Citrix Cloud

Contents

Citrix Cloud

April 29, 2022

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.

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? Gehen Sie zum Abschnitt **Citrix Cloud Services** im Inhaltsverzeichnis links auf dieser Seite. Wählen Sie den Service aus, um die Produktdokumentation für diesen Service aufzurufen.

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

May 13, 2022

Datum des Inkrafttretens: 30. Oktober 2020

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

Die vorliegenden SLA (Servicelevelziele) repräsentieren das Leistungsversprechen von Citrix hinsichtlich der Verfügbarkeit von Citrix Cloud Services. Diese SLA ist Teil des Citrix Endbenutzerservicevertrags (EUSA) 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.

- Der Ausfall wurde durch eine nicht von Citrix verwaltete Komponente verursacht, 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.
Citrix Application Delivery Management-Service	Durchschnittliche Zeit, in der der Service für alle POPs verfügbar ist.
Citrix App Delivery and Security Service – Citrix Managed	Durchschnittliche Zeit, in der der Service für alle POPs verfügbar ist.

Service	Monatliche Betriebszeit
Citrix Content Collaboration	Die Zeit, in der Benutzer Dateien und Ordner enumerieren können, die mit ihrem Konto verknüpft sind, oder Dateien herunterladen können, die in von Citrix verwalteten Speicherzonen gehostet werden.
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.
Citrix Intelligent Traffic Management	Die Zeit, die Benutzer über DNS-Abfragen oder HTTP-API-Aufrufe auf Datenverkehrsmanagementfunktionen zugreifen können.
Citrix 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.
Citrix Wrike	Zeitdauer, die die Benutzer auf den Service zugreifen und diesen nutzen können.

> **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 EUSA 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.

Leitfaden zur sicheren Bereitstellung für die Citrix Cloud-Plattform

October 16, 2022

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
- ShareFile - 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 für Administratoren wird durch Integration von Citrix Cloud in Azure Active Directory erreicht.
- Standardmäßig werden Administratorsitzungen in Citrix Cloud nach 60 Minuten Inaktivität automatisch beendet. Diese Timeoutzeit von 60 Minuten kann nicht geändert werden. *Inaktiv* bedeutet, dass die Sitzung vollständig im Leerlauf ist und der Administrator in keiner Weise mit der Citrix Cloud-Konsole interagiert. *Aktivität* bezieht sich auf Aktionen wie das Gehen in der grafischen Benutzeroberfläche, das Auswählen von Konfigurationsoptionen, das Speichern von Konfigurationsänderungen oder das Warten auf die Umsetzung einer Änderung.

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). Es liegen keine ruhenden Daten vor, die vertraulich oder verschlüsselt sind, sodass eine Schlüsselverwaltung nicht erforderlich ist.

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-Steuerebene zugreifen, werden die folgenden starken Verschlüsselungssammlungen empfohlen: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA2
- Wenn Sie von Windows Server 2012 R2 auf die Citrix Cloud-Steuerebene 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 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
- Konfigurieren von ShareFile StorageZones Controller für TLS 1.2: CTX209211, Konfigurieren von StorageZone Controller für eingehende TLS v1.2-Verbindungen
- 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.

Die folgenden Ressourcen enthalten Informationen, wie Sie in Content Collaboration den Speicherort Ihrer Daten festlegen:

- Content Collaboration Service-Dokumentation
- Häufig gestellte Fragen zur Sicherheit in ShareFile
- Sicherheit und Compliance in Citrix ShareFile
- Implementieren von Speicherzonen für die On-Premises-Speicherung

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 mit installiertem Cloud Connector

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	636/TCP	LDAP SSL
49152 -65535/TCP	3268/TCP	LDAP GC
49152 -65535/TCP	3269/TCP	LDAP GC SSL
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

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
- Portanforderungen für den Application Delivery Management Service
- 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

Das Connectorgerät 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 das Connectorgerät 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 das Connectorgerät 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 mit dem Connectorgerät anmelden (z. B. für Wartungsvorgänge). Zur allgemeinen Verwaltung eines Citrix Produkts ist es nicht erforderlich, dass ein Administrator sich an diesen Hypervisoren anmeldet. Das Connectorgerät wird selbstverwaltet.

Konfiguration von eingehenden und ausgehenden Ports

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

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

Das Connectorgerät kann andere ausgehende Ports mit Internetzugriff haben. Wenn andere Ports zur Verfügung stehen, kann das Connectorgerät darüber die Netzwerkbandbreite und Leistung optimieren.

Innerhalb des internen Netzwerks muss das Connectorgerät 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
Ausgehend	49152 -65535/TCP	464/TCP/UDP	Kerberos-Kennwortänderung
Ausgehend	49152 - 65535/TCP/UDP	389/TCP/UDP	LDAP
Ausgehend	49152 -65535/TCP	636/TCP	LDAP SSL
Ausgehend	49152 -65535/TCP	3268/TCP	LDAP GC
Ausgehend	49152 -65535/TCP	3269/TCP	LDAP GC SSL
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

Das Connectorgerät 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 das Connectorgerät 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

Das Connectorgerät benötigt keine spezielle SSL/TLS-Konfiguration.

Das Connectorgerät 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 das Connectorgerät 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 das Connectorgerät selbstverwaltet, und Sie können sich nicht über die Konsole anmelden.

Es ist nicht Ihre Aufgabe, auf Sicherheitsrisiken des Connectors zu reagieren. Das Connectorgerät 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.

Hilfe und Support

September 27, 2022

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:**
>
> Wenn bei der Anmeldung bei einer Citrix Website oder bei der Registrierung für die mehrstufige Authentifizierung (MFA) ein Problem auftritt, lesen Sie zunächst diesen Artikel mit Ressourcen zur Problembehandlung. 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 Support von Citrix.

Um ein neues Citrix Konto für Ihr Unternehmen zu erstellen oder einem bestehenden Citrix Konto Ihres Unternehmens beizutreten, besuchen Sie https://www.citrix.com/welcome/create-account/.

Informationen zur Registrierung bei Citrix Cloud finden Sie unter Registrierung bei Citrix Cloud.

Falls bei der Registrierung für ein Citrix Konto oder ein Citrix Cloud-Konto ein Fehler auftritt, wenden Sie sich bitte an den Citrix Customer Service.

Anmeldung bei Citrix Websites und Citrix Cloud

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 web sites
- CTX283814: Sign in issue after setting up Citrix account

Falls beim Anmelden an Citrix Cloud Probleme auftreten:

- Stellen Sie sicher, dass Sie die E-Mail-Adresse und das Kennwort verwenden, die Sie bei der Registrierung angegeben haben.
- 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 Ihr Kennwort nicht den Anforderungen für sichere Kennwörter entspricht. 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 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 AD- bzw. Azure AD-Anmeldeinformationen 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.

Wenn Sie weiterhin Probleme bei der Anmeldung bei einer Citrix Website haben, wenden Sie sich an den Citrix Customer Service.

Mehrstufige Authentifizierung für Citrix Konten und Citrix Cloud-Konten

Bei Citrix Cloud müssen sich Administratoren mit der mehrstufigen Authentifizierung anmelden. Die Registrierung bei der mehrstufigen Authentifizierung erfolgt bei der Registrierung eines neuen Kontos bei Citrix Cloud oder wenn ein neuer Administrator einem bestehenden Citrix Cloud-Konto beitritt.

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

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

Bestätigungs-E-Mail nicht erhalten

Wenn Sie die Registrierung für die mehrstufige Authentifizierung beginnen, sendet Ihnen Citrix eine E-Mail mit einem Bestätigungscode. Die E-Mail kommt normalerweise innerhalb weniger Minuten an. Wenn Sie diese E-Mail 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.
- Vergewissern Sie sich, dass `donotreplynotifications@citrix.com` und `cloud@citrix.com` als vertrauenswürdige Absender aufgeführt sind. Ihre Firewall hat die E-Mail möglicherweise blockiert.

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.

Mehrstufige Authentifizierung ohne Mobilgerät

Bei der Registrierung für die mehrstufige Authentifizierung fordert Citrix Sie auf, eine Authentifikator-App einzurichten, damit Sie Ihr Gerät registrieren können. Die Verwendung eines Mobilgeräts (z. B. Smartphone oder Tablet) für diese Aufgabe ist zwar üblich, jedoch nicht zwingend erforderlich.

Für die Registrierung zur mehrstufigen Authentifizierung müssen Sie eine Authentifikator-App verwenden, die RFC6238 (TOTP: Algorithmus für zeitbasiertes Einmalkennwort) unterstützt. Sie können eine Authentifikator-App auf anderen Geräten wie einem Desktop-Computer verwenden.

Desktop-kompatible Authentifikator-App stehen in der Regel als Browsererweiterung oder eigenständige Anwendung zur Verfügung, die Sie auf Ihrem Computer installieren. Für Hardwaretoken bieten einige Tokenhersteller zugehörige desktopkompatible Authentifikator-Apps an.

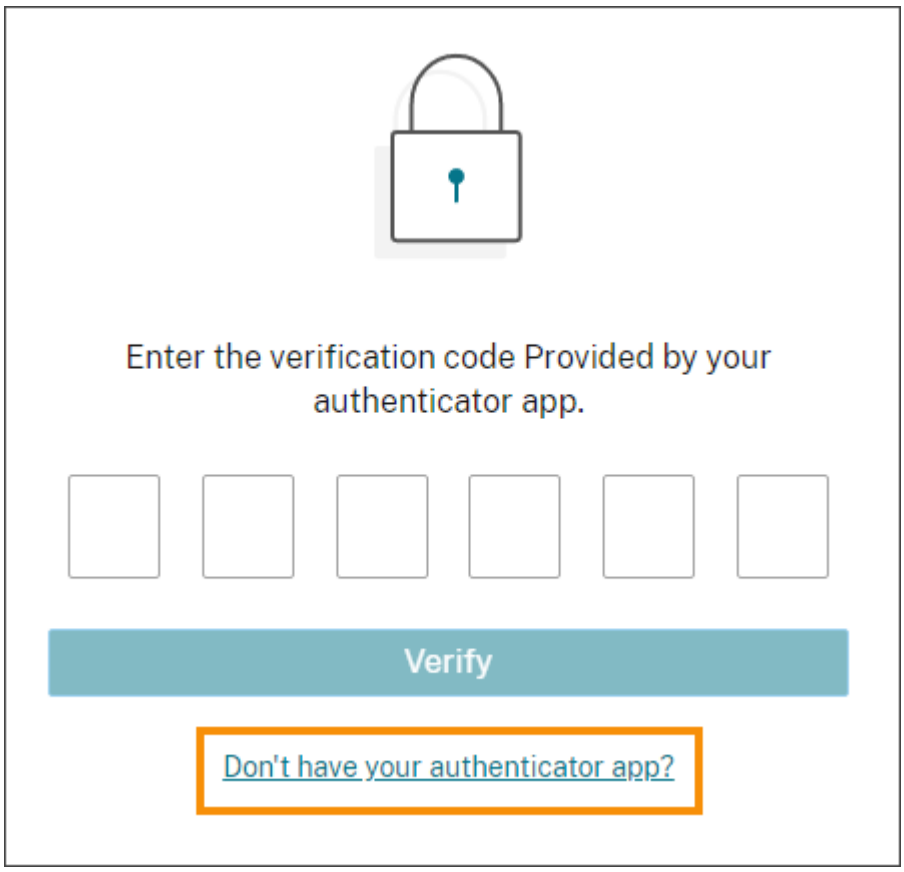
Kontowiederherstellung

Je nach den Wiederherstellungsmethoden, die Sie bei der Registrierung für die mehrstufige Authentifizierung konfiguriert haben, können Sie den Zugriff auf Ihr Konto mit einer der folgenden Methoden wiederherstellen:

- Verwenden eines einmaligen Codes, den Citrix an Ihre Wiederherstellungs-E-Mail-Adresse sendet.
- Verwenden eines der Backupcodes, die Sie bei der Registrierung generiert haben.
- Erlauben Sie Citrix Support, Ihre Telefonnummer für die Wiederherstellung anzurufen, 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 mehrstufige Authentifizierung erforderlich.

Gehen Sie zur Anmeldung ohne Authentifikator-App folgendermaßen vor:

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 von Ihrer Authentifikator-App zur Eingabe des Codes aufgefordert werden, wählen Sie **Haben Sie keine Authentifikator-App?** aus.



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** aus. 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**.

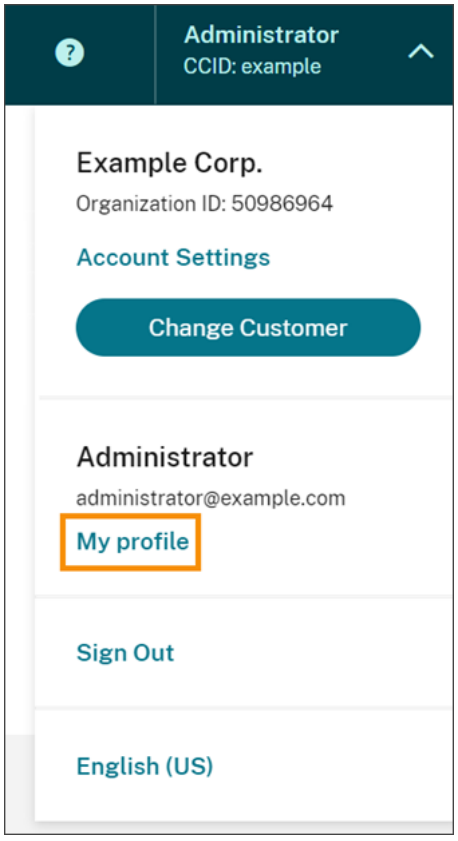
Aktualisieren Sie nach der Anmeldung Ihre Kontowiederherstellungsmethoden, um Verzögerungen bei der Anmeldung künftig zu vermeiden.

Aktualisieren der Methoden zur Kontowiederherstellung

Über die Seite **Mein Profil** können Sie Ihre Kontowiederherstellungsmethoden aktualisieren und Ihr registriertes Gerät ändern. Sie können über Ihr Citrix Konto oder über Citrix Cloud auf diese Seite zugreifen.

Zum Aufrufen der Seite **Mein Profil** gehen Sie folgendermaßen vor:

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 **Mein Profil**.



Informationen zum Ändern Ihres Geräts oder zum Aktualisieren Ihrer Wiederherstellungsmethoden finden Sie in den folgenden Abschnitten:

- Ändern Ihrer Geräteregistrierung

- Wiederherstellungs-E-Mail-Adresse hinzufügen oder ändern
- Telefonnummer für die Wiederherstellung ändern
- Neue Backupcodes generieren

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.

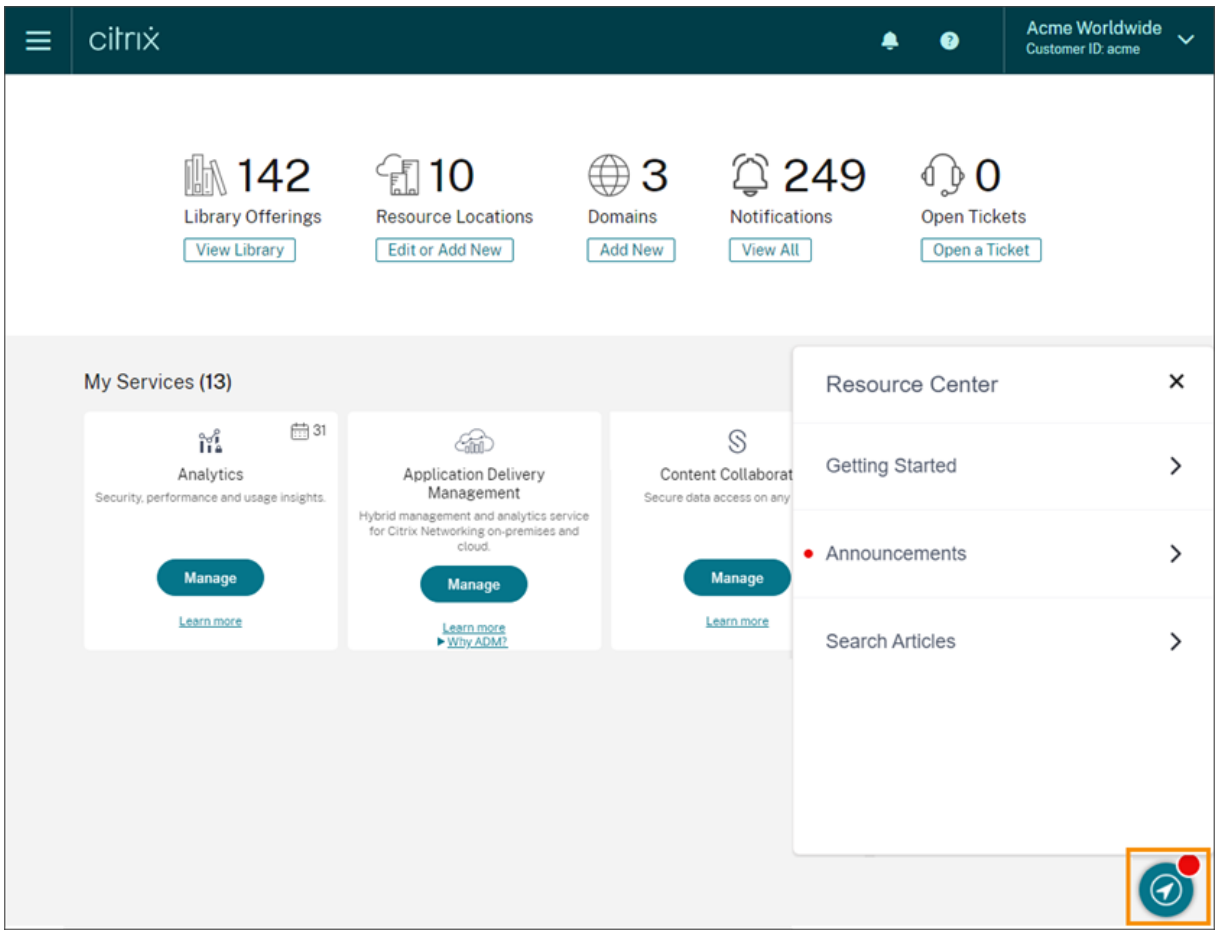
Sie müssen sich nicht anmelden, um Forumsbeiträge zu lesen. Um selbst einen Kommentar zu posten oder auf ein Thema zu antworten, müssen Sie jedoch angemeldet sein. Verwenden Sie zur Anmeldung die Anmeldeinformationen für Ihr Citrix Konto oder die E-Mail-Adresse und das Kennwort, die Sie beim Erstellen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

Das Citrix Cloud-Ressourcencenter erleichtert Ihnen den Einstieg in Citrix Cloud. Hier finden Sie Informationen über Features und können nach Lösungen für Probleme suchen. Klicken Sie unten rechts auf der Seite auf das blaue Kompasssymbol. Dieses Feature ist für die Citrix Cloud-Plattform, Citrix DaaS und den Application Delivery Management Service verfügbar.



- **Erste Schritte**: Bietet eine kurze Anleitung zu den wichtigsten Aufgaben speziell für den Service, mit dem Sie gerade arbeiten. Außerdem finden Sie Links zu Schulungs- und Onboardingressourcen, die Sie nutzen können, um mehr über Servicefunktionen zu erfahren und Ihre Endbenutzer erfolgreich zu unterstützen.
- **Ankündigungen**: Bietet Benachrichtigungen über neu veröffentlichte Features und Links zu wichtigen Mitteilungen von Citrix. Wählen Sie eine Feature-Benachrichtigung, um eine kurze Anleitung zu dem Feature zu erhalten.
- **Artikel durchsuchen**: Enthält eine Liste mit Produktdokumentation und Knowledge Center-Artikeln für häufige Aufgaben und hilft Ihnen, weitere Artikel zu finden, ohne Citrix Cloud zu verlassen. Geben Sie eine Suchabfrage in das Feld **How do I ...** ein, um eine gefilterte Liste von Artikeln für den Service anzuzeigen, mit dem Sie arbeiten. Im Allgemeinen werden Supportartikel zuerst in der Liste angezeigt, gefolgt von Artikeln in der Produktdokumentation.

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 Files.

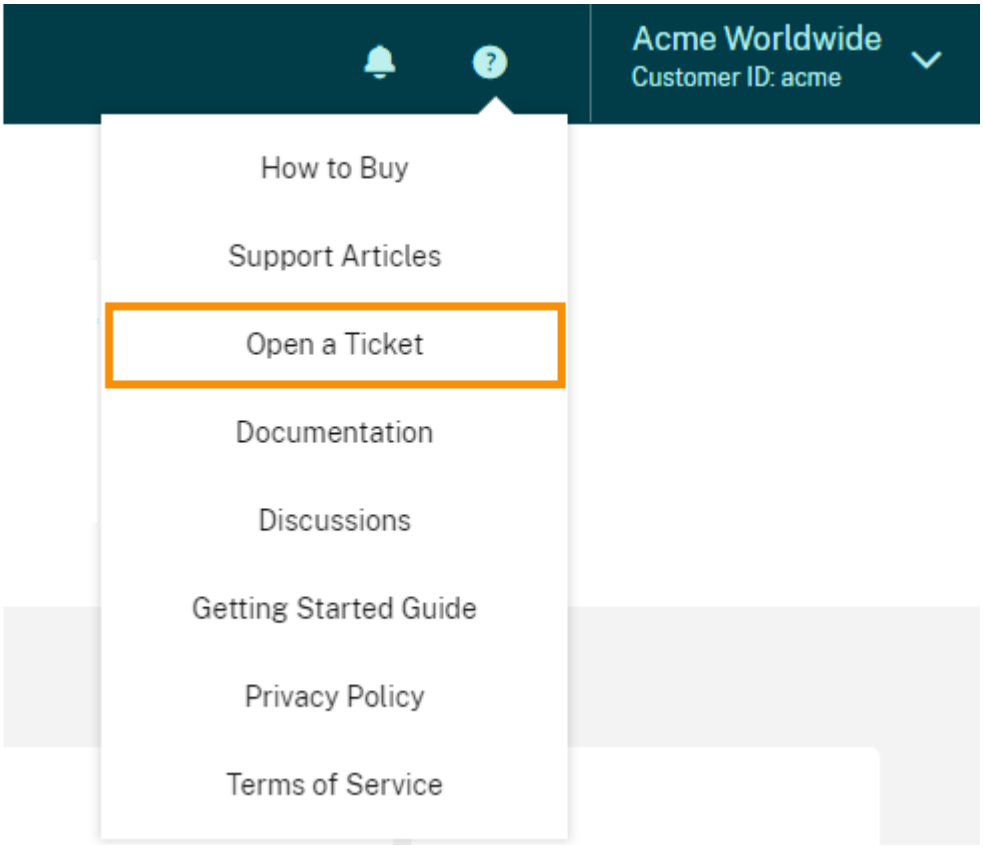
Technischer Support

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

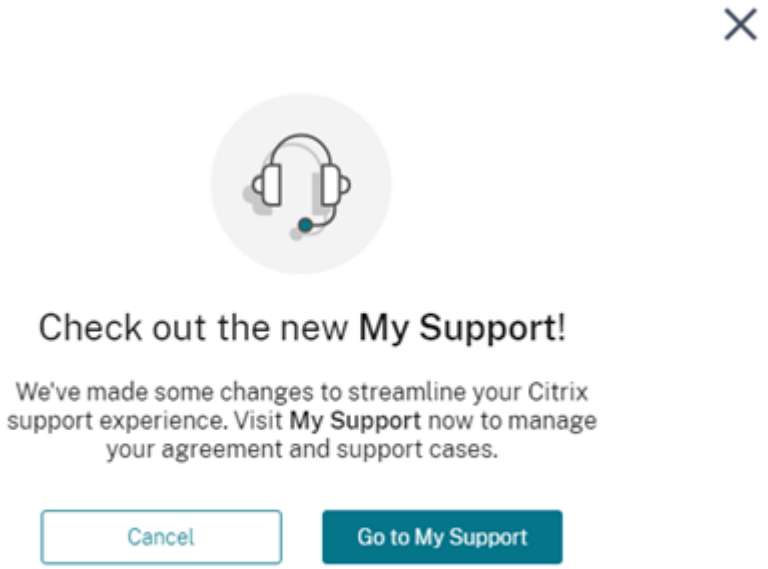
Um auf das My Support-Portal zuzugreifen, gehen Sie zu https://support.citrix.com/case/manage.

Gehen Sie zum Zugriff auf das Portal von Citrix Cloud aus folgendermaßen vor:

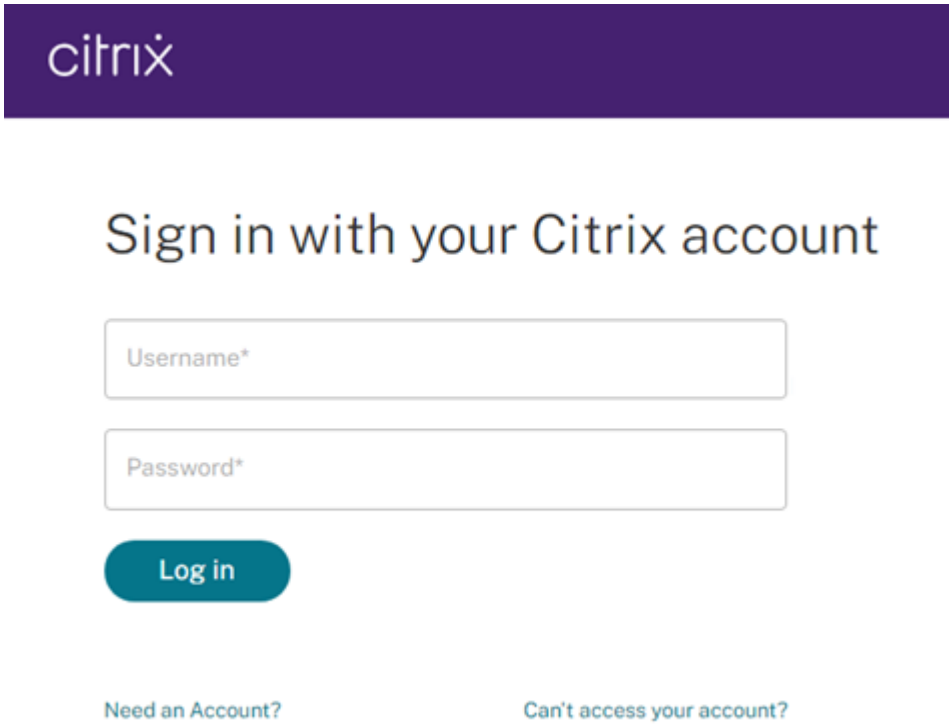
1. Wählen Sie das **Hilfesymbol** rechts oben im Bildschirm.



2. Wählen Sie **Ticket erstellen > Zu My Support**.

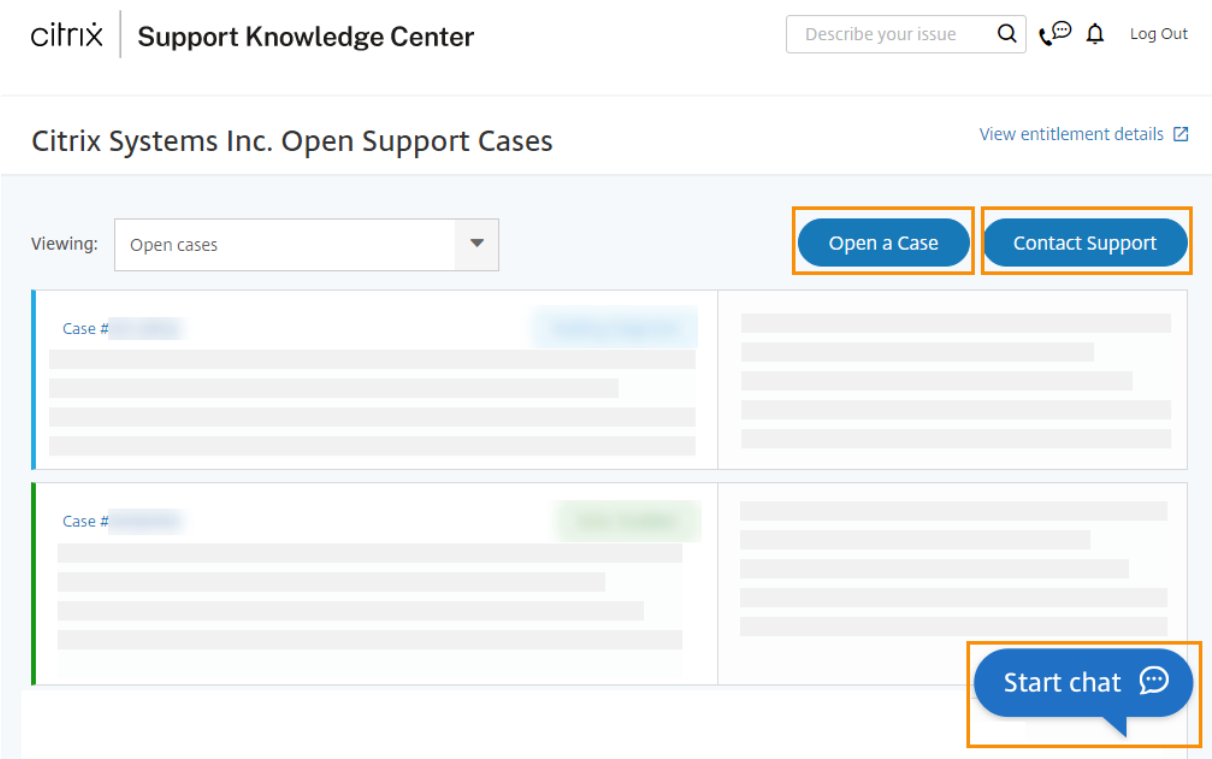


3. Melden Sie sich mit Ihrem Citrix-Konto an.



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

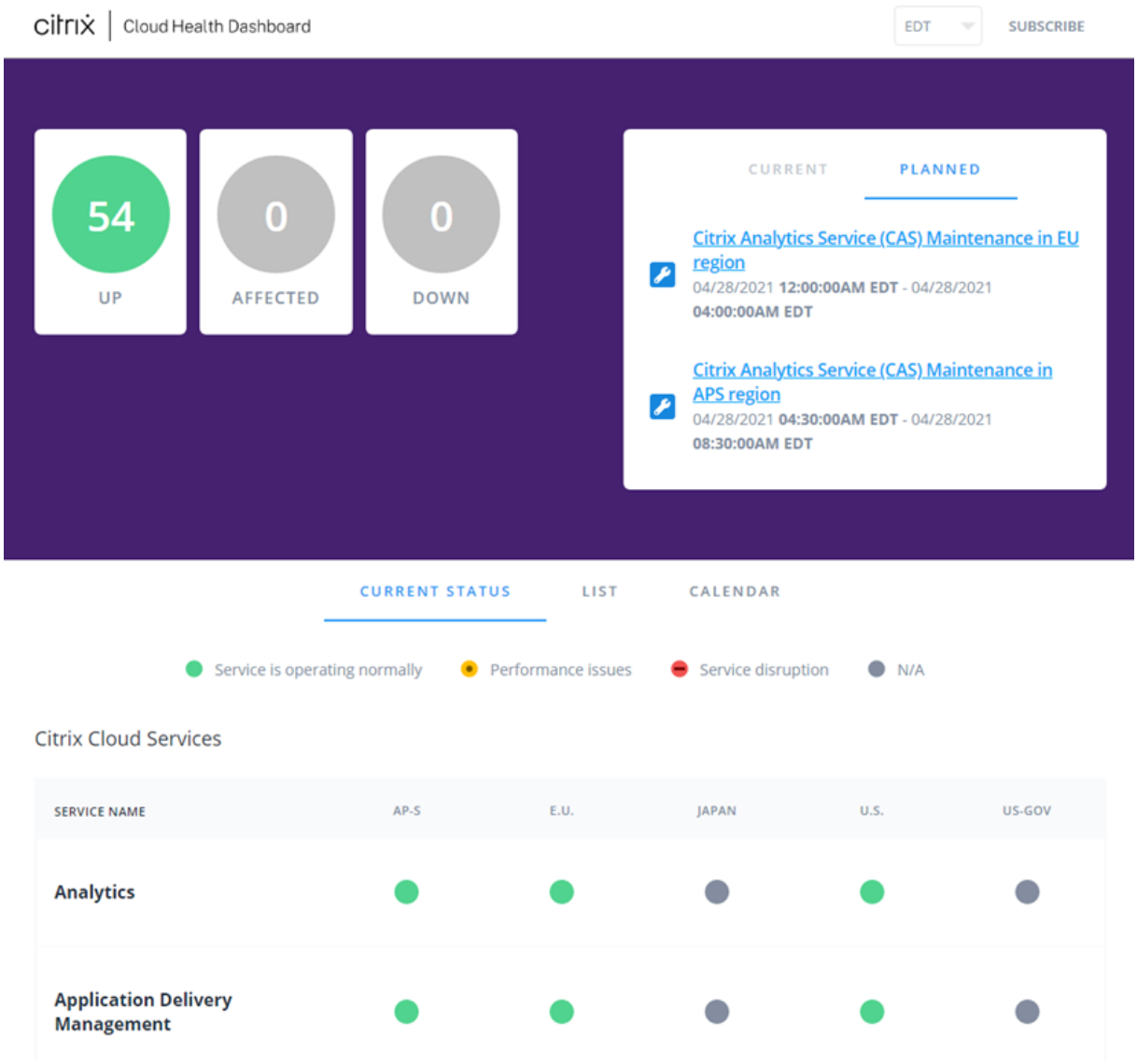
- Öffnen Sie einen Supportfall: Wählen Sie **Open a Case** und geben Sie Details zu Ihrem Problem ein.
- Per Telefon: Wählen Sie **Contact Support**, um eine Liste lokaler Telefonnummern anzuzeigen, über die Sie den technischen Support von Citrix erreichen.
- Live-Chat: Wählen Sie **Start chat** rechts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



Integrität des Citrix Cloud-Diensts

September 27, 2022

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.



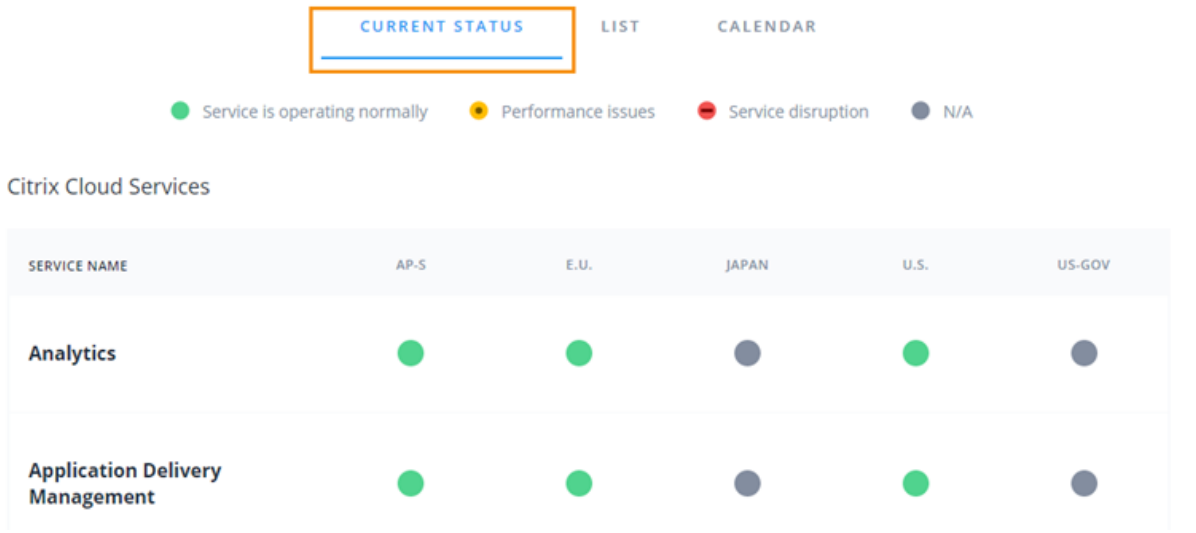
Über das Dashboard erhalten Sie Informationen zu folgenden Elementen:

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

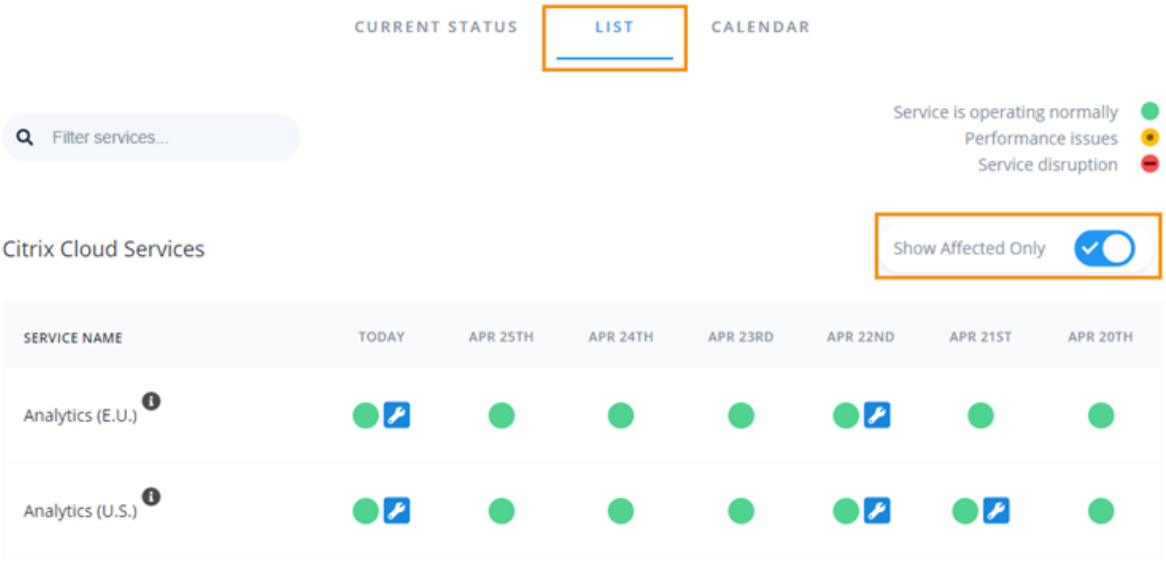
Sie können auch Benachrichtigungen über Ereignisse wie Wartungsfenster und Service-Incidents abonnieren.

Anzeigen von Zustand und Wartungsstatus

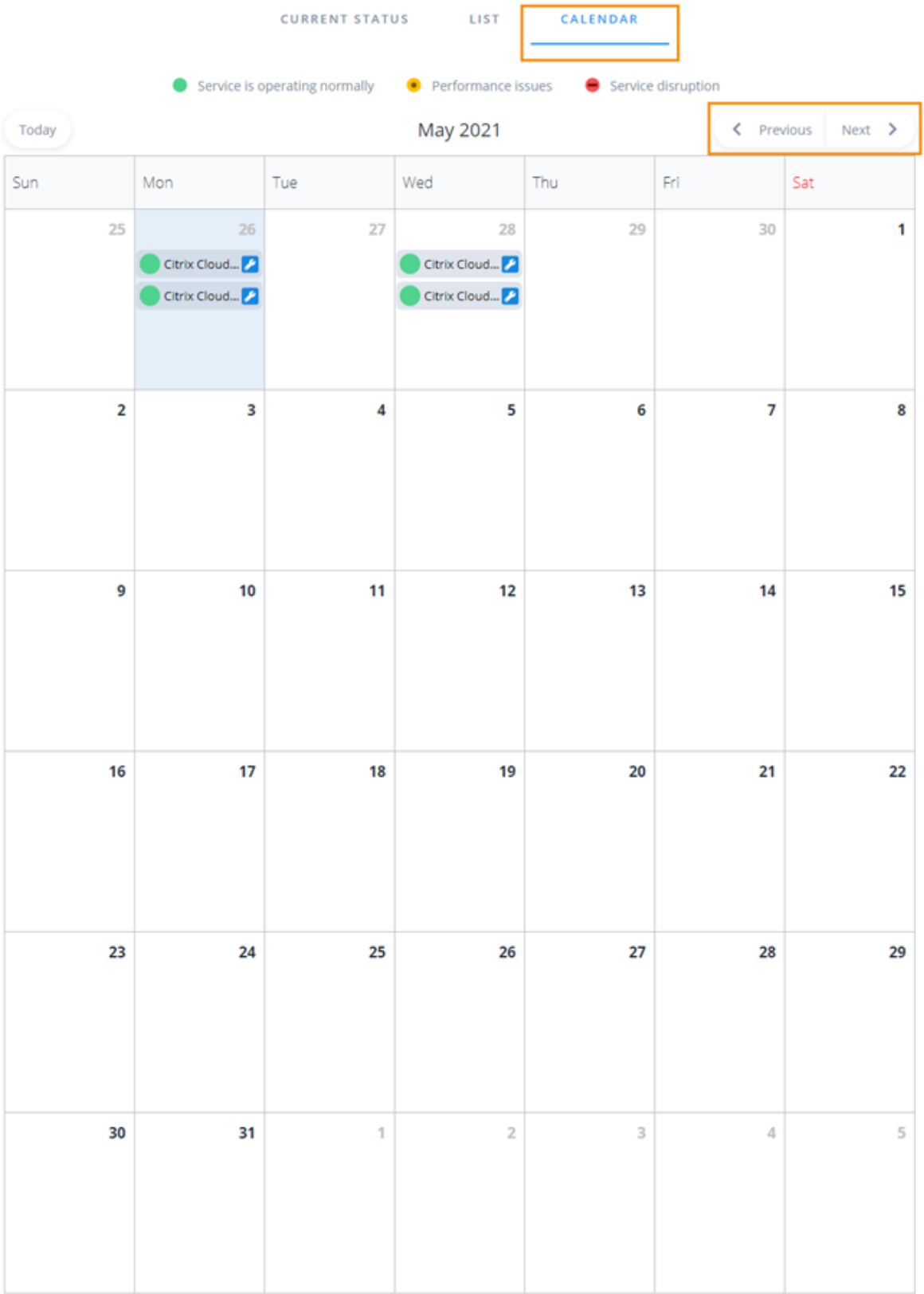
Wählen Sie **Current Status**, um den aktuellen Status aller Citrix Cloud-Services und -Komponenten in den einzelnen geografischen Regionen anzuzeigen.



Wählen Sie **List**, 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.



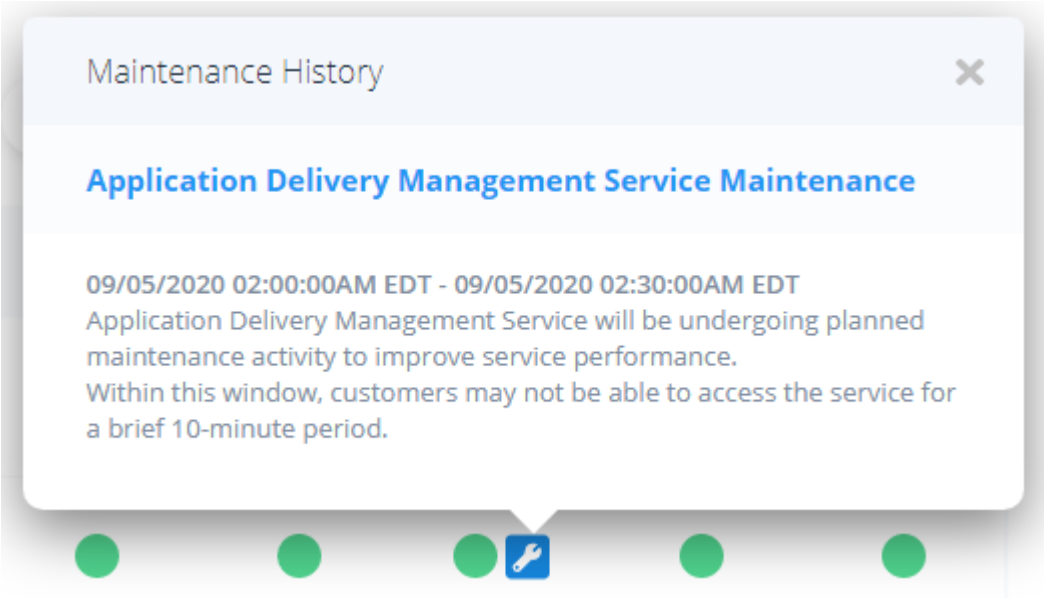
Wählen Sie **Calendar**, um eine Kalenderansicht der Wartungsfenster anzuzeigen. Wählen Sie **Next** bzw. **Previous**, um durch die geplanten Wartungsereignisse jedes Monats zu blättern.



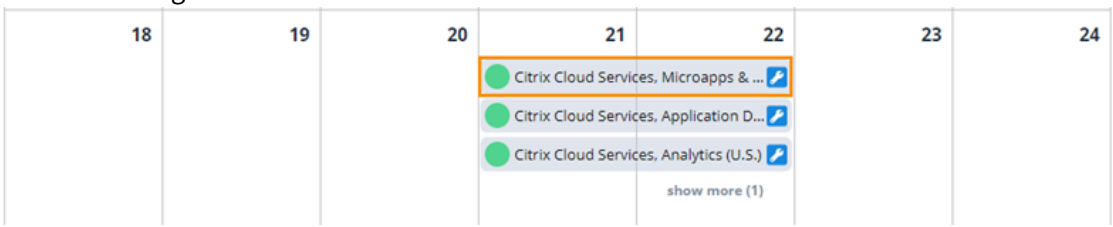
Anzeigen von Details zu Service-Incidents

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

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



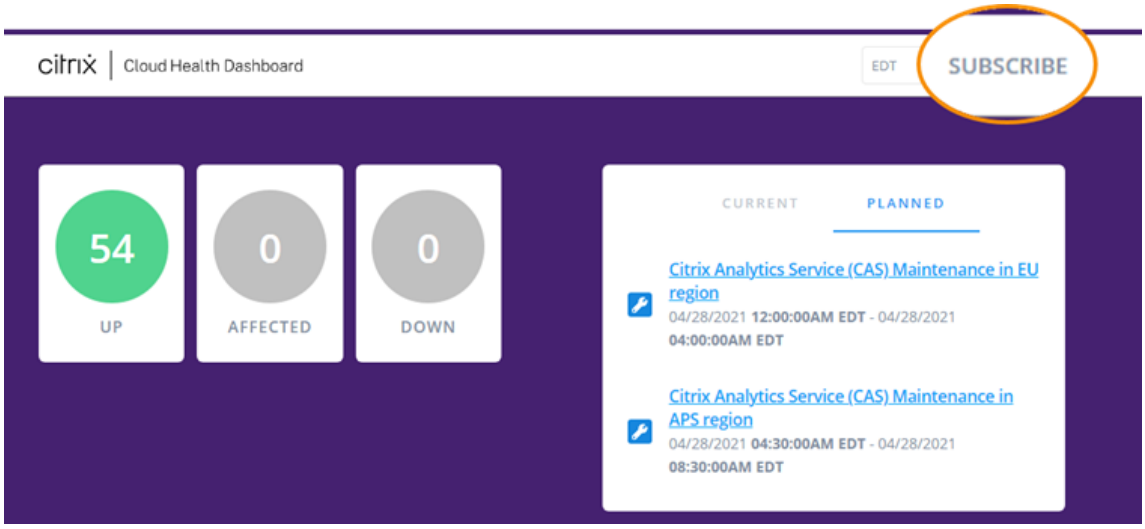
- Klicken Sie in der Kalenderansicht auf den Serviceeintrag, um die Statusseite für das Wartungsfenster anzuzeigen.



Abonnieren von Benachrichtigungen

Benachrichtigungen über Serviceintegritätsereignisse können Sie auf folgende Weise einholen:

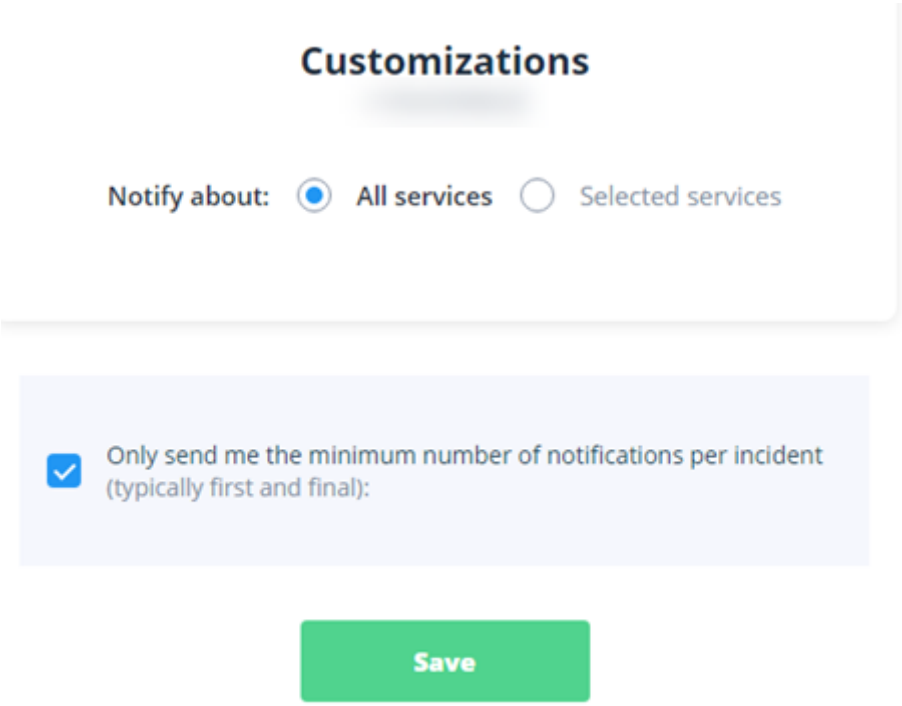
- Wählen Sie oben rechts im Dashboard **Subscribe** und dann die gewünschte Benachrichtigungsmethode. Sie können zwischen verschiedenen Methoden wählen, einschließlich E-Mail und Telefon.



- 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`.

Zum Abonnieren aller Service-Benachrichtigungen für alle geografischen Regionen gehen Sie folgendermaßen vor:

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. Wählen Sie **Weiter**.
3. Wählen Sie auf der Seite **Anpassungen** die Option **Alle Services** aus, um Benachrichtigungen für alle Services in allen geografischen Regionen zu erhalten.
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**.



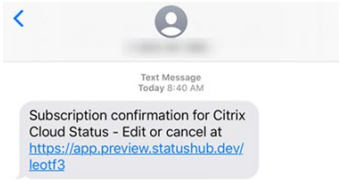
Zum Abonnieren von Benachrichtigungen für bestimmte Services oder Regionen gehen Sie folgendermaßen vor:

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. Wählen Sie **Weiter**.
3. Wählen Sie auf der Seite **Customizations** die Option **Selected services**. Es wird eine mehrseitige Liste mit allen Services in jeder unterstützten Region angezeigt.
4. Wählen Sie die Services in den geografischen Regionen aus, über die Sie benachrichtigt werden möchten. Um über alle Services einer geografischen Region informiert zu werden, wählen Sie **Aggregate by groups** und dann die Region aus.
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**.

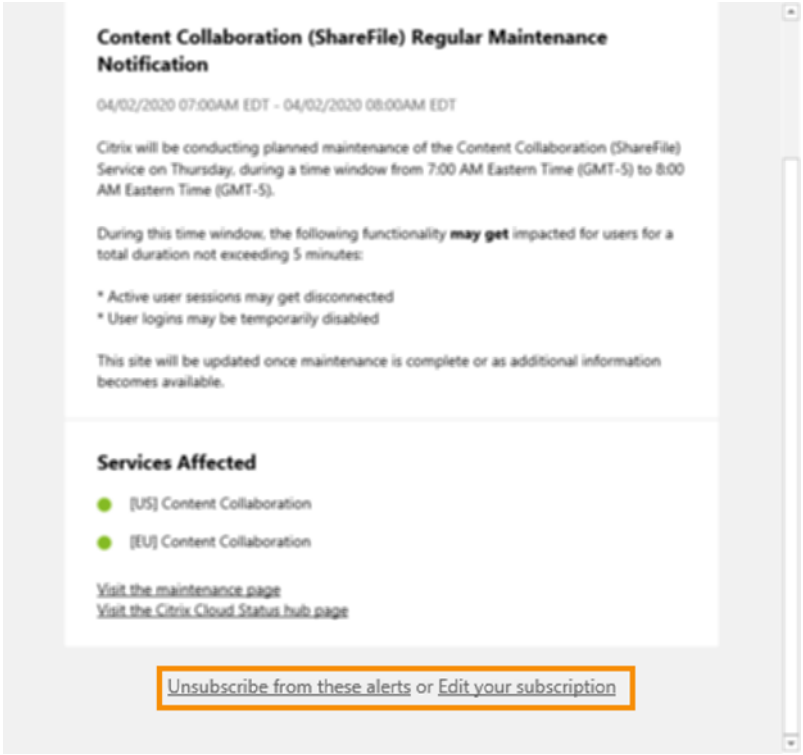
Abonnement von Benachrichtigungen abbestellen

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:



- E-Mail-Benachrichtigung 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**.

Hinweise zu Drittanbietern

October 16, 2022

- 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)
- Citrix ShareFile Sync for Mac Third Party Notices (PDF)
- Citrix ShareFile Sync for Windows Third Party Notices (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 Microapps Service Third Party Notices (PDF)
- Citrix Gateway 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.

Registrierung bei Citrix Cloud

August 31, 2022

In diesem Artikel werden Sie durch die Anmeldung bei Citrix Cloud und die erforderlichen Schritte zum erfolgreichen Onboarding Ihres Kontos geführt.

> **Tipp:**
>
> Das Modul "Getting Started with Citrix Cloud" im Kurs Fundamentals of Citrix Cloud enthält kurze Videos zu den in diesem Artikel beschriebenen Aufgaben. Der Kurs vermittelt zudem ein solides Grundlagenwissen zu Citrix Cloud und dessen Vorteilen für Unternehmen sowie wichtige Anwendungsfälle für die Citrix Cloud-Services.

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 Finden einer OrgID benötigen, können Sie sich auch an den Citrix Customer Support wenden. Kontaktieren Sie den Citrix Customer Support unter https://www.citrix.com/contact/support.html.

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 wie Ihr Citrix-Konto ebenfalls von einer OrgID identifiziert. 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, muss einer der Administratoren von OrgID 1234 sich mit dieser OrgID bei Citrix Cloud registrieren und dabei einen Webbenutzernamen oder eine E-Mail-Adresse verwenden, der bzw. die mit der OrgID verknüpft ist. Wenn sich das Unternehmen dann zum Kauf eines Citrix DaaS-Abonnements (früher Virtual Apps and Desktops Service) entschließt, kann die Bestellung über OrgID 1234 erfolgen und der Übergang ist reibungslos.

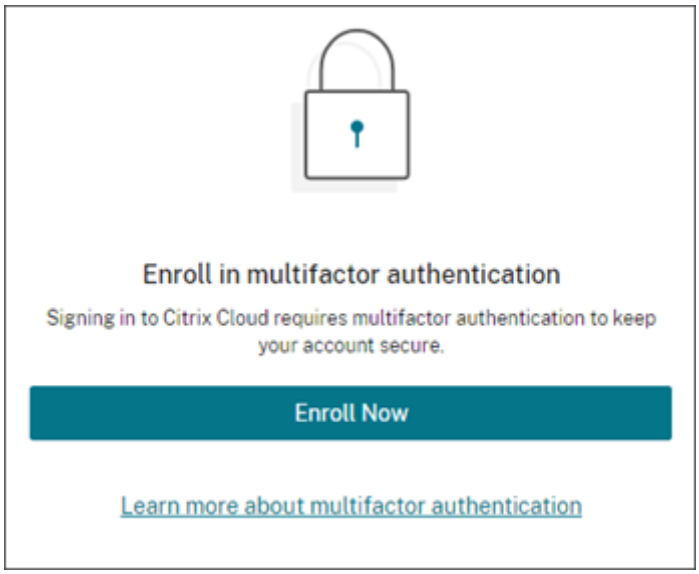
> **Wichtig:**
>
> Benutzer mit Zugriff auf ein bestimmtes Citrix-Konto haben nicht automatisch Zugriff auf das Citrix Cloud-Konto, das mit der OrgID dieses Citrix-Kontos verknüpft ist. Da der Citrix Cloud-Zugriff es Benutzern potenziell ermöglicht, den Service zu beeinträchtigen, ist es wichtig, den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

Anforderungen für die mehrstufige Authentifizierung

Um die Sicherheit Ihres Citrix Cloud-Kontos zu gewährleisten, müssen alle Kunden sich für die mehrstufige Authentifizierung registrieren. Für die Registrierung benötigen Sie nur ein Gerät (z. B.

einen Computer oder ein Mobilgerät) mit installierter Authentifikator-App, z. B. Citrix SSO.

Vorhandene Citrix-Kunden werden von Citrix Cloud zur Registrierung aufgefordert, wenn sie die Anmeldeseite besuchen und die Anmeldeinformationen für ihr Citrix.com-Konto eingeben. Neue Citrix-Benutzer werden von Citrix Cloud zur Registrierung aufgefordert, nachdem sie im Rahmen des Anmeldevorgangs ein Citrix-Konto erstellt haben.

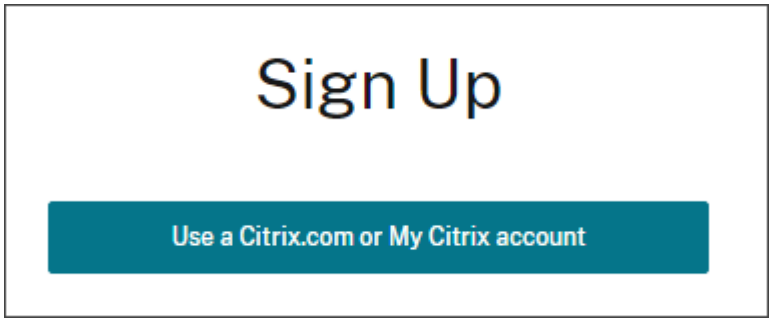


Schritt 1: Aufrufen der Registrierungsseite

Rufen Sie in einem Webbrowser https://onboarding.cloud.com auf.

Sie sind bereits Citrix-Kunde oder verfügen über ein Citrix.com- oder My Citrix-Konto

1. Wählen Sie **Verwenden Sie ein Citrix.com- oder My Citrix-Konto**.

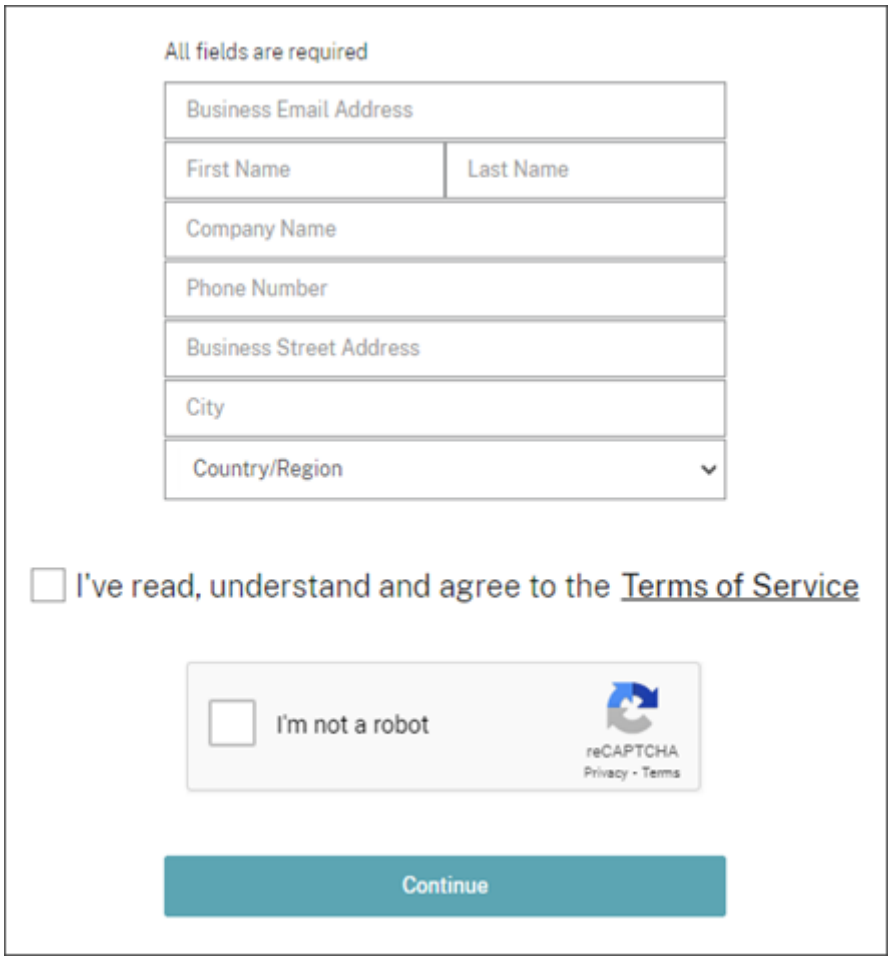


2. Geben Sie Ihren Benutzernamen und Ihr Kennwort (auch als Webbenutzername bezeichnet) oder die E-Mail-Adresse und das Kennwort Ihres Citrix.com-Kontos ein.
3. Wenn Sie zur Registrierung für die mehrstufige Authentifizierung aufgefordert werden, wählen Sie **Jetzt registrieren**.

4. Schließen Sie den Registrierungsprozess wie unter Schritt 5: Registrierung für die mehrstufige Authentifizierung in diesem Artikel beschrieben ab.

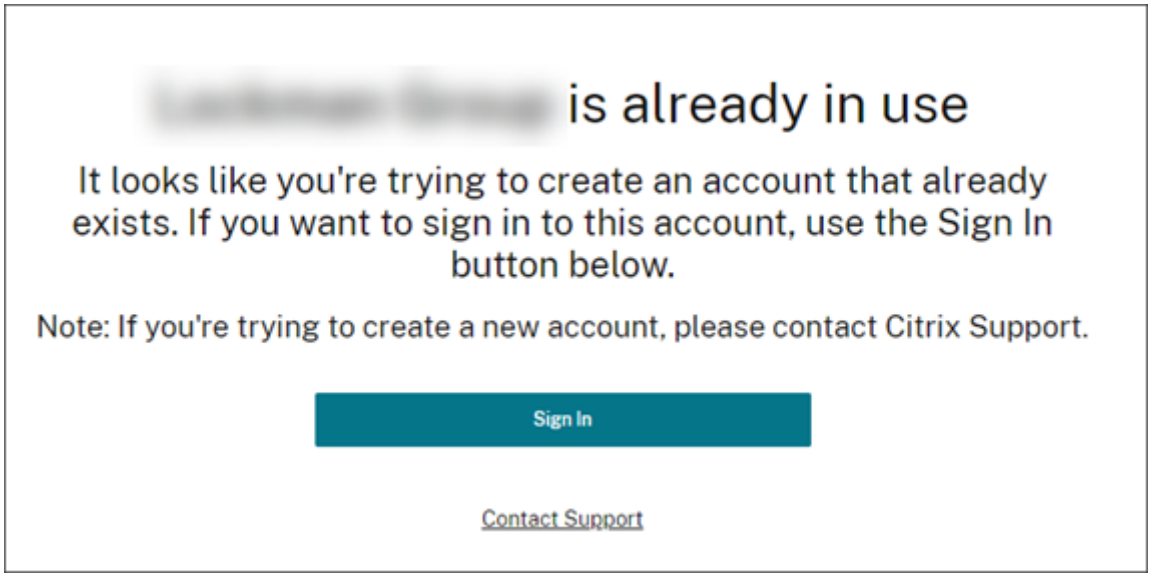
Sie sind neu bei Citrix und Citrix Cloud

Füllen Sie die Formularfelder aus und wählen Sie **Weiter**.



Verwenden Sie Ihre Firmen-E-Mail-Adresse und die Firmenadresse. Die Verwendung einer persönlichen E-Mail-Adresse oder persönlichen Adresse kann zu Verzögerungen bei der Anforderung von Testversionen führen.

Was passiert, wenn das Konto bereits verwendet wird?

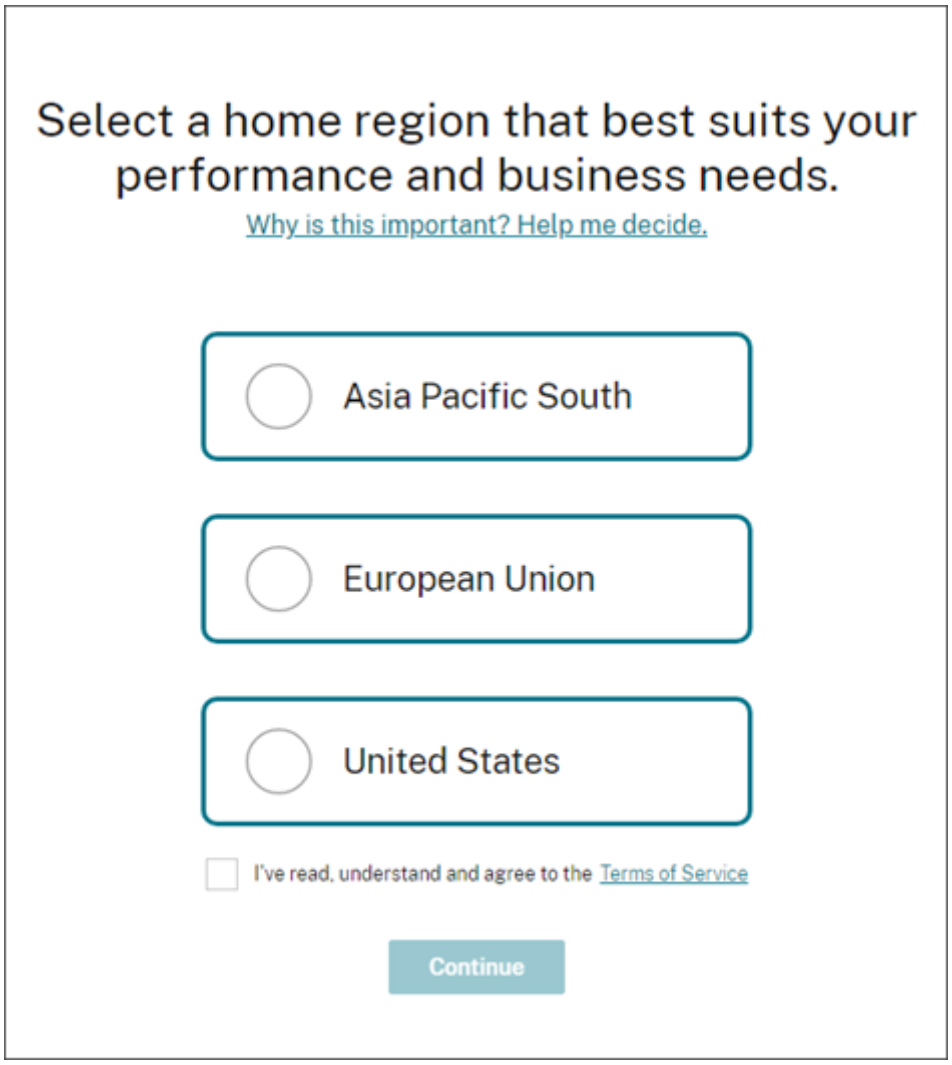


Wenn Sie diese Nachricht sehen, bedeutet dies, dass ein anderer Administrator Ihres Citrix-Kontos das Citrix Cloud-Konto bereits erstellt hat.

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.

Wenn Sie **Anfragegenehmigung** auswählen, werden alle bestehenden Administratoren des Kontos über Ihre Anfrage benachrichtigt. Wenn die bestehenden Administratoren nicht mehr in Ihrer Organisation sind, wenden Sie sich an den Citrix Support.

Schritt 2: Auswählen der Citrix Cloud-Region

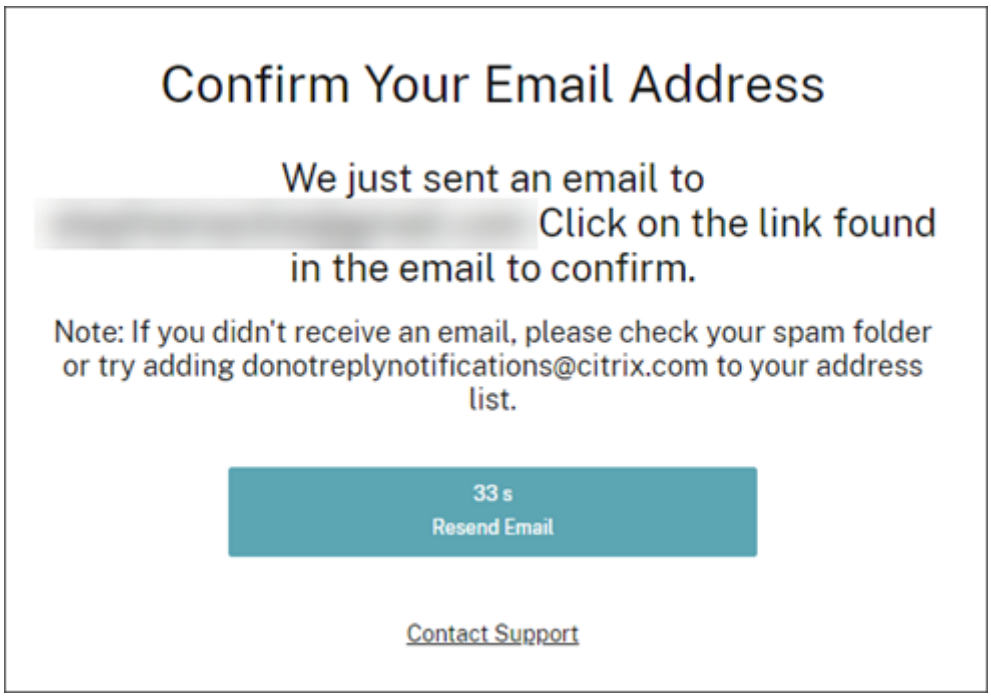


Eine Citrix Cloud-Region ist ein geografischer Raum, in dem Citrix Dienste und Daten für die Bereitstellung von Citrix Cloud Services betreibt, speichert und repliziert. Citrix verwendet u. U. mehrere öffentliche oder private Clouds in mindestens einem Land in der Region, um Dienste bereitzustellen. Weitere Informationen zu Citrix Cloud-Regionen finden Sie unter Geografische Überlegungen.

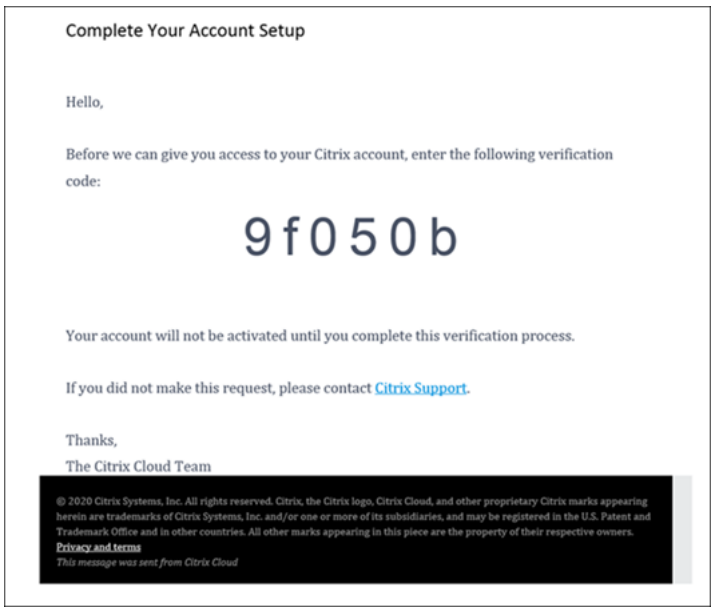
> **Wichtig:**
>
> Wenn Sie eine Region ausgewählt haben, kann Ihre Auswahl nicht rückgängig gemacht oder geändert werden.

Schritt 3: Verifizieren der E-Mail-Adresse

Wenn Ihre E-Mail-Adresse noch nicht verifiziert wurde, werden Sie möglicherweise aufgefordert, diese zu bestätigen.



Citrix Cloud sendet Ihnen eine Verifizierungs-E-Mail. Nachfolgend sehen Sie eine Beispiel-E-Mail:



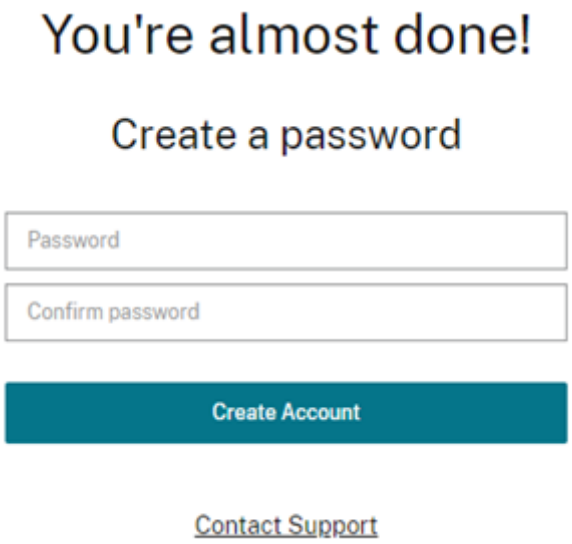
Wenn Sie die Verifizierungs-E-Mail erhalten und Ihre E-Mail-Adresse bestätigt haben, ist Ihr Citrix Cloud-Konto aktiviert.

Schritt 4: Auswählen eines Kennworts

> **Hinweis:**
>
> Citrix Cloud fordert Sie auf, nur dann ein Kennwort auszuwählen, wenn Sie zum ersten Mal ein

> Citrix Konto erstellen.

Geben Sie Ihr Citrix Cloud-Kennwort ein und bestätigen Sie es, um die Erstellung Ihres Kontos abzuschließen.

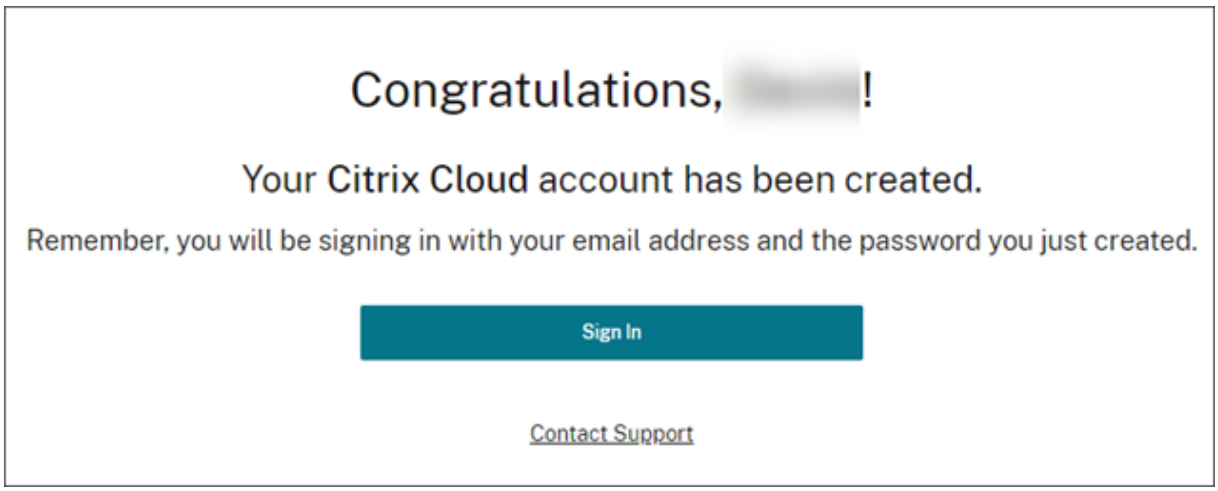


Bei Ihrem gewählten Kennwort wird zwischen Groß- und Kleinschreibung unterschieden, und es muss folgende Kriterien erfüllen:

- Mindestens 8 Zeichen
- Mindestens einen Großbuchstaben
- Mindestens eine Zahl
- Mindestens ein Symbol: ! @ # $ % ^ * ? + = -

Gültige Kennwörter dürfen keine Wörter, die im Wörterbuch stehen, enthalten. Wenn Citrix nach der Auswahl des Kennworts feststellt, dass Ihr Kennwort nicht ausreichend komplex ist oder in einer bekannten Datenbank mit kompromittierten Kennwörtern aufgeführt wird, werden Sie von Citrix Cloud möglicherweise dazu aufgefordert, das Kennwort bei der nächsten Anmeldung bei Citrix Cloud zu ändern. Weitere Informationen finden Sie unter Ändern des Kennworts.

Nachdem Ihr Konto erstellt wurde, können Sie sich bei Citrix Cloud anmelden.



Schritt 5: Registrierung für die mehrstufige Authentifizierung

Um die Sicherheit Ihres Administratorkontos zu gewährleisten, müssen Sie beim Anmelden bei Citrix Cloud die mehrstufige Authentifizierung verwenden. Die Registrierung für die mehrstufige Authentifizierung verhindert den unberechtigten Zugriff auf Ihr Administratorkonto und erfordert nur ein Gerät, z. B. einen Computer oder ein Mobilgerät, auf dem eine Authentifikator-App installiert ist, die dem Standard Zeitbasiertes Einmalkennwort entspricht, z. B. Citrix SSO.

Wenn Sie nicht für die mehrstufige Authentifizierung registriert sind, werden Sie bei der Anmeldung bei Citrix Cloud dazu aufgefordert.

Während der Registrierung präsentiert Citrix Cloud einen QR-Code und einen Schlüssel. Je nach verwendeter Authentifikator-App können Sie entweder den QR-Code scannen oder den Schlüssel eingeben, um Ihr Gerät zu registrieren. Für eine reibungslose Registrierung empfiehlt Citrix, die App vorher herunterzuladen und auf dem Gerät zu installieren.

Sie müssen in Citrix Cloud zudem mindestens zwei Wiederherstellungsmethoden konfigurieren, damit Sie den Zugriff auf Ihr Konto wiederherstellen können, falls Sie Ihr Gerät verlieren oder Ihre Authentifikator-App nicht verwenden können. Eine Telefonnummer für die Wiederherstellung ist erforderlich. Sie können auch eine Wiederherstellungs-E-Mail-Adresse angeben und Backupcodes generieren. Citrix empfiehlt dringend, eine Wiederherstellungs-E-Mail-Adresse anzugeben, über die Sie schnell einen Einmalcode erhalten und sich anmelden können. Anweisungen zum Wiederherstellen Ihres Citrix Cloud-Kontos mithilfe dieser Methoden finden Sie unter Wiederherstellen des Zugriffs auf Ihr Konto.

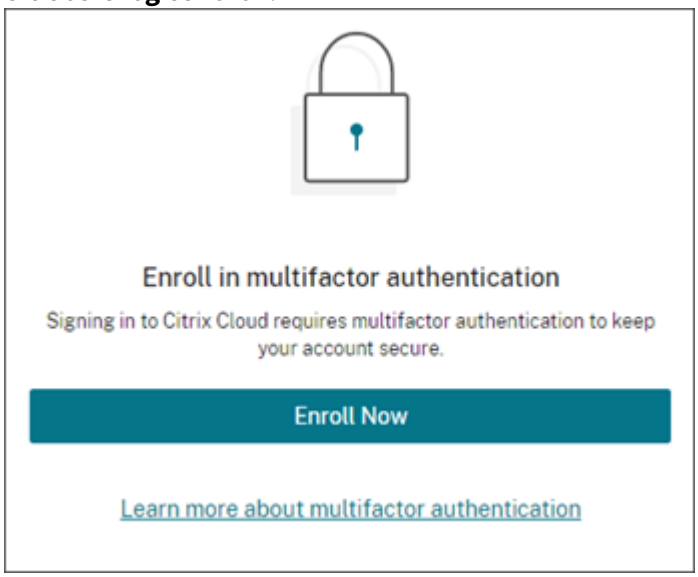
> **Hinweise:**
>
> - Stellen Sie bei der Anmeldung bei Citrix Cloud sicher, dass die Citrix Cloud-Anmeldeseite unter `https://accounts.cloud.com` angezeigt wird. Wenn Sie sich mit einer anderen URL bei Citrix Cloud anmelden (z. B. `https://accounts-internal.cloud.com`),

schlägt die Registrierung für die mehrstufige Authentifizierung fehl.

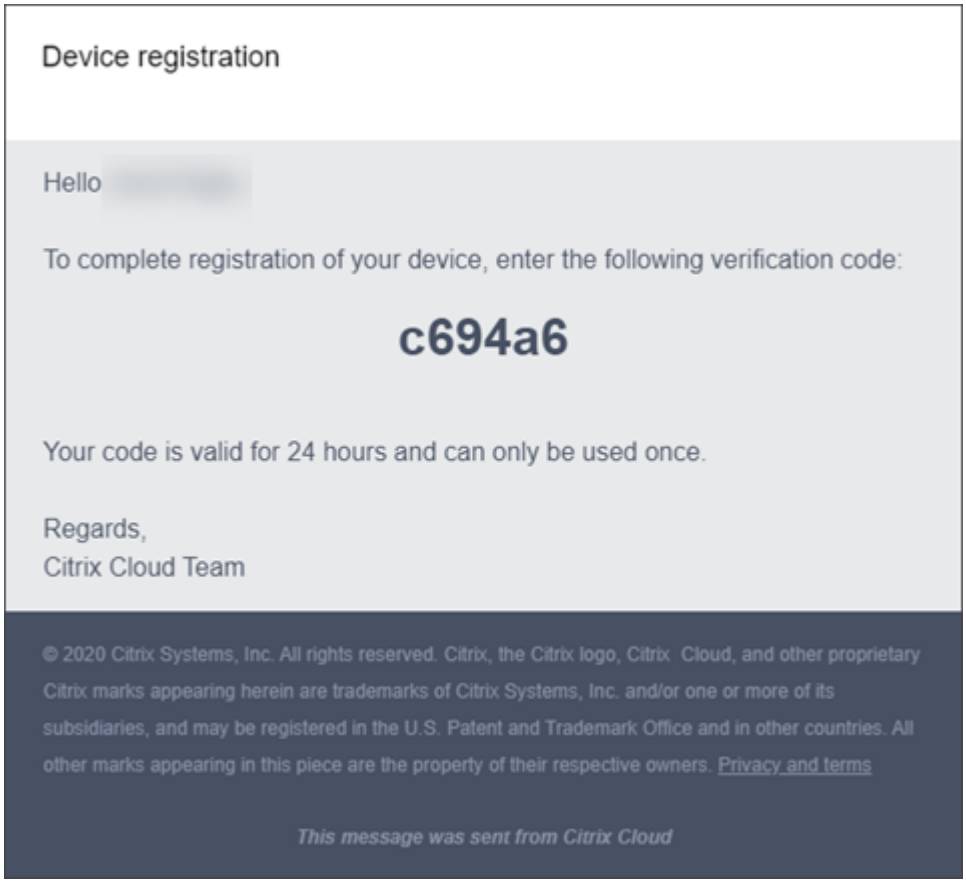
- Nur Administratoren unter dem Citrix-Identitätsanbieter können sich über Citrix Cloud für die mehrstufige Authentifizierung registrieren. Wenn Sie Azure AD zum Verwalten von Citrix Cloud-Administratoren verwenden, können Sie die mehrstufige Authentifizierung über das Azure-Portal konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von Azure AD Multi-Factor Authentication-Einstellungen auf der Microsoft-Website.
- Nach der Registrierung wird die mehrstufige Authentifizierung für alle Kundenorganisationen verwendet, denen Sie in Citrix Cloud angehören. Sie können die mehrstufige Authentifizierung nach Abschluss des Registrierungsvorgangs nicht 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 Ändern des Geräts für die mehrstufige Authentifizierung.

Registrieren des Geräts für die mehrstufige Authentifizierung

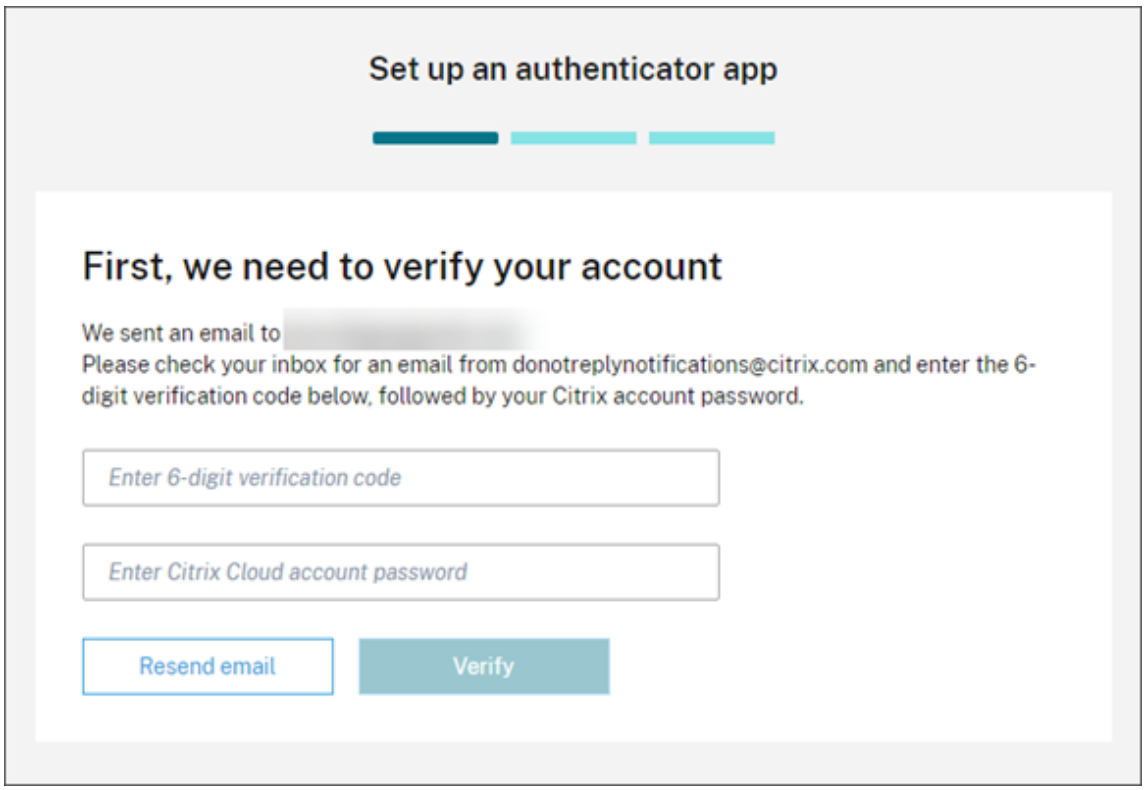
1. Gehen Sie zu https://citrix.cloud.com und vergewissern Sie sich, dass die URL auf `https://accounts.cloud.com` umleitet. Melden Sie sich mit Ihren Citrix Cloud-Anmeldeinformationen an.
2. Wenn Sie zur Registrierung für die mehrstufige Authentifizierung aufgefordert werden, wählen Sie **Jetzt registrieren**.



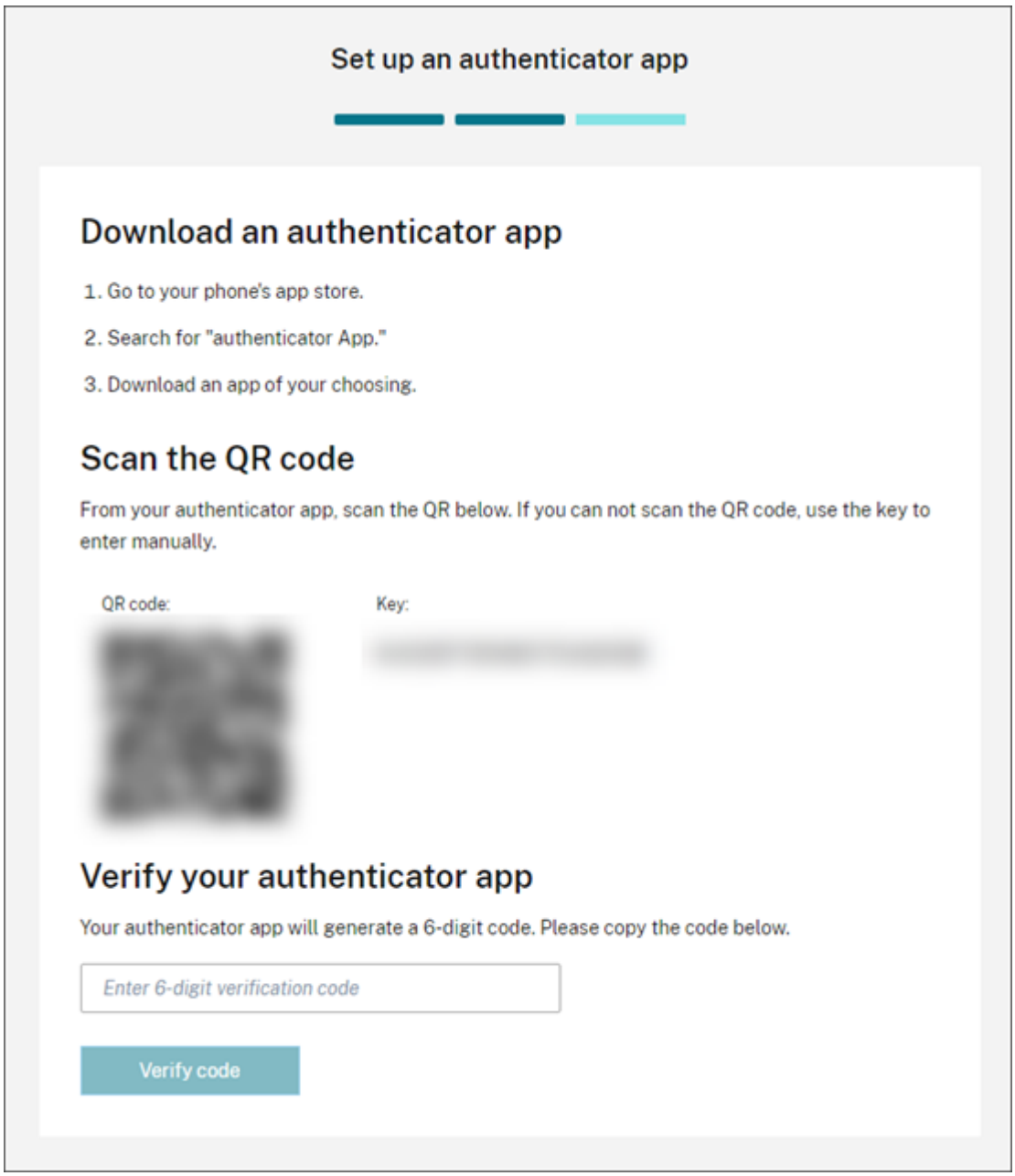
Citrix Cloud sendet Ihnen eine E-Mail mit einem Verifizierungscode.



3. Geben Sie nach Erhalt der E-Mail den 6-stelligen Verifizierungscode und Ihr Citrix Cloud-Kennwort ein, und wählen Sie **Überprüfen** aus.

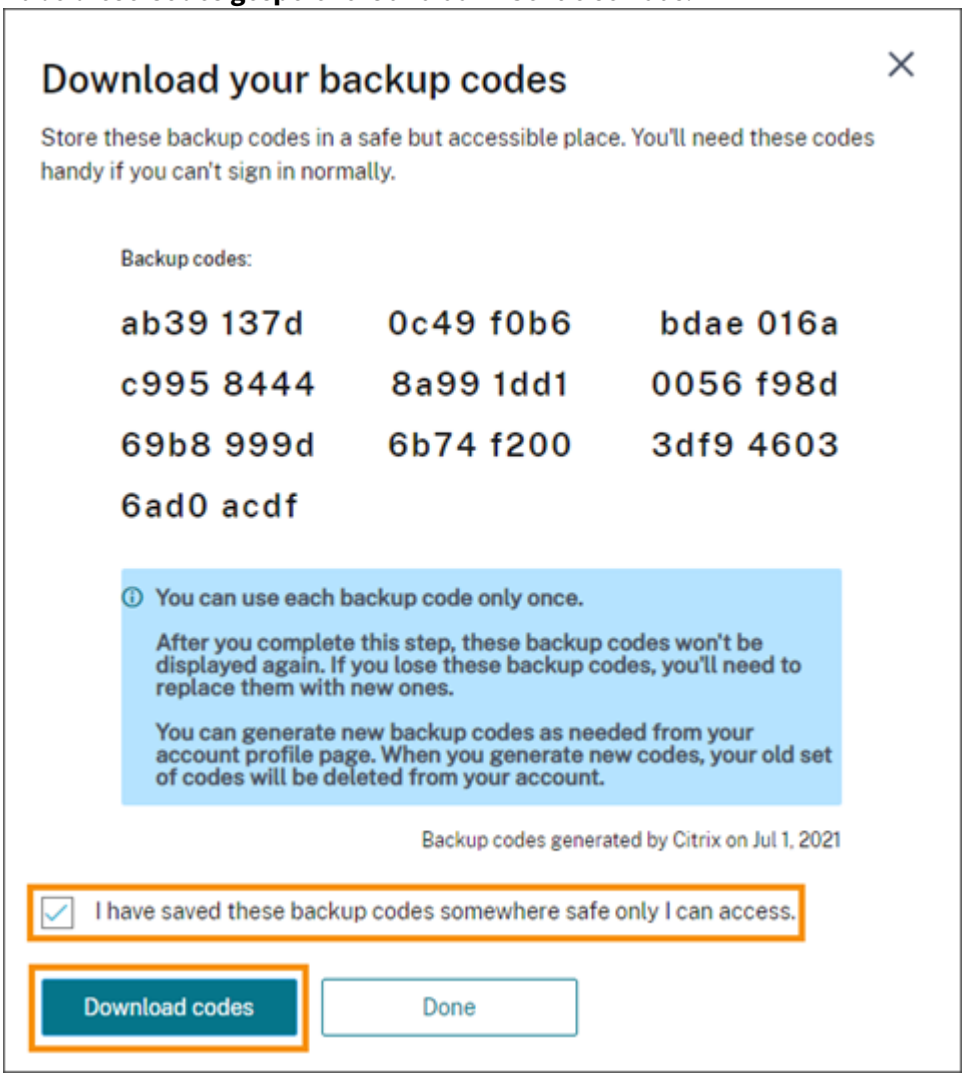


4. Scannen Sie in der Authentifikator-App den QR-Code, oder geben Sie den Schlüssel manuell ein. Die Authentifikator-App zeigt einen Eintrag für Citrix Cloud an und generiert einen 6-stelligen Code.



5. Geben Sie unter **Authentifikator-App verifizieren** den Code aus Ihrer Authentifikator-App ein, und wählen Sie **Code verifizieren** aus.
6. Konfigurieren Sie mindestens zwei der folgenden Methoden zur Kontowiederherstellung für den Fall, dass Sie Ihre Authentifikator-App nicht verwenden können:
   - Wiederherstellungstelefon (erforderlich): Wählen Sie **Wiederherstellungstelefon hinzufügen** und geben Sie eine Telefonnummer ein, über die ein Citrix Supportmitarbeiter Sie zur Identitätsprüfung anrufen kann. Citrix Support verwendet diese Telefonnummer nur, wenn Sie Hilfe zur Anmeldung anfordern. Citrix empfiehlt die Verwendung einer Festnetznummer.

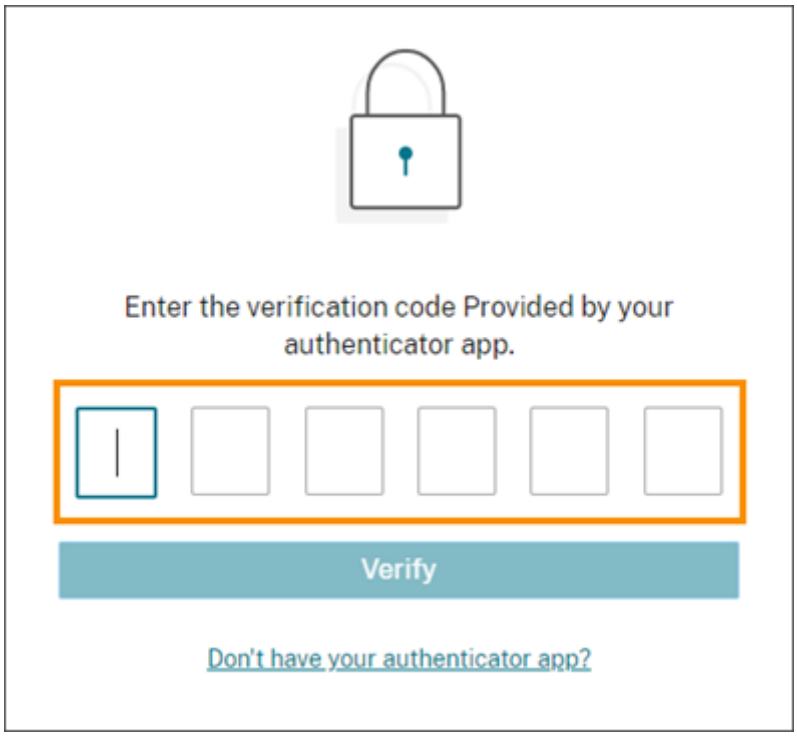
- Wiederherstellungs-E-Mail-Adresse (empfohlen): Wählen Sie **Wiederherstellungs-E-Mail-Adresse hinzufügen** und geben Sie eine E-Mail-Adresse ein, die sich von der für Citrix Cloud verwendeten unterscheidet. Über diese Adresse erhalten Sie von Citrix einen einmaligen Code, wenn Sie ihn anfordern. Nachdem Sie Ihre Adresse eingegeben haben, wählen Sie **Verifizierungs-E-Mail senden**. Citrix sendet Ihnen eine E-Mail mit einem Verifizierungscode. Geben Sie den Code ein und wählen Sie **Code verifizieren**.
- Backupcodes: Wählen Sie **Backupcodes generieren**, um mehrere Einmalcodes zu erstellen, mit denen Sie sich anmelden können, wenn Sie Ihre Authentifikator-App nicht verwenden können. Wählen Sie **Codes herunterladen**, wenn Sie dazu aufgefordert werden, um die Backupcodes als Textdatei herunterzuladen. Wählen Sie als Nächstes **Ich habe diese Codes gespeichert** und dann **Schließen** aus.



7. Wählen Sie **Fertig stellen** aus, um die Registrierung abzuschließen.

Wenn Sie sich das nächste Mal mit Ihren Citrix Cloud-Administratoranmeldeinformationen anmelden, werden Sie von Citrix Cloud zur Eingabe des Verifizierungscodes aus Ihrer Authentifikator-App aufge-

fordert.



Verwalten der Geräteregistrierung

Auf der Seite “Mein Profil” können Sie ein anderes Gerät registrieren, Ihre Wiederherstellungs-E-Mail-Adresse ändern, weitere Backupcodes generieren und Ihre Telefonnummer für die Wiederherstellung aktualisieren. Anweisungen finden Sie in folgenden Artikeln:

- Ändern des Geräts für die mehrstufige Authentifizierung
- Verwalten von Verifizierungsmethoden.

Schritt 6: Verifizieren der OrgID und Einladen von Administratoren

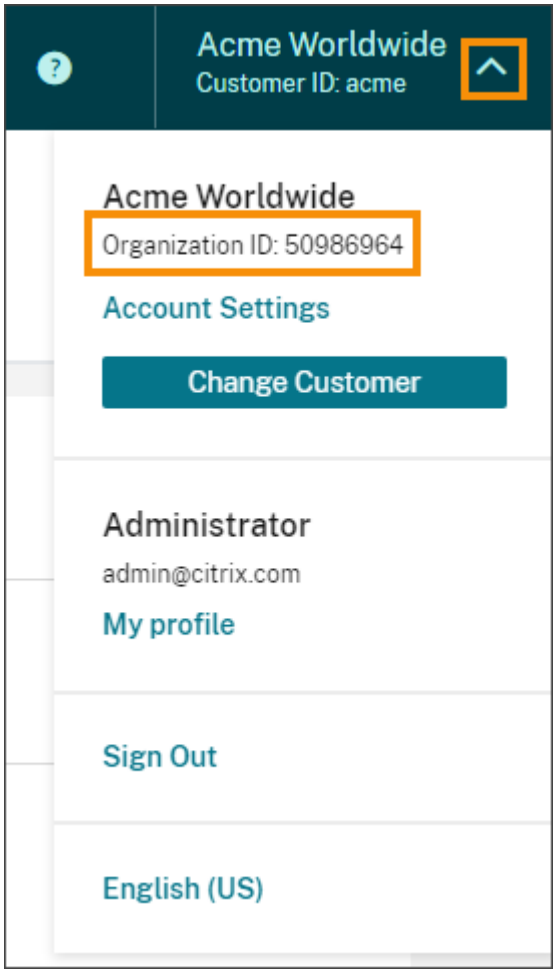
Herzlichen Glückwunsch, Ihr Citrix Cloud-Konto ist eingerichtet! Bevor Sie Citrix Cloud verwenden, verifizieren Sie Ihre OrgID und laden Sie weitere Administratoren zum Verwalten des Citrix Cloud-Kontos ein.

Verifizieren der Konto-OrgID

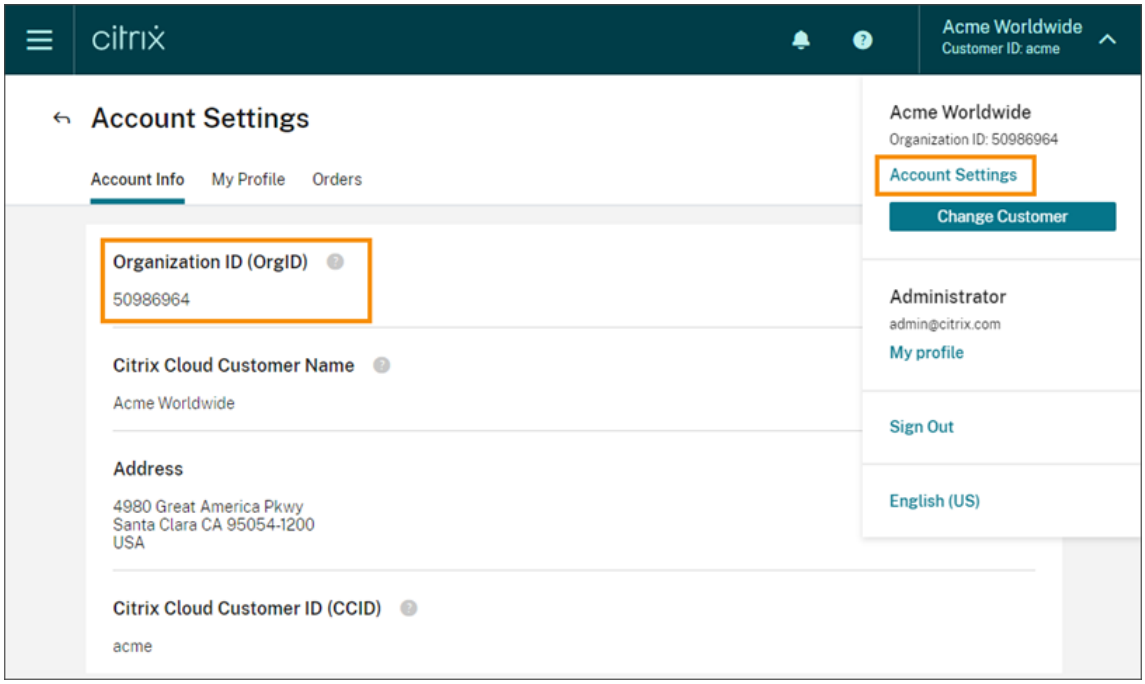
Stellen Sie sicher, dass die OrgID des Kontos mit der OrgID übereinstimmt, mit der Sie Bestellungen aufgeben. Einer der Vorteile von Citrix Cloud besteht darin, dass Sie einen Service ausprobieren können und alle von Ihnen in der Testversion vorgenommenen Konfigurationen beim Kauf erhalten bleiben, da 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.

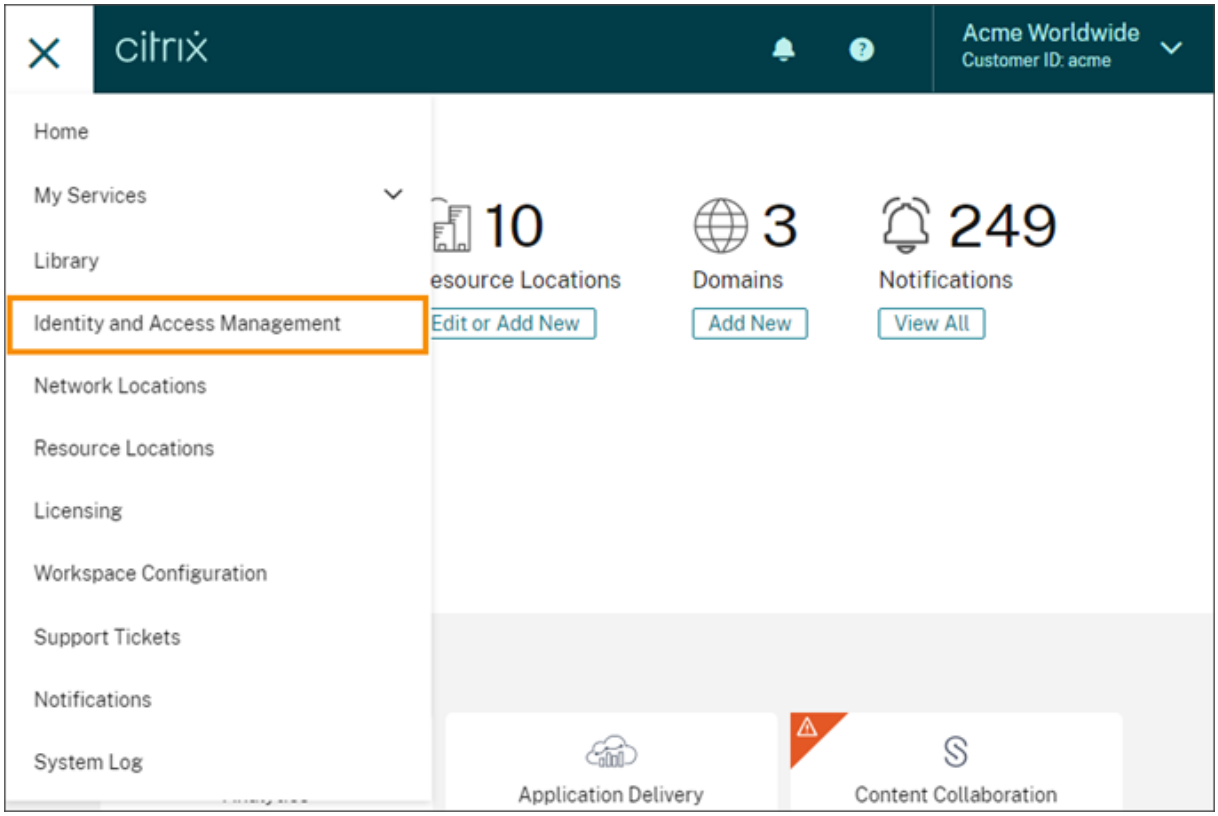


- Auf der Seite **den Kontoeinstellungen**. Wählen Sie im Kundenmenü die Option **Kontoeinstellungen**.



Einladen von Administratoren

Auch wenn die anderen Administratoren Zugriff auf das Citrix-Konto unter Citrix.com haben, müssen Sie sie dennoch zum Citrix Cloud-Konto einladen. Klicken Sie dazu in der Citrix Cloud-Verwaltungskonsole oben links auf die Menüschaltfläche und wählen Sie **Identitäts- und Zugriffsverwaltung**. Weitere Informationen finden Sie unter Hinzufügen von Administratoren zu einem Citrix Cloud-Konto.



Schritt 7: Anfordern von Testversionen der Citrix Cloud Services

Testversionen sind für einen Test Ihrer Infrastruktur oder einer öffentlichen Cloud mit Ihren Anwendungen und Microsoft Active Directory konzipiert. Sie können Services, Workspaces und Ressourcenstandorte einrichten und konfigurieren.

Wenn Sie während der Testphase ein Abonnementpaket erwerben möchten, ist dies jederzeit möglich. Ihre vorhandenen Konfigurationen werden alle gespeichert und sind dann zur weiteren Verwendung verfügbar.

Zum Anfordern einer Testversion klicken Sie auf “Testversion anfordern” für den Service, den Sie ausprobieren möchten. Weitere Informationen finden Sie unter Citrix Cloud Service - Testversionen.

Geografische Überlegungen

October 16, 2022

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

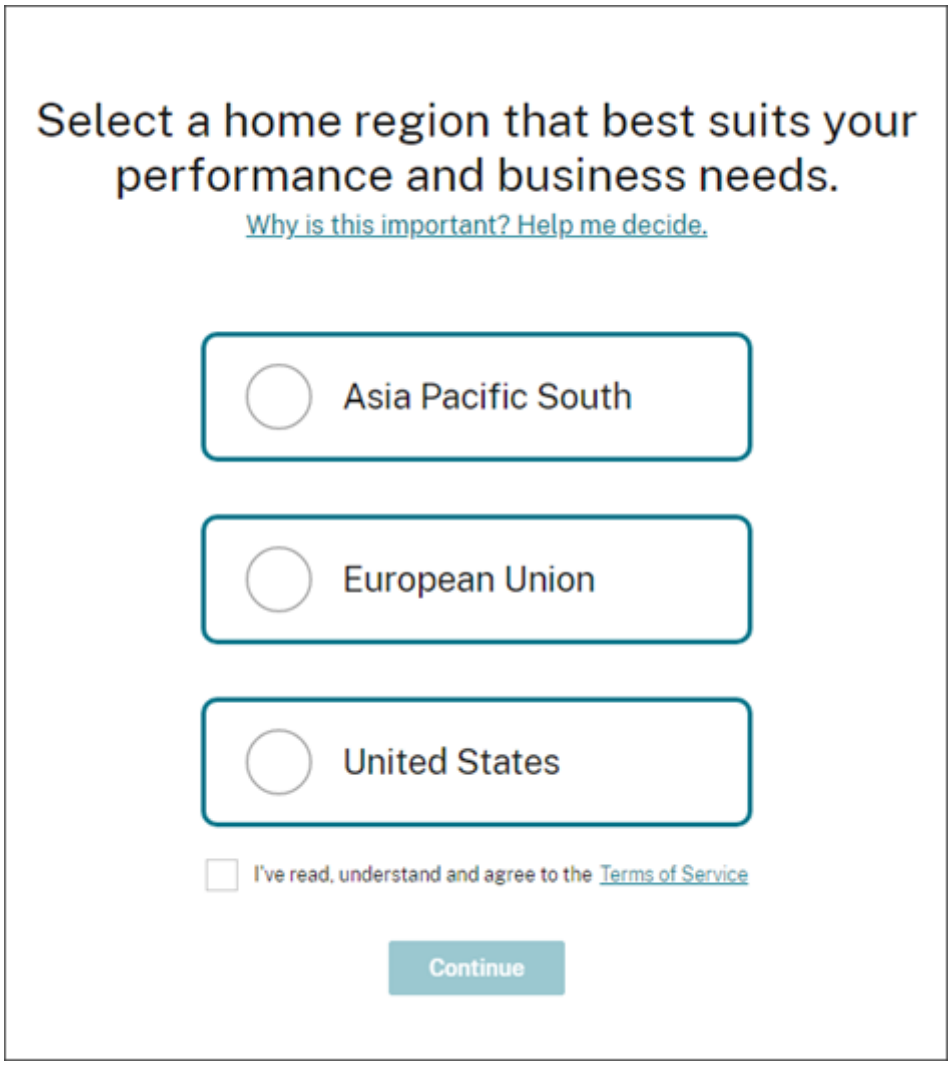
Weitere Informationen zu geografischen Regionen und Services, die Citrix für Cloud-Plattformen für den öffentlichen Sektor bzw. für dedizierte Umgebungen bietet, finden Sie unter Andere Cloud-Plattformen von Citrix in diesem Artikel.

Auswahl einer Region

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

- Vereinigte Staaten
- Europäische Union
- Asien-Pazifik

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 Sie sich nicht in einer Region befinden, die Citrix Cloud unterstützt, können Sie Citrix Cloud dennoch verwenden. Wählen Sie einfach die Region, die der Mehrheit Ihrer Benutzer am nächsten ist oder welche die besten Optionen für den Schutz der Integrität Ihrer Daten bietet.

Datenarten, die in Regionen gespeichert werden

In der Region werden bestimmte Metadaten zu Ihrer Umgebung gespeichert. Beispiel:

- Citrix Cloud-Administratorinformationen, einschließlich Name, Benutzername und Kennwort.
- Daten aus dem Datenverkehr, der von Ihren installierten Connectors durch Ihre Region geleitet wird. Zum Beispiel die von den Domänencontrollern verwendete Authentifizierungsdaten (im firmeneigenen Rechenzentrum verwaltet oder per Abonnement vom Anbieter einer öffentlichen Cloud) bleiben in Ihrer Region.
- Daten, anhand derer Benutzer Bibliotheksangeboten zugeordnet werden. Wenn Sie beispielsweise Microsoft Office der Bibliothek als Angebot für Ihre Benutzer hinzufügen und Sie dann dem Angebot fünf Benutzer als Abonnenten hinzufügen, werden die Daten, die die einzelnen Benutzer mit dem Angebot verknüpfen (z. B. Benutzername und Domänenname), in Ihrer Region gespeichert.
- Daten über Benutzer der in Ihrer Region verfügbaren Services. Wenn Sie beispielsweise Endpoint Management in Ihrer Region verwenden, werden Daten wie Name, Adresse und Telefonnummer in der Region gespeichert.

Servicepräsenz in jeder Region

Alle Services sind weltweit verfügbar, unabhängig von der Region, die Sie für Ihre Organisation auswählen. Außerdem werden Ihre Daten möglicherweise global von Citrix Subprozessoren oder verbundenen Unternehmen 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.

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.

Wenn ein Service global repliziert wurde, werden alle Daten für den Service in allen Regionen gespeichert.

Service	USA	EU	Asien-Pazifik	Hinweise
Citrix Cloud-Steuerungsebene	Ja	Ja	Ja	
Citrix Analytics für Sicherheit	Ja	Ja	Ja	
Citrix Analytics für Leistung	Ja	Ja	Ja	
Citrix App Delivery and Security Service – Citrix Managed	Ja	Ja	Ja	
Application Delivery Management	Ja	Ja	Ja	Weitere Informationen finden Sie unter Low-Touch-Onboarding von Citrix ADC-Instanzen mithilfe von Application Delivery Management Service Connect in diesem Artikel.

Service	USA	EU	Asien-Pazifik	Hinweise
Citrix Content Collaboration	Ja	Ja	Nein - Wählen Sie zwischen USA oder EU	Speicherzone kann aus mehreren Standorten ausgewählt werden. Weitere Informationen finden Sie unter Content Collaboration-Standorte und Speicherzonen in diesem Artikel.
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 Premium für Google Cloud (früher Virtual Apps and Desktops Premium für Google Cloud)	Ja	Nein - verwendet Region USA	Nein - verwendet Region USA	

Service	USA	EU	Asien-Pazifik	Hinweise
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.
SD-WAN Orchestrator	Ja	Ja	Ja	
Remote Browser Isolation-Dienst	Ja	Ja	Ja	Der Service verwendet die Citrix Cloud-Region.
Citrix Secure Private Access	Global repliziert	Global repliziert	Global repliziert	
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	
Citrix Workspace	Ja	Ja	Ja	Der Service verwendet die Citrix Cloud-Region.

Service	USA	EU	Asien-Pazifik	Hinweise
Workspace Environment Management	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	
Citrix Gateway-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	
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 über die Daten, die von den einzelnen Services gespeichert werden, finden Sie unter Technische Sicherheit für den jeweiligen Service.

Low-Touch-Onboarding von Citrix ADC-Instanzen mithilfe von Application Delivery Management Service Connect

Das kontaktarme Low-Touch-Onboarding von ADC-Instanzen auf der Basis von Application Delivery Management (ADM) Service Connect umfasst Folgendes:

- Wenn Sie bereits ein Citrix Cloud-Kunde sind, wird der ADM 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 ADM Service-Platzhaltermandant wird in der geografischen Region erstellt, die der Region dieser angegebenen Adresse entspricht. Bei einem zukünftigen Citrix Cloud-Onboarding wird der ADM Service-Mandant in der geografischen Region erstellt, die Sie beim Erstellen Ihres Citrix Cloud-Kontos ausgewählt haben. Außerdem werden die Daten des ADM Service-Platzhaltermandanten zum neuen ADM Service-Mandanten migriert.

Endpoint Management-Servicestandorte

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

- US East
- US West
- EU West
- 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

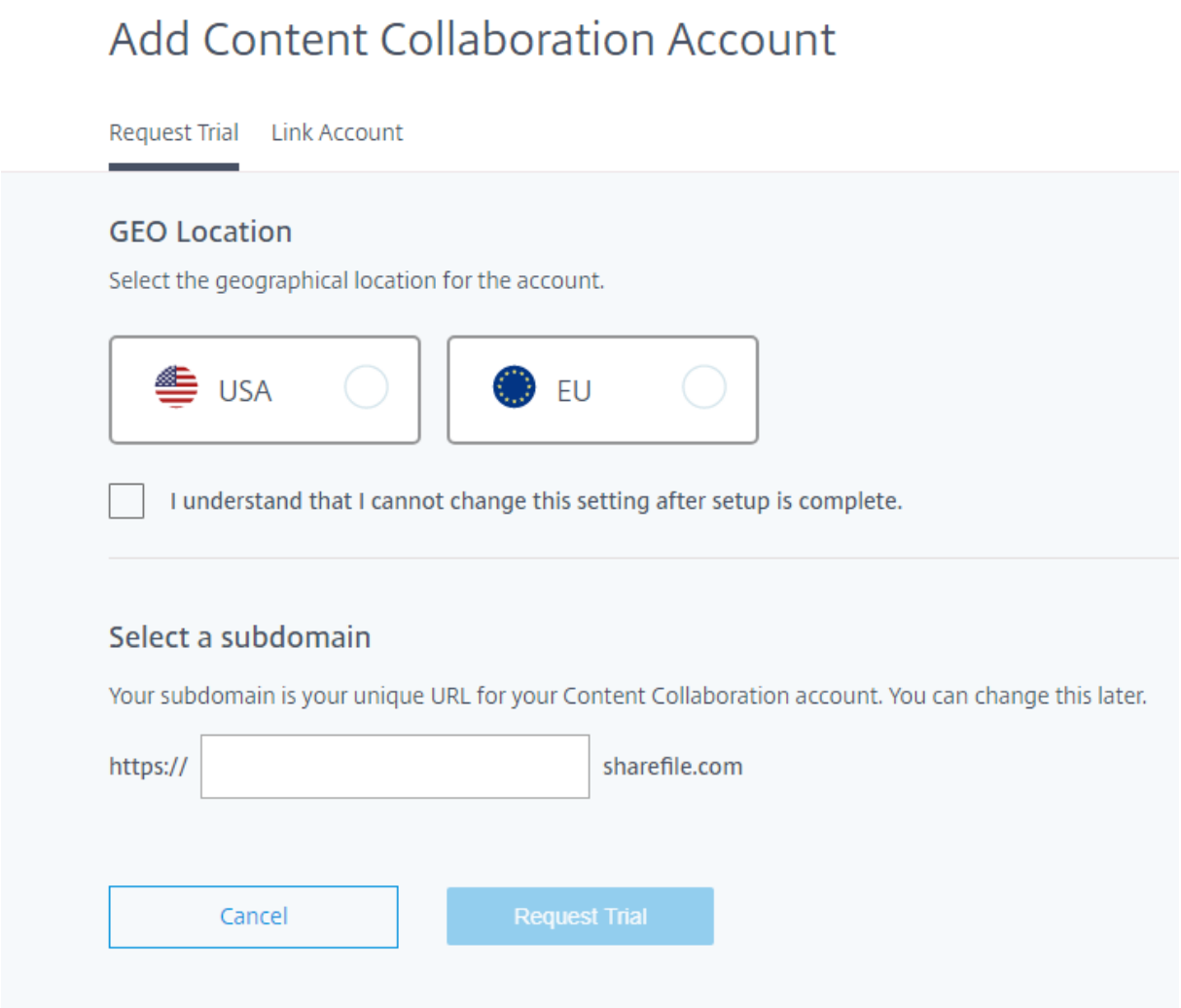
- London, Großbritannien
- Manchester, Großbritannien
- Frankfurt, Deutschland
- Düsseldorf, Deutschland
- Mannheim, Deutschland
- Paris, Frankreich

Europa

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

Content Collaboration-Standorte und Speicherzonen

Wenn Sie ein Content Collaboration-Konto in Citrix Cloud einrichten, können Sie eine Region in den USA oder in der EU auswählen. Ihre Content Collaboration-Region ist unabhängig von Ihrer Citrix Cloud-Region. Wie bei der Citrix Cloud-Region können Sie die Content Collaboration-Region jedoch nicht mehr ändern, wenn Sie die Einrichtung des Content Collaboration-Kontos abgeschlossen haben.



Bei Content Collaboration-Konten, die in Citrix Cloud erstellt werden, ist Ihre Standardspeicherzone zunächst in der Region USA.

Bei ShareFile Enterprise-Konten, die außerhalb von Citrix Cloud erstellt werden, ist Ihre Speicherzone in der von Ihnen gewählten Region, entweder in den USA oder in der EU. Die Verknüpfung mit Citrix Cloud ändert Ihre Auswahl nicht.

Nachdem Ihr Content Collaboration-Konto eingerichtet wurde, können Sie Speicherzonen auf der ganzen Welt aktivieren und deaktivieren sowie eine neue Standardzone auswählen. Sie können auch einen bestimmten Standard für einzelne Benutzer oder Ordner basierend auf den Speicherzonen angeben, die in der Content Collaboration-Verwaltungskonsole aktiviert sind. Folgende Standorte stehen zur Auswahl:

- Japan
- Singapur
- Australien

- Europäische Union
- Kanada
- USA - Osten
- USA - Westen
- USA - Nordwesten
- Brasilien

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.

Verifizieren Ihrer E-Mail-Adresse für Citrix Cloud

January 26, 2022

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.

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 E-Mail erhalten. Welche Schritte sind erforderlich? Gehen Sie wie folgt vor:

- Suchen Sie im Posteingang nach einer E-Mail von "Citrix".
- 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.
- 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.

Kontaktaufnahme mit dem technischen Support von Citrix

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

Citrix Cloud Services – Testversionen

April 29, 2022

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
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.

Kulanzzeitraum und Datenspeicherung bei Testversionen

Für die meisten Service-Testversionen gilt ein Kulanzzeitraum, sodass Sie nach Ablauf der Testversion weiterhin auf den Service zugreifen können. Der Kulanzzeitraum ermöglicht es Ihnen, einen Service zu abonnieren, ohne dessen Bereitstellung für die Benutzer zu unterbrechen. Wenn Sie sich gegen ein Abonnement entscheiden, können Sie während des Kulanzzeitraums alle Daten entfernen, die Sie

dem Service hinzugefügt haben. Nach Ablauf des Kulanzzeitraums sperrt Citrix den Zugriff auf den Service.

Citrix speichert alle Daten, die Sie einem Service hinzugefügt haben, für 90 Tage nach Ablaufdatum. Nach Ablauf von 90 Tagen löscht Citrix diese Daten.

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 Ser-

vice 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**.

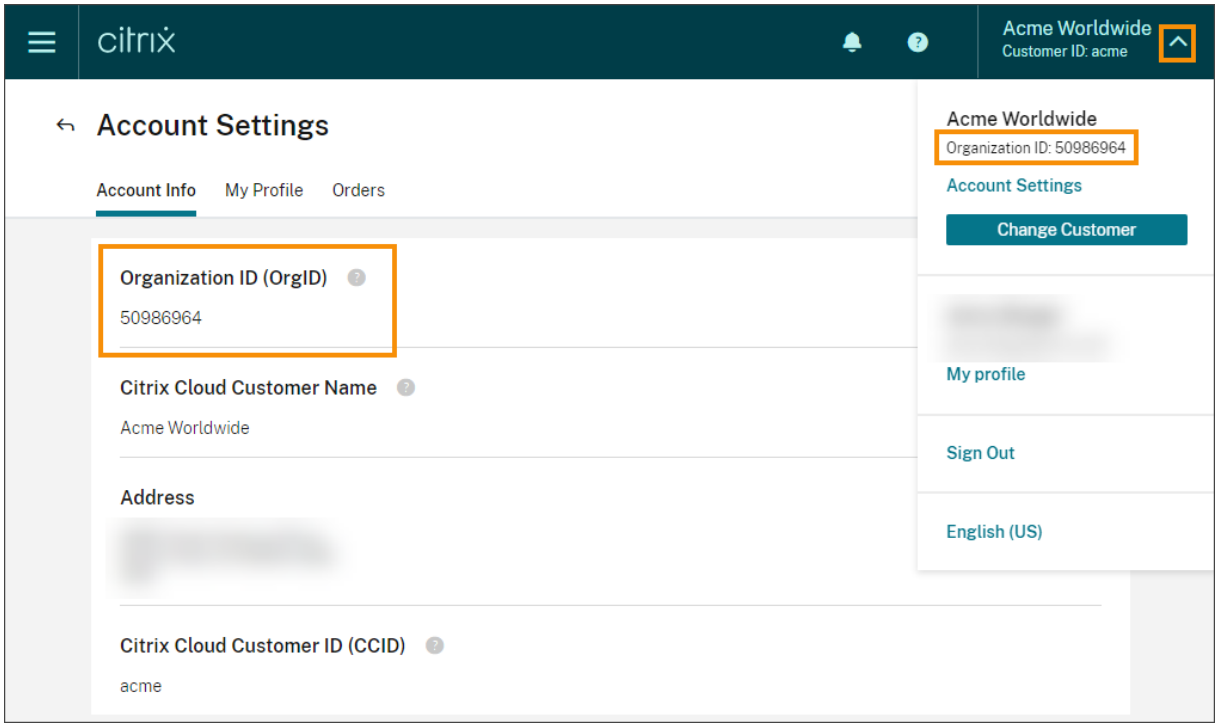
Sobald die Testversion genehmigt und einsatzbereit ist, sendet Citrix Ihnen eine E-Mail-Benachrichtigung.

> **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, besuchen Sie https://www.citrix.com/products/citrix-cloud/.

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.

Verlängern von Citrix Cloud-Serviceabonnements

September 1, 2022

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 zum CSP-Programm finden

> Sie unter Citrix Service Provider Program FAQ.

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: Dienstkulanzzeitraum

Wenn Ihr Abonnement abläuft, gewährt Citrix einen Kulanzzeitraum, während dessen Sie Ihr Abonnement verlängern oder Ihre Daten aus dem Service entfernen können. Der Kulanzzeitraum ist bei Monats- und Jahresabonnements unterschiedlich.

Monatliche Abonnements

Wenn Sie ein monatliches Abonnement kündigen, sendet Citrix Ihnen zum Ablaufdatum eine E-Mail mit einer Ablaufbenachrichtigung. Das Ablaufdatum ist der letzte Tag des Monats, in dem Sie das Abonnement kündigen. Nach Ablauf können, erlaubt Citrix Administratoren und Benutzern weitere fünf Tage lang den Zugriff auf den Service. Während dieser Zeit können Administratoren nur

Enumerations- und Löschfeatures nutzen. Citrix stellt die Gebühren für jegliche Ressourcennutzung während des fünftägigen Kulanzzeitraums in Rechnung.

Wenn Sie Ihr Abonnement während des Kulanzzeitraums nicht verlängern, sperrt Citrix nach Ablauf der Frist den Zugriff auf den Service für Administratoren und Benutzer. Zur Erinnerung sendet Citrix eine E-Mail-Benachrichtigung in folgenden Abständen:

- Ein Tage nach Ablauf (fünf Tage vor Sperrung des Service)
- Drei Tage nach Ablauf (zwei Tage vor Sperrung des Service)

Nach Ablauf des Kulanzzeitraums werden alle mit dem Service verknüpften Ressourcen heruntergefahren. Wenn Sie Daten, die Sie dem Service nach Ablauf des Kulanzzeitraums hinzugefügt haben, abrufen müssen, können Sie innerhalb von 30 Tagen nach dem Service-Ablaufdatum eine entsprechende Anfrage an den technischen Support von Citrix senden.

Jahres- und Mehrjahresabonnements

Bei Jahres- und Mehrjahresabonnements erlaubt Citrix bei Ablauf des Serviceabonnements weitere 30 Tage Zugriff auf den Dienst. Wenn Sie Ihr Abonnement in dieser Zeit nicht verlängern, sperrt Citrix nach Ablauf der Frist den Zugriff auf den Dienst für Administratoren und Benutzer. Zur Erinnerung sendet Citrix eine E-Mail-Benachrichtigung in folgenden Abständen:

- 15 Tage nach Ablauf (15 Tage vor Sperrung des Dienstes)
- 22 Tage nach Ablauf (sieben Tage vor Sperrung des Dienstes)
- 29 Tage nach Ablauf (einen Tag vor Sperrung des Dienstes)

Die E-Mail-Benachrichtigung enthält eine Liste der abgelaufenen Dienste und ihre Ablaufdaten.

Wenn Sie Ihr Abonnement während des 30-tägigen Kulanzzeitraums verlängern, beginnt Ihre Abonnementlaufzeit mit dem ursprünglichen Ablaufdatum des Service. Wenn der Service beispielsweise am 31. Mai abläuft und Sie Ihr Abonnement am 25. Juni verlängern (also vor Ende des Kulanzzeitraums), beginnt das neue Abonnement am 31. Mai.

Support im Kulanzzeitraum

Wenn bei dem Service während des Kulanzzeitraums ein technisches Problem auftritt, müssen Sie das Abonnement verlängern, bevor Sie eine Supportanfrage einreichen. Citrix bietet keine Unterstützung für Services mit abgelaufenem Abonnement.

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 30 Tage nach Ablaufdatum. Wenn Sie Ihr Abonnement vor Ablauf des 30-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 1. jedes Folgemonats.
- Die Verlängerung von Jahres- und Mehrjahresabonnements beginnt zu dem Termin, an dem Sie die Verlängerung erworben haben.

Wenn Sie Ihr Abonnement vor Ablauf des 30-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 30-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

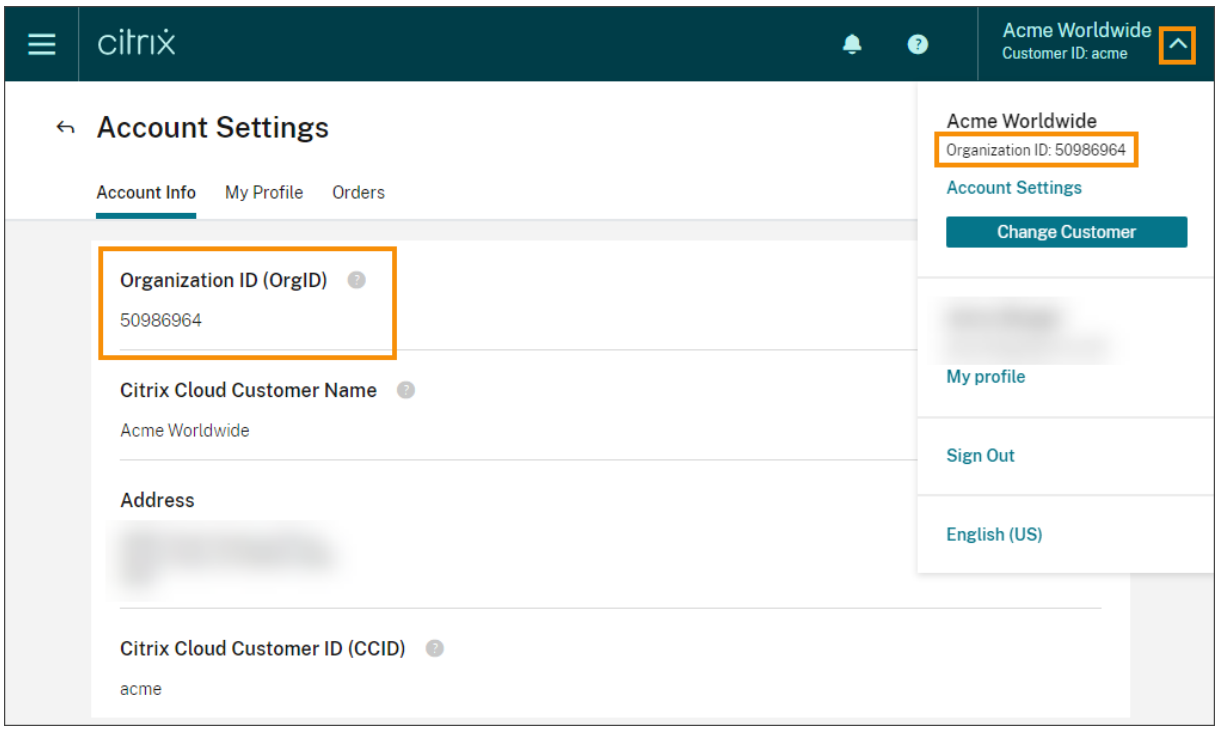
Wenn Sie Ihr eigenes Azure-Abonnement für einen Citrix Cloud-Service verwenden, installiert der Service eine App, wenn Sie das Azure-Abonnement mit dem Service verbinden. Wenn Sie Ihr Citrix Cloud-Abonnement nicht verlängern, entfernt Citrix diese App nicht aus Ihrem Azure-Abonnement, wenn der 30-tägige 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

Unter https://www.citrix.com/products/citrix-cloud/ können Sie Ihr Abonnement für Citrix Cloud Services verlängern.

Sie benötigen für den Kauf die ID Ihres Unternehmens, die Sie in der Citrix Cloud-Verwaltungskonsole finden. Diese finden Sie oben rechts in der Konsole oder unter den Kontoeinstellungen.



Anforderungen an System und Konnektivität

October 16, 2022

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 auszuführen. 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
- Microsoft Internet Explorer 11
- 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 beim späteren Ausführen bestimmter Prozesse.

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.

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:

- Analytics
- Content Collaboration
- Citrix DaaS (früher "Citrix Virtual Apps and Desktops Service")
- 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 folgender Intervalle beendet:

- Sitzung im Leerlauf (keine Konsolenaktivität erkannt): 60 Minuten
- Maximales Sitzungstimeout (unabhängig von der Konsolenaktivität): 24 Stunden

Nach Ablauf des maximalen Sitzungstimeouts gehen alle nicht gespeicherten Konfigurationsänderungen verloren und der Administrator muss sich erneut anmelden.

Registrieren Ihrer On-Premises-Produkte

Wenn Sie Citrix Cloud mit Citrix Lizenzserver zum Registrieren Ihrer On-premises-Produkte verwenden, müssen die folgenden Adressen kontaktiert werden können:

- `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 mit dem Cloud Connector befindet sich 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.

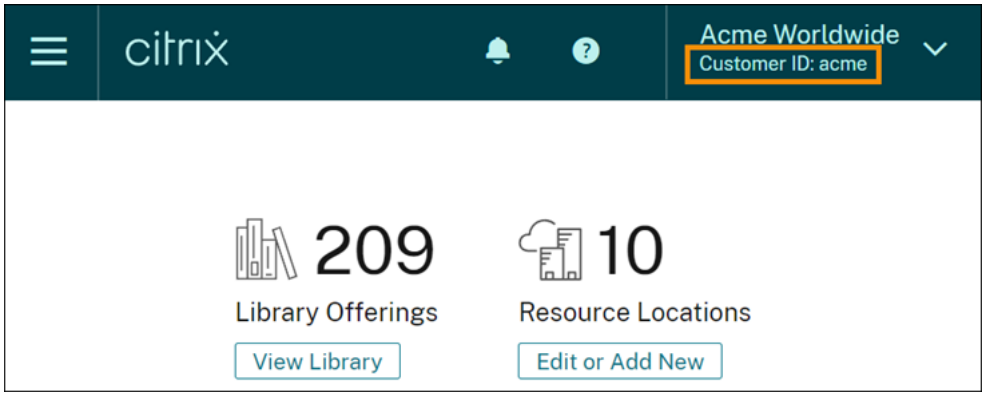
Wenn Sie Citrix Cloud mit Citrix Lizenzserver zum Registrieren Ihrer On-premises-Produkte verwenden, finden Sie unter Registrieren Ihrer On-Premises-Produkte in diesem Artikel Informationen zu zusätzlich erforderlichen kontaktierbaren Adressen.

Positivliste der FQDNs für den Cloud Connector

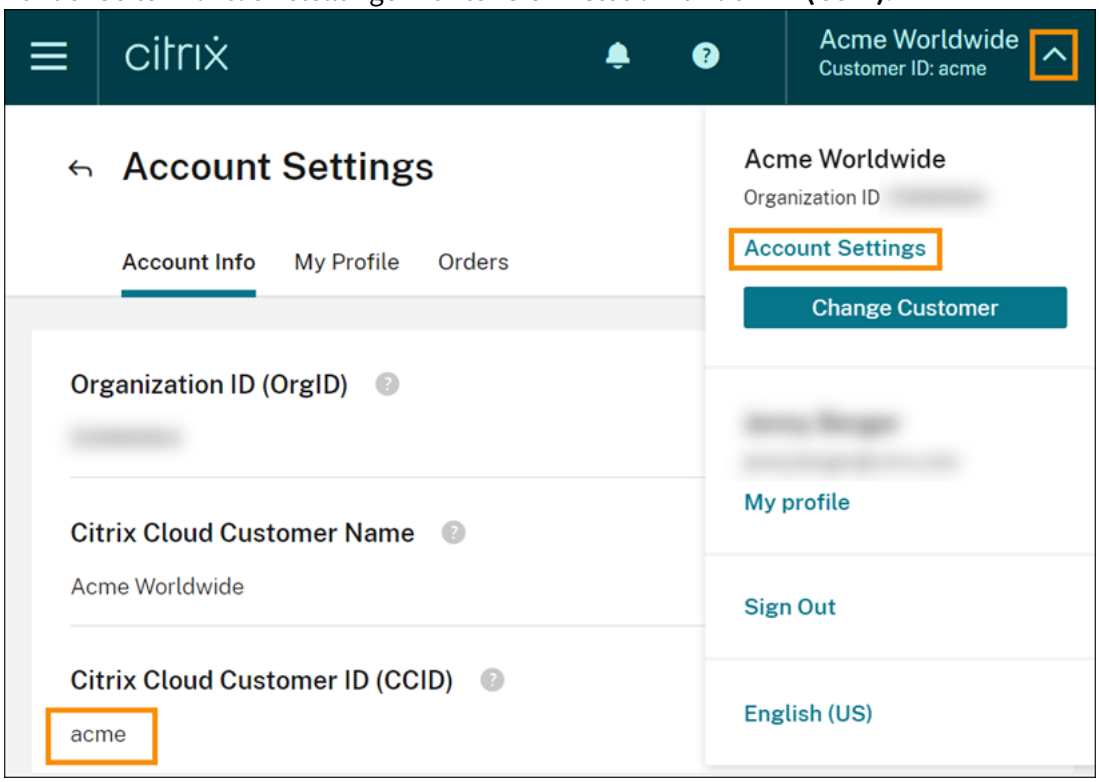
Eine vollständige Liste der vollqualifizierten Domainnamen (FQDNs), auf die der Cloud Connector zugreift, finden Sie in der JSON-Datei unter https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.json. Die Liste ist nach Produkt unterteilt und enthält ein Änderungsprotokoll 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:

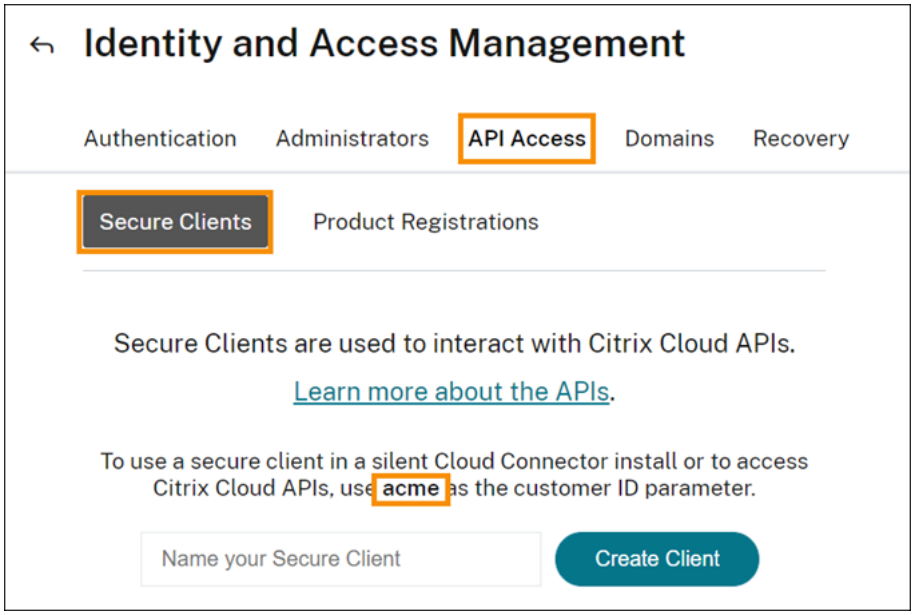
- Oben rechts unter dem Kundennamen Ihres Citrix Cloud-Kontos.



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



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



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 mit der Connector Appliance 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 des Application Delivery Management Service

Die vollständigen Anforderungen an die Internetkonnektivität finden Sie im Artikel zu Unterstützten Ports.

Content Collaboration-Servicekonnektivität

Citrix Ressourcenstandort / Cloud Connector:

- Verbindungsanforderungen für den Cloud Connector
- `https://*.sharefile.com`
- Zusätzliche Voraussetzungen: ShareFile Firewall Configuration and IP Address (CTX208318)
- Für produktinterne Meldungen einschließlich zu neuen Features und wichtigen Informationen: `https://citrix-cloud-content.customer.pendo.io/`

Verwaltungskonsole:

- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- Zusätzliche Voraussetzungen: ShareFile Firewall Configuration and IP Address (CTX208318)

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

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.

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 kann nicht für Citrix Gateway-Adressen durchgeführt werden. Auf einigen Proxys wird durch Aktivieren des SSL-Abfangens u. U. ein erfolgreicher Verbindungsaufbau zwischen Cloud Connector und Citrix Cloud verhindert.

Citrix 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/

Um sicherzustellen, dass Abonnenten erfolgreich auf ihre Inhalte in Citrix Files und Content Collaboration über Workspace zugreifen können, empfiehlt Citrix, die unter CTX208318 aufgeführten Domänen in eine Positivliste aufzunehmen.

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
  - *.cloud.com
  - *.citrixworkspacesapi.net
  - Adressen, die von einem externen Identitätsanbieter benötigt werden (sofern dieser in Ihrer Umgebung verwendet wird)
- FAS-Dienst, unter dem Netzwerkdienstkonto: *.citrixworkspacesapi.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.

Workspace Environment Management Service-Konnektivität

https://*.wem.cloud.com

Verbindung mit Citrix Cloud herstellen

September 22, 2022

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

- (Preview) Mit dem **Hypervisor Management Service** können Sie Updates für Ihre Citrix Hypervisor 8 Cloud-Pools von der Cloudsteuerungsebene aus verwalten. Durch Umstellen auf ein kontinuierliches Aktualisierungsmodell, von Citrix Cloud orchestriert, können Citrix Hypervisor-Kunden von einem effizienten Releaseprozess profitieren, mit dem neue Funktionen schneller bereitgestellt werden. Weitere Informationen finden Sie unter Citrix Hypervisor Cloud.
- Mit **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

October 16, 2022

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.

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 2012 R2, 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 Bereitstellungen 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

September 27, 2022

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
- Windows Server 2012 R2

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.
- Bei Verwendung von Internet Explorer als Standard-Systembrowser müssen Sie die verstärkte Sicherheitskonfiguration für Internet Explorer (IE ESC) deaktivieren. Wenn diese Einstellung aktiviert ist, kann der Cloud Connector möglicherweise keine Verbindung mit Citrix Cloud herstellen.
- Citrix empfiehlt dringend, Windows-Updates auf allen Maschinen zu aktivieren, auf denen ein Cloud Connector gehostet wird. Konfigurieren Sie Windows bei der Konfiguration von Windows Update so, dass Updates außerhalb der Geschäftszeiten automatisch heruntergeladen und installiert werden, lassen Sie jedoch keine automatischen Neustarts für mindestens 4 Stunden zu. Die Citrix Cloud-Plattform steuert Maschinenneustarts, wenn sie erkennt, dass ein Update auf einen Neustart wartet, und ermöglicht einen Neustart für jeweils nur einen Cloud Connector. Sie können über Gruppenrichtlinien oder einem Systemverwaltungstool einen Fallback-Neustart für den Fall konfigurieren, dass die Maschine nach einem Update neu gestartet werden muss. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart.

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://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`
- Folgende Zertifikate werden installiert:
  - `https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt`
  - `https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootG2.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootCA.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`

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 unter Anforderungen an System und Konnektivität.

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

Funktionsebene:	Domänenfunktionsebene	Unterstützte Domänencontroller
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
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

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

Dienstname	Beschreibung	Ausgeführt als
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
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

Dienstname	Beschreibung	Ausgeführt als
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
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. Durch Verschachteln von "forest2.local"-Benutzern in "forest1.local"-

Sicherheitsgruppen lässt sich dieses Problem 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

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 Citrix ADC verwenden, wird evtl. für jeden STA-Server als ID in der ADC-Verwaltungskonsole und in der ICA-Datei für Anwendungs- und Desktopstarts als **CWSSTA** 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 ADC-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

Konfiguration von Cloud Connector-Proxy und Firewall

May 25, 2022

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 unter Anforderungen an System und Konnektivität. Eine Liste mit häufigen Adressen für die meisten Citrix Cloud Services samt ihrer Funktion finden Sie unter Verbindungsanforderungen für Cloud Connectors.

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.

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

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.

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

> **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.

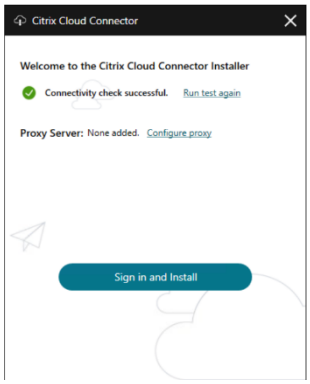
Installer

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 anzugeben.

> **Hinweis:**
>
> Die automatische Erkennung, PAC-Skripts oder authentifizierte Proxys werden nicht unterstützt.

Cloud Connector-Installation

September 27, 2022

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.

- 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.
- Verschieben Sie nach der Installation die Maschine, auf der der Cloud Connector gehostet wird, nicht in eine andere Domäne. Wenn Sie die Maschine in eine andere Domäne verschieben müssen, deinstallieren Sie den Cloud Connector und installieren Sie ihn wieder, nachdem die Maschine in die neue Domäne eingefügt wurde.
- Lassen Sie nach der Installation alle Cloud Connectors dauerhaft eingeschaltet, um eine ständige Verbindung mit Citrix Cloud sicherzustellen.

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.

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.

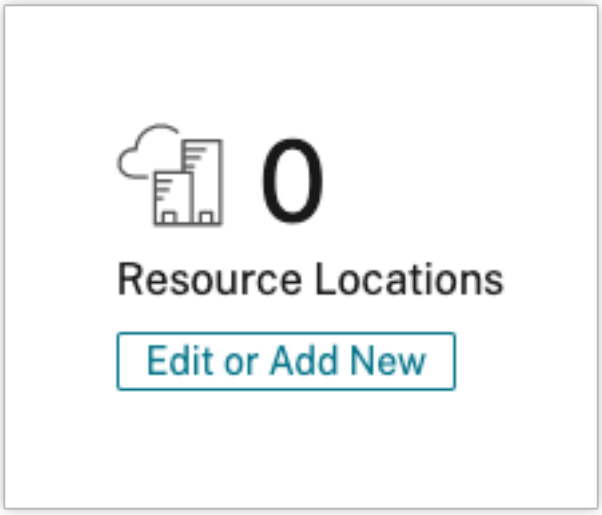
Alternativ können Sie zuerst die benötigten Ressourcenstandorte in der Konsole erstellen, bevor Sie Cloud Connectors in Ihren Domänen installieren. Das Cloud Connector-Installationsprogramm fordert Sie während der Installation auf, den gewünschten Ressourcenstandort auszuwählen.

Interaktive Installation

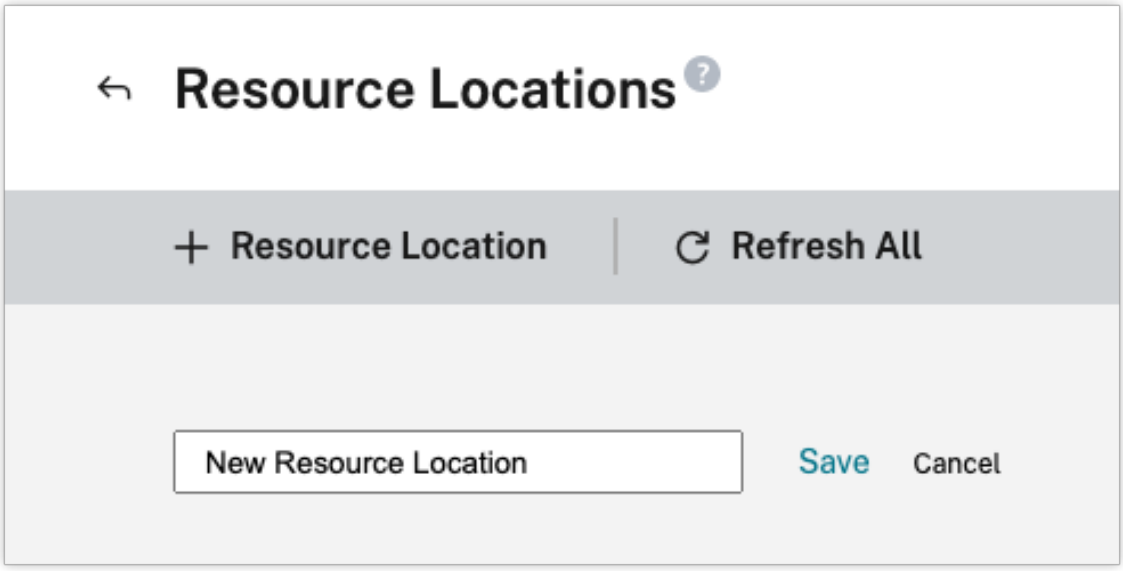
Sie können Cloud Connectors über das grafische Installationsprogramm herunterladen und installieren. Zuvor müssen Sie mindestens einen Ressourcenstandort in der Citrix Cloud-Verwaltungskonsole zur Bereitstellung von Cloud Connectors erstellen. Weitere Informationen finden Sie unter Ressourcenstandorte.

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.

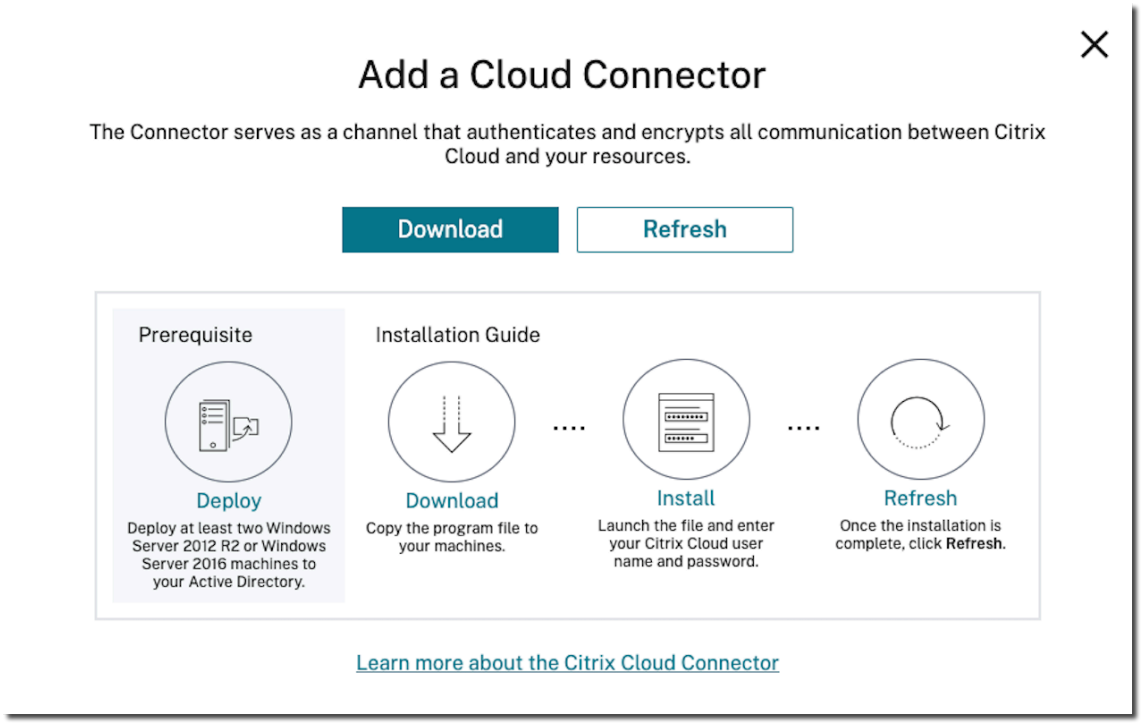


5. Wiederholen Sie diese Schritte auf allen Maschinen, die Sie als Cloud Connector verwenden möchten.

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 hinzuzufügen.
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 Verbindungsprüfung 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.

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 **Download**, 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 einer Konfigurationsdatei:

```
{

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

<!--NeedCopy-->
```

Beispiel einer Befehlszeile zur Installation mit der Parameterdatei:

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

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\Cl** 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

May 25, 2022

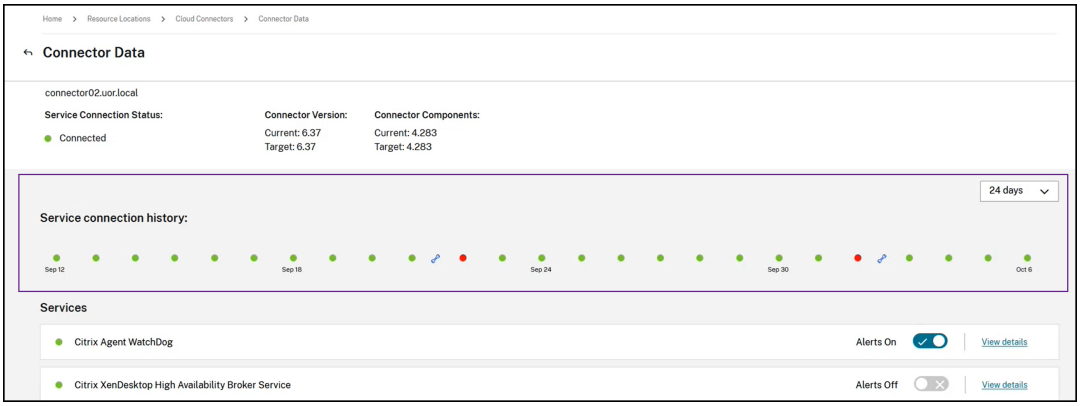
Vor und nach Updates führt Cloud Connector Integritätsprüfungen durch, um unnötige Ausfallzeiten für Anbieter durch Updates zu vermeiden. Sie können den Verbindungs- und Integritätsstatus des Connectors und jedes seiner Dienste und Anbieter sehen.

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:

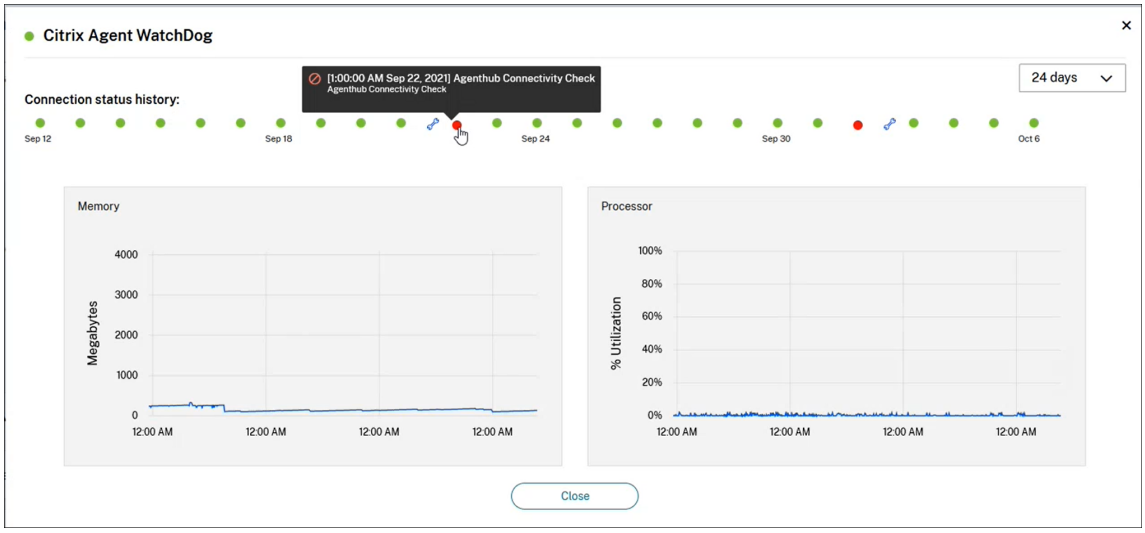
1. Verwenden Sie das Dropdownmenü im Bereich **Dienstverbindung - Verlauf**, um den Zeitraum zu wählen. Sie können die letzten 24 Stunden in Ein-Stunden-Intervallen oder die letzten 24 Tage in Ein-Tages-Intervallen anzeigen.
2. Wählen Sie auf der Seite "Connectordaten" neben dem gewünschten Dienst die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



Protokollsammlung für Citrix Cloud Connector

January 26, 2022

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.

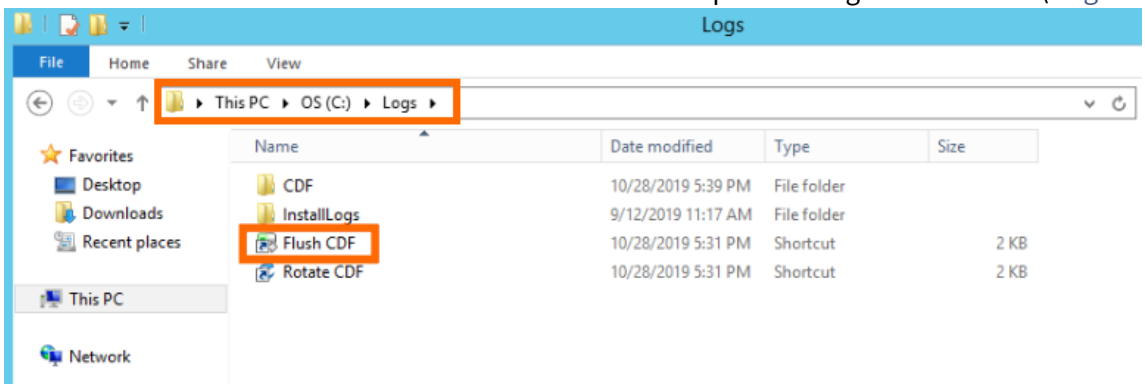
Schritt 1: Problem reproduzieren

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.

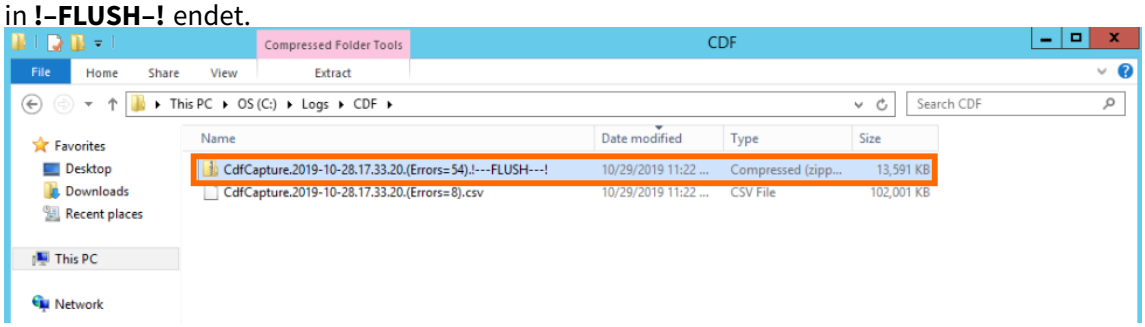
Schritt 2: CDF-Tracingberichte sammeln

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.

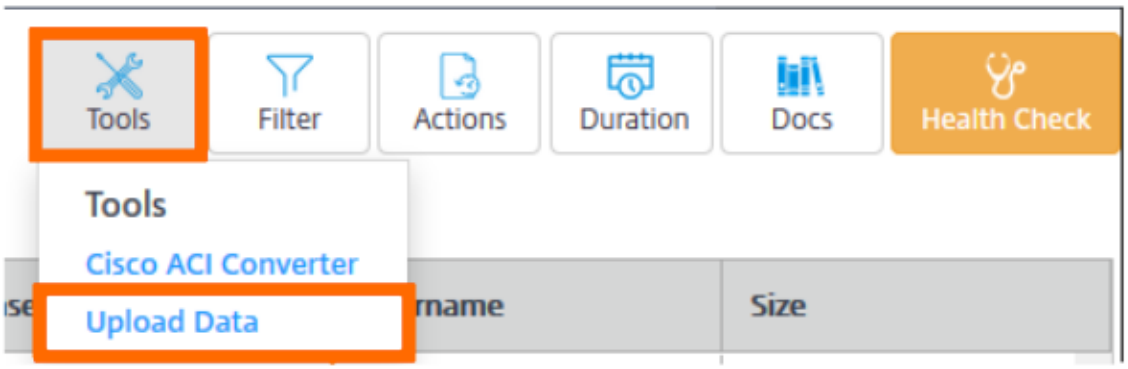


5. Führen Sie die Schritte 1 bis 5 auf jeder Cloud Connector-Maschine des Ressourcenstandorts aus und erstellen Sie eine ZIP-Datei aus allen Flush-Tracingdateien. Wenn Sie keine ZIP-Datei erstellen, müssen Sie alle Flush-Tracingdateien der Cloud Connector-Maschine einzeln an Citrix senden.

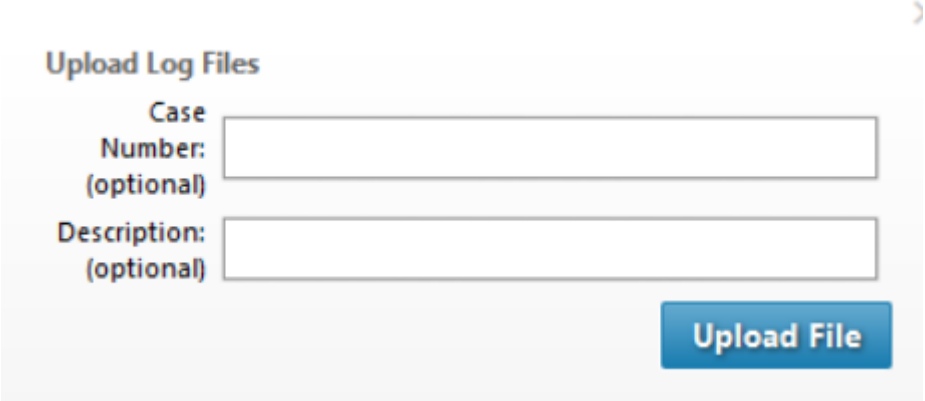
Schritt 3: Daten an Citrix senden

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.

Wählen eines primären Ressourcenstandorts

April 29, 2022

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

September 27, 2022

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:

- (Preview) Mit dem **Hypervisor Management Service** können Sie Updates für Ihre Citrix Hypervisor 8 Cloud-Pools von der Cloudsteuerungsebene aus verwalten. Durch Umstellen auf ein kontinuierliches Aktualisierungsmodell, von Citrix Cloud orchestriert, können Citrix Hypervisor-Kunden von einem effizienten Releaseprozess profitieren, mit dem neue Funktionen schneller bereitgestellt werden. Weitere Informationen finden Sie unter Citrix Hypervisor Cloud.
- Mit **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.

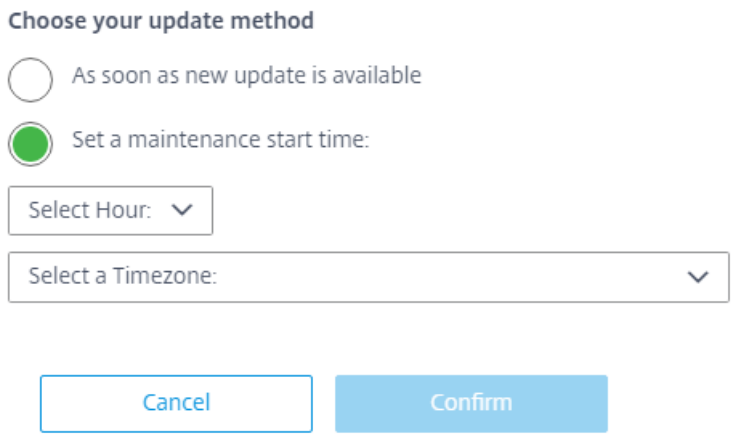
Wenn nur ein Connector für einen Ressourcenstandort konfiguriert ist, zeigt Citrix Cloud auf den Seiten **Ressourcenstandorte** und **Connectors** einen Warnhinweis an.

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. So konfigurieren Sie das Wartungsfenster:

1. Klicken Sie an Ihrem Ressourcenstandort auf die Auslassungspunkte (…) und wählen Sie **Ressourcenstandort verwalten** aus.
2. Wählen Sie im Abschnitt **Updatemethode wählen** die Option **Startzeit für Wartung festlegen** aus.
3. Wählen Sie die Startzeit und die Zeitzone aus den Listen aus.
4. Klicken Sie auf **Bestätigen**.



Während des Updates ist die Connector Appliance vorübergehend nicht verfügbar. Bei der automatischen Aktualisierung wird immer nur eine Connector Appliance gleichzeitig am Ressourcenstandort aktualisiert. Aus diesem Grund ist es wichtig, an jedem Ressourcenstandort mindestens zwei Connector Appliances zu registrieren, damit zu jeder Zeit mindestens eine Connector Appliance 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 werden keine eingehenden Verbindungen akzeptiert.

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 XenServer 7.1 CU2 LTSR
- Citrix Hypervisor 8.2 LTSR
- VMware ESXi Version 7 Update 2
- Hyper-V unter Windows Server 2016, Windows Server 2019 oder Windows Server 2022.
- Microsoft Azure
- AWS
- Google Cloud Platform

Ihr Hypervisor muss die folgenden Mindestfunktionen bereitstellen:

- 20 GiB Stammdatenträger
- 2 vCPUs
- 4 GiB Arbeitsspeicher
- 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.

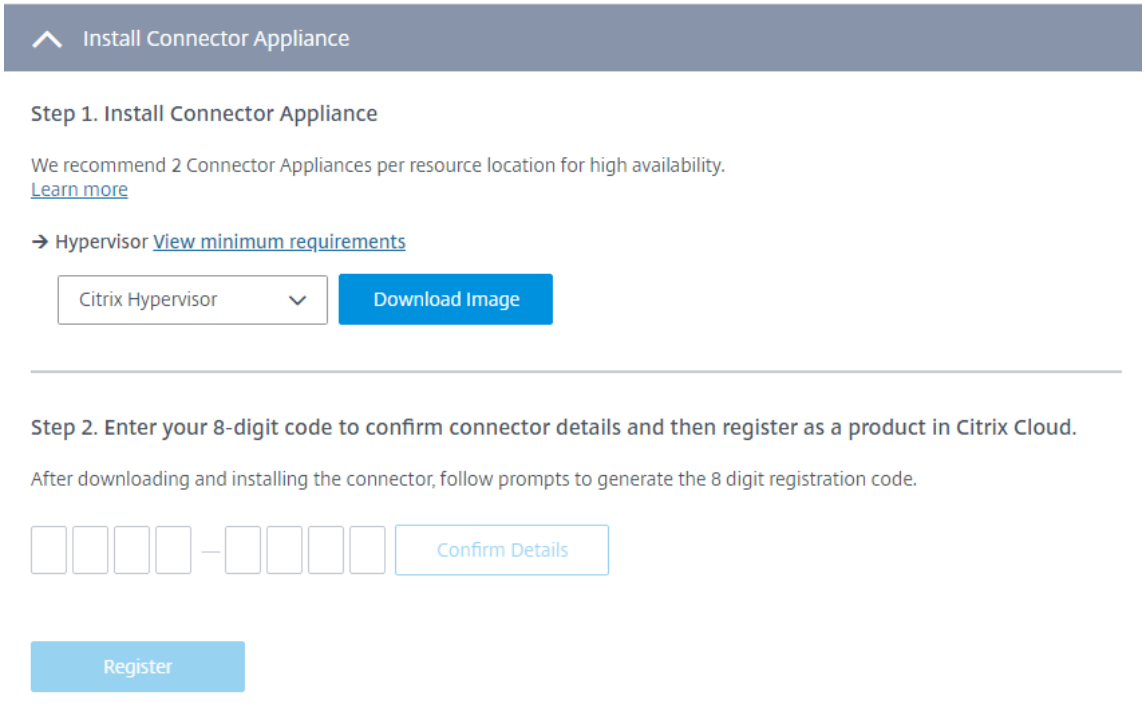
> **Hinweis:**
>
> Das Klonen, Anhalten und Erstellen von Snapshots der Connector Appliance-VM werden nicht unterstützt.

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 installieren** 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 hier 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

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 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.

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: 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 im Feld **Name** verwendet werden soll. Klicken Sie auf **Weiter**.
8. Wählen Sie im Bereich **Generation angeben** die Option “Generation 1” aus. Klicken Sie auf **Weiter**.
9. Führen Sie im Bereich **Speicher zuweisen** folgende Schritte aus:

a) 4 GB RAM zuweisen
b) Dynamischen Speicher deaktivieren

Klicken Sie auf **Weiter**.

10. Wählen Sie im Bereich **Netzwerk konfigurieren** einen Switch aus der Liste aus. Beispiel: Standardswitch. 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. Wechseln Sie im Fenster **Einstellungen** zu **Hardware > Prozessoren**. Ändern Sie den Wert für **Anzahl virtueller Prozessoren** in 2. Klicken Sie auf **Übernehmen** und dann 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
```

5. Wenn Sie dazu aufgefordert werden, geben Sie einen Namen für Ihre VM ein, oder drücken Sie die Eingabetaste, 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 Dateinamen für den Stammdatenträger ein, oder drücken Sie die Eingabetaste, um den Standardwert vom `connector-appliance.vhdx` zu übernehmen.
8. Wenn Sie dazu aufgefordert werden, wählen Sie den zu verwendenden Schalter aus. Drücken Sie die Eingabetaste.
9. Überprüfen Sie die Zusammenfassung der VM-Importinformationen. Wenn die Informationen korrekt sind, drücken Sie die Eingabetaste, 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: https://azuremarketplace.microsoft.com/en-us/marketplace/apps/citrix.citrix-connector-appliance?tab=Overview

   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. Geben Sie auf der Seite **Create a virtual machine** die folgenden Informationen ein:
    - Wählen Sie unter **Subscription** ein Abonnement.
    - Wählen Sie unter **Resource group** eine Ressourcengruppe.
    - Legen Sie unter **Virtual machine name** einen Namen für die VM fest.
    - Wählen Sie eine **Region** für die Connector Appliance.
    - Belassen Sie für alle übrigen Optionen unter **Instance details** die Standardeinstellungen.
    - Wählen Sie unter **Authentication type** die Option **Password**.
    - Geben Sie Werte für **Username** und **Password** ein. Diese Werte werden nicht vom der Connector Appliance verwendet, sodass Sie beim erstmaligen Aufrufen der Verwaltungsseite ein Kennwort für die Connector Appliance festlegen müssen.
4. Klicken Sie auf **Next : Disks >**.
5. Lassen Sie auf der Registerkarte **Disks** alle Standardwerte unverändert.
6. Klicken Sie auf **Next : Networking >**.
7. Geben Sie auf der Registerkarte **Networking** folgende Informationen 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.
    - Wählen Sie unter **Public IP** die Option **None**.
    - Wählen Sie unter **Configure a network security group** eine vorhandene Sicherheitsgruppe aus, oder erstellen Sie eine neue Gruppe.
    - Wählen Sie **Delete NIC when VM is deleted**.
8. Klicken Sie auf **Review + 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. (Link zum 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-04597bf4c0ada741b”.
3. Überprüfen Sie die AMI-ID (ami-04597bf4c0ada741b) 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, rufen Sie die Instanzdetails auf und verwenden **Private IPv4 address**, um sich mit der Connector Appliance zu verbinden 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 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.

Die Datei `connector-appliance-gcp.zip` enthält die Datei `connector-appliance.tar.gz` (das Datenträgerimage der Connector Appliance) und ein PowerShell-Skript, mit dem die Connector Appliance automatisch bereitgestellt werden kann.

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/instances/connecting-advanced#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/instances/connecting-advanced#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.

Die Benutzeroberfläche der Connector Appliance verwendet ein selbstsigniertes Zertifikat. 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.

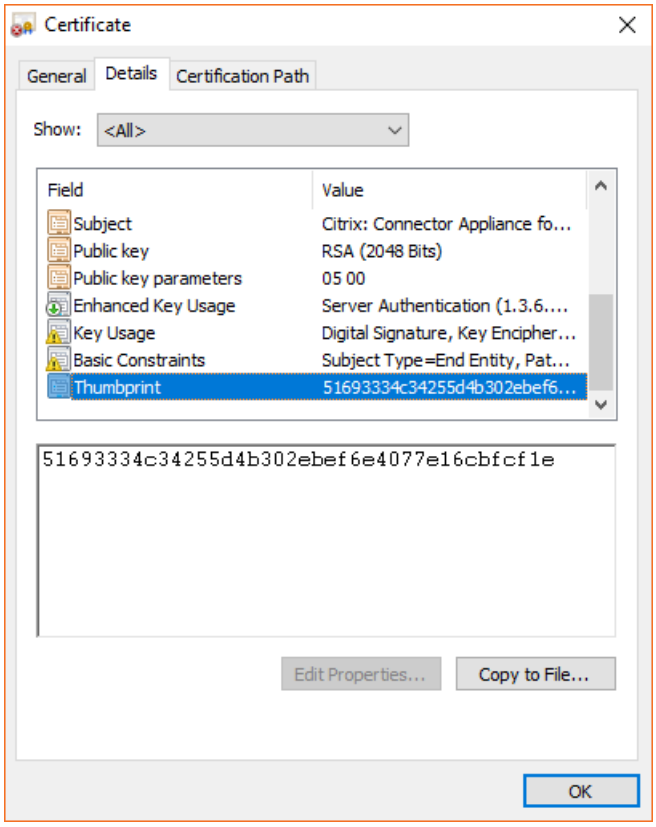
Führen Sie beispielsweise im Google Chrome-Browser die folgenden Schritte aus:

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**.

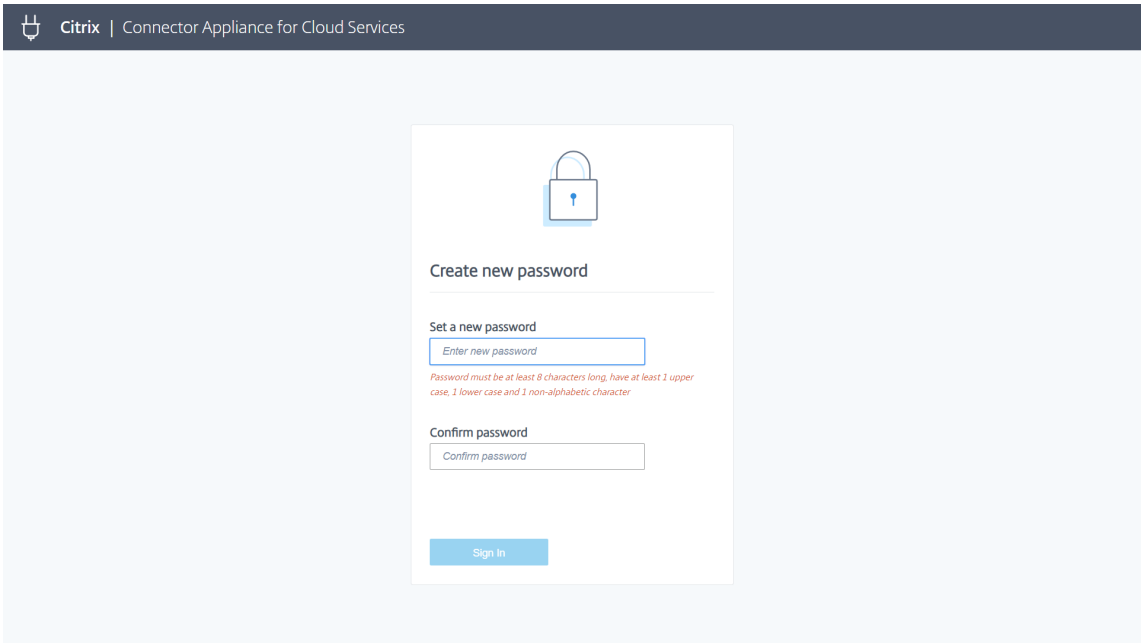
Wenn der Wert im Feld **Fingerabdruck** mit dem SSL-Fingerabdruck in der Konsole übereinstimmt, können Sie bestätigen, dass Ihr Browser direkt mit der Benutzeroberfläche der Connector Appliance verbunden ist.



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**.



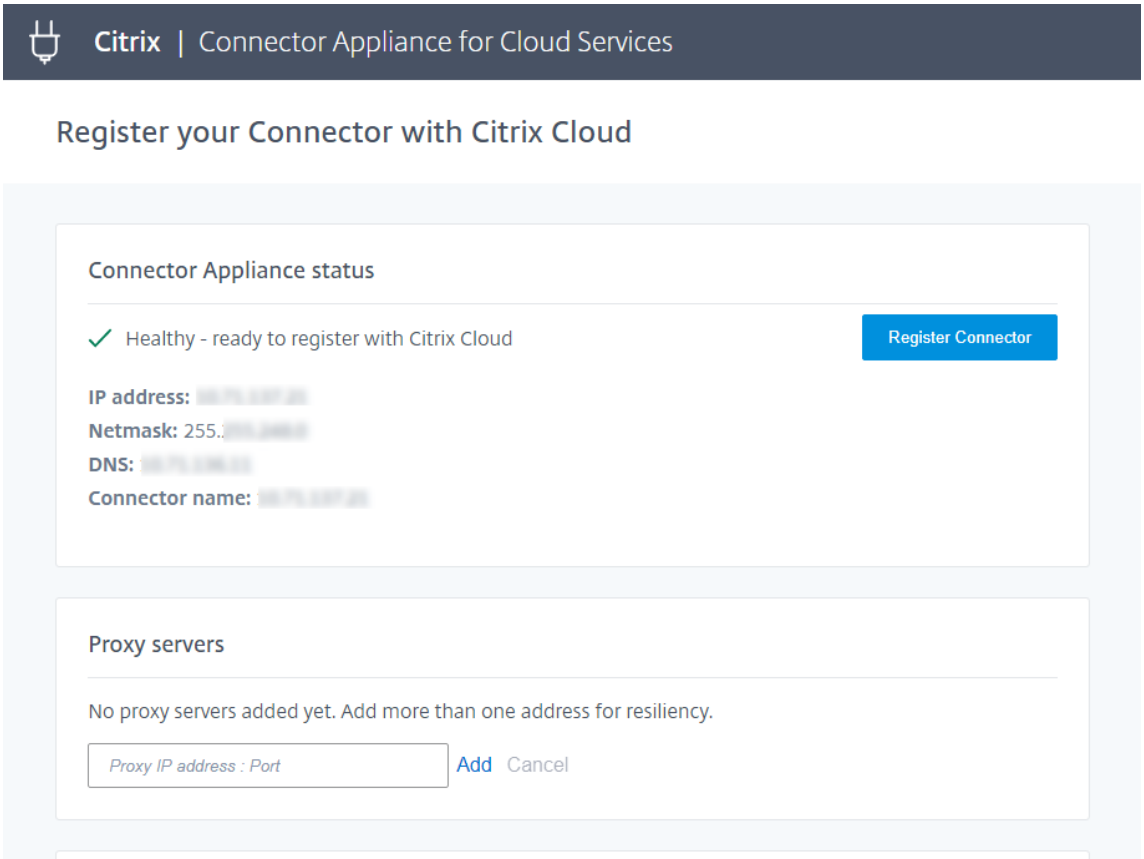
Ihr Kennwort muss die folgenden Anforderungen erfüllen:

- 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 **Connector Appliance-Verwaltungsseite** wird geöffnet.



5. (Optional) Wenn Sie einen oder mehrere Webproxys verwenden, können Sie hier 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.

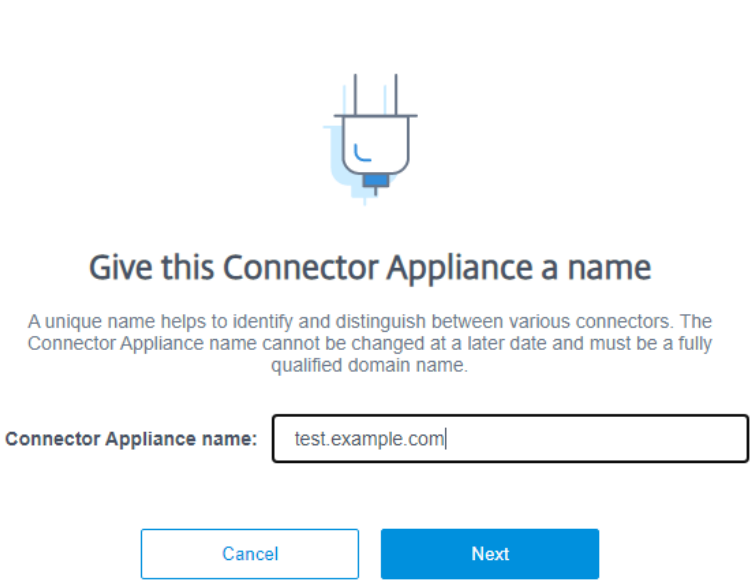
   > **Hinweis:**
   >
   > Es wird nur die Standard-Proxy-Authentifizierung unterstützt. Andere Authentifizierungsmethoden werden nicht unterstützt.

   Nur der Datenverkehr zu externen Systemen wird über den Webproxy geleitet. Weitere Informationen finden Sie unter Kommunikation der Connector Appliance.

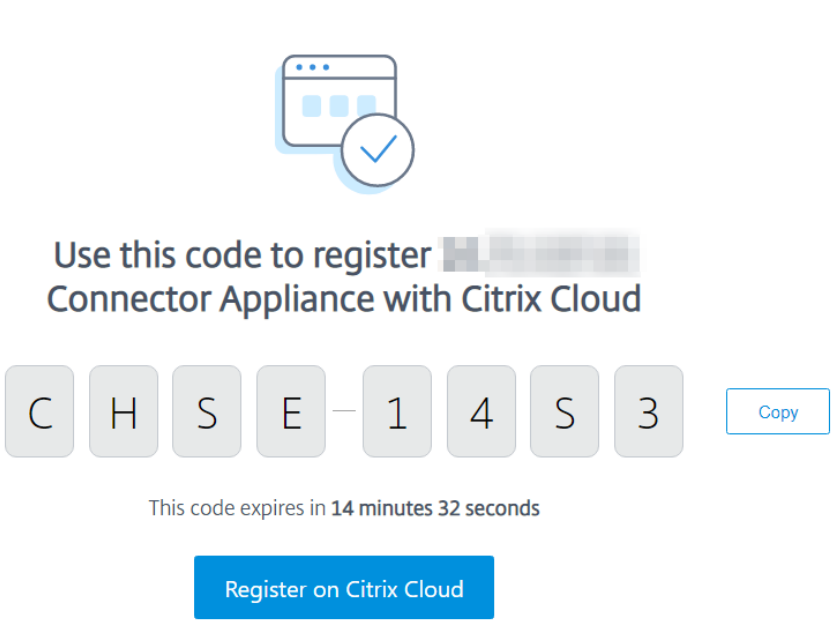
6. Klicken Sie auf **Connector registrieren**, um die Registrierungsaufgabe zu öffnen.

7. 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**.



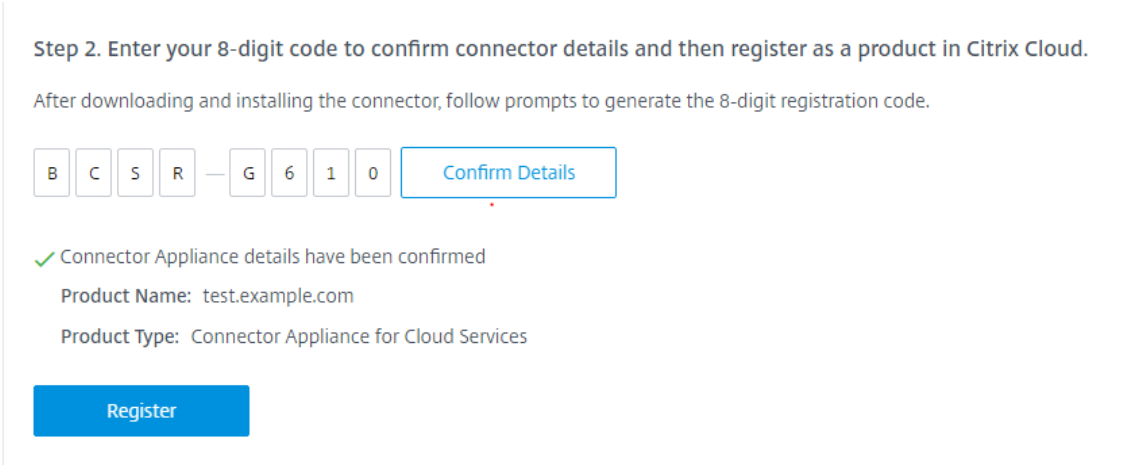
Die Webseite zeigt einen Code an, mit dem Sie sich bei Citrix Cloud registrieren können. Der Code läuft nach 15 Minuten ab.



8. Klicken Sie auf die Schaltfläche **Kopieren**, um den Code in die Zwischenablage zu kopieren.
9. Kehren Sie zur Webseite **Ressourcenstandorte** zurück.
10. 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.



11. Klicken Sie auf **Registrieren**.

    Es wird angezeigt, ob die Registrierung erfolgreich war. Bei fehlgeschlagener Registrierung werden Sie aufgefordert, es erneut zu versuchen.

12. 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

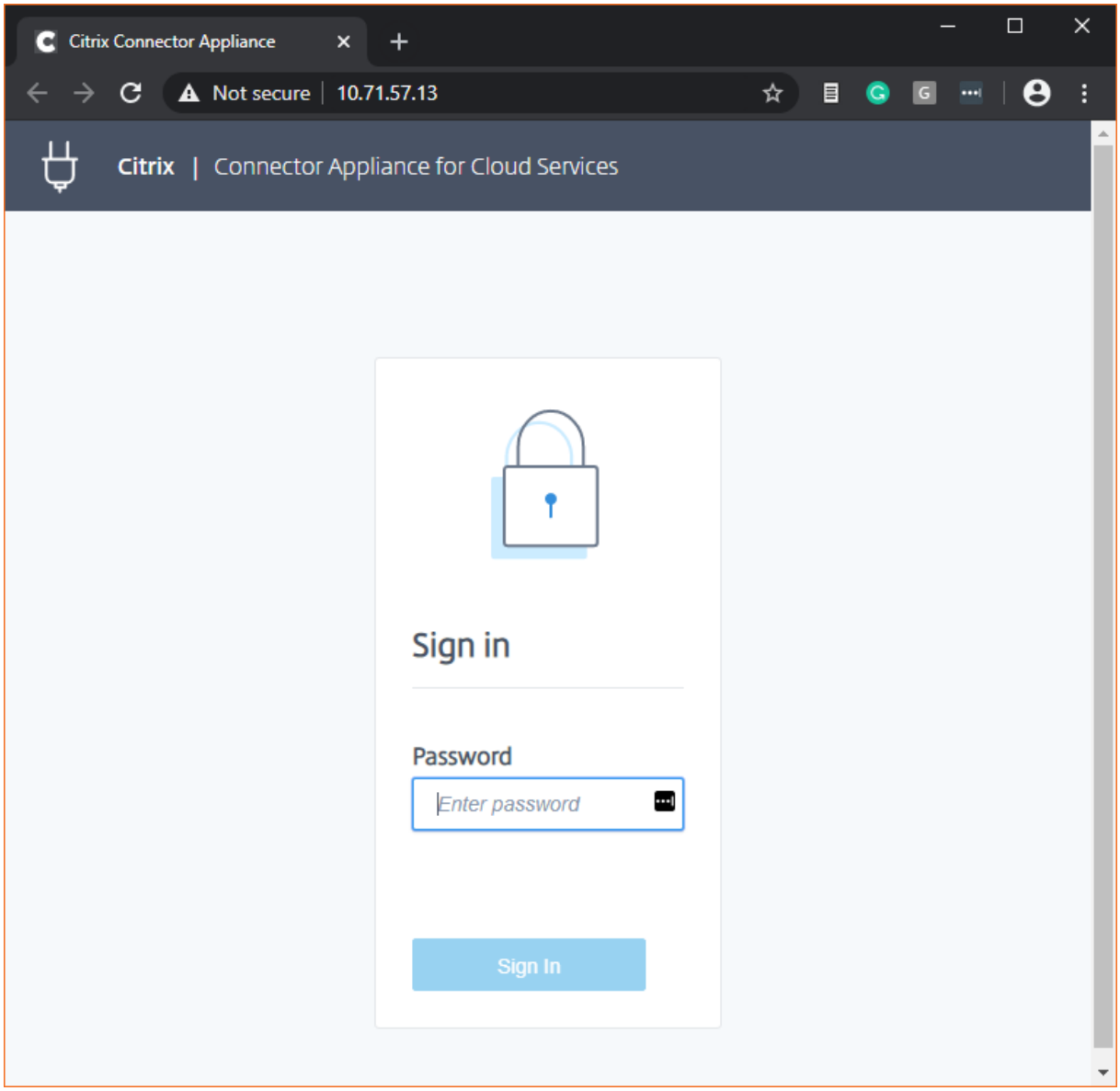
Wir empfehlen, dass Sie für jeden Ressourcenstandort zwei oder mehr Connector Appliances installieren und registrieren. Diese Konfiguration gewährleistet eine kontinuierliche Verfügbarkeit und ermöglicht den Lastausgleich zwischen Connectors.

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.

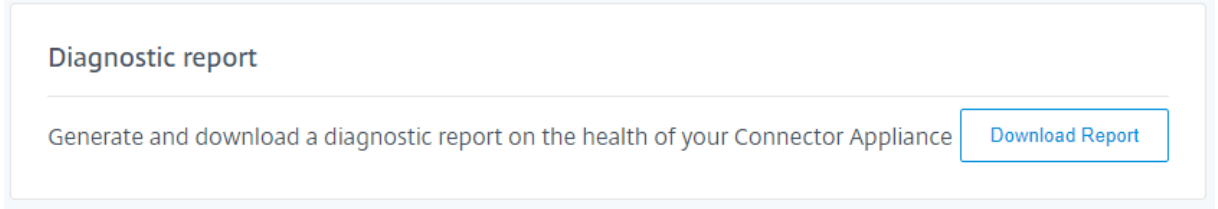
Sie sollten die Connector Appliance-VMs weder klonen oder anhalten und auch keinen Snapshot erstellen. Diese Aktionen werden nicht unterstützt.

Die Seite **Neues Kennwort erstellen** wird nur beim ersten Verbinden mit der Benutzeroberfläche der Connector Appliance angezeigt. 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.

1. Rufen Sie die **Connector Appliance-Verwaltungsseite** auf.
   a) Kopieren Sie von der Connector Appliance-Konsole in Ihrem Hypervisor die IP-Adresse in die Adressleiste Ihres Browsers.
   b) Geben Sie das Kennwort ein, das Sie bei der Registrierung der Connector Appliance festgelegt haben.
2. Wählen Sie im Admin-Menü oben rechts die Option **Kerberos-Validierung** aus.
3. Wählen Sie im Dialogfeld **Kerberos-Validierung** den **Kerberos-Validierungsmodus** aus.
4. Geben Sie die **Active Directory-Domäne** an oder wählen Sie sie aus.
   - Wenn Sie eine Konfiguration im Kerberos Realm-Only-Modus validieren, können Sie eine beliebige Active Directory-Domäne angeben.
   - Wenn Sie eine Konfiguration mit eingeschränkter Kerberos-Delegierung überprüfen, müssen Sie Ihre Auswahl aus einer Liste von Domänen in der verbundenen Gesamtstruktur treffen.
5. Geben Sie den **Dienst-FQDN** an. Als Standarddienstname wird “http” angenommen. Wenn Sie “computer.example.com” angeben, wird dieser Wert als “http/computer.example.com” angesehen.
6. Geben Sie den **Benutzernamen** an.
7. Wenn Sie eine Konfiguration im Kerberos Realm-Only-Modus validieren, geben Sie das **Kennwort** für diesen Benutzernamen an.
8. 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.

Active Directory mit Connector Appliance

September 19, 2022

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.

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.

Verbinden einer Active Directory-Domäne mit Citrix Cloud über die Connector Appliance

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. Klicken Sie im Abschnitt **Active Directory-Domänen** auf **+ Active Directory-Domäne hinzufügen**.

4. Geben Sie den Domänennamen in das Feld **Domänenname** ein. Klicken Sie auf **Hinzufügen**.

   Die Connector Appliance überprüft die Domäne. Wenn die Prüfung erfolgreich ist, wird das Dialogfeld **Active Directory beitreten** geöffnet.

5. Geben Sie den Benutzernamen und das Kennwort eines Active Directory-Benutzers ein, der über eine Beitrittsberechtigung für diese Domäne verfügt.

6. 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.

7. Klicken Sie auf **Beitreten**.

Die Domäne wird jetzt im Abschnitt **Active Directory-Domänen** der Benutzeroberfläche der Connector Appliance aufgeführt.

8. Zum Hinzufügen weiterer Active Directory-Domänen wählen Sie **+ Active Directory-Domäne hinzufügen** aus, und wiederholen Sie die vorherigen Schritte.
9. 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 Con-

nector 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

September 17, 2021

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 umgehend installiert werden und die Benutzererfahrung mit Citrix

Cloud nicht beeinträchtigen, können Sie einen Wochentag und eine Uhrzeit für die Installation festlegen. 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.

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

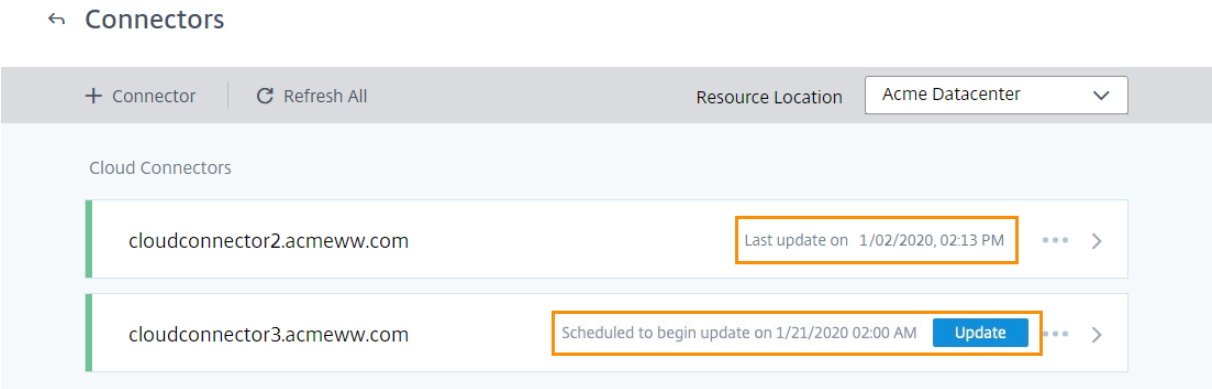
Am Montag konfigurieren Sie “Dienstag 18:00 Uhr” als bevorzugte Updatezeit. Später am Tag erhalten Sie eine Update-Benachrichtigung in Citrix Cloud und es wird die Schaltfläche **Aktualisieren** angezeigt. Wenn Sie das Update nicht starten, wartet Citrix Cloud sieben Tage und installiert das Update dann 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.

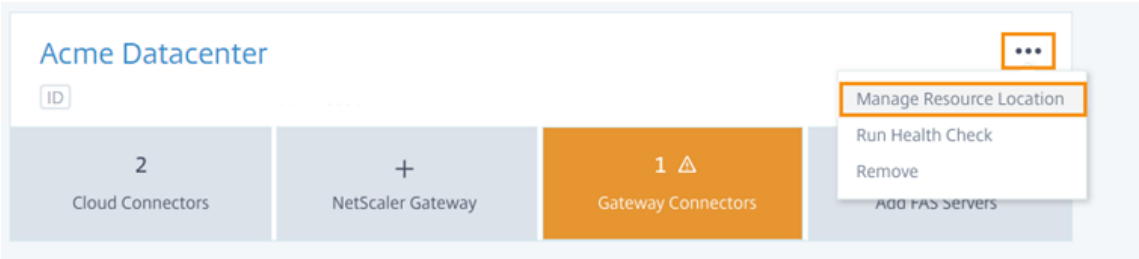


Nachdem Citrix Cloud Sie über ein verfügbares Update benachrichtigt hat, wird für jeden Connector eine Schaltfläche **Aktualisieren** angezeigt, sodass Sie das Update schon vor dem bevorzugten Termin installieren können. Nachdem Sie **Aktualisieren** für jeden Connector ausgewählt haben, werden die Updates 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.

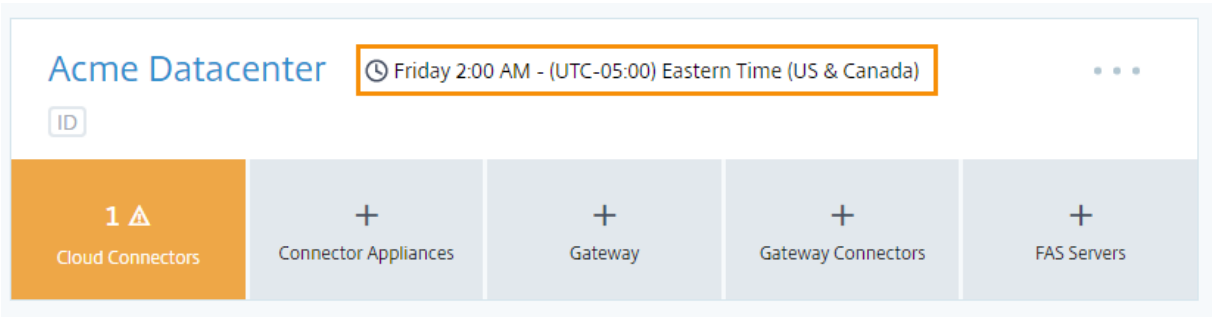
Auswahl eines Aktualisierungszeitplans

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.

> **Hinweis:**
>
> 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.

Ungeplante Updates

Auch bei gewähltem Tag und Zeitpunkt für die Installation von Updates kann es vorkommen, dass Citrix Cloud ein Update möglichst schnell installiert. Ungeplante Updates treten in folgenden Fällen auf:

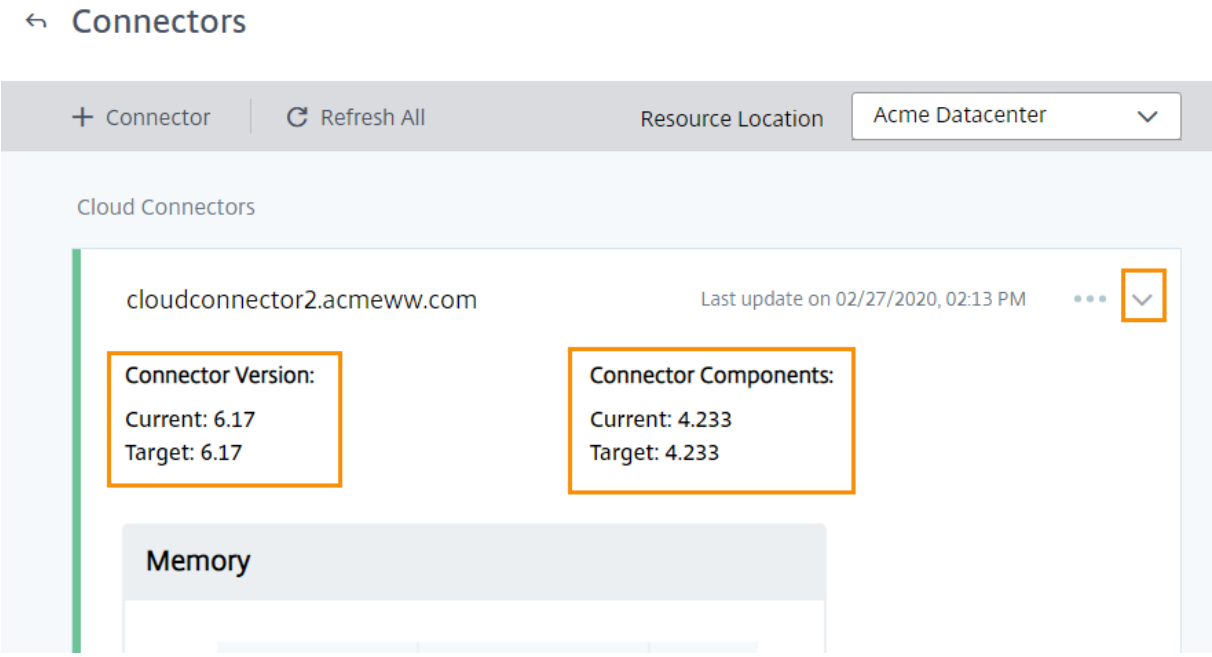
- Das Update kann nicht innerhalb von 48 Stunden nach Veröffentlichung zum bevorzugten Zeitpunkt installiert werden. Wenn Ihre bevorzugte Zeit beispielsweise 2:00 Uhr und der Connector nach Veröffentlichung des Updates drei Tage lang offline ist, installiert Citrix Cloud das Update, sobald der Connector 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. Erweitern Sie dann die Kachel für den Cloud Connector.



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

September 19, 2022

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	Administratoren	Abonnenten
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 Identity	Nein	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.

Sie können Ihrem Citrix Cloud-Konto die folgenden Identitätsanbieter hinzufügen:

- On-Premises-Active Directory. Nur für die Authentifizierung von Workspace-Abonnenten.
- Active Directory plus Token. Nur für die Authentifizierung von Workspace-Abonnenten.
- Azure Active Directory. Für die Authentifizierung von Citrix Cloud-Administratoren und Workspace-Abonnenten.

- Citrix Gateway. Nur für die Authentifizierung von Workspace-Abonnenten.
- Google Identity. Nur für die Authentifizierung von Workspace-Abonnenten.
- Okta. Nur für die Authentifizierung von Workspace-Abonnenten.
- SAML 2.0. Für die Authentifizierung von Citrix Cloud-Administratorgruppen und Workspace-Abonnenten.

Citrix Cloud unterstützt auch den Citrix Verbundauthentifizierungsdienst (FAS) zum Single Sign-On für Workspace-Abonnenten. Weitere Informationen finden Sie unter Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst (FAS).

> **Tipp:**
>
> Im Kurs Introduction to Citrix Identity and Authentication erfahren Sie mehr über unterstützte Identitätsanbieter. Jedes Modul bietet kurze Videos zum Verbinden der Identitätsanbieter mit Citrix Cloud und zum Aktivieren der Authentifizierung für Citrix Workspace.

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.

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.

Zurücksetzen des Kennworts

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 von Citrix Cloud nicht in Ihrem Spamordner oder Papierkorb landet.

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 Wählen eines primären Ressourcenstandorts.

Administratorzugriff auf Citrix Cloud verwalten

October 16, 2022

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 mehrstufige Authentifizierung registrieren und Token mithilfe einer beliebigen App generieren, die dem Standard Zeitbasiertes Einmalkennwort entspricht, z. B. Citrix SSO oder Google Authenticator.

> **Tipp:**
>
> Das im Kurs Fundamentals of Citrix Cloud enthaltene Modul "Citrix Cloud Platform" bietet kurze Videos über die Verwaltung von Citrix Cloud und Services. Der Kurs vermittelt zudem ein solides Grundlagenwissen zu Citrix Cloud und dessen Vorteilen für Unternehmen sowie wichtige Anwendungsfälle für die Citrix Cloud-Services.

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 können nur auf Citrix DaaS zugreifen. 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.

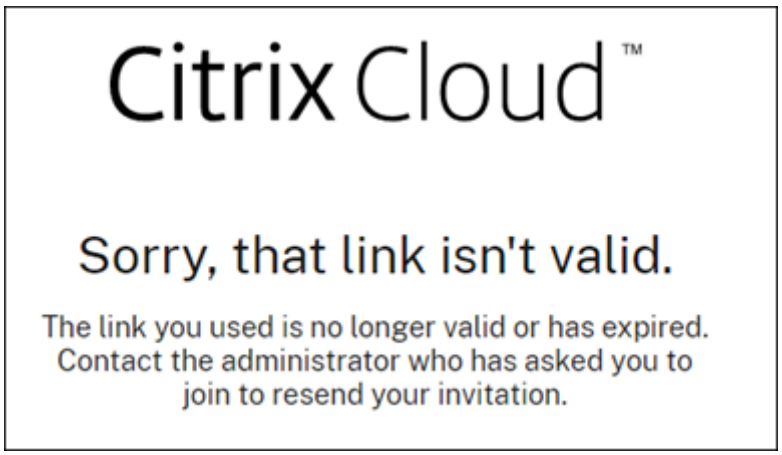
Der Workflow beim Hinzufügen neuer Administratoren ist wie folgt:

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.

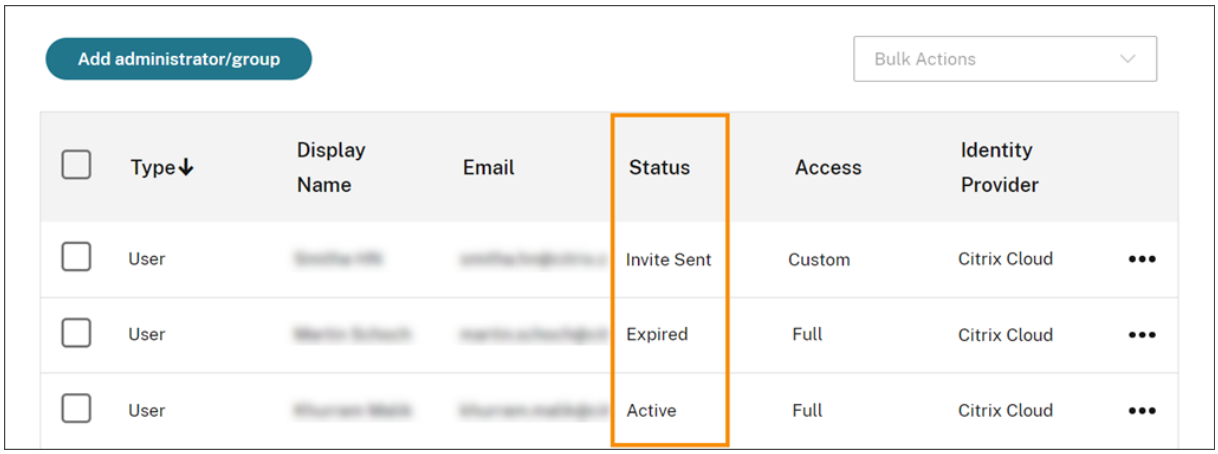
Einladen einzelner Administratoren

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.

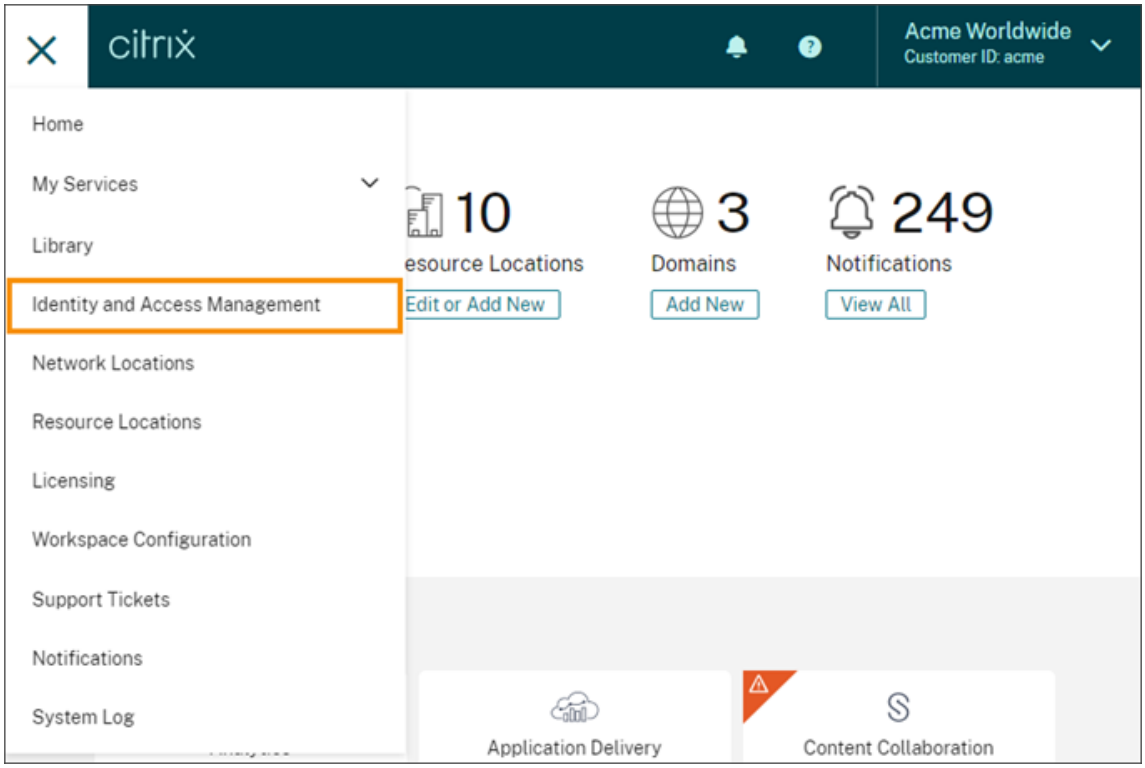


In Citrix Cloud wird außerdem der Status der Einladung angezeigt, damit Sie sehen können, ob der Administrator sie angenommen und sich bei Citrix Cloud angemeldet hat.

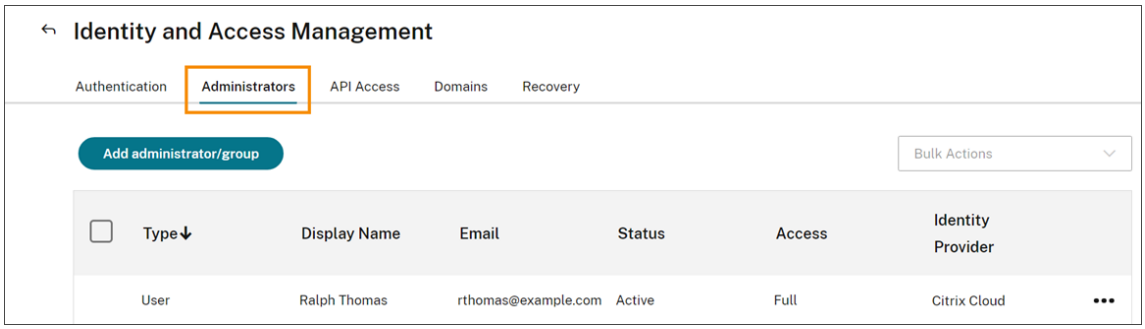


Einladen eines Administrators

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.



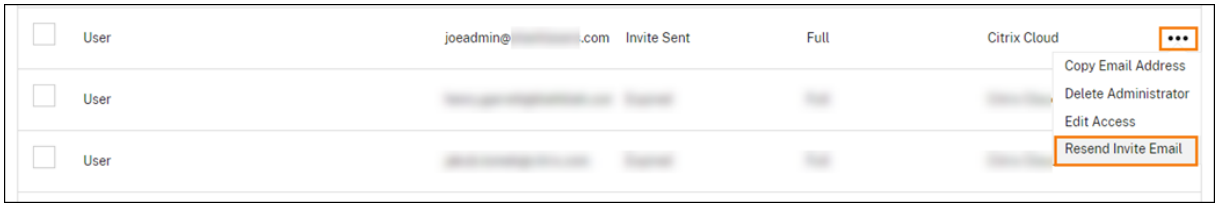
3. Wählen Sie **Administrator/Gruppe hinzufügen**.
4. Wählen Sie unter **Administratordetails** den Identitätsanbieter aus, den Sie verwenden möchten. Wenn Sie Azure AD verwenden, werden Sie von Citrix Cloud möglicherweise aufgefordert, sich zuerst anzumelden.
5. Bei Auswahl von **Citrix Identität** 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 Administra-

tor. **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 eine Einladungs-E-Mail abläuft und Sie eine neue Einladung an einen Administrator senden möchten, löschen Sie den Administrator aus Citrix Cloud und laden Sie ihn dann erneut ein.

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.

Hinzufügen von Administratorgruppen

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.

Ändern der E-Mail-Adresse eines Administrators

Um die E-Mail-Adresse eines Administrators für Citrix Cloud zu ändern, empfiehlt Citrix die folgende Schrittfolge:

1. Erstellen Sie ein neues Administratorkonto mit der neuen E-Mail-Adresse in Ihrem AD.
2. Fügen Sie das neue Konto in Citrix Cloud hinzu, wie in diesem Artikel unter Einladen eines Administrators beschrieben.

Wenn Sie den Administrator aus Citrix Cloud entfernen und die E-Mail-Adresse in Ihrem AD ändern, müssen Sie auch die folgenden Schritte ausführen:

1. Erstellen Sie ein Supportticket beim technischen Support von Citrix, um anzufordern, dass der vorhandene Prinzipal manuell entfernt wird.
2. Geben Sie in den Ticketdetails die alte E-Mail-Adresse oder die OID des Administratorkontos an.
3. Nachdem der vorhandene Prinzipal entfernt wurde, fügen Sie das Administratorkonto in Citrix Cloud hinzu, wie in diesem Artikel unter Einladen eines Administrators beschrieben.

Wenn der vorhandene Prinzipal für das Administratorkonto nicht entfernt wird, kann der Administrator sich nicht mit der neuen E-Mail-Adresse bei Citrix Cloud anmelden.

Weitere Informationen finden Sie unter CTX463477 im Citrix Support Knowledge Center.

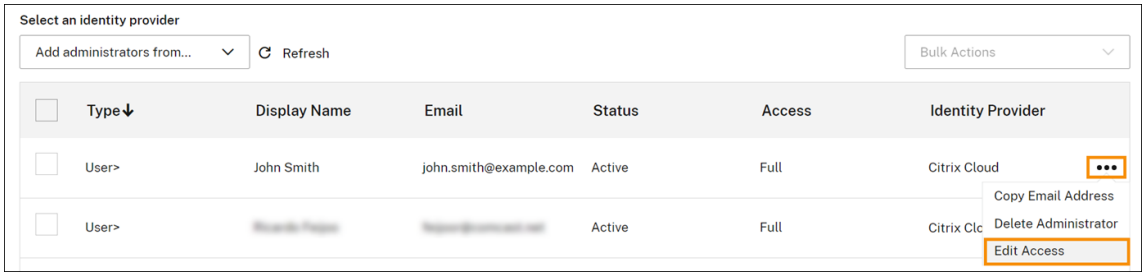
Ändern von Administratorberechtigungen

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.

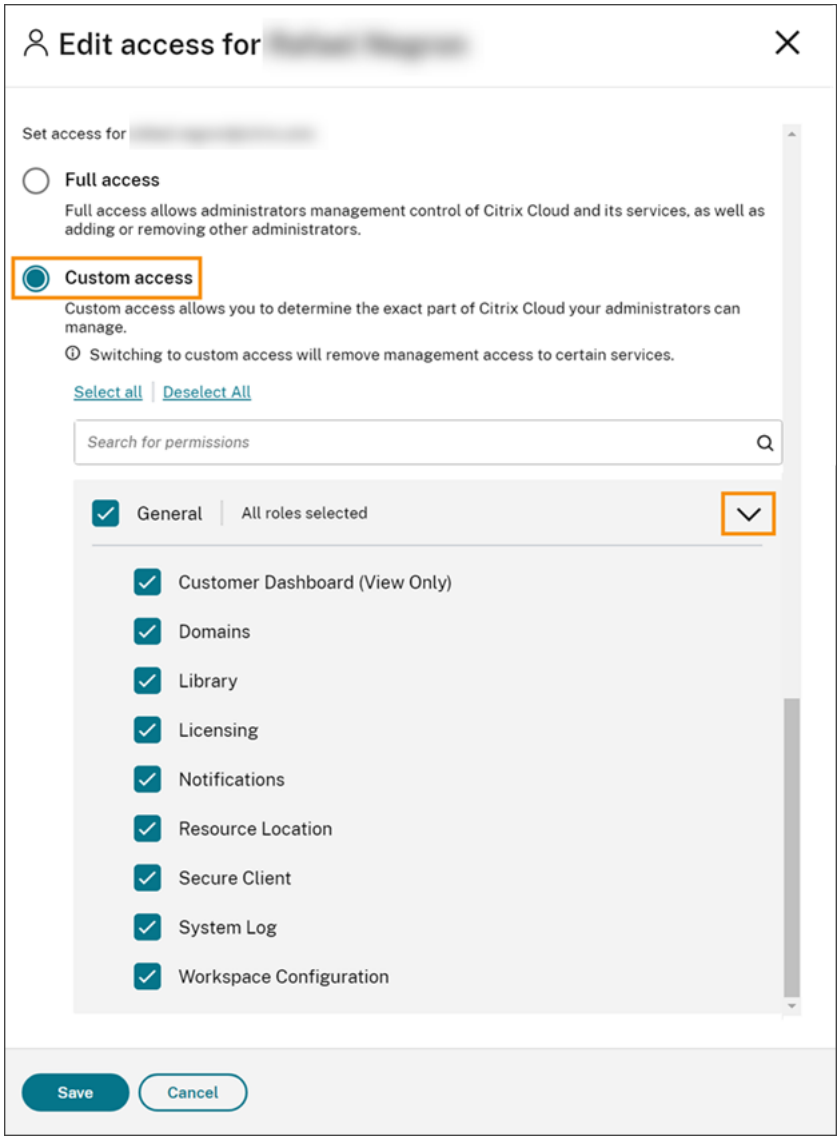
Nur Citrix Cloud-Administratoren mit Vollzugriff können Berechtigungen für andere Administratoren festlegen.

Gehen Sie zum Ändern von Administratorberechtigungen folgendermaßen vor:

1. Melden Sie sich bei Citrix Cloud unter https://citrix.cloud.com an.
2. Klicken Sie im Menü “Citrix Cloud” auf **Identitäts- und Zugriffsverwaltung** und wählen Sie dann **Administratoren** aus.
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

Verwenden Sie die folgenden Berechtigungen, um benutzerdefinierten Zugriff auf die Citrix Cloud-Verwaltungskonsole festzulegen:

- **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 Connectors hinzufügen und 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.
- **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.

> **Hinweis:**
>
> Um den Zugriff auf eine Seite in der Citrix Cloud-Verwaltungskonsole zu verhindern, stellen Sie sicher, dass alle benutzerdefinierten Zugriffsberechtigungen für diese Seite nicht ausgewählt sind. Um beispielsweise die Seite **Identitäts- und Zugriffsverwaltung** auszublenden, deaktivieren Sie die Berechtigungen **Domänen** und **Sicherer Client**.

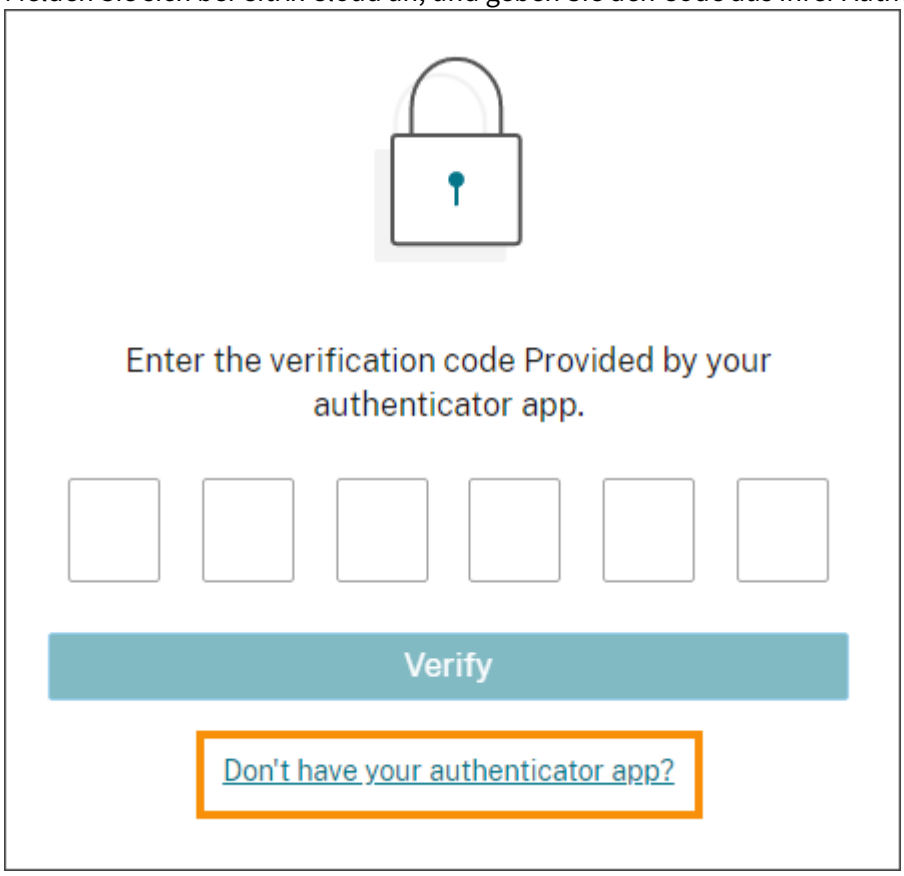
Geräts für die mehrstufige Authentifizierung ändern

Wenn Sie Ihr registriertes Gerät verlieren, ein anderes Gerät mit Citrix Cloud verwenden möchten oder die Authentifikator-App zurücksetzen, können Sie sich erneut für die mehrstufige Authentifizierung (MFA) in Citrix Cloud 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 Neuregistrierung 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.

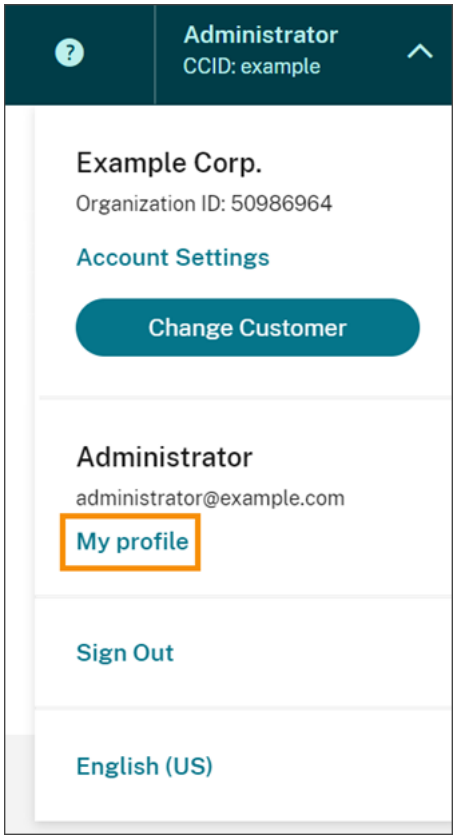
1. Melden Sie sich bei Citrix Cloud an, und geben Sie den Code aus Ihrer Authentifikator-App ein.



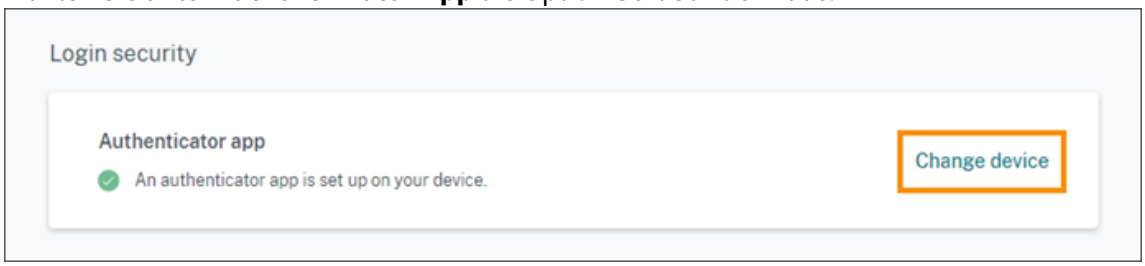
Wenn Sie keine Authentifikator-App haben, klicken Sie auf **Haben Sie keine Authentifikator-App?**, und wählen Sie eine Wiederherstellungsmethode aus, die Ihnen die Anmeldung ermöglicht. Geben Sie je nach ausgewählter Wiederherstellungsmethode den empfangenen

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 die Option **Mein Profil**.



4. Wählen Sie unter **Authentifikator-App** die Option **Gerät ändern** aus.



5. Wenn Sie aufgefordert werden, das Ändern des Geräts zu bestätigen, wählen Sie **Ja, Gerät ändern** aus.
6. Verifizieren Sie Ihre Identität, indem Sie einen Bestätigungscode aus Ihrer Authentifikator-App eingeben. Wenn Sie keine Authentifikator-App haben, wählen Sie **Haben Sie keine Authentifikator-App?**, und wählen Sie eine Wiederherstellungsmethode aus. Geben Sie je nach ausgewählter Wiederherstellungsmethode den Verifizierungscode oder den Wiederher-

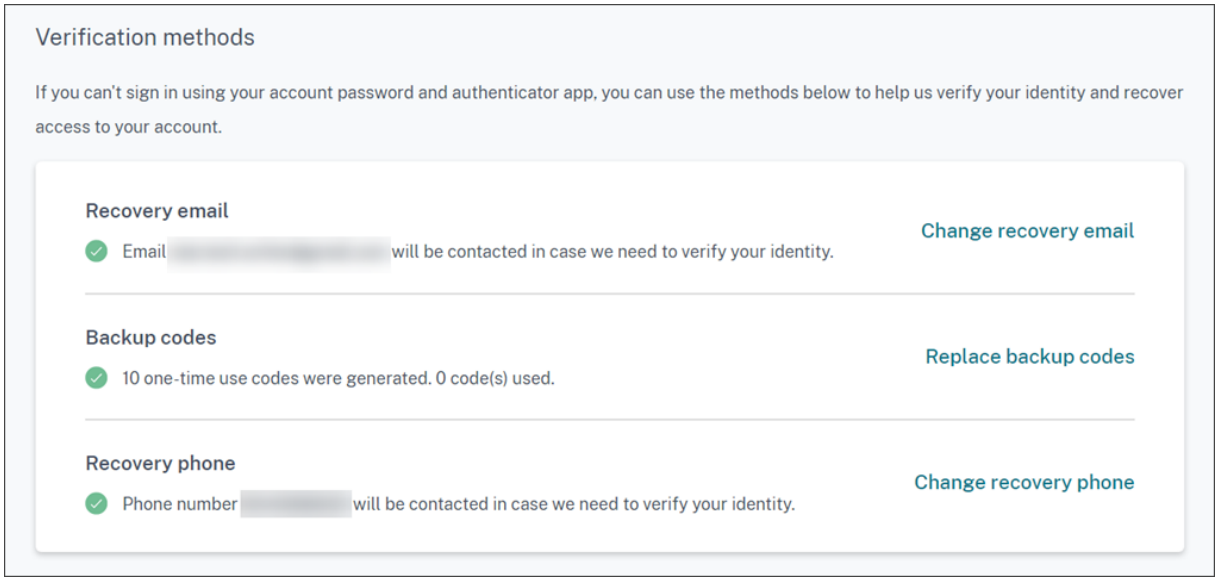
stellungscode ein, den Sie erhalten, oder einen nicht verwendeten Backupcode. Wählen Sie **Überprüfen** aus.

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.

Verifizierungsmethoden verwalten

> **Wichtig:**
>
> Halten Sie Ihre Verifizierungsmethoden mit genauen Informationen auf dem neuesten Stand, um die Sicherheit Ihres Citrix Cloud-Kontos zu gewährleisten. Wenn Sie den Zugriff auf Ihre Authentifikator-App verlieren, können Sie den Zugriff auf Ihr Konto nur mit diesen Verifizierungsmethoden wiederherstellen.



Wiederherstellungs-E-Mail-Adresse hinzufügen oder ändern

1. Melden Sie sich bei Citrix Cloud an, und geben Sie den Code aus Ihrer Authentifikator-App ein.

2. Wenn Sie Administrator für mehrere Kundenorganisationen sind, wählen Sie die Kundenorganisation aus, bei der Sie sich ursprünglich für die mehrstufige Authentifizierung registriert haben.
3. Wählen Sie im Menü oben rechts die Option **Mein Profil**.
4. Wählen Sie unter **Verifizierungsmethoden** in **Wiederherstellungs-E-Mail-Adresse** die Option **Wiederherstellungs-E-Mail-Adresse hinzufügen** aus, wenn Sie noch keine Wiederherstellungs-E-Mail-Adresse hinzugefügt haben. Wenn Sie bereits eine Wiederherstellungs-E-Mail-Adresse hinzugefügt haben, wählen Sie **Wiederherstellungs-E-Mail-Adresse ändern**aus.
5. Geben Sie die neue E-Mail-Adresse ein, die Sie verwenden möchten, und wählen Sie dann **Speichern** aus.

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. Melden Sie sich bei Citrix Cloud an, und geben Sie den Code aus Ihrer Authentifikator-App ein.
2. Wenn Sie Administrator für mehrere Kundenorganisationen sind, wählen Sie eine beliebige Kundenorganisation aus.
3. Wählen Sie im Menü oben rechts die Option **Mein Profil**.
4. Wenn Sie noch nie Backupcodes generiert haben, wählen Sie unter **Verifizierungsmethoden** im Bereich **Backupcodes** die Option **Neue Backupcodes generieren**. Wenn Sie bereits Backupcodes erstellt haben, wählen Sie **Backupcodes ersetzen**.
5. Wenn Sie aufgefordert werden, Ihre Backupcodes zu ersetzen, wählen Sie **Ja, ersetzen** aus.
6. Geben Sie zur Identitätsprüfung einen Verifizierungscode aus Ihrer Authentifikator-App ein. Citrix Cloud generiert dann einen neuen Satz von Backupcodes.
7. Wählen Sie **Codes herunterladen** aus, um Ihre neuen Codes als Textdatei herunterzuladen. Wählen Sie dann **Ich habe diese Codes gespeichert**.
8. Wählen Sie **Schließen**.

Telefonnummer für die Wiederherstellung ändern

1. Melden Sie sich bei Citrix Cloud an, und geben Sie den Code aus Ihrer Authentifikator-App ein.
2. Wenn Sie Administrator für mehrere Kundenorganisationen sind, wählen Sie eine Kundenorganisation aus, bei der Sie sich ursprünglich für die mehrstufige Authentifizierung registriert haben.
3. Wählen Sie im Menü oben rechts die Option **Mein Profil**.
4. Wählen Sie unter **Verifizierungsmethoden** in **Wiederherstellungstelefon** die Option **Wiederherstellungstelefon ändern** aus.
5. Geben Sie die neue Telefonnummer ein, die Sie verwenden möchten, und wählen Sie dann **Speichern** aus.

> **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

October 16, 2022

Sie können Ihrem Citrix Cloud-Konto Administratoren über Gruppen in Ihrem Active Directory oder Azure Active Directory (AD) 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:

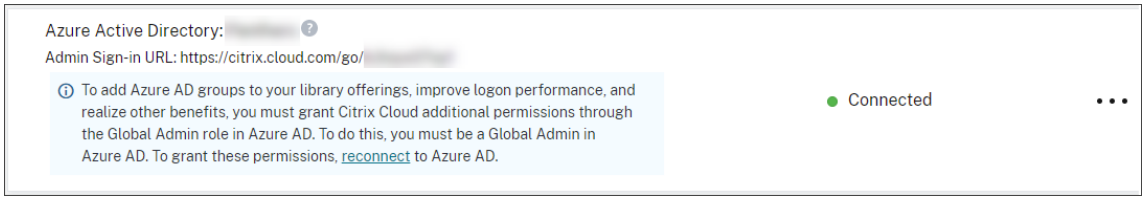
1. Überprüfen Sie, ob Sie die neueste Anwendung für Ihre Azure AD-Verbindung verwenden. Citrix Cloud zeigt eine Benachrichtigung an, wenn Sie nicht die neueste Anwendung verwenden.

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.

Unterstützte Dienste und Berechtigungen

Die folgenden Services unterstützen benutzerdefinierte Zugriffsberechtigungen für Administratorgruppen:

- Citrix Application Delivery Management-Service
- Citrix DaaS
- Workspace Environment Management Service

Sie können benutzerdefinierte Zugriffsberechtigungen nur für unterstützte Services zuweisen. Vollzugriffsberechtigungen werden nicht unterstützt.

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- und Azure AD-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 AD- oder Azure AD-Identität verfügt. In der Tabelle in diesem Abschnitt werden die Berechtigungen beschrieben, die für jede Kombination dieser Identitäten verfügbar sind.

AD- oder Azure AD-Identität für Einzelbenutzer sind AD- oder Azure AD-Berechtigungen, die dem Administrator über ein Einzelkonto erteilt werden. *Gruppenbasierte AD- oder Azure AD-Identität* sind AD- oder Azure AD-Berechtigungen, die dem Administrator als Mitglied einer Azure AD-Gruppe erteilt werden.

Citrix-Identität	AD- oder Azure AD-Identität für Einzelbenutzer	Gruppenbasierte AD- oder Azure AD-Identität	Nach der Authentifizierung verfügbare Berechtigungen
X	X		Administrator verfügt nach erfolgreicher Authentifizierung mit der Citrix- oder Azure AD-Identität über kumulative Berechtigungen beider Identitäten.

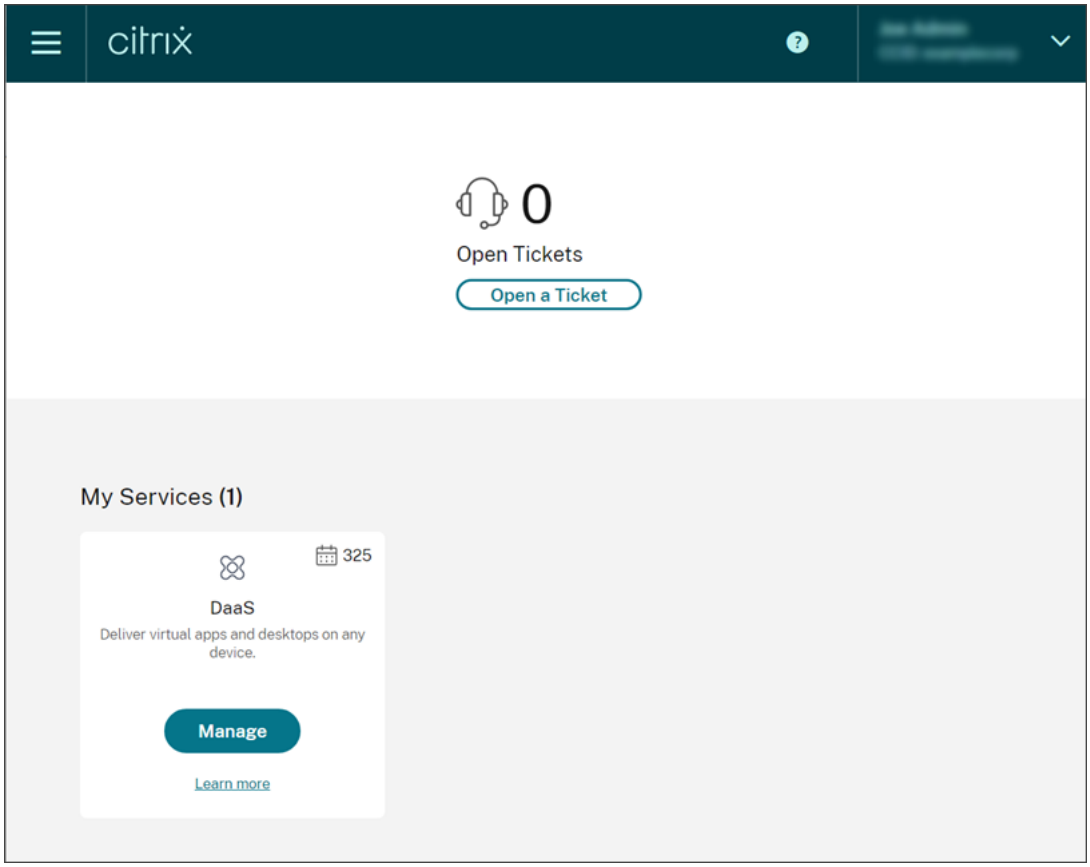
Citrix-Identität	AD- oder Azure AD-Identität für Einzelbenutzer	Gruppenbasierte AD- oder Azure AD-Identität	Nach der Authentifizierung verfügbare Berechtigungen
X		X	Jede Identität wird wie eine unabhängige Einheit behandelt. Verfügbare Berechtigungen hängen davon ab, ob sich der Administrator mit der Citrix-Identität oder der Azure AD-Identität authentifiziert.
	X	X	Administrator hat kumulative Berechtigungen beider Identitäten, wenn er sich mit Azure AD bei Citrix Cloud authentifiziert.

Citrix-Identität	AD- oder Azure AD-Identität für Einzelbenutzer	Gruppenbasierte AD- oder Azure AD-Identität	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 eine AD- oder Azure AD-Gruppe Citrix Cloud hinzufügen und Dienstberechtigungen definieren, melden sich die Administratoren in der Gruppe einfach 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

Die unter Konsolenberechtigungen beschriebenen Citrix Cloud-Plattformfeatures stehen Mitgliedern von Administratorgruppen nicht zur Verfügung.

Außerdem sind Citrix DaaS-Features, die auf Funktionen der Citrix Cloud-Plattform wie Quick Deploy-Benutzerzuweisung basieren, 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. Klicken Sie im Menü “Citrix Cloud” auf **Identitäts- und Zugriffsverwaltung** und wählen Sie dann **Administratoren** aus.
2. Wählen Sie **Administrator/Gruppe hinzufügen**.
3. Wählen Sie in den **Administratordetails** Ihr Azure AD aus und melden Sie sich gegebenenfalls bei Azure an. Wählen Sie **Weiter**.
4. Wenn Sie AD verwenden, wählen Sie die Domain 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

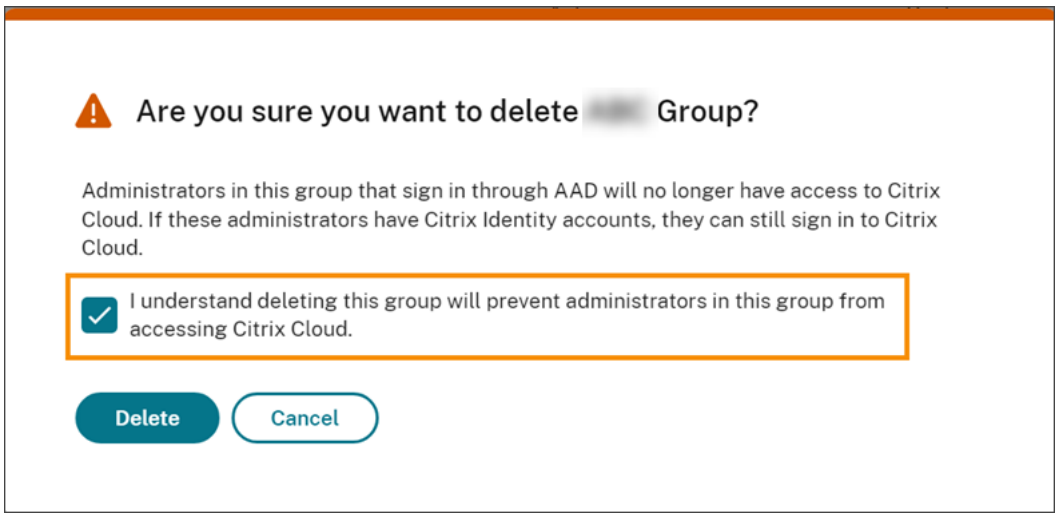
1. Klicken Sie im Menü “Citrix Cloud” auf **Identitäts- und Zugriffsverwaltung** und wählen Sie dann **Administratoren** aus.
2. Suchen Sie die Administratorgruppe, die Sie verwalten möchten, klicken Sie auf die Auslassungspunkte und wählen Sie **Zugriff bearbeiten** aus.

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. Klicken Sie im Menü “Citrix Cloud” auf **Identitäts- und Zugriffsverwaltung** und wählen Sie dann **Administratoren** aus.
2. Suchen Sie die Administratorgruppe, die Sie verwalten möchten, klicken Sie auf die Auslassungspunkte und wählen Sie **Gruppe löschen** aus.

Eine Bestätigungsmeldung wird angezeigt.

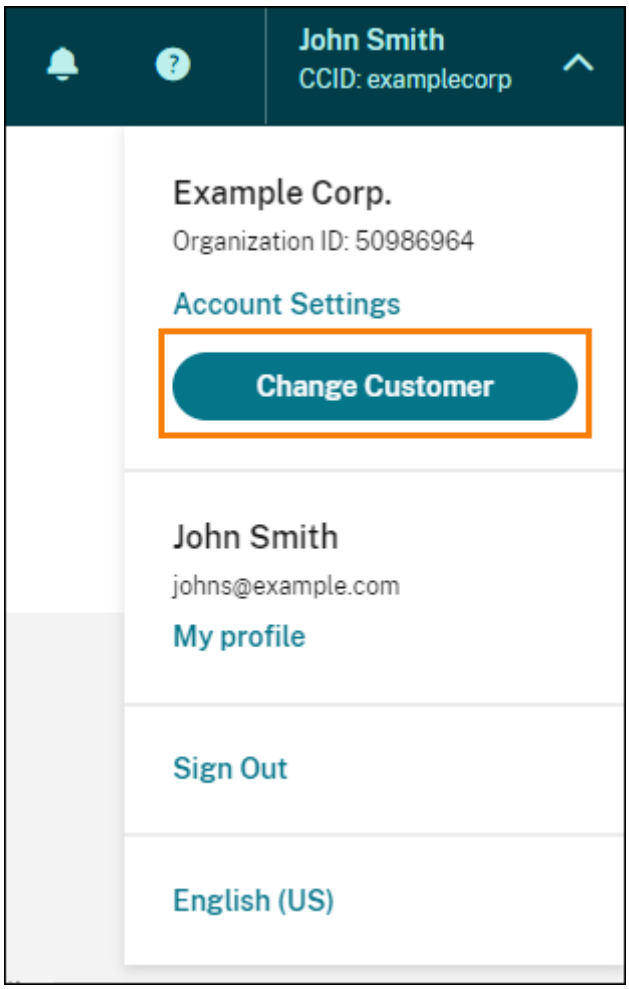


3. Wählen Sie **Ich verstehe, dass Administratoren in dieser Gruppe nach dem Löschen dieser Gruppe nicht mehr auf Citrix Cloud zugreifen können** aus. Damit bestätigen Sie, dass Sie sich der Auswirkungen des Löschens der Gruppe bewusst sind.
4. Wählen Sie **Löschen** aus.

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.

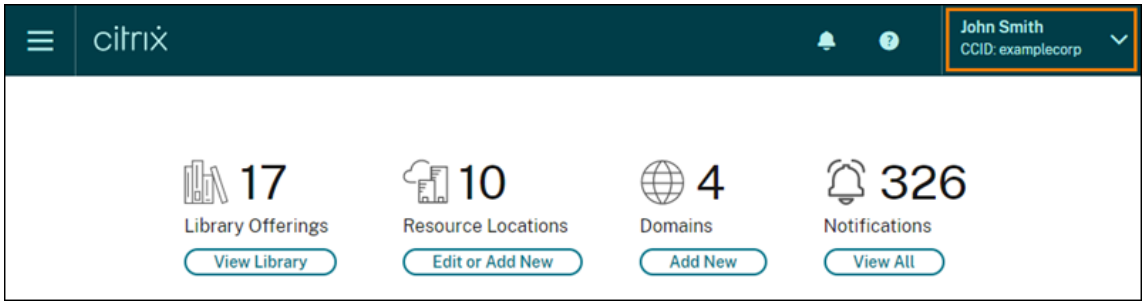


Um diese Menüoption zu aktivieren und Azure AD-Gruppenmitgliedern das Wechseln zwischen Citrix Cloud-Konten zu ermöglichen, müssen Sie die Konten verknüpfen, zwischen denen gewechselt werden soll.

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.

Verbinden von Active Directory mit Citrix Cloud

May 13, 2022

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 mithilfe 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 (Preview) 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 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.

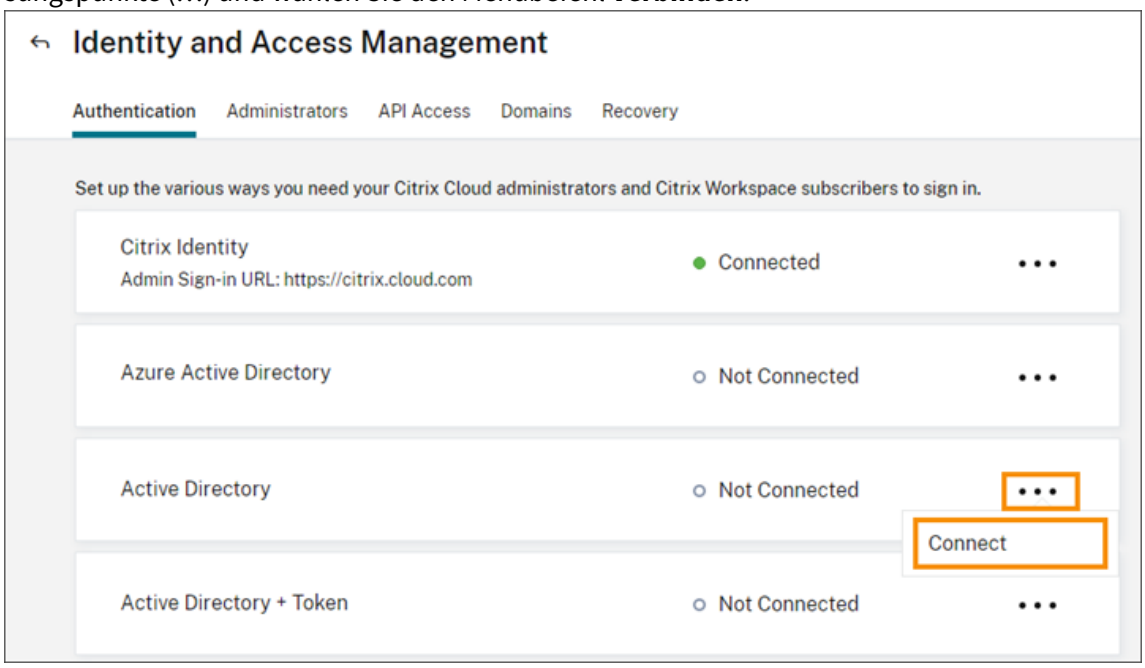
Zum Verbinden von Active Directory mit Citrix Cloud müssen Sie folgende Aufgaben erledigen:

1. Installieren von Cloud Connectors in Ihrer Domäne. Citrix empfiehlt die Installation von zwei Cloud Connectors für hohe Verfügbarkeit.

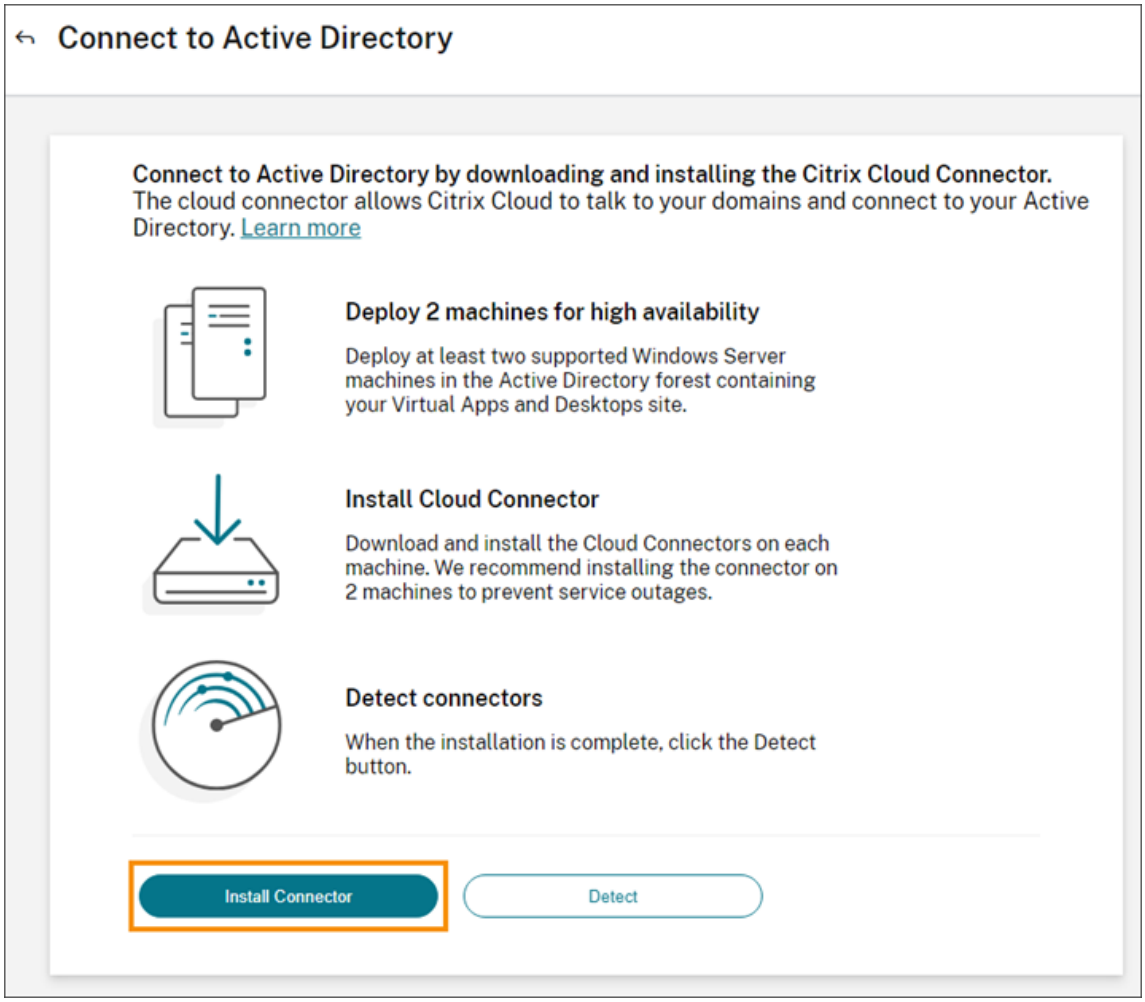
2. Wenn zutreffend, Aktivieren von Token für Benutzergeräte. Die Abonnenten können jeweils nur ein Gerät registrieren.

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 Installationssassistenten.
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.

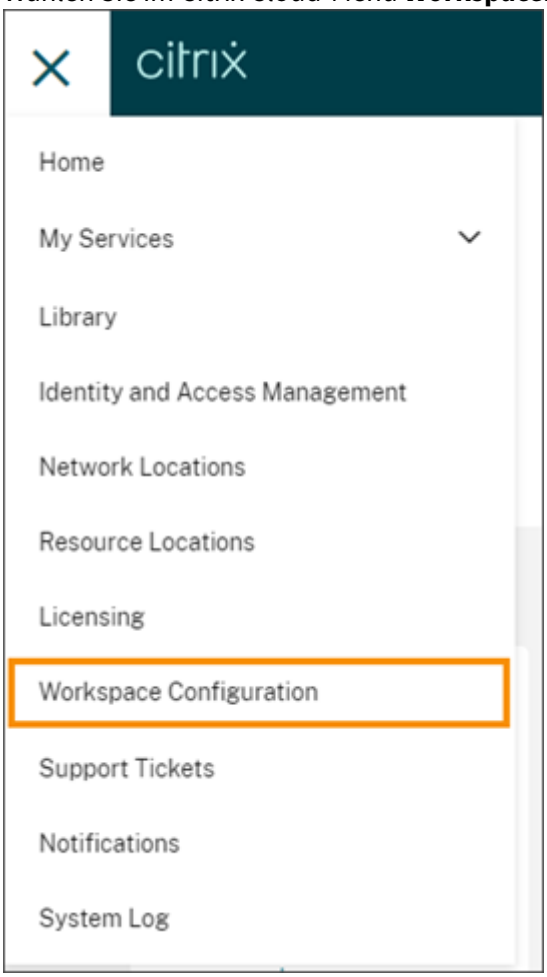
Active Directory über Connectorgeräte verbinden (Preview)

Sie können Connectorgeräte 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

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.

Verbinden von Azure Active Directory mit Citrix Cloud

October 16, 2022

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 mehrstufigen Authentifizierung 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. ADFS, 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-Anwendungen 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.

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 Anwendungsberechtigungen, 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.

1. Melden Sie sich bei Citrix Cloud unter https://citrix.cloud.com an.
2. Klicken Sie oben links auf die Menüschaltfläche und wählen Sie **Identitäts- und Zugriffsverwaltung**.
3. Suchen Sie Azure Active Directory, klicken Sie auf die Auslassungspunkte (…) und wählen Sie **Verbinden**.
4. 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.
5. 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.
6. Klicken Sie auf **Akzeptieren**, um die Berechtigungsanforderung zu akzeptieren.

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 mehrstufige Authentifizierung, 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 globaler Administrator in Azure AD. Wenn Sie Ihr Azure AD erneut verbinden, gewähren Sie Citrix Cloud als globaler Administrator in Azure AD Berechtigungen auf Anwendungsebene. So kann Citrix Cloud an Ihrer Stelle erneut eine Verbindung zu Azure AD herstellen. Weitere Informationen finden Sie unter Azure Active Directory-Berechtigungen für Citrix Cloud.
- 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**.
5. Melden Sie sich bei Erscheinen der entsprechenden Aufforderung als globaler Administrator bei Ihrem Azure-Konto an. Azure zeigt Ihnen die Berechtigungen an, die Citrix Cloud benötigt, um auf das Konto zuzugreifen und die für die Verbindung erforderlichen Informationen abzurufen.
6. Wählen Sie **Akzeptieren**, um die Berechtigungsanforderung zu akzeptieren.

Azure Active Directory-Berechtigungen für Citrix Cloud

August 31, 2022

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
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	Administratoreinladungen 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 hinzufügen.
  - **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.

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	Directory.Read.All	Verzeichnisdaten lesen	Anwendung

API-Name	Anspruchswert	Berechtigung	Typ
Microsoft Graph	User.Read.All	Vollständiges Profil aller Benutzer lesen	Anwendung
Microsoft Graph	User.Read	Anmelden und Benutzerprofil lesen	Anwendung

Administratoreinladungen 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

API-Name	Anspruchswert	Berechtigungswert	Typ
Microsoft Graph	Directory.AccessAsUser	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	Als angemeldeter Benutzer auf das Verzeichnis zugreifen	Delegiert

Verbinden eines on-premises Citrix Gateway als Identitätsanbieter mit Citrix Cloud

May 13, 2022

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 zwischen 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 mehrstufige Authentifizierung 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

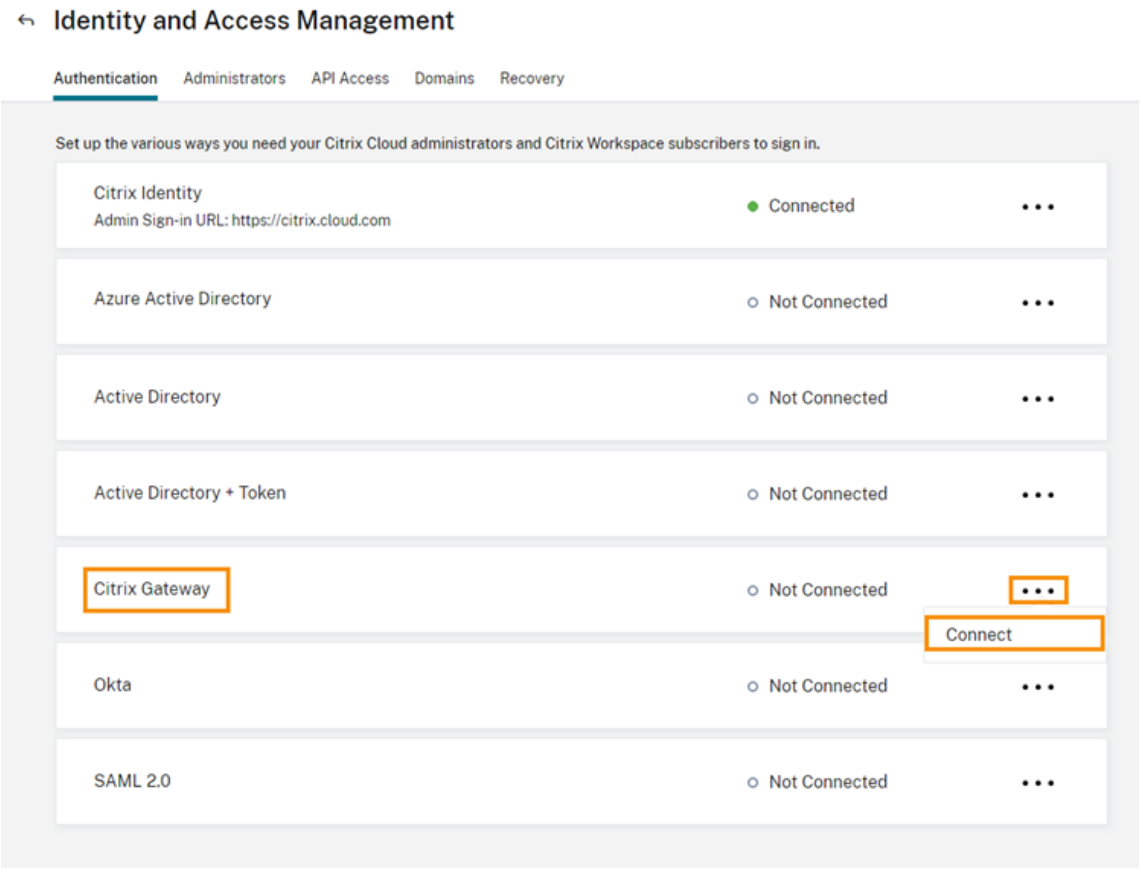
Zum Einrichten der Authentifizierung mit Citrix Gateway führen Sie die folgenden Aufgaben aus:

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.

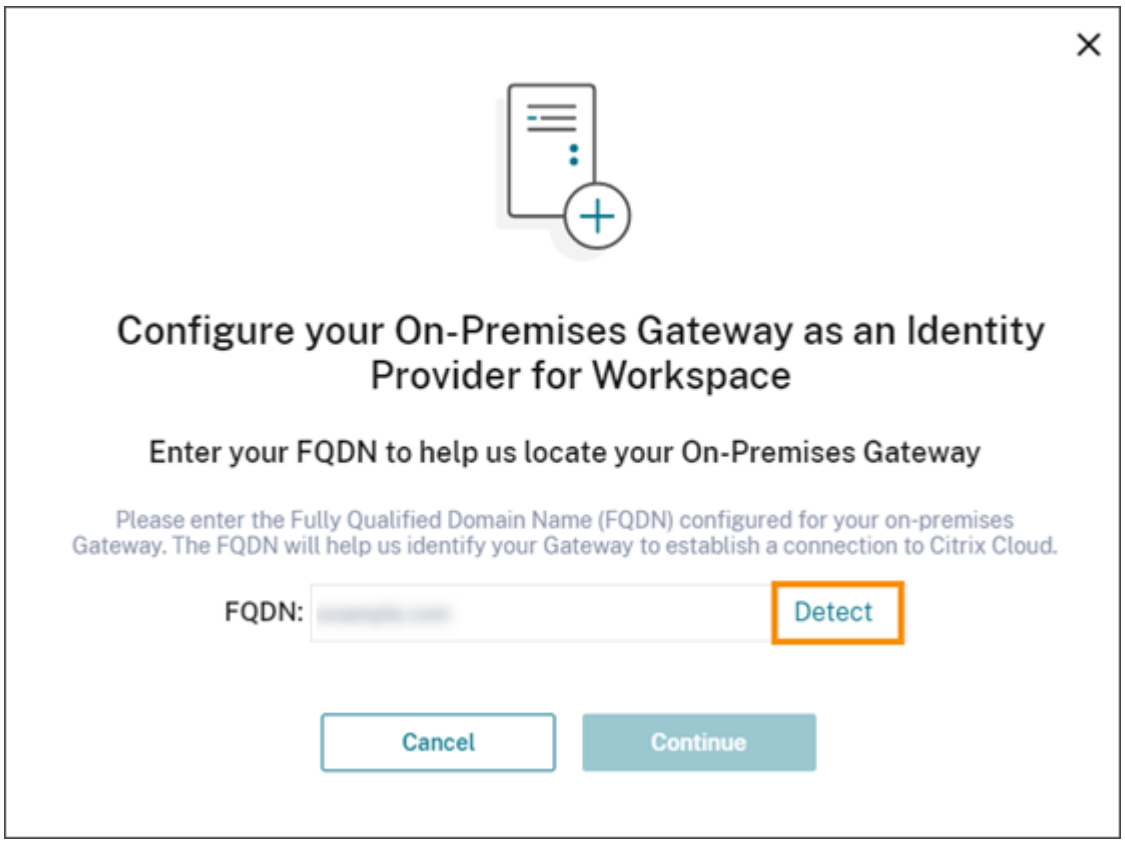
Aktivieren der Authentifizierung mit Citrix Gateway für Workspace-Abonnenten

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**.

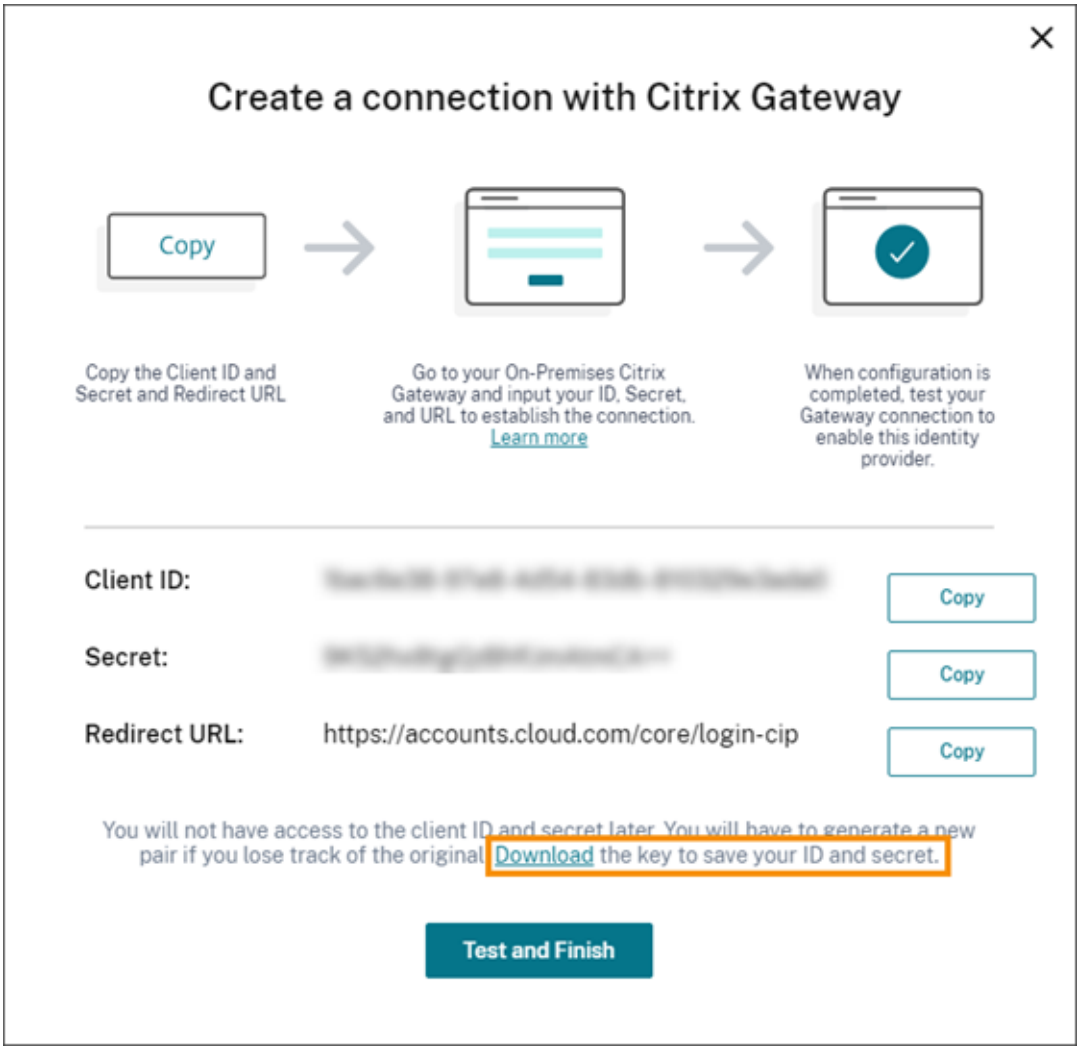


3. Geben Sie den FQDN des On-Premises-Gateways ein und klicken Sie auf **Ermitteln**.



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 **Speich-**

ern.

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 mehrstufige Authentifizierung

Wenn Sie die mehrstufige Authentifizierung 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.

Verbinden von Google als Identitätsanbieter mit Citrix Cloud

July 22, 2022

Citrix Cloud unterstützt die Verwendung von Google 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.

> **Hinweis:**
>
> Die Google-Authentifizierung ist als Preview verfügbar. Citrix empfiehlt, Preview-Features nur in Nicht-Produktionsumgebungen zu verwenden.

Anforderungen für die Konfiguration mit und ohne Domäneneinbindung

Sie können Google 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	Mit Domänenbindung	Ohne Domänenbindung	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.

Voraussetzung	Mit Domänenbindung	Ohne Domänenbindung	Weitere Informationen
AD-Synchronisierung mit Google Cloud	Nur optional, wenn Gateway Service oder Mikroapps und keine anderen Services verwendet werden. Andernfalls erforderlich.	Nein	Siehe Synchronisieren von Active Directory mit Google Cloud 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.

Google-Authentifizierung mit mehreren Citrix Cloud-Konten

In diesem Artikel wird beschrieben, wie Sie Google 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** zum Konfigurieren der Google-Authentifizierung 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

Wenn Sie eine Maschine **mit Domänenbindung** zum Konfigurieren der Google-Authentifizierung 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 ist optional, wenn Sie nur den Citrix Gateway-Dienst oder Mikroapps 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 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 Verwendung der in diesem Abschnitt angegebenen Schreibweise (groß/klein) 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 **Erstellen**. 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 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.

Verbinden von Google mit Citrix Cloud

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, klicken Sie auf die Auslassungspunkte (…) und wählen Sie im Menü **Verbinden** aus.
4. 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.
5. Geben Sie im Feld **Imitierter Benutzer** den Namen des API-Benutzerkontos mit Schreibzugriff ein.
6. Wählen Sie **Weiter**. Citrix Cloud überprüft Ihre Google-Kontodetails und testet die Verbindung.
7. Überprüfen Sie die Liste der verknüpften Domänen. Ist sie korrekt, wählen Sie **Bestätigen**, um Ihre Konfiguration zu speichern.

Aktivieren von Google für die Workspace-Authentifizierung

1. Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration > Authentifizierung**.
2. Wählen Sie **Google**. 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 22, 2022

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.

> **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.

Voraussetzungen

Cloud Connectors

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.
- Mitglied 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.

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:

- Erstellen einer Okta-OIDC-Webintegration
- 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. Übertragen Sie beim Importieren auch die Werte für Sicherheits-ID, UPN und Objekt-ID, die Ihren AD-Konten zugewiesen sind.

> 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.

Erstellen einer Okta-OIDC-Webintegration

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** und dann **Web Application**. Wählen Sie **Weiter**.
4. Geben Sie einen App-Integrationsnamen ein.

5. Wählen Sie für **Grant type** folgende Optionen:
   - Autorisierungscode
   - Implicit (Hybrid)
6. Geben Sie unter **Sign-in redirect URIs** `https://accounts.cloud.com/core/login-okta` ein.
7. Geben Sie unter **Sign-out redirect URIs** Ihre Workspace-URL aus Citrix Cloud ein.
8. Geben Sie unter **Assignments** an, ob Sie die App-Integration allen in Ihrer Organisation, nur von Ihnen angegebenen Gruppen oder später zuweisen möchten.
9. Wählen Sie **Speichern**.

Wenn Sie die App-Integration gespeichert haben, werden in der Konsole im Bereich **Client Credentials** Werte für **Client ID** und **Client Secret** angezeigt. 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) Wählen Sie auf der Konfigurationsseite der Okta-Anwendung unter **General Settings** die Option **Edit**.
   b) Löschen Sie im Abschnitt **Application** unter **Client acting on behalf of itself** die Option **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) Suchen Sie das Okta-Profil **user** und wählen Sie **Profile**. Wählen Sie unter **Attributes** die Option **Add attribute**.
   c) Geben Sie die folgenden Informationen ein:
      - Anzeigename: cip_sid
      - Variablenname: cip_sid
      - Beschreibung: AD-Benutzer-Sicherheits-ID
      - Attributlänge: größer als 1
      - Erforderliches Attribut: Ja
   d) Wählen Sie **Save and Add Another**.
   e) Geben Sie die folgenden Informationen ein:

- Anzeigename: cip_upn
- Variablenname: cip_upn
- Beschreibung: AD-Benutzerprinzipalname
- Attributlänge: größer als 1
- Erforderliches Attribut: Ja

f) Wählen Sie **Save and Add Another**.

g) Geben Sie die folgenden Informationen ein:

- Anzeigename: cip_oid
- Variablenname: cip_oid
- Beschreibung: AD-Benutzer-GUID
- Attributlänge: größer als 1
- Erforderliches Attribut: Ja

h) Wählen Sie **Speichern**.

3. Bearbeiten von Attributzuordnungen für die Anwendung:
   a) Wählen Sie in der Okta-Konsole **Directory > Directory Integrations**.
   b) Wählen Sie das zuvor integrierte AD aus. Weitere Informationen finden Sie unter Synchronisieren von Konten mit dem Okta-AD-Agent.
   c) Wählen Sie die Registerkarte **Provisioning** und dann **Settings > To Okta**.
   d) Ordnen Sie unter **Okta Attribute Mappings** die folgenden Attribute zu. Wählen Sie nach dem Ändern jedes Attributs **Save**.
      - Wählen Sie `appuser.objectSid` aus und ordnen Sie es dem Attribut `cip_sid` zu.
      - Wählen Sie `appuser.userName` aus und ordnen Sie es dem Attribut `cip_upn` zu.
      - Wählen Sie `appuser.externalId` aus und ordnen Sie es dem Attribut `cip_oid` zu.
   e) Wählen Sie **Force Sync**.

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.

Verbinden von Citrix Cloud mit Ihrer Okta-Organisation

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.

Aktivieren der Okta-Authentifizierung für Workspaces

1. Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration > Authentifizierung**.
2. Wählen Sie **Okta**. Wählen Sie **Ich verstehe die Auswirkungen auf Abonnenten**, wenn Sie dazu aufgefordert werden.
3. Klicken Sie auf **Akzeptieren**, um die Berechtigungsanforderung zu akzeptieren.

SAML als Identitätsanbieter mit Citrix Cloud verbinden

October 16, 2022

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.

Bei den meisten SAML-Anbietern können Sie die SAML-Authentifizierung gemäß den Informationen in diesem Artikel einrichten. Wenn Sie die SAML-Authentifizierung mit Ihrem Azure AD verwenden möchten, können Sie die Citrix Cloud-SAML-SSO-App aus der Azure AD-App-Galerie verwenden. Weitere Informationen zur Verwendung der Citrix Cloud-SAML-SSO-App zum Einrichten der SAML-Authentifizierung in Citrix Cloud finden Sie unter Tutorial: Integration des einmaligen Anmeldens (SSO) von Azure Active Directory mit Citrix Cloud SAML SSO auf der Website mit der Azure AD-Dokumentation.

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 Active Directory (AD) verfügen. Abonnenten ohne AD-Konto können sich nicht erfolgreich bei ihrem Workspace anmelden, wenn die SAML-Authentifizierung konfiguriert ist.
- 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 bei Citrix Workspace zu erfassen. Wenn diese Eigenschaften nicht ausgefüllt werden, können Abonnenten sich nicht anmelden. Zu diesen Eigenschaften gehören:
  - E-Mail-Adresse
  - Anzeigename (optional)

  - Allgemeiner Name
  - SAM-Kontoname
  - Benutzerprinzipalname
  - Objekt-GUID
  - SID
- Verbinden Sie Ihr Active Directory (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.

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:

- SecurityIDentifier (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- Mail (E-Mail)

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.
2. Wenn Sie noch keine benutzerdefinierten Attribute haben, die den oben beschriebenen AD-Benutzerattributen zugeordnet sind, erstellen Sie die benutzerdefinierten Attribute und ordnen Sie sie AD 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.

> **Hinweis:**
>
> Wenn Sie bereits benutzerdefinierte Attribute erstellt haben, die den oben in diesem Abschnitt aufgeführten erforderlichen AD-Benutzerattributen zugeordnet sind, müssen Sie keine weiteren benutzerdefinierten Attribute erstellen und zuordnen. Verwenden Sie stattdessen die vorhandenen benutzerdefinierten Attribute beim Konfigurieren der Metadaten von Ihrem SAML-Anbieter in Citrix Cloud.

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.

Weitere Informationen finden Sie in diesem Artikel unter Aufgabenüberblick.

Aufgabenüberblick

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.

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- und E-Mail-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 8.

> **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 die folgenden Attribute hinzu:
   - cip_sid
   - cip_upn
   - cip_oid
   - cip_email
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:
   - Wählen Sie `objectSid` aus und ordnen Sie es dem Attribut `cip_sid` zu.
   - Wählen Sie `userPrincipalName` aus und ordnen Sie es dem Attribut `cip_upn` zu.
   - Wählen Sie `ObjectGUID` aus und ordnen Sie es dem Attribut `cip_oid` zu.
   - Wählen Sie `mail` aus und ordnen Sie es dem Attribut `cip_email` 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.

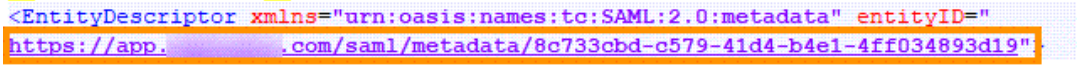
4. Geben Sie die folgenden Details für die Connectoranwendung ein:
   - Geben Sie im Feld **Zielgruppe** `https://saml.cloud.com` ein.
   - Geben Sie im Feld **Empfänger** `https://saml.cloud.com/saml/acs` ein.
   - Geben Sie im Feld für ACS-URL-Validator `https://saml.cloud.com/saml/acs` ein.
   - Geben 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	cip_sid oder Ihr vorhandenes SID-Attribut
cip_upn	cip_upn oder Ihr vorhandenes UPN-Attribut
cip_oid	cip_oid oder Ihr vorhandenes OID-Attribut
cip_email	cip_email oder Ihr vorhandenes E-Mail-Attribut

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** 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.
- Wählen Sie unter **SAML-Antwort** die Signiermethode aus, die Ihr SAML-Anbieter für die SAML-Antwort und SAML-Assertion verwendet. Standardmäßig lehnt Citrix Cloud 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 PEM-Datei herunter.
4. Wählen Sie im Bildschirm **SAML konfigurieren** in Citrix Cloud die Option **Datei hochladen** und wählen Sie die im vorherigen Schritt heruntergeladene PEM-Datei 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.
7. Suchen Sie unter **Abmelde-URL** das **SingleSignOnService**-Element mit der HTTP-Redirect-Bindung in der Metadatendatei Ihres SAML-Anbieters und geben Sie die URL ein. Wenn Sie die Abmelde-URL weglassen, sendet Citrix Cloud keine Abmeldeanforderung an den Identitätsanbieter. Stattdessen leitet Citrix Cloud zur Workspace-URL um. Citrix Cloud unterstützt kein Single Log Out (SLO) oder das Senden signierter Abmeldeanforderungen.
8. Stellen Sie sicher, dass die folgenden Standardnamen-Attributwerte in Citrix Cloud mit den entsprechenden Attributwerten in der Verwaltungskonsole Ihres SAML-Anbieters übereinstimmen. Wenn die Werte Ihres SAML-Anbieters abweichen, können Sie diese Werte in Citrix Cloud ändern, um sicherzustellen, dass sie mit Ihrem SAML-Anbieter übereinstimmen.
   - **Attributname für Benutzeranzeigename**: `displayName`
   - **Attributname für Vorname**: `givenName`
   - **Attributname für Nachname**: `familyName`
9. Geben Sie in Citrix Cloud die benutzerdefinierten SAML-Attribute Ihres SAML-Anbieters ein:
   - Geben Sie unter **Attributname für Sicherheits-ID (SID)** Ihren benutzerdefinierten SID-Attributnamen ein. Der Standardwert ist `cip_sid`.
   - Geben Sie unter **Attributname für Benutzerprinzipalname (UPN)** Ihren benutzerdefinierten UPN-Attributnamen ein. Der Standardwert ist `cip_upn`.
   - Geben Sie unter **Attributname für E-Mail** den Namen Ihres benutzerdefinierten E-Mail-Attributs ein. Der Standardwert ist `cip_email`.
   - Geben Sie unter **Attributname für AD-Objektbezeichner (OID)** Ihren benutzerdefinierten OID-Attributnamen ein. Der Standardwert ist `cip_oid`.

10. 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.

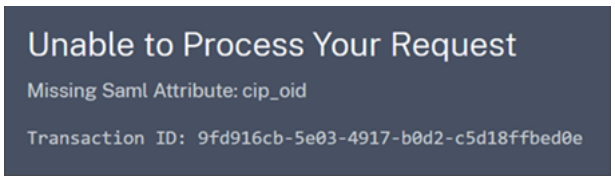
SAML-Authentifizierung für Workspaces aktivieren

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 auftreten, wenn die erforderlichen Attribute in Ihrer SAML-Konfiguration nicht korrekt codiert sind. Wenn ein Attributfehler auftritt, zeigt Citrix Cloud eine Fehlermeldung an, die das fehlerhafte Attribut enthält.



Um diese Art von Fehler zu beheben, stellen Sie sicher, dass die Attribute gemäß der folgenden Tabelle codiert sind.

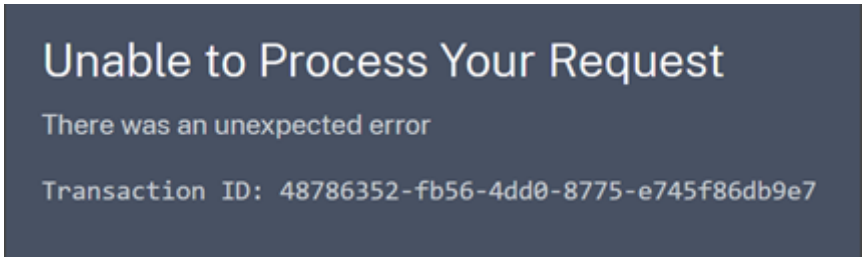
Attribut	Codierung
cip_email	Zeichenfolge (`user@domain`)
cip_oid	Base64 oder Zeichenfolge
cip_sid	Base64 oder Zeichenfolge
cip_upn	Zeichenfolge (`user@domain`)

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 den Parameter “Prompt=Login”, um zusätzliche Kennwortanforderungen zu entfernen.

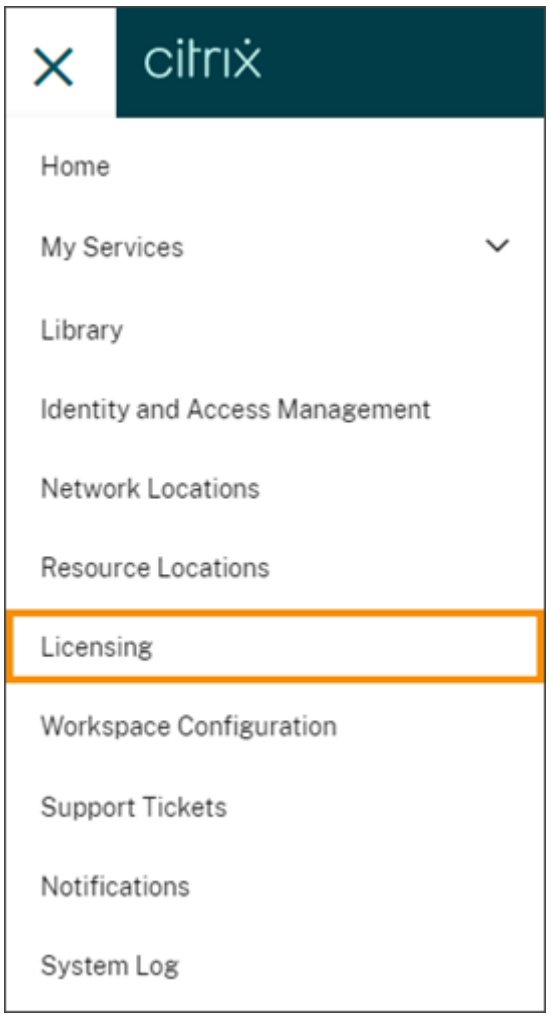
Lizenzierung für Citrix Cloud

April 29, 2022

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:
  - Überwachung von Kundenlizenzen und Lizenznutzung für Citrix DaaS
  - Überwachung von Kundenlizenzen und Lizenznutzung für Citrix DaaS Standard für Azure

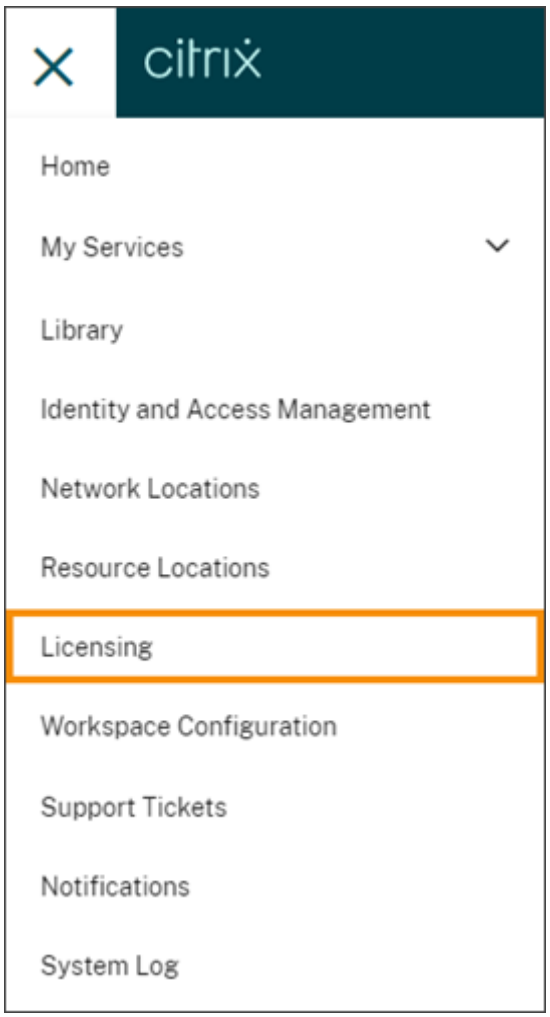
Überwachen der Lizenzen und der aktiven Nutzung von Cloud Services

August 1, 2022

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:

- Überwachen von Lizenzen und aktiver Nutzung für Citrix DaaS (Benutzer/Gerät)
- Überwachen von Lizenzen und Spitzenauslastung für Citrix DaaS und Citrix DaaS Standard für Azure (gleichzeitig)
- 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.

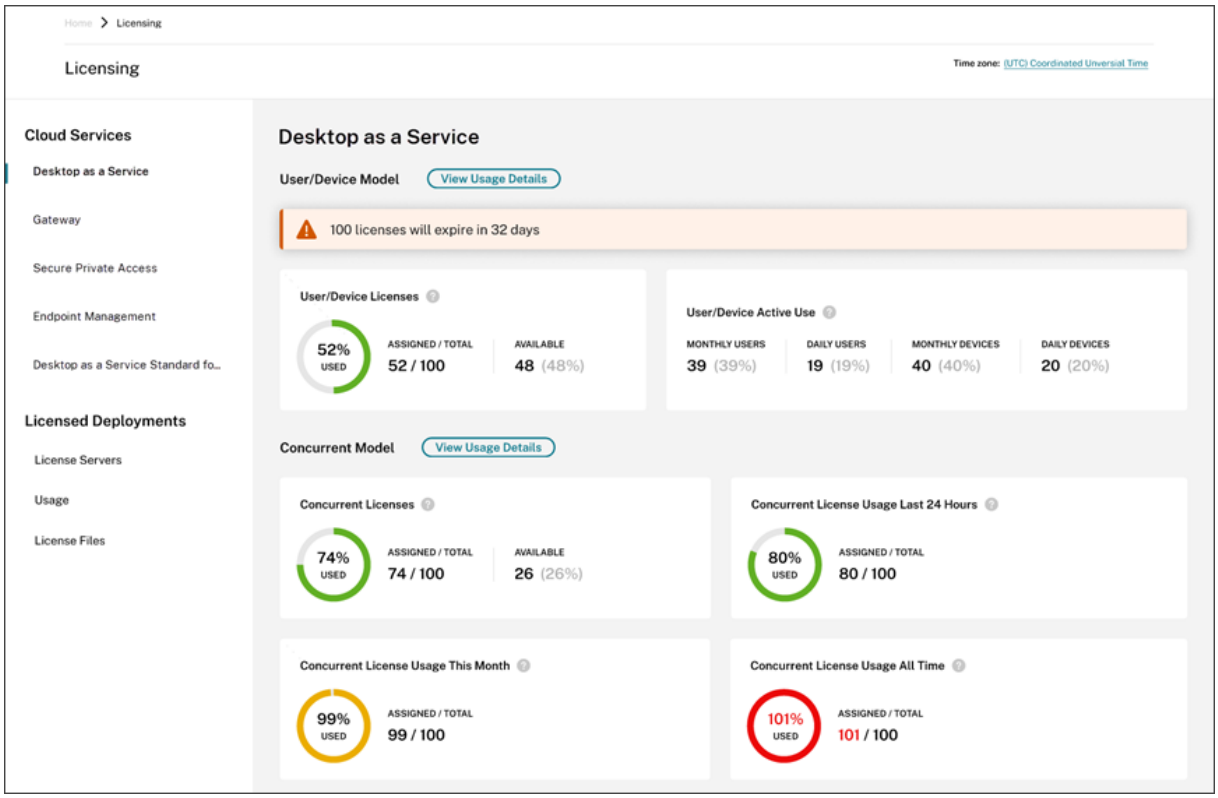
Wenn auf der Konsolenseite "Lizenzierung" die Lizenznutzung mit Multityplizenzierung trotz erfolgreicher Einrichtung mit Web Studio oder PowerShell nicht korrekt angezeigt wird, haben Sie folgende Optionen:

- 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



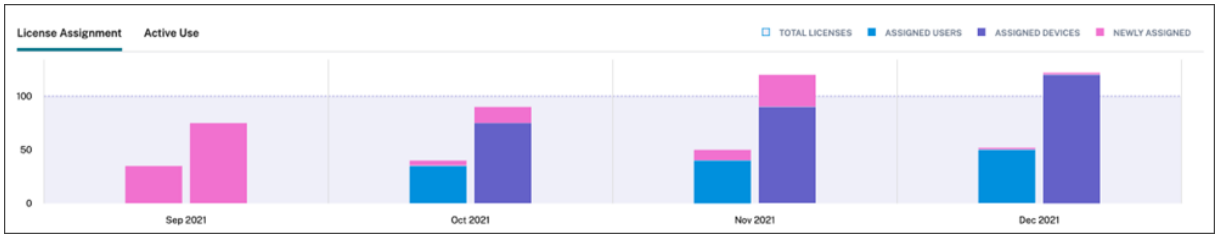
Die Zusammenfassung unter “Lizenzierung” bietet für jeden unterstützten Service einen Überblick über Folgendes:

- 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.

Überwachen von Lizenzen und aktiver Nutzung für Citrix DaaS (Benutzer/Gerät)

July 11, 2022

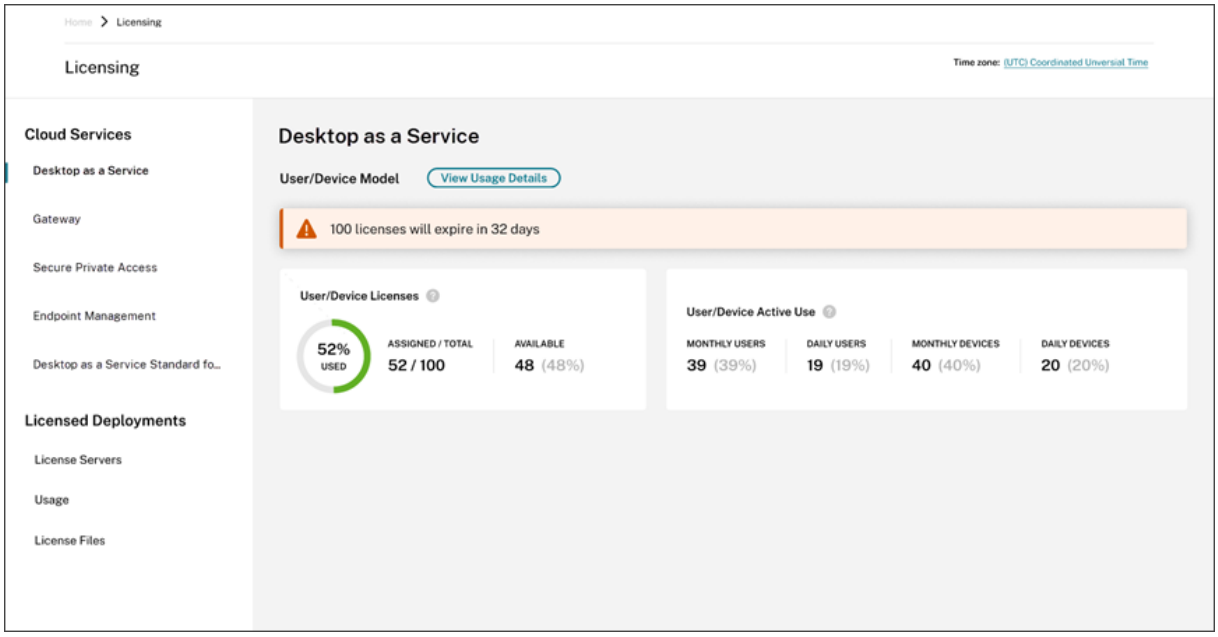
In diesem Artikel wird beschrieben, wie Sie Cloudservice-Lizenzzuweisungen verwalten und die aktive Nutzung mithilfe der Lizenzierungskonsole in Citrix Cloud überwachen können.

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.

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

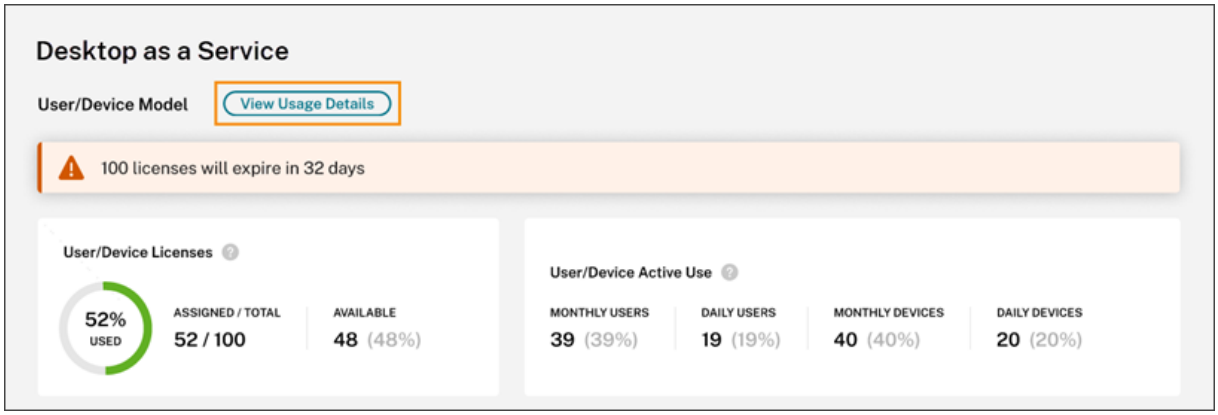
Wenn der Service von 100 eindeutigen Benutzern und 50 eindeutigen Geräten verwendet wurde, berechnet Citrix Cloud die Anzahl der zugewiesenen Lizenzen anhand des niedrigeren Werts (50). Der Prozentsatz der verwendeten Lizenzen und die Anzahl der verfügbaren Lizenzen basieren auf diesen 50 zugewiesenen Lizenzen.

Beispiel für die Berechnung der aktiven Nutzung

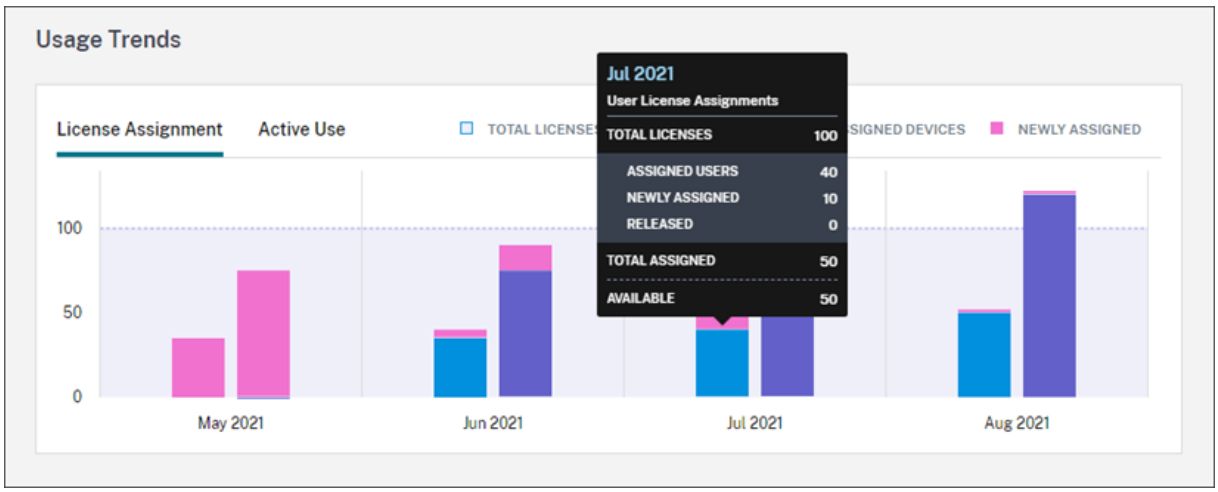
Wenn der Service in den letzten 30 Tagen von 10 eindeutigen Benutzern und 20 eindeutigen Geräten genutzt wurde, liegt die monatliche aktive Nutzung laut Citrix Cloud bei 10 aktiven Benutzern und 20 aktiven Geräten. Analog liegt die tägliche aktive Nutzung bei 30 aktiven Benutzern und 15 aktiven Geräten, 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.

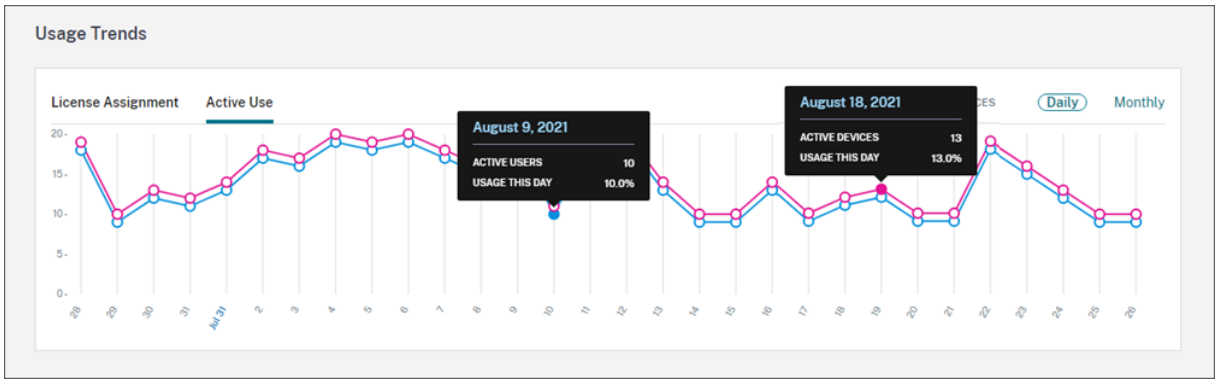


Im Diagramm **Lizenzzuweisung** werden folgende Informationen angezeigt, wenn Sie auf den Balken für einen bestimmten Monat oder Tag zeigen:

- **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.

Das Diagramm **Aktive Nutzung** zeigt die aktiven Benutzer und Geräte für den vergangenen Kalender-

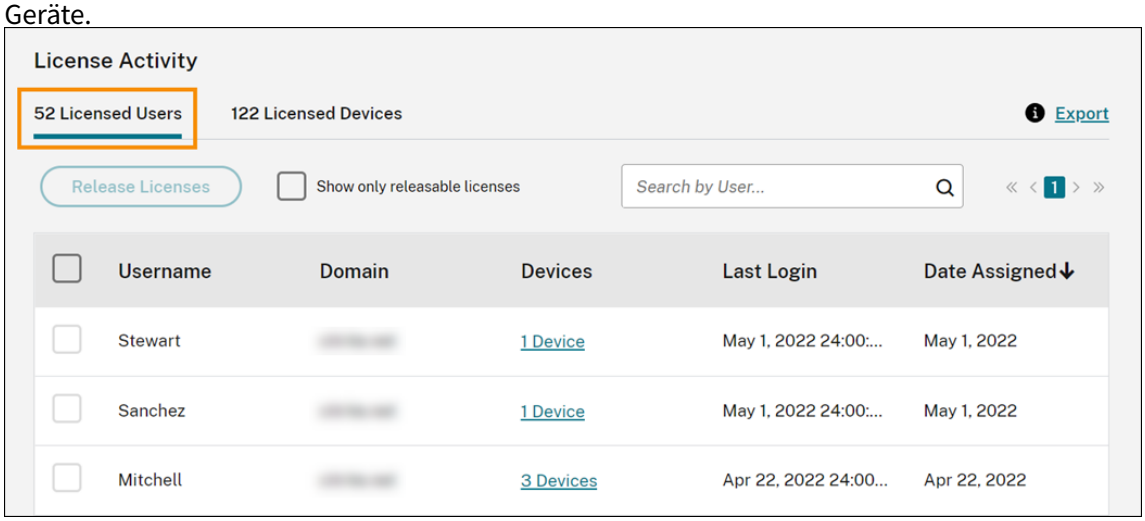
monat bzw. das Kalenderjahr an. Wenn Sie auf einen bestimmten Punkt im Diagramm zeigen, werden die Anzahl der aktiven Benutzer oder Geräte und die prozentuale Nutzung angezeigt.



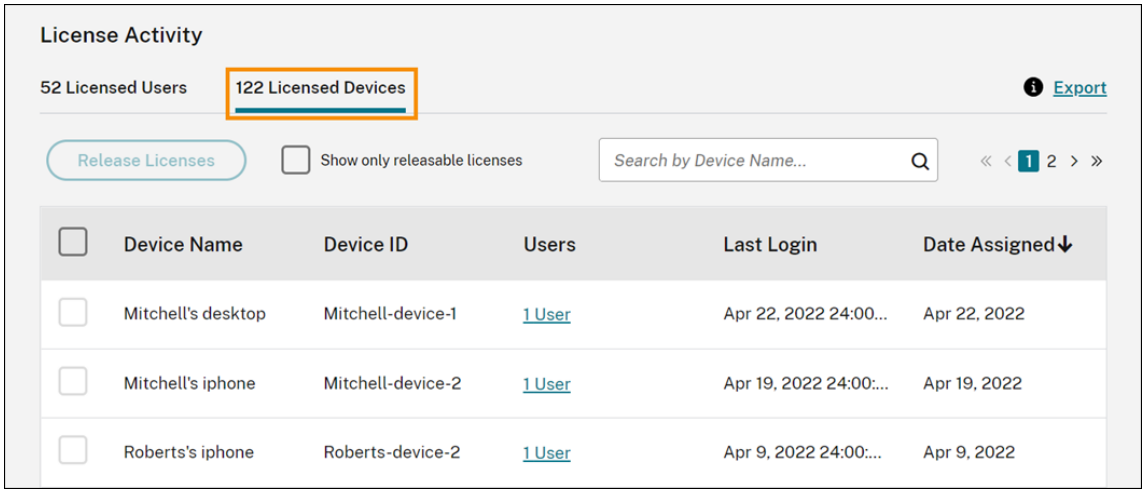
Lizenzaktivität

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

Benutzerlizenzen können freigegeben werden, wenn ein Benutzer in den letzten 30 Tagen keine App oder keinen Desktop gestartet hat. Gerätelizenzen können freigegeben werden, wenn ein Gerät in den letzten 30 Tagen nicht zum Starten von Apps oder Desktops verwendet wurde.

Sie können einzelne Lizenzen über die Liste **Lizenzierte Benutzer** oder **Lizenzierte Geräte** freigeben. Für Benutzer und Geräte mit Lizenzen, die freigegeben werden können, wird ein dunkelgraues Kontrollkästchen angezeigt, das Sie auswählen können. Bei Benutzern und Geräten, die in den letzten 30 Tagen Apps oder Desktops gestartet haben, wird das Kontrollkästchen hellgrau angezeigt und ist inaktiv.

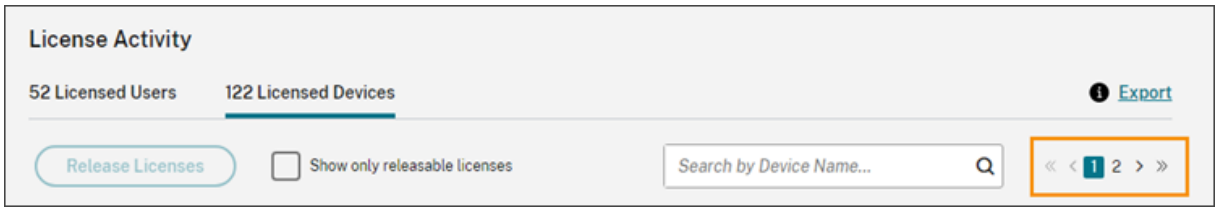
Wenn Sie Citrix Azure Consumption Fund erworben haben, hängt die Freigabeberechtigung für zugewiesene Lizenzen von dem erworbenen Plan ab. Weitere Informationen finden Sie unter Monitor

Citrix Managed Azure resource consumption for Citrix DaaS.

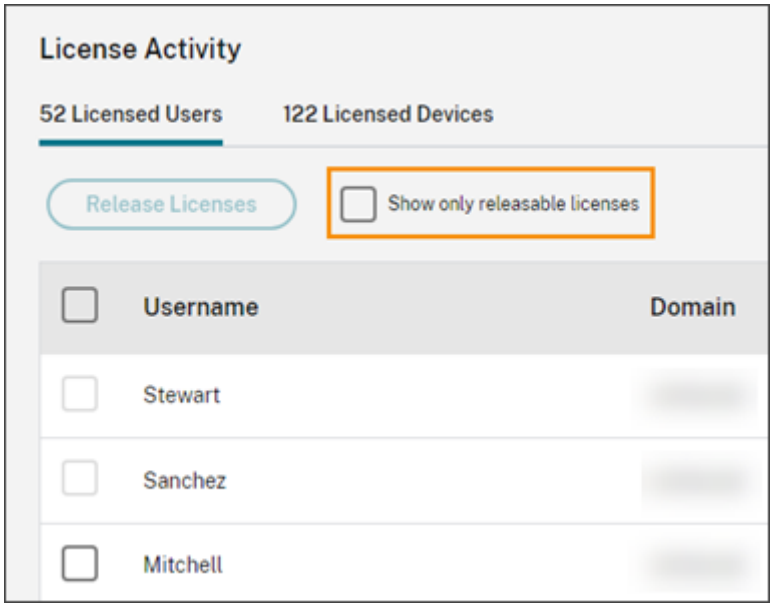
Nach der Freigabe ihrer Lizenz können Benutzer eine neue Lizenz erhalten, indem sie sich anmelden und den Cloudservice verwenden.

Finden geeigneter Lizenzen

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

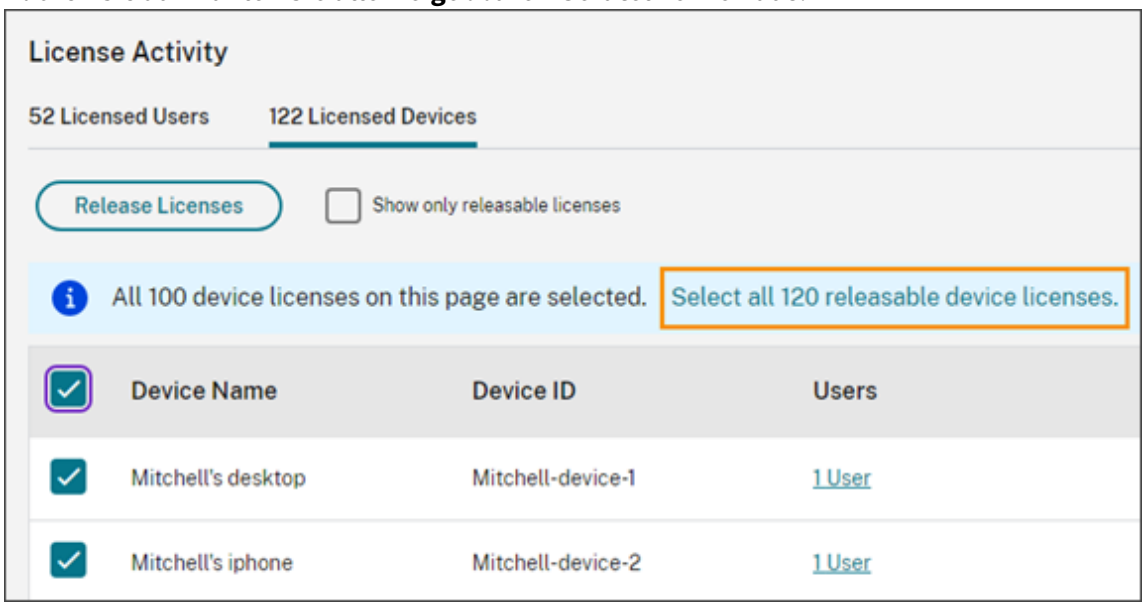
Aktivieren Sie das dunkelgraue Kontrollkästchen neben jeder Lizenz, um diese für die Freigabe auszuwählen. Wenn Sie eine Lizenz aus der Liste auswählen, wird die Schaltfläche **Lizenzen freigeben** aktiv.

Sie können auch alle geeigneten Lizenzen in einem einzigen Vorgang auswählen. Wenn Sie nicht mehr

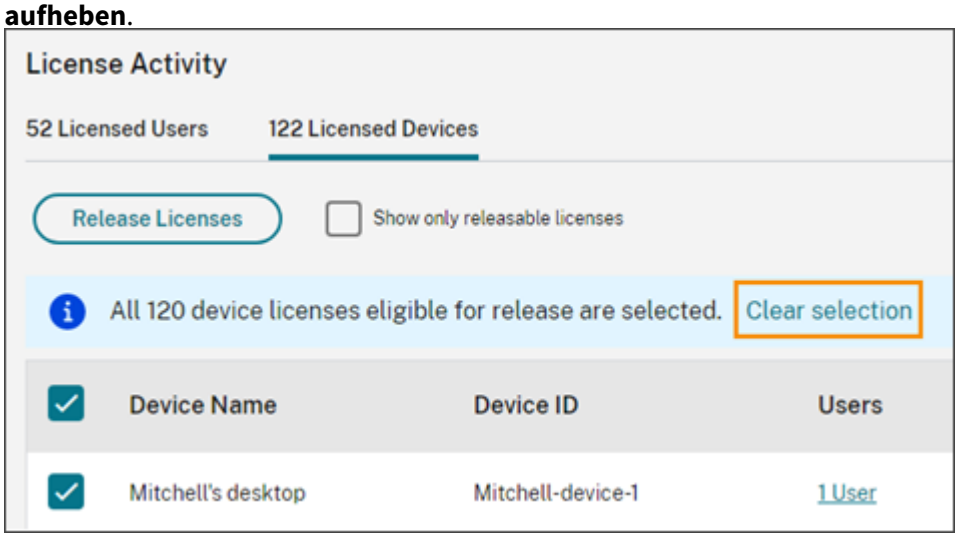
als 100 berechtigte Lizenzen haben, aktivieren Sie einfach das Kontrollkästchen neben **Benutzername** in der Kopfzeile der Liste, um alle geeigneten Lizenzen auszuwählen.

Wenn Sie mehr als 100 berechtigte Lizenzen haben:

1. Aktivieren Sie das Kontrollkästchen neben **Benutzername** in der Kopfzeile der Liste, um alle geeigneten Lizenzen auszuwählen, die auf der Seite angezeigt werden.
2. Klicken Sie auf **Wählen Sie alle freigebbaren Gerätelizenzen aus**.



3. Um die Auswahl aller Lizenzen auf allen Seiten der Liste aufzuheben, klicken Sie auf **Auswahl aufheben**.



Freigeben zugewiesener Lizenzen

1. Wählen Sie unter **Lizenzaktivität** die Registerkarte **Lizenzierte Benutzer** oder **Lizenzierte Geräte**.

2. Wählen Sie bei Bedarf **Nur freigebbare Lizenzen anzeigen**, um nur die Benutzer mit Lizenzen anzuzeigen, die für die Freigabe in Frage kommen.
3. Wählen Sie die Benutzer oder Geräte aus, die Sie verwalten möchten, und wählen Sie dann **Lizenzen freigeben**.
4. Überprüfen Sie die ausgewählten Benutzer bzw. Geräte und wählen Sie **Lizenzen freigeben**.

Überwachen von Lizenzen und Verwendungsspitzen für Citrix DaaS und Citrix DaaS Standard für Azure (Gleichzeitig-Lizenzmodell)

August 31, 2022

In diesem Artikel wird die Verwaltung von Gleichzeitig-Lizenzen für **Citrix DaaS** und **Citrix DaaS Standard für Azure** beschrieben.

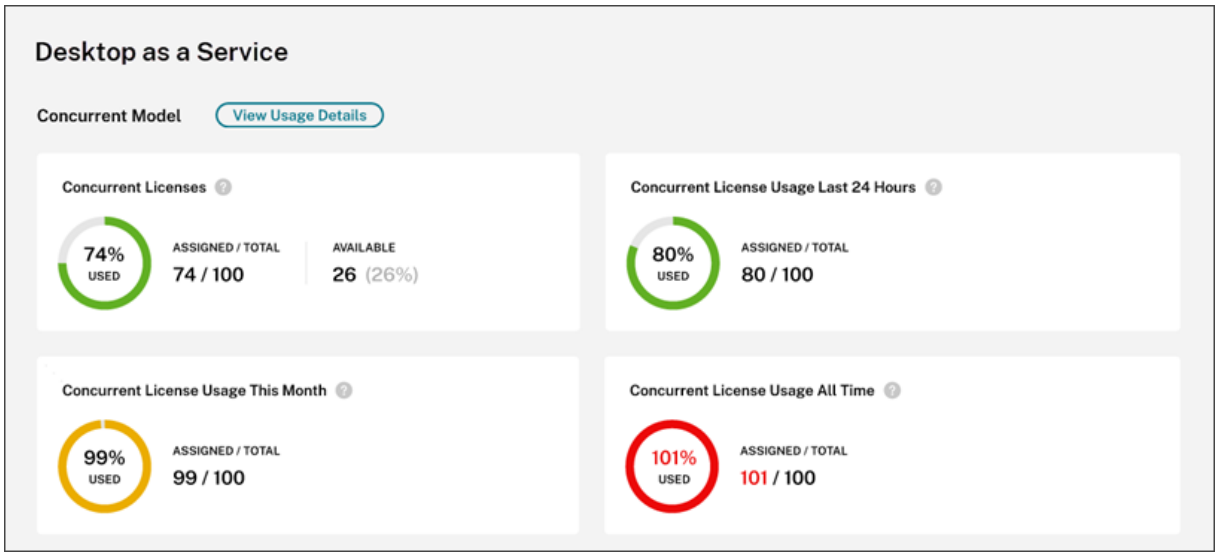
Informationen zur Benutzer/Gerät-Lizenzierung für diese Services finden Sie in den folgenden Artikeln:

- Überwachen von Lizenzen und aktiver Nutzung für Citrix DaaS (Benutzer/Gerät)
- Überwachen von Lizenzen und Nutzung für Citrix DaaS Standard für Azure

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 (CCU-Lizenzen) finden Sie unter CCU-Lizenzen.

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 oder 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.

> **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.

Nutzungstrends und Lizenzaktivität

Klicken Sie für auf **Nutzungsdetails anzeigen**, um historische Nutzungsdaten Ihrer Lizenzen anzuzeigen.

Der Bereich **Nutzungstrends** stellt folgende Informationen bereit:

- **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.

Überwachen von Lizenzen und aktiver Nutzung für Citrix DaaS Standard für Azure

July 22, 2022

Lizenzierungsmodelle

Citrix Cloud kann Ihnen bei der Verwaltung von Lizenzen für Citrix DaaS Standard für Azure helfen, in dem das Benutzer/Gerät- oder das Gleichzeitig-Lizenzmodell verwendet wird. In diesem Artikel wird nur die Verwaltung von Lizenzzuweisungen per **Benutzer-/Gerätelizenzmodell** beschrieben.

Die Verwaltung mit Gleichzeitig-Lizenzmodell bei Citrix DaaS Standard für Azure entspricht der von Citrix DaaS. Weitere Informationen finden Sie unter Überwachen von Lizenzen und Verwendungsspitzen für Citrix DaaS (gleichzeitig).

Citrix Azure Consumption Fund

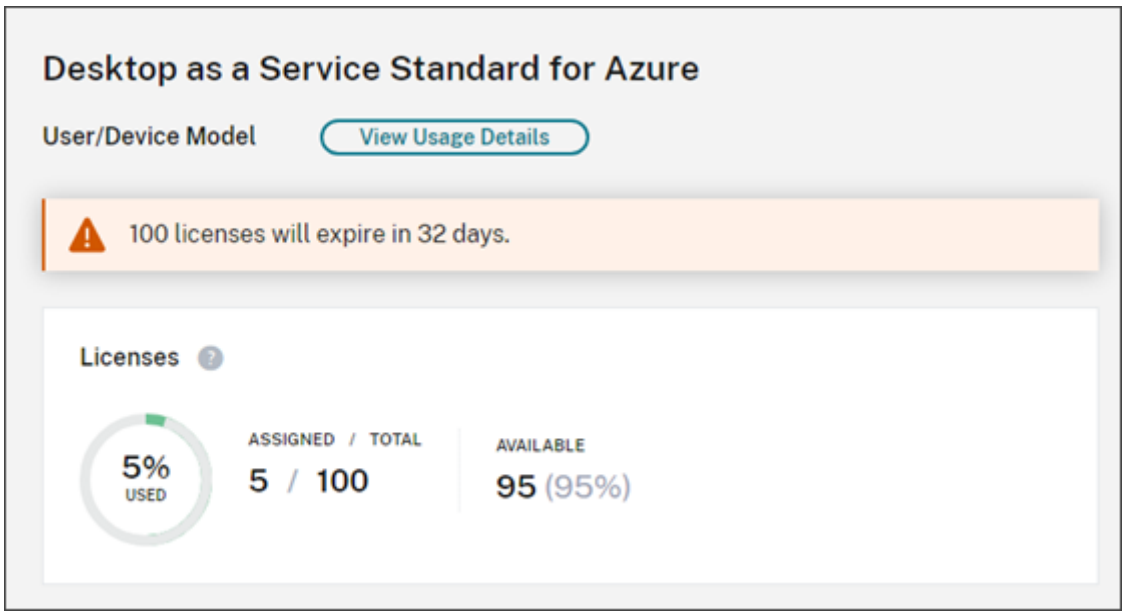
Wenn Sie Citrix Azure Consumption Fund für Ihre Service-Bereitstellung erworben haben, finden Sie Informationen zur Nutzungsberichterstattung für von Citrix verwaltete Ressourcen unter Monitor Citrix Managed Azure resource consumption for Citrix DaaS.

Lizenzzuweisung

Beim Benutzer/Gerät-Lizenzierungsmodell weist Citrix Cloud eine Lizenz zu, wenn ein eindeutiger Benutzer oder ein eindeutiges Gerät zum ersten Mal einen Desktop startet.

Beim Gleichzeitig-Lizenzierungsmodell weist Citrix Cloud eine Lizenz zu, wenn ein Benutzer eine App oder einen Desktop auf dem Gerät startet. Weitere Informationen dazu, wie Citrix Cloud die Anzahl der verwendeten Gleichzeitig-Lizenzen ermittelt, finden Sie unter Überwachen von Lizenzen und Verwendungsspitzen für Citrix DaaS (gleichzeitig).

Zusammenfassung zur Lizenzierung

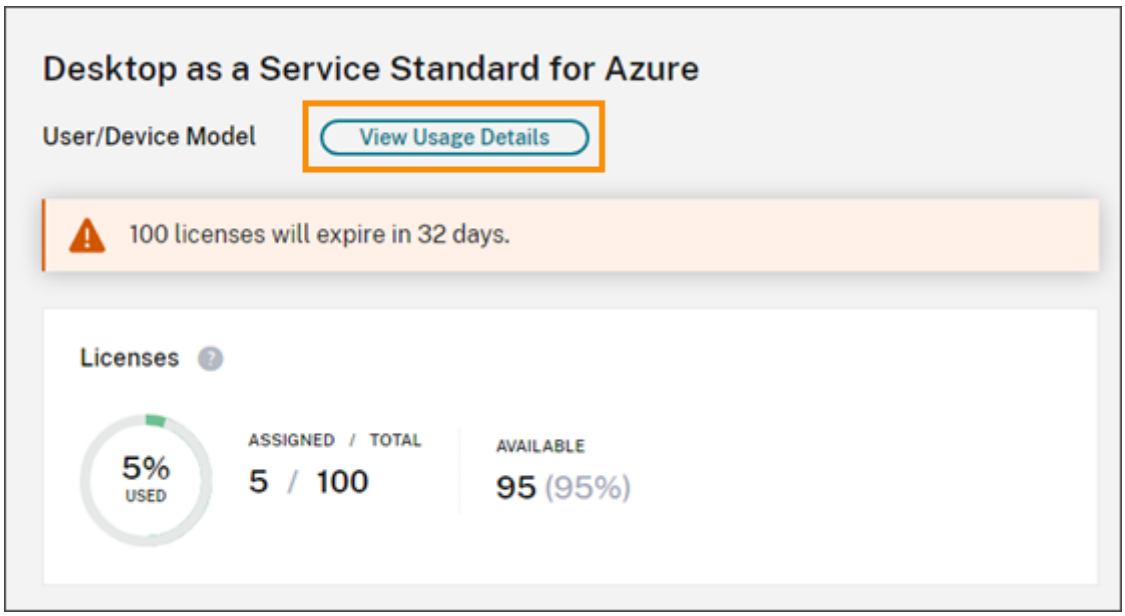


Die Zusammenfassung der Lizenzierung bietet einen Überblick über die folgenden Informationen:

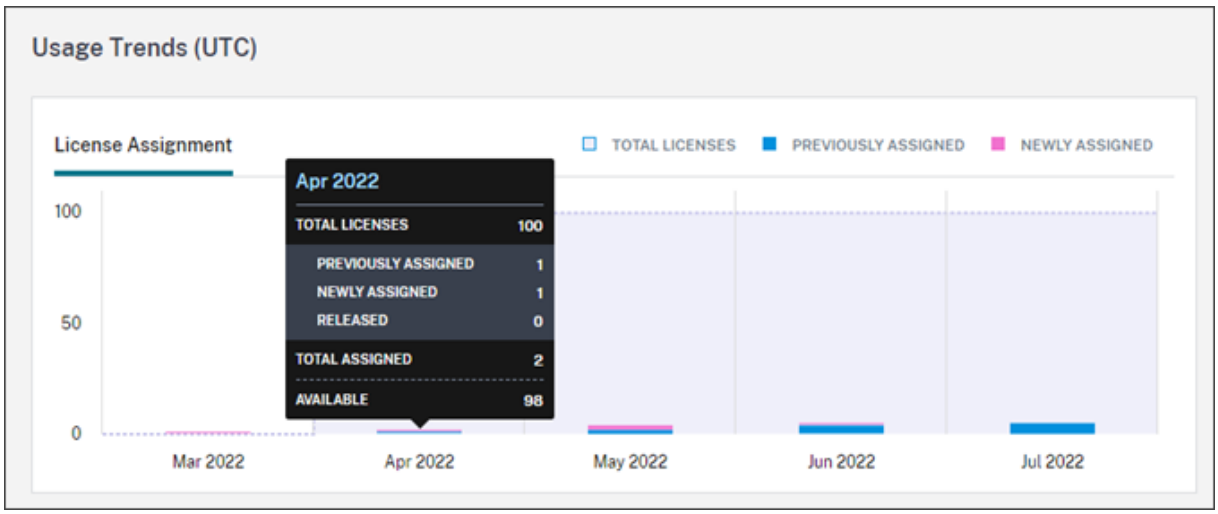
- Prozentsatz der insgesamt erworbenen Lizenzen, die zugewiesen sind (verwendet werden). Wenn sich der Prozentsatz 100 % nähert, wechselt der Prozentsatz von grün zu gelb. Wenn der Prozentsatz 100 % überschreitet, wird der Prozentsatz rot angezeigt.
- Das Verhältnis zugewiesener zu erworbenen Lizenzen und die Anzahl der verbleibenden verfügbaren Lizenzen.

Nutzungstrends und Lizenzaktivität

Klicken Sie auf **Nutzungsdetails anzeigen**, um eine Aufschlüsselung der Nutzungsberichte und -trends sowie eine Liste der Benutzer anzuzeigen, die Citrix DaaS Standard für Azure-Lizenzen verwenden.



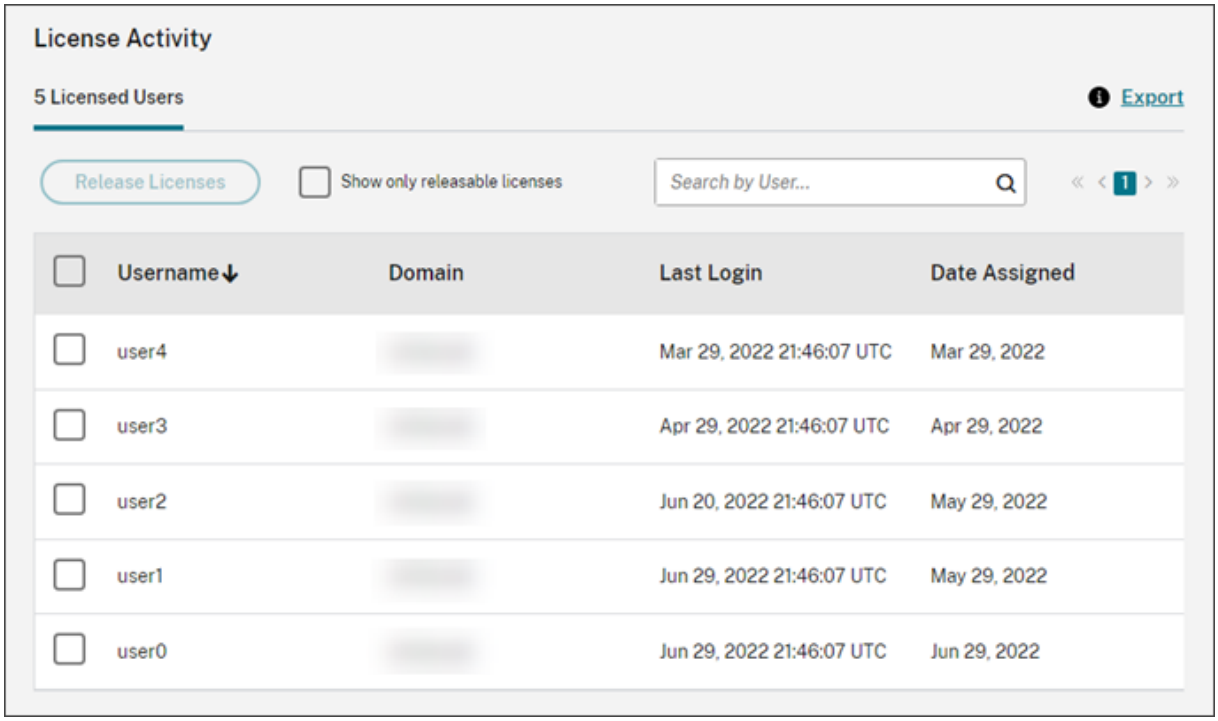
Im Abschnitt **Nutzungstrends** wird diese Aufschlüsselung als Diagramm angezeigt.



Wenn Sie auf den Balken für einen bestimmten Monat zeigen werden folgende 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".

Lizenzaktivität



Im Abschnitt **Lizenzaktivität** wird eine Liste der Benutzer angezeigt, denen Lizenzen zugewiesen wurden. Außerdem wird das Datum angezeigt, an dem 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

In diesem Abschnitt wird die Freigabe von **Benutzer/Gerät-Lizenzen** bei Citrix DaaS Standard für Azure beschrieben. Gleichzeitig-Lizenzen werden automatisch freigegeben, wenn Benutzer sich ab-

melden oder die Sitzung trennen. Weitere Informationen zu Zuweisung von Gleichzeitig-Lizenzen finden Sie unter Überwachen von Lizenzen und Verwendungsspitzen für Citrix DaaS (gleichzeitig).

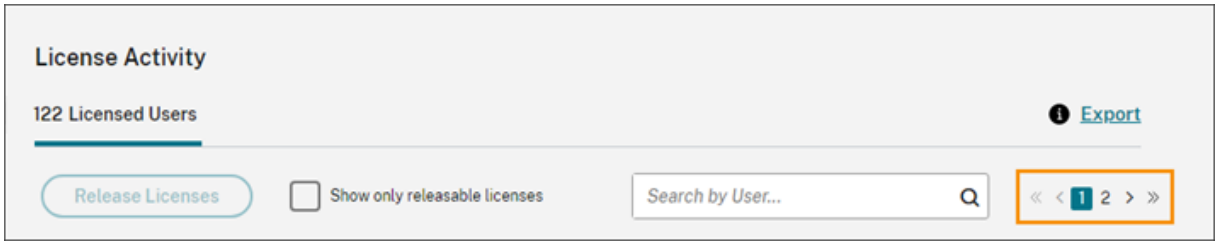
Nach dem Freigeben einer Lizenz erhöht sich die Anzahl der verfügbaren Lizenzen und die Anzahl der zugewiesenen Lizenzen nimmt entsprechend ab. Nach der Freigabe ihrer Lizenz können Benutzer eine neue Lizenz erhalten, indem sie sich anmelden und den Cloudservice verwenden.

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.

Finden geeigneter Lizenzen

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.

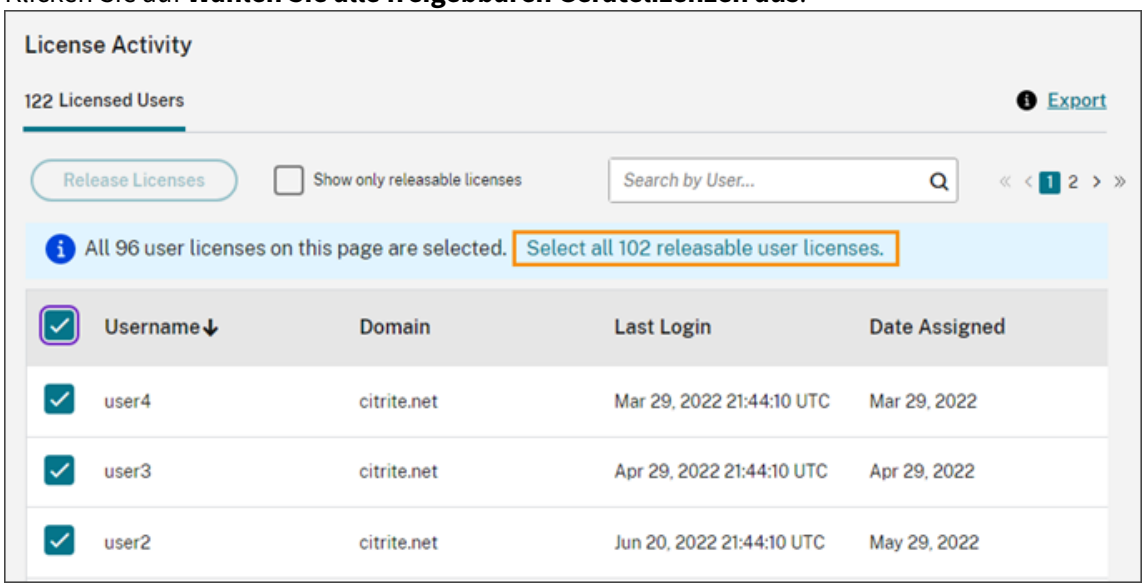
Auswählen geeigneter Lizenzen

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.

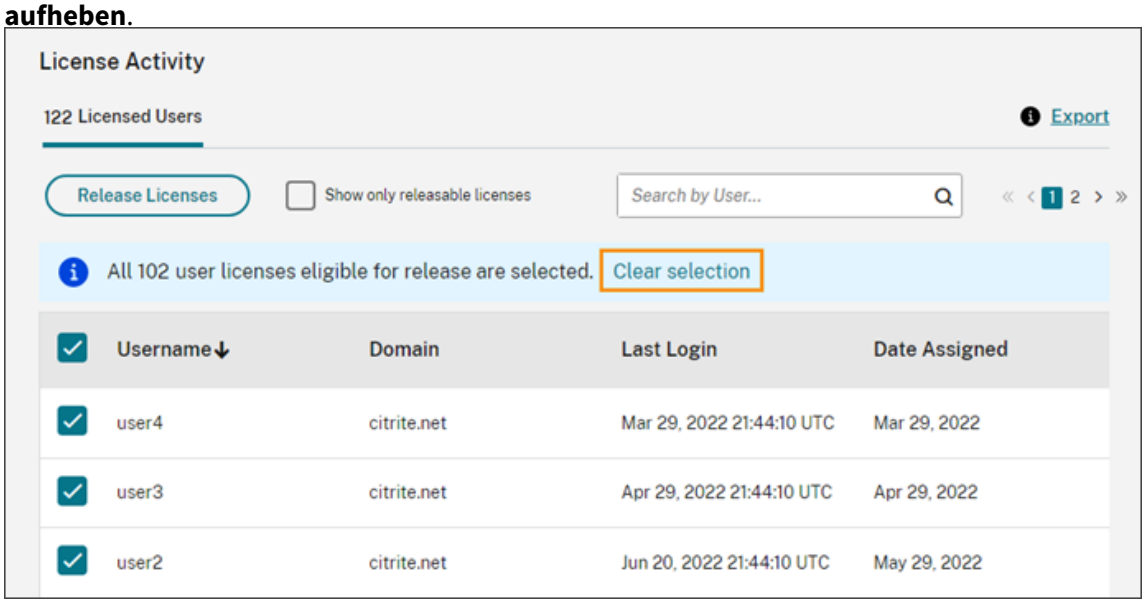
Sie können auch alle geeigneten Lizenzen in einem einzigen Vorgang auswählen. Wenn Sie nicht mehr als 100 berechtigte Lizenzen haben, aktivieren Sie einfach das Kontrollkästchen neben Benutzername in der Kopfzeile der Liste, um alle geeigneten Lizenzen auszuwählen.

Wenn Sie mehr als 100 berechtigte Lizenzen haben:

1. Aktivieren Sie das Kontrollkästchen neben **Benutzername** in der Kopfzeile der Liste, um alle geeigneten Lizenzen auszuwählen, die auf der Seite angezeigt werden.
2. Klicken Sie auf **Wählen Sie alle freigebbaren Gerätelizenzen aus**.



3. Um die Auswahl aller Lizenzen auf allen Seiten der Liste aufzuheben, klicken Sie auf **Auswahl aufheben**.



Freigeben zugewiesener Lizenzen

1. Wählen Sie bei Bedarf **Nur freigebbare Lizenzen anzeigen**, um nur die Benutzer mit Lizenzen anzuzeigen, die für die Freigabe in Frage kommen.
2. Wählen Sie die Benutzer aus, die Sie verwalten möchten, und wählen Sie dann **Lizenzen freigeben**.
3. Überprüfen Sie die ausgewählten Benutzer und wählen Sie **Lizenzen freigeben**.

Überwachen von Lizenzen und aktiver Nutzung für Endpoint Management

May 13, 2022

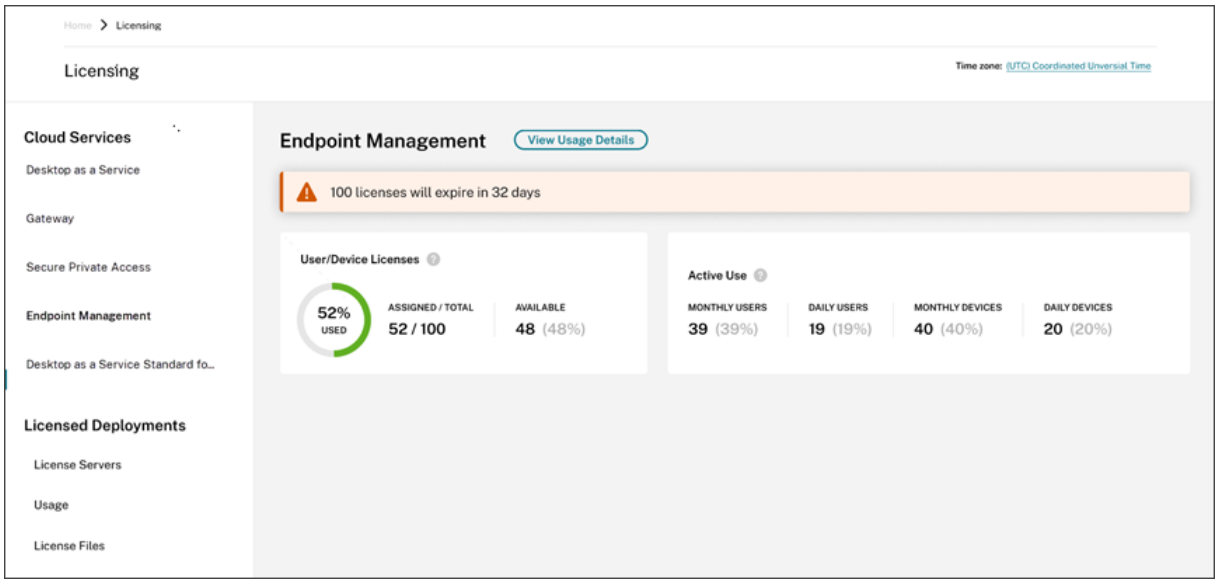
Lizenzzuweisung

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

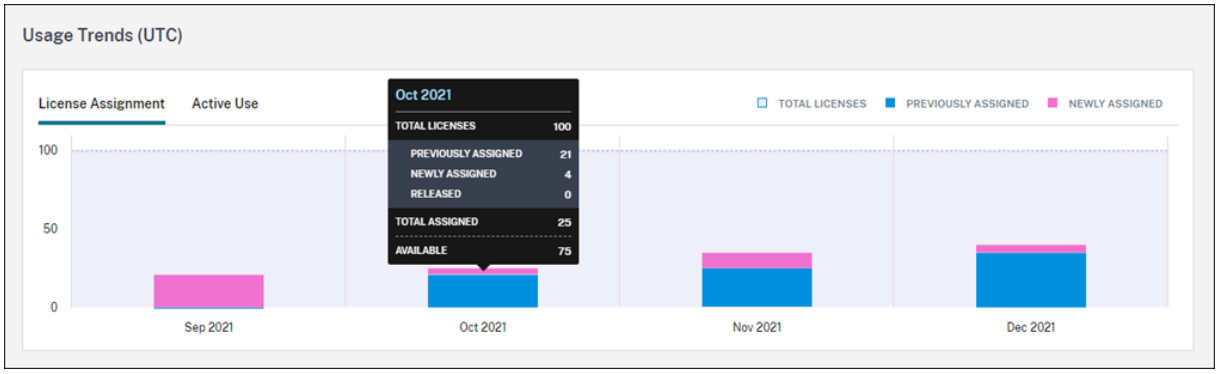


Die Zusammenfassung unter “Lizenzierung” bietet für jeden unterstützten Service einen Überblick über Folgendes:

- 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.

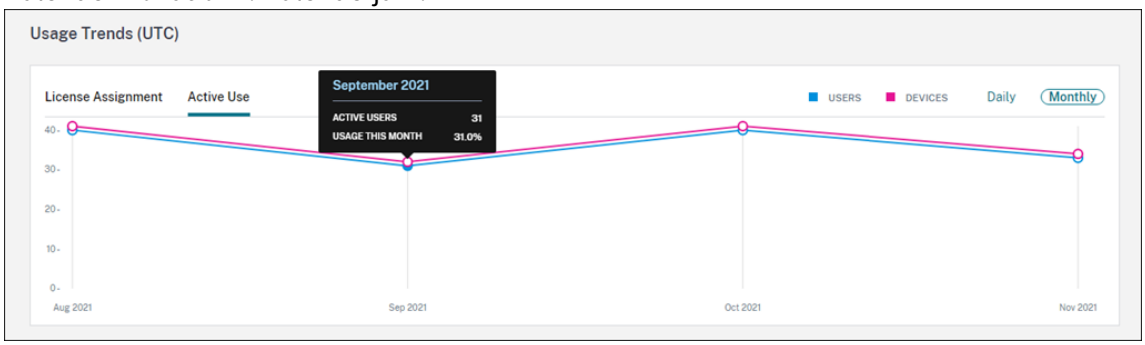
Nutzungstrends

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:

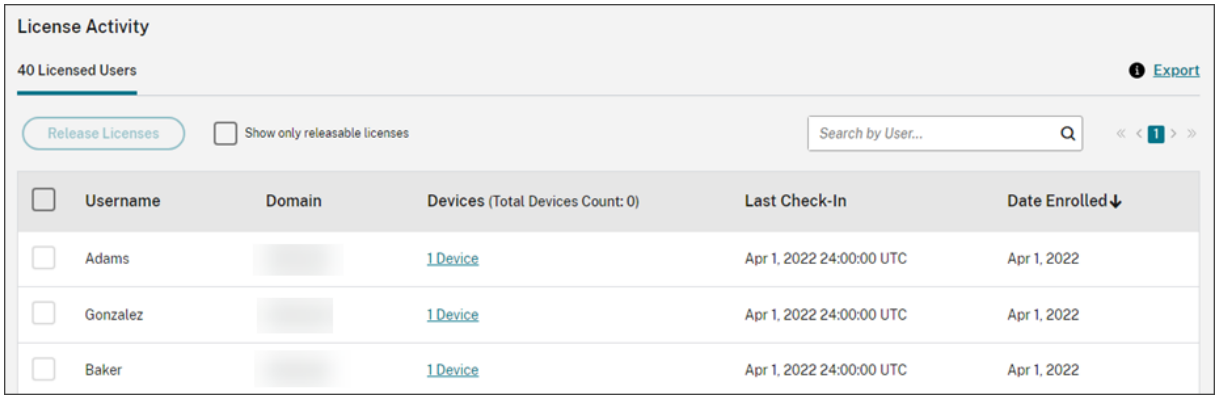
- **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.
- **Zuvor zugewiesen:** Die Cloudservicelizenzen, die bereits zu Beginn eines jeden Monats zugewiesen waren. Wenn einem Benutzer beispielsweise im Juli eine Lizenz zugewiesen wird, wird diese Zuweisung unter “Zuvor 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 Einchecken für jeden Benutzer

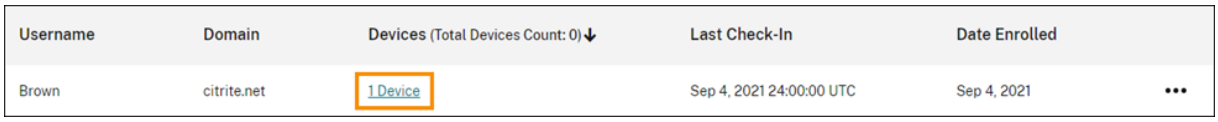


An dieser Liste können Sie die folgenden Aufgaben ausführen:

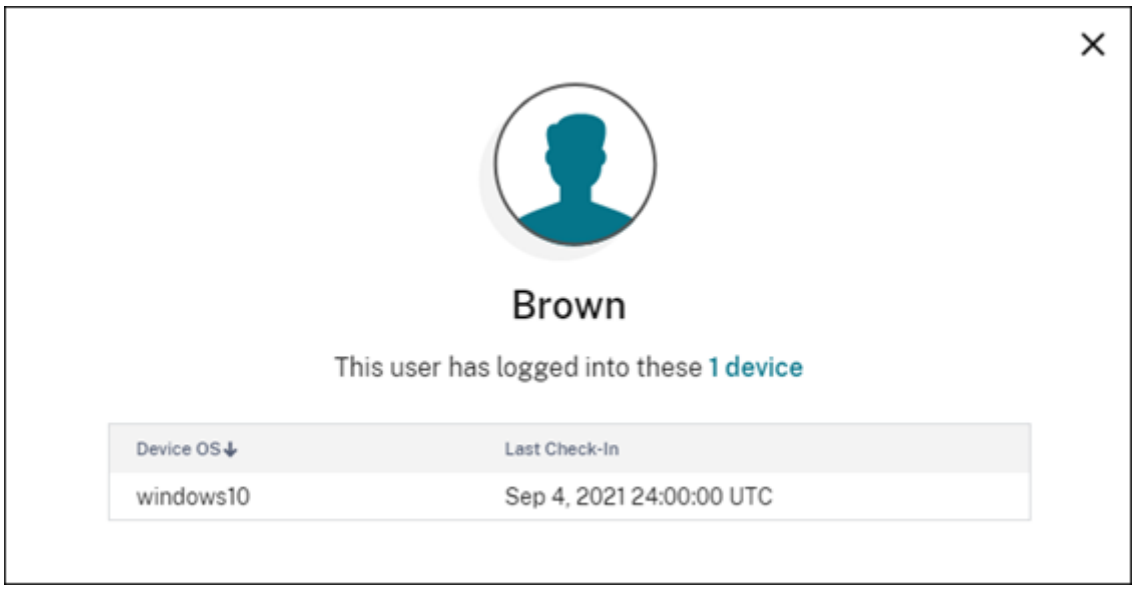
- Anzeigen der registrierten Geräte für einen bestimmten Benutzer
- Filtern der Liste der Benutzer, sodass nur freigebbare Lizenzen angezeigt werden
- Freigeben zugewiesener Lizenzen, die in den letzten 30 Tagen nicht verwendet wurden

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.

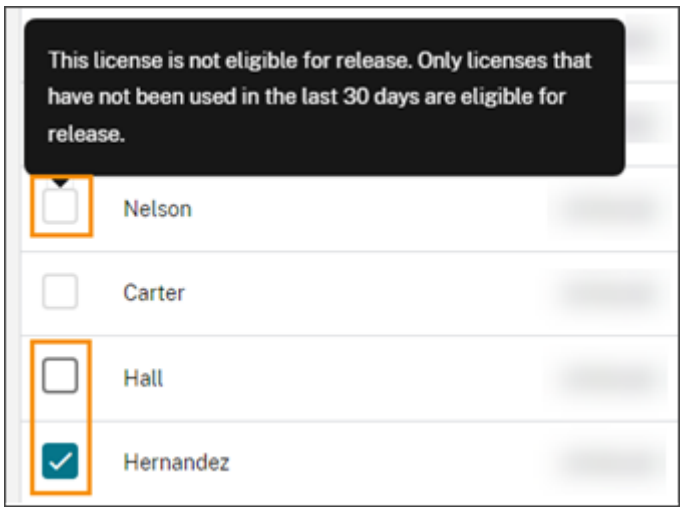


Freigeben zugewiesener Lizenzen

Sie können Lizenzen für Benutzer freigeben, 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.

Lizenzen, die freigegeben werden können, haben ein dunkelgraues Kontrollkästchen, das Sie auswählen können. Das Kontrollkästchen ist hellgrau und inaktiv bei Lizenzen, die noch nicht freigegeben werden können.

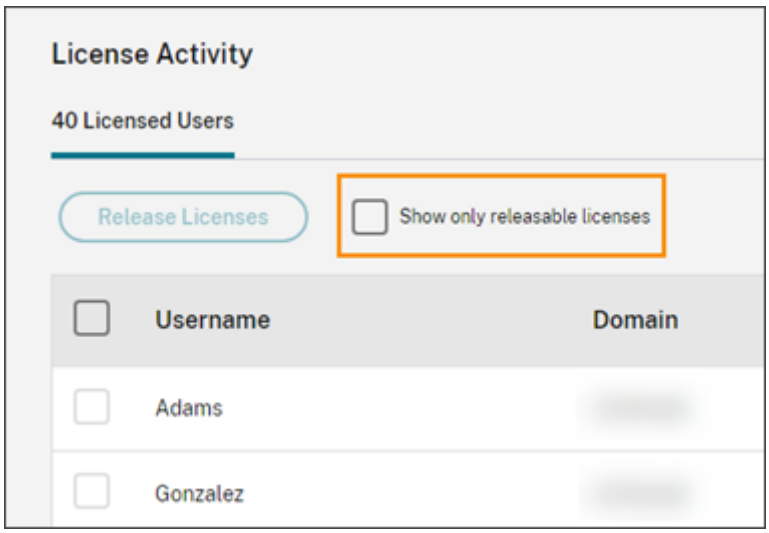


Nach der Freigabe einer Lizenz kann der Benutzer eine neue erhalten, indem er ein Gerät registriert.

Finden geeigneter Lizenzen

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.



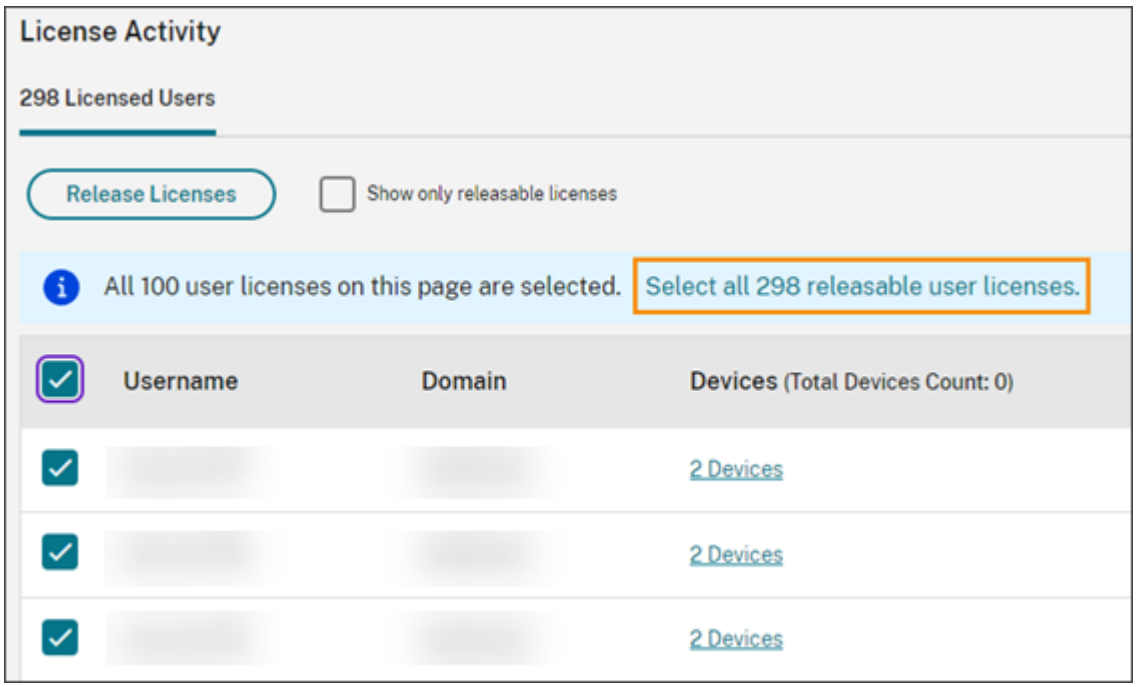
Auswählen geeigneter Lizenzen

Aktivieren Sie das dunkelgraue Kontrollkästchen neben jeder Lizenz, um diese für die Freigabe auszuwählen. Wenn Sie Lizenzen aus der Liste auswählen, wird die Schaltfläche **Lizenzen freigeben** aktiv.

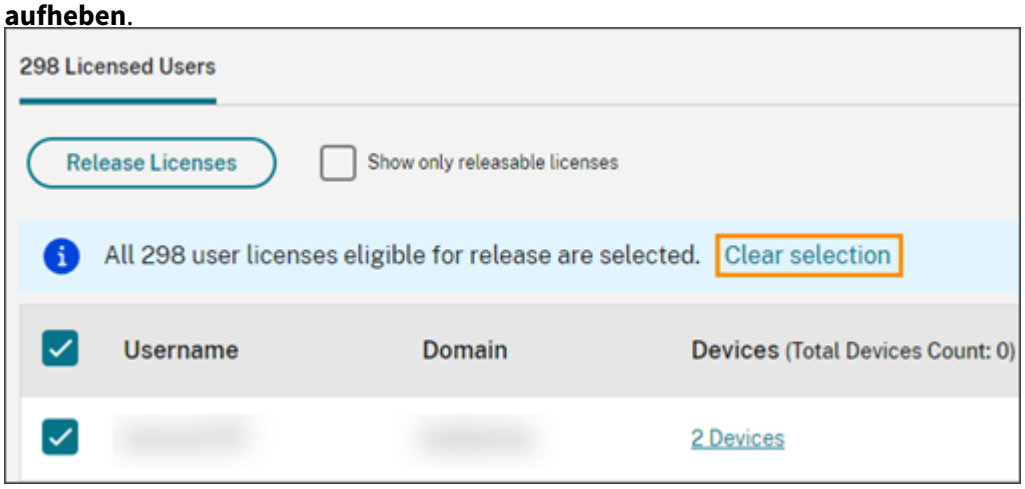
Sie können auch alle geeigneten Lizenzen in einem einzigen Vorgang auswählen. Wenn Sie nicht mehr als 100 berechtigte Lizenzen haben, aktivieren Sie einfach das Kontrollkästchen neben **Benutzername** in der Kopfzeile der Liste, um alle geeigneten Lizenzen auszuwählen.

Wenn Sie mehr als 100 berechtigte Lizenzen haben:

1. Aktivieren Sie das Kontrollkästchen neben **Benutzername** in der Kopfzeile der Liste, um alle geeigneten Lizenzen auszuwählen, die auf der Seite angezeigt werden.
2. Klicken Sie auf **Wählen Sie alle freigebbaren Gerätelizenzen aus**.



3. Um die Auswahl aller Lizenzen auf allen Seiten der Liste aufzuheben, klicken Sie auf **Auswahl aufheben**.



Freigeben geeigneter Lizenzen

1. Wählen Sie bei Bedarf **Nur freigebbare Lizenzen anzeigen**, um nur die Benutzer mit Lizenzen anzuzeigen, die für die Freigabe in Frage kommen.
2. Wählen Sie die Lizenzen aus, die Sie freigeben möchten.
3. Wählen Sie **Lizenzen freigeben** aus.
4. Überprüfen Sie die ausgewählten Lizenzen und wählen Sie **Lizenzen freigeben**.

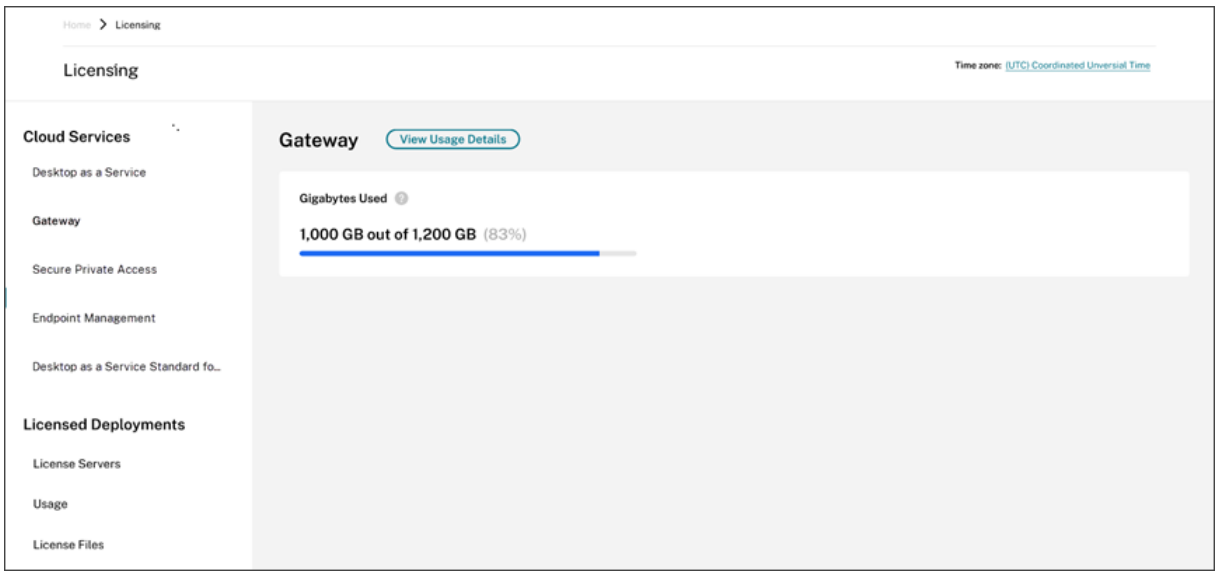
Überwachen der Bandbreitennutzung für Gateway Service

May 13, 2022

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.

Zusammenfassung zur Lizenzierung



Die Zusammenfassung der Lizenzierung für Gateway Service bietet einen Überblick über die folgenden Informationen:

- Die Menge der genutzten Bandbreite aus der Gesamtbandbreite für alle Abonnements.
- Die Zeitspanne bis zum Ablauf des Cloudserviceabonnements. Wenn das Abonnement innerhalb der nächsten 90 Tage abläuft, wird eine Warnmeldung angezeigt.

Genutzte Lizenzen und Bandbreite

Jeder Gateway Service-Benutzer hat Zugriff auf 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 3 Jahre kaufen, erhalten Sie 3600 GB Gesamtbandbreite (1200 GB pro Jahr). Die Bandbreite wird für den Zeitraum von 3 Jahren auf alle lizenzierten Benutzer verteilt. Wenn Sie zusätzliche Abonnements erwerben, zeigt Citrix Cloud die Gesamtzahl der Lizenzen und Bandbreite für alle Abonnements an.

Für Testversionen von Gateway Service werden 50 GB Bandbreite für den 60-tägigen Testzeitraum und 25 Benutzer gebündelt.

Restliche Bandbreite

Während des Abonnementzeitraums nicht genutzte Bandbreite wird bei Verlängerung in Citrix Cloud nicht übertragen.

Bandbreite für mehrere Abonnements

Bei mehreren Abonnements mit überlappenden Fristen zeigt Citrix Cloud nur die Bandbreite an, die dem nicht abgelaufenen Abonnement zugeordnet ist.

Nehmen wir zum Beispiel an, Sie haben zwei Abonnements erworben. Citrix Cloud zeigt die Gesamtlizenzen und die Gesamtbandbreite für beide Abonnements an. Nach Ablauf eines Abonnements zeigt Citrix Cloud nur die Bandbreite für das nicht abgelaufene Abonnement an. Wenn das letzte Abonnement abläuft, zeigt Citrix Cloud die Menge der genutzten Bandbreite und eine gesamte Bandbreite von Null an. Diese Anzeige bleibt während des unter Verlängern von Citrix Cloud-Serviceabonnements beschriebenen Service-Kulanzzeitraums und des Aufbewahrungszeitraums für Daten bestehen.

Nutzungstrends

Klicken Sie für eine detaillierte Ansicht Ihrer Lizenzen auf **Nutzungsdetails anzeigen**.

Im Abschnitt **Nutzungstrends** wird auf der Registerkarte **Verwendete Gigabytes** die Menge der verbrauchten Bandbreite angezeigt. Die Menge der genutzten Bandbreite ist nach Zugriffsmethode aufgeschlüsselt:

- VAD-Dienst: Bandbreite, die für extern verbundene Citrix DaaS-Benutzer verwendet wird.
- Siteaggregation: Bandbreite, die zum Starten von On-premises-Apps und -Desktops über Workspace mit Siteaggregation verwendet wird.

> **Hinweis:**
>
> Nutzungstrends werden kumulativ für die Dauer der aktuellen Abonnementlaufzeit dargestellt.

Lizenzaktivität

Im Abschnitt **Lizenzaktivität** werden folgende Informationen angezeigt:

- Liste der einzelnen Benutzer, denen Lizenzen zugewiesen sind.
- Die Domäne, zu der der Benutzer gehört.
- Die Menge der genutzten Bandbreite in GB.
- Das Datum, an dem der Benutzer zuletzt einen Dienst verwendete, der Bandbreitennutzung erforderte.

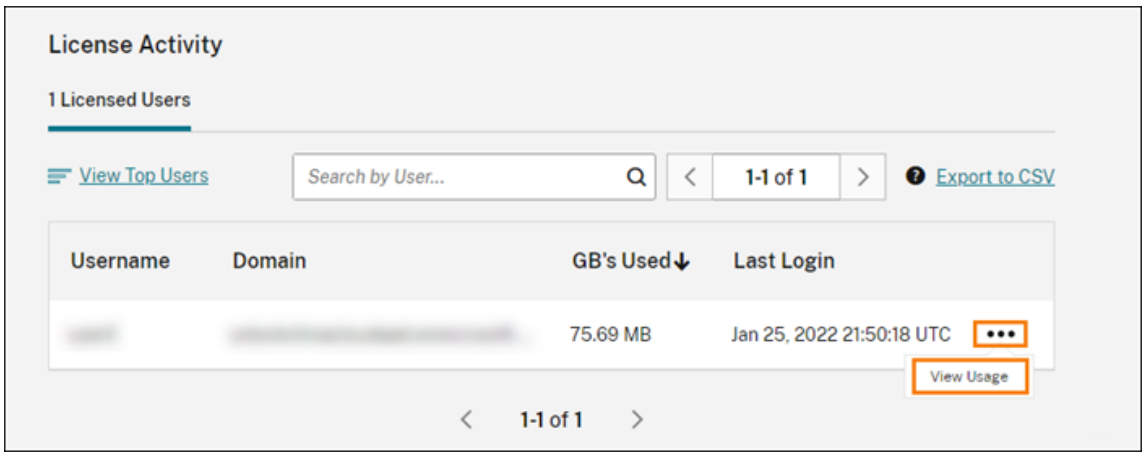
Nutzungsdetails für Benutzer anzeigen

Sie können die Bandbreitennutzung der letzten 30 Tage anzeigen für:

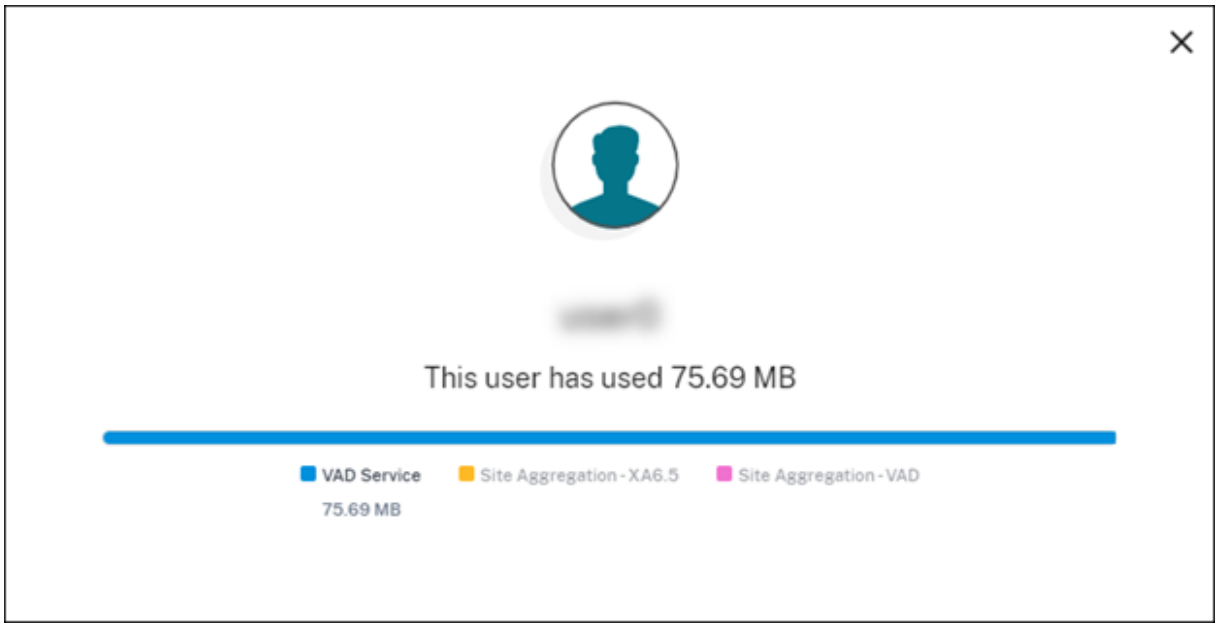
- Einen bestimmten Benutzer, der in der Liste “Lizenzaktivität” angezeigt wird.
- Die Top 10 Benutzer mit der höchsten Bandbreitennutzung.

So zeigen Sie Nutzungsdetails für einen bestimmten Benutzer an:

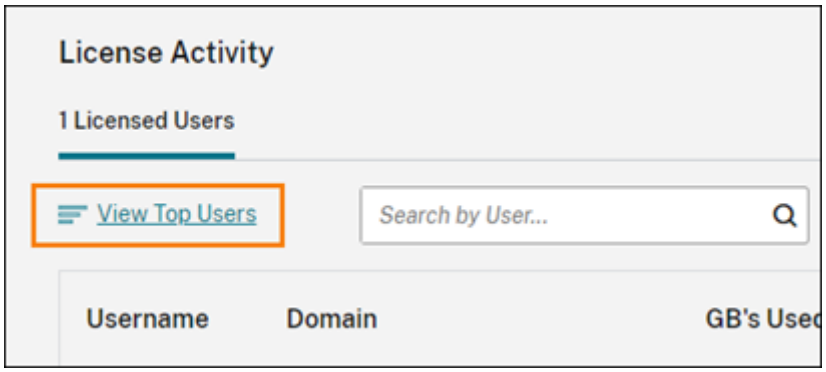
1. Suchen Sie unter **Lizenzaktivität** einen Benutzer in der Liste, den Sie anzeigen möchten.
2. Klicken Sie auf die drei Punkte (…) ganz rechts auf der Seite und wählen Sie im Menü die Option **Nutzung anzeigen** aus.



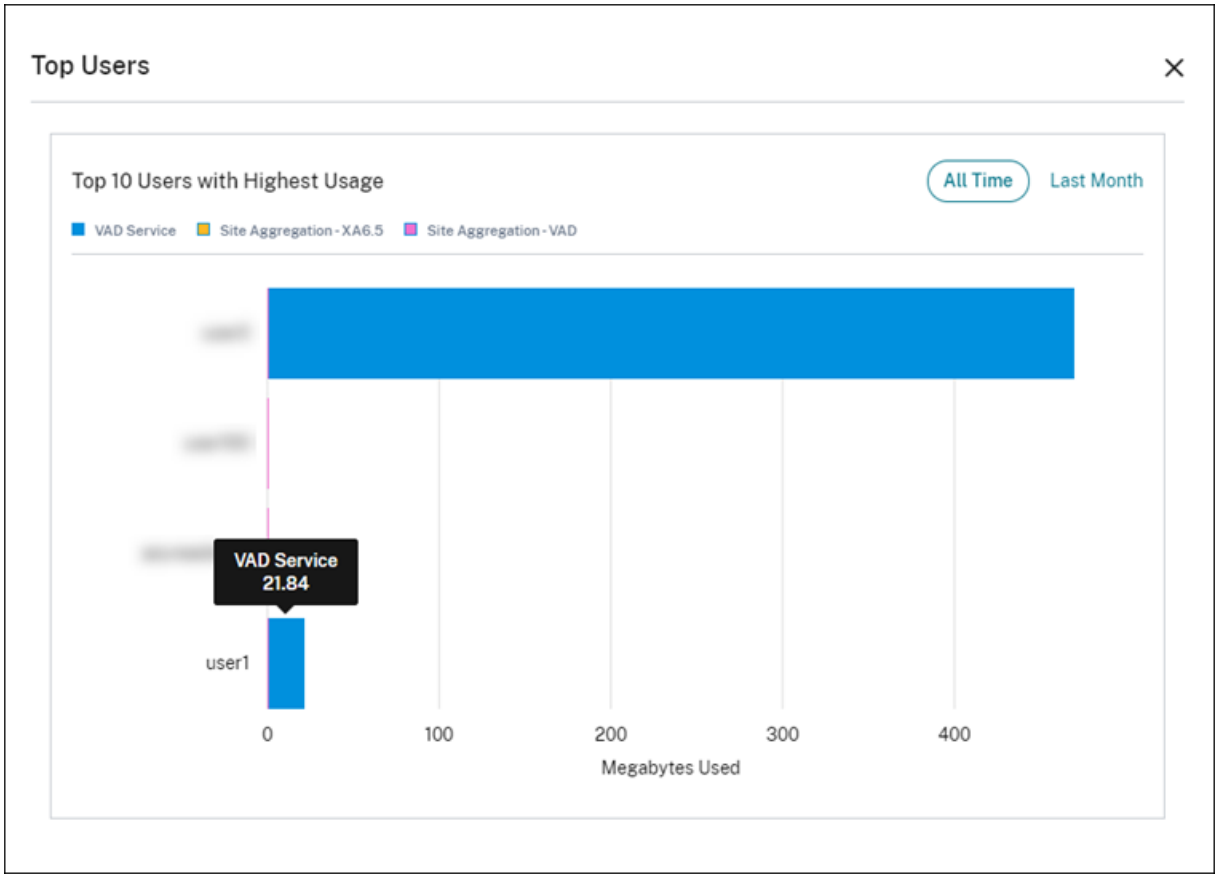
Citrix Cloud zeigt die Bandbreite des Benutzers aufgeschlüsselt nach Zugriff an.



Um Nutzungsdetails für die 10 Top-Benutzer anzuzeigen, wählen Sie **Top-Benutzer anzeigen** aus.



Citrix Cloud zeigt ein Diagramm der Bandbreitennutzung für die Top-Benutzer an.



Citrix Cloud zeigt die Bandbreitennutzung der letzten 30 Tage für Benutzer auch dann an, wenn deren Lizenz freigegeben wurde. Wenn ein Gateway Service-Abonnement abläuft, zeigt Citrix Cloud weiterhin die Bandbreite an, die einzelne Benutzer im Zeitraum von 30 Tagen verbraucht haben.

Überwachen von Lizenzen und Nutzung für Secure Private Access

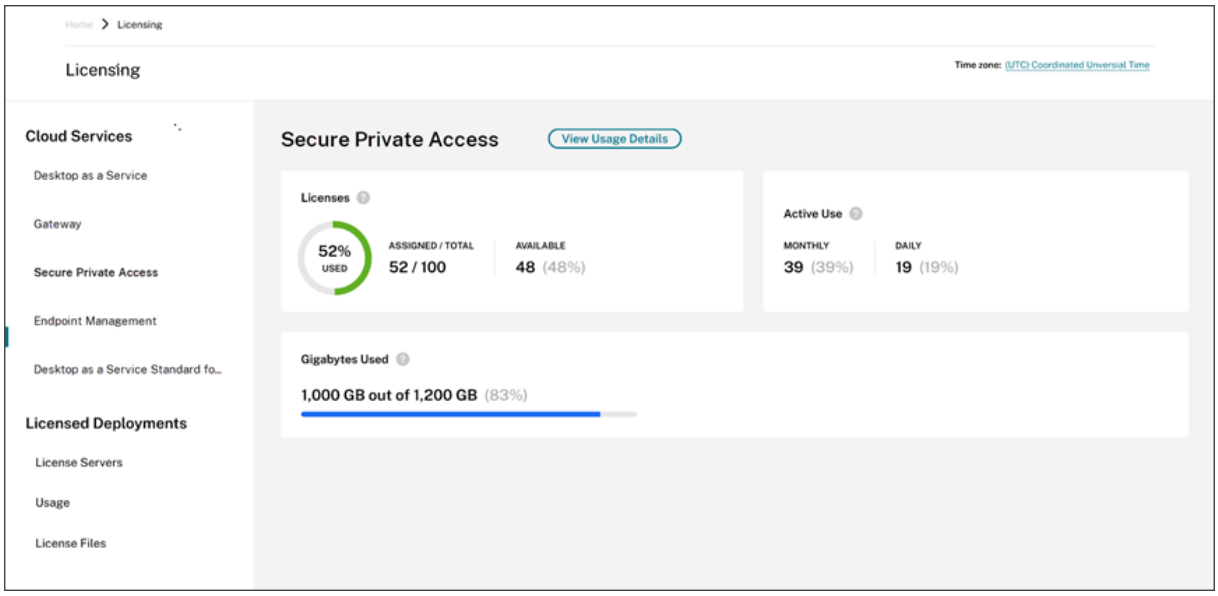
May 25, 2022

> **Hinweis:**
>
> Die Lizenzierung für Secure Private Access (zuvor “Secure Workspace Access”) ist ein Preview-Feature. Preview-Features stehen Ihnen zu Test- und Evaluierungszwecken in Umgebungen zur Verfügung, die nicht oder nur eingeschränkt zur Produktion verwendet werden. Sie sind nicht für den Einsatz in Produktionsumgebungen vorgesehen.

Lizenzzuweisung

Eine Lizenz wird zugewiesen, wenn ein eindeutiger Benutzer zum ersten Mal eine SaaS- oder Web-App startet.

Zusammenfassung zur Lizenzierung



Die Zusammenfassung der Lizenzierung bietet einen Überblick über 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

Für Secure Private Access Advanced-Abonnements hat jeder Benutzer 5 GB Bandbreite pro Monat (60 GB pro Benutzer und Jahr). Für 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

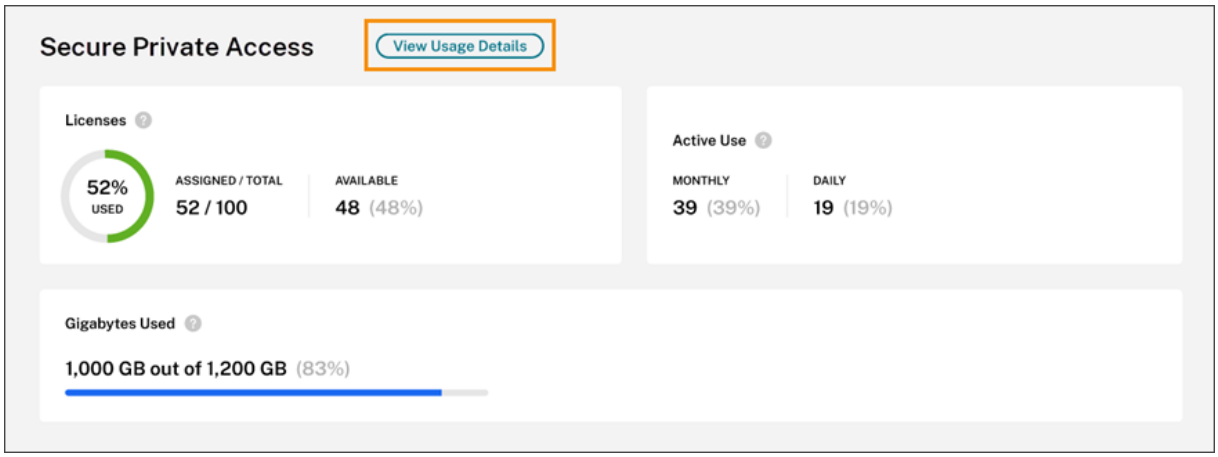
Abonnements erwerben, zeigt Citrix Cloud die Gesamtzahl der Lizenzen und Bandbreite für alle Abonnements an.

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.

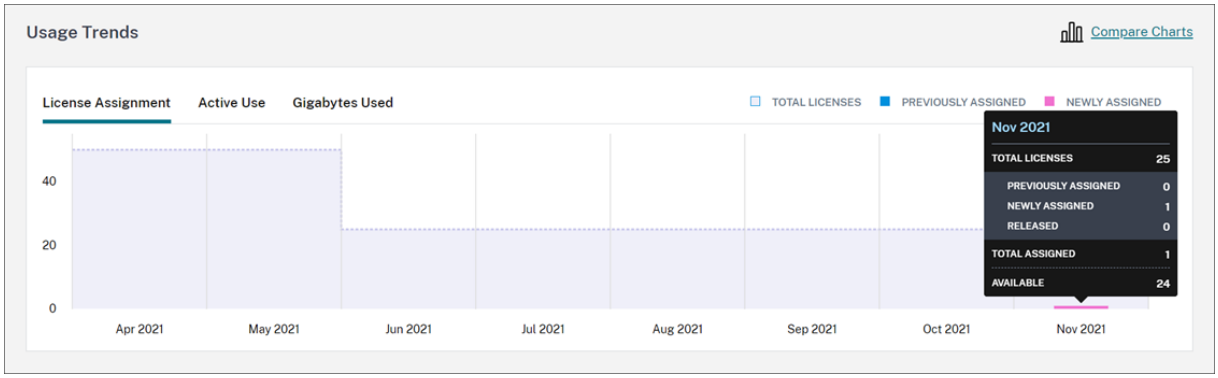
Bei mehreren Abonnements mit überlappenden Fristen wird die einem Abonnement zugeordnete Bandbreite aus der Lizenzierung entfernt, wenn dieses abläuft. Wenn Sie beispielsweise zwei Abonnements erwerben, zeigt Citrix Cloud die Gesamtlizenzen und die Gesamtbandbreite für beide Abonnements an. Wenn das erste Abonnement abläuft, zeigt Citrix Cloud nur die Bandbreite an, die mit dem nicht abgelaufenen Abonnement verknüpft ist.

Nutzungstrends und Lizenzaktivität

Klicken Sie für eine detaillierte Ansicht Ihrer Lizenzen auf **Nutzungsdetails anzeigen**.



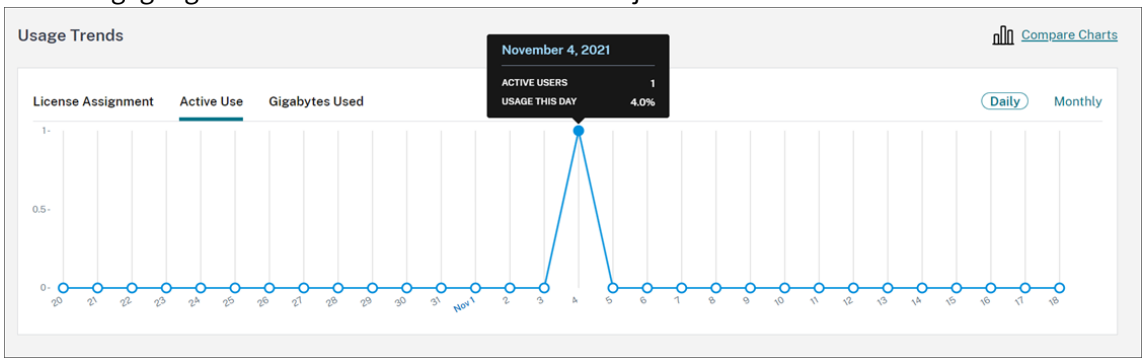
Sie sehen dann eine Aufschlüsselung der Nutzungstrends sowie einzelne Benutzer, die Cloudservicelizenzen und Bandbreite verwenden.



Diese Aufschlüsselung unter **Nutzungstrends** zeigt Ihnen folgende Informationen:

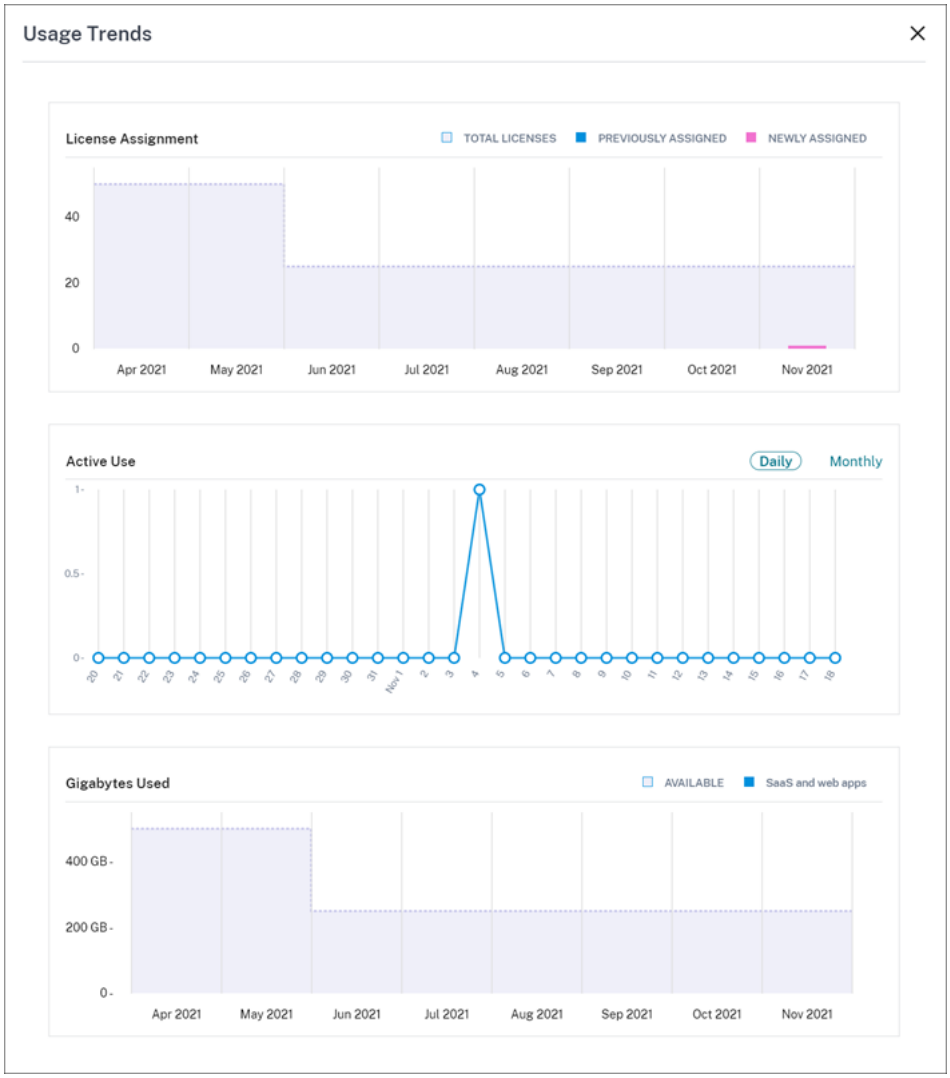
- Auf der Registerkarte **Lizenzzuweisung**:

  - **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 greift ein Benutzer im Juli das erste Mal auf den Cloudservice zu und ihm wird 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.



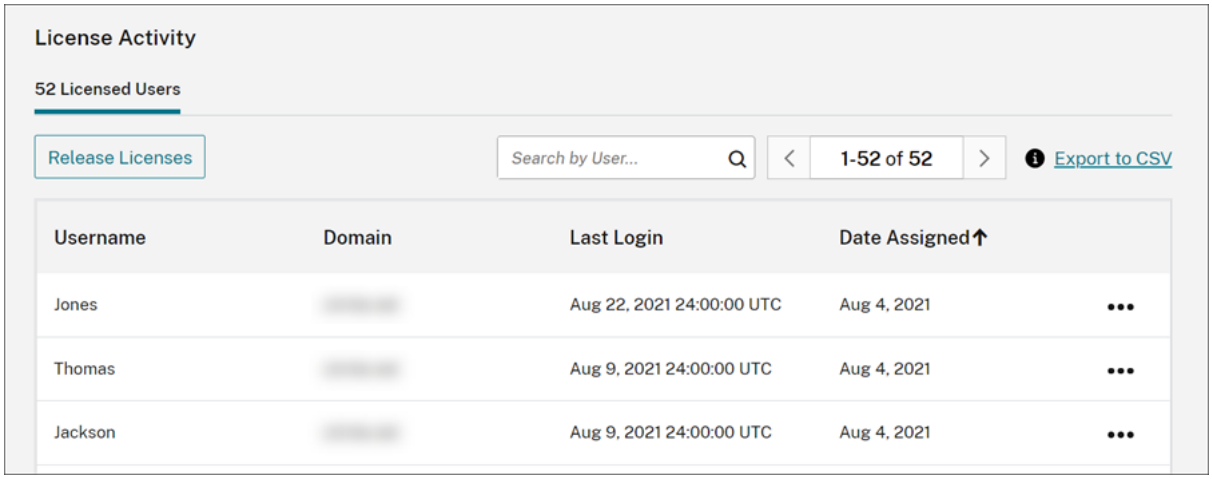
- Auf der Registerkarte **Verwendete Gigabytes**: Die Menge der genutzten Bandbreite aus der gesamten verfügbaren Bandbreite.

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.

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.

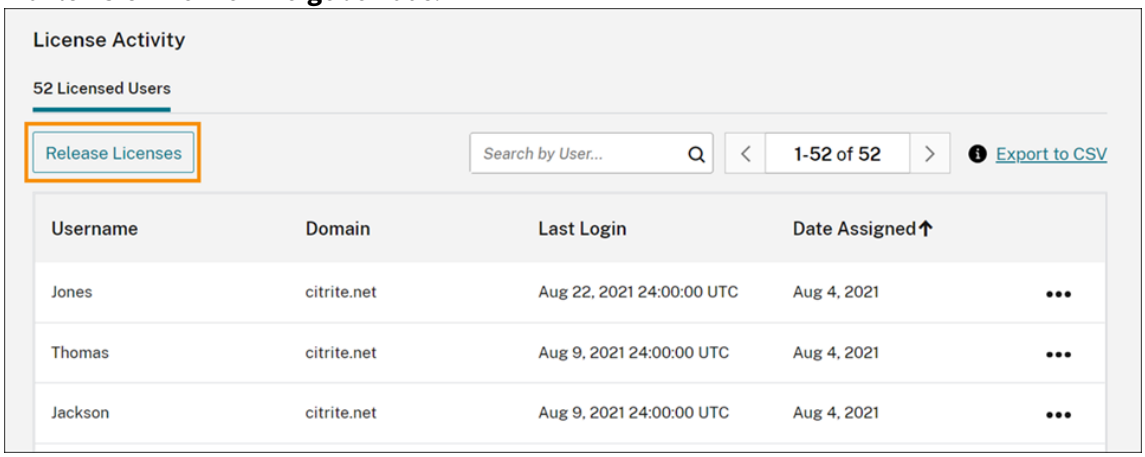
Freigeben zugewiesener Lizenzen

Sie können Lizenzen für Benutzer freigeben, die den Dienst in den letzten 30 Tagen nicht genutzt haben. Mehrere Lizenzen können Sie einzeln oder per Massenaktion freigeben.

Nach dem Freigeben einer Lizenz erhöht sich die Anzahl der verfügbaren Lizenzen und die Anzahl der zugewiesenen Lizenzen nimmt entsprechend ab. Nach der Freigabe ihrer Lizenz können Benutzer eine neue Lizenz erhalten, indem sie sich anmelden und den Cloudservice verwenden.

Freigeben mehrerer zugewiesener Lizenzen

1. Wählen Sie **Lizenzen freigeben** aus.



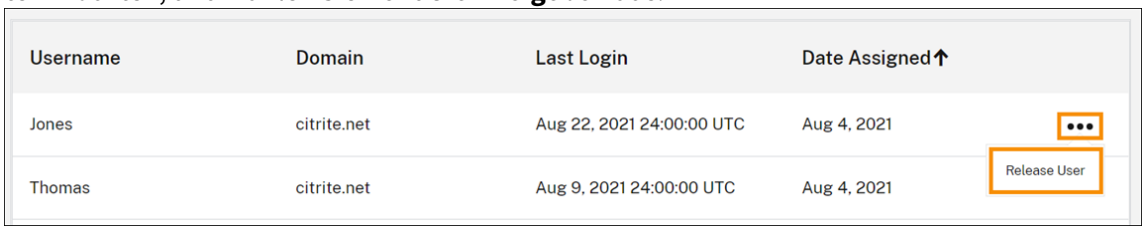
2. Wählen Sie in der Liste die gewünschten Benutzer aus und klicken Sie auf **Weiter**.

3. Überprüfen Sie die ausgewählten Lizenzen und wählen Sie **Freigeben** aus.

Freigeben einer einzelnen zugewiesenen Lizenz

Sie können einzelne Lizenzen über die Liste Lizenzierte Benutzer oder Lizenzierte Geräte freigeben. In diesen Listen werden nur für Benutzer bzw. Geräte mit Lizenzen, die freigegeben werden können, klickbare Auslassungspunkte angezeigt. Die Auslassungpunkte sind für Benutzer und Geräte inaktiv, die in den letzten 30 Tagen keine Apps oder Desktops gestartet haben.

1. Klicken Sie unter **Lizenzaktivität** auf die Auslassungspunkte für den Benutzer, den Sie verwalten möchten, und wählen Sie **Benutzer freigeben** aus.



2. Überprüfen Sie Ihre Auswahl und klicken Sie auf **Weiter**.
3. Wenn Sie aufgefordert werden, die Freigabe zu bestätigen, klicken Sie auf **Freigeben**.

Überwachen des Citrix Managed Azure-Ressourcenverbrauchs für Citrix DaaS

August 31, 2022

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.

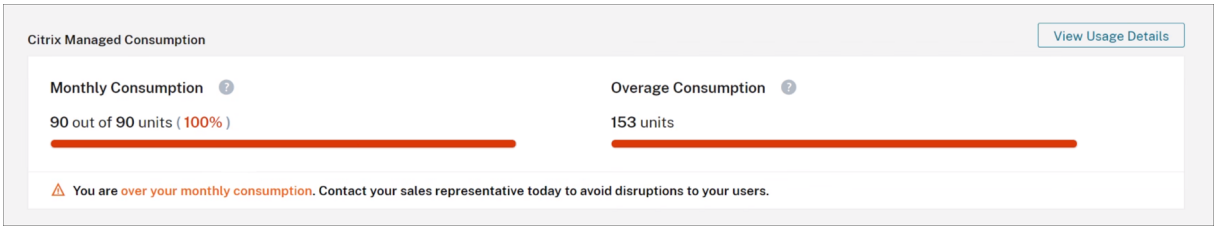
Unterstützte Produkte

Die Verbrauchsüberwachung ist für die folgenden Editionen von Virtual Apps and Desktops Service 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.

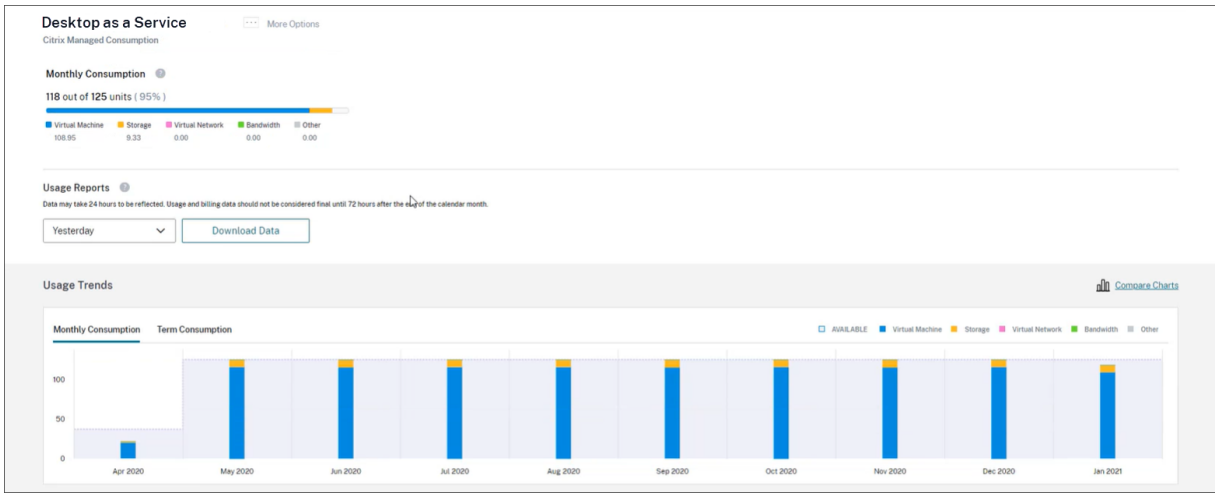
Wenn Sie den Verbrauch auf Monats- oder Jahresbasis im Voraus bezahlt haben, zeigt Citrix Cloud die Anzahl der monatlichen Verbrauchseinheiten oder der Verbrauchseinheiten für die Laufzeit an, die Sie für den aktuellen Monat oder das aktuelle Jahr verwendet haben. Wenn Sie mehr Einheiten verbrauchen, 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

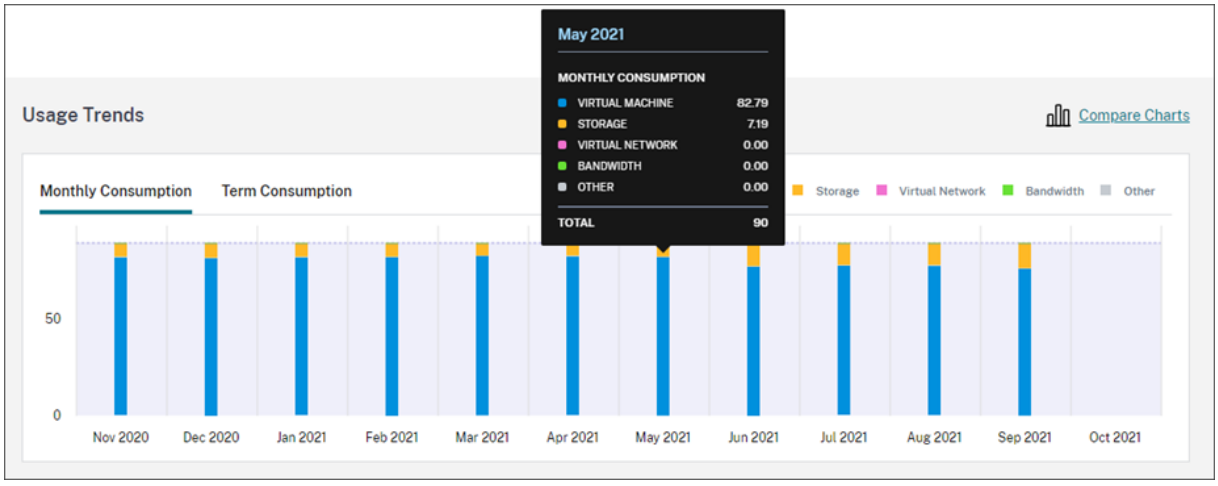
- Gemessene Nutzung von Azure-VMs, Netzwerkverbindungen, Azure-Speicher und Bandbreite für jeden Tag des Berichtdatumsbereichs.

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

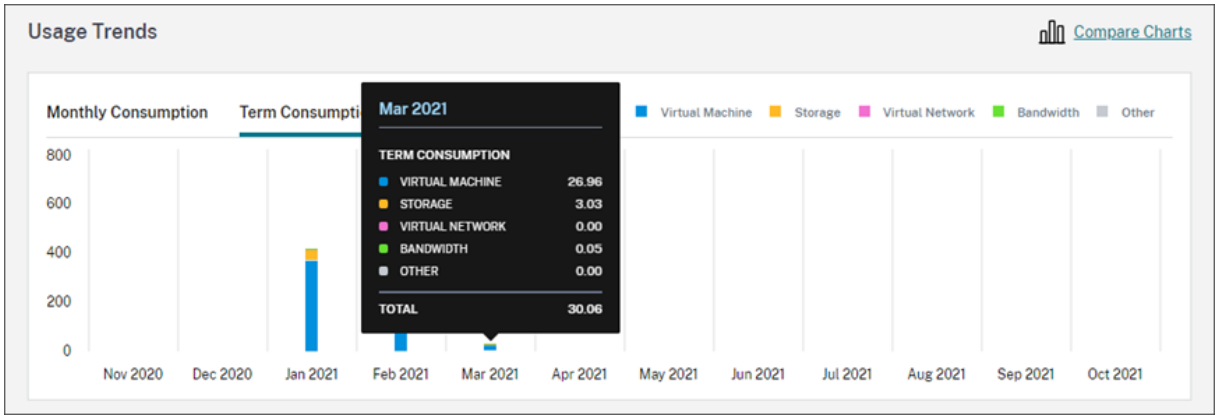
Nutzungstrends und Verbrauchsaktivität

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.

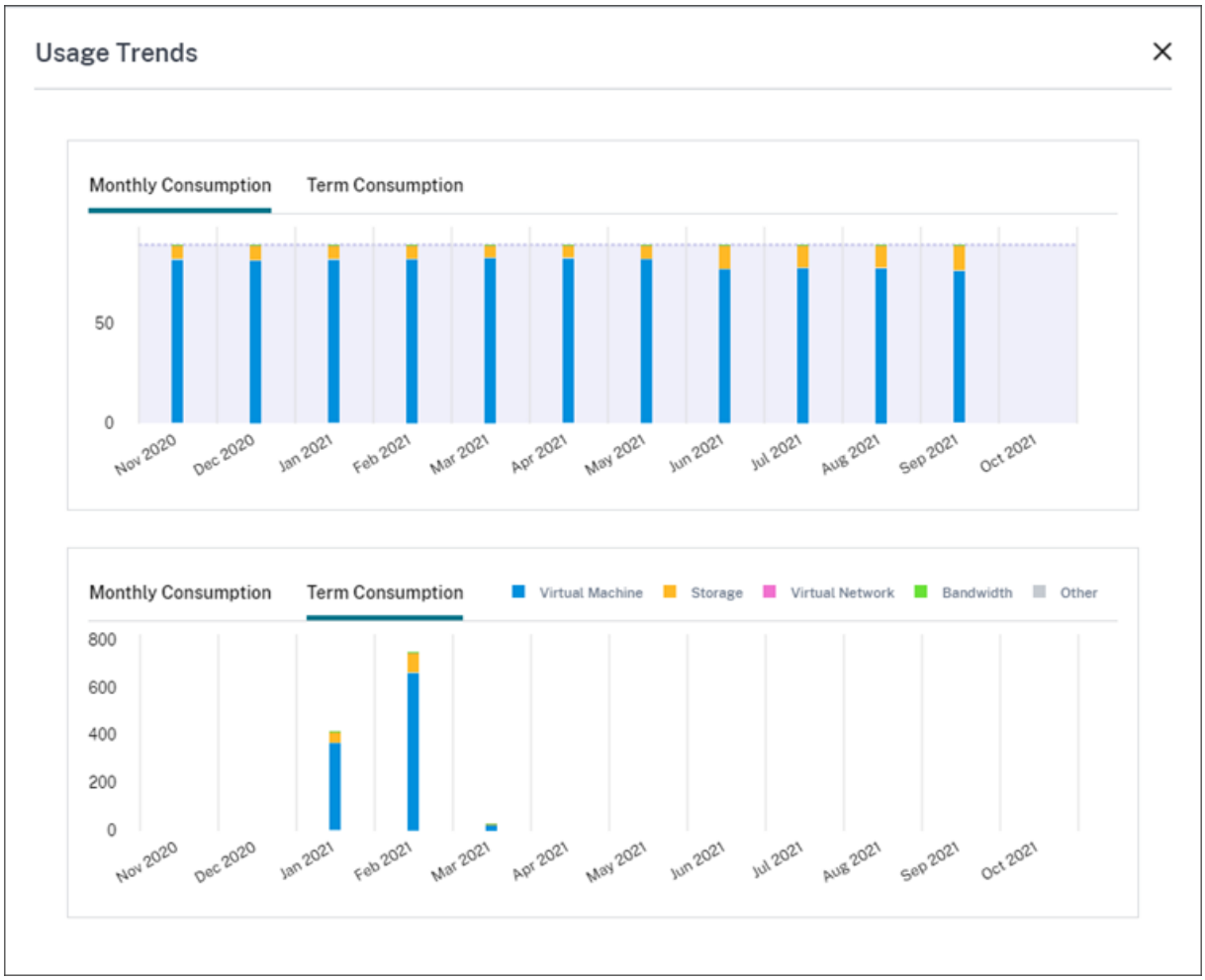
Wählen Sie **Monatlicher Verbrauch** aus, um Ihren monatlichen Verbrauch für die letzten 12 Monate anzuzeigen.



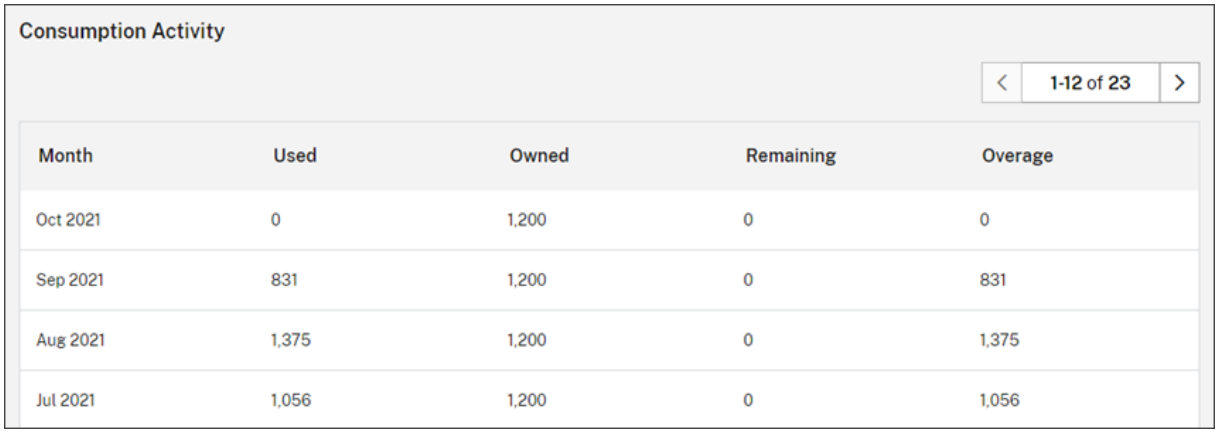
Wählen Sie **Laufzeitverbrauch** aus, um Ihren Laufzeitverbrauch für jeden Monat des Vorjahres anzuzeigen.



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.



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

July 11, 2022

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. Weitere Informationen zur Registrierung der Lizenzserver finden Sie unter Registrieren von On-Premises-Produkten bei Citrix Cloud.
- 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.

Voraussetzungen

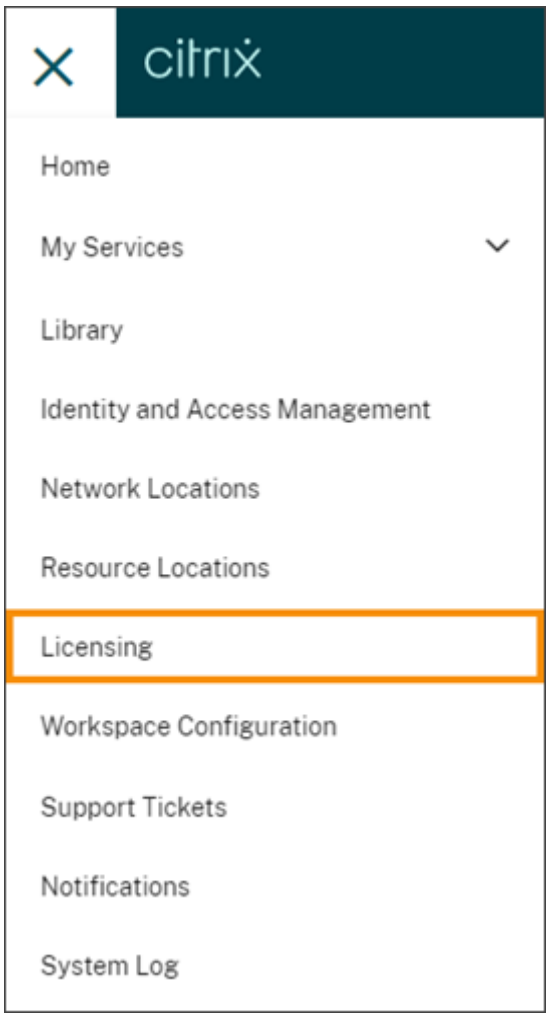
Zur Verwendung von Citrix Lizenzserver-Nutzungsstatistiken benötigen Sie die Folgendes:

- Einen Citrix Lizenzserver ab Version 11.15.0.0
- Ein Citrix Cloud-Konto
- Netzwerkzugriff von Citrix Lizenzserver auf Citrix Cloud

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**.



Anzeige der on-premises genutzten Produktlizenzen

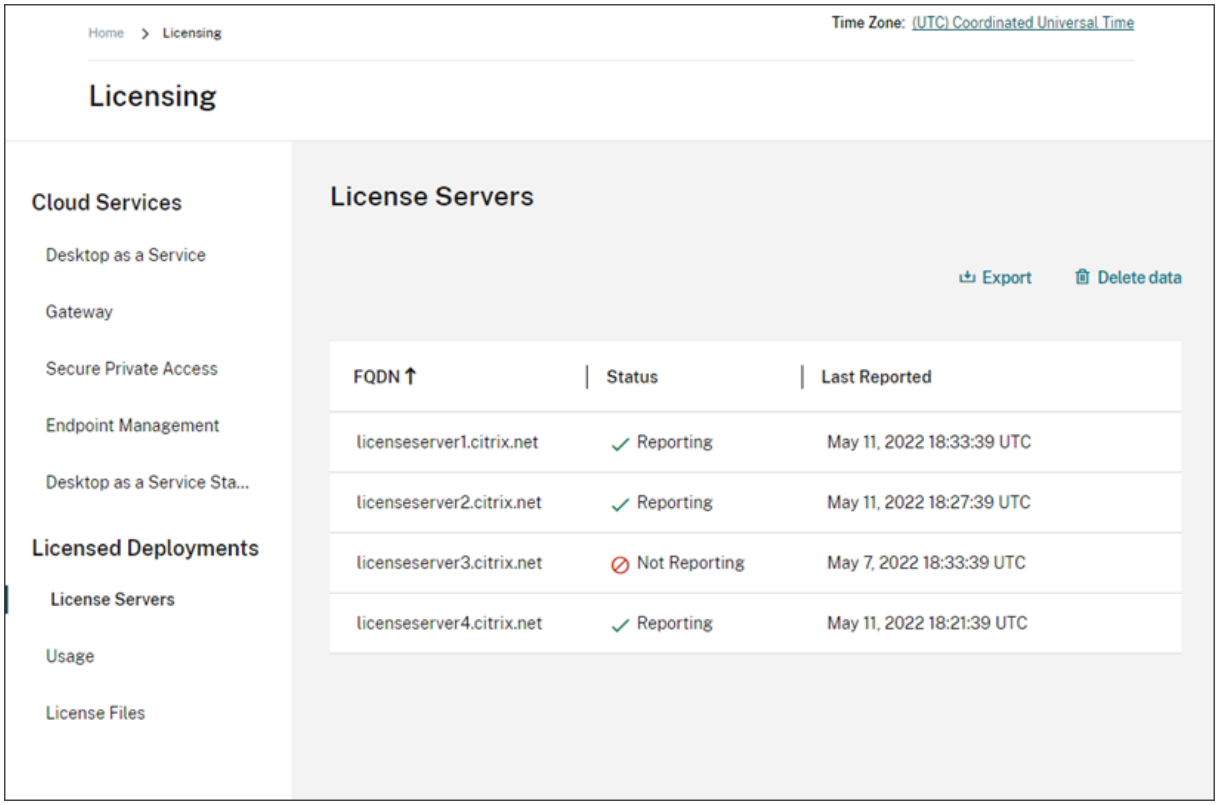
Citrix Lizenzserver-Nutzungsstatistiken geben Einblick in die Lizenznutzung Ihres gesamten Citrix-Bestands. Nach dem Aktivieren der Nutzungsstatistiken für Ihre Lizenzserver und dem Registrieren der Server bei Citrix Cloud können Sie auf folgende Nutzungsberichte zugreifen:

- 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

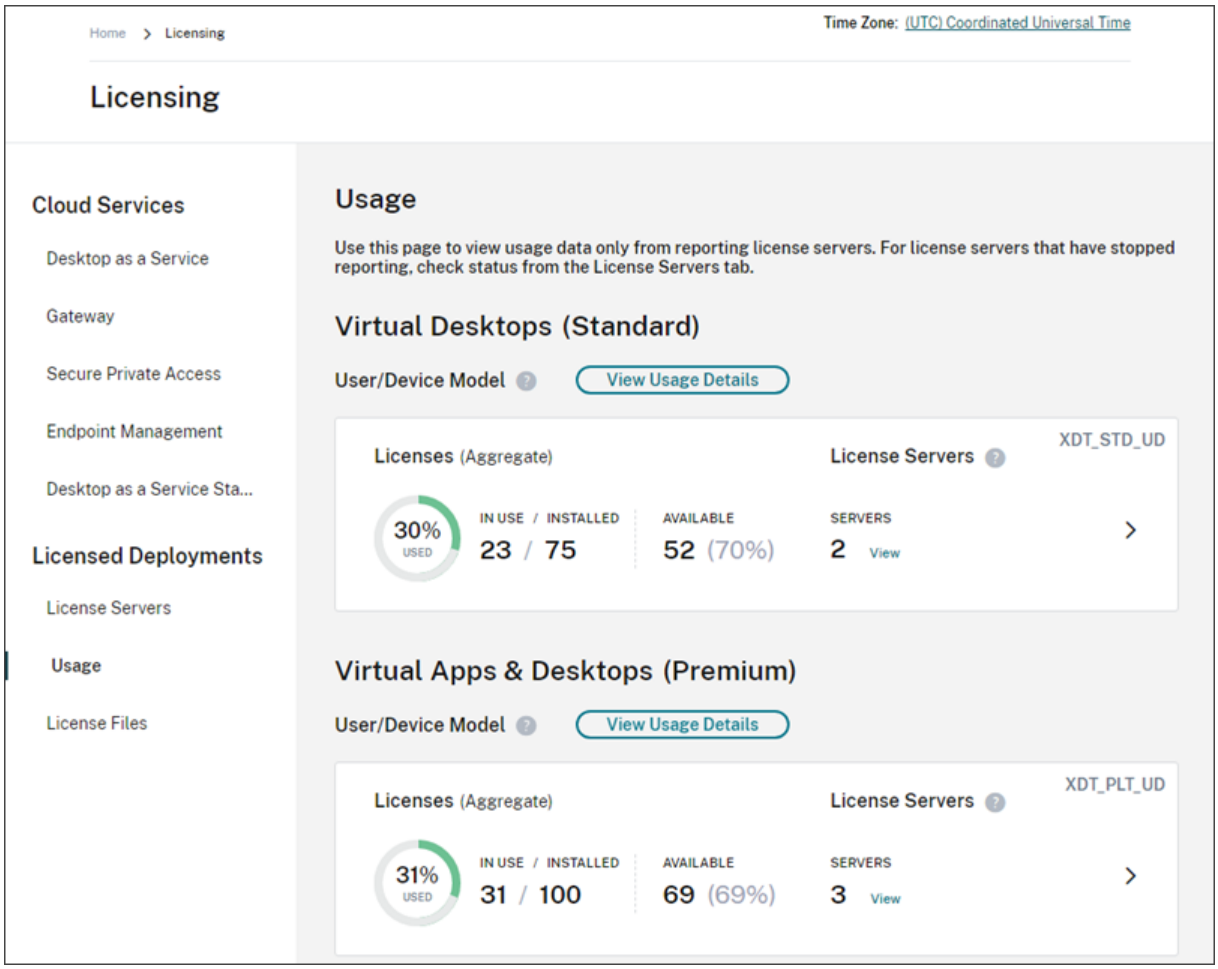
Berichterstellungsstatus und Datum des letzten Berichts legen fest, ob die Nutzungsdaten eines Lizenzservers in Berichte und Nutzungsstatistiken einfließen.

- 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.

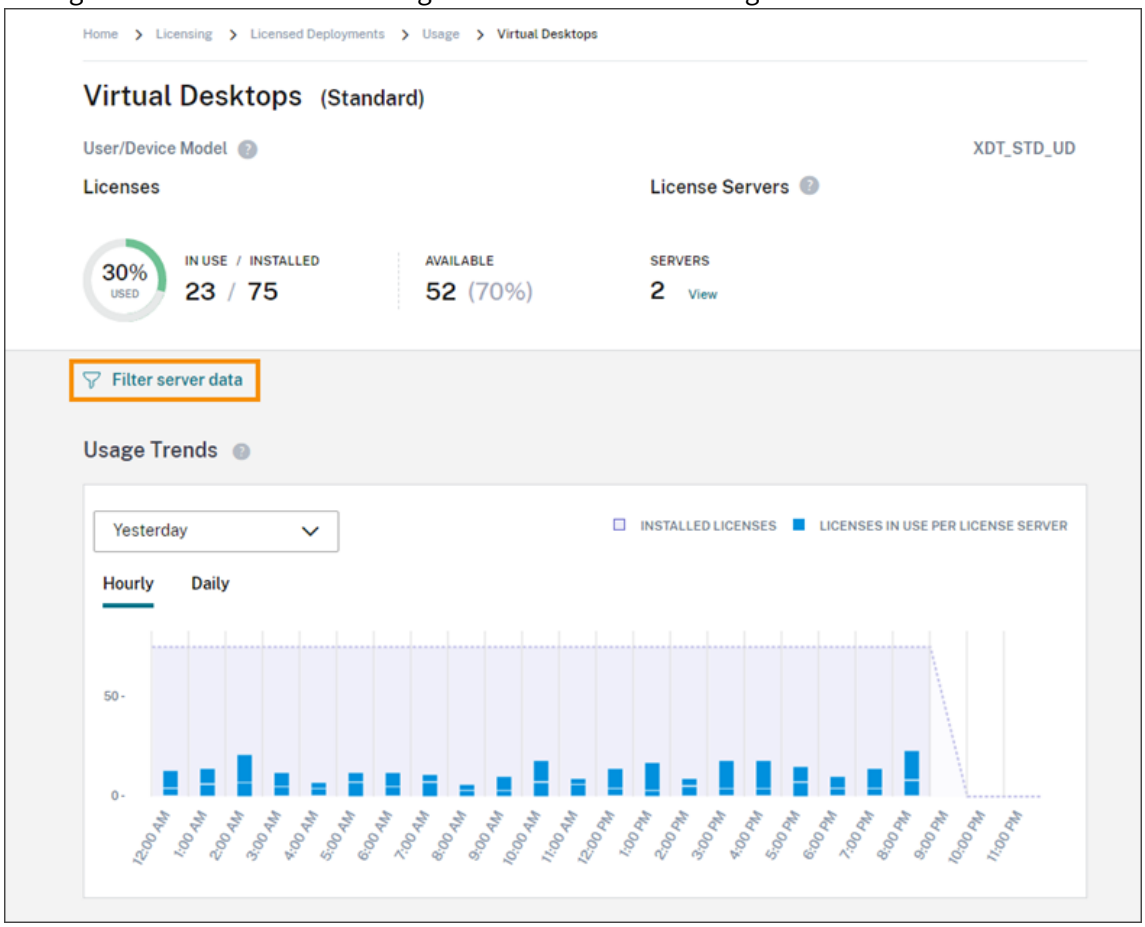


Die Lizenznutzung wird für mehrere Lizenzserver organisiert und zusammengefasst und nach Produktedition und Lizenzmodell unterteilt. Eine Übersichtskarte zur Lizenznutzung wird für jede Lizenzedition angezeigt, die auf den Lizenzservern mit aktivierter Berichtsfunktion gefunden wird. Eine Übersichtskarte 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.

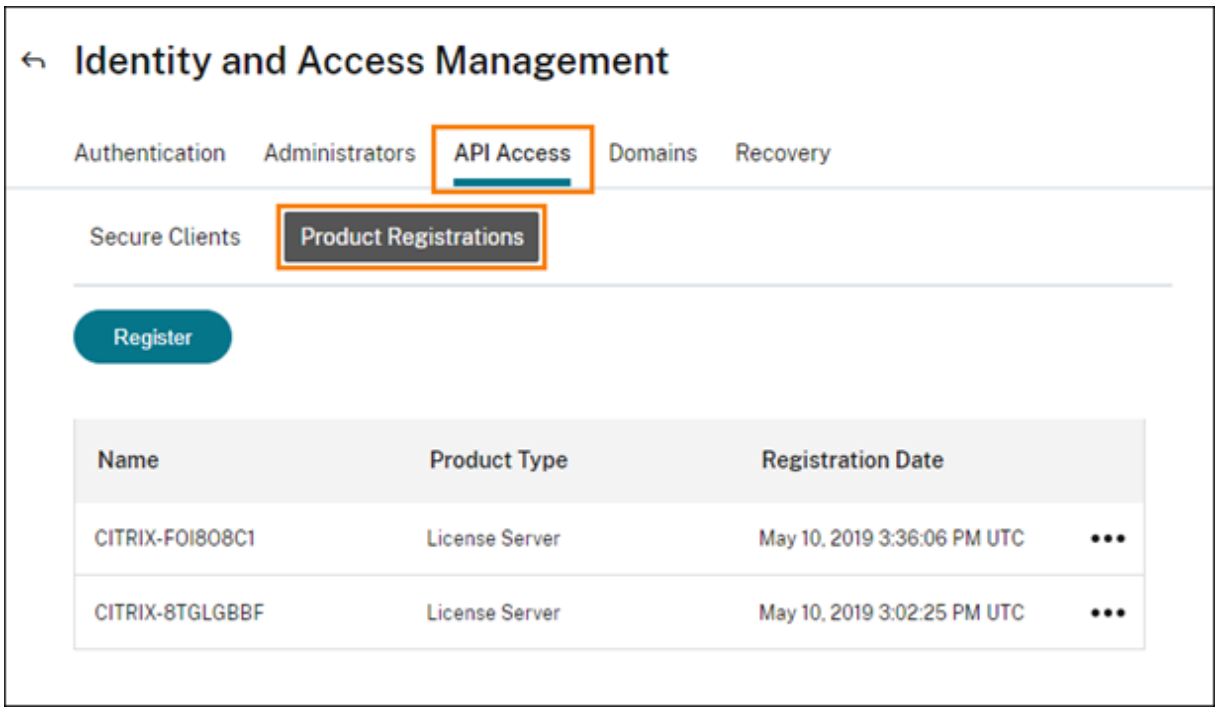
Registrieren von On-Premises-Produkten bei Citrix Cloud

April 29, 2022

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.



Unterstützte Produkte

Das Feature wird für die Verwendung mit Citrix Lizenzserver unterstützt.

Konnektivitätsanforderungen

Um Ihre On-Premises-Produkte erfolgreich zu registrieren, stellen Sie sicher, dass die folgenden Adressen kontaktiert werden können:

- `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`

Wenn Sie einen Proxyserver mit Citrix Lizenzserver verwenden, stellen Sie sicher, dass der Proxyserver wie im Abschnitt “Manuelles Konfigurieren eines Proxyservers” unter Schritt 3: Installieren Sie die .CRT- und .KEY-Dateien auf dem Lizenzserver in der Lizenzserverdokumentation beschrieben konfiguriert ist.

Registrieren des Lizenzservers

Führen Sie mit der Citrix Licensing Manager-Konsole die folgenden Aufgaben aus:

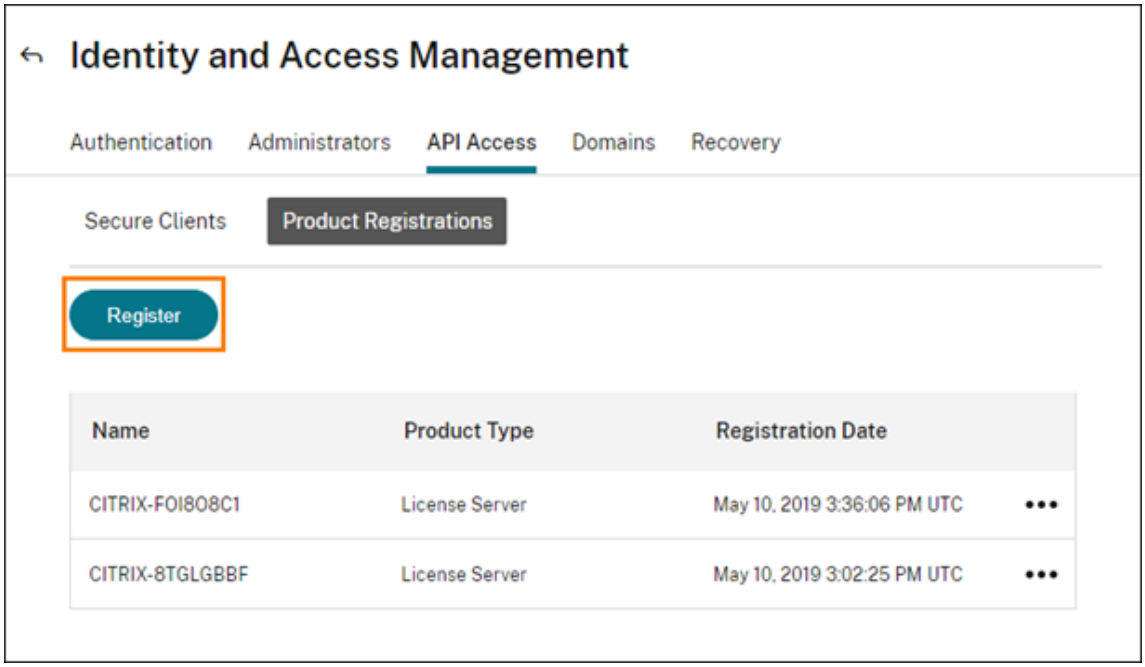
1. Zulassen der Freigabe der vom Lizenzserver über Call Home erfassten Nutzungsstatistik.
2. Registrieren des Lizenzservers bei Citrix Cloud.

Vollständige Anweisungen finden Sie unter Registrieren des Citrix Lizenzservers.

Weitere Informationen über die von Citrix erfassten Statistiken finden Sie unter Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) für die Citrix Lizenzierung, Call Home und Programme zur Compliance-Nutzung und Analyse.

Manuelles 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 8-stelligen Registrierungscode für Ihr Citrix Produkt ein und klicken Sie auf **Weiter**.
4. Überprüfen Sie die Registrierungsdetails und klicken Sie auf **Registrieren**.

Aufheben der Lizenzserverregistrierung

Zum Entfernen eines registrierten Lizenzservers aus Citrix Cloud ist die Citrix Licensing Manager-Konsole erforderlich. Vollständige Anweisungen finden Sie unter Registrieren des Citrix Lizenzservers.

Nach dem Aufheben der Registrierung sammelt Citrix Cloud keine Nutzungsdaten mehr von diesem Lizenzserver. Historische Daten bleiben jedoch gespeichert. Informationen zum Entfernen dieser Daten aus Citrix Cloud finden Sie unter Entfernen von Nutzungsdaten in diesem Artikel.

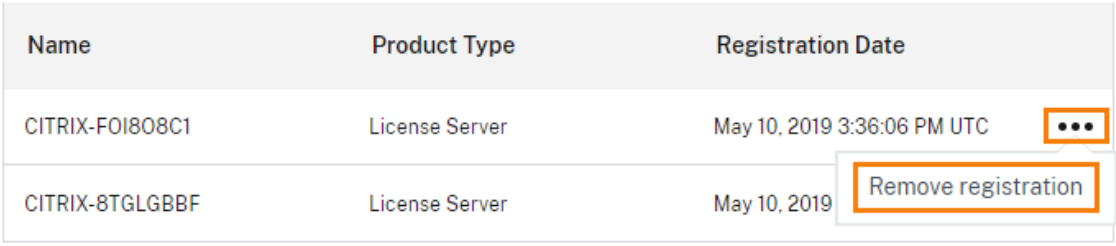
Stellen Sie sicher, dass der Lizenzserver nicht mehr in Citrix Cloud auf der Seite “Produktregistrierungen” angezeigt wird. Wenn der Lizenzserver weiterhin in der Liste angezeigt wird, entfernen Sie ihn (siehe Entfernen einer Produktregistrierung im vorliegenden Artikel).

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.

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

April 29, 2022

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, ADC 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:

- Überwachung von Kundenlizenzen und Lizenznutzung für Citrix DaaS
- Überwachung von Kundenlizenzen und Lizenznutzung für Citrix DaaS Standard für Azure

Erste Schritte mit License Usage Insights

April 29, 2022

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)
- Citrix ADC 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\SimpleLicenseServiceC
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 Pro-

duktnutzung, 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.

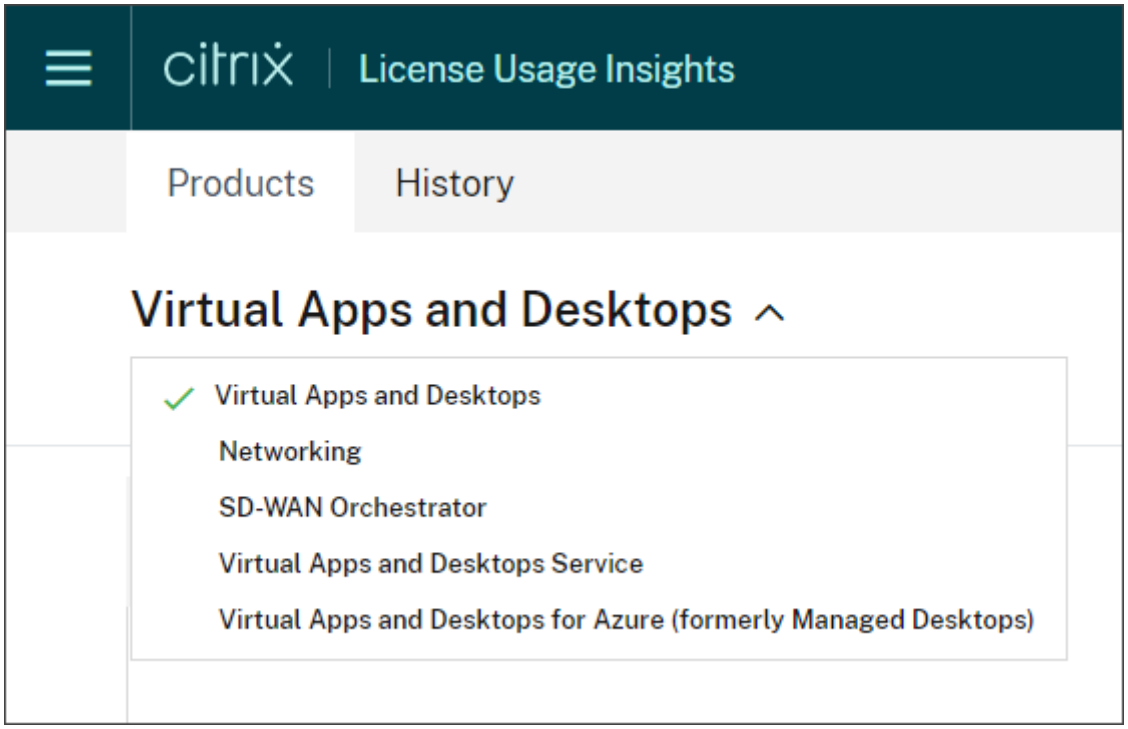
- **Steht License Usage Insights auch Citrix Kunden oder Partnern zur Verfügung, die keine Citrix Service Provider sind?** Nein. License Usage Insights steht nur für Citrix Service Provider mit laufendem Partnervertrag zur Verfügung.
- **Kann ich "Call Home" auf dem Lizenzserver deaktivieren?** Nein. 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.

Verwalten von Produktnutzung, Lizenzservern und Benachrichtigungen

September 15, 2021

Produktauswahl

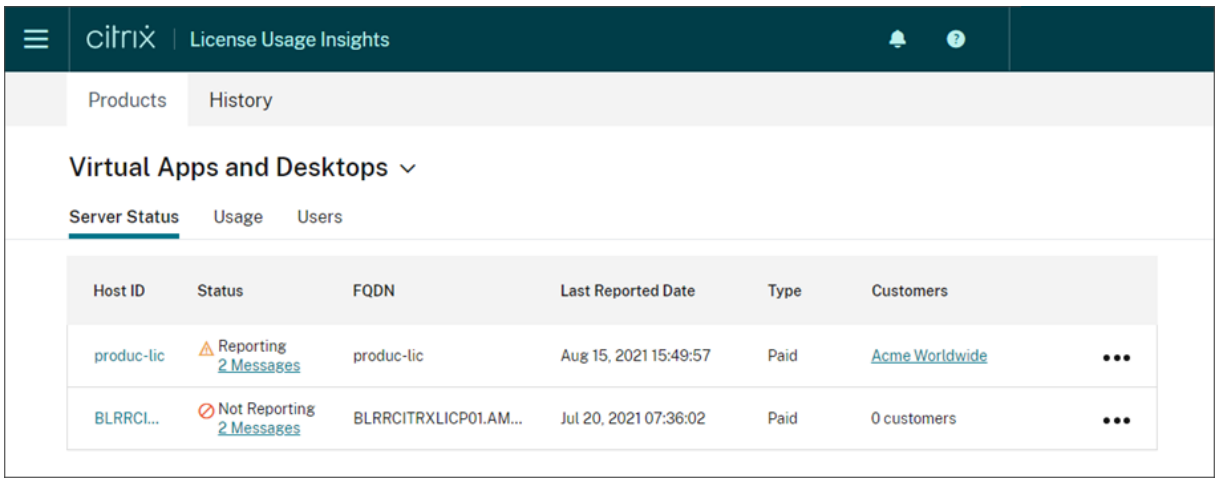
Um die Lizenzdetails für ein anderes Produkt anzuzeigen, klicken Sie auf den Pfeil neben dem Produktnamen, und wählen Sie das anzuzeigende Produkt bzw. den Service aus.



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

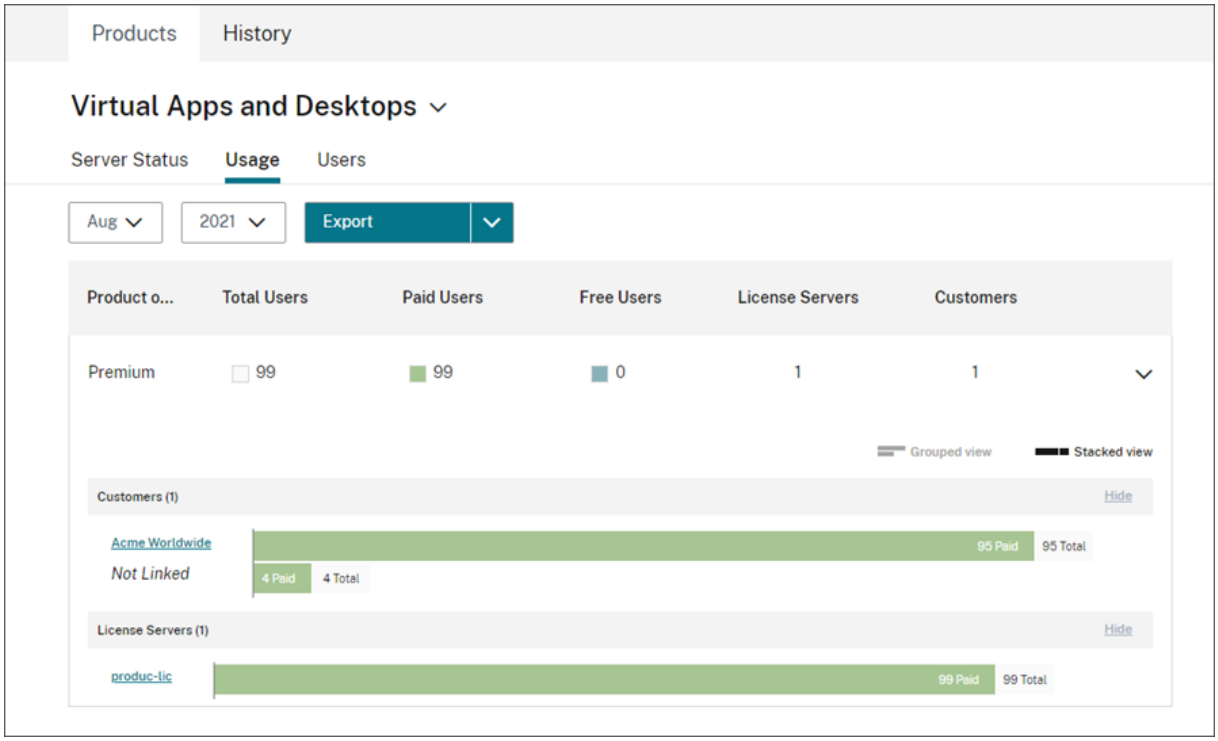
> **Hinweis:**
>
> Erfolgreiche Uploads werden mit Ausnahme des Letzten gelöscht. Fehlgeschlagene Uploads bleiben bis zum nächsten erfolgreichen Upload auf der Festplatte. Beim nächsten erfolgreichen Upload werden alle bis auf das letzte Upload gelöscht.

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

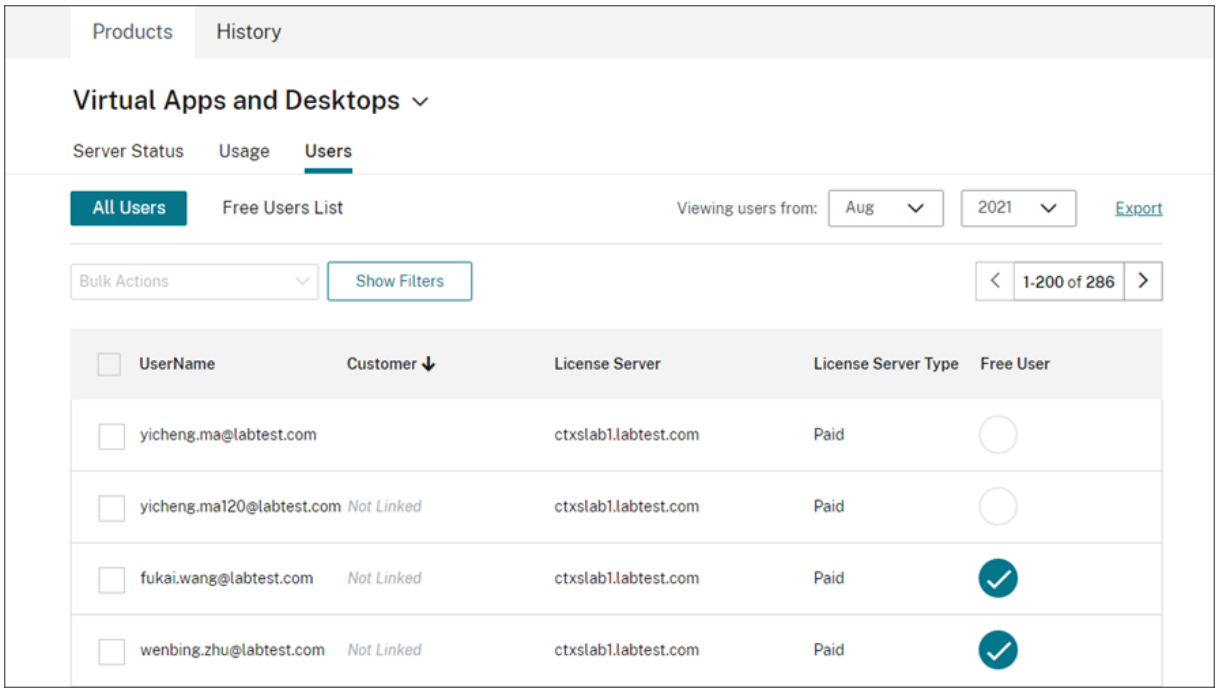
Sie können die Lizenznutzung auch pro Benutzer aufschlüsseln. Hierzu müssen Sie erst Benutzer mit den Kunden oder Mandanten verknüpfen, denen sie angehören. Wenn in Ihrem Kundendashboard keine Kunden definiert sind, können Sie neue Kunden hinzufügen oder eine Verbindung mit vorhandenen Citrix Cloud-Kunden 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-

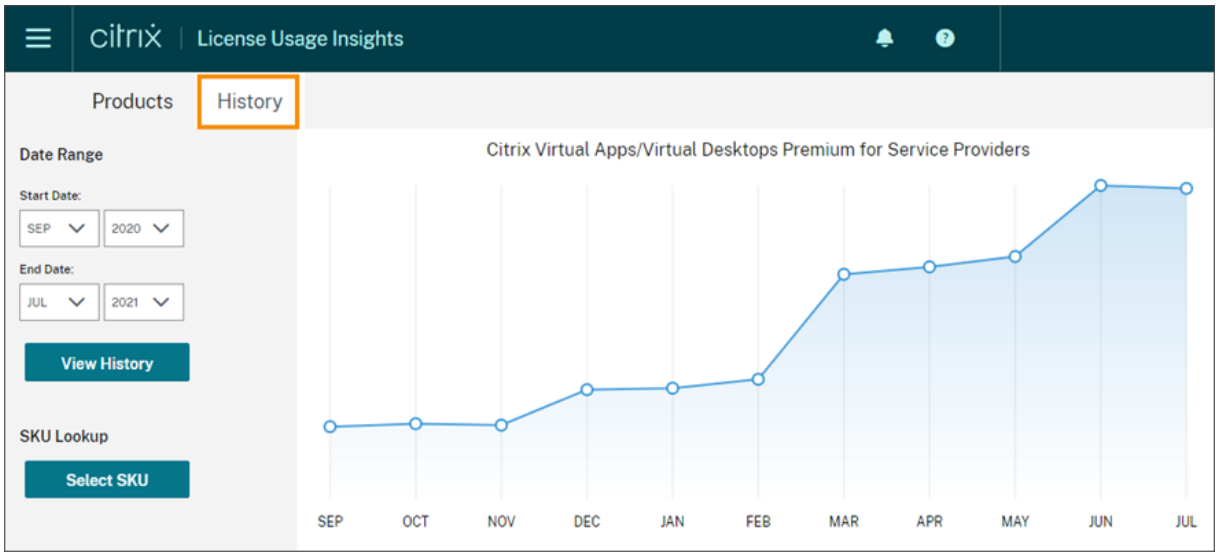
Lizenzprogramms einschließlich Test- und Administratorkonten voll auszuschöpfen.



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

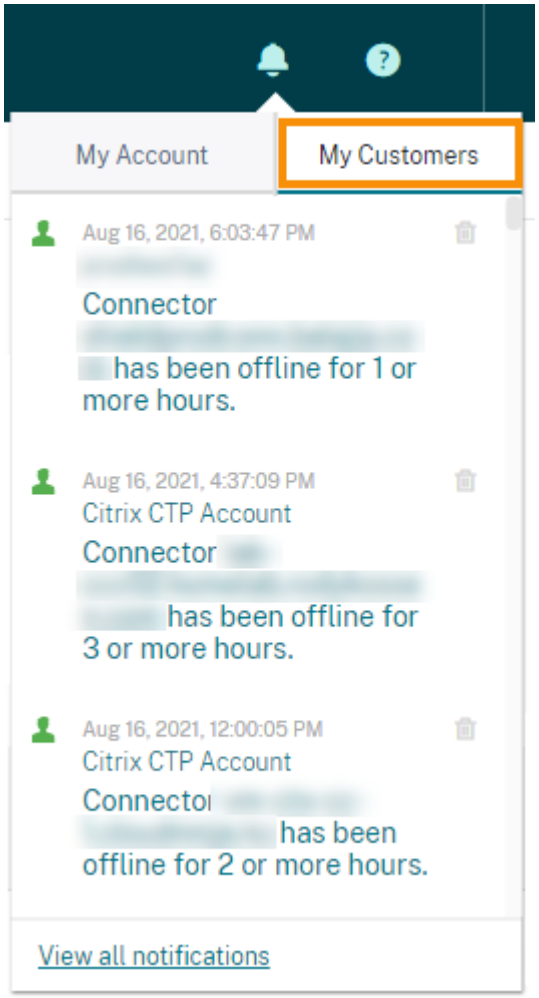
Sie können die folgenden Datentypen als CSV-Datei aus License Usage Insights exportieren:

- Virtual Apps and Desktops-Produktverwendung und Benutzerliste für einen bestimmten Monat
- Aktuelle ADC 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**.

Anzeigen von Kundenbenachrichtigungen

Mit Citrix Cloud können Sie den Lösungsstatus für mehrere Kunden überwachen, 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.

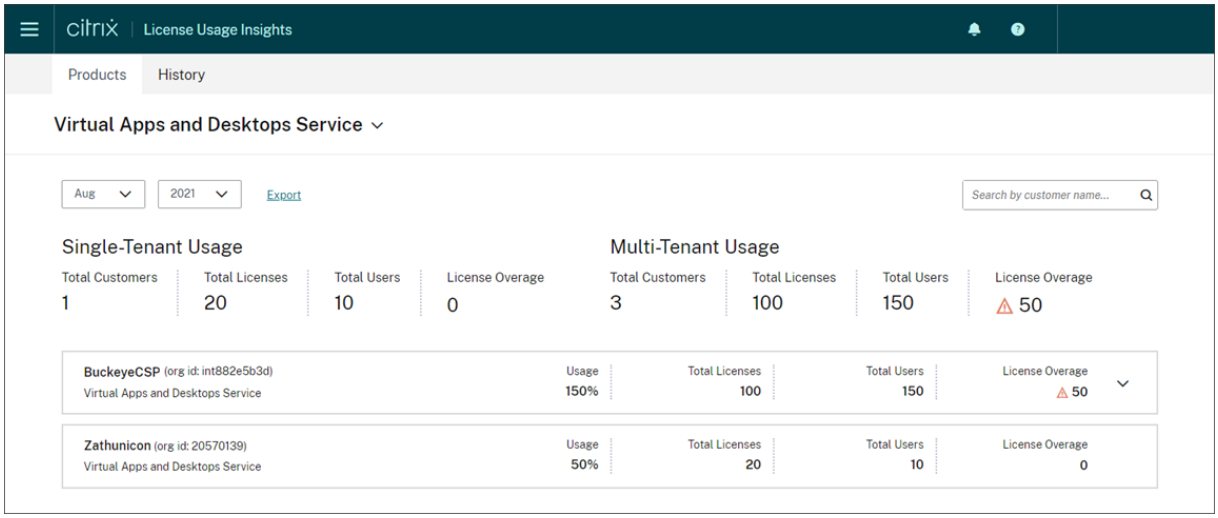


1. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf das Symbol **Benachrichtigungen** und anschließend auf **Meine Kunden**. Eine Liste der letzten Benachrichtigungen wird angezeigt.
2. Um eine vollständige Liste der Kundenbenachrichtigungen anzuzeigen, klicken Sie auf **Alle Benachrichtigungen anzeigen**.

Cloudservice-Lizenznutzung und -Berichterstellung für Citrix Service Provider

April 29, 2022

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:

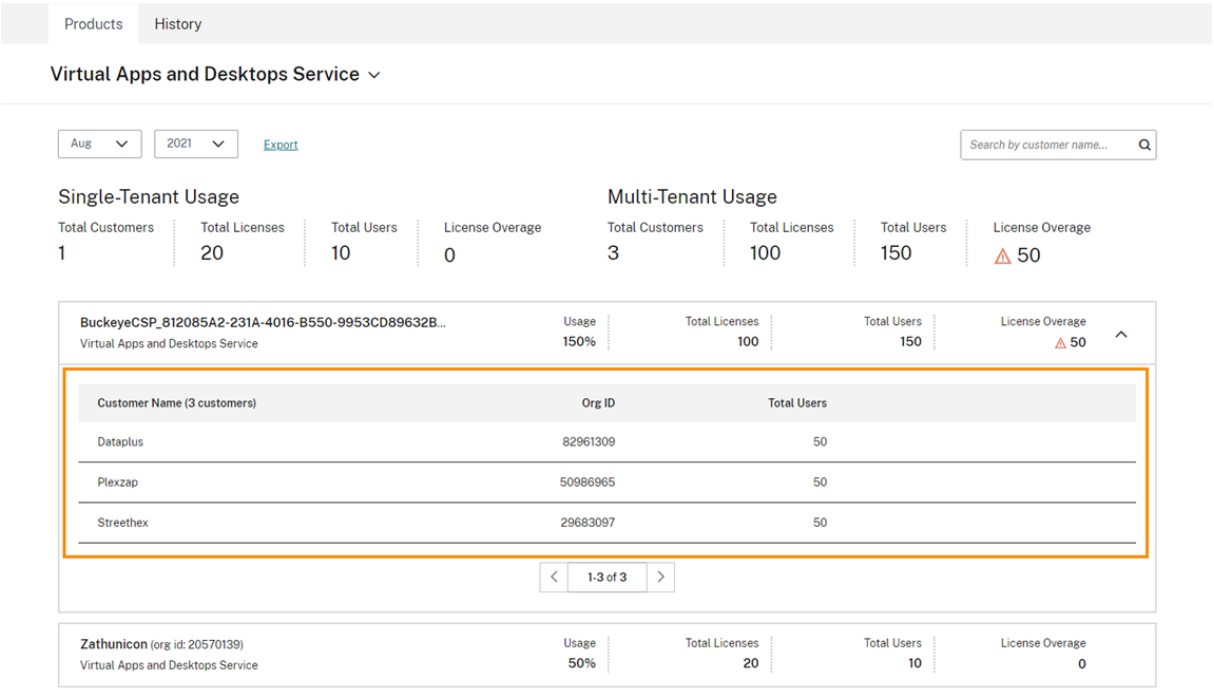
- Citrix DaaS (früher Virtual Apps and Desktops Service)
- Citrix DaaS Standard für Azure (früher Virtual Apps and Desktops Standard für Azure)

Lizenzübersichten

License Usage Insights bietet die folgende Aufschlüsselung der Einzel- und Mehrmandantennutzung:

- 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.

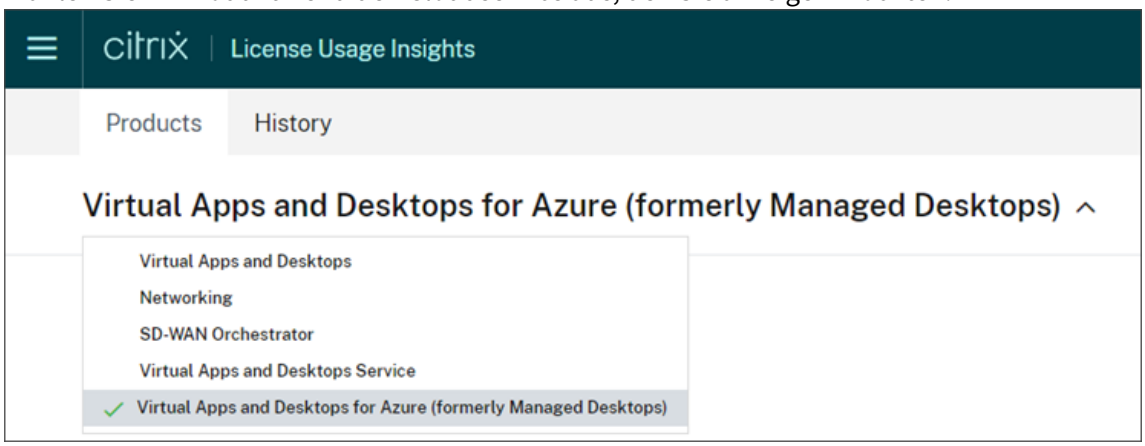
Für Mehrmandantenservices können Sie die Nutzungsübersicht erweitern, um die Kunden, die OrgID und die Anzahl aller Benutzer anzuzeigen, die dem jeweiligen Partner zugeordnet sind.



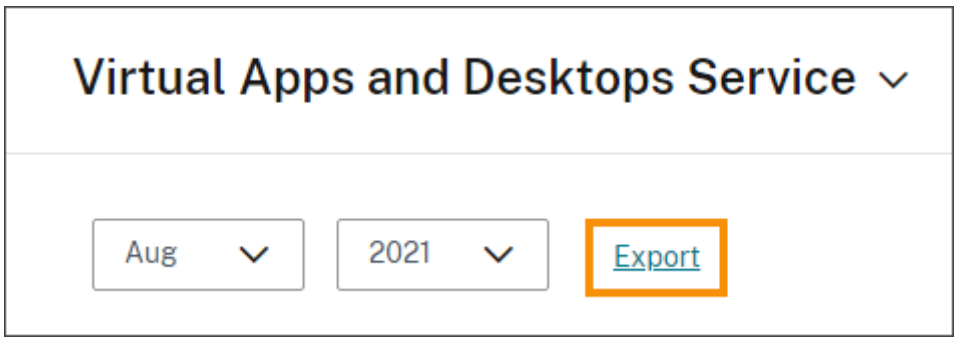
Anzeigen und Exportieren der monatlichen Nutzung

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.

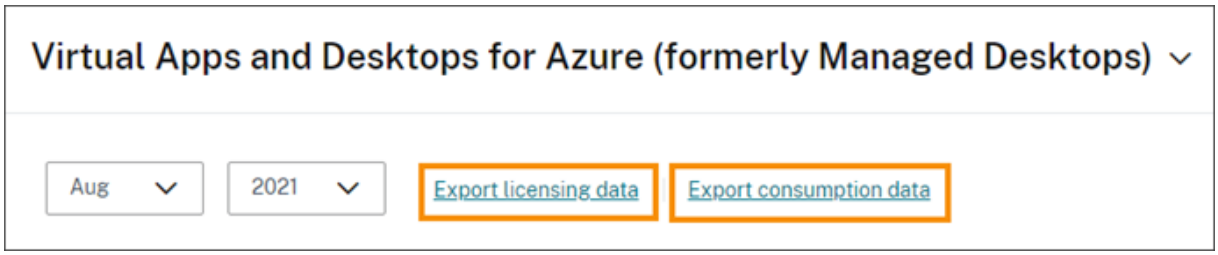
1. Wählen Sie im Produktmenü den Cloudservice aus, den Sie anzeigen möchten.



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.



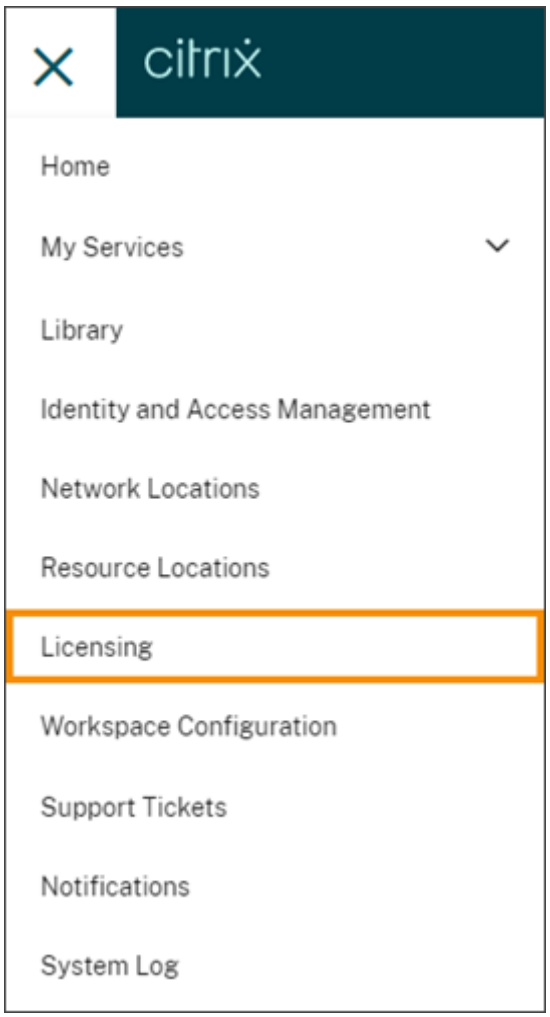
Überwachung von Kundenlizenzen und Lizenznutzung für Citrix DaaS

April 29, 2022

> **Hinweis:**
>
> Citrix DaaS war früher Citrix Virtual Apps and Desktops Service. Einige Anzeigen enthalten evtl. den alten Namen.

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

Citrix Cloud weist eine Lizenz zu, wenn ein eindeutiger Kundenbenutzer zum ersten Mal im aktuellen Monat eine App oder einen Desktop startet.

Zusammenfassung zur Lizenzierung

Auf der Registerkarte **Cloudservices** wird eine Lizenzübersicht mit folgenden Informationen angezeigt:

- 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 Anzahl von Lizenzüberschreitungen (falls vorhanden). Wenn die Anzahl der zugewiesenen Lizenzen die Gesamtanzahl der erworbenen Lizenzen überschreitet, wird eine Warnmeldung angezeigt.

Nutzungstrends und Lizenzaktivität

Wählen Sie **Nutzungsdetails anzeigen** ganz rechts in der Lizenzübersicht, um eine detaillierte Ansicht der Lizenzen anzuzeigen.

Im Abschnitt **Nutzungstrends** sind folgende Informationen aufgeschlüsselt:

- **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.
- **Zugewiesene Benutzer:** Die kumulative Anzahl aller Lizenzen, die Kundenbenutzern in jedem Monat zugewiesen wurden.
- **Benutzer überschritten:** Die Anzahl zugewiesener Lizenzen pro Monat, die den Gesamtwert der erworbenen Lizenzen überschritten haben.

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.

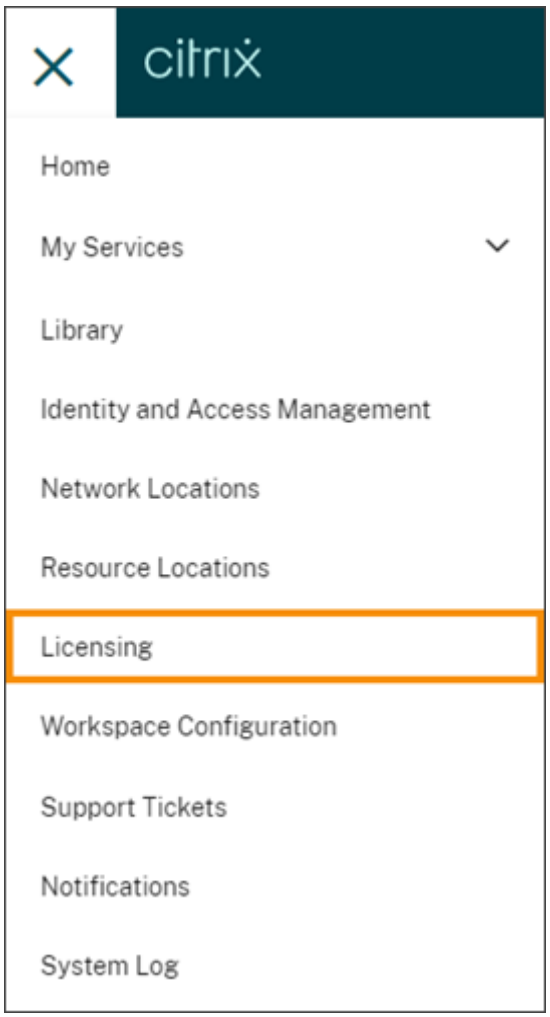
Überwachung von Kundenlizenzen und Lizenznutzung für Citrix DaaS Standard für Azure

April 29, 2022

> **Hinweis:**
>
> Citrix DaaS Standard für Azure war früher Citrix Virtual Apps and Desktops Standard für Azure. Einige Anzeigen enthalten evtl. den alten Namen.

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

Citrix Cloud weist eine Lizenz zu, wenn ein eindeutiger Benutzer zum ersten Mal einen Desktop startet.

Zusammenfassung zur Lizenzierung

Auf der Registerkarte **Cloudservices** wird eine Lizenzübersicht mit folgenden Informationen angezeigt:

- 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 Anzahl von Lizenzüberschreitungen (falls vorhanden). Wenn die Anzahl der zugewiesenen Lizenzen die Gesamtanzahl der erworbenen Lizenzen überschreitet, wird eine Warnmeldung

angezeigt.

Klicken Sie auf **Nutzungsdetails anzeigen** am rechten Rand der Zusammenfassung, um eine Aufschlüsselung der Nutzungsberichte und -trends sowie eine Liste der Benutzer anzuzeigen, die Citrix DaaS Standard für Azure-Lizenzen verwenden.

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.

Nutzungstrends und Lizenzaktivität

Im Abschnitt **Nutzungstrends** der Verwaltungskonsole sind folgende Informationen aufgeschlüsselt:

- **Gesamtlizenzen:** Alle Ihre erworbenen Lizenzen für den Cloudservice für alle Bereiche.
- **Zugewiesene Benutzer:** Die kumulative Anzahl aller Lizenzen, die Kundenbenutzern in jedem Monat zugewiesen wurden.
- **Benutzer überschritten:** Die Anzahl zugewiesener Lizenzen pro Monat, die den Gesamtwert der erworbenen Lizenzen überschritten haben.

Wenn Sie auf einen Balken im Diagramm eines bestimmten Monats zeigen, wird die Gesamtanzahl der Lizenzen, der zugewiesenen Lizenzen, der zugewiesenen Benutzer und der Lizenzüberschreitungen 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

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.

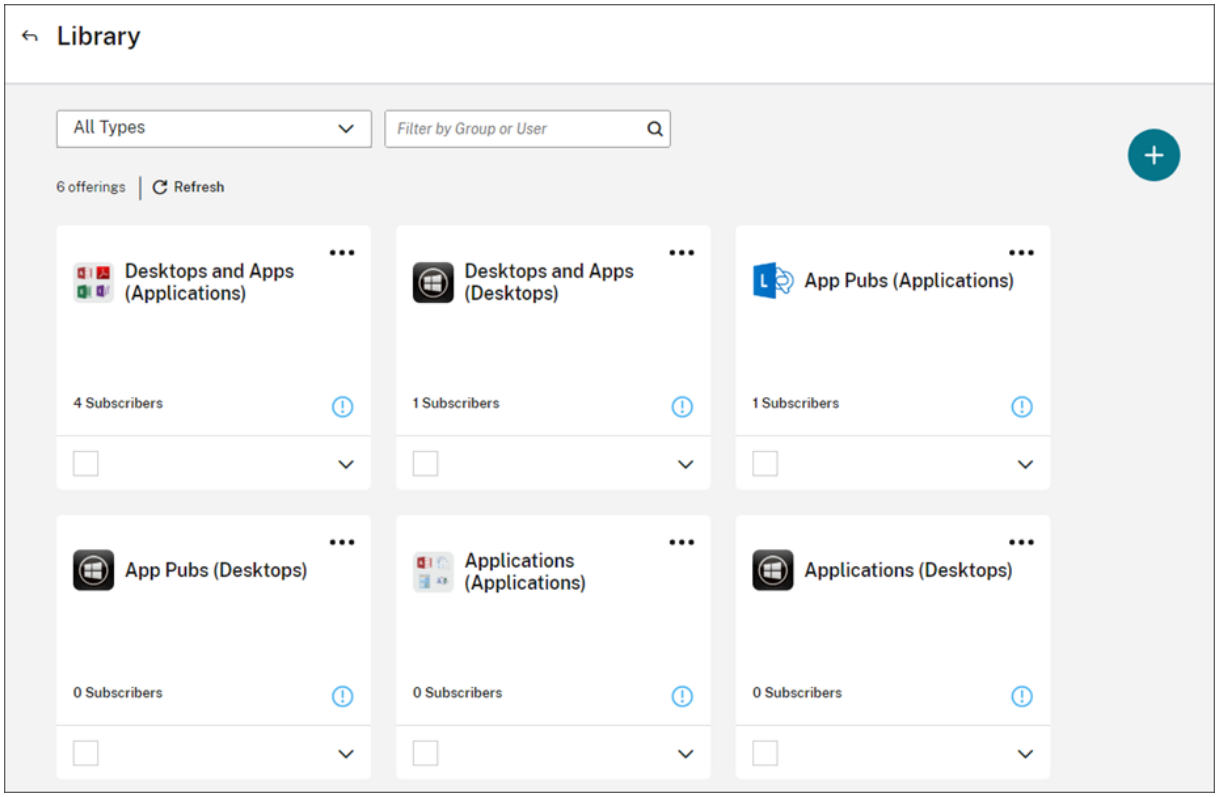
Um die Details für den aktuellen Monat zu exportieren, wählen Sie im Bereich **Lizenzaktivität** am rechten Rand **Als CSV-Datei exportieren** und speichern Sie die Datei.

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.

Zuweisen von Benutzern und Gruppen zu Serviceangeboten über die Bibliothek

April 29, 2022

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.



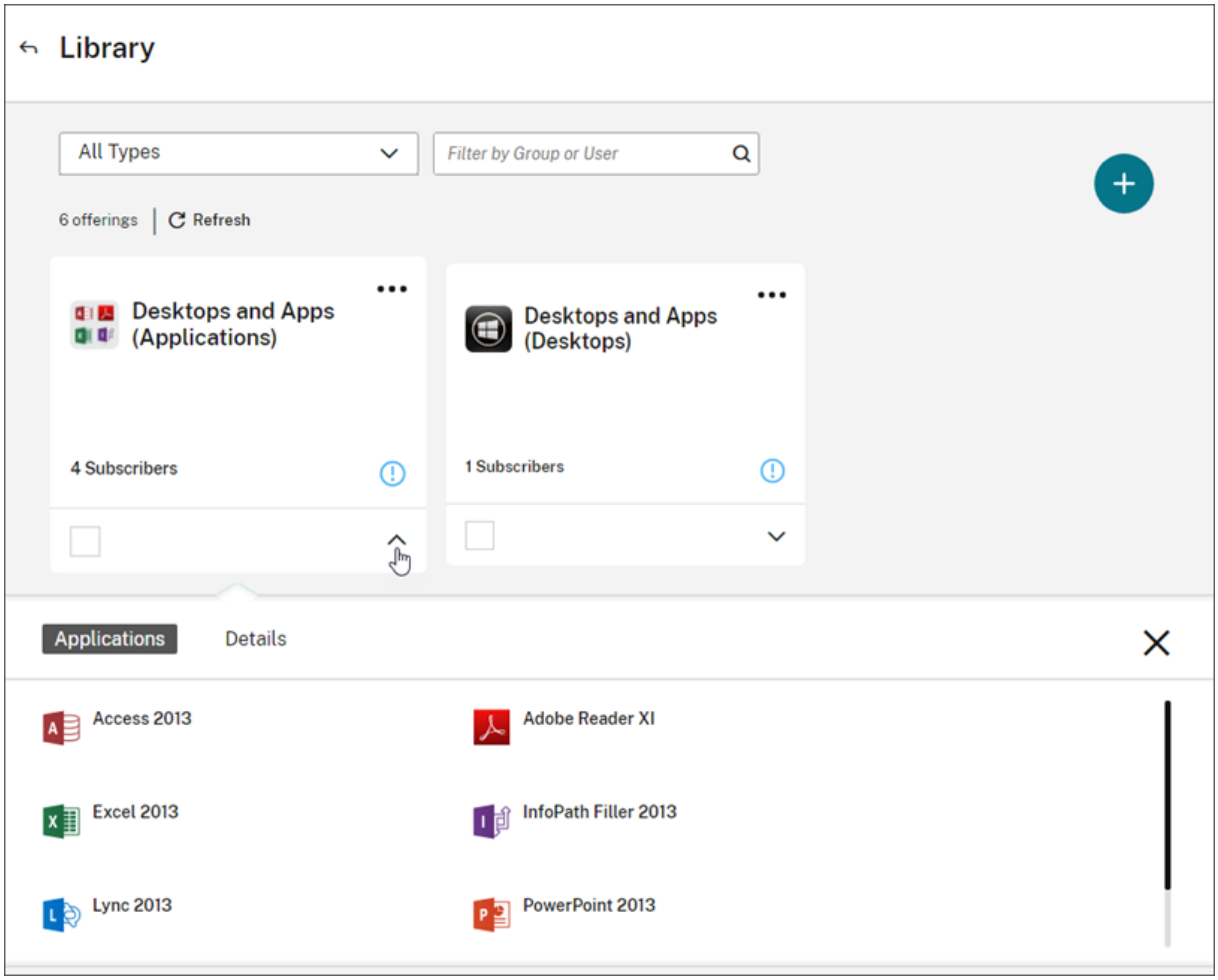
Wichtig:

Wenn Sie On-Premises-StoreFront mit Citrix DaaS (früher Virtual Apps and Desktops Service) verwenden, sollten Sie beim Erstellen von Bereitstellungsgruppen Ressourcen nicht mithilfe 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**.

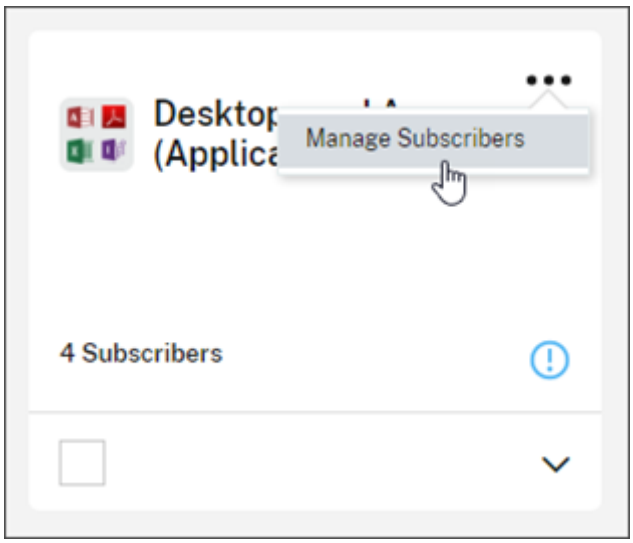
Anzeigen von Angebotsdetails

Klicken Sie auf der Angebotskarte auf den Pfeil, um Anwendungen, Desktops, Richtlinien und andere Angebotsinformationen anzuzeigen.

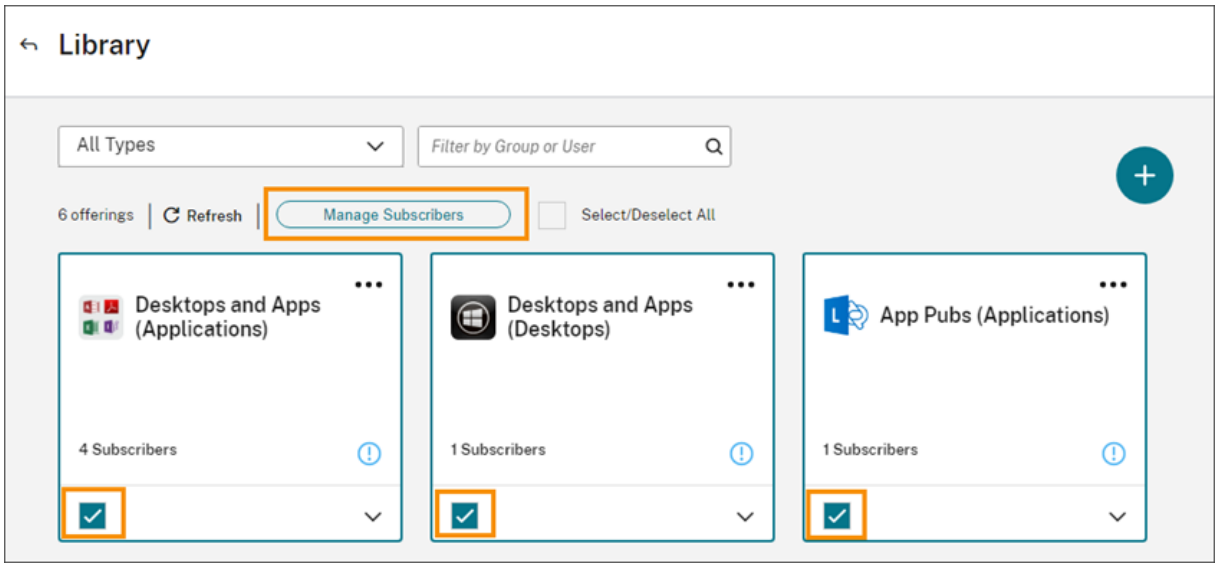


Abonnenten hinzufügen oder entfernen

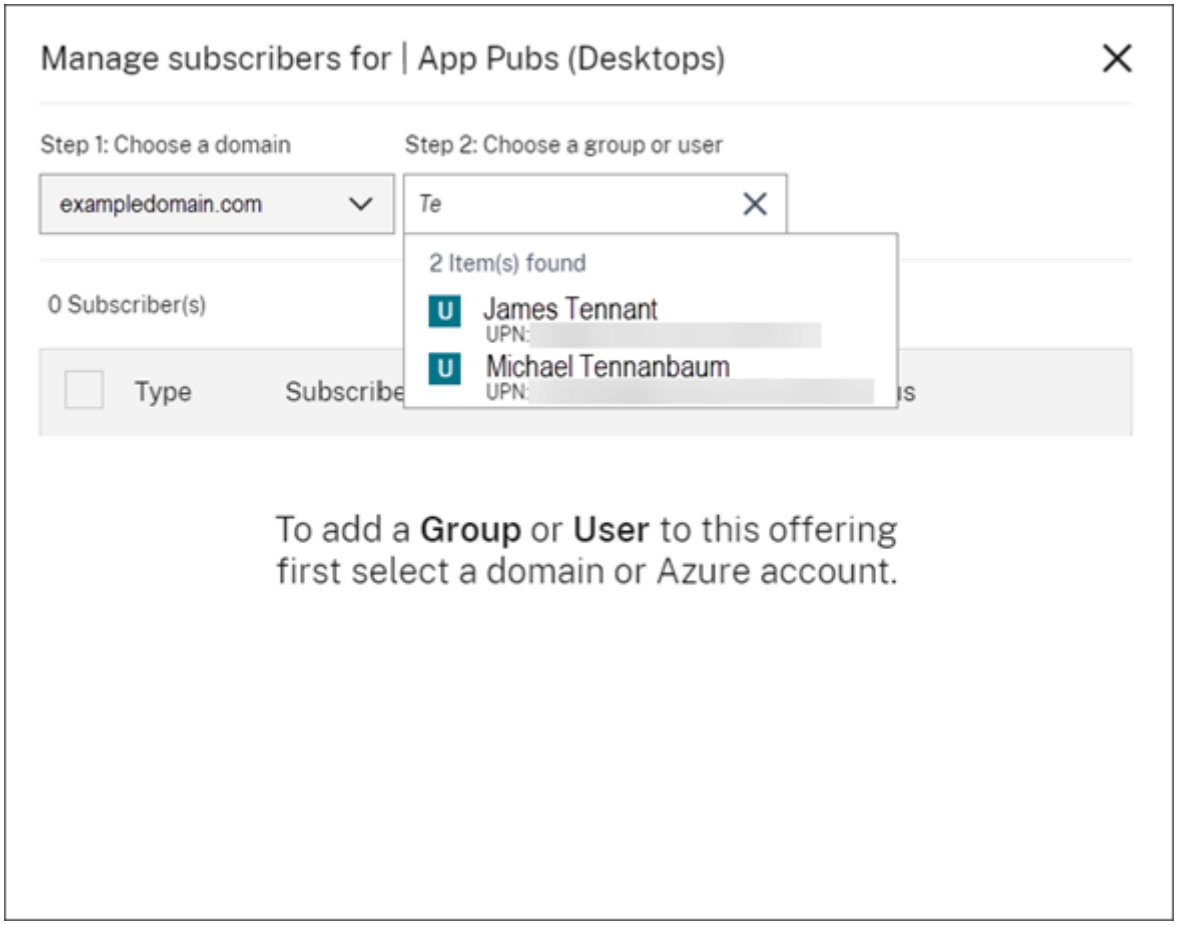
Klicken Sie zum Verwalten von Benutzern oder Gruppen für ein einzelnes Angebot im Menü der Angebotskarte auf **Abonnenten verwalten**.



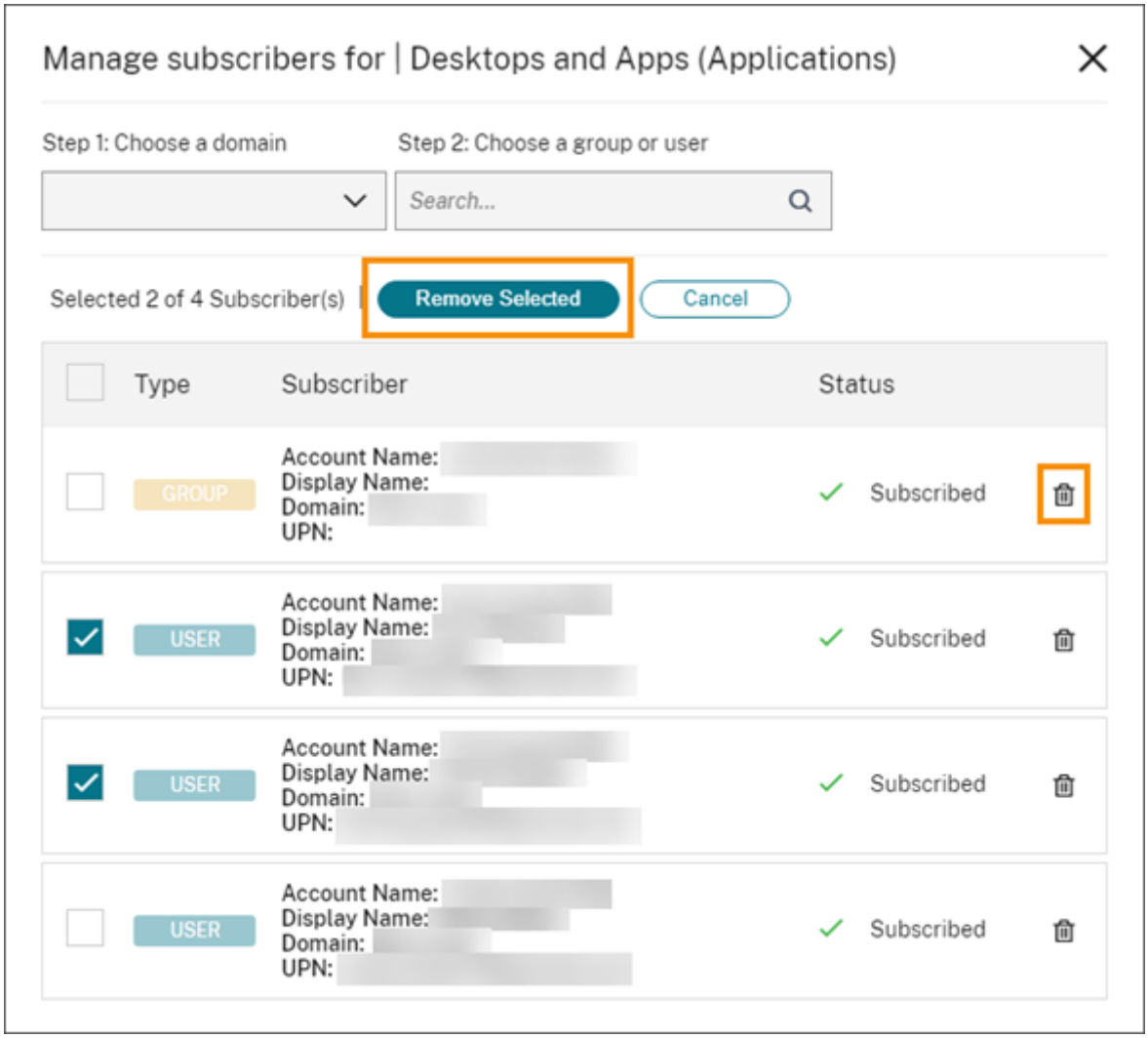
Um Abonnenten für mehrere Angebote zu verwalten, aktivieren Sie das Kontrollkästchen für jedes Angebot und klicken Sie dann auf **Abonnenten verwalten**.



Zum Hinzufügen von Abonnenten zum Angebot wählen Sie eine Domäne und dann die Benutzer oder Gruppen, die Sie hinzufügen möchten.



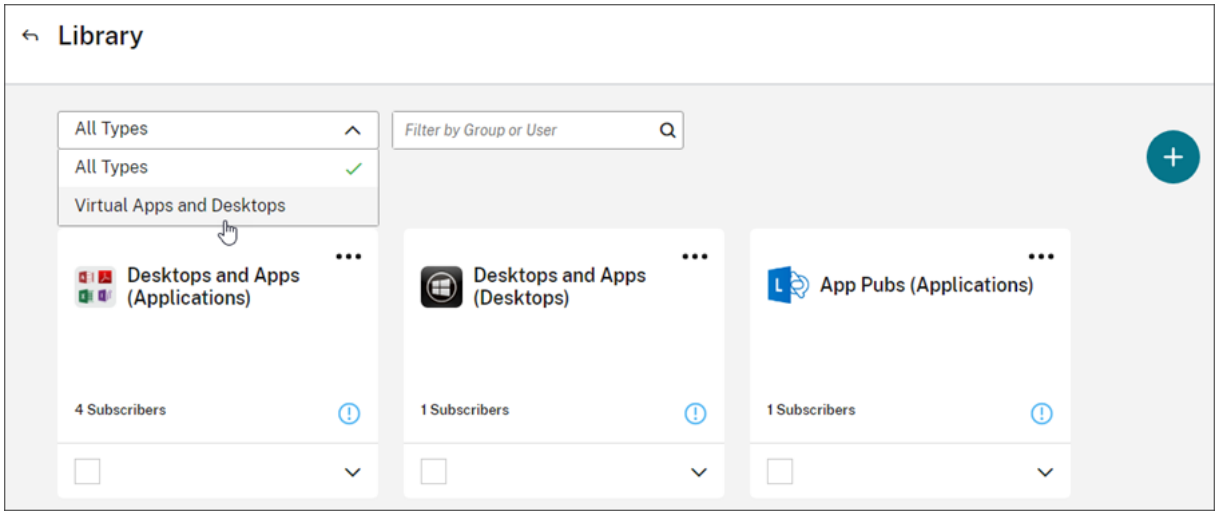
Klicken Sie zum Entfernen einzelner Abonnenten auf das zum Abonnenten gehörende Papierkorbsymbol. Um mehrere Abonnenten zu entfernen, wählen Sie die Benutzer (bzw. Gruppen) und klicken Sie auf **Ausgewählte entfernen**.



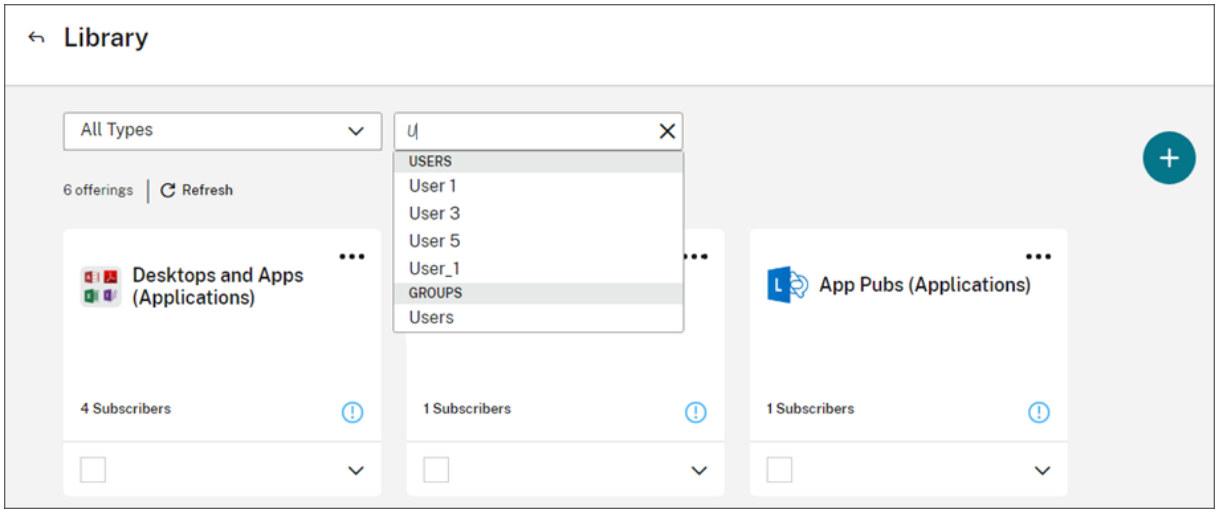
Nachdem Sie Abonnenten hinzugefügt oder entfernt haben, zeigt die Angebotskarte die aktuelle Abonnentenzahl an.

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.



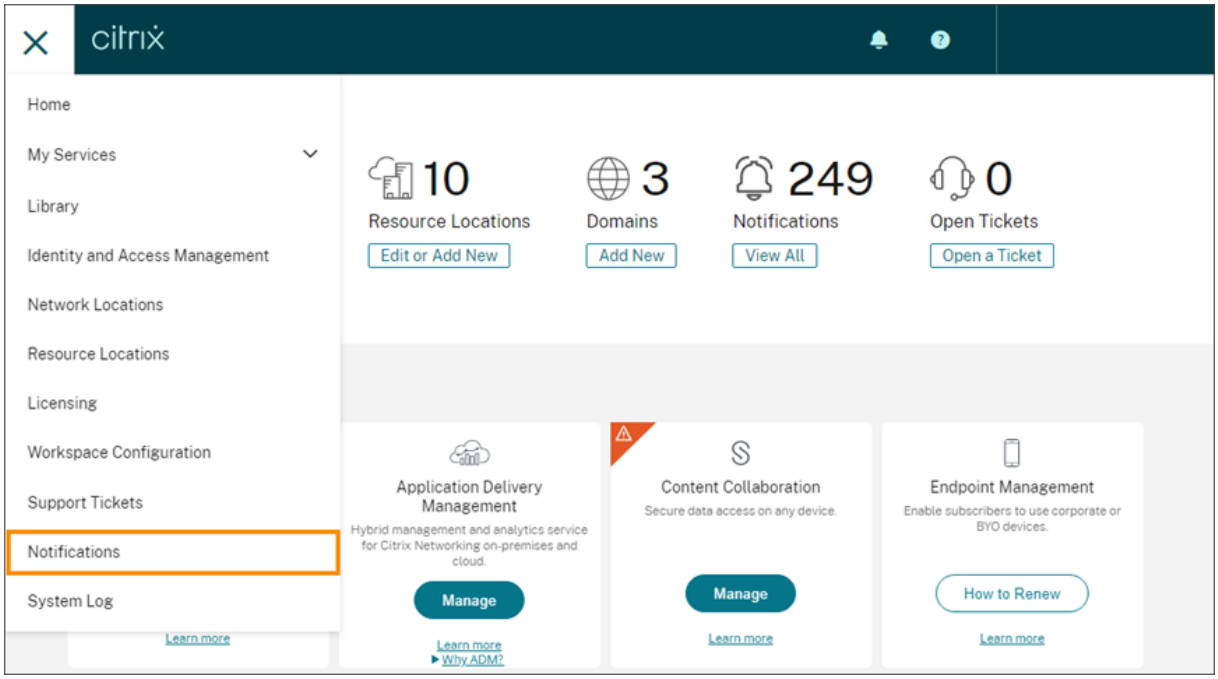
Benachrichtigungen

October 16, 2022

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.

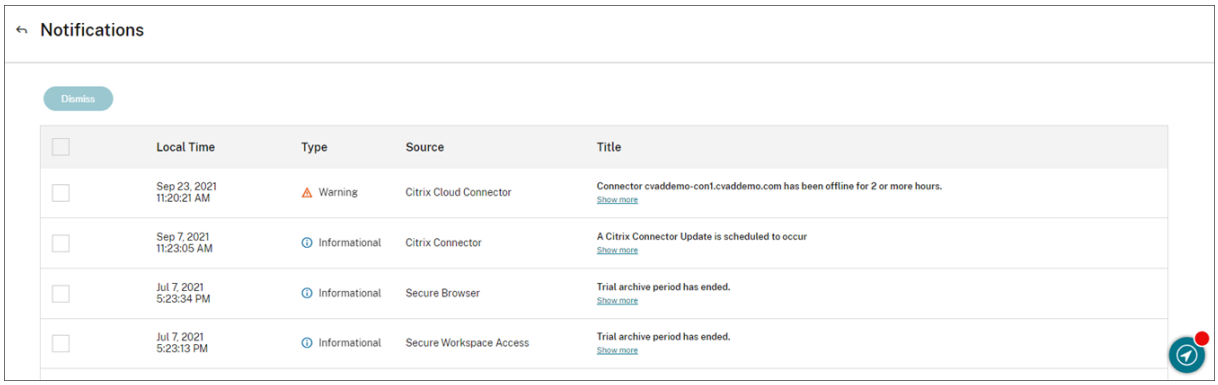
Anzeigen von Benachrichtigungen

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.



Schließen von Benachrichtigungen

Wenn Sie eine Benachrichtigung gelesen haben, können Sie sie mit einem Klick auf **Schließen** schließen. Durch Schließen von Benachrichtigungen werden diese aus Ihrer Liste entfernt und Citrix Cloud aktualisiert die Anzahl der Benachrichtigungen, wenn Sie zur Startseite der Konsole zurückkehren.



Administratoren erhalten ihre eigenen Benachrichtigungen in Citrix Cloud. Das Schließen von Benachrichtigungen verhindert also nicht, dass andere Administratoren ihre Benachrichtigungen einsehen können.

Empfang von Benachrichtigungen per E-Mail

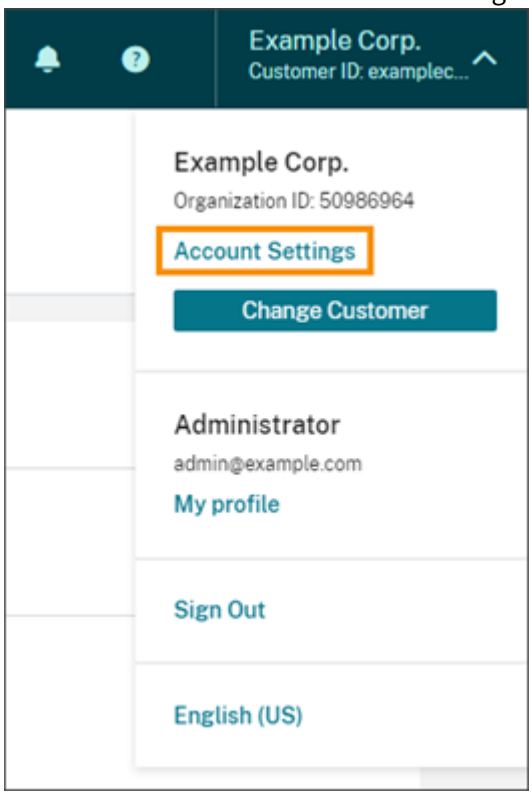
Sie können Benachrichtigungen auch per E-Mail erhalten und müssen sich dann nicht erst anmelden, um sie zu lesen. Standardmäßig sind E-Mail-Benachrichtigungen deaktiviert.

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. Klicken Sie in der Citrix Cloud-Verwaltungskonsole auf **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.

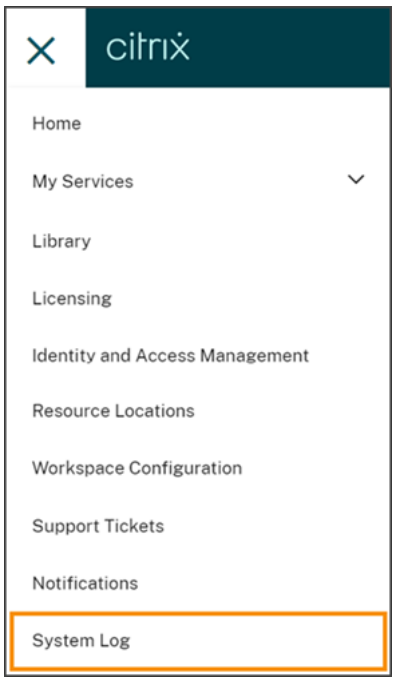
Citrix Cloud entfernt den Kontakt aus der Tabelle.

Systemprotokoll

April 29, 2022

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.

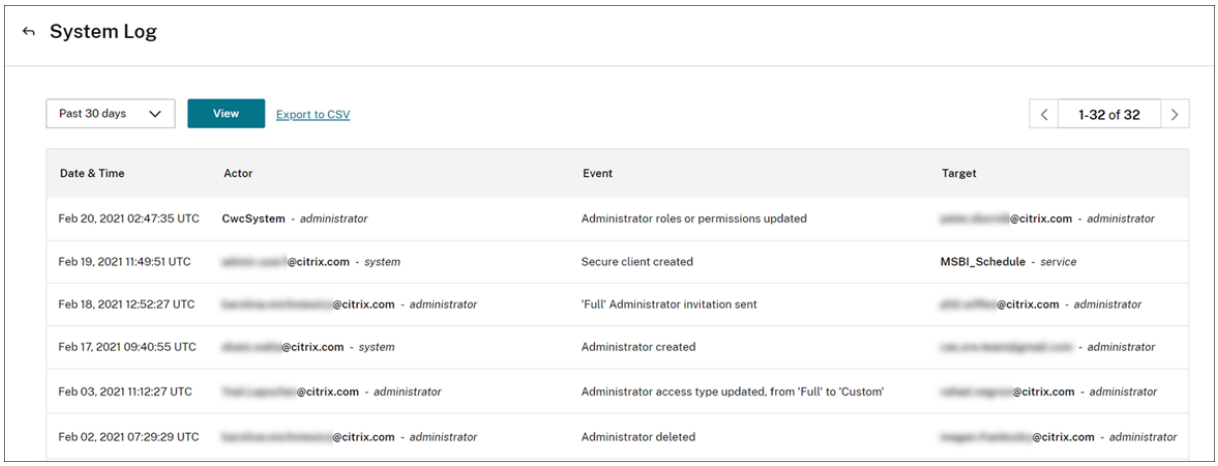


Weitere Informationen zur Aufbewahrung von Daten in Systemprotokollen finden Sie unter Datenaufbewahrung in diesem Artikel.

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.

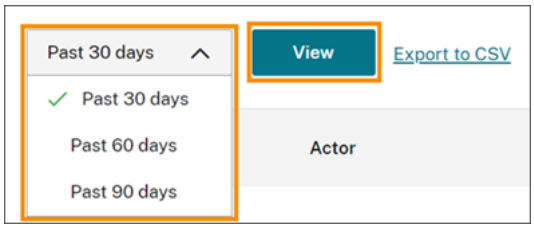


Die angezeigte Liste enthält die folgenden Informationen:

- 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.

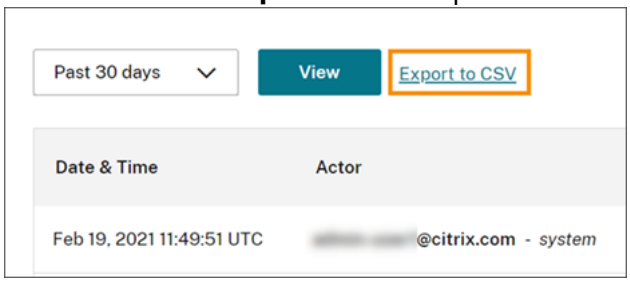


Um ältere Ereignisse abzurufen, können Sie die SystemLog-API verwenden. Weitere Informationen finden Sie unter Abrufen von Ereignissen eines bestimmten Zeitraums in diesem Artikel.

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.

Add-Ons für andere SIEM-Lösungen (Security Information and Event Management) wie Microsoft Azure Sentinel und IBM QRadar sind noch nicht verfügbar. Konsultieren Sie regelmäßig die folgenden Quellen zu neuen Informationen über Entwicklungen und Releases:

- Citrix Blogs
- Citrix Cloud-Diskussionsforum
- Citrix in den sozialen Medien: Twitter, LinkedIn, Facebook

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

May 13, 2022

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 Citrix Cloud-Administratoren, Administratorgruppen, Geräterücksetzungen für Workspace-Abonnenten und Azure AD-Mandanten.
- 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

April 29, 2022

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.

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/create	administrator	system	Nein	Ja
Administratoreinladung gesendet	platform/administrator/invite	administrator	administrator	Nein	Ja
Administratorrollen oder -berechtigungen aktualisiert	platform/administrator/update	administrator	administrat
Vom Administrator gelöscht	platform/administrator/delete	administrator	administrator	Nein	Ja
Sicherer Client erstellt	platform/clientadministrator/create	service	system	Nein	Ja
Sicherer Client gelöscht	platform/clientadministrator/delete	service	administrator	Ja	Nein
Administratorgruppe erstellt	platform/administratorgroup/create	administratorgroup		Nein	Ja
Rollen oder Berechtigungen der Administratorgruppe aktualisiert	platform/administratorgroup/update	administr
Administratorgruppe gelöscht	platform/administratorgroup/delete	administratorgroup		administrators	Ja	Nein

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/authe	subscriber	administrator	Nein	Ja

Azure AD-Mandanten

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Akteur-ID	Aufzeichnung aktueller Objekt-felder vor dem Ereignis	Aufzeichnung aktual-isierter Objekt-felder nach dem Ereignis
Azure AD-Mandant verbunden	platform/ider	service	administrato		Ja	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Akteurtyp	Akteur-ID	Aufzeichnung aktueller Objekt-felder vor dem Ereignis	Aufzeichnung aktual-isierter Objekt-felder nach dem Ereignis
Azure AD-Mandant getrennt	platform/identityprovider/azuread/disconnect				Ja	Nein
Azure AD auth domain name changed	platform/ider	cws		CustomerID	Nein	Nein
Azure AD auth domain name change failed	platform/identityprovider/azuread/authdomainupdatefailed			CustomerID	Nein	Nein

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/edges	**Cloud Connector** oder **Connectorgerät**	Der Administrator, der den Connector registriert hat	Ja	Ja
Connector gelöscht	platform/edges/cloud	**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/resou	Der Name des geänderten Ressourcenstandorts	Der Administrator, der die Konfiguration geändert hat	Ja	Ja
Connector-Upgrade wurde vom Administrator ausgelöst	platform/edges/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/edges	**Cloud Connector** oder **Connectorgerät**	**Automatisch** oder der Administrator, der das Update initiiert hat	Ja	Nein
Connector-Upgrade abgeschlossen	platform/edges/cloudupgradecompleted	**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/authe		Der Administrator, der den Vorgang ausgeführt hat	Nein	Nein
Public Key removed from trust	platform/authentication/deleteedgesadminkey		Der 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/onpremlicer	Lizenzierung	Der Administrator, der den Lizenzserver gelöscht hat	Nein	Nein
Fehler beim Löschen der On-Premise-Lizenzserver	lui/onpremlicenslizenzierung/delete	Lizenzierung	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	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 Benutzerlistendaten von Partner exportiert	lui/csp/userlist	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	LicenseExportFailed	Der Administ-rator, 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
Lizenznutzungs exportiert	lui/cloudlicense	CloudLicense oder Lizenzierung	Der Administ-rator, der Lizen-znutzungs-daten exportiert hat	Nein	Nein
Fehler beim Exportieren von Lizen-znutzungs-daten	lui/cloudlicense/UsageDataExportFailed	CloudLicense oder Lizenzierung	Der Administ-rator, 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/websaaspplic	websaaspplicatior	Nein	Ja
Web-/SaaS-Anwendung aktualisiert	swa/websaaspplicatio	websaaspplication	Ja	Ja
Web-/SaaS-Anwendung gelöscht	swa/websaaspplic	websaaspplicatior	Ja	Nein
Fehler beim Erstellen der Web-/SaaS-Anwendung	swa/websaaspplicatio	websaaspplication	Nein	Nein
Fehler beim Aktualisieren der Web-/SaaS-Anwendung	swa/websaaspplic	websaaspplicatior	Ja	Ja
Fehler beim Löschen der Web-/SaaS-Anwendung	swa/websaaspplicatio	websaaspplication	Ja	Ja

Benutzer- und Gruppenabonnements

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Benutzer-/Gruppenabonnen hinzugefügt	swa/websaaspplic	websaaspplicatior	Nein	Ja
Benutzer-/Gruppenabonnement entfernt	swa/websaaspplicatiwebsaaspplicat/unsubscribers		Nein	Ja
Benutzer-/Gruppenabonnen fehlgeschlagen	swa/websaaspplic	websaaspplicatior	Nein	Nein
Fehler beim Abbestellen des Benutzer-/Gruppenabonnements	swa/websaaspplicatiwebsaaspplicat/unsubscribefailed		Nein	Nein

Kontextbezogene Richtlinien

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Kontextbezogene Richtlinie erstellt	swa/contextualpol	contextualpolicy	Nein	Ja
Kontextbezogene Richtlinie aktualisiert	swa/contextualpolicy/upda	contextualpolicy	Ja	Ja
Kontextbezogene Richtlinie gelöscht	swa/contextualpol	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/contextualpol	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
Anwendungsdoma erstellt	swa/applicationdc	applicationdomai	Nein	Ja
Anwendungsdomäne aktualisiert	swa/applicationdomain/updated	applicationdomain	Ja	Ja
Anwendungsdoma gelöscht	swa/applicationdc	applicationdomai	Ja	Nein
Fehler beim Erstellen der Anwendungsdomäne	swa/applicationdomain/createfailed	applicationdomain	Nein	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Aktualisieren der Anwendungs-domäne	swa/applicationdc	applicationdomai	Ja	Nein
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/browserexten	browserextensions	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/filter	websiteurllistcateg	Ja	Ja
Websitefilterlisten aktiviert und -filterkategorien deaktiviert	swa/website/filterlist	websiteurllistcategoryisdisabled/upda	Ja	Ja
Websitefilterlisten deaktiviert und -filterkategorien aktiviert	swa/website/filter	websiteurllistcateg	Ja	Ja
Websitefilterlisten und -kategorien deaktiviert	swa/website/filterlist	websiteurllistcategoryisdisabled/upda	Ja	Ja
Fehler beim Aktivieren von Websitefilterlisten und -kategorien	swa/website/filter	websiteurllistcateg	Ja	Ja
Fehler beim Aktivieren von Websitefilterlisten und Deaktivieren von Websitefilterkategorien	swa/website/filterlist	websiteurllistcategoryisdisabled/upda	Ja	Jafailed

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Deaktivieren von Websitefilterlisten und Aktivieren von Websitefilterkategorien	swa/website/filter	websiteurllistcateg	Ja	Ja
Fehler beim Deaktivieren von Websitefilterlisten und -kategorien	swa/website/filterlist	websiteurlfiltercategoryassis	disabled/upda	Jafailed
Website-URL-Liste erstellt	swa/websiteurlfilt	websiteurlfiltering	Nein	Ja
Website-URL-Liste aktualisiert	swa/websiteurlfilteringlist/	websiteurlfilteringlist	Ja	Ja
Website-URL-Liste gelöscht	swa/websiteurlfilt	websiteurlfiltering	Ja	Nein
Fehler beim Erstellen der Website-URL-Liste	swa/websiteurlfilteringlist/	websiteurlfilteringlist	Nein	Nein
Fehler beim Aktualisieren der Website-URL-Liste	swa/websiteurlfilt	websiteurlfiltering	Ja	Nein

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Löschen der Website-URL-Liste	swa/websiteurlfilterwebsiteurlfilterfailedlist	websiteurlfilterwebsiteurlfilterfailedlist	Ja	Nein
Website-URL-Filterkategorie erstellt	swa/websiteurlfilt	websiteurlfiltercat	Nein	Ja
Website-URL-Filterkategorie aktualisiert	swa/websiteurlfilterwebsiteurlfilterupdatecategory	websiteurlfilterwebsiteurlfilterupdatecategory	Ja	Ja
Website-URL-Filterkategorie gelöscht	swa/websiteurlfilt	websiteurlfiltercat	Nein	Nein
Fehler beim Erstellen der Website-URL-Filterkategorie	swa/websiteurlfilterwebsiteurlfiltercreatecategoryfailed	websiteurlfilterwebsiteurlfiltercreatecategoryfailed	Nein	Nein
Fehler beim Aktualisieren der Website-URL-Filterkategorie	swa/websiteurlfilt	websiteurlfiltercat	Ja	Nein
Fehler beim Löschen der Website-URL-Filterkategorie	swa/websiteurlfilterwebsiteurlfilterdeletecategoryfailed	websiteurlfilterwebsiteurlfilterdeletecategoryfailed	Nein	Nein

Voreingestellte Websitefilterkategorien

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Voreingestellte Websitefilterkategorie aktualisiert	swa/websiteurlfilte	websiteurlfiltercat	Ja	Ja
Fehler beim Aktualisieren der voreingestellten Websitefilterkategorie	swa/websiteurlfilte	websiteurlfiltercat	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/websiteurlfilte	websiteurlfiltering	Nein	Ja
Liste mit blockierten Website-URLs aktualisiert	swa/websiteurlfilte	websiteurlfiltering	Nein	Ja
Liste mit blockierten Website-URLs gelöscht	swa/websiteurlfilte	websiteurlfiltering	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Erstellen von Liste mit blockierten Website-URLs	swa/websiteurlfiltering/blocked/create failed	websiteurlfiltering/blocked/list	Nein	Ja
Fehler beim Aktualisieren von Liste mit blockierten Website-URLs	swa/websiteurlfiltering/blocked/update failed	websiteurlfiltering	Nein	Ja
Fehler beim Löschen von Liste mit blockierten Website-URLs	swa/websiteurlfiltering/blocked/delete failed	websiteurlfiltering/blocked/list	Nein	Ja
Filterkategorie für blockierte Website-URLs erstellt	swa/websiteurlfiltering/blocked/create	websiteurlfiltering	Nein	Ja
Filterkategorie für blockierte Website-URLs aktualisiert	swa/websiteurlfiltering/blocked/update	websiteurlfiltering/blocked/list	Nein	Ja
Filterkategorie für blockierte Website-URLs gelöscht	swa/websiteurlfiltering/blocked/delete	websiteurlfiltering	Nein	Ja
Fehler beim Erstellen von Filterkategorie für blockierte Website-URLs	swa/websiteurlfiltering/blocked/create failed	websiteurlfiltering/blocked/list	Nein	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Fehler beim Aktualisieren von Filterkategorie für blockierte Website-URLs	swa/websiteurlfilt	websiteurlfiltering	Nein	Ja
Fehler beim Löschen von Filterkategorie für blockierte Website-URLs	swa/websiteurlfilter	category/blocked/delete	failed	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/websiteurlfilt	websiteurlfiltering	Nein	Ja
Liste mit zulässigen Website-URLs aktualisiert	swa/websiteurlfilter	websiteurlfiltering/allowed/update	Nein	Ja
Liste mit zulässigen Website-URLs gelöscht	swa/websiteurlfilt	websiteurlfiltering	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/websiteurlfiltering/allowedlist/create/failed	websiteurlfiltering	Nein	Ja
Fehler beim Aktualisieren von Liste mit zulässigen Website-URLs	swa/websiteurlfiltering/allowedlist/update/failed	websiteurlfiltering	Nein	Ja
Fehler beim Löschen von Liste mit zulässigen Website-URLs	swa/websiteurlfiltering/allowedlist/delete/failed	websiteurlfiltering	Nein	Ja
Filterkategorie für zulässige Website-URLs erstellt	swa/websiteurlfiltering/allowedlist/create	websiteurlfiltering	Nein	Ja
Filterkategorie für zulässige Website-URLs aktualisiert	swa/websiteurlfiltering/allowedlist/update	category/allowedlist	Nein	Ja
Filterkategorie für zulässige Website-URLs gelöscht	swa/websiteurlfiltering/allowedlist/delete	websiteurlfiltering	Nein	Ja
Fehler beim Erstellen von Filterkategorie für zulässige Website-URLs	swa/websiteurlfiltering/allowedlist/create/failed	category/allowedlist	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/websiteurlfilt	websiteurlfiltering	Nein	Ja
Fehler beim Löschen von Filterkategorie für zulässige Website-URLs	swa/websiteurlfilter	category/allowedlist	failed	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/redir
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/redir
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-Identitätsanbie aktualisiert	wxp/identitypr	subscriber	Der Administrator, der die Workspace-Authentifizieru aktualisiert hat	Ja	Ja
Fehler beim Aktualisieren des Identitäts-sanbieters	wxp/identityprovider/upda	subscriber	tefailed 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-Verbundauthen (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-Verbundauthen (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/e	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/c	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/disablefailed	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-Kennwortänderung aktualisiert	wxp/changepassword/updatepolicy	subscriber	Der Administrator, der die Richtlinie für die Kennwortänderung in Citrix Workspace aktualisiert hat	Ja	Ja
Fehler beim Aktualisieren der Richtlinie für Workspace-Kennwortänderungsoptionen	wxp/changepassword/updatepolicyfailed	subscriptions	Der Administrator, der versucht hat, die Richtlinie für die Kennwortänderung in Citrix Workspace zu aktualisieren	Ja	Ja

Ereignismeldung	Ereignistyp	Zieltyp	Akteur-ID	Aufzeichnung aktueller Objektfelder vor dem Ereignis	Aufzeichnung aktualisierter Objektfelder nach dem Ereignis
Workspace-Kennwortänderung aktiviert	wxp/changepass	subscriber	Der Administrator, der die Einstellung zum Ändern von Kennwörtern in Citrix Workspace aktiviert hat	Nein	Ja
Fehler beim Aktivieren der Workspace-Kennwortänderungsoptionen	wxp/changepasswordoptions/enable/failed	subscriber	Der Administrator, der versucht hat, die Einstellung zum Ändern von Kennwörtern in Citrix Workspace zu aktivieren	Nein	Ja
Workspace-Kennwortänderung deaktiviert	wxp/changepass	subscriber	Der Administrator, der die Einstellung zum Ändern von Kennwörtern in Citrix Workspace 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-Kennwortänderungsoptionen	wxp/changepasswordoptions/disable/failed	subscriber	Der 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-Tokenkonfigura aktualisiert	wxp/longlivedt	subscriber	Der Administrator, der die Tokenkonfiguration aktualisiert hat	Ja	Ja
Fehler beim Aktualisieren der langlebigen Workspace-Tokenkonfiguration	wxp/longlivedtoken/update/failed	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-Sitzungskonfigu aktualisiert	wxp/sessions/u	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/up	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/featur	subscriber	Der Administrator, der die zugewiesenen Benutzer und Gruppen für den Zugriff auf Aktivitätsfeed-Benachrichtigu in Citrix Workspace aktualisiert hat	Nein	Nein
Fehler beim Zuweisen von Benutzern und Gruppen, die für den intelligenten Workspace aktualisiert wurden	wxp/iws/features/updatebusersgroups/failed	subscriber	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/featur	subscriber	Der Administrator, der Aktivitätsfeed-Benachrichtigu in Citrix Workspace aktiviert hat	Nein	Nein
Fehler beim Aktivieren des intelligenten Workspace	wxp/iws/features/enablefai	subscriber	Der Administrator, der versucht hat, Aktivitätsfeed-Benachrichtigungen in Citrix Workspace zu aktivieren	Nein	Nein
Intelligenter Workspace deaktiviert	wxp/iws/featur	subscriber	Der Administrator, der Aktivitätsfeed-Benachrichtigu in Citrix Workspace deaktiviert hat	Nein	Nein
Fehler beim Deaktivieren des intelligenten Workspace	wxp/iws/features/disablefai	subscriber	Der Administrator, der versucht hat, die Aktivitätsfeed-Benachrichtigungen in Citrix Workspace zu deaktivieren	Nein	Nein

SDKs und APIs

May 13, 2022

Citrix Cloud umfasst mehrere APIs, mit denen Sie Informationen abrufen und komplexe Routineaufgaben automatisieren können:

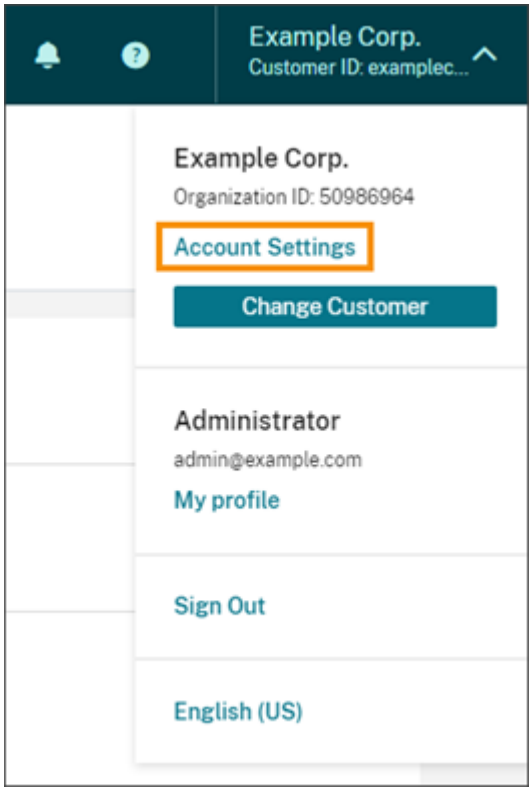
- Automatische Installation von Citrix Cloud Connector
- Erstellen und Nutzen von Berichten für die Verwaltung von Cloud-Lizenzen
- Ermitteln des Anspruchsstatus eines Kunden
- Senden von Benachrichtigungen an Citrix Cloud-Administratoren
- Abrufen von Systemprotokollereignissen
- Abrufen von Details 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.

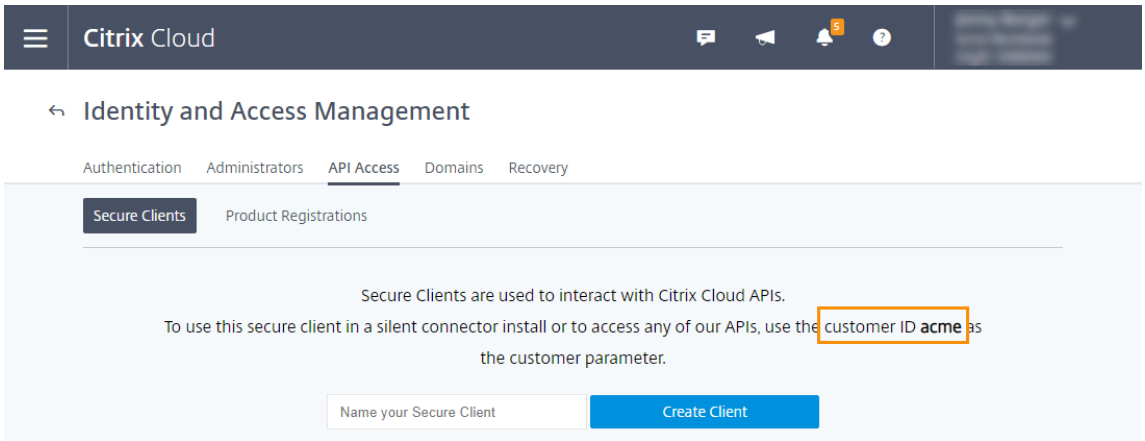
Sichere Clients

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.

Wenn Sie Administrator für mehrere Kunden sind, müssen Sie für jede Kunden-ID eigene sichere

Clients erstellen. Sichere Clients, die Sie unter einer Kunden-ID erstellen, sind für andere Administratoren oder wenn Sie bei einem anderen Kunden angemeldet sind, nicht sichtbar.

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 über diese API finden Sie unter Citrix Cloud - SystemLog in der Citrix Dokumentation für Entwickler.

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 über diese API finden Sie unter Citrix Cloud - Resource Location in der Citrix Dokumentation für Entwickler.

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 über diese API finden Sie unter Citrix Cloud - Service Entitlement in der Citrix Dokumentation für Entwickler.

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, Content Collaboration und Citrix Workspace.
- Digital workspaces: SDKs und APIs für Netzwerk und Anwendungsbereitstellung wie Application Delivery Management, 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

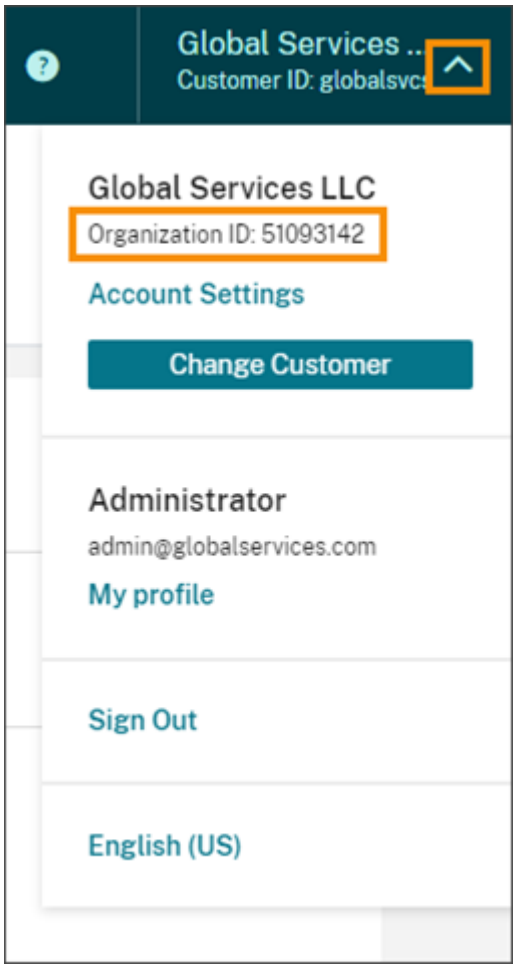
May 13, 2022

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.

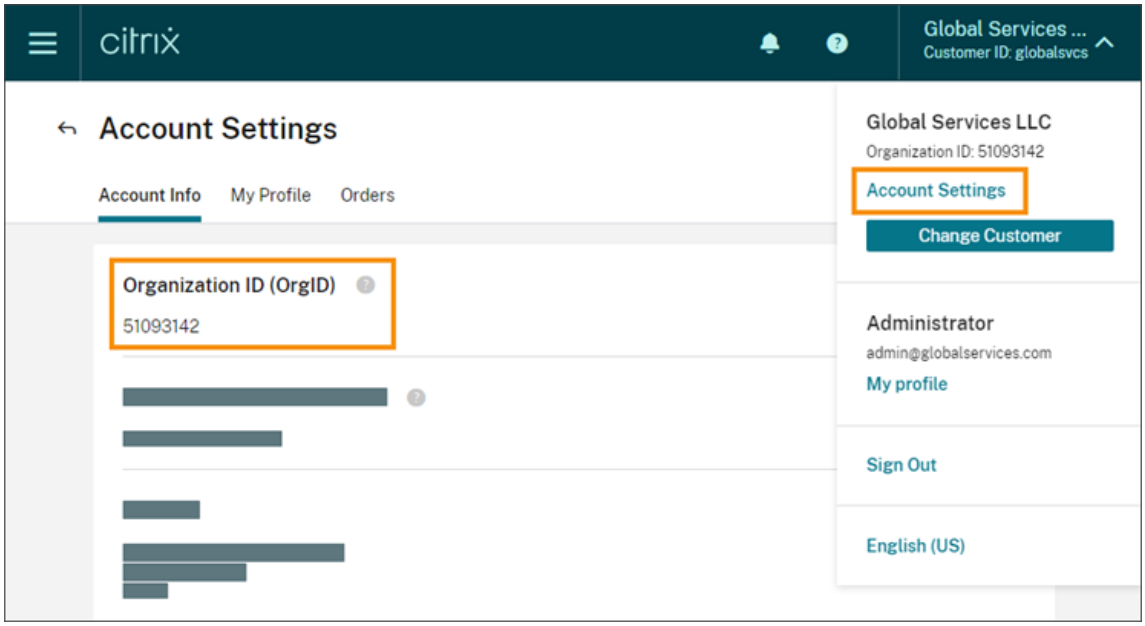
Partneridentifizierung

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:

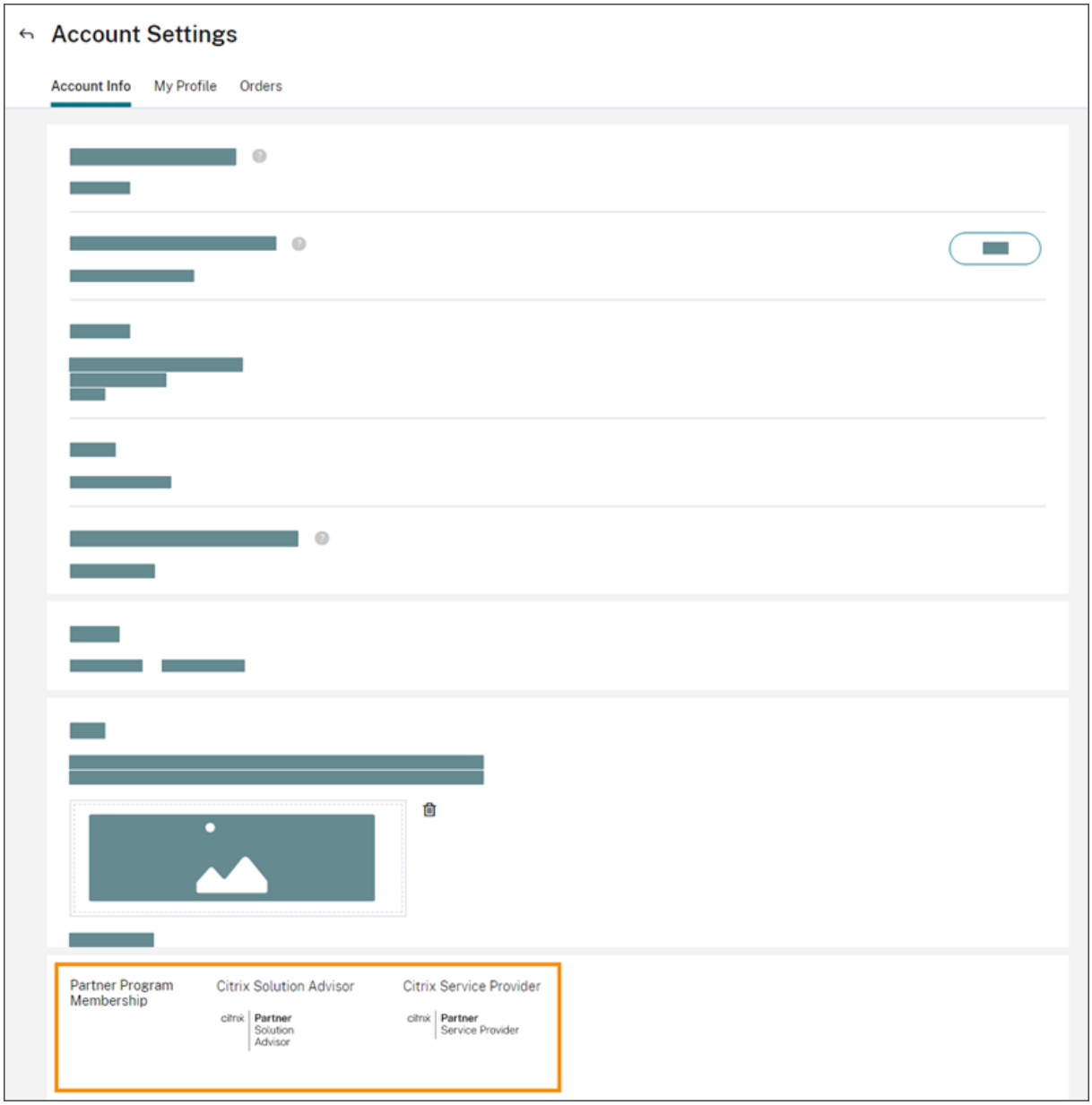
- Über das Kundenmenü: Klicken Sie in der oberen rechten Ecke der Konsole auf Ihren Kundennamen. Ihre ORGID wird unter Ihrem Firmennamen im Menü angezeigt.



- Auf der Seite **Kontoeinstellungen**: Wählen Sie im Kundenmenü in der oberen rechten Ecke **Kontoeinstellungen**.

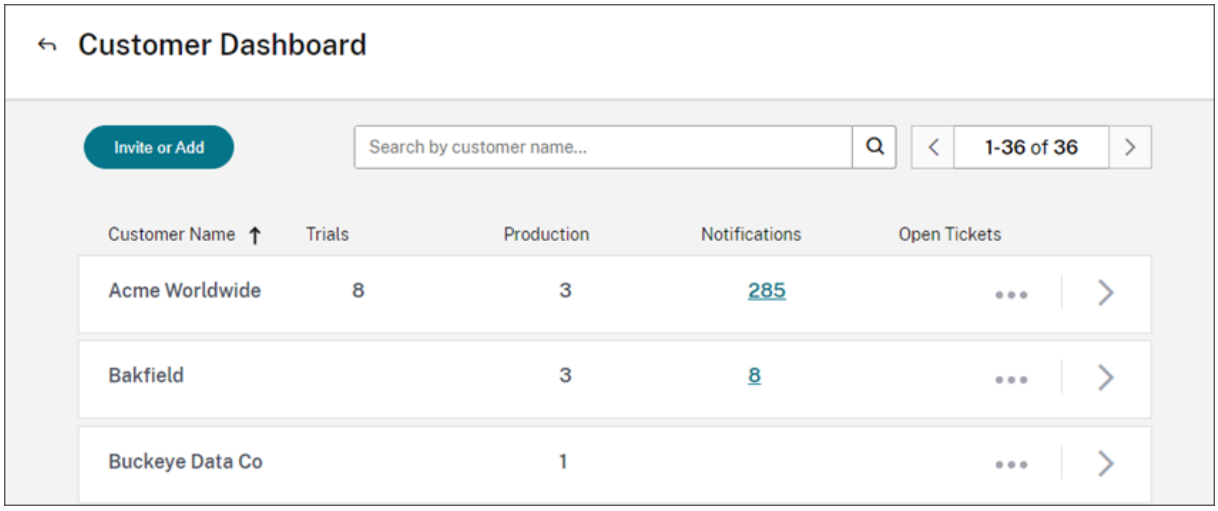


Falls die ORGID im Konto auf ein aktives Mitglied eines Citrix Partnerprogramms verweist (z. B. Citrix Solution Advisor oder Citrix Service Provider), zeigt der Programmbadge an, dass dieses Konto einem Citrix Partner gehört. Die Partneridentifizierung kann dann verwendet werden, um den Zugriff auf zusätzliche Services oder Features in der Cloud zu steuern.

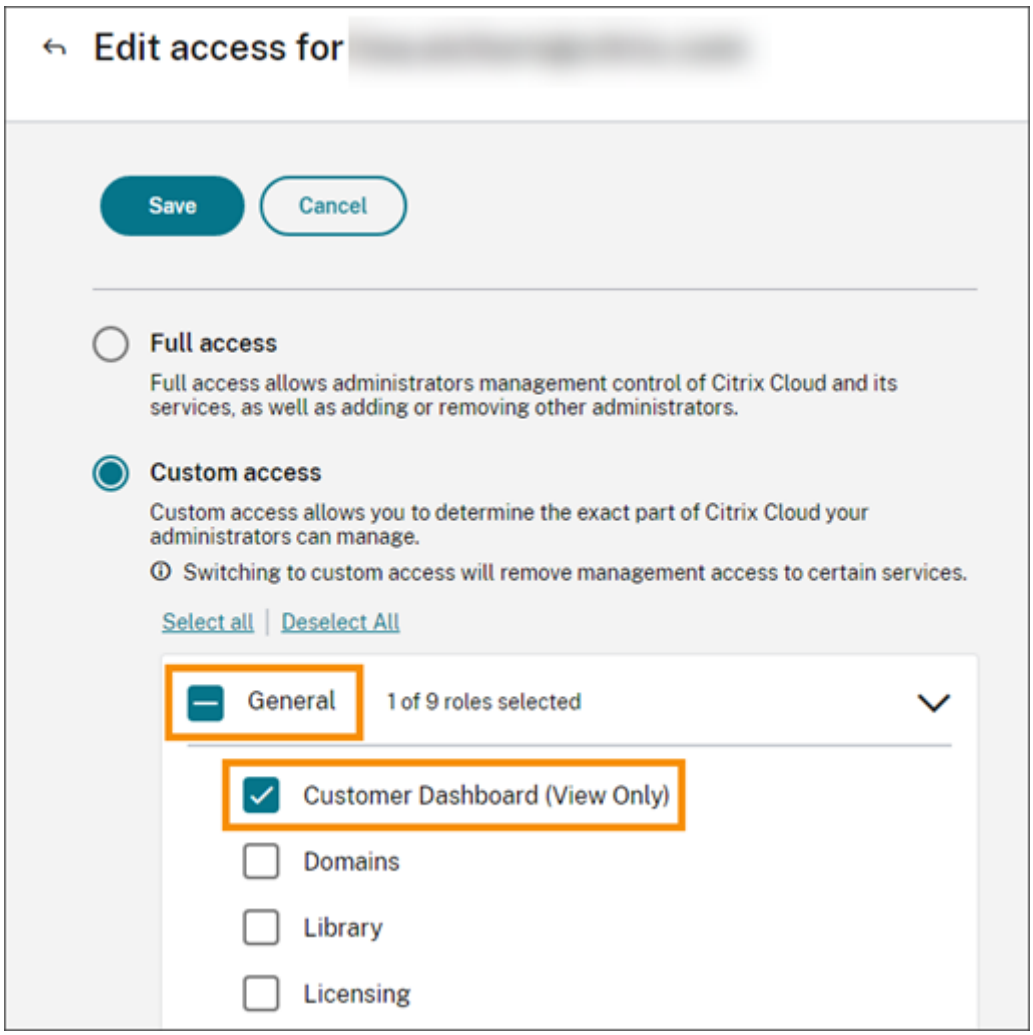


Kundendashboard

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.



Verbinden 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 der Kunde der Verbindung zugestimmt 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

Weitere Informationen über Partnerverbindungen:

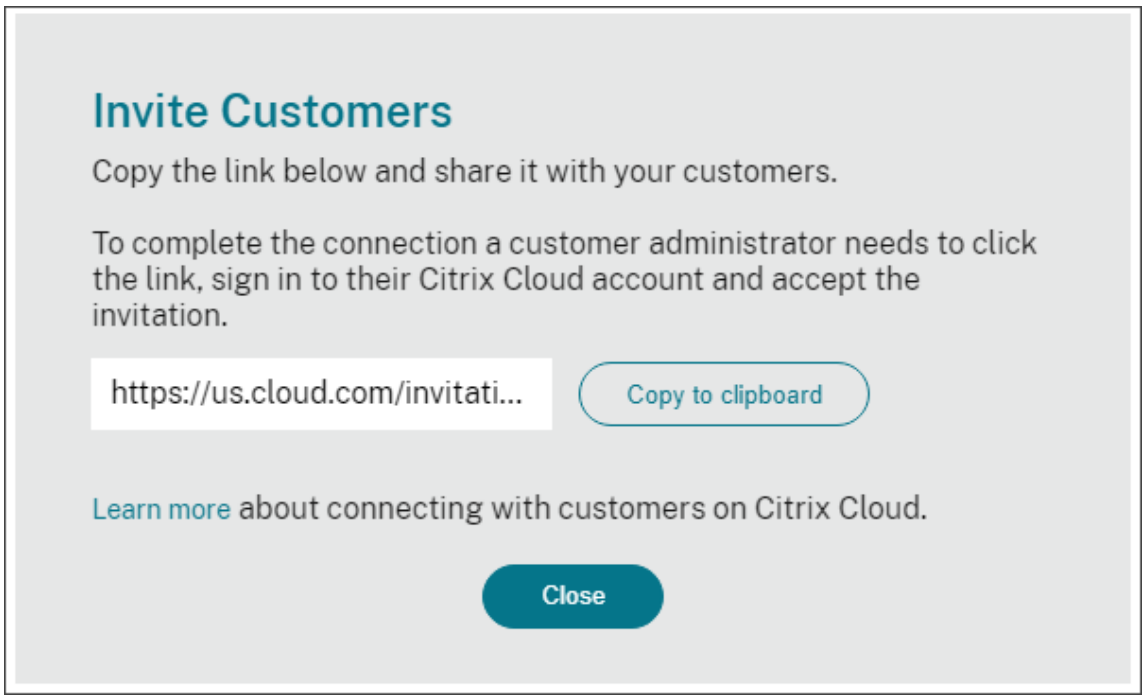
- Partner können Verbindungen mit mehreren Kunden herstellen.
- Kunden können Verbindungen mit mehreren Partnern herstellen.
- Es gibt keine Höchstgrenze für Verbindungen zwischen Kunden und Partnern.
- Verbindungen können jederzeit durch Kunden oder Partner beendet werden.
  - vom Kunden auf ihrer Kontodetailseite
  - vom Partner über das Kundendashboard
- Citrix Cloud-Benachrichtigungen werden je nach Verbindungsworkflow gesendet
  - Der Partner wird benachrichtigt, wenn eine Verbindung vom Kunden hergestellt wird
  - Der Partner wird benachrichtigt, wenn die Verbindung vom Kunden beendet wird
  - Der Kunde wird benachrichtigt, wenn die Verbindung vom Partner beendet wird.
- Die Anzeige von Lizenzierungen beschränkt sich auf Zusammenfassungen der Lizenzzuweisungen und historische Nutzungstrends
- Verbindungen zwischen Partner und Kunden laufen nicht ab.

Sobald die Verbindung zwischen dem Partner und einem Kunden hergestellt ist, können die Partneradministratoren grundlegende Kontoinformationen des Kunden und die von diesem aufgegebenen Bestellungen sowie Berechtigungsinformationen wie Services, Lizenzzahlen und Ablaufdaten anzeigen.

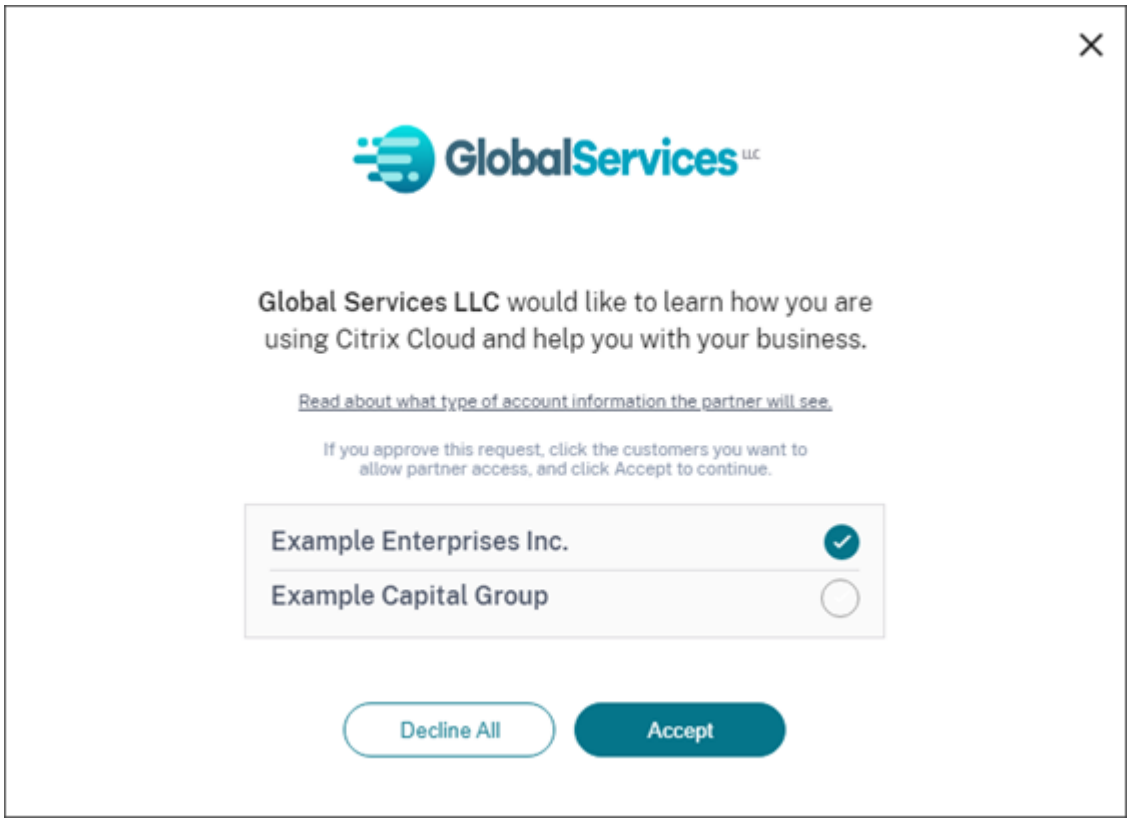
Senden einer Verbindungseinladung an einen Kunden

Die Verbindung eines Partners mit einem Kunden erfolgt über drei einfache Schritte:

1. Der Partner ruft den Einladungslink vom Kundendashboard ab Wählen Sie **Einladen oder hinzufügen** und geben Sie an, ob der Kunde ein Citrix Cloud-Konto hat oder ein Onboarding erforderlich ist. Ist ein Onboarding erforderlich, geben Sie seine Geschäftskontaktdaten an, um eine Citrix Cloud für den Kunden zu erstellen. Danach erscheint die Einladung.



2. Der Partner kopiert den Einladungslink und sendet ihn an den Kunden
3. Der Kunde klickt auf den Link, meldet sich an (oder registriert sich) und akzeptiert die Verbindungsanfrage



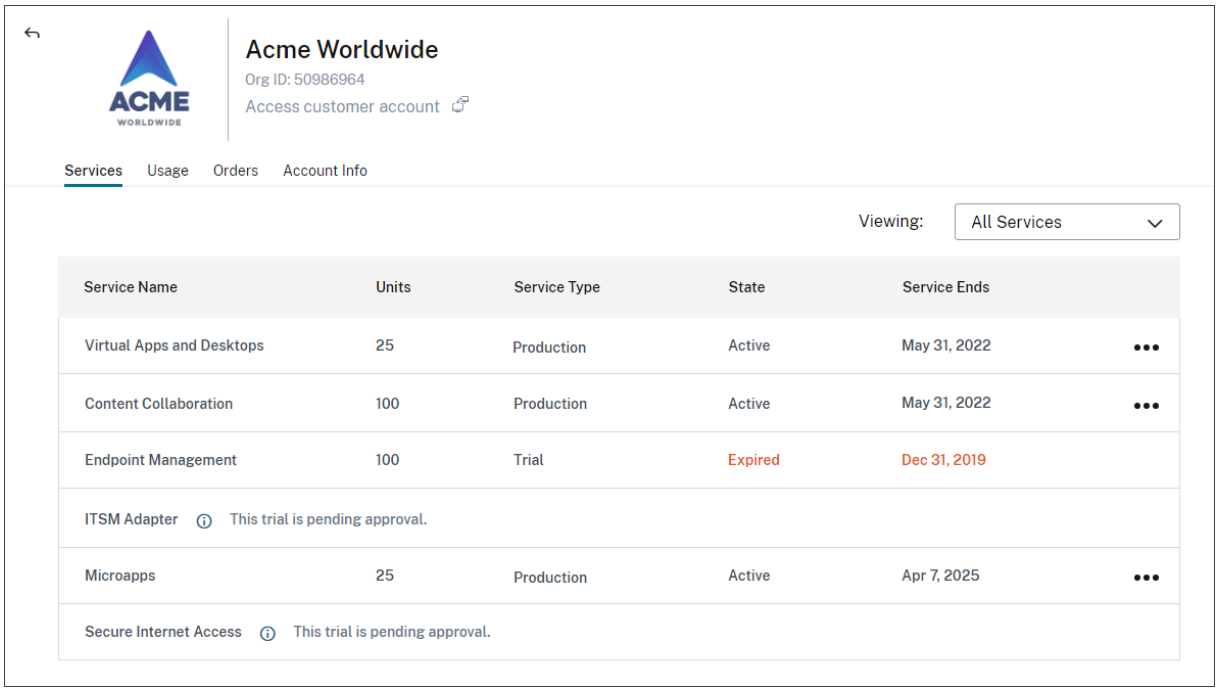
Weitere Informationen über Partnereinladungslinks:

- Partner erhalten einen Einladungslink. Der Link ist fest und kann nicht verändert werden.
- Der Link kann beliebig oft zum Herstellen einer Verbindung verwendet werden.
- Der Link kann wiederverwendet werden, wenn eine Verbindung neu hergestellt werden muss.
- Der Link läuft nicht ab.

Der Partner erhält Einblick in die Citrix Cloud-Serviceansprüche

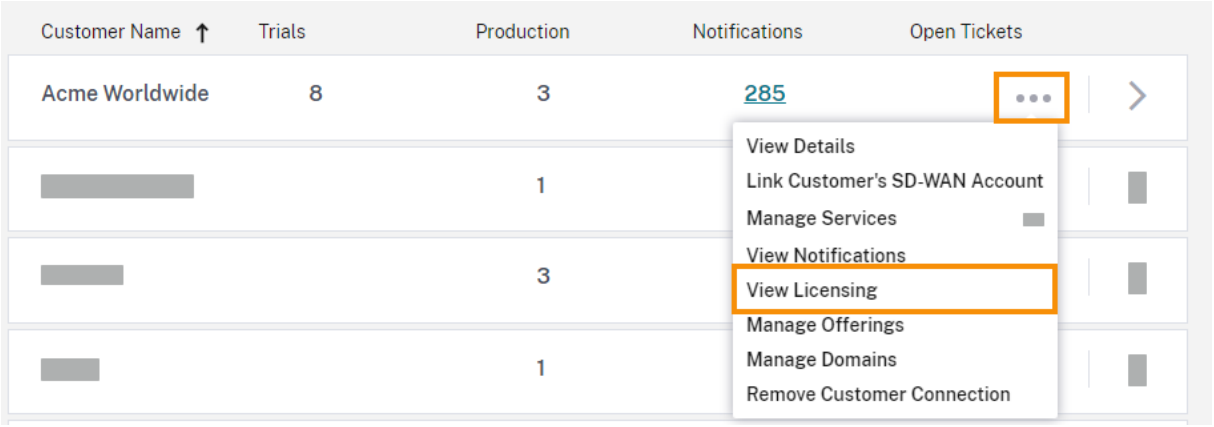
Wenn ein Kunde die Verbindungseinladung eines Citrix Partners akzeptiert, kann dieser grundlegende Daten zum Citrix Cloud-Servicesanspruch für diesen Kunden anzeigen. Zu diesen Informationen gehören der Status von Testversions- und Nicht-Testversionsansprüchen. Weitere Informationen, einschließlich:

- 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



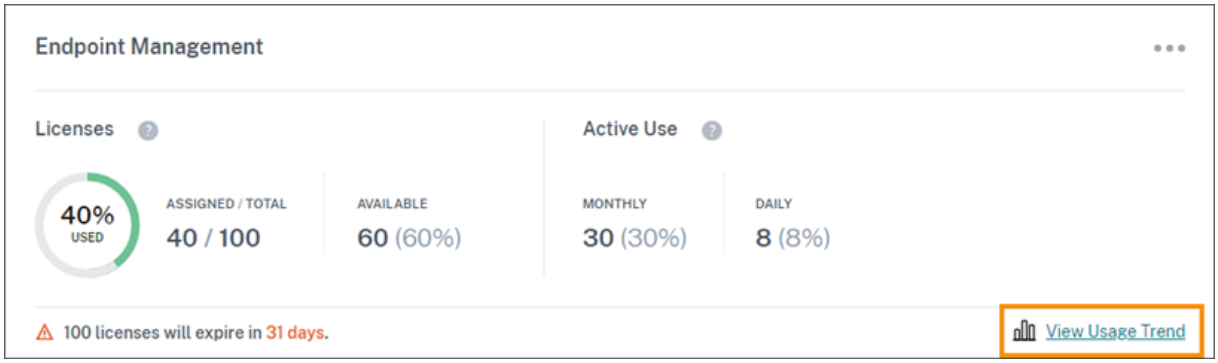
Lizenzierungstrends

Partner können Lizenzierungsinformationen im Kundendashboard anzeigen, indem sie auf die Auslassungspunkte für den Kunden klicken und **Lizenzierung anzeigen** auswählen.

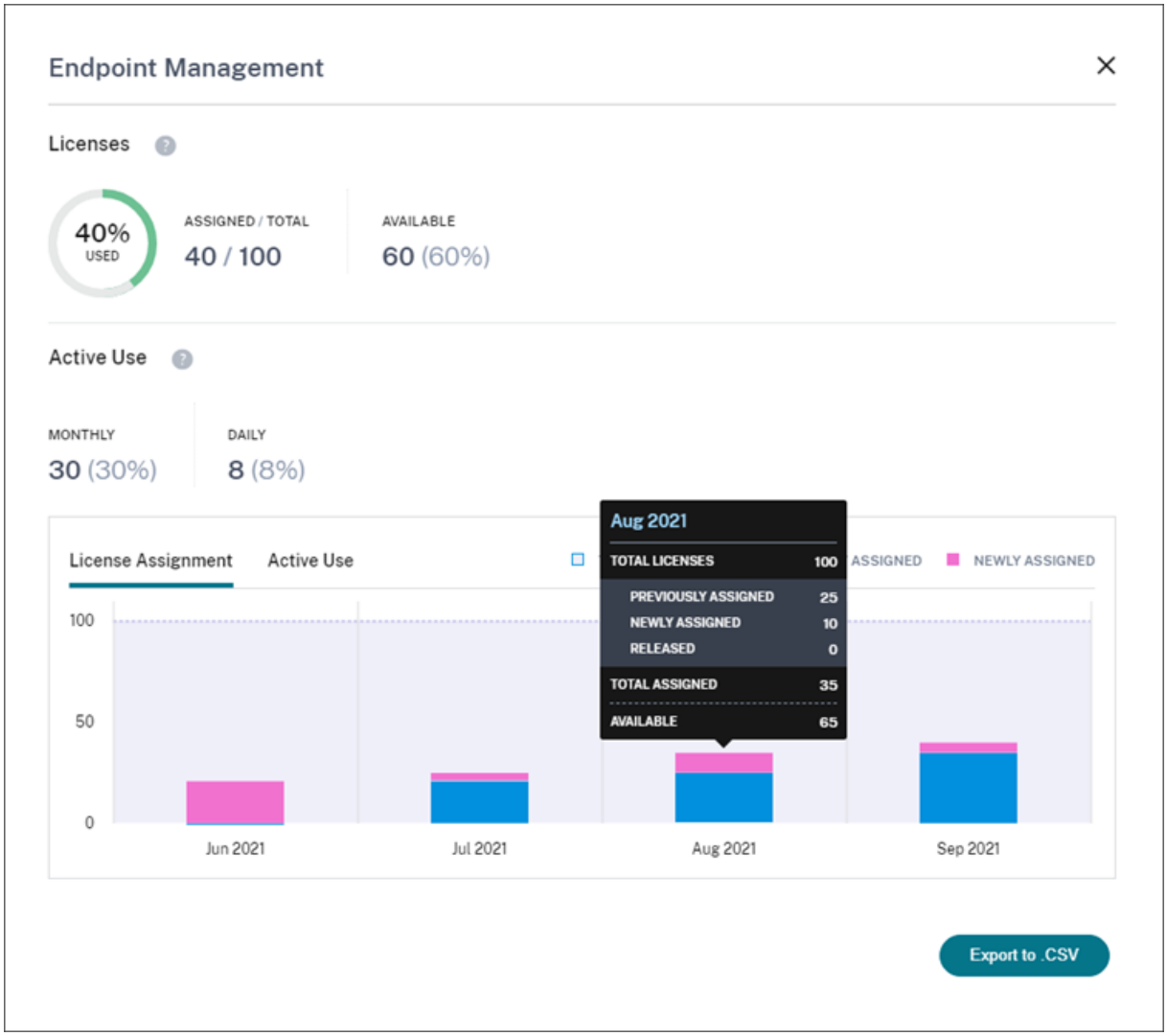


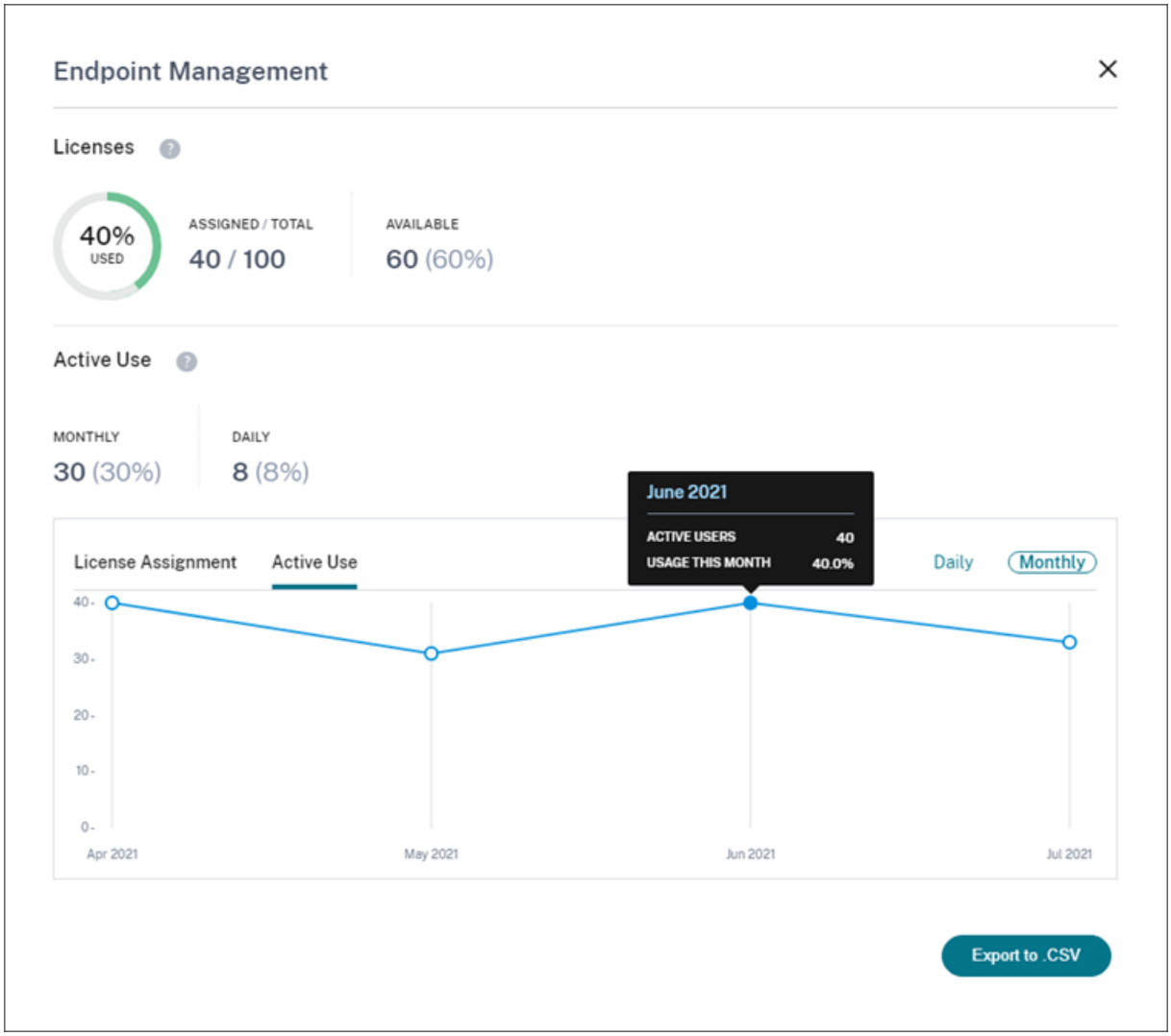
> **Hinweis:**
>
> Citrix Partner können nur die Zusammenfassung unter “Lizenzierung” sowie historische Trends der aktiven Nutzung anzeigen. Sie können keine einzelnen Benutzer, die Lizenzen für einen bestimmten Service verwenden, anzeigen.

Um eine Zusammenfassung anzuzeigen, wählen Sie auf der Registerkarte **Nutzung** der Kundenseite die Option **Nutzungstrend anzeigen** aus.



Die Zusammenfassung enthält das Verhältnis der zugewiesenen Lizenzen zur Gesamtmenge, die Aufschlüsselung der zugewiesenen Lizenzen und aktive Benutzer pro Monat und Tag. Bei Bedarf können diese Informationen als CSV-Datei exportiert werden.





Kundenlizenzierung und Lizenznutzung für Citrix Service Provider

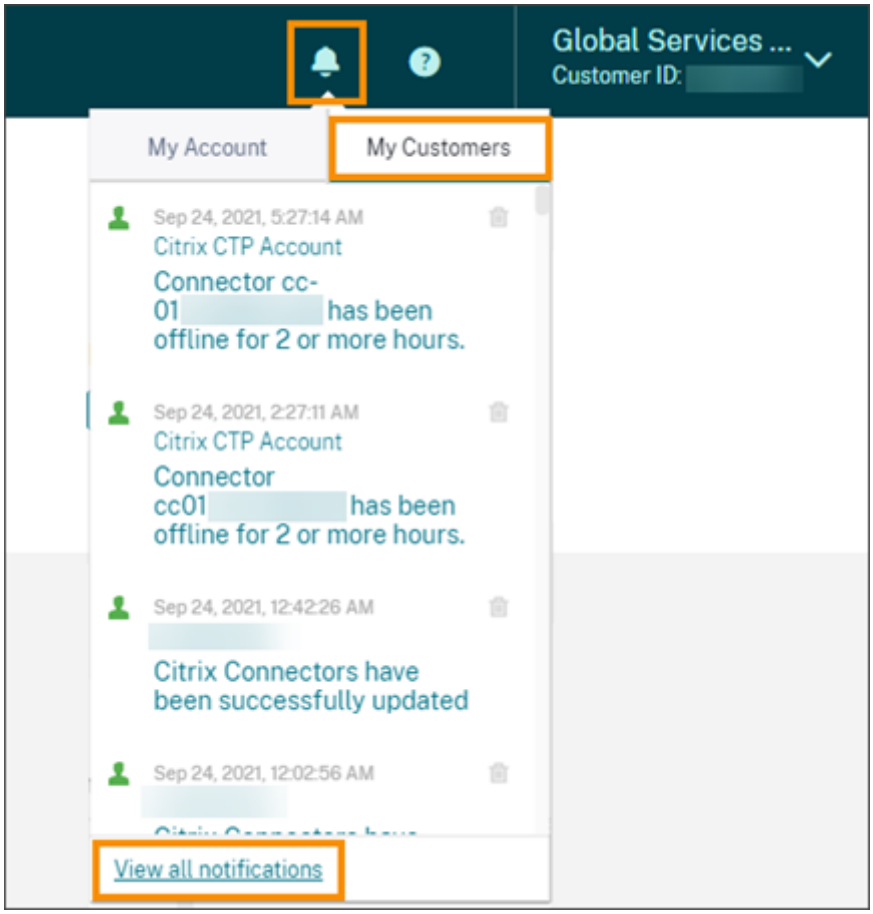
Die Lizenzierungsfunktion in Citrix Cloud ermöglicht Kunden von Citrix Service Providern (CSP) die Überwachung ihrer Lizenzen und des Lizenzverbrauchs für unterstützte Citrix DaaS-Produkte (früher Citrix Virtual Apps and Desktops). CSPs können sich unter dem Citrix Cloud-Konto ihres Kunden anmelden, 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

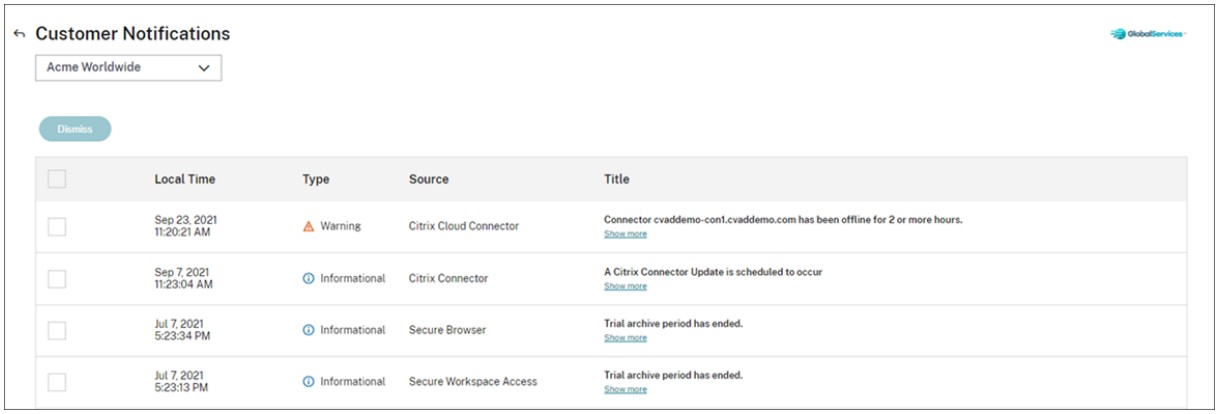
Sichtbarkeit von Supporttickets und Benachrichtigungen der Kunden für Partner

Partner können Supporttickets und 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.

Um Kundenbenachrichtigungen anzuzeigen, klicken Sie auf das Glockensymbol oben in der Verwaltungskonsole und wählen Sie **Meine Kunden** und dann **Alle Benachrichtigungen anzeigen**.



Wählen Sie im Dropdownmenü einen Kunden aus, um dessen Benachrichtigungen anzuzeigen.



Die Anzeige der Supporttickets für Kunden hilft Partnern beim Lösen von Problemen für ihre Kunden, wodurch eine optimierte und fehlerfreie Benutzererfahrung ermöglicht wird.

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.

Citrix Cloud Services

October 16, 2022

In diesem Artikel werden die Dienste aufgeführt, die Citrix über Citrix Cloud anbietet. Darüber hinaus finden Sie hier Links zur Produktdokumentation für jeden Dienst. Beschreibungen dieser Dienste und der Citrix-Angebote, in denen sie enthalten sind, finden Sie unter Service Descriptions for Citrix Services.

Analytics

- Analytics for Security
- Analytics for Performance
- Analytics – Usage

App Builder

Application Delivery Management

App Delivery and Security

Content Collaboration

- Erstellen oder Verknüpfen eines Content Collaboration (ShareFile)-Kontos mit Citrix Cloud
- ShareFile einrichten

Citrix DaaS (früher “Citrix Virtual Apps and Desktops Service”)

Citrix DaaS Standard für Azure (früher Citrix Virtual Apps and Desktops Standard für Azure)

Endpoint Management

Gateway

Hypervisorverwaltung

ITSM-Adapter für ServiceNow

Managed Desktops (Neuer Name: Citrix DaaS Standard für Azure)

MDX Service

SD-WAN Orchestrator

Remote Browser Isolation

Secure Internet Access

Secure Private Access

Sitzungsaufzeichnungsdienst

Virtual Apps Essentials

Virtual Desktops Essentials

Web App Firewall

Workspace Environment Management

Erweiterte Konzepte

February 1, 2022

Der Abschnitt “Erweiterte Konzepte” der Website mit der Citrix Cloud-Dokumentation enthält eine Auswahl an technischen Artikeln von Citrix Teams. Die Artikel enthalten ausführliche Anleitungen für die Bereitstellung wichtiger Komponenten, anhand derer Sie Apps und Daten sicher und zuverlässig bereitstellen können.

Ausführlichere technische Artikel, Referenzarchitekturen und Empfehlungen zu bewährten Methoden von Citrix Technologieexperten finden Sie in der Citrix Tech Zone.

Community-Supportforen rund um die Citrix Cloud-Plattform und -Dienste finden Sie unter Citrix Discussions.

Referenzarchitekturen der StoreFront-Authentifizierung im eigenen Rechenzentrum für Citrix DaaS

May 13, 2022

Es gibt verschiedene Gründe, Citrix StoreFront im eigenen Rechenzentrum zu hosten, statt die Citrix Workspace-Plattform zu nutzen. Angesichts der Komplexität einiger Umgebungen ist es wichtig zu wissen, wie Citrix Cloud-Komponenten mit StoreFront und Active Directory interagieren, wenn StoreFront als primäres Benutzerfrontend für den Dienst fungiert.

Citrix Workspace erfüllt zwar die Anforderungen der meisten Anwendungsfälle von Citrix DaaS (früher Citrix Virtual Apps and Desktops Service), in Einzelfällen muss jedoch StoreFront im Rechenzentrum oder an Ressourcenstandorten des Kunden gehostet werden.

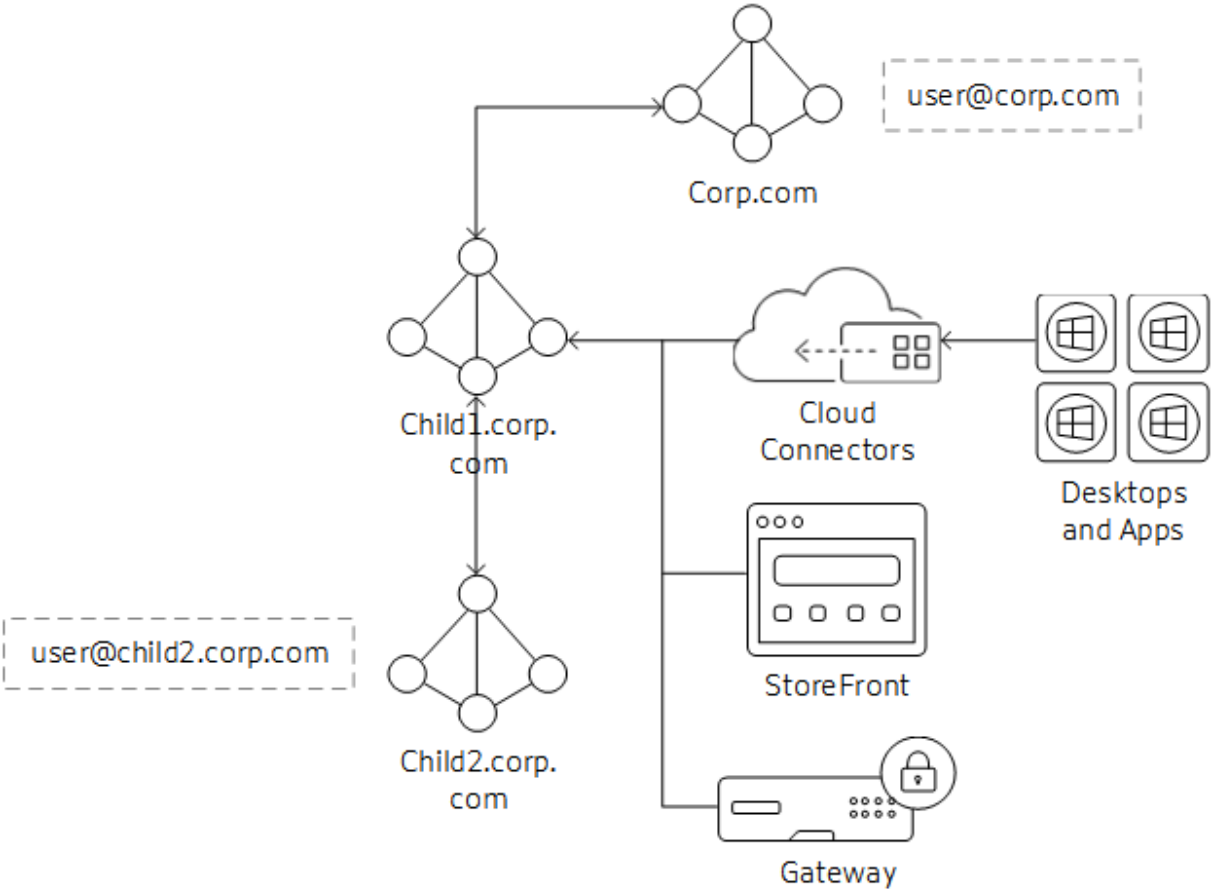
Gründe für das Hosten von StoreFront im eigenen Rechenzentrum

- Unterstützung der lokalen Hostcache-Funktionalität in Cloud Connectors
- Citrix Workspace unterstützt keine Authentifizierung per Smartcard
- Nicht standardmäßige Store-Konfigurationen (Änderungen in web.config)
- Hosting mehrerer Store-Konfigurationen für interne und externe Benutzer

Dieser Artikel enthält einen Überblick über die Architekturen und die Interaktion der Komponenten mit verschiedenen, von Active Directory-Designs unterstützten Authentifizierungsszenarien. Cloud Connectors treten einer Domäne bei und ermöglichen Citrix DaaS die Active Directory-Zuweisung von Benutzern und Gruppen der Domäne bzw. vertrauenswürdiger Domänen. Die Cloud Connectors fungieren außerdem als Delivery Controller und STA-Server für StoreFront- und Citrix Gateway-Komponenten.

In diesem Artikel wird davon ausgegangen, dass StoreFront- und Gateway-Komponenten im selben Rechenzentrum gehostet werden.

Übergeordnete und untergeordnete Domänen als Ressourcendomänen



In diesem Szenario fungiert die untergeordnete Domäne als Ressourcendomäne für Virtual Desktop

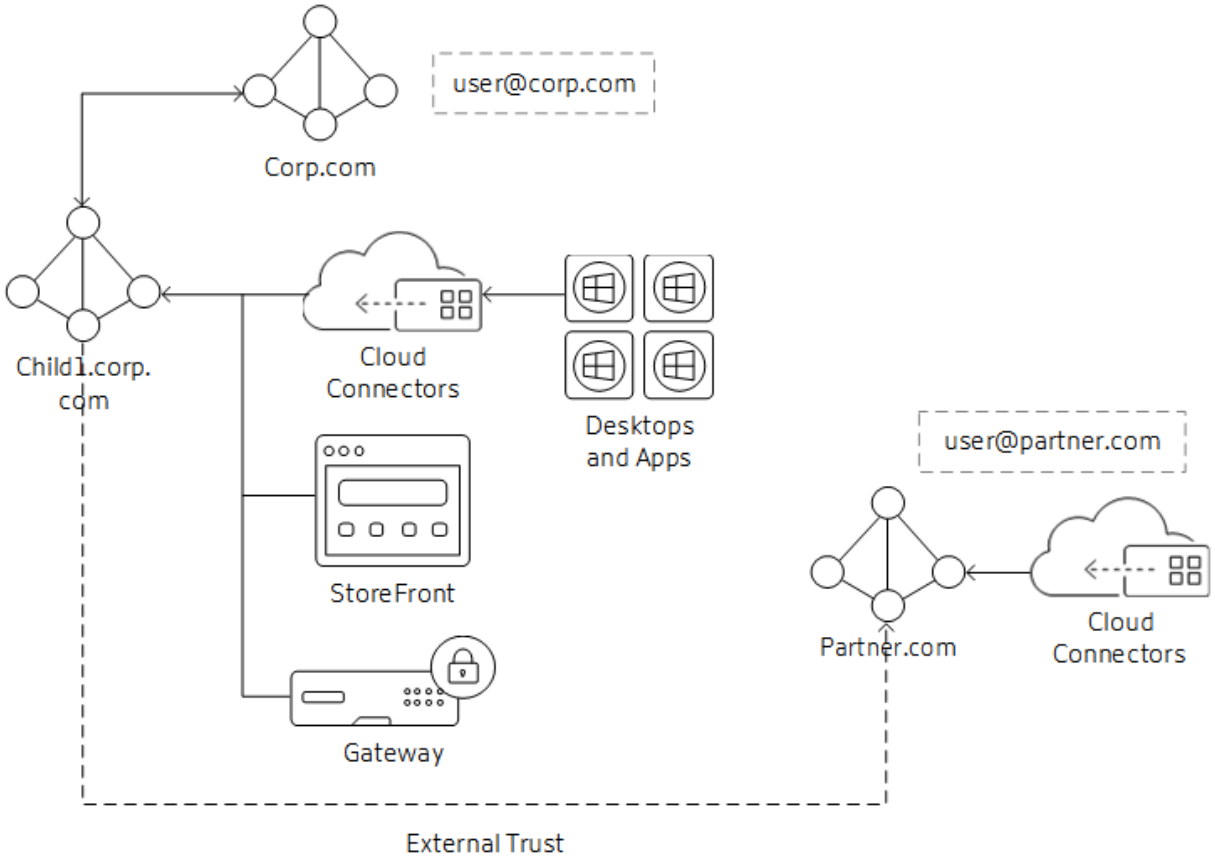
Agents (VDAs) und StoreFront-Instanzen. Die übergeordnete Domäne enthält die Benutzer, die auf die Ressourcen in der untergeordneten Domäne zugreifen.

1. Cloud Connectors treten nur der untergeordneten Domäne bei. Die bidirektionale, transitive Vertrauensstellung zwischen untergeordneter und übergeordneter Domäne ermöglicht dem Cloud Connector die Kommunikation mit dem globalen Katalog in der übergeordneten Domäne.
2. StoreFront gehört der untergeordneten Domäne an. Die Store-Authentifizierung ist für Benutzername/Kennwort und Passthrough von Citrix Gateway konfiguriert. Die Benutzername/Kennwort-Authentifizierung ist so konfiguriert, dass jeder Domäne vertraut wird.
3. Das Citrix Gateway-Authentifizierungsprofil ist so konfiguriert, dass die übergeordnete Domäne den UPN als primäre Anmeldemethode verwendet. Müssen sich auch Benutzer aus der untergeordneten Domäne authentifizieren, dann müssen LDAP-Authentifizierungsprofil und -richtlinie für die untergeordnete Domäne ebenfalls an den virtuellen Gateway-Server gebunden sein.
4. Bearbeiten Sie die Citrix Gateway-Sitzungsbetriebssystem- und Webprofile und legen Sie die Option “Published Applications/Single Sign-On” auf leer fest (möglicherweise muss eine Außerkraftsetzung festgelegt werden).

Verbindungsworkflow

1. User@corp.com meldet sich bei Citrix Gateway an. Gateway sucht den Benutzer anhand des Authentifizierungsprofils und wählt die Richtlinienaktion.
2. Die Anmeldeinformationen werden an StoreFront übergeben. StoreFront akzeptiert die Anmeldeinformationen und übergibt sie an die Cloud Connectors (die als Delivery Controller fungieren).
3. Die Cloud Connectors suchen die von Citrix Cloud benötigten Benutzerobjektdetails.
4. Die Cloud Connectors übergeben die Identitätsinformationen an Citrix Cloud, der Benutzer wird durch Identitätstoken authentifiziert und ihm zugewiesenen Ressourcen werden aufgelistet.
5. Die Cloud Connectors geben die zugewiesenen Ressourcen an StoreFront zurück, damit sie für den Benutzer aufgelistet werden.
6. Wenn der Benutzer eine Anwendung oder einen Desktop startet, generiert Citrix Gateway mithilfe der konfigurierten Cloud Connectors eine STA-Ticketanforderung.
7. Die Citrix Cloud-Broker verwalten die Sitzungen zwischen der Ressourcendomäne und den Cloud Connectors und VDAs, die am Ressourcenstandort registriert sind.
8. Die Sitzung wird zwischen Client, Citrix Gateway und dem aufgelösten VDA eingerichtet.

Externe vertrauenswürdige Domänen an Ressourcendomäne



In diesem Szenario benötigt ein Geschäftspartner Zugriff auf für Unternehmensbenutzer veröffentlichte Ressourcen. Die Unternehmensdomäne ist corp.com und die Partnerdomäne ist partner.com.

1. Die Unternehmensdomäne hat eine ausgehende Vertrauensstellung zur Partnerdomäne. Die Benutzer der Partnerdomäne können sich bei Ressourcen in der Unternehmensdomäne authentifizieren.
2. Der Citrix Cloud-Kunde benötigt zwei Ressourcenstandorte: einen für corp.com-Cloud Connectors und den zweiten für partner.com-Cloud Connectors. Die partner.com-Cloud Connectors werden nur für Authentifizierungs- und Identitätsaufrufe an die Domäne benötigt. Sie verhandeln keine VDAs oder Sitzungen.
3. StoreFront gehört der Domäne corp.com an. Die Cloud Connectors in der Domäne corp.com werden als Delivery Controller in der Store-Konfiguration verwendet. Die Store-Authentifizierung ist für Benutzername/Kennwort und Passthrough von Citrix Gateway konfiguriert. Die Benutzername/Kennwort-Authentifizierung ist so konfiguriert, dass jeder Domäne vertraut wird.
4. Das Citrix Gateway-Authentifizierungsprofil ist so konfiguriert, dass die Domäne corp.com den UPN als primäre Anmeldemethode verwendet. Konfigurieren Sie ein zweites Profil und eine

zweite Richtlinie für die Domäne partner.com zur Verwendung des UPN und binden Sie diese an denselben virtuellen Gateway-Server wie für die Domäne corp.com.

5. Bearbeiten Sie die Citrix Gateway-Sitzungsbetriebssystem- und Webprofile und legen Sie die Option “Published Applications/Single Sign-On” auf leer fest (möglicherweise muss eine Außerkraftsetzung festgelegt werden).

> **Hinweis:**
>
> Abhängig vom Standort der externen vertrauenswürdigen Domäne sind die Startzeiten für die externen Domänenbenutzer möglicherweise länger als für Benutzer in der übergeordneten Domäne.

Verbindungsworkflow

1. User@partner.com meldet sich bei Citrix Gateway an. Gateway sucht anhand des Authentifizierungsprofils den Benutzer, der dem UPN entspricht, und wählt die Richtlinienaktion.
2. Die Anmeldeinformationen werden an StoreFront übergeben. StoreFront akzeptiert die Anmeldeinformationen und übergibt sie an die Cloud Connectors (die als Delivery Controller fungieren).
3. Die Cloud Connectors suchen die von Citrix Cloud benötigten Benutzerobjektdetails.
4. Die Cloud Connectors übergeben die Identitätsinformationen an Citrix Cloud, der Benutzer wird durch Identitätstoken authentifiziert und ihm zugewiesenen Ressourcen werden aufgelistet.
5. Die Cloud Connectors geben die zugewiesenen Ressourcen an StoreFront zurück, damit sie für den Benutzer aufgelistet werden.
6. Wenn der Benutzer eine Anwendung oder einen Desktop startet, generiert Citrix Gateway mithilfe der konfigurierten Cloud Connectors (in diesem Fall aus child1.corp.com) eine STA-Ticketanforderung.
7. Die Citrix Cloud-Broker verwalten die Sitzungen zwischen der Ressourcendomäne und den Cloud Connectors und VDAs, die am Ressourcenstandort registriert sind.
8. Die Sitzung wird zwischen Client, Citrix Gateway und dem aufgelösten VDA eingerichtet.

Gesamtstruktur-/Verknüpfungsvertrauensstellungen an Ressourcendomänen

Domänen mit Gesamtstruktur- oder Verknüpfungsvertrauensstellung werden nur unterstützt, wenn sie als externe Domänenvertrauensstellung zur Ressourcendomäne behandelt werden. Für Gesamtstruktur-Vertrauensstellungen gilt das unter Externe vertrauenswürdige Domänen an Ressourcendomäne beschriebene Verfahren. Der Inhalt dieses Abschnitt kann sich künftig ändern, je nachdem wie native Gesamtstruktur-Vertrauensstellungen zwischen Benutzer- und Ressourcendomänen/-gesamtstrukturen unterstützt werden können.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States