Citrix Cloud

Contents

Citrix Cloud

July 2, 2024

> **Hinweis:**
>
> Citrix Virtual Apps Essentials und Citrix Virtual Desktops Essentials haben das End of Sales (EOS) und das End of Life (EOL) erreicht. Weitere Informationen finden Sie unter CTX583004.

Citrix Cloud ist eine Plattform, die Citrix Cloudservices hostet und verwaltet. Über Connectors erhalten Sie Zugriff auf Ressourcen, die sich in einer beliebigen Cloud oder Infrastruktur befinden (z. B. firmeneigenes Rechenzentrum, öffentliche Cloud, private Cloud oder Hybridcloud). Mit nur einer Konsole können Sie Workspaces mit Apps und Daten für Endbenutzer erstellen, verwalten und bereitstellen.

Was ist neu

Unter Citrix Cloud Updates finden Sie aktuelle Informationen zu neuen und kommenden Features in Citrix Cloud und zu den folgenden Diensten:

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

Testen Sie Citrix Cloud

Erleben Sie eine vollständige Produktionsumgebung in einer Machbarkeitsstudie für einen oder mehrere Citrix Cloud Services. Nach dem Registrieren bei Citrix Cloud können Sie über die Konsole eine Testversion der Services anfordern. Diese können Sie nach Ablauf der Testversion in eine Produktionsumgebung umwandeln und so alle Konfigurationen beibehalten. Weitere Informationen finden Sie unter Citrix Cloud Service - Testversionen.

Citrix Cloud Service-Dokumentation

Suchen Sie Informationen zum Einrichten oder Verwalten von Citrix Cloud Services? Unter Citrix Cloud Services finden Sie Links zur Produktdokumentation für alle Cloudservices.

Architektur- und Bereitstellungsressourcen

Citrix Tech Zone enthält zahlreiche Informationen zu Citrix Cloud und zu anderen Citrix Produkten. Hier finden Sie Referenzarchitekturen, Diagramme und technische Papiere, die das Entwickeln und Bereitstellen von Citrix Technologien erleichtern.

Weitere Informationen zu wichtigen Servicekomponenten in Citrix Cloud finden Sie in den folgenden Ressourcen:

- Konzeptdiagramm von Citrix Workspace: Überblick über wichtige Bereiche wie Identität, Intelligenter Workspace und Single Sign-On.
- Referenzarchitekturen: Umfassende Leitfäden für die Planung Ihrer Citrix Workspace-Implementierung, mit Anwendungsfällen, Empfehlungen und zugehörigen Ressourcen.
- Referenzarchitekturen für Citrix DaaS: Ausführliche Anleitungen für die Bereitstellung von Citrix DaaS (früher Virtual Apps and Desktops Service) mit zugehörigen Diensten.

Lernressourcen

Das Citrix Cloud Learning Series-Portal bietet Schulungsmodule zu Citrix Cloud und den zugehörigen Services. Sie können alle Module, vom Überblick bis zu Planung und Aufbau nacheinander durcharbeiten. Beginnen Sie mit folgenden Kursen:

- Fundamentals of Citrix Cloud
- Introduction to Citrix Identity and Authentication
- Moving from StoreFront to Workspace

Die Citrix Education-Videobibliothek enthält Onlinevideos zu wichtigen Bereitstellungsaufgaben und zur Fehlerbehebung bei mit Citrix Cloud Services verwendeten Komponenten. Erfahren Sie mehr über das Installieren von Cloud Connectors, das Registrieren von VDAs sowie andere Aufgaben und über die Fehlerbehebung an diesen Komponenten.

Servicelevelziele

July 2, 2024

Datum des Inkrafttretens: 30. Oktober 2020

Citrix Cloud basiert auf bewährten Methoden der Branche, um einen hohen Grad an Dienstverfügbarkeit zu erreichen.

Diese Servicelevelziele (SLA) beschreiben den Leistungsumfang, den Citrix bei der Bereitstellung von Citrix Cloud Service zusichert. Die SLA sind Teil der Endbenutzervereinbarung (EULA) der Cloud Software Group für abgedeckte Dienste (“Dienste”).

Das Leistungsversprechen für Dienste von Citrix (“Leistungsversprechen”) ist, eine monatliche Verfügbarkeit von mindestens 99,9 % (monatliche Betriebszeit) der Dienste aufrechtzuerhalten. Die monatliche Betriebszeit wird berechnet, indem für einen vollen Monat der prozentuale Anteil der Minuten, während der die Dienstinstanz den Status “Nicht verfügbar”hatte, von 100 % subtrahiert wird. Die Dienste und das Verfügbarkeitsmaß für jeden Dienst sind in der folgenden Tabelle aufgeführt. Die prozentualen Messwerte für monatlichen Betriebszeit schließen durch folgende Faktoren verursachten Ausfallzeiten aus:

- Regelmäßig geplante Wartungsfenster.
- Ausfälle, wenn der Kunde die unter https://docs.citrix.com dokumentierten Konfigurationsanforderungen für den Dienst nicht erfüllt hat, oder durch missbräuchliches Verhalten oder fehlerhafte Eingaben verursachte Ausfälle.
- Ausfälle, die durch die Nutzung eines Dienstes durch den Kunden verursacht werden, wenn Citrix dem Kunden eine Nutzungsänderung empfohlen hatte und der Kunde diese Empfehlung nicht befolgt hat.
- Ausfälle, die durch eine nicht von Citrix verwaltete Komponente verursacht wurden, einschließlich, aber nicht beschränkt auf vom Kunden gesteuerte physische und virtuelle Maschinen, vom Kunden installierte und gepflegte Betriebssysteme, vom Kunden installierte und gesteuerte Netzwerkgeräte oder andere Hardware, vom Kunden definierte und gesteuerte Sicherheitseinstellungen, Gruppenrichtlinien und andere Konfigurationsrichtlinien, mit dem Anbieter der öffentlichen Cloud oder dem Internetdienstanbieter zusammenhängende Störungen sowie andere Ausfälle und Störungen aufgrund anderer Kundensupportfaktoren, die sich der Kontrolle von Citrix entziehen.
- Ausfälle, die dadurch verursacht wurden, dass Mitarbeiter des Kunden, Vertreter, Auftragnehmer oder Lieferanten oder andere Personen sich Zugang zu Kennwörtern oder Geräten des Kunden verschaffen konnten, oder die sich aus der Nichteinhaltung von angemessenen Sicherheitsmaßnahmen durch den Kunden ergeben.
- Versuche des Kunden, Vorgänge auszuführen, die die Dienstberechtigungen überschreiten.
- Dienstunterbrechung aufgrund von höherer Gewalt, einschließlich, aber nicht beschränkt auf Naturkatastrophen, Krieg oder Terrorakte oder Regierungsmaßnahmen.

Es wird kein Leistungsversprechen für Testversionen von Citrix-Produkten, Tech Preview-Versionen, Labs- oder Beta-Dienste angeboten.

Für das von Citrix angebotene Leistungsversprechen müssen Kunden folgende Bedingungen erfüllen:

- Kunden haben die Dienste mit einem laufzeitbasierten Abonnement erworben (1 Jahr Mindestlaufzeit).

- Während des Anspruchszeitraums haben Kunden mindestens 100 Abonnementeinheiten (bzw. mindestens 1000 für Citrix Service Provider) pro Lizenzmodell, das für den Dienst gültig ist.

Citrix Service Provider (CSPs) sind ab 1. Oktober 2018 berechtigt.

Verfügbarkeitsmaß pro Dienst

Service	Monatliche Betriebszeit
Citrix Analytics für Leistung	Die Zeit, in der Benutzer auf Apps zugreifen und Apps und Desktopleistung verbessern können.
Citrix Analytics für Sicherheit	Die Zeit, in der Benutzer Risiken für Benutzerzugriff und Aktivitäten erkennen und mindern können.
NetScaler Console-Dienst	Durchschnittliche Zeit, in der der Service für alle POPs verfügbar ist.
Citrix Endpoint Management	Die Zeit, in der Benutzer über den Dienst auf ihre von Citrix bereitgestellten mobilen Apps und registrierten Geräte zugreifen können.
Citrix Gateway Service für HDX-Proxy	Die Zeit, die Benutzer über den Dienst auf ihre App- oder Desktopsitzung zugreifen können.
NetScaler Intelligent Traffic Management	Die Zeit, die Benutzer über DNS-Abfragen oder HTTP-API-Aufrufe auf Datenverkehrsmanagementfunktionen zugreifen können.
NetScaler SD-WAN Orchestrator	Zeitdauer, die Benutzer über den Service auf ihr SD-WAN Orchestrator-Konto zugreifen und ihr SD-WAN-Netzwerk verwalten können.
Citrix Secure Private Access	Die Zeit, die Benutzer über den Service auf ihre SaaS- oder interne Web-App zugreifen können.
Citrix DaaS	Die Zeit, die Benutzer über den Dienst auf ihre App- oder Desktopsitzung zugreifen können.
Citrix Workspace	Wie oben für Komponentendienste angegeben, schließt jedoch die Verfügbarkeit für jede Komponente ein. Gutschriften können anteilig gewährt werden, wenn sich ein Anspruch nicht auf alle Komponenten bezieht.

> **Hinweis:**
>
> Citrix DaaS ist der neue Name für Citrix Virtual Apps Service, Citrix Virtual Desktops Service und Citrix Virtual Apps and Desktops Service.

Leistungsversprechen und Abhilfemaßnahmen

Sollte Citrix das Leistungsversprechen in mindestens 3 von 5 aufeinanderfolgenden Monaten am oder nach dem SLA-Stichtag nicht erfüllen, ist das ausschließliche Rechtsmittel eine Dienstgutschrift von 10 % auf Monatsbasis für die Monate, in denen Citrix das Leistungsversprechen nicht erfüllt, bei der nächsten jährlichen Dienstverlängerung in der unmittelbaren Verlängerungsphase für den gleichen Dienst und die gleiche Anzahl an betroffenen Einheiten.

- Monatlicher Betriebszeitprozentsatz: > 99,9 %
- Dienstgutschrift: 10 % für die betroffenen Monate (als Gutschein für den Kunden)

Um die oben genannte Gutschrift zu erhalten, muss der Kunde die EULA einhalten und der Kunde muss die Störung innerhalb von dreißig (30) Tagen nach dem Ende des letzten Monats des aufeinanderfolgenden Fünfmonatszeitraums melden, für den eine Gutschrift angefordert wird. Anweisungen, wie Sie mögliche Verstöße gegen diese Servicelevelziele melden, finden Sie unter CTX237141.

In der Anforderung müssen betroffene Dienste identifiziert sowie die Daten, Zeiten und Dauer der Nichtverfügbarkeit definiert werden. Darüber hinaus müssen Protokolle oder Datensätze, die die Nichtverfügbarkeit bestätigen, die betroffenen Benutzer und deren Standorte sowie jegliche technische Unterstützung oder durchgeführte Korrektur angegeben werden. Pro Dienst wird nur eine Gutschrift für die jeweilige Anzahl von Monaten ausgestellt, wobei für die gesamten Monate der Verlängerung ein Maximum von einer Gutschrift von 10 % gilt. Der Kunde muss die Gutschrift beim Kauf der Verlängerung vorlegen.

Wenn Sie die Verlängerung über einen Vertriebspartner erwerben, erhalten Sie eine Gutschrift über den Vertriebspartner. Die Gutschrift, die wir Ihnen bei einem direkten Kauf geben oder bei einem indirekten Kauf an Ihren Vertriebspartner weitergeben, basiert auf dem anteiligen kombinierten Verkaufspreis der Verlängerung für dieselbe Anzahl von Einheiten. Citrix kontrolliert keine Vertriebspreise oder Vertriebsgutschriften. Gutschriften umfassen kein Recht zur Verrechnung mit Zahlungen, die an Citrix oder einen Vertriebspartner gehen. Diese Bedingungen werden von Citrix gelegentlich aktualisiert. Bei Aktualisierungen passt Citrix ebenfalls das Veröffentlichungsdatum der Servicelevelziele an. Änderungen gelten nur für Ihre neu erworbenen Dienste oder Dienstverlängerungen am oder nach dem aktuellen Veröffentlichungsdatum.

Hinweise zu Drittanbietern

November 2, 2023

- Citrix Cloud Third Party Notifications (PDF)
- Citrix Analytics Service Third Party Notifications (PDF)
- Citrix DaaS Third Party Notifications (PDF)
- Citrix DaaS Standard for Azure Third Party Notifications (PDF)
- Remote Browser Isolation (formerly Secure Browser) (PDF)
- Citrix Endpoint Management Third Party Notifications (PDF)
- Citrix Cloud Linux VDA Image Service Third Party Notices (PDF)
- Connector Appliance for Cloud Services Third Party Notices (PDF)
- Citrix Gateway Service Third Party Notices (PDF)
- Citrix Device Posture Service Third Party Notices (PDF)

> **Hinweis:**
>
> Citrix DaaS war früher Citrix Virtual Apps and Desktops Service. Citrix DaaS Standard für Azure war früher Citrix Virtual Apps and Desktops Standard für Azure.

So erhalten Sie Hilfe und Unterstützung

July 2, 2024

In diesem Artikel wird beschrieben, wie Sie Probleme beim Erstellen eines Kontos oder bei der Anmeldung bei Citrix Cloud oder einer anderen Citrix Website behandeln und Hilfe erhalten. Der Artikel enthält überdies weitere Ressourcen zur Selbsthilfe und Optionen für Support unter Anleitung.

> **Wichtig:**
>
> Tritt bei der Anmeldung bei einer Citrix Website oder bei der Registrierung für die Multifaktorauthentifizierung ein Problem auf, lesen Sie zunächst den vorliegenden Artikel zur Problembehandlung bei Ressourcen. Wenn Sie das Problem mit diesen Ressourcen nicht lösen können, wenden Sie sich an den Citrix Customer Service unter https://www.citrix.com/contact/customer-service.html.

Erstellen eines Kontos

Für den Zugriff auf bestimmte Ressourcen auf der Citrix Website ist ein Citrix Konto erforderlich. Dazu gehören u. a. Diskussionforen, Schulungen, bestimmte Produktdownloads und der technische Sup-

port von Citrix.

Wenden Sie sich an Citrix, um ein neues Citrix-Konto für Ihr Unternehmen zu erstellen. Folgende Methoden sind möglich:

- Wenden Sie sich an den Citrix Customer Service.
- Wenden Sie sich an einen Citrix Partner oder ein Citrix-Vertriebsbüro in Ihrer Nähe.

Wenn Sie bereits ein Citrix-Konto haben, können Sie ein Citrix Cloud-Konto erstellen und den Onboarding-Prozess abschließen. Führen Sie hierfür die unter Citrix Cloud-Konto erstellen beschriebenen Aufgaben aus.

Bei Problemen mit der Registrierung bei Citrix Cloud wenden Sie sich bitte an den Citrix Customer Service.

Bei Citrix Websites und Citrix Cloud anmelden

Wenn Sie Probleme bei der Anmeldung bei einer Citrix Website mit Ihrem Citrix Konto haben, nutzen Sie die folgenden Ressourcen zur Problembehandlung:

- CTX228792: Troubleshooting login issues on Citrix websites
- CTX283814: Sign in issue after setting up Citrix account

Ich kann die Multifaktorauthentifizierung nicht einrichten bzw. nicht zur Authentifizierung nutzen, wenn ich mich bei meinem Citrix-Konto anmelde

Informationen zur Problembehandlung finden Sie in den folgenden Artikeln:

- CTX461297: How to Enroll into Multi Factor Authentication (MFA)
- CTX463758: How to recover access to your account

Wenn Sie sich weiterhin nicht mit der Multifaktorauthentifizierung anmelden können, wenden Sie sich an den Citrix Customer Service unter https://www.citrix.com/contact/customer-service.html.

Wie finde ich den Benutzernamen meines Citrix-Kontos oder setze mein Citrix-Kennwort zurück?

Führen Sie folgende Schritte aus, um den Benutzernamen Ihres Citrix-Kontos zu überprüfen und Ihr Kennwort zurückzusetzen.

1. Besuchen Sie https://www.citrix.com/welcome/request-password.html.
2. Benutzernamen Ihres Citrix-Kontos überprüfen:
    a) Wählen Sie unter **Find my account by** die Option **Email**.

b) Geben Sie die mit Ihrem Citrix-Konto verknüpfte E-Mail-Adresse ein.

3. Kennwort für Ihr Citrix-Konto zurücksetzen:

   a) Wählen Sie unter **Find my account by** die Option **User name**.
   b) Geben Sie den Benutzernamen Ihres Citrix-Kontos ein.

4. Klicken Sie auf **Find My Account**.

Wenn Ihr Konto über Ihre E-Mail-Adresse gefunden wird, sendet Citrix Ihnen eine E-Mail mit dem Benutzer- und Firmennamen, der mit Ihrer E-Mail-Adresse verknüpft ist. Wenn Ihr Konto über Ihren Citrix-Benutzernamen gefunden wird, sendet Citrix Ihnen eine E-Mail mit Anweisungen zum Zurücksetzen Ihres Kennworts.

Wenn Sie nach mehreren Minuten keine E-Mail erhalten, lesen Sie Citrix-E-Mails werden nicht in meinem E-Mail-Posteingang angezeigt in diesem Artikel.

Ich kann mich nicht bei Citrix Cloud anmelden

- Stellen Sie sicher, dass Sie die richtigen Kontoanmeldeinformationen zur Anmeldung verwenden. Um den Benutzernamen Ihres Kontos zu überprüfen, wählen Sie unter https://citrix.cloud.com/ die Option **Haben Sie Ihren Benutzernamen vergessen?** und geben Sie Ihre E-Mail-Adresse ein. Citrix sendet Ihnen eine E-Mail mit dem Benutzernamen Ihres Kontos.
- Möglicherweise müssen Sie Ihr Kennwort zurücksetzen. Citrix Cloud fordert Sie auf, Ihr Kennwort zu ändern, wenn Sie sich in letzter Zeit nicht angemeldet haben oder wenn Ihr Kennwort nicht stark genug ist. Weitere Informationen finden Sie in diesem Artikel unter Ändern des Kennworts.
- Möglicherweise müssen Sie sich mit einer benutzerdefinierten Anmelde-URL anmelden. Wenn Ihr Citrix Cloud-Konto Azure AD, Google Cloud Identity oder SAML zur Authentifizierung von Administratoren verwendet, wählen Sie **Mit Firmenanmeldeinformationen anmelden** und geben Sie die Anmelde-URL Ihres Unternehmens ein. Sie können dann Ihre Firmenanmeldeinformationen eingeben, um auf das Citrix Cloud-Konto Ihres Unternehmens zuzugreifen. Wenden Sie sich an Ihren Administrator, wenn Sie die Anmelde-URL Ihres Unternehmens nicht kennen.

Wenden Sie sich an den Citrix Customer Service, wenn Sie sich weiterhin nicht bei Citrix Cloud anmelden können.

Keine Citrix-E-Mails im E-Mail-Posteingang

Wenn Citrix Ihnen eine E-Mail sendet, um Ihre Identität für die Multifaktorauthentifizierung zu verifizieren bzw. weil Sie Ihr Citrix-Konto suchen oder Kennwort ändern , erhalten Sie die E-Mail in der Regel innerhalb weniger Minuten. Wenn Sie diese E-Mails nicht erhalten:

- Überprüfen Sie die für Ihr Citrix Konto registrierte E-Mail-Adresse auf Korrektheit. Wenn Sie kürzlich Ihre E-Mail-Adresse geändert haben, wird die Bestätigungs-E-Mail möglicherweise an Ihre alte Adresse gesendet.
- Die E-Mail wurde möglicherweise versehentlich gefiltert. Überprüfen Sie den Spamordner und den Papierkorb in Ihrem E-Mail-Client. Sie können Ihr E-Mail-Konto auch nach E-Mails von `donotreplynotifications@citrix.com` oder `cloud@citrix.com` durchsuchen.
- Ihre Firewall hat die E-Mail möglicherweise blockiert. Stellen Sie sicher, dass die folgenden Adressen als vertrauenswürdige Absender aufgeführt sind:
  - `donotreplynotifications@citrix.com`
  - `cloud@citrix.com`
  - `CustomerService@citrix.com`

Wenn Sie die E-Mail nach einigen Minuten nicht erhalten oder ein anderes Problem bei der Anmeldung auftritt, wenden Sie sich an den Citrix Customer Service.

Multifaktorauthentifizierung für Citrix Konten und Citrix Cloud-Konten

Citrix-Kunden müssen sich mit Multifaktorauthentifizierung bei ihrem Citrix-Konto und bei Citrix Cloud anmelden. Die Registrierung mit Multifaktorauthentifizierung ist in folgenden Situationen erforderlich:

- Ein Neukunde meldet sich zum ersten Mal bei seinem Citrix-Konto an.
- Ein Citrix-Kunde führt das Onboarding für ein neues Citrix Cloud-Konto durch und hat sich noch nicht bei der Multifaktorauthentifizierung registriert.
- Ein neuer Administrator tritt einem vorhandenen Citrix Cloud-Konto bei.

Wenn Sie bei der Anmeldung bei Ihrem Citrix-Konto oder bei Citrix Cloud aufgefordert werden, sich für die Multifaktorauthentifizierung zu registrieren, führen Sie die Schritte unter CTX461297: How to Enroll into Multi Factor Authentication (MFA) aus.

Weitere Informationen zur Multifaktorauthentifizierung für Citrix-Konten finden Sie unter CTX463482: Frequently asked questions when setting up Multi-Factor Authentication (MFA) on Citrix properties.

Kontowiederherstellung

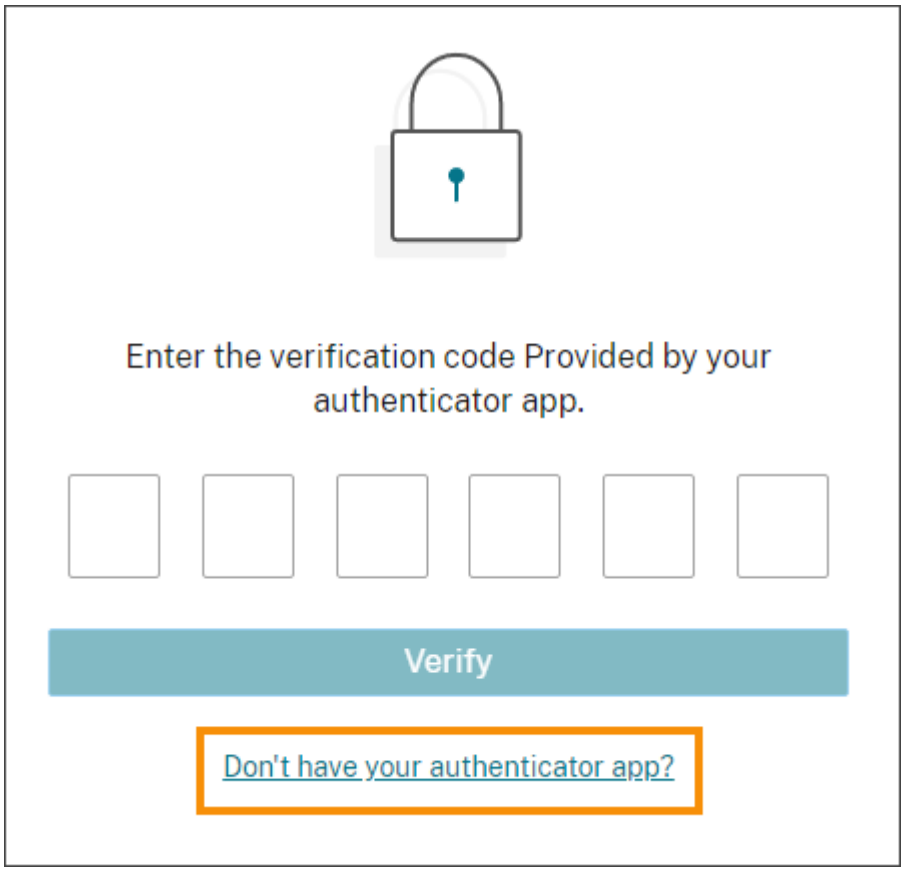
Wenn Sie Hilfe beim Wiederherstellen der Anmeldeinformationen für Ihr Citrix-Konto benötigen, lesen Sie Wie finde ich den Benutzernamen meines Citrix-Kontos oder setze mein Citrix-Kennwort zurück? in diesem Artikel.

Wenn Sie Hilfe bei der Wiederherstellung des Zugriffs auf Ihr Citrix Cloud-Konto benötigen, können Sie die Wiederherstellungsmethoden verwenden, die Sie bei der Registrierung für die Multifaktorauthentifizierung konfiguriert haben. Zu diesen Wiederherstellungsmethoden gehören:

- Ein einmaliger Code, den Citrix an Ihre Wiederherstellungs-E-Mail-Adresse sendet.
- Ein Backupcode aus der Liste, die Sie bei der Registrierung für die Multifaktorauthentifizierung generiert haben.
- Ein Telefonanruf vom Citrix Support an Ihre Telefonnummer für die Wiederherstellung, um Ihre Identität zu überprüfen und Ihnen den Zugriff auf Ihr Konto zu ermöglichen. Die Einrichtung einer Telefonnummer für die Wiederherstellung ist bei der Registrierung für die Multifaktorauthentifizierung erforderlich.

Anmeldung mit einer Wiederherstellungsmethode:

1. Geben Sie auf der Anmeldeseite für das Citrix Konto oder Citrix Cloud Ihren Citrix Cloud-Benutzernamen und das Kennwort ein und wählen Sie dann **Anmelden**.
2. Wenn Sie aufgefordert werden, den Code Ihrer primären Multifaktorauthentifizierungsmethode einzugeben, wählen Sie **Verwenden Sie eine Wiederherstellungsmethode**.



3. Wählen Sie gegebenenfalls die gewünschte Wiederherstellungsmethode aus. Wenn Sie neben der Telefonnummer nur eine weitere Wiederherstellungsmethode konfiguriert haben, fordert

Citrix Cloud Sie automatisch auf, diese Methode zu verwenden.

4. Wenn Sie Ihre Wiederherstellungs-E-Mail-Adresse verwenden, geben Sie den von Citrix gesendeten einmaligen Code ein und wählen Sie **Verifizieren** aus. Wenn Sie den Code nicht innerhalb einer gewissen Zeit erhalten, wählen Sie **E-Mail erneut senden**. Nach der Verifizierung sind Sie bei Citrix Cloud angemeldet.
5. Wenn Sie einen Backupcode verwenden, geben Sie den Code bei Aufforderung ein und wählen Sie **Verifizieren und fortfahren**. Sie werden bei Citrix Cloud angemeldet und per E-Mail informiert, dass ein Backupcode verwendet wurde und wie viele gültige Backupcodes verbleiben. Notieren oder löschen Sie den verwendeten Backupcode, damit Sie ihn nicht erneut verwenden.
6. Wenn Sie Ihre Wiederherstellungs-E-Mail-Adresse oder Backupcodes nicht verwenden können:
   a) Wählen Sie **Kontaktieren Sie Citrix Support**.
   b) Geben Sie im Formular ein, welches Problem aufgetreten ist. Ein Citrix Supportmitarbeiter ruft Sie unter der Telefonnummer für die Wiederherstellung an, um Ihre Identität zu überprüfen. Anschließend sendet Ihnen der Mitarbeiter einen Wiederherstellungscode, mit dem Sie sich anmelden können.
   c) Kehren Sie zur Anmeldeseite von Citrix Cloud zurück und melden Sie sich mit Ihren Citrix Cloud-Anmeldeinformationen an.
   d) Wenn Sie zur Eingabe eines Codes aufgefordert werden, geben Sie den vom Citrix Support erhaltenen Wiederherstellungscode ein und wählen **Verifizieren**.

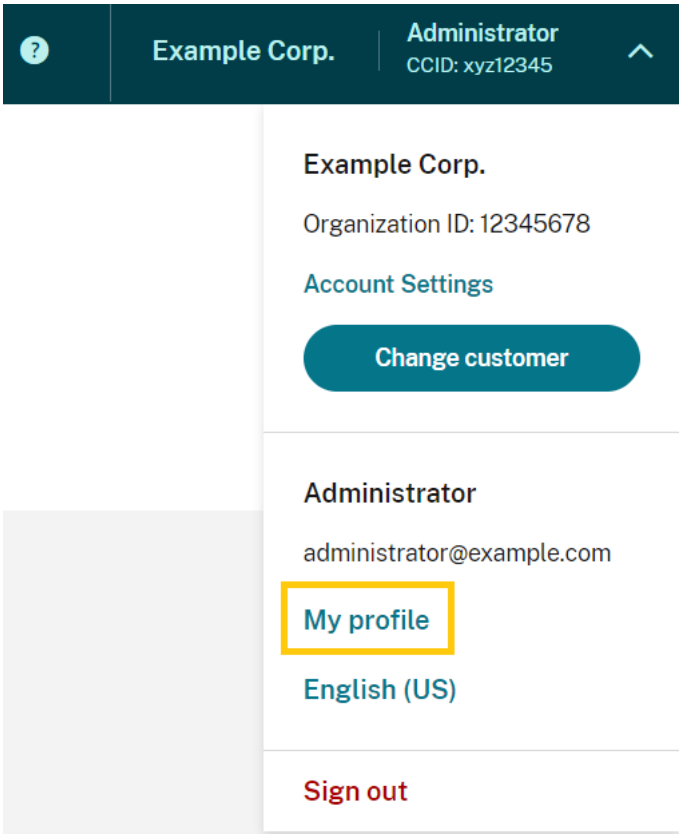
Aktualisieren Sie nach der Anmeldung Ihre Kontowiederherstellungsmethoden, um Verzögerungen bei der Anmeldung künftig zu vermeiden.

Einstellungen für die Multifaktorauthentifizierung aktualisieren

Sie können Ihre Zugriffs- und Wiederherstellungseinstellungen für die Multifaktorauthentifizierung auf der Seite **Meine Einstellungen** aktualisieren. Sie können über Ihr Citrix Konto oder über Citrix Cloud auf diese Seite zugreifen.

So greifen Sie auf die Seite **Meine Einstellungen** zu:

1. Melden Sie sich bei Ihrem Citrix Konto bzw. bei Citrix Cloud an.
2. Gehen Sie von Ihrem Citrix Konto aus zu https://accounts.cloud.com/core/profile.
3. Wählen Sie in Citrix Cloud im Menü oben rechts **Meine Einstellungen** aus.



Informationen zum Ändern Ihrer Einstellungen für die Multifaktorauthentifizierung finden Sie in den folgenden Abschnitten:

- Primäre MFA-Methode verwalten
- MFA-Wiederherstellungsmethoden verwalten

Ändern Ihres Kennworts

Wenn Sie Ihr Kontokennwort vergessen haben, wählen Sie **Kennwort vergessen?** und geben Sie bei Erscheinen der Aufforderung Ihren Benutzernamen ein. Citrix sendet eine E-Mail an die E-Mail-Adresse Ihres Kontos mit einem Link zum Einrichten eines neuen Kennworts. Wenn Sie diese E-Mail nach mehreren Minuten nicht erhalten oder zusätzliche Hilfe benötigen, wenden Sie sich an den Citrix Customer Service.

Citrix Cloud fordert Sie beim Anmelden möglicherweise auf, Ihr Kennwort zurückzusetzen. Diese Aufforderung wird in folgenden Situationen angezeigt:

- Ihr Kennwort entspricht nicht den Komplexitätsvorgaben von Citrix Cloud.
- Ihr Kennwort enthält im Wörterbuch enthaltene Wörter.
- Ihr Kennwort wird in einer bekannten Datenbank mit gefährdeten Kennwörtern aufgeführt.
- Sie haben sich in den vergangenen 60 Tagen nicht bei Citrix Cloud angemeldet.

Kennwörter müssen 8 bis 128 Zeichen lang sein und Folgendes enthalten:

- Mindestens eine Zahl
- Mindestens einen Großbuchstaben
- Mindestens ein Symbol: ! @ # $ % ^ * ? + = -

Wenn Sie dazu aufgefordert werden, wählen Sie **Kennwort zurücksetzen**, um ein neues sicheres Kennwort für Ihr Konto zu erstellen.

Integrität des Cloud-Diensts

Das Citrix Cloud-Integritäts-Dashboard (https://status.cloud.com) bietet einen Überblick über die Echtzeitverfügbarkeit der Citrix Cloud-Plattform und der Services für jede geografische Region. Wenn Probleme mit Citrix Cloud auftreten, überprüfen Sie das Cloud-Integritäts-Dashboard, um sicherzustellen, dass Citrix Cloud bzw. einzelne Services normal funktionieren.

Weitere Informationen zum Cloud-Integritäts-Dashboard finden Sie unter Integrität des Citrix Cloud-Diensts.

Supportforen für Citrix Cloud

In den Supportforen für Citrix Cloud können Sie Hilfe erhalten, Feedback und Verbesserungsvorschläge hinterlassen, Unterhaltungen anderer Benutzer anzeigen oder selbst ein Thema diskutieren.

Citrix Supportmitarbeiter verfolgen diese Foren und beantworten Ihre Fragen. Andere Mitglieder der Citrix Cloud-Community können ebenfalls Hilfe anbieten oder mitdiskutieren.

Sie müssen sich nicht anmelden, um Forumsbeiträge zu lesen. Um selbst einen Kommentar zu posten oder auf ein Thema zu antworten, müssen Sie jedoch angemeldet sein. Verwenden Sie zur Anmeldung die Anmeldeinformationen für Ihr Citrix Konto oder die E-Mail-Adresse und das Kennwort, die Sie beim Erstellen Ihres Citrix Cloud-Kontos angegeben haben.

Supportartikel und Dokumentation

Citrix stellt umfangreiche Produkt- und Supportinhalte bereit, die Ihnen helfen, Citrix Cloud optimal zu nutzen und Probleme mit Citrix Produkten zu lösen.

Citrix Support Knowledge Center

Das Knowledge Center bietet Inhalte zur Fehlerbehebung sowie Sicherheitsbulletins und Hinweise zu Softwareupdates für alle Citrix Produkte. Geben Sie einfach eine Suchzeichenfolge ein, um relevante Inhalte zu finden. Sie können das Suchergebnis nach Produkt und Artikeltyp filtern.

Citrix Tech Zone

Citrix Tech Zone enthält Informationen zu Citrix Cloud und zu anderen Citrix Produkten. Hier finden Sie Referenzarchitekturen, Diagramme, Videos und technische Papiere, die das Entwickeln und Bereitstellen von Citrix Technologien erleichtern.

Benutzerhilfe

Die Citrix Benutzerhilfe bietet Citrix Produktdokumentationen nur für Endbenutzer in Ihrer Organisation. In der Benutzerhilfe finden Sie leicht verständliche Anweisungen für Endbenutzer-orientierte Produkte wie die Citrix Workspace-App und Citrix SSO. Die Endbenutzerdokumentation für ShareFile finden Sie unter Citrix Files-Apps auf der Website mit der ShareFile-Produktdokumentation.

Technischer Support

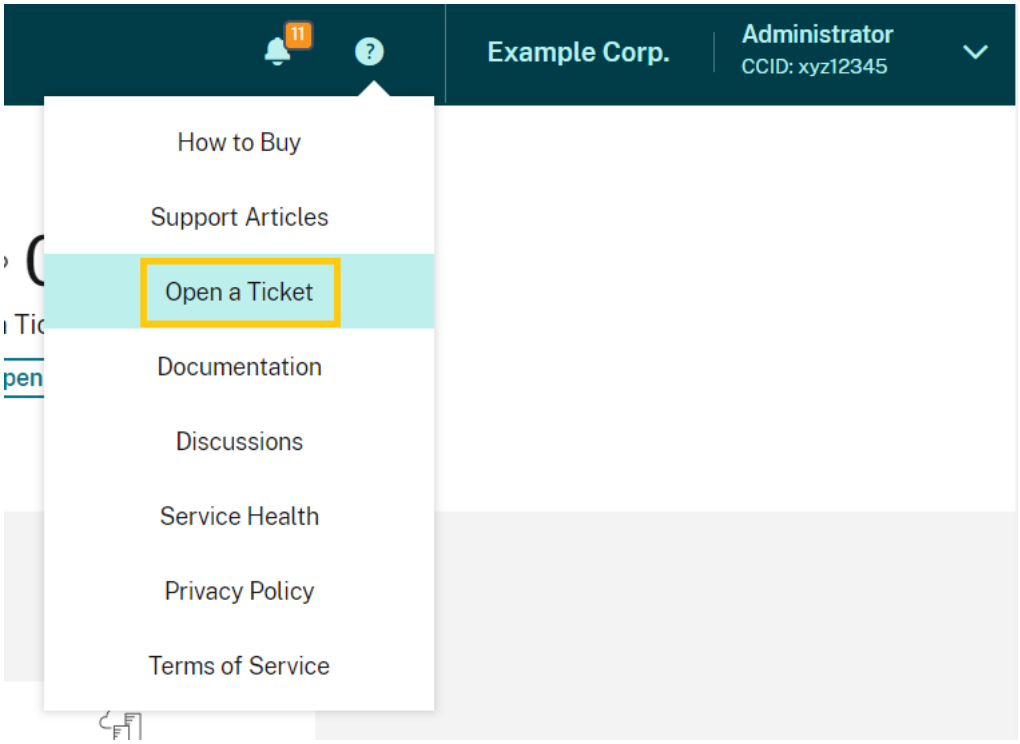
Bei auftretenden Problemen, die technische Hilfe erfordern, können Sie im My Support-Portal einen Supportfall öffnen oder mit einem Supportmitarbeiter von Citrix chatten.

Um auf das My Support-Portal zuzugreifen, gehen Sie zu https://support.citrix.com/case/manage.

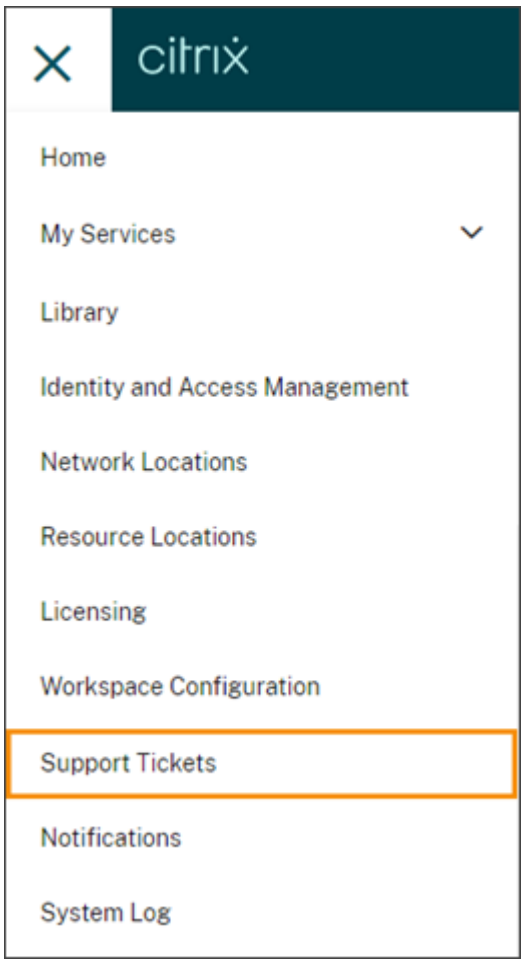
Um von Citrix Cloud aus auf das Portal zuzugreifen, benötigen Sie die Berechtigung **Supporttickets**. Weitere Informationen zu Administratorberechtigungen finden Sie unter Ändern von Administratorberechtigungen.

Von der Citrix Cloud-Verwaltungskonsole aus können Sie mit den folgenden Methoden auf My Support zugreifen:

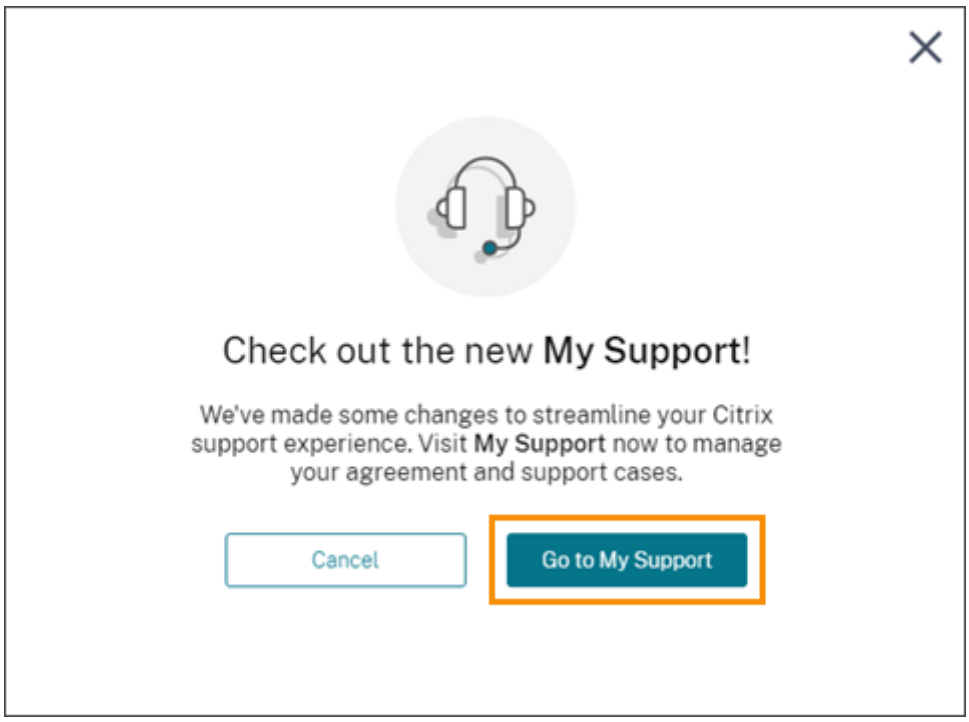
- Wählen Sie unter dem **Hilfesymbol** oben rechts auf dem Bildschirm die Option **Ticket erstellen** aus.



- Wählen Sie im Citrix Cloud-Menü oben links auf dem Bildschirm die Option **Supporttickets** aus.

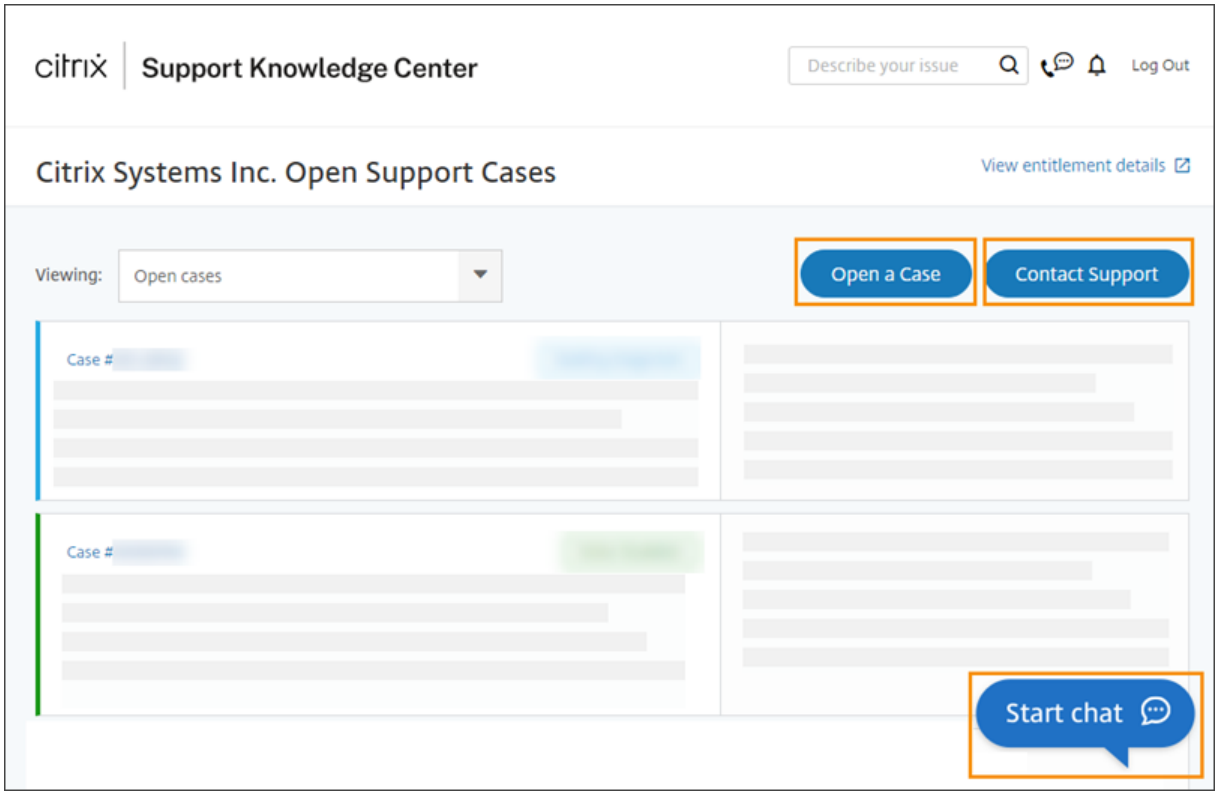


Nachdem Sie eine dieser Optionen ausgewählt haben, wählen Sie **Zu My Support** und melden Sie sich dann mit Ihren Citrix-Kontoanmeldeinformationen an.



Nach der Anmeldung erreichen Sie den technischen Support von Citrix über eines der folgenden Verfahren:

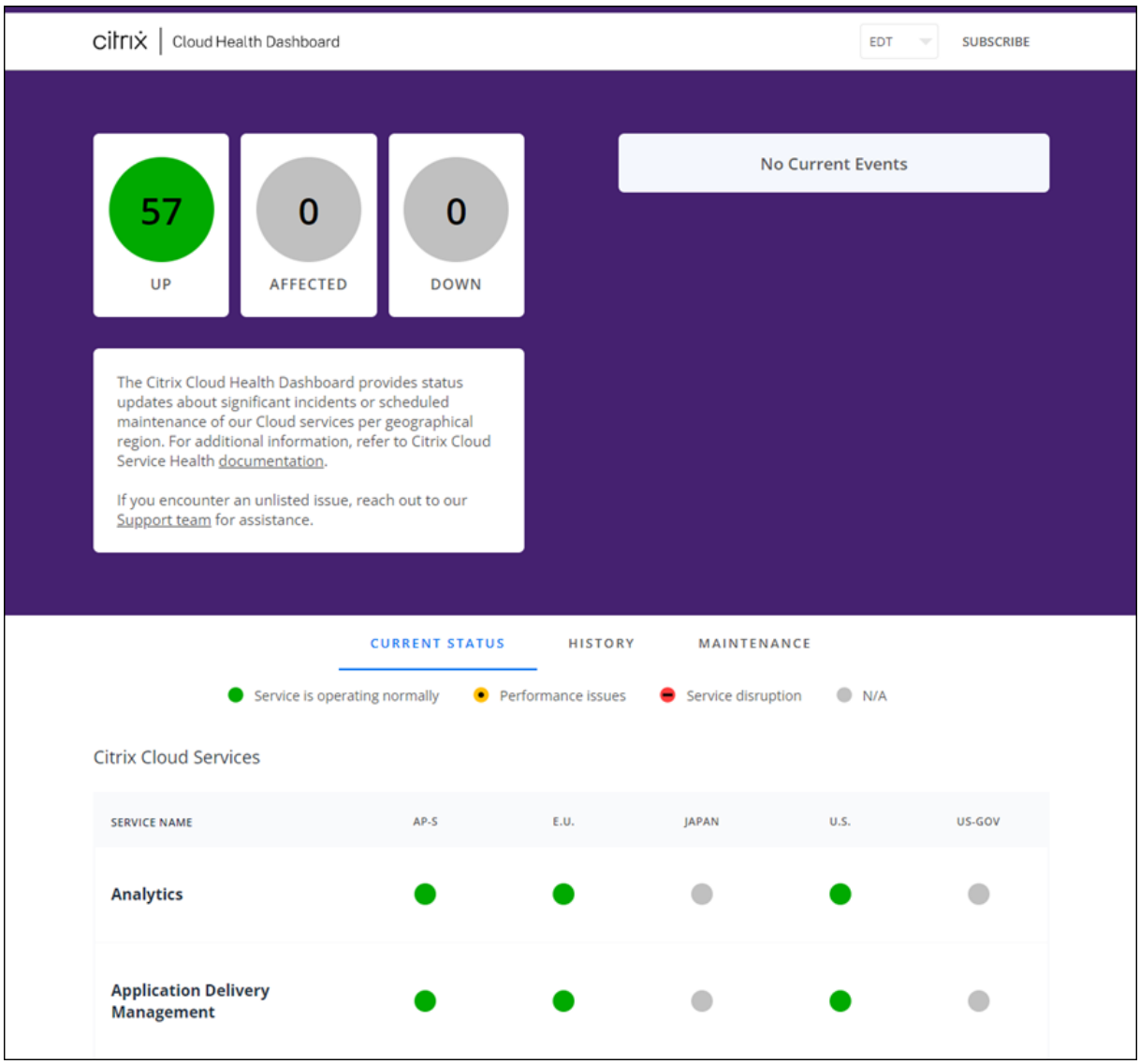
- Öffnen Sie einen Supportfall: Wählen Sie **Open a Case** und geben Sie Details zu Ihrem Problem ein.
- Per Telefon: Wählen Sie **Contact Support**, um eine Liste lokaler Telefonnummern anzuzeigen, über die Sie den technischen Support von Citrix erreichen.
- Live-Chat: Wählen Sie **Start chat** rechts unten auf der Seite, um mit einem Mitarbeiter des technischen Supports von Citrix zu chatten.



Integrität des Citrix Cloud-Diensts

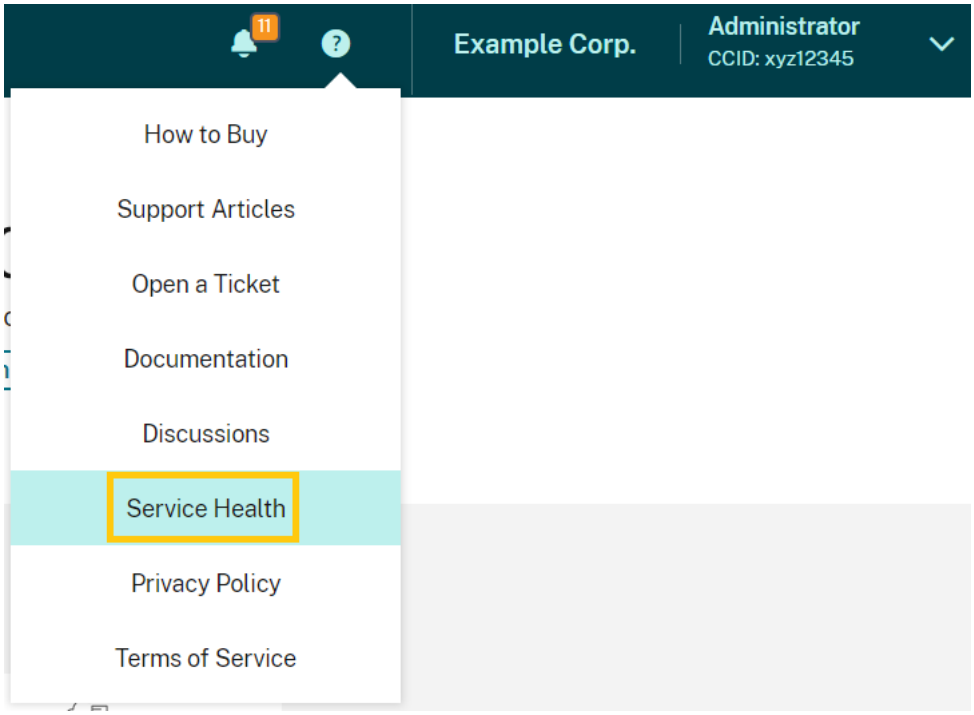
November 24, 2023

Das Citrix Cloud-Integritäts-Dashboard bietet einen Überblick über die Echtzeitverfügbarkeit der Citrix Cloud-Plattform und der Services für jede geografische Region. Wenn Probleme mit Citrix Cloud auftreten, überprüfen Sie das Cloud-Integritäts-Dashboard, um sicherzustellen, dass Citrix Cloud bzw. einzelne Services normal funktionieren.



Sie können mit den folgenden Methoden auf das Cloud Health Dashboard zugreifen:

- Gehen Sie in einem Webbrowser zu https://status.cloud.com.
- Wählen Sie **Service Health** aus dem Hilfemenü in Citrix Cloud aus.



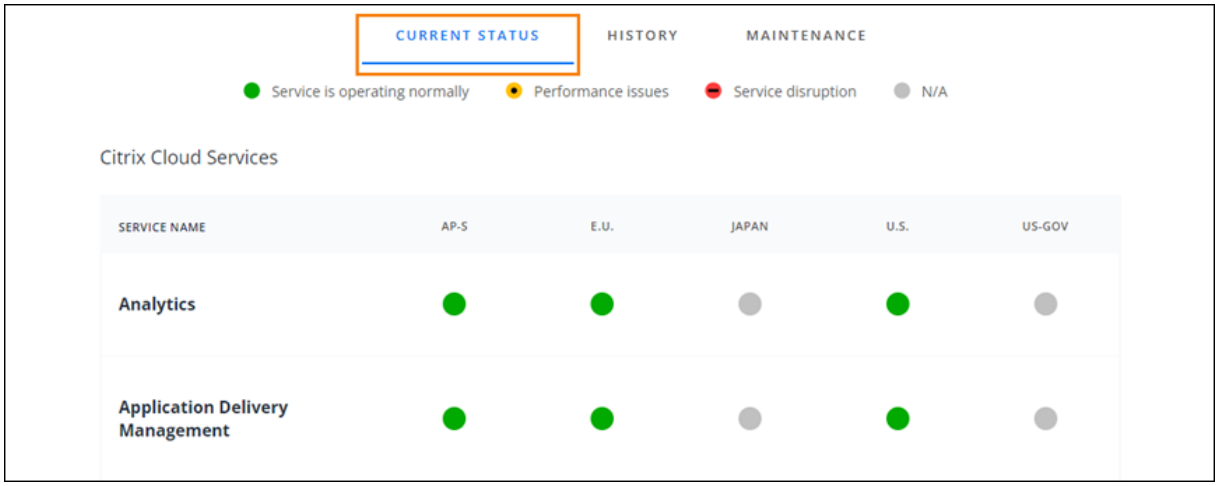
Über das Dashboard erhalten Sie Informationen zu folgenden Elementen:

- Zustand aller Citrix Cloud-Services nach geografischer Region
- 7-Tage-Integritätsverlauf für jeden Service
- Wartungsfenster für bestimmte Services

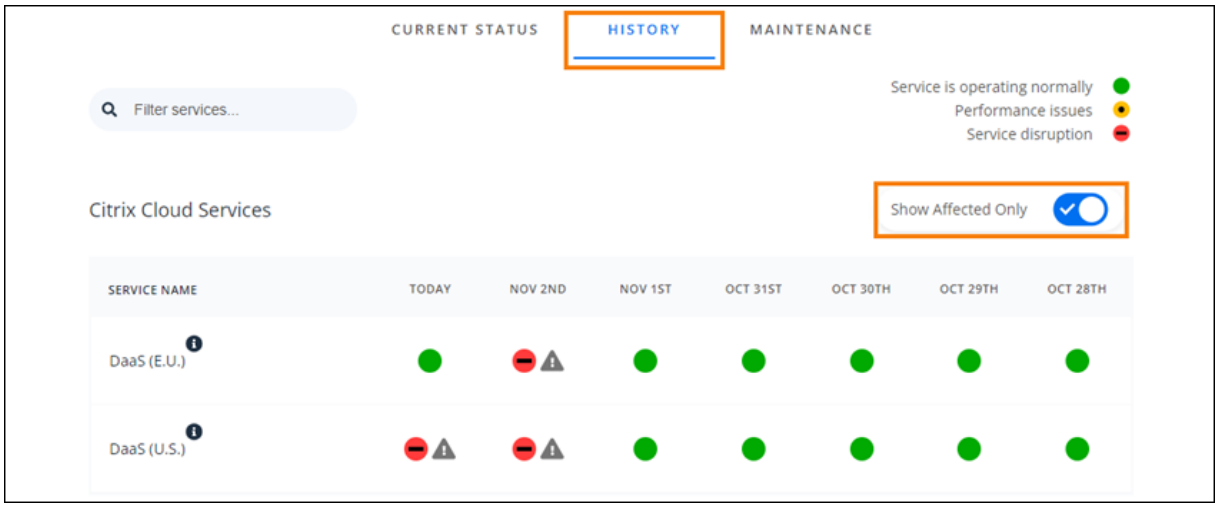
Sie können auch Benachrichtigungen über Ereignisse wie Wartungsfenster und Service-Incidents abonnieren.

Anzeigen von Zustand und Wartungsstatus

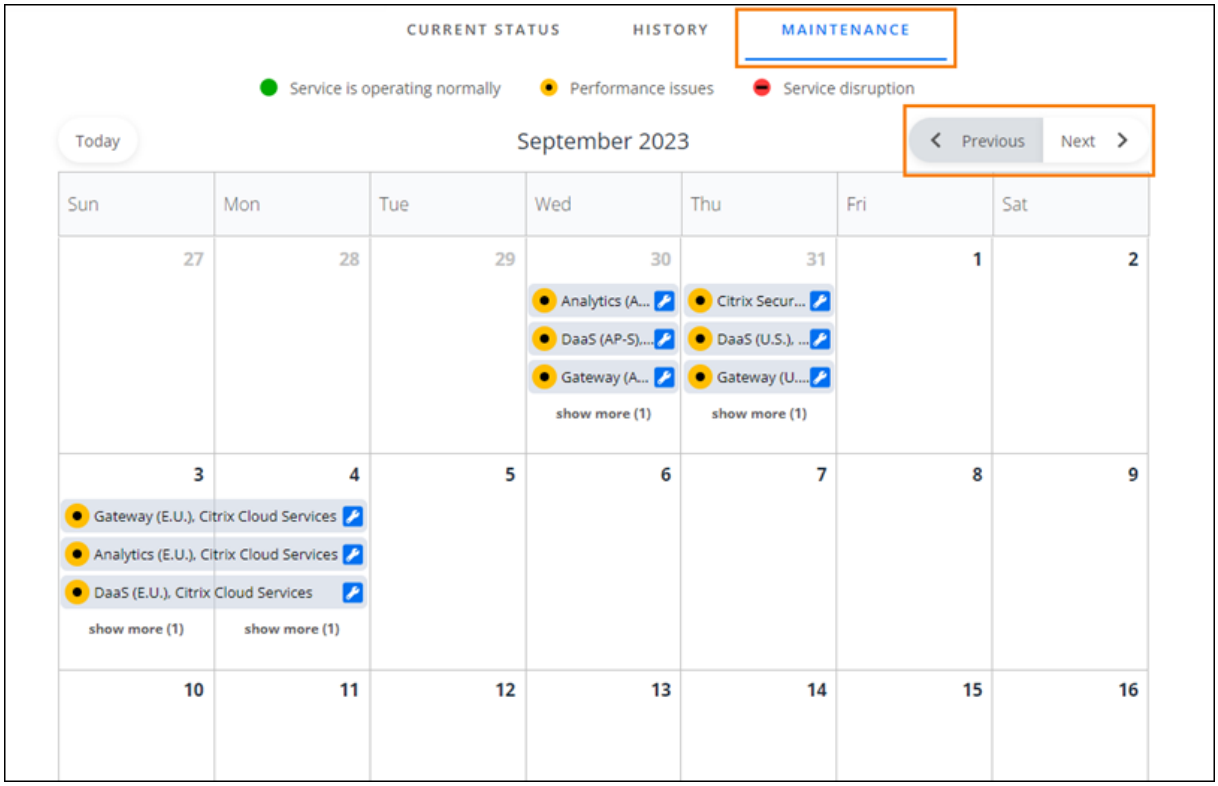
Wählen Sie **Current Status**, um den aktuellen Status aller Citrix Cloud-Services und -Komponenten in den einzelnen geografischen Regionen anzuzeigen.



Wählen Sie **Verlauf**, um den Integritätsstatus der Citrix Cloud-Services und -Komponenten für die vergangenen sieben Tage anzuzeigen. Wählen Sie **Show Affected Only**, um nur die Services anzuzeigen, bei denen in den letzten sieben Tagen Wartungs- oder Integritätsereignisse auftraten.



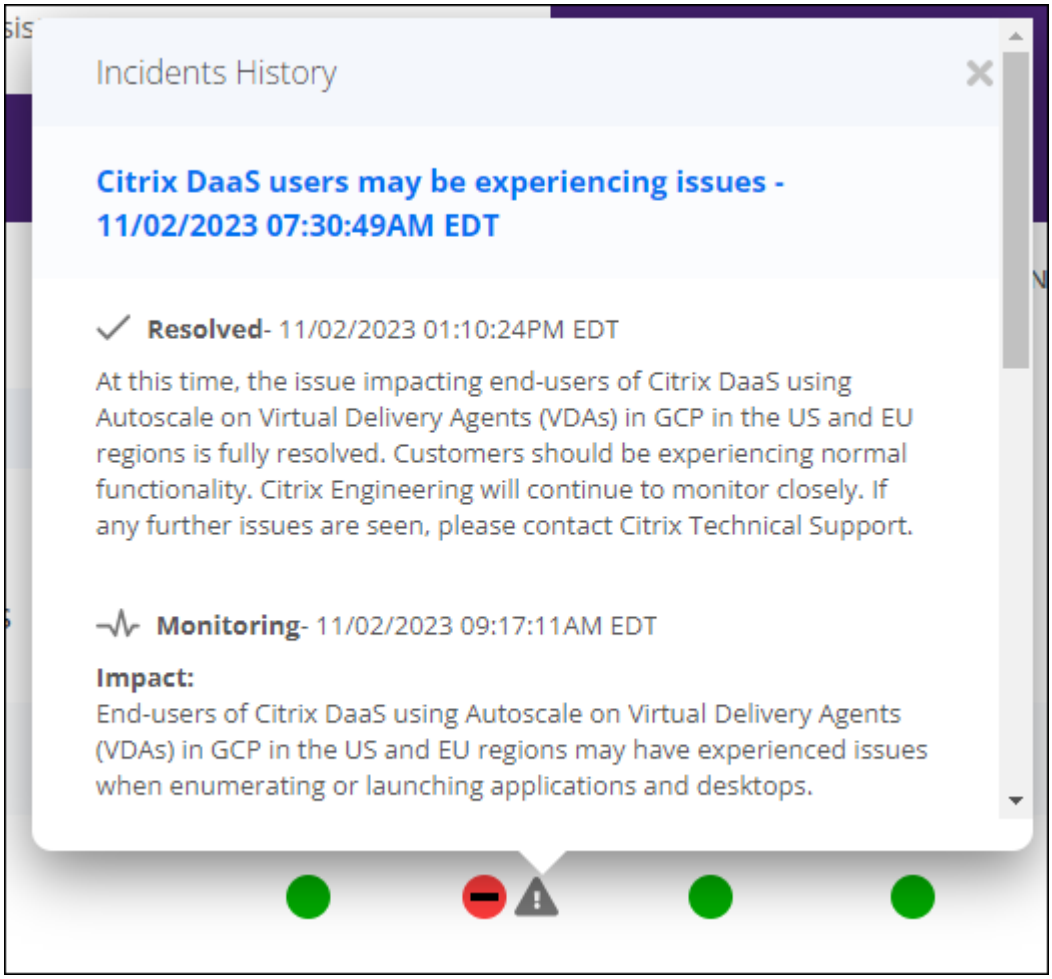
Wählen Sie **Wartung**, um eine Kalenderansicht der Wartungsfenster anzuzeigen. Wählen Sie **Weiter**, um für zukünftige Monate geplante Wartungsereignisse anzuzeigen. Wählen Sie **Zurück**, um zu den Ereignissen für den aktuellen Monat zurückzukehren.



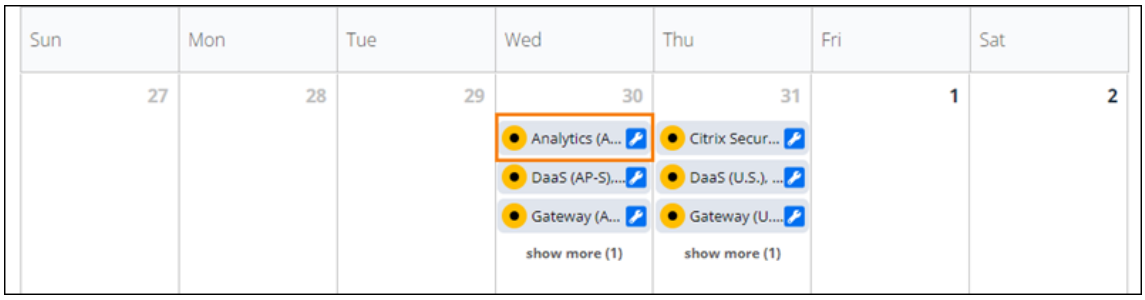
Anzeigen von Details zu Service-Incidents

Zum Anzeigen detaillierter Informationen zu einem Service-Incident gehen Sie folgendermaßen vor:

- Klicken Sie in der Verlaufsansicht auf das Symbol neben dem Serviceindikator, um detaillierte Informationen zu dem Incident anzuzeigen.



- Klicken Sie in der Wartungsansicht auf den Serviceeintrag, um die Statusseite für das Wartungsfenster anzuzeigen.



Häufigkeit der Incident-Meldungen

Tritt ein Servicestatus-Incident auf, berücksichtigt Citrix bei der Veröffentlichung auf status.cloud.com Folgendes:

- Dauer der Auswirkungen
- Häufigkeit der Auswirkungen

Während der Behebung eines Incidents veröffentlicht Citrix die folgenden Arten von Meldungen im Cloud-Integritäts-Dashboard:

- **Investigating:** Diese Meldung weist darauf hin, dass Citrix das Problem als dringend eingestuft hat und es untersucht.
- **Monitoring:** Diese Meldung weist darauf hin, dass Citrix die Problemursache ermittelt hat und das Problem löst.
- **Resolved:** Diese Meldung weist darauf hin, dass Citrix das Problem behoben hat und der Service wieder in einem fehlerfreien Zustand ist.

Während der Untersuchung und Überwachung eines Incidents veröffentlicht Citrix alle 60 bis 120 Minuten Updates. Diese Updates können Informationen folgender Art enthalten:

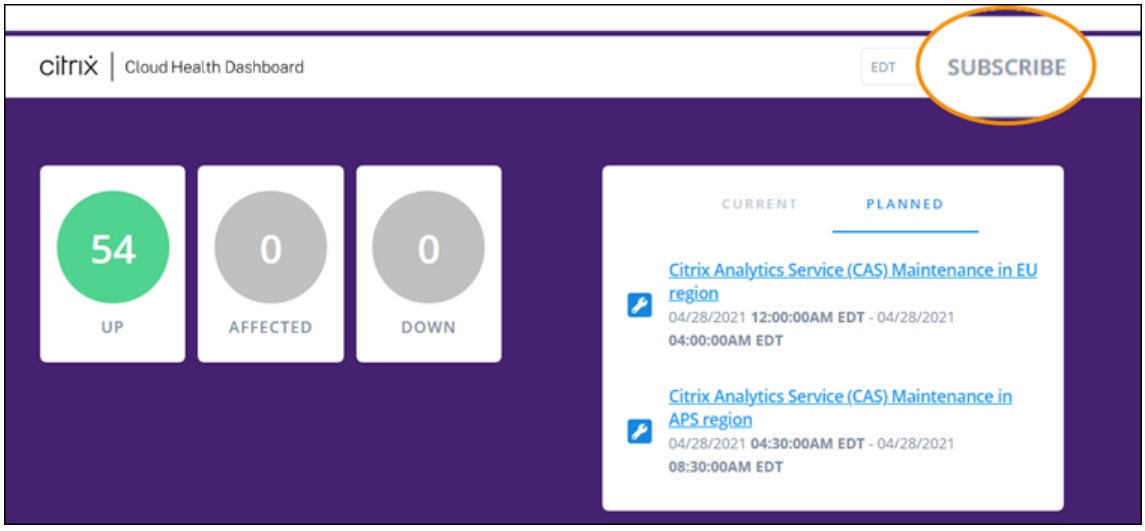
- Weitere Details zum Incident.
- Eine Beschreibung der Maßnahmen, die Citrix zur Behebung des Incidents ergreift.
- Ein Hinweis darauf, dass es seit dem letzten Update keine neuen Änderungen gibt.

Wenn ein Incident behoben ist, veröffentlicht Citrix ein letztes Update. Dieses Update kann darauf hinweisen, dass der Incident behoben wurde und der Service wieder in einen fehlerfreien Zustand versetzt wurde.

Benachrichtigungen abonnieren

Benachrichtigungen über Serviceintegritätsereignisse können Sie auf folgende Weise einholen:

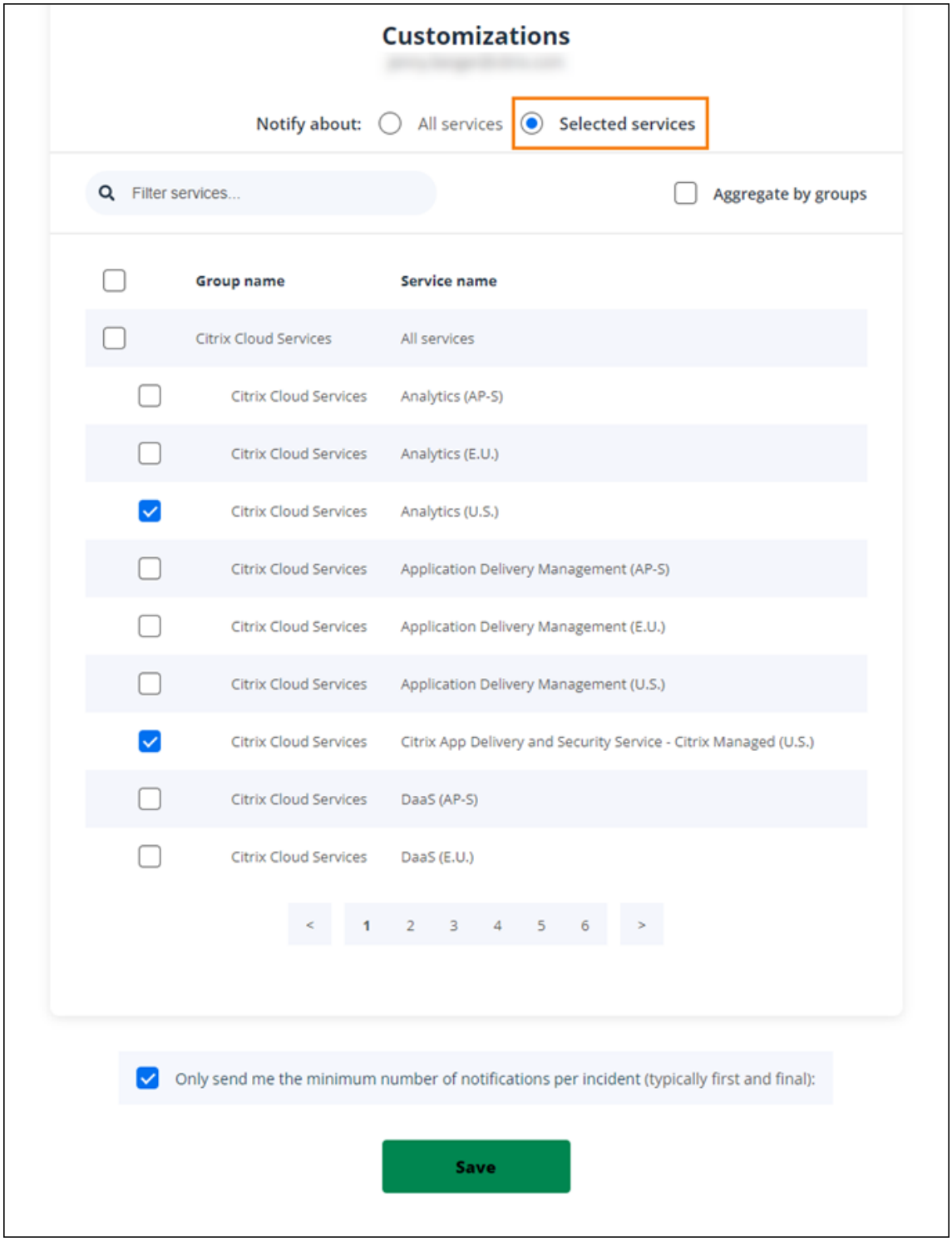
- Wählen Sie oben rechts im Dashboard **Subscribe** und dann die gewünschte Benachrichtigungsmethode. Sie können zwischen verschiedenen Methoden wählen, einschließlich E-Mail und Telefon (SMS).



- Geben Sie die folgenden URLs in Ihrem RSS-Reader ein, um den RSS-Feed für die Citrix Cloud-Integrität zu abonnieren:
  - Für Benachrichtigungen zu Service-Incidents und Wartung abonnieren Sie `https://status.cloud.com/?format=atom`.
  - Für Benachrichtigungen zu Service-Incidents abonnieren Sie `https://status.cloud.com/atom/incidents`.
  - Für Benachrichtigungen zu Wartung abonnieren Sie `https://status.cloud.com/atom/maintenances`.

Spezifische Services in einer Region abonnieren

1. Wählen Sie oben rechts im Dashboard **Subscribe** und dann die gewünschte Benachrichtigungsmethode.
2. Geben Sie die Kontaktdaten oder die URL für die gewählte Abonnementmethode ein und akzeptieren Sie unter **Terms & Services** die Nutzungsbedingungen. Wählen Sie **Weiter**. Die Seite **Customizations** wird angezeigt, **Selected services** ist standardmäßig ausgewählt.
3. Wählen Sie auf der Seite **Customizations** die Services in den gewünschten Regionen aus der (mehrseitigen) Liste aus.

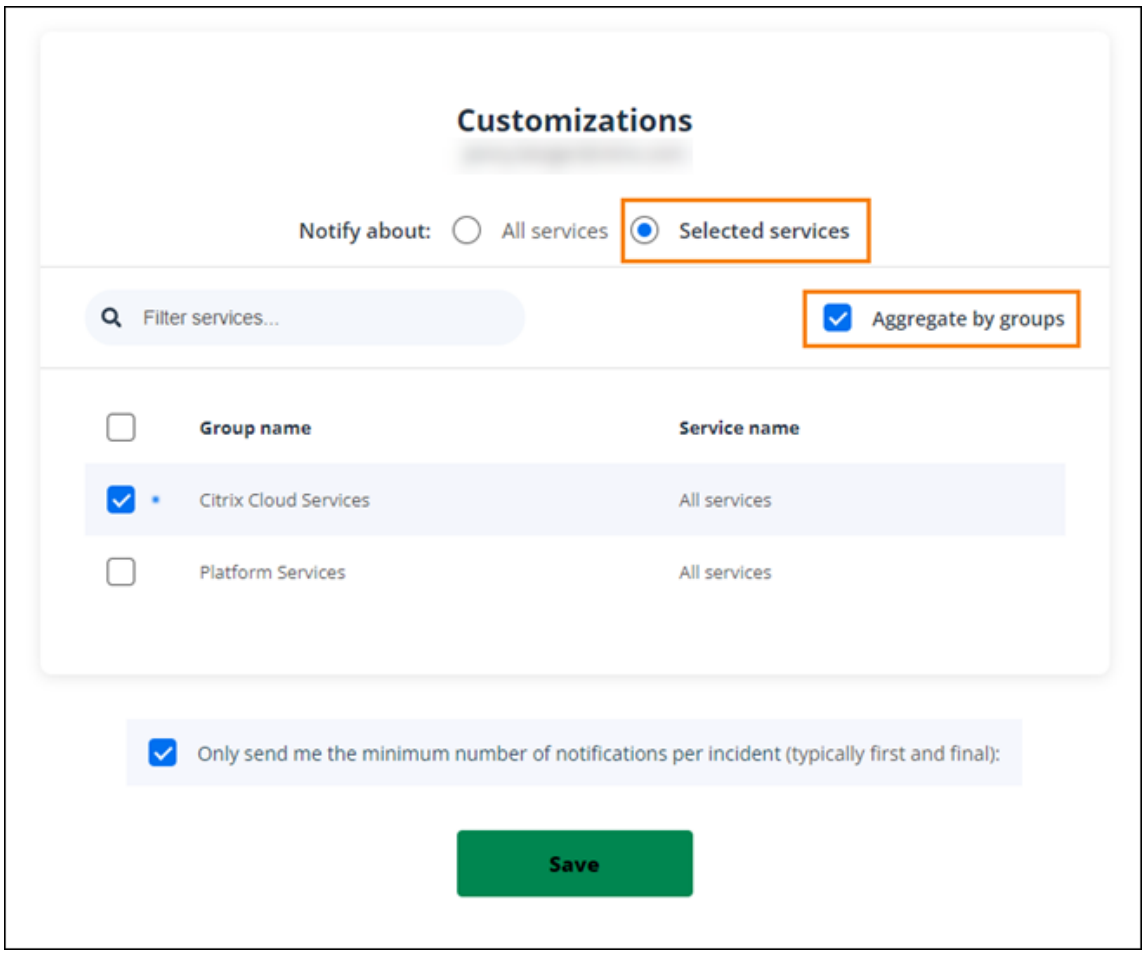


4. Um nur die erste und die letzte Benachrichtigung für einen Incident zu erhalten, wählen Sie **Only send me the minimum number of notifications per incident**.
5. Klicken Sie auf **Speichern**.

Spezifische Servicegruppen abonnieren

Sie können Benachrichtigungen für alle Cloud-Services (z. B. Analytics und DaaS) oder alle Plattformservices (z. B. die Steuerungsebenen- und Cloud-APIs) in allen Regionen abonnieren.

1. Wählen Sie oben rechts im Dashboard **Subscribe** und dann die gewünschte Benachrichtigungsmethode.
2. Geben Sie die Kontaktdaten oder die URL für die gewählte Abonnementmethode ein und akzeptieren Sie unter **Terms & Services** die Nutzungsbedingungen. Wählen Sie **Weiter**. Die Seite **Customizations** wird angezeigt, **Selected services** ist standardmäßig ausgewählt.
3. Wählen Sie auf der Seite **Customizations** die Option **Aggregate by groups**.
4. Wählen Sie entweder **Citrix Cloud Services** oder **Platform Services**.

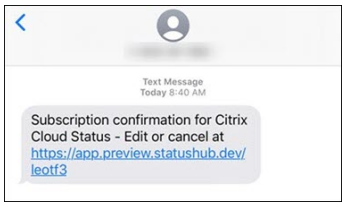


5. Um nur die erste und die letzte Benachrichtigung für einen Incident zu erhalten, wählen Sie **Only send me the minimum number of notifications per incident**.
6. Klicken Sie auf **Speichern**.

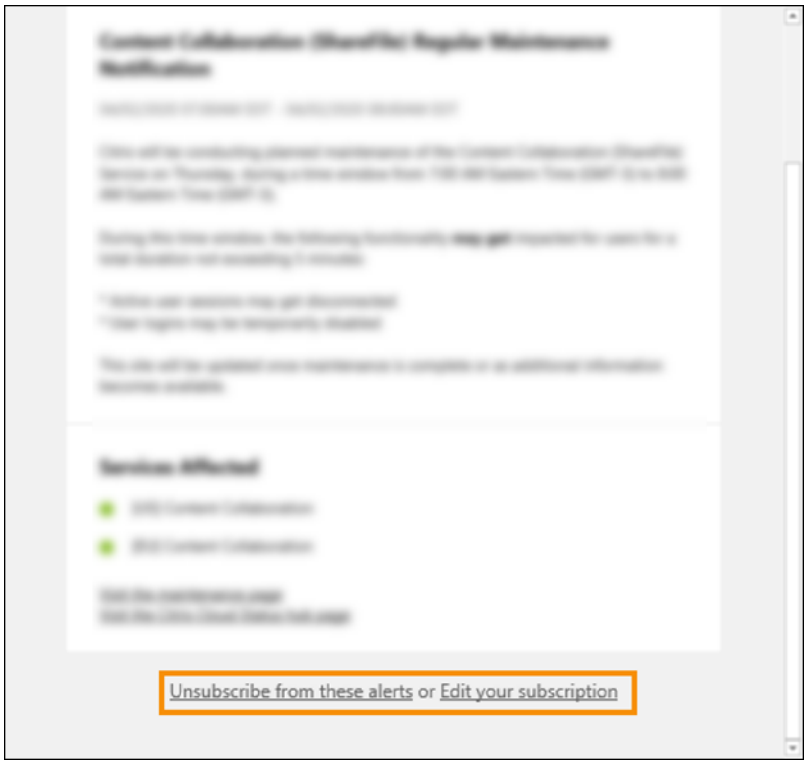
Benachrichtigungen abbestellen

Je nach Benachrichtigungsmethode finden Sie die Links zum Abbestellen oder Ändern Ihres Abonnements in der Bestätigungsnachricht, die Sie zu Beginn des Abonnements erhalten (z. B. beim Abonnieren von Telefonbenachrichtigungen), oder in jeder einzelnen Benachrichtigung (z. B. wenn Sie E-Mail-Benachrichtigungen abonnieren). Beispiel:

- Telefonische Benachrichtigung mit Abonnementoptionen:



- Benachrichtigungs-E-Mail mit Abonnementoptionen



Zum Abbestellen aller Benachrichtigungen und Entfernen aller Abonnementmethoden gehen Sie folgendermaßen vor:

1. Wählen Sie in Ihrer Abonnementbestätigung oder einer eingegangenen Benachrichtigung den Link zum Abbestellen. Manche Abonnementmethoden bieten einen Einzellink zum Bearbeiten oder Abbestellen des Abonnements.
2. Verwenden Sie je nach Abonnementmethode eine der folgenden Optionen auf der Seite **Edit Subscriptions**:

- Wählen Sie **Remove all subscriptions**.
- Wählen Sie **Unsubscribe**. Wählen Sie auf der Seite **Unsubscribe methods** die Option **Remove all subscriptions**.

Zum Abbestellen aller Benachrichtigungen für eine einzelne Abonnementmethode gehen Sie folgendermaßen vor:

1. Wählen Sie in Ihrer Abonnementbestätigung oder einer eingegangenen Benachrichtigung den Link zum Abbestellen. Manche Abonnementmethoden bieten einen Einzellink zum Bearbeiten oder Abbestellen des Abonnements.
2. Verwenden Sie je nach Abonnementmethode eine der folgenden Optionen auf der Seite **Edit Subscriptions**:

   - Wählen Sie die betreffende Abonnementmethode. Ihr Abonnement wird mit sofortiger Wirkung gekündigt.
   - Wählen Sie **Unsubscribe**. Wählen Sie auf der Seite **Unsubscribe methods** die betreffende Abonnementmethode. Ihr Abonnement wird mit sofortiger Wirkung gekündigt.

Ändern von Servicebenachrichtigungen

1. Wählen Sie in Ihrer Abonnementbestätigung oder einer eingegangenen Benachrichtigung den Link zum Bearbeiten Ihres Abonnements. Manche Abonnementmethoden bieten einen Einzellink zum Bearbeiten oder Abbestellen des Abonnements.
2. Wählen Sie auf der Seite **Edit Subscriptions page** die betreffende Abonnementmethode.
3. Wählen Sie auf der Seite **Customizations** die Services, über die Sie benachrichtigt werden möchten, bzw. deaktivieren Sie Benachrichtigungen für Services, die Sie nicht mehr benötigen.
4. Wählen Sie **Speichern**.

Anforderungen an System und Konnektivität

July 2, 2024

Citrix Cloud bietet administrative Funktionen (über einen Webbrowser) und operative Anfragen (von anderen installierten Komponenten), die auf Ressourcen in Ihrer Bereitstellung zugreifen. In diesem Artikel werden die Systemanforderungen, erforderlichen kontaktierbaren Internetadressen und Voraussetzungen beschrieben, die beim Verbinden von Ressourcen und Citrix Cloud berücksichtigt werden müssen.

Systemanforderungen

Citrix Cloud erfordert die folgende Mindestkonfiguration:

- Eine Active Directory-Domäne
- Zwei physische oder virtuelle Maschinen in Ihrer Domäne für den Citrix Cloud Connector: Weitere Informationen finden Sie unter Technische Daten zu Citrix Cloud Connector.
- Physische oder virtuelle Computer, die in Ihre Domäne eingebunden sind, um Workloads und andere Komponenten wie StoreFront zu hosten. Weitere Informationen zu den Systemanforderungen für bestimmte Services finden Sie in der Citrix Dokumentation für den jeweiligen Service.

Weitere Informationen zu Skalierungs- und Größenanforderungen finden Sie unter Überlegungen zur Skalierung und Größe für Cloud Connectors.

Unterstützte Webbrowser

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

Anforderungen für TLS (Transport Layer Security)

Citrix Cloud unterstützt Transport Layer Security (TLS) 1.2 für TCP-basierte Verbindungen zwischen Komponenten. Citrix Cloud erlaubt keine Kommunikation über TLS 1.0 oder TLS 1.1.

Für den Zugriff auf Citrix Cloud müssen Sie einen TLS 1.2-kompatiblen Browser verwenden und zulässige Verschlüsselungssammlungen konfigurieren. Weitere Informationen finden Sie unter Verschlüsselung und Schlüsselverwaltung.

Citrix Cloud-Verwaltungskonsole

Die Citrix Cloud-Verwaltungskonsole ist eine webbasierte Konsole, auf die Sie nach der Anmeldung unter https://citrix.cloud.com zugreifen können. Für die Webseiten der Konsole werden u. U. andere Ressourcen im Internet benötigt, entweder bei der Anmeldung oder wenn später bestimmte Vorgänge ausgeführt werden.

Proxykonfiguration

Wenn Sie eine Verbindung über einen Proxyserver herstellen, gilt für die Verwaltungskonsole die gleiche Konfiguration wie für den Webbrowser. Die Konsole funktioniert im Benutzerkontext, sodass die Konfiguration aller Proxyserver mit erforderlicher Benutzerauthentifizierung erwartungsgemäß erfolgen sollte.

Firewallkonfiguration

Für den Betrieb der Verwaltungskonsole muss Port 443 für ausgehende Verbindungen geöffnet sein. Gehen Sie in der Konsole, um die allgemeine Netzwerkkonnektivität zu testen. Weitere Informationen zu den erforderlichen Ports finden Sie unter Konfiguration von eingehenden und ausgehenden Ports.

Konsolenbenachrichtigungen

Die Managementkonsole verwendet Pendo, um kritische Warnungen, Benachrichtigungen über neue Features und produktinterne Anleitungen für einige Features und Services anzuzeigen. Um sicherzustellen, dass Sie Pendo-Inhalte in der Managementkonsole anzeigen können, empfiehlt Citrix, dass die Adresse `https://citrix-cloud-content.customer.pendo.io/` kontaktierbar ist.

Zu den Services, die Pendo-Inhalte anzeigen, gehören:

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

Pendo ist ein Drittanbieter-Unterauftragsverarbeiter, den Citrix verwendet, um Kunden Cloud- und Supportdienste bereitzustellen. Eine vollständige Liste dieser Unterauftragsverarbeiter finden Sie unter Sub-Processors for Citrix Cloud & Support Services and Citrix Affiliates.

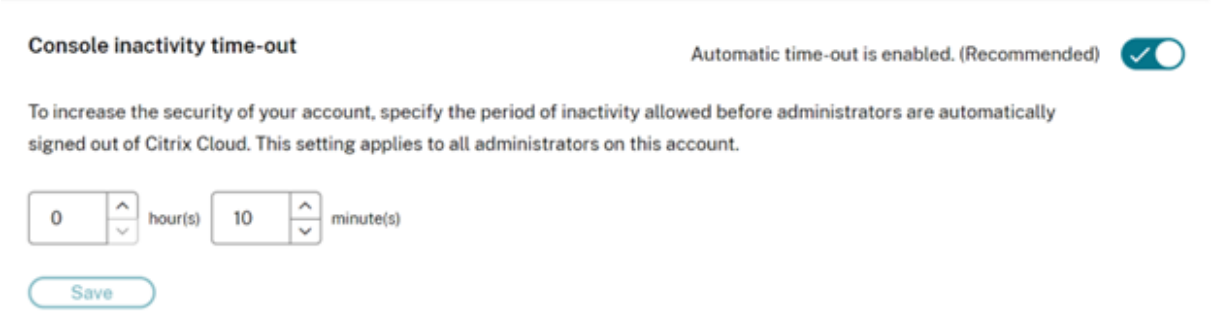
Sitzungstimeout

Wenn ein Administrator sich bei Citrix Cloud anmeldet, wird die Verwaltungskonsolensitzung nach Ablauf von 72 Stunden beendet: Dieses Timeout tritt unabhängig von der Konsolenaktivität auf.

Konfigurierbares Inaktivitätstimeout für die Konsole

Als Administrator mit vollem Zugriff können Sie die Dauer der Inaktivität in der Citrix Cloud-Konsole konfigurieren, bevor Administratoren automatisch abgemeldet werden. Nach der Konfiguration wird

der angegebene Timeout-Zeitraum auf alle Administratoren des Citrix Cloud-Kontos angewendet.



Wenn die Funktion aktiviert ist, werden Administratoren nach dem konfigurierten Zeitraum der Inaktivität abgemeldet, und das Sitzungs-Timeout wird bei jeder nachfolgenden Anmeldung zurückgesetzt.

Wenn die Funktion deaktiviert ist, gibt es keinen Inaktivitäts-Timer und Administratoren werden erst abgemeldet, wenn das 72-Stunden-Sitzungslimit erreicht ist.

> **Hinweis:**
>
> - Standardmäßig ist dieses Feature deaktiviert.
> - Das konfigurierbare Inaktivitätstimeout beträgt 10 Minuten bis 12 Stunden.
> - Die Standardeinstellung für das Inaktivitätstimeout ist 60 Minuten.

Lizenzserver bei Citrix Cloud registrieren

Wenn Sie Ihren on-premises bereitgestellten Citrix Lizenzserver bei Citrix Cloud registrieren, um die Nutzung von On-Premises-Bereitstellungen zu überwachen, müssen die folgenden Adressen erreichbar sein:

- `https://trust.citrixnetworkapi.net` (zum Abrufen eines Codes)
- `https://trust.citrixworkspacesapi.net/` (zur Bestätigung, dass der Lizenzserver registriert ist)
- `https://cis.citrix.com` (für den Datenupload)
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

Wenn Sie einen Proxyserver mit Citrix Lizenzserver verwenden, muss der Proxyserver gemäß den Anweisungen unter Konfigurieren eines Proxyservers in der Dokumentation zur Lizenzierung konfiguriert sein.

Citrix Cloud Connector

Der Citrix Cloud Connector ist ein Softwarepaket, das mehrere Services bereitstellt, die auf Microsoft Windows-Servern ausgeführt werden. Die Maschine, die den Cloud Connector hostet, ist im gleichen Netzwerk wie die Ressourcen, die Sie mit Citrix Cloud verwenden. Der Cloud Connector stellt eine Verbindung zu Citrix Cloud her und sorgt dafür, dass Ressourcen je nach Bedarf genutzt und verwaltet werden können.

Informationen zu den Anforderungen für die Installation des Cloud Connectors finden Sie unter Systemanforderungen. Für den Betrieb des Cloud Connectors sind ausgehende Verbindungen auf Port 443 erforderlich. Nach der Installation müssen möglicherweise weitere Zugriffsanforderungen für den Cloud Connector konfiguriert werden, je nachdem, mit welchem Citrix Cloud Service er verwendet wird.

Die Maschine, auf der der Cloud Connector gehostet wird, muss eine stabile Netzwerkverbindung mit Citrix Cloud haben. Netzwerkkomponenten müssen HTTPS und langlebige sichere Web-Sockets unterstützen. Falls ein Timeout in den Netzwerkkomponenten konfiguriert ist, muss er länger als 2 Minuten sein.

Bei Problemen mit der Konnektivität zwischen Cloud Connector und Citrix Cloud verwenden Sie das Hilfsprogramm zur Cloud Connector-Konnektivitätsprüfung. Dieses Dienstprogramm prüft anhand einer Reihe von Tests auf der Cloud Connector-Maschine, ob sie Citrix Cloud und zugehörige Dienste erreichen kann. Wenn Sie einen Proxyserver in Ihrer Umgebung verwenden, werden alle Verbindungstests über Ihren Proxyserver getunnelt. Informationen zum Herunterladen des Hilfsprogramms finden Sie unter CTX260337 im Citrix Support Knowledge Center.

Verbindungsanforderungen für den Cloud Connector

Um Ihre Datencenter mit dem Internet zu verbinden, muss Port 443 für ausgehende Verbindungen geöffnet sein. Für Umgebungen mit Internetproxyserver oder Firewall sind jedoch u. U. weitere Konfigurationsschritte erforderlich. Weitere Informationen finden Sie unter Konfiguration von Cloud Connector-Proxy und Firewall.

Die Adressen für jeden Service in diesem Artikel müssen kontaktierbar sein, damit der Dienst ordnungsgemäß ausgeführt und in Anspruch genommen werden kann. Die folgende Liste enthält Adressen für die meisten Citrix Cloud Services.

- `https://*.citrixworkspacesapi.net` (bietet Zugriff auf Citrix Cloud-APIs, die von den Diensten verwendet werden)

- `https://*.cloud.com` (bietet Zugriff auf die Citrix Cloud-Anmeldeoberfläche)
- `https://*.blob.core.windows.net` (bietet Zugriff auf den Azure Blob Storage, in dem Updates für den Citrix Cloud Connector gespeichert werden)
- `https://*.servicebus.windows.net` (bietet Zugriff auf Azure Service Bus, der für die Protokollierung verwendet wird, und Active Directory-Agent)

Diese Adressen werden nur als Domänennamen bereitgestellt, da Citrix Cloud Services dynamisch ist und die IP-Adressen sich routinemäßig ändern.

Verwenden Sie als bewährte Methode die Gruppenrichtlinie, um diese Adressen zu konfigurieren und zu verwalten. Konfigurieren Sie außerdem nur die Adressen, die für die Services gelten, die Sie und Ihre Endbenutzer nutzen.

Wenn Sie Citrix Cloud mit Citrix Lizenzserver zum Registrieren Ihrer On-premises-Produkte verwenden, finden Sie unter Lizenzserver bei Citrix Cloud registrieren in diesem Artikel Informationen zu zusätzlich erforderlichen kontaktierbaren Adressen.

Positivliste der FQDNs für den Cloud Connector

Damit Sie sicherstellen können, dass alle erforderlichen vollqualifizierten Domänennamen (FQDNs) durch Ihre Firewall zugelassen werden, stellt Citrix die folgenden Ressourcen bereit:

- allowlist.json
- CTX270584: Citrix Gateway Service –Points of Presence (PoPs)

Konsultieren Sie bei der Konfiguration Ihrer Firewall diese beiden Ressourcen, um sicherzustellen, dass die FQDNs, die für Ihre Servicebereitstellung erforderlich sind, zulässig sind.

Lokaler Hostcache (Dienst für hohe Verfügbarkeit) Wenn Sie den lokalen Hostcache (LHC) in Connectors verwenden, achten Sie darauf, dass die Connectors den gewählten Endpunkt jedes anderen Connectors am Ressourcenstandort erreichen können. Der gewählte Endpunkt befindet sich auf Port 80 und kann über die folgende URL aufgerufen werden: `http://<FQDN_OR_IP_OF_PEER_CONNECTOR>/Citrix/CdsController/ISecondaryBrokerElection`.

Wenn Connectors unter dieser Adresse nicht kommunizieren können, werden während eines LHC-Ereignisses mehrere Broker ausgewählt, was zu zeitweiligen Fehlern beim Start virtueller Apps und Desktops führen kann. Weitere Informationen finden Sie unter Ressourcenstandorte mit mehreren Cloud Connectors.

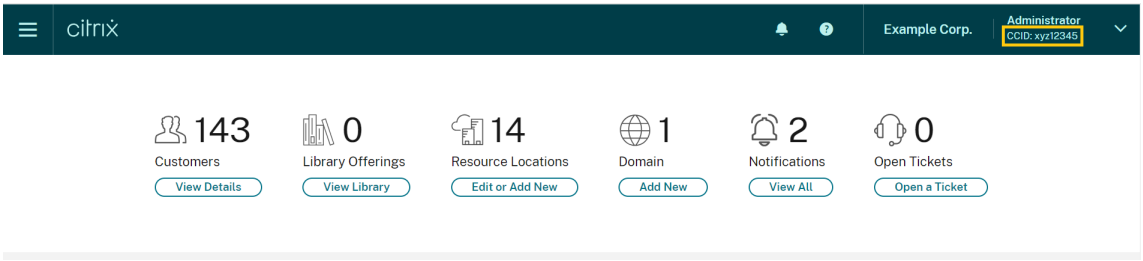
Adaptive Authentifizierung Wenn Sie den Cloud Connector für die Verbindung mit einem Dienst zur adaptiven Authentifizierung verwenden, müssen Sie Ihrem Citrix Cloud Connector den Zugriff

auf die Domäne oder URL ermöglichen, die Sie für die adaptive Authentifizierungsinstanz reserviert haben. Lassen Sie beispielsweise `https://aauth.xyz.com` zu. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

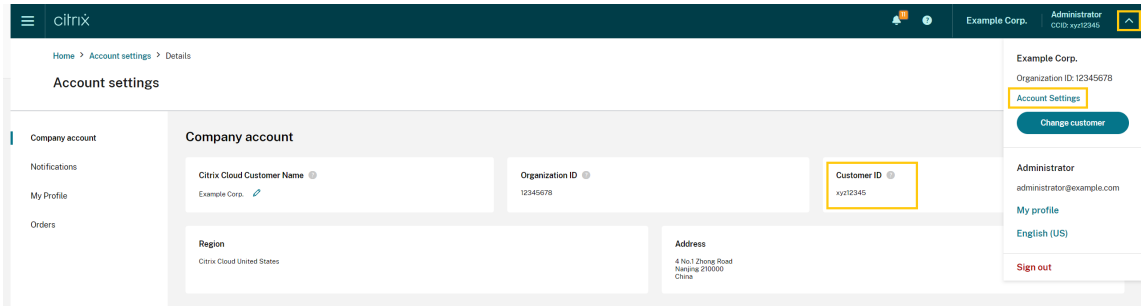
Allowlist.json Die Datei allowlist.json ist auf https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.json und enthält eine Liste der FQDNs, auf die der Cloud Connector zugreift. Die Liste ist nach Produkt unterteilt und enthält ein Änderungsprotokoll für jede FQDN-Kategorie.

Einige FQDNs sind kundenspezifisch und enthalten Vorlagenabschnitte in eckigen Klammern. Diese Vorlagenabschnitte müssen vor der Verwendung durch die tatsächlichen Werte ersetzt werden. Beispiel `<CUSTOMER_ID>.xendesktop.net`: Sie ersetzen `<CUSTOMER_ID>` durch die Kunden-ID für Ihr Citrix Cloud-Konto. Sie finden die Kunden-ID in der Konsole wie folgt:

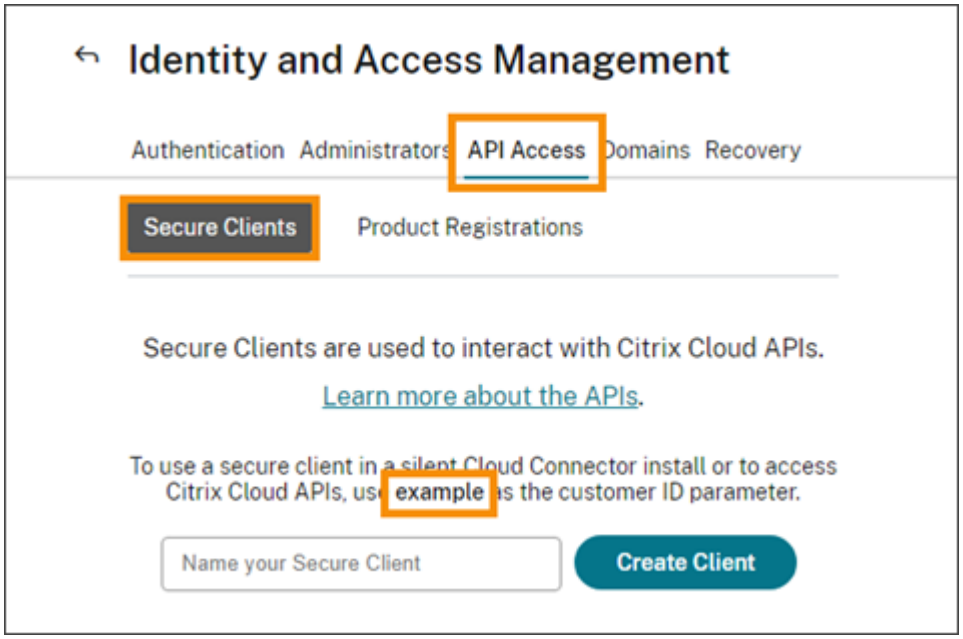
- Oben rechts unter dem Kundennamen Ihres Citrix Cloud-Kontos.



- Auf der Seite “Kontoeinstellungen”unter **Citrix Cloud-Kunden-ID (CCID)**.



- Auf der Registerkarte **Sichere Clients** unter **Identitäts- und Zugriffsmanagement > API-Zugriff > Sichere Clients**.



Gateway-Service: Points of Presence Einige der in der Datei allowlist.json enthaltenen FQDNs sind auch in CTX270584: Citrix Gateway Service –Points of Presence (PoPs) aufgeführt. CTX270584 enthält jedoch auch FQDNs, auf die Clients zugreifen, z. B. die folgenden:

- global-s.g.nssvc.net
- azure-s.g.nssvc.net

Zertifikatvalidierung

Cloud Connector-Binärdateien und Endpunkte, die der Cloud Connector kontaktiert, sind durch X.509-Zertifikate geschützt, die bei der Installation der Software überprüft werden. Um diese Zertifikate zu validieren, muss jede Cloud Connector-Maschine bestimmte Anforderungen erfüllen: Eine vollständige Liste dieser Anforderungen finden Sie unter Anforderungen für die Zertifikatvalidierung.

SSL-Entschlüsselung

Auf einigen Proxys wird durch Aktivieren der SSL-Verschlüsselung u. U. ein erfolgreicher Verbindungsaufbau zwischen Cloud Connector und Citrix Cloud verhindert. Weitere Informationen zum Beheben des Problems finden Sie unter CTX221535.

Citrix Connector Appliance für Cloudservices

Die Connector Appliance ist eine Appliance, die Sie in Ihrem Hypervisor bereitstellen können. Der Hypervisor, der die Connector Appliance hostet, ist im gleichen Netzwerk wie die Ressourcen, die Sie

mit Citrix Cloud verwenden. Die Connector Appliance stellt eine Verbindung zu Citrix Cloud her und sorgt dafür, dass Ressourcen je nach Bedarf genutzt und verwaltet werden können.

Informationen zu den Anforderungen für die Installation der Connector Appliance finden Sie unter Systemanforderungen.

Für den Betrieb der Connector Appliance sind ausgehende Verbindungen auf Port 443 erforderlich. Für Umgebungen mit Internetproxyserver oder Firewall sind jedoch u. U. weitere Konfigurationsschritte erforderlich.

Die folgenden Adressen müssen kontaktierbar sein, damit die Citrix Cloud Services ordnungsgemäß ausgeführt und in Anspruch genommen werden können:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.*.nssvc.net`

  Kunden, die nicht alle Unterdomänen aktivieren können, können stattdessen die folgenden Adressen verwenden:

  - `https://*.g.nssvc.net`
  - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

Netzwerkanforderungen

Stellen Sie sicher, dass Ihre Connector Appliance-Umgebung die folgende Konfiguration hat:

- Entweder, das Netzwerk lässt zu, das die Connector Appliance über DHCP DNS- und NTP-Server, eine IP-Adresse, einen Hostnamen und einen Domänennamen abruft, oder Sie legen die Netzwerkeinstellungen manuell in der Connector Appliance-Konsole fest.
- Das Netzwerk ist nicht für die Verwendung der Link-Local-IP-Bereiche 169.254.0.1/24, 169.254.64.0/18 oder 169.254.192.0/18 konfiguriert, die intern von der Connector Appliance verwendet werden.
- Entweder ist die Hypervisor-Uhr auf koordinierte Weltzeit (UTC) eingestellt und mit einem Zeitserver synchronisiert oder die Connector Appliance erhält NTP-Serverinformationen über DHCP.
- Wenn Sie einen Proxy mit der Connector Appliance verwenden, darf der Proxy nicht authentifiziert sein oder er muss die Standardauthentifizierung verwenden.

Citrix Analytics-Servicekonnektivität

- Für produktinterne Meldungen einschließlich zu neuen Features und wichtigen Informationen: `https://citrix-cloud-content.customer.pendo.io/`
- Zusätzliche Anforderungen: Voraussetzungen

Weitere Informationen zum Onboarding von Datenquellen für den Service finden Sie unter Supported data sources.

Konnektivität zum Konsolendienst

Vollständige Anforderungen an die Internetkonnektivität finden Sie unter Unterstützte Ports in der NetScaler-Produktdokumentation.

Konnektivität von Citrix DaaS

Citrix Ressourcenstandort / Cloud Connector:

- Verbindungsanforderungen für den Cloud Connector
- `https://[customerid].xendesktop.net`, wobei `[customerid]` der Parameter der Kunden-ID ist, der auf der Registerkarte **Sichere Clients** (**Identitäts- und Zugriffsverwaltung > API-Zugriff > Sichere Clients**) in der Citrix Cloud-Verwaltungskonsole angezeigt wird.
  - Kunden, die Citrix Virtual Apps Essentials verwenden, müssen stattdessen `https://*.xendesktop.net` verwenden.
- Kunden, die Citrix DaaS mit Quick Deploy installieren, müssen diese zusätzlichen Adressen kontaktierbar machen:
  - `https://*.apps.cloud.com`
  - `AzureCloud` Service-Tag
- `https://*.*.nssvc.net`
  - Kunden, die nicht alle Unterdomänen aktivieren können, können stattdessen die folgenden Adressen verwenden:
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

Eine Übersicht über die Kommunikation zwischen Cloud Connector und Dienst finden Sie im Diagramm für Citrix DaaS auf der Citrix Tech Zone-Website.

Verwaltungskonsole:

- `https://*.citrixworkspacesapi.net` (für Rendezvous nicht erforderlich)
- `https://*.citrixnetworkapi.net` (für Rendezvous nicht erforderlich)
- `https://*.cloud.com` (für Rendezvous nicht erforderlich)
- `https://[customerid].xendesktop.net`, wobei `[customerid]` der Parameter der Kunden-ID ist, der auf der Registerkarte **Sichere Clients** (**Identitäts- und Zugriffsverwaltung > API-Zugriff > Sichere Clients**) in der Citrix Cloud-Verwaltungskonsole angezeigt wird.
  - Kunden, die Citrix Virtual Apps Essentials verwenden, müssen stattdessen `https://*.xendesktop.net` verwenden.
- `https://*.*.nssvc.net` (für Citrix DaaS Standard für Azure nicht erforderlich)
  - Kunden, die nicht alle Unterdomänen aktivieren können, können stattdessen die folgenden Adressen verwenden:
    * `https://*.g.nssvc.net`
    * `https://*.c.nssvc.net`
- Für produktinterne Meldungen einschließlich zu neuen Features und wichtigen Informationen: `https://citrix-cloud-content.customer.pendo.io/`

Rendezvous-Protokoll

Wenn Sie Citrix Gateway Service verwenden, ermöglicht das Rendezvous-Protokoll VDAs, die Citrix Cloud Connectors zu umgehen, um eine direkte und sichere Verbindung mit der Citrix Cloud-Steuerungsebene herzustellen.

Unabhängig von der verwendeten Protokollversion müssen VDAs in der Lage sein, die oben aufgeführten Adressen für die Verwaltungskonsole zu kontaktieren, sofern nicht anders angegeben. Eine vollständige Liste der Anforderungen für das Rendezvous-Protokoll finden Sie in den folgenden Abschnitten der Citrix DaaS-Produktdokumentation:

- Rendezvous V1
- Rendezvous V2

Anforderung für lokalen Hostcache

Wenn Ihre Firewall eine Paketprüfung durchführt und Sie den lokalen Hostcache verwenden möchten, müssen Sie sicherstellen, dass Ihre Firewall XML- und SOAP-Datenverkehr akzeptiert. Für dieses Feature ist der Download von MDF-Dateien erforderlich. Dies geschieht, wenn der Cloud Connector Konfigurationsdaten mit Citrix Cloud synchronisiert. Diese Dateien werden über XML- und SOAP-Datenverkehr an den Cloud Connector übermittelt. Wenn die Firewall diesen Datenverkehr blockiert, schlägt die Synchronisierung zwischen dem Cloud Connector und Citrix Cloud fehl. Wenn ein Ausfall

auftritt, können Benutzer nicht weiterarbeiten, da die Konfigurationsdaten im Cloud Connector veraltet sind.

Weitere Informationen zu diesem Feature finden Sie unter Lokaler Hostcache in der Citrix DaaS-Produktdokumentation.

Anforderungen für VDA-Upgrade

Mit der Benutzeroberfläche "Vollständige Konfiguration"in Citrix DaaS können Sie VDAs pro Katalog oder pro Maschine aktualisieren. Das Upgrade kann sofort oder zu einem festgelegten Zeitpunkt ausgeführt werden. Weitere Informationen zum Feature "VDA-Upgrade"finden Sie unter Aktualisieren von VDAs über die Benutzeroberfläche "Vollständige Konfiguration".

Um das Feature zu verwenden, müssen folgende Konnektivitätsanforderungen erfüllt sein:

- Die folgenden Azure CDN-URLs wurden der Positivliste hinzugefügt. Das Feature lädt die VDA-Installationsprogramme von den Azure CDN-Endpunkten herunter.
  - Produktion–USA (US): `https://prod-us-vus-storage-endpoint.azureedge.net/*`
  - Produktion–Europäische Union (EU): `https://prod-eu-vus-storage-endpoint.azureedge.net/*`
  - Produktion–Südasien-Pazifik (APS): `https://prod-aps-vus-storage-endpoint.azureedge.net/*`
  - Produktion–Japan (JP): `https://prod-jp-vus-storage-endpoint.azureedge.net/*`
- Anschließend wird überprüft, ob das VDA-Installationsprogramm mit einem gültigen Zertifikat signiert ist. Zum Ausführen der Zertifikatsgültigkeits- und -sperrüberprüfung müssen die folgenden URLs zur Positivliste hinzugefügt sein:
  - `http://crl3.digicert.com/*`
  - `http://crl4.digicert.com/*`
  - `http://ocsp.digicert.com/*`
  - `http://cacerts.digicert.com/*`
- Zur Verwendung des Features ist der VDA Upgrade Agent erforderlich. Der auf dem VDA ausgeführte VDA Upgrade Agent kommuniziert mit Citrix DaaS. Vergewissern Sie sich, dass die folgenden URLs der Positivliste hinzugefügt wurden:
  - `https://[customerId].xendesktop.net/citrix/VdaUpdateService/*`, wobei `[customerid]` der Parameter der Kunden-ID ist, der auf der Registerkarte **Sichere Clients** (**Identitäts- und Zugriffsverwaltung > API-Zugriff > Sichere Clients**) in der Citrix Cloud-Verwaltungskonsole angezeigt wird.

    - http://xendesktop.net/citrix/VdaUpdateService/*

Endpoint Management-Servicekonnektivität

Citrix Ressourcenstandort / Cloud Connector:

- Verbindungsanforderungen für den Cloud Connector
- Zusätzliche Anforderungen: /en-us/citrix-endpoint-management/endpoint-management.html

Verwaltungskonsole:

- https://*.citrix.com
- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net
- Zusätzliche Anforderungen: /en-us/citrix-endpoint-management/endpoint-management.html

Citrix Gateway-Servicekonnektivität

- Verbindungsanforderungen für den Cloud Connector
- https://*.*.nssvc.net
    - Kunden, die nicht alle Unterdomänen aktivieren können, können stattdessen die folgenden Adressen verwenden:
        * https://*.g.nssvc.net
        * https://*.c.nssvc.net

> **Wichtig:**
>
> SSL-Abfangen ist an Citrix Gateway-Adressen nicht möglich. Auf einigen Proxys wird durch Aktivieren des SSL-Abfangens u. U. ein erfolgreicher Verbindungsaufbau zwischen Cloud Connector und Citrix Cloud verhindert.

NetScaler Intelligent Traffic Management-Servicekonnektivität

- https://*.cedexis-test.com
- https://*.citm-test.com
- https://cedexis.com
- https://cedexis-radar.net

SD-WAN Orchestrator-Servicekonnektivität

Die vollständigen Anforderungen an die Internetverbindung finden Sie unter Prerequisites for Citrix SD-WAN Orchestrator service usage.

Remote Browser Isolation (zuvor "Secure Browser") –Dienstverbindung

Citrix Ressourcenstandort / Cloud Connector:

Verbindungsanforderungen für den Cloud Connector

Verwaltungskonsole:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://browser-release-a.azureedge.net`
- `https://browser-release-b.azureedge.net`

Citrix Secure Private Access Service-Konnektivität

- `https://*.netscalergateway.net`
- `https://*.*.nssvc.net`
  - Kunden, die nicht alle Unterdomänen aktivieren können, können stattdessen die folgenden Adressen verwenden:
    * `https://*.g.nssvc.net`
    * `https://*.c.nssvc.net`

Citrix Workspace-Servicekonnektivität

- `https://*.cloud.com`
- `https://*.citrixdata.com`
- Für produktinterne Meldungen einschließlich zu neuen Features und wichtigen Informationen: `https://citrix-cloud-content.customer.pendo.io/`

Konnektivität des Global App Configuration Service

`https://discovery.cem.cloud.us`

Weitere Informationen zu diesem Service finden Sie in den folgenden Ressourcen:

- Einstellungen der Workspace-App anpassen - Citrix Workspace-Produktdokumentation
- Global App Configuration Service - Citrix Developer-Dokumentation

Citrix Workspace-App-Konnektivität

Fügen Sie die folgenden URLs zur Positivliste hinzu:

- `https://*.cloud.com`
- Adresse des Identitätsanbieters. Lesen Sie die Anweisungen in der entsprechenden Identitätsanbieter-Dokumentation.
- `https://*.wsp.cloud.com`

Erlauben bestimmten URLs den Zugriff auf die folgenden Adressen:

- `<yourcustomer>.cloud.com`

Citrix Secure Private Access

- `ngspolicy.netscalergateway.net`
- `config.netscalergateway.net`
- `app.netscalergateway.net`
- `http://tunnel.netscalergateway.net/`

Global App Configuration Service

Weitere Informationen finden Sie unter Konnektivität des Global App Configuration Service in diesem Artikel.

Authentifizierung

- `accounts.cloud.com`
- `accounts-dsauthweb.cloud.com`

Stellen Sie sicher, dass die URLs des Identitätsanbieters auch von den Endbenutzergeräten aus zugänglich sind.

Citrix Analytics Service

- `locus.analytics.cloud.com`

Ermöglichen Sie je nach Standort den Zugriff auf die entsprechende URL aus der folgenden Liste:

- USA: `citrixanalyticseh.servicebus.windows.net`
- EU: `citrixanalyticseheu.servicebus.windows.net`
- APS: `citrixanalyticsehaps.servicebus.windows.net`

Elemente der grafischen Workspace-Oberfläche

- ctx-ws-assets.cloud.com

Personalisierung, Benachrichtigungen und Feature-Rollout

- customer-**interface**-personalization.us.wsp.cloud.com
- user-personalization.us.wsp.cloud.com
- admin-notification.us.wsp.cloud.com
- customer-**interface**-personalization.eu.wsp.cloud.com
- user-personalization.eu.wsp.cloud.com
- admin-notification.eu.wsp.cloud.com
- customer-**interface**-personalization.ap-s.wsp.cloud.com
- user-personalization.ap-s.wsp.cloud.com
- admin-notification.ap-s.wsp.cloud.com
- feature-rollout.us.wsp.cloud.com
- feature-rollout.eu.wsp.cloud.com
- feature-rollout.ap-s.wsp.cloud.com

Geräteregistrierungsdienst

- device-registration.us.wsp.cloud.com
- device-registration.eu.wsp.cloud.com
- device-registration.ap-s.wsp.cloud.com

Pushbenachrichtigungsdienst

- push-events-signalr.us.wsp.cloud.com
- push-events-signalr.eu.wsp.cloud.com
- push-events-signalr.ap-s.wsp.cloud.com

Citrix Gateway Service

- https://*.g.nssvc.net

Single Sign-On für Workspace mit dem Citrix Verbundauthentifizierungsdienst (FAS)

Die Konsole und der FAS-Dienst greifen über das Benutzerkonto bzw. das Netzwerkdienstkonto auf folgende Adressen zu.

- FAS-Verwaltungskonsole, unter dem Benutzerkonto:
  - `https://*.cloud.com`
  - `https://*.citrixworkspacesapi.net`
  - `https://*.citrixnetworkapi.net/`
  - Adressen, die von einem externen Identitätsanbieter benötigt werden (sofern dieser in Ihrer Umgebung verwendet wird)
- FAS-Dienst, über das Netzwerkdienstkonto:
  - `https://*.citrixworkspacesapi.net`
  - `https://*.citrixnetworkapi.net/`

Wenn Ihre Umgebung Proxyserver enthält, konfigurieren Sie den Benutzerproxy mit den Adressen für die FAS-Verwaltungskonsole. Stellen Sie außerdem sicher, dass die Adresse für das Netzwerkdienstkonto entsprechend Ihrer Umgebung konfiguriert ist.

Wenn Sie Active Directory oder Active Directory plus zeitbasiertes Einmalkennwort (TOTP) als Identitätsanbieter für die Citrix Workspace-App verwenden, müssen Sie auch `login.cloud.com` auf die Positivliste setzen. Wenn Sie andere Identitätsanbieter verwenden, lassen Sie die Identitätsanbieter-URLs separat zu.

CAS Event Hub-URLs sind ebenfalls standortabhängig. citrixanalyticseh-alias.servicebus.windows.net

Workspace Environment Management Service-Konnektivität

Citrix Ressourcenstandort/Cloud Connector/Agent:

`https://*.wem.cloud.com`

Die vollständigen Anforderungen finden Sie unter Voraussetzungen für Konnektivität in der Dokumentation zu Workspace Environment Management Service.

Bereitstellung planen

July 2, 2024

Die Customer Journey-Perspektive finden Sie im Citrix Success Center. Das Success Center bietet Unterstützung bei den fünf wichtigsten Phasen der Citrix Journey: Planen, Erstellen, Rollout, Verwalten und Optimieren. Die Artikel und Leitfäden im Success Center bieten in Ergänzung zu dieser Dokumentation eine weite, lösungsbasierte Perspektive.

Testversionen und Abonnements von Diensten

Citrix Cloud bietet Testversionen für die meisten Clouddienste. Testversionen haben dieselben Merkmale und Funktionen wie kostenpflichtige Dienste und eignen sich daher für eine Machbarkeitsstudie oder ein Pilotprojekt. Weitere Informationen finden Sie unter Citrix Cloud Service - Testversionen.

Kostenpflichtige Dienstansprüche haben in der Regel eine monatliche, jährliche oder befristete Dauer. Gegen Ende des Anspruchs sendet Citrix Cloud Erinnerungen, und es wird ein Kulanzzeitraum gewährt, damit Sie Ihren Anspruch ohne größere Serviceunterbrechungen verlängern können. Weitere Informationen zur Verlängerung Ihrer Ansprüche finden Sie unter Citrix Cloud-Serviceabonnements verlängern.

Regionen und Servicepräsenz

Citrix Cloud bietet Dienste in drei Regionen: USA, Europäische Union und Asien-Pazifik. Wenn Sie sich bei Citrix Cloud registrieren, müssen Sie die Region auswählen, die Ihren Leistungs- und Geschäftsanforderungen am besten entspricht.

Weitere Informationen zur Auswahl einer Region und zu den Diensten, die in jeder Region verfügbar sind, finden Sie unter Geografische Überlegungen.

Ressourcen für die Bereitstellung

- Citrix Cloud Resiliency
- Tech Zone –Proof of Concept guides
- Tech Zone –Reference Architectures
- Überlegungen zur Skalierung und Größe für Cloud Connectors
- Überlegungen zur Skalierung und Größe für den lokalen Hostcache
- Referenzarchitekturen der On-Premises-StoreFront-Authentifizierung für Citrix DaaS

Ressourcen zur Migration

- Proof of Concept: Automated Configuration Tool
- Migrieren der On-Premises-Version von Citrix Virtual Apps and Desktops zu Citrix Cloud
- Migrating Citrix Virtual Apps and Desktops from VMware vSphere to Citrix DaaS on Microsoft Azure
- Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management

Weitere Informationen

- Citrix Discussions: Citrix Cloud: Community-Supportforen für Citrix Cloud und Citrix Cloud Services
- Citrix-Schulungen:
  - Fundamentals of Citrix Cloud
  - Introduction to Citrix Identity and Authentication

Citrix Cloud Services –Testversionen

July 2, 2024

Testversionen für einzelne Citrix Cloud Services werden über die Citrix Cloud-Verwaltungskonsole bereitgestellt. Testversionen entsprechen in ihrer Funktionsweise einer erworbenen Vollversion und sind daher für Machbarkeitsstudien oder Testumgebungen geeignet.

Wenn Sie Citrix Cloud Services erwerben, wird Ihre Testversion in eine Produktionsversion umgewandelt. Sie müssen nichts neu konfigurieren und kein separates Produktionskonto erstellen.

Überblick über die Services-Testversion

Die Informationen in diesem Abschnitt gelten für die meisten Citrix Cloud Services-Testversionen. Services, für die andere Bestimmungen gelten, werden in eigenen Abschnitten beschrieben.

		Citrix Cloud-Testversion
	Anzahl der zugelassenen Abonnenten	25
	Maximale Testdauer	60 Kalendertage
	Kulanzzeitraum	14 Tage nach Ablauf der Testversion
	Aufbewahrungszeitraum für Daten	90 Kalendertage nach Ablauf der Testversion
	Verfügbarkeit	Eingeschränkte Verfügbarkeit
	Ressourcenstandort	Bereitgestellt und konfiguriert vom Kunden
	Dauer der Benutzersitzung	Unbegrenzt

		Citrix Cloud-Testversion
	Integration mit lokalem Microsoft Active Directory	Ja
	Wahl der Ressourcenstandorte	Ja
	On-Premises-Bereitstellung	Ja
	Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)	Kompletter Funktionsumfang
	Endpoint Management	Kompletter Funktionsumfang
	Anpassungsfähigkeit	Ja

Anfordern einer Service-Testversion

Der Citrix Cloud-Testzugriff wird pro Service verwaltet. Für einige Services können Sie eine Testversion anfordern (siehe Anfordern einer Testversion im vorliegenden Artikel). Für andere müssen Sie vor Erhalt des Testzugriffs eine Vorführung anfordern (siehe Anfordern einer Servicevorführung im vorliegenden Artikel).

Länge des Service-Testzeitraums

Bei den meisten Services haben Sie nach Genehmigung Ihrer Anforderung 60 Tage Zeit zum Testen. Sie können die Service-Testversion nur einmal anfordern.

Abonnement eines Service

Sie können während der Testphase oder während des Datenaufbewahrungszeitraums jederzeit ein Serviceabonnement erwerben. Weitere Informationen finden Sie unter Erwerb von Citrix Cloud Services.

Wenn Sie einen Service abonniert haben, wird Ihre Testversion in einen Produktionsservice umgewandelt. Administratoren und Benutzer können auf den Service zugreifen und alle Daten, die Sie der Testversion hinzugefügt haben, bleiben erhalten.

Citrix DaaS Standard für Azure

In diesem Abschnitt werden die folgenden Testarten für Citrix DaaS Standard für Azure (früher Citrix Virtual Apps and Desktops Standard für Azure) beschrieben:

- **Automatisch genehmigte Testversion:** Nachdem Sie die Testversion über die Citrix Cloud-Verwaltungskonsole angefordert haben, wird sie automatisch genehmigt und kann verwendet werden.
- **Vom Vertrieb genehmigte Testversion:** Nachdem Sie eine Testversion bei einem Citrix Vertriebsbeauftragten angefordert haben, genehmigt dieser die Testversion. Nach der Genehmigung ist die Testversion einsatzbereit.

		Automatisch genehmigte Testversion	Vom Vertrieb genehmigte Testversion
	Maximale Testdauer	7 Kalendertage	14 Kalendertage
	Kulanzzeitraum	1 Kalendertag nach Ablauf der Testversion	14 Kalendertage nach Ablauf der Testversion
	Aufbewahrungszeitraum für Daten	30 Kalendertage nach Ablauf der Testversion	90 Kalendertage nach Ablauf der Testversion

Je nach Testtyp haben Sie sieben oder 14 Tage Zeit, um den Service zu nutzen. Sie können die Testversion für den Service nur einmal anfordern.

Testversionen umfassen einen Kulanzzeitraum für den Zugriff nach Ablauf der Testphase. Während des Kulanzzeitraums können Sie den Service abonnieren oder alle Daten entfernen, die Sie dem Service hinzugefügt haben. Nach Ablauf des Kulanzzeitraums sperrt Citrix den Zugriff auf den Service für Benutzer und Administratoren.

Je nach Testtyp bewahrt Citrix alle Daten, die Sie dem Service hinzufügen, 30 oder 90 Tage nach Ablauf der Testversion auf. Wenn Sie während des Aufbewahrungszeitraums den Service abonnieren, können Ihre Administratoren und Benutzer wieder auf diesen und die Daten zugreifen.

Sie können Services über Azure Marketplace oder beim Citrix Vertrieb abonnierem.

Anfordern einer Servicevorführung

Bei einigen Services müssen Sie eine Vorführung durch einen Citrix Vertriebsmitarbeiter anfordern, bevor Sie den Service testen können. Bei der Vorführung können Sie die Anforderungen Ihres Unternehmens mit dem Citrix Vertriebsbeauftragten besprechen. Dieser stellt außerdem sicher, dass Sie über alle Informationen verfügen, die für die Nutzung des Service erforderlich sind.

1. Melden Sie sich bei Ihrem Citrix Cloud-Konto an.
2. Wählen Sie in der Verwaltungskonsole für den gewünschten Service **Demo anfordern**. Die Anforderungsseite wird angezeigt.

3. Füllen Sie das Formular aus und senden Sie es ab. Ein Citrix Vertriebsmitarbeiter wird sich mit Ihnen in Verbindung setzen, um Ihnen weitere Informationen zu geben und die Nutzung des Service zu erläutern.

Anfordern der Testversion für einen Service

1. Melden Sie sich bei Ihrem Citrix Cloud-Konto an.
2. Wählen Sie in der Verwaltungskonsole für den gewünschten Service **Testversion anfordern**.

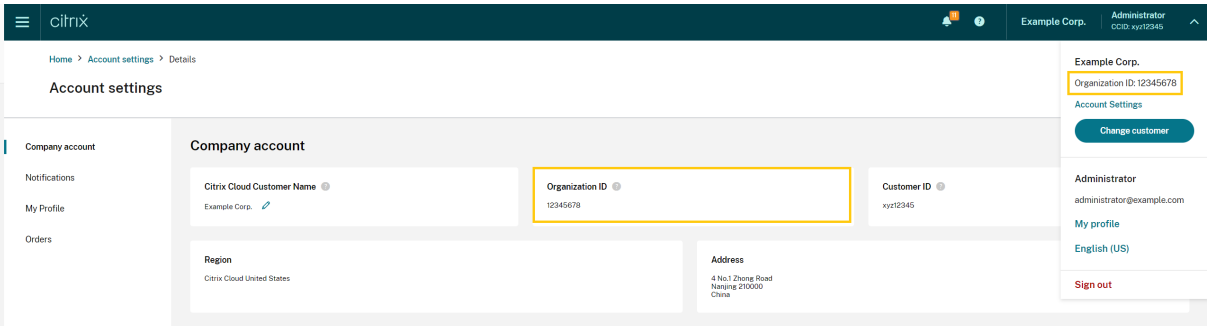
Sobald die Testversion genehmigt und einsatzbereit ist, sendet Citrix Ihnen eine E-Mail-Benachrichtigung.

> **Hinweis:**
>
> Um das beste Kundenerlebnis zu bieten, behält sich Citrix das Recht vor, Testversionen für eine begrenzte Anzahl von Teilnehmern zu genehmigen.

Erwerb von Citrix Cloud Services

Wenn Sie Ihre Testversion in einen Produktionsservice umwandeln möchten, finden Sie unter https://www.citrix.com/buy/ einen Citrix Partner in Ihrer Nähe.

Für den Erwerb von Citrix Cloud Services benötigen Sie Ihre Organisations-ID (OrgID). Ihre OrgID wird im Kundenmenü in der oberen rechten Ecke der Citrix Cloud-Verwaltungskonsole angezeigt. Ihre OrgID wird auch auf der Seite **Kontoeinstellungen** angezeigt.



Weitere Informationen

- Nutzungsbedingungen für Citrix Cloud Services
- Das im Kurs Fundamentals of Citrix Cloud enthaltene kurze Video erklärt die Anforderung einer Testversion. Der vollständige Kurs deckt außerdem die Komponenten der Citrix Cloud-Plattform und ihrer Service ab.

Citrix Cloud-Serviceabonnements verlängern

July 2, 2024

In diesem Artikel wird beschrieben, was geschieht, wenn erworbene Abonnements für Citrix Cloud Services ablaufen, und wie Sie Ihr Abonnement verlängern können.

In diesem Artikel bezieht sich der Begriff *Monatsabonnement* auf Services, die von Monat zu Monat erworben werden. *Jahresabonnements* sind Services, die jährlich erworben werden. *Mehrjahresabonnements* sind Services, die für mehrere Jahre erworben werden.

> **Hinweis:**
>
> Citrix Service Provider (CSPs) können ihre Abonnements verlängern, indem sie eine Null-Dollar-Bestellung an ihren CSP-Distributor senden. Weitere Informationen zur Verlängerung und Lizenzierung von CSP-Produkten finden Sie im *Citrix Service Provider Licensing Guide for Citrix Cloud* auf der Website Citrix Partner Central.

Vor dem Ablauf

Für Monatsabonnements sendet Citrix Cloud vor Ablauf keine Benachrichtigungen.

Bei Jahres- und Mehrjahresabonnements benachrichtigt Citrix Cloud Sie in bestimmten Intervallen, wenn Ihr Abonnement bald abläuft. Diese Benachrichtigungen weisen Sie darauf hin, das Abonnement zu verlängern, um Serviceunterbrechungen zu vermeiden. Folgende Benachrichtigungen werden in der Citrix Cloud-Verwaltungskonsole angezeigt:

- 90 Tage vor Ablauf: Ein gelbes Banner zeigt die zu verlängernden Dienste und ihr Ablaufdatum an. Diese Benachrichtigung erscheint alle sieben Tage in der Konsole oder bis der Dienst verlängert wird.
- Sieben Tage vor Ablauf: Ein rotes Banner zeigt die zu verlängernden Services und ihr Ablaufdatum an. Diese Benachrichtigung wird in der Konsole angezeigt, bis der Dienst verlängert wurde oder bis zum Ende des 30-tägigen Kulanzzeitraums.

Sie können diese Benachrichtigungen schließen. Nach sieben Tagen werden sie jedoch erneut angezeigt.

Citrix sendet Ihnen außerdem eine E-Mail-Benachrichtigung mit einer Liste aller zu verlängernden Dienste und ihrem Ablaufdaten. Citrix sendet diese Benachrichtigung in folgenden Abständen:

- 90 Tage vor Ablauf
- 60 Tage vor Ablauf
- 30 Tage vor Ablauf

- Sieben Tage vor Ablauf
- Einen Tag vor Ablauf

Nach Ablauf: Dienstsperre und Datenbeibehaltung

Wird das Abonnement während des Kulanzzeitraums nicht verlängert, sperrt Citrix den Zugriff wie folgt:

- Bei abgelaufenen Monatsabonnements werden Administratoren und Benutzer fünf Tage nach Ablaufdatum ausgesperrt.
- Bei abgelaufenen Jahres- und Mehrjahresabonnements werden Administratoren und Benutzer 30 Tage nach Ablaufdatum ausgesperrt.

Citrix speichert alle Daten, die Sie einem Service hinzugefügt haben, für 90 Tage nach Ablaufdatum. Wenn Sie Ihr Abonnement vor Ablauf des 90-tägigen Beibehaltungszeitraums verlängern, können Ihre Administratoren und Benutzer wieder auf den Dienst und Ihre Daten zugreifen. Ein verlängertes Abonnement beginnt wie folgt:

- Bei Monatsabonnements ist das Anfangsdatum des ersten Abonnementmonats das Datum, an dem Sie die Verlängerung erwerben. Danach erfolgt automatisch eine Verlängerung am ersten Tag jedes Folgemonats.
- Die Verlängerung von Jahres- und Mehrjahresabonnements beginnt am Tag nach dem Datum von deren Erwerb. Wenn Ihr Abonnement beispielsweise am 30. September abläuft und Sie es am 23. Oktober verlängern, ist das Startdatum der Verlängerung der 1. Oktober.

Wenn Sie Ihr Abonnement vor Ablauf des 90-tägigen Aufbewahrungszeitraums nicht verlängern, setzt Citrix den Service zurück und löscht alle von Ihnen hinzugefügten Daten. Wenn Sie zugestimmt haben, dass Citrix Ihre Cloudbereitstellung verwaltet (z. B. bei Citrix Essentials Services oder der Azure Quick Deploy-Option in Citrix DaaS), führt Citrix die folgenden Aktionen durch, wenn der 90-tägige Aufbewahrungszeitraum abgelaufen ist:

- Alle kundenbezogenen Daten werden aus Citrix Datenbanken entfernt.
- Alle Ressourcen im Zusammenhang mit Citrix Cloud-Services, einschließlich von Citrix verwalteter VMs, die Citrix in Ihrer Cloud-Umgebung bereitgestellt hat, werden gelöscht. Eine Beschreibung der von Citrix verwalteten Komponenten in den verschiedenen Citrix Cloud-Services finden Sie in der Dokumentation zum jeweiligen Service.

Vom Kunden verwaltete Azure-Abonnements

Wenn Sie Ihr eigenes Azure-Abonnement für einen Citrix Cloud-Service verwenden, installiert der Service eine App, wenn Sie das Azure-Abonnement mit dem Service verbinden. Wenn Sie Ihr Citrix Cloud-Abonnement nicht verlängern, entfernt Citrix diese App nicht aus Ihrem Azure-Abonnement, wenn

der 90-tägige Aufbewahrungszeitraum abgelaufen ist. Sie müssen die App löschen, um den Service vollständig aus Ihrem Azure-Abonnement zu entfernen. Sie können die App mit einer der folgenden Methoden löschen:

- Wenn Sie noch Administratorzugriff auf den Service haben, löschen Sie die App im Service.
- Wenn Sie keinen Administratorzugriff mehr auf den Service haben, löschen Sie die App im Azure-Portal.

Erwerb von Dienstverlängerungen

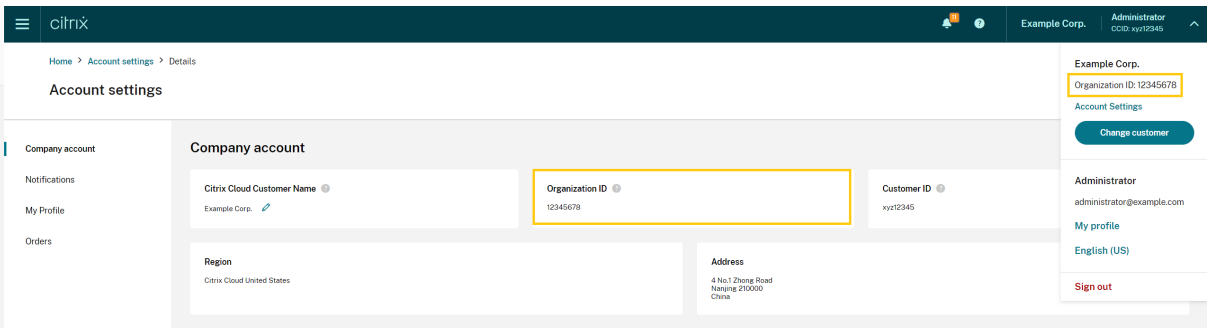
Um Ihr Abonnement für Citrix Cloud Services zu verlängern, wenden Sie sich an Ihren Citrix-Vertriebsmitarbeiter. Gehen Sie wie folgt vor, um Ihren Vertriebsmitarbeiter zu finden:

1. Melden Sie sich an Ihrem Citrix-Konto an.
2. Wählen Sie **Quoting (DOTI)** und dann **Transactions** aus. Ihr Vertriebsmitarbeiter und seine E-Mail-Adresse werden oben in dieser Ansicht angezeigt.

Alternativ finden Sie auf der Seite Citrix Customer Service Kontaktinformationen für Ihre geografische Region.

Um den Kauf abzuschließen, benötigt Ihr Vertriebsmitarbeiter die Organisations-ID für Ihr Citrix Cloud-Konto. Um Ihre Organisations-ID zu finden, melden Sie sich an Ihrem Citrix Cloud-Konto an. Ihre Organisations-ID wird an den folgenden Stellen angezeigt:

- Im Kundenmenü in der oberen rechten Ecke der Citrix Cloud-Konsole.
- Auf der Seite **Kontoeinstellungen**.



Geografische Überlegungen

July 2, 2024

In diesem Artikel werden die von Citrix Cloud genutzten kommerziellen Regionen und vorhandene kommerzielle Citrix Cloud Services in jeder Region erläutert.

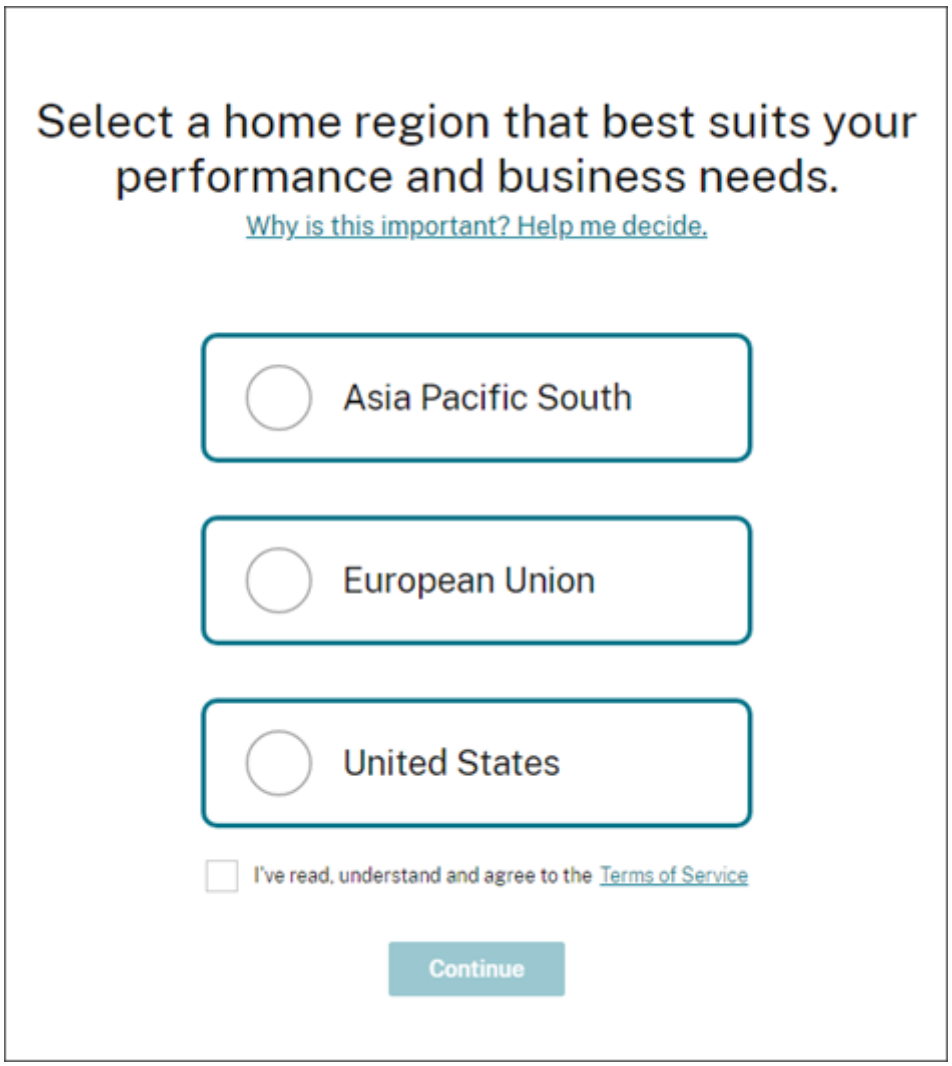
Weitere Informationen zu geografischen Regionen und Services, die Citrix für Cloud-Plattformen für den öffentlichen Sektor bzw. für dedizierte Umgebungen bietet, finden Sie unter Andere Cloud-Plattformen von Citrix.

Region wählen

Wenn Ihre Organisation bei Citrix Cloud registriert wurde und Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, eine der folgenden Regionen auszuwählen:

- USA
- Europäische Union
- Asien-Pazifik

Wenn Sie eine Region auswählen, werden in dieser geografischen Region gehostete Dienste nach Möglichkeit für Aktionen verwendet, die der Organisation zugeordnet sind. Wählen Sie eine Region, die dem Standort der Mehrheit Ihrer Benutzer und Ressourcen entspricht.



> **Wichtige Hinweise:**
>
> - Sie können die Region nur einmal beim Onboarding Ihrer Organisation auswählen. Sie können die Region später nicht ändern.
> - Wenn Sie einen Service in einer anderen Region als der eigenen verwenden, sind Leistungseinbußen minimal. Citrix Cloud Services wurden für die globale Verwendung entwickelt. Beispielsweise sind die Auswirkungen durch Latenz minimal bei Kunden in den USA, die Benutzer und Connectors in Australien haben.
> - Wenn Citrix Cloud in Ihrer Region nicht unterstützt wird, wählen Sie eine Region aus, die dem Standort der meisten Benutzer und Ressourcen am nächsten liegt.

Servicepräsenz in jeder Region

Die meisten Citrix Cloud-Dienste werden weltweit repliziert. Die ausgewählte Region gilt als der bevorzugte Ort, an dem Verbindungen hergestellt werden müssen. Es können jedoch immer noch Verbindungen zu anderen geografischen Regionen hergestellt werden. Wenn ein Service weltweit repliziert wurde, werden alle Daten für den Service in allen Regionen gespeichert.

Außerdem werden Ihre Daten möglicherweise global von verbundenen Citrix-Unternehmen oder Unterauftragsverarbeitern verarbeitet, wenn dies für die Erbringung der Dienste erforderlich ist.

Bestimmte Services haben dedizierte regionale Instanzen. Für einige Services gibt es aber nur Instanzen in den USA. In diesen Fällen sind Verbindungen und Daten in der geografischen Region enthalten.

Wenn ein Service in der Region, die Sie für Ihre Organisation ausgewählt haben, nicht verfügbar ist, werden bestimmte Informationen (z. B. Authentifizierungsdaten) bei Bedarf zwischen Regionen übertragen.

Service	US	EU	Asien-Pazifik	Hinweise
Citrix Cloud-Steuerungsebene	Ja	Ja	Ja	
Citrix Analytics für Sicherheit	Ja	Ja	Ja	
Citrix Analytics für Leistung	Ja	Ja	Ja	

Service	US	EU	Asien-Pazifik	Hinweise
NetScaler Console (früher Application Delivery Management)	Ja	Ja	Ja	Weitere Informationen finden Sie in diesem Artikel unter Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von Console Advisory Connect . Informationen zum lokalen Telemetrie-Programm für die Konsole finden Sie hier.
Citrix DaaS (früher Virtual Apps and Desktops Service)	Ja	Ja	Ja	Der Service verwendet die Citrix Cloud-Region.
Citrix DaaS Standard für Azure (früher Virtual Apps and Desktops Standard für Azure)	Ja	Ja	Ja	Der Service verwendet die Citrix Cloud-Region.
Citrix DaaS Standard für Google Cloud (früher Virtual Apps and Desktops Standard für Google Cloud)	Ja	Nein - verwendet Region USA	Nein - verwendet Region USA	

Service	US	EU	Asien-Pazifik	Hinweise
Citrix DaaS Premium für Google Cloud (früher Virtual Apps and Desktops Premium für Google Cloud)	Ja	Nein - verwendet Region USA	Nein - verwendet Region USA	
Citrix Endpoint Management	Ja	Ja	Ja	Zur Auswahl stehen mehrere Standorte in mehreren Regionen. Weitere Informationen finden Sie unter Endpoint Management-Servicestandorte in diesem Artikel.
Remote Browser Isolation-Dienst	Ja	Ja	Ja	Der Service verwendet die Citrix Cloud-Region.
SD-WAN Orchestrator	Ja	Ja	Ja	
Citrix Secure Internet Access-Knoten/POP	Mehrere globale Knoten; Datenverkehr wird nach Bedarf weitergeleitet, um eine erstklassige Benutzererfahrung zu gewährleisten	Mehrere globale Knoten; Datenverkehr wird nach Bedarf weitergeleitet, um eine erstklassige Benutzererfahrung zu gewährleisten	Mehrere globale Knoten; Datenverkehr wird nach Bedarf weitergeleitet, um eine erstklassige Benutzererfahrung zu gewährleisten	Weitere Informationen finden Sie unter Servicestandorte für sicheren Internetzugriff

Service	US	EU	Asien-Pazifik	Hinweise
Citrix Secure Private Access	Global repliziert	Global repliziert	Global repliziert	Weitere Informationen finden Sie unter Secure Private Access Points of Presence in diesem Artikel.
Sitzungsaufzeichnungsdienst	Ja	Ja	Ja	
Citrix Virtual Apps Essentials	Ja	Ja	Ja	Der Service verwendet die Citrix Cloud-Region.
Citrix Virtual Desktops Essentials	Ja	Ja	Ja	Der Service verwendet die Citrix Cloud-Region.
Web App Firewall	Ja	Ja	Nein - verwendet Region USA	
Workspace Environment Management; Citrix Optimization Pack	Ja	Ja	Ja	
Networking-Services	Ja	Nein - verwendet Region USA	Nein - verwendet Region USA	
License Usage Insights Service (nur CSPs)	Global repliziert	Global repliziert	Global repliziert	

Service	US	EU	Asien-Pazifik	Hinweise
Citrix Gateway Service-Zugriffsknoten/POP	Mehrere globale Knoten; Datenverkehr wird nach Bedarf weitergeleitet, um eine erstklassige Benutzererfahrung zu gewährleisten	Mehrere globale Knoten; Datenverkehr wird nach Bedarf weitergeleitet, um eine erstklassige Benutzererfahrung zu gewährleisten	Mehrere globale Knoten; Datenverkehr wird nach Bedarf weitergeleitet, um eine erstklassige Benutzererfahrung zu gewährleisten	Sie können Ressourcenstandorte so konfigurieren, dass der Benutzerverkehr an bestimmte Regionen weitergeleitet wird. Weitere Informationen finden Sie unter Geolocation Routing – Vorschau

> **Hinweis:**
>
> Bestimmte regionale Services können mit Ansprüchen auf nicht-regionale Komponentenservices bereitgestellt werden, die an anderer Stelle in der obigen Tabelle aufgeführt sind, und können nach Wahl des Kunden genutzt werden.
>
> Citrix Cloud Services nutzt die vom Kunden angegebene Region zum Speichern von Kundeninhalten und Protokollen. Ausnahme bilden bestimmte Protokolle, die von Citrix Auftragsverarbeitern erfasst werden, oder wenn für die Serviceleistung eine nicht regionale Speicherung erforderlich ist, u. a. Support oder Fehlerbehebung, Leistungsüberwachung, Sicherheit und Audits, sowie zum Ermöglichen einer regionsübergreifenden Authentifizierung (z. B. wenn ein in der EU ansässiger Support-Techniker auf eine Umgebung in den USA zugreifen muss). Auf Kundeninhalte und -protokolle kann weltweit zugegriffen werden, sofern dies für die Erbringung des Service erforderlich ist.

Weitere Informationen über die Daten, die von den einzelnen Services gespeichert werden, finden Sie unter Technische Sicherheit für den jeweiligen Service.

Low-Touch-Onboarding von NetScaler Console-Instanzen mithilfe von Console Advisory Connect

Im Rahmen des Console Advisory Connect-basierten Low-Touch-Onboarding von Console-Instanzen:

- Wenn Sie bereits ein Citrix Cloud-Kunde sind, wird der Console Service-Mandant in der geografischen Region erstellt, die Sie beim Erstellen Ihres Citrix Cloud-Kontos ausgewählt haben.
- Wenn Sie noch kein Citrix Cloud-Kunde sind, wird auf die für diesen Kunden angegebene Adresse im Citrix.com-Portal verwiesen. Ein Console Service-Platzhaltermandant wird in der geografischen Region erstellt, die der Region dieser angegebenen Adresse entspricht. Bei einem zukünftigen Citrix Cloud-Onboarding wird ein neuer Console Service-Mandant in der geografischen Region erstellt, die Sie beim Erstellen Ihres Citrix Cloud-Kontos ausgewählt haben. Außerdem werden die Daten des Console Service-Platzhaltermandanten zum neuen Console Service-Mandanten migriert.

Endpoint Management-Servicestandorte

Sie können einen der folgenden Endpoint Management-Servicestandorte für Ihre Heimatregion auswählen:

- USA Osten
- USA Westen
- EU Westen
- SE Asia
- Sydney

Servicestandorte für sicheren Internetzugriff

Der Datenverkehr wird basierend auf Verfügbarkeit und Nähe für Endbenutzer an die folgenden Servicestandorte für sicheren Internetzugriff weitergeleitet, um die beste Benutzererfahrung zu gewährleisten.

Nordamerika

- Sterling, VA, USA
- Toronto, Kanada
- Los Angeles, CA, USA
- Irvine, CA, USA
- Seattle, WA, USA
- Denver, CO, USA
- Charlotte, NC, USA
- Dallas, TX, USA
- Allen, TX, USA

- Miami, FL, USA
- Chicago, IL, USA
- New York, NY, USA
- Boston, MA, USA
- Vancouver, Kanada

Südamerika

- Queretaro, Mexiko
- Sao Paulo, Brasilien
- Buenos Aires, Argentinien
- Bogota, Kolumbien

Asien-Pazifik-Raum

- Perth, Australien
- Sydney, Australien
- Tokio, Japan
- Singapur, Singapur
- Mumbai, Indien
- Delhi, Indien

Afrika

Johannesburg, Südafrika

Naher Osten

- Dubai, Vereinigte Arabische Emirate
- Istanbul, Türkei

Westeuropa

- London, Großbritannien
- Manchester, Großbritannien
- Frankfurt, Deutschland
- Düsseldorf, Deutschland
- Mannheim, Deutschland
- Paris, Frankreich

Europa

- Helsinki, Finnland
- Amsterdam, Niederlande
- Stockholm, Schweden
- Warschau, Polen
- Madrid, Spanien
- Sofia, Bulgarien
- Zürich, Schweiz
- Mailand, Italien

Secure Private Access Points of Presence

Eine Liste der Points of Presence (PoPs), mit deren Hilfe Secure Private Access die Servicekontinuität und -qualität gewährleistet, finden Sie in der Dokumentation zu Secure Private Access Service unter What are the Secure Private Access PoP locations?.

Andere Cloud-Plattformen von Citrix

Neben Citrix Cloud bietet Citrix weitere Clouds an, die isoliert und von Citrix Cloud getrennt sind.

Citrix Cloud Government

Citrix Cloud Government ermöglicht es US-Regierungsbehörden und anderen Kunden aus dem öffentlichen Sektor in den USA, Citrix Cloud Services im Einklang mit regulatorischen Vorgaben und Complianceanforderungen zu nutzen. Citrix Cloud Government ist ein geografisch abgegrenzter Raum, in dem Citrix verschiedene Services und Daten für die Bereitstellung von Citrix Cloud Government-Services ausführt, speichert und repliziert. Citrix verwendet u. U. mehrere öffentliche oder private Clouds in mindestens einem Bundesstaat der USA, um Services bereitzustellen.

Citrix Cloud Government und angebotene Services sind nur in der US-Region verfügbar.

Weitere Informationen finden Sie in der Produktdokumentation zu Citrix Cloud Government.

Citrix Cloud Japan

Citrix Cloud Japan ermöglicht japanischen Kunden die Nutzung bestimmter Citrix Cloud Services in einer dedizierten und von Citrix verwalteten Umgebung. Citrix Cloud Japan und angebotene Services sind nur in Japan verfügbar.

Weitere Informationen finden Sie in der Produktdokumentation zu Citrix Cloud Japan.

Leitfaden zur sicheren Bereitstellung für die Citrix Cloud-Plattform

July 2, 2024

Der Leitfaden zur sicheren Bereitstellung von Citrix Cloud gibt eine Übersicht über bewährte Verfahren zur sicheren Verwendung von Citrix Cloud und beschreibt, welche Daten von Citrix Cloud erfasst und verwaltet werden.

Informationen zur technischen Sicherheit für Services

Die folgenden Artikel enthalten weitere Informationen zur Datensicherheit in Citrix Cloud Services:

- Analytics –Technische Sicherheit
- Endpoint Management –Technische Sicherheit
- Remote Browser Isolation –Technische Sicherheit
- Citrix DaaS —Technische Sicherheit —Überblick
- Citrix DaaS Standard für Azure —Technische Sicherheit —Überblick

Hinweise für Administratoren

- Verwenden Sie sichere Kennwörter und ändern Sie diese regelmäßig.
- Alle Administratoren innerhalb eines Kundenkontos können andere Administratoren hinzufügen und entfernen. Stellen Sie sicher, dass nur vertrauenswürdige Administratoren auf Citrix Cloud zugreifen können.
- Administratoren eines Kunden erhalten standardmäßig vollen Zugriff auf alle Services. Einige Services bieten die Möglichkeit, den Zugriff eines Administrators zu beschränken. Weitere Informationen hierzu finden Sie in der Dokumentation für den Service.
- Die zweistufige Authentifizierung von Citrix Cloud-Administratoren erfolgt anhand des standardmäßigen Citrix Identitätsanbieters. Wenn Administratoren sich für Citrix Cloud registrieren oder zu einem Citrix Cloud-Konto eingeladen werden, müssen sie sich für die Multifaktorauthentifizierung registrieren. Wenn ein Kunde Microsoft Azure zum Authentifizieren von Citrix Cloud-Administratoren verwendet, kann die Multifaktorauthentifizierung gemäß den Erläuterungen unter Konfigurieren von Azure AD Multi-Factor Authentication-Einstellungen auf der Microsoft-Website konfiguriert werden.
- Standardmäßig werden Administratorsitzungen in Citrix Cloud nach 24 Stunden Inaktivität, unabhängig von der Konsolenaktivität, automatisch beendet. Dieses Timeout kann nicht geändert werden.
- Administratorkonten können mit maximal 100 Kundenkonten verknüpft werden. Wenn ein Administrator mehr als 100 Kundenkonten verwalten muss, muss er ein separates Administra-

torkonto mit einer anderen E-Mail-Adresse erstellen, um die zusätzlichen Kundenkonten zu verwalten. Alternativ können Sie den Administrator aus Kundenkonten entfernen, die er nicht mehr verwalten muss.

Kennwort-Compliance

Citrix Cloud fordert Administratoren auf, ihre Kennwörter zu ändern, wenn eine der folgenden Bedingungen erfüllt ist:

- Das aktuelle Kennwort wurde seit über 60 Tagen nicht zur Anmeldung verwendet.
- Das aktuelle Kennwort ist in einer bekannten Datenbank mit gefährdeten Kennwörtern aufgeführt.

Neue Kennwörter müssen alle der folgenden Kriterien erfüllen:

- Mindestens 8 Zeichen lang (maximal 128 Zeichen)
- Mindestens ein Groß- und Kleinbuchstabe
- Mindestens eine Ziffer
- Mindestens ein Sonderzeichen wie ! @ # $% ^ *? + = -

Regeln zum Ändern von Kennwörtern:

- Das aktuelle Kennwort kann nicht als neues Kennwort verwendet werden.
- Die vorherigen 5 Kennwörter können nicht erneut verwendet werden.
- Das neue Kennwort darf nicht dem Benutzernamen des Kontos ähneln.
- Das neue Kennwort darf nicht in einer bekannten Datenbank mit gefährdeten Kennwörtern aufgeführt sein. Citrix Cloud prüft anhand einer von https://haveibeenpwned.com/ bereitgestellten Liste, ob neue Kennwörter gegen diese Bedingung verstoßen.

Verschlüsselung und Schlüsselverwaltung

In der Citrix Cloud-Steuerungsebene werden keine vertraulichen Kundeninformationen gespeichert. Stattdessen ruft Citrix Cloud Informationen wie Administratorkennwörter bei Bedarf ab (wobei der Administrator explizit zur Eingabe aufgefordert wird).

Für ruhende Daten werden zur Verschlüsselung des Citrix Cloud-Speichers Schlüssel verwendet, die AES-256-Bit oder höher sind. Diese Schlüssel werden von Citrix verwaltet.

Für Daten im Übertragungsprozess (Data-in-Flight) verwendet Citrix branchenübliches TLS 1.2 mit den stärksten Verschlüsselungssammlungen. Kunden haben keinen Einfluss auf das verwendete TLS-Zertifikat, da Citrix Cloud auf der Citrix-eigenen Domäne cloud.com gehostet wird. Für den Zugriff auf Citrix Cloud müssen Kunden einen TLS 1.2-kompatiblen Browser mit zulässigen Verschlüsselungssammlungen verwenden.

- Wenn Sie von Windows Server 2016, Windows Server 2019 oder Windows Server 2022 auf die Citrix Cloud-Steuerungsebene zugreifen, werden die folgenden starken Verschlüsselungssammlungen empfohlen: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GC
- Wenn Sie von Windows Server 2012 R2 auf die Citrix Cloud-Steuerungsebene zugreifen, sind die starken Verschlüsselungssammlungen nicht verfügbar, sodass die folgenden verwendet werden müssen: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Weitere Informationen zum Datenschutz in Citrix Cloud Services finden Sie auf der Citrix-Website unter Citrix Cloud Services Data Protection Overview.

Weitere Informationen zur Verschlüsselung und Schlüsselverwaltung in jedem Cloudservice finden Sie in der Dokumentation zum Service.

Weitere Informationen zur TLS 1.2-Konfiguration finden Sie in den folgenden Artikeln:

- Erzwingen der Verwendung von TLS 1.2 auf Clientcomputern: CTX245765, Fehlermeldung "Die zugrundeliegende Verbindung wurde geschlossen: Unerwarteter Fehler beim Senden."beim Abfragen des OData-Endpunkts des Überwachungsdiensts
- Aktualisieren und Konfigurieren des .NET-Frameworks zur Unterstützung von TLS 1.2 auf der Microsoft Docs-Website.

Datenhoheit

Die Citrix Cloud-Steuerungsebene wird in den USA, in der Europäischen Union und in Australien gehostet. Kunden haben keine Kontrolle darüber.

Der Kunde besitzt und verwaltet die Ressourcenstandorte, die er mit Citrix Cloud verwendet. Ressourcenstandorte können nach Wunsch in jedem Datencenter oder Standort, in der Cloud oder in einer geografischen Region erstellt werden. Alle wichtigen Geschäftsdaten (z. B. Dokumente, Kalkulationstabellen usw.) sind in den Ressourcenstandorten gespeichert und unter Kundenkontrolle.

Andere Services haben u. U. eine Option, wie Sie Daten in anderen Regionen speichern können. Lesen Sie auch die Geografischen Überlegungen und die Technische Übersicht über die Sicherheit für jeden Service am Anfang dieses Artikels.

Einsicht in Sicherheitsfragen

Die Website status.cloud.com bietet Transparenz in Sicherheitsfragen, die sich dauerhaft auf den Kunden auswirken. Die Site protokolliert Status- und Betriebszeitinformationen. Eine Option zum Abonnieren von Updates für die Plattform oder für einzelne Services ist vorhanden.

Citrix Cloud Connector

Installieren des Cloud Connectors

Aus Sicherheits- und Leistungsgründen empfiehlt Citrix, die Cloud Connector-Software nicht auf einem Domänencontroller zu installieren.

Citrix empfiehlt zudem dringend, dass Maschinen, auf denen der Cloud Connector installiert ist, sich im privaten Netzwerk des Kunden und nicht in der DMZ befinden. Die Netzwerk- und Systemanforderungen des Cloud Connectors sowie Anweisungen für die Installation finden Sie unter Citrix Cloud Connector.

Konfigurieren des Cloud Connectors

Der Kunde ist dafür verantwortlich, die Maschinen, auf denen der Cloud Connector installiert ist, mit Windows-Sicherheitsupdates zu aktualisieren.

Kunden können Antivirensoftware zusammen mit dem Cloud Connector verwenden. Citrix verwendet McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8 für Tests. Citrix unterstützt Kunden, die andere branchenübliche Antivirenprodukte verwenden.

Citrix empfiehlt dringend, im Active Directory (AD) des Kunden das Maschinenkonto des Cloud Connectors auf schreibgeschützten Zugriff zu beschränken. Dies ist die Standardkonfiguration in Active Directory. Kunden können auch die AD-Protokollierung und -Überwachung im Maschinenkonto des Cloud Connectors aktivieren, um den Zugriff auf Active Directory zu überwachen.

Anmeldung an der Maschine, die Cloud Connector hostet

Der Cloud Connector ermöglicht die Übertragung sensibler Daten an andere Plattformkomponenten in Citrix Cloud und speichert außerdem folgende vertraulichen Informationen:

- Dienstschlüssel für die Kommunikation mit Citrix Cloud
- Hypervisor-Dienst-Anmeldeinformationen für die Energieverwaltung in Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)

Diese vertraulichen Informationen werden mit der Data Protection API (DPAPI) auf dem Windows-Server mit dem Cloud Connector verschlüsselt. Citrix empfiehlt dringend, nur den ranghöchsten Administratoren das Anmelden an den Cloud Connector-Maschinen zu erlauben (z. B. für Wartungsvorgänge). Zur allgemeinen Verwaltung eines Citrix Produkts ist es nicht erforderlich, dass ein Administrator sich an diesen Maschinen anmeldet. Der Cloud Connector wird in dieser Hinsicht selbstverwaltet.

Erlauben Sie Endbenutzern nicht, sich an Cloud Connector-Maschinen anzumelden.

Installieren anderer Software auf Cloud Connector-Maschinen

Kunden können Antivirensoftware und Hypervisortools (bei Installation auf einer virtuellen Maschine) auf Cloud Connector-Maschinen installieren. Citrix empfiehlt jedoch, dass Kunden keine weitere Software auf diesen Maschinen installieren. Andere Software kann mögliche Sicherheitslücken schaffen und die Sicherheit der gesamten Citrix Cloud-Lösung gefährden.

Konfiguration von eingehenden und ausgehenden Ports

Für den Cloud Connector muss der ausgehende Port 443 geöffnet sein und Zugriff auf das Internet bieten. Citrix empfiehlt dringend, dass der Cloud Connector keine eingehenden Ports hat, auf die über das Internet zugegriffen werden kann.

Kunden können den Cloud Connector hinter einem Webproxy platzieren, um seine ausgehende Internetkommunikation zu überwachen. Der Webproxy muss jedoch eine SSL/TLS-verschlüsselte Kommunikation unterstützen.

Der Cloud Connector kann andere ausgehende Ports mit Internetzugriff haben. Wenn andere Ports zur Verfügung stehen, kann der Cloud Connector darüber die Netzwerkbandbreite und Leistung optimieren.

Innerhalb des internen Netzwerks muss der Cloud Connector eine Vielzahl eingehender und ausgehender Ports geöffnet haben. Die folgende Tabelle enthält die erforderliche Grundkonfiguration geöffneter Ports.

Clientport	Serverport	Service
49152 -65535/UDP	123/UDP	W32Time
49152 -65535/TCP	135/TCP	RPC-Endpunktzuordnung
49152 -65535/TCP	464/TCP/UDP	Kerberos-Kennwortänderung
49152 -65535/TCP	49152-65535/TCP	RPC für LSA, SAM, Netlogon (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
49152 -65535/TCP/UDP	445/TCP	SMB

Der Cloud Connector verwendet die LDAP-Signatur und -versiegelung, um Verbindungen zum Domänencontroller zu sichern. Dies bedeutet, dass LDAP über SSL (LDAPS) nicht erforderlich ist. Weitere Informationen zur LDAP-Signatur finden Sie unter How to enable LDAP signing in Windows Server und Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing.

Jeder in Citrix Cloud verwendete Service erweitert die Liste der erforderlichen geöffneten Ports. Weitere Informationen finden Sie in folgenden Ressourcen:

- Technischer Überblick über die Sicherheit für jeden Service (siehe Liste am Anfang dieses Artikels)
- Anforderungen an die Internetkonnektivität für Citrix Cloud Services
- Anforderungen an den Konsolendienstport
- Portanforderungen für Endpoint Management

Überwachung der ausgehenden Kommunikation

Der Cloud Connector verwendet Port 443 für die ausgehende Internetkommunikation mit Citrix Cloud-Servern und mit Microsoft Azure Service Bus-Servern.

Der Cloud Connector kommuniziert mit Domänencontrollern im lokalen Netzwerk, die sich in der gleichen Active Directory-Gesamtstruktur wie die Maschinen mit dem Cloud Connector befinden.

Im Normalbetrieb kommuniziert der Cloud Connector nur mit Domänencontrollern in Domänen, die auf der Seite **Identitäts- und Zugriffsverwaltung** von Citrix Cloud nicht deaktiviert sind.

Jeder Service in Citrix Cloud erweitert die Liste der Server und internen Ressourcen, die der Cloud Connector im Rahmen des Normalbetriebs kontaktieren kann. Kunden können nicht steuern, welche Daten vom Cloud Connector an Citrix gesendet werden. Weitere Informationen über interne Ressourcen und Daten, die von Services an Citrix gesendet werden, finden Sie in den folgenden Ressourcen:

- Technischer Überblick über die Sicherheit für jeden Service (siehe Liste am Anfang dieses Artikels)
- Anforderungen an die Internetkonnektivität für Citrix Cloud Services

Anzeigen von Cloud Connector-Protokollen

Alle Informationen, die für einen Administrator relevant sind oder eine Aktion erfordern, sind im Windows-Ereignisprotokoll auf der Cloud Connector-Maschine verfügbar.

Sie finden die Installationsprotokolle für den Cloud Connector in folgenden Verzeichnissen:

- %AppData%\Local\Temp\CitrixLogs\CloudServicesSetup
- %windir%\Temp\CitrixLogs\CloudServicesSetup

Protokolle der Daten, die vom Cloud Connector an die Cloud gesendet werden, sind hier gespeichert: %ProgramData%\Citrix\WorkspaceCloud\Logs.

Wenn Protokolle im Verzeichnis "WorkspaceCloud\Logs"eine bestimmte Größe überschritten haben, werden sie gelöscht. Administratoren können diesen Schwellenwert durch Anpassen des folgenden Registrierungsschlüssels steuern: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CloudServices\AgentAdministration\

SSL/TLS-Konfiguration

Auf dem Windows Server mit dem Cloud Connector müssen die unter Verschlüsselung und Schlüsselverwaltung aufgeführten Verschlüsselungssammlungen aktiviert sein.

Der Cloud Connector muss der Zertifizierungsstelle (ZS) vertrauen, die von SSL/TLS-Zertifikaten von Citrix Cloud und SSL/TLS-Zertifikaten von Microsoft Azure Service Bus verwendet wird. Citrix und Microsoft können Zertifikate und Zertifizierungsstellen zukünftig ändern, sie verwenden jedoch stets Zertifizierungsstellen, die in der Windows-Standardliste vertrauenswürdiger Herausgeber aufgeführt sind.

Jeder Service in Citrix Cloud kann unterschiedliche Anforderungen an die SSL-Konfiguration stellen. Weitere Informationen finden Sie im Technischen Überblick über die Sicherheit für jeden Service (siehe Liste am Anfang dieses Artikels).

Sicherheitskonformität

Zur Gewährleistung der Sicherheitskonformität ist der Cloud Connector selbstverwaltet. Deaktivieren Sie keine Neustarts und definieren Sie keine anderen Einschränkungen auf dem Cloud Connector. Diese Aktionen verhindern, dass der Cloud Connector bei kritischen Updates aktualisiert wird.

Es ist nicht Aufgabe des Kunden, auf Sicherheitsrisiken zu reagieren. Der Cloud Connector wendet automatisch alle Sicherheitsfixes an.

Citrix Connector Appliance für Cloudservices

Installieren des Connectorgeräts

die Connector Appliance wird auf Ihrem Hypervisor gehostet. Der Hypervisor muss sich in Ihrem privaten Netzwerk befinden und darf nicht in der DMZ sein.

Stellen Sie sicher, dass sich die Connector Appliance hinter einer Firewall befindet, die den Zugriff standardmäßig blockiert. Verwenden Sie eine Positivliste, um nur erwarteten Datenverkehr vom Connectorgerät zuzulassen.

Stellen Sie sicher, dass aktuelle Sicherheitsupdates auf den Hypervisoren installiert sind, die Ihr Connectorgerät hosten.

Die Netzwerk- und Systemanforderungen für die Connector Appliance sowie Anweisungen für die Installation finden Sie unter Connector Appliance for Cloud Services.

Anmelden beim Hypervisor, der ein Connectorgerät hostet

Das Connector-Gerät enthält einen Dienstschlüssel für die Kommunikation mit Citrix Cloud. Nur die ranghöchsten Administratoren dürfen sich an dem Hypervisor anmelden, der die Connector Appliance hostet (z. B. für Wartungsvorgänge). Zur allgemeinen Verwaltung eines Citrix Produkts ist es nicht erforderlich, dass ein Administrator sich an diesen Hypervisoren anmeldet. Die Connector Appliance ist selbstverwaltet.

Konfiguration von eingehenden und ausgehenden Ports

Für die Connector Appliance muss der ausgehende Port 443 geöffnet sein und Zugriff auf das Internet bieten. Citrix empfiehlt dringend, dass die Connector Appliance keine eingehenden Ports hat, auf die über das Internet zugegriffen werden kann.

Platzieren Sie die Connector Appliance hinter einem Webproxy, um seine ausgehende Internetkommunikation zu überwachen. Der Webproxy muss jedoch eine SSL/TLS-verschlüsselte Kommunikation unterstützen.

Die Connector Appliance kann andere ausgehende Ports mit Internetzugriff haben. Wenn andere Ports zur Verfügung stehen, kann die Connector Appliance darüber die Netzwerkbandbreite und Leistung optimieren.

Innerhalb des internen Netzwerks muss die Connector Appliance eine Vielzahl eingehender und ausgehender Ports geöffnet haben. Die folgende Tabelle enthält die erforderliche Grundkonfiguration geöffneter Ports.

Verbindungsrichtung	Port des Connectorgeräts	Externer Port	Service
Eingehend	443/TCP	Beliebig	Lokale Weboberfläche
Ausgehend	49152-65535/UDP	123/UDP	NTP
Ausgehend	53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
Ausgehend	67/UDP	68/UDP	DHCP und Broadcast
Ausgehend	49152 -65535/UDP	123/UDP	W32Time

Verbindungsrichtung	Port des Connectorgeräts	Externer Port	Service
Ausgehend	49152 -65535/TCP	464/TCP/UDP	Kerberos-Kennwortänderung
Ausgehend	49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
Ausgehend	49152 -65535/TCP	3268/TCP	LDAP GC
Ausgehend	49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
Ausgehend	49152 -65535/TCP/UDP	445/TCP	SMB
Ausgehend	137/UDP	137/UDP	NetBIOS-Namensdienst
Ausgehend	138/UDP	138/UDP	NetBIOS-Datagramm
Ausgehend	139/TCP	139/TCP	NetBIOS-Sitzung

Jeder in Citrix Cloud verwendete Service erweitert die Liste der erforderlichen geöffneten Ports. Weitere Informationen finden Sie in folgenden Ressourcen:

- Technischer Überblick über die Sicherheit für jeden Service (siehe Liste am Anfang dieses Artikels)
- Anforderungen an System und Konnektivität für Citrix Cloud Services

Überwachung der ausgehenden Kommunikation

Die Connector Appliance verwendet Port 443 für die ausgehende Internetkommunikation mit Citrix Cloud-Servern.

Jeder Service in Citrix Cloud erweitert die Liste der Server und internen Ressourcen, die die Connector Appliance im Rahmen des Normalbetriebs kontaktieren kann. Kunden können zudem nicht steuern, welche Daten vom Connectorgerät an Citrix gesendet werden. Weitere Informationen über interne Ressourcen und Daten, die von Services an Citrix gesendet werden, finden Sie in den folgenden Ressourcen:

- Technischer Überblick über die Sicherheit für jeden Service (siehe Liste am Anfang dieses Artikels)
- Anforderungen an System und Konnektivität für Citrix Cloud Services

Anzeigen von Connectorgerät-Protokollen

Sie können einen Diagnosebericht für Ihr Connectorgerät herunterladen, der verschiedene Protokolldateien enthält. Weitere Informationen zum Abrufen dieses Berichts finden Sie unter Connectorgerät für Cloudservices.

SSL/TLS-Konfiguration

die Connector Appliance benötigt keine spezielle SSL/TLS-Konfiguration.

Die Connector Appliance muss der Zertifizierungsstelle (ZS) vertrauen, die von SSL/TLS-Zertifikaten von Citrix Cloud verwendet wird. Citrix kann Zertifikate und Zertifizierungsstellen in Zukunft ändern. Verwenden Sie jedoch stets Zertifizierungsstellen, denen die Connector Appliance vertraut.

Jeder Service in Citrix Cloud kann unterschiedliche Anforderungen an die SSL-Konfiguration stellen. Weitere Informationen finden Sie im Technischen Überblick über die Sicherheit für jeden Service (siehe Liste am Anfang dieses Artikels).

Sicherheitskonformität

Um die Sicherheitskonformität zu gewährleisten, wird die Connector Appliance selbstverwaltet, und Sie können sich nicht über die Konsole anmelden.

Es ist nicht Ihre Aufgabe, auf Sicherheitsrisiken des Connectors zu reagieren. Die Connector Appliance wendet automatisch alle Sicherheitsfixes an.

Stellen Sie sicher, dass aktuelle Sicherheitsupdates auf den Hypervisoren installiert sind, die Ihr Connectorgerät hosten.

Wir empfehlen, im Active Directory (AD) das Maschinenkonto des Connectorgeräts auf schreibgeschützten Zugriff zu beschränken. Dies ist die Standardkonfiguration in Active Directory. Kunden können auch die AD-Protokollierung und -Überwachung im Maschinenkonto des Connectorgeräts aktivieren, um den Zugriff auf Active Directory zu überwachen.

Hinweise zum Umgang mit gefährdeten Konten

- Überwachen Sie die Liste der Administratoren in Citrix Cloud und entfernen Sie Administratoren, die nicht vertrauenswürdig sind.
- Deaktivieren Sie alle gefährdeten Konten im Active Directory des Unternehmens.
- Fordern Sie Citrix auf, die geheimen Autorisierungsinformationen zu wechseln, die für alle Cloud Connectors des Kunden gespeichert sind. Ergreifen Sie je nach Schweregrad des Verstoßes die folgenden Maßnahmen:

- **Niedriges Risiko:** Citrix kann die Geheimnisse im Laufe der Zeit wechseln. Die Cloud Connectors funktionieren weiterhin normal. Die alten Autorisierungsgeheimnisse werden innerhalb von 2-4 Wochen ungültig. Überwachen Sie in dieser Zeit den Cloud Connector, um sicherzustellen, dass es nicht zu unerwarteten Vorgängen kommt.
- **Dauerhaft hohes Risiko:** Citrix kann alle alten Geheimnisse widerrufen. Vorhandene Cloud Connectors werden funktionsunfähig. Zur Wiederaufnahme des Normalbetriebs müssen Kunden den Cloud Connector auf allen betroffenen Maschinen deinstallieren und neu installieren.

Citrix Cloud-Konto erstellen

December 11, 2023

In diesem Artikel werden Sie durch das Erstellen eines Citrix Cloud-Kontos und die erforderlichen Schritte zum erfolgreichen Onboarding Ihres Kontos geführt.

Kunden mit bestehender Geschäftsbeziehung zu Citrix, die Citrix Cloud Services zum ersten Mal verwenden, können das Onboarding anhand der Aufgaben in diesem Artikel abschließen.

Anmeldevorgang für neue Citrix-Kunden

Wenn Sie neu bei Citrix und Citrix Cloud sind, müssen Sie sich an Citrix wenden, um ein neues Citrix-Konto für Ihr Unternehmen zu erstellen. Verwenden Sie eine der folgenden Kontaktmethoden:

- Wenden Sie sich an den Citrix Customer Service.
- Wenden Sie sich an einen Citrix Partner oder ein Citrix-Vertriebsbüro in Ihrer Nähe.

Wenn Sie sich an Citrix wenden, können Sie Ihr Geschäftsanliegen mit einem Mitarbeiter von Citrix besprechen. Der Mitarbeiter hilft Ihnen beim Abschluss des Anmeldevorgangs und stellt Ihnen Ihre Citrix-Anmeldeinformationen bereit.

Nachdem Sie Ihre Anmeldeinformationen für das Citrix-Konto erhalten haben, können Sie sich mit den in diesem Artikel aufgeführten Aufgaben bei Citrix Cloud anmelden.

Was ist ein Citrix-Konto?

Mit einem Citrix-Konto (auch Citrix.com-Konto oder My Citrix-Konto) können Sie den Zugriff auf die erworbenen Lizenzen verwalten. Ihr Citrix-Konto verwendet eine Organisations-ID (OrgID) als eindeutigen Bezeichner. Sie können auf Ihr Citrix Konto zugreifen, indem Sie sich unter https://www.citrix.com mit einem Benutzernamen (auch "Webbenutzername") oder Ihrer E-Mail-Adresse anmelden, sofern eine E-Mail-Adresse mit Ihrem Konto verbunden ist.

> **Wichtig:**
>
> Ein Benutzername ist einem einzigen eindeutigen Citrix-Konto zugeordnet, eine E-Mail-Adresse kann jedoch mehreren Citrix-Konten zugeordnet sein.

Was ist eine OrgID?

Eine OrgID (Organisations-ID) ist der eindeutige Bezeichner, der Ihrem Citrix-Konto zugewiesen ist. Ihre OrgID ist einer physischen Siteadresse zugeordnet. Dies ist normalerweise die Firmenadresse Ihres Unternehmens. Unternehmen haben in der Regel eine einzige OrgID. In einigen Fällen, z. B. bei unterschiedlichen Niederlassungen oder wenn verschiedene Abteilungen ihre Ressourcen getrennt verwalten, kann Citrix einem Unternehmen mehrere OrgIDs gewähren.

Citrix räumt OrgIDs routinemäßig auf, wobei in einigen Fällen Duplikate zusammengeführt werden. Wenn Ihr Unternehmen über OrgIDs verfügt, die Sie mit einer gültigen und aktiven OrgID zusammenführen möchten, können Sie sich mit den entsprechenden OrgIDs an den Citrix Customer Support wenden.

> **Hinweis:**
>
> Unternehmen haben OrgIDs basierend darauf eingerichtet, wie sie ihre Assets verwalten möchten. Wenn Sie also nicht wissen, welche OrgID Sie verwenden müssen oder wie viele OrgIDs Sie haben, wenden Sie sich an die IT-Abteilung oder den Citrix Administrator in Ihrem Unternehmen. Wenn Sie Hilfe beim Auffinden Ihrer OrgID benötigen, erreichen Sie den Citrix Customer Service unter https://www.citrix.com/support/.

Was ist ein Citrix Cloud-Konto?

Mit einem Citrix Cloud-Konto können Sie beliebige Citrix Cloud-Services verwenden, um Ihre Apps und Daten sicher bereitzustellen. Ein Citrix Cloud-Konto wird durch eine Kunden-ID identifiziert und mit einer OrgID verknüpft. Eine OrgID kann mehreren Citrix Cloud-Kunden-IDs zugeordnet werden, eine Kunden-ID kann jedoch nur einer OrgID zugeordnet sein.

Es ist wichtig, das richtige Citrix Cloud-Konto entsprechend den von Ihrer Organisation eingerichteten OrgIDs zu verwenden, damit Ihre Käufe und der Administratorzugriff mit denselben OrgIDs fortgesetzt werden können. Wenn beispielsweise die Designabteilung eines Unternehmens mit OrgID 1234 Virtual Apps and Desktops on-premises verwendet und Citrix Cloud ausprobieren möchte, kann ein Administrator von OrgID 1234 sich mit dieser OrgID bei Citrix Cloud registrieren und dabei die Anmeldeinformationen für das Citrix-Konto oder eine E-Mail-Adresse verwenden, die mit der OrgID verknüpft ist. Wenn das Unternehmen beschließt, ein Citrix DaaS-Abonnement zu erwerben, kann die Bestellung korrekt unter OrgID 1234 aufgegeben werden.

> **Wichtig:**
>
> Benutzer mit Zugriff auf ein bestimmtes Citrix-Konto haben nicht automatisch Zugriff auf das Citrix Cloud-Konto, das mit der OrgID dieses Citrix-Kontos verknüpft ist. Da der Citrix Cloud-Zugriff es Benutzern potenziell ermöglicht, den Service zu beeinträchtigen, ist es wichtig, den Zugriff auf das Citrix Cloud-Konto zu kontrollieren.

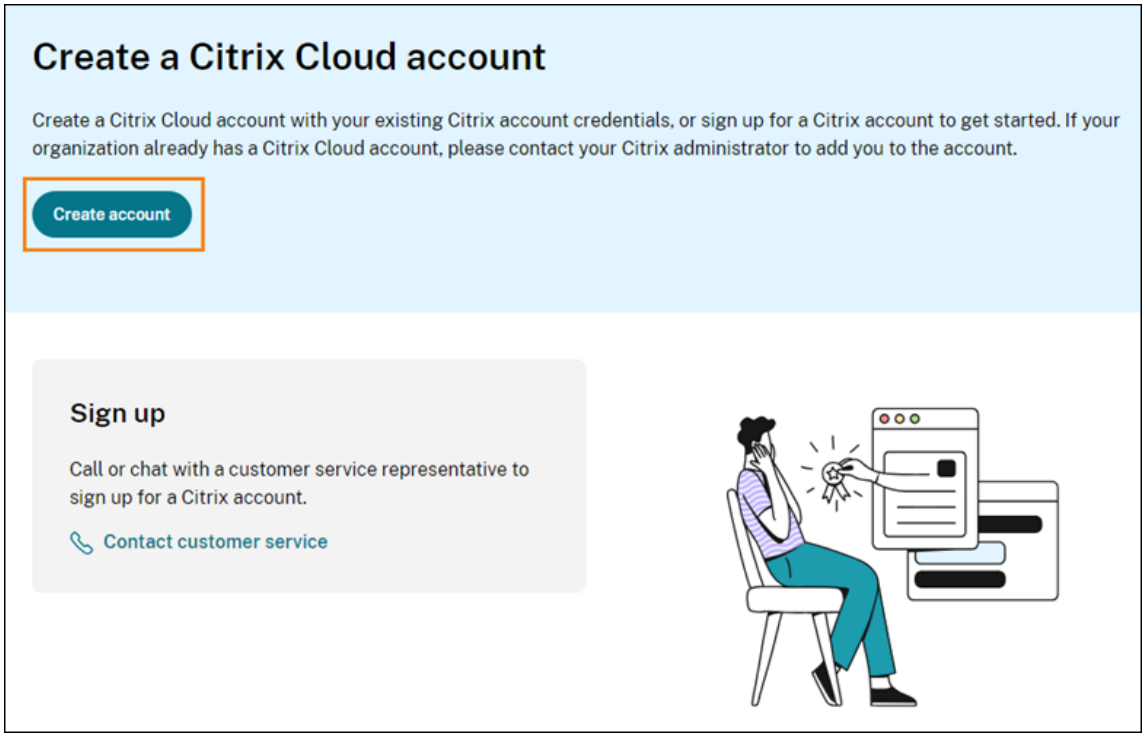
Multifaktorauthentifizierung

Um die Sicherheit Ihres Citrix Cloud-Kontos zu gewährleisten, müssen alle Kunden sich für die Multifaktorauthentifizierung registrieren. Für die Registrierung benötigen Sie nur ein Gerät (z. B. einen Computer oder ein Mobilgerät) mit installierter Authentifikator-App, z. B. Citrix SSO. Wenn die Verwendung eines Geräts mit Authentifikator-App nicht möglich ist, können Sie stattdessen eine E-Mail-Adresse verwenden.

Wenn Sie noch nicht für die Multifaktorregistrierung registriert sind, werden Sie von Citrix zur Registrierung aufgefordert, wenn Sie sich mit den Anmeldeinformationen Ihres Citrix-Kontos anmelden. Anforderungen und Anweisungen finden Sie in diesem Artikel unter Schritt 2: Multifaktorauthentifizierung einrichten.

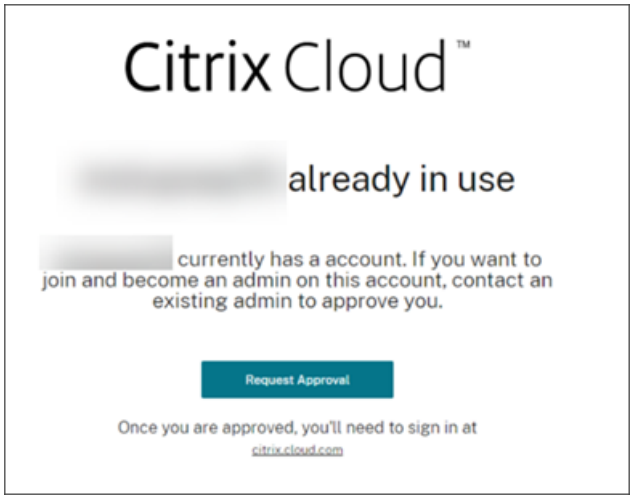
Schritt 1: Citrix Cloud-Website besuchen

1. Rufen Sie in einem Webbrowser https://onboarding.cloud.com auf.
2. Wählen Sie **Konto erstellen**.



3. Geben Sie Ihren Benutzernamen und Ihr Kennwort oder die E-Mail-Adresse und das Kennwort Ihres Citrix.com-Kontos ein.

Was passiert, wenn das Konto bereits verwendet wird?



Wenn in einer Meldung angezeigt wird, dass bereits ein Citrix Cloud-Konto für Ihre Organisation existiert, wurde dieses Citrix Cloud-Konto von einem anderen Administrator Ihres Citrix-Kontos erstellt. Damit Sie auf das Konto zugreifen können, muss ein vorhandener Administrator Sie einladen, Administrator zu werden, auch wenn Sie bereits Mitglied im Citrix-Konto sind.

Da ein Citrix Cloud-Konto den Administratoren größere Kontrolle über den Service ermöglicht, muss

der erste Administrator, der das Citrix Cloud-Konto erstellt, anderen Administratoren explizit Zugriff gewähren, auch wenn diese bereits Mitglieder des Citrix-Kontos sind.

Um eine Einladung zum Beitritt zu einem Citrix Cloud-Konto anzufordern, wählen Sie **Anforderungsgenehmigung**. Alle bestehenden Administratoren des Kontos werden dann per E-Mail über Ihre Anforderung informiert. Wenn die bestehenden Administratoren nicht mehr in Ihrer Organisation sind, wenden Sie sich an den Citrix Support.

Wenn ein Administrator Ihre Genehmigungsanforderung erhält, lädt er Sie ein, Administrator zu werden, wie unter Einzelne Administratoren einladenbeschrieben.

Beim Empfang der Einladungs-E-Mail klicken Sie auf den Link **Anmelden**, um die Einladung anzunehmen. Wenn Ihr Browser geöffnet wird, werden Sie von Citrix Cloud aufgefordert, ein Kennwort zu erstellen und sich beim Citrix Cloud-Konto anzumelden.

Schritt 2: Multifaktorauthentifizierung einrichten

Wenn Sie nicht für die Multifaktorauthentifizierung registriert sind, werden Sie vor der Anmeldung bei Citrix Cloud dazu aufgefordert. Sie können sich für die Multifaktorauthentifizierung mit einer Authentifikator-App (empfohlen) oder mit Ihrer E-Mail-Adresse registrieren.

> **Hinweise:**
>
> - Nur Administratoren unter dem Citrix-Identitätsanbieter können die Multifaktorauthentifizierung über Citrix Cloud einrichten. Wenn Sie Azure AD zum Verwalten von Citrix Cloud-Administratoren verwenden, können Sie die Multifaktorauthentifizierung über das Azure-Portal konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von Azure AD Multi-Factor Authentication-Einstellungen auf der Microsoft-Website.
> - Nach abgeschlossener Einrichtung wird die Multifaktorauthentifizierung für alle Kundenorganisationen verwendet, denen Sie in Citrix Cloud angehören. Sie können die Multifaktorauthentifizierung nach der Einrichtung nicht mehr deaktivieren.
> - Sie können nur ein Gerät registrieren. Wenn Sie später ein anderes Gerät registrieren, löscht Citrix Cloud die Registrierung des aktuellen Geräts und ersetzt sie durch das neue Gerät. Weitere Informationen finden Sie unter Primäre MFA-Methode verwalten.

E-Mail als Authentifizierungsmethode

Wenn Sie für den Zugriff auf Citrix Cloud keine Authentifikator-App verwenden können, ist die Multifaktorauthentifizierung mithilfe von E-Mail eine praktische Alternative. Citrix empfiehlt jedoch dringend, dass Sie einen gesicherten Zugriff auf Ihre E-Mail-Adresse sicherstellen.

Anforderungen für die Multifaktorauthentifizierung

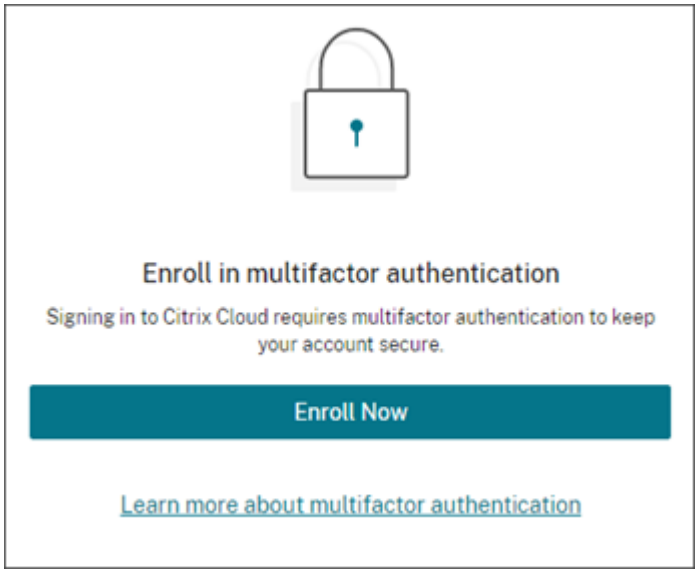
Um die Multifaktorauthentifizierung per Authentifikator-App einzurichten, müssen Sie auf Ihrem Gerät eine App mit dem Standard Zeitbasiertes Einmalkennwort installieren. Das Gerät kann zum Beispiel ein Smartphone oder ein Desktop-Computer sein. Je nach registriertem Gerät benötigt die App möglicherweise Zugriff auf die Gerätekamera, um einen QR-Code zu scannen. Wenn das Gerät keine Kamera hat, können Sie einen von Citrix Cloud bereitgestellten Schlüssel eingeben.

Um die Multifaktorauthentifizierung per E-Mail-Adresse einzurichten, müssen Sie eine E-Mail-Adresse verwenden, die die folgenden Anforderungen erfüllt:

- Die E-Mail-Adresse unterscheidet sich von der E-Mail-Adresse, die Sie für Ihr Citrix-Konto verwenden.
- Sie haben Zugriff auf die E-Mail-Adresse, um Verifizierungs-E-Mails von Citrix zu empfangen.

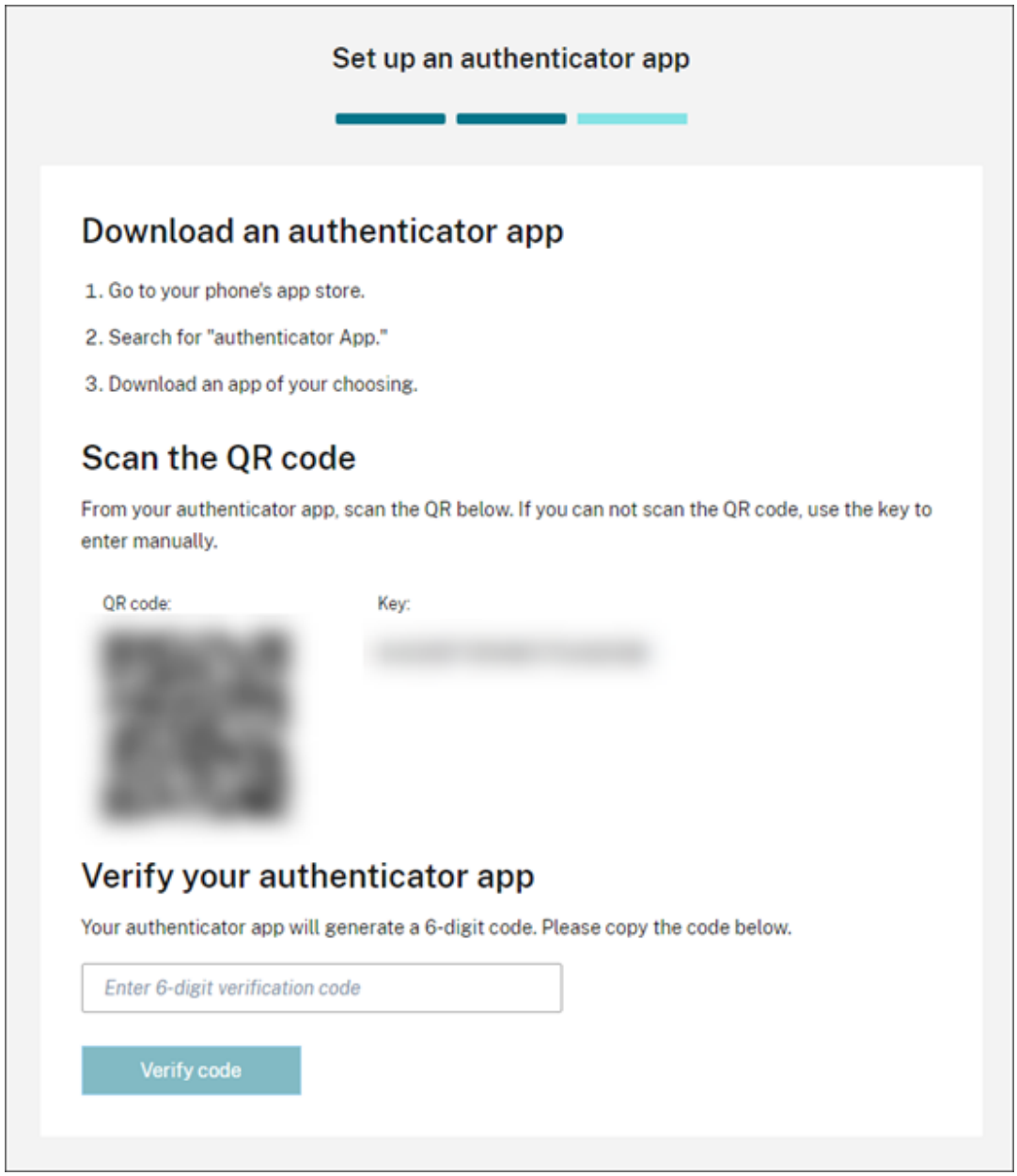
Registrierung für die Multifaktorauthentifizierung

1. Wenn Sie zur Registrierung für die Multifaktorauthentifizierung aufgefordert werden, wählen Sie **Jetzt registrieren**.



2. Wenn Sie dazu aufgefordert werden, geben Sie Ihre E-Mail-Adresse ein und wählen Sie **E-Mail senden**. Citrix Cloud sendet Ihnen eine E-Mail mit einem Verifizierungscode.
3. Geben Sie den Verifizierungscode aus der E-Mail und das Kennwort Ihres Citrix-Kontos ein. Klicken Sie auf **Verifizieren und fortfahren**.
4. Wählen Sie die Authentifizierungsmethode, die Sie verwenden möchten (Authentifikator-App oder E-Mail).
5. Wenn Sie die **Authentifikator-App** ausgewählt haben, führen Sie die folgenden Aktionen aus:

a) Scannen Sie in der Authentifikator-App den QR-Code, oder geben Sie den Schlüssel manuell ein. Die Authentifikator-App zeigt einen Eintrag für Citrix Cloud an und generiert einen sechsstelligen Code.



b) Geben Sie unter **Authentifikator-App verifizieren** den Code aus Ihrer Authentifikator-App ein, und wählen Sie **Code verifizieren** aus.

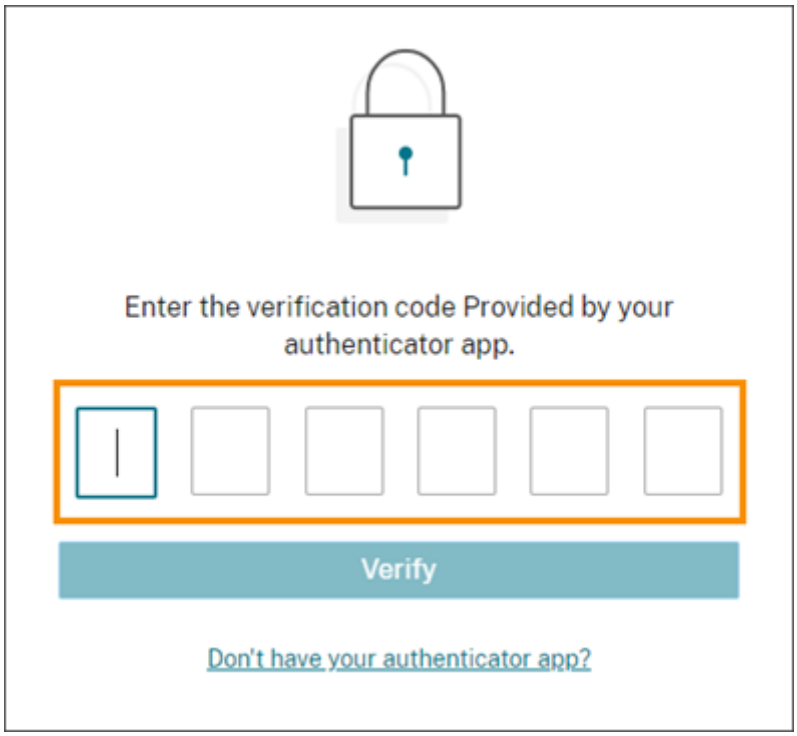
6. Klicken Sie auf **Nächster Schritt: Wiederherstellungsmethoden**.
7. Wählen Sie **Wiederherstellungstelefon hinzufügen** und geben Sie eine Telefonnummer zur Wiederherstellung ein, über die der Citrix Support Sie zur Identitätsprüfung anrufen kann. Citrix empfiehlt die Verwendung einer Festnetznummer. Klicken Sie zum Schluss auf **Telefonnum-**

mer für die Wiederherstellung speichern.

8. Wählen Sie **Weiter**.
9. Wählen Sie **Wiederherstellungs-E-Mail-Adresse hinzufügen** und geben Sie eine E-Mail-Adresse ein, auf die Sie Zugriff haben. Dies darf nicht die E-Mail-Adresse sein, die Sie mit Citrix Cloud verwenden. Citrix sendet an diese E-Mail-Adresse einen Verifizierungscode zur Überprüfung Ihrer Identität.

   Wenn Sie keine andere E-Mail-Adresse haben, wählen Sie **Haben Sie keine Wiederherstellungs-E-Mail-Adresse?**, um stattdessen eine Liste mit Backupcodes zu generieren. Backupcodes werden nicht empfohlen, da sie leicht verloren gehen können. Wenn Sie diese Option wählen, laden Sie die Codes herunter und bewahren Sie sie an einem Ort auf, auf den Sie bei Bedarf zugreifen können.
10. Wählen Sie **Fertig stellen** aus, um die Registrierung abzuschließen.

Bei Ihrer nächsten Anmeldung als Citrix Cloud-Administrator werden Sie von Citrix Cloud zur Eingabe des Verifizierungscodes aus Ihrer gewählten Multifaktorauthentifizierungsmethode aufgefordert.



Registrierung für Multifaktorauthentifizierung verwalten

In den folgenden Artikeln erfahren Sie, wie Sie Ihr Gerät ändern, die Multifaktorauthentifizierungsmethode wechseln oder Ihre Wiederherstellungsmethoden aktualisieren:

- Primäre MFA-Methode verwalten

- MFA-Wiederherstellungsmethoden verwalten

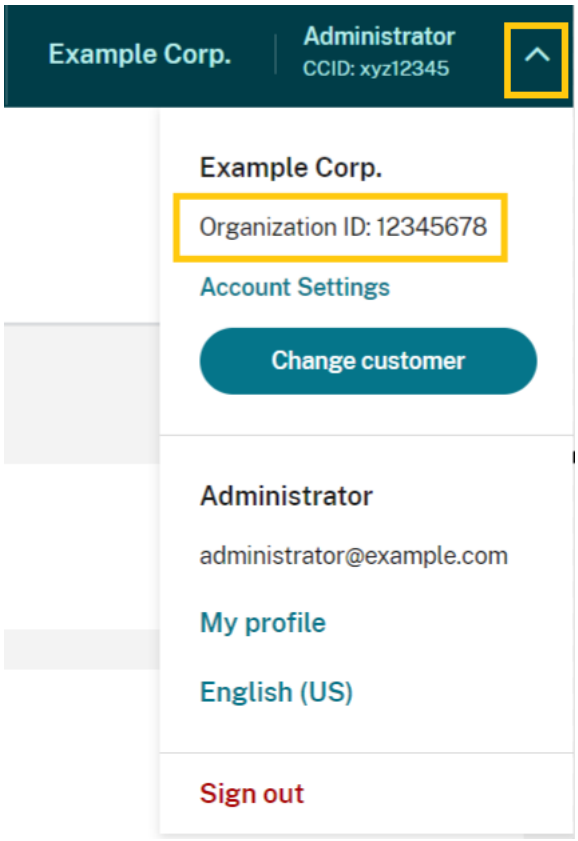
Schritt 3: OrgID verifizieren

Bevor Sie Citrix Cloud verwenden, sollten Sie sich einen Moment Zeit nehmen, um Ihre OrgID zu überprüfen.

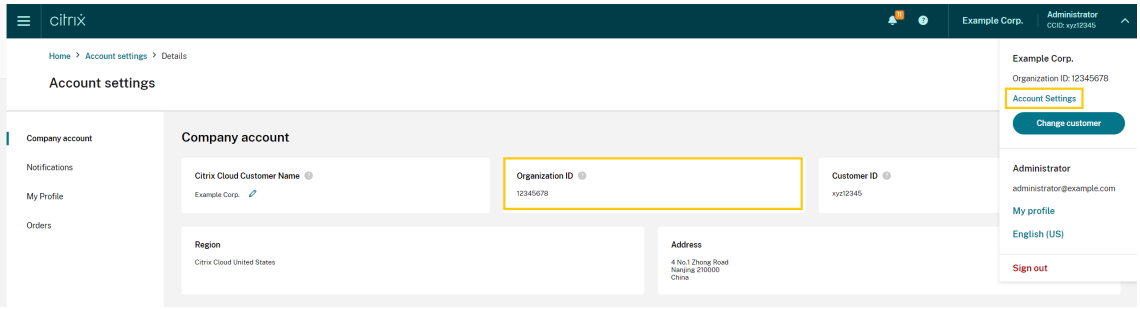
Stellen Sie sicher, dass die OrgID des Kontos mit der OrgID übereinstimmt, mit der Sie Bestellungen aufgeben. Einer der Vorteile von Citrix Cloud besteht darin, dass Sie einen Service ausprobieren können und alle von Ihnen in der Testversion vorgenommenen Konfigurationen beim Kauf erhalten bleiben, da das gleiche Konto verwendet wird. Wenn Sie also die Testversion mit der richtigen OrgID starten, sparen Sie sich im Falle des Erwerbs viel Aufwand.

Ihre OrgID wird an folgenden Stellen in der Verwaltungskonsole angezeigt:

- Im Menü unter Ihrem Kundennamen. Klicken Sie oben rechts auf den Kundennamen, um das Menü aufzurufen.



- Auf der Seite **den Kontoeinstellungen**. Wählen Sie im Kundenmenü die Option **Kontoeinstellungen**.



Nächste Schritte

Nach dem Onboarding können Sie mit den folgenden Aufgaben fortfahren:

- Identitätsanbieter hinzufügen, um Administratoren oder Workspace-Benutzer zu authentifizieren.
- Administratoren zu Ihrem Citrix Cloud-Konto hinzufügen. Auch wenn die anderen Administratoren Zugriff auf das Citrix-Konto unter Citrix.com haben, müssen Sie sie dennoch zu Ihrem Citrix Cloud-Konto hinzufügen.
- Testversionen von Clouddiensten anfordern. Testversionen sind für einen Test Ihrer Infrastruktur oder einer öffentlichen Cloud mit Ihren Anwendungen und Microsoft Active Directory konzipiert.

Weitere Informationen

- Citrix Schulung: Fundamentals of Citrix Cloud
- Citrix Kanal auf YouTube: Citrix Cloud Master Class

E-Mail-Adresse für Citrix Cloud verifizieren

October 27, 2023

Von Zeit zu Zeit kann Citrix Sie auffordern, Ihr Citrix Cloud-Konto zu bestätigen. Dies kann folgende Gründe haben:

- Sie waren längere Zeit nicht an Citrix Cloud angemeldet.
- Sie haben Ihre E-Mail-Adresse geändert.
- Sie haben einen neuen Administrator zum Citrix Cloud-Konto hinzugefügt.
- Aufgrund von Sicherheitsupdates an Citrix Cloud müssen Sie Ihr Citrix Cloud-Konto erneut überprüfen.

Häufig gestellte Fragen

Wie oft werde ich zur Bestätigung aufgefordert?

Sie müssen Ihr Konto nur einmal bestätigen. Sie werden nicht bei jeder Anmeldung oder Änderung, die Sie an Ihrem Konto vornehmen, von Citrix Cloud zur Bestätigung aufgefordert. Wenn Sie Ihre Angaben häufig bestätigen müssen, wenden Sie sich an den technischen Support von Citrix.

Wurde etwas an meinem Konto geändert?

Nein. Die Aufforderung, Ihr Konto zu bestätigen, deutet nicht auf ein Problem mit dem Konto oder den Citrix Cloud Services hin. Sie ist lediglich Bestandteil der Sicherheitsstrategie von Citrix zum Schutz Ihrer Daten.

Ich habe keine Überprüfungs-E-Mail erhalten. Welche Schritte sind erforderlich?

Gehen Sie wie folgt vor:

1. Suchen Sie im Posteingang nach einer Überprüfungs-E-Mail von "Citrix". Die Überprüfungs-E-Mail läuft nach 24 Stunden ab. Melden Sie sich erneut bei Citrix Cloud an, um eine neue Überprüfungs-E-Mail auszulösen. Dabei handelt es sich um einen einmaligen Prozess für jede Webanmeldung.
2. Prüfen Sie die gegebenenfalls auch die übrigen Ordner. Die E-Mail kann durch einen Spamfilter oder eine E-Mail-Regel verschoben worden sein und sich im Spam-Ordner oder Papierkorb befinden. Überprüfen Sie vorhandene Firewalls.
3. Stellen Sie sicher, dass Sie das richtige E-Mail-Konto prüfen. Citrix sendet die Bestätigungsanfrage an die aktuell gespeicherte E-Mail-Adresse für Ihr Konto. In der Regel ist dies die E-Mail-Adresse, mit der Sie bei Citrix Cloud registriert sind oder mit der Sie eingeladen und zum Citrix Cloud-Konto hinzugefügt wurden.
4. Bestätigen Sie, dass die angegebene E-Mail-Adresse gültig ist, indem Sie sich bei Ihrem Citrix-Konto unter https://www.citrix.com/account anmelden. Wenn die E-Mail-Adresse ungültig ist, aktualisieren Sie sie und melden Sie sich erneut bei Citrix Cloud an, um eine neue Überprüfungs-E-Mail auszulösen. Weitere Informationen finden Sie unter CTX126336 oder CTX130452 im Citrix Support Knowledge Center.
5. Wenn Sie weiterhin keine Überprüfungs-E-Mail erhalten haben, wenden Sie sich an den Citrix Support, um einen Supportfall zu öffnen. Bei bildungsbezogenen Websites (siehe **Partner Services Delivery > eLearning > Citrix Training**) öffnen Sie einen Fall beim zuständigen Team (Education) zur weiteren Untersuchung. Um einen Fall zu öffnen, fordern Sie **General Support** auf der Seite Contact us an.

Wenn Sie Ihre E-Mail verifiziert haben, sich jedoch immer noch nicht bei Citrix Cloud anmelden können, konsultieren Sie den Artikel Troubleshooting login issues on Citrix websites.

Wenden Sie sich an den Citrix Support

Wenn ein Problem auftritt, das hier nicht behandelt wird, wenden Sie sich an den technischen Support von Citrix, um einen Supportfall zu erstellen.

Verbindung mit Citrix Cloud herstellen

April 5, 2024

Das Verbinden Ihrer Ressourcen mit Citrix Cloud umfasst das Bereitstellen von Connectors in Ihrer Umgebung und das Erstellen von *Ressourcenstandorten*.

Ressourcenstandorte enthalten die Ressourcen zum Bereitstellen von Cloud Services für Ihre Abonnenten. Sie verwalten diese Ressourcen über die Citrix Cloud-Konsole. Ressourcenstandorte enthalten unterschiedliche Ressourcen, je nachdem, welche Citrix Cloud-Services Sie verwenden und welche Services Sie Abonnenten bereitstellen möchten.

Zum Erstellen eines Ressourcenstandorts installieren Sie mindestens zwei Connectors in Ihrer Domäne. Abhängig von den Cloudservices, die Sie verwenden, sind entweder Cloud Connectors oder Connectorgeräte erforderlich, um die Kommunikation zwischen Citrix Cloud und Ihren Ressourcen zu ermöglichen. Weitere Informationen zum Bereitstellen von Connectors finden Sie in den folgenden Artikeln:

- Technische Daten zu Cloud Connector
- Connector Appliance für Cloudservices

Ressourcentypen

Ressourcenstandorte enthalten unterschiedliche Ressourcen, je nachdem, welche Citrix Cloud-Services Sie verwenden und welche Services Sie Abonnenten bereitstellen möchten. Nicht alle Ressourcen verwenden denselben Connectortyp. Die meisten Services nutzen den Citrix Cloud Connector, einige bestimmte Dienste benötigen jedoch ein Connectorgerät.

Services, die Citrix Cloud Connector verwenden

- **Citrix DaaS** (früher Citrix Virtual Apps and Desktops Service) benötigt den Cloud Connector für die Veröffentlichung von Apps und Desktops und die Bereitstellung von Maschinenkatalogen an

Ihren Ressourcenstandorten. Eine Übersicht über die Kommunikation zwischen Cloud Connector und diesem Dienst finden Sie im Diagramm für Citrix DaaS in der Citrix Tech Zone.

- **Citrix DaaS Standard für Azure** (früher Citrix Virtual Apps and Desktops Standard für Azure) benötigt den Cloud Connector für die Bereitstellung von Azure Virtual Desktops, die von Citrix gehostet werden, und Apps von Multisitzungsmaschinen.
- **Endpoint Management** benötigt den Cloud Connector zur Verwaltung von App- und Geräterichtlinien und zur Bereitstellung von Apps für Benutzer.

Services, die das Connectorgerät verwenden

- Mit dem **Image Portability Service** können Sie Images einfacher plattformübergreifend verwalten. Das Feature erleichtert das Verwalten von Images zwischen einem On-Premises-Ressourcenstandort und einem Standort in einer öffentlichen Cloud. REST-APIs für Citrix Virtual Apps and Desktops ermöglichen die automatisierte Verwaltung von Ressourcen innerhalb einer Citrix Virtual Apps and Desktops-Site.

  Der Image Portability-Workflow setzt ein, wenn Sie mit Citrix Cloud die Migration eines Images vom On-Premises-Standort zur abonnierten öffentlichen Cloud initiieren. Nachdem Sie das Image vorbereitet haben, können Sie es mit Image Portability Service in die abonnierte öffentliche Cloud übertragen und zum Ausführen vorbereiten. Zum Schluss stellen Sie das Image mit Citrix Provisioning oder den Maschinenerstellungsdiensten in Ihrer abonnierten öffentlichen Cloud bereit.

  Weitere Informationen finden Sie unter Image Portability Service.

- Mit **Citrix Secure Private Access** können Administratoren eine einheitliche Benutzeroberfläche bereitstellen, die Single Sign-On, Remotezugriff und Inhaltsinspektion in einer Lösung integriert und eine umfassende Zugriffssteuerung gewährleistet. Weitere Informationen finden Sie unter Secure Private Access mit Connector Appliance.

Möglicherweise gibt es als Preview weitere Services, die auch von der Connector Appliance abhängen.

Ressourcenstandort

Ein Ressourcenstandort ist dort, wo sich die Ressourcen befinden, unabhängig davon, ob es sich um eine öffentliche oder private Cloud, eine Niederlassung oder ein Datencenter handelt. Wenn Sie bereits Ressourcen in einer eigenen Cloud oder einem Datencenter haben, verbleiben die Ressourcen dort. Sie müssen zur Verwendung mit Citrix Cloud nicht verschoben werden.

Folgende Faktoren können die Standortwahl beeinflussen:

- die Nähe zu Abonnenten

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

Beispiel einer Ressourcenstandortbereitstellung

- Erstellen Sie einen ersten Ressourcenstandort im Datencenter für den Firmenhauptsitz, basierend auf Abonnenten und Anwendungen, die in Datennähe sein müssen.
- Fügen Sie einen zweiten 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.
- Fügen Sie einen weiteren Ressourcenstandort in einem anderen Netzwerk mit eingeschränkten Anwendungen hinzu. Dies schränkt die Sichtbarkeit für andere Ressourcen und Abonnenten ein, ohne die anderen Ressourcenstandorte anpassen zu müssen.

Limits für Ressourcenstandorte

Sie können maximal 50 Ressourcenstandorte in Ihrem Citrix Cloud-Konto haben.

Namenseinschränkungen

Namen, die Sie Ressourcenstandorten zuweisen, müssen den folgenden Einschränkungen entsprechen:

- Maximale Länge: 64 Zeichen
- Unzulässige Zeichen:
  - #, $, %, ^, &, ?, +
  - Klammern: [], { }
  - Senkrechte Striche (|)
  - Kleiner-als-Zeichen (<) und Größer-als-Zeichen (>)
  - Schrägstriche und umgekehrte Schrägstriche (/, \)
- Dürfen mit keinem anderen Ressourcenstandortnamen (Groß-/Kleinschreibung unerheblich) im Citrix Cloud-Konto übereinstimmen.

Primäre Ressourcenstandorte

Ein primärer Ressourcenstandort ist ein Ressourcenstandort, den Sie für bestimmte Kommunikationen zwischen Ihrer Domäne und Citrix Cloud als "bevorzugt"festlegen. Die Cloud Connectors in einem

primären Ressourcenstandort werden für Benutzeranmeldungen und das Provisioning verwendet. Der Ressourcenstandort, den Sie als "primär"auswählen, sollte Cloud Connectors mit der besten Leistung und Konnektivität zu Ihrer Domäne haben. So können sich Ihre Benutzer schnell an Citrix Cloud anmelden.

Weitere Informationen finden Sie unter [Primären Ressourcenstandort wählen].(/en-us/citrix-cloud/citrix-cloud-management/identity-access-management/primary-resource-locations.html)

Citrix Cloud Connector

April 5, 2024

Der Citrix Cloud Connector ist eine Citrix Komponente, die als Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten dient und die Cloudverwaltung ohne komplexe Netzwerk- oder Infrastrukturkonfiguration ermöglicht. Dadurch entfällt der Aufwand für die Verwaltung der Bereitstellungsinfrastruktur. Sie können sich dadurch auf die Ressourcen konzentrieren, die Ihren Benutzern einen Mehrwert bieten.

> **Hinweis:**
>
> Installieren Sie das Remote PowerShell SDK nicht auf einer Citrix Cloud Connector-Maschine. Es kann auf jeder in der Domäne eingebundenen Maschine am gleichen Ressourcenstandort installiert werden.
>
> Citrix rät davon ab, die Cmdlets dieses SDKs auf Cloud Connectors auszuführen. Am SDK-Betrieb sind die Cloud Connectors nicht beteiligt.

Services, die den Cloud Connector erfordern

Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) erfordert den Cloud Connector. Eine Übersicht über die Kommunikation zwischen Cloud Connector und Dienst finden Sie im Diagramm für Citrix DaaS in der Citrix Tech Zone.

Citrix Endpoint Management erfordert den Cloud Connector für die Unternehmensverbindung mit dem Endpoint Management Service. Der Remote Browser Isolation-Dienst erfordert den Cloud Connector für authentifizierte externe Web-Apps.

Funktionen des Cloud Connectors

- **Active Directory (AD):** ermöglicht die AD-Verwaltung und die Verwendung von Active Directory-Gesamtstrukturen und -Domänen an Ihren Ressourcenstandorten. Dadurch müssen

keine zusätzlichen AD-Vertrauensstellungen hinzugefügt werden.

- **Virtual Apps and Desktops-Veröffentlichung:** ermöglicht Citrix DaaS die Veröffentlichung von Ressourcen an Ihren Ressourcenstandorten.
- **Endpoint Management:** Ermöglicht die Verwaltung einer mobilen Gerätverwaltung (MDM) und mobilen Anwendungsverwaltung (MAM) für die Verwaltung von Geräte- und Anwendungsrichtlinien und die Bereitstellung von Apps für Benutzer.
- **Bereitstellung über Maschinen:** Ermöglicht die direkte Bereitstellung von Maschinen an Ihren Ressourcenstandorten.

> **Hinweis:**
>
> Wenn die Verbindung zur Citrix Cloud nicht verfügbar ist, ist ein Betrieb zwar möglich, jedoch ggf. mit eingeschränkter Funktionalität. Sie können die Integrität des Cloud Connectors von der Citrix Cloud-Konsole aus überwachen.

Kommunikation mit dem Cloud Connector

Der Cloud Connector authentifiziert und verschlüsselt die gesamte Kommunikation zwischen Citrix Cloud und Ihren Ressourcenstandorten. Nach der Installation initiiert der Cloud Connector die Kommunikation mit Citrix Cloud über eine ausgehende Verbindung. Alle Verbindungen werden vom Cloud Connector zur Cloud unter Verwendung des Standard-HTTPS-Ports (443) und des TCP-Protokolls hergestellt. Es werden keine eingehenden Verbindungen akzeptiert.

Verfügbarkeit des Cloud Connectors und Lastverwaltung

Installieren Sie mehrere Cloud Connectors an jedem Ihrer Ressourcenstandorte, damit die kontinuierliche Verfügbarkeit gesichert ist und die Last verwaltet werden kann. Es sind mindestens zwei Cloud Connectors an jedem Ressourcenstandort erforderlich, um eine hochverfügbare Verbindung mit Citrix Cloud sicherzustellen. Wenn ein Cloud Connector ausfällt, können die anderen die Verbindung erhalten. Da die Cloud Connectors zustandslos sind, kann die Last auf alle verfügbaren Cloud Connectors verteilt werden. Der Lastausgleich muss nicht konfiguriert werden. Es ist vollständig automatisiert.

Solange ein Cloud Connector verfügbar ist, wird die Kommunikation mit Citrix Cloud nicht unterbrochen. Die Verbindung des Endbenutzers mit den Ressourcen am Ressourcenstandort ist nach Möglichkeit nicht auf eine Verbindung mit Citrix Cloud angewiesen. Dadurch kann der Ressourcenstandort Benutzern unabhängig von der Verbindung mit Citrix Cloud Zugriff auf seine Ressourcen gewähren.

Herunterladen des Cloud Connectors

Sie können die Cloud Connector-Software aus Citrix Cloud herunterladen.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links die Option **Ressourcenstandorte** aus.
3. Wenn Sie keinen Ressourcenstandort haben, klicken Sie auf der Seite "Ressourcenstandorte" auf **Download**. Wenn Sie dazu aufgefordert werden, speichern Sie die Datei **cwcconnector.exe**.
4. Wenn Sie einen Ressourcenstandort haben, in dem jedoch keine Cloud Connectors installiert sind, klicken Sie auf die Cloud Connectors-Leiste und dann auf **Download**. Wenn Sie dazu aufgefordert werden, speichern Sie die Datei **cwcconnector.exe**.

Wie viele Cloud Connectors brauche ich?

Es sind mindestens zwei (2) Cloud Connectors erforderlich, um eine hochverfügbare Verbindung zwischen Citrix Cloud und Ihrem Ressourcenstandort herzustellen. Abhängig von Ihrer Umgebung und den Workloads, die Sie unterstützen, benötigen Sie möglicherweise mehr Cloud Connectors, um Ihren Benutzern die beste Benutzererfahrung zu bieten.

Als bewährte Methode empfiehlt Citrix die Verwendung des N+1-Redundanzmodells, um die Anzahl der bereitzustellenden Cloud Connectors zu bestimmen. Ermitteln Sie die Zahl der an einem Ressourcenstandort benötigten Cloud Connectors basierend auf Ihrer Umgebung, Workloads, Active Directory-Konfiguration und Diensten. Erhöhen Sie diese Zahl um mindestens einen weiteren Cloud Connector, um Resilienz zu gewährleisten. Wenn Sie beispielsweise fünf Cloud Connectors benötigen, fügen Sie einen weiteren hinzu und installieren Sie sechs Cloud Connectors an Ihrem Ressourcenstandort.

Weitere Richtlinien zu Skalierung und Größe finden Sie unter Überlegungen zu Skalierung und Größe für Cloud Connectors.

Installieren des Cloud Connectors

Informationen zu den unterstützten Betriebssystemen, Plattformen und Versionen finden Sie unter Systemanforderungen.

Installieren Sie den Cloud Connector auf einer dedizierten Maschine mit Windows Server 2016, Windows Server 2019 oder Windows Server 2022. Die Maschine muss zu Ihrer Domäne gehören und mit den Ressourcen kommunizieren können, die Sie über Citrix Cloud verwalten möchten.

> **Wichtig:**
>
> - Installieren Sie den Cloud Connector und andere Citrix-Komponenten nicht auf einem Active Directory-Domänencontroller.
> - Installieren Sie den Cloud Connector nicht auf Maschinen, die Teil anderer Citrix Bereitstel-

> lungen sind (z. B. Delivery Controller in einer On-Premises-Bereitstellung von Virtual Apps and Desktops).

Weitere Informationen zur Bereitstellung finden Sie in den folgenden Artikeln:

- Bereitstellungsszenarios für Cloud Connectors in Active Directory
- Cloud Connector-Installation

Technische Daten zu Citrix Cloud Connector

July 2, 2024

Der Citrix Cloud Connector ist eine Komponente, die eine Verbindung zwischen Citrix Cloud und Ihren Ressourcenstandorten bereitstellt. In diesem Artikel werden Bereitstellungsanforderungen und -Szenarien, die Unterstützung von Active Directory und FIPS sowie Optionen zur Problembehandlung beschrieben.

Systemanforderungen

Die Maschine, auf der der Cloud Connector gehostet wird, muss die folgenden Anforderungen erfüllen: Es sind mindestens zwei Cloud Connectors an jedem Ressourcenstandort erforderlich, um eine hohe Verfügbarkeit zu gewährleisten. Als bewährte Methode empfiehlt Citrix die Verwendung des N+1-Redundanzmodells bei der Bereitstellung von Cloud Connectors, um eine hochverfügbare Verbindung mit Citrix Cloud zu gewährleisteten.

Hardwareanforderungen

Die Mindestanforderung für jeden Cloud Connector ist:

- 2 vCPU
- 4 GB RAM
- 20 GB Speicherplatz

Mit mehr vCPU-Speicher kann ein Cloud Connector für größere Sites vertikal skaliert werden. Empfohlene Konfigurationen finden Sie unter Überlegungen zur Skalierung und Größe für Cloud Connectors.

Betriebssysteme

Folgende Betriebssysteme werden unterstützt:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Die Verwendung des Cloud Connectors mit Windows Server Core wird nicht unterstützt.

.NET-Anforderungen

Microsoft .NET Framework 4.7.2 oder höher ist erforderlich. Ein Download der aktuellen Version ist über die Microsoft-Website möglich.

> **Hinweis:**
>
> Verwenden Sie Microsoft .NET Core nicht mit dem Cloud Connector. Wenn Sie .NET Core anstelle von .NET Framework verwenden, schlägt die Installation des Cloud Connector möglicherweise fehl. Verwenden Sie nur .NET Framework mit dem Cloud Connector.

Serveranforderungen

Wenn Sie Cloud Connectors mit Citrix DaaS (zuvor "Citrix Virtual Apps and Desktops Service") verwenden, lesen Sie die Anweisungen zur Maschinenkonfiguration unter Überlegungen zur Skalierung und Größe für Cloud Connectors.

Die folgenden Anforderungen gelten für alle Maschinen, auf denen der Cloud Connector installiert ist:

- Verwenden Sie dedizierte Maschinen zum Hosten des Cloud Connectors. Installieren Sie keine anderen Komponenten auf diesen Maschinen.
- Die Maschinen sind **nicht** als Active Directory-Domänencontroller konfiguriert. Die Installation des Cloud Connectors auf einem Domänencontroller wird nicht unterstützt.
- Serveruhr auf die korrekte UTC-Zeit eingestellt
- Wenn Sie das grafische Installationsprogramm verwenden, müssen Sie einen Browser installiert und den Standardsystembrowser festgelegt haben.

Anleitung zu Windows Update

Citrix empfiehlt dringend, Windows Updates auf allen Maschinen zu aktivieren, auf denen ein Citrix Cloud Connector gehostet wird. Der Citrix Cloud Connector prüft regelmäßig alle fünf Minuten

auf ausstehende Neustarts, die durch verschiedene Faktoren, einschließlich Windows Updates, ausgelöst werden können. Jeder erkannte Neustart wird sofort ausgeführt, unabhängig vom bevorzugten Tagesablauf, der am Ressourcenstandort festgelegt wurde. Dieser proaktive Ansatz stellt sicher, dass der Citrix Cloud Connector nicht über einen längeren Zeitraum in einem Status mit ausstehenden Aktualisierungen verbleibt, wodurch die Systemstabilität gewährleistet wird.

Die Citrix Cloud-Plattform verwaltet Neustarts, um die Verfügbarkeit aufrechtzuerhalten, sodass jeweils nur ein Citrix Cloud Connector neu gestartet werden kann. Stellen Sie beim Einrichten von Windows Update sicher, dass Windows so eingerichtet ist, dass Updates automatisch außerhalb der Geschäftszeiten heruntergeladen und installiert werden. Die automatischen Neustarts sind jedoch mindestens vier Stunden lang nicht zulässig, damit der Citrix Cloud Connector ausreichend Zeit hat, den Neustartvorgang zu verwalten. Darüber hinaus können Sie mithilfe einer Gruppenrichtlinie oder eines Systemverwaltungstools einen Fallback-Neustartmechanismus für Situationen einrichten, in denen eine Maschine nach einem Update neu gestartet werden muss. Weitere Informationen finden Sie unter Verwalten von Geräteneustarts nach Updates.

> **Hinweis:**
>
> - Wenn der Kunde nicht beabsichtigt, seinen Citrix Cloud Connector während der Geschäftszeiten neu zu starten, empfehlen wir dem Kunden, Windows Updates außerhalb der Geschäftszeiten entsprechend zu planen.
> - Jeder Citrix Cloud Connector benötigt etwa 10 Minuten für den Neustart. Dazu gehört auch die Zeit, die für die Synchronisierung mit der Citrix Cloud Platform erforderlich ist, um sicherzustellen, dass zu einem bestimmten Zeitpunkt nur ein Citrix Cloud Connector neu gestartet wird. Daher kann die oben empfohlene Mindestverzögerung von vier Stunden für automatische Neustarts je nach Anzahl der Citrix Cloud Connectors im Mandanten entsprechend auf eine kürzere oder längere Dauer angepasst werden.

Anforderungen für die Zertifikatvalidierung

Cloud Connector-Binärdateien und Endpunkte, die der Cloud Connector kontaktiert, sind durch X.509-Zertifikate geschützt, die von weithin anerkannten Unternehmenszertifizierungsstellen (ZS) ausgestellt werden. Die Zertifikatsprüfung in der Public Key-Infrastruktur (PKI) umfasst die Zertifikatsperrliste (CRL). Wenn ein Client ein Zertifikat empfängt, überprüft der Client, ob er der ZS, die die Zertifikate ausgestellt hat, vertraut, und ob das Zertifikat auf einer Zertifikatsperrliste ist. Wenn das Zertifikat auf einer Zertifikatsperrliste ist, wird das Zertifikat gesperrt und ist nicht vertrauenswürdig, obwohl es gültig erscheint.

Die Zertifikatsperrlistenserver verwenden HTTP an Port 80 anstelle von HTTPS an Port 443. Cloud Connector-Komponenten selbst kommunizieren nicht über den externen Port 80. Die Notwendigkeit des externen Ports 80 ist ein Nebenprodukt des Prozesses der Zertifikatsprüfung, den das Betriebssystem ausführt.

Die X.509-Zertifikate werden während der Cloud Connector-Installation überprüft. Daher müssen alle Cloud Connector-Maschinen diesen Zertifikaten vertrauen, damit die Cloud Connector-Software erfolgreich installiert werden kann.

Citrix Cloud-Endpunkte werden durch Zertifikate geschützt, die von DigiCert oder von einer Azure-Stammzertifizierungsstelle ausgestellt wurden. Weitere Informationen zu den von Azure verwendeten Stammzertifizierungsstellen finden Sie unter https://docs.microsoft.com/en-us/azure/security/fundamentals/tls-certificate-changes.

Um die Zertifikate zu validieren, muss jede Cloud Connector-Maschine die folgenden Anforderungen erfüllen:

- HTTP-Port 80 ist für die folgenden Adressen offen. Dieser Port wird während der Cloud Connector-Installation und während der regelmäßigen Überprüfung der Zertifikatsperrlisten verwendet. Weitere Informationen zum Testen der Konnektivität für Zertikatsperrliste und OCSP finden Sie auf der DigiCert-Website unter https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm.
  - http://cacerts.digicert.com/
  - http://dl.cacerts.digicert.com/
  - http://crl3.digicert.com
  - http://crl4.digicert.com
  - http://ocsp.digicert.com
  - http://www.d-trust.net
  - http://root-c3-ca2-2009.ocsp.d-trust.net
  - http://crl.microsoft.com
  - http://oneocsp.microsoft.com
  - http://ocsp.msocsp.com
- Die Kommunikation mit den folgenden Adressen ist aktiviert:
  - https://*.digicert.com
- Die folgenden Stammzertifikate sind installiert:
  - https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootG2.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootCA.crt
  - https://cacerts.digicert.com/DigiCertTrustedRootG4.crt
  - https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt
  - https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt

  - https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt

- Die folgenden Zwischenzertifikate sind installiert:

  - https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA384.crt
  - https://cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt

Wenn ein Zertifikat fehlt, wird es vom Cloud Connector-Installationsprogramm von http://cacerts.digicert.com heruntergeladen.

Ausführliche Anweisungen zum Herunterladen und Installieren der Zertifikate finden Sie unter CTX223828.

Citrix DaaS Die Verwendung des Cloud Connector für die Konnektivität zu DaaS-Ressourcen erfordert die Installation zusätzlicher Zertifikate und die Gewährung des Zugriffs auf eine erweiterte PKI-Infrastruktur. Jede Cloud Connector-Maschine muss die folgenden Anforderungen erfüllen:

- HTTP-Port 80 ist für die folgenden Adressen offen:

  - crl.*.amazontrust.com
  - ocsp.*.amazontrust.com
  - *.ss2.us

- Die Kommunikation mit den folgenden Adressen ist aktiviert:

  - https://*.amazontrust.com
  - https://*.ss2.us

- Die folgenden Stammzertifikate sind installiert:

  - https://www.amazontrust.com/repository/AmazonRootCA1.cer
  - https://www.amazontrust.com/repository/AmazonRootCA2.cer
  - https://www.amazontrust.com/repository/AmazonRootCA3.cer
  - https://www.amazontrust.com/repository/AmazonRootCA4.cer
  - https://www.amazontrust.com/repository/SFSRootCAG2.cer

- Die folgenden Zwischenzertifikate sind installiert:

  - https://www.amazontrust.com/repository/G2-RootCA4.orig.cer
  - https://www.amazontrust.com/repository/R3-ServerCA3A.cer
  - https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.cer


```
- https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.v2.
  cer
- https://www.amazontrust.com/repository/G2-RootCA1.orig.cer
- https://www.amazontrust.com/repository/R1-ServerCA1A.cer
- https://www.amazontrust.com/repository/G2-RootCA3.cer
- https://www.amazontrust.com/repository/R3-ServerCA3A.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA2.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA4.cer
- https://www.amazontrust.com/repository/R2-ServerCA2A.cer
- https://www.amazontrust.com/repository/R4-ServerCA4A.cer
- https://www.amazontrust.com/repository/R1-ServerCA1A.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA1.cer
- https://www.amazontrust.com/repository/G2-RootCA2.cer
- https://www.amazontrust.com/repository/G2-RootCA3.orig.cer
- https://www.amazontrust.com/repository/R4-ServerCA4A.orig.cer
- https://www.amazontrust.com/repository/G2-ServerCA0A.cer
- https://www.amazontrust.com/repository/G2-ServerCA0A.orig.cer
- https://www.amazontrust.com/repository/SFSRootCA-SFSRootCAG2.
  cer
```

Wenn ein Zertifikat fehlt, lädt der Cloud Connector es von https://www.amazontrust.com herunter.

Ausführliche Anweisungen zum Herunterladen und Installieren der Zertifikate finden Sie unter CTX223828.

Active Directory-Anforderungen

- Teil einer Active Directory-Domäne, die die Ressourcen und Benutzer enthält, die Sie zum Erstellen von Angeboten für Ihre Benutzer verwenden. Informationen zu Umgebungen mit mehreren Domänen finden Sie im vorliegenden Artikel unter Bereitstellungsszenarios für Cloud Connectors in Active Directory.
- Jede Active Directory-Gesamtstruktur, die für Citrix Cloud verwendet werden soll, muss immer über zwei Cloud Connectors erreichbar sein.
- Der Cloud Connector muss Domänencontroller in der Stammdomäne der Gesamtstruktur und in den Domänen, die Sie mit Citrix Cloud verwenden möchten, erreichen können. Weitere Informationen hierzu finden Sie in den folgenden Microsoft-Supportartikeln:
  - Konfigurieren von Domänen und Vertrauensstellungen
  - Abschnitt “Ports für Systemdienste”in Dienstübersicht und Netzwerkportanforderungen für Windows

- Verwenden Sie universelle Sicherheitsgruppen anstelle von globalen Sicherheitsgruppen. Diese Konfiguration stellt sicher, dass die Benutzergruppenzugehörigkeit von jedem Domänencontroller in der Gesamtstruktur bezogen werden kann.

Netzwerkanforderungen

- Mit einem Netzwerk verbunden, über das Zugriff auf die Ressourcen besteht, die Sie am Ressourcenstandort verwenden. Weitere Informationen finden Sie unter Konfiguration von Cloud Connector-Proxy und Firewall.
- Eine Verbindung mit dem Internet muss bestehen. Weitere Informationen finden Sie in den folgenden Abschnitten unter Anforderungen an System und Konnektivität:
  - Verbindungsanforderungen für den Cloud Connector
  - Positivliste der FQDNs für den Cloud Connector

Unterstützte Funktionsebenen von Active Directory

Der Citrix Cloud Connector unterstützt die folgenden Funktionsebenen für Active Directory-Gesamtstrukturen und -Domänen:

Funktionsebene	Domänenfunktionsebene	Unterstützte Domänencontroller
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016

Funktionsebene	Domänenfunktionsebene	Unterstützte Domänencontroller
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019, Windows Server 2022.

Unterstützung von FIPS (Federal Information Processing Standard)

Der Cloud Connector unterstützt derzeit die FIPS-validierten kryptografischen Algorithmen, die auf FIPS-aktivierten Maschinen verwendet werden. Nur die neueste Version der Cloud Connector-Software, die in Citrix Cloud verfügbar ist, unterstützt dies. Wenn Sie Cloud Connector-Maschinen haben, die vor November 2018 installiert wurden, und den FIPS-Modus dort aktivieren möchten, gehen Sie folgendermaßen vor:

1. Deinstallieren Sie die Cloud Connector-Software von allen Maschinen an Ihrem Ressourcenstandort.
2. Aktivieren Sie den FIPS-Modus auf jeder Maschine.
3. Installieren Sie die neueste Cloud Connector-Version auf den FIPS-aktivierten Maschinen.

> **Wichtig:**
>
> - Führen Sie kein Upgrade der Cloud Connector-Installation auf die neueste Version durch. Deinstallieren Sie immer zuerst den alten Cloud Connector und installieren Sie dann die neue Version.
> - Aktivieren Sie den FIPS-Modus nicht auf Maschinen, auf denen eine ältere Cloud Connector-Version gehostet wird. Cloud Connector-Versionen vor 5.102 unterstützen den FIPS-Modus nicht. Wenn Sie den FIPS-Modus auf einer Maschine mit einem älteren Cloud Connector aktivieren, kann Citrix Cloud keine regelmäßigen Wartungsupdates für den Cloud Connector durchführen.

Anweisungen zum Herunterladen der neuesten Cloud Connector-Version finden Sie unter Herunterladen des Cloud Connectors.

Mit Cloud Connector installierte Dienste

In diesem Abschnitt werden die mit dem Cloud Connector installierten Dienste und ihre Systemberechtigungen beschrieben.

Während der Installation des Citrix Cloud Connectors installiert die ausführbare Datei die erforderliche Dienstkonfiguration mit den notwendigen Standardeinstellungen. Wird diese Standardkonfiguration manuell geändert, kann dies die Funktion des Cloud Connectors beeinträchtigen. In diesem Fall wird die Konfiguration beim nächsten Cloud Connector-Update auf den Standardzustand zurückgesetzt, sofern die Dienste, die den Aktualisierungsprozess steuern, weiterhin funktionieren.

Das Citrix Cloud Agent System ermöglicht alle höheren Aufrufe, die für die Funktion der anderen Cloud Connector-Dienste erforderlich sind, und kommuniziert nicht direkt im Netzwerk. Wenn ein Dienst im Cloud Connector eine Aktion ausführen muss, für die lokale Systemberechtigungen erforderlich sind, nutzt er einen vordefinierten Satz von Vorgängen, die das Citrix Cloud Agent System ausführen kann.

Dienstname	Beschreibung	Ausgeführt als
Citrix Cloud Agent System	Verarbeitet die für On-premises-Agents erforderlichen Systemaufrufe. Umfasst Installation, Neustarts und Zugriff auf die Registrierung. Kann nur von Citrix Cloud Services Agent WatchDog aufgerufen werden.	Lokales System
Citrix Cloud Services Agent WatchDog	Überwacht und aktualisiert die On-Premises-Agenten (Evergreen).	Netzwerkdienst
Citrix Cloud Services Agent Logger	Bietet ein Support-Protokollierungsframework für die Citrix Cloud Connector-Dienste.	Netzwerkdienst
Citrix Cloud Services AD Provider	Ermöglicht die Verwaltung von Ressourcen, die mit den Active Directory-Domänenkonten verbunden sind, in denen Citrix Cloud installiert ist.	Netzwerkdienst
Citrix Cloud Services Agent Discovery	Ermöglicht die Verwaltung älterer On-Premises-Produkte von Citrix XenApp und XenDesktop in Citrix Cloud.	Netzwerkdienst
Citrix Cloud Services Credential Provider	Ermöglicht das Speichern und Abrufen verschlüsselter Daten.	Netzwerkdienst

Dienstname	Beschreibung	Ausgeführt als
Citrix Cloud Services WebRelay Provider	Ermöglicht die Weiterleitung von HTTP-Anfragen vom WebRelay Cloud-Dienst an On-Premises-Webserver.	Netzwerkdienst
Citrix CDF Capture Service	Erfasst CDF-Traces von allen konfigurierten Produkten und Komponenten.	Netzwerkdienst
Citrix Config Synchronizer Service	Kopiert die Brokerkonfiguration lokal für den Hochverfügbarkeitsmodus.	Netzwerkdienst
Citrix Connection Lease Exchange Service	Ermöglicht den Austausch von Verbindungsleasingdateien zwischen Workspace-App und Cloud Connector zur Gewährleistung der Workspace-Servicekontinuität	Netzwerkdienst
Citrix Dienst für hohe Verfügbarkeit	Gewährleistet die Servicekontinuität bei einem Ausfall der zentralen Site.	Netzwerkdienst
Citrix ITSM Adapter Provider	Automatisiert das Provisioning und die Verwaltung virtueller Apps und Desktops.	Netzwerkdienst
Citrix NetScaler CloudGateway	Bietet Internetkonnektivität zu on-premises vorhandenen Desktops und Anwendungen ohne Öffnen eingehender Firewallregeln oder Bereitstellen von Komponenten in der DMZ.	Netzwerkdienst
Citrix Remote Broker Provider	Ermöglicht die Kommunikation mit einem Remotebrokerdienst von lokalen VDAs und StoreFront-Servern aus.	Netzwerkdienst
Citrix Remote HCL Server	Agiert als Proxy für die Kommunikation zwischen Delivery Controller und Hypervisoren.	Netzwerkdienst

Dienstname	Beschreibung	Ausgeführt als
Citrix WEM Cloud Authentication Service	Stellt den Authentifizierungsdienst zur Verbindung von Citrix WEM-Agents mit Cloud-Infrastrukturservern bereit.	Netzwerkdienst
Citrix WEM Cloud Messaging Service	Ermöglicht dem Citrix WEM-Clouddienst den Empfang von Nachrichten von Cloud-Infrastrukturservern.	Netzwerkdienst

Bereitstellungsszenarios für Cloud Connectors in Active Directory

Sie können sowohl über Cloud Connector als auch Connector Appliances eine Verbindung zu Active Directory-Controllern herstellen. Welche Art von Connector verwendet werden sollte, hängt von Ihrer Bereitstellung ab.

Weitere Informationen zur Verwendung von Connectorgeräten mit Active Directory finden Sie unter Bereitstellungsszenarios für Connectorgeräte in Active Directory.

Installieren Sie Cloud Connector in Ihrem sicheren internen Netzwerk.

Wenn Sie eine Einzeldomäne in einer einzelnen Gesamtstruktur verwenden, müssen Sie Cloud Connectors nur in dieser Domäne installieren, um einen Ressourcenstandort einzurichten. Wenn Ihre Umgebung mehrere Domänen umfasst, müssen die Cloud Connectors so installiert werden, dass Benutzer auf die bereitgestellten Ressourcen zugreifen können.

Wenn die Vertrauensstellung zwischen den Domänen nicht hierarchisch ist, müssen Sie möglicherweise separate Cloud Connectors für jede Domäne oder Gesamtstruktur installieren. Diese Konfiguration ist evtl. erforderlich, um die Ressourcenaufzählung zu verarbeiten, wenn zum Zuweisen von Ressourcen Sicherheitsgruppen verwendet werden, oder für VDA-Registrierungen aus allen Domänen.

> **Hinweis:**
>
> Die folgenden Ressourcenstandorte bilden einen Blueprint, der möglicherweise an anderen physischen Standorten wiederholt werden muss, je nachdem, wo Ihre Ressourcen gehostet werden.

Einzeldomäne in einer Gesamtstruktur mit einem Cloud Connectors-Satz

In diesem Szenario enthält eine Einzeldomäne alle Ressourcen- und Benutzerobjekte (forest1.local). Ein Cloud Connectors-Satz wird an einem einzigen Ressourcenstandort bereitgestellt und in die Domäne "forest1.local"eingebunden.

- Vertrauensstellung: Ohne - Einzeldomäne
- Aufgelistete Domänen in der **Identitäts- und Zugriffsverwaltung**: forest1.local
- Benutzeranmeldungen bei Citrix Workspace: Für alle Benutzer unterstützt
- Benutzeranmeldungen bei einem On-Premises-StoreFront: Für alle Benutzer unterstützt

> **Hinweis:**
>
> Wenn Sie eine Hypervisor-Instanz in einer separaten Domäne haben, können Sie weiterhin einen einzigen Cloud Connectors-Satz bereitstellen, solange die Hypervisor-Instanz und die Cloud Connectors über dasselbe Netzwerk erreichbar sind. Citrix Cloud verwendet die Hostverbindung und ein verfügbares Netzwerk, um die Kommunikation mit dem Hypervisor herzustellen. Obwohl der Hypervisor sich in einer anderen Domäne befindet, müssen Sie keinen weiteren Cloud Connector-Satz in dieser Domäne bereitstellen, damit Citrix Cloud mit dem Hypervisor kommunizieren kann.

Über- und untergeordnete Domänen in einer Gesamtstruktur mit einem Cloud Connectors-Satz

Dieses Szenario umfasst eine übergeordnete Domäne (forest1.local) und eine ihr untergeordnete Domäne (user.forest1.local) in einer einzelnen Gesamtstruktur. Die übergeordnete Domäne ist die Ressourcendomäne. Die untergeordnete Domäne ist die Benutzerdomäne. Ein Cloud Connectors-Satz wird an einem einzigen Ressourcenstandort bereitgestellt und in die Domäne "forest1.local" eingebunden.

- Vertrauensstellung: Übergeordnete/untergeordnete Domäne mit Vertrauensstellung
- Aufgelistete Domänen in der **Identitäts- und Zugriffsverwaltung**: forest1.local, user.forest1.local
- Benutzeranmeldungen bei Citrix Workspace: Für alle Benutzer unterstützt
- Benutzeranmeldungen bei einem On-Premises-StoreFront: Für alle Benutzer unterstützt

> **Hinweis:**
>
> Möglicherweise ist ein Neustart der Cloud Connectors erforderlich, damit Citrix Cloud die untergeordnete Domäne registriert.

Benutzer und Ressourcen in separaten Gesamtstrukturen (mit Vertrauensstellung) mit einem Cloud Connectors-Satz

In diesem Szenario enthält eine Gesamtstruktur (forest1.local) Ihre Ressourcendomäne und eine zweite Gesamtstruktur (forest2.local) Ihre Benutzerdomäne. Eine unidirektionale Vertrauensstellung liegt vor, wenn die Gesamtstruktur mit der Ressourcendomäne der Gesamtstruktur mit der Benutzerdomäne vertraut. Ein Cloud Connectors-Satz wird an einem einzigen Ressourcenstandort bereitgestellt und in die Domäne "forest1.local"eingebunden.

- Vertrauensstellung: Unidirektionale Gesamtstruktur-Vertrauensstellung
- Aufgelistete Domänen in der **Identitäts- und Zugriffsverwaltung**: forest1.local
- Benutzeranmeldungen bei Citrix Workspace: Nur für "forest1.local"-Benutzer unterstützt
- Benutzeranmeldungen bei einem On-Premises-StoreFront: Für alle Benutzer unterstützt

> **Hinweis:**
>
> Die Vertrauensstellung zwischen den beiden Gesamtstrukturen muss es Benutzern in der Benutzergesamtstruktur ermöglichen, sich an Maschinen in der Ressourcengesamtstruktur anzumelden.

Da Cloud Connectors eine Vertrauensstellung auf Gesamtstrukturebene nicht nutzen können, wird die Domäne "forest2.local"auf der Seite **Identitäts- und Zugriffsverwaltung** in der Citrix Cloud-Konsole nicht angezeigt und kann von keiner cloudseitigen Funktionalität genutzt werden. Dies führt zu folgenden Einschränkungen:

- Ressourcen können nur für Benutzer und Gruppen in "forest1.local"in Citrix Cloud veröffentlicht werden. Bei Verwendung von StoreFront-Stores lässt sich dieses Problem durch Verschachteln von "forest2.local"-Benutzern in "forest1.local"-Sicherheitsgruppen eventuell umgehen.
- Citrix Workspace kann Benutzer aus der Domäne "forest2.local"nicht authentifizieren.
- Die Überwachungskonsole in Citrix DaaS kann die Benutzer aus der Domäne forest2.local nicht auflisten.

Um diese Einschränkungen zu umgehen, nutzen Sie zum Bereitstellen der Cloud Connectors das Verfahren unter Benutzer und Ressourcen in separaten Gesamtstrukturen (mit Vertrauensstellung) mit je einem Cloud Connectors-Satz in jeder Gesamtstruktur.

Benutzer und Ressourcen in separaten Gesamtstrukturen (mit Vertrauensstellung) mit je einem Cloud Connectors-Satz in jeder Gesamtstruktur

In diesem Szenario enthält eine Gesamtstruktur (forest1.local) Ihre Ressourcendomäne und eine zweite Gesamtstruktur (forest2.local) Ihre Benutzerdomäne. Eine unidirektionale Vertrauensstellung

liegt vor, wenn die Gesamtstruktur mit der Ressourcendomäne der Gesamtstruktur mit der Benutzerdomäne vertraut. Ein Cloud Connectors-Satz wird in der Domäne "forest1.local"bereitgestellt, ein zweiter Satz wird in der Domäne "forest2.local"bereitgestellt.

- Vertrauensstellung: Unidirektionale Gesamtstruktur-Vertrauensstellung
- Aufgelistete Domänen in der **Identitäts- und Zugriffsverwaltung**: forest1.local, forest2.local
- Benutzeranmeldungen bei Citrix Workspace: Für alle Benutzer unterstützt
- Benutzeranmeldungen bei einem On-Premises-StoreFront: Für alle Benutzer unterstützt

In diesem Szenario können Connector Appliances anstelle von Cloud Connectors in Benutzergesamtstrukturen ohne Ressourcen verwendet werden, um Kosten und Verwaltungsaufwand zu reduzieren, insbesondere wenn mehrere Benutzergesamtstrukturen vorhanden sind. Weitere Informationen finden Sie unter Benutzer und Ressourcen in getrennten Gesamtstrukturen (mit Vertrauensstellung) mit einem einzigen Connector Appliances-Satz für alle Gesamtstrukturen

Anzeigen der Integrität des Cloud Connectors

Auf der Seite "Ressourcenstandorte"in Citrix Cloud wird der Integritätsstatus aller Cloud Connectors in Ihren Ressourcenstandorten angezeigt. Sie können auch erweiterte Integritätsprüfungsdaten für jeden Cloud Connector anzeigen. Weitere Informationen finden Sie unter Erweiterte Cloud Connector-Integritätsprüfungen.

Ereignismeldungen

Der Cloud Connector generiert Ereignismeldungen, die Sie über die Windows-Ereignisanzeige anzeigen können. Wenn Sie diesen Meldungen mit einer Überwachungssoftware suchen möchten, können Sie sie als ZIP-Archiv herunterladen. Der ZIP-Download enthält diese Meldungen in folgenden XML-Dateien:

- Citrix.CloudServices.Agent.Core.dll.xml (Connector Agent Provider)
- Citrix.CloudServices.AgentWatchDog.Core.dll.xml (Connector AgentWatchDog Provider)

Laden Sie Cloud Connector-Ereignismeldungen herunter.

Ereignisprotokolle

Standardmäßig sind Ereignisprotokolle im Verzeichnis C:\ProgramData\Citrix\WorkspaceCloud\Logs auf der Maschine mit dem Cloud Connector.

Problembehandlung

Der erste Schritt bei der Diagnose von Problemen mit dem Cloud Connector ist die Überprüfung der Ereignismeldungen und Ereignisprotokolle. Wenn der Cloud Connector am Ressourcenstandort nicht aufgeführt wird oder als "nicht in Kontakt"angezeigt wird, enthalten die Ereignisprotokolle diverse anfängliche Informationen.

Cloud Connector-Konnektivität

Wenn die Verbindung zum Cloud Connector getrennt wird, können Sie mit dem Hilfsprogramm zur Cloud Connector-Konnektivitätsprüfung überprüfen, ob Citrix Cloud und die zugehörigen Dienste vom Cloud Connector erreicht werden können.

Das Hilfsprogramm zur Cloud Connector-Konnektivitätsprüfung wird auf der Hostmaschine des Cloud Connectors ausgeführt. Wenn Sie einen Proxyserver in Ihrer Umgebung verwenden, können Sie mit dem Hilfsprogramm durch Tunneln aller Verbindungstests die Konnektivität über Ihren Proxyserver überprüfen. Bei Bedarf kann das Hilfsprogramm auch fehlende vertrauenswürdige Sites von Citrix zur Zone vertrauenswürdiger Sites im Internet Explorer hinzufügen.

Weitere Informationen zum Herunterladen und Verwenden dieses Hilfsprogramms finden Sie im Citrix Support Knowledge Center unter CTX260337.

Installation

Wenn der Cloud Connector den Status "Fehler"hat, könnte es ein Problem beim Hosting des Cloud Connectors geben. Installieren Sie den Cloud Connector auf einer neuen Maschine. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support. Informationen zum Beheben häufiger Probleme bei der Installation oder der Verwendung des Cloud Connectors finden Sie unter CTX221535.

Bereitstellung von Cloud Connectors als Secure Ticket Authority-Server

Wenn Sie mehrere Cloud Connectors als Secure Ticket Authority-Server mit NetScaler Console verwenden, wird evtl. für jeden STA-Server in der NetScaler Console-Verwaltung und in der ICA-Datei für Anwendungs- und Desktopstarts **CWSSTA** als ID angegeben. STA-Tickets werden dann nicht korrekt geroutet und das Starten von Sitzungen schlägt fehl. Das Problem kann auftreten, wenn die Cloud Connectors unter separaten Citrix Cloud-Konten mit unterschiedlichen Kunden-IDs bereitgestellt wurden. In diesem Szenario tritt eine Ticket-Diskrepanz zwischen den einzelnen Konten auf, die verhindert, dass Sitzungen erstellt werden.

Um das Problem zu vermeiden, stellen Sie sicher, dass die Cloud Connectors, die Sie als STA-Server verwenden, demselben Citrix Cloud-Konto mit derselben Kunden-ID angehören. Wenn Sie mehrere Kundenkonten über eine NetScaler Console-Bereitstellung unterstützen, erstellen Sie für jedes Konto einen virtuellen Gateway-Server. Weitere Informationen hierzu finden Sie in den folgenden Artikeln:

- Erstellen virtuelle Gateway-Server: Create virtual servers
- Configuring the Secure Ticket Authority on Citrix Gateway
- Bereitstellungshandbuch: Migrieren der On-Premises-Version von Citrix Virtual Apps and Desktops zu Citrix Cloud
- CTX232640: How do I configure Citrix Gateway to use a Cloud Connector as a STA

Cloud Connector-Proxy und Firewall konfigurieren

April 6, 2024

Der Cloud Connector unterstützt die Verbindung zum Internet über einen nicht authentifizierten Webproxyserver. Das Installationsprogramm und die von ihm installierten Services erfordern Verbindungen mit Citrix Cloud.
An beiden Punkten muss Internetzugriff möglich sein.

Konnektivitätsanforderungen

Verwenden Sie Port 443 mit HTTP-Datenverkehr (nur Ausgang). Eine Liste der erforderlichen kontaktierbaren Adressen finden Sie in den folgenden Ressourcen:

- Anforderungen an System und Konnektivität
- Verbindungsanforderungen für den Cloud Connector

Die erforderlichen kontaktierbaren Adressen für Citrix Cloud werden als Domänennamen und nicht als IP-Adressen angegeben. Da IP-Adressen sich ändern können, stellt die Positivliste mit Domänennamen sicher, dass die Verbindung mit Citrix Cloud stabil bleibt.

Eine Liste der erforderlichen Ports finden Sie unter Konfiguration von eingehenden und ausgehenden Ports.

> **Wichtig:**
>
> - Auf einigen Proxys wird durch Aktivieren des SSL-Abfangens u. U. ein erfolgreicher Verbindungsaufbau zwischen Cloud Connector und Citrix Cloud verhindert.

- SSL-Abfangen ist an Citrix Gateway-Adressen nicht möglich. Weitere Informationen finden Sie unter Anforderungen an die Citrix Gateway-Servicekonnektivität.
- Durch SSL-Abfangen darf die Netzwerkkonnektivität oder -stabilität nicht beeinträchtigt werden. Weitere Informationen finden Sie unter Citrix Cloud Connector
- Wenn Sie einen Proxy verwenden, wird empfohlen, dass die folgenden Datenflüsse den Proxy umgehen:
  - Kommunikation zwischen Connectors (z. B. bei LHC-Ereignissen)
  - Kommunikation zwischen Connectors und VDA (WCF-Verbindung)
  - Kommunikation zwischen Connectors und Domänencontrollern (AD-Anforderungen)

Darüber hinaus ist zu beachten, dass der Connector die WinHTTP-Proxyeinstellungen verwendet. Konfigurationseinstellungen finden Sie unter CTX222727.

Überprüfen der Cloud Connector-Konnektivität

Mit dem Hilfsprogramm zur Cloud Connector-Konnektivitätsprüfung können Sie die Konnektivität zwischen Cloud Connector und Citrix Cloud mithilfe verschiedener Verbindungstests überprüfen. Wenn Sie einen Proxyserver in Ihrer Umgebung verwenden, können Sie mit dem Hilfsprogramm Proxyeinstellungen im Cloud Connector konfigurieren und die Konnektivität über den Proxyserver testen. Bei konfiguriertem Proxyserver werden die Verbindungstests über den Proxyserver getunnelt.

> **Hinweis:**
>
> Das Hilfsprogramm zur Cloud Connector-Konnektivitätsprüfung kann nur mit kommerziellen Citrix Cloud-Konten verwendet werden. Verwenden Sie es nicht mit Citrix Cloud Government oder Citrix Cloud Japan.

Weitere Informationen zum Herunterladen und Verwenden des Hilfsprogramms zur Cloud Connector-Konnektivitätsprüfung finden Sie unter CTX260337.

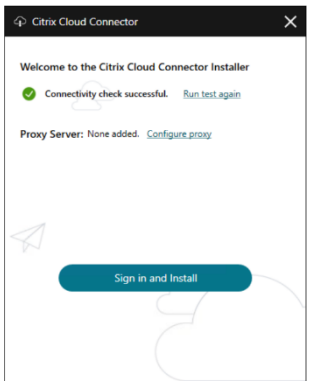
Installer

Das Installationsprogramm verwendet die für Internetverbindungen konfigurierten Einstellungen. Wenn Sie von der Maschine aus im Internet surfen können, müsste auch das Installationsprogramm funktionieren.

Services zur Laufzeit

Der Laufzeitdienst läuft im Kontext eines lokalen Diensts. Die für den Benutzer definierten Einstellungen (siehe oben) werden nicht verwendet.

Sie können die Proxyeinstellungen während des Installationsvorgangs konfigurieren.



Klicken Sie nach dem Start des Installationsprogramms und bevor Sie sich bei Citrix Cloud anmelden auf **Proxy konfigurieren**. Sie werden aufgefordert, die Proxyinformationen und Adressen hinzuzufügen, um den Proxy zu umgehen. Sowohl vollqualifizierte Domänennamen (FQDNs) als auch Platzhalteradressen werden bei der Angabe von Bypass-Adressen unterstützt.

> **Hinweis:**
>
> Wenn Sie einen Proxyserver verwenden, müssen Sie die Proxyeinstellung manuell vornehmen. Die automatische Proxyeinstellung, entweder durch automatische Erkennung oder durch PAC/Setup-Skripts, wird nicht unterstützt.

Cloud Connector-Installation

July 2, 2024

Sie können die Cloud Connector-Software interaktiv oder über die Befehlszeile installieren.

Die Installation erfolgt mit den Berechtigungen des Benutzers, der die Installation beginnt. Der Cloud Connector benötigt für folgende Aufgaben Zugriff auf die Cloud:

- Authentifizieren des Benutzers, der die Installation ausführt
- Validieren der Berechtigungen des installierenden Benutzers
- Download und Konfigurieren der Cloud Connector-Services

Vor Installation zu lesende Informationen

- Systemvoraussetzungen zur Vorbereitung der Maschinen für das Hosting des Cloud Connectors.
- Abschnitt Antivirus Exclusions des Tech Zone-Artikels Endpoint Security and Antivirus Best Practices mit Richtlinien zur Ermittlung des richtigen Gleichgewichts zwischen Sicherheit und Leistung für die Cloud Connectors in Ihrer Umgebung. Citrix empfiehlt dringend, diese Richtlinien

mit den für Virenschutz und Sicherheit verantwortlichen Teams im Unternehmen durchzuarbeiten und sie erst nach rigorosen Labortests in der Produktionsumgebung zu implementieren.
- Anforderungen an System und Konnektivität um sicherzustellen, dass alle Maschinen, die Cloud Connectors hosten, mit Citrix Cloud kommunizieren können.
- Konfiguration von Cloud Connector-Proxy und Firewall, wenn Sie den Cloud Connector in einer Umgebung mit Webproxy oder strikten Firewallregeln installieren.
- Überlegungen zur Skalierung und Größe für Cloud Connectors mit Informationen zu den getesteten maximalen Kapazitäten und Empfehlungen zu bewährten Methoden für die Konfiguration der Maschinen, die Cloud Connectors hosten.

Installationsleitfaden

- Installieren Sie den Cloud Connector nicht auf einem Active Directory-Domänencontroller oder einer anderen Maschine, die für Ihre Ressourcenstandortinfrastruktur kritisch ist. Normale Wartungsarbeiten am Cloud Connector bewirken Maschinenvorgänge, die zu einem Ausfall dieser zusätzlichen Ressourcen führen.
- Laden oder installieren Sie keine anderen Citrix Produkte auf den Maschinen, auf denen ein Cloud Connector gehostet wird.
- Aktualisieren Sie Cloud Connector-Komponenten nicht einzeln.
- Laden oder installieren Sie den Cloud Connector nicht auf Maschinen, die zu anderen Citrix Produktbereitstellungen gehören (z. B. Delivery Controller in einer On-Premises-Bereitstellung von Citrix Virtual Apps and Desktops).
- Führen Sie kein Upgrade eines installierten Cloud Connectors durch. Deinstallieren Sie stattdessen den alten Cloud Connector und installieren Sie den neuen.
- Das Cloud Connector-Installationsprogramm wird aus Citrix Cloud heruntergeladen. Ihr Browser muss daher das Herunterladen von ausführbaren Dateien zulassen.
- Wenn Sie das grafische Installationsprogramm verwenden, müssen Sie einen Browser installiert und den Standardsystembrowser festgelegt haben.

Empfehlungen für die Phase nach der Bereitstellung

Lassen Sie nach der Installation alle Cloud Connectors dauerhaft eingeschaltet, um eine ständige Verbindung mit Citrix Cloud sicherzustellen.

Maschinen umbenennen

Benennen Sie nach der Installation die Maschine, auf der der Cloud Connector gehostet wird, nicht um. Wenn Sie den Servernamen später ändern müssen, führen Sie die folgenden Schritte aus:

1. Entfernen Sie die Maschine aus dem Ressourcenstandort:
    a) Wählen Sie im Citrix Cloud-Menü die Option **Ressourcenstandorte**.
    b) Suchen Sie den Ressourcenstandort, den Sie verwalten möchten, und wählen Sie die Kachel **Cloud Connectors**.
    c) Suchen Sie die gewünschte Maschine und klicken Sie auf die Auslassungspunkte. Wählen Sie **Connector entfernen**.
2. Deinstallieren Sie die Cloud Connector-Software.
3. Benennen Sie die Maschine um.
4. Installieren Sie die neueste Version der Cloud Connector-Software, wie in diesem Artikel beschrieben.

Maschinen in eine andere Domäne verschieben

Verschieben Sie nach der Installation die Maschine, auf der der Cloud Connector gehostet wird, nicht in eine andere Domäne. Wenn Sie die Maschine später einer anderen Domäne hinzufügen müssen, führen Sie die folgenden Schritte aus:

1. Entfernen Sie die Maschine aus dem Ressourcenstandort.
2. Deinstallieren Sie die Cloud Connector-Software.
3. Trennen Sie die Maschine von der aktuellen Domäne und fügen Sie sie der neuen Domäne hinzu.
4. Installieren Sie die neueste Version der Cloud Connector-Software, wie in diesem Artikel beschrieben.

Überlegungen zu geklonten Maschinen

Jede Maschine, auf der ein Cloud Connector gehostet wird, muss über eine eindeutige SID und eine eindeutige Connector-ID verfügen, damit Citrix Cloud zuverlässig mit den Maschinen am Ressourcenstandort kommunizieren kann. Wenn Sie den Cloud Connector auf mehreren Maschinen am Ressourcenstandort hosten und geklonte Maschinen verwenden möchten, führen Sie die folgenden Schritte aus:

1. Bereiten Sie die Maschinenvorlage gemäß den Anforderungen für Ihre Umgebung vor.
2. Stellen Sie so viele Maschinen bereit, wie Sie Cloud Connectors verwenden möchten.
3. Installieren Sie den Cloud Connector manuell oder im unbeaufsichtigten Modus auf allen Maschinen.

Installation des Cloud Connectors auf einer Maschinenvorlage (vor dem Klonen) wird nicht unterstützt. Wenn Sie eine Maschine mit installiertem Cloud Connector klonen, werden die Cloud Connector-Services nicht ausgeführt und die Maschine kann keine Verbindung mit Citrix Cloud herstellen.

Überlegungen zu Services

Die Installationsschritte in diesem Artikel beschreiben den Prozess für die Bereitstellung von Cloud Connectors, unabhängig davon, für welchen Service sie verwendet werden.

Stellen Sie bei der Bereitstellung von Cloud Connectors für Citrix DaaS sicher, dass die AD-Domänen der Connectors aktiv sind und in der Citrix Cloud-Konsole nicht als "unbenutzt"angezeigt werden. Wenn Sie beim Einrichten des Maschinenkatalogs in Citrix DaaS eine unbenutzte Domäne angeben, kann ein Fehler auftreten. Weitere Informationen finden Sie unter Ressourcentyp hinzufügen oder eine unbenutzte Domäne in Citrix Cloud aktivieren in der Citrix DaaS-Produktdokumentation.

Weitere Überlegungen zu anderen Services finden Sie in der Dokumentation des Service.

Standardressourcenstandorte

Wenn Sie keine Ressourcenstandorte in Ihrem Citrix Cloud-Konto haben und Cloud Connectors in Ihrer Domäne installieren, wird der von Citrix Cloud erstellte Ressourcenstandort zum Standardressourcenstandort. Sie können nur einen Standardressourcenstandort in Ihrem Konto haben. Bei Bedarf können Sie zusätzliche Ressourcenstandorte in Citrix Cloud erstellen und dann den gewünschten auswählen, wenn Sie Cloud Connectors in anderen Domänen installieren.

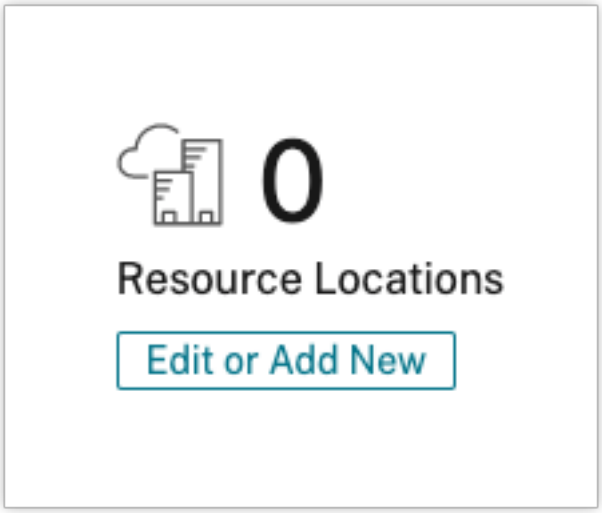
Alternativ können Sie zuerst die benötigten Ressourcenstandorte in der Konsole erstellen, bevor Sie Cloud Connectors in Ihren Domänen installieren. Das Cloud Connector-Installationsprogramm fordert Sie während der Installation auf, den gewünschten Ressourcenstandort auszuwählen.

Interaktive Installation

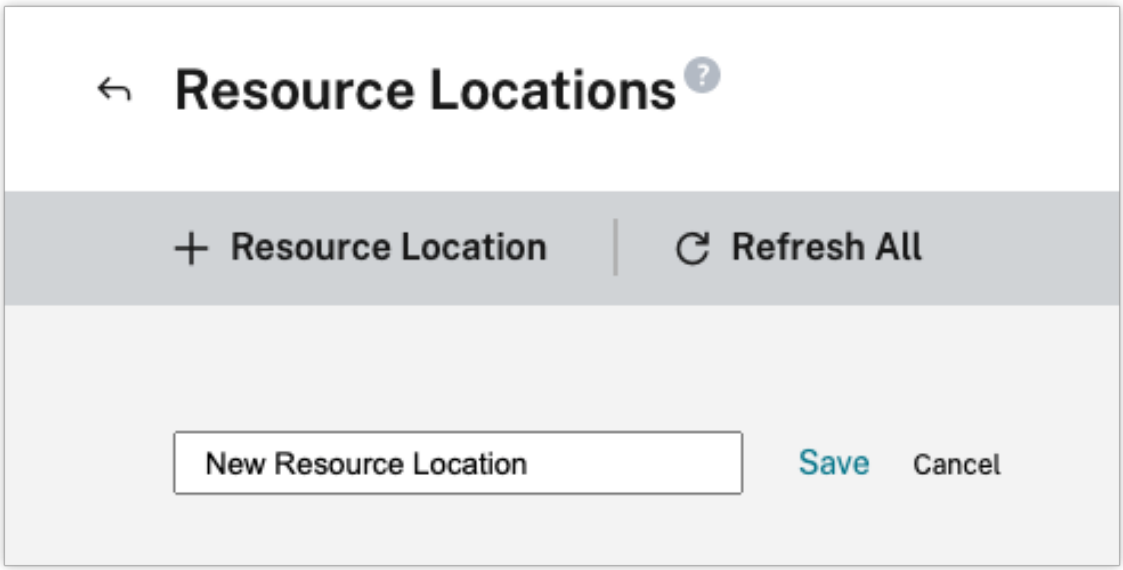
Sie können Cloud Connectors über das grafische Installationsprogramm herunterladen und installieren. Zuvor müssen Sie mindestens einen Ressourcenstandort in der Citrix Cloud-Verwaltungskonsole zur Bereitstellung von Cloud Connectors erstellen. Weitere Informationen finden Sie unter Ressourcenstandorte.

Erstellen eines Ressourcenstandorts

1. Melden Sie sich als Windows-Administrator bei der Maschine an, auf der Sie Citrix Cloud Connectors installieren möchten.
2. Melden Sie sich auf https://citrix.cloud.com mit Ihrem Administratorkonto an.
3. Wählen Sie in der Citrix Cloud-Konsole im Hauptmenü **Ressourcenstandorte** oder oben auf der Seite unter **Ressourcenstandorte** die Option **Bearbeiten oder hinzufügen**.



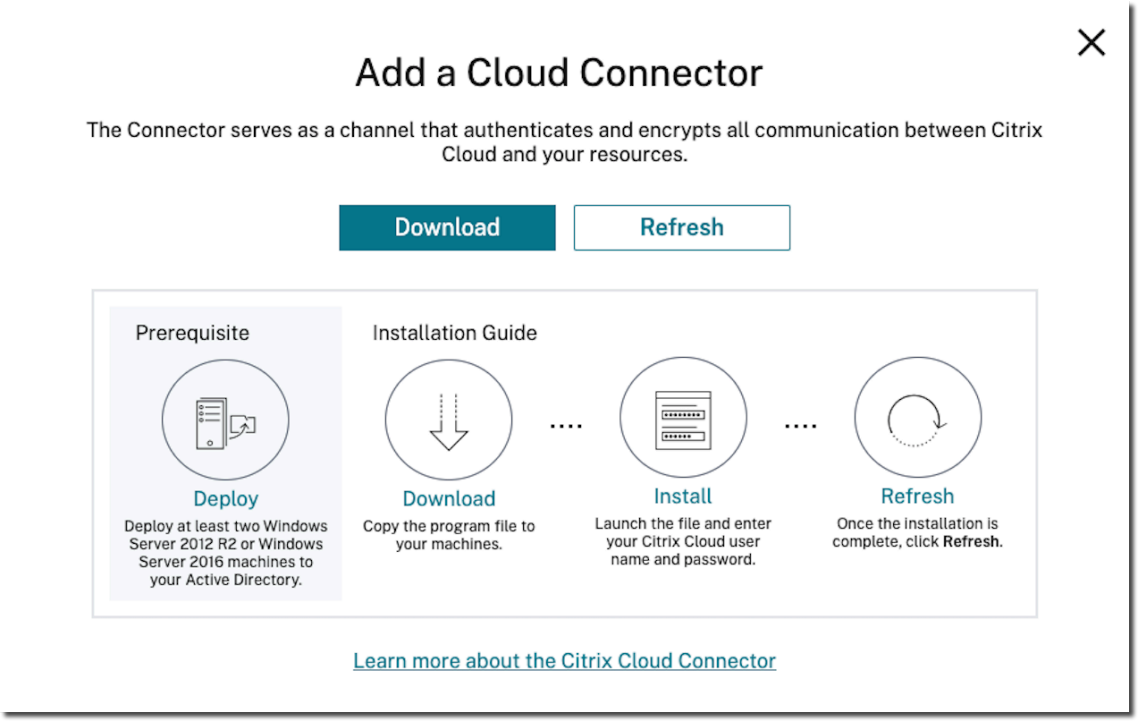
4. Wählen Sie unter "Ressourcenstandorte"oben auf der Seite **+ Ressourcenstandort** und geben Sie einen aussagekräftigen Namen an.



Herunterladen der Citrix Cloud Connector-Software

1. Suchen Sie den Ressourcenstandort, den Sie verwalten möchten, und wählen Sie **+ Cloud Connectors**.

2. Wählen Sie in dem nun geöffneten Fenster **Herunterladen**. Speichern Sie die Datei **cwcconnector.exe** lokal auf der Connector-Maschine.



Installieren der Citrix Cloud Connector-Software

1. Klicken Sie mit der rechten Maustaste auf das Installationsprogramm **cwcconnector.exe** und wählen Sie **Als Administrator ausführen** aus. Das Installationsprogramm führt eine erste Konnektivitätsprüfung durch, um sicherzustellen, dass Sie eine Verbindung mit Citrix Cloud herstellen können.
2. Optional:Klicken Sie bei Bedarf auf **Proxy konfigurieren**, um einen Proxyserver hinzuzufügen. Sie werden aufgefordert, die Proxyinformationen und Adressen hinzuzufügen, um den Proxy zu umgehen. Sowohl vollqualifizierte Domänennamen (FQDNs) als auch Platzhalteradressen werden bei der Angabe von Bypass-Adressen unterstützt.
3. Klicken Sie auf **Anmelden und Installieren**, um sich bei Citrix Cloud anzumelden.
4. Folgen Sie dem Assistenten, um den Cloud Connector zu installieren und zu konfigurieren. Wenn die Installation abgeschlossen ist, prüft das Installationsprogramm als letzte Verbindung-

sprüfung die Kommunikation zwischen Cloud Connector und Citrix Cloud.

5. Wiederholen Sie diese Schritte auf allen Maschinen, die Sie als Citrix Cloud Connector verwenden möchten. Für eine hohe Verfügbarkeit empfiehlt Citrix die Installation von mindestens zwei Cloud Connectors pro Ressourcenstandort.

Citrix Cloud zeigt den neuen Cloud Connector auf der Seite **Connectors** für Ihren Ressourcenstandort an.

Nach der Installation registriert Citrix Cloud außerdem Ihre Domäne in **Identitäts- und Zugriffsverwaltung > Domänen**. Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung.

Ungenutzte Domänen aktivieren

Wenn Sie Ressourcenstandorte erstellen und Cloud Connectors für Citrix DaaS bereitstellen, stellen Sie sicher, dass die AD-Domänen, die Sie mit Citrix DaaS verwenden, aktiv sind und nicht als ungenutzt gelten. Wenn Sie beim Einrichten von Maschinenkatalogen in Citrix DaaS eine unbenutzte Domäne angeben, kann ein Fehler auftreten.

Weitere Informationen finden Sie unter Ressourcentyp hinzufügen oder eine unbenutzte Domäne in Citrix Cloud aktivieren in der Citrix DaaS-Produktdokumentation.

Erstellen zusätzlicher Ressourcenstandorte

1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf die Menüschaltfläche und wählen Sie **Ressourcenstandorte**.
2. Klicken Sie auf **+ Ressourcenstandort** und geben Sie einen aussagekräftigen Namen

3. Klicken Sie auf **Speichern**. Citrix Cloud zeigt eine Kachel für den neuen Ressourcenstandort an.
4. Klicken Sie auf **Cloud Connectors** und dann auf **Herunterladen**, um die Cloud Connector-Software zu beschaffen.
5. Installieren Sie auf jeder vorbereiteten Maschine die Cloud Connector-Software mit dem Installationsassistenten oder über die Befehlszeile. Sie werden von Citrix Cloud aufgefordert, den Ressourcenstandort auszuwählen, den Sie dem Cloud Connector zuordnen möchten.

Installation mit mehreren Kunden und vorhandenen Ressourcenstandorten

Wenn Sie Administrator mehrerer Kundenkonten sind, werden Sie von Citrix Cloud aufgefordert, das Kundenkonto auszuwählen, das Sie dem Cloud Connector zuordnen möchten.

Wenn Ihr Kundenkonto bereits mehrere Ressourcenstandorte hat, werden Sie von Citrix Cloud aufgefordert, denjenigen auszuwählen, den Sie dem Cloud Connector zuordnen möchten.

Befehlszeileninstallation

Eine automatische bzw. unbeaufsichtigte Installation wird unterstützt. Die Verwendung desselben Installationsprogramms für wiederholte Installationen wird jedoch nicht empfohlen. Laden Sie einen neuen Cloud Connector von der Seite “Ressourcenstandorte”in der Citrix Cloud-Konsole herunter.

Anforderungen

Um die Befehlszeileninstallation für Citrix Cloud zu verwenden, müssen Sie die folgenden Informationen angeben:

- Kunden-ID des Citrix Cloud-Kontos, für das Sie den Cloud Connector installieren. Die ID wird oben auf der Registerkarte **API-Zugriff** unter **Identitäts- und Zugriffsverwaltung** angezeigt.
- Client-ID und Geheimnis des sicheren API-Clients, den Sie zur Installation des Cloud Connectors verwenden möchten. Um diese Werte zu erhalten, müssen Sie zuerst einen sicheren Client erstellen. Die Client-ID und das Geheimnis stellen den ordnungsgemäßen Schutz Ihres Zugriffs auf die Citrix Cloud-API sicher. Wenn Sie einen sicheren Client erstellen, läuft dieser mit der gleichen Administratorberechtigung, die Sie haben. Um einen Cloud Connector zu installieren, müssen Sie einen sicheren Client verwenden, der von einem Administrator mit Vollzugriff erstellt wurde, sodass auch der sichere Client über Vollzugriff verfügt.
- ID des Ressourcenstandorts, den Sie dem Cloud Connector zuordnen möchten. Um diesen Wert abzurufen, klicken Sie auf die Schaltfläche **ID** unterhalb des Namens des Ressourcenstandorts auf der Seite **Ressourcenstandorte**. Wenn Sie diesen Wert nicht angeben, verwendet Citrix Cloud die ID des Standardressourcenstandorts.

Erstellen eines sicheren Clients

Beim Erstellen eines sicheren Clients generiert Citrix Cloud eine eindeutige Client-ID und ein Geheimnis. Sie müssen diese Werte angeben, wenn Sie die API über die Befehlszeile aufrufen.

1. Wählen Sie im Menü "Citrix Cloud"**Identitäts- und Zugriffsverwaltung** und dann **API-Zugriff**.
2. Geben Sie auf der Registerkarte **Sichere Clients** einen Namen für den Client ein und wählen Sie **Client erstellen**. Citrix Cloud generiert eine Client-ID und ein Geheimnis für den sicheren Client und zeigt sie an.
3. Wählen Sie **Herunterladen**, um die Client-ID und das Geheimnis als CSV-Datei herunterzuladen und speichern Sie diese an einem sicheren Ort. Alternativ wählen Sie **Kopieren**, um die Werte manuell zu erhalten. Wenn Sie fertig sind, wählen Sie **Schließen**, um zur Konsole zurückzukehren.

Unterstützte Parameter

Zur Gewährleistung der Sicherheit der Details des sicheren Clients erfordert das Installationsprogramm eine JSON-Konfigurationsdatei. Diese Datei muss nach Abschluss der Installation gelöscht werden. Für die Konfigurationsdatei werden folgende Werte unterstützt:

- **customerName** (erforderlich). Die Kunden-ID wird auf der Seite "API-Zugriff"in der Citrix Cloud-Konsole im Bereich "Identitäts- und Zugriffsverwaltung"angezeigt.
- **clientId** (erforderlich). ID des sicheren Clients, die ein Administrator erstellen kann (ist auf der Seite "API-Zugriff").
- **clientSecret** (erforderlich). Geheimnis des sicheren Clients, das nach dessen Erstellung heruntergeladen werden kann. Befindet sich auf der Seite "API-Zugriff".
- **resourceLocationId** (empfohlen). Der eindeutige Bezeichner eines vorhandenen Ressourcenstandorts. Wählen Sie die Schaltfläche "ID", um in der Citrix Cloud-Konsole auf der Seite "Ressourcenstandorte"die ID für den Ressourcenstandort abzurufen. Wenn kein Wert angegeben wird, verwendet Citrix Cloud die ID des ersten Ressourcenstandorts des Kontos.
- **acceptTermsOfService** (erforderlich). Muss auf **true** gesetzt werden.

Beispiel für eine Konfigurationsdatei

```
{

"customerName": "*CustomerID*",
"clientId": "*ClientID*",
"clientSecret": "*ClientSecret*",
"resourceLocationId": "*ResourceLocationId*",
"acceptTermsOfService": "true"
 }
```



```
9
10 <!--NeedCopy-->
```

Beispiel für einen Befehl

Mit dem folgenden Befehl wird die Cloud Connector-Software automatisch mithilfe einer JSON-Konfigurationsdatei installiert:

```
1 CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
     json
2 <!--NeedCopy-->
```

Verwenden Sie `/q`, um eine automatische Installation festzulegen.

Verwenden Sie **Start /Wait CWCConnector.exe /ParametersFilePath:value**, um bei Problemen einen möglichen Fehlercode zu untersuchen. Sie können den Standardmechanismus **echo% ErrorLevel%** ausführen, nachdem die Installation abgeschlossen ist.

> **Hinweis:**
>
> Die Verwendung von Parametern zum Übergeben der Client-ID und des Clientgeheimnisses wird nicht mehr unterstützt. Die Konfigurationsdatei muss für automatisierte Installationen verwendet werden.

Nächste Schritte

1. Richten Sie den Updatezeitplan für den Citrix Cloud Connector ein. Informationen zu Citrix Cloud Connector-Updates und zum Verwalten von Updatezeitplänen finden Sie unter Connector-Updates.
2. Richten Sie einen Identitätsanbieter zur Authentifizierung der Workspace-Abonnenten ein. In der Konsole **Identitäts- und Zugriffsmanagement** können Sie den standardmäßigen Citrix Identitätsanbieter in Ihr Active Directory oder andere Identitätsanbieter ändern. Weitere Informationen finden Sie unter Verbinden von Azure Active Directory mit Citrix Cloud.

Problembehebung bei der Installation

In diesem Abschnitt werden Diagnose und Behebung von potenzieller Problemen bei der Installation beschrieben. Weitere Informationen zur Behebung von Installationsproblemen finden Sie unter Citrix Cloud Connector Troubleshooting Guide.

Installationsprotokolle

Sie können Probleme beheben, die bei der Installation aufgetreten sind, indem Sie zuerst die verfügbaren Protokolldateien konsultieren.

Ereignisse, die während der Installation aufgetreten sind, werden in der **Windows-Ereignisanzeige** angezeigt. Sie können auch die Cloud Connector-Installationsprotokolle **%LOCALAPPDATA%\Temp\CitrixLogs\C** überprüfen.
Protokolle werden nach der Installation auch zu **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** hinzugefügt.

Exitcodes

Die folgenden Exitcodes werden je nach Erfolg oder Misserfolg des Installationsvorgangs angezeigt:

- 1603 - Ein unerwarteter Fehler ist aufgetreten.
- 2 - Eine Voraussetzungsprüfung wurde nicht bestanden.
- 0 - Installation erfolgreich abgeschlossen.

Installationsfehler

Wenn Sie die Citrix Cloud Connector-Software durch Doppelklicken auf das Installationsprogramm installieren, wird möglicherweise die folgende Fehlermeldung angezeigt:

```
Can't reach this page.
```

Dieser Fehler kann auch dann auftreten, wenn Sie als Administrator bei der Maschine angemeldet sind, auf der Sie den Citrix Cloud Connector installieren. Um den Fehler zu vermeiden, führen Sie die Citrix Cloud Connector-Software als Administrator aus, indem Sie mit der rechten Maustaste auf das Installationsprogramm klicken und “Als Administrator ausführen”auswählen.

Verbindungsfehler

Um sicherzustellen, dass der Cloud Connector mit Citrix Cloud kommunizieren kann, vergewissern Sie sich, dass die folgenden Citrix Dienste den Status **Gestartet** haben:

- Citrix Cloud AD Provider
- Citrix Cloud Agent Logger
- Citrix Cloud Agent System
- Citrix Cloud Agent Watchdog
- Citrix Cloud Credential Provider
- Citrix Config Synchronizer Service

- Citrix Dienst für hohe Verfügbarkeit
- Citrix NetScaler CloudGateway
- Citrix Remote Broker Provider
- Citrix Remote HCL Server
- Citrix Session Manager Proxy

Weitere Informationen zu diesen Diensten finden Sie unter Installierte Dienste.

Wenn weiterhin Verbindungsfehler auftreten, verwenden Sie das Hilfsprogramm Cloud Connector Connectivity Check Utility aus dem Citrix Support Knowledge Center. Weitere Informationen finden Sie unter CTX260337 im Knowledge Center.

Das Tool kann für Folgendes verwendet werden:

- Tests zur Erreichbarkeit von Citrix Cloud und zugehöriger Dienste.
- Suchen häufig falsch konfigurierter Einstellungen.
- Konfiguration von Proxy-Einstellungen auf dem Citrix Cloud Connector

Weitere Informationen zum Beheben von Verbindungsfehlern finden Sie unter CTX224133: Cloud Connector Connectivity Check Failed.

Erweiterte Cloud Connector-Integritätsprüfungen

December 11, 2023

Vor und nach Updates führt Cloud Connector Integritätsprüfungen durch, um unnötige Ausfallzeiten für Anbieter durch Updates zu vermeiden. Sie können den Verbindungs- und Integritätsstatus des Connectors und jedes seiner Dienste und Anbieter sehen.

Anzeigen von Connector-Integritätsprüfungsdaten

1. Wählen Sie im Citrix Cloud-Menü die Option **Ressourcenstandorte**.
2. Wählen Sie den Connector, dessen Integritätsprüfungsdaten Sie anzeigen möchten.
3. Klicken Sie auf der Seite “Connectors”auf die Auslassungspunkte neben dem Connector und wählen Sie **Connectordaten anzeigen**.

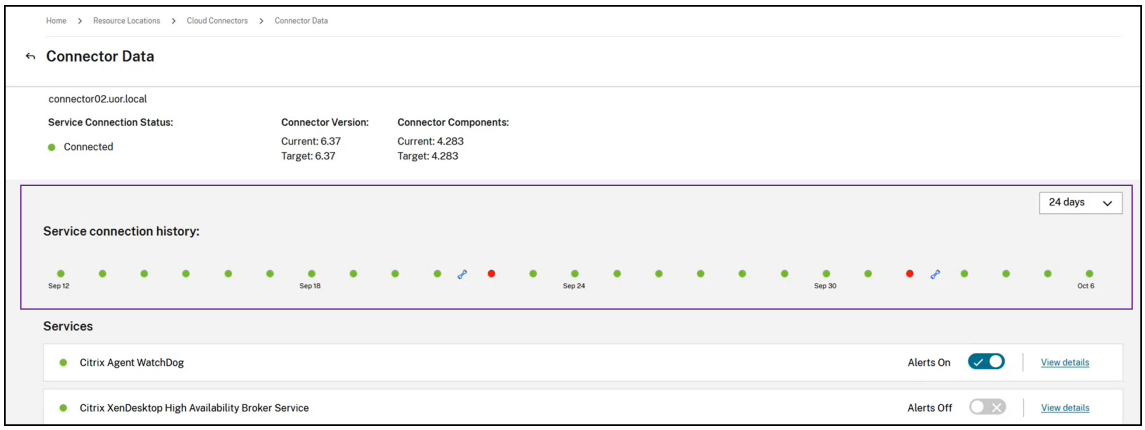
Die Seite “Connectordaten”wird mit den folgenden Informationen angezeigt.

- **Status der Dienstverbindung:** Dieser Bereich enthält Folgendes:
  - Status der Verbindung zwischen Connector und Cloud

  - Installierte Version des Connectors und seiner Komponenten sowie Zielversion, die im nächsten Update installiert werden soll

- **Dienstverbindung - Verlauf:** 24 Statusanzeigen zur Integrität des Connectors im Zeitverlauf. Standardmäßig wird der Status der Dienstverbindungen über die vergangenen 24 Stunden in Intervallen von einer Stunde angezeigt. Zum Anzeigen weiterer Daten, wählen Sie **24 Tage** im Dropdownmenü. In dieser Ansicht wird der Status der letzten 24 Tage in Intervallen von einem Tag angezeigt.

  - Ein grüner Punkt kennzeichnet einen fehlerfreien Status während des Zeitintervalls.
  - Ein roter Punkt weist auf einen Fehler- oder Ausnahmestatus während des Zeitintervalls hin. Zeigen Sie mit der Maus auf den Punkt, um weitere Informationen einzublenden.
  - Ein Schraubenschlüsselsymbol zeigt an, dass während des Zeitintervalls eine Aktualisierung stattgefunden hat. Zeigen Sie mit der Maus auf das Schraubenschlüsselsymbol, um weitere Informationen einzublenden.
  - Ein grauer Punkt zeigt an, dass während des Zeitintervalls keine Integritätsstatusinformationen empfangen wurden.



- **Dienste:** In diesem Bereich werden alle im Connector ausgeführten Dienste aufgeführt.

  - Der Punkt neben den einzelnen Diensten zeigt den aktuellen Dienststatus an.
  - Mit **Warnungen ein** und **Warnungen aus** können Sie die Warnungen zu Diensten aktivieren oder deaktivieren. Bei Auswahl “Warnungen ein”führen Ausfälle im Dienst zu einem Fehler des Connector-Verbindungsstatus insgesamt.
  - Wählen Sie **Details anzeigen**, um Details zum Integritätsstatus eines Diensts im Zeitverlauf anzuzeigen.

- **Connectormetriken:** In diesem Bereich wird die Nutzung von Arbeitsspeicher, CPU, Netzwerkdaten und Festplattenspeicher durch den Connector für die letzten 24 Stunden oder 24 Tage angezeigt. Verwenden Sie das Dropdownmenü im Bereich **Dienstverbindung - Verlauf**, um den angezeigten Zeitraum zu wählen.

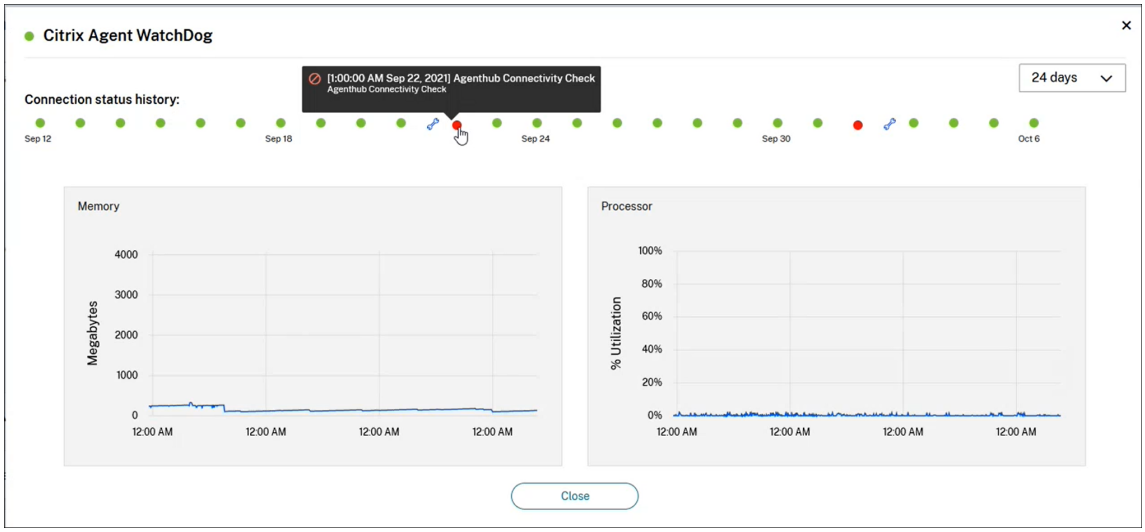
Anzeigen von Details zu Diensten

Zum Anzeigen des Verbindungsverlaufs und der Metriken für einzelne Dienste gehen Sie folgendermaßen vor:

1. Verwenden Sie das Dropdownmenü im Bereich **Dienstverbindung - Verlauf**, um den Zeitraum zu wählen. Sie können die letzten 24 Stunden in Ein-Stunden-Intervallen oder die letzten 24 Tage in Ein-Tages-Intervallen anzeigen.
2. Wählen Sie auf der Seite "Connectordaten"neben dem gewünschten Dienst die Option **Details anzeigen**.

Die angezeigte Seite enthält Folgendes:

- 24 Statusanzeigen zur Integrität des Dienst im Zeitverlauf.
  - Ein grüner Punkt kennzeichnet einen fehlerfreien Status während des Zeitintervalls.
  - Ein roter Punkt weist auf einen Fehler- oder Ausnahmestatus während des Zeitintervalls hin. Zeigen Sie mit der Maus auf den Punkt, um weitere Informationen einzublenden.
  - Ein Schraubenschlüsselsymbol zeigt an, dass während des Zeitintervalls eine Aktualisierung stattgefunden hat. Zeigen Sie mit der Maus auf das Schraubenschlüsselsymbol, um weitere Informationen einzublenden.
  - Ein grauer Punkt zeigt an, dass während des Zeitintervalls keine Integritätsstatusinformationen empfangen wurden.
- Diagramme zur Speicher- und Prozessornutzung durch den Dienst während des angegebenen Zeitraums



Connector-Benachrichtigungen

November 1, 2022

Connectors generieren innerhalb von zwei Stunden nach Auftreten eines Warn- oder Fehlerzustands eine Benachrichtigung. Sie können neue Benachrichtigungen im Glockensymbol in der Citrix Cloud-Kopfzeile sehen.

Klicken Sie auf dieses Symbol, um die Benachrichtigungen anzuzeigen, oder wählen Sie im Konsolenmenü die Option **Benachrichtigungen**.

Weitere Informationen finden Sie unter Benachrichtigungen.

Cloud Connector

Die folgende Tabelle enthält die Benachrichtigungen, die von einem Cloud Connector gesendet werden können:

Warnmeldung	Warnungstyp	Details	Auflösung
Connector *CONNECTORNAME* ist offline und veraltet, nachdem die reguläre Wartung fehlgeschlagen ist. Veraltete Connectors wirken sich auf Serviceverfügbarkeit aus und verhindern Wartung.	Fehler	Wenn ein Connector lange offline war und dann wieder online geht, kann es sich um eine alte Version handelt, die nicht auf die aktuelle Version aktualisiert werden kann. Veraltete Connectors können keine Wartung durchführen und wirken sich möglicherweise auf den Wartungsprozess anderer Connectors in der Umgebung aus.	Veralteten Cloud Connector aktualisieren

Warnmeldung	Warnungstyp	Details	Auflösung
Connector *CONNECTORNAME* ist nicht mit UTC-Zeit synchronisiert. Connectors in diesem Zustand können die Verfügbarkeit, Funktionalität oder Leistung von Services beeinträchtigen.	Fehler		How Do I Synchronize the Cloud Connector Time
Wartung auf Connector *CONNECTORNAME* ist fehlgeschlagen. Die fehlgeschlagene Wartung an dem Connector verhindert die Wartung anderer Connectors in der Umgebung. Connectors mit fehlgeschlagener Wartung können die Verfügbarkeit, Funktionalität oder Leistung von Services beeinträchtigen.	Fehler	Connector-Upgrade oder anderer Wartungsvorgang fehlgeschlagen.	How Do I Resolve a Failed Cloud Connector Maintenance
Connector *CONNECTOR_NAME* ist seit mindestens *ANZAHL* Stunde(n) offline. Connectors, die offline sind, wirken sich auf Serviceverfügbarkeit aus und verhindern Wartung.	Warnung	Wenn ein Connector eine bestimmte Zeit lang nicht kontaktiert werden kann, wird er als offline betrachtet.	How Do I Restore an Offline Cloud Connector to an Online State

Warnmeldung	Warnungstyp	Details	Auflösung
Connector *CONNECTOR_NAME* ist bei kürzlich durchgeführter Konnektivitätsprüfung fehlgeschlagen. Eine fehlgeschlagene Konnektivitätsprüfung kann die Serviceverfügbarkeit oder -funktionalität beeinträchtigen.	Warnung	Fehler bei einer Konnektivitätsprüfung mit Fehlercode *CODE*. Der Connector konnte in der Benachrichtigung aufgelistete Web- oder IP-Adressen nicht kontaktieren.	Cloud Connector Connectivity Check Failed
Hohe CPU-Auslastung bei Connector *CONNECTORNAME*. Connectors mit begrenzten Ressourcen können die Verfügbarkeit, Funktionalität oder Leistung von Services beeinträchtigen.	Warnung	Bei dem Connector wurde eine CPU-Auslastung von 80 % über einen Zeitraum von einer Stunde überschritten.	How Do I Resolve a Cloud Connector Resource Availability Alert
Connector *CONNECTORNAME* hat wenig freien Speicherplatz. Connectors, die mit eingeschränktem Speicherplatz arbeiten, beeinträchtigen die Serviceleistung und -wartung.	Warnung	Der Connector hat weniger als 2 GB freien Speicherplatz.	How Do I Resolve a Cloud Connector Resource Availability Alert

Warnmeldung	Warnungstyp	Details	Auflösung
Der Connector *CONNECTORNAME* hat erkannt, dass ein wichtiger Prozess oder Dienst nicht mehr ausgeführt wird. Dieser Zustand kann die Verfügbarkeit, Funktionalität oder Leistung von Services beeinträchtigen.	Warnung		

Protokollsammlung für Citrix Cloud Connector

September 28, 2023

CDF-Protokolle werden zur Problembehandlung bei Citrix Produkten verwendet. Der Citrix Support verwendet CDF-Tracingberichte zur Problemdiagnose beim Anwendungs- und Desktop-Brokering, der Benutzerauthentifizierung und der VDA-Registrierung. In diesem Artikel wird erläutert, wie Sie Cloud Connector-Daten zur Behebung von eventuell auftretenden Problemen erfassen.

> **Wichtige Hinweise:**
>
> - Aktivieren Sie die Protokollierung auf allen Cloud Connector-Maschinen an den Ressourcenstandorten.
> - Um sicherzustellen, dass Sie alle Daten erfassen, empfiehlt Citrix die Verwendung des CDFControl-Tools auf dem VDA. Weitere Informationen finden Sie unter CTX111961 im Citrix Support Knowledge Center. Weitere Informationen zur Protokollerfassung für die Citrix Workspace-App finden Sie unter CTX141751.
> - Um CDF-Tracingberichte an Citrix zu übermitteln, muss ein geöffneter Citrix Supportfall vorliegen. Die Citrix Support-Mitarbeiter können keine CDF-Tracingberichte überprüfen, die nicht an einen vorhandenen Supportfall angehängt sind.

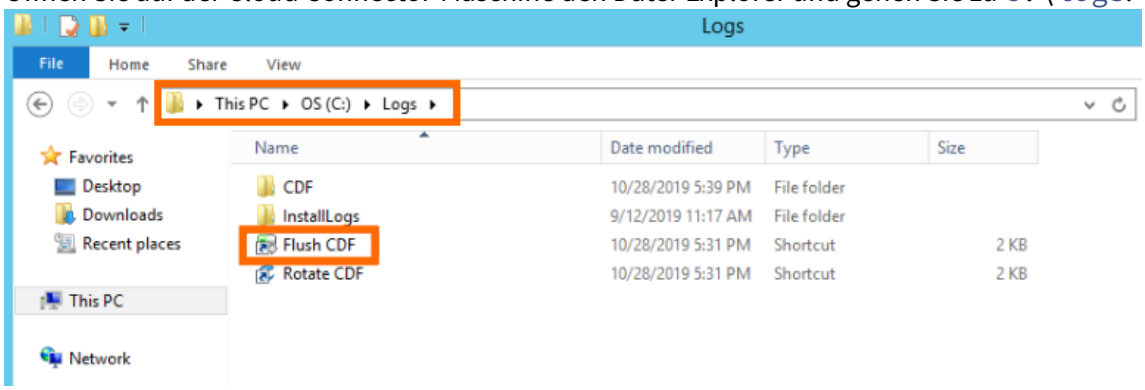
Schritt 1: Problem reproduzieren

Reproduzieren Sie das Problem. Wenn das Problem mit Anwendungsstarts oder Anwendungs-Brokering zusammenhängt, reproduzieren Sie den Startfehler. Wenn das Problem mit der VDA-Registrierung zusammenhängt, reproduzieren Sie den Registrierungsversuch, indem Sie Citrix Desktop Service auf der VDA-Maschine manuell neu starten.

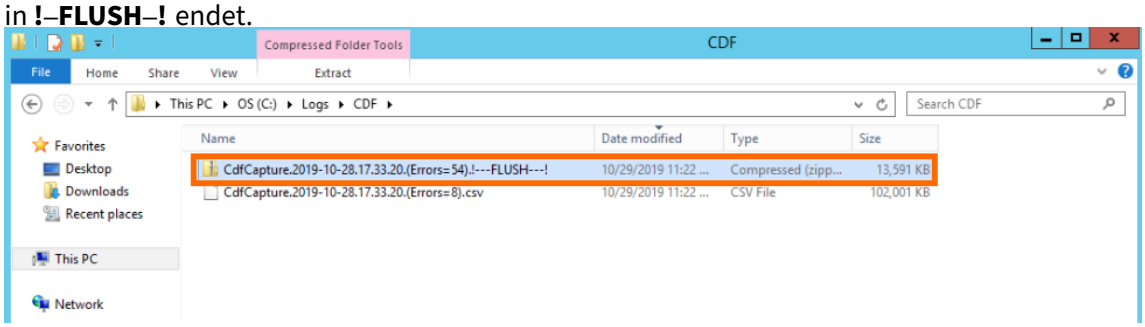
Schritt 2: CDF-Tracingberichte sammeln

Sammeln Sie CDF-Tracingberichte von jedem Cloud Connector am Ressourcenstandort.

1. Stellen Sie unter Verwendung eines Domänenadministratorkontos oder eines lokalen Administratorkontos eine RDP-Verbindung mit der Cloud Connector-Maschine her.
2. Öffnen Sie auf der Cloud Connector-Maschine den Datei-Explorer und gehen Sie zu `C:\logs`.



3. Führen Sie **Flush CDF** aus. Auf der Taskleiste der Cloud Connector-Maschine wird für kurze Zeit ein Symbol eingeblendet.
4. Gehen Sie im Datei-Explorer zu C:\logs\CDF und suchen Sie den neuesten Ordner, dessen Name in **!–FLUSH–!** endet.

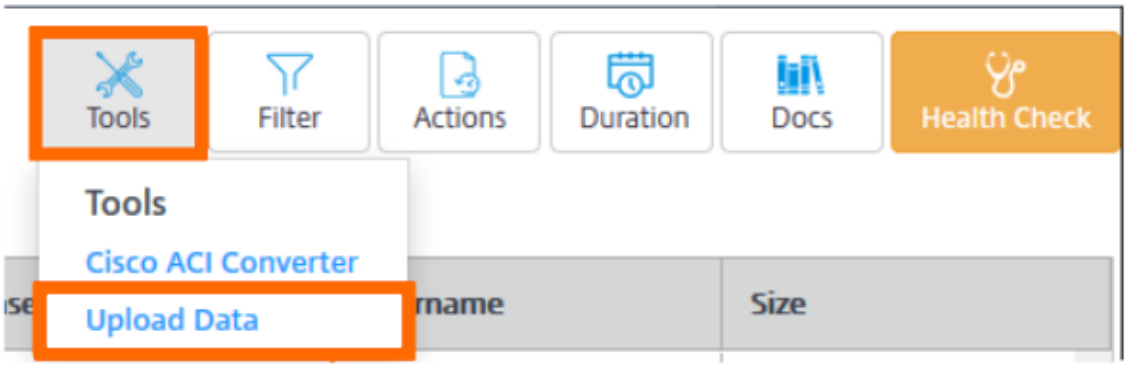


5. Führen Sie die Schritte 1 bis 5 auf jeder Cloud Connector-Maschine des Ressourcenstandorts aus und erstellen Sie eine ZIP-Datei aus allen Flush-Tracingdateien. Wenn Sie keine ZIP-Datei erstellen, müssen Sie alle Flush-Tracingdateien der Cloud Connector-Maschine einzeln an Citrix senden.

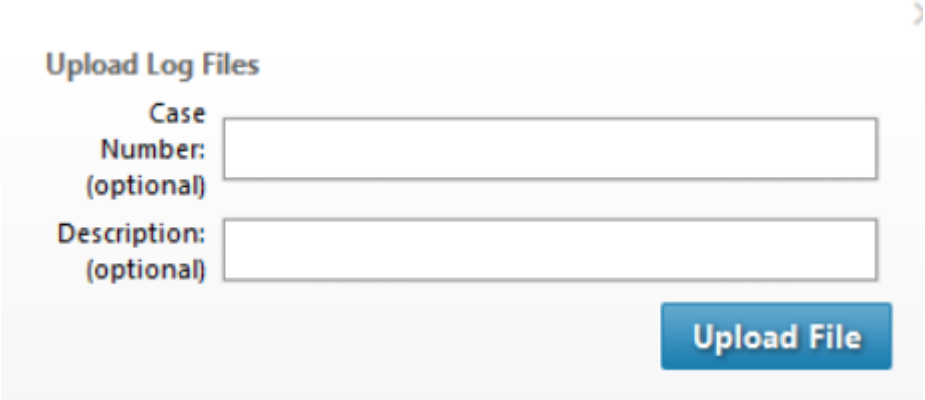
Schritt 3: Daten an Citrix senden

Fügen Sie die Tracingberichte an Ihren Citrix Supportfall an und reichen sie zur Überprüfung ein.

1. Melden Sie sich auf https://cis.citrix.com/ mit Ihren Citrix.com-Anmeldeinformationen an.
2. Wählen Sie **Diagnostics**.
3. Wählen Sie **Tools** und dann **Upload data**.



4. Geben Sie unter **Case Number**die Nummer des Citrix Supportfalls ein. Die Citrix Support-Mitarbeiter CDF-Tracingdateien nur prüfen, wenn dem Upload eine Supportfallnummer angefügt wird.



5. Im Feld **Description** können Sie optional eine kurze Beschreibung eingeben.
6. Wählen Sie **Upload File** und wählen Sie die zuvor erstellte ZIP-Datei aus. Wenn Sie keine ZIP-Datei der Flush-Tracingdateien aller Cloud Connector-Maschinen erstellt haben, wiederholen Sie die Schritte 3–6, um jede Tracingdatei einzeln anzufügen.

Nach dem Upload der Tracingdateien werden diese von Citrix Insight Services verarbeitet und an den von Ihnen angegebenen Supportfall anhängt. Dieser Vorgang kann je nach Größe der Dateien bis zu 24 Stunden dauern.

Primären Ressourcenstandort wählen

September 28, 2023

Wenn Ihre Domäne mehrere Ressourcenstandorte hat, können Sie einen Standort als "primären"oder "bevorzugten"Standort für Citrix Cloud auswählen. Der primäre Ressourcenstandort bietet die beste Leistung und Konnektivität zwischen Citrix Cloud und Ihrer Domäne, sodass Benutzer sich schnell anmelden können.

Wenn Sie einen primären Ressourcenstandort auswählen, werden die Cloud Connectors sofern möglich an diesem Ressourcenstandort für Benutzeranmeldungen und Provisioning verwendet. Wenn die Cloud Connectors im primären Ressourcenstandort nicht verfügbar sind, werden diese Vorgänge mit einem anderen Cloud Connector in der Domäne ausgeführt. Anmeldungen mit Benutzerprinzipalnamen (UPN) enthalten möglicherweise nicht den Domänennamen und verwenden möglicherweise nicht den primären Ressourcenstandort.

> **Hinweis:**
>
> Installieren Sie mindestens zwei Cloud Connectors an jedem Ressourcenstandort, um sicherzustellen, dass Cloud Connectors stets an jedem Ressourcenstandort verfügbar sind.

Beachten Sie Folgendes bei der Entscheidung, welcher Ressourcenstandort primärer Ressourcenstandort sein soll:

- Hat der Ressourcenstandort die beste Konnektivität zu Ihrer Domäne?
- Ist der Ressourcenstandort der geografischen Region am nächsten, in der Sie die Citrix Cloud-Verwaltungskonsole verwenden? Wenn Ihre Citrix Cloud-Konsole beispielsweise auf https://us.cloud.com ist, wählen Sie den Ressourcenstandort, der am nächsten zur Region USA ist.

Wählen eines primären Ressourcenstandorts

1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf die Menüschaltfläche und wählen Sie **Identitäts- und Zugriffsverwaltung**.
2. Klicken Sie auf **Domänen** und erweitern Sie die Domäne mit dem Ressourcenstandort, den Sie verwenden möchten.
3. Klicken Sie auf **Primären Ressourcenstandort festlegen** und wählen Sie dann den Ressourcenstandort, den Sie als primär festlegen möchten.
4. Klicken Sie auf **Speichern**. Citrix Cloud zeigt "Primär"neben dem ausgewählten Ressourcenstandort an.

> **Hinweis:**
>
> Speichern Sie Ihre Domänenauswahl, bevor Sie eine andere Domäne erweitern. Wenn Sie eine Domäne erweitern und dann eine andere Domäne erweitern, wird die zuerst erweiterte Domäne zugeklappt und alle nicht gespeicherten Änderungen gehen verloren.

Wählen eines anderen primären Ressourcenstandorts

1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf die Menüschaltfläche und wählen Sie **Identitäts- und Zugriffsverwaltung**.
2. Klicken Sie auf **Domänen** und erweitern Sie die Domäne mit dem Ressourcenstandort, den Sie verwenden möchten.
3. Klicken Sie auf **Primären Ressourcenstandort ändern** und wählen Sie den Ressourcenstandort, den Sie verwenden möchten.
4. Klicken Sie auf **Speichern**.

Zurücksetzen eines primären Ressourcenstandorts

Durch das Zurücksetzen des primären Ressourcenstandorts können Sie die Kennzeichnung "Primär" von einem Ressourcenstandort entfernen, ohne einen anderen auszuwählen. Wenn Sie die Kennzeichnung "Primär"entfernen, können alle Cloud Connectors in der Domäne Anmeldevorgänge für Benutzer ausführen. Daher kann es bei einigen Benutzern zu langsameren Anmeldungen kommen.

1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf die Menüschaltfläche und wählen Sie **Identitäts- und Zugriffsverwaltung**.
2. Wählen Sie **Domänen** und erweitern Sie dann die Domäne mit dem Ressourcenstandort, den Sie verwenden möchten.
3. Wählen Sie **Primären Ressourcenstandort ändern** und anschließend **Zurücksetzen**. Es wird eine Warnung angezeigt, dass die Anmeldeleistung beeinträchtigt werden könnte.
4. Wählen Sie **Ich verstehe die potenziellen Auswirkungen auf Abonnenten** und klicken Sie dann auf **Zurücksetzen bestätigen**.

Connector Appliance für Cloudservices

April 5, 2024

Die Connector Appliance ist eine Citrix-Komponente, die in Ihrem Hypervisor gehostet wird. Es dient als Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten und ermöglicht die

Cloudverwaltung ohne komplexe Netzwerk- oder Infrastrukturkonfiguration. Mit der Connector Appliance können Sie sich ganz auf die Ressourcen konzentrieren, die Ihren Benutzern einen Mehrwert bieten.

Die Connector Appliance bietet folgende Funktionen:

- **Das Verbinden von Active Directory mit Citrix Cloud** ermöglicht die Active Directory-Verwaltung und die Verwendung von Active Directory-Gesamtstrukturen und -Domänen an Ihren Ressourcenstandorten. Dadurch müssen keine zusätzlichen AD-Vertrauensstellungen hinzugefügt werden. Weitere Informationen finden Sie unter Active Directory mit Connector Appliance.
- Mit dem **Image Portability Service** können Sie Images einfacher plattformübergreifend verwalten. Das Feature erleichtert das Verwalten von Images zwischen einem On-Premises-Ressourcenstandort und einem Standort in einer öffentlichen Cloud. REST-APIs für Citrix Virtual Apps and Desktops ermöglichen die automatisierte Verwaltung von Ressourcen innerhalb einer Citrix Virtual Apps and Desktops-Site.

  Der Image Portability-Workflow setzt ein, wenn Sie mit Citrix Cloud die Migration eines Images vom On-Premises-Standort zur abonnierten öffentlichen Cloud initiieren. Nachdem Sie das Image vorbereitet haben, können Sie es mit Image Portability Service in die abonnierte öffentliche Cloud übertragen und zum Ausführen vorbereiten. Zum Schluss stellen Sie das Image mit Citrix Provisioning oder den Maschinenerstellungsdiensten in Ihrer abonnierten öffentlichen Cloud bereit.

  Weitere Informationen finden Sie unter Image Portability Service.
- Mit **Citrix Secure Private Access** können Administratoren eine einheitliche Benutzeroberfläche bereitstellen, die Single Sign-On, Remotezugriff und Inhaltsinspektion in einer Lösung integriert und eine umfassende Zugriffssteuerung gewährleistet. Weitere Informationen finden Sie unter Secure Private Access mit Connector Appliance.

Möglicherweise gibt es als Preview weitere Services, die auch von der Connector Appliance abhängen.

Die Connector Appliance-Plattform ist Teil der Citrix Cloud-Platform und der Citrix-Identitätsplattform. Sie ermöglicht die Datenverarbeitung, einschließlich der folgenden Informationen:

- IP-Adressen oder FQDNs
- Geräte-, Benutzer- und Ressourcenstandort-IDs
- Zeitstempel
- Ereignisdaten
- Benutzer- und Gruppendetails aus Active Directory (z. B. zur Authentifizierung und zur Suche nach Benutzern und Gruppen)

Details zu den von der Connector Appliance verarbeiteten Informationen finden Sie im Dokument Citrix Cloud Services Data Protection Overview in der Tabelle *Data Collected by Citrix Cloud Platform*.

Connector Appliance-Verfügbarkeit und Lastverwaltung

Installieren Sie an jedem Ressourcenstandort mehrere Connector Appliances, um Lastausgleich und kontinuierliche Verfügbarkeit zu gewährleisten. Citrix empfiehlt die Installation von mindestens zwei Connector Appliances an jedem Ressourcenstandort. Wenn eine Connector Appliance ausfällt, können die anderen die Verbindung aufrechterhalten. Da die Connector Appliances zustandslos sind, kann die Last auf alle verfügbaren Connector Appliances verteilt werden. Der Lastausgleich muss nicht konfiguriert werden. Er ist automatisiert. Wenn mindestens eine Connector Appliance verfügbar ist, wird die Kommunikation mit Citrix Cloud nicht unterbrochen.

Wenn nur ein Connector für einen Ressourcenstandort konfiguriert ist, zeigt Citrix Cloud auf den Seiten **Ressourcenstandorte** und **Connectors** einen Warnhinweis an.

Connector Appliance-Updates

Die Connector Appliance wird automatisch aktualisiert. Sie müssen keine Aktionen ausführen, um den Connector zu aktualisieren.

Sie können Ihren Ressourcenstandort so konfigurieren, dass Updates entweder sofort bei Verfügbarkeit oder in einem bestimmten Wartungsfenster angewendet werden.

Weitere Informationen zum Konfigurieren von Updates finden Sie unter Connector-Updates.

Während des Updates ist die Connector Appliance vorübergehend nicht verfügbar. Updates werden jeweils nur auf eine Connector Appliance an einem Ressourcenstandort angewendet. Registrieren Sie daher an jedem Ressourcenstandort mindestens zwei Connector Appliances, damit zu jeder Zeit mindestens eine verfügbar ist.

Kommunikation der Connector Appliance

Die Connector Appliance authentifiziert und verschlüsselt die gesamte Kommunikation zwischen Citrix Cloud und Ihren Ressourcenstandorten. Nach der Installation initiiert die Connector Appliance die Kommunikation mit Citrix Cloud über eine ausgehende Verbindung. Alle Verbindungen werden von der Connector Appliance zur Cloud über den HTTPS-Standardport (443) und per TCP-Protokoll hergestellt. Es sind keine eingehenden Verbindungen zugelassen.

In der folgenden Tabelle sind die Ports aufgeführt, auf die die Connector Appliance Zugriff benötigt:

Service	Port	Unterstütztes Domänenprotokoll	Konfigurationsdetails
DNS	53	TCP/UDP	Dieser Port muss für das lokale Setup offen sein.
NTP	123	UDP	Dieser Port muss für das lokale Setup offen sein.
HTTPS	443	TCP	Für die Connector Appliance ist ausgehender Zugriff auf diesen Port erforderlich.

Zum Konfigurieren der Connector Appliance müssen IT-Administratoren auf Port 443 (HTTPS) der Connector Appliance zugreifen können.

> **Hinweis:**
>
> Sie müssen u. U. `https://` am Anfang der IP-Adresse angeben.

Die Connector Appliance kann sowohl mit On-Premises-Systemen am Ressourcenstandort als auch mit externen Systemen kommunizieren. Wenn Sie bei der Registrierung der Connector Appliance einen oder mehrere Webproxys definieren, wird nur der Datenverkehr von der Connector Appliance zu externen Systemen über diesen Webproxy geleitet. Wenn sich Ihr On-Premises-System in einem privaten Adressraum befindet, wird der Datenverkehr von der Connector Appliance zu diesem System nicht über den Webproxy geleitet.

Die Connector Appliance definiert private Adressräume als folgende IPv4-Adressbereiche:

- 10.0.0.0 –10.255.255.255
- 172.16.0.0 –172.31.255.255
- 192.168.0.0 –192.168.255.255

Anforderungen an die Internetkonnektivität

Um Ihre Datencenter mit dem Internet zu verbinden, muss Port 443 für ausgehende Verbindungen geöffnet sein. Für Umgebungen mit Internetproxyserver oder Firewall sind jedoch u. U. weitere Konfigurationsschritte erforderlich.

Die folgenden Adressen müssen mit unveränderten HTTPS-Verbindungen kontaktierbar sein, damit die Citrix Cloud Services ordnungsgemäß ausgeführt und in Anspruch genommen werden können:

- https://*.cloud.com
- https://*.citrixworkspacesapi.net
- https://*.citrixnetworkapi.net
- https://*.nssvc.net
  - Kunden, die nicht alle Unterdomänen aktivieren können, können stattdessen die folgenden Adressen verwenden:
    * https://*.g.nssvc.net
    * https://*.c.nssvc.net
- https://*.servicebus.windows.net
- https://iwsprodeastusuniconacr.azurecr.io
- https://iwsprodeastusuniconacr.eastus.data.azurecr.io

Netzwerkanforderungen

Stellen Sie sicher, dass Ihre Umgebung die folgende Konfiguration bietet:

- Entweder, das Netzwerk lässt zu, das die Connector Appliance über DHCP DNS- und NTP-Server, eine IP-Adresse, einen Hostnamen und einen Domänennamen abruft, oder Sie legen die Netzwerkeinstellungen manuell in der Connector Appliance-Konsole fest.
- Das Netzwerk ist nicht für die Verwendung der Link-Local-IP-Bereiche 169.254.0.1/24, 169.254.64.0/18 oder 169.254.192.0/18 konfiguriert, die intern von der Connector Appliance verwendet werden.
- Entweder ist die Hypervisor-Uhr auf koordinierte Weltzeit (UTC) eingestellt und mit einem Zeitserver synchronisiert oder die Connector Appliance erhält NTP-Serverinformationen über DHCP.
- Wenn Sie einen Proxy mit der Connector Appliance verwenden, darf der Proxy nicht authentifiziert sein oder er muss die Standardauthentifizierung verwenden.

Systemanforderungen

Die Connector Appliance wird auf den folgenden Hypervisoren unterstützt:

- Citrix Hypervisor 8.2 CU1 LTSR
- VMware ESXi Version 7 Update 2
- Hyper-V unter Windows Server 2016, Windows Server 2019 oder Windows Server 2022.
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform

Ihr Hypervisor muss die folgenden Mindestfunktionen bereitstellen:

- 20 GB Stammdatenträger
- 2 vCPUs
- 4 GB RAM
- Ein IPv4-Netzwerk

Sie können mehrere Connector Appliances auf demselben Hypervisorhost hosten. Die Anzahl der Connector Appliances auf einem Host wird nur durch die Hypervisor- und Hardwarebeschränkungen begrenzt.

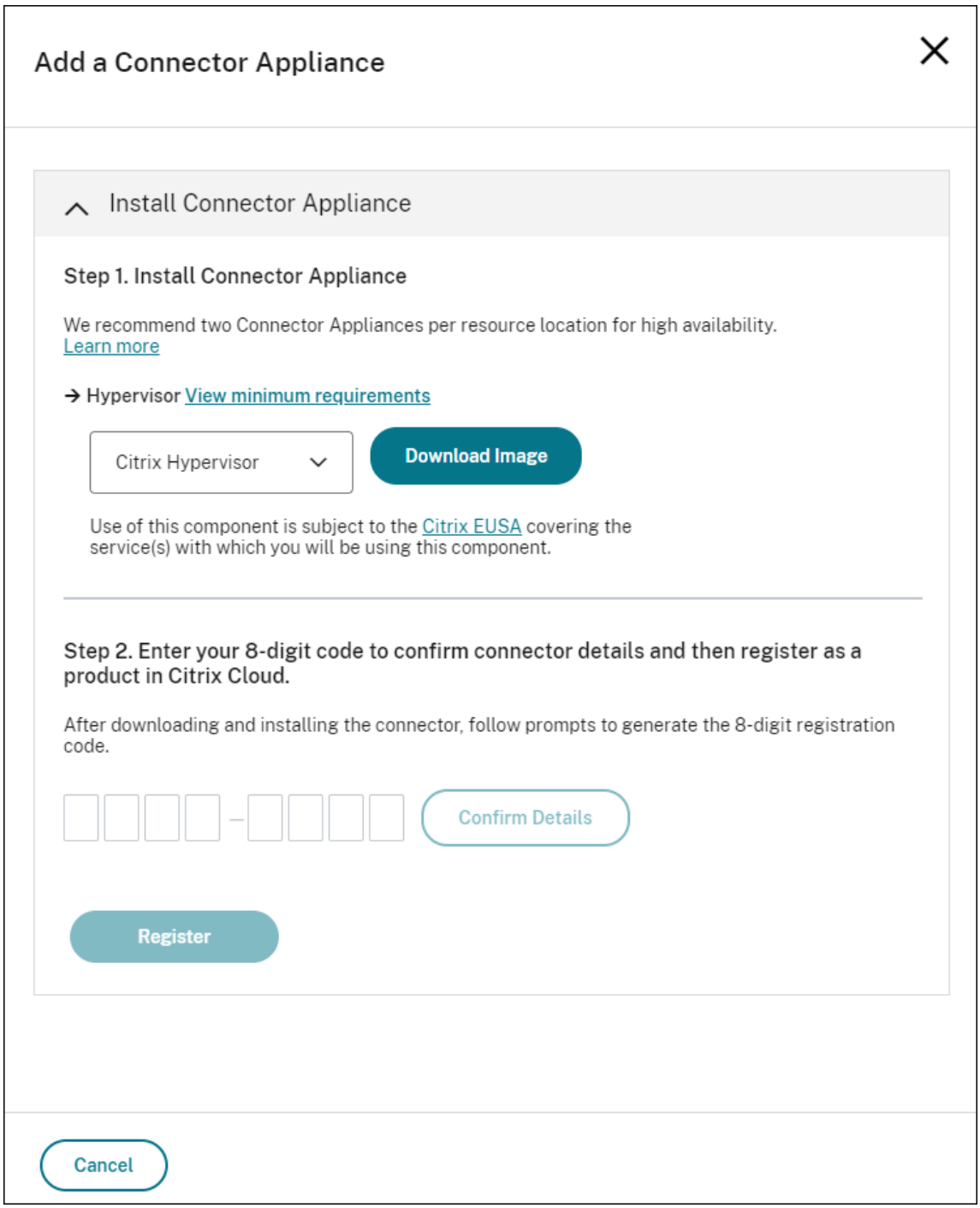
> **Hinweis:**
>
> Das Klonen, Anhalten und Erstellen von Snapshots der Connector Appliance-VM werden nicht unterstützt.

Connector Appliance anfordern

Laden Sie die Connector Appliance-Software von Citrix Cloud herunter.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links die Option **Ressourcenstandorte** aus.
3. Wenn Sie noch keinen Ressourcenstandort haben, klicken Sie auf das Pluszeichen (+) oder wählen Sie **Ressourcenstandort hinzufügen**.
4. Klicken Sie am Ressourcenstandort, an dem Sie die Connector Appliance registrieren möchten, auf das Pluszeichen (+) für **Connector Appliances**.

   Die Aufgabe **Connector Appliance hinzufügen** wird geöffnet.



5. Wählen Sie in der Liste **Hypervisor** in **Schritt 1** den Typ des Hypervisors oder Cloudanbieters aus, den Sie zum Hosten der Connector Appliance verwenden möchten.

   - Für On-Premises-Hypervisoren und Cloudumgebungen können Sie die Connector Appliance in Citrix Cloud herunterladen:

     a) Klicken Sie auf **Image herunterladen**.

b) Überprüfen Sie den Citrix Endbenutzerservicevertrag und wählen Sie, wenn Sie zustimmen, **Zustimmen und fortfahren**aus.

c) Wenn Sie dazu aufgefordert werden, speichern Sie die bereitgestellte Connector Appliance-Datei.

Die Dateinamenerweiterung der Connector Appliance-Datei hängt vom ausgewählten Hypervisor ab.

- Für einige Cloudumgebungen können Sie die Connector Appliance auch über den Marketplace erhalten:
  - AWS
  - Microsoft Azure
  - Google Cloud

6. Lassen Sie die Aufgabe **Connector Appliance installieren** geöffnet. Nach der Installation der Connector Appliance geben Sie in **Schritt 2** Ihren Registrierungscode ein.

Sie können die Aufgabe **Connector Appliance installieren** auch über die Seite **Connectors** aufrufen. Wählen Sie das Pluszeichen (+), um einen Connector hinzuzufügen, und fügen Sie eine Connector Appliance hinzu.

Connector Appliance auf dem Hypervisor installieren

- Citrix Hypervisor
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google Cloud Platform
- AWS

Citrix Hypervisor

In diesem Abschnitt wird beschrieben, wie Sie die Connector Appliance mit XenCenter auf einem Citrix Hypervisor-Server importieren.

1. Stellen Sie eine Verbindung zum Citrix Hypervisor-Server oder -Pool her, indem Sie XenCenter auf einem System verwenden, das Zugriff auf die heruntergeladene XVA-Datei mit der Connector Appliance hat.
2. Wählen Sie **Datei** > **Importieren** .

3. Geben Sie den Pfad an (oder gehen Sie zum Verzeichnis), wo sich die XVA-Datei mit der Connector Appliance befindet. Klicken Sie auf **Weiter**.
4. Wählen Sie den Citrix Hypervisor-Server aus, auf dem Sie die Connector Appliance hosten möchten. Alternativ können Sie auch den Pool auswählen, in dem die Connector Appliance gehostet werden soll. Citrix Hypervisor wählt dann einen geeigneten verfügbaren Server aus. Klicken Sie auf **Weiter**.
5. Geben Sie das Speicherrepository an, das für die Connector Appliance verwendet werden soll. Klicken Sie auf **Importieren**.
6. Klicken Sie auf **Hinzufügen**, um eine virtuelle Netzwerkschnittstelle hinzuzufügen. Wählen Sie in der Liste **Netzwerk** das Netzwerk aus, das von der Connector Appliance verwendet werden soll. Klicken Sie auf **Weiter**.
7. Überprüfen Sie die Optionen, die zum Bereitstellen der Connector Appliance verwendet werden sollen. Wählen Sie **Zurück**, falls die Optionen geändert werden müssen.
8. Stellen Sie sicher, dass die Option **Start the new VM(s) automatically as soon as the import is complete** aktiviert ist. Klicken Sie auf **Fertig stellen**.

Nach dem erfolgreichen Bereitstellen und Start der Connector Appliance wird in der Konsole die Startseite mit der IP-Adresse der Connector Appliance angezeigt. Verwenden Sie diese IP-Adresse, um eine Verbindung mit der Connector Appliance-Verwaltungsseite herzustellen und die Registrierung abzuschließen.

Standardmäßig verwendet die Connector Appliance DHCP zum Festlegen der Netzwerkkonfiguration. Wenn DHCP in Ihrer Umgebung nicht verfügbar ist, müssen Sie die Netzwerkkonfiguration in der Konsole der Connector Appliance festlegen, bevor Sie auf die Verwaltungskonsole der Connector Appliance zugreifen können. Weitere Informationen finden Sie unter Netzwerkkonfiguration über die Connector Appliance-Konsole festlegen.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

VMware ESXi

In diesem Abschnitt wird beschrieben, wie Sie die Connector Appliance auf einem VMware ESXi-Host mit dem VMware vSphere-Client bereitstellen.

1. Stellen Sie eine Verbindung zum ESXi-Host her, indem Sie den vSphere-Client auf einem System verwenden, das Zugriff auf die heruntergeladene OVA-Datei mit der Connector Appliance hat.
2. Wählen Sie **Datei** > **OVF-Vorlage bereitstellen…**.
3. Geben Sie den Pfad an (oder gehen Sie zum Verzeichnis), an dem die OVA-Datei mit der Connector Appliance ist. Klicken Sie auf **Weiter**.
4. Überprüfen Sie die Vorlagendetails. Klicken Sie auf **Weiter**.
5. Sie können einen eindeutigen Namen für die Connector Appliance-Instanz angeben. Standardmäßig ist der Name auf **Connector Appliance** festgelegt. Wählen Sie einen Namen, der diese

Instanz der Connector Appliance von anderen Instanzen auf dem ESXi-Host unterscheidet. Klicken Sie auf **Weiter**.

6. Geben Sie den Zielspeicher an, der für die Connector Appliance verwendet werden soll. Klicken Sie auf **Weiter**.
7. Wählen Sie das Format aus, in dem die virtuellen Datenträger gespeichert werden sollen. Klicken Sie auf **Weiter**.
8. Überprüfen Sie die Optionen, die zum Bereitstellen der Connector Appliance verwendet werden sollen. Wählen Sie **Zurück**, falls die Optionen geändert werden müssen.
9. Wählen Sie **Nach Bereitstellung einschalten**. Klicken Sie auf **Fertig stellen**.

Nach dem erfolgreichen Bereitstellen und Start der Connector Appliance wird in der Konsole die Startseite mit der IP-Adresse der Connector Appliance angezeigt. Verwenden Sie diese IP-Adresse, um eine Verbindung mit der Connector Appliance-Verwaltungsseite herzustellen und die Registrierung abzuschließen.

Standardmäßig verwendet die Connector Appliance DHCP zum Festlegen der Netzwerkkonfiguration. Wenn DHCP in Ihrer Umgebung nicht verfügbar ist, müssen Sie die Netzwerkkonfiguration in der Konsole der Connector Appliance festlegen, bevor Sie auf die Benutzeroberfläche der Connector Appliance zugreifen können. Weitere Informationen finden Sie unter Netzwerkkonfiguration über die Connector Appliance-Konsole festlegen.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Hyper-V

In diesem Abschnitt wird beschrieben, wie die Connector Appliance auf einem Hyper-V-Host bereitgestellt wird. Sie können die VM mit Hyper-V-Manager oder mit dem enthaltenen PowerShell-Skript bereitstellen.

Connector Appliance über Hyper-V-Manager bereitstellen

1. Stellen Sie eine Verbindung zum Hyper-V-Host her.
2. Kopieren Sie die Connector Appliance-ZIP-Datei auf den Hyper-V-Host oder laden Sie sie herunter.
3. Extrahieren Sie den Inhalt der ZIP-Datei. Die ZIP-Datei enthält ein PowerShell-Skript und die Datei connector-appliance.vhdx.
4. Kopieren Sie die VHDX-Datei an die Stelle, an der Sie Ihre VM-Datenträger aufbewahren möchten. Beispiel: `C:\ConnectorApplianceVMs`.
5. Öffnen Sie den Hyper-V-Manager.

6. Klicken Sie mit der rechten Maustaste auf den Servernamen und wählen Sie **Neu > Virtuelle Maschine** aus.
7. Geben Sie im **Assistent für neue virtuelle Computer** im Bereich **Name und Speicherort angeben** einen eindeutigen Namen ein, der zur Identifizierung Ihrer Connector Appliance verwendet werden soll. Klicken Sie auf **Weiter**.
8. Wählen Sie im Bereich **Generation angeben** die Option **Generation 1** aus. Klicken Sie auf **Weiter**.
9. Konfigurieren Sie im Bereich **Speicher zuweisen** die folgenden Einstellungen und klicken Sie dann auf **Weiter**:

    a) Weisen Sie 4 GB RAM zu.
    b) Deaktivieren Sie den dynamischen Speicher.

10. Wählen Sie im Bereich **Netzwerk konfigurieren** einen Switch (Beispiel: Standardswitch) aus der Liste aus. Klicken Sie auf **Weiter**.
11. Wählen Sie im Bereich **Virtuelle Festplatte verbinden** die Option **Vorhandene virtuelle Festplatte verwenden** aus.
12. Gehen Sie zum Speicherort der Datei connector-appliance.vhdx und wählen Sie sie aus. Klicken Sie auf **Weiter**.
13. Überprüfen Sie im Bereich **Zusammenfassung** die ausgewählten Werte und klicken Sie auf **Fertig stellen**, um die VM zu erstellen.
14. Klicken Sie im Bereich **Virtuelle Computer** mit der rechten Maustaste auf die Connector Appliance-VM und wählen Sie **Einstellungen** aus.
15. Wählen Sie im Fenster **Einstellungen** die Option **Hardware > Prozessoren** und führen Sie die folgenden Schritte aus:

    a) Ändern Sie unter **Anzahl der virtuellen Prozessoren** den Wert auf **2**.
    b) Klicken Sie auf **Anwenden**.
    c) Klicken Sie auf **OK**.

16. Klicken Sie im Bereich **Virtuelle Computer** mit der rechten Maustaste auf die Connector Appliance-VM und wählen Sie **Starten** aus.
17. Klicken Sie mit der rechten Maustaste auf die Connector Appliance-VM und wählen Sie **Verbinden** aus, um die Konsole zu öffnen.

Nachdem die Connector Appliance bereitgestellt und erfolgreich gestartet wurde, stellen Sie mit Hyper-V-Manager eine Verbindung zur Konsole her. Die Konsole zeigt eine Startseite an, die die IP-Adresse der Connector Appliance enthält. Verwenden Sie diese IP-Adresse, um eine Verbindung mit der Connector Appliance-Verwaltungsseite herzustellen und die Registrierung abzuschließen.

Standardmäßig verwendet die Connector Appliance DHCP zum Festlegen der Netzwerkkonfiguration. Wenn DHCP in Ihrer Umgebung nicht verfügbar ist, müssen Sie die Netzwerkkonfiguration in der Konsole der Connector Appliance festlegen, bevor Sie auf die Benutzeroberfläche der Connector Appliance zugreifen können. Weitere Informationen finden Sie unter Netzwerkkonfiguration über die Connector Appliance-Konsole festlegen.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Connector Appliance über ein PowerShell-Skript bereitstellen Die Datei connector-appliance.zip enthält ein PowerShell-Skript, das eine neue VM erstellt und startet.

> **Hinweis:**
>
> Um dieses nicht signierte PowerShell-Skript auszuführen, müssen Sie möglicherweise die Ausführungsrichtlinien im Hyper-V-System ändern. Weitere Informationen finden Sie unter https://go.microsoft.com/fwlink/?LinkID=135170. Sie können auch das bereitgestellte Skript als Grundlage verwenden, um ein eigenes lokales Skript zu erstellen oder zu ändern.

1. Stellen Sie eine Verbindung zum Hyper-V-Host her.
2. Kopieren Sie die Connector Appliance-ZIP-Datei auf den Hyper-V-Host oder laden Sie sie herunter.
3. Extrahieren Sie den Inhalt der ZIP-Datei: ein PowerShell-Skript und eine VHDX-Datei.
4. Geben Sie in einer PowerShell-Konsole das aktuelle Verzeichnis an, in dem sich der Inhalt der ZIP-Datei befindet, und führen Sie den folgenden Befehl aus:

   ```
   .\connector-appliance-install.ps1
   <!--NeedCopy-->
   ```

5. Wenn Sie dazu aufgefordert werden, geben Sie einen Namen für Ihre VM ein, oder wählen Sie **Eingabe**, um den Standardwert **Connector Appliance** zu akzeptieren.
6. Wenn Sie dazu aufgefordert werden, geben Sie ein Ziel für den Stammdatenträger ein, oder drücken Sie die Eingabetaste, um das Systemstandardverzeichnis für VHDs zu verwenden.
7. Wenn Sie dazu aufgefordert werden, geben Sie einen Namen für den Stammdatenträger ein oder wählen Sie **Eingabe**, um den Standardwert “connector-appliance.zip”zu akzeptieren.
8. Wenn Sie dazu aufgefordert werden, wählen Sie den zu verwendenden Schalter aus. Wählen Sie **Eingabe**.
9. Überprüfen Sie die Zusammenfassung der VM-Importinformationen. Wenn die Informationen korrekt sind, wählen Sie **Eingabe**, um fortzufahren. Die Connector Appliance-VM wird vom Skript erstellt und gestartet.

Nach dem erfolgreichen Bereitstellen und Start der Connector Appliance wird in der Konsole die Startseite mit der IP-Adresse der Connector Appliance angezeigt. Verwenden Sie diese IP-Adresse, um eine Verbindung mit der Connector Appliance herzustellen und die Registrierung abzuschließen.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Nutanix AHV

In diesem Abschnitt wird beschrieben, wie Sie die Connector Appliance über die Nutanix Prism-Webkonsole aus der Datei `connector-appliance.vhdx` auf einem Nutanix AHV-Host bereitstellen.

1. Wählen Sie im Hauptmenü der Nutanix Prism-Webkonsole die Ansicht **Storage** aus.
2. Klicken Sie auf **+ Storage Container**, um einen Speichercontainer für die Imagedatei der Connector Appliance zu erstellen. Alternativ können Sie einen vorhandenen Storagecontainer verwenden.
3. Laden Sie die Datei `connector-appliance.vhdx` in Ihren Speichercontainer hoch.
    a) Wählen Sie im Hauptmenü der Webkonsole **Settings**.
    b) Wählen Sie die Registerkarte **Image Configuration** und klicken Sie auf **+ Upload Image**.
    c) Geben Sie unter **Create Image** einen **Namen** für das Image an.
    d) Wählen Sie in der Liste **Image Type** die Option **DISK**.
    e) Wählen Sie in der Liste **Storage Container** den von Ihnen erstellten Speichercontainer.
    f) Wählen Sie **Upload a file**.
    g) Klicken Sie auf **Choose file** und gehen Sie zu der Datei `connector-appliance.vhdx` auf Ihrem lokalen System.
    h) Klicken Sie auf **Speichern**.
4. Warten Sie, bis das Image erstellt ist und sein Status auf der Seite **Image Configuration** als **ACTIVE** angezeigt wird.
5. Wählen Sie die Registerkarte **Network Configuration**.
6. Klicken Sie auf **+ Create Network**, um ein Netzwerk für die Connector-Appliance zu erstellen.
7. Geben Sie auf der Seite **Create Network** die folgenden Informationen an:
    - Netzwerkname
    - Netzwerk-VLAN-ID
8. Wählen Sie im Hauptmenü der Webkonsole die Ansicht **VM** aus.
9. Klicken Sie auf **+ Create VM**, um eine Connector-Appliance-Instanz zu erstellen
10. Geben Sie unter **Create VM** die folgenden Informationen an:

- VM-Name
- Anzahl der vCPUs
- Speichergröße in GiB

11. Wählen Sie **Legacy BIOS**.
12. Klicken Sie auf **+ Add New Disk**, um der VM einen Datenträger hinzuzufügen.
13. Geben Sie unter **Add Disk** die folgenden Informationen an:

    a) Wählen Sie für **Type** die Option **DISK**.
    b) Wählen Sie für **Operation** die Option **Clone from Image Service**.
    c) Wählen Sie für **Bus Type** die Option **SCSI**.
    d) Wählen Sie für **Image** das Image, das Sie beim Hochladen der Connector Appliance-Datei erstellt haben.

14. Klicken Sie auf **Add**, um das Hinzufügen des Datenträgers abzuschließen.
15. Klicken Sie unter **Create VM** auf **+ Add New NIC**.
16. Wählen Sie unter **Create NIC** das Netzwerk aus, dem die VM hinzugefügt werden soll.
17. Wählen Sie für **Network Connection State** die Option **Connected**.
18. Klicken Sie auf **Add**, um das Hinzufügen der NIC abzuschließen.
19. Klicken Sie auf **Save**, um die VM zu erstellen.

    Standardmäßig sind neue VMs ausgeschaltet.

20. Wählen Sie in der Ansicht **VM** die VM und klicken Sie auf **Power on**.
21. Warten Sie, bis die VM gestartet ist. Dieser Vorgang kann mehrere Minuten dauern.

Wenn die Connector Appliance bereitgestellt und gestartet ist, finden Sie ihre IP-Adresse an folgenden Stellen:

- In der Ansicht **VM** der Nutanix Prism-Webkonsole.
- In der Connector Appliance-Konsole.

Verwenden Sie diese IP-Adresse, um eine Verbindung mit der Connector Appliance-Verwaltungsseite herzustellen und die Registrierung abzuschließen.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Microsoft Azure

In diesem Abschnitt wird beschrieben, wie die Connector Appliance in Microsoft Azure bereitgestellt wird. Sie können die Connector Appliance über Azure Marketplace bereitstellen oder über das heruntergeladene Datenträgerimage mit dem enthaltenen PowerShell-Skript.

Connector Appliance über Azure Marketplace bereitstellen Führen Sie die folgenden Schritte aus, um die Connector Appliance über Azure Marketplace bereitzustellen:

1. Rufen Sie die Connector Appliance in Azure Marketplace auf. (Azure Marketplace)

   Alternativ können Sie im Suchfeld von Marketplace auch "Connector Appliance für Cloud-Dienste"eingeben.

2. Klicken Sie auf **Get It Now** und dann auf **Create**.

3. Füllen Sie auf der Seite **Create Citrix Connector Appliance for Cloud Services** die folgenden Informationen aus:

   - Wählen Sie unter **Subscription** ein Abonnement.
   - Wählen Sie unter **Resource group** eine Ressourcengruppe.
   - Wählen Sie eine **Region** für die Connector Appliance.
   - Geben Sie unter **VM Name** einen Namen ein.
   - Wählen Sie unter **Virtual network** ein Netzwerk, dem die Connector Appliance hinzugefügt werden soll. Dieses Netzwerk dient dann zum Zugriff auf Citrix Cloud, die lokalen Ressourcen und die Connector Appliance-Verwaltungsseite. Das Netzwerk kann nicht nachträglich geändert werden.
   - Geben Sie einen Wert für **Subnet** ein.

   Klicken Sie auf **Next : Tags >**.

4. Fügen Sie bei Bedarf auf der Registerkarte **Tags** erforderliche Tags hinzu.

   Klicken Sie auf **Next : Review + create >**.

5. Prüfen Sie die Bereitstellungsdetails und klicken Sie auf **Create**.

Nach dem erfolgreichen Bereitstellen und Start der Connector Appliance wird in der Konsole die Startseite mit der IP-Adresse der Connector Appliance angezeigt. Verwenden Sie diese IP-Adresse, um eine Verbindung mit der Connector Appliance-Verwaltungsseite herzustellen und die Registrierung abzuschließen.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Connector Appliance-VM über PowerShell-Skript bereitstellen Die Datei `connector-appliance-azure.zip` enthält ein PowerShell-Skript, das eine neue VM erstellt und startet. Sie können das enthaltene Skript als Grundlage verwenden, um ein eigenes lokales Skript zu erstellen oder zu ändern.

Vor der Ausführung des Skripts müssen Sie die folgenden Voraussetzungen erfüllen:

- Installieren Sie das Az PowerShell-Modul in Ihrer lokalen PowerShell-Umgebung.
- Führen Sie das PowerShell-Skript im Verzeichnis aus, in dem sich die VHD-Datei befindet.

Führen Sie hierzu die folgenden Schritte aus:

1. Kopieren oder laden Sie die ZIP-Datei der Connector Appliance in Ihr Windows-System.
2. Extrahieren Sie den Inhalt der ZIP-Datei: ein PowerShell-Skript und eine VHD-Datei.
3. Öffnen Sie die PowerShell-Konsole als Administrator.
4. Geben Sie das Verzeichnis an, in dem sich der Inhalt der ZIP-Datei befindet, und führen Sie den folgenden Befehl aus:

   ```
   .\connector-appliance-upload-Azure.ps1
   ```

5. Sie werden dann in einem Dialogfeld aufgefordert, sich bei Microsoft Azure anzumelden. Geben Sie Ihre Anmeldeinformationen ein.
6. Wenn Sie vom PowerShell-Skript dazu aufgefordert werden, wählen Sie das zu verwendende Abonnement aus. Drücken Sie die Eingabetaste.
7. Folgen Sie den Anweisungen im Skript zum Image-Upload und zum Erstellen einer virtuellen Maschine.
8. Nach dem Erstellen der ersten VM werden Sie gefragt, ob Sie eine weitere VM aus dem hochgeladenen Image erstellen möchten.

   - Geben Sie `y` ein, um eine weitere VM zu erstellen.
   - Geben Sie `n` ein, um das Skript zu beenden.

Nach dem erfolgreichen Bereitstellen und Start der Connector Appliance wird in der Konsole die Startseite mit der IP-Adresse der Connector Appliance angezeigt. Verwenden Sie diese IP-Adresse, um eine Verbindung mit der Connector Appliance-Verwaltungsseite herzustellen und die Registrierung abzuschließen.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

AWS

In diesem Abschnitt wird beschrieben, wie die Connector Appliance in AWS bereitgestellt wird. Die Connector Appliance ist als AMI im AWS Marketplace verfügbar und es wird empfohlen, die Connector Appliance aus dem AMI zu installieren. Alternativ können Sie ein heruntergeladenes Datenträgerimage mit der AWS-Benutzeroberfläche oder dem enthaltenen PowerShell-Skript bereitstellen.

Voraussetzungen für das Netzwerk Zum Bereitstellen der Connector Appliance in AWS stellen Sie sicher, dass Sie über das Subnetz, in dem die Connector Appliance erstellt wurde, auf Citrix Cloud zugreifen können.

Wir empfehlen die Verwendung einer privaten IP-Adresse für die Appliance, was eine bestimmte Konfiguration für den Zugriff auf Citrix Cloud erfordert. Führen Sie für diese Konfiguration die folgenden Schritte in der **AWS-Managementkonsole** aus:

1. Erstellen Sie das NAT-Gateway.
    a) Wählen Sie in der oberen Navigationsleiste **Services > VPC > NAT Gateways**.
    b) Klicken Sie rechts oben auf **Create NAT Gateway**. Geben Sie die folgenden Informationen ein:
        - Geben Sie den **Namen** ein.
        - Wählen Sie das **Subnetz** aus.
        - Legen Sie für **Connectivity type** die Option **Public** fest.
        - Wählen Sie in der Liste **Elastic IP allocation ID** einen Eintrag. Wenn keine Elastic IP verfügbar ist, klicken Sie auf **Allocate Elastic IP** und folgen Sie den Anweisungen zum Erstellen.
    c) Klicken Sie auf **Create NAT Gateway**.
2. Erstellen Sie einen Routingtabelleneintrag mit dem NAT-Gateway.
    a) Wählen Sie in der oberen Navigationsleiste **Services > VPC > Route Tables**.
    b) Klicken Sie rechts oben auf **Create route table**. Geben Sie die folgenden Informationen ein:
        - Geben Sie den **Namen** ein.
        - Wählen Sie in der Liste die VPC mit dem Subnetz, das Sie beim Erstellen des NAT-Gateways ausgewählt haben.
    c) Klicken Sie auf **Create route table**.
    d) Klicken Sie in der Registerkarte **Routes** der erstellten Routingtabelle auf **Edit routes > Add route**.
    e) Machen Sie Angaben für **Destination** und **Target**.
        - Wählen Sie für "Destination"0.0.0.0/0.
        - Wählen Sie für "Target"das von Ihnen erstellte **NAT-Gateway**.
    f) Klicken Sie auf **Save change**.
3. Fügen Sie das für die Connector Appliance zu verwendende Subnetz an diese Routingtabelle an.
    a) Wählen Sie in der oberen Navigationsleiste **Services > VPC > Route Tables**.
    b) Wählen Sie die Routentabelle aus, die das NAT-Gateway enthält.

c) Wechseln Sie zur Registerkarte **Subnet Associations**.
d) Klicken Sie auf **Edit subnet associations**.
e) Wählen Sie das Subnetz oder die Subnetze aus, die an die Routentabelle angefügt werden sollen.
f) Klicken Sie auf **Save Associations**.

Connector Appliance aus AWS Marketplace bereitstellen Sorgen Sie zunächst dafür, dass folgende Voraussetzungen erfüllt sind:

- Sie haben Berechtigungen zum Betrieb von EC2-Ressourcen.
- Sie haben die Konfiguration unter Netzwerkvoraussetzungen ausgeführt.
- (Optional) Sie können eine Sicherheitsgruppe erstellen, um einzuschränken, welche IP-Adressen auf Ihre Connector Appliance zugreifen dürfen.

Führen Sie hierzu die folgenden Schritte aus:

1. Melden Sie sich bei der **AWS-Managementkonsole** an.
2. Suchen Sie die Connector Appliance-AMI im AWS Marketplace. Dazu gibt es mehrere Methoden:
   - Verwenden Sie den in Citrix Cloud bereitstellten Link zum Marketplace. (AWS Marketplace)
   - Suchen Sie in der AWS Management Console nach dem AMI:
     a) Gehen Sie zu **Services > Compute > EC2 > AMIs**.
     b) Stellen Sie sicher, dass Sie in der Region "US East (Ohio)"sind.
     c) Suchen Sie in **Public images** nach "Citrix Connector Appliance"oder nach der AMI-ID "ami-026eaf9b3b232577f".
3. Überprüfen Sie die AMI-ID (ami-026eaf9b3b232577f) und die Besitzer-ID (414337923189), um sicherzustellen, dass Sie das richtige AMI verwenden.
4. Kopieren Sie das AMI in Ihr Abonnement:
   a) Gehen Sie zu **Actions > Copy AMI**.
   b) Im Dialogfeld **Copy AMI** können Sie unter **Destination Region** die gewünschte Zielregion auswählen.
   c) Klicken Sie auf **Copy AMI**.
5. Klicken Sie auf der kopierten AMI-Zusammenfassungsseite auf **Launch instance from AMI**.
6. Führen Sie im Dialogfeld **Launch an instance** die folgenden Schritte aus:
   a) Wählen Sie die Anzahl der zu erstellenden Instanzen. Aus Resilienzgründen empfehlen wir, an jedem Ressourcenstandort mindestens zwei Connector Appliances zu haben.

b) Geben Sie einen Namen für die Instanz an.
c) Wählen Sie unter **Instance type** die Option **t2.medium**. Der Instanztyp muss mindestens 4 GB und 2 CPUs haben.
d) Wählen Sie für **Key pair (login)** die Option **Proceed without a key pair**. Eine SSH-Anmeldung bei der Connector Appliance ist nicht zulässig, daher ist kein Schlüsselpaar erforderlich.
e) Konfigurieren Sie unter **Network settings** im Abschnitt **Firewall (security group)** die folgenden Einstellungen:
   i. Wählen Sie aus, ob Sie **Create security group** oder **Select existing security group** verwenden möchten.
   ii. Deaktivieren Sie **Allow SSH traffic from the internet**.
   iii. Wählen Sie **Allow HTTPs traffic from the internet**.
   iv. Wählen Sie **Allow HTTP traffic from the internet**.

Klicken Sie auf **Launch Instance**.

7. Nachdem die Instanz erstellt ist, klicken Sie im Abschnitt **Success** auf den Link der Instanz-ID, um die Instanz Ihrer Connector Appliance anzuzeigen.

   Alternativ können Sie auf dieser Seite auf die Schaltfläche **View all Instances** klicken oder in der AWS Management Console unter **Services > EC2 > Instances** eine Liste Ihrer Instanzen anzeigen.

8. Wenn der Instanzstatus unter **Instance state** als **Running** angezeigt wird, gehen Sie zu den Instanzdetails und verwenden **Private IPv4 address**, um sich mit der Connector Appliance-Verwaltungsseite zu verbinden und den Registrierungsvorgang fortzusetzen.

Sie benötigen evtl. einen Bastionshost, um aus dem Browser die Connector Appliance-Verwaltungsseite unter der internen IP-Adresse aufzurufen und die Registrierung abzuschließen.

Standardmäßig verwendet die Connector Appliance DHCP zum Festlegen der Netzwerkkonfiguration. Sie können diese Netzwerkkonfiguration über die Connector Appliance-Weboberfläche bearbeiten. Weitere Informationen finden Sie unter Netzwerkeinstellungen auf der Connector Appliance-Verwaltungsseite konfigurieren.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Connector Appliance über die AWS-Benutzeroberfläche bereitstellen Sorgen Sie zunächst dafür, dass folgende Voraussetzungen erfüllt sind:

- Sie haben Berechtigungen zum Betrieb von S3- und EC2-Ressourcen.
- Sie haben eine Dienstrolle und eine Richtlinie mit VM-Importzugriff erstellt. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

> **Hinweis:**
>
> Um eine Dienstrolle zu erstellen, müssen Sie einen S3-Bucket erstellen. Legen Sie beim Erstellen der Richtlinie das S3-Bucket fest, das Sie mit VM-Importzugriff erstellt haben.

- Sie haben Zugriff auf AWS CloudShell. Das Tool ist nur in bestimmten Regionen verfügbar. Eine Liste der Regionen, in denen AWS CloudShell unterstützt wird, finden Sie unter https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html.
- Sie haben die Konfiguration unter Netzwerkvoraussetzungen ausgeführt.

Führen Sie hierzu die folgenden Schritte aus:

1. Extrahieren Sie den Inhalt von `connector-appliance-aws.zip` auf dem lokalen System.
2. Melden Sie sich bei der **AWS-Managementkonsole** an.
3. Erstellen Sie ein Speicher-Bucket, indem Sie die folgenden Schritte ausführen. (Alternativ können Sie die Schritte überspringen und ein bestehendes Speicher-Bucket verwenden.)

   a) Wählen Sie in der oberen Navigationsleiste **Services** > **S3** > **Create bucket**.
   b) Geben Sie einen eindeutigen Namen für das Bucket ein. Informationen zur Benennung von Buckets in Amazon S3 finden Sie unter https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html.
   c) Wählen Sie die Region für das Bucket aus. Die Region muss mit Ihrer AWS-Region übereinstimmen, da Sie die Dateien im Bucket nicht verwenden können, wenn die Regionen unterschiedlich sind.
   d) Übernehmen Sie für die verbleibenden Optionen die Standardeinstellungen und klicken Sie auf **Create bucket**.

4. Klicken Sie auf den Namen des Buckets, das Sie erstellt haben. Klicken Sie auf **Upload** > **Add files** und wählen Sie dann die Datei `connector-appliance.vhd` aus. Übernehmen Sie für die verbleibenden Optionen die Standardeinstellungen und klicken Sie auf **Upload**.
5. Klicken Sie auf die hochgeladene Datei. Klicken Sie auf **Copy S3 URI**.
6. Klicken Sie in der oberen Navigationsleiste auf das **AWS CloudShell-Symbol** und führen Sie die folgenden Befehle aus:

   a) Erstellen Sie einen Task, um Ihre VHD-Datei in einen Snapshot zu konvertieren:

   ```
   aws ec2 import-snapshot --disk-container Format=VHD,Url="<
       S3_URI>"
   ```

   Ersetzen Sie den Platzhalter durch Ihren S3-URI, den Sie aus dem vorherigen Schritt kopiert haben. Beispiel: `aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`.

Der Befehl ist abgeschlossen, wenn der folgende Befehl eine JSON-Zeichenfolge mit `"Status": "completed"` zurückgibt. Notieren Sie sich die `ImportTaskId` in der JSON-Ausgabe.

b) Führen Sie den folgenden Befehl aus:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids <
    ImportTaskId>
```

Ersetzen Sie den Platzhalter durch die `ImportTaskId` aus dem vorherigen Schritt. Beispiel: `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`.

7. Wählen Sie in der **AWS-Managementkonsole** in der oberen Navigationsleiste **Services** > **EC2**.
8. Klicken Sie im Menü links auf **Snapshots**.
9. Klicken Sie mit der rechten Maustaste auf den von Ihnen erstellten Snapshot und dann auf **Create Image**
10. Führen Sie auf der nun geöffneten Seite die folgenden Schritte aus:

    a) Geben Sie einen Namen für das AMI ein.
    b) Wählen Sie **Hardware-assisted virtualization**.

    Klicken Sie auf **Erstellen**.
11. Klicken Sie im Menü links auf **AMIs**.
12. Klicken Sie mit der rechten Maustaste auf das erstellte AMI und dann auf **Launch**.
13. Führen Sie auf der nun geöffneten Seite die folgenden Schritte aus:

    a) Wählen Sie den Instanztyp.
    b) (Optional) Passen Sie das Netzwerk auf der Registerkarte **Configure Instance** an.
    c) (Optional) Fügen Sie auf der Registerkarte **Add Storage** ein weiteres Volume an.
    d) Legen Sie auf der Registerkarte **Configure Security Group** Sicherheitsgruppenregeln fest.

    Wenn Sie den Start der Instanz überprüft haben, klicken Sie auf **Review and Launch**.

Wenn die Connector Appliance bereitgestellt und gestartet ist, gehen Sie zu **Services** > **EC2** > **Instances** und wählen Sie die Instanz aus, die Sie erstellt haben. Verwenden Sie die Adresse unter **Private IPv4 address**, um eine Verbindung mit der Connector Appliance-Verwaltungsseite herzustellen und die Registrierung abzuschließen. Sie benötigen evtl. einen Bastionshost, um aus dem Browser die Connector Appliance-Verwaltungsseite unter der internen IP-Adresse aufzurufen und die Installation fortzusetzen.

Standardmäßig verwendet die Connector Appliance DHCP zum Festlegen der Netzwerkkonfiguration. Sie können diese Netzwerkkonfiguration über die Connector Appliance-Weboberfläche

bearbeiten. Weitere Informationen finden Sie unter Netzwerkeinstellungen auf der Connector Appliance-Verwaltungsseite konfigurieren.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Connector Appliance über ein PowerShell-Skript bereitstellen Die Datei `connector-appliance-aws.zip` enthält ein PowerShell-Skript, das eine neue VM erstellt und startet. Vor der Ausführung des Skripts müssen Sie die folgenden Voraussetzungen erfüllen:

- Sie haben AWS.Tools, AWSPowerShell.NetCore oder AWSPowerShell auf Ihrem System installiert. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html.
- Sie haben eine Dienstrolle und eine Richtlinie mit VM-Importzugriff erstellt. Sowohl die Dienstrolle als auch die Richtlinie müssen mit `vmimport` benannt sein, damit das PowerShell-Skript funktioniert. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

  > **Hinweis:**
  >
  > Um eine Dienstrolle zu erstellen, müssen Sie einen S3-Bucket erstellen. Legen Sie beim Erstellen der Richtlinie das S3-Bucket fest, das Sie mit VM-Importzugriff erstellt haben.

- Sie haben eine Amazon EC2-Sicherheitsgruppe erstellt.
- Sie haben S3-Berechtigungen und API-Zugriff.
- Sie haben die Konfiguration unter Netzwerkvoraussetzungen ausgeführt.

Führen Sie hierzu die folgenden Schritte aus:

1. Extrahieren Sie den Inhalt von `connector-appliance-aws.zip` auf dem lokalen System in einen Ordner.
2. Führen Sie in PowerShell die folgenden Befehle aus:

   a) Zum Ausführen eines AWS-Cmdlets in Ihrer lokalen Umgebung führen Sie den folgenden Befehl aus, um dem AWS SDK-Speicher ein neues Profil hinzuzufügen:

   ```
   Set-AWSCredential -AccessKey <access_key_ID> -SecretKey <
       secret_key> -StoreAs MyProfile
   ```

   Ersetzen Sie die Platzhalter durch Ihren Zugriffsschlüssel und Ihren geheimen Schlüssel. Geben Sie einen eindeutigen Profilnamen an. In unserem Beispiel ist es `MyProfile`.

   b) Legen Sie das Profil als Standard fest:

   ```
   Initialize-AWSDefaultConfiguration -ProfileName MyProfile
   ```


c) Wechseln Sie in den Ordner, in dem sich die extrahierten Dateien befinden, und führen Sie den folgenden Befehl aus:

```
.\connector-appliance-upload-aws.ps1
```

3. Folgen Sie den Anweisungen im Skript zur Auswahl der Region für Ihre Connector Appliance-Bereitstellung, zum Hochladen des Images in das von Ihnen ausgewählte Bucket und zur Eingabe eines Namens für Ihre VM.

   - Sie müssen das Bucket mit VM-Importzugriff verwenden, das Sie zuvor erstellt haben.
   - Wenn Sie zur Angabe der VPC aufgefordert werden, wählen Sie die VPC aus, in der das NAT-Gateway und die Routingtabellen konfiguriert sind.
   - Wählen Sie als Subnetz dasjenige aus, das an die Routingtabelle mit dem NAT-Gateway anfügt wurde.

   Weitere Informationen finden Sie unter Voraussetzungen für das Netzwerk.

Nach dem Bereitstellen und erfolgreichen Start der Connector Appliance wird die private IP-Adresse der Connector Appliance angezeigt. Sie benötigen evtl. einen Bastionshost, um aus dem Browser die Connector Appliance-Verwaltungsseite unter der internen IP-Adresse aufzurufen und die Registrierung abzuschließen.

Standardmäßig verwendet die Connector Appliance DHCP zum Festlegen der Netzwerkkonfiguration. Sie können diese Netzwerkkonfiguration über die Connector Appliance-Weboberfläche bearbeiten. Weitere Informationen finden Sie unter Netzwerkeinstellungen auf der Connector Appliance-Verwaltungsseite konfigurieren.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Google Cloud Platform

In diesem Abschnitt wird beschrieben, wie die Connector Appliance auf der Google Cloud Platform bereitgestellt wird. Sie können die Connector Appliance vom Google Cloud Marketplace installieren. Alternativ können Sie ein heruntergeladenes Datenträgerimage mit der Google Cloud Platform-Konsole oder dem enthaltenen PowerShell-Skript bereitstellen.

Die Datei `connector-appliance-gcp.zip` enthält Folgendes:

- `connector-appliance.tar.gz` –Datenträgerimage der Connector Appliance
- `connector-appliance-upload-gcp.ps1` –PowerShell-Skript, mit dem die Connector Appliance automatisch bereitgestellt werden kann

Connector Appliance aus Google Cloud Marketplace bereitstellen

1. Melden Sie sich an Ihrem Google-Konto an.
2. Verwenden Sie den in Citrix Cloud bereitstellten Link zum Marketplace. (Google Cloud Marketplace)

   Alternativ können Sie im Suchfeld von Marketplace auch "Connector Appliance für Cloud-Dienste"eingeben.
3. Klicken Sie auf **Launch**.
4. Füllen Sie auf der Seite **New Citrix Connector Appliance for Cloud Services deployment** die folgenden Informationen aus:

   - Geben Sie einen **Bereitstellungsnamen** für den Bereitstellungsauftrag an.
   - Wählen Sie eine **Zone** für die Connector Appliance.
   - Wählen Sie die zu verwendenden **Maschinenfamilie**, die **Serie** und den **Maschinentyp**.
   - Wählen Sie den **Startdatenträgertyp** und die **Größe des Startdatenträgers in GB**.
   - Geben Sie im Abschnitt **Networking** die Netzwerkschnittstelle an, die von der Connector Appliance verwendet werden soll. Wenn Sie über ein öffentliches Netzwerk eine Verbindung mit der Verwaltungsseite herstellen möchten, geben Sie eine externe IP unter **External IP** an.

   Klicken Sie auf **Bereitstellen**. Sie werden zur Seite **Deployment Manager** weitergeleitet.

   > **Hinweis:**
   >
   > Nach dem Bereitstellen und erfolgreichen Start der Connector Appliance erhalten Sie eine E-Mail zur Bestätigung, dass die Connector Appliance auf Google Cloud Platform bereitgestellt wurde.

5. Klicken Sie auf der Seite **Deployment Manager** auf den Instanznamen. Alternativ können Sie nach der Connector Appliance-Instanz suchen, die Sie unter **Compute Engine** erstellt haben.
6. Wenn Sie beim Einrichten der Netzwerkschnittstelle für die Connector Appliance eine Angabe unter **External IP** gemacht haben, kopieren Sie diese aus dem Feld **External IP address** im Bereich **Network interfaces** auf der Registerkarte **Details**. Verwenden Sie diese IP-Adresse, um eine Verbindung mit der Connector Appliance-Verwaltungsseite herzustellen und die Registrierung abzuschließen. Alternativ können Sie die für **Primary internal IP address** angegebene Adresse verwenden, um die Verwaltungsseite der Connector Appliance von einer anderen Maschine aus aufzurufen, die sich im selben Subnetz wie die Connector Appliance befindet.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Connector Appliance über die Google Cloud Platform-Konsole bereitstellen

1. Extrahieren Sie den Inhalt von `connector-appliance-gcp.zip` auf dem lokalen System.

2. Erstellen Sie in Ihrem Google Cloud Platform-Projekt einen Storage-Bucket. (Alternativ können Sie einen vorhandenen Storage-Bucket verwenden.)

   a) Wählen Sie im Hauptmenü **Cloud Storage**.
   b) Wählen Sie im Hauptbereich **Create bucket**.
   c) Geben Sie einen Namen für den Bucket ein.
   d) Konfigurieren Sie die Einstellungen für Datenspeicher und Zugriff. Sie können auch die Standardeinstellungen belassen.
   e) Klicken Sie auf **Erstellen**.

3. Wählen Sie im Storage-Bucket **Upload files** und wählen Sie die Datei `connector-appliance.tar.gz`. Warten Sie, bis der Dateiupload abgeschlossen ist.

4. Wählen Sie die hochgeladene Datei, um die Details anzuzeigen. Kopieren Sie den Wert von **gsutil URI** in die Zwischenablage.

5. Öffnen Sie die Cloudshell, indem Sie in der Kopfzeilenleiste auf das Symbol für **Cloudshell aktivieren** klicken.

6. Führen Sie in der Cloudshell den folgenden Befehl aus, um ein Image zu erstellen:

   ```
   gcloud compute images create "Image name" --guest-os-features=
       MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded connector-
       appliance.tar.gz file"
   ```

7. Wählen Sie im Hauptmenü **Compute Engine** > **VM Instances**.

8. Wählen Sie **Create Instance**. Geben Sie im nun geöffneten Bereich die folgenden Informationen ein:

   a) Geben Sie im Feld **Name** einen Namen für die Connector Appliance-Instanz ein.
   b) Wählen Sie eine Region als Standort der Connector Appliance.
   c) Legen Sie die Maschinenkonfiguration fest.
   d) Klicken Sie im Bereich **Boot disk** auf **Change**.
   e) Wechseln Sie im nun geöffneten Abschnitt zur Registerkarte **Custom images**.
   f) Wählen Sie in der Liste **Image** das erstellte Image.
   g) Klicken Sie auf **Select**.
   h) Aktivieren Sie im Abschnitt **Firewall** “HTTPS Traffic”, um den Zugriff auf die Connector Appliance-Verwaltungsseite zu ermöglichen.
   i) Konfigurieren Sie ggf. weitere Optionen. Vielleicht möchten Sie beispielsweise nicht die Standardnetzwerkkonfiguration verwenden.

   Klicken Sie auf **Erstellen**.

9. Wählen Sie im Abschnitt **VM Instances** die neu erstellte VM aus, um die Details anzuzeigen.

Nach dem Bereitstellen und erfolgreichen Start der Connector Appliance werden im Abschnitt **VM Instances** die IP-Adressen der Connector Appliance angezeigt.

Wenn die Connector Appliance eine externe IP-Adresse hat, können Sie sie verwenden, um aus dem Browser die Connector Appliance-Verwaltungsseite aufzurufen und die Registrierung abzuschließen.

Wenn die Connector Appliance nur eine interne IP-Adresse hat, verwenden Sie einen Bastionshost, um aus dem Browser die Connector Appliance-Verwaltungsseite aufzurufen und die Registrierung abzuschließen. Weitere Informationen finden Sie unter https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Connector Appliance über ein PowerShell-Skript bereitstellen Um das bereitgestellte PowerShell-Skript zum Bereitstellen der Connector Appliance zu verwenden, muss auf Ihrem System das Google Cloud SDK installiert sein.

1. Extrahieren Sie den Inhalt von `connector-appliance-gcp.zip` auf dem lokalen System in einen Ordner.
2. Ändern Sie in PowerShell das Verzeichnis in den Ordner, in dem sich die extrahierten Dateien befinden.
3. Führen Sie den Befehl `.\connector-appliance-upload-GCP.ps1` aus.
4. Authentifizieren Sie sich im geöffneten Browserfenster beim Google Cloud SDK mit einem Konto, das Zugriff auf das Projekt hat, für das Sie die Connector Appliance bereitstellen möchten.
5. Wählen Sie das zu verwendende Projekt in Google Cloud Tools for PowerShell aus, wenn Sie vom PowerShell-Skript dazu aufgefordert werden. Drücken Sie die Eingabetaste.
6. Folgen Sie den Anweisungen im Skript zum Upload des Datenträgers, Erstellen eines Images und Erstellen einer virtuellen Maschine.
7. Nach dem Erstellen der ersten VM werden Sie gefragt, ob Sie eine weitere VM aus dem hochgeladenen Image erstellen möchten.
    - Geben Sie `y` ein, um eine weitere VM zu erstellen.
    - Geben Sie `n` ein, um das Skript zu beenden.

Nach dem Bereitstellen und erfolgreichen Start der Connector Appliance wird die interne IP-Adresse der Connector Appliance angezeigt. Alternativ können Sie die interne IP-Adresse der Connector Appliance in der Google Cloud Platform-Konsole suchen. Im Abschnitt **Compute Engine** > **VM Instances** wird die IP-Adresse der Connector Appliance angezeigt.

Verwenden Sie einen Bastionshost, um aus dem Browser die Connector Appliance-Verwaltungsseite unter der internen IP-Adresse aufzurufen und die Registrierung abzuschließen. Weitere Informationen finden Sie unter https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Nächster Schritt: Connector Appliance bei Citrix Cloud registrieren.

Connector Appliance bei Citrix Cloud registrieren

Durch Registrieren einer Connector Appliance bei Citrix Cloud schaffen Sie einen Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten.

Nachdem Sie die Connector Appliance auf dem Hypervisor installiert und gestartet haben, wird in der Konsole die IP-Adresse der Connector Appliance angezeigt. Die Konsole zeigt außerdem einen SSL-Fingerabdruck, mit dem Sie Ihre Verbindung zur Benutzeroberfläche der Connector Appliance validieren können.

1. Kopieren Sie die IP-Adresse der Connector Appliance in die Adressleiste Ihres Browsers.

   > **Hinweis:**
   >
   > Sie müssen u. U. am Anfang der IP-Adresse `https://` angeben.

   Die Benutzeroberfläche der Connector Appliance verwendet ein selbstsigniertes Zertifikat, das fünf Jahre gültig ist. Daher wird möglicherweise eine Meldung angezeigt, dass die Verbindung nicht sicher ist. Um die Verbindung zu Ihrer Connector Appliance zu überprüfen, können Sie den SSL-Fingerabdruck in der Konsole mit dem Fingerabdruck vergleichen, den der Browser von der Webseite erhält.

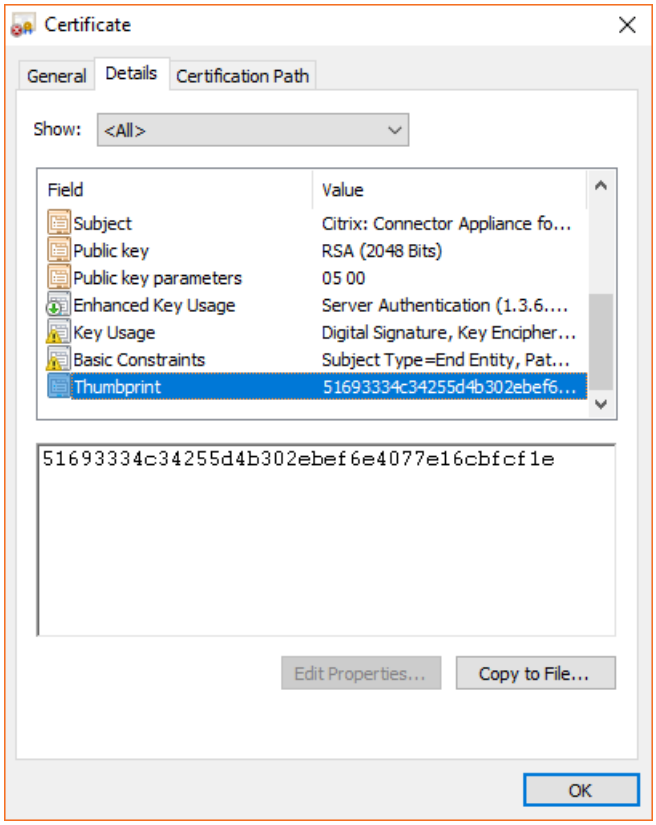
Führen Sie beispielsweise im Google Chrome-Browser die folgenden Schritte aus:

a) Klicken Sie neben der Adressleiste auf den Marker **Nicht sicher**.

b) Wählen Sie **Zertifikat**. Das Fenster **Zertifikat** wird geöffnet.

c) Wechseln Sie zur Registerkarte **Details** und suchen Sie das Feld **Fingerabdruck**.

Wenn der Wert im Feld **Fingerabdruck** mit dem SSL-Fingerabdruck in der Konsole übereinstimmt, können Sie bestätigen, dass Ihr Browser direkt mit der Benutzeroberfläche der Connector Appliance verbunden ist.

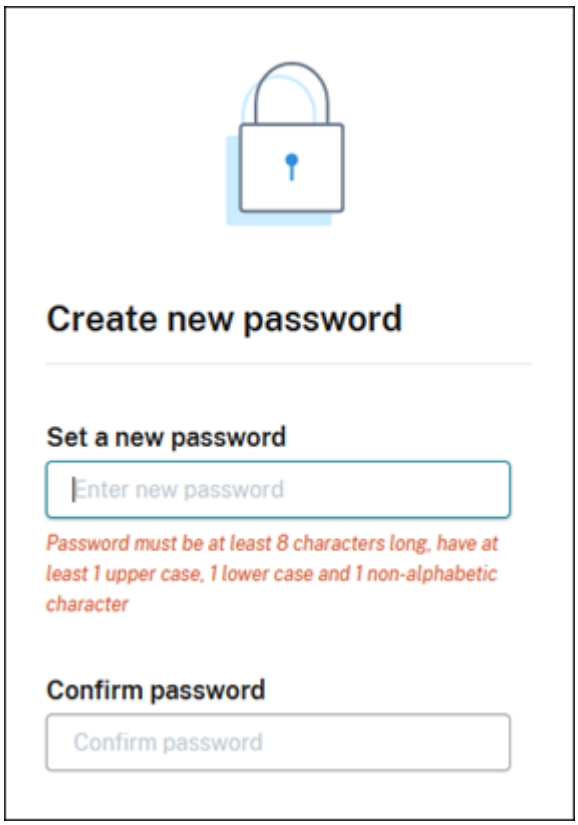


Sie können dieses selbstsignierte Zertifikat durch ein eigenes ersetzen, das von Ihrer Organisation signiert oder mithilfe der Vertrauenskette Ihrer Organisation generiert wurde. Weitere Informationen finden Sie unter Zertifikate verwalten.

2. Wenn Sie im Browser bestätigen müssen, dass Sie die Website aufrufen möchten, führen Sie diesen zusätzlichen Schritt jetzt aus.

   Die Webseite **Neues Kennwort erstellen** wird geöffnet.

3. Erstellen Sie ein Kennwort für die Benutzeroberfläche Ihrer Connector Appliance und klicken Sie auf **Kennwort festlegen**.

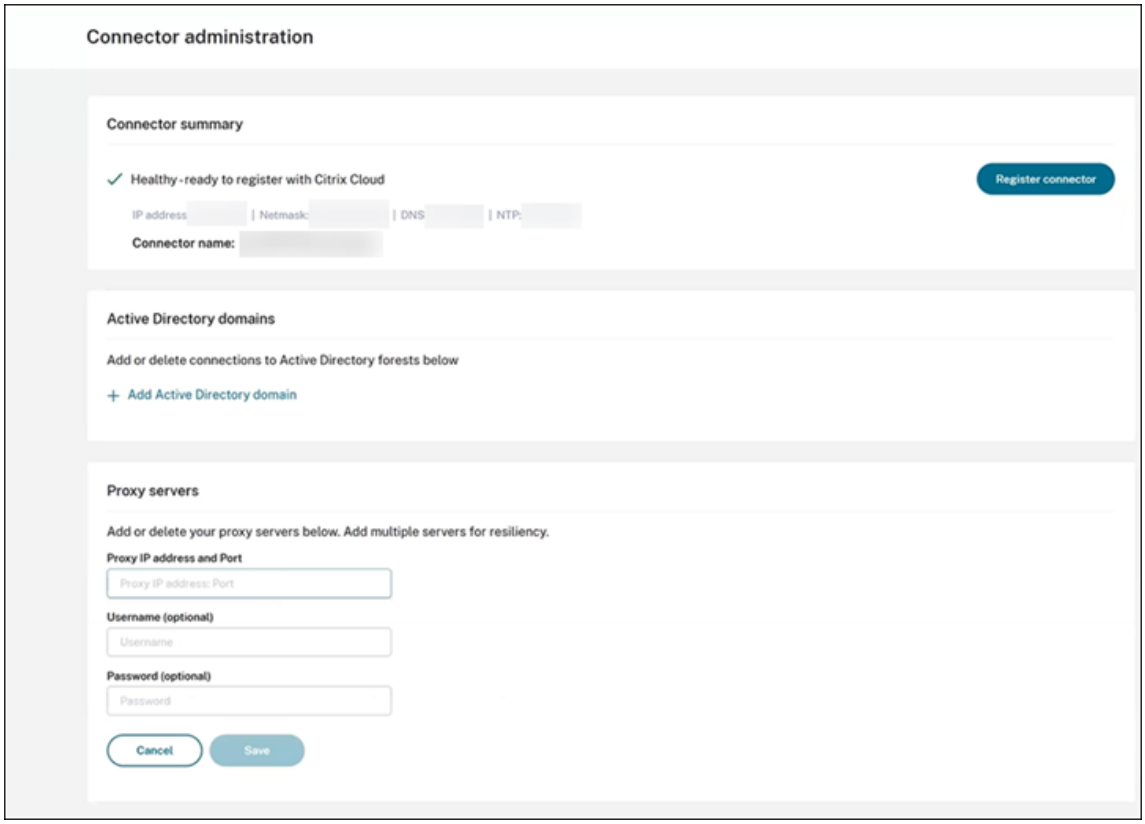


Ihr Kennwort muss die folgenden Anforderungen erfüllen:

- Kennwortlänge mindestens 8 Zeichen
- Groß- und Kleinbuchstaben enthalten
- Mindestens ein nicht alphabetisches Zeichen enthalten

Stellen Sie sicher, dass Sie dieses Kennwort für die zukünftige Verwendung an einem sicheren Ort speichern.

4. Melden Sie sich mit dem erstellten Kennwort an. Die Seite **Connectorverwaltung** wird geöffnet.



5. (Optional) Wenn Sie einen oder mehrere Webproxys verwenden, können Sie im Abschnitt **Proxyserver** die Proxyadressen hinzufügen. Es werden authentifizierte und nicht authentifizierte Proxys unterstützt. Um einen nicht authentifizierten Proxy hinzuzufügen, machen Sie für **Proxy-IP-Adresse und Port** gültige Angaben. Um einen authentifizierten Proxy hinzuzufügen, geben Sie außerdem einen gültigen **Benutzernamen** und ein **Kennwort** an.

   > **Hinweis:**
   >
   > Es wird nur die Standard-Proxy-Authentifizierung unterstützt. Andere Authentifizierungsmethoden werden nicht unterstützt.

   Nur der Datenverkehr zu externen Systemen wird über den Webproxy geleitet. Weitere Informationen finden Sie unter Kommunikation der Connector Appliance.

6. (Optional) Wenn Ihr Netzwerk für den Zugriff auf das Internet TLS abfangende Webproxys verwendet, müssen Sie möglicherweise festlegen, dass der Connector der Stammzertifizierungsstelle vertraut, um erfolgreich mit der Cloud kommunizieren zu können.

   a) Wählen Sie unter **Stammzertifizierungsstellen** die Option **Zertifikat hinzufügen**.

   b) Kopieren Sie den Inhalt des Zertifikats im PEM-Format:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate-base64-bytes>
   ```



```
-----END CERTIFICATE-----
<!--NeedCopy-->
```

c) Fügen Sie den Inhalt des Zertifikats in **Vollständige Zertifikatdetails** ein.

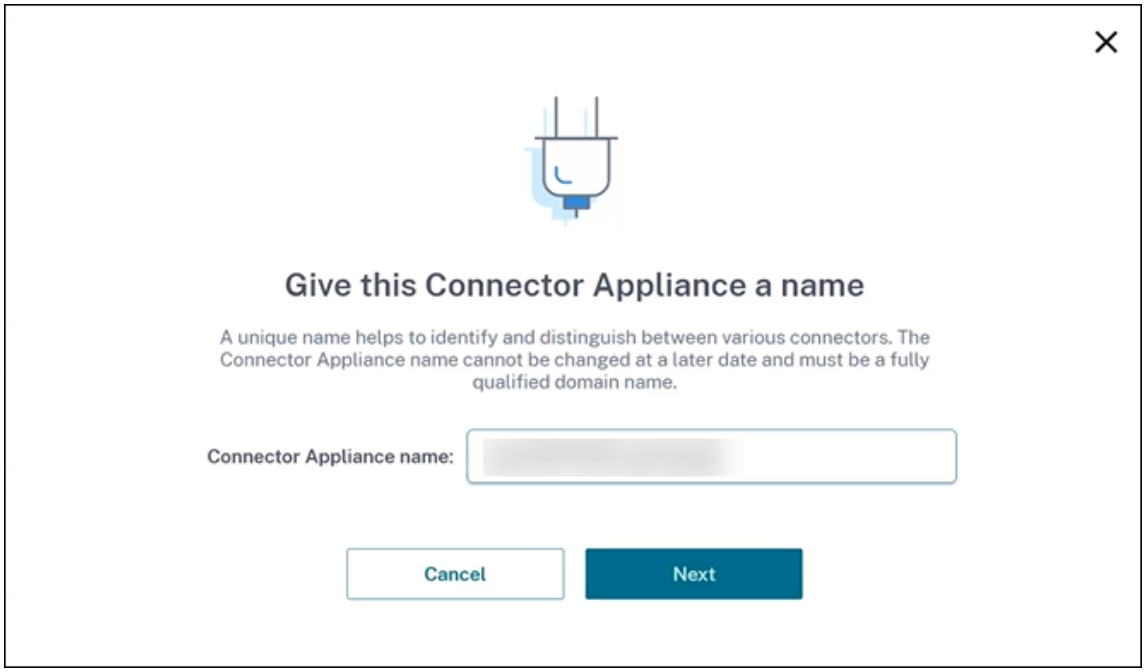
d) Wählen Sie **Zertifikat hinzufügen**.

Informationen zum Hinzufügen einer Stammzertifizierungsstelle mithilfe der Connector Appliance-APIs finden Sie unter Managing root certificate authorities in der Citrix Developer-Dokumentation.

> **Hinweis:**
>
> Zertifikate, die abgelaufen sind oder in den nächsten 30 Tagen ablaufen, werden mit einer Warnung angezeigt.

7. Klicken Sie auf **Connector registrieren**, um die Registrierungsaufgabe zu öffnen.
8. Wählen Sie einen Namen für Ihre Connector Appliance. Dieser Name hilft Ihnen, die einzelnen Connector Appliances am Ressourcenstandort zu unterscheiden. Nachdem Sie die Connector Appliance registriert haben, kann der Name nicht mehr geändert werden.

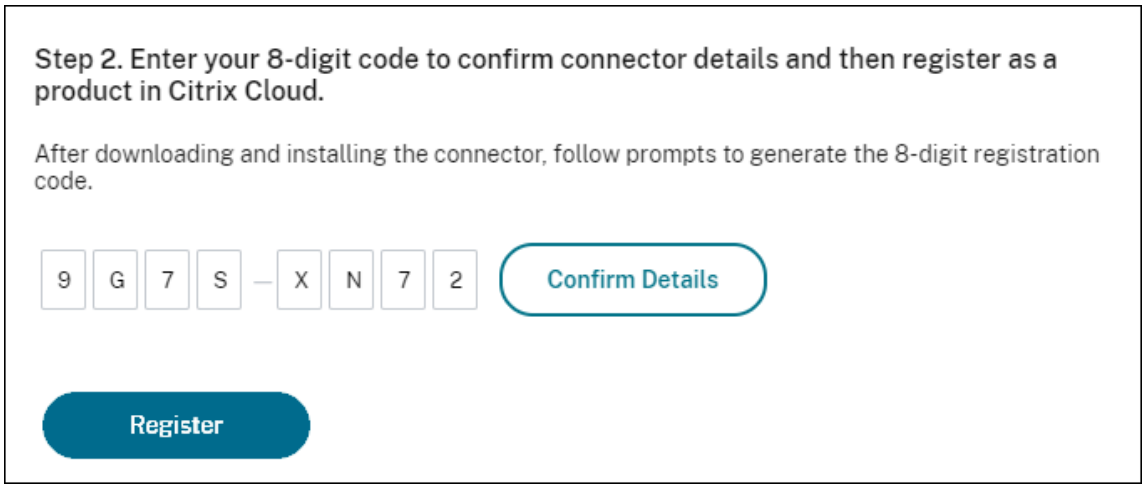
   Geben Sie den Namen im Feld **Name der Connector Appliance** ein und klicken Sie auf **Weiter**.



   Die Webseite zeigt einen Code an, mit dem Sie sich bei Citrix Cloud registrieren können. Der Code läuft nach 15 Minuten ab.

9. Klicken Sie auf die Schaltfläche **Kopieren**, um den Code in die Zwischenablage zu kopieren.
10. Kehren Sie zur Webseite **Ressourcenstandorte** zurück.
11. Fügen Sie den Code in **Schritt 2** der Aufgabe **Connector Appliance installieren** ein. Klicken Sie auf **Details bestätigen**.

    Citrix Cloud überprüft, ob die Connector Appliance vorhanden ist und kontaktiert werden kann. Wenn der Registrierungscode abgelaufen ist, werden Sie aufgefordert, einen neuen Code zu generieren.



12. Klicken Sie auf **Registrieren**.

    Es wird angezeigt, ob die Registrierung erfolgreich war. Bei fehlgeschlagener Registrierung werden Sie aufgefordert, es erneut zu versuchen.

13. Klicken Sie auf **Schließen**.

Auf der **Connector Appliance-Verwaltungsseite** können Sie auch einen Diagnosebericht für die Connector Appliance herunterladen. Weitere Informationen finden Sie unter Erstellen eines Diagnoseberichts.

Nach der Registrierung Ihrer Connector Appliance

Wir empfehlen, dass Sie für jeden Ressourcenstandort zwei oder mehr Connector Appliances installieren und registrieren. Diese Konfiguration gewährleistet eine kontinuierliche Verfügbarkeit und ermöglicht den Lastausgleich zwischen Connectors.

Sie können Ihre Connector Appliance nicht direkt verwalten.

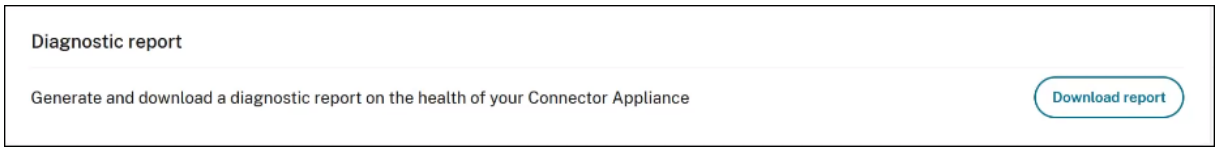
Die Connector Appliance wird automatisch aktualisiert. Sie müssen keine Aktionen ausführen, um den Connector zu aktualisieren. Sie können die Uhrzeit und den Tag angeben, an dem Connector Appliance-Updates an Ihrem Ressourcenstandort angewendet werden sollen. Weitere Informationen finden Sie unter Connector-Updates.

Sie sollten die Connector Appliance-VMs weder klonen oder anhalten und auch keinen Snapshot erstellen. Diese Aktionen werden nicht unterstützt.

Die Seite **Neues Kennwort erstellen** wird nur beim ersten Verbinden mit der Benutzeroberfläche der Connector Appliance angezeigt. Stellen Sie sicher, dass Sie dieses Kennwort für die zukünftige Verwendung an einem sicheren Ort speichern. Dieses Kennwort kann nicht zurückgesetzt werden. Wenn Sie das Kennwort vergessen, müssen Sie die Connector Appliance neu installieren. Wenn Sie sich anschließend wieder mit der Benutzeroberfläche verbinden, müssen Sie das Kennwort eingeben, das Sie bei der Registrierung der Connector Appliance festgelegt haben.

Erstellen eines Diagnoseberichts

Sie können auf der **Connector Appliance-Verwaltungsseite** einen Diagnosebericht erstellen und ihn herunterladen.



1. Kopieren Sie von der Connector Appliance-Konsole in Ihrem Hypervisor die IP-Adresse in die Adressleiste Ihres Browsers.
2. Geben Sie das Kennwort ein, das Sie bei der Registrierung der Connector Appliance festgelegt haben.
3. Klicken Sie im Abschnitt **Diagnosebericht** der Seite auf **Bericht herunterladen**.

Die Diagnoseberichte werden in einer `.zip`-Datei bereitgestellt.

Verifizieren der Netzwerkverbindung

Sie können Ihre Netzwerkverbindung mit der **TCP-Erfassung** auf der **Connector Appliance**-Verwaltungsseite überprüfen.

1. Klicken Sie auf der **Connector Appliance-Verwaltungsseite** in der Kopfzeilenleiste auf Ihren Kontonamen und wählen Sie **Netzwerkdiagnose**.
2. (Optional) Geben Sie im Bereich **TCP-Erfassung** die Ziel-IP-Adresse, den Hostnamen oder den Port ein, um die TCP-Erfassung zu limitieren.
3. Wählen Sie im Menü **Tracingdauer** aus, wie lange das Tracing ausgeführt werden soll.
4. (Optional) Aktivieren Sie **Pakettracing**, um den Inhalt von Paketen zu erfassen.

   Wenn das Pakettracing deaktiviert ist, werden bei der TCP-Erfassung nach Möglichkeit die Header für die Diagnose erfasst. Es werden die ersten 94 Byte jedes Pakets erfasst. Da Header keine feste Größe haben, werden sie bei diesem Ansatz möglicherweise nicht komplett erfasst.
5. Klicken Sie auf **Trace starten**.
6. Warten Sie, bis das Tracing abgeschlossen ist. Anschließend können Sie einen Tracingbericht herunterladen oder ein neues Tracing starten.

   - Klicken Sie auf **Herunterladen**, um den Tracingbericht herunterzuladen. Der Tracingbericht wird als `.pcap`Datei bereitgestellt.
   - Klicken Sie auf **Neues Tracing starten**, um das Tracing neu zu starten.

Active Directory mit Citrix Cloud verbinden

Sie können Connector Appliances verwenden, um einen Ressourcenstandort mit Gesamtstrukturen zu verbinden, die keine Citrix Virtual Apps and Desktops-Ressourcen enthalten. Zum Beispiel im Fall von Citrix Secure Private Access-Kunden oder Citrix Virtual Apps and Desktops-Kunden mit einigen Gesamtstrukturen, die nur für die Benutzerauthentifizierung verwendet werden.

Weitere Informationen finden Sie unter Active Directory mit Connector Appliance.

Validierung der Kerberos-Konfiguration

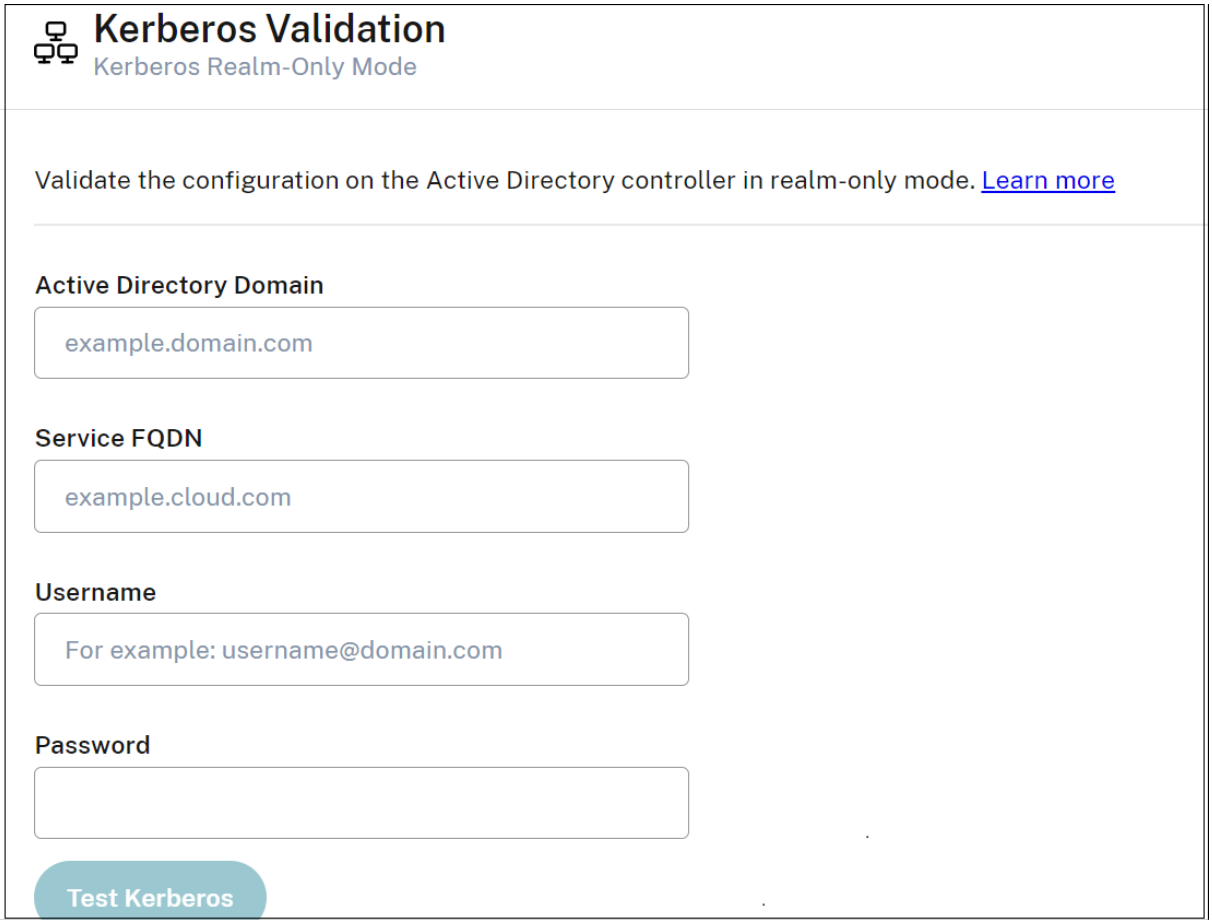
Wenn Sie Kerberos für Single Sign-On verwenden, können Sie auf der **Connector Appliance-Verwaltungsseite** überprüfen, ob die Konfiguration auf Ihrem Active Directory-Controller korrekt ist. Mit dem Feature **Kerberos-Validierung** können Sie eine Konfiguration im Kerberos Realm-Only-Modus oder eine Konfiguration mit eingeschränkter Kerberos-Delegierung (KCD) validieren.

Kerberos-Realm-Only-Konfiguration validieren:

1. Rufen Sie die **Connector Appliance-Verwaltungsseite** auf.
2. Kopieren Sie von der Connector Appliance-Konsole in Ihrem Hypervisor die IP-Adresse in die Adressleiste Ihres Browsers.
3. Geben Sie das Kennwort ein, das Sie bei der Registrierung der Connector Appliance festgelegt haben.
4. Zum Validieren der Realm-Only-Kerberos-Konfiguration wählen Sie **Kerberos Validation Realm-Only** im Bereich **Active Directory domains**.
5. Geben Sie die **Active Directory-Domäne** an.

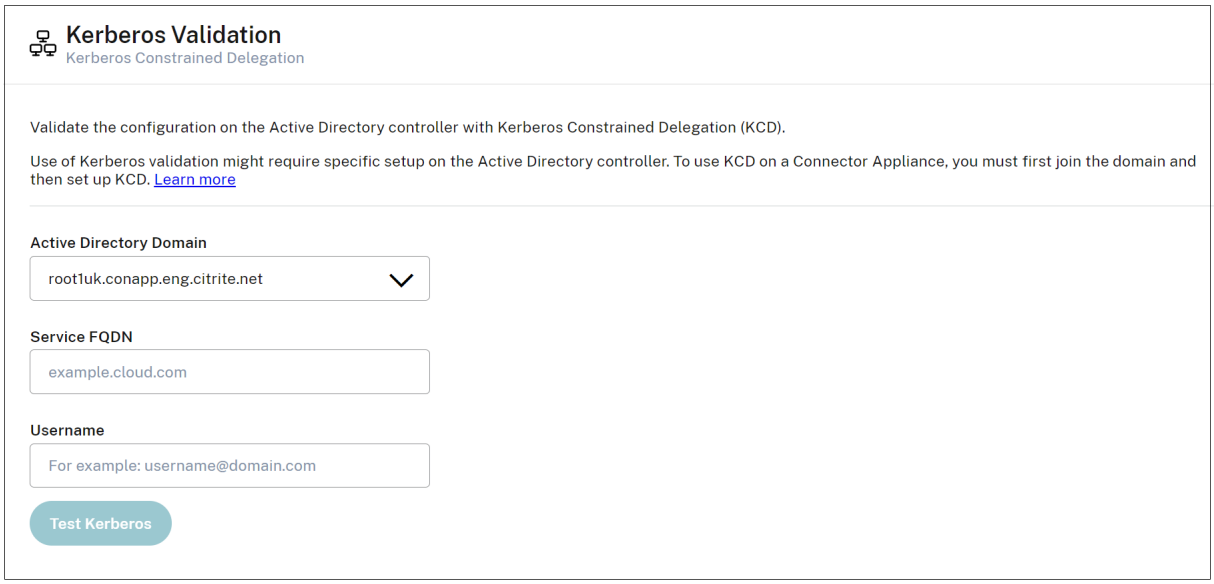
    - Wenn Sie eine Konfiguration im Kerberos Realm-Only-Modus validieren, können Sie eine beliebige Active Directory-Domäne angeben. Dieser Modus hängt nicht von einer Domänenzugehörigkeit ab.

6. Geben Sie den **Dienst-FQDN** an. Als Standarddienstname wird “https”angenommen. Wenn Sie “computer.example.com”angeben, wird dieser Wert als https://computer.example.com angesehen.
7. Geben Sie den **Benutzernamen** an.
8. Geben Sie das **Kennwort** an.
9. Klicken Sie auf **Kerberos testen**.



Konfiguration der eingeschränkten Kerberos-Delegierung validieren:

1. Rufen Sie die **Connector Appliance-Verwaltungsseite** auf.
2. Um die **eingeschränkte Kerberos-Delegierung** für die Domänen mit der Connector Appliance zu validieren, wählen Sie über die auf die Auslassungspunkte der entsprechenden Domäne die Option **Kerberos-Validierung**.
3. Geben Sie die **Active Directory-Domäne** an.
   - Wenn Sie eine Konfiguration mit eingeschränkter Kerberos-Delegierung überprüfen, müssen Sie Ihre Auswahl in einer Liste verbundener Domänen treffen.
4. Geben Sie den **Dienst-FQDN** an. Als Standarddienstname wird “https”angenommen. Wenn Sie beispielsweise “computer.example.com”angeben, wird dieser Wert als https://computer.example.com%E2%80%9D angesehen.
5. Geben Sie den **Benutzernamen** an.
   - Für die eingeschränkte Kerberos-Delegierung können Sie die Kerberos-Konfiguration auch über Dienstkonten validieren, indem Sie die Registerkarte **Dienstkonten** auswählen.
6. Klicken Sie auf **Kerberos testen**.



Wenn die Kerberos-Konfiguration korrekt ist, wird die Meldung "Kerberos-Setup wurde erfolgreich validiert"angezeigt. Wenn die Kerberos-Konfiguration nicht korrekt ist, wird eine Fehlermeldung angezeigt, die Informationen zur fehlgeschlagenen Validierung enthält.

Weitere Informationen zu Kerberos finden Sie in der Dokumentation von Microsoft.

Netzwerkeinstellungen für Ihre Connector Appliance

Standardmäßig werden die IP-Adresse und Netzwerkeinstellungen der Connector Appliance automatisch über DHCP zugewiesen.

Nachdem Sie die Connector Appliance mit DHCP registriert haben, können Sie die Netzwerkeinstellungen auf der **Connector Appliance-Verwaltungsseite** bearbeiten.

Wenn DHCP in Ihrer Umgebung jedoch nicht verfügbar ist oder wenn Sie keinen Zugriff auf die **Connector Appliance-Verwaltungsseite** haben, können Sie die Netzwerkkonfiguration direkt in der Connector Appliance-Konsole festlegen.

Netzwerkeinstellungen auf der Connector Appliance-Verwaltungsseite konfigurieren

Nachdem Sie die Connector Appliance mit DHCP registriert haben, können Sie die Netzwerkeinstellungen auf der **Connector Appliance-Verwaltungsseite** bearbeiten.

Manuelles Konfigurieren der Netzwerkeinstellungen:

1. Wählen Sie im Abschnitt **Connector - Zusammenfassung** die Option **Netzwerkeinstellungen bearbeiten**.

2. Wählen Sie im Dialogfeld **Netzwerkeinstellungen** die Option **Eigene Netzwerkeinstellungen konfigurieren**.
3. Geben Sie **IP-Adresse**, **Subnetzmaske**und **Standardgateway** ein.
4. Fügen Sie einen oder mehrere **DNS-Server** hinzu.
5. Fügen Sie einen oder mehrere **NTP-Server** hinzu.
6. Klicken Sie auf **Speichern**.

Wenn Sie Änderungen an den Netzwerkeinstellungen speichern, wird die Connector Appliance neu gestartet. Während des Neustarts ist die Connector Appliance vorübergehend nicht verfügbar. Sie werden von der **Connector Appliance-Verwaltungsseite** abgemeldet und die URL der Seite ändert sich. Sie finden die neue URL in der Connector Appliance-Konsole oder in den Netzwerkinformationen Ihres Hypervisors.

Ändern der Netzwerkkonfiguration zur Verwendung automatisch zugewiesener Werte:

1. Wählen Sie im Abschnitt **Connector - Zusammenfassung** die Option **Netzwerkeinstellungen bearbeiten**.
2. Wählen Sie im Dialogfeld **Netzwerkeinstellungen** die Option **IP-Adresse automatisch abrufen**.
3. Klicken Sie auf **Speichern**.

Wenn Sie Änderungen an den Netzwerkeinstellungen speichern, wird die Connector Appliance neu gestartet. Während des Neustarts ist die Connector Appliance vorübergehend nicht verfügbar. Sie werden von der **Connector Appliance-Verwaltungsseite** abgemeldet und die URL der Seite ändert sich. Sie finden die neue URL in der Connector Appliance-Konsole oder in den Netzwerkinformationen Ihres Hypervisors.

Netzwerkkonfiguration über die Connector Appliance-Konsole festlegen

Standardmäßig werden die IP-Adresse und Netzwerkeinstellungen der Connector Appliance automatisch über DHCP zugewiesen. Wenn DHCP in Ihrer Umgebung jedoch nicht verfügbar ist oder wenn Sie keinen Zugriff auf die **Connector Appliance-Verwaltungsseite** haben, können Sie die Netzwerkkonfiguration direkt in der Connector Appliance-Konsole festlegen.

Festlegen der Netzwerkkonfiguration:

1. Starten Sie auf dem Hypervisor die Connector Appliance neu.
2. Warten Sie beim Start der Connector Appliance in der Konsole auf die Meldung `Welcome to GRUB!`.
3. Wenn Sie diese Meldung sehen, drücken Sie **Esc**, um das GRUB-Menü zu öffnen.
4. Drücken Sie **e**, um die Startparameter zu bearbeiten.

Sie sehen eine Ansicht, die der folgenden Abbildung ähnelt:

5. Bearbeiten Sie die Zeile, die mit `linux` beginnt, um Ihre erforderliche Netzwerkkonfiguration einzufügen.

   - Um DHCP-Netzwerke anzugeben, hängen Sie `network=dhcp` am Zeilenende an.
   - Um statische Netzwerke anzugeben, hängen Sie die folgenden Parameter am Zeilenende an:

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route
        =<default_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<
        ntp_server_1>,<ntp_server_2>
     <!--NeedCopy-->
     ```

     Ersetzen Sie die Platzhalterwerte durch die Werte für Ihre Konfiguration.

6. Drücken Sie **Strg+X**, um die Connector Appliance mit der neuen Konfiguration zu starten.

Administratorkennwort für die Connector Appliance ändern

1. Wählen Sie im Benutzermenü oben rechts in der Konsole die Option **Kennwort ändern**.

   Die Seite “Kennwort ändern”wird angezeigt.

2. Geben Sie Ihr aktuelles Kennwort ein und geben Sie dann das neue Kennwort ein und bestätigen Sie es. Das neue Kennwort muss die folgenden Anforderungen erfüllen:

   - Kennwortlänge mindestens 8 Zeichen
   - Groß- und Kleinbuchstaben enthalten

- Mindestens ein nicht alphabetisches Zeichen enthalten
- Darf nicht mit dem aktuellen Kennwort identisch sein

3. Wählen Sie **Kennwort ändern**, um Ihre Änderungen zu speichern.

Citrix Cloud meldet Sie ab und leitet Sie zur Anmeldeseite weiter.

Active Directory mit Connector Appliance

April 5, 2024

Sie können Connector Appliances verwenden, um einen Ressourcenstandort mit Gesamtstrukturen zu verbinden, die keine Citrix Virtual Apps and Desktops-Ressourcen enthalten. Zum Beispiel im Fall von Citrix Secure Private Access-Kunden oder Citrix Virtual Apps and Desktops-Kunden mit einigen Gesamtstrukturen, die nur für die Benutzerauthentifizierung verwendet werden.

Wenn Sie Active Directory mit mehreren Domänen mit Connector Appliance verwenden, gelten die folgenden Einschränkungen:

- Connector Appliances können nicht anstelle von Cloud Connectors in Gesamtstrukturen verwendet werden, die VDAs enthalten.

Anforderungen

Active Directory-Anforderungen

- Teil einer Active Directory-Domäne, die die Ressourcen und Benutzer enthält, die Sie zum Erstellen von Angeboten für Ihre Benutzer verwenden. Weitere Informationen finden Sie unter Bereitstellungsszenarios für Connector Appliances in Active Directory in diesem Artikel.
- Jede Active Directory-Gesamtstruktur, die für Citrix Cloud verwendet werden soll, muss immer über zwei Connector Appliances erreichbar sein.
- Die Connector Appliance muss Domänencontroller in der Stammdomäne der Gesamtstruktur und in den Domänen, die Sie mit Citrix Cloud verwenden möchten, erreichen können. Weitere Informationen hierzu finden Sie in den folgenden Microsoft-Supportartikeln:
  - Konfigurieren von Domänen und Vertrauensstellungen
  - Abschnitt "Ports für Systemdienste"in Dienstübersicht und Netzwerkportanforderungen für Windows
- Verwenden Sie universelle Sicherheitsgruppen anstelle von globalen Sicherheitsgruppen. Diese Konfiguration stellt sicher, dass die Benutzergruppenzugehörigkeit von jedem Domänencontroller in der Gesamtstruktur bezogen werden kann.

Netzwerkanforderungen

- Mit einem Netzwerk verbunden, über das Zugriff auf die Ressourcen besteht, die Sie am Ressourcenstandort verwenden.
- Eine Verbindung mit dem Internet muss bestehen. Weitere Informationen finden Sie unter Anforderungen an System und Konnektivität.

Zusätzlich zu den unter Kommunikation der Connector Appliance aufgeführten Ports erfordert die Connector Appliance eine ausgehende Verbindung zur Active Directory-Domäne über folgende Ports:

Service	Port	Unterstütztes Domänenprotokoll
Kerberos	88	TCP/UDP
End Point Mapper (DCE/RPC Locator Service)	135	TCP
NetBIOS-Namensdienst	137	UDP
NetBIOS-Datagramm	138	UDP
NetBIOS-Sitzung	139	TCP
LDAP	389	TCP/UDP
SMB über TCP	445	TCP
Kerberos kpasswd	464	TCP/UDP
Globaler Katalog	3268	TCP
Dynamische RPC-Ports	49152–65535	TCP

Das Connectorgerät verwendet LDAP-Signatur zum Sichern von Verbindungen zum Domänencontroller. Dies bedeutet, dass LDAP über SSL (LDAPS) nicht erforderlich ist. Weitere Informationen zur LDAP-Signatur finden Sie unter How to enable LDAP signing in Windows Server und Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing.

Unterstützte Funktionsebenen von Active Directory

Die Connector Appliance wurde getestet und wird durch die folgenden Funktionsebenen für Active Directory-Gesamtstrukturen und -Domänen unterstützt.

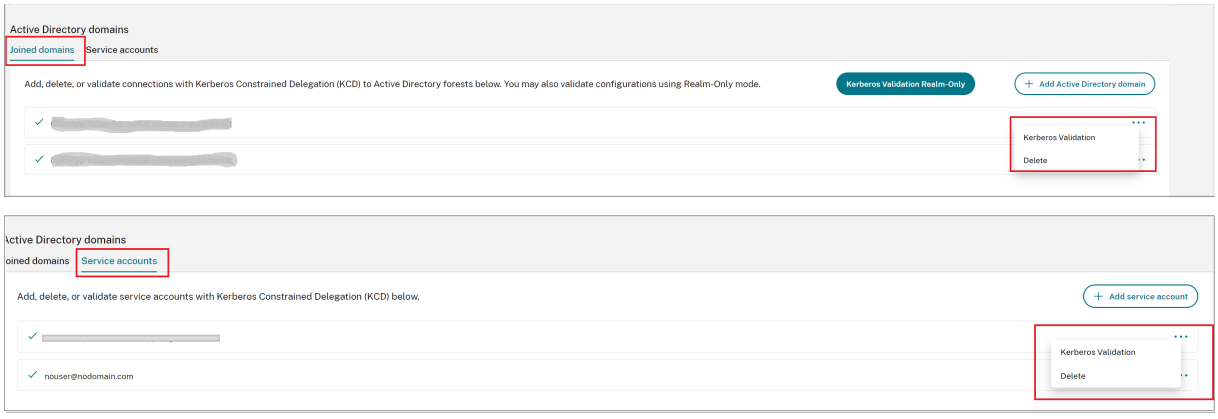
Funktionsebene	Domänenfunktionsebene	Unterstützte Domänencontroller
Windows Server 2016	Windows Server 2016	Windows Server 2019

Andere Kombinationen aus Domänencontroller, Gesamtstrukturfunktionsebene und Domänenfunktionsebene wurden nicht mit der Connector Appliance getestet. Diese Kombinationen sollten jedoch funktionieren und werden unterstützt.

Active Directory-Domäne mit Citrix Cloud über die Connector Appliance verbinden

Wenn Sie eine Verbindung zur Verwaltungswebseite der Connector Appliance herstellen, werden im Abschnitt der Active Directory-Domänen zwei Registerkarten angezeigt.

- **Joined Domains:** Wird verwendet, um die Connector Appliance mit AD-Domänen zu verbinden, indem ein Maschinenkonto für die Appliance in der Domäne erstellt wird. Kerberos kann validiert werden, indem Sie auf die Auslassungspunkte rechts neben der verbundenen Domäne klicken. Das Vorhandensein eines Maschinenkontos in der Domäne ist erforderlich.
- **Service Accounts:** Wird als Teil einer Secure Private Access-Lösung (SPA) verwendet, um Kerberos-SSO über ein Dienstkonto anstelle des Maschinenkontos, das durch den Beitritt zur Domäne erstellt wurde, zu implementieren. Kerberos kann validiert werden, indem Sie auf die Auslassungspunkte rechts neben dem Dienstkonto klicken. Es ist nicht zwingend erforderlich, dass der Maschine eine bestimmte Domäne zugeordnet ist. Selbst wenn die Connector Appliance nicht mit der Domäne verbunden ist, kann sie eine Verbindung zum Domänencontroller herstellen.



Führen Sie die folgenden Schritte aus, um Active Directory für die Verbindung mit Citrix Cloud über die Connector Appliance zu konfigurieren.

1. Installieren Sie eine Connector Appliance an Ihrem Ressourcenstandort.

Sie können den Informationen in der Produktdokumentation zur Connector Appliance folgen.

2. Stellen Sie in Ihrem Browser über die in der Connector Appliance-Konsole angegebene IP-Adresse eine Verbindung zur Connector Appliance-Verwaltungsseite her.
3. Gehen Sie im Abschnitt **Active Directory domains** zur Registerkarte **Joined domains**.
4. Klicken Sie auf **+ Add Active Directory domain**. Ein Popup-Fenster zum Eingeben des Domänennamens wird angezeigt.

   Die Connector Appliance überprüft die Domäne. Wenn die Prüfung erfolgreich ist, wird das Dialogfeld **Active Directory beitreten** geöffnet. In diesem Fenster können Sie den Benutzernamen und das Kennwort für den Domänenbetritt eingeben.
5. Klicken Sie auf **Hinzufügen**.
6. Geben Sie den Benutzernamen und das Kennwort eines Active Directory-Benutzers ein, der über eine Beitrittsberechtigung für die Domäne verfügt.
7. Die Connector Appliance schlägt einen Maschinennamen vor. Sie können den vorgeschlagenen Namen überschreiben und Ihren eigenen Maschinennamen mit einer Länge von bis zu 15 Zeichen angeben.

   Dieser Maschinenname wird in der Active Directory-Domäne erstellt, wenn die Connector Appliance beitritt.
8. Klicken Sie auf **Beitreten**.

   Die Domäne wird jetzt im Abschnitt **Active Directory-Domänen** der Benutzeroberfläche der Connector Appliance aufgeführt.
9. Zum Hinzufügen weiterer **Active Directory-Domänen** wählen Sie **+ Active Directory-Domäne hinzufügen** aus, und wiederholen Sie die vorherigen Schritte.
10. Gehen Sie zur Seite “Domänen”in der **Citrix Cloud-Konsole** und wählen Sie **Connector Appliance**, um Ihre Domänen zu warten.
11. Wenn Sie Ihre Connector Appliance noch nicht registriert haben, fahren Sie mit den unter Connector Appliance bei Citrix Cloud registrieren beschriebenen Schritten fort.

Tritt beim Domänenbeitritt ein Fehler auf, vergewissern Sie sich, dass Ihre Umgebung die Anforderungen an Active Directory und Netzwerk erfüllt.

Nächste Schritte

- Sie können dieser Connector Appliance weitere Domänen hinzufügen.

> **Hinweis:**
>
> Die Connector Appliance wurde mit bis zu 10 Gesamtstrukturen getestet.

- Fügen Sie aus Gründen der Ausfallsicherheit jede Domäne mehr als einer Connector Appliance an jedem Ressourcenstandort hinzu.

Anzeigen der Active Directory-Konfiguration

Sie können die Konfiguration der Active Directory-Domänen und Connector Appliances an Ihren Ressourcenstandorten an folgenden Stellen anzeigen:

- In Citrix Cloud:
  1. Gehen Sie im Menü zur Seite **Identitäts- und Zugriffsverwaltung**.
  2. Gehen Sie zur Registerkarte **Domänen**.

     Ihre Active Directory-Domänen werden mit den Ressourcenstandorten aufgeführt, zu denen sie gehören.
- Auf der Connector Appliance-Webseite:
  1. Stellen Sie über die in der Connector Appliance-Konsole angegebene IP-Adresse eine Verbindung zur Connector Appliance-Webseite her.
  2. Melden Sie sich mit dem Kennwort an, das Sie bei Ihrer ersten Registrierung erstellt haben.
  3. Im Abschnitt **Active Directory-Domänen** der Seite sehen Sie die Liste der Active Directory-Domänen, mit denen diese Connector Appliance verbunden ist.

Active Directory-Domäne von einer Connector Appliance entfernen

Führen Sie die folgenden Schritte aus, um eine Active Directory-Domäne zu verlassen:

1. Stellen Sie über die in der Connector Appliance-Konsole angegebene IP-Adresse eine Verbindung zur Connector Appliance-Webseite her.
2. Melden Sie sich mit dem Kennwort an, das Sie bei Ihrer ersten Registrierung erstellt haben.
3. Suchen Sie im Abschnitt **Active Directory-Domänen** der Seite in der Liste der verbundenen Active Directory-Domänen die Domäne, die Sie verlassen möchten.
4. Notieren Sie den Namen des Maschinenkontos, das von Ihrer Connector Appliance erstellt wurde.
5. Klicken Sie auf das Symbol zum Löschen (Papierkorb) neben der Domäne. Ein Bestätigungsdialogfeld wird angezeigt.
6. Klicken Sie auf **Weiter**, um die Aktion zu bestätigen.

7. Gehen Sie zu Ihrem Active Directory-Controller.
8. Löschen Sie das von Ihrer Connector Appliance erstellte Maschinenkonto aus dem Controller.

Bereitstellungsszenarios für die Verwendung von Connector Appliances mit Active Directory

Sie können sowohl über Cloud Connector als auch Connector Appliances eine Verbindung zu Active Directory-Controllern herstellen. Welche Art von Connector verwendet werden sollte, hängt von Ihrer Bereitstellung ab.

Weitere Informationen zur Verwendung von Cloud Connectors mit Active Directory finden Sie unter Bereitstellungsszenarios für Cloud Connectors in Active Directory.

Verwenden Sie die Connector Appliance, um Ihren Ressourcenstandort in den folgenden Situationen mit der Active Directory-Gesamtstruktur zu verbinden:

- Sie richten Secure Private Access ein. Weitere Informationen finden Sie unter Secure Private Access mit Connector Appliance.
- Eine oder mehrere Ihrer Gesamtstrukturen werden nur für die Benutzerauthentifizierung verwendet.
- Sie möchten die Anzahl der für die Unterstützung mehrerer Gesamtstrukturen erforderlichen Connectors reduzieren.
- Sie benötigen eine Connector Appliance für andere Anwendungsfälle

Nur Benutzer in einer oder mehreren Gesamtstrukturen mit einem einzigen Connector Appliances-Satz für alle Gesamtstrukturen

Dieses Szenario gilt für Kunden der Standardversion von Workspace oder Kunden, die Connector Appliances für Secure Private Access verwenden.

In diesem Szenario gibt es mehrere Gesamtstrukturen, die nur Benutzerobjekte (`forest1.local`, `forest2.local`) enthalten. Diese Gesamtstrukturen enthalten keine Ressourcen. Ein Satz von Connector Appliances wird innerhalb eines Ressourcenstandorts bereitgestellt und mit den Domänen für jede dieser Gesamtstrukturen verbunden.

- Vertrauensstellung: Ohne
- In **Identitäts- und Zugriffsverwaltung** aufgeführte Domänen: `forest1.local`, `forest2.local`
- Benutzeranmeldungen bei Citrix Workspace: Für alle Benutzer unterstützt
- Benutzeranmeldungen bei einem On-Premises-StoreFront: Für alle Benutzer unterstützt

Benutzer und Ressourcen in getrennten Gesamtstrukturen (mit Vertrauensstellung) mit einem einzigen Connector Appliances-Satz für alle Gesamtstrukturen

Dieses Szenario gilt für Kunden von Citrix Virtual Apps and Desktops mit mehreren Gesamtstrukturen.

In diesem Szenario enthalten einige Gesamtstrukturen (`resourceforest1.local`, `resourceforest2.local`) Ihre Ressourcen (z. B. VDAs), und einige Gesamtstrukturen (`userforest1.local`, `userforest2.local`) enthalten nur Ihre Benutzer. Zwischen diesen Gesamtstrukturen besteht eine Vertrauensstellung, sodass Benutzer sich an Ressourcen anmelden können.

Ein Cloud Connector-Satz wird innerhalb der Gesamtstruktur `resourceforest1.local` bereitgestellt. Ein separater Cloud Connector-Satz wird innerhalb der Gesamtstruktur `resourceforest2.local` bereitgestellt.

Ein Connector Appliances-Satz wird innerhalb der Gesamtstruktur `userforest1.local` bereitgestellt, und derselbe Satz wird innerhalb der Gesamtstruktur `userforest2.local` bereitgestellt.

- Vertrauensstellung: Bidirektionale Gesamtstruktur-Vertrauensstellung oder unidirektionale Vertrauensstellung von den Ressourcengesamtstrukturen zu den Benutzergesamtstrukturen
- In **Identitäts- und Zugriffsverwaltung** aufgeführte Domänen: `resourceforest1.local`, `resourceforest2.local`, `userforest1.local`, `userforest2.local`
- Benutzeranmeldungen bei Citrix Workspace: Für alle Benutzer unterstützt
- Benutzeranmeldungen bei einem On-Premises-StoreFront: Für alle Benutzer unterstützt

Connector-Updates

August 3, 2023

In regelmäßigen Abständen veröffentlicht Citrix Updates, um die Leistung, Sicherheit und Zuverlässigkeit des Cloud Connectors oder Connectorgeräts zu erhöhen. Citrix Cloud installiert Updates standardmäßig nacheinander auf jedem Connector, sobald die Updates verfügbar sind. Um sicherzustellen, dass Updates zeitig und ohne übermäßige Störung der Citrix Cloud-Benutzer installiert werden, können Sie Connector-Updates wie folgt steuern:

- Planen von Updates für eine bestimmte Tageszeit und einen bestimmten Wochentag.
- Veranlassen einer einmaligen Verzögerung, sodass die von Ihnen angegebenen Connectors zwei Wochen später als geplant aktualisiert werden.
- Erneutes Starten eines Updates, wenn es aufgrund eines Problems auf der Hostmaschine fehlschlägt, nachdem das Problem behoben wurde.

Sie können auch die aktuelle Connectorversion am Ressourcenstandort mit der Zielversion in Citrix Cloud vergleichen, um zu überprüfen, ob Ihre Connectors auf dem neuesten Stand sind.

> **Hinweis:**
>
> In diesem Artikel wird beschrieben, wie Sie Connector-Updates über die Citrix Cloud-Verwaltungskonsole planen. Informationen zur Planung von Connector-Updates mithilfe von Citrix Cloud-APIs finden Sie in der Citrix Developer-Dokumentation unter Citrix Cloud - Maintenance Schedules.

Bevorzugte Tageszeit

Wenn Sie eine bevorzugte Tageszeit angeben, werden Updates 24 Stunden nach Veröffentlichung zum angegebenen Zeitpunkt von Citrix Cloud installiert. Wenn Ihre bevorzugte Tageszeit beispielsweise 2:00 Uhr US Pacific Time ist und das Update am Dienstag veröffentlicht wird, wartet Citrix Cloud 24 Stunden und installiert das Update am nächsten Tag um 2:00 Uhr.

Bevorzugter Wochentag

Wenn Sie einen bevorzugten Wochentag angeben, wartet Citrix Cloud sieben Tage, bevor Updates am festgelegten Wochentag installiert werden. Damit haben Sie ausreichend Zeit, um zu entscheiden, ob Sie das Update selbst installieren oder warten, bis Citrix Cloud es am bevorzugten Tag installiert. Abhängig vom ausgewählten Wochentag und dem Tag, an dem Updates verfügbar werden, wartet Citrix Cloud also bis zu 13 Tage mit der Installation des Updates.

Beispiel für eine Wartezeit von 8 Tagen

Am Montag konfigurieren Sie “Dienstag 18:00 Uhr”als bevorzugte Updatezeit. Später am Tag erhalten Sie eine Update-Benachrichtigung in Citrix Cloud und es wird die Schaltfläche **Aktualisieren** angezeigt. Wenn Sie das Update nicht starten, wartet Citrix Cloud sieben Tage und installiert das Update dann am nächsten Dienstag um 18.00 Uhr.

Beispiel für eine Wartezeit von 13 Tagen

Sie haben “Montag 18:00 Uhr”als bevorzugte Updatezeit konfiguriert. Am Dienstag erhalten Sie eine Update-Benachrichtigung in Citrix Cloud und es wird die Schaltfläche **Aktualisieren** angezeigt. Wenn Sie das Update nicht starten, wartet Citrix Cloud sieben Tage und installiert das Update dann sechs Tage später, am Montag um 18.00 Uhr.

Update-Benachrichtigungen und manuell gestartete Updates

Verfügbare Updates werden von Citrix Cloud in Ihren Benachrichtigungen angezeigt. Für jeden Connector wird zudem die geplante Updatezeit angezeigt.

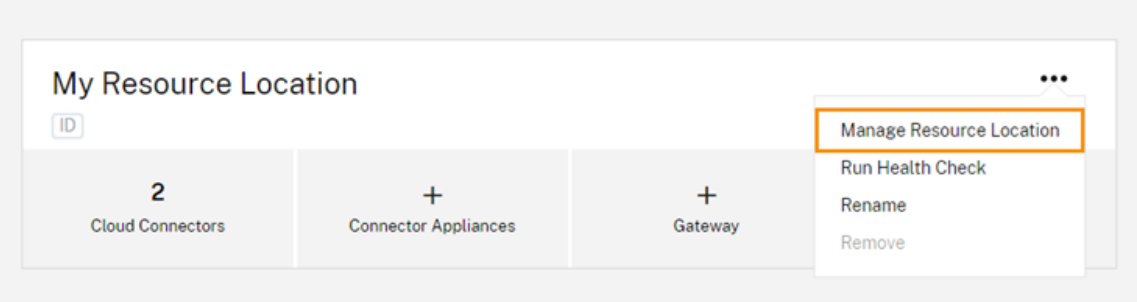
Nachdem Citrix Cloud Sie über ein verfügbares Update benachrichtigt hat, wird für jeden Connector eine Schaltfläche **Aktualisieren** angezeigt, sodass Sie das Update schon vor dem bevorzugten Termin installieren können. Nachdem Sie **Aktualisieren** für jeden Connector ausgewählt haben, werden die Updates von Citrix Cloud in eine Warteschlange gestellt und nacheinander installiert. Gestartete Updates können nicht mehr abgebrochen werden.

Nach Abschluss des Updates zeigt Citrix Cloud das Datum des letzten Updates an. Wenn Updates nicht abgeschlossen werden konnten, werden Sie darüber in einer Benachrichtigung informiert.

Auswahl eines Aktualisierungszeitplans

Gehen Sie wie in diesem Abschnitt beschrieben vor, um Connector-Updates über die Citrix Cloud-Verwaltungskonsole zu planen. Informationen zur Planung von Updates mithilfe von Citrix Cloud-APIs finden Sie in der Citrix Developer-Dokumentation unter Citrix Cloud - Maintenance Schedules.

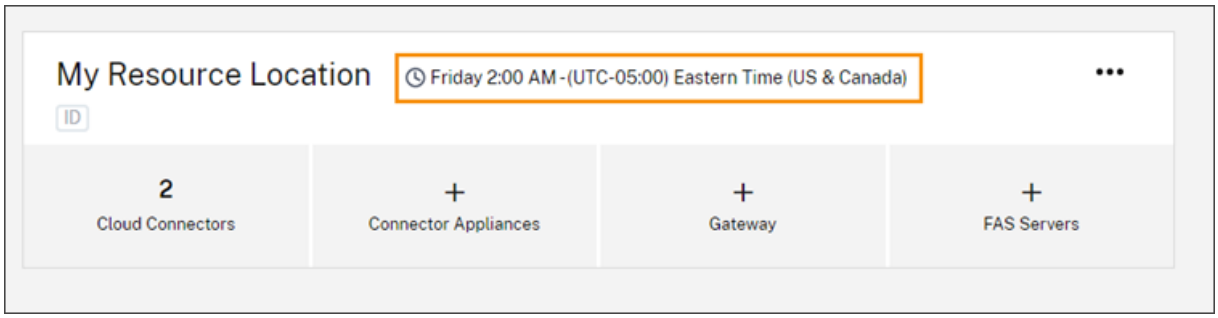
1. Wählen Sie im Citrix Cloud-Menü die Option **Ressourcenstandorte**.
2. Suchen Sie den Ressourcenstandort, den Sie ändern möchten, klicken Sie auf die Auslassungspunkte (…) und wählen Sie **Ressourcenstandort verwalten**.



3. Wählen Sie unter **Updatemethode wählen** die Option **Startzeit für Wartung festlegen** und wählen Sie den bevorzugten Wochentag sowie Uhrzeit und Zeitzone für die Installation von Updates aus.

    - Um nur eine bevorzugte Tageszeit anzugeben, wählen Sie Uhrzeit und Zeitzone, zu der Updates installiert werden sollen. Citrix Cloud wartet 24 Stunden nach Veröffentlichung und installiert Updates dann zum von Ihnen festgelegten Zeitpunkt.
    - Um einen bevorzugten Wochentag festzulegen, wählen Sie Uhrzeit, Tag und Zeitzone. Citrix Cloud wartet sieben Tage nach Veröffentlichung und installiert Updates dann am gewünschten Wochentag.

Die konfigurierte Updatezeit wird in Citrix Cloud neben dem Namen des Ressourcenstandorts angezeigt.



Die ausgewählte Startzeit wird auf alle Connectors angewendet, unabhängig von der Zeitzone, in der sie sich befinden. Bei Connectors in unterschiedlichen Zeitzonen installiert Citrix Cloud die Updates zu dem Zeitpunkt und in der Zeitzone, die Sie ausgewählt haben. Wenn Sie beispielsweise Updates für 2:00 Uhr US-Pazifikzeit planen und auch Connectors in London haben, startet Citrix Cloud die Installation des Updates auf diesen Connectors um 2:00 Uhr US-Pazifikzeit.

Updates neu starten

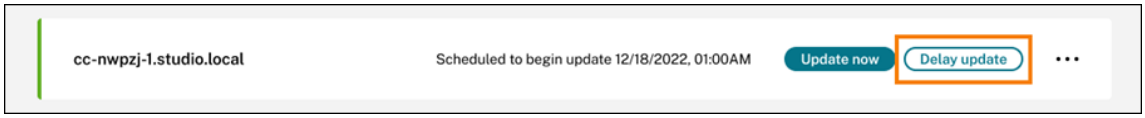
Wenn beim Connector während der Installation des Updates ein Problem auftritt, wird die Installation angehalten, bis das Problem behoben ist. Da Updates auf jedem Connector einzeln installiert werden, kann ein angehaltenes Update auf einem Connector die Updateinstallation auf allen verbleibenden Cloud Connectors in Ihrem Citrix Cloud-Konto verhindern. Wenn das Problem behoben ist, können Sie das Update erneut starten.

1. Wählen Sie im Citrix Cloud-Menü die Option **Ressourcenstandorte**.
2. Suchen Sie den Ressourcenstandort, den Sie verwalten möchten, und wählen Sie die Kachel **Cloud Connectors** oder **Connector-Geräte**.
3. Suchen Sie den Connector, den Sie verwalten möchten, und wählen Sie **Update neu starten**.

Updates verschieben

Sie können ein geplantes Update für ausgewählte Connectors um zwei Wochen verschieben. Sie können ein geplantes Update nur einmal verschieben. Wenn Sie das Update einmal verschoben haben, können Sie es nicht erneut verschieben. Außerdem können Sie den Standardzeitraum von zwei Wochen nicht ändern.

1. Wählen Sie im Citrix Cloud-Menü die Option **Ressourcenstandorte**.
2. Suchen Sie den Ressourcenstandort, den Sie verwalten möchten, und wählen Sie die Kachel **Cloud Connectors** oder **Connector-Geräte**.
3. Suchen Sie den Connector, den Sie verwalten möchten, und wählen Sie **Update verzögern**.



Das geplante Datum wird durch das zwei Wochen später liegende Datum ersetzt.

Ungeplante Updates

Selbst wenn Sie Updates für später geplant haben, installiert Citrix Cloud ein Update u. U. sobald es verfügbar ist. Ungeplante Updates treten in folgenden Fällen auf:

- Das Update kann nicht innerhalb von 48 Stunden nach Veröffentlichung zum bevorzugten Zeitpunkt installiert werden. Wenn Ihre bevorzugte Zeit beispielsweise 2:00 Uhr und der Connector nach Veröffentlichung des Updates drei Tage lang offline ist, installiert Citrix Cloud das Update, sobald der Connector wieder online ist.
- Das Update enthält einen Fix für ein kritisches Sicherheits- oder Funktionsproblem.

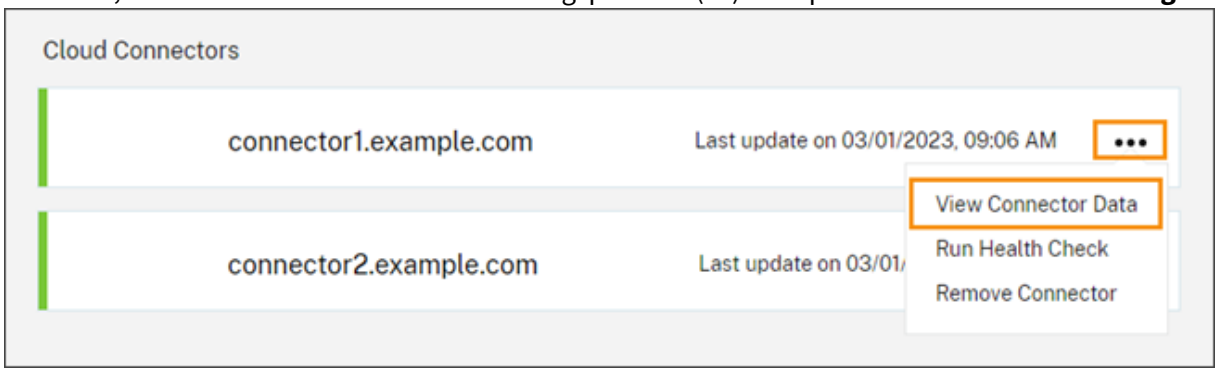
Vergleich von Cloud Connector-Versionen

Sie können überprüfen, welche Cloud Connector-Version an Ihrem Ressourcenstandort ausgeführt wird und ob es die aktuelle Version ist. Mit diesen Informationen können Sie sicherstellen, dass der Cloud Connector erfolgreich aktualisiert wird.

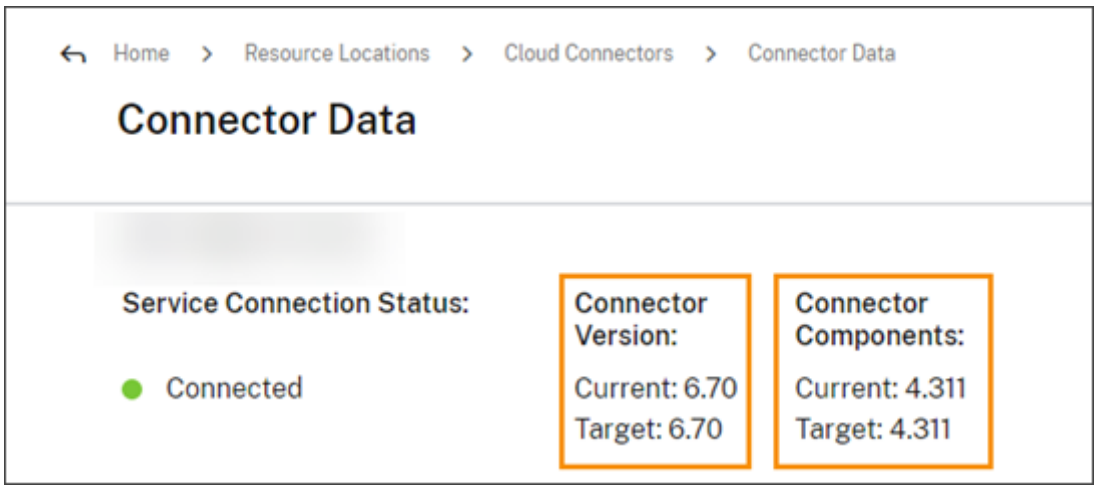
> **Hinweis:**
>
> Diese Informationen sind für Connectorgeräte nicht verfügbar.

Wählen Sie auf der Seite **Ressourcenstandorte** die Kachel **Cloud Connectors** für den Ressourcenstandort, den Sie verwalten möchten. Suchen Sie den Cloud Connector, den Sie untersuchen

möchten, und wählen Sie unter den Auslassungspunkten (…) die Option **Connectordaten anzeigen**.



Die **aktuelle Versionsnummer** ist die Version der Cloud Connector-Software, die derzeit auf der Cloud Connector-Maschine ausgeführt wird. Die **Zielversionsnummer** ist die neueste Version der Cloud Connector-Software, die von Citrix veröffentlicht wurde. Wurde die Maschine erfolgreich aktualisiert, stimmen aktuelle Versionsnummer und Zielversionsnummer überein.



Problembehandlung bei Updatefehlern

Konflikte bei der auf der Cloud Connector-Maschine installierten Software oder Fehler bei der Wartung können dazu führen, dass Cloud Connector-Updates fehlschlagen und Serviceausfälle auftreten. Informationen zum Vorgehen bei einem fehlgeschlagenen Update nach der Cloud Connector-Wartung finden Sie unter Behebung von Fehlern bei der Cloud Connector-Wartung.

Wenn der Cloud Connector nicht erfolgreich aktualisiert wird, können Sie zur Problembehandlung zunächst folgende Bedingungen überprüfen:

- Der Cloud Connector ist eingeschaltet und mit dem Hilfsprogramm zur Cloud Connector-Konnektivitätsprüfung mit Citrix Cloud verbunden.
- Proxy und Firewalls sind ordnungsgemäß konfiguriert.
- Erforderliche Windows-Dienste haben den Status "Gestartet".

- Die erweiterte Protokollierung ist auf dem Cloud Connector aktiviert.

Anweisungen zur Problembehandlung bei Cloud Connector- Updatefehlern finden Sie unter CTX270718 im Citrix Support Knowledge Center.

Zur Unterstützung bei der Problembehandlung können Sie Citrix Cloud Connector-Protokolle an Citrix senden. Weitere Informationen finden Sie unter Protokollsammlung für Citrix Cloud Connector.

Identitäts- und Zugriffsverwaltung

July 2, 2024

Die Identitäts- und Zugriffsverwaltung definiert die Identitätsanbieter und Konten, die für Citrix Cloud-Administratoren und Workspace-Abonnenten verwendet werden.

Identitätsanbieter

Für die Authentifizierung von Citrix Cloud-Administratoren, Workspace-Abonnenten oder beiden können für Citrix Cloud unterstützte Identitätsanbieter verwendet werden.

Identitätsanbieter	Administratorauthentifizierung	Abonnentenauthentifizierung
Citrix-Identitätsanbieter	Ja	Nein
On-Premises-Active Directory	Nein	Ja
Active Directory plus Token	Nein	Ja
Azure Active Directory	Ja	Ja
Citrix Gateway	Nein	Ja
Google Cloud Identity	Ja	Ja
Okta	Nein	Ja
SAML 2.0	Ja (nur AD-Gruppen)	Ja

Standardmäßig verwendet Citrix Cloud den Citrix Identitätsanbieter zur Verwaltung Ihres Citrix Cloud-Kontos. Der Citrix Identitätsanbieter authentifiziert nur Citrix Cloud-Administratoren.

Citrix-Identitätsanbieter

Citrix Cloud enthält den integrierten Citrix-Identitätsanbieter, um Administratoren bei der Anmeldung zu authentifizieren. In der Citrix Cloud-Konsole trägt der Citrix-Identitätsanbieter die Bezeichnung Cit-

rix Identity.
Wenn Sie einen anderen Identitätsanbieter für die Administratorauthentifizierung verwenden, empfiehlt Citrix, mindestens einen Administrator mit vollem Zugriff unter dem **Citrix-Identitätsanbieter** zu haben. Diese Bedingung stellt Folgendes sicher:

- Sie werden nicht von Ihrem Citrix Cloud-Konto gesperrt, wenn Ihr primärer Identitätsanbieter nicht mehr verfügbar ist.
- Sie können auf Ihr Citrix Cloud-Konto zugreifen, um bestimmte Vorgänge auszuführen, die nicht abgeschlossen werden können, wenn Sie bei einem anderen Identitätsanbieter wie Azure AD angemeldet sind. Wenn Azure AD beispielsweise Ihr ausgewählter Identitätsanbieter ist und Sie die Verbindung zwischen Ihrem Azure AD und Citrix Cloud erneut herstellen müssen, können Sie diese Aufgabe ausführen, nachdem Sie sich mit dem Citrix-Identitätsanbieter angemeldet haben.

Citrix-Identitätsanbieter entfernen

Der Citrix-Identitätsanbieter ist standardmäßig für alle neuen Citrix Cloud-Konten verbunden. Wenn Sie den Citrix-Identitätsanbieter nicht verwenden möchten, können Sie die Verbindung bei Bedarf entfernen. Beispielsweise können Sie diese Verbindung entfernen, um die Richtlinien Ihrer Organisation für Sicherheit und Administratorverwaltung einzuhalten.

Durch das Entfernen dieser Verbindung wird der Citrix-Identitätsanbieter deaktiviert, sodass er nicht zur Authentifizierung von Citrix Cloud-Administratoren verwendet werden kann.

Bevor Sie die Verbindung zum Citrix-Identitätsanbieter entfernen können, muss ein anderer Identitätsanbieter in Citrix Cloud konfiguriert sein. In Citrix Cloud können Sie diese Verbindung nur entfernen, wenn ein anderer konfigurierter Identitätsanbieter vorhanden ist.

> **Wichtig**
>
> Wenn Sie den Zugriff auf den von Ihnen ausgewählten Identitätsanbieter verlieren, müssen Sie sich an den Citrix Support wenden, um Ihr Citrix Cloud-Konto wiederherzustellen. Dieser Vorgang kann mehrere Tage in Anspruch nehmen.

So entfernen Sie die Verbindung zum Citrix-Identitätsanbieter:

1. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.
2. Suchen Sie auf der Registerkarte **Authentifizierung** den Citrix-Identitätsanbieter.
3. Klicken Sie auf das Dreipunktmenü und wählen Sie **Identitätsanbieter löschen** aus.

4. Wenn Sie aufgefordert werden, das Löschen zu bestätigen, wählen Sie **Ich verstehe, dass beim Löschen dieses Identitätsanbieters auch die Konfigurationsdaten für diesen Identitätsanbieter in Citrix Cloud gelöscht werden**.
5. Klicken Sie auf **Identitätsanbieter löschen**.

Citrix Verbundauthentifizierungsdienst

Citrix Cloud unterstützt auch den Citrix Verbundauthentifizierungsdienst (FAS) zum Single Sign-On für Workspace-Abonnenten. Weitere Informationen hierzu finden Sie in den folgenden Artikeln:

- Verbinden von FAS mit Citrix Cloud: Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst (FAS)
- Citrix Tech Zone:
  - Referenzarchitektur: Übersicht über die Architekturen des Verbundauthentifizierungsdienst
  - Tech Insight: Federated Authentication Service

Administratoren

Administratoren können mit ihrer Identität auf Citrix Cloud zuzugreifen, Verwaltungsaktivitäten ausführen und den Citrix Cloud Connector installieren.

Ein Citrix Identitätsmechanismus ermöglicht Administratoren die Authentifizierung per E-Mail-Adresse und Kennwort. Administratoren können sich auch mit den My Citrix-Anmeldeinformationen bei Citrix Cloud anmelden.

Multifaktorauthentifizierung

Citrix Cloud bietet Methoden zur Multifaktorauthentifizierung für Administratoren und für Workspace-Abonnenten.

Für Administratoren ist die Anmeldung bei Citrix Cloud mit Multifaktorauthentifizierung obligatorisch. Administratoren können ihr Gerät beim Onboarding ihres Citrix Cloud-Kontos registrieren oder nachdem sie die Einladung eines anderen Administrators angenommen haben. Weitere Informationen finden Sie in den folgenden Artikeln:

- Multifaktorauthentifizierung einrichten
- Primäre MFA-Methode verwalten
- MFA-Wiederherstellungsmethoden verwalten

Für Workspace-Abonnenten ist die Multifaktorauthentifizierung aktiviert, wenn Administratoren die Authentifizierungsmethode "Active Directory plus Token"konfigurieren. "Active Directory plus Token" ist der Standardidentitätsanbieter für Citrix Workspace. Nach der Konfiguration registrieren Abonnenten ihr Gerät für die Multifaktorauthentifizierung. Weitere Informationen finden Sie in den folgenden Artikeln:

- Authentifizierung über Active Directory plus Token aktivieren
- Gerät für die Zweifaktorauthentifizierung registrieren
- Erneute Registrierung von Geräten

Alternativ können Sie die Multifaktorauthentifizierung mit Azure AD für Citrix Cloud-Administratoren und für Workspace-Abonnenten verwenden. Weitere Informationen zu Bereitstellungsmethoden finden Sie unter Microsoft Azure MFA deployment methods.

Administratoren hinzufügen

Beim Onboarding eines Kontos wird ein anfänglicher Administrator erstellt. Als Erstadministrator können Sie weitere Administratoren zu Ihrem Citrix Cloud-Konto hinzufügen. Die neuen Administratoren können vorhandene Citrix-Anmeldeinformationen verwenden oder bei Bedarf ein neues Konto einrichten. Sie können auch die Zugriffsberechtigungen der von Ihnen hinzugefügten Administratoren anpassen. Durch Festlegen dieser Berechtigungen können Sie den Zugriff auf der Basis der Rolle des Administrators in Ihrer Organisation festlegen.

Weitere Informationen zum Hinzufügen von Administratoren und zum Festlegen von Zugriffsberechtigungen finden Sie unter Administratorzugriff verwalten.

Kennwort zurücksetzen

Wenn Sie Ihr Kennwort vergessen haben oder zurücksetzen möchten, klicken Sie auf der Citrix Cloud-Anmeldeseite auf **Benutzername oder Kennwort vergessen?**. Nachdem Sie Ihre E-Mail-Adresse oder Ihren Benutzernamen zur Suche Ihres Kontos eingegeben haben, erhalten Sie eine E-Mail von Citrix mit einem Link zum Zurücksetzen Ihres Kennworts.

Citrix erfordert unter bestimmten Bedingungen eine Rücksetzung Ihres Kennworts, damit dessen Sicherheit geschützt wird. Weitere Informationen zu diesen Bedingungen finden Sie unter Ändern Ihres Kennworts.

> **Hinweis:**
>
> Fügen Sie Ihrer Liste zulässiger E-Mail-Adressen den Eintrag **customerservice@citrix.com** hinzu, damit E-Mail-Nachrichten von Citrix Cloud nicht in Ihrem Spamordner oder Papierkorb landen.

Entfernen von Administratoren

Sie können Administratoren aus Ihrem Citrix Cloud-Konto über die Registerkarte **Administrator** entfernen. Wenn Sie einen Administrator entfernen, kann dieser sich nicht mehr bei Citrix Cloud anmelden.

Ist der Administrator angemeldet, während sein Konto entfernt wird, bleibt er maximal eine Minute lang aktiv. Danach wird der Zugriff auf Citrix Cloud verweigert.

> **Hinweis:**
>
> - Wenn ein Konto nur einen Administrator hat, können Sie diesen nicht entfernen. Bei Citrix Cloud ist mindestens ein Administrator pro Kundenkonto erforderlich.
> - Citrix Cloud Connectors sind nicht mit Administratorkonten verknüpft. Cloud Connectors werden somit auch dann ausgeführt, wenn Sie den Administrator entfernen, der sie installiert hat.

Abonnenten

Die Identität der Abonnenten legt fest, auf welche Citrix Cloud-Services sie zugreifen können. Die Identität entstammt Active Directory-Domänenkonten, die über die Domänen im Ressourcenstandort bereitgestellt werden. Die Zuweisung eines Abonnenten zu einem Bibliotheksangebot berechtigt ihn zum Zugriff auf das Angebot.

Administratoren können auf der Registerkarte **Domänen** vorgeben, welche Domänen zum Bereitstellen der Identitäten verwendet werden sollen. Wenn Sie Domänen aus mehreren Gesamtstrukturen verwenden möchten, installieren Sie mindestens zwei Citrix Cloud Connectors in jeder Gesamtstruktur. Citrix empfiehlt den Einsatz von mindestens zwei Citrix Cloud Connectors in einer Umgebung, um eine hohe Verfügbarkeit zu gewährleisten. Weitere Informationen zum Bereitstellen von Cloud Connectors in Active Directory finden Sie unter Bereitstellungsszenarios für Cloud Connectors in Active Directory.

> **Hinweis:**
>
> - Das Deaktivieren von Domänen verhindert nur die Auswahl neuer Identitäten. Bereits zugewiesene Identitäten können von den Abonnenten weiterhin verwendet werden.

> - Jeder Citrix Cloud Connector kann sämtliche Domänen aus der Gesamtstruktur, in der er installiert ist, auflisten und verwenden.

Verwalten der Nutzung durch Abonnenten

Sie können einzelne Konten oder Active Directory-Gruppen verwenden, um Abonnenten zu Angeboten hinzuzufügen. Bei Verwendung von Active Directory-Gruppen ist nach deren Zuweisung zu einem Angebot keine Verwaltung über Citrix Cloud mehr erforderlich.

Wenn ein Administrator Abonnenten oder Abonnentengruppen aus einem Angebot entfernt, können die Abonnenten nicht mehr auf den Service zugreifen. Weitere Informationen zum Entfernen von Abonnenten aus Services finden Sie in der Dokumentation des jeweiligen Service auf der Website mit der Citrix Produktdokumentation.

Primäre Ressourcenstandorte

Ein primärer Ressourcenstandort ist ein Ressourcenstandort, den Sie für die Kommunikation zwischen Ihrer Domäne und Citrix Cloud als "bevorzugt"festlegen. Wählen Sie als primären Ressourcenstandort den Ressourcenstandort, der Citrix Cloud Connectors mit der besten Leistung und Konnektivität zu Ihrer Domäne hat. Wenn Sie diesen Ressourcenstandort zu Ihrem primären Ressourcenstandort machen, können Benutzer sich schnell bei Citrix Cloud anmelden.

Weitere Informationen finden Sie unter Primären Ressourcenstandort wählen.

Weitere Informationen

- Im Kurs Introduction to Citrix Identity and Authentication auf der Citrix Training-Website erfahren Sie mehr über unterstützte Identitätsanbieter.
- Citrix Tech Zone:
  - Tech Brief: Workspace Identity
  - Tech Brief: Workspace Single Sign-On
  - Tech Insight: Mobile SSO

Administratorzugriff auf Citrix Cloud verwalten

April 5, 2024

Administratoren werden über die Citrix Cloud-Konsole verwaltet. Je nachdem, welchen Identitätsanbieter Sie zur Authentifizierung von Administratoren verwenden, können Sie Administratoren einzeln oder in Gruppen hinzufügen.

Für alle Citrix Cloud-Administratoren, die sich bei Citrix Cloud anmelden, ist die Verwendung von Token als zweite Stufe der Authentifizierung erforderlich. Nachdem Sie einen Administrator hinzugefügt haben, kann dieser sein Gerät für die Multifaktorauthentifizierung registrieren und Token mit einer beliebigen App generieren, die dem Standard Zeitbasiertes Einmalkennwort entspricht, z. B. Citrix SSO oder Google Authenticator.

Administratoren hinzufügen

Citrix Cloud unterstützt die folgenden Identitätsanbieter für die Authentifizierung von Administratoren:

- Citrix Identitätsanbieter: Standardidentitätsanbieter in Citrix Cloud. Unterstützt nur das Hinzufügen einzelner Administratoren.
- Azure AD: Unterstützt das Hinzufügen einzelner Administratoren und von AAD-Gruppen. Administratoren in AAD-Gruppen sind nur auf benutzerdefinierte Zugriffsrollen beschränkt. Weitere Informationen finden Sie unter Administratorgruppen verwalten.
- SAML 2.0: Unterstützt nur das Hinzufügen von Administratoren in AD-Gruppen. Weitere Informationen finden Sie unter Verbinden von SAML als Identitätsanbieter mit Citrix Cloud.

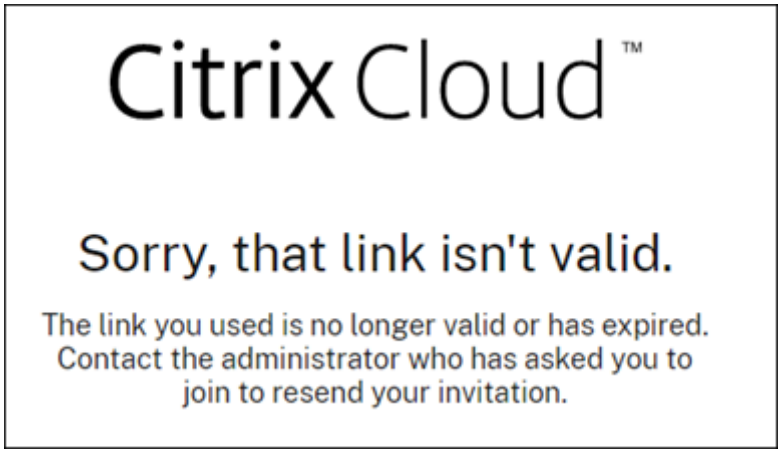
Der Workflow beim Hinzufügen neuer Administratoren ist wie folgt:

1. Sie wählen den Identitätsanbieter aus, den Sie für die Authentifizierung von Administratoren verwenden möchten.
2. Sie laden je nach Identitätsanbieter einzelne Administratoren ein oder wählen die Gruppen aus, zu denen die Administratoren gehören.
3. Sie geben die Zugriffsberechtigungen an, die für die Rollen der Administratoren in Ihrer Organisation geeignet sind. Weitere Hinweise zu Administratorrechten finden Sie unter Ändern von Administratorberechtigungen im vorliegenden Artikel.

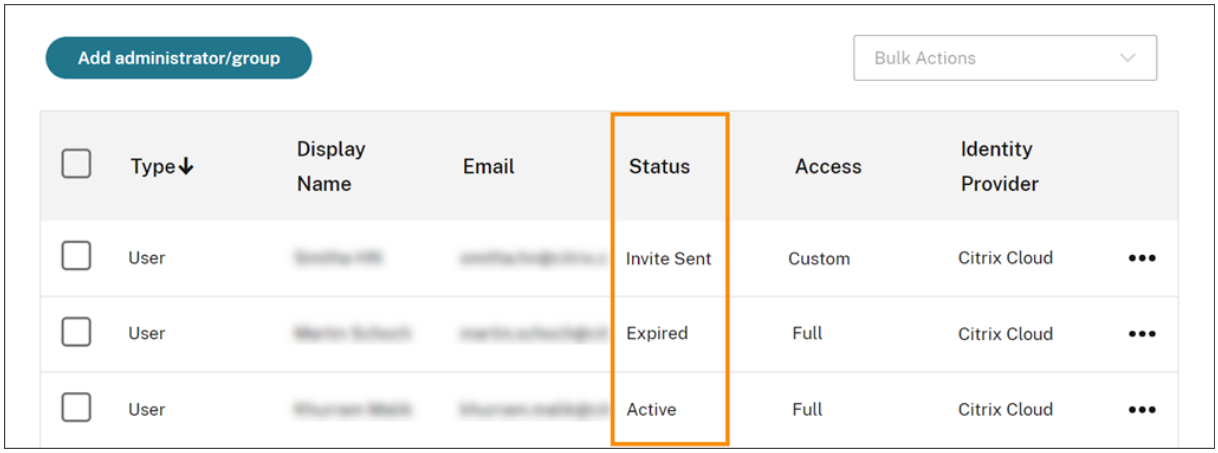
Einladen einzelner Administratoren

Um einzelne Administratoren hinzuzufügen, müssen Sie sie einladen, Ihrem Citrix Cloud-Konto beizutreten. Wenn Sie einen Administrator hinzufügen, sendet Citrix ihm eine Einladungs-E-Mail. Bevor sich der Administrator anmelden kann, muss er die Einladung annehmen. Administratoren, die Sie in Gruppen hinzufügen, erhalten keine Einladung und können sich sofort anmelden, nachdem Sie sie hinzugefügt haben.

Einladungs-E-Mails werden von `cloud@citrix.com` gesendet und enthalten Anweisungen für den Zugriff auf das Konto. Die Einladung ist ab dem Tag des Versands fünf Tage lang gültig. Nach Ablauf von fünf Tagen wird der Einladungslink ungültig. Wenn der eingeladene Administrator den abgelaufenen Link verwendet, wird von Citrix Cloud eine entsprechende Meldung angezeigt.



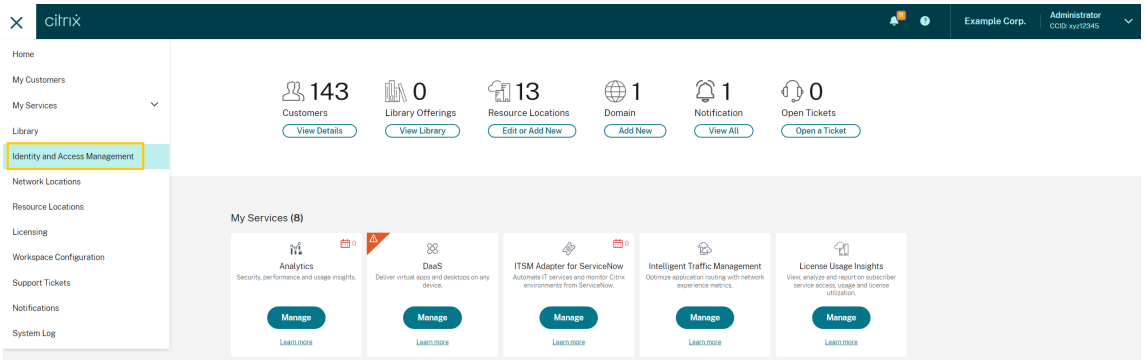
In Citrix Cloud wird außerdem der Status der Einladung angezeigt, damit Sie sehen können, ob der Administrator sie angenommen und sich bei Citrix Cloud angemeldet hat.



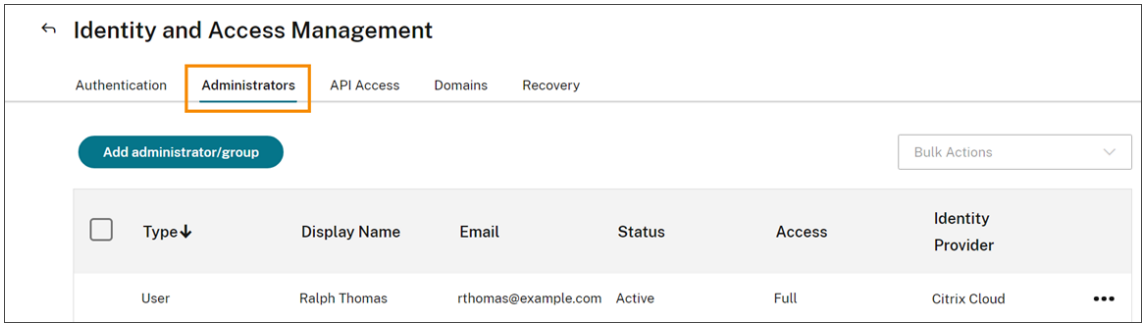
> **Hinweis**
>
> Administratorkonten können mit bis zu 100 Kundenkonten verknüpft werden. Wenn ein Administrator mehr als 100 Kundenkonten verwalten muss, muss er ein separates Administratorkonto mit einer anderen E-Mail-Adresse erstellen, um die zusätzlichen Kunden zu verwalten. Alternativ können Sie den Administrator aus Kundenkonten entfernen, die sie nicht mehr verwalten müssen.

Einladen eines Administrators

1. Melden Sie sich bei Citrix Cloud an und wählen Sie im Menü **Identitäts- und Zugriffsverwaltung**.



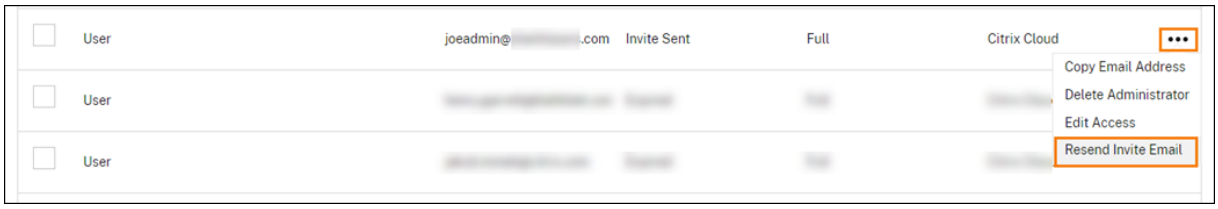
2. Wählen Sie auf der Seite **Identitäts- und Zugriffsverwaltung** die Option **Administratoren**. Es werden alle aktuellen Administratoren im Konto angezeigt.



3. Wählen Sie **Administrator/Gruppe hinzufügen**.
4. Wählen Sie unter **Administratordetails** den Identitätsanbieter aus, den Sie verwenden möchten. Wenn Sie Azure AD verwenden, werden Sie von Citrix Cloud möglicherweise aufgefordert, sich zuerst anzumelden.
5. Bei Auswahl von **Citrix Identität** geben Sie die E-Mail-Adresse des Benutzers ein und wählen dann **Weiter**.
6. Bei Auswahl von **Azure Active Directory** geben Sie den Namen des Benutzers ein, den Sie hinzufügen möchten, und klicken dann auf **Weiter**. Das Einladen von AAD-Gastbenutzern wird nicht unterstützt.
7. Konfigurieren Sie unter **Zugriff festlegen** die Zugriffsberechtigungen für den Administrator. **Vollzugriff** (standardmäßig ausgewählt) ermöglicht die Steuerung aller Citrix Cloud-Funktionen und abonnierten Services. **Benutzerdefinierter Zugriff** ermöglicht die Steuerung der von Ihnen ausgewählten Funktionen und Services.
8. Überprüfen Sie die Administratordetails. Wählen Sie **Zurück**, um Änderungen vorzunehmen.
9. Wählen Sie **Einladung senden**. Citrix Cloud sendet eine Einladung an den Benutzer und fügt den Administrator der Liste hinzu.

Erneutes Senden einer Einladung

Um die Einladung erneut zu senden, wählen Sie über die Auslassungspunkte rechts in der Konsole die Option **Einladungs-E-Mail erneut senden**. Das erneute Senden einer Einladung hat keinen Einfluss auf die Frist von fünf Tagen bis Ablauf der Einladung.



Erneutes Senden einer Einladung mit neuem Anmeldelink

Wenn die ursprüngliche Einladungs-E-Mail abläuft, können Sie eine neue an den Administrator senden. Gehen Sie wie folgt vor:

1. Löschen Sie den Administrator aus Citrix Cloud: Suchen Sie auf der Seite **Administratoren** den Administrator in der Liste und wählen Sie dann über die Auslassungspunkte die Option **Administrator löschen**.
2. Warten Sie mehrere Minuten ab, um sicherzustellen, dass Citrix Cloud den Löschvorgang abgeschlossen hat. Eine erneute Einladung des Administrators unmittelbar nach dem Löschen kann u. U. dazu führen, dass die Einladung mit einem fehlerhaften Anmeldelink gesendet wird.
3. Laden Sie den Administrator erneut ein (siehe Einladen eines Administrators).

Annehmen einer Administratoreinladung

Wenn Sie zu einem Citrix Cloud-Konto eingeladen werden, sendet Citrix Ihnen eine E-Mail mit der Organisations-ID und dem Kundennamen des Kontos.

Um die Einladung anzunehmen, klicken Sie auf **Anmelden**. Danach öffnet sich ein Browserfenster. Wenn Sie noch kein Citrix Cloud-Konto haben, wird eine Seite zum Erstellen des Kennworts angezeigt. Wenn Sie bereits ein Konto haben, fordert Citrix Cloud Sie auf, Ihr Kennwort für die Anmeldung zu verwenden.

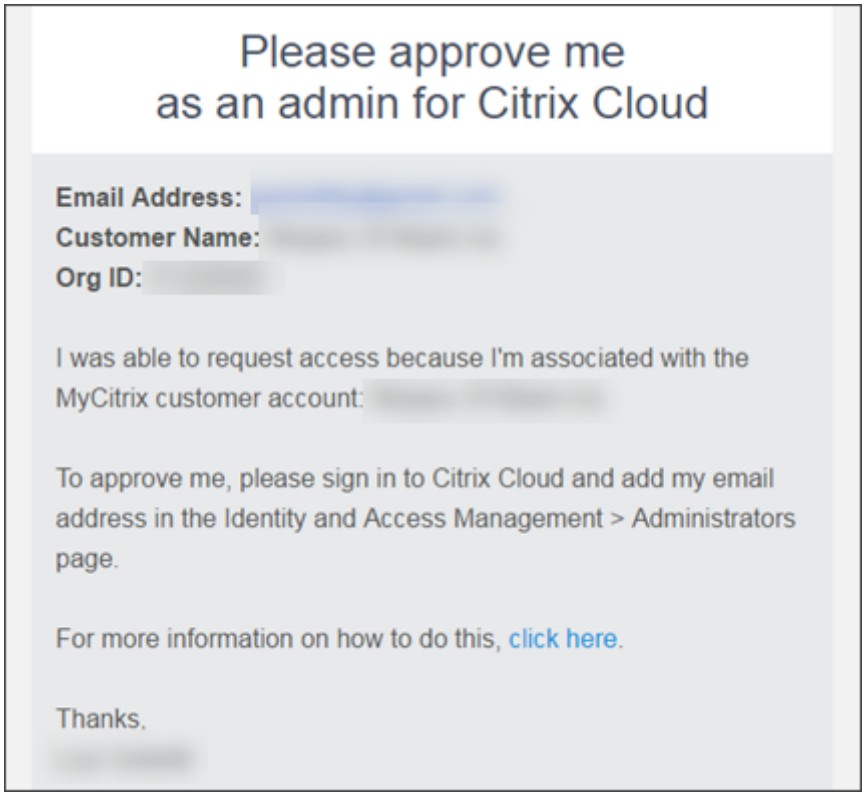
Während der Anmeldung werden Sie möglicherweise aufgefordert, sich für die Multifaktorauthentifizierung zu registrieren. Anweisungen zur Registrierung finden Sie unter Multifaktorauthentifizierung einrichten.

Administratorgruppen hinzufügen

Sie können Administratoren in AD-Gruppen (für die SAML-Authentifizierung) oder Azure AD-Gruppen (für die Azure AD-Authentifizierung) hinzufügen. Weitere Informationen finden Sie unter Administratorgruppen verwalten.

Beitrittsanforderungen für Citrix Cloud genehmigen

Gelegentlich können Sie von Citrix Cloud eine Genehmigungsanforderung erhalten, da eine Person in Ihrer Organisation Ihrem Citrix Cloud-Konto als Administrator beitreten möchte.



Zum Genehmigen dieser Anforderungen senden Sie eine Einladung an die Person, die den Zugriff als Administrator beantragt, wie in diesem Artikel unter Einzelne Administratoren einladen beschrieben. Sie müssen dieselbe E-Mail-Adresse verwenden, die in der E-Mail mit der Genehmigungsanforderung angegeben ist.

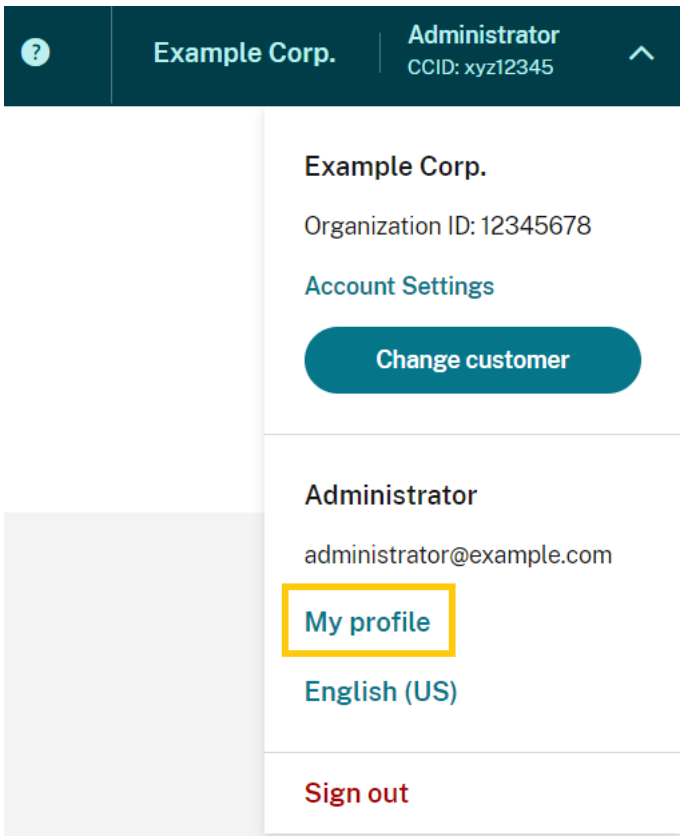
Nach dem Empfang der Einladung klickt die Person, die den Zugriff beantragt, auf den Link **Anmelden**, um die Einladung anzunehmen. Die Person kann dann ein Kennwort für Citrix Cloud erstellen und sich bei Ihrem Konto anmelden.

Weitere Informationen zum Erstellen von Genehmigungsanforderungen finden Sie unter Was passiert, wenn das Konto bereits verwendet wird?.

E-Mail-Adresse ändern

Sie können Ihre eigene E-Mail-Adresse in Citrix Cloud ändern. Ihre neue Adresse muss sich von Ihrer Wiederherstellungs-E-Mail-Adresse für die Multifaktorauthentifizierung (MFA) unterscheiden. Wenn Sie Ihre E-Mail-Adresse ändern, sendet Citrix Cloud eine Verifizierungs-E-Mail an die neue Adresse. Nach der Verifizierung werden Sie abgemeldet, damit die Änderung abgeschlossen werden kann. Nach ein paar Minuten können Sie sich mit der neuen E-Mail-Adresse neu anmelden.

1. Wählen Sie im Menü oben rechts **Meine Einstellungen** aus.



2. Wählen Sie unter **E-Mail-Adresse** die Option **E-Mail-Adresse ändern**.
3. Geben Sie die neue E-Mail-Adresse ein und wählen Sie **Verifizierungs-E-Mail senden**.
4. Geben Sie den 6-stelligen Verifizierungscode aus der E-Mail ein und wählen Sie **Überprüfen und abschließen**.
5. Wählen Sie **Ja, meine E-Mail-Adresse ändern**, um die Änderung zu bestätigen.

Nachdem Sie Ihre Änderungen bestätigt haben, meldet Citrix Cloud Sie ab. Nach ein paar Minuten können Sie sich mit der neuen E-Mail-Adresse neu anmelden.

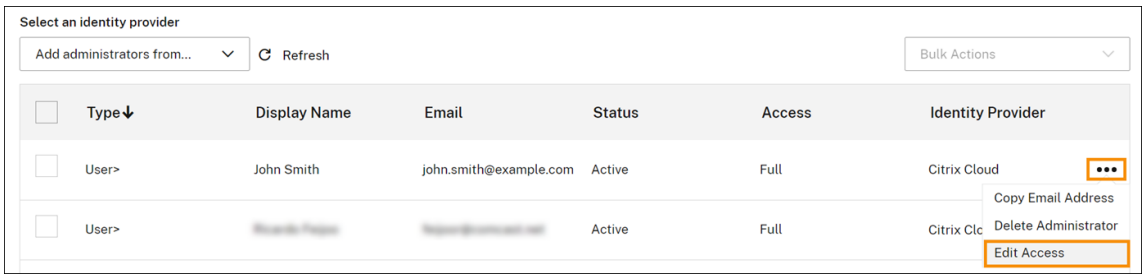
Ändern von Administratorberechtigungen

Wenn Sie Ihrem Citrix Cloud-Konto Administratoren hinzufügen, definieren Sie die für die Rolle der Administratoren in Ihrem Unternehmen geeigneten Administratorberechtigungen. Standardmäßig erhalten neue Administratoren *Vollzugriffsberechtigungen* für alle Citrix Cloud-Kontofunktionen und verfügbaren Dienste. Wenn Sie den Zugriff auf bestimmte Bereiche der Verwaltungskonsole oder auf bestimmte Dienste beschränken möchten, können Sie *benutzerdefinierte Zugriffsberechtigungen* festlegen.

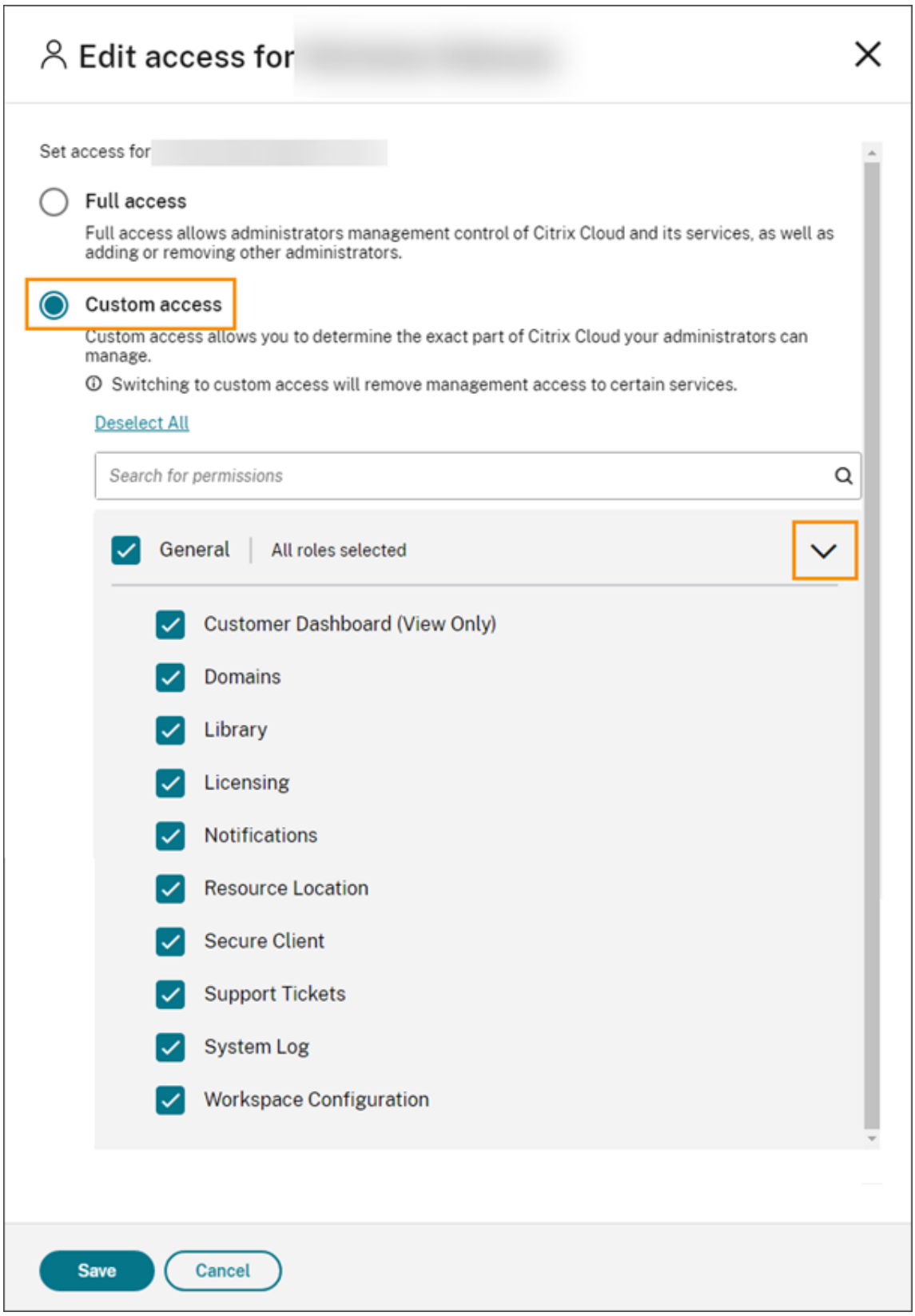
Nur Citrix Cloud-Administratoren mit Vollzugriff können Berechtigungen für andere Administratoren festlegen.

Gehen Sie zum Ändern von Administratorberechtigungen folgendermaßen vor:

1. Melden Sie sich bei Citrix Cloud unter https://citrix.cloud.com an.
2. Wählen Sie im Citrix Cloud-Menü **Identitäts- und Zugriffsverwaltung** und dann **Administratoren**.
3. Wählen Sie den Identitätsanbieter aus, den Sie verwalten möchten: Citrix-Identität (Standard), Active Directory (bei Verwendung von SAML als Identitätsanbieter) oder Azure AD (falls verbunden).
4. Suchen Sie den gewünschten Administrator oder die Gruppe, klicken Sie auf die drei Punkte (…) und wählen Sie **Zugriff bearbeiten**.



5. Um bestimmte Berechtigungen zuzulassen bzw. zu verweigern, wählen Sie **Benutzerdefinierter Zugriff**. Um den Zugriff auf alle Citrix Cloud-Funktionen zu ermöglichen, wählen Sie **Vollzugriff**.
6. Um eine Dienstberechtigung schnell zu finden, geben Sie ihren Namen ins Suchfeld ein. Citrix Cloud zeigt während der Eingabe passende Berechtigungen an. Wenn Sie beispielsweise “Lesezugriff”eingeben, werden Berechtigungen mit “Lesezugriff”im Titel angezeigt. Bei der Suche nach Berechtigungen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
7. Um benutzerdefinierte Zugriffsberechtigungen für die Citrix Cloud-Verwaltungskonsole festzulegen, erweitern Sie **Allgemein**.



8. Um benutzerdefinierte Zugriffsberechtigungen für einen bestimmten Dienst festzulegen,

erweitern Sie den Dienst.

9. Aktivieren oder deaktivieren Sie jede Berechtigung nach Bedarf.
10. Wählen Sie **Speichern**.

Konsolenberechtigungen

In diesem Abschnitt werden die benutzerdefinierten Zugriffsberechtigungen für die Citrix Cloud-Verwaltungskonsole beschrieben. Informationen zu den benutzerdefinierten Zugriffsberechtigungen für spezifische Services finden Sie in der Dokumentation zum Service.

- **Kundendashboard (schreibgeschützt):** Nur für Citrix Service Provider (CSPs). Ermöglicht das Anzeigen des Kundendashboards.
- **Domänen:** Gewährt Zugriff auf die Registerkarte **Identitäts- und Zugriffsverwaltung > Domänen**. Administratoren können eine Active Directory-Domäne hinzufügen, indem sie die Citrix Cloud Connector-Software von dieser Registerkarte herunterladen und auf einem Server in der Domäne installieren.
- **Bibliothek:** Gewährt Zugriff auf die Konsolenseite **Bibliothek**. Abhängig von den Services, auf die Administratoren Zugriff haben, können Administratoren Benutzer zu Bereitstellungsgruppen für Citrix DaaS zuweisen, verwaltete Intune-Apps aus Endpoint Management hinzufügen oder Lesezugriffadministratoren das Anzeigen von App-Details für Secure Private ermöglichen.
- **Lizenzierung:** Gewährt Zugriff auf die Registerkarten **Cloudservices** und **Lizenzierte Bereitstellungen** der Konsolenseite **Lizenzierung**.
- **Benachrichtigungen:** Gewährt Zugriff auf die Konsolenseite **Benachrichtigungen**. Administratoren können Citrix Cloud-Benachrichtigungen anzeigen und verwerfen.
- **Ressourcenstandorte:** Gewährt Zugriff auf die Konsolenseite **Ressourcenstandorte**. Administratoren können neue Ressourcenstandorte hinzufügen und FAS-Server für Citrix Workspace Single Sign-on hinzufügen. Sie können auch Connector-Updates verwalten.
- **Sicherer Client:** Gewährt Zugriff auf die Registerkarte **Identitäts- und Zugriffsverwaltung > API-Zugriff > Sichere Clients**. Administratoren können ihre eigenen sicheren Clients für die Verwendung mit Citrix Cloud-APIs erstellen und verwalten. Diese Berechtigung umfasst nicht den Zugriff auf die Registerkarte **Identitäts- und Zugriffsverwaltung > API-Zugriff > Produktregistrierungen**. Nur Administratoren mit Vollzugriff können auf die Registerkarte **Produktregistrierungen** zugreifen.
- **Supporttickets:** Gewährt Zugriff auf die Konsolenmenüoption **Supporttickets** und die Hilfemenüoption **Ticket erstellen**. Wenn Sie eine dieser Optionen auswählen, wird der Administrator zum My Support-Portal weitergeleitet. Weitere Informationen finden Sie unter Technischer Support.
- **Systemprotokoll:** Gewährt Zugriff auf die Konsolenseite **Systemprotokoll**. Administratoren können Systemprotokollereignisse anzeigen und Ereignisse in eine CSV-Datei exportieren.

- **Workspacekonfiguration:** Gewährt Zugriff auf die Konsolenseite **Workspacekonfiguration**. Administratoren können Authentifizierungsmethoden ändern, die Darstellung und das Verhalten von Workspaces anpassen, Dienste aktivieren und deaktivieren und die Siteaggregation konfigurieren. Weitere Informationen finden Sie in der Produktdokumentation zu Citrix Workspace.
- **Workspace-OAuth-Clients (Vorschau):** Gewährt Zugriff auf die Registerkarte **Identitäts- und Zugriffsverwaltung > API-Zugriff > Workspace-API**. Administratoren können einen eigenen OAuth-Client erstellen und verwalten, um mit den APIs der Citrix Workspace-Plattform zu interagieren. OAuth-Clients werden ausschließlich für Workspace-APIs verwendet und bieten die Option, private Clients mit automatischem Ablaufdatum zu erstellen.

> **Hinweis:**
>
> Bei der Zuweisung der benutzerdefinierten Rolle **Workspace-OAuth-Clients** ist Vorsicht geboten. Die mit dieser Rolle verknüpften Zugriffsrechte ermöglichen Administratoren möglicherweise den Zugriff auf die Ressourcen der Endbenutzer (VDAs oder Anwendungen) auf der Workspace-Plattform. Es ist auch wichtig zu beachten, dass Administratoren mit **Vollzugriff** automatisch über Zugriffsberechtigungen verfügen, die denen eines Administrators mit der Berechtigung des **Workspace-OAuth-Clients** entsprechen.

Primäre MFA-Methode verwalten

Um sich bei Citrix Cloud mit Multifaktorauthentifizierung anzumelden, können Sie eine Authentifikator-App oder Ihre E-Mail-Adresse verwenden. In diesem Abschnitt wird beschrieben, wie Sie das für die Multifaktorauthentifizierung registrierte Gerät ändern oder eine andere Methode zur Multifaktorauthentifizierung verwenden.

Gerät für die Multifaktorauthentifizierung ändern

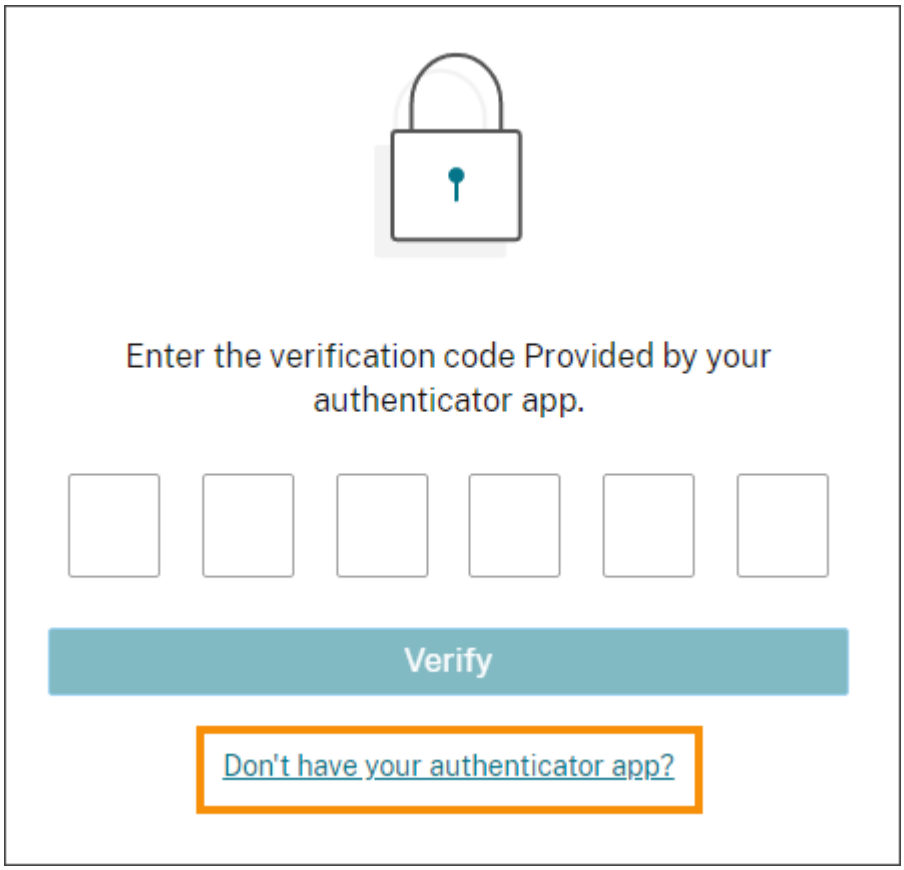
Wenn Sie Ihr registriertes Gerät verlieren, ein anderes Gerät mit Citrix Cloud verwenden möchten oder die Authentifikator-App zurücksetzen, können Sie sich in Citrix Cloud neu für die Multifaktorauthentifizierung registrieren.

> **Hinweise**
>
> - Wenn Sie Ihr Gerät ändern, wird die aktuelle Geräteregistrierung gelöscht und ein neuer Authentifikator-App-Schlüssel generiert.
> - Wenn Sie sich mit derselben Authentifikator-App aus der ursprünglichen Registrierung neu registrieren, löschen Sie den Eintrag für Citrix Cloud aus der Authentifikator-App, bevor Sie sich neu registrieren. Nach Abschluss der Neuregistrierung funktionieren die in diesem Eintrag angezeigten Codes nicht mehr. Wenn Sie diesen Eintrag vor oder nach der Neureg-

istrierung nicht löschen, zeigt die Authentifikator-App zwei Einträge für Citrix Cloud mit unterschiedlichen Codes an, die bei der Anmeldung bei Citrix Cloud zu Verwirrung führen können.

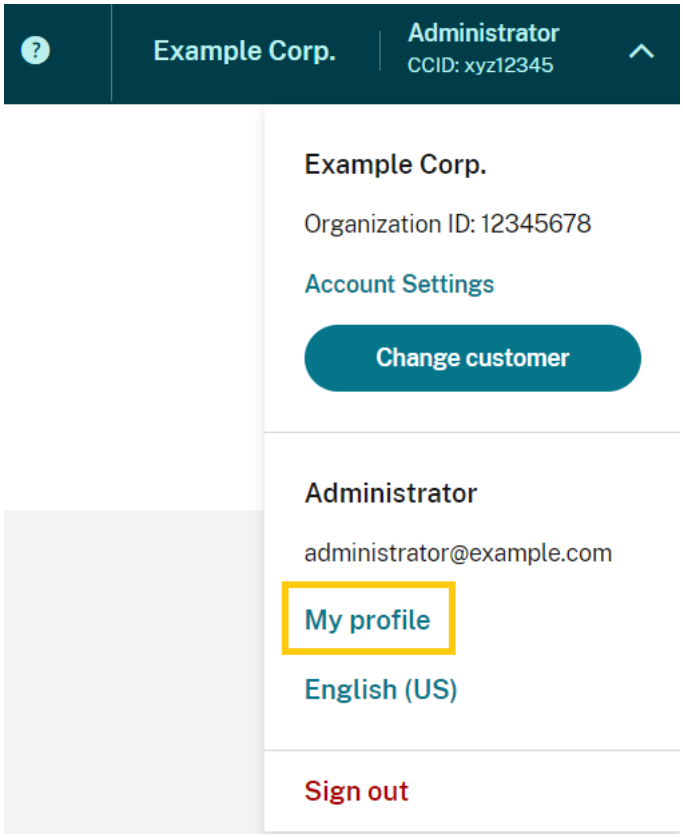
- Wenn Sie sich mit einem neuen Gerät neu registrieren und keine Authentifikator-App haben, laden Sie eine App aus dem App Store Ihres Geräts herunter und installieren Sie sie. Für eine bessere Benutzererfahrung empfiehlt Citrix, eine Authentifikator-App zu installieren, bevor Sie das Gerät neu registrieren.

1. Melden Sie sich bei Citrix Cloud an, und geben Sie den Code aus Ihrer Authentifikator-App ein.

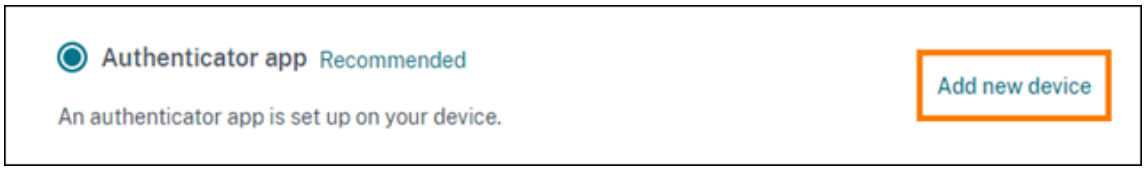


   Wenn Sie keine Authentifikator-App haben, klicken Sie auf **Haben Sie keine Authentifikator-App?**, und wählen Sie eine Wiederherstellungsmethode aus, die Ihnen die Anmeldung ermöglicht. Geben Sie je nach ausgewählter Wiederherstellungsmethode den empfangenen Wiederherstellungscode oder einen nicht verwendeten Backupcode ein, und wählen Sie **Überprüfen**aus.

2. Wenn Sie Administrator für mehrere Kundenorganisationen sind, wählen Sie eine beliebige Kundenorganisation aus.
3. Wählen Sie im Menü oben rechts **Meine Einstellungen** aus.



4. Wählen Sie in der **Authentifikator-App** die Option **Neues Gerät hinzufügen**.



5. Wenn Sie aufgefordert werden, die Änderung des Geräts zu bestätigen, wählen Sie **Ja, mein Gerät ändern**.
6. Verifizieren Sie Ihre Identität, indem Sie einen Verifizierungscode aus der Authentifikator-App eingeben. Wenn Sie keine Authentifikator-App haben, wählen Sie **Verwenden Sie eine Wiederherstellungsmethode**, um Ihre Identität mit der gewählten Wiederherstellungsmethode zu verifizieren. Geben Sie je nach ausgewählter Wiederherstellungsmethode den Verifizierungscode oder den Wiederherstellungscode ein, den Sie erhalten, oder einen nicht verwendeten Backupcode. Wählen Sie **Verifizieren und fortfahren**.
7. Wenn Sie das ursprünglich registrierte Gerät und die ursprüngliche Authentifikator-App verwenden, löschen Sie den vorhandenen Eintrag für Citrix Cloud aus der Authentifikator-App.
8. Wenn Sie ein neues Gerät registrieren und keine Authentifikator-App haben, laden Sie eine App aus dem App Store Ihres Geräts herunter.
9. Scannen Sie in Ihrer Authentifikator-App den QR-Code mit Ihrem Gerät oder geben Sie den

Schlüssel manuell ein.

10. Geben Sie den 6-stelligen Verifizierungscode aus Ihrer Authentifikator-App ein, und wählen Sie **Code verifizieren** aus.

Nachdem Sie Ihr Gerät gewechselt haben, empfiehlt Citrix dringend, zu überprüfen, ob die Verifizierungsmethoden auf der Seite "Mein Profil"auf dem neuesten Stand sind.

Methode zur Multifaktorauthentifizierung ändern

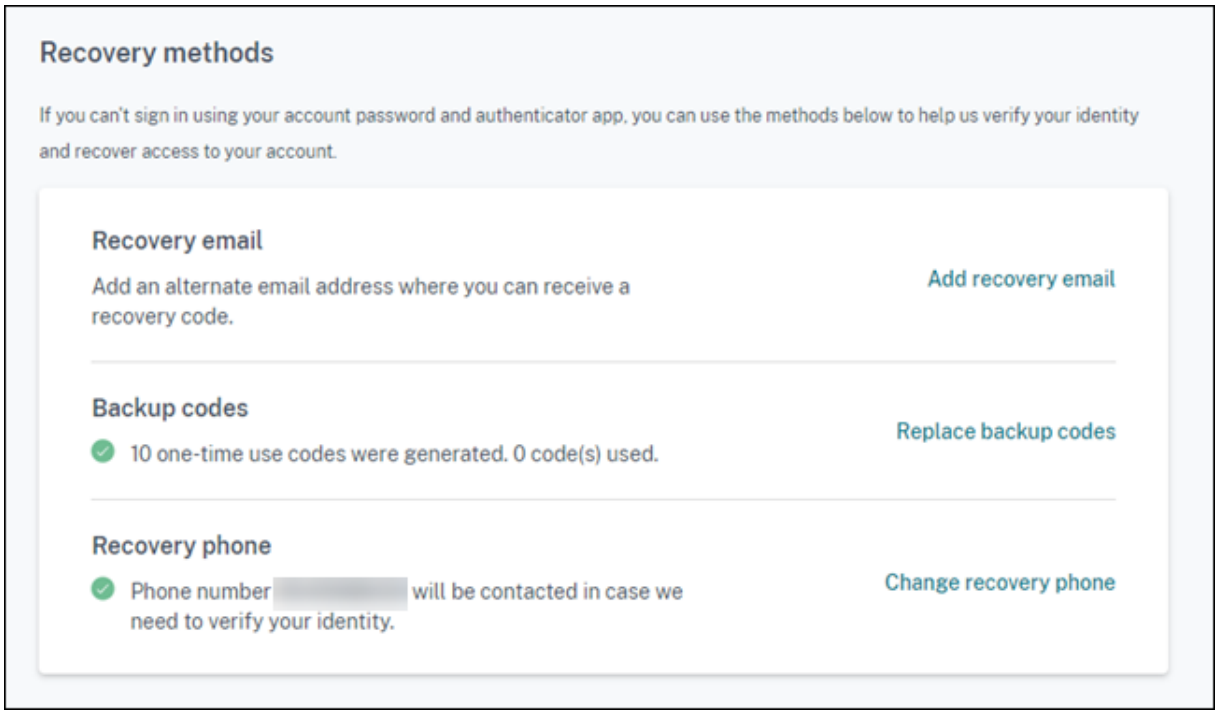
Wenn Sie bei der Multifaktorauthentifizierung mit einer Authentifikator-App registriert sind und stattdessen Ihre E-Mail-Adresse verwenden möchten, beachten Sie, dass durch Änderung Ihrer Authentifizierungsmethode Ihre Geräteregistrierung gelöscht wird. Wenn Sie erneut eine Authentifikator-App zur Multifaktorauthentifizierung verwenden möchten, müssen Sie Ihr Gerät neu registrieren.

1. Wählen Sie in der Citrix Cloud-Konsole im Menü rechts oben die Option **Meine Einstellungen**.
2. Wählen Sie unter **Multifaktorauthentifizierung (MFA)** die Authentifizierungsmethode aus, zu der Sie wechseln möchten.
3. Wechsel zur Multifaktorauthentifizierung per E-Mail-Adresse:
    a) Wählen Sie **Ja, zu E-Mail wechseln**, um die Änderung der MFA-Methode zu bestätigen.
    b) Geben Sie den Code aus Ihrer Authentifikator-App ein oder verwenden Sie eine Wiederherstellungsmethode, um Ihre Identität zu bestätigen.
    c) Wählen Sie **Verifizieren und fortfahren**, um die Änderung abzuschließen.
4. Wechsel zur Authentifikator-App:
    a) Geben Sie nach Aufforderung den Verifizierungscode ein, den Citrix Cloud an Ihre E-Mail-Adresse sendet, und wählen Sie **Verifizieren und fortfahren**. Oder verwenden Sie eine Wiederherstellungsmethode, um Ihre Identität zu bestätigen.
    b) Scannen Sie in der Authentifikator-App den QR-Code per Gerätekamera oder geben Sie den alphanumerischen Schlüssel ein.
    c) Geben Sie unter **Authentifikator-App verifizieren** den sechsstelligen Code aus der Authentifikator-App ein.
    d) Klicken Sie auf **Code verifizieren**, um die Geräteregistrierung abzuschließen.

MFA-Wiederherstellungsmethoden verwalten

> **Wichtig:**
>
> Halten Sie Ihre Verifizierungsmethoden aktuell, um die Sicherheit Ihres Citrix Cloud-Kontos zu gewährleisten. Bei verlorenem Zugriff auf die Authentifikator-App oder die E-Mail-Adresse

> zur Multifaktorauthentifizierung können Sie den Zugriff auf Ihr Konto nur mit diesen Verifizierungsmethoden wiederherstellen.



Wiederherstellungs-E-Mail-Adresse hinzufügen oder ändern

1. Wählen Sie im Menü oben rechts **Meine Einstellungen** aus.
2. Falls Sie noch keine Wiederherstellungs-E-Mail-Adresse hinzugefügt haben, wählen Sie unter **Wiederherstellungsmethoden** im Bereich **Wiederherstellungs-E-Mail-Adresse** die Option **Wiederherstellungs-E-Mail-Adresse hinzufügen**. Falls bereits eine Wiederherstellungs-E-Mail-Adresse vorliegt, wählen Sie **Wiederherstellungs-E-Mail-Adresse ändern**.
3. Geben Sie nach Aufforderung den Verifizierungscode aus der Authentifikator-App ein oder den Code, der an Ihre E-Mail-Adresse gesendet wurde.
4. Geben Sie die neue E-Mail-Adresse ein, die Sie verwenden möchten, und wählen Sie **Verifizierungs-E-Mail senden**. Die E-Mail-Adresse darf nicht die E-Mail-Adresse sein, die Sie für Ihr Citrix Cloud-Konto verwenden. Citrix Cloud sendet eine Verfizierungs-E-Mail an die eingegebene E-Mail-Adresse.
5. Geben Sie den Code aus der Verfifizierungs-E-Mail ein und klicken Sie auf **Code verifizieren und abschließen**.

Neue Backupcodes generieren

Sie können jederzeit neue Backupcodes generieren. Wenn Sie Backupcodes verwenden, zeichnet Citrix Cloud die Ziffernfolge auf, die auf der Seite "Mein Profil"verwendet wurde.

Nachdem Sie neue Backupcodes generiert haben, sollten Sie diese an einem sicheren Ort speichern.

1. Wählen Sie im Menü oben rechts **Meine Einstellungen** aus.
2. Wenn Sie noch nie Backupcodes generiert haben, wählen Sie unter **Wiederherstellungsmethoden** im Bereich **Backupcodes** die Option **Neue Backupcodes generieren**. Wenn Sie bereits Backupcodes erstellt haben, wählen Sie **Backupcodes ersetzen**.
3. Wenn Sie aufgefordert werden, Ihre Backupcodes zu ersetzen, wählen Sie **Ja, meine Codes ersetzen**.
4. Geben Sie zur Verifizierung der Identität einen Verifizierungscode aus der Authentifikator-App ein oder den Code, den Sie per E-Mail erhalten haben.
5. Wählen Sie **Verifizieren und fortfahren**. Citrix Cloud generiert und zeigt einen neuen Satz von Backupcodes an.
6. Wählen Sie **Codes herunterladen** aus, um Ihre neuen Codes als Textdatei herunterzuladen. Wählen Sie dann **Ich habe meine Backupcodes gespeichert**.
7. Wählen Sie **Ich habe meine Backupcodes gespeichert**, um das Ersetzen der Backupcodes abzuschließen.

Telefonnummer für die Wiederherstellung ändern

1. Wählen Sie im Menü oben rechts **Meine Einstellungen** aus.
2. Wählen Sie unter **Wiederherstellungsmethoden** im Bereich **Wiederherstellungstelefon** die Option **Wiederherstellungstelefon ändern**.
3. Geben Sie den Verifizierungscode aus der Authentifikator-App ein oder den Code, den Sie per E-Mail erhalten haben. Wählen Sie **Verifizieren und fortfahren**.
4. Geben Sie die neue Telefonnummer ein, die Sie verwenden möchten. Geben Sie dann die Telefonnummer zur Bestätigung erneut ein.
5. Wählen Sie **Telefonnummer für die Wiederherstellung speichern**.

> **Hinweis:**
>
> Sie können die Berechtigungen von Citrix Endpoint Management (CEM)-Administratoren erst ändern, nachdem die Administratoren eine Administratoreinladung angenommen und auf der CEM-Kachel auf **Verwalten** geklickt haben. Wie alle Citrix Cloud-Administratoren haben CEM-Administratoren standardmäßig Vollzugriff.

Administratorgruppen verwalten

February 15, 2024

Sie können Ihrem Citrix Cloud-Konto Administratoren über Gruppen in Ihrem Active Directory, Azure Active Directory (AD) oder Google Cloud Identity hinzufügen. Sie können dann die Dienstzugriffsberechtigungen für alle Administratoren in der Gruppe verwalten.

AD-Voraussetzungen

Citrix Cloud unterstützt die AD-Gruppenauthentifizierung über SAML 2.0. Bevor Sie Mitglieder Ihrer AD-Administratorgruppen zu Citrix Cloud hinzufügen, müssen Sie eine Verbindung zwischen Citrix Cloud und Ihrem SAML-Anbieter konfigurieren. Weitere Informationen finden Sie unter SAML als Identitätsanbieter mit Citrix Cloud verbinden.

Wenn Sie bereits eine SAML-Verbindung in Citrix Cloud haben, müssen Sie Ihren SAML-Anbieter neu mit Citrix Cloud verbinden, bevor Sie AD-Administratorgruppen hinzufügen. Wenn Sie SAML nicht neu verbinden, schlägt das Hinzufügen von AD-Administratorgruppen möglicherweise fehl. Weitere Informationen finden Sie unter Vorhandene SAML-Verbindung für die Administratorauthentifizierung verwenden.

Voraussetzungen für Azure AD

Um Azure AD-Gruppen zu verwenden, brauchen Sie die neueste Version der Azure AD-Anwendung zum Verbinden von Azure AD mit Citrix Cloud. Citrix Cloud erwarb diese Anwendung, als Sie Ihr Azure AD zum ersten Mal verbunden haben. Wenn Sie Azure AD vor Mai 2019 mit Citrix Cloud verbunden haben, verwenden Sie möglicherweise nicht die aktuelle Anwendung für die Verbindung mit Azure AD. Citrix Cloud kann Ihre Azure AD-Gruppen nicht anzeigen, wenn Ihr Konto nicht die neueste Anwendung verwendet.

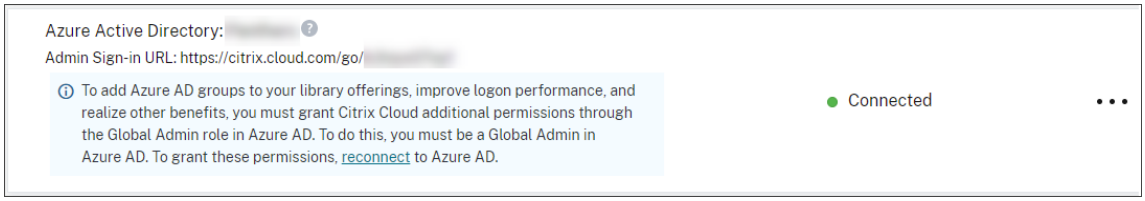
Führen Sie die folgenden Aufgaben aus, bevor Sie Azure AD-Gruppen in Citrix Cloud verwenden:

1. Überprüfen Sie, ob Sie die neueste Anwendung für Ihre Azure AD-Verbindung verwenden. Citrix Cloud zeigt eine Benachrichtigung an, wenn Sie nicht die neueste Anwendung verwenden.
2. Wenn die Anwendung aktualisiert werden muss, verbinden Sie Azure AD erneut mit Citrix Cloud. Durch die Wiederverbindung mit Azure AD erteilen Sie Citrix Cloud Lesezugriff auf Anwendungsebene und ermöglichen Citrix Cloud, in Ihrem Namen wieder eine Verbindung mit Azure AD herzustellen. Während der Wiederverbindung wird eine Liste dieser Berechtigungen angezeigt, die Sie überprüfen können. Weitere Informationen zu den Berechtigungen, die Citrix Cloud anfordert, finden Sie unter Azure Active Directory-Berechtigungen für Citrix Cloud.

> **Wichtig:**
>
> Für diese Aufgabe müssen Sie ein globaler Administrator in Azure AD sein. Außerdem müssen Sie mit einem Administratorkonto mit Vollzugriff unter dem Citrix-Identitätsanbieter bei Citrix Cloud angemeldet sein. Wenn Sie sich mit Ihren Azure AD-Anmeldeinformationen anmelden, schlägt die Wiederverbindung fehl. Wenn Sie keine Administratoren haben, die den Citrix-Identitätsanbieter verwenden, können Sie vorübergehend einen hinzufügen, um diese Aufgabe auszuführen, und ihn anschließend löschen.

Verbindung mit Azure AD überprüfen

1. Melden Sie sich mit einem Administratorkonto mit Vollzugriff unter dem Citrix-Identitätsanbieter bei Citrix Cloud an.
2. Wählen Sie im Menü "Citrix Cloud"**Identitäts- und Zugriffsverwaltung** und dann **Authentifizierung** aus.
3. Suchen Sie **Azure Active Directory**. Es wird eine Benachrichtigung angezeigt, wenn Citrix Cloud die Anwendung für die Azure AD-Verbindung aktualisieren muss.



   Wenn Citrix Cloud bereits die neueste Anwendung verwendet, wird keine Benachrichtigung angezeigt.

Verbindung mit Azure AD wiederherstellen

1. Klicken Sie in der Azure AD-Benachrichtigung in der Citrix Cloud-Konsole auf den Link für die **Wiederverbindung**. Eine Liste der angeforderten Azure-Berechtigungen wird angezeigt.
2. Prüfen Sie die Berechtigungen und wählen Sie dann **Akzeptieren** aus.

Google Cloud Identity

Citrix Cloud unterstützt die Administratorgruppenauthentifizierung über Google Cloud Identity. Bevor Sie Administratorgruppen in Citrix Cloud hinzufügen, müssen Sie eine Verbindung zwischen Citrix Cloud und Google Cloud Identity konfigurieren. Weitere Informationen finden Sie unter Google Cloud Identity als Identitätsanbieter mit Citrix Cloud verbinden.

Unterstützte Cloudservices

Die folgenden Services unterstützen benutzerdefinierte Zugriffsberechtigungen für Administratorgruppen:

- Citrix Analytics
- NetScaler-Konsole
- Citrix DaaS
- Workspace Environment Management Service
- License Usage Insights

Unterstützte Berechtigungen

Sie können benutzerdefinierte Zugriffsberechtigungen nur für unterstützte Services und bestimmte Features der Citrix Cloud-Plattform zuweisen. Vollzugriffsberechtigungen werden nicht unterstützt.

Für Citrix Cloud-Features werden die folgenden benutzerdefinierten Zugriffsberechtigungen unterstützt:

- Domänen
- Lizenzierung
- Ressourcenstandorte
- Supporttickets
- Systemprotokoll
- Workspacekonfiguration

Weitere Informationen zu diesen Berechtigungen finden Sie unter Konsolenberechtigungen.

Administratorgruppen haben keinen Zugriff auf andere Services. Sie können nur den unterstützte Service verwalten, für den sie eine Zugriffsberechtigung haben.

Berechtigungsänderungen für ein Mitglied der Administratorgruppe, das bereits angemeldet ist, werden erst wirksam, nachdem es sich ab- und neu angemeldet hat.

Resultierende Berechtigungen für Administratoren mit Citrix-, AD-, Azure AD- und Google Cloud-Identitäten

Wenn sich ein Administrator bei Citrix Cloud anmeldet, sind möglicherweise nur bestimmte Berechtigungen verfügbar, wenn der Administrator sowohl über eine Citrix-Identität (Standard-Identitätsanbieter in Citrix Cloud) als auch über eine Azure AD-Identität für Einzelbenutzer oder eine gruppenbasierte Identität durch AD, Azure AD oder Google Cloud Identity verfügt. In der Tabelle

in diesem Abschnitt werden die Berechtigungen beschrieben, die für jede Kombination dieser Identitäten verfügbar sind.

Identität für Einzelbenutzer bezieht sich auf AD-, Azure AD- oder Google Cloud Identity-Berechtigungen, die dem Administrator über ein Einzelkonto erteilt werden. *Gruppenbasierte Identität* bezieht sich auf AD-, Azure AD- oder Google Cloud Identity-Berechtigungen, die den Mitgliedern einer Gruppe erteilt werden.

Citrix-Identität	AD- oder Azure AD-Identität für Einzelbenutzer	Gruppenbasierte AD- oder Azure AD-Identität	Google Cloud Identity für Einzelbenutzer oder Gruppen	Nach der Authentifizierung verfügbare Berechtigungen
X	X			Der Administrator verfügt nach erfolgreicher Authentifizierung mit der Citrix-, der AD- oder der Azure AD-Identität über kumulative Berechtigungen der Identitäten.
X		X		Jede Identität wird wie eine unabhängige Einheit behandelt. Verfügbare Berechtigungen hängen davon ab, ob sich der Administrator mit der Citrix-Identität oder der Azure AD-Identität authentifiziert.

Citrix-Identität	AD- oder Azure AD-Identität für Einzelbenutzer	Gruppenbasierte AD- oder Azure AD-Identität	Google Cloud Identity für Einzelbenutzer oder Gruppen	Nach der Authentifizierung verfügbare Berechtigungen
X			X	Jede Identität wird wie eine unabhängige Einheit behandelt. Verfügbare Berechtigungen hängen davon ab, ob sich der Administrator mit der Citrix-Identität oder Google Cloud Identity authentifiziert.
	X	X		Der Administrator hat kumulative Berechtigungen beider Identitäten, wenn er sich mit AD oder Azure AD bei Citrix Cloud authentifiziert.

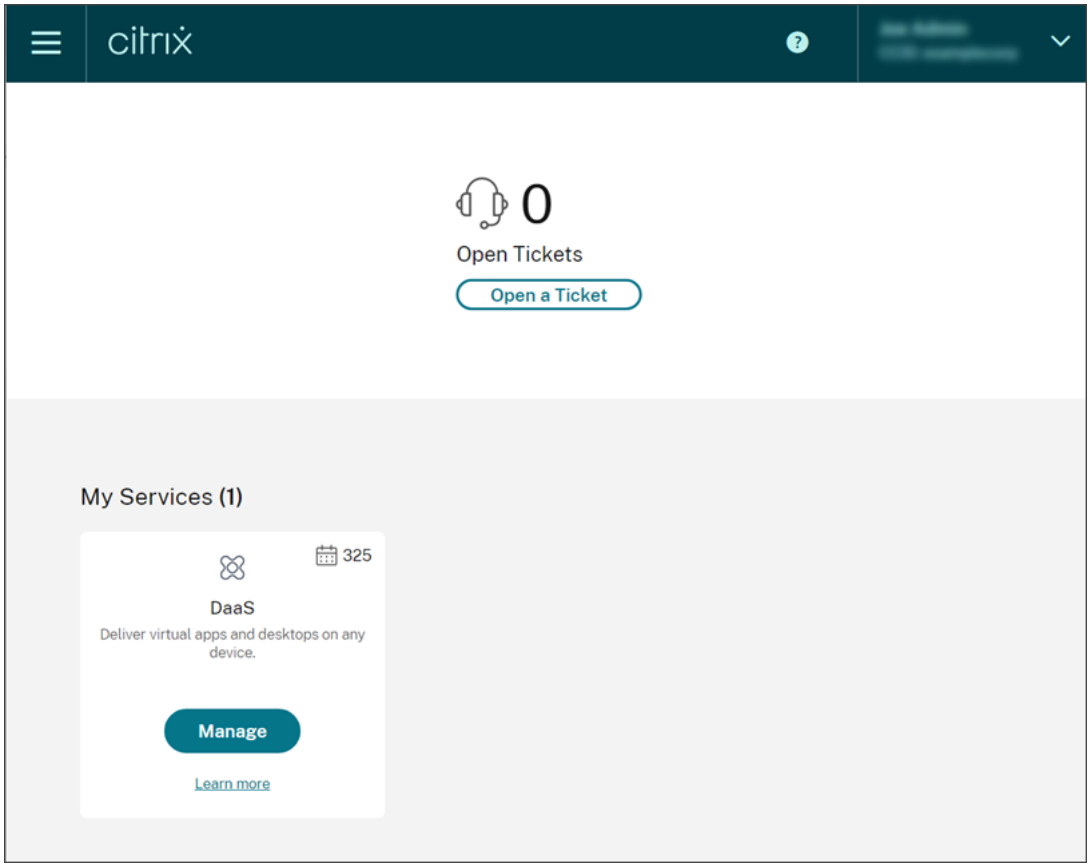
Citrix-Identität	AD- oder Azure AD-Identität für Einzelbenutzer	Gruppenbasierte AD- oder Azure AD-Identität	Google Cloud Identity für Einzelbenutzer oder Gruppen	Nach der Authentifizierung verfügbare Berechtigungen
	X		X	Jede Identität wird wie eine unabhängige Einheit behandelt. Verfügbare Berechtigungen hängen davon ab, ob sich der Administrator mit der Citrix-Identität oder Google Cloud Identity authentifiziert.
		X	X	Jede Identität wird wie eine unabhängige Einheit behandelt. Verfügbare Berechtigungen hängen davon ab, ob sich der Administrator mit der Citrix-Identität oder Google Cloud Identity authentifiziert.

Citrix-Identität	AD- oder Azure AD-Identität für Einzelbenutzer	Gruppenbasierte AD- oder Azure AD-Identität	Google Cloud Identity für Einzelbenutzer oder Gruppen	Nach der Authentifizierung verfügbare Berechtigungen
X	X	X		Bei Authentifizierung mit seiner Citrix-Identität verfügt der Administrator über kumulative Berechtigungen sowohl der Citrix-Identität als auch der Azure AD-Identität für Einzelbenutzer. Bei Authentifizierung mit Azure AD verfügt der Administrator über kumulative Berechtigungen aller drei Identitäten.

Anmeldeumgebung für Administratoren

Nachdem Sie Citrix Cloud eine Gruppe hinzufügen und Dienstberechtigungen definieren, melden sich die Administratoren in der Gruppe an, indem sie auf der Citrix Cloud-Anmeldeseite **Mit Firmenanmeldeinformationen anmelden** auswählen und die Anmelde-URL für das Konto eingeben (z. B. `https://citrix.cloud.com/go/mycompany`). Anders als beim Hinzufügen einzelner Administratoren werden Administratoren in der Gruppe nicht explizit eingeladen und erhalten daher keine E-Mails mit einer Einladung, Citrix Cloud-Administratoren zu werden.

Nach der Anmeldung wählen Administratoren in der Servicekachel die Option **Verwalten** aus, um auf die Verwaltungskonsole des Diensts zuzugreifen.



Administratoren, denen nur Berechtigungen als Mitglieder von Gruppen erteilt wurden, können über die Anmelde-URL für das Konto auf das Citrix Cloud-Konto zugreifen.

Administratoren, denen Berechtigungen über ein Einzelkonto und als Gruppenmitglied erteilt wurden, können das Citrix Cloud-Konto auswählen, auf das sie zugreifen möchten. Administratoren, die Mitglied mehrerer Citrix Cloud-Konten sind, können nach erfolgreicher Authentifizierung ein Citrix Cloud-Konto aus der Kundenauswahl auswählen.

Einschränkungen

Zugriff auf Plattform- und Service-Features

Benutzerdefinierte Zugriffsberechtigungen für die folgenden Citrix Cloud-Features sind für Mitglieder von Administratorgruppen nicht verfügbar:

- Bibliothek
- Benachrichtigungen
- Sichere Clients

Weitere Informationen zu verfügbaren Berechtigungen finden Sie in diesem Artikel unter Unterstützte Berechtigungen.

Citrix DaaS-Features, die auf Funktionen der Citrix Cloud-Plattform wie Quick Deploy-Benutzerzuweisung basieren, sind nicht verfügbar.

Auswirkung mehrerer Gruppen auf die Anwendungsleistung

Citrix empfiehlt, dass ein einzelner Administrator in höchstens 20 Gruppen, die Citrix Cloud hinzugefügt wurden, Mitglied sein sollte. Die Mitgliedschaft in einer größeren Anzahl von Gruppen kann zur Verringerung der Anwendungsleistung führen.

Auswirkung mehrerer Gruppen auf die Authentifizierung

Wenn ein gruppenbasierter Administrator mehreren Gruppen in AD oder Azure AD zugewiesen ist, schlägt die Authentifizierung möglicherweise fehl, da die Anzahl der Gruppen zu groß ist. Dieses Problem tritt aufgrund einer Einschränkung der Integration zwischen Citrix Cloud und AD oder Azure AD auf. Wenn der Administrator versucht, sich anzumelden, versucht Citrix Cloud, die Anzahl der abgerufenen Gruppen zu komprimieren. Wenn Citrix Cloud die Komprimierung nicht erfolgreich anwenden kann, können nicht alle Gruppen abgerufen werden und die Authentifizierung schlägt fehl.

Dieses Problem kann auch Benutzer betreffen, die sich über AD oder Azure AD bei Citrix Workspace authentifizieren. Wenn ein Benutzer zu mehreren Gruppen gehört, schlägt die Authentifizierung möglicherweise fehl, da die Anzahl der Gruppen zu groß ist.

Um dieses Problem zu beheben, überprüfen Sie das Administrator- oder Benutzerkonto und stellen Sie sicher, dass Benutzer nur den Gruppen angehören, die für ihre Rolle in der Organisation erforderlich sind.

Hinzufügen von Gruppen schlägt aufgrund zu vieler zugewiesener Rollen-/Bereichspaare fehl

Beim Hinzufügen einer Gruppe mit mehreren Rollen-/Bereichspaaren kann ein Fehler auftreten, der anzeigt, dass die Gruppe nicht erstellt werden kann. Dieser Fehler tritt auf, weil die Anzahl der Rollen-/Bereichspaare, die der Gruppe zugewiesen sind, zu groß ist. Um diesen Fehler zu beheben, teilen Sie die Rollen-/Bereichspaare in zwei oder mehr Gruppen auf und weisen Sie die Administratoren diesen Gruppen zu.

Administratorgruppe zu Citrix Cloud hinzufügen

1. Wählen Sie im Citrix Cloud-Menü **Identitäts- und Zugriffsverwaltung** und dann **Administratoren**.
2. Wählen Sie **Administrator/Gruppe hinzufügen**.

3. Wählen Sie unter **Administratordetails** den Identitätsanbieter aus, den Sie verwenden möchten. Wenn Azure AD ausgewählt ist, melden Sie sich ggf. bei Azure an. Wählen Sie **Weiter**.
4. Wählen Sie ggf. die Domäne aus, die Sie verwenden möchten.
5. Suchen Sie nach der Gruppe, die Sie hinzufügen möchten, und wählen Sie die Gruppe aus.
6. Wählen Sie unter **Zugriff festlegen** die Rollen aus, die Sie der Gruppe zuweisen möchten. Sie müssen mindestens eine Rolle auswählen.
7. Wenn Sie fertig sind, wählen Sie **Speichern**.

Serviceberechtigungen für eine Administratorgruppe ändern

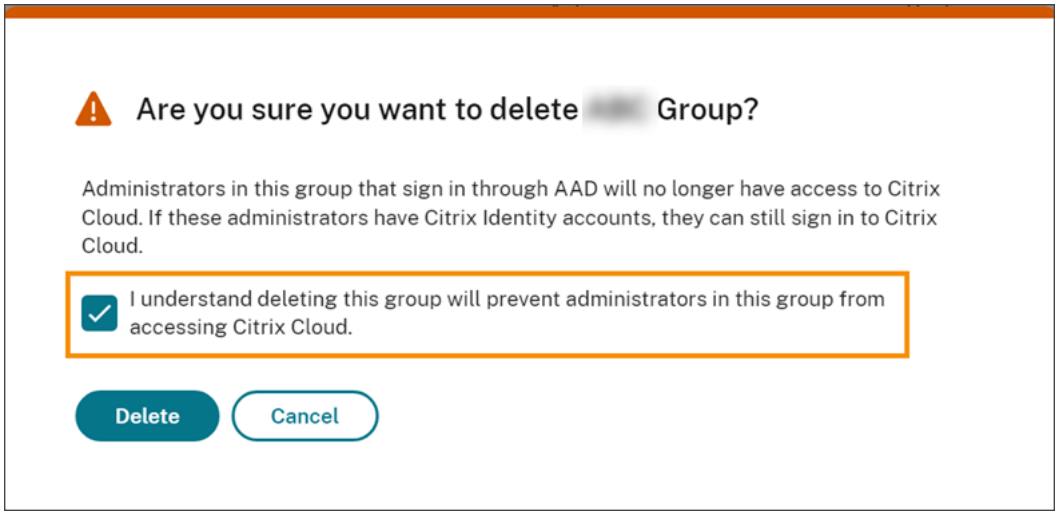
1. Wählen Sie im Citrix Cloud-Menü **Identitäts- und Zugriffsverwaltung** und dann **Administratoren**.
2. Suchen Sie die Administratorgruppe, die Sie verwalten möchten, klicken Sie auf die Auslassungspunkte und wählen Sie **Zugriff bearbeiten** aus.

3. Setzen oder entfernen Sie die Häkchen neben einem oder mehreren Rollen- und Bereichspaaren nach Bedarf.
4. Wenn Sie fertig sind, wählen Sie **Speichern**.

Administratorgruppe löschen

1. Wählen Sie im Citrix Cloud-Menü **Identitäts- und Zugriffsverwaltung** und dann **Administratoren**.
2. Suchen Sie die Administratorgruppe, die Sie verwalten möchten, klicken Sie auf die Auslassungspunkte und wählen Sie **Gruppe löschen** aus.

Eine Bestätigungsmeldung wird angezeigt.

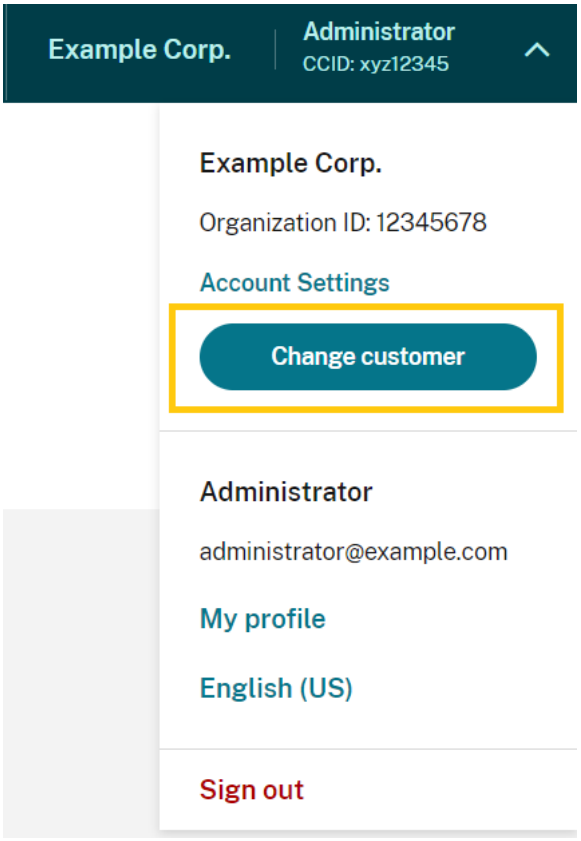


3. Wählen Sie **Ich verstehe, dass Administratoren in dieser Gruppe nach dem Löschen dieser Gruppe nicht mehr auf Citrix Cloud zugreifen können** aus. Damit bestätigen Sie, dass Sie sich der Auswirkungen des Löschens der Gruppe bewusst sind.
4. Wählen Sie **Löschen** aus.

Wechseln zwischen mehreren Citrix Cloud-Konten

> **Hinweis:**
>
> In diesem Abschnitt wird ein Szenario beschrieben, das nur Mitglieder von Azure AD-Administratorgruppen betrifft.

Standardmäßig können Mitglieder von Azure AD-Administratorgruppen nicht zwischen Citrix Cloud-Konten wechseln, auf die sie zugreifen können. Für diese Administratoren wird die in der Abbildung unten gezeigte Option **Kunden ändern** nicht im Citrix Cloud-Benutzermenü angezeigt.

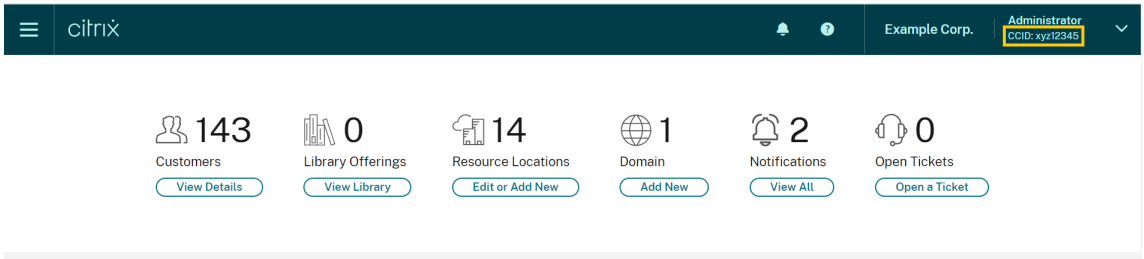


Um diese Menüoption zu aktivieren und Azure AD-Gruppenmitgliedern das Wechseln zwischen Citrix Cloud-Konten zu ermöglichen, müssen Sie die Konten verknüpfen, zwischen denen gewechselt werden soll.

Das Verknüpfen von Citrix Cloud-Konten erfordert einen Hub-and-Spoke-Ansatz. Entscheiden Sie vor dem Verknüpfen von Konten, welches Citrix Cloud-Konto als das Konto fungieren soll, von dem aus auf die anderen Konten zugegriffen wird (“Hub”), und welche Konten in der Kundenauswahl (“Spokes”) aufgeführt werden sollen.

Stellen Sie vor dem Verknüpfen von Konten sicher, dass die folgenden Anforderungen erfüllt sind:

- Sie haben Vollzugriffsberechtigungen in Citrix Cloud.
- Sie haben Zugriff auf die Windows PowerShell Integrated Scripting Environment (ISE).
- Sie haben die Kunden-IDs für die Citrix Cloud-Konten, die Sie verknüpfen möchten. Die Kunden-ID wird oben rechts in der Verwaltungskonsole für jedes Konto angezeigt.



- Sie haben das Citrix CWSAuth-Bearertoken für das Citrix Cloud-Konto, das Sie als Hub-Konto verknüpfen möchten. Folgen Sie den Anweisungen in CTX330675, um dieses Bearertoken abzurufen. Sie müssen diese Informationen angeben, wenn Sie Ihre Citrix Cloud-Konten verknüpfen.

So verknüpfen Sie Citrix Cloud-Konten

1. Öffnen Sie die PowerShell ISE und fügen Sie das folgende Skript in den Arbeitsbereich ein:

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links"
9
10 $resp = Invoke-RestMethod -Method Get -Uri $uri -Headers $headers
11 $allLinks = $resp.linkedCustomers + @("SpokeCustomerID")
12
13 $body = @{
14  "customers"=$allLinks }
15
16 $bodyjson = $body | ConvertTo-Json
17
18 $resp = Invoke-WebRequest -Method Post -Uri $uri -Headers $headers
       -Body $bodyjson -ContentType 'application/json'
19 Write-Host "Citrix Cloud Status Code: $($resp.RawContent)"
20 <!--NeedCopy-->
```

2. Ersetzen Sie in Zeile 4 `CWSAuth bearer=XXXXXXX` durch Ihren CWSAuth-Wert (z. B. `CWSAuth bearer=AbCdef123Ghik...`). Dieser Wert ist ein langer Hash, der einem Zertifikatsschlüssel ähnelt.
3. Ersetzen Sie in Zeile 6 `HubCustomerID` durch die Kunden-ID des Hub-Kontos.
4. Ersetzen Sie in Zeile 9 `SpokeCustomerID` durch die Kunden-ID des Spoke-Kontos.
5. Führen Sie das Skript aus.
6. Wiederholen Sie die Schritte 3 bis 5, um weitere Konten als Spokes zu verknüpfen.

So heben Sie die Verknüpfung von Citrix Cloud-Konten auf

1. Öffnen Sie die PowerShell ISE. Wenn die PowerShell ISE bereits geöffnet ist, löschen Sie den Arbeitsbereich.
2. Fügen Sie das folgende Skript in den Arbeitsbereich ein:


```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links/
       SpokeCustomerID"
9
10 $resp = Invoke-WebRequest -Method Delete -Uri $uri -Headers
       $headers
11 Write-Host "Response: $($resp.RawContent)"
12 <!--NeedCopy-->
```

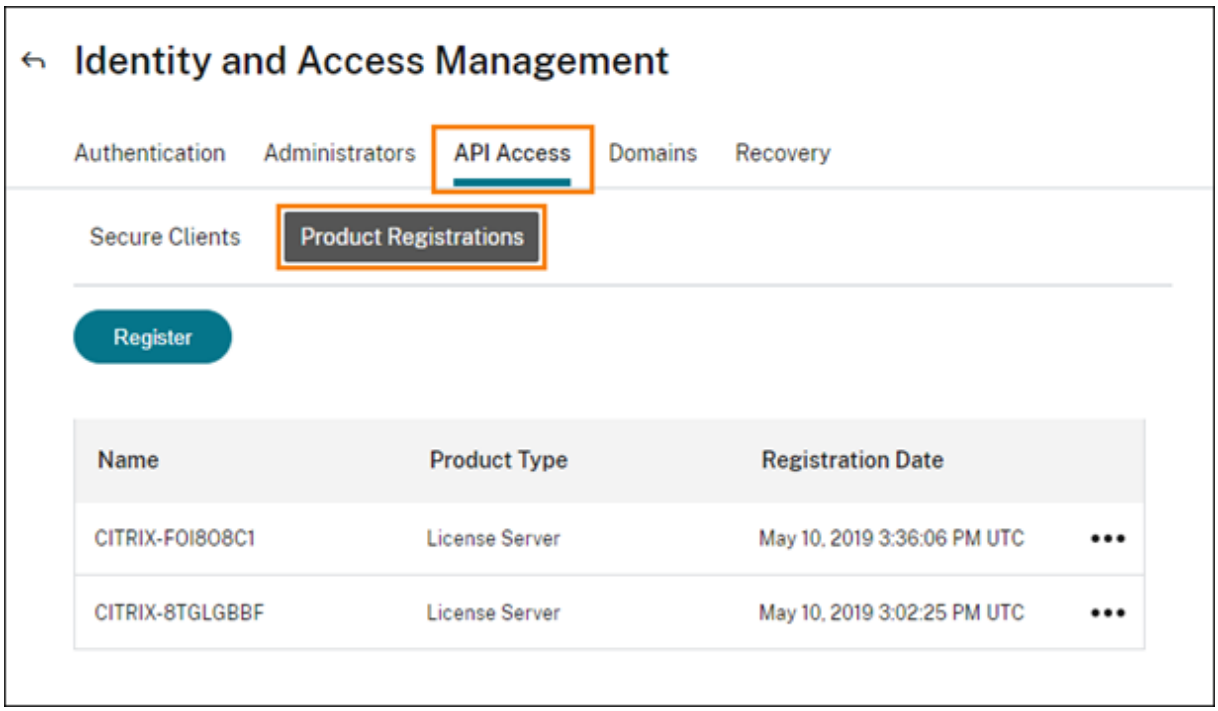
3. Ersetzen Sie in Zeile 4 `CWSAuth bearer=xxxxxxx1` durch Ihren CWSAuth-Wert (z. B. `CWSAuth bearer=AbCdef123Ghik...`). Dieser Wert ist ein langer Hash, der einem Zertifikatsschlüssel ähnelt.
4. Ersetzen Sie in Zeile 6 `HubCustomerID` durch die Kunden-ID des Hub-Kontos.
5. Ersetzen Sie in Zeile 6 `SpokeCustomerID` durch die Kunden-ID des Spoke-Kontos.
6. Führen Sie das Skript aus.
7. Wiederholen Sie die Schritte 4 bis 6, um die Verknüpfung weiterer Konten aufzuheben.

Registrieren von On-Premises-Produkten bei Citrix Cloud

September 28, 2023

Sie können Ihr on-premises Citrix-Produkt ganz einfach per Kurzcodeaktivierung über Citrix Cloud registrieren. Abhängig vom Produkt wird dieser 8-stellige Code während der Produktinstallation oder beim Ausführen der Produktverwaltungskonsole generiert. Wenn Sie vom Produkt zur Registrierung aufgefordert werden, wird der Code von Citrix Cloud angefordert und angezeigt. Sie können ihn dann per Kopieren und Einfügen oder manuell in Citrix Cloud eingeben.

Nach der Registrierung werden auf der Seite "Produktregistrierungen"(**Identitäts- und Zugriffsverwaltung > API-Zugriff > Produktregistrierungen**) die Server angezeigt, auf denen sich die registrierten Produkte befinden.



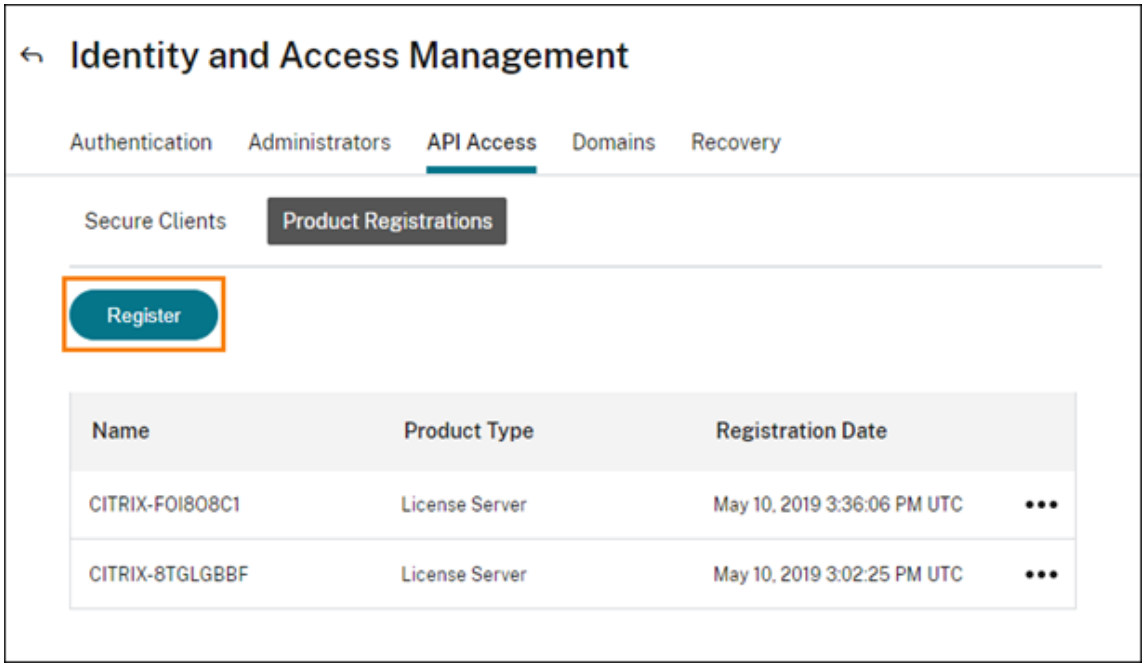
Sie können folgende On-Premises-Produkte bei Citrix Cloud registrieren:

- Citrix Connector Appliance für Cloudservices
- Citrix Verbundauthentifizierungsdienst
- Citrix Lizenzserver
- Citrix Virtual Apps and Desktops, wenn Sie eine Site bei Citrix Analytics für Leistung registrieren

> **Hinweis:**
>
> In diesem Artikel werden die Schritte zum Registrieren eines On-Premises-Produkts bei Citrix Cloud beschrieben. Weitere Angaben zu produktspezifischen Anforderungen finden Sie in der Dokumentation zu diesem Produkt.

Registrieren eines Produkts

1. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.
2. Wählen Sie **API-Zugriff > Produktregistrierungen** und dann **Registrieren**.

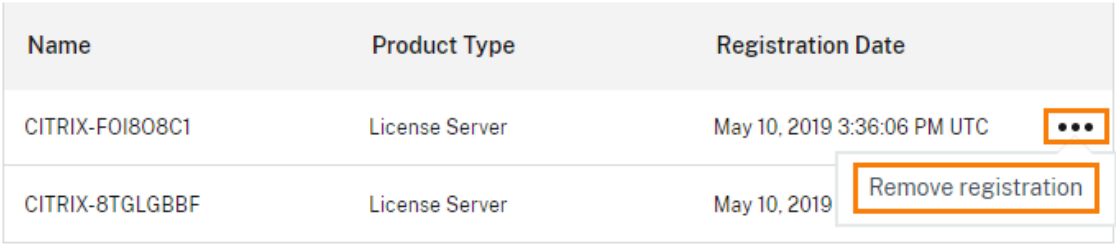


3. Geben Sie den achtstelligen alphanumerischen Code für Ihr Citrix Produkt ein und klicken Sie auf **Weiter**.
4. Überprüfen Sie die Registrierungsdetails und klicken Sie auf **Registrieren**.

Entfernen einer Produktregistrierung

Wenn Sie Server mit registriertem Citrix-Produkt aus Ihrer Umgebung entfernen, werden die Server auf der Seite "Produktregistrierungen"weiterhin angezeigt. Führen Sie folgende Schritte aus, um die Server aus Citrix Cloud zu entfernen. Bei Bedarf können Sie das Produkt später erneut registrieren, um die Server auf der Seite "Produktregistrierungen"anzuzeigen.

1. Suchen Sie auf der Seite "Produktregistrierungen"den Server, den Sie entfernen möchten.
2. Klicken Sie auf die Auslassungspunkte (…) und wählen Sie **Registrierung entfernen**.



3. Wählen Sie **Entfernen**, wenn Sie dazu aufgefordert werden.

Verbinden von Active Directory mit Citrix Cloud

July 2, 2024

Citrix Cloud unterstützt die Authentifizierung von Workspace-Abonnenten über Ihr On-premises-Active Directory (AD). Für einige Workspace-Authentifizierungsverfahren ist außerdem eine Verbindung zwischen Ihrem Active Directory und Citrix Cloud erforderlich. Weitere Informationen finden Sie unter Auswählen und Ändern von Authentifizierungsmethoden.

Citrix Cloud unterstützt auch die Verwendung von Token als zweiten Authentifizierungsfaktor für Abonnenten, die sich über Active Directory bei ihrem Workspace anmelden. Workspace-Abonnenten können Token mit jeder App generieren, die dem Standard Zeitbasiertes Einmalkennwort entspricht, z. B. Citrix SSO.

Weitere Hinweise zur Authentifizierung von Workspace-Abonnenten mit Active Directory plus Token finden Sie unter Active Directory plus Token.

> **Tipp:**
>
> Im Kurs Introduction to Citrix Identity and Authentication erfahren Sie mehr über unterstützte Identitätsanbieter. Das Modul „Planning Citrix Identity and Access Management“enthält kurze Videos zum Verbinden des Identitätsanbieters mit Citrix Cloud und zum Aktivieren der Authentifizierung für Citrix Workspace.

Active Directory verbinden

Wenn Sie Active Directory mit Citrix Cloud verbinden, müssen Sie Connectors in Ihrer Domäne installieren. Sie können entweder Cloud Connectors oder Connectorgeräte als Connectors für Active Directory verwenden. Informationen zum Auswählen des für Ihre Umgebung zu verwendenden Connectortyps finden Sie in den folgenden Artikeln:

- Bereitstellungsszenarios für Cloud Connectors in Active Directory
- Bereitstellungsszenarios für Connectorgeräte in Active Directory

Active Directory über Connectorgeräte verbinden

Sie können Connector Appliances verwenden, um einen Ressourcenstandort mit Gesamtstrukturen zu verbinden, die keine Citrix Virtual Apps and Desktops-Ressourcen enthalten. Zum Beispiel im Fall von Citrix Secure Private Access-Kunden oder Citrix Virtual Apps and Desktops-Kunden mit einigen Gesamtstrukturen, die nur für die Benutzerauthentifizierung verwendet werden.

Weitere Informationen finden Sie unter Active Directory mit Connectorgerät

Active Directory über Cloud Connectors verbinden

Mindestens zwei Cloud Connectors sind erforderlich, um eine hochverfügbare Verbindung zu Citrix Cloud sicherzustellen. Weitere Informationen finden Sie in den folgenden Artikeln:

- Technische Daten zu Citrix Cloud Connector: Systemanforderungen und Empfehlungen zur Bereitstellung.
- Cloud Connector-Installation: Anweisungen zur Installation über die grafische Benutzeroberfläche oder die Befehlszeile.

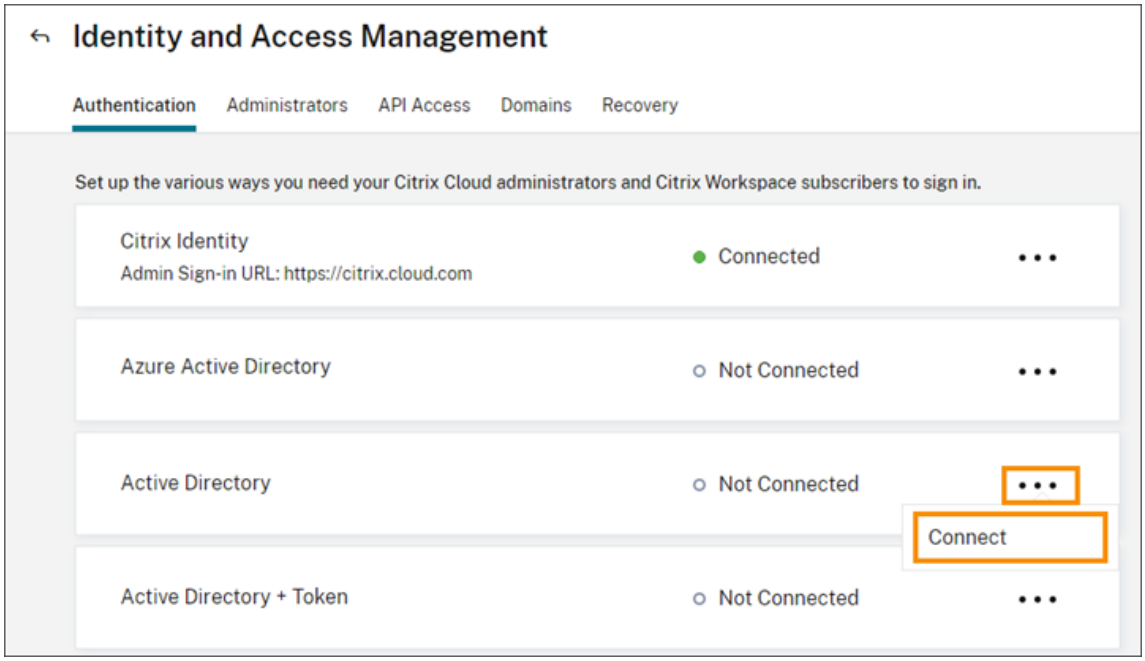
Zum Verbinden von Active Directory mit Citrix Cloud müssen Sie folgende Aufgaben erledigen:

1. Installieren von Cloud Connectors in Ihrer Domäne. Citrix empfiehlt die Installation von zwei Cloud Connectors für hohe Verfügbarkeit.
2. Wenn zutreffend, Aktivieren von Token für Benutzergeräte. Die Abonnenten können jeweils nur ein Gerät registrieren.

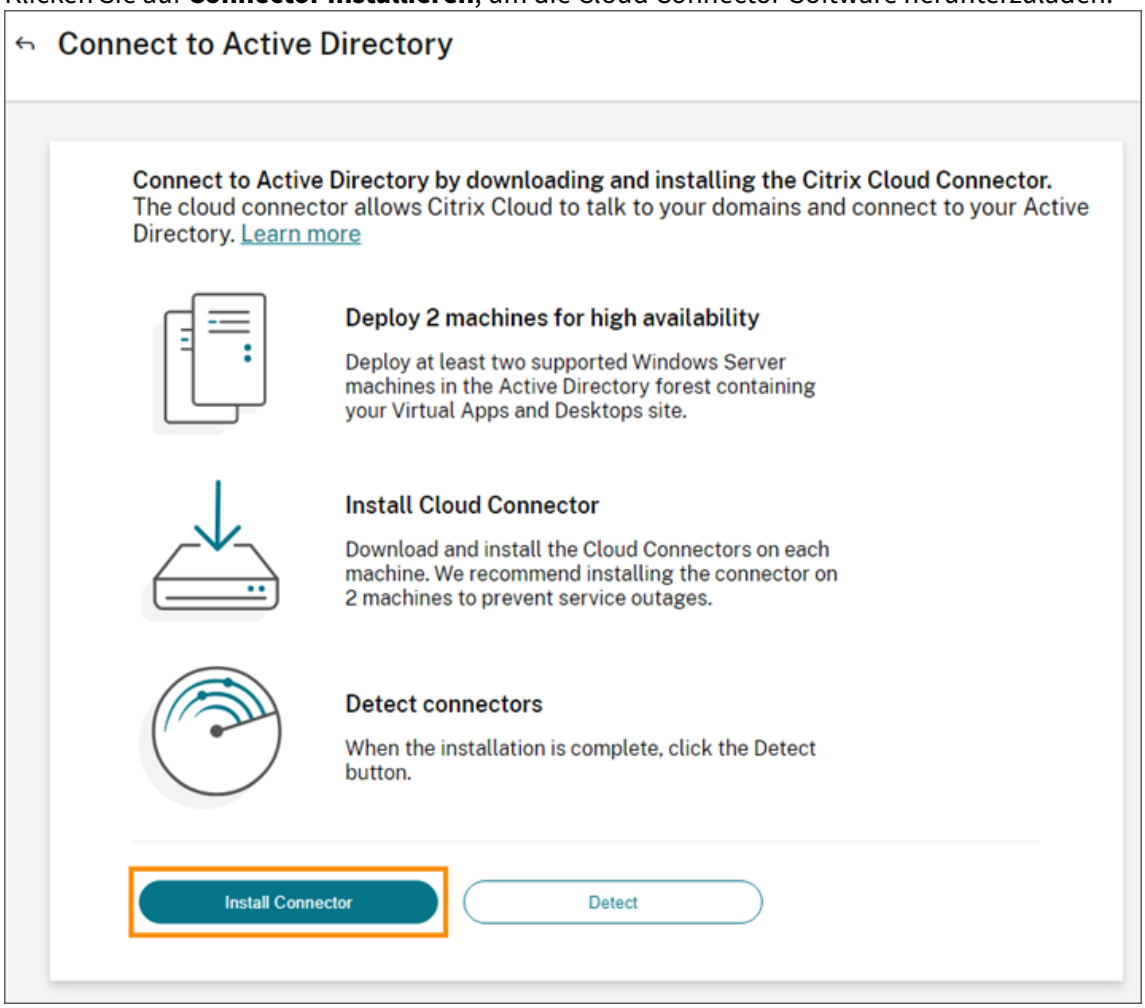
> **Wichtig:**
>
> Wenn Sie Cloud Connectors für Citrix DaaS bereitstellen, sind möglicherweise zusätzliche Schritte erforderlich, um sicherzustellen, dass Ihre AD-Domänen nach der Cloud Connector-Bereitstellung registriert und aktiv sind. Durch Überprüfen, ob Ihre AD-Domänen in Citrix Cloud aktiv sind, wird sichergestellt, dass das Einrichten des Maschinenkatalogs reibungslos erfolgt. Weitere Informationen über Schritte für Citrix DaaS, die nach der Bereitstellung durchgeführt werden, fifinden Sie unter Ressourcentyp hinzufügen oder eine unbenutzte Domäne in Citrix Cloud aktivieren in der Citrix DaaS-Produktdokumentation.

Verbinden von Azure Active Directory mit Citrix Cloud

1. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.
2. Klicken Sie in **Active Directory** auf der Registerkarte **Authentifizierung** auf die Auslassungspunkte (…) und wählen Sie den Menübefehl **Verbinden**.



3. Klicken Sie auf **Connector installieren**, um die Cloud Connector-Software herunterzuladen.

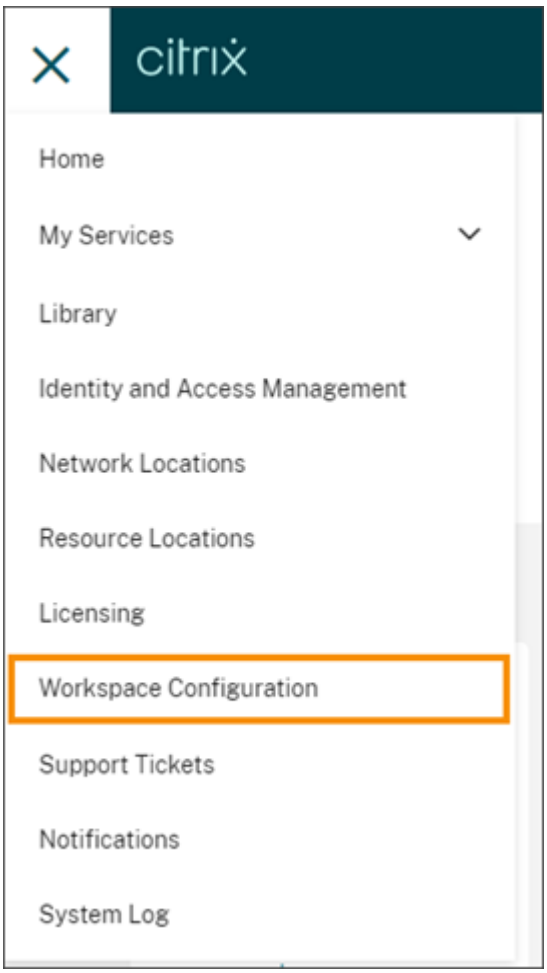


4. Starten Sie das Installationsprogramm für den Cloud Connector und folgen Sie dem Installationsassistenten.
5. Klicken Sie auf der Seite **Mit Active Directory verbinden** auf **Ermitteln**. Nach der Überprüfung zeigt Citrix Cloud eine Bestätigung an, dass Ihr Active Directory verbunden ist.
6. Klicken Sie auf **Zurück zur Authentifizierung**. Der **Active Directory**-Eintrag ist auf der Registerkarte **Authentifizierung** als **Aktiviert** markiert.

Aktivieren der Authentifizierung über Active Directory plus Token

1. Verbinden Sie Active Directory mit Citrix Cloud, indem Sie entweder Connectorgeräte oder Cloud Connectors verwenden.
2. Überprüfen Sie im Abschnitt **Identitäts- und Zugriffsverwaltung** in Citrix Cloud auf der Registerkarte **Authentifizierung**, ob der Eintrag **Active Directory** als **Aktiviert** markiert ist.
3. Klicken Sie auf **Weiter**. Die Seite **Token konfigurieren** wird angezeigt und die Option **Ein Gerät** ist standardmäßig ausgewählt.
4. Klicken Sie auf **Speichern und Fertig stellen**, um die Konfiguration abzuschließen. Der Eintrag **Active Directory + Token** auf der Registerkarte **Authentifizierung** ist als **Aktiviert** markiert.
5. Aktivieren der Authentifizierung per Token für Workspaces:

    a) Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration**.



b) Wählen Sie auf der Registerkarte **Authentifizierung** die Option **Active Directory + Token**.

Nach Aktivierung der Authentifizierung über Active Directory plus Token können Workspace-Abonnenten ihr Gerät registrieren und Token mithilfe einer Authentifizierungs-App generieren. Die Abonnenten können jeweils nur ein Gerät registrieren. Anweisungen zum Registrieren von Abonnentengeräten finden Sie unter Zweistufige Authentifizierung (optional).

Optionen zum erneuten Registrieren von Abonnentengeräten finden Sie unter Erneute Registrierung von Geräten.

Weitere Informationen

Citrix Tech Zone:

- Tech Insight: Authentication - TOTP
- Tech Insight: Authentication - Push

Verbinden von Azure Active Directory mit Citrix Cloud

June 3, 2024

Citrix Cloud unterstützt die Authentifizierung von Citrix Cloud-Administratoren und Workspace-Abonnenten über Azure Active Directory (AD).

Durch die Verwendung von Azure AD mit Citrix Cloud ist Folgendes möglich:

- Nutzung Ihres eigenen Active Directory und somit Steuerung von Überwachung und Kennwortrichtlinien sowie Deaktivierung von Konten bei Bedarf
- Konfigurieren der Multifaktorauthentifizierung zum verbesserten Schutz vor dem Diebstahl von Anmeldeinformationen
- Verwendung einer Anmeldeseite mit Branding, die Benutzern die Gewissheit gibt, dass sie sich bei der richtigen Stelle anmelden
- Verbund mit einem Identitätsanbieter nach Wahl, z. B. AD FS, Okta oder Ping

Azure AD-App und -Berechtigungen

Citrix Cloud enthält eine Azure AD-App, mit der Citrix Cloud sich mit Azure AD verbinden kann, ohne dass Sie bei einer aktiven Azure AD-Sitzung angemeldet sein müssen. Seit der Einführung dieser App hat Citrix Updates veröffentlicht, die die Leistung verbessern und neue Features und Berechtigungen unterstützen.

Wenn Sie eine bestehende Azure AD-Verbindung zu Citrix Cloud haben und die aktuelle App verwenden möchten, müssen Sie Ihre Azure AD-Verbindung in Citrix Cloud aktualisieren. Weitere Informationen finden Sie unter Wiederverbinden mit Azure AD für die aktualisierte App in diesem Artikel. Wenn Sie die App nicht aktualisieren, funktioniert Ihre bestehende Verbindung weiterhin normal.

Weitere Informationen über die Azure AD-Apps und -Berechtigungen, die Citrix Cloud für die Verbindung mit dem Azure AD verwendet, finden Sie unter Azure Active Directory-Berechtigungen für Citrix Cloud.

> **Tipp:**
>
> Im Kurs Introduction to Citrix Identity and Authentication erfahren Sie mehr über unterstützte Identitätsanbieter. Das Modul „Planning Citrix Identity and Access Management“enthält kurze Videos zum Verbinden des Identitätsanbieters mit Citrix Cloud und zum Aktivieren der Authentifizierung für Citrix Workspace.

Authentifizierung mit mehreren Citrix Cloud-Konten

In diesem Artikel wird beschrieben, wie Sie Ihr Azure AD als Identitätsanbieter mit einem Citrix Cloud-Konto verbinden. Wenn Sie mehrere Citrix Cloud-Konten haben, können Sie jedes mit demselben Azure AD-Mandanten verbinden. Führen Sie die folgenden Aufgaben aus:

1. Melden Sie sich bei Ihrem Citrix Cloud-Konto an und wählen Sie die entsprechende Kunden-ID aus der Kundenauswahl aus.
2. Wenn Sie einen ersten Kunden mit Ihrem Azure AD verbinden, folgen Sie allen Schritten in diesem Artikel, um Ihr AD und Azure AD zu synchronisieren, den Kunden mit Citrix Cloud zu verbinden und Administratoren hinzuzufügen.
3. Um einen weiteren Kunden zu verbinden, klicken Sie auf das Benutzermenü oben rechts in der Citrix Cloud-Konsole, wählen Sie **Kunde ändern** und wählen Sie dann die nächste Kunden-ID, mit der Sie eine Verbindung herstellen möchten.
4. Verbinden Sie den Kunden mit Ihrem Azure AD (siehe Verbinden von Citrix Cloud mit Azure AD).
5. Wiederholen Sie die Schritte 3 und 4 für jede Kunden-ID.

Vorbereiten von Active Directory und Azure AD

Stellen Sie vor der Verwendung von Azure AD sicher, dass die folgenden Anforderungen erfüllt sind:

- Sie haben ein Microsoft Azure-Konto. Jedes Azure-Konto enthält Azure AD kostenlos. Wenn Sie kein Azure-Konto haben, registrieren Sie sich unter https://azure.microsoft.com/en-us/free/?v=17.36.
- Sie haben die globale Administratorrolle in Azure AD. Diese Rolle ist erforderlich, damit Sie zustimmen können, dass Citrix Cloud sich mit Azure AD verbindet.
- Die Eigenschaft "E-Mail"von Administratorkonten ist in Azure AD konfiguriert. Zu diesem Zweck können Sie Konten im lokalen Active Directory mit dem Microsoft-Tool Azure AD Connect per Synchronisierung in Azure AD übertragen. Alternativ können Sie nicht synchronisierte Azure AD-Konten mit Office 365-E-Mail konfigurieren.

Synchronisieren von Konten mit Azure AD Connect

1. Stellen Sie sicher, dass die Benutzereigenschaft "E-Mail"von Active Directory-Konten konfiguriert ist:
    a) Öffnen Sie Active Directory-Benutzer und -Computer.
    b) Suchen Sie im Ordner **Benutzer** das Konto, das Sie überprüfen möchten, klicken Sie mit der rechten Maustaste und wählen Sie **Eigenschaften**. Überprüfen Sie auf der Registerkarte **Allgemein**, ob das Feld **E-Mail** einen gültigen Eintrag enthält. Citrix Cloud

erfordert, dass Administratoren, die aus Azure AD hinzugefügt werden, andere E-Mail-Adressen haben als Administratoren, die sich mit einer von Citrix gehosteten Identität anmelden.

2. Installieren Sie Azure AD Connect und konfigurieren Sie es. Vollständige Anweisungen finden Sie unter Erste Schritte mit Azure AD Connect mit Expresseinstellungen auf der Microsoft Azure-Website.

Verbinden von Citrix Cloud mit Azure AD

Wenn Sie Ihr Citrix Cloud-Konto mit Azure AD verbinden, benötigt Citrix Cloud die Berechtigung zum Zugriff auf Ihr Benutzerprofil (d. h. das Profil des angemeldeten Benutzers) und auf die grundlegenden Profile der Benutzer in Azure AD. Citrix fordert diese Berechtigung an, um Ihren Namen und Ihre E-Mail-Adresse als Administrator zu erhalten und Ihnen zu ermöglichen, später andere Benutzer zu suchen und sie als Administratoren hinzuzufügen. Weitere Informationen zu den App-Berechtigungen, die Citrix Cloud anfordert, finden Sie unter Azure Active Directory-Berechtigungen für Citrix Cloud.

> **Wichtig:**
>
> Sie müssen ein globaler Administrator in Azure AD sein, um diese Aufgabe abzuschließen, oder einen globalen Administrator bitten, die Voraussetzungen zu erfüllen, bevor Sie sich bei Citrix Cloud anmelden.

1. Klicken Sie links oben auf der Seite auf **Menü** und wählen Sie **Identitäts- und Zugriffsverwaltung**.
2. Suchen Sie Azure Active Directory, klicken Sie auf die Auslassungspunkte (…) und wählen Sie **Verbinden**.
3. Geben Sie bei der entsprechenden Aufforderung einen kurzen, URL-freundlichen Bezeichner für Ihr Unternehmen ein und klicken Sie auf **Verbinden**. Der Bezeichner muss innerhalb von Citrix Cloud global eindeutig sein.
4. Melden Sie sich bei entsprechender Aufforderung bei dem Azure-Konto an, mit dem Sie die Verbindung herstellen möchten. Azure zeigt Ihnen die Berechtigungen an, die Citrix Cloud benötigt, um auf das Konto zuzugreifen und die für die Verbindung erforderlichen Informationen abzurufen. Die meisten dieser Berechtigungen sind für Lesezugriff. Mit ihnen kann Citrix Cloud grundlegende Informationen aus Microsoft Graph sammeln, z. B. Gruppen und Benutzerprofile. Wenn Sie Citrix Endpoint Management oder XenMobile Server mit Microsoft Intune integriert haben, müssen Sie Lese-/Schreibberechtigungen für Microsoft Intune erteilen. Weitere Informationen finden Sie unter Azure Active Directory-Berechtigungen für Citrix Cloud.
5. Klicken Sie auf **Akzeptieren**, um die Berechtigungsanforderung zu akzeptieren.

Alternative Verbindungsmethode

Sie können den Verbindungsfluss in die folgenden zwei Phasen unterteilen:

1. Erstellung von Azure AD-Apps (Entra ID) in Azure.
2. Citrix Cloud-Verbindung zur Azure AD-App (Entra ID) in Citrix Cloud.

Zunächst müssen Sie eine URL erstellen, die der globale Administrator verwenden kann, um die Unternehmensapps zum Mandanten hinzuzufügen. Weitere Informationen finden Sie unter Erstellen der URL zum Erteilen der mandantenweiten Administratoreinwilligung.

Die Erläuterung der erstellten URL:
`https://login.microsoftonline.com/<tenant url>/adminconsent?client_id=f9c0e999-22e7-409f-bb5e-956986abdf02&redirect_uri=https://portal.azure.com`

Wo:
`tenant url` ist Ihre Mandanten-URL oder ID.
`f9c0e999-22e7-409f-bb5e-956986abdf02` ist die Client-ID für Citrix Cloud.

Hinzufügen von Administratoren aus Azure AD zu Citrix Cloud

Citrix Cloud unterstützt das Hinzufügen von Administratoren (einzeln oder über Azure AD-Gruppen).

Informationen zum Hinzufügen einzelner Administratoren aus Azure AD finden Sie unter Administratorzugriff verwalten.

Informationen zum Hinzufügen von Azure AD-Administratorgruppen zu Citrix Cloud finden Sie unter Administratorgruppen verwalten.

Anmelden bei Citrix Cloud mit Azure AD

Wenn die Azure AD-Benutzerkonten verbunden sind, können sich die Benutzer mit einer der folgenden Methoden bei Citrix Cloud anmelden:

- Über die Anmelde-URL für Administratoren, die Sie beim ersten Verbinden des Azure AD-Identitätsanbieters für Unternehmen konfiguriert haben. Beispiel:`https://citrix.cloud.com/go/mycompany`
- Über die Citrix Cloud-Anmeldeseite durch Klicken auf **Mit Firmenanmeldeinformationen anmelden**, Eingeben der ID, die Sie beim ersten Verbinden des Azure AD-Identitätsanbieters für Unternehmen konfiguriert haben (z. B. “mycompany”), und Klicken auf **Weiter**.

Aktivieren Sie die Azure AD-Authentifizierung für Workspaces

Nachdem Sie Azure AD mit Citrix Cloud verbunden haben, können Sie Ihren Abonnenten erlauben, sich über Azure AD bei ihren Workspaces zu authentifizieren.

> **Wichtig:**
>
> Überprüfen Sie vor dem Aktivieren der Workspaceauthentifizierung über Azure AD den Abschnitt Azure Active Directory mit Überlegungen zum Verwenden von Azure AD mit Workspaces.

1. Klicken Sie in Citrix Cloud auf das Menü in der oberen linken Ecke und wählen Sie **Workspacekonfiguration**.
2. Wählen Sie auf der Registerkarte **Authentifizierung** die Option **Azure Active Directory**.
3. Klicken Sie auf **Bestätigen**, um die Änderungen an der Workspace-Benutzeroberfläche zu akzeptieren, die wirksam werden, wenn die Azure AD-Authentifizierung aktiviert ist.

Aktivieren erweiterter Azure AD-Funktionen

Azure AD bietet eine moderne Multifaktorauthentifizierung, erstklassige Sicherheitsfunktionen, einen Verbund von 20 Identitätsanbietern, Features wie Kennwortänderung und -zurücksetzung im Self-Service-Verfahren usw. Wenn Sie diese Features für Ihre Azure AD-Benutzer aktivieren, kann Citrix Cloud sie automatisch nutzen.

Informationen zum Servicelevel- und Preisvergleich für Azure AD finden Sie unter https://azure.microsoft.com/en-us/pricing/details/active-directory/.

Wiederverbinden mit Azure AD für die aktualisierte App

Citrix Cloud enthält eine Azure AD-App, mit der Citrix Cloud sich mit Azure AD verbinden kann, ohne dass Sie bei einer aktiven Azure AD-Sitzung angemeldet sein müssen. Seit der Einführung dieser App hat Citrix sie wie folgt aktualisiert:

- Im August 2018 wurde diese App aktualisiert, um die Leistung zu verbessern und sie auf zukünftige Versionen vorzubereiten.
- Im Mai 2019 wurde die App aktualisiert, um das Hinzufügen von Azure AD-Administratorgruppen zu Citrix Cloud zu unterstützen.
- Im April 2022 wurde die App aktualisiert, sodass sie die Berechtigung GroupMember.Read.All anstelle von Group.Read.All verwendet.

Wenn Sie Ihr Azure AD vor der Veröffentlichung dieser Updates mit Citrix Cloud verbunden haben und die neueste App verwenden möchten, müssen Sie Ihr Azure AD von Citrix Cloud trennen und dann erneut verbinden. Die Verwendung der neuesten App ist optional. Wenn Sie die App nicht aktualisieren, funktioniert Ihre bestehende Verbindung weiterhin normal.

Anforderungen

Bevor Sie Ihr Azure AD erneut verbinden, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Sie sind Administrator mit Vollzugriff unter dem standardmäßigen Citrix Identitätsanbieter. Wenn Sie sich mit Ihren Azure AD-Anmeldeinformationen bei Citrix Cloud anmelden, schlägt die Wiederverbindung fehl. Wenn Ihr Konto keine Administratoren enthält, die den Citrix Identitätsanbieter verwenden, können Sie einen solchen temporär hinzufügen und dann löschen, wenn Sie Ihr Azure AD erneut verbunden haben. Anweisungen finden Sie unter Einladen einzelner Administratoren.
- Wenn Sie Azure AD zur Authentifizierung von Workspace-Abonnenten verwenden, wählen Sie vorübergehend einen anderen Identitätsanbieter aus. Citrix Cloud gestattet keine Trennung Ihres Azure AD, wenn es gleichzeitig als Authentifizierungsmethode für Citrix Workspace verwendet wird. Weitere Informationen finden Sie unter Auswählen und Ändern von Authentifizierungsmethoden in der Dokumentation zu Citrix Workspace.

Wiederverbinden von Azure AD

1. Melden Sie sich als Administrator mit Vollzugriff unter dem Citrix Identitätsanbieter bei Citrix Cloud an.
2. Wählen Sie im Menü “Citrix Cloud”**Identitäts- und Zugriffsverwaltung** und dann **Authentifizierung** aus.
3. Suchen Sie **Azure Active Directory** und wählen Sie im Menü mit den Auslassungspunkten **Trennen**.
4. Wählen Sie im Menü die Option **Verbinden**.

> **Hinweis:**
>
> Wenn Sie die Verbindung zum Azure Active Directory wie in Schritt 3 beschrieben trennen, fordert Citrix Cloud den Administrator auf, alle Administratorprofile unter diesem Identitätsanbieter zu löschen.
> Um diesen Aufwand zu umgehen, kann der Administrator die folgenden Schritte ausführen, um den Azure AD-Identitätsanbieter wieder zu verbinden.
>
> 1. Navigieren Sie als globaler Administrator zu Azure und löschen Sie die App.
> 2. Melden Sie sich bei Citrix Cloud an, navigieren Sie zu **Identitäts- und Zugriffsverwaltung** und klicken Sie auf **Authentifizierung**. Auf der Registerkarte **Authentifizierung** können Sie feststellen, dass Azure AD immer noch verbunden ist.
> 3. Fügen Sie einen neuen Administrator in Citrix Cloud für Azure AD hinzu.

> Dies löst die Neuerstellung der App und die erneute Verbindung aus, ohne dass die Administratoren gelöscht werden.

Azure Active Directory-Berechtigungen für Citrix Cloud

December 11, 2023

In diesem Artikel werden die Berechtigungen beschrieben, die von Citrix Cloud beim Verbinden und Verwenden von Azure Active Directory (AD) angefordert werden. Je nach Art der Verwendung von Azure AD mit dem Citrix Cloud-Konto werden möglicherweise eine oder mehrere Unternehmensanwendungen im Azure AD-Zielmandanten erstellt. Sie können mehrere Citrix Cloud-Konten mit einem Azure AD-Mandanten verbinden und dieselben Unternehmensanwendungen verwenden, ohne für jedes Konto einen Anwendungssatz zu erstellen.

> **Hinweis:**
>
> Ab April 2022 verwendet die Azure AD-App, die Citrix Cloud zum Verbinden Ihres Azure AD verwendet, die Berechtigung GroupMember.Read.All anstelle von Group.Read.All. Wenn Sie eine bestehende Azure AD-Verbindung (vor April 2022) haben und möchten, dass die App die neue Berechtigung verwendet, müssen Sie Ihr Azure AD trennen und dann erneut mit Citrix Cloud verbinden. Diese Aktion stellt sicher, dass Ihr Konto die neueste Azure AD-App in Citrix Cloud verwendet. Weitere Informationen finden Sie unter Wiederverbinden mit Azure AD für die aktualisierte App.
>
> Wenn Sie die App nicht aktualisieren, funktioniert Ihre bestehende Verbindung weiterhin normal.

Unternehmensanwendungen

Die folgende Tabelle enthält die Azure AD-Unternehmensanwendungen, die von Citrix Cloud beim Verbinden und Verwenden von Azure AD genutzt werden, und der Verwendungszweck jeder Anwendung.

Name	Anwendungs-ID	Verwendung
Citrix Cloud	e95c4605-aeab-48d9-9c36-1a262ef8048e	Workspace-Abonnentenanmeldung
Citrix Cloud	f9c0e999-22e7-409f-bb5e-956986abdf02	Standardverbindung zwischen Azure AD und Citrix Cloud

Name	Anwendungs-ID	Verwendung
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	Administratorseinladungen und -anmeldungen
Citrix Cloud	5c913119-2257-4316-9994-5e8f3832265b	Standardverbindung zwischen Azure AD und Citrix Cloud mit Citrix Endpoint Management
Citrix Cloud	e067934c-b52d-4e92-b1ca-70700bd1124e	Legacy-Verbindung zwischen Azure AD und Citrix Cloud mit Citrix Endpoint Management

Berechtigungen

Die Berechtigungen in den Unternehmensanwendungen von Citrix Cloud ermöglichen Citrix Cloud den Zugriff auf bestimmte Daten in Ihrem Azure AD-Mandanten. Anhand dieser Daten kann Citrix Cloud bestimmte Funktionen ausführen, zum Beispiel die Verbindung zu Ihrem Azure AD-Mandanten herstellen, Administratoren mit einer dedizierten Anmelde-URL bei Citrix Cloud anmelden und Ihren Azure AD-Mandanten mit Endpoint Management verbinden. Citrix Cloud kann nur mit Ihrer Zustimmung auf diese Daten zugreifen. Die Berechtigungen stellen das Mindestmaß an Privilegien dar, die Citrix Cloud benötigt, um mit Ihrem Azure AD zu funktionieren. Weitere Informationen zu Azure AD-Berechtigungen und zur Zustimmung finden Sie unter Permissions and consent in the Microsoft identity platform in der Dokumentation zu Microsoft Azure.

In diesem Artikel enthält jede Gruppe von Azure AD-Anwendungsberechtigungen die folgenden Informationen:

- **API-Name:** Die Ressourcenanwendungen, von denen Citrix Cloud Berechtigungen anfordert. Diese Anwendungen sind Microsoft Graph und Windows Azure Active Directory. Citrix Cloud fordert von beiden Ressourcenanwendungen dieselben Berechtigungen an.
- **Typ:** Die Zugriffsebenen, die Citrix Cloud für eine bestimmte Berechtigung anfordert. Berechtigungen in einer Unternehmensanwendung können eine der folgenden Zugriffsebenen haben:
  - **Delegierte Berechtigungen** werden verwendet, um im Namen eines angemeldeten Benutzers zu agieren, z. B. beim Abfragen des Benutzerprofils.
  - **Anwendungsberechtigungen** werden verwendet, wenn die Anwendung eine Aktion in Abwesenheit des Benutzers ausführt, z. B. beim Abfragen von Benutzern innerhalb einer bestimmten Gruppe. Dieser Berechtigungstyp erfordert die Zustimmung eines globalen Administrators in Azure AD.
- **Anspruchswert:** Die Zeichenfolge, die Azure AD einer bestimmten Berechtigung zuweist.

Berechtigungen in einer Unternehmensanwendung können einen der folgenden Zugriffswerte haben:

- **User.Read:** Hiermit können Citrix Cloud-Administratoren Benutzer aus dem verbundenen Azure AD als Administratoren zum Citrix Cloud-Konto hinzuzufügen.
- **User.ReadBasic.All:** Sammelt grundlegende Informationen aus dem Benutzerprofil. Dies ist eine Teilmenge von User.Read.All, die Berechtigung selbst verbleibt jedoch zur Abwärtskompatibilität.
- **User.Read.All:** Citrix Cloud ruft Benutzer auflisten in Microsoft Graph auf, um das Durchsuchen und Auswählen von Benutzern aus dem verbundenen Azure AD des Kunden zu aktivieren. Beispielsweise können Benutzer von Azure AD aus Zugriff auf eine Citrix DaaS-Ressource mit dem Workspace erhalten. Citrix Cloud kann `User.ReadBasic.All` nicht verwenden, da Citrix Cloud Zugriff auf Eigenschaften außerhalb des grundlegenden Profils (z. B. `onPremisesSecurityIdentifier`) benötigt.
- **GroupMember.Read.All:** Citrix Cloud ruft Gruppen auflisten in Microsoft Graph auf, um das Durchsuchen und Auswählen von Gruppen aus dem verbundenen Azure AD des Kunden zu aktivieren. Beispielsweise können Gruppen von Azure AD aus auch Zugriff auf Citrix DaaS-Anwendungen erhalten.
- **Directory.Read.All:** Citrix Cloud ruft memberOf auflisten in Microsoft Graph auf, um die Gruppenmitgliedschaft des Benutzers abzurufen, da `Groups.Read.All` nicht ausreicht.
- **DeviceManagementApps.ReadWrite.All:** Hiermit kann Citrix Cloud von Microsoft Intune verwaltete Eigenschaften, Gruppenzuweisungen, den Status von Apps, App-Konfigurationen und App-Schutzrichtlinien lesen und bearbeiten.
- **Directory.AccessAsUser.All:** Hiermit erhält Citrix Cloud den gleichen Zugriff auf Informationen im Verzeichnis wie der angemeldete Benutzer.

> **Hinweis:**
>
> **Directory.Read.All** gilt nur für **Standardverbindung zwischen Azure AD und Citrix Cloud mit Endpoint Management**.

Workspace-Abonnentenanmeldung

Diese Citrix Cloud-Anwendung (ID: e95c4605-aeab-48d9-9c36-1a262ef8048e) verwendet die folgenden Berechtigungen:

API-Name	Anspruchswert	Berechtigungswert	Typ
Microsoft Graph	User.Read	Anmelden und Benutzerprofil lesen	Delegiert

Standardverbindung zwischen Azure AD und Citrix Cloud

Diese Citrix Cloud-Anwendung (ID: f9c0e999-22e7-409f-bb5e-956986abdf02) verwendet die folgenden Berechtigungen:

API-Name	Anspruchswert	Berechtigung	Typ
Microsoft Graph	GroupMember.Read.All	Alle Gruppen lesen	Delegiert
Microsoft Graph	User.ReadBasic.All	Grundlegende Profile aller Benutzer lesen	Delegiert
Microsoft Graph	User.Read.All	Vollständige Profile aller Benutzer lesen	Delegiert
Microsoft Graph	User.Read	Anmelden und Benutzerprofil lesen	Delegiert
Microsoft Graph	GroupMember.Read.All	Alle Gruppen lesen	Anwendung
Microsoft Graph	User.Read.All	Vollständiges Profil aller Benutzer lesen	Anwendung
Microsoft Graph	User.Read	Anmelden und Benutzerprofil lesen	Anwendung

Administratorseinladungen und -anmeldungen

Diese Citrix Cloud-Anwendung (ID: 1b32f261-b20c-4399-8368-c8f0092b4470) verwendet die folgenden Berechtigungen:

API-Name	Anspruchswert	Berechtigungswert	Typ
Microsoft Graph	User.Read	Anmelden und Benutzerprofil lesen	Delegiert
Microsoft Graph	User.ReadBasic.All	Grundlegende Profile aller Benutzer lesen	Delegiert

Standardverbindung zwischen Azure AD und Citrix Cloud mit Endpoint Management

Diese Citrix Cloud-Anwendung (ID: 5c913119-2257-4316-9994-5e8f3832265b) verwendet die folgenden Berechtigungen:

API-Name	Anspruchswert	Berechtigungswert	Typ
Microsoft Graph	GroupMember.Read.All	Alle Gruppen lesen	Delegiert
Microsoft Graph	User.ReadBasic.All	Grundlegende Profile aller Benutzer lesen	Delegiert
Microsoft Graph	User.Read	Anmelden und Benutzerprofil lesen	Delegiert
Microsoft Graph	Directory.Read.All	Verzeichnisdaten lesen	Anwendung
Microsoft Graph	Directory.Read.All	Verzeichnisdaten lesen	Delegiert
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Microsoft Intune-Apps lesen und schreiben	Delegiert
Microsoft Graph	Directory.AccessAsUser.All	Als angemeldeter Benutzer auf das Verzeichnis zugreifen	Delegiert

Legacy-Verbindung zwischen Azure AD und Citrix Cloud mit Endpoint Management

Diese Citrix Cloud-Anwendung (ID: e067934c-b52d-4e92-b1ca-70700bd1124e) verwendet die folgenden Berechtigungen:

API-Name	Anspruchswert	Berechtigungswert	Typ
Microsoft Graph	GroupMember.Read.All	Alle Gruppen lesen	Delegiert
Microsoft Graph	User.ReadBasic.All	Grundlegende Profile aller Benutzer lesen	Delegiert
Microsoft Graph	User.Read	Anmelden und Benutzerprofil lesen	Delegiert
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Microsoft Intune-Apps lesen und schreiben	Delegiert
Microsoft Graph	Directory.AccessAsUser.All	Als angemeldeter Benutzer auf das Verzeichnis zugreifen	Delegiert

Verbinden eines on-premises Citrix Gateway als Identitätsanbieter mit Citrix Cloud

July 2, 2024

Citrix Cloud unterstützt die Verwendung eines on-premises Citrix Gateway als Identitätsanbieter für die Authentifizierung von Abonnenten, wenn diese sich bei ihrem Workspace anmelden.

Vorteile der Authentifizierung mit Citrix Gateway:

- Fortdauernde Authentifizierung von Benutzern über das vorhandene Citrix Gateway, damit sie über Citrix Workspace auf die Ressourcen in der On-Premises-Bereitstellung von Virtual Apps and Desktops zugreifen können.
- Verwenden Sie die AAA-Funktionen (Authentifizierung, Autorisierung und Auditing) von Citrix Gateway mit Citrix Workspace.
- Verwendung von Features wie Passthrough-Authentifizierung, Smartcards, Sicherheitstoken, Richtlinien für bedingten Zugriff, Verbund usw. für den Benutzerzugriff auf erforderliche Ressourcen über Citrix Workspace.

> **Tipp:**
>
> Im Kurs Introduction to Citrix Identity and Authentication erfahren Sie mehr über unterstützte Identitätsanbieter. Das Modul „Planning Citrix Identity and Access Management“enthält kurze Videos zum Verbinden des Identitätsanbieters mit Citrix Cloud und zum Aktivieren der Authentifizierung für Citrix Workspace.

Unterstützte Versionen

Die Authentifizierung mit Citrix Gateway wird für folgende On-Premises-Produktversionen unterstützt:

- Citrix Gateway 12.1 54.13 Advanced Edition oder höher
- Citrix Gateway 13.0 41.20 Advanced Edition oder höher

Voraussetzungen

Cloud Connectors

Sie benötigen mindestens zwei (2) Server zum Installieren der Citrix Cloud Connector-Software. Die Server müssen die folgenden Anforderungen erfüllen:

- Die unter Technische Daten zu Citrix Cloud Connector beschriebenen Systemanforderungen müssen erfüllt sein.
- Es dürfen keine anderen Komponenten von Citrix installiert sein. Die Server dürfen keine Active Directory-Domänencontroller oder Maschinen sein, die für Ihre Ressourcenstandortinfrastruktur kritisch sind.
- Sie müssen mit der Domäne verbunden sein, in der sich Ihre Site befindet. Wenn Benutzer auf Anwendungen zugreifen, die sich in mehreren Domänen der Site befinden, müssen Sie in jeder Domäne mindestens zwei Cloud Connectors installieren.
- Die Server müssen mit einem Netzwerk verbunden sein, das Ihre Site kontaktieren kann.
- Eine Verbindung mit dem Internet muss bestehen. Weitere Informationen finden Sie unter Anforderungen an System und Konnektivität.
- Mindestens zwei Cloud Connectors sind erforderlich, um eine hochverfügbare Verbindung mit Citrix Cloud sicherzustellen. Nach der Installation ermöglichen die Cloud Connectors Citrix Cloud, Ihre Site zu lokalisieren und mit ihr zu kommunizieren.

Weitere Informationen zur Installation des Cloud Connectors finden Sie unter Cloud Connector-Installation.

Active Directory

Führen Sie vor dem Aktivieren der Authentifizierung mit Citrix Gateway die folgenden Aufgaben aus:

- Stellen Sie sicher, dass Ihre Workspace-Abonnenten über Benutzerkonten in Active Directory (AD) verfügen. Abonnenten ohne AD-Konto können sich nicht erfolgreich bei ihrem Workspace anmelden.
- Stellen Sie sicher, dass die Benutzereigenschaften in den AD-Konten Ihrer Abonnenten ausgefüllt sind. Citrix Cloud benötigt diese Eigenschaften, um den Benutzerkontext bei der Anmeldung von Abonnenten zu erfassen. Wenn diese Eigenschaften nicht ausgefüllt werden, können Abonnenten sich nicht bei ihrem Workspace anmelden. Zu diesen Eigenschaften gehören:
  - E-Mail-Adresse
  - Anzeigename
  - Allgemeiner Name
  - SAM-Kontoname
  - Benutzerprinzipalname
  - OID
  - SID
- Verbinden Sie Ihr Active Directory (AD) mit Ihrem Citrix Cloud-Konto. Diese Aufgabe umfasst das Installieren der Cloud Connector-Software auf den vorbereiteten Servern, wie im Abschnitt Cloud Connectors beschrieben. Die Cloud Connectors ermöglichen eine Kommunikation zwis-

chen Citrix Cloud und der On-Premises-Umgebung. Anweisungen finden Sie unter Verbinden von Active Directory mit Citrix Cloud.

- Synchronisieren Sie bei einer Verbundauthentifizierung mit Citrix Gateway Ihre AD-Benutzer mit dem Verbundanbieter. Citrix Cloud benötigt die AD-Benutzerattribute Ihrer Workspace-Abonnenten, damit diese sich erfolgreich anmelden können.

Anforderungen

Erweiterte Citrix Gateway-Richtlinien

Für die Citrix Gateway-Authentifizierung müssen erweiterte Richtlinien auf dem On-Premises-Gateway verwendet werden, da klassische Richtlinien veraltet sind. Erweiterte Richtlinien unterstützen die Multifaktorauthentifizierung für Citrix Cloud, einschließlich Optionen wie Identitätsanbieterverkettung. Wenn Sie bislang klassische Richtlinien nutzen, müssen Sie neue erweiterte Richtlinien erstellen, um die Citrix Gateway-Authentifizierung in Citrix Cloud zu verwenden. Beim Erstellen der erweiterten Richtlinie können Sie den Aktionsbestandteil der klassischen Richtlinie übernehmen.

Zertifikate für die Signatur

Beim Konfigurieren des Gateways für die Authentifizierung von Abonnenten bei Citrix Workspace fungiert das Gateway als OpenID Connect-Anbieter. Nachrichten zwischen Citrix Cloud und Gateway entsprechen dem OIDC-Protokoll, was auch die digitale Signatur von Token umfasst. Daher müssen Sie ein Zertifikat zur Signatur dieser Token konfigurieren. Dieses Zertifikat muss von einer öffentlichen Zertifizierungsstelle (ZS) ausgestellt werden. Zertifikate einer privaten Zertifizierungsstelle werden nicht unterstützt, da Citrix Cloud nicht auf das Stammzertifikat der privaten Zertifizierungsstelle zugreifen kann. Daher kann keine Vertrauenskette für das Zertifikat hergestellt werden. Wenn Sie mehrere Zertifikate für die Signatur konfigurieren, wird für jede Nachricht ein anderer Schlüssel verwendet.

Schlüssel müssen an **vpn global** gebunden sein. Ohne diese Schlüssel können Abonnenten nach der Anmeldung nicht auf ihren Workspace zugreifen.

Uhrsynchronisierung

Da digital signierte Nachrichten in OIDC einen Zeitstempel aufweisen, muss das Gateway mit der NTP-Zeit synchronisiert werden. Wenn die Uhr nicht synchronisiert wird, werden Token in Citrix Cloud bei der Gültigkeitsprüfung als veraltet eingestuft.

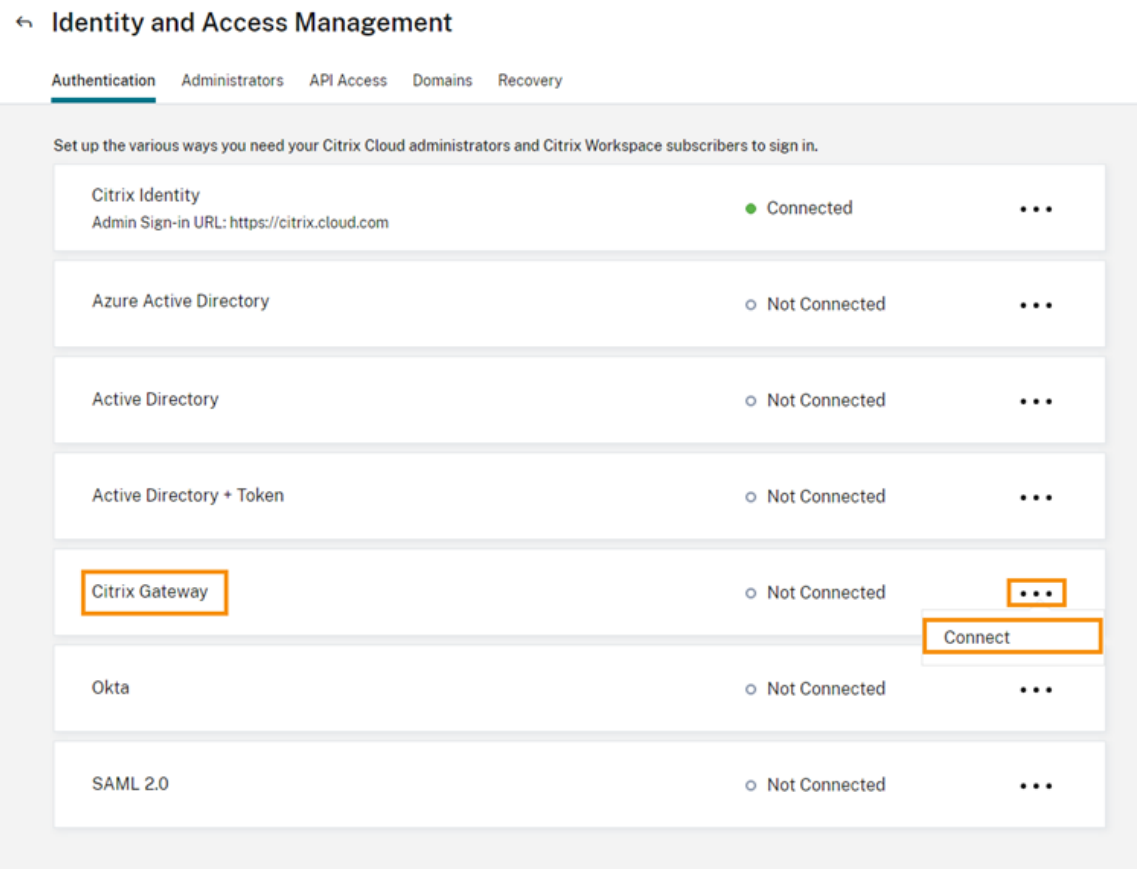
Aufgabenüberblick

Zum Einrichten der Authentifizierung mit Citrix Gateway führen Sie die folgenden Aufgaben aus:

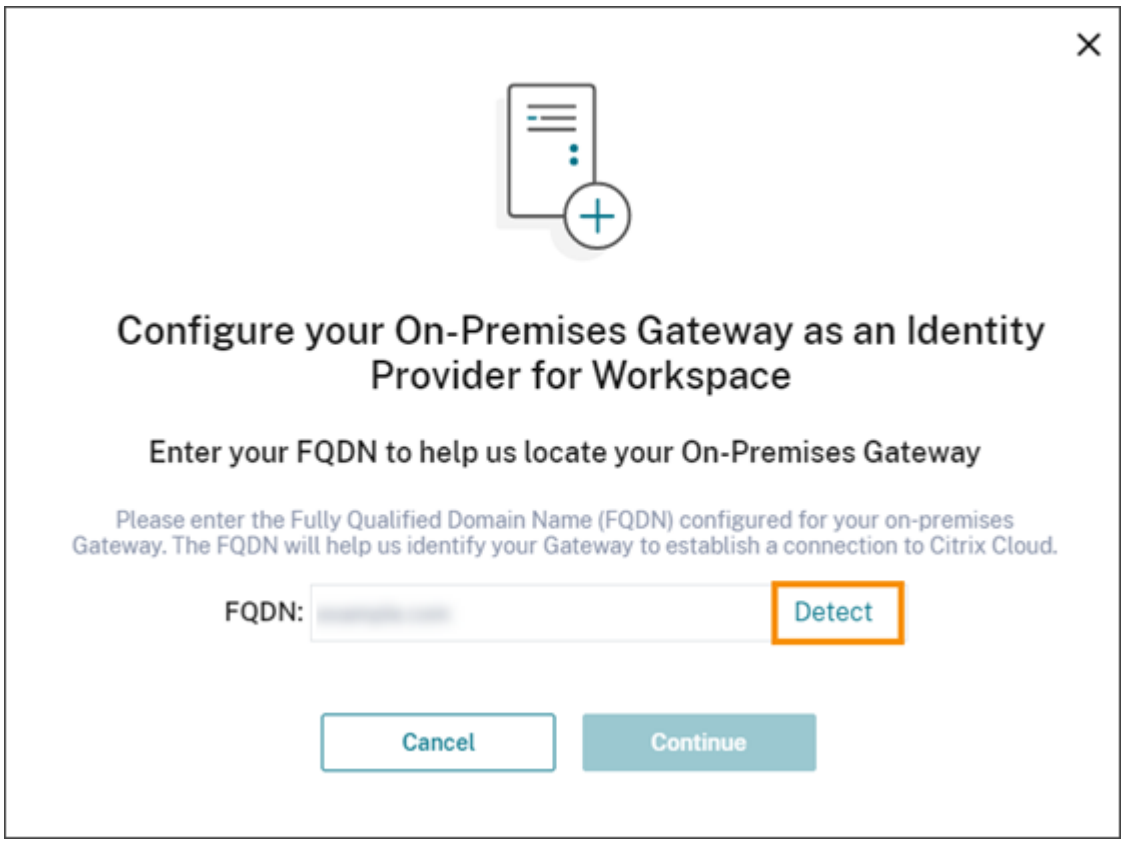
1. Konfigurieren Sie unter **Identitäts- und Zugriffsverwaltung** die Verbindung zum Gateway. In diesem Schritt generieren Sie Client-ID, Geheimnis und Umleitungs-URL für das Gateway.
2. Erstellen Sie auf dem Gateway eine erweiterte OAuth-IdP-Richtlinie mit den generierten Informationen aus Citrix Cloud. Dadurch kann Citrix Cloud eine Verbindung mit Ihrem On-Premises-Gateway herstellen. Anweisungen finden Sie in folgenden Artikeln:
   - Citrix Gateway 12.1: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
   - Citrix Gateway 13.0: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
3. Aktivieren Sie unter **Workspacekonfiguration** die Citrix Gateway-Authentifizierung für Abonnenten.

Aktivieren der Authentifizierung mit Citrix Gateway für Workspace-Abonnenten

1. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.
2. Klicken Sie auf der Registerkarte **Authentifizierung** auf die Auslassungspunkte (…) für **Citrix Gateway** und wählen Sie den Menübefehl **Verbinden**.



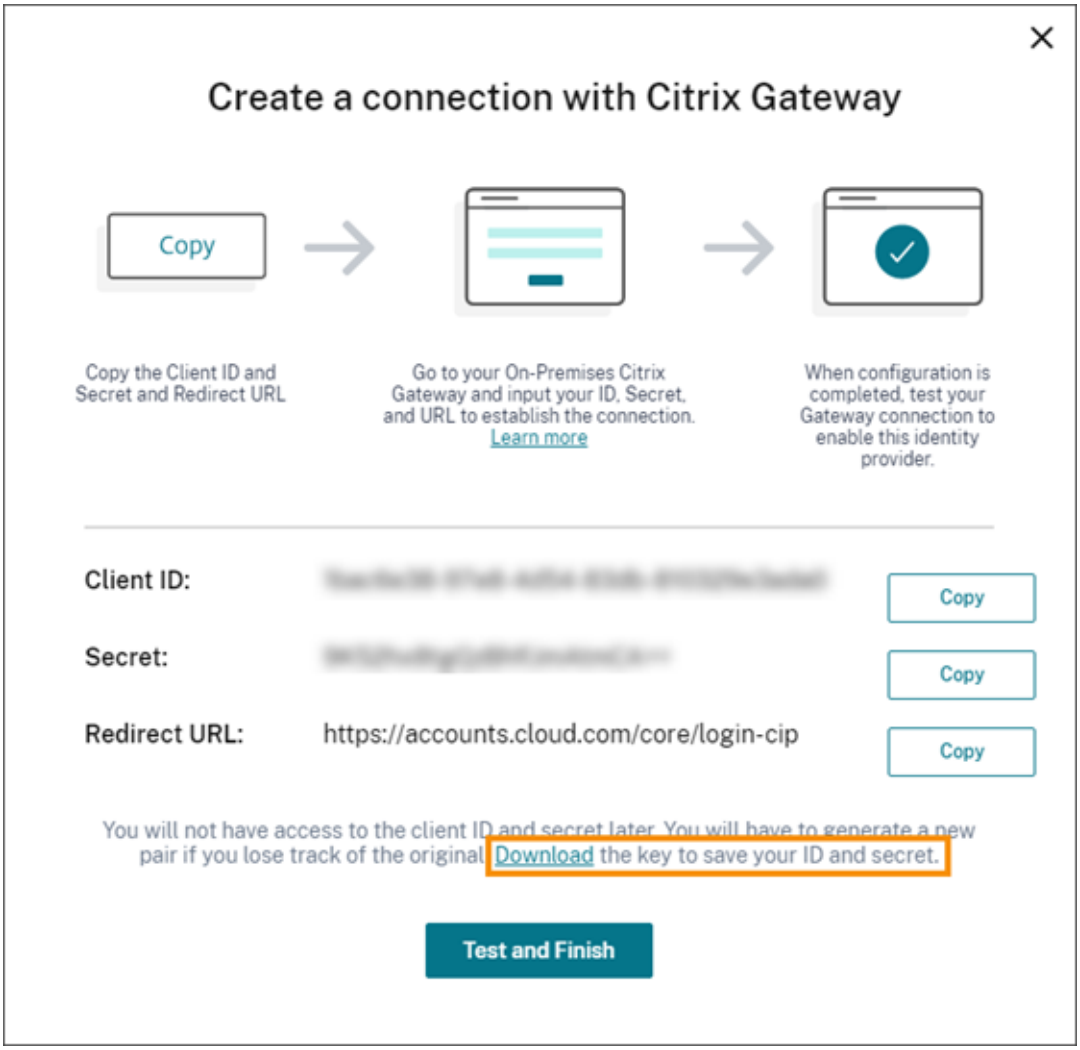
3. Geben Sie den FQDN des On-Premises-Gateways ein und klicken Sie auf **Ermitteln**.



Nachdem der FQDN von Citrix Cloud ermittelt wurde, klicken Sie auf **Weiter.**.

4. Erstellen Sie eine Verbindung mit dem On-premises-Gateway:

   a) Kopieren Sie Client-ID, Geheimnis und Umleitungs-URL, die in Citrix Cloud angezeigt werden.



Laden Sie eine Kopie der Informationen herunter und speichern Sie sie offline an einem sicheren Ort. Die Informationen sind nach dem Generieren in Citrix Cloud nicht mehr verfügbar.

b) Erstellen Sie auf dem Gateway eine erweiterte OAuth-IdP-Richtlinie mit Client-ID, Geheimnis und Umleitungs-URL aus Citrix Cloud. Anweisungen finden Sie in folgenden Artikeln:

- Für Citrix Gateway 12.1: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
- Für Citrix Gateway 13.0: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud

c) Klicken Sie auf **Testen und schließen**. Citrix Cloud überprüft, ob Ihr Gateway erreichbar und ordnungsgemäß konfiguriert ist.

5. Aktivieren Sie die Authentifizierung mit Citrix Gateway für Workspaces:

a) Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration**.
b) Wählen Sie auf der Registerkarte **Authentifizierung** die Option **Citrix Gateway**.

c) Wählen Sie **Ich verstehe die Auswirkungen auf Abonnenten** und klicken Sie auf **Speichern**.

Problembehandlung

Lesen Sie zunächst die Abschnitte Voraussetzung und Anforderungen in diesem Artikel. Stellen Sie sicher, dass alle erforderlichen Komponenten in der On-Premises-Umgebung vorhanden sind und dass Sie alle erforderlichen Konfigurationen vorgenommen haben. Wenn eines dieser Elemente fehlt oder falsch konfiguriert ist, funktioniert die Authentifizierung beim Workspace mit Citrix Gateway nicht.

Bei Problemen mit der Verbindung zwischen Citrix Cloud und dem On-Premises-Gateway stellen Sie Folgendes sicher:

- Der Gateway-FQDN kann über das Internet erreicht werden.
- Der Gateway-FQDN wurde korrekt in Citrix Cloud eingegeben.
- Sie haben die Gateway-URL korrekt in den Parameter `-issuer` der OAuth-IdP-Richtlinie eingegeben. Beispiel: `-issuer https://GatewayFQDN.com`. Bei dem Parameter `issuer` wird zwischen Groß- und Kleinschreibung unterschieden.
- Die Werte für Client-ID, Geheimnis und Umleitungs-URL aus Citrix Cloud wurden korrekt in die Felder für Client-ID, Clientgeheimnis, Umleitungs-URL und Zielgruppe der OAuth-IdP-Richtlinie eingegeben. Überprüfen Sie, ob im Feld “Zielgruppe”der Richtlinie die richtige Client-ID eingegeben wurde.
- Die OAuth-IdP-Authentifizierungsrichtlinie ist korrekt konfiguriert. Anweisungen finden Sie in folgenden Artikeln:
  - Citrix Gateway 12.1: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
  - Citrix Gateway 13.0: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
- Stellen Sie sicher, dass die Richtlinie ordnungsgemäß an den AAA-Authentifizierungsserver gebunden ist, wie unter Binding Authentication Policies beschrieben.

Globale Katalogserver

Neben den Details zum Benutzerkonto ruft Gateway auch den Domänennamen der Benutzer, den AD NETBIOS-Namen und den Namen der AD-Stammdomäne ab. Zum Abrufen des AD NETBIOS-Namen durchsucht Gateway das Active Directory, in dem sich die Benutzerkonten befinden. NETBIOS-Namen werden nicht auf globalen Katalogservern repliziert.

Wenn Sie globale Katalogserver in Ihrer AD-Umgebung verwenden, funktionieren die auf diesen Servern konfigurierten LDAP-Aktionen nicht mit Citrix Cloud. Stattdessen müssen Sie die einzelnen Active Directorys in der LDAP-Aktion konfigurieren. Wenn Sie mehrere Domänen oder Gesamtstrukturen verwenden, können Sie mehrere LDAP-Richtlinien konfigurieren.

AD-Suche nach Single Sign-On mit Kerberos- oder IdP-Verkettung

Bei Einsatz von Kerberos oder eines externen Identitätsanbieters, der SAML- oder OIDC-Protokolle zum Anmelden von Abonnenten verwendet, muss die AD-Suche konfiguriert ist. Gateway benötigt die AD-Suche zum Abrufen der AD-Benutzereigenschaften von Abonnenten und der AD-Konfigurationseigenschaften.

Stellen Sie sicher, dass LDAP-Richtlinien konfiguriert sind, auch wenn die Authentifizierung über Server von Drittanbietern erfolgt. Um diese Richtlinien zu konfigurieren, fügen Sie Ihrem vorhandenen Anmeldeschemaprofil einen zweiten Authentifizierungsfaktor hinzu, indem Sie die folgenden Aufgaben ausführen:

1. Erstellen Sie einen LDAP-Authentifizierungsserver, der nur Attribut- und Gruppenextraktion aus Active Directory durchführt.
2. Erstellen Sie eine erweiterte LDAP-Authentifizierungsrichtlinie.
3. Erstellen Sie eine Authentifizierungsrichtlinienbezeichnung.
4. Definieren Sie die Authentifizierungsrichtlinienbezeichnung als nächsten Faktor nach dem primären Identitätsanbieter.

So fügen Sie LDAP als zweiten Authentifizierungsfaktor hinzu

1. Erstellen Sie den LDAP-Authentifizierungsserver:
    a) Wählen Sie **System > Authentifizierung > Grundlegende Richtlinien > LDAP > Server > Hinzufügen**.
    b) Geben Sie auf der Seite **LDAP-Authentifizierungsserver erstellen** die folgenden Informationen ein:
        - Wählen Sie unter **Servertyp auswählen** die Option **LDAP** aus.
        - Geben Sie unter **Name** einen Anzeigenamen für den Server ein.
        - Wählen Sie **Server-IP** aus, und geben Sie dann die IP-Adresse des LDAP-Servers ein.
        - Wählen Sie unter **Sicherheitstyp** den gewünschten LDAP-Sicherheitstyp aus.
        - Wählen Sie unter **Servertyp** die Option **AD** aus.
        - Aktivieren Sie unter **Authentifizierung** nicht das Kontrollkästchen. Dieses Kontrollkästchen muss deaktiviert werden, da dieser Authentifizierungsserver nur zum Extrahieren von Benutzerattributen und -gruppen aus Active Directory dient und nicht zur Authentifizierung.

c) Geben Sie unter **Andere Einstellungen** die folgenden Informationen ein:

- Geben Sie unter **Namensattribut für Serveranmeldung UserPrincipalName** ein.
- Wählen Sie unter **Gruppenattribut** die Option **MemberOf** aus.
- Wählen Sie unter **Unterattributname** die Option **cn** aus.

2. Erstellen Sie die erweiterte LDAP-Authentifizierungsrichtlinie:

a) Wählen Sie **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie > Hinzufügen** aus.
b) Geben Sie auf der Seite **Authentifizierungsrichtlinie erstellen** die folgenden Informationen ein:

- Geben Sie unter **Name** einen Anzeigenamen für die Richtlinie ein.
- Wählen Sie unter **Aktionstyp LDAP**aus.
- Wählen Sie unter **Aktion** den zuvor erstellten LDAP-Authentifizierungsserver aus.
- Geben Sie unter **Ausdruck TRUE**ein.

c) Klicken Sie auf **Erstellen**, um die Konfiguration zu speichern.

3. Erstellen Sie die Authentifizierungsrichtlinienbezeichnung.

a) Wählen Sie **Sicherheit > AAA –Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinienbezeichnung > Hinzufügen**.
b) Geben Sie unter **Name**einen Anzeigenamen für die Authentifizierungsrichtlinienbezeichnung ein.
c) Wählen Sie unter Anmeldeschema **LSCHEMA_INT** aus.
d) Wählen Sie unter **Richtlinienbindung** unter **Richtlinie auswählen** die erweiterte LDAP-Authentifizierungsrichtlinie aus, die Sie zuvor erstellt haben.
e) Wählen Sie unter **Gehe zu Ausdruck END**aus.
f) Klicken Sie auf **Binden**, um die Konfiguration abzuschließen.

4. Definieren Sie die LDAP-Authentifizierungsrichtlinienbezeichnung als nächster Faktor nach dem primären Identitätsanbieter:

a) Wählen Sie **System > Sicherheit > AAA - Anwendungsverkehr > Virtuelle Server**.
b) Wählen Sie den virtuellen Server aus, der die Bindung für Ihren primären Identitätsanbieter enthält, und wählen Sie **Bearbeiten** aus.
c) Wählen Sie unter **Erweiterte Authentifizierungsrichtlinien** die vorhandenen Bindungen für **Authentifizierungsrichtlinie** aus.
d) Wählen Sie die Bindung für Ihren primären Identitätsanbieter aus, und wählen Sie dann **Bindung bearbeiten** aus.
e) Wählen Sie auf der Seite **Richtlinienbindung** unter **Nächsten Faktor auswählen** die LDAP-Authentifizierungsrichtlinienbezeichnung aus, die Sie zuvor erstellt haben.
f) Klicken Sie auf **Binden**, um die Konfiguration zu speichern.

Standardkennwort für die Multifaktorauthentifizierung

Wenn Sie die Multifaktorauthentifizierung für Workspace-Abonnenten verwenden, nutzt Gateway das Kennwort der letzten Stufe als Standardkennwort für den Single Sign-On. Dieses Kennwort wird an Citrix Cloud gesendet, wenn Abonnenten sich an ihrem Workspace anmelden. Wenn in Ihrer Umgebung nach der LDAP-Authentifizierung eine weitere Stufe folgt, müssen Sie das LDAP-Kennwort als Standardkennwort konfigurieren, das an Citrix Cloud gesendet wird. Aktivieren Sie **SSOCredentials** im Anmeldeschema, das der LDAP-Stufe entspricht.

Weitere Informationen

Citrix Tech Zone: Tech Insight: Authentication - Gateway

Google Cloud Identity als Identitätsanbieter mit Citrix Cloud verbinden

September 28, 2023

Citrix Cloud unterstützt die Verwendung von Google Cloud Identity als Identitätsanbieter für die Authentifizierung von Abonnenten, die sich an ihrem Workspace anmelden. Indem Sie das Google-Konto Ihrer Organisation mit Citrix Cloud verbinden, können Sie eine einheitliche Anmeldung für Citrix Workspace- und Google-Ressourcen bereitstellen.

Anforderungen für die Konfiguration mit und ohne Domäneneinbindung

Sie können Google Cloud Identity als Identitätsanbieter in Citrix Cloud unter Verwendung einer Maschine mit oder ohne Domäneneinbindung konfigurieren.

- Mit Domäneneinbindung bedeutet, dass die Maschinen zu einer Domäne in Ihrem On-Premises-Active Directory (AD) gehören und bei der Authentifizierung die dort gespeicherten Benutzerprofile verwendet werden.
- Ohne Domäneneinbindung bedeutet, dass die Maschinen keiner AD-Domäne angehören und bei der Authentifizierung die im Google Workspace-Verzeichnis gespeicherten Benutzerprofile verwendet werden (= Google-native Benutzer).

In der folgenden Tabelle sind die Anforderungen für beide Konfigurationen aufgeführt.

Voraussetzung	In Domäne	Nicht in Domäne	Weitere Informationen
On-Premises-AD	Ja	Nein	Siehe Vorbereiten von Active Directory und Citrix Cloud Connectors in diesem Artikel.
Am Ressourcenstandort bereitgestellte Citrix Cloud Connectors	Ja	Nein, Cloud Connectors werden nicht benötigt, um auf Maschinen ohne Domänenbindung zuzugreifen.	Siehe Vorbereiten von Active Directory und Citrix Cloud Connectors in diesem Artikel.
AD-Synchronisierung mit Google Cloud	Nur optional, wenn Gateway Service und keine anderen Services verwendet werden. Andernfalls erforderlich.	Nein	Siehe Synchronisieren von Active Directory mit Google Cloud Identity in diesem Artikel.
Entwicklerkonto mit Zugriff auf die Google Cloud Platform-Konsole. Erforderlich, um ein Dienstkonto und einen Schlüssel zu erstellen und die Admin SDK-API zu verwenden.	Ja	Ja	Siehe Erstellen eines Dienstkontos, Erstellen eines Dienstkontoschlüssels und Konfigurieren der domänenweiten Delegierung in diesem Artikel.
Administratorkonto mit Zugriff auf die Google Workspace-Administratorkonsole. Für die Konfiguration der domänenweiten Delegierung und eines API-Benutzerkontos mit Schreibzugriff erforderlich.	Ja	Ja	Siehe Konfigurieren der domänenweiten Delegierung und Hinzufügen eines API-Benutzerkontos mit Schreibzugriff in diesem Artikel.

Authentifizierung mit mehreren Citrix Cloud-Konten

In diesem Artikel wird beschrieben, wie Sie Google Cloud Identity als Identitätsanbieter mit einem Citrix Cloud-Konto verbinden. Wenn Sie mehrere Citrix Cloud-Konten haben, können Sie alle mit demselben Google Cloud-Konto verbinden, indem Sie dasselbe Dienstkonto und dasselbe schreibgeschützte API-Benutzerkonto verwenden. Melden Sie sich einfach bei Citrix Cloud an und wählen Sie die entsprechende Kunden-ID aus der Kundenauswahl aus.

Vorbereiten von Active Directory und Citrix Cloud Connectors

Wenn Sie eine Maschine **mit Domänenbindung** mit Google Cloud Identity verwenden, bereiten Sie das On-Premises-AD wie in diesem Abschnitt erläutert vor. Wenn Sie Maschine ohne Domänenbindung verwenden, überspringen Sie diese Aufgabe und fahren Sie mit Erstellen eines Dienstkontos in diesem Artikel fort.

Sie benötigen in Ihrer Active Directory-Domäne mindestens zwei (2) Server, auf denen Sie die Citrix Cloud Connector-Software installieren. Cloud Connectors sind für die Kommunikation zwischen Citrix Cloud und Ihrem Ressourcenstandort erforderlich. Mindestens zwei Cloud Connectors sind erforderlich, um eine hochverfügbare Verbindung mit Citrix Cloud sicherzustellen. Die Server müssen die folgenden Anforderungen erfüllen:

- Die unter Technische Daten zu Citrix Cloud Connector beschriebenen Anforderungen müssen erfüllt sein.
- Es dürfen keine anderen Komponenten von Citrix installiert sein. Die Server dürfen keine Active Directory-Domänencontroller oder Maschinen sein, die für Ihre Ressourcenstandortinfrastruktur kritisch sind.
- Gehört zu Ihrer Active Directory-Domäne. Wenn sich Ihre Workspace-Ressourcen und -Benutzer in mehreren Domänen befinden, müssen Sie in jeder Domäne mindestens zwei Cloud Connectors installieren. Weitere Informationen finden Sie unter Bereitstellungsszenarios für Cloud Connectors in Active Directory.
- Es muss eine Verbindung zum Netzwerk bestehen, das die Ressourcen abrufen kann, auf die Benutzer über Citrix Workspace zugreifen.
- Eine Verbindung mit dem Internet muss bestehen. Weitere Informationen finden Sie unter Anforderungen an System und Konnektivität.

Weitere Informationen zur Installation von Cloud Connectors finden Sie unter Cloud Connector-Installation.

Synchronisieren von Active Directory mit Google Cloud Identity

Wenn Sie eine Maschine **mit Domänenbindung** mit Google Cloud Identity verwenden, bereiten Sie das On-Premises-AD wie in diesem Abschnitt erläutert vor. Wenn Sie Maschine ohne Domänenbindung verwenden, überspringen Sie diese Aufgabe und fahren Sie mit Erstellen eines Dienstkontos in diesem Artikel fort.

Das Synchronisieren Ihres AD mit Google Cloud Identity ist optional, wenn Sie nur den Citrix Gateway Service verwenden, ohne dass andere Dienste aktiviert sind. Nur für diese Dienste können Sie Google-native Benutzer verwenden, ohne eine Synchronisierung mit Ihrem AD durchführen zu müssen.

Wenn Sie andere Citrix Cloud-Dienste verwenden, ist die Synchronisierung Ihres AD mit Google Cloud Identity erforderlich. Google Cloud muss die folgenden AD-Benutzerattribute an Citrix Cloud übergeben:

- SecurityIDentifier (SID)
- objectGUID
- userPrincipalName (UPN)

Synchronisieren von AD mit Google Cloud

1. Laden Sie das Hilfsprogramm Google Cloud Directory Sync von der Google-Website herunter und installieren Sie es. Weitere Informationen zu diesem Hilfsprogramm finden Sie in der Dokumentation zu Google Cloud Directory Sync auf der Google-Website.
2. Starten Sie nach der Installation des Hilfsprogramms den Configuration Manager (**Start > Configuration Manager**).
3. Geben Sie die Google-Domäneneinstellungen und LDAP-Einstellungen an (siehe Set up your sync with Configuration Manager in der Dokumentation zum Hilfsprogramm).
4. Wählen Sie unter **General Settings** die Option **Custom Schemas**. Behalten Sie die Standardauswahl bei.
5. Konfigurieren Sie ein benutzerdefiniertes Schema, das auf alle Benutzerkonten angewendet wird. Geben Sie die erforderlichen Informationen unter Befolgung der in diesem Abschnitt angegebenen Groß- und Kleinschreibung ein.

    a) Wählen Sie die Registerkarte **Custom Schemas** und dann **Add Schema**.
    b) Wählen Sie **Use rules defined in "User Accounts"**.
    c) Geben Sie im Feld **Schema Name** die Zeichenfolge **citrix-schema** ein.
    d) Wählen Sie **Add Field** und geben Sie dann die folgenden Informationen ein:
        - Wählen Sie unter **Schema field template** in **Schema Field** die Option **userPrincipalName**.
        - Geben Sie unter **Google field details** in **Field Name** die Zeichenfolge **UPN** ein.
    e) Wiederholen Sie Schritt 4, um die folgenden Felder zu erstellen:

- objectGUID: Wählen Sie unter **Schema field template** die Option **objectGUID**. Geben Sie unter **Google field details** die Zeichenfolge **objectGUID** ein.
- SID: Wählen Sie unter **Schema field template** die Option **Custom**. Geben Sie unter **Google field details** die Zeichenfolge **SID** ein.
- objectSID: Wählen Sie unter **Schema field template** die Option **Custom**. Geben Sie unter **Google field details** die Zeichenfolge **objectSID** ein.

f) Wählen Sie **OK**, um Ihre Einträge zu speichern.

6. Konfigurieren Sie die verbleibenden Einstellungen für Ihre Organisation und überprüfen Sie die Synchronisierungseinstellungen (siehe Set up your sync with Configuration Manager in der Dokumentation zum Hilfsprogramm).
7. Wählen Sie **Sync & apply changes**, um Ihr Active Directory mit Ihrem Google-Konto zu synchronisieren.

Nach Abschluss der Synchronisierung werden im Abschnitt "User Information"in Google Cloud die Active Directory-Informationen der Benutzer angezeigt.

Erstellen eines Dienstkontos

Um diese Aufgabe auszuführen, benötigen Sie ein Google Cloud Platform-Entwicklerkonto.

1. Melden Sie sich bei https://console.cloud.google.com an.
2. Wählen Sie in der Seitenleiste die Option **IAM & Admin** und dann **Service Accounts**.
3. Wählen Sie **Create service account**.
4. Geben Sie unter **Service account details** den Dienstkontonamen und die Dienstkonto-ID ein.
5. Wählen Sie **Done**.

Erstellen eines Dienstkontoschlüssels

1. Wählen Sie auf der Seite **Service accounts** das soeben erstellte Dienstkonto.
2. Wählen Sie die Registerkarte **Keys** und dann **Add key > Create new key**.
3. Lassen Sie die Standardtypoption JSON ausgewählt.
4. Wählen Sie **Create**. Speichern Sie den Schlüssel an einem sicheren Ort, auf den Sie später zugreifen können. Sie geben den privaten Schlüssel in der Citrix Cloud-Konsole ein, wenn Sie Google Cloud Identity als Identitätsanbieter verbinden.

Konfigurieren der domänenweiten Delegierung

1. Aktivieren Sie die Admin SDK-API:

a) Wählen Sie im Google Cloud Platform-Menü die Option **APIs & Services > Enabled APIs & services**.
b) Wählen Sie oben in der Konsole **Enable APIs and services**. Die Homepage der API-Bibliothek wird angezeigt.
c) Suchen Sie **Admin SDK API** und wählen Sie den Eintrag in der Ergebnisliste aus.
d) Wählen Sie **Aktivieren**.

2. Erstellen Sie einen API-Client für das Dienstkonto:

a) Wählen Sie im Google Cloud Platform-Menü die Option **IAM & Admin > Service Accounts** und dann das zuvor erstellte Dienstkonto.
b) Erweitern Sie auf der Registerkarte **Details** des Dienstkontos **Advanced settings**.
c) Kopieren Sie unter **Domain-wide Delegation** die Client-ID und wählen Sie dann **View Google Workspace Admin Console**.
d) Wählen Sie gegebenenfalls das Google Workspace-Administratorkonto aus, das Sie verwenden möchten. Die Google Admin-Konsole wird angezeigt.
e) Wählen Sie in der Google Admin-Seitenleiste **Security > Access and data control > API controls**.
f) Klicken Sie unter **Domain wide delegation** auf **Manage Domain Wide Delegation**.
g) Wählen Sie **Add new**.
h) Fügen Sie unter **Client ID** die Client-ID des Dienstkontos ein, das Sie in Schritt C kopiert haben.
i) Geben Sie in **OAuth scopes** die folgenden Bereiche durch Kommas getrennt auf einer Zeile ein:

```
https://www.googleapis.com/auth/admin.directory.user.readonly,
    https://www.googleapis.com/auth/admin.directory.group.
    readonly,https://www.googleapis.com/auth/admin.directory.
    domain.readonly
<!--NeedCopy-->
```

j) Wählen Sie **Autorisieren**.

Hinzufügen eines API-Benutzerkontos mit Schreibzugriff

Bei dieser Aufgabe erstellen Sie ein Google Workspace-Benutzerkonto mit Schreibzugriff auf die API für Citrix Cloud. Das Konto wird nicht für andere Zwecke verwendet und hat keine weiteren Berechtigungen.

1. Wählen Sie im Google Admin-Menü **Directory > Users**.
2. Wählen Sie **Add new user** und geben Sie die Benutzerinformationen ein.

3. Wählen Sie **Add new user**, um die Kontoinformationen zu speichern.
4. Erstellen Sie eine benutzerdefinierte Rolle für das Benutzerkonto mit Schreibzugriff:

    a) Wählen Sie im Google Admin-Menü **Account > Admin roles**.
    b) Wählen Sie **Create new role**.
    c) Geben Sie einen Namen für die neue Rolle ein. Beispiel: API-ReadOnly
    d) Wählen Sie **Weiter**.
    e) Wählen Sie unter **Admin API privileges** die folgenden Berechtigungen aus:

        - Users > Read
        - Groups > Read
        - Domain Management

    f) Wählen Sie **Continue** und dann **Create role**.

5. Weisen Sie die benutzerdefinierte Rolle dem Benutzerkonto mit Schreibzugriff zu, das Sie zuvor erstellt haben:

    a) Wählen Sie auf der Seite mit den Details der benutzerdefinierten Rolle im Bereich **Admins** die Option **Assign users**.
    b) Beginnen Sie mit der Eingabe des Namens des Benutzerkontos mit Schreibzugriff und wählen Sie es aus der Benutzerliste aus.
    c) Wählen Sie **Assign role**.
    d) Um die Rollenzuweisung zu überprüfen, kehren Sie zur Benutzerseite zurück (**Directory > Users**) und wählen Sie das Benutzerkonto mit Schreibzugriff aus. Die benutzerdefinierte Rollenzuweisung wird unter **Admin roles and privileges** angezeigt.

Google Cloud Identity mit Citrix Cloud verbinden

1. Melden Sie sich bei Citrix Cloud unter https://citrix.cloud.com an.
2. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.
3. Suchen Sie **Google Cloud Identity**, klicken Sie auf die Auslassungspunkte (…) und wählen Sie im Menü **Verbinden** aus.
4. Geben Sie bei der entsprechenden Aufforderung einen kurzen, URL-freundlichen Bezeichner für Ihr Unternehmen ein und wählen Sie **Speichern und Fortfahren**. Der Bezeichner muss innerhalb von Citrix Cloud global eindeutig sein.
5. Wählen Sie **Datei importieren** und wählen Sie dann die JSON-Datei aus, die Sie beim Erstellen des Schlüssels für das Dienstkonto gespeichert haben. Durch diese Aktion werden der private Schlüssel und die E-Mail-Adresse für das von Ihnen erstellte Google Cloud-Dienstkonto importiert.
6. Geben Sie im Feld **Imitierter Benutzer** den Namen des API-Benutzerkontos mit Schreibzugriff ein.
7. Wählen Sie **Weiter**. Citrix Cloud überprüft Ihre Google-Kontodetails und testet die Verbindung.

8. Überprüfen Sie die Liste der verknüpften Domänen. Ist sie korrekt, wählen Sie **Bestätigen**, um Ihre Konfiguration zu speichern.

Administratoren Citrix Cloud hinzufügen

Sie können einzelne Citrix Cloud-Administratoren und Administratorgruppen über Google Cloud hinzufügen. Weitere Informationen finden Sie in den folgenden Artikeln:

- Für einzelne Administratoren: Administratorzugriff auf Citrix Cloud verwalten
- Für Administratorgruppen: Administratorgruppen verwalten

Nachdem Sie Administratoren zu Citrix Cloud hinzugefügt haben, können sie sich mit einer der folgenden Methoden anmelden:

- Navigieren Sie zu der Anmelde-URL für Administratoren, die Sie bei der ursprünglichen Konfiguration von Google Cloud als Identitätsanbieter konfiguriert haben. Beispiel:`https://citrix.cloud.com/go/mycompany`
- Wählen Sie auf der Citrix Cloud-Anmeldeseite die Option **Mit Firmenanmeldeinformationen anmelden**, geben Sie die eindeutige ID für Ihr Unternehmen ein (z. B. "mycompany") und klicken Sie auf **Weiter**.

Google Cloud Identity für die Workspace-Authentifizierung aktivieren

1. Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration > Authentifizierung**.
2. Wählen Sie **Google Cloud Identity**. Wählen Sie **Ich verstehe die Auswirkungen auf Abonnenten**, wenn Sie dazu aufgefordert werden und klicken Sie auf **Speichern**.

Verbinden von Okta als Identitätsanbieter mit Citrix Cloud

July 2, 2024

Citrix Cloud unterstützt die Verwendung von Okta als Identitätsanbieter für die Authentifizierung von Abonnenten, die sich an ihrem Workspace anmelden. Wenn Sie Ihre Okta-Organisation mit Citrix Cloud verbinden, können Abonnenten über eine vertraute Anmeldeoberfläche auf Ressourcen in Citrix Workspace zugreifen.

Nach dem Aktivieren der Okta-Authentifizierung in der Workspacekonfiguration ändert sich das Anmeldefenster für Abonnenten. Bei Auswahl der Okta-Authentifizierung wird eine Verbundanmeldung und kein Single Sign-On ermöglicht. Wenn Abonnenten sich über eine Okta-Anmeldeseite am Workspace anmelden, müssen sie sich möglicherweise erneut authentifizieren, wenn sie eine App oder

einen Desktop in Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) öffnen. Um dies zu vermeiden und einen Single Sign-On zu aktivieren, müssen Sie den Citrix Verbundauthentifizierungsdienst (FAS) mit Citrix Cloud verwenden. Weitere Informationen finden Sie unter Verbinden des Citrix Verbundauthentifizierungsdiensts (FAS) mit Citrix Cloud.

Voraussetzungen

Cloud Connectors oder Connector Appliances

Für die Kommunikation zwischen Citrix Cloud und Ihrem Ressourcenstandort sind Cloud Connectors oder Connector Appliances erforderlich. Mindestens zwei Cloud Connectors oder Connector Appliances sind erforderlich, um eine hochverfügbare Verbindung mit Citrix Cloud sicherzustellen. Sie benötigen mindestens zwei Connectors, die mit Ihrer Active Directory-Domäne verbunden sind. Dabei kann es sich um Cloud Connectors oder Connector Appliances handeln.

Die Connectors müssen die folgenden Anforderungen erfüllen:

- Die in der zum Connector gehörigen Dokumentation aufgeführten Anforderungen
- Gehört zu Ihrer Active Directory-Domäne. Wenn die Workspace-Benutzer in mehreren Domänen residieren, kann das Multidomänen-Feature der Connector Appliance für die Verbindung mehrerer Domänen verwendet werden.
- Es muss eine Verbindung zum Netzwerk bestehen, das die Ressourcen abrufen kann, auf die Benutzer über Citrix Workspace zugreifen.
- Eine Verbindung mit dem Internet muss bestehen. Weitere Informationen finden Sie unter Anforderungen an System und Konnektivität.

Weitere Informationen zur Installation von Cloud Connectors finden Sie unter Cloud Connector-Installation.
Informationen zur Installation von Connector Appliances finden Sie unter Connector Appliance installieren.

Okta-Domäne

Beim Verbinden von Okta mit Citrix Cloud müssen Sie die Okta-Domäne für Ihre Organisation angeben. Citrix unterstützt die folgenden Okta-Domänen:

- okta.com
- okta-eu.com
- oktapreview.com

Sie können auch benutzerdefinierte Okta-Domänen mit Citrix Cloud verwenden. Lesen Sie hierfür die Hinweise zur Verwendung benutzerdefinierter Domänen unter Customize the Okta URL domain auf der Okta-Website.

Weitere Informationen zum Suchen der benutzerdefinierten Domäne für Ihre Organisation finden Sie unter Finding Your Okta Domain auf der Okta-Website.

Okta-OIDC-Webanwendung

Um Okta als Identitätsanbieter zu verwenden, müssen Sie zunächst eine Okta-OIDC-Webanwendung erstellen, deren Clientanmeldeinformationen Sie dann mit Citrix Cloud verwenden. Nachdem Sie die Anwendung erstellt und konfiguriert haben, notieren Sie sich die Client-ID und das Clientgeheimnis. Diese Werte geben Sie dann in Citrix Cloud beim Verbinden mit Ihrer Okta-Organisation ein.

Informationen zum Erstellen und Konfigurieren dieser Anwendung finden Sie in den folgenden Abschnitten dieses Artikels:

- Okta OIDC-Web-App-Integration erstellen
- Konfigurieren der Okta-OIDC-Webanwendung

Workspace-URL

Beim Erstellen der Okta-Anwendung müssen Sie Ihre Workspace-URL aus Citrix Cloud angeben. Um die Workspace-URL zu erfassen, wählen Sie im Citrix Cloud-Menü die Option **Workspacekonfiguration**. Die Workspace-URL wird auf der Registerkarte **Zugriff** angezeigt.

> **Wichtig:**
>
> Wenn Sie später die Workspace-URL ändern, müssen Sie die neue URL in der Konfiguration der Okta-Anwendung eingeben. Andernfalls können Probleme auftreten, wenn Abonnenten sich von ihrem Workspace abmelden.

Okta-API-Token

Bei Verwendung von Okta als Identitätsanbieter mit Citrix Cloud benötigen Sie einen API-Token für Ihre Okta-Organisation. Erstellen Sie diesen Token mit einem Administratorkonto mit Lesezugriff in Ihrer Okta-Organisation. Der Token muss Benutzer und Gruppen in Ihrer Okta-Organisation lesen können.

Informationen zum Erstellen des API-Token finden Sie unter Erstellen eines Okta-API-Token in diesem Artikel. Weitere Informationen zu API-Token finden Sie unter Create an API Token auf der Okta-Website.

> **Wichtig:**
>
> Notieren Sie sich beim Erstellen des API-Token den Tokenwert (zum Beispiel, indem Sie ihn in eine temporäre Textdatei kopieren). Okta zeigt diesen Wert nur einmal an. Erstellen Sie den Token daher vielleicht direkt vor der Ausführung der Schritte in Verbinden von Citrix Cloud mit Ihrer Okta-Organisation.

Synchronisieren von Konten mit dem Okta-AD-Agent

Um Okta als Identitätsanbieter zu verwenden, müssen Sie zunächst Ihr On-Premises-Active Directory mit Okta integrieren. Installieren Sie dafür den Okta-AD-Agent in Ihrer Domäne und fügen Ihr AD zu Ihrer Okta-Organisation hinzu. Hinweise zum Bereitstellen des Okta-AD-Agent finden Sie unter Get started with Active Directory integration auf der Okta-Website.

Anschließend importieren Sie Ihre AD-Benutzer und -Gruppen in Okta. Schließen Sie beim Importieren die folgenden Werte ein, die Ihren AD-Konten zugeordnet sind:

- E-Mail
- SID
- UPN
- OID

> Hinweis:
>
> Wenn Sie den Citrix Gateway Service mit Workspace verwenden, müssen Sie Ihre AD-Konten nicht mit Ihrer Okta-Organisation synchronisieren.

Synchronisieren der AD-Benutzer und -Gruppen mit Ihrer Okta-Organisation:

1. Installieren und konfigurieren Sie den Okta-AD-Agent. Ausführliche Anweisungen finden Sie in den folgenden Artikeln auf der Okta Website:
   - Install the Okta Active Directory agent
   - Configure Active Directory import and account settings
   - Configure Active Directory provisioning settings
2. Fügen Sie Ihre AD-Benutzer und -Gruppen durch manuellen oder automatisierten Import zu Okta hinzu. Weitere Hinweise zu Importverfahren finden Sie unter Manage Active Directory users and groups auf der Okta-Website.

Okta OIDC-Web-App-Integration erstellen

1. Wählen Sie in der Okta-Verwaltungskonsole unter **Applications** die Option **Applications**.

2. Wählen Sie **Create App Integration**.
3. Wählen Sie unter **Sign in method** die Option **OIDC - OpenID Connect** aus.
4. Wählen Sie unter **Application type** die Option **Web Application** aus. Wählen Sie **Weiter**.
5. Geben Sie unter **App Integration Name** einen Anzeigenamen für die App-Integration ein.
6. Wählen Sie unter **Grant type** die Option **Authorization Code** (standardmäßig ausgewählt).
7. Geben Sie unter **Sign-in redirect URIs** `https://accounts.cloud.com/core/login-okta` ein.
8. Geben Sie unter **Sign-out redirect URIs** Ihre Workspace-URL aus Citrix Cloud ein.
9. Wählen Sie unter **Assignments** für **Controlled access** aus, ob Sie die App-Integration allen in Ihrer Organisation, nur von Ihnen angegebenen Gruppen oder später zuweisen möchten.
10. Wählen Sie **Speichern**. Nachdem Sie die App-Integration gespeichert haben, zeigt die Konsole die Anwendungskonfigurationsseite an.
11. Kopieren Sie im Abschnitt **Clientanmeldeinformationen** die Werte **Client-ID** und **Geheimer Clientschlüssel**. Diese Werte verwenden Sie, wenn Sie Citrix Cloud mit Ihrer Okta-Organisation verbinden.

Konfigurieren der Okta-OIDC-Webanwendung

In diesem Schritt konfigurieren Sie Ihre Okta-OIDC-Webanwendung mit den erforderlichen Einstellungen für Citrix Cloud. Citrix Cloud benötigt diese Einstellungen, um Ihre Abonnenten über Okta zu authentifizieren, wenn sie sich bei ihrem Workspace anmelden.

1. (Optional) Aktualisieren Sie die Clientberechtigungen für "Grant type = implicit". Sie können diesen Schritt ausführen, wenn Sie die geringste Anzahl an Privilegien für diesen Berechtigungstyp zulassen möchten.

    a) Auf der Seite mit der Okta-Anwendungskonfiguration scrollen Sie auf der Registerkarte **Allgemein** zum Abschnitt **Allgemeine Einstellungen** und wählen Sie **Bearbeiten** aus.
    b) Navigieren Sie im Abschnitt **Anwendung** unter **Gewährungstyp** zu **Client acting on behalf of a user** und deaktivieren Sie die Einstellung **Allow Access Token with implicit grant type**.
    c) Wählen Sie **Speichern**.

2. Fügen Sie Anwendungsattribute hinzu. Bei diesen Attributen muss Groß- und Kleinschreibung beachtet werden.

    a) Wählen Sie im Okta-Konsolenmenü **Directory > Profile Editor**.
    b) Wählen Sie das Okta-Profil **User (default)** aus. Okta zeigt die Profilseite **User** an.
    c) Wählen Sie unter **Attributes** die Option **Add attribute**.
    d) Geben Sie die folgenden Informationen ein:

        - Anzeigename: cip_email

- Variablenname: cip_email
- Beschreibung: AD-Benutzer-E-Mail
- Attributlänge: Wählen Sie **größer als** und geben Sie **1** ein.
- Erforderliches Attribut: Ja

e) Wählen Sie **Save and Add Another**.

f) Geben Sie die folgenden Informationen ein:

- Anzeigename: cip_sid
- Variablenname: cip_sid
- Beschreibung: AD-Benutzer-Sicherheits-ID
- Attributlänge: Wählen Sie **größer als** und geben Sie **1** ein.
- Erforderliches Attribut: Ja

g) Wählen Sie **Save and Add Another**.

h) Geben Sie die folgenden Informationen ein:

- Anzeigename: cip_upn
- Variablenname: cip_upn
- Beschreibung: AD-Benutzerprinzipalname
- Attributlänge: Wählen Sie **größer als** und geben Sie **1** ein.
- Erforderliches Attribut: Ja

i) Wählen Sie **Save and Add Another**.

j) Geben Sie die folgenden Informationen ein:

- Anzeigename: cip_oid
- Variablenname: cip_oid
- Beschreibung: AD-Benutzer-GUID
- Attributlänge: Wählen Sie **größer als** und geben Sie **1** ein.
- Erforderliches Attribut: Ja

k) Wählen Sie **Speichern**.

3. Bearbeiten von Attributzuordnungen für die Anwendung:

a) Wählen Sie in der Okta-Konsole **Directory > Profile Editor**.

b) Suchen Sie das Profil **active_directory** für Ihr AD. Dieses Profil kann im Format `myDomain User` beschriftet sein. `myDomain` ist der Name Ihrer integrierten AD-Domäne.

c) Wählen Sie **Mappings** aus. Die Seite "User Profile Mappings"für Ihre AD-Domäne wird angezeigt und die Registerkarte zum Zuordnen Ihres AD zu einem Okta-Benutzer ist ausgewählt.

d) Suchen Sie in der Spalte **Okta User Profile** die Attribute, die Sie in Schritt 2 erstellt haben, und ordnen Sie sie wie folgt zu:

- Wählen Sie für `cip_email` die Option `email` aus der Spalte "Benutzerprofil"für Ihre Domäne aus. Bei dieser Auswahl wird die Zuordnung als `appuser.email` angezeigt.

- Wählen Sie für `cip_sid` die Option `objectSid` aus der Spalte "Benutzerprofil"für Ihre Domäne aus. Bei dieser Auswahl wird die Zuordnung als `appuser.objectSid` angezeigt.
- Wählen Sie für `cip_upn` die Option `userName` aus der Spalte "Benutzerprofil"für Ihre Domäne aus. Bei dieser Auswahl wird die Zuordnung als `appuser.userName` angezeigt.
- Wählen Sie für `cip_oid` die Option `externalId` aus der Spalte "Benutzerprofil" für Ihre Domäne aus. Bei dieser Auswahl wird die Zuordnung als `appuser.externalId` angezeigt.

e) Wählen Sie **Save Mappings** aus.
f) Wählen Sie **Apply updates now** aus. Okta beginnt mit dem Anwenden der Zuordnungen.
g) Synchronisieren Sie Okta mit Ihrem AD.
   i. Wählen Sie in der Okta-Konsole **Directory > Directory Integrations**.
   ii. Wählen Sie Ihr integriertes AD aus.
   iii. Wählen Sie die Registerkarte **Provisioning** aus.
   iv. Wählen Sie unter **Settings** die Option **To Okta** aus.
   v. Scrollen Sie zum Abschnitt **Okta Attribute Mappings** und wählen Sie dann **Force Sync** aus.

Erstellen eines Okta-API-Token

1. Melden Sie sich mit einem Administratorkonto mit Lesezugriff bei der Okta-Konsole an.
2. Wählen Sie im Menü der Okta-Konsole **Security > API**.
3. Wählen Sie die Registerkarte **Token** und dann **Create Token**.
4. Geben Sie einen Namen für den Token ein.
5. Wählen Sie **Create Token**.
6. Kopieren Sie den Tokenwert. Diesen Wert geben Sie dann beim Verbinden Ihrer Okta-Organisation mit Citrix Cloud ein.

Citrix Cloud mit Ihrer Okta-Organisation verbinden

1. Melden Sie sich bei Citrix Cloud unter https://citrix.cloud.com an.
2. Klicken Sie im Menü "Citrix Cloud"auf **Identitäts- und Zugriffsverwaltung**.
3. Suchen Sie **Okta**, klicken Sie auf die Auslassungspunkte (...) und wählen Sie im Menü **Verbinden** aus.
4. Geben Sie unter **Okta-URL** Ihre Okta-Domäne ein.
5. Geben Sie unter **Okta-API-Token** den API-Token für Ihre Okta-Organisation ein.
6. Geben Sie für **Client-ID** und **Geheimer Clientschlüssel**die Client-ID und den geheimen Clientschlüssel der zuvor erstellten OIDC-Webanwendungsintegration ein. Um diese Werte aus

der Okta-Konsole zu kopieren, wählen Sie **Anwendungen** und suchen die Okta-Anwendung. Klicken Sie unter **Client-Anmeldeinformationen** auf die Schaltfläche **In Zwischenablage kopieren** für jeden Wert.

7. Klicken Sie auf **Testen und schließen**. Citrix Cloud überprüft Ihre Okta-Details und testet die Verbindung.

Nachdem die Verbindung erfolgreich verifiziert wurde, können Sie die Okta-Authentifizierung für Workspace-Abonnenten aktivieren.

Aktivieren der Okta-Authentifizierung für Workspaces

1. Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration > Authentifizierung**.
2. Wählen Sie **Okta**.
3. Wählen Sie **Ich verstehe die Auswirkungen auf Abonnenten**, wenn Sie dazu aufgefordert werden.
4. Wählen Sie **Speichern**.

Nach der Umstellung auf die Okta-Authentifizierung deaktiviert Citrix Cloud die Workspaces vorübergehend für einige Minuten. Wenn die Workspaces wieder aktiviert sind, können sich Ihre Abonnenten mit Okta anmelden.

Weitere Informationen

- Citrix Tech Zone:
  - Tech Insight: Authentication - Okta
  - Tech Brief: Workspace Identity
  - Tech Brief: Workspace SSO

SAML als Identitätsanbieter mit Citrix Cloud verbinden

July 2, 2024

Citrix Cloud unterstützt die Verwendung von SAML (Security Assertion Markup Language) als Identitätsanbieter für die Authentifizierung von Citrix Cloud-Administratoren und Abonnenten, die sich bei ihrem Workspace anmelden. Sie können den SAML 2.0-Anbieter Ihrer Wahl mit Ihrem On-Premises-Active Directory (AD) verwenden.

Über diesen Artikel

In diesem Artikel werden die Schritte zur Konfiguration einer Verbindung zwischen Citrix Cloud und Ihrem SAML-Anbieter beschrieben. In einigen Schritten werden Aktionen beschrieben, die Sie in der Verwaltungskonsole Ihres SAML-Anbieters ausführen. Die speziellen Befehle, die Sie zur Durchführung dieser Aktionen verwenden, können je nach ausgewähltem SAML-Anbieter von den in diesem Artikel beschriebenen Befehlen abweichen. Die hier aufgeführten SAML-Anbieter-Befehle dienen nur als Beispiele. Weitere Informationen zu den entsprechenden Befehlen für Ihren SAML-Anbieter finden Sie in der Dokumentation Ihres SAML-Anbieters.

SAML-Anbieterkonfigurationen

Citrix stellt die folgenden Konfigurationsanleitungen zur Verfügung, um sicherzustellen, dass Ihr SAML-Anbieter reibungslos mit Citrix Cloud interagiert:

- SAML mit Active Directory-Verbunddienste (AD FS): Siehe SAML-Authentifizierung in Citrix Cloud mit AD FS konfigurieren.
- SAML mit Azure Active Directory-Identitäten: siehe Anmeldung bei Workspaces mit SAML und Azure Active Directory-Identität.
- Citrix Cloud-SAML-SSO-App für Azure AD: Siehe Tutorial: Integration des einmaligen Anmeldens (SSO) von Azure Active Directory mit Citrix Cloud SAML SSO auf der Website mit der Microsoft Azure AD-Dokumentation.
- SAML mit benutzerdefinierten Citrix Workspace-Domänen: siehe Anmelden bei Workspaces mit SAML unter Verwendung benutzerdefinierter Domänen.
- SAML mit Okta: Siehe Okta als SAML-Anbieter für die Workspace-Authentifizierung konfigurieren

Unterstützte SAML-Anbieter

SAML-Anbieter, die die offizielle SAML 2.0-Spezifikation unterstützen, werden für die Verwendung mit Citrix Cloud unterstützt.

Citrix hat folgende SAML-Anbieter für die Authentifizierung von Citrix Cloud-Administratoren und Citrix Workspace-Abonnenten mit Single Sign-On (SSO) und Single Logout (SLO) getestet. Auch SAML-Anbieter, die nicht in dieser Liste aufgeführt sind, werden unterstützt.

- Microsoft ADFS
- Microsoft Azure AD
- Duo
- Okta
- OneLogin

- PingOne SSO
- PingFederate

Für die Tests dieser Anbieter verwendete Citrix die folgenden Konfiguration der SAML-Verbindung in der Citrix Cloud-Konsole:

- Bindungsmechanismus: HTTP Post
- SAML-Antwort: Antwort oder Assertion signieren
- Authentifizierungskontext: Keine Angabe, exakt

Dies sind die Standardwerte, wenn Sie die SAML-Verbindung in Citrix Cloud konfigurieren. Citrix empfiehlt, diese Einstellungen bei der Konfiguration der Verbindung mit dem ausgewählten SAML-Anbieter zu verwenden.

Weitere Informationen zu diesen Einstellungen finden Sie unter SAML-Anbietermetadaten zu Citrix Cloud hinzufügen.

Unterstützung für bereichsbezogene Entitäts-IDs

In diesem Artikel wird beschrieben, wie Sie die SAML-Authentifizierung mit einer SAML-Anwendung und der standardmäßigen generischen Entitäts-ID von Citrix Cloud konfigurieren.

Wenn Sie für Ihre SAML-Authentifizierung mehrere SAML-Anwendungen innerhalb eines einzigen SAML-Anbieters benötigen, konsultieren Sie SAML-Anwendung mit bereichsbezogener Entitäts-ID in Citrix Cloud konfigurieren.

Voraussetzungen

Für die Verwendung von SAML-Authentifizierung mit Citrix Cloud gelten die folgenden Anforderungen:

- SAML-Anbieter, der SAML 2.0 unterstützt.
- On-Premises-AD-Domäne.
- Zwei Cloud Connectors, an einem Ressourcenstandort bereitgestellt und mit Ihrer On-Premises-AD-Domäne verbunden. Die Cloud Connectors werden verwendet, um sicherzustellen, dass Citrix Cloud mit Ihrem Ressourcenstandort kommunizieren kann.
- AD-Integration mit Ihrem SAML-Anbieter.

Cloud Connectors

Sie benötigen mindestens zwei (2) Server zum Installieren der Citrix Cloud Connector-Software. Für hohe Cloud Connector-Verfügbarkeit empfiehlt Citrix mindestens zwei Server. Die Server müssen die folgenden Anforderungen erfüllen:

- Die unter Technische Daten zu Citrix Cloud Connector beschriebenen Systemanforderungen müssen erfüllt sein.
- Es dürfen keine anderen Komponenten von Citrix installiert sein. Die Server dürfen keine AD-Domänencontroller oder Maschinen sein, die für Ihre Ressourcenstandortinfrastruktur kritisch sind.
- Sie müssen mit der Domäne verbunden sein, in der sich Ihre Ressourcen befinden. Wenn sich die Ressourcen in mehreren Domänen befinden und Benutzer darauf zugreifen, müssen Sie in jeder Domäne mindestens zwei Cloud Connectors installieren.
- Es muss eine Verbindung zum Netzwerk bestehen, das die Ressourcen abrufen kann, auf die Abonnenten über Citrix Workspace zugreifen.
- Eine Verbindung mit dem Internet muss bestehen. Weitere Informationen finden Sie unter Anforderungen an System und Konnektivität.

Weitere Informationen zur Installation des Cloud Connectors finden Sie unter Cloud Connector-Installation.

Active Directory

Führen Sie vor dem Konfigurieren der SAML-Authentifizierung die folgenden Aufgaben aus:

- Stellen Sie sicher, dass Ihre Workspace-Abonnenten über Benutzerkonten in Ihrem AD verfügen. Abonnenten ohne AD-Konto können sich nicht erfolgreich bei ihrem Workspace anmelden, wenn die SAML-Authentifizierung konfiguriert ist.
- Verbinden Sie Ihr AD mit Ihrem Citrix Cloud-Konto, indem Sie Cloud Connectors in Ihrem On-Premises-AD bereitstellen.
- Synchronisieren Sie Ihre AD-Benutzer mit dem SAML-Anbieter. Citrix Cloud benötigt die AD-Benutzerattribute Ihrer Workspace-Abonnenten, damit diese sich erfolgreich anmelden können.

Active Directory-Benutzerattribute Die Angabe der folgenden Attribute ist für alle AD-Benutzerobjekte erforderlich:

- Allgemeiner Name
- SAM-Kontoname
- User Principal Name (UPN)
- Objekt-GUID
- SID

Citrix Cloud verwendet die Objekt-GUID und die SID aus Ihrem AD, um den Benutzerkontext bei der Anmeldung von Abonnenten bei Citrix Workspace zu erfassen. Wenn eine dieser Eigenschaften nicht ausgefüllt wird, können Abonnenten sich nicht anmelden.

Die folgenden Attribute sind für die Verwendung der SAML-Authentifizierung mit Citrix Cloud nicht erforderlich, aber Citrix empfiehlt, sie anzugeben, um die beste Benutzererfahrung zu gewährleisten:

- E-Mail-Adresse
- Anzeigename

Citrix Cloud verwendet das Anzeigenamen-Attribut, um die Namen der Abonnenten in Citrix Workspace korrekt anzuzeigen. Wird das Attribut nicht angegeben, können sich die Abonnenten zwar anmelden, ihre Namen werden jedoch ggf. nicht wie erwartet angezeigt.

SAML-Integration in Active Directory

Bevor Sie die SAML-Authentifizierung aktivieren, müssen Sie Ihr On-Premises-AD in Ihren SAML-Anbieter integrieren. Diese Integration ermöglicht es dem SAML-Anbieter, die folgenden erforderlichen AD-Benutzerattribute in der SAML-Assertion an Citrix Cloud zu übergeben:

- objectSID (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- E-Mail (email)
- Anzeigename (displayName)

Sie können eine Teilmenge dieser Attribute konfigurieren, sofern entweder das SID- oder das UPN-Attribut in der SAML-Assertion enthalten ist. Citrix Cloud ruft die anderen Attribute nach Bedarf aus Ihrem AD ab.

> **Hinweis:**
>
> Zur Gewährleistung der besten Leistung empfiehlt Citrix, alle in diesem Abschnitt genannten Attribute zu konfigurieren.

Obwohl die genauen Integrationsschritte von SAML-Anbieter zu SAML-Anbieter unterschiedlich sind, umfasst der Integrationsprozess in der Regel die folgenden Aufgaben:

1. Installieren Sie einen Synchronisierungs-Agenten in Ihrer AD-Domäne, um eine Verbindung zwischen Ihrer Domäne und Ihrem SAML-Anbieter herzustellen. Wenn Sie AD FS als SAML-Anbieter verwenden, ist dieser Schritt nicht erforderlich.
2. Erstellen Sie benutzerdefinierte Attribute und weisen Sie sie den o. g. erforderlichen AD-Benutzerattributen zu. Die allgemeinen Schritte bei dieser Aufgabe werden uner Erstellen und Zuordnen benutzerdefinierter SAML-Attribute in diesem Artikel beschrieben.
3. Synchronisieren Sie Ihre AD-Benutzer mit Ihrem SAML-Anbieter.

Weitere Informationen zur Integration Ihres AD in Ihren SAML-Anbieter finden Sie in der Produktdokumentation Ihres SAML-Anbieters.

Administratorauthentifizierung mit SAML 2.0

Citrix Cloud unterstützt die Verwendung von SAML 2.0 zur Authentifizierung von Mitgliedern von Administratorgruppen in AD. Weitere Informationen zum Hinzufügen von Administratorgruppen zu Citrix Cloud finden Sie unter Administratorgruppen verwalten.

Vorhandene SAML-Verbindung für die Administratorauthentifizierung verwenden

Wenn Sie bereits eine SAML 2.0-Verbindung in Citrix Cloud haben und diese zur Authentifizierung von Administratoren verwenden möchten, müssen Sie zuerst SAML 2.0 in **Identitäts- und Zugriffsverwaltung** trennen und dann die Verbindung neu konfigurieren. Wenn Sie Ihre SAML-Verbindung zur Authentifizierung von Citrix Workspace-Abonnenten verwenden, müssen Sie auch die SAML-Authentifizierungsmethode in der **Workspace-Konfiguration** deaktivieren. Nachdem Sie die SAML-Verbindung neu konfiguriert haben, können Sie Administratorgruppen zu Citrix Cloud hinzufügen.

Wenn Sie versuchen, Administratorgruppen hinzuzufügen, ohne zuerst SAML 2.0 zu trennen und neu zu verbinden, wird die unter Administratorgruppe zu Citrix Cloud hinzufügen beschriebene **Active Directory**-Identitätsoption nicht angezeigt.

Übersicht über die Einrichtung einer SAML-Verbindung

Um eine neue SAML 2.0-Verbindung in Citrix Cloud einzurichten, führen Sie die folgenden Aufgaben aus:

1. Verbinden Sie unter **Identitäts- und Zugriffsverwaltung** Ihr On-Premises-AD mit Citrix Cloud wie unter Verbinden von Active Directory mit Citrix Cloud beschrieben.
2. Integrieren Sie Ihren SAML-Anbieter in Ihr On-Premises-AD wie unter SAML-Integration in Active Directory in diesem Artikel beschrieben.
3. Konfigurieren Sie die Anmelde-URL, mit der sich die Administratoren bei Citrix Cloud anmelden können.
4. Unter **Identitäts- und Zugriffsverwaltung** konfigurieren Sie die SAML-Authentifizierung in Citrix Cloud. Diese Aufgabe umfasst die Konfiguration des SAML-Anbieters mit den SAML-Metadaten aus Citrix Cloud und die anschließende Konfiguration von Citrix Cloud mit den Metadaten von Ihrem SAML-Anbieter, um die SAML-Verbindung zu erstellen.

Übersicht über die Verwendung einer bestehenden SAML-Verbindung für Citrix Cloud-Administratoren

Wenn Sie bereits eine SAML 2.0-Verbindung in Citrix Cloud haben und diese für die Administratorauthentifizierung verwenden möchten, führen Sie die folgenden Aufgaben aus:

1. Deaktivieren Sie gegebenenfalls die SAML 2.0-Workspaceauthentifizierung: Wählen Sie unter **Workspacekonfiguration > Authentifizierung** eine andere Authentifizierungsmethode aus und wählen Sie dann **Bestätigen**, wenn Sie dazu aufgefordert werden.
2. Trennen Sie Ihre bestehende SAML 2.0-Verbindung: Suchen Sie unter **Identitäts- und Zugriffsverwaltung > Authentifizierung** die SAML-Verbindung. Klicken Sie ganz rechts auf die Auslassungspunkte und wählen Sie die Option **Trennen** aus. Wählen Sie **Ja, trennen**, um die Aktion zu bestätigen.
3. Verbinden Sie SAML 2.0 neu und konfigurieren Sie die Verbindung: Klicken Sie auf die Auslassungspunkte neben **SAML 2.0** und wählen Sie die Option **Verbinden** aus.
4. Wenn Sie dazu aufgefordert werden, geben Sie einen eindeutiger Bezeichner für die Anmelde-URL ein, mit der sich Administratoren anmelden.
5. Konfigurieren Sie die SAML-Verbindung wie unter SAML-Anbietermetadaten konfigurieren in diesem Artikel beschrieben.

Nachdem Sie Ihre SAML-Verbindung konfiguriert haben, können Sie Ihre AD-Administratorgruppen zu Citrix Cloud hinzufügen, wie unter Administratorgruppen verwalten beschrieben. Sie können SAML auch für Workspace-Abonnenten neu aktivieren, wie in diesem Artikel beschrieben.

Erstellen und Zuordnen benutzerdefinierter SAML-Attribute

Wenn bereits benutzerdefinierte Attribute für die SID-, UPN-, OID-, email- und displayName-Attribute in Ihrem SAML-Anbieter konfiguriert sind, müssen Sie diese Aufgabe nicht ausführen. Fahren Sie mit dem Erstellen einer SAML-Connectoranwendung fort und verwenden Sie Ihre vorhandenen benutzerdefinierten SAML-Attribute in Schritt 5.

> **Hinweis:**
>
> In den Schritten in diesem Abschnitt werden Aktionen beschrieben, die Sie in der Verwaltungskonsole Ihres SAML-Anbieters ausführen. Die speziellen Befehle, die Sie zur Durchführung dieser Aktionen verwenden, können je nach ausgewähltem SAML-Anbieter von den in diesem Abschnitt beschriebenen Befehlen abweichen. Die Befehle des SAML-Anbieters in diesem Abschnitt werden nur als Beispiele angegeben. Weitere Informationen zu den entsprechenden Befehlen für Ihren SAML-Anbieter finden Sie in der Dokumentation Ihres SAML-Anbieters.

1. Melden Sie sich bei der Verwaltungskonsole Ihres SAML-Anbieters an und wählen Sie die Option zum Erstellen benutzerdefinierter Benutzerattribute aus. Je nach der Konsole Ihres SAML-Anbieters können Sie beispielsweise **Users > Custom User Fields > New User Field** auswählen.
2. Fügen Sie Attribute für die folgenden AD-Eigenschaften hinzu. Benennen Sie die Attribute unter Verwendung der angezeigten Standardwerte.

AD-Eigenschaft	Erforderlich oder optional	Standardwert
userPrincipalName	Erforderlich, wenn kein SID-Attribut hinzugefügt wird (empfohlen).	`cip_upn`
objectSID	Erforderlich, wenn kein UPN-Attribut hinzugefügt wird.	`cip_sid`
objectGUID	Optional für die Authentifizierung	`cip_oid`
mail	Optional für die Authentifizierung	`cip_email`
displayName	Erforderlich für die Workspace-Benutzeroberfläche	`displayName`
givenName	Erforderlich für die Workspace-Benutzeroberfläche	`firstName`
sn	Erforderlich für die Workspace-Benutzeroberfläche	`lastName`
AD Forest	Optional für die Authentifizierung	`cip_forest`
AD Domain	Optional für die Authentifizierung	`cip_domain`

3. Wählen Sie das AD aus, das Sie mit Citrix Cloud verbunden haben. Je nach der Konsole Ihres SAML-Anbieters können Sie beispielsweise **Users > Directories** auswählen.
4. Wählen Sie die Option zum Hinzufügen von Verzeichnisattributen aus. Je nach der Konsole Ihres SAML-Anbieters können Sie beispielsweise **Directory Attributes** auswählen.
5. Wählen Sie die Option zum Hinzufügen von Attributen aus und ordnen Sie die folgenden AD-Attribute den in Schritt 2 erstellten benutzerdefinierten Benutzerattributen zu:
   - Wenn Sie in Schritt 2 das SID-Attribut hinzugefügt haben (z. B. `cip_sid`), wählen Sie **objectSid** und ordnen Sie es dem von Ihnen erstellten Attribut zu.
   - Wenn Sie in Schritt 2 das UPN-Attribut hinzugefügt haben (z. B. `cip_upn`), wählen Sie **userPrincipalName** und ordnen Sie es dem von Ihnen erstellten Attribut zu.
   - Wenn Sie in Schritt 2 das ObjectGUID-Attribut hinzugefügt haben (z. B. `cip_oid`), wählen Sie **ObjectGUID** und ordnen Sie es dem von Ihnen erstellten Attribut zu.
   - Wenn Sie in Schritt 2 das E-Mail-Attribut hinzugefügt haben (z. B. `cip_email`), wählen Sie **mail** und ordnen Sie es dem von Ihnen erstellten Attribut zu.
   - Wenn Sie in Schritt 2 das Anzeigenamen-Attribut hinzugefügt haben (z. B. `displayName`), wählen Sie **displayName** und ordnen Sie es dem von Ihnen erstellten Attribut zu.

Konfigurieren der Anmelde-URL für Administratoren

1. Melden Sie sich bei Citrix Cloud unter https://citrix.cloud.com an.
2. Klicken Sie im Menü "Citrix Cloud"auf **Identitäts- und Zugriffsverwaltung**.
3. Suchen Sie **SAML 2.0**, klicken Sie auf die Auslassungspunkte (...) und wählen Sie **Verbinden** aus.
4. Geben Sie bei der entsprechenden Aufforderung einen kurzen, URL-freundlichen Bezeichner für Ihr Unternehmen ein und wählen Sie **Speichern und Fortfahren**. Die Seite **SAML konfigurieren** wird angezeigt.
5. Fahren Sie mit dem nächsten Abschnitt fort, um die SAML-Verbindung zu Citrix Cloud zu konfigurieren.

Konfigurieren der SAML-Anbieter-Metadaten

In dieser Aufgabe erstellen Sie eine Connectoranwendung mit SAML-Metadaten aus Citrix Cloud. Nach Konfiguration der SAML-Anwendung verwenden Sie die SAML-Metadaten Ihrer Connectoranwendung, um die SAML-Verbindung zu Citrix Cloud zu konfigurieren.

> **Hinweis:**
>
> In einigen Schritten in diesem Abschnitt werden Aktionen beschrieben, die Sie in der Verwaltungskonsole Ihres SAML-Anbieters ausführen. Die speziellen Befehle, die Sie zur Durchführung dieser Aktionen verwenden, können je nach ausgewähltem SAML-Anbieter von den in diesem Abschnitt beschriebenen Befehlen abweichen. Die Befehle des SAML-Anbieters in diesem Abschnitt werden nur als Beispiele angegeben. Weitere Informationen zu den entsprechenden Befehlen für Ihren SAML-Anbieter finden Sie in der Dokumentation Ihres SAML-Anbieters.

SAML-Connectoranwendung erstellen

1. Fügen Sie in der Verwaltungskonsole Ihres SAML-Anbieters eine Anwendung für einen Identitätsanbieter mit Attributen und Signierantwort hinzu. Beispielsweise können Sie je nach Konsole Ihres Anbieters **Applications > Applications > Add App** auswählen und dann **SAML Test Connector (IdP w/attr w/sign response)** auswählen.
2. Falls zutreffend, geben Sie einen Anzeigenamen ein und speichern Sie die App.
3. Wählen Sie im Bildschirm **SAML konfigurieren** in Citrix Cloud in **SAML-Metadaten**die Option **Herunterladen** aus. Die Metadaten-XML-Datei wird in einer anderen Browserregisterkarte angezeigt

> **Hinweis:**
>
> Bei Bedarf können Sie diese Datei auch von `https://saml.cloud.com/saml/metadata.xml` herunterladen. Dieser Endpunkt ist möglicherweise für einige Identitätsanbieter benutzerfreundlicher, wenn die SAML-Anbietermetadaten importiert und überwacht werden.

4. Geben Sie die folgenden Details für die Connectoranwendung ein:
   - Geben Sie im Feld **Zielgruppe** `https://saml.cloud.com` ein.
   - Geben Sie im Feld **Empfänger** `https://saml.cloud.com/saml/acs` ein.
   - Geben Sie im Feld für ACS-URL-Validator `https://saml.cloud.com/saml/acs` ein.
   - Geben Sie im Feld für ACS-URL `https://saml.cloud.com/saml/acs` ein.
5. Fügen Sie Ihre benutzerdefinierten SAML-Attribute als Parameterwerte in der Anwendung hinzu:

Dieses Feld erstellen	Dieses benutzerdefinierte Attribut zuweisen
cip_sid	Das benutzerdefinierte Attribut, das Sie für SID erstellt haben. Beispiel: cip_sid
cip_upn	Das benutzerdefinierte Attribut, das Sie für UPN erstellt haben. Beispiel: cip_upn
cip_oid	Das benutzerdefinierte Attribut, das Sie für ObjectGUID erstellt haben. Beispiel: cip_oid
cip_email	Das benutzerdefinierte Attribut, das Sie für E-Mail erstellt haben. Beispiel: cip_email
displayName	Das benutzerdefinierte Attribut, das Sie für den Anzeigenamen erstellt haben. Beispiel: displayName

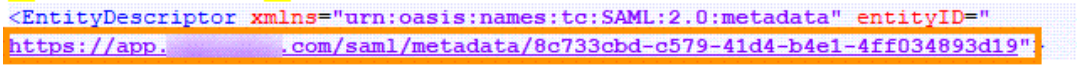
6. Fügen Sie Ihre Workspace-Abonnenten als Benutzer hinzu, damit sie auf die Anwendung zugreifen können.

SAML-Anbietermetadaten zu Citrix Cloud hinzufügen

1. Rufen Sie die SAML-Metadaten von Ihrem SAML-Anbieter ab. Die folgende Abbildung ist ein Beispiel dafür, wie diese Datei aussehen könnte:

2. Geben Sie im Bildschirm **SAML konfigurieren** in Citrix Cloud die folgenden Werte aus der Metadatendatei Ihres SAML-Anbieters ein:

   - Geben Sie unter **Entitäts-ID des Identitätsanbieters** den **entityID**-Wert aus dem **EntityDescriptor**-Element in den Metadaten ein.

   - Wählen Sie unter **Authentifizierungsanforderung signieren** die Option **Ja** aus, damit Citrix Cloud Authentifizierungsanforderungen signieren und so bestätigen kann, dass sie von Citrix Cloud stammen und nicht von einem schädlichen Akteur. Wählen Sie **Nein** aus, wenn Sie die Citrix ACS-URL lieber einer Positivliste hinzufügen möchten, die Ihr SAML-Anbieter verwendet, um SAML-Antworten sicher zu veröffentlichen.

   - Geben Sie unter **SSO-Dienst-URL** die URL für den Bindungsmechanismus ein, den Sie verwenden möchten. Sie können entweder HTTP-POST- oder HTTP-Redirect-Bindung verwenden. Suchen Sie in der Metadatendatei die **SingleSignOnService**-Elemente mit den Bindungswerten von **HTTP-POST** oder **HTTP-Redirect**.

- Wählen Sie unter **Bindungsmechanismus** den Mechanismus aus, der der Bindung für die SSO-Dienst-URL entspricht, die Sie aus der Metadatendatei ausgewählt haben. Standardmäßig ist **HTTP-Post** ausgewählt.
- Wählen Sie unter **SAML-Antwort** die Signiermethode aus, die Ihr SAML-Anbieter für die SAML-Antwort und SAML-Assertion verwendet. Standardmäßig ist **Antwort oder Assertion signieren** ausgewählt. Citrix Cloud lehnt alle Antworten ab, die nicht wie in diesem Feld angegeben signiert sind.

3. Führen Sie in der Verwaltungskonsole Ihres SAML-Anbieters die folgenden Aktionen aus:
   - Wählen Sie **SHA-256** für den SAML-Signaturalgorithmus aus.
   - Laden Sie das X.509-Zertifikat als mit Base64 verschlüsselte PEM-, CRT- oder CER-Datei herunter.
4. Wählen Sie auf der Seite **SAML konfigurieren** in Citrix Cloud unter **X.509-Zertifikat** die Option **Datei hochladen** und wählen Sie die im vorherigen Schritt heruntergeladene Zertifikatdatei aus.
5. Wählen Sie **Weiter** aus, um den Upload abzuschließen.
6. Wählen Sie unter **Authentifizierungskontext** den Kontext aus, den Sie verwenden möchten, und wählen Sie aus, wie streng Citrix Cloud diesen Kontext durchsetzen soll. Wählen Sie **Minimum** aus, um die Authentifizierung im ausgewählten Kontext anzufordern, ohne die Authentifizierung in diesem Kontext durchzusetzen. Wählen Sie **Genau** aus, um die Authentifizierung im ausgewählten Kontext anzufordern und nur in diesem durchzusetzen. Wenn Ihr SAML-Anbieter keine Authentifizierungskontexte unterstützt oder Sie diese nicht verwenden, wählen Sie **Keine Angabe** und **Minimum** aus. Standardmäßig sind **Keine Angabe** und **Exakt** ausgewählt.
7. Geben Sie unter **Abmelde-URL** (optional) an, ob Benutzer, die sich von Citrix Workspace oder Citrix Cloud abmelden, auch von allen Webanwendungen abgemeldet werden sollen, bei denen sie sich zuvor über den SAML-Anbieter angemeldet haben.
   - Sollen die Benutzer bei Abmeldung von Citrix Workspace oder Citrix Cloud bei ihren Webanwendungen angemeldet bleiben, lassen Sie das Feld **Abmelde-URL** leer.
   - Sollen die Benutzer bei Abmeldung von Citrix Workspace oder Citrix Cloud bei ihren Webanwendungen abgemeldet werden, geben Sie den Single Logout-Endpunkt Ihres SAML-Anbieters ein. Wenn Sie Microsoft AD FS oder Azure Active Directory als SAML-Anbieter verwenden, entspricht der SLO-Endpunkt dem Single Sign-On-Endpunkt.

8. Stellen Sie sicher, dass die folgenden Standardattributwerte in Citrix Cloud mit den entsprechenden in der Verwaltungskonsole Ihres SAML-Anbieters konfigurierten Attributwerten übereinstimmen. Damit Citrix Cloud diese Attribute in der SAML-Assertion findet, müssen die hier eingegebenen Werte mit denen im SAML-Anbieter übereinstimmen. Wenn Sie ein Attribut nicht in Ihrem SAML-Anbieter konfiguriert haben, können Sie den Standardwert in Citrix Cloud verwenden oder das Feld leer lassen, sofern nicht anders angegeben.

   - **Attributname für Benutzeranzeigename**: Standardwert ist `displayName`.
   - **Attributname für Vorname**: Standardwert ist `firstName`.
   - **Attributname für Nachname**: Standardwert ist `lastName`.
   - **Attributname für Sicherheits-ID (SID):** Sie müssen diesen Attributnamen aus Ihrem SAML-Anbieter eingeben, wenn Sie kein Attribut für UPN erstellt haben. Der Standardwert ist `cip_sid`.
   - **Attributname für Benutzerprinzipalname (UPN):** Sie müssen diesen Attributnamen aus Ihrem SAML-Anbieter eingeben, wenn Sie kein Attribut für SID erstellt haben. Der Standardwert ist `cip_upn`.
   - **Attributname für E-Mail**: Standardwert ist `cip_email`.
   - **Attributname für AD-Objektbezeichner (OID):**: Standardwert ist `cip_oid`.
   - **Attributname für AD-Gesamtstruktur:**: Standardwert ist `cip_forest`.
   - **Attributname für AD-Domäne:**: Standardwert ist `cip_domain`.

9. Wählen Sie **Testen und schließen** aus, um zu überprüfen, ob Sie die Verbindung erfolgreich konfiguriert haben.

Administratoren aus AD zu Citrix Cloud hinzufügen

Anweisungen zum Hinzufügen und Verwalten von AD-Gruppen in Citrix Cloud finden Sie unter Administratorgruppen verwalten.

SAML-Authentifizierung für Workspaces aktivieren

1. Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration**.
2. Wählen Sie die Registerkarte **Authentifizierung** aus.
3. Wählen Sie **SAML 2.0** aus.

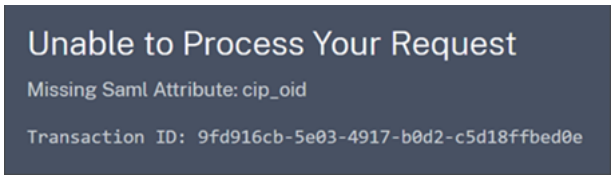
Problembehandlung

Attributfehler

Attributfehler können unter den folgenden Bedingungen auftreten:

- Die erforderlichen Attribute in Ihrer SAML-Konfiguration sind nicht korrekt codiert.
- Die Attribute `cip_sid` und `cip_upn` fehlen in der SAML-Assertion.
- Attribut `cip_sid` oder `cip_oid` fehlt in der SAML-Assertion und Citrix Cloud kann es aufgrund eines Verbindungsproblems nicht aus Active Directory abrufen.

Wenn ein Attributfehler auftritt, zeigt Citrix Cloud eine Fehlermeldung an, die die fehlerhaften Attribute enthält.



Gehen Sie wie folgt vor, um diese Art von Fehler zu beheben:

1. Vergewissern Sie sich, dass Ihr SAML-Anbieter die erforderlichen Attribute mit der richtigen Codierung sendet (siehe folgende Tabelle). Es muss zumindest das SID- oder das UPN-Attribut enthalten sein.

Attribut	Codierung	Erforderlich
cip_email	Zeichenfolge (`user@domain`)	
cip_oid	Base64 oder Zeichenfolge	
cip_sid	Base64 oder Zeichenfolge	Ja, wenn `cip_upn` nicht verwendet wird
cip_upn	Zeichenfolge (`user@domain`)	Ja, wenn `cip_sid` nicht verwendet wird

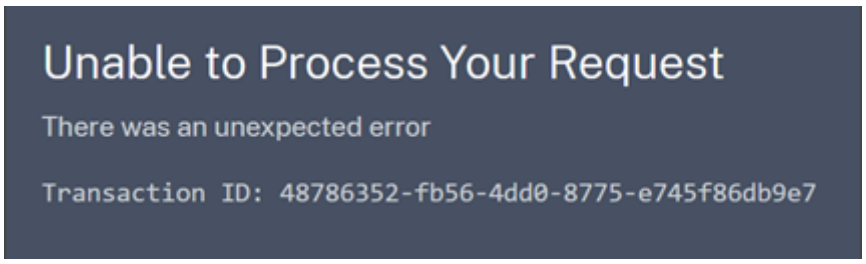
2. Vergewissern Sie sich, dass die Cloud Connectors online sind und einwandfrei funktionieren, damit Citrix Cloud jegliche fehlenden Attribute abrufen kann. Weitere Informationen finden Sie unter Erweiterte Cloud Connector-Integritätsprüfungen.

Unerwartete Fehler

In Citrix Cloud tritt möglicherweise ein unerwarteter Fehler auf, wenn:

- Ein Benutzer eine SAML-Anforderung mithilfe eines IDP-initiierten Flows macht. Beispiel: Die Anforderung wird gestellt, indem eine Kachel über das App-Portal des Identitätsanbieters ausgewählt wird, anstatt direkt zur Workspace-URL (`customer.cloud.com`) zu wechseln.
- Das SAML-Zertifikat ungültig oder abgelaufen ist.
- Der Authentifizierungskontext ungültig ist.
- SAML-Assertion und Antwortsignatur nicht übereinstimmen.

Wenn dieser Fehler auftritt, zeigt Citrix Cloud eine generische Fehlermeldung an.

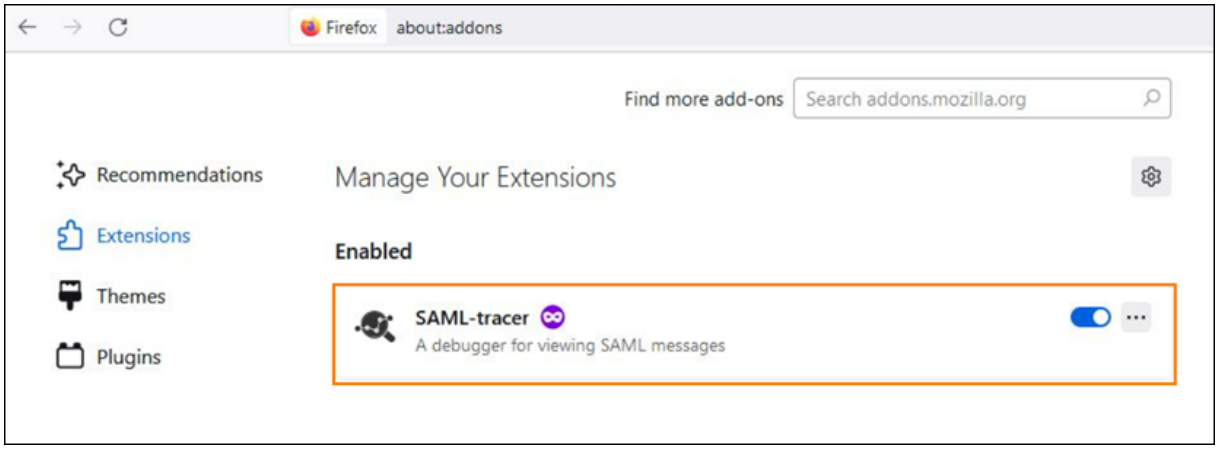


Wenn der Fehler auf den Wechsel zu Citrix Cloud über das App-Portal eines Identitätsanbieters zurückzuführen ist, können Sie folgenden Workaround verwenden:

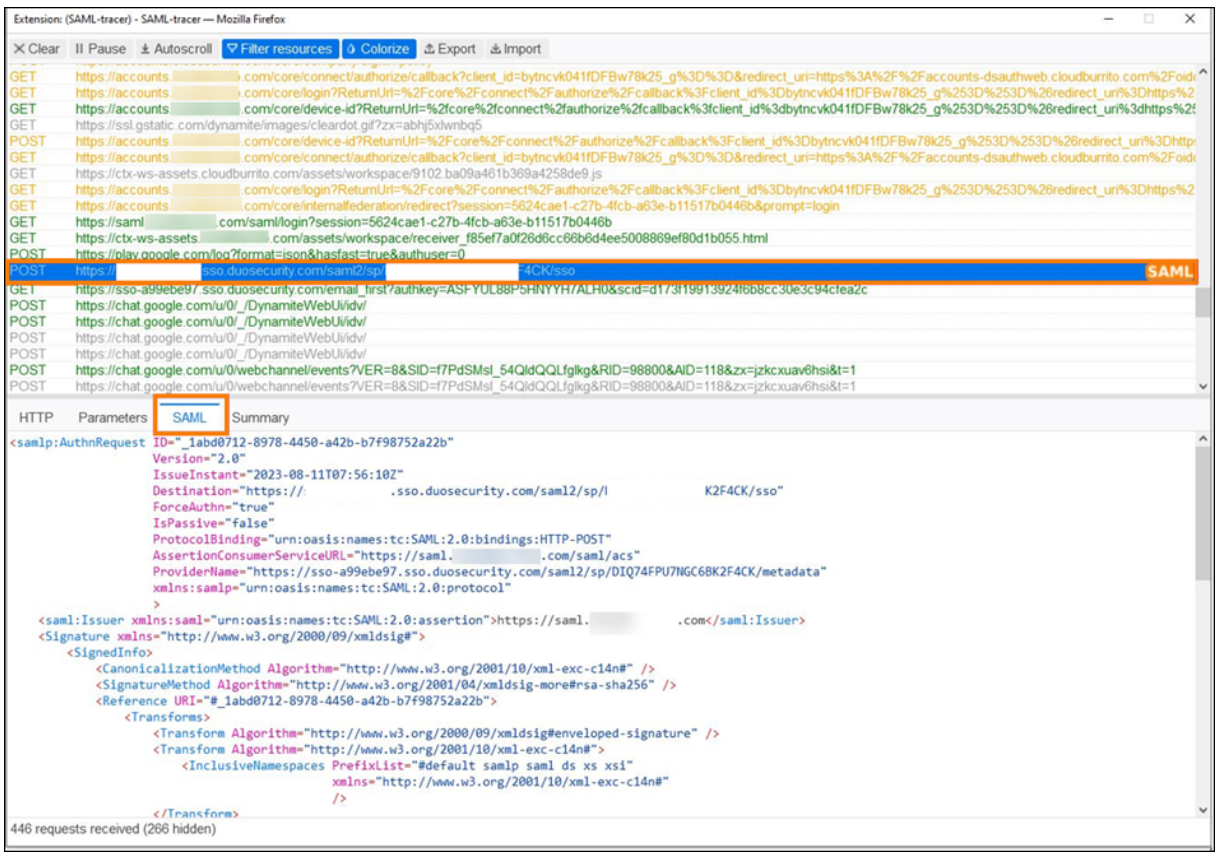
1. Erstellen Sie im App-Portal des Identitätsanbieters eine Lesezeichen-App, die auf Ihre Workspace-URL verweist (z. B. `https://customer.cloud.com`).
2. Weisen Sie Benutzer sowohl der SAML-App als auch der Lesezeichen-App zu.
3. Ändern Sie die Sichtbarkeit der SAML-App und der Lesezeichen-App so, dass die Lesezeichen-App sichtbar und die SAML-App im App-Portal verborgen ist.
4. Deaktivieren Sie die Einstellung **Verbundidentitätsanbietersitzungen** in der Workspace-Konfiguration, um zusätzliche Kennwortaufforderungen zu entfernen. Anweisungen finden Sie unter Verbundidentitätsanbietersitzungen in der Citrix Workspace-Produktdokumentation.

Empfehlungen zum Debuggen

Citrix empfiehlt die Verwendung der Browsererweiterung SAML-tracer für das gesamte SAML-Debugging. Die Erweiterung ist für die meisten der gängigen Webbrowser verfügbar. Die Erweiterung decodiert Base64-Anfragen und -Antworten in SAML-XML, wodurch sie für Menschen lesbar werden.



Mit diesem Tool können Sie als Administrator den Wert der für einen Benutzer gesendeten SAML-Attribute und das Vorhandensein von Signaturen in SAML-Anfragen und -Antworten überprüfen. Falls Sie Hilfe bei einem SAML-Problem benötigen, fordert der Citrix Support die SAML-Tracer-Datei an, um das Problem zu analysieren und zu lösen.



Weitere Informationen

- Microsoft-Dokumentation: Tutorial: Integration des einmaligen Anmeldens (SSO) von Azure Active Directory mit Citrix Cloud SAML SSO

- SAML mit Active Directory-Verbunddienste (AD FS): SAML-Authentifizierung in Citrix Cloud mit AD FS konfigurieren.
- Citrix Tech Zone: Tech Insight: Authentication - SAML

SAML-Anwendung mit bereichsbezogener Entitäts-ID in Citrix Cloud konfigurieren

December 11, 2023

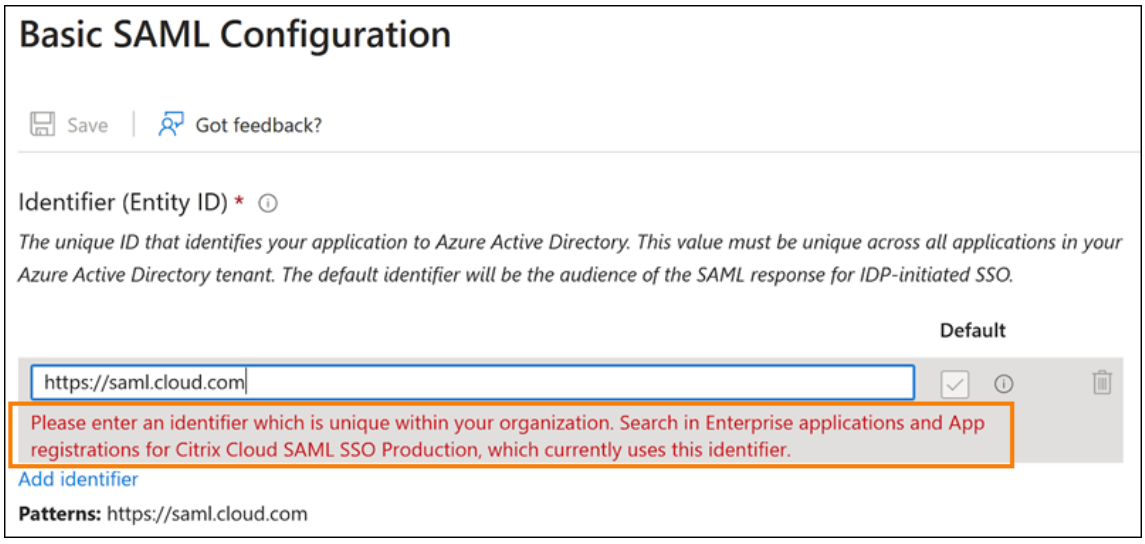
Author:
Mark Dear

In diesem Artikel wird beschrieben, wie Sie mehrere SAML-Anwendungen im selben SAML-Anbieter bereitstellen.

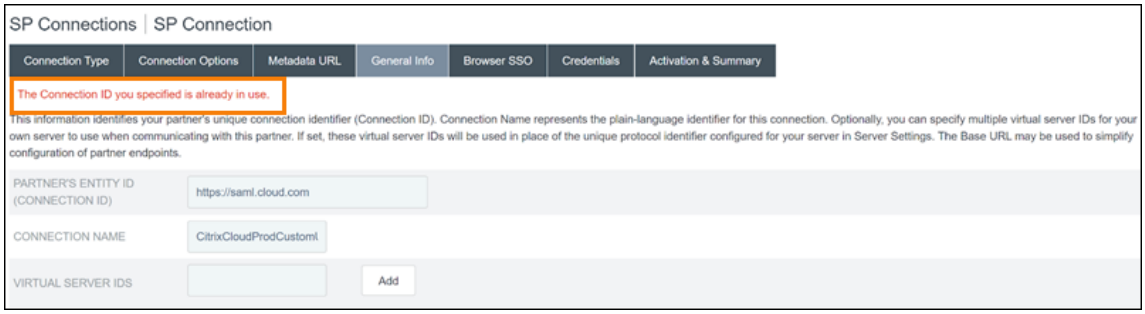
Manche SAML-Anbieter, wie etwa Azure Active Directory (AD), Active Directory-Verbunddienste (ADFS), PingFederate und PingSSO, gestatten keine Wiederverwendung derselben Dienstanbieter-Entitäts-ID in mehreren SAML-Anwendungen. Daher können Administratoren, die zwei oder mehr SAML-Anwendungen im selben SAML-Anbieter erstellen, diese nicht mit denselben oder unterschiedlichen Citrix Cloud-Mandanten verknüpfen. Wird versucht, eine zweite SAML-Anwendung mit einer Dienstanbieter Entitäts-ID zu erstellen, die bereits für eine andere SAML-Anwendung verwendet wird (z. B. `https:\\saml.cloud.com`), wird eine entsprechende Fehlermeldung angezeigt.

Die folgenden Abbildungen zeigen die Fehlermeldung:

- Azure Active Directory:



- PingFederate:



Bereichsbezogene Entitäts-IDs in Citrix Cloud beseitigen diese Einschränkung, sodass Sie mehrere SAML-Anwendungen in einem SAML-Anbieter (z. B. einem Azure AD-Mandanten) erstellen und mit einem Citrix Cloud-Mandanten verknüpfen können.

Was ist eine Entitäts-ID?

Eine SAML-Entitäts-ID ist ein eindeutiger Bezeichner, zur Identifizierung einer Entität im Authentifizierungs- und Autorisierungsprotokoll SAML. In der Regel ist die Entitäts-ID eine URL oder ein URI, die/der Entität zugewiesen und in SAML-Meldungen und -Metadaten verwendet wird. Jede SAML-Anwendung, die Sie in Ihrem SAML-Anbieter erstellen, wird als eindeutige Entität betrachtet.

In einer SAML-Verbindung zwischen Citrix Cloud und Azure AD ist beispielsweise Citrix Cloud der Dienstanbieter (SP) und Azure AD der SAML-Anbieter. Beide haben eine Entitäts-ID, die jeweils am anderen Ende der SAML-Verbindung konfiguriert werden muss. Die Entitäts-ID von Citrix Cloud muss also in Azure AD konfiguriert werden und die Entitäts-ID von Azure AD in Citrix Cloud.

Beispiele einer generischen Entitäts-ID und einer bereichsbezogenen Entitäts-ID in Citrix Cloud:

- Generisch: `https://saml.cloud.com`
- Bereichsbezogen: `https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`

Generische SP-Entitäts-IDs und bereichsbezogene Entitäts-IDs nach Region

Vor November 2023 in Citrix Cloud erstellte SAML-Verbindungen verwenden dieselbe generische Entitäts-ID für alle SAML-Verbindungen und Citrix Cloud-Mandanten. Nur neue Citrix Cloud SAML-Verbindungen bieten die Möglichkeit, eine bereichsbezogene Entitäts-ID zu verwenden.

Wenn Sie bereichsbezogene Entitäts-IDs für neue Verbindungen verwenden, funktionieren die vorhandenen SAML-Verbindungen mit den ursprünglichen generischen Entitäts-IDs weiterhin.

Die folgende Tabelle enthält die generischen SP-Entitäts-IDs und bereichsbezogene Entitäts-IDs für die einzelnen Citrix Cloud-Regionen:

Citrix Cloud-Region	Generische SP-Entitäts-ID	Bereichsbezogene Entitäts-ID
Vereinigte Staaten, Europäische Union, Asien-Pazifik-Süd	https://saml.cloud.com	https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb
Japan	https://saml.citrixcloud.jp	https://saml.citrixcloud.jp/db642d4c-ad2c-4304-adcf-f96b6aa16c29
Behörden	https://saml.cloud.us	https://saml.cloud.us/20f1cf66-cfe9-4dd3-865c-9c59a6710820

Eindeutige SP-Entitäts-IDs für neue und bestehende SAML-Verbindungen generieren

Wenn Sie eine neue SAML-Verbindung erstellen, generiert Citrix Cloud eine eindeutige ID (GUID). Um eine bereichsbezogene Entitäts-ID zu generieren, aktivieren Sie die Einstellung **Konfigurieren der bereichsbezogenen SAML-Entitäts-ID**, wenn Sie die neue Verbindung erstellen.

Wenn Sie eine vorhandene SAML-Verbindung auf die Verwendung von bereichsbezogenen Entitäts-IDs aktualisieren möchten, müssen Sie den SAML-Anbieter auf der Seite **Identitäts- und Zugriffsverwaltung > Authentifizierung** in Citrix Cloud trennen und dann erneut verbinden. In Citrix Cloud können Sie SAML-Verbindungen nicht direkt bearbeiten. Sie können eine Konfiguration jedoch klonen und den Klon ändern.

> **Wichtig:**
>
> Wenn Sie den SAML-Verbindungsprozess vor Fertigstellung schließen, wird die von Citrix Cloud automatisch generierte Entitäts-ID verworfen. Wenn Sie den SAML-Verbindungsprozess neu starten, generiert Citrix Cloud eine neue bereichsbezogene Entitäts-ID. Verwenden Sie diese neue bereichsbezogene Entitäts-ID, wenn Sie den SAML-Anbieter konfigurieren. Wenn Sie eine vorhandene SAML-Verbindung auf die Verwendung von bereichsbezogenen Entitäts-IDs aktualisieren, müssen Sie die SAML-Anwendung für die Verbindung mit der von Citrix Cloud generierten Entitäts-ID mit Bereich aktualisieren.

Häufig gestellte Fragen zu bereichsbezogenen Entitäts-IDs

Kann man mehrere Azure AD SAML-Anwendung im selben Azure AD-Mandanten erstellen und sie mit einem oder mehreren Citrix Cloud-Mandanten verknüpfen?

Das Feature der bereichsbezogenen Entitäts-IDs in Citrix Cloud löst das Problem des bei einigen SAML-Anbietern geltenden Verbots doppelter Entitäts-IDs. Mithilfe des Features können Sie mehrere SAML-Anwendungen in einem Azure AD-Mandanten bereitstellen und jede mit einer bereichsbezogenen Entitäts-ID von einem Citrix Cloud-Mandanten konfigurieren.

Kann man eine Azure AD SAML-Anwendung weiterhin mit mehreren Citrix Cloud-Mandanten verknüpfen?

Dies ist bei Citrix Cloud-Kunden üblich und wird weiterhin von Citrix unterstützt. Um dies zu implementieren, müssen Sie die folgenden Anforderungen erfüllen:

- Verwenden einer generischen Entitäts-ID, z. B. `https://saml.cloud.com`
- Bereichsbezogene Entitäts-IDs für die SAML-Verbindung nicht aktiviert

Wie entscheidet man, ob man eine bereichsbezogene Entitäts-ID im SAML-Anbieter verwenden sollte?

In Citrix Cloud können Sie nach Bedarf bereichsbezogene Entitäts-IDs oder eine generische Entitäts-ID verwenden. Berücksichtigen Sie die Zahl der benötigten SAML-Anwendungen und die Zahl Ihrer Citrix Cloud-Mandanten. Überlegen Sie außerdem, ob die Mandanten eine SAML-Anwendung gemeinsam nutzen können oder ob eine eigene, bereichsbezogene SAML-Anwendung erforderlich ist.

> **Wichtig:**
>
> Wenn Ihr SAML-Anbieter die Erstellung mehrerer SAML-Anwendungen mit derselben Entitäts-ID bereits ermöglicht (z. B. `https://saml.cloud.com`), müssen Sie bereichsbezogene Entitäts-IDs nicht aktivieren und keine Änderungen an Ihrer SAML-Konfiguration vornehmen. Sie müssen weder in Citrix Cloud noch in Ihrer SAML-Anwendung Einstellungen aktualisieren.

Betroffene SAML-Anbieter

Die folgende Tabelle enthält Informationen zur Möglichkeit der Verwendung doppelter Entitäts-IDs bei verschiedenen SAML-Anbietern.

SAML-Anbieter	Unterstützt doppelte Entitäts-IDs
Azure AD (Cloud)	Nein
AD FS (on-premises)	Nein
PingFederate (on-premises)	Nein
PingOneSSO (Cloud)	Nein
Okta (Cloud)	Ja
Duo (Cloud)	Ja
OneLogin (Cloud)	Ja

Betroffene Anwendungsfälle

Die folgende Tabelle enthält Informationen zur Unterstützung der generischen bzw. bereichsbezogener Entitäts-IDs basierend auf den für verschiedene Anwendungsfälle erforderlichen SAML-Anwendungen sowie zur Unterstützung doppelter Entitäts-IDs durch die SAML-Anbieter.

Anforderung aufgrund Anwendungsfall	Unterstützung doppelter Entitäts-IDs	Unterstützte Konfiguration
Nur eine SAML-Anwendung	Ja	Generische oder bereichsbezogene Entitäts-ID
Nur eine SAML-Anwendung	Nein	Generische oder bereichsbezogene Entitäts-ID
Zwei oder mehr SAML-Anwendungen	Ja	Generische oder bereichsbezogene Entitäts-ID
Zwei oder mehr SAML-Anwendungen	Nein	Bereichsbezogene Entitäts-ID
Paarzuordnung: benutzerdefinierte Workspace-URL/SAML-Anwendung	Ja	Generische oder bereichsbezogene Entitäts-ID
Paarzuordnung: benutzerdefinierte Workspace-URL/SAML-Anwendung	Nein	Bereichsbezogene Entitäts-ID
Verknüpfen der Azure AD SAML-Anwendung mit mehreren Citrix Cloud-Mandanten	Ja	Generische Entitäts-ID

Anforderung aufgrund Anwendungsfall	Unterstützung doppelter Entitäts-IDs	Unterstützte Konfiguration
Verknüpfen der Azure AD SAML-Anwendung mit mehreren Citrix Cloud-Mandanten	Nein	Generische Entitäts-ID

Primäre SAML-Verbindung mit einer bereichsbezogenen Entitäts-ID konfigurieren

Bei diesem Arbeitsgang erstellen Sie eine SAML-Verbindung in Citrix Cloud unter Einsatz einer bereichsbezogenen Entitäts-ID für die primäre SAML-Anwendung (SAML App 1).

1. Klicken Sie im Menü "Citrix Cloud"auf **Identitäts- und Zugriffsverwaltung**.
2. Wählen Sie auf der Registerkarte **Authentifizierung** für **SAML 2.0** über die Auslassungspunkte (…) **Verbinden**.
3. Geben Sie bei Erscheinen der Aufforderung, Ihre eindeutige Anmelde-URL zu erstellen, einen kurzen, URL-freundlichen Bezeichner für Ihr Unternehmen ein (z. B. `https://citrix.cloud.com/go/mycompany`) und wählen Sie **Speichern und Fortfahren**. Dieser Bezeichner muss in Citrix Cloud eindeutig sein.
4. Wählen Sie unter **SAML-Identitätsanbieter konfigurieren** die Option **Konfigurieren der bereichsbezogenen SAML-Entitäts-ID**. Citrix Cloud generiert automatisch bereichsbezogene Entitäts-IDs und füllt die Felder für Entitäts-ID, Assertion Consumer Service und Abmelde-URL aus.
5. Geben Sie unter **SAML-Verbindung mit Citrix Cloud konfigurieren** die Verbindungsdetails aus Ihrem SAML-Anbieter ein.
6. Akzeptieren Sie die standardmäßigen SAML-Attributzuordnungen.
7. Wählen Sie **Testen und schließen**.

Primäre SAML-Verbindung mit einer generischen Entitäts-ID konfigurieren

Bei diesem Arbeitsgang erstellen Sie eine SAML-Verbindung in Citrix Cloud unter Einsatz einer generischen Entitäts-ID für die primäre SAML-Anwendung (SAML App 1).

1. Klicken Sie im Menü "Citrix Cloud"auf **Identitäts- und Zugriffsverwaltung**.
2. Wählen Sie auf der Registerkarte **Authentifizierung** für **SAML 2.0** über die Auslassungspunkte (…) **Verbinden**.
3. Geben Sie bei Erscheinen der Aufforderung, Ihre eindeutige Anmelde-URL zu erstellen, einen kurzen, URL-freundlichen Bezeichner für Ihr Unternehmen ein (z. B. `https://citrix`

.cloud.com/go/mycompany) und wählen Sie **Speichern und Fortfahren**. Dieser Bezeichner muss in Citrix Cloud eindeutig sein.

4. Stellen Sie sicher, dass unter **SAML-Identitätsanbieter konfigurieren** die Option **Konfigurieren der bereichsbezogenen SAML-Entitäts-ID** deaktiviert ist.
5. Geben Sie unter **SAML-Verbindung mit Citrix Cloud konfigurieren** die Verbindungsdetails aus Ihrem SAML-Anbieter ein.
6. Klicken Sie unter **SAML-Metadaten des Dienstanbieters** auf **Herunterladen**, um die generischen SAML-Metadaten bei Bedarf herunterzuladen.
7. Akzeptieren Sie die standardmäßigen SAML-Attributzuordnungen.
8. Wählen Sie **Testen und schließen**.

SAML-Verbindung mit benutzerdefinierten Citrix Workspace-Domänen konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie eine SAML-Verbindung mithilfe einer benutzerdefinierten Workspace-URL mit einer bereichsbezogenen oder generischen Entitäts-ID konfigurieren.

Die Aufgaben in diesem Abschnitt gelten nur in Fällen, wenn eine benutzerdefinierte Workspace-URL mit SAML verwendet wird. Wenn Sie keine benutzerdefinierte Workspace-URL mit SAML-Authentifizierung verwenden, können Sie die Aufgaben in diesem Abschnitt überspringen.

Weitere Informationen hierzu finden Sie in den folgenden Artikeln:

- Benutzerdefinierte Domäne konfigurieren
- Anmeldung bei Workspace mit SAML unter Verwendung benutzerdefinierter Domänen

SAML-Verbindung mit einer benutzerdefinierten Workspace-URL und einer generischen Entitäts-ID konfigurieren

In dieser Aufgabe ist die Einstellung **Entity-ID mit Bereich konfigurieren** deaktiviert.

1. Wählen Sie im Citrix Cloud-Menü **Workspaceauthentifizierung**.
2. Wählen Sie unter **Benutzerdefinierte Workspace-URL** die Auslassungspunkte und dann die Option **Bearbeiten**.
3. Wählen Sie **Verwenden Sie die URL "<kundenname>.cloud.com"und die benutzerdefinierte Domänen-URL**.
4. Geben Sie die generische Entitäts-ID, die SSO-URL und optional die SLO-URL für SAML App 2 ein und laden Sie das zuvor von Ihrem SAML-Anbieter heruntergeladene Signaturzertifikat hoch.
5. Klicken Sie unter **SAML-Metadaten des DIenstanbieters für benutzerdefinierte Domäne** auf **Herunterladen**, um die generischen SAML-Metadaten für die SAML-Anwendung für die benutzerdefinierte Workspace-URL bei Bedarf herunterzuladen.
6. Klicken Sie auf **Speichern**.

SAML-Verbindung mit einer benutzerdefinierten Workspace-URL und einer bereichsbezogenen Entitäts-ID konfigurieren

In dieser Aufgabe ist die Einstellung **Konfigurieren der bereichsbezogenen SAML-Entitäts-ID** aktiviert.

1. Wählen Sie im Citrix Cloud-Menü **Workspaceauthentifizierung**.
2. Wählen Sie unter **Benutzerdefinierte Workspace-URL** die Auslassungspunkte und dann die Option **Bearbeiten**.
3. Wählen Sie **Verwenden Sie die URL "<kundenname>.cloud.com"und die benutzerdefinierte Domänen-URL**.
4. Geben Sie die bereichsbezogene Entitäts-ID, die SSO-URL und optional die SLO-URL für SAML App 2 ein und laden Sie das zuvor von Ihrem SAML-Anbieter heruntergeladene SAML-Signaturzertifikat hoch.
5. Klicken Sie auf **Speichern**.

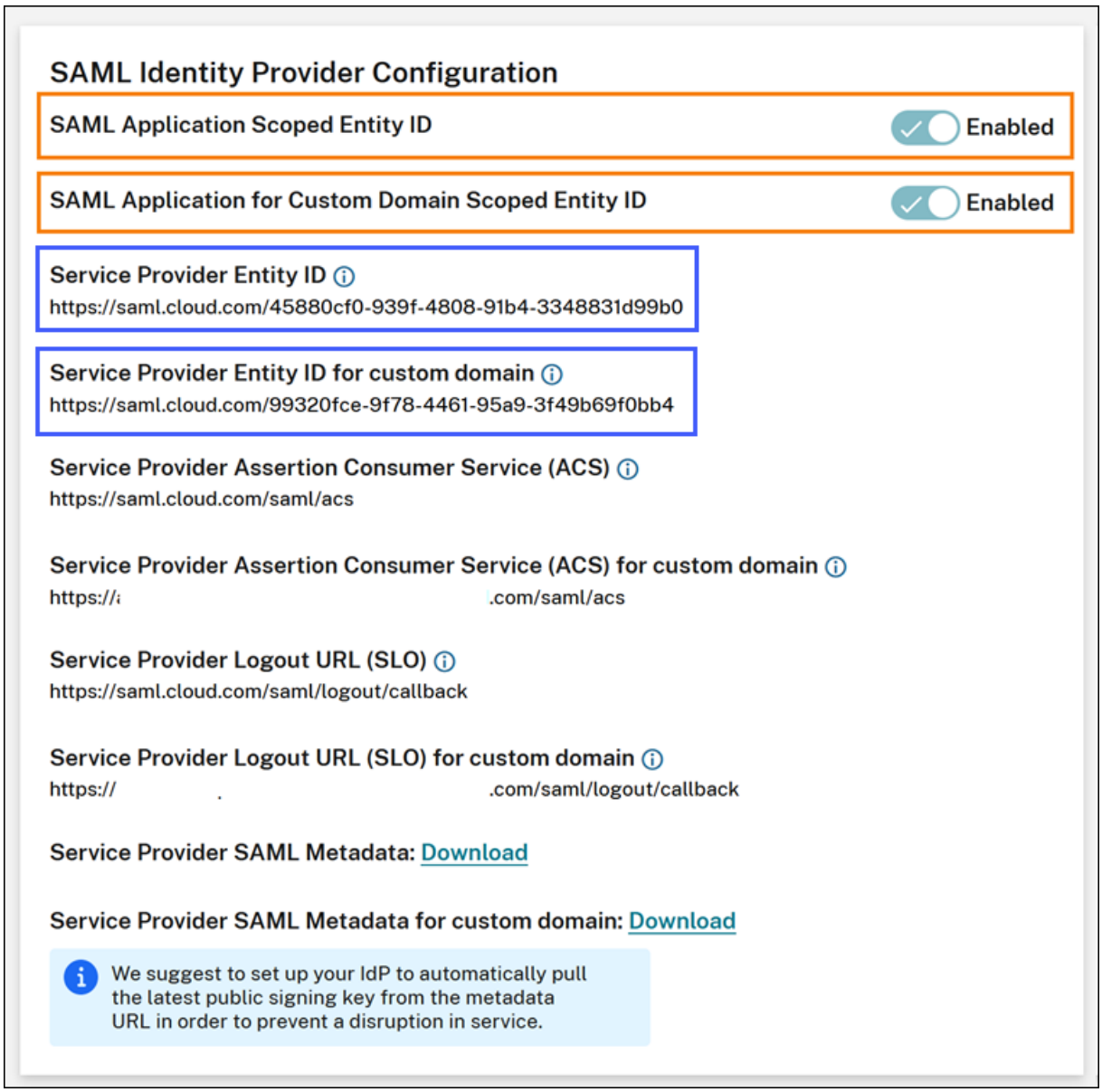
Nach dem Speichern der Konfiguration generiert Citrix Cloud die bereichsbezogenen SAML-Metadaten mit der richtige GUID. Bei Bedarf können Sie eine Kopie der bereichsbezogenen Metadaten für die SAML-Anwendung für die benutzerdefinierte Workspace-URL abrufen.

1. Suchen Sie auf der Seite **Identitäts- und Zugriffsverwaltung** die SAML-Verbindung, wählen Sie die Auslassungspunkte und dann die Option **Anzeigen**.
2. Klicken Sie unter **SAML-Metadaten des DIenstanbieters für benutzerdefinierte Domäne** auf **Herunterladen**.

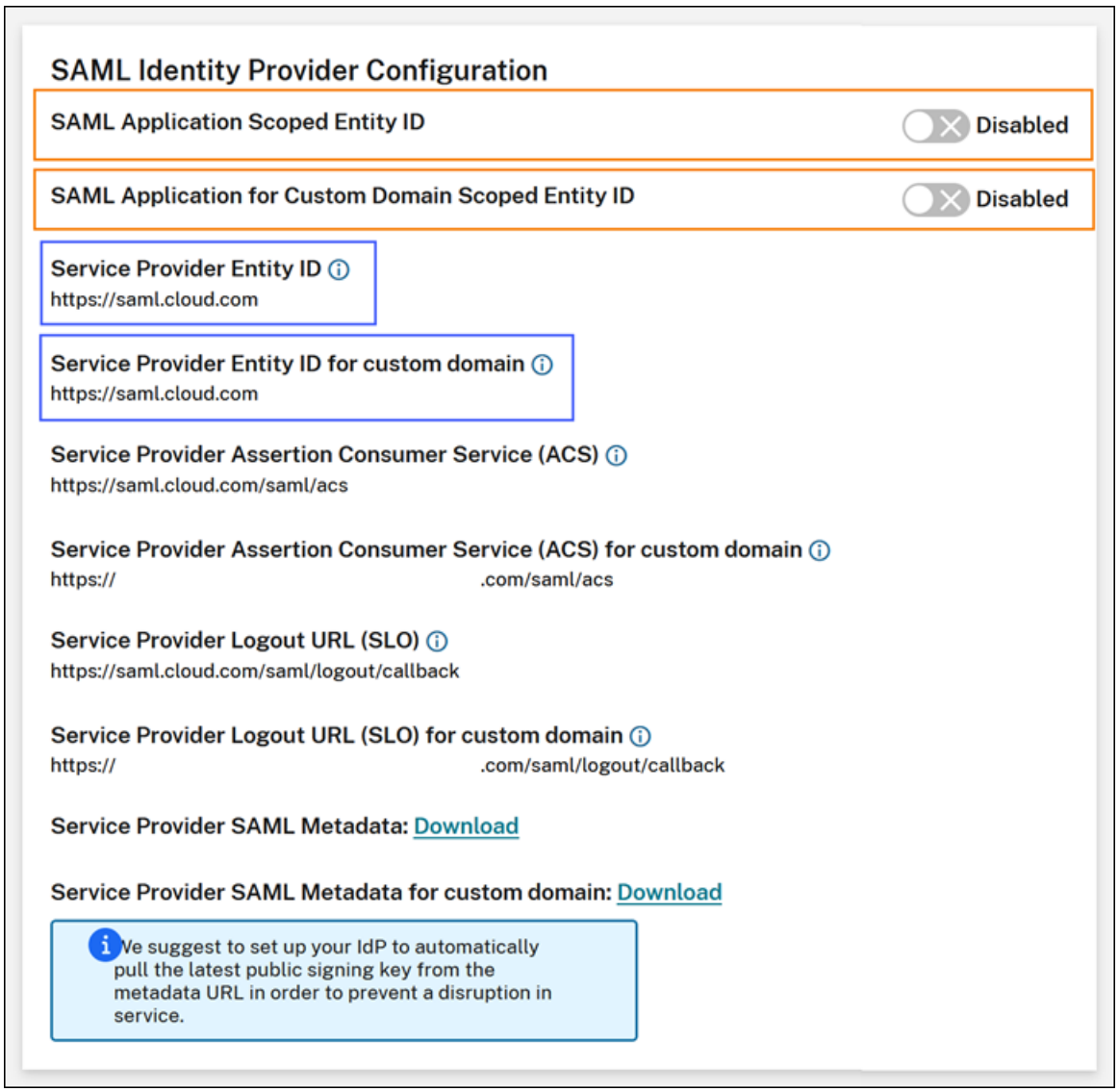
SAML-Konfiguration der primären SAML-Anwendung und der SAML-Anwendung für die benutzerdefinierte Workspace-URL anzeigen

Beim Anzeigen der Konfiguration für die bereichsbezogene SAML-Verbindung zeigt Citrix Cloud die Einstellungen der bereichsbezogenen Entitäts-ID für die primäre SAML-Anwendung und für die SAML-Anwendung für die benutzerdefinierte Workspace-Domäne an.

Wenn beispielsweise bereichsbezogene Entitäts-IDs aktiviert sind, enthalten die Felder **Entitäts-ID des Dienstanbieters** und **Entitäts-ID des Dienstanbieters für benutzerdefinierte Domäne** die von Citrix Cloud generierten bereichsbezogenen Entitäts-IDs.



Wenn bereichsbezogene Entitäts-IDs deaktiviert sind, enthalten die Felder **Entitäts-ID des Dienstanbieters** und **Entitäts-ID des Dienstanbieters für benutzerdefinierte Domäne** die generischen Entitäts-IDs.



Sie können vorhandene SAML-Anwendungen im SAML-Anbieter aktualisieren, indem Sie die bereichsbezogene Entitäts-ID an den vorhandenen Entitäts-ID-Wert anhängen.

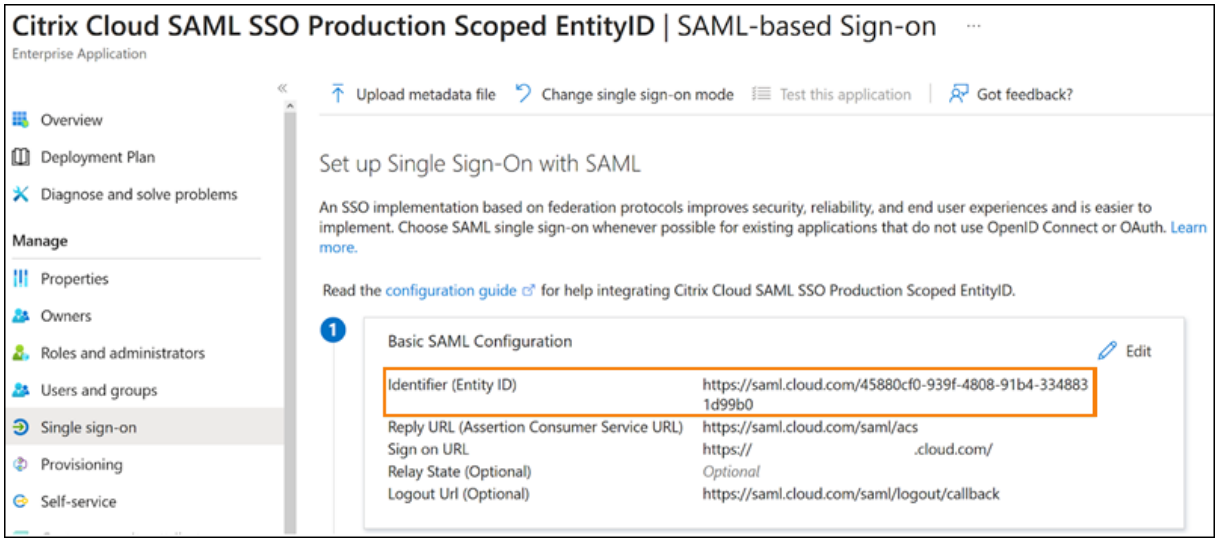
SAML-Anbieterkonfiguration mit bereichsbezogenen Entitäts-IDs

Wenn Sie die SAML-Verbindung in Citrix Cloud mit bereichsbezogenen Entitäts-IDs konfiguriert haben, können Sie die bereichsbezogene Entitäts-ID zu Ihrem SAML-Anbieter hinzufügen.

Dieser Abschnitt umfasst Konfigurationsbeispiele für Azure AD und PingFederate.

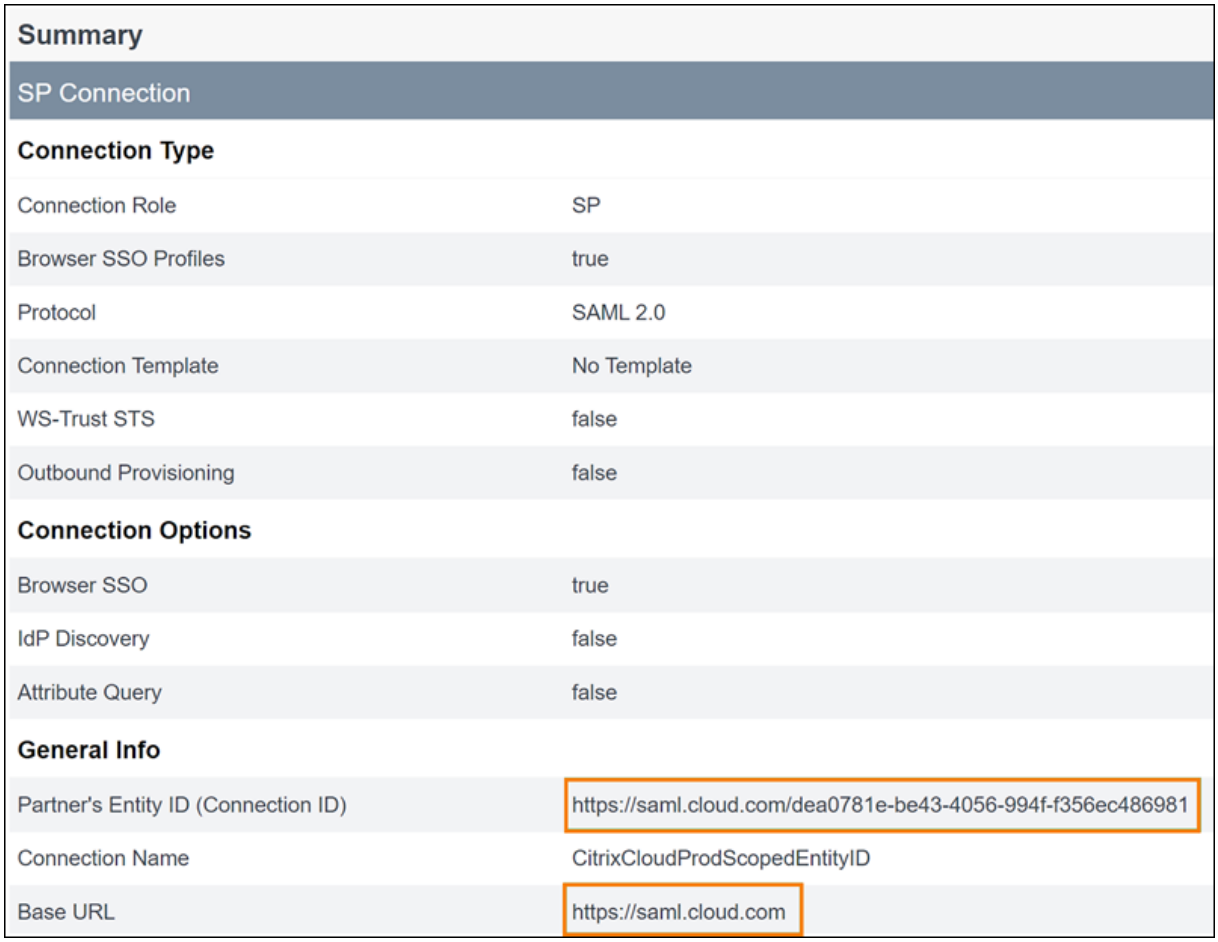
Azure AD-SAML-Konfiguration mit bereichsbezogener Entitäts-ID

In diesem Beispiel wird die bereichsbezogene Entitäts-ID aus Citrix Cloud in das Feld **Identifier** in Azure AD eingegeben.



PingFederate-SAML-Konfiguration mit bereichsbezogener Entitäts-ID

In diesem Beispiel entspricht die bereichsbezogene Entitäts-ID dem Feld **Partner's Entity ID** und die genrische Entitäts-ID aus Citrix Cloud dem Feld **Base URL**.



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com

Problembehandlung

Citrix empfiehlt, die Verwendung der Browsererweiterung SAML-tracer, um Probleme mit der SAML-Konfiguration zu beheben. Die Erweiterung decodiert Base64-Anforderungen und -Antworten nach SAML-XML und macht die Informationen für Menschen lesbar. Sie können mithilfe von SAML-tracer von Citrix Cloud (“Dienstanbieter”) generierte und an Ihren SAML-Anbieter (“Identitätsanbieter”) gesendete SSO- und SLO-SAML-Anforderungen untersuchen. Die Erweiterung kann anzeigen, ob der Entitäts-ID-Bereich (GUID) in beiden Anforderungen enthalten ist.

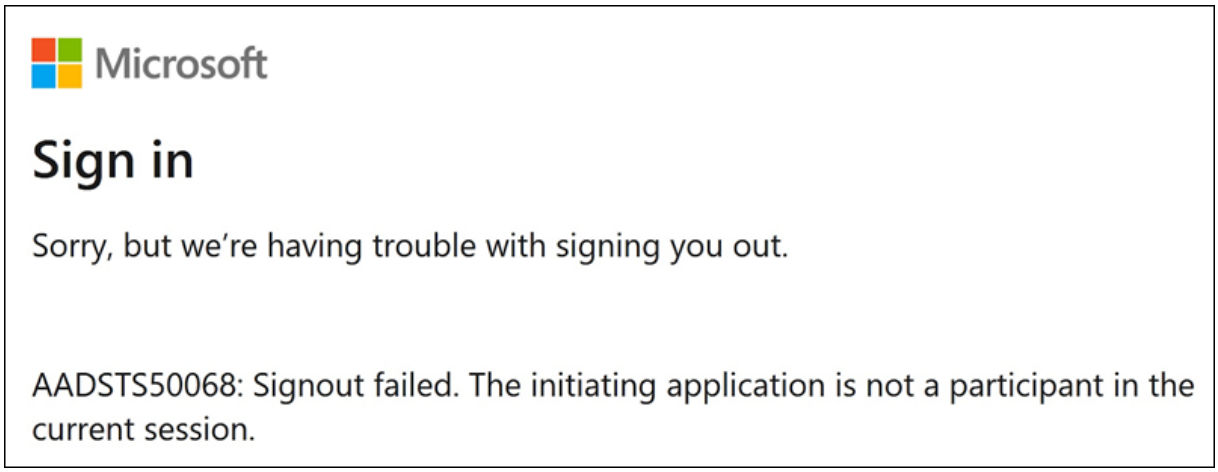
1. Installieren und aktivieren Sie SAML-tracer im Erweiterungsbereich Ihres Browsers.
2. Führen Sie eine SAML-Anmeldung und Abmeldung durch und erfassen Sie den gesamten Ablauf mit SAML-tracer.
3. Suchen Sie die folgende Zeile in der SAML-SSO-Anforderung oder der SLO-Anforderung.

```
1 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://saml.cloud.com/cfee4a86-97a8-49cf-9bb6-fd15ab075b92</
     saml:Issuer>
2 <!--NeedCopy-->
```


4. Vergewissern Sie sich, dass die Entitäts-ID mit der konfigurierten Entitäts-ID in Ihrer SAML-Anbieteranwendung übereinstimmt.
5. Vergewissern Sie sich, dass die bereichsbezogene Entitäts-ID im Feld **Issuer** vorhanden ist und dass sie in Ihrem SAML-Anbieter korrekt konfiguriert ist.
6. Exportieren und speichern Sie die SAML-tracer-JSON-Ausgabe. Wenn Sie zusammen mit dem Citrix Support ein Problem lösen, laden Sie die Ausgabe in Ihren Citrix Support Case hoch.

Azure AD-Problembehandlung

Problem: Das Abmelden von Azure AD schlägt fehl, wenn SLO konfiguriert ist. Azure AD zeigt dem Benutzer den folgenden Fehler an:



Wenn bereichsbezogene Entitäts-IDs für die SAML-Verbindung in Citrix Cloud aktiviert sind, muss die Entitäts-ID sowohl in den SSO- als auch in den SLO-Anforderungen gesendet werden.

Ursache: Die bereichsbezogene Entität ist konfiguriert, doch die Entitäts-ID fehlt in der SLO-Anforderung. Vergewissern Sie sich, dass die bereichsbezogene Entitäts-ID in der SLO-Anforderung in der SAML-tracer-Ausgabe vorhanden ist.

Problembehebung bei On-Premises-PingFederate

Problem: Das An- oder Abmelden bei PingFederate schlägt fehl, nachdem die Einstellung für bereichsbezogene Entitäts-IDs aktiviert wurde.

Ursache: Der PingFederate-Administrator hat die bereichsbezogene Entitäts-ID zur Basis-URL der SP-Verbindung hinzugefügt.

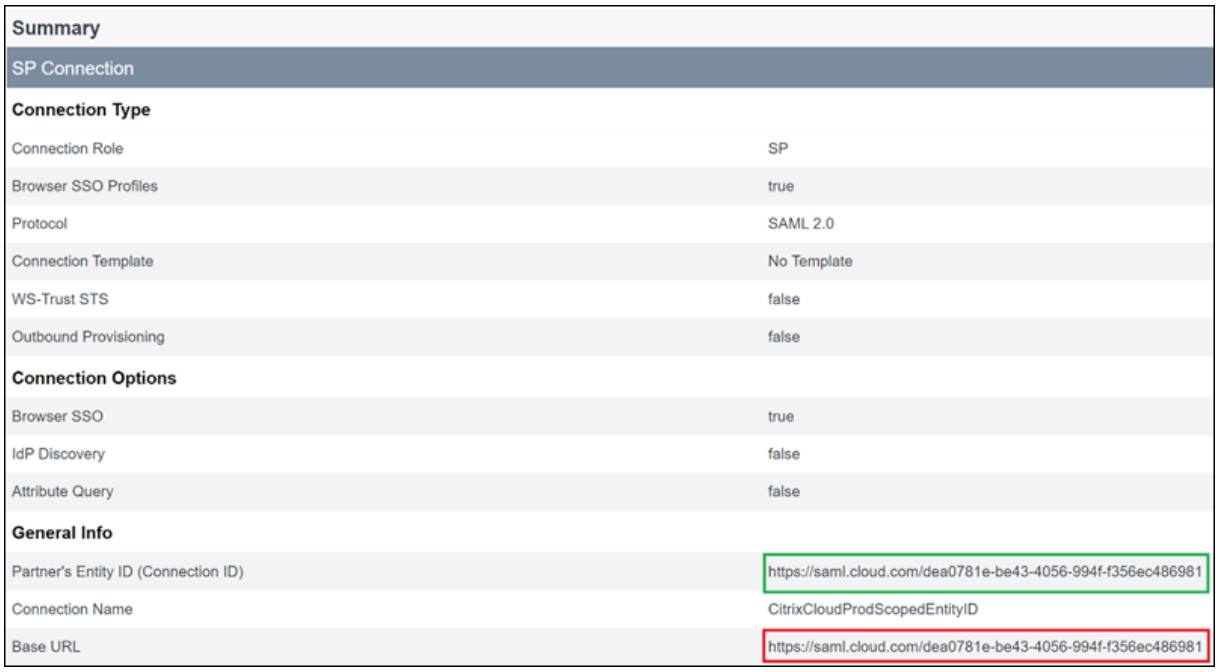
Fügen Sie zur Problembehebung die bereichsbezogene Entitäts-ID nur dem Feld **Partner's EntityID** hinzu. Das Hinzufügen der bereichsbezogenen Entitäts-ID zur Basis-URL führt zu einem fehlerhaften

SAML-Endpunkt. Wenn die Citrix Cloud-Basis-URL falsch aktualisiert wird, führen alle relativen SAML-Endpunkt-URLs, die von der Basis-URL abgeleitet werden, zu Anmeldefehlern.

Folgendes sind Beispiele für fehlerhafte Citrix Cloud-SAML-Endpunkte, die in der SAML-tracer-Ausgabe erscheinen können:

- `https://saml.cloud.com/<GUID>/saml/acs`
- `https://saml.cloud.com/<GUID>/saml/logout/callback`

Die folgende Abbildung zeigt eine falsch konfigurierte PingFederate-SAML-Anwendung. Das korrekt konfigurierte Feld ist grün gekennzeichnet. Das falsch konfigurierte Feld ist rot gekennzeichnet.



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981

SAML unter Verwendung von Azure AD- und AAD-Identitäten für die Workspace-Authentifizierung

March 12, 2024

Author:
Mark Dear

In diesem Artikel wird beschrieben, wie Sie SAML für die Workspace-Authentifizierung mit Azure AD-Identitäten anstelle von AD-Identitäten konfigurieren können. Verwenden Sie diese Konfiguration, wenn Azure AD-Benutzer Windows 365-Cloud-PC oder in Azure AD-Domänen eingebundene VDAs nicht anzeigen können, nachdem sie sich bei Citrix Workspace mit Standard-SAML-Verhalten

angemeldet haben. Nach Abschluss der Konfiguration können sich die Benutzer mit der SAML-Authentifizierung bei Citrix Workspace anmelden, um über Citrix DaaS auf HDX-Apps und -Desktops und über Azure auf Windows 365 Cloud-PC zuzugreifen.

Das Standardverhalten bei der Citrix Cloud- und SAML-Authentifizierung bei Citrix Workspace besteht in der Bestätigung einer AD-Benutzeridentität. Für die in diesem Artikel beschriebene Konfiguration ist die Verwendung von Azure AD Connect zum Importieren der AD-Identitäten in Azure AD erforderlich. Die AD-Identitäten enthalten die Benutzer-SIDs, die Citrix Workspace an Citrix DaaS senden kann und die die Anzeige und den Start der HDX-Ressourcen ermöglichen. Da die Azure AD-Version der Benutzeridentitäten verwendet wird, können die Benutzer auch Azure-Ressourcen wie Windows 365 Cloud-PC von Citrix Workspace aus anzeigen und starten.

> **Wichtig:**
>
> "Anzeigen"bezieht sich auf die Liste der Ressourcen, die Benutzer nach der Anmeldung bei Citrix Workspace anzeigen können. Auf welche Ressourcen ein Benutzer zugreifen darf, hängt von seiner Benutzeridentität und den ihr in Citrix DaaS zugeordneten Ressourcen ab. Es gibt einen zugehörigen Artikel, der Anweisungen zur Verwendung von Azure AD- und AD-Identitäten als SAML-Anbieter für die Authentifizierung bei Workspace enthält. Eine detaillierte Anleitung finden Sie unter SAML unter Verwendung von Azure AD- und AD-Identitäten für die Workspace-Authentifizierung

Featureumfang

Dieser Artikel bezieht sich auf Benutzer, die die folgende Kombination aus Citrix Cloud- und Azure-Features verwenden:

- SAML zur Workspace-Authentifizierung
- Citrix DaaS- und HDX-Anzeige von Ressourcen, die mit in AD-Domänen eingebundenen VDAs veröffentlicht wurden
- Ressourcenanzeige von in Azure AD-Domänen eingebundenen VDAs
- Ressourcenanzeige von in Azure Hybrid-Domänen eingebundenen VDAs
- W365 Cloud PC-Enumerierung und Start

> **Wichtig:**
>
> Verwenden Sie diesen AAD-SAML-Flow nicht für die SAML-Anmeldung bei Citrix Cloud, da der Citrix Cloud-Admin-Benutzer Mitglied einer AD-Gruppe sein muss und daher eine AD-Benutzeridentität obligatorisch ist. Eine detaillierte Anleitung finden Sie unter SAML unter Verwendung von Azure AD- und AD-Identitäten für die Workspace-Authentifizierung

Sind AD-Identitäten oder Azure AD-Identitäten vorzuziehen?

Zur Entscheidung darüber, ob Workspace-Benutzer sich mit SAML AD- oder SAML Azure AD-Identitäten authentifizieren sollen, gehen Sie folgendermaßen vor:

1. Überlegen Sie, welche Kombination von Ressourcen Sie den Benutzern in Citrix Workspace zur Verfügung stellen möchten.
2. Ermitteln Sie anhand der folgenden Tabelle, welcher Benutzeridentitätstyp für die jeweiligen Ressourcentypen geeignet ist.

Ressourcentyp (VDA)	Benutzeridentität bei der Anmeldung bei Citrix Workspace	SAML-Identität mit Azure AD erforderlich?	FAS bietet Single Sign-On für VDA?
AD-Einbindung	AD, Azure AD aus AD importiert (enthält SID)	Nein. Verwenden Sie Standard-SAML.	Ja
Hybrid-Einbindung	AD, Azure AD aus AD importiert (enthält SID)	Nein. Verwenden Sie Standard-SAML.	Ja, für AD als Identitätsanbieter. FAS ist nicht erforderlich, wenn Azure AD für den VDA ausgewählt ist.
In Azure AD eingebunden	Azure AD-Nativbenutzer, aus Azure AD importiert (enthält SID)	Ja, verwenden Sie SAML über Azure AD.	SSO funktioniert mit der modernen Azure AD-Authentifizierung. FAS ist nicht erforderlich.
Windows 365-Cloud-PC	Azure AD-Nativbenutzer, aus Azure AD importiert (enthält SID)	Ja, verwenden Sie SAML über Azure AD.	SSO funktioniert mit der modernen Azure AD-Authentifizierung. FAS ist nicht erforderlich.
AD-Einbindung, Azure AD-Einbindung, Windows 365 Cloud PC	Azure AD aus AD importiert (enthält SID)	Ja, verwenden Sie SAML über Azure AD.	Ja, für AD-Einbindung. Nein, für Azure AD-Einbindung und Windows 365 Cloud PC

Weitere Informationen

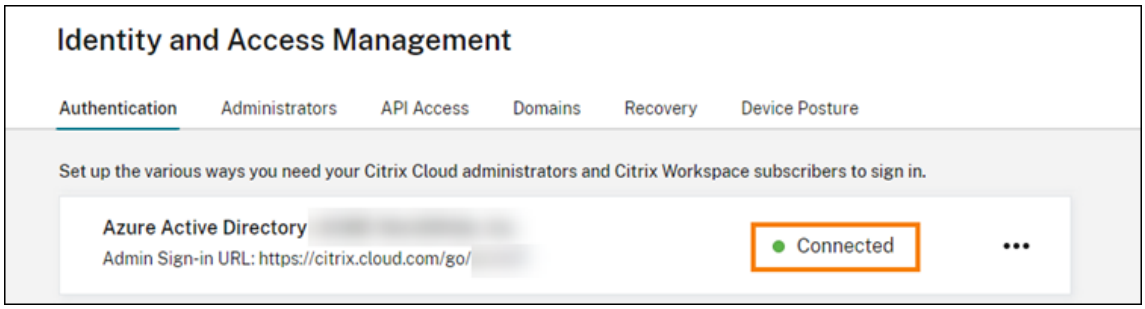
- Citrix DaaS-Dokumentation:

  - Maschinenidentitäten
  - Citrix HDX Plus für Windows 365

- Citrix FAS-Dokumentation: Installation und Konfiguration
- Microsoft Azure-Dokumentation: Was ist Azure AD Connect?

Anforderungen

- Der Azure AD-Mandant muss mit dem Citrix Cloud-Mandanten verbunden sein. In der Citrix Cloud-Konsole finden Sie Ihre Azure AD-Verbindung durch Auswahl von **Identitäts- und Zugriffsverwaltung > Authentifizierung**.



- Die Workspace-Authentifizierungsmethode muss auf **SAML 2.0** festgelegt sein. Verwenden Sie nicht Azure AD als Authentifizierungsmethode. Um die Workspace-Authentifizierungsmethode zu ändern, gehen Sie in der Citrix Cloud-Konsole zu **Workspace-Konfiguration > Authentifizierung**.
- Das UPN-Suffix `@yourdomain.com` muss importiert und in Azure AD als benutzerdefinierter Domänenname verifiziert werden. Im Azure-Portal befindet sich dies unter **Azure Active Directory > Benutzerdefinierte Domänennamen**.
- Azure AD-Benutzeridentitäten müssen mithilfe von Microsoft Azure AD Connect aus AD importiert werden. Dadurch wird sichergestellt, dass die Benutzeridentitäten einwandfrei importiert werden und das richtige UPN-Suffix haben. Azure AD-Benutzer mit UPN-Suffix `@yourtenant.onmicrosoft.com` werden nicht unterstützt.
- Citrix FAS muss bereitgestellt und mit dem Citrix Cloud-Mandanten und dem Ressourcenstandort verbunden sein. FAS bietet Single Sign-On für HDX-Desktops und -Anwendungen, die von Citrix Workspace aus gestartet werden. Sie müssen keine AD-Schattenkonten konfigurieren, da der UPN `user@customerdomain` für die AD- und die Azure AD-Benutzeridentität identisch sein muss. FAS generiert die erforderlichen Benutzerzertifikate mit dem richtigen UPN und führt eine Smartcard-Anmeldung durch, wenn HDX-Ressourcen gestartet werden.

Benutzerdefinierte Azure AD Enterprise SAML-Anwendung konfigurieren

Standardmäßig erfolgt die SAML-Anmeldung bei Workspaces anhand der Bestätigung einer AD-Benutzeridentität. Das SAML-Attribut **cip_directory** ist ein hartcodierter Zeichenkettenwert, der für alle Abonnenten gleich ist und als Switch fungiert. Citrix Cloud und Citrix Workspace ermitteln dieses Attribut bei der Anmeldung und lösen die SAML-Assertion der Azure AD-Version der Benutzeridentität aus. Die Verwendung des Parameters **azuread** mit diesem Attribut setzt das Standard-SAML-Verhalten außer Kraft und löst stattdessen die Verwendung von SAML in Azure AD aus.

Die Schritte in diesem Abschnitt beziehen sich zwar auf Azure AD, Sie können jedoch eine ähnliche SAML-Anwendung mit einem anderen SAML 2.0-Anbieter (z. B. ADFS, Duo, Okta, OneLogin, PingOneSSO) erstellen, vorausgesetzt Sie führen dieselben Aufgaben aus. Der verwendete SAML-Anbieter muss das Konfigurieren eines fest codierten SAML-Attributs (cip_directory = azuread) innerhalb der SAML-Anwendung ermöglichen. Erstellen Sie einfach dieselben SAML-Attributzuordnungen wie in diesem Abschnitt beschrieben.

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie im Portalmenü **Azure Active Directory**.
3. Wählen Sie im linken Bereich unter **Verwalten** die Option **Unternehmensanwendungen**.
4. Wählen Sie in der Befehlsleiste im Arbeitsbereich **Neue Anwendung**.
5. Wählen Sie in der Befehlsleiste **Eigene Anwendung erstellen**. Verwenden Sie nicht die Citrix Cloud SAML SSO-Unternehmensanwendungsvorlage. Die Vorlage gestattet keine Änderungen an der Liste der Ansprüche und SAML-Attribute.
6. Geben Sie einen Namen für die Anwendung ein und wählen Sie dann **Beliebige andere, nicht im Katalog gefundene Anwendung integrieren**. Klicken Sie auf **Erstellen**. Die Anwendungsübersicht wird angezeigt.
7. Wählen Sie links **Single Sign-On**. Wählen Sie im Arbeitsbereich **SAML**.
8. Wählen Sie im Abschnitt **Grundlegende SAML-Konfiguration** die Option **Bearbeiten** und konfigurieren Sie die folgenden Einstellungen:

    a) Wählen Sie im Abschnitt **Bezeichner (Entitäts-ID)** die Option **Bezeichner hinzufügen** und geben Sie dann den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:

    - Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com` ein.
    - Geben Sie für die Region Japan `https://saml.citrixcloud.jp` ein.
    - Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us` ein.

b) Wählen Sie im Abschnitt **Antwort-URL (Assertionsverbraucherdienst-URL)** die Option **Antwort-URL hinzufügen** und geben Sie dann den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:

- Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com/saml/acs` ein.
- Geben Sie für die Region Japan `https://saml.citrixcloud.jp/saml/acs` ein.
- Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us/saml/acs` ein.

c) Geben Sie im Abschnitt **Abmelde-URL** (optional) den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:

- Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com/saml/logout/callback` ein.
- Geben Sie für die Region Japan `https://saml.citrixcloud.jp/saml/logout/callback` ein.
- Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us/saml/logout/callback` ein.

d) Wählen Sie in der Befehlsleiste **Speichern**.

9. Wählen Sie im Abschnitt **Attribute und Ansprüche** die Option **Bearbeiten**, um die folgenden Ansprüche zu konfigurieren. Diese Ansprüche erscheinen in der SAML-Assertion der SAML-Antwort.

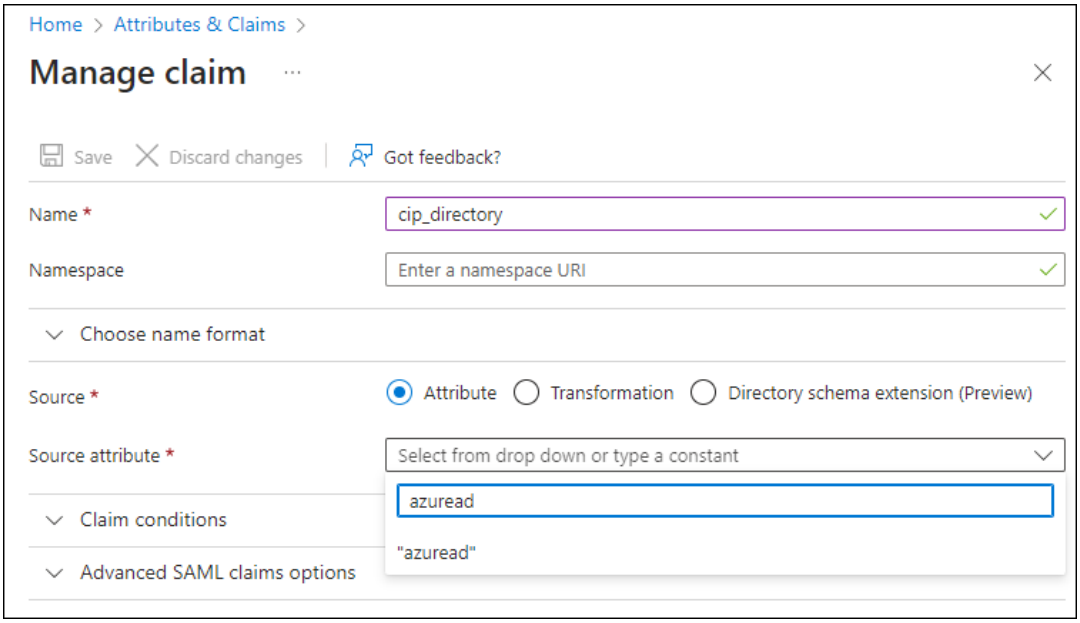
a) Übernehmen Sie für den Anspruch **Eindeutiger Benutzerbezeichner (Namens-ID)** den Standardwert `user.userprincipalname`.

b) Wählen Sie in der Befehlsleiste **Neuen Anspruch hinzufügen**.

c) Geben Sie im Feld **Name** den Namen **cip_directory** ein.

d) Übernehmen Sie unter **Quelle** die Auswahl **Attribut**.

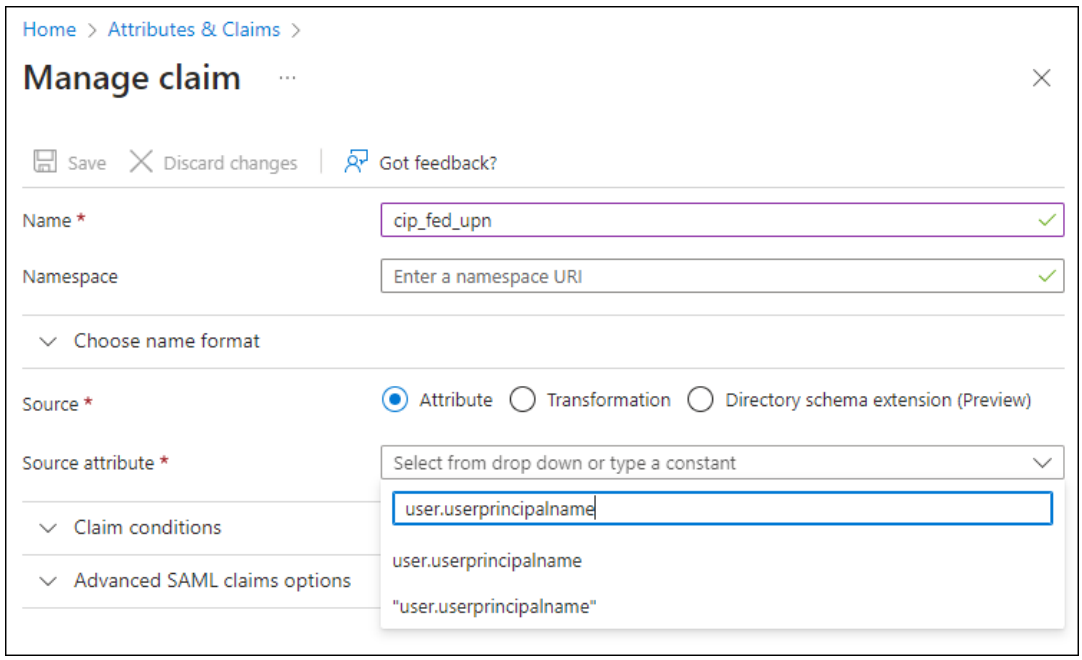
e) Geben Sie im Feld **Quellattribut** den Wert **azuread** ein. Der Wert wird nach der Eingabe in Anführungszeichen angezeigt.



f) Wählen Sie in der Befehlsleiste **Speichern**.

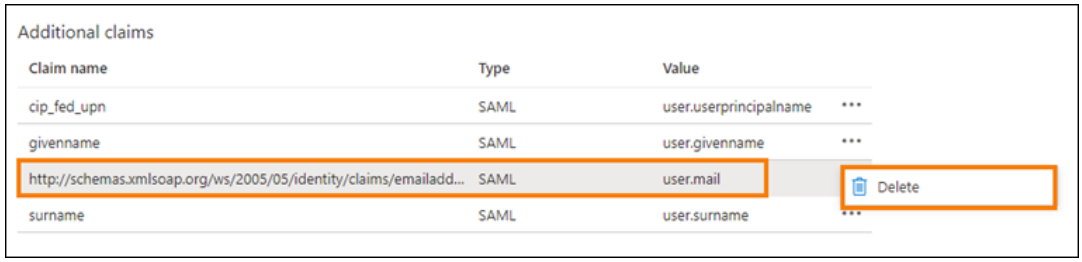
g) Erstellen Sie weitere Ansprüche mit den folgenden Werten in den Feldern **Name** und **Quellattribut**:

Name	Quellattribut
cip_fed_upn	user.userprincipalname
displayName	user.displayname
firstName	user.givenname
lastName	user.surname

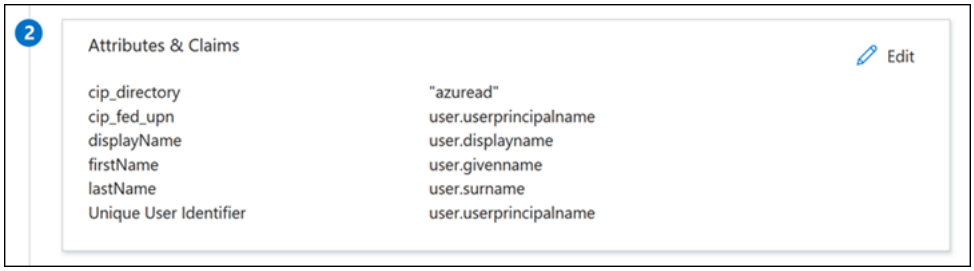


> **Wichtig:**
>
> Sie können diese zusätzlichen Ansprüche erstellen, indem Sie entweder die Schritte b bis f jeweils wiederholen oder indem Sie die Standardansprüche im Abschnitt **Zusätzliche Ansprüche** ändern, die bereits die in der Tabelle oben aufgeführten Quellattribute besitzen. Die Standardansprüche umfassen den Namespace `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`.
>
> Wenn Sie die Standardansprüche ändern, müssen Sie den Namespace aus jedem Anspruch entfernen. Wenn Sie neue Ansprüche erstellen, müssen Sie die Ansprüche löschen, die den Namespace enthalten. Enthält die resultierende SAML-Assertion Ansprüche mit dem Namespace, ist sie ungültig und enthält falsche SAML-Attributnamen.

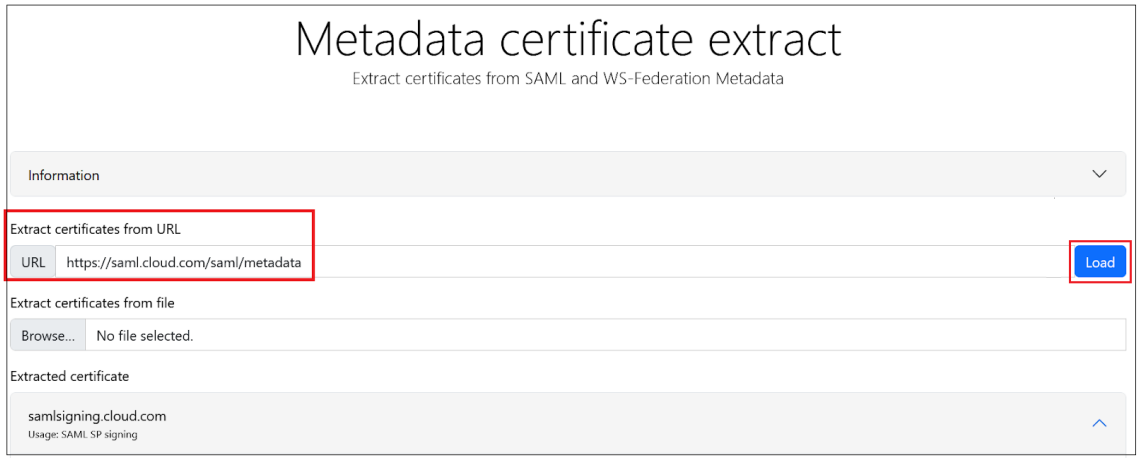
h) Klicken Sie im Abschnitt **Zusätzliche Ansprüche** für alle verbleibenden Ansprüche mit dem Namespace `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` auf das Menü (…) und dann auf **Löschen**.



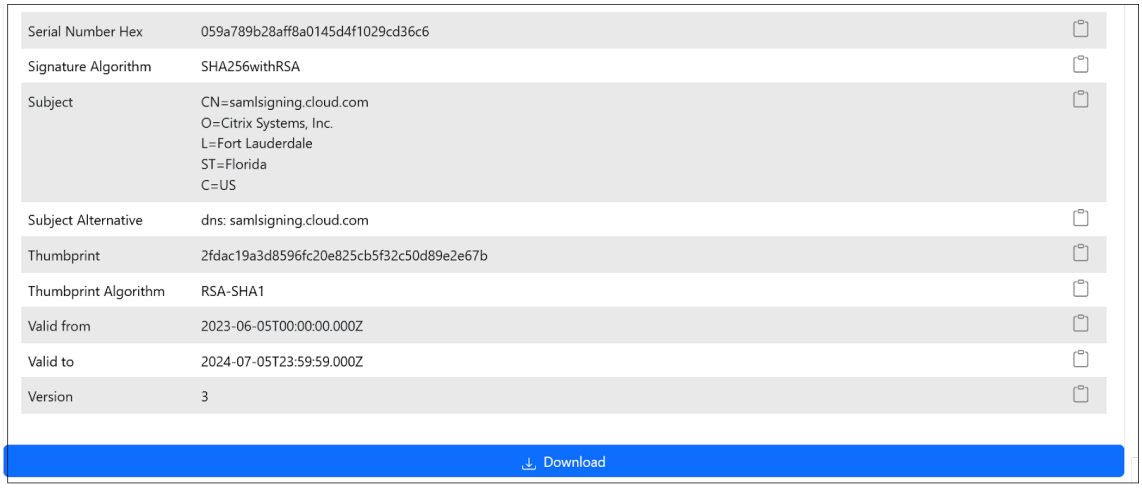
Wenn Sie fertig sind, wird der Abschnitt **Attribute und Ansprüche** wie unten dargestellt angezeigt:

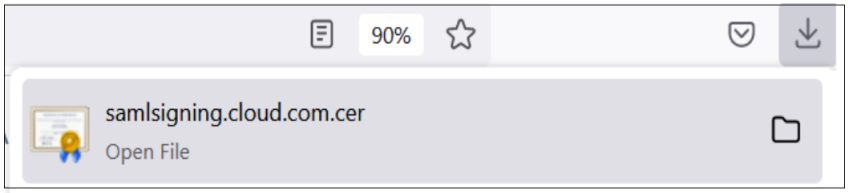


10. Besorgen Sie sich mit diesem Online-Tool eines Drittanbieters eine Kopie des Citrix Cloud SAML-Signaturzertifikats.
11. Geben Sie https://saml.cloud.com/saml/metadata in das URL-Feld ein und klicken Sie auf **Laden**.



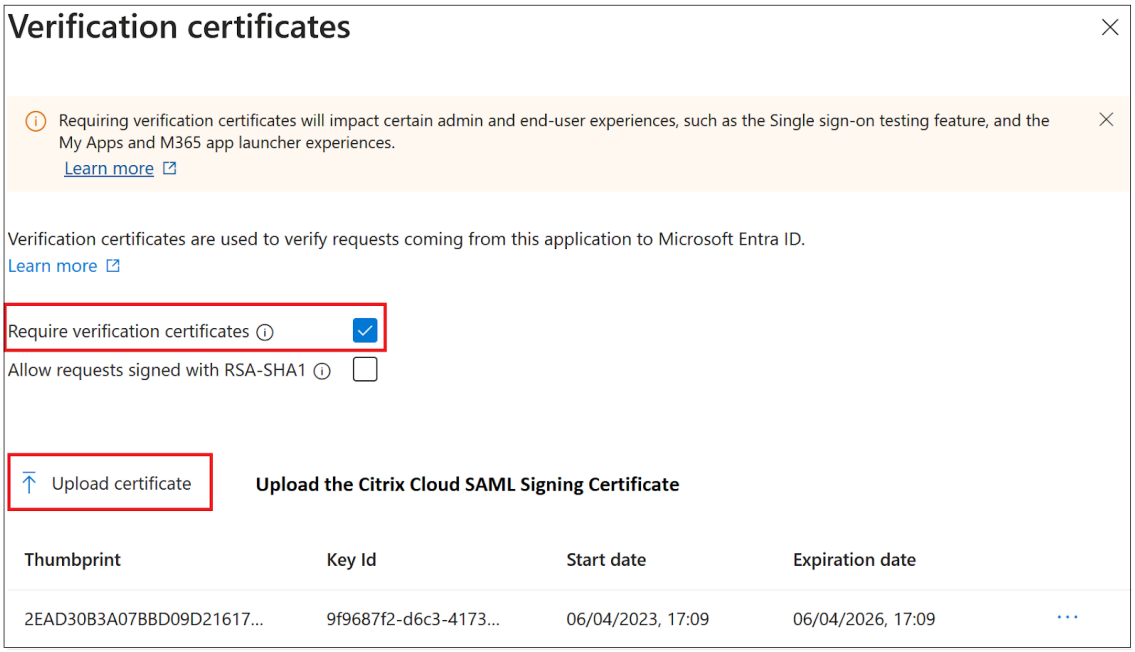
12. Scrollen Sie zum Ende der Seite und klicken Sie auf **Download**.

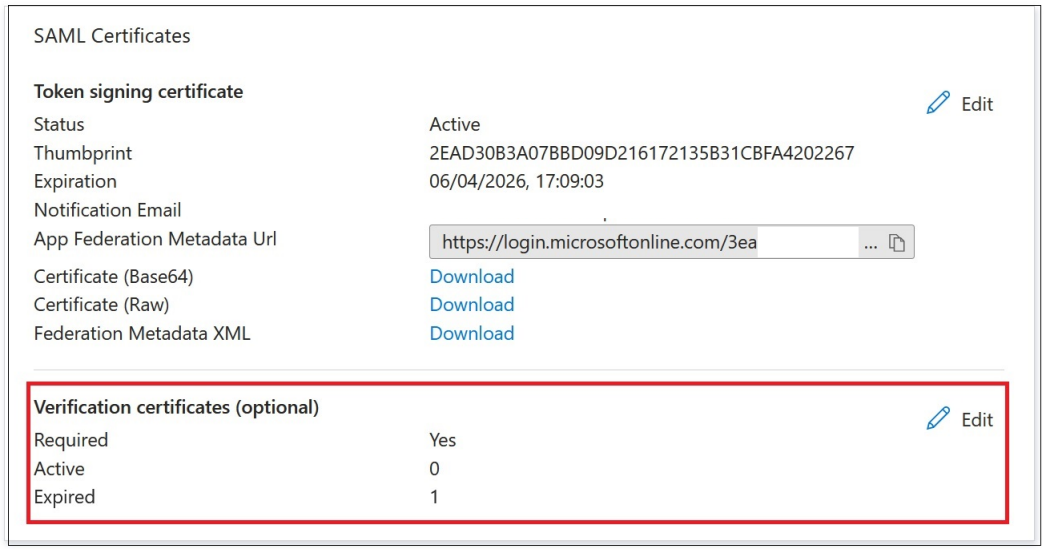




13. Konfigurieren Sie die Signatureinstellungen der Azure Active Directory-SAML-Anwendung.
14. Laden Sie das in Schritt 10 erhaltene SAML-Signaturzertifikat für die Produktion in die SAML-Anwendung von Azure Active Directory hoch.

    - Aktivieren Sie die Option **Verifizierungszertifikate erforderlich**.





Problembehandlung

1. Stellen Sie mithilfe eines SAML-Netzwerktools wie der Browsererweiterung SAML-tracer sicher, dass die SAML-Assertions die richtigen Benutzerattribute enthalten.

2. Suchen Sie die gelb dargestellte SAML-Antwort und vergleichen Sie sie mit diesem Beispiel:

3. Klicken Sie im unteren Bereich auf die Registerkarte **SAML**, um die SAML-Antwort zu decodieren und als XML anzuzeigen.

4. Scrollen Sie zum Ende der Antwort und überprüfen Sie, ob die SAML-Assertion die richtigen SAML-Attribute und Benutzerwerte enthält.

Wenn sich Ihre Abonnenten immer noch nicht in ihrem Workspace anmelden können, wenden Sie sich an den Citrix Support und geben Sie die folgenden Informationen an:

- SAML-tracer-Aufzeichnung
- Datum und Uhrzeit der fehlgeschlagenen Anmeldung bei Citrix Workspace
- Betroffener Benutzername
- Aufrufer-IP-Adresse des Clientcomputers, der für die Anmeldung bei Citrix Workspace verwendet wurde. Sie die IP-Adresse mithilfe eines Tools wie https://whatismyip.com ermitteln.

SAML unter Verwendung von Azure AD- und AD-Identitäten für die Workspace-Authentifizierung

May 31, 2024

Author:
Mark Dear

In diesem Artikel wird beschrieben, wie Sie SAML für die Workspace-Authentifizierung mit AD-Identitäten konfigurieren können. Das Standardverhalten bei der Citrix Cloud- und SAML-Authentifizierung bei Citrix Workspace oder Citrix Cloud besteht unabhängig vom verwendeten SAML-Anbieter in der Bestätigung einer AD-Benutzeridentität. Für die in diesem Artikel beschriebene Konfiguration ist die Verwendung von Azure AD Connect zum Importieren der AD-Identitäten in Azure AD erforderlich.

> **Wichtig:**
>
> Es ist wichtig, den geeigneten SAML-Flow für Ihre Workspace-Endbenutzer zu ermitteln, da er sich direkt auf ihren Anmeldevorgang und die Sichtbarkeit der Ressourcen auswirkt. Die gewählte Identität beeinflusst die Arten von Ressourcen, auf die ein Workspace-Endbenutzer zugreifen kann.
> Es gibt einen diesbezüglichen Artikel, der Anweisungen zur Verwendung von Azure AD-Identitäten als SAML-Anbieter für die Authentifizierung bei Workspace mit AAD-Identitäten enthält. Eine detaillierte Anleitung finden Sie unter SAML unter Verwendung von Azure AD- und AAD-Identitäten für die Workspace-Authentifizierung.
> In der Regel müssen Workspace-Endbenutzer Apps und Desktops öffnen, die von in die AD-Domäne eingebundenen VDAs bereitgestellt werden. Es ist wichtig, die in beiden Artikeln beschriebenen Anwendungsfälle sorgfältig zu prüfen, bevor Sie sich für den für Ihr Unternehmen am besten geeigneten SAML-Flow entscheiden. Wenn Sie sich nicht sicher sind, empfiehlt Citrix, den **AD SAML-Flow** zu verwenden und die Anweisungen in diesem Artikel zu befolgen, da dies dem gängigsten DaaS-Szenario entspricht.

Featureumfang

Dieser Artikel bezieht sich auf Benutzer, die die folgende Kombination aus Citrix Cloud- und Azure-Features verwenden:

- SAML für Workspace-Authentifizierung mit AD-Identitäten
- SAML für Citrix Cloud-Administratoranmeldung mit AD-Identitäten
- Citrix DaaS- und HDX-Anzeige von Ressourcen, die mit in AD-Domänen eingebundenen VDAs veröffentlicht wurden
- Ressourcenenumerierung von in AD-Domänen eingebundenen VDAs

Sind AD-Identitäten oder Azure AD-Identitäten vorzuziehen?

Zur Entscheidung darüber, ob Workspace-Benutzer sich mit SAML AD- oder SAML Azure AD-Identitäten authentifizieren sollen, gehen Sie folgendermaßen vor:

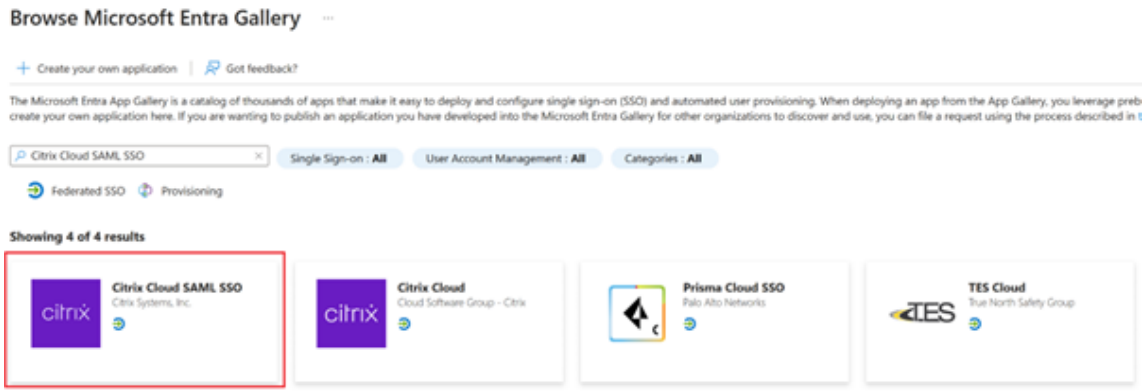
1. Überlegen Sie, welche Kombination von Ressourcen Sie den Benutzern in Citrix Workspace zur Verfügung stellen möchten.
2. Ermitteln Sie anhand der folgenden Tabelle, welcher Benutzeridentitätstyp für die jeweiligen Ressourcentypen geeignet ist.

Ressourcentyp (VDA)	Benutzeridentität bei der Anmeldung bei Citrix Workspace	SAML-Identität mit Azure AD erforderlich?	FAS bietet Single Sign-On für VDA?
AD-Einbindung	AD, Azure AD aus AD importiert (enthält SID)	Nein. Verwenden Sie Standard-SAML.	Ja

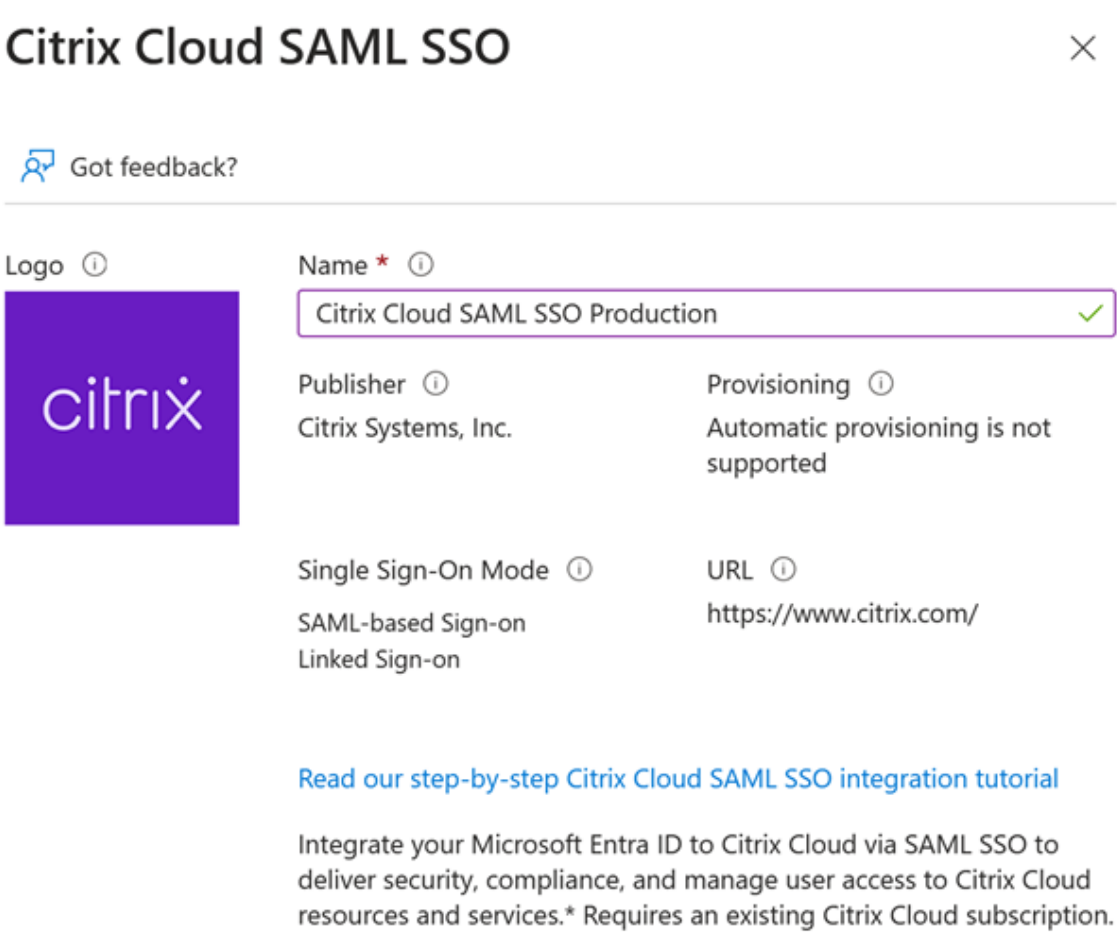
Benutzerdefinierte Azure AD Enterprise SAML-Anwendung konfigurieren

Standardmäßig erfolgt die SAML-Anmeldung bei Workspaces anhand der Bestätigung einer AD-Benutzeridentität.

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie im Portalmenü **Azure Active Directory**.
3. Wählen Sie im linken Bereich unter **Verwalten** die Option **Unternehmensanwendungen**.
4. Geben Sie `Citrix Cloud SAML SSO` in das Suchfeld ein, um die Citrix SAML-Anwendungsvorlage zu suchen.



5. Geben Sie einen geeigneten Namen für die SAML-Anwendung ein, z. B. `Citrix Cloud SAML SSO Production`



6. Wählen Sie im linken Navigationsbereich **Single Sign-On** aus und klicken Sie im Arbeitsbereich auf **SAML**.
7. Klicken Sie im Abschnitt **Grundlegende SAML-Konfiguration** auf die Option **Bearbeiten** und konfigurieren Sie die folgenden Einstellungen:

   a) Wählen Sie im Abschnitt **Bezeichner (Entitäts-ID)** die Option **Bezeichner hinzufügen** und geben Sie dann den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:
      - Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com` ein.
      - Geben Sie für die Region Japan `https://saml.citrixcloud.jp` ein.
      - Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us` ein.

   b) Wählen Sie im Abschnitt **Antwort-URL (Assertionsverbraucherdienst-URL)** die Option **Antwort-URL hinzufügen** und geben Sie dann den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:
      - Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com/saml/acs` ein.
      - Geben Sie für die Region Japan `https://saml.citrixcloud.jp/saml/acs`

ein.

- Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us/saml/acs` ein.

c) Geben Sie im Abschnitt **Anmelde-URL** Ihre Workspace-URL ein.

d) Geben Sie im Abschnitt **Abmelde-URL** (optional) den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:

- Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com/saml/logout/callback` ein.
- Geben Sie für die Region Japan `https://saml.citrixcloud.jp/saml/logout/callback` ein.
- Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us/saml/logout/callback` ein.

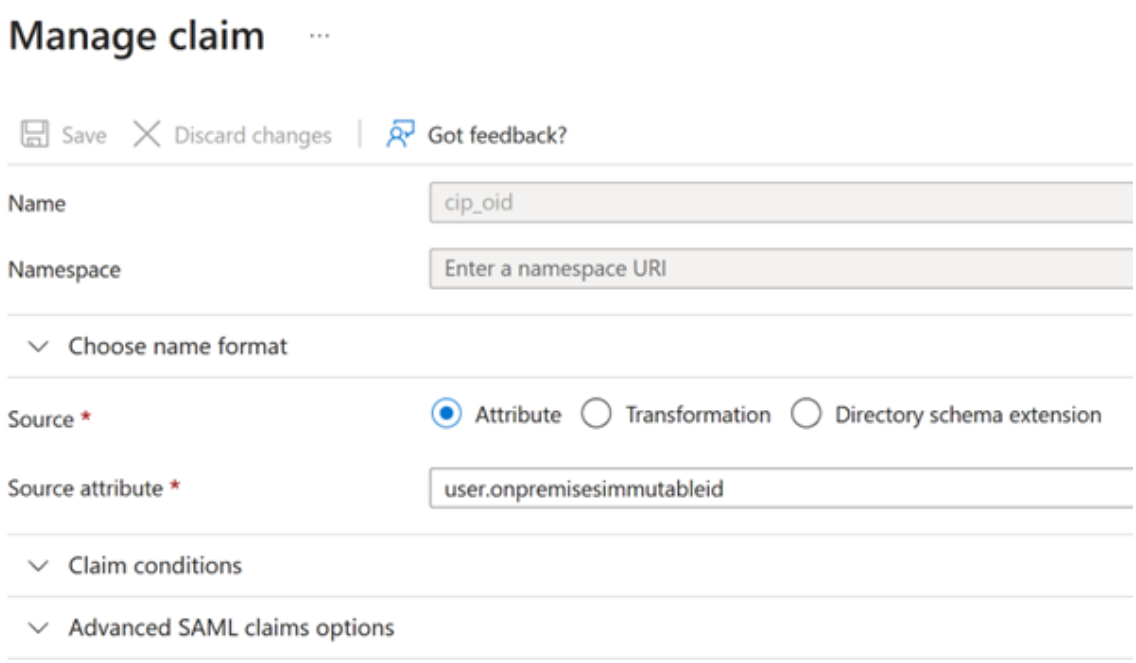
e) Klicken Sie in der Befehlsleiste auf **Speichern**. Der Abschnitt **Grundlegende SAML-Konfiguration** sieht wie folgt aus:

8. Wählen Sie im Abschnitt **Attribute und Ansprüche** die Option **Bearbeiten**, um die folgenden Ansprüche zu konfigurieren. Diese Ansprüche erscheinen in der SAML-Assertion der SAML-Antwort. Konfigurieren Sie nach der Erstellung der SAML-App die folgenden Attribute.

a) Übernehmen Sie für den Anspruch **Eindeutiger Benutzerbezeichner (Namens-ID)** den Standardwert `user.userprincipalname`.

b) Lassen Sie für den Anspruch **cip_upn** den Standardwert `user.userprincipalname`.

c) Lassen Sie für den Anspruch **cip_email** den Standardwert `user.mail`.
d) Lassen Sie für den Anspruch **cip_sid** den Standardwert `user.onpremisesecurityidentitier` .
e) Für den Anspruch **cip_oid** bearbeiten Sie den vorhandenen Anspruch und wählen Sie **Quellattribut** aus. Suchen Sie nach der Zeichenfolge `object` und wählen Sie `user.onpremisesimmutableid` aus.

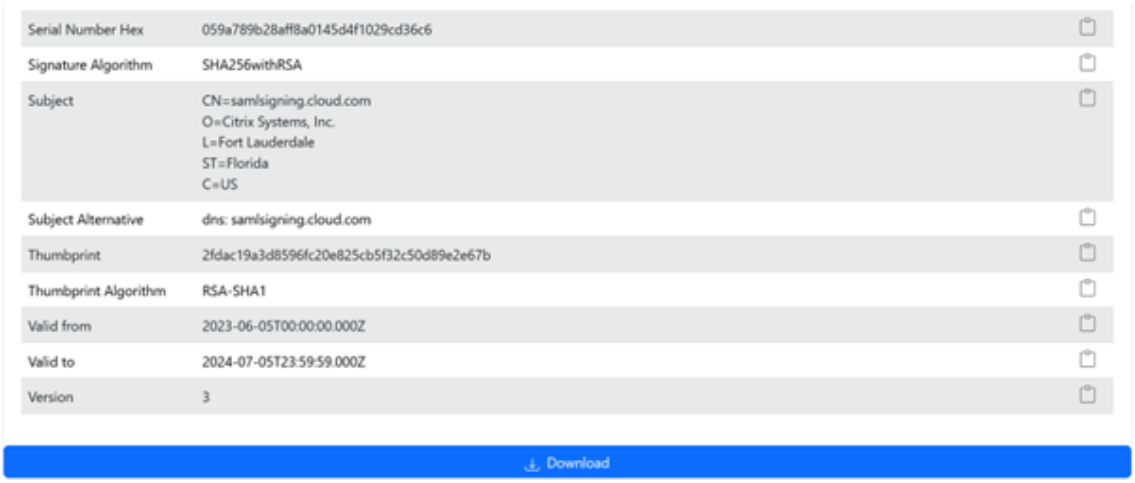


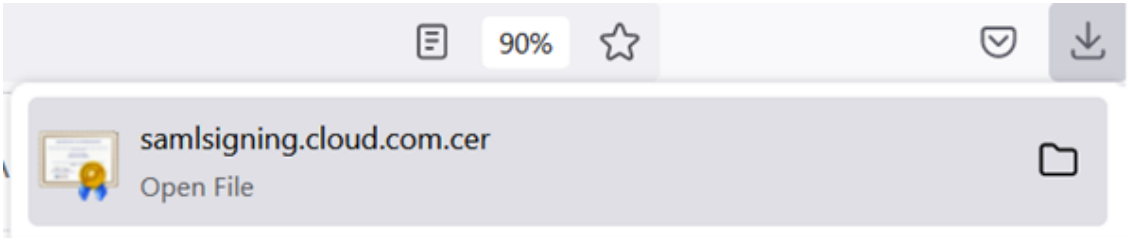
a) Lassen Sie für **displayName** den Standardwert `user.displayname`.
b) Klicken Sie im Abschnitt **Zusätzliche Ansprüche** für alle verbleibenden Ansprüche mit dem Namespace `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` auf das Menü (...) und dann auf **Löschen**. Diese Ansprüche müssen nicht aufgenommen werden, da es sich um Duplikate der oben genannten Benutzerattribute handelt.

Wenn Sie fertig sind, wird der Abschnitt **Attribute und Ansprüche** wie unten dargestellt angezeigt:

a) Besorgen Sie sich mit diesem Online-Tool eines Drittanbieters eine Kopie des Citrix Cloud SAML-Signaturzertifikats.
b) Geben Sie `https://saml.cloud.com/saml/metadata` in das URL-Feld ein und klicken Sie auf **Laden**.

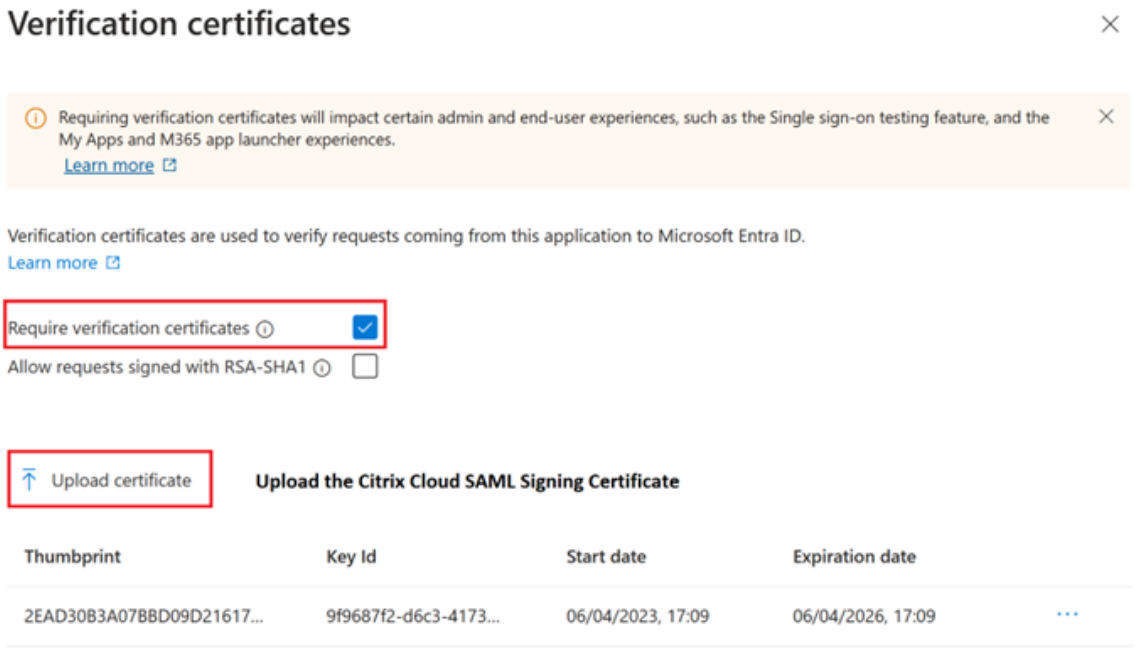
9. Scrollen Sie zum Ende der Seite und klicken Sie auf **Download**.

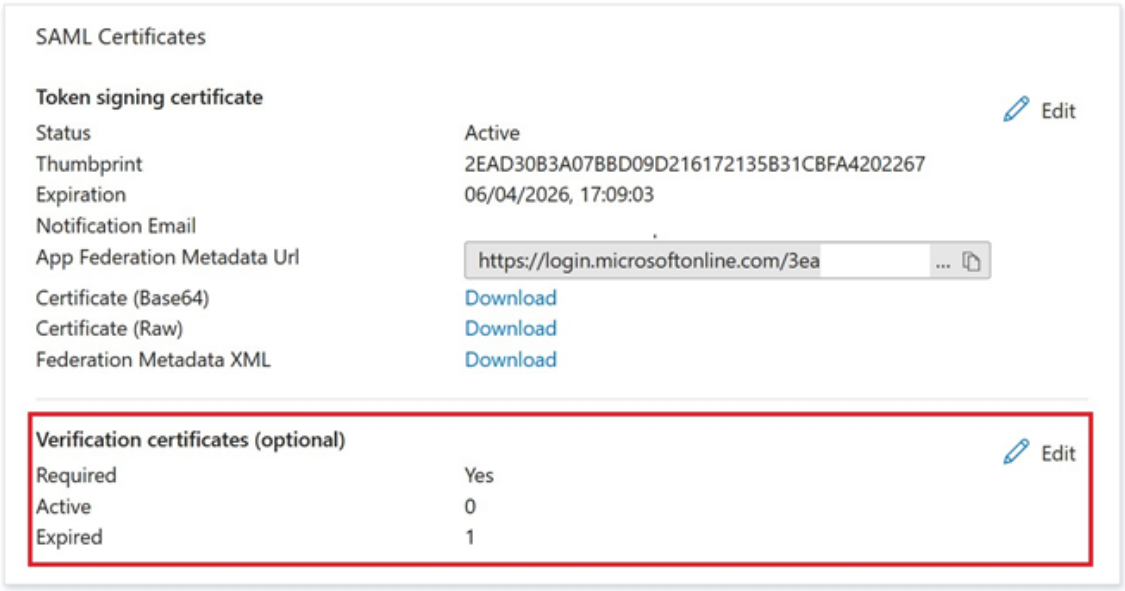




10. Konfigurieren Sie die Signatureinstellungen der Azure Active Directory-SAML-Anwendung.
11. Laden Sie das in Schritt 10 erhaltene SAML-Signaturzertifikat für die Produktion in die SAML-Anwendung von Azure Active Directory hoch

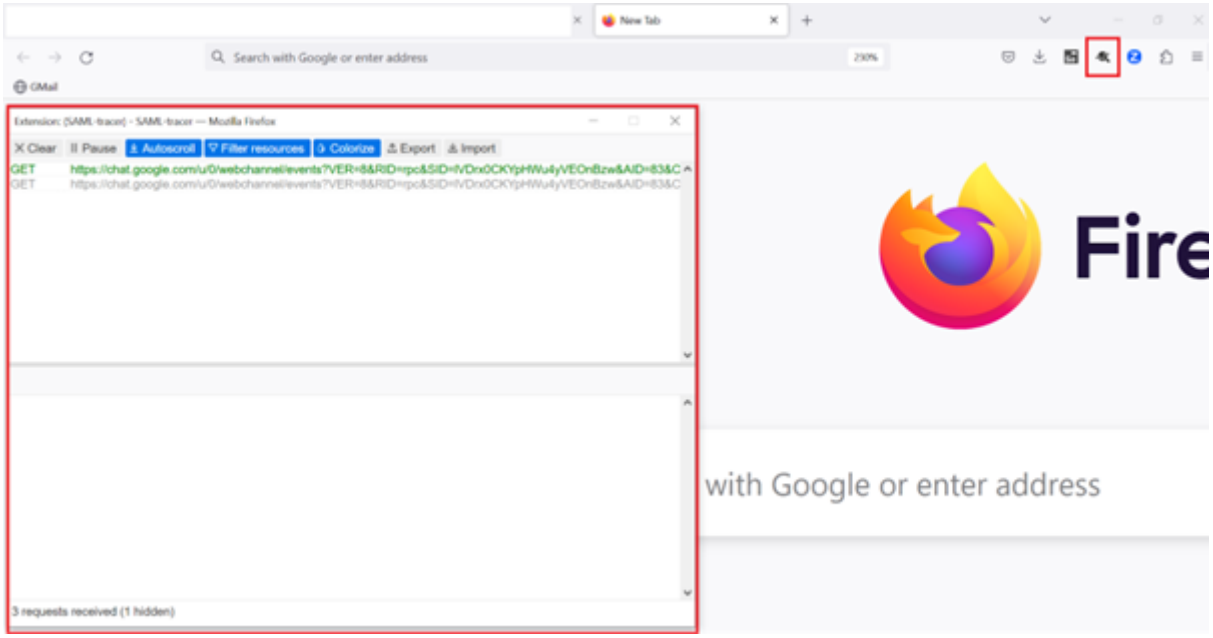
    a) Aktivieren Sie die Option **Verifizierungszertifikate erforderlich**.





Problembehandlung

1. Stellen Sie mithilfe eines SAML-Netzwerktools wie der Browsererweiterung SAML-tracer sicher, dass die SAML-Assertions die richtigen Benutzerattribute enthalten.



1. Suchen Sie die gelb dargestellte SAML-Antwort und vergleichen Sie sie mit diesem Beispiel:

2. Klicken Sie im unteren Bereich auf die Registerkarte **SAML**, um die SAML-Antwort zu decodieren und als XML anzuzeigen.
3. Scrollen Sie zum Ende der Antwort und überprüfen Sie, ob die SAML-Assertion die richtigen SAML-Attribute und Benutzerwerte enthält.

Können sich die Abonnenten weiterhin nicht bei ihrem Workspace anmelden oder ihre Citrix HDX Plus für Windows 365-Desktops anzeigen, wenden Sie sich mit folgenden Informationen an den Citrix Support:

- SAML-tracer-Aufzeichnung
- Datum und Uhrzeit der fehlgeschlagenen Anmeldung bei Citrix Workspace
- Betroffener Benutzername
- Aufrufer-IP-Adresse des Clientcomputers, der für die Anmeldung bei Citrix Workspace verwendet wurde. Sie die IP-Adresse mithilfe eines Tools wie https://whatismyip.com ermitteln.

Konfigurieren von vereinfachtem SAML für die Verwendung mit nativen und Gast-SAML-Benutzern

July 3, 2024

Author:
Mark Dear, Javier Lopez Santacruz

Bevor Sie die Schritte in diesem Artikel befolgen, sollten Sie sich unbedingt vergewissern, ob "vereinfachtes SAML"für Ihren Anwendungsfall bei der Authentifizierung geeignet ist. Lesen Sie die Anwendungsfallbeschreibungen und häufig gestellten Fragen gründlich durch, bevor Sie sich für die Implementierung dieser speziellen SAML-Lösung für Sonderfälle entscheiden. Bevor Sie fortfahren, stellen Sie sicher, dass Sie die Szenarien, in denen vereinfachtes SAML angemessen ist, vollständig verstanden haben und wissen, welche Arten von Identitäten Sie verwenden müssen. Die meisten SAML-Anwendungsfälle können erreicht werden, indem Sie andere SAML-Artikel befolgen und alle vier cip_*-Attribute zur Authentifizierung senden.

> **Hinweis:**
>
> Die Verwendung von "vereinfachtem SAML"erhöht die Belastung der Citrix Cloud Connectors, da sie die Benutzer-E-Mail, SID und OID für jede Workspace-Endbenutzeranmeldung nachschlagen müssen, statt dass diese Werte von der SAML-Assertion bereitgestellt werden. Das Senden aller vier cip_*-Attribute in der SAML-Assertion ist aus Sicht der Citrix Cloud Connector-Leistung vorzuziehen, wenn vereinfachtes SAML nicht tatsächlich erforderlich ist.

Voraussetzungen

- Eine SAML-Anwendung, die speziell für die Verwendung mit vereinfachtem SAML konfiguriert wurde und nur **cip_upn** zur Authentifizierung innerhalb der SAML-Assertion sendet.
- Frontend-Benutzer innerhalb Ihres SAML-Anbieters.
- Ein Ressourcenstandort, der ein Paar Citrix Cloud Connectors enthält, die mit der AD-Gesamtstruktur und der Domäne verbunden sind, in der die AD-Schattenkonten erstellt werden.
- Alternative UPN-Suffixe wurden der Backend-AD-Gesamtstruktur hinzugefügt, in der die AD-Schattenkonten erstellt werden.
- Backend-AD-Schattenkonten mit passenden UPNs.
- DaaS- oder Citrix Virtual Apps and Desktops-Ressourcen, die den Benutzern des AD-Schattenkontos zugeordnet sind.
- Ein oder mehrere FAS-Server, die mit demselben Ressourcenstandort verknüpft sind.

Häufig gestellte Fragen

Warum sollte ich vereinfachtes SAML verwenden?

Es ist üblich, dass große Unternehmen Auftragnehmer und Zeitarbeitskräfte in ihre Identitätsplattform einladen. Ziel ist es, dem Auftragnehmer temporären Zugriff auf Citrix Workspace unter Verwen-

dung der vorhandenen Benutzeridentität zu gewähren, z. B. einer Auftragnehmer-E-Mail-Adresse oder einer E-Mail-Adresse außerhalb Ihrer Organisation. Vereinfachtes SAML ermöglicht die Verwendung von nativen oder Gast-Frontend-Identitäten, die in der AD-Domäne, in der DaaS-Ressourcen veröffentlicht werden, nicht existieren.

Was ist vereinfachtes SAML?

Normalerweise werden bei der Anmeldung bei Citrix Workspace vier SAML-Attribute cip_* und die entsprechenden AD-Benutzerattribute verwendet, um den Endbenutzer zu authentifizieren. Es wird erwartet, dass diese vier SAML-Attribute in der SAML-Assertion vorhanden sind und mithilfe von AD-Benutzerattributen aufgefüllt werden. Vereinfachtes SAML bezieht sich auf die Tatsache, dass für eine erfolgreiche Authentifizierung nur das SAML-Attribut cip_upn erforderlich ist.

AD-Attribut	Standardattributname in der SAML-Assertion
userPrincipalName	cip_upn
Mail	cip_email
objectSID	cip_sid
objectGUID	cip_oid

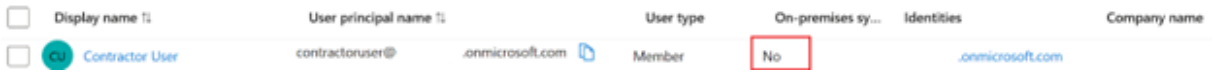
Die anderen drei AD-Benutzerattribute objectSID, objectGUID und mail, die für die Authentifizierung erforderlich sind, werden mithilfe der Citrix Cloud Connectors abgerufen, die mit der AD-Domäne verbunden sind, in der das AD-Schattenkonto vorhanden ist. Sie müssen während eines SAML-Anmeldeflusses für Workspace oder Citrix Cloud nicht mehr in die SAML-Assertion eingeschlossen werden.

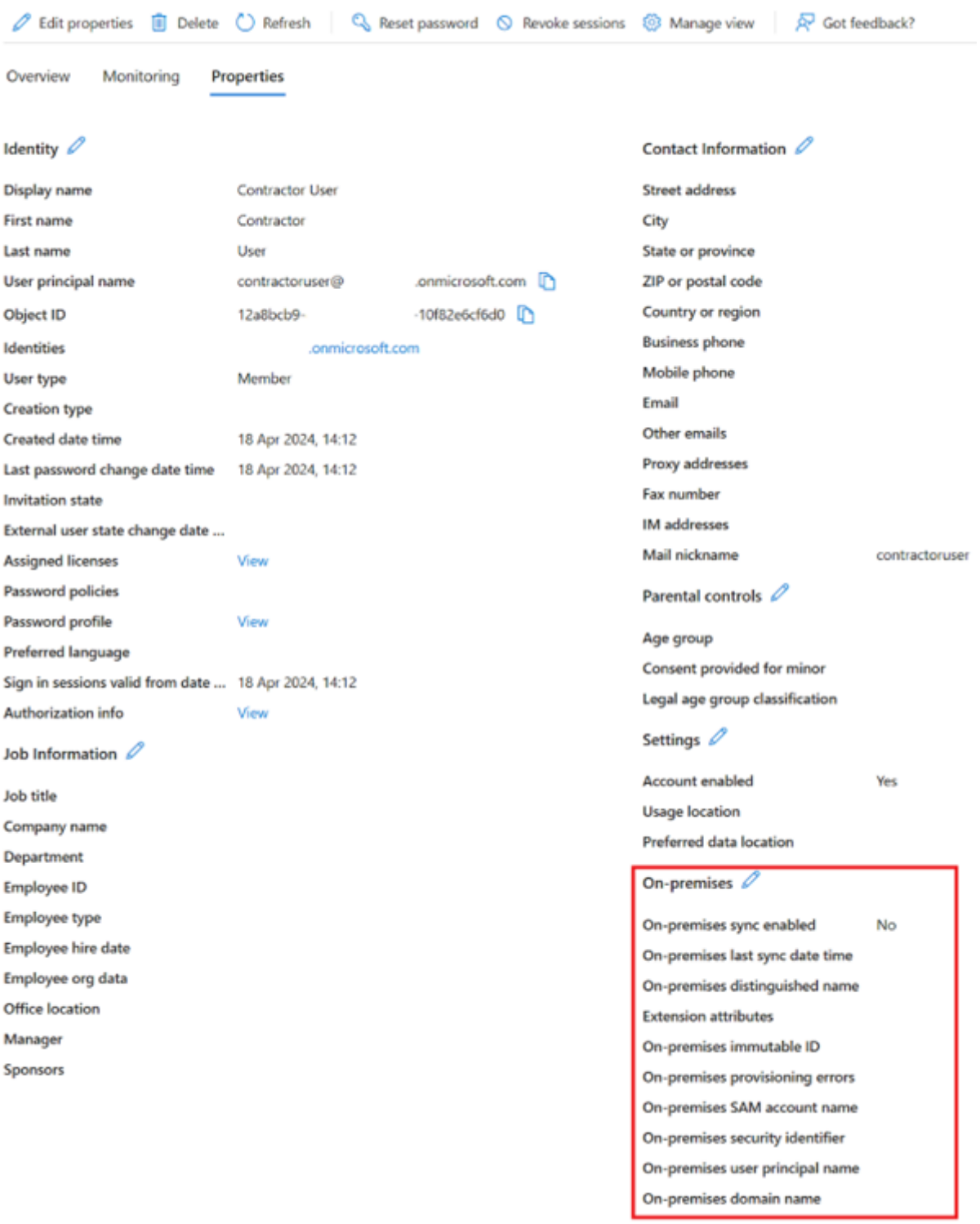
AD-Attribut	Standardattributname in der SAML-Assertion
userPrincipalName	cip_upn

> **Wichtig:**
>
> Es ist für alle SAML-Flüsse weiterhin erforderlich, den **displayName** zu senden. Dies gilt auch für vereinfachtes SAML. Der **displayName** wird von der Workspace-Benutzeroberfläche benötigt, um den vollständigen Namen des Workspace-Benutzers korrekt anzuzeigen.

Was ist eine native SAML-Benutzeridentität?

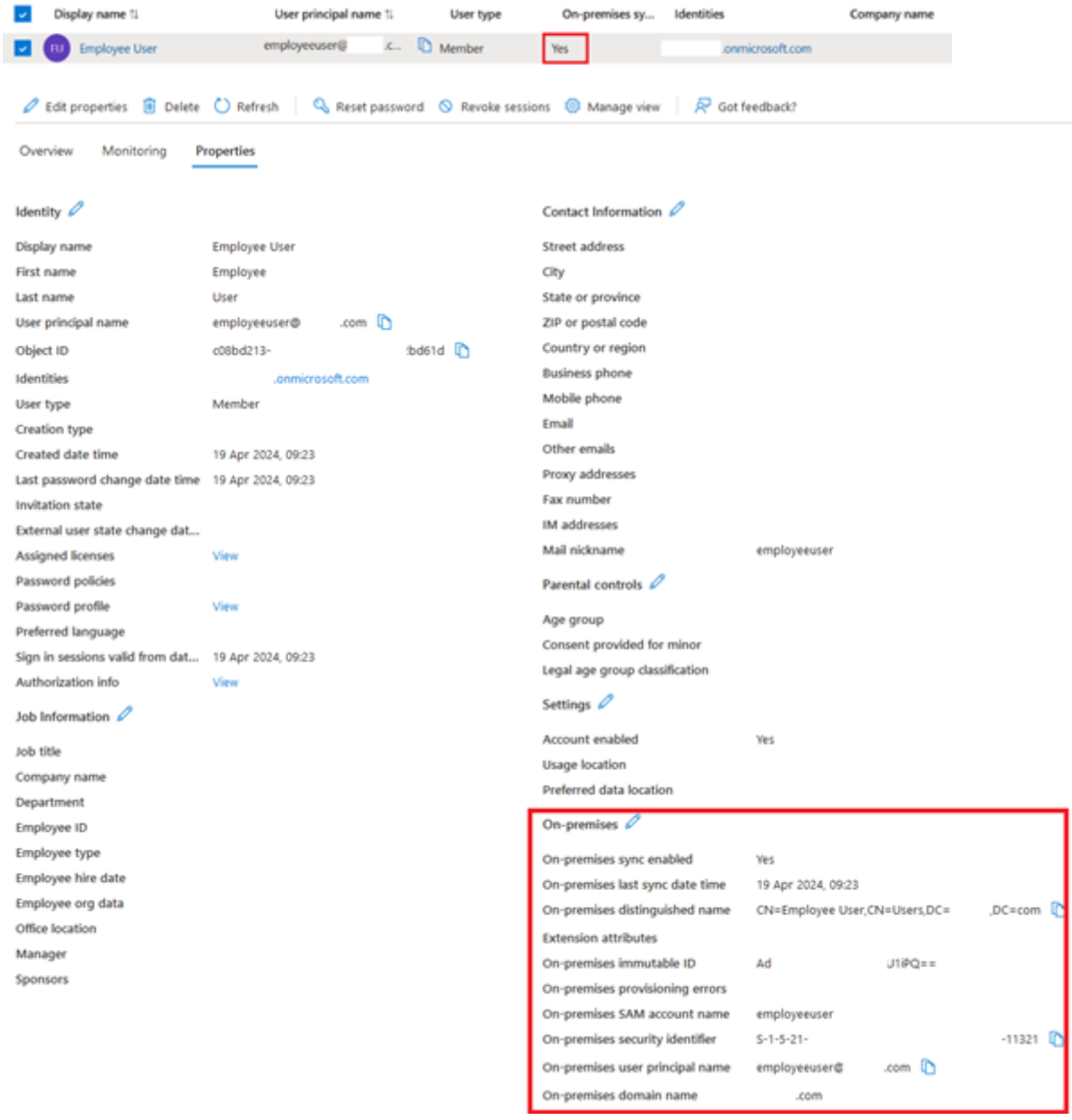
Ein nativer SAML-Benutzer ist eine Benutzeridentität, die nur in Ihrem SAML-Anbieterverzeichnis existiert, z. B. Entra ID oder Okta. Diese Identitäten enthalten keine lokalen Benutzerattribute, da sie nicht über AD-Synchronisierungstools wie Entra ID Connect erstellt werden. Sie benötigen passende AD-Backend-Schattenkonten, um DaaS-Ressourcen auflisten und starten zu können. Der native SAML-Benutzer muss einem entsprechenden Konto in Active Directory zugeordnet sein.





Was ist eine AD-gestützte SAML-Benutzeridentität?

Ein AD-gestützter SAML-Benutzer ist eine Benutzeridentität, die in Ihrem SAML-Anbieterverzeichnis wie Entra ID oder Okta und auch in Ihrer lokalen AD-Gesamtstruktur existiert. Diese Identitäten enthalten lokale Benutzerattribute, da sie über AD-Synchronisierungstools wie Entra ID Connect erstellt werden. AD-Backend-Schattenkonten sind für diese Benutzer nicht erforderlich, da sie lokale SIDs und OIDs enthalten und daher DaaS-Ressourcen auflisten und starten können.

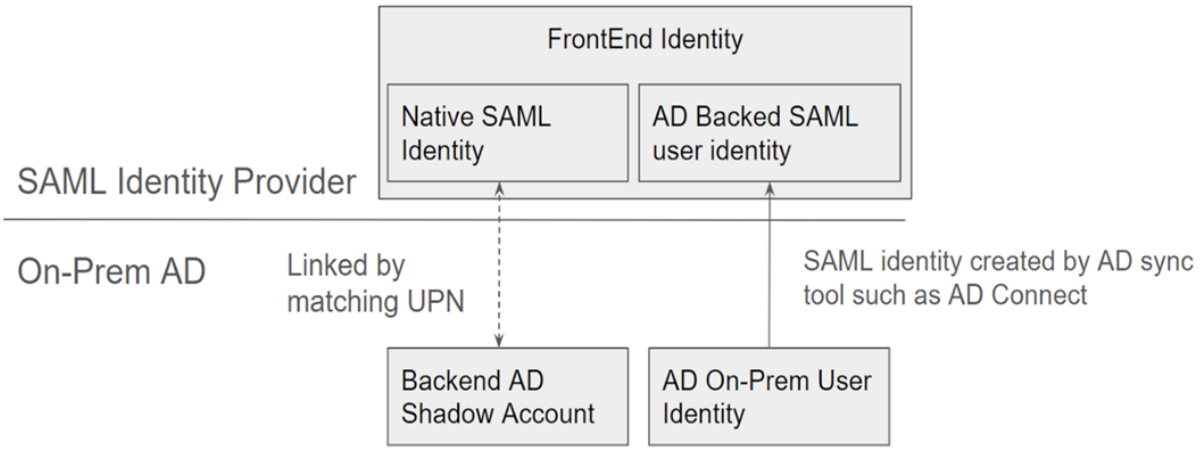


Was ist eine Frontend-Identität?

Eine Frontend-Identität ist die Identität, die für die Anmeldung sowohl beim SAML-Anbieter als auch bei Workspace verwendet wird. Frontend-Identitäten haben unterschiedliche Benutzerattribute, je nachdem, wie sie innerhalb des SAML-Anbieters erstellt wurden.

1. Native SAML-Benutzeridentität
2. AD-gestützte SAML-Benutzeridentität

Ihr SAML-Anbieter verfügt möglicherweise über eine Kombination dieser beiden Arten von Identitäten. Wenn Sie beispielsweise sowohl Auftragnehmer als auch festangestellte Mitarbeiter in Ihrer Identitätsplattform haben, funktioniert vereinfachtes SAML für beide Arten von Frontend-Identitäten, ist aber nur erforderlich, wenn Sie einige Konten haben, die vom Typ native SAML-Benutzeridentität sind.



Was ist ein Backend-AD-Schattenkonto?

Ein Backend-AD-Schattenkonto ist ein von DaaS verwendetes AD-Konto, das einer entsprechenden Frontend-Identität innerhalb Ihres SAML-Anbieters zugeordnet ist.

Warum werden Backend-AD-Schattenkonten benötigt?

Um DaaS- oder CVAD-Ressourcen aufzulisten, die mithilfe von der AD-Domäne beigetretenen VDAs veröffentlicht wurden, sind AD-Konten innerhalb der Active Directory-Gesamtstruktur erforderlich, der die VDAs beigetreten sind. Ordnen Sie Ressourcen innerhalb Ihrer DaaS-Bereitstellungsgruppe Schattenkontobenutzern und AD-Gruppen zu, die Schattenkonten innerhalb der AD-Domäne enthalten, der Ihre VDAs beigetreten sind.

> **Wichtig:**
>
> Nur native SAML-Benutzer ohne AD-Domänenattribute benötigen übereinstimmende AD-Schattenkonten. Wenn Ihre Frontend-Identitäten aus Active Directory importiert werden, müssen Sie vereinfachte SAML nicht verwenden und auch keine Backend-AD-Schattenkonten erstellen.

Wie verknüpfen wir die Frontend-Identität mit dem entsprechenden Backend-AD-Schattenkonto?

Die Methode, die verwendet wird, um die Frontend-Identität und die Backend-Identität zu verknüpfen, besteht darin, passende UPNs zu verwenden. Die beiden verknüpften Identitäten müssen identische UPNs haben, damit Workspace erkennen kann, dass sie denselben Endbenutzer repräsentieren, der sich bei Workspace anmelden muss, und damit DaaS-Ressourcen aufgelistet und gestartet werden können.

Wird Citrix FAS für vereinfachtes SAML benötigt?

Ja. FAS ist für SSON beim VDA während des Starts erforderlich, wenn Sie eine Verbundauthentifizierungsmethode verwenden, um sich bei Workspace anzumelden.

Was ist das "SID-Nichtübereinstimmungsproblem"und wann kann es auftreten?

Das "SID-Nichtübereinstimmungsproblem"wird verursacht, wenn die SAML-Assertion eine SID für einen Frontend-Benutzer enthält, die nicht mit der SID des AD-Schattenkontobenutzers übereinstimmt. Dies kann vorkommen, wenn das Konto, das sich bei Ihrem SAML-Anbieter anmeldet, eine lokale SID hat, die nicht mit der SID des Schattenkontobenutzers identisch ist. Dies kann nur passieren, wenn die Frontend-Identität von AD-Synchronisierungstools wie Entra ID Connect bereitgestellt wird und aus einer anderen AD-Gesamtstruktur als der stammt, in der das Schattenkonto erstellt wurde.

Vereinfachtes SAML verhindert das Auftreten des "SID-Nichtübereinstimmungsproblems". Die richtige SID wird für den Schattenkontobenutzer immer über die Citrix Cloud Connectors abgerufen, die mit der Backend-AD-Domäne verbunden sind. Die Suche nach dem Schattenkontobenutzer wird anhand des UPN des Frontend-Benutzers durchgeführt, der dann mit dem entsprechenden Backend-Schattenkontobenutzer abgeglichen wird.

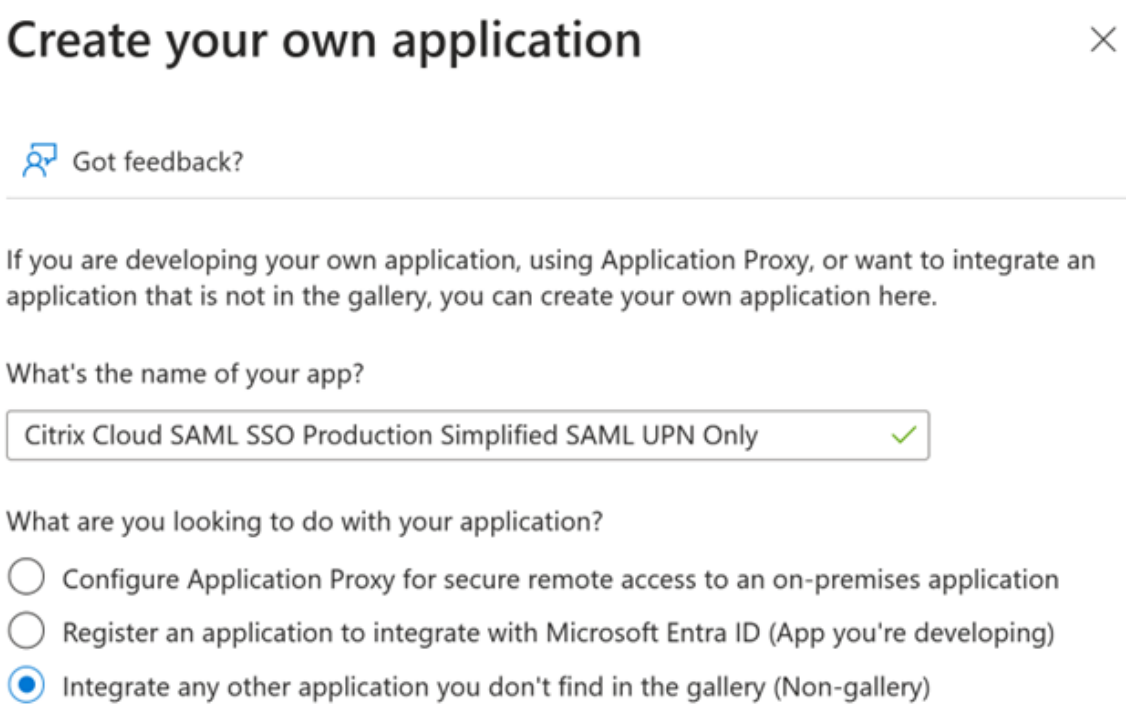
Beispiel für das SID-Nichtübereinstimmungsproblem: Der **Frontend-Benutzer** wurde von Entra ID Connect erstellt und über die **AD-Gesamtstruktur 1** synchronisiert.
`S-1-5-21-000000000-0000000000-0000000001-0001`

Der **Backend-Schattenkontobenutzer** wurde in **AD-Gesamtstruktur 2** erstellt und DaaS-Ressourcen zugeordnet
`S-1-5-21-000000000-0000000000-0000000002-0002`.

Die SAML-Assertion enthält alle vier cip_*-Attribute und **cip_sid** enthält den Wert `S-1-5-21-000000000-0000`, der nicht mit der SID des Schattenkontos übereinstimmt und einen Fehler auslöst.

Konfigurieren von vereinfachtem SAML mithilfe der Entra ID für externe Gastkonten

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie im Portalmenü die Option **Entra ID** aus.
3. Wählen Sie im linken Bereich unter **Verwalten** die Option **Unternehmensanwendungen**.
4. Wählen Sie **Eigene Anwendung erstellen** aus.
5. Geben Sie einen geeigneten Namen für die SAML-Anwendung ein, z. B. `Citrix Cloud SAML SSO Production Simplified SAML`.



6. Wählen Sie im linken Navigationsbereich **Single Sign-On** aus und klicken Sie im Arbeitsbereich auf **SAML**.
7. Klicken Sie im Abschnitt **Grundlegende SAML-Konfiguration** auf die Option **Bearbeiten** und konfigurieren Sie die folgenden Einstellungen:

    a) Wählen Sie im Abschnitt **Bezeichner (Entitäts-ID)** die Option **Bezeichner hinzufügen** und geben Sie dann den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:

- Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com` ein.
- Geben Sie für die Region Japan `https://saml.citrixcloud.jp` ein.
- Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us` ein.

b) Wählen Sie im Abschnitt **Antwort-URL (Assertionsverbraucherdienst-URL)** die Option **Antwort-URL hinzufügen** und geben Sie dann den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:

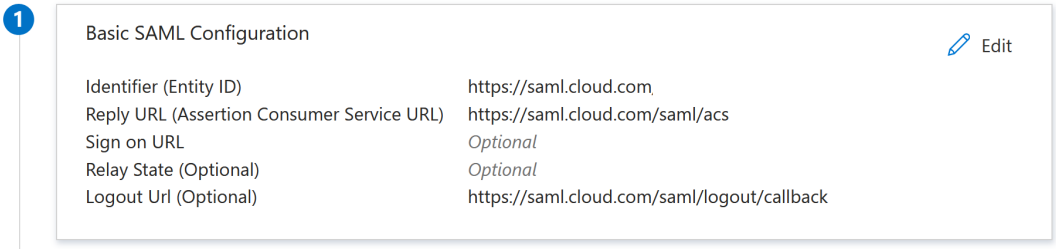
- Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com/saml/acs` ein.
- Geben Sie für die Region Japan `https://saml.citrixcloud.jp/saml/acs` ein.
- Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us/saml/acs` ein.

c) Geben Sie im Abschnitt **Anmelde-URL** Ihre Workspace-URL ein.

d) Geben Sie im Abschnitt **Abmelde-URL** (optional) den Wert für die Region ein, in der sich der Citrix Cloud-Mandant befindet:

- Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com/saml/logout/callback` ein.
- Geben Sie für die Region Japan `https://saml.citrixcloud.jp/saml/logout/callback` ein.
- Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us/saml/logout/callback` ein.

e) Klicken Sie in der Befehlsleiste auf **Speichern**. Der Abschnitt **Grundlegende SAML-Konfiguration** sieht wie folgt aus:



8. Wählen Sie im Abschnitt **Attribute und Ansprüche** die Option **Bearbeiten**, um die folgenden Ansprüche zu konfigurieren. Diese Ansprüche erscheinen in der SAML-Assertion der SAML-Antwort. Konfigurieren Sie nach der Erstellung der SAML-App die folgenden Attribute.

a) Übernehmen Sie für den Anspruch **Eindeutiger Benutzerbezeichner (Namens-ID)** den Standardwert `user.userprincipalname`.

b) Lassen Sie für den Anspruch **cip_upn** den Standardwert `user.userprincipalname`.

c) Lassen Sie für **displayName** den Standardwert `user.displayname`.

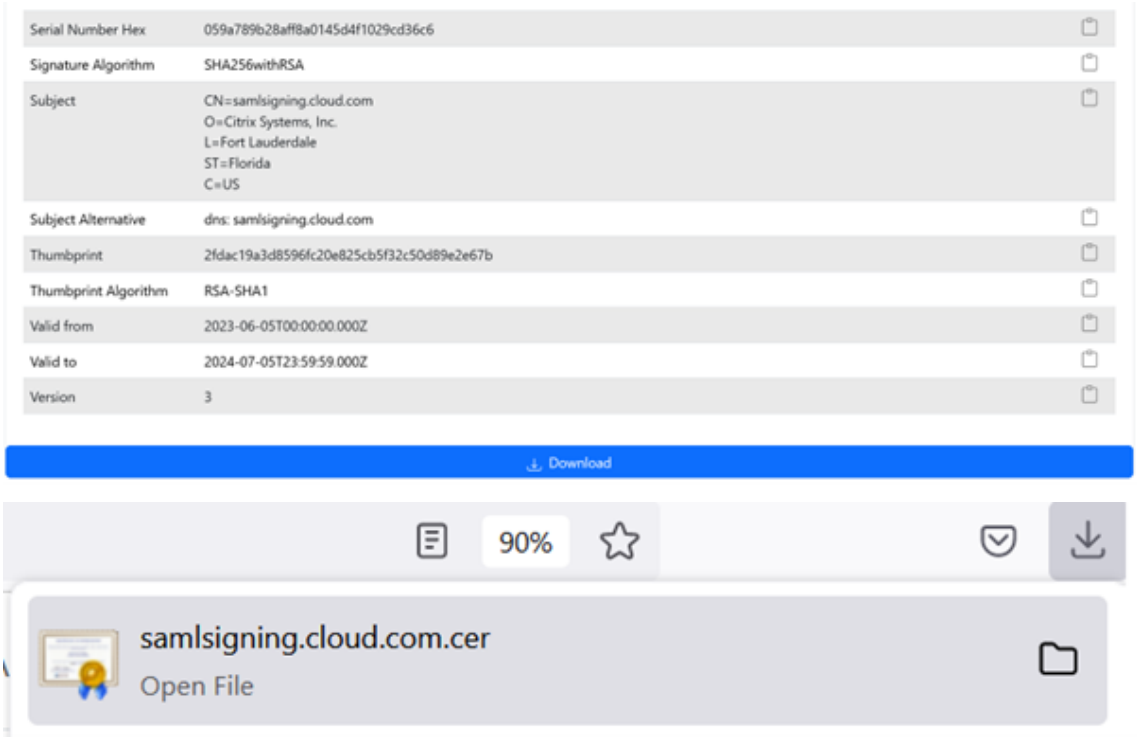
d) Klicken Sie im Abschnitt **Zusätzliche Ansprüche** für alle verbleibenden Ansprüche mit dem Namespace `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` auf das Menü (…) und dann auf **Löschen**. Diese Ansprüche müssen nicht aufgenommen werden, da es sich um Duplikate der oben genannten Benutzerattribute handelt.

   Wenn Sie fertig sind, wird der Abschnitt **Attribute und Ansprüche** wie unten dargestellt angezeigt:

e) Besorgen Sie sich mit diesem Online-Tool eines Drittanbieters eine Kopie des Citrix Cloud SAML-Signaturzertifikats.

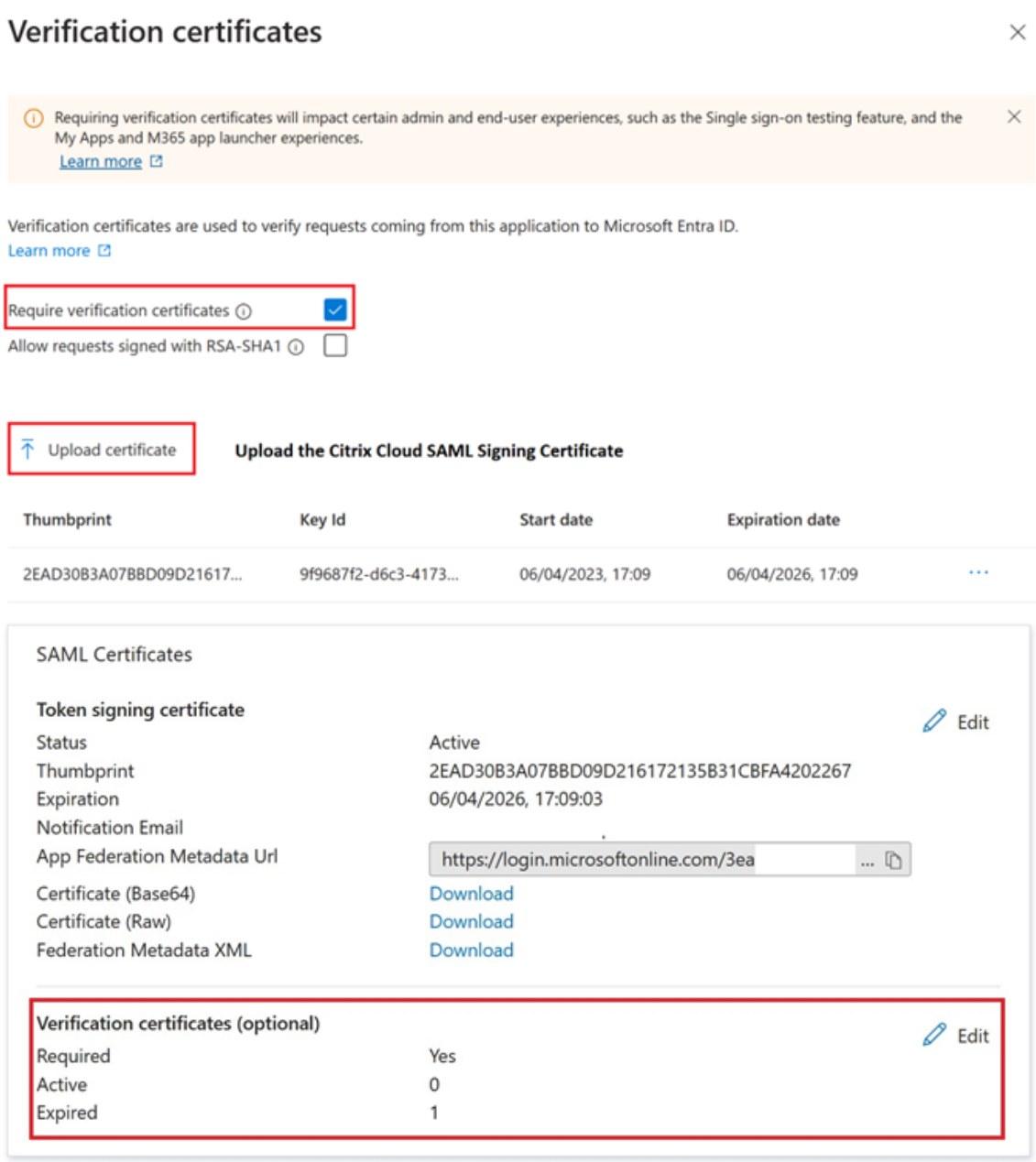
f) Geben Sie `https://saml.cloud.com/saml/metadata` in das URL-Feld ein und klicken Sie auf **Laden**.

9. Scrollen Sie zum Ende der Seite und klicken Sie auf **Download**.



10. Konfigurieren Sie die Signatureinstellungen der Azure Active Directory-SAML-Anwendung.
11. Laden Sie das in Schritt 10 erhaltene SAML-Signaturzertifikat für die Produktion in die SAML-Anwendung von Azure Active Directory hoch

    a) Aktivieren Sie die Option **Verifizierungszertifikate erforderlich**.



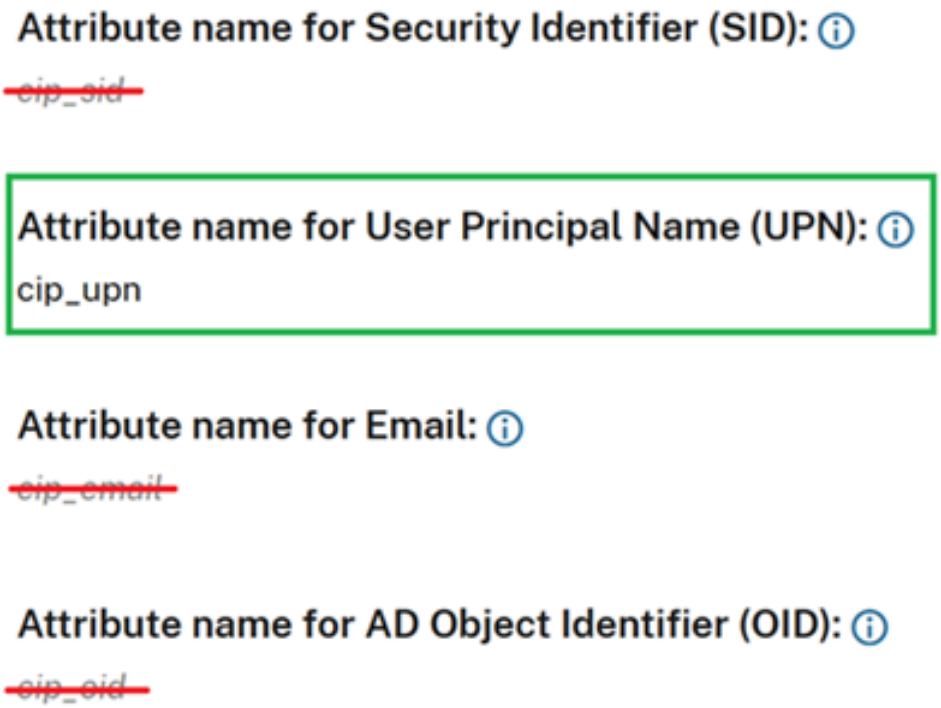
Konfigurieren der vereinfachten SAML-Verbindung für Citrix Cloud

Standardmäßig erwartet Citrix Cloud, dass cip_upn, cip_email, cip_sid und cip_oid in der SAML-Assertion vorhanden sind, und die SAML-Anmeldung schlägt fehl, wenn diese Attribute nicht gesendet werden. Um dies zu verhindern, deaktivieren Sie die Kontrollkästchen für diese Attribute, wenn Sie Ihre neue SAML-Verbindung erstellen.

1. Erstellen Sie eine neue SAML-Verbindung mit den Standardeinstellungen.
2. Navigieren Sie unten zum Abschnitt für die **Konfiguration der SAML-Attributzuordnungen**

und nehmen Sie Änderungen vor, bevor Sie die neue SAML-Konfiguration speichern.

3. Entfernen Sie den SAML-Attributnamen aus jedem der Felder **cip_email**, **cip_sid** und **cip_oid**.
4. Entfernen Sie **cip_upn** nicht aus seinem Feld.
5. Entfernen Sie keine anderen Attribute aus den jeweiligen Feldern. Der **displayName** wird weiterhin von der Workspace-Benutzeroberfläche benötigt und darf nicht geändert werden.



Konfigurieren des Ressourcenstandorts und der Connectors Ihres AD-Schattenkontos

Ein Ressourcenstandort und ein Connector-Paar innerhalb der AD-Gesamtstruktur des Backend-Schattenkontos ist erforderlich. Citrix Cloud benötigt Connectors in dieser AD-Gesamtstruktur, um Schattenkonto-Benutzeridentitäten und Attribute wie cip_email, cip_sid und cip_oid nachzuschlagen, wenn nur cip_upn direkt in der SAML-Assertion bereitgestellt wird.

1. Erstellen Sie einen neuen **Ressourcenstandort**, der Citrix Cloud Connectors enthält, die der AD-Gesamtstruktur des Backend-Schattenkontos beigetreten sind.

2. Benennen Sie den Ressourcenstandort so, dass er der AD-Gesamtstruktur mit den Backend-AD-Schattenkonten entspricht, die Sie verwenden möchten.

3. Konfigurieren Sie ein Paar Citrix Cloud Connectors innerhalb des neu erstellten Ressourcenstandorts.

Beispiel:
`ccconnector1.shadowaccountforest.com`
`ccconnector2.shadowaccountforest.com`

Konfigurieren von FAS innerhalb der Backend-AD-Gesamtstruktur

Contractor Frontend-Benutzer benötigen auf jeden Fall FAS. Bei DaaS-Starts können Auftragnehmer-Benutzer Windows-Anmeldeinformationen nicht manuell eingeben, um den Start durchzuführen, da sie das AD-Schattenkonto-Passwort wahrscheinlich nicht kennen.

1. Konfigurieren Sie einen oder mehrere FAS-Server innerhalb der Backend-AD-Gesamtstruktur, in der Ihre Schattenkonten erstellt wurden.
2. Verknüpfen Sie die FAS-Server mit demselben Ressourcenstandort, der ein Paar Citrix Cloud Connectors enthält, die mit der Backend-AD-Gesamtstruktur verbunden sind, in der Ihre Schattenkonten erstellt wurden.

Konfigurieren alternativer UPN-Suffixe in der AD-Domäne

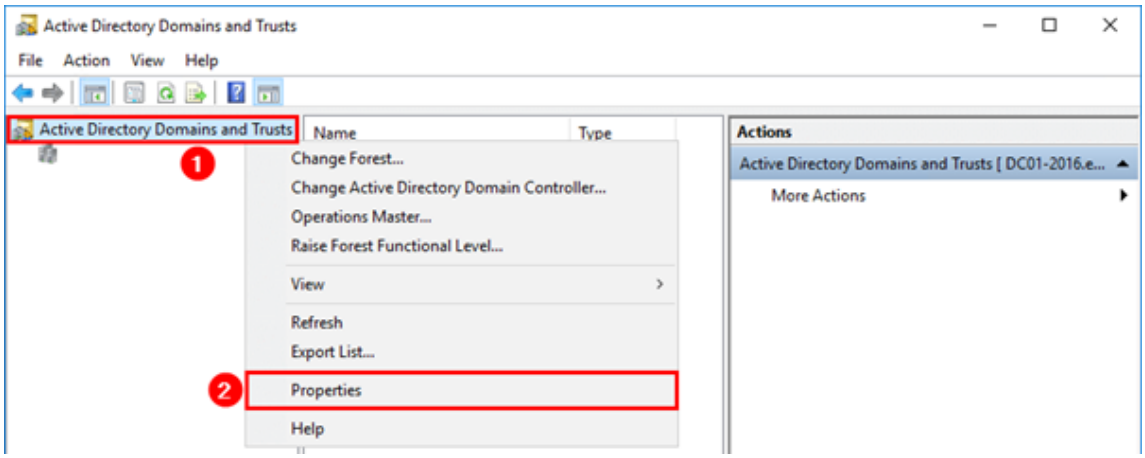
> **Wichtig:**
>
> Ein UPN ist nicht dasselbe wie die E-Mail-Adresse des Benutzers. In vielen Fällen haben sie aus Gründen der Benutzerfreundlichkeit den gleichen Wert, aber UPN und E-Mail werden intern unterschiedlich verwendet und sind in unterschiedlichen Active Directory-Attributen definiert.

Das UPN-Suffix (User Principal Name) ist Teil des Anmeldenamens in AD. Wenn Sie ein neues Konto erstellen, verwendet es standardmäßig das implizite UPN-Suffix Ihrer AD-Gesamtstruktur, z. B. yourforest.com. Sie müssen für jeden externen Frontend-Benutzer, den Sie zu Ihren Okta- oder Azure AD-Mandanten einladen möchten, ein passendes alternatives UPN-Suffix hinzufügen.

Wenn Sie beispielsweise einen externen Benutzer `contractoruser@hotmail.co.uk` einladen und diesen mit einem Backend-AD-Schattenkonto `contractoruser@yourforest.com` verknüpfen möchten, fügen Sie `yourforest.com` als ALT UPN-Suffix in Ihrer AD-Gesamtstruktur hinzu.

Hinzufügen alternativer UPN-Suffixe in Active Directory mithilfe der Benutzeroberfläche von Active Directory-Domänen und -Vertrauensstellungen

1. Melden Sie sich bei einem Domänencontroller in Ihrer Backend-AD-Gesamtstruktur an.
2. Öffnen Sie das **Fenster "Ausführen"**, geben Sie den Text `domain.msc` ein und klicken Sie dann auf **OK**.
3. Klicken Sie im Fenster "Active Directory-Domänen und -Vertrauensstellungen"mit der rechten Maustaste auf **Active Directory-Domänen und -Vertrauensstellungen**, und wählen Sie dann **Eigenschaften** aus.
4. Fügen Sie auf der Registerkarte **UPN-Suffixe** im Feld "Alternative UPN-Suffixe"ein alternatives UPN-Suffix hinzu, und wählen Sie dann **Hinzufügen** aus.



5. Klicken Sie auf **OK**.

Verwalten der UPN-Suffixe Ihrer Backend-AD-Gesamtstruktur mithilfe von PowerShell

Möglicherweise müssen Sie Ihrer Backend-AD-Gesamtstruktur eine große Anzahl neuer UPN-Suffixe hinzufügen, um die erforderlichen UPNs für Schattenkonten zu erstellen. Die Anzahl der alternativen UPN-Suffixe, die Sie Ihrer Backend-AD-Gesamtstruktur hinzufügen müssen, hängt davon ab, wie viele verschiedene externe Benutzer Sie in Ihren SAML-Anbieter-Mandanten einladen möchten.

Hier finden Sie einige PowerShell-Suffixe, um dies zu erreichen, wenn eine große Anzahl neuer alternativer UPN-Suffixe erstellt werden muss.

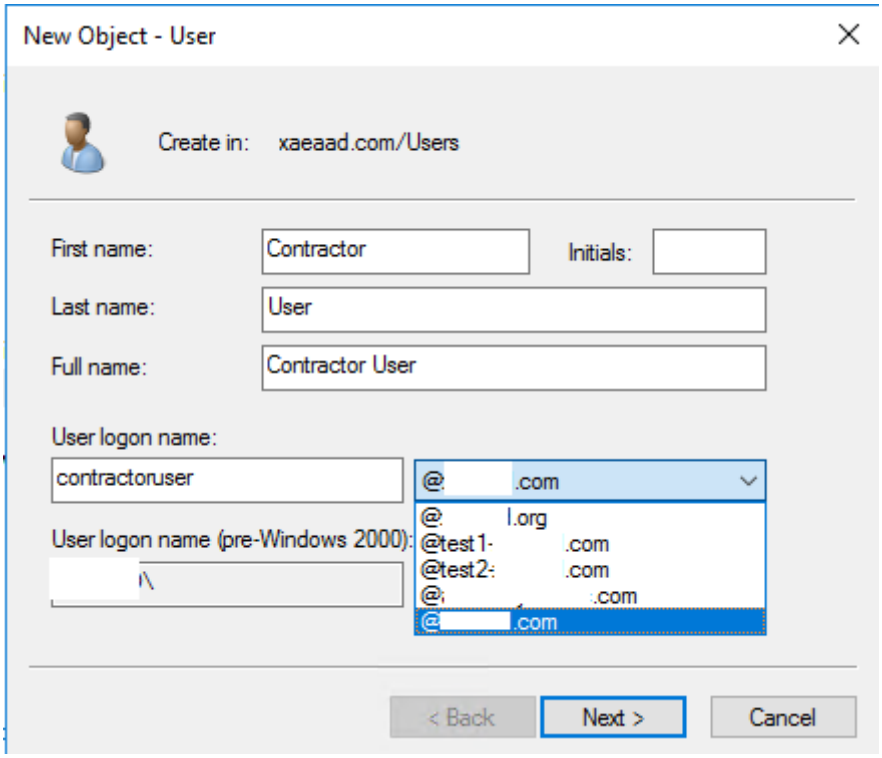
```
# Get the list of existing ALT UPN suffixes within your AD Forest
(Get-ADForest).UPNSuffixes

# Add or remove ALT UPN Suffixes
$NewUPNSuffixes = @("yourforest.com","externalusers.com")

```



```
# Set action to "add" or "remove" depending on the operation you wish
    to perform.
$Action = "add"
foreach($NewUPNSuffix in $NewUPNSuffixes)
{

    Get-ADForest | Set-ADForest -UPNSuffixes @{
 $Action=$NewUPNSuffix }

 }

<!--NeedCopy-->
```

Konfigurieren eines AD-Schattenkontos in der Backend-AD-Gesamtstruktur

1. Erstellen Sie einen neuen AD-Schattenkontobenutzer.
2. Der implizite UPN der AD-Gesamtstruktur, z. B. `yourforest.local`, ist standardmäßig für neue AD-Benutzer ausgewählt. Wählen Sie das entsprechende alternative UPN-Suffix aus, das Sie zuvor erstellt haben. Wählen Sie beispielsweise `yourforest.com` als das UPN-Suffix des Schattenkontobenutzers aus.



Der UPN des Schattenkontobenutzers kann auch über PowerShell aktualisiert werden.

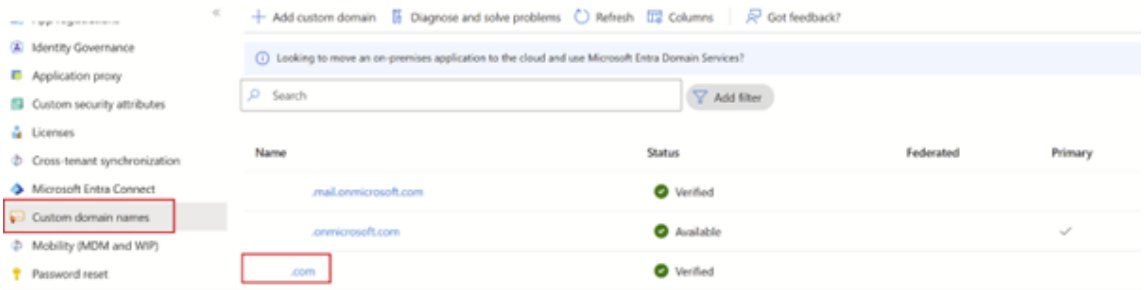
```
Set-ADUser "contractoruser" -UserPrincipalName "
    contractoruser@yourforest.com"
<!--NeedCopy-->
```


3. Der UPN des Schattenkontobenutzers muss exakt dem UPN des externen Frontend-Identitätsbenutzers entsprechen.
4. Testen Sie die Anmeldung des Frontend-Benutzers bei Workspace.
5. Stellen Sie sicher, dass alle erwarteten Ressourcen in Workspace aufgeführt sind, nachdem die Anmeldung erfolgreich war. Ressourcen, die dem AD-Schattenkonto zugeordnet sind, sollten angezeigt werden.

Konfigurieren des Benutzer-UPN für die Gast-Entra-ID, sodass er dem UPN des AD-Schattenkontos entspricht

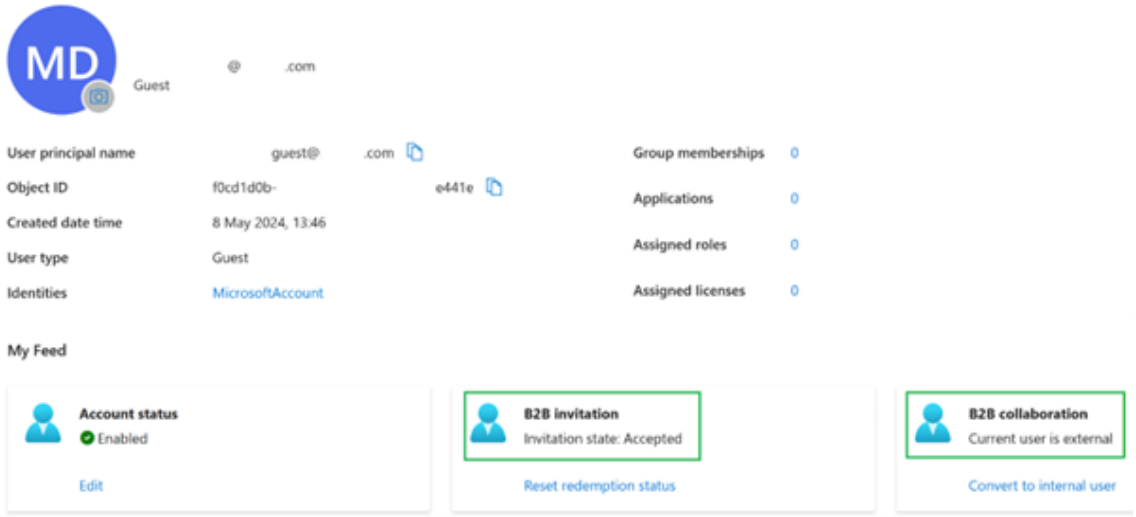
Wenn externe Gastbenutzer zu einem Entra ID-Mandanten eingeladen werden, wird ein automatisch generierter UPN erstellt, der angibt, dass es sich um einen externen Benutzer handelt. Dem externen Entra ID-Benutzer wird automatisch das UPN-Suffix @Entra IDtenant.onmicrosoft.com zugewiesen, das für die Verwendung mit vereinfachtem SAML ungeeignet ist und nicht mit Ihrem AD-Schattenkonto übereinstimmt. Es muss aktualisiert werden, damit es einer importierten DNS-Domäne innerhalb von Entra ID und dem alternativen UPN-Suffix entspricht, das Sie in Ihrer AD-Gesamtstruktur erstellt haben.

1. Importieren Sie eine benutzerdefinierte Domäne in Entra ID, die dem alternativen UPN-Suffix entspricht, das Sie Ihrer AD-Gesamtstruktur hinzugefügt haben.



2. Laden Sie einen Gastbenutzer wie `contractoruser@hotmail.co.uk` ein und stellen Sie sicher, dass der eingeladene Gastbenutzer die Microsoft-Einladung zum Entra ID-Mandanten akzeptiert.

   Beispiel für ein von Microsoft generiertes UPN-Format für externe Gastbenutzer.
   `contractoruser_hotmail.co.uk#EXT#@yourEntra IDtenant.onmicrosoft.com`



> **Wichtig:**
>
> Citrix Cloud und Workspace können keine UPNs, die das #-Zeichen enthalten, für die SAML-Authentifizierung verwenden.

3. Installieren Sie die erforderlichen Azure PowerShell Graph-Module, um Entra ID-Benutzer verwalten zu können.

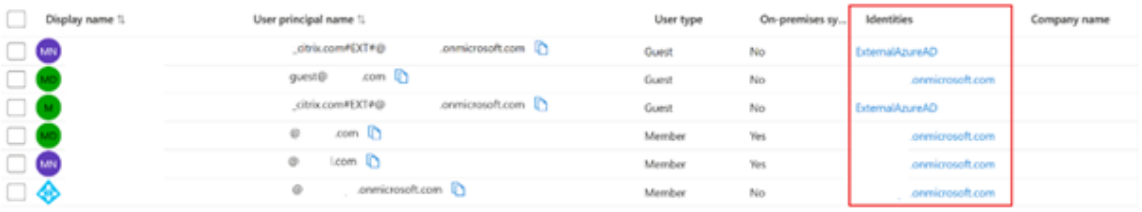
```
Install-Module -Name "Microsoft.Graph" -Force
Get-InstalledModule -Name  "Microsoft.Graph"
<!--NeedCopy-->
```

4. Melden Sie sich mit einem globalen Administratorkonto und mit dem Geltungsbereich `Directory.AccessAsUser.All` bei Ihrem Entra ID-Mandanten an.

> **Wichtig:**
>
> Wenn Sie ein Konto mit weniger Rechten verwenden oder den Geltungsbereich `Directory.AccessAsUser.All` nicht angeben, können Sie Schritt 4 nicht abschließen und den UPN des Gastbenutzers nicht aktualisieren.

```
$EntraTenantID = "<yourEntraTenantID>"
Connect-MgGraph -Tenant $EntraTenantID -Scopes "Directory.
    AccessAsUser.All"
<!--NeedCopy-->
```

5. Rufen Sie die gesamte Liste der externen Gastbenutzer in Ihrem Entra ID-Mandanten ab (optional).




```
Get-MgUser -filter "userType eq 'Guest'" | Select Id,DisplayName,
    UserPrincipalName,Mail
<!--NeedCopy-->
```

6. Rufen Sie die Gastbenutzeridentität ab, deren UPN aktualisiert werden muss, und aktualisieren Sie dann das UPN-Suffix.

```
$GuestUserId = (Get-MgUser -UserId "contractoruser_hotmail.co.uk#
    EXT#@yourEntra IDtenant.onmicrosoft.com").Id

Update-MgUser -UserId $GuestUserId -UserPrincipalName "
    contractoruser@yourforest.com"
<!--NeedCopy-->
```

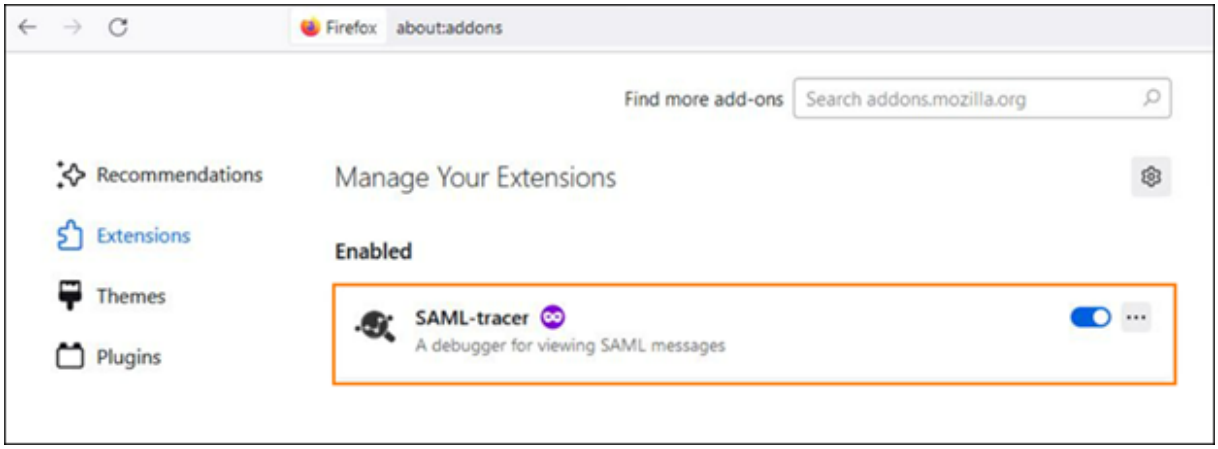
7. Prüfen Sie, ob die Gastbenutzeridentität anhand des neu aktualisierten UPN gefunden werden kann.

```
Get-MgUser -UserId "contractoruser@yourforest.com"
<!--NeedCopy-->
```

Testen der vereinfachten SAML-Lösung

Sobald alle dokumentierten Schritte in AD, Citrix Cloud und Ihrem SAML-Anbieter abgeschlossen sind, müssen Sie die Anmeldung testen und sicherstellen, dass die richtige Ressourcenliste für den Gastbenutzer in Workspace angezeigt wird.

Citrix empfiehlt die Verwendung der Browsererweiterung SAML-tracer für das gesamte SAML-Debugging. Die Erweiterung ist für die meisten der gängigen Webbrowser verfügbar. Die Erweiterung decodiert Base64-Anfragen und -Antworten in SAML-XML, wodurch sie für Menschen lesbar werden.



Beispiel für eine vereinfachte SAML-Assertion, bei der nur cip_upn für die Authentifizierung verwendet wird, die mit dem SAML-Tracer erfasst wurde.

```
<AttributeStatement>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider">
        <AttributeValue>https://sts.windows.net/                                    /</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
        <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/        </AttributeValue>
    </Attribute>
    <Attribute Name="cip_upn">
        <AttributeValue>                    </AttributeValue>
    </Attribute>
    <Attribute Name="lastName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="firstName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="displayName">
        <AttributeValue>        </AttributeValue>
    </Attribute>
</AttributeStatement>
```

FrontEnd Identity Type	Synched from AD	Has Connectors in AD	Needs AD Shadow Account	Login using Attribute
Internal AD Backed User in Shadow Account Forest	Yes	Yes	No	UPN
Internal AD Backed User in Different Forest	Yes	No	Yes	UPN
Internal Native User	No	Not applicable	Yes	UPN
External Guest User	No	Not applicable	Yes	Email

1. Ordnen Sie AD-gestützten Benutzern und Schattenkontobenutzern oder Gruppen, die diese enthalten, die richtigen DaaS-Ressourcen zu.
2. Starten Sie die SAML-Tracer-Browsererweiterung und erfassen Sie den gesamten An- und Abmeldeablauf.
3. Melden Sie sich mit dem in der Tabelle angegebenen Attribut für den Frontend-Benutzertyp,

den Sie testen möchten, bei Workspace an.

Entra ID-Gastbenutzeranmeldung: Der Auftragnehmer, den Sie als Gastbenutzer zu Ihrem Entra ID-Mandanten eingeladen haben, hat die E-Mail-Adresse `contractoruser@hotmail.co.uk`.

Geben Sie die **E-Mail-Adresse** des Gastbenutzers ein, wenn Sie von Entra ID dazu aufgefordert werden.

ODER

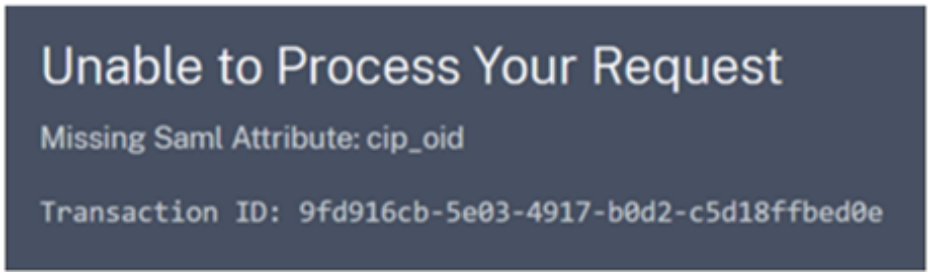
AD-gestützte EntraID-Benutzer/native EntraID-Benutzeranmeldung: Diese Entra ID-Benutzer erhalten UPNs im Format von `adbackeduser@yourforest.com` oder `nativeuser@yourforest.com`.

Geben Sie den **UPN** des Benutzers ein, wenn Sie von Entra ID dazu aufgefordert werden.

4. Stellen Sie sicher, dass die Assertion nur das Attribut **cip_upn** für die Authentifizierung enthält und dass sie auch das für die Workspace-Benutzeroberfläche erforderliche Attribut **displayName** enthält.
5. Stellen Sie sicher, dass der Benutzer die erforderlichen DaaS-Ressourcen in der Benutzeroberfläche sehen kann.

Problembehandlung für die vereinfachte SAML-Lösung

Fehler wegen fehlendem Attribut cip_*



Ursache 1: Das SAML-Attribut ist in der SAML-Assertion nicht vorhanden, aber Citrix Cloud ist so konfiguriert, dass es erwartet wird. Sie haben es versäumt, die unnötigen cip_*-Attribute aus der Citrix Cloud-SAML-Verbindung im Abschnitt "SAML-Attribute"zu entfernen. Trennen Sie die SAML-Verbindung und stellen Sie sie her, um Verweise auf die unnötigen cip_*-Attribute zu entfernen.

Ursache 2: Dieser Fehler kann auch auftreten, wenn es kein entsprechendes AD-Schattenkonto gibt, nach dem die Citrix Cloud Connectors in Ihrer Backend-AD-Gesamtstruktur suchen können. Möglicherweise haben Sie die Frontend-Identität korrekt konfiguriert, aber die Backend-AD-Schattenkontoidentität mit einem übereinstimmenden UPN ist nicht vorhanden oder kann nicht gefunden werden.

Die Anmeldung ist erfolgreich, aber es werden keine DaaS-Ressourcen angezeigt, nachdem sich der Benutzer bei Workspace angemeldet hat

Ursache: Dies wird höchstwahrscheinlich durch falsche UPN-Zuordnungen der Frontend-Identität zum Backend verursacht.

Stellen Sie sicher, dass die beiden UPNs für die Frontend- und Backend-Identitäten genau übereinstimmen und denselben Endbenutzer darstellen, der sich bei Workspace anmeldet. Stellen Sie sicher, dass die DaaS-Bereitstellungsgruppe Zuordnungen zu den richtigen AD-Schattenkontobenutzern oder AD-Gruppen enthält, die diese enthalten.

Beim Start der DaaS-Ressourcen schlägt das FAS-SSON zur den VDAs fehl, die der AD-Domäne beigetreten sind

Beim Versuch, DaaS-Ressourcen zu starten, wird der Workspace-Endbenutzer aufgefordert, seine Windows-Anmeldeinformationen in der GINA einzugeben. Außerdem erscheint die Ereignis-ID 103 in den Windows-Ereignisprotokollen auf Ihren FAS-Servern.

[S103] Server [CC:FASServer] hat UPN [frontenduser@yourforest.com] `SID S-1-5-21-000000000-0000000` angefordert, aber das Lookup gab `SID S-1-5-21-000000000-0000000000-0000000001-0002` zurück. [Korrelation: cc#967472c8-4342-489b-9589-044a24ca57d1]

Ursache: Ihre vereinfachte SAML-Bereitstellung ist von dem "SID-Nichtübereinstimmungsproblem" betroffen. Sie haben Frontend-Identitäten, die SIDs aus einer AD-Gesamtstruktur enthalten, die sich von der AD-Gesamtstruktur des Backend-Schattenkontos unterscheidet.
Senden Sie in der SAML-Assertion nicht **cip_sid**.

Die Anmeldung schlägt für AD-gestützte Benutzer fehl, wenn dasselbe UPN-Suffix in mehreren verbundenen AD-Gesamtstrukturen vorhanden ist

Citrix Cloud verfügt über mehrere Ressourcenstandorte und Connectors, die mit verschiedenen AD-Gesamtstrukturen verbunden sind. Die Anmeldung schlägt fehl, wenn AD-gestützte Benutzer verwendet werden, die aus einer anderen AD-Gesamtstruktur als der Schattenkonto-AD-Gesamtstruktur in Entra ID importiert wurden.

AD-Gesamtstruktur 1 wird mit Entra ID synchronisiert, um Frontend-Benutzer mit UPNs wie `frontenduser@yourforest.com` zu erstellen.

AD-Gesamtstruktur 2 enthält die Backend-Schattenkonten mit UPNs wie `frontenduser@yourforest.com`.

Ursache: Ihre vereinfachte SAML-Bereitstellung ist von dem "UPN-Zweideutigkeitsproblem"betroffen. Citrix Cloud kann nicht ermitteln, welche Connectors verwendet werden sollen, um die Backend-Identität des Benutzers nachzuschlagen.

Senden Sie in der SAML-Assertion nicht **cip_sid**.
Der UPN Ihres Benutzers ist in mehr als einer AD-Gesamtstruktur vorhanden, die mit Citrix Cloud verbunden ist.

On-Premises-PingFederate-Server als SAML-Anbieter für Workspaces und Citrix Cloud konfigurieren

April 26, 2024

Author:
Mark Dear

Dieser Artikel wurde in Zusammenarbeit zwischen den Ingenieuren von Citrix und Ping verfasst und von beiden Parteien überprüft, um die technische Genauigkeit zum Zeitpunkt der Erstellung sicherzustellen. Anweisungen zur Bereitstellung, Konfiguration und Lizenzierung eines On-Premises-PingFederate-Servers zur Verwendung als SAML-Anbieter finden Sie in der Ping-Dokumentation, da dies den Rahmen dieses Artikels sprengen würde.

Dieses Dokument wurde mit den PingFederate-Versionen 11.3 und 12 geschrieben.

Voraussetzungen

Dieser Artikel befasst sich speziell mit der SAML-Konfiguration und stellt sicher, dass die folgenden Bedingungen erfüllt sind.

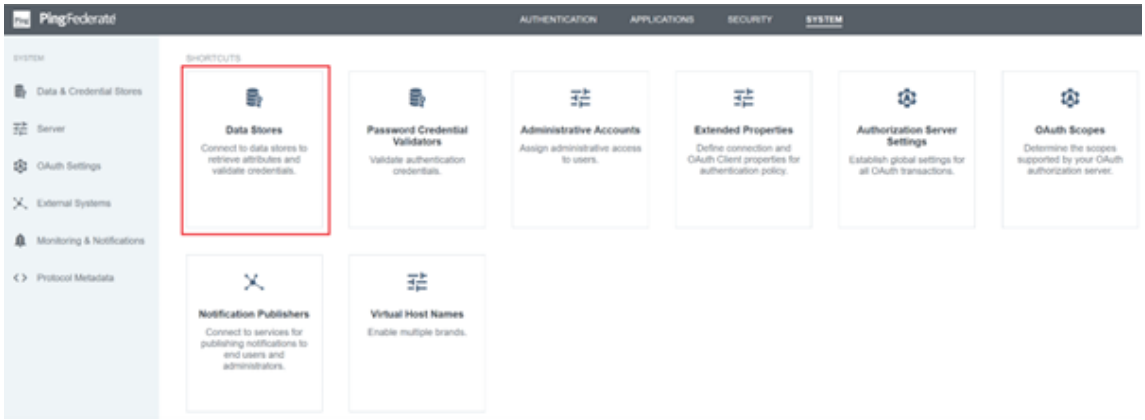
- Sie haben bereits einen On-Premises-PingFederate-Server in Ihrer Organisation bereitgestellt und die erforderliche Lizenz erhalten. Weitere Informationen finden Sie unter PingFederate-Installation.
- Sie müssen eine unterstützte Version von Java auf dem PingFederate-Server installiert haben. Die unterstützten Java-Versionen finden Sie in der Ping Identity-Dokumentation. Weitere Informationen finden Sie unter Anforderung für Java PingFederate.
- Sie haben die erforderlichen Netzwerk- und Firewallregeln so konfiguriert, dass Citrix Cloud und Workspace während des SAML-Anmeldevorgangs für die Workspace/Citrix Cloud-Verwaltungskonsole zum lokalen PingFederate-Server umleiten können. Weitere Informationen finden Sie unter Netzwerkanforderungen für PingFederate.
- Sie haben ein öffentlich signiertes x509-Zertifikat auf Ihren PingFederate-Server importiert, das als Serverzertifikat für den PingFederate-Server dienen kann.
- Sie haben ein öffentlich signiertes x509-Zertifikat auf Ihren PingFederate-Server importiert, das als SAML-Signaturzertifikat für den IdP dienen kann. Dieses Zertifikat muss während des SAML-Verbindungsprozesses in Citrix Cloud hochgeladen werden.

- Sie haben Ihr On-Premises Active Directory mit PingFederate verbunden. Weitere Informationen finden Sie unter PingFederate LDAP Datastore.

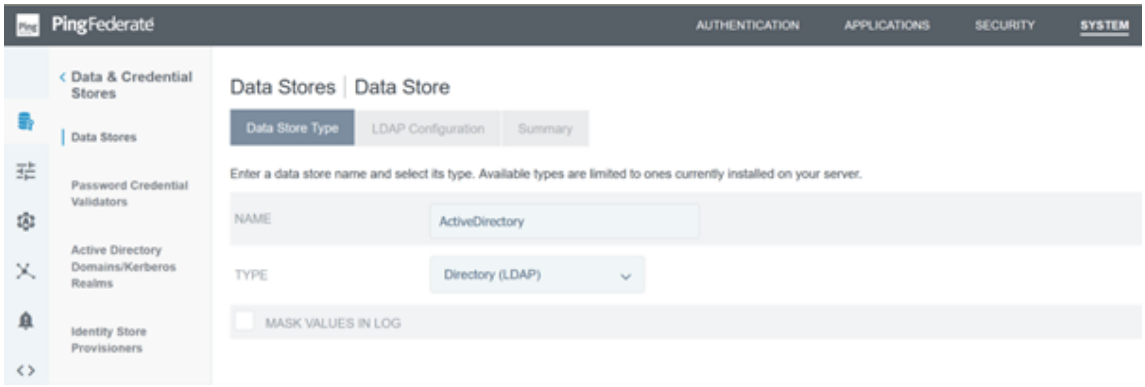
> **Hinweis:**
>
> Lesen Sie bei der Konfiguration von PingFederate für die Verwendung mit Citrix Cloud und Workspace in der PingFederate-Dokumentation nach, was die einzelnen SAML-Einstellungen bewirken, damit Sie gegebenenfalls die hier bereitgestellten Anweisungen ergänzen.

Active Directory-Verbindung zu Ihrer AD-Domain mit DataStore in PingFederate konfigurieren

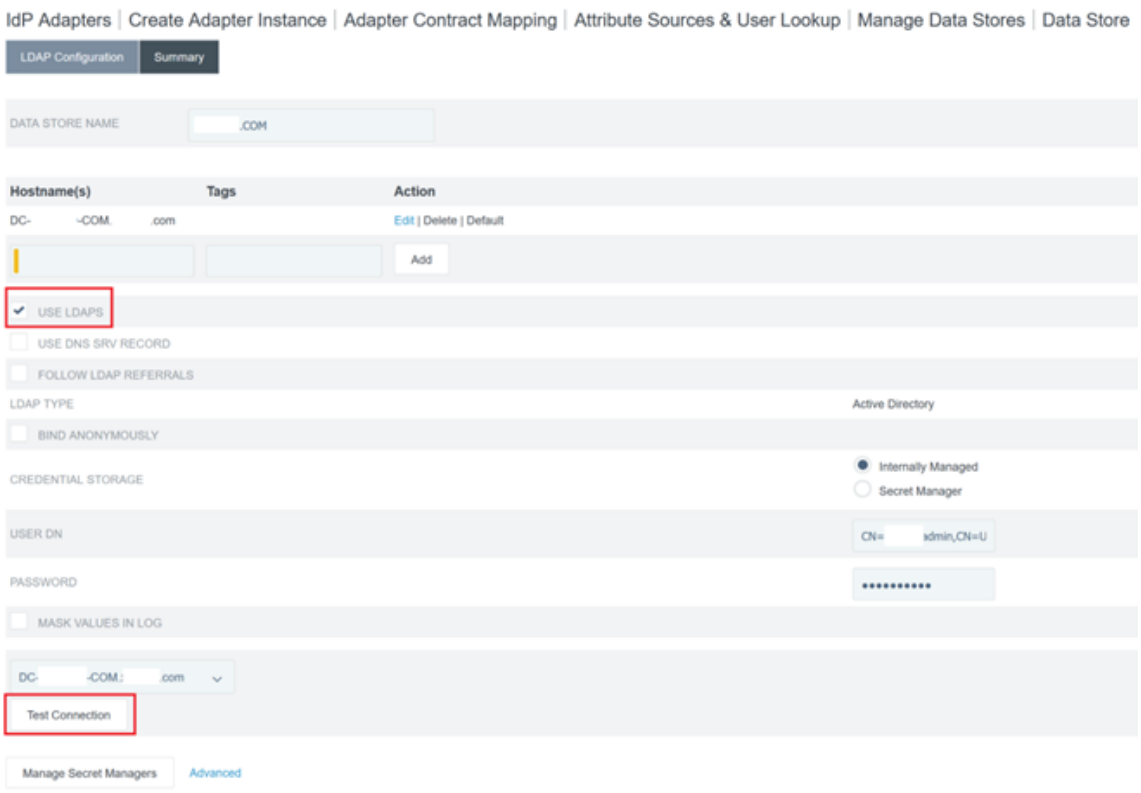
1. Konfigurieren Sie eine Active Directory-Verbindung innerhalb von Data Stores.



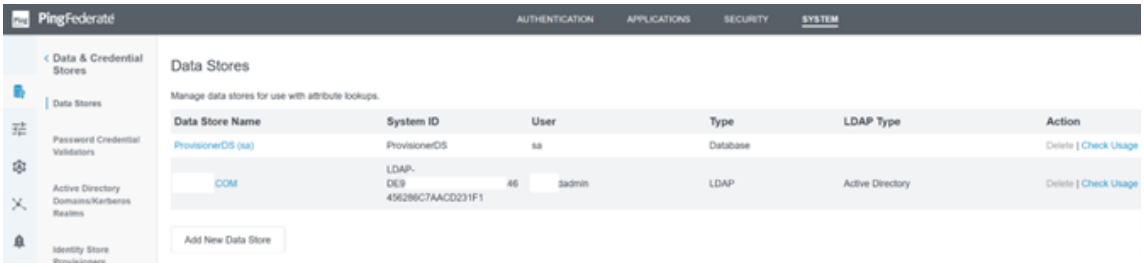
2. Wählen Sie als Typ **Verzeichnis (LDAP)** aus.



3. Konfigurieren Sie Ihre Domänencontroller für LDAPS-Verbindungen und fügen Sie Ihre Liste der Domänencontroller-FQDNs in das Feld “Hostnamen”ein. Klicken Sie dann auf **Verbindung testen**.

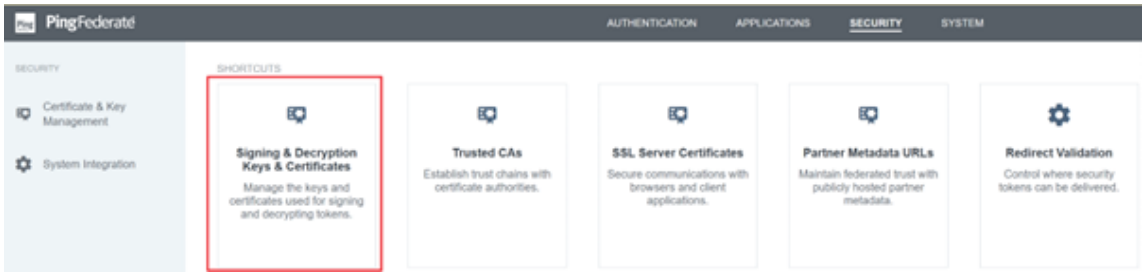


4. Nach der Konfiguration muss die Active Directory-Verbindung so aussehen, wie im folgenden Beispiel gezeigt:



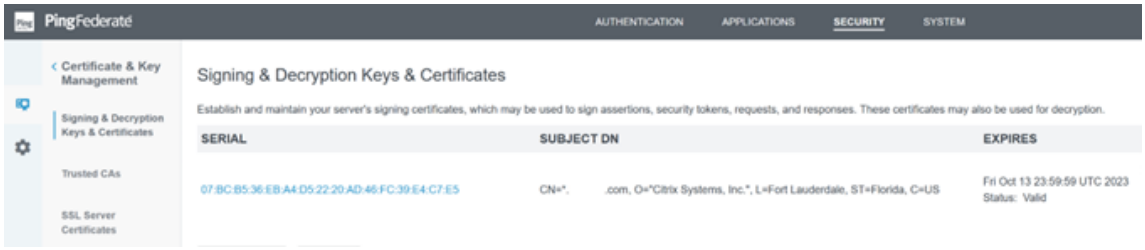
Citrix Cloud SAML-Signaturzertifikat hochladen

1. Klicken Sie auf die Registerkarte **Sicherheit**.
2. Laden Sie das SAML-Signaturzertifikat hoch, das PingFederate in **Signing & Decryption Keys and Certificates** verwenden soll.

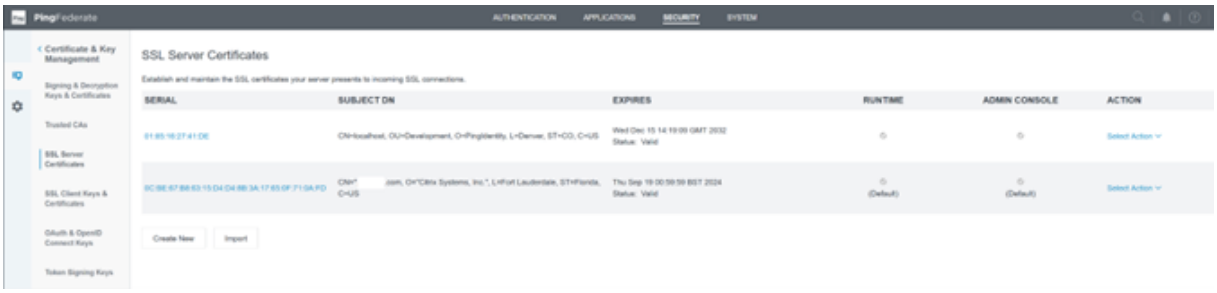


> **Hinweis:**
>
> Das verwendete Zertifikat ist in diesem Beispiel ein öffentlich signiertes Digicert-Zertifikat `pingfederateserver.domain.com`.

3. Laden Sie alle ZS-Zertifikate hoch, die zum Signieren Ihres PingFederate-Server-SAML-Signaturzertifikats verwendet wurden.



> **Hinweis:**
>
> Das PingFederate-Serverzertifikat und das SAML-Signaturzertifikat können dasselbe SSL-Zertifikat sein, oder Sie können verschiedene SSL-Zertifikate verwenden. Sie müssen Citrix Cloud eine Kopie des SAML-Signaturzertifikats zur Verfügung stellen, wenn Sie die SAML-Verbindung konfigurieren.

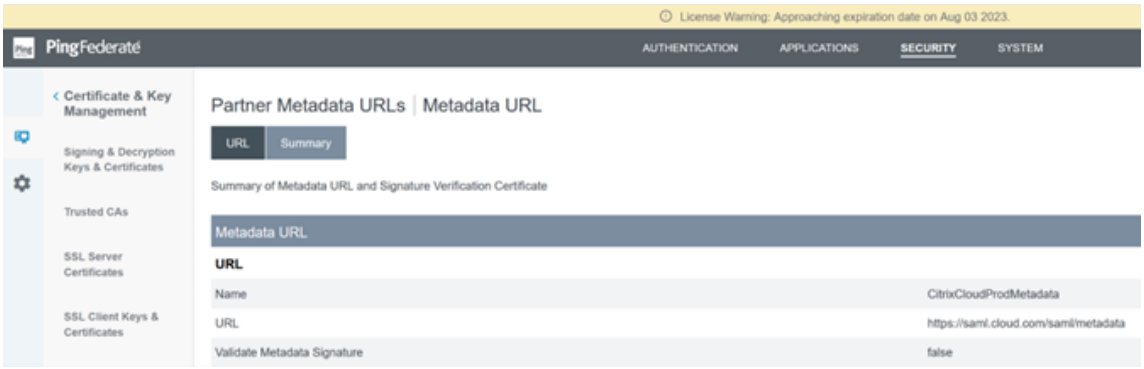


Laden Sie die Citrix Cloud-Metadaten hoch

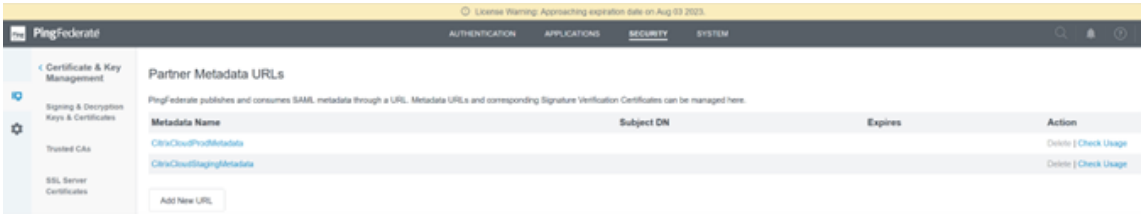
1. Geben Sie einen Namen für die Citrix Cloud-Metadaten ein und geben Sie die Metadaten-URL ein, die der Citrix Cloud-Region entspricht, in der sich Ihr Citrix Cloud-Mandant befindet.

    - https://saml.cloud.com/saml/metadata – Kommerzielle Lizenzen EU, USA und APS

- https://saml.citrixcloud.jp/saml/metadata – Japan
- https://saml.cloud.us/saml/metadata – US-Regierung



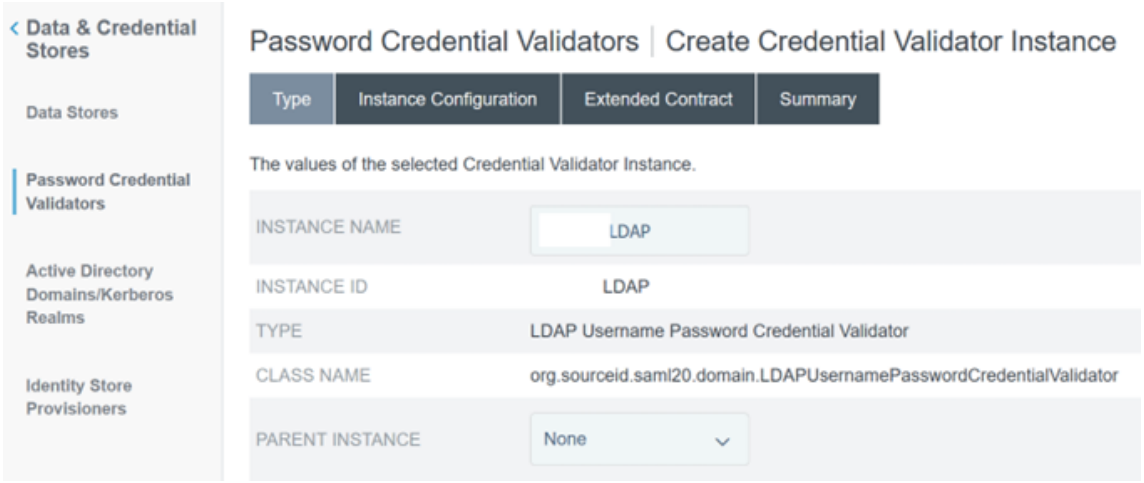
2. Nach der Konfiguration sieht die Citrix Cloud-Metadatenkonfiguration etwa wie folgt aus:



Prüfung der Anmeldeinformationen mit Kennwort in PingFederate

Weitere Informationen finden Sie unter Prüfung der Anmeldeinformationen mit Kennwort in PingFederate

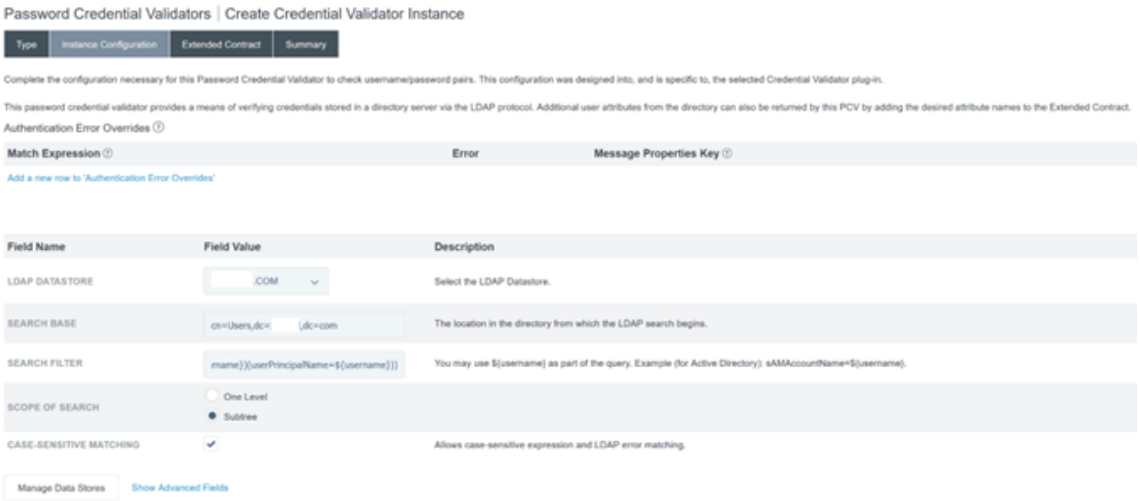
1. Konfigurieren Sie den Typ der Prüfung der Anmeldeinformationen als LDAP-Benutzername und -Kennwort.



2. Konfigurieren Sie die **Instanzkonfiguration**. Wählen Sie die AD-Domänenverbindung und den Datenspeicher aus, die Sie zuvor unter Active Directory-Verbindung zu Ihrer AD-Domain

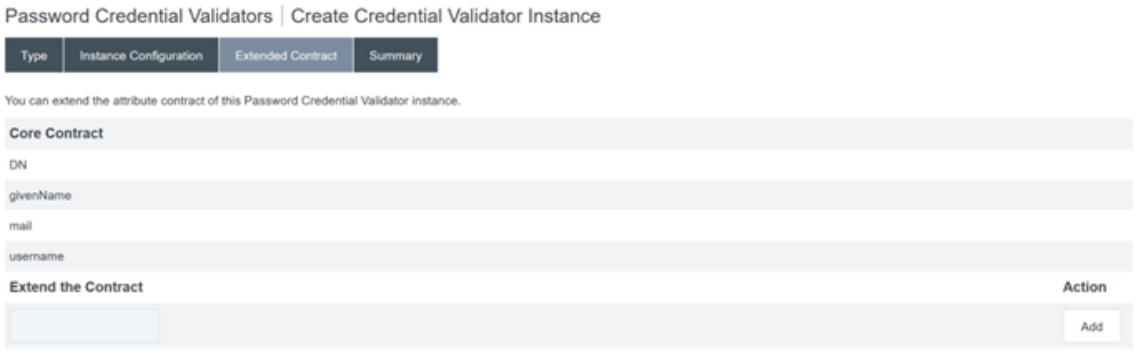
mit DataStore in PingFederate konfigurieren konfiguriert haben. Geben Sie einen geeigneten LDAP-Filter ein, wie im Beispiel gezeigt.

```
(((sAMAccountName=${ username } )(userPrincipalName=${ username } ))
```

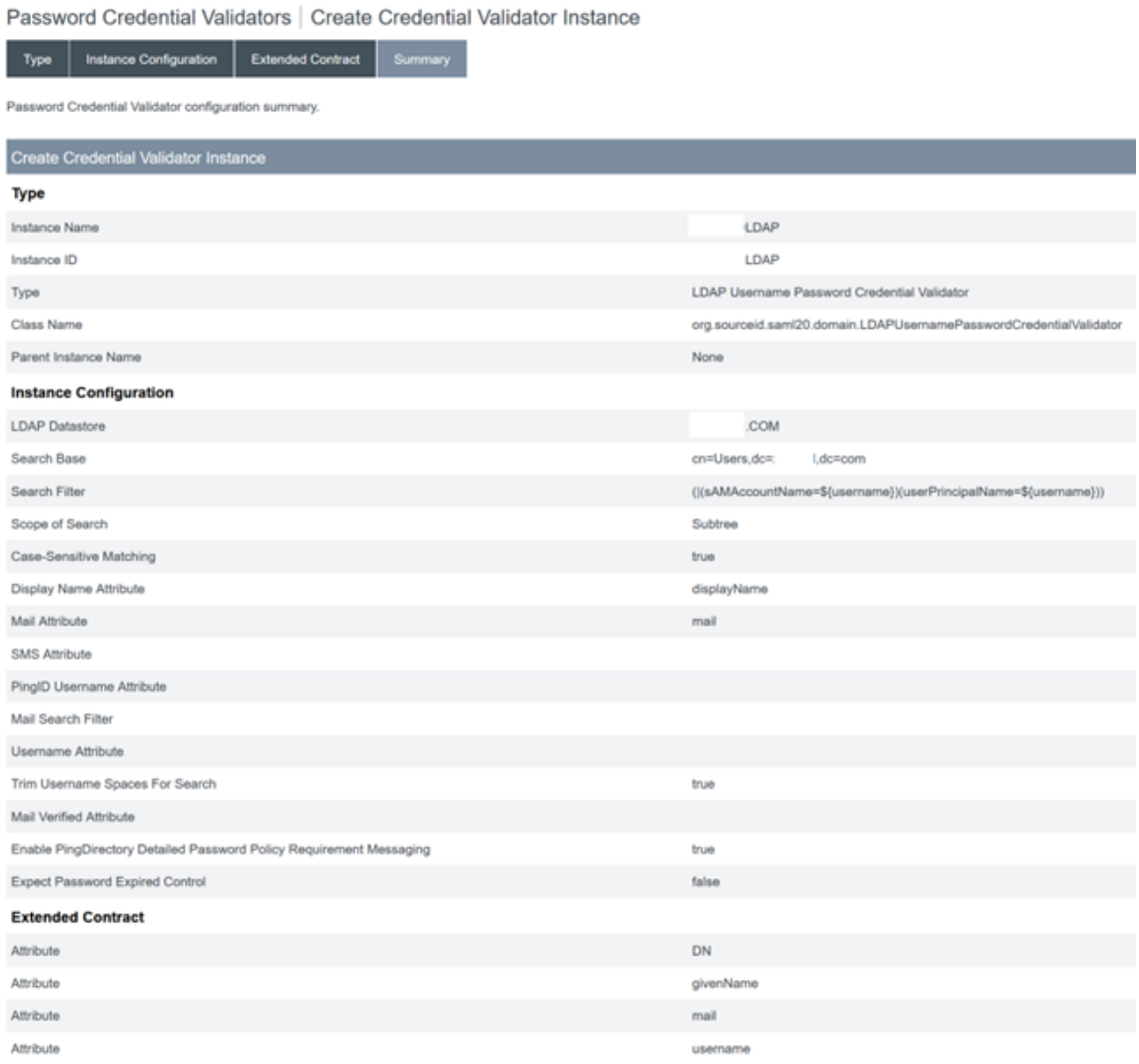


> **Hinweis:** Der Beispielfilter unterstützt die AD-Benutzernamensformate sAMAccount-Name und userPrincipalName. Endbenutzer können sich daher mit einem dieser Formate bei Workspace oder Citrix Cloud anmelden. Der Beispielfilter unterstützt die AD-Benutzernamensformate sAMAccountName und userPrincipalName. Endbenutzer können sich daher mit einem dieser Formate bei Workspace oder Citrix Cloud anmelden.

3. Konfigurieren Sie den **erweiterten Vertrag**.



4. Die Zusammenfassung der **Prüfung der Anmeldeinformationen mit Kennwort** sieht danach etwa wie folgt aus:



Password Credential Validators | Create Credential Validator Instance

Type | Instance Configuration | Extended Contract | Summary

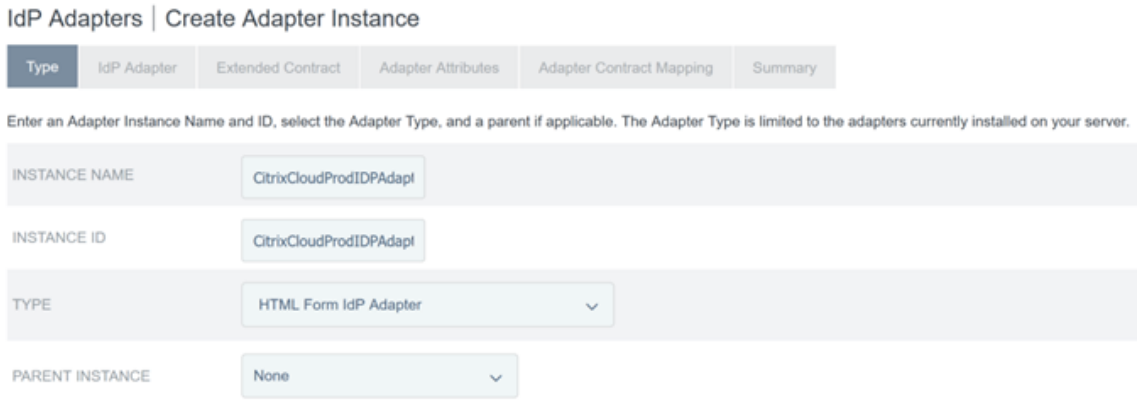
Password Credential Validator configuration summary.

Create Credential Validator Instance	
Type	
Instance Name	LDAP
Instance ID	LDAP
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None
Instance Configuration	
LDAP Datastore	.COM
Search Base	cn=Users,dc= l,dc=com
Search Filter	(|(sAMAccountName=${username})(userPrincipalName=${username}))
Scope of Search	Subtree
Case-Sensitive Matching	true
Display Name Attribute	displayName
Mail Attribute	mail
SMS Attribute	
PingID Username Attribute	
Mail Search Filter	
Username Attribute	
Trim Username Spaces For Search	true
Mail Verified Attribute	
Enable PingDirectory Detailed Password Policy Requirement Messaging	true
Expect Password Expired Control	false
Extended Contract	
Attribute	DN
Attribute	givenName
Attribute	mail
Attribute	username

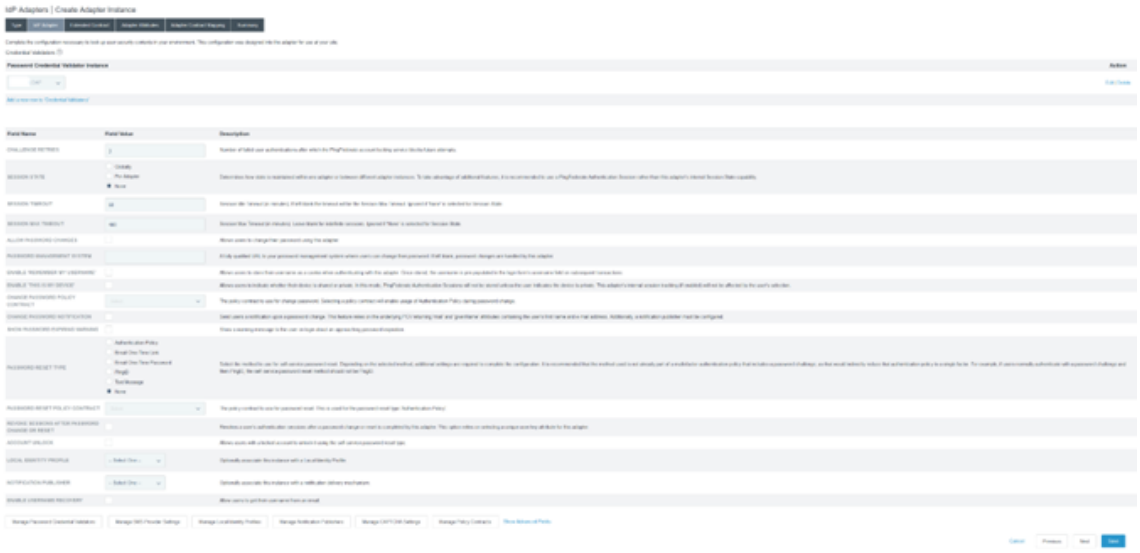
IDP-Adapter in PingFederate konfigurieren

Weitere Informationen finden Sie unter PingFederate HTML-Formularadapter.

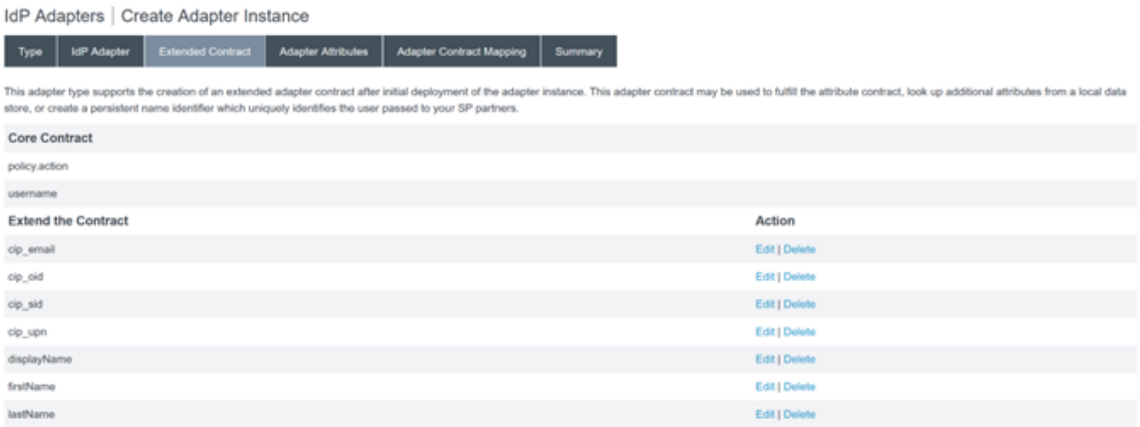
1. Erstellen Sie einen neuen IDP-Adapter vom Typ HTML Form IdP Adapter.



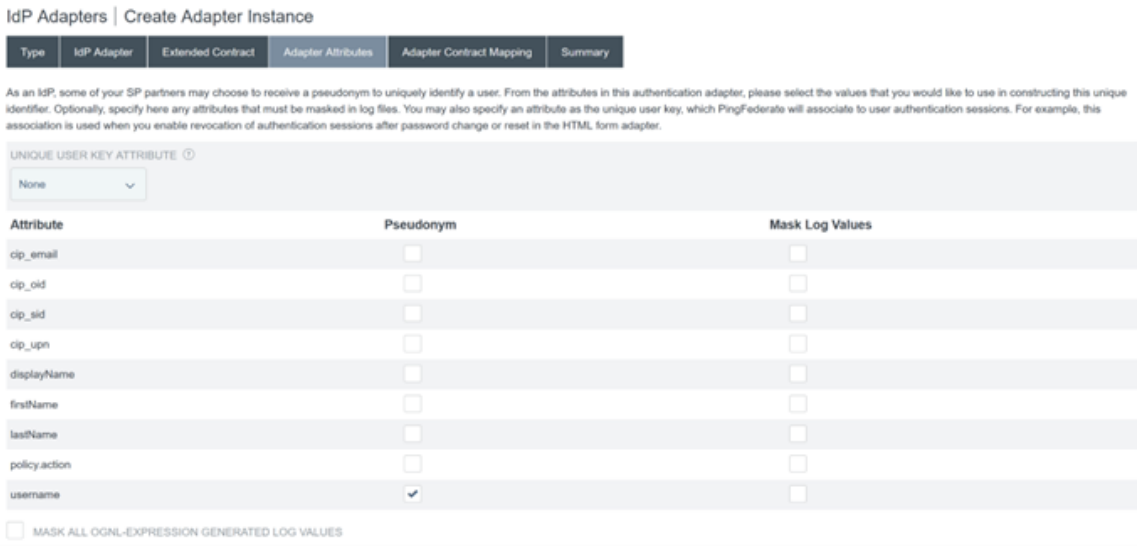
2. Wählen Sie die vorher konfigurierte **Prüfung der Anmeldeinformationen mit Kennwort** aus, die Sie zuvor konfiguriert haben, und konfigurieren Sie den IDP-Adapter. Weitere Informationen finden Sie unter Prüfung der Anmeldeinformationen mit Kennwort in PingFederate.



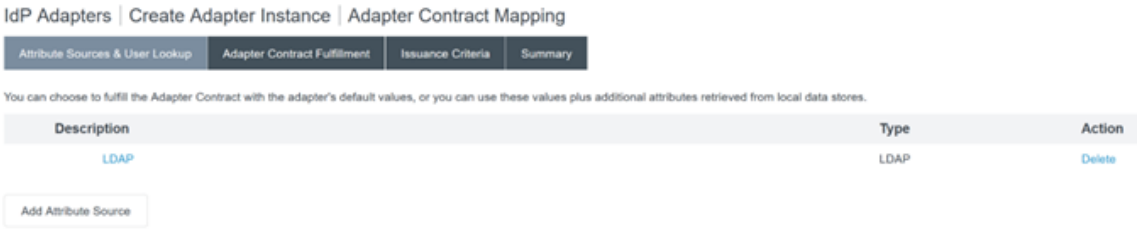
3. Konfigurieren Sie den **erweiterten Vertrag** mit SAML-Attributen, die bei der SAML-Anmeldung an Citrix Cloud oder Workspaces übergeben werden.



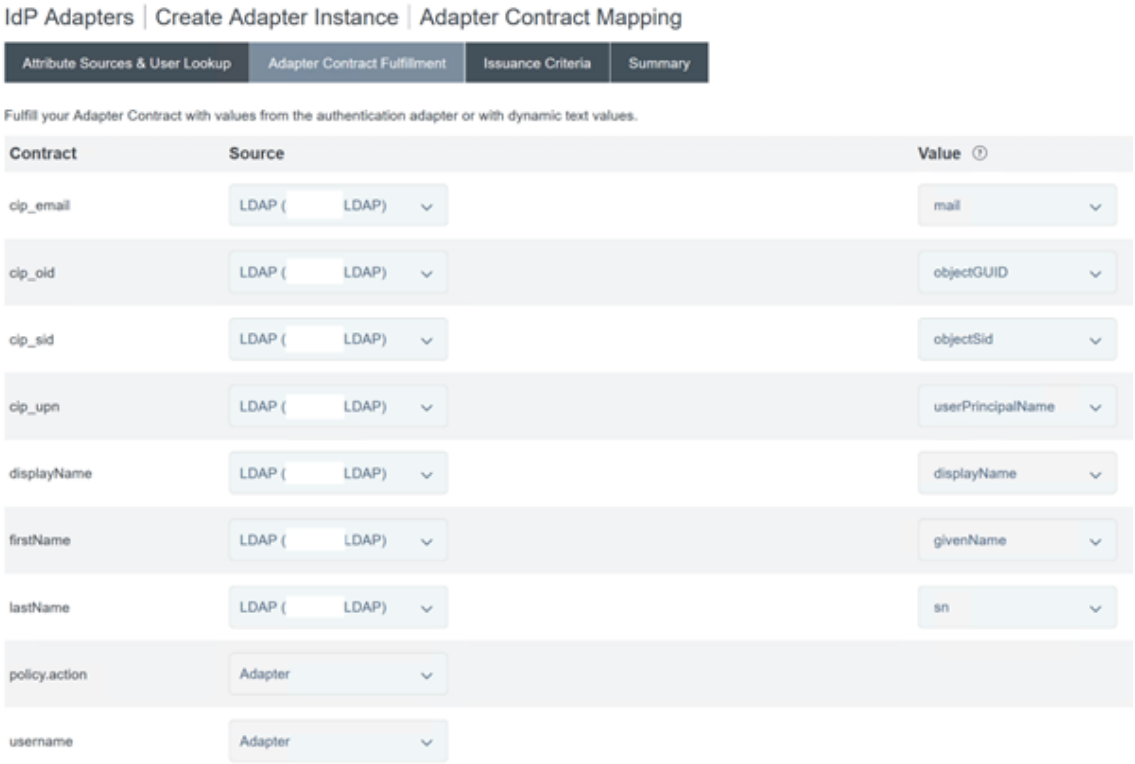
4. Konfigurieren Sie **Adapter Attributes**.



5. Konfigurieren Sie **Adapter Contract Mapping**, bei der SAML-Attribute LDAP-Benutzerattributen von AD-Identitäten zugeordnet werden. Klicken Sie auf **Configure the adapter contract**.
6. Konfigurieren Sie **Attribute Sources & User Lookup**.



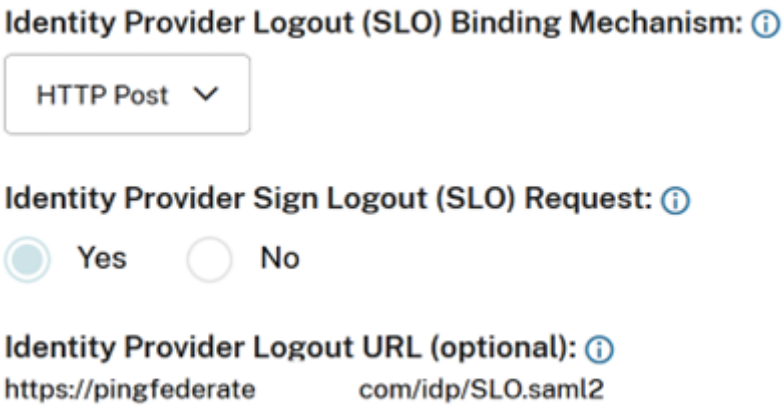
7. Konfigurieren Sie **Adapter Contract Fulfilment**. Wählen Sie **LDAP** und den Namen Ihres Active Directory-Datenspeichers als Quelle der Benutzerattributdaten aus. “Value”ist das Active Directory-Attribut für den Benutzer, z. B. `objectGUID` oder `objectSid`.



Service Provider Connection (SAML-Anwendung) für Citrix Cloud oder Workspaces konfigurieren

Die unten angegebene PingFederate-Beispielkonfiguration setzt die folgenden SAML-Authentifizierungsanforderun in Ihrer Organisation voraus.

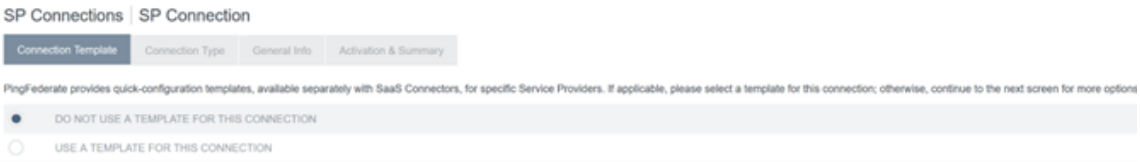
- SAML-Authentifizierungsanforderungen, die von der Workspace/Citrix Cloud-Verwaltungskonsole gesendet werden, MÜSSEN signiert werden.
- SAML-HTTP-POST-Bindungen werden sowohl für SSO- als auch für SLO-Anfragen verwendet.
- Single Logout (SLO) ist eine Anforderung in Ihrem Unternehmen. Wenn sich ein Endbenutzer von Workspace oder der Citrix Cloud-Verwaltungskonsole abmeldet, wird eine SAML-SLO-Anforderung von Citrix Cloud an den SAML-Anbieter (IdP) gesendet, um den Benutzer abzumelden.
- PingFederate benötigt signierte HTTP-POST-Anforderungen, um die Abmeldung zu initiieren. Der SAML-Anbieter benötigt signierte SLO-Anfragen.



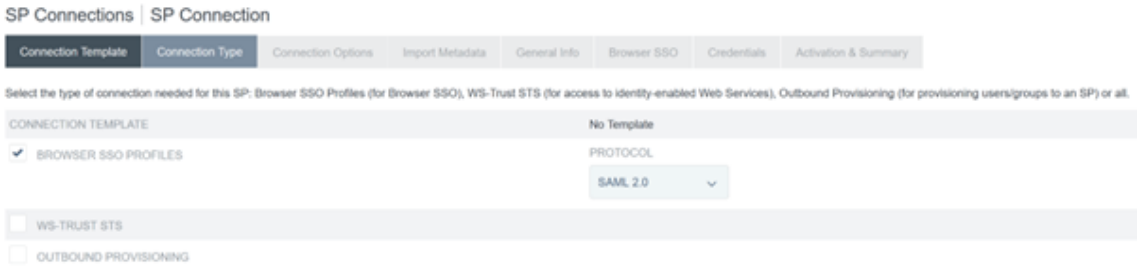
Weitere Informationen finden Sie unter PingFederate SP-Verwaltung

Verfahren

1. Konfigurieren Sie die Registerkarte **Connection Template**.

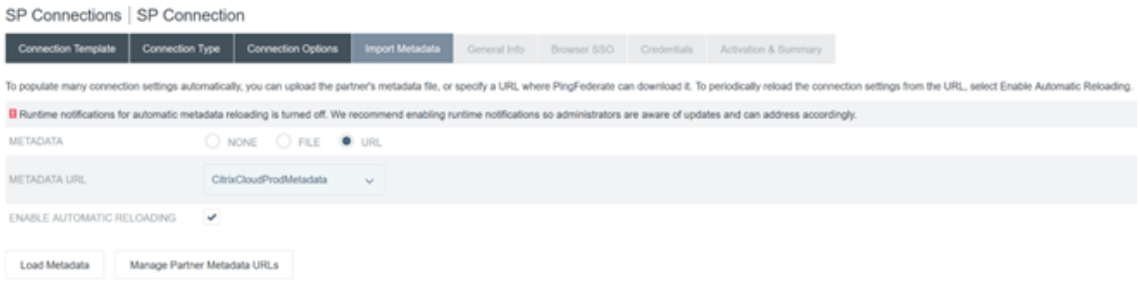


2. Konfigurieren Sie die Registerkarte **Connection Type** und wählen Sie **Browser-SSO-Profile und SAML 2.0** aus.



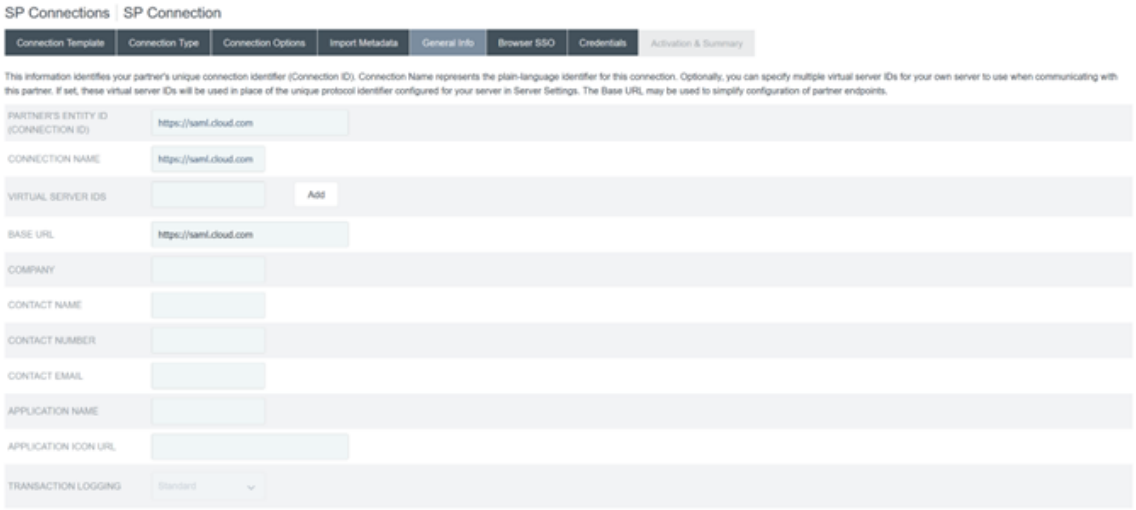
3. Konfigurieren Sie die Registerkarte **Connection Options**.

4. Importieren Sie die Citrix Cloud-Metadaten. Wählen Sie URL und die URL `CitrixCloudProdMetadata`, die Sie zuvor erstellt haben, und klicken Sie auf **Load Metadata**.

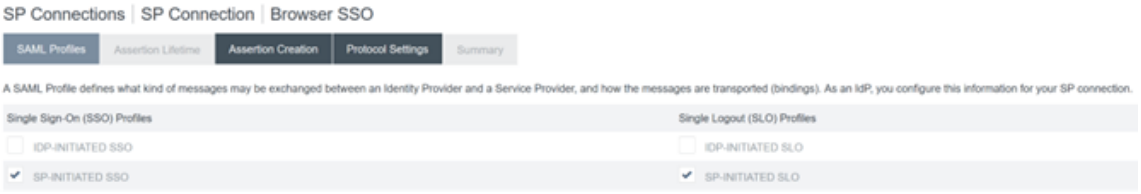


5. Konfigurieren Sie die Registerkarte **General Info**. Stellen Sie die Service Provider-Verbindungsentitäts-ID, die Basis-URL und den Verbindungsnamen auf den Citrix Cloud-SAML-Endpunkt für Ihre Citrix Cloud-Kundenregion ein.

   - https://saml.cloud.com – Kommerzielle Lizenzen EU, USA und APS
   - https://saml.citrixcloud.jp – Japan
   - https://saml.cloud.us – US-Regierung



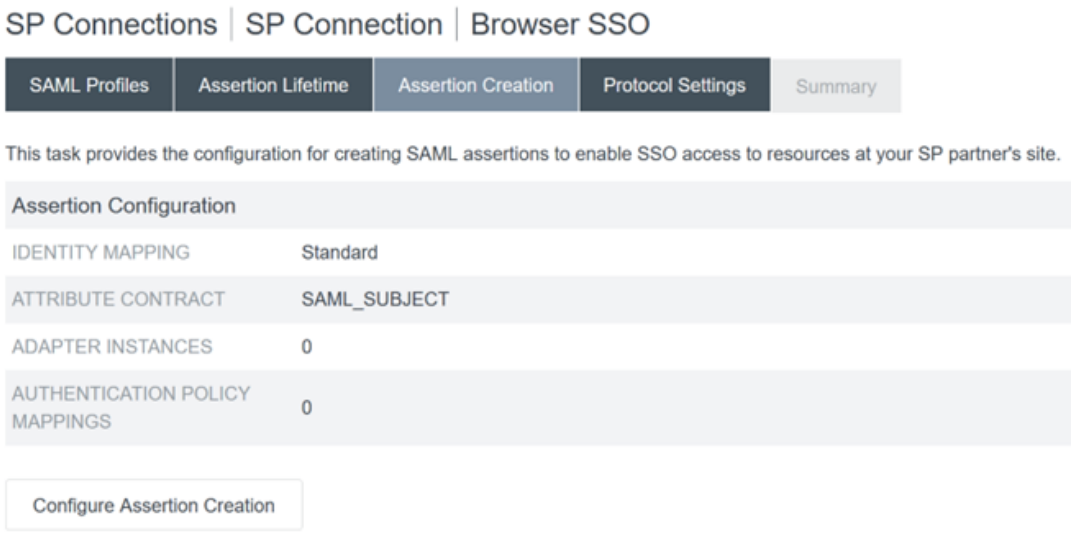
6. Konfigurieren Sie die **Protokolleinstellungen**.



7. Verwenden Sie die Standardeinstellungen für **Assertion Lifetime** .

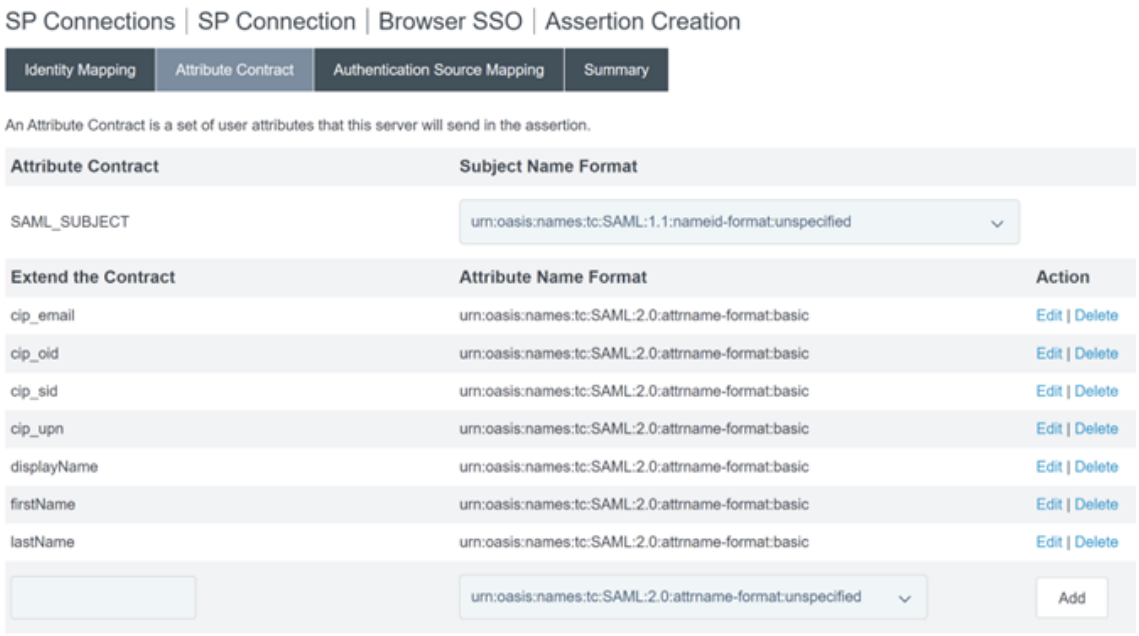
8. Konfigurieren Sie die SAML-Assertionserstellung.

   a) Klicken Sie auf **Configure Assertion Creation**.



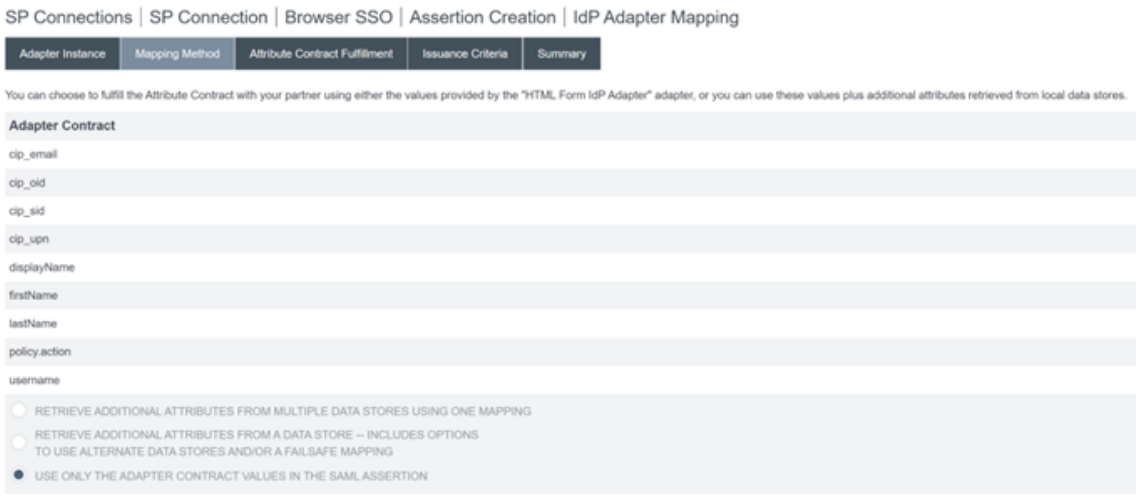
   b) Wählen Sie **Standard** aus.

9. Konfigurieren Sie die Registerkarte **Attribute Contract**.

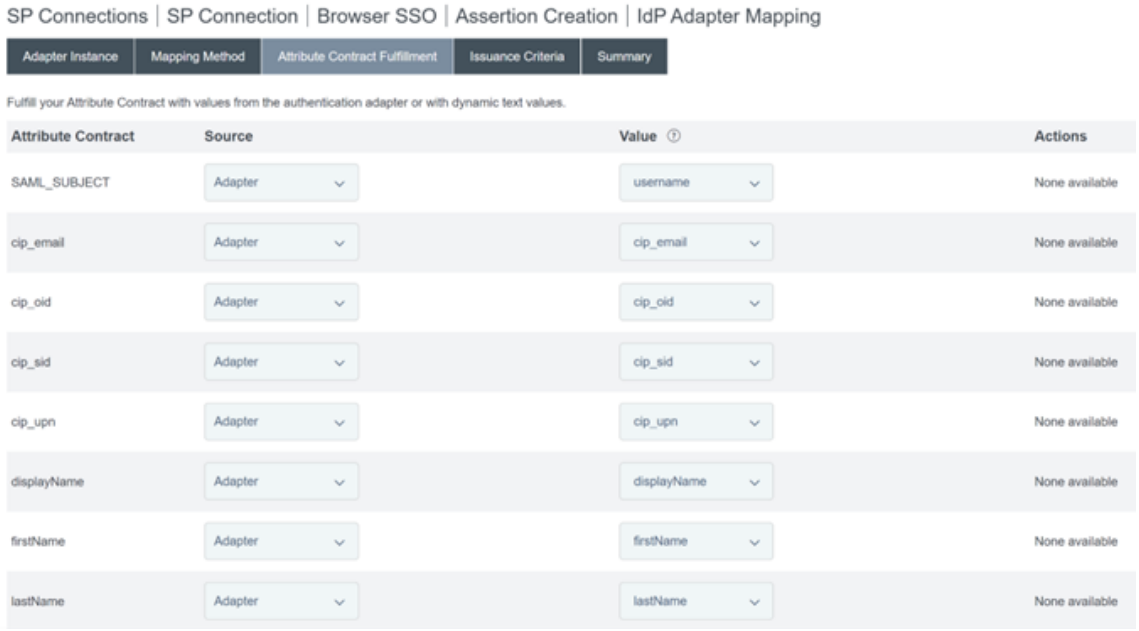


10. Konfigurieren Sie die Registerkarte **Adapter Instance**.

11. Konfigurieren Sie die Registerkarte **Mapping Method**.



12. Konfigurieren Sie die Registerkarte **Attribute Contract Fulfilment**.

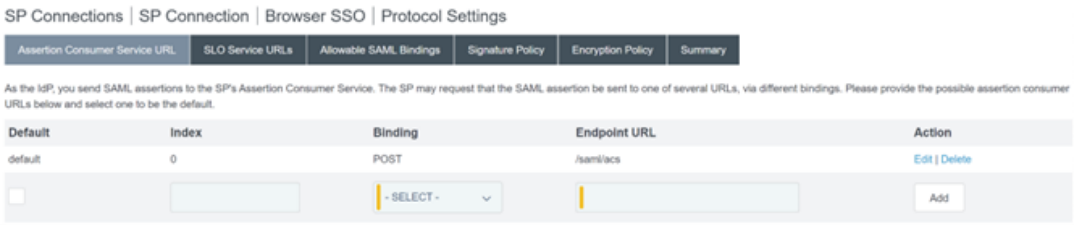


13. Konfigurieren Sie die Registerkarte **Issuance Criteria** mit den Standardkriterien ohne Bedingungen.

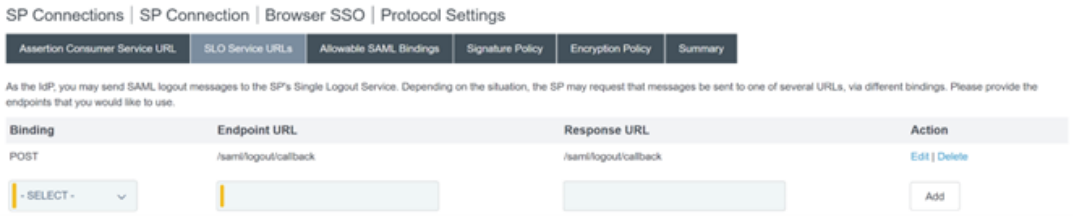
14. Die abgeschlossene **IDP-Adapterzuordnung** sieht wie folgt aus:
15. Konfigurieren Sie die **Protokolleinstellungen**. Die von Citrix Cloud benötigten SAML-Pfade werden an die Basis-URL Ihres PingFederate-Servers angehängt. Sie können die Basis-URL über-

schreiben, indem Sie einen vollständigen Pfad in das Feld für die Endpunkt-URL eingeben. Dies ist jedoch normalerweise unnötig und unerwünscht.
Basis-URL – https://youpingfederateserver.domain.com

a) Konfigurieren Sie die Assertion Consumer Service-URL, die den SAML-Pfad an die Basis-URL des PingFederate-Servers anhängt. EndpointURL – `/saml/acs`

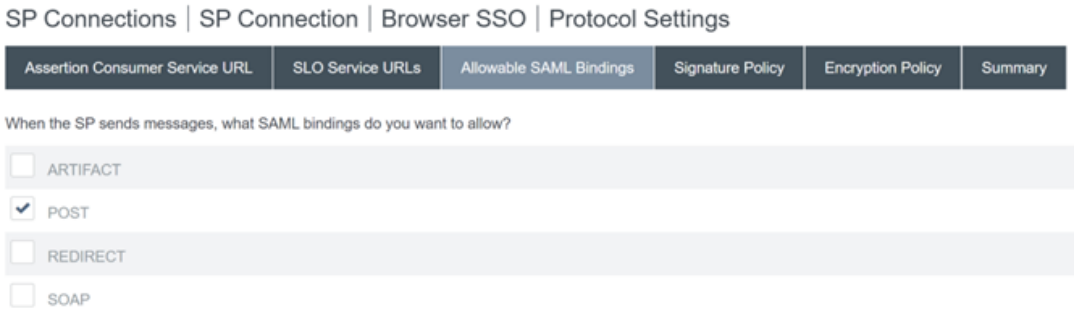


b) Konfigurieren Sie die Registerkarte **SLO Service URL**. EndpointURL – `/saml/logout/callback`

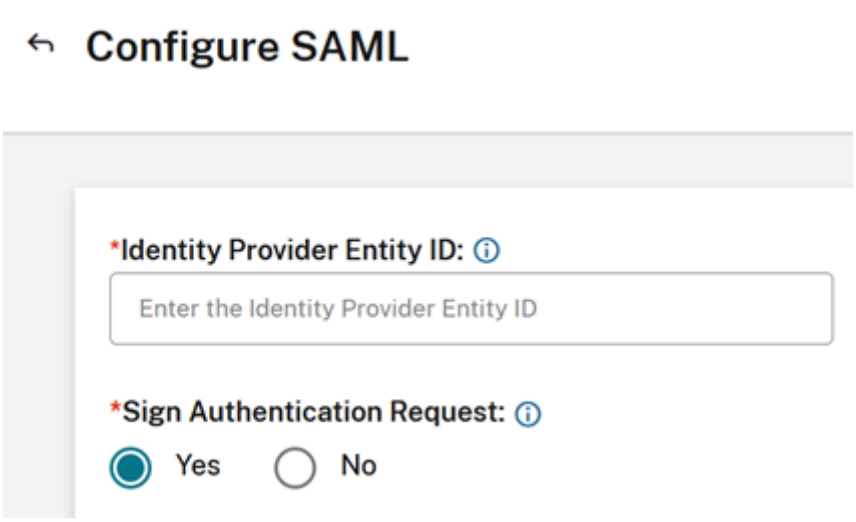


> **Wichtig:**
>
> Für die Citrix Cloud SAML-Verbindung muss eine PingFederate-Abmelde-URL als Entsprechung konfiguriert werden, wenn Sie beim Abmelden von Workspace oder Citrix Cloud SLO ausführen möchten. Wenn Sie die Abmelde-URL in Ihrer SAML-Verbindung nicht konfigurieren, melden sich Endbenutzer einfach von Workspace ab, aber nicht von PingFederate.

a) Konfigurieren Sie die Registerkarte **Allowable SAML Bindings**.

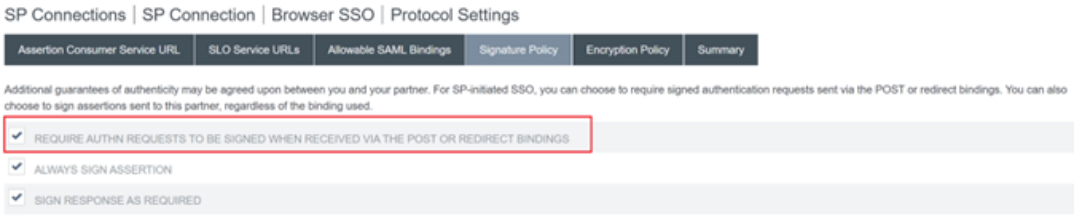


b) Konfigurieren Sie die Registerkarte **Signature Policy**.

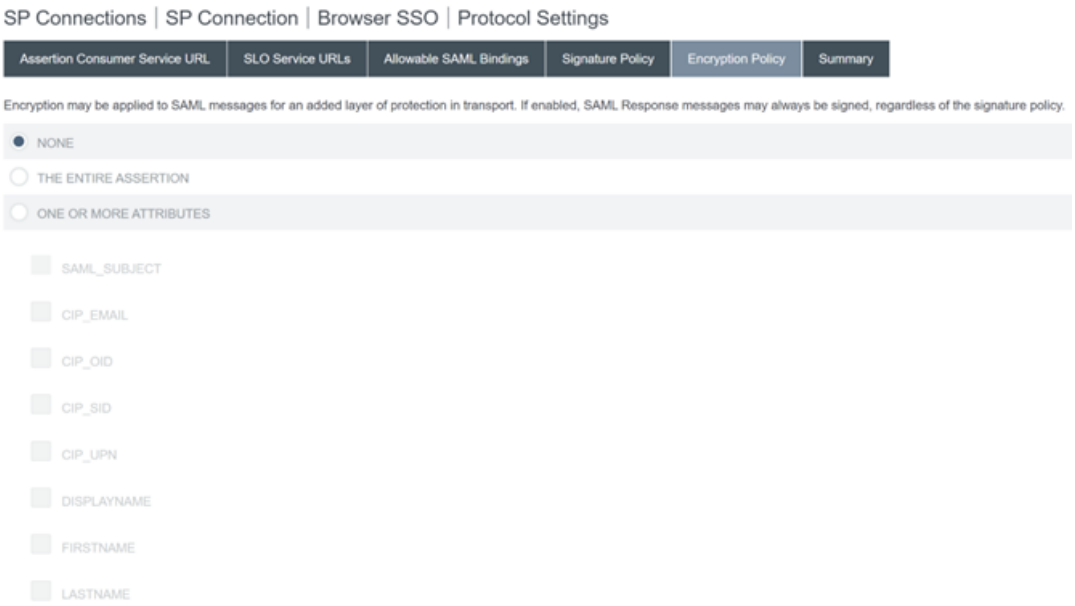


> **Wichtig:**
>
> Die SAML-Signatureinstellungen müssen auf beiden Seiten der SAML-Verbindung konsistent konfiguriert werden. Workspace oder Citrix Cloud (SP) müssen so konfiguriert sein, dass signierte SSO- und SLO-Anforderungen gesendet werden.

a) PingFederate (IDP) muss so konfiguriert sein, dass signierte Anforderungen über das Citrix Cloud SAML-Signaturverifizierungszertifikat durchgesetzt werden.

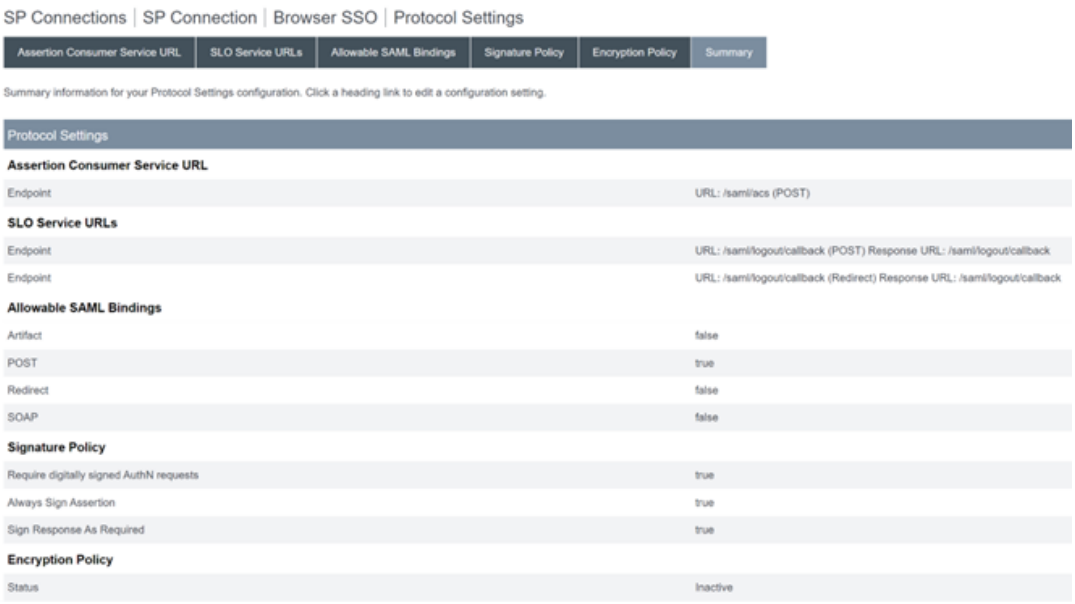


b) Konfigurieren Sie die Registerkarte **Encryption Policy**.

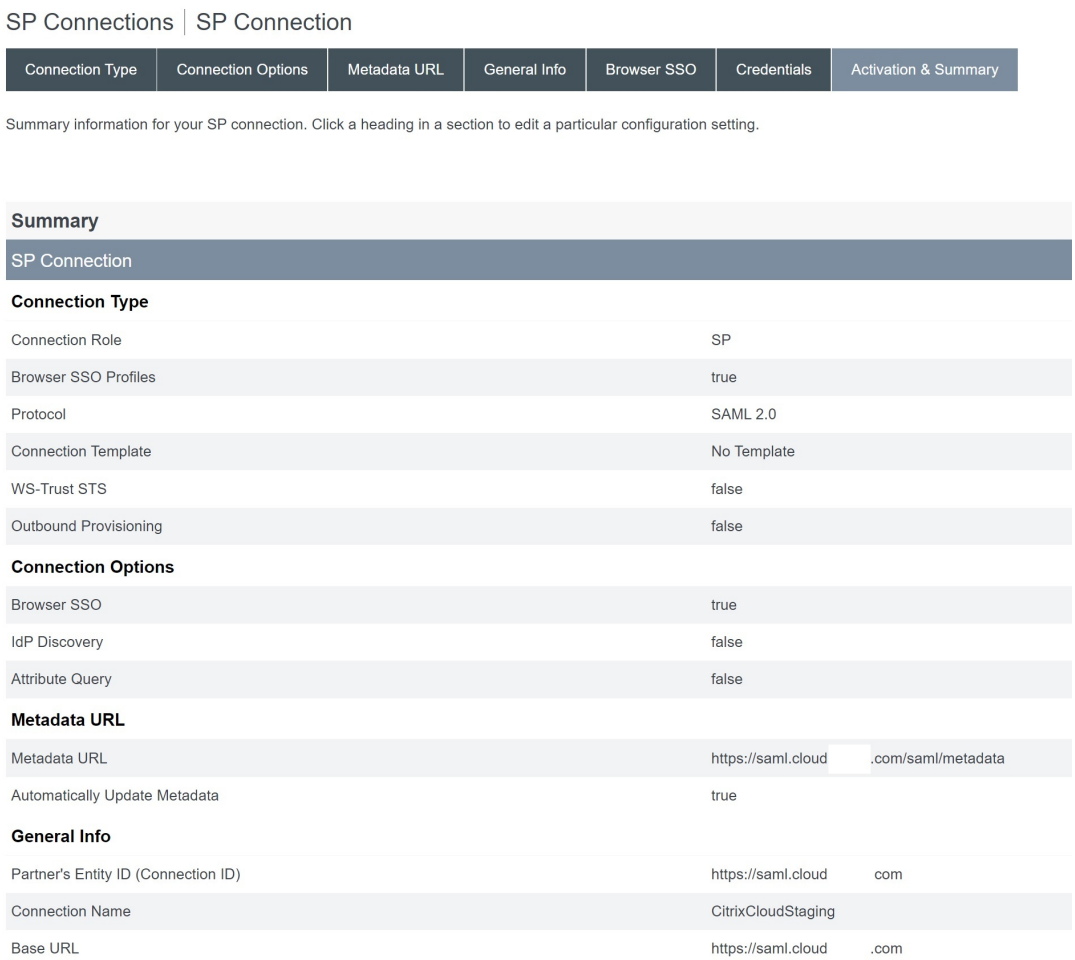


> **Hinweis:**
>
> Es wird empfohlen, die Verschüsselung bei der Ersteinrichtung und beim Testen auf **NONE** zu setzen, damit Sie alle Probleme mit fehlenden oder falschen SAML-Attributen in der Assertion debuggen können. Wenn Sie verschlüsselte Assertions benötigen, wird empfohlen, die Verschlüsselung zu aktivieren, nachdem Sie nachgewiesen haben, dass die Anmeldung bei Workspace oder Citrix Cloud erfolgreich war und alle Ressourcen erfolgreich aufgelistet wurden und gestartet werden können. Das Debuggen von Problemen mit SAML bei aktivierter Verschlüsselung ist unmöglich, wenn Sie den Klartext-Inhalt der SAML-Assertion nicht einsehen können.

c) Überprüfen Sie die Registerkarte **Summary**.

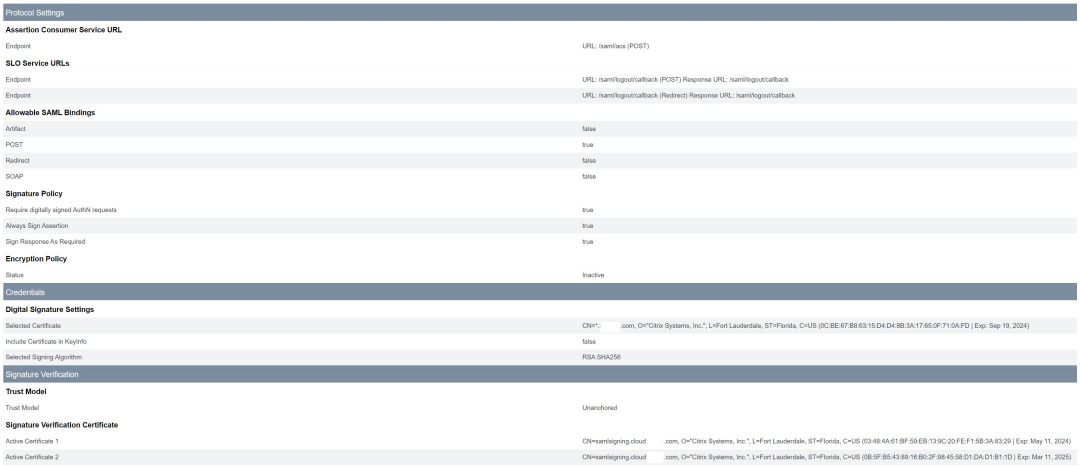


d) Überprüfen Sie die **Citrix Cloud Service Provider-Verbindung**. Sobald die **Citrix Cloud Service Provider-Verbindung** konfiguriert ist, sollte sie wie in diesem Beispiel aussehen:



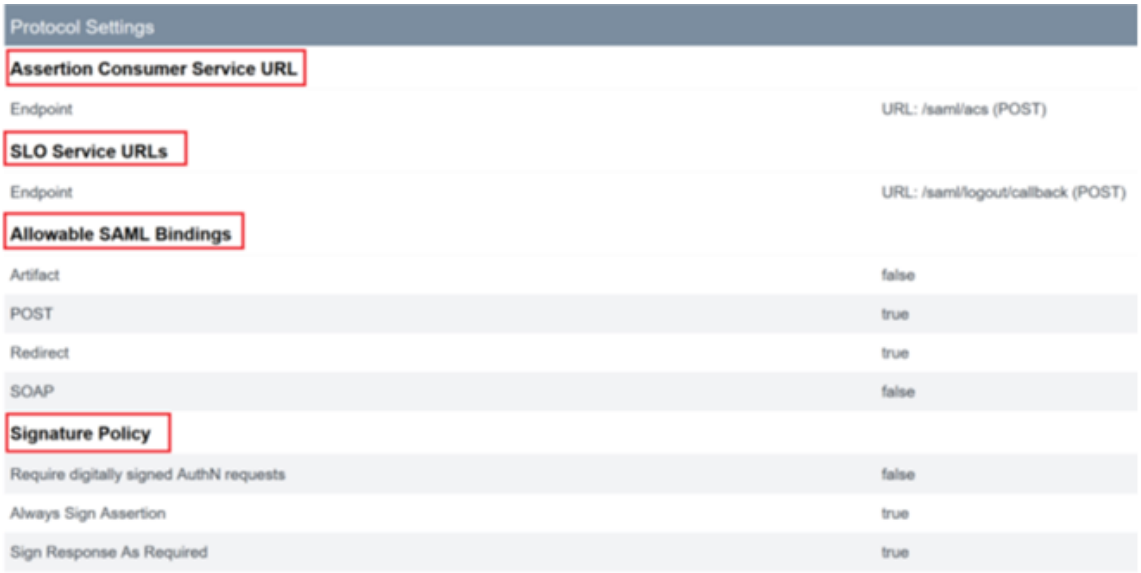
Browser SSO	
SAML Profiles	
IdP-Initiated SSO	false
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	true
Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	cip_email
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_oid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_sid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_upn
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	displayName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	firstName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	lastName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Authentication Source Mapping	
Adapter instance name	CitrixCloudStagingIDPAdaptor
Adapter Instance	
Selected adapter	CitrixCloudStagingIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
cip_email	cip_email (Adapter)
cip_oid	cip_oid (Adapter)
cip_sid	cip_sid (Adapter)
cip_upn	cip_upn (Adapter)
displayName	displayName (Adapter)
firstName	firstName (Adapter)
lastName	lastName (Adapter)
Issuance Criteria	
Criterion	(None)



Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive
Credentials	
Digital Signature Settings	
Selected Certificate	CN=*. .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0C:BE:67:B8:63:15:D4:D4:8B:3A:17:65:0F:71:0A:FD | Exp: Sep 19, 2024)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256
Signature Verification	
Trust Model	
Trust Model	Unanchored
Signature Verification Certificate	
Active Certificate 1	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (03:48:4A:61:BF:59:EB:13:9C:20:FE:F1:5B:3A:83:29 | Exp: May 11, 2024)
Active Certificate 2	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0B:5F:B5:43:89:16:B0:2F:98:45:58:D1:DA:D1:B1:1D | Exp: Mar 11, 2025)

> **Nützlicher Hinweis:**
>
> Verwenden Sie die Seite “SP Connection Activation”und “Summary”, um Ihre SAML-Anwendung zu überprüfen und für das Debugging, da auf diese Weise schnelle und einfache Konfigurationsänderungen vorgenommen werden können. Auf der Seite „SP-Verbindungsaktivierung und Zusammenfassung“können Sie zu einem der Unterabschnitte der SAML-Konfiguration navigieren, indem Sie auf den Titel dieses Abschnitts klicken. Klicken Sie auf einen der rot hervorgehobenen Titel, um diese Einstellungen zu aktualisieren.



Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	true

16. Die abgeschlossene **Citrix Cloud SP-Verbindung** sollte wie folgt in der Liste erscheinen.

17. Die SP-Verbindung kann im Format einer XML-Datei exportiert werden. Citrix empfiehlt, ein Backup Ihrer SP-Verbindung zu erstellen, nachdem Sie sie mit Citrix Cloud und Workspace getestet haben.

Aktualisieren Sie das SAML-Signaturzertifikat des Identitätsanbieters

May 31, 2024

Author:
Mark Dear

SAML-Verbindungen, die signierte Anforderungen und Antworten verwenden, hängen von zwei verschiedenen SAML-Signaturzertifikaten ab. Eins für jede Seite der SAML-Verbindung.

SAML-Anbieter-Signaturzertifikat

Dieses Zertifikat wird von Ihrem SAML-Anbieter bereitgestellt und bei der Konfiguration der SAML-Verbindung in Citrix Cloud hochgeladen.

SAML-Signaturzertifikate müssen vor ihrem Ablaufdatum rotiert werden, damit Citrix Cloud-Administratoren Zeit haben, sich auf die Bereitstellung vorzubereiten. Die Zertifikatsrotation wird sowohl von Dienstanbietern als auch Identitätsanbietern verlangt, um die Abstimmung sicherzustellen und Downtime zu vermeiden.

Häufig gestellte Fragen

Wofür wird das SAML-Anbieterzertifikat verwendet?

Das SAML-Anbieterzertifikat wird verwendet, um die Signatur von SAML-Antworten zu verifizieren, die während des Authentifizierungsprozesses vom SAML-Anbieter an Citrix Cloud gesendet wurden.

Wo erhalte ich eine Kopie des neuesten Identitätsanbieter-(IdP-)Signaturzertifikats?

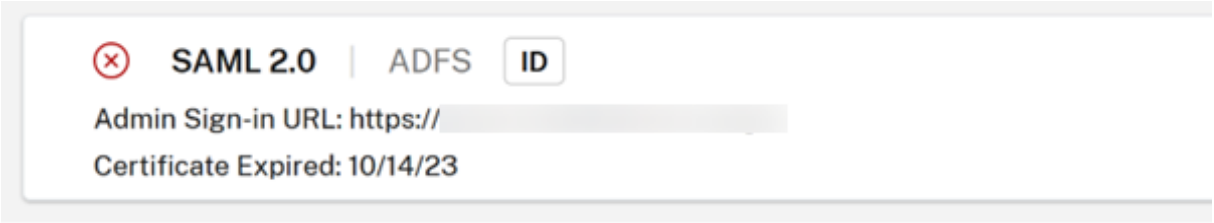
Dieses Zertifikat wird von Ihrem SAML-Anbieter wie Azure AD, Okta, PingFederate oder ADFS bereitgestellt. Citrix kontrolliert die Rotation und Aktualisierung dieses Zertifikats nicht. Dieses Zertifikat wird in Citrix Cloud hochgeladen, wenn Sie die SAML-Verbindung zum ersten Mal erstellen. **IdP-Signaturzertifikate** laufen in der Regel erst nach einem langen Zeitraum ab. Sie müssen möglicherweise alle paar Jahre ausgetauscht werden, nicht so häufig wie das **Dienstanbieter-Signaturzertifikat**

Woher weiß ich, ob mein SAML-Anbieter-Signaturzertifikat bald abläuft und sich auf meine Citrix Cloud SAML-Verbindung auswirkt?

Citrix Cloud zeigt 30 Tage vor Ablaufdatum Ihres SAML-Anbieter-Signaturzertifikats Warnungen an.

`Certificate Expiring Soon: <certExpirationDate>`

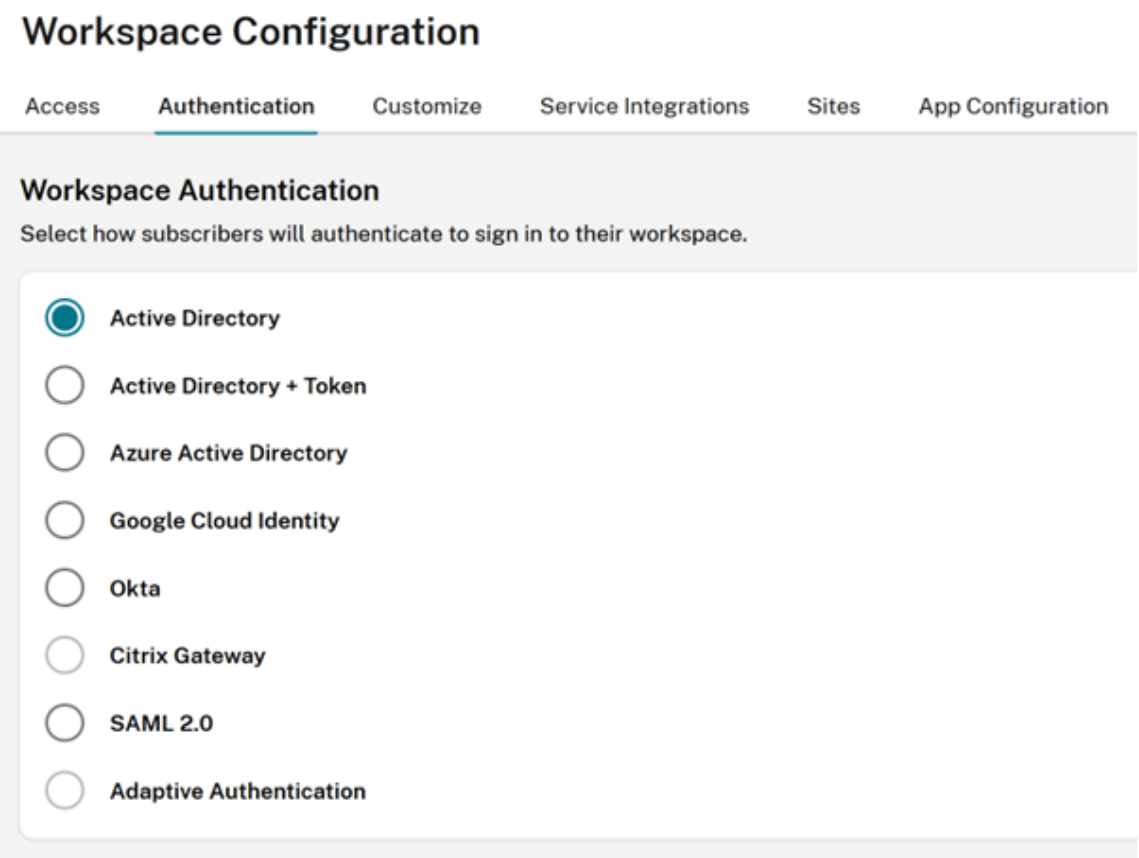
Es wird auch ein Fehler angezeigt, sobald das Zertifikat tatsächlich abgelaufen ist, wie unten gezeigt.



Kann ich das SAML-Anbieterzertifikat ohne Downtime aktualisieren, während ich die SAML-Verbindung weiterhin verwende?

Nein. Es ist notwendig, während eines geplanten Wartungsfensters eine SAML-Verbindung zu trennen und die Verbindung wiederherzustellen.
Das Identitätsanbieter-(IdP-)Signaturzertifikat aktualisieren

1. Wählen Sie in der **Workspace-Konfiguration** einen alternativen IdP aus und wählen Sie **Authentifizierung** aus, während Sie den Vorgang zum Trennen und erneuten Herstellen der SAML-Verbindung ausführen, z. B. Active Directory.



2. Sichern Sie Ihre vorhandene GO-URL, wie beispielsweise `https://citrix.cloud.com/go/<yourgourl>`, die für die SAML-Anmeldung bei Citrix Cloud verwendet wird.
3. Erstellen Sie ein Backup Ihrer vorhandenen SAML-Endpunkte. Diese können von der Citrix Cloud-Konsole kopiert werden. Sichern Sie die folgenden SAML-Endpunkte von Ihrer vorhandenen SAML-Verbindung aus.

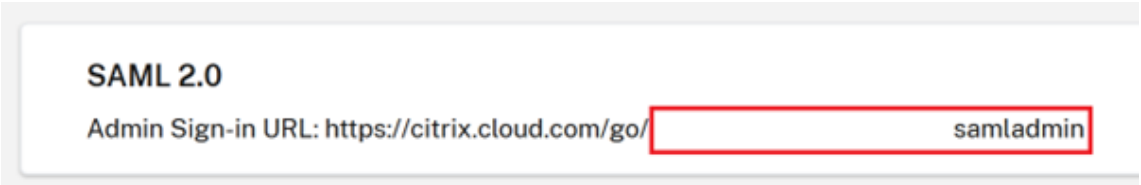
   - Entitäts-ID des Identitätsanbieters
   - URL für den SSO-Dienst des Identitätsanbieters
   - Abmelde-URL des Identitätsanbieters

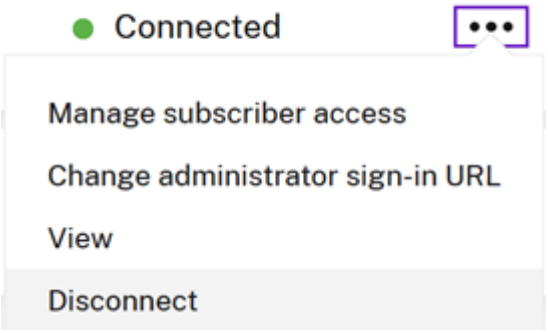
   Sichern Sie die EntityID, die SSO-URL und die Abmelde-URL.

> **Wichtig:**
>
> Stellen Sie sicher, dass Sie über eine Kopie des vorhandenen und des Ersatz-IdP-Signaturzertifikats verfügen, bevor Sie die Verbindung trennen. Auf diese Weise können Sie ein Rollback auf das alte Zertifikat ausführen, falls das neue SAML-Anbieterzertifikat ungültig ist und Anmeldeprobleme verursacht. Sie können keine Kopie des alten Zertifikats von der Citrix Cloud-Benutzeroberfläche abrufen, bevor Sie die Verbindung trennen. Sie müssen es aus Ihrer SAML-Anwendung beziehen.

1. Trennen Sie SAML in **Identitäts- und Zugriffsverwaltung**, navigieren Sie zu **Authentifizierung**, wählen Sie die SAML-Verbindung aus, klicken Sie auf die Ellipse und wählen Sie **Trennen**

2. Verbinden Sie SAML erneut in **Identitäts- und Zugriffsverwaltung** und klicken Sie auf **Authentifizierung**





3. Akzeptieren Sie alle standardmäßigen SAML-Verbindungseinstellungen.
4. Geben Sie alle SAML-Anwendungsendpunkte, die Sie zuvor gesichert haben, erneut ein, oder rufen Sie diese erneut für Ihre SAML-App über die Benutzeroberfläche Ihres SAML-Anbieters ab.
    - Entitäts-ID des Identitätsanbieters
    - URL für den SSO-Dienst des Identitätsanbieters
    - Abmelde-URL des Identitätsanbieters

> **Wichtig:**
>
> Wenn Sie das Feature "Scoped EntityID"verwenden, müssen Sie auch Ihre SAML-Anwendung mit der neuen Bereichs-ID aktualisieren, nachdem Sie die SAML-Verbindung trennen/wiederherstellen. Weitere Informationen zur Funktion "Scoped EntityID"finden Sie unter SAML-Anwendung mit bereichsbezogener Entitäts-ID in Citrix Cloud konfigurieren. Kopieren Sie die neu generierte Bereichs-ID aus der Citrix Cloud SAML-Benutzeroberfläche und aktualisieren Sie die Entitäts-ID Ihrer SAML-Anwendung mit der Ersatzbereichs-ID.
> EntityId sollte auf `https://saml.cloud.com/<new scope ID after reconnect>` aktualisiert werden.

SAML-Signaturzertifikat des Dienstanbieters aktualisieren

May 31, 2024

Author:
Mark Dear

SAML-Verbindungen, die signierte Anforderungen und Antworten verwenden, hängen von zwei verschiedenen SAML-Signaturzertifikaten ab. Eins für jede Seite der SAML-Verbindung.

Dienstanbieter-Signaturzertifikat

Dieses Zertifikat wird regelmäßig von Citrix bereitgestellt und in Ihre SAML-Anwendung hochgeladen oder über die Citrix Cloud SAML-Metadaten abgerufen.

SAML-Signaturzertifikate müssen vor ihrem Ablaufdatum rotiert werden, damit Citrix Cloud-Administratoren Zeit haben, sich auf die Bereitstellung vorzubereiten. Die Zertifikatsrotation wird sowohl von Dienstanbietern als auch Identitätsanbietern verlangt, um die Abstimmung sicherzustellen und Downtime zu vermeiden.

Wenn ein ausgewählter SAML-Anbieter die automatische Rotation des SP-SAML-Signaturzertifikats nicht unterstützt, muss eine manuelle Rotation des SAML-Signaturzertifikats innerhalb Ihres SAML-Anbieters durchgeführt werden, um das ablaufende Zertifikat zu ersetzen.

> **Wichtig:**
>
> Alle vorhandenen Anleitungen in diesem SAML-eDoc-Abschnitt enthalten Details zur Konfiguration der Signierung auf beiden Seiten der SAML-Verbindung. Citrix empfiehlt nur signierte SAML-Konfigurationen, da diese sicherer sind und bei einigen SAML-Anbietern für eine erfolgreiche Abmeldung (SLO) erforderlich sind.

Häufig gestellte Fragen

Was ist eine SAML-Signatur?

SAML-Signaturzertifikate sind X.509-Zertifikate, die zur Überprüfung von Daten verwendet werden, die zwischen dem Dienstanbieter (SP) und dem SAML-Anbieter (IdP) gesendet werden. Ihr SAML-Anbieter (IdP) verwendet das Citrix Cloud SAML-Signaturzertifikat, um die von Citrix Cloud in der SAML-Authentifizierungsanforderung gesendete Signatur zu überprüfen. Citrix Cloud verwendet das SAML-Anbieter-Signaturzertifikat, um zu überprüfen, ob die SAML-Antwort von einem vertrauenswürdigen und verbundenen IdP stammt.

Was ist die Durchsetzung von SAML-signierten Anforderungen?

Nur weil Citrix Cloud so konfiguriert ist, dass signierte Anfragen gesendet werden, garantiert dies nicht, dass der SAML-Anbieter die Verwendung von Signaturen erzwingt und alle unsignierten eingehenden

SAML-Anforderungen ablehnt. Die meisten SAML-Anbieter haben die Option, signierte Anforderungen durchzusetzen. Wenn also eine unsignierte Anforderung zur Anmeldung beim SAML-Anbieter eingeht, schlägt die Anmeldung fehl. Es liegt in der Verantwortung des SAML-Anbieter-Administrators, den Status der IdP-Konfiguration zu überprüfen. Der Citrix Support kontrolliert nicht und hat keinen Überblick darüber, ob signierte Anforderungen in Ihrer SAML-Anwendung durchgesetzt werden.

Wie oft rotiert Citrix sein Dienstanbieter-SAML-Signaturzertifikat?

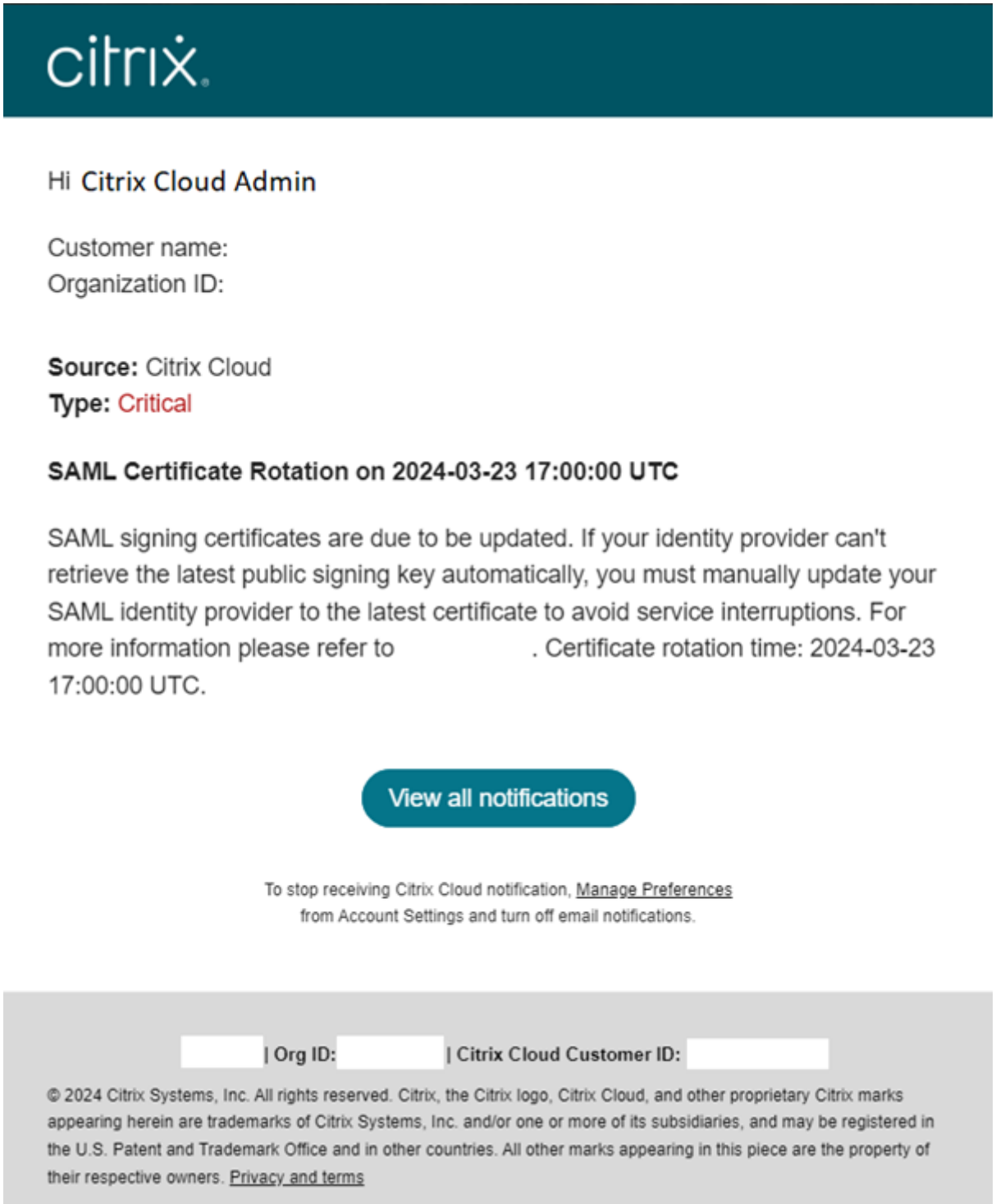
Um viele Überschneidungen zwischen dem aktiven Dienstanbieter-Signaturzertifikat und dem neu ausgestellten zu ermöglichen, rotiert Citrix das Dienstanbieter-Signaturzertifikat ungefähr alle 11 Monate. Dadurch wird sichergestellt, dass Citrix Cloud-Kunden 30 Tage vor Ablauf des vorhandenen Zertifikats ein gültiges Zertifikat zur Verfügung steht.

Was ist die Ankündigungsphase für das Dienstanbieter-SAML-Signaturzertifikat?

Während der Ankündigungsphase sind das aktuelle und das Ersatz-SAML-Signaturzertifikat in den Citrix Cloud-Metadaten vorhanden. Nur das aktive Zertifikat kann bis zum Datum und zur Uhrzeit der Rotation für die Überprüfung der SAML-Anforderung verwendet werden.

Warum habe ich per E-Mail und in der Citrix Cloud-Verwaltungskonsole eine Benachrichtigung erhalten, dass das aktuelle Citrix Cloud-SAML-Signaturzertifikat bald abläuft und ersetzt werden muss?

SAML-Anbieter (IdP) benötigen ein gültiges und aktuelles Zertifikat, um die Signatur eingehender SAML-Anforderungen von Dienstanbietern wie Workspace und der Citrix Cloud-Administratorkonsole zu überprüfen. Citrix Cloud-Kunden, die SAML für Workspace oder die Anmeldung an der Citrix Cloud-Admin-Konsole verwenden, werden kontaktiert, um sie über eine bevorstehende Rotation des SAML-Signaturzertifikats zu informieren.



citrix.

Hi **Citrix Cloud Admin**

Customer name:
Organization ID:

Source: Citrix Cloud
Type: Critical

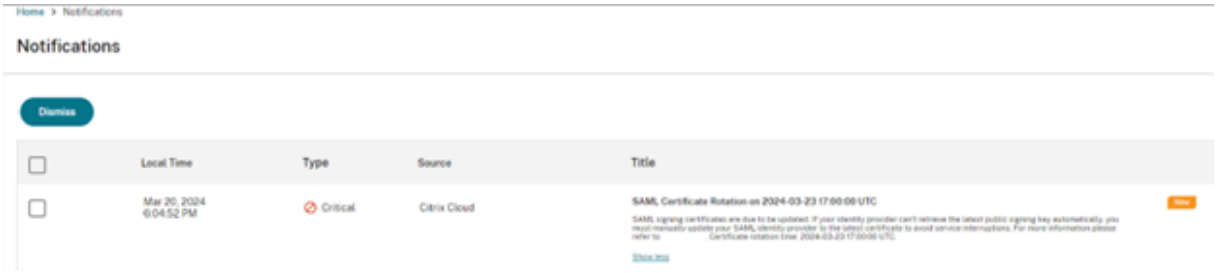
SAML Certificate Rotation on 2024-03-23 17:00:00 UTC

SAML signing certificates are due to be updated. If your identity provider can't retrieve the latest public signing key automatically, you must manually update your SAML identity provider to the latest certificate to avoid service interruptions. For more information please refer to . Certificate rotation time: 2024-03-23 17:00:00 UTC.

View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

| Org ID: | Citrix Cloud Customer ID:



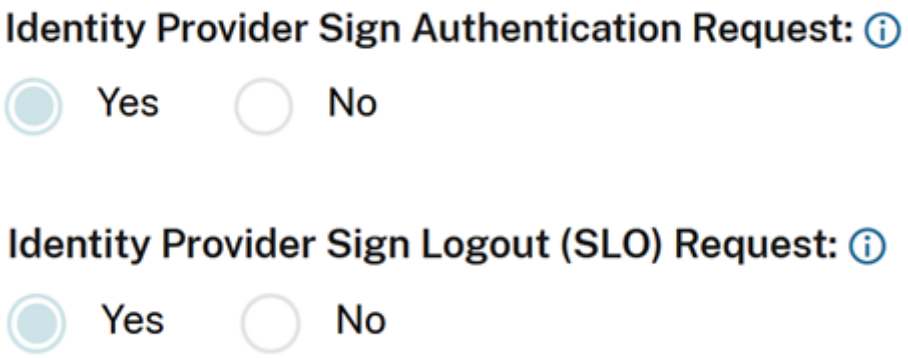
Woher weiß ich, ob mein Citrix Cloud-Kunde von der Rotation des Citrix Cloud SAML-Signaturzertifikats betroffen ist?

Dies wirkt sich auf Citrix Cloud-Kunden mit der folgenden SAML-Konfiguration aus.

- Ihre SAML-Verbindung in Citrix Cloud ist mit **Authentifizierungsanforderungen signieren = Ja**konfiguriert
- Sie haben Ihren SAML-Anbieter wie Azure Active Directory, ADFS oder Okta so konfiguriert, dass unsignierte SAML-Anforderungen abgelehnt werden (Durchsetzung signierter Anforderungen).
- Sie haben Single Logout (SLO) in Ihrer Citrix Cloud SAML-Verbindung und in Ihrem SAML-Anbieter konfiguriert. Ihr SAML-Anbieter verlangt möglicherweise, dass SLO-Anforderungen signiert werden, z. B. für Okta und PingFederate.

Wie überprüfe ich die Signaturkonfiguration meiner Citrix Cloud SAML-Verbindung?

Navigieren Sie zu **Identitäts- und Zugriffsmanagement** > **SAML 2.0** > **Anzeigen**, um zu überprüfen, ob Sie **Authentifizierungsanforderungen signieren** in Ihrer Citrix Cloud SAML-Verbindung aktiviert haben. Alle neuen SAML-Verbindungen in Citrix Cloud verwenden standardmäßig **Identitätsanbieter-Authentifizierungsanforderung/-Abmeldungsanforderung (SLO) signieren = Ja** sowohl für die Anmeldung (SSO) als auch für die Abmeldung (SLO).



Wie überprüfe ich, ob die Durchsetzung von Signaturen in meiner SAML-App konfiguriert ist?

Dies hängt vom verwendeten SAML-Anbieter ab. Einige bieten diese Option möglicherweise nicht einmal an. AzureAD, ADFS, Okta und PingFederate unterstützen alle die Durchsetzung von Signaturen. Es ist wichtig, dass der SAML-Administrator die Funktionen Ihres SAML-Anbieters und dessen aktuelle Konfiguration kennt. Der Citrix-Support hat diesbezüglich keine Kontrolle oder Sichtbarkeit.

Wo erhalte ich eine Kopie des neuesten Dienstanbieter-Signaturzertifikats?

Dieses Zertifikat wird von Citrix über die Citrix Cloud SAML-Metadaten bereitgestellt und während der Ankündigungsphase der SP-Signaturzertifikatsrotation regelmäßig aktualisiert. Dies geschieht mindestens einmal im Kalenderjahr.

USA, EU und APS: https://saml.cloud.com/saml/metadata

JP: https://saml.citrixcloud.jp/saml/

GOV: https://saml.cloud.us/saml/metadata

Wann ist es sicher, das alte Citrix Cloud SAML-Signaturzertifikat zu entfernen, wenn meine SAML-App mehrere Verifizierungszertifikate unterstützt?

Entfernen Sie das alte Citrix Cloud-Signaturzertifikat erst nach dem Datum und der Uhrzeit der Zertifikatsrotation, die in der E-Mail und der Benachrichtigung der Citrix Cloud-Verwaltungskonsole angegeben sind.

Metadatenaustausch verwenden, um den SAML-Anbieter automatisch mit dem neuesten Citrix Cloud SP SAML-Signaturzertifikat zu aktualisieren

Mithilfe des SAML-Metadatenaustauschs verbraucht der SAML-Anbieter die Citrix Cloud SAML-Metadaten automatisch, indem er die Metadaten-URL überwacht, z. B. https://saml.cloud.com/saml/metadata. Wenn Ihr SAML-Anbieter den SAML-Metadatenaustausch unterstützt, wird das SP-Signaturzertifikat möglicherweise bereits automatisch aktualisiert.
Stellen Sie sicher, dass Ihr SAML-Anbieter den Metadatenaustausch unterstützt. Anschließend können Sie überprüfen, ob das Update erfolgt ist, bevor das aktuelle SAML-Signaturzertifikat abläuft.

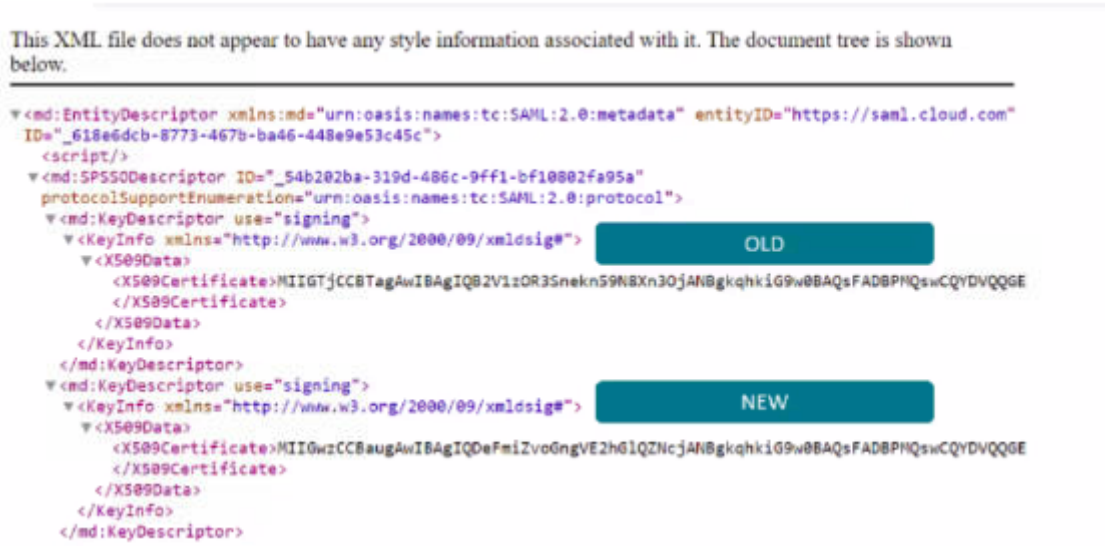
> **Wichtig**
>
> Es gibt große Unterschiede in Bezug auf die SAML-Funktionen, die jeder SAML-Drittanbieter unterstützt. Der Citrix Cloud-Administrator ist dafür verantwortlich, die Funktionen und Anforderungen des von Ihnen verwendeten SAML-Anbieters zu kennen und zu verstehen. Dies ist erforderlich, um sicherzustellen, dass sowohl die Citrix Cloud SAML-Verbindungskonfiguration (SP) als auch die SAML-Anbieterkonfiguration (IdP) übereinstimmen. Lesen Sie in der Dokumentation Ihres SAML-Anbieters nach, ob er die Signaturüberprüfung unterstützt und ob SAML-Anforderungen und -Antworten signiert werden müssen.

SAML-Anbieter manuell mit dem neuesten Citrix Cloud SP SAML-Signaturzertifikat aktualisieren

> **Wichtig**
>
> Die Rotation des SP-Zertifikats muss jedes Mal erfolgen, wenn ein neues Zertifikat aus Citrix Cloud veröffentlicht wird. Andernfalls wird die SAML-Anmeldung beeinträchtigt und es kommt zu Ausfallzeiten.

1. Rufen Sie die neuesten SAML-Metadaten von Citrix Cloud ab, indem Sie Ihre aktuelle SAML-Verbindung in **Identitäts- und Zugriffsverwaltung** anzeigen, auf **Authentifizierung**klicken, **SAML-Verbindung** auswählen und auf **Anzeigen** klicken.
   Das folgende Bild ist ein Beispiel dafür, wie diese Datei für Citrix Cloud-Regionen wie USA, EU und APS aussehen könnte:

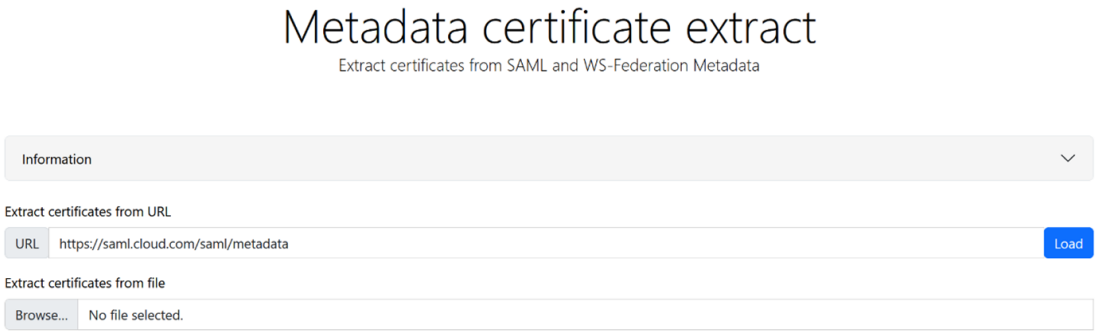
   https://saml.cloud.com/saml/metadata



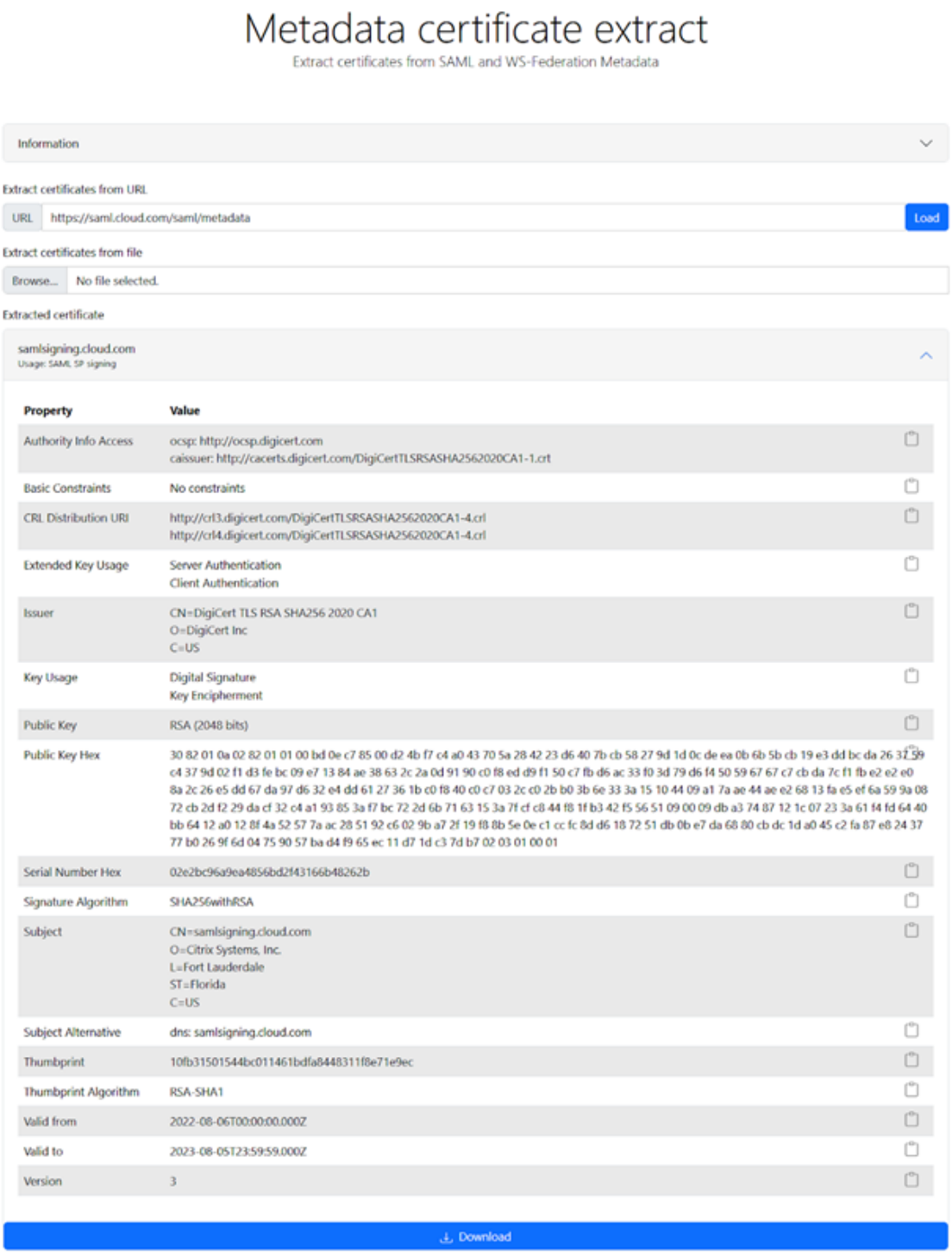
In diesem Beispiel für eine Metadaten-XML-Datei gibt es zwei x509 Citrix Cloud SAML-Signaturzertifikate.

2. Es ist möglich, das x509-Zertifikat aus den Metadaten zu extrahieren, indem Sie die XML-Datei in ein Drittanbieter-Tool hochladen oder die Metadaten-URL angeben.
3. Navigieren Sie zu https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract
4. Geben Sie die SAML-Metadaten-URL ein, die Ihrer Citrix Cloud-Kundenregion entspricht:

   - USA, EU und APS: https://saml.cloud.com/saml/metadata
   - JP: https://saml.citrixcloud.jp/saml/metadata
   - GOV: https://saml.cloud.us/saml/metadata



Laden Sie das SAML-Signaturzertifikat von https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtractherunter.



5. Laden Sie das neu extrahierte Citrix Cloud SP SAML-Zertifikat auf Ihren SAML-Anbieter hoch. Dieser Prozess unterscheidet sich je nach SAML-Anbieter. Überprüfen Sie das richtige Verfahren zur Rotation von SP-Signaturzertifikaten anhand der Dokumentation Ihres spezifischen SAML-Anbieters.

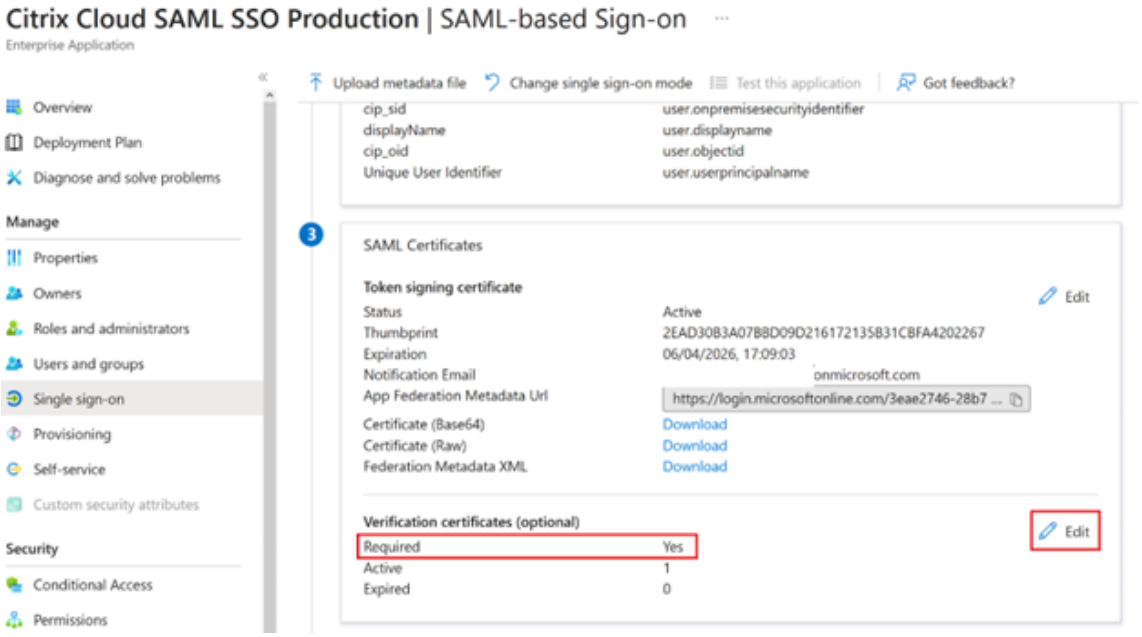
   Abhängig von Ihrem SAML-Anbieter muss das vorhandene SAML-Signaturzertifikat möglicher-

weise durch das neue ersetzt werden. In einigen Fällen unterstützt der SAML-Anbieter möglicherweise mehrere SP-Signaturzertifikate gleichzeitig, sodass nur das Hochladen des neuen Zertifikats ausreicht. Es wird empfohlen, das alte Zertifikat zu entfernen, sobald es abgelaufen ist.

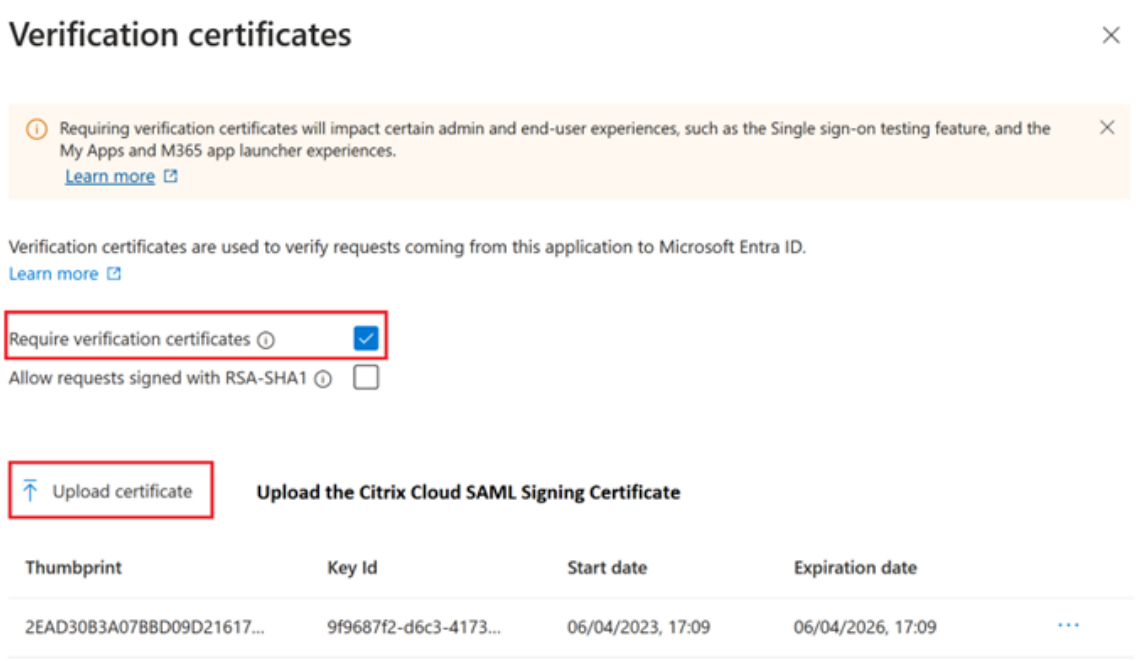
Ersatz-SAML-Signaturzertifikat von Citrix Cloud in Ihre Azure Active Directory-SAML-Anwendung hochladen

Bevor Sie die Azure Active Directory-SAML-App konfigurieren, lesen Sie Überprüfung der SAML-Anforderungssignatur, um weitere Informationen zu erhalten.

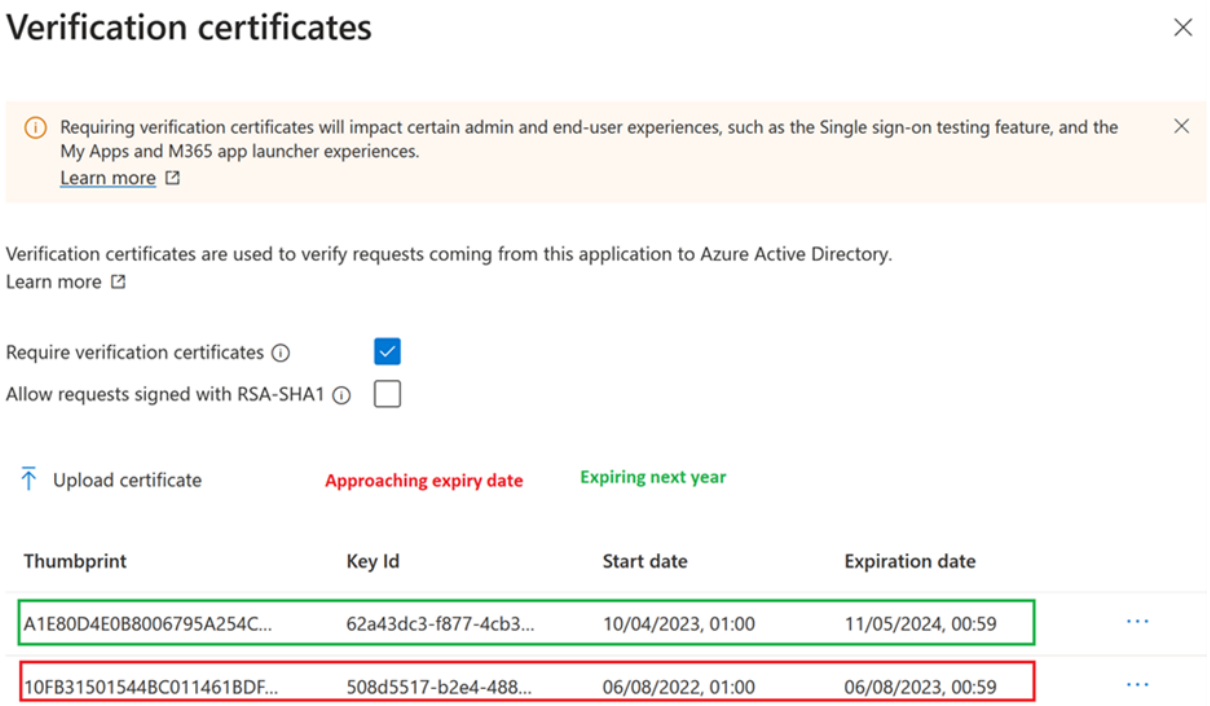
1. Navigieren Sie zu **Azure Active Directory**, wählen Sie **Unternehmensanwendungen** aus und klicken Sie auf Ihre SAML-App.
2. Suchen Sie den Abschnitt für die SAML-Zertifikate in der SAML-Anwendung.



3. Wählen Sie **Zertifikat hochladen** und laden Sie das Citrix Cloud SAML-Signaturzertifikat als Ersatz hoch, das Sie aus den SAML-Metadaten erhalten haben.



> **Hinweis:**
>
> In Azure Active Directory-SAML-Apps können mehrere Signaturüberprüfungszertifikate konfiguriert werden, sodass es möglich ist, ein Ersatzzertifikat hochzuladen, lange bevor das aktuelle Zertifikat abgelaufen ist. Der folgende Screenshot zeigt zwei gültige Zertifikate. Eines der Zertifikate läuft in naher Zukunft ab. Sofern mindestens eines der hochgeladenen Zertifikate gültig und noch nicht abgelaufen ist, ist eine SAML-Anmeldung bei Citrix Workspace und Citrix Cloud weiterhin erfolgreich und es kommt zu keinem Ausfall.

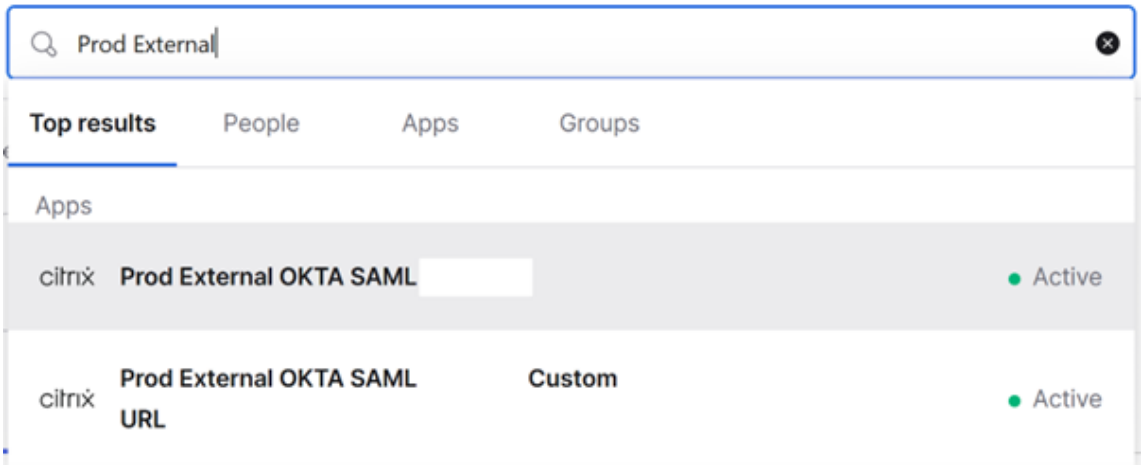


> **Wichtig:**
>
> Entfernen Sie das vorhandene Überprüfungszertifikat erst, nachdem das Datum und die Uhrzeit der SAML-Rotation, die in der E-Mail und der Benachrichtigung über die Citrix Cloud-Verwaltungskonsole angegeben sind, abgelaufen sind. Das neue Citrix Cloud-Zertifikat wird erst an dem Datum und zu der Uhrzeit aktiv, die in diesen beiden Benachrichtigungen angegeben sind.

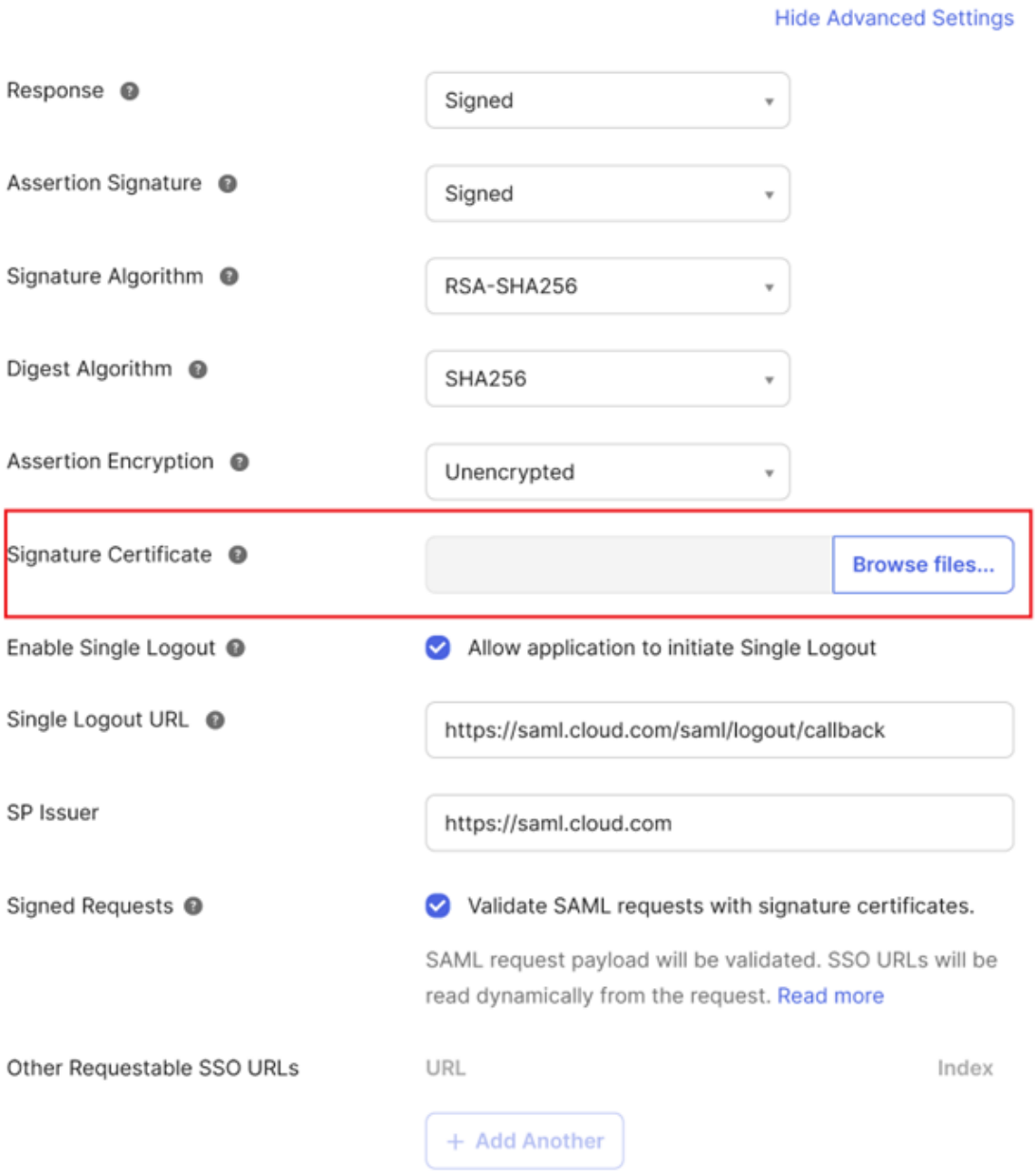
Neues Citrix Cloud SAML-Signaturzertifikat in Ihre Okta SAML-Anwendung hochladen

Okta unterstützt nicht mehrere SP-SAML-Signaturzertifikate gleichzeitig. Sie haben keine andere Wahl, als das vorhandene Citrix Cloud SP-Signaturzertifikat, das Sie derzeit verwenden, mit dem neuen zu überschreiben. Es wird empfohlen, dies in einem geplanten Wartungsfenster zu tun.

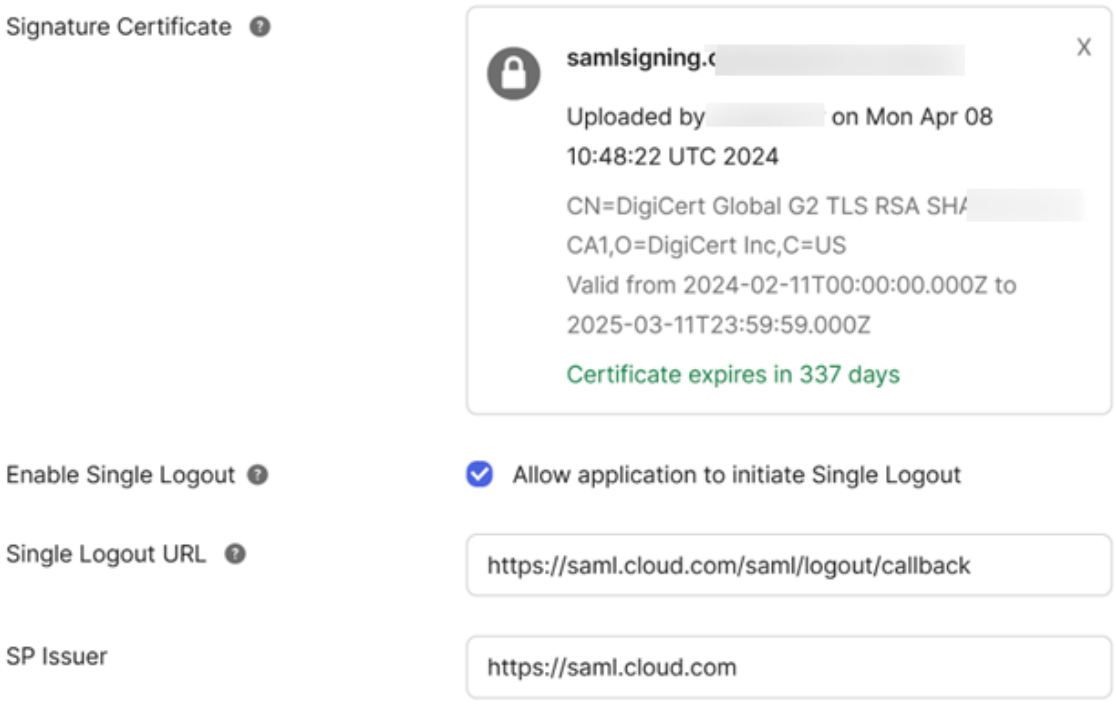
1. Navigieren Sie zu **Anwendungen**, wählen Sie **Anwendungen** aus und suchen Sie nach Ihrer Okta SAML-App



2. Navigieren Sie unter **Allgemein** zu **SAML-Einstellungen**, klicken Sie auf **Bearbeiten**, wählen Sie **SAML konfigurieren** aus, wählen Sie **Erweiterte Einstellungen anzeigen**und klicken Sie auf **Signaturzertifikat**, um ein Ersatzzertifikat hochzuladen. Okta zeigt das aktuelle Citrix Cloud SAML-Signaturzertifikat nicht in der Upload-Benutzeroberfläche an. Das Ersatzzertifikat wird erst angezeigt, nachdem es hochgeladen wurde.



3. Wählen Sie **Signaturzertifikat**, klicken Sie auf **Dateien durchsuchen** und laden Sie das Citrix Cloud SAML-Signaturzertifikat als Ersatz hoch, das Sie aus den Citrix Cloud SAML-Metadaten erhalten haben.



> **Wichtig**
>
> Überschreiben Sie das vorhandene Überprüfungszertifikat erst nach dem Datum und der Uhrzeit der SAML-Rotation, die in der E-Mail und der Benachrichtigung der Citrix Cloud-Verwaltungskonsole angegeben sind. Das neue Citrix Cloud-Zertifikat wird erst an dem Datum und zu der Uhrzeit aktiv, die in diesen beiden Benachrichtigungen angegeben sind.

ADFS als SAML-Anbieter für die Workspace-Authentifizierung konfigurieren

July 2, 2024

Author:
Mark Dear

In diesem Artikel wird beschrieben, wie Sie die von Citrix Cloud für die Anmeldung bei Citrix Workspace oder Citrix Cloud mit SAML benötigte Vertrauensstellung zwischen vertrauenden Seiten konfigurieren.

Wenn Sie die Schritte in diesem Artikel ausgeführt haben, können Sie die SAML-Verbindung zwischen Ihrem AD FS-Server und Citrix Cloud gemäß den Anweisungen unter Connect SAML as an identity

provider in Citrix Cloud konfigurieren. Informationen zur Eingabe der richtigen AD FS-Werte für Ihre SAML-Verbindung finden Sie in diesem Artikel unter SAML-Konfiguration in Citrix Cloud.

Voraussetzungen

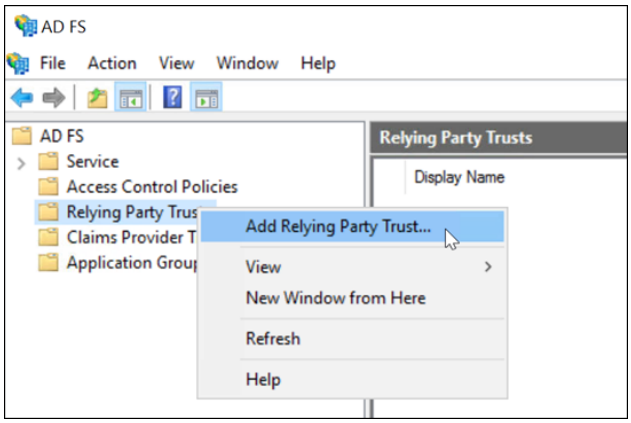
Bei den Anweisungen in diesem Artikel wird davon ausgegangen, dass Sie über eine funktionierende AD FS-Serverbereitstellung mit Citrix FAS verfügen. Citrix FAS ist für das Single Sign-On bei VDAs während des Sitzungsstarts erforderlich.

Weitere Informationen hierzu finden Sie in den folgenden Artikeln:

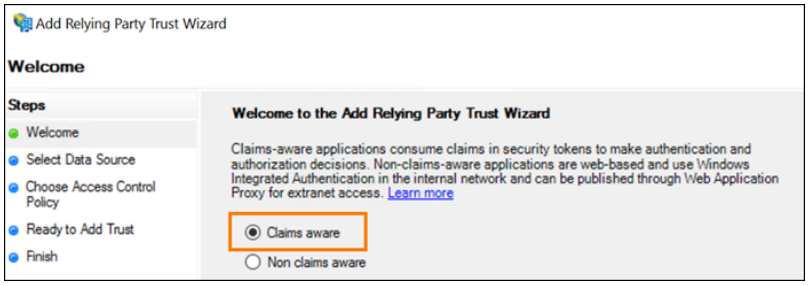
- Citrix FAS-Dokumentation:
  - Installation
  - AD FS-Bereitstellung
- Citrix Tech Zone: Referenzarchitektur: Übersicht über die Architekturen des Verbundauthentifizierungsdiensts

Vertrauensstellung für vertrauende Seite für Citrix Cloud konfigurieren

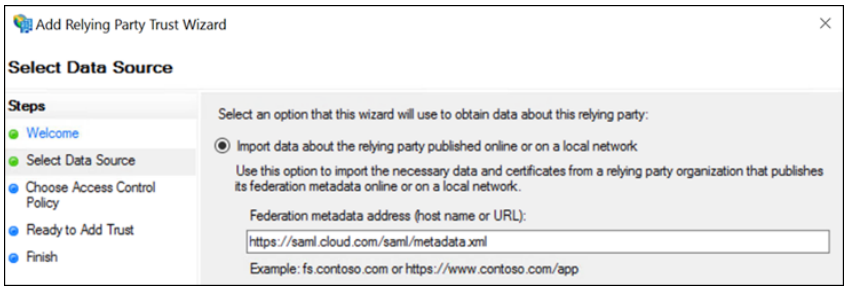
1. Erweitern Sie in der AD FS-Verwaltungskonsole den Knoten **AD FS** im linken Bereich.
2. Klicken Sie mit der rechten Maustaste auf **Vertrauensstellung der vertrauenden Seite** und wählen **Vertrauensstellung der vertrauenden Seite hinzufügen**.



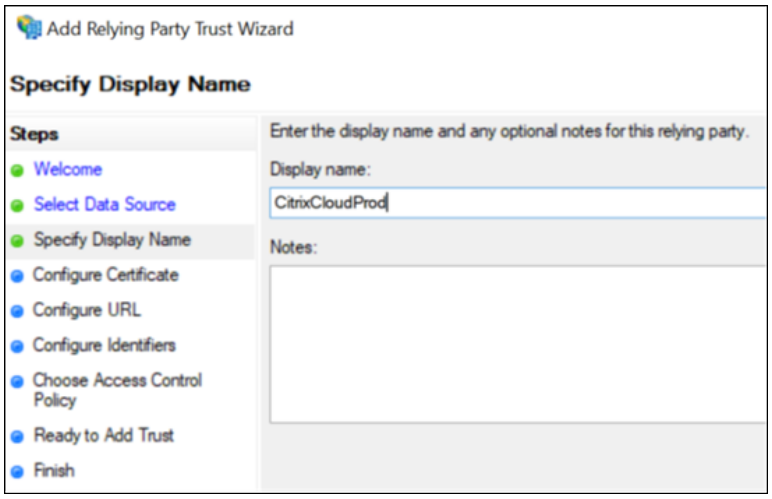
   Der Assistent zum Hinzufügen vertrauender Seiten wird angezeigt.
3. Wählen Sie **Ansprüche unterstützend** und dann **Weiter**.



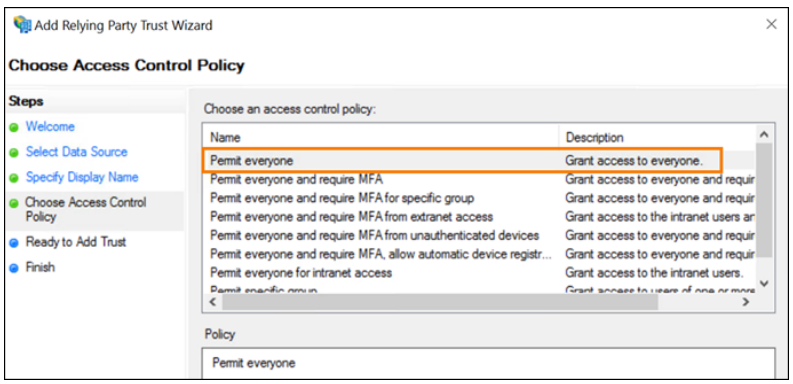
4. Geben Sie im Feld **Verbundmetadaten-Adresse** den Wert `https://saml.cloud.com/saml/metadata.xml` ein. Wählen Sie **Weiter**.



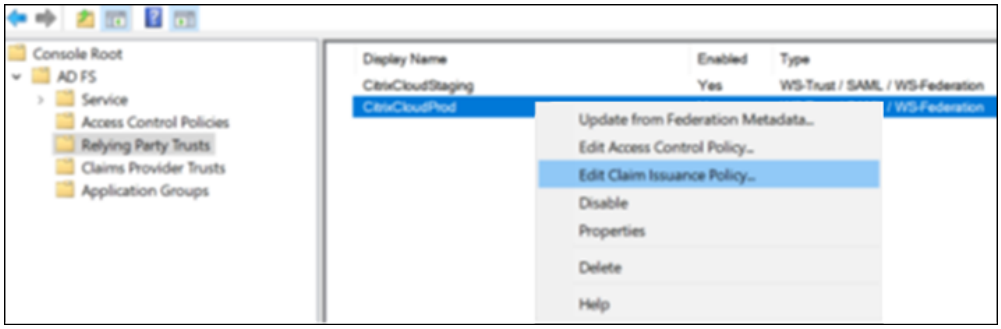
5. Geben Sie als Anzeigenamen `CitrixCloudProd` ein. Wählen Sie **Weiter**.



6. Wählen Sie als Zugriffssteuerungsrichtlinie **Alle zulassen**. Wählen Sie **Weiter**.

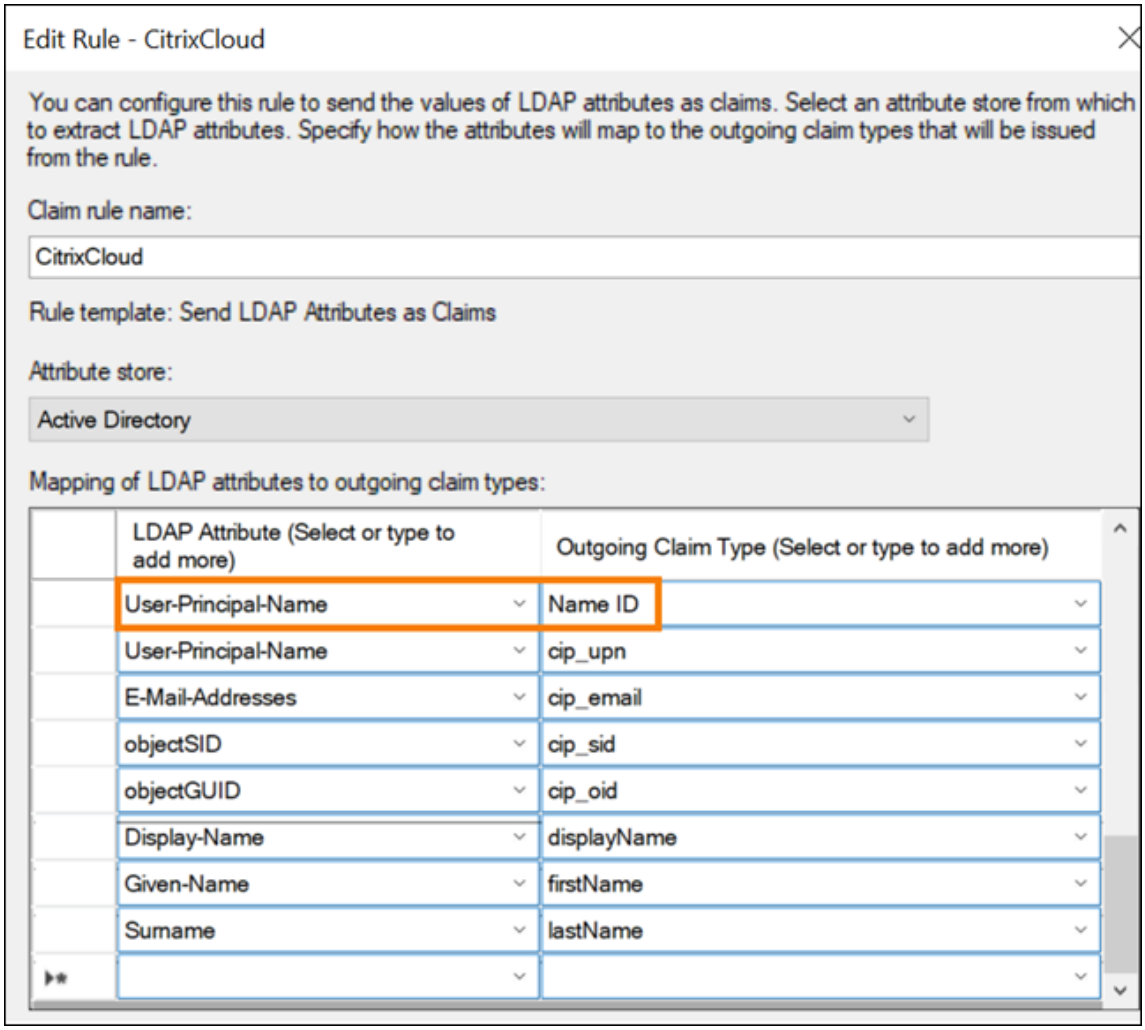


7. Wählen Sie auf der Seite **Bereit zum Hinzufügen der Vertrauensstellung** die Option **Weiter**.
8. Wählen Sie auf der Seite **Fertig stellen** die Option **Configure claims issuance policy for this application**. Wählen Sie **Weiter**.



9. Klicken Sie mit der rechten Maustaste auf die neue Vertrauensstellung und wählen Sie **Edit Claim Issuance Policy**.
10. Klicken Sie auf **Regel hinzufügen** und wählen Sie **Send LDAP Attributes as Claims**. Wählen Sie **Weiter**.
11. Geben Sie im Feld **Claim rule name** den Wert `CitrixCloud` ein.
12. Wählen Sie für **Attributspeicher** die Option **Active Directory**.
13. Fügen Sie unter **Mapping of LDAP attributes to outgoing claim types** die folgenden LDAP-Attribute genau wie hier gezeigt hinzu:

LDAP-Attribut	Art des ausgehenden Anspruchs
User-Principal-Name	Name ID
User-Principal-Name	cip_upn
E-Mail-Addresses	cip_email
objectSID	cip_sid
objectGUID	cip_oid
Display-Name	displayName
givenname	firstName
Nachname	lastName



14. Wählen Sie **Fertig stellen**.

Vertrauensstellung einer vertrauenden Citrix Cloud-Seite mit PowerShell ändern

Wenn Sie Ihren AD FS-Server mit der Standardkonfiguration konfiguriert haben, können Sie ihn anhand der Schritte in diesem Abschnitt aktualisieren, sodass er der von Citrix empfohlenen Konfiguration entspricht. Dieser Arbeitsgang ist erforderlich, um das Problem des Fehlschlagens des SAML-SLO von Citrix Cloud oder Citrix Workspace zu lösen, wenn das Attribut `nameidentifier` nicht im Anspruchsregelsatz enthalten ist oder nicht das erste SAML-Attribut im Anspruchsregelsatz ist.

> **Hinweis:**
>
> Sie müssen diese Schritte nicht ausführen, wenn Sie Ihren Anspruchsregelsatz wie unter Vertrauensstellung für vertrauende Seite für Citrix Cloud konfigurieren in diesem Artikel erstellt haben.

Zum Erledigen der Aufgabe ersetzen Sie den vorhandenen Regelsatz mithilfe von PowerShell durch

einen neuen Anspruchsregelsatz. Die AD FS-Verwaltungskonsole unterstützt diese Art von Vorgang nicht.

1. Suchen Sie auf dem AD FS-Server das PowerShell ISE. Klicken Sie mit der rechten Maustaste darauf und wählen Sie **Als Administrator ausführen**.
2. Sichern Sie Ihre AD FS-Anspruchsregeln in einer Textdatei:

```
Get-ADFSRelyingPartyTrust -name "CitrixCloudStaging" | Select-
    Object -ExpandProperty IssuanceTransformRules | Out-File "$env:
    USERPROFILE\desktop\claimrulesbackup.txt"
<!--NeedCopy-->
```

3. Laden Sie die Datei claimrules.txt herunter, die Citrix unter https://github.com/citrix/sample-scripts/tree/master/citrix-cloud bereitstellt.
4. Kopieren Sie die Datei claimrules.txt auf Ihren Desktop.
5. Importieren Sie die erforderlichen Anspruchsregeln mithilfe der Datei claimrules.txt:

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                      -MetadataUrl "https://saml.cloud.com/saml/
                         metadata" `
                      -AutoUpdateEnabled $True `
                      -IssuanceTransformRulesFile "$env:
                         USERPROFILE\desktop\claimrules.txt" `
                      -SignedSamlRequestsRequired $True `
                      -SamlResponseSignature "MessageAndAssertion"
                          `
                      -Enabled $True
<!--NeedCopy-->
```

Aktualisieren Sie die SAML-Signatureinstellungen für die Vertrauensstellung der vertrauenden Seite mithilfe von PowerShell

Standardmäßig haben Vertrauensstellungen der vertrauenden Seite bei AD FS die folgenden Einstellungen:

- EncryptClaims: True
- SignedSamlRequestsRequired: False
- SamlResponseSignature: AssertionOnly

Zur Erhöhung der Sicherheit empfiehlt Citrix, sowohl für Single Sign-On als auch für Single Logout signierte SAML-Anforderungen zu verwenden. In diesem Abschnitt wird beschrieben, wie Sie die Signatureinstellungen für die Vertrauensstellung einer vertrauenden Seite mit PowerShell aktualisieren, sodass sie der von Citrix empfohlenen Konfiguration entsprechen.

1. Rufen Sie die aktuelle RelyingPartyTrust-Konfiguration auf Ihrem AD FS-Server auf.


```
Get-ADFSRelyingPartyTrust -TargetName "CitrixCloudProd"
<!--NeedCopy-->
```

2. Aktualisieren Sie die Einstellungen der Vertrauensstellungen der vertrauenden Seite **Citrix-CloudProd**.

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                      -SignedSamlRequestsRequired $True `
                      -SamlResponseSignature "MessageAndAssertion"
<!--NeedCopy-->
```

3. Bitten Sie den Citrix Support um Aktivierung des Authentifizierungsfeatures **EnableSaml-LogoutSigningAndPost** für Ihren Citrix Cloud-Kunden. Dadurch sendet Citrix Cloud SAML Single Logout-Anforderungen als signierte POST-Anforderungen anstelle unsignierter Redirect-Anforderungen, wenn sich Benutzer von Citrix Workspace oder Citrix Cloud abmelden. Das Senden signierter POST-Anforderungen ist erforderlich, wenn der SAML-Anbieter signierte Anforderungen für Single Logout verlangt und unsignierte Weiterleitungen ablehnt.

SAML-Konfiguration in Citrix Cloud

Wenn Sie die SAML-Verbindung in Citrix Cloud konfigurieren (siehe SAML-Anbietermetadaten zu Citrix Cloud hinzufügen), geben Sie die Werte für AD FS wie folgt ein:

Feld in Citrix Cloud	Wert
Entitäts-ID	`https://adfs.YourDomain.com/adfs/services/trust`, wobei `YourDomain.com` Ihre AD FS-Serverdomäne ist.
Authentifizierungsanforderung signieren	Ja
SSO-Dienst-URL	`https://adfs.YourDomain.com/adfs/ls`, wobei `YourDomain.com` Ihre AD FS-Serverdomäne ist.
Bindungsmechanismus	HTTP-Post
SAML-Antwort	Antwort oder Assertion signieren
Authentifizierungskontext	Keine Angabe, exakt
Abmelde-URL	`https://adfs.YourDomain.com/adfs/ls`, wobei `YourDomain.com` Ihre AD FS-Serverdomäne ist.

Anmeldung bei Workspace mit SAML unter Verwendung benutzerdefinierter Domänen

November 24, 2023

Author:
Mark Dear

Wenn Sie eine benutzerdefinierte Domäne in Citrix Workspace konfiguriert haben (z. B. `https://workspaces.yourdomain.com`), ist abhängig von den SAML-Anmeldeszenarien, die Sie in Citrix Cloud unterstützen möchten, evtl. eine zusätzliche Konfiguration in Citrix Cloud und Ihrem SAML-Anbieter erforderlich.

Für diese Konfiguration benötigen Sie möglicherweise ein Paar SAML-Anwendungen. Citrix Cloud erfordert unterschiedliche SAML-Dienstanbieter-Endpunkte, je nachdem, ob die SAML-Anwendung die cloud.com- oder workspaces.yourdomain.com-URLs für die Anmeldung verwendet.

Informationen zur Konfiguration benutzerdefinierter Domänen in Citrix Workspace finden Sie unter Benutzerdefinierte Domäne konfigurieren in der Citrix Workspace-Produktdokumentation.

Überlegungen zur Bereitstellung einer oder zweier SAML-Anwendungen

Um festzustellen, ob Sie eine SAML-Lösung mit einer oder dualen Anwendungen benötigen, betrachten Sie die Kombination von SAML-Anmeldeszenarien, die Ihr SAML-Anbieter unterstützen muss.

Die folgenden Anmeldeszenarien verwenden standardmäßig dieselbe SAML-Anwendung (SAML-App 1):

- SAML-Authentifizierung für Citrix Workspace, bei der die Workspace-Anmelde-URL für Ihre Region (cloud.com, citrixcloud.jp, cloud.us) in Ihrem SAML-Anbieter als Anbieter-Entitäts-ID konfiguriert ist.
- SAML-Authentifizierung für Citrix Cloud unter Verwendung Ihrer eigenen Anmelde-URL (z. B. `https://citrix.cloud.com/go/mycompany`). In diesem Szenario werden Administratoren basierend auf ihrer Active Directory-Gruppenmitgliedschaft mithilfe von SAML bei Citrix Cloud authentifiziert.

Das Hinzufügen der SAML-Authentifizierung für Benutzer über eine benutzerdefinierte Domäne (z. B. `https://workspaces.mycompany.com`), die Sie in der Workspacekonfiguration festlegen, erfordert eine zweite SAML-Anwendung (SAML-App 2).

In der folgenden Tabelle werden die unterstützten Kombinationen von SAML-Anmeldeszenarien und die erforderlichen SAML-Apps aufgeführt.

Anmeldung mit der Workspace-URL bei Workspace	Anmeldung bei Workspace unter Verwendung einer benutzerdefinierten Domänen-URL	Anmeldung bei bei Citrix Cloud mit der SAML-Anmelde-URL	SAML-App 1 erforderlich?	SAML-App 2 erforderlich?
Ja	Nein	Nein	Ja: SAML-Endpunkte von cloud.com verwenden	Nein
Nein	Ja	Nein	Ja: SAML-Endpunkte von benutzerdefinierter Domäne verwenden	Nein
Nein	Nein	Ja	Ja: SAML-Endpunkte von cloud.com verwenden	Nein
Ja	Nein	Ja	Ja: SAML-Endpunkte von cloud.com verwenden	Nein
Nein	Nein	Ja	Ja: SAML-Endpunkte von cloud.com verwenden	Ja: SAML-Endpunkte von benutzerdefinierter Domäne verwenden
Ja	Ja	Ja	Ja: SAML-Endpunkte von cloud.com verwenden	Ja: SAML-Endpunkte von benutzerdefinierter Domäne verwenden

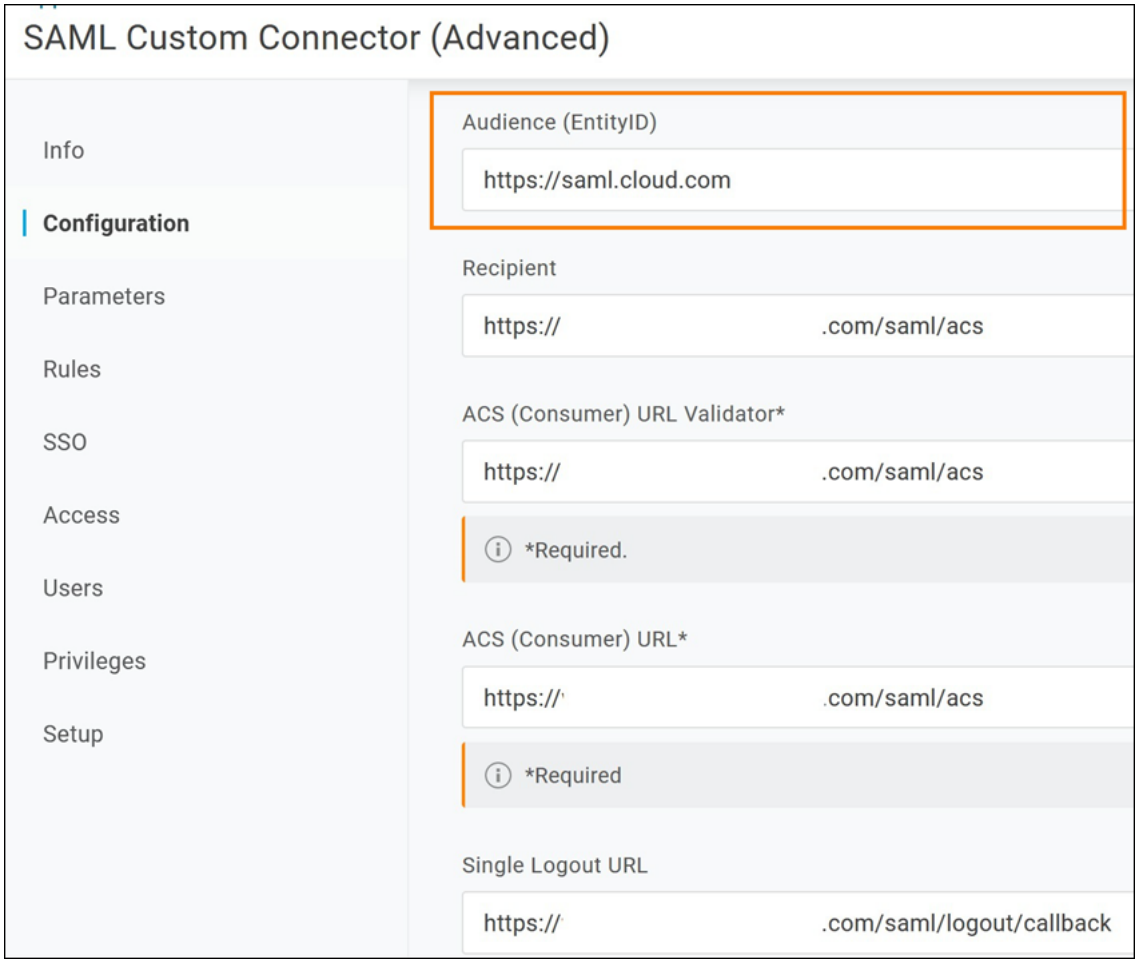
Einzelne SAML-Anwendung konfigurieren

1. Gehen Sie in Citrix Cloud zu **Workspacekonfiguration > Zugriff** und konfigurieren Sie eine benutzerdefinierte Domäne. Weitere Informationen finden Sie unter Benutzerdefinierte Domäne konfigurieren.
2. Konfigurieren Sie in der Verwaltungskonsole des SAML-Anbieters eine SAML-Anwendung mit Verwendung der benutzerdefinierten Domäne als Anbieterendpunkte.
3. Laden Sie das SAML-Signaturzertifikat für die SAML-Anwendung herunter. In einem späteren Schritt laden Sie dieses Zertifikat an Citrix Cloud hoch.
4. Vergewissern Sie sich, dass `https://saml.cloud.com` als Entitäts-ID eingegeben wurde. Abhängig von Ihrem SAML-Anbieter kann diese Einstellung stattdessen **Audience** heißen. Ersetzen Sie für alle anderen Endpunkte `https://saml.cloud.com` durch die benutzerdefinierte Workspace-Domäne, die Sie in Schritt 1 konfiguriert haben.

   Das folgende Beispiel zeigt die Endpunktkonfiguration für Okta, wobei **Audience Restriction** den Entitäts-ID-Wert enthält:

   Das folgende Beispiel zeigt die Endpunktkonfiguration für OneLogin, wobei **Audience** den Entitäts-ID-Wert enthält:



5. Gehen Sie in Citrix Cloud zu **Identitäts- und Zugriffsverwaltung > Authentifizierung** und konfigurieren Sie die SAML-Verbindung.
6. Gehen Sie zu **Workspacekonfiguration > Authentifizierung** und wählen Sie **SAML 2.0**.
7. Gehen Sie zu **Workspacekonfiguration > Benutzerdefinierte Workspace-URL > Bearbeiten** und wählen Sie **Nur die URL der benutzerdefinierten Domäne verwenden**.
8. Wählen Sie **Speichern**, um Ihre Änderungen zu speichern.
9. Um die Konfiguration zu testen, melden Sie sich mit Ihrer benutzerdefinierten Workspace-URL (`https://workspaces.mycompany.com`) bei Citrix Workspace an.

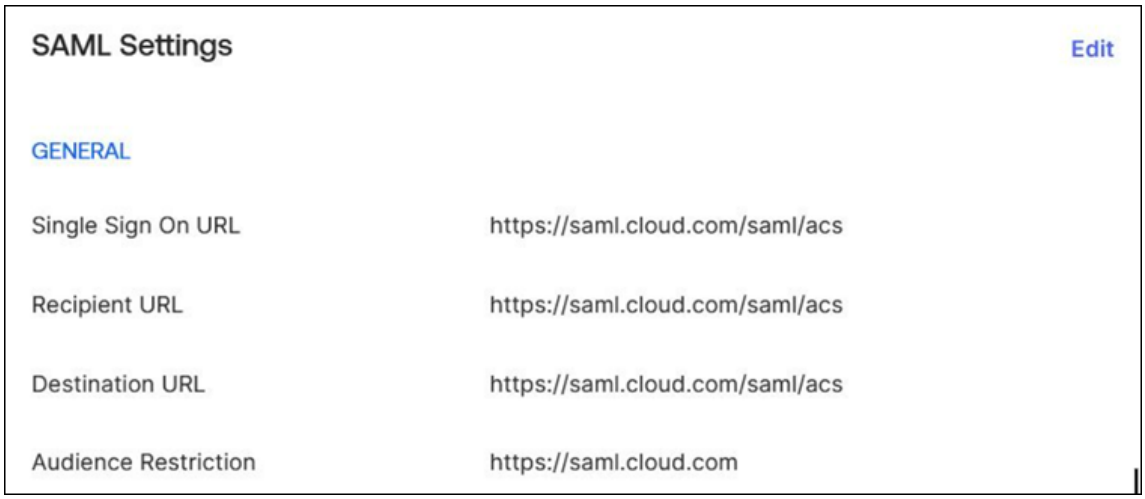
Duale SAML-Anwendungen konfigurieren

1. Gehen Sie in Citrix Cloud zu **Workspacekonfiguration > Zugriff** und konfigurieren Sie eine benutzerdefinierte Domäne. Weitere Informationen finden Sie unter Benutzerdefinierte Domäne konfigurieren.

2. Konfigurieren Sie in der Verwaltungskonsole Ihres SAML-Anbieters zwei SAML-Anwendungen. Konfigurieren Sie diese identisch, einschließlich identischer Signatureinstellungen für SSO- und SLO-Anfragen, Bindungstyp und Abmeldeeinstellungen. Wenn die Konfigurationen dieser SAML-Anwendungen nicht übereinstimmen, kann es zu Unterschieden im An- und Abmeldeverhalten kommen, wenn Sie zwischen Ihrer Workspace-URL und Ihrer benutzerdefinierten Workspace-Domäne wechseln.
3. Konfigurieren Sie für die erste SAML-Anwendung die folgenden Anbieter-Endpunkte:

   - Entitäts-ID: `https://saml.cloud.com`
   - Assertion Consumer Service: `https://saml.cloud.com/saml/acs`
   - Abmelden: `https://saml.cloud.com/saml/logout/callback`

   Das folgende Beispiel zeigt diese Endpunktkonfiguration in der Okta-Verwaltungskonsole:

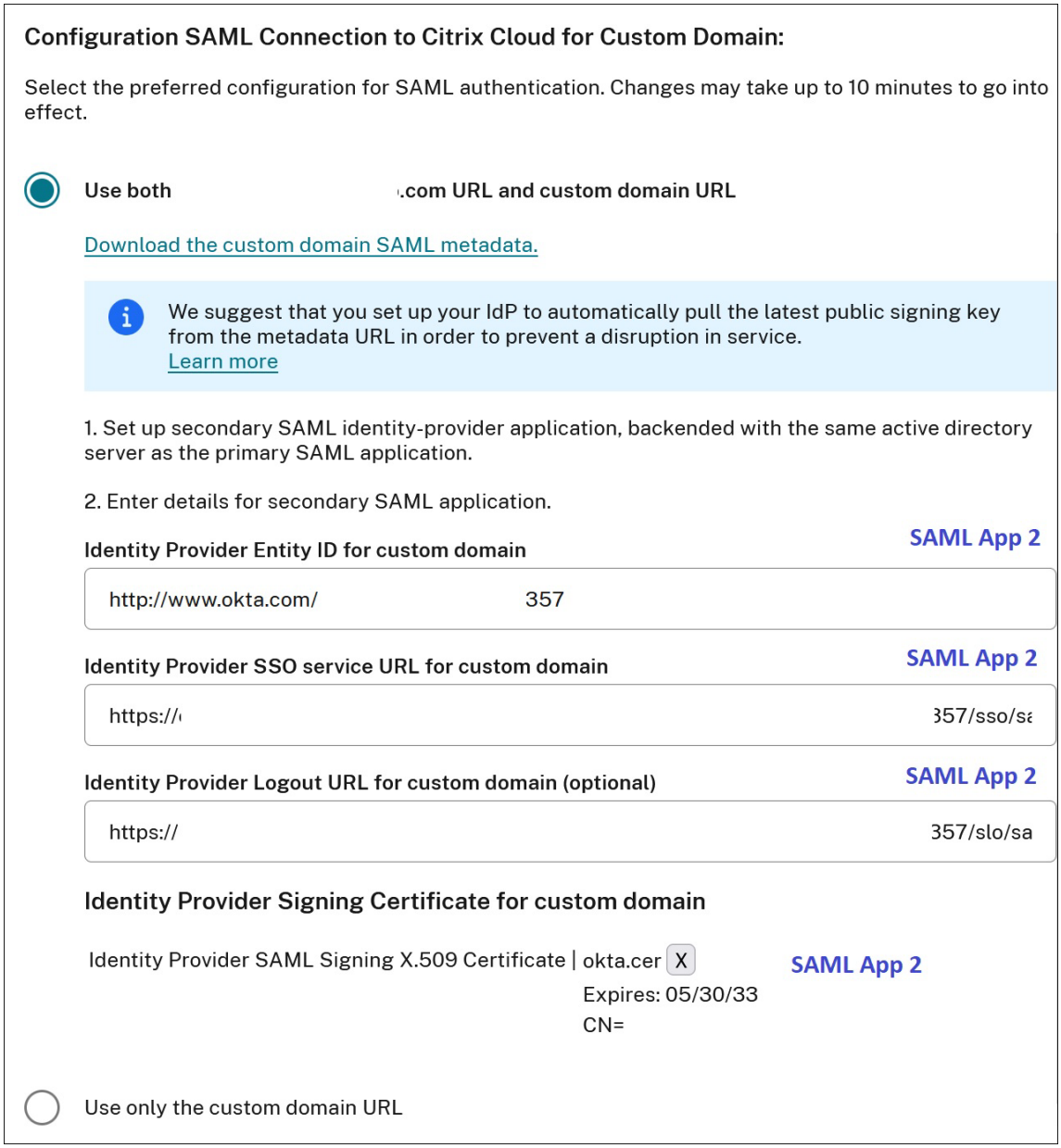
   

4. Konfigurieren Sie für die zweite SAML-Anwendung die folgenden Anbieter-Endpunkte: Verwenden Sie die benutzerdefinierte Workspace-Domäne nur für die Assertion Consumer Service- und Logout-Endpunkte.

   - Entitäts-ID: `https://saml.cloud.com`
   - Assertion Consumer Service: `https://workspaces.mycompany.com/saml/acs`
   - Abmelden: `https://workspaces.mycompany.com/saml/logout/callback`

   Das folgende Beispiel zeigt diese Endpunktkonfiguration in der Okta-Verwaltungskonsole: Beachten Sie, dass **Audience Restriction** den Entitäts-ID-Wert enthält.

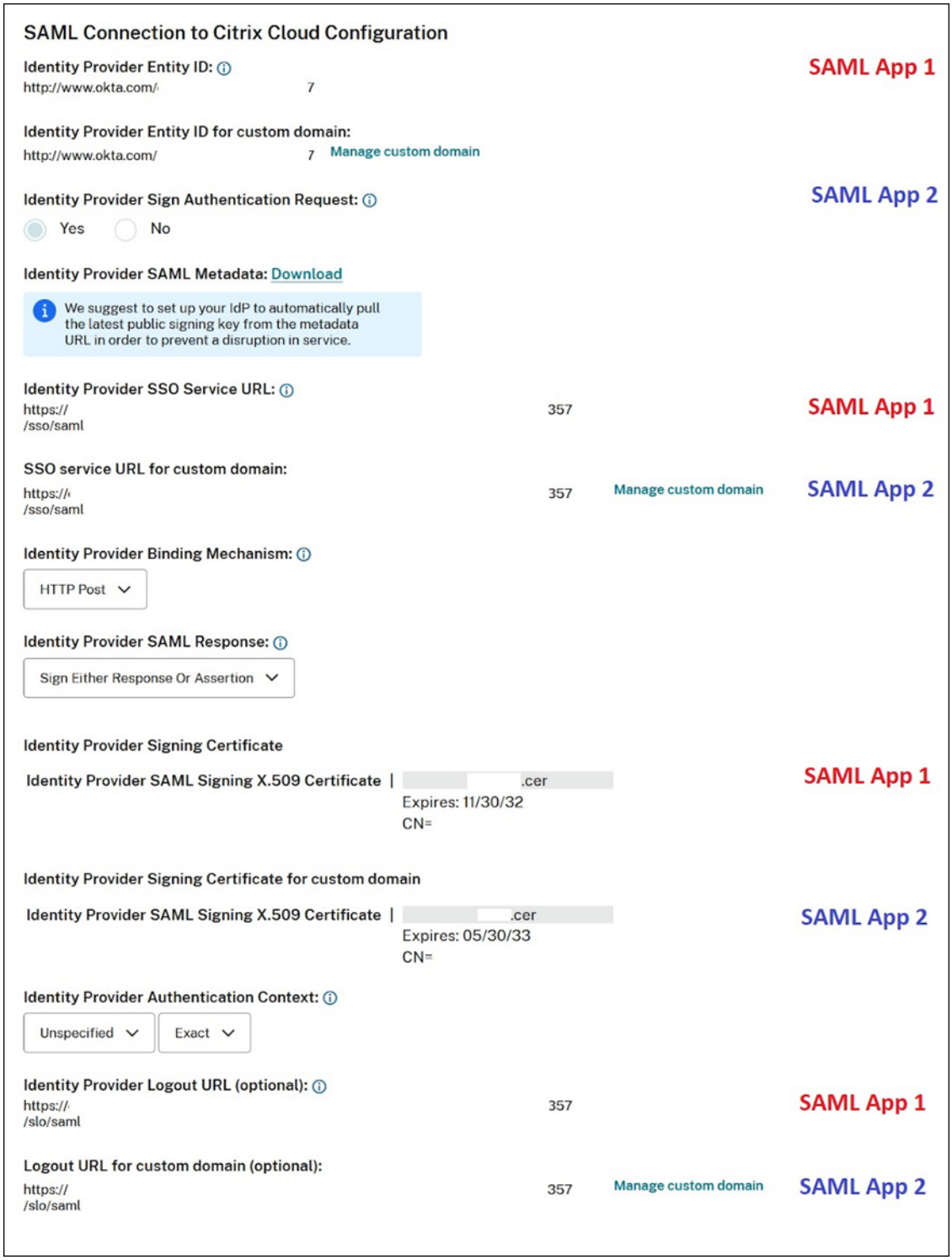
5. Laden Sie die SAML-Signaturzertifikate für beide SAML-Anwendungen herunter. Sie laden diese in einem späteren Schritt in Citrix Cloud hoch.
6. Konfigurieren Sie in der Citrix Cloud-Verwaltungskonsole eine SAML-Verbindung:
   a) Klicken Sie im Menü "Citrix Cloud"auf **Identitäts- und Zugriffsverwaltung**.
   b) Klicken Sie auf der Registerkarte **Authentifizierung** für **SAML 2.0** auf die Auslassungspunkte (…) und wählen Sie **Verbinden**.
   c) Geben Sie auf der Seite **SAML konfigurieren** die Details der ersten SAML-Anwendung ein, die Sie in Schritt 2 erstellt haben.
7. Konfigurieren Sie Citrix Workspace zur Verwendung der neuen SAML-Verbindung:
   a) Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration**.
   b) Wählen Sie auf der Registerkarte **Authentifizierung** die Option **SAML 2.0**.
8. Wählen Sie auf der Registerkarte **Zugriff** unter **Benutzerdefinierte Workspace-URL** die Option **Bearbeiten**.
9. Wählen Sie auf der Seite **Für SAML konfigurieren** die Option **cloud.com-URL und URL der benutzerdefinierten Domäne verwenden**.
10. Geben Sie die folgenden Informationen ein:
    - Geben Sie im Feld **Entitäts-ID des Identitätsanbieters für benutzerdefinierte Domäne** die Entitäts-ID aus der zweiten SAML-Anwendung ein, die Sie in Schritt 2 erstellt haben.
    - Geben Sie im Feld **SSO-Dienst-URL für benutzerdefinierte Domäne** die SSO-URL aus der zweiten SAML-Anwendung ein.
    - Geben Sie im Feld **Abmelde-URL für benutzerdefinierte Domäne** die SLO-URL aus der zweiten SAML-Anwendung ein.
    - Laden Sie unter **Signaturzertifikat des Identitätsanbieters für benutzerdefinierte Domäne** das SAML-Signaturzertifikat aus der zweiten SAML-Anwendung hoch.



11. Wählen Sie **Speichern**, um Ihre Änderungen zu speichern.

SAML-Verbindungsdetails anzeigen

Gehen Sie nach der Konfiguration zu **Identitäts- und Zugriffsverwaltung > Authentifizierung**. Wählen Sie unter **SAML 2.0** über die Auslassungspunkte die Option **SAML-Anbieter auswählen > Ansicht**. Auf der SAML-Konfigurationsseite werden SAML-Endpunktpaare angezeigt, die für Entitäts-ID, SSO-URL und Abmelde-URL konfiguriert sind.



Alle anderen SAML-Konfigurationseinstellungen gelten sowohl für die erste als auch für die zweite SAML-Anwendung.

Anmeldungen bei Citrix Workspace überprüfen

Führen Sie die folgenden Tests durch, um das von Ihnen konfigurierte An- und Abmeldeverhalten zu überprüfen:

- Melden Sie sich mit Ihrer Workspace-URL (`https://mycompany.cloud.com`) und Ihrem SAML-Anbieter bei Citrix Workspace an.
- Melden Sie sich mit Ihrer benutzerdefinierten Workspace-Domäne (`https://workspace.mycompany.com`) und Ihrem SAML-Anbieter bei Citrix Workspace an.
- Melden Sie sich mit Ihrer eindeutigen Anmelde-URL (`https://citrix.cloud.com/go/mycompany`) und Ihrem SAML-Anbieter bei Citrix Cloud an.

Okta als SAML-Anbieter für die Workspace-Authentifizierung konfigurieren

March 12, 2024

Author:
Mark Dear

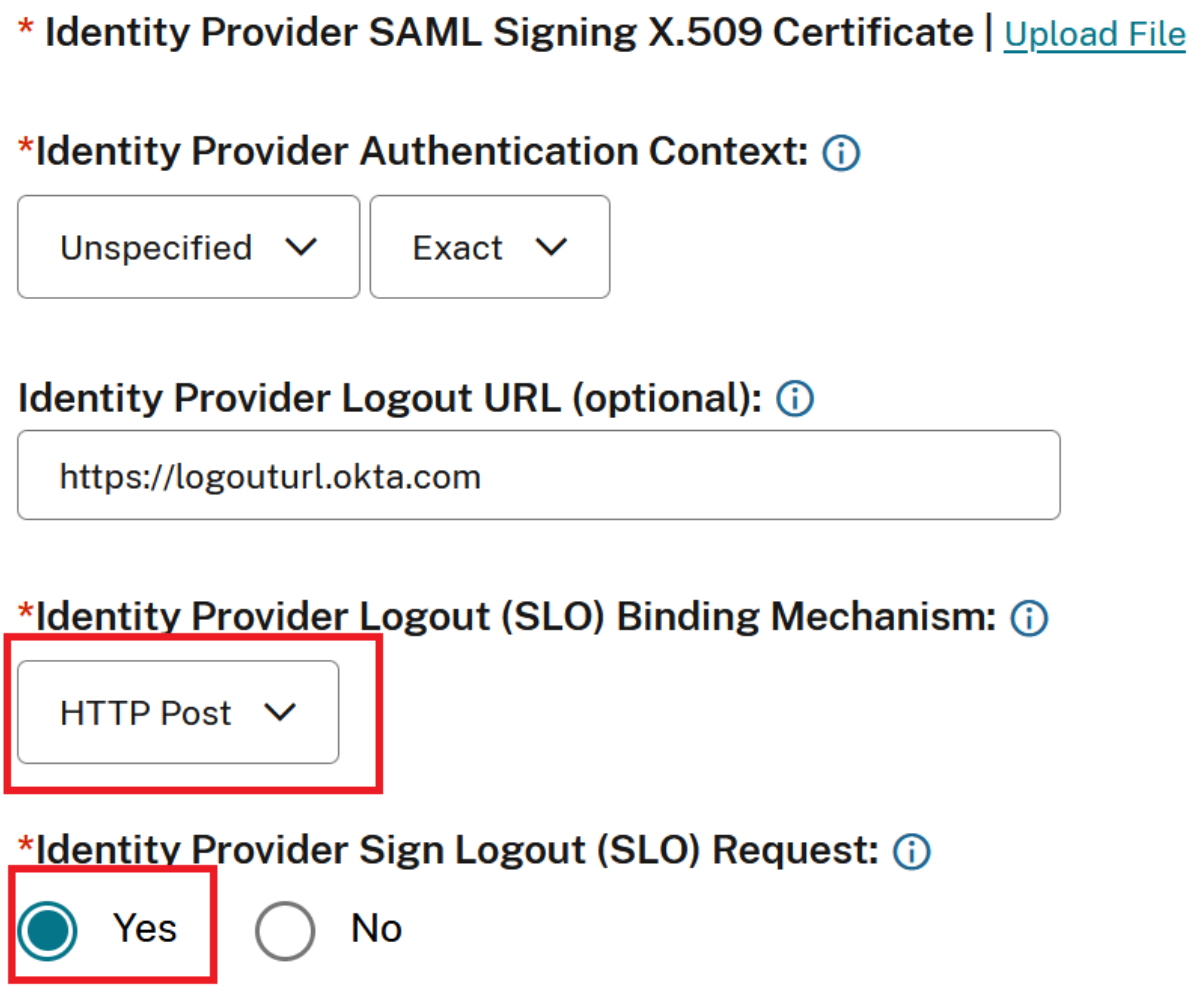
In diesem Artikel werden die Schritte zur Konfiguration einer Okta SAML-Anwendung und der Verbindung zwischen Citrix Cloud und Ihrem SAML-Anbieter beschrieben. In einigen Schritten werden Aktionen beschrieben, die Sie in der Verwaltungskonsole Ihres SAML-Anbieters ausführen.

Voraussetzungen

Bevor Sie die hier aufgeführten Aufgaben ausführen, stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Citrix Support hat das Feature **SendNameIDPolicyInSAMLRequest** in Citrix Cloud aktiviert. Dieses Feature wird auf Anfrage aktiviert. Weitere Informationen zu den Features finden Sie unter Für SAML mit Okta erforderliche Cloud-Features.
- Sie haben eine Okta-Organisation, die eine der folgenden Okta-Domänen verwendet:
  - okta.com
  - okta-eu.com
  - oktapreview.com
- Sie haben Ihr Active Directory (AD) mit Ihrer Okta-Organisation synchronisiert.
- **Authentifizierungsanforderung signieren** ist in Ihrer Okta-Organisation aktiviert.

- **Single Logout (SLO) des Identitätsanbieters** ist sowohl in Citrix Cloud als auch in der Okta SAML-Anwendung konfiguriert. Wenn SLO konfiguriert ist und sich ein Endbenutzer von Citrix Workspace abmeldet, meldet er sich auch bei Okta und allen anderen Dienstanbietern ab, die die Okta-SAML-Anwendung gemeinsam nutzen.
- **SLO-Anforderungen (Identity Provider Sign Logout)** sind in Citrix Cloud aktiviert.
- **SLO-Bindungsmechanismus (Identity Provider Logout)** ist HTTPPost in Citrix Cloud.



Für SAML mit Okta erforderliche Cloud-Features

Bevor Sie die Aufgaben in diesem Artikel ausführen, müssen Sie sich an den Citrix Support wenden, um das Feature **SendNameIDPolicyInSAMLRequest** zu aktivieren. Mit diesem Feature kann Citrix Cloud die Richtlinie **NameID** in der SAML-Anforderung an Ihren SAML-Anbieter als **Keine Angabe** übergeben. Das Feature ist nur für die Verwendung mit Okta aktiviert.

Sie können diese Features anfordern, indem Sie sich bei Ihrem Citrix Konto anmelden und ein Ticket über die Citrix Support-Website öffnen.

Anforderungen

Dieser Artikel umfasst eine Aufgabe zur Erstellung einer SAML-Anwendung in der Okta-Verwaltungskonsole. Diese Anwendung erfordert ein SAML-Signaturzertifikat für Ihre Citrix Cloud-Region.

> **Wichtig:**
>
> Das Signaturzertifikat muss im PEM-Format codiert sein. Citrix Cloud akzeptiert keine Signaturzertifikate in anderen Codierungsformaten.

Sie können das Zertifikat aus den Citrix Cloud SAML-Metadaten für Ihre Region mithilfe eines Extraktionstools extrahieren (z. B. https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract). Citrix empfiehlt die Beschaffung des Citrix Cloud-SAML-Zertifikats im Voraus, damit es bei Bedarf zur Verfügung steht.

In den Schritten in diesem Abschnitt wird beschrieben, wie Sie das Signaturzertifikat mithilfe des Extraktionstools auf https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract erhalten.

Zum Abrufen der Citrix Cloud-Metadaten für Ihre Region gehen Sie folgendermaßen vor:

1. Geben Sie in dem verwendeten Extraktionstool die Metadaten-URL Ihrer Citrix Cloud-Region ein:
   - Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com/saml/metadata` ein.
   - Geben Sie für die Region Japan `https://saml.citrixcloud.jp/saml/metadata` ein.
   - Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us/saml/metadata` ein.
2. Klicken Sie auf **Load**. Das extrahierte Zertifikat wird unter der eingegebenen URL angezeigt.
3. Klicken Sie auf **Download**, um das Zertifikat im PEM-Format herunterzuladen.

Synchronisieren von Konten mit dem Okta-AD-Agent

Um Okta als SAML-Anbieter zu verwenden, müssen Sie zunächst Ihr On-Premises-Active Directory mit Okta integrieren. Installieren Sie dafür den Okta-AD-Agent in Ihrer Domäne und fügen Ihr AD zu Ihrer Okta-Organisation hinzu. Hinweise zum Bereitstellen des Okta-AD-Agent finden Sie unter Get started with Active Directory integration auf der Okta-Website.

Anschließend importieren Sie Ihre AD-Benutzer und -Gruppen in Okta. Schließen Sie beim Importieren die folgenden Werte ein, die Ihren AD-Konten zugeordnet sind:

- E-Mail
- SID

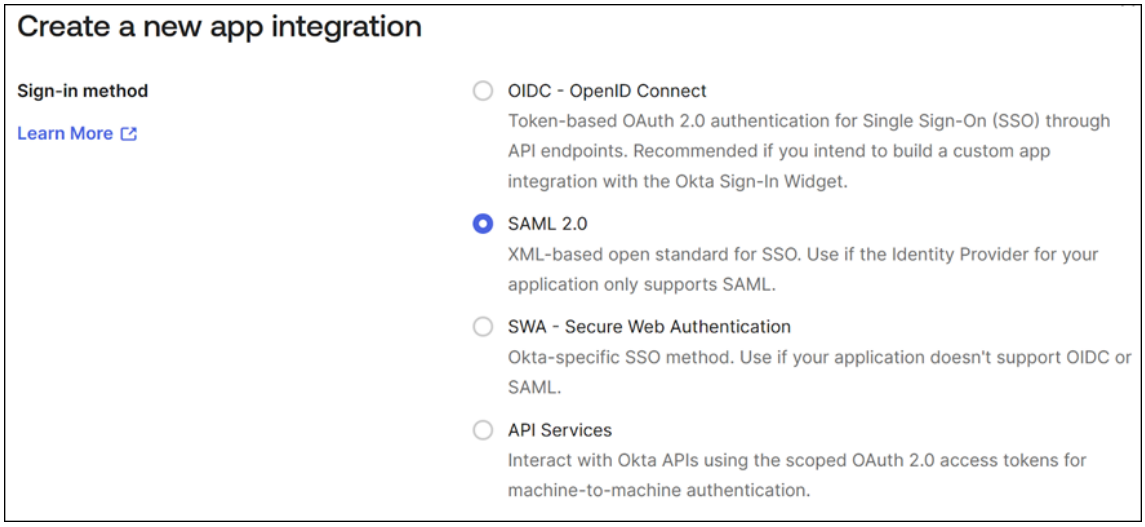
- UPN
- OID

Synchronisieren der AD-Benutzer und -Gruppen mit Ihrer Okta-Organisation:

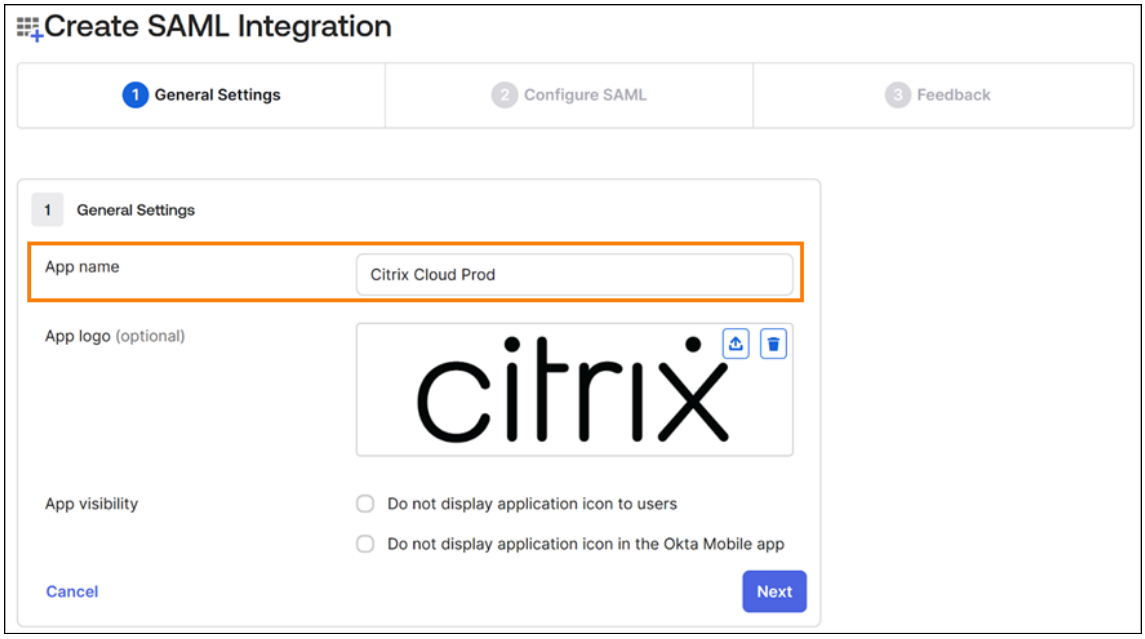
1. Installieren und konfigurieren Sie den Okta-AD-Agent. Ausführliche Anweisungen finden Sie in den folgenden Artikeln auf der Okta Website:
   - Install the Okta Active Directory agent
   - Configure Active Directory import and account settings
   - Configure Active Directory provisioning settings
2. Fügen Sie Ihre AD-Benutzer und -Gruppen durch manuellen oder automatisierten Import zu Okta hinzu. Weitere Hinweise zu Importverfahren finden Sie unter Manage Active Directory users and groups auf der Okta-Website.

Okta-SAML-Anwendung für die Workspace-Authentifizierung konfigurieren

1. Melden Sie sich mit einem Administratorkonto mit Berechtigungen zum Hinzufügen und Konfigurieren von SAML-Anwendungen bei Ihrer Okta-Organisation an.
2. Wählen Sie in der Verwaltungskonsole **Applications > Applications > Create App Integration** und dann **SAML 2.0**. Wählen Sie **Weiter**.



3. Geben Sie unter **App Name** einen Anzeigenamen für die Anwendung ein. Wählen Sie **Weiter**.



4. Konfigurieren Sie im Abschnitt **SAML Settings** die Citrix Cloud-Dienstanbieterverbindung:

   a) Geben Sie unter **Single sign-on URL** die URL ein, die der Citrix Cloud-Region für Ihren Citrix Cloud-Kunden entspricht:

   - Geben Sie für Kundennummern in der Region Europäische Union, USA oder Asien-Pazifik Süd `https://saml.cloud.com/saml/acs` ein.
   - Geben Sie für Kundennummern in Japan `https://saml.citrixcloud.jp/saml/acs` ein.
   - Geben Sie für Kundennummern in der Region Citrix Cloud Government `https://saml.cloud.us/saml/acs` ein.

   b) Wählen Sie **Use this for Recipient and Destination URL**.

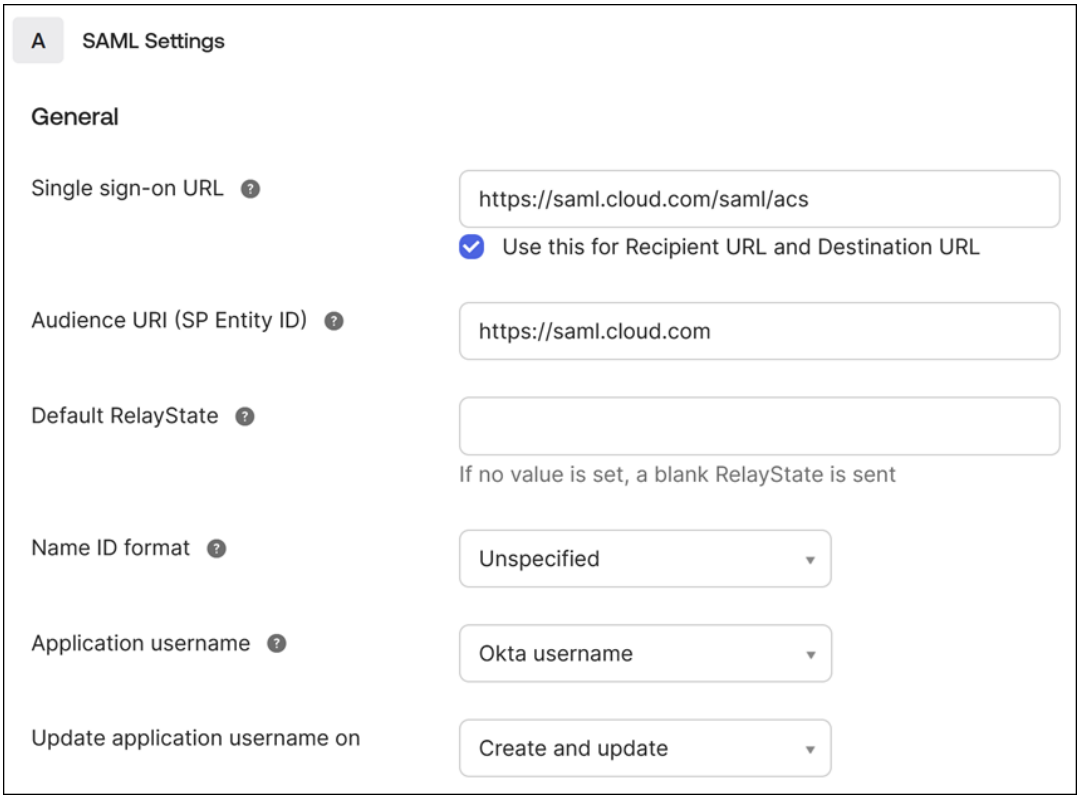
   c) Geben Sie unter **Audience URI (SP Entity ID)** die URL ein, die der Citrix Cloud-Region für Ihren Citrix Cloud-Kunden entspricht:

   - Geben Sie für Kundennummern in der Region Europäische Union, USA oder Asien-Pazifik Süd `https://saml.cloud.com` ein.
   - Geben Sie für Kundennummern in Japan `https://saml.citrixcloud.jp` ein.
   - Geben Sie für Kundennummern in der Region Citrix Cloud Government `https://saml.cloud.us` ein.

   d) Wählen Sie unter **Name ID Format** die Option **Unspecified**. Die NameID-Richtlinie, die Citrix Cloud innerhalb der SAML-Anfrage sendet, muss dem in der Okta-SAML-Anwendung angegebenen NameID-Format entsprechen. Wenn diese Elemente nicht übereinstimmen, führt die Aktivierung von **Authentifizierungsanforderung signieren** zu einem Fehler von Okta.

e) Wählen Sie unter **Application username** die Option **Okta username**.

Das folgende Beispiel zeigt die korrekte Konfiguration für die Regionen USA, EU und Asien-Pazifik Süd:



> **Wichtig:**
>
> Die Einstellung **Namens-ID** muss als **Keine Angabe** konfiguriert werden. Wenn Sie für diese Einstellung einen anderen Wert verwenden, schlägt die SAML-Anmeldung fehl.

f) Klicken Sie auf **Show Advanced Settings** und konfigurieren Sie die folgenden Einstellungen:

- Wählen Sie unter **Response** die Option **Signed**.
- Wählen Sie unter **Assertion Signature** die Option **Signed**.
- Wählen Sie unter **Signature Algorithm** die Option **RSA-SHA256**.
- Wählen Sie unter **Assertion Encryption** die Option **Unencrypted**.

g) Laden Sie unter **Signature Certificate** das SAML-Signaturzertifikat für Ihre Citrix Cloud-Region im PEM-Format hoch. Anweisungen zur Beschaffung des SAML-Signaturzertifikats finden Sie unter Anforderungen in diesem Artikel.

h) Wählen Sie unter **Enable Single Logout** die Option **Allow application to initiate Single Logout**.

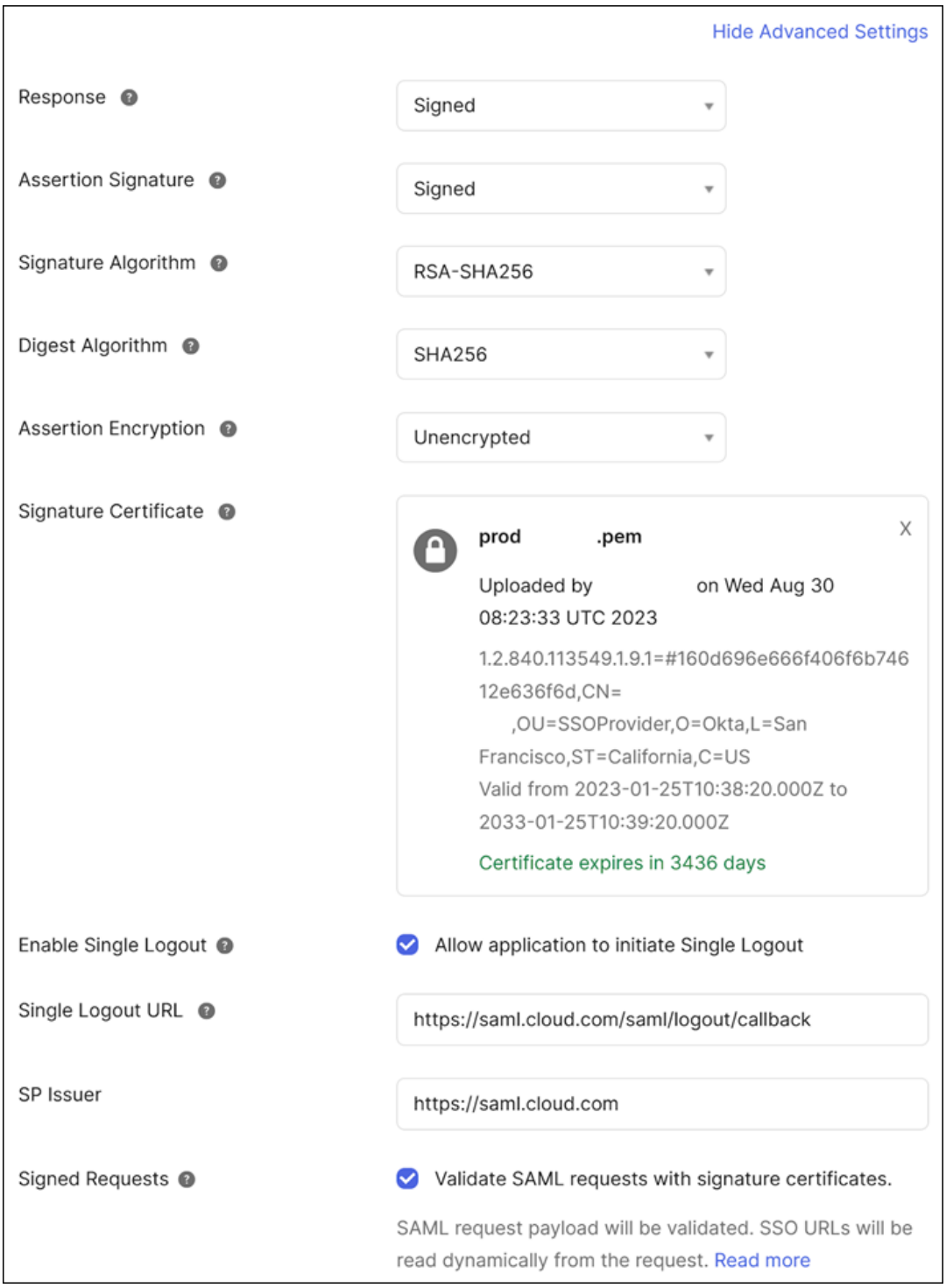
i) Geben Sie unter **Single Logout URL** die URL ein, die Ihrer Citrix Cloud-Region entspricht:

- Geben Sie für die Regionen Europäische Union, USA und Asien-Pazifik Süd `https://saml.cloud.com/saml/logout/callback` ein.
- Geben Sie für die Region Japan `https://saml.citrixcloud.jp/saml/saml/logout/callback` ein.
- Geben Sie für die Region Citrix Cloud Government `https://saml.cloud.us/saml/logout/callback` ein.

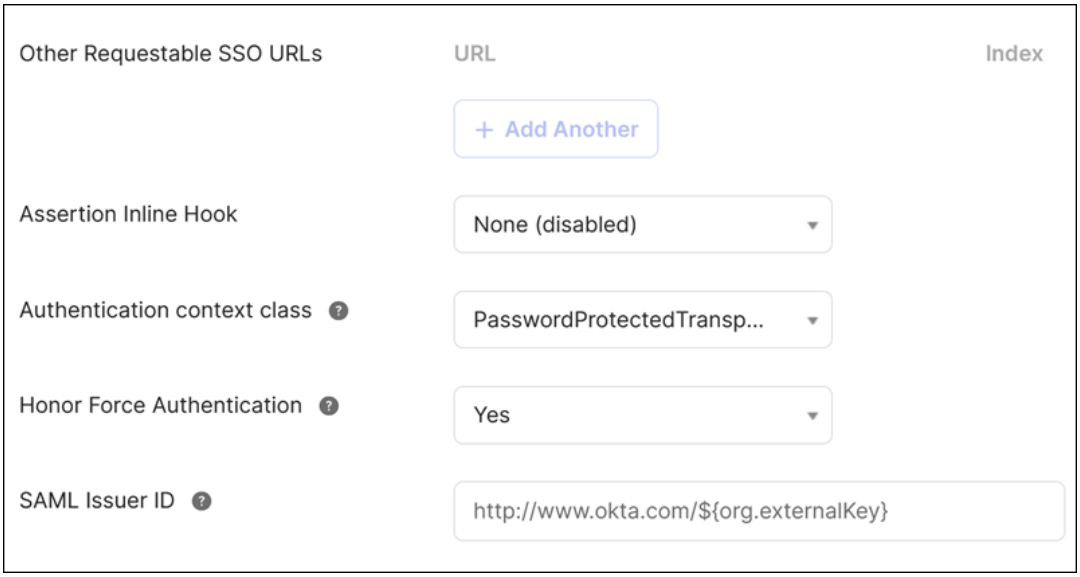
j) Geben Sie für **SP Issuer** den Wert ein, den Sie zuvor in **Audience URI (SP Entity ID)** eingegeben haben (Schritt 4c dieser Aufgabe).

k) Wählen Sie unter **Signed Requests** die Option **Validate SAML requests with signature certificates**.

Die folgende Abbildung zeigt die korrekte Konfiguration für die Regionen USA, EU und Asien-Pazifik Süd:

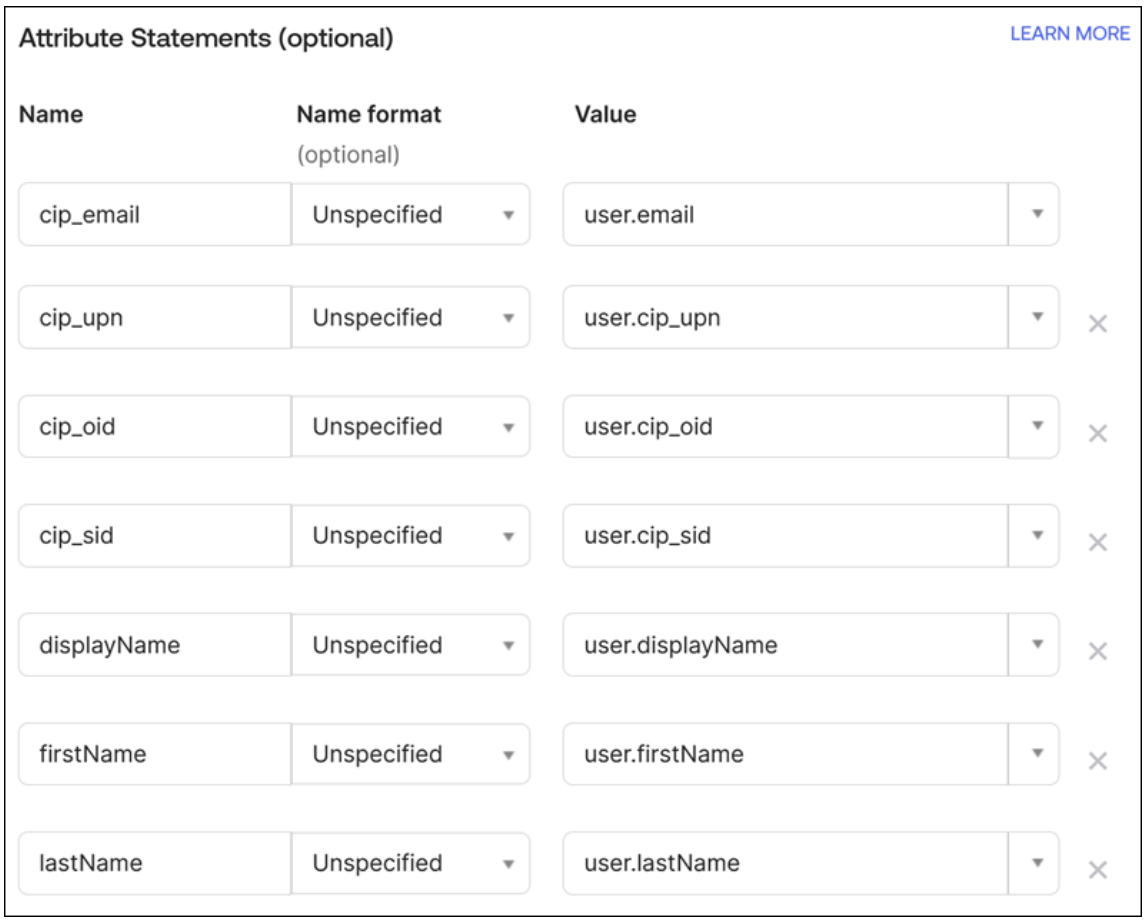


l) Übernehmen Sie für alle anderen erweiterten Einstellungen die Standardwerte.

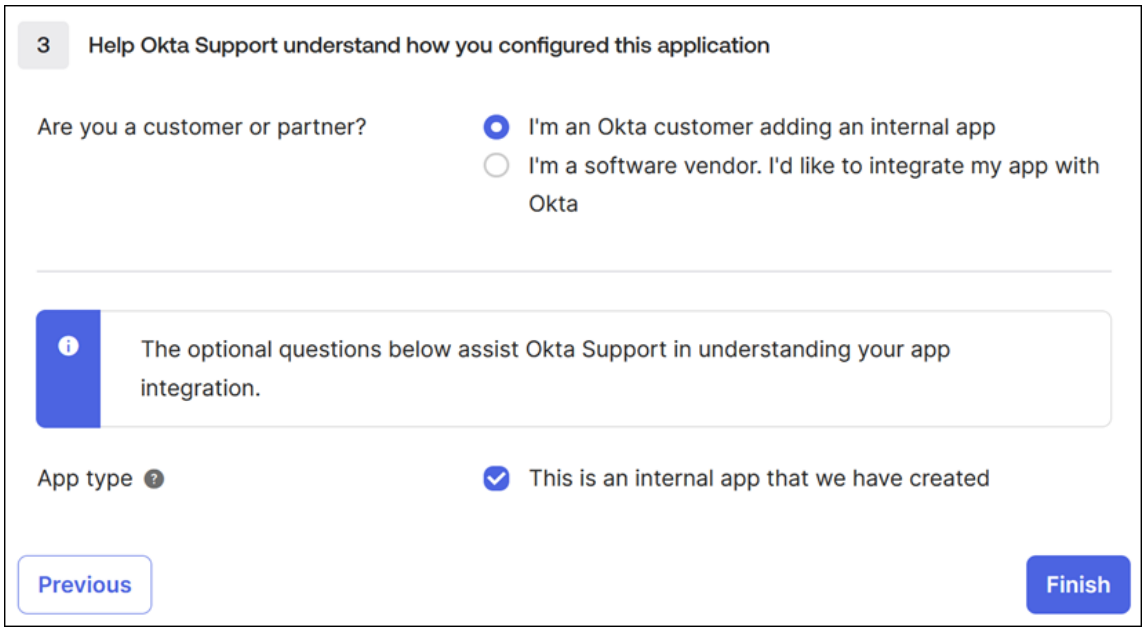


5. Geben Sie unter **Attribute Statements (optional)**die folgenden Werte für **Name**, **Name format** und **Value** ein:

Name	Name format	Wert
cip_email	Keine Angabe	user.email
cip_upn	Keine Angabe	user.cip_upn
cip_oid	Keine Angabe	user.cip_oid
cip_sid	Keine Angabe	user.cip_sid
displayName	Keine Angabe	user.displayName
firstName	Keine Angabe	user.firstName
lastName	Keine Angabe	user.lastName



6. Wählen Sie **Weiter**. Die Okta-Konfigurationserklärung wird angezeigt.



7. Wählen Sie für **Are you a customer or partner?** die Option **I'm an Okta customer adding an internal app**.

8. Wählen Sie unter **App type** die Option **This is an internal app that we have created**.
9. Wählen Sie **Finish**, um Ihre Konfiguration zu speichern. Die Profilseite für Ihre SAML-Anwendung mit dem Inhalt der Registerkarte **Sign On** wird angezeigt.

Wählen Sie nach der Konfiguration die Registerkarte **Assignments** und weisen Sie der SAML-Anwendung Benutzer und Gruppen zu.

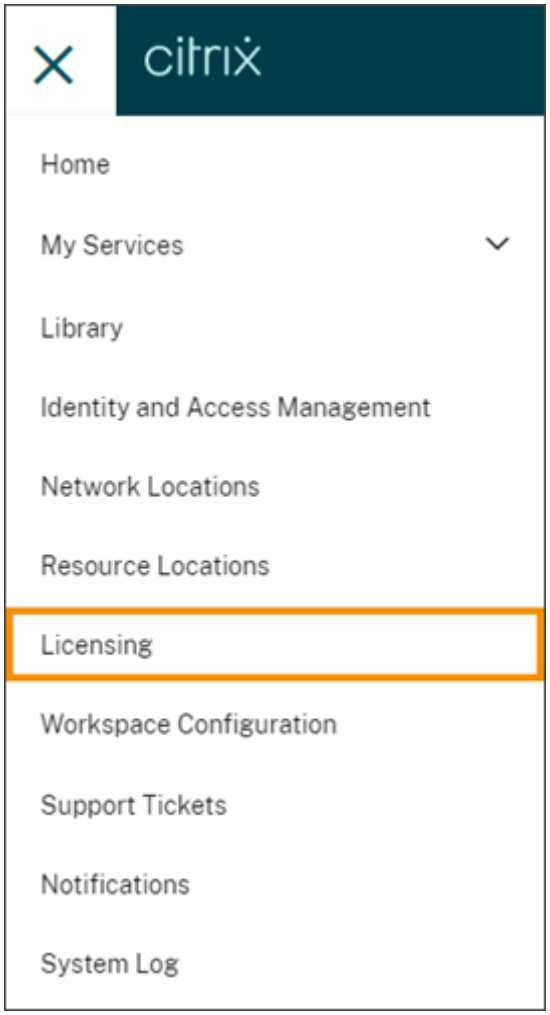
Lizenzierung für Citrix Cloud

September 28, 2023

Citrix Cloud bietet die Überwachung von Lizenzen und Lizenznutzung für bestimmte Cloudservices. Die Überwachung von Lizenzen und Lizenznutzung ist auch für On-premises-Bereitstellungen verfügbar, in denen Citrix Lizenzserver bei Citrix Cloud registriert ist.

Lizenzierung für Unternehmenskunden

Unternehmenskunden können zugewiesene Lizenzen und Lizenznutzung für unterstützte Cloudservices überwachen, indem sie im Menü von Citrix Cloud die Option **Lizenzierung** wählen.



Weitere Informationen zur unternehmensbezogenen Überwachung von Lizenzen und Lizenznutzung für Cloudservices finden Sie unter Überwachen der Lizenzen und der aktiven Nutzung von Cloud Services.

Lizenzierung für On-premises-Bereitstellungen

Unternehmenskunden mit einer On-premises-Bereitstellung von Citrix Virtual Apps and Desktops können mit Citrix Cloud Lizenzen und Lizenznutzung für das Benutzer-/Gerätelizenzmodell und das Gleichzeitig-Lizenzmodell überwachen. Wenn Kunden Citrix Lizenzserver bei Citrix Cloud registrieren, können sie auf der Seite **Lizenzierte Bereitstellungen** in Citrix Cloud folgende Aufgaben ausführen:

- Überwachen des Berichtsstatus registrierter Lizenzserver
- Anzeigen von Lizenzzuweisungen und Nutzungstrends für Bereitstellungen, die das Benutzer-/Gerätelizenzmodell verwenden.

- Anzeigen von Spitzennutzungstrends für Bereitstellungen, die das Gleichzeitig-Lizenzmodell verwenden.

Weitere Informationen zur Überwachung von Lizenzen und Verbrauch für On-premises-Bereitstellungen von Virtual Apps and Desktops finden Sie unter Überwachen von Lizenzen und Lizenznutzung für on-premises Bereitstellungen.

Lizenzierung für Citrix Service Provider (CSP)

Citrix Service Provider können die folgenden Tools verwenden, um Produktlizenzen und Lizenznutzung zu verstehen und Berichte zu erstellen:

- License Usage Insights ist ein kostenloser Service in Citrix Cloud, der Daten zur Produktnutzung für Einzelmandanten- und Mehrmandantenkunden sammelt und zusammenfasst. Weitere Informationen finden Sie unter Lizenzierung für Citrix Service Provider (CSP).
- Die Lizenzierungsfunktion in Citrix Cloud ermöglicht Kunden von CSPs die Überwachung ihrer Lizenzen und des Lizenzverbrauchs für unterstützte Citrix DaaS-Produkte (früher Citrix Virtual Apps and Desktops Service). CSPs können sich unter dem Citrix Cloud-Konto ihres Kunden anmelden, um diese Informationen anzuzeigen und zu exportieren. Weitere Informationen finden Sie in den folgenden Artikeln:
  - Überwachen von Kundenlizenzen und -nutzung für Citrix DaaS
  - Überwachen von Kundenlizenzen und -nutzung für Citrix DaaS Standard für Azure

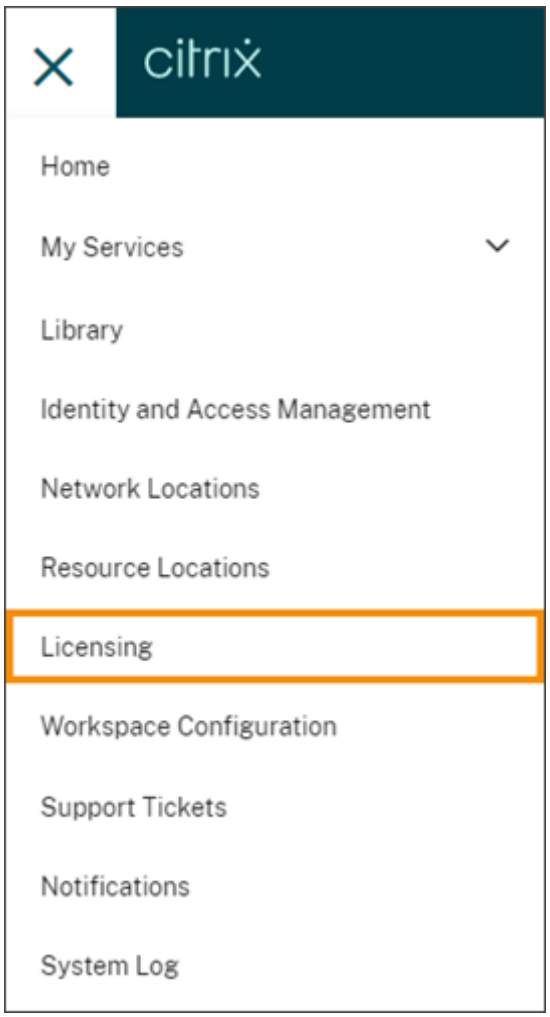
Überwachen der Lizenzen und der aktiven Nutzung von Cloud Services

September 28, 2023

Unter “Lizenzierung”in der Citrix Cloud können Sie den Lizenzverbrauch für die von Ihnen erworbenen Cloudservices im Auge behalten. Mit den Zusammenfassungs- und Detailberichten können Sie:

- Lizenzverfügbarkeit und -zuweisungen auf einen Blick anzeigen
- Aktive Nutzungstrends pro Tag und Monat für zutreffende Cloudservices anzeigen
- Einzelne Lizenzzuweisungsdetails und Verwendungstrends anzeigen
- Lizenzverwendungsdaten in CSV exportieren

Um Lizenzdaten für Ihre Cloudservices anzuzeigen, wählen Sie im Konsolenmenü **Lizenzierung**.



Hinweis:

In diesem Artikel werden die Lizenzierungsfeatures, die für alle unterstützten Citrix Cloud-Services gelten, beschrieben. Einige Aspekte der Lizenzierung (z. B. die Lizenzzuweisung) können je nach Service unterschiedlich sein. Weitere Informationen zu Lizenzen und zur Nutzung der einzelnen Services finden Sie in den folgenden Artikeln:

- Lizenzen und aktive Nutzung für Citrix DaaS überwachen (Benutzer/Gerät)
- Überwachen von Lizenzen und Verwendungsspitzen für Citrix DaaS und Citrix DaaS Standard für Azure (Gleichzeitig-Lizenzmodell)
- Überwachen von Lizenzen und aktiver Nutzung für Citrix DaaS Standard für Azure (Benutzer/Gerät)
- Überwachen von Lizenzen und aktiver Nutzung für Endpoint Management Service
- Überwachen der Bandbreitennutzung für Gateway Service
- Überwachen von Lizenzen und Nutzung für Secure Private Access

Unterstützte Regionen und Cloudservices

Die Übersicht unter "Lizenzierung"ist nur für unterstützte Services in den Regionen USA, EU und Asien-Pazifik verfügbar.

"Lizenzierung"wird für folgende Cloudservices unterstützt:

- Citrix DaaS (Benutzer-/Geräte- und Gleichzeitig-Lizenzmodell) —früher Citrix Virtual Apps and Desktops Service
- Citrix DaaS Standard für Azure (Benutzer-/Gerätelizenzmodell) —früher Citrix Virtual Apps and Desktops Standard für Azure
- Endpoint Management
- Gateway
- Secure Private Access (zuvor "Secure Workspace Access")

Multityplizenzierung für Citrix DaaS

Die Lizenzierung in Citrix Cloud unterstützt die Multityplizenzierung für Citrix DaaS. Wenn sowohl das Benutzer-/Gerätelizenzmodell als auch das Gleichzeitig-Lizenzmodell (CCU-Lizenzen) in ein Citrix Cloud-Konto eingeführt werden, wird die Lizenznutzung auf der Konsolenseite "Lizenzierung"unter dem jeweiligen Lizenzierungsmodus angezeigt.

Citrix empfiehlt, die Multityplizenzierung auf Site- und Bereitstellungsgruppenebene einzurichten, bevor Sie die Seite "Lizenzierung"aufrufen. Andernfalls sind die angezeigten Informationen möglicherweise nicht korrekt. Anweisungen finden Sie unter Multityplizenzierung in der Dokumentation zu Citrix DaaS.

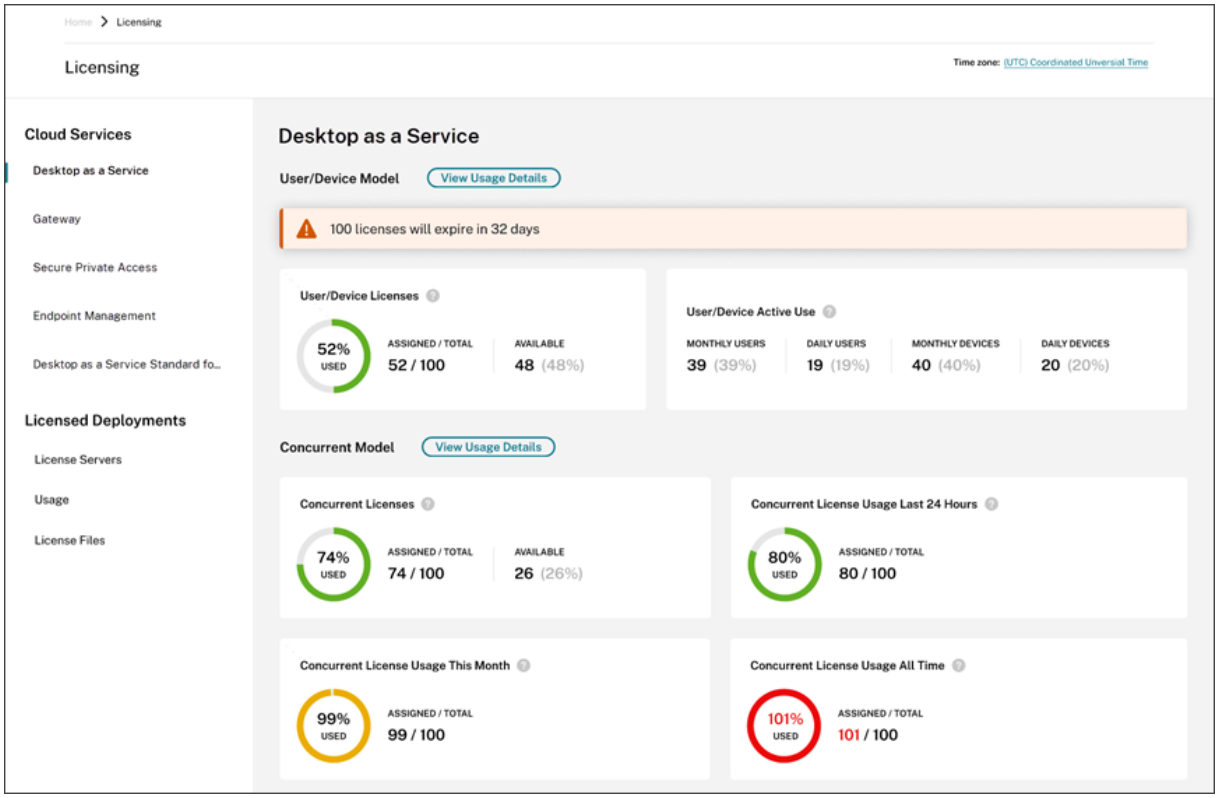
Wenn auf der Konsolenseite "Lizenzierung"die Lizenznutzung mit Multityplizenzierung trotz erfolgreicher Einrichtung mit Web Studio oder PowerShell nicht korrekt angezeigt wird, haben Sie folgende Optionen:

- Warten Sie 30 Tage und geben Sie ungenutzte Lizenzen frei.
- Wenden Sie sich an den Citrix Customer Service.

Lizenzzuweisung

Benutzern wird generell bei der ersten Verwendung des Cloudservices eine Lizenz zugewiesen. Einige Services weisen Lizenzen je nach verwendetem Lizenzmodell unterschiedlich zu. Weitere Informationen dazu, wie Lizenzen für jeden Service zugewiesen werden, finden Sie in den oben erwähnten Artikeln zu "Lizenzierung".

Zusammenfassung und Details zur Lizenzierung



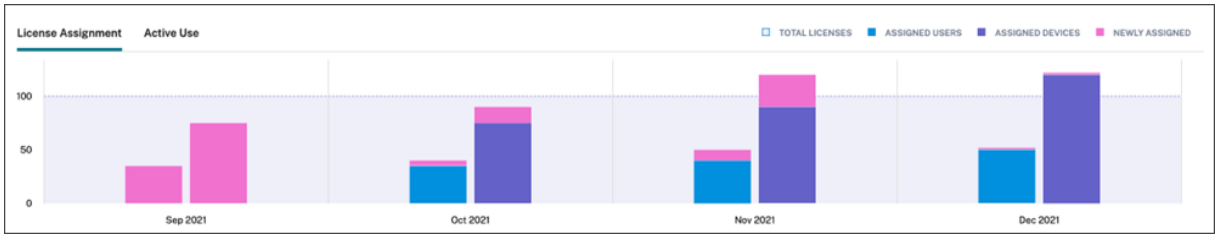
Die Zusammenfassung unter “Lizenzierung”bietet für jeden unterstützten Service einen Überblick über Folgendes:

- Prozentsatz der insgesamt erworbenen Lizenzen, die zugewiesen sind Wenn sich der Prozentsatz 100 % nähert, wechselt der Prozentsatz von grün zu gelb. Wenn der Prozentsatz 100 % überschreitet, wird der Prozentsatz rot angezeigt.
- Das Verhältnis zugewiesener zu erworbenen Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen.
- Die verbleibende Zeit bis zum Ablauf des Cloudserviceabonnements. Wenn das Abonnement innerhalb der nächsten 90 Tage abläuft, wird eine Warnmeldung angezeigt.

Bei einigen Services kann diese Zusammenfassung weitere Informationen enthalten, z. B. zur aktiven Nutzung. Weitere Informationen zu servicespezifischen Details finden Sie in den oben erwähnten Artikeln zu “Lizenzierung”.

Nutzungstrends und Lizenzaktivität

Klicken Sie für eine detaillierte Ansicht Ihrer Cloudservicelizenzen auf **Nutzungsdetails anzeigen**. Sie können dann eine Aufschlüsselung der Nutzungstrends und der Verbraucher von Cloudservicelizenzen anzeigen.



Diese Aufschlüsselung enthält je nach Cloudservice unterschiedliche Informationen. Weitere Informationen zu servicespezifischen Nutzungstrends und zur Lizenzaktivität finden Sie in den oben erwähnten Artikeln zu "Lizenzierung".

Freigeben zugewiesener Lizenzen

Eine zugewiesene Lizenz kann in der Regel freigegeben werden, wenn der Lizenzverbraucher den Cloudservice an 30 aufeinanderfolgenden Tagen nicht genutzt hat. Nach dem Freigeben einer Lizenz erhöht sich die Anzahl der verfügbaren Lizenzen und die Anzahl der zugewiesenen Lizenzen nimmt entsprechend ab.

Bei einigen Services kann die Freigabe von Lizenzen je nach verwendetem Lizenzmodell unterschiedlich verlaufen. Weitere Informationen zur Freigabe von Lizenzen für einen spezifischen Service finden Sie in den oben erwähnten Artikeln zu "Lizenzierung".

Häufig gestellte Fragen

- **Verhindert Citrix die Verwendung des Cloudservices, wenn zugewiesene Lizenzen erworbene Lizenzen überschreiten?** Nein, Citrix verhindert keine Servicestarts, wenn Sie Ihr Cloudlizenzkontingent überschreiten. Die Lizenznutzung enthält Informationen zum Verständnis Ihrer Cloudlizenzverwendung. Daher erwartet Citrix, dass Sie Ihre Lizenzzuweisungen überwachen und innerhalb Ihrer erworbenen Lizenzmenge bleiben. Wenn Sie zu irgendeinem Zeitpunkt glauben, dass Sie Ihren Service überbeanspruchen werden, empfiehlt Citrix Ihnen, sich an Ihren Vertriebsmitarbeiter zu wenden, um Ihre Lizenzanforderungen zu besprechen.
- **Welche Lizenzinformationen werden erfasst?** Derzeit werden nur Lizenzinformationen erfasst, die mit Benutzeranmeldungen verknüpft sind.
- **Wird Multityplizenzierung mit Citrix DaaS unterstützt (z. B. mit Benutzer-/Geräte- und Gleichzeitig-Lizenzmodell)?** Ja. Weitere Informationen finden Sie unter Multityplizenzierung in diesem Artikel.
- **Wird die Lizenzierung mehrerer Editionen für Citrix DaaS unterstützt? Kann ich beispielsweise die Premium Edition und die Advanced Edition mit demselben Citrix Cloud-Konto verwenden?** Nein, dieser Anwendungsfall wird nicht unterstützt. Eine Citrix DaaS-Site kann nur für eine Edition lizenziert werden. Wenn Sie mehrere Citrix DaaS-Instanzen in demselben Citrix Cloud-Konto verwenden möchten, muss die Edition dieselbe sein.

- **Was ist der Unterschied zwischen Überwachungsberichten (in Director) und den Angaben zu CCU-Lizenzen?** Der Überwachungsbericht mit den Angaben zu gleichzeitigen Sitzungen misst nicht die Anzahl verwendeter CCU-Lizenzen, sondern bietet eine andere Interpretation. Wenn Sie Verwendungsspitzen für CCU-Lizenzen anhand der Anzahl gleichzeitiger Sitzungen in Director darstellen und prognostizieren, ist die sich daraus ergebende Anzahl erforderlicher CCU-Lizenzen in den meisten Fällen zu hoch. Verwenden Sie nicht den Überwachungsbericht in Director als Ersatz für einen Bericht zur CCU-Lizenznutzung. Die beiden Hauptunterschiede zwischen diesen Berichterstellungstools sind:
  - **Prüfintervall:** Für die Lizenzierung gilt ein Prüfintervall von fünf Minuten. Alle fünf Minuten erfasst Citrix Cloud, wie viele eindeutige Geräte aktuell mit dem Dienst verbunden sind. Die Ergebnisse aller Fünf-Minuten-Prüfintervalle werden aggregiert, um die Verwendungsspitze für 24 Stunden, einen Monat bzw. die Vertragsdauer zu bestimmen. Der Überwachungsbericht in Director kann Intervalle von bis zu zwei Stunden anzeigen, je nachdem, wie der Bericht ausgeführt wird.
  - **Eindeutigkeit:** Die Lizenzierung überprüft beim Sitzungsstart, ob es sich um eindeutige Geräte handelt. Der Überwachungsbericht unterscheidet nicht nach eindeutigen Geräten.
- **Nachdem Benutzer zu einer neuen Cloudservice-Instanz migriert wurden (z. B. weil ich den Domänennamen für meine Organisation geändert habe), warum werden meine verwendeten Lizenzen für die gleichen Benutzer doppelt gezählt?* - Citrix Cloud verwendet den Benutzerprinzipalnamen (UPN), um eindeutige Benutzer zu zählen. Wenn ein Benutzer vor und nach der Migration auf den Cloudservice zugegriffen hat, erfasst Citrix Cloud zwei eindeutige UPNs für den Benutzer, jeweils mit einem anderen Domänennamen. Aus diesem Grund wird derselbe Benutzer in Citrix Cloud zweimal erfasst. Sie können die ältere Lizenzzuweisung nach 30 Tagen freigeben, sofern der Benutzer nicht unter dem alten Domänennamen auf den Service zugreift. Citrix verhindert keine Servicestarts, wenn Sie Ihr Cloudlizenzkontingent überschreiten.
- **Warum sehe ich doppelte Lizenzen für einen Benutzer oder ein Gerät?* - Grund ist die beabsichtigte Funktionsweise der Workspace-App für HTML5 und der lokal installierten Workspace-App. Starts über die Workspace-App für HTML5 verbrauchen eine Benutzer/Gerätelizenz. Starts über die lokal installierte Workspace-App verbrauchen auch eine Benutzer-/Gerätelizenz. Wenn ein Benutzer eine App über die Workspace-App für HTML5 startet und später über eine lokal installierte Version der Workspace-App, zeigt Citrix Cloud den Verbrauch von zwei Lizenzen an. Dies wirkt sich nicht auf die Benutzerkonnektivität aus, kann jedoch zu überhöhten Angaben zur Gerätelizenznutzung in der Lizenzierungskonsole führen Citrix verhindert keine Servicestarts, wenn Sie Ihr Cloudlizenzkontingent überschreiten.

Lizenzen und aktive Nutzung für Citrix DaaS überwachen (Benutzer/Gerät)

November 2, 2023

In diesem Artikel wird beschrieben, wie Sie Cloudservice-Lizenzzuweisungen verwalten und die aktive Nutzung mithilfe der Lizenzierungskonsole in Citrix Cloud überwachen können.

Wenn Sie Citrix Azure Consumption Fund für Ihre Service-Bereitstellung erworben haben, finden Sie weitere Informationen unter Monitor Citrix Managed Azure resource consumption for Citrix DaaS.

Lizenzzuweisung

Citrix Cloud weist eine Lizenz zu, wenn ein eindeutiger Benutzer oder ein eindeutiges Gerät zum ersten Mal eine App oder einen Desktop startet.

Kürzung von Domänennamen

Wenn Sie mehrere Domänen hosten und Benutzer mit ähnlichen Konten in diesen Domänen haben (z. B. `johnsmith@company.com` und `johnsmith@mycompany.com`), können Sie zulassen, dass Citrix Cloud die Kontodomäne ignoriert und nur den Benutzernamen des Kontos berücksichtigt (z. B. johnsmith). Dies wird als *Kürzung von Domänennamen* bezeichnet. Standardmäßig ist die Kürzung von Domänennamen deaktiviert.

Wenn die Kürzung von Domänenamen aktiviert ist, ändert sich die Berechnung eindeutiger Benutzer in Citrix Cloud. `johnsmith@company.com` und `johnsmith@mycompany.com` werden in Citrix Cloud nicht mehr als zwei eindeutige Benutzer gezählt, sondern als eindeutiger Benutzer “johnsmith” . Diese Berechnungsänderung wirkt sich auf die folgenden Lizenzdaten aus:

- Lizenzzuweisung
- Aktive Nutzung
- Lizenznutzungstrends im Zeitverlauf
- Lizenzen, die zur Freigabe in Frage kommen

Die Änderungen der Lizenzdaten werden auch beim Exportieren von Daten aus der Lizenzierungskonsole in eine CSV-Datei angewendet.

> **Hinweis:**
>
> Wenn Sie mehrere Domänen mit ähnlichen Konten hosten, bei denen der Benutzername geringfügige Unterschiede aufweist (z. B. wenn ein Benutzer die Konten `johnsmith@company`

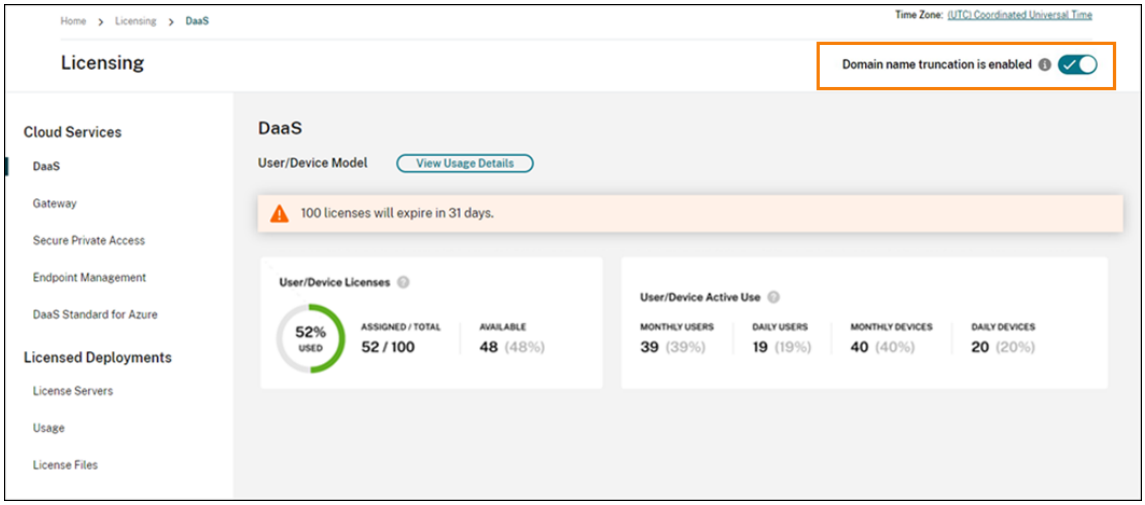
> .com und jsmith@newcompany.com) hat, hat die Kürzung des Domänennamens keine Auswirkung auf die Berechnungen in Citrix Cloud. Citrix Cloud zählt johnsmith und jsmith weiterhin als Einzelbenutzer, selbst wenn die Konten derselben Person gehören.

Kürzung von Domänenamen aktivieren oder deaktivieren

Standardmäßig ist die Kürzung von Domänennamen deaktiviert. Die Kürzung von Domänennamen wirkt sich auf die Benutzer-/Gerätenutzungsdaten aus, sobald Sie das Feature aktivieren oder deaktivieren. Wenn Sie die Kürzung von Domänennamen beispielsweise in einem bestimmten Monat deaktivieren, sind die Daten betroffen, die Citrix Cloud in diesem Monat aufzeichnet. Historische Daten der vergangenen Monate, in denen das Feature deaktiviert war, bleiben unberührt. Wenn Sie die Kürzung von Domänennamen hingegen in einem bestimmten Monat deaktivieren, sind die Daten betroffen, die Citrix Cloud in diesem Monat aufzeichnet. Historische Daten der vergangenen Monate, in denen das Feature aktiviert war, bleiben unberührt.

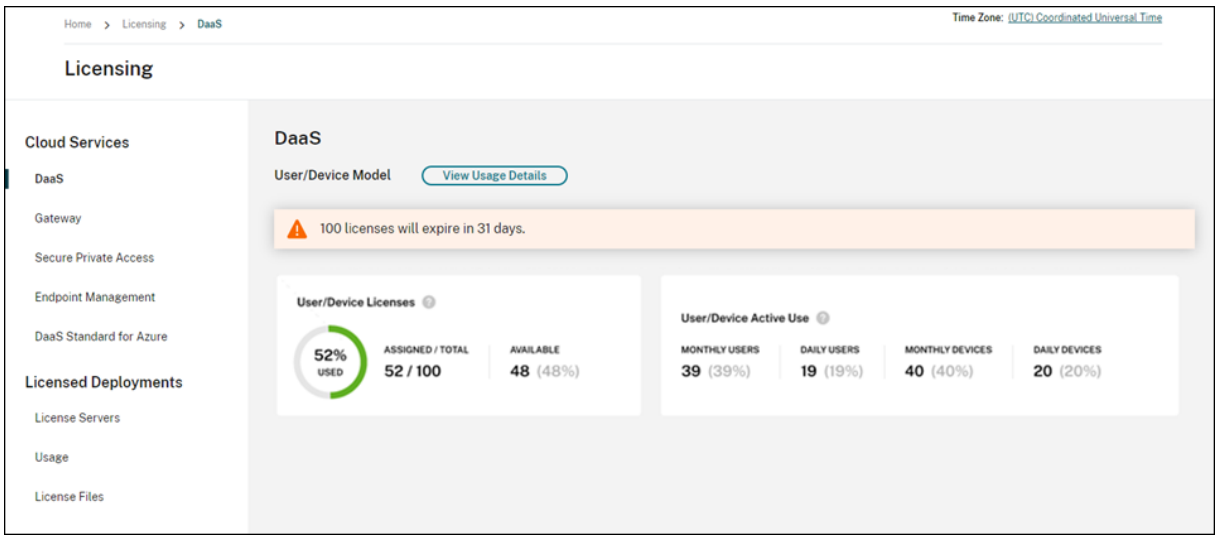
Gehen Sie zum Aktivieren oder Deaktivieren der Kürzung von Domänennamen folgendermaßen vor:

1. Klicken Sie in der Lizenzierungskonsole oben rechts auf den Schalter.



2. Wenn Sie aufgefordert werden, Ihre Aktion zu bestätigen, wählen Sie **Ja, ich verstehe**.

Zusammenfassung zur Lizenzierung



Die Zusammenfassung der Lizenzierung bietet einen Überblick über die folgenden Informationen:

- Prozentsatz der insgesamt erworbenen Lizenzen, die zugewiesen wurden. Wenn sich der Prozentsatz 100 % nähert, wechselt der Prozentsatz von grün zu gelb. Wenn der Prozentsatz 100 % überschreitet, wird der Prozentsatz rot angezeigt.

  Die Gesamtanzahl an erworbenen Lizenzen umfasst alle erworbenen Lizenzen für Citrix DaaS-Editionen, die das Benutzer-/Gerätelizenzmodell verwenden.

- Das Verhältnis zugewiesener zu erworbenen Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen.
- Statistik der aktiven Nutzung pro Monat und Tag:
  - "Monatliche aktive Nutzung"bezieht sich auf die Anzahl eindeutiger Benutzer oder Geräte, die den Service in den letzten 30 Tagen genutzt haben.
  - "Tägliche aktive Nutzung"bezieht sich auf die Anzahl eindeutiger Benutzer oder Geräte, die den Service in den letzten 24 Stunden genutzt haben.
- Die verbleibende Zeit bis zum Ablauf des Cloudserviceabonnements. Wenn das Abonnement innerhalb der nächsten 90 Tage abläuft, wird eine Warnmeldung angezeigt.

Berechnung von zugewiesenen Lizenzen und aktiver Nutzung

Um das Benutzer-/Gerätelizenzmodell für Citrix DaaS genau wiederzugeben, erfasst Citrix Cloud, wie viele eindeutigen Benutzer und Geräte den Service verwendet haben. Zum Bestimmen der zugewiesenen Lizenzen verwendet Citrix Cloud den niedrigeren der beiden Werte. Zum Bestimmen der aktiven Nutzung verwendet Citrix Cloud jeden Wert als Anzahl der aktiven Benutzer und aktiven Geräte in einem bestimmten Zeitraum.

Beispiel für die Berechnung zugewiesener Lizenzen

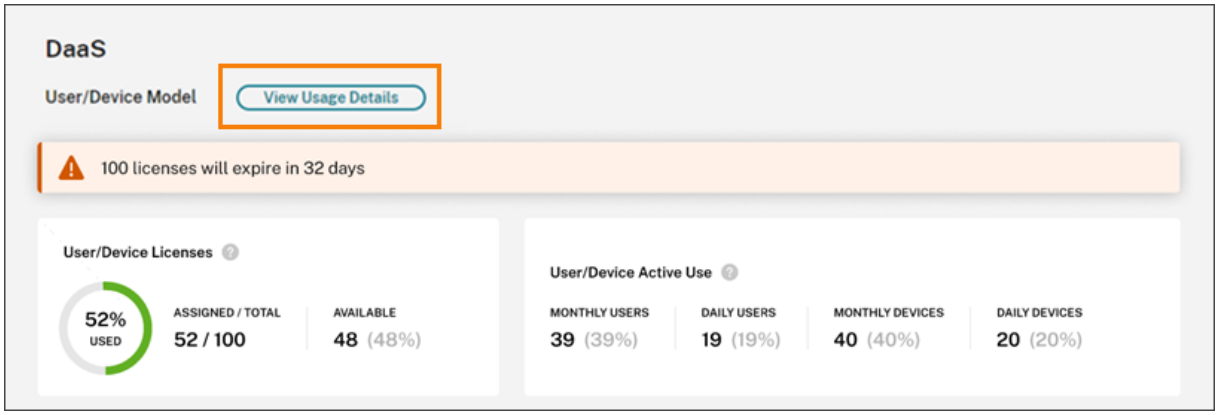
Wenn der Service von 100 eindeutigen Benutzern und 50 eindeutigen Geräten verwendet wurde, berechnet Citrix Cloud die Anzahl der zugewiesenen Lizenzen anhand des niedrigeren Werts (50). Der Prozentsatz der verwendeten Lizenzen und die Anzahl der verfügbaren Lizenzen basieren auf diesen 50 zugewiesenen Lizenzen.

Beispiel für die Berechnung der aktiven Nutzung

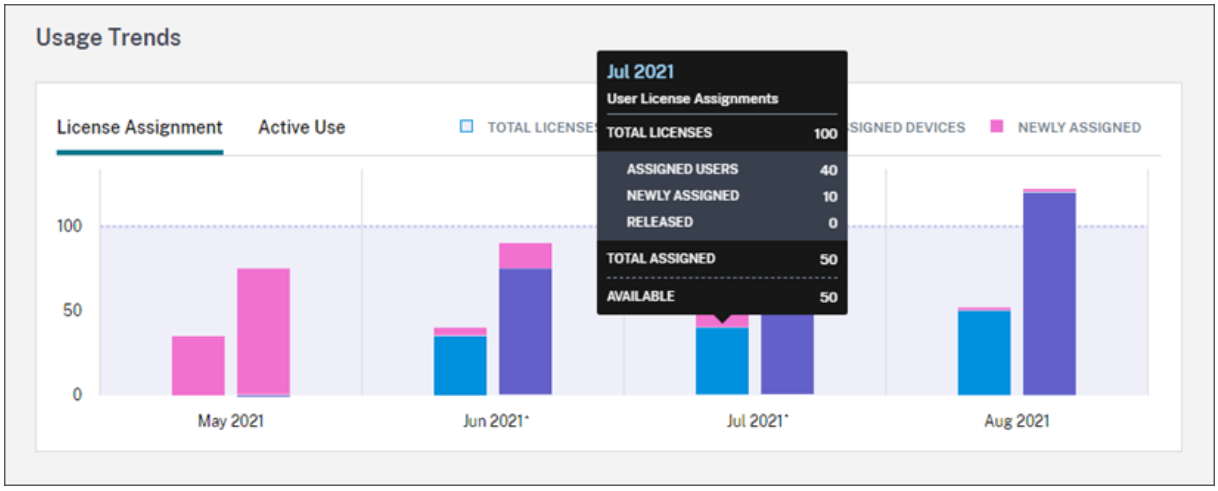
Wenn der Service in den letzten 30 Tagen von 10 eindeutigen Benutzern und 20 eindeutigen Geräten genutzt wurde, liegt die monatliche aktive Nutzung laut Citrix Cloud bei 10 aktiven Benutzern und 20 aktiven Geräten. Analog liegt die tägliche aktive Nutzung bei 30 aktiven Benutzern und 15 aktiven Geräten, wenn Citrix Cloud in den vergangenen 24 Stunden 30 eindeutige Benutzer und 15 eindeutige Geräte erfasst hat.

Nutzungstrends

Klicken Sie am rechten Rand der Zusammenfassung auf **Nutzungsdetails anzeigen**, um eine detaillierte Ansicht Ihrer Lizenzen zu erhalten. Sie sehen dann eine Aufschlüsselung der Nutzungstrends sowie einzelne Benutzer und Geräte, die Cloudservicelizenzen verwenden.



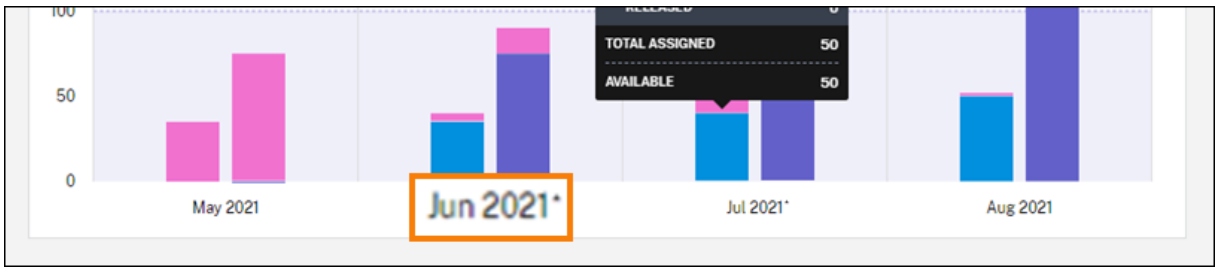
Im Abschnitt **Nutzungstrends** wird diese Aufschlüsselung als Diagramm angezeigt.



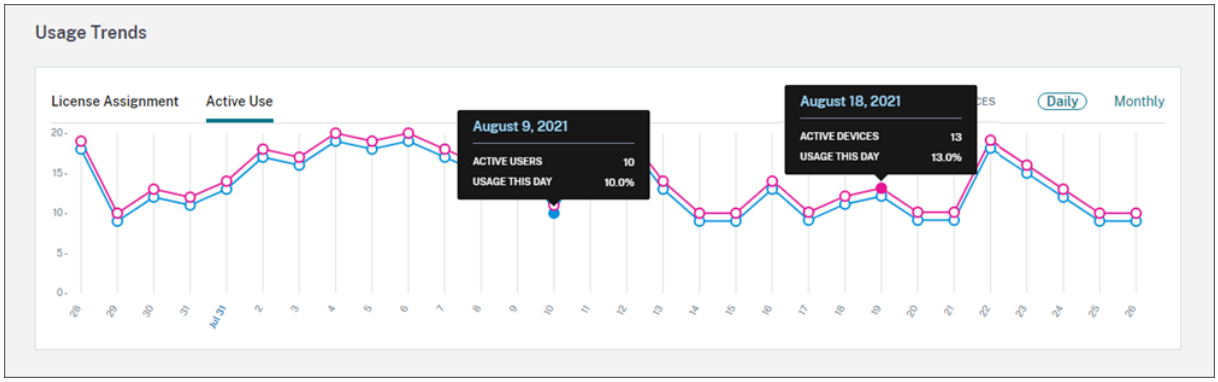
Im Diagramm **Lizenzzuweisung** werden folgende Informationen angezeigt, wenn Sie auf den Balken für einen bestimmten Monat oder Tag zeigen:

- **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.
- **Zugewiesene Benutzer:** Die kumulative Anzahl aller Lizenzen, die Benutzern bis zum aktuellen Monat zugewiesen wurden.
- **Zugewiesene Geräte:** Die kumulative Anzahl aller Lizenzen, die Geräten bis zum aktuellen Monat zugewiesen wurden. Wenn diese Zahl für einen bestimmten Monat besonders hoch erscheint, könnte dies an App- oder Desktopstarts über einen Webbrowser liegen. Um diese Zahl zu verringern, empfiehlt Citrix die Verwendung einer lokal installierten Workspace-App.
- **Neu zugewiesen:** Die Anzahl neuer Lizenzen, die pro Monat zugewiesen wurden. Beispielsweise greift ein Benutzer im Juli das erste Mal auf den Cloudservice zu und ihm wird eine Lizenz zugewiesen. Diese Lizenz gilt für den Monat Juli als "Neu zugewiesen".
- **Freigegeben:** Die Anzahl der Lizenzen, die pro Monat freigegeben wurden. Wenn beispielsweise die Freigabe von 20 Lizenzen möglich war und Sie 10 davon im Juli freigegeben haben, liegt die Anzahl der freigegebenen Lizenzen für den Juli bei 10.

Die Zeitintervalle mit aktivierter Domänennamenkürzung sind mit einem Sternchen gekennzeichnet.



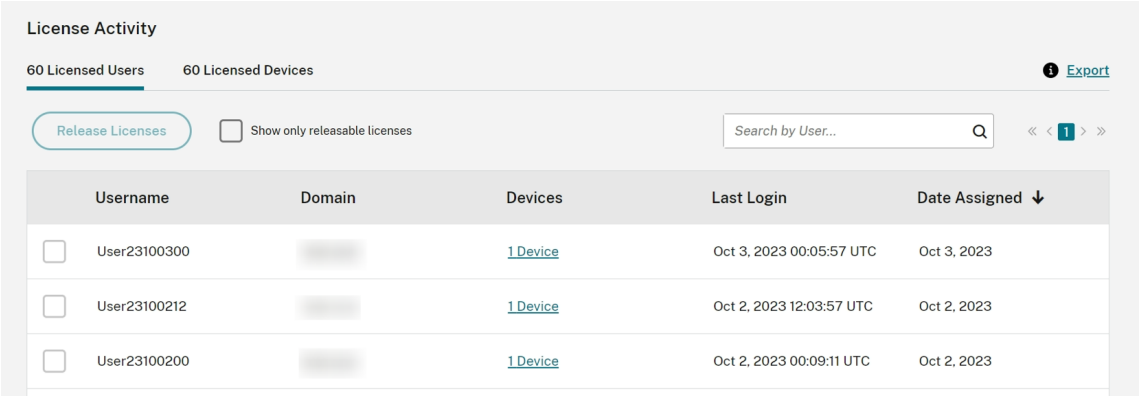
Das Diagramm **Aktive Nutzung** zeigt die aktiven Benutzer und Geräte für den vergangenen Kalendermonat bzw. das Kalenderjahr an. Wenn Sie auf ein Intervall im Diagramm zeigen, werden die Anzahl der aktiven Benutzer oder Geräte und die prozentuale Nutzung angezeigt.



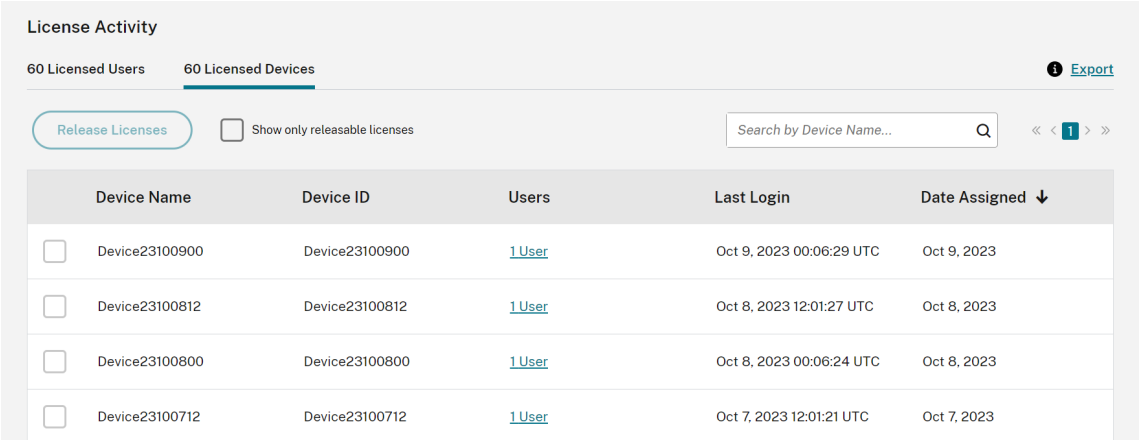
Lizenzaktivität

Im Abschnitt **Lizenzaktivität** werden folgende Informationen angezeigt:

- Liste der einzelnen Benutzer, denen Lizenzen zugewiesen sind, einschließlich der zugehörigen Geräte.



- Liste der Geräte, denen Lizenzen zugewiesen wurden, einschließlich der zugehörigen Benutzer.



- Das Datum, an dem Benutzern oder Geräten eine Lizenz zugewiesen wurde.

Sie können die Liste auch filtern, sodass nur freigebbare Lizenzen angezeigt werden. Siehe Freigeben zugewiesener Lizenzen in diesem Artikel.

Freigeben zugewiesener Lizenzen

Wird eine Lizenz zugewiesen, ist sie 90 Tage gültig und die Verbindung zum Service wird hergestellt. Wenn ein Benutzer oder Gerät 90 Tage lang keine App oder keinen Desktop startet, gilt die Lizenz als ungenutzt und wird nach 90 Tagen von Citrix Cloud freigegeben. Dies erfolgt automatisch, ohne dass der Administrator Maßnahmen ergreifen muss.

Nach Ablauf des Zuweisungszeitraums (90 Tage) darf der Administrator Lizenzen nur in den folgenden Szenarien manuell freigeben:

- Der Benutzer ist nicht mehr mit dem Unternehmen verbunden.
- Der Benutzer ist längere Zeit beurlaubt.

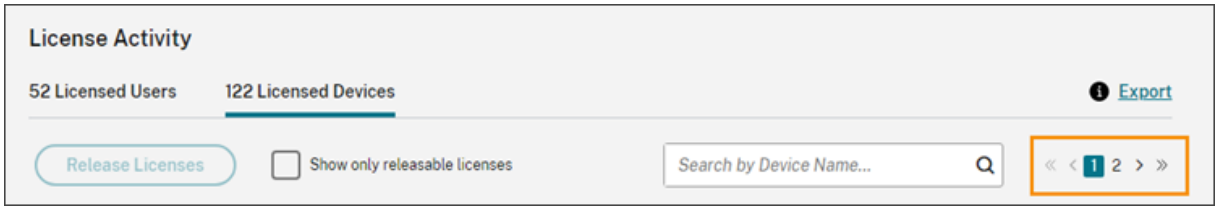
Die Administratoren können die Lizenzen für Geräte nur freigeben, wenn die Geräte ungenutzt sind.

> **Hinweis:**
>
> - Es wird empfohlen, die automatische Lizenzfreigabe zu nutzen. Eine Freigabe von Lizenzen vor Ablauf der 90-Tage-Frist aus einem anderen als den oben genannten Gründen kann gegen die Citrix EULA verstoßen. Bevor Sie diese Aktion ausführen, wenden Sie sich an Citrix.
> - Der Administrator kann eine einzelne Lizenz manuell über die Benutzeroberfläche freigeben. Alternativ kann er Lizenzen mithilfe der Cloud-Lizenzierungs-API freigeben. Weitere Informationen finden Sie unter APIs to manage Citrix cloud licensing.

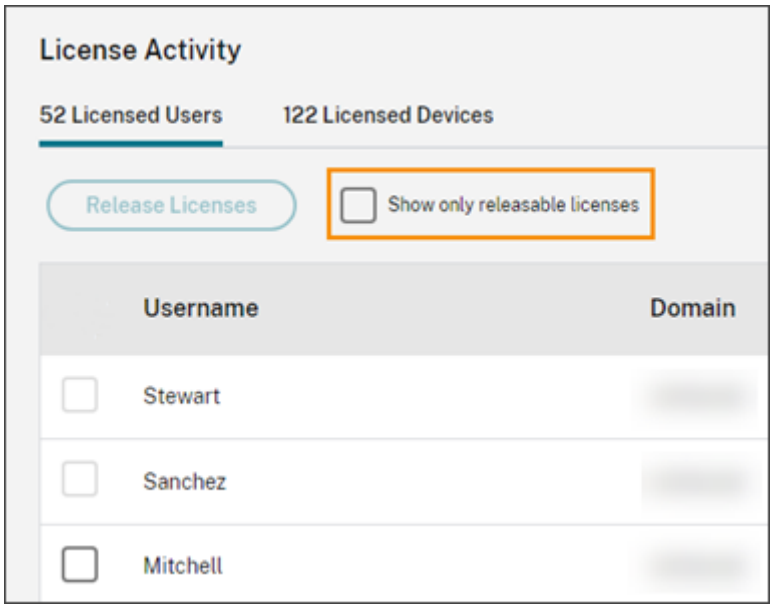
Freigebbare Lizenzen finden

Wenn der Benutzer oder das Gerät 30 Tage lang keine App bzw. keinen Desktop startet, versetzt Citrix Cloud die Lizenz in einen freigebbaren Zustand. Freigebbare Lizenzen werden in der Liste “Lizenzierte Benutzer”oder “Lizenzierte Geräte”mit einem dunkelgrauen Kontrollkästchen angezeigt, das Sie aktivieren können. Nicht freigabeberechtigte Lizenzen werden mit einem hellgrauen Kästchen angezeigt, das nicht ausgewählt werden kann.

Die Liste im Abschnitt **Lizenzaktivität** zeigt bis zu 100 zugewiesene Lizenzen gleichzeitig an. Wenn Sie mehr als 100 Lizenzen haben, verwenden Sie die Seitensteuerelemente, um die Liste durchzugehen.



Zur schnellen Anzeige freigebbarer Lizenzen klicken Sie auf **Nur freigebbare Lizenzen anzeigen** neben der Schaltfläche **Lizenzen freigeben**. Diese Aktion blendet zugewiesene Lizenzen aus, die noch nicht freigegeben werden können.



Freigebbare Lizenzen auswählen

Aktivieren Sie das dunkelgraue Kontrollkästchen neben jeder Lizenz, um diese für die Freigabe auszuwählen. Wenn Sie eine Lizenz aus der Liste auswählen, wird die Schaltfläche **Lizenzen freigeben** aktiv.

Sie können alle freigabeberechtigten Lizenzen nacheinander auswählen und auf **Lizenzen freigeben** klicken.

Freigeben zugewiesener Lizenzen

1. Klicken Sie unter **Lizenzaktivität** auf die Registerkarte **Lizenzierte Benutzer** oder **Lizenzierte Geräte**.
2. Klicken Sie bei Bedarf auf **Nur freigebbare Lizenzen anzeigen**, um nur die Benutzer mit Lizenzen anzuzeigen, die freigegeben werden können.
3. Wählen Sie die Benutzer oder Geräte aus, die Sie verwalten möchten, und klicken Sie dann auf **Lizenzen freigeben**.
4. Überprüfen Sie die ausgewählten Benutzer bzw. Geräte und klicken Sie auf **Lizenzen freigeben**.

Lizenzen und Verwendungsspitzen für Citrix DaaS überwachen (Gleichzeitig-Lizenzmodell)

September 28, 2023

In diesem Artikel wird die Verwaltung von Gleichzeitig-Lizenzen für **Citrix DaaS** beschrieben.

Informationen zur Benutzer-/Gerätelizenzierung für Citrix DaaS finden Sie unter Lizenzen und aktive Nutzung für Citrix DaaS (Benutzer/Gerät) überwachen.

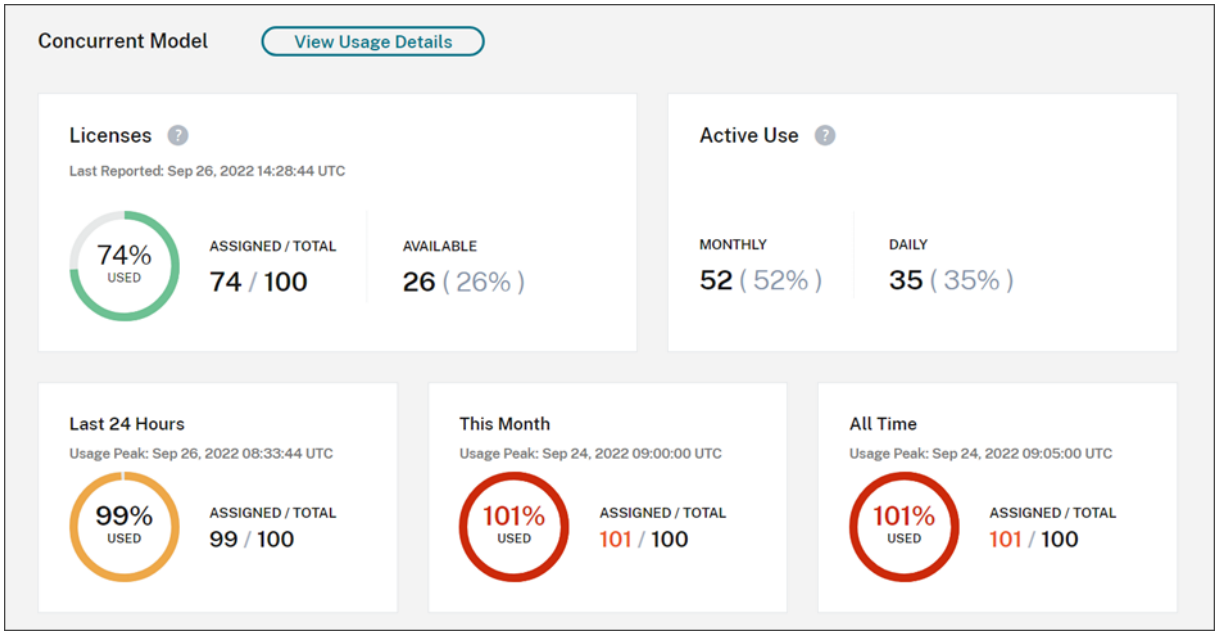
Informationen zur Benutzer-/Gerätelizenzierung und zur Gleichzeitig-Lizenzierung für Citrix DaaS Standard für Azure finden Sie unter Lizenzen und Nutzung für Citrix DaaS Standard für Azure überwachen.

Lizenzzuweisung

Citrix Cloud weist eine Lizenz zu, wenn ein Benutzer eine App oder einen Desktop auf dem Gerät startet. Wenn der Benutzer sich abmeldet oder die Verbindung zur Sitzung trennt, ist die Lizenz nicht länger zugewiesen. Da die Lizenzzuweisung davon abhängt, wie viele Geräte aktuell auf Apps oder Desktops zugreifen, erfasst Citrix Cloud alle fünf Minuten die Anzahl verwendeter Lizenzen.

Weitere Informationen zum Gleichzeitig-Lizenzmodell finden Sie unter Gleichzeitig-Lizenzmodell in der Produktdokumentation zur Lizenzierung.

Zusammenfassung zur Lizenzierung



Die Zusammenfassung der Lizenzierung bietet einen Überblick über die folgenden Informationen:

- Prozentsatz der erworbenen Lizenzen, die verwendet wurden, als die letzte Lizenzprüfung durch Citrix Cloud erfolgte. Citrix Cloud berechnet diesen Prozentsatz alle fünf Minuten basierend auf eindeutigen Geräten mit aktiven Verbindungen zum Dienst. Die Gesamtanzahl an erworbenen Lizenzen umfasst alle erworbenen Lizenzen für Citrix DaaS-Editionen, die das Gleichzeitig-Lizenzmodell verwenden.
- Das Verhältnis aktuell zugewiesener Lizenzen zur Gesamtanzahl erworbener Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen. Unter **Gesamt** sehen Sie die Gesamtanzahl aller erworbenen Lizenzen (gemäß Zeitpunkt unter "Letzter Bericht").
- Statistiken zu Verwendungsspitzen. Bei der Berechnung von Verwendungsspitzen für Lizenzen erfasst Citrix Cloud die maximale Anzahl verwendeter Lizenzen für folgende Zeiträume:

  - **Letzte 24 Stunden:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen in den letzten 24 Stunden.
  - **In diesem Monat:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen im aktuellen Monat.
  - **Gesamte Zeit:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen seit Beginn des Abonnements.

  Unter **Gesamt** sehen Sie für den jeweiligen Zeitraum, wie viele Lizenzen während der Verwendungsspitze insgesamt im Besitz waren. Wenn die Gesamtzahl der erworbenen Lizenzen ansteigt oder sinkt und sich die Anzahl zugewiesener Lizenzen entsprechend erhöht, ändert sich auch der Wert unter **Gesamt**. Wenn keine entsprechende Verwendungsspitze auftritt, ändert sich der Wert unter **Gesamt** nicht.
- Statistiken zur aktiven Nutzung. Citrix Cloud zeigt die Gesamtzahl der eindeutigen Verbindungen für die folgenden Zeiträume an:

  - **Monatlich:** Gesamtzahl der Verbindungen im vorherigen Kalendermonat.
  - **Täglich:** Gesamtzahl der Verbindungen der letzten 24 Stunden.
    Diese Zahlen werden auch als Prozentsätze der Gesamtzahl der Lizenzen im Besitz während dieser Zeiträume dargestellt.

Berechnung von Verwendungsspitzen für Lizenzen

Um das Gleichzeitig-Modell (CCU-Lizenzen) akkurat wiederzugeben, erfasst Citrix Cloud alle fünf Minuten, wie viele eindeutige Geräte gleichzeitig auf den Dienst zugreifen. Liegt die Zahl über der aktuellen Verwendungsspitze, zeigt Citrix Cloud die neue Verwendungsspitze mit Datum und Uhrzeit an. Wenn die Anzahl unter der aktuellen Verwendungsspitze liegt, ändert sich der aktuelle Spitzenwert nicht.

> **Wichtig:**
>
> Wenn Sie die Überwachungsfunktion in Director nutzen, um Informationen zu gleichzeitigen Sitzungen anzuzeigen, müssen Sie beachten, dass gleichzeitige Sitzungen im Überwachungsbericht anders interpretiert werden und verwendete CCU-Lizenzen hier nicht akkurat angegeben sind. Weitere Informationen zu den Unterschieden zwischen Überwachungs- und Lizenzierungsberichten finden Sie unter Häufig gestellte Fragen.

Berechnung der monatlichen aktiven Nutzung

Zu Beginn jedes Monats erstellt Citrix Cloud einen Snapshot des vorherigen Kalendermonats. Citrix Cloud zeigt die Gesamtzahl der eindeutigen Verbindungen an, die in diesem Kalendermonat hergestellt wurden.

Berechnung der täglichen aktiven Nutzung

Jeden Tag zur gleichen Zeit erstellt Citrix Cloud einen Snapshot der letzten 24 Stunden. Citrix Cloud zeigt die Gesamtzahl der eindeutigen Verbindungen an, die in diesem diesem Zeitraum von 24 Stunden hergestellt wurden.

Nutzungstrends und Lizenzaktivität

Klicken Sie für auf **Nutzungsdetails anzeigen**, um historische Nutzungsdaten Ihrer Lizenzen anzuzeigen.

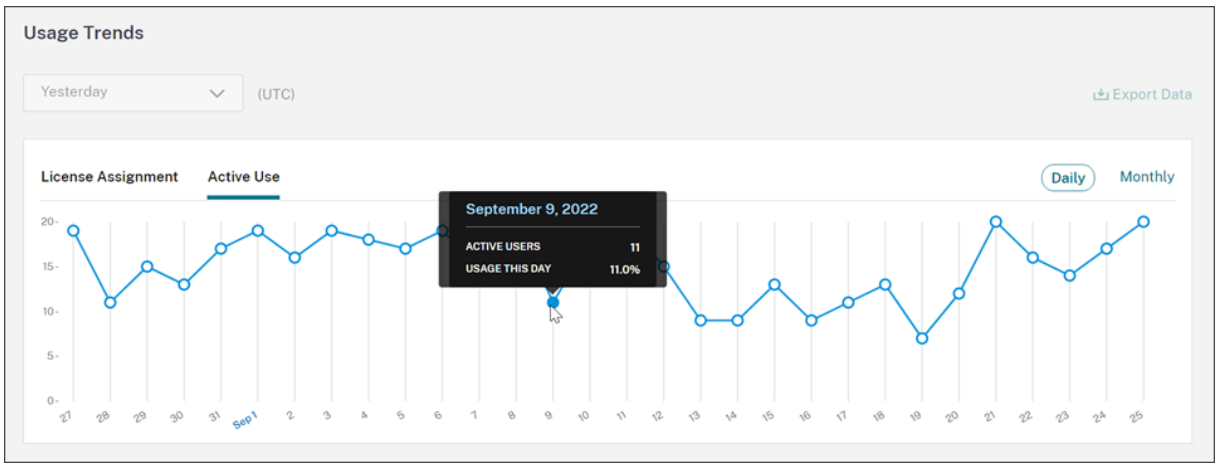
Der Bereich **Nutzungstrends** stellt folgende Informationen bereit:

- **Lizenzzuweisung** zeigt ein Diagramm mit den folgenden Informationen an:
  - **Lizenzen insgesamt:** Gesamtanzahl Ihrer erworbenen CCU-Lizenzen.
  - **Spitzennutzung Lizenzen:** Die maximale Anzahl zugewiesener Lizenzen im ausgewählten Zeitraum. Standardmäßig zeigt Citrix Cloud Verwendungsspitzen für jeden Monat im aktuellen Kalenderjahr an. Um monatliche oder stündliche Verwendungsspitzen anzuzeigen, wählen Sie im Dropdownmenü den Kalendermonat oder Kalendertag aus, den Sie untersuchen möchten.

  Wenn der ausgewählte Datumsbereich noch nicht abgeschlossen ist, zeigt Citrix Cloud die aktuelle Verwendungsspitze für das derzeitige Zeitintervall an. Wenn Sie beispielsweise die Details für den aktuellen Kalendertag anzeigen, ist die maximale Anzahl verwendeter Lizenzen für jede Stunde bis zum aktuellen Zeitpunkt zu sehen. Wenn die maximale Anzahl verwendeter Lizenzen im nächsten Fünf-Minuten-Zählintervall ansteigt, aktualisiert Citrix Cloud die Verwendungsspitze für die aktuelle Stunde.

- **Aktive Nutzung** zeigt ein Diagramm mit den folgenden Informationen an:
  - **Täglich:** Die Gesamtzahl der Verbindungen für jeden Tag während der letzten 30 Tage.
  - **Monatlich:** Die Gesamtzahl der Verbindungen für jeden Monat des vorangegangenen Kalenderjahres.

Wenn Sie in den Diagrammen **Lizenzzuweisung** oder **Aktive Nutzung** auf ein Intervall zeigen, werden die Details für dieses Intervall angezeigt.



Lizenzen freigeben

Gleichzeitig-Lizenzen werden automatisch freigegeben, wenn Benutzer sich abmelden oder die Sitzung trennen. Sie müssen diese Lizenzen nicht manuell freigeben.

Überwachen von Lizenzen und Nutzung für Citrix DaaS Standard für Azure

November 2, 2023

In diesem Artikel wird die Verwaltung von Lizenzzuweisungen per Benutzer-/Gerätelizenzmodell sowie per Gleichzeitig-Lizenzmodell erläutert.

Citrix Azure Consumption Fund (nur Benutzer/Gerät)

Wenn Sie Citrix Azure Consumption Fund für Ihre Service-Bereitstellung erworben haben, finden Sie Informationen zur Nutzungsberichterstattung für von Citrix verwaltete Ressourcen unter Monitor Citrix Managed Azure resource consumption for Citrix DaaS.

Lizenzzuweisung

Benutzer-/Gerätelizenzmodell: Citrix Cloud weist eine Lizenz zu, wenn ein eindeutiger Benutzer oder ein eindeutiges Gerät zum ersten Mal einen Desktop startet.

Gleichzeitig-Lizenzmodell: Citrix Cloud weist eine Lizenz zu, wenn ein Benutzer eine App oder einen Desktop auf dem Gerät startet. Wenn der Benutzer sich abmeldet oder die Verbindung zur Sitzung trennt, ist die Lizenz nicht länger zugewiesen. Da die Lizenzzuweisung davon abhängt, wie viele Geräte aktuell auf Desktops zugreifen, erfasst Citrix Cloud alle fünf Minuten die Anzahl verwendeter Lizenzen.

Weitere Informationen zum Gleichzeitig-Lizenzmodell (CCU-Lizenzen) finden Sie unter CCU-Lizenzen in der Produktdokumentation zur Lizenzierung.

Berechnung von Verwendungsspitzen für Lizenzen

Um das Gleichzeitig-Modell (CCU-Lizenzen) akkurat wiederzugeben, erfasst Citrix Cloud alle fünf Minuten, wie viele eindeutige Geräte gleichzeitig auf den Dienst zugreifen. Liegt die Zahl über der aktuellen Verwendungsspitze, zeigt Citrix Cloud die neue Verwendungsspitze mit Datum und Uhrzeit an. Wenn die Anzahl unter der aktuellen Verwendungsspitze liegt, ändert sich der aktuelle Spitzenwert nicht.

Kürzung von Domänennamen

Dieses Feature wird nur für das **Benutzer-/Gerät**-Lizenzmodell unterstützt.

Wenn Sie mehrere Domänen hosten und Benutzer mit ähnlichen Konten in diesen Domänen haben (z. B. `johnsmith@company.com` und `johnsmith@mycompany.com`), können Sie zulassen, dass Citrix Cloud die Kontodomäne ignoriert und nur den Benutzernamen des Kontos berücksichtigt (z. B. johnsmith). Dies wird als *Kürzung von Domänennamen* bezeichnet. Standardmäßig ist die Kürzung von Domänennamen deaktiviert.

Wenn die Kürzung von Domänenamen aktiviert ist, ändert sich die Berechnung eindeutiger Benutzer in Citrix Cloud. `johnsmith@company.com` und `johnsmith@mycompany.com` werden in Citrix Cloud nicht mehr als zwei eindeutige Benutzer gezählt, sondern als eindeutiger Benutzer “johnsmith” . Diese Berechnungsänderung wirkt sich auf die folgenden Lizenzdaten aus:

- Lizenzzuweisung
- Aktive Nutzung
- Lizenznutzungstrends im Zeitverlauf
- Lizenzen, die zur Freigabe in Frage kommen

Die Änderungen der Lizenzdaten werden auch beim Exportieren von Daten aus der Lizenzierungskonsole in eine CSV-Datei angewendet.

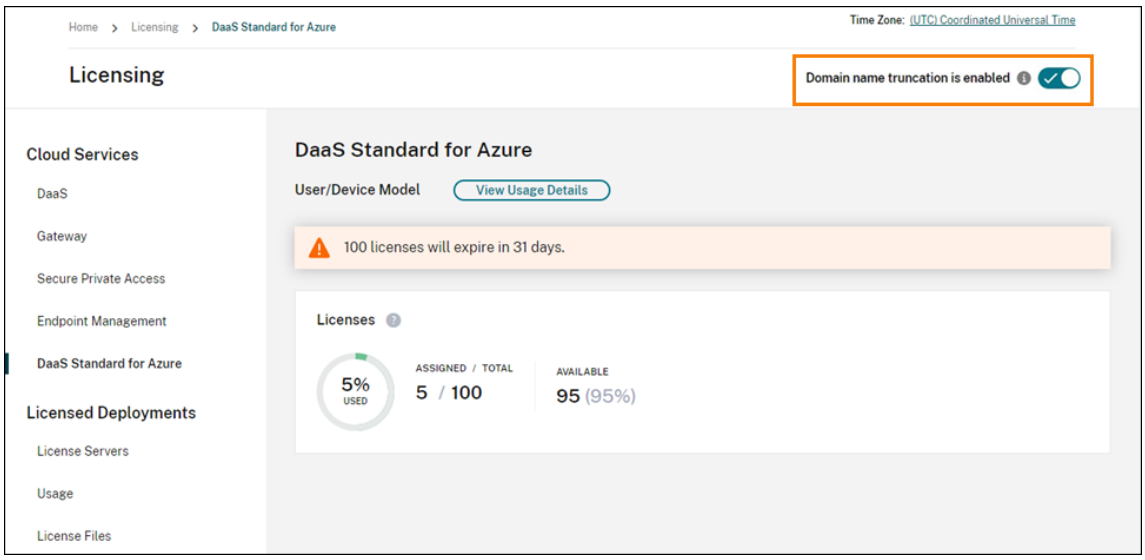
> **Hinweis:**
>
> Wenn Sie mehrere Domänen mit ähnlichen Konten hosten, bei denen der Benutzername geringfügige Unterschiede aufweist (z. B. wenn ein Benutzer die Konten `johnsmith@company.com` und `jsmith@newcompany.com`) hat, hat die Kürzung des Domänennamens keine Auswirkung auf die Berechnungen in Citrix Cloud. Citrix Cloud zählt johnsmith und jsmith weiterhin als Einzelbenutzer, selbst wenn die Konten derselben Person gehören.

Kürzung von Domänenamen aktivieren oder deaktivieren

Standardmäßig ist die Kürzung von Domänennamen deaktiviert. Die Kürzung von Domänennamen wirkt sich auf die Benutzer-/Gerätenutzungsdaten aus, sobald Sie das Feature aktivieren oder deaktivieren. Wenn Sie die Kürzung von Domänennamen beispielsweise in einem bestimmten Monat deaktivieren, sind die Daten betroffen, die Citrix Cloud in diesem Monat aufzeichnet. Historische Daten der vergangenen Monate, in denen das Feature deaktiviert war, bleiben unberührt. Wenn Sie die Kürzung von Domänennamen hingegen in einem bestimmten Monat deaktivieren, sind die Daten betroffen, die Citrix Cloud in diesem Monat aufzeichnet. Historische Daten der vergangenen Monate, in denen das Feature aktiviert war, bleiben unberührt.

Gehen Sie zum Aktivieren oder Deaktivieren der Kürzung von Domänennamen folgendermaßen vor:

1. Klicken Sie in der Lizenzierungskonsole oben rechts auf den Schalter.



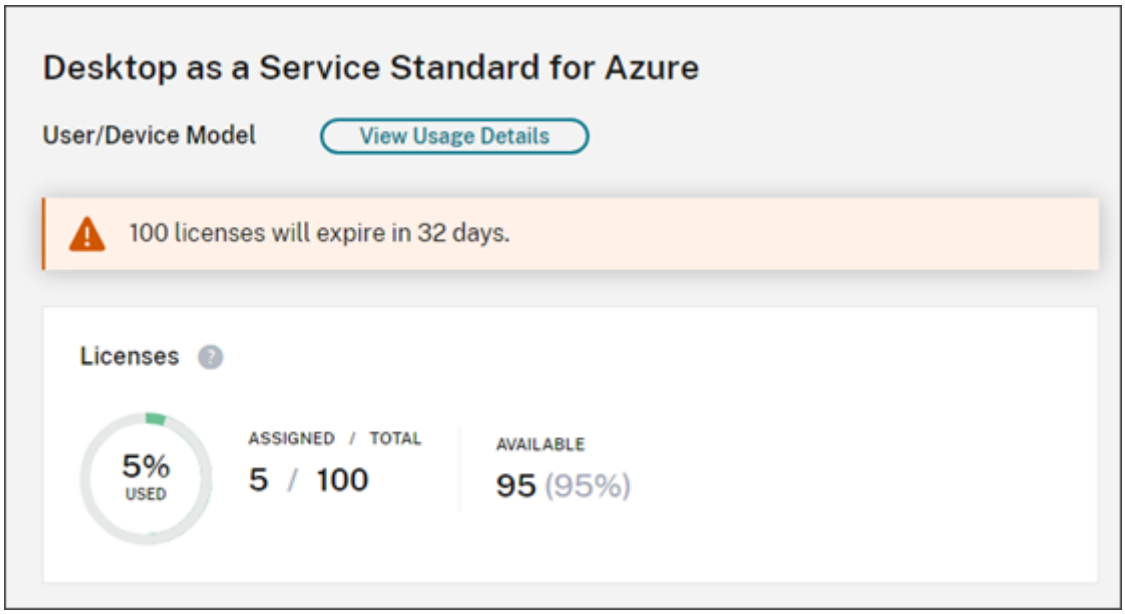
2. Wenn Sie aufgefordert werden, Ihre Aktion zu bestätigen, wählen Sie **Ja, ich verstehe**.

Zusammenfassung zur Lizenzierung

Citrix Cloud zeigt Zusammenfassungen der im Rahmen des Benutzer-/Gerätelizenzmodells und Gleichzeitig-Lizenzmodells verwendeten Lizenzen an.

Zusammenfassung für Benutzer und Geräte

Die Benutzer/Gerät-Lizenzübersicht zeigt die verwendeten Lizenzen im Verhältnis zur Gesamtzahl der Lizenzen, die Sie besitzen.

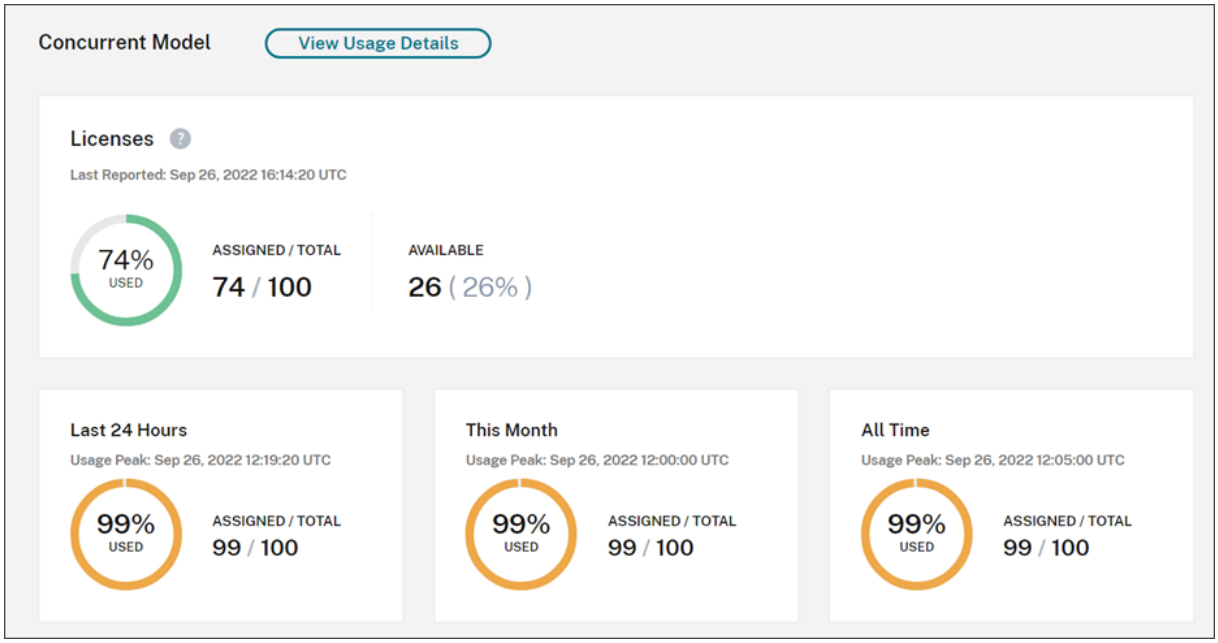


Wenn sich der Prozentsatz 100 % nähert, wechselt der Prozentsatz von grün zu gelb. Wenn der Prozentsatz 100 % überschreitet, wird der Prozentsatz rot angezeigt.

Citrix Cloud zeigt auch das Verhältnis zugewiesener zu erworbenen Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen.

Zusammenfassung für gleichzeitige Benutzer

Die Gleichzeitig-Lizenzübersicht bietet einen Überblick über die folgenden Informationen:

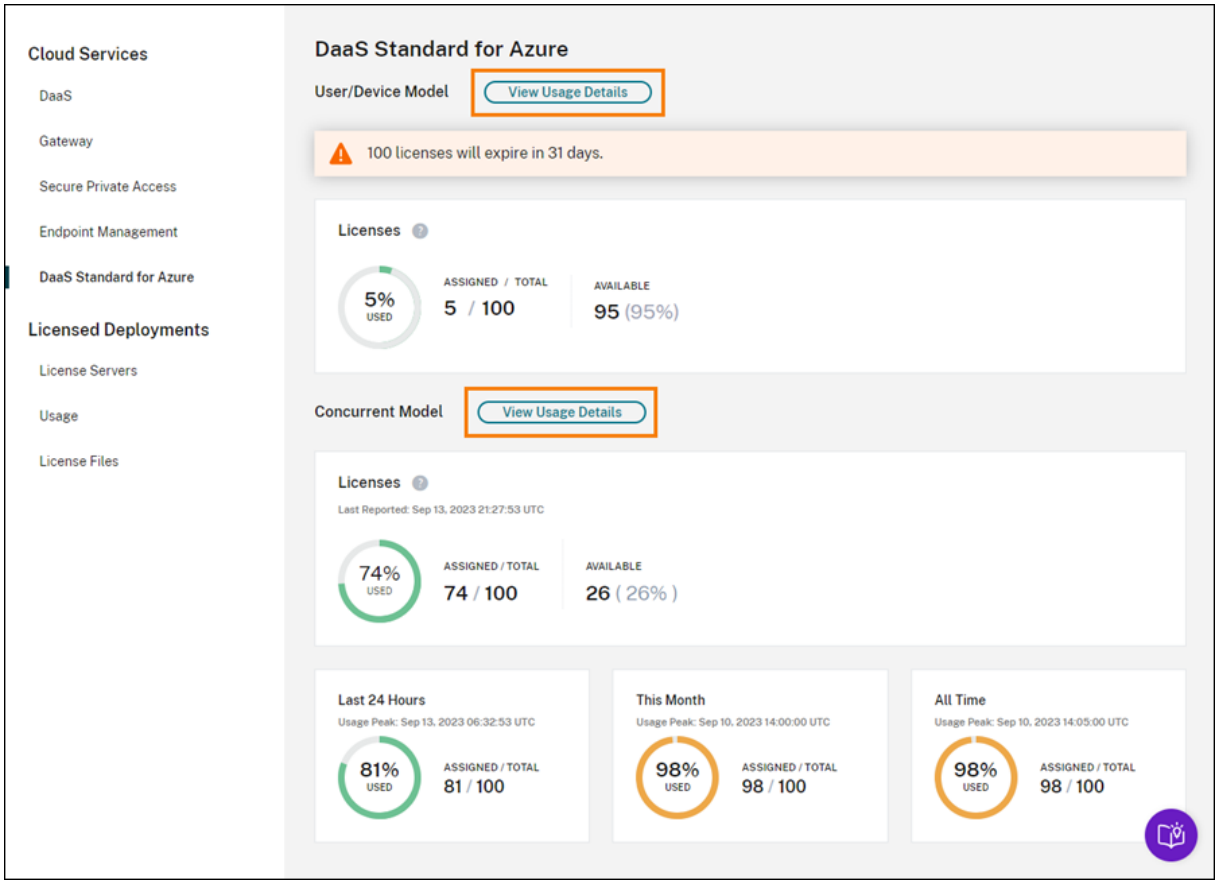


- Prozentsatz der erworbenen Lizenzen, die verwendet wurden, als die letzte Lizenzprüfung durch Citrix Cloud erfolgte. Citrix Cloud berechnet diesen Prozentsatz alle fünf Minuten basierend auf eindeutigen Geräten mit aktiven Verbindungen zum Dienst. Die Gesamtanzahl an erworbenen Lizenzen umfasst alle erworbenen Lizenzen für Citrix DaaS Standard für Azure, die das Gleichzeitig-Lizenzmodell verwenden.
- Das Verhältnis aktuell zugewiesener Lizenzen zur Gesamtanzahl erworbener Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen. Unter **Gesamt** sehen Sie die Gesamtanzahl aller erworbenen Lizenzen (gemäß Zeitpunkt unter "Letzter Bericht").
- Statistiken zu Verwendungsspitzen. Bei der Berechnung von Verwendungsspitzen für Lizenzen erfasst Citrix Cloud die maximale Anzahl verwendeter Lizenzen für folgende Zeiträume:
  - **Letzte 24 Stunden:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen in den letzten 24 Stunden.
  - **In diesem Monat:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen im aktuellen Monat.
  - **Gesamte Zeit:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen seit Beginn des Abonnements.

  Unter **Gesamt** sehen Sie für den jeweiligen Zeitraum, wie viele Lizenzen während der Verwendungsspitze insgesamt im Besitz waren. Wenn die Gesamtzahl der erworbenen Lizenzen ansteigt oder sinkt und sich die Anzahl zugewiesener Lizenzen entsprechend erhöht, ändert sich auch der Wert unter **Gesamt**. Wenn keine entsprechende Verwendungsspitze auftritt, ändert sich der Wert unter **Gesamt** nicht.

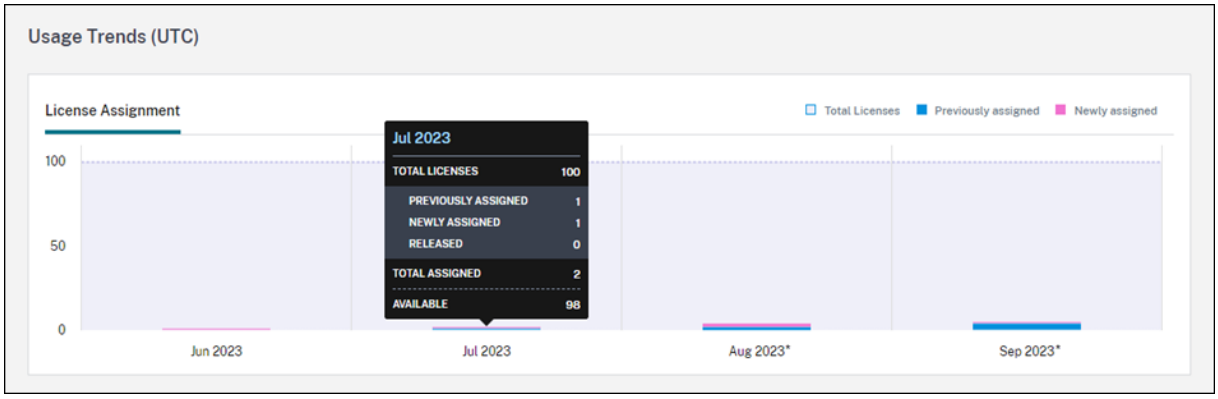
Nutzungstrends

Citrix Cloud zeigt eine Aufschlüsselung der Nutzungstrends für Benutzer/Gerät- oder Gleichzeitig-Lizenzen an. Um diese Aufschlüsselung anzuzeigen, wählen Sie auf der Seite mit der Lizenzübersicht die Option **Nutzungsdetails anzeigen**.



Trends für Benutzer und Geräte

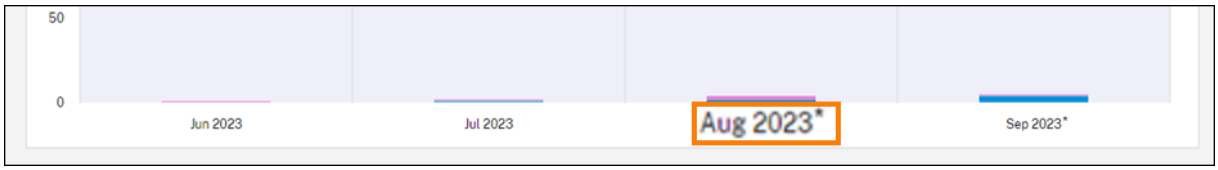
Für Benutzer/Gerät-Lizenzen zeigt der Abschnitt **Nutzungstrends** eine Aufschlüsselung der zugewiesenen Lizenzen als Diagramm.



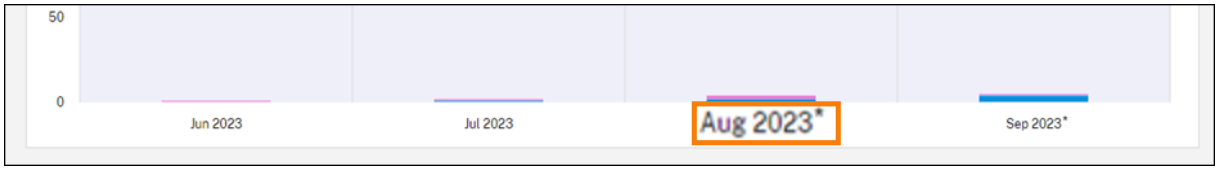
Wenn Sie auf ein Intervall im Diagramm zeigen, werden die folgenden Informationen angezeigt:

- **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.
- **Zuvor zugewiesen:** die Anzahl der Lizenzen, die im Vormonat zugewiesen wurden. Beispielsweise greift ein Benutzer im Juli das erste Mal auf den Cloudservice zu und ihm wird eine Lizenz zugewiesen. Diese Lizenz gilt für den Monat Juli als "Neu zugewiesen". Für den Monat August wird diese Lizenz als "Zuvor zugewiesen"gezählt.
- **Neu zugewiesen:** Die Anzahl neuer Lizenzen, die pro Monat zugewiesen wurden. Beispielsweise greift ein Benutzer im Juli das erste Mal auf den Cloudservice zu und ihm wird eine Lizenz zugewiesen. Diese Lizenz gilt für den Monat Juli als "Neu zugewiesen".

Die Zeitintervalle mit aktivierter Domänennamenkürzung sind mit einem Sternchen gekennzeichnet.



Die Zeitintervalle mit aktivierter Domänennamenkürzung sind mit einem Sternchen gekennzeichnet.



Trends für Gleichzeitig-Modell

Für das Gleichzeitig-Modell werden im Bereich **Nutzungstrends** folgende Informationen angezeigt:

- **Lizenzen insgesamt:** Gesamtanzahl Ihrer erworbenen CCU-Lizenzen.

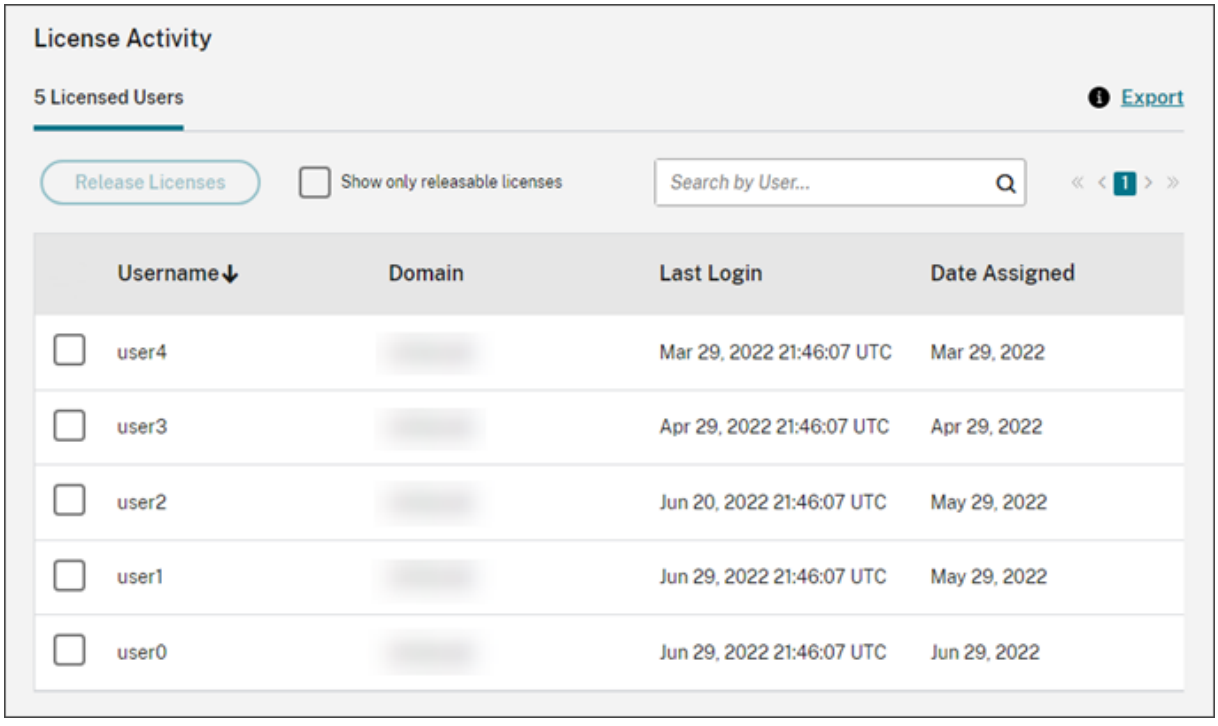
- **Spitzennutzung Lizenzen:** Die maximale Anzahl zugewiesener Lizenzen im ausgewählten Zeitraum. Standardmäßig zeigt Citrix Cloud Verwendungsspitzen für jeden Monat im aktuellen Kalenderjahr an. Um monatliche oder stündliche Verwendungsspitzen anzuzeigen, wählen Sie im Dropdownmenü den Kalendermonat oder Kalendertag aus, den Sie untersuchen möchten.

  Wenn der ausgewählte Datumsbereich noch nicht abgeschlossen ist, zeigt Citrix Cloud die aktuelle Verwendungsspitze für das derzeitige Zeitintervall an. Wenn Sie beispielsweise die Details für den aktuellen Kalendertag anzeigen, ist die maximale Anzahl verwendeter Lizenzen für jede Stunde bis zum aktuellen Zeitpunkt zu sehen. Wenn die maximale Anzahl verwendeter Lizenzen im nächsten Fünf-Minuten-Zählintervall ansteigt, aktualisiert Citrix Cloud die Verwendungsspitze für die aktuelle Stunde.

Wenn Sie auf ein Intervall zeigen, werden die Gesamtzahl der Lizenzen und die Höchstzahl der im Intervall verwendeten Lizenzen angezeigt.

Lizenzaktivität für Benutzer und Geräte

Für Benutzer-/Gerätelizenzen wird im Abschnitt **Lizenzaktivität** eine Liste der Benutzer angezeigt, denen Lizenzen zugewiesen wurden. Außerdem wird das Datum angezeigt, an dem eine Lizenz zugewiesen wurde. Dieser Abschnitt ist für Gleichzeitig-Lizenzen nicht verfügbar.



Sie können die Liste auch filtern, sodass nur freigebbare Lizenzen angezeigt werden. Siehe Zugewiesene Lizenzen freigeben in diesem Artikel.

Benutzer-/Gerätelizenzen freigeben

Die Freigabe berechtigter Benutzer-/Gerätelizenzen variiert je nach Art des Serviceabonnements.

- **Jahresabonnements:** Wenn Sie ein Jahresabonnement haben, können Sie die Lizenzen von Benutzern freigeben, die in den vergangenen 30 Tagen keine App und keinen Desktop gestartet haben. Mehrere Lizenzen können Sie einzeln oder per Massenaktion freigeben.
- **Monatsabonnements:** Wenn Sie ein Monatsabonnement haben, können Sie Lizenzen am ersten Tag eines jeden Monats freigeben, unabhängig vom Inaktivitätszeitraum.

Wird eine Lizenz zugewiesen, ist sie 90 Tage gültig und die Verbindung zum Service wird hergestellt. Wenn ein Benutzer oder Gerät 90 Tage lang keine App oder keinen Desktop startet, gilt die Lizenz als ungenutzt und wird nach 90 Tagen von Citrix Cloud freigegeben. Dies erfolgt automatisch, ohne dass der Administrator Maßnahmen ergreifen muss.

Nach Ablauf des Zuweisungszeitraums (90 Tage) darf der Administrator Lizenzen nur in den folgenden Szenarien manuell freigeben:

- Der Benutzer ist nicht mehr mit dem Unternehmen verbunden.
- Der Benutzer ist längere Zeit beurlaubt.

Die Administratoren können die Lizenzen für Geräte nur freigeben, wenn die Geräte ungenutzt sind.

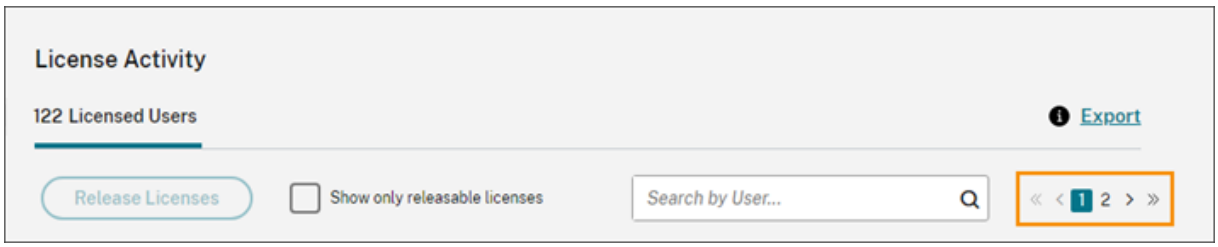
> **Hinweis:**
>
> - Es wird empfohlen, die automatische Lizenzfreigabe zu nutzen. Eine Freigabe von Lizenzen vor Ablauf der 90-Tage-Frist aus einem anderen als den oben genannten Gründen kann gegen die Citrix EULA verstoßen. Bevor Sie diese Aktion ausführen, wenden Sie sich an Citrix.
> - Der Administrator kann eine einzelne Lizenz manuell über die Benutzeroberfläche freigeben. Alternativ kann er Lizenzen mithilfe der Cloud-Lizenzierungs-API freigeben. Weitere Informationen finden Sie unter APIs to manage Citrix cloud licensing.

Finden geeigneter Lizenzen

Wenn der Benutzer oder das Gerät 30 Tage lang keine App bzw. keinen Desktop startet, versetzt Citrix Cloud die Lizenz in einen freigebbaren Zustand. Freigebbare Lizenzen werden in der Liste “Lizenzierte Benutzer”oder “Lizenzierte Geräte”mit einem dunkelgrauen Kontrollkästchen angezeigt, das Sie aktivieren können. Nicht freigabeberechtigte Lizenzen werden mit einem hellgrauen Kästchen angezeigt, das nicht ausgewählt werden kann.

Die Liste im Abschnitt **Lizenzaktivität** zeigt bis zu 100 zugewiesene Lizenzen gleichzeitig an. Wenn

Sie mehr als 100 Lizenzen haben, verwenden Sie die Seitensteuerelemente, um die Liste durchzugehen.



Um schnell nach geeigneten Lizenzen zu suchen, wählen Sie **Nur freigebbare Lizenzen anzeigen** neben der Schaltfläche **Lizenzen freigeben**. Diese Aktion blendet zugewiesene Lizenzen aus, die noch nicht freigegeben werden können.

Auswählen geeigneter Lizenzen

Aktivieren Sie das dunkelgraue Kontrollkästchen neben jeder Lizenz, um diese für die Freigabe auszuwählen. Wenn Sie eine Lizenz auswählen, wird die Schaltfläche **Lizenzen freigeben** aktiv.

Sie können alle freigabeberechtigten Lizenzen nacheinander auswählen und auf **Lizenzen freigeben** klicken.

Freigeben zugewiesener Lizenzen

1. Klicken Sie bei Bedarf auf **Nur freigebbare Lizenzen anzeigen**, um nur die Benutzer mit Lizenzen anzuzeigen, die freigegeben werden können.
2. Wählen Sie die Benutzer aus, die Sie verwalten möchten, und klicken Sie dann auf **Lizenzen freigeben**.
3. Überprüfen Sie die ausgewählten Benutzer und klicken Sie auf **Lizenzen freigeben**.

Gleichzeitig-Lizenzen freigeben

Gleichzeitig-Lizenzen werden automatisch freigegeben, wenn Benutzer sich abmelden oder die Sitzung trennen. Sie müssen diese Lizenzen nicht manuell freigeben.

Überwachen von Lizenzen und aktiver Nutzung für Endpoint Management

November 24, 2023

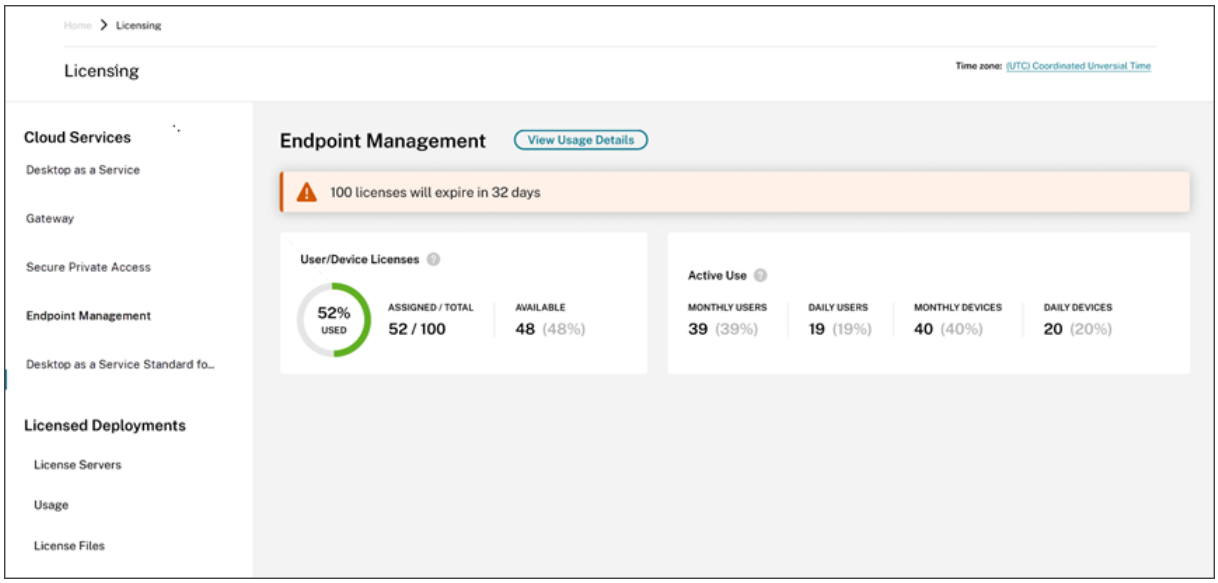
Lizenzzuweisung

Benutzern wird generell bei der ersten Verwendung des Cloudservices eine Lizenz zugewiesen. Für Endpoint Management wird eine Lizenz zugewiesen, wenn ein Benutzer ein Gerät anmeldet. Nach der Registrierung checkt das regelmäßig bei Citrix Cloud ein. Anhand des Eincheckimpulses berechnet Citrix Cloud die monatliche Nutzung, sodass Administratoren über die aktuelle Servicenutzung durch die Benutzer informiert sind.

Als erstmalige Nutzung gilt die erste Registrierung eines Geräts oder das Auftreten eines Eincheckimpulses für das Gerät.

Lizenzen werden auf Benutzerbasis zugewiesen. Wenn sich also zwei Benutzer anmelden und dasselbe Gerät verwenden, werden zwei Lizenzen zugewiesen.

Zusammenfassung und Details zur Lizenzierung

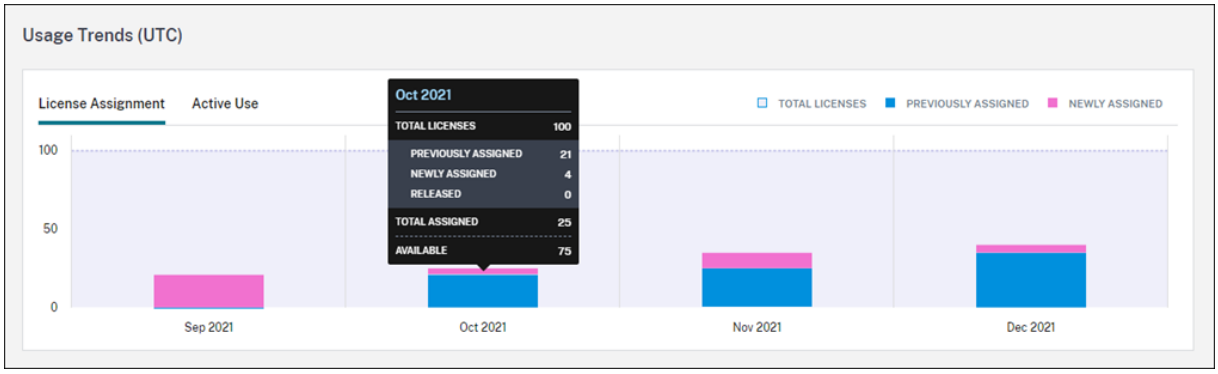


Die Zusammenfassung unter “Lizenzierung”bietet für jeden unterstützten Service einen Überblick über Folgendes:

- Prozentsatz der insgesamt erworbenen Lizenzen, die zugewiesen sind Wenn sich der Prozentsatz 100 % nähert, wechselt der Prozentsatz von grün zu gelb. Wenn der Prozentsatz 100 % überschreitet, wird der Prozentsatz rot angezeigt.
- Das Verhältnis zugewiesener zu erworbenen Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen.
- Statistik der aktiven Nutzung pro Monat und Tag:
  - “Monatliche aktive Nutzung”bezieht sich auf die Anzahl einzelner Benutzer, die den Service in den letzten 30 Tagen genutzt haben.
  - “Tägliche aktive Nutzung”bezieht sich auf die Anzahl einzelner Benutzer, die den Service in den letzten 24 Stunden genutzt haben.
- Die verbleibende Zeit bis zum Ablauf des Cloudserviceabonnements. Wenn das Abonnement innerhalb der nächsten 90 Tage abläuft, wird eine Warnmeldung angezeigt.

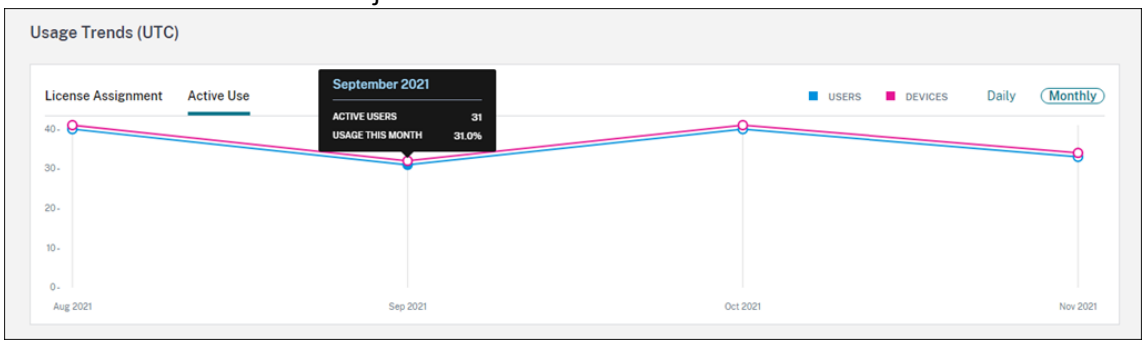
Nutzungstrends

Klicken Sie für eine detaillierte Ansicht Ihrer Lizenzen auf **Nutzungsdetails anzeigen**. Sie sehen dann eine Aufschlüsselung der Nutzungstrends sowie einzelne Benutzer und Geräte, die Cloudservicelizenzen verwenden.



Diese Aufschlüsselung zeigt Ihnen die folgenden Informationen:

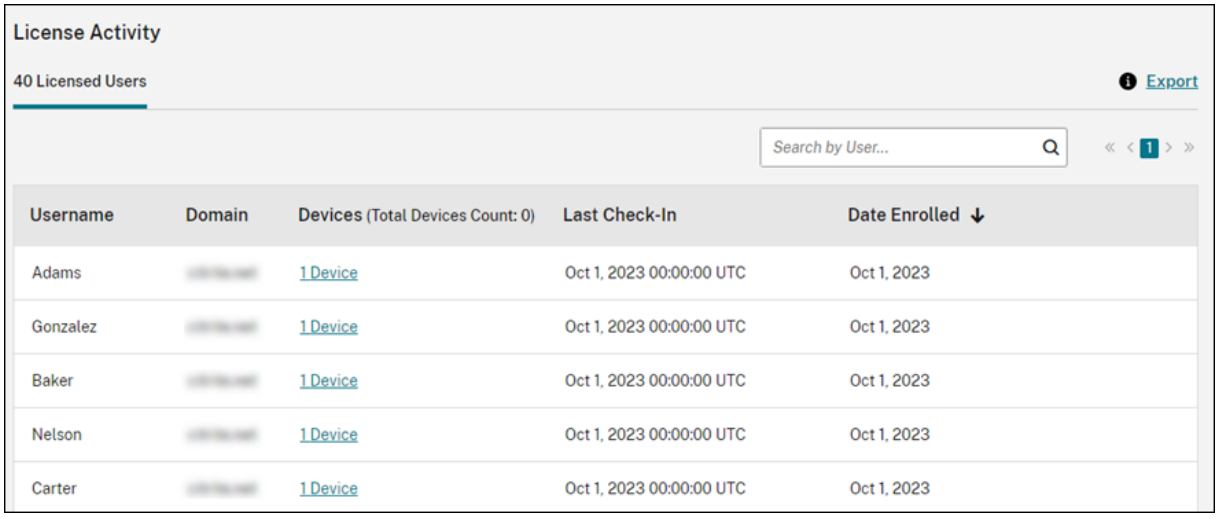
- **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.
- **Zuvor zugewiesen:** Die Cloudservicelizenzen, die bereits zu Beginn eines jeden Monats zugewiesen waren. Wenn einem Benutzer beispielsweise im Juli eine Lizenz zugewiesen wird, wird diese Zuweisung unter "Zuvor zugewiesen"für August mitgezählt.
- **Neu zugewiesen:** Die Cloudservicelizenzen, die pro Monat zugewiesen wurden. Beispielsweise wird einem Benutzer, der im Juli das erste Mal auf den Cloudservice zugreift, eine Lizenz zugewiesen. Diese Lizenz wird im Juli unter den neu zugewiesenen Lizenzen gezählt.
- **Aktive Nutzung:** Trends der täglichen und monatlichen aktiven Nutzung im vorangegangenen Kalendermonat bzw. Kalenderjahr.



Lizenzaktivität

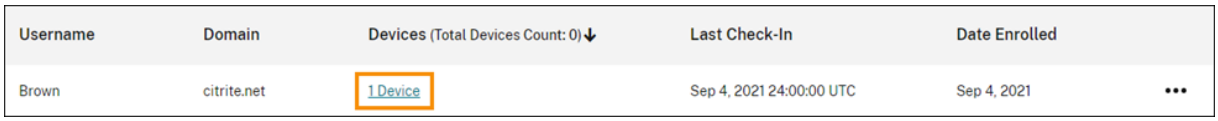
Im Abschnitt **Lizenzaktivität** wird eine Liste mit folgenden Informationen angezeigt:

- Verbraucher, denen Lizenzen zugewiesen sind
- Datum, an dem Lizenzen zugewiesen wurden
- Anzahl der registrierten Geräte und das Datum des letzten Eincheckens für jeden Benutzer

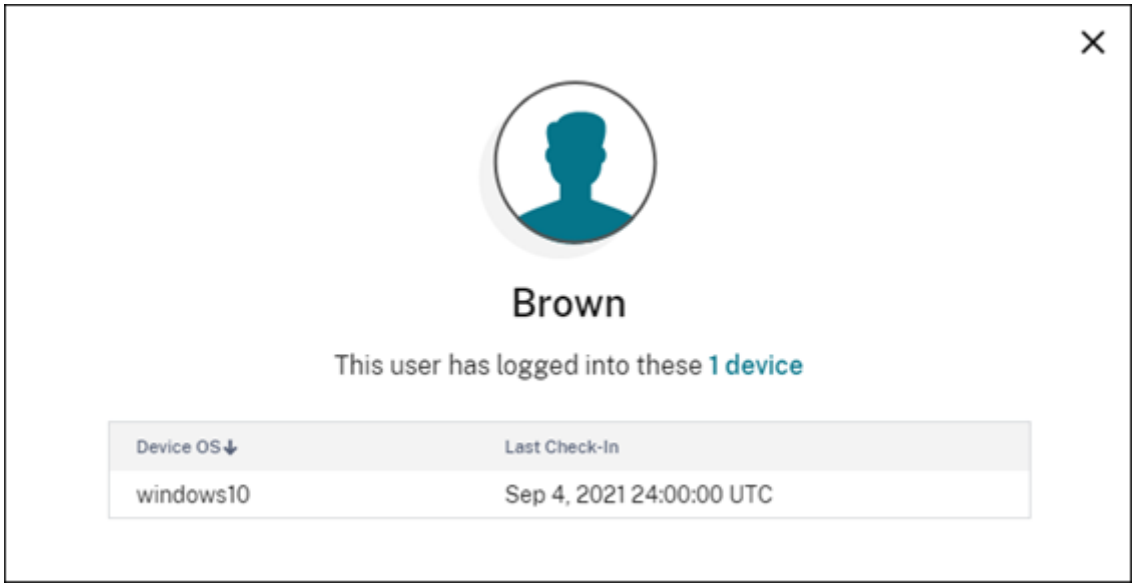


Anzeigen der registrierten Geräte

Um die Anzahl der registrierten Geräte für einen bestimmten Benutzer anzuzeigen, klicken Sie auf den Link in der Spalte **Geräte**.



Citrix Cloud zeigt eine Liste der registrierten Geräte für den Benutzer und das Datum des letzten Einchecken für jedes Gerät an.



Zugewiesene Lizenzen automatisch freigeben

Citrix Cloud gibt Lizenzen für Benutzer automatisch frei, die in den letzten 30 Tagen **alle** der folgenden Bedingungen erfüllt haben:

- Der Benutzer hat kein neues Gerät registriert.
- Der Benutzer hat ein Gerät, das sich nicht bei Citrix Cloud angemeldet hat.

Es sind keine weiteren Maßnahmen erforderlich, um berechtigte Lizenzen freizugeben.

Nach der Freigabe berechtigter Lizenzen können Benutzer eine neue Lizenz erhalten, indem sie ein Gerät registrieren.

Überwachen der Bandbreitennutzung für Gateway Service

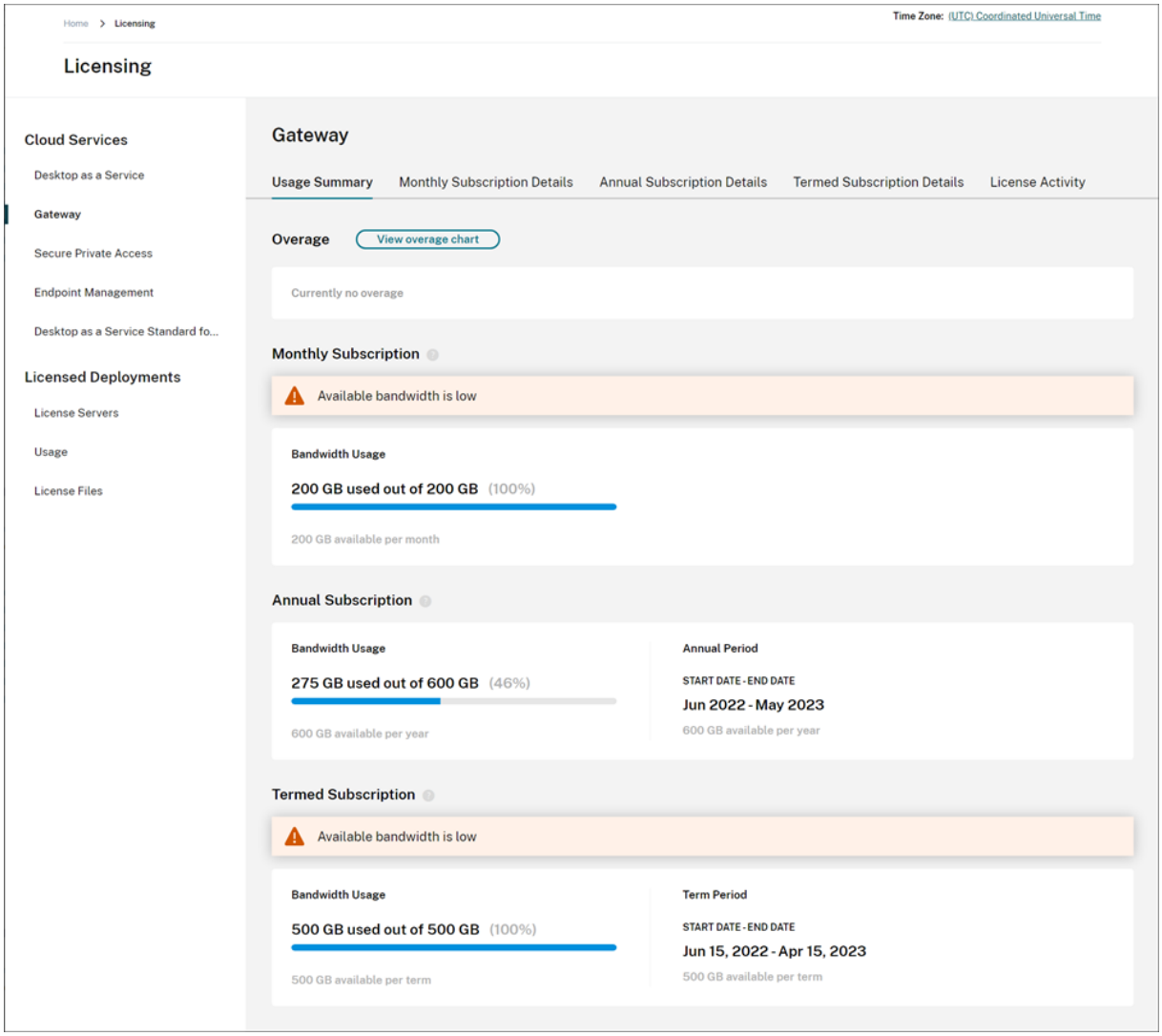
September 28, 2023

In diesem Artikel wird die Bandbreitennutzung durch den Gateway Service bei Verwendung mit Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) und Citrix Workspace beschrieben. Die Bandbreitennutzung für den in Virtual Apps Essentials enthaltenen Gateway Service wird auf der Seite **Lizenzierung** der Citrix Cloud-Verwaltungskonsole nicht angezeigt.

> **Hinweis:**
>
> Die Lizenzierung für Gateway Service erleichtert es Ihnen, Ihre Bandbreitennutzung im Zusammenhang mit der Verwendung virtueller Apps und Desktops zu verstehen. Citrix erzwingt keine Bandbreitenzuteilungen in Ihrer Umgebung. Bei einer übermäßigen Nutzung der Bandbreitenzuteilung greift Citrix nicht in Produktionsworkloads oder den Betrieb des Diensts ein. Wenn Citrix die Durchsetzung von Richtlinien für den Gateway Service und die Bandbreitennutzung ändert, werden Sie von Citrix benachrichtigt, bevor diese Änderungen wirksam werden.

Nutzungszusammenfassung

Die Nutzungszusammenfassung zeigt die Bandbreitennutzung für jedes Gateway Service-Abonnement und den Gesamtwert der Überschreitung für alle Abonnements (monatlich, jährlich und befristet).



Citrix Cloud zeigt für jeden Abonnementtyp die Gesamtbandbreite und die Menge der genutzten Bandbreite an.

Je nach Abonnementtyp wird auch der Abrechnungszeitraum für das Abonnement in Citrix Cloud angezeigt:

- Monatliches Abonnement: Der aktuelle Abrechnungszeitraum wird nicht in Citrix Cloud angezeigt. Für diese Abonnements beginnt der Abrechnungszeitraum am ersten Tag des Monats und endet am letzten Tag des Monats.
- Jahresabonnement: Citrix Cloud zeigt das Start- und Enddatum des Abrechnungszeitraums an. Für diese Abonnements beträgt der Abrechnungszeitraum ein Jahr.
- Abonnement für Laufzeit: Citrix Cloud zeigt das Start- und Enddatum des Abrechnungszeitraums an. Der Abrechnungszeitraum ist bei diesen Abonnements der Zeitraum, für den das Abonnement erworben wurde. Wurde beispielsweise ein Abonnement für eine Laufzeit von drei Jahren erworben, entsprechen Start- und Enddatum des Abrechnungszeitraums diesem

Dreijahresintervall.

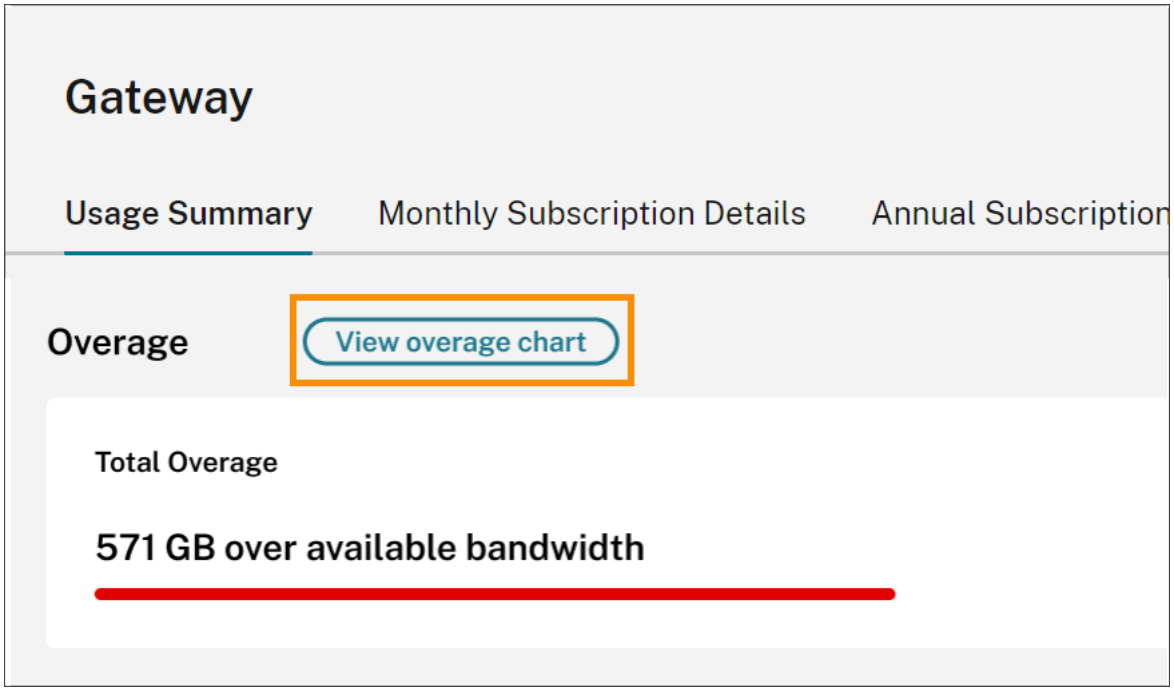
Wenn ein Abonnement innerhalb von 90 Tagen abläuft, wird eine Warnmeldung für das Abonnement angezeigt.

Überschreitung

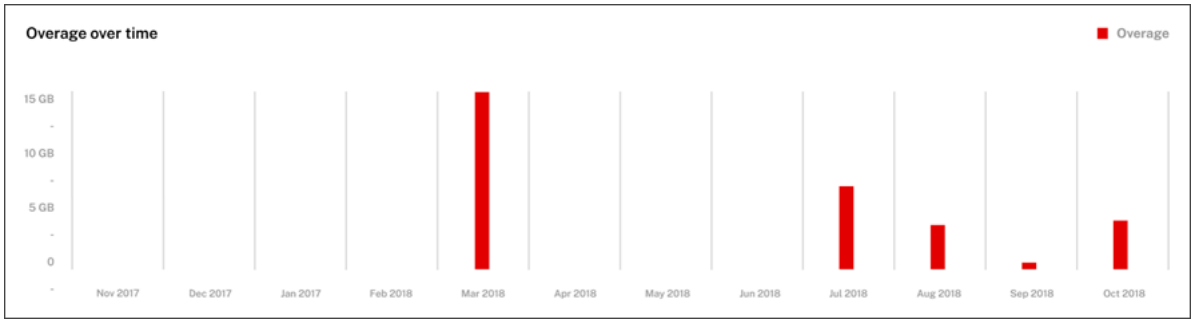
Citrix Cloud berechnet die monatliche Überschreitung der Bandbreite über alle Abonnements hinweg. Wenn Sie mehr Bandbreite verbrauchen, als Sie erworben haben, zeigt Citrix Cloud diese zusätzliche Bandbreite als Überschreitung an.

Wenn Sie mehrere Abonnements haben, misst Citrix Cloud Ihre Bandbreitennutzung zuerst anhand des Abonnements, das zuerst abläuft. Wenn Sie die Bandbreitenzuteilung in diesem Abonnement ausschöpfen, misst Citrix Cloud Ihre Bandbreitennutzung anhand des Abonnements, das als Nächstes abläuft. Wenn Sie die Bandbreitenzuteilung in allen Abonnements ausschöpfen, zeigt Citrix Cloud den zusätzlichen Mehrverbrauch als Überschreitung an.

Auf der Seite „Nutzungszusammenfassung“wird der Gesamtwert der Überschreitung für den aktuellen Monat angezeigt. Um die Bandbreitenüberschreitung im Zeitverlauf anzuzeigen, wählen Sie **Überschreitungsdiagramm anzeigen**.



Citrix Cloud zeigt dann in einem Diagramm die Überschreitungswerte für die letzten 12 Monate an.



Die Überschreitung für den aktuellen Monat wird nicht auf den nächsten Monat übertragen. Zu Beginn des nächsten Monats wird der Gesamtwert der Überschreitung auf null zurückgesetzt.

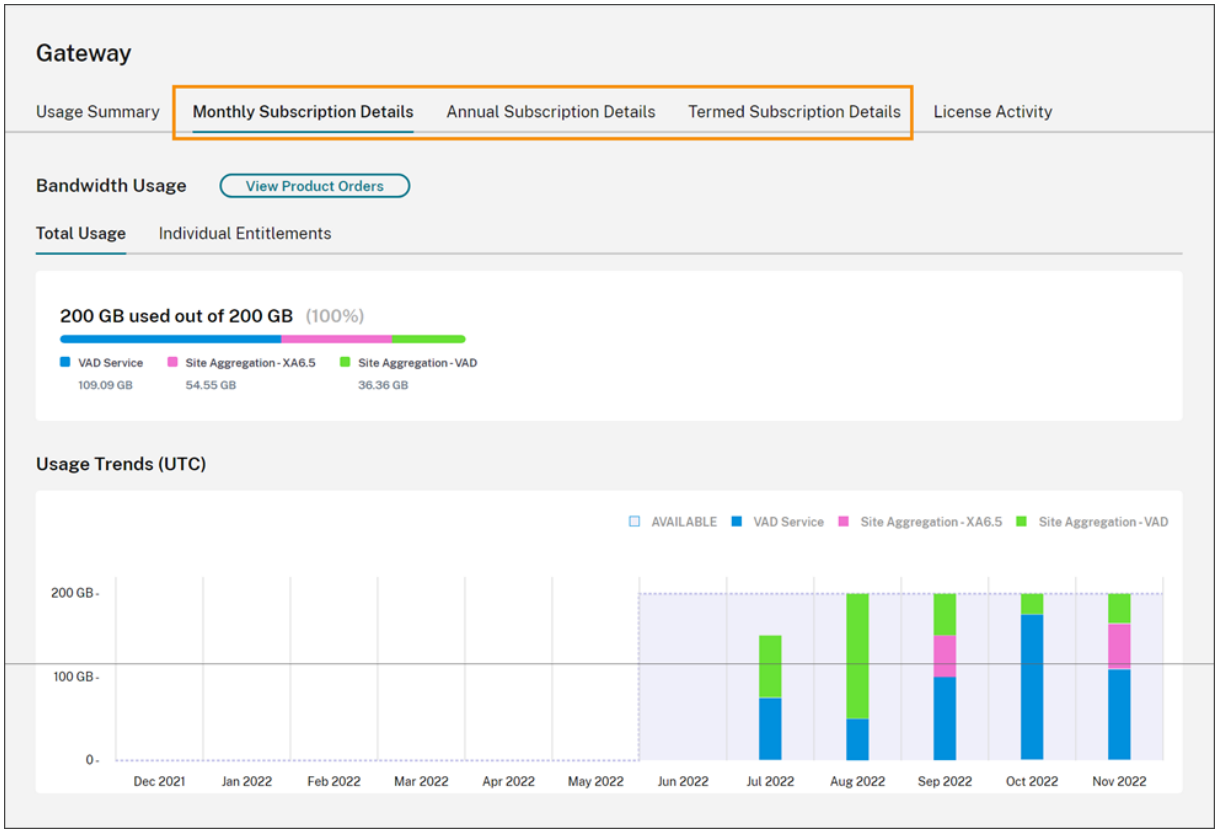
Ungenutzte Bandbreite

Citrix Cloud setzt die Bandbreitennutzung für ein Abonnement im nächsten Abrechnungszeitraum automatisch zurück. Wenn Sie die Bandbreite in einem Abonnementzeitraum nicht vollständig ausnutzen, überträgt Citrix Cloud die ungenutzte Bandbreite nicht auf den nächsten Abrechnungszeitraum.

Wenn Ihr monatliches Abonnement beispielsweise 150 GB Gesamtbandbreite umfasst und Sie in einem Monat nur 100 GB Bandbreite verwenden, setzt Citrix Cloud zu Beginn des nächsten Monats die Nutzung auf null zurück und zeigt 150 GB als Gesamtbandbreite an. Die ungenutzte Bandbreite wird nicht zum Gesamtwert Ihrer Bandbreitenzuteilung hinzugefügt.

Nutzungsdetails

Um eine detaillierte Ansicht Ihrer monatlichen, jährlichen oder befristeten Abonnements zu erhalten, wählen Sie oben in der Konsole die entsprechenden Registerkarten aus.



Für jeden Abonnementtyp werden auf der Registerkarte “Details”die folgenden Informationen angezeigt:

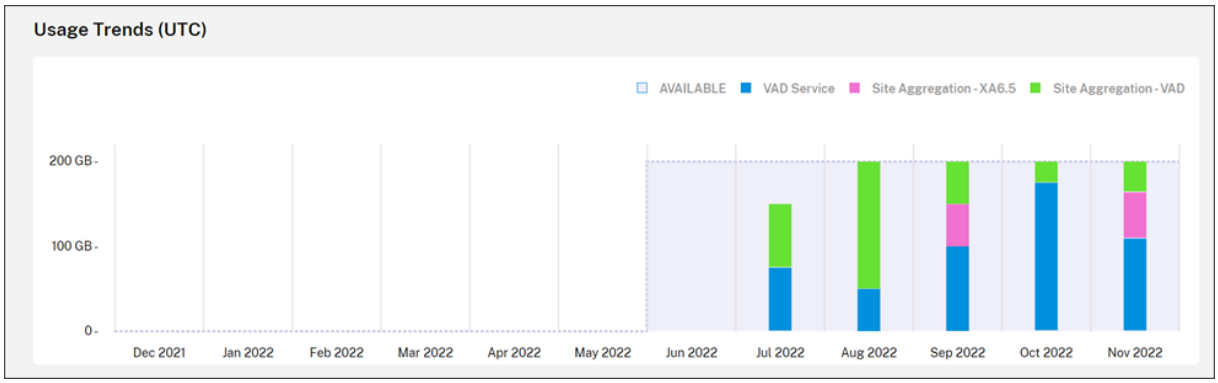
- **Gesamtnutzung:** Die Menge der genutzten Bandbreite aus der verfügbaren Gesamtbandbreite für alle Abonnements eines bestimmten Typs. Bei monatlichen Abonnements wird die Gesamtnutzung für den aktuellen Monat angezeigt. Bei Jahresabonnements und Abonnements für Laufzeit wird die Gesamtnutzung für alle Abonnements des Abonnementtyps zusammengefasst.
- **Individuelle Ansprüche:** Die Gesamtmenge an Bandbreite, die von jedem Abonnement eines bestimmten Typs verbraucht wurde. Wenn Sie beispielsweise mehrere Jahresabonnements haben, wird auf dieser Registerkarte die Nutzung für jedes Jahresabonnement separat aufgeschlüsselt.

Die Menge an verbrauchter Bandbreite wird nach Zugriff über Citrix DaaS (**VAD-DIENST**) oder über Ihre on-premises Virtual Apps and Desktops-Bereitstellung per Siteaggregation in Citrix Workspace aufgeschlüsselt.

Nutzungstrends

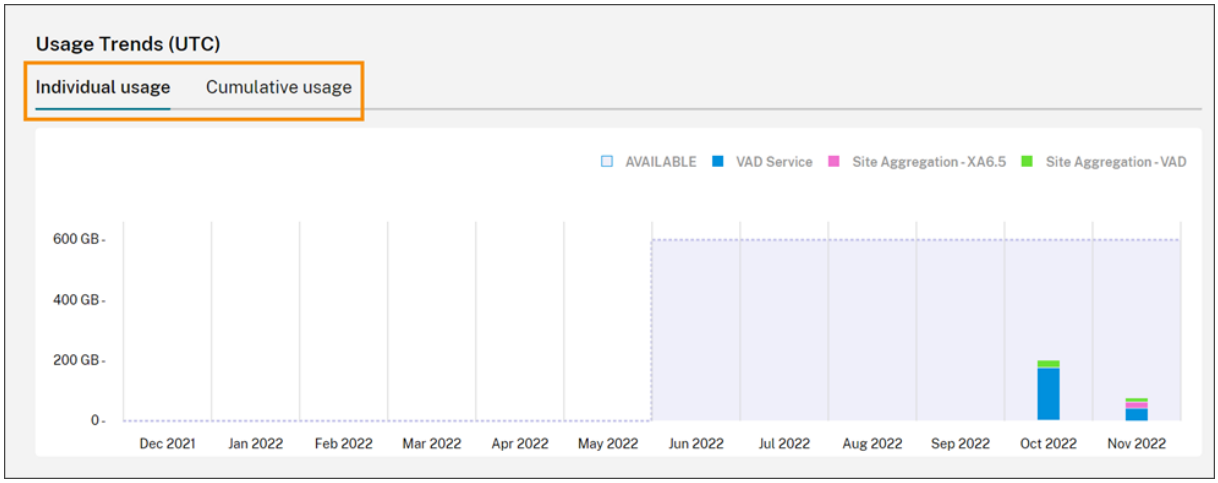
Im Abschnitt **Nutzungstrends** werden die Nutzungsdaten der letzten 12 Monate aufgeschlüsselt.

Bei monatlichen Abonnements wird die Nutzung für jeden einzelnen Monat angezeigt, in dem das Abonnement genutzt wurde.

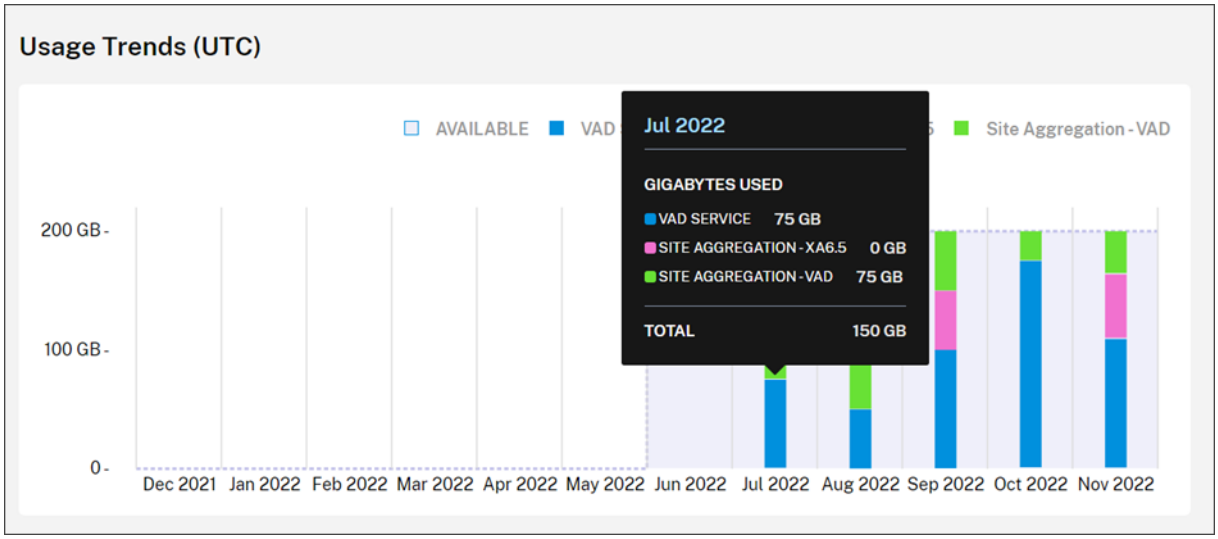


Bei Jahresabonnements und Abonnements für Laufzeit enthält dieser Abschnitt die folgenden Ansichten:

- **Individuelle Nutzung:** Die Bandbreitennutzung in jedem Monat des aktuellen Abrechnungszeitraums.
- **Kumulative Nutzung:** Die kumulierte Bandbreitennutzung für jeden Monat während des aktuellen Abrechnungszeitraums.



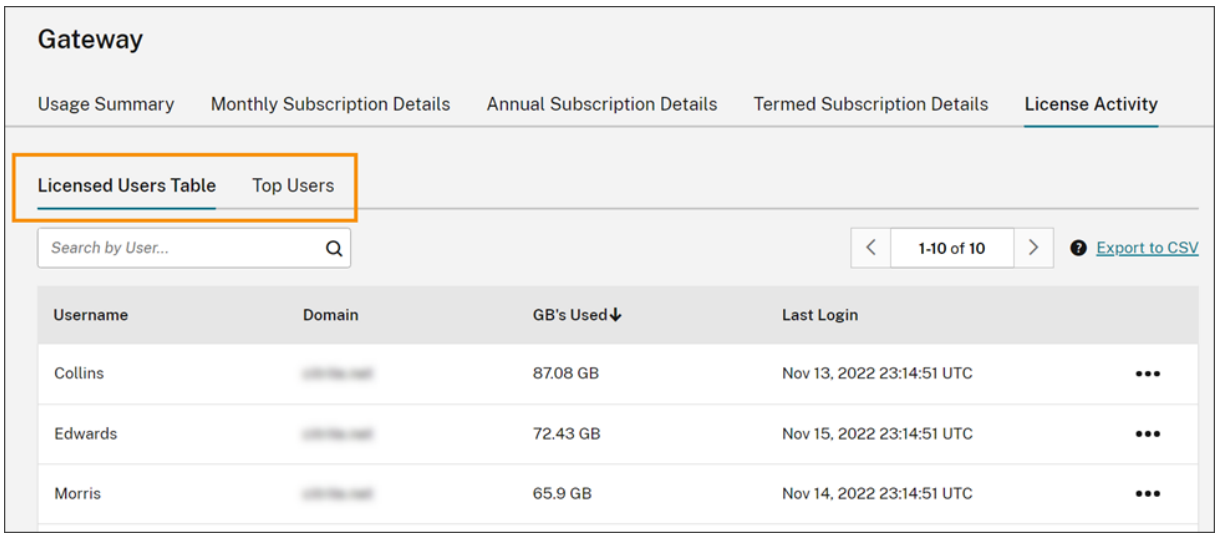
Für alle Abonnementtypen gilt: Wenn Sie auf einen Balken im Diagramm "Nutzungstrends"zeigen, sehen Sie die Bandbreitennutzung für diesen Zeitraum, unterteilt nach Zugriffstyp.



Lizenzaktivität

Der Abschnitt **Lizenzaktivität** bietet folgende Informationen:

- **Lizenzierte Benutzer:** Liste der einzelnen Benutzer, denen Lizenzen zugewiesen wurden. Aufgeführt sind die Domäne, zu der ein Benutzer gehört, die in den vergangenen 30 Tagen genutzte Bandbreite und das Datum der letzten Nutzung eines Diensts, bei der Bandbreite verbraucht wurde.
- **Top-Benutzer**: Liste der 10 Benutzer mit der höchsten Bandbreitennutzung. Aufgeführt ist die Bandbreitennutzung für jeden Benutzer in den vergangenen 30 Tagen, aufgeschlüsselt nach Zugriffstyp (Citrix DaaS oder on-premises Virtual Apps and Desktops über Siteaggregation).

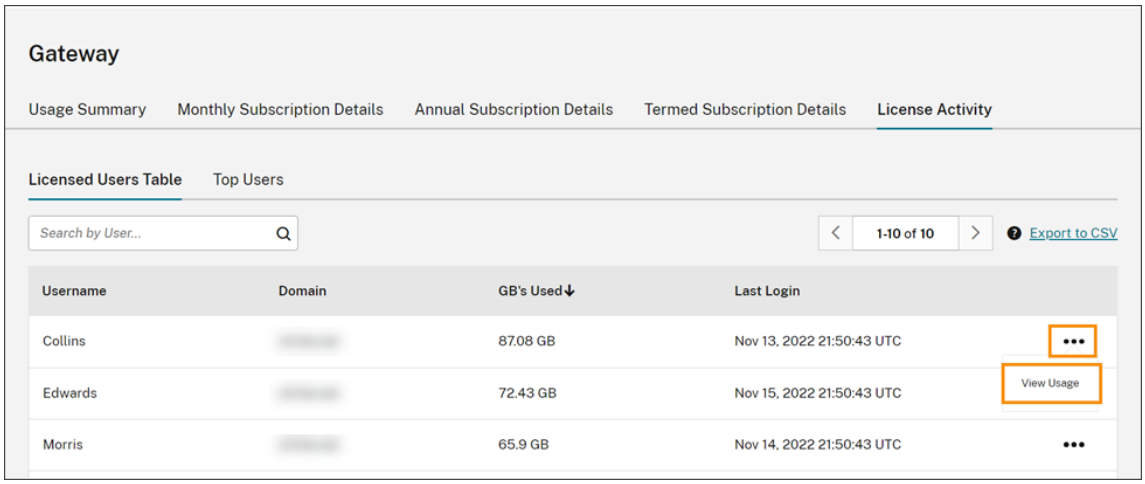


Citrix Cloud zeigt die Bandbreitennutzung der letzten 30 Tage auch für Benutzer, die nicht länger eine Lizenz verwenden. Wenn ein Gateway Service-Abonnement abläuft, zeigt Citrix Cloud weiterhin die

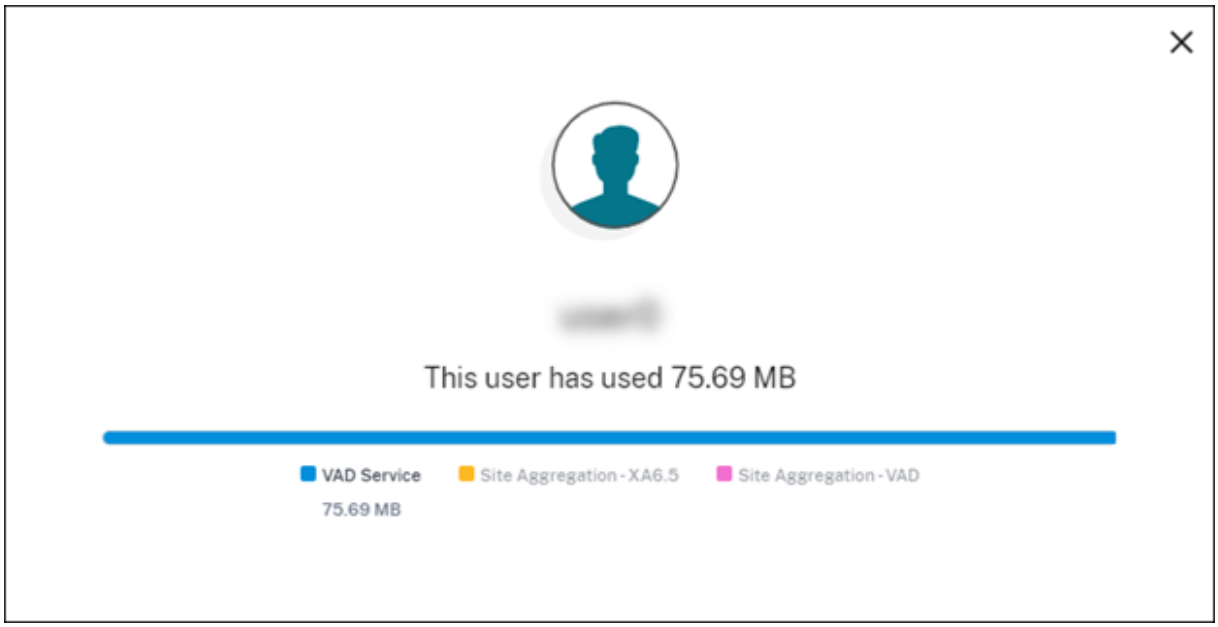
Bandbreite an, die einzelne Benutzer im Zeitraum von 30 Tagen verbraucht haben.

Nutzungsdetails für einen bestimmten Benutzer anzeigen

1. Wählen Sie **Tabelle der lizenzierten Benutzer** und suchen Sie den gewünschten Benutzer in der Liste.
2. Klicken Sie auf die drei Punkte (…) ganz rechts auf der Seite und wählen Sie im Menü die Option **Nutzung anzeigen** aus.

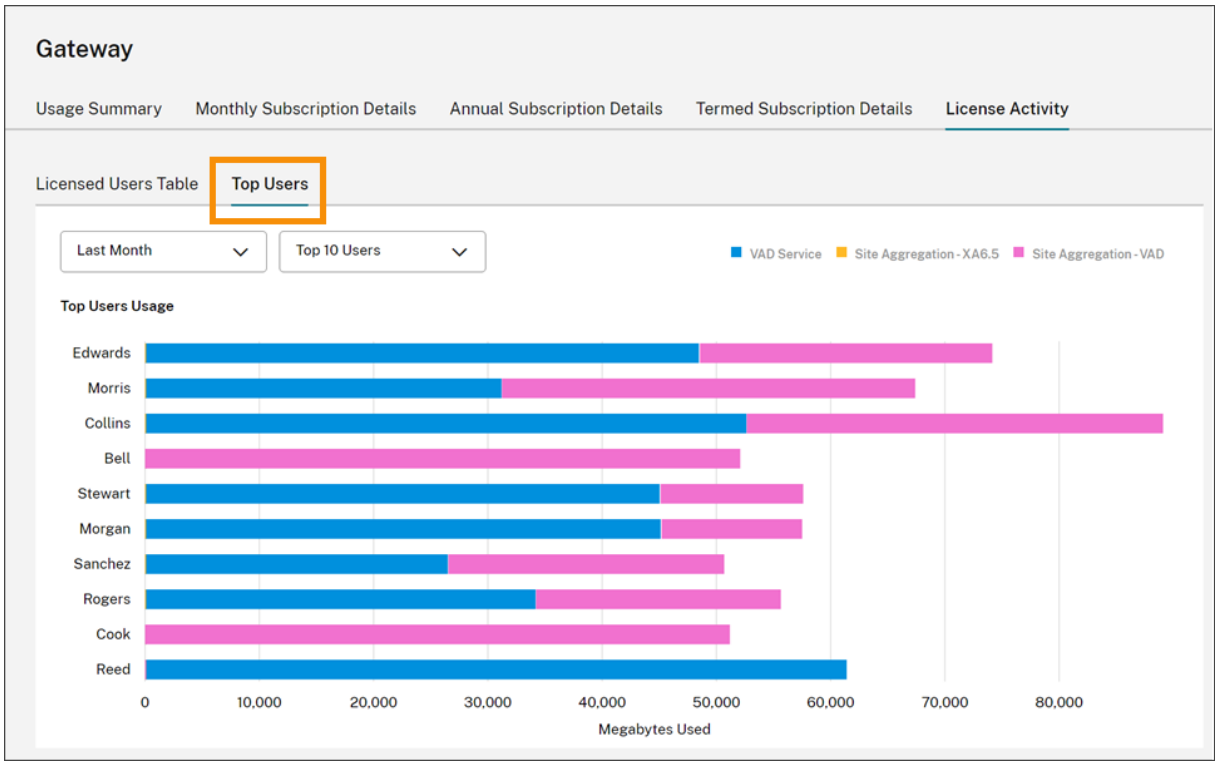


Citrix Cloud zeigt die Bandbreite des Benutzers aufgeschlüsselt nach Zugriff an.



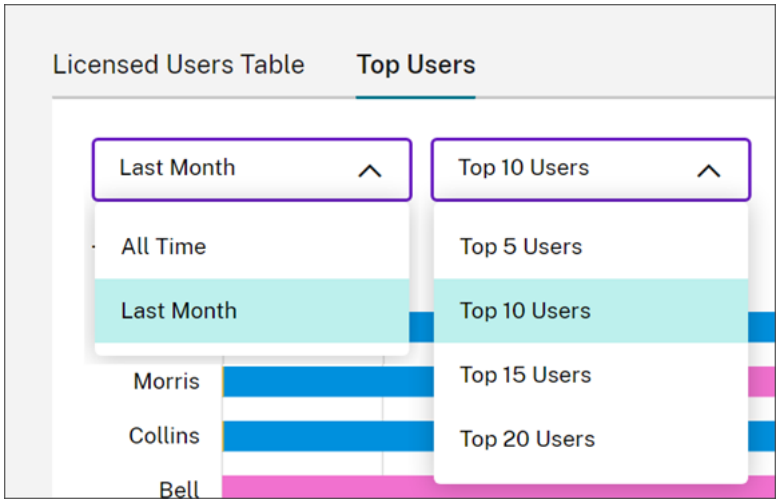
Nutzungsdetails für Top-Benutzer anzeigen

Wählen Sie **Top-Benutzer**.



Citrix Cloud zeigt ein Diagramm der Bandbreitennutzung der Top-Benutzer, aufgeschlüsselt nach Zugriffstyp.

In der Standardeinstellung werden im Diagramm **Top-Benutzer** die 10 Benutzer angezeigt, die in den letzten 30 Tagen die meiste Bandbreite genutzt haben. Sie können diese Ansicht ändern, um fünf, 15 oder 20 Benutzer mit dem höchsten Verbrauch anzuzeigen. Sie können den Zeitraum auch in **Gesamte Zeit** ändern, um die Top-Benutzer während der Laufzeit Ihres Abonnements anzuzeigen. Um diese Ansicht zu ändern, wählen Sie eine Option aus dem jeweiligen Menü aus.



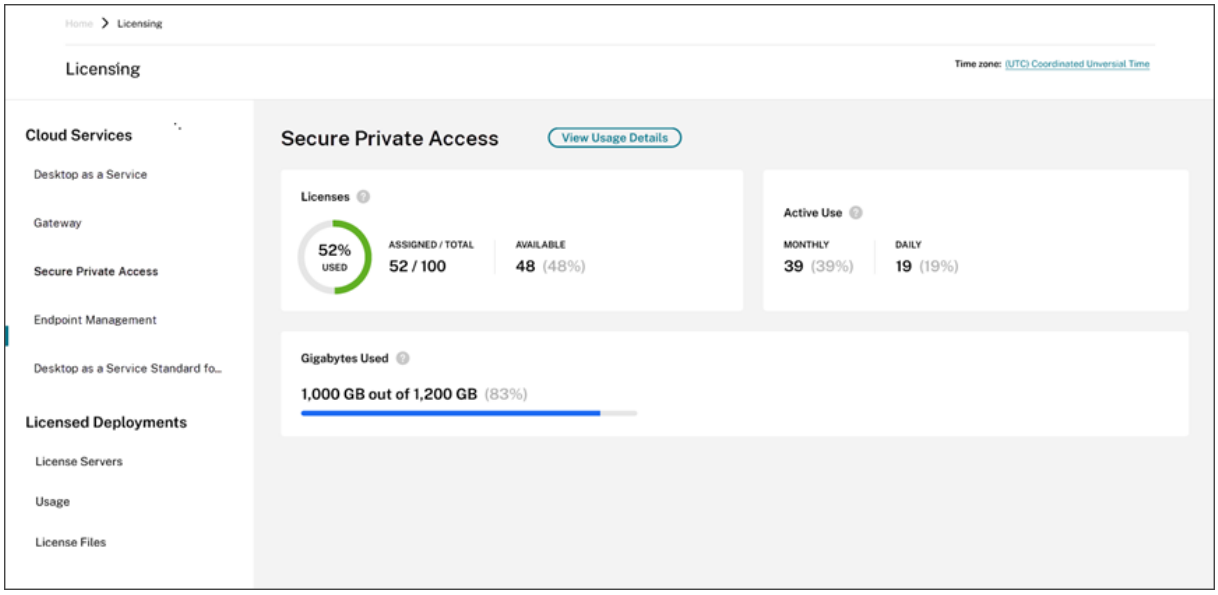
Überwachen von Lizenzen und Nutzung für Secure Private Access

November 24, 2023

Lizenzzuweisung

Eine Lizenz wird zugewiesen, wenn ein eindeutiger Benutzer zum ersten Mal eine SaaS-App oder TCP und UDP-Apps startet.

Zusammenfassung zur Lizenzierung



Die Lizenzübersicht enthält die folgenden Informationen:

- Prozentsatz der insgesamt erworbenen Lizenzen, die zugewiesen sind.
  - Wenn sich der Prozentsatz 100 % nähert, wechselt der Prozentsatz von grün zu gelb. Wenn der Prozentsatz 100 % überschreitet, wird der Prozentsatz rot angezeigt.
- Das Verhältnis zugewiesener zu erworbenen Lizenzen und die Anzahl der Lizenzen, die für die Zuweisung verfügbar sind.
- Statistik der aktiven Nutzung pro Monat und Tag:
  - "Monatliche aktive Nutzung"bezieht sich auf die Anzahl einzelner Benutzer, die den Service in den letzten 30 Tagen genutzt haben.
  - "Tägliche aktive Nutzung"bezieht sich auf die Anzahl einzelner Benutzer, die den Service in den letzten 24 Stunden genutzt haben.
- Die Menge der genutzten Bandbreite aus der Gesamtbandbreite für alle Abonnements.
- Die verbleibende Zeit bis zum Ablauf des Cloudserviceabonnements. Wenn das Abonnement innerhalb der nächsten 90 Tage abläuft, wird eine Warnmeldung angezeigt.

Genutzte Lizenzen und Bandbreite

Bei Secure Private Access Advanced-Abonnements hat jeder Benutzer 5 GB Bandbreite pro Monat (60 GB pro Benutzer und Jahr). Bei Secure Private Access Standard-Abonnements hat jeder Benutzer 1 GB Bandbreite pro Monat (12 GB pro Benutzer und Jahr). Diese Bandbreite wird für die Lizenzen und den Abonnementzeitraum gebündelt.

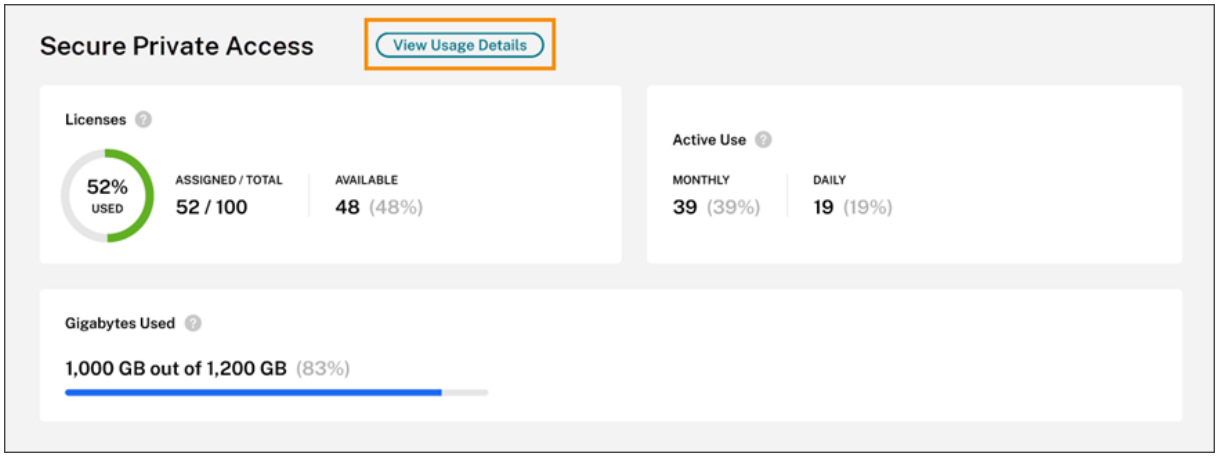
Wenn Sie beispielsweise 100 Lizenzen für drei Jahre kaufen, erhalten Sie eine Gesamtbandbreite von 18000 GB (6000 GB pro Jahr für drei Jahre). Die Bandbreite wird für den Zeitraum von drei Jahren auf alle lizenzierten Benutzer verteilt. Wenn Sie zusätzliche Abonnements erwerben, zeigt Citrix Cloud die Gesamtzahl der Lizenzen und Bandbreite für alle Abonnements an.

Während des Abonnementzeitraums nicht genutzte Bandbreite wird bei Verlängerung in Citrix Cloud nicht übertragen. Wenn Sie bei Ablauf des Abonnements mehr als die gekaufte Bandbreite genutzt haben, bleibt die verfügbare Bandbreite bei null, wenn Sie das Abonnement verlängern.

Bei mehreren Abonnements mit überlappenden Fristen wird die einem Abonnement zugeordnete Bandbreite aus der Lizenzierung entfernt, wenn dieses abläuft. Wenn Sie beispielsweise zwei Abonnements erwerben, zeigt Citrix Cloud die Gesamtlizenzen und die Gesamtbandbreite für beide Abonnements an. Wenn das erste Abonnement abläuft, zeigt Citrix Cloud nur die Bandbreite an, die mit dem nicht abgelaufenen Abonnement verknüpft ist.

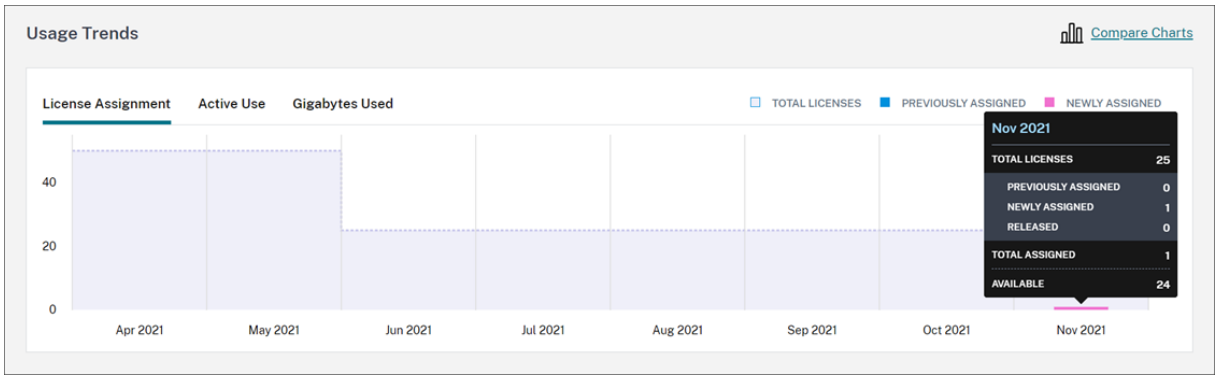
Nutzungstrends

Klicken Sie für eine detaillierte Ansicht Ihrer Bandbreitennutzung und Lizenzen auf **Nutzungsdetails anzeigen**.



Citrix Cloud zeigt eine Aufschlüsselung des Bandbreitenverbrauchs basierend auf der Art der Apps, auf die Benutzer zugreifen können, an.

Sie sehen außerdem eine Aufschlüsselung der Nutzungstrends sowie einzelne Benutzer, die Cloudservicelizenzen und Bandbreite verwenden.

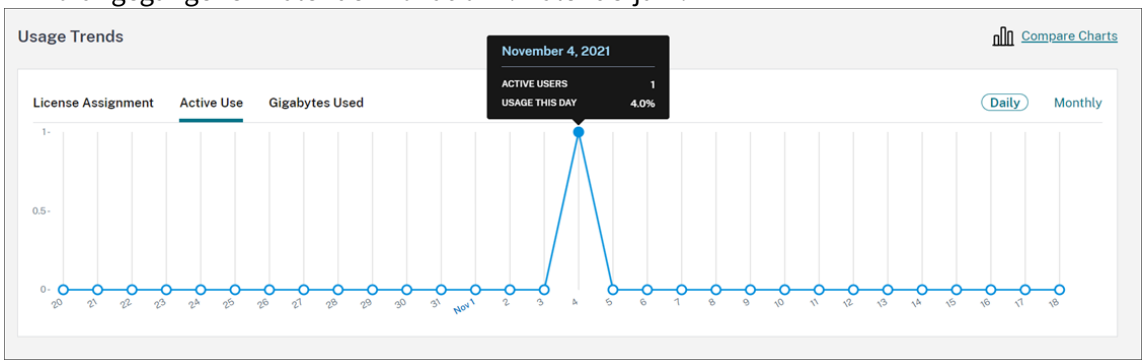


Diese Aufschlüsselung unter **Nutzungstrends** zeigt Ihnen folgende Informationen:

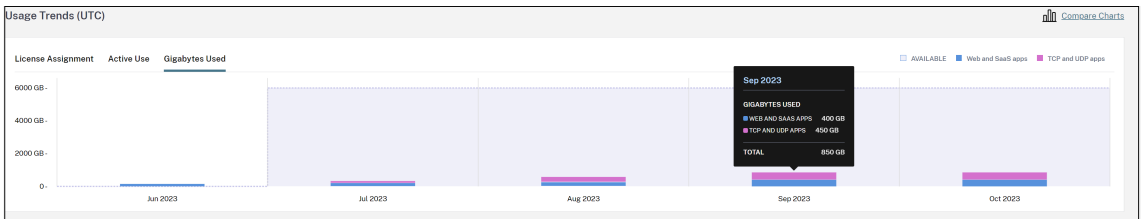
- Auf der Registerkarte **Lizenzzuweisung**:
  - **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.

  - **Zuvor zugewiesen:** Die Cloudservicelizenzen, die bereits zu Beginn eines jeden Monats zugewiesen waren. Wenn einem Benutzer beispielsweise im Juli eine Lizenz zugewiesen wird, zählt Citrix Cloud diese Zuweisung unter "Zuvor zugewiesen"für August mit.
  - **Neu zugewiesen:** Die Anzahl der Lizenzen, die pro Monat zugewiesen wurden. Beispielsweise greifen Sie im Juli das erste Mal auf den Cloudservice zu und es wird Ihnen eine Lizenz zugewiesen. Citrix Cloud zählt diese Lizenz unter den neu zugewiesenen Lizenzen für Juli.

- Auf der Registerkarte **Aktive Nutzung:** Trends der täglichen und monatlichen aktiven Nutzung im vorangegangenen Kalendermonat bzw. Kalenderjahr.



- Auf der Registerkarte **Verwendete Gigabytes**: Die Menge der genutzten Bandbreite aus der gesamten verfügbaren Bandbreite. Es werden Informationen zur Nutzung pro Benutzer und pro Anwendung (Web- und SaaS-Apps sowie TCP- und UDP-Apps) angezeigt.



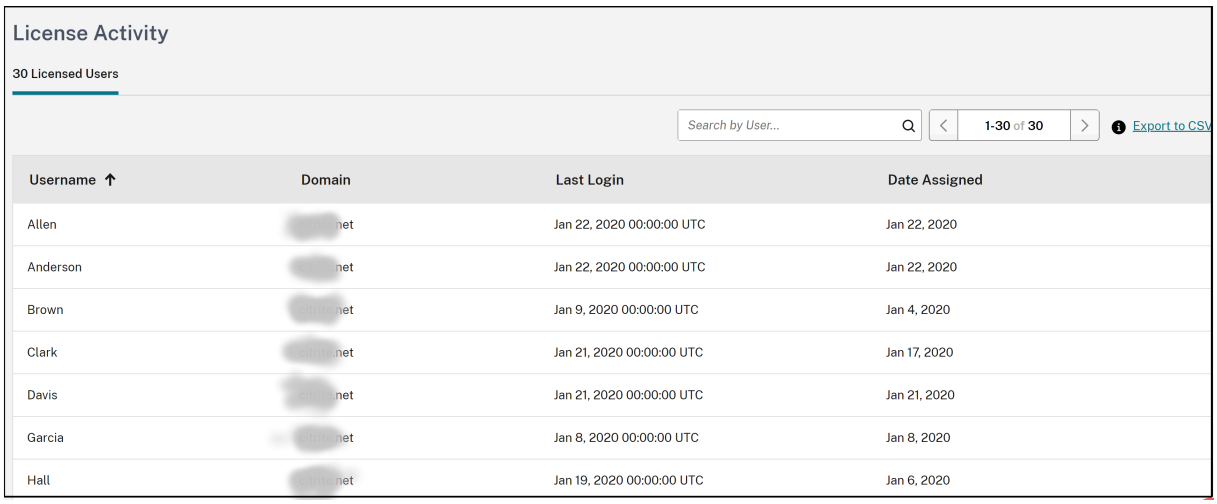
Wählen Sie **Diagramme vergleichen** aus, um Lizenzzuweisung, aktive Nutzung und Trends der Bandbreitennutzung zu vergleichen.

Hinweis:

Nutzungstrends werden kumulativ für die Dauer der aktuellen Abonnementlaufzeit dargestellt. Wenn Sie das Abonnement verlängern, werden die Nutzungstrends zu Beginn der neuen Abonnementlaufzeit zurückgesetzt.

Lizenzaktivität

Im Abschnitt **Lizenzaktivität** werden außerdem folgende Informationen angezeigt:



- Liste der einzelnen Benutzer, denen Lizenzen zugewiesen sind.
- Die Domäne, zu der der Benutzer gehört.
- Das Datum, an dem der Benutzer den Dienst zuletzt genutzt hat.
- Das Datum, an dem Benutzern eine Lizenz zugewiesen wurde.

Freigeben zugewiesener Lizenzen

Citrix Cloud gibt automatisch Lizenzen frei, wenn Sie den Service in den letzten 30 Tagen nicht genutzt haben. Der Citrix Administrator muss nichts unternehmen, um die Lizenzen freizugeben.

Nach dem Freigeben einer Lizenz erhöht sich die Anzahl der verfügbaren Lizenzen und die Anzahl der zugewiesenen Lizenzen nimmt entsprechend ab. Nach der Freigabe einer Lizenz können Sie eine neue Lizenz erhalten, indem Sie sich anmelden und den Cloudservice verwenden.

Überwachen des Citrix Managed Azure-Ressourcenverbrauchs für Citrix DaaS

September 28, 2023

Wenn Sie eine Berechtigung für Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) erwerben, können Sie auch den Citrix Azure Consumption Fund erwerben, mit dem Sie Ressourcen in einem Citrix Managed Azure-Abonnement verwenden können. Sie können diese Ressourcen verwenden, um neben Ihren On-Premises-VDAs auch Apps und Desktops für Ihre Benutzer bereitzustellen.

Wenn Sie den Citrix Azure Consumption Fund erwerben, können Sie mit einer der folgenden Methoden für den Verbrauch zahlen:

- Nutzungsbasiert: Die Citrix Managed Azure-Ressourcen, die Sie in einem bestimmten Monat verwenden, stellt Citrix Ihnen im Folgemonat in Rechnung. Citrix Cloud zeigt Ihre Nutzung als Überschreitung an.
- Vorausbezahlter Verbrauch: Sie können den Verbrauch monatlich oder jährlich (laufzeitbasiert) im Voraus bezahlen. Für jede Nutzung, die Ihren vorausbezahlten Verbrauch übersteigt, zeigt Citrix Cloud diese Nutzung als Überschreitung an. Überschreitung in einem bestimmten Monat stellt Citrix Ihnen im Folgemonat in Rechnung.

Jede Verbrauchseinheit wird mit 1,00 USD bewertet. Über die Lizenzierungskonsole in Citrix Cloud können Sie Ihren Verbrauch in Einheiten verfolgen.

Verwenden Sie den Citrix Managed Azure Consumption Calculator zur Schätzung der Verbrauchskosten. Um den Verbrauch und die Lizenzkosten für Citrix DaaS Standard for Azure (früher Citrix Virtual Apps and Desktops Standard für Azure) zu schätzen, verwenden Sie den Licensing and Consumption Calculator.

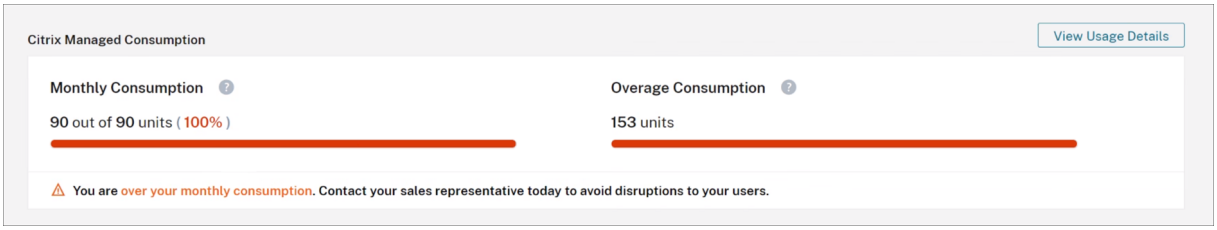
Unterstützte Produkte

Die Verbrauchsüberwachung ist für die folgenden Editionen von Citrix DaaS verfügbar:

- Citrix DaaS Advanced (früher Virtual Apps Advanced)
- Citrix DaaS Premium (früher Virtual Apps Premium)
- Citrix DaaS Advanced Plus (früher Virtual Apps and Desktops Advanced)
- Citrix DaaS Premium (früher Virtual Apps and Desktops Premium)
- Citrix DaaS Standard für Azure (früher Virtual Apps and Desktops Standard für Azure)

Verbrauchsübersicht

Im Abschnitt “Citrix Managed Consumption”wird eine Übersicht der Einheiten angezeigt, die Sie in Ihrem Consumption Fund genutzt haben.



Unter **Monatlicher Verbrauch** wird die Anzahl der Verbrauchseinheiten angezeigt, die Sie im aktuellen Monat verwendet haben, bezogen auf die Gesamtzahl der monatlichen Consumption

Fund-Einheiten, die Sie gekauft haben. Der monatliche Verbrauch wird jeden Monat zurückgesetzt. Nicht genutzte Verbrauchseinheiten werden nicht auf den nächsten Monat übertragen.

Unter **Laufzeitverbrauch** wird die Anzahl der von Ihnen genutzten Verbrauchseinheiten angezeigt, bezogen auf die Gesamtzahl der von Ihnen gekauften Consumption Fund-Einheiten für die Laufzeit. Wie bei den monatlichen Verbrauchseinheiten werden ungenutzte Verbrauchseinheiten für die Laufzeit nicht auf das nächste Jahr übertragen.

Unter **Mehrverbrauch** wird die Anzahl der Verbrauchseinheiten angezeigt, die Sie über die Anzahl der Einheiten in Ihrem Azure Consumption Fund hinaus verwendet haben. Wenn Sie Citrix Managed Azure-Ressourcen nutzungsabhängig verwenden, wird Ihr Verbrauch standardmäßig als Überschreitung angezeigt.

Messung von Überschreitung

Wenn Sie den Azure Consumption Fund nutzungsbasiert verwenden, zeigt Citrix Cloud die Anzahl der Verbrauchseinheiten, die Sie für den aktuellen Monat verwendet haben, als Überschreitung an.

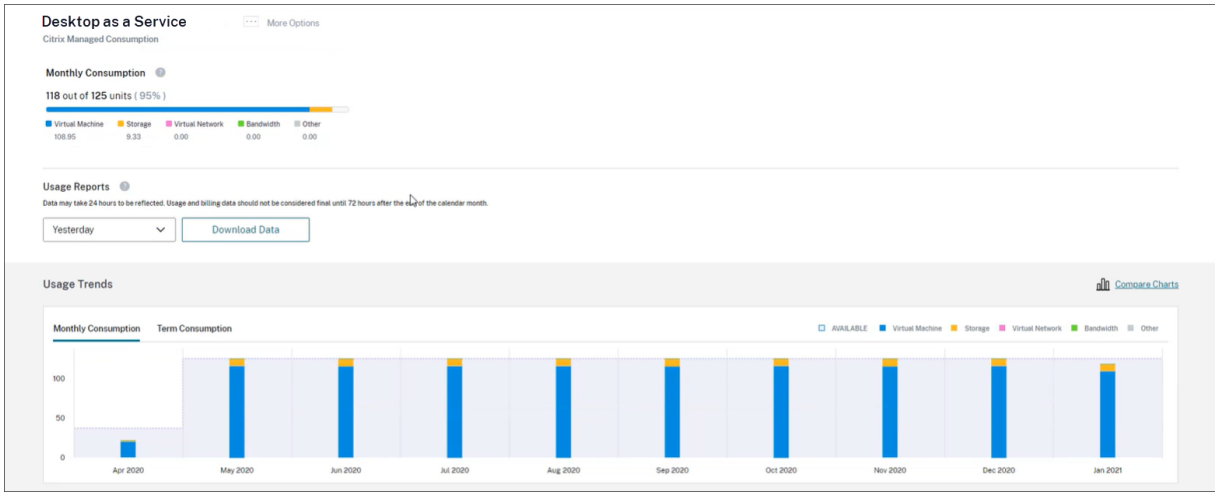
Wenn Sie den Verbrauch auf Monats- oder Jahresbasis im Voraus bezahlt haben, zeigt Citrix Cloud die Anzahl der monatlichen Verbrauchseinheiten oder der Verbrauchseinheiten für die Laufzeit an, die Sie für den aktuellen Monat oder das aktuelle Jahr verwendet haben. Wenn Sie mehr Einheiten verbrauchen, als Sie gekauft haben, zeigt Citrix Cloud die überschüssigen Einheiten als Überschreitung an.

Wenn Sie den Verbrauch sowohl auf Monats- als auch Jahresbasis im Voraus bezahlt haben, misst Citrix Cloud Ihren Verbrauch zuerst an Ihren gekauften monatlichen Einheiten. Nachdem diese Einheiten verbraucht wurden, misst Citrix Cloud Ihren Verbrauch an Ihren Jahreseinheiten. Nachdem diese Einheiten verbraucht wurden, zeigt Citrix Cloud alle überschüssigen Einheiten, die Sie verbrauchen, als Überschreitung an.

Wenn Sie zusätzliche Verbrauchseinheiten kaufen und in Ihrem Konto bereits Überschreitungen vorhanden sind, werden die neuen Verbrauchseinheiten nicht auf die Überschreitung angewendet. Die neuen Verbrauchseinheiten gelten nur für die Nutzung, zu der es nach dem Kauf dieser Einheiten kommt.

Verbrauchsdetails

Klicken Sie am rechten Rand der Zusammenfassung auf **Nutzungsdetails anzeigen**, um eine detaillierte Ansicht Ihrer Verbrauchseinheiten zu erhalten. Auf der Detailseite finden Sie eine Aufschlüsselung Ihres Verbrauchs und Ihrer Nutzungstrends.



Nutzungsberichte

Sie können Nutzungsinformationen für ein von Ihnen angegebenes Intervall als CSV-Datei herunterladen. Klicken Sie auf **Daten herunterladen**, um eine CSV-Datei zu generieren und auf Ihren lokalen Computer herunterzuladen.

Nach Ablauf eines Tages oder Monats kann es bis zu 72 Stunden dauern, bis Daten die gesamte Nutzung widerspiegeln.

Die CSV-Datei enthält die folgenden Abschnitte:

- Berichtszusammenfassung, in der die vor und nach dem Berichtdatumsbereich verfügbaren Verbrauchseinheiten, die gesamten Nutzungsgebühren und die ausstehenden Überschreitungen angezeigt werden.

Data may take 24 hours to be reflected. Usage and billing data should not be considered final until 72 hours after the end of the calendar month.			
Org ID	51938754		
Report Date	12/3/2021		
Date Start	11/1/2021		
Date End	11/30/2021		
Report Summary			
	Credits	Debits	
Monthly Consumption Units Available before 11/01/2021	$0		
Termed Consumption Units Available before 11/01/2021	$0		
Trial Consumption Units Available before 11/01/2021	$0		
Total Usage to Charge		$851.96	
Expired Consumption Commitment		$0.00	
Total	$0.00	$851.96	

Monthly Consumption Units Available after 11/30/2021	$0		
Termed Consumption Units Available after 11/30/2021	$0		
Trial Consumption Units Available after 11/30/2021	$0		
Pending Overage by 11/30/2021	$0.00		

- Tägliche Zusammenfassung, die die gesamte Nutzungsgebühr, die verbleibenden Mittel für den Monat und die Laufzeit sowie die Überschreitungsgebühren für jeden Tag des Berichtdatumsbereichs anzeigt.

Daily Summary				
Date	Total Usage	Remaining Monthly Funds	Remaining Termed Funds	Overage Amount
11/1/2021	$28.40	$0	$0	$0
11/2/2021	$28.40	$0	$0	$0
11/3/2021	$28.40	$0	$0	$0
11/4/2021	$28.40	$0	$0	$0
11/5/2021	$28.39	$0	$0	$0
11/6/2021	$28.39	$0	$0	$0
11/7/2021	$28.40	$0	$0	$0
11/8/2021	$28.40	$0	$0	$0

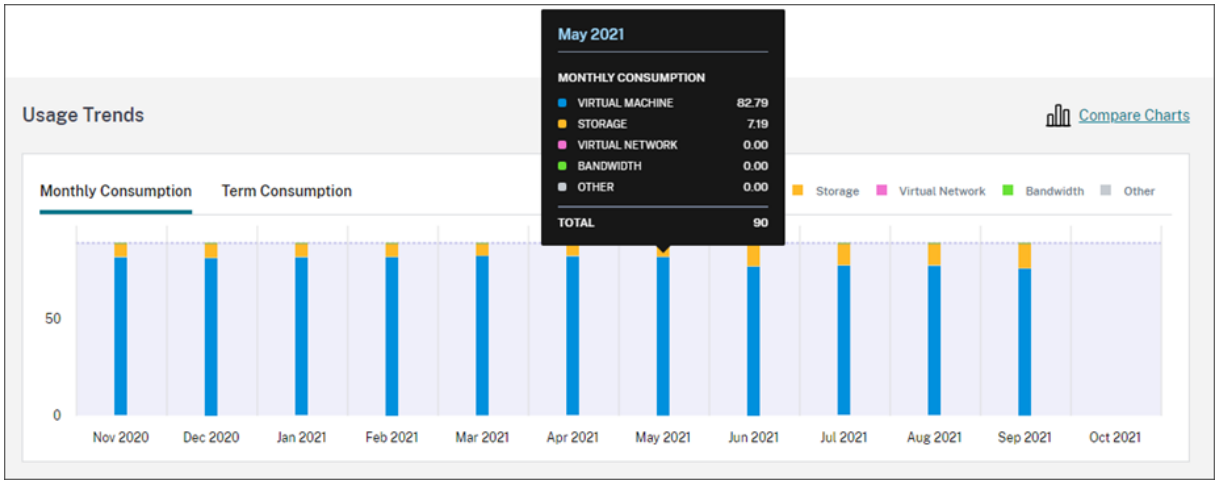
- Gemessene Nutzung von Azure-VMs, Netzwerkverbindungen, Azure-Speicher und Bandbreite für jeden Tag des Berichtdatumsbereichs.

Date	Citrix Meter Name	Citrix Meter Description	Catalog Id	Catalog Name	Citrix Meter Region	Citrix Meter Category	Citrix Meter Sub Category	Citrix Meter Unit	Quantity	SRP	Total	Total Charged
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000444	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	Bandwidth		10 GB	0.0000018	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		N/A	N/A	None	Bandwidth		10 GB	0.0064263	$1.13	$0.01	$0.01
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	Bandwidth		10 GB	0.0000137	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	Bandwidth		10 GB	0.0000015	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	Bandwidth		10 GB	0.0000073	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	Bandwidth		10 GB	0.0000334	$1.13	$0.00	$0.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Network Peering - Ingress		N/A	N/A	None	VirtualNetwork		100 GB	0.00016714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000034	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000422	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000165	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000307	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000129	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000148	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000115	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000342	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		N/A	N/A	None	VirtualNetwork		100 GB	0.00012714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000121	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000094	$1.30	$0.00	$0.00
11/1/2021	General Block Blob - Read Operations		N/A	N/A	None	Storage		100000000	0.00000016	$4.68	$0.00	$0.00
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		N/A	N/A	US East	Storage		1 /Month	0.400032	$7.64	$3.06	$3.06
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	Storage		1 /Month	0.033336	$7.64	$0.25	$0.25
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	Storage		1 /Month	0.100008	$7.64	$0.76	$0.76
11/1/2021	Virtual Machines Av2 Series - A2 v2 - US East		N/A	N/A	US East	VirtualMachine		100 Hours	0.48	$11.83	$5.68	$5.68
11/1/2021	Premium SSD Managed Disks - P10 - Disks - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	Storage		1 /Month	0.033336	$19.22	$0.64	$0.64
11/2/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000235	$1.13	$0.00	$0.00

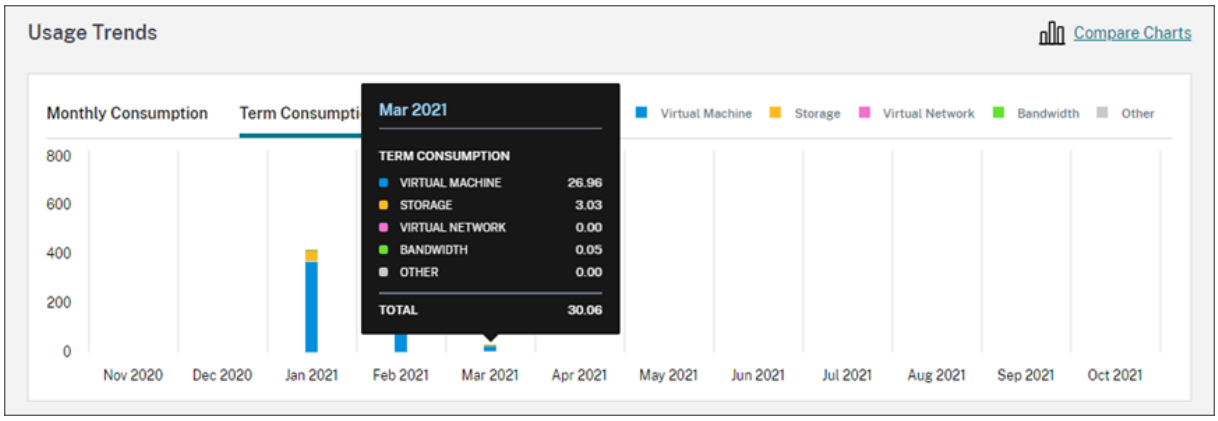
Nutzungstrends und Verbrauchsaktivität

Im Abschnitt **Nutzungstrends** wird ein Diagramm der Citrix Managed Azure-Ressourcen angezeigt, die Sie verwendet haben. Wenn Sie auf einen Balken im Diagramm zeigen, wird die Menge der Ressourcen angezeigt, die Sie in diesem Monat verbraucht haben, einschließlich virtueller Maschinen, Speicher, virtueller Netzwerkressourcen und Bandbreite.

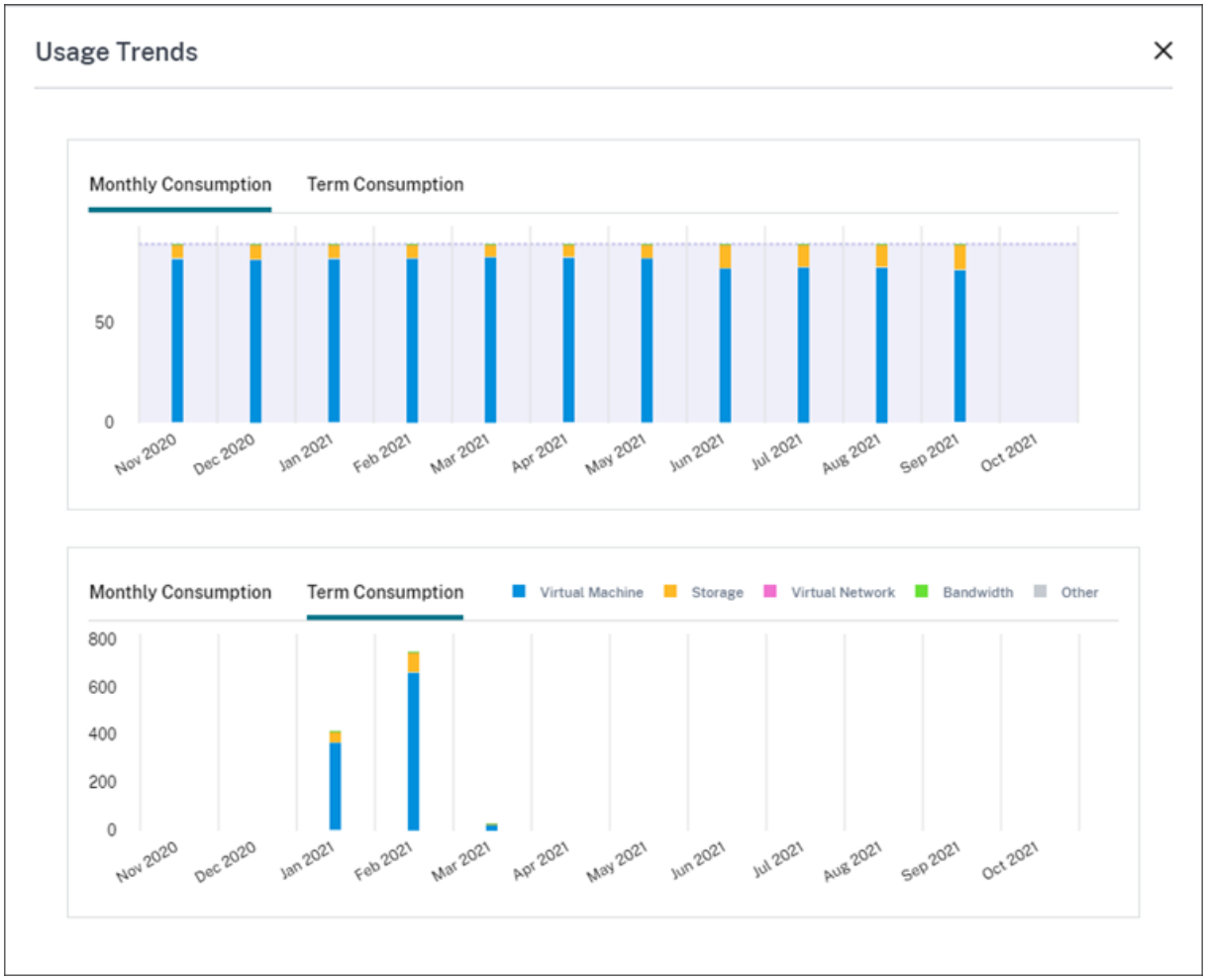
Wählen Sie **Monatlicher Verbrauch** aus, um Ihren monatlichen Verbrauch für die letzten 12 Monate anzuzeigen.



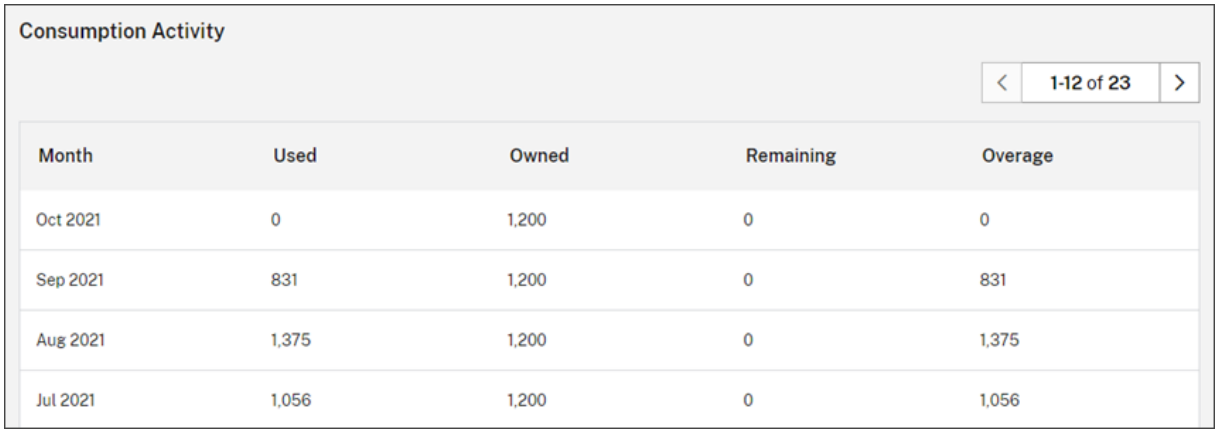
Wählen Sie **Laufzeitverbrauch** aus, um Ihren Laufzeitverbrauch für jeden Monat des Vorjahres anzuzeigen.



Wenn Sie sowohl monatliche als auch jährliche Verbrauchseinheiten gekauft haben, wählen Sie ganz rechts im Diagramm **Diagramme vergleichen** aus, um die Trends für den Monats- und den Laufzeitverbrauch in einer einzigen Ansicht anzuzeigen.



Im Abschnitt **Verwendungsaktivität** wird außerdem eine Liste Ihrer Verbrauchseinheiten für jeden Monat angezeigt.



Month	Used	Owned	Remaining	Overage
Oct 2021	0	1,200	0	0
Sep 2021	831	1,200	0	831
Aug 2021	1,375	1,200	0	1,375
Jul 2021	1,056	1,200	0	1,056

Die Liste “Verwendungsaktivität”umfasst die folgenden Informationen:

- **Verwendet:** Anzahl der Einheiten, die in jedem Monat verwendet wurden.
- **Besitz:** Gesamtzahl der gekauften Einheiten für jeden Monat.

- **Verbleibend:** Anzahl der gekauften Einheiten, die im betreffenden Monat nicht verwendet wurden.
- **Überschreitung:** Anzahl der verbrauchten Einheiten über Ihre gekauften Einheiten im Monat hinaus.

Freigeben zugewiesener Lizenzen

Der Zeitpunkt, zu dem Lizenzzuweisungen zur Freigabe berechtigt sind, hängt von den Consumption Fund-Einheiten ab, die Sie gekauft haben.

Sie können inaktive Lizenzen nach 30 Tagen freigeben, wenn folgende Bedingungen erfüllt sind:

- Sie verwenden kein Citrix Managed Azure-Abonnement mit Ihrer Servicebereitstellung.
- Sie haben jährliche Verbrauchseinheiten gekauft, um sie für Ihre Servicebereitstellung zu verwenden.

Sofern keine Benutzer oder Geräte Apps oder Desktops gestartet haben, können Sie im laufenden Monat inaktive Lizenzen freigeben, wenn folgende Bedingungen erfüllt sind:

- Sie haben monatliche Consumption Fund-Einheiten gekauft, um sie für Ihre Servicebereitstellung zu verwenden.
- Sie haben sowohl monatliche als auch jährliche Consumption Fund-Einheiten gekauft.

Anweisungen zur Freigabe berechtigter Lizenzen finden Sie in den folgenden Artikeln:

- Citrix DaaS (Benutzer-/Gerätelizenzmodell): Freigeben zugewiesener Lizenzen
- Citrix DaaS Standard für Azure: Freigeben zugewiesener Lizenzen

Überwachen von Lizenzen und Lizenznutzung für on-premises Bereitstellungen

September 28, 2023

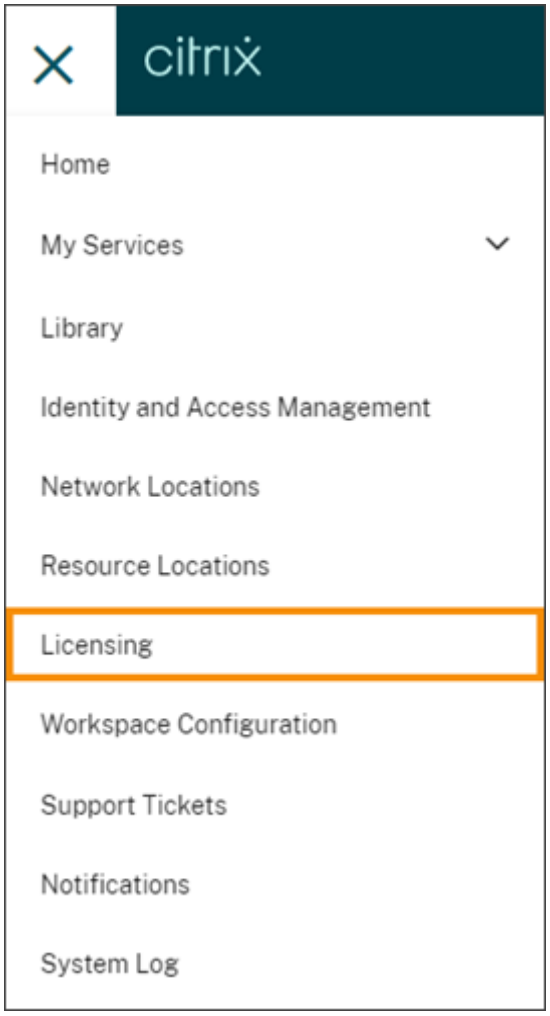
Citrix Cloud bietet folgende Funktionen für lizenzierte Bereitstellungen:

- Produktregistrierung: Registrieren Sie vorhandene Citrix Lizenzserver bei Citrix Cloud, um zusätzliche Nutzungsstatistiken und Berichte zu Ihren Bereitstellungen zu erhalten.
- Lizenzserverstatus: Überprüfen Sie anhand des Citrix Lizenzserverstatus, auf welchen Servern Berichte zur Lizenznutzung erstellt und wann der letzte Bericht an Citrix Cloud übermittelt wurde.
- Nutzungsstatistiken: Zeigen Sie an, wie viele Lizenzen auf Ihren Citrix Lizenzservern installiert und genutzt werden, und erfassen Sie Nutzungstrends anhand historischer Daten.

Unterstützte Produkte

Citrix Lizenzserver-Nutzungsstatistiken sind für alle Editionen von Virtual Apps and Desktops im Rahmen der CCU- und Benutzer-/Gerätelizenzmodelle verfügbar.

Um Citrix Lizenzserver-Nutzungsstatistiken aufzurufen, wählen Sie **Lizenzierung** im Konsolenmenü und dann **Lizenzierte Bereitstellungen**.



Voraussetzungen

Zur Verwendung von Citrix Lizenzserver-Nutzungsstatistiken benötigen Sie die Folgendes:

- Einen Citrix Lizenzserver ab Version 11.15.0.0
- Ein Citrix Cloud-Konto
- Netzwerkzugriff von Citrix Lizenzserver auf Citrix Cloud

Konnektivitätsanforderungen

Um Ihren Lizenzserver bei Citrix Cloud zu registrieren, müssen die folgenden Adressen erreichbar sein:

- `https://citrix.cloud.com/` (für den Zugriff auf die Administratorkonsole, um den Code einzugeben und den Lizenzserverstatus anzuzeigen)
- `https://trust.citrixnetworkapi.net` (zum Abrufen eines Codes)
- `https://trust.citrixworkspacesapi.net/` (zur Bestätigung, dass der Lizenzserver registriert ist)
- `https://cis.citrix.com` (für den Datenupload)
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

Verbindung mit Citrix Cloud herstellen

Um Nutzungsstatistiken für Citrix Lizenzserver zu aktivieren, sind folgende Schritte erforderlich:

1. Aktivieren Sie Nutzungsstatistiken für Ihre Lizenzserver mithilfe der License Manager-Konsole. Weitere Informationen finden Sie in der Produktdokumentation zur Lizenzierung unter Teilen von Nutzungsstatistiken.
2. Lesen Sie den Abschnitt zu Konnektivitätsanforderungen in diesem Artikel und stellen Sie sicher, dass die Adressen erreichbar sind. Wenn Sie einen Proxyserver mit Citrix Lizenzserver verwenden, muss der Proxyserver so konfiguriert sein, wie unter Schritt 5: Konfigurieren eines Proxyservers in der Produktdokumentation zur Lizenzierung beschrieben.
3. Registrieren Sie Ihren Lizenzserver bei Citrix Cloud, wie unter Registrieren von On-Premises-Produkten bei Citrix Cloud beschrieben.

Anzeige der on-premises genutzten Produktlizenzen

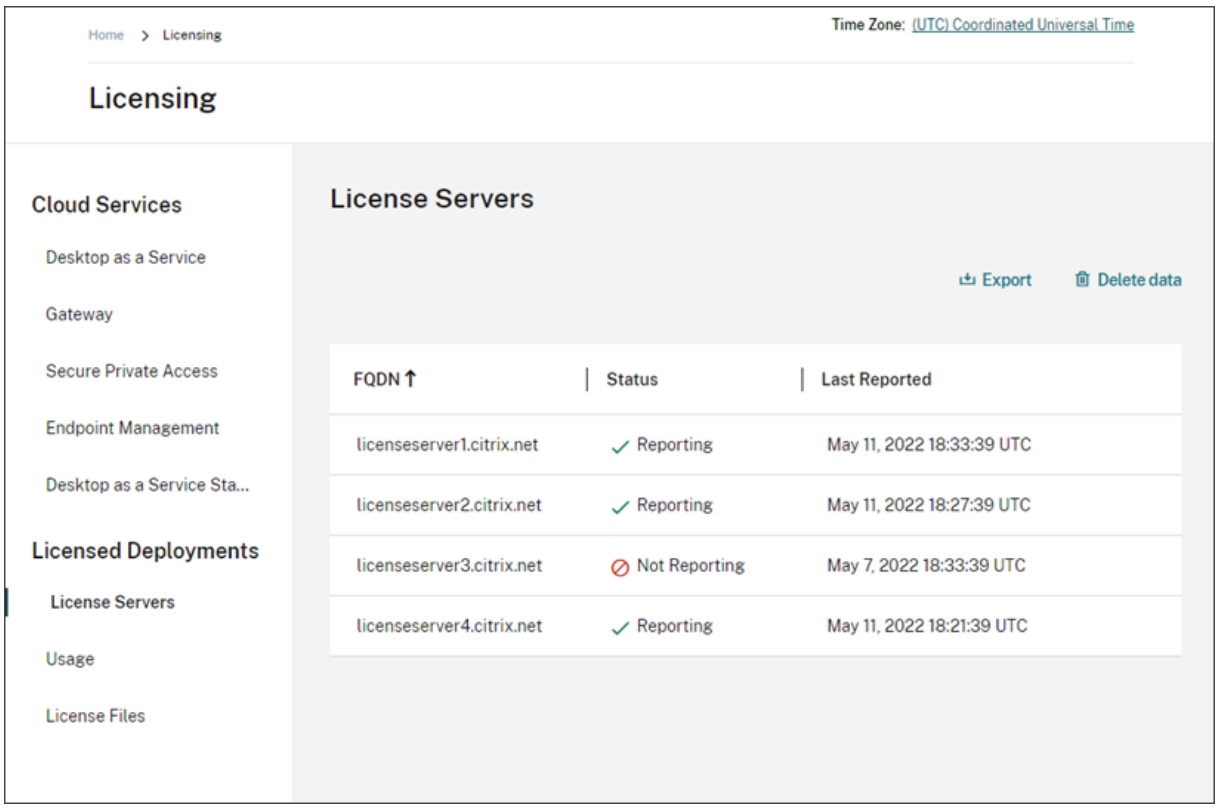
Citrix Lizenzserver-Nutzungsstatistiken geben Einblick in die Lizenznutzung Ihres gesamten Citrix-Bestands. Nutzungsberichte bieten folgende Möglichkeiten:

- Bestimmen Sie, wie viele Lizenzserver bereitgestellt und registriert sind und ob sie Nutzungsdaten an Citrix Cloud melden.
- Zeigen Sie genutzte CCU- und Benutzer-/Gerätelizenzen für Virtual Apps and Desktops an.

- Ermitteln Sie die aggregierte Nutzung von CCU- und Benutzer-/Gerätelizenzen über mehrere Bereitstellungen hinweg.
- Erstellen Sie Nutzungstrends anhand historischer und monatlicher Daten zur Lizenznutzung.
- Prüfen Sie die letzte Anmeldezeit einzelner Benutzer.
- Vergleichen Sie die Anzahl installierter Lizenzen mit den verwendeten Lizenzen auf allen Citrix Lizenzservern.
- Überwachen Sie Lizenzüberziehungen.
- Zeigen Sie aufgeschlüsselte Daten zur Nutzung von CCU- und Benutzer-/Gerätelizenzen an.

Anzeige des Lizenzserverstatus

Die Lizenzserverstatusansicht enthält jeden Lizenzserver, der Berichte zur Lizenznutzung an Citrix Cloud übermittelt.



Lizenzserver mit dem Status “Berichterstellung”haben innerhalb der letzten drei Tage Nutzungsdaten an Citrix Cloud gesendet. Lizenzserver mit dem Status “Keine Berichterstellung”haben zwar innerhalb der vergangenen 30 Tage Nutzungsdaten gesendet, jedoch nicht in den letzten drei Tagen. Lizenzserver, die keinen Nutzungsbericht innerhalb der vergangenen 30 Tage gesendet haben, werden aus der Liste entfernt.

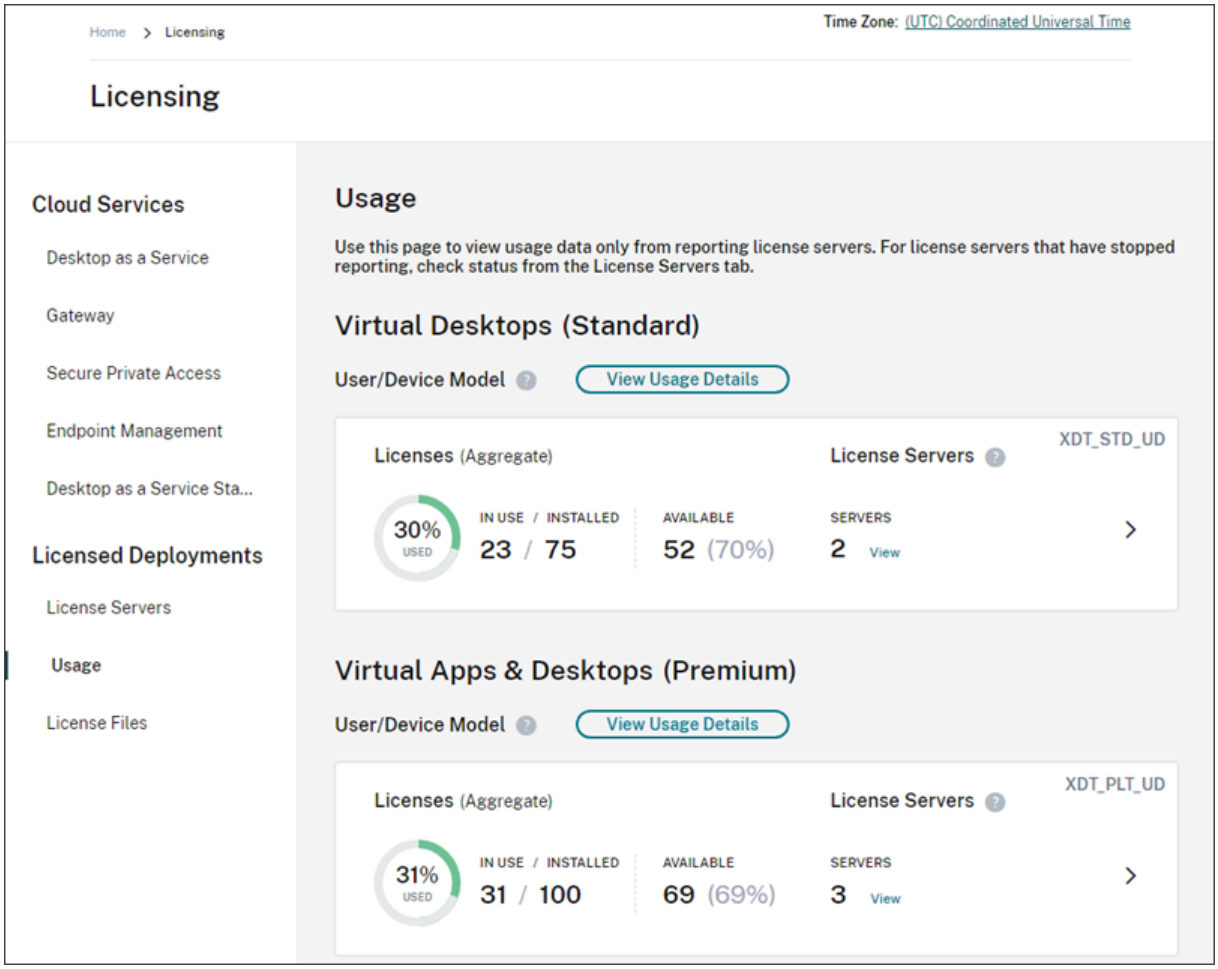
Einfluss des Lizenzserverstatus auf die Lizenznutzungsansichten

Berichterstellungsstatus und Datum des letzten Berichts legen fest, ob die Nutzungsdaten eines Lizenzservers in Berichte und Nutzungsstatistiken einfließen.

- Die Angaben zu aktuell installierten und verwendeten Lizenzen basieren ausschließlich auf den Daten von Lizenzservern mit aktivierter Berichtsfunktion. Wenn für einen Lizenzserver "Keine Berichterstellung"angezeigt wird, werden installierte und verwendete Lizenzen dieses Lizenzservers nicht in den Nutzungsstatistiken erfasst.
- Das Datum unter "Letzter Bericht"zeigt für jeden Lizenzserver, wie aktuell die Lizenznutzungsdaten in den Nutzungsstatistiken sind. Die angezeigten Lizenznutzungsberichte umfassen nur Daten bis zum Datum des letzten Berichts für jeden Lizenzserver.
- Citrix Lizenzserver, die Nutzungsstatistiken erfassen und bei Citrix Cloud registriert sind, werden einmal täglich aktualisiert. Bei Bedarf können Sie ein Update über die Verwaltungskonsole des Citrix Lizenzmanagers auf dem Lizenzserver erzwingen.

Lizenznutzung

Die Registerkarte "Nutzung"bietet eine konsolidierte Ansicht der Lizenznutzung in Ihren Citrix Bereitstellungen. Die Lizenzdaten aller Lizenzserver mit aktivierter Berichtsfunktion werden in einer Ansicht zusammengefasst. Dadurch erhalten Sie ein vollständiges Bild über mehrere Bereitstellungen und Lizenzserver hinweg.

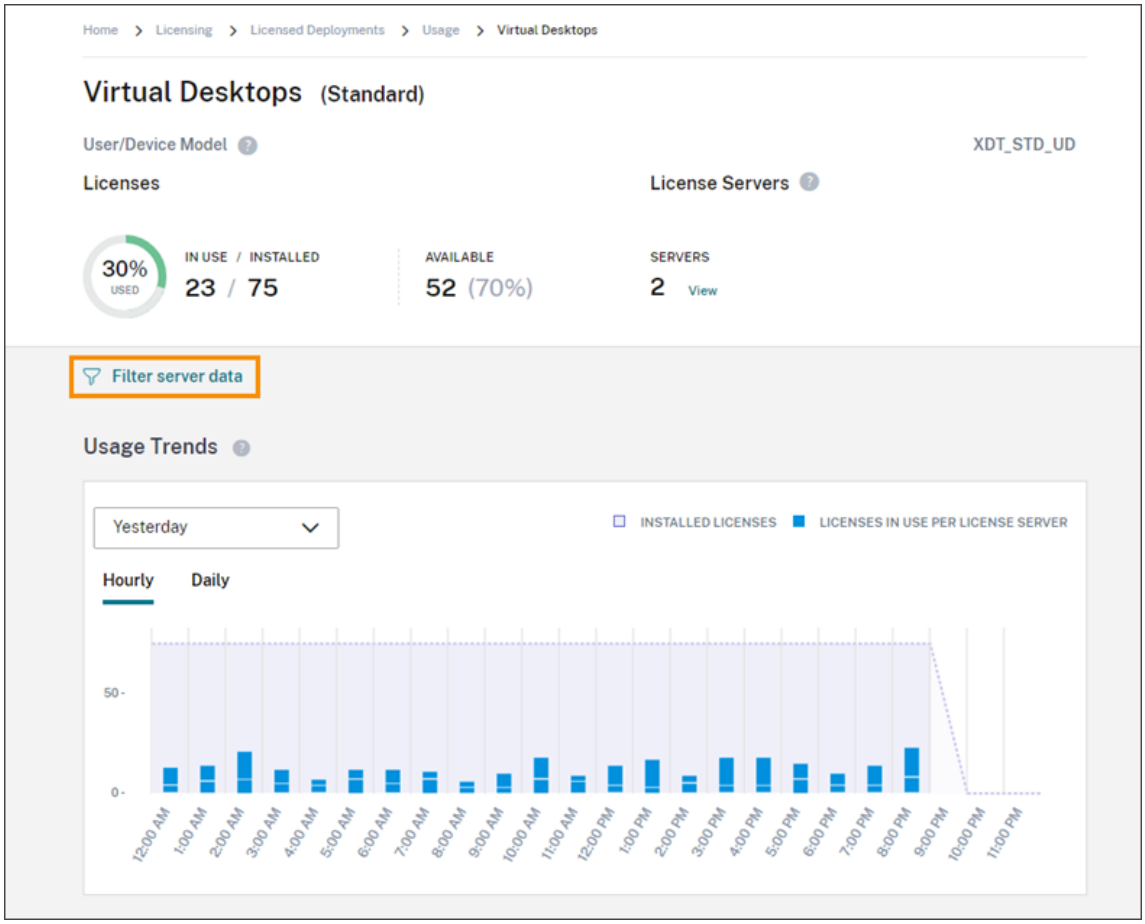


Die Lizenznutzung wird für mehrere Lizenzserver organisiert und zusammengefasst und nach Produktedition und Lizenzmodell unterteilt. Eine Übersichtskarte zur Lizenznutzung wird für jede Lizenzedition angezeigt, die auf den Lizenzservern mit aktivierter Berichtsfunktion gefunden wird. Eine Übersichtskarte wird für jede erkannte Produktedition angezeigt.

Verwendung pro Lizenzserver

Um die Produktlizenznutzung für jeden Lizenzserver anzuzeigen, können Sie die Serverdaten filtern.

1. Wählen Sie auf der Seite **Nutzung** die Option **Nutzungsdetails anzeigen** für das Produkt, das Sie verwalten möchten.
2. Klicken Sie auf **Serverdaten filtern** und wählen Sie die Lizenzserver aus, für die Sie die Nutzung anzeigen möchten. Standardmäßig sind alle Lizenzserver ausgewählt.



3. Wählen Sie **Übernehmen**.

Nachdem Sie den Filter angewendet haben, zeigt Citrix Cloud die Nutzungstrends, die Lizenzserver-Aufschlüsselung und die Lizenzaktivität für die ausgewählten Server an.

Spitzennutzung von CCU-Lizenzen

Die Berichterstellung für CCU-Lizenzen basiert auf folgenden Datenpunkten:

- Installierte Lizenzen: Die Anzahl der auf jedem Lizenzserver installierten Lizenzen.
- Spitzennutzung Lizenzen: Die höchste Anzahl von Lizenzen, die in einem bestimmten Zeitraum verwendet wurden.

Bei der Berechnung der Spitzennutzung für Lizenzen erfasst Citrix Cloud die höchste Anzahl verwendeter Lizenzen für folgende Zeiträume:

- Letzten 7 Tage: Die höchste Anzahl von Lizenzen, die in den letzten sieben Tagen gleichzeitig verwendet wurden.
- In diesem Monat: Die höchste Anzahl von Lizenzen, die im aktuellen Kalendermonat gleichzeitig verwendet wurden.

- Gesamte Zeit: Die höchste Anzahl von Lizenzen, die seit der Registrierung des Lizenzservers bei Citrix Cloud gleichzeitig verwendet wurden.

> **Wichtig:**
>
> Die Daten für diese Zeiträume stimmen möglicherweise nicht mit der Anzahl der auf dem Lizenzserver verwendeten Lizenzen überein. Der Lizenzserver meldet nur die Anzahl der zu einem bestimmten Zeitpunkt verwendeten Lizenzen. Citrix Cloud empfängt diese einzelnen Datenpunkte und berechnet den Spitzenwert für diese Zeiträume.

Überlegungen zur Auswertung der Lizenznutzung

Die Citrix-Lizenzierung unterstützt viele Nutzungsszenarios und enthält detaillierte Informationen. Berücksichtigen Sie Folgendes bei der Nutzungsüberwachung:

- Die Nutzungsdaten basieren auf allen Lizenzen, die auf den Lizenzservern mit aktivierter Berichtsfunktion installiert sind. Wenn auf einem Lizenzserver keine Lizenzen mehr verfügbar sind, können Sie ihm zusätzliche Lizenzen zuweisen, um die Anzahl der verfügbaren Lizenzen zu erhöhen.
- Die Angaben in den Citrix Lizenzserver-Nutzungsstatistiken basieren nur auf Informationen, die von registrierten Citrix Lizenzservern mit aktivierter Berichtsfunktion erfasst und gemeldet werden. Die lizenzierten Bereitstellungen entsprechen nicht immer der Gesamtzahl aller Lizenzen, die Sie tatsächlich besitzen oder erworben haben.
- Der Prozentsatz der verfügbaren Lizenzen berechnet sich aus der Anzahl der genutzten Lizenzen im Verhältnis zu den Lizenzen, die auf den Lizenzservern mit Berichtsfunktion installiert sind.

Aufheben der Lizenzserverregistrierung

Führen Sie folgende Schritte aus, um die Lizenzserverregistrierung vollständig aus Citrix Cloud zu entfernen:

1. Entfernen Sie den registrierten Lizenzserver aus Citrix Cloud mit der Citrix Licensing Manager-Konsole. Vollständige Anweisungen finden Sie unter Lizenzserverregistrierung aufheben.
2. Entfernen Sie alle Nutzungsdaten, die zuvor erfasst wurden.
3. Stellen Sie sicher, dass der Lizenzserver nicht mehr in Citrix Cloud auf der Seite “Produktregistrierungen”angezeigt wird. Wenn der Lizenzserver weiterhin in der Liste angezeigt wird, entfernen Sie ihn gemäß der Schrittfolge unter Entfernen einer Produktregistrierung.

Entfernen von Nutzungsdaten

Wenn Sie einen registrierten Lizenzserver aus Citrix Cloud entfernen, verbleiben die gesammelten Nutzungsdaten im Speicher. Wenn Sie diese Daten nicht mehr behalten möchten, können Sie sie löschen.

> **Wichtig:**
>
> Das Löschen von Nutzungsdaten ist dauerhaft und kann nicht rückgängig gemacht werden. Wenn Sie Nutzungsdaten löschen, die Registrierung für Ihren Lizenzserver jedoch nicht entfernen, sammelt Citrix Cloud weiterhin Nutzungsdaten.

1. Wählen Sie im Citrix Cloud-Menü **Lizenzierung**.
2. Wählen Sie auf der Registerkarte **Lizenzserver** die Option **Daten löschen**.
3. Wenn Sie dazu aufgefordert werden, aktivieren Sie die Kontrollkästchen zur Bestätigung, dass Sie die Auswirkungen der Löschung kennen.
4. Wählen Sie **Serverdaten löschen**.

Lizenzierung für Citrix Service Provider

July 2, 2024

License Usage Insights ist ein kostenloser Cloudservice in Citrix Cloud, mit dem **Citrix Service Provider (CSP)** Produktlizenzen und Lizenznutzung analysieren und entsprechende Berichte erstellen können. Nur CSP-Partner haben Zugriff auf License Usage Insights.

> **Hinweis:**
>
> Citrix DaaS war früher Citrix Virtual Apps and Desktops Service. Citrix DaaS Standard für Azure war früher Citrix Virtual Apps and Desktops Standard für Azure. Einige Anzeigen enthalten evtl. den alten Namen.

Der License Usage Insights Service bietet folgende Funktionen:

- Automatische Sammlung und Aggregation von Produktnutzungsinformationen auf den Citrix Lizenzservern
- Automatische Aggregation von Nutzung und Verbrauch von Cloudlizenzen für Einzel- und Mehrmandantenkunden
- Anzeige der Benutzer, die jeden Monat auf Virtual Apps and Desktops-Bereitstellungen zugreifen
- Erstellen einer Kundenaufschlüsselung der Lizenznutzung
- Optimierung der Lizenzkosten durch Ermittlung und Rückverfolgung einer Liste kostenloser Benutzer

- Anzeige und Analyse historischer Nutzungsdaten mit Citrix
- Export von Virtual Apps and Desktops- sowie Citrix DaaS-Lizenznutzungsdaten, NetScaler VPX-Zuweisungsdaten sowie Lizenz- und Verbrauchsdaten für Citrix DaaS Standard für Azure im CSV-Format

Weitere Informationen

Weitere Hinweise zu Anforderungen und Setup finden Sie unter Erste Schritte mit License Usage Insights.

Eine aggregierte Nutzungsübersicht für Einzelmandatenkunden und Mehrmandantenpartner sehen Sie unter Cloudservice-Lizenznutzung und Berichterstellung für Citrix Service Provider.

Eine Nutzungsübersicht unterstützter Services für Kunden mittels Lizenzierungskonsole finden Sie in den folgenden Artikeln:

- Überwachen von Kundenlizenzen und -nutzung für Citrix DaaS
- Überwachen von Kundenlizenzen und -nutzung für Citrix DaaS Standard für Azure

Erste Schritte mit License Usage Insights

July 2, 2024

Unterstützte Citrix Produkte

Der License Usage Insights-Service stellt Nutzungsinformationen für die folgenden Citrix Produkte bereit:

- Virtual Apps and Desktops (on-premises) –Produktnutzung
- Citrix DaaS Premium (früher Virtual Apps Premium und Virtual Apps and Desktops Premium Services)
- Citrix DaaS Standard für Azure (früher Citrix Virtual Apps and Desktops Standard für Azure)
- NetScaler Console VPX-Zuweisungen

Anforderungen

Zum Erfassen von Lizenz- und Nutzungsinformationen für Citrix On-premises-Produkte ist Citrix Lizenzserver 11.16.3.0 oder höher erforderlich. Nur Windows-und VPX-basierte Lizenzserver werden unterstützt.

Der Citrix Lizenzserver enthält ab Version 11.16.3.0 wichtige Features für Citrix Service Provider-Partner (CSP).

- Optimierte Nutzungserfassung: Neue Features des Lizenzservers optimieren das Lizenzierungsverhalten und die Nachverfolgung zur besseren Unterstützung der CSP.
- Call Home: Der Lizenzserver umfasst ein Call Home-Feature, das die Erfassung der Produktnutzungsdaten für CSP-Partner automatisiert. Diese Features sind exklusiv für CSP-Partner und werden nur aktiviert, wenn eine CSP-Lizenz auf dem Lizenzserver erkannt wird.

Schritt 1: Ausführen eines Updates des Citrix Lizenzservers

Wenn Ihre Lizenzserver älter als Version 11.16.3.0 sind, müssen Sie sie zuerst aktualisieren, bevor Sie License Usage Insights verwenden können. Das direkte Update ist einfach und schnell. Führen Sie die folgenden Schritte aus:

1. Laden Sie die aktuelle Lizenzserverversion herunter. Weitere Informationen zur aktuellen Version von Citrix Lizenzserver finden Sie in der Dokumentation zur Citrix Lizenzierung.
2. Führen Sie ein Upgrade Ihres Lizenzservers durch.
3. Wiederholen Sie diese Schritte für jeden Ihrer Lizenzserver.

Schritt 2: Anmelden bei Citrix Cloud mit My Citrix-Anmeldeinformationen

Bevor Sie sich anmelden, müssen Sie ein Citrix Cloud-Konto beantragen. Folgen Sie den Anweisungen unter Registrieren für Citrix Cloud.

Verwenden Sie bei der Erstellung Ihres Kontos dieselben My Citrix-Anmeldeinformationen, die Sie für die Zuweisung und den Download von Citrix Lizenzen auf citrix.com verwenden. Citrix Cloud sendet eine E-Mail an die mit Ihren My Citrix-Anmeldeinformationen verknüpften Adresse, um das Konto zu bestätigen.

Wenn Ihr Citrix Cloud-Konto einsatzbereit ist, melden Sie sich unter https://citrix.cloud.com mit Ihrer E-Mail-Adresse und Ihrem Kennwort an.

Schritt 3 (optional): Anonymisieren der Benutzernamen über den Lizenzserver

Standardmäßig werden mit Virtual Apps and Desktops- oder Citrix DaaS-Lizenzverbrauch verknüpfte Benutzernamen per sicheres Phone Home an Citrix gemeldet.

Benutzernamen werden gemeldet, damit CSP-Partner die Vorteile der License Usage Insights-Features und des CSP-Lizenzprogramms, welches kostenlose Benutzer für Test- und Verwaltungszwecke unterstützt, voll ausschöpfen können.

Die Benutzerinformationen beschränken sich auf einen einzelnen benutzer@domäne-Eintrag; es werden keine weiteren personenbezogenen Daten weitergeleitet. Citrix gibt diese Informationen nicht weiter.

Partner, die Vorbehalte gegen das Hochladen von Benutzernamen haben, können die Anonymisierung von Benutzernamen aktivieren. Bei aktiver Anonymisierung werden lesbare Benutzernamen unter Verwendung eines sichereren und irreversiblen Algorithmus vor dem Hochladen in eindeutige Zeichenfolgen umgewandelt.

Die Nutzungsverfolgung durch License Usage Insights erfolgt dann anhand dieser eindeutigen Bezeichner anstelle des Benutzernamens. Auf diese Weise erhalten Citrix Service Provider Einblick in die monatliche Produktnutzung, ohne dass die tatsächlichen Benutzernamen auf der Benutzeroberfläche des Cloud Service angezeigt werden.

Konfigurieren der Anonymisierung von Benutzernamen

1. Öffnen Sie die Konfigurationsdatei auf dem Lizenzserver in einem Texteditor. Normalerweise ist die Konfigurationsdatei in C:\Programme\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseService
2. Fügen Sie im Abschnitt **Configurations** die Einstellung **UsageBasedBillingScramble** hinzu:

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
<EncoreConfiguration>
<SamplingPeriod>15</SamplingPeriod>
<RetentionTime>180</RetentionTime>
<Enabled>true</Enabled>
</EncoreConfiguration>
<SARenewalConfigOptions>Notify</SARenewalConfigOptions>
<UsageBasedBillingScramble>1</UsageBasedBillingScramble>
</Configurations>
<!--NeedCopy-->
```

3. Speichern Sie die Datei.

Schritt 4: Verwenden des License Usage Insights Service

Suchen Sie in der Citrix Cloud-Konsole den License Usage Insights-Service und klicken Sie auf **Verwalten**. Eine Übersicht über die wichtigsten Features des Service finden Sie unter Verwalten von Produktnutzung, Lizenzserver und Benachrichtigungen.

Weitere Details

Berücksichtigen Sie Folgendes bei der Verwendung des Citrix Lizenzservers mit License Usage Insights:

- Es kann bis zu 24 Stunden dauern, bis ein neu aktualisierter Lizenzserver in der License Usage Insights-Verwaltungskonsole angezeigt wird.
- Wenn Nutzungsdaten von einem Lizenzserver hochgeladen werden, werden sie sicher verarbeitet und gespeichert, sodass License Usage Insights zu einem späteren Zeitpunkt darauf zugreifen kann. Dies kann bis zu 24 Stunden dauern.
- Standardmäßig werden mit Virtual Apps and Desktops- oder Citrix DaaS-Lizenzverbrauch verknüpfte Benutzernamen per sicheres Phone Home an Citrix gemeldet.
- Benutzernamen werden gemeldet, damit CSP-Partner die Vorteile der License Usage Insights-Features und des CSP-Lizenzprogramms, welches kostenlose Benutzer für Test- und Verwaltungszwecke unterstützt, voll ausschöpfen können.
- Die Benutzerinformationen beschränken sich auf einen einzelnen benutzer@domäne-Eintrag; es werden keine weiteren personenbezogenen Daten weitergeleitet. Citrix gibt diese Informationen unter keinen Umständen weiter.

Hilfe und Support

Wenn Sie Unterstützung für License Usage Insights benötigen, erstellen Sie im Portal My Support ein Supportticket. Zugriff auf "My Support"von Citrix Cloud:

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf das **Hilfesymbol** rechts oben im Bildschirm.
3. Wählen Sie **Ticket erstellen**.
4. Wählen Sie **Zu My Support** und melden Sie sich mit Ihren My Citrix-Anmeldeinformationen an.
5. Füllen Sie das Formular aus und senden Sie es ab.

Ein Mitarbeiter des technischen Supports von Citrix wird Ihnen helfen.

Häufig gestellte Fragen

- **Welche Informationen werden verschickt? Kann ich die Informationen, die meine Lizenzserver an Citrix senden, anzeigen?** Ja, Sie können eine Kopie der Informationen anzeigen, die an Citrix geschickt werden. Weitere Informationen finden Sie unter In Uploads enthaltene Lizenzserverinformationen.
- **Steht License Usage Insights auch Citrix Kunden oder Partnern zur Verfügung, die keine Citrix Service Provider sind?** Nein. License Usage Insights steht nur für Citrix Service Provider mit laufendem Partnervertrag zur Verfügung.
- **Kann ich "Call Home"auf dem Lizenzserver deaktivieren?** Nein. Gemäß Citrix Service Provider-Lizenzvereinbarung müssen alle Lizenzserver die Produktnutzungsdaten an Citrix übertragen. Bestehen Vorbehalte bezüglich der Übertragung, kann das Feature zur

Anonymisierung des Nutzernamens verwendet werden. Weitere Informationen finden Sie unter Anonymisieren des Benutzernamens über den Lizenzserver.

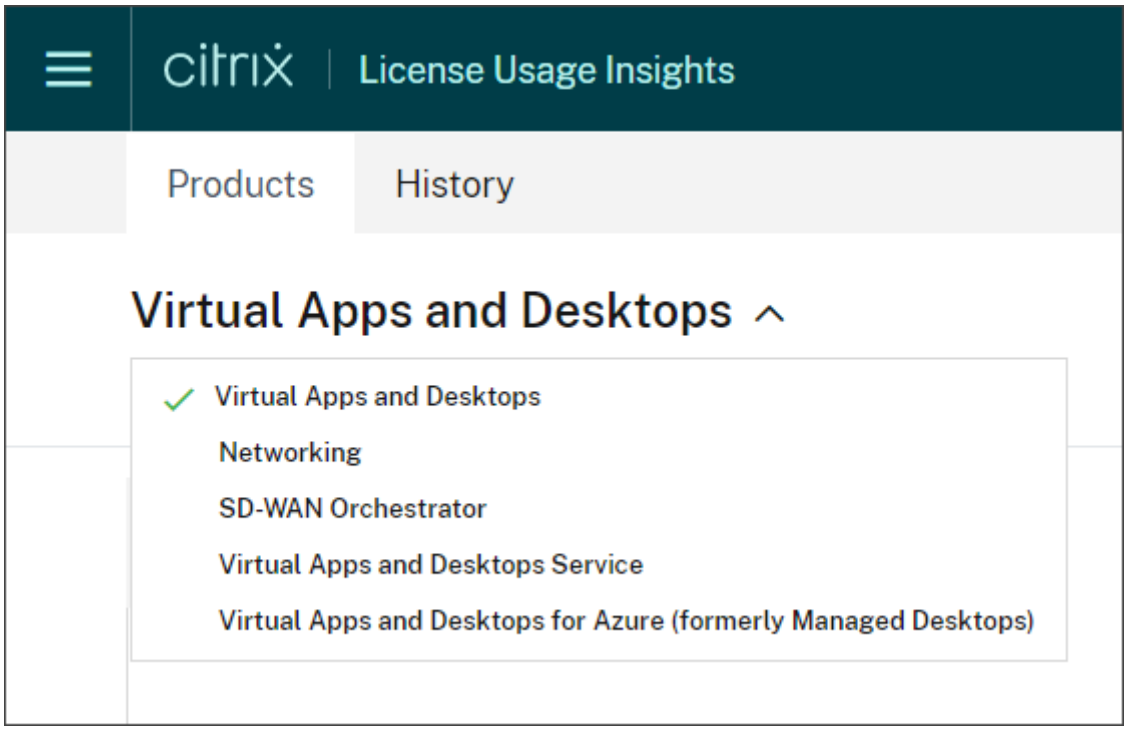
- **Erfolgt die Rechnungsstellung auf der Grundlage der Produktnutzung, die in License Usage Insights angezeigt wird?** Nein. License Usage Insights hilft Partnern bei der Rückverfolgung der Produktnutzung, sodass sie diese schnell und präzise an ihren Citrix Vertragshändler melden können. Die Rechnungsstellung erfolgt weiterhin auf der Grundlage der Daten, die der CSP an seinen Citrix Vertragshändler meldet. Citrix Vertragshändler sind weiterhin für die Rechnungsstellung bei CSP-Partnern zuständig.

Produktnutzung, Lizenzserver und Benachrichtigungen verwalten

July 2, 2024

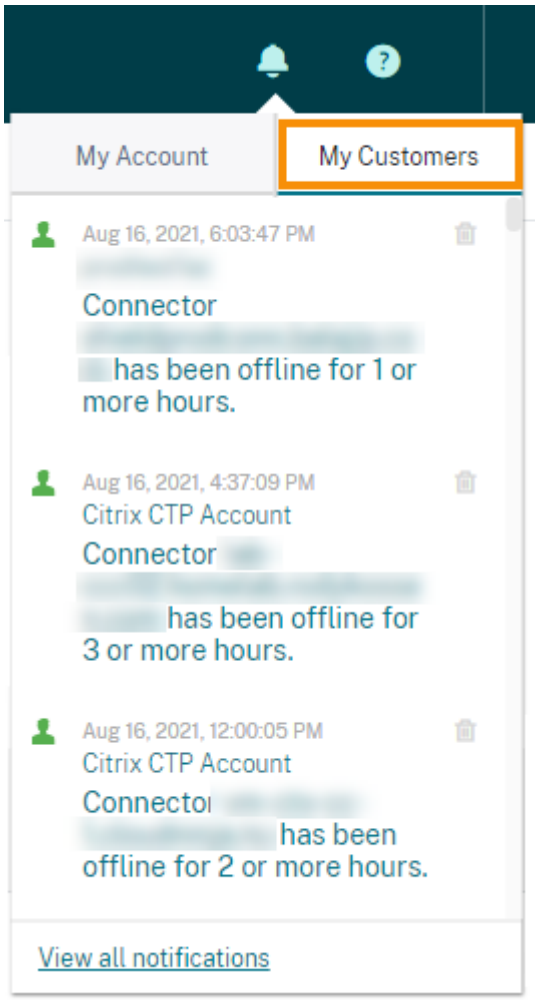
Produktauswahl

Um die Lizenzdetails für ein anderes Produkt anzuzeigen, klicken Sie auf den Pfeil neben dem Produktnamen, und wählen Sie das anzuzeigende Produkt bzw. den Service aus.



Kundenbenachrichtigungen

Überwachen Sie den Lösungsstatus für mehrere Kunden, ohne jede Bereitstellung einzeln aufrufen zu müssen. Der Benachrichtigungsbereich in der Citrix Cloud aggregiert Benachrichtigungen über Kunden in Ihrem Dashboard, sodass Sie sicherstellen können, dass Warnungen behoben und Services weiterhin ausgeführt werden.

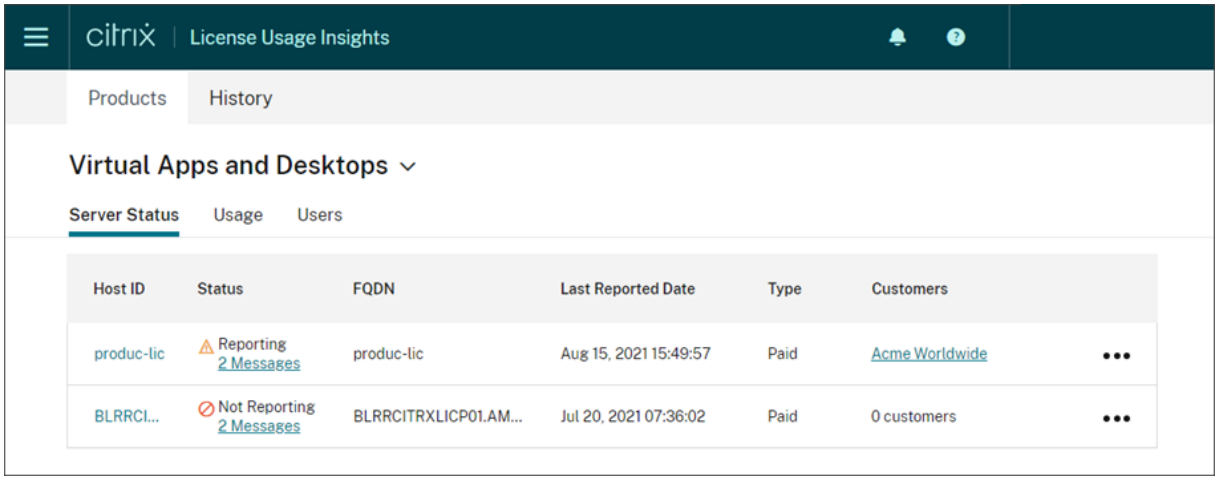


1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf das Symbol **Benachrichtigungen** und anschließend auf **Meine Kunden**. Eine Liste der letzten Benachrichtigungen wird angezeigt.
2. Um eine vollständige Liste der Kundenbenachrichtigungen anzuzeigen, klicken Sie auf **Alle Benachrichtigungen anzeigen**.

Lizenzserverstatus

Zur Erfüllung der Citrix Service Provider-Lizenzrichtlinien müssen alle aktiven Lizenzserver aktualisiert sein und Daten übertragen. Anhand des Lizenzserverstatus können Sie prüfen, welche Lizenzserver Sie haben und ob diese für die Verwendung mit License Usage Insights aktualisiert wurden.

Der Service zeigt unter Verwendung der Lizenzzuweisungsdaten des Citrix Backoffice eine Liste der aktiven Lizenzserver an. Wenn ein Lizenzserver aktualisiert wurde und Daten überträgt, wird für ihn in License Usage Insights die Statusangabe "Berichterstellung"und die Uhrzeit des letzten Datenuploads angezeigt.



In Uploads enthaltene Lizenzserverinformationen

Wenn "Call Home"auf einem Lizenzserver aktiviert ist, werden täglich folgende Informationen hochgeladen:

- Lizenzserverversion
- Lizenzdateiinformationen:
  - Installierte Lizenzdateien
  - Ablaufdatum der Lizenzdateien
  - Informationen zu Berechtigungen auf Features/Editionen
  - Zahl der Lizenzen
- Lizenznutzung:
  - Im laufenden Monat verwendete Lizenzen
  - Mit dem Auschecken von Lizenzen verknüpfte Benutzernamen
  - Aktivierte Produktfeatures und -editionen

Anzeigen des Lizenzserveruploads

CSP-Partner können die zuletzt hochgeladene Nutzlast auf ihrem Lizenzserver einsehen, um zu erfahren, welche Daten der Lizenzserver an Citrix übermittelt. Eine Kopie der Nutzlast wird als ZIP-Datei auf dem Lizenzserver gespeichert. Standardmäßig ist der Speicherort C:\Programme(x86)\Citrix\Licensing\LS\resc

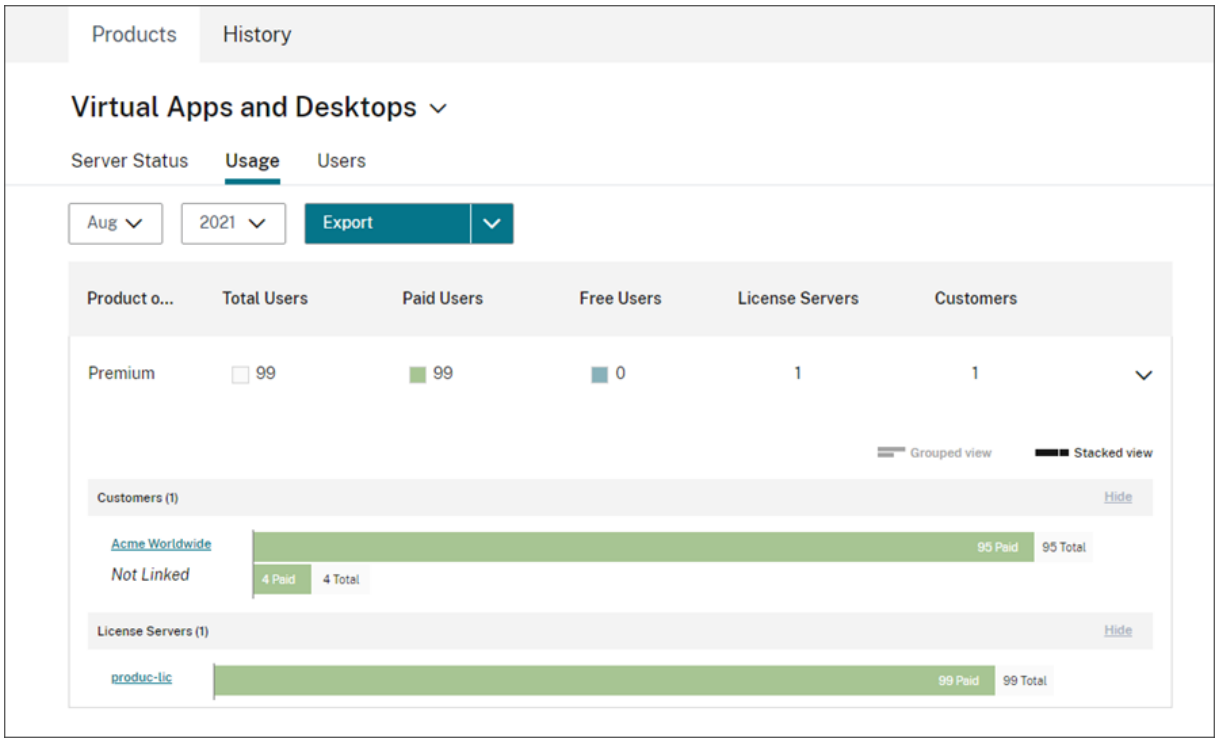
> **Hinweis:**
>
> Erfolgreiche Uploads werden mit Ausnahme des Letzten gelöscht. Fehlgeschlagene Uploads bleiben bis zum nächsten erfolgreichen Upload auf dem Datenträger. Beim nächsten erfolgreichen Upload werden alle bis auf das letzte Upload gelöscht.

Nutzungserfassung

Die Nutzungserfassung ermöglicht die Analyse der Produktnutzung anhand automatisch gesammelter und aggregierter Daten. Es müssen keine zusätzlichen Tools bereitgestellt werden.

License Usage Insights aggregiert automatisch die Produktnutzung für alle Citrix Lizenzserver und bietet so einen vollständigen Überblick über die Nutzung in allen Bereitstellungen. Sie können auch eine Aufschlüsselung der Lizenznutzung erstellen, indem Sie bestimmte Benutzer mit den Kunden oder Mandanten verknüpfen, denen sie angehören.

Die Lizenzserver erfassen und verfolgen die Produktlizenzverwendung und melden diese über den sicheren Phone-Home-Kanal an Citrix. Dieses automatisierte Verfahren liefert konstant aktuelle Nutzungsdaten, die nicht nur Zeit einsparen, sondern auch helfen, Nutzungstrends in Bereitstellungen besser zu erkennen.



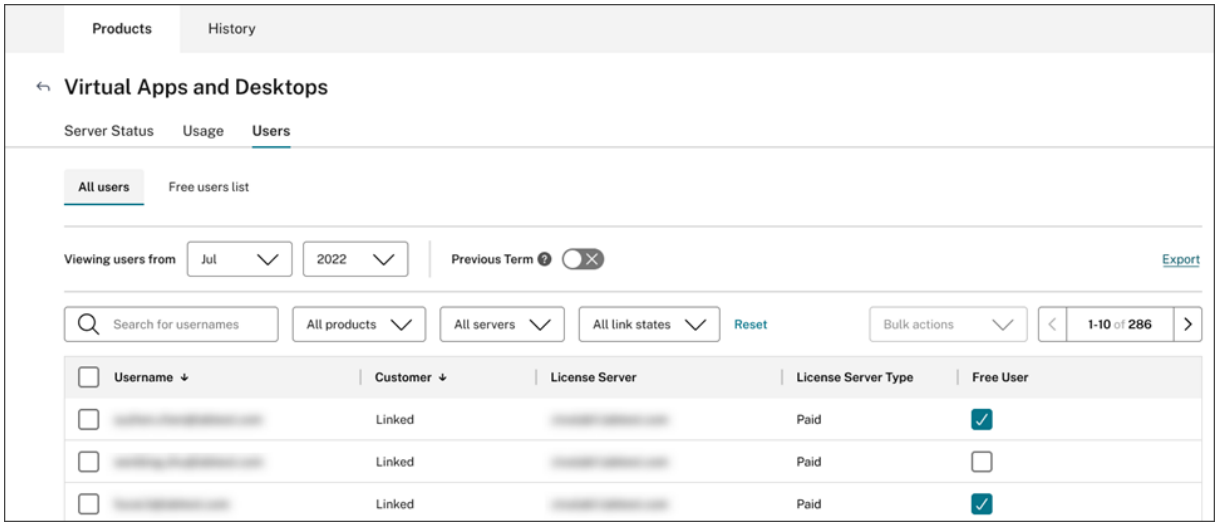
Erstellen einer Kundenaufschlüsselung zur Produktnutzung von Virtual Apps and Desktops

Sie können die Lizenznutzung auch pro Benutzer aufschlüsseln. Hierzu müssen Sie erst Benutzer mit den Kunden oder Mandanten verknüpfen, denen sie angehören. Wenn in Ihrem Kundendashboard keine Kunden definiert sind, können Sie neue Kunden hinzufügen oder eine Verbindung mit vorhandenen Citrix Cloud-Kunden herstellen.

1. Fügen Sie gegebenenfalls Kunden zum Kundendashboard hinzu: Klicken Sie auf der Homepage der Citrix Cloud-Verwaltungskonsole auf **Kunden** und anschließend auf **Hinzufügen oder einladen** und folgen Sie dann den Anweisungen auf dem Bildschirm.
2. Klicken Sie auf die Menüschaltfläche und wählen Sie **Eigene Services > License Usage Insights**.
3. Klicken Sie bei ausgewähltem **Virtual Apps and Desktops**-Produkt auf **Benutzer**.
4. Wählen Sie die Benutzer aus, die Sie verknüpfen möchten, und klicken Sie dann auf **Massenaktionen > Link zum Kunden verwalten**.
5. Wählen Sie den Kunden aus der Liste aus, mit dem Sie die Benutzer verknüpfen möchten.
6. Klicken Sie auf **Speichern**.
7. Um die Aufschlüsselung pro Kunde anzuzeigen, klicken Sie auf die Ansicht **Verwendung**.

Verwalten kostenloser Benutzer

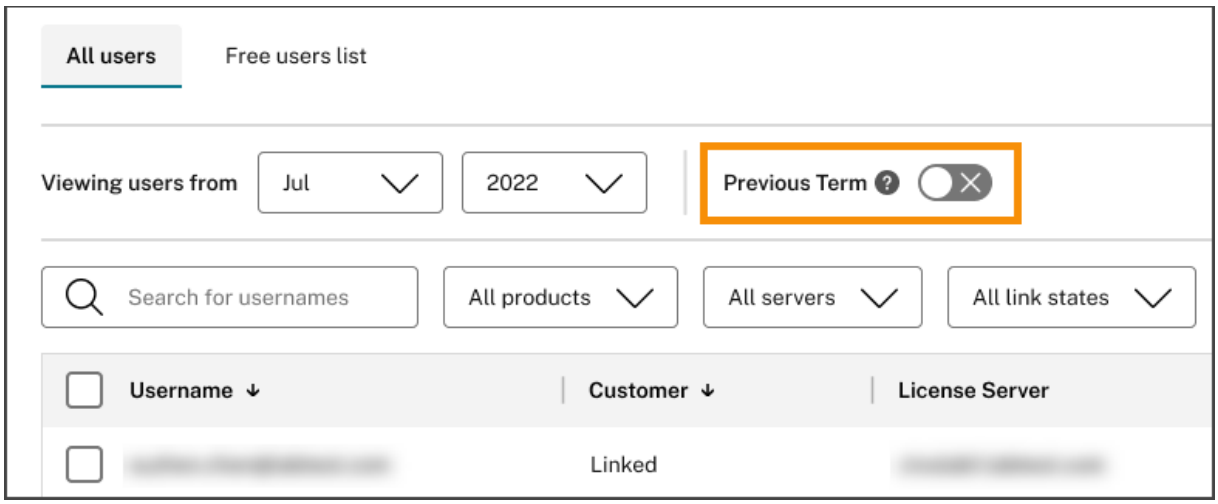
License Usage Insights bietet einen umfassenden Überblick über die Produktnutzung in allen Bereitstellungen und ermöglicht es Ihnen gleichzeitig, die Vorteile des Citrix Service Provider-Lizenzprogramms einschließlich Test- und Administratorkonten voll auszuschöpfen.



Um sicherzustellen, dass Ihnen bezahlte Nutzer in einem bestimmten Abrechnungszyklus angemessen in Rechnung gestellt werden, können Sie bestimmte Benutzer für diesen Zeitraum als kostenlose Benutzer festlegen. Während eines bestimmten Monats in Ihrem aktuellen Abrechnungszyklus können Sie jederzeit, bis zum 10. Tag des Folgemonats kostenlose Benutzer auswählen.

Im März können Sie beispielsweise bis zum 10. April jederzeit kostenlose Benutzer auswählen.

Zwischen dem ersten und dem 10. Tag eines jeden Monats können Sie auch kostenlose Benutzer für den vorherigen Abrechnungszyklus auswählen. Während dieses Zeitraums können Sie die Einstellung **Vorheriger Zeitraum** aktivieren und die kostenlosen Benutzer für diesen Abrechnungszyklus auswählen. Nach dem 10. Tag des Monats zeigt Citrix Cloud die Einstellung **Vorheriger Zeitraum** nicht mehr an.



Die kostenlosen Benutzer, die Sie in einem bestimmten Monat auswählen, werden berücksichtigt, wenn Ihnen kostenpflichtige Benutzer in Rechnung gestellt werden. Wenn Sie einen kostenlosen Benutzer in einen kostenpflichtigen Benutzer ändern, zeichnet Citrix das Datum der Änderung auf und bezieht diesen Benutzer in den Abrechnungszyklus ein, in dem die Änderung stattgefunden hat.

Tagging von Benutzerkunden

Diese Funktion bietet eine Aufschlüsselung der Lizenznutzungsdaten für jeden Kunden, einschließlich Unterstützung für die Verwaltung und Berichterstellung für Einzel- oder Mehrmandantenarchitekturen. Die Objekte von License Usage Insights sind:

- Lizenzserver: ein Lizenzserver auf der Liste, der Berichte erstellt oder nicht.
- Benutzer: ein einzelner Benutzername, der in den Call Home-Nutzungsdaten enthalten ist.
- NetScaler: eine einzelne NetScaler VPX-Lizenzzuweisung (VPX auf der VPX-Liste).

> **Hinweis**
>
> Das Taggingfeature für Kundenbenutzer hat dasselbe Verhalten wie das Taggingfeature für kostenlose Server, bei dem ein CSP das Kundentagging für den aktuellen Abrechnungszeitraum bis zum 10. des Folgemonats aktualisieren kann.

Tagging von kostenlosen Servern

Diese Funktion bietet Flexibilität bei der Verwaltung von Ressourcen in der Citrix Cloud-Umgebung, da Administratoren Server anhand ihrer spezifischen Rollen, Standorte oder anderer relevanter Kriterien organisieren und identifizieren können, ohne sich Gedanken über Lizenzauswirkungen machen zu müssen.

> **Hinweis**
>
> Ein CSP kann das Tagging kostenloser Server oder das Kundentagging ausschließlich für den aktuellen Monat ändern, wobei die Änderungen sowohl für den aktuellen als auch für die kommenden Monate gelten.

Tagging von Serverkunden

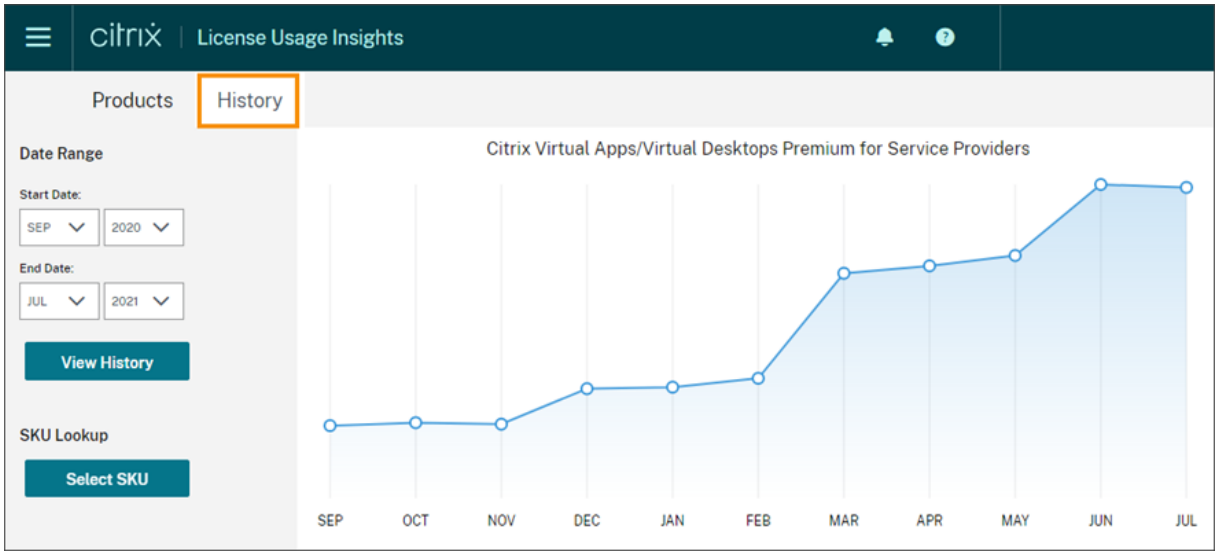
Diese Funktion ermöglicht eine bessere Organisation und Verwaltung von Ressourcen in der Citrix Cloud-Umgebung und stellt sicher, dass die Server gemäß den kundenspezifischen Anforderungen getaggt werden. Durch das Tagging von Serverkunden können Administratoren Ressourcen, die verschiedenen Kunden zugeordnet sind, leicht identifizieren, nachverfolgen und effizienter zuweisen sowie verwalten.

> **Hinweis**
>
> Ein CSP kann das Tagging kostenloser Server oder das Kundentagging ausschließlich für den aktuellen Monat ändern, wobei die Änderungen sowohl für den aktuellen als auch für die kommenden Monate gelten.

Historische Trends

Sie können eine vollständige Aufzeichnung Ihrer bisherigen Geschäfte mit Citrix einsehen. Sie können die Nutzung des letzten Monats, des letzten Jahrs oder für einen anderen, frei konfigurierbaren Zeitraum prüfen.

Historische Ansichten bieten wertvolle Daten für das Geschäft. Als Citrix Service Provider können Sie so schnell nachvollziehen, wie sich Ihr Geschäft mit Citrix entwickelt und welche Produkte bei Ihren Kunden und Abonnenten das stärkste Wachstum verzeichnen.



Exportieren von Verwendungs- und Zuweisungsdaten

Sie können die folgenden Datentypen als CSV-Datei aus License Usage Insights exportieren:

- Virtual Apps and Desktops-Produktverwendung und Benutzerliste für einen bestimmten Monat
- Aktuelle NetScaler VPX-Zuweisungsdetails

1. Wählen Sie **Virtual Apps and Desktops** oder **Networking** aus der Produktliste aus.
2. Wählen Sie ggf. die Ansicht aus, die Sie exportieren möchten. Um beispielsweise Virtual Apps and Desktops-Verwendungsdetails zu exportieren, klicken Sie auf die Ansicht **Verwendung**.
3. Wählen Sie ggf. den Monat oder das Jahr, den oder das Sie exportieren möchten.
4. Klicken Sie rechts auf **Exportieren**.

Zugriff auf Lizenzdaten über APIs

Citrix bietet mehrere APIs, mit denen Sie außerhalb von Citrix Cloud auf Ihre Lizenzdaten zugreifen können. Weitere Informationen zu diesen APIs finden Sie in der Citrix Developer-Dokumentation unter APIs to manage Citrix cloud licensing.

Zur Verwendung der APIs müssen Sie zunächst einen sicheren Client erstellen und einen Bearertoken generieren. Um einen sicheren Client zu erstellen, benötigen Sie die Berechtigung **Sicherer Client** in Citrix Cloud. Weitere Informationen finden Sie unter Konsolenberechtigungen.

Weitere Informationen zu den Aufgaben, die für die Verwendung von Citrix Cloud-APIs erforderlich sind, finden Sie in der Citrix Developer-Dokumentation unter Get started with Citrix Cloud APIs.

API-Zugriff für Vertragshändler

Mit Citrix Cloud-APIs können Sie Ihrem Citrix-Vertragshändler Zugriff auf Ihre Lizenzdaten gewähren, ohne dass er vollen Administratorzugriff auf Ihr Citrix Cloud-Konto erhält. Ihr Vertragshändler kann so Ihre Nutzungsberichte prüfen und eine genaue Abrechnung sicherstellen.

Um Vertragshändlern Zugriff auf Ihre Lizenzdaten zu gewähren, erstellen Sie einen Administrator mit benutzerdefiniertem Zugriff, der nur berechtigt ist, sichere Clients zu erstellen und auf den License Usage Insights Service zuzugreifen. Dieses Konto kann nur auf Citrix Cloud-APIs und nicht auf andere Citrix Cloud-Funktionen zugreifen. Wenn das Konto erstellt ist, können Sie die Kontoanmeldeinformationen mit Ihrem Vertragshändler teilen. Er kann sich dann bei Ihrem Citrix Cloud-Konto anmelden und den sicheren Client erstellen, der für die Verwendung von Citrix Cloud-APIs erforderlich ist. Alternativ können Sie sich als Administrator mit benutzerdefiniertem Zugriff anmelden, den sicheren Client erstellen und dann die Daten zum sicheren Client an Ihren Vertragshändler weitergeben.

Konto mit benutzerdefiniertem Zugriff für Ihren Vertragshändler erstellen:

1. Erstellen Sie ein neues Administratorkonto speziell für Ihren Citrix-Vertragshändler. Anweisungen finden Sie unter Einladen einzelner Administratoren.
2. Wählen Sie unter **Zugriff festlegen** die Option **Benutzerdefinierter Zugriff** und wählen Sie dann die folgenden Berechtigungen:
    - **Allgemein > Secure Client**
    - **License Usage Insights > License Usage Insights: Zugriff für Vertragshändler**

Sicheren Client erstellen:

1. Melden Sie sich bei Citrix Cloud mit den Anmeldeinformationen des neuen Kontos an.
2. Erstellen Sie einen neuen sicheren Client, wie unter Get started with Citrix Cloud APIs beschrieben.
3. Notieren Sie sich die Client-ID und den geheimen Clientschlüssel, die von Citrix Cloud generiert werden. Diese Details sind erforderliche Eingaben für alle Citrix Cloud-APIs.

Verfügbare Lizenzdaten für Vertragshändler

In diesem Abschnitt werden die Lizenzdaten und APIs beschrieben, auf die Ihr Citrix-Vertragshändler mit den von Ihnen bereitgestellten Details zum sicheren Client Zugriff erhält. Verwenden Sie die folgenden Links, um weitere Informationen zu den einzelnen APIs zu erhalten.

CSP-Berichte zur monatlichen und historischen Nutzung von Virtual Apps and Desktops-Lizenzen (License Usage Insights):

- Virtual Apps and Desktops –Aktuelle Nutzung
- Virtual Apps and Desktops –Historische Nutzung

CSP-Berichte zur Nutzung von Einzel- und Mehrmandanten-Cloud-Lizenzen (License Usage Insights):

- DaaS –Aktuelle Nutzung
- DaaS –Historische Nutzung

Cloud-Lizenznutzung durch den CSP (Lizenzierung):

- DaaS –Aktuelle Nutzung
- DaaS –Historische Nutzung

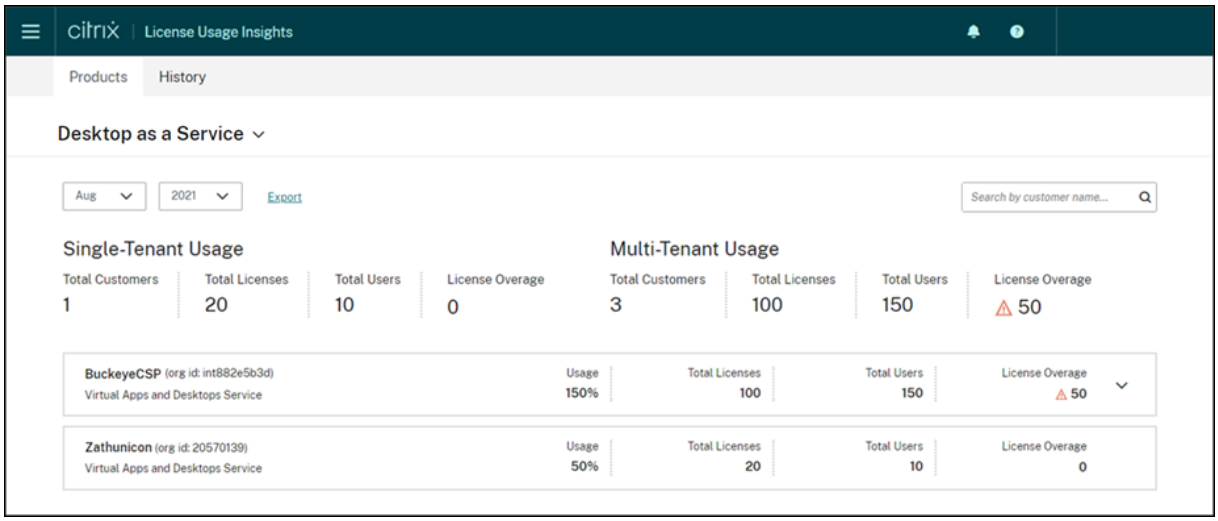
Cloud-Lizenznutzung durch den Mandanten (Kundendashboard -> Lizenzierung anzeigen)

- DaaS –CCU-Lizenzen –Aktuelle Nutzung
- DaaS –CCU-Lizenzen –Historische Nutzung
- DaaS –Benutzer-/Gerätelizenzen –Aktuelle Nutzung
- DaaS –Benutzer-/Gerätelizenzen –Historische Nutzung

Cloudservice-Lizenznutzung und -Berichterstellung für Citrix Service Provider

September 28, 2023

License Usage Insights aggregiert automatisch die Cloudservicenutzung und bietet so einen vollständigen Überblick über alle Einzelmandatenkunden und Mehrmandantenpartner hinweg. Sie können diese Details auch für einen bestimmten Monat in eine CSV-Datei exportieren.



Unterstützte Cloudservices

Einzelmandanten-Lizenznutzung ist für Citrix DaaS Premium (früher Virtual Apps Premium und Virtual Apps and Desktops Premium) verfügbar.

Die Mehrmandanten-Lizenznutzung ist für folgende Services verfügbar:

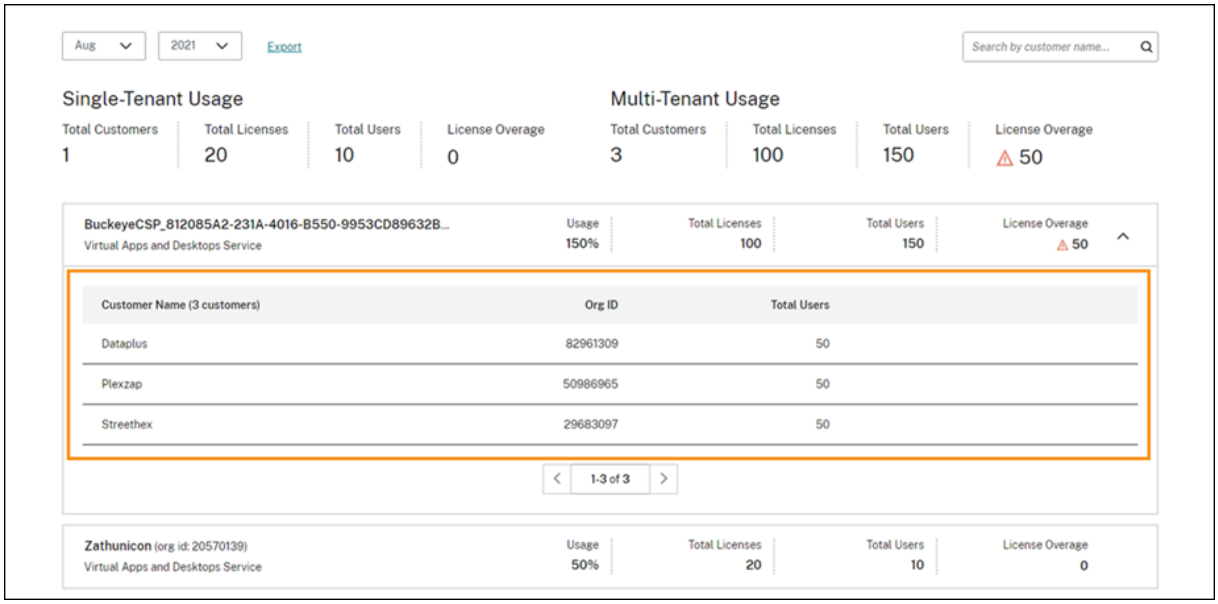
- Citrix DaaS (früher Virtual Apps and Desktops Service)
- Citrix DaaS Standard für Azure (früher Virtual Apps and Desktops Standard für Azure)

Lizenzübersichten

License Usage Insights bietet die folgende Aufschlüsselung der Einzel- und Mehrmandantennutzung für Citrix Service Provider:

- Eine allgemeine Übersicht, unterteilt nach Mandantentyp und mit Angabe der Gesamtwerte für Kunden, erworbene Lizenzen, Benutzer und überschrittene Lizenzen für alle Kunden.
- Eine Übersicht über die Nutzung für jeden Kunden oder Partner, einschließlich des prozentualen Gesamtanteils der verwendeten Lizenzen und mit Gesamtwerten für erworbene Lizenzen, Benutzer und Lizenzüberschreitungen.

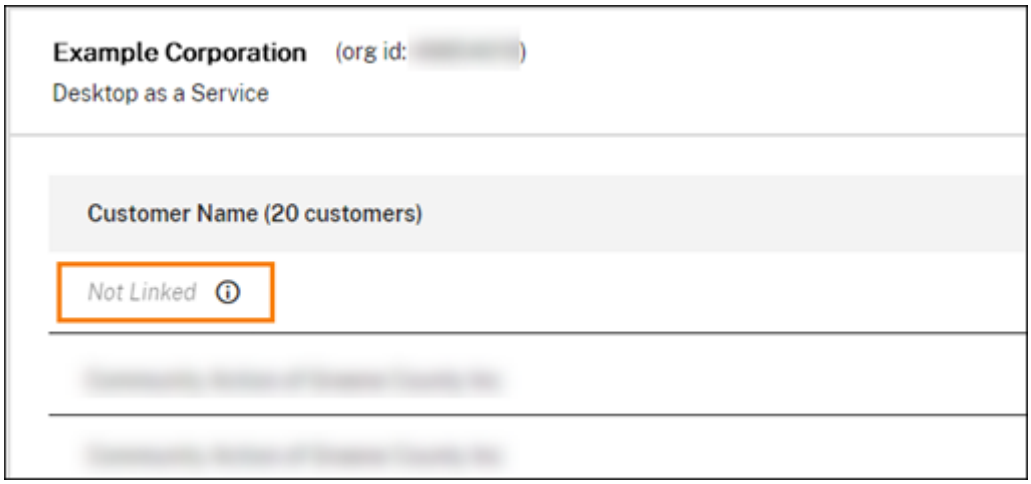
Für Mehrmandantenservices können Sie die Nutzungsübersicht erweitern, um die Kunden, die OrgID und die Anzahl aller Benutzer anzuzeigen, die dem jeweiligen Partner zugeordnet sind.



Mandantenkunden nicht verbunden

Mandantenkunden werden u. U. als "nicht verbunden" aufgeführt. Dieser Status kann eintreten, wenn Benutzer des Mandanten über die Workspace-URL des Citrix Service Providers anstelle der Workspace-

URL des Mandanten auf einen Cloud-Service zugreifen.

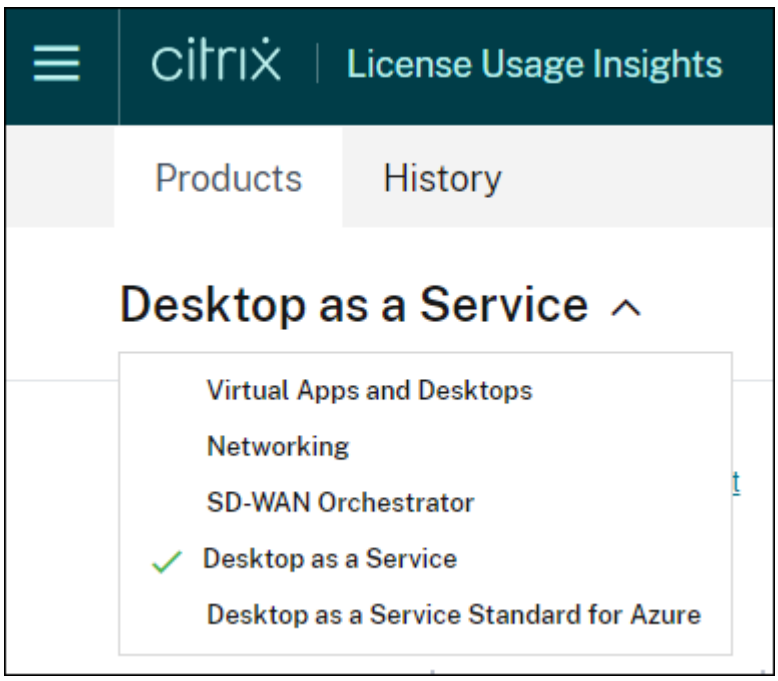


Wenn der Mandantenbenutzer über die Mandanten-Workspace-URL auf den Service zugreift, zählt Citrix Cloud den Benutzer als zum Mandanten gehörig und die Nicht-verbunden-Meldung wird entfernt.

Anzeigen und Exportieren der monatlichen Nutzung

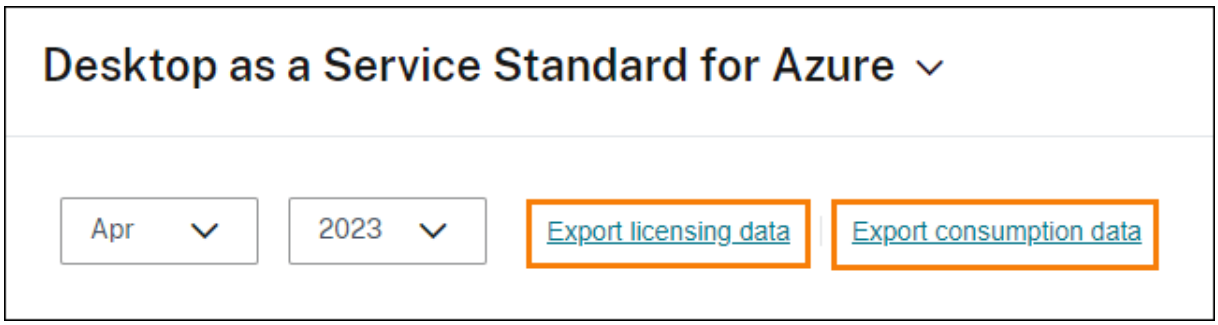
Sie können jederzeit die Lizenznutzung der vergangenen Monate für alle Kunden und Partner anzeigen. Sie können die Daten auch zur weiteren Analyse in eine CSV-Datei exportieren. Für Citrix DaaS Standard für Azure können Sie auch monatliche Verbrauchsdaten exportieren.

1. Wählen Sie im Produktmenü den Cloudservice aus, den Sie anzeigen möchten.



Wählen Sie für Citrix DaaS den gewünschten Monat und das Jahr und wählen Sie **Exportieren** aus.

Wählen Sie für Citrix DaaS Standard für Azure den anzuzeigenden Monat und das Jahr und wählen Sie dann **Lizenzdaten exportieren** oder **Verbrauchsdaten exportieren** aus.

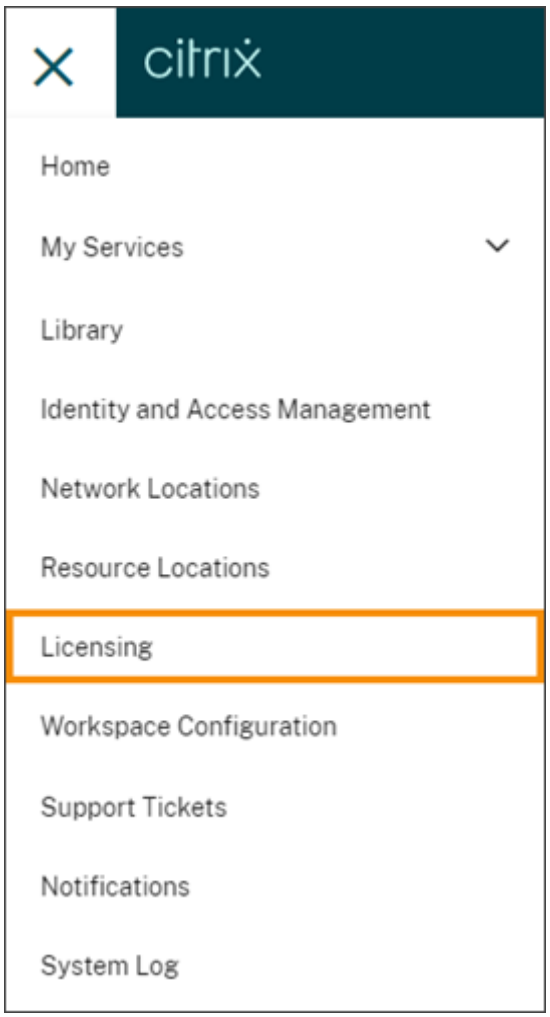


Überwachen von Kundenlizenzen und -nutzung für Citrix DaaS

September 28, 2023

Kunden von **Citrix Service Provider (CSP)** können Citrix DaaS-Lizenzen für ihre Benutzer in Citrix Cloud mühelos überwachen. Als CSP können Sie auf diese Details zugreifen, indem Sie sich bei ihrem Kundenkonto in Citrix Cloud anmelden. Eine aggregierte Übersicht der Lizenznutzung für Einzel- und Mehrmandantenkunden finden Sie unter Cloudservice-Lizenznutzung und -Berichterstellung für Citrix Service Provider.

Kunden können ihre Lizenzdaten durch Auswahl von **Lizenzierung** im Citrix Cloud-Menü anzeigen.



Lizenzzuweisung

Benutzer-/Gerätelizenzmodell: Citrix Cloud weist eine Lizenz zu, wenn ein eindeutiger Kundenbenutzer zum ersten Mal im aktuellen Monat eine App oder einen Desktop startet.

Gleichzeitig-Lizenzmodell: Citrix Cloud weist eine Lizenz zu, wenn ein Benutzer einen Desktop auf dem Gerät startet. Wenn der Benutzer sich abmeldet oder die Verbindung zur Sitzung trennt, ist die Lizenz nicht länger zugewiesen. Da die Lizenzzuweisung davon abhängt, wie viele Geräte aktuell auf Apps oder Desktops zugreifen, erfasst Citrix Cloud alle fünf Minuten die Anzahl verwendeter Lizenzen.

Weitere Informationen zum Gleichzeitig-Lizenzmodell (CCU-Lizenzen) finden Sie unter CCU-Lizenzen in der Produktdokumentation zur Lizenzierung.

Zusammenfassung zur Lizenzierung

Citrix Cloud zeigt Zusammenfassungen der im Rahmen des Benutzer-/Gerätelizenzmodells und Gleichzeitig-Lizenzmodells verwendeten Lizenzen an.

Zusammenfassung für Benutzer und Geräte

Die Benutzer/Gerät-Lizenzübersicht zeigt einen Überblick über die verwendeten Lizenzen im Verhältnis zur Gesamtzahl der Lizenzen, die Sie besitzen.

Wenn sich der Prozentsatz 100 % nähert, wechselt der Prozentsatz von grün zu gelb. Wenn der Prozentsatz 100 % überschreitet, wird der Prozentsatz rot angezeigt.

Citrix Cloud zeigt auch das Verhältnis zugewiesener zu erworbenen Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen.

Zusammenfassung für gleichzeitige Benutzer

Die Gleichzeitig-Lizenzübersicht bietet einen Überblick über die folgenden Informationen:

- Prozentsatz der erworbenen Lizenzen, die verwendet wurden, als die letzte Lizenzprüfung durch Citrix Cloud erfolgte. Citrix Cloud berechnet diesen Prozentsatz alle fünf Minuten basierend auf eindeutigen Geräten mit aktiven Verbindungen zum Dienst. Die Gesamtanzahl an erworbenen Lizenzen umfasst alle erworbenen Lizenzen für Citrix DaaS, die das Gleichzeitig-Lizenzmodell verwenden.
- Das Verhältnis aktuell zugewiesener Lizenzen zur Gesamtanzahl erworbener Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen. Unter **Gesamt** sehen Sie die Gesamtanzahl aller erworbenen Lizenzen (gemäß Zeitpunkt unter "Letzter Bericht").
- Statistiken zu Verwendungsspitzen. Bei der Berechnung von Verwendungsspitzen für Lizenzen erfasst Citrix Cloud die maximale Anzahl verwendeter Lizenzen für folgende Zeiträume:
  - **Letzte 24 Stunden:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen in den letzten 24 Stunden.
  - **In diesem Monat:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen im aktuellen Monat.
  - **Gesamte Zeit:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen seit Beginn des Abonnements.

  Unter **Gesamt** sehen Sie für den jeweiligen Zeitraum, wie viele Lizenzen während der Verwendungsspitze insgesamt im Besitz waren. Wenn die Gesamtzahl der erworbenen Lizenzen ansteigt oder sinkt und sich die Anzahl zugewiesener Lizenzen entsprechend erhöht, ändert

sich auch der Wert unter **Gesamt**. Wenn keine entsprechende Verwendungsspitze auftritt, ändert sich der Wert unter **Gesamt** nicht.

- Statistiken zur aktiven Nutzung. Citrix Cloud zeigt die Gesamtzahl der eindeutigen Verbindungen für die folgenden Zeiträume an:
  - **Monatlich:** Gesamtzahl der Verbindungen im vorherigen Kalendermonat.
  - **Täglich:** Gesamtzahl der Verbindungen der letzten 24 Stunden. Diese Zahlen werden auch als Prozentsätze der Gesamtzahl der Lizenzen im Besitz während dieser Zeiträume dargestellt.

Berechnung von Verwendungsspitzen für Lizenzen

Um das Gleichzeitig-Modell (CCU-Lizenzen) akkurat wiederzugeben, erfasst Citrix Cloud alle fünf Minuten, wie viele eindeutige Geräte gleichzeitig auf den Dienst zugreifen. Liegt die Zahl über der aktuellen Verwendungsspitze, zeigt Citrix Cloud die neue Verwendungsspitze mit Datum und Uhrzeit an. Wenn die Anzahl unter der aktuellen Verwendungsspitze liegt, ändert sich der aktuelle Spitzenwert nicht.

> **Wichtig:**
>
> Wenn Sie die Überwachungsfunktion in Director nutzen, um Informationen zu gleichzeitigen Sitzungen anzuzeigen, müssen Sie beachten, dass gleichzeitige Sitzungen im Überwachungsbericht anders interpretiert werden und verwendete CCU-Lizenzen hier nicht akkurat angegeben sind. Weitere Informationen zu den Unterschieden zwischen Überwachungs- und Lizenzierungsberichten finden Sie unter Häufig gestellte Fragen.

Berechnung der monatlichen aktiven Nutzung

Zu Beginn jedes Monats erstellt Citrix Cloud einen Snapshot des vorherigen Kalendermonats. Citrix Cloud zeigt die Gesamtzahl der eindeutigen Verbindungen an, die in diesem Kalendermonat hergestellt wurden.

Berechnung der täglichen aktiven Nutzung

Jeden Tag zur gleichen Zeit erstellt Citrix Cloud einen Snapshot der letzten 24 Stunden. Citrix Cloud zeigt die Gesamtzahl der eindeutigen Verbindungen an, die in diesem diesem Zeitraum von 24 Stunden hergestellt wurden.

Nutzungstrends

Citrix Cloud zeigt eine Aufschlüsselung der Nutzungstrends für Benutzer/Gerät- oder Gleichzeitig-Lizenzen an. Um diese Aufschlüsselung anzuzeigen, wählen Sie auf der Seite mit der Lizenzübersicht die Option **Nutzungsdetails anzeigen**.

Trends für Benutzer und Geräte

Für Benutzer/Gerät-Lizenzen zeigt der Abschnitt **Nutzungstrends** eine Aufschlüsselung der zugewiesenen Lizenzen als Diagramm.

Wenn Sie auf ein Intervall im Diagramm zeigen, werden die folgenden Informationen angezeigt:

- **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.
- **Zuvor zugewiesen:** die Anzahl der Lizenzen, die im Vormonat zugewiesen wurden. Beispielsweise greift ein Benutzer im Juli das erste Mal auf den Cloudservice zu und ihm wird eine Lizenz zugewiesen. Diese Lizenz gilt für den Monat Juli als "Neu zugewiesen". Für den Monat August wird diese Lizenz als "Zuvor zugewiesen"gezählt.
- **Neu zugewiesen:** Die Anzahl neuer Lizenzen, die pro Monat zugewiesen wurden. Beispielsweise greift ein Benutzer im Juli das erste Mal auf den Cloudservice zu und ihm wird eine Lizenz zugewiesen. Diese Lizenz gilt für den Monat Juli als "Neu zugewiesen".

Trends für Gleichzeitig-Modell

Für das Gleichzeitig-Modell werden im Bereich **Nutzungstrends** folgende Informationen angezeigt:

- **Lizenzen insgesamt:** Gesamtanzahl Ihrer erworbenen CCU-Lizenzen.
- **Spitzennutzung Lizenzen:** Die maximale Anzahl zugewiesener Lizenzen im ausgewählten Zeitraum. Standardmäßig zeigt Citrix Cloud Verwendungsspitzen für jeden Monat im aktuellen Kalenderjahr an. Um monatliche oder stündliche Verwendungsspitzen anzuzeigen, wählen Sie im Dropdownmenü den Kalendermonat oder Kalendertag aus, den Sie untersuchen möchten.

  Wenn der ausgewählte Datumsbereich noch nicht abgeschlossen ist, zeigt Citrix Cloud die aktuelle Verwendungsspitze für das derzeitige Zeitintervall an. Wenn Sie beispielsweise die Details für den aktuellen Kalendertag anzeigen, ist die maximale Anzahl verwendeter Lizenzen für jede Stunde bis zum aktuellen Zeitpunkt zu sehen. Wenn die maximale Anzahl verwendeter Lizenzen im nächsten Fünf-Minuten-Zählintervall ansteigt, aktualisiert Citrix Cloud die Verwendungsspitze für die aktuelle Stunde.
- **Aktive Nutzung** zeigt ein Diagramm mit den folgenden Informationen an:
  - **Täglich:** Die Gesamtzahl der Verbindungen für jeden Tag während der letzten 30 Tage.

- **Monatlich:** Die Gesamtzahl der Verbindungen für jeden Monat des vorangegangenen Kalenderjahres.

Wenn Sie in den Diagrammen **Lizenzzuweisung** oder **Aktive Nutzung** auf ein Intervall zeigen, werden die Details für dieses Intervall angezeigt.

Lizenzierte Benutzer

Der Abschnitt **Lizenzaktivität** enthält eine Liste der einzelnen Kundenbenutzer, denen Lizenzen im aktuellen Monat zugewiesen wurden. In dieser Liste wird auch die Domäne für jeden Benutzer, das Datum der Lizenzzuweisung und die letzte Verwendung des Service angezeigt.

Monatliche Freigabe von Lizenzen

Am ersten Tag jedes Monats werden zugewiesene Lizenzen aus dem Vormonat automatisch freigegeben. In diesem Fall wird die Anzahl zugewiesener Lizenzen auf null zurückgesetzt, und die Liste der lizenzierten Kundenbenutzer wird gelöscht. Lizenzen werden neu zugewiesen, wenn Benutzer Apps oder Desktops zum ersten Mal innerhalb des neuen Monats starten.

Überprüfen des monatlichen Lizenzverlaufs

Am ersten Tag jedes Monats wird die Liste der lizenzierten Kundenbenutzer des Vormonats unter **Lizenzaktivität** gelöscht, wenn die Anzahl der zugewiesenen Lizenzen auf null zurückgesetzt wird. Sie können jedoch jederzeit auf Benutzerdetails aus vorherigen Monaten zugreifen und sie bei Bedarf als CSV-Datei herunterladen.

1. Wählen Sie unter **Lizenzaktivität** die Option **Lizenzverlauf anzeigen** am rechten Rand.
2. Wählen Sie den Monat aus, den Sie anzeigen möchten. Eine Liste der Benutzerdetails für den ausgewählten Monat wird angezeigt.
3. Zum Exportieren der Liste wählen Sie am rechten Rand **Als CSV-Datei exportieren** und speichern Sie die Datei.

Exportieren von Lizenzdetails

Kunden können lizenzierte Benutzerdetails jederzeit in eine CSV-Datei exportieren. Diese Datei kann dann bei Bedarf zum Analysieren der Lizenzdetails verwendet werden.

Um die Details für den aktuellen Monat zu exportieren, wählen Sie im Bereich **Lizenzaktivität** am rechten Rand **Als CSV-Datei exportieren** und speichern Sie die Datei.

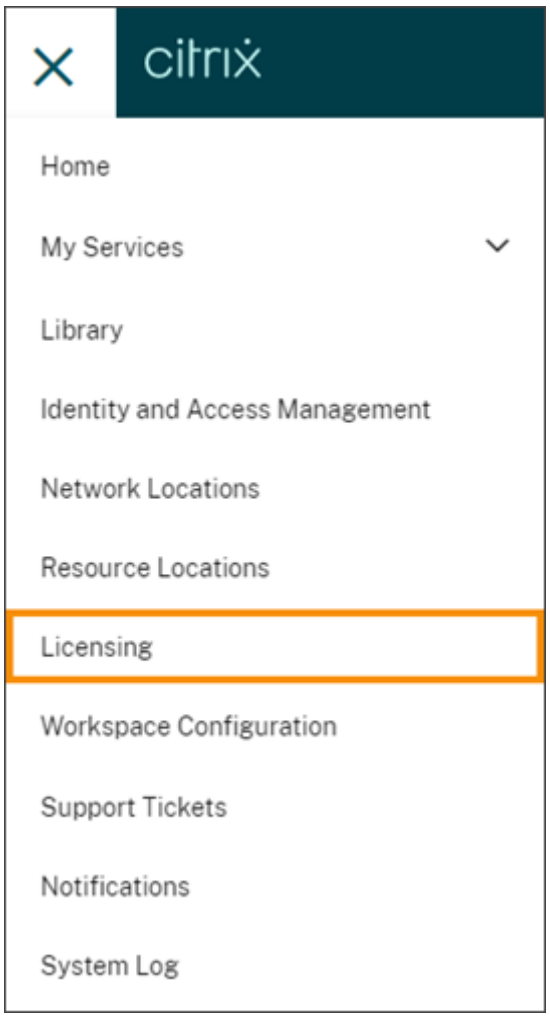
Um die Details für vergangene Monate zu exportieren, erstellen Sie eine Liste für den ausgewählten Monat, wie unter Überprüfen des monatlichen Lizenzverlaufs beschrieben. Wählen Sie **In CSV exportieren** und speichern Sie die Datei.

Überwachen von Kundenlizenzen und -nutzung für Citrix DaaS Standard für Azure

September 28, 2023

Kunden von **Citrix Service Provider (CSP)** können Citrix DaaS Standard für Azure-Lizenzen für ihre Benutzer in Citrix Cloud mühelos überwachen. Als CSP können Sie auf diese Details zugreifen, indem Sie sich bei ihrem Kundenkonto in Citrix Cloud anmelden. Eine aggregierte Übersicht der Lizenznutzung für Einzel- und Mehrmandantenkunden finden Sie unter Cloudservice-Lizenznutzung und -Berichterstellung für Citrix Service Provider.

Kunden können ihre Lizenzdaten durch Auswahl von **Lizenzierung** im Citrix Cloud-Menü anzeigen.



Lizenzzuweisung

Benutzer-/Gerätelizenzmodell: Citrix Cloud weist eine Lizenz zu, wenn ein eindeutiger Benutzer oder ein eindeutiges Gerät zum ersten Mal einen Desktop startet.

Gleichzeitig-Lizenzmodell: Citrix Cloud weist eine Lizenz zu, wenn ein Benutzer eine App oder einen Desktop auf dem Gerät startet. Wenn der Benutzer sich abmeldet oder die Verbindung zur Sitzung trennt, ist die Lizenz nicht länger zugewiesen. Da die Lizenzzuweisung davon abhängt, wie viele Geräte aktuell auf Desktops zugreifen, erfasst Citrix Cloud alle fünf Minuten die Anzahl verwendeter Lizenzen.

Weitere Informationen zum Gleichzeitig-Lizenzmodell (CCU-Lizenzen) finden Sie unter CCU-Lizenzen in der Produktdokumentation zur Lizenzierung.

Zusammenfassung zur Lizenzierung

Citrix Cloud zeigt Zusammenfassungen der im Rahmen des Benutzer-/Gerätelizenzmodells und Gleichzeitig-Lizenzmodells verwendeten Lizenzen an.

Zusammenfassung für Benutzer und Geräte

Die Benutzer/Gerät-Lizenzübersicht zeigt einen Überblick über die verwendeten Lizenzen im Verhältnis zur Gesamtzahl der Lizenzen, die Sie besitzen.

Wenn sich der Prozentsatz 100 % nähert, wechselt der Prozentsatz von grün zu gelb. Wenn der Prozentsatz 100 % überschreitet, wird der Prozentsatz rot angezeigt.

Citrix Cloud zeigt auch das Verhältnis zugewiesener zu erworbenen Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen.

Zusammenfassung für gleichzeitige Benutzer

Die Gleichzeitig-Lizenzübersicht bietet einen Überblick über die folgenden Informationen:

- Prozentsatz der erworbenen Lizenzen, die verwendet wurden, als die letzte Lizenzprüfung durch Citrix Cloud erfolgte. Citrix Cloud berechnet diesen Prozentsatz alle fünf Minuten basierend auf eindeutigen Geräten mit aktiven Verbindungen zum Dienst. Die Gesamtanzahl an erworbenen Lizenzen umfasst alle erworbenen Lizenzen für Citrix DaaS Standard für Azure, die das Gleichzeitig-Lizenzmodell verwenden.
- Das Verhältnis aktuell zugewiesener Lizenzen zur Gesamtanzahl erworbener Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen. Unter **Gesamt** sehen Sie die Gesamtanzahl aller erworbenen Lizenzen (gemäß Zeitpunkt unter "Letzter Bericht").
- Statistiken zu Verwendungsspitzen. Bei der Berechnung von Verwendungsspitzen für Lizenzen erfasst Citrix Cloud die maximale Anzahl verwendeter Lizenzen für folgende Zeiträume:
  - **Letzte 24 Stunden:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen in den letzten 24 Stunden.
  - **In diesem Monat:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen im aktuellen Monat.
  - **Gesamte Zeit:** Die maximale Anzahl gleichzeitig verwendeter Lizenzen seit Beginn des Abonnements.

  Unter **Gesamt** sehen Sie für den jeweiligen Zeitraum, wie viele Lizenzen während der Verwendungsspitze insgesamt im Besitz waren. Wenn die Gesamtzahl der erworbenen Lizenzen ansteigt oder sinkt und sich die Anzahl zugewiesener Lizenzen entsprechend erhöht, ändert

sich auch der Wert unter **Gesamt**. Wenn keine entsprechende Verwendungsspitze auftritt, ändert sich der Wert unter **Gesamt** nicht.

Berechnung von Verwendungsspitzen für Lizenzen

Um das Gleichzeitig-Modell (CCU-Lizenzen) akkurat wiederzugeben, erfasst Citrix Cloud alle fünf Minuten, wie viele eindeutige Geräte gleichzeitig auf den Dienst zugreifen. Liegt die Zahl über der aktuellen Verwendungsspitze, zeigt Citrix Cloud die neue Verwendungsspitze mit Datum und Uhrzeit an. Wenn die Anzahl unter der aktuellen Verwendungsspitze liegt, ändert sich der aktuelle Spitzenwert nicht.

Nutzungstrends

Citrix Cloud zeigt eine Aufschlüsselung der Nutzungstrends für Benutzer/Gerät- oder Gleichzeitig-Lizenzen an. Um diese Aufschlüsselung anzuzeigen, wählen Sie auf der Seite mit der Lizenzübersicht die Option **Nutzungsdetails anzeigen**.

Trends für Benutzer und Geräte

Für Benutzer/Gerät-Lizenzen zeigt der Abschnitt **Nutzungstrends** eine Aufschlüsselung der zugewiesenen Lizenzen als Diagramm.

Wenn Sie auf ein Intervall im Diagramm zeigen, werden die folgenden Informationen angezeigt:

- **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.
- **Zuvor zugewiesen:** die Anzahl der Lizenzen, die im Vormonat zugewiesen wurden. Beispielsweise greift ein Benutzer im Juli das erste Mal auf den Cloudservice zu und ihm wird eine Lizenz zugewiesen. Diese Lizenz gilt für den Monat Juli als "Neu zugewiesen". Für den Monat August wird diese Lizenz als "Zuvor zugewiesen"gezählt.
- **Neu zugewiesen:** Die Anzahl neuer Lizenzen, die pro Monat zugewiesen wurden. Beispielsweise greift ein Benutzer im Juli das erste Mal auf den Cloudservice zu und ihm wird eine Lizenz zugewiesen. Diese Lizenz gilt für den Monat Juli als "Neu zugewiesen".

Trends für Gleichzeitig-Modell

Für das Gleichzeitig-Modell werden im Bereich **Nutzungstrends** folgende Informationen angezeigt:

- **Lizenzen insgesamt:** Gesamtanzahl Ihrer erworbenen CCU-Lizenzen.

- **Spitzennutzung Lizenzen:** Die maximale Anzahl zugewiesener Lizenzen im ausgewählten Zeitraum. Standardmäßig zeigt Citrix Cloud Verwendungsspitzen für jeden Monat im aktuellen Kalenderjahr an. Um monatliche oder stündliche Verwendungsspitzen anzuzeigen, wählen Sie im Dropdownmenü den Kalendermonat oder Kalendertag aus, den Sie untersuchen möchten.

  Wenn der ausgewählte Datumsbereich noch nicht abgeschlossen ist, zeigt Citrix Cloud die aktuelle Verwendungsspitze für das derzeitige Zeitintervall an. Wenn Sie beispielsweise die Details für den aktuellen Kalendertag anzeigen, ist die maximale Anzahl verwendeter Lizenzen für jede Stunde bis zum aktuellen Zeitpunkt zu sehen. Wenn die maximale Anzahl verwendeter Lizenzen im nächsten Fünf-Minuten-Zählintervall ansteigt, aktualisiert Citrix Cloud die Verwendungsspitze für die aktuelle Stunde.

Wenn Sie auf ein Intervall zeigen, werden die Gesamtzahl der Lizenzen und die Höchstzahl der im Intervall verwendeten Lizenzen angezeigt.

Nutzungsberichte

Sie können Nutzungsinformationen für ein Standardintervall oder ein bestimmtes Intervall herunterladen.
Die Informationen umfassen die gemessene Nutzung für:

- Azure-VMs
- Netzwerkverbindungen, z. B. VNet-Peering
- Azure-Speicherelemente, z. B. verwaltete Datenträger, Block-Blobs und Seitenblobs

Nach Ablauf eines Tages/Monats kann es bis zu 72 Stunden dauern, bis Daten die gesamte Nutzung widerspiegeln.

Wählen Sie unter **Nutzungsberichte** ein Intervall aus, und wählen Sie **Daten herunterladen**, um eine CSV-Datei zu erstellen und auf Ihre lokale Maschine herunterzuladen.

Lizenzierte Benutzer

Für Benutzer-/Gerätelizenzen enthält der Abschnitt **Lizenzaktivität** eine Liste der einzelnen Kundenbenutzer, denen Lizenzen im aktuellen Monat zugewiesen wurden. In dieser Liste wird auch die Domäne für jeden Benutzer, das Datum der Lizenzzuweisung und die letzte Verwendung des Service angezeigt. Dieser Abschnitt ist für Gleichzeitig-Lizenzen nicht verfügbar.

Monatliche Freigabe von Lizenzen

Am ersten Tag jedes Monats werden zugewiesene Lizenzen aus dem Vormonat automatisch freigegeben. In diesem Fall wird die Anzahl zugewiesener Lizenzen auf null zurückgesetzt, und

die Liste der lizenzierten Kundenbenutzer wird gelöscht. Lizenzen werden neu zugewiesen, wenn Benutzer Apps oder Desktops zum ersten Mal innerhalb des neuen Monats starten.

Überprüfen des monatlichen Lizenzverlaufs

Am ersten Tag jedes Monats wird die Liste der lizenzierten Kundenbenutzer des Vormonats unter **Lizenzaktivität** gelöscht, wenn die Anzahl der zugewiesenen Lizenzen auf null zurückgesetzt wird. Sie können jedoch jederzeit auf Benutzerdetails aus vorherigen Monaten zugreifen und sie bei Bedarf als CSV-Datei herunterladen.

1. Wählen Sie unter **Lizenzaktivität** die Option **Lizenzverlauf anzeigen** am rechten Rand.
2. Wählen Sie den Monat aus, den Sie anzeigen möchten. Eine Liste der Benutzerdetails für den ausgewählten Monat wird angezeigt.
3. Zum Exportieren der Liste wählen Sie am rechten Rand **Als CSV-Datei exportieren** und speichern Sie die Datei.

Exportieren von Lizenzdetails

Sie können lizenzierte Benutzerdetails für einen Kunden jederzeit in eine CSV-Datei exportieren. Diese Datei können Sie dann bei Bedarf zum Analysieren der Lizenzdetails verwenden.

Um die Details für den aktuellen Monat zu exportieren, wählen Sie im Bereich **Lizenzaktivität** am rechten Rand **Als CSV-Datei exportieren** und speichern Sie die Datei.

Um die Details für vergangene Monate zu exportieren, erstellen Sie eine Liste für den ausgewählten Monat, wie unter Überprüfen des monatlichen Lizenzverlaufs beschrieben. Wählen Sie **In CSV exportieren** und speichern Sie die Datei.

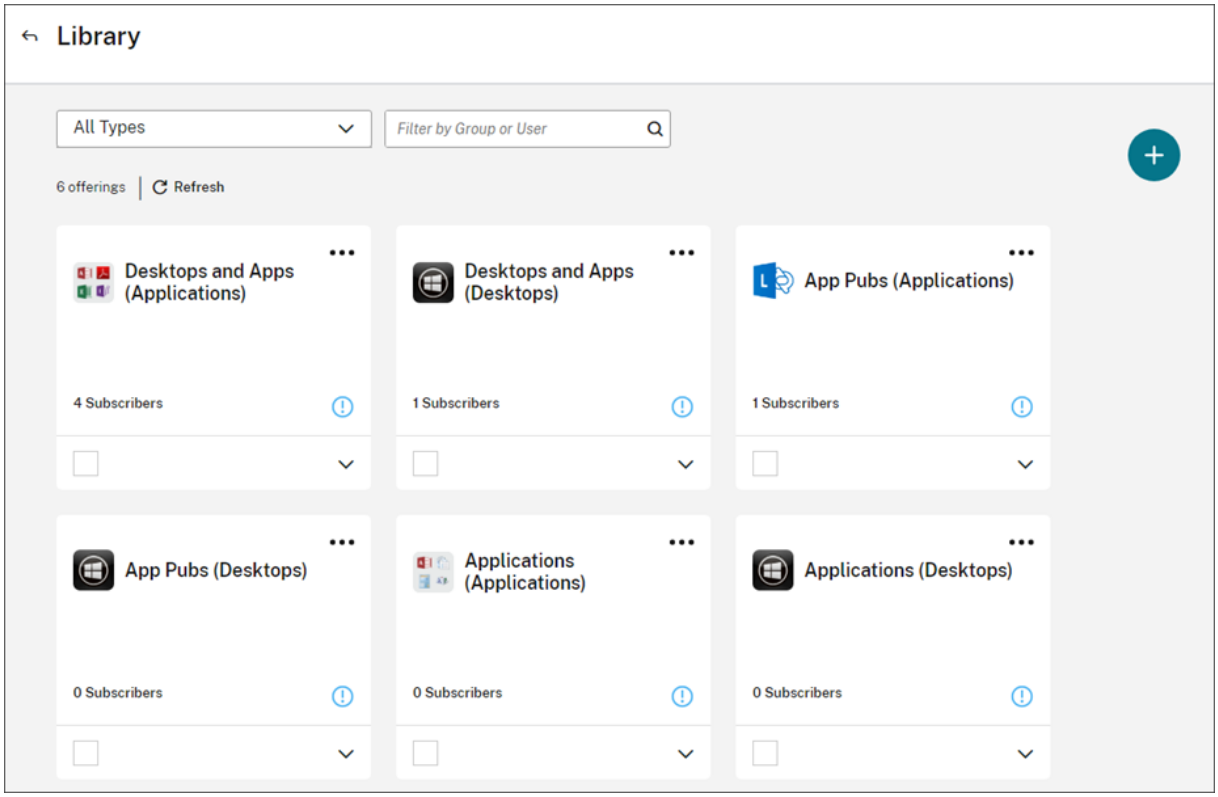
Benutzer und Gruppen über die Bibliothek zu Serviceangeboten zuweisen

April 26, 2024

> **Hinweis:**
>
> Für Bereitstellungsgruppen in *Verwaltet von Citrix Cloud* können Benutzerzuweisungen jetzt direkt in der Web Studio-Konsole verwaltet werden. Weitere Informationen finden Sie in der DaaS-Dokumentation. Bisher war die Verwaltung dieser Bereitstellungsgruppen auf die Bibliothek beschränkt, aber jetzt können Sie dieselben Verwaltungsfunktionen in der Web

> Studio-Konsole verwenden. Dieses Feature ist jetzt für alle Kunden verfügbar. Im Juni 2024 werden DaaS-spezifische Anwendungsfälle in der Cloud Library vollständig veraltet sein.

Sie können Ressourcen und andere in einem Service konfigurierte Elemente Active Directory-Benutzern und -Gruppen mit der Bibliothek zuweisen. Solche Angebote können aus Anwendungen, Desktops, Datenfreigaben und Webanwendungen bestehen, die Sie über einen Citrix Service erstellen. In der Bibliothek werden Ihre gesamten Angebote in einer einzelnen Ansicht angezeigt.



Administratorzugriff

Um auf die Bibliothek zugreifen zu können, müssen Administratoren:

- sich über den Citrix-Identitätsanbieter oder Azure AD authentifizieren.
- sich als einzelner Administrator (nicht als Mitglied einer Administratorgruppe) anmelden.
- Vollzugriff auf Citrix Cloud oder benutzerdefinierten Zugriff haben, sofern die Bibliotheksrolle ausgewählt ist.

Wenn Sie über Einzel- und Gruppenadministratorkonten in Citrix Cloud verfügen, hängt Ihr Zugriff auf die Bibliothek möglicherweise von den jeweils für ein Konto geltenden Berechtigungen ab. Weitere Informationen finden Sie unter Resultierende Berechtigungen für Administratoren mit Citrix-, AD-, Azure AD- und Google Cloud-Identitäten.

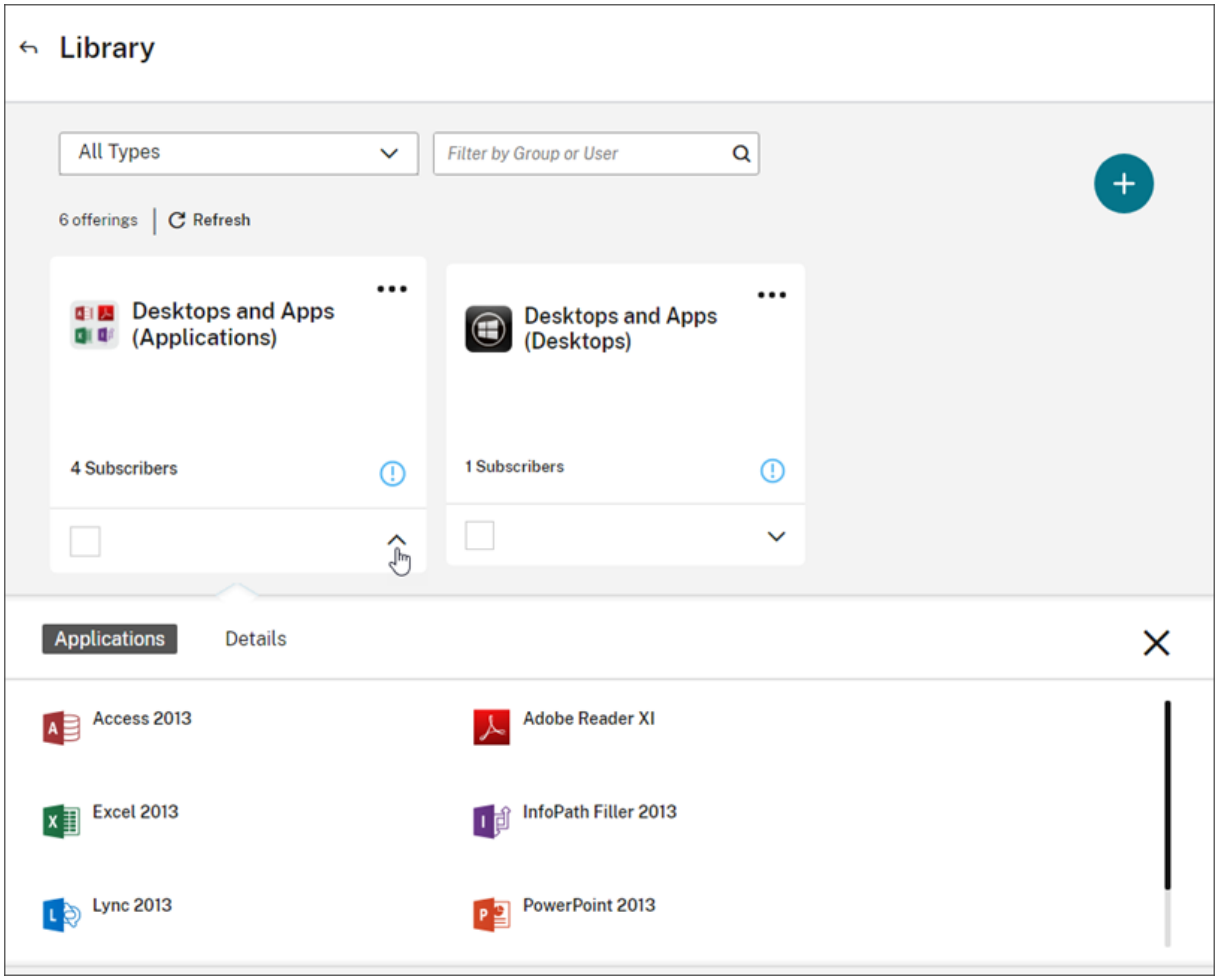
Überlegungen zur Verwendung von StoreFront mit Citrix DaaS

Wenn Sie On-Premises-StoreFront mit Citrix DaaS verwenden, sollten Sie beim Erstellen von Bereitstellungsgruppen Ressourcen nicht mit der Bibliothek zuweisen. Verwenden Sie stattdessen Studio, um Benutzern Ressourcen zuzuweisen. Wenn Sie in diesem Szenario die Bibliothek verwenden, werden Ressourcen möglicherweise nicht für Benutzer angezeigt.

Wenn Sie eine Bereitstellungsgruppe in Studio erstellen, wählen Sie nicht die Option **Benutzerverwaltung mit Citrix Cloud** auf der Seite **Benutzer**. Wählen Sie stattdessen **Alle authentifizierten Benutzer dürfen diese Bereitstellungsgruppe verwenden** oder **Verwenden der Bereitstellungsgruppe auf diese Benutzer beschränken**.

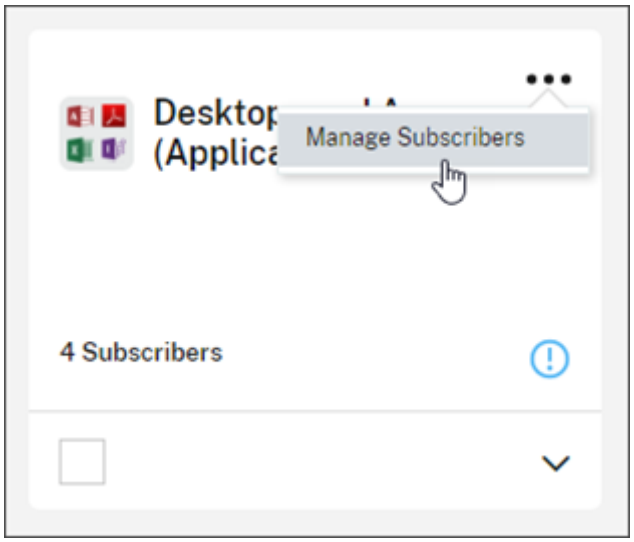
Anzeigen von Angebotsdetails

Klicken Sie auf der Angebotskarte auf den Pfeil, um Anwendungen, Desktops, Richtlinien und andere Angebotsinformationen anzuzeigen.

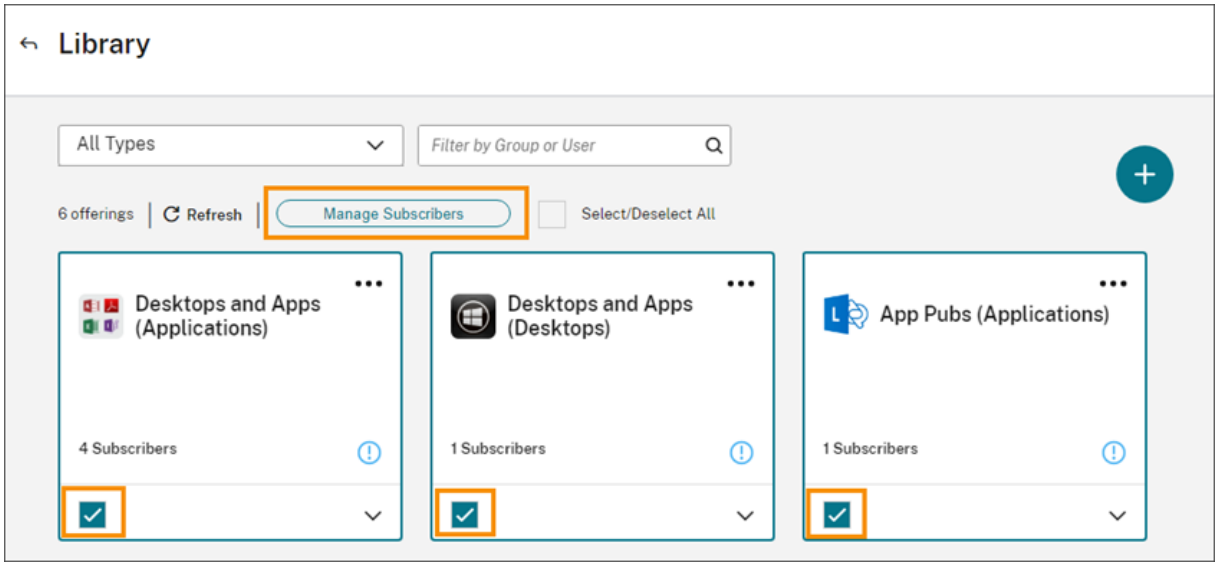


Abonnenten hinzufügen oder entfernen

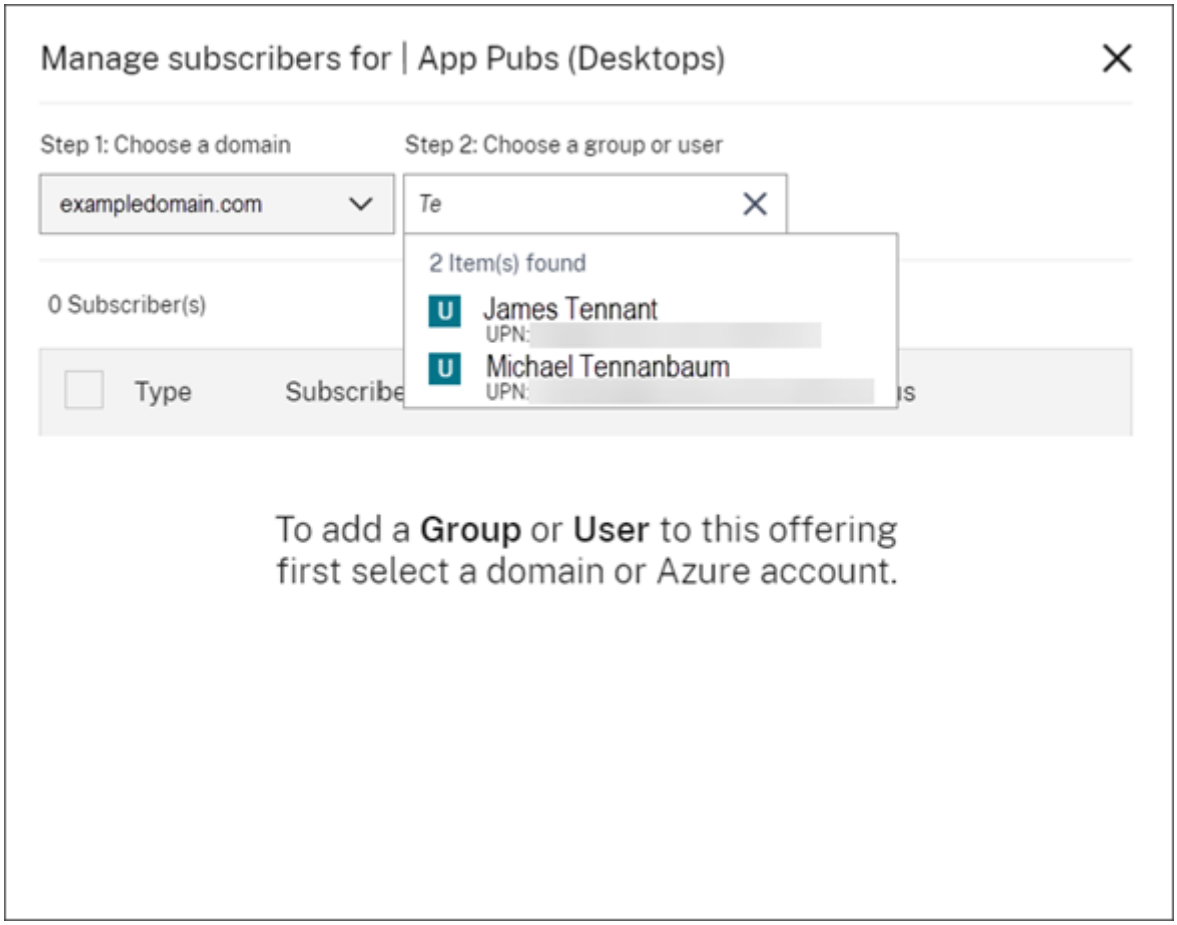
Klicken Sie zum Verwalten von Benutzern oder Gruppen für ein einzelnes Angebot im Menü der Angebotskarte auf **Abonnenten verwalten**.



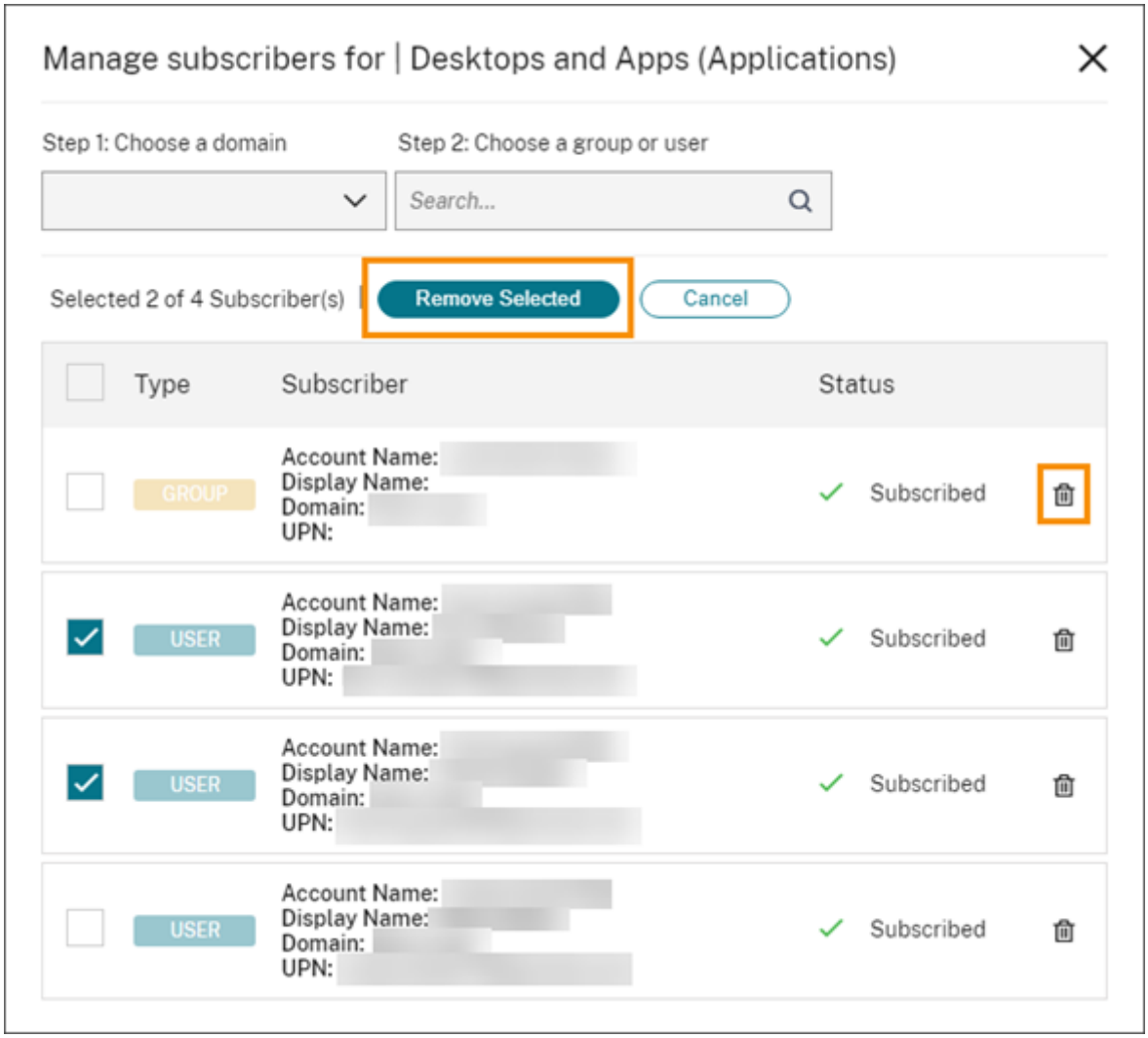
Um Abonnenten für mehrere Angebote zu verwalten, aktivieren Sie das Kontrollkästchen für jedes Angebot und klicken Sie dann auf **Abonnenten verwalten**.



Zum Hinzufügen von Abonnenten zum Angebot wählen Sie eine Domäne und dann die Benutzer oder Gruppen, die Sie hinzufügen möchten.



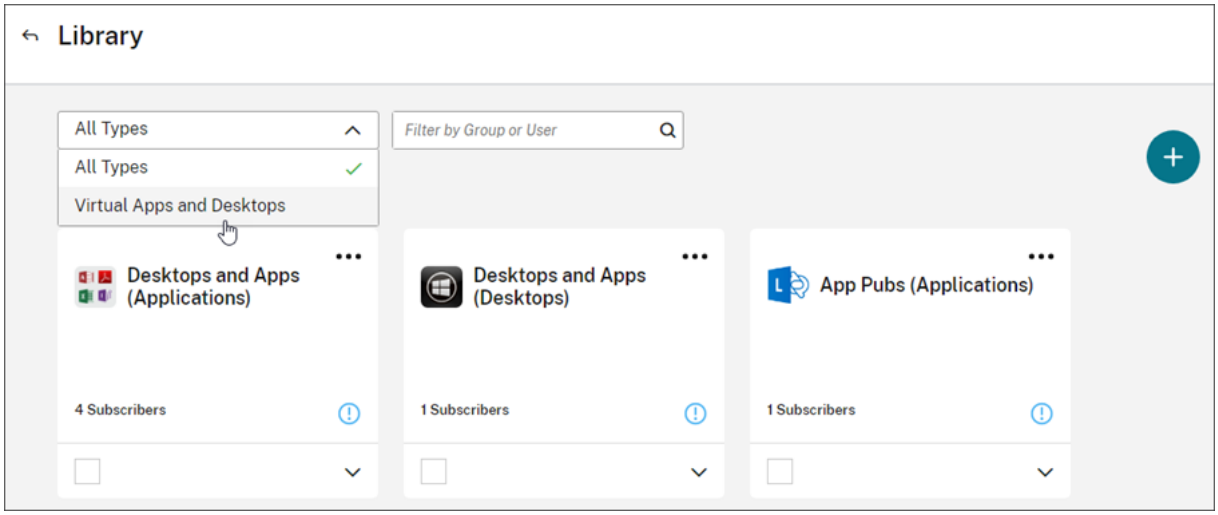
Klicken Sie zum Entfernen einzelner Abonnenten auf das zum Abonnenten gehörende Papierkorbsymbol. Um mehrere Abonnenten zu entfernen, wählen Sie die Benutzer (bzw. Gruppen) und klicken Sie auf **Ausgewählte entfernen**.



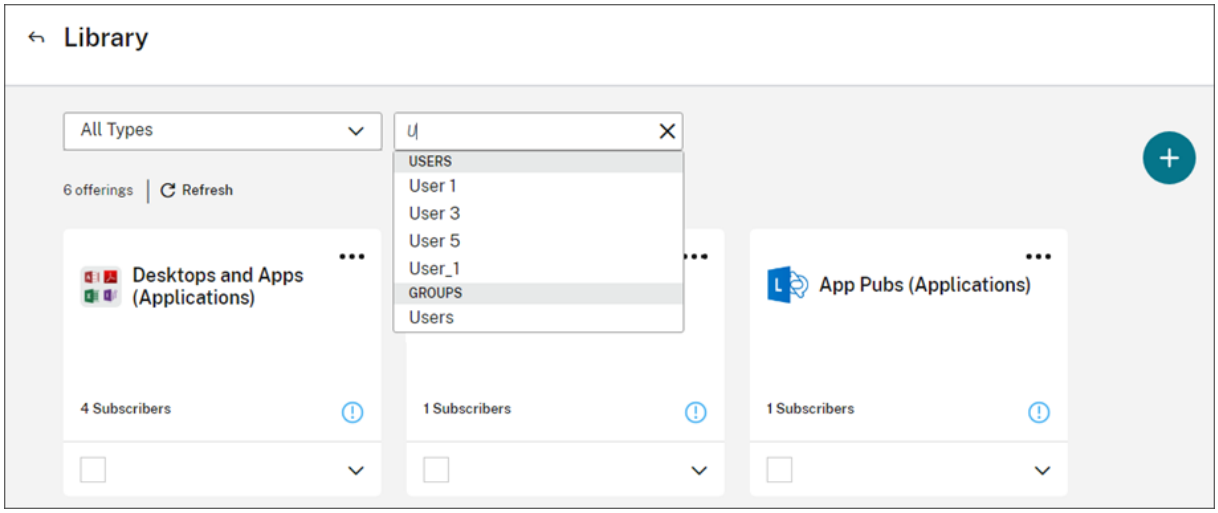
Nachdem Sie Abonnenten hinzugefügt oder entfernt haben, zeigt die Angebotskarte die aktuelle Abonnentenzahl an.

Filtern von Angeboten

Standardmäßig werden in der Bibliothek alle Angebote angezeigt. Zum Anzeigen der Angebote eines bestimmten Service wählen Sie den Filter für diesen Service.



Sie können auch alle Benutzer oder Gruppen suchen, die zurzeit ein Angebot in der Bibliothek abonniert haben. Citrix Cloud zeigt nur die Angebote an, die sich auf den ausgewählten Benutzer bzw. die ausgewählte Gruppe beziehen. Um alle Angebote für alle Benutzer anzuzeigen, klicken Sie auf das X, um den Filter zu löschen.



Benutzerdefinierte Landingpage

April 5, 2024

Viele Administratoren greifen auf die Cloud-Konsole zu, um bestimmte Aufgaben wie die Verwaltung von Anwendungen in der Web Studio-Konsole oder das Anzeigen von Daten in DaaS-Monitor auszuführen.

Diese Aufgaben erfordern jedoch jedes Mal, wenn sich Administratoren anmelden, mehrere Klicks sowie das Navigieren durch mehrere Seiten und kann daher zeitaufwendig sein. Dieses neue Feature

ermöglicht es Administratoren, eine benutzerdefinierte Landingpage einzurichten oder zu ändern, wodurch Zeit gespart und eine Kosteneinsparung erreicht wird.

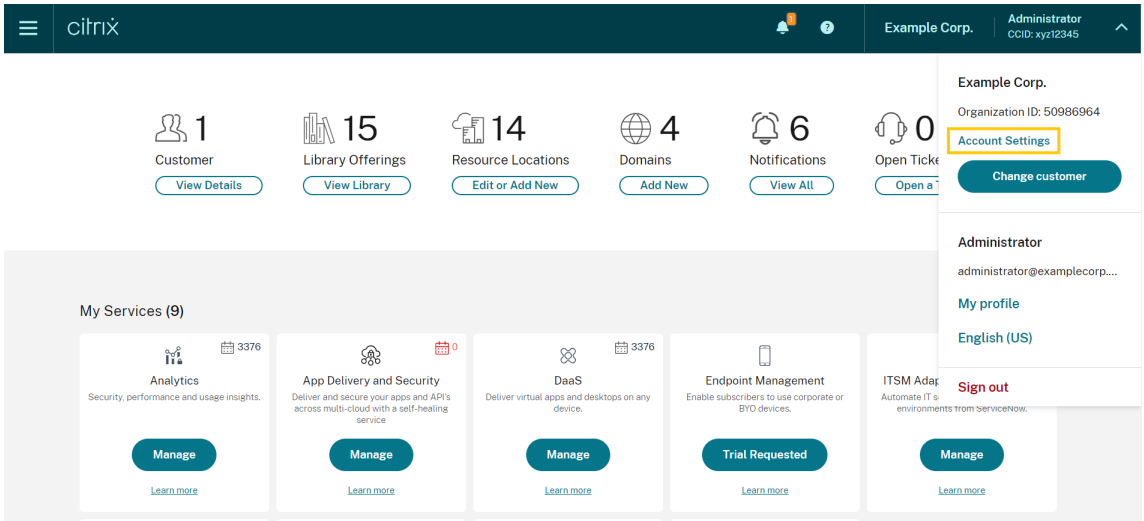
Derzeit können die folgenden Seiten als benutzerdefinierte Landingpage konfiguriert werden. Weitere werden voraussichtlich in Zukunft hinzugefügt:

- DaaS
- DaaS-Monitor
- NetScaler-Konsole
- CAS
- CAS Sicherheit
- CAS Leistung
- WEM
- Allgemein

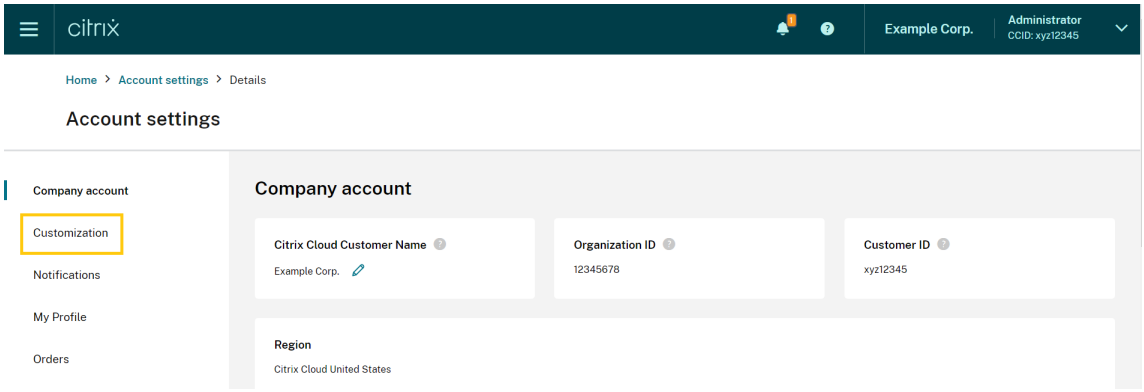
> **Hinweis:**
>
> Die Einstellung der benutzerdefinierten Landingpage ist optional und wird pro Konto festgelegt. So kann jeder Administrator seine eigene Benutzeroberfläche in Citrix Cloud anpassen. Alle Administratoren (ob benutzerdefiniert oder voll) haben Zugriff auf dieses Feature.

Benutzerdefinierte Landingpage konfigurieren

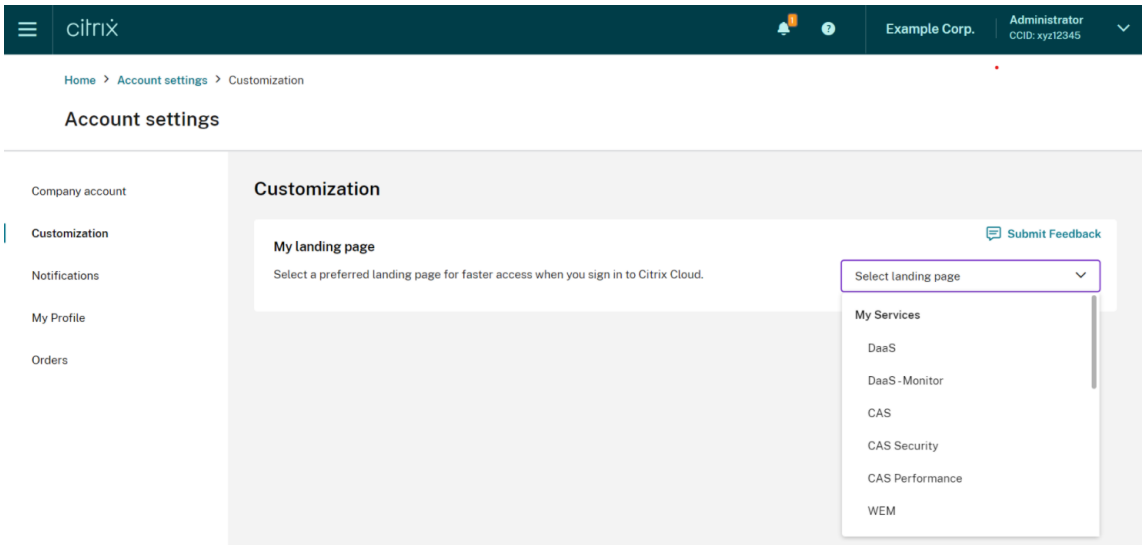
1. Klicken Sie auf den Profilnamen und wählen Sie **Kontoeinstellungen** aus.



2. Klicken Sie auf **Anpassung**.



3. Wählen Sie den Dienst aus, den Sie als Ihre benutzerdefinierte Landingpage konfigurieren möchten.



4. Klicken Sie auf **Anwenden**.

   Ihre benutzerdefinierte Landingpage ist jetzt eingerichtet.

> **Hinweis:**
>
> - Sie können Ihre benutzerdefinierte Landingpage jederzeit auf die Standard-Cloud-Homepage zurücksetzen, indem Sie auf **Auf Standard zurücksetzen** klicken.
> - Wenn Sie sich erneut auf derselben Seite anmelden, auf der Sie sich gerade abgemeldet haben, gelangen Sie zu Ihrer zuletzt angesehenen Seite und nicht zu Ihrer neuen Landingpage.

Zulassen, dass Kunden das Citrix Cloud-Konto löschen und erneut integrieren

April 26, 2024

Citrix Cloud bietet Kunden die Möglichkeit, ihr Citrix Cloud-Konto sicher zu löschen und bei Bedarf nahtlos wieder zu integrieren.

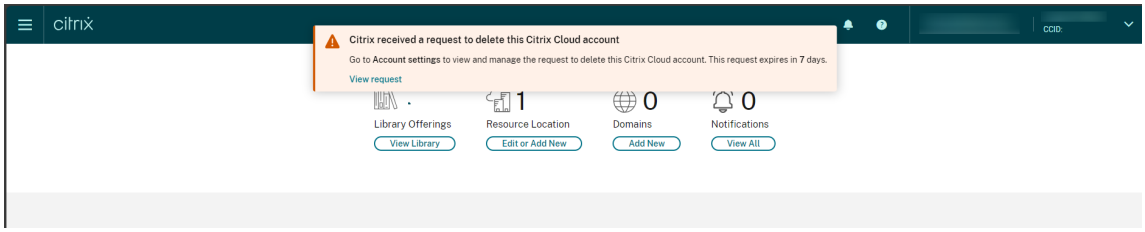
Voraussetzungen

- Wenn Ihr Konto über aktive DaaS-Berechtigungen verfügt und Ihre DaaS-Umgebung bereitgestellt ist, wenden Sie sich an den technischen Support von Citrix, um eine schnelle Außerbetriebnahme auszuführen, bevor Sie fortfahren. Weitere Informationen dazu, wie Sie überprüfen können, ob Ihre DaaS-Umgebung bereitgestellt ist, finden Sie im Artikel Studio Console Shows "Enable DaaS"for First Time Use.
- Entfernen Sie alle Cloud Connectors und Connector Appliances, die mit diesem Konto verknüpft sind.

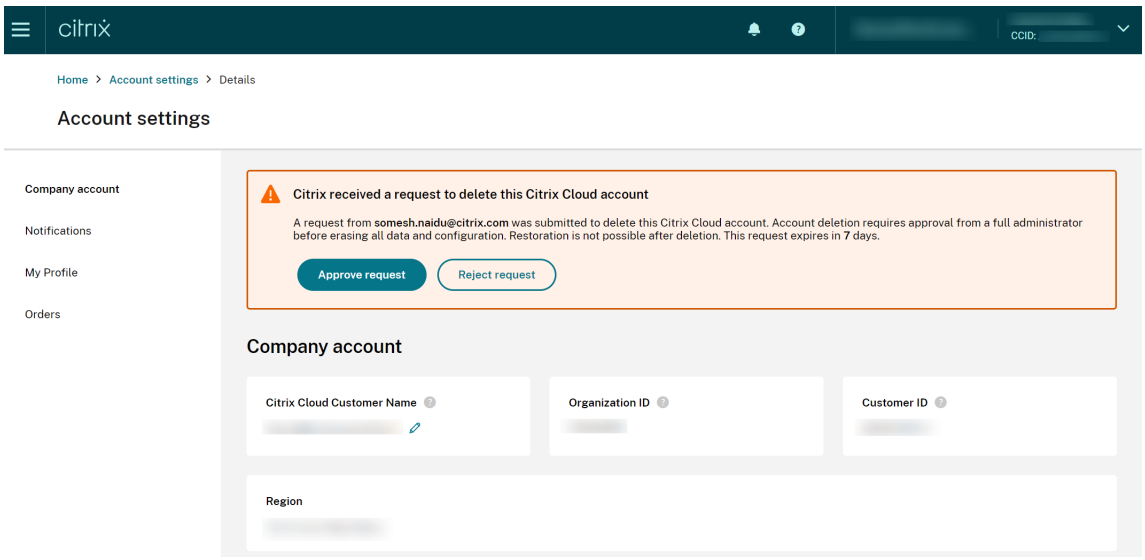
> **Wichtig**
>
> Beachten Sie die folgenden Punkte, bevor Sie ein Citrix Cloud-Konto löschen:
>
> - Alle kundenbezogenen Daten werden aus Citrix Datenbanken entfernt.
> - Alle Ressourcen im Zusammenhang mit Citrix Cloud Services, einschließlich von Citrix verwalteter VMs, die Citrix in Ihrer Cloudumgebung bereitgestellt hat, werden gelöscht. Eine Beschreibung der von Citrix verwalteten Komponenten, die in bestimmten Citrix Cloud Services enthalten sind, finden Sie unter Citrix Cloud Services.
> - Der Administrator- und Benutzerzugriff auf Citrix Cloud und Services wird deaktiviert.
> - Administratoren oder Benutzer, die den Service aktiv nutzen, werden Serviceunterbrechungen feststellen.
> - Diese Aktion kann nicht rückgängig gemacht werden. Nachdem die Daten gelöscht wurden, können sie nicht wiederhergestellt werden.

Schritte

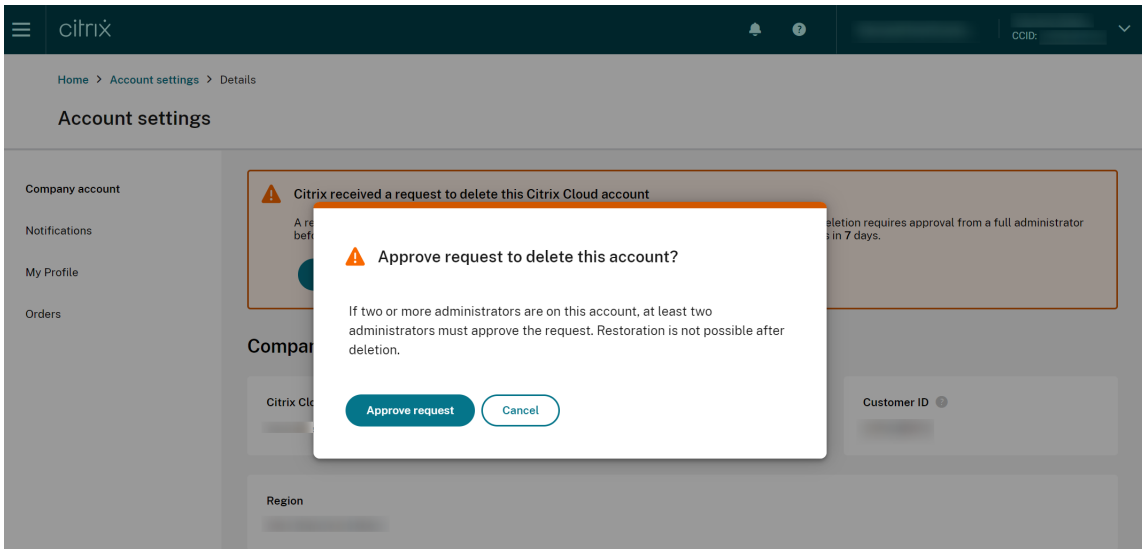
1. Wenden Sie sich an Citrix Customer Service, um eine Löschanforderung zu stellen. Diese Anforderung muss von einem *Volladministrator* für das Citrix Cloud-Konto gestellt werden.
2. Nachdem Ihre Anforderung initiiert wurde, melden Sie sich bei Ihrem Citrix Cloud-Konto an. Dort sehen Sie den Workflow zum Löschen von Citrix Cloud-Konten.



3. Folgen Sie den Anweisungen auf dem Bildschirm, um diese Anforderung entweder zu genehmigen oder abzulehnen.



4. Um diese Löschanforderung zu genehmigen, melden Sie sich beim Konto an, navigieren Sie zu den **Kontoeinstellungen** und klicken Sie im Banner des Genehmigungsworkflows auf **Anforderung genehmigen**.



Um die Löschanforderung abzubrechen, melden Sie sich beim Konto an, navigieren Sie zu den **Kontoeinstellungen** und klicken Sie im Banner des Löschgenehmigungsworkflows auf **Anforderung**

ablehnen und entfernen .

> **Hinweis:**
>
> - Wenn diesem Konto zwei oder mehr Administratoren zugeordnet sind, müssen mindestens zwei Administratoren die Anforderung genehmigen.
> - Diese Anforderung läuft ab, wenn die erforderlichen Genehmigungen nicht innerhalb von 7 Tagen eingehen.

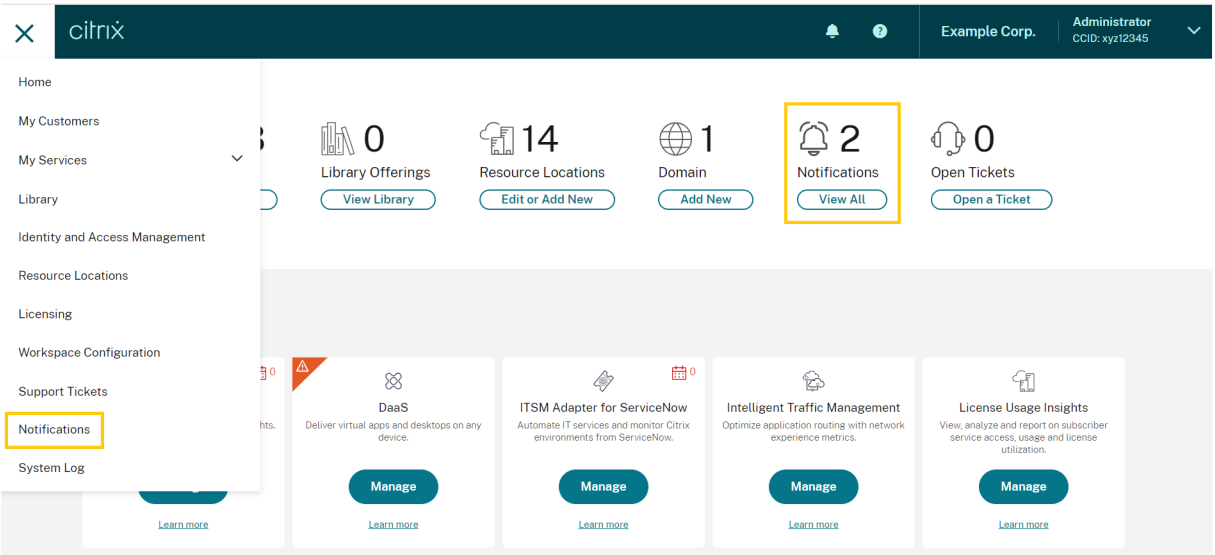
Benachrichtigungen

September 28, 2023

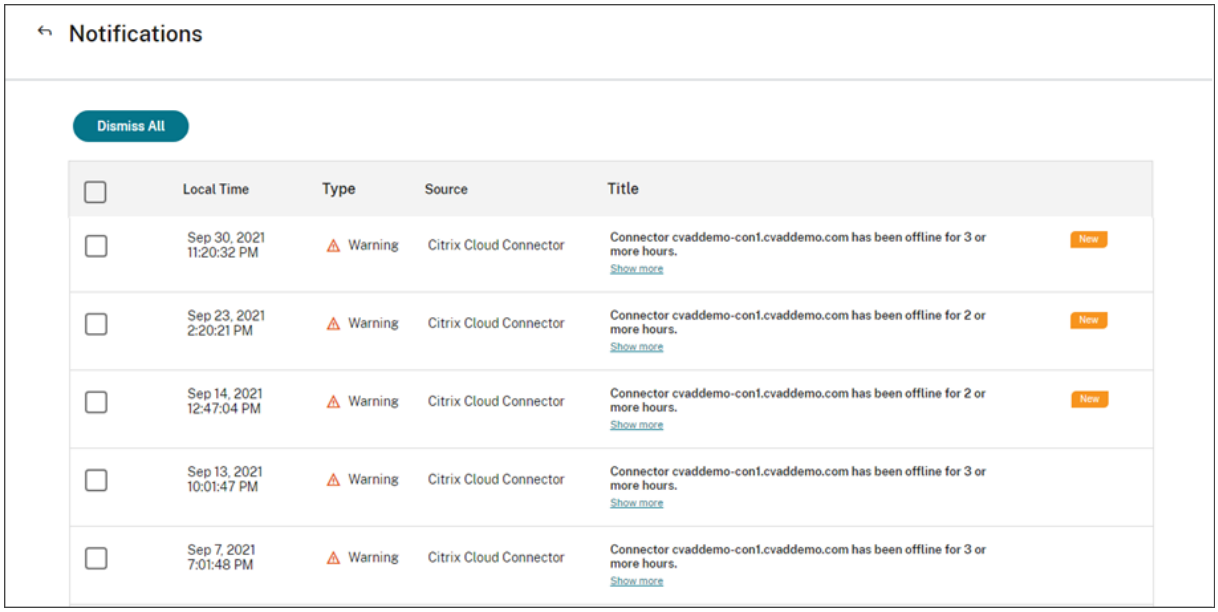
Benachrichtigungen enthalten Informationen zu Problemen oder Ereignissen, die für Administratoren von Interesse sein könnten, z. B. neue Citrix Cloud-Features oder Probleme mit einer Maschine an einem Ressourcenstandort. Benachrichtigungen können von jedem Service in Citrix Cloud gesendet werden.

Anzeigen von Benachrichtigungen

Die Anzahl der Benachrichtigungen wird oben auf der Citrix Cloud-Konsolenseite angezeigt. Um weitere Informationen aufzurufen, klicken Sie unter **Benachrichtigungen** in der Konsole auf **Alle anzeigen** oder wählen Sie im Konsolenmenü die Option **Benachrichtigungen** aus.



Auf der Seite “Benachrichtigungen”werden die Benachrichtigungen angezeigt, die Sie erhalten. Die neuesten Benachrichtigungen stehen oben auf der Liste.

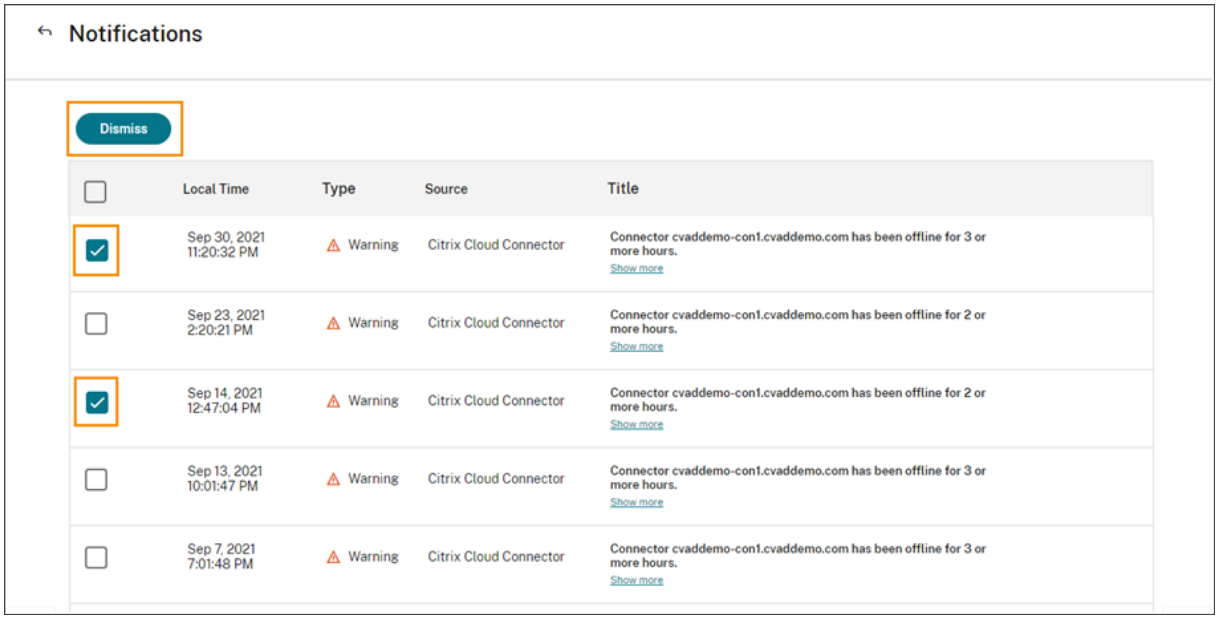


Benachrichtigungen schließen

Benachrichtigungen werden pro Administrator verwaltet. Wenn Sie Benachrichtigungen schließen, erfolgt die Schließung unter Ihrer eigenen Administratoridentität in Citrix Cloud. Andere Administratoren können ihre eigenen Benachrichtigungen weiterhin anzeigen und schließen, auch wenn Sie alle Ihre Benachrichtigungen geschlossen haben.

Um alle erhaltenen Benachrichtigungen zu verwerfen, wählen Sie oben auf der Seite die Option **Alle verwerfen** aus.

Um einzelne Benachrichtigungen zu verwerfen, wählen Sie jede Benachrichtigung aus und wählen Sie dann **Schließen** aus.



E-Mail-Benachrichtigungen empfangen

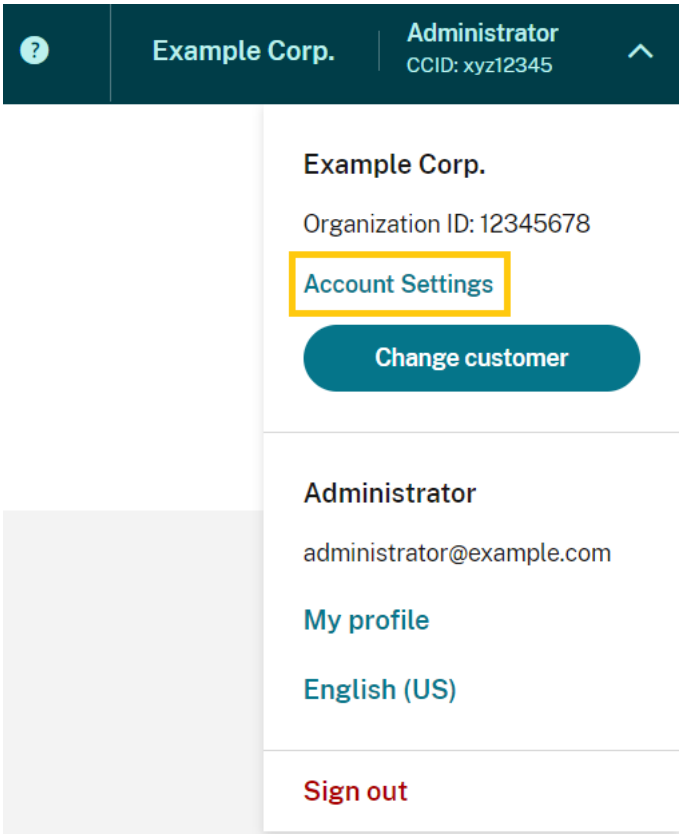
Sie können Benachrichtigungen auch per E-Mail erhalten und müssen sich dann nicht erst anmelden, um sie zu lesen. Standardmäßig sind E-Mail-Benachrichtigungen deaktiviert.

Sie können E-Mail-Benachrichtigungen auch für andere Nutzer ohne Administratorzugriff auf Ihr Citrix Cloud-Konto aktivieren, z. B. Mitglieder der Sicherheits- und Auditteams Ihrer Organisation.

Wenn Sie die E-Mail-Benachrichtigungen aktivieren, erhalten Sie von Citrix Cloud bei jeder Benachrichtigung eine E-Mail. Benachrichtigungen werden so schnell wie möglich gesendet. Sie werden nicht in einer E-Mail zusammengefasst oder gebündelt zu einem späteren Zeitpunkt gesendet.

E-Mail-Benachrichtigungen für Sie selbst aktivieren

1. Wählen Sie in der Citrix Cloud-Verwaltungskonsole **Kontoeinstellungen**.



2. Wählen Sie **Benachrichtigungen**.
3. Aktivieren Sie die Einstellung **Meine E-Mail-Benachrichtigungen**.
4. Wählen Sie unter **Meine Benachrichtigungseinstellungen verwalten** die Benachrichtigungstypen, die Sie erhalten möchten. Standardmäßig sind alle Benachrichtigungstypen ausgewählt.
5. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern

E-Mail-Benachrichtigungen für Nicht-Administratoren aktivieren

Führen Sie die Schritte in diesem Abschnitt aus, um Nicht-Administratoren als Kontakte für E-Mail-Benachrichtigungen hinzuzufügen. Wenn Sie versuchen, einen Administrator als Kontakt hinzuzufügen, wird in Citrix Cloud ein Fehler angezeigt.

1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf **Kontoeinstellungen**.
2. Wählen Sie **Benachrichtigungen**.
3. Wählen Sie unter **Kontaktverwaltung** die Option **Kontakt hinzufügen**.
4. Geben Sie den Namen, die E-Mail-Adresse und die bevorzugte Sprache des Kontakts ein.
5. Wählen Sie unter **Benachrichtigungseinstellungen verwalten** die zu sendenden Benachrichtigungstypen aus.

6. Wählen Sie **Kontakt hinzufügen**, um die Informationen des Kontakts zu speichern.

Benachrichtigungseinstellungen ändern

Als Administrator können Sie die Art der Benachrichtigungen, die Sie erhalten, ändern, indem Sie die Kontrollkästchen unter **Meine Benachrichtigungseinstellungen verwalten** aktivieren oder deaktivieren. Das Ändern Ihrer eigenen Benachrichtigungen wirkt sich nicht auf diejenigen aus, die andere Administratoren erhalten.

Sie können auch die Benachrichtigungen ändern, die Nicht-Administratoren erhalten.

Benachrichtigungen für Nicht-Administratoren ändern

1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf **Kontoeinstellungen**.
2. Wählen Sie **Benachrichtigungen**.
3. Suchen Sie unter **Kontaktverwaltung** den gewünschten Kontakt.
4. Zeigen Sie auf den Kontakt und wählen Sie das Stiftsymbol.
5. Aktivieren oder deaktivieren Sie unter **Benachrichtigungseinstellungen verwalten** die Kontrollkästchen der einzelnen Benachrichtigungstypen.

Um die E-Mail-Adresse eines Kontakts zu ändern, müssen Sie den Kontakt löschen und ihn dann neu mit der neuen E-Mail-Adresse hinzufügen.

E-Mail-Benachrichtigungen deaktivieren

Als Administrator können Sie Ihre eigenen E-Mail-Benachrichtigungen jederzeit deaktivieren, indem Sie die Einstellung **Meine E-Mail-Benachrichtigungen** deaktivieren.

Nicht-Administratoren können die Benachrichtigungen deaktivieren, indem sie auf den Link “Abonnement aufheben”klicken, der in jeder Benachrichtigungs-E-Mail angezeigt wird. Kontakte, die sich abgemeldet haben, haben den Benachrichtigungsstatus **Abonnement gekündigt** in der Tabelle unter **Kontaktverwaltung**.

Um Benachrichtigungen für Nicht-Administratoren zu deaktivieren, können Sie eine der folgenden Aktionen ausführen:

- Deaktivieren Sie alle Kontrollkästchen unter **Benachrichtigungseinstellungen verwalten** für den jeweiligen Kontakt.
- Löschen Sie den Kontakt aus der Tabelle unter **Kontaktverwaltung**.

Kontakteinträge von Nicht-Administratoren löschen

1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf **Kontoeinstellungen**.
2. Wählen Sie **Benachrichtigungen**.
3. Suchen Sie unter **Kontaktverwaltung** den gewünschten Kontakt.
4. Zeigen Sie auf den Kontakt und wählen Sie das Papierkorbsymbol.

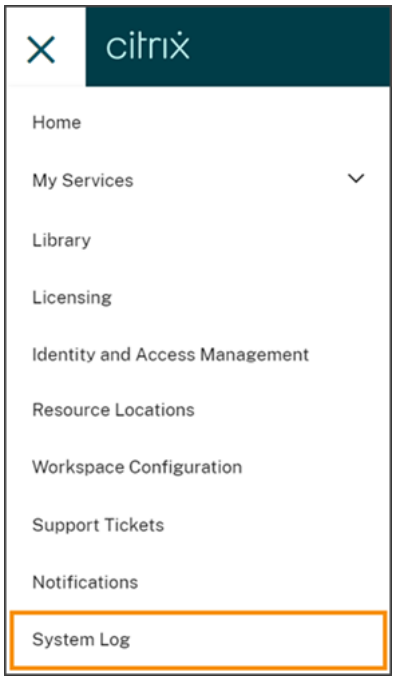
Citrix Cloud entfernt den Kontakt aus der Tabelle.

Systemprotokoll

September 28, 2023

Das Systemprotokoll enthält eine Liste mit Ereignissen in Citrix Cloud und Zeitstempeln. Sie können diese als CSV-Datei exportieren, um Compliance-Anforderungen Ihres Unternehmens zu erfüllen oder Sicherheitsanalysen durchzuführen.

Um das Systemprotokoll anzuzeigen, wählen Sie im Citrix Cloud-Menü die Option **Systemprotokoll** aus.

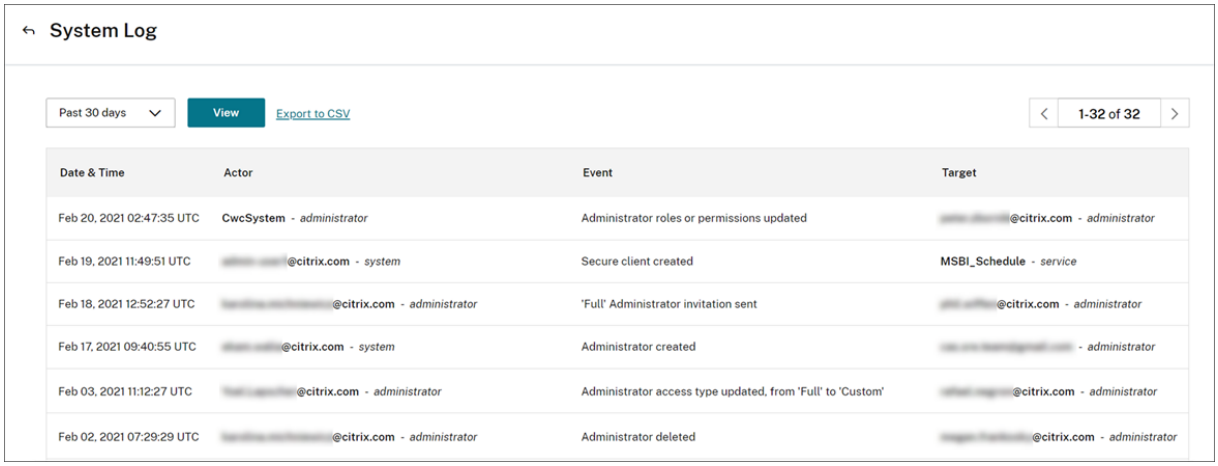


Weitere Informationen zur Aufbewahrung von Daten in Systemprotokollen finden Sie unter Datenaufbewahrung in diesem Artikel.

Protokollierte Ereignisse

Das Systemprotokoll erfasst Ereignisse für bestimmte Citrix Cloud-Plattform- und Cloudservice-Vorgänge. Eine vollständige Liste dieser Ereignisse und Beschreibungen der erfassten Daten finden Sie unter Referenz zu Systemprotokollereignissen.

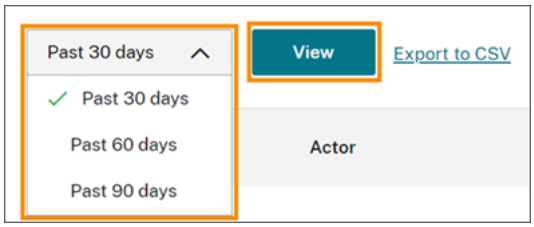
Standardmäßig zeigt das Systemprotokoll Ereignisse an, die in den letzten 30 Tagen aufgetreten sind. Die neuesten Ereignisse werden zuerst angezeigt.



Die angezeigte Liste enthält die folgenden Informationen:

- Datum und Uhrzeit (UTC) des Ereignisses.
- Initiator des Ereignisses, z. B. ein Administrator oder sicherer Client. Bei dem Initiator **CwcSystem** handelt es sich um Citrix Cloud.
- Kurze Beschreibung des Ereignisses, z. B. Bearbeiten eines Administrators oder Erstellen eines sicheren Clients.
- Ziel des Ereignisses. Das Ziel ist das Systemobjekt, das infolge des Ereignisses betroffen oder geändert wurde. Beispiel: ein Benutzer, der als Administrator hinzugefügt wurde.

Um vor mehr als 30 Tagen aufgetretene Ereignisse anzuzeigen, filtern Sie die Liste, indem Sie den gewünschten Zeitraum auswählen, und wählen Sie **Anzeigen**. Sie können Ereignisse nach bis zu 90 Tagen anzeigen.

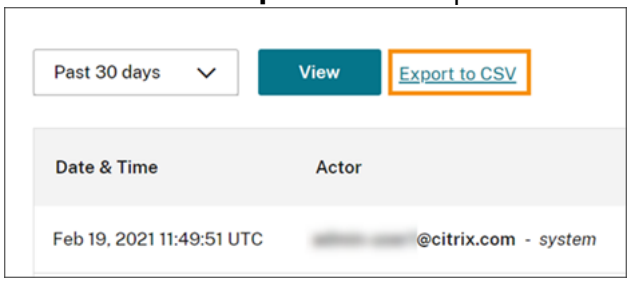


Um ältere Ereignisse abzurufen, können Sie die SystemLog-API verwenden. Weitere Informationen finden Sie unter Abrufen von Ereignissen eines bestimmten Zeitraums in diesem Artikel.

Exportieren von Ereignissen

Sie können eine CSV-Datei mit Systemprotokollereignissen exportieren, die in den letzten 90 Tagen aufgetreten sind. Der Name der heruntergeladenen Datei folgt dem Format `SystemLog-CustomerName-OrgID-DateTimeStamp.csv`.

1. Wählen Sie im Citrix Cloud-Menü **Systemprotokoll**aus.
2. Filtern Sie bei Bedarf die Liste nach dem gewünschten Zeitraum.
3. Wählen Sie **In CSV exportieren** und speichern Sie die Datei.



Die CSV-Datei enthält die folgenden Informationen:

- UTC-Zeitstempel jedes Ereignisses
- Initiator des Ereignisses, einschließlich Name und ID.
- Ereignisdetails wie Art und Text des Ereignisses
- Ziel des Ereignisses wie Ziel-ID, Name des Administrators oder eines sicheren Clients.

Abrufen von Ereignissen eines bestimmten Zeitraums

Wenn Sie Ereignisse für bestimmte Zeiträume abrufen müssen, können Sie die SystemLog-API verwenden. Bevor Sie die API verwenden, müssen Sie einen sicheren Client erstellen (siehe Get Started auf der Citrix Developer Docs-Website).

Weitere Informationen zur Verwendung der SystemLog-API finden Sie unter Citrix Cloud - SystemLog auf der Citrix Developer Docs-Website.

Weiterleiten von Systemprotokollereignissen

Mit dem Citrix Systemprotokoll-Add-On für Splunk können Sie Ihre Splunk-Instanz mit Citrix Cloud verbinden. Diese Verbindung gestattet das Weiterleiten von Systemprotokollereignissen an Splunk. Weitere Informationen finden Sie in der Add-On-Dokumentation im Citrix Repository auf GitHub.

Datenaufbewahrung

Citrix übernimmt zusammen mit den Kunden die Verantwortung für die Aufbewahrung der Systemprotokolldaten, die Citrix Cloud erfasst.

Citrix bewahrt Systemprotokolleinträge 90 Tage lang auf.

Sie sind dafür verantwortlich, die Systemprotokolleinträge, die Sie zur Erfüllung der Compliance-Anforderungen Ihres Unternehmens aufbewahren möchten, herunterzuladen und in einem Langzeitspeicher zu archivieren.

Referenz zu Systemereignissen

September 28, 2023

Um alle Systemprotokollereignisdaten für Ihr Citrix Cloud-Konto anzuzeigen, können Sie:

- Eine CSV-Datei mit allen Ereignissen herunterladen, die in den letzten 30, 60 oder 90 Tagen aufgetreten sind.
- Die SystemLog-API verwenden, um Ereignisse eines bestimmten Zeitraums abzurufen.

Unter Ereignisdatenbeschreibungen in diesem Artikel finden Sie Beschreibungen der Daten, die beim Abrufen von Systemprotokollereignissen erfasst werden. Unter Cloudkomponenten und -services, die Ereignisse generieren finden Sie ereignisspezifische Werte wie Ereignismeldungstext und Ereignistypen sowie Informationen dazu, ob Objektfelddaten vor und nach dem Auftreten von Ereignissen aufgezeichnet werden.

Cloudkomponenten und -services, die Ereignisse generieren

Das Systemprotokoll zeichnet Ereignisse für die folgenden Citrix Cloud-Entitäten, -Komponenten und -Dienste auf:

- Citrix Cloud-Plattform: Ereignisse im Zusammenhang mit Funktionen der Citrix Cloud-Plattform wie die Verwaltung von Administratoren, das Zurücksetzen von Geräten für Workspace-Abonnenten, Azure AD-Mandanten und die Verwaltung von Domänen und Netzwerkspeicherorten.
- Connectors: Ereignisse im Zusammenhang mit der Registrierung und Aktualisierung von Citrix Cloud Connectors und Connectorgeräten
- Lizenzierung: Ereignisse im Zusammenhang mit der Registrierung von On-Premises-Lizenzservern, der Verwaltung zugewiesener Lizenzen für Cloud-Services und dem Export von Lizenzdaten

- Secure Private Access Service: Ereignisse im Zusammenhang mit Secure Private Access Service-Konfigurationen.
- Citrix Workspace: Ereignisse im Zusammenhang mit den Workspacekonfigurationseinstellungen.

Ereignisdatenbeschreibungen

Wenn Sie Systemprotokollereignisse herunterladen oder mithilfe der SystemLog-API abrufen, sind die folgenden Daten enthalten:

- **RecordID:** Der eindeutige Bezeichner für das Ereignis.
- **UtcTimestamp:** Das Datum und die Uhrzeit (UTC) des Ereignisses.
- **CustomerID:** Die eindeutige Organisations-ID des Citrix Cloud-Kontos.
- **EventType:** Der Bezeichner für den Typ des aufgezeichneten Ereignisses. Der Ereignistyp wird im Format `OriginatingService/Actor/Action` aufgezeichnet. Beispiel: Der Ereignistyp zum Erstellen eines Administrators ist `platform/administrator/create`.
- **TargetID:** Die ID des Systemobjekts, das betroffen oder geändert wurde.
- **TargetDisplayName:** Der Anzeigename des Systemobjekts, das betroffen oder geändert wurde. Beispiel: Name eines Administrators, der erstellt wurde.
- **TargetEmail:** Die E-Mail-Adresse des Systemobjekts. Beispiel: E-Mail-Adresse eines Administrators, der erstellt wurde.
- **TargetUserID:** Die Benutzer-ID des Systemobjekts, das betroffen oder geändert wurde. Beispiel: Wenn Sie einen Administrator erstellen, ist die TargetUserID die Benutzer-ID des Administrators, der erstellt wurde.
- **TargetType:** Die Zielkategorie für das Ereignis.
- **BeforeChanges** und **AfterChanges:** Der Inhalt der Objektfelder vor bzw. nach dem Ereignis. Für einige Ereignisse beinhalten diese Objektfelder:
  - CustomerID
  - Benutzerprinzipal
  - UserID
  - Administratorzugriffstyp, z. B. “Benutzerdefinierter Zugriff”oder “Vollzugriff”
  - CreatedDate
  - UpdatedDate
  - DisplayName
- **AgentID:** Die Ereigniskategorie.

- **ActorID:** Die ID des Systemobjekts, das Initiator des Ereignisses war. Zum Erstellen eines Administrators ist dies beispielsweise die Objekt-ID des Administrators, der einen anderen Benutzer in das Citrix Cloud-Konto eingeladen hat.
- **ActorDisplayName:** Der Anzeigename der Person oder Entität, die das Ereignis initiiert hat. Zum Beispiel der Name des Administrators, der einen anderen Benutzer in das Citrix Cloud-Konto eingeladen hat.
- **ActorType:** Der Dienst, der das Ereignis generiert hat.
- **EventMessage:** Die kurze Beschreibung des aufgetretenen Ereignisses.

Systemprotokollereignisse für die Citrix Cloud-Plattform

July 13, 2023

In diesem Artikel werden die Ereignisdaten beschrieben, die das Systemprotokoll für die Citrix Cloud-Plattform erfasst. Weitere Informationen zu Systemprotokollereignisdaten finden Sie unter Referenz zu Systemprotokollereignissen.

Weitere Informationen zum Systemprotokoll finden Sie unter Systemprotokoll.

Azure AD-Mandanten

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Azure AD-Mandant verbunden	platform/identityprovider/azuread/connect	Directory	Administrator		Ja	No
Azure AD-Mandant getrennt	platform/identityprovider/azuread/disconnect	Directory	Administrator		Ja	No

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Akteur-ID	Aufzeichnung aktueller Objekt-felder vor dem Ereignis	Aufzeichnung aktual-isierter Objekt-felder nach dem Ereignis
Azure AD auth domain name changed	platform/identity	provider/azuread/authdomain	customer	CustomerName	No	No
Azure AD auth domain name change failed	platform/identity	provider/azuread/authdomain	customer	CustomerName	No	No

Citrix Cloud-Administratoren und sichere Clients

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Vom Administrator erstellt	platform/administrator	administrator	system	No	Ja
Administratoreinladung gesendet	platform/administrator	administrator	Administrator	No	Ja
Administratorrollen oder -berechtigungen aktualisiert	platform/administrator	administrator	Administrator	Ja	Ja
Vom Administrator gelöscht	platform/administrator	administrator	Administrator	No	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Sicherer Client erstellt	platform/clientadministrator/create	Dienst	System	No	Ja
Sicherer Client gelöscht	platform/clientadministrator/delete	Dienst	Administrator	Ja	No
Administratorgruppe erstellt	platform/administratorgroup/create	administratorgroup		No	Ja
Rollen oder Berechtigungen der Administratorgruppe aktualisiert	platform/administratorgroup/update	administratorgroup		Ja	Ja
Administratorgruppe gelöscht	platform/administratorgroup/delete	administratorgroup	Administrator	Ja	No

Gerätezurücksetzung für Active Directory plus Token

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Zurücksetzen des Gerätetokens des Abonnenten abgeschlossen	platform/authentication/device/delete	subscriber	Administrator	No	Ja

Domänenverwaltung

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Domäne entfernt	platform/domain/remove	Directive	Administrator	No	No

Netzwerkspeicherorte

Ereignismeldung	Ereignistyp	Ziel-ID	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Netzwerkspeicherort erstellt	sdwan/networklocation/create	Die ID des Netzwerkspeicherorts, der erstellt wurde	Der Name des Administrators, der den Netzwerkspeicherort hinzugefügt hat	No	Ja
Netzwerkspeicherort aktualisiert	sdwan/networklocation/edit	Die ID des Netzwerkspeicherorts, der geändert wurde	Der Name des Administrators, der den Netzwerkspeicherort geändert hat	Ja	Ja
Netzwerkspeicherort gelöscht	sdwan/networklocation/delete	Die ID des Netzwerkspeicherorts, der gelöscht wurde	Der Name des Administrators, der den Netzwerkspeicherort gelöscht hat	Ja	No

Ressourcenstandorte

Ereignismeldung	Ereignistyp	Ziel-ID	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Resource Location created	platform/resourcelocation/create	Name des Ressourcenstandorts, der erstellt wurde	Name des Administrators, der den Ressourcenstandort erstellt hat	Ja	Ja
Resource Location updated	platform/resourcelocation/update	Der Name des geänderten Ressourcenstandorts	Name des Administrators, der den Ressourcenstandort geändert hat	Ja	Ja
Resource Location deleted	platform/resourcelocation/delete	Der Name des gelöschten Ressourcenstandorts	Name des Administrators, der den Ressourcenstandort gelöscht hat	Ja	Ja

Systemprotokollereignisse für Connectors

April 29, 2022

In diesem Artikel werden die Ereignisdaten beschrieben, die das Systemprotokoll für Citrix Cloud Connector und Connectorgerät für Cloudservices erfasst. Weitere Informationen zu Systemprotokollereignisdaten finden Sie unter Referenz zu Systemprotokollereignissen.

Weitere Informationen zum Systemprotokoll finden Sie unter Systemprotokoll.

Connectorregistrierung

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Connector registriert	platform/edgeservice/cloud/create	**Cloud Connector** oder **Connectorgerät**	Der Administrator, der den Connector registriert hat	Ja	Ja
Connector gelöscht	platform/edgeservice/cloud/delete	**Cloud Connector** oder **Connectorgerät**	Der Administrator, der den Connector gelöscht hat	Ja	Ja

Connector-Updates

Ereignismeldung	Ereignistyp	Ziel-ID	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Wartungsfenster für Ressourcenstandort aktualisiert	platform/resourcelocation/maintenancewindow	Der Name des geänderten Ressourcenstandorts	Der Administrator, der die Konfiguration geändert hat	Ja	Ja
Connector-Upgrade wurde vom Administrator ausgelöst	platform/edgeservice/cloud/manualupgrade	**Cloud Connector** oder **Connectorgerät**	Der Administrator, der das Update initiiert hat	Nein	Nein

Ereignismeldung	Ereignistyp	Ziel-ID	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Connector-Upgrade gestartet	platform/edgeservice/upgradestarted	**Cloud Connector** oder **Connectorgerät**	**Automatisch** oder der Administrator, der das Update initiiert hat	Ja	Nein
Connector-Upgrade abgeschlossen	platform/edgeservice/upgradecompleted	**Cloud Connector** oder **Connectorgerät**	**Automatisch** oder der Administrator, der das Update initiiert hat	Nein	Ja

Connector –öffentliche Schlüssel

Ereignismeldung	Ereignistyp	Ziel-ID	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Public Key added to trust	platform/authentication/createedgeser	Der verkey	Administrator, der den Vorgang ausgeführt hat	Nein	Nein
Public Key removed from trust	platform/authentication/deleteedgeser	Der verkey	Administrator, der den Vorgang ausgeführt hat	Nein	Nein

Systemprotokollereignisse für die Lizenzierung in Citrix Cloud

April 29, 2022

In diesem Artikel werden die Ereignisdaten beschrieben, die das Systemprotokoll für die Registrierung der On-Premises-Citrix Lizenzierung bei Citrix Cloud erfasst. Weitere Informationen zu Systemprotokollereignisdaten finden Sie unter Referenz zu Systemprotokollereignissen.

Weitere Informationen zum Systemprotokoll finden Sie unter Systemprotokoll.

On-Premises-Lizenzserver

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
On-Premise-Lizenzserver gelöscht	lui/onpremlicenseserver/delete	Lizenzserver	Der Administrator, der den Lizenzserver gelöscht hat	Nein	Nein
Fehler beim Löschen der On-Premise-Lizenzserver	lui/onpremlicenseserver/delete	Lizenzserver	Der Administrator, der versucht hat, den Lizenzserver zu löschen	Nein	Nein

Cloudservicelizenzierung

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Citrix Cloud-Servicelizenzen freigegeben	lui/cloudlicense/release	CloudLicense	Der Administrator, der Lizenzen für den Cloudservice freigegeben hat	Nein	Nein
Fehler beim Freigeben von Citrix Cloud-Servicelizenzen	lui/cloudlicense/releasefailed	CloudLicense	Der Administrator, der versucht hat, Lizenzen für den Cloudservice freizugeben	Nein	Nein

License Usage Insights für Citrix Service Provider

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
On-premise Benutzerlis-tendaten von Partner exportiert	lui/csp/userlistdataexport	Lizenzierung	Der Administrator, der die Daten der Partner-Benutzerliste exportiert hat	Nein	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Exportieren der on-premise Benutzerlis-tendaten von Partner	lui/csp/userlistdataexportfailed	Lizenzierung	Der Administrator, der versucht hat, die Daten der Partner-Benutzerliste zu exportieren	Nein	Nein

Lizenznutzung für Cloudservices und On-Premises-Produkte

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Lizenznutzungsdaten exportiert	lui/cloudlicense/usagedataexport	Cloudlizenzierung oder Lizenzierung	Der Administrator, der Lizen-znutzungs-daten exportiert hat	Nein	Nein
Fehler beim Exportieren von Lizen-znutzungs-daten	lui/cloudlicense/usagedataexportfailed	Cloudlizenzierung oder Lizenzierung	Der Administrator, der versucht hat, Lizen-znutzungs-daten zu exportieren	Nein	Nein

Systemprotokollereignisse für Secure Private Access

October 16, 2022

In diesem Artikel werden die Ereignisdaten beschrieben, die das Systemprotokoll für Secure Private Access Service erfasst. Weitere Informationen zu Systemprotokollereignisdaten finden Sie unter Referenz zu Systemprotokollereignissen.

Weitere Informationen zum Systemprotokoll finden Sie unter Systemprotokoll.

Web- und SaaS-Anwendungen

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Web-/SaaS-Anwendung erstellt	swa/websaasppplicationcreate	web/saasapplication	Nein	Ja
Web-/SaaS-Anwendung aktualisiert	swa/websaasppplicationupdate	web/saasapplication	Ja	Ja
Web-/SaaS-Anwendung gelöscht	swa/websaasppplicationdelete	web/saasapplication	Ja	Nein
Fehler beim Erstellen der Web-/SaaS-Anwendung	swa/websaasppplicationcreatefailed	web/saasapplication	Nein	Nein
Fehler beim Aktualisieren der Web-/SaaS-Anwendung	swa/websaasppplicationupdatefailed	web/saasapplication	Ja	Ja
Fehler beim Löschen der Web-/SaaS-Anwendung	swa/websaasppplicationdeletefailed	web/saasapplication	Ja	Ja

Benutzer- und Gruppenabonnements

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Benutzer-/Gruppenabonnement hinzugefügt	swa/websaaspplicationsubscription/subscribers	websaaspplicationsubscription	Nein	Ja
Benutzer-/Gruppenabonnement entfernt	swa/websaaspplicationsubscription/subscribers	websaaspplicationsubscription	Nein	Ja
Benutzer-/Gruppenabonnement fehlgeschlagen	swa/websaaspplicationsubscription/subscribefailed	websaaspplicationsubscription	Nein	Nein
Fehler beim Abbestellen des Benutzer-/Gruppenabonnements	swa/websaaspplicationsubscription/unsubscribefailed	websaaspplicationsubscription	Nein	Nein

Kontextbezogene Richtlinien

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Kontextbezogene Richtlinie erstellt	swa/contextualpolicy/create	contextualpolicy	Nein	Ja
Kontextbezogene Richtlinie aktualisiert	swa/contextualpolicy/update	contextualpolicy	Ja	Ja
Kontextbezogene Richtlinie gelöscht	swa/contextualpolicy/delete	contextualpolicy	Ja	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Erstellen der kontextbezogenen Richtlinie	swa/contextualpolicy/createfailed	contextualpolicy	Nein	Nein
Fehler beim Aktualisieren der kontextbezogenen Richtlinie	swa/contextualpolicy/updatefailed	contextualpolicy	Nein	Nein
Fehler beim Löschen der kontextbezogenen Richtlinie	swa/contextualpolicy/deletefailed	contextualpolicy	Ja	Nein

Anwendungsdomänen

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Anwendungsdomäne erstellt	swa/applicationdomain/create	applicationdomain	Nein	Ja
Anwendungsdomäne aktualisiert	swa/applicationdomain/update	applicationdomain	Ja	Ja
Anwendungsdomäne gelöscht	swa/applicationdomain/delete	applicationdomain	Ja	Nein
Fehler beim Erstellen der Anwendungsdomäne	swa/applicationdomain/createfailed	applicationdomain	Nein	Nein
Fehler beim Aktualisieren der Anwendungsdomäne	swa/applicationdomain/updatefailed	applicationdomain	Ja	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Löschen der Anwendungs-domäne	swa/applicationdomain/delete/failed	applicationdomain	Ja	Nein

Browsererweiterungseinstellungen

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Einstellungen der Browser-erweiterung aktualisiert	swa/browserextensionsettings/update	browserextensionsettings	Ja	Ja
Fehler beim Aktualisieren der Browser-erweiterungsein-stellungen	swa/browserextensionsettings/update/failed	browserextensionsettings	Ja	Nein

Website-URL-Listen und -Filterkategorien

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Websitefilterlisten und -kategorien aktiviert	swa/website/filterlists/enabled/update	websitefilterlistcategory	Ja	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Websitefilterlisten aktiviert und -filterkategorien deaktiviert	swa/website/filterlist/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature	Ja	
Websitefilterlisten deaktiviert und -filterkategorien aktiviert	swa/website/filterlist/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature	Ja	
Websitefilterlisten und -kategorien deaktiviert	swa/website/filterlist/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature	Ja	
Fehler beim Aktivieren von Websitefilterlisten und -kategorien	swa/website/filterlist/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature		failed
Fehler beim Aktivieren von Websitefilterlisten und Deaktivieren von Websitefilterkategorien	swa/website/filterlist/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature		failed
Fehler beim Deaktivieren von Websitefilterlisten und Aktivieren von Websitefilterkategorien	swa/website/filterlist/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature		failed
Fehler beim Deaktivieren von Websitefilterlisten und -kategorien	swa/website/filterlist/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature		failed

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Website-URL-Liste erstellt	swa/websiteurlfiltering/create	website/urlfilteringlist	Nein	Ja
Website-URL-Liste aktualisiert	swa/websiteurlfiltering/update	website/urlfilteringlist	Ja	Ja
Website-URL-Liste gelöscht	swa/websiteurlfiltering/delete	website/urlfilteringlist	Ja	Nein
Fehler beim Erstellen der Website-URL-Liste	swa/websiteurlfiltering/createfailed	website/urlfilteringlist	Nein	Nein
Fehler beim Aktualisieren der Website-URL-Liste	swa/websiteurlfiltering/updatefailed	website/urlfilteringlist	Ja	Nein
Fehler beim Löschen der Website-URL-Liste	swa/websiteurlfiltering/deletefailed	website/urlfilteringlist	Ja	Nein
Website-URL-Filterkategorie erstellt	swa/websiteurlfiltercategory/create	category/urlfiltercategory	Nein	Ja
Website-URL-Filterkategorie aktualisiert	swa/websiteurlfiltercategory/update	category/urlfiltercategory	Ja	Ja
Website-URL-Filterkategorie gelöscht	swa/websiteurlfiltercategory/delete	category/urlfiltercategory	Ja	Nein
Fehler beim Erstellen der Website-URL-Filterkategorie	swa/websiteurlfiltercategory/createfailed	category/urlfiltercategory	Nein	Nein
Fehler beim Aktualisieren der Website-URL-Filterkategorie	swa/websiteurlfiltercategory/updatefailed	category/urlfiltercategory	Ja	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Löschen der Website-URL-Filterkategorie	swa/websiteurlfiltercategory/deletefailed	category	Ja	Nein

Voreingestellte Websitefilterkategorien

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Voreingestellte Websitefilterkategorie aktualisiert	swa/websiteurlfiltercategorypreset/updated	categorypreset	Ja	Ja
Fehler beim Aktualisieren der voreingestellten Websitefilterkategorie	swa/websiteurlfiltercategorypreset/updatefailed	categorypreset	Ja	Ja

Listen und Filterkategorien für blockierte Website-URLs

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Liste mit blockierten Website-URLs erstellt	swa/websiteurlfilterweblist/blockedcreated	weblist	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Liste mit blockierten Website-URLs aktualisiert	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	Nein	Ja
Liste mit blockierten Website-URLs gelöscht	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	Nein	Ja
Fehler beim Erstellen von Liste mit blockierten Website-URLs	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	Nein	Ja
Fehler beim Aktualisieren von Liste mit blockierten Website-URLs	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	Nein	Ja
Fehler beim Löschen von Liste mit blockierten Website-URLs	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	Nein	Ja
Filterkategorie für blockierte Website-URLs erstellt	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	Nein	Ja
Filterkategorie für blockierte Website-URLs aktualisiert	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	Nein	Ja
Filterkategorie für blockierte Website-URLs gelöscht	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Erstellen von Filterkategorie für blockierte Website-URLs	swa/websiteurlfiltercategory/blockedlist/create/failed	category/blockedlist	Nein	Ja
Fehler beim Aktualisieren von Filterkategorie für blockierte Website-URLs	swa/websiteurlfiltercategory/blockedlist/update/failed	category/blockedlist	Nein	Ja
Fehler beim Löschen von Filterkategorie für blockierte Website-URLs	swa/websiteurlfiltercategory/blockedlist/delete/failed	category/blockedlist	Nein	Ja

Listen und Filterkategorien für zulässige Website-URLs

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Liste mit zulässigen Website-URLs erstellt	swa/websiteurlfilterwebsite/allowedlist/create	website/allowedlist	Nein	Ja
Liste mit zulässigen Website-URLs aktualisiert	swa/websiteurlfilterwebsite/allowedlist/update	website/allowedlist	Nein	Ja
Liste mit zulässigen Website-URLs gelöscht	swa/websiteurlfilterwebsite/allowedlist/delete	website/allowedlist	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Erstellen von Liste mit zulässigen Website-URLs	swa/websiteurlfilterwebsiteallowlist/createfailed	websiteallowlist	Nein	Ja
Fehler beim Aktualisieren von Liste mit zulässigen Website-URLs	swa/websiteurlfilterwebsiteallowlist/updatefailed	websiteallowlist	Nein	Ja
Fehler beim Löschen von Liste mit zulässigen Website-URLs	swa/websiteurlfilterwebsiteallowlist/deletefailed	websiteallowlist	Nein	Ja
Filterkategorie für zulässige Website-URLs erstellt	swa/websiteurlfiltercategoryallowlist/create	categoryallowlist	Nein	Ja
Filterkategorie für zulässige Website-URLs aktualisiert	swa/websiteurlfiltercategoryallowlist/update	categoryallowlist	Nein	Ja
Filterkategorie für zulässige Website-URLs gelöscht	swa/websiteurlfiltercategoryallowlist/delete	categoryallowlist	Nein	Ja
Fehler beim Erstellen von Filterkategorie für zulässige Website-URLs	swa/websiteurlfiltercategoryallowlist/createfailed	categoryallowlist	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Aktualisieren von Filterkategorie für zulässige Website-URLs	swa/websiteurlfiltercategory/allowed/updatefailed	category/allowed/websiteurlfilteringlist	Nein	Ja
Fehler beim Löschen von Filterkategorie für zulässige Website-URLs	swa/websiteurlfiltercategory/allowed/deletefailed	category/allowed/websiteurlfilteringlist	Nein	Ja

Listen und Filterkategorien für zu Remote Browser Isolation (zuvor “Secure Browser”) umgeleitete Website-URLs

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Agent-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Liste mit zu Secure Browser umgeleiteten Website-URLs erstellt	swa/websiteurlfilteringlist/redirected/create	webs
Liste mit zu Secure Browser umgeleiteten Website-URLs aktualisiert	swa/websiteurlfilteringlist/redirected/update
Liste mit zu Secure Browser umgeleiteten Website-URLs gelöscht	swa/websiteurlfilteringlist/redirected/delete	we
Fehler beim Erstellen von Liste mit zu Secure Browser umgeleiteten Website-URLs	swa/websiteurlfilteringlist/redi
Fehler beim Aktualisieren von Liste mit zu Secure Browser umgeleiteten Website-URLs	swa/websiteurlfilteringlist/
Fehler beim Löschen von Liste mit zu Secure Browser umgeleiteten Website-URLs	swa/websiteurlfilteringlist/redi
Filterkategorie für zu Secure Browser umgeleitete Website-URLs erstellt	swa/websiteurlfiltercategory/redirected/c
Filterkategorie für zu Secure Browser umgeleitete Website-URLs aktualisiert	swa/websiteurlfiltercategory/redirect
Fehler beim Erstellen von Filterkategorie für zu Secure Browser umgeleitete Website-URLs	swa/websiteurlfiltercate
Fehler beim Erstellen von Filterkategorie für zu Secure Browser umgeleitete Website-URLs	swa/websiteurlfiltercate
Fehler beim Aktualisieren von Filterkategorie für zu Secure Browser umgeleitete Website-URLs	swa/websiteurlfiltercategory/redirected/updatefailed	websiteurlfilteringlist	Nein	Ja
Fehler beim Löschen von Filterkategorie für zu Secure Browser umgeleitete Website-URLs	swa/websiteurlfiltercate

Systemprotokollereignisse für Citrix Workspace

April 29, 2022

In diesem Artikel werden die Ereignisdaten beschrieben, die das Systemprotokoll für Citrix Workspace erfasst. Weitere Informationen zu Systemprotokollereignisdaten finden Sie unter Referenz zu Systemprotokollereignissen.

Weitere Informationen zum Systemprotokoll finden Sie unter Systemprotokoll.

Workspace-URL

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Workspace-URL aktualisiert	wxp/url/update	subscriber	Der Administrator, der die URL aktualisiert hat	Ja	Ja
Fehler beim Aktualisieren der Workspace-URL	wxp/url/updatefailed	subscriber	Der Administrator, der versucht hat, die URL zu aktualisieren	Ja	Ja
Workspace-URL aktiviert	wxp/url/enable	subscriber	Der Administrator, der die Anpassung der Workspace-URL aktiviert hat	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Aktivieren der Workspace-URL	wxp/url/enablefailed	subscriber	Der Administrator, der versucht hat, die Anpassung der Workspace-URL zu aktivieren	Nein	Ja
Workspace-URL deaktiviert	wxp/url/disable	subscriber	Der Administrator, der die Anpassung der Workspace-URL deaktiviert hat	Nein	Ja
Fehler beim Deaktivieren der Workspace-URL	wxp/url/disablefailed	subscriber	Der Administrator, der versucht hat, die Anpassung der Workspace-URL zu deaktivieren	Nein	Ja

Workspaceauthentifizierung

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Workspace-Identitätsanbieter aktualisiert	wxp/identityprovider/update	subscriber	Der Administrator, der die Workspace-Authentifizierungsmethode aktualisiert hat	Ja	Ja
Fehler beim Aktualisieren des Identitätsanbieters	wxp/identityprovider/updatefailed	subscriber	Der Administrator, der versucht hat, die Workspace-Authentifizierungsmethode zu aktualisieren	Ja	Ja

Citrix Verbundauthentifizierungsdienst

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Workspace-Verbundauthentifizierungsdienst (FAS) aktiviert	wxp/fas/enable	subscriber	Der Administrator, der FAS aktiviert hat	Nein	Ja
Fehler beim Aktivieren von Workspace-Verbundauthentifizierungsdienst (FAS)	wxp/fas/enablefailed	subscriber	Der Administrator, der versucht hat, FAS zu aktivieren	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Workspace-Verbundauthentifizierungsdienst (FAS) deaktiviert	wxp/fas/disable	subscriber	Der Administrator, der FAS deaktiviert hat	Nein	Ja
Fehler beim Deaktivieren von Workspace-Verbundauthentifizierungsdienst (FAS)	wxp/fas/disablefailed	subscriber	Der Administrator, der versucht hat, FAS zu deaktivieren	Nein	Ja

Favoriten

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Workspace-Favoriten aktiviert	wxp/favorites/enable	subscriber	Der Administrator, der Favoriten aktiviert hat	Nein	Ja
Fehler beim Aktivieren der Workspace-Favoriten	wxp/favorites/enablefailed	subscriber	Der Administrator, der versucht hat, Favoriten zu aktivieren	Nein	Ja
Workspace-Favoriten deaktiviert	wxp/favorites/disable	subscriber	Der Administrator, der Favoriten deaktiviert hat	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Deaktivieren der Workspace-Favoriten	wxp/favorites/disable/failed	subscriber	Der Administrator, der versucht hat, Favoriten zu deaktivieren	Nein	Ja

Kennwort ändern

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Richtlinie für Workspace-Kennwortänderungsoptionen aktualisiert	wxp/changepasswordoptions/update	policy	Der Administrator, der die Richtlinie für die Kennwortänderung in Citrix Workspace aktualisiert hat	Ja	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Aktualisieren der Richtlinie für Workspace-Kennwortänderungsoptionen	wxp/changepasswordoptions/updatepolicyfailed	workspaceconfiguration	Der Administrator, der versucht hat, die Richtlinie für die Kennwortänderung in Citrix Workspace zu aktualisieren	Ja	Ja
Workspace-Kennwortänderungsoptionen aktiviert	wxp/changepasswordoptions/enabled	workspaceconfiguration	Der Administrator, der die Einstellung zum Ändern von Kennwörtern in Citrix Workspace aktiviert hat	Nein	Ja
Fehler beim Aktivieren der Workspace-Kennwortänderungsoptionen	wxp/changepasswordoptions/enablefailed	workspaceconfiguration	Der Administrator, der versucht hat, die Einstellung zum Ändern von Kennwörtern in Citrix Workspace zu aktivieren	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Workspace-Kennwortänderungsoptionen deaktiviert	wxp/changepasswordoptions/disable	wxpchangepasswordoptions	Der Administrator, der die Einstellung zum Ändern von Kennwörtern in Citrix Workspace deaktiviert hat	Nein	Ja
Fehler beim Deaktivieren der Workspace-Kennwortänderungsoptionen	wxp/changepasswordoptions/disable	wxpchangepasswordoptions	Der failed Administrator, der versucht hat, die Einstellung zum Ändern von Kennwörtern in Citrix Workspace zu deaktivieren	Nein	Ja

Langlebige Token

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Langlebige Workspace-Tokenkonfiguration aktualisiert	wxp/longlivedtoken/update	subscriber	Der Administrator, der die Tokenkonfiguration aktualisiert hat	Ja	Ja
Fehler beim Aktualisieren der langlebigen Workspace-Tokenkonfiguration	wxp/longlivedtoken/updatefailed	subscriber	Der Administrator, der versucht hat, die Tokenkonfiguration zu aktualisieren	Ja	Ja

Inaktivitätstimeout für das Internet

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Workspace-Sitzungskonfiguration aktualisiert	wxp/sessions/update	Subscriber	Der Administrator, der die Leerlaufzeit für die Einstellung "Inaktivitäts-timeout für das Internet" aktualisiert hat	Ja	Ja
Fehler beim Aktualisieren der Workspace-Sitzungskonfiguration	wxp/sessions/updatefailed	Subscriber	Der Administrator, der versucht hat, die Leerlaufzeit für die Einstellung "Inaktivitäts-timeout für das Internet" zu aktualisieren	Ja	Ja

Feature-Rollout

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Zugewiesene Benutzer und Gruppen für den intelligenten Workspace aktualisiert	wxp/iws/features/subscribers/updated	subscribersgroups	Der Administrator, der die zugewiesenen Benutzer und Gruppen für den Zugriff auf Aktivitätsfeed-Benachrichtigungen in Citrix Workspace aktualisiert hat	Nein	Nein
Fehler beim Zuweisen von Benutzern und Gruppen, die für den intelligenten Workspace aktualisiert wurden	wxp/iws/features/subscribers/updatefailed	subscribersgroups	Der Administrator, der versucht hat, die zugewiesenen Benutzer und Gruppen für den Zugriff auf Aktivitätsfeed-Benachrichtigungen in Citrix Workspace zu aktualisieren	Nein	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Intelligenter Workspace aktiviert	wxp/iws/features/enable	subscriber	Der Administrator, der Aktivitätsfeed-Benachrichtigungen in Citrix Workspace aktiviert hat	Nein	Nein
Fehler beim Aktivieren des intelligenten Workspace	wxp/iws/features/enablefailed	subscriber	Der Administrator, der versucht hat, Aktivitätsfeed-Benachrichtigungen in Citrix Workspace zu aktivieren	Nein	Nein
Intelligenter Workspace deaktiviert	wxp/iws/features/disable	subscriber	Der Administrator, der Aktivitätsfeed-Benachrichtigungen in Citrix Workspace deaktiviert hat	Nein	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Deaktivieren des intelligenten Workspace	wxp/iws/features/disable/failed	wxp/iws/features/disable/failed	Der Administrator, der versucht hat, die Aktivitätsfeed-Benachrichtigungen in Citrix Workspace zu deaktivieren	Nein	Nein

SDKs und APIs

July 2, 2024

Citrix Cloud umfasst mehrere APIs, mit denen Sie Informationen abrufen und komplexe Routineaufgaben automatisieren können:

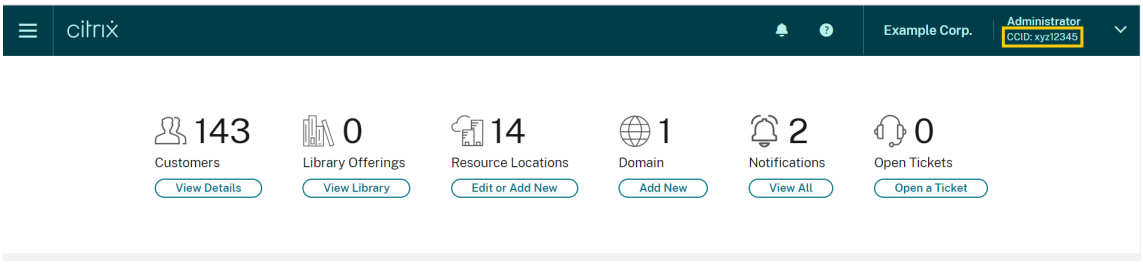
- Automatische Installation von Citrix Cloud Connector
- Erstellen und Nutzen von Berichten für die Verwaltung von Cloud-Lizenzen
- Ermitteln des Anspruchsstatus eines Kunden
- Senden von Benachrichtigungen an Citrix Cloud-Administratoren
- Abrufen von Systemprotokollereignissen
- Abrufen von Details zu Ihren Ressourcenstandorten zur Verwendung mit anderen APIs

Verschiedene Citrix Cloud-Dienste bieten auch SDKs und APIs, mit denen Sie Informationen abrufen, Daten abfragen und Verwaltungsaufgaben ausführen können.

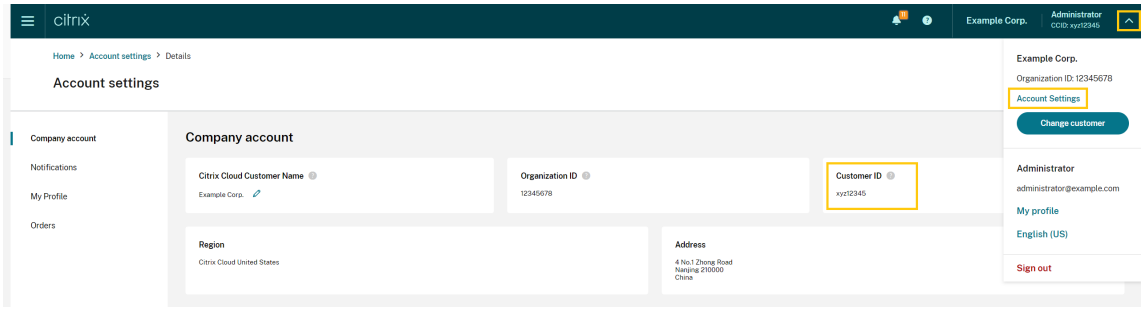
Sichere Clients

Um Citrix Cloud-APIs verwenden zu können, müssen Sie einen sicheren Client erstellen, der für Sie auf Citrix Cloud zugreift. Um einen sicheren Client zu erstellen, müssen Sie die Kunden-ID Ihres Citrix Cloud-Kontos angeben. Die Kunden-ID finden Sie an den folgenden Stellen in der Verwaltungskonsole:

- Oben rechts, unterhalb Ihres Benutzernamens.



- Auf der Seite **Kontoeinstellungen**.



- Auf der Seite **API-Zugriff**.

Geerbte Berechtigungen

Sichere Clients sind in Citrix Cloud mit einem Administrator und einer Kunden-ID verknüpft. Das bedeutet, dass Ihre sicheren Clients die gleichen Berechtigungen erben, die Sie unter einer spezifischen Kunden-ID haben. Wenn Sie über Vollzugriff verfügen, haben Ihre sicheren Clients auch Vollzugriff. Wenn Ihre Berechtigung zu einem späteren Zeitpunkt eingeschränkt wird, erben die sicheren Clients, die Sie bereits erstellt haben, automatisch die eingeschränkten Berechtigungen.

Anweisungen zum Erstellen sicherer Clients finden Sie unter Erste Schritte mit Citrix Cloud-APIs in der Citrix Dokumentation für Entwickler.

Cloud-Lizenzierungs-APIs

Unternehmenskunden können Cloud-Lizenzierungs-APIs verwenden, um Verwaltungsaufgaben wie das Exportieren von Nutzungsdaten und das Freigeben zugewiesener Lizenzen auszuführen. Citrix-Partner können mit diesen diese APIs Übersichts- und historische Daten für On-Premises-Citrix Virtual Apps and Desktops und Citrix DaaS abrufen.

Weitere Informationen finden Sie unter APIs to manage Citrix cloud licensing in der Citrix Dokumentation für Entwickler.

SystemLog-API

Mit der SystemLog-API können Sie Ereignisse abrufen, die in Ihrem Citrix Cloud-Konto in einem von Ihnen angegebenen Zeitraum aufgetreten sind. Weitere Informationen zur Verwendung dieser API finden Sie in der Citrix Developer-Dokumentation unter Citrix Cloud –SystemLog.

API für Ressourcenstandorte

Die API für Ressourcenstandorte ermöglicht den Abruf von Informationen über Ihre Ressourcenstandorte zur Verwendung in anderen Anwendungen und Skripts. Beispiel: Sie möchten Citrix Cloud Connector automatisch an einem von mehreren Ressourcenstandorten in Ihrem Citrix Cloud-Konto installieren. Sie können mit der API die ID des Ressourcenstandorts abrufen und an Ihr Installationsskript übergeben.

Weitere Informationen zur Verwendung dieser API finden Sie in der Citrix Developer-Dokumentation unter Citrix Cloud –Resource Location.

API für Servicesanspruch

Die API für Servicesanspruch ruft die Services ab, auf die ein Kunde Anspruch hat, die verbleibenden Tage jedes Anspruchs und die Zahl der von dem Kunden erworbenen Ansprüche. Weitere Informationen zur Verwendung dieser API finden Sie in der Citrix Developer-Dokumentation unter Citrix Cloud – Service Entitlement.

API für Benachrichtigungen

Mit dieser API können Sie Benachrichtigungen an andere Citrix Cloud-Administratoren senden. Die Empfänger erhalten Ihre Benachrichtigungen über die Seite Benachrichtigungen in der Verwaltungskonsole.

SDKs und APIs für andere Services

Informationen zu SDKs und APIs für andere Citrix Cloud-Services finden Sie in den folgenden Artikeln:

- Digital workspaces: SDKs und APIs für Workspace-Services wie Citrix DaaS und Citrix Workspace.
- App Delivery and Security: Umfasst SDKs und APIs für Netzwerk und Anwendungsbereitstellungsdienste wie Console, Intelligent Traffic Management und SD-WAN Orchestrator.

Weitere Informationen

Informationen darüber, wie Sie mit Citrix Cloud-APIs und sicheren Clients komplexe Vorgänge wie die Migration in die Cloud und die Konfiguration der Authentifizierung mit Push-Token ausführen, finden Sie in den folgenden Tech Zone-Artikeln:

- PoC Guide: nFactor for Citrix Gateway Authentication with Push Token
- Deployment Guide: Migrating Citrix Virtual Apps and Desktops from VMware vSphere to Citrix Virtual Apps and Desktops service on Microsoft Azure
- PoC Guide: Automated Configuration Tool

Citrix Cloud für Partner

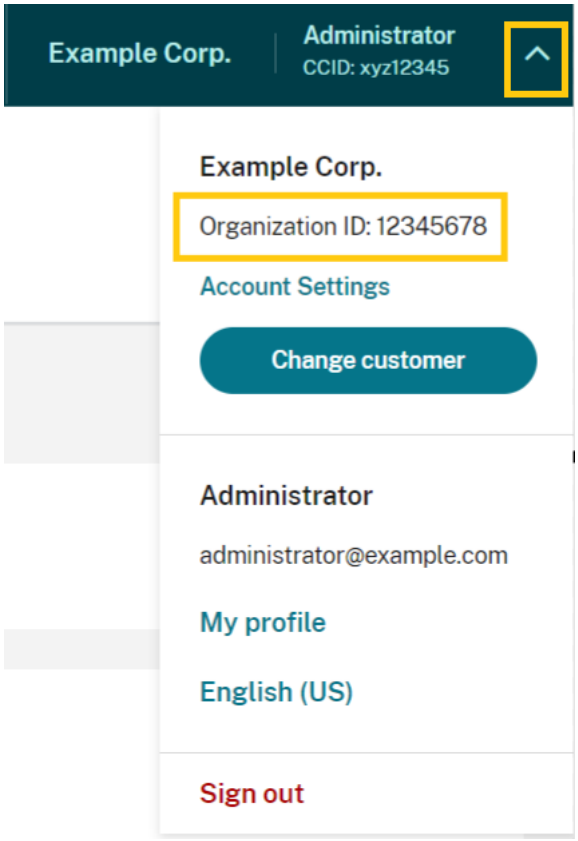
April 5, 2024

Citrix Cloud enthält Services, Features und Optionen für Kunden und Partner. In diesem Abschnitt werden Features aufgeführt, die es Citrix Partnern ermöglichen, gemeinsam mit Kunden an Services und Lösungen von Citrix Cloud zu arbeiten.

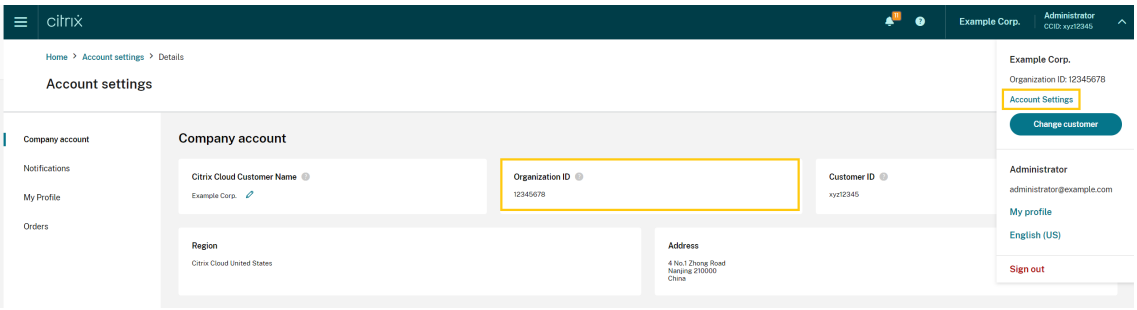
Partneridentifizierung

Partner werden in Citrix Cloud anhand ihrer Citrix Organisations-ID (ORGID) identifiziert. Partner können die mit ihrem Citrix Cloud-Konto verknüpfte ORGID in der Citrix Cloud-Verwaltungskonsole folgendermaßen anzeigen:

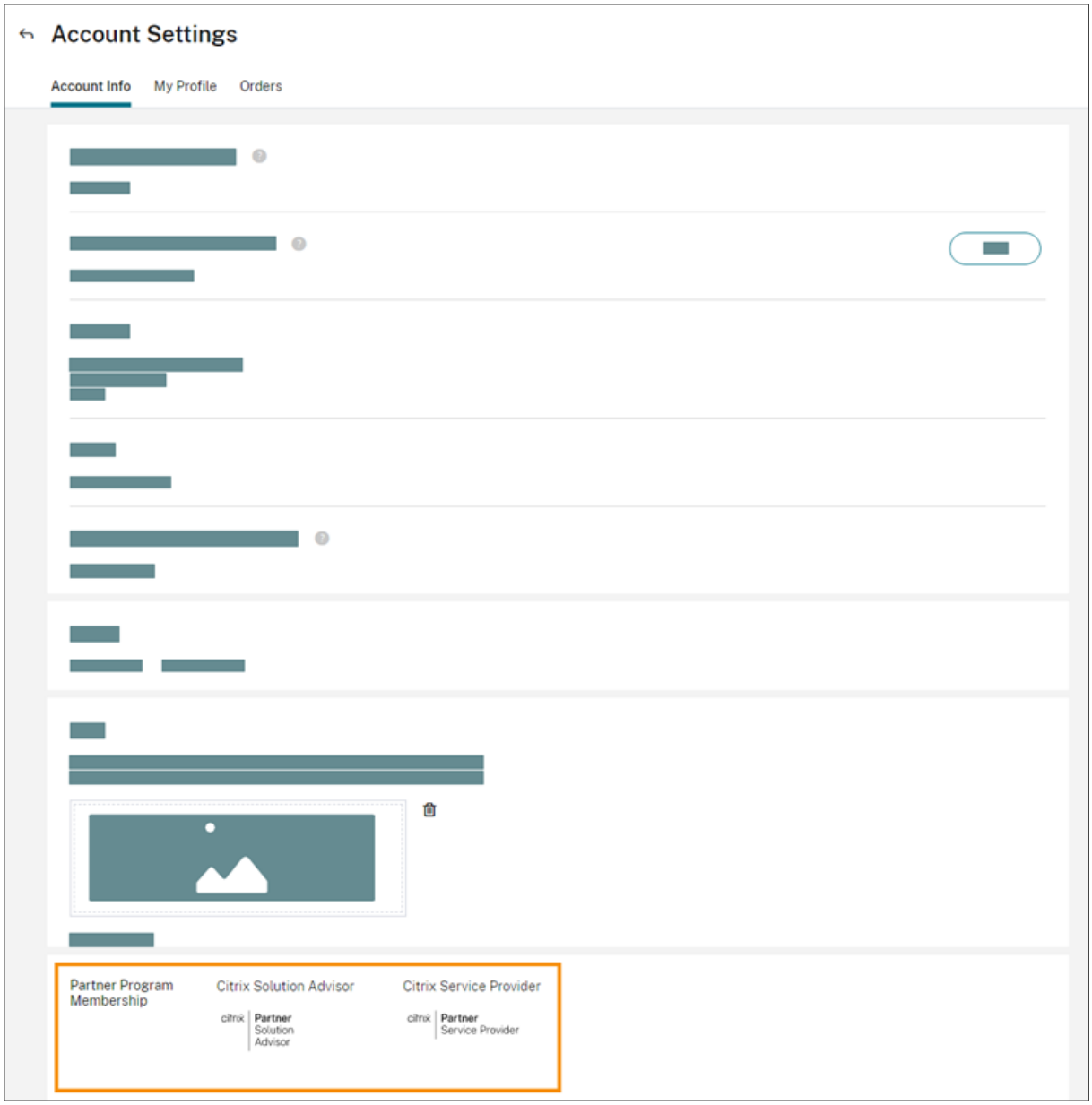
- Über das Kundenmenü: Klicken Sie in der oberen rechten Ecke der Konsole auf Ihren Kundennamen. Ihre ORGID wird unter Ihrem Firmennamen im Menü angezeigt.



- Auf der Seite **Kontoeinstellungen**: Wählen Sie im Kundenmenü in der oberen rechten Ecke **Kontoeinstellungen**.

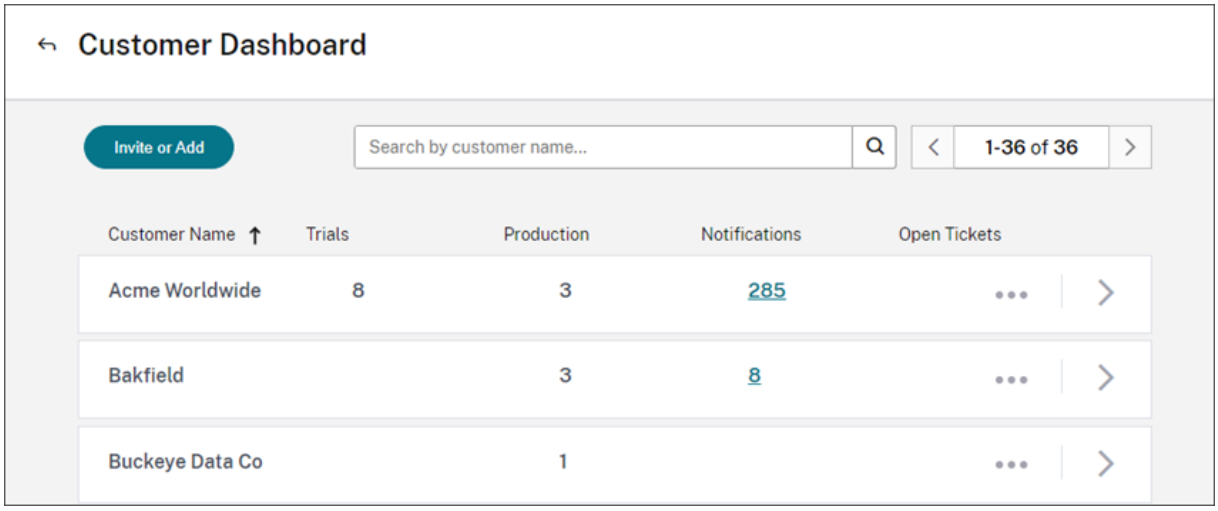


Falls die ORGID im Konto auf ein aktives Mitglied eines Citrix Partnerprogramms verweist (z. B. Citrix Solution Advisor oder Citrix Service Provider), zeigt der Programmbadge an, dass dieses Konto einem Citrix Partner gehört. Die Partneridentifizierung kann dann verwendet werden, um den Zugriff auf zusätzliche Services oder Features in der Cloud zu steuern.

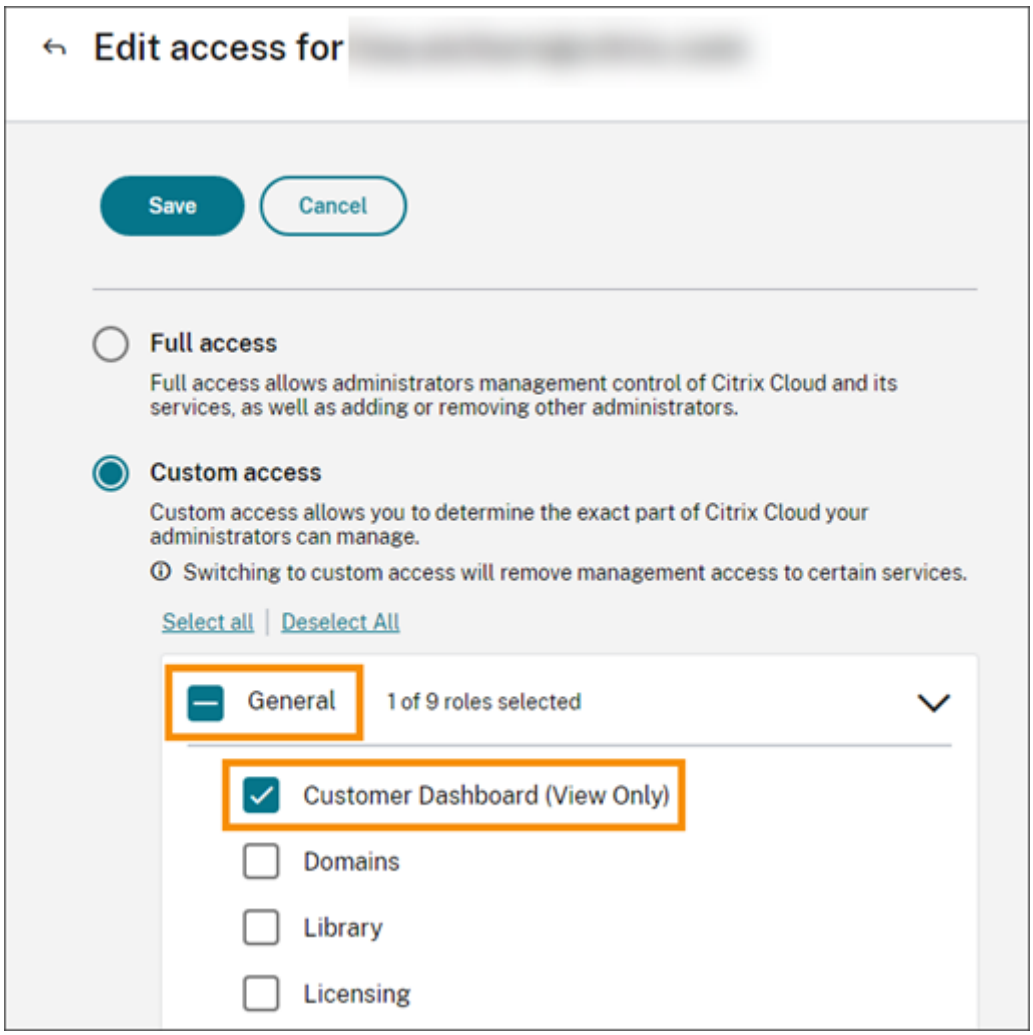


Kundendashboard

Mit dem Kundendashboard können Partner den Status mehrerer Citrix Cloud-Kunden in einer konsolidierten Ansicht anzeigen. Damit ein Kunde im Dashboard erscheint, müssen Partner und Kunde miteinander verbunden sein. Das Kundendashboard ist für Citrix Cloud-Konten mit Partnerbadge verfügbar.



Standardmäßig können Administratoren mit Vollzugriff das Kundendashboard anzeigen. Administratoren mit benutzerdefiniertem Zugriff können das Dashboard anzeigen, wenn die Berechtigung **Kundendashboard (schreibgeschützt)** ausgewählt ist. Weitere Hinweise zu Administratorrechten in Citrix Cloud finden Sie unter Ändern von Administratorberechtigungen.



Partnerverbindungen mit Kunden

Partner, die gemeinsam mit Kunden an Citrix Cloud-Lösungen arbeiten, können eine vertrauenswürdige Verbindung zwischen ihren Konten einrichten. Diese Beziehung auf Kontoebene erleichtert es dem Kunden, spezielle Informationen an den Partner zu übermitteln. Nachdem ein Kunde sich mit einem Partner verbunden hat, kann der Partner Informationen über das Citrix Cloud-Konto des Kunden und über dessen Beziehung zu Citrix anzeigen.

Das Herstellen einer Partnerverbindung bewirkt Folgendes:

- Der Kunde wird im Dashboard des Partners angezeigt.
- Der Partner wird als aktive Verbindung in den Kontoeinstellungen des Kunden angezeigt
- Der Partner erhält Einblick in die Citrix Cloud-Serviceansprüche
- Partnereinblick in Lizenznutzung und aktive Nutzung von Citrix Cloud-Ansprüchen

Sobald die Verbindung zwischen dem Partner und einem Kunden hergestellt ist, können die Partner-

administratoren grundlegende Kontoinformationen des Kunden und die von diesem aufgegebenen Bestellungen sowie Berechtigungsinformationen wie Services, Lizenzzahlen und Ablaufdaten anzeigen.

Partnerverbindungen mit Kunden laufen nicht ab.

Verbindungen mit mehreren Partnern oder Kunden

Partner können Verbindungen mit mehreren Kunden herstellen. Partner können mit bis zu 100 Kundenkonten verknüpft werden. Wenn ein Partner mehr als 100 Kundenkonten verwaltet, muss er für die zusätzlichen Kunden ein separates Partnerkonto mit einer anderen E-Mail-Adresse erstellen. Alternativ kann der Partner Kundenkonten entfernen, die er nicht mehr verwalten muss.

Kunden können Verbindungen mit mehreren Partnern herstellen. Es gibt keine Höchstgrenze für Verbindungen zwischen Kunden und Partnern.

Verbindungsbenachrichtigungen

Citrix Cloud sendet Benachrichtigungen an Partner, wenn:

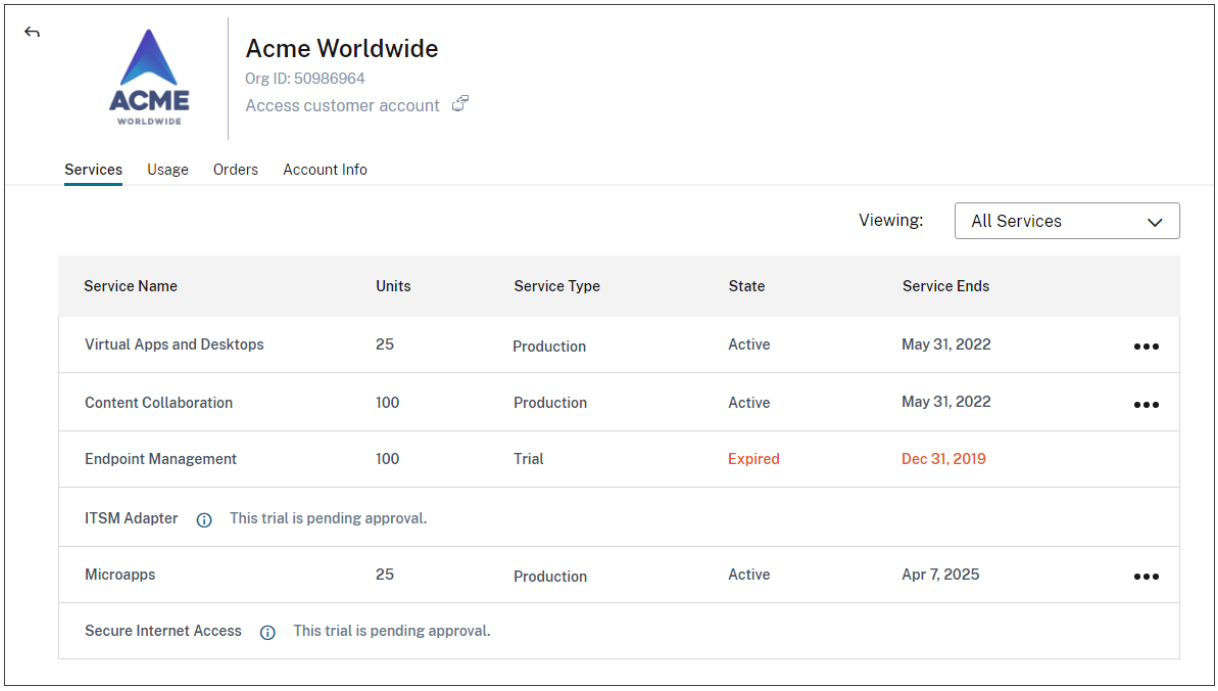
- Der Partner eine Verbindung zu einem Kunden herstellt
- Ein Kunde seine Verbindung zum Partner beendet

Citrix Cloud sendet Benachrichtigungen an Kunden, wenn der Partner seine Verbindung mit dem Kunden beendet.

Partnereinblick in Serviceansprüche

Wenn der Partner mit einem Kunden verbunden ist, kann er den Status von dessen Serviceanspruch einsehen. Zu diesen Informationen gehören der Status von Testversions- und Nicht-Testversionsansprüchen. Die Partner können außerdem die folgenden Informationen anzeigen:

- Aktive Servicetestversionen
- Ausstehende Servicetestanfragen
- Abgelaufene Servicetestversionen
- Aktive Serviceansprüche; Services, die erworben oder dem Kunden auf andere Weise bereitgestellt wurden
- Lizenzanzahl und Ablaufdatum für die Berechtigung



Die Anzeige von Lizenzierungen beschränkt sich auf Zusammenfassungen der Lizenzzuweisungen und historische Nutzungstrends.

Verbindungen zu Kunden herstellen

Partner stellen mithilfe eines einmaligen Einladungslinks Verbindungen zu Kunden her. Der Link ist fest vorgegeben und kann nicht geändert werden.

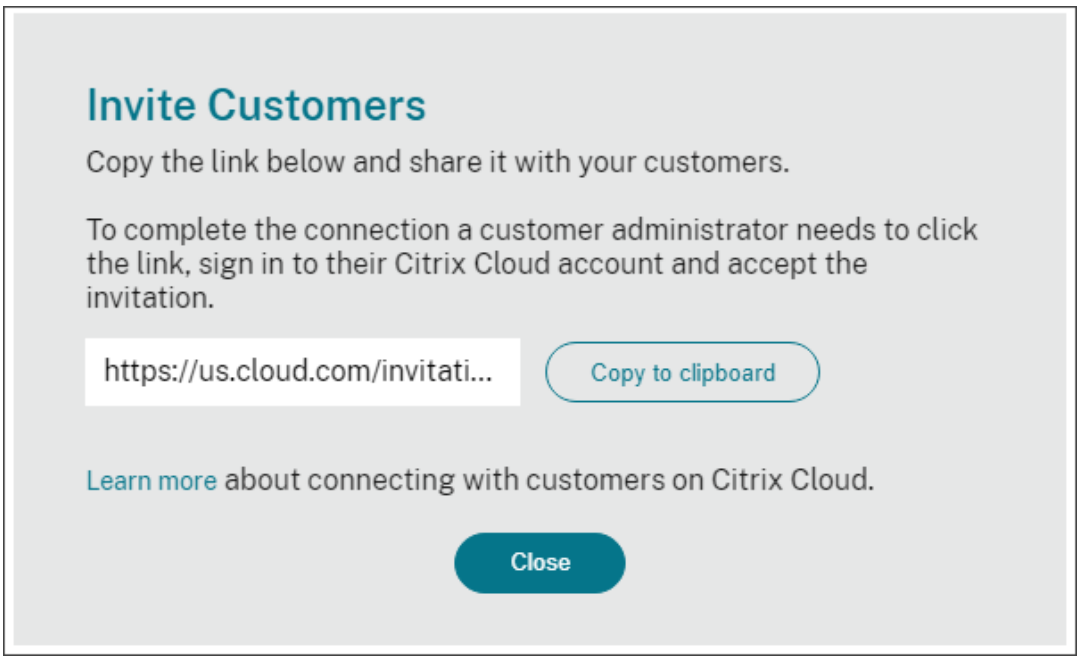
Partner können ihren Einladungslink unbegrenzt oft verwenden, um Verbindungen herzustellen bzw. wiederherzustellen. Einladungslinks laufen nicht ab.

Verbindung erstellen:

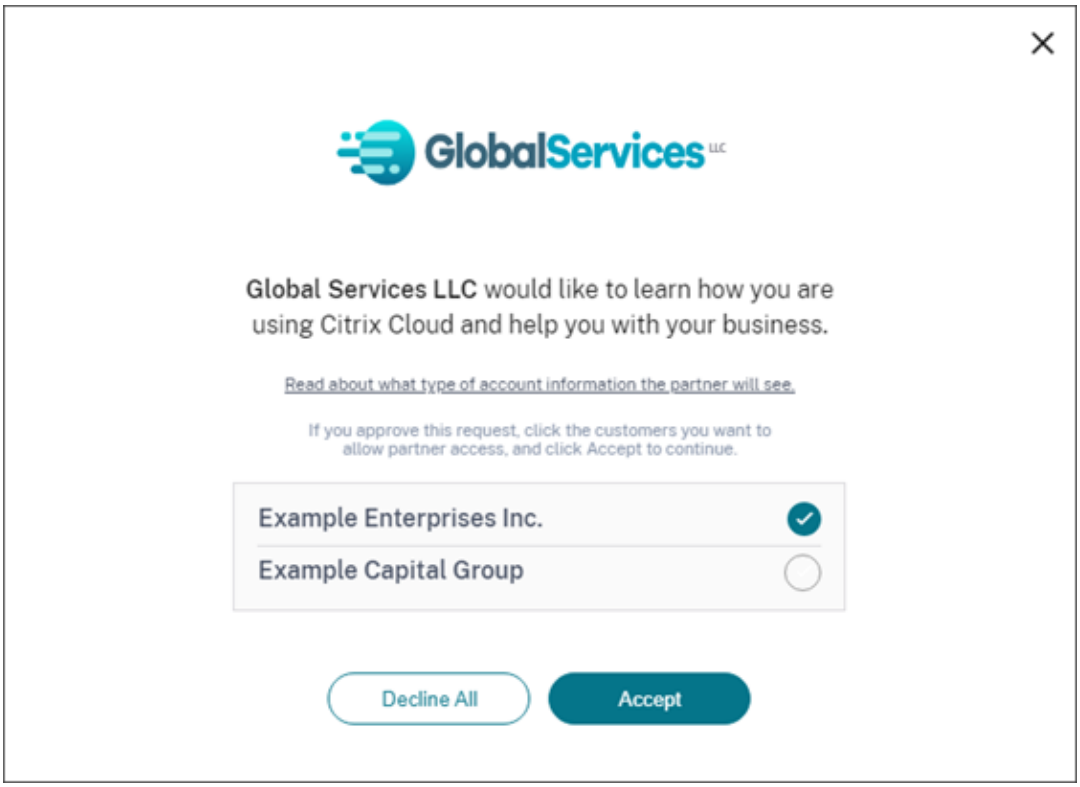
1. Wählen Sie im Citrix Cloud-Menü **Meine Kunden**.
2. Wählen Sie im Kundendashboard **Einladen oder hinzufügen**.
3. Gehen Sie zum Herstellen einer Verbindung zu einem bestehenden Citrix Cloud-Kunden folgendermaßen vor:

    a) Wählen Sie **Citrix Cloud-Kunde einladen** und dann **Weiter**.

    b) Kopieren Sie den Einladungslink und senden Sie ihn an den Kunden.



Um die Verbindung herzustellen, klickt der Kunde auf den Einladungslink, meldet sich bei Citrix Cloud an und akzeptiert die Einladung.



4. Gehen Sie zum Herstellen einer Verbindung zu einem neuen Kunden ohne Citrix Cloud-Konto folgendermaßen vor:

    a) Wählen Sie **Kunde hinzufügen** und dann **Weiter**.

b) Geben Sie die geschäftlichen Kontaktdaten des Kunden ein und wählen Sie dann **Fertig stellen**. Citrix Cloud erstellt ein neues Konto für den Kunden.

Anschließend erhält der Kunde eine Benachrichtigung, dass der Partner dem neuen Konto als Administrator hinzugefügt wurde. Der Kunde kann mit dem Link **Kennwort vergessen?** auf der Citrix Cloud-Anmeldeseite ein Kennwort für das neue Konto einrichten. Nachdem der Kunde sein Kennwort festgelegt hat, kann er sich mit seiner geschäftlichen E-Mail-Adresse bei seinem Konto anmelden und das Onboarding abschließen (siehe Bei Citrix Cloud registrieren).

Partner- oder Kundenverbindungen entfernen

Verbindungen können jederzeit durch Kunden oder Partner beendet werden.

Verbindung mit einem Kunden entfernen

Um eine Verbindung mit einem Kunden zu beenden, führen Sie die folgenden Schritte aus:

1. Wählen Sie oben rechts im Citrix Cloud-Menü der Konsole **Meine Kunden**.
2. Suchen Sie im Kundendashboard den Kunden, den Sie verwalten möchten.
3. Klicken Sie auf die Auslassungspunkte für den Kunden und wählen Sie **Kundenverbindung entfernen**.
4. Wenn Sie aufgefordert werden, das Entfernen zu bestätigen, wählen Sie **Entfernen**.

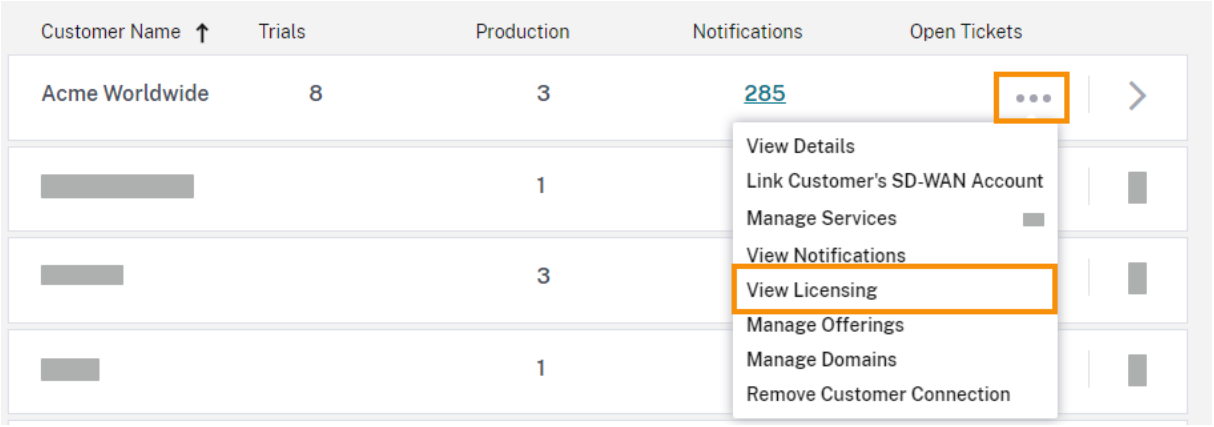
Verbindung mit einem Partner entfernen

Um eine Verbindung mit einem Partner zu beenden, führt der Kunde die folgenden Schritte aus:

1. Wählen Sie im Benutzermenü oben links **Kontoeinstellungen**.
2. Suchen Sie auf der Seite **Firmenkonto** den Bereich **Partnerverbindungen**.
3. Suchen Sie den Partner, den Sie verwalten möchten, und wählen Sie dann **Entfernen**.
4. Wenn Sie aufgefordert werden, das Entfernen zu bestätigen, wählen Sie **Bestätigen**.

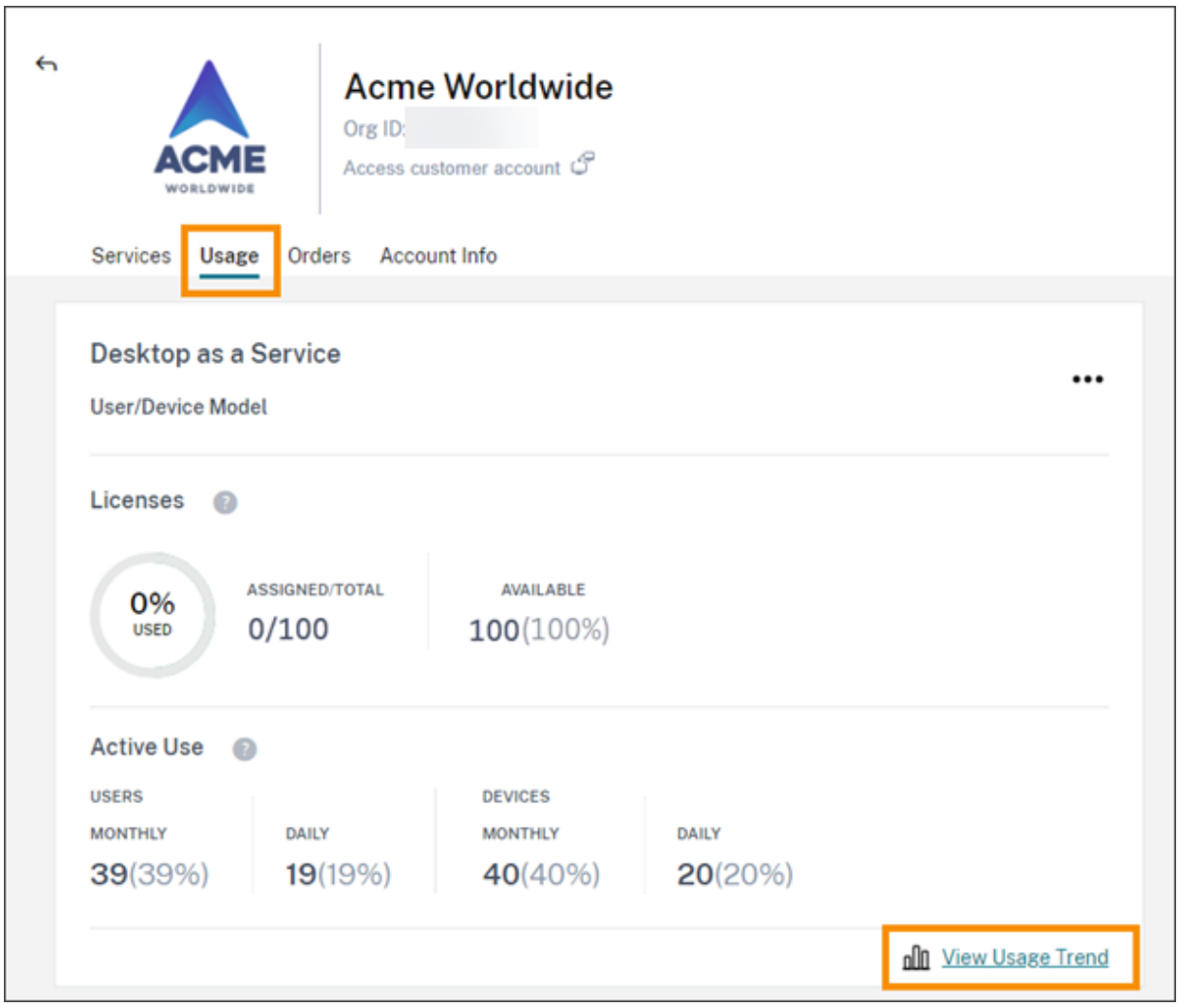
Lizenzierungstrends

Partner können die Lizenzinformationen für einen Kunden einsehen, indem sie im Kunden-Dashboard indem sie auf die Auslassungspunkte klicken und die Option **Lizenzierung anzeigen** auswählen.



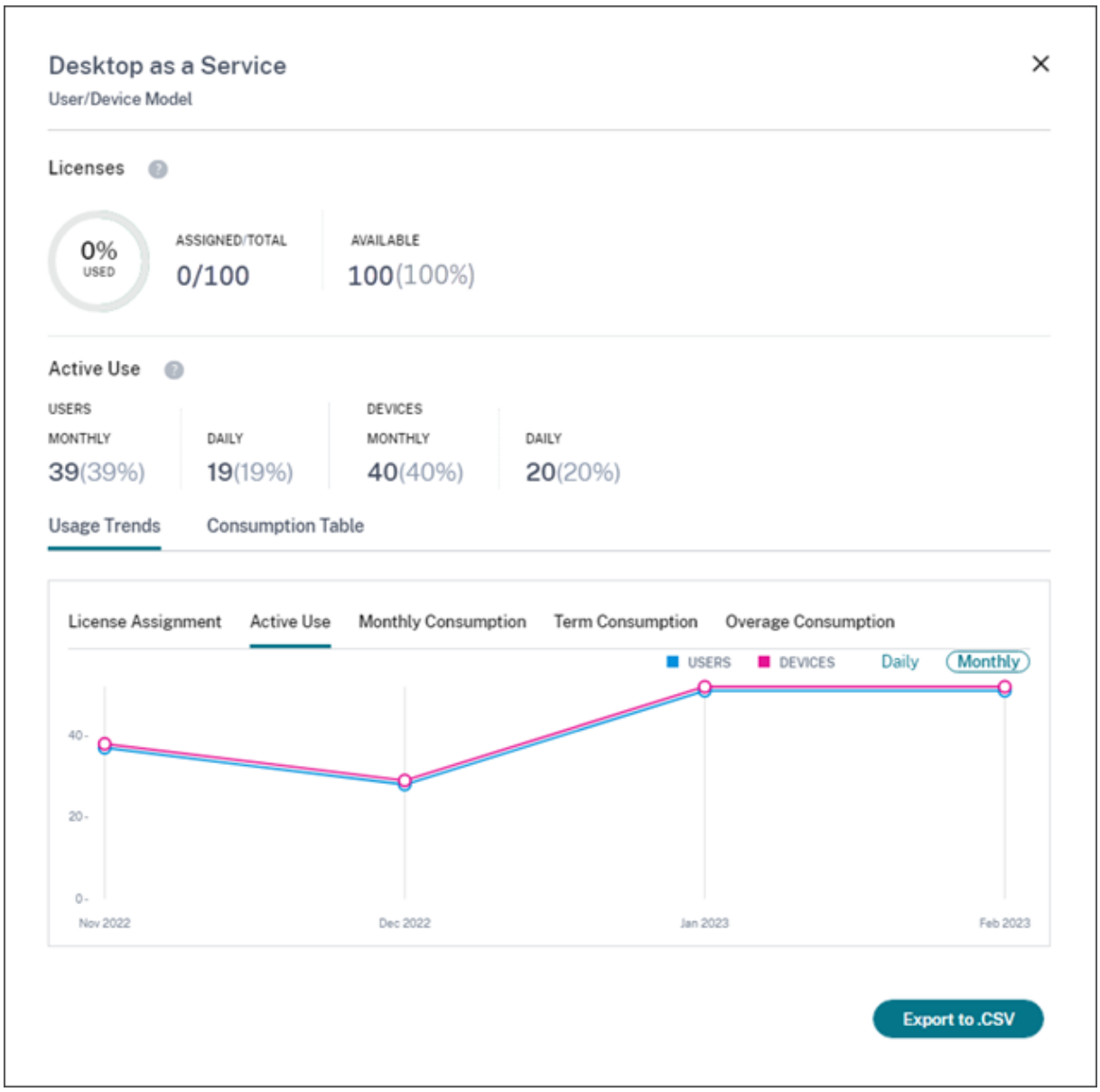
> **Hinweis:**
>
> Citrix Partner können nur die Zusammenfassung unter "Lizenzierung"sowie historische Trends der aktiven Nutzung anzeigen. Sie können keine einzelnen Benutzer, die Lizenzen für einen bestimmten Service verwenden, anzeigen.

Um die Lizenzübersicht des Kunden für jeden Service einzusehen, wählen Sie die Registerkarte **Nutzung**. Zum Anzeigen weiterer Nutzungsinformationen wählen Sie **Nutzungstrend anzeigen** für den jeweiligen Service.



Je nach Service umfassen die Nutzungstrends die folgenden Informationen:

- Das Verhältnis der zugewiesenen Lizenzen zur Gesamtzahl der gekauften Lizenzen
- Monatlich und täglich aktive Nutzer
- Eine visuelle Aufschlüsselung der Lizenzzuweisungen, der aktiven Nutzung, der Nutzung pro Anspruch und der Überschreitung.



Bei Bedarf können diese Informationen als CSV-Datei exportiert werden.

Bandbreitennutzung

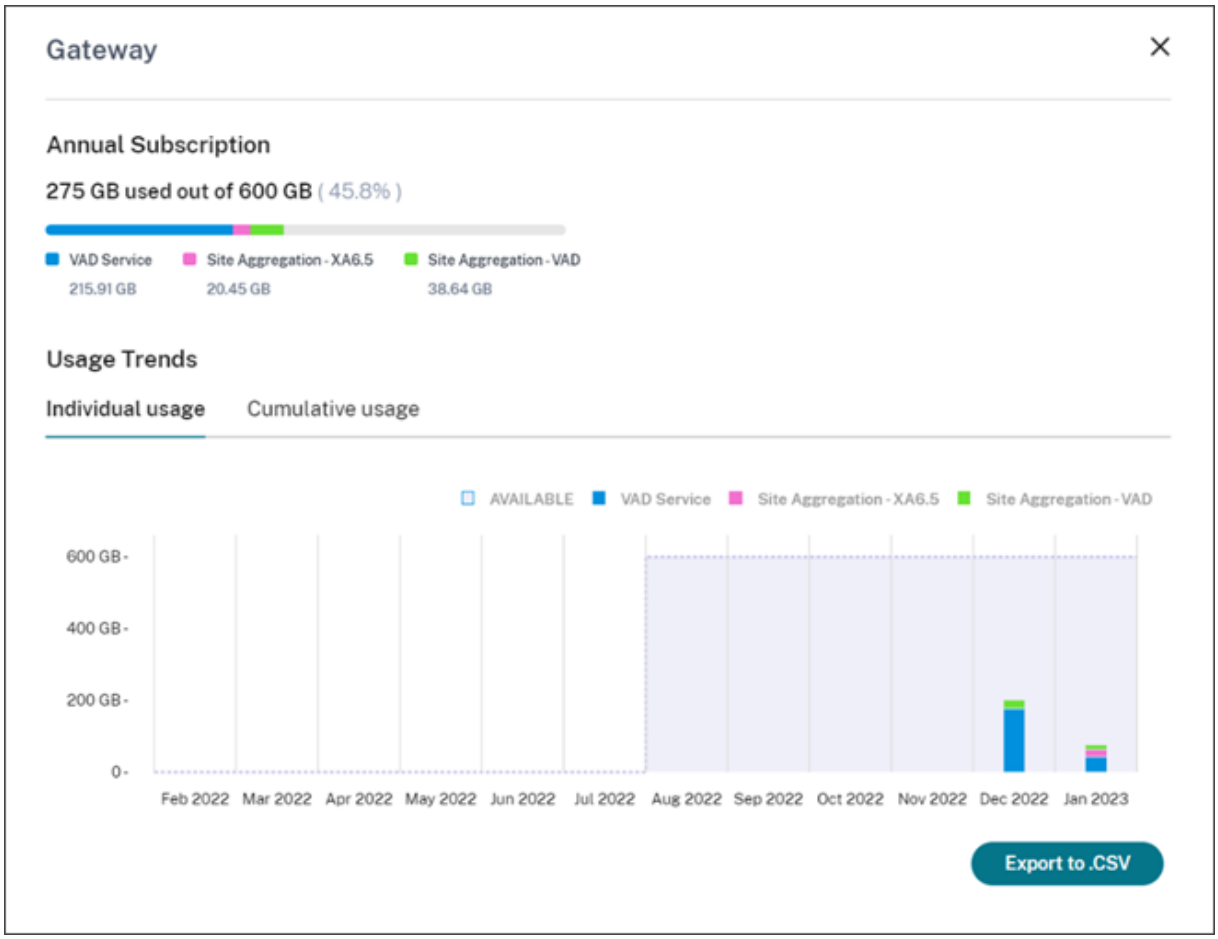
Für Citrix Gateway Service besteht die Lizenzzusammenfassung aus den folgenden Informationen:

- Gesamtbandbreitennutzung für alle Ansprüche des Kunden.
- Gesamtbandbreitennutzung, aufgeschlüsselt nach den monatlichen, jährlichen und befristeten Ansprüchen des Kunden.
- Gesamtüberschreitung für den laufenden Monat. Weitere Informationen zur Berechnung der Überschreitung finden Sie unter Überschreitung.

Wählen Sie ganz rechts auf der Seite eines Anspruchs die Option **Nutzungstrend anzeigen**, um die Nutzungsübersicht anzuzeigen. Wählen Sie **Überschreitungsdiagramm anzeigen**, um das Überschreitungsdiagramm für die letzten 12 Monate anzuzeigen.

Je nach Anspruch umfassen die Nutzungstrends die folgenden Informationen:

- Die Menge der genutzten Bandbreite zwischen Citrix DaaS (**VAD-Service**) und On-Premises-Bereitstellungen von Virtual Apps and Desktops mit Siteaggregation.
- Eine visuelle Aufschlüsselung der Bandbreitennutzung für jeden Nutzungsmonat. (Monatliche Ansprüche)
- Eine visuelle Aufschlüsselung der **individuellen Bandbreitennutzung** in jedem Monat des Abrechnungszeitraums. (Jährliche und befristete Ansprüche)
- Eine visuelle Aufschlüsselung der **kumulierten Bandbreitennutzung** in jedem Monat des Abrechnungszeitraums. (Jährliche und befristete Ansprüche)



Bei Bedarf können diese Informationen als CSV-Datei exportiert werden.

Kundenlizenzierung und Lizenznutzung für Citrix Service Provider

Die Lizenzierungsfunktion in Citrix Cloud ermöglicht Kunden von Citrix Service Providern (CSP) die Überwachung ihrer Lizenzen und des Lizenzverbrauchs für unterstützte Citrix DaaS-Produkte (früher Citrix Virtual Apps and Desktops). CSPs können sich unter dem Citrix Cloud-Konto ihres Kunden anmelden, um diese Informationen anzuzeigen und zu exportieren. Weitere Informationen finden Sie in den folgenden Artikeln:

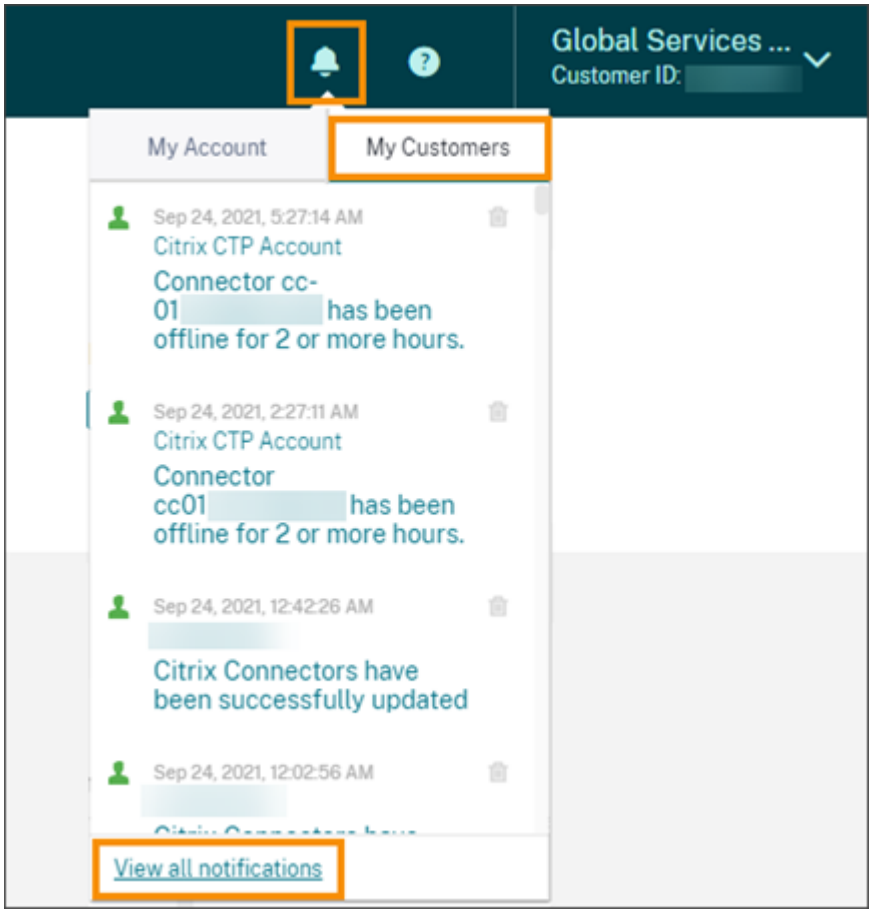
- Überwachen von Kundenlizenzen und -nutzung für Citrix DaaS
- Überwachen von Kundenlizenzen und -nutzung für Citrix DaaS Standard für Azure

Sichtbarkeit von Supporttickets und Benachrichtigungen der Kunden für Partner

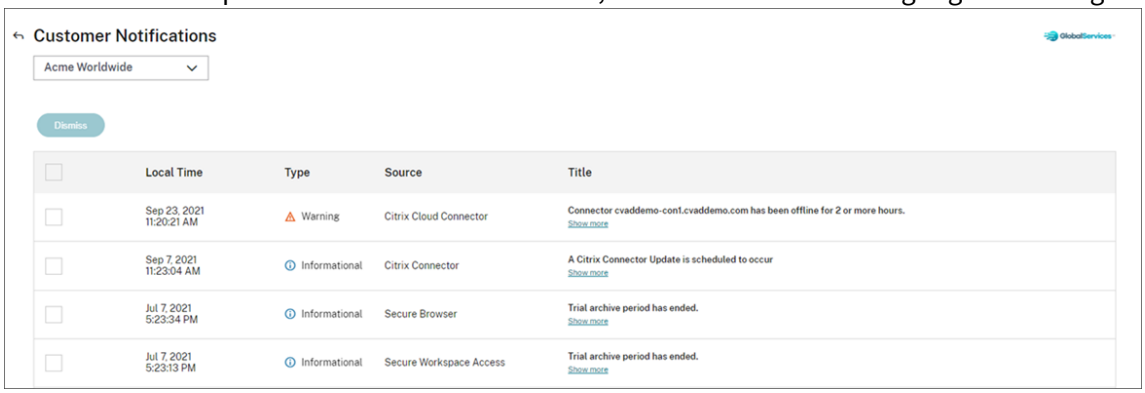
Partner können Benachrichtigungen für die verbundenen Kunden anzeigen. Sie können außerdem die kundenspezifischen Benachrichtigungen filtern und Maßnahmen ergreifen, z. B. die Benachrichtigung abweisen. Abgewiesene Benachrichtigungen werden für den Partner nicht angezeigt. Die Kunden können die Benachrichtigung jedoch in ihrem Konto sehen, nachdem sie sich bei Citrix Cloud angemeldet haben.

Kundenbenachrichtigungen anzeigen:

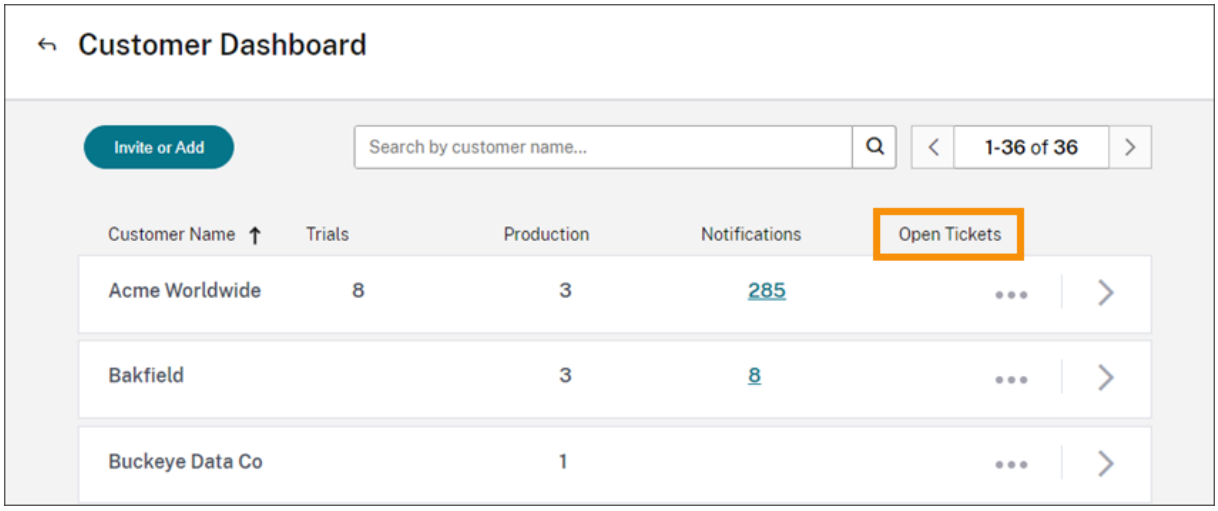
1. Klicken Sie auf das Glockensymbol oben in der Verwaltungskonsole und wählen Sie **Meine Kunden** und dann **Alle Benachrichtigungen anzeigen**.



2. Wählen Sie im Dropdownmenü einen Kunden aus, um dessen Benachrichtigungen anzuzeigen.



Partner können die Zahl der Supporttickets für ihre Kunden im Kundendashboard anzeigen.



Verbunddomänen für Citrix Service Provider

Über *Verbunddomänen* können Kundenbenutzer sich mit Anmeldeinformationen aus einer mit Ihrem CSP-Ressourcenstandort verknüpften Domäne beim Workspace anmelden. Auf diese Weise können Sie Ihren Kunden dedizierte Workspaces mit einer benutzerdefinierten Workspace-URL wie *customer.cloud.com* bereitstellen. Der Ressourcenstandort ist weiterhin in Ihrem Citrix Cloud-Partnerkonto. Sie können dedizierte Workspaces neben dem gemeinsam genutzten Workspace bereitstellen, auf den die Kunden über Ihre CSP-Workspace-URL zugreifen (z. B. csppartner.cloud.com). Damit Kunden auf ihren dedizierten Workspace zugreifen können, fügen Sie sie den entsprechenden, von Ihnen verwalteten Domänen hinzu. Nach Konfiguration des Workspace können sich die Benutzer des Kunden bei ihrem Workspace anmelden und auf die Apps und Desktops zugreifen, die Sie über Citrix DaaS zur Verfügung gestellt haben.

Wenn Sie einen Kunden aus einer Verbunddomäne entfernen, können die Benutzer des Kunden nicht mehr mit Anmeldeinformationen aus Ihrer Domäne auf ihre Workspaces zugreifen.

Weitere Informationen über die Verwendung von Verbunddomänen zum Bereitstellen von Apps und Desktops finden Sie unter Citrix DaaS für Citrix Service Providers.

Workspace-Darstellungsoptionen für Citrix Service Provider

Sie können Workspace-Farben und -Logos mit benutzerdefinierten Designs konfigurieren. Informationen zum Erstellen benutzerdefinierter Designs finden Sie unter Anpassen der Darstellung von Workspaces.

> **Hinweis**
>
> Benutzerdefinierte Designs sind eine Funktion für Einzelmandanten. Citrix Service Provider,

> deren Mandanten einen Ressourcenstandort, Cloud Connectors und eine Active Directory-Domäne teilen (Mehrmandantenumgebung), werden derzeit nicht unterstützt. Citrix Service Provider-Mandanten mit eigenem Ressourcenstandort, eigenen Cloud Connectors und einer eigenen Active Directory-Domäne (Einzelmandanten) werden voll unterstützt.

Cloudservices

July 2, 2024

In diesem Artikel werden die Cloudservices aufgeführt, die über Citrix Cloud angeboten werden. Darüber hinaus finden Sie hier Links zur Produktdokumentation der Services. Beschreibungen dieser Services und der Angebote, in denen sie enthalten sind, finden Sie unter Service Descriptions for Citrix Services.

Citrix-Services

Analytics

- Analytics for Security
- Analytics for Performance
- Analytics –Usage

Citrix DaaS

Citrix DaaS Standard für Azure

Endpoint Management

Gateway

ITSM-Adapter für ServiceNow

Remote Browser Isolation

Secure Private Access

Sitzungsaufzeichnungsdienst

Virtual Apps Essentials

Virtual Desktops Essentials

Workspace Environment Management

NetScaler-Services

Konsole

App Delivery and Security

SD-WAN Orchestrator

Secure Internet Access

Web App Firewall