammlung “Vertrieb”konfigurieren, der nur Apps für den Vertrieb zugewiesen werden.

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps > Apps anordnen**. Das Fenster **Verwalteter Google Play Store** wird angezeigt.



2. Klicken Sie auf **Sammlung erstellen** und wählen Sie die Apps aus, die dieser Sammlung hinzugefügt werden sollen.
3. Wenn Sie mit dem Hinzufügen von Sammlungen fertig sind, klicken Sie auf **Speichern**.

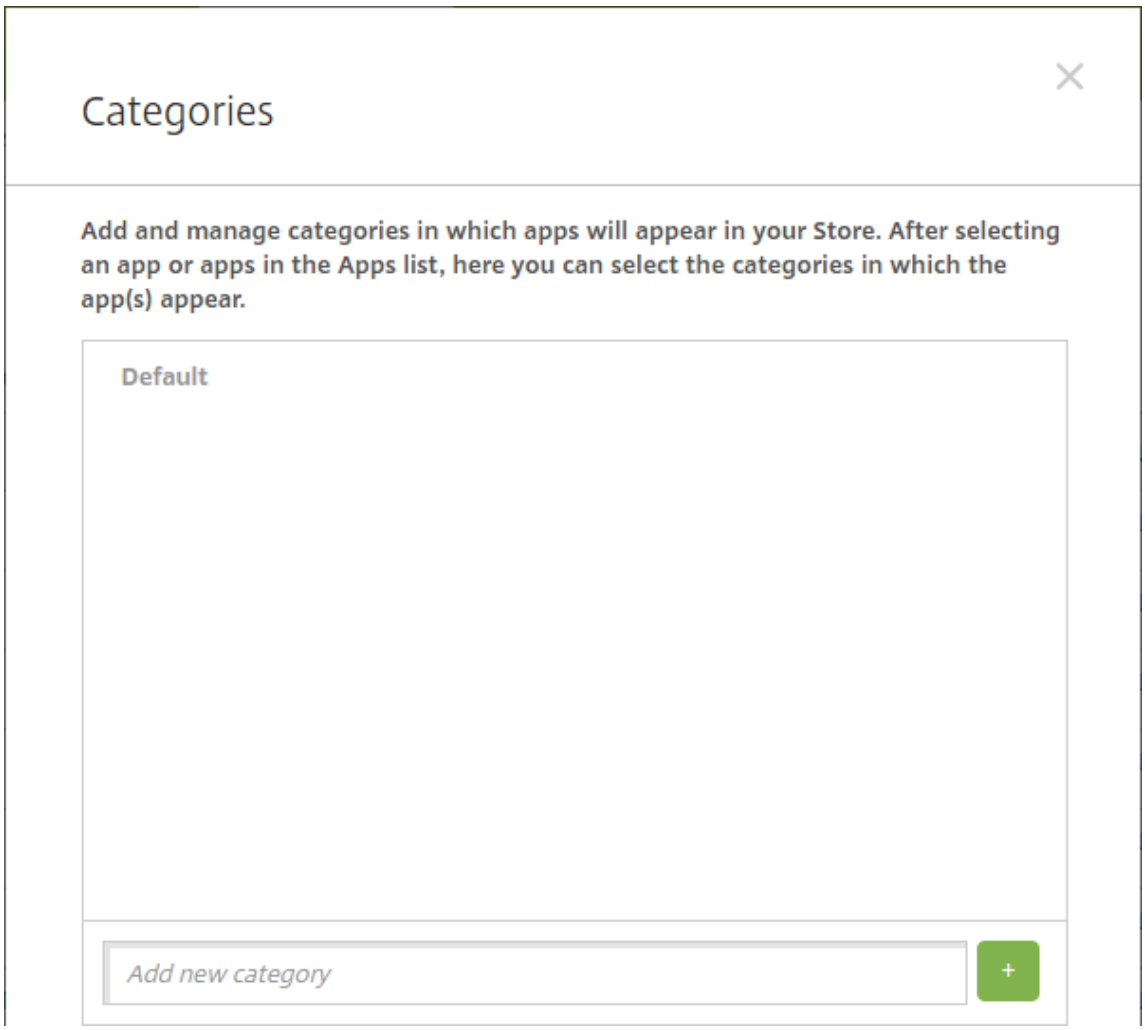
> **Hinweis:**
>
> IT-Administratoren müssen eine App genehmigen, bevor sie einer Sammlung im Fenster "Verwalteter Google Play Store"hinzugefügt werden kann. Ein IT-Administrator kann eine App unter https://play.google.com/work genehmigen. In zukünftigen Releases müssen Sie eine App nicht genehmigen, bevor Sie sie einer Sammlung hinzufügen.

Info zu App-Kategorien (iOS und MDX)

Wenn Benutzer sich bei Citrix Secure Hub anmelden, erhalten sie eine Liste der Apps, Weblinks und Stores, die Sie in Citrix Endpoint Management konfiguriert haben. In iOS oder MDX können Sie mit App-Kategorien 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.

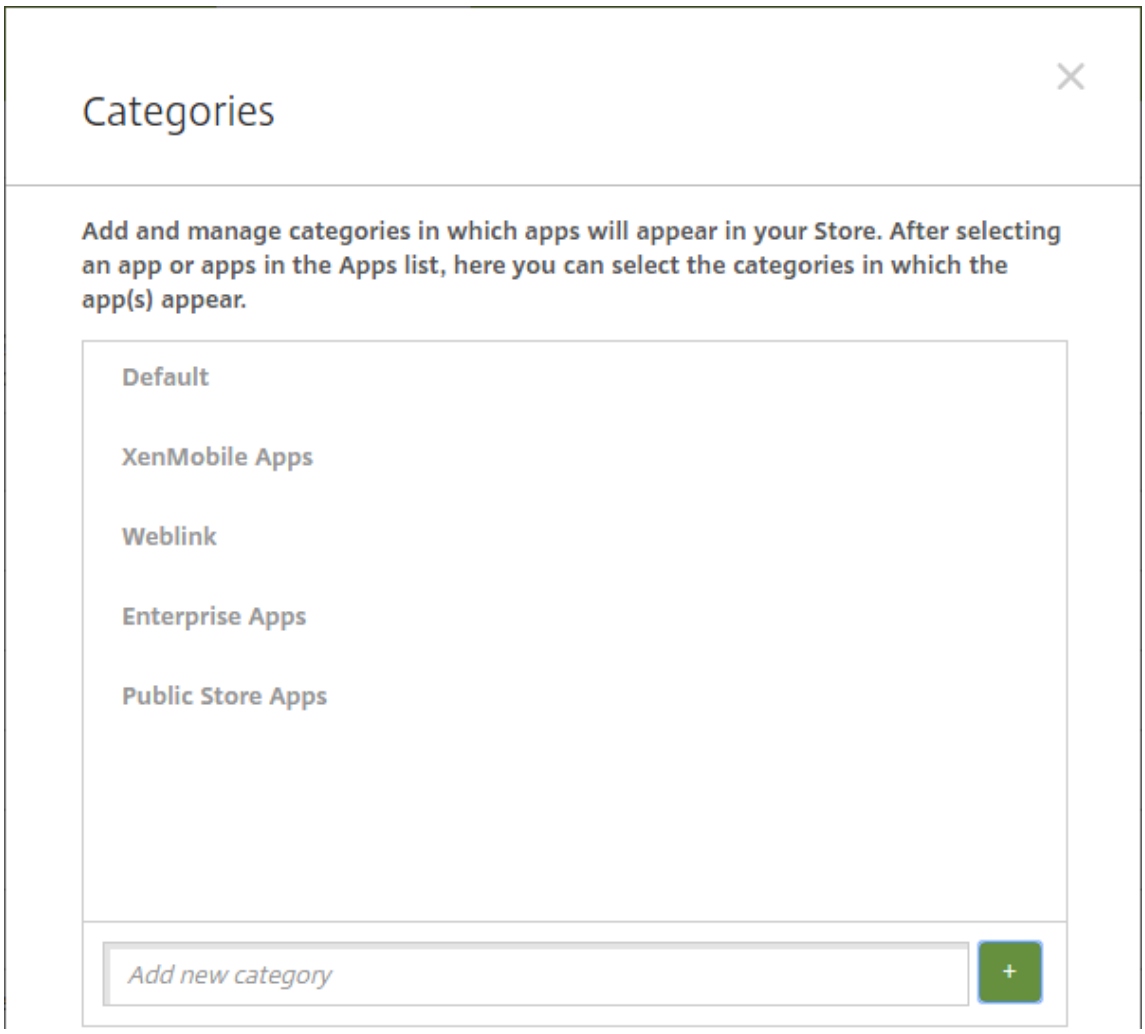
Wenn Sie eine App, einen Weblink oder einen Store hinzugefügt bzw. bearbeitet haben, können Sie diese(n) einer oder mehreren Kategorien zuweisen.

1. Klicken Sie in der Citrix Endpoint Management-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.



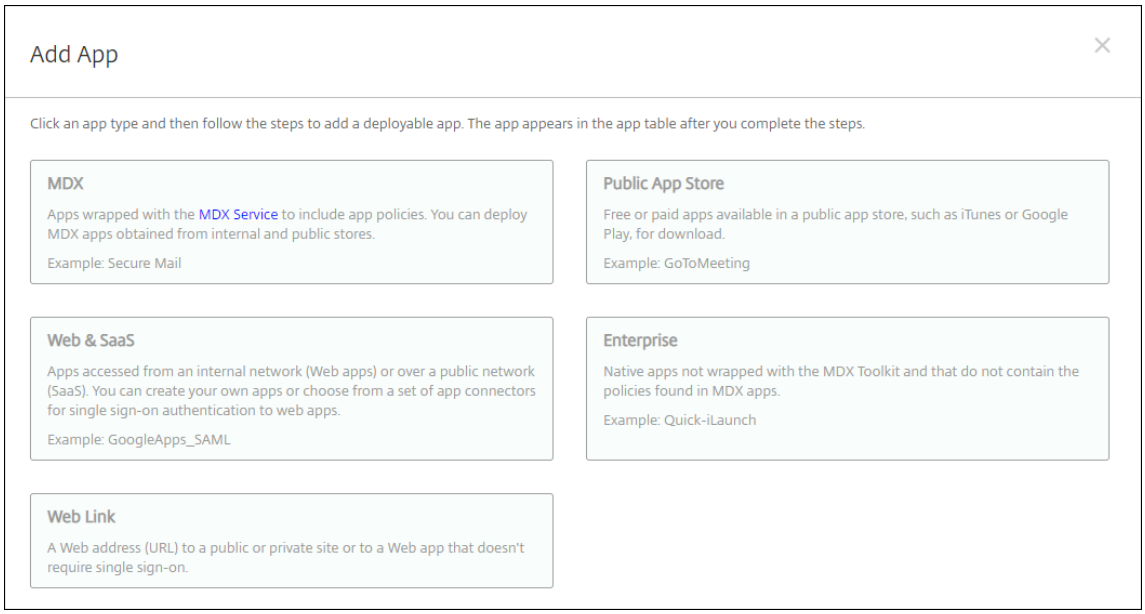
3. Wenn Sie alle Kategorien hinzugefügt haben, schließen Sie das Dialogfeld **Kategorien**.
4. Auf der Seite **Apps** können Sie vorhandene Apps einer neuen Kategorie zuweisen.
    - Wählen Sie die App aus, die Sie kategorisieren möchten.
    - Klicken Sie auf **Bearbeiten**. Die Seite **App-Informationen** wird angezeigt.
    - Wenden Sie die neue Kategorie an, indem Sie das zugehörige Kontrollkästchen in der Liste **App-Kategorie** aktivieren. Deaktivieren Sie die Kontrollkästchen aller Kategorien, die Sie der App nicht zuweisen möchten.
    - Klicken Sie auf die Registerkarte **Zuweisungen für Bereitstellungsgruppen** oder auf allen folgenden Seiten auf **Weiter**, um durch die verbleibenden Seiten zur App-Einrichtung zu gehen.
    - Klicken Sie auf der Seite **Zuweisungen für Bereitstellungsgruppen** auf **Speichern**, um die Kategorie anzuwenden. Die neue Kategorie wird auf die App angewendet und in der Tabelle **Apps** angezeigt.

Eine MDX-App hinzufügen

Wenn Sie eine MDX-Datei für eine iOS- oder Android-App erhalten, können Sie die App in Citrix Endpoint Management 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 hier:

- Überblick über das MAM-SDK
- MDX-Richtlinien auf einen Blick

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**.
2. Für andere Arten von MDX-Apps benötigen Sie die MDX-Datei.
3. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps > Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

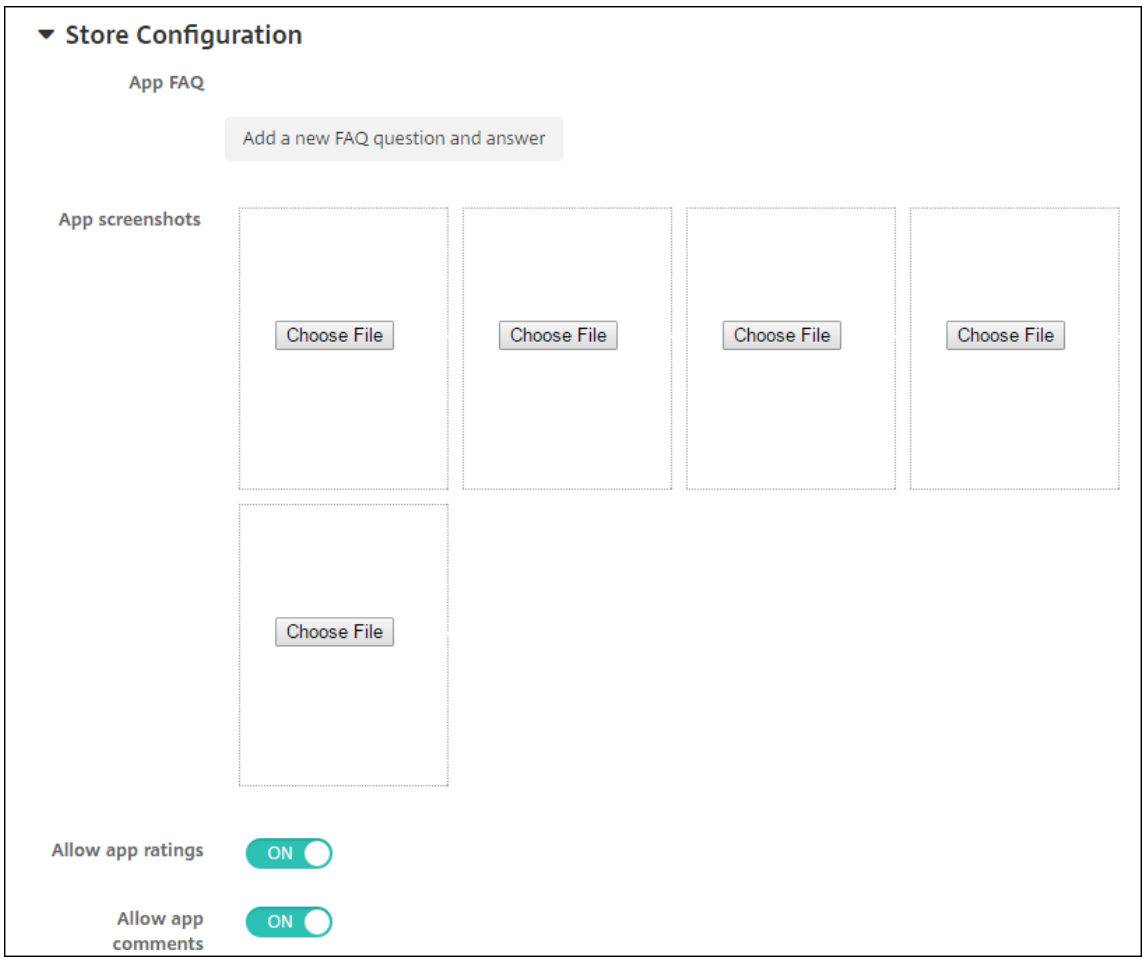


4. Klicken Sie auf **MDX**. Die Seite **App-Informationen** für MDX wird angezeigt.
5. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter **App-Name** in der Tabelle **Apps** angezeigt.
   - **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 **Plattform** wird angezeigt.

7. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.
8. Klicken Sie zum Auswählen einer MDX-Datei auf **Upload** und navigieren Sie zum Speicherort der Datei.
9. 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 aus dem verwalteten Google Play Store ein.
    - **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 Citrix Secure Hub nur die Volume Purchase-Instanz angezeigt. Die Standardeinstellung ist **Aus**.

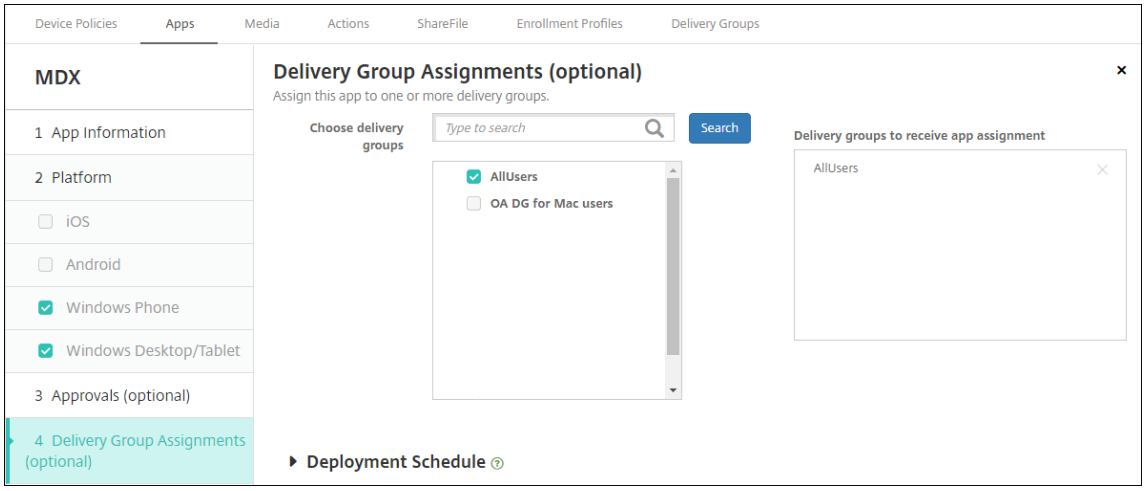
10. Konfigurieren Sie die **MDX-Richtlinien**. MDX-Richtlinien variieren je nach Plattform und bieten Optionen für Richtlinienbereiche wie Authentifizierung, Gerätesicherheit und App-Einschränkungen. In der Konsole kann eine QuickInfo mit einer Beschreibung der Richtlinien angezeigt werden.
11. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Konfigurieren von Bereitstellungsregeln.
12. Erweitern Sie **Storekonfiguration**.



Optional können Sie Folgendes konfigurieren:

- **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.

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.

    Die Option “Always-On”:

    - Ist nicht verfügbar für iOS-Geräte
    - Ist nicht verfügbar für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version ab 10.18.19 verwenden
    - Wird nicht empfohlen für Kunden, die Android und Android Enterprise sowie Citrix 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**.

16. Klicken Sie auf **Speichern**.

Apps aus einem öffentlichen App-Store hinzufügen

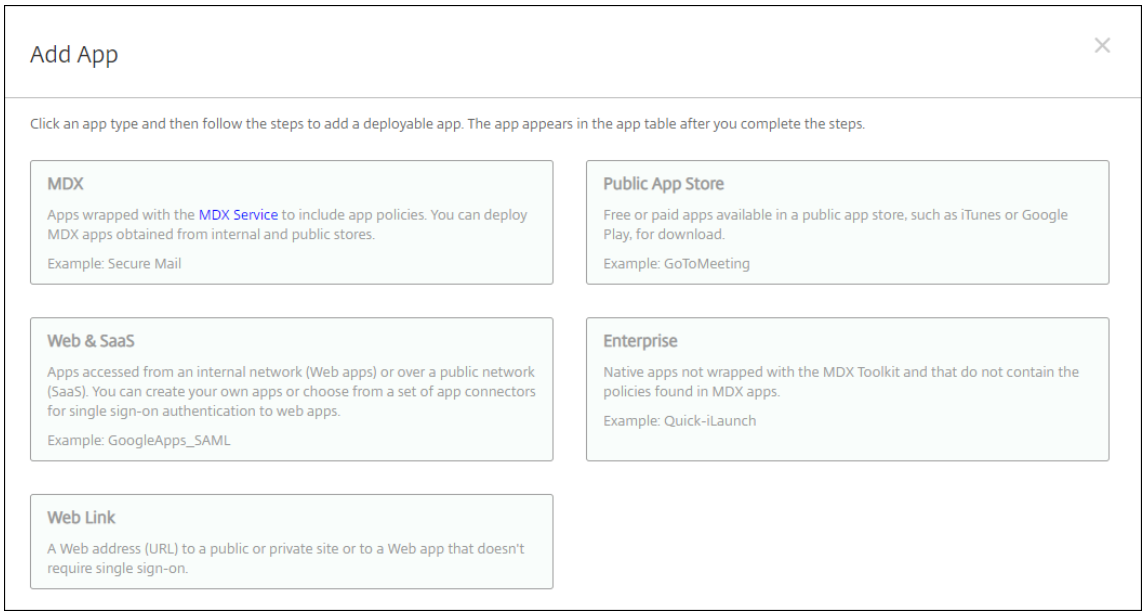
Sie können in Citrix Endpoint Management kostenlose oder kostenpflichtige Apps, die in einem öffentlichen App Store (z. B. Apple App Store) verfügbar sind, hinzufügen.

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 Citrix Endpoint Management überschrieben. Konfigurieren Sie die App-Informationen für Google Play Store manuell.

> **Hinweis:**
>
> Bezahlte Apps für Android über Android Enterprise Managed Google Play werden von Google nicht mehr unterstützt. Weitere Informationen finden Sie in der Dokumentation zur verwalteten Google Play-Hilfe.

Konfigurieren von App-Informationen und Auswählen von Plattformen, auf denen App bereitgestellt werden soll:

1. Klicken Sie in der Citrix Endpoint Management-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.

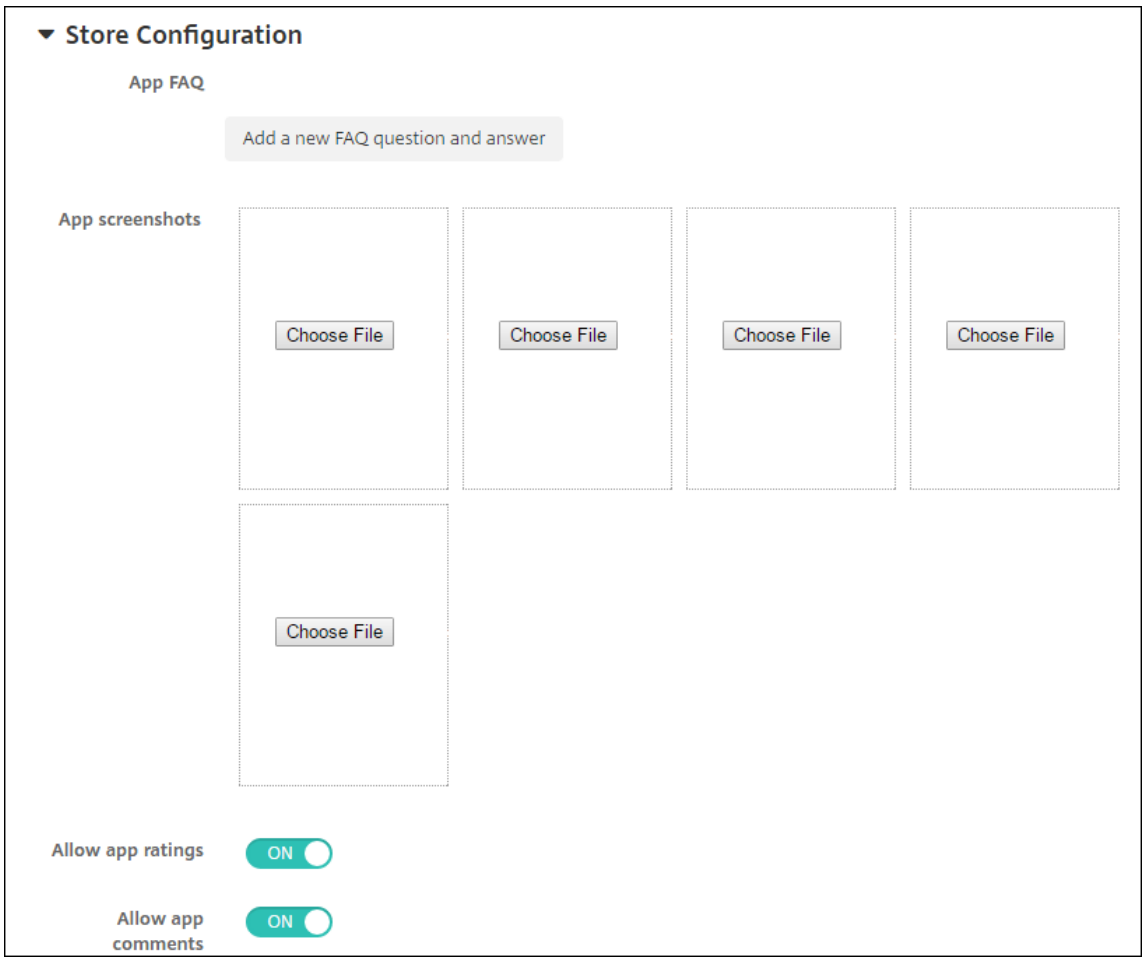
4. Klicken Sie auf **Weiter**. Die Seite **Plattform** wird angezeigt.
5. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

Als Nächstes konfigurieren Sie die App-Einstellungen für jede Plattform. Siehe:

- Konfigurieren von App-Einstellungen für Google Play-Apps
- Verwaltete App Store-Apps
- 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 Konfigurieren von Bereitstellungsregeln.
2. Erweitern Sie **Storekonfiguration**.



Optional können Sie Folgendes konfigurieren:

- **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.

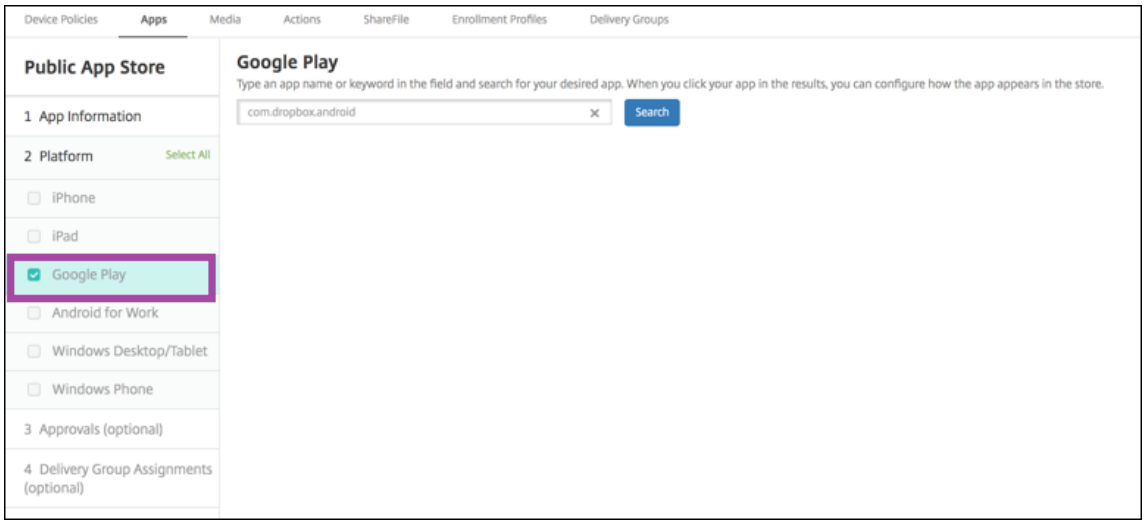
Konfigurieren von App-Einstellungen für Google Play-Apps

> **Hinweis:**
>
> Um alle Apps in Google Play über den verwalteten Google Play-Store zugänglich zu machen, verwenden Sie die Servereigenschaft **Zugriff auf alle Apps im verwalteten Google Play Store**. (Siehe Servereigenschaften.) Wenn Sie diese Eigenschaft auf **Wahr** setzen, können alle Android

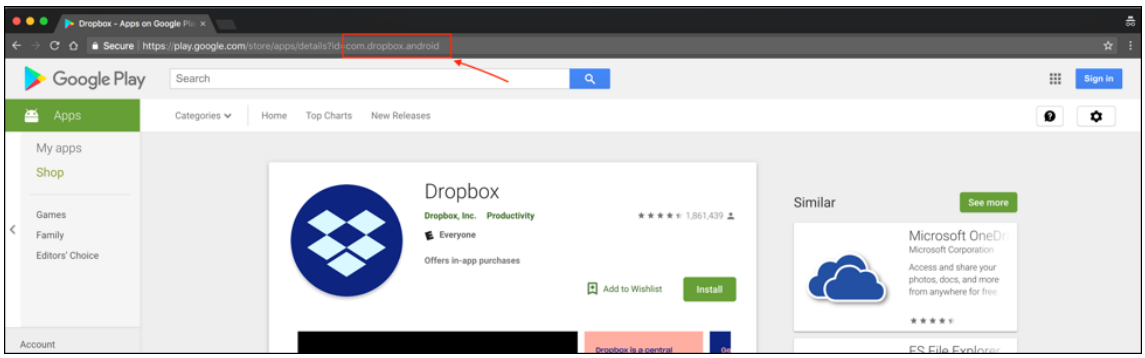
> Enterprise-Benutzer auf Apps aus dem öffentlichen Google Play Store zugreifen. Mit der Einschränkungsrichtlinie können Sie dann den Zugriff auf diese Apps steuern.

Das Konfigurieren von Einstellungen für Google Play Store-Apps erfordert andere Schritte als bei Apps für andere Plattformen. Konfigurieren Sie die App-Informationen für Google Play Store manuell.

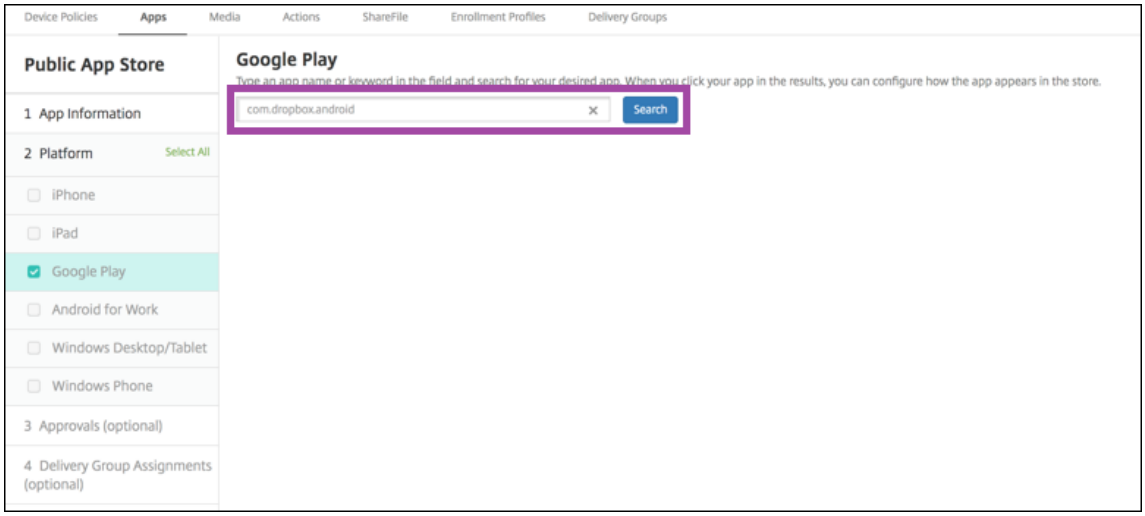
1. Stellen Sie sicher, dass **Google Play** unter **Plattformen** ausgewählt ist.



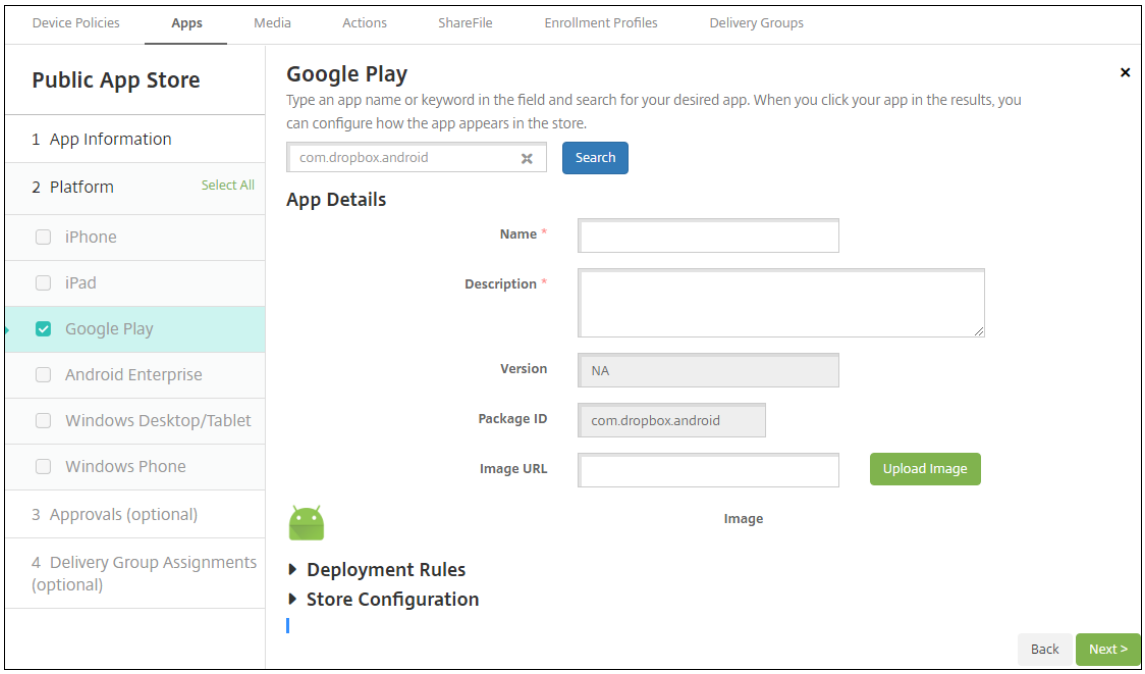
2. Rufen Sie Google Play auf. Kopieren Sie die Paket-ID aus Google Play. Die ID finden Sie in der URL der App.



3. Beim Hinzufügen einer App aus einem öffentlichen Store in der Citrix Endpoint Management-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.

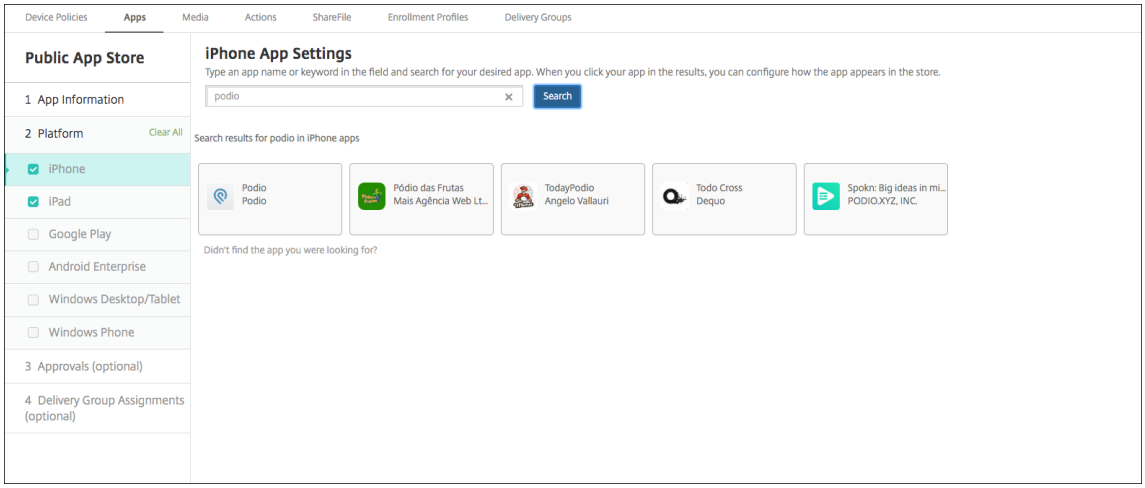
   c) Klicken Sie auf **Bild hochladen**. Das Bild wird neben **Bild** angezeigt.

Wenn Sie kein Bild konfigurieren, wird das generische Android-Bild mit der App angezeigt.

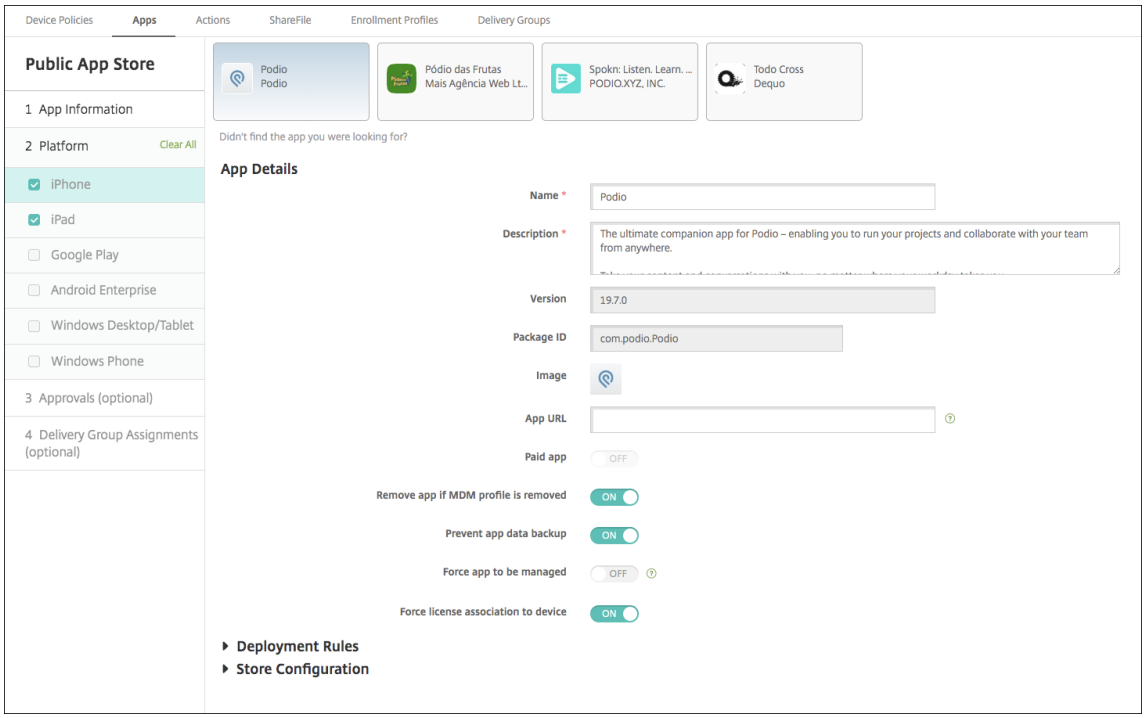
Konfigurieren der App-Einstellungen für iOS-Apps

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.



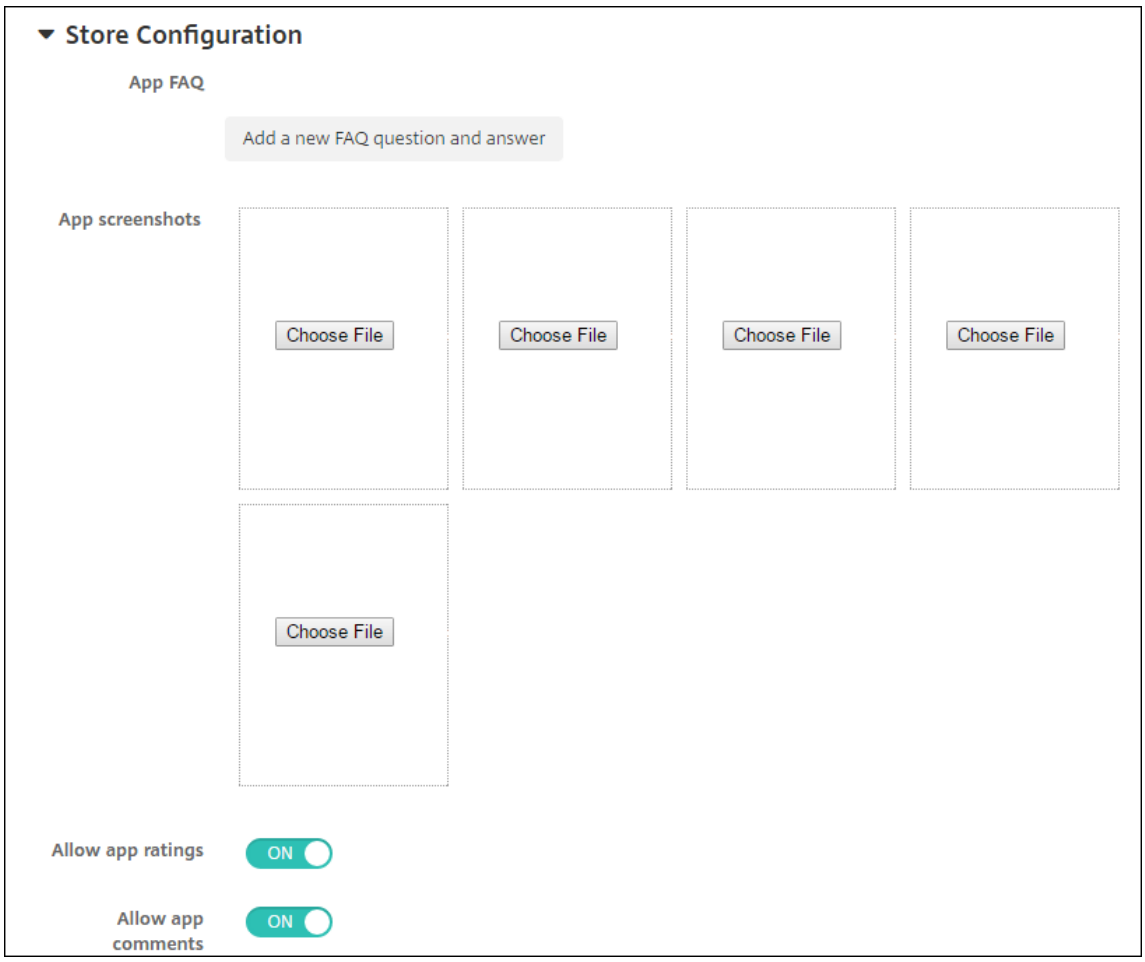
2. Klicken Sie auf die gewünschte App.
3. Die Felder im Bereich **App-Details** (Name, Beschreibung, Versionsnummer und zugeordnetes Bild) enthalten bereits Informationen zu der gewählten App.



4. Konfigurieren Sie folgende Einstellungen:

- Falls erforderlich, ändern Sie Namen und Beschreibung der App.
- **App-URL:** Geben Sie eine durch Trennzeichen getrennte Liste von URLs ein, um Ihre Apps aus der Citrix Workspace-App zu starten. Dieses Feld ist nur für iPhone- und iPad- Geräte verfügbar.
- 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 iOS-Geräten zuzulassen. Die Standardeinstellung ist **Aus**. Bei iOS-Geräten, die per Benutzerregistrierung registriert wurden, erzwingt Citrix Endpoint Management diese Einstellung nicht und fordert die Benutzer nicht auf, die App-Verwaltung zuzulassen.
- **Lizenzzuordnung zu Gerät erzwingen:** Wählen Sie aus, ob Apps, die mit aktivierter Gerätezuordnung entwickelt wurden, Geräten statt Benutzern zugewiesen werden sollen. Wenn die App keine Zuweisung zu Geräten unterstützt, können Sie diese Einstellung nicht ändern.

5. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Konfigurieren von Bereitstellungsregeln.
6. Erweitern Sie **Storekonfiguration**.



Optional können Sie Folgendes konfigurieren:

- **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) Zum Aktivieren der Anwendung von einer Purchase-Lizenz für die App in Citrix Endpoint Management 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.

c) 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. Wenn für eine App die Einstellung **Verwaltung der App erzwingen** aktiviert ist, wird sie ohne Aufforderung des Benutzers aktualisiert. Das Update erfolgt unabhängig davon, ob die App erforderlich oder optional ist.

8. Wenn Sie die Einstellungen für **Volume Purchase** 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.

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.

    Die Option “Always-On”:

    - Ist nicht verfügbar für iOS-Geräte
    - Ist nicht verfügbar für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version ab 10.18.19 verwenden

- Wird nicht empfohlen für Kunden, die Android und Android Enterprise sowie Citrix 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**.

12. Klicken Sie auf **Speichern**.

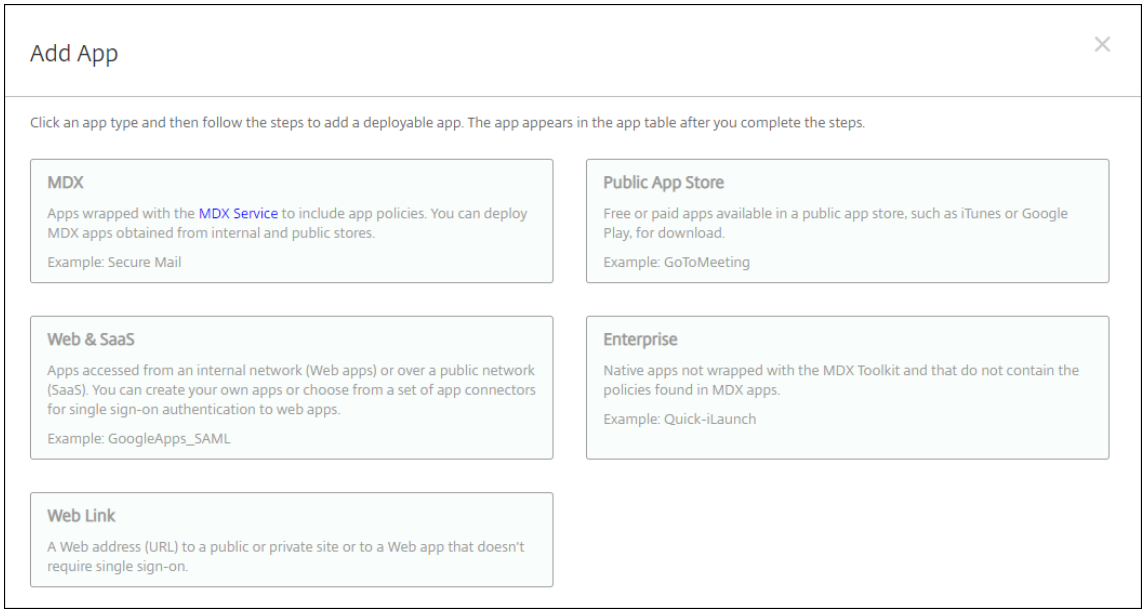
Hinzufügen von Web- und SaaS-Apps

Mit der Citrix Endpoint Management-Konsole können Sie Benutzern SSO-Zugriff (Single Sign-On) auf Unternehmens-, Web- und SaaS-Apps gewähren.

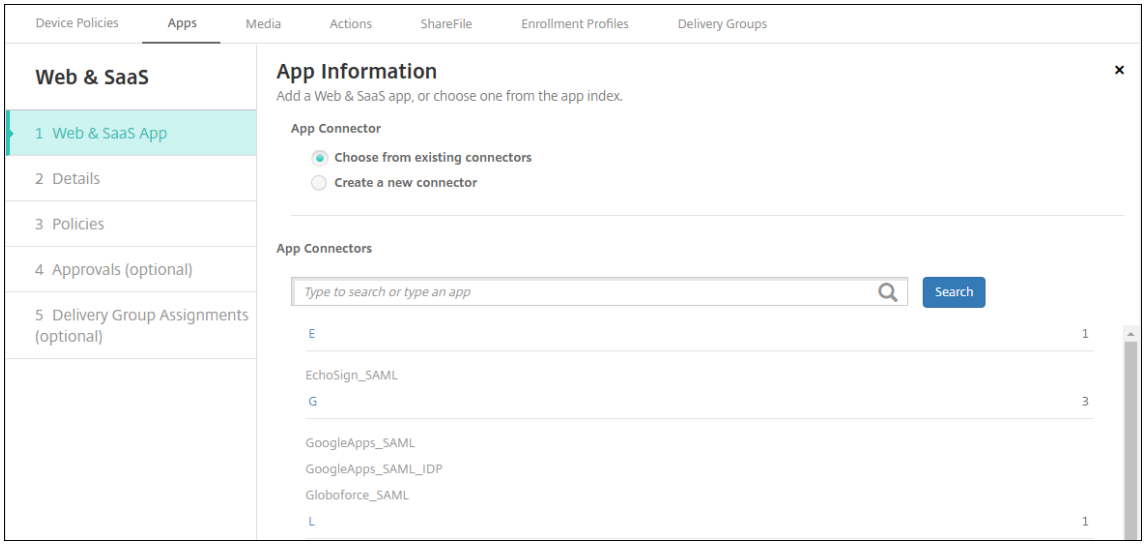
Sie können beim Hinzufügen einer Web- oder SaaS-App einen eigenen Connector in Citrix Endpoint Management erstellen. Eine Liste der in Citrix Endpoint Management verfügbaren Connectortypen finden Sie unter Anwendungsconnectortypen.

Wenn eine App nur für SSO verfügbar ist, wird die App nach dem Speichern der Einstellungen auf der Registerkarte **Apps** in der Citrix Endpoint Management-Konsole angezeigt.

1. Klicken Sie in der Citrix Endpoint Management-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.

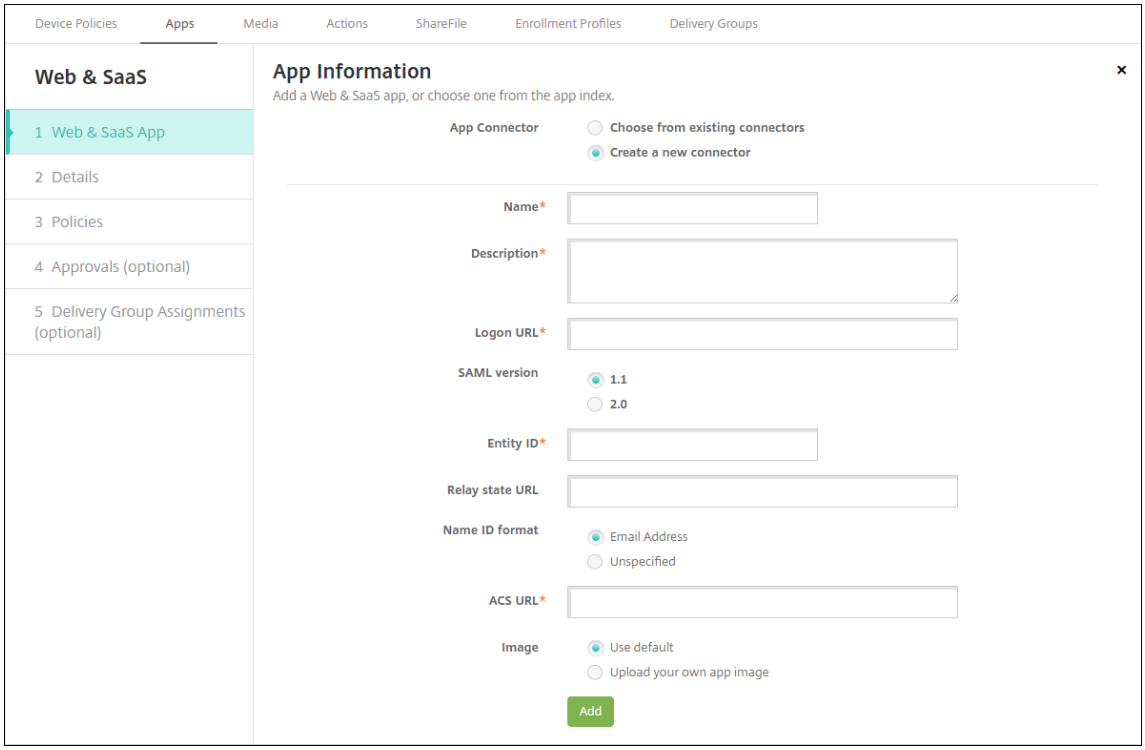
Konfigurieren eines vorhandenen App-Connectors

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 NetScaler Gateway erfolgen. Wenn Sie diese Option auf **Ein** festlegen, wird das VPN-Schlüsselwort der App hinzugefügt, sodass Benutzer eine Verbindung über NetScaler Gateway herstellen können. Die Standardeinstellung ist **Aus**.
   - **App-Kategorie:** Klicken Sie in der Liste auf eine optionale 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 ermöglichen.
- Wenn Sie **Benutzerkontoprovisioning** aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **Dienstkonto**
    - **Benutzername:** Geben Sie den Namen des App-Administrators ein. Dieses Feld ist erforderlich.
    - **Kennwort:** Geben Sie das Kennwort des App-Administrators ein. Dieses Feld ist erforderlich.
  - **Benutzerkonto**
    - **Nach Ende des Benutzeranspruchs:** Klicken Sie in der Dropdownliste 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 Dropdownliste auf die Benutzerattribute, die Sie der Regel hinzufügen möchten.
      - **Länge (Zeichen):** Klicken Sie in der Dropdownliste 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.

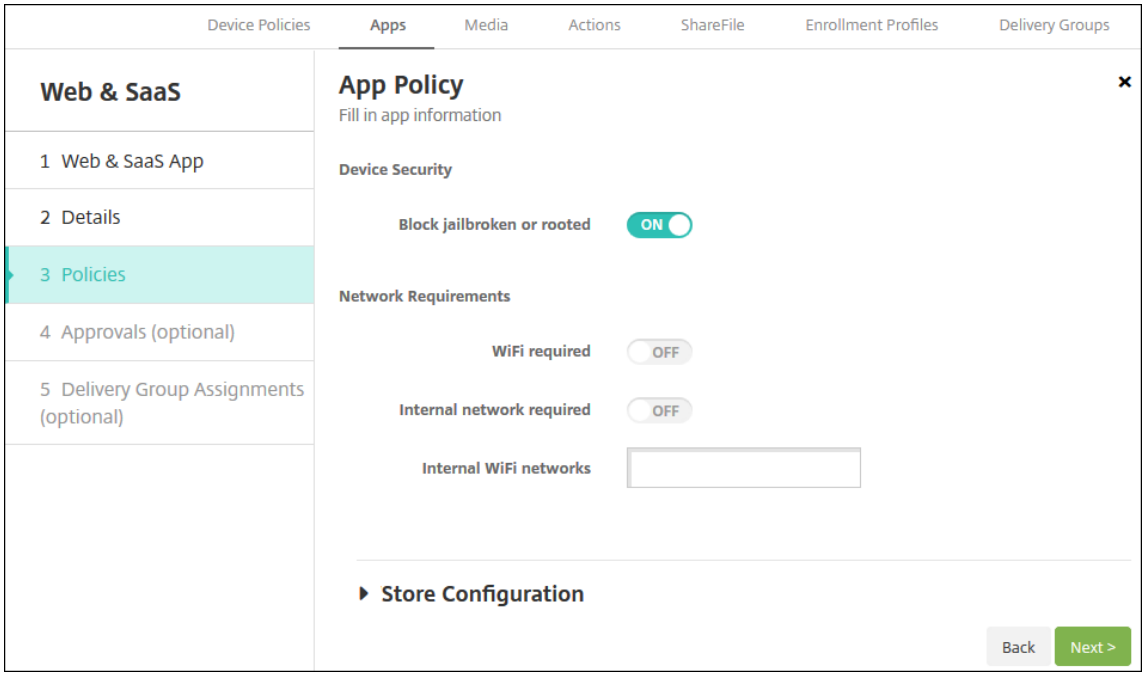


2. Konfigurieren Sie folgende Einstellungen:

   - **Name:** Geben Sie einen Namen für den Connector ein. Dieses Feld ist erforderlich.
   - **Beschreibung:** Geben Sie eine Beschreibung für den Connector ein. Dieses Feld 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`. Dieses Feld 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.

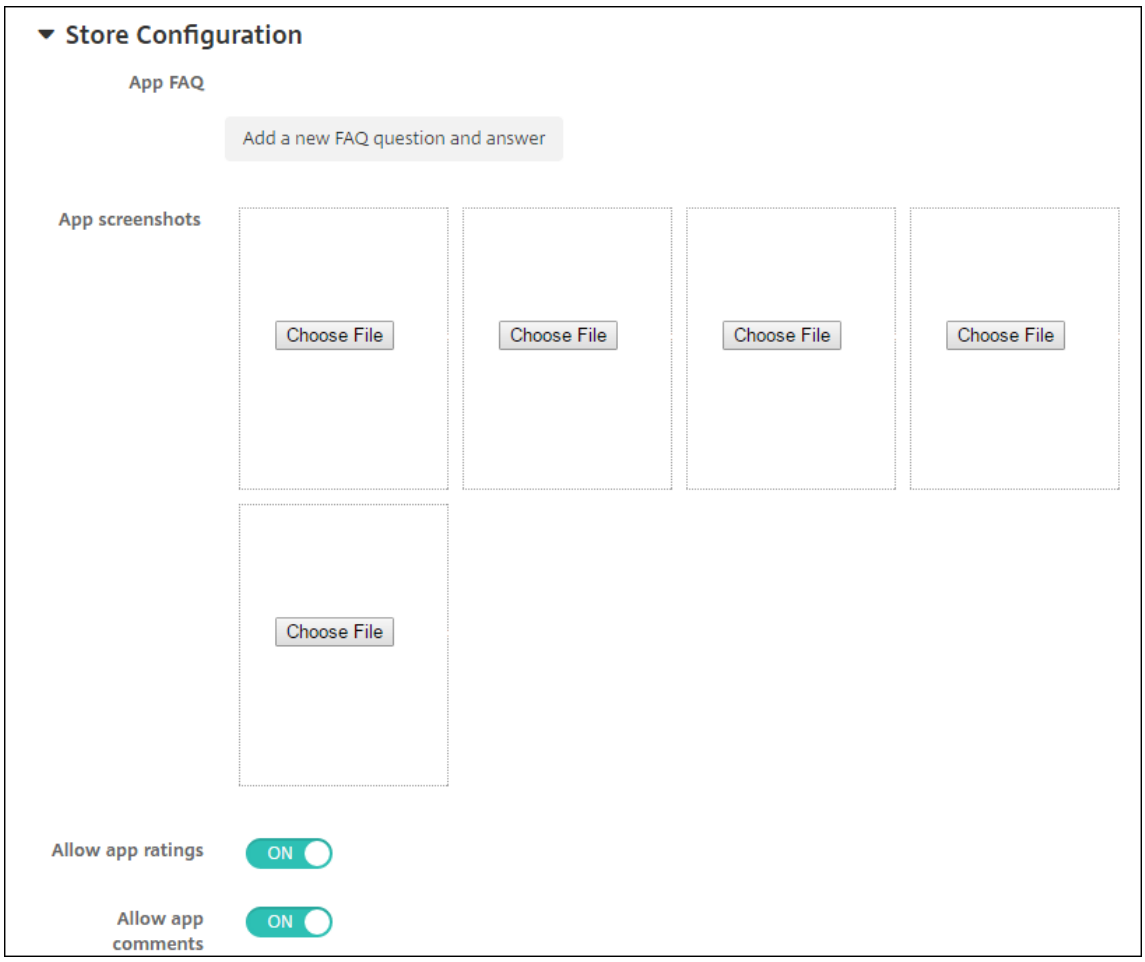
3. Wenn Sie fertig sind, klicken Sie auf **Hinzufügen**. Die Seite **Details** wird angezeigt.
4. Klicken Sie auf **Weiter**. Die Seite **App-Richtlinie** wird angezeigt.



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 das interne Wi-Fi-Netzwerk an, das verwendet werden soll.

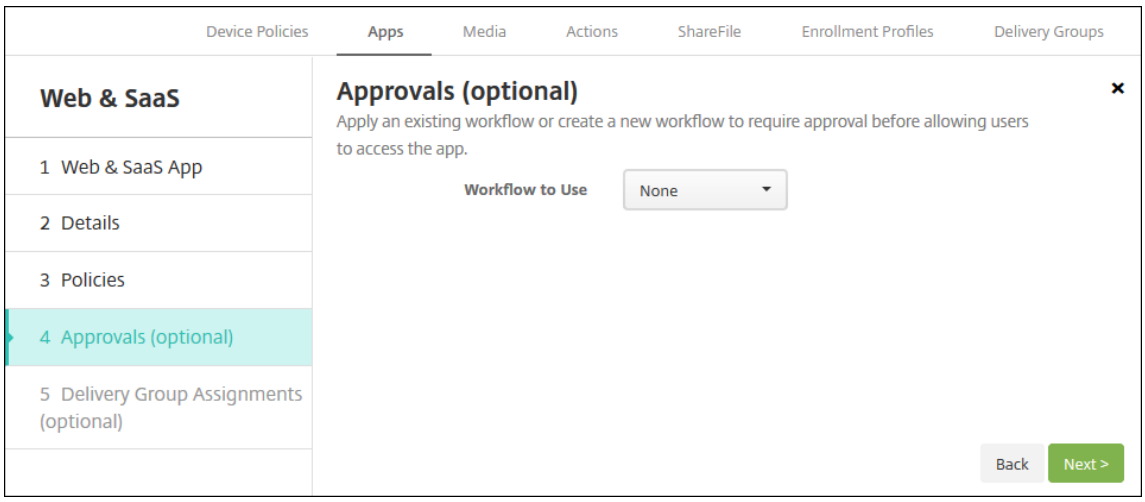
6. Erweitern Sie **Storekonfiguration**.



Optional können Sie Folgendes konfigurieren:

- **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. 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.

8. Klicken Sie auf **Weiter**. Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.
9. 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.
10. 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.

    Die Option “Always-On”:

    - Ist nicht verfügbar für iOS-Geräte
    - Ist nicht verfügbar für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version ab 10.18.19 verwenden
    - Wird nicht empfohlen für Kunden, die Android und Android Enterprise sowie Citrix 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**.

11. Klicken Sie auf **Speichern**.

Unternehmensapp hinzufügen

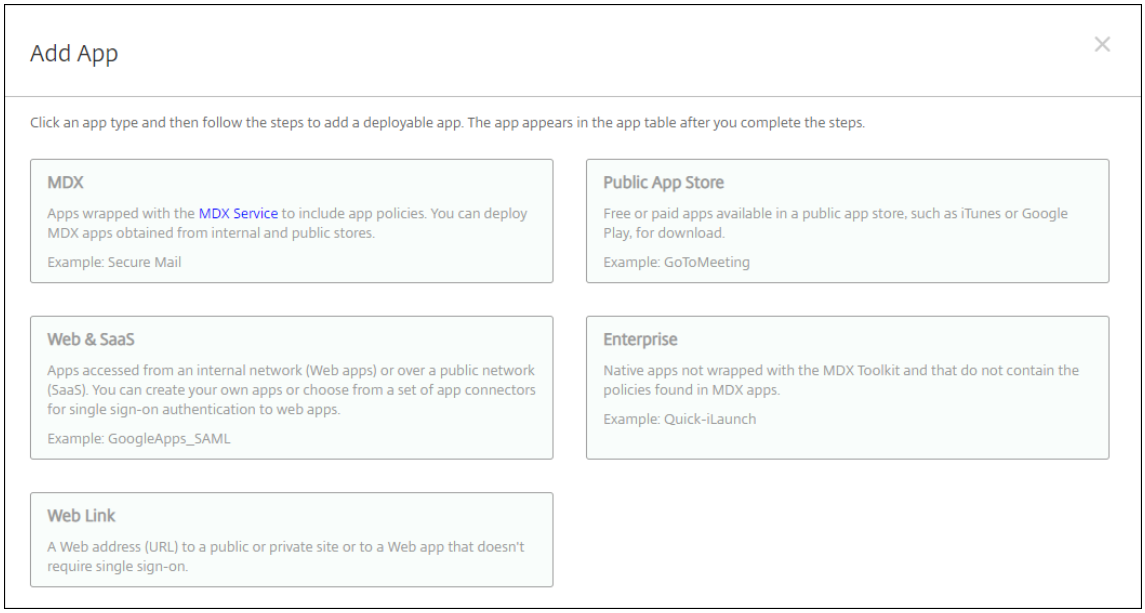
Unternehmensapps in Citrix Endpoint Management sind private Apps, die Sie selbst entwickeln oder von einer anderen Quelle beziehen. Mit Ausnahme von privaten Android Enterprise-Apps, die als MDX-fähige Apps bereitgestellt werden, werden Unternehmensapps nicht mit dem MAM-SDK oder MDX Toolkit vorbereitet. Sie können Unternehmensapps mit der Registerkarte **Apps** der Citrix Endpoint Management-Konsole hochladen. Unternehmensapps unterstützen folgende Plattformen (und die entsprechenden Dateitypen):

- iOS (.ipa)
- macOS (.pkg)

  Citrix Endpoint Management begrenzt nicht die Größe der hochgeladenen PKG-Dateien, schränkt jedoch die Uploadzeiten für Dateien ein. Standardmäßig müssen Sie Ihren Upload innerhalb von 100 s abschließen. Weitere Informationen finden Sie unter Servereigenschaften.
- Android (APK-Datei)
- Android Enterprise (APK-Datei)
- Siehe auch: Hinzufügen von Win32-Apps als Unternehmensapps
- 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 Citrix Endpoint Management-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:

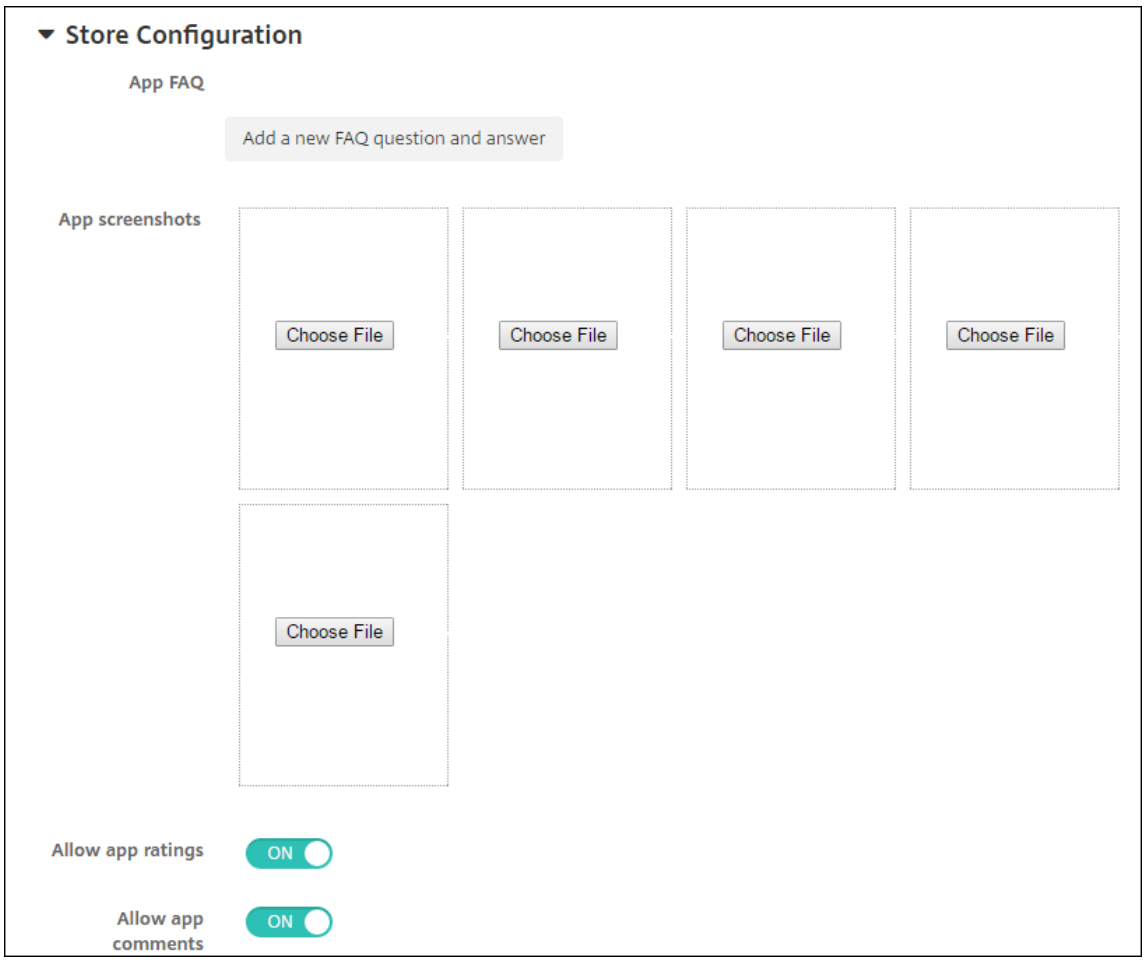
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter "App-Name"in der Tabelle "Apps"angezeigt.
   - **Beschreibung:** Geben Sie optional eine Beschreibung der App ein.
   - **App-Kategorie:** Klicken Sie optional in der Liste auf die Kategorie, der Sie die App hinzufügen 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:**Eindeutiger Bezeichner 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**. Diese Einstellung gilt nicht für macOS.
- **App-Datenbackup verhindern:** Wählen Sie aus, ob die App Daten sichern können soll. Die Standardeinstellung ist **Ein**. Diese Einstellung gilt nicht für macOS.
- **Verwaltung der App erzwingen:** Wählen Sie aus, ob eine App auf nicht betreuten Geräten als verwaltet installiert werden soll. Der Gerätetyp bestimmt, wie Citrix Endpoint Management diese Einstellung verarbeitet, wenn sie aktiviert ist. Wenn Sie diese Einstellung aktivieren, wird die App ohne Aufforderung des Benutzers aktualisiert. Das Update erfolgt unabhängig davon, ob die App erforderlich oder optional ist. Die Standardeinstellung ist **Aus**.
  - Wenn die App auf iOS-Geräten bereits installiert ist, erhalten Benutzer eine Aufforderung, die Verwaltung der App zuzulassen. Wenn Sie eine App auf Geräten bereitstellen, auf denen die App nicht existiert, wird die App unabhängig vom Status dieser Einstellung als verwaltete App installiert. Verfügbar in iOS 9.0 und höher. Bei iOS-Geräten, die per Benutzerregistrierung registriert wurden, erzwingt Citrix Endpoint Management diese Einstellung nicht und fordert die Benutzer nicht auf, die App-Verwaltung zuzulassen.
  - Aktivieren Sie auf macOS-Geräten diese Einstellung und stellen Sie die App dann auf den Geräten bereit. Die App wird automatisch als verwaltete App installiert. Benutzer erhalten keine Aufforderung. Wenn Sie eine App auf Geräten bereitstellen, auf denen die App nicht existiert, wird die App unabhängig vom Status dieser Einstellung als verwaltete App installiert. Verfügbar in macOS 11.0 und höher.

9. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Konfigurieren von Bereitstellungsregeln.
10. Erweitern Sie **Storekonfiguration**.



Optional können Sie Folgendes konfigurieren:

- **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.

    Die Option “Always-On”:

    - Ist nicht verfügbar für iOS-Geräte
    - Ist nicht verfügbar für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version ab 10.18.19 verwenden
    - Wird nicht empfohlen für Kunden, die Android und Android Enterprise sowie Citrix 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**.

15. Klicken Sie auf **Speichern**.

Hinzufügen von Win32-Apps als Unternehmensapps

Sie können MSI-, APPX-, AppxBundle-, PS1- oder EXE-Dateien für Win32-Apps in Citrix Endpoint Management hochladen, um diese auf verwalteten Windows 10- und Windows 11-Desktop- und Tablet-Geräten bereitzustellen. Nach dem Bereitstellen der Dateien mit Citrix Endpoint Management installiert das Windows-Gerät die App wie folgt:

- Falls die alte Version bei der Installation durch die aktualisierte App entfernt wird, ist auf dem Gerät nur die aktualisierte App.
- Falls die aktualisierte App die alte Version zwar nicht entfernen kann, aber dennoch installiert wird, sind auf dem Gerät beide Versionen der App vorhanden. Die Informationen zur alten Version sind jedoch nicht mehr in Citrix Endpoint Management enthalten.

- Wenn die aktualisierte App wegen der vorhandenen Version nicht installiert werden kann, wird die neue App nicht installiert. In diesem Fall müssen Sie zunächst die Geräterichtlinie zur App-Deinstallation bereitstellen, um die alte Version zu entfernen. Stellen Sie dann die neue Version bereit.

Anforderungen

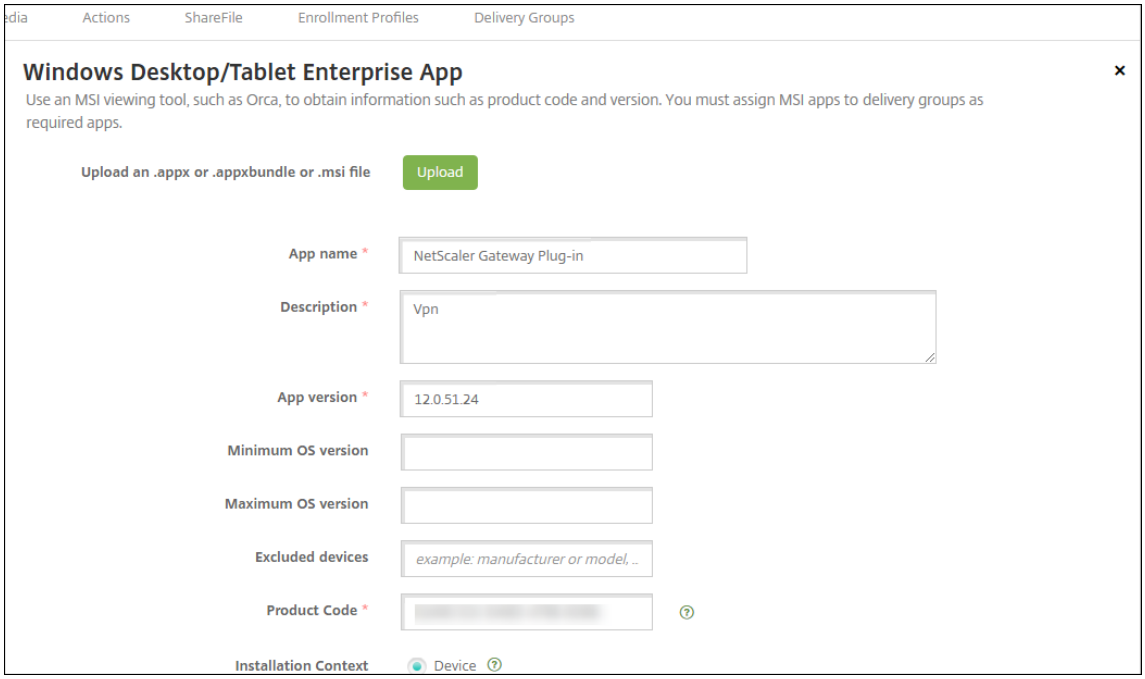
- Windows 10 (Version 1607 oder höher) oder Windows 11
- Windows 10 Professional oder Windows 11 Professional
- Windows 10 Enterprise oder Windows 11 Enterprise
- Eigenständige Win32 MSI-Apps, installiert mit der Befehlszeilenoption /quiet. Für diesen Anwendungsfall unterstützt Microsoft keine MSI-Pakete mit mehreren Apps, verschachtelten MSIs oder interaktiver Installation.

Abfrage von Metadaten Beim Hinzufügen einer Win32-App zu Citrix Endpoint Management müssen Sie die Metadaten für die App angeben. Sie ermitteln diese, indem Sie die Orca-Anwendung auf einem Windows-Computer ausführen und folgende Informationen notieren:

- Produktcode
- Produktname
- Produktversion
- Paket-Installationstyp (pro Benutzer oder pro Maschine)

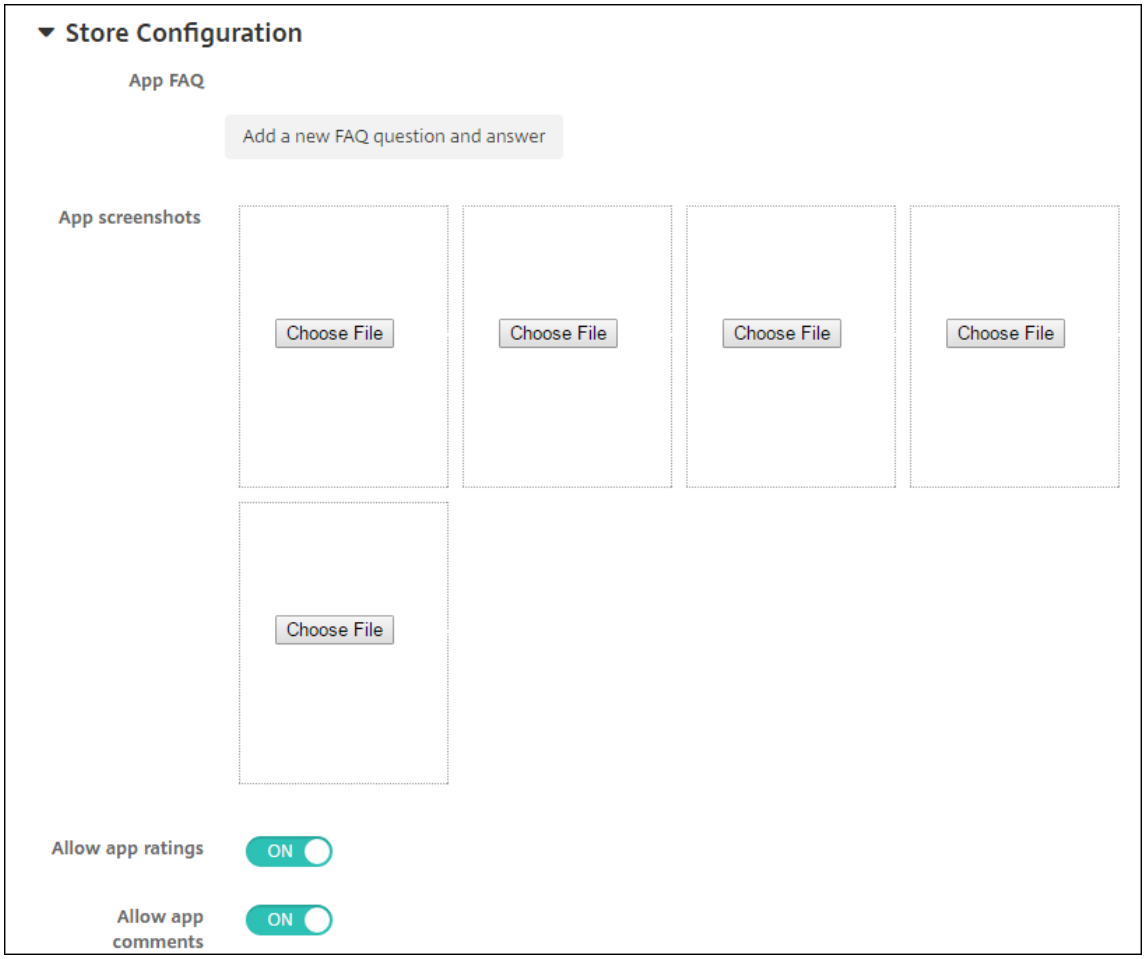
Hinzufügen einer Win32-App zu Citrix Endpoint Management

1. Navigieren Sie zu **Konfigurieren > Apps**, klicken Sie auf **Unternehmen** und geben Sie auf der Seite **App-Informationen** einen Namen für die App ein.
2. Deaktivieren Sie die Kontrollkästchen aller Plattformen mit Ausnahme von **Windows Desktop/Tablet**.
3. Klicken Sie auf der Seite der **Unternehmensapps für Windows Desktop/Tablet** auf **Hochladen** und navigieren Sie zur Datei.
4. Konfigurieren Sie folgende Einstellungen:



- **App-Name:** Name der App (aus den App-Metadaten).
- **Beschreibung:** Beschreibung der App.
- **App-Version:** Versionsnummer der App (aus den App-Metadaten).
- **OS-Version (Minimum):** optional. Älteste Betriebssystemversion, unter der die App ausgeführt werden kann.
- **OS-Version (Maximum):** optional. Neueste Betriebssystemversion, unter der die App ausgeführt werden kann.
- **Ausgeschlossene Geräte:** optional Hersteller oder Gerätemodelle, auf denen die App nicht ausgeführt werden kann.
- **Produktcode:** Produktcode der MSI-App, im UUID-Format (aus den App-Metadaten).
- **Installationskontext:** Wählen Sie entsprechend der App-Metadaten aus, ob die App für das Gerät oder den Benutzer installiert werden soll. Diese Einstellung ist für EXE-Dateien nicht verfügbar.
- **Befehlszeile:** Befehlszeilenoptionen beim Aufrufen von MSIEXEC.exe.
- **Installationsbefehlszeile:** Fügen Sie Befehlszeilenargumente für eine automatische Installation von EXE-Dateien hinzu.
- **Deinstallationsbefehlszeile:** Fügen Sie Befehlszeilenargumente für eine automatische Deinstallation von EXE-Dateien hinzu.
- **Wiederholungszahl:** Anzahl möglicher Download- und Installationsversuche, bevor eine Installation als fehlgeschlagen gekennzeichnet wird.
- **Timeout:** Dauer (in Minuten), die eine Installation ausgeführt wird, bevor eine Installation als fehlgeschlagen eingestuft und nicht länger überwacht wird.
- **Wiederholungsintervall:** Dauer (in Minuten) zwischen zwei Wiederholungen.

5. Konfigurieren Sie die Bereitstellungsregeln. Weitere Informationen finden Sie unter Konfigurieren von Bereitstellungsregeln.
6. Erweitern Sie **Storekonfiguration**.



Optional können Sie Folgendes konfigurieren:

- **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. Klicken Sie auf **Weiter,** bis die **Zusammenfassung** angezeigt wird und klicken Sie auf **Speichern**.
8. Navigieren Sie zu **Konfigurieren > Bereitstellungsgruppen** und fügen Sie die Win32-App als erforderliche App hinzu.

9. Nach dem Bereitstellen der App informieren Sie Ihre Benutzer, das die App zur Verfügung steht.

Aktualisieren einer Win32-App

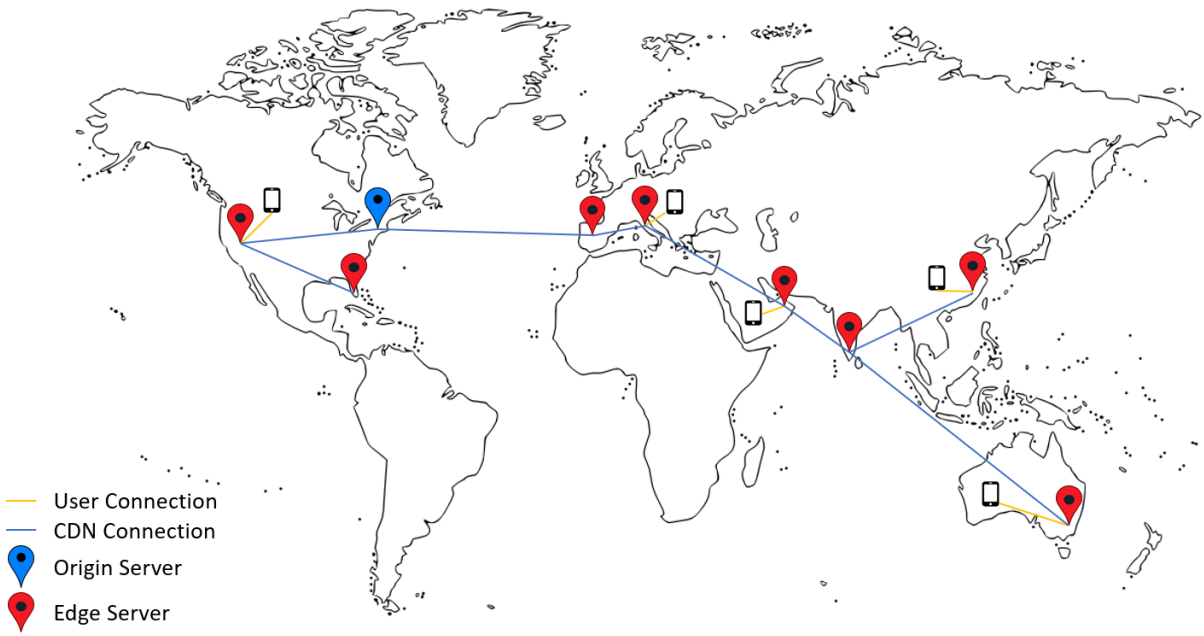
1. Ermitteln Sie die Metadaten für die App, wie zuvor unter “Abfrage von Metadaten”beschrieben.
2. Navigieren Sie zu **Konfigurieren > Apps**, um die neue Version der App hochzuladen. Aktualisieren Sie die **App-Version**. Wenn die neue App-Version einen anderen **Produktcode** hat, müssen Sie diese Einstellung aktualisieren.
3. Übermitteln Sie die Änderungen und stellen Sie die App bereit.

Bereitstellen von Unternehmensapps und MDX-Apps über das Citrix CDN

Sie können Unternehmensapps und MDX-Apps über das Citrix Netzwerk für die Inhaltsübermittlung (CDN) bereitstellen. Ein CDN umfasst geografisch verteilte Server, die zusammenarbeiten, um eine sichere und schnelle Bereitstellung von App-Inhalten zu ermöglichen. Ein lokaler Server stellt die Apps dann für Mobilgeräte bereit.

Ein CDN bietet verbesserte App-Downloadzeiten, da die Inhalte jeweils an einen Verteilungspunkt in geografischer Nähe zum Mobilgerät verteilt werden. In einem CDN werden Apps vom dem Benutzer nächstgelegenen Point of Presence-Speicherort bereitgestellt.

Die folgende Abbildung zeigt beispielhaft, wie Apps in einem CDN an den Edgeserver in nächster Nähe zu den Benutzern von Mobilgeräten verteilt werden. Ein Edgeserver dient zum Zwischenspeichern von Inhalten des Ursprungsservers, wenn Mobilgeräte Apps anfordern.



Die Benutzer können eine Verbindung mit Apps über Citrix Secure Hub herstellen. Beim Hinzufügen einer App wird der erforderliche App-Connector von Citrix Endpoint Management erstellt.

Das Bereitstellen von Unternehmensapps über das Citrix CDN wird für folgende Plattformen unterstützt:

- iOS (MDM- oder MAM-Registrierung)
- Android (MDM- oder MAM-Registrierung)
- Windows-Desktop oder -Tablet (MDM-Registrierung)
- macOS (MDM-Registrierung)

Das Bereitstellen von MDX-Apps über das Citrix CDN wird für folgende Plattformen unterstützt:

- iOS (MDM- oder MAM-Registrierung)
- Android (MDM- oder MAM-Registrierung)

Funktionsweise des CDNs

Das Herzstück des CDN-Diensts bilden miteinander verbundene Server, die Apps schneller bereitstellen sollen. Dieses Ziel wird erreicht, indem die Apps sicher an verschiedenen Verteilungspunkten weltweit platziert werden. Der DNS-Server, der von einem Mobilgerät bei der ersten Verbindung mit dem Citrix Endpoint Management-Server verwendet wurde, bestimmt den Verteilungspunkt.

Beispiel: Die DNS-Server-IP-Adresse des Mobilgeräts stammt aus Fort Lauderdale in Florida. Das CDN verwendet einen lokalen Verteilungspunkt, der möglichst nahe an diesem Standort liegt, um die App bereitzustellen. Durch die Verwendung des CDNs wird die Downloadzeit der App verbessert.

Wenn ein Mobilgerät zum ersten Mal eine Unternehmensapp übermittelt oder anfordert, kopiert Citrix Endpoint Management die App in den lokalen Verteilungspunkt und speichert sie dort für 24 Stunden, damit sie auch von anderen lokalen Geräten heruntergeladen werden kann.

Bereitstellen von Unternehmensapps über das Citrix CDN

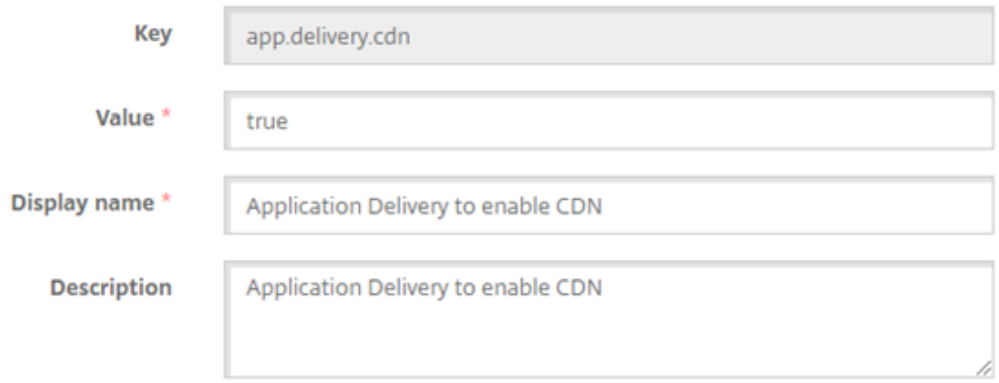
Ab Citrix Endpoint Management Release 19.4.1 erfolgt die Bereitstellung von Unternehmensapps für Neukunden mit mehreren Mandanten standardmäßig über ein CDN. Bestandskunden mit einem früheren Release befolgen die Anweisungen in diesem Abschnitt.

Unternehmensapps, die bereits auf dem Citrix Endpoint Management-Server sind, werden weiterhin von diesem bereitgestellt, bis die Apps nach Durchführung der folgenden Schritte erneut hochgeladen werden.

> **Wichtig:**
>
> Nur Citrix Cloud-Administratoren können CDN für ein Konto aktivieren. Die Servereigenschaft

> `app.delivery.cdn` ist in Citrix Endpoint Management nur sichtbar, wenn Sie sich als Citrix Cloud-Administrator anmelden. Weitere Informationen zu Citrix Cloud-Administratoren finden Sie unter Verwalten von Citrix Cloud-Administratoren.

1. CDN für Ihr Konto aktivieren: Gehen Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Servereigenschaften**.
2. Suchen Sie `app.delivery.cdn` und klicken Sie auf **Bearbeiten**.
3. Ändern Sie den Wert in **true**.



4. Laden Sie Ihre Unternehmensapps in der Citrix Endpoint Management-Konsole erneut hoch:
   a) Gehen Sie zu **Konfigurieren > Apps** und filtern Sie die App-Liste nach **Typ** (**Unternehmensanwendungen**) und **Plattform**.
   b) Wählen Sie eine App, klicken Sie auf **Bearbeiten**, klicken Sie auf **Weiter** und dann auf **Hochladen**.
   c) Wiederholen Sie diese Schritte für jede Unternehmensapp.

Bereitstellen von MDX-Apps über das Citrix CDN

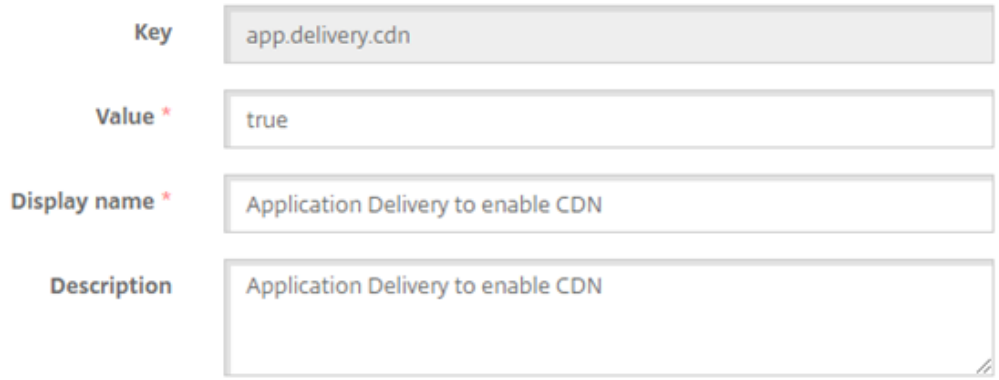
Ab Citrix Endpoint Management Release 20.12.0 erfolgt die Bereitstellung von MDX-Apps für Neukunden mit mehreren Mandanten standardmäßig über ein CDN. Bestandskunden mit einem früheren Release befolgen die Anweisungen in diesem Abschnitt.

MDX-Apps, die bereits auf dem Citrix Endpoint Management-Server sind, werden weiterhin von diesem bereitgestellt, bis die Apps nach Durchführung der folgenden Schritte erneut hochgeladen werden.

> **Wichtig:**
>
> Nur Citrix Cloud-Administratoren können CDN für ein Konto aktivieren. Die Servereigenschaft `app.delivery.cdn` ist in Citrix Endpoint Management nur sichtbar, wenn Sie sich als Citrix

> Cloud-Administrator anmelden. Weitere Informationen zu Citrix Cloud-Administratoren finden Sie unter Verwalten von Citrix Cloud-Administratoren.

1. CDN für Ihr Konto aktivieren: Gehen Sie in der Citrix Endpoint Management-Konsole zu **Einstellungen > Servereigenschaften**.
2. Suchen Sie `app.delivery.cdn` und klicken Sie auf **Bearbeiten**.
3. Ändern Sie den Wert in **true**.



4. Laden Sie Ihre MDX-Apps in der Citrix Endpoint Management-Konsole erneut hoch:
   a) Gehen Sie zu **Konfigurieren > Apps** und filtern Sie die App-Liste nach **Typ** (**MDX**) und **Plattform**.
   b) Wählen Sie eine App, klicken Sie auf **Bearbeiten**, klicken Sie auf **Weiter** und dann auf **Hochladen**.
   c) Wiederholen Sie diese Schritte für jede MDX-App.

Weblink hinzufügen

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 Citrix Secure Hub anmelden.

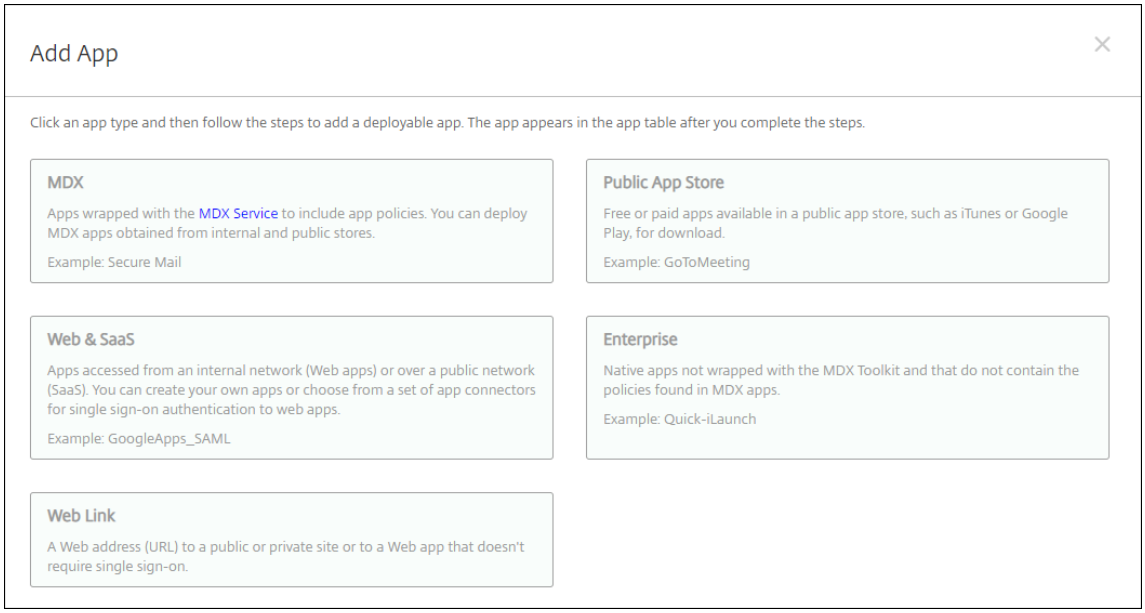
Sie können Weblinks über die Registerkarte **Apps** in der Citrix Endpoint Management-Konsole konfigurieren. Wenn Sie die Konfiguration des Weblinks abgeschlossen haben, wird der Link als Symbol in der Liste der Tabelle **Apps** angezeigt. Der Link wird mit der Liste der verfügbaren Anwendungen und Desktops angezeigt, wenn Benutzer sich bei Citrix Secure Hub anmelden.

Sehen Sie sich dieses Video an, um mehr zu erfahren:

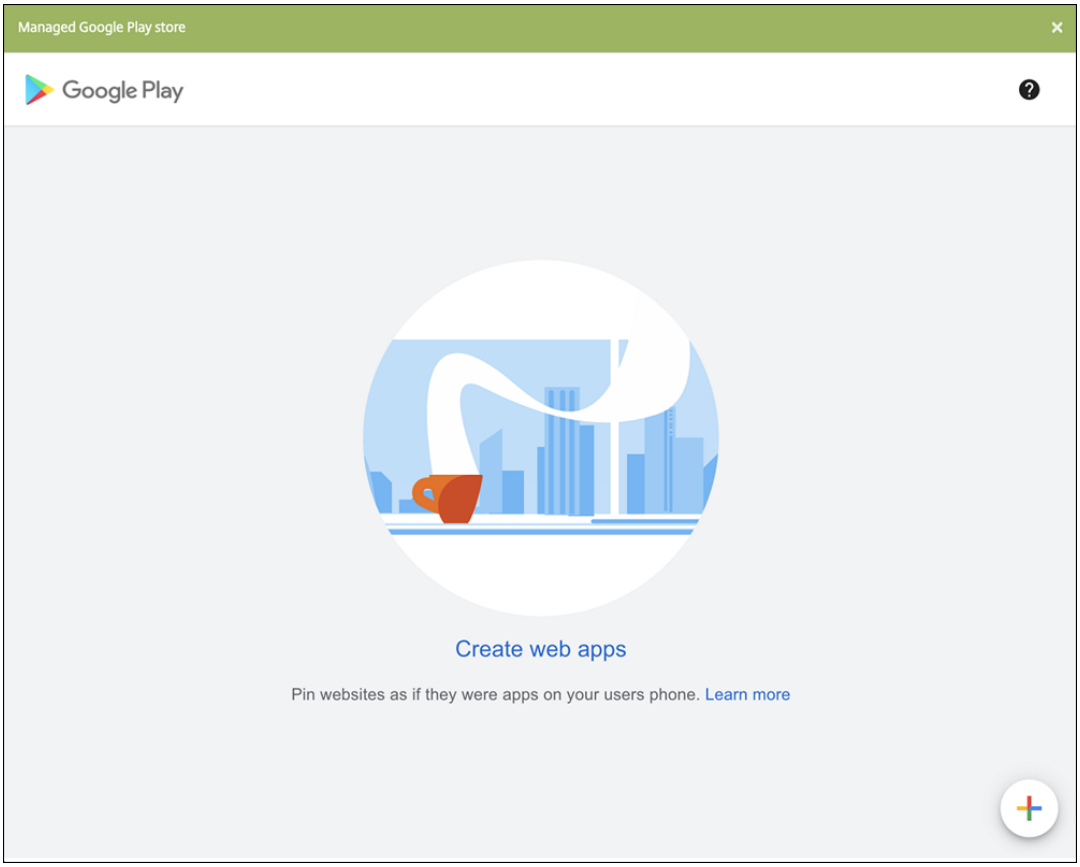
Für den hinzuzufügenden Link müssen Sie die folgenden Informationen angeben:

- Name für den Link
- Beschreibung des Links
- Webadresse (URL)
- Kategorie
- Rolle
- Bild im PNG-Format (optional)

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps > Hinzufügen**. Das Dialogfeld **App hinzufügen** wird angezeigt.

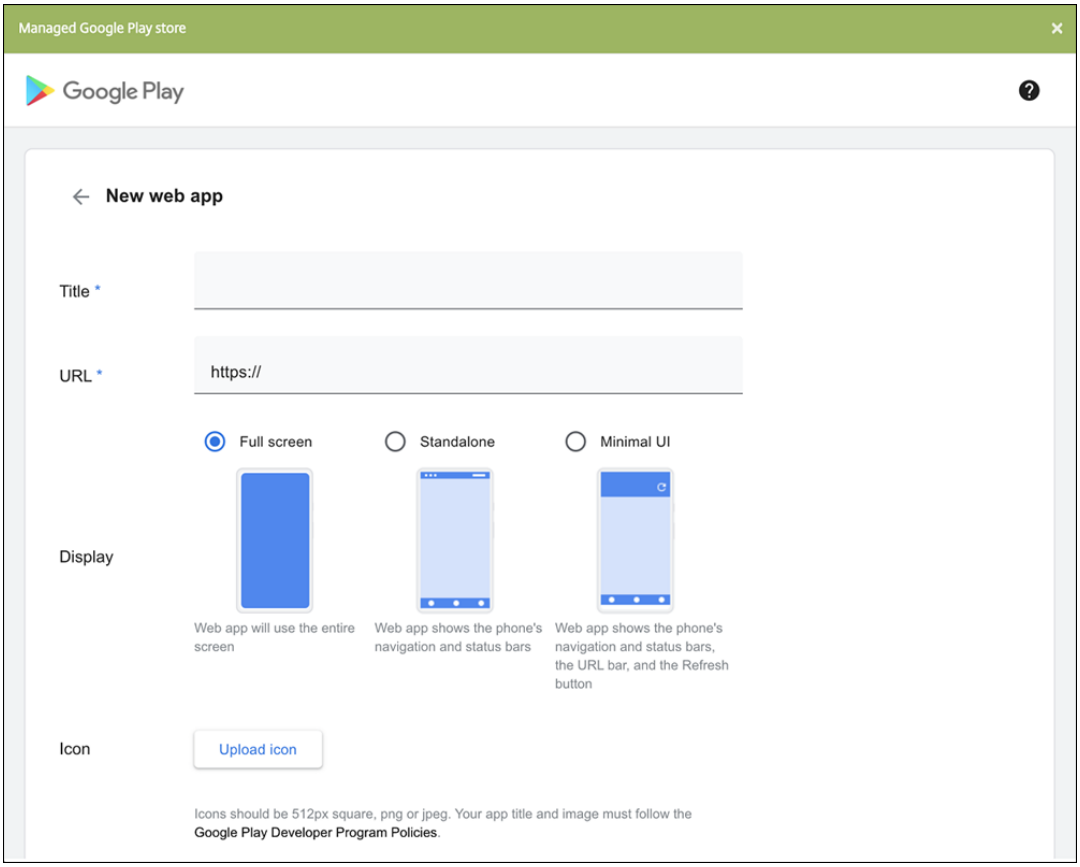


2. Klicken Sie auf **Weblinks**. Die Seite **App-Informationen** wird angezeigt.
3. Geben Sie auf der Seite **App-Informationen** die folgenden Informationen ein:
   - **Name:** Geben Sie einen aussagekräftigen Namen für die App ein. Dieser wird unter “App-Name”in der Tabelle “Apps”angezeigt.
   - **Beschreibung:** 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) und Windows 8 hinzuzufügen, oder wählen Sie **Android Enterprise**. Deaktivieren Sie das Kontrollkästchen für alle Plattformen, die Sie nicht einbeziehen 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:

- **Titel:** Geben Sie einen Namen für die Web-App ein.
- **URL:** Geben Sie die Webadresse für die App ein.
- **Anzeige:** Wählen Sie aus, wie die Web-App auf Benutzergeräten angezeigt werden soll. Verfügbare Optionen sind **Vollbild**, **Eigenständig**und **Minimalistische Benutzeroberfläche**.
- **Symbol:** Laden Sie Ihr eigenes Symbolbild für die Web-App hoch.



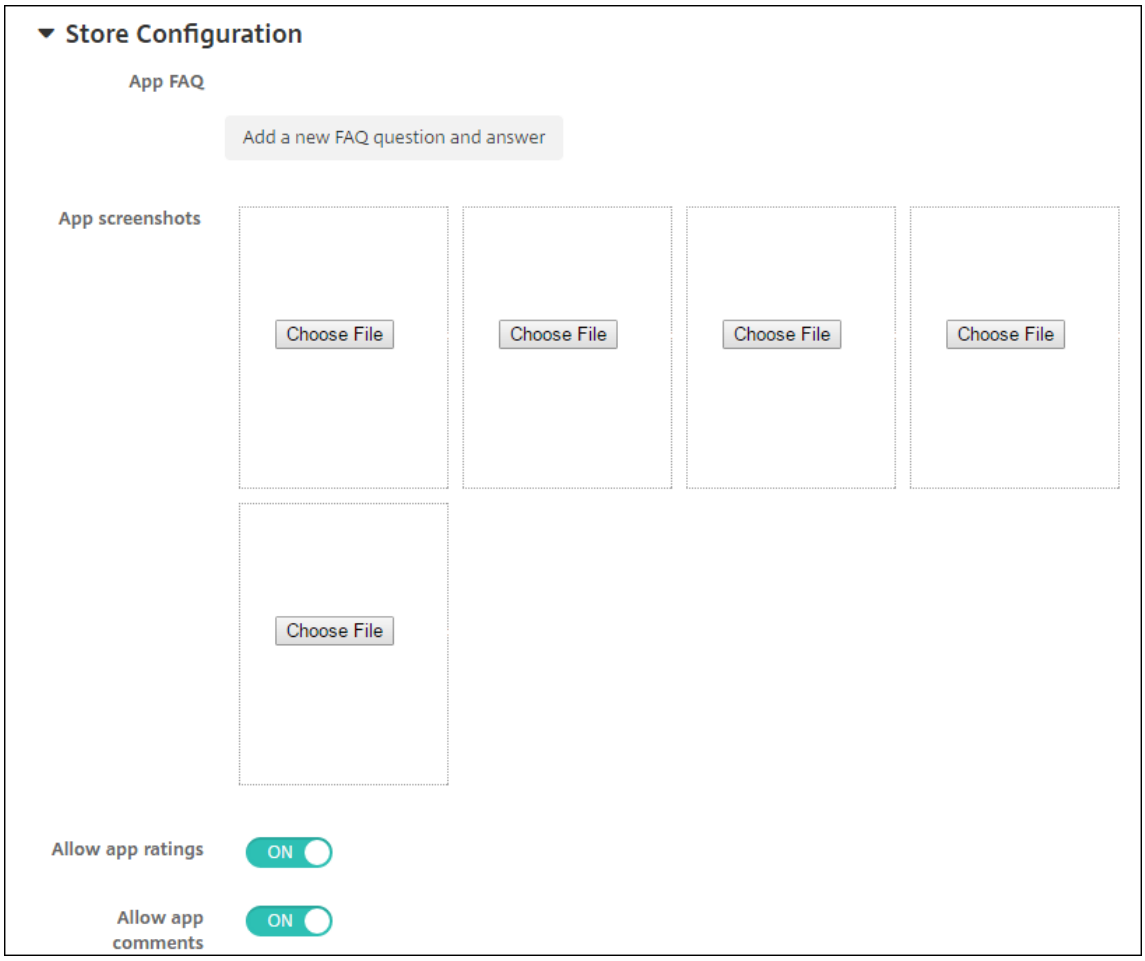
Wenn Sie fertig sind, klicken Sie auf **Erstellen**. Es kann bis zu 10 Minuten dauern, bis Ihre Web-App veröffentlicht wird.

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 NetScaler Gateway erfolgen. Wenn Sie diese Option auf **Ein** festlegen, wird das VPN-Schlüsselwort der App hinzugefügt, sodass Benutzer eine Verbindung über NetScaler Gateway herstellen können. Die Standardeinstellung ist **Aus**.
   - **App-Kategorie:** Klicken Sie in der Liste auf eine optionale 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 Konfigurieren von Bereitstellungsregeln.
8. Erweitern Sie **Storekonfiguration**.



Optional können Sie Folgendes konfigurieren:

- **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.

    Die Option “Always-On”:

    - Ist nicht verfügbar für iOS-Geräte
    - Ist nicht verfügbar für Kunden, die Android und Android Enterprise sowie Citrix Endpoint Management in einer Version ab 10.18.19 verwenden
    - Wird nicht empfohlen für Kunden, die Android und Android Enterprise sowie Citrix 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**.
12. Klicken Sie auf **Speichern**.

Aktivieren von Microsoft 365-Apps

Sie können den MDX-Container öffnen, um Citrix Secure Mail, Citrix 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.

Workflows anwenden

Konfigurieren Sie folgende Einstellungen zum Erstellen oder Zuweisen eines Workflows:

- **Verwendete Workflows:** Klicken Sie in der Dropdownliste 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

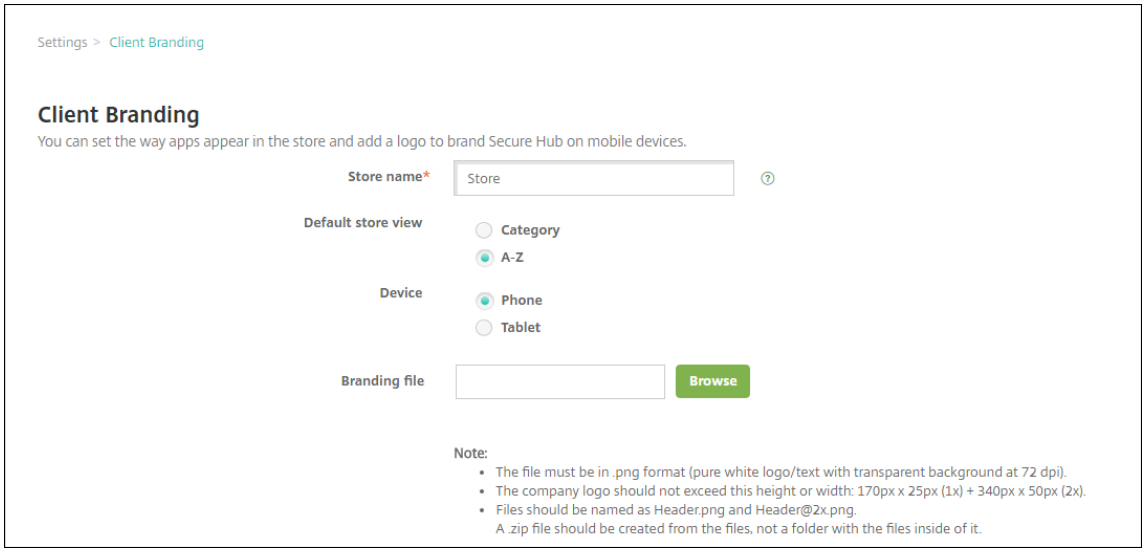
Sie können einstellen, wie Apps im Store angezeigt werden und Ihr Logo zu Citrix Secure Hub und zum App-Store hinzufügen. Diese Branding-Features stehen für iOS- und Android-Geräte zur Verfügung.

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 Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Client** auf **Clientbranding**. Die Seite **Clientbranding** wird angezeigt.



Konfigurieren Sie die folgenden Einstellungen:

- **Storename:** Der Storename wird mit den Kontoinformationen des Benutzers angezeigt. Das Ändern des Namens ändert auch die URL, die für den Zugriff auf Storedienste verwendet wird. Sie müssen in der Regel den Standardnamen nicht ändern.

  > **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:** Zum Wählen einer Bilddatei oder einer ZIP-Datei mit Bildern klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.

3. Klicken Sie auf **Speichern**.

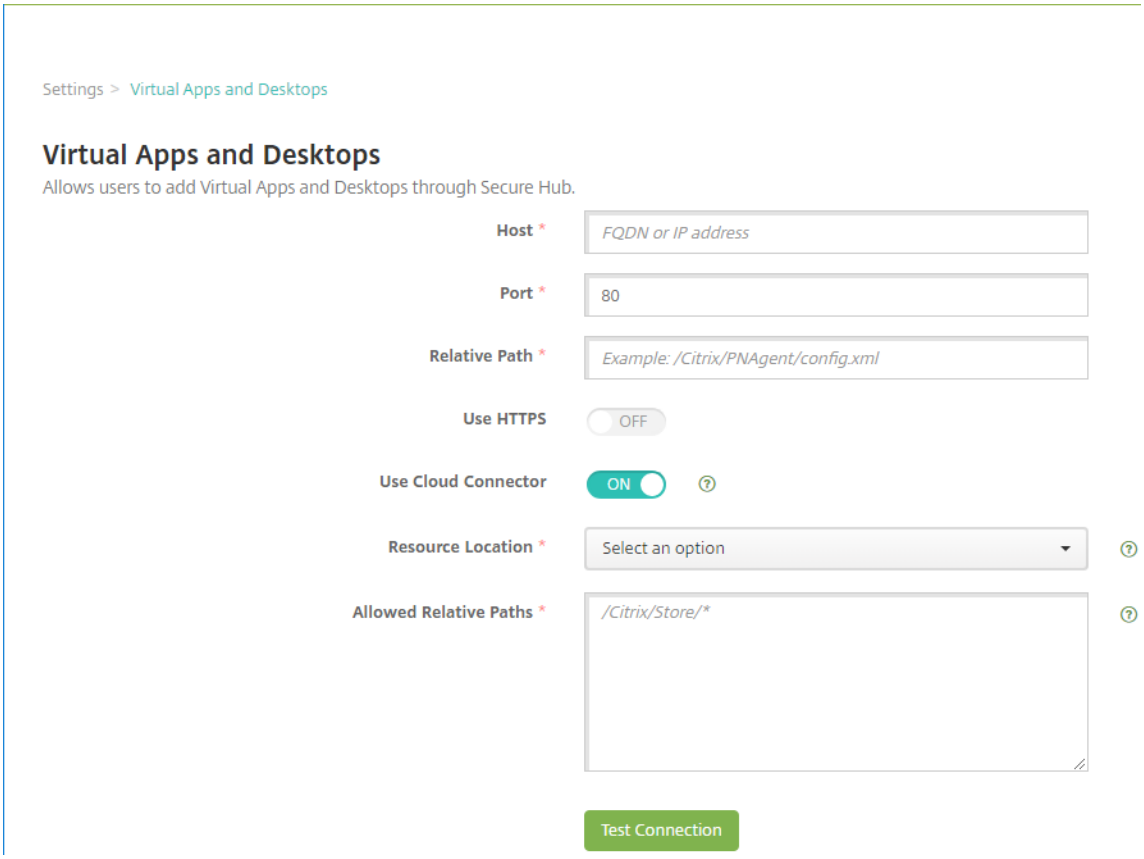
Zum Bereitstellen dieses Pakets auf den Geräten müssen Sie ein Bereitstellungspaket erstellen und bereitstellen.

Citrix Virtual Apps and Desktops über den App-Store

Citrix Endpoint Management kann Apps aus Citrix Virtual Apps and Desktops sammeln und Benutzern von Mobilgeräten im App-Store zur Verfügung stellen. Die Benutzer abonnieren Apps direkt im App-Store und starten sie über Citrix Workspace. Die Citrix Workspace-App muss auf den Geräten installiert sein, um die Apps zu starten.

Zum Konfigurieren dieser Einstellung benötigen Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse und Portnummer von On-Premises-StoreFront.

1. Klicken Sie in der Citrix Endpoint Management-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 von StoreFront ein.
   - **Port:** Geben Sie die Portnummer von StoreFront ein. Der Standardwert ist 80.
   - **Relativer Pfad:** Geben Sie den Pfad ein. Beispiel: /Citrix/PNAgent/config.xml
   - **HTTPS verwenden:** Wählen Sie aus, ob die sichere Authentifizierung zwischen StoreFront und dem Clientgerät aktiviert werden soll. Die Standardeinstellung ist **Aus**.
   - **Cloud Connector verwenden:** Wählen Sie **Ein**, um Cloud Connector für Verbindungen mit dem StoreFront-Server zu verwenden. Geben Sie dann einen **Ressourcenstandort** und **Zulässige relative Pfade** für die Verbindung an.
     - **Ressourcenstandort:** Treffen Sie Ihre Auswahl unter den unter Citrix Cloud Connector definierten Ressourcenstandorten.
     - **Zulässige relative Pfade:** die relativen Pfade, die für den angegebenen Ressourcenstandort zulässig sind. Geben Sie einen Pfad pro Zeile an. Sie können das Sternchen (*) als Platzhalter verwenden.

     Beispiel: Der Ressourcenstandort ist `https://StoreFront.company.com` und Sie möchten Zugriff auf die folgenden URLs gewähren:

- `https://StoreFront.company.com/Citrix/PNAgent/Config.xml`
- `https://StoreFront.company.com/Citrix/PNAgent/enum.aspx`
- `https://StoreFront.company.com/Citrix/PNAgent/launch.aspx`

Um alle Anfragen mit der URL `https://StoreFront.company.com/Citrix/PNAgent/*` zuzulassen, geben Sie diesen Pfad ein: `/Citrix/PNAgent/*`

Citrix Endpoint Management blockiert alle anderen Pfade.

4. Klicken Sie auf **Verbindung testen**, um zu prüfen, ob Citrix Endpoint Management eine Verbindung mit dem angegebenen StoreFront-Server herstellen kann.
5. Klicken Sie auf **Speichern**.

App-Connectortypen

March 11, 2024

In der folgenden Tabelle finden Sie die Connectors und Connectortypen, die in Citrix Endpoint Management beim Hinzufügen einer Web- oder SaaS-App verfügbar sind. Sie können auch einen Connector zu Citrix Endpoint Management hinzufügen, wenn Sie eine Web-oder SaaS-App hinzufügen.

Die Tabelle enthält Angaben dazu, ob ein Connector die Benutzerkontenverwaltung unterstützt, mit der 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

Connectorname	Single Sign-On SAML	Unterstützt Benutzerkontenverwaltung
Salesforce_SAML_SP	J	J
SandBox_SAML	J	
SuccessFactors_SAML	J	
ShareFile_SAML	J	
ShareFile_SAML_SP	J	
WebEx_SAML_SP	J	J

Citrix Launcher

December 1, 2023

Mit Citrix Launcher können Sie die Benutzererfahrung für über Citrix Endpoint Management bereitgestellte Android Enterprise-Geräte und Android-Legacygeräte anpassen. Mit Citrix Launcher können Sie den Benutzerzugriff auf bestimmte Geräteeinstellungen verhindern und Geräte auf eine oder wenige Apps begrenzen.

Die Mindestversion von Android, die für die Citrix Secure Hub-Verwaltung von Citrix Launcher unterstützt wird, ist Android 6.0.

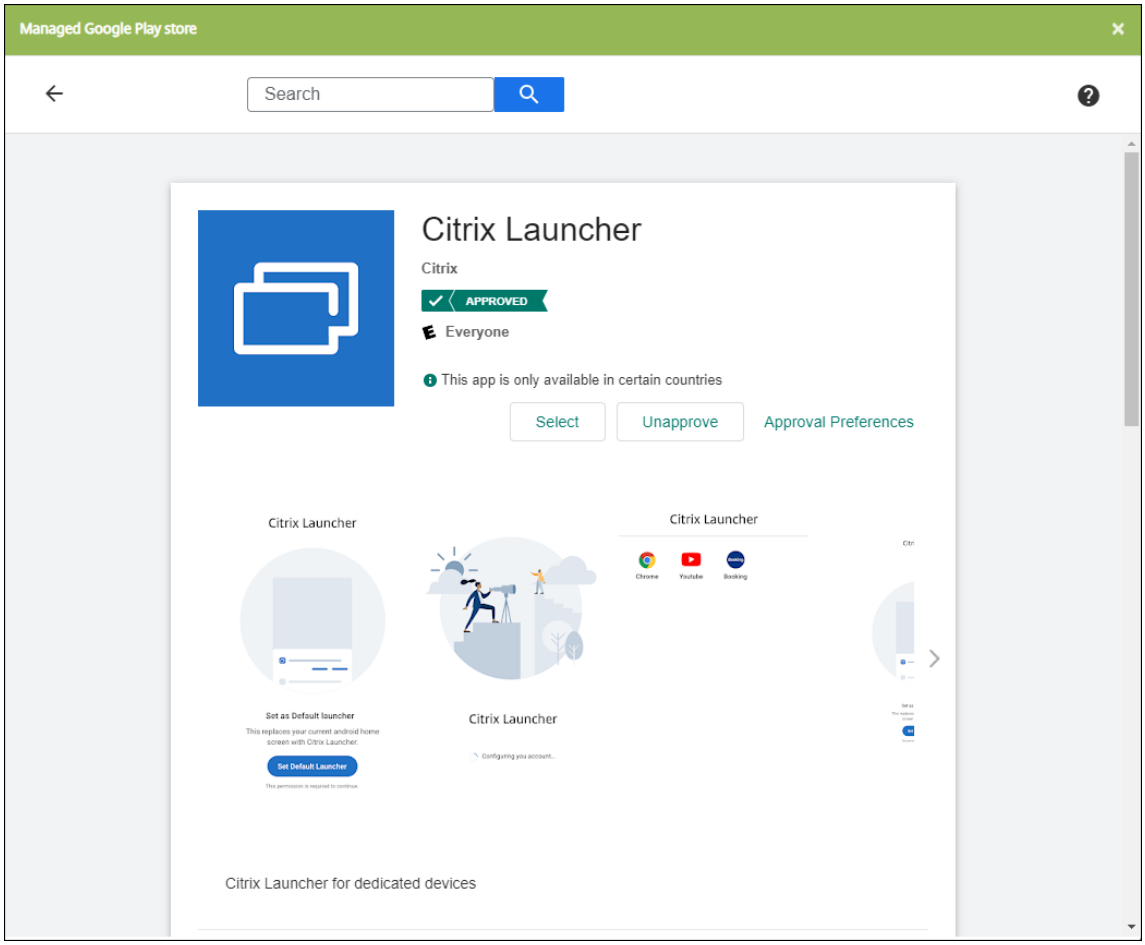
Mit einer **Launcher-Konfigurationsrichtlinie** steuern Sie folgende Citrix Launcher-Features:

- Verwalten von Android Enterprise-Geräten und Android-Legacygeräten, sodass Benutzer nur auf von Ihnen festgelegte Apps zugreifen können
- Optionale Angabe eines benutzerdefinierten Logos als Citrix Launcher-Symbol sowie eines benutzerdefinierten Hintergrundbilds für Citrix Launcher
- Festlegen eines Kennworts, das Benutzer zum Beenden von Launcher eingeben müssen

Citrix Launcher ist nicht als zusätzliche Sicherheitsstufe gedacht.

Einrichten von Citrix Launcher für Android Enterprise-Geräte

1. Fügen Sie die Citrix Launcher-App (com.citrix.launcher.droid) als App aus dem öffentlichen App-Store zu Citrix Endpoint Management hinzu. Klicken Sie unter **Konfigurieren > Apps** auf **Hinzufügen** und dann auf **Öffentlicher App-Store**. Weitere Informationen finden Sie unter Hinzufügen von Apps aus einem öffentlichen App-Store.



2. Geben Sie in der Kioskgeräterichtlinie an, welche Apps auf unternehmenseigenen Geräten zur dedizierten Nutzung verfügbar sein müssen (auch bekannt als unternehmenseigene Android-Einzweckgeräte (COSU)). Gehen Sie zu **Konfigurieren > Geräterichtlinien**, klicken Sie auf **Hinzufügen**und wählen Sie **Kiosk**. Wählen Sie die Citrix Launcher-App und alle weiteren Apps in der Positivliste aus. Wenn Sie zuvor Apps zur Liste hinzugefügt haben, müssen Sie die Apps nicht erneut hochladen. Weitere Informationen finden Sie unter Android Enterprise-Einstellungen.

3. Fügen Sie die Launcher-Konfigurationsrichtlinie hinzu. Gehen Sie zu **Konfigurieren > Geräterichtlinien**, klicken Sie auf **Hinzufügen** und wählen Sie **Launcher-Konfiguration**. Fügen Sie in der Launcher-Konfigurationsrichtlinie beliebige Apps hinzu, die Sie in der Kiosk-Richtlinie angegeben haben. Sie müssen nicht alle Apps hinzufügen, die Sie in der Kiosk-Richtlinie angegeben haben. Sie müssen die Citrix Launcher-App nur in der Kiosk-Richtlinie hinzufügen. Weitere Informationen finden Sie unter Launcher-Konfigurationsrichtlinie.

4. Erstellen Sie eine Bereitstellungsgruppe und stellen Sie Ressourcen bereit. Weitere Informationen hierzu finden Sie weiter unten unter Bereitstellungsgruppe hinzufügen und Ressourcen bereitstellen.

Nachdem Sie Citrix Launcher auf unternehmenseigenen Android Enterprise-Geräten zur dedizierten Verwendung bereitgestellt haben, installiert Citrix Endpoint Management die App und ersetzt den standardmäßigen Citrix Secure Hub-Launcher. Wenn Sie die Citrix Launcher-App beenden, wird Citrix Secure Hub wieder zum Standardlauncher.

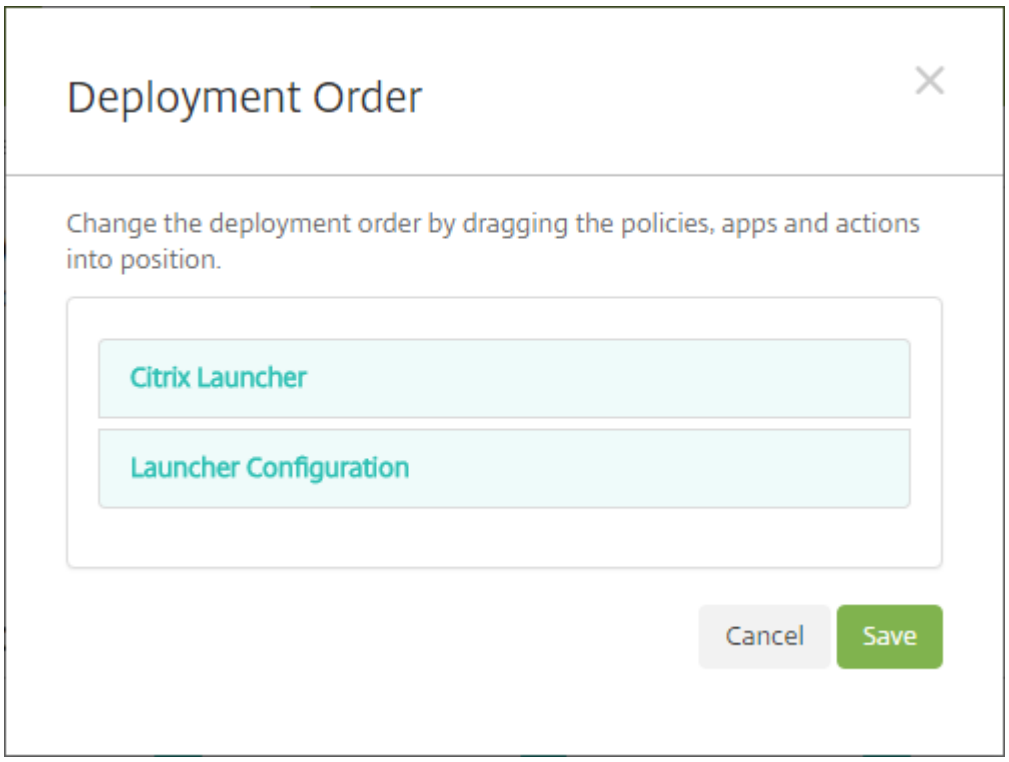
Einrichten von Citrix Launcher für Android-Legacygeräte

> **Hinweis:**
>
> Seit August 2020 wird CitrixLauncher.apk von Citrix für Android-Legacygeräte nicht mehr unterstützt. Sie können die veraltete Citrix Launcher-App (com.citrix.launcher) weiterhin für Android-Geräte verwenden, erhalten jedoch keine neuen Featureupdates.

1. Für den Download der Citrix Launcher-App gehen Sie zur Downloadseite für Citrix Endpoint Management und suchen **Citrix Launcher**. Laden Sie die neueste Datei herunter. Die Datei kann ohne Umschließen in Citrix Endpoint Management hochgeladen werden.
2. Fügen Sie die Launcher-Konfigurationsrichtlinie hinzu. Gehen Sie zu **Konfigurieren > Geräterichtlinien**, klicken Sie auf **Hinzufügen** und wählen Sie **Launcher-Konfiguration**. Weitere Informationen finden Sie unter Launcher-Konfigurationsrichtlinie.
3. Fügen Sie die Citrix Launcher-App als Unternehmensapp zu Citrix Endpoint Management hinzu. Klicken Sie unter **Konfigurieren > Apps** auf **Hinzufügen** und dann auf **Unternehmensanwendungen**. Weitere Informationen finden Sie unter Hinzufügen einer Unternehmensapp.
4. Erstellen Sie eine Bereitstellungsgruppe und stellen Sie Ressourcen bereit. Weitere Informationen hierzu finden Sie weiter unten unter Bereitstellungsgruppe hinzufügen und Ressourcen bereitstellen.

Bereitstellungsgruppe hinzufügen und Ressourcen bereitstellen

1. Erstellen Sie über **Konfigurieren > Bereitstellungsgruppen** eine Bereitstellungsgruppe für Citrix Launcher mit der folgenden Konfiguration:
   - Fügen Sie auf der Seite **Richtlinien** eine **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.



2. Stellen Sie Ressourcen für eine Bereitstellungsgruppe bereit, indem Sie eine Pushbenachrichtigung an alle Benutzer in der Bereitstellungsgruppe senden. Weitere Informationen zum Hinzufügen von Ressourcen zu einer Bereitstellungsgruppe finden Sie unter Ressourcen bereitstellen.

Verwalten von Geräten ohne Citrix Launcher

Anstelle von Citrix Launcher können Sie auch bereits vorhandene Funktionen verwenden.

Provisioning dedizierter Geräte:

1. Erstellen Sie ein Registrierungsprofil, indem Sie den **Gerätebesitzermodus** auf **Dediziertes Gerät** einstellen. Siehe Provisioning von dedizierten Android Enterprise-Geräten und Registrierungsprofile.
2. Erstellen Sie eine Kioskgeräterichtlinie, um Apps zur Positivliste hinzuzufügen und den LockTask-Modus festzulegen. Wenn Sie zuvor Apps zur Liste hinzugefügt haben, müssen Sie die Apps nicht erneut hochladen. Weitere Informationen finden Sie unter Android Enterprise-Einstellungen.
3. Registrieren Sie jedes Gerät im erstellten Registrierungsprofil.

Apps mit Apple Volume Purchase hinzufügen

June 25, 2024

Mit Apple Business Manager (ABM) und Apple School Manager (ASM) können Sie Volumenlizenzen für Apps und Bücher erwerben und zugehörige Informationen mit Citrix Endpoint Management synchronisieren. Die Apps und Bücher können Sie dann mit Citrix Endpoint Management auf iOS- und macOS-Geräten bereitstellen. Der Volumenkauf von Inhalten erleichtert Organisationen die Suche, den Erwerb und das Verteilen von Apps und Büchern.

Weitere Informationen zum Erwerb von Inhalten mit ABM oder ASM finden Sie im Apple Business Manager-Benutzerhandbuch oder im Apple School Manager-Benutzerhandbuch. In diesem Artikel wird beschrieben, wie Sie die per Volume Purchase erworbenen Lizenzen zwischen ABM bzw. ASM und Citrix Endpoint Management synchronisieren und die Lizenzen verwalten.

> **Hinweis:**
>
> Das Apple-Programm für Volumenlizenzen (VPP) ist ab 14. Januar 2021 nicht mehr verfügbar. Die Volume Purchase-Funktion wurde in ABM und ASM integriert. Wenn Sie derzeit VPP oder das Programm zur Geräteregistrierung (DEP) verwenden, können Sie ein Upgrade auf ABM oder ASM durchführen. Weitere Informationen finden Sie in der Apple-Dokumentation unter Upgrade from Apple Deployment Programs.

Info zu Apple Volume Purchase

Beachten Sie Folgendes beim Volumenkauf von Inhalten mit ABM oder ASM:

- Sie können Lizenzen für folgende Inhalte erwerben:
  - Öffentliche Apps und Bücher
  - Benutzerdefinierte Apps, die speziell für Ihre Organisation entwickelt wurden
- Sie können per Volume Purchase erworbene Apps und Bücher auf organisationseigenen Geräten und auf Privatgeräten (BYOD) bereitstellen. Organisationseigene Geräte, die über ABM oder ASM registriert sind, unterstützen die MDM- oder MDM+MAM-Registrierung, jedoch nicht die MAM-Registrierung.
- Weitere Informationen zum Verteilen von Apps finden Sie unter Verteilen von Apple-Apps.
- Eine Liste bekannter Probleme finden Sie im Knowledge Center-Artikel CTX222633.

Volume Purchase-Konto hinzufügen

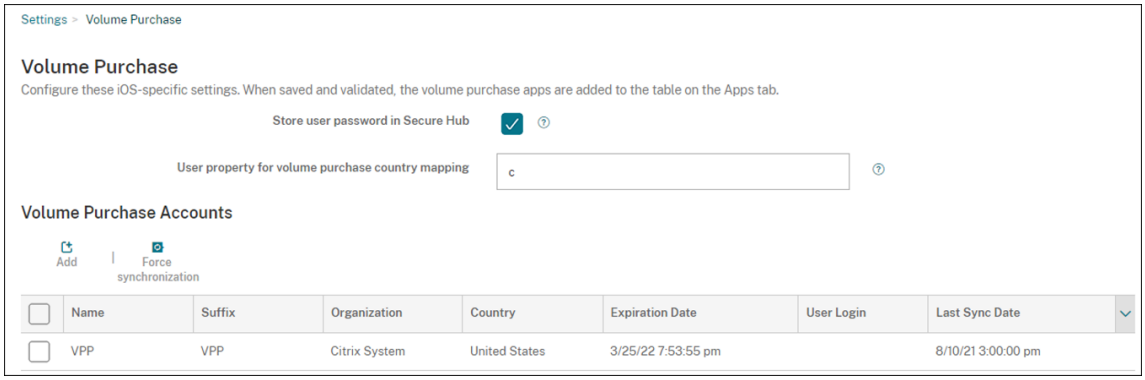
Nach dem Erwerb von Inhalten im ABM- oder ASM-Portal laden Sie den Inhaltstoken für Citrix Endpoint Management aus dem Portal herunter. Erstellen Sie dann in Citrix Endpoint Management ein

Volume Purchase-Konto, das auf diesem Inhaltscode basiert. Mit diesem Code kann Citrix Endpoint Management Inhaltslizenzen aus ABM oder ASM synchronisieren.

Mit Volume Purchase können Sie Inhalte erwerben und mit verwalteten Lizenzen auf Geräten bereitstellen. Wenn Sie bislang Einlösungscodes verwenden und auf verwaltete Lizenzen umstellen möchten, lesen Sie dieses Apple-Supportdokument.

Hinzufügen eines Volume Purchase-Kontos in Citrix Endpoint Management

1. Erwerben Sie die gewünschten Inhalte im ABM- oder ASM-Portal, laden Sie die Inhaltscodedatei herunter und speichern Sie sie an einem sicheren Ort.
2. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
3. Klicken Sie auf **Volume Purchase**. Die Konfigurationsseite **Volume Purchase** wird angezeigt.

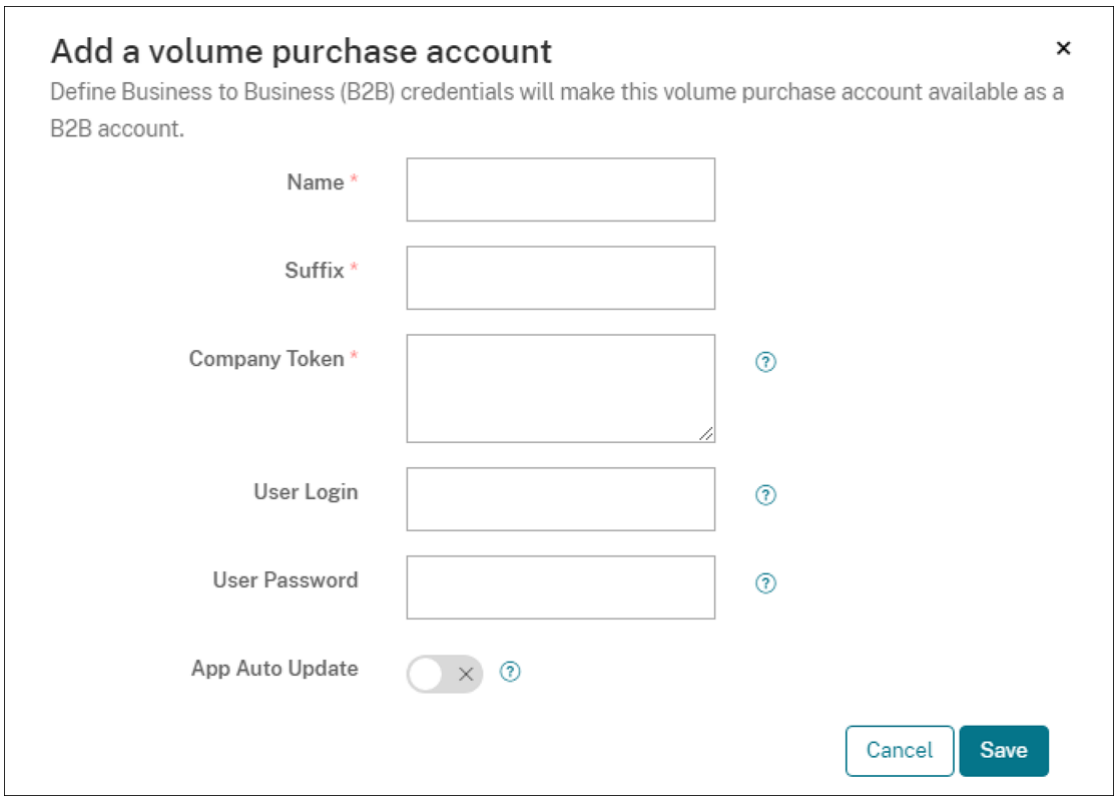


4. Konfigurieren Sie die folgenden Einstellungen:

   - **Benutzerkennwort in Citrix Secure Hub speichern:** Wählen Sie aus, ob ein Benutzername mit Kennwort in Citrix Secure Hub für die Citrix Endpoint Management-Authentifizierung gespeichert werden soll. Die Standardeinstellung ist **Ein**.
   - **Benutzereigenschaft für Volume Purchase-Länderzuordnung:** Geben Sie einen Länderzuweisungscode ein, um das Herunterladen aus dem landesspezifischen App-Store zuzulassen. Sie erhalten diesen Code bei Ihrem Content Manager.

     Der Länderzuweisungscode wird von Citrix Endpoint Management zur Auswahl des Eigenschaftenpools von Volume Purchase verwendet. Mit der Benutzereigenschaft “United States”können Benutzer beispielsweise keine Apps mit dem Zuweisungscode für Deutschland herunterladen.

5. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Volume Purchase-Konto hinzufügen** wird angezeigt.



6. Konfigurieren Sie die folgenden Kontoeinstellungen:

> **Hinweis:**
>
> Wenn Sie Apple Configurator 1 verwenden, laden Sie eine Lizenzdatei wie folgt hoch: Klicken Sie auf **Konfigurieren > Apps**, rufen Sie die Plattformseite einer App auf und erweitern Sie **Volume Purchase**.

- **Name:** Geben Sie einen aussagekräftigen Namen für das Konto ein.
- **Suffix:** Geben Sie das Suffix ein, das mit den Namen von Apps aus den Apple Stores angezeigt werden soll. Beispiel: Bei Eingabe von **VP** wird die App **Citrix Secure Mail** in der App-Liste als **Citrix Secure Mail – VP** angezeigt.
- **Unternehmenstoken:** Kopieren Sie den in Schritt 1 heruntergeladenen Inhaltstoken und fügen Sie ihn hier ein.
- **Benutzeranmeldung:** (Optional) Geben Sie einen Benutzernamen für den Administrator dieses Volume Purchase-Kontos ein. Wenn konfiguriert, sind Benutzername und Kennwort erforderlich, um per Volume Purchase erworbene, benutzerdefinierte Apps in Citrix Endpoint Management zu synchronisieren.
- **Benutzerkennwort:** (Optional) Geben Sie ein Kennwort für den von Ihnen eingegebenen Benutzernamen ein.
- **Automatische App-Updates:** Wird für diese Einstellung **Ein** festgelegt, werden per Volume Purchase erworbene Apps und optionale Apps in der Citrix Endpoint Management-Konsole automatisch aktualisiert, sobald eine neue Version verfügbar ist. Unternehmen-

sapps und Apps aus dem öffentlichen App-Store müssen Sie nach wie vor manuell in der Citrix Endpoint Management-Konsole aktualisieren. Bei der Einstellung **Aus** können Sie eine per Volume Purchase erworbene App in der Citrix Endpoint Management-Konsole weiterhin manuell aktualisieren. Sobald eine App in der Konsole aktualisiert wird, erhalten Geräte mit installierter App das Update ebenfalls. Die Standardeinstellung ist **Aus**.

Nachdem das Volume Purchase-Konto erfolgreich hinzugefügt wurde, werden Sie in einer Meldung über Folgendes informiert:

- Auf der Seite **Konfigurieren > Apps** werden die per Volume Purchase erworbenen Apps in der App-Liste angezeigt. Die App-Namen werden mit dem von Ihnen konfigurierten Suffix angezeigt.
- Erworbene Bücher werden auf der Seite **Konfigurieren > Medien** in der Medienliste angezeigt. Die Buchnamen werden mit dem von Ihnen konfigurierten Suffix angezeigt.

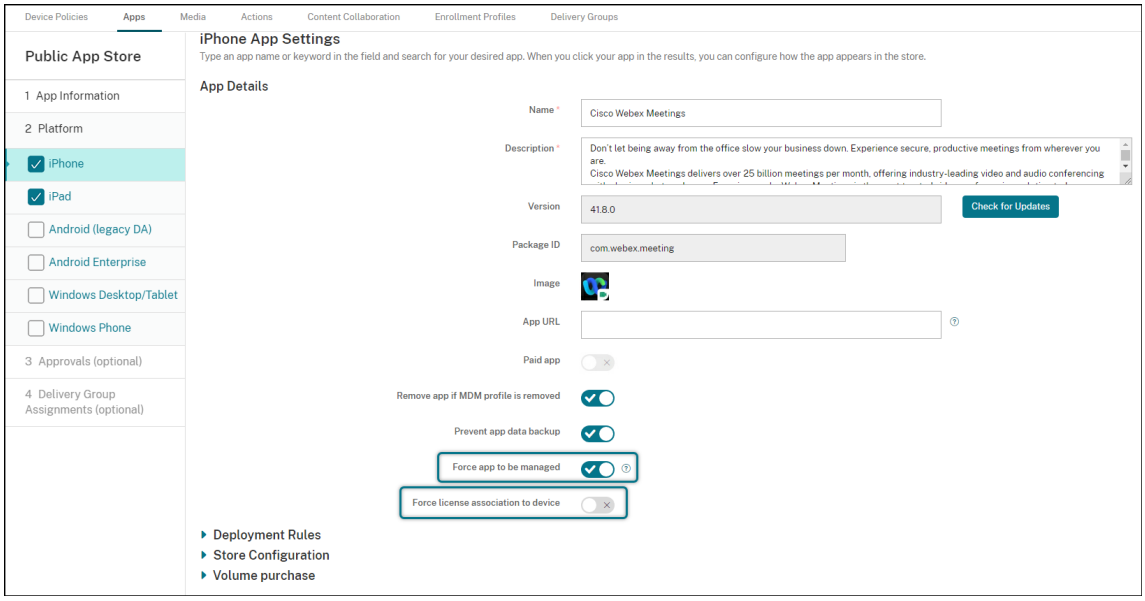
Konfigurieren von per Volume Purchase erworbenen Apps

Nach dem Hinzufügen eines Volume Purchase-Kontos werden die App-Informationen mit Citrix Endpoint Management synchronisiert und auf der Seite **Konfigurieren > Apps** angezeigt. Sie können diese Apps nun konfigurieren, die Bereitstellungsgruppe festlegen und Richtlinieneinstellungen für iOS- und macOS-Geräte anpassen. Wenn Sie die Konfiguration abgeschlossen haben, können Benutzer ihre Geräte registrieren.

Beachten Sie beim Konfigurieren einer mit Volume Purchase erworbenen App die folgenden Einstellungen:

- Auf der Seite **Konfigurieren > Apps**:
  - Damit Citrix Endpoint Management eine App nicht für einen Benutzer, sondern für ein Gerät bereitstellt, aktivieren Sie **Lizenzzuordnung zu Gerät erzwingen**. Wenn diese Einstellung aktiviert ist, müssen Benutzer ihre Apple-ID nicht verwenden und können Apps ohne Anmeldung bei ihrem App Store-Konto herunterladen.
  - Wir empfehlen, für Apps die Option **Verwaltung der App erzwingen** zu aktivieren, damit sie automatisch als verwaltete App installiert werden.

> **Hinweis:**
>
> Damit die Einstellung **Verwaltung der App erzwingen** wirksam wird, müssen Sie die Servereigenschaft `apple.app.force.managed` auf der Seite **Einstellungen > Eigenschaften** auf **True** setzen. Weitere Informationen finden Sie unter Servereigenschaften.



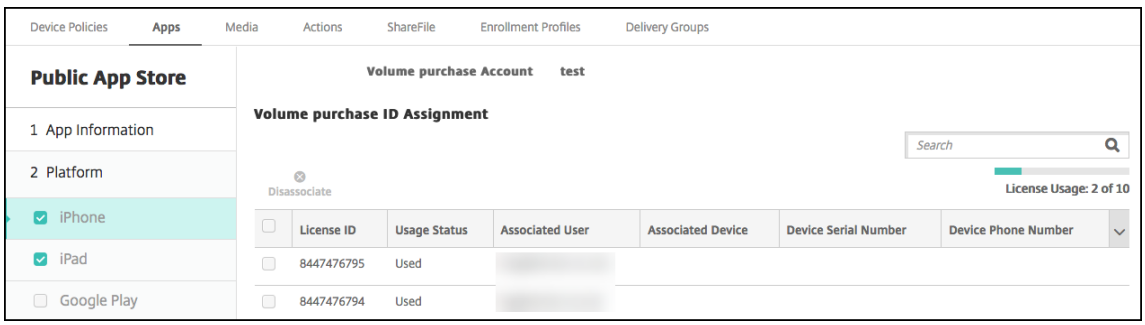
- Auf der Seite **Konfigurieren > Bereitstellungsgruppe**:

  Um die App automatisch bzw. mit minimaler Benutzerinteraktion auf Benutzergeräten zu installieren, rufen Sie die Seite **Apps** auf und ziehen die App in die Liste **Erforderliche Apps**. Standardmäßig sind Apps mit Ausnahme von Citrix Secure Hub **optionale Apps**, d. h. Benutzer müssen die App-Installation manuell über Citrix Secure Hub starten.

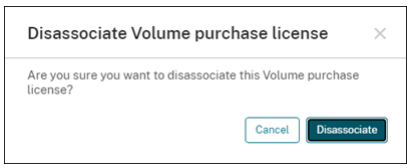
Nachverfolgung und Verwaltung der Verwendung von App-Lizenzen

Sie können die Lizenznutzung für eine App verfolgen und eine verwendete Lizenz bei Bedarf zurücknehmen und einem anderen Benutzer oder Gerät zuweisen.

1. Klicken Sie auf **Konfigurieren > Apps**.
2. Wählen Sie eine App aus und klicken Sie auf **Bearbeiten**.
3. Rufen Sie die Seite **Plattform** auf und erweitern Sie **Volume Purchase**.
   In der Tabelle **Volume Purchase-ID-Zuweisung** können Sie verfolgen, wie viele Lizenzen verwendet werden und von welchem Benutzer oder Gerät.



4. Um eine Lizenz zurückzunehmen, wählen Sie die Lizenz aus und klicken auf **Zuordnung aufheben**.

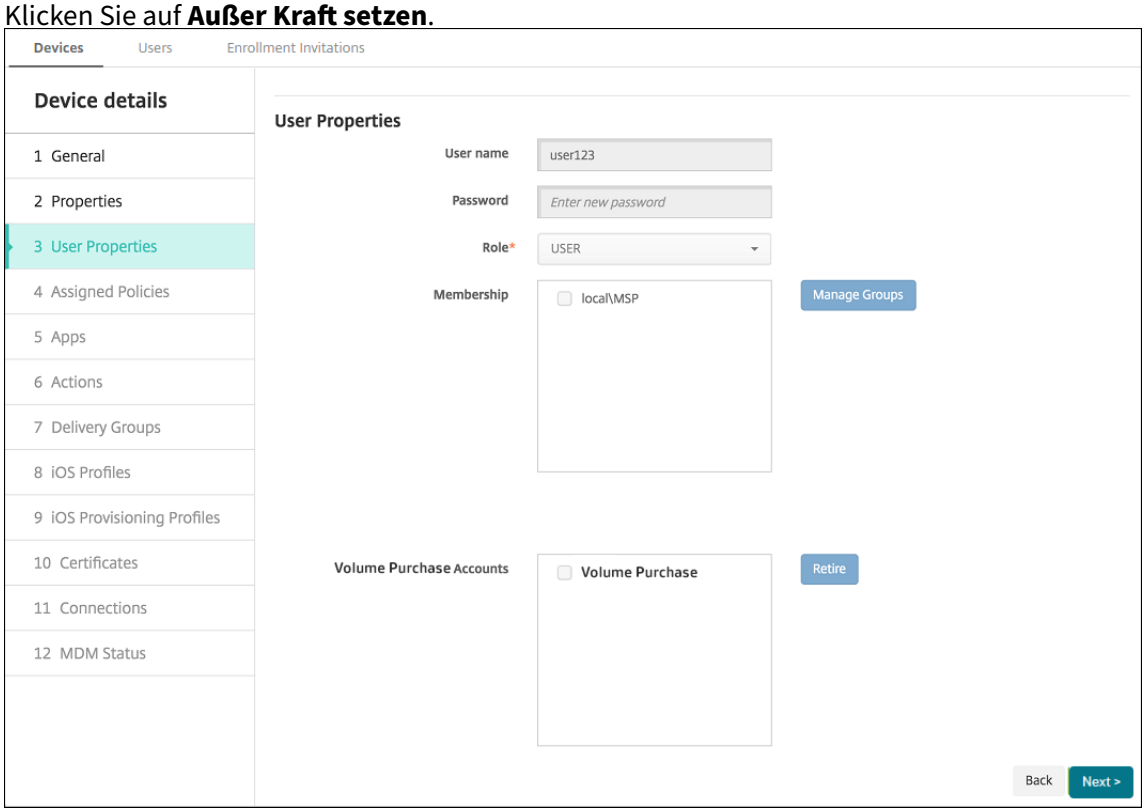


5. Klicken Sie auf **Zuordnung aufheben**, um die Aktion zu bestätigen.

Entfernen eines Benutzers aus einem Volume Purchase-Konto

Sie können Benutzer, denen Sie App-Lizenzen zugewiesen haben, auch aus Volume Purchase-Konten entfernen, um alle zugewiesenen Lizenzen zurückzunehmen. Ein Anwendungsfall hierfür könnte sein, wenn ein Benutzer Ihre Organisation verlässt.

1. Klicken Sie auf **Verwalten > Geräte**.
2. Wählen Sie das Gerät aus, das zu dem Zielbenutzer gehört und klicken Sie auf **Bearbeiten**.
3. Rufen Sie die Seite **Benutzereigenschaften** auf und wählen Sie die benötigten Volume Purchase-Konten aus.
4. Klicken Sie auf **Außer Kraft setzen**.



Citrix Endpoint Management widerruft die App-Lizenzen in den ausgewählten Volume Purchase-Konten für den Benutzer.

Synchronisieren der App-Informationen

Citrix Endpoint Management synchronisiert in regelmäßigen Abständen die App-Informationen mit ABM oder ASM. Bei Bedarf können Sie die App-Informationen auch manuell synchronisieren. Stellen Sie bei der Synchronisierung sicher, dass die App-Lizenzen und andere App-Informationen alle Änderungen enthalten. Eine Änderung kann das manuelle Löschen einer App aus dem Volume Purchase-Konto sein.

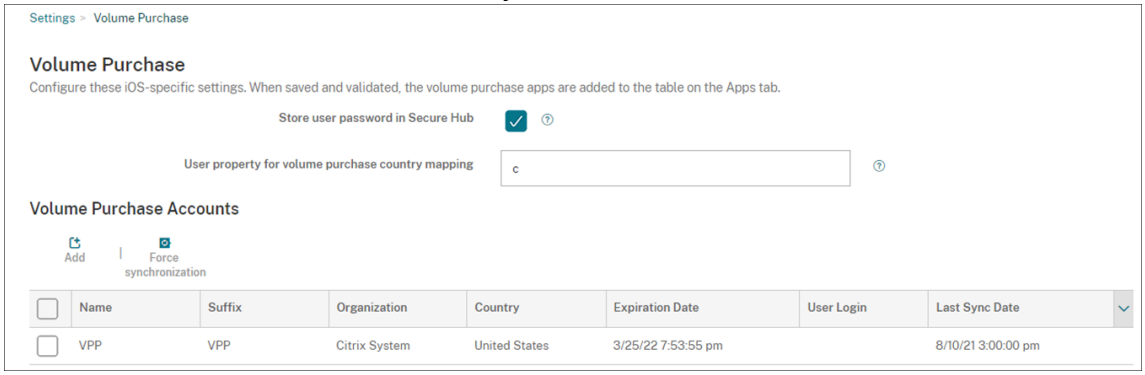
Ändern des Standardsynchronisierungsintervalls

Standardmäßig aktualisiert Citrix Endpoint Management die Volume Purchase-Lizenzbasis mindestens alle 1440 Minuten (24 Stunden). Ein Citrix Cloud-Administrator kann das Standardintervall über die Servereigenschaft `vpp.baseline` ändern. Weitere Informationen finden Sie unter Servereigenschaften.

Manuelles Synchronisieren der App-Informationen

Sie können eine Synchronisierung mit ABM oder ASM erzwingen, um sofort die neuesten App-Informationen abzurufen.

1. Klicken Sie auf **Einstellungen > Volume Purchase**.
2. Wählen Sie ein Volume Purchase-Konto aus und klicken Sie auf **Synchronisierung erzwingen**. Oder klicken Sie auf **Synchronisierung erzwingen**, ohne ein Volume Purchase-Konto auszuwählen. Dann werden alle Konten synchronisiert.



3. Bestätigen Sie die Synchronisierungsaktion. Die Synchronisierung wird gestartet.

   Die Synchronisierung kann je nach Anzahl der Volume Purchase-Lizenzen mehrere Minuten dauern. Nach Abschluss der Synchronisierung lädt Citrix Endpoint Management die Seite **Volume Purchase** neu und aktualisiert Datum und Uhrzeit der Synchronisierung in der neuen Spalte **Zuletzt synchronisiert**.

Suche nach App-Updates

Wenn Sie beim Hinzufügen eines Volume Purchase-Kontos die Einstellung **Automatische App-Updates** aktivieren, sucht Citrix Endpoint Management regelmäßig nach neuen Versionen für per Volume Purchase erworbene Apps und optionale Apps und führt Aktualisierungen durch. Bei Bedarf können Sie manuell nach der neuen Version für eine beliebige App suchen und die App-Updates auf Citrix Endpoint Management anwenden.

Sobald Citrix Endpoint Management für eine erforderliche App eine neue Version erhält, wird diese automatisch zur Installation an Geräte übertragen, ohne dass Benutzer eine Aufforderung erhalten.

Suchen und Anwenden einer neuen App-Version

1. Klicken Sie auf **Konfigurieren > Apps**. Die Seite **Apps** wird angezeigt.
2. Wählen Sie eine App aus und klicken Sie auf **Bearbeiten**.
3. Rufen Sie die Seite **Plattform** auf und klicken Sie neben **Version** auf **Nach Updates suchen**.
4. Wenden Sie das Update im Dialogfeld **Update** an, wenn eine neue Version verfügbar ist.

Erneuern des Inhaltstokens für Ihr Volume Purchase-Konto

Inhaltstoken laufen nach einem Jahr ab. Kurz vor Ablauf des Tokens zeigt Citrix Endpoint Management eine Lizenzablaufwarnung an. Erneuern Sie den Inhaltstoken rechtzeitig, um Unterbrechungen für Benutzer zu vermeiden.

1. Laden Sie vom ABM- oder ASM-Portal einen aktuellen Token herunter.
2. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
3. Klicken Sie auf **Volume Purchase**. Die Konfigurationsseite Volume Purchase wird angezeigt.
4. Geben Sie in Ihrem Volume Purchase-Konto die aktualisierten Tokeninformationen ein.

ShareFile über Citrix Endpoint Management verwenden

March 11, 2024

Citrix Endpoint Management bietet zwei Optionen für die Integration in ShareFile. Diese sind Citrix Files und Speicherzonenconnectors.

Citrix Files

Sie können Citrix Endpoint Management so konfigurieren, dass Sie auf Ihr ShareFile-Konto zugreifen können. Diese Konfiguration:

- Bietet mobilen Benutzern Zugriff auf alle ShareFile-Features, wie Dateifreigabe, Dateisynchronisierung und Speicherzonenconnectors.
- Kann Citrix Files mit Single Sign-On-Authentifizierung von Benutzern mobiler Produktivitätsapps und mit umfassenden Zugriffssteuerungsrichtlinien bereitstellen.
- Bietet ShareFile-Konfiguration, Servicelevel- und Lizenznutzungsüberwachung über die Citrix Endpoint Management-Konsole.

Weitere Informationen zur Konfiguration von Citrix Endpoint Management für Enterprise-Konten finden Sie unter SAML für Single Sign-On mit Citrix Files.

Speicherzonenconnectors

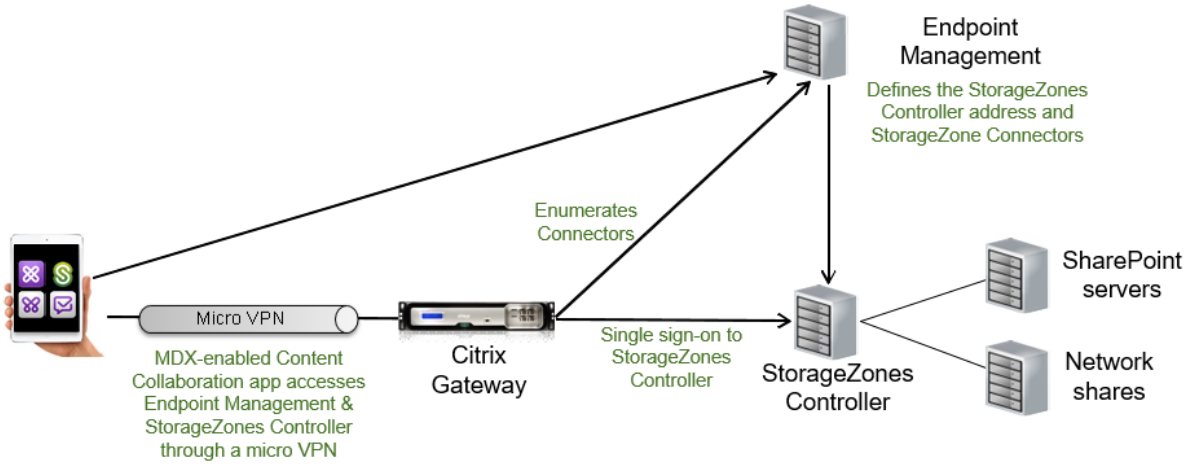
Sie können Citrix Endpoint Management so konfigurieren, dass der Zugriff nur auf die Speicherzonenconnectors limitiert wird, die Sie über die Citrix Endpoint Management-Konsole erstellen. Diese Konfiguration:

- Bietet sicheren mobilen Zugriff auf vorhandene lokale Speicherrepositorys, wie SharePoint-Sites und Netzwerkdateifreigaben.
- Erfordert nicht, dass Sie eine ShareFile-Unterdomäne einrichten oder Citrix Files-Daten hosten.
- Bietet Benutzern mobilen Zugriff auf Daten über die mobilen Produktivitätsapps von Citrix für Citrix Files 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.
- Ermöglicht das einfache Einrichten von Speicherzonenconnectors über die Citrix Endpoint Management-Konsole. Wenn Sie zu einem späteren Zeitpunkt alle Citrix Files-Funktionen mit Citrix Endpoint Management verwenden möchten, können Sie die Konfiguration in der Citrix Endpoint Management-Konsole ändern.

Bei einer ausschließlichen Integration von Citrix Endpoint Management mit Speicherzonenconnectors gilt:

- ShareFile nutzt die Konfiguration mit Single Sign-On bei NetScaler Gateway zur Authentifizierung mit Speicherzonencontrollern.
- Citrix Endpoint Management authentifiziert nicht über SAML, da die Citrix Files-Steuerungsebene nicht verwendet wird.

Das folgende Diagramm zeigt die allgemeine Architektur für die Verwendung von Citrix Endpoint Management mit Speicherzonenconnectors.



Anforderungen

- Mindestversionen der Komponenten:
  - ShareFile für iOS (MDX) 5.3
  - ShareFile für Android (MDX) 5.3
  - Speicherzonencontroller 5.11.20
    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 Citrix Endpoint Management mit Speicherzonenconnectors.

Citrix Endpoint Management 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 Schritte gelten für die ausschließliche Integration von Citrix End-

point Management mit Speicherzonenconnectors: Einige dieser Artikel sind in der Dokumentation für den Speicherzonencontroller aufgeführt.

1. Konfigurieren von NetScaler für Speicherzonencontroller

   Sie können NetScaler Gateway 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. Speicherzonencontroller installieren

5. Speicherzonencontroller für die ausschließliche Verwendung mit Speicherzonenconnector vorbereiten

6. Proxyserver für Speicherzonen festlegen

   Über die Konsole des Speicherzonencontrollers können Sie einen Proxyserver für den 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. Sekundären Speicherzonencontroller mit einer Speicherzone verbinden

   Konfigurieren Sie eine Speicherzone mit hoher Verfügbarkeit durch Einbinden von mindestens zwei Speicherzonencontrollers.

Speicherzonencontroller installieren

1. Führen Sie Download und Installation der Speicherzonencontroller-Software durch:

   a) Melden Sie sich auf der Citrix Files-Downloadseite unter https://www.citrix.com/downloads/sharefile.html an und laden Sie die aktuelle Version des Speicherzonencontroller-Installationsprogramms herunter.

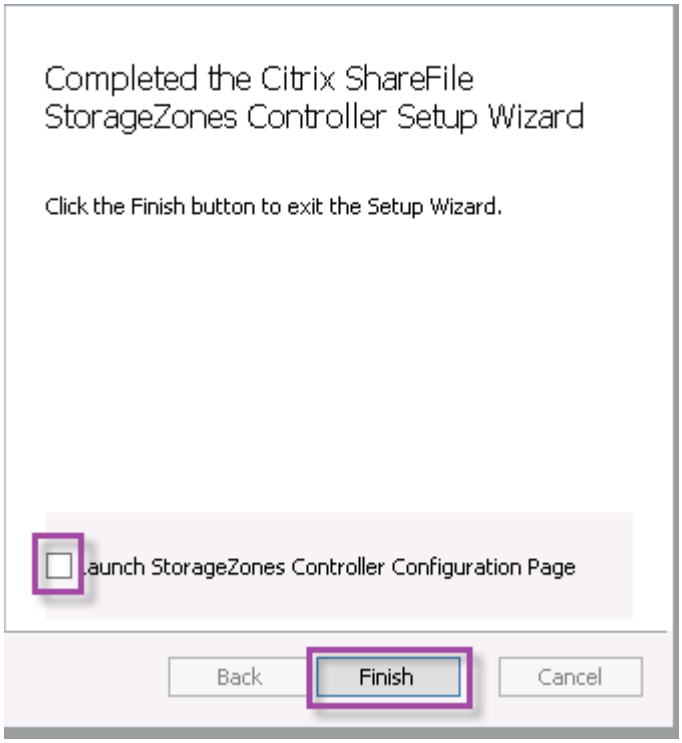
   b) Durch Installation des Speicherzonencontrollers wechselt die Standardwebsite des Servers zum Installationspfad des Controllers. Aktivieren Sie **Anonyme Authentifizierung** auf der Standardwebsite.

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. (Wenn Sie einen Zertifikatfehler erhalten, erwägen Sie, die Verbindung mit HTTP herzustellen.) Wenn die Installation erfolgreich ist, wird das Citrix Files-Logo angezeigt.

   Wird das Citrix Files-Logo nicht angezeigt, löschen Sie den Browsercache und versuchen es noch einmal.

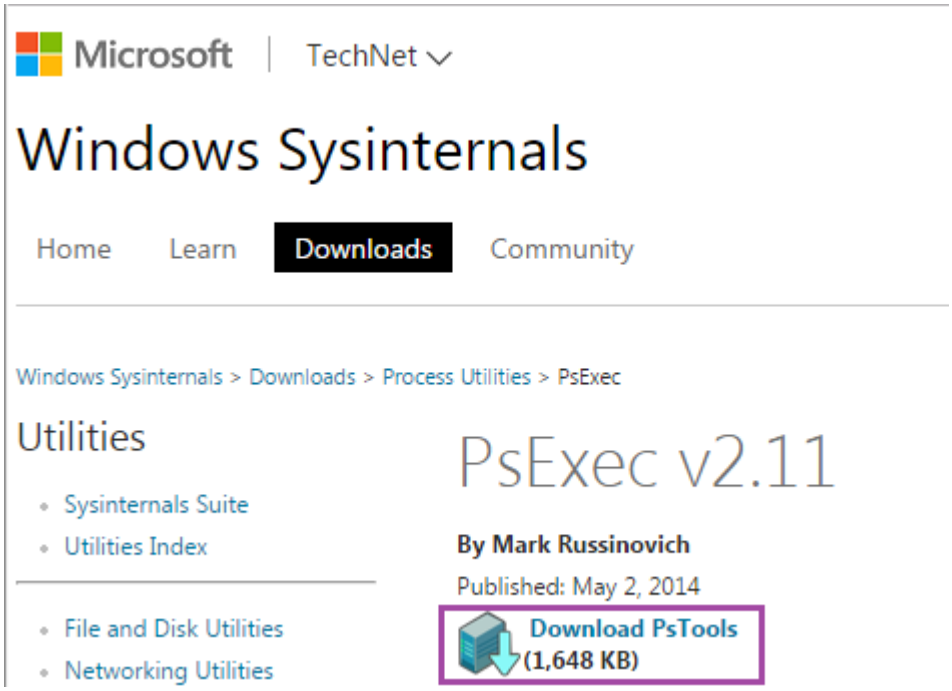
   > **Wichtig:**
   >
   > Wenn Sie den Speicherzonencontroller klonen möchten, erstellen Sie zunächst ein Datenträgerimage, bevor Sie mit der Konfiguration des Speicherzonencontrollers fortfahren.

Speicherzonencontroller für die ausschließliche Verwendung mit Speicherzonenconnector vorbereiten

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:

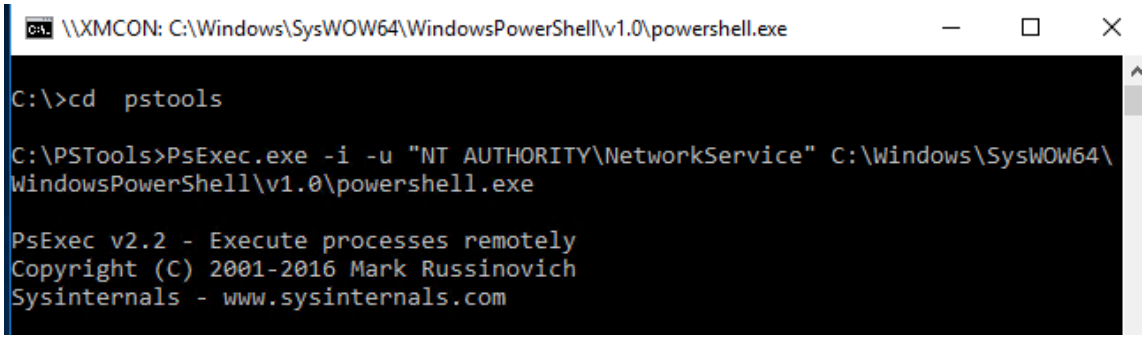
- Registrieren des aktuellen Speicherzonencontrollers als primären Speicherzonencontroller. Sie können später einen sekundären Speicherzonencontroller zum primären Controller hinzufügen.
- Erstellen einer Zone und Festlegen der Passphrase.

1. Laden Sie vom Speicherzonencontroller-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.

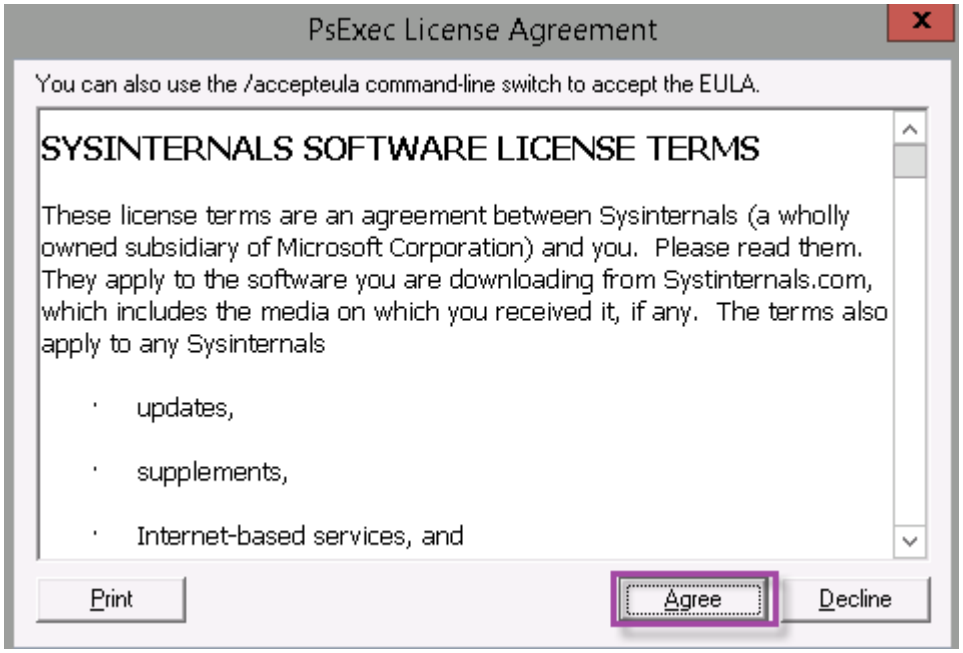


2. Führen Sie das Tool PsExec aus: Öffnen Sie die Eingabeaufforderung als Administrator und geben Sie Folgendes ein:

```
1 ```
2 cd c:\pstools
3 PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
     \WindowsPowerShell\v1.0\powershell.exe
4 <!--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:

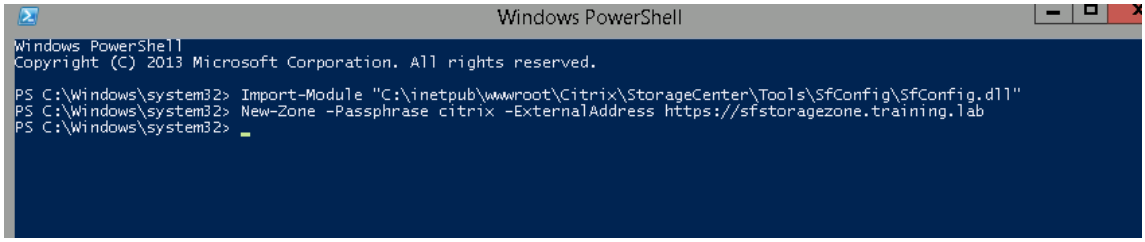
```
1 ```
2 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
     SfConfig\SfConfig.dll"
3 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
     com
4 <!--NeedCopy--> ```
```

Ort:

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 Citrix Endpoint Management anmelden, um Speicherzonenconnectors zu erstellen:

Proxyserver für Speicherzonen festlegen

Konfiguration des Domänencontrollers, sodass er dem Speicherzonencontroller für die Delegierung vertraut

Sekundären Speicherzonencontroller mit einer Speicherzone verbinden

Informationen zum Erstellen von Speicherzonenconnectoren finden Sie unter Definieren von Speicherzonencontroller-Verbindungen in Citrix Endpoint Management.

Sekundären Speicherzonencontroller mit einer Speicherzone verbinden

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
   >
   ```

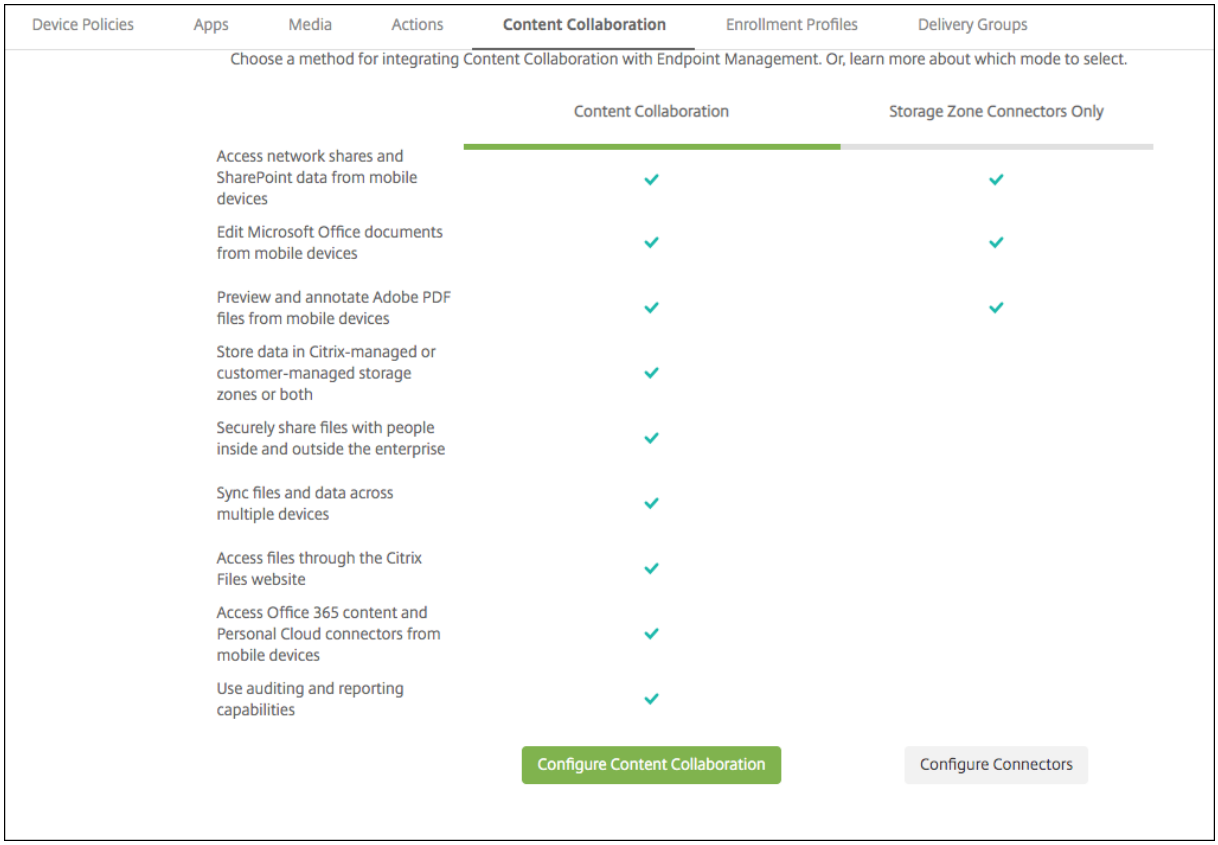
   Beispiel:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

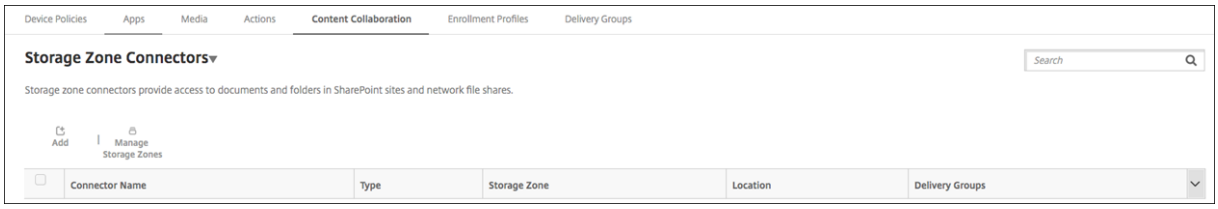

Definieren von Speicherzonencontroller-Verbindungen in Citrix Endpoint Management

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.

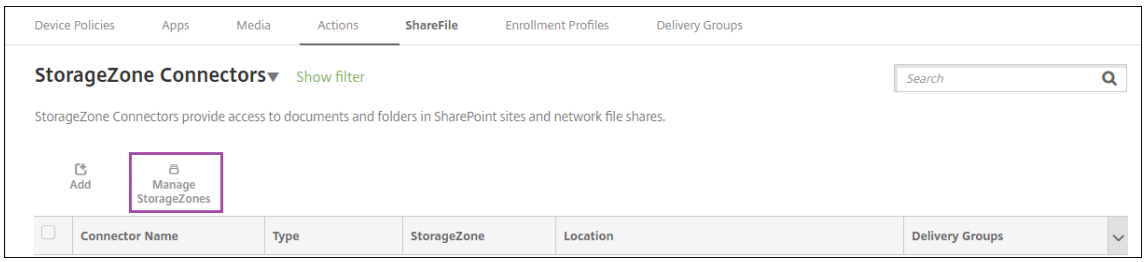
Beim ersten Aufrufen der Seite **Konfigurieren > ShareFile** werden dort die Unterschiede zwischen der Verwendung von Citrix Endpoint Management mit Enterprise-Konten und Speicherzonenconnectors erläutert.



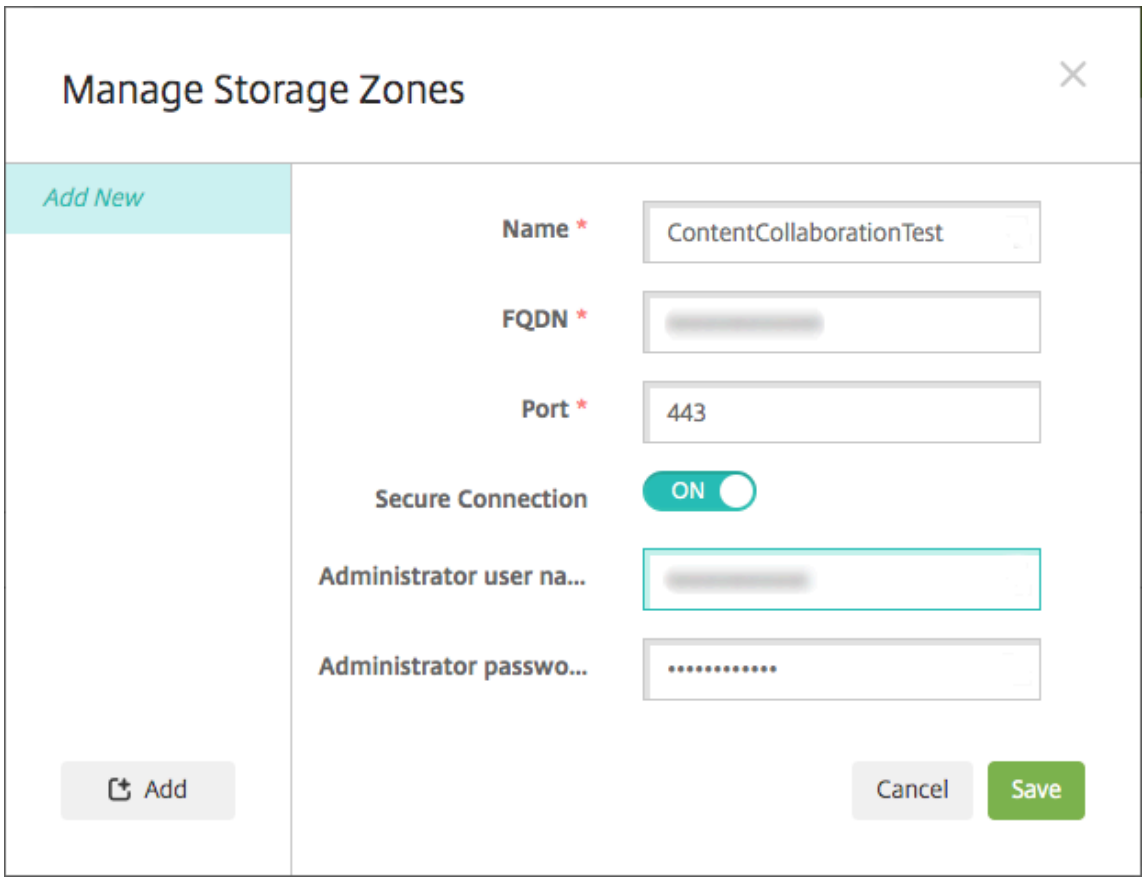
Klicken Sie auf **Connectors konfigurieren**, um mit den Konfigurationsschritten in diesem Artikel fortzufahren.



1. Klicken Sie unter **Konfigurieren > ShareFile** auf **Speicherzonen verwalten**.



2. Fügen Sie unter **Speicherzonen verwalten** die Verbindungsinformationen hinzu.



- **Name:** Aussagekräftiger Name für die Speicherzone, der zur Erkennung der Speicherzone in Citrix Endpoint Management dient. Verwenden Sie kein Leerzeichen oder Sonderzeichen im Namen.
- **FQDN und Port:** Der vollqualifizierte Domänenname und die Portnummer für den Speicherzonencontroller, der vom Citrix Endpoint Management-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

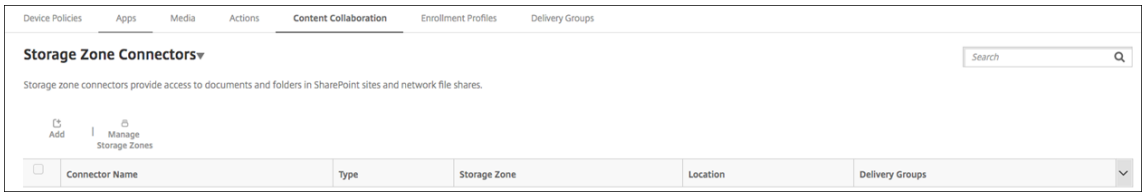
verwenden.

3. Klicken Sie auf **Speichern**.
4. Zum Testen der Verbindung stellen Sie sicher, dass der Citrix Endpoint Management-Server den vollqualifizierten Domänennamen des Speicherzonencontrollers auf Port 443 erreichen kann.
5. Klicken Sie zum Definieren einer weiteren Speicherzonencontroller-Verbindung unter **Speicherzonen verwalten** auf die Schaltfläche **Hinzufügen**.

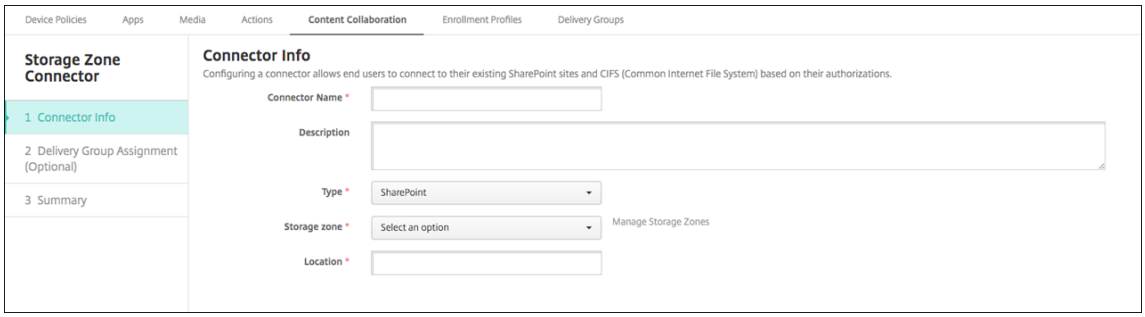
   Zum Bearbeiten oder Löschen der Informationen für eine Speicherzonencontroller-Verbindung wählen Sie den Verbindungsnamen in **Speicherzonen verwalten** aus. Klicken Sie auf **Bearbeiten** oder **Löschen**.

Hinzufügen eines Speicherzonenconnectors in Citrix Endpoint Management

1. Gehen Sie zu **Konfigurieren > ShareFile** und klicken Sie dann auf **Hinzufügen**.



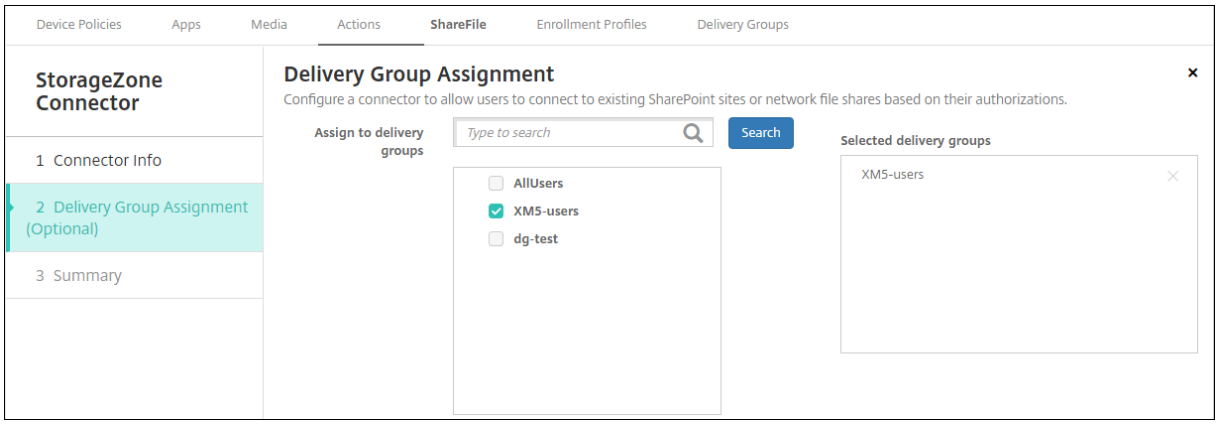
2. Konfigurieren Sie auf der Seite **Connectorinfo** die folgenden Einstellungen:



   - **Connectorname:** Name, der den Speicherzonenconnector in Citrix Endpoint Management bezeichnet.
   - **Beschreibung:** optionale Anmerkungen zu diesem Connector.
   - **Typ:** Wählen Sie entweder **SharePoint** oder **Netzwerk** aus.
   - **Speicherzone:** Wählen Sie die mit diesem Connector verbundene Speicherzone aus. Wenn die Speicherzone nicht aufgeführt wird, klicken Sie auf **Speicherzonen 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:

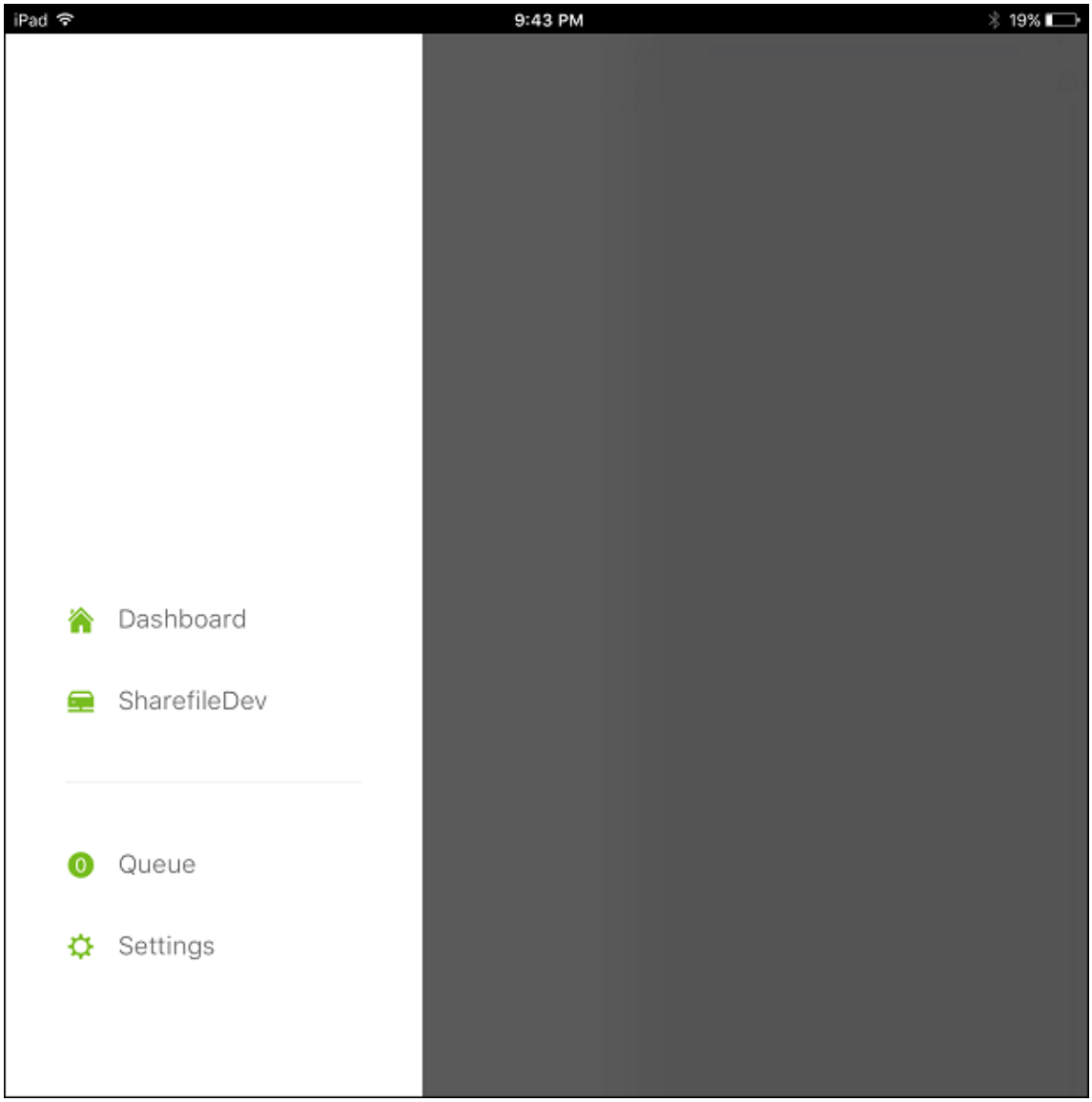
   a) Wenn Sie die Citrix Files-Clients umschließen , legen Sie die Netzwerkzugriffsrichtlinie auf **Tunneled - Web SSO** fest.

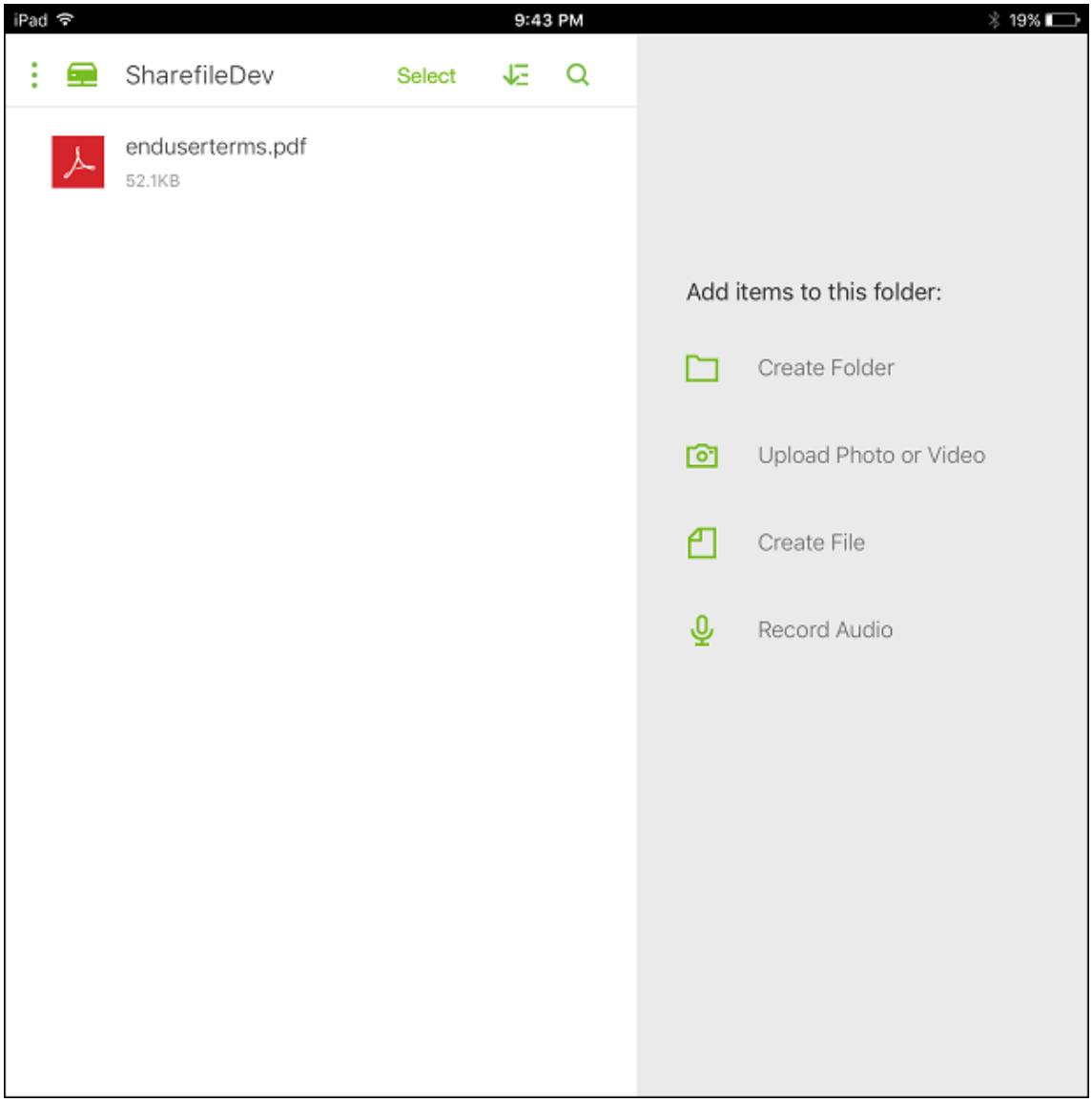
   In diesem Tunnelmodus beendet das MDX Framework den SSL/HTTP-Datenverkehr von einer MDX-App und startet für den Benutzer neue Verbindungen zu internen Verbindungen. Mit dieser Einstellung kann das MDX Framework Authentifizierungsaufforderungen von Webservern erkennen und darauf reagieren.

   b) Fügen Sie die Citrix Files-Clients zu Citrix Endpoint Management hinzu. Weitere Informationen finden Sie unter Hinzufügen von Citrix Files-Clients zu Citrix Endpoint Management.

   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.

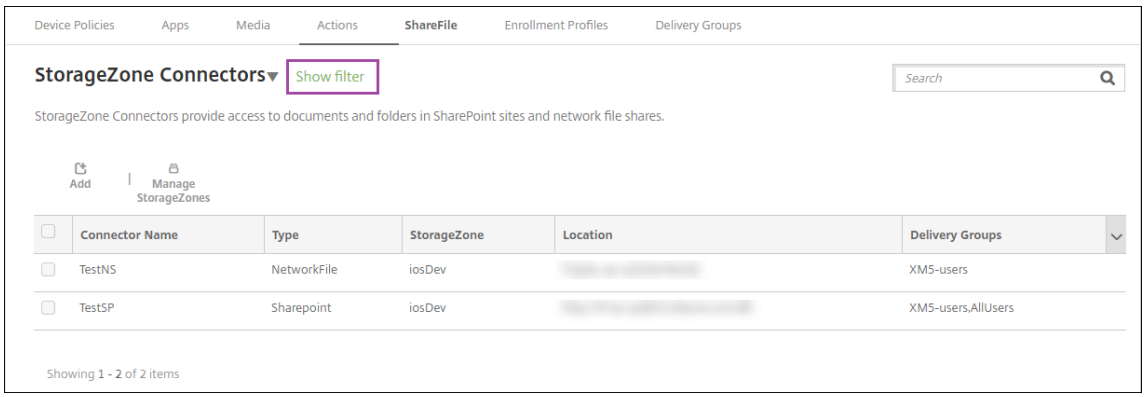




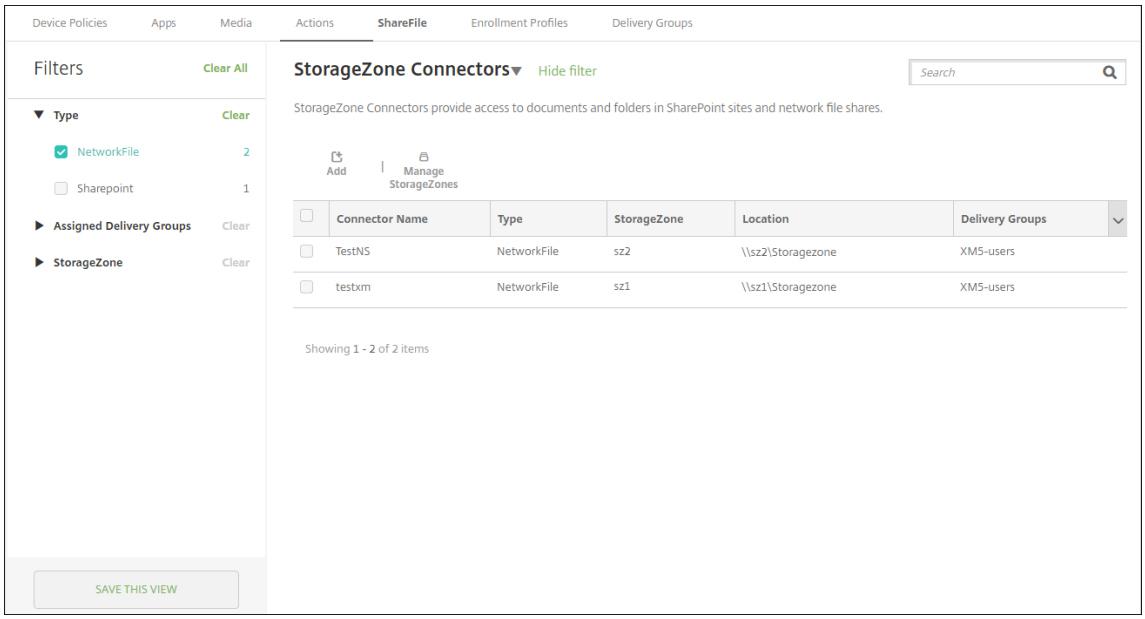
Filtern der Speicherzonenconnectors-Liste

Sie können die Liste der Speicherzonenconnectors nach Connector-Typ, zugewiesenen Bereitstellungsgruppen und Speicherzone filtern.

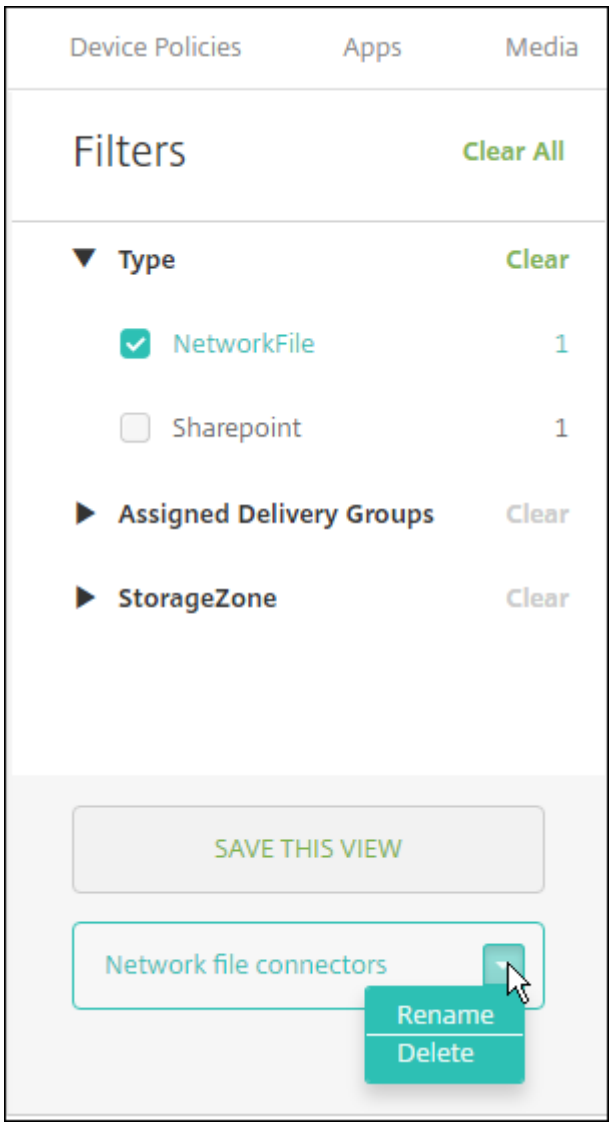
1. Wechseln Sie zu **Konfigurieren > ShareFile** und klicken Sie dann auf **Filter einblenden**.



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**.



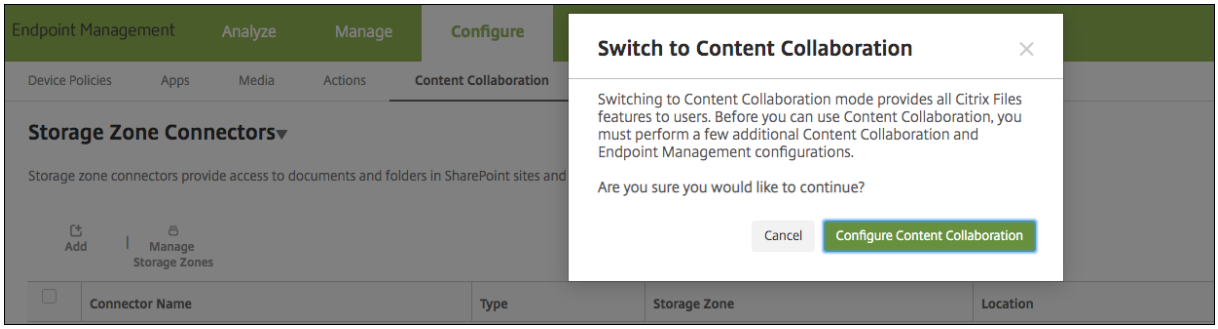
3. Klicken Sie zum Umbenennen oder Löschen eines Filters auf das Pfeilsymbol neben dem Filternamen.



Zum Enterprise-Konto wechseln

Nach der Integration von Speicherzonenconnectors mit Citrix Endpoint Management können Sie später zum gesamten Enterprise-Featuresatz wechseln. Citrix Endpoint Management behält die vorhandenen Integrationseinstellungen für den Speicherzonenconnector bei.

Wechseln Sie zu **Konfigurieren > ShareFile**, klicken Sie auf das Dropdownmenü **Speicherzonenonnectors** und klicken Sie dann auf **ShareFile konfigurieren**.



Informationen zur Konfiguration von Enterprise-Konten finden Sie unter SAML für Single Sign-On mit Citrix Files.

SmartAccess für HDX-Apps

March 11, 2024

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 Citrix Virtual Apps and Desktops anhand einer SmartAccess-Richtlinie konfiguriert, die nicht richtlinientreuen Geräten den Zugriff verweigert. Citrix Endpoint Management übermittelt den Gerätestatus an StoreFront mit einem signierten verschlüsselten Tag. StoreFront gewährt oder verweigert dann den Zugriff entsprechend der Zugriffssteuerungsrichtlinie der App.

Für die Verwendung dieses Features muss die Bereitstellung folgende Komponenten umfassen:

- Citrix Virtual Apps and Desktops
- Citrix Endpoint Management
- Citrix Endpoint Management mit SAML-Zertifikat für das Signieren und Verschlüsseln von Tags. Das gleiche Zertifikat ohne privaten Schlüssel wird auf den StoreFront-Server hochgeladen.

Um diese Funktion verwenden zu können, gehen Sie wie folgt vor:

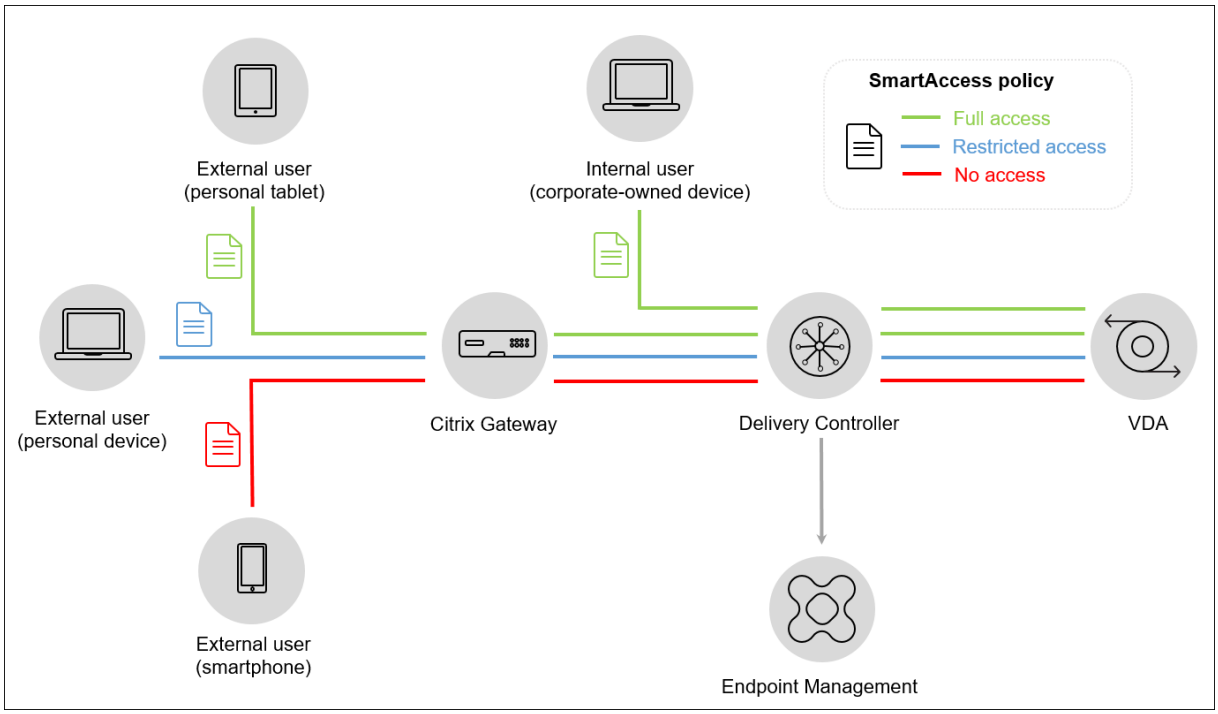
- Konfigurieren Sie das Citrix Endpoint Management-Serverzertifikat für den StoreFront-Store
- Konfigurieren Sie mindestens eine Citrix Virtual Apps and Desktops-Bereitstellungsgruppe mit der erforderlichen SmartAccess-Richtlinie
- Legen Sie die automatisierter Aktion in Citrix Endpoint Management fest

SmartAccess zu HDX-Apps für Endpunkte

Mit diesem Feature können Sie über eine richtlinienbasierte Zugriffssteuerung den Gerätezugriff auf HDX-Apps beschränken. Sie können auf HDX-Apps folgende Zugriffsebenen anwenden:

- **Vollzugriff**. Das Gerät kann auf alle HDX-Apps im Citrix Secure Hub-Store zugreifen.
- **Eingeschränkter Zugriff:** Das Gerät kann auf einige HDX-Apps zugreifen.
- **Kein Zugriff**. Das Gerät kann nicht auf HDX-Apps zugreifen.

Die folgende Grafik veranschaulicht die Funktionsweise der Zugriffssteuerung. Der Versuch, eine HDX-App in Citrix Secure Hub zu starten, löst eine Anforderung an einen Delivery Controller aus. Der Delivery Controller leitet die Anforderung zur Validierung an den Citrix Endpoint Management-Server weiter. Das Ergebnis der Validierung bestimmt, welchen Zugriff das Gerät erhält. Beispielsweise wird der Zugriff auf eine HDX-App verweigert, wenn ein Gerät einen Jailbreak aufweist.



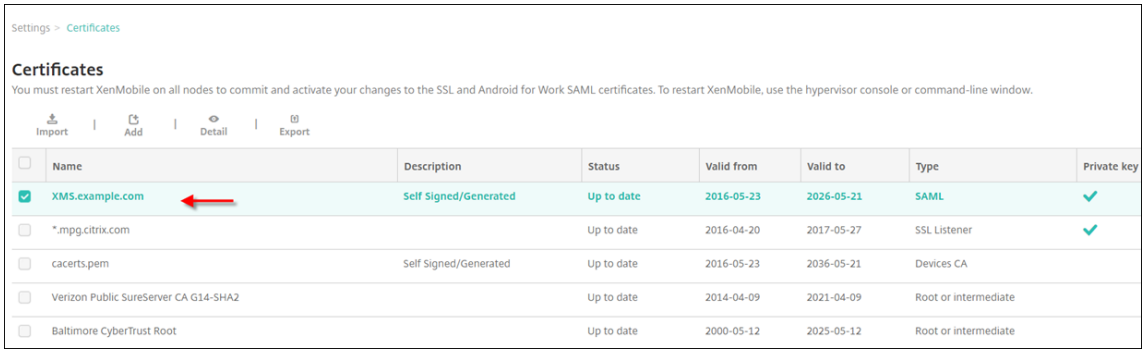
Exportieren und konfigurieren Sie das Citrix Endpoint Management-Serverzertifikat für den StoreFront-Store

SmartAccess verwendet signierte und verschlüsselte Tags für die Kommunikation zwischen Citrix Endpoint Management- und StoreFront-Servern. Um diese Kommunikation zu ermöglichen, fügen Sie das Citrix Endpoint Management-Serverzertifikat dem StoreFront-Store hinzu.

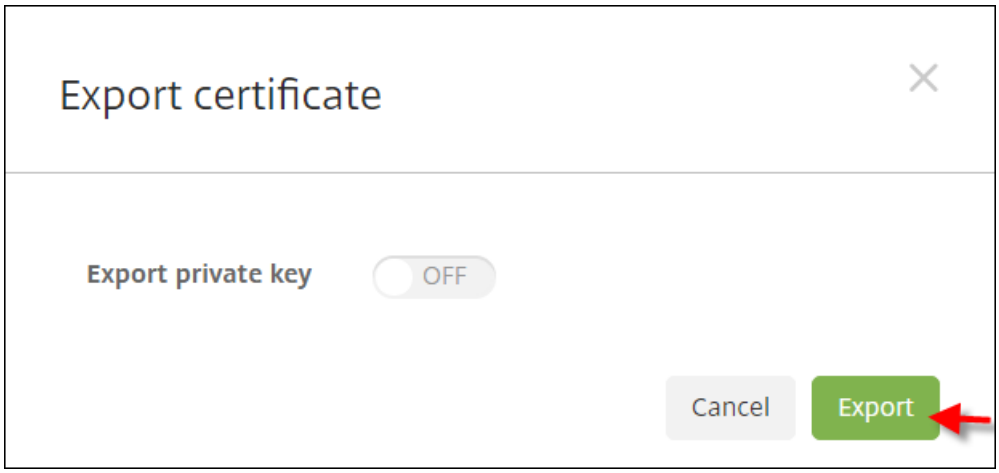
Weitere Informationen zur Integration von StoreFront in Citrix Endpoint Management, wenn für Citrix Endpoint Management die domänen- und zertifikatbasierte Authentifizierung konfiguriert ist, finden Sie im Support Knowledge Center.

Exportieren des SAML-Zertifikats von Citrix Endpoint Management

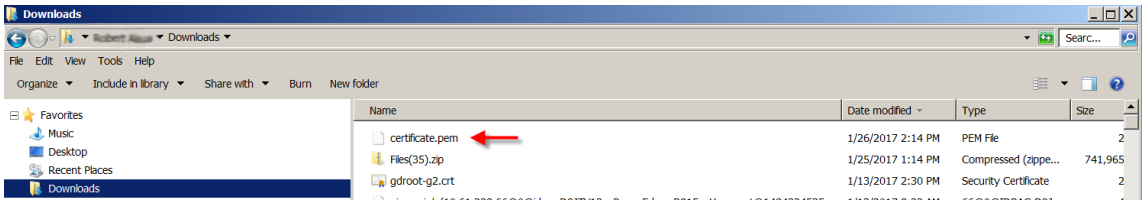
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt. Klicken Sie auf **Zertifikate**.
2. Suchen Sie das SAML-Zertifikat für den Citrix Endpoint Management-Server.



3. Vergewissern Sie sich, dass **Privaten Schlüssel exportieren** auf **Aus** festgelegt ist. Klicken Sie auf **Exportieren**, um das Zertifikat in das Downloadverzeichnis zu exportieren.

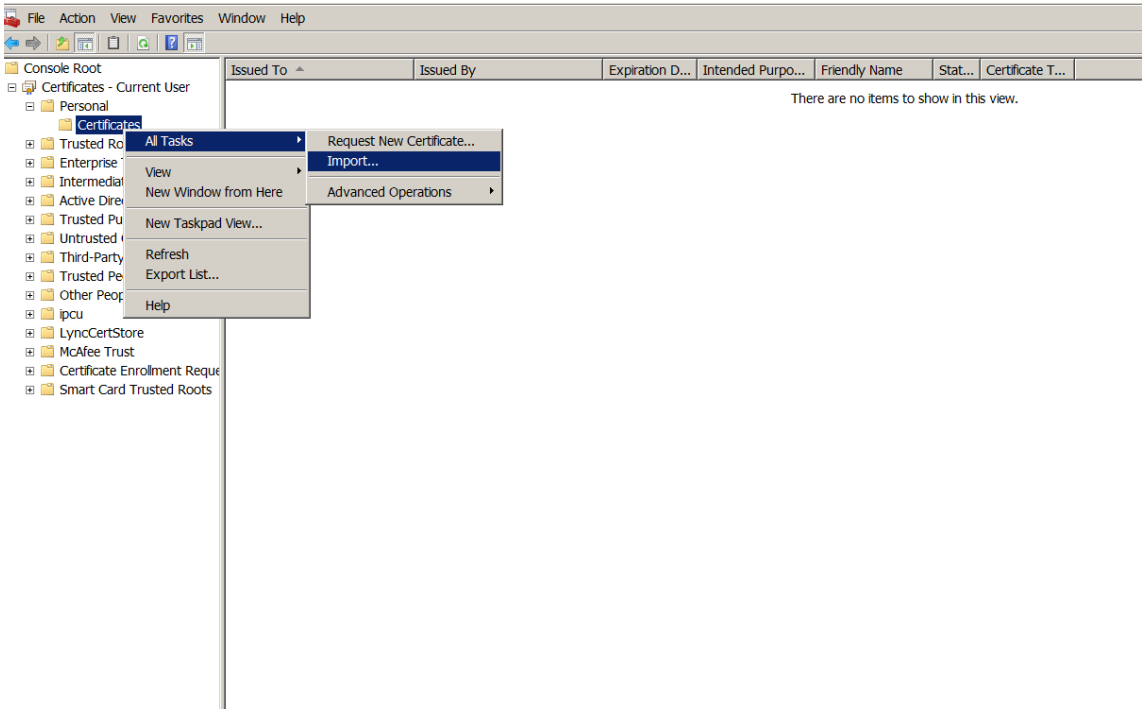


4. Suchen Sie das Zertifikat im Downloadverzeichnis. Das Zertifikat weist das PEM-Format auf.

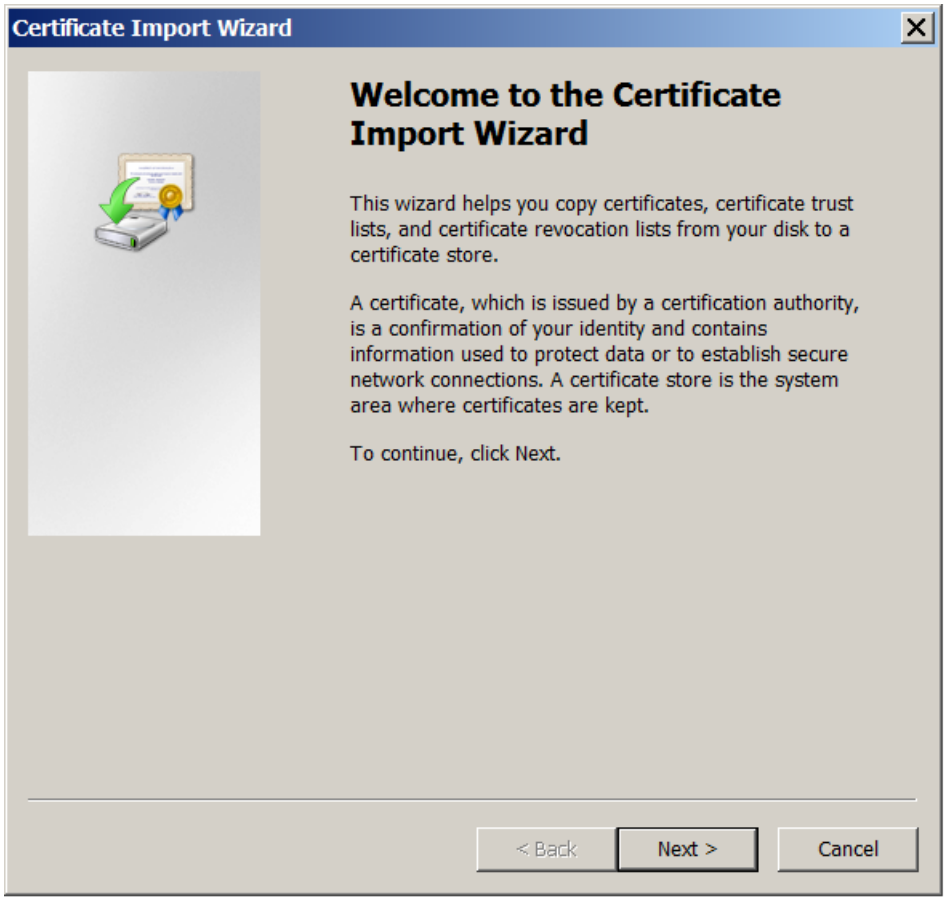


Konvertieren des Zertifikats von PEM in CER

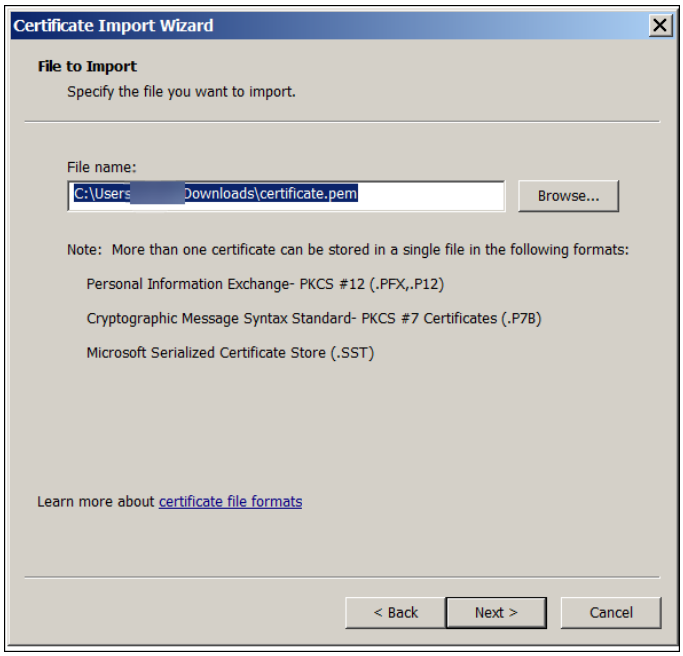
1. Öffnen Sie die Microsoft Management Console (MMC) und klicken Sie mit der rechten Maustaste auf **Zertifikate > Alle Aufgaben > Importieren**.



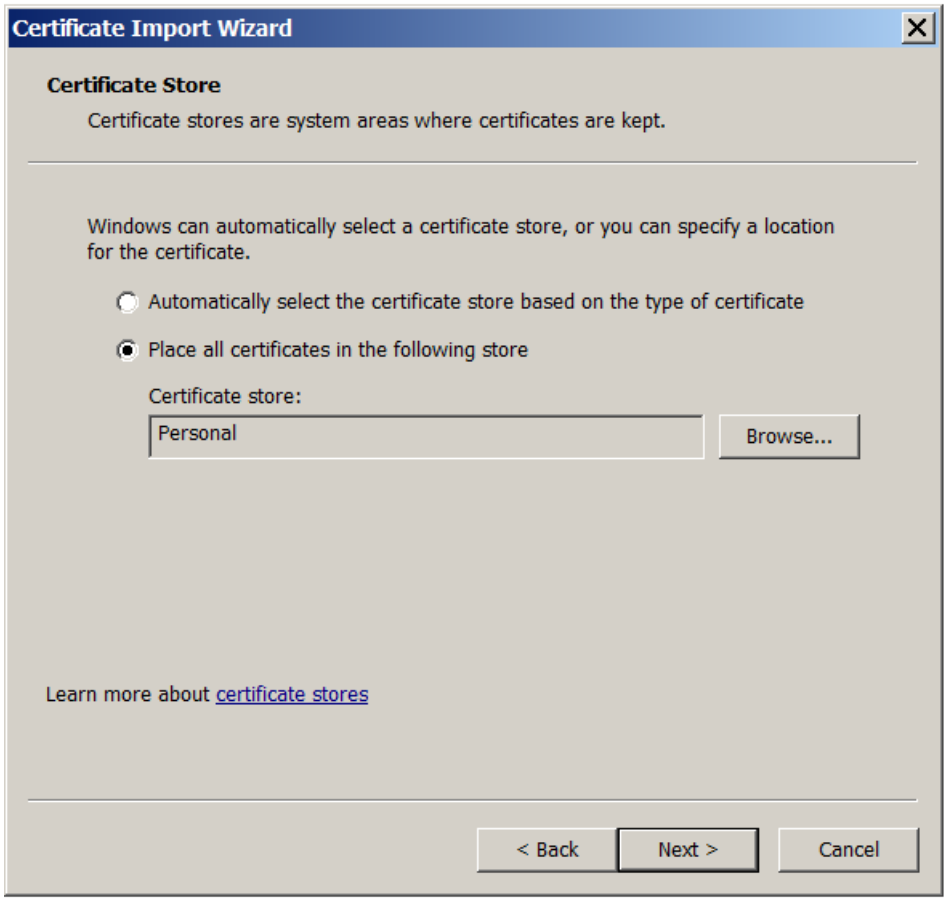
2. Wenn der Zertifikatimport-Assistent geöffnet wird, klicken Sie auf **Weiter**.



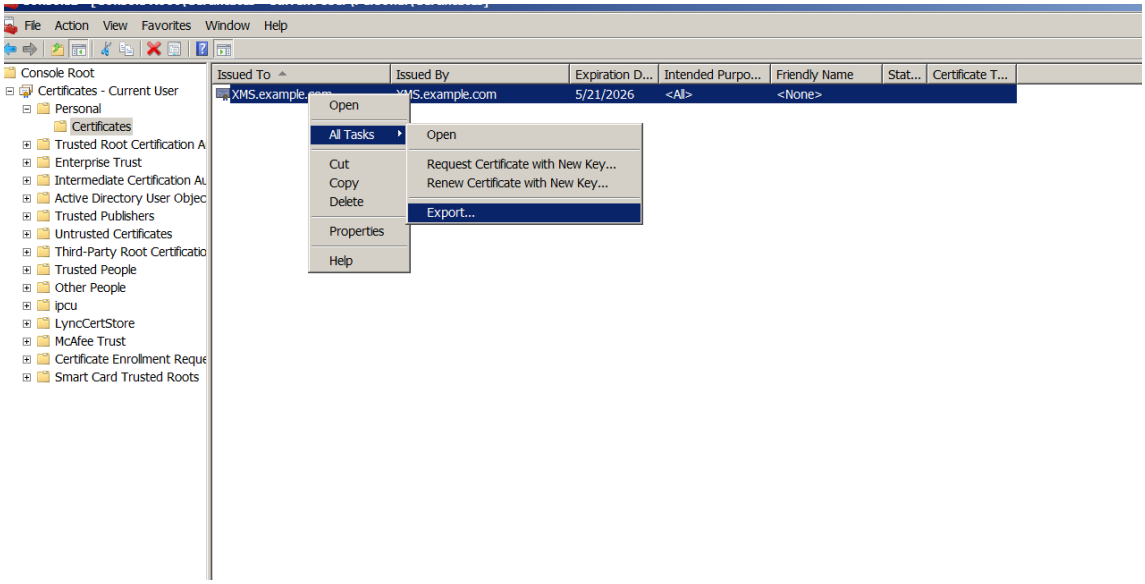
3. Navigieren Sie zum Zertifikat im Downloadverzeichnis.



4. Markieren Sie **Alle Zertifikate in folgendem Speicher speichern** und wählen Sie **Eigene Zertifikate** als Zertifikatspeicher. Klicken Sie auf **Weiter**.

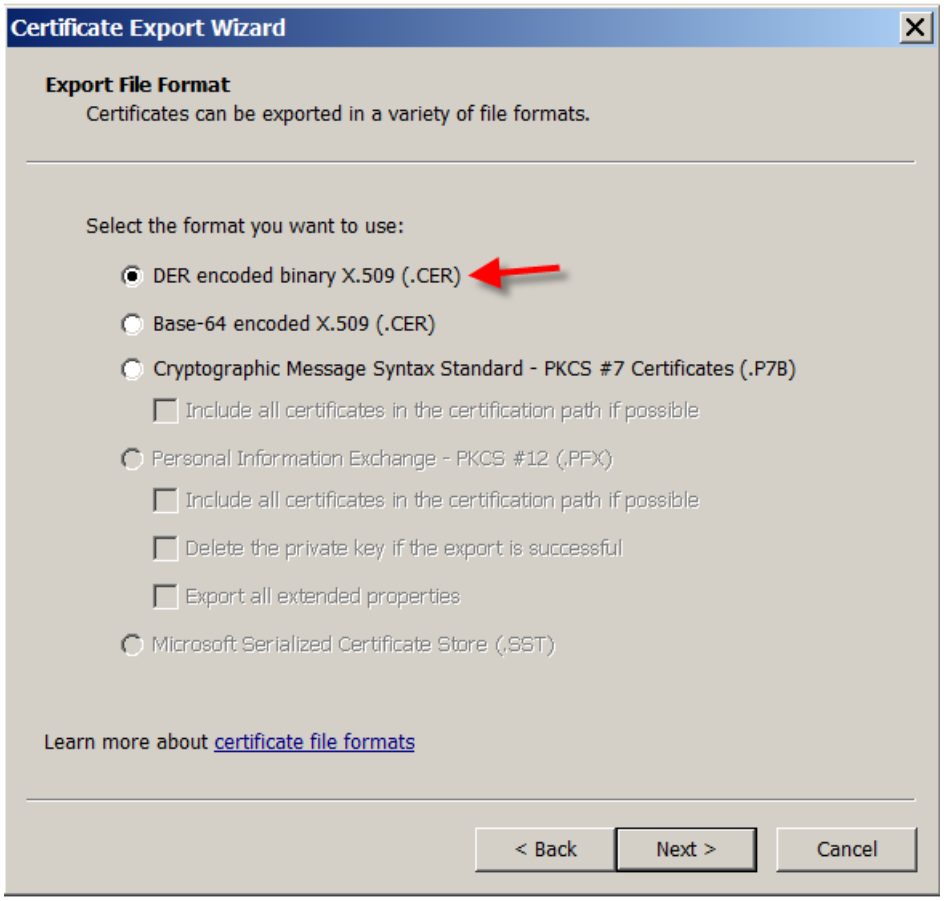


5. Überprüfen Sie Ihre Auswahl und klicken Sie auf **Fertig stellen**. Klicken Sie im Bestätigungsfenster auf **OK**.
6. Klicken Sie in der MMC mit der rechten Maustaste auf das Zertifikat und dann auf **Alle Aufgaben > Exportieren**.

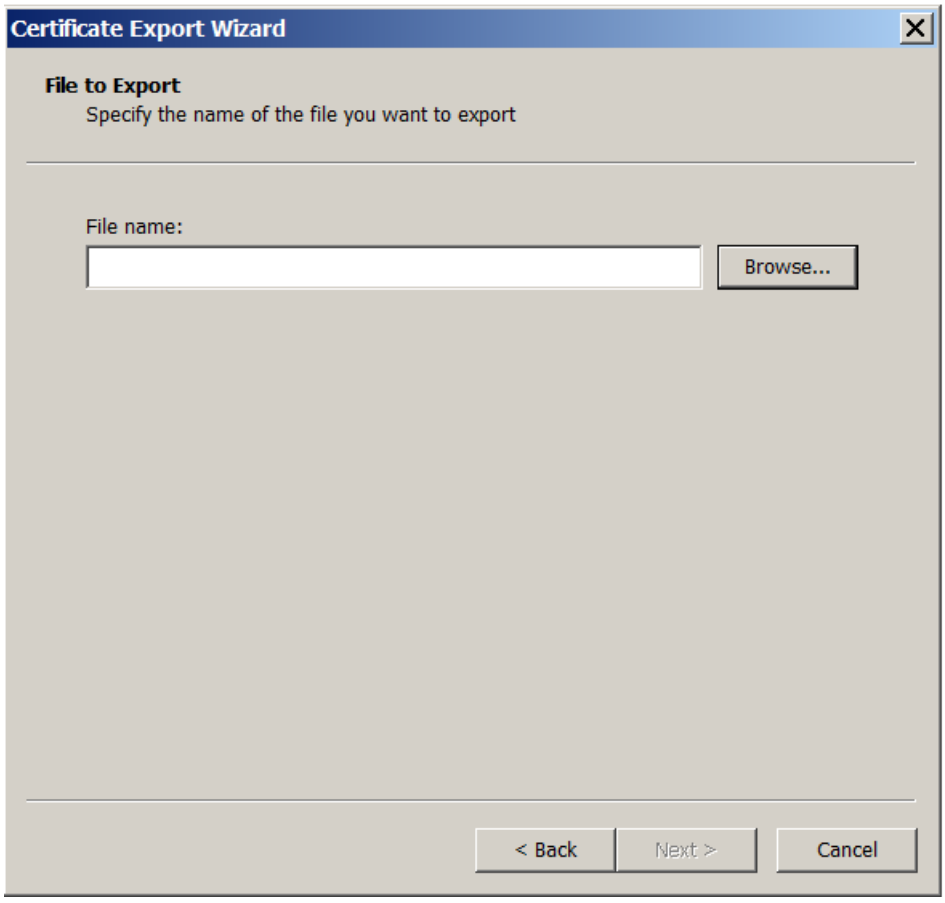


7. Wenn der Zertifikatexport-Assistent geöffnet wird, klicken Sie auf **Weiter**.

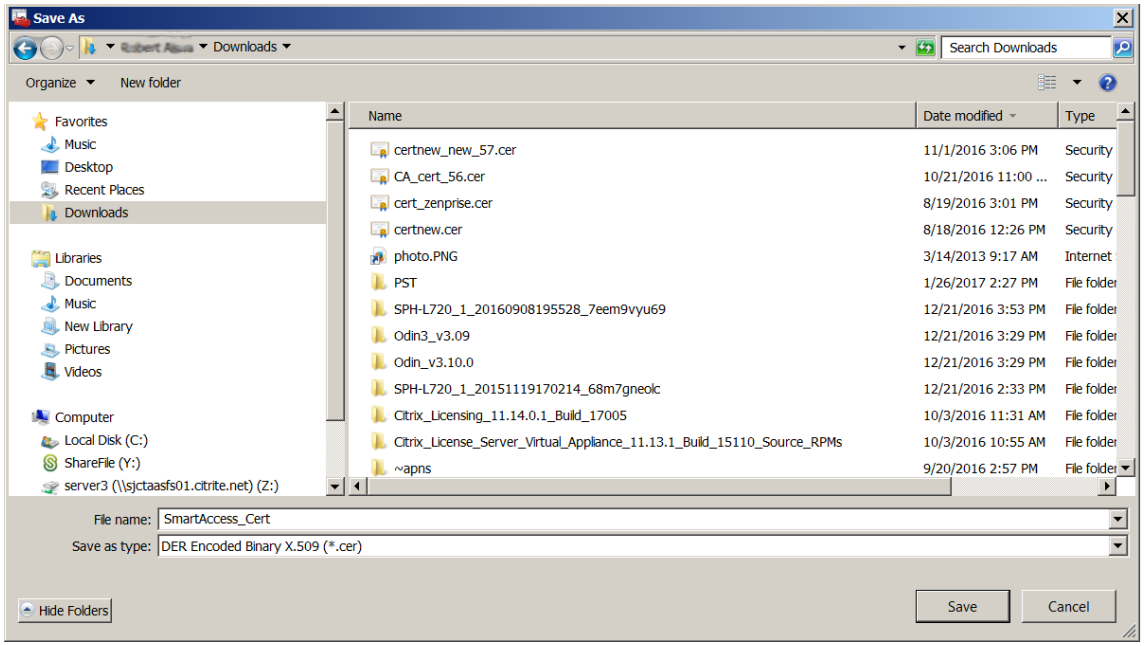
8. Wählen Sie das Format **DER-codiert-binär X.509 (.CER)**. Klicken Sie auf **Weiter**.



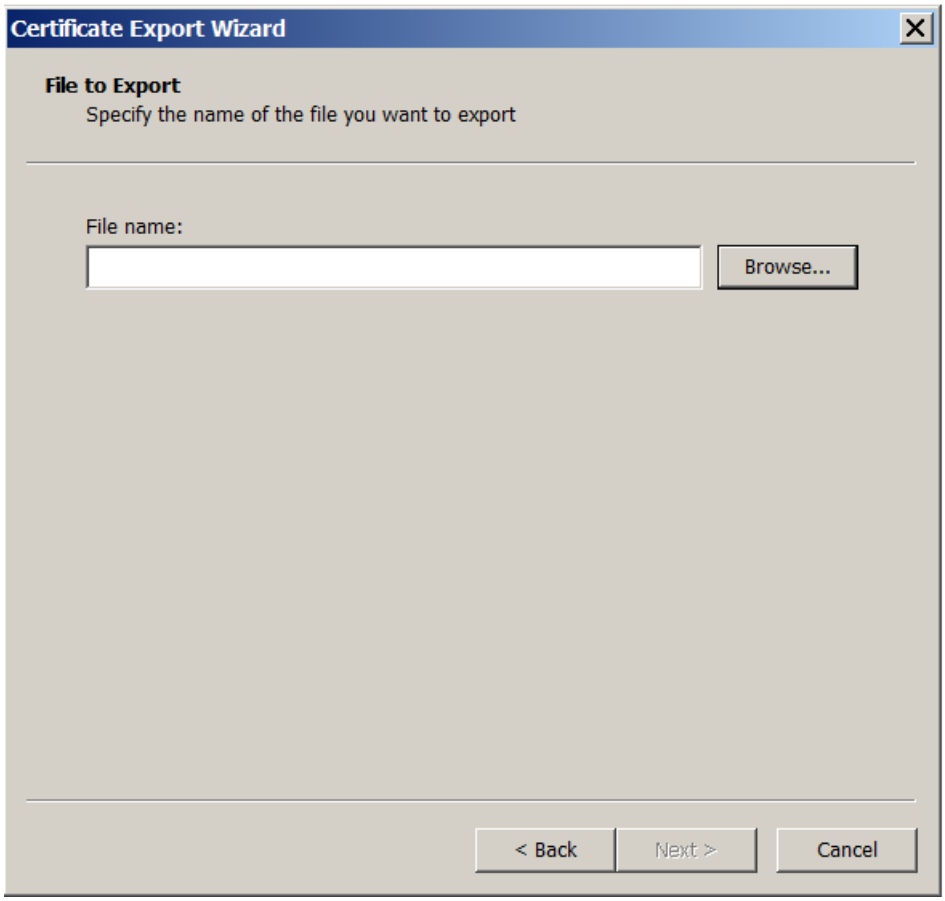
9. Navigieren Sie zu dem Zertifikat. Geben Sie einen Namen für das Zertifikat ein und klicken Sie auf **Weiter**.



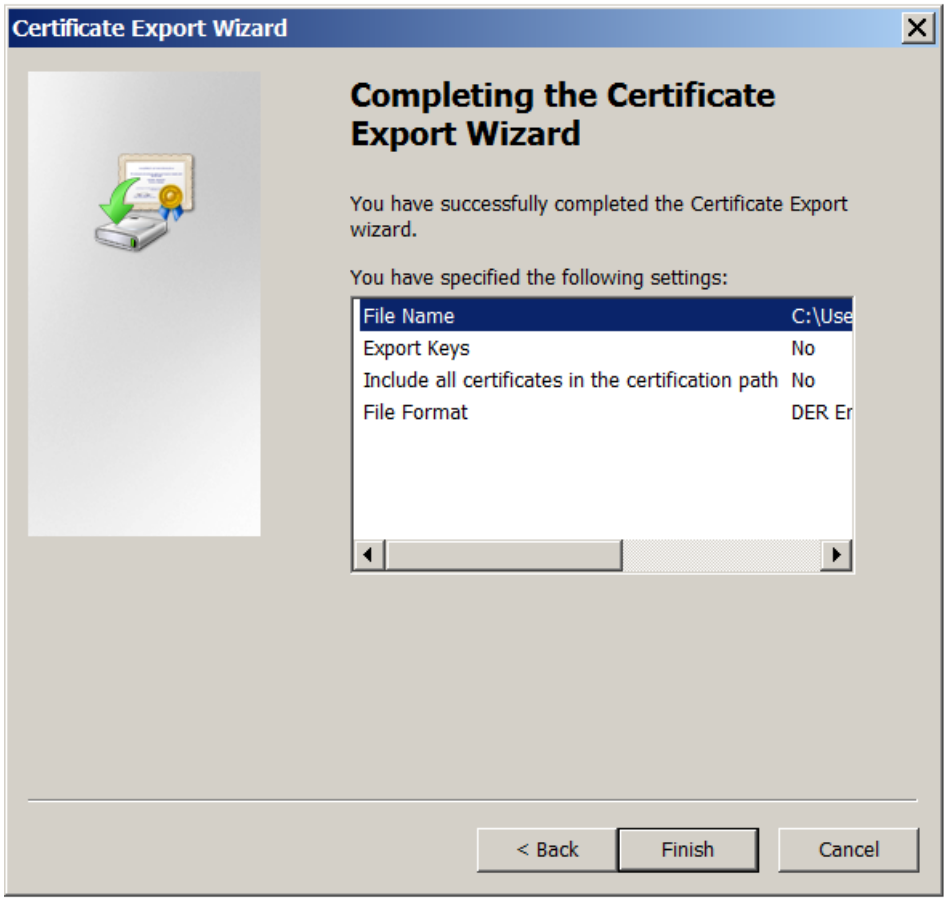
10. Speichern Sie das Zertifikat.



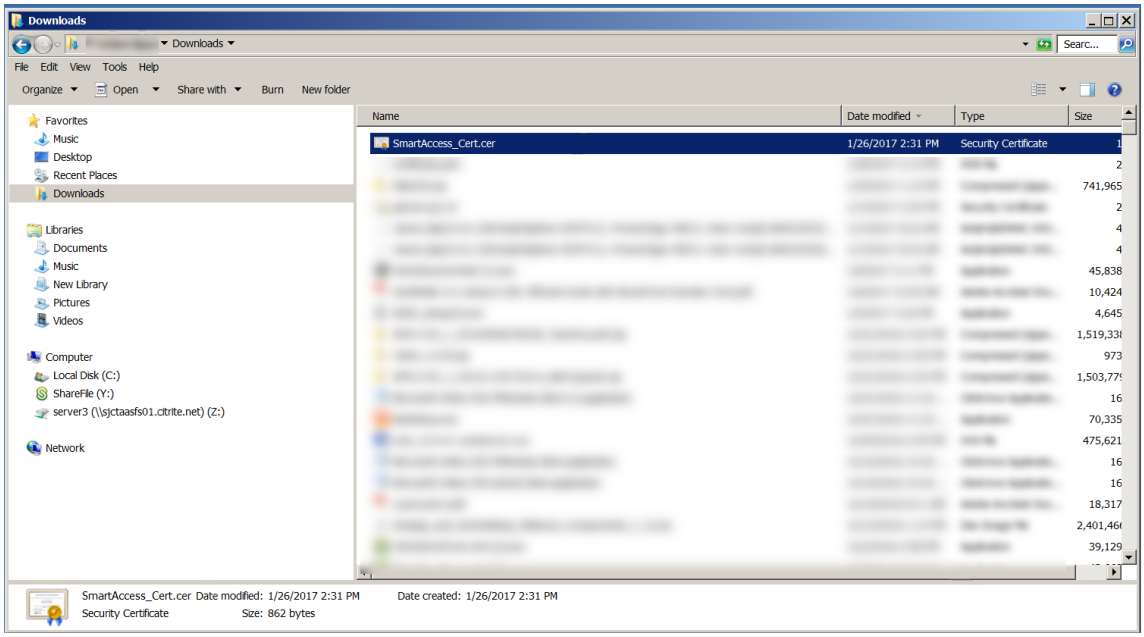
11. Navigieren Sie zu dem Zertifikat und klicken Sie auf **Weiter**.



12. Überprüfen Sie Ihre Auswahl und klicken Sie auf **Fertig stellen**. Klicken Sie im Bestätigungsfenster auf **OK**.

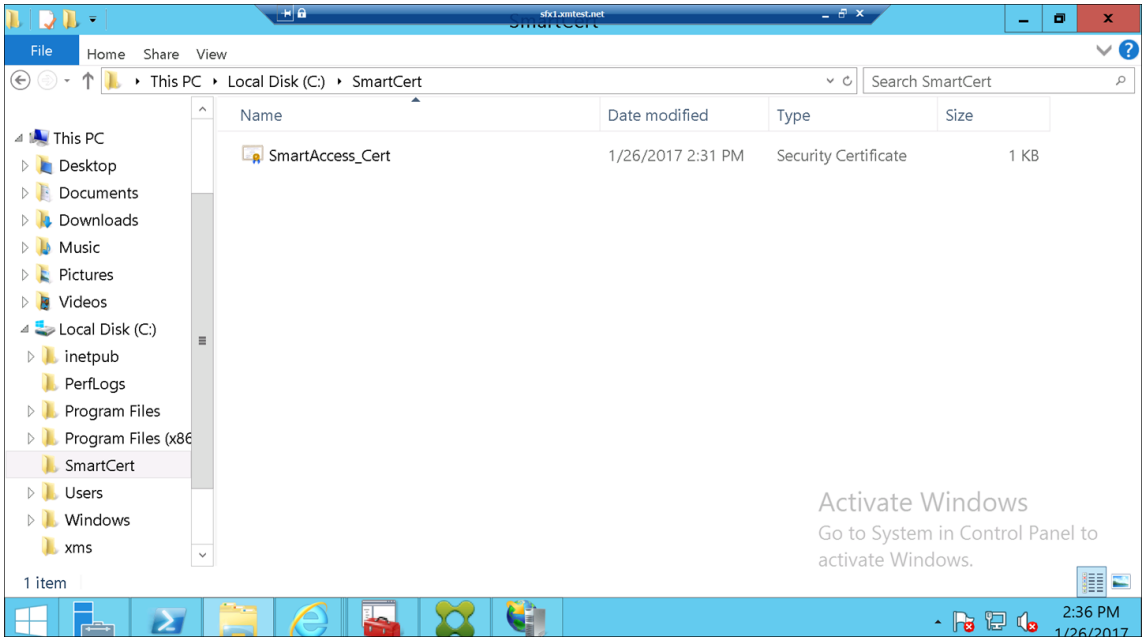


13. Suchen Sie das Zertifikat im Downloadverzeichnis. Das Zertifikat ist im CER-Format.



Kopieren Sie das Zertifikat auf den StoreFront-Server

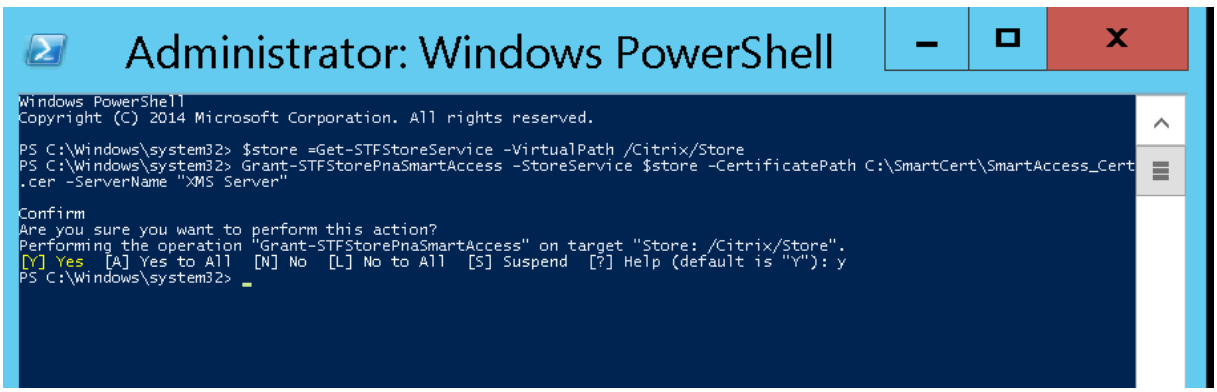
1. Erstellen Sie auf dem StoreFront-Server einen Ordner mit dem Namen **SmartCert**.
2. Kopieren Sie das Zertifikat in den Ordner **SmartCert**.



Konfigurieren des Zertifikats im StoreFront-Store

Führen Sie auf dem StoreFront-Server den folgenden PowerShell-Befehl aus, um das konvertierte Citrix Endpoint Management-Serverzertifikat 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 "[Thumbprint]
<!--NeedCopy-->
```

- Nach Serverobjekt widerrufen:

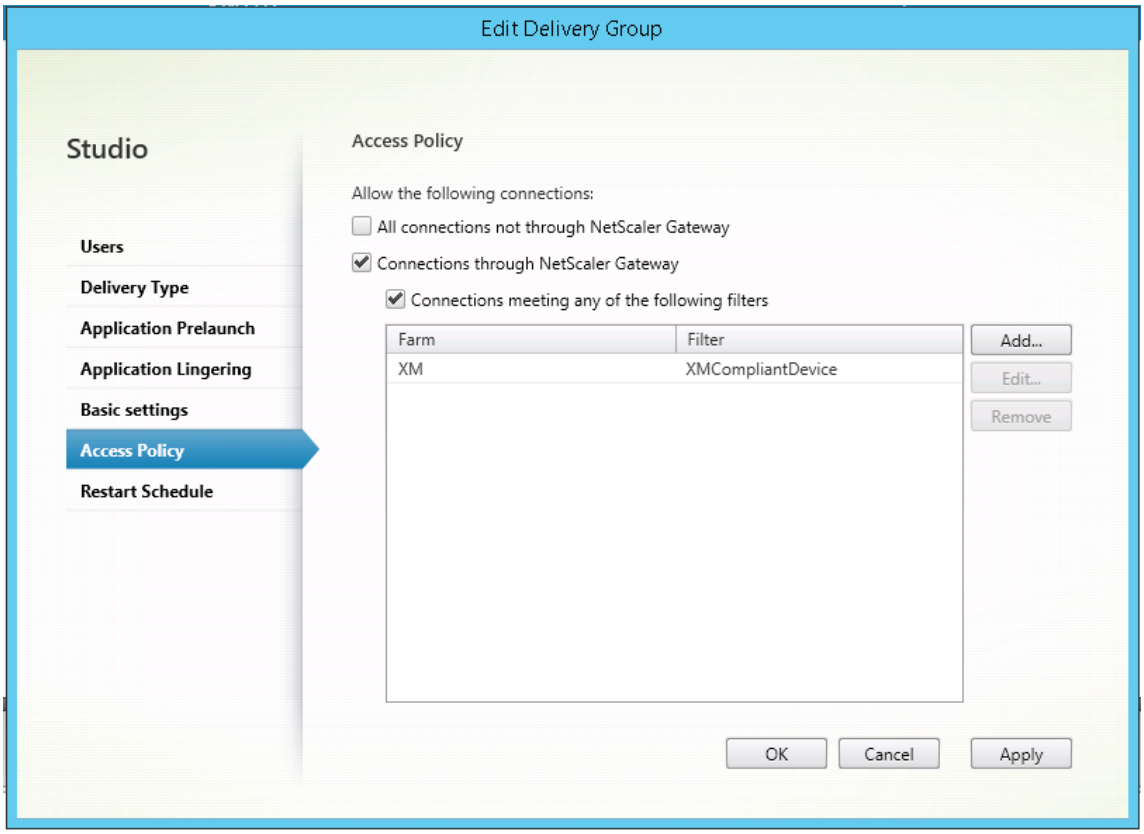
```
    $store = Get-STFStoreService  – VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess  – StoreService $store

    Revoke-STFStorePnaSmartAccess  – StoreService $store  – SmartAccess
       $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

Konfigurieren der SmartAccess-Richtlinie für Citrix Virtual Apps and Desktops

Hinzufügen der erforderlichen SmartAccess-Richtlinie zur Bereitstellungsgruppe, die die HDX-App bereitstellt

1. Öffnen Sie Citrix Studio über die Citrix Cloud-Konsole.
2. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
3. Wählen Sie eine Gruppe aus, die die Apps bereitstellt, deren Zugriff Sie steuern möchten. Wählen Sie dann im Bereich **Aktion** die Option **Bereitstellungsgruppe bearbeiten** aus.

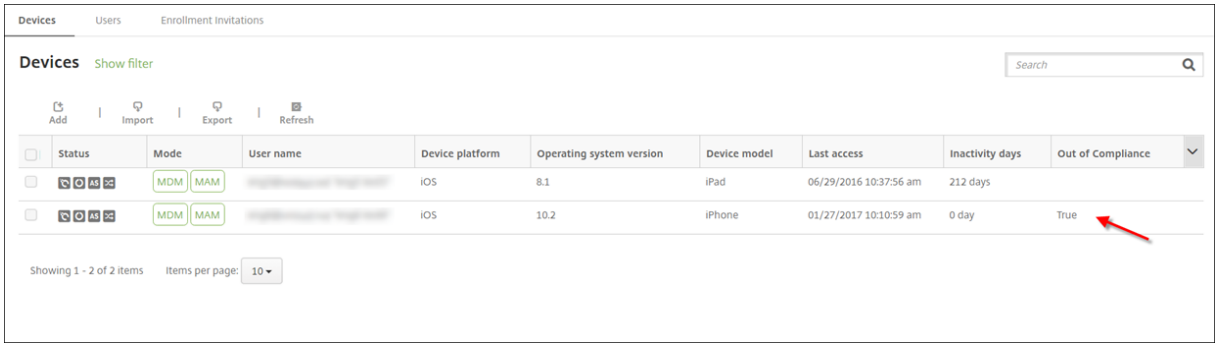
4. Wählen Sie auf der Seite **Zugriffsrichtlinie** die Optionen **Über NetScaler Gateway hergestellte Verbindungen** und **Verbindungen, auf die mindestens einer der folgenden Filter zutrifft** aus.
5. Klicken Sie auf **Hinzufügen**.
6. Fügen Sie eine Zugriffsrichtlinie hinzu, in der **Farm XM** und **Filter XMCompliantDevice** ist.



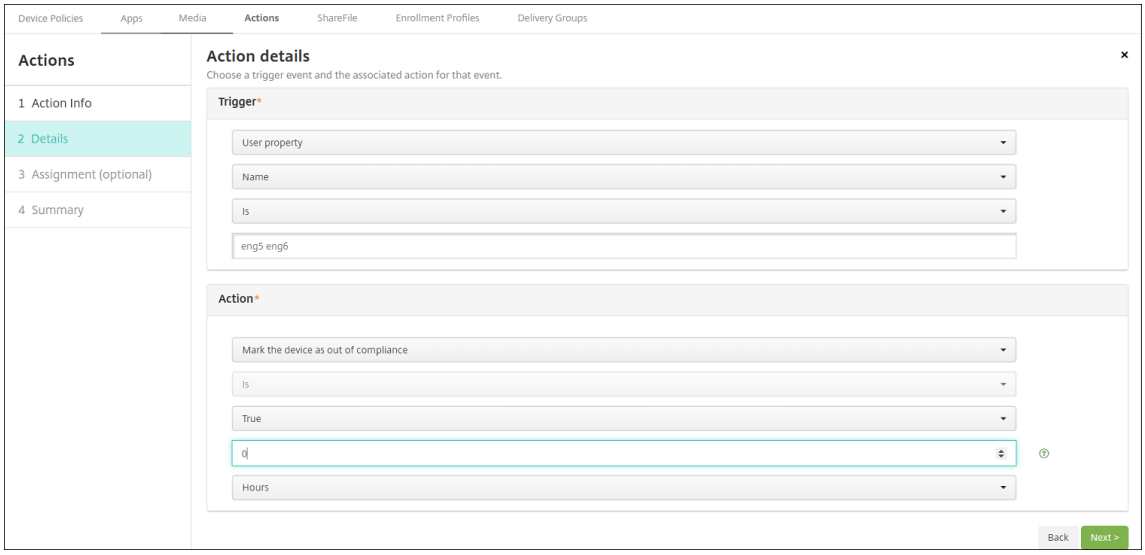
7. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Festlegen automatisierter Aktionen in Citrix Endpoint Management

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 Citrix Endpoint Management-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** aus.
   - Wählen Sie **Ist**.
   - Wählen Sie **Wahr**.

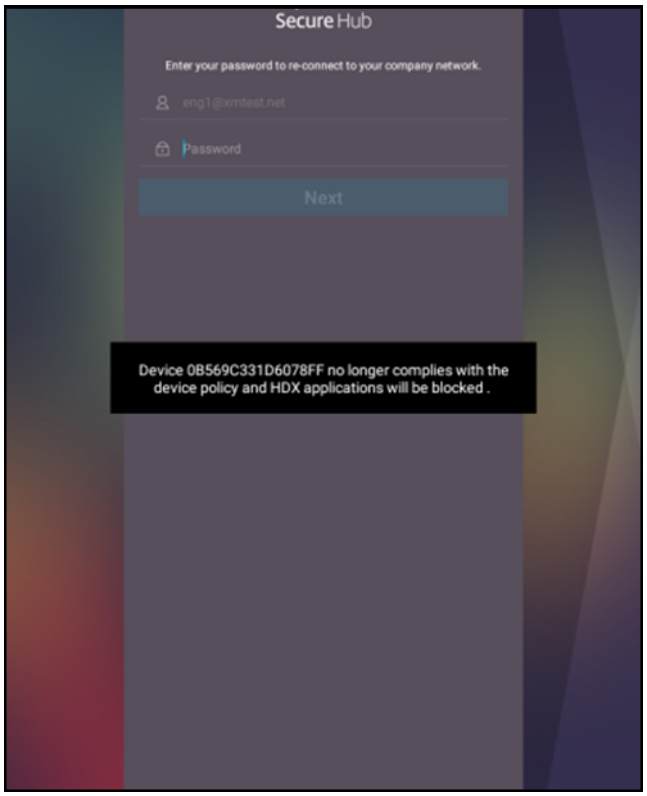
- Wenn das Gerät sofort bei Erfüllen der Auslösebedingung als nicht richtlinientreu markiert werden soll, legen Sie den Zeitrahmen auf **0** fest.

7. Wählen Sie die Citrix Endpoint Management-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 Citrix Secure Hub-Store angezeigt. Der Benutzer hat die Apps nicht mehr abonniert. Es wird keine Benachrichtigung an das Gerät gesendet und nichts im Citrix Secure Hub-Store weist darauf hin, dass die HDX-Apps zuvor verfügbar waren.

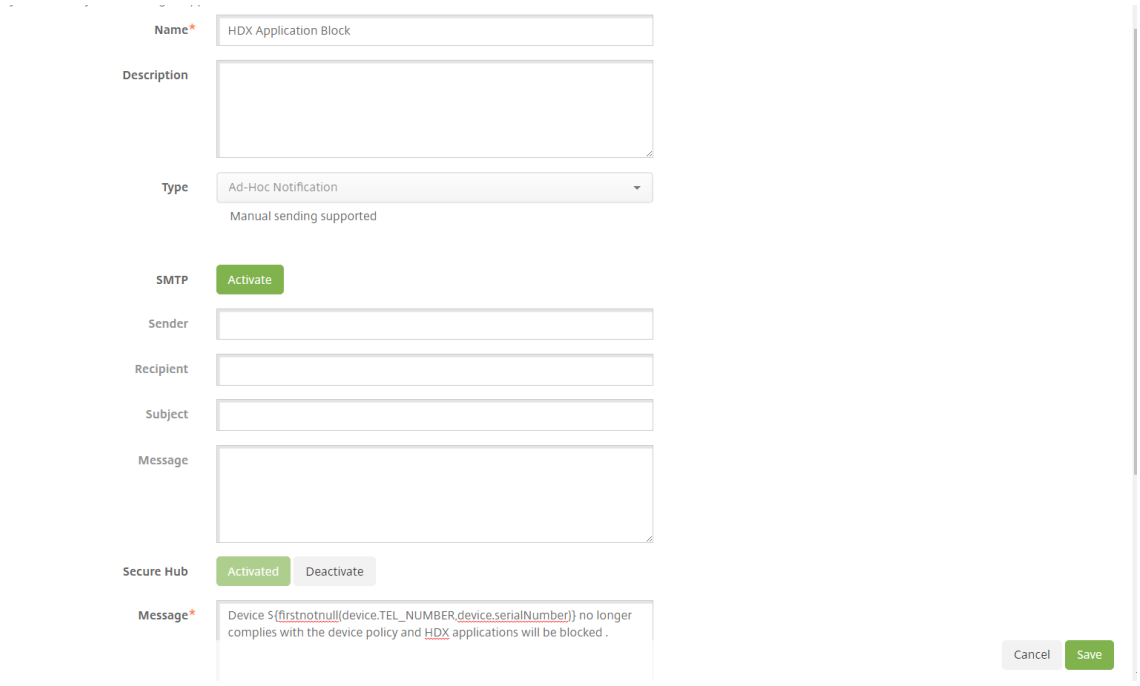
Wenn Sie möchten, dass Benutzer benachrichtigt werden, wenn ein Gerät als nicht richtlinientreu markiert wird, erstellen Sie eine Benachrichtigung und dann eine automatisierte Aktion zum Senden der Benachrichtigung.

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

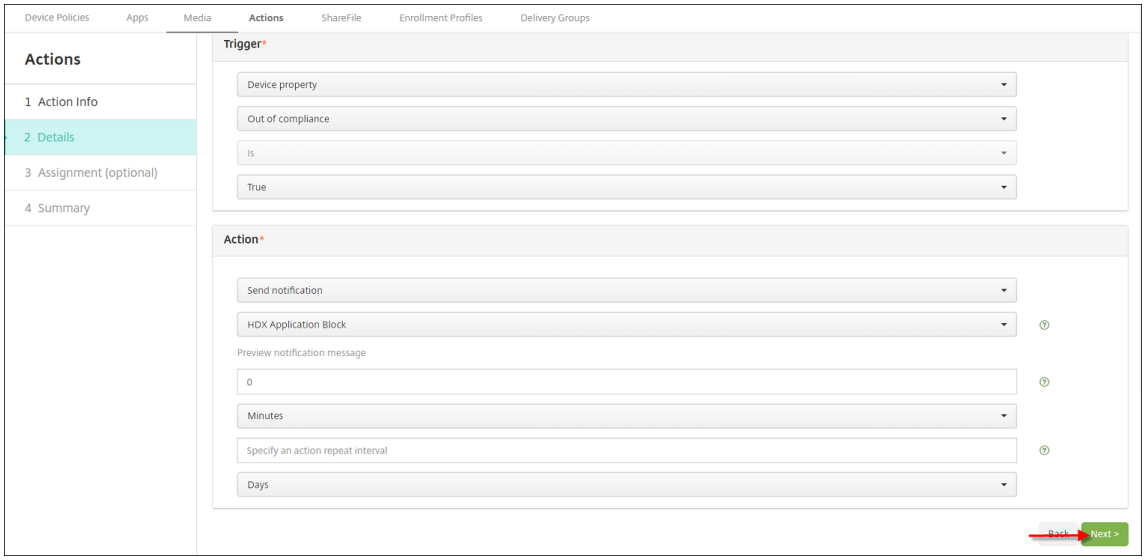
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf **Benachrichtigungsvorlagen**. Die Seite **Benachrichtigungsvorlagen** wird angezeigt.
3. Klicken Sie auf **Hinzufügen**, um auf der Seite **Benachrichtigungsvorlagen** eine Vorlage hinzuzufügen.
4. Konfigurieren Sie folgende Einstellungen:
   - **Name:** HDX-Anwendungsblockierung
   - **Beschreibung:** Agent-Benachrichtigung, wenn ein Gerät nicht richtlinientreu ist
   - **Typ:** Ad-Hoc-Benachrichtigung
   - **Citrix Secure Hub:** Aktiviert
   - **Nachricht:** Gerät `${ firstnotnull(device.TEL_NUMBER,device.serialNumber ) }` erfüllt die Geräterichtlinie nicht mehr und HDX-Apps werden gesperrt.



5. 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 Citrix Endpoint Management-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** aus.
   - 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, wenn die Auslösebedingung erfüllt ist.

7. Wählen Sie die Citrix Endpoint Management-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**.

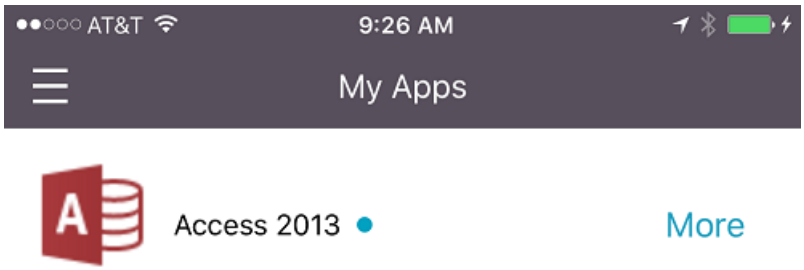
Details über das Festlegen von automatisierten Aktionen finden Sie unter Automatisierte Aktionen.

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 Citrix 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.



Upgrades von MDX- oder Unternehmensapps

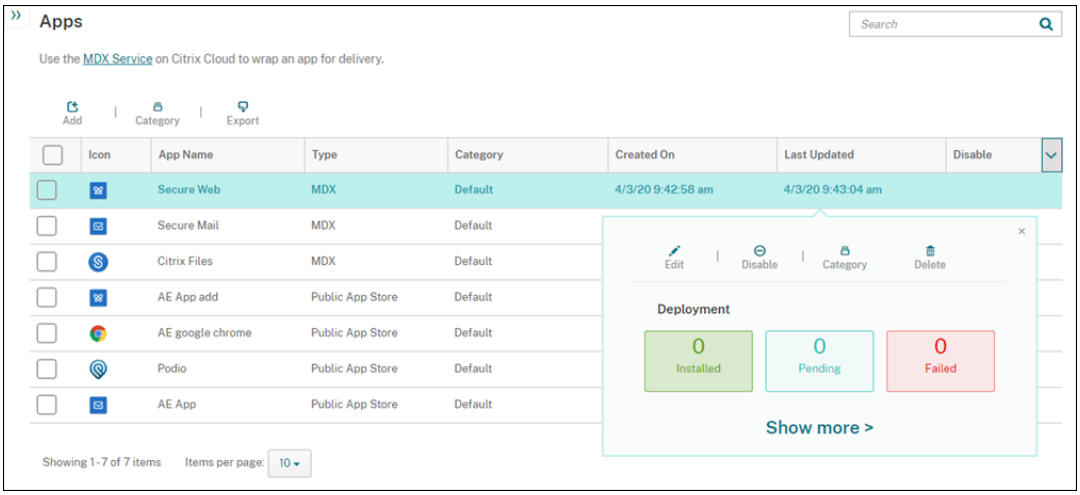
December 1, 2023

Zum Aktualisieren einer MDX- oder Unternehmensapp in Citrix Endpoint Management deaktivieren Sie diese in der Citrix Endpoint Management-Konsole und laden Sie die neue App-Version hoch.

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Apps**. Die Seite **Apps** wird angezeigt.
2. Fahren Sie bei verwalteten Geräten (d. h. bei Citrix Endpoint Management für die Mobilgeräteverwaltung registrierten Geräten) mit Schritt 3 fort. Führen Sie für nicht verwaltete, d. h. bei Citrix Endpoint Management 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:**
>
> Bei deaktivierter App können Benutzer sich nach dem Abmelden nicht erneut mit der App verbinden. Das Deaktivieren von Apps ist optional, es wird jedoch empfohlen, um Probleme bei der App-Funktionalität zu vermeiden. Beispielsweise kann ein Prob-

> lem 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 Citrix Endpoint Management 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 optional Bereitstellungsregeln und den App-Store. Informationen hierzu finden Sie unter 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.

Medien hinzufügen

March 11, 2024

Sie fügen Medien zu Citrix Endpoint Management hinzu, um sie auf Benutzergeräten zu verteilen. Mit Citrix Endpoint Management können Sie Apple-Bücher bereitstellen, die Sie über Apple Volume Purchase erworben haben.

Nachdem Sie ein Volume Purchase-Konto in Citrix Endpoint Management 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.

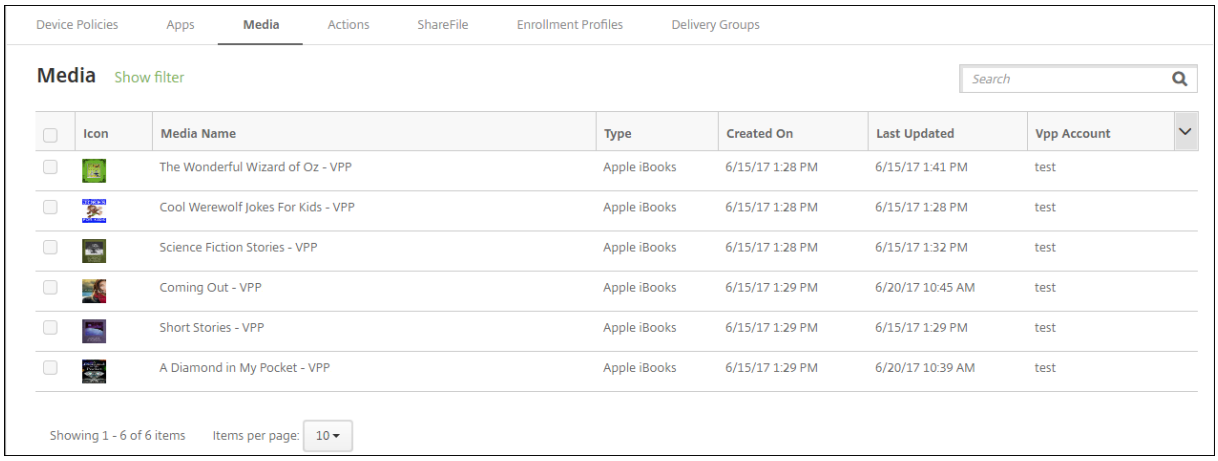
Wenn ein Benutzer das erste Mal ein Buch erhält und die Volume Purchase-Lizenz akzeptiert, werden bereitgestellte Bücher auf dem Gerät installiert. Die Bücher werden in Apple Books angezeigt. Sie können die Zuweisung zwischen Benutzer und Lizenz nicht aufheben und das Buch nicht vom Gerät entfernen. Citrix Endpoint Management 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 Citrix Endpoint Management wie unter Apple Volume Purchase beschrieben.

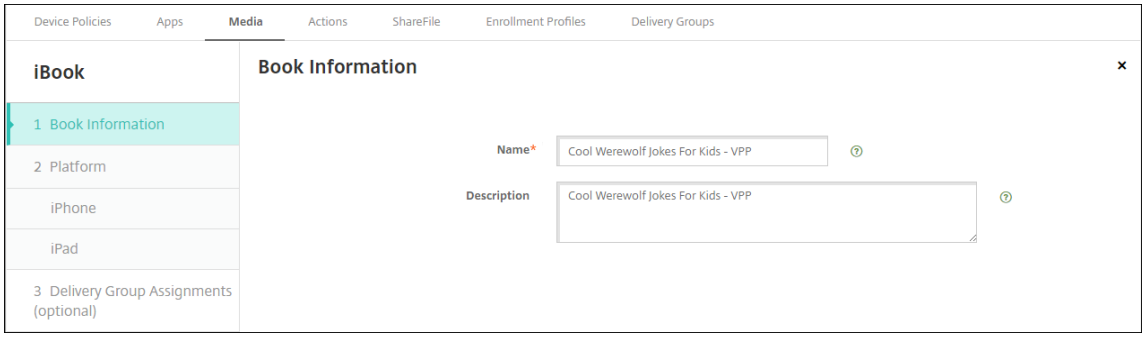
Konfigurieren von Büchern

Über Volume Purchase erworbene Bücher werden auf der Seite **Konfigurieren** > **Medien** angezeigt.



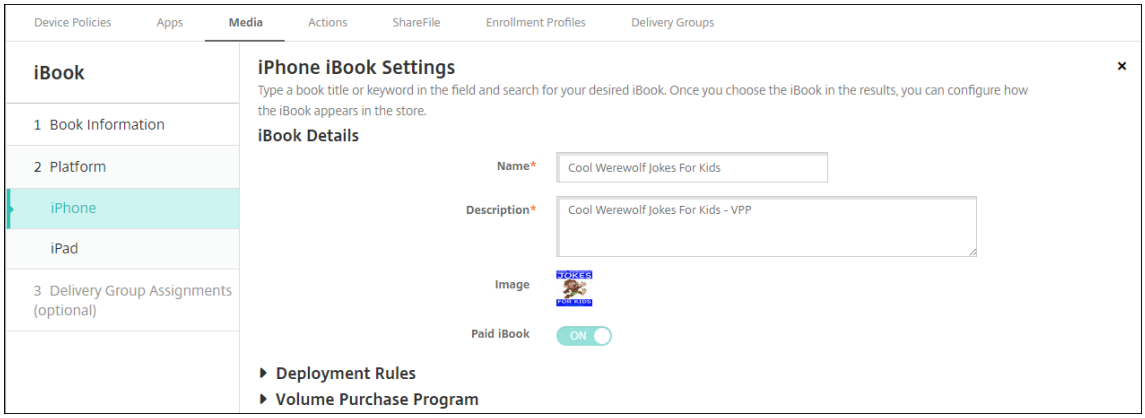
Konfigurieren eines Apple-Buchs für die Bereitstellung

1. Wählen Sie unter **Konfigurieren > Medien** ein Buch aus und klicken Sie auf **Bearbeiten**. Die Seite **Buchinformationen** wird angezeigt.

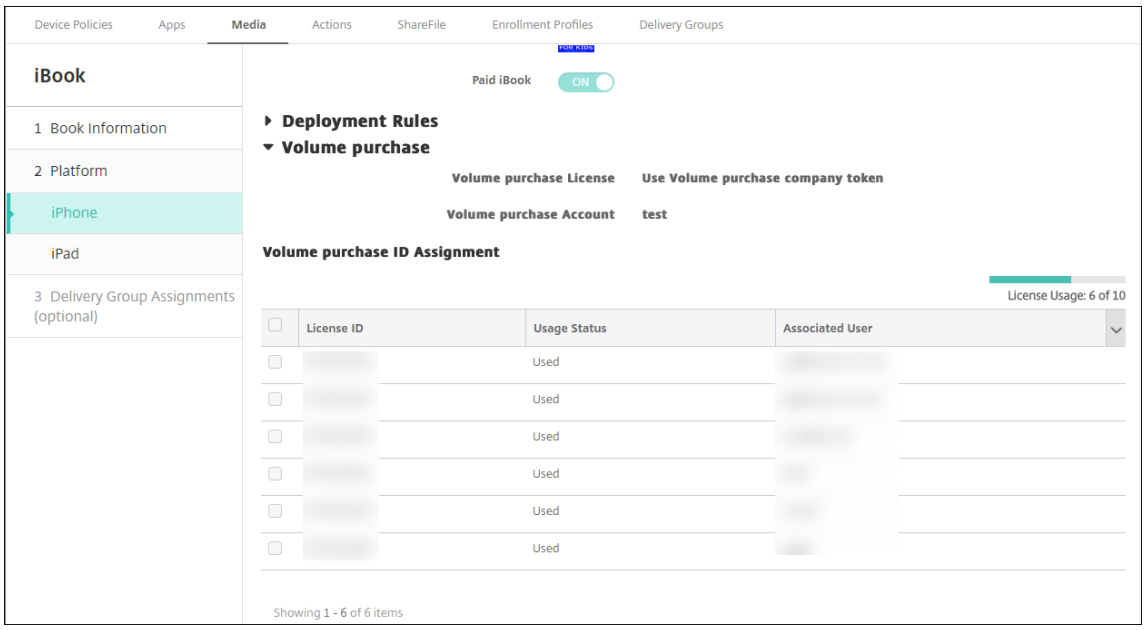


   Der **Name** und die **Beschreibung** werden nur in der Citrix Endpoint Management-Konsole und den Protokollen angezeigt.

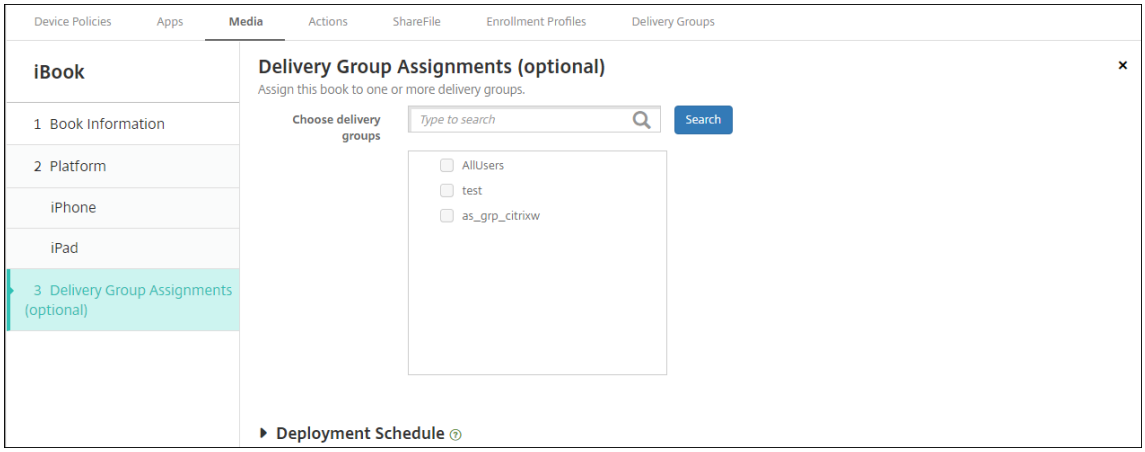
2. Auf den Seiten **iBook-Einstellungen für iPhone** und **iBook-Einstellungen iPad**: Sie können den Namen und die Beschreibung des Buchs optional ändern. Citrix empfiehlt jedoch, diese Einstellungen nicht zu ändern. Das Bild dient zur Information und kann nicht bearbeitet werden. **Bezahltes iBook:** zeigt an, dass ein Buch über Volume Purchase erworben wurde.



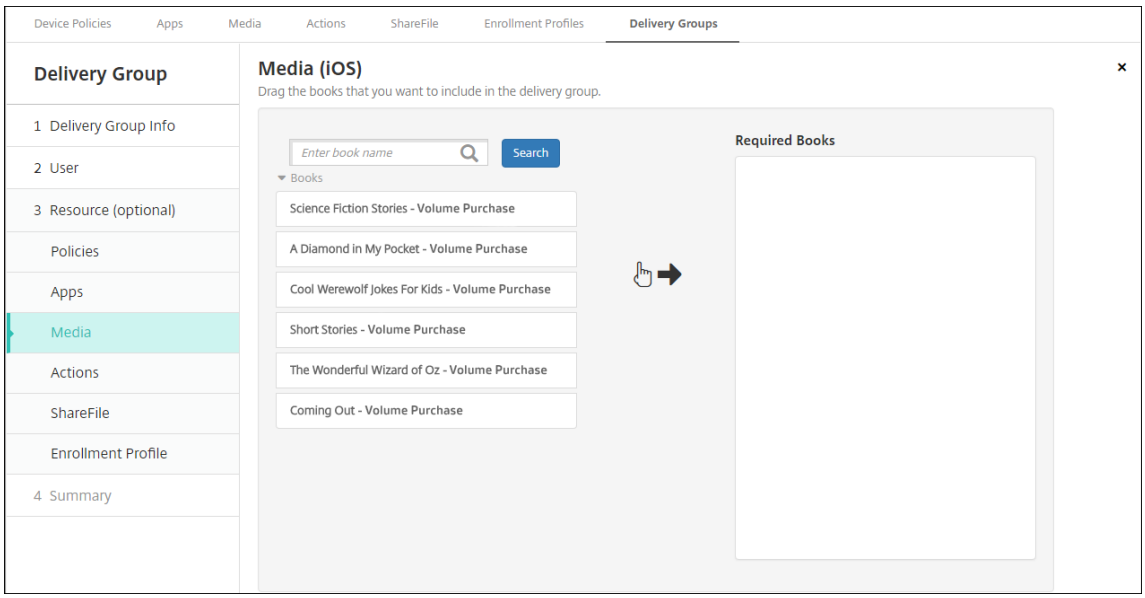
   Sie können auch Volume Purchase-Informationen anzeigen oder Bereitstellungsregeln festlegen.



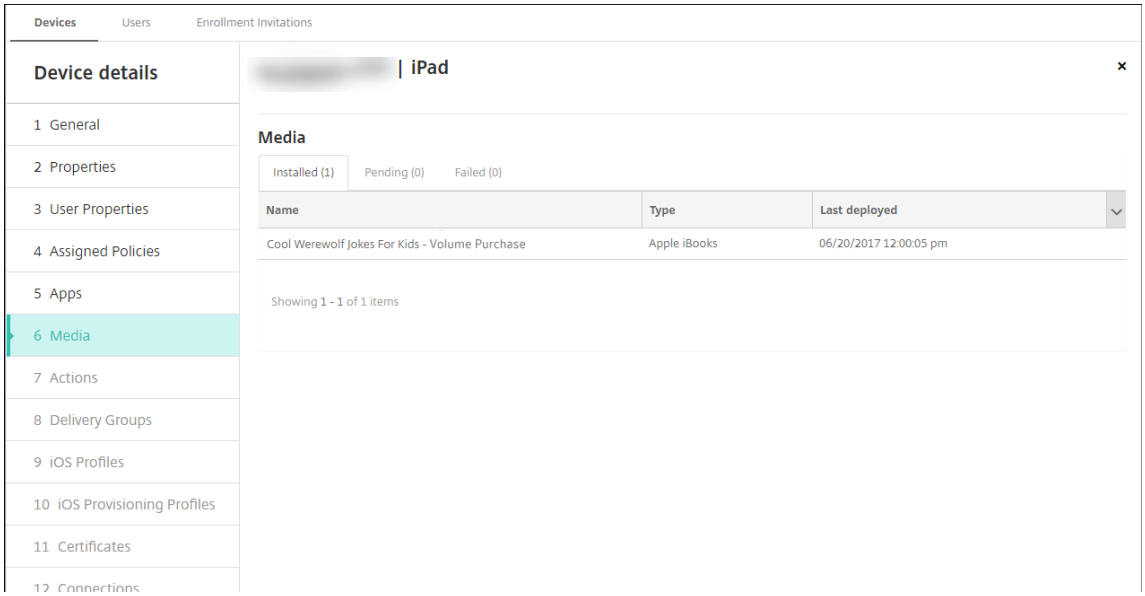
3. Optional können Sie das Buch Bereitstellungsgruppen zuordnen und einen Bereitstellungsplan festlegen.



Sie können Bücher Bereitstellungsgruppen auch über die Registerkarte **Medien** des Bereichs **Konfigurieren > Bereitstellungsgruppen** zuordnen. Citrix Endpoint Management unterstützt nur die Bereitstellung von erforderlichen Büchern.

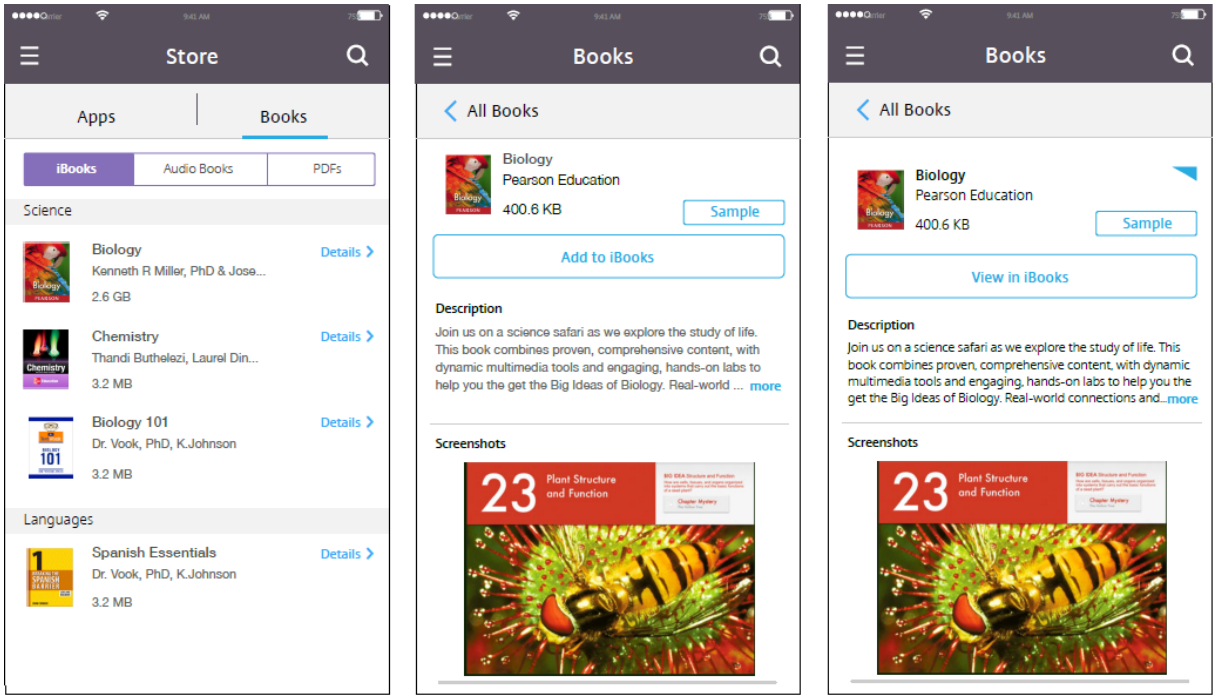


4. Verwenden Sie die Registerkarte **Medien** unter **Verwalten > Geräte**, um den Bereitstellungsstatus anzuzeigen.



> **Hinweis:**
>
> Wenn Sie auf der Seite **Konfigurieren** > **Medien** ein Buch auswählen und auf **Löschen** klicken, entfernt Citrix Endpoint Management das Buch aus der Liste. Wenn Citrix Endpoint Management 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 vom Gerät.

Bücher erscheinen auf Benutzergeräten wie im nachstehenden Beispiel gezeigt.



Ressourcen bereitstellen

March 11, 2024

Die Gerätekonfiguration und -verwaltung umfasst üblicherweise das Erstellen von Ressourcen (Richtlinien, Apps und Medien) und Aktionen in der Citrix Endpoint Management-Konsole und anschließend das Verpacken dieser Ressourcen für die Verwendung mit Bereitstellungsgruppen. Bereitstellungsgruppen definieren Kategorien von Benutzern, damit Sie festgelegte Richtlinien, Apps, Medien und Aktionen auf ihren Geräten bereitstellen können. Die Citrix Endpoint Management-Konsole bietet folgende Funktionen:

- Bereitstellungsgruppen hinzufügen, verwalten und bereitstellen.
- Reihenfolge ändern, in der Citrix Endpoint Management Ressourcen und Aktionen auf Geräten in einer Bereitstellungsgruppe bereitstellt. Diese Reihenfolge wird als *Bereitstellungsreihenfolge* bezeichnet.

  Sie können die Bereitstellungsreihenfolge in der Citrix Endpoint Management-Konsole festlegen. Wenn ein Benutzer Mitglied mehrerer Bereitstellungsgruppen mit doppelten oder widersprüchlichen Richtlinien ist, wird die Bereitstellungsreihenfolge von Citrix Endpoint Management festgelegt. Siehe Berechnungsschritte.

Bereitstellungsgruppen

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 entweder allen Benutzern oder einer definierten Benutzergruppe bereitstellen.

Durch Installation und Konfiguration von Citrix Endpoint Management wird die Standardbereitstellungsgruppe "AllUsers"erstellt. Diese Gruppe enthält alle lokalen und Active Directory-Benutzer. Die Gruppe "AllUsers"kann nicht gelöscht werden, Sie können sie jedoch deaktivieren, wenn Sie Ressourcen nicht für alle Benutzer bereitstellen möchten. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der Bereitstellungsgruppe "AllUsers".

Wenn Sie eine Ressource für eine Bereitstellungsgruppe bereitstellen, senden Sie eine Pushbenachrichtigung an alle Benutzer in der Bereitstellungsgruppe. Verwenden Sie für Apple-Geräte den Apple Dienst für Push-Benachrichtigungen (APN), um Benachrichtigungen zu senden. Weitere Informationen finden Sie unter APNs-Zertifikate. Für Android-Geräte verwenden Sie Firebase Cloud Messaging (FCM). Weitere Informationen finden Sie unter Firebase Cloud Messaging. Verwenden Sie für Windows-Geräte den Windows-Pushbenachrichtigungsdienst (WNS).

Ressourcen bereitstellen

Wenn Sie Ressourcen per Push-Übertragung auf Geräten bereitstellen möchten, sollten Sie Folgendes berücksichtigen:

- **Bereitstellungsreihenfolge:** Die Bereitstellungsreihenfolge ist die Reihenfolge, in der Citrix Endpoint Management Ressourcen (Richtlinien, Apps und Medien) und Aktionen auf einem Gerät bereitstellt. Die Bereitstellungsreihenfolge gilt für Geräte in einer Bereitstellungsgruppe mit einem für die Geräteverwaltung (MDM) konfigurierten Registrierungsprofil oder für eine Kombination aus Anwendungsverwaltung (MAM) und MDM.
- **Bereitstellungsregeln:** Citrix Endpoint Management verwendet die Bereitstellungsregeln, die Sie für Benutzer- und Geräteeigenschaften 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.

  Innerhalb einer Bereitstellungsgruppe können Sie eine Teilmenge von Benutzern und Geräten angeben, die die Ressourcen basierend auf ihren Benutzer- und Geräteeigenschaften erhalten. Das Filtern nach Benutzer- und Geräteeigenschaften innerhalb einer Bereitstellungsgruppe hat Vorrang vor Bereitstellungsregeln, die auf der Ressource festgelegt sind.
- **Bereitstellungszeitplan:** Citrix Endpoint Management 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 unmittelbar, zu einem festgelegten Termin und Zeitpunkt oder basierend auf Bereitstellungsbedingungen erfolgt. Sie legen den Zeitplan fest, wenn Sie die Regel erstellen. Weitere Informationen finden Sie unter Bereitstellungsregeln konfigurieren.

Überlegen Sie sich vor dem Hinzufügen von Bereitstellungsgruppen, wie Bereitstellungsreihenfolge, Regeln und Zeitplan sich auf Ihre Bereitstellungsziele auswirken.

Bereitstellungsreihenfolge

Die Bereitstellungsreihenfolge ist die Reihenfolge, in der Citrix Endpoint Management Ressourcen per Push auf den Geräten bereitstellt. Die Bereitstellungsreihenfolge ist wichtig, wenn Voraussetzungen für Ressourcen und Abhängigkeiten zwischen Ressourcen bestehen. Ressourcen sind Richtlinien, Apps, Aktionen und Bereitstellungsgruppen.

Wenn Sie beispielsweise eine Wi-Fi-Richtlinie mit zertifikatbasierter Authentifizierung per Push übermitteln, müssen Sie erst die Zertifizierungsrichtlinie und dann die Wi-Fi-Richtlinie bereitstellen. Andernfalls treten Fehler auf. Umgekehrt spielt bei einigen Richtlinien (zum Beispiel für Geschäftsbedingungen, Softwarebestand und Aktionen) die Bereitstellungsreihenfolge keine Rolle.

Wenn Sie eine Bereitstellungsgruppe hinzufügen, können Sie die Reihenfolge festlegen, in der Ressourcen auf Geräten bereitgestellt werden. Citrix Endpoint Management erkennt jedoch stets, wenn ein Benutzer Mitglied mehrerer Bereitstellungsgruppen mit doppelten oder widersprüchliche Richtlinien ist. In diesen Fällen berechnet Citrix Endpoint Management eine Bereitstellungsreihenfolge für bereitgestellte Objekte und für ausgeführte Aktionen.

Beim Ermitteln der Bereitstellungsreihenfolge wendet Citrix Endpoint Management Filter- und Steuerungskriterien für Ressourcen an, z. B. Bereitstellungsregeln und Bereitstellungszeitpläne. Die folgende Tabelle zeigt, welche dieser Kriterien Sie auf jeden Ressourcentyp anwenden können.

Ressource	Geräteplattform	Bereitstellungsregeln	Bereitstellungszeitpläne	Benutzer/Gruppen
Geräterichtlinie	J	J	J	-
App	J	J	J	-
Medien	J	J	J	-
Aktion	-	J	J	-
Bereitstellungsgruppe		J	-	J

Berechnungsschritte

Wenn Citrix Endpoint Management eine Bereitstellungsreihenfolge berechnen muss, führt es diese Schritte aus.

> **Hinweis:**
>
> Die Geräteplattform hat keinen Einfluss auf die 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 aus Bereitstellungsgruppen mit administratordefinierter Bereitstellungsreihenfolge stehen vor Ressourcen aus Bereitstellungsgruppen ohne Bereitstellungsreihenfolge. Weitere Informationen finden Sie im Beispiel für eine Berechnung mit benutzerdefinierter Reihenfolge.

    b) Bei einem Gleichstand zwischen Bereitstellungsgruppen werden Ressourcen aus Bereitstellungsgruppen nach dem Gruppennamen in umgekehrter alphabetischer Reihenfolge sortiert. So stellt Citrix Endpoint Management Ressourcen aus der Bereitstellungsgruppe B beispielsweise vor Ressourcen aus der Bereitstellungsgruppe A.

    c) Wurde eine administratordefinierte Bereitstellungsreihenfolge für die Ressourcen in einer Bereitstellungsgruppe angegeben, ist sie einzuhalten. Sonst die Ressourcen in der Bereitstellungsuppe in alphabetischer Reihenfolge nach dem Ressourcennamen sortieren.

    d) Kommt dieselbe Ressource mehrmals vor, wird das Duplikat der Ressource entfernt. Stellen Sie nur die erste dieser Ressourcen bereit.

Ressourcen, die einer administratordefinierten Reihenfolge zugeordnet sind, werden vor Ressourcen ohne administratordefinierte Reihenfolge bereitgestellt.

Beispiel für eine Berechnung mit administratordefinierter Reihenfolge Angenommen, Sie haben zwei Bereitstellungsgruppen:

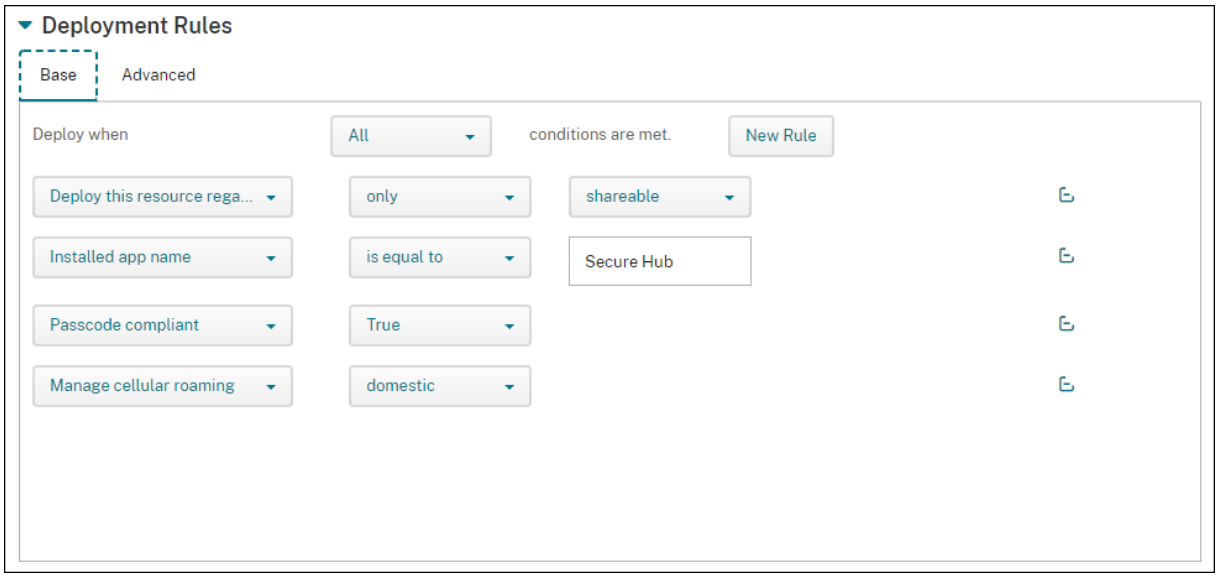
- Bereitstellungsgruppe Kontomanager 1: Bei einer *nicht angegebenen* Ressourcenreihenfolge sind die Richtlinien **Netzwerk** und **Passcode** enthalten.
- Bereitstellungsgruppe Kontomanager 2: Bei einer *angegebenen* Ressourcenreihenfolge sind die Richtlinien **Verbindungszeitplan**, **Einschränkungen**, **Passcode** und **Netzwerk** in einer Reihenfolge enthalten.

Wenn Bereitstellungsgruppen nur nach Namen sortiert werden, führt Citrix Endpoint Management die Bereitstellung beginnend mit der Bereitstellungsgruppe “Kontomanager 1”in der Reihenfolge **Netzwerk**, **Passcode**, **Verbindungszeitplan**, **Einschränkungen** durch. Citrix Endpoint Management ignoriert in diesem Fall **Passcode** und **Netzwerk** (beides Duplikate) aus der Bereitstellungsgruppe “Kontomanager 2”.

Für die Gruppe “Kontomanager 2”gibt es jedoch eine vom Administrator festgelegte Bereitstellungsreihenfolge. Die Ressourcen aus der Bereitstellungsgruppe “Kontomanager 2”werden daher höher in der Liste platziert als die Ressourcen aus der Bereitstellungsgruppe “Kontomanager1” . Die Richtlinien werden daher von Citrix Endpoint Management in der folgenden Reihenfolge bereitgestellt: **Verbindungszeitplan**, **Einschränkungen**, **Passcode**, **Netzwerk**. Citrix Endpoint Management ignoriert die Richtlinien **Netzwerk** und **Passcode** aus der Bereitstellungsgruppe “Kontomanager 1”, da es sich um Duplikate handelt. Der Algorithmus wendet die vom Citrix Endpoint Management-Administrator festgelegte Reihenfolge an.

Bereitstellungsregeln konfigurieren

Konfigurieren Sie Bereitstellungsregeln, um Ressourcen 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.

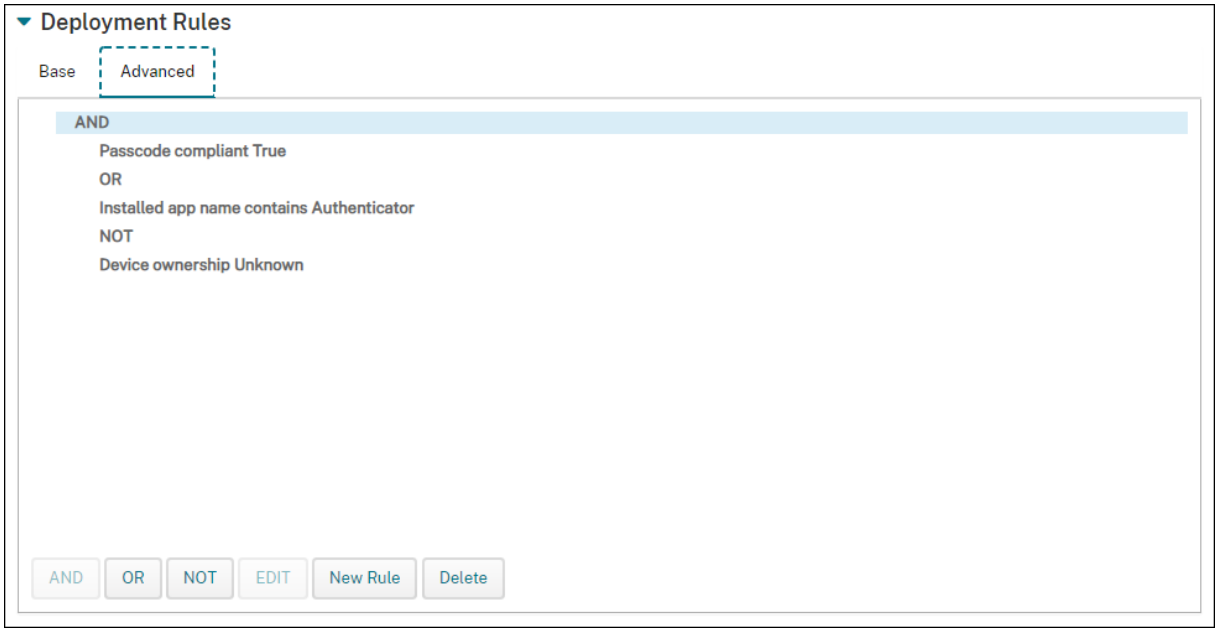
- **Alle:** Stellen Sie die Ressource bereit, wenn der Benutzer oder das Gerät alle von Ihnen konfigurierten Bedingungen erfüllt.
- **Beliebig:** Stellen Sie die Ressource bereit, wenn der Benutzer oder das Gerät mindestens eine der von Ihnen konfigurierten Bedingungen erfüllt.

Klicken Sie auf **Neue Regel**, um eine Regel aus einer Liste verfügbarer Regeln auszuwählen und hinzuzufügen. Die verfügbaren Regeln variieren je nach bereitgestellter Ressource und der Plattform, für die Sie die Ressource konfigurieren. Innerhalb jeder Regel gelten Bedingungen.

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 einer 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.



Mit Bereitstellungsgruppen arbeiten

Folgendes ist bei der Arbeit mit Bereitstellungsgruppen möglich:

- Bereitstellungsgruppe hinzufügen
- In Bereitstellungsgruppen bereitstellen
- Bereitstellungsgruppe löschen
- Bereitstellungsgruppe barbeiten
- Bereitstellungsgruppe “AllUsers”aktivieren oder deaktivieren

Bereitstellungsgruppe hinzufügen

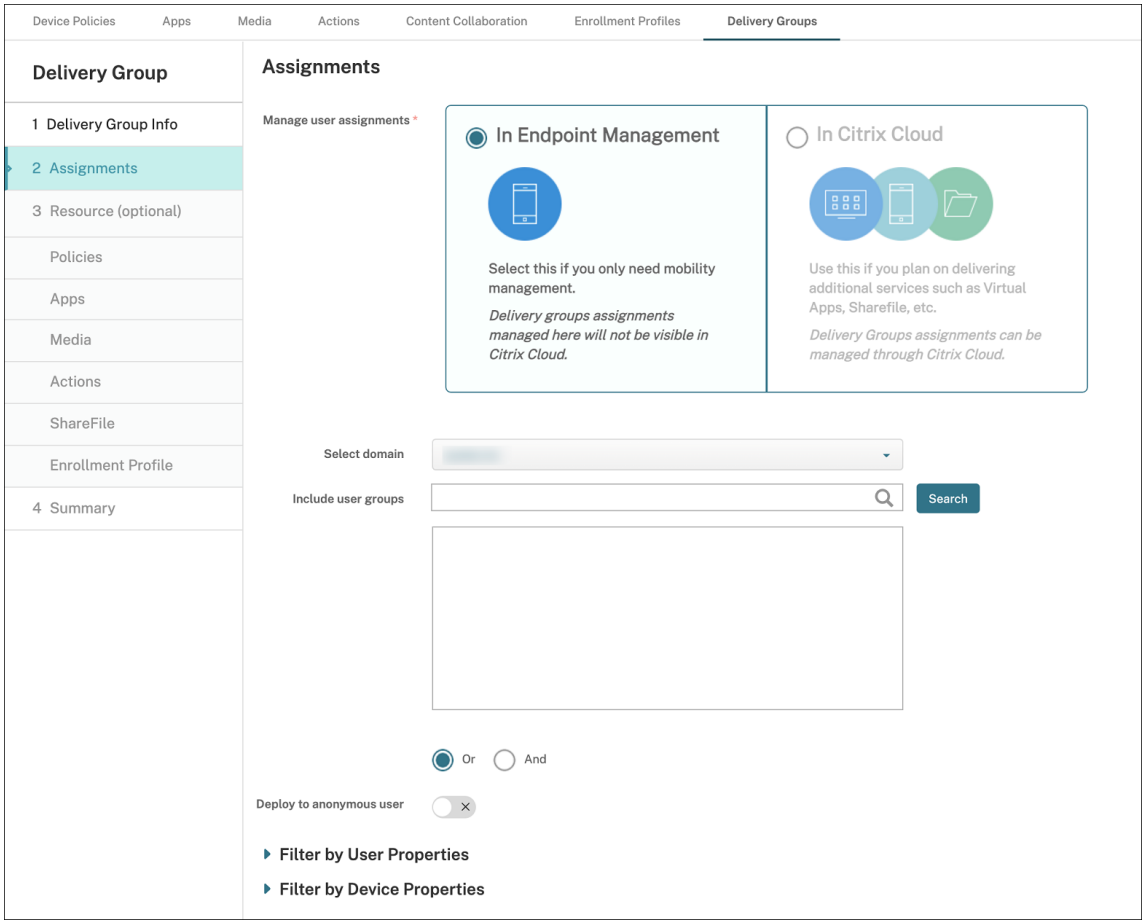
Beim Erstellen einer Bereitstellungsgruppe legen Sie fest, ob die Benutzerzuweisungen in Citrix Endpoint Management oder Citrix Cloud verwaltet werden sollen. Sie können diese Spezifikation nach dem Erstellen der Bereitstellungsgruppe nicht mehr ändern.

Wenn Sie die Bereitstellungsgruppe für die Bereitstellung anderer Citrix Cloud-Dienste verwenden möchten, wählen Sie die Verwaltung der Benutzerzuweisungen in Citrix Cloud aus. Andere Citrix Cloud-Dienste sind u. a. Citrix Virtual Apps and Desktops, ShareFile oder Secure Browser Service. Sie können Active Directory-Benutzer nur zu Bereitstellungsgruppen hinzufügen, die in Citrix Cloud verwaltet werden.

Wenn Sie eine Bereitstellungsgruppe für Benutzer und Apps erstellen, die nur Mobilitätsverwaltung erfordern, wählen Sie für **Benutzerzuweisungen verwalten** die Option **In Citrix Endpoint Management**. Bereitstellungsgruppen mit Benutzern, die in Citrix Endpoint Management verwaltet werden, sind in der Citrix Cloud nicht sichtbar. Daher können Sie keine in Citrix Endpoint Management verwalteten Bereitstellungsgruppen zum Bereitstellen anderer Services verwenden.

> **Hinweis:**
>
> Wir empfehlen, erst Bereitstellungsgruppen hinzuzufügen und dann Geräterichtlinien und Registrierungsprofile zu erstellen. Weitere Informationen, wie Sie diese erstellen, finden Sie unter Geräterichtlinien und Registrierungsprofile.

1. Klicken Sie in der Citrix Endpoint Management-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**.
4. Geben Sie auf der Seite **Zuweisungen** an, wie die Zuweisungen der Bereitstellungsgruppe verwaltet werden sollen.



- **Benutzerzuweisungen verwalten:**
  - **In Citrix Endpoint Management:** Wählen Sie diese Option, um eine Bereitstellungsgruppe für Benutzer und Apps zu erstellen, die nur Mobilitätsverwaltung erfordern. Bereitstellungsgruppen, deren Benutzerzuweisungen in Citrix Endpoint Management verwaltet werden, sind in der Citrix Cloud nicht sichtbar und können nicht zur Bereitstellung anderer Services verwendet werden.
  - **In Citrix Cloud:** Wählen Sie diese Option, wenn Sie die Bereitstellungsgruppe zur Bereitstellung weiterer Services verwenden möchten. Dies können Dienste wie Citrix Virtual Apps and Desktops oder ShareFile sein.

5. Fügen Sie der Bereitstellungsgruppe Benutzer hinzu.

> **Wichtig:**
>
> Sie können die Einstellung **Benutzerzuweisungen verwalten** nach dem Erstellen 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. Sie können auch einen vollständigen oder teilweisen Gruppennamen in das Suchfeld eingeben und dann auf **Suchen** klicken, um Ihre Suche einzugrenzen.

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 jeder Gruppe, die Sie entfernen möchten.
- Klicken Sie auf **Suchen**, um eine Liste aller Benutzergruppen in der ausgewählten Domäne anzuzeigen. Oder geben Sie einen vollständigen oder teilweisen Gruppennamen ein, bevor Sie auf **Suchen** klicken, um Ihre Suche einzugrenzen. Deaktivieren Sie das Kontrollkästchen jeder Gruppe, die Sie entfernen möchten.

- **Oder/Und:** Wählen Sie aus, ob Benutzer für die bereitgestellte Ressource einer einzelnen Gruppe angehören (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 Citrix Endpoint Management gestattet wurde.

6. Erweitern Sie **Nach Benutzereigenschaften filtern** oder **Nach Geräteeigenschaften filtern**, um anzugeben, wie die Bereitstellungsgruppe Ressourcen verwaltet.

   - Wenn Sie **Nach Geräteeigenschaften filtern** wählen, erweitern Sie die Geräteplattform, um die Bereitstellungsregeln zu konfigurieren:
     - **Geräteeigenschaften –Android** (weitere Informationen finden Sie unter Regel zum Bereitstellen von Ressourcen für Android Enterprise erstellen)
     - **Geräteeigenschaften –iOS**
     - **Geräteeigenschaften –nur Windows Desktop/Tablet**
   - Standardmäßig wird die Registerkarte **Basis** angezeigt. Geben Sie auf der Registerkarte **Basis** an, wann die Richtlinie bereitgestellt werden soll. Sie können die Richtlinie bereitstellen, wenn **alle** oder **beliebige** Bedingungen erfüllt sind. Die Standardoption ist auf **Alle**festgelegt.
     - Klicken Sie auf **Neue Regel**, um Bedingungen zu definieren.
     - Wählen Sie in den Listen die Bedingungen aus. Wählen Sie beispielsweise Gerätebesitz und BYOD aus.
     - Klicken Sie für jede Bedingung, die Sie hinzufügen möchten, auf **Neue Regel**.

- 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.
  - Klicken Sie auf **UND**, **ODER** oder **NICHT** und dann auf **Neue Regel**.
  - Wählen Sie in den Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite.
    Sie können jederzeit auf eine Bedingung und dann auf **Bearbeiten** klicken, um die Bedingung zu ändern. Oder klicken Sie auf **Löschen**, um die Bedingung zu entfernen.

7. Klicken Sie auf **Weiter**, um die Seite **Richtlinien** aufzurufen. Hier können Sie für die Bereitstellungsgruppe optional Richtlinien, Apps, Medien oder Aktionen hinzufügen. Einzelheiten finden Sie in den folgenden Abschnitten:

   - Richtlinien zu einer Bereitstellungsgruppe hinzufügen
   - Apps zu einer Bereitstellungsgruppe hinzufügen
   - Medien zu einer Bereitstellungsgruppe hinzufügen
   - Aktionen zu einer Bereitstellungsgruppe hinzufügen

8. Wenn Sie mit Ihrer Bereitstellungsgruppe zufrieden sind, klicken Sie auf **Zusammenfassung**, um eine Zusammenfassung der Konfiguration anzuzeigen.
9. Klicken Sie auf **Speichern**. Die neue Bereitstellungsgruppe wird auf der Seite **Bereitstellungsgruppen** angezeigt.

Richtlinien zu einer Bereitstellungsgruppe hinzufügen

1. Klicken Sie in der Liste **Ressource (optional)** auf **Richtlinien**.
2. 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: Geben Sie den Richtliniennamen vollständig oder teilweise im Suchfeld ein und klicken Sie dann auf **Suchen**.
   - Ziehen Sie die hinzuzufügende Richtlinie in das Feld auf der rechten Seite.

   Um eine Richtlinie aus dem Feld zu entfernen, klicken Sie auf das **X** neben ihrem Namen.

3. Klicken Sie auf **Weiter**, um zur Seite **Apps** zu wechseln.

Apps zu einer Bereitstellungsgruppe hinzufügen

1. Führen Sie für jede hinzuzufügende App die folgenden Schritte durch:

- Suchen Sie die gewünschte App in der Liste der verfügbaren Apps. Alternative: Geben Sie den App-Namen vollständig oder teilweise im Suchfeld ein und klicken Sie dann auf **Suchen**.
- Ziehen Sie die App 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 Citrix Secure Hub-Update.

Weitere Informationen zur erzwungenen Bereitstellung erforderlicher Apps und zur Aktivierung des Features finden Sie unter Erforderliche und optionale Apps.

Um eine App aus dem Feld zu entfernen, klicken Sie auf das **X** neben ihrem Namen.

2. Klicken Sie auf **Weiter**, um zur Seite **Medien** zu wechseln.

Medien zu einer Bereitstellungsgruppe hinzufügen

1. Führen Sie für jedes gewünschte Medium folgende Schritte aus:

   - Suchen Sie das gewünschte Buch in der Liste der verfügbaren Bücher. Alternative: Geben Sie den Buchnamen vollständig oder teilweise im Suchfeld ein und klicken Sie dann auf **Suchen**.
   - Ziehen Sie das hinzuzufügende Buch 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 Citrix Secure Hub-Update.

   Um ein Buch aus dem Feld zu entfernen, klicken Sie auf das **X** neben seinem Namen.

2. Klicken Sie auf **Weiter**, um zur Seite **Aktionen** zu wechseln.

Aktionen zu einer Bereitstellungsgruppe hinzufügen

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: Geben Sie den Aktionsnamen vollständig oder teilweise im Suchfeld ein und klicken Sie dann auf **Suchen**.
- Ziehen Sie die hinzuzufügende Aktion in das Feld auf der rechten Seite.

Um eine Aktion aus dem Feld zu entfernen, klicken Sie auf das **X** neben ihrem Namen.

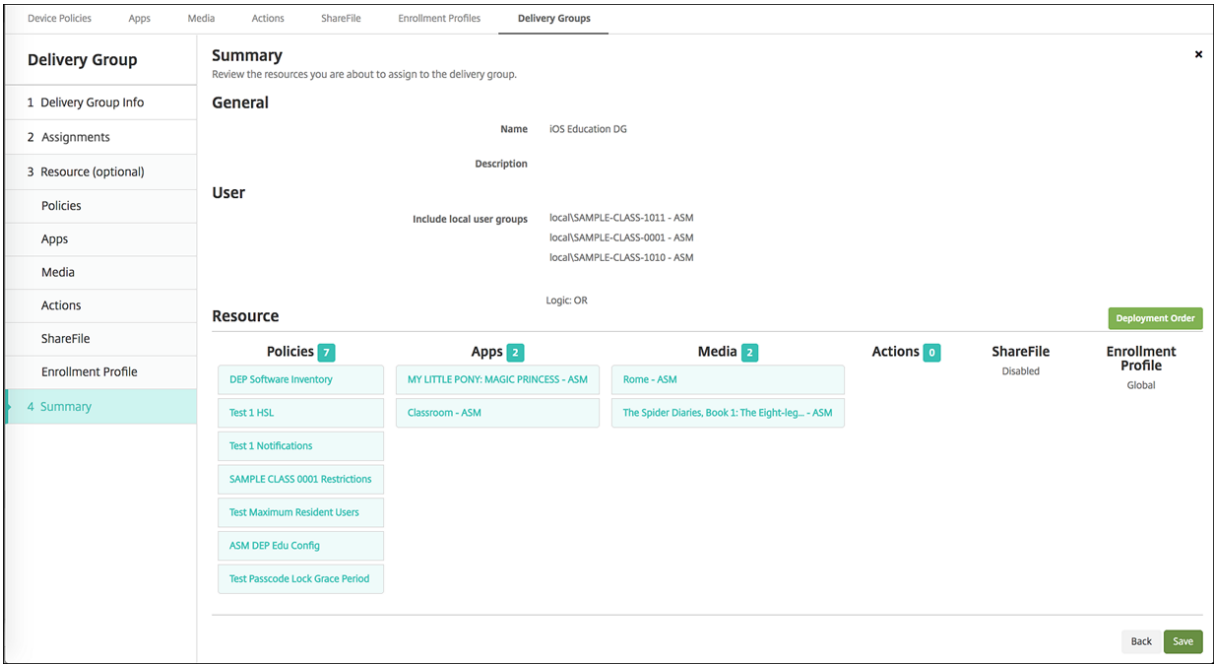
2. Klicken Sie auf **Weiter**, um zur Seite **ShareFile** zu gelangen.

ShareFile-Konfiguration anwenden Die Seite "ShareFile"unterscheidet sich je nachdem, ob Sie Citrix Endpoint Management (**Konfigurieren > ShareFile**) für Enterprise-Konten oder für Speicherzonenconnectors konfiguriert haben.

- Wenn Sie Enterprise-Konten für Citrix Endpoint Management konfiguriert haben, setzen Sie **ShareFile aktivieren** auf **Ein**. Mit dieser Einstellung können Bereitstellungsgruppen per Single Sign-On auf Inhalte und Daten von ShareFile zugreifen.
- Wenn Sie Speicherzonenconnectors für Citrix Endpoint Management konfiguriert haben, ziehen Sie die Speicherzonenconnectors, die in die Bereitstellungsgruppe aufgenommen werden sollen, in das Feld auf der rechten Seite.

Konfigurierte Optionen überprüfen und Bereitstellungsreihenfolge ändern Auf der Seite "Zusammenfassung"können Sie die konfigurierten Optionen für die Bereitstellungsgruppe prüfen und die Bereitstellungsreihenfolge der Ressourcen ändern. Auf der Seite "Zusammenfassung" werden die Ressourcen nach Kategorie angezeigt. Auf der Seite "Zusammenfassung"wird die Bereitstellungsreihenfolge nicht angezeigt.

> **Hinweis:**
>
> Klicken Sie auf **Zurück**, um zu vorherigen Seiten zurückzukehren und die Konfiguration zu ändern.

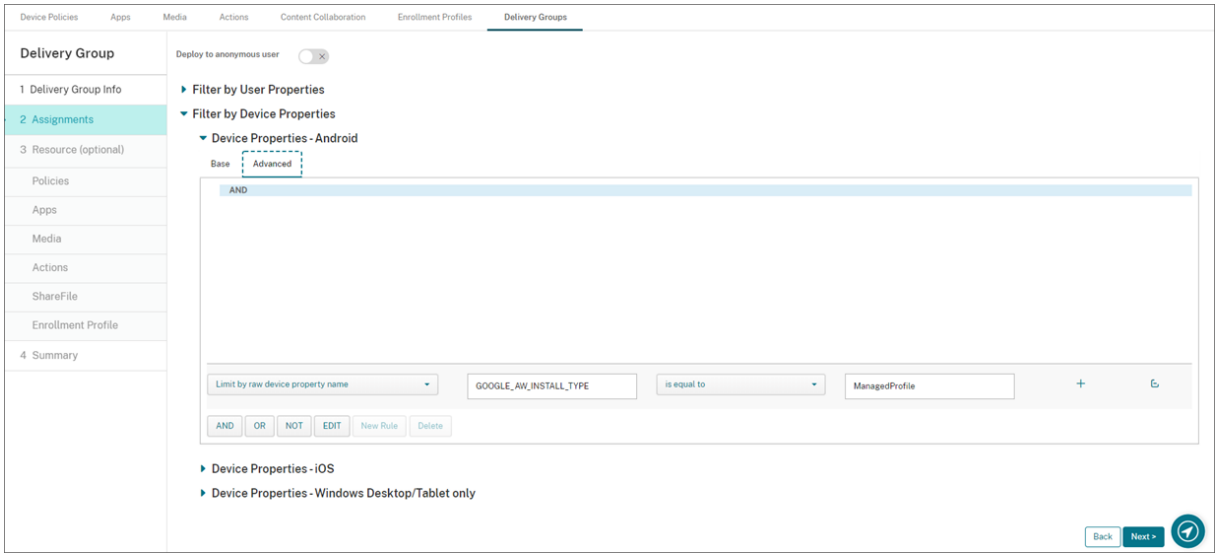


Bereitstellungsreihenfolge anzeigen oder ändern:

1. Klicken Sie auf **Bereitstellungsreihenfolge**.
2. Ziehen Sie im Dialogfeld "Bereitstellungsreihenfolge"eine Ressource an die Stelle in der Reihenfolge, an der Sie sie bereitstellen möchten. Die Ressourcen werden in der angegebenen Reihenfolge von oben nach unten bereitgestellt.
3. Klicken Sie auf **Speichern**, um die Bereitstellungsreihenfolge zu speichern.

Wenn Sie mit der Konfiguration der Bereitstellungsgruppe fertig sind, klicken Sie auf der Seite "Zusammenfassung"auf **Speichern**.

Regel zum Bereitstellen von Ressourcen für Android Enterprise erstellen Mit den Eigenschaftsregeln für Android-Geräte können Sie die Bereitstellung einer Bereitstellungsgruppe für Android Enterprise-Geräte verwalten. Wenn Sie mehrere Geräte für denselben Benutzer registrieren, können Sie erweiterte Filter für Android Enterprise erstellen, basierend auf dem Geräteregistrierungsmodus oder der Anwendungspaket-ID des Geräts.



Bereitstellungsgruppe auf Android Enterprise-Geräten mit dem Geräteregistrierungsmodus bereitstellen:

1. Erstellen Sie eine Bereitstellungsgruppe.
2. Erweitern Sie auf der Seite **Zuweisungen** den Eintrag **Nach Geräteeigenschaften filtern**.
3. Öffnen Sie unter **Geräteeigenschaften** —**Android** die Registerkarte **Erweitert** und klicken Sie auf **Neue Regel**.
4. Wählen Sie in der Liste die Bedingung aus, die der Regel hinzugefügt werden soll:
    - Wählen Sie für neue Android Enterprise-Geräte die Option **Durch rohen Geräteeigenschaftsnamen beschränken** und geben Sie im ersten Wertefeld **GOOGLE_AW_INSTALL_TYPE** ein. Legen Sie dann die Bedingung fest, die einem der Registrierungsmodi entspricht.
    - Wählen Sie für vorhandene Android Enterprise-Geräte die Option **Durch bekannten Geräteeigenschaftsnamen beschränken** und wählen Sie im ersten Wertefeld **Android Enterprise - Installationstyp**. Legen Sie dann die Bedingung fest, die einem der Registrierungsmodi entspricht.
5. Geben Sie im zweiten Feld einen Registrierungsmodus für Ihre Android Enterprise-Geräte ein:
    - **DeviceAdministrator:** Legt unternehmenseigene Geräte fest, die nur für Arbeitszwecke zu verwenden sind (auch als Gerätebesitzermodus bezeichnet)
    - **ManagedProfile:** Legt BYOD-Geräte fest, also Privatgeräte, die für Arbeitszwecke verwendet werden, und die mit Arbeitsprofilverwaltung registriert sind (auch als Profilbesitzermodus bezeichnet)
    - **CorporateOwnedSingleUse:** Legt dedizierte Geräte fest (früher COSU-Geräte: unternehmenseigene Einzweckgeräte)
    - **CorporateOwnedPersonallyEnabled:** Legt vollständig verwaltete Geräte mit Arbeitsprofil fest (früher COPE-Geräte: Unternehmenseigentum, vom Benutzer verwaltet)

6. Schließen Sie das Konfigurieren der Bereitstellungsgruppe wie unter Hinzufügen einer Bereitstellungsgruppe beschrieben ab.

   Weitere Informationen finden Sie unter Szenarien und Profile für die Gerätebereitstellung.

Bereitstellungsgruppe auf Android Enterprise-Geräten mit der Anwendungspaket-ID des Geräts bereitstellen:

1. Öffnen Sie unter **Geräteeigenschaften** —**Android** die Registerkarte **Erweitert** und klicken Sie auf **Neue Regel**.
2. Wählen Sie in der Liste **Name der installierten App** und geben Sie die Anwendungspaket-ID ein.

Bereitstellungsgruppe barbeiten

Sie können den Namen einer vorhandenen Bereitstellungsgruppe nicht ändern. Zum Aktualisieren anderer Einstellungen wählen Sie unter **Konfigurieren > Bereitstellungsgruppen** die gewünschte Gruppe und klicken Sie auf **Bearbeiten**.

Bereitstellungsgruppe “AllUsers”aktivieren oder deaktivieren

“AllUsers”ist die einzige Bereitstellungsgruppe, die Sie aktivieren oder deaktivieren können. Sie können “AllUsers”nicht wie andere Bereitstellungsgruppen löschen.

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 dann verfügbar, wenn die Gruppe “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 dann verfügbar, wenn die Gruppe “AllUsers”deaktiviert ist. **Deaktiviert** wird nicht länger unter der Überschrift **Deaktiviert** in der Tabelle der Bereitstellungsgruppen angezeigt.

In Bereitstellungsgruppen bereitstellen

Das Bereitstellen in einer Bereitstellungsgruppe bedeutet, dass eine Pushbenachrichtigung an alle Benutzer mit Apple-, Android- und Windows Tablet-Geräten gesendet wird.

Für Benutzer anderer Geräteplattformen gilt: Sind diese Geräte bereits mit Citrix Endpoint Management 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 App-Store auf Android-Geräten angezeigt werden, stellen Sie auf den Benutzergeräten 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.

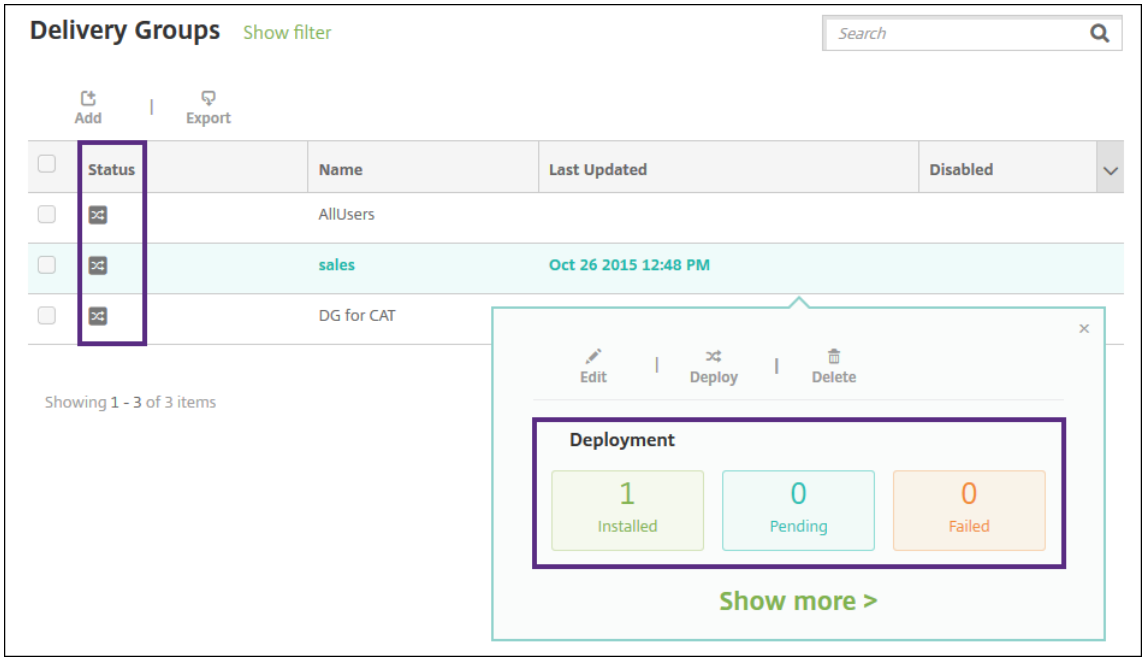
2. Klicken Sie auf **Bereitstellen**.

    Der Befehl **Bereitstellen** wird je nach Auswahl der einzelnen Bereitstellungsgruppen oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

    Stellen Sie sicher, dass die Gruppen, für die Sie Apps, Richtlinien und Aktionen bereitstellen möchten, aufgelistet sind. 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.



Bereitstellungsgruppe klonen

Klonen Sie eine Bereitstellungsgruppe, um eine Bereitstellungsgruppe zu erstellen, die einer vorhandenen ähnelt. Der Klon dient dann als Ausgangspunkt für die neue Bereitstellungsgruppe. Durch Hinzufügen von Registrierungsprofilen oder neuen Gruppen von AD-Benutzern können Sie den Klon nach dem Erstellen anpassen.

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren** und wählen Sie die Registerkarte **Bereitstellungsgruppen**.
2. Wählen Sie aus der Liste der Bereitstellungsgruppen diejenige aus, die Sie als Basis für die neue Gruppe verwenden möchten.
3. Wählen Sie **Klonen**.
4. Geben Sie im Dialogfeld “Klonen einer Bereitstellungsgruppe”den Namen der neuen Gruppe und optional eine Beschreibung ein.
5. Wählen Sie **Klonen**.

Bereitstellungsgruppen löschen

Die Bereitstellungsgruppe “AllUsers”kann nicht gelöscht werden, Sie können sie jedoch deaktivieren, wenn Sie Ressourcen nicht per Push für alle Benutzer bereitstellen möchten. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der Bereitstellungsgruppe “AllUsers”.

> **Wichtig:**
>
> Sie können einen Löschvorgang nicht rückgängig machen.

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**.

   Der Befehl **Löschen** wird je nach Auswahl der einzelnen Bereitstellungsgruppen oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.
3. Klicken Sie im Dialogfeld **Löschen** auf **Löschen**.

Bereitstellungsgruppentabelle exportieren

1. Klicken Sie auf **Exportieren** oberhalb der Tabelle **Bereitstellungsgruppen**. Citrix Endpoint Management extrahiert die Informationen in die Tabelle **Bereitstellungsgruppen** und konvertiert sie in eine CSV-Datei.
2. Öffnen oder speichern Sie die CSV-Datei mit dem bei Ihrem Browser üblichen Verfahren.

Makros

March 11, 2024

Citrix Endpoint Management bietet Makros zum Eintragen von Benutzer- und Geräteeigenschaften im Textfeld folgender Elemente:

- Richtlinien
- Benachrichtigungen
- Registrierungsvorlagen
- XML-Datei zur Gerätekonfiguration
- Automatisierte Aktionen
- Zertifikatsignieranforderungen für Anmeldeinformationsanbieter

Citrix Endpoint Management 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)] }`

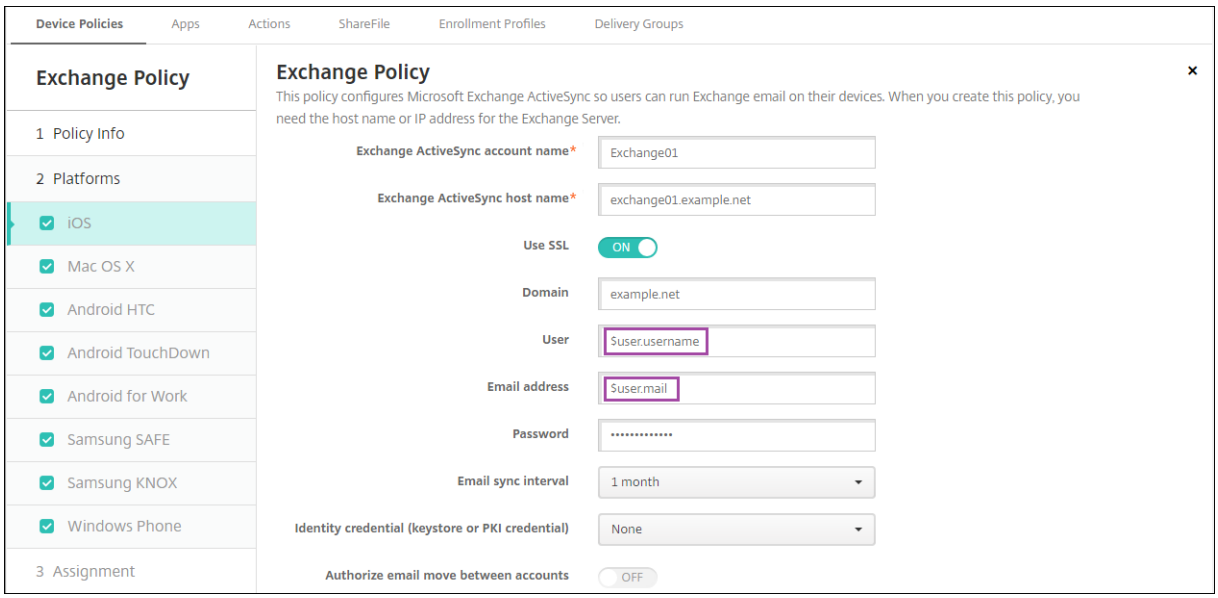
Umschließen Sie den gesamten Teil nach dem Dollarzeichen ($) mit geschweiften Klammern ({}).

- 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`:

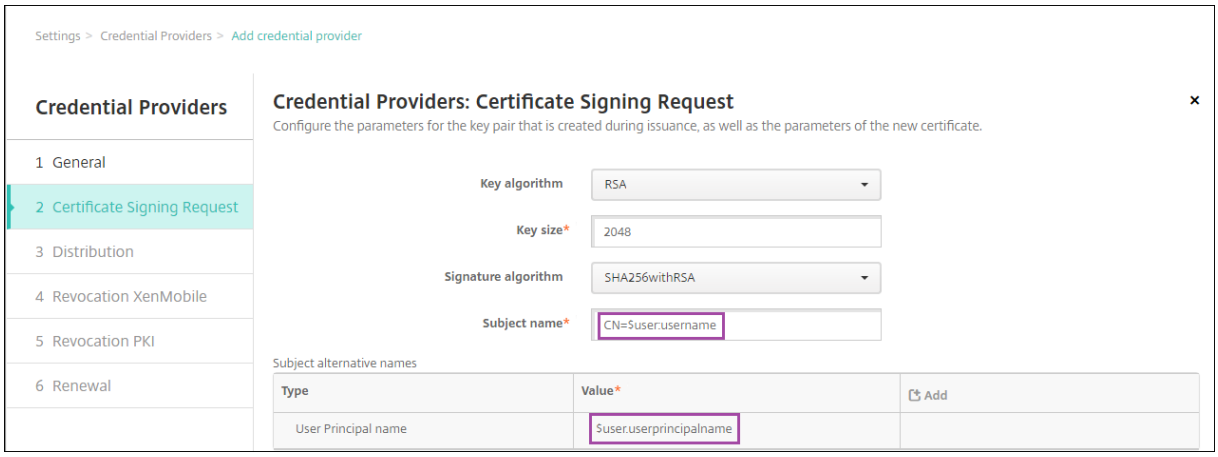
Gerät `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` wurde gesperrt...

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

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 }`.

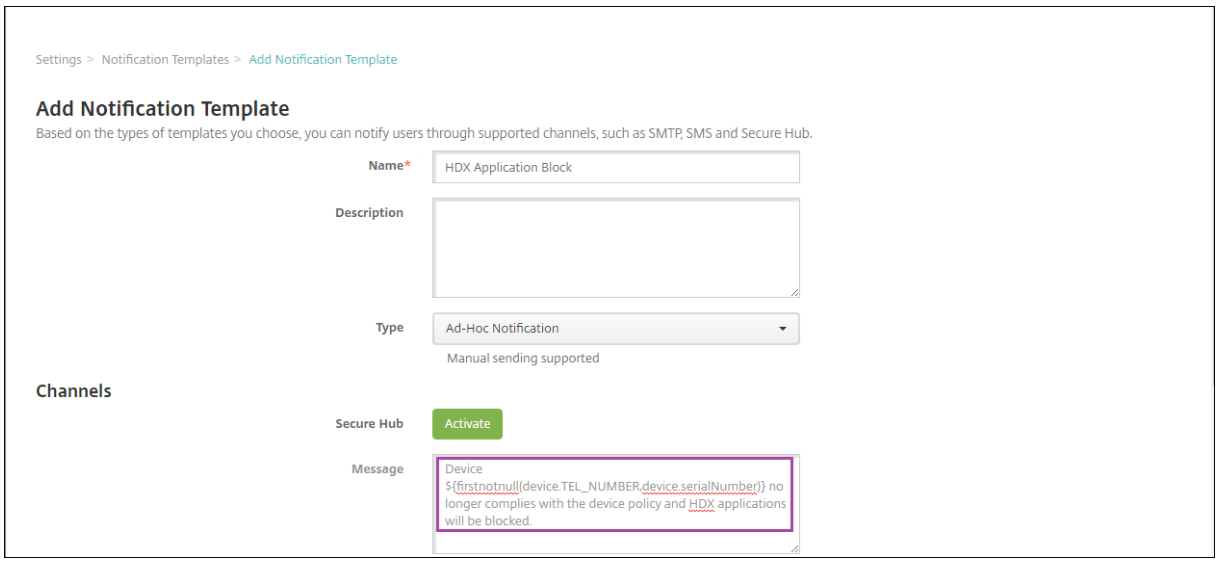


Das folgende Beispiel zeigt, wie Makros für eine Zertifikatsignieranforderung verwendet werden. Das Makro für **Antragstellername** ist **CN=$user.username**. Das Makro für den **Wert** von **Alternativer Antragstellername** ist **$user.userprincipalname**.



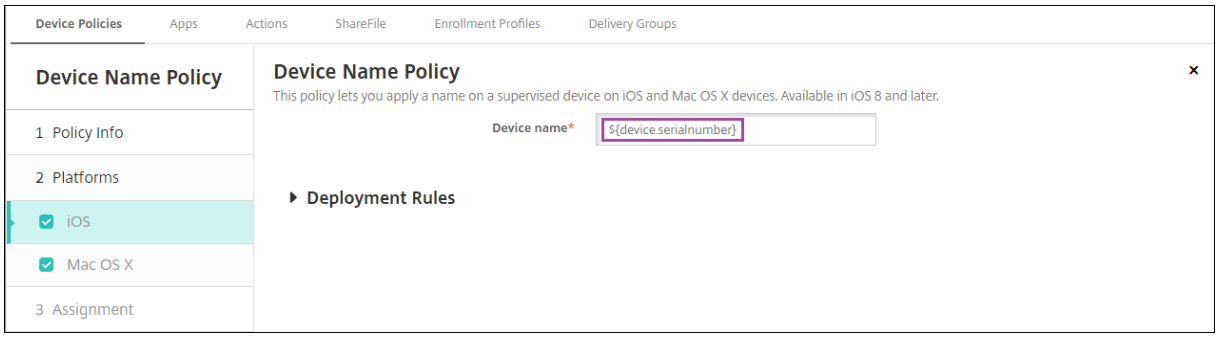
Das folgende Beispiel zeigt, wie Makros in einer Benachrichtigungsvorlage verwendet werden. Die Vorlage in dem Beispiel definiert die Nachricht, die an Benutzer gesendet wird, wenn HDX-Anwendungen aufgrund mangelnder Richtlinientreue des Geräts blockiert werden. Das Makro für **Meldung** ist:

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:

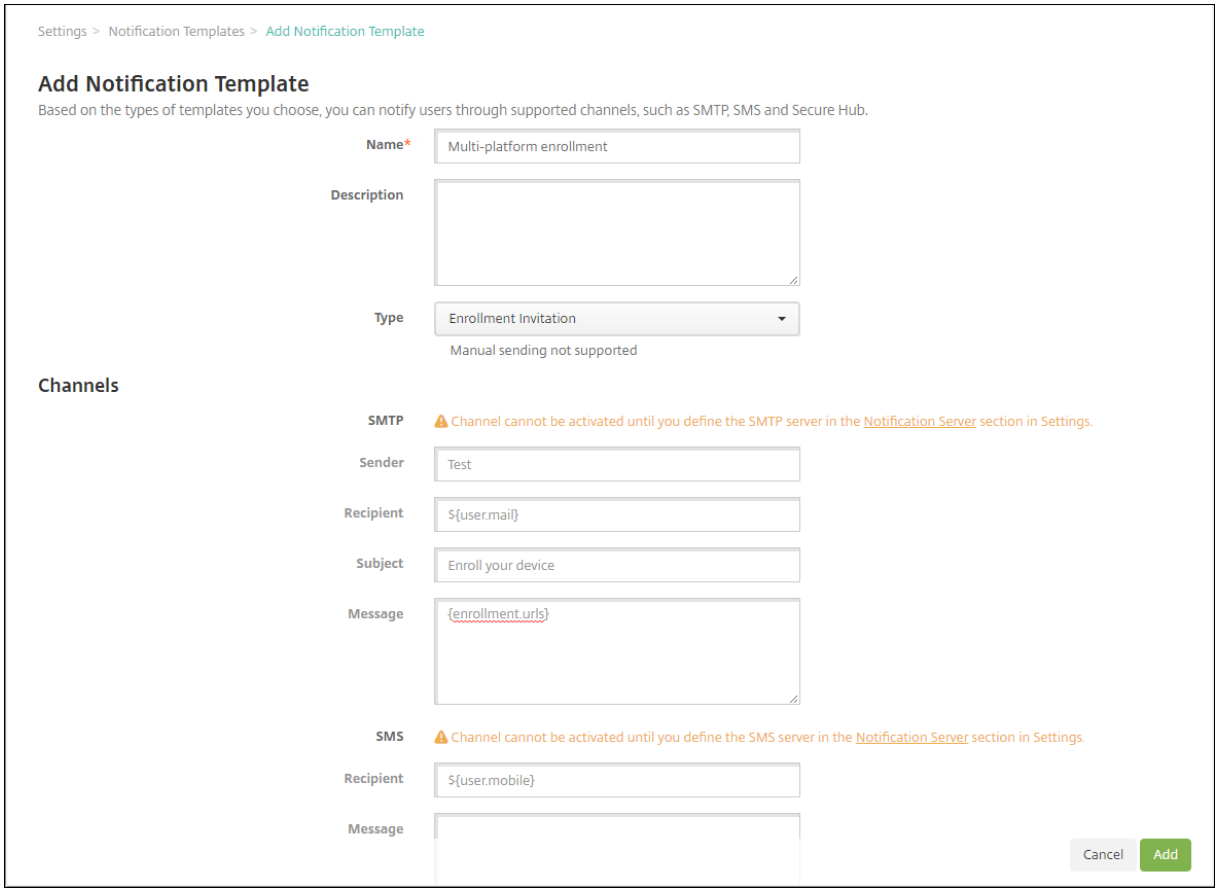
- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`

- ${ 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)}
- ${ vpp.account }
- ${ vpp.appname }
- ${ vpp.url }
- ${ zdmserver.hostPath } /enroll

> **Hinweis:**
>
> Die Citrix Endpoint Management-Konsole enthält im Englischen die Begriffe “Blacklist”und “Whitelist”. Diese Bezeichnungen werden demnächst geändert. Die deutschen Begriffe (Positiv- und Sperrliste) bleiben unverändert.

Das nachstehende Beispiel zeigt, wie Sie eine Benachrichtigung erstellen, die Registrierungs-URLs für mehrere Geräteplattformen enthält. Das Makro für **Meldung** ist:

${enrollment.urls}



Die nachstehenden Beispiele zeigen, wie Sie Text für Benachrichtigungen erstellen, der die Benutzer zum Klicken auf die Registrierungs-URL für ihre Geräteplattform auffordert:

Beispiel 1:

```
To enroll, click the link below that applies to your device platform:

${
 enrollment.ios.platform }
  - ${
 enrollment.ios.url }


${
 enrollment.macos.platform }
  - ${
 enrollment.macos.url }


${
 enrollment.android.platform }
  - ${
 enrollment.android.url }

```



```
<!--NeedCopy-->
```

Beispiel 2:

```
To enroll an iOS device, click the link ${
 enrollment.ios.url }
 .

To enroll a macOS device, click the link ${
 enrollment.macos.url }
 .

To enroll an Android device, click the link ${
 enrollment.android.url }
 .

<!--NeedCopy-->
```

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 }`

In der Mobilfunkrichtlinie für iOS-Geräte können Sie Makros für Werte in Feldern, die keine Zeichenfolgefelder sind (z. B. für den Proxyserverport), verwenden. Beispielsweise können Sie ein Makro wie `${ device.xyz }` oder `${ setting.xyz }` verwenden, das in eine Ganzzahl erweitert wird.

Sie können die Makros auch für Felder in einer XML-Datei zu Gerätekonfiguration, die keine Zeichenfolgen sind, verwenden, die Sie mit der Geräterichtlinie **iOS- und macOS-Profilimport** in Citrix Endpoint Management importieren.

Bei der Geräterichtlinie für Samsung MDM-Lizenzschlüssel können Sie dieses Makro für den **ELM-Lizenzschlüssel** verwenden:

- `${ elm.license.key }`

Bei der Webclip-Geräterichtlinie können Sie folgendes Makro für die **URL** verwenden:

- `${ webeas-url }`

Makros zum Abrufen integrierter Geräteeigenschaften

Anzeigename	Makros
Geräte-ID	`$device.id`
Geräte-GUID	`$device.uniqueid`
Geräte-IMEI	`$device.imei`
OS-Familie	`$device.OSFamily`
Seriennummer	`$device.serialNumber`

Makros für alle Geräteeigenschaften

Anzeigename: Konto vorübergehend gesperrt?

- **Webelement:** `GOOGLE_AW_DIRECTORY_SUSPENDED`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_SUSPENDED }`

Anzeigename: Code zum Umgehen der Aktivierungssperre

- **Webelement:** `ACTIVATION_LOCK_BYPASS_CODE`
- **Makros:** `${ device.ACTIVATION_LOCK_BYPASS_CODE }`

Anzeigename: Aktivierungssperre aktiviert

- **Webelement:** `ACTIVATION_LOCK_ENABLED`
- **Makros:** `${ device.ACTIVATION_LOCK_ENABLED }`

Anzeigename: Aktives Apple App Store-Konto

- **Webelement:** `ACTIVE_ITUNES`
- **Makros:** `${ device.ACTIVE_ITUNES }`

Anzeigename: Administrator deaktiviert

- **Webelement:** `ADMIN_DISABLED`
- **Makros:** `${ device.ADMIN_DISABLED }`

Anzeigename: AIK Present?

- **Webelement:** `WINDOWS_HAS_AIK_PRESENT`

- **Makros:** `${ device.WINDOWS_HAS_AIK_PRESENT }`

Anzeigename: Amazon MDM-API verfügbar

- **Webelement:** `AMAZON_MDM`
- **Makros:** `${ device.AMAZON_MDM }`

Anzeigename: Android Enterprise-Geräte-ID

- **Webelement:** `GOOGLE_AW_DEVICE_ID`
- **Makros:** `${ device.GOOGLE_AW_DEVICE_ID }`

Anzeigename: Android Enterprise-fähiges Gerät?

- **Webelement:** `GOOGLE_AW_ENABLED_DEVICE`
- **Makros:** `${ device.GOOGLE_AW_ENABLED_DEVICE }`

Anzeigename: Android Enterprise-Installationstyp

- **Webelement:** `GOOGLE_AW_INSTALL_TYPE`
- **Makros:** `${ device.GOOGLE_AW_INSTALL_TYPE }`

Anzeigename: Status der Antispywaresignatur

- **Webelement:** `ANTI_SPYWARE_SIGNATURE_STATUS`
- **Makros:** `${ device.ANTI_SPYWARE_SIGNATURE_STATUS }`

Anzeigename: Antispywarestatus

- **Webelement:** `ANTI_SPYWARE_STATUS`
- **Makros:** `${ device.ANTI_SPYWARE_STATUS }`

Anzeigename: Status der Antivirenprogrammsignatur

- **Webelement:** `ANTI_VIRUS_SIGNATURE_STATUS`
- **Makros:** `${ device.ANTI_VIRUS_SIGNATURE_STATUS }`

Anzeigename: Antivirusstatus

- **Webelement:** `ANTI_VIRUS_STATUS`
- **Makros:** `${ device.ANTI_VIRUS_STATUS }`

Anzeigename: Code zum Umgehen der Aktivierungssperre für ASM-Bereitstellungsprogramm

- **Webelement:** `DEP_ACTIVATION_LOCK_BYPASS_CODE`

- **Makros:** `${ device.DEP_ACTIVATION_LOCK_BYPASS_CODE }`

Anzeigename: Hinterlegter Schlüssel für ASM-Bereitstellungsprogramm

- **Webelement:** `DEP_ESCROW_KEY`
- **Makros:** `${ device.DEP_ESCROW_KEY }`

Anzeigename: Bestandskennzeichen

- **Webelement:** `ASSET_TAG`
- **Makros:** `${ device.ASSET_TAG }`

Anzeigename: Automatisch auf Softwareupdates prüfen

- **Webelement:** `AutoCheckEnabled`
- **Makros:** `${ device.AutoCheckEnabled }`

Anzeigename: Softwareupdates im Hintergrund automatisch herunterladen

- **Webelement:** `BackgroundDownloadEnabled`
- **Makros:** `${ device.BackgroundDownloadEnabled }`

Anzeigename: App-Updates automatisch installieren

- **Webelement:** `AutomaticAppInstallationEnabled`
- **Makros:** `${ device.AutomaticAppInstallationEnabled }`

Anzeigename: OS-Updates automatisch installieren

- **Webelement:** `AutomaticOSInstallationEnabled`
- **Makros:** `${ device.AutomaticOSInstallationEnabled }`

Anzeigename: Sicherheitsupdates automatisch installieren

- **Webelement:** `AutomaticSecurityUpdatesEnabled`
- **Makros:** `${ device.AutomaticSecurityUpdatesEnabled }`

Anzeigename: Status für automatische Updates

- **Webelement:** `AUTOUPDATE_STATUS`
- **Makros:** `${ device.AUTOUPDATE_STATUS }`

Anzeigename: Verfügbarer RAM

- **Webelement:** `MEMORY_AVAILABLE`

- **Makros:** `${ device.MEMORY_AVAILABLE }`

Anzeigename: Verfügbare Softwareupdates

- **Webelement:** `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- **Makros:** `${ device.AVAILABLE_OS_UPDATE_HUMAN_READABLE }`

Anzeigename: Verfügbarer Speicherplatz

- **Webelement:** `FREEDISK`
- **Makros:** `${ device.FREEDISK }`

Anzeigename: Backupakku

- **Webelement:** `BACKUP_BATTERY_PERCENT`
- **Makros:** `${ device.BACKUP_BATTERY_PERCENT }`

Anzeigename: Basisbandfirmwareversion

- **Webelement:** `MODEM_FIRMWARE_VERSION`
- **Makros:** ‘${device.MODEM_FIRMWARE_VERSION}

Anzeigename: Akku wird geladen

- **Webelement:** `BATTERY_CHARGING_STATUS`
- **Makros:** `${ device.BATTERY_CHARGING_STATUS }`

Anzeigename: Akku wird geladen

- **Webelement:** `BATTERY_CHARGING`
- **Makros:** `${ device.BATTERY_CHARGING }`

Anzeigename: Verbleibender Akku

- **Webelement:** `BATTERY_ESTIMATED_CHARGE_REMAINING`
- **Makros:** `${ device.BATTERY_ESTIMATED_CHARGE_REMAINING }`

Anzeigename: Akkulaufzeit

- **Webelement:** `BATTERY_RUNTIME`
- **Makros:** `${ device.BATTERY_RUNTIME }`

Anzeigename: Akkustatus

- **Webelement:** `BATTERY_STATUS`

- **Makros:** `${ device.BATTERY_STATUS }`

Anzeigename: BES-PIN

- **Webelement:** `BES_PIN`
- **Makros:** `${ device.BES_PIN }`

Anzeigename: Agent-ID für BES-Server

- **Webelement:** `AGENT_ID`
- **Makros:** `${ device.AGENT_ID }`

Anzeigename: BES-Servername

- **Webelement:** `BES_SERVER`
- **Makros:** `${ device.BES_SERVER }`

Anzeigename: BES-Serverversion

- **Webelement:** `BES_VERSION`
- **Makros:** `${ device.BES_VERSION }`

Anzeigename: BIOS-Info

- **Webelement:** `BIOS_INFO`
- **Makros:** `${ device.BIOS_INFO }`

Anzeigename: BitLocker-Status

- **Webelement:** `WINDOWS_HAS_BIT_LOCKER_STATUS`
- **Makros:** `${ device.WINDOWS_HAS_BIT_LOCKER_STATUS }`

Anzeigename: Bluetooth-MAC-Adresse

- **Webelement:** `BLUETOOTH_MAC`
- **Makros:** `${ device.BLUETOOTH_MAC }`

Anzeigename: Boot Debugging Enabled?

- **Webelement:** `WINDOWS_HAS_BOOT_DEBUGGING_ENABLED`
- **Makros:** `${ device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED }`

Anzeigename: Boot Manager Rev List Version

- **Webelement:** `WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION`

- **Makros:** `${ device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION }`

Anzeigename: Code des Netzbetreibers

- **Webelement:** `CARRIER_CODE`
- **Makros:** `${ device.CARRIER_CODE }`

Anzeigename: Version der Netzbetreibereinstellungen

- **Webelement:** `CARRIER_SETTINGS_VERSION`
- **Makros:** `${ device.CARRIER_SETTINGS_VERSION }`

Anzeigename: Katalog-URL

- **Webelement:** `CatalogURL`
- **Makros:** `${ device.CatalogURL }`

Anzeigename: Mobilnetzhöhenwert

- **Webelement:** `GPS_ALTITUDE_FROM_CELLULAR`
- **Makros:** `${ device.GPS_ALTITUDE_FROM_CELLULAR }`

Anzeigename: Mobilnetz - Kurs

- **Webelement:** `GPS_COURSE_FROM_CELLULAR`
- **Makros:** `${ device.GPS_COURSE_FROM_CELLULAR }`

Anzeigename: Mobilnetz - horizontale Genauigkeit

- **Webelement:** `GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`
- **Makros:** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR }`

Anzeigename: Mobilnetzbreitengrad

- **Webelement:** `GPS_LATITUDE_FROM_CELLULAR`
- **Makros:** `${ device.GPS_LATITUDE_FROM_CELLULAR }`

Anzeigename: Mobilnetzlängengrad

- **Webelement:** `GPS_LONGITUDE_FROM_CELLULAR`
- **Makros:** `${ device.GPS_LONGITUDE_FROM_CELLULAR }`

Anzeigename: Mobilnetz - Geschwindigkeit

- **Webelement:** `GPS_SPEED_FROM_CELLULAR`

- **Makros:** `${ device.GPS_SPEED_FROM_CELLULAR }`

Anzeigename: Mobilnetztechnologie

- **Webelement:** `CELLULAR_TECHNOLOGY`
- **Makros:** `${ device.CELLULAR_TECHNOLOGY }`

Anzeigename: Mobilnetzzeitstempel

- **Webelement:** `GPS_TIMESTAMP_FROM_CELLULAR`
- **Makros:** `${ device.GPS_TIMESTAMP_FROM_CELLULAR }`

Anzeigename: Mobilnetz - vertikale Genauigkeit

- **Webelement:** `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- **Makros:** `${ device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR }`

Anzeigename: Kennwort bei nächster Anmeldung ändern?

- **Webelement:** `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- **Makros:** ‘${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

Anzeigename: Clientgeräte-ID

- **Webelement:** `CLIENT_DEVICE_ID`
- **Makros:** `${ device.CLIENT_DEVICE_ID }`

Anzeigename: Cloudbackup aktiviert

- **Webelement:** `CLOUD_BACKUP_ENABLED`
- **Makros:** `${ device.CLOUD_BACKUP_ENABLED }`

Anzeigename: Code Integrity Enabled?

- **Webelement:** `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- **Makros:** `${ device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED }`

Anzeigename: Code Integrity Rev List Version

- **Webelement:** `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- **Makros:** `${ device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION }`

Anzeigename: Farbe

- **Webelement:** `COLOR`

- **Makros:** `${ device.COLOR }`

Anzeigename: CPU-Taktfrequenz

- **Webelement:** `CPU_CLOCK_SPEED`
- **Makros:** `${ device.CPU_CLOCK_SPEED }`

Anzeigename: CPU-Typ

- **Webelement:** `CPU_TYPE`
- **Makros:** `${ device.CPU_TYPE }`

Anzeigename: Erstellungszeit

- **Webelement:** `GOOGLE_AW_DIRECTORY_CREATION_TIME`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_CREATION_TIME }`

Anzeigename: Kritische Softwareupdates

- **Webelement:** `AVAILABLE_OS_UPDATE_IS_CRITICAL`
- **Makros:** `${ device.AVAILABLE_OS_UPDATE_IS_CRITICAL }`

Anzeigename: Aktuelles Betreibernetzwerk

- **Webelement:** `CARRIER`
- **Makros:** `${ device.CARRIER }`

Anzeigename: Aktueller Ländercode für mobiles Gerät

- **Webelement:** `CURRENT_MCC`
- **Makros:** `${ device.CURRENT_MCC }`

Anzeigename: Code für aktuelles mobiles Netzwerk

- **Webelement:** `CURRENT_MNC`
- **Makros:** `${ device.CURRENT_MNC }`

Anzeigename: Datenroaming zugelassen

- **Webelement:** `DATA_ROAMING_ENABLED`
- **Makros:** `${ device.DATA_ROAMING_ENABLED }`

Anzeigename: Datum des letzten iCloud-Backups

- **Webelement:** `LAST_CLOUD_BACKUP_DATE`

- **Makros:** `${ device.LAST_CLOUD_BACKUP_DATE }`

Anzeigename: Standardkatalog

- **Webelement:** `IsDefaultCatalog`
- **Makros:** `${ device.IsDefaultCatalog }`

Anzeigename: Kontoname für Apple-Bereitstellungsprogramm

- **Webelement:** `BULK_ENROLLMENT_DEP_ACCOUNT_NAME`
- **Makros:** `${ device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME }`

Anzeigename: Richtlinie für Apple-Bereitstellungsprogramm

- **Webelement:** `WINDOWS_HAS_DEP_POLICY`
- **Makros:** `${ device.WINDOWS_HAS_DEP_POLICY }`

Anzeigename: Profil für Apple-Bereitstellungsprogramm zugewiesen

- **Webelement:** `PROFILE_ASSIGN_TIME`
- **Makros:** `${ device.PROFILE_ASSIGN_TIME }`

Anzeigename: Profil für Apple-Bereitstellungsprogramm per Push bereitgestellt

- **Webelement:** `PROFILE_PUSH_TIME`
- **Makros:** `${ device.PROFILE_PUSH_TIME }`

Anzeigename: Profil für Apple-Bereitstellungsprogramm entfernt

- **Webelement:** `PROFILE_REMOVE_TIME`
- **Makros:** `${ device.PROFILE_REMOVE_TIME }`

Anzeigename: Registrierung bei Apple-Bereitstellungsprogramm durch

- **Webelement:** `DEVICE_ASSIGNED_BY`
- **Makros:** `${ device.DEVICE_ASSIGNED_BY }`

Anzeigename: Registrierungsdatum für Apple-Bereitstellungsprogramm

- **Webelement:** `DEVICE_ASSIGNED_DATE`
- **Makros:** `${ device.DEVICE_ASSIGNED_DATE }`

Anzeigename: Beschreibung

- **Webelement:** `DESCRIPTION`

- **Makros:** `${ device.DESCRIPTION }`

Anzeigename: Gerätemodell

- **Webelement:** `SYSTEM_OEM`
- **Makros:** `${ device.SYSTEM_OEM }`

Anzeigename: Gerätename

- **Webelement:** `DEVICE_NAME`
- **Makros:** `${ device.DEVICE_NAME }`

Anzeigename: Gerätetyp

- **Webelement:** `DEVICE_TYPE`
- **Makros:** `${ device.DEVICE_TYPE }`

Anzeigename: ‘Nicht stören’aktiviert

- **Webelement:** `DO_NOT_DISTURB`
- **Makros:** `${ device.DO_NOT_DISTURB }`

Anzeigename: ELAM Driver Loaded?

- **Webelement:** `WINDOWS_HAS_ELAM_DRIVER_LOADED`
- **Makros:** `${ device.WINDOWS_HAS_ELAM_DRIVER_LOADED }`

Anzeigename: Verschlüsselungscompliance

- **Webelement:** `ENCRYPTION_COMPLIANCE`
- **Makros:** `${ device.ENCRYPTION_COMPLIANCE }`

Anzeigename: ENROLLMENT_KEY_GENERATION_DATE

- **Webelement:** `ENROLLMENT_KEY_GENERATION_DATE`
- **Makros:** `${ device.ENROLLMENT_KEY_GENERATION_DATE }`

Anzeigename: Unternehmens-ID

- **Webelement:** `ENTERPRISEID`
- **Makros:** `${ device.ENTERPRISEID }`

Anzeigename: Externer Speicher 1: Verfügbarer Speicherplatz

- **Webelement:** `EXTERNAL_STORAGE1_FREE_SPACE`

- **Makros:** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

Anzeigename: Externer Speicher 1: Verfügbarer Speicherplatz

- **Webelement:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Makros:** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

Anzeigename: Externer Speicher 1: Name

- **Webelement:** `EXTERNAL_STORAGE1_NAME`
- **Makros:** `${ device.EXTERNAL_STORAGE1_NAME }`

Anzeigename: Externer Speicher 1: Gesamtspeicherplatz

- **Webelement:** `EXTERNAL_STORAGE1_TOTAL_SPACE`
- **Makros:** `${ device.EXTERNAL_STORAGE1_TOTAL_SPACE }`

Anzeigename: Externer Speicher 2: Verfügbarer Speicherplatz

- **Webelement:** `EXTERNAL_STORAGE2_FREE_SPACE`
- **Makros:** `${ device.EXTERNAL_STORAGE2_FREE_SPACE }`

Anzeigename: Externer Speicher 2: Name

- **Webelement:** `EXTERNAL_STORAGE2_NAME`
- **Makros:** `${ device.EXTERNAL_STORAGE2_NAME }`

Anzeigename: Externer Speicher 2: Gesamtspeicherplatz

- **Webelement:** `EXTERNAL_STORAGE2_TOTAL_SPACE`
- **Makros:** `${ device.EXTERNAL_STORAGE2_TOTAL_SPACE }`

Anzeigename: Externer Speicher verschlüsselt

- **Webelement:** `EXTERNAL_ENCRYPTION`
- **Makros:** `${ device.EXTERNAL_ENCRYPTION }`

Anzeigename: FileVault aktiviert

- **Webelement:** `IS_FILEVAULT_ENABLED`
- **Makros:** `${ device.IS_FILEVAULT_ENABLED }`

Anzeigename: Firewallstatus

- **Webelement:** `DEVICE_FIREWALL_STATUS`

- **Makros:** `${ device.DEVICE_FIREWALL_STATUS }`

Anzeigename: Firewallstatus

- **Webelement:** `DEVICE_FIREWALL_STATUS`
- **Makros:** `${ device.DEVICE_FIREWALL_STATUS }`

Anzeigename: Firewallstatus

- **Webelement:** `FIREWALL_STATUS`
- **Makros:** `${ device.FIREWALL_STATUS }`

Anzeigename: Firmwareversion

- **Webelement:** `FIRMWARE_VERSION`
- **Makros:** `${ device.FIRMWARE_VERSION }`

Anzeigename: Erstsynchronisierung

- **Webelement:** `ZMSP_FIRST_SYNC`
- **Makros:** `${ device.ZMSP_FIRST_SYNC }`

Anzeigename: Google Directory - Alias

- **Webelement:** `GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS }`

Anzeigename: Google Directory - Familienname

- **Webelement:** `GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_FAMILY_NAME }`

Anzeigename: Google Directory - Name

- **Webelement:** `GOOGLE_AW_DIRECTORY_NAME`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_NAME }`

Anzeigename: Google Directory - primäre E-Mail

- **Webelement:** `GOOGLE_AW_DIRECTORY_PRIMARY`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_PRIMARY }`

Anzeigename: Google Directory - Benutzer-ID

- **Webelement:** `GOOGLE_AW_DIRECTORY_USER_ID`

- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_USER_ID }`

Anzeigename: GPS-Höhe

- **Webelement:** `GPS_ALTITUDE_FROM_GPS`
- **Makros:** `${ device.GPS_ALTITUDE_FROM_GPS }`

Anzeigename: GPS - Kurs

- **Webelement:** `GPS_COURSE_FROM_GPS`
- **Makros:** `${ device.GPS_COURSE_FROM_GPS }`

Anzeigename: GPS - horizontale Genauigkeit

- **Webelement:** `GPS_HORIZONTAL_ACCURACY_FROM_GPS`
- **Makros:** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_GPS }`

Anzeigename: GPS-Breitengrad

- **Webelement:** `GPS_LATITUDE_FROM_GPS`
- **Makros:** `${ device.GPS_LATITUDE_FROM_GPS }`

Anzeigename: GPS-Längengrad

- **Webelement:** `GPS_LONGITUDE_FROM_GPS`
- **Makros:** `${ device.GPS_LONGITUDE_FROM_GPS }`

Anzeigename: GPS - Geschwindigkeit

- **Webelement:** `GPS_SPEED_FROM_GPS`
- **Makros:** `${ device.GPS_SPEED_FROM_GPS }`

Anzeigename: GPS-Zeitstempel

- **Webelement:** `GPS_TIMESTAMP_FROM_GPS`
- **Makros:** `${ device.GPS_TIMESTAMP_FROM_GPS }`

Anzeigename: GPS - vertikale Genauigkeit

- **Webelement:** `GPS_VERTICAL_ACCURACY_FROM_GPS`
- **Makros:** `${ device.GPS_VERTICAL_ACCURACY_FROM_GPS }`

Anzeigename: Hardwaregeräte-ID

- **Webelement:** `HW_DEVICE_ID`

- **Makros:** `${ device.HW_DEVICE_ID }`

Anzeigename: Hardwareverschlüsselung

- **Webelement:** `HARDWARE_ENCRYPTION_CAPS`
- **Makros:** `${ device.HARDWARE_ENCRYPTION_CAPS }`

Anzeigename: HAS_CONTAINER

- **Webelement:** `HAS_CONTAINER`
- **Makros:** `${ device.HAS_CONTAINER }`

Anzeigename: Hash des aktuell angemeldeten Apple App Store-Kontos

- **Webelement:** `ITUNES_STORE_ACCOUNT_HASH`
- **Makros:** `${ device.ITUNES_STORE_ACCOUNT_HASH }`

Anzeigename: Netzbetreiber für Heimnetzwerk

- **Webelement:** `SIM_CARRIER_NETWORK`
- **Makros:** `${ device.SIM_CARRIER_NETWORK }`

Anzeigename: Heimatländercode für mobiles Gerät

- **Webelement:** `SIM_MCC`
- **Makros:** `${ device.SIM_MCC }`

Anzeigename: Code für mobiles Heimnetzwerk

- **Webelement:** `SIM_MNC`
- **Makros:** `${ device.SIM_MNC }`

Anzeigename: ICCID

- **Webelement:** `ICCID`
- **Makros:** `${ device.ICCID }`

Anzeigename: Identität

- **Webelement:** `AS_DEVICE_IDENTITY`
- **Makros:** `${ device.AS_DEVICE_IDENTITY }`

Anzeigename: IMEI/MEID-Nummer

- **Webelement:** `IMEI`

- **Makros:** `${ device.IMEI }`

Anzeigename: IMSI

- **Webelement:** `SIM_ID`
- **Makros:** `${ device.SIM_ID }`

Anzeigename: Interner Speicher verschlüsselt

- **Webelement:** `LOCAL_ENCRYPTION`
- **Makros:** `${ device.LOCAL_ENCRYPTION }`

Anzeigename: IP-Standort

- **Webelement:** `IP_LOCATION`
- **Makros:** `${ device.IP_LOCATION }`

Anzeigename: IPv4-Adresse

- **Webelement:** `IP_ADDRESSV4`
- **Makros:** `${ device.IP_ADDRESSV4 }`

Anzeigename: IPv6-Adresse

- **Webelement:** `IP_ADDRESSV6`
- **Makros:** `${ device.IP_ADDRESSV6 }`

Anzeigename: Issued At

- **Webelement:** `WINDOWS_HAS_ISSUED_AT`
- **Makros:** `${ device.WINDOWS_HAS_ISSUED_AT }`

Anzeigename: Jailbreak/Rooting

- **Webelement:** `ROOT_ACCESS`
- **Makros:** `${ device.ROOT_ACCESS }`

Anzeigename: Kernel Debugging Enabled?

- **Webelement:** `WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- **Makros:** `${ device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED }`

Anzeigename: Kioskmodus

- **Webelement:** `IS_KIOSK`

- **Makros:** `${ device.IS_KIOSK }`

Anzeigename: Letzte bekannte IP-Adresse

- **Webelement:** `LAST_IP_ADDR`
- **Makros:** `${ device.LAST_IP_ADDR }`

Anzeigename: Zeit der letzten Richtlinienaktualisierung

- **Webelement:** `LAST_POLICY_UPDATE_TIME`
- **Makros:** `${ device.LAST_POLICY_UPDATE_TIME }`

Anzeigename: Datum des letzten Scans

- **Webelement:** `PreviousScanDate`
- **Makros:** `${ device.PreviousScanDate }`

Anzeigename: Ergebnis des letzten Scans

- **Webelement:** `PreviousScanResult`
- **Makros:** `${ device.PreviousScanResult }`

Anzeigename: Letztes geplantes Softwareupdate

- **Webelement:** `AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME`
- **Makros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME }`

Anzeigename: Fehlermeldung für letztes geplantes Softwareupdate

- **Webelement:** `AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG`
- **Makros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG }`

Anzeigename: Status des letzten geplanten Softwareupdates

- **Webelement:** `AVAILABLE_OS_UPDATE_INSTALL_STATUS`
- **Makros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_STATUS }`

Anzeigename: Letzte Synchronisierung

- **Webelement:** `ZMSP_LAST_SYNC`
- **Makros:** `${ device.ZMSP_LAST_SYNC }`

Anzeigename: Ortungsdienst aktiviert

- **Webelement:** `DEVICE_LOCATOR`

- **Makros:** `${ device.DEVICE_LOCATOR }`

Anzeigename: MAC-Adresse

- **Webelement:** `MAC_ADDRESS`
- **Makros:** `${ device.MAC_ADDRESS }`

Anzeigename: Netzwerkverbindung per MAC-Adresse

- **Webelement:** `MAC_NETWORK_CONNECTION`
- **Makros:** `${ device.MAC_NETWORK_CONNECTION }`

Anzeigename: MAC-Adresstyp

- **Webelement:** `MAC_ADDRESS_TYPE`
- **Makros:** `${ device.MAC_ADDRESS_TYPE }`

Anzeigename: Postfachsetup

- **Webelement:** `GOOGLE_AW_DIRECTORY_MAILBOX_SETUP`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP }`

Anzeigename: Hauptakku

- **Webelement:** `MAIN_BATTERY_PERCENT`
- **Makros:** `${ device.MAIN_BATTERY_PERCENT }`

Anzeigename: MDM-Modus ‘Verloren’aktiviert

- **Webelement:** `IS_MDM_LOST_MODE_ENABLED`
- **Makros:** `${ device.IS_MDM_LOST_MODE_ENABLED }`

Anzeigename: MDX_SHARED_ENCRYPTION_KEY

- **Webelement:** `MDX_SHARED_ENCRYPTION_KEY`
- **Makros:** `${ device.MDX_SHARED_ENCRYPTION_KEY }`

Anzeigename: MEID

- **Webelement:** `MEID`
- **Makros:** `${ device.MEID }`

Anzeigename: Mobiltelefonnummer

- **Webelement:** `TEL_NUMBER`

- **Makros:** `${ device.TEL_NUMBER }`

Anzeigename: Modell-ID

- **Webelement:** `MODEL_ID`
- **Makros:** `${ device.MODEL_ID }`

Anzeigename: Modellnummer

- **Webelement:** `MODEL_NUMBER`
- **Makros:** `${ device.MODEL_NUMBER }`

Anzeigename: Netzwerkadaptertyp

- **Webelement:** `NETWORK_ADAPTER_TYPE`
- **Makros:** `${ device.NETWORK_ADAPTER_TYPE }`

Anzeigename: Betriebssystembuild

- **Webelement:** `SYSTEM_OS_BUILD`
- **Makros:** `${ device.SYSTEM_OS_BUILD }`

Anzeigename: Edition des Betriebssystems

- **Webelement:** `OS_EDITION`
- **Makros:** `${ device.OS_EDITION }`

Anzeigename: Betriebssystemsprache (Gebietsschema)

- **Webelement:** `SYSTEM_LANGUAGE`
- **Makros:** `${ device.SYSTEM_LANGUAGE }`

Anzeigename: Betriebssystemversion

- **Webelement:** `SYSTEM_OS_VERSION`
- **Makros:** `${ device.SYSTEM_OS_VERSION }`

Anzeigename: Adresse der Organisation

- **Webelement:** `ORGANIZATION_ADDRESS`
- **Makros:** `${ device.ORGANIZATION_ADDRESS }`

Anzeigename: E-Mail (Organisation)

- **Webelement:** `ORGANIZATION_EMAIL`

- **Makros:** `${ device.ORGANIZATION_EMAIL }`

Anzeigename: Organization Magic

- **Webelement:** `ORGANIZATION_MAGIC`
- **Makros:** `${ device.ORGANIZATION_MAGIC }`

Anzeigename: Organisationsname

- **Webelement:** `ORGANIZATION_NAME`
- **Makros:** `${ device.ORGANIZATION_NAME }`

Anzeigename: Telefonnummer der Organisation

- **Webelement:** `ORGANIZATION_PHONE`
- **Makros:** `${ device.ORGANIZATION_PHONE }`

‘**Anzeigename:** Nicht richtlinientreu

- **Webelement:** `OUT_OF_COMPLIANCE`
- **Makros:** `${ device.OUT_OF_COMPLIANCE }`

Anzeigename: Besitz von

- **Webelement:** `CORPORATE_OWNED`
- **Makros:** `${ device.CORPORATE_OWNED }`

Anzeigename: Passcode richtlinientreu

- **Webelement:** `PASSCODE_IS_COMPLIANT`
- **Makros:** `${ device.PASSCODE_IS_COMPLIANT }`

Anzeigename: Passcode richtlinientreu gemäß Konfiguration

- **Webelement:** `PASSCODE_IS_COMPLIANT_WITH_CFG`
- **Makros:** `${ device.PASSCODE_IS_COMPLIANT_WITH_CFG }`

Anzeigename: Passcode vorhanden

- **Webelement:** `PASSCODE_PRESENT`
- **Makros:** `${ device.PASSCODE_PRESENT }`

Anzeigename: PCR0

- **Webelement:** `WINDOWS_HAS_PCR0`

- **Makros:** `${ device.WINDOWS_HAS_PCR0 }`

Anzeigename: Umkreisverletzung

- **Webelement:** `GPS_PERIMETER_BREACH`
- **Makros:** `${ device.GPS_PERIMETER_BREACH }`

Anzeigename: Periodische Prüfung

- **Webelement:** `PerformPeriodicCheck`
- **Makros:** `${ device.PerformPeriodicCheck }`

Anzeigename: Persönlicher Hotspot aktiviert

- **Webelement:** `PERSONAL_HOTSPOT_ENABLED`
- **Makros:** `${ device.PERSONAL_HOTSPOT_ENABLED }`

Anzeigename: PIN-Code für Geofence

- **Webelement:** `PIN_CODE_FOR_GEO_FENCE`
- **Makros:** `${ device.PIN_CODE_FOR_GEO_FENCE }`

Anzeigename: Plattform

- **Webelement:** `SYSTEM_PLATFORM`
- **Makros:** `${ device.SYSTEM_PLATFORM }`

Anzeigename: API-Level der Plattform

- **Webelement:** `API_LEVEL`
- **Makros:** `${ device.API_LEVEL }`

Anzeigename: Richtlinienname

- **Webelement:** `POLICY_NAME`
- **Makros:** `${ device.POLICY_NAME }`

Anzeigename: Primäre Telefonnummer

- **Webelement:** `IDENTITY1_PHONENUMBER`
- **Makros:** `${ device.IDENTITY1_PHONENUMBER }`

Anzeigename: Anbieter der primären SIM

- **Webelement:** `IDENTITY1_CARRIER_NETWORK_OPERATOR`

- **Makros:** `${ device.IDENTITY1_CARRIER_NETWORK_OPERATOR }`

Anzeigename: Primäre SIM-ICCID

- **Webelement:** `IDENTITY1_ICCID`
- **Makros:** `${ device.IDENTITY1_ICCID }`

Anzeigename: Primäre SIM, IMEI

- **Webelement:** `IDENTITY1_IMEI`
- **Makros:** `${ device.IDENTITY1_IMEI }`

Anzeigename: Primäre SIM, IMSI

- **Webelement:** `IDENTITY1_IMSI`
- **Makros:** `${ device.IDENTITY1_IMSI }`

Anzeigename: Primäre SIM, Roaming

- **Webelement:** `IDENTITY1_ROAMING`
- **Makros:** `${ device.IDENTITY1_ROAMING }`

Anzeigename: Primäre SIM, Roaming

- **Webelement:** `IDENTITY1_ROAMING_COMPLIANCE`
- **Makros:** `${ device.IDENTITY1_ROAMING_COMPLIANCE }`

Anzeigename: Produktname

- **Webelement:** `PRODUCT_NAME`
- **Makros:** `${ device.PRODUCT_NAME }`

Anzeigename: Geräte-ID des Herausgebers

- **Webelement:** `PUBLISHER_DEVICE_ID`
- **Makros:** `${ device.PUBLISHER_DEVICE_ID }`

Anzeigename: Reset Count

- **Webelement:** `WINDOWS_HAS_RESET_COUNT`
- **Makros:** `${ device.WINDOWS_HAS_RESET_COUNT }`

Anzeigename: Restart Count

- **Webelement:** `WINDOWS_HAS_RESTART_COUNT`

- **Makros:** `${ device.WINDOWS_HAS_RESTART_COUNT }`

Anzeigename: Safe Mode Enabled?

- **Webelement:** `WINDOWS_HAS_SAFE_MODE`
- **Makros:** `${ device.WINDOWS_HAS_SAFE_MODE }`

Anzeigename: SBCP Hash

- **Webelement:** `WINDOWS_HAS_SBCP_HASH`
- **Makros:** `${ device.WINDOWS_HAS_SBCP_HASH }`

Anzeigename: Bildschirm: Höhe

- **Webelement:** `SCREEN_HEIGHT`
- **Makros:** `${ device.SCREEN_HEIGHT }`

Anzeigename: Bildschirm: Anzahl der Farben

- **Webelement:** `SCREEN_NB_COLORS`
- **Makros:** `${ device.SCREEN_NB_COLORS }`

Anzeigename: Bildschirm: Größe

- **Webelement:** `SCREEN_SIZE`
- **Makros:** `${ device.SCREEN_SIZE }`

Anzeigename: Bildschirm: Breite

- **Webelement:** `SCREEN_WIDTH`
- **Makros:** `${ device.SCREEN_WIDTH }`

Anzeigename: Bildschirm: Auflösung X-Achse

- **Webelement:** `SCREEN_XDPI`
- **Makros:** `${ device.SCREEN_XDPI }`

Anzeigename: Bildschirm: Auflösung Y-Achse

- **Webelement:** `SCREEN_YDPI`
- **Makros:** `${ device.SCREEN_YDPI }`

Anzeigename: Sekundäre Telefonnummer

- **Webelement:** `IDENTITY2_PHONENUMBER`

- **Makros:** `${ device.IDENTITY2_PHONENUMBER }`

Anzeigename: Anbieter der sekundären SIM

- **Webelement:** `IDENTITY2_CARRIER_NETWORK_OPERATOR`
- **Makros:** `${ device.IDENTITY2_CARRIER_NETWORK_OPERATOR }`

Anzeigename: Sekundäre SIM-ICCID

- **Webelement:** `IDENTITY2_ICCID`
- **Makros:** `${ device.IDENTITY2_ICCID }`

Anzeigename: Sekundäre SIM, IMEI

- **Webelement:** `IDENTITY2_IMEI`
- **Makros:** `${ device.IDENTITY2_IMEI }`

Anzeigename: Sekundäre SIM, IMSI

- **Webelement:** `IDENTITY2_IMSI`
- **Makros:** `${ device.IDENTITY2_IMSI }`

Anzeigename: Sekundäre SIM, Roaming

- **Webelement:** `IDENTITY2_ROAMING`
- **Makros:** `${ device.IDENTITY2_ROAMING }`

Anzeigename: Roamingcompliance für sekundäre SIM

- **Webelement:** `IDENTITY2_ROAMING_COMPLIANCE`
- **Makros:** `${ device.IDENTITY2_ROAMING_COMPLIANCE }`

Anzeigename: Secure Boot Enabled?

- **Webelement:** `WINDOWS_HAS_SECURE_BOOT_ENABLED`
- **Makros:** `${ device.WINDOWS_HAS_SECURE_BOOT_ENABLED }`

Anzeigename: Status von Secure Boot

- **Webelement:** `SECURE_BOOT_STATE`
- **Makros:** `${ device.SECURE_BOOT_STATE }`

Anzeigename: SecureContainer aktiviert

- **Webelement:** `DLP_ACTIVE`

- **Makros:** `${ device.DLP_ACTIVE }`

Anzeigename: Sicherheitspatchebene

- **Webelement:** `SYSTEM_SECURITY_PATCH_LEVEL`
- **Makros:** `${ device.SYSTEM_SECURITY_PATCH_LEVEL }`

Anzeigename: Seriennummer

- **Webelement:** `SERIAL_NUMBER`
- **Makros:** `${ device.SERIAL_NUMBER }`

Anzeigename: SMS-fähig

- **Webelement:** `IS_SMS_CAPABLE`
- **Makros:** `${ device.IS_SMS_CAPABLE }`

Anzeigename: Betreut

- **Webelement:** `SUPERVISED`
- **Makros:** `${ device.SUPERVISED }`

Anzeigename: Grund für vorübergehende Sperrung

- **Webelement:** `GOOGLE_AW_DIRECTORY_SUSPENTION_REASON`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON }`

Anzeigename: Manipulierter Status

- **Webelement:** `TAMPERED_STATUS`
- **Makros:** `${ device.TAMPERED_STATUS }`

Anzeigename: AGB

- **Webelement:** `TERMS_AND_CONDITIONS`
- **Makros:** `${ device.TERMS_AND_CONDITIONS }`

Anzeigename: Nutzungsbedingungen und Vereinbarung angenommen?

- **Webelement:** `GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- **Makros:** `${ device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS }`

Anzeigename: Test Signing Enabled?

- **Webelement:** `WINDOWS_HAS_TEST_SIGNING_ENABLED`

- **Makros:** `${ device.WINDOWS_HAS_TEST_SIGNING_ENABLED }`

Anzeigename: Gesamt-RAM

- **Webelement:** `MEMORY`
- **Makros:** `${ device.MEMORY }`

Anzeigename: Gesamtspeicherplatz

- **Webelement:** `TOTAL_DISK_SPACE`
- **Makros:** `${ device.TOTAL_DISK_SPACE }`

Anzeigename: TPM-Version

- **Webelement:** `TPM_VERSION`
- **Makros:** `${ device.TPM_VERSION }`

Anzeigename: UDID

- **Webelement:** `UDID`
- **Makros:** `${ device.UDID }`

Anzeigename: Status der Benutzerkontensteuerung

- **Webelement:** `UAC_STATUS`
- **Makros:** `${ device.UAC_STATUS }`

Anzeigename: Benutzeragent

- **Webelement:** `USER_AGENT`
- **Makros:** `${ device.USER_AGENT }`

Anzeigename: Benutzerdefiniert 1

- **Webelement:** `USER_DEFINED_1`
- **Makros:** `${ device.USER_DEFINED_1 }`

Anzeigename: Benutzerdefiniert 2

- **Webelement:** `USER_DEFINED_2`
- **Makros:** `${ device.USER_DEFINED_2 }`

Anzeigename: Benutzerdefiniert 3

- **Webelement:** `USER_DEFINED_3`

- **Makros:** `${ device.USER_DEFINED_3 }`

Anzeigename: Benutzersprache (Gebietsschema)

- **Webelement:** `USER_LANGUAGE`
- **Makros:** `${ device.USER_LANGUAGE }`

Anzeigename: Hersteller

- **Webelement:** `VENDOR`
- **Makros:** `${ device.VENDOR }`

Anzeigename: Sprachfähig

- **Webelement:** `IS_VOICE_CAPABLE`
- **Makros:** `${ device.IS_VOICE_CAPABLE }`

Anzeigename: Sprachroaming zugelassen

- **Webelement:** `VOICE_ROAMING_ENABLED`
- **Makros:** `${ device.VOICE_ROAMING_ENABLED }`

Anzeigename: VSM Enabled?

- **Webelement:** `WINDOWS_HAS_VSM_ENABLED`
- **Makros:** `${ device.WINDOWS_HAS_VSM_ENABLED }`

Anzeigename: Wi-Fi MAC-Adresse

- **Webelement:** `WIFI_MAC`
- **Makros:** `${ device.WIFI_MAC }`

Anzeigename: WINDOWS_ENROLLMENT_KEY

- **Webelement:** `WINDOWS_ENROLLMENT_KEY`
- **Makros:** `${ device.WINDOWS_ENROLLMENT_KEY }`

Anzeigename: WinPE Enabled?

- **Webelement:** `WINDOWS_HAS_WINPE`
- **Makros:** `${ device.WINDOWS_HAS_WINPE }`

Anzeigename: WNS-Benachrichtigungsstatus

- **Webelement:** `PROPERTY_WNS_PUSH_STATUS`

- **Makros:** `${ device.PROPERTY_WNS_PUSH_STATUS }`

Anzeigename: WNS-Benachrichtigungs-URL

- **Webelement:** `PROPERTY_WNS_PUSH_URL`
- **Makros:** `${ device.PROPERTY_WNS_PUSH_URL }`

Anzeigename: Ablaufdatum der URL für WNS-Benachrichtigung

- **Webelement:** `PROPERTY_WNS_PUSH_URL_EXPIRY`
- **Makros:** `${ device.PROPERTY_WNS_PUSH_URL_EXPIRY }`

Anzeigename: Citrix Endpoint Management-Agent-ID

- **Webelement:** `ENROLLMENT_AGENT_ID`
- **Makros:** {device.ENROLLMENT_AGENT_ID}‘

Anzeigename: Citrix Endpoint Management-Agentrevision

- **Webelement:** `EW_REVISION`
- **Makros:** `${ device.EW_REVISION }`

Anzeigename: Citrix Endpoint Management-Agentversion

- **Webelement:** `EW_VERSION`
- **Makros:** `${ device.EW_VERSION }`

Anzeigename: Zebra API verfügbar

- **Webelement:** `ZEBRA_MDM`
- **Makros:** `${ device.ZEBRA_MDM }`

Anzeigename: Zebra MXMF-Version

- **Webelement:** `ZEBRA_MDM_VERSION`
- **Makros:** `${ device.ZEBRA_MDM_VERSION }`

Anzeigename: Zebra Patch-Version

- **Webelement:** `ZEBRA_PATCH_VERSION`
- **Makros:** `${ device.ZEBRA_PATCH_VERSION }`

Makros zum Abrufen integrierter Benutzereigenschaften

Anzeigename	Makros
`domainname` (Domänenname; Standarddomäne)	`${ user.domainname }`
`loginname` (Benutzername plus Domänenname)	`${ user.loginname }`
`username` (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`	`${ user.asmpersonsource }`
ASM Deployment Program-Kontoname	`asmdepaccount`	`${ user.asmdepaccount }`
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 }`

Anzeigename	Webelement	Makros
ASM-Klassenstufe	asmpersongrade	${ user.asmpersongrade }
BES-Benutzer-E-Mail	besuseremail	${ user.besuseremail }
Firma	company	${ user.company }
Firmenname	companyname	${ user.companyname }
Land	c	${ user.c }
Abteilung	department	${ user.department }
Beschreibung	description	${ user.description }
Deaktivierter Benutzer	disableduser	${ user.disableduser }
Anzeigename	displayname	${ user.displayname }
Distinguished Name	distinguishedname	${ user.distinguishedname }
Domänenname	domainname	${ user.domainname }
E-Mail	mail	${ user.mail }
Vorname	givenname	${ user.givenname }
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 }
Mobiltelefon	mobile	${ user.mobile }

Anzeigename	Webelement	Makros
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 }
SAM-Konto	samaccountname	${ user.samaccountname }
Straße	streetaddress	${ user.streetaddress }
Nachname	sn	${ user.sn }
Titel	title	${ user.title }
Benutzeranmeldename	userprincipalname	${ user.userprincipalname }

Automatisierte Aktionen

March 11, 2024

Mit automatisierten Aktionen in Citrix Endpoint Management programmieren Sie eine Reaktion auf:

- Ereignisse
- Benutzer- oder Geräteeigenschaften
- vorhandene Apps auf Benutzergeräten

Beim Erstellen einer automatisierten Aktion legen Sie über Auslöser die Auswirkungen auf den Geräten von Benutzern fest, wenn diese mit Citrix Endpoint Management 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.

Sie können automatisierte Aktionen verwenden, um mit Azure Active Directory (AD) verbundene Windows 10- und Windows 11-Geräte als nicht richtlinientreu in Azure AD zu kennzeichnen.

> **Hinweis:**
>
> Sie können Benutzer nur benachrichtigen, wenn Sie in den Citrix Endpoint Management-Einstellungen Benachrichtigungsserver für SMTP konfiguriert haben, damit Citrix Endpoint Management Nachrichten senden kann. Weitere Informationen finden Sie unter Benachrichtigungen. Bevor Sie fortfahren, richten Sie alle Benachrichtigungsvorlagen ein, die Sie verwenden möchten. Weitere Informationen finden Sie unter Benachrichtigungen. Siehe Benachrichtigungsvorlagen erstellen und aktualisieren.

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 angeben, der das Benutzergerät nach dem Erkennen der App

"Words with Friends"als nicht richtlinientreu einstuft. Die Aktion informiert die Benutzer dann darüber, dass sie die App entfernen müssen, damit ihr Gerät wieder den Richtlinien entspricht. 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 Citrix Endpoint Management-Konsole zu **Einstellungen > Netzwerkzugriffssteuerung** und wählen Sie **Inaktive Geräte** aus. 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.

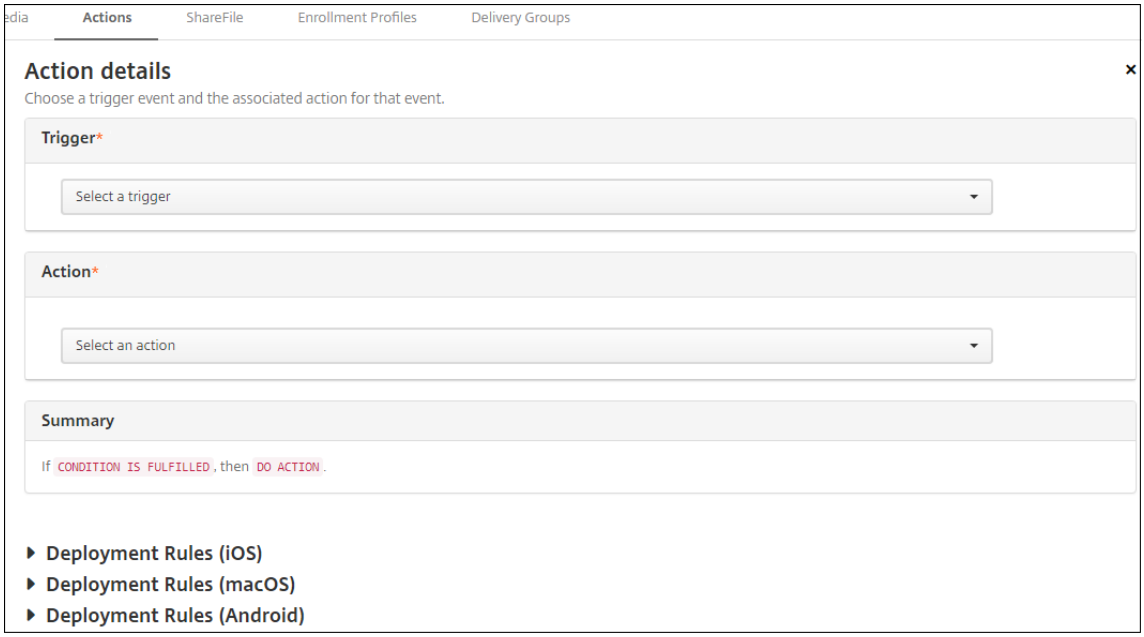
> **Tipp:**
>
> Zum Löschen inaktiver Geräte in großen Mengen verwenden Sie die öffentliche REST-API von Citrix Endpoint Management. Sie beschaffen zunächst manuell die IDs der inaktiven Geräte und führen dann die Lösch-API aus, um sie in einem Durchgang zu löschen.

Hinzufügen und Verwalten von Aktionen

Hinzufügen, Bearbeiten und Filtern von automatisierten Aktionen:

1. Klicken Sie in der Citrix Endpoint Management-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. Dieses Feld 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:

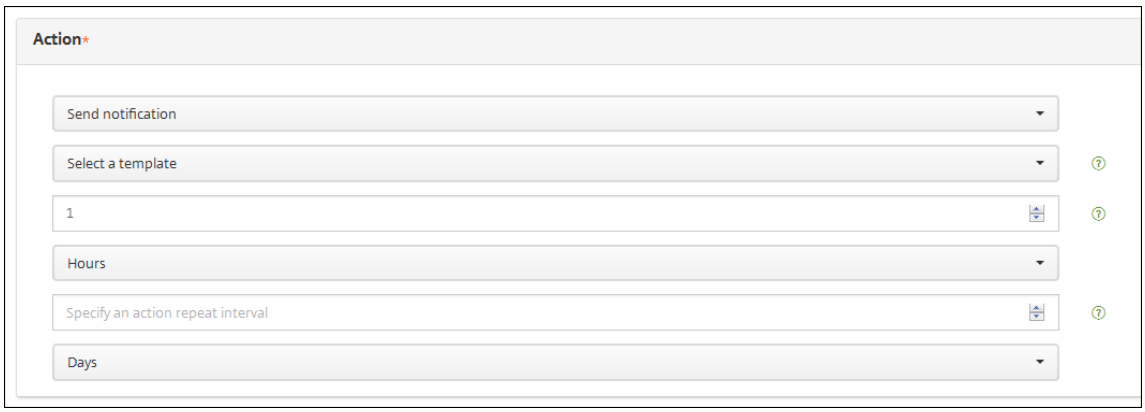
   Klicken Sie in der Liste **Auslöser** auf den Auslösertyp für die Aktion. Wählen Sie einen der folgenden Auslöser:

- **Ereignis:** Überprüft, ob der Gerätestatus mit dem von Ihnen gewählten Ereignis für Nichtlinientreue übereinstimmt und reagiert darauf.
- **Geräteeigenschaft:** Überprüft, ob auf einem mit MDM verwalteten Gerät ein bestimmter Wert für ein Geräteattribut vorliegt, und reagiert darauf. Weitere Informationen finden Sie unter Namen und Werte von Geräteeigenschaften.
- **Benutzereigenschaft:** Reagiert auf einen bestimmten Wert für 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.
- **Von der Richtlinie zurückgegebener Wert:** Überprüft, ob der von PowerShell-Skripts zurückgegebene Wert spezifische Logikkriterien erfüllt. Die Windows Agent-Geräterichtlinie muss aktiviert und konfiguriert sein. Weitere Informationen zu dieser Richtlinie finden Sie unter Windows Agent-Geräterichtlinie.

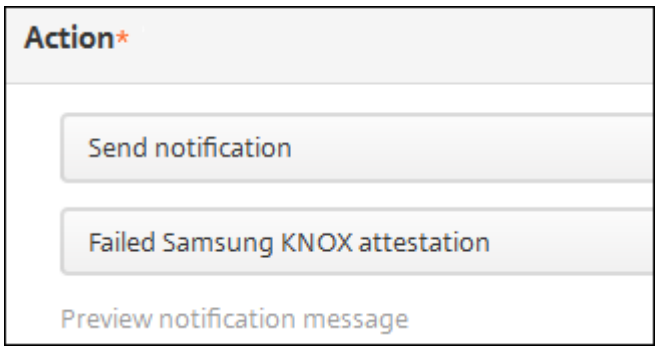
7. Klicken Sie in der nächsten Liste auf die Reaktion auf den Auslöser.
8. Klicken Sie in der Liste **Aktion** auf die Aktion, die ausgeführt werden soll, wenn das Auslösekriterium erfüllt wird. Mit Ausnahme der Aktion **Benachrichtigung senden** können Sie für alle Optionen einen Zeitraum festlegen, 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. Gibt es keine Vorlage für den Benachrichtigungstyp werden Sie aufgefordert, eine Vorlage zu konfigurieren. Erstellen Sie eine Vorlage mit der Option **Benachrichtigungsvorlage** in **Einstellungen**.

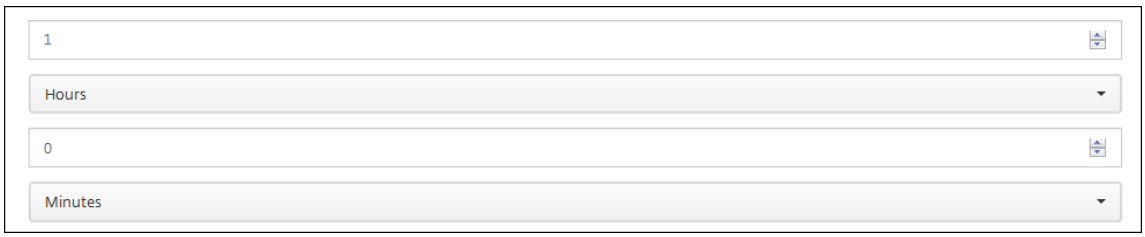
   Um Benutzer zu benachrichtigen, konfigurieren Sie unter **Einstellungen > Benachrichtigungsserver** die Einstellungen für SMTP, damit Citrix Endpoint Management Nachrichten senden kann. Siehe Benachrichtigungen. Richten Sie außerdem unter **Einstellungen > Benachrichtigungsvorlage** alle gewünschten Benachrichtigungsvorlagen ein, bevor Sie fortfahren. Siehe Benachrichtigungsvorlagen erstellen und aktualisieren.



Nach Auswahl der Vorlage klicken Sie auf **Vorschau für Benachrichtigung**.



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 Ressourcen bereitstellen.

    Im vorliegenden Beispiel:

    - Der Gerätebesitz muss **BYOD** 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.

      > **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
      > - Ist nicht verfügbar für Kunden, die Android und Android Enterprise sowie Citrix

> Endpoint Management in einer Version ab 10.18.19 verwenden
> – Wird nicht empfohlen für Kunden, die Android und Android Enterprise sowie Citrix 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**.

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 für die vier Auslöserkategorien in der Citrix Endpoint Management-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 Citrix Endpoint Management-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.

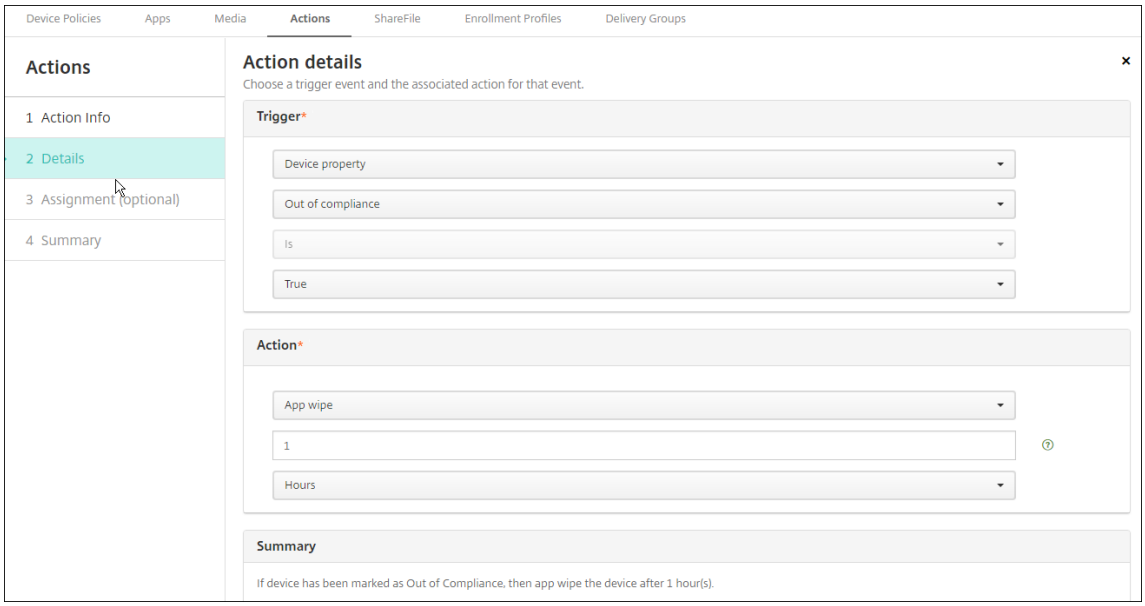
   Wenn der Auslöser **Geräteeigenschaft** und der Wert **MDM-Modus** '**Verloren**' aktiviert ist, werden die folgenden Aktionen nicht angezeigt:

   - 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.

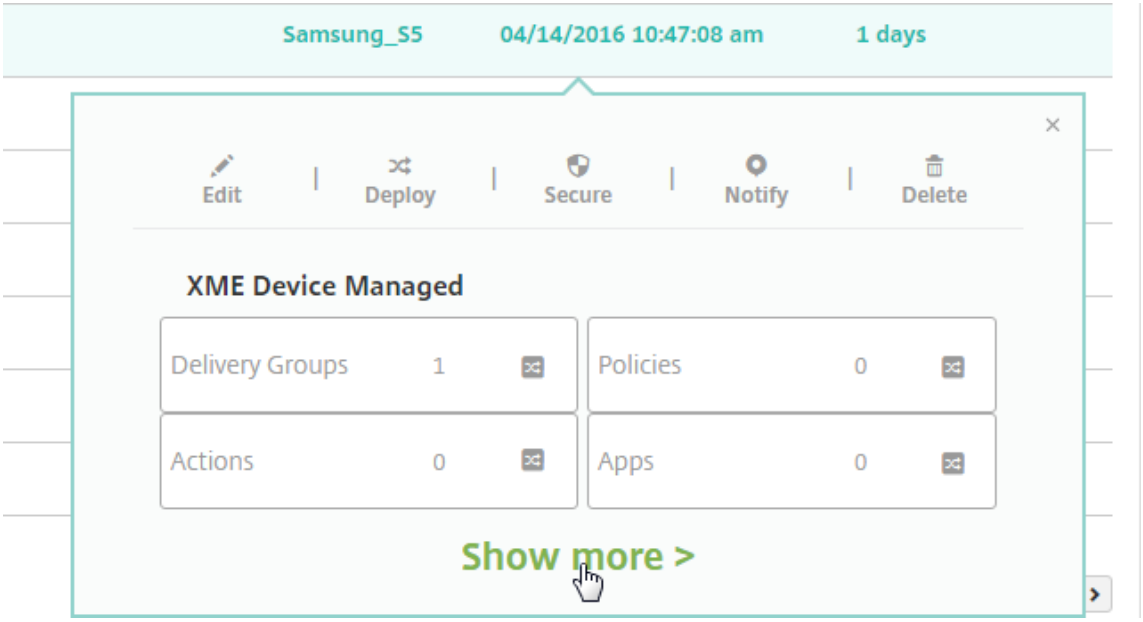
> **Hinweis:**
>
> Wenn Sie den Auslöser auf **Ereignis** festlegen, wird als Wiederholungsintervall automatisch mindestens 1 Stunde festgelegt. Das Gerät muss eine Aktualisierung der Richtlinien zur Synchronisierung mit dem Server ausführen, damit Benachrichtigung empfangen werden. Normalerweise erfolgt die Synchronisierung eines Geräts mit dem Server, wenn der Benutzer sich anmeldet oder die Richtlinien manuell über Citrix Secure Hub aktualisiert.
>
> Eine zusätzliche Verzögerung von etwa 1 Stunde vor der Ausführung der Aktion ist möglich, damit die Active Directory-Datenbank mit Citrix Endpoint Management synchronisiert werden kann.



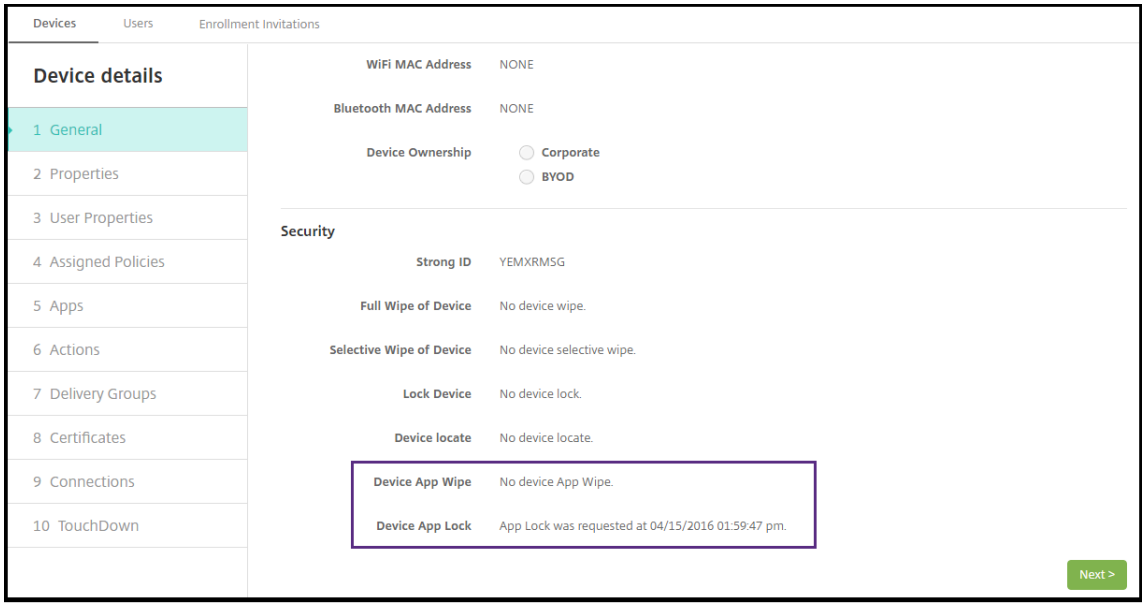
6. Konfigurieren Sie die Bereitstellungsregeln und klicken Sie auf **Weiter**.
7. Konfigurieren Sie die Zuweisungen für Bereitstellungsgruppen und einen Bereitstellungszeitplan, und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Speichern**.

Überprüfen des Status für App-Sperre oder App-Löschen

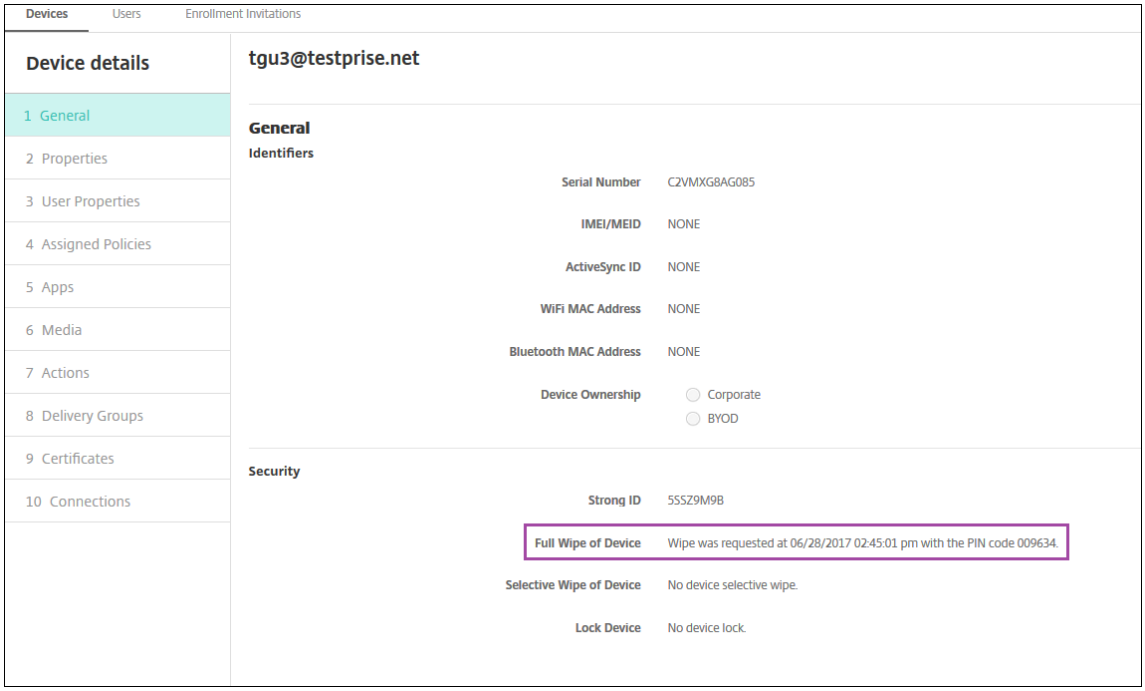
1. Gehen Sie zu **Verwalten > Geräte**, wählen Sie ein Gerät aus und klicken Sie auf **Mehr anzeigen**.



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.



Kennzeichnen von Windows 10- und Windows 11-Geräten als nicht richtlinientreu in Azure AD

Wenn mit Azure AD verbundene Windows 10- und Windows 11-Geräte in Citrix Endpoint Management als nicht richtlinientreu gekennzeichnet werden, können sie auch in Azure AD als nicht richtlinientreu gekennzeichnet werden. Um diese Funktionalität zu aktivieren, fügen Sie im Azure AD-Portal der On-Premises-MDM-Anwendung die Berechtigung zum Zugriff auf die Microsoft Graph-API hinzu.

1. Melden Sie sich mit Ihren Azure AD-Administratoranmeldeinformationen am Azure AD-Portal an.
2. Navigieren Sie im Azure AD-Portal zu **Azure Active Directory > Mobility (MDM and MAM)**. Wählen Sie **On-premises MDM application**.
3. Klicken Sie auf **On-premises Application Settings > Required Permissions > Add > Select an API > Microsoft Graph**. Klicken Sie auf **Select** und Speichern Sie.
4. Wählen Sie unter **Required permissions** die Option **Microsoft Graph**. Wählen Sie unter **Enable Access** die Option **Read and write directory data**.
5. Wählen Sie unter **Required permissions** die Option **Microsoft Graph**. Klicken Sie dann auf **Grant permissions**.
6. Klicken Sie auf **Yes**, um die Berechtigung zu gewähren.

Wenn ein in Azure AD registriertes Gerät, auf dem Windows 10 oder Windows 11 ausgeführt wird, in

Citrix Endpoint Management als nicht richtlinientreu gekennzeichnet wird, wird es auch in Azure AD als nicht richtlinientreu gekennzeichnet.

Erstellen einer automatisierten Aktion basierend auf einem Ergebnis der Windows Agent-Geräterichtlinie

Über die Windows Agent-Geräterichtlinie können Sie Skripts bereitstellen, die Registrierungswerte auf verwalteten Windows-Desktops und -Tablets überwachen. Sie können dann eine automatisierte Aktion basierend auf den von einem Skript zurückgegebenen Werten konfigurieren.

1. Konfigurieren Sie eine Windows Agent-Geräterichtlinie und überprüfen Sie die vom Skript zurückgegebenen Werte. Informationen zu dieser Richtlinie finden Sie unter Windows Agent-Geräterichtlinie.

   Der Artikel und der vorliegende Abschnitt enthalten ein Beispiel mit einem Skript namens `EntApp_2019_checkFirewall`. Die zugehörige Windows Agent-Geräterichtlinie definiert eine Konfiguration namens `cName_checkFirewall`. Diese Konfiguration führt das Beispielskript aus.

   Nach Ausführung des Skripts auf einem Gerät erhalten Sie die zum Erstellen einer Aktion erforderlichen Informationen (siehe Windows Agent-Geräterichtlinie).

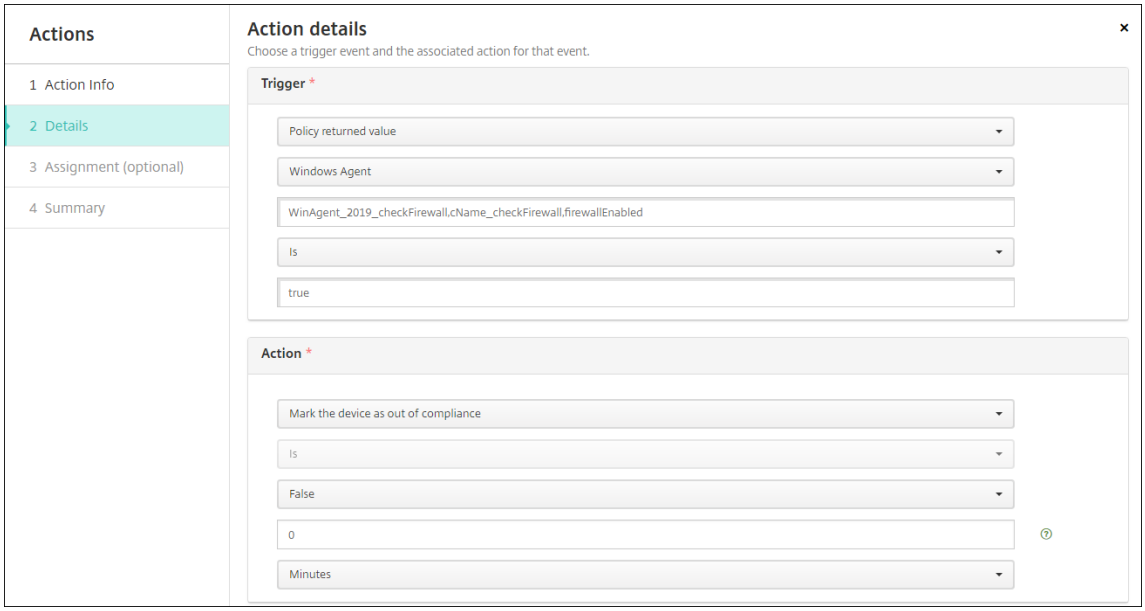
2. Klicken Sie in der Citrix Endpoint Management-Konsole auf **Konfigurieren > Aktionen**.
3. Klicken Sie auf der Seite **Aktionen** auf **Hinzufügen**.
4. Geben Sie auf der Seite **Aktionsinformationen** einen Namen für die Aktion und optional eine Beschreibung ein.
5. Wählen Sie auf der Seite **Aktionsdetails** unter **Von der Richtlinie zurückgegebener Wert** den gewünschten Auslöser aus.

6. Definieren Sie in den angezeigten Feldern den Auslöser und die Aktion:

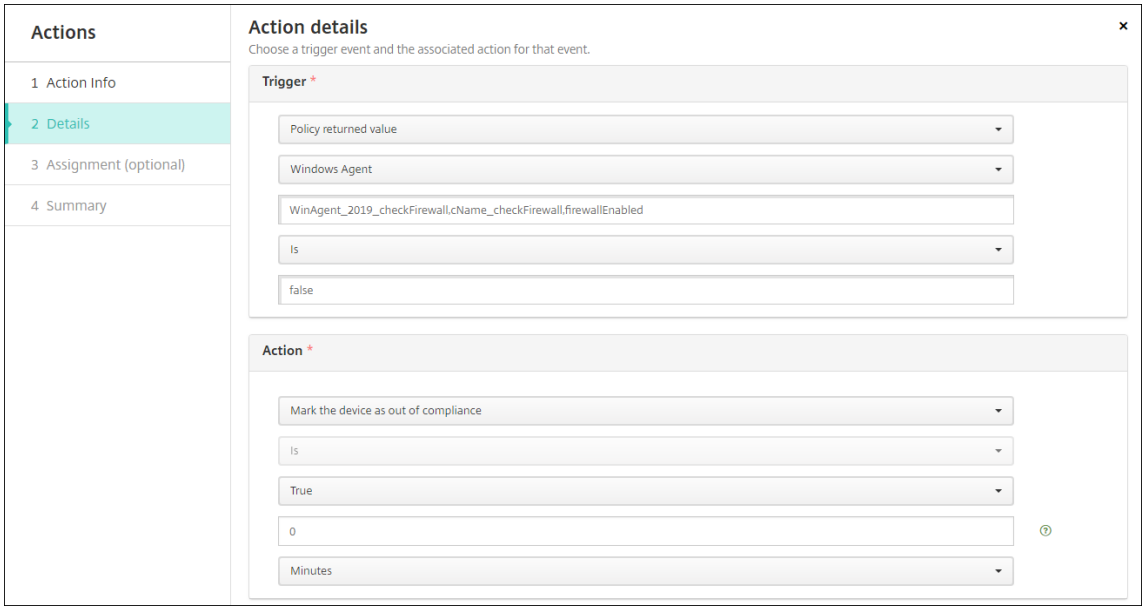
   - **Windows Agent-Einstellungen:** Geben Sie den Richtliniennamen, den Konfigurationsnamen und den Schlüsselnamen für die erstellte Windows Agent-Richtlinie ein.

- **Dropdownmenü:** Wählen Sie **Is**, **Is Not**, **Contains** oder **Does Not Contain**. Diese Logik gilt für das nächste Feld und bewirkt, dass die Aktion ausgelöst wird, sofern die Logik zutrifft.
- **Geben Sie eine Zeichenfolge ein:** Geben Sie die Zeichenfolge ein, die durch die Ausführung des in die Richtlinie hochgeladenen PowerShell-Skripts zurückgegeben wurde. Informationen zum Auffinden dieser Zeichenfolge finden Sie unter Windows Agent-Geräterichtlinie.
- **Aktion:** Wählen Sie eine Aktion sowie einen Wert und Zeitrahmen für die Aktion aus.

Im gezeigten Beispiel: Wenn Schlüssel `firewallEnabled` den Wert **`true`** zurückgibt, markiert die folgende Aktion das Gerät als richtlinientreu.



Wenn Schlüssel `firewallEnabled` den Wert **`false`** zurückgibt, markiert die folgende Aktion das Gerät als nicht richtlinientreu.



7. Legen Sie bei Bedarf einen Bereitstellungsplan und Bereitstellungsgruppen fest.

Überwachen und unterstützen

March 11, 2024

Nutzen Sie das Citrix Endpoint Management-Dashboard und die Citrix Endpoint Management-Supportseite zur Überwachung und zum Support des Citrix Endpoint Management-Servers. Auf der Seite “Citrix Endpoint Management Support”finden Sie Supportinformationen und -tools.

Klicken Sie in der Citrix Endpoint Management-Konsole auf das Schraubenschlüsselsymbol rechts oben.

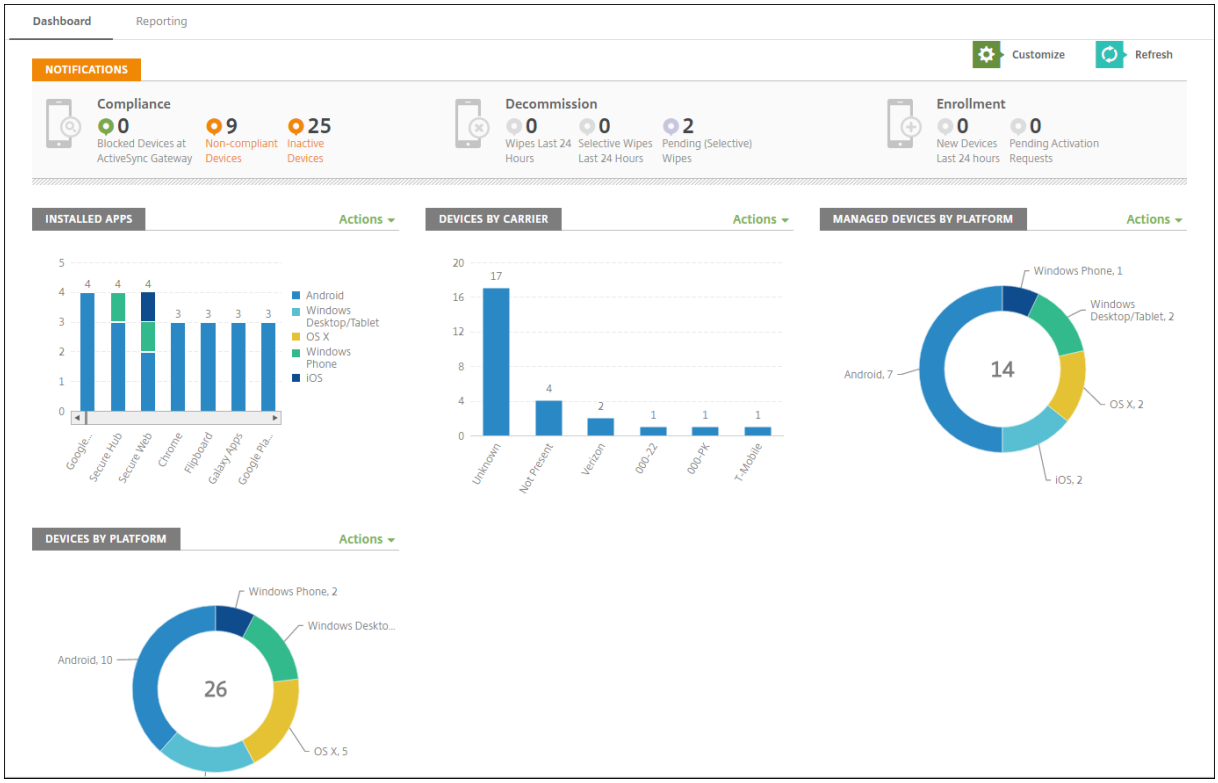
Die Seite **Problembehandlung und Support** wird angezeigt.

Verwenden Sie die Seite **Problembehandlung und Support** von Citrix Endpoint Management für Folgendes:

- Diagnose
- Zugriff auf Links zur Citrix Produktdokumentation und Knowledge Center
- Zugriff auf Protokollvorgänge

- Erweiterte Konfigurationsoptionen
- Zugriff auf diverse Tools und Hilfsprogramme

Das Dashboard der Citrix Endpoint Management-Konsole ermöglicht die übersichtliche Anzeige von Informationen auf einen Blick. Mit diesen Informationen können Sie Probleme und erfolgreiche Aktionen schnell mit Widgets erfassen.

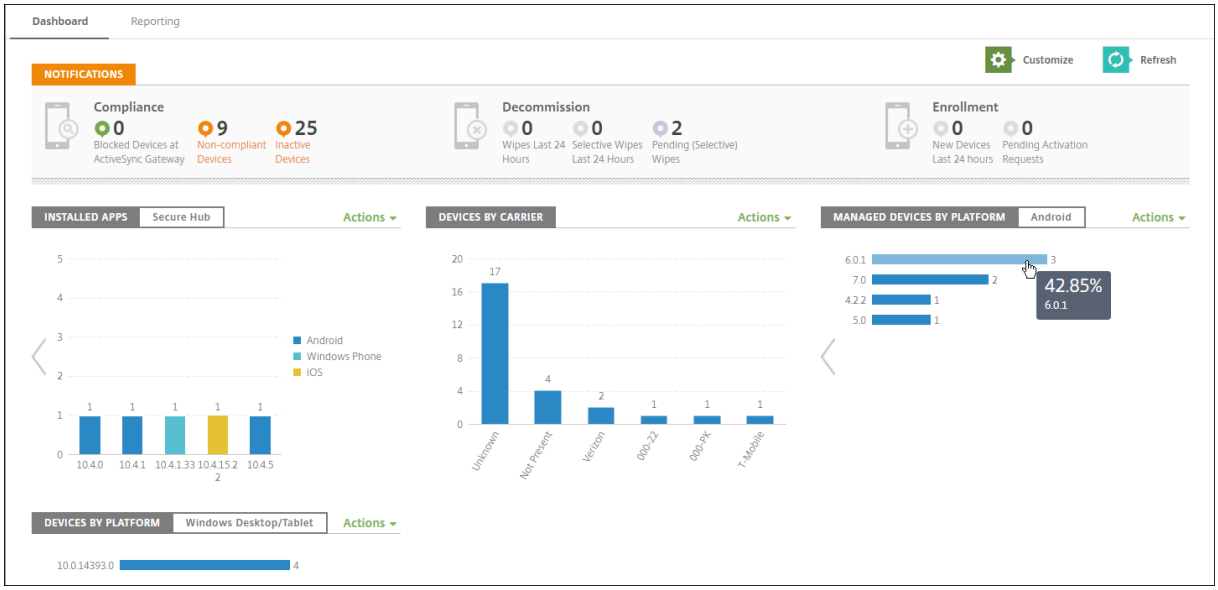


Das Dashboard ist normalerweise der erste Seite, die beim Anmelden an der Citrix Endpoint Management-Konsole angezeigt wird. Um das Dashboard von anderer Stelle aus aufzurufen, klicken Sie auf **Analysieren**. Klicken Sie im Dashboard auf **Anpassen**, um das Seitenlayout und die angezeigten Widgets 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.

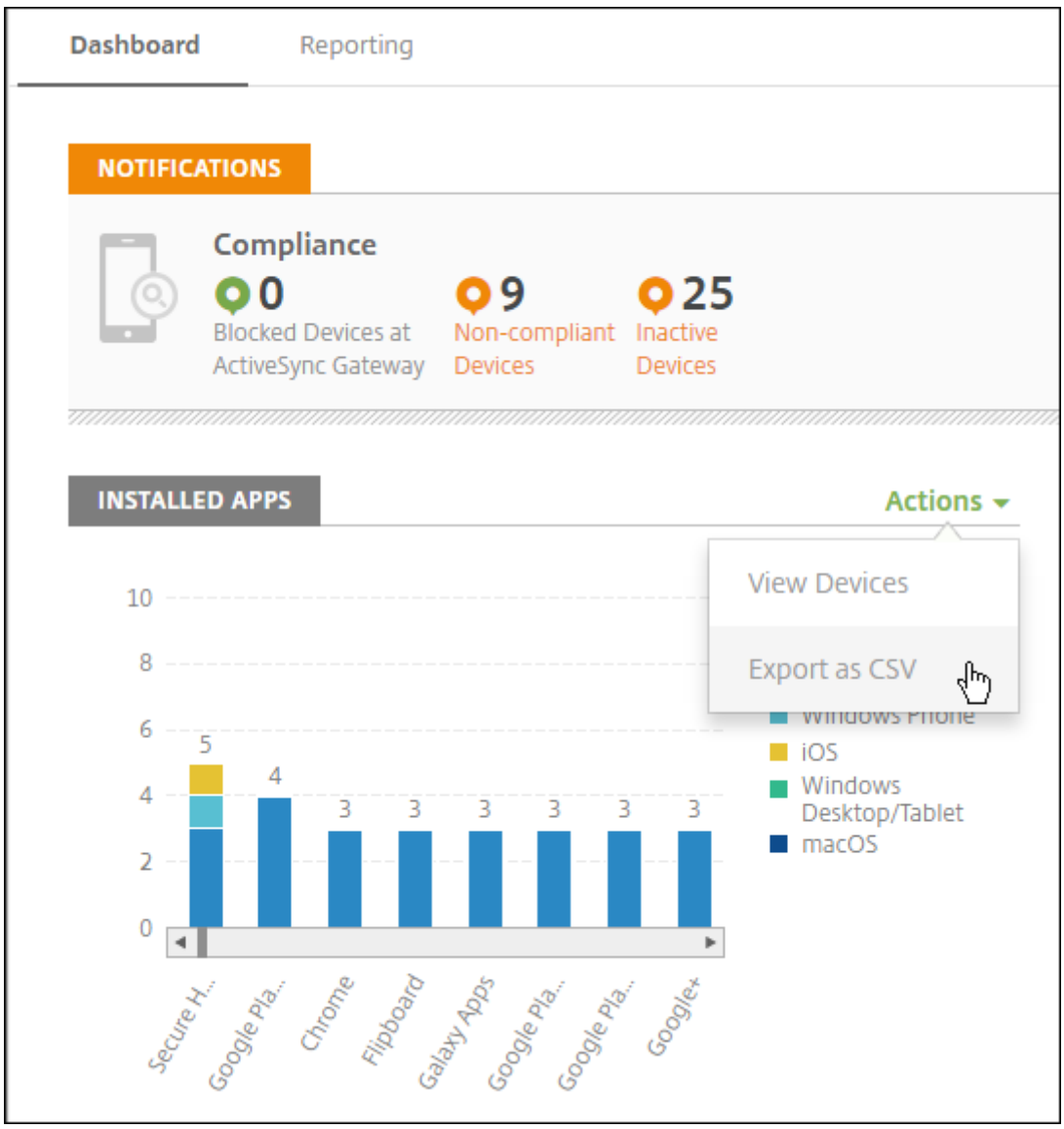
- **Geräte nach Netzbetreiber:** Anzahl der verwalteten und nicht verwalteten Geräte pro Netzbetreiber. Klicken Sie auf die einzelnen Balken, um eine Aufschlüsselung nach Plattform anzuzeigen.
- **Verwaltete Geräte nach Plattform:** Anzahl der verwalteten Geräte pro Plattform.
- **Nicht verwaltete Geräte 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 Volume 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 Menü **Aktio-**

nen.



Seite “Überwachen”für Helpdeskadministratoren

Sie können Citrix Endpoint Management jetzt über die neue Seite **Überwachen** überwachen und warten. Diese Schnittstelle ermöglicht Helpdeskadministratoren eine angepasste und effiziente Problembehandlung auf Benutzerbasis.

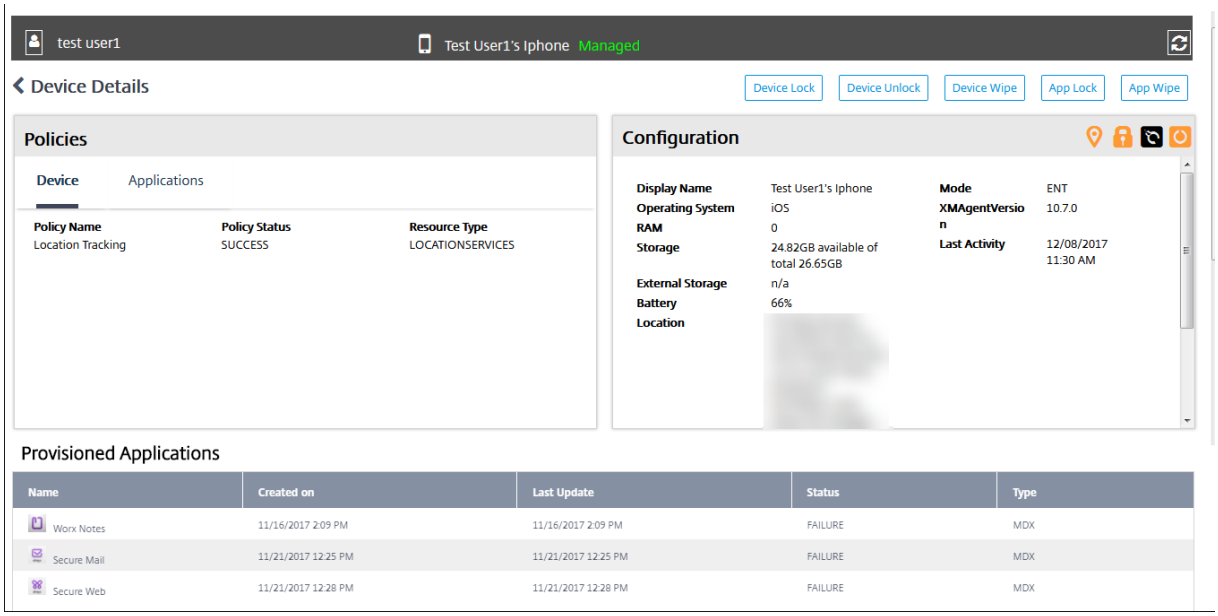
Helpdeskadministratoren müssen die folgenden Berechtigungen haben, um auf die Seite **Überwachen** und alle verfügbaren Workflows zugreifen zu können:

- Autorisierter Zugriff
  - Zugriff über Administratorkonsole

  - Zugriff über öffentliche API

- Konsolenfeatures
  - Überwachung
  - Geräte
  - Gerät vollständig löschen
  - Standorte anzeigen
    - Gerät orten
    - Gerätetracking
  - Gerät sperren
  - Gerät entsperren
  - App-Sperre
  - Apps löschen
  - App

Die Seite **Überwachen** bietet eine Übersicht über Geräterichtlinien und Konfigurationen. Die Ansicht umfasst Aktionen zur Problembehandlung, z. B. App sperren/entsperren, App löschen, Gerät sperren/entsperren und Gerät löschen.



Verwenden Sie die Seite **Überwachen** für folgende Aufgaben:

- Suche nach Active Directory (AD)-Benutzern und -Geräten, um eine Fehlerbehebung durchzuführen.
- Analysieren Sie die Seite mit den **Gerätedetails**, die Folgendes enthält:
  - **Richtlinien:** Anzeige der Geräte- und App-Richtlinien für das ausgewählte Gerät und die App. Informationen zum Ändern von Richtlinien finden Sie unter Geräterichtlinien und Apps hinzufügen.

  - **Konfiguration:** Anzeige der Gerätekonfiguration. Symbole geben an, ob Positionsdienste aktiviert sind, ob ein Jailbreak vorliegt und ob das Gerät per MAM oder MDM verwaltet wird. Angaben zum Speicherverschlüsselungsstatus werden ebenfalls angezeigt.
  - **Ausgeführte Anwendungen:** Diese Tabelle enthält die Details aller Anwendungen, die aktuell auf dem Gerät ausgeführt werden.

- Führen Sie eine Problembehandlung auf dem Gerät durch. Die verfügbaren Sicherheitsaktionen auf der Seite basieren auf der Registrierung des Geräts und den Berechtigungen des angemeldeten Administrators:

  - Gerät sperren/entsperren
  - Gerät löschen
  - App sperren/entsperren (verfügbar auf Geräten, die für MAM registriert sind)
  - App löschen (verfügbar auf Geräten, die für MAM registriert sind)

Weitere Informationen zu verfügbaren Aktionen finden Sie unter Sicherheitsaktionen.

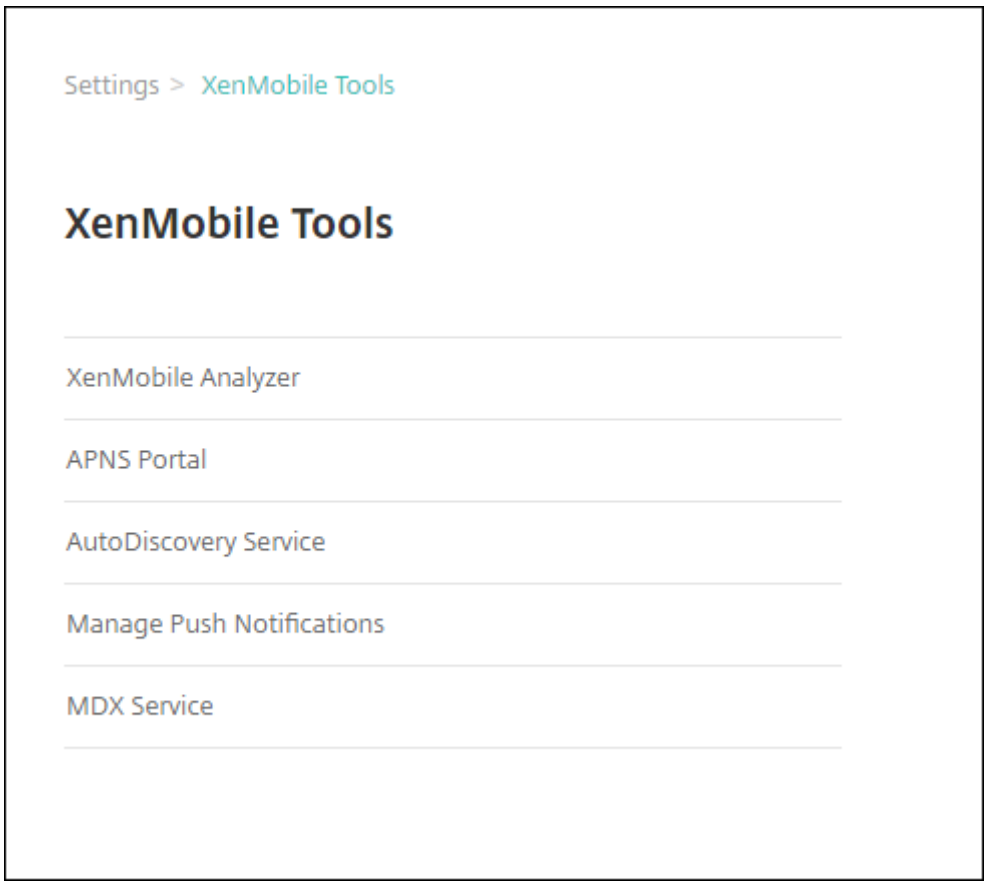
Es kann vorkommen, dass die Seite "Überwachen"60 Minuten nach dem letzten Laden nicht wie erwartet funktioniert, da das Anmelde-Token nicht aktualisiert wurde. Als Workaround aktualisieren Sie den Token indem Sie die Seite neu laden: Klicken Sie in der Dienstkonsole auf den **Citrix Cloud**-Link und dann auf **Citrix Endpoint Management > Verwalten > Überwachen**.

Zugriff auf Citrix Endpoint Management-Tools über die Konsole

Sie können auf diese Citrix Endpoint Management-Tools über die Citrix Endpoint Management-Konsole zugreifen:

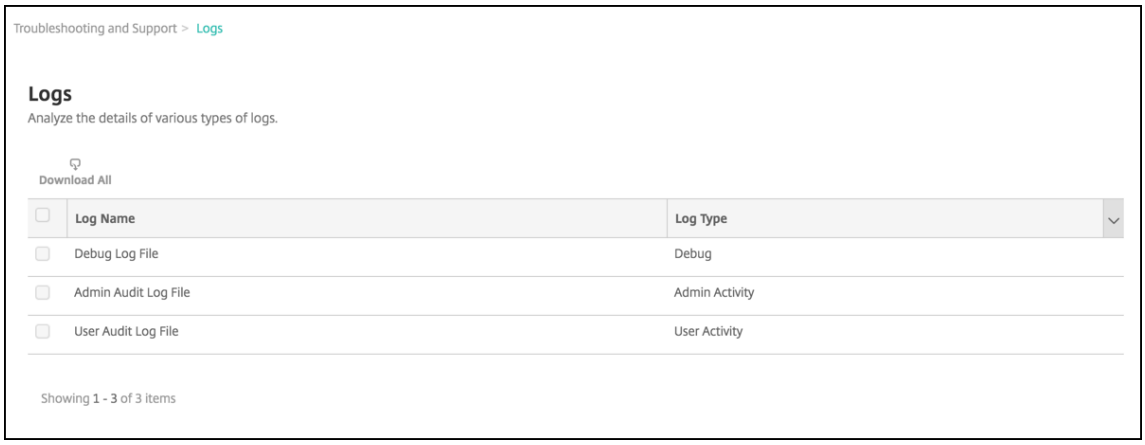
- **APNs-Portal:** Fordern Sie ein signiertes APNs-Zertifikat von Citrix an und senden Sie das Zertifikat dann an Apple.
- **Auto Discovery Service:** Konfigurieren Sie AutoDiscovery für Citrix Endpoint Management in Ihrer Domäne.
- **Verwalten von Pushbenachrichtigungen** –Verwalten Sie Pushbenachrichtigungen für iOS und Windows mobile Apps.

Zum Zugriff auf diese Tools gehen Sie zu **Einstellungen > Citrix Endpoint Management Tools**. Diese Seite steht Benutzern mit Cloudadministrator- oder Kundenadministrator-Rolle zur Verfügung.



Anzeigen und Analysieren von Protokolldateien in Citrix Endpoint Management

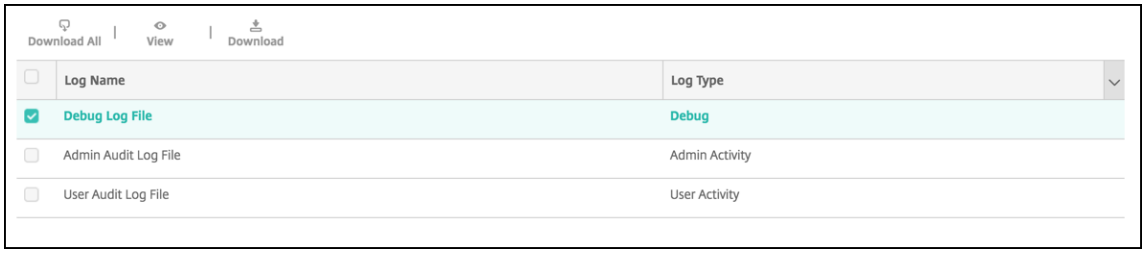
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite **Problembehandlung und Support** wird geöffnet.
2. Klicken Sie unter **Protokollvorgänge** auf **Protokolle**. Die Seite **Protokolle** wird angezeigt. Einzelne Protokolle werden in einer 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 Citrix Endpoint Management-Konsole.
- Benutzerüberwachungsprotokolle enthalten Informationen über konfigurierte Benutzer.

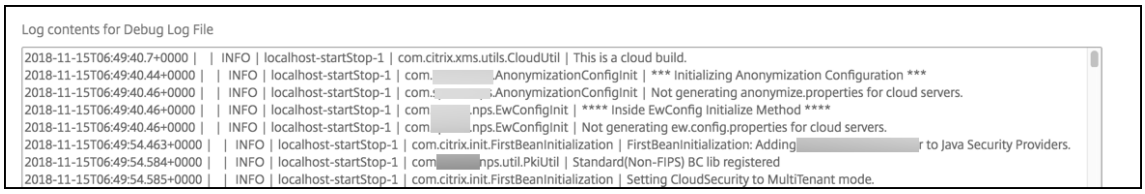
4. Verwenden Sie die Aktionen oberhalb der Tabelle zum Herunterladen aller Protokolle sowie zum Anzeigen oder Herunterladen eines einzelnen Protokolls.



> **Hinweis:**
>
> Wenn Sie mehrere Protokolle auswählen, ist nur die Aktion **Alle herunterladen** verfügbar.

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.
- **Download:** Die Konsole lädt nur den ausgewählten Protokolldateityp herunter. Die Konsole lädt auch alle archivierten Protokolle desselben Typs herunter.



Citrix Endpoint Management 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.

Konnektivitätsprüfungen

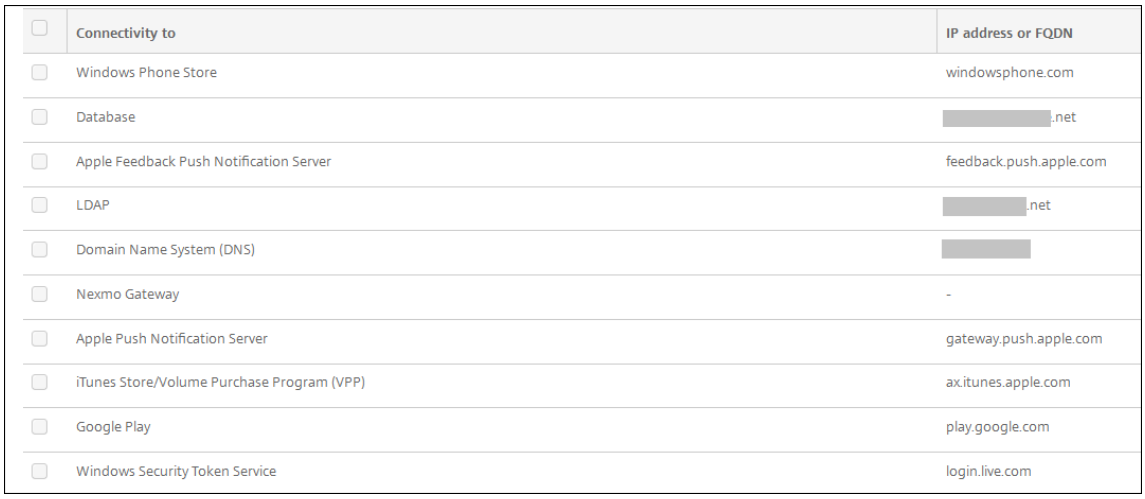
June 25, 2024

Über die Seite **Problembehandlung und Support** können Sie die Verbindung zwischen Citrix Endpoint Management und NetScaler Gateway sowie Citrix Endpoint Management und anderen Servern

und Speicherorten prüfen. Um Konnektivitätsprüfungen in Citrix Endpoint Management auszuführen, benötigen Sie die Support- oder Administrator-Rolle. Legen Sie diese Rolle mit der rollenbasierten Zugriffssteuerung (RBAC) fest. Weitere Informationen zum Zuweisen von Rollen finden Sie unter Rollen mit RBAC konfigurieren.

Ausführen der Citrix Endpoint Management-Konnektivitätsprüfung

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite **Problembehandlung und Support** wird angezeigt.
2. Klicken Sie unter **Diagnose** auf **Citrix Endpoint Management-Konnektivitätsprüfung**. Die Seite **Citrix Endpoint Management-Konnektivitätsprüfung** wird angezeigt. Wenn die Citrix Endpoint Management-Umgebung Clusterknoten enthält, werden alle Knoten angezeigt.

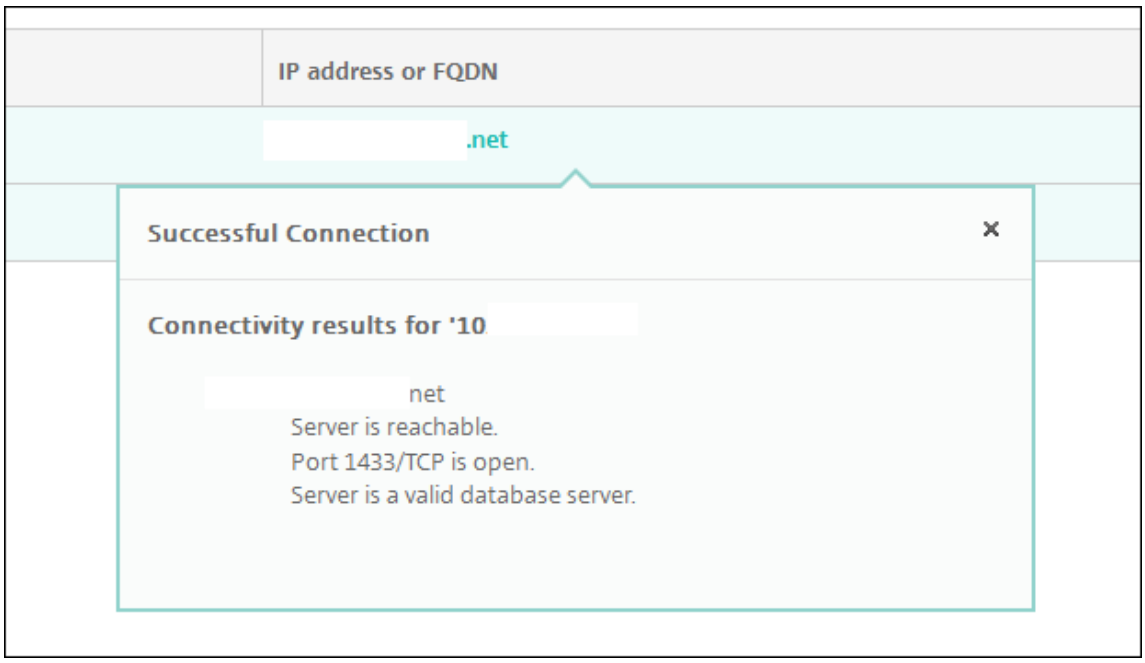


Connectivity to	IP address or FQDN
Windows Phone Store	windowsphone.com
Database	[redacted].net
Apple Feedback Push Notification Server	feedback.push.apple.com
LDAP	[redacted].net
Domain Name System (DNS)	[redacted]
Nexmo Gateway	-
Apple Push Notification Server	gateway.push.apple.com
iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
Google Play	play.google.com
Windows Security Token Service	login.live.com

3. Wählen Sie die Server aus, deren Verbindung geprüft werden soll, und klicken Sie dann auf **Konnektivität testen**. Die Testergebnisseite wird angezeigt.

Connectivity to	IP address or FQDN	
Database	net	✓
Windows Phone Store	windowsphone.com	✓

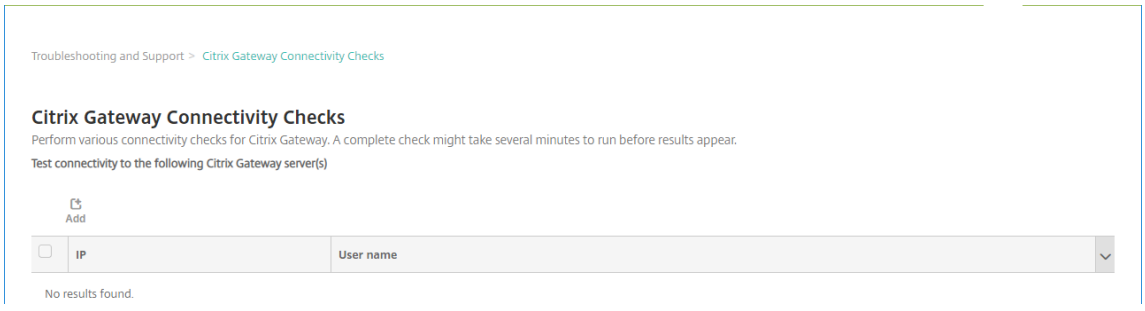
4. Wählen Sie einen Server in der Tabelle mit den Testergebnissen aus, um detaillierte Ergebnisse für den Server anzuzeigen.



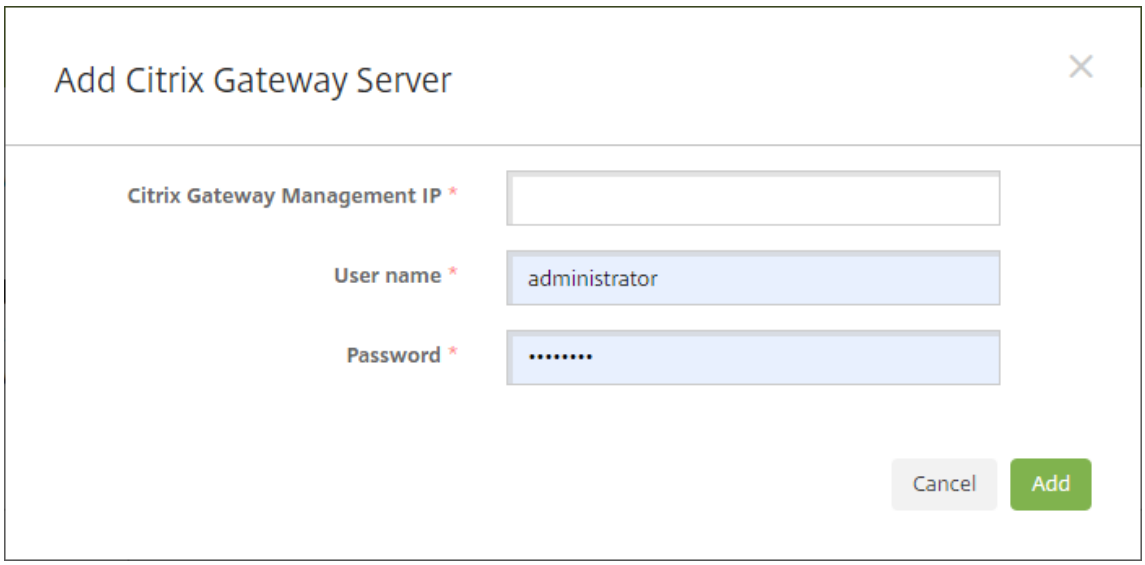
Informationen zu verfügbaren Konnektivitätsprüfungen in Citrix Endpoint Management finden Sie unter Einzelheiten zu Konnektivitätsprüfungen.

Ausführen von NetScaler Gateway-Konnektivitätsprüfungen

1. Klicken Sie auf der Seite **Problembehandlung und Support** unter **Diagnose** auf **NetScaler Gateway-Konnektivitätsprüfung**. Die Seite **NetScaler Gateway-Konnektivitätsprüfung** wird angezeigt. Die Tabelle ist leer, wenn zwischen Citrix Endpoint Management und NetScaler Gateway keine Verbindung besteht.



2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **NetScaler Gateway-Server hinzufügen** wird angezeigt.



3. Geben Sie unter **NetScaler Gateway-Management-IP** die IP-Adresse des Servers mit NetScaler Gateway ein, den Sie testen möchten.

   Wenn Sie eine Konnektivitätsprüfung für einen NetScaler Gateway-Server durchführen, der bereits hinzugefügt wurde, wird die IP-Adresse bereitgestellt.

4. Geben Sie die Administratoranmeldeinformationen für das NetScaler Gateway ein.

   Wenn Sie eine Konnektivitätsprüfung für einen NetScaler Gateway-Server durchführen, der bereits hinzugefügt wurde, wird der Benutzername bereitgestellt.

5. Klicken Sie auf **Hinzufügen**. Das NetScaler Gateway wird der Tabelle auf der Seite **NetScaler Gateway-Konnektivitätsprüfung** hinzugefügt.

6. Wählen Sie den NetScaler Gateway-Server aus und klicken Sie dann auf **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.

Einzelheiten zu Konnektivitätsprüfungen

Die folgende Tabelle enthält verfügbare Konnektivitätsprüfungen in Citrix Endpoint Management und Einzelheiten zu jeder Prüfung.

Konnektivität	IP-Adresse oder FQDN	Details
Apple Push-Benachrichtigungsserver	api.push.apple.com	Überprüft die Konnektivität zwischen dem Apple Push-Benachrichtigungsserver und dem Citrix Endpoint Management-Knoten. Dieser Server ist erforderlich, um Nachrichten an iOS- und macOS-Geräte zu senden.
Apple Feedback-Push-Benachrichtigungsserver	feedback.push.apple.com	Überprüft die Konnektivität zwischen dem Apple Feedback-Server und dem Citrix Endpoint Management-Knoten. Der Server sendet Informationen zu fehlgeschlagenen Remote-Benachrichtigungen, die an iOS- und macOS-Geräte gesendet wurden.
Citrix Lizenzserver	IP-Adresse des Lizenzservers	Überprüft die Konnektivität zwischen dem Citrix Lizenzserver und dem Citrix Endpoint Management-Knoten. Server mit Citrix Produkten rufen Lizenzen vom Citrix Lizenzserver ab.
NetScaler Gateway	FQDN von NetScaler Gateway in Citrix Endpoint Management konfiguriert	Überprüft die Konnektivität zwischen dem NetScaler Gateway und dem Citrix Endpoint Management-Knoten. Citrix Endpoint Management Client-Apps (wie Citrix Secure Mail und Citrix Secure Web) stellen mit NetScaler Gateway eine Verbindung über einen VPN-Server her, um auf interne Netzwerke zuzugreifen.

Konnektivität	IP-Adresse oder FQDN	Details
Datenbank	IP-Adresse oder FQDN des Datenbankservers	Überprüft die Konnektivität zwischen der Citrix Endpoint Management-Datenbank und dem Citrix Endpoint Management-Knoten.
Domain Name System (DNS)	In Citrix Endpoint Management konfigurierte IP-Adresse	Überprüft die Konnektivität zwischen dem DNS-Server und dem Citrix Endpoint Management-Knoten.
Secure Ticket Authority (STA)-Service	localhost	Überprüft die Verbindung zwischen dem Citrix Endpoint Management-Knoten und Authentifizierungs-, STA (Secure Ticket Authority)- und Clusterdiensten.
Firebase Cloud Messaging (FCM)-Server		Überprüft die Konnektivität zwischen dem FCM-Server und dem Citrix Endpoint Management-Knoten. Mit FCM können Sie eine Client-App benachrichtigen, sobald eine neue E-Mail oder andere Daten für die Synchronisierung verfügbar sind. Mit diesen Benachrichtigungen können Sie die Benutzerinteraktion und Kundenbindung fördern. FCM ist ein Ersatz für Google Cloud Messaging (GCM).

Konnektivität	IP-Adresse oder FQDN	Details
Google Play	play.google.com	Überprüft die Konnektivität zwischen dem Google Store-Server und dem Citrix Endpoint Management-Knoten. Google Play wird verwendet, um Dienste wie einen verwalteten, privaten Store für die Bereitstellung von Unternehmensapps anzubieten.
iTunes Store/Volume Purchase	vpp.itunes.apple.com	Überprüft die Konnektivität zwischen dem Apple Store-Server und dem Citrix Endpoint Management-Knoten. Apple Store wird verwendet, um Dienste wie einen verwalteten, privaten Store für die Bereitstellung von Unternehmensapps anzubieten.
LDAP	IP-Adresse oder FQDN des in Citrix Endpoint Management konfigurierten LDAP	Überprüft die Konnektivität zwischen dem LDAP-Server und dem Citrix Endpoint Management-Knoten.
Microsoft Push-Benachrichtigungsserver	sin.notifiy.windows.com	Überprüft die Konnektivität zwischen dem Windows-Benachrichtigungsserver und dem Citrix Endpoint Management-Knoten. Dieser Server wird verwendet, um Nachrichten an Windows-Geräte zu senden.

Konnektivität	IP-Adresse oder FQDN	Details
ShareFile-Service	IP-Adresse oder FQDN des in Citrix Endpoint Management konfigurierten ShareFile Service	Überprüft die Konnektivität zwischen dem ShareFile Service und Citrix Endpoint Management. Der ShareFile Service ist eine sichere cloudbasierte Plattform, auf der Unternehmen große Dateien speichern und freigeben können.
Windows Desktop/Tablet Store	windows.microsoft.com	Überprüft die Konnektivität zwischen dem Windows Desktop/Tablet Store und dem Citrix Endpoint Management-Knoten. Der Windows Desktop/Tablet Store wird verwendet, um Dienste wie einen verwalteten, privaten Store für die Bereitstellung von Unternehmensapps anzubieten.
Windows Sicherheitstokendienst	login.live.com	Überprüft die Konnektivität zwischen dem Windows Sicherheitstoken-Server und dem Citrix Endpoint Management-Knoten. Der Windows-Sicherheitstokendienst unterstützt die zweistufige Authentifizierung (Domäne plus Sicherheitstoken) für Windows-Geräte.

Mobilfunkanbieter

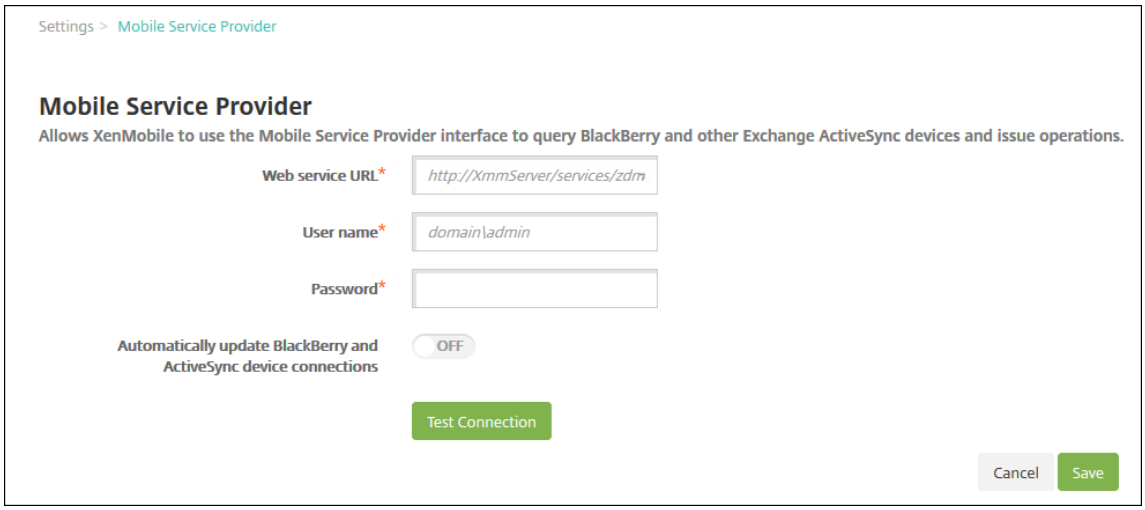
December 1, 2023

Sie können Citrix Endpoint Management so konfigurieren, dass die Schnittstelle der Mobilfunkanbieter zum Abfragen von BlackBerry- und Exchange ActiveSync-Geräten und Auslösen von Vorgängen verwendet wird.

Beispiel: Ihr Unternehmen hat 1000 Benutzer und jeder Benutzer hat mindestens ein Gerät. Nachdem Sie alle Benutzer angewiesen haben, ihre Geräte bei Citrix Endpoint Management zu registrieren, wird in der Citrix Endpoint Management-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 Citrix Endpoint Management-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. Der Standardwert ist **Aus**.
   - Klicken Sie auf **Verbindung testen**, um die Konnektivität zu prüfen.
4. Klicken Sie auf **Speichern**.

Berichte

June 25, 2024

Citrix Endpoint Management 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 im Diagramm zum Anzeigen 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 per Citrix Endpoint Management-Servereigenschaft `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 fehlgeschlagene Bereitstellungen**: Liste mit bis zu 10 Apps, deren Bereitstellung fehlgeschlagen ist
- **Gesperrte Apps nach Geräten & Benutzer:** Liste mit gesperrten Apps, die Benutzer auf ihren Geräten haben
- **Nicht richtlinientreue Geräte:** Listet alle Geräte auf, die nicht die Kriterien zur Richtlinientreue erfüllen. Kriterien sind beispielsweise, ob ein Jailbreak vorliegt, welche Betriebssystemversion ausgeführt wird oder ob ein Passcode vorhanden ist. Der Bericht zeigt auch den Benutzernamen an, der dem Gerät zugeordnet ist, und ob das Gerät verschlüsselt ist. Bei iOS-Geräten wird in der Spalte zur Verschlüsselung "N/A"angezeigt.

Sie können die Daten der Tabellen im CSV-Format exportieren und dann mit einem Programm wie Microsoft Excel öffnen. Diagramme für jeden Bericht können im PDF-Format exportiert werden.

Die Registerkarte **Berichterstellung** zeigt Gerätedetails wie Seriennummer, IMEI/MEID, Apps und Verbindungen an. Um umfassendere Berichte für ein bestimmtes Gerät zu erhalten, gehen Sie zu **Verwalten > Geräte**, klicken auf das Gerät und dann auf **Mehr anzeigen** und rufen die Seite **Gerätedetails** auf. Auf der Seite **Gerätedetails** sind Gerätesicherheitseigenschaften, Geräteeigenschaften, zugewiesene Richtlinien, Apps, Aktionen, Zertifikate und mehr aufgeführt. Informationen über die

Seite mit den **Gerätedetails** finden Sie unter Informationen über Geräte abrufen.

Die folgenden Aspekte bestimmen, wie Informationen zu bereitgestellten oder installierten Apps auf verwalteten Geräten in Citrix Endpoint Management erfasst werden:

- Gerätetyp
- Registrierungsmethode
- Ob die App-Bestandsrichtlinie für Geräte bereitgestellt ist

Bei Android-Geräten ist das Verhalten je nach Gerätetyp und Registrierungsmethode unterschiedlich. Die folgende Tabelle zeigt an, wo Apps für **Android Enterprise** aufgeführt werden (Seite **Gerätedetails**, Berichte oder nicht verfügbar). App-Listen enthalten alle Apps (sofern nicht anders angegeben).

	MDM + MAM (alle Apps)	MDM (alle Apps)
Erforderliche Apps (die App-Bestandsrichtlinie ist nicht bereitgestellt)	Seite **Gerätedetails** und Berichte	Öffentliche Apps; Seite **Gerätedetails** und Berichte
Optionale Apps (die App-Bestandsrichtlinie ist nicht bereitgestellt)	Nicht verfügbar	Nicht verfügbar
Erforderliche Apps (die App-Bestandsrichtlinie ist bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte
Optionale Apps (die App-Bestandsrichtlinie ist bereitgestellt)	Unternehmensapps, MDX-Apps, öffentliche und Weblink-Apps; Berichte	Seite **Gerätedetails** und Berichte

Die folgende Tabelle zeigt an, wo Apps für **Android (Legacy-Geräteadmin)** aufgeführt werden (Seite **Gerätedetails**, Berichte oder nicht verfügbar). App-Listen enthalten alle Apps (sofern nicht anders angegeben).

	MDM + MAM (alle Apps)	MDM (öffentliche und Unternehmensapps)	MAM
Erforderliche Apps (die App-Bestandsrichtlinie ist nicht bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte	–

	MDM + MAM (alle Apps)	MDM (öffentliche und Unternehmensapps)	MAM
Optionale Apps (die App-Bestandsrichtlinie ist nicht bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte	Nicht verfügbar
Erforderliche Apps (die App-Bestandsrichtlinie ist bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte	–
Optionale Apps (die App-Bestandsrichtlinie ist bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte	Nicht verfügbar

Bei iOS-Geräten ist das Verhalten je nach Registrierungsmethode unterschiedlich. Die folgende Tabelle zeigt an, wo Apps aufgeführt werden (Seite **Gerätedetails** oder Berichte). App-Listen enthalten alle Apps (sofern nicht anders angegeben).

	MDM + MAM (alle Apps)	MDM (öffentliche und Unternehmensapps)	MAM (alle Apps)
Erforderliche Apps (die App-Bestandsrichtlinie ist nicht bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte. Diese Apps werden im Status “Ausstehend” angezeigt (auch wenn sie nicht installiert sind) oder bleiben nach der manuellen Installation im Status “Ausstehend”.

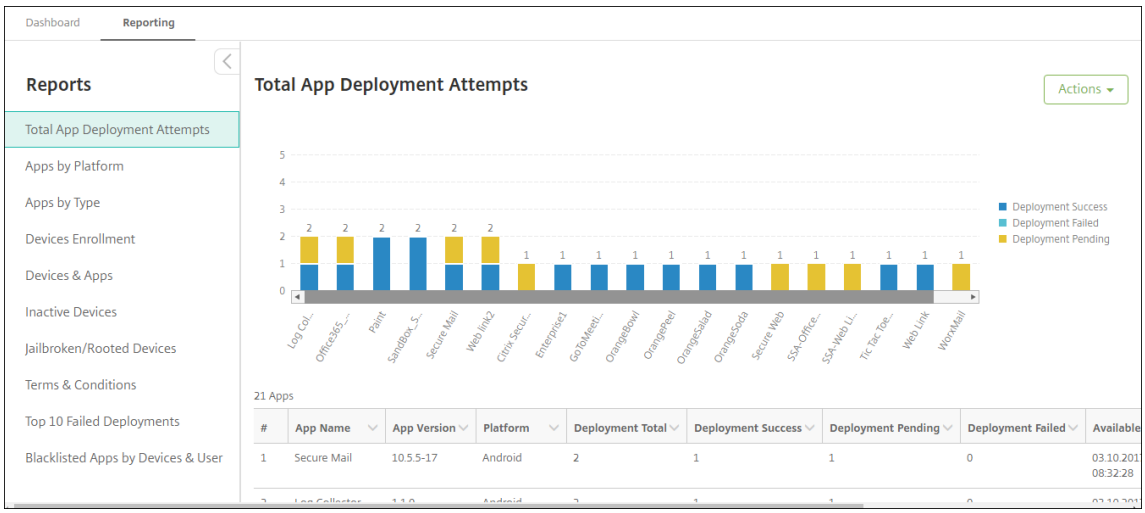
	MDM + MAM (alle Apps)	MDM (öffentliche und Unternehmensapps)	MAM (alle Apps)
Optionale Apps (die App-Bestandsrichtlinie ist nicht bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte	Web-, SaaS- und Weblink-Apps werden auf der Seite **Gerätedetails** als installierte Apps angezeigt. Sie werden nicht in Berichten aufgeführt. Unternehmensapps, MDX-Apps und öffentliche Apps werden nicht auf der Seite **Gerätedetails** aufgeführt, nachdem sie manuell installiert wurden. Apps werden nicht in Berichten aufgeführt, nachdem sie manuell installiert wurden.
Erforderliche Apps (die App-Bestandsrichtlinie ist bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte	Die App-Bestandsrichtlinie kann nicht auf Geräten bereitgestellt werden. Apps werden auf der Seite **Gerätedetails** und in Berichten aufgeführt. Diese Apps werden im Status “Ausstehend” angezeigt (auch wenn sie nicht installiert sind) oder bleiben nach der manuellen Installation im Status “Ausstehend”.

	MDM + MAM (alle Apps)	MDM (öffentliche und Unternehmensapps)	MAM (alle Apps)
Optionale Apps (die App-Bestandsrichtlinie ist bereitgestellt)	Seite **Gerätedetails** und Berichte	Seite **Gerätedetails** und Berichte	Die App-Bestandsrichtlinie kann nicht auf Geräten bereitgestellt werden. Web-, SaaS- und Weblink-Apps werden auf der Seite **Gerätedetails** als installierte Apps angezeigt. Sie werden nicht in Berichten aufgeführt. Unternehmensapps, MDX-Apps und öffentliche Apps werden nicht auf der Seite **Gerätedetails** aufgeführt, nachdem sie manuell installiert wurden. Apps werden nicht in Berichten aufgeführt, nachdem sie manuell installiert wurden.

Für macOS - und Windows-Geräte wird der App-Bestand in Citrix Endpoint Management *nur dann* erfasst, wenn die App-Bestandsrichtlinie bereitgestellt wird.

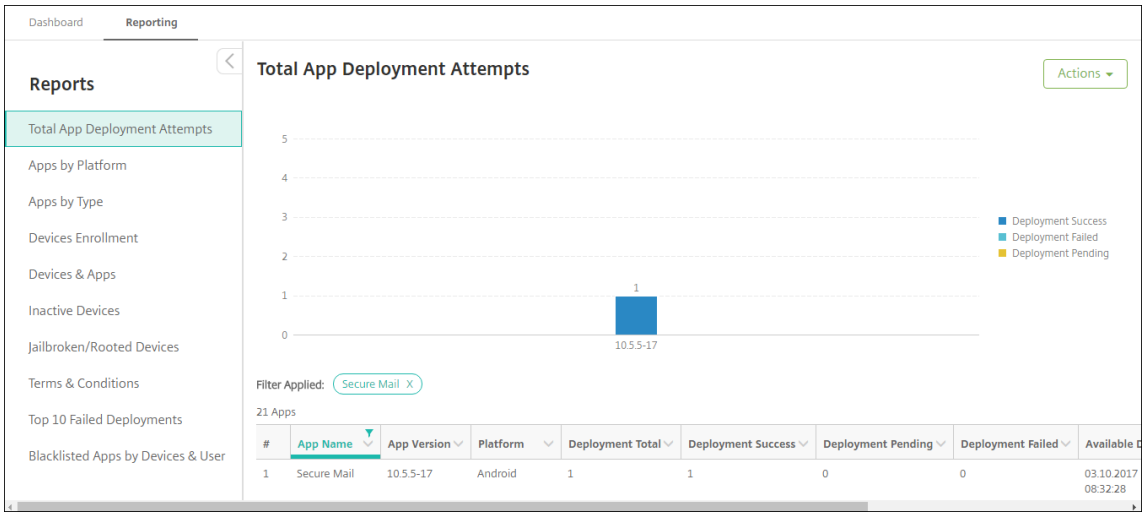
Erstellen eines Berichts

1. Klicken Sie in der Citrix Endpoint Management-Konsole auf**Analysieren > Berichterstellung**. Die Seite **Berichterstellung** wird angezeigt.
2. Klicken Sie auf den gewünschten Bericht.

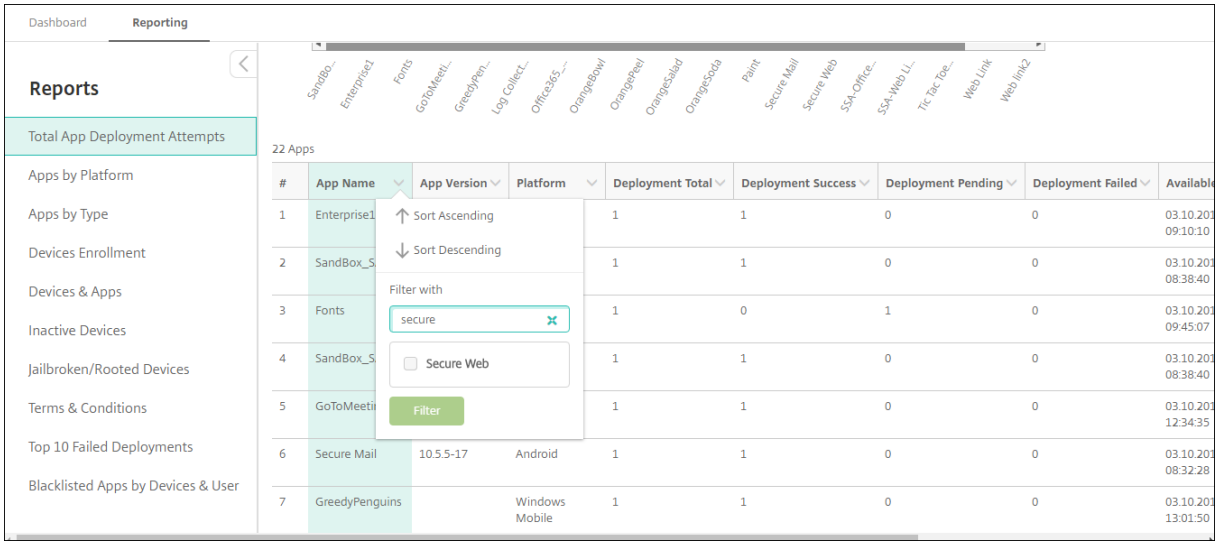


Anzeigen von Berichtdetails

1. Klicken Sie auf einzelne Bereiche des Diagramms, um weitere Details anzuzeigen.

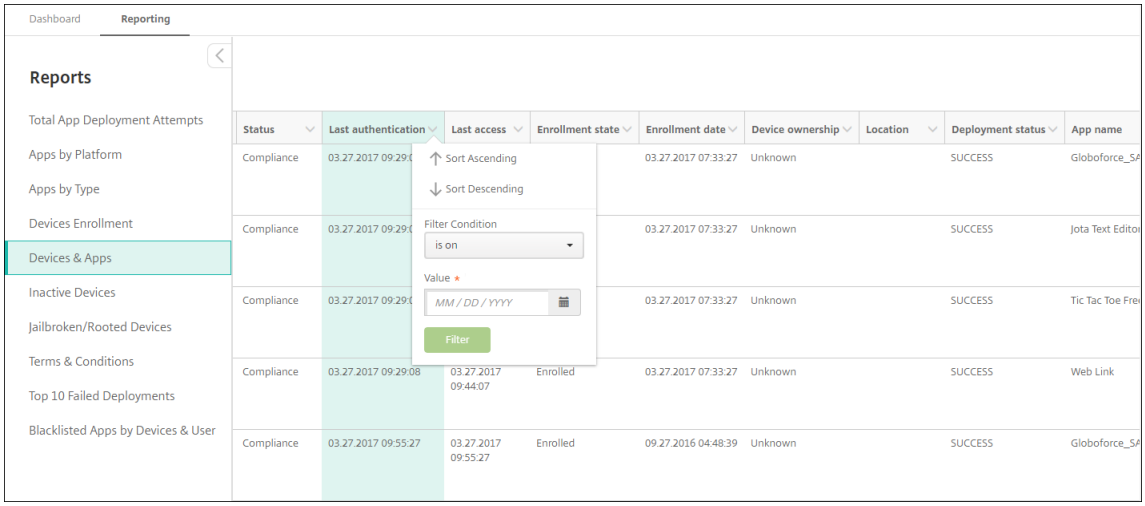


Zum Sortieren, Filtern oder Durchsuchen einer Tabellenspalte klicken Sie auf die Spaltenüberschrift

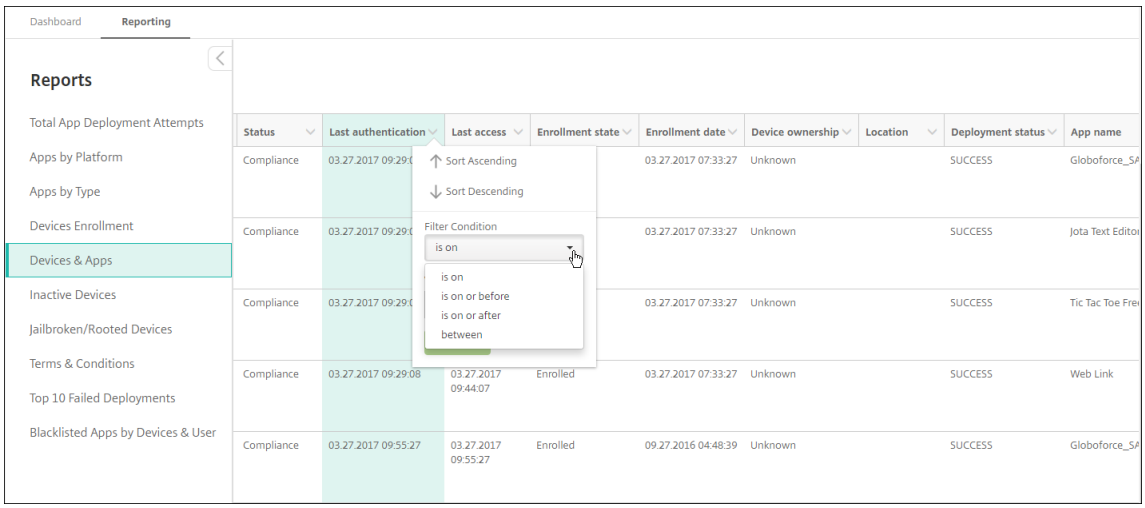


Filtern eines Berichts nach Datum

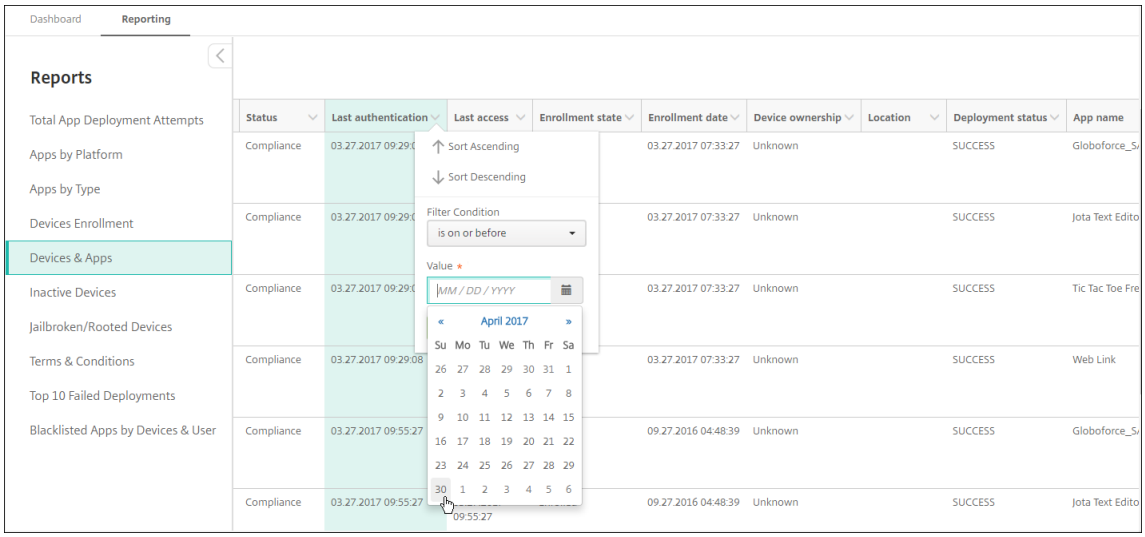
1. Klicken Sie auf eine Spaltenüberschrift, um die Filtereinstellungen anzuzeigen.



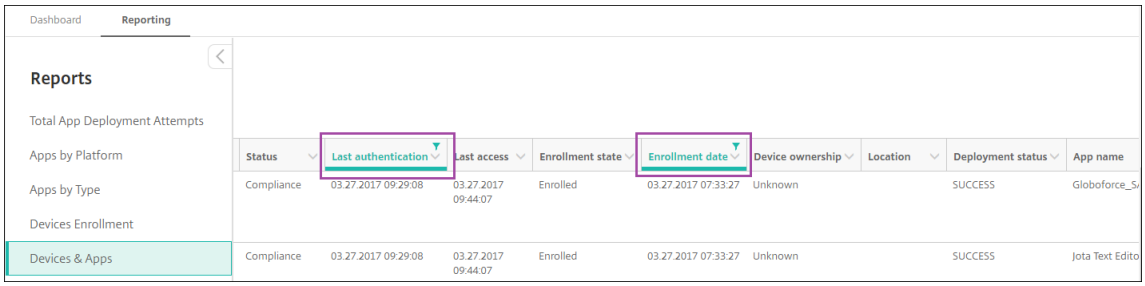
2. Wählen Sie über **Filterbedingung** aus, wie Sie die angezeigten Daten filtern möchten.



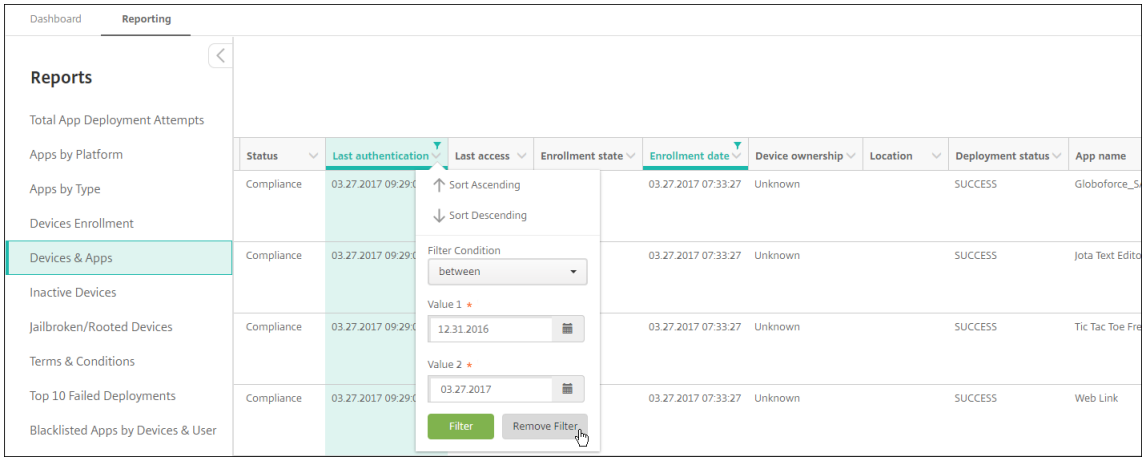
3. Verwenden Sie für Datumsangaben die Datumsauswahl.



4. Spalten mit Datumsfilter werden wie im folgenden Beispiel gezeigt angezeigt.

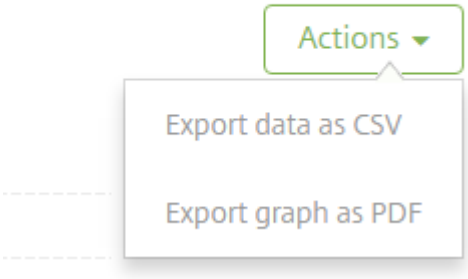


5. Um einen Filter zu entfernen, klicken Sie auf die Spaltenüberschrift und dann auf **Filter entfernen**.



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**.



REST-APIs

March 11, 2024

Mit der Citrix Endpoint Management-REST-API haben Sie folgende Möglichkeiten:

- Aufrufen von Diensten, die in der Citrix Endpoint Management-Konsole angezeigt werden
- Aufrufen von REST-Diensten über einen beliebigen REST-Client

Die API erfordert zum Aufrufen der Dienste keine Anmeldung an der Citrix Endpoint Management-Konsole.

Eine umfassende, aktuelle Liste der verfügbaren APIs finden Sie in der PDF-Datei Public API for REST Services.

Zur Verwaltung Ihrer mobilen und Desktop-Endgeräte und zur Konfiguration der Einstellungen für Ihre Workspace-Apps stehen APIs zur Verfügung. Gehen Sie zu https://developer.cloud.com/citrixworkspace und navigieren Sie zu **Citrix Endpoint Management > Mobile Application Integration**.

Erforderliche Berechtigungen für den Zugriff auf die REST API

Für den Zugriff auf die REST API ist eine der folgenden Berechtigungen erforderlich:

- Citrix Cloud-Administrator
- Zugriffsberechtigung für öffentliche APIs, die bei der Konfiguration des rollenbasierten Zugriffs festgelegt wird Informationen finden Sie unter Konfigurieren von Rollen mit RBAC.
- Superuser-Benutzerberechtigung

Um mit dem Citrix Cloud-Konto auf die REST-API zuzugreifen, generieren Sie die **API**-Schlüssel:

1. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.
2. Wählen Sie **API-Zugriff > Sichere Clients**.
3. Geben Sie einen Namen für den sicheren Client ein und klicken Sie auf **Client erstellen**.

Citrix Cloud erstellt dann die Client-ID und den geheimen Clientschlüssel für den Client. Laden Sie eine Kopie der Informationen herunter und speichern Sie sie offline an einem sicheren Ort. Citrix Cloud speichert diese eindeutigen Bezeichner nicht, nachdem Sie das Dialogfeld geschlossen haben.

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

Das folgende Beispiel zeigt die Anmeldung mit einem Token, der über die Citrix Cloud-API abgerufen wird.

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

Methodentyp: POST

Inhaltstyp: application/json

Anforderungsbeispiel:

```
{

 "bearerToken": "eyJ0eOiJSUzJiibGcI1AiONiJ9.
    eyJkIjoMDExN1c2VIXiMzNDc1OTk4...qf0iQ"
 }

<!--NeedCopy-->
```

Sie müssen den Bearertoken mit der Citrix Cloud-API `https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clients` abrufen. Informationen hierzu finden Sie in der Dokumentation für Entwickler.

Antwortbeispiel:

```
{

 "auth_token": "q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"
 }

<!--NeedCopy-->
```

Verwandte Informationen

- Citrix Endpoint Management REST-API

ActiveSync-Gateway

December 1, 2023

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 Citrix Endpoint Management konfigurieren. Das ActiveSync-Gateway speichert eine Liste der ActiveSync-IDs für alle in Citrix Endpoint Management konfigurierten Geräte. Je nach konfigurierten Regeln können Sie Geräten dann auf der Basis dieser ActiveSync-IDs den Zugriff auf ActiveSync-Daten bewilligen oder verweigern. Wenn Sie beispielsweise die Regel **Fehlende Pflicht-Apps** aktivieren, prüft Citrix Endpoint Management per App-Zugriffsrichtlinie auf erforderliche Apps. Wenn die erforderlichen Apps fehlen, verweigert die Richtlinie den Zugriff auf

ActiveSync-Daten. 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.

Citrix Endpoint Management unterstützt die folgenden Regeln:

Anonyme Geräte: Prüft, ob ein Gerät im anonymen Modus ist. Diese Prüfung ist verfügbar, wenn Citrix Endpoint Management bei einer Wiederverbindung den Benutzer des Geräts nicht erneut authentifizieren kann.

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. Basierend auf dieser Liste werden Verbindungen dann zugelassen oder blockiert. 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 meist von automatisierten Aktionen geändert oder von Drittanbietern, die Citrix Endpoint Management-APIs verwenden.

Widerrufenstatus: Prüft, ob das Gerätezertifikat widerrufen worden ist. Ein widerrufenes Gerät kann erst erneut registriert werden, wenn es wieder autorisiert ist.

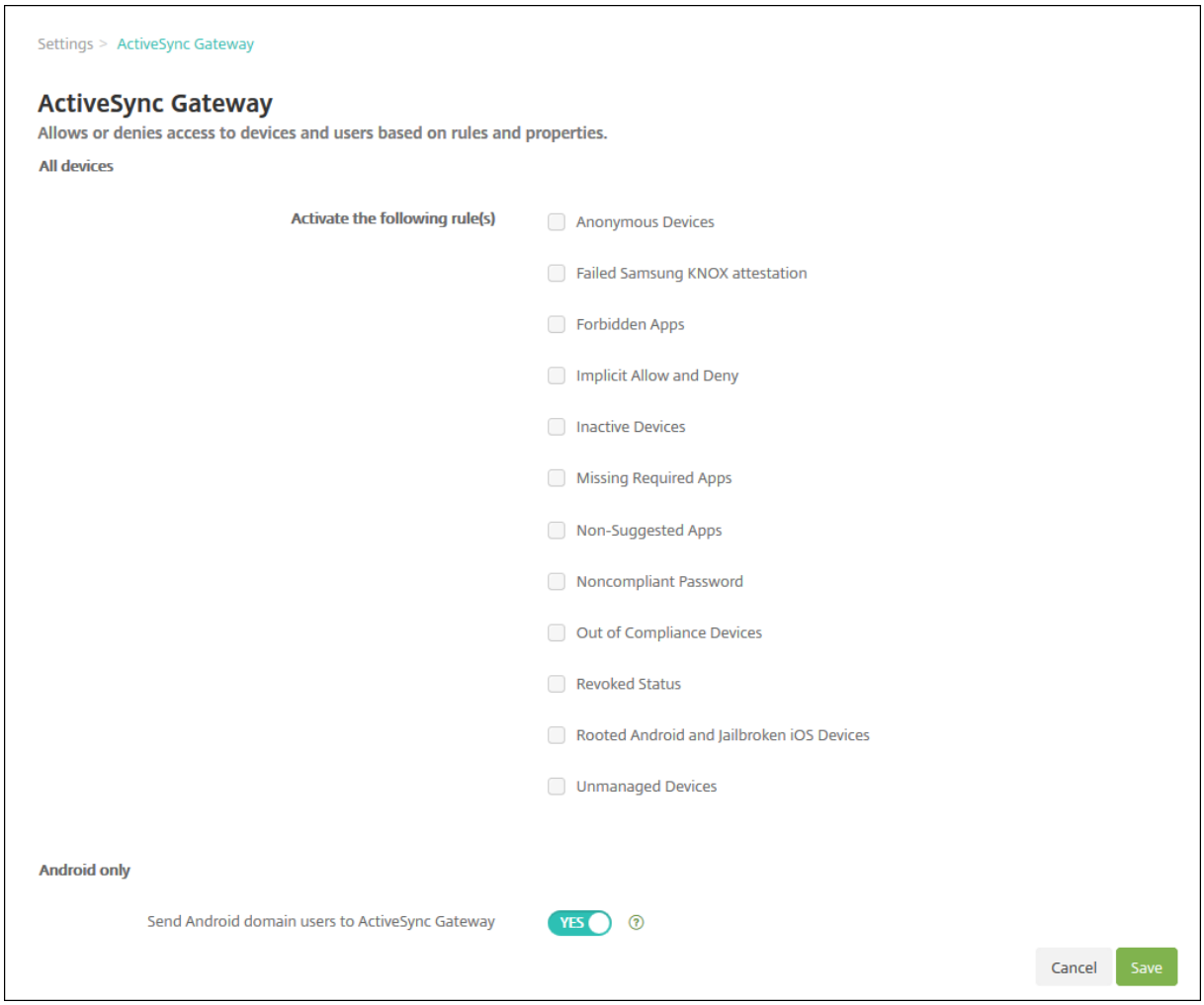
Android-Geräte mit Rooting oder iOS-Geräte mit Jailbreak: Prüft, ob auf einem Android- oder iOS-Gerät ein Jailbreak vorliegt.

Nicht verwaltete Geräte: Prüft, ob ein Gerät verwaltet, d. h. von Citrix Endpoint Management 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 Citrix Endpoint Management Benutzernamen und ActiveSync-ID von Android-Gerätebesitzern an das ActiveSync-Gateway sendet. Aktivieren Sie diese Funktion nur, wenn Sie eine Legacy-Konfiguration ausführen. In neueren Konfigurationen ermöglicht diese Funktion jedem Gerät den Zugriff auf ActiveSync-Daten, solange der Benutzername, der dem Gerät zugeordnet ist, auf dem Gateway vorhanden ist.

Konfigurieren der Einstellungen für ActiveSync-Gateway

1. Klicken Sie in der Citrix Endpoint Management-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**, damit Citrix Endpoint Management Android-Geräteinformationen an das ActiveSync-Gateway sendet.
3. Klicken Sie auf **Speichern**.

Citrix Endpoint Management Connector für Exchange ActiveSync

June 25, 2024

XenMobile Mail Manager heißt jetzt Citrix Endpoint Management Connector für Exchange ActiveSync. Informationen zum vereinheitlichten Citrix-Portfolio finden Sie im Citrix product name guide.

Der Connector erweitert die Funktionalität von Citrix Endpoint Management 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 Citrix Endpoint Management auf durch Exchange bereitgestellte EAS-Gerätepartnerschaftsinform
- Löschen eines mobilen Geräts durch Citrix Endpoint Management auf der Basis des EAS-Status.
- Zugriff von Citrix Endpoint Management 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.

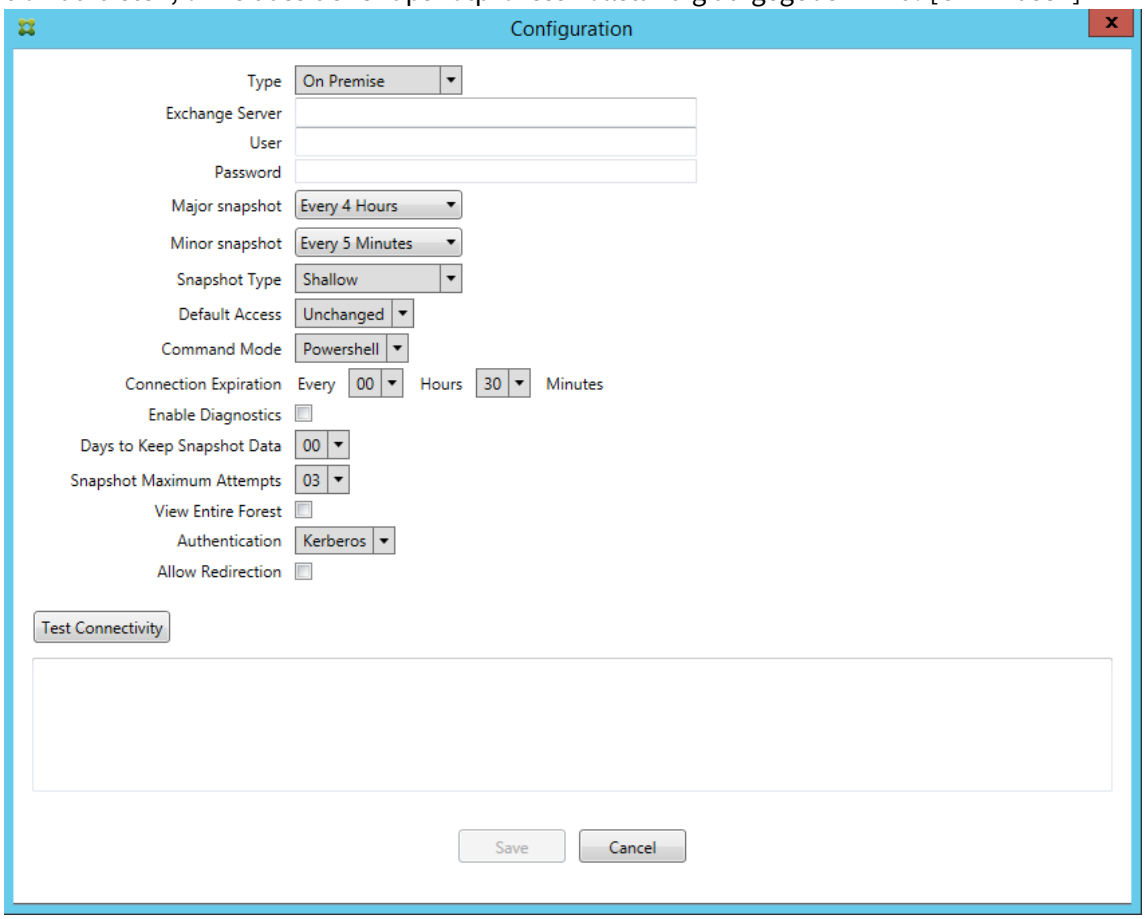
> **Wichtig:**
>
> Ab Oktober 2022 bieten Citrix Endpoint Management Connector und NetScaler Gateway Connector für Exchange ActiveSync angesichts der von Microsoft hier angekündigten Authentifizierungsänderungen keine Unterstützung mehr für Exchange Online. Der Citrix Endpoint Management Connector für Exchange funktioniert weiterhin mit Microsoft Exchange Server (on-premises).

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]

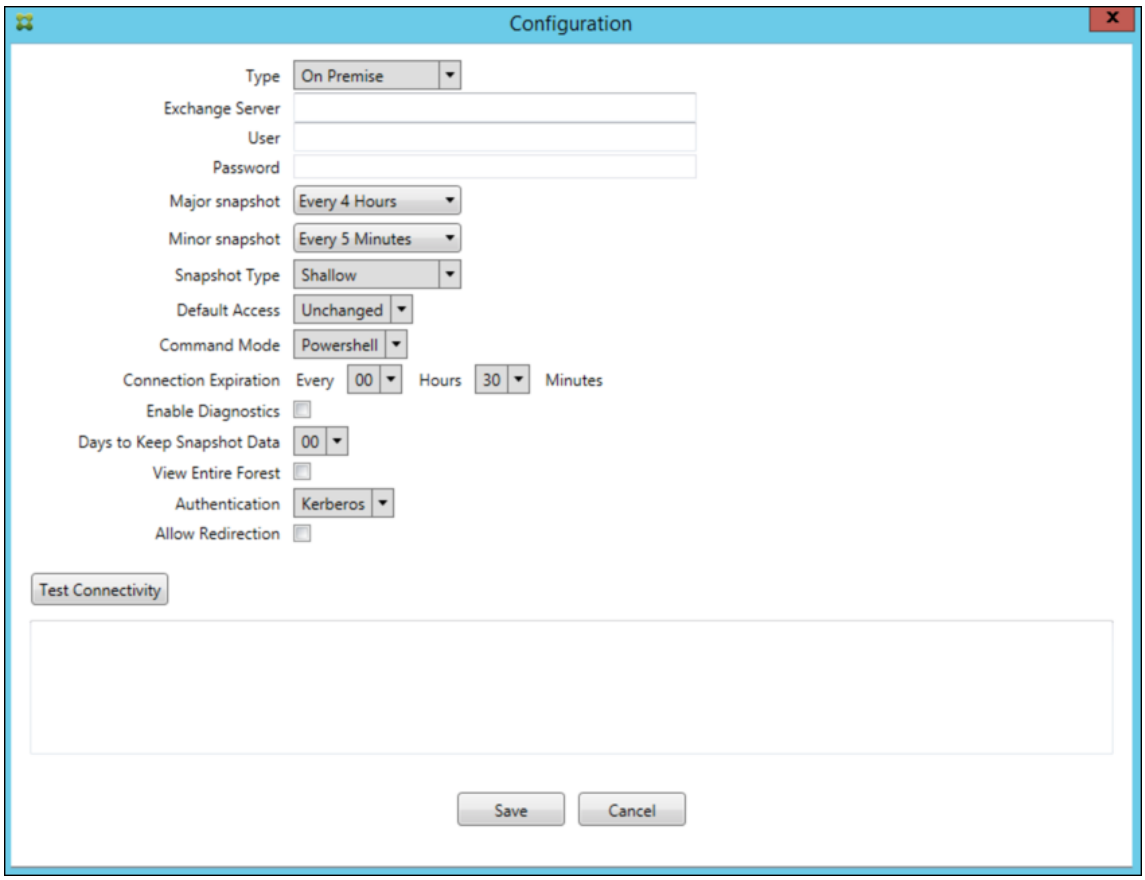


- In früheren Versionen wurde der Snapshottyp nicht in der Liste der Exchange-Konfigurationen angezeigt. Nun wird der Snapshottyp angezeigt. [CXM-70846]
- Die von PowerShell gemeldete PSRemotingTransport-Ausnahme weist darauf hin, dass die Exchange-Sitzung nicht mehr funktionsfähig ist. Der Status wird 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]

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]



Was ist neu in früheren Releases

Im folgenden Abschnitt werden die neuen Features und behobenen Probleme in früheren Versionen des Citrix Endpoint Management Connectors für Exchange ActiveSync aufgeführt.

Neue Features in Version 10.1.8

- Es kann vorkommen, dass Exchange verhindert, dass der Citrix Endpoint Management Connector für Exchange ActiveSync zu häufig Befehle ausgibt. Dies tritt häufig in Verbindungen mit Office 365 auf. 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 sonst "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 Citrix 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 Citrix 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 oder nach dem Gleichheitszeichen und vor dem Wert, ordnet der Citrix 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 "Neue Features"-Abschnitten wird für den Citrix Endpoint Management Connector für Exchange ActiveSync der bisherige Name "XenMobile Mail Manager"verwendet. Der Name wurde gegenüber Version 10.1.7 geändert.

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. Dies führt zu unvollständigen Daten. 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]
- Bei einem nicht auflösbaren Fehler in einem Richtlinienaktualisierungsbefehl für Exchange 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. bis zum nächsten Snapshotversuch nicht lang genug gewartet. Dies führte zu einer weiteren Drosselung und dem Fehlschlagen des Snapshots. XenMobile Mail Manager hält jetzt die von Exchange festgelegte Wartezeit zwischen Snapshotversuchen 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 `lastname, firstname` 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 Einschränkungen

> **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 die Richtlinien für die Geräte des Postfachs können nicht 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 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]

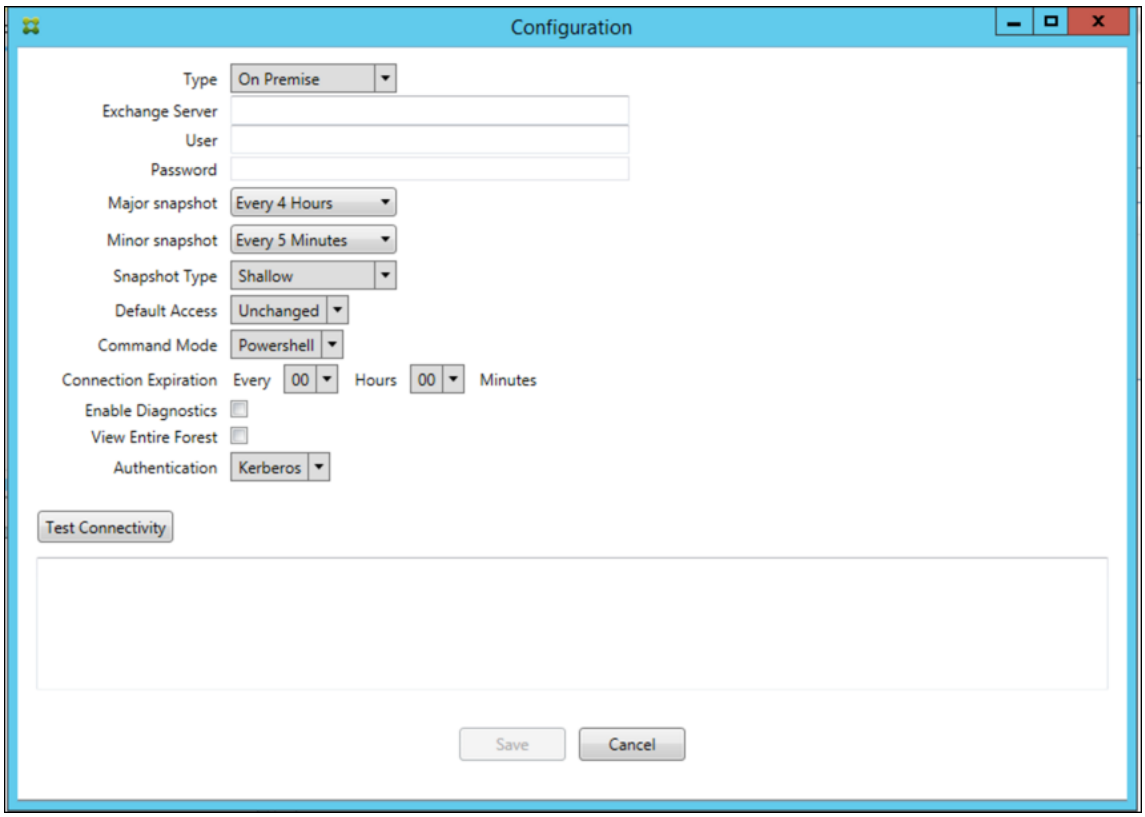
Neue Features in Version 10.1.4

Bei Version 10.1.4 von XenMobile Mail Manager wurden folgende Probleme behoben:

- Aufgrund der schwächeren Sicherheit werden TLS 1.0 und TLS 1.1 vom PCI Council nicht mehr unterstützt. XenMobile Mail Manager unterstützt jetzt TLS 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 gelegentlich 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

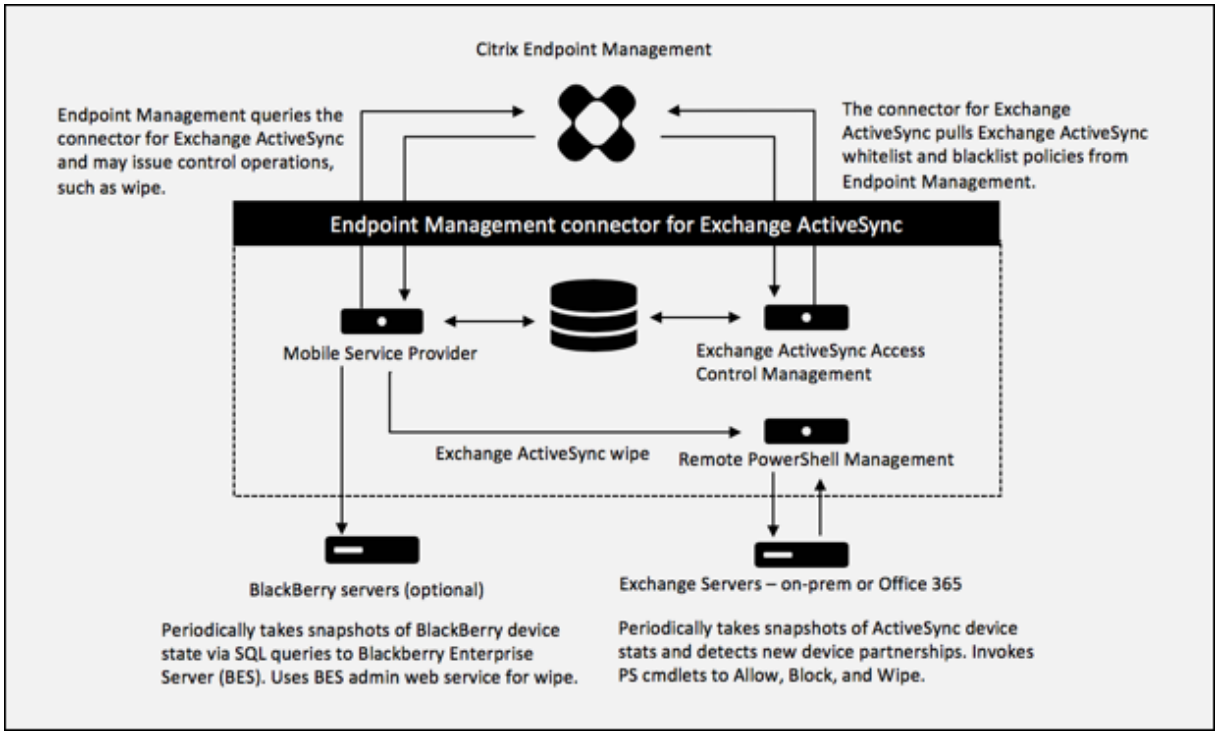
- **Verbesserte Verbindung mit Exchange:** XenMobile Mail Manager verwendet PowerShell-Sitzungen für die Kommunikation mit Exchange. Eine PowerShell-Sitzung kann –insbesondere bei Office 365 –nach einiger Zeit instabil werden, sodass Befehle nicht mehr ausgeführt werden. In XenMobile Mail Manager können 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 durch drei neue Diagnosedateien erleichtert, 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

Das folgende Diagramm zeigt die Hauptkomponenten des Citrix Endpoint Management-Connectors für Exchange ActiveSync. Ein detailliertes Architekturdiagramm finden Sie unter Architektur.



Die zwei Hauptkomponenten sind:

- **Exchange ActiveSync Access Control Management:** ruft eine Exchange ActiveSync-Richtlinie bei Citrix Endpoint Management 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.

Systemanforderungen und Voraussetzungen

Für den Citrix 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 und die Unterstützung für Windows Server 2012 R2 endet am 10. Oktober 2023.
- Microsoft SQL Server 2016 Service Pack 2, SQL Server 2014 Service Pack 3 oder SQL Server 2012 Service Pack 4.
- 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 (Unterstützung endet am 11. April 2023)
- 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 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 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 on-premises 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 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 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 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

1. Klicken Sie auf die Datei XmmSetup.msi und folgen Sie den Anweisungen des Installers zum Installieren des Citrix 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 Connector für Exchange ActiveSync über das Menü **Start**.
3. Konfigurieren Sie die folgenden Datenbankeigenschaften:

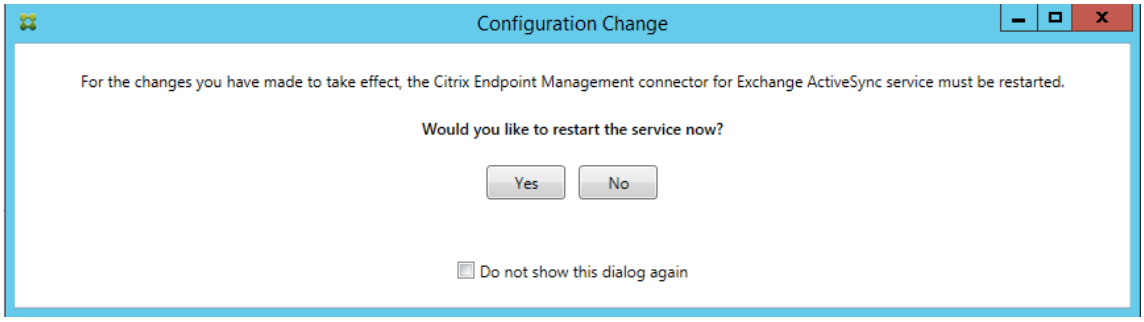
- Wählen Sie die Registerkarte **Configure > Database** aus.
- Geben Sie den Namen des SQL-Servers ein (standardmäßig “localhost”).
- Behalten Sie den Standarddatenbanknamen **CitrixXmm** bei.

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 XenMobile Mail Manager-Diensts 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 XenMobile Mail Manager-Diensteintrag und klicken Sie dann auf die Registerkarte **Anmelden**.

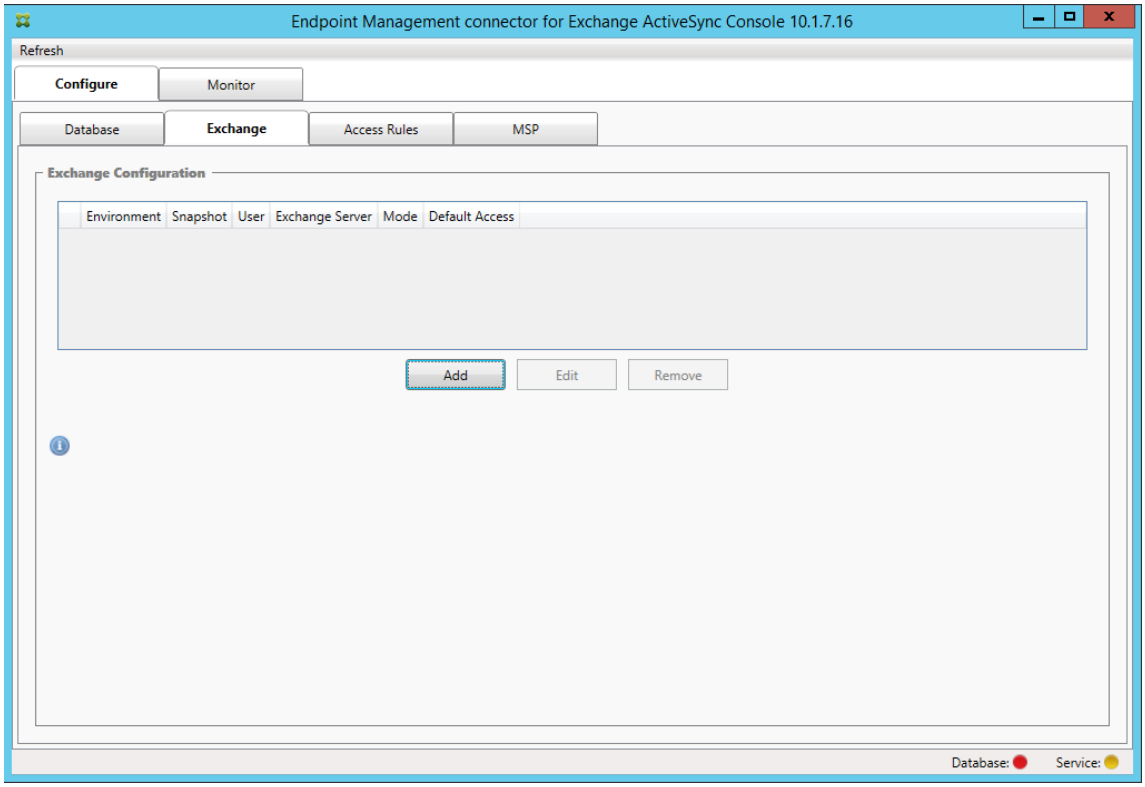
   Wenn “Windows Integrated”auch für die BlackBerry-Datenbankverbindung ausgewählt wird, muss dem hier angegebenen Windows-Konto Zugriff auf die BlackBerry-Datenbank erteilt werden.

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**.

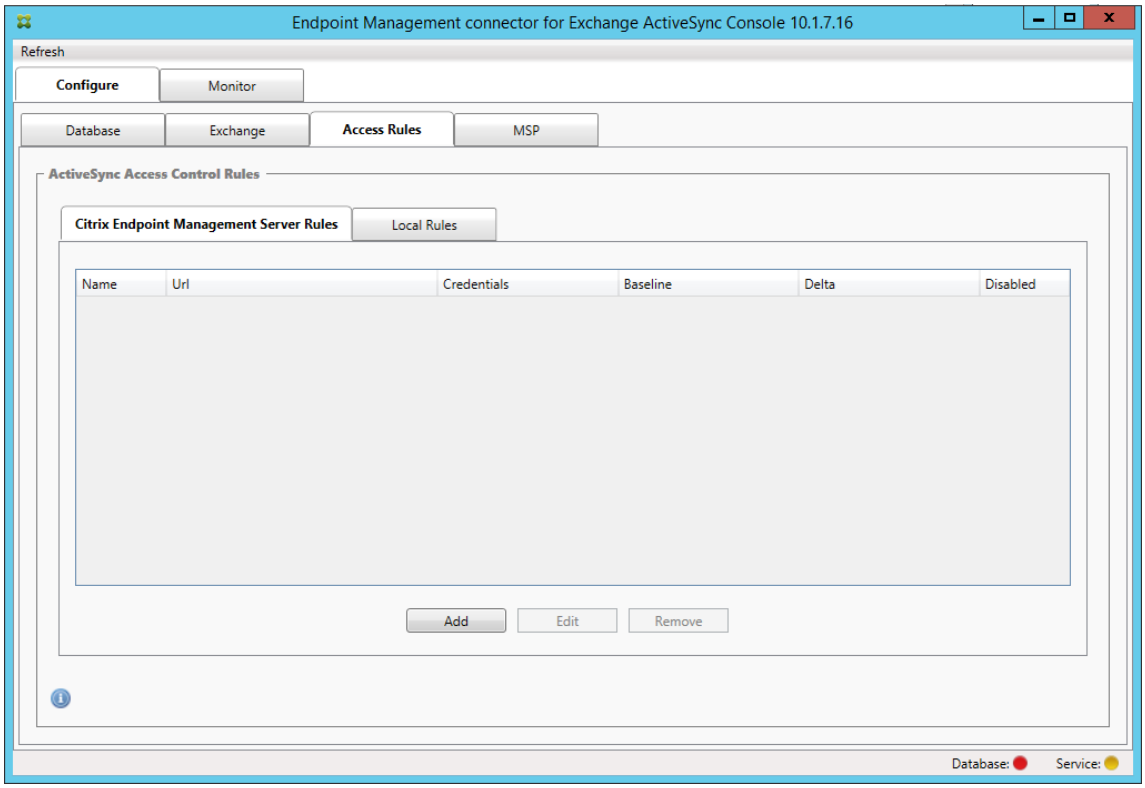


8. Wählen Sie den Typ der Exchange Server-Umgebung aus: **On Premise** oder **Office 365**.

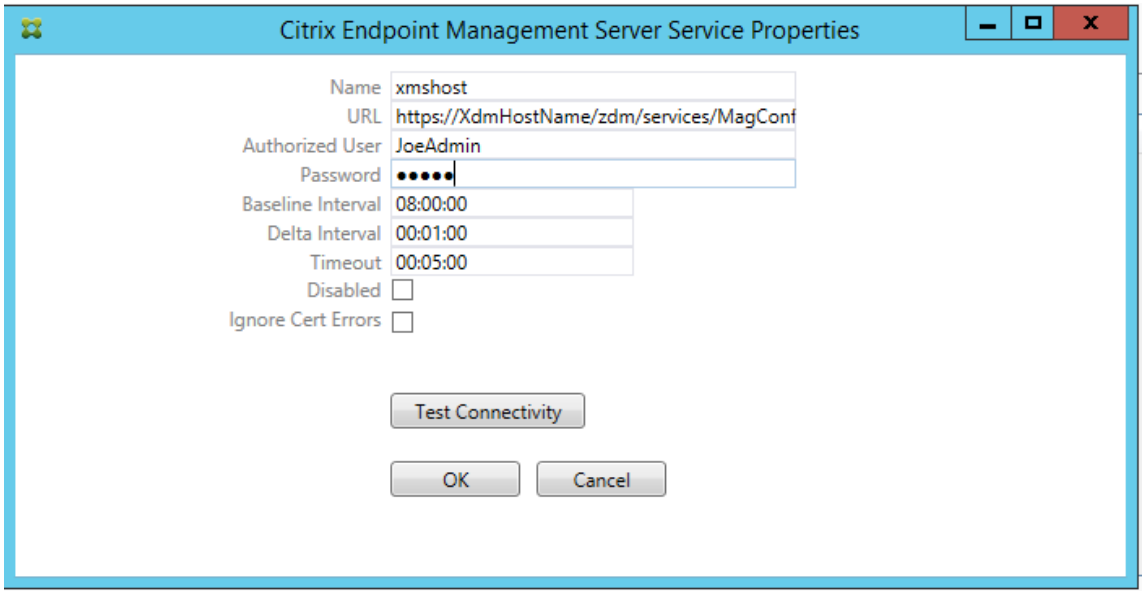
   - Wenn Sie **On Premise** auswählen, geben Sie den Namen des für Remote PowerShell-Befehle verwendeten Exchange Servers ein.
   - Geben Sie den **Benutzernamen** einer Windows-Identität ein, die die unter "Anforderungen"aufgeführten Berechtigungen auf dem Exchange Server-Computer hat, und geben Sie das 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 Connector für Exchange ActiveSync aus.
   - Wählen Sie den Standardzugriff aus: **Allow**, **Block** oder **Unchanged**. Durch die Einstellung wird gesteuert, wie Geräte behandelt werden, die keine der Kriterien von Citrix Endpoint Management-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 Connector für Exchange ActiveSync die PowerShell-Befehle für die gewünschte Zugriffssteuerung aus. Im Simulationsmodus werden vom 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 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 Connector für Exchange ActiveSync die gesamte Active Directory-Struktur in der Exchange-Umgebung anzeigt.
- Wählen Sie das Authentifizierungsprotokoll aus: **Kerberos** oder **Basic**. Der Connector für Exchange ActiveSync unterstützt die Standardauthentifizierung für On-Premises-Bereitstellungen. Dadurch kann der Connector auch dann verwendet werden, wenn der Connector-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 **Citrix Endpoint Management Rules** und dann auf **Add**.



10. Ändern Sie auf der Diensteigenschaftenseite für den **Citrix Endpoint Management-Server**die URL-Zeichenfolge so, dass sie auf den Citrix Endpoint Management-Server verweist. Wenn der Instanzname beispielsweise `zdm` lautet, geben Sie `https://<XdmHostName>/zdm/services/MagConfigService` ein. Ersetzen Sie `XdmHostName` im Beispiel durch die IP- oder DNS-Adresse des Citrix Endpoint Management-Servers.

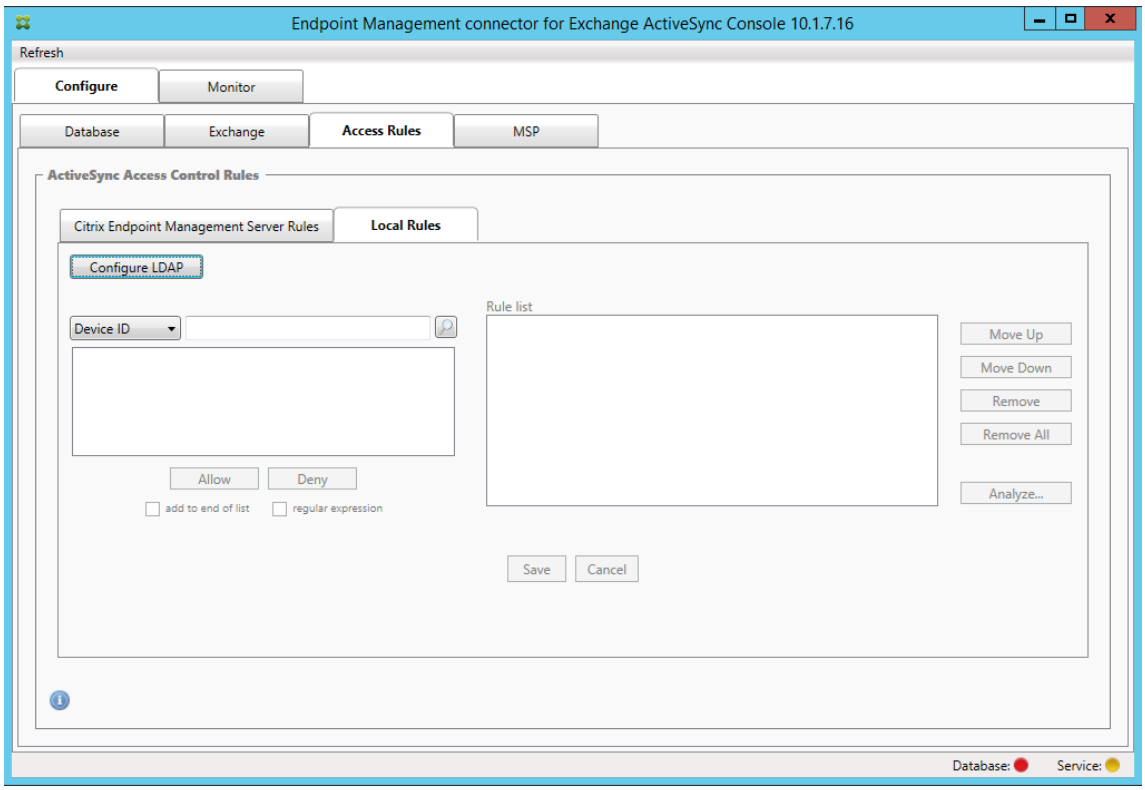


- Geben Sie einen berechtigten Serverbenutzer an.

- 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 Citrix Endpoint Management Mail-Dienst keine Richtlinien von Citrix Endpoint Management 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.

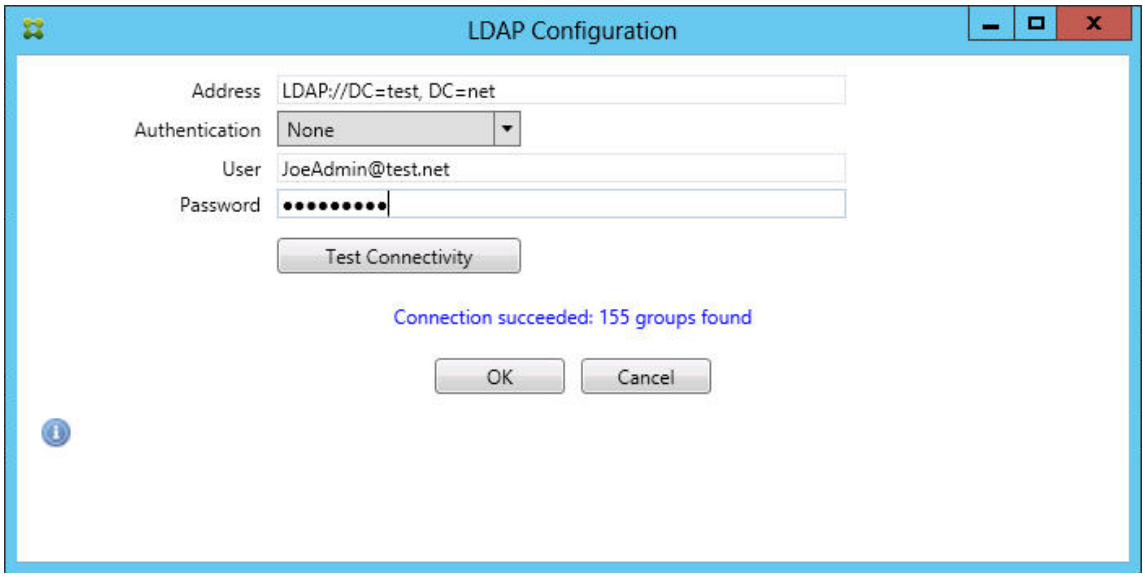
Bei allen Typen mit Ausnahme von Group verwendet das System die in einem Snapshot gefundenen Geräte. Wenn Sie gerade erst anfangen und noch keinen Snapshot erstellt haben, ist daher noch nichts verfügbar.

- 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

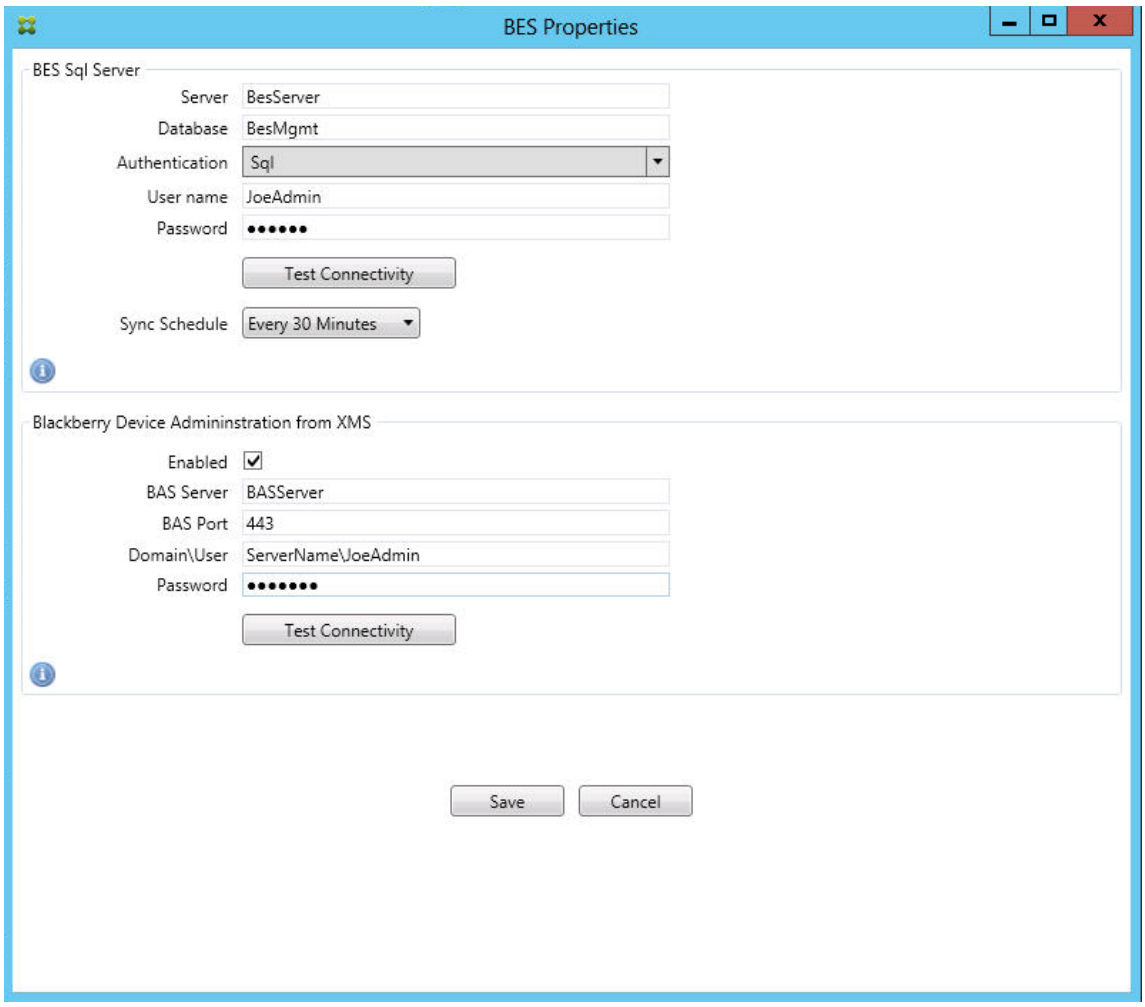
ist wichtig, weil die Regeln für jeden Benutzer bzw. jedes Gerät in der angegebenen Reihenfolge bewertet werden und eine Übereinstimmung bei einer höher stehenden Regel dazu führt, dass darunter stehende Regeln wirkungslos bleiben. Beispiel: Wenn Sie eine Regel zum Zulassen aller iPads und darunter eine 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 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



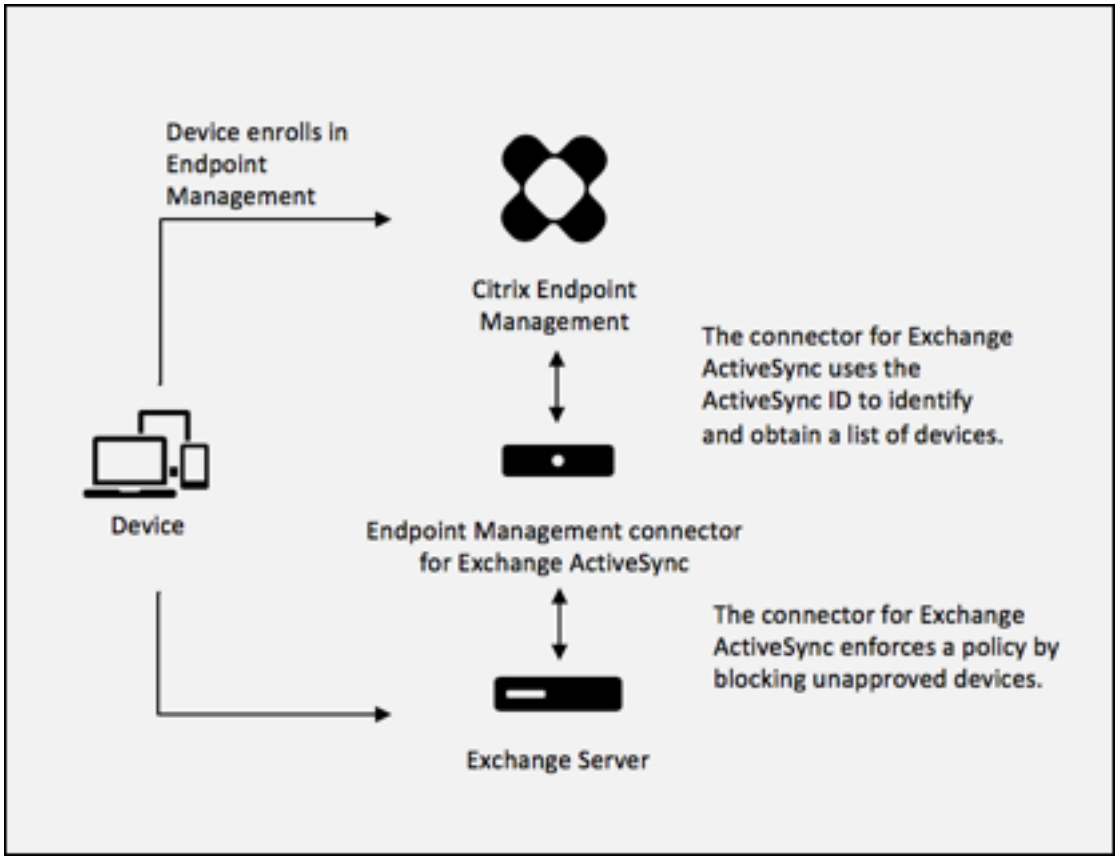
- Geben Sie den Namen der BES-Verwaltungsdatenbank ein.
- Wählen Sie unter **Authentication** den Authentifizierungsmodus aus. Bei Auswahl von "Windows Integrated"wird das Dienstbenutzerkonto des Connectors für Exchange ActiveSync für die Verbindung mit dem BES SQL-Server verwendet. Wenn "Windows Integrated"auch für die Connector-Datenbankverbindung ausgewählt wird, muss dem hier angegebenen Windows-Konto Zugriff auf die Connector-Datenbank erteilt werden.
- 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 Connector-Dienstkontos verwendet und die SQL-Authentifizierung daher nicht richtig getestet.

- Wenn Sie Remotelöschen und Zurücksetzen des Kennworts auf BlackBerry-Geräten von Citrix Endpoint Management 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, und klicken Sie dann auf **Save**.

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 Citrix Endpoint Management Connector für Exchange ActiveSync und Citrix Endpoint Management setzen eine solche E-Mail-Richtlinie zusammen durch. Citrix Endpoint Management legt die Richtlinien für den E-Mail-Zugriff in Unternehmen fest. Wenn ein nicht genehmigtes Gerät bei Citrix Endpoint Management registriert wird, erzwingt der 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. Citrix Secure Hub ruft eine ähnliche ID ab und sendet sie Citrix Endpoint Management, wenn das Gerät registriert wird. Durch den Vergleich der beiden Geräte-IDs kann der Connector für Exchange ActiveSync ermitteln, ob ein bestimmtes Gerät auf Unternehmens-E-Mail zugreifen darf. Das Konzept wird in folgender Abbildung dargestellt:



Wenn Citrix Endpoint Management dem Connector für Exchange ActiveSync eine ActiveSync-ID sendet, die sich von der von dem Gerät in Exchange veröffentlichten ID unterscheidet, kann der Connector Exchange 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 Android-Plattformen empfiehlt Citrix die Verwendung von Citrix Secure Mail.

Um sicherzustellen, dass die Unternehmensrichtlinie für den E-Mail-Zugriff ordnungsgemäß durchgesetzt wird, können Sie eine defensive Sicherheitsstrategie anwenden. Konfigurieren Sie den Citrix Endpoint Management Connector für Exchange ActiveSync so, dass E-Mails blockiert werden, indem Sie die statische Richtlinie standardmäßig auf **Verweigern** festlegen. Wenn ein Mitarbeiter dann einen anderen E-Mail-Client auf einem Android-Gerät konfiguriert und die ActiveSync-ID-Erkennung nicht funktioniert, wird dem Mitarbeiter der Zugriff auf Unternehmens-E-Mail verweigert.

Regeln für die Zugriffssteuerung

Der Citrix Endpoint Management Connector für Exchange ActiveSync bietet eine regelbasierte Methode zur dynamischen Konfiguration der Zugriffssteuerung für Exchange ActiveSync-Geräte. Connector-Zugriffsregeln bestehen aus zwei Teilen: einem Abgleichausdruck und dem gewünschten Zugriffszustand (Zulassen oder Blockieren). Eine Regel kann gegen ein Exchange ActiveSync-Gerät ausgewertet werden, um zu ermitteln, ob die Regel auf das Gerät zutrifft, d. h. ob der Abgleichausdruck auf das Gerät zutrifft. Es gibt mehrere Arten von Abgleichausdrücken, eine Regel kann beispielsweise auf alle Geräten eines bestimmten Typs, eine bestimmte Exchange ActiveSync-Geräte-ID, alle Geräte eines bestimmten Benutzers usw. zutreffen.

Beim Hinzufügen, Entfernen und Umordnen von Regeln in der Regelliste kann die Liste jederzeit mit einem Klick auf die Schaltfläche **Abbrechen** auf den Zustand zurückgesetzt werden, den sie beim ersten Öffnen hatte. Wenn Sie nicht auf **Speichern** klicken, gehen alle im Fenster gemachten Änderungen verloren, wenn Sie das Tool zum Konfigurieren schließen.

Der Citrix Endpoint Management Connector für Exchange ActiveSync bietet drei Regeltypen: lokale Regeln, Citrix Endpoint Management-Serverregeln (XDM-Regeln) und die Standardzugriffsregel.

Lokale Regeln: Diese haben die höchste Priorität, d. h. sobald eine lokale Regel auf ein Gerät zutrifft, wird die Regelauswertung eingestellt. Es werden weder die Citrix Endpoint Management-Serverregeln noch die Standardzugriffsregel konsultiert. Lokale Regeln werden in Bezug auf den 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.

Citrix Endpoint Management-Serverregeln: Diese Regeln sind Verweise auf einen externen Citrix Endpoint Management-Server, der Regeln zu verwalteten Geräten bereitstellt. Der Citrix Endpoint Management-Server kann mit eigenen allgemeinen Regeln konfiguriert werden, bei denen Geräte basierend auf in Citrix Endpoint Management bekannten Eigenschaften (z. B. Vorliegen von Jailbreak oder Vorhandensein verbotener Apps) zugelassen oder blockiert werden. Citrix Endpoint Management wertet die allgemeinen Regeln aus und generiert eine Liste zulässiger bzw. blockierter ActiveSync-Geräte-IDs, die dann an XenMobile Mail Manager gesendet werden.

Standardzugriffsregel: Die Besonderheit der Standardzugriffsregel besteht darin, dass sie the-

oretisch 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 Citrix Endpoint Management-Serverregel zu, wird der gewünschte Zugriffszustand durch die Standardzugriffsregel bestimmt.

- **Default Access –Allow:** Geräte, auf die weder eine lokale noch eine Citrix Endpoint Management-Serverregel zutrifft, werden alle zugelassen.
- **Default Access –Block:** Geräte, auf die weder eine lokale noch eine Citrix Endpoint Management-Serverregel zutrifft, werden alle blockiert.
- **Default Access –Unchanged:** Bei Geräten, auf die weder eine lokale noch eine Citrix Endpoint Management-Serveregel zutrifft, wird der Zugriffszustand vom Connector für Exchange ActiveSync nicht geändert. Wenn ein Gerät von Exchange in den Quarantänemodus versetzt wurde, erfolgt keine Aktion. Beispielsweise kann ein Gerät nur aus dem Quarantänemodus geholt werden, wenn es eine explizite lokale oder XDM-Regel gibt, die die Quarantäne außer Kraft setzt.

Regelauswertung

Für jedes Gerät, das Exchange dem 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
- Citrix Endpoint Management-Serverregeln
- Standardzugriffsregel

Sobald eine Regel zutrifft, wird die Auswertung beendet. Trifft beispielsweise eine lokale Regel auf ein Gerät zu, erfolgt für dieses keine Auswertung der Citrix Endpoint Management-Serverregeln oder der Standardzugriffsregel. Das gleiche Prinzip gilt für die Regeln desselben Regeltyps. Beispiel: Treffen mehrere lokale Regeln auf ein Gerät zu, wird die Auswertung beendet, wenn die erste Übereinstimmung gefunden wird.

Der 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 Connectors für Exchange ActiveSync funktionieren. In Exchange können Regeln dreierlei Ebenen konfiguriert werden: persönliche Ausnahmen, Geräteregeln und Organisationseinstellungen. Der 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 Connector für Exchange ActiveSync übernimmt bei seiner Bereitstellung die Verwaltung der Ausnahmelistenfunktion in Exchange. Weitere Informationen finden Sie im Microsoft-Artikel Device management with Exchange and Configuration Manager.

Eine Analyse ist nützlich, wenn mehrere Regeln für das gleiche Feld definiert wurden. Sie können die Beziehungen zwischen Regeln auf Konflikte untersuchen. Sie führen Analysen aus der Perspektive der Regelfelder durch. Regeln werden beispielsweise in Gruppen nach abgeglichenen Feld (ActiveSync Device ID, ActiveSync Device Type, User, User Agent) analysiert.

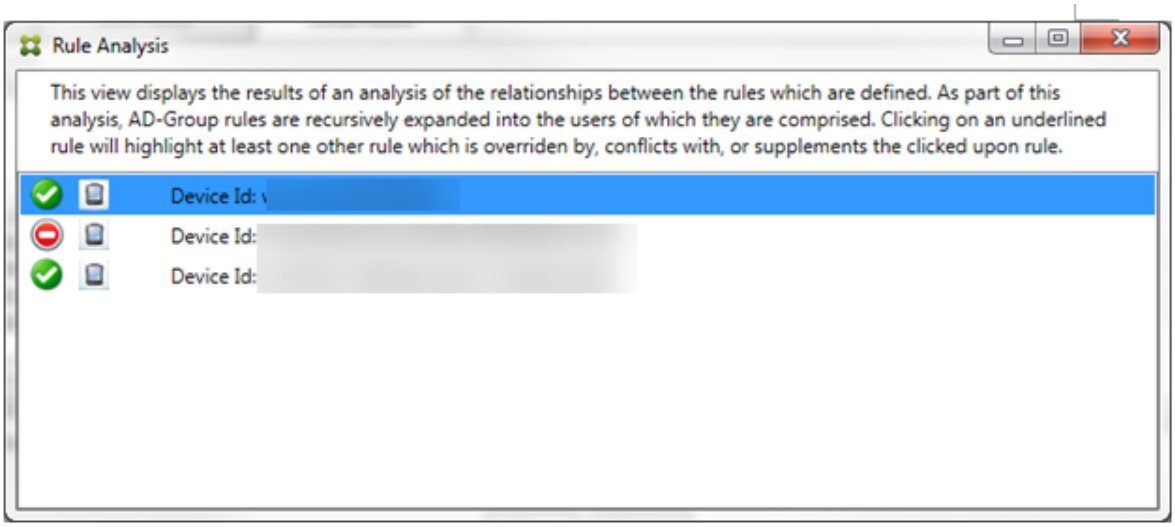
Terminologie der Regeln

- **Außerkraftsetzung:** Eine Außerkraftsetzung tritt auf, wenn mehrere Regeln auf ein Gerät zutreffen können. 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 können, 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 oder die Nebenregel verursacht einen Konflikt beim Zugriffszustand mit der primären Regel oder die Nebenregel ergänzt die primäre Regel.

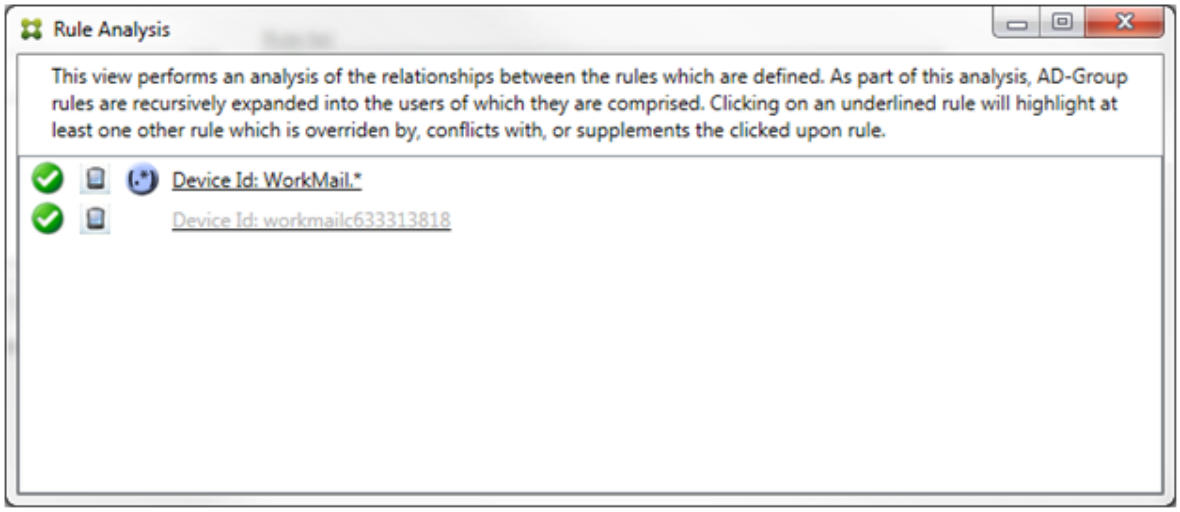
Darstellung des Regeltyps im Dialogfeld "Rule Analysis"

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.

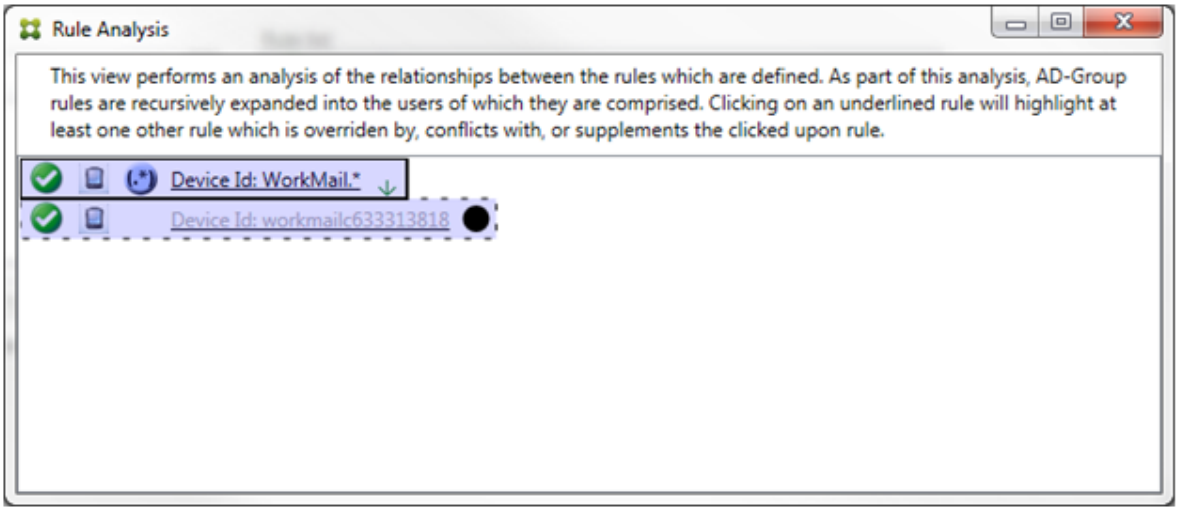
Im Fenster **Rule Analysis** ist ein Kontrollkästchen, bei dessen Aktivierung nur die Regeln angezeigt werden, die Konflikte, Überschreibungen, Redundanzen oder Ergänzungen sind.



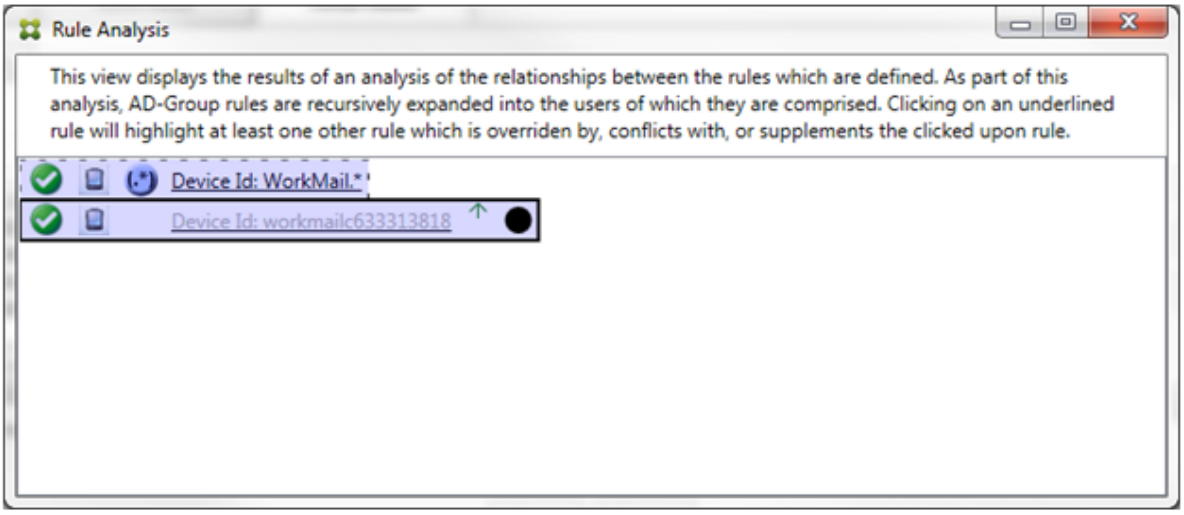
Wenn eine Außerkraftsetzung vorliegt, werden mindestens zwei Regeln unterstrichen dargestellt: die primäre Regel und die Nebenregel(n). Mindestens eine Nebenregel erscheint in einer helleren Schrift, um anzuzeigen, dass sie durch eine höhere Regel außer Kraft gesetzt wird. Sie können auf die außer Kraft 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:

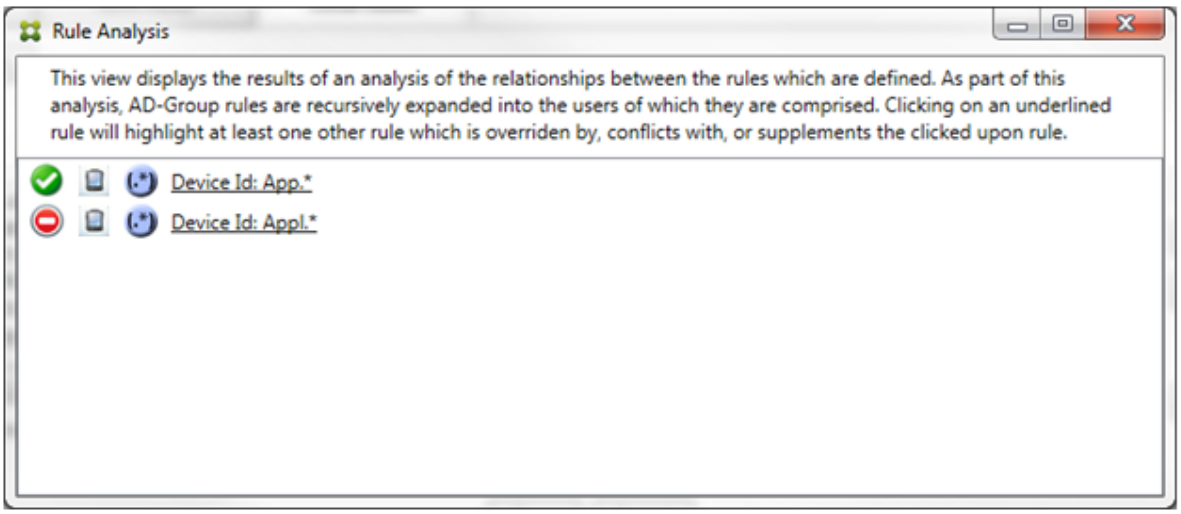


In diesem Beispiel ist die Regel mit regulären Ausdrücken `WorkMail.*` die primäre Regel (angezeigt durch den durchgehenden Rahmen) und die normale Regel `workmailc633313818` ist eine Nebenregel (angezeigt durch den gestrichelten Rahmen). Der schwarze Punkt neben der Nebenregel weist deutlich darauf 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:



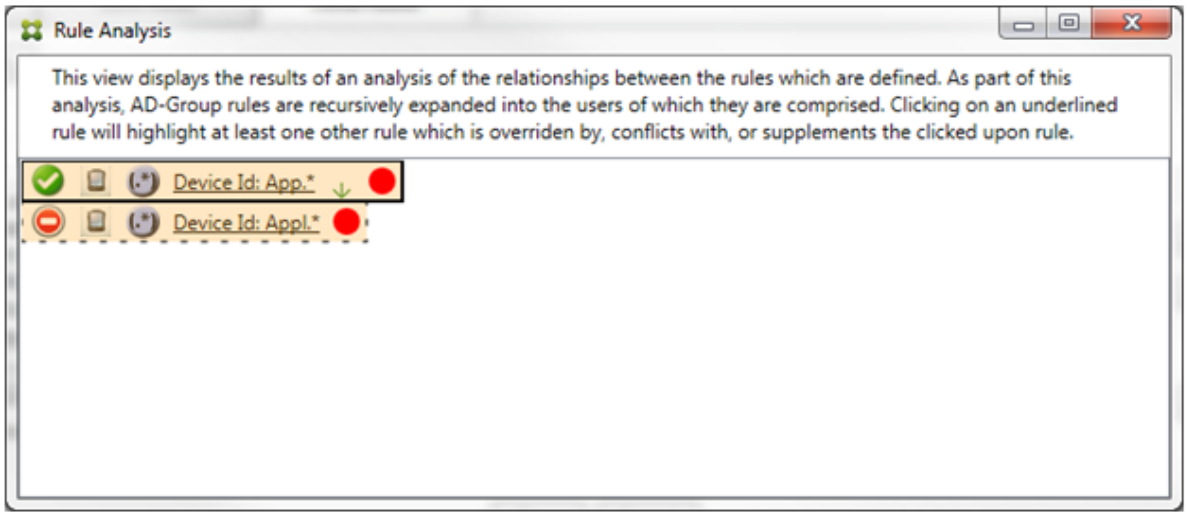
Im obigen Beispiel ist die Regel mit regulären Ausdrücken `WorkMail.*` die Nebenregel (angezeigt durch den gestrichelten Rahmen) und die normale Regel `workmailc633313818` ist eine primäre Regel (angezeigt durch den durchgehenden Rahmen). In diesem einfachen Beispiel ist der Unterschied nicht groß. Ein 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 gekennzeichnet. 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:



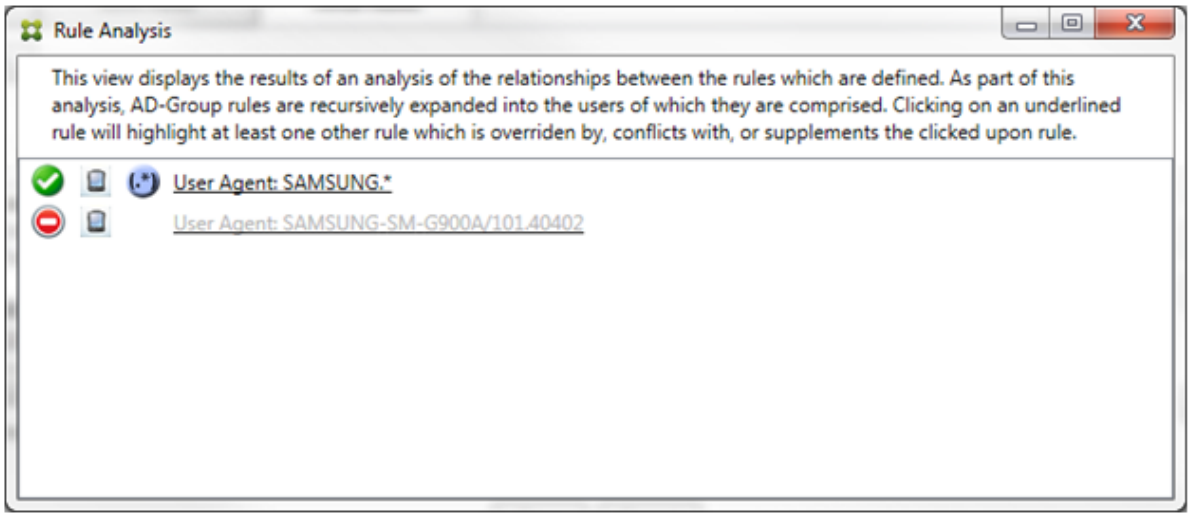
Eine Untersuchung der beiden Regeln mit regulären Ausdrücken ergibt, dass die erste Regel alle Geräte zulässt, deren ID “App”enthält, und die zweite Regel alle Geräte blockiert, deren ID `Appl`

enthält. Obwohl die zweite Regel alle Geräte blockiert, deren ID `Appl` enthält, 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:



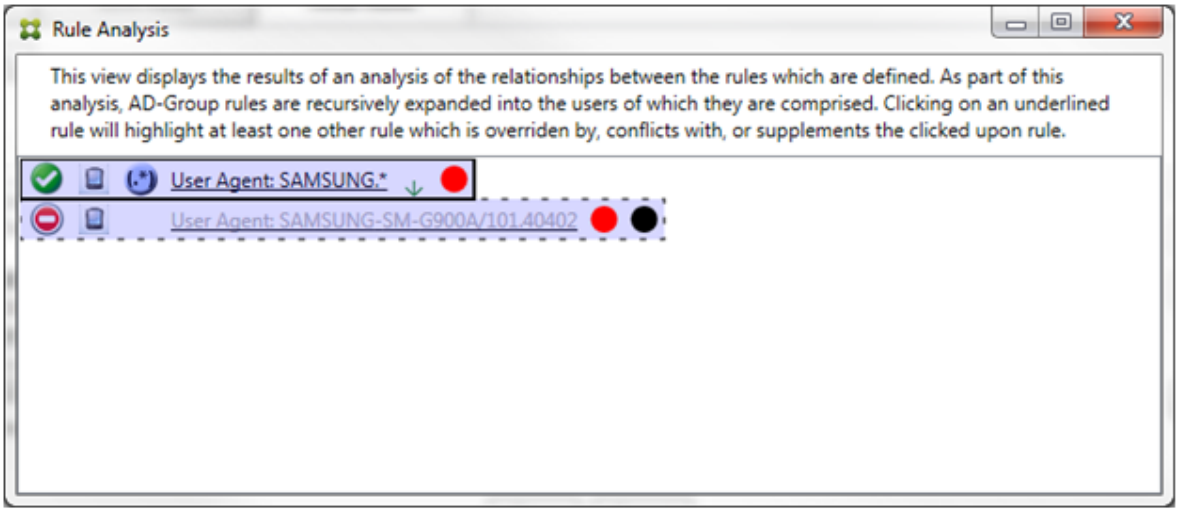
Im vorherigen Szenario wird sowohl die primäre Regel (mit dem regulären Ausdruck `App.*`) und die Nebenregel (mit dem regulären Ausdruck `Appl.*`) gelb markiert angezeigt. Dies ist ein einfacher optischer Warnhinweis auf den Umstand, dass mehrere Regeln mit regulärem Ausdruck für ein einzelnes Feld angewendet 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.



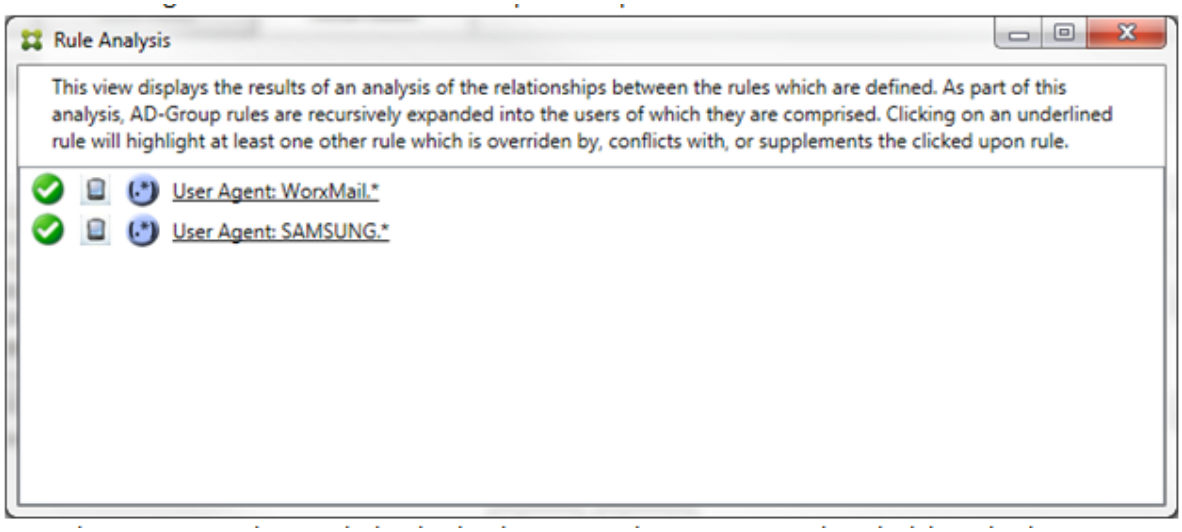
Im vorherigen Beispiel ist leicht zu erkennen, dass die erste Regel (mit dem regulären Ausdruck `SAMSUNG.*`) die nächste Regel (normale Regel `SAMSUNG-SM-G900A/101.40402`) außer Kraft setzt und überdies ein Konflikt beim Zugriffszustand (primäre Regel = Zulassen, Nebenregel = Blockieren) vorliegt. Die 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:

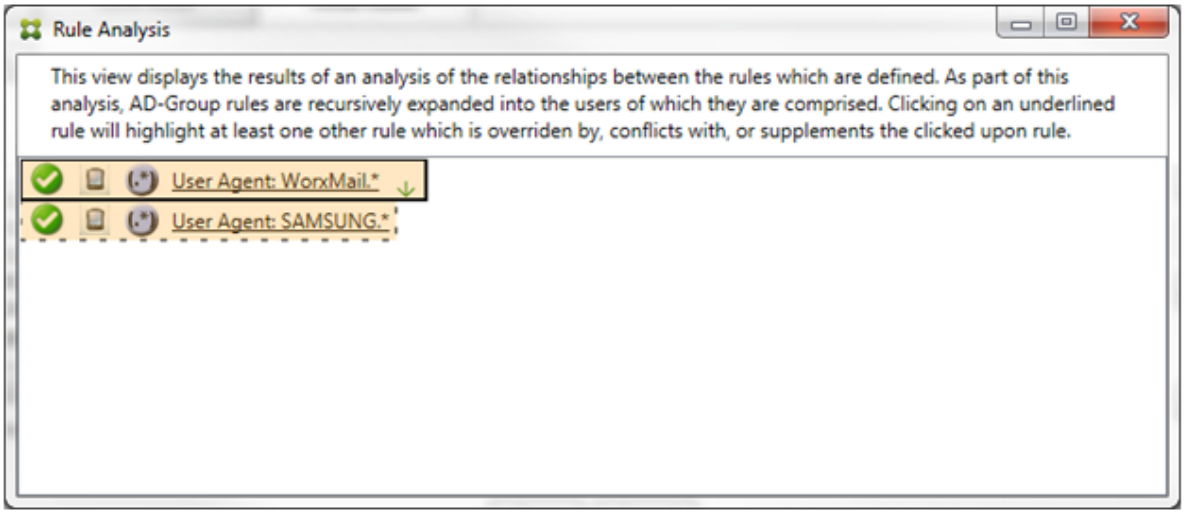


Die primäre Regel (mit dem regulären Ausdruck `SAMSUNG.*`) ist mit einem roten Punkt gekennzeichnet, um anzuzeigen, dass ihr Zugriffszustand im Widerspruch mit dem von mindestens einer Nebenregel steht. Die Nebenregel (normale Regel `SAMSUNG-SM-G900A/101.40402`) ist mit einem roten Punkt gekennzeichnet, 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 Citrix Endpoint Management Connector für Exchange ActiveSync angewendet werden. Nach dem Klicken auf die erste Regel sieht das Dialogfeld folgendermaßen aus:

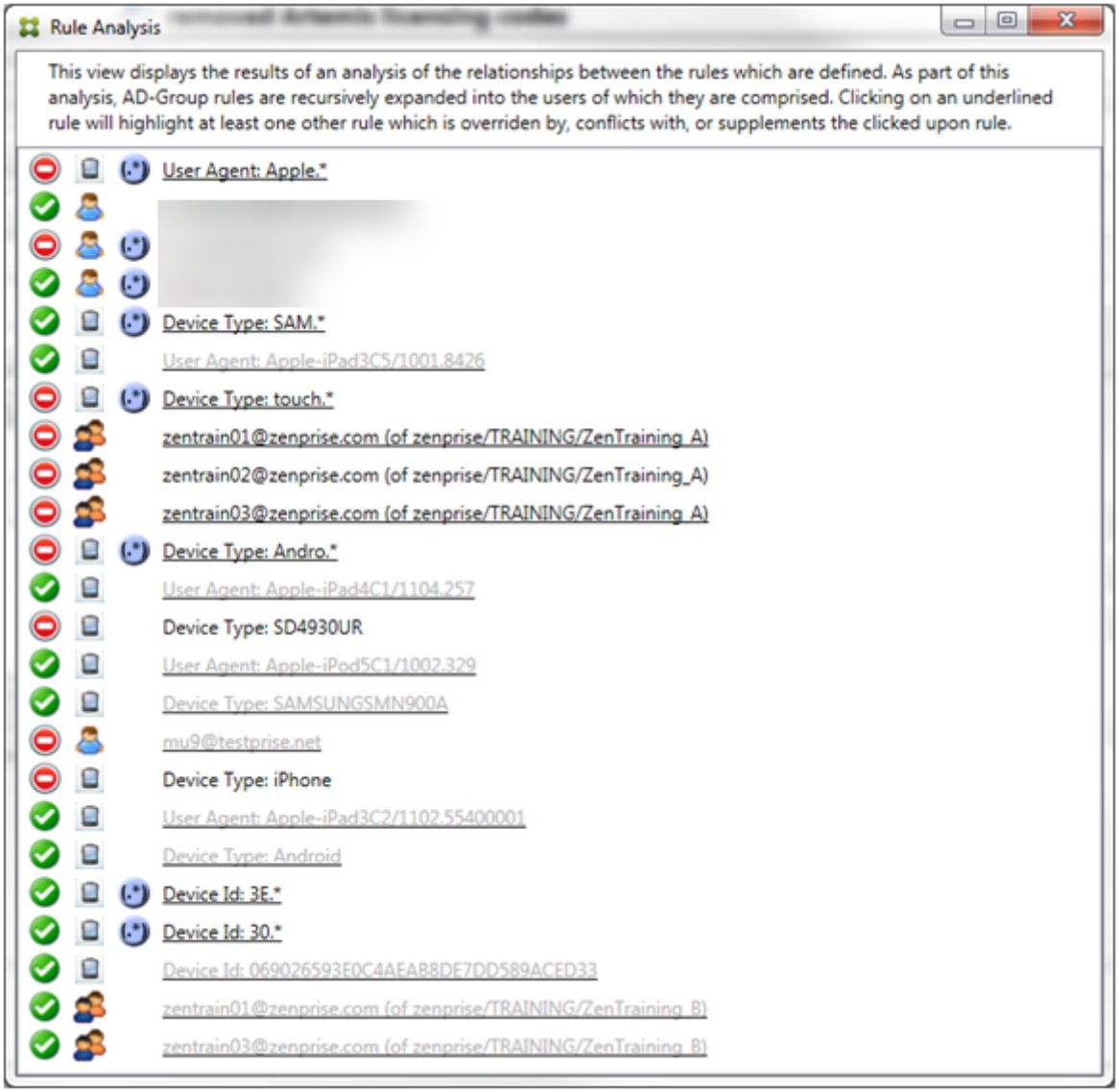


Die primäre Regel (mit dem regulären Ausdruck `WorkMail.*`) ist gelb hinterlegt, um anzuzeigen, dass es mindestens eine Nebenregel mit einem regulären Ausdruck gibt. Die Nebenregel (mit dem regulären Ausdruck `SAMSUNG.*`) ist gelb hinterlegt, um anzuzeigen, dass sie und die primäre Regel als Regel mit einem regulären Ausdruck auf dasselbe Feld im 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.

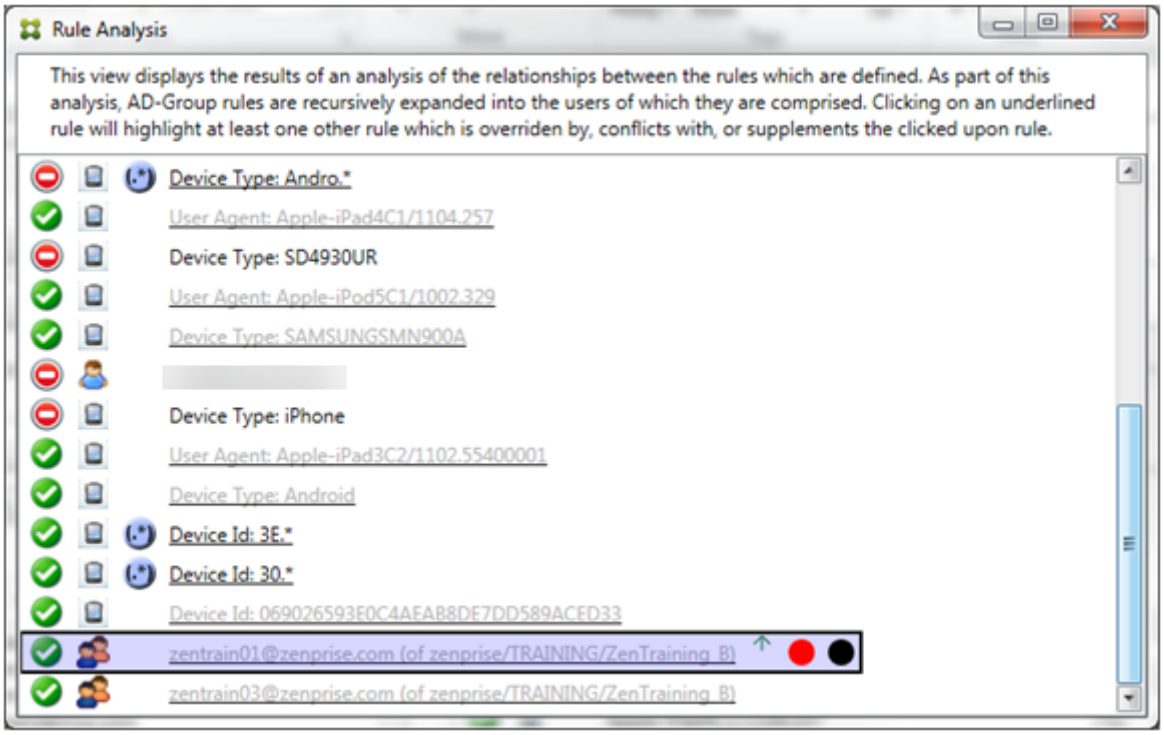
Die Liste enthält auch eine Reihe von Regeln mit regulären Ausdrücken, die durch das Symbol  gekennzeichnet sind.



Analysieren einer Außerkraftsetzung

Um zu sehen, welche Regeln eine bestimmte Regel außer Kraft setzen, klicken Sie auf die Regel.

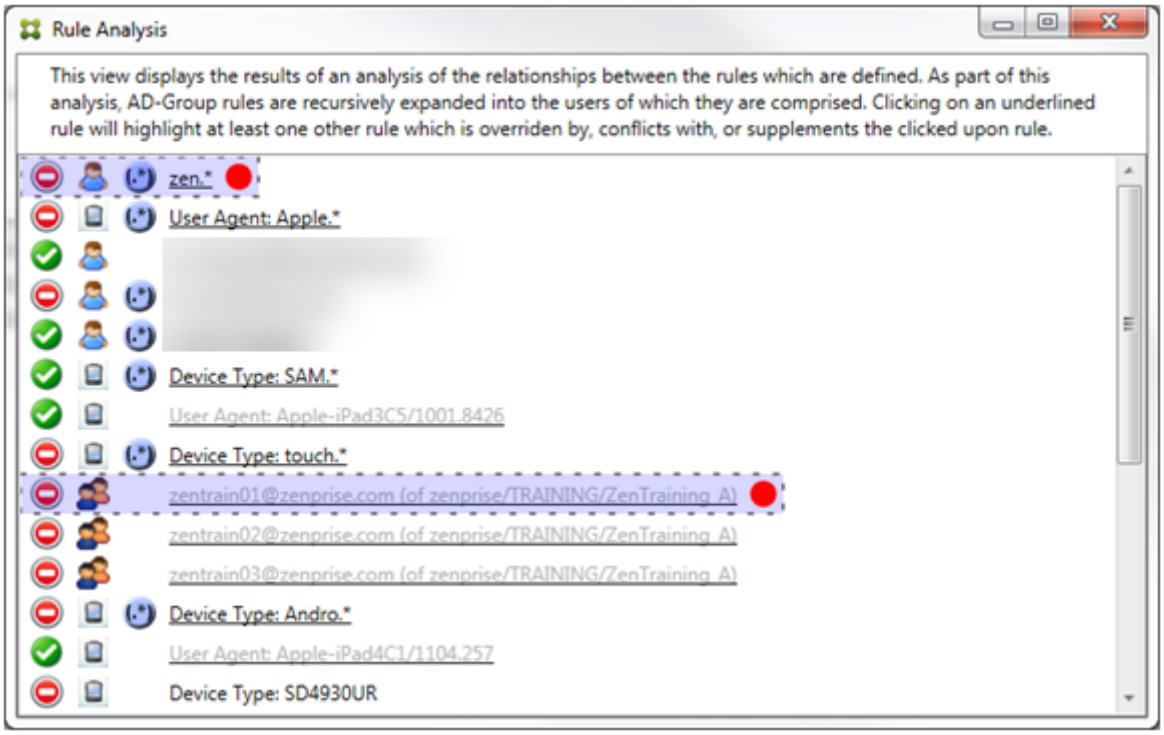
Beispiel 1: In diesem Beispiel wird untersucht, warum `zentrain01@zenprise.com` außer Kraft gesetzt wird.



Die primäre Regel (AD-Gruppenregel `zenprise/TRAINING/ZenTraining B`, bei der `zentrain01@zenprise.com` Mitglied ist) hat die folgenden Merkmale:

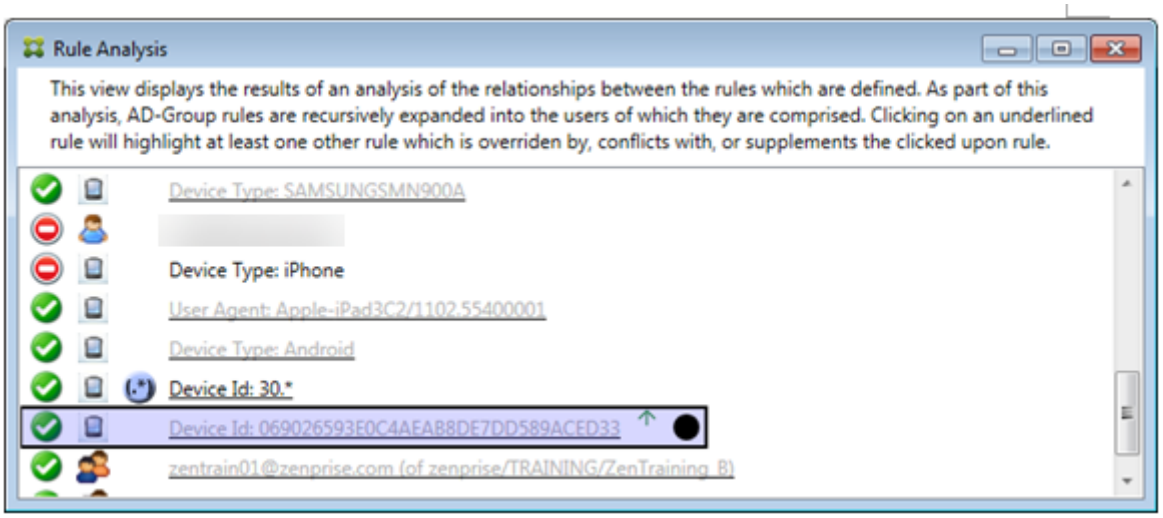
- Sie ist blau unterlegt und wird von einem durchgehenden Rahmen umgeben.
- Sie hat einen nach oben weisenden grünen Pfeil, was anzeigt, dass alle Nebenregeln weiter oben sind.
- Sie ist mit einem roten und einem schwarzen Punkt gekennzeichnet, um anzuzeigen, dass erstens mindestens eine Nebenregel einen 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:



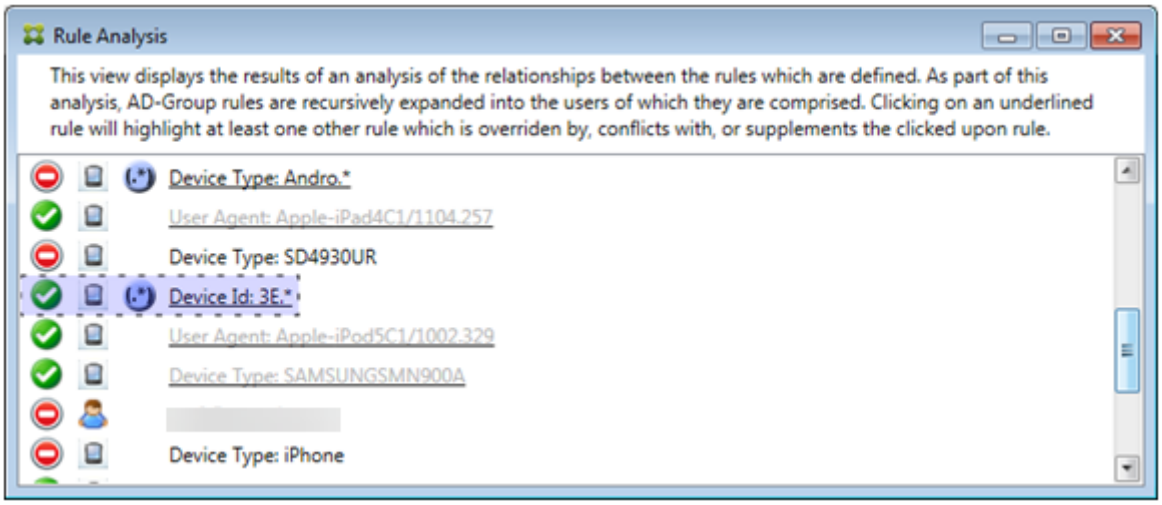
In diesem Fall gibt es zwei Nebenregeln, die die primäre Regel außer Kraft setzen: die Regel mit regulärem Ausdruck `zen.*` und die normale Regel `zentrain01@zenprise.com` (von `zenprise/TRAINING/ZenTraining A`). Bei der letzteren Nebenregel besteht das Problem darin, dass die Active Directory-Gruppenregel `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.

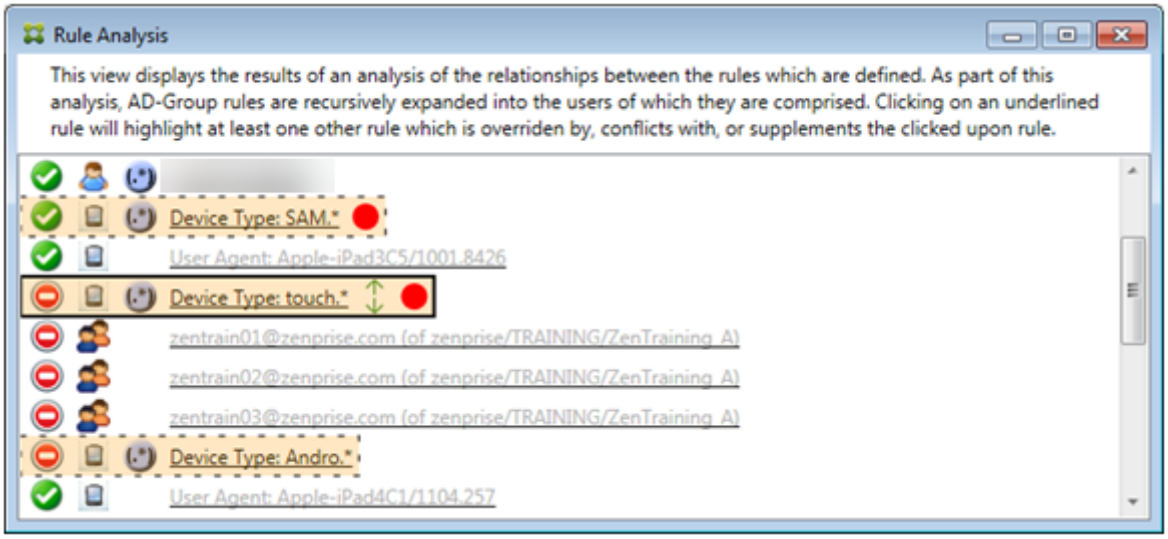


In diesem Fall wird die primäre Regel von einer einzigen Nebenregel außer Kraft gesetzt: der Regel mit der ActiveSync Geräte-ID und dem regulären Ausdruck `3E.*`. Da der reguläre Ausdruck `3E.*` auf `069026593E0C4AEAB8DE7DD589ACED33` zutrifft, würde die primäre Regel niemals ausgewertet.

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 Feld der ActiveSync-Gerätetypregel angewendet werden.
- In solchen Szenarien müssen Sie sicherstellen, dass ihre Regeln für reguläre Ausdrücke nicht überflüssig sind.



Weitere Analyse von Regeln

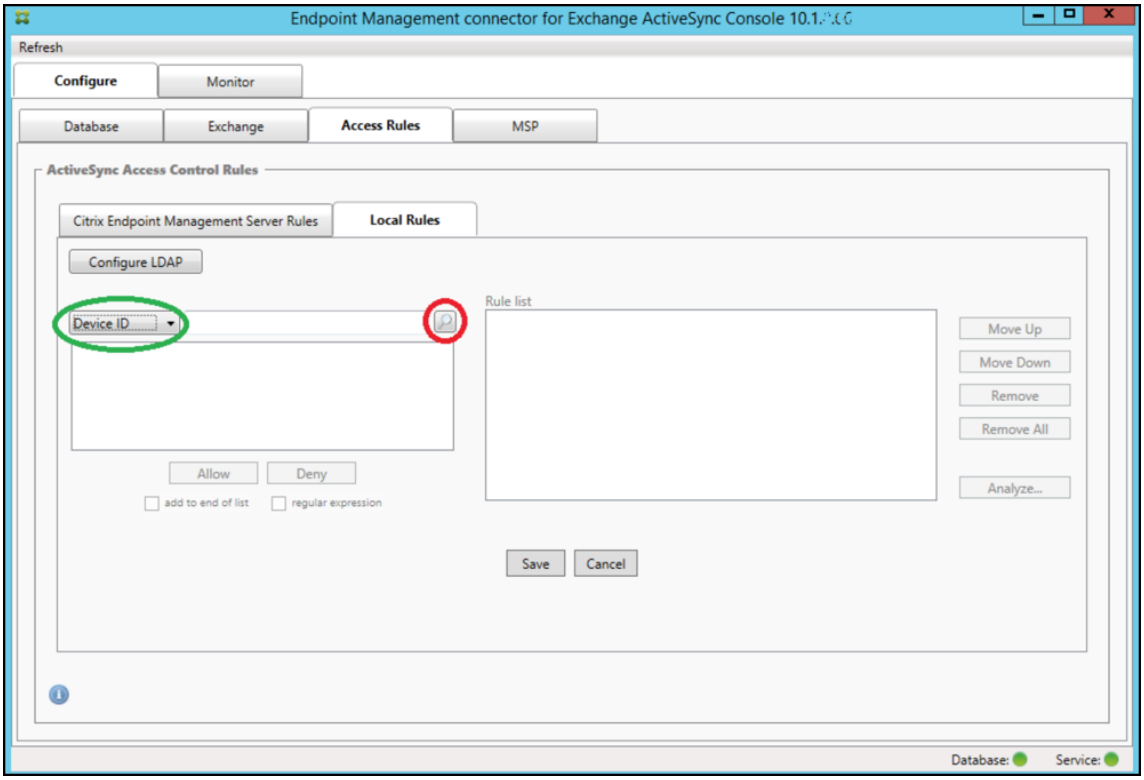
In diesem Beispiel wird demonstriert, dass Regelbeziehungen immer aus der Sicht der primären Regel dargestellt werden. Im vorherigen Beispiel wurde gezeigt, was ein Klick auf die Regel mit dem regulären Ausdruck für den Wert `touch.*` des Felds "device type"bewirkt. Wenn Sie auf die Nebenregel

`Andro.*` klicken, werden andere Nebenregeln hervorgehoben.

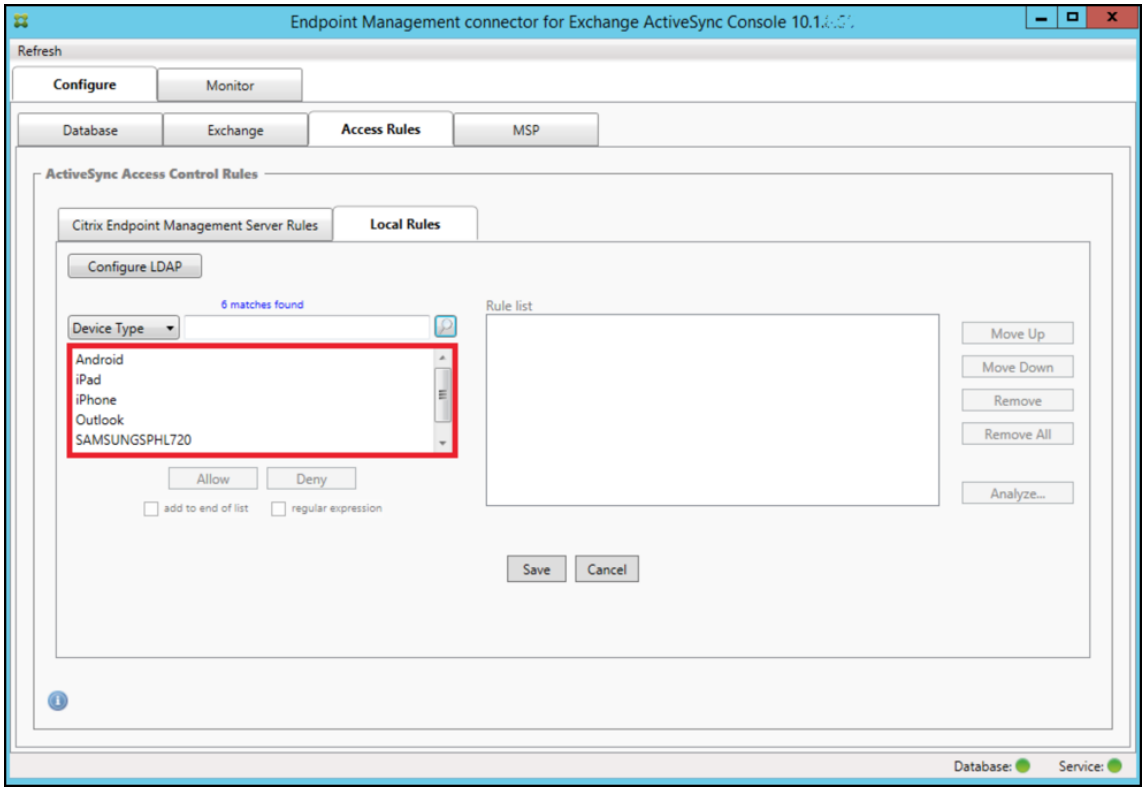
In diesem Beispiel wird eine außer Kraft gesetzte Regel, die Teil der Regelbeziehung ist, gezeigt. Diese Regel ist die normale ActiveSync-Gerätetypregel `Android`, die außer Kraft gesetzt ist (sichtbar an der helleren Schrift und dem schwarzen Punkt) und deren Zugriffszustand mit dem der primären ActiveSync-Gerätetypregel 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**.



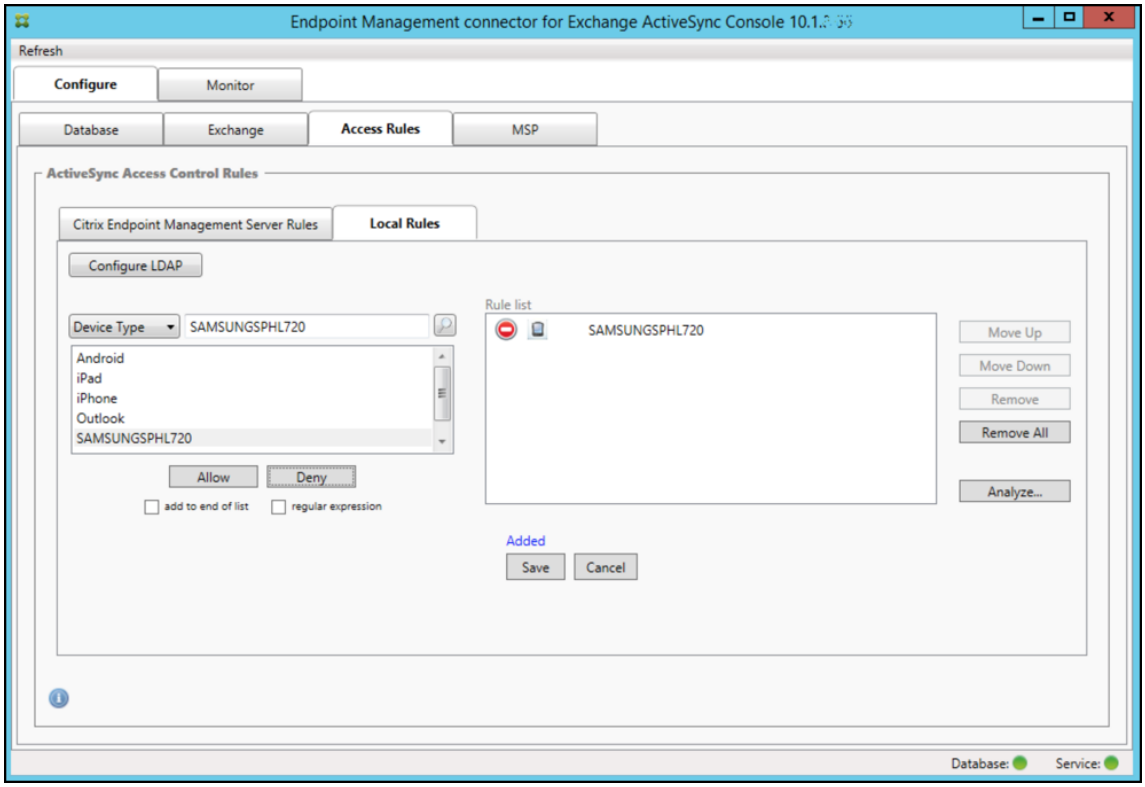
2. Wählen Sie in der Liste **Device ID** das Feld aus, für das Sie eine lokale Regel erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld **Gerätetyp** ausgewählt und die Auswahlmöglichkeiten 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.

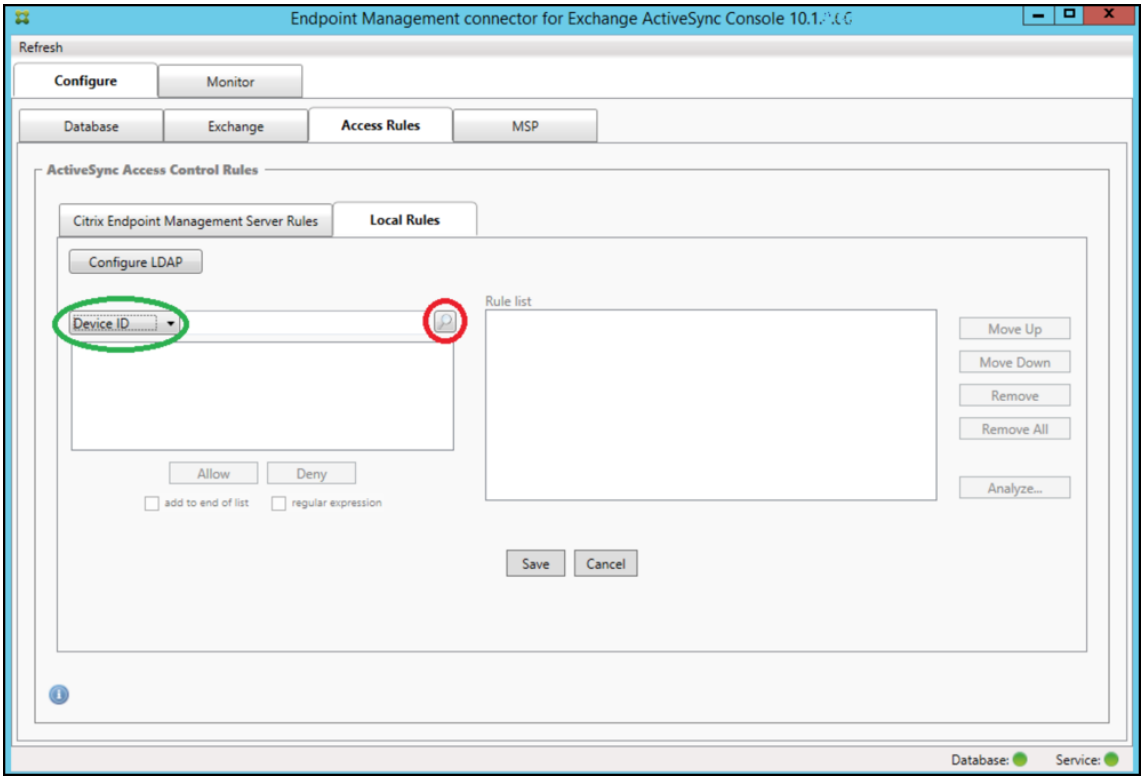


Hinzufügen eines regelmäßigen Ausdrucks

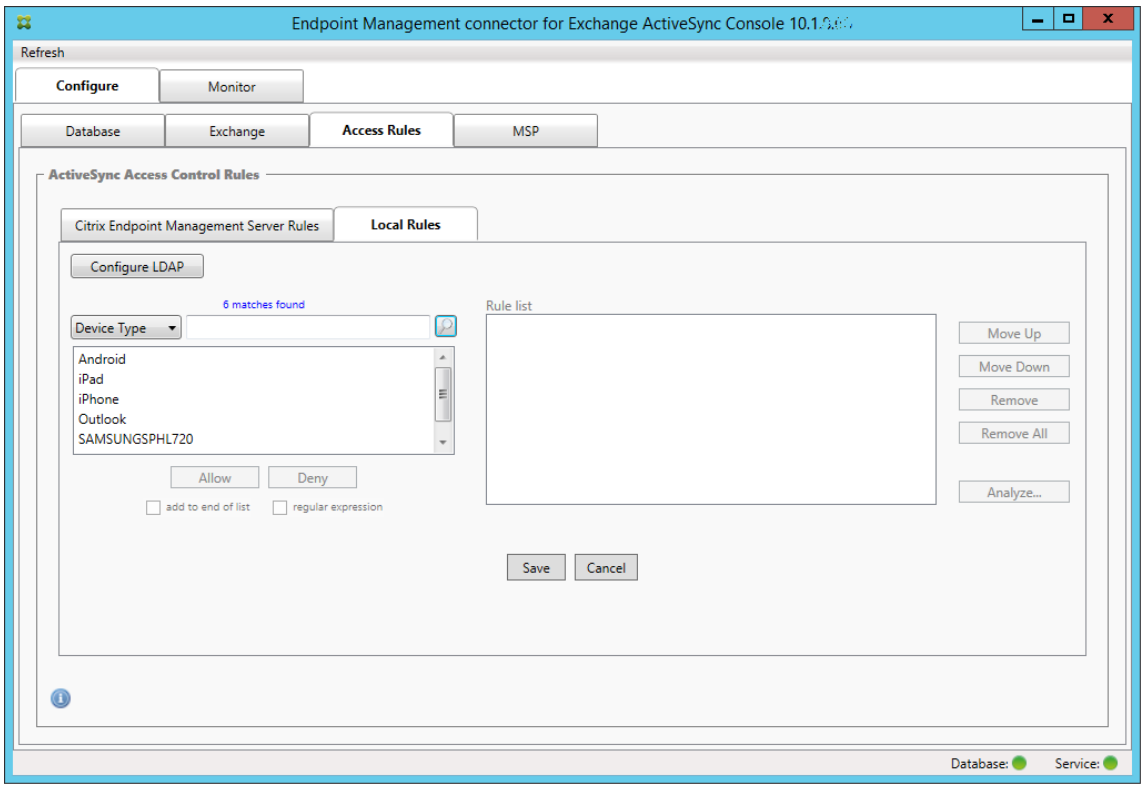
Lokale Regeln mit regulären Ausdrücken sind an dem Symbol  zu erkennen. Zum Hinzufügen einer Regel mit regulärem Ausdruck können Sie entweder einen Wert aus der Ergebnisliste für ein spezifisches Feld als Grundlage verwenden (sofern bereits ein größerer Snapshot durchgeführt wurde) oder den regulären Ausdruck selbst eingeben.

Erstellen eines regulären Ausdrucks aus einem vorhandenen Feldwert

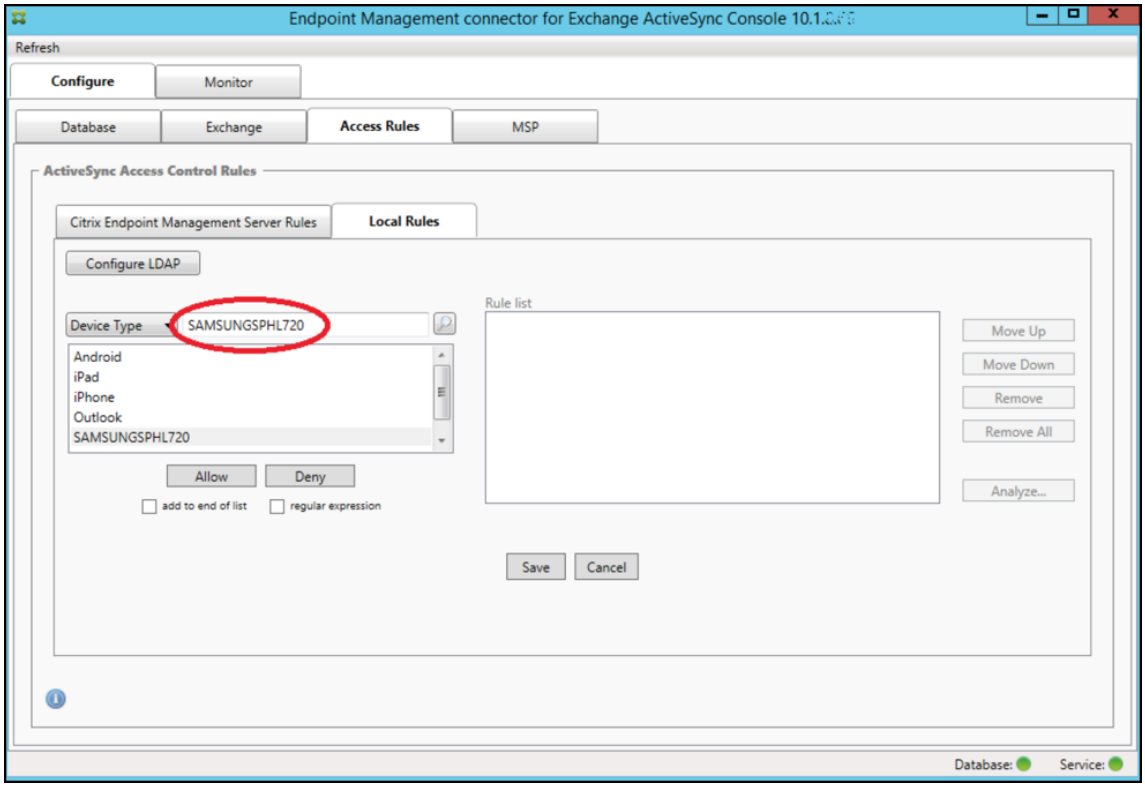
1. Klicken Sie auf die Registerkarte **Access Rules**.



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.



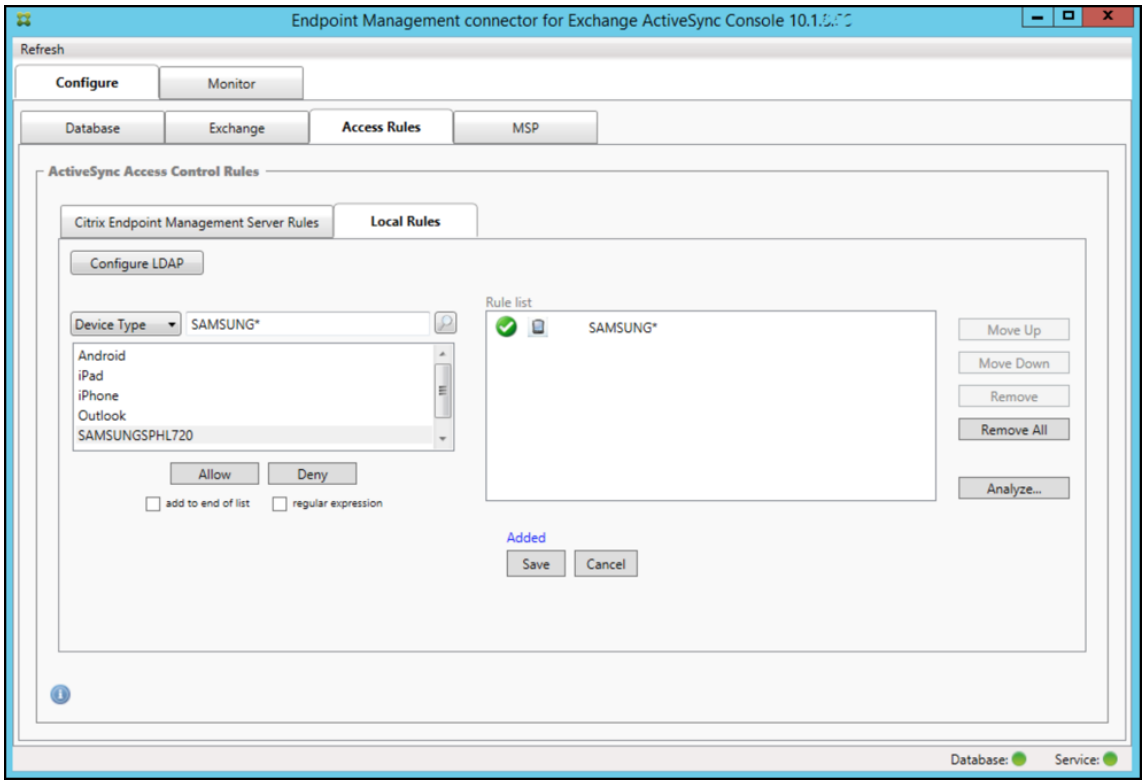
5. Um alle Gerätetypen zuzulassen, deren Gerätetypwert “Samsung”enthält, fügen Sie eine Regel mit regulärem Ausdruck hinzu, indem Sie die folgenden Schritte ausführen:

   a) Klicken Sie in das Textfeld des ausgewählten Elements.

   b) Ändern Sie den Text **SAMSUNGSPHL720** in **SAMSUNG.***.

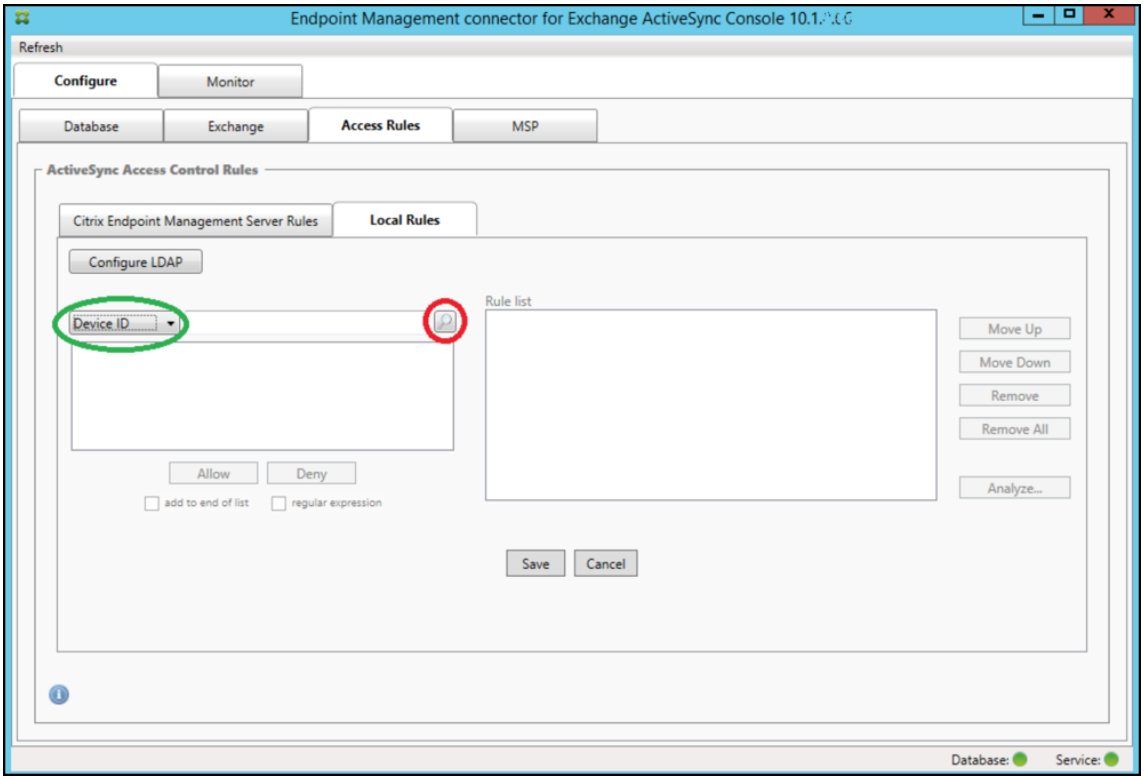
   c) Stellen Sie sicher, dass das Kontrollkästchen “regular expression”aktiviert ist.

   d) Klicken Sie auf **Zulassen**.

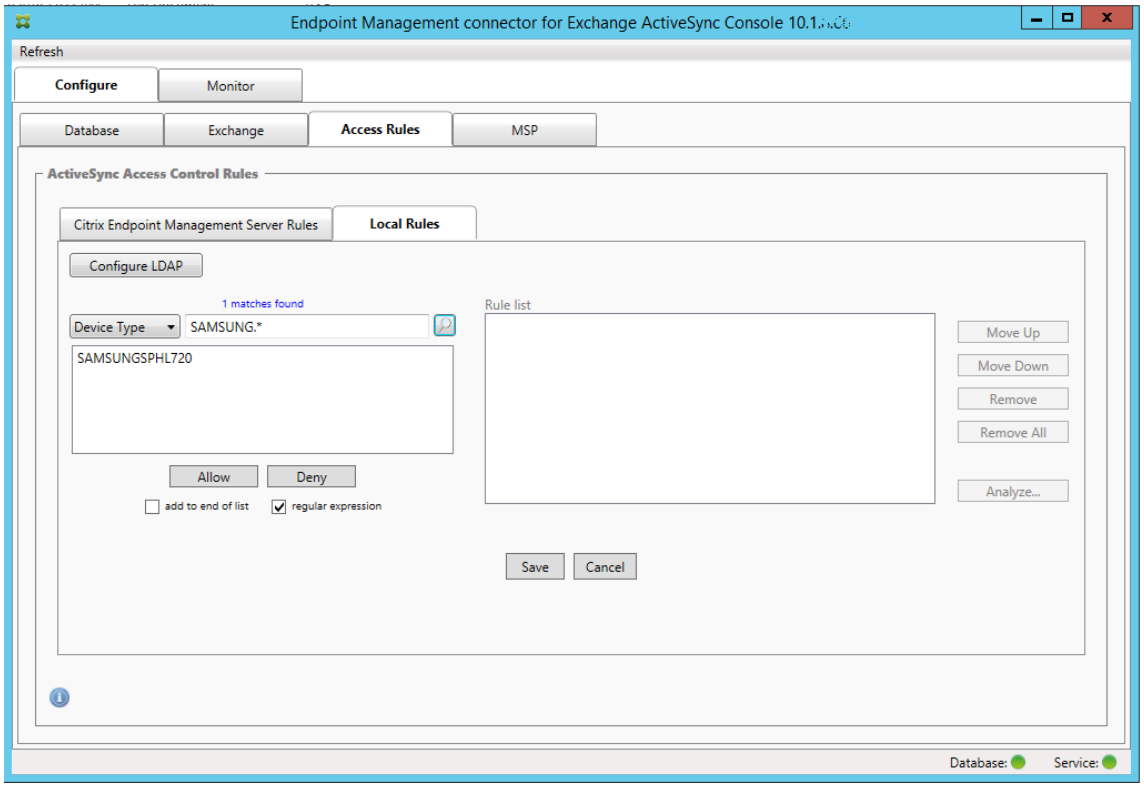


Erstellen einer Zugriffsregel

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.



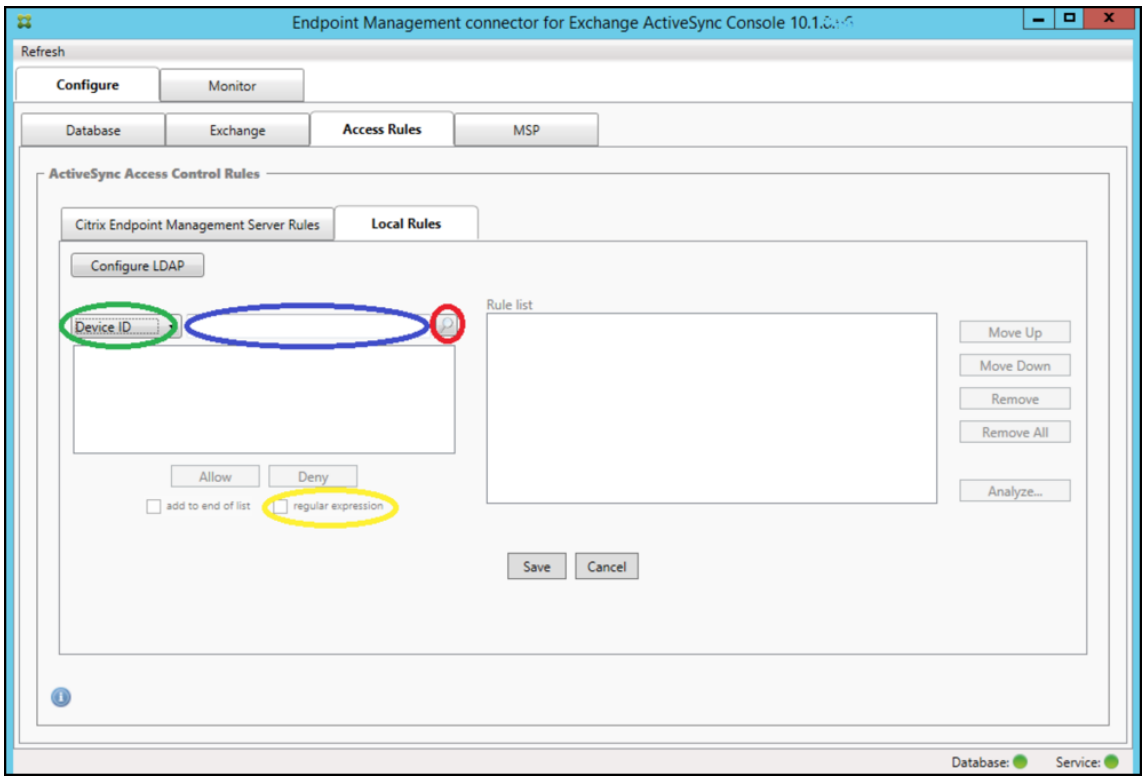
3. Wählen Sie das gewünschte Kriterienfeld aus. In diesem Beispiel ist dies **Device Type**.
4. Geben Sie den regulären Ausdruck ein. In diesem Beispiel ist dies `samsung.*`
5. Stellen Sie sicher, dass das Kontrollkästchen “regular expression”aktiviert ist, und klicken Sie auf **Allow** oder **Deny**. In diesem Beispiel ist die Auswahl **Allow**. Endergebnis:



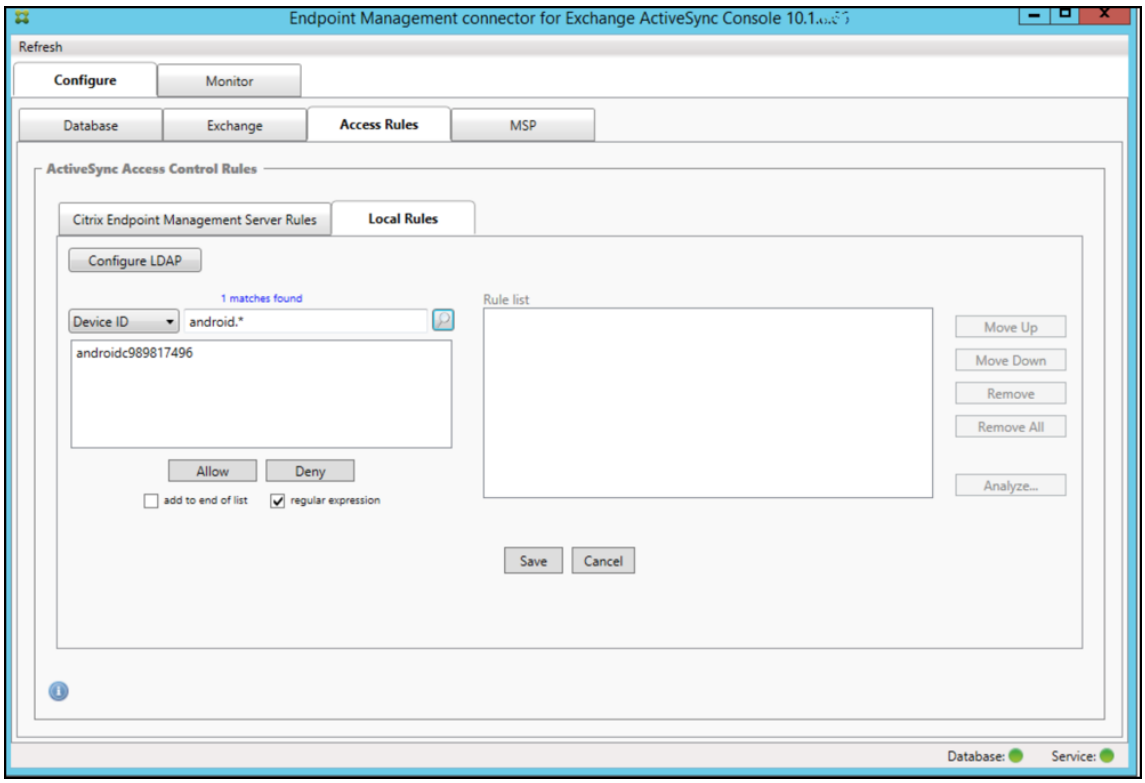
Suchen von Geräten

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).

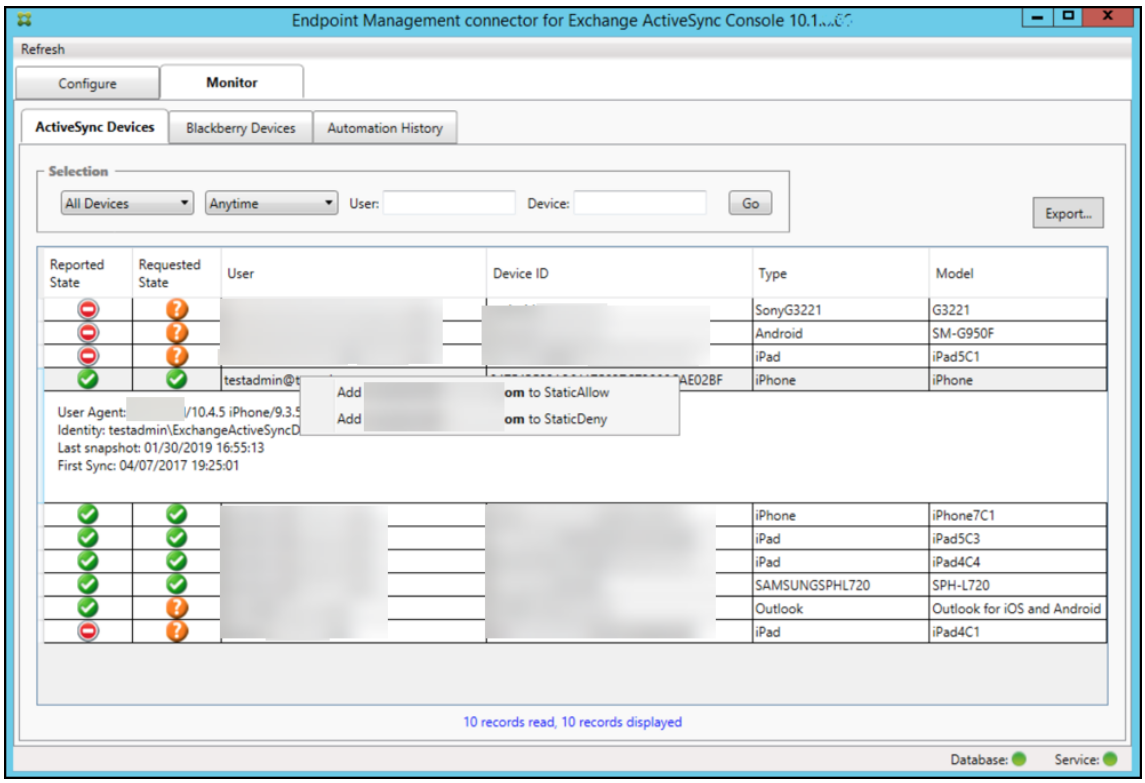


Hinzufügen eines einzelnen Benutzers, eines einzelnen Geräts oder eines einzelnen Gerätetyps zu einer statischen Regel

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 Citrix 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.

Problembehandlung und Diagnose

In folgender Protokolldatei des Citrix Endpoint Management-Connectors für Exchange ActiveSync werden Fehler und andere Betriebsinformationen aufgezeichnet: *Install Folder*\log\XmmWindowsService.log. Der Connector für Exchange ActiveSync protokolliert außerdem wichtige Ereignisse im Windows-Ereignisprotokoll.

Ändern der Protokollierungsstufe

Der Citrix 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:\Program Files\Citrix\Citrix` Citrix Endpoint Management Connector die Datei nlog.config.
2. Ändern Sie im Abschnitt `<rules>` den Parameter *minilevel* in die gewünschte Protokollierungsstufe. Beispiel:

```
    <rules >

    <logger name="*" writeTo="file" minlevel="Debug" />

    </rules>
<!--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 Connectors für Exchange ActiveSync wird nicht gestartet.

  Prüfen Sie die Protokolldatei und das Windows-Ereignisprotokoll auf Fehler. Typische Ursachen:

  - Der Dienst des Connectors für Exchange ActiveSync kann nicht auf den SQL Server zugreifen. Dafür kann Folgendes Ursache sein:
    * Der SQL Server-Dienst wird nicht ausgeführt.
    * Authentifizierungsfehler.

    Wenn die integrierte Windows-Authentifizierung konfiguriert ist, muss das Benutzerkonto des Connectors für Exchange ActiveSync als zulässige SQL-Anmeldung konfiguriert sein. Standardmäßig ist das Konto des Diensts des 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.

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.

NetScaler Gateway Connector für Exchange ActiveSync

June 25, 2024

XenMobile NetScaler Connector ist jetzt der NetScaler 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 NetScaler Gateway, der als Reverseproxy für das Exchange ActiveSync-Protokoll fungiert. Sie steuern die Autorisierung durch eine Kombination aus:

- Richtlinien, die Sie in Citrix Endpoint Management definieren
- Lokal vom NetScaler Gateway Connector für Exchange ActiveSync definierten Regeln

Weitere Informationen finden Sie unter ActiveSync-Gateway.

Ein detailliertes Architekturdiagramm finden Sie unter Architektur.

Die aktuelle Version des NetScaler Gateway Connector für Exchange ActiveSync ist Version 8.5.3.

Cloud Connector herunterladen:

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 **NetScaler Gateway Connector** auf **Download File**.

Informationen zur Installation des Connectors finden Sie unter NetScaler Gateway Connector für Exchange ActiveSync installieren.

> **Wichtig:**
>
> Ab Oktober 2022 bieten Citrix Endpoint Management Connector und NetScaler Gateway Connector für Exchange ActiveSync angesichts der von Microsoft hier angekündigten Authentifizierungsänderungen keine Unterstützung mehr für Exchange Online. Der Citrix Endpoint Management Connector für Exchange funktioniert weiterhin mit Microsoft Exchange Server (on-premises).

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]

Was ist neu in früheren Releases

> **Hinweis:**
>
> Im folgenden "Neue Features"-Abschnitt wird für den NetScaler Gateway Connector für Exchange ActiveSync der bisherige Name "XenMobile NetScaler Connector"verwendet. Der Name hat sich seit Version 8.5.2 geändert.

Neue Features in Version 8.5.2

- XenMobile NetScaler Connector ist jetzt der NetScaler Gateway Connector für Exchange ActiveSync.

Die folgenden Probleme wurden in dieser Version 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 nicht auch überprüft. [CXM-55355]

Neue Features in Version 8.5.1.11

- **Geänderte Systemanforderungen:** Die aktuelle Version von NetScaler Connector erfordert Microsoft .NET Framework 4.5.
- **Unterstützung von Google Analytics:** Wir möchten wissen, wie Sie den Connector verwenden, damit wir wissen, wo wir das Produkt verbessern können.
- **Unterstützung für TLS 1.1 und 1.2:** Aufgrund der schwächeren Sicherheit werden TLS 1.0 und TLS 1.1 vom PCI Council nicht mehr unterstützt. XenMobile NetScaler Connector unterstützt jetzt TLS 1.2.

NetScaler Gateway Connector für Exchange ActiveSync überwachen

Das Konfigurationsprogramm für den NetScaler Gateway Connector für Exchange ActiveSync bietet eine detaillierte Protokollierung. Mit diesen Protokollen können Sie den gesamten Datenverkehr über den Exchange Server anzeigen, der vom Secure Mobile Gateway zugelassen oder blockiert wird.

Auf der Registerkarte **Protokollierung** wird der Verlauf der von NetScaler Gateway zur Autorisierung an den Connector für Exchange ActiveSync weitergeleiteten ActiveSync-Anforderungen angezeigt.

Vergewissern Sie sich außerdem, dass der Connector für den Exchange ActiveSync-Webdienst 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 Connector für Exchange ActiveSync

Sie können den NetScaler 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 Connector für Exchange ActiveSync

NetScaler 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 sind für den Connector für Exchange ActiveSync in Citrix Endpoint Management verfügbar. Die Optionen für jeden Filter sind **Zulassen** oder **Verweigern**.

- **Anonyme Geräte:** dient zum Zulassen oder Blockieren von Geräten, die bei Citrix Endpoint Management registriert sind, bei denen die Identität des Benutzers jedoch unbekannt ist. Ein registrierter Benutzer hat beispielsweise eine unbekannte Identität, wenn er ein abgelaufenes Active Directory-Kennwort oder unbekannte Anmeldeinformationen hat.
- **Unzulässige Apps:** Zulassen oder Blockieren von Geräten basierend auf Sperrlisten in Richtlinien und vorhandenen Apps auf einer Sperrliste.
- **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 Connector für Exchange ActiveSync-Status für die Registerkarte "Geräte"aktiviert ist und den Connector-Status für die Geräte anzeigt. Die Option "Implizit zulassen/verweigern"steuert auch alle anderen Connector-Filter, die nicht ausgewählt wurden. Beispielsweise werden Apps auf der Sperrliste vom Connector blockiert. Alle übrigen Filter werden vom Connector 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 Citrix Endpoint Management 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 registriert, erhält er eine Liste der zu installierenden Apps. 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 erstellen und den Wert festlegen. Oder Sie können diese Eigenschaft mit automatisierten Aktionen auf einem Gerät erstellen, sofern das Gerät bestimmte Kriterien 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 Citrix Endpoint Management-Datenbank. Stellen Sie das Mobile Application Gateway im Modus "Blockieren"bereit.

Konfigurieren einer Verbindung zum NetScaler Gateway Connector für Exchange ActiveSync

Der NetScaler Gateway Connector für Exchange ActiveSync kommuniziert mit Citrix Endpoint Management und anderen Remotekonfigurationsanbietern über Citrix Secure Webdienste.

1. Klicken Sie im Connector für Exchange ActiveSync-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 Citrix Endpoint Management-Server verwendet wird.
3. Geben Sie unter **Url** die Webadresse des Citrix Endpoint Management-GCS (normalerweise im Format `https://<FQDN>/<instanceName>/services/<MagConfigService>`) ein. Beim Namen *MagConfigService* wird zwischen Groß- und Kleinschreibung unterschieden.
4. Geben Sie unter **Password** das Kennwort für die HTTP-Standardauthentifizierung beim Citrix Endpoint Management-Server an.
5. Geben Sie unter **Managing Host** den Namen des Servers mit dem Connector für Exchange ActiveSync ein.
6. Geben Sie unter **Baseline Interval** das Intervall ein, in dem von Citrix Endpoint Management 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 Connector für Exchange ActiveSync die Blockierung eines Geräts an Citrix Endpoint Management melden soll. Die Option ist erforderlich, wenn Sie die Connector-Regeln in Citrix Endpoint Management 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 Konfigurationsanbieter hinzufügen, erstellt der 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` definiert. 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 Citrix Endpoint Management

1. Klicken Sie im Connector für Exchange ActiveSync-Konfigurationsprogramm auf die Registerkarte **Config Providers** und dann auf **Add**.
2. Geben Sie im Dialogfeld **Config Providers** unter **Name** den Benutzernamen des Kontos ein, das für die HTTP-Standardauthentifizierung bei Citrix Endpoint Management verwendet wird. Der Benutzer muss über Administratorrechte verfügen.
3. Geben Sie unter **Url** die Webadresse des Citrix Endpoint Management Gateway Configuration Service (GCS) ein, normalerweise im Format `https://<xdmHost>/xdm/services/<MagConfigService>`. Beim Namen MagConfigService wird zwischen Groß- und Kleinschreibung unterschieden.
4. Geben Sie unter **Password** das Kennwort des Kontos mit Administratorrechten ein, das für die grundlegende HTTP-Autorisierung auf dem Citrix Endpoint Management-Server verwendet werden soll.
5. Klicken Sie auf **Test Connectivity**, um die Verbindung zwischen Gateway und Konfigurationsanbieter zu testen. Wenn die Verbindung fehlschlägt, überprüfen Sie, ob die lokalen Firewalleinstellungen die Verbindung gestatten, oder wenden Sie sich an den Administrator.
6. 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 Citrix Endpoint Manage-

ment 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 NetScaler Gateway-Connectors für Exchange ActiveSync

Der NetScaler Gateway Connector für Exchange ActiveSync kann in folgenden sechs Modi ausgeführt werden:

- **Allow All:** In diesem Richtlinienmodus erhält der gesamte Datenverkehr, der den Connector für Exchange ActiveSync passiert, Zugriff. Es werden keine anderen Filterregeln verwendet.
- **Deny All:** In diesem Richtlinienmodus wird der gesamte Datenverkehr, der den 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 für Exchange ActiveSync 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 für Exchange ActiveSync zugelassen.
- **Static + ZDM Rules**: Block Mode: In diesem Richtlinienmodus werden statische Regeln und anschließend dynamische Regeln aus Citrix Endpoint Management mit einer impliziten Blockieren-Anweisung am Ende ausgeführt. Geräte werden basierend auf Filtern und Citrix Endpoint Management-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 aus Citrix Endpoint Management mit einer impliziten Zulassen-Anweisung am Ende ausgeführt. Geräte werden basierend auf Filtern und Citrix Endpoint Management-Regeln zugelassen oder blockiert. Alle Geräte, die keinem Filter und keiner Regel entsprechen, werden zugelassen.

Das Ausführen dynamischer Regeln durch den Connector für Exchange ActiveSync-Prozess basiert auf eindeutigen ActiveSync-Kennungen von iOS- und Windows-Mobilgeräten, die von Citrix Endpoint Management empfangen werden. Bei Android-Geräten ist das Verhalten je nach Hersteller unterschiedlich, einige stellen ihre eindeutige ActiveSync-ID nicht einfach zur Verfügung. Ersatzweise sendet Citrix Endpoint Management 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 auf dem Connector für Exchange ActiveSync 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. Sie können die Werte aus den Protokollen abrufen. 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 Connector für Exchange ActiveSync den Datenverkehr basierend auf folgenden Kriterien zulassen oder blockieren:

- **User:** Der Connector für Exchange ActiveSync verwendet die bei der Geräteregistrierung erfasste Struktur aus autorisiertem Benutzerwert und Namen. Diese Struktur ist normalerweise `domain\username` gemäß Verweis von dem Citrix Endpoint Management-Server, der mit Active Directory über LDAP verbunden ist. Auf der Registerkarte **Log** des Connector-Konfigurationsprogramms werden die durch den Connector gesendeten Werte angezeigt. Die Werte werden übertragen, wenn der Connector die Wertstruktur bestimmen muss oder wenn sich die Struktur unterscheidet.
- **DeviceID (ActiveSyncID):** Wird auch als “ActiveSyncID”des verbundenen Geräts bezeichnet. Dieser Wert ist häufig auf der spezifischen Geräteeigenschaftenseite der Citrix Endpoint Management-Konsole. Er kann auch auf der Registerkarte **Log** im Konfigurationsprogramm des Connectors für Exchange ActiveSync ermittelt werden.
- **DeviceType:** Der Connector für Exchange ActiveSync 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 NetScaler Gateway-Connectors für Exchange ActiveSync alle verbundenen Gerätetypen, die für die ActiveSync-Verbindung verarbeitet werden, anzeigen.

- **UserAgent:** Enthält Informationen zu dem verwendeten ActiveSync-Client. In der Regel entspricht der Wert einem bestimmten Betriebssystem-Build-/Versionspaar für die Mobilgeräteplattform.

Das Connector für Exchange ActiveSync-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. Sie können auch 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 Citrix Endpoint Management definiert und können einen dynamischen Connector für Exchange ActiveSync-Filter auslösen. Die Filter werden bei einem Verstoß gegen eine Richtlinie oder Eigenschaft ausgelöst. 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 zum Blockieren. Es ist lediglich eine Liste der Geräte, die die Kriterien erfüllen. Über die folgenden Konfigurationsoptionen können Sie mithilfe des Connectors für Exchange ActiveSync festlegen, ob die Geräte in der Geräteliste zugelassen oder blockiert werden sollen.

> **Hinweis:**
>
> Verwenden Sie die Citrix Endpoint Management-Konsole, um dynamische Regeln zu konfigurieren.

1. Klicken Sie in der Citrix Endpoint Management-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 **Android-Domänenbenutzer an ActiveSync-Gateway senden** auf **Ja**, um sicherzustellen, dass Citrix Endpoint Management Android-Geräteinformationen an

das Secure Mobile Gateway sendet.

Wenn diese Option aktiviert ist, sendet Citrix Endpoint Management Android-Geräteinformationen an den Connector, wenn Citrix Endpoint Management keine ActiveSync-ID für den Gerätebenutzer hat.

Konfigurieren benutzerdefinierter Richtlinien mithilfe der XML-Datei des Connectors für Exchange ActiveSync Sie können die grundlegenden Richtlinien der Standardkonfiguration auf der Registerkarte **Richtlinien** des Konfigurationsprogramms des Connectors für Exchange ActiveSync anzeigen. Zum Erstellen benutzerdefinierter Richtlinien können Sie die XML-Konfigurationsdatei des NetScaler Gateway-Connectors für Exchange ActiveSync (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 Connectors für Exchange ActiveSync Die Aktionen des 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 NetScaler 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 auch 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 dieser Version werden nur externe XML-Dateien unterstützt.

In der Standardinstallation sind zwei XML-Dateien in der Konfiguration implementiert: allow.xml und deny.xml.

Konfigurieren des NetScaler Gateway-Connectors für Exchange ActiveSync

Sie können den NetScaler 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 Benutzeragent.

Dynamische Gruppen werden von einer externen Quelle, dem Gateway-Konfigurationsanbieter, gepflegt. Der Connector für Exchange ActiveSync verbindet die Gruppen regelmäßig. Citrix Endpoint Management kann Gruppen zugelassener und blockierter Geräte und Benutzer in den Connector für Exchange ActiveSync exportieren.

Dynamische Gruppen werden von einer externen Quelle, dem Gateway-Konfigurationsanbieter, gepflegt. Der Connector für Exchange ActiveSync erfasst dynamische Gruppen in regelmäßigen Abständen. Citrix Endpoint Management 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 NetScaler 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 Connectors für Exchange ActiveSync in Citrix Endpoint Management 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 NetScaler Gateway-Connectors für Exchange ActiveSync

Sie können unter Einsatz des NetScaler 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 Connectors für Exchange ActiveSync können Sie dynamische und statische Regeln zum Erzwingen von Unternehmensrichtlinien für E-Mail erstellen. Mit diesen Regeln und Richtlinien können Sie Benutzer blockieren, die die Richtlinien nicht einhalten. Sie können außerdem die Verschlüsselung von E-Mail-Anlagen einrichten, sodass alle Anlagen, die über Exchange Server an verwaltete Geräte gesendet werden, verschlüsselt werden. Verschlüsselte Anlagen können nur von autorisierten Benutzern auf verwalteten Geräten angezeigt werden.

Deinstallieren von XNC

1. Führen Sie XncInstaller.exe als Administrator aus.
2. Folgen Sie den Anweisungen zum Durchführen der Deinstallation.

Installieren, Aktualisieren oder Deinstallieren des Connectors für Exchange ActiveSync

1. Führen Sie XncInstaller.exe als Administrator aus, um den Connector für Exchange ActiveSync 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 für Exchange ActiveSync müssen Sie den Citrix Endpoint Management-Konfigurationsdienst und den Benachrichtigungsdienst manuell neu starten.

Installieren des NetScaler Gateway-Connectors für Exchange ActiveSync

Sie können den Connector für Exchange ActiveSync auf einem eigenen Server oder auf demselben Server wie Citrix Endpoint Management installieren.

Die Installation des Connectors für Exchange ActiveSync auf einem eigenen Server (getrennt von Citrix Endpoint Management) könnte sich aus folgenden Gründen anbieten:

- Der Citrix Endpoint Management-Server wird remote in einer Cloud gehostet (physischer Speicherort)
- Der Connector für Exchange ActiveSync soll nicht durch Neustarts des Citrix Endpoint Management-Servers beeinträchtigt werden (Verfügbarkeit)
- Sie möchten sämtliche Systemressourcen des Servers für den Connector für Exchange ActiveSync nutzen (Leistung).

Die CPU-Last, die der Connector für Exchange ActiveSync einem Server zuweist, hängt von der Anzahl der verwalteten Geräte ab. Grundsätzlich wird empfohlen, dass ein weiterer CPU-Kern bereitzustellen ist, wenn der Connector auf demselben Server wie Citrix Endpoint Management bereitgestellt wird. Bei hohen Gerätezahlen (über 50.000) müssen Sie möglicherweise weitere Kerne bereitstellen, wenn Sie keine Clusterumgebung nutzen. Der Speicherbedarf des Connectors ist so gering, dass kein zusätzlicher Speicher erforderlich ist.

Systemanforderungen für den NetScaler Gateway Connector für Exchange ActiveSync

Der NetScaler Gateway Connector für Exchange ActiveSync kommuniziert mit NetScaler Gateway über eine auf dem NetScaler Gateway-Gerät konfigurierte SSL-Brücke. Über diese Brücke kann das Gerät sämtlichen sicheren Datenverkehr direkt an Citrix Endpoint Management übergeben. Der Connector für Exchange ActiveSync 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 Gateway	Citrix Gateway-Gerät mit Softwareversion 10
Speicher	1 GB
Festplatte	NTFS-formatierte lokale Partition mit 150 MB freiem Speicherplatz
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 und die Unterstützung für Windows Server 2012 R2 endet am 10. Oktober 2023.
Sonstige Geräte	Mit dem Hostbetriebssystem kompatibler Netzwerkadapter für die Kommunikation mit dem internen Netzwerk

Komponente	Voraussetzung
Microsoft .NET Framework	Version 8.5.1.11 erfordert Microsoft .NET Framework 4.5.
Anzeige	VGA-Monitor oder höher

Auf dem Hostcomputer für den 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 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 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 NetScaler Gateway-Connectors für Exchange ActiveSync

Mit dem NetScaler Gateway Connector für Exchange ActiveSync können Sie NetScaler Gateway als Proxy und für den Lastausgleich bei der Kommunikation zwischen dem Citrix Endpoint Management-Server und mit Citrix Endpoint Management verwalteten Geräten verwenden. Der Connector für Exchange ActiveSync kommuniziert periodisch mit Citrix Endpoint Management, um Richtlinien zu synchronisieren. Sie können den Connector für Exchange ActiveSync und Citrix Endpoint Management zusammen oder separat in Clustern zusammenfassen.

Komponenten des Connectors für Exchange ActiveSync

- **Der Connector für Exchange ActiveSync-Dienst:** Dieser Dienst bietet eine REST-Webdienstschnittstelle, die von NetScaler Gateway aufgerufen werden kann, um zu ermitteln, ob eine ActiveSync-Anforderung von einem Gerät autorisiert ist.

- **Citrix Endpoint Management-Konfigurationsdienst:** Dieser Dienst kommuniziert mit Citrix Endpoint Management, um die Citrix Endpoint Management-Richtlinienänderungen mit dem Connector für Exchange ActiveSync zu synchronisieren.
- **Citrix Endpoint Management-Benachrichtigungsdienst:** Dieser Dienst sendet Benachrichtigungen über unautorisierten Gerätezugriff an Citrix Endpoint Management. Citrix Endpoint Management kann dann die nötigen Schritte ergreifen und beispielsweise den Benutzer benachrichtigen, warum sein Gerät blockiert wurde.
- **Connector für Exchange ActiveSync-Konfigurationshilfsprogramm:** Mit dieser Anwendung kann der Administrator den Connector für Exchange ActiveSync konfigurieren und überwachen.

Einrichten von Überwachungsadressen für den NetScaler Gateway Connector für Exchange ActiveSync

Führen Sie folgende Schritte aus, damit der NetScaler Gateway Connector für Exchange ActiveSync Anforderungen von NetScaler Gateway zur Autorisierung von ActiveSync-Datenverkehr empfangen kann. Geben Sie den Port an, den der Connector für Exchange ActiveSync auf Aufrufe des NetScaler Gateway-Webdiensts überwacht.

1. Wählen Sie im Menü **Start** das Konfigurationshilfsprogramm des 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. Wenn sich der Connector für Exchange ActiveSync auf dem gleichen Server wie Citrix Endpoint Management befindet, wählen Sie Ports aus, die keinen Konflikt mit denen von Citrix Endpoint Management 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 NetScaler Gateway Connector für Exchange ActiveSync

Zum Konfigurieren einer Zugriffssteuerungsrichtlinie für verwaltete Geräte gehen Sie folgendermaßen vor:

1. Klicken Sie im Konfigurationsprogramm des 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 Citrix Endpoint Management-Richtlinien umfassen, wählen Sie **Static + ZDM: Permit Mode oder Static + ZDM:**

Block Mode. Diese Richtlinien kombinieren lokale (statische) Regeln mit denen von Citrix Endpoint Management. 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 Citrix Endpoint Management

Geben Sie Namen und Eigenschaften des Citrix Endpoint Management-Servers an, den Sie mit dem NetScaler Gateway Connector für Exchange ActiveSync und NetScaler Gateway verwenden möchten.

> **Hinweis:**
>
> Es wird davon ausgegangen, dass Sie Citrix Endpoint Management bereits installiert und konfiguriert haben. Das Exchange ActiveSync-Konfigurationsprogramm verwendet den Begriff "Config Provider"für Citrix Endpoint Management.

1. Klicken Sie im Connector für Exchange ActiveSync-Konfigurationsprogramm auf die Registerkarte **Config Providers** und dann auf **Add**.
2. Geben Sie den Namen und die URL des Citrix Endpoint Management-Servers ein, den Sie in der Bereitstellung verwenden. Wenn Sie mehrere Citrix Endpoint Management-Server in einer Bereitstellung mit mehreren Mandanten haben, muss der Name für jede Serverinstanz eindeutig sein.
3. Geben Sie unter **Url** die Webadresse von Citrix Endpoint Management GlobalConfig Provider (normalerweise im Format `https://<FQDN>/<instanceName>/services/<MagConfigService>`) ein. Beim Namen *MagConfigService* wird zwischen Groß- und Kleinschreibung unterschieden.
4. Geben Sie unter **Password** das Kennwort für die HTTP-Standardauthentifizierung beim Citrix Endpoint Management-Server an.
5. Geben Sie unter **Managing Host** den Namen des Servers an, auf dem Sie den Connector für Exchange ActiveSync installiert haben.
6. Geben Sie unter **Baseline Interval** das Intervall ein, in dem von Citrix Endpoint Management 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 diese Option unter **Events Enabled**, wenn Secure Mobile Gateway die Blockierung eines Geräts an Citrix Endpoint Management melden soll. Die Option ist erforderlich, wenn Sie Secure Mobile Gateway-Regeln in Citrix Endpoint Management für eine automatische Aktion verwenden.

10. Klicken Sie nach Abschluss der Konfiguration des Servers auf **Test Connectivity**, um die Verbindung mit Citrix Endpoint Management zu testen.
11. Wenn die Verbindung hergestellt wird, klicken Sie auf **Save**.

Bereitstellen des NetScaler Gateway-Connectors für Exchange ActiveSync für Redundanz und Skalierbarkeit

Um Ihre Bereitstellung des NetScaler Gateway-Connectors für Exchange ActiveSync und von Citrix Endpoint Management zu skalieren, installieren Sie Instanzen des Connectors für Exchange ActiveSync auf mehreren Windows-Servern. Alle Connector-Instanzen verweisen auf dieselbe Citrix Endpoint Management-Instanz. Anschließend können Sie mit NetScaler Gateway einen Lastausgleich der Server durchführen.

Es gibt zwei Modi zur Konfiguration des Connectors für Exchange ActiveSync:

- Im Modus ohne Freigabe kommuniziert jede Instanz des Connectors für Exchange ActiveSync mit einem Citrix Endpoint Management-Server und speichert eine eigene Kopie der daraus resultierenden Richtlinie. Beispielsweise können Sie für einen Cluster von Citrix Endpoint Management-Servern eine Connector-Instanz auf jedem Citrix Endpoint Management-Server ausführen. Der Connector ruft dann Richtlinien von der lokalen Citrix Endpoint Management-Instanz ab.
- Im gemeinsamen Modus wird ein Connector für Exchange ActiveSync-Knoten als primärer Knoten bezeichnet. Der Connector kommuniziert mit Citrix Endpoint Management. Die resultierende Konfiguration wird dann per Windows-Netzwerkfreigabe oder per Windows-Replikation (bzw. per Drittanbieter-Replikation) an die anderen Knoten weitergegeben.

Die Connector Exchange ActiveSync-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. Die letzte funktionsfähige Konfiguration ist im Connector-Prozess zwischengespeichert.

Erweiterte Konzepte

March 11, 2024

Die Artikel zu erweiterten Konzepten bieten einen tieferen Einblick in Citrix Endpoint Management. 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 Citrix Endpoint Management finden Sie unter Citrix Endpoint Management bereitstellen.

Community-Supportforen zu Citrix Endpoint Management finden Sie unter Citrix Discussions.

Citrix Endpoint Management bereitstellen

March 11, 2024

Bei der Planung einer Citrix Endpoint Management-Bereitstellung sind zahlreiche Faktoren zu berücksichtigen. Welche Geräte möchten Sie verwenden? Wie sollen sie 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 Citrix Endpoint Management-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 Ihrer Anforderungen an erster Stelle. Welche Aufgaben soll Citrix Endpoint Management primär erfüllen? Müssen alle Geräte in der Umgebung oder nur die Apps oder beides verwaltet werden? Welches Sicherheitsniveau ist für die Citrix Endpoint Management-Umgebung erforderlich? Erörtern wir zunächst häufige Anwendungen und allgemeine Fragen, die bei der Planung der Bereitstellung zu berücksichtigen sind.

- Verwaltungsmodi
- Geräteanforderungen
- Sicherheit und Benutzererfahrung
- Apps
- Communities
- E-Mail-Strategie
- Integration von Citrix Endpoint Management

Design und Konfiguration

Nachdem Sie die Anforderungen an Ihre Bereitstellung analysiert haben, können Sie den Aufbau und die Konfiguration der Umgebung wählen. Elemente für die Planung:

- 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 NetScaler Gateway und Citrix ADC
- SSO- und Proxy-Überlegungen für MDX-Apps
- Authentifizierung
- Servereigenschaften
- Richtlinien für Geräte und Apps
- Optionen der Benutzerregistrierung

Betrieb und Überwachung

Nach der Inbetriebnahme der Citrix Endpoint Management-Umgebung gewährleistet eine effiziente Überwachung einen reibungslosen Betrieb. Im Abschnitt zur Überwachung wird erläutert, wo Sie die von Citrix Endpoint Management 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.

- Provisioning von Apps und Provisioning aufheben
- Über das Dashboard steuerbare Vorgänge
- Unterstützung für die rollenbasierte Zugriffssteuerung in Citrix Endpoint Management
- Überwachen und unterstützen
- Citrix Support-Prozess

Verwaltungsmodi

March 11, 2024

Der Begriff “Verwaltungsmodus”bezieht sich auf Mobile Device Management (MDM) und Mobile App Management (MAM). Sie können Folgendes konfigurieren:

- Registrierungsprofile zur Registrierung von Android- und iOS-Geräte bei MDM, MAM oder beidem (MDM+MAM). Wenn Sie MDM+MAM wählen, können Sie den Benutzern die Möglichkeit geben, MDM abzuwählen.
- Registrierungsprofile zum Registrieren von Windows 10- und Windows 11-Geräten bei MDM.

Sie geben Registrierungsoptionen in Registrierungsprofilen an, die Sie Bereitstellungsgruppen anfügen. Weitere Informationen über Registrierungsoptionen finden Sie unter Registrierungsprofile. In den folgenden Abschnitten geht es um Überlegungen zur Verwaltung von Geräten und Apps.

Mobilgeräteverwaltung (MDM)

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.

Auch wenn Sie sich gegen eine Verwaltung von Apps auf Geräten entscheiden, können Sie Apps bereitstellen, z. B. aus einem öffentlichen App-Store oder Unternehmensapps.

MDM empfiehlt sich generell für folgende Szenarien:

- MDM ist eine Überlegung für unternehmenseigene Geräte, bei denen Verwaltungsrichtlinien auf Geräteebene oder bestimmte Einschränkungen erforderlich sind. Zu solchen Einschränkungen gehören vollständiges oder selektives Löschen und Geolocation.
- Wenn Kunden die Verwaltung eines Geräts, jedoch keine MDX-Richtlinien benötigen.
- 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)

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 Citrix Endpoint Management für MAM konfiguriert ist, können Sie MDX-aktivierte mobile Apps für die Containerization und Steuerung auf App-Basis verwenden.

Durch die Nutzung von MDX-Richtlinien können Netzwerkzugriff (z. B. Micro-VPN), App- und Geräteinteraktion und App-Zugriff in Citrix Endpoint Management 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 Citrix Produktivitätsapps. Die Unterstützung umfasst Folgendes:

- Sichere E-Mail-Zustellung an Citrix Secure Mail
- Datenaustausch zwischen den geschützten mobilen Citrix Produktivitätsapps
- 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

Sie können in Citrix Endpoint Management angeben, ob Benutzer die Geräteverwaltung abwählen können. 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.

Geräteverwaltung und MDM-Registrierung

Eine Citrix Endpoint Management Enterprise-Umgebung kann unterschiedliche Anwendungsfälle enthalten, von denen einige eine Geräteverwaltung über MDM-Richtlinien für den Zugriff auf MAM-Ressourcen erfordern.

Bevor Sie mobile Citrix 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 ihre Geräte möglicherweise neu registrieren. Weitere Informationen finden Sie unter Registrierungsprofile.

Weitere Informationen zur Registrierung und zu NetScaler Gateway finden Sie unter Integration in NetScaler Gateway und Citrix ADC.

Nachfolgend sind die Vor- und Nachteile (einschließlich Abhilfemöglichkeiten) des Erzwingens einer MDM-Registrierung 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 NetScaler Gateway, Citrix Endpoint Management und App-basierten Timeouts sowie der Citrix-PIN bietet eine zusätzliche Sicherheitsebene.
- MDM-Aktionen gelten zwar nicht für ein Gerät, es gibt jedoch MDX-Richtlinien zum Verweigern des MAM-Zugriffs. Die Verweigerung basiert 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.

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 Citrix Endpoint Management auf ihren Geräten verwaltet wird und auf welche Informationen die Administratoren zugreifen können.

Geräteanforderungen

December 1, 2023

Überlegen Sie bei jeder Bereitstellung genau, welche Geräte Sie für das Rollout verwenden möchten. Zahlreiche Optionen stehen für die Plattformen iOS, Android und Windows zur Verfügung. Eine Liste der in Citrix Endpoint Management 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 Citrix Endpoint Management 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

March 11, 2024

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 Sicherheitsfeatures im Detail behandelt. Dieser Artikel enthält einen Überblick über allgemeine Sicherheitsanliegen und die in Citrix Endpoint Management 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?
- Nach welcher Zeitdauer soll bei Benutzersitzungen ein Timeout auftreten? 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 auf App-Ebene einrichten? Wie viele Anmeldeversuche möchten Sie zulassen? Denken Sie an die zusätzlichen Anforderungen der Authentifizierung pro App, die ggf. mit MAM implementiert werden, und wie dies von den Benutzern wahrgenommen wird.
- Welche weiteren Einschränkungen möchten Sie den Benutzern auferlegen? Sollen Benutzer Zugriff auf Cloudservices wie Siri erhalten? Was können die Benutzer mit den einzelnen von Ihnen zur Verfügung gestellten Apps tun und was nicht? Möchten Sie unternehmensweite Netzwerkrichtlinien (Wi-Fi) bereitstellen, damit mobile Datenkontingente nicht im Büro verbraucht werden?

App oder Gerät

Zunächst sollten Sie überlegen, was Sie schützen möchten:

- Nur bestimmte Apps (Mobilanwendungsverwaltung oder MAM)
- Das gesamte Gerät (Mobilgeräteverwaltung oder MDM).
- MDM+MAM

Wenn Sie keine Steuerung auf Geräteebene benötigen, müssen Sie meist nur die mobilen Apps verwalten, insbesondere wenn Sie BYOD-Geräte (Bring Your Own Device) zulassen.

Benutzer mit nicht von Citrix Endpoint Management 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 Citrix Endpoint Management 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. Mit MDM können Sie 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. Dies ist möglicherweise keine ideale Option für alle Organisationen oder Anwendungsfälle.

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 Citrix Secure Hub gespeichert. Wenn Sie die Benutzerentropie über die Option **Encrypt Secrets** aktivieren, erstellt Citrix Endpoint Management einen Tresor namens "User-Entropy". Citrix Endpoint Management verschiebt die Informationen aus dem allgemeinen Tresor in diesen neuen Tresor. Damit Citrix 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. Daher müssen sich die Benutzer immer authentifizieren, wenn eine App Zugriff auf freigegebene Daten im UserEntropy-Tresor (einschließlich Kennwörter, PINs und Zertifikate) benötigt.

Weitere Informationen zur Benutzerentropie finden Sie unter Informationen zum MDX Toolkit. 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. In manchen Situationen mag dies erwünscht sein, Richtlinien können jedoch ein System

auch unbrauchbar machen. Beispielsweise können Sie den Zugriff auf Cloudanwendungen wie Siri oder iCloud sperren, von denen aus sensible Daten an externe 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. Beispielsweise benötigt das iOS-Tastaturmikrofon auf Cloudzugriff.

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. Mit der zunehmenden Akzeptanz von BYOD können Sie in der Regel eine MAM-Lösung wie Citrix Endpoint Management zur Unterstützung folgender Verfahren implementieren:

- App-Bereitstellung
- Softwarelizenzierung
- Konfiguration
- App-Lebenszyklusmanagement

Mit Citrix Endpoint Management können Sie diese Apps noch sicherer machen, indem Sie bestimmte MAM-Richtlinien und VPN-Einstellungen konfigurieren, um Datenlecks und andere Sicherheitsbedrohungen zu vermeiden. Bei Citrix Endpoint Management können MDM- und MAM-Funktionen in derselben Umgebung flexibel eingesetzt werden.

Zusätzlich zur App-Bereitstellung für Mobilgeräte ermöglicht Citrix Endpoint Management 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 Apps löschen und sperren. 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 Citrix Endpoint Management werden die 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management-Lizenz enthalten sind. Weitere Informationen finden Sie unter Mobile Produktivitätsapps. Citrix bietet auch andere Business-fähige Apps. ISV entwickeln einsatzfertige Apps mit dem Mobile Apps SDK.

HDX-Apps: HDX-Apps sind unter Windows gehostete Apps, die mit StoreFront veröffentlicht werden. In einer Citrix Virtual Apps and Desktops-Umgebung können Sie solche Apps in Citrix Endpoint Management 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 Citrix Endpoint Management bereitstellen und verwalten möchten. Beispiel: Mehrere Benutzergruppen mit diversen Berechtigungsstufen sollen eine einzige App verwenden. In dem Fall können Sie separate Bereitstellungsgruppen erstellen, um zwei Versionen der App bereitzustellen. Stellen Sie sicher, 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. Diese Option erfordert die Registrierung für das Apple Volume Purchase-Programm. Sie müssen zudem die Volume Purchase-Einstellungen über die Citrix Endpoint Management-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 Citrix Endpoint Management-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. Kategorisieren Sie diese dann, z. B. als öffentliche oder native Apps, mobile Citrix Produktivitäts-Apps, Web-Apps, hausinterne Apps und ISV-Apps. Kategorisieren Sie die Apps auch nach Geräteplattform (z. B. iOS und Android). Diese Kategorisierung hilft beim Koordinieren der Citrix Endpoint Management-Einstellungen, die für jeden App-Typ erforderlich sind. Beispielsweise sind bestimmte Apps möglicherweise nicht für das Umschließen geeignet. Oder für einige Apps muss möglicherweise das Mobile Apps SDK verwendet werden, um spezielle APIs für die Interaktion mit anderen Apps zu aktivieren.

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. Definieren Sie Netzwerkanforderungen für jede App, um die Architektur vorab zu wählen. Durch diese Vorbereitung wird die Implementierung rationalisiert.

Sicherheitsanforderungen: Definieren Sie die Sicherheitsanforderungen, die für einzelne und/oder alle Apps gelten sollen. Manche Einstellungen, z. B. die MDX-Richtlinien, gelten für einzelne Apps Sitzungs- und Authentifizierungseinstellungen gelten für alle Apps. Einige Apps haben möglicherweise besondere Anforderungen an Verschlüsselung, Containerization, Umschließen, Authentifizierung, Geofencing, Passcode oder Datenfreigabe. Stellen Sie im Voraus eine Übersicht über diese Anforderungen zusammen, 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. Möglicherweise sollen bestimmte Apps Folgendes erfordern:

- Geräteplattformbasierte Verschlüsselung ist aktiviert
- Gerät wird verwaltet
- Gerät hat eine Mindestversion des Betriebssystems
- bestimmte Apps nur für Unternehmensbenutzer verfügbar

Stellen Sie solche Anforderungen im Voraus zusammen, damit Sie die entsprechenden Bereitstellungsregeln oder -aktionen konfigurieren können.

Lizenzanforderungen: Machen Sie eine Liste der Lizenzanforderungen für die Apps. Anhand der Liste können Sie die Lizenznutzung effektiv verwalten und entscheiden, ob Sie zur Vereinfachung der Lizenzierung bestimmte Features in Citrix Endpoint Management konfigurieren müssen. Wenn Sie beispielsweise eine kostenlose oder kostenpflichtige iOS-App bereitstellen, setzt Apple Lizenzanforderungen durch, indem Benutzer sich bei ihrem Apple Store-Konto anmelden müssen. Sie können sich für das Apple Volume Purchase registrieren, um solche Apps über Citrix Endpoint Management zu verteilen und zu verwalten. Über Volume Purchase können Benutzer die Apps ohne Anmeldung bei ihrem Apple

Store-Konto herunterladen. Außerdem müssen Tools wie 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 Citrix Endpoint Management 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.
- **Citrix Files:** App für den Zugriff auf geteilte Daten und zum Teilen, Synchronisieren und Bearbeiten von Dateien.

Öffentlicher App-Store

- **Citrix Secure Hub:** Client, der von allen Mobilgeräten zur Kommunikation mit Citrix Endpoint Management verwendet wird. Die IT überträgt über den Citrix Secure Hub-Client per Push Sicherheitseinstellungen, Konfigurationen und mobile Apps auf Mobilgeräte. Android- und iOS-Geräte registrieren sich über Citrix Secure Hub bei Citrix Endpoint Management.
- **Citrix Workspace-App:** 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 in Citrix Workspace 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
Citrix Secure Mail	Mobile Produktivitätsapp	Ab Version 10.4.1 nein	Ja	Ja
Citrix Secure Web	Mobile Produktivitätsapp	Ab Version 10.4.1 nein	Ja	Ja
Citrix Files	Mobile Produktivitätsapp	Ab Version 10.4.1 nein	Ja	Ja
Citrix Secure Hub	Öffentliche App	Nicht verfügbar	Ja	Ja
Citrix Workspace-App	Öffentliche App	Nicht verfügbar	Ja	Ja
GoToMeeting	Öffentliche App	Nicht verfügbar	Ja	Ja
SalesForce1	Öffentliche App	Nicht verfügbar	Ja	Ja

App-Name	App-Typ	Mit MDX umschlossen	iOS	Android
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 Citrix Endpoint Management konsultieren können.

App-Name	VPN erforderlich	Interaktion (mit Container-externen Apps)	Interaktion (von Container-externen Apps)	Geräteplattformbasierte Verschlüsselung
Citrix Secure Mail	J	Selektiv zugelassen	Zulässig	Nicht erforderlich
Citrix Secure Web	J	Zulässig	Zulässig	Nicht erforderlich
Citrix Files	J	Zulässig	Zulässig	Nicht erforderlich
Citrix Secure Hub	J	–	–	–
Citrix Workspace-App	J	–	–	–
GoToMeeting	N	–	–	–
SalesForce1	N	–	–	–
RSA SecurID	N	–	–	–
Epic Haiku	J	–	–	–
Epic Canto	J	–	–	–
Epic Rover	J	–	–	–

App-Name	VPN erforderlich	Interaktion (mit Container-externen Apps)	Interaktion (von Container-externen Apps)	Geräteplattformbasierte Verschlüsselung
Epic Hyperspace	J	–	–	–
Vocera	J	Blockiert	Blockiert	Nicht erforderlich
HCMail	J	Blockiert	Blockiert	Erforderlich
PatientRounding	J	–	–	Erforderlich
Outlook Web Access	J	–	–	Nicht erforderlich
SharePoint	J	–	–	Nicht erforderlich

App-Name	Proxy-Filter	Lizenzierung	Geofencing	Mobile Apps SDK	Mindestversion des Betriebssystems
Citrix Secure Mail	Erforderlich	–	Selektiv erforderlich	–	Erzwungen
Citrix Secure Web	Erforderlich	–	Nicht erforderlich	–	Erzwungen
Secure Notes	Erforderlich	–	Nicht erforderlich	–	Erzwungen
Citrix Files	Erforderlich	–	Nicht erforderlich	–	Erzwungen
Citrix Secure Hub	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Citrix Workspace-App	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
GoToMeeting	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
SalesForce1	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
RSA SecurID	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Epic Haiku	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen

App-Name	Proxy-Filter	Lizenzierung	Geofencing	Mobile Apps SDK	Mindestversion des Betriebssystems
Epic Canto	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Epic Rover	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Epic Hyperspace	Nicht erforderlich	–	Nicht erforderlich	–	Nicht erzwungen
Vocera	Erforderlich	–	Erforderlich	Erforderlich	Erzwungen
HCMail	Erforderlich	–	Erforderlich	Erforderlich	Erzwungen
PatientRounding	Erforderlich	–	Nicht erforderlich	–	Nicht erzwungen
Outlook Web Access	Erforderlich	–	Nicht erforderlich	–	Nicht erzwungen
SharePoint	Erforderlich	–	Nicht erforderlich	–	Nicht erzwungen

Communities

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 Benutzergeräte bereitstellen. Manche Benutzer arbeiten von zu Hause oder an Remotestandorten und verwenden dabei die von Ihnen bereitgestellten Mobilgeräte. Andere Benutzer verwenden eigene Mobilgeräte für den Zugriff auf Tools, für die bestimmte Regeln zur Sicherheitskonformität gelten.

Je mehr Benutzer mit Mobilgeräten arbeiten, desto bedeutender wird das Enterprise Mobility Management (EMM), um Datenlecks zu verhindern. EMM ist auch wichtig, um die 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 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 Gerät verwalten. Dabei kann es sich um unternehmenseigene oder private Geräte (BYOD, Bring Your Own Device) handeln. 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)
- 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 Citrix Endpoint Management finden Sie unter Ressourcen bereitstellen.

Active Directory-Organisationseinheiten (OUs) und -Gruppen Für OU **=** Citrix Endpoint Management-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 Benutzer und Gruppen in Citrix Endpoint Management Für Gruppe = Auftragnehmer, Benutzer =

- Vendor1
- Vendor2
- Anbieter 3
- …Anbieter 10

Bereitstellungsgruppen in Citrix Endpoint Management

- 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	Bereitstellungsgruppen in Citrix Endpoint Management
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.

Bereitstellungsgruppen in Citrix Endpoint Management	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

Bereitstellungsgruppen in Citrix Endpoint Management	Öffentliche App: RSA SecurID	Öffentliche App: EpicCare Haiku	HDX-App: Epic Hyperspace	Passcoderichtlinie	Geräteeinschränkungen	Automatisierte Aktionen	Netzwerkrichtlinie
Klinik - Pflegepersonal							X

Bereitstellungsgruppen in Citrix Endpoint Management	Öffentliche App: RSA SecurID	Öffentliche App: EpicCare Haiku	HDX-App: Epic Hyperspace	Passcoderichtlinie	Gerät einschränken	Automatisierte Aktionen	Netzwerkrichtlinie
Klinik - Mediziner					X		
Klinik - Fachärzte							
Klinik - Externe Mediziner							
Klinik - Hausbesuchsdienste							
Klinik - Forschungsspezialisten							
Klinik - Schulungen, Aus- und Weiterbildung		X	X				
Verwaltung - Gemeinsam genutzte Dienste		X	X				
Verwaltung - Arztbezogene Dienste		X	X				
Verwaltung - Supportdienste		X	X				

Hinweise und Überlegungen

- Citrix Endpoint Management erstellt bei der Erstkonfiguration die Standardbereitstellungsgruppe "Alle Benutzer". Wenn Sie diese Bereitstellungsgruppe nicht deaktivieren, sind alle Active Directory-Benutzer berechtigt, sich bei Citrix Endpoint Management zu registrieren.
- Citrix Endpoint Management 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 Citrix Endpoint Management zugeordnet ist, kann der Benutzer sich nicht registrieren. Wenn ein Benutzer Mitglied in mehreren Gruppen ist, kategorisiert Citrix Endpoint Management den Benutzer nur als Mitglied der Gruppen, die Citrix Endpoint Management zugeordnet sind.

Sicherheitsanforderungen

Die bei einer Citrix Endpoint Management-Umgebung zu beachtenden Sicherheitsaspekte können schnell zu einer Herausforderung werden. Es gibt viele ineinandergreifende Elemente und Einstellungen. Sie sind sich daher vielleicht nicht sicher, wo Sie anfangen und was Sie für ein akzeptables Sicherheitsniveau wählen sollen. Um diese Auswahl zu vereinfachen, gibt Citrix Empfehlungen für hohe, höhere und höchste Sicherheit. Diese sind in der folgenden Tabelle aufgeführt.

Die Auswahl des Verwaltungsmodus für Geräte (MAM, MDM+MAM mit optionalem MDM oder MDM+MAM mit erforderlichem MDM) sollte nicht allein auf der Basis von Sicherheitsüberlegungen erfolgen. 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.

Verwaltungsmodus –Sicherheitsüberlegungen

Die folgende Tabelle enthält die Verwaltungsmodi für jede Sicherheitsstufe.

Hohe Sicherheit	Höhere Sicherheit	Höchste Sicherheit
MAM, MDM+MAM	MDM+MAM	MDM+MAM

Hinweise:

- Je nach Anwendungsfall kann eine Nur-MAM-Bereitstellung die Sicherheitsanforderungen erfüllen und eine gute Benutzererfahrung bieten.
- 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.

Citrix ADC und NetScaler Gateway –Sicherheitsüberlegungen

Die folgende Tabelle enthält Empfehlungen für Citrix ADC und NetScaler Gateway für jede Sicherheitsstufe.

Hohe Sicherheit	Höhere Sicherheit	Höchste Sicherheit
Citrix ADC wird empfohlen. NetScaler Gateway ist für MAM und MDM+MAM erforderlich	Standardkonfiguration des NetScaler für XenMobile-Assistenten mit SSL-Brücke, wenn Citrix Endpoint Management in der DMZ ist.	SSL-Offload mit End-to-End-Verschlüsselung

Hinweise:

- Das Öffnen des Citrix Endpoint Management-Servers zum Internet über NAT oder Proxys/Loadbalancer von Drittanbietern kann eine Option für MDM darstellen. In diesem Fall endet SSL-Datenverkehr jedoch auf einem Citrix Endpoint Management-Server, was ein Sicherheitsrisiko bedeutet.
- In Umgebungen mit hoher Sicherheit werden die Sicherheitsanforderungen von NetScaler Gateway mit der standardmäßigen Citrix Endpoint Management-Konfiguration erfüllt oder übertroffen.
- Bei MDM-Registrierungen mit höchsten Sicherheitsanforderungen können Sie durch die SSL-Terminierung am NetScaler Gateway den Datenverkehr am Umkreis untersuchen, wobei eine Ende-zu-Ende-SSL-Verschlüsselung gewährleistet ist.
- Optionen zum Definieren von SSL-/TLS-Verschlüsselungsverfahren.
- Weitere Information finden Sie unter Integration in NetScaler Gateway und Citrix ADC.

Registrierung –Sicherheitsüberlegungen

Die folgende Tabelle enthält Empfehlungen für Citrix ADC und NetScaler 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. Für diese Einschränkung 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. Kann über MDM erzwungen werden. Kann für Nur-MAM-Umgebungen über die MDX-Richtlinie “Verhalten für nicht richtlinientreue Geräte”erzwungen werden.	Wird über eine MDM-, MAM- oder MDM+MAM-Richtlinie 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 Geräte-Passcode Voraussetzung für die Verwendung verwalteter Apps ist, beispielsweise für Anwendungsfälle mit BYOD.
- Citrix empfiehlt, die Kombination von MDM- und MDX-Richtlinien zur größeren Sicherheit für MDM+MAM-Registrierungen.
- 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

December 1, 2023

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. Mit der zunehmenden Akzeptanz von BYOD können Sie in der Regel eine MAM-Lösung wie Citrix Endpoint Management implementieren. Citrix Endpoint Management unterstützt Sie bei der Anwendungsbereitstellung, Softwarelizenzierung, Konfiguration und Anwendungslebenszyklusverwaltung. Sie können vorschreiben oder zulassen, dass Benutzer sich auch für die MDM-Verwaltung entscheiden können.

Mit Citrix Endpoint Management können Sie Apps sichern, indem Sie MAM-Richtlinien und VPN-Einstellungen konfigurieren, um Datenlecks und andere Sicherheitsbedrohungen zu vermeiden. Citrix Endpoint Management bietet Unternehmen die Flexibilität, Geräte als Nur-MAM oder MDM+MAM zu registrieren.

Zusätzlich zur App-Bereitstellung für Mobilgeräte ermöglicht Citrix Endpoint Management 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 Citrix Endpoint Management werden die 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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Endpoint Management-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 Citrix Endpoint Management 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 Citrix Endpoint Management-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 Citrix Endpoint Management-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 Citrix Endpoint Management-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 Citrix 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 kann 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 Citrix Endpoint Management 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 Citrix Endpoint Management verteilen und verwalten. Über Volume Purchase können Benutzer die Apps ohne Anmeldung bei ihrem Apple App Store-Konto herunterladen.

  Einige Plattformen 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 Citrix Endpoint Management 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:

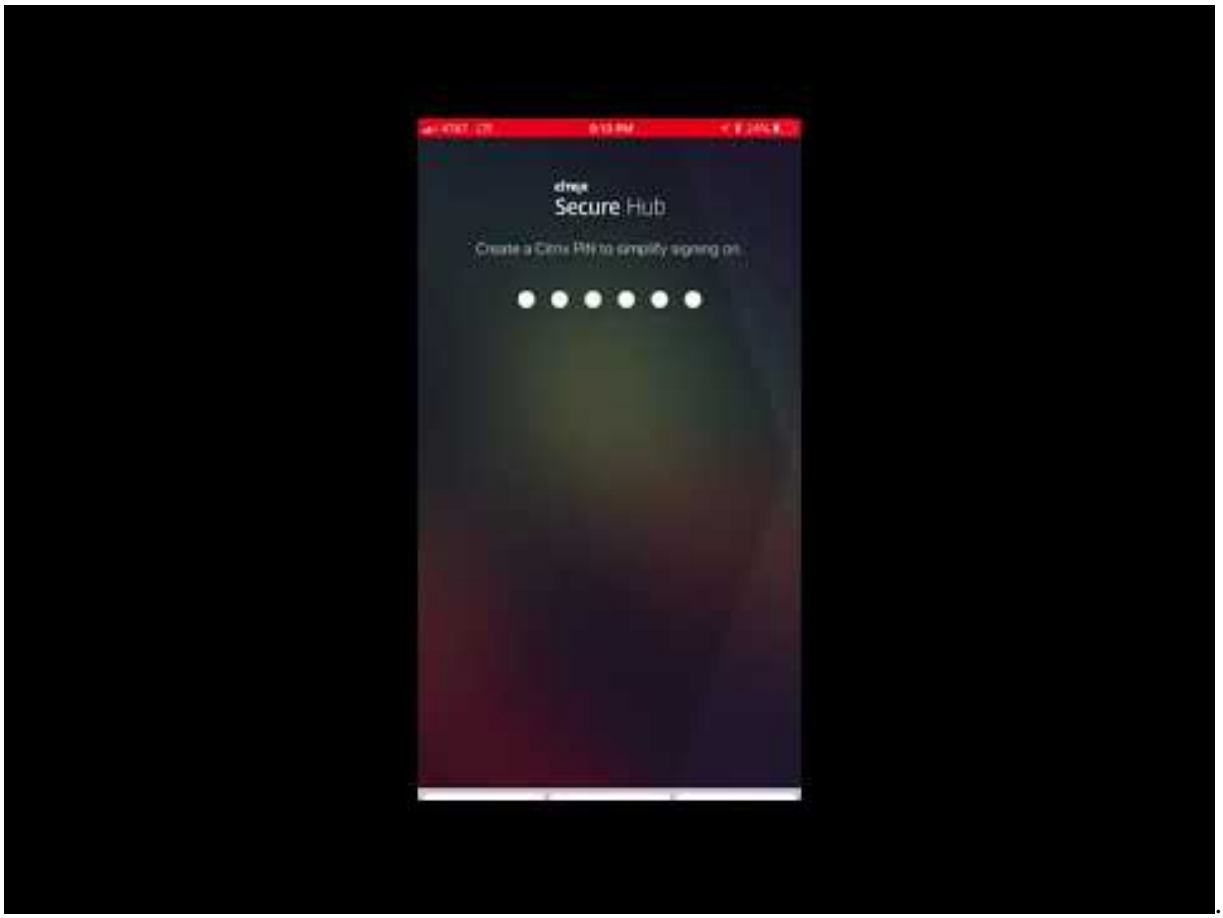
Mobile Produktivitätsapps: iOS- und Android-Apps von Citrix. Weitere Informationen finden Sie unter Mobile Produktivitätsapps.

Citrix Secure Hub: Für Kunden, die Citrix Endpoint Management vor Version 10.18.14 erworben

haben: Sie übermitteln Sicherheitseinstellungen, Konfigurationen und mobile Apps über Citrix Secure Hub auf mobile Geräte. Android- und iOS-Geräte registrieren sich über Citrix Secure Hub bei Citrix Endpoint Management.

Für Neukunden ab Citrix Endpoint Management-Version 10.18.14: Citrix Secure Hub unterstützt die Verwendung des Workspace-App-Stores. Der Citrix Secure Hub-Store wird beim Öffnen von Citrix Secure Hub nicht mehr angezeigt. Benutzer werden über die Schaltfläche "Apps hinzufügen"zum Workspace-App-Store geleitet.

Das folgende Video zeigt, wie ein iOS-Gerät über die Citrix Workspace-App bei Citrix Endpoint Management registriert wird.



Citrix Workspace-App: Die Citrix Workspace-App umfasst vorhandene Citrix Receiver-Technologie, Citrix Secure Hub und andere Citrix Workspace-Clienttechnologien. Die Citrix Workspace-App bietet Endbenutzern eine einheitliche, kontextbezogene Benutzererfahrung.

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 in Citrix Workspace 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	MDX-fähig	iOS	Android
Citrix Secure Mail	Mobile Produktivitätsapp	Nein	Ja	Ja
Citrix Secure Web	Mobile Produktivitätsapp	Nein	Ja	Ja
Citrix Files	Mobile Produktivitätsapp	Nein	Ja	Ja
Citrix Secure Hub	Öffentliche App	–	Ja	Ja

App-Name	App-Typ	MDX-fähig	iOS	Android
Citrix Workspace-App	Öffentliche App	–	Ja	Ja
GoToMeeting	Öffentliche App	–	Ja	Ja
SalesForce1	Öffentliche App	–	Ja	Ja
RSA SecurID	Öffentliche App	–	Ja	Ja
Epic Haiku	Öffentliche App	–	Ja	Ja
Epic Canto	Öffentliche App	–	Ja	Nein
Epic Rover	Öffentliche App	–	Ja	Nein
Epic Hyperspace	HDX-App	–	Ja	Ja
Vocera	ISV-App	Ja	Ja	Ja
HCMail	Interne App	Ja	Ja	Ja
PatientRounding	Web-App	–	Ja	Ja
Outlook Web Access	Web-App	–	Ja	Ja
SharePoint	Web-App	–	Ja	Ja

In der folgenden Tabelle sind die spezifischen Anforderungen aufgeführt, die bei der Konfiguration von MAM-Richtlinien in Citrix Endpoint Management zu berücksichtigen sind.

App-Name	VPN erforderlich	Interaktion (mit Container-externen Apps)	Interaktion (von Container-externen Apps)	Proxy-Filter	Lizenzierung	Geofencing	Mobile Apps SDK	Mindestversion des Betriebssystems
Citrix Secure Mail	J	Selektiv zugelassen	Zulässig	Erforderlich	–	Selektiv erforderlich	–	Erzwungen
Citrix Secure Web	J	Zulässig	Zulässig	Erforderlich	–	Nicht erforderlich	–	Erzwungen
Citrix Files	J	Zulässig	Zulässig	Erforderlich	–	Nicht erforderlich	–	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
Citrix Secure Hub	J	–	–	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Citrix Workspace-App	J	–	–	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
GoToMeeting	N	–	–	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
SalesForce1	N	–	–	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
RSA SecurID	N	–	–	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Epic Haiku	J	–	–	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Epic Canto	J	–	–	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Epic Rover	J	–	–	Nicht erforderlich	Volume Purchase	Nicht erforderlich	–	Nicht erzwungen
Epic Hyperspace	J	–	–	Nicht erforderlich	–	Nicht erforderlich	–	Nicht erzwungen
Vocera	J	Blockiert	Blockiert	Erforderlich	–	Erforderlich	Erforderlich	Erzwungen
HCMail	J	Blockiert	Blockiert	Erforderlich	–	Erforderlich	Erforderlich	Erzwungen
PatientRoulding	–	–	Erforderlich	–	Nicht erforderlich	–	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
Outlook Web Access	J	–	–	Erforderlich	–	Nicht erforderlich	–	Nicht erzwungen
SharePoint	J	–	–	Erforderlich	–	Nicht erforderlich	–	Nicht erzwungen

Communities

December 1, 2023

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 angewandt 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 Citrix Endpoint Management-Ressourcen zugreifen.

- Lokale Benutzer und Gruppen in Citrix Endpoint Management

  Für Benutzer ohne Active Directory-Konto können Sie ein Konto als lokale Citrix Endpoint Management-Benutzer erstellen. Diese lokalen Benutzer können Sie dann zu Bereitstellungsgruppen hinzufügen und ihnen dieselben Ressourcen wie Active Directory-Benutzern bereitstellen.

- Bereitstellungsgruppen in Citrix Endpoint Management

  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. Citrix empfiehlt, zunächst die Bereitstellungsgruppen und dann die Geräterichtlinien zu erstellen.

- 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 (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 Citrix Endpoint Management finden Sie in der Produktdokumentation zu Citrix Endpoint Management unter Ressourcen bereitstellen.

Active Directory-Organisationseinheiten (OUs) und -Gruppen

Für OU = Citrix Endpoint Management-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 Benutzer und Gruppen in Citrix Endpoint Management

Für Gruppe = Auftragnehmer, Benutzer =

- Vendor1
- Vendor2
- Anbieter 3
- …Anbieter 10

Bereitstellungsgruppen in Citrix Endpoint Management

- 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	Bereitstellungsgruppen in Citrix Endpoint Management
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	Citrix Files	Workspace-App	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Klinik - Pflegeper-sonal	X	X	X					
Klinik - Medi-ziner								
Klinik - Fachärzte								
Klinik - Externe Medi-ziner	X		X					

	Secure Mail	Secure Web	Citrix Files	Workspace-App	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Klinik - Hausbesuchsdienste	X		X					
Klinik - Forschungsspezialisten	X		X					
Klinik - Schulungen, Aus- und Weiterbildung							X	X
Verwaltung - Gemeinsam genutzte Dienste							X	X
Verwaltung - Arztbezogene Dienste	X		X				X	X
Verwaltung - Supportdienste	X		X				X	X
Gemeinnützige Stiftungen								
Auftragnehmer	X		X	X	X		X	X

Bereitstellungsgruppen und die Ressourcenzuordnung von MDM-Ressourcen

	MDM: Passcoderichtlinie	MDM: Geräteeinschränkungen	MDM: Automatisierte Aktionen	MDM: Netzwerkrichtlinie
Klinik - Pflegepersonal				X
Klinik - Mediziner		X		
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				
Auftragnehmer				X

Hinweise und Überlegungen

- Citrix Endpoint Management erstellt bei der Erstkonfiguration die Standardbereitstellungsgruppe “Alle Benutzer”. Wenn Sie diese Bereitstellungsgruppe nicht deaktivieren, sind alle Active Directory-Benutzer berechtigt, sich bei Citrix Endpoint Management zu registrieren.

- Citrix Endpoint Management 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 Citrix Endpoint Management zugeordnet ist, kann der Benutzer sich nicht registrieren. Wenn ein Benutzer Mitglied in mehreren Gruppen ist, kategorisiert Citrix Endpoint Management den Benutzer nur als Mitglied der Gruppen, die Citrix Endpoint Management zugeordnet sind.

E-Mail-Strategie

March 11, 2024

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 gehört zu den Hauptkriterien eines Citrix Endpoint Management-Designs. Citrix Endpoint Management 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	Citrix Secure Mail	Systemeigene Clients (z. B. iOS Mail)	Drittanbieterclients

Konfiguration	Über eine MDX-Richtlinie konfigurierte Exchange-Kontoprofile.	Über eine MDM-Richtlinie konfigurierte Exchange-Kontoprofile. Android-Unterstützung beschränkt auf: 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. Citrix Secure Mail ist eine vollständig verwaltete App (per MDX-Richtlinie). Zusätzliche Authentifizierungsstufe per Citrix-PIN.	Je nach Anbieter/App-Features. Bietet höhere Sicherheit. Verwendet Einstellungen der Geräteverschlüsselung. 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 Citrix Secure Mail über MDM aus öffentlichen App-Stores. In Lizenz für Citrix Endpoint Management 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 Citrix 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 zum ActiveSync-E-Mail-Verkehr im Kontext von Citrix Endpoint Management 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. NetScaler Gateway) 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 Citrix Secure Mail-Client verwenden. Dadurch können Sie die Sicherheitsfunktionen der MDX-Richtlinien und der App-Verwaltung nutzen.

Szenario 2: Tunneling über NetScaler Gateway (Micro-VPN und STA)

Dieses Szenario ist Standard bei Verwendung des Citrix Secure Mail-Clients aufgrund von dessen Micro-VPN-Funktionen. Der Citrix Secure Mail-Client stellt über NetScaler Gateway eine sichere Verbindung mit ActiveSync her. Im Wesentlichen ist Citrix Secure Mail hier der Client, der aus dem internen Netzwerk eine direkte Verbindung mit ActiveSync herstellt. Citrix Kunden verwenden Citrix 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 Citrix Endpoint Management 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. Citrix Secure Mail oder andere systemeigene oder Drittanbieterclients.

Citrix Endpoint Management bietet bei diesem Szenario in drei Bereichen Vorteile:

- Clients mit MDX-Richtlinien und App-Verwaltung mit Citrix Secure Mail
- Clientkonfiguration unter Verwendung einer MDM-Richtlinie bei unterstützten systemeigenen E-Mail-Clients
- ActiveSync-Filteroptionen mit Einsatz des Citrix 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. Citrix Endpoint Management umfasst zwei Komponenten, die ActiveSync-Filterfunktionen für systemeigene Clients und für Drittanbieterclients bereitstellen: NetScaler Gateway Connector für Exchange ActiveSync und Citrix Endpoint Management Connector für Exchange ActiveSync.

NetScaler Gateway Connector für Exchange ActiveSync

NetScaler Gateway Connector für Exchange ActiveSync ermöglicht eine ActiveSync-Filterung im Umkreis, wobei NetScaler Gateway 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 Connector für Exchange ActiveSync fungiert als Vermittler zwischen NetScaler Gateway und Citrix Endpoint Management. Wenn ein Gerät über den virtuellen ActiveSync-Server auf dem NetScaler Gateway mit Exchange kommuniziert, führt dieser einen HTTP-Callout an den Connector für Exchange ActiveSync-Dienst aus. Dieser Dienst überprüft dann den Gerätestatus bei Citrix Endpoint Management. Je nach Gerätestatus weist der Connector für Exchange ActiveSync NetScaler Gateway 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 Citrix Endpoint Management Connector für Exchange ActiveSync verwenden.
- **NetScaler Gateway-Skalierbarkeit:** Angesichts der Notwendigkeit, den ActiveSync-Datenverkehr über NetScaler Gateway als Proxy zu leiten, ist die richtige Dimensionierung der NetScaler Gateway-Instanz entscheidend, um die zusätzliche Workload aller ActiveSync-SSL-Verbindungen zu bewältigen.
- **Integrated Caching bei NetScaler Gateway:** Der Connector für Exchange ActiveSync auf dem NetScaler Gateway ist so konfiguriert, dass die Antworten des Connectors mit Integrated Caching zwischengespeichert werden. Daher muss NetScaler Gateway nicht jede ActiveSync-Transaktion in einer bestimmten Sitzung beim Connector anfordern. Diese Konfiguration ist auch entscheidend für eine angemessene Leistung und Skalierung. Integrated Caching ist mit der NetScaler Gateway Platinum Edition verfügbar.
- **Benutzerdefinierte Filterrichtlinien:** Sie müssen ggf. eigene NetScaler Gateway-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 NetScaler Gateway-Responderrichtlinien.
- **Citrix Secure Mail-Clients:** Citrix Secure Mail hat Micro-VPN-Funktionen, die das Filtern am Umkreis überflüssig machen. Der Citrix Secure Mail-Client wird im Allgemeinen als interner

(vertrauenswürdiger) ActiveSync-Client behandelt, wenn er über NetScaler Gateway verbunden ist. Werden sowohl systemeigene Clients und Drittanbieterclients (mit dem Connector für Exchange ActiveSync) als auch Citrix Secure Mail-Clients verwendet, empfiehlt Citrix, den Citrix Secure Mail-Datenverkehr nicht über den für den Connector verwendeten virtuellen NetScaler Gateway-Server zu leiten. Sie können den Datenverkehr über DNS leiten und Auswirkungen der Connector-Richtlinie auf die Citrix Secure Mail-Clients verhindern.

Ein Diagramm mit dem NetScaler Gateway Connector für Exchange ActiveSync in einer Citrix Endpoint Management-Bereitstellung finden Sie unter Architektur.

Citrix Endpoint Management Connector für Exchange ActiveSync

Der Citrix Endpoint Management Connector für Exchange ActiveSync ermöglicht eine ActiveSync-Filterung auf der Exchange-Dienstebene. Das Resultat ist, dass die Filterung erst dann erfolgt, wenn die E-Mail den Exchange-Dienst erreicht, und nicht sobald sie in die Citrix Endpoint Management-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 Citrix Endpoint Management Connectors für Exchange ActiveSync unter Quarantäne gestellt, bzw. aus dieser befreit.

Ähnlich wie der NetScaler Gateway Connector für Exchange ActiveSync überprüft der Connector für Exchange ActiveSync den Gerätestatus mit Citrix Endpoint Management, 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 NetScaler Gateway. Sie können den Connector für Exchange ActiveSync ohne Änderungen am Routing des ActiveSync-Datenverkehrs bereitstellen. Es sind folgende Punkte zu berücksichtigen:

- **Windows-Server:** Der Connector für Exchange ActiveSync erfordert einen Windows-Server.
- **Filterregelsatz:** Wie der NetScaler Gateway Connector für Exchange ActiveSync umfasst der Connector für Exchange ActiveSync Filterregeln zur Bewertung des Gerätezustands. Darüber hinaus unterstützt der Connector für Exchange ActiveSync auch statische Regeln zum Filtern nach Active Directory-Gruppenmitgliedschaft.
- **Exchange-Integration:** Der 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 Connector für Exchange ActiveSync auf der ActiveSync-Dienstebene filtert, sollten Sie andere ActiveSync-Clients außerhalb der Citrix Endpoint

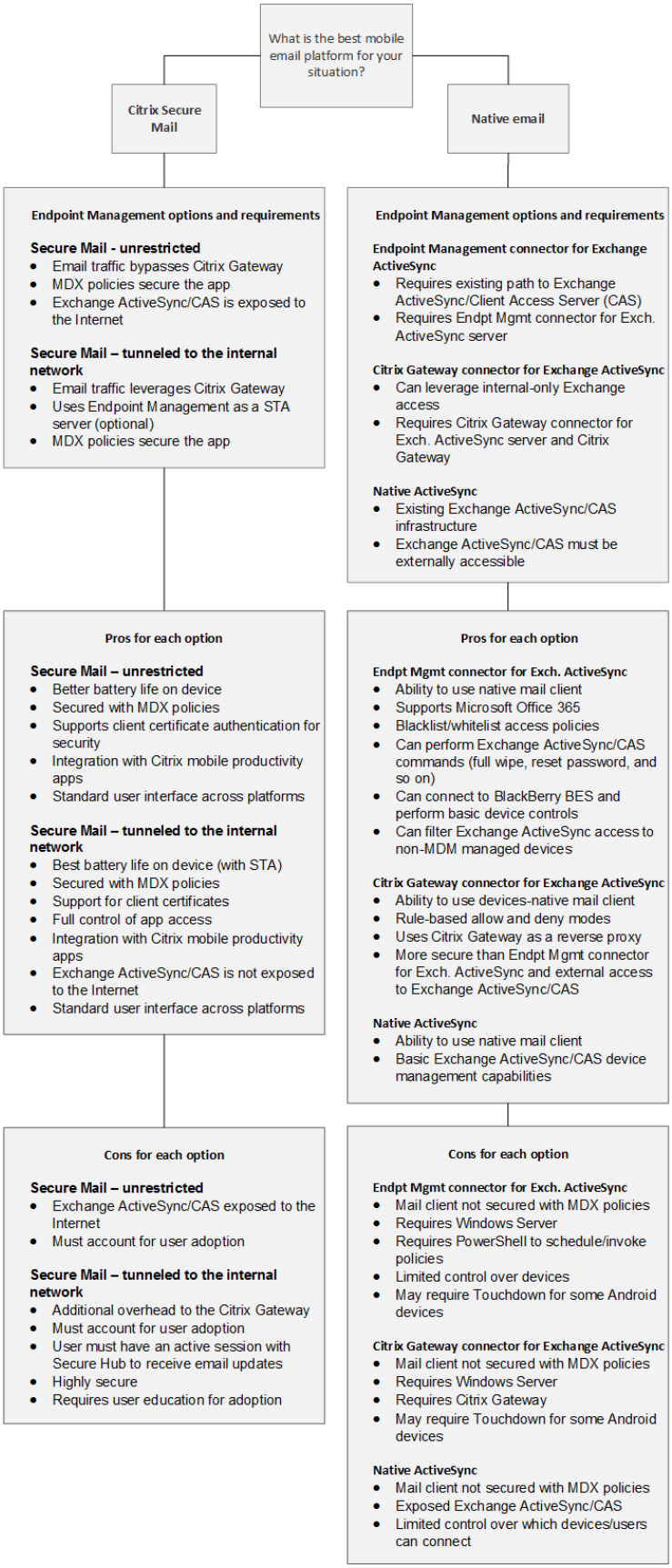
Management-Umgebung berücksichtigen. Sie können statische Regeln für den Connector für Exchange ActiveSync konfigurieren, um unbeabsichtigte Auswirkungen auf andere ActiveSync-Clients zu vermeiden.

- **Erweiterte Exchange-Funktionen:** Durch die direkte Integration in Exchange ActiveSync bietet der Connector für Exchange ActiveSync die Möglichkeit, über Citrix Endpoint Management eine Exchange ActiveSync-Löschung auf einem Mobilgerät durchzuführen. Mit dem Connector für Exchange ActiveSync kann Citrix Endpoint Management außerdem auf Blackberry-Geräteinformationen zugreifen und andere Steuerungsvorgänge durchführen.

Ein Diagramm mit dem Citrix Endpoint Management Connector für Exchange ActiveSync in einer Citrix Endpoint Management-Bereitstellung finden Sie unter Architektur.

Entscheidungsbaum zur Wahl der E-Mail-Plattform

Die folgende Abbildung bietet einen Überblick über die Vor- und Nachteile der Verwendung systemeigener E-Mail-Lösungen bzw. von Citrix Secure Mail in einer Citrix Endpoint Management-Bereitstellung. Für jede Option gibt es spezifische Citrix Endpoint Management-Optionen und -Anforderungen, die den Zugriff auf Server, Netzwerk und Datenbank regeln. Die Vor- und Nachteile umfassen Aspekte im Hinblick auf Sicherheit, Richtlinien und Benutzeroberfläche.



Integration von Citrix Endpoint Management

March 11, 2024

In diesem Artikel werden die Punkte beschrieben, die bei der Integration von Citrix Endpoint Management in ein Netzwerk und in bestehende Lösungen berücksichtigt werden müssen. Falls Sie beispielsweise NetScaler Gateway bereits für Citrix Virtual Apps and Desktops verwenden:

- Möchten Sie die vorhandene NetScaler Gateway-Instanz oder eine neue dedizierte Instanz verwenden?
- Möchten Sie die mit StoreFront veröffentlichten HDX-Apps in Citrix Endpoint Management integrieren?
- Planen Sie die Verwendung von Citrix Files mit Citrix Endpoint Management?
- Haben Sie eine Network Access Control-Lösung, die Sie in Citrix Endpoint Management integrieren möchten?

NetScaler Gateway

NetScaler Gateway ist für Citrix Endpoint Management erforderlich. NetScaler Gateway bietet einen Micro-VPN-Pfad für den Zugriff auf alle Unternehmensressourcen und unterstützt eine starke Multifaktorauthentifizierung.

Sie können vorhandene NetScaler Gateway-Instanzen verwenden oder neue Instanzen für Citrix Endpoint Management einrichten. In den folgenden Abschnitten werden die Vor- und Nachteile der Verwendung vorhandener und neuer NetScaler Gateway-Instanzen aufgeführt.

Gemeinsames NetScaler Gateway MPX mit einer für Citrix Endpoint Management erstellten virtuellen NetScaler Gateway-IP-Adresse

Vorteile:

- Verwendung einer NetScaler Gateway-Instanz für alle Citrix Remoteverbindungen: Citrix Virtual Apps, vollständiges/clientloses VPN.
- Verwendung der bestehenden NetScaler Gateway-Konfigurationen, z. B. für die Zertifikatauthentifizierung und den Zugriff auf Dienste wie DNS, LDAP und NTP.
- Verwendung einer einzelnen NetScaler Gateway-Plattformlizenz.

Nachteile:

- Die Skalierungsplanung ist schwieriger, wenn zwei unterschiedliche Anwendungsfälle auf demselben NetScaler Gateway bewältigt werden.

- In Einzelfällen wird für einen Citrix Virtual Apps-Anwendungsfall eine bestimmte NetScaler Gateway-Version benötigt. Diese Version kann jedoch zu Problemen bei Citrix Endpoint Management führen. Umgekehrt kann Citrix Endpoint Management zu Problemen bei der NetScaler Gateway-Version führen.
- Bei einem vorhandenen NetScaler Gateway können Sie den NetScaler für XenMobile-Assistenten nicht ein zweites Mal ausführen, um die NetScaler Gateway-Konfiguration für Citrix Endpoint Management zu erstellen.
- Auf NetScaler Gateway installierte Benutzerzugriffslizenzen, die für die VPN-Konnektivität erforderlich sind, werden gepoolt (außer bei Verwendung von Platinum-Lizenzen für NetScaler Gateway 11.1 oder höher). Da diese Lizenzen für alle virtuellen NetScaler Gateway-Server verfügbar sind, können auch andere Dienste als Citrix Endpoint Management sie verbrauchen.

Dedizierte NetScaler Gateway VPX-/MPX-Instanz

Vorteile:

Citrix empfiehlt die Verwendung einer dedizierten NetScaler Gateway-Instanz.

- Einfachere Skalierungsplanung und Trennung des Citrix Endpoint Management-Datenverkehrs von einer möglicherweise bereits mit eingeschränkten Ressourcen laufenden NetScaler Gateway-Instanz.
- Keine Probleme, wenn Citrix Endpoint Management und Citrix Virtual Apps unterschiedliche NetScaler Gateway-Softwareversionen erfordern. Normalerweise empfiehlt sich die Verwendung der neuesten kompatiblen NetScaler Gateway-Version für Citrix Endpoint Management.
- Konfiguration von NetScaler Gateway für Citrix Endpoint Management über den integrierten NetScaler für XenMobile-Assistenten möglich.
- Virtuelle und physische Trennung von Diensten.

Nachteile:

- Erfordert die Einrichtung zusätzlicher Dienste auf NetScaler Gateway für die Citrix Endpoint Management-Konfiguration.
- Erfordert eine zusätzliche NetScaler Gateway-Plattformlizenz. Lizenzierung jeder NetScaler Gateway-Instanz für NetScaler Gateway.

Informationen darüber, was bei der Integration von NetScaler Gateway und Citrix ADC für Citrix Endpoint Management-Verwaltungsmodi zu beachten ist, finden Sie unter Integration in NetScaler Gateway und Citrix ADC.

StoreFront

In Citrix Virtual Apps and Desktops-Umgebungen können HDX-Anwendungen mithilfe von StoreFront in Citrix Endpoint Management integriert werden. Für die Integration von HDX-Apps in Citrix Endpoint Management gilt Folgendes:

- Die Apps stehen Benutzern zur Verfügung, die bei Citrix Endpoint Management registriert sind.
- Die Apps werden zusammen mit anderen mobilen Apps im App-Store angezeigt.
- Citrix Endpoint Management verwendet Citrix Receiver auf StoreFront.
- Ist die Citrix Workspace-App auf einem Gerät installiert, wird sie von HDX-Apps verwendet.

Bei StoreFront gilt die Beschränkung auf eine Service-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 Citrix Endpoint Management in Betracht zu ziehen.

Folgende Punkte sind 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 Citrix Endpoint Management mit demselben NetScaler Gateway aufgelistet werden.
- Sollten Sie den gleichen Store verwenden oder einen Store 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 Citrix Workspace und mobile Citrix Produktivitätsapps aufgeführt.

Integration der bestehenden StoreFront-Instanz in Citrix Endpoint Management

Vorteile:

- Gleicher Store: Citrix Endpoint Management erfordert keine zusätzliche Konfiguration von StoreFront, vorausgesetzt es wird dieselbe NetScaler Gateway-VIP für den HDX-Zugriff verwendet. Angenommen, Sie entscheiden sich für die Verwendung desselben Stores und möchten den Citrix Workspace-Zugriff auf eine neue NetScaler Gateway-VIP umleiten. Fügen Sie in diesem Fall StoreFront die entsprechende NetScaler 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 Citrix Endpoint Management auswirken.

- Gleicher StoreFront-Server: In großen Umgebungen müssen Sie die zusätzliche Belastung von Citrix Receiver durch Citrix Endpoint Management für die App-Auflistung und den Start berücksichtigen.

Verwenden einer neuen, dedizierten StoreFront-Instanz zur Integration in Citrix Endpoint Management

Vorteile:

- Neuer Store: Konfigurationsänderungen am StoreFront-Store für Citrix Endpoint Management haben keine Auswirkungen auf Virtual Apps and Desktops-Workloads.
- Neuer StoreFront-Server: Änderungen an der Serverkonfiguration wirken sich nicht auf den Virtual Apps and Desktops-Workflow aus. Außerdem beeinträchtigt die Citrix Endpoint Management-externe Nutzung von Citrix Receiver für App-Auflistung und -Start die Skalierbarkeit nicht.

Nachteile:

- Neuer Store: StoreFront-Store-Konfiguration.
- Neuer StoreFront-Server: erfordert eine neue StoreFront-Installation und -Konfiguration.

Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops über den App-Store.

ShareFile und Citrix Files

ShareFile ermöglicht Ihnen den einfachen und sicheren Austausch von Dokumenten, das Senden umfangreicher Dokumente per E-Mail und die sichere Übertragung von Dokumenten an Dritte. Die Citrix Files-App 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.

Citrix Endpoint Management bietet folgende Funktionen für Citrix Files:

- Single Sign-On-Authentifizierung für mobile Produktivitätsappbenutzer.
- Active Directory-basierte Benutzerkontobereitstellung.
- Umfassende Richtlinien zur Zugriffssteuerung.

Mobile Benutzer können alle Funktionen des Enterprise-Kontos verwenden.

Alternativ können Sie Citrix Endpoint Management für die ausschließliche Integration mit 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. Sie konfigurieren die Integration mit Enterprise-Konten oder Speicherzonenconnectors über die Citrix Endpoint Management-Konsole. Weitere Informationen finden Sie unter Citrix Files für Citrix Endpoint Management.

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

Zu klärende Fragen:

- Möchten Sie Daten in von Citrix verwalteten Speicherzonen speichern?
- 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, sollte die Integration mit einem Enterprise-Konto erfolgen.
- 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 Citrix Files-Unterdomäne einrichten, Benutzer für Citrix Files bereitstellen oder Citrix Files-Daten hosten. Die Verwendung von Speicherzonenconnectors mit Citrix Endpoint Management entspricht den Sicherheitsbeschränkungen, die verhindern, dass Benutzerdaten außerhalb des Unternehmensnetzwerks gelangen.

Standort des Speicherzonencontroller-Servers

Zu klärende 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 und NAT/PAT-Konfigurationen.

Speicherzonenconnectors

Zu klärende 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 NetScaler Gateway anzusiedeln.

SAML-Integration in Citrix Endpoint Management

Zu klärende Fragen:

- Ist eine Active Directory-Authentifizierung für Citrix Files erforderlich?
- Ist SSO bei der ersten Verwendung der Citrix Files-App für Citrix Endpoint Management erforderlich?
- 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:

SAML kann als Authentifizierungsmechanismus für Citrix Files verwendet werden. Authentifizierungsoptionen:

- Verwendung des Citrix Endpoint Management-Servers 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.

Der Citrix Endpoint Management-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 beide Anwendungsfälle zu erfüllen, lesen Sie ShareFile Single Sign-On-Konfigurationsleitfaden für Anbieter von dualen Identitäten.

Mobile Apps

Zu klärende Fragen:

- Welche mobile Citrix Files-App (öffentlich, MDM, MDX) möchten Sie verwenden?

Designentscheidung:

- Sie verteilen mobile Citrix 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 niedrigen Sicherheitsanforderungen (Containerization nicht erforderlich) ist die öffentliche Citrix Files-App möglicherweise ungeeignet.
- Weitere Informationen finden Sie unter Apps und Citrix Files für Citrix Endpoint Management.

Sicherheit, Richtlinien und Zugriffssteuerung

Zu klärende 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 verwalten. Weitere Informationen finden Sie unter Mitarbeiterberechtigungen.
- Einige Citrix Files-Einstellungen zur Gerätesicherheit steuern dieselben Features wie MDX-Richtlinien. In diesen Fällen haben die Citrix Endpoint Management-Richtlinien Vorrang, gefolgt von den Citrix Files-Einstellungen. Beispiel: Wenn Sie externe Apps in Citrix Files deaktivieren, in Citrix Endpoint Management jedoch aktivieren, werden die externen Apps in Citrix Files deaktiviert. Sie können die Apps so konfigurieren, dass Citrix Endpoint Management keine(n) PIN/Passcode anfordert, die Citrix Files-App jedoch schon.

Standard-Speicherzonen oder eingeschränkte Speicherzonen

Zu klärende 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.

Zugriffssteuerung

Unternehmen können mobile Geräte innerhalb und außerhalb von Netzwerken verwalten. Enterprise Mobility Management-Lösungen wie Citrix Endpoint Management 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 Citrix Endpoint Management in Ihre NAC-Lösung hinein. Die NAC-Lösung kann dann anhand der Citrix Endpoint Management-Sicherheitsbewertung Authentifizierungsentscheidungen vereinfachen und bewältigen.

Sie können NAC-Richtlinien mit jeder der folgenden Lösungen durchsetzen:

- NetScaler Gateway
- ForeScout

Citrix übernimmt keine Gewährleistung für die Integration anderer NAC-Lösungen.

Vorteile einer NAC-Integration in Citrix Endpoint Management:

- 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 Citrix Endpoint Management.
  - Entscheidung über Zulassen, Blockieren, Einschränken oder Umleiten der Geräte auf der Basis der abgefragten Geräteinformationen. Die Entscheidung hängt von den von Ihnen festgelegten Sicherheitsrichtlinien ab.
- Eine NAC-Lösung bietet IT-Administratoren eine Übersicht über nicht verwaltete und nicht richtlinientreue Geräte.

Eine Beschreibung der von Citrix Endpoint Management unterstützten NAC-Richtlinientreuefilter und eine Konfigurationsübersicht finden Sie unter Netzwerkzugriffssteuerung (NAC).

Integration in NetScaler Gateway und Citrix ADC

June 25, 2024

Bei Integration in Citrix Endpoint Management bietet NetScaler Gateway für MAM-Geräte einen Authentifizierungsmechanismus für den Remotezugriff auf das interne Netzwerk. Durch die Integration können mobile Citrix Produktivitätsapps über ein Micro-VPN auf Unternehmensserver im Intranet zugreifen. Citrix Endpoint Management erstellt ein Micro-VPN von den Apps auf dem Gerät zu NetScaler Gateway. NetScaler Gateway bietet einen Micro-VPN-Pfad für den Zugriff auf alle Unternehmensressourcen und unterstützt eine starke Multifaktorauthentifizierung.

Wenn ein Benutzer die MDM-Registrierung abwählt, erfolgt die Geräteregistrierung per NetScaler Gateway-FQDN.

Citrix Cloud Operations verwaltet den Citrix ADC-Lastausgleich.

Designentscheidungen

Nachfolgend finden Sie eine Zusammenfassung der zahlreichen Design-Entscheidungen, die bei der Planung einer NetScaler Gateway-Integration in Citrix Endpoint Management getroffen werden müssen.

Zertifikate

Entscheidungsdetails:

- Benötigen Sie ein höheres Maß an Sicherheit für Registrierungen und den Zugriff auf die Citrix Endpoint Management-Umgebung?
- Ist LDAP keine Option?

Designhilfen:

Standardmäßig ist Citrix Endpoint Management für die Authentifizierung per Benutzernamen und Kennwort konfiguriert. Als zusätzliche Sicherheitsstufe für die Registrierung bei und den Zugriff auf die Citrix Endpoint Management-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 Citrix Endpoint Management eine Smartcard präsentieren. Die Benutzer registrieren sich in diesem Fall mit einer eindeutigen PIN, die von Citrix Endpoint Management generiert wird. Sobald ein Benutzer Zugriff hat, erstellt Citrix Endpoint Management das Zertifikat für die spätere Authentifizierung bei der Citrix Endpoint Management-Umgebung und stellt es bereit.

Citrix Endpoint Management unterstützt Zertifikatsperrlisten (CRL) nur für Drittanbieterzertifizierungsstellen. Wenn Sie eine Microsoft-Zertifizierungsstelle konfiguriert haben, wird in Citrix Endpoint Management zum Verwalten der Zertifikatsperre NetScaler Gateway verwendet. Bedenken Sie beim Konfigurieren der Clientzertifikatauthentifizierung, ob Sie die NetScaler Gateway-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. Citrix Endpoint Management stellt ein neues Zertifikat aus, da es Benutzer nicht daran hindert, ein Benutzerzertifikat zu generieren, falls eines gesperrt wurde. Diese Einstellung erhöht die Sicherheit von PKI-Entitäten, wenn über die Zertifikatsperrliste auf abgelaufene PKI-Entitäten geprüft wird.

Dedizierte oder gemeinsam genutzt NetScaler Gateway-VIPs

Entscheidungsdetails:

- Verwenden Sie zurzeit NetScaler Gateway für Citrix Virtual Apps and Desktops?
- Wird Citrix Endpoint Management dasselbe NetScaler Gateway wie Citrix Virtual Apps and Desktops nutzen?
- Welche Authentifizierungsanforderungen gelten für beide Datenströme?

Designhilfen:

Wenn Ihre Citrix Umgebung sowohl Citrix Endpoint Management als auch Virtual Apps and Desktops enthält, können Sie für beides denselben virtuellen NetScaler Gateway-Server verwenden. Aufgrund

möglicher Versionskonflikte und der Umgebungsisolierung wird für jede Citrix Endpoint Management-Umgebung ein dediziertes NetScaler Gateway empfohlen.

Wenn Sie die LDAP-Authentifizierung verwenden, ist eine Authentifizierung von Citrix Secure Hub bei demselben NetScaler Gateway problemlos möglich. Bei Verwendung der zertifikatbasierten Authentifizierung überträgt Citrix Endpoint Management ein Zertifikat in den MDX-Container und Citrix Secure Hub verwendet das Zertifikat zur Authentifizierung beim NetScaler Gateway.

Mit folgendem Workaround können Sie denselben FQDN für zwei NetScaler Gateway-VIPs verwenden: Sie können zwei NetScaler Gateway-VIPs mit derselben IP-Adresse erstellen. Die für Citrix Secure Hub verwendet dann den Standardport 443 und die für Citrix Virtual Apps and Desktops (= Citrix Workspace-App-Bereitstellung) den Port 444. Ein FQDN wird dann in die gleiche IP-Adresse aufgelöst. Für diesen Workaround müssen Sie ggf. StoreFront so konfigurieren, dass eine ICA-Datei für Port 444 anstelle des Standardports 443 zurückgegeben wird. Der Workaround erfordert keine Eingabe einer Portnummer durch die Benutzer.

NetScaler Gateway-Timeouts

Entscheidungsdetails:

- Wie möchten Sie die NetScaler Gateway-Timeouts für den Citrix Endpoint Management-Datenverkehr konfigurieren?

Designhilfen:

NetScaler Gateway enthält die Einstellungen "Session time-out"und "Forced time-out". Weitere Informationen finden Sie unter Empfohlene Konfigurationen. Beachten Sie, dass es für Hintergrunddienste, NetScaler Gateway und für den Offlinezugriff auf Anwendungen unterschiedliche Timeoutwerte gibt.

Registrierungs-FQDN

> **Wichtig:**
>
> Eine Änderung des Registrierungs-FQDN erfordert eine neue SQL Server-Datenbank und die Neuerstellung des Citrix Endpoint Management-Servers.

Citrix Secure Web-Datenverkehr

Entscheidungsdetails:

- Soll Citrix Secure Web auf das interne Webbrowsing beschränkt werden?
- Soll Citrix Secure Web für das interne und das externe Webbrowsing aktiviert werden?

Designhilfen:

Wenn Sie Citrix Secure Web nur für das interne Webbrowsing verwenden, bereitet das Konfigurieren von NetScaler Gateway keine Probleme. Wenn Citrix Secure Web jedoch nicht alle internen Sites standardmäßig erreichen kann, müssen Sie gegebenenfalls Firewalls und Proxyserver konfigurieren.

Wenn Sie Citrix 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 Citrix Secure Web-Verbindungen zu NetScaler Gateway zurückgehen und über einen Proxyserver in das Internet führen. Für den Zugriff auf Citrix Secure Web wird standardmäßig ein Tunnel zum internen Netzwerk verwendet. Citrix Secure Web verwendet pro Anwendung einen VPN-Tunnel zum internen Netzwerk für den gesamten Netzwerkzugriff zusammen mit NetScaler Gateway Split-Tunnel-Einstellungen verwendet.

Eine Beschreibung von Citrix Secure Web-Verbindungen finden Sie unter Konfigurieren von Benutzerverbindungen.

Pushbenachrichtigungen für Citrix Secure Mail

Entscheidungsdetails:

- Möchten Sie Pushbenachrichtigungen verwenden?

Designhilfe für iOS:

Wenn die NetScaler Gateway-Konfiguration Secure Ticket Authority (STA) umfasst und Split-Tunneling deaktiviert ist, muss NetScaler Gateway den Datenverkehr von Citrix Secure Mail zu den Citrix Listenerdienst-URLs zulassen. Diese URLs sind in den Pushbenachrichtigungen für Citrix Secure Mail für iOS festgelegt.

Designhilfe für Android:

Steuern Sie mit Firebase Cloud Messaging (FCM), wie und wann Android-Geräte eine Verbindung zu Citrix Endpoint Management herstellen. Wenn FCM konfiguriert ist, lösen Sicherheitsaktionen oder Bereitstellungsbefehle eine Pushbenachrichtigung an Citrix Secure Hub aus, sodass der Benutzer aufgefordert wird, erneut eine Verbindung mit dem Citrix Endpoint Management-Server herzustellen.

HDX-STAs

Entscheidungsdetails:

- Welche STAs sollte man bei Integration des Zugriffs auf HDX-Anwendungen verwenden?

Designhilfen:

HDX STAs müssen mit den STAs in StoreFront übereinstimmen und für die Virtual Apps and Desktops-Site gültig sein.

Citrix Files und ShareFile

Entscheidungsdetails:

- Möchten Sie einen Speicherzonencontroller in der Umgebung verwenden?
- Welche Citrix Files-VIP-URL möchten Sie verwenden?

Designhilfen:

Wenn die Umgebung Speicherzonencontroller enthält, müssen Sie Folgendes korrekt konfigurieren:

- Citrix Files Content 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 SAML für Citrix Files erforderlich ist, soll Citrix Endpoint Management als SAML-Identitätsanbieter verwendet werden?

Designhilfen:

Die empfohlene bewährte Methode ist die Integration von Citrix Files in Citrix Endpoint Management –eine einfachere Alternative zur Konfiguration eines SAML-basierten Verbunds. Citrix Endpoint Management bietet folgende Funktionen für Citrix Files:

- Authentifizierung per Single Sign-On (SSO) für mobile Citrix Produktivitätsappbenutzer.
- Active Directory-basiertes Benutzerkontoprovisioning.
- Umfassende Richtlinien zur Zugriffssteuerung.

Mit der Citrix Endpoint Management-Konsole können Sie Citrix Files konfigurieren sowie Servicelevel und Lizenznutzung überwachen.

Es gibt zwei Arten von Citrix Files-Clients: Citrix Files für Citrix Endpoint Management-Clients ("umschlossenes Citrix Files") und mobile Citrix Files-Clients ("nicht umschlossenes Citrix Files"). Die Unterschiede werden unter Unterschiede zwischen Citrix Files für Citrix Endpoint Management-Clients und mobilen Citrix Files-Clients erläutert.

Sie können Citrix Endpoint Management und Citrix Files so konfigurieren, dass Sie mit SAML per SSO auf Folgendes zugreifen können:

- 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

Wenn Sie Citrix Endpoint Management als SAML-Identitätsanbieter für Citrix Files verwenden möchten, stellen Sie sicher, dass die richtigen Konfigurationen vorhanden sind. Weitere Informationen finden Sie unter SAML für SSO bei Citrix Files.

Direkte ShareConnect-Verbindungen

Entscheidungsdetails:

- Sollen Benutzer von einem Computer oder Mobilgerät mit ShareConnect direkt auf einen Hostcomputer zugreifen?

Designhilfen:

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 Citrix Endpoint Management über NetScaler Gateway sicheren Benutzerzugriff auf Ressourcen außerhalb des lokalen Netzwerks. Informationen zur Konfiguration finden Sie unter ShareConnect.

Registrierungs-FQDN für jeden Verwaltungsmodus

Verwaltungsmodus	Registrierungs-FQDN
MDM+MAM mit verbindlicher MDM-Registrierung	Citrix Endpoint Management-Server-FQDN
MDM+MAM mit optionaler MDM-Registrierung	Citrix Endpoint Management-Server-FQDN oder NetScaler Gateway-FQDN
Nur MAM	Citrix Endpoint Management-Server-FQDN
Nur-MAM (Legacy)	NetScaler Gateway-FQDN

Zusammenfassung der Bereitstellung

Wenn Sie mehrere Citrix Endpoint Management-Instanzen haben (z. B. für die Test-, die Entwicklungs- und die Produktionsumgebung), müssen Sie NetScaler Gateway für die zusätzlichen Umgebungen manuell konfigurieren. Notieren Sie sich bei einer funktionierenden Umgebung die Einstellungen, bevor Sie NetScaler Gateway manuell für Citrix Endpoint Management konfigurieren.

Eine wichtige Entscheidung ist die Wahl zwischen HTTPS und HTTP für die Kommunikation mit dem Citrix Endpoint Management-Server. HTTPS bietet eine sichere Back-End-Kommunikation, da der Datenverkehr zwischen NetScaler Gateway und Citrix Endpoint Management verschlüsselt wird. Die erneute Verschlüsselung hat allerdings Auswirkungen auf die Leistung des Citrix Endpoint Management-Servers. HTTP bietet die bessere Citrix Endpoint Management-Serverleistung. Der Datenverkehr zwischen NetScaler Gateway und Citrix Endpoint Management wird jedoch nicht verschlüsselt. Die folgenden Tabellen enthalten die erforderlichen HTTP- und HTTPS-Ports für NetScaler Gateway und Citrix Endpoint Management.

HTTPS

Citrix empfiehlt normalerweise die Verwendung einer SSL-Brücke für NetScaler Gateway in Konfigurationen mit virtuellem MDM-Server. Bei Verwendung von SSL-Offload für NetScaler Gateway mit virtuellen MDM-Servern unterstützt Citrix Endpoint Management nur Port 80 als Back-End-Dienst.

Verwaltungsmodus	NetScaler Gateway-Lastausgleichsmethode	SSL-Neuverschlüsselung	Citrix Endpoint Management-Serverport
MAM	SSL-Offload	Aktiviert	8443
MDM+MAM	MDM: SSL-Brücke	–	443, 8443
MDM+MAM	MAM: SSL-Offload	Aktiviert	8443

HTTP

Verwaltungsmodus	NetScaler Gateway-Lastausgleichsmethode	SSL-Neuverschlüsselung	Citrix Endpoint Management-Serverport
MAM	SSL-Offload	Aktiviert	8443
MDM+MAM	MDM: SSL-Offload	Nicht unterstützt	80
MDM+MAM	MAM: SSL-Offload	Aktiviert	8443

Diagramme von NetScaler Gateway in Citrix Endpoint Management-Bereitstellungen finden Sie unter Architektur.

SSO- und Proxy-Überlegungen für MDX-Apps

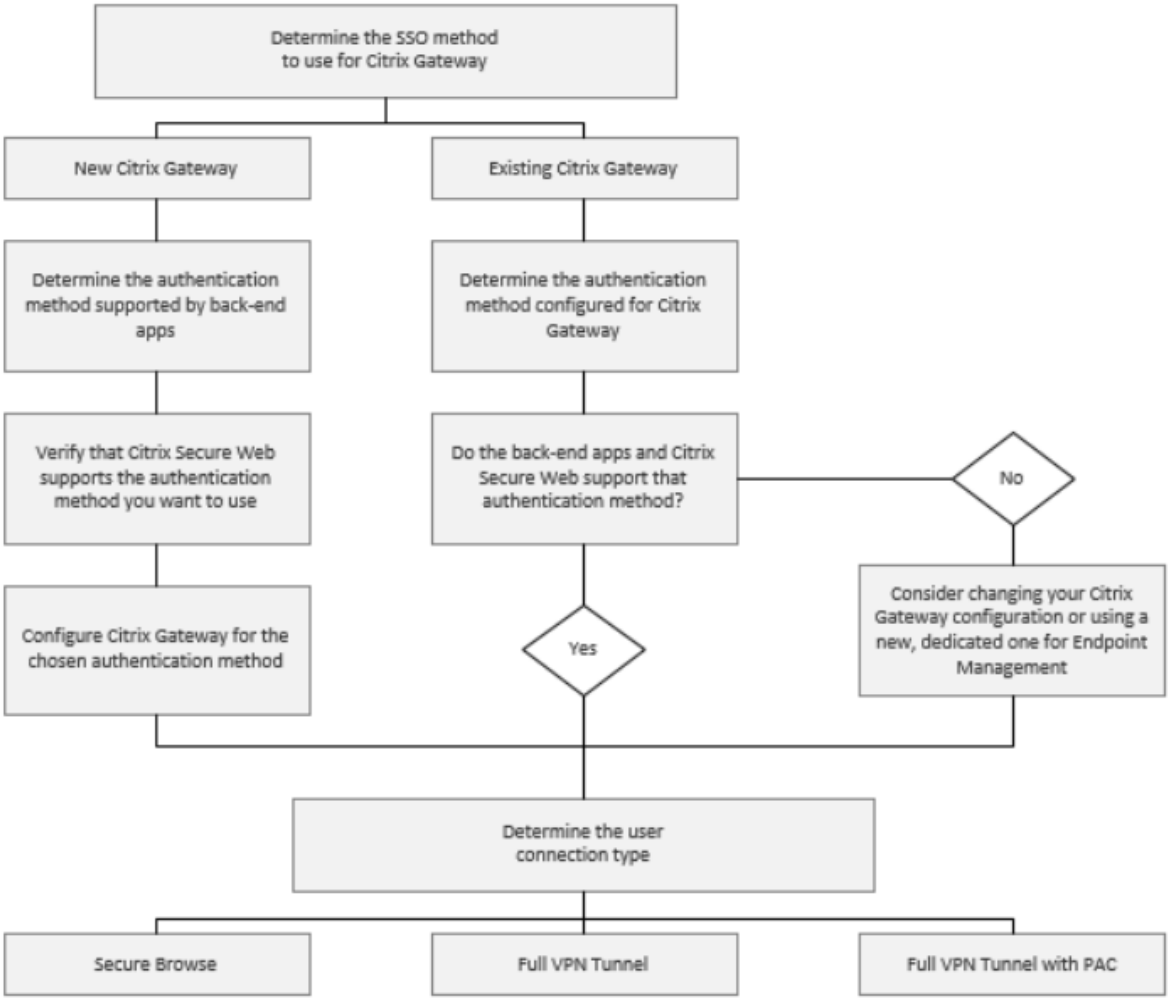
March 11, 2024

Durch die Citrix Endpoint Management-Integration in NetScaler Gateway können Sie Benutzern Single Sign-On (SSO) für alle HTTP- und HTTPS-Ressourcen im Back-End bereitstellen. Je nach SSO-Authentifizierungsanforderungen können Sie für MDX-Apps festlegen, dass Benutzer sich über Secure Browse (Tunnel - Web-SSO), eine Art clientloses VPN, verbinden.

> **Wichtig:**
>
> Unterstützung für einen vollständigen VPN-Tunnel und eine PAC-Datei (Proxy Automatic Configuration) mit einem vollständigen VPN-Tunnel für iOS- und Android-Geräte wurde von Citrix eingestellt. Weitere Informationen finden Sie unter Einstellung von Features und Plattformen.

Bietet NetScaler Gateway 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 Citrix Secure Web liegt. Die Konzepte gelten für weitere MDX-Apps.

Das folgende Flussdiagramm stellt die Entscheidungsfindung bei der Wahl der SSO- und Benutzerverbindungen zusammen.



NetScaler Gateway-Authentifizierungsmethoden

Dieser Abschnitt enthält allgemeine Informationen zu den von NetScaler Gateway unterstützten Authentifizierungsmethoden.

SAML-Authentifizierung

Wenn Sie NetScaler Gateway für Security Assertion Markup Language (SAML) konfigurieren, können die Benutzer eine Verbindung mit Web-Apps herstellen, die SAML für Single Sign-On unterstützen. NetScaler Gateway unterstützt Single Sign-On per Identitätsanbieter (IdP) für SAML-Web-Apps.

Erforderliche Konfiguration:

- Konfigurieren von SAML-SSO im NetScaler Gateway-Traffic-Profil.
- Konfigurieren des SAML-IdP für den angeforderten Dienst.

NTLM-Authentifizierung

Wenn SSO bei Web-Apps im Sitzungsprofil aktiviert ist, führt NetScaler Gateway die NTLM-Authentifizierung automatisch durch.

Erforderliche Konfiguration:

- Aktivieren von SSO im NetScaler Gateway-Session- oder Traffic-Profil.

Kerberos-Identitätswechsel

Citrix Endpoint Management unterstützt Kerberos nur für Citrix Secure Web. Wenn Sie NetScaler Gateway für Kerberos-SSO konfigurieren, verwendet NetScaler Gateway einen Identitätswechsel, wenn ein Benutzerkennwort für NetScaler Gateway verfügbar ist. Das bedeutet, dass NetScaler Gateway die Benutzeranmeldeinformationen verwendet, um das für den Zugriff auf Dienste wie Citrix Secure Web erforderliche Ticket zu erhalten.

Erforderliche Konfiguration:

- Konfigurieren der NetScaler Gateway-Sitzungsrichtlinie `Worx`, sodass sie den Kerberos-Bereich der Verbindung identifizieren kann.
- Konfigurieren eines Kontos zur eingeschränkten Kerberos-Delegierung auf NetScaler Gateway. Konfigurieren Sie dieses Konto ohne Kennwort und binden Sie es an eine Trafficrichtlinie im Citrix Endpoint Management-Gateway.
- Einzelheiten zu dieser und weiteren Konfigurationen finden Sie im Citrix Blog unter WorxWeb and Kerberos Impersonation SSO.

Eingeschränkte Kerberos-Delegierung

Citrix Endpoint Management unterstützt Kerberos nur für Citrix Secure Web. Wenn Sie NetScaler Gateway für Kerberos-SSO konfigurieren, verwendet NetScaler Gateway die eingeschränkte Delegierung, wenn kein Benutzerkennwort für NetScaler Gateway verfügbar ist.

Bei der eingeschränkten Delegierung verwendet NetScaler Gateway 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 NetScaler Gateway.
- Aktivieren Sie SSO im NetScaler Gateway-Traffic-Profil.
- Konfigurieren Sie die Backend-Website für die Kerberos-Authentifizierung.

Formularbasierte Authentifizierung

Wenn Sie NetScaler Gateway 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 der Modus "Tunnel - Web-SSO"verwendet wird.

Erforderliche Konfiguration:

- Konfigurieren von formularbasiertem SSO im NetScaler Gateway Traffic-Profil.

Digest-HTTP-Authentifizierung

Wenn SSO bei Web-Apps im Sitzungsprofil aktiviert ist, führt NetScaler Gateway die Digest-HTTP-Authentifizierung automatisch durch. Diese Authentifizierungsmethode gilt für Apps, für die der Modus "Tunnel - Web-SSO"verwendet wird.

Erforderliche Konfiguration:

- Aktivieren von SSO im NetScaler Gateway-Session- oder Traffic-Profil.

Einfache HTTP-Authentifizierung

Wenn SSO bei Web-Apps im Sitzungsprofil aktiviert ist, führt NetScaler Gateway die einfache HTTP-Authentifizierung automatisch durch. Diese Authentifizierungsmethode gilt für Apps, für die der Modus "Tunnel - Web-SSO"verwendet wird.

Erforderliche Konfiguration:

- Aktivieren von SSO im NetScaler Gateway-Session- oder Traffic-Profil.

“Tunnel - Web-SSO”für Secure Web

Im folgenden Abschnitt wird die Benutzerverbindungsart **Tunnel - Web-SSO** für Citrix Secure Web beschrieben.

Verbindungen, die einen Tunnel zum internen Netzwerk benötigen, können “Tunnel - Web-SSO”verwenden, eine Variante eines clientlosen VPNs. “Tunnel - Web-SSO”ist die Standardkonfiguration für die Citrix Secure Web-Richtlinie **Bevorzugter VPN-Modus**. Citrix empfiehlt die Einstellung Tunnel - Web-SSO für Verbindungen, die Single Sign-On (SSO) erfordern.

Bei Verwendung von “Tunnel - Web-SSO”unterteilt NetScaler Gateway die HTTPS-Sitzung in zwei Teile:

- Client zu NetScaler Gateway
- NetScaler Gateway zum Backend-Ressourcenserver.

Auf diese Weise genießt NetScaler Gateway volle Transparenz in allen Transaktionen zwischen dem Client und dem Server und kann SSO bereitstellen.

Sie können auch Proxyserver für Citrix Secure Web konfigurieren, wenn “Tunnel - Web-SSO”aktiviert ist. Weitere Informationen finden Sie in dem Blog Citrix Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

> **Hinweis:**
>
> Citrix hat bekanntgegeben, dass der Modus “Vollständiger VPN-Tunnel mit PAC”nicht mehr zur Verfügung steht. Siehe Auslaufende Features.

Citrix Endpoint Management unterstützt die von NetScaler Gateway 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. Citrix Secure Web analysiert die Regeln in der PAC-Datei und sendet die Proxyserverinformationen an NetScaler Gateway. NetScaler Gateway sieht weder PAC-Datei noch Proxyserver.

Für die Authentifizierung bei HTTPS-Websites ermöglicht die Citrix Secure Web-MDX-Richtlinie **Webkennwortcaching aktivieren**, dass Citrix Secure Web Authentifizierungen durchführen und Single Sign-On beim Proxyserver über MDX bereitstellen kann.

NetScaler Gateway Split-Tunneling

Bei der Planung der SSO- und Proxykonfiguration müssen Sie auch überlegen, ob Sie NetScaler Gateway Split-Tunneling verwenden möchten. Citrix empfiehlt, NetScaler Gateway Split-Tunneling nur zu verwenden, wenn es erforderlich ist. In diesem Abschnitt finden Sie einen Überblick über die Funktionsweise von Split-Tunneling: NetScaler Gateway ermittelt den Datenverkehrspfad anhand seiner

Routingtabelle. Wenn NetScaler Gateway Split-Tunneling aktiviert ist, unterscheidet Citrix Secure Hub internen (geschützten) Netzwerkverkehr und Internetverkehr. Citrix Secure Hub unterscheidet anhand des DNS-Suffixes und der Intranetanwendungen. Citrix Secure Hub leitet dann nur den internen Datenverkehr durch den VPN-Tunnel. Ist das NetScaler Gateway Split-Tunneling deaktiviert, wird der gesamte Datenverkehr durch den VPN-Tunnel geleitet.

Wenn Sie aus Sicherheitsgründen den gesamten Datenverkehr überwachen möchten, deaktivieren Sie Split-Tunneling in NetScaler Gateway. Der gesamte Datenverkehr fließt dann durch den VPN-Tunnel.

NetScaler Gateway bietet auch Modus mit umgekehrtem Split-Tunnel und Micro-VPN. In diesem Modus kann eine Ausschlussliste mit IP-Adressen verwendet werden, die nicht an NetScaler Gateway getunnelt werden. Stattdessen wird die Internetverbindung des Geräts verwendet. Weitere Informationen über Reverse-Split-Tunneling finden Sie in der NetScaler Gateway-Dokumentation.

Citrix Endpoint Management bietet eine **Ausschlussliste für Reverse-Split-Tunneling**. Wenn bestimmte Websites keinen Tunnel durch NetScaler 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 Modus “Tunnel - Web-SSO”verwendet, wenn NetScaler Gateway für Reverse-Split-Tunneling konfiguriert ist.

Authentifizierung

March 11, 2024

In einer Citrix Endpoint Management-Bereitstellung sind bei der Konfiguration der Authentifizierung verschiedene Faktoren zu berücksichtigen. In diesem Abschnitt werden diverse Faktoren beschrieben, die sich auf die Authentifizierung auswirken:

- Die wichtigsten MDX-Richtlinien, Citrix Endpoint Management-Clienteigenschaften und NetScaler 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. Sehen Sie sich die drei empfohlenen Konfigurationen an, um das Zusammenspiel der verschiedenen Authentifizierungsoptionen zu verstehen.

Authentifizierungsmodi

Onlineauthentifizierung: Ermöglicht Benutzern den Zugriff auf das Citrix Endpoint Management-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 Citrix Endpoint Management eine Verbindung mit einem oder mehreren LDAP-kompatiblen Verzeichnissen herstellen. Dies ist eine häufig verwendete Methode, um in Unternehmensumgebungen einen Single Sign-On (SSO) mit einmaliger Anmeldung bereitzustellen. Um die Benutzererfahrung zu optimieren, können Sie die Citrix-PIN mit Active Directory-Kennwortzwischenspeicherung verwenden. Gleichzeitig können Sie durch komplexe Kennwörter bei Registrierung, Kennwortablauf und Kontosperrung die Sicherheit gewährleisten.

Weitere Details finden Sie unter Authentifizierung mit Domäne bzw. mit Domäne und Sicherheitstoken.

Clientzertifikat: Citrix Endpoint Management ermöglicht die Integration mit branchenüblichen Zertifizierungsstellen zur Verwendung von Zertifikaten als einzige Methode für eine Online-Authentifizierung. Citrix Endpoint Management 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.

Citrix Endpoint Management unterstützt Zertifikatsperrlisten (CRL) nur für Drittanbieterzertifizierungsstellen. Wenn Sie eine Microsoft-Zertifizierungsstelle konfiguriert haben, wird in Citrix Endpoint Management zum Verwalten der Zertifikatsperre NetScaler Gateway verwendet. Bedenken Sie beim Konfigurieren der Clientzertifikatauthentifizierung, ob Sie die NetScaler Gateway-Einstellung für Zertifikatsperrlisten (CRL) Enable CRL Auto Refresh konfigurieren müssen. Dadurch wird sichergestellt, dass Benutzer von nur in MAM registrierten Geräten sich nicht mit einem existierenden Zertifikat auf dem Gerät authentifizieren können. Citrix Endpoint Management stellt ein neues Zertifikat aus, da es Benutzer nicht daran hindert, ein Benutzerzertifikat zu generieren, falls eines gesperrt wurde. Diese Einstellung erhöht die Sicherheit von PKI-Entitäten, wenn über die Zertifikatsperrliste auf abgelaufene PKI-Entitäten geprüft wird.

Bereitstellungsdiagramme für eine zertifikatbasierte Authentifizierung oder die Ausstellung von Gerätezertifikaten über die Zertifizierungsstelle (ZS) Ihres Unternehmens finden Sie unter Architektur.

Zweistufige Authentifizierung LDAP + Clientzertifikat: Diese Konfiguration bietet die beste Kombination aus Sicherheit und Benutzererfahrung für Citrix Endpoint Management. Eine Authentifizierung mit LDAP und Clientzertifikat bietet folgende Vorteile:

- Beste Möglichkeiten für Single Sign-On, und hohe Sicherheit durch zweistufige Authentifizierung bei NetScaler Gateway.
- Sicherheit wird durch etwas, das Benutzer wissen (ihr Active Directory-Kennwort) und etwas, das sie haben (Clientzertifikate auf ihrem Gerät) gewährleistet.

Citrix Secure Mail bietet mit der Clientzertifikatauthentifizierung eine automatische Konfiguration und intuitive Benutzererfahrung für Erstbenutzer. Für dieses Feature ist eine Umgebung mit ordnungsgemäß konfiguriertem Exchange-Clientzugriffsserver erforderlich.

Die optimale Benutzerfreundlichkeit erreichen Sie, wenn Sie die Authentifizierung per LDAP und Clientzertifikat mit der Citrix-PIN und 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 Citrix Endpoint Management-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.

Micro-VPN-Sitzung 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 Citrix Endpoint Management neu bestätigt werden müssen. Eine iOS-App ruft automatisch neue Richtlinien für MDX-Apps von Citrix Endpoint Management ab, wenn die folgenden Bedingungen erfüllt sind:

- Sie definieren eine maximale Offlinezeit und
- Citrix Secure Hub für iOS besitzt einen gültigen NetScaler Gateway-Token.

Wenn Citrix Secure Hub keinen gültigen NetScaler Gateway-Token hat, müssen Benutzer sich über Citrix Secure Hub authentifizieren, bevor App-Richtlinien aktualisiert werden können. Der NetScaler Gateway-Token kann durch NetScaler Gateway-Sitzungsinaktivität oder eine erzwungene Sitzungstimeoutrichtlinie ungültig werden. Benutzer können die App jedoch weiter verwenden, wenn sie sich wieder bei Citrix 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 könnte.

Ticketablauf für Hintergrunddienste: die Zeitspanne, die ein Netzwerkdienstticket im Hintergrund gültig bleibt. Wenn Citrix Secure Mail sich über NetScaler Gateway mit einem Exchange Server verbindet, auf dem ActiveSync ausgeführt wird, gibt Citrix Endpoint Management einen Token aus. Mit diesem Token stellt Citrix Secure Mail dann eine Verbindung zum internen Exchange Server her. Diese Eigenschaft bestimmt, wie lange Citrix 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 für erforderliche Micro-VPN-Sitzung: Legt fest, wie viele Minuten ein Benutzer die App offline verwenden kann, 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: Citrix Endpoint Management MDX-Richtlinien für iOS und Citrix Endpoint Management MDX-Richtlinien für Android.

Citrix Endpoint Management-Clienteigenschaften

> **Hinweis:**
>
> Clienteigenschaften sind globale Einstellungen und gelten für alle Geräte, die mit Citrix Endpoint Management 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 Citrix Endpoint Management-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 Citrix Endpoint Management 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 Citrix 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

NetScaler Gateway-Einstellungen

Session time-out: Wenn Sie diese Einstellung aktivieren, wird die Sitzung getrennt, wenn NetScaler Gateway im angegebenen Zeitraum keine Netzwerkaktivität erkennt. Die Einstellung wird für Benutzer durchgesetzt, die eine Verbindung mit dem NetScaler Gateway Plug-in, Citrix 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 NetScaler 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 NetScaler Gateway Plug-in, Citrix Secure Hub oder über einen Webbrowser herstellen. Bei Verwendung der Secure Ticket Authoritiy (STA), einem speziellen NetScaler Gateway-Modus in Citrix Secure Mail, wird diese Einstellung nicht auf Citrix Secure Mail-Sitzungen angewendet. Standardmäßig ist kein Wert angegeben, sodass Sitzungen bei Aktivität verlängert werden.

Weitere Informationen zu den Timeouteinstellungen für NetScaler Gateway finden Sie in der NetScaler Gateway-Dokumentation.

Weitere Informationen zu den Szenarios, bei denen Benutzer zur Authentifizierung bei Citrix Endpoint Management 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
- Citrix Endpoint Management-Konsole

Einstellung	Ort der Einstellung	Standardeinstellung
Session time-out	NetScaler Gateway	1440 Minuten
Forced time-out	NetScaler Gateway	Kein Wert (aus)
Maximale Offlinezeit	MDX-Richtlinien	72 Stunden
Ticketablauf für Hintergrunddienste	MDX-Richtlinien	168 Stunden (7 Tage)
Micro-VPN-Sitzung erforderlich	MDX-Richtlinien	Aus
Kulanzzeitraum für erforderliche Micro-VPN-Sitzung	MDX-Richtlinien	0
App-Passcode	MDX-Richtlinien	Ein
Encrypt secrets using passcode	Citrix Endpoint Management-Clienteigenschaften	false

Einstellung	Ort der Einstellung	Standardeinstellung
Enable Citrix-PIN Authentication	Citrix Endpoint Management-Clienteigenschaften	false
PIN Strength Requirement	Citrix Endpoint Management-Clienteigenschaften	Medium
PIN-Typ	Citrix Endpoint Management-Clienteigenschaften	Numerisch
Enable User Password Caching	Citrix Endpoint Management-Clienteigenschaften	false
Inactivity Timer	Citrix Endpoint Management-Clienteigenschaften	15
Enable Touch ID Authentication	Citrix Endpoint Management-Clienteigenschaften	false

Empfohlene Konfigurationen

Der folgende Abschnitt enthält Beispiele für drei Citrix Endpoint Management-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. Wenn Sie diese Einstellungen ändern, müssen möglicherweise auch andere Einstellungen angepasst werden. Beispielsweise darf die maximale Offlinezeit nicht höher 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	NetScaler Gateway	1440	Benutzer geben ihre Anmeldeinformationen in Citrix Secure Hub nur bei erforderlicher Onlineauthentifizierung ein –alle 24 Stunden.
Forced time-out	NetScaler Gateway	Kein Wert	Sitzungen werden bei Aktivität verlängert.
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 NetScaler Gateway. In Citrix Secure Mail verhindert ein STA-Timeout, das länger ist als das Sitzungstimeout, dass E-Mail-Benachrichtigungen beendet werden. Benutzer erhalten in diesem Fall von Citrix Secure Mail keine Aufforderung, wenn sie die App nicht vor Sitzungsablauf öffnen.
Micro-VPN-Sitzung erforderlich	MDX-Richtlinien	Aus	Gewährleistet eine gültige Netzwerkverbindung und NetScaler Gateway-Sitzung zur Verwendung von Apps.

Kulanzzeitraum für erforderliche Micro-VPN-Sitzung	MDX-Richtlinien	0	Kein Kulanzzeitraum (bei aktivierter Option “Micro-VPN-Sitzung erforderlich”).
App-Passcode	MDX-Richtlinien	Ein	Passcode für Anwendung erforderlich.
Encrypt secrets using passcode	Citrix Endpoint Management-Clienteigenschaften	true	Tresor wird durch einen von der Benutzerentropie abgeleiteten Schlüssel geschützt.
Enable Citrix-PIN Authentication	Citrix Endpoint Management-Clienteigenschaften	true	Citrix-PIN zur vereinfachten Benutzerauthen-tifizierung aktivieren.
PIN Strength Requirement	Citrix Endpoint Management-Clienteigenschaften	Gut	Hohe Anforderungen an die Kennwortkomplexität.
PIN-Typ	Citrix Endpoint Management-Clienteigenschaften	Alphanumerisch	PIN ist eine alphanumerische Sequenz.
Enable Password Caching	Citrix Endpoint Management-Clienteigenschaften	false	Das Active Directory-Kennwort wird nicht zwischengespeichert, und die Citrix-PIN wird für Offlineauthen-tifizierungen verwendet.

Inactivity Timer	Citrix Endpoint Management-Clienteigenschaften	15	Aufforderung zur Offlineauthentifizierung anzeigen, wenn ein Benutzer keine MDX-Apps oder Citrix Secure Hub im festgelegten Zeitraum verwendet.
Enable Touch ID Authentication	Citrix Endpoint Management-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 zu mehr Datensicherheit führt, wenn Geräte nicht verwendet werden.

Einstellung	Ort der Einstellung	Empfohlene Einstellung	Auswirkungen
Session time-out	NetScaler Gateway	4320	Benutzer geben ihre Anmeldeinformationen in Citrix Secure Hub nur bei erforderlicher Onlineauthentifizierung ein –alle 3 Tage.
Forced time-out	NetScaler 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 NetScaler Gateway. In Citrix Secure Mail verhindert ein STA-Timeout, das länger ist als das Sitzungstimeout, dass E-Mail-Benachrichtigungen unaufgefordert beendet werden.
Micro-VPN-Sitzung erforderlich	MDX-Richtlinien	Aus	Gewährleistet eine gültige Netzwerkverbindung und NetScaler Gateway-Sitzung zur Verwendung von Apps.
Kulanzzeitraum für erforderliche Micro-VPN-Sitzung	MDX-Richtlinien	0	Kein Kulanzzeitraum (bei aktivierter Option “Micro-VPN-Sitzung erforderlich”).
App-Passcode	MDX-Richtlinien	Ein	Passcode für Anwendung erforderlich.
Encrypt secrets using passcode	Citrix Endpoint Management-Clienteigenschaften	false	Keine Benutzerentropie zum Verschlüsseln des Tresors erforderlich.

Enable Citrix-PIN Authentication	Citrix Endpoint Management-Clienteigenschaften	true	Citrix-PIN zur vereinfachten Benutzerauthentifizierung aktivieren.
PIN Strength Requirement	Citrix Endpoint Management-Clienteigenschaften	Medium	Erzwingt Kennwörter mittlerer Komplexität.
PIN-Typ	Citrix Endpoint Management-Clienteigenschaften	Numerisch	Eine PIN ist eine numerische Sequenz.
Enable Password Caching	Citrix Endpoint Management-Clienteigenschaften	true	Die Benutzer-PIN speichert und schützt das Active Directory-Kennwort.
Inactivity Timer	Citrix Endpoint Management-Clienteigenschaften	30	Aufforderung zur Offlineauthentifizierung anzeigen, wenn ein Benutzer keine MDX-Apps oder Citrix Secure Hub im festgelegten Zeitraum verwendet.
Enable Touch ID Authentication	Citrix Endpoint Management-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	NetScaler Gateway	10080	Benutzer geben ihre Anmeldeinformationen in Citrix Secure Hub nur bei erforderlicher Onlineauthentifizierung ein –alle 7 Tage.
Forced time-out	NetScaler 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 NetScaler Gateway. In Citrix Secure Mail verhindert ein STA-Timeout, das länger ist als das Sitzungstimeout, dass E-Mail-Benachrichtigungen beendet werden. Benutzer erhalten in diesem Fall von Citrix Secure Mail keine Aufforderung, wenn sie die App nicht vor Sitzungsablauf öffnen.

Micro-VPN-Sitzung erforderlich	MDX-Richtlinien	Aus	Gewährleistet eine gültige Netzwerkverbindung und NetScaler Gateway-Sitzung zur Verwendung von Apps.
Kulanzzeitraum für erforderliche Micro-VPN-Sitzung	MDX-Richtlinien	0	Kein Kulanzzeitraum (bei aktivierter Option "Micro-VPN-Sitzung erforderlich").
App-Passcode	MDX-Richtlinien	Ein	Passcode für Anwendung erforderlich.
Encrypt secrets using passcode	Citrix Endpoint Management-Clienteigenschaften	false	Keine Benutzerentropie zum Verschlüsseln des Tresors erforderlich.
Enable Citrix-PIN Authentication	Citrix Endpoint Management-Clienteigenschaften	true	Citrix-PIN zur vereinfachten Benutzerauthentifizierung aktivieren.
PIN Strength Requirement	Citrix Endpoint Management-Clienteigenschaften	Niedrig	Keine Anforderungen an die Kennwortkomplexität.
PIN-Typ	Citrix Endpoint Management-Clienteigenschaften	Numerisch	Eine PIN ist eine numerische Sequenz.
Enable Password Caching	Citrix Endpoint Management-Clienteigenschaften	true	Die Benutzer-PIN speichert und schützt das Active Directory-Kennwort.

Inactivity Timer	Citrix Endpoint Management-Clienteigenschaften	90	Aufforderung zur Offlineauthentifizierung anzeigen, wenn ein Benutzer keine MDX-Apps oder Citrix Secure Hub im festgelegten Zeitraum verwendet.
Enable Touch ID Authentication	Citrix Endpoint Management-Clienteigenschaften	true	Aktiviert Touch ID für Anwendungsfälle mit Offlineauthentifizierung in iOS.

Verwenden der verstärkten Authentifizierung

Einige Apps erfordern möglicherweise eine erweiterte Authentifizierung. Dies können ein sekundärer Authentifizierungsfaktor (z. B. ein Token) oder aggressive Sitzungstimeout ein. Sie können diese Authentifizierungsmethode über eine MDX-Richtlinie steuern. Dieses Verfahren erfordert einen eigenen virtuellen Server (auf demselben oder einem separaten NetScaler Gateway-Gerät) zur Steuerung der Authentifizierungsmethoden.

Einstellung	Ort der Einstellung	Empfohlene Einstellung	Auswirkungen
Alternatives NetScaler Gateway	MDX-Richtlinien	Erfordert den FQDN und Port des sekundären NetScaler Gateway-Geräts.	Ermöglicht eine erweiterte Authentifizierung, die durch die Authentifizierungs- und Sitzungsrichtlinien des sekundären NetScaler Gateway-Geräts gesteuert wird.

Öffnet ein Benutzer eine App, die das alternative NetScaler Gateway verwendet, verwenden auch alle übrigen Apps diese NetScaler Gateway-Instanz zur Kommunikation mit dem internen Netzwerk. Die

Sitzung wechselt nur dann zurück zur NetScaler Gateway-Instanz mit geringerer Sicherheit, wenn bei der NetScaler Gateway-Instanz mit erhöhter Sicherheit ein Sitzungstimeout auftritt.

Verwendung von "Micro-VPN-Sitzung erforderlich"

Für bestimmte Anwendungen wie Citrix Secure Web können Sie sicherstellen, dass Benutzer eine App nur dann ausführen, wenn sie eine authentifizierte Sitzung verwenden. Diese Richtlinie erzwingt diese Option und ermöglicht einen Kulanzzeitraum, damit Benutzer ihre Arbeit beenden können.

Einstellung	Ort der Einstellung	Empfohlene Einstellung	Auswirkungen
Micro-VPN-Sitzung erforderlich	MDX-Richtlinien	Ein	Gewährleistet, dass ein Gerät online ist und einen gültigen Authentifizierungstoken hat.
Kulanzzeitraum für erforderliche Micro-VPN-Sitzung	MDX-Richtlinien	15	Gewährt einen Kulanzzeitraum von 15 Minuten, bevor der Benutzer die Apps nicht mehr verwenden kann.

Servereigenschaften

March 11, 2024

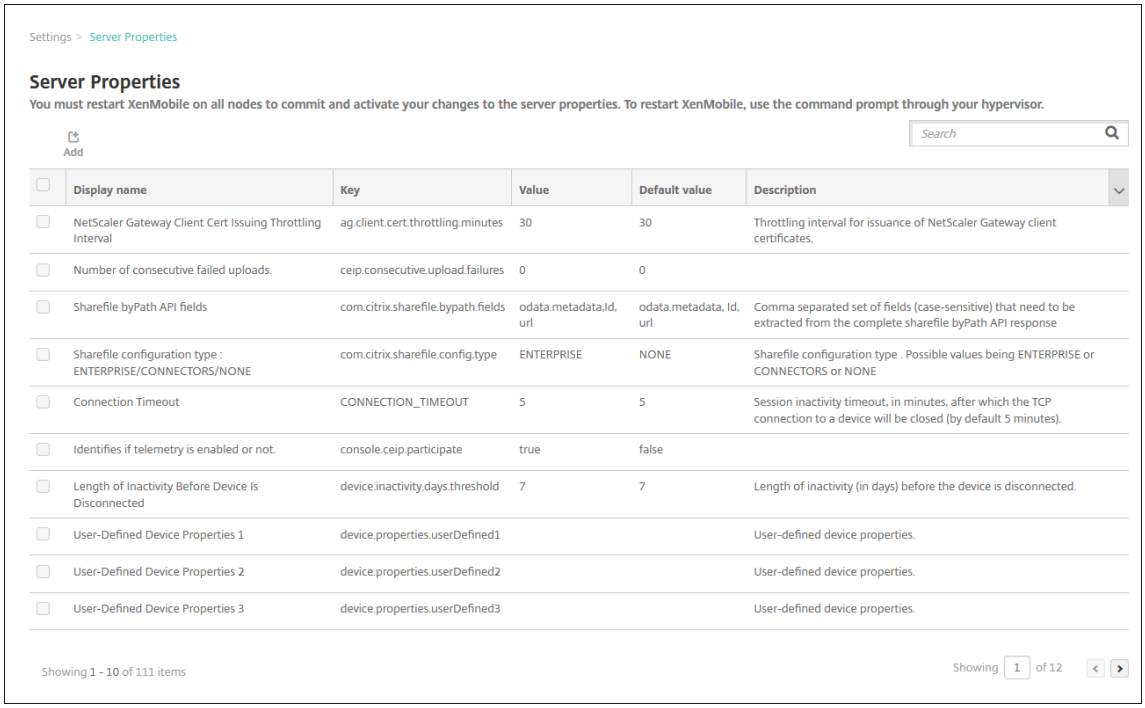
Servereigenschaften sind global und gelten für alle Vorgänge, Benutzer und Geräte einer Citrix Endpoint Management-Instanz. Citrix empfiehlt, die in diesem Artikel behandelten Servereigenschaften für Ihre Umgebung zu bewerten. Setzen Sie sich mit Citrix in Verbindung, bevor Sie andere Servereigenschaften ändern.

Um die Servereigenschaften zu aktualisieren, gehen Sie zu **Einstellungen > Servereigenschaften**.

Servereigenschaften hinzufügen, bearbeiten oder löschen

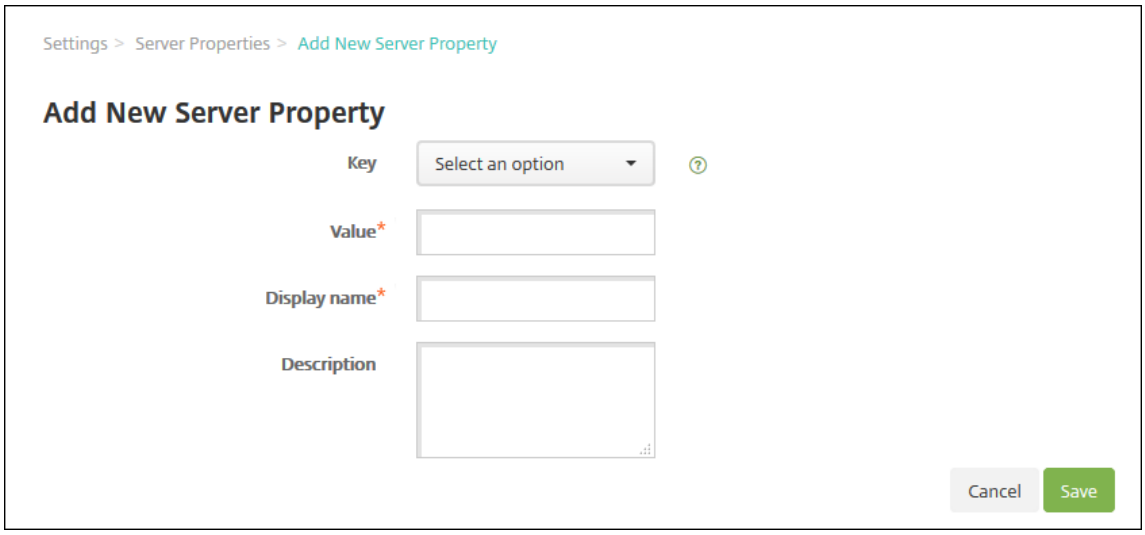
In Citrix Endpoint Management können Sie Eigenschaften auf den Server anwenden.

1. Klicken Sie in der Citrix Endpoint Management-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.



Servereigenschaften hinzufügen

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.

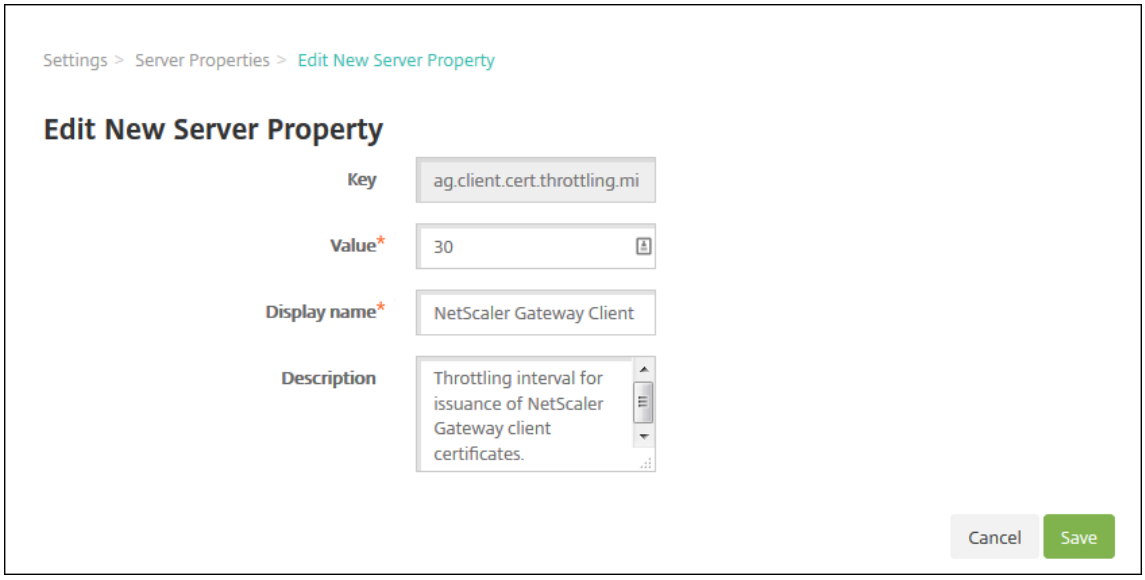
3. Klicken Sie auf **Speichern**.

Servereigenschaften bearbeiten

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 **Bearbeiten**. Die Seite **Neue Servereigenschaft bearbeiten** wird angezeigt.



3. Ändern Sie nach Bedarf die folgenden Informationen:

   - Schlüssel: Sie können dieses Feld nicht ändern.
   - Wert: Wert der 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.

Servereigenschaften löschen

1. Wählen Sie in der Tabelle **Servereigenschaften** die zu löschenden Servereigenschaften aus.
2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf **Delete**.

Servereigenschaften –Definitionen

Zugriff auf alle Apps im verwalteten Google Play Store

- Wenn **Wahr**, macht Citrix Endpoint Management alle Apps aus dem öffentlichen Google Play Store über den verwalteten Google Play Store zugänglich. Mit der Einschränkungsrichtlinie können Sie den Zugriff auf diese Apps steuern. Der Standardwert ist **Falsch**.

Gerät immer hinzufügen

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

AG Clientzertifikatausstellung - Drosselungsintervall

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

Ermöglicht das Entfernen von Geräten, die für einen bestimmten Zeitraum als inaktiv markiert wurden

- Wenn **Wahr**, werden Geräte, die für eine bestimmte Zeit (in Tagen) inaktiv waren, entfernt und aus Citrix Endpoint Management gelöscht. Der Aktivitätszeitraum wird durch die Servereigenschaft **Length of Time Device Can Be Inactive Before Being Automatically Removed From CEM** festgelegt. Die Standardeinstellung ist **Wahr**. Wenden Sie sich an Ihren Citrix Vertreter, um den Wert dieser Eigenschaft zu ändern.

Auditprotokollierung

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

Registrierung für Android- und iOS-Geräte mit Rooting/Jailbreak blockieren

Wenn diese Eigenschaft auf **Wahr** festgelegt ist, blockiert Citrix Endpoint Management die Registrierung von Android-Geräten mit Rooting und von iOS-Geräten mit Jailbreak. Die empfohlene Einstellung von **Wahr** gilt für alle Sicherheitsstufen. Der Standardwert ist **Wahr**.

cdn.s3.retry.interval und cdn.s3.max.retry

Die Servereigenschaften `cdn.s3.retry.interval` und `cdn.s3.max.retry` legen gemeinsam das maximale Zeitlimit für jeden Upload von macOS PKG-Dateien fest. Standardmäßig begrenzt Citrix Endpoint Management die Uploadzeiten für Dateien auf 100 Sekunden. Wenn ein Dateiupload dieses Limit überschreitet, schlägt der Upload fehl. Um die Standardeinstellung zu ändern, konfigurieren Sie die Schlüssel `cdn.s3.retry.interval` und `cdn.s3.max.retry` wie folgt:

- `cdn.s3.retry.interval`. Hiermit können Sie das Intervall in Millisekunden definieren, in dem Citrix Endpoint Management überprüft, ob ein Dateiupload erfolgreich abgeschlossen wird. Der Standardwert ist `10000`.
- `cdn.s3.max.retry`. Hiermit können Sie festlegen, nach wie vielen Überprüfungsversuchen der Upload fehlschlägt. Der Standardwert ist `10`.

Beide Schlüssel begrenzen gemeinsam die Dateiuploadzeiten. Standardmäßig beträgt das Zeitlimit 100 Sekunden (10.000 x 10 Millisekunden).

Zertifikatserneuerung (in Sekunden)

- Der Zeitpunkt in Sekunden vor Ablauf eines Zertifikats, zu dem Citrix Endpoint Management die Verlängerung beginnt. Ein Beispiel ist, wenn ein Zertifikat am 30. Dezember abläuft und die Eigenschaft auf 30 Tage festgelegt ist. Citrix Endpoint Management versucht, das Zertifikat zu erneuern, 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 Citrix Endpoint Management bei Sitzungsinaktivität die TCP-Verbindung zum Gerät beendet. Die Sitzung bleibt geöffnet. Gilt für Android Geräte. Der Standardwert ist **5** Minuten.

Standardbereitstellungskanal

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

Mobilfunkanbieter nicht mehr unterstützen

- Stellt die Unterstützung für die Mobilfunkanbieterschnittstelle zum Abfragen von Blackberry- und anderen Exchange ActiveSync-Geräten ein. Bei Aktivierung ist die Schnittstelle **Mobilfunkanbieter** in der Konsole ausgeblendet. Die Standardeinstellung ist **true**.

Zuweisen von Geräte-Tags

- Wenn Sie `enable.device.tagging` auf **true** festlegen, werden Geräte automatisch in Citrix Endpoint Management nach Gerätetyp gekennzeichnet. Sie können Geräte-Tags verwenden, um Richtlinien und Apps bereitzustellen oder um Bereitstellungsgruppen zu konfigurieren. Citrix Endpoint Management kann Geräten folgende Tags zuweisen:
  - BYOD-Tags
    - iOS-Benutzerregistrierung
    - Android Enterprise-Arbeitsprofil
  - Unternehmens-Tags
    - Vollständig verwaltete Android Enterprise-Unternehmensgeräte
    - Massenregistrierung
      - Apple Business Manager-Geräte
      - Apple School Manager-Geräte
      - Windows AutoPilot-Geräte
      - Android Enterprise-Massenregistrierung

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 für Citrix Endpoint Management aktiviert.
  - Das Zertifikat wurde vom Microsoft-Zertifizierungsstellenserver ausgestellt.
  - Das Zertifikat wurde von einer internen Zertifizierungsstelle signiert, deren Stammzertifikat Citrix Endpoint Management als nicht vertrauenswürdig ansieht.

  Der Standardwert ist **Wahr**.

Absturzberichterstellung

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

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 Citrix Endpoint Management und einem 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. Citrix Endpoint Management 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 Citrix Secure Hub-Clientbenachrichtigungen. Mit **Wahr** werden Benachrichtigungen aktiviert. Der Standardwert ist **Wahr**.

Vollständiger Pull von zulässigen und abgelehnten ActiveSync-Benutzern

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

Gibt an, ob Telemetrie aktiviert ist

- Gibt an, ob Telemetrie aktiviert ist. Telemetrie wird auch als CEIP bezeichnet und ist ein Programm zur Verbesserung der Benutzerfreundlichkeit. Sie können beim Installieren oder Aktualisieren von Citrix Endpoint Management festlegen, ob Sie am CEIP teilnehmen möchten. Wenn in Citrix Endpoint Management nacheinander 15 Uploads fehlgeschlagen sind, wird die Telemetrie deaktiviert. Der Standardwert ist **Falsch**.

Inaktivitätstimeout in Minuten

- Die Zeit in Minuten, nach deren Ablauf ein inaktiver Benutzer in Citrix Endpoint Management abgemeldet wird. Der Benutzer muss über die öffentliche Citrix Endpoint Management-API auf die Citrix Endpoint Management-Konsole oder eine Drittanbieter-App zugegriffen haben. 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. Der Standardwert ist **5**.
- Wird für die Servereigenschaft **Timeouttyp für Webservices** der Wert **INACTIVITY_TIMEOUT** festgelegt, definiert diese Eigenschaft, nach wie vielen Minuten Citrix Endpoint Management einen inaktiven Administrator abmeldet, der folgende Schritte ausgeführt hat:
  - Zugriff auf die Citrix Endpoint Management-Konsole über die öffentliche Citrix Endpoint Management API für REST-Dienste
  - Zugriff auf eine beliebige Drittanbieter-App über die öffentliche API für REST-Dienste. Ein Timeoutwert von **0** bedeutet, dass ein inaktiver Benutzer angemeldet bleibt.

include.device.properties.during.search

- Schließt alle Geräteeigenschaften in eine Gerätesuche ein. Die Standardeinstellung ist **Aus**. Dadurch wird der Suchbereich auf folgende Geräteeigenschaften beschränkt, um die Suche zu beschleunigen:
  - Seriennummer
  - IMEI
  - WiFi MAC-Adresse

- Bluetooth MAC-Adresse
- Active Sync ID
- Benutzername

Wenn diese Eigenschaft auf **Ein**gesetzt ist, kann die Gerätesuche länger dauern.

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- Legt fest, nach wie vielen Tagen ein iOS- oder macOS-Gerät im Offlinemodus als nicht erreichbar gilt. Wenn auf iOS- oder macOS-Geräten der Grenzwert erreicht wird, senden die Geräte keine weiteren Abfragen an Citrix Endpoint Management. Der Standardwert für beide Eigenschaften ist **45** Tage.

Registrierung für iOS-Geräteverwaltung: Stammzertifizierungsstelle ggf. installieren

- Die Servereigenschaft **ios.mdm.enrollment.installRootCaIfRequired** ist für alle Citrix Endpoint Management-Umgebungen auf **Falsch** festgelegt. In Citrix Endpoint Management wird eine öffentlich vertrauenswürdige Zertifikatkette verwendet, sodass es nicht notwendig ist, eine Stammzertifizierungsstelle an die Geräte zu übertragen. (Diese Eigenschaft wird nur für On-Premises-Umgebungen verwendet.)

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 Citrix Endpoint Management 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 Citrix Endpoint Management-iOS-Agent-Identitäten. Standardeinstellung ist **2048**.

iOS-Geräteverwaltung: Identitätserneuerung (Tage)

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

iOS MDM APNs – Kennwort für privaten Schlüssel

- Diese Eigenschaft enthält das APNs-Kennwort, das Citrix Endpoint Management 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 Citrix Endpoint Management die Verbindung trennt. Der Standardwert ist **7** Tage.

Der Zeitdauer, die ein Gerät inaktiv sein kann, bevor es automatisch aus CEM entfernt wird

- Der Zeitdauer (in Tagen), die ein Gerät inaktiv sein kann, bevor es automatisch aus Citrix Endpoint Management entfernt wird. Das Minimum ist **14** Tage und die Standardeinstellung **30** Tage. Die Servereigenschaft **Allows The Removal of Devices That Have Been Marked Inactive For A Specified Period Of Time**, muss auf **Wahr** festgelegt sein, damit diese Eigenschaft wirksam wird.

local.user.account.lockout.time

- Gibt den Zeitraum in Minuten ein, den ein Benutzer nach einer Überschreitung des Sperrlimits abwarten muss. Unterstützte Werte sind 0 bis 999. Die Standardeinstellung ist **30** Minuten.

local.user.account.lockout.limit

- Gibt die maximale Anzahl aufeinanderfolgender ungültiger Anmeldeversuche pro Benutzer an. Unterstützte Werte sind 0 bis 999. Der Standardwert ist auf **6**festgelegt.

mac.dep.admin.passwd.rotate

Hiermit können Sie für macOS-Geräte, die über das Apple-Bereitstellungsprogramm registriert sind, Rotationsintervalle für Administratorkennwörter konfigurieren. Citrix Endpoint Management prüft, ob das Kennwort des Administratorkontos täglich rotiert werden soll. Standardmäßig wechselt Citrix Endpoint Management das Kennwort alle 10.080 Minuten (7 Tage). Konfigurieren Sie den Schlüssel `mac.dep.admin.passwd.rotate` wie folgt:

- Wert: *administrator-defined*
  Das Intervall in Minuten, in dem Citrix Endpoint Management das Kennwort rotiert. Geben Sie einen Wert größer oder gleich 360 (6 Stunden) ein. Werte unter 360 werden von Citrix Endpoint Management ignoriert. Das Kennwort wird dann alle 360 Minuten (6 Stunden) geändert.
- Anzeigename: *administrator-defined*
- Beschreibung: *administratordefiniert*

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. Eine größere Anzahl von Threads führt jedoch zu einer hohen CPU-Auslastung.

NetScaler Gateway (NetScaler) Single Sign-On

- Bei der Einstellung **Falsch** ist das Rückruffeature von Citrix Endpoint Management beim Single Sign-On von NetScaler Gateway bei Citrix Endpoint Management deaktiviert. Wenn die NetScaler Gateway-Konfiguration eine Rückruf-URL enthält, prüft Citrix Endpoint Management mit dem Rückruffeature die NetScaler 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. Citrix Endpoint Management erhöht den Wert, wenn ein Upload fehlschlägt. Nach 15 Upload-Fehlern deaktiviert Citrix Endpoint Management das CEIP (auch als Telemetrie bezeichnet). Weitere Informationen siehe Servereigenschaft **Gibt an, ob Telemetrie aktiviert ist.**. Citrix Endpoint Management 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**.

optional.user.identity.attributes

- Mit dieser Servereigenschaft können Sie die optionalen Active Directory-Benutzerattribute anpassen.

  Erstellen Sie den benutzerdefinierten Schlüssel und bearbeiten Sie im Feld **Wert** Benutzerattribute, um festzulegen, auf welche Attribute Citrix Endpoint Management zugreifen kann, um ein Benutzerkonto zu erstellen. Weitere Informationen finden Sie unter Anpassen von Benutzereigenschaften.

  - Schlüssel: **Benutzerdefinierter Schlüssel**
  - Schlüssel: **optional.user.identity.attributes**
  - Wert: **commonName, firstName, lastName, displayName, streetAddress, city, state, country, workPhone, homePhone, mobilePhone, company, department, description, employeeID, faxNumber, initials, ipPhone, manager, homePostalAddress, otherMobile, pager, physicalDeliveryOfficeName, postalCode, postOfficeBox, title, organization, preferredLanguage**
  - Anzeigename: **optional.user.identity.attributes**
  - Beschreibung: **Optionale Active Directory-Benutzerattribute**

Organisationsname für macOS- und iOS/iPadOS-Registrierungsprofile

- Der Wert, den Sie für `apple.mdm.enrollment.profile.organization.name` eingeben, entspricht dem Namen der Organisation, die das Registrierungsprofil bereitstellt. Der Name wird angezeigt, wenn Benutzer ihr Gerät bei Citrix Endpoint Management registrieren. Der angezeigte Standardname lautet **Citrix Workspace**.

Pull der inkrementellen Änderung der zulässigen und abgelehnten Benutzer

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

Lesetimeout zum Microsoft-Zertifizierungsserver

- Die Zeitdauer in Sekunden, die Citrix Endpoint Management 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**.

shp.console.enable

- Die Auswahl von **Falsch** verhindert den Zugriff auf das Selbsthilfeportal. Benutzer, die über Port 4443 zum Portal navigieren, erhalten die Meldung "Zugriff verweigert". Bei Auswahl von **Wahr** erfolgt der Zugriff auf das Selbsthilfeportal über Port 443.

  Die Standardeinstellung ist **Falsch**.

enable.new.shp

- Mit **Falsch** wird verhindert, dass Benutzer ihre Geräte über das Selbsthilfeportal aktivieren. Mit **Wahr** können Benutzer ihre Geräte über das Selbsthilfeportal aktivieren.

Für den BitLocker-Wiederherstellungsschlüssel ist es erforderlich, dass Sie diese Eigenschaft auf **Falsch** und die `shp.console.enable`-Eigenschaft auf **Wahr** festlegen.

Die Standardeinstellung ist **Falsch**.

Sitzungsprotokollbereinigung (in Tagen)

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

ShareFile-Konfigurationstyp

- Gibt den Citrix Files-Speichertyp an. **ENTERPRISE** aktiviert den Citrix Files Enterprise-Modus. **CONNECTORS** limitiert den Zugriff auf Speicherzonenconnectors, die Sie über die Citrix Endpoint Management-Konsole erstellen. Der Standardwert ist **NONE**. Dabei wird die Startansicht des Bildschirms **Konfigurieren > Citrix Files** 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 Citrix Endpoint Management einen Administrator abmeldet, der folgende Schritte ausgeführt hat:
  - Zugriff auf die Citrix Endpoint Management-Konsole über die öffentliche API für REST-Dienste.
  - Zugriff auf eine beliebige Drittanbieter-App über die öffentliche API für REST-Dienste.

  Der Standardwert ist **60**.

Unterdrückung von Agentnachrichten auslösen

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

Unterdrückung von Agenttönen auslösen

- Aktiviert oder deaktiviert Citrix 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. Citrix Endpoint Management 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 Citrix Secure Hub verwendet, die Einmaltickets nicht validieren. Mit der Einstellung **Falsch** können Sie nicht authentifizierte Apps von Citrix Endpoint Management auf Windows-Geräte herunterladen. Die Standardeinstellung ist **Falsch**.

ActiveSync-ID zum Löschen von Gerät mit ActiveSync verwenden

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

Nur Benutzer von Exchange

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

Volume Purchase-Basisintervall

- Das Mindestintervall in dem Citrix Endpoint Management Volume Purchase-Lizenzen von Apple neu importiert. Durch Aktualisierung der Lizenzinformationen wird sichergestellt, dass Citrix Endpoint Management alle Änderungen enthält, beispielsweise das manuelle Löschen einer importierten App aus Volume Purchase. Standardmäßig aktualisiert Citrix Endpoint Management 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 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 Citrix Endpoint Management fortlaufend mit den Änderungen aktualisiert wird.
  - Das Mindestintervall zwischen den zwei Basiswerten beträgt 60 Minuten. Außerdem führt Citrix Endpoint Management 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 Wahl von **STATIC_TIMEOUT** erfasst Citrix Endpoint Management über den Wert der Servereigenschaft **Statisches Timeout in Minuten**, ob ein Token abgelaufen ist.
  - Bei Wahl von **INACTIVITY_TIMEOUT** erfasst Citrix Endpoint Management über den Wert der Servereigenschaft **Inaktivitätstimeout in Minuten**, ob ein Token abgelaufen ist. Der Standardwert ist **STATIC_TIMEOUT**.

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

- Die Gültigkeitsdauer des von MDM für Windows 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 Citrix Endpoint Management 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 Citrix Endpoint Management MDM-Selbsthilfeportal

- Dieser Eigenschaftsname spiegelt die älteren Citrix Endpoint Management-Versionen wider. Die Eigenschaft steuert das maximale Inaktivitätsintervall der Citrix Endpoint Management-Konsole. Das Intervall ist die Zeit in Minuten, nach der ein inaktiver Benutzer von der Citrix Endpoint Management-Konsole abgemeldet wird. Ein Timeoutwert von **0** bedeutet, dass ein inaktiver Benutzer angemeldet bleibt. Die Standardeinstellung ist **30**.

Richtlinien für Geräte und Apps

March 11, 2024

Die Geräte- und App-Richtlinien von Citrix Endpoint Management 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

Die Geräte- und App-Richtlinien von Citrix Endpoint Management 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 verlegt ein Gerät.
- Benutzer müssen immer sicher auf das Netzwerk zugreifen.
- Benutzer verwenden 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 Citrix Endpoint Management

Daten, die auf mobilen Geräten gespeichert sind, werden auch ruhende Daten genannt. Citrix Endpoint Management verwendet die von den iOS- und Android-Plattformen bereitgestellte Geräteverschlüsselung. Citrix Endpoint Management ergänzt die plattformbasierte Verschlüsselung um Features wie die Compliancеprüfung, die über das Citrix MAM SDK verfügbar ist.

Die MAM-Funktionen in Citrix Endpoint Management ermöglichen die sichere und kontrollierte Verwaltung von mobilen Citrix Produktivitätsapps, MDX-aktivierten Apps und ihrer zugehörigen Daten.

Das SDK für mobile Apps ermöglicht die Bereitstellung von Apps über Citrix Endpoint Management mithilfe 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.

Citrix Endpoint Management umfasst auch eine Verschlüsselung auf App-Ebene. Citrix Endpoint Management verschlüsselt die in einer MDX-fähigen App gespeicherten Daten separat und ohne erforderlichen Passcode des Gerätes. Sie müssen das Gerät auch nicht verwalten, um die Richtlinie umsetzen zu können.

- Auf iOS-Geräten verwendet Citrix Endpoint Management starke FIPS-validierte Kryptografiedienste und Bibliotheken wie Schlüsselbund.
- OpenSSL bietet FIPS-validierte Module für verschiedene Geräteplattformen. OpenSSL sichert weiterhin Daten in der Übertragung und die zum Verwalten und Registrieren von Geräten erforderlichen Zertifikate.
- Citrix Endpoint Management verwendet die MAM SDK Shared Vault API zum Verwalten der von Apps mit derselben Schlüsselbundgruppe gemeinsam verwendeten Inhalte. Sie können beispielsweise Benutzerzertifikate über eine registrierte App freigeben, sodass Apps Zertifikate aus dem Tresor beziehen können.
- Citrix Endpoint Management verwendet die von den Plattformen bereitgestellte Geräteverschlüsselung.
- Citrix Endpoint Management MAM-Steuerelemente auf App-Ebene validieren per Konformitätsprüfung, ob die Geräteverschlüsselung bei jedem App-Start aktiviert ist.

Schutz von Daten im Übertragungsprozess durch Citrix Endpoint Management

Daten, die zwischen Mobilgeräten des Benutzers und dem internen Netzwerk übertragen werden, heißen auch Daten im Übertragungsprozess. Das MDX-App-Container-Verfahren bietet einen anwendungsspezifischen VPN-Zugriff auf Ihr internes Netzwerk über NetScaler 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 können. 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 NetScaler Gateway konfigurieren. Diese Richtlinie wird für die Authentifizierung und Micro-VPN-Sitzungen einer App verwendet. Sie können ein alternatives NetScaler Gateway mit der Richtlinie "Micro-VPN-Sitzung 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:

- Eine neue Version von Citrix Endpoint Management umfasst neue oder aktualisierte Richtlinien aufgrund veröffentlichter Gerätebetriebssystemupdates.
- 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 Citrix Endpoint Management 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 Citrix Secure Hub verfügbar sind, vielleicht möchten Sie aber auch die Interaktion dieser Apps mit Citrix Endpoint Management 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 Citrix 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 der Citrix Endpoint Management-Konsole unter **Einstellungen > Clienteigenschaften** konfigurieren. Sie können unter "Clienteigenschaften"einen Inaktivitätstimer festlegen, damit Citrix Secure Hub Benutzer erst nach Ablauf des Timers zur erneuten Authentifizierung bei der verwalteten App auffordert.

  Der App-Passcode unterscheidet sich von einem Gerätepasscode. Wenn eine Geräte-Passcoderichtlinie an ein Gerät übertragen wird, fordert Citrix Secure Hub den Benutzer auf, einen Passcode oder eine PIN zu konfigurieren. Der Benutzer muss sein Gerät beim Einschalten bzw. nach Ablauf des Inaktivitäts-Timers entsperren. Weitere Informationen finden Sie unter Authentifizierung in Citrix Endpoint Management.

  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.

- **Micro-VPN-Sitzung erforderlich**

  Verwendungszweck dieser Richtlinie: Wenn eine Anwendung zur Ausführung Zugriff auf eine Web-App (Webdienst) benötigt, aktivieren Sie diese Richtlinie. Citrix Endpoint Management fordert den Benutzer dann auf, sich mit dem Unternehmensnetzwerk zu verbinden oder eine aktive Sitzung zu erstellen, bevor er die App verwendet.

Benutzerbeispiel: Wenn Benutzer eine MDX-App öffnen, für die die Richtlinie "Micro-VPN-Sitzung erforderlich"aktiviert ist, können sie die App erst dann verwenden, wenn sie eine Verbindung mit dem Netzwerk herstellen. Die Verbindung muss über einen Mobilfunk- oder Wi-Fi-Dienst erstellt werden.

- **Maximale Offlinezeit**

  Verwendungszweck dieser Richtlinie: Verwenden Sie diese Richtlinie als zusätzliche Sicherheitsoption. Die Richtlinie sorgt dafür, dass Benutzer, die eine App eine bestimmte Zeitlang offline ausführen, den App-Anspruch erneut bestätigen und Richtlinien aktualisieren müssen.

  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 App-Store verfügbar ist. 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 Citrix Secure Mail in den App-Store und definieren einen Kulanzzeitraum für das App-Update von 6 Stunden. Citrix Secure Hub-Benutzer haben dann sechs Stunden Zeit, um Citrix Secure Mail zu aktualisieren, bevor sie zum App-Store weitergeleitet werden.

- **Aktives Abfrageintervall (Minuten)**

  Verwendungszweck der Richtlinie: Das aktive Abfrageintervall ist der Zeitraum, in dem Citrix Endpoint Management 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 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 ein Benutzer:

- Daten in persönliche Apps außerhalb des Containers verschiebt
- Daten von außerhalb des Containers in die Apps im Container einfügt

Benutzerbeispiel: Sie wählen für eine App-Interaktionsrichtlinie die Einstellung "Eingeschränkt". Benutzer können Texte dann von Citrix Secure Mail in Citrix Secure Web kopieren. Sie können sie aber nicht in ihren persönlichen Safari- oder Chrome-Browser außerhalb des Containers kopieren. Benutzer können außerdem Dokumente im Anhang aus Citrix Secure Mail in Citrix Files oder QuickEdit öffnen. Sie können angehängte Dokumente nicht in ihren eigenen Apps zur Dateianzeige außerhalb des Containers öffnen.

App-Einschränkungsrichtlinien

Verwendungszweck dieser Richtlinien: Mit App-Einschränkungsrichtlinien legen Sie fest, auf welche Features Benutzer aus einer geöffneten MDX-App heraus zugreifen können. Diese Einschränkungen sind 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 beispielsweise 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. Die Option "Tunnel - Web-SSO"erlaubt nur das Tunneln von HTTP- und HTTPS-Datenverkehr. Sie bietet Single Sign-On (SSO) für HTTP- und HTTPS-Datenverkehr sowie PKINIT-Authentifizierung.

Benutzerbeispiel: Wenn ein Benutzer eine MDX-App mit aktivierter Tunnelfunktion öffnet, öffnet der Browser eine Intranetsite, ohne dass der Benutzer ein VPN starten muss. Die 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.

Citrix Secure Mail-App-Richtlinien

- **Hintergrundnetzwerkdienste**

  Verwendungszweck dieser Richtlinie: Hintergrundnetzwerkdienste in Citrix Secure Mail verwenden Secure Ticket Authority (STA), eine Art SOCKS5-Proxy, um über NetScaler 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 Citrix Secure Mail konfigurieren. Der NetScaler für XenMobile-Assistent richtet STA für Citrix Secure Mail automatisch ein.

  Benutzerbeispiel: Wenn STA nicht aktiviert ist, werden Android-Benutzer beim Öffnen von Citrix Secure Mail aufgefordert, ein VPN zu öffnen, das dann auf dem Gerät geöffnet bleibt. Wenn STA aktiviert ist, wird beim Öffnen von Citrix 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 Citrix Secure Mail erfolgt, wenn ein Benutzer das erste Mal auf Citrix Secure Mail zugreift. Die Synchronisierung von E-Mails aus zwei Wochen dauert länger als die aus drei Tagen. Mehr zu synchronisierende Daten verlängern den Einrichtungsprozess für den Benutzer.

  Benutzerbeispiel: Angenommen, das Standardsynchronisierungsintervall wurde bei der Ersteinrichtung von Citrix Secure Mail auf drei Tage festgelegt. Der Benutzer sieht alle E-Mails in seinem Posteingang, die er in den letzten drei Tagen erhalten hat. Wenn ein Benutzer E-Mails anzeigen möchte, die älter als drei Tage sind, kann er eine Suche durchführen. Citrix Secure Mail zeigt dann auch ältere E-Mails an, die auf dem Server gespeichert sind. Nach der Installation von Citrix Secure Mail kann jeder Benutzer diese Einstellung an seine Anforderungen anpassen.

Geräterichtlinien und Anwendungsverhalten

Geräterichtlinien (gelegentlich auch als MDM-Richtlinien bezeichnet) legen fest, wie Citrix Endpoint Management Geräte verwaltet. 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: Um sämtliche von einem Benutzer installierten Apps anzuzeigen, stellen Sie die App-Bestandsrichtlinie auf einem Gerät bereit. Wenn Sie die Richtlinie nicht bereitstellen, können Sie nur die vom Benutzer aus dem App-Store installierten Apps anzeigen, nicht jedoch persönlich installierte Apps. Verwenden Sie die App-Bestandsrichtlinie, wenn Sie bestimmte Apps auf Unternehmensgeräten sperren möchten.

  Benutzerbeispiel: Benutzer mit einem MDM-verwalteten Gerät können diese Funktion nicht deaktivieren. Die persönlich installierten Anwendungen des Benutzers sind für Citrix Endpoint Management-Administratoren sichtbar.

- **App-Sperre**

  Verwendungszweck dieser Richtlinie: Mit der App-Sperre können Sie in Android Sperr- oder Positivlisten für Apps einrichten. Für zulässige 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: Die Verbindungszeitplanrichtlinie ermöglicht es Windows Mobile-Geräten, für Funktionen wie MDM-Verwaltung, App-Push und Richtlinienbereitstellung eine Verbindung mit Citrix Endpoint Management herzustellen. Für Android- und Android Enterprise-Geräte verwenden Sie Google Firebase Cloud Messaging (FCM). FCM steuert Verbindungen mit Citrix Endpoint Management. Es gibt folgende Verbindungszeitplanoptionen:

  - **Nie:** Die Verbindung muss manuell hergestellt werden. Die Benutzer müssen die Verbindung mit Citrix Endpoint Management auf ihrem Gerät herstellen. Citrix empfiehlt, diese Option nicht für Produktionsumgebungen zu verwenden, da sie die Bereitstellung von Sicherheitsrichtlinien auf Geräten verhindert. Benutzer erhalten dann keine neuen Apps und Richtlinien. Die Option **Nie** ist standardmäßig aktiviert.
  - **Alle:** Die Verbindung wird in dem hier ausgewählten Intervall hergestellt. Wenn Sie eine Sicherheitsrichtlinie wie eine Sperrung oder eine Datenlöschung senden, verarbeitet Citrix Endpoint Management die Richtlinie auf dem Gerät, wenn das Gerät das nächste Mal eine Verbindung herstellt.
  - **Zeitplan festlegen:** Citrix Endpoint Management versucht nach einer Netzwerkverbindungsunterbrechung eine Wiederherstellung der Verbindung zwischen Benutzergerät und Citrix Endpoint Management-Server. Citrix Endpoint Management überwacht die Verbindung durch regelmäßige Übertragung von Kontrollpaketen in dem von Ihnen festgelegten Zeitrahmen.

  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 mit einer Netzwerkrichtlinie verwendet. Sie ermöglicht es Ihnen, Authentifizierungszertifikate bereitzustellen, die für die Authentifizierung bei internen Ressourcen benötigt werden, die eine Zertifikatauthentifizierung erfordern.

  Benutzerbeispiel: Sie stellen eine Netzwerkrichtlinie 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: Citrix Endpoint Management bietet zwei Optionen zum Bereitstellen von E-Mail mit Microsoft Exchange ActiveSync.

  - **Citrix Secure Mail-App:** Versand von E-Mails mit der Citrix Secure Mail-App, die Sie über den öffentlichen App-Store oder den App-Store verteilen.
  - **Systemeigene E-Mail-App:** Aktiviert ActiveSync-E-Mail für den systemeigenen E-Mail-Client auf dem Gerät. Sie können 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 Citrix 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 Citrix Secure Hub aktiviert. Wenn Sie nach dem Bereitstellen der Richtlinie einen Ortungsbefehl von Citrix Endpoint Management 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 Citrix Endpoint Management-Selbsthilfeportal anmelden und mit der Option “Orten”den Standort des Geräts auf einer Karte anzeigen. Die Benutzer entscheiden, ob Citrix Secure Hub Ortungsdienste verwenden darf. 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: Wenn Sie eine Passcoderichtlinie auf einem verwalteten Gerät bereitstellen, fordert Citrix Secure Hub den Benutzer auf, einen Passcode oder eine PIN zu konfigurieren. Mit dem Passcode bzw. der PIN erhält der Benutzer während des Startvorgangs oder nach Ablauf des Inaktivitäts-Timers Zugriff auf sein Gerät.

- **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 mithilfe der Profilentfernungsrichtlinie entfernen. Verwenden Sie dann Bereitstellungsregeln, um die Profilentfernungsrichtlinie nur für bestimmte Benutzer bereitzustellen.

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, bemerkt der Benutzer diese Änderung nicht. 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. Einschränkungsoptionen sind beispielsweise das Deaktivieren der Kamera oder des Mikrofons auf einem Gerät, das Durchsetzen von Roamingregeln und ein gesteuerter Zugriff 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: Benutzer müssen möglicherweise auf rechtliche Auswirkungen hingewiesen werden, 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 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 diverse VPN-Anbieter, einschließlich Cisco AnyConnect, Juniper und 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 öffnen, um Zugriff auf benötigte Services zu erhalten. Der Einsatz eines Weblinks ist benutzerfreundlicher als die Eingabe einer Linkadresse im Browser.

- **Netzwerkrichtlinie**

  Verwendungszweck dieser Richtlinie: Mit der Netzwerkrichtlinie können Sie auf einem verwalteten Gerät Wi-Fi-Netzwerkangaben wie SSID, Authentifizierungs- und Konfigurationsdaten bereitstellen.

  Benutzerbeispiel: Wenn Sie die Netzwerkrichtlinie bereitstellen, verbindet sich das Gerät automatisch mit dem Wi-Fi-Netzwerk und authentifiziert den Benutzer, der damit Zugriff auf das Netzwerk erhält.

- **Endpoint Management Store-Richtlinie**

  Verwendungszweck dieser Richtlinie: Der App-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 Citrix Endpoint Management registriert hat, kann er über Citrix Secure Hub auf den App-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 App-Store herunterladen.

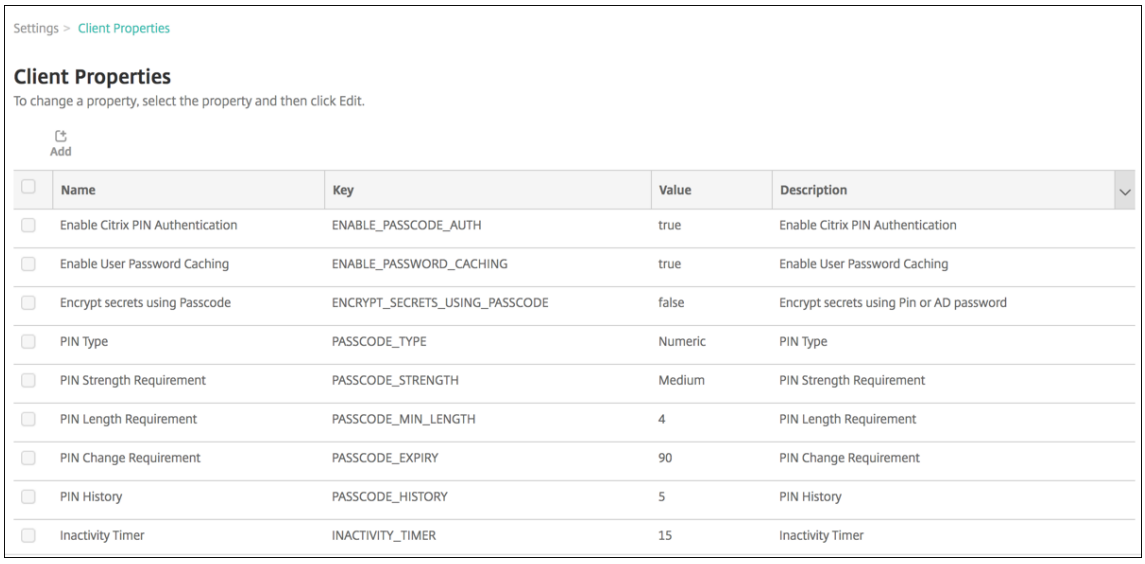
Clienteigenschaften

March 11, 2024

Clienteigenschaften enthalten Informationen, die direkt in Citrix 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 Citrix 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.

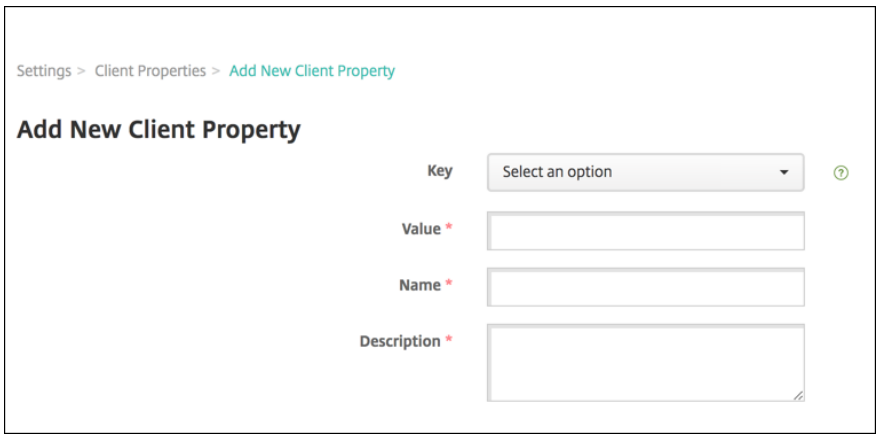
1. Klicken Sie in der Citrix Endpoint Management-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Client** auf **Clienteigenschaften**. Die Seite **Clienteigenschaften** wird angezeigt. Auf dieser Seite können Sie Clienteigenschaften hinzufügen, bearbeiten und löschen.



Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	true	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	true	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Type	PASSCODE_TYPE	Numeric	PIN Type
PIN Strength Requirement	PASSCODE_STRENGTH	Medium	PIN Strength Requirement
PIN Length Requirement	PASSCODE_MIN_LENGTH	4	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

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 Dropdownliste 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.

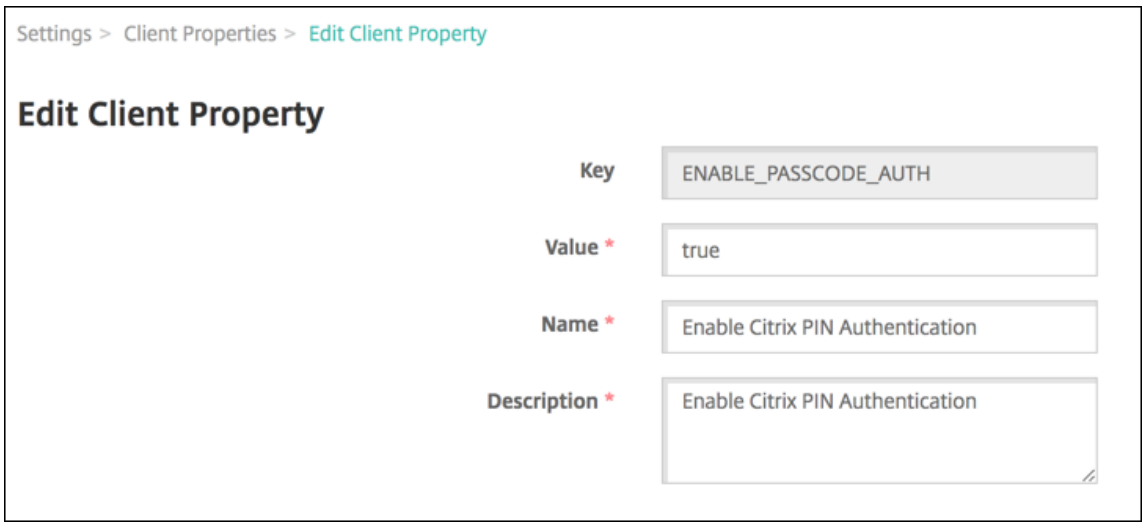
3. Klicken Sie auf **Speichern**.

Bearbeiten einer Clienteigenschaft

1. Wählen Sie in der Tabelle **Clienteigenschaften** die zu bearbeitende Clienteigenschaft aus.

   Aktivieren Sie das Kontrollkästchen neben einer Clienteigenschaft, um oberhalb der Liste der Clienteigenschaften ein Optionsmenü anzuzeigen. Klicken Sie an eine andere Stelle in der Liste, um das Menü mit den Optionen rechts daneben zu öffnen.

2. Klicken Sie auf **Bearbeiten**. Die Seite **Clienteigenschaft bearbeiten** wird angezeigt.



3. Ändern Sie nach Bedarf die folgenden Informationen:

   - **Schlüssel:** Sie können dieses Feld nicht ändern.
   - **Wert:** Wert der Eigenschaft.
   - **Name:** Name der Eigenschaft.
   - **Beschreibung:** Beschreibung der Eigenschaft.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die 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 Clienteigenschaften und deren Standardeinstellungen für Citrix Endpoint Management sind wie folgt:

- **ALLOW_CLIENTSIDE_PROXY**
  - Anzeigename: ALLOW_CLIENTSIDE_PROXY

- Wenn Benutzer einen auf ihren iOS-Geräten konfigurierten Proxy verwenden möchten, belassen Sie für diese benutzerdefinierte Richtlinie den Standardwert **true**.

  Manche Benutzer haben evtl. unter **Einstellungen > WLAN > Proxy konfigurieren** einen Proxy auf ihrem Gerät konfiguriert. Wenn Citrix Secure Hub für diese Benutzer nicht geöffnet wird, führen Sie eine der folgenden Aktionen aus:

  * Entfernen der Proxykonfiguration vom Gerät und Neustart von Citrix Secure Hub.
  * Verbinden des Geräts mit einem anderen Wi-Fi-Netzwerk. Nach der erneuten Citrix Secure Hub-Authentifizierung erhält Citrix Secure Hub die Eigenschaft **ALLOW_CLIENTSIDE_PROXY** und wird geöffnet.

- Wenn **ALLOW_CLIENTSIDE_PROXY** auf **false** gesetzt ist und Benutzer einen Proxy auf ihrem Gerät konfigurieren, erkennt Citrix Endpoint Management den Proxy. Citrix Secure Hub verwendet den Proxy jedoch nicht und zeigt eine Fehlermeldung an. Wenn ein Gerät eine Verbindung zu einem Zugriffspunkt oder Router herstellt, für den ein Proxy aktiviert wurde, erkennt Citrix Endpoint Management den Proxy nicht. Um höchste Sicherheit zu gewährleisten, empfehlen wir die Verwendung von Zertifikatpinning. Informationen zum Aktivieren von Zertifikatpinning für Citrix Secure Hub finden Sie unter Zertifikatpinning.

- Navigieren Sie zum Konfigurieren dieser benutzerdefinierten Clientrichtlinie zu **Einstellungen > Clienteigenschaften**, fügen Sie den benutzerdefinierten Schlüssel **ALLOW_CLIENTSIDE_PROXY** hinzu und legen Sie den **Wert** fest.

- **CONTAINER_SELF_DESTRUCT_PERIOD**

  - Anzeigename: MDX Container Self-Destruct Period

  - Self-destruct verhindert den Zugriff auf Citrix 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. Angenommen, Sie haben die Eigenschaft auf 30 Tage festgelegt. Wenn der Benutzer die App mehr als 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 Citrix 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 Citrix Endpoint Management-Konsole für Citrix Secure Hub- und MDX-Apps.

    Wenn diese Eigenschaft auf **true** festgelegt wird, wird die Eigenschaft **App-Protokolle blockieren** in Citrix 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 Citrix 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 Citrix Produktivitätsapps ein. Sie können den Anmeldeinformationsspeicher verwenden. Dabei spielt es keine Rolle, ob Sie die Citrix-PIN aktivieren. Wenn Sie Citrix-PIN nicht aktivieren, geben Benutzer ihr

Active Directory-Kennwort ein. Citrix Endpoint Management unterstützt die Verwendung von Active Directory-Kennwörtern mit dem Anmeldeinformationsspeicher ausschließlich für Citrix Secure Hub und öffentliche Store-Apps. Wenn Sie Active Directory-Kennwörter mit dem Anmeldeinformationsspeicher verwenden, bietet Citrix Endpoint Management keine Unterstützung für PKI-Authentifizierung.

- Für die automatische Registrierung bei Citrix 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_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 Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix 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 “Benutzerkennwortcaching”aktiviert ist, werden die Benutzer von Citrix Endpoint Management 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 Citrix Endpoint Management 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 Citrix Secure Hub 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 Citrix Endpoint Management verbessern.
  - Wert: **true** oder **false**
  - Standardwert: **false**
- **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 Citrix 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 Citrix 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 the 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 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	Zulässig	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	Zulässig	Nicht zulässig
Niedrig	Muss mindestens eine Ziffer und einen Buchstaben enthalten.	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef

Passcodestärke	Regeln für alphanumerischen Passcodetyp	Zulässig	Nicht zulässig
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 Citrix Endpoint Management dem AutoDiscovery 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 Citrix Endpoint Management so konfigurieren, dass Benutzer, die sich mit E-Mail-Anmeldeinformationen bei Citrix Secure Hub registrieren, automatisch bei Citrix Secure Mail registriert werden. Die Benutzer müssen dann zur Anmeldung bei Citrix 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 Citrix Endpoint Management 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 Dienstendpunkte vom Micro-VPN-Tunneling aus, die von Mobile Apps-SDKs und -Apps für diverse Features verwendet werden. 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. Dies ist die Standardeinstellung:

    ```
    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
    ```

Die benutzerdefinierten Clienteigenschaften für Citrix Endpoint Management sind wie folgt:

ENABLE_MAM_NFACTOR_SSO:

- Mit dieser Eigenschaft können Sie MAM nFactor SSO während der MAM-Registrierung oder Anmeldung für Secure Hub aktivieren oder deaktivieren, während Sie die erweiterte Authentifizierungsrichtlinie im NetScaler Gateway verwenden. Wenn der Wert auf **true** gesetzt ist, wird MAM nFactor SSO während der MAM-Registrierung oder Anmeldung für Secure Hub aktiviert.
- Um diese Eigenschaft zu konfigurieren, gehen Sie zu **Einstellungen > Clienteigenschaften** und klicken Sie auf **Hinzufügen**. Wählen Sie im Dropdownmenü **Schlüssel** die Option **Be-**

nutzerdefinierter Schlüssel aus und aktualisieren Sie die folgenden Informationen nach Bedarf:

- Schlüssel: ENABLE_MAM_NFACTOR_SSO
- Wert: “true”oder “false”
- Name: ENABLE_MAM_NFACTOR_SSO
- Beschreibung: Fügen Sie die entsprechende Beschreibung hinzu

Optionen der Benutzerregistrierung

March 11, 2024

Es gibt mehrere Verfahren, mit denen Benutzer ihre Geräte bei Citrix Endpoint Management 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 Citrix Secure Hub herunterladen, eine Registrierung anfordern oder Geräteinformationen anzeigen können.
- **Manuelle Registrierung:** Informieren Sie Benutzer per E-Mail, Handbuch oder auf anderem Wege, dass das System betriebsbereit ist und dass sie sich registrieren können. Benutzer laden dann Citrix 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 sind für Windows-Geräte nicht verfügbar.

Sie können auch einen Installationslink über SMTP an Benutzer mit iOS-, macOS-, Android Enterprise-, 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** von Citrix Endpoint Management aktivieren oder deaktivieren.

Weitere Informationen zu jedem Registrierungssicherheitsmodus finden Sie unter Registrierungssicherheitsmodi konfigurieren.

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 SMTP erfordert 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 Citrix Secure Hub auf ihre E-Mails zugreifen können. Verwenden Sie gegebenenfalls Registrierungssicherheitsmodi mit Einmalkennwort (OTP) als Alternative zu Active Directory-Kennwörtern für die MDM-Registrierung.

Selbsthilfeportal

Für das Selbsthilfeportal kann dieselbe URL verwendet werden, mit der Administratoren auf die Citrix Endpoint Management-Konsole zugreifen. Die Endbenutzer sehen das Selbsthilfeportal anstelle der Verwaltungskonsole. Im Selbsthilfeportal können Benutzer Citrix Secure Hub herunterladen, die Registrierung anfordern und Geräteinformationen anzeigen.

Zum Einrichten des Portals aktualisieren Sie diese Servereigenschaften unter **Einstellungen > Servereigenschaften**:

- `shp.console.enable`: Mit **Wahr** können Benutzer auf das Selbsthilfeportal zugreifen.

- `enable.new.shp`: Mit **Wahr** können Benutzer ihre Geräte über das Selbsthilfeportal aktivieren.

Manuelle Registrierung

Bei einer manuellen Registrierung verbinden sich Benutzer über AutoDiscovery oder über Eingabe der Serverinformationen mit Citrix Endpoint Management. 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 Einrichten von Citrix Endpoint Management 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- 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 oder 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 Citrix Endpoint Management-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 Registrierungseinladungen.

Senden Sie eine Einladung für jeden Benutzer oder jede Gruppe, die sich in Ihrer Umgebung registrieren sollen. Dieser Prozess kann je nach Größe Ihrer Organisation sehr lange dauern. Es ist möglich, Einladungen mithilfe von Active Directory-Gruppen zu bündeln, dies muss jedoch gestaffelt erfolgen.

Erster Kontakt mit Benutzern

Nachdem Sie entschieden haben, ob Sie eine offene Registrierung oder eine selektive Einladung verwenden möchten, und Sie diese Umgebungen eingerichtet haben, informieren Sie die Benutzer über ihre Anmeldungsoptionen.

Beim selektiven Einladungsverfahren sind E-Mail-Nachrichten Teil des Verfahrens. Auch bei der offenen Registrierung können Sie E-Mails über die Citrix Endpoint Management-Konsole senden. Weitere Einzelheiten finden Sie unter Registrierungseinladungen.

Bedenken Sie in beiden Fällen, dass Sie für E-Mails einen SMTP-Server benötigen. Ein solcher Server kann zusätzliche Kosten verursachen, die bei der Entscheidung zu berücksichtigen sind. Berücksichtigen Sie, wie neue Benutzer auf Informationen zugreifen sollen. Wenn alle Benutzer über Citrix Endpoint Management 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 Citrix Endpoint Management senden. Achten Sie bei dieser Option darauf, alle relevanten Informationen einzubeziehen. Teilen Sie den Benutzern mit, wo sie die Citrix 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 Citrix Endpoint Management-Serveradresse mitteilen. Weitere Informationen zur Discovery finden Sie unter Einrichten von Citrix Endpoint Management Autodiscovery Service.

Provisioning von Apps und Provisioning aufheben

March 11, 2024

Bei der App-Bereitstellung dreht sich alles um die App-Lebenszyklusverwaltung, d. h. um das Vorbereiten, Konfigurieren, Bereitstellen und Verwalten mobiler Apps in der Citrix Endpoint Management-Umgebung. In einigen Fällen kann das Entwickeln oder Modifizieren von App-Code Teil des Provisioningprozesses sein. Citrix Endpoint Management bietet verschiedene Tools und Prozesse für die App-Bereitstellung.

Vor der Lektüre des vorliegenden Artikels zur App-Bereitstellung sollten Sie Apps und Benutzergemeinschaften lesen. 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 Provisioningprozesses 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. Tunneln von HTTP- und HTTPS-Datenverkehr mit Single Sign-On (Tunnel - Web SSO).

Beispiel:

Faktor	Citrix Secure Mail	E-Mail	Intern	Epic Rover
Version	10.1	10.1	X.x	X.x

Faktor	Citrix Secure Mail	E-Mail	Intern	Epic Rover
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	–
Lizenzierung	–	–	–	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 normalerweise 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: kleinere Upgrades, etwa zur Korrektur eines Fehlers und Hauptreleases mit umfassenderen Änderungen. Lesen Sie in jedem Fall die Versionshinweise zu Apps, um zu ermitteln, 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 Juli 2023 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 Citrix Endpoint Management-Umgebung ändern. Die Änderungen hängen von der Art der für die Apps benötigten Sicherheitskonformität ab. Beispielsweise kann für bestimmte Apps End-to-End-SSL-Verschlüsselung oder

Geofencing erforderlich sein.

- **Bereitstellungsart:** In Citrix Endpoint Management können Sie Apps als MDM- oder MAM-Apps bereitstellen. MDM-Apps werden im App-Store angezeigt. Über diesen Store können Sie Benutzern öffentliche oder native Apps bequem bereitstellen. Abgesehen von der Erzwingung von Einschränkungen auf Geräteebene sind keine weiteren App-Steuerungen erforderlich. Im MAM-Modus haben Sie jedoch die vollständige Kontrolle über die App-Bereitstellung und die Apps selbst. Die Bereitstellung der 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, damit bei etwaigen Problemen nach einem Upgrade ein Fallback möglich ist. Entwickeln Sie 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 im Voraus.
  - 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 umfasst den gesamten 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.

Über das Dashboard steuerbare Vorgänge

March 11, 2024

Das Dashboard der Citrix Endpoint Management-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 der Bildschirm, der beim Anmelden an der Citrix Endpoint Management-Konsole normalerweise als Erstes 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 Volume 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 Citrix 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 keine mobilen Citrix Produktivitätsapps 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. Citrix Endpoint Management enthält eine Reihe von Berichten, anhand derer Sie sich über die Geräte in Ihrer Umgebung informieren können. Einzelheiten finden Sie unter Berichte.

Unterstützung für die rollenbasierte Zugriffssteuerung in Citrix Endpoint Management

March 11, 2024

In Citrix Endpoint Management wird der Benutzer- und Gruppenzugriff auf Citrix Endpoint Management-Systemfunktionen (z. B. Citrix Endpoint Management-Konsole, Selbsthilfeportal, öffentliche API) über die rollenbasierte Zugriffssteuerung (RBAC) beschränkt. In diesem Artikel

werden die in Citrix Endpoint Management integrierten Rollen und Überlegungen zur Wahl eines Citrix Endpoint Management-Supportmodells, für das RBAC verwendet wird, beschrieben.

Integrierte Rollen

Sie können den Zugriff für die folgenden integrierten Rollen ändern und Rollen hinzufügen. Den vollständigen Satz von Zugriffs- und Featureberechtigungen der Rollen und die Standardeinstellungen finden Sie unter Role-Based Access Control Defaults. Eine Definition der einzelnen Features finden Sie unter Rollen mit RBAC konfigurieren.

Administratorrolle

Standardzugriff:

- Vollzugriff auf das System mit Ausnahme des Selbsthilfeportals.
- Standardmäßig können Administratoren einige Supportaufgaben ausführen, z. B. Verbindungsprüfungen oder Supportpaketerstellung.

Überlegungen:

- Benötigen einige oder alle Administratoren Zugriff auf das Selbsthilfeportal? 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.

Benutzer

Standardzugriff:

- Zugriff auf das Selbsthilfeportal, über das authentifizierte Benutzer Registrierungslinks generieren können. Über solche Links können sie ihre Geräte registrieren oder sich selbst eine Registrierungseinladung senden.
- Eingeschränkter Zugriff auf die Citrix Endpoint Management-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 Citrix Endpoint Management-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 Citrix Endpoint Management-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 Citrix Endpoint Management-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 Citrix Endpoint Management-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 Ausbildung ist erforderlich?

Sollen die Benutzer Zugriff auf das Citrix Endpoint Management-Selbsthilfeportal erhalten?
Manche Unternehmen möchten Benutzern zwar keinen Zugriff auf Citrix Endpoint Management gewähren, die Bereitstellung einer Selbsthilfefunktion kann den Support jedoch entlasten. Wenn die RBAC-Standardbenutzerrolle Berechtigungen enthält, die Sie nicht gewähren möchten, können Sie ggf. eine Rolle mit den gewünschten Berechtigungen erstellen. Sie können so viele Rollen erstellen, wie Sie benötigen.

Citrix Support-Prozess

March 11, 2024

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 hilft bei den produktbezogenen Projekten von Citrix, einschließlich der Folgenden:

- Proof of concepts
- Wirtschaftliche Folgenabschätzung
- Infrastrukturintegritätsprüfungen
- Analyse der Entwurfsanforderungen
- Überprüfung des Architekturentwurfs
- Integration
- Operative 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 Citrix Endpoint Management, Citrix Virtual Apps and Desktops, Citrix Hypervisor und NetScaler 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. Informationen zum Support bei Problemen mit Citrix Endpoint Management finden Sie unter Citrix Support Services.

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.

Registrierungseinladungen an Gruppen senden in Citrix Endpoint Management

March 11, 2024

Author:
John Bartel III

In Citrix Endpoint Management 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 Benachrichtigungsvorlagen erstellen und aktualisieren.

Weitere Informationen zur Grundkonfiguration von Benutzerkonten, Rollen, Registrierungssicherheitsmodi und Einladungen finden Sie unter Benutzerkonten, Rollen und Registrierung.

Allgemeine Schritte

1. Gehen Sie in der Citrix Endpoint Management-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 Registrierungssicherheitstyp für Benutzer festlegen.

   - Benutzername + Kennwort
   - Hohe Sicherheit
   - Einladungs-URL
   - Einladungs-URL + PIN
   - Einladungs-URL + Kennwort
   - Zwei Faktoren
   - Benutzername + PIN

   > **Hinweis:**
   >
   > Der Registrierungssicherheitsmodus **Hohe Sicherheit** ist veraltet. 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 Citrix Secure Hub herunterladen und ihre Anmeldeinformationen manuell 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.

   Verwenden Sie für diese Benachrichtigungsvorlagen den konfigurierten SMTP-Server in Citrix Endpoint Management. 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 Citrix Endpoint Management 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 Benutzer senden.

Zertifikatbasierten Authentifizierung mit EWS für Citrix Secure Mail-Pushbenachrichtigungen konfigurieren

March 11, 2024

Damit Citrix Secure Mail-Pushbenachrichtigungen funktionieren, müssen Sie die folgenden Schritte ausführen:

- Konfigurieren Sie Exchange Server für die zertifikatbasierte Authentifizierung. Dies ist vor allem dann erforderlich, wenn Citrix Secure Hub mit zertifikatbasierter Authentifizierung bei Citrix Endpoint Management registriert ist.
- Konfigurieren Sie das virtuelle Verzeichnis für Active Sync und Exchange Web Services (EWS) auf dem Exchange-Mailserver mit zertifikatbasierter Authentifizierung.

Wenn Sie diese Konfigurationen nicht durchführen, schlägt das Abonnement für Citrix Secure Mail-Pushbenachrichtigungen fehl und der Badge in Citrix Secure Mail wird nicht aktualisiert.

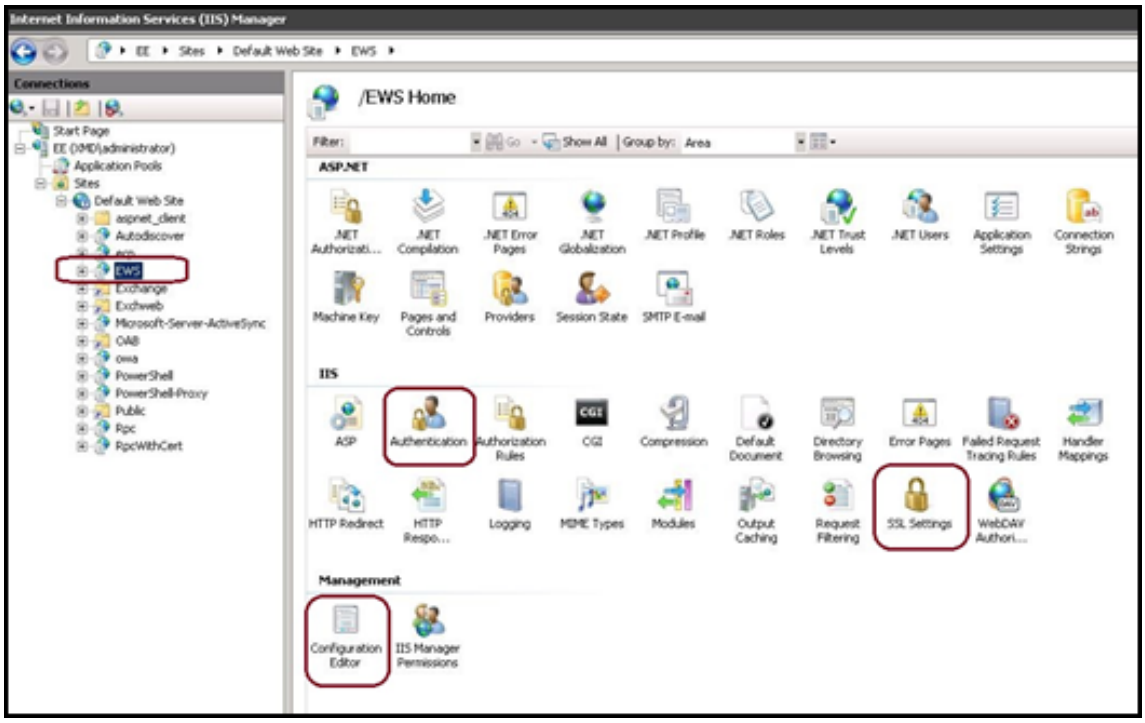
In diesem Artikel wird die Schrittfolge zum Konfigurieren der zertifikatbasierten Authentifizierung beschrieben. Diese Konfigurationen betreffen speziell das virtuelle EWS-Verzeichnis auf Exchange Server.

Führen Sie zu Beginn der Konfiguration zunächst folgende Schritte aus:

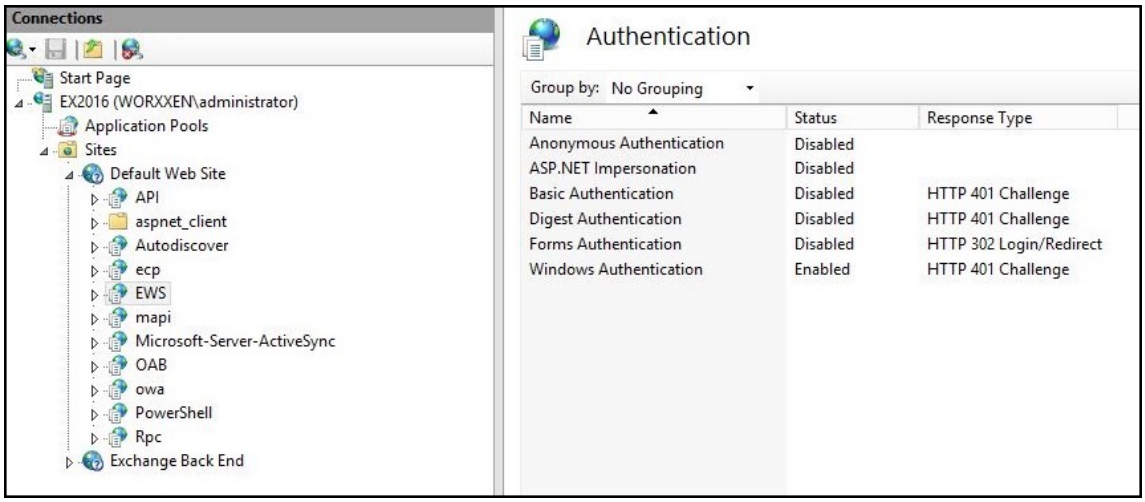
1. Melden Sie sich an allen Servern an, auf denen das virtuelle EWS-Verzeichnis installiert ist.
2. Öffnen Sie IIS-Manager.

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.

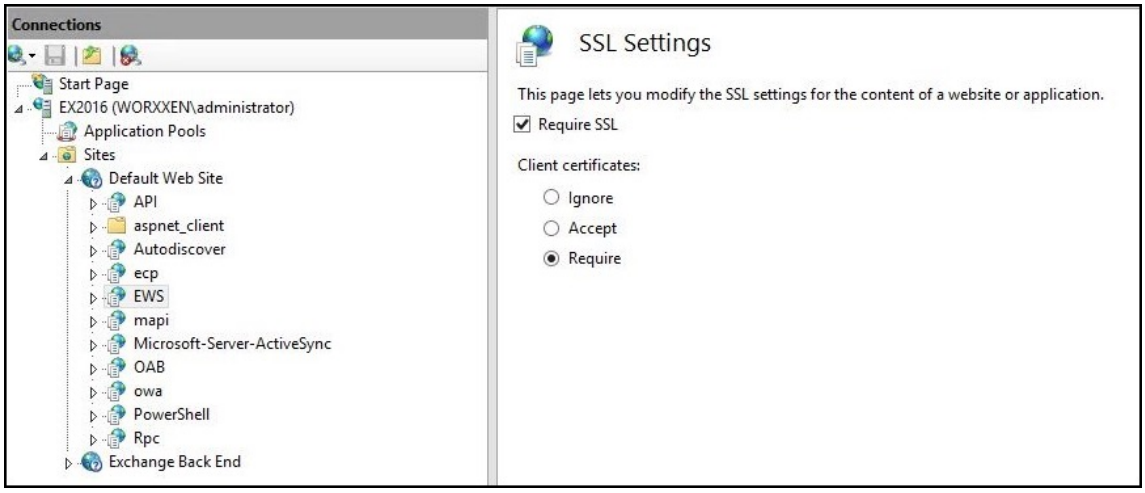


5. Konfigurieren Sie die **SSL-Einstellungen** für das virtuelle EWS-Verzeichnis.

   a) Aktivieren Sie das Kontrollkästchen **SSL erforderlich**.

   b) Klicken Sie unter **Clientzertifikate** auf **Erfordern**. Oder wenn andere EWS-E-Mail-Clients für Exchange Server die Authentifizierung per Benutzername und Kennwort verwenden,

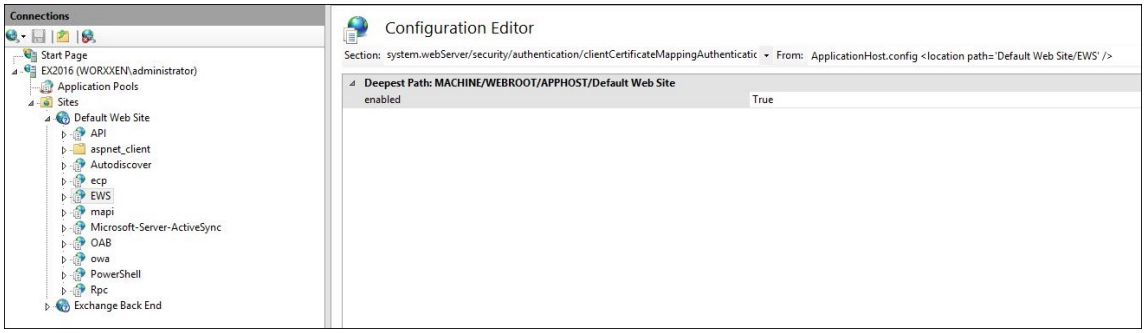
klicken Sie auf **Akzeptieren**.



6. Klicken Sie auf **Konfigurationseditor**. Navigieren Sie in der Dropdownliste **Abschnitt** zum folgenden Abschnitt:

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Setzen Sie **Aktiviert** auf **Wahr**.



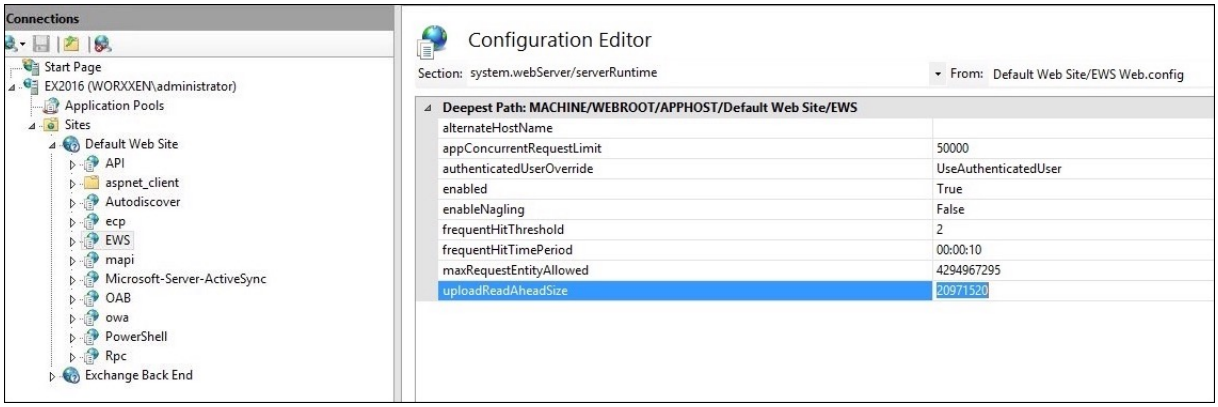
8. Klicken Sie auf **Konfigurationseditor**. Navigieren Sie in der Dropdownliste **Abschnitt** zum folgenden Abschnitt:

   - **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 im Microsoft-Artikel Microsoft IIS server runtime.



Weitere Informationen zur Problembehandlung in Citrix Secure Mail bei Problemen mit iOS-Pushbenachrichtigungen finden Sie in diesem Artikel im Citrix Support Knowledge Center.

Verwandte Informationen

Pushbenachrichtigungen für Citrix Secure Mail für iOS

On-Premises DHA-Server zum Nachweis der Geräteintegrität konfigurieren

March 11, 2024

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 Citrix Endpoint Management-Richtlinie, um den DHA-Dienst on-premises zu aktivieren. Weitere Informationen 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 während der Übertragung, einschließlich:
    * Server-zu-Server-Kommunikation (DHA-Dienst und MDM-Server)
    * Server-zu-Client-Kommunikation (DHA-Dienst 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.

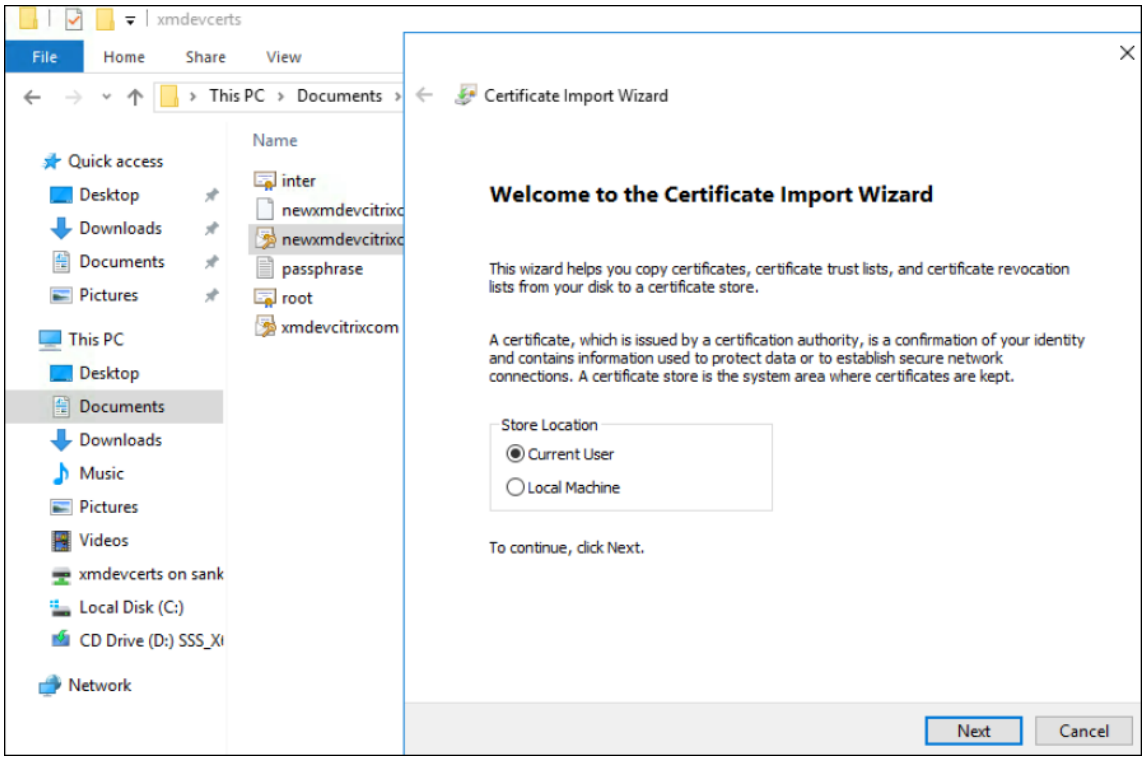
Hinzufügen der DHA-Serverrolle zum Windows-Server

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 **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**.

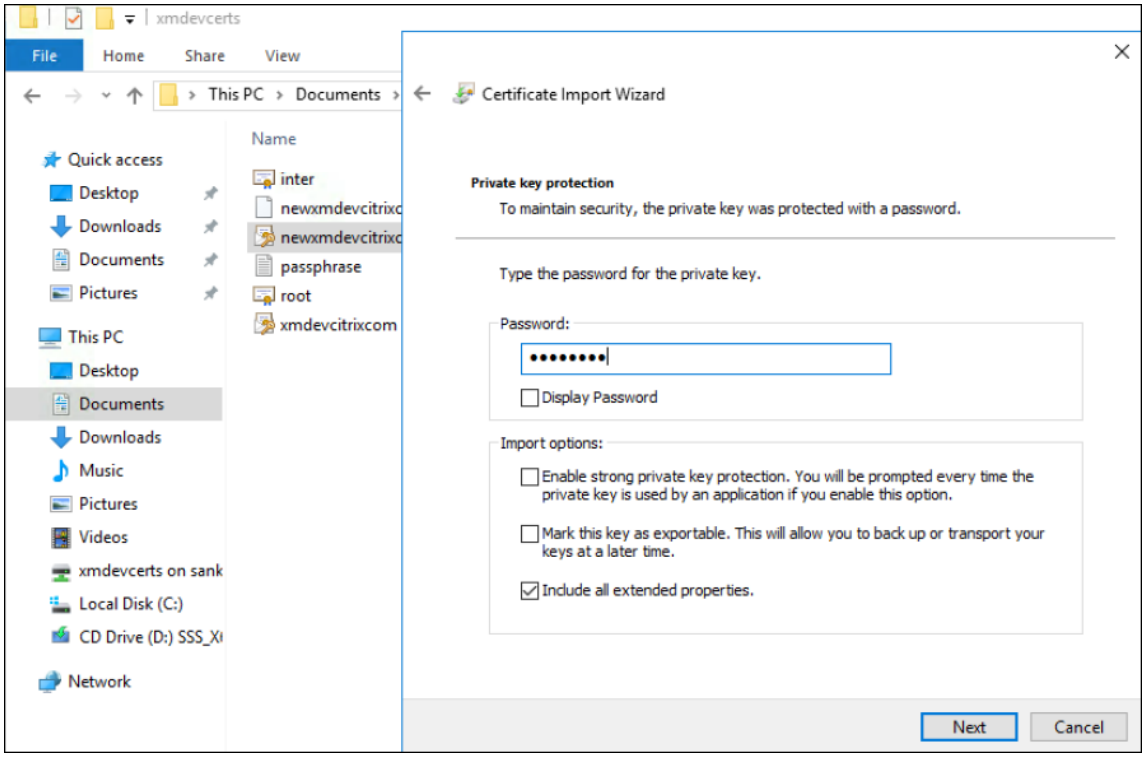
11. Klicken Sie auf der Seite **Rollendienste auswählen** auf **Weiter**.
12. Klicken Sie auf der Seite **Device Health Attestation Service** auf **Weiter**.
13. Klicken Sie auf der Seite **Installationsauswahl bestätigen** auf **Installieren**.
14. Nach Abschluss der Installation klicken Sie auf **Schließen**.

Hinzufügen des SSL-Zertifikats zum Zertifikatspeicher des Servers

1. Gehen Sie zur SSL-Zertifikatsdatei und wählen Sie sie aus.
2. Wählen Sie als Speicherort **Aktueller Benutzer** 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**.

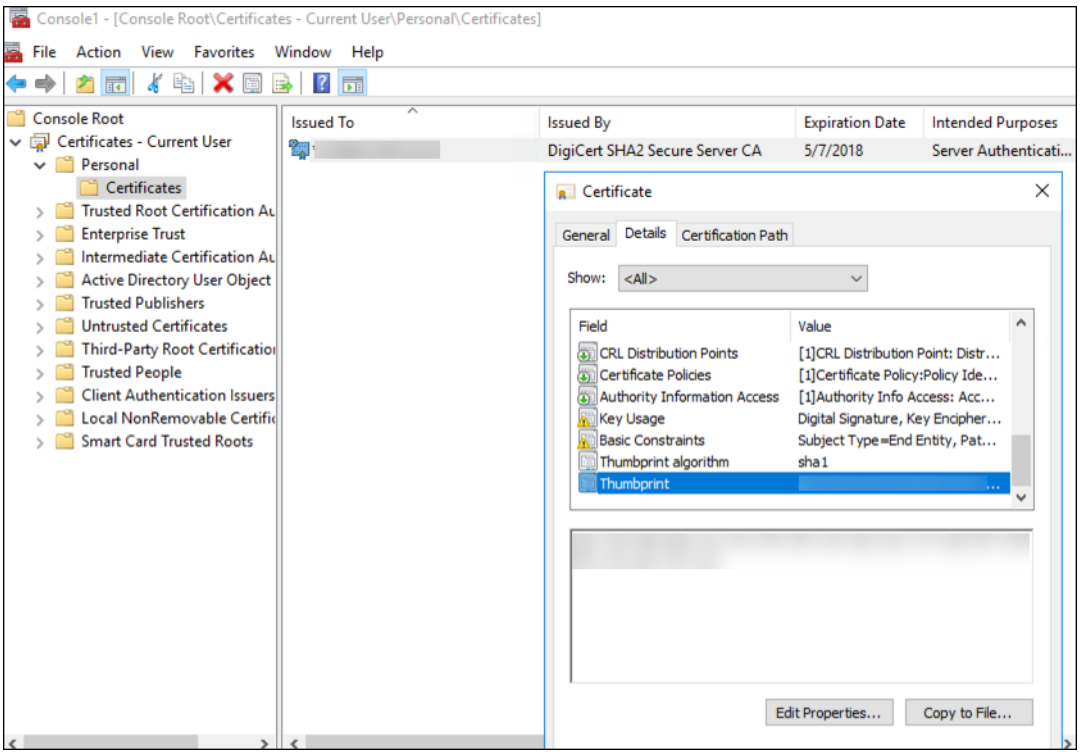
    d) Klicken Sie auf **Hinzufügen**.

    e) Wählen Sie im Dialogfeld “Eigenständiges Snap-In hinzufügen”die Option **Zertifikate**.

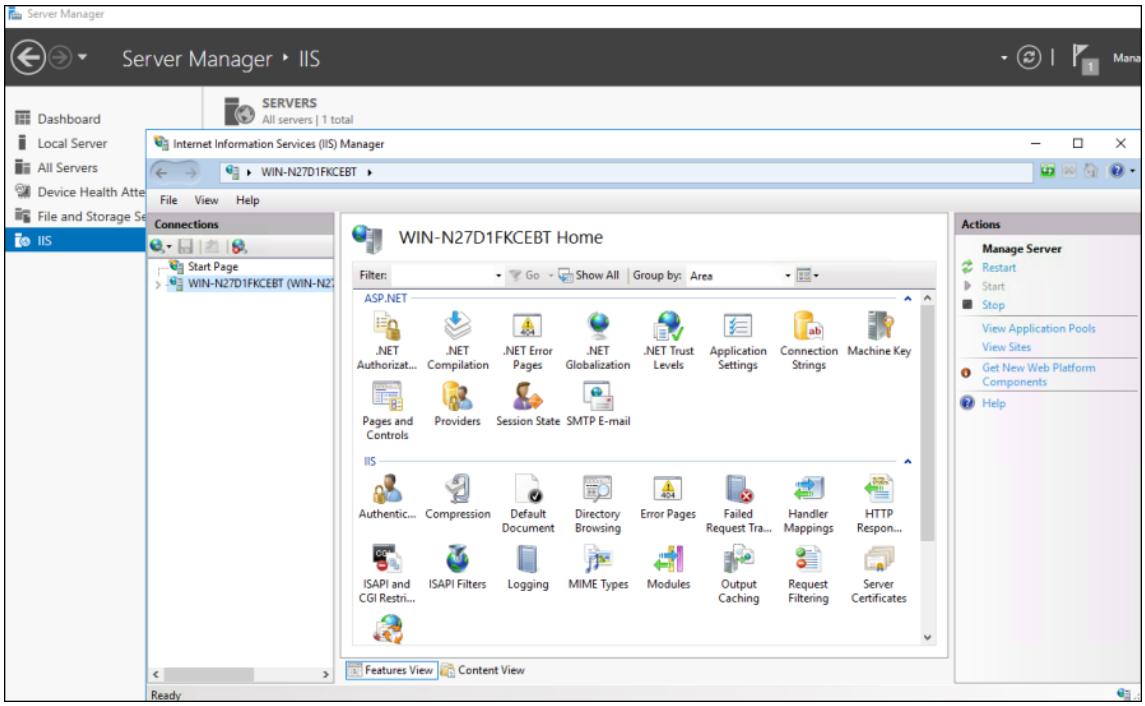
    f) Klicken Sie auf **Hinzufügen**.

    g) Wählen Sie im Dialogfeld “Zertifikat-Snap-In”die Option **Eigenes Benutzerkonto** aus. (Wenn Sie als Dienstkontoinhaber angemeldet sind, wählen Sie **Dienstkonto**.)

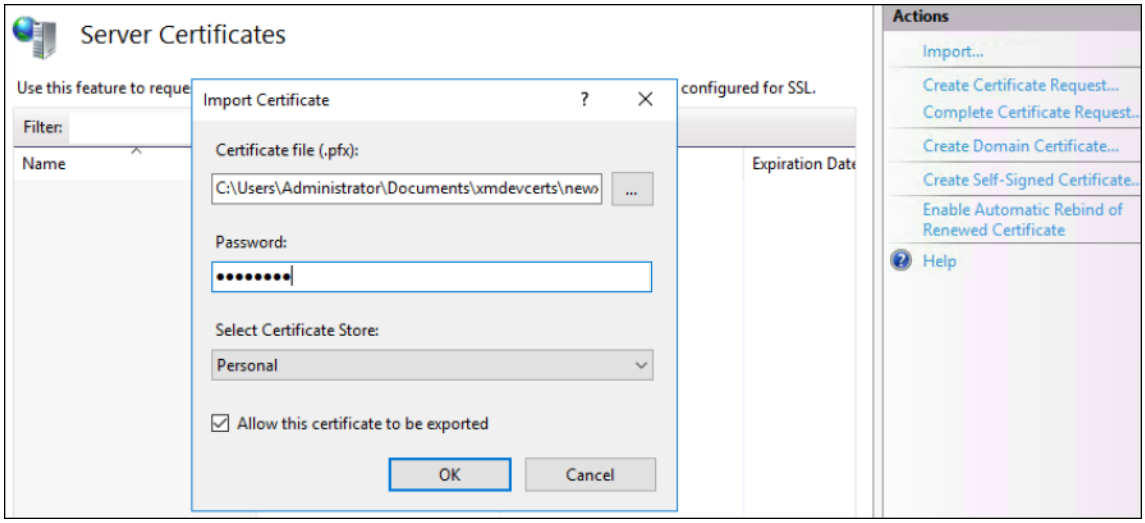
    h) Klicken Sie im Dialogfeld “Computer auswählen”auf **Fertig stellen**.



7. Navigieren Sie zu **Server-Manager > IIS** und wählen Sie das Symbol **Serverzertifikate** aus.

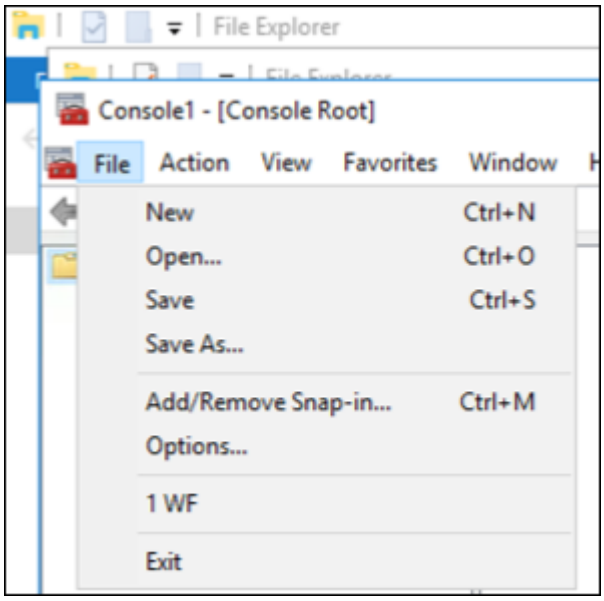


8. Wählen Sie im Menü “Aktion”den Befehl **Importieren...**, um das SSL-Zertifikat zu importieren.

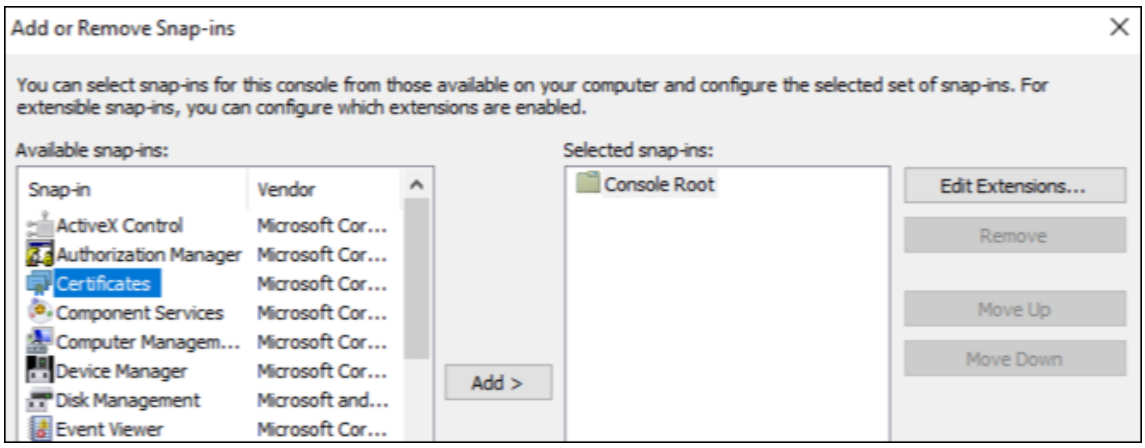


Abrufen und Speichern des Zertifikatfingerabdrucks

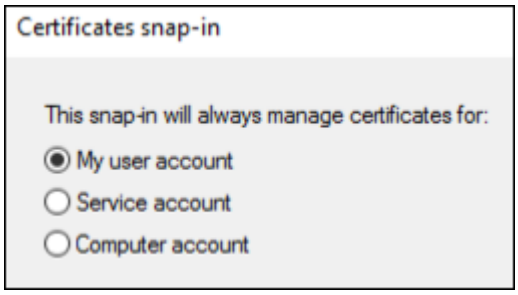
1. Geben Sie in der Suchleiste des Datei-Explorers `mmc` ein.
2. Klicken Sie im Fenster "Konsolenstamm"auf **Datei > Snap-In hinzufügen/entfernen**.



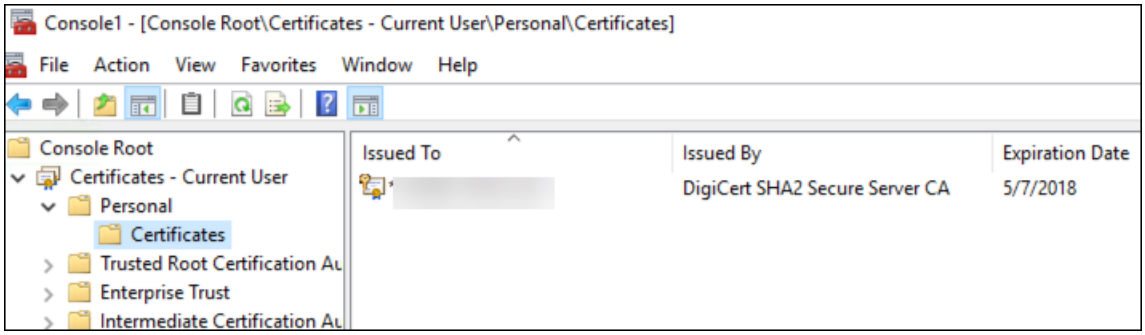
3. Wählen Sie das Zertifikat in der Liste der verfügbaren Snap-Ins aus und fügen Sie es den ausgewählten Snap-Ins hinzu.



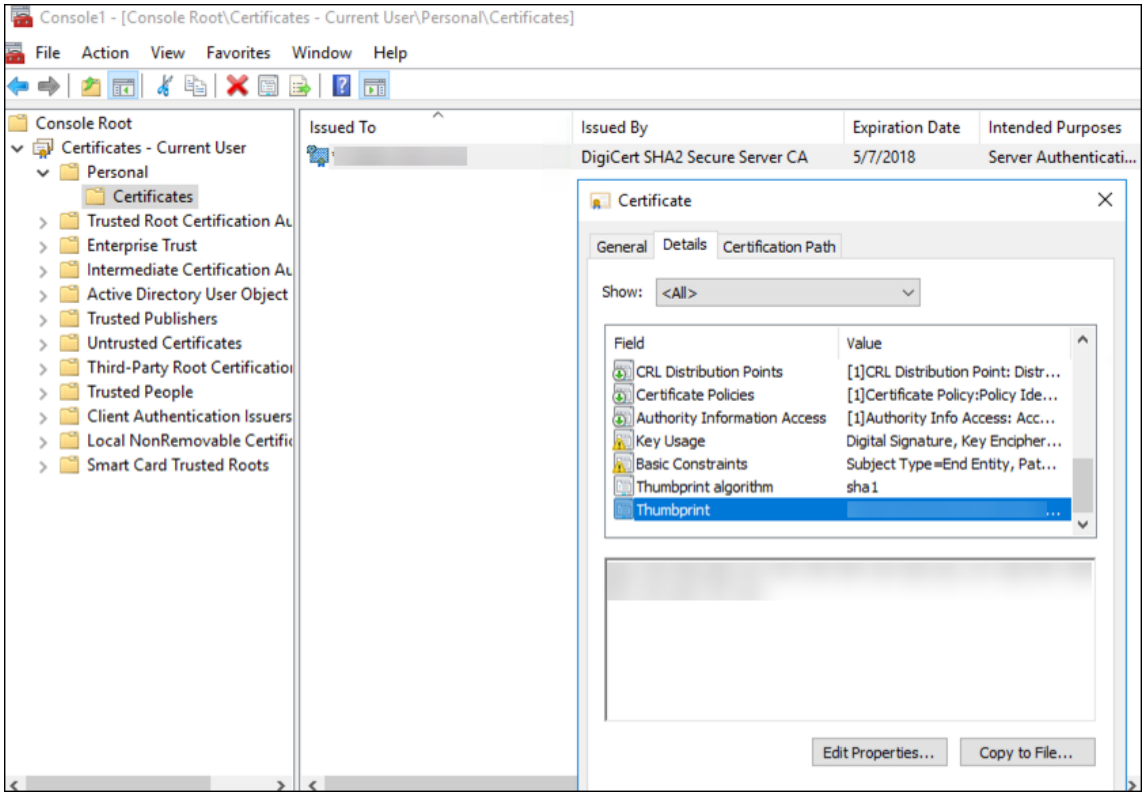
4. Wählen Sie **Eigenes Benutzerkonto**.



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 "[Machine Name]".

```



```
    [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?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
<!--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.

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
    -Force

Get-DHASActiveEncryptionCertificate
<!--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.