



# Citrix Gateway Service

**Machine translated content**

## **Disclaimer**

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

## Contents

<b>Versionshinweise</b>	<b>2</b>
<b>Beginnen Sie mit Citrix Gateway Service</b>	<b>7</b>
<b>Technische Sicherheit</b>	<b>8</b>
<b>Routing für geografische Standorte —Tech Preview</b>	<b>12</b>
<b>Migrieren Sie NetScaler Gateway zu Citrix Gateway Service für HDX Proxy</b>	<b>14</b>
<b>HDX Adaptive Transport mit EDT-Unterstützung für Citrix Gateway Service</b>	<b>20</b>
<b>Citrix Gateway-Dienst auf der Google Cloud Platform</b>	<b>24</b>
<b>Unterstützung für Citrix Virtual Apps and Desktops</b>	<b>25</b>
<b>Citrix Gateway Service für StoreFront – Preview</b>	<b>27</b>
<b>Häufig gestellte Fragen</b>	<b>40</b>

## Versionshinweise

June 4, 2024

In den Versionshinweisen zum Citrix Gateway Service Release zu Cloud werden die neuen Funktionen, Verbesserungen vorhandener Funktionen, behobene Probleme und bekannte Probleme beschrieben, die in einer Serviceversion verfügbar sind. Die Versionshinweise enthalten einen oder mehrere der folgenden Abschnitte:

**Neue Features:** Neue Funktionen und Verbesserungen in der aktuellen Version verfügbar.

**Behobene Probleme:** Probleme, die in der aktuellen Version behoben wurden.

**Bekannte Probleme:** Probleme in der aktuellen Version und deren Workarounds, sofern zutreffend.

### April 25, 2024

#### Was ist neu

- **Citrix Gateway Service für StoreFront – Preview**

Citrix Gateway Service for StoreFront ist eine cloudbasierte HDX-Lösung, die sicheren Remotezugriff auf Ressourcen bietet, auf die über StoreFront on-premises zugegriffen wird. Sie können die Skalierbarkeit und Zuverlässigkeit von Citrix Cloud (für HDX-Proxy) nutzen, ohne Ihre on-premises StoreFront- und On-Premises NetScaler Gateway-Umgebungen zu ändern.

Diese Lösung befindet sich im Preview. Einzelheiten finden Sie unter [Citrix Gateway Service für StoreFront – Preview](#).

### April 24, 2024

#### Was ist neu

- **Unterstützung des Verlusttoleranzmodus für Audiorichtlinien**

Citrix Gateway Service unterstützt jetzt den neuesten verlusttoleranten Modus für die Audiorichtlinie von Citrix Virtual Apps and Desktops. Dieser Modus verbessert das Audioerlebnis für Benutzer, die eine Verbindung zu Netzwerken mit hoher Latenz und Paketverlust herstellen. Benutzer müssen Citrix Virtual Apps and Desktops 7 2402 LTSR oder höhere Versionen verwenden, um diese Funktionalität nutzen zu können.

Der verlusttolerante Modus für Audiorichtlinien basiert auf dem EDT-Transportprotokoll Lossy. EDT Lossy ist ein verlusttolerantes Transportprotokoll, das Paketverluste bei der Übertragung ohne erneutes Senden von Multimediainhalten toleriert und so für ein eher echtzeitähnliches Erlebnis sorgt. Es ist auch der bevorzugte Audiomodus, der im Vergleich zu EDT bei verlustbehafteten Netzwerkbedingungen eine überlegene Audioqualität gewährleistet.

Einzelheiten zu den Einstellungen für den verlusttoleranten Modus finden Sie unter [Verlusttoleranter Modus für Audio](#).

## April 19, 2024

### Was ist neu

- **Unterstützung für Toronto (Kanada) Azure POP**

Unterstützung für Azure POP in Toronto, Kanada, ist jetzt verfügbar.

**POP-FQDN:** `az-ca-c-rdvz.g.nssvc.net`

Einzelheiten finden Sie unter [Geo-Location-Routing – Preview](#).

[CGS-12933]

## 27. Februar 2024

### Was ist neu

- **Unterstützung für Google Cloud Platform**

Die Unterstützung von Google Cloud Platform (GCP) PoPs zusammen mit den vorhandenen Azure- und AWS-POPs ist in den kommenden Service Releases geplant.

Derzeit gibt es 5 GCP-POPs, die über geografische Standorte verteilt sind. Mit dieser bevorstehenden Unterstützung können Sie diese GCP-POPs zusammen mit den vorhandenen Azure- und AWS-POPs nutzen.

**Wichtig:**

Um den kontinuierlichen Betrieb Ihrer Citrix DaaS-Bereitstellung sicherzustellen, führen Sie die in [Citrix Gateway Service – POPs](#)) angegebenen Anweisungen vor dem 15. März 2024 aus.

## February 01, 2024

### Was ist neu

- **Unterstützung für Toronto (Kanada) Azure POP**

Die Unterstützung von Azure POP in Toronto, Kanada, ist in den kommenden Service Releases geplant.

**POP-FQDN:** `az-ca-c-rdvz.g.nssvc.net`

[CGS-12933]

## 02. November 2023

### Was ist neu

- **Unterstützung für die neueste Version von Reducer for HDX**

Citrix Gateway Service unterstützt die neueste Version des Reducers für HDX. Reducer for HDX ist ein Allzweckkompressor, der über virtuelle Kanäle hinweg funktioniert. Der neueste Reducer verbessert die Gesamtleistung von Citrix DaaS mit den folgenden Funktionen:

- Reduziert die Netzwerkbandbreitennutzung für HDX-Sitzungen.
- Datenpakete werden in kürzerer Zeit übertragen, was zu einer schnelleren Antwort führt.

Die folgenden Softwareversionen unterstützen den neuesten Reducer.

- Citrix Virtual Apps and Desktops 7 2303 (Windows) und höher.
- Citrix Workspace-App 2303 (Windows) und höher.

[CGS-16258]

## 29. August 2023

### Was ist neu

- **Routing für geografische Standorte —Tech Preview**

Der Citrix Gateway Service bietet den Administratoren die Möglichkeit, ihren Benutzern zu ermöglichen, unabhängig vom Standort des Benutzers eine Verbindung zu POPs in einer bestimmten Region oder nur über einen bestimmten Cloud-Dienstanbieter herzustellen. Weitere Informationen finden Sie unter [Routing für geografische Standorte —Technical Preview](#).

[CGS-13782]

- **HDX-Leistungsanalyse**

Citrix Gateway Service unterstützt die HDX-Leistungsanalysefunktion, mit der Citrix Analytics-Administratoren Leistungsdaten im Zusammenhang mit der Connector-Gateway-PoP-Latenz anzeigen können. Weitere Informationen finden Sie unter [Connector-Statistiken](#).

[CGS-15829]

- **Beschleunigtes Netzwerken**

Die Citrix Gateway Service-Infrastruktur wurde erweitert, um beschleunigte Netzwerke zu unterstützen, wobei sie Single-Root-I/O-Virtualisierung (SR-IOV) verwendet, um Benutzern leistungsstarke Netzwerkfunktionen bereitzustellen.

[CGS-15684]

- **Veraltete schwache Chiffren**

Die aktualisierte Liste der veralteten Chiffren von Citrix Gateway Service finden Sie unter [Technische Sicherheitsübersicht](#).

[CGS-14234]

## Behobene Probleme

- EDT-Sitzungen werden getrennt, wenn der Backend-Pool im Azure Load Balancer geändert wird.

[CGS-15808]

## 10. November 2022

### Was ist neu

- **Unterstützung für Rendezvous-Protokoll Version V2**

Der Citrix Gateway Service unterstützt jetzt die Rendezvous-Protokollversion V2 für Citrix Gateway Service auf der Google Cloud Platform. Einzelheiten finden Sie unter [Unterstützte Funktionen des Citrix Gateway Service](#).

- **Verfügbarkeit des Citrix Gateway Service auf der Google Cloud Platform in Europa**

Der Citrix Gateway Service auf der Google Cloud Platform ist jetzt in Europa in den folgenden Regionen verfügbar.

- London
- Zürich

Einzelheiten finden Sie unter [Citrix Gateway Service auf der Google Cloud Platform](#).

## **Bekannte Probleme**

- Die Rendezvous V2-VDA-Registrierung schlägt fehl, wenn die Kunden-ID aus weniger als 6 Zeichen besteht.

[CGS-15036]

## **30. Juni 2022**

### **Was ist neu**

- **Verfügbarkeit des Citrix Gateway-Dienstes auf der Google Cloud Platform**

Mit der Unterstützung des Citrix Gateway Service auf der Google Cloud Platform (GCP) können Kunden, die ihre Workloads in Google Cloud ausführen, mithilfe der optimalen Routing-Funktion von Citrix Gateway die Vorteile des leistungsstarken globalen Netzwerks von Google Cloud nutzen. Die optimale Gateway-Routing-Funktion leitet Clients zum nächstgelegenen GCP Citrix Gateway Service POP weiter. Darüber hinaus bietet der Citrix Gateway Service auf Google Cloud eine sichere Konnektivität zwischen Citrix Workspace-Clients und Virtualisierungsressourcen, um Sitzungen mit der niedrigsten Latenz und der bestmöglichen Benutzererfahrung bereitzustellen. Einzelheiten finden Sie unter [Citrix Gateway Service auf der Google Cloud Platform](#).

## **04. April 2022**

### **Was ist neu**

- **Änderungen beim Rebranding**

- Citrix Secure Workspace Access wurde jetzt in Citrix Secure Private Access umbenannt.
- Citrix Virtual Apps and Desktops Service wurde jetzt in Citrix DaaS umbenannt.

### **Was ist neu**

- **Zusammenführung der Citrix Gateway Service-Kachel zu einem einzigen Citrix Secure Private Access in Citrix Cloud**

## 11. Oktober 2021

### Was ist neu

- **Zusammenführung der Citrix Gateway Service-Kachel zu einem einzigen Citrix Secure Private Access in Citrix Cloud**

Die Citrix Gateway Service-Kachel und die Citrix Secure Private Access-Kachel werden zur Citrix Secure Private Access-Kachel zusammengeführt, und die Citrix Gateway-Landingpage wurde für Citrix Secure Private Access geändert. Daher werden die **Virtual Apps and Desktops** die Verknüpfungen zum **Hinzufügen einer Web-/SaaS-App** nicht angezeigt. Die Kunden von Citrix Virtual Apps and Desktops können den Citrix Gateway Service jedoch über **Workspace-Konfiguration > Access > Externe Konnektivität** aktivieren. Sonst ändert sich die Funktionalität nicht.

Die folgenden Funktionen des Citrix Gateway Service wurden in den Citrix Secure Private Access-Dienst verschoben.

- Konfigurieren von SaaS- und Unternehmens-Webanwendungen
- Ermöglichen verbesserter Sicherheitskontrollen
- Konfigurieren kontextbezogener Richtlinien

Kunden von Citrix Secure Private Access, darunter Citrix Workspace Essentials und Citrix Workspace Standard, können jetzt eine einzige Citrix Secure Private Access-Kachel verwenden, um SaaS- und Enterprise-Web-Apps, erweiterte Sicherheitskontrollen, kontextbezogene Richtlinien sowie Webfilterrichtlinien zu konfigurieren.

[ACS-645]

## Beginnen Sie mit Citrix Gateway Service

June 6, 2023

Kunden, die Anspruch auf Citrix DaaS haben, erhalten standardmäßig den Citrix Gateway Service aktiviert. Kunden müssen keine separate Citrix Gateway Service-Testversion anfordern. Einzelheiten finden Sie unter [Registrierung für Service](#).

### Wichtig:

Auf der Citrix Cloud-Startseite wird die Citrix Gateway Service-Kachel nicht angezeigt. Die Citrix Gateway Service-Kachel und die Citrix Secure Private Access-Kachel werden zur Citrix Secure Private Access-Kachel zusammengeführt, und die Landingpage wurde für Citrix Secure Private



Access geändert. Daher wird die Verknüpfung **Virtual Apps and Desktops** nicht angezeigt. Die Kunden von Citrix Virtual Apps and Desktops können den Citrix Gateway Service jedoch über **Workspace-Konfiguration > Access > Externe Konnektivität** aktivieren. Sonst ändert sich die Funktionalität nicht.

## Technische Sicherheit

November 8, 2023

Citrix Cloud verwaltet den Betrieb für Citrix Gateway Services, sodass Kunden das NetScaler Gateway-Gerät nicht mehr verwalten müssen. Der Citrix Gateway Service wird über die Citrix Workspace-App bereitgestellt.

Citrix Gateway Service bietet die folgenden Funktionen:

**HDX-Konnektivität:** Die Virtual Delivery Agents (VDAs), die die Apps und Desktops hosten, bleiben unter der Kontrolle des Kunden im Rechenzentrum seiner Wahl, entweder in der Cloud oder on-premises. Diese Komponenten sind über einen Agent ("Citrix Cloud Connector") mit dem Cloud-Service verbunden.

**DTLS 1.2-Protokollunterstützung:** Citrix Gateway Service unterstützt Datagram Transport Layer Security (DTLS) 1.2 für HDX-Sitzungen über EDT (UDP-basiertes Transportprotokoll). Die folgenden Verschlüsselungssammlungen werden unterstützt:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384

**Unterstützung des TLS-Protokolls:** Citrix Gateway Service unterstützt die folgenden TLS-Verschlüsselungssammlungen:

- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1-ECDHE-RSA-AES128-SHA
- TLS1.2-AES256-GCM-SHA384
- TLS1-AES-256-CBC-SHA

**Endpoint Management-Integration:** In Kombination mit Citrix Endpoint Management plus Citrix Workspace bietet der Citrix Gateway Service sicheren Remote-Gerätezugriff auf Ihr internes Netzwerk und Ihre Ressourcen. Das Onboarding des Citrix Gateway Service mit Endpoint Management ist schnell und einfach. Der Citrix Gateway Service beinhaltet die vollständige Unterstützung von Citrix SSO für Apps wie Secure Mail und Secure Web.

## Datenfluss

Citrix Gateway Service ist ein global verteilter Multitenant-Service. Endbenutzer verwenden den nächstgelegenen Point-of-Presence (PoP), an dem die jeweilige Funktion verfügbar ist, die sie benötigen, unabhängig von der Geoauswahl der Citrix Cloud Control-Ebene oder dem Standort der Anwendungen, auf die zugegriffen wird. Konfigurationen, z. B. Autorisierungsmetadaten werden auf alle PoPs repliziert.

Protokolle, die von Citrix für Diagnose-, Überwachungs-, Geschäfts- und Kapazitätsplanung verwendet werden, werden an einem zentralen Ort gesichert und gespeichert.

Die Kundenkonfiguration wird an einem zentralen Ort gespeichert und global an alle PoPs verteilt.

Die Übertragung von Daten zwischen Cloud und Kundenstandort erfolgt über eine sichere TLS-Verbindung über Port 443.

Verschlüsselungsschlüssel, die für die Benutzerauthentifizierung und das einmalige Anmelden verwendet werden, werden in Hardware-Sicherheitsmodulen

## Datenisolierung

Der Citrix Gateway Service speichert die folgenden Daten:

- Konfigurationsdaten, die für die Vermittlung und Überwachung der Kundenanwendungen benötigt werden —Daten werden vom Kunden erfasst, wenn sie bestehen bleiben.
- TOTP-Seeds für jedes Benutzergerät —TOTP-Seeds werden vom Kunden, Benutzer und Gerät erfasst.

## Audit und Change Control

Derzeit stellt der Citrix Gateway Service Kunden keine Überwachungs- und Änderungskontrollprotokolle zur Verfügung. Für Citrix stehen Protokolle zur Verfügung, mit denen die Aktivitäten von Endbenutzer und Administrator überprüft werden können.

## Handhabung von Anmeldeinformationen

Der Dienst verarbeitet zwei Arten von Anmeldeinformationen:

- Benutzeranmeldeinformationen: Anmeldeinformationen von Endbenutzern (Passwörter und Authentifizierungstoken) können dem Citrix Gateway Service zur Verfügung gestellt werden, um Folgendes auszuführen:

- Citrix Secure Private Access —Der Dienst verwendet die Identität des Benutzers, um den Zugriff auf SaaS- und Enterprise-Webanwendungen und andere Ressourcen zu bestimmen.
- Single Sign-On - Der Dienst hat möglicherweise Zugriff auf das Kennwort des Benutzers, um die SSO-Funktion für interne Webanwendungen mithilfe von HTTP Basic, NTLM oder formularbasierter Authentifizierung abzuschließen. Das Verschlüsselungsprotokoll, das für das Kennwort verwendet wird, ist TLS, es sei denn, Sie konfigurieren die HTTP Basic-Authentifizierung.
- Administratoranmeldeinformationen: Administratoren authentifizieren sich bei Citrix Cloud. Dadurch wird ein einmalig signiertes JSON-Web-Token (JWT) generiert, das dem Administrator Zugriff auf die Verwaltungskonsolen in Citrix Cloud ermöglicht.

### Wichtige Hinweise

- Der gesamte Datenverkehr über öffentliche Netzwerke wird mit TLS verschlüsselt, wobei von Citrix verwaltete Zertifikate verwendet werden.
- Schlüssel, die für SaaS-App SSO (SAML-Signaturschlüssel) verwendet werden, werden vollständig von Citrix verwaltet.
- Für MFA speichert der Citrix Gateway Service die gerätespezifischen Schlüssel, die zum Starten des TOTP-Algorithmus verwendet werden.
- Um die Kerberos Single Sign-On-Funktion zu aktivieren, können Kunden die Connector Appliance mit Anmeldeinformationen (Benutzername und Kennwort) für ein Dienstkonto konfigurieren, dem die eingeschränkte Kerberos-Delegierung zuträglich ist.

## Überlegungen zur Bereitstellung

Citrix empfiehlt Benutzern, die veröffentlichte Dokumentation zu bewährten Methoden für die Bereitstellung von Citrix Gateway Services zu lesen. Weitere Überlegungen zu SaaS-Apps und der Bereitstellung von Unternehmens-Web-Apps sowie zum Netzwerkconnector lauten wie folgt.

**Auswahl des richtigen Connectors:** Je nach Anwendungsfall muss der richtige Connector ausgewählt werden:

---

Anwendungsfall	Connector	Formfaktor
Benutzerauthentifizierung: Active Directory	Citrix Cloud Connector	Windows
HDX-Konnektivität	Citrix Cloud Connector	Windows
Zugriff auf SaaS-Apps	Citrix Cloud Connector	–

---

Anwendungsfall	Connector	Formfaktor
Zugriff auf Unternehmens-Webanwendungen	Citrix Cloud Connector, Citrix Connector Appliance	–
Von Citrix Endpoint Management bereitgestellte Unternehmensanwendungen und -dateien	Citrix Cloud Connector, Citrix Connector Appliance	–

---

## Anforderungen für den Citrix Cloud Connector-Netzwerkzugriff

Informationen zu den Anforderungen für den Netzwerkzugriff von Citrix Cloud Connector finden Sie unter <https://docs.citrix.com/en-us/citrix-cloud/overview/requirements/internet-connectivity-requirements.html>

## HDX-Konnektivität des Citrix Gateway-Dienstes

Durch die Verwendung des Citrix Gateway Service entfällt die Notwendigkeit, NetScaler Gateway in den Rechenzentren des Kunden bereitzustellen. Um den Citrix Gateway Service verwenden zu können, müssen Sie Citrix Workspace verwenden, der von Citrix Cloud bereitgestellt wird.

## Best Practices für Kunden

Kunden werden empfohlen, TLS in ihrem Netzwerk zu verwenden und SSO für Anwendungen über HTTP nicht zu aktivieren.

## Veraltete Verschlüsselungssammlungen

Die folgenden Verschlüsselungssammlungen sind aus Sicherheitsgründen veraltet:

- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES-128-SHA256
- TLS1.2-AES256-GCM-SHA384
- TLS1.2-AES-256-SHA256
- TLS1.2-DHE-RSA-AES-256-SHA256
- TLS1.2-DHE-RSA-AES-128-SHA256
- TLS1.2-DHE-RSA-AES256-GCM-SHA384
- TLS1.2-DHE-RSA-AES128-GCM-SHA256

- SSL3-DES-CBC3-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1-DHE-RSA-AES-128-CBC-SHA
- TLS1-DHE-DSS-AES-256-CBC-SHA
- TLS1-DHE-DSS-AES-128-CBC-SHA
- TLS1-ECDHE-RSA-DES-CBC3-SHA
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-ECDSA-AES128-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256

## Routing für geografische Standorte —Tech Preview

June 4, 2024

Der Citrix Gateway Service bietet den Administratoren die Möglichkeit, ihren Benutzern die Verbindung zu einer bestimmten Region (POPs) zu ermöglichen. Dadurch wird sichergestellt, dass der Benutzerverkehr unabhängig vom Standort des Benutzers in die bestimmte Region geleitet wird.

**Hinweis:**

Melden Sie sich für die Vorschau an mit <https://podio.com/webforms/27328175/2108260>.

In der folgenden Tabelle sind die Regionen und POPs in dieser Region aufgeführt, die standortbasierte Verkehrsweiterleitung unterstützen:

---

Geolocation	POPs
USA - Osten	Azure-USA-Ost, AWS USA Ost, AWS-US-Nord-Zentral
Vereinigte Staaten - Zentral und West	Azure-USA-West, AWS-US-West, Azure-US-Süd-Zentral

---

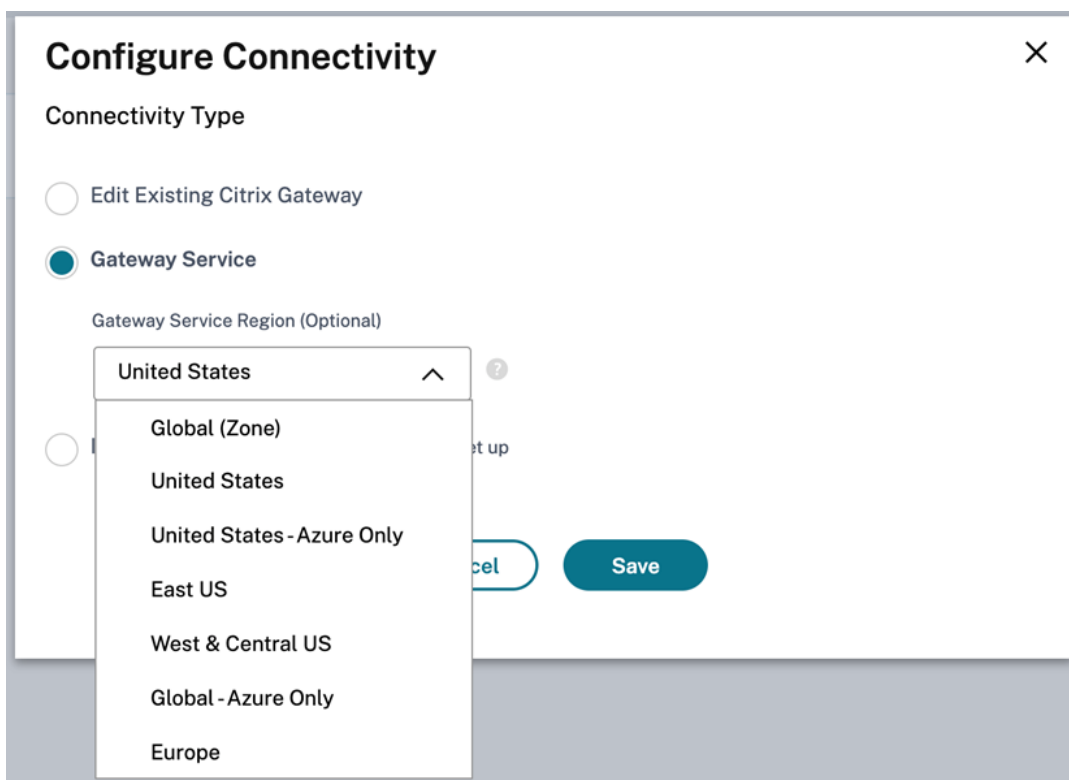
Geolocation	POPs
USA	Azure-US-Süd-Zentral, Azure-USA-Ost, Azure-US-West, AWS-US-Ost, AWS-US-West, AWS-US-Nord-Zentral
Vereinigte Staaten —nur Azure	Azure-USA-Ost, Azure-US-West, Azure-US-Süd-Zentral
Europa	AWS-Europa-Mitte, Azure-Europa-West, Azure-Europa-Nord
Australien	Azure-Australien-Ost, AWS-Australien-Ost
Global —nur Azure	Azure-US-Ost, Azure-US-West, Azure-US-Süd-Central, Azure-Brasilien-Süd, Azure-Europa-West, Azure-Europa-Nord, Azure-Australien-Ost, Azure-Asien-Süd-Ost, Azure-Japan-Ost, Azure-Indien-Süd, Azure-UAE-Nord, Azure-Südafrika, Azure-Hongkong, Azure-Toronto-Kanada

---

## Informationen zur Konfiguration

Sie können eine bestimmte Region für den Benutzerdatenverkehr auf der Seite **Ressourcenstandorte** oder **Workspace-Konfiguration** in Citrix Cloud konfigurieren.

1. Melden Sie sich bei [Citrix Cloud](#) an.
2. Klicken Sie auf das Hamburger-Menü und wählen Sie **Ressourcenstandorte** oder **Workspace-Konfiguration** aus.
  - a) Wählen Sie auf der Seite **Ressourcenstandorte** einen Standort aus und klicken Sie auf **Gateway**. Der Bildschirm „**Konnektivität konfigurieren**“ wird angezeigt.
  - b) Wählen Sie auf der Seite **Workspace-Konfiguration** unter Externe Konnektivität einen Standort aus und klicken Sie auf die Ellipse. Der Bildschirm „**Konnektivität konfigurieren**“ wird angezeigt.



3. Wählen Sie **unter Gateway Service Region (optional)** die Region aus, in die Sie Ihren Kundenverkehr weiterleiten möchten.

**Hinweise:**

Wenn Sie keine Region auswählen, ist standardmäßig **Global** ausgewählt. Wenn die Region **Global** ist, wird der Verkehr an den POP umgeleitet, der sich in der Nähe des Kunden befindet.

In seltenen Szenarien, wenn es zu einem Ausfall kommt und nicht alle POPs einer bestimmten Region verfügbar sind, fällt die Konfiguration auf **Global** zurück, anstatt den Datenverkehr zu blockieren.

4. Klicken Sie auf **Speichern**.

## Migrieren Sie NetScaler Gateway zu Citrix Gateway Service für HDX Proxy

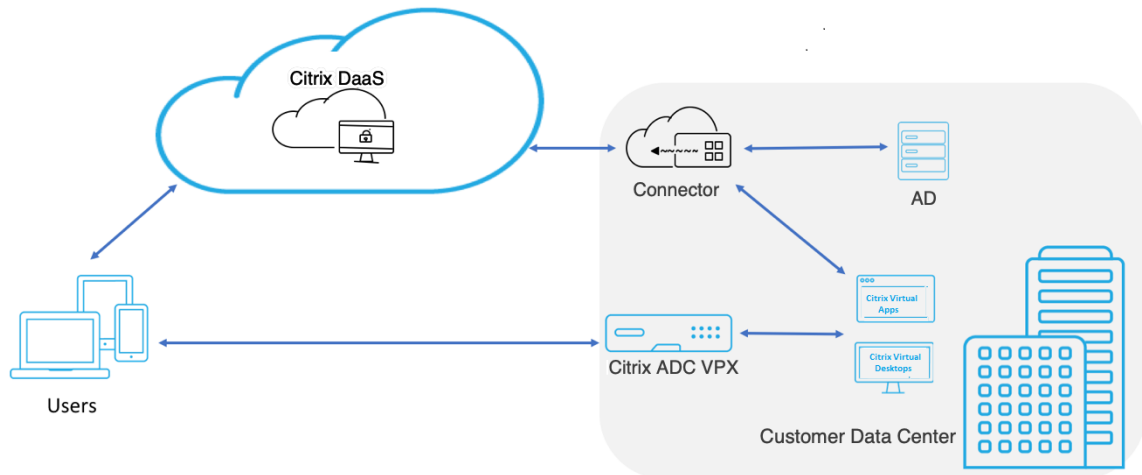
November 8, 2023

Sie können von einem Citrix Gateway für HDX Proxy zu einem vollständig verwalteten cloudbasierten HDX-Proxy migrieren, der vom Citrix Gateway Service in Citrix Cloud unterstützt wird.

## Cloud-basierter HDX-Proxy

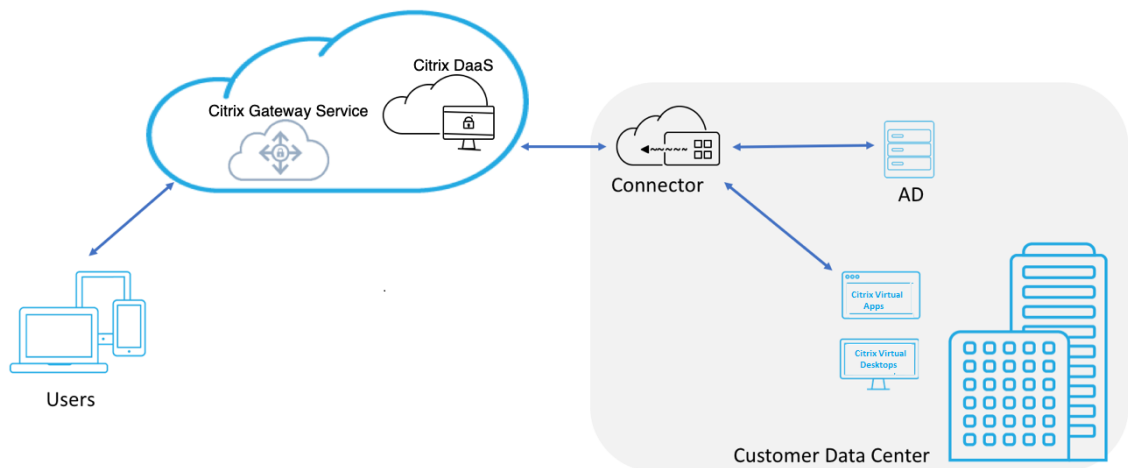
Kunden, die Anspruch auf Citrix DaaS haben, erhalten standardmäßig den Citrix Gateway Service aktiviert. Kunden müssen keine separate Citrix Gateway Service-Testversion anfordern.

**Abbildung 1. Bereitstellung mit NetScaler Gateway als HDX Proxy**



Citrix Gateway Service ist ein cloudbasierter HDX-Proxy, der sicheren Remotezugriff über ein cloud-basiertes Gateway bietet, das virtuelle Apps und Desktop-Umgebungen, die Citrix DaaS-Umgebungen sind, als Frontend dient.

**Abbildung 2. Bereitstellung mit Citrix Gateway Service als HDX Proxy**



Diese Funktion ist jetzt in Ihren Citrix DaaS- und Workspace Service-Berechtigungen enthalten. Sie können diese Funktion aktivieren.



## Migration von einem on-premises NetScaler Gateway zu einem cloudbasierten Citrix Gateway Service

Das NetScaler Gateway-Gerät wird vom Kunden verwaltet und der cloudbasierte Citrix Gateway Service wird von Citrix verwaltet. In diesem Abschnitt wird erklärt, wie Sie von einem on-premises NetScaler Gateway zu einem in der Cloud gehosteten Citrix Gateway Service für HDX Proxy migrieren. Obwohl NetScaler Gateway und Citrix Gateway Service HDX Proxy bereitstellen, unterscheiden sich die zugrundeliegende Infrastruktur und der Arbeitsmechanismus. Die Schritte zum Aktivieren von HDX Proxy on Cloud sind jedoch mit nur wenigen Klicks einfach und unkompliziert.

Um diese Migration zu aktivieren, aktivieren Sie den Citrix Gateway Service für Citrix DaaS. Nach der Aktivierung wird der Datenverkehr über den Citrix Gateway Service geleitet, und ein lokales NetScaler Gateway ist nicht mehr erforderlich.

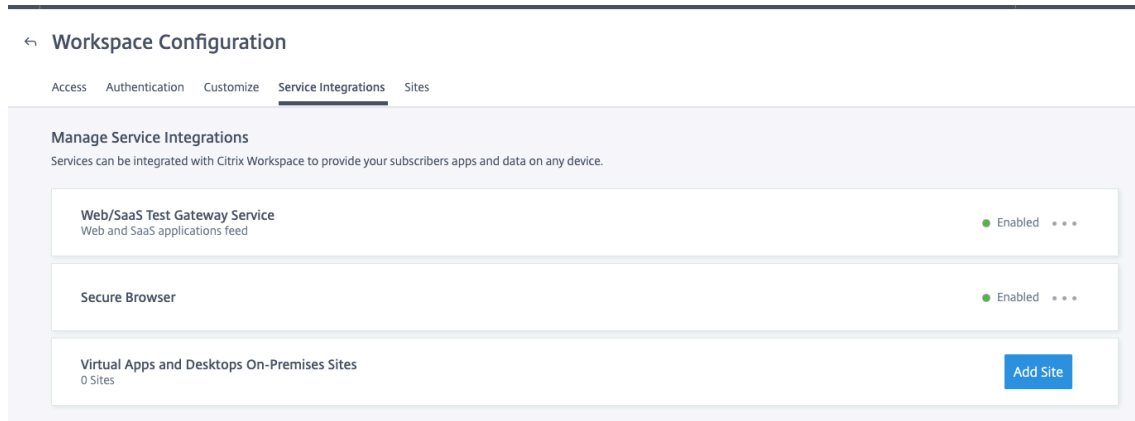
Im Folgenden sind die Annahmen aufgeführt, die getroffen wurden, bevor Sie mit der Migration von einem on-premises NetScaler Gateway zu einem cloudbasierten Citrix Gateway Service beginnen.

- Der Kunde hat Citrix Cloud Service abonniert und Citrix DaaS gekauft.
- Der Kunde verwendet ein on-premises vorgestelltes Active Directory, um Benutzer in der Cloud zu authentifizieren.

### Citrix Gateway Service aktivieren

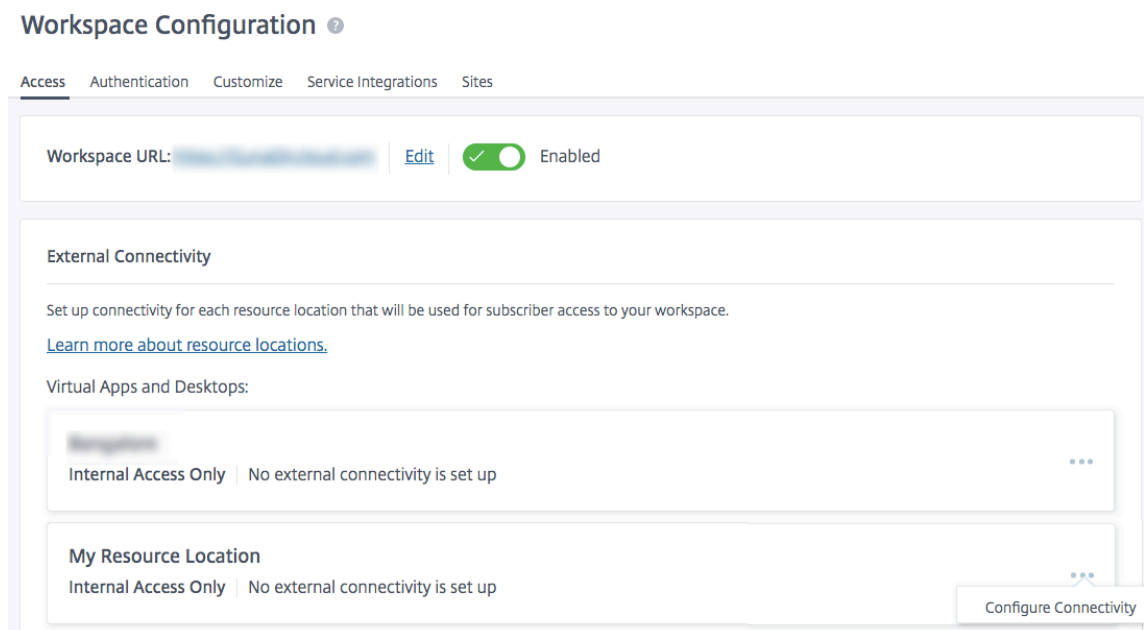
Im Folgenden finden Sie die Schritte, um den Citrix Gateway Service für Citrix DaaS-Benutzer zu aktivieren:

1. Melden Sie sich bei Citrix Cloud Services als Administratorbenutzer an.
2. Klicken Sie auf das Hamburger-Symbol und wählen Sie **Workspace-Konfiguration**.
3. Klicken Sie auf **Dienstintegrationen**.
4. Suchen Sie die Ellipse neben **Gateway**, klicken Sie auf die Ellipse und klicken Sie dann auf **Aktivieren**.



Im Folgenden werden die Schritte beschrieben, um den Citrix Gateway Service für Citrix Workspace-Benutzer zu aktivieren.

1. Melden Sie sich bei Citrix Cloud Services als Administratorbenutzer an.
2. Klicken Sie auf das Hamburger-Symbol und wählen Sie **Workspace-Konfiguration**.
3. Suchen Sie auf der Registerkarte **Zugriff** im Abschnitt **Externe Konnektivität** die Ellipse neben **Mein Ressourcenstandort** unter **Citrix DaaS**.
4. Klicken Sie auf die Auslassungspunkte, und klicken Sie auf **Konnektivität konfigurieren**.



5. Wählen Sie im Popup-Fenster **Citrix Gateway Service** und klicken Sie dann auf **Speichern**.

## Configure Connectivity

### Connectivity Type

- Traditional Gateway
- Gateway Service
- Internal Only | No external connectivity is set up

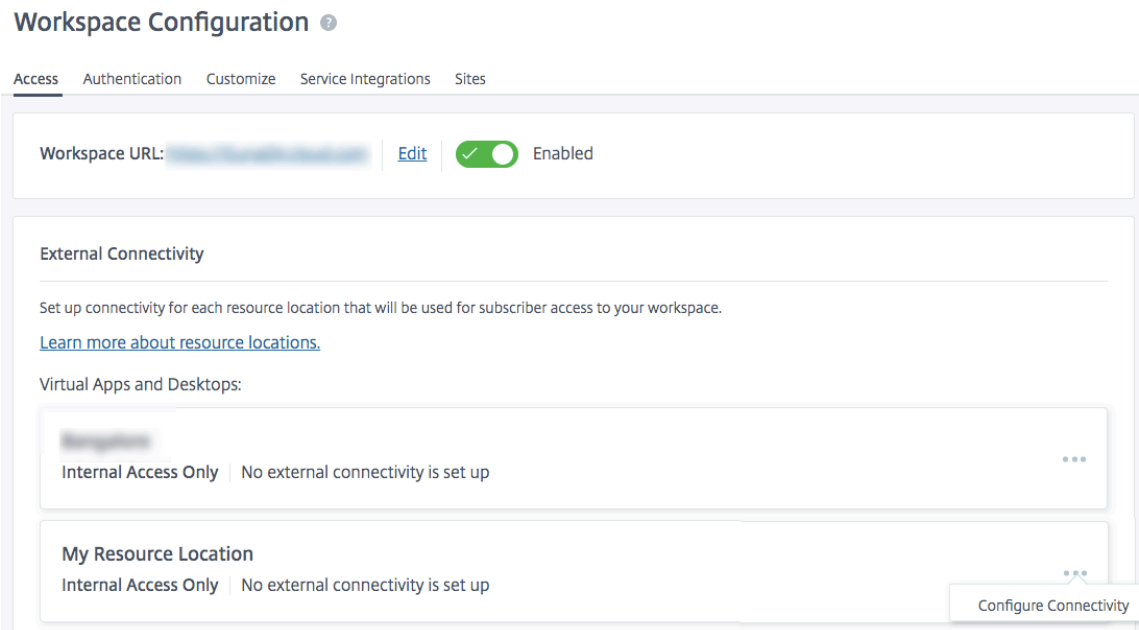
Cancel

Save

### Rollback auf NetScaler Gateway

Um den HDX Proxy auf ein on-premises festes NetScaler Gateway zurückzusetzen, führen Sie die folgenden Schritte aus.

1. Melden Sie sich bei Citrix Cloud Services als Administratorbenutzer an.
2. Klicken Sie auf das Hamburger-Symbol oben links und wählen Sie **Workspace-Konfiguration**.
3. Suchen Sie **auf der Registerkarte Zugriff** im Abschnitt **Externe Konnektivität** die Ellipse neben **Mein Ressourcenstandort** unter **Citrix DaaS**.



4. Klicken Sie auf die Auslassungspunkte, und klicken Sie auf **Konnektivität konfigurieren**.
5. Wählen Sie **Traditionelles Gateway** und geben Sie den FQDN ein

## Configure Connectivity

### Connectivity Type

Traditional Gateway

External FQDN \*  
aha.com

Add

Gateway Service

Internal Only | No external connectivity is set up

Cancel

Save

6. Klicken Sie auf **Hinzufügen** und dann auf **Speichern**.

## HDX Adaptive Transport mit EDT-Unterstützung für Citrix Gateway Service

June 6, 2023

Enlightened Data Transport (EDT) ist ein Citrix-proprietäres Transportprotokoll, das auf UDP aufbaut. EDT bietet eine überlegene Benutzererfahrung bei anspruchsvollen Langstreckenverbindungen unter Beibehaltung der Serverskalierbarkeit.

Adaptiver Transport ist ein Datentransportmechanismus für Citrix Virtual Apps and Desktops. Adaptive Transport bietet die Möglichkeit, EDT als Transportprotokoll für ICA zu verwenden und zu TCP zu wechseln, wenn EDT nicht verfügbar ist.

Weitere Informationen zu adaptivem Transport und EDT finden Sie in der [Dokumentation zu adaptivem Transport](#).

### Voraussetzungen

- Citrix DaaS
- Virtual Delivery Agent (VDA) 2012 oder höher
- Citrix Workspace-App
  - Windows: Version 1912 oder höher (2105 oder höher empfohlen)
  - Linux: Version 1912 oder höher (2104 oder höher empfohlen)
  - Mac: Version 1912 oder höher
  - iOS: aktuell verfügbare Version im Apple App Store
  - Android: aktuell verfügbare Version in Google Play
- Der UDP-Port 443 muss für ausgehenden Datenverkehr von VDA zum Citrix Gateway Service zugelassen sein
- Rendezvousprotokoll muss aktiviert sein und funktionieren. Einzelheiten finden Sie in der [Rendezvous-Protokoll-Dokumentation](#).
- Stellen Sie sicher, dass der adaptive Transport aktiviert ist. Einzelheiten finden Sie in der [Dokumentation zu Einstellungen für den adaptiven Transport](#).
- Weitere Informationen zu adaptivem Transport und EDT finden Sie in der [Dokumentation zu adaptivem Transport](#).

### Überlegungen

Im Folgenden sind einige Überlegungen zur Verwendung von EDT mit dem Citrix Gateway Service aufgeführt.

- Es wird dringend empfohlen, EDT MTU Discovery zu aktivieren. Einzelheiten finden Sie in der [Dokumentation zu adaptivem Transport](#).
- EDT mit Citrix Gateway Service ist nur bei Verwendung von Rendezvous verfügbar. Wenn HDX-Sitzungen über den Cloud Connector proxiiert werden, steht nur TCP für den Datentransport zur Verfügung.
- Wenn eine Einrichtung einer EDT-Sitzung fehlschlägt, fällt die Sitzung auf TCP zurück, was zu einer Verlängerung der Startzeit der Sitzung führt.
- Wenn Sie weiterhin für HDX-Sitzungen den Cloud Connector als Proxy verwenden möchten, sollten Sie den adaptiven Transport über die Citrix Studio-Richtlinie deaktivieren, um die potenzielle Erhöhung der Sitzungsstartzeiten durch die Fallback-Sequenz zu vermeiden.
- Citrix empfiehlt, EDT über den Citrix Gateway Service nur mit VDAs zu verwenden, die unter Windows 10 und Windows Server 2019 ausgeführt werden. Es gibt Einschränkungen für Windows Server 2012 R2 und 2016, die keine MTU größer als 1024 für DTLS-verschlüsselte Sitzungen zulassen, was sich auf die Leistung und Benutzererfahrung auswirken kann.
- Mit Adaptive Transport unterstützt der Citrix Gateway Service kein UDP-Audio.

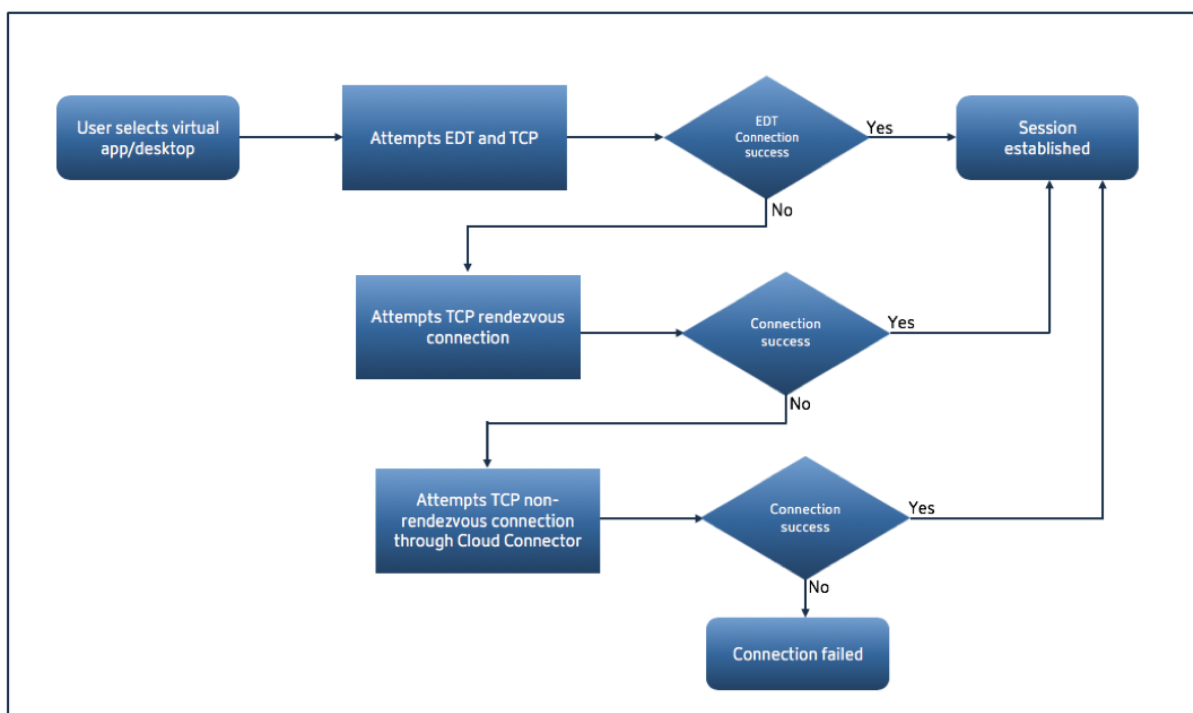
## Validierung von Transportprotokollen

Um zu erfahren, ob Ihre Sitzungen EDT verwenden, lesen Sie Folgendes:

- Verbindungsprotokoll in Citrix Director: <https://support.citrix.com/article/CTX220730>.
- Nachdem Sie eine App oder einen Desktop gestartet haben, gehen Sie zu **Citrix Workspace-App > Connection Center**, wählen Sie die entsprechende Sitzung aus, klicken Sie auf **Eigenschaften** und sehen Sie sich die Eigenschaft Transportverschlüsselung an. Wenn es DTLS anzeigt, verwendet die Sitzung EDT für den Transport. Wenn es TLS anzeigt, verwendet die Sitzung TCP für den Transport.
- Wenn Sie einen Desktop gestartet haben, können Sie eine PowerShell oder eine Eingabeaufforderung öffnen und ausführen “`ctxsession -v`”. Die Eigenschaft Transport Protocols zeigt die verwendete Verbindungsmethode an:
  - EDT Rendezvous: **UDP > DTLS > CGP > ICA**
  - TCP Rendezvous: **TCP > SSL > CGP > ICA**
  - Proxy über Cloud Connector: **TCP > CGP > ICA**

## Fallback der Verbindung

Wenn die EDT-Verhandlung aus irgendeinem Grund fehlschlägt, greift die Sitzung mit Rendezvous auf TCP zurück. Und wenn das fehlschlägt, greift die Sitzung auf Proxying über die Cloud Connectors zurück.



## MTU-Discovery durch EDT

Es wird dringend empfohlen, EDT MTU Discovery zu aktivieren, um sicherzustellen, dass jede Sitzung die optimale MTU für diese Verbindung verwendet.

Falls EDT MTU Discovery deaktiviert ist oder der Client des Benutzers die Funktion nicht unterstützt, wird die EDT MTU automatisch auf 1380 eingestellt, um Fragmentierungsprobleme zu vermeiden.

Benutzer können sich über ein Netzwerk verbinden, das eine MTU unter 1380 benötigt, was hauptsächlich bei Mobilfunknetzen (3G, 4G) oder VPN-Verbindungen zu sehen ist. Wenn dies in Ihrer Umgebung der Fall ist und die von den Benutzern verwendeten Clients EDT MTU Discovery nicht unterstützen, empfiehlt Citrix, den Adaptive Transport zu deaktivieren, bis die Funktion auf Ihrer Ziel-Client-Plattform verfügbar ist.

Weitere Einzelheiten zur EDT MTU Discovery finden Sie in der [Dokumentation zu adaptivem Transport](#).

## Problembehandlung

Im Folgenden finden Sie einige allgemeine Anleitungen zur Problembehandlung.

### Sitzungen verbinden sich aber nicht mit EDT:

1. Wenn die Sitzungen über den Cloud Connector weitergeleitet werden, stellen Sie sicher, dass Rendezvous aktiviert ist und ordnungsgemäß funktioniert, da dies eine Voraussetzung für

die Verwendung von EDT mit dem Citrix Gateway Service ist. Einzelheiten finden Sie in der [Rendezvous-Dokumentation](#).

2. Wenn die Sitzungen TCP-Rendezvous verwenden:

- Stellen Sie sicher, dass Sie die VDA-Version 2012 oder höher verwenden.
- Überprüfen Sie, ob Adaptiver Transport in Citrix Richtlinien aktiviert ist.
- Stellen Sie sicher, dass die entsprechenden Firewallregeln vorhanden sind, um UDP 443 von den VDA-Maschinen zum Citrix Gateway Service zu öffnen. Weitere Einzelheiten finden Sie in der [Rendezvous\]\(/en-us/citrix-virtual-apps-desktops-service/hdx/rendezvous-protocol.html\)-Dokumentation](#).
- Wenn auf dem VDA-Computer eine lokale Firewall aktiviert ist (z. B. Windows Defender Firewall), stellen Sie sicher, dass es keine Regeln gibt, die UDP 443 blockieren.
- Wenn Sie einen Proxy verwenden, können nur SOCKS5-Proxys zum Proxy EDT verwendet werden. Einzelheiten finden Sie in der [Rendezvous-Dokumentation](#).

**Sitzungen verbinden sich mit EDT, trennen die Verbindung jedoch nach einiger Zeit nach dem Zufallsprinzip:**

1. Stellen Sie sicher, dass Sie die VDA-Version 2012 oder höher verwenden.

**Die Sitzung kann keine Verbindung herstellen:**

1. Stellen Sie sicher, dass Sie die VDA-Version 2012 oder höher verwenden.
2. Wenn Sie einen Client verwenden, der EDT MTU Discovery unterstützt, stellen Sie sicher, dass EDT MTU Discovery aktiviert ist. Dies trägt dazu bei, Fragmentationsprobleme zu minimieren. Einzelheiten finden Sie in der [Dokumentation zu adaptivem Transport](#).
3. Bei Verwendung eines Linux- oder Android-Clients:
  - Prüfen Sie, ob Windows- oder Mac-Clients ordnungsgemäß funktionieren.
  - Prüfen Sie, ob die CWA-Version auf Linux 2104, Android 21.5.0 oder höher aktualisiert wurde.
  - Wenn Sie eine ältere Version von CWA verwenden, deaktivieren Sie Adaptive Transport und stellen Sie sicher, dass TCP Rendezvous ordnungsgemäß funktioniert.
  - Sobald TCP Rendezvous funktioniert und die Sitzung nach dem erneuten Aktivieren von Adaptive Transport keine Verbindung herstellen kann, lesen Sie die Schritte zur Fehlerbehebung, die in Schritt **Sessions connect erwähnt werden, aber kein EDT verwenden > Wenn die Sitzungen TCP Rendezvous verwenden**.



## Citrix Gateway-Dienst auf der Google Cloud Platform

July 21, 2023

Mit der Unterstützung des Citrix Gateway Service auf der Google Cloud Platform (GCP) können Kunden, die ihre Workloads in Google Cloud ausführen, mithilfe der optimalen Routing-Funktion von Citrix Gateway das leistungsstarke globale Netzwerk von Google Cloud nutzen. Die optimale Gateway-Routing-Funktion leitet Clients zum nächstgelegenen GCP Citrix Gateway Service POP weiter. Darüber hinaus bietet der Citrix Gateway Service auf Google Cloud eine sichere Konnektivität zwischen Citrix Workspace-Clients und Virtualisierungsressourcen, um Sitzungen mit der niedrigsten Latenz und der bestmöglichen Benutzererfahrung bereitzustellen.

Derzeit ist Citrix Gateway Service für GCP in den folgenden Regionen verfügbar.

- Vereinigte Staaten
  - Los Angeles
  - Oregon
  - South Carolina
- Europa
  - London
  - Zürich

### Hinweis:

- GCP-POPs sind nur für Citrix DaaS-Kunden verfügbar, die Abonnements im Google Cloud Marketplace gekauft haben und ihre Workloads in Google Cloud ausführen.
- Citrix Gateway Service-Konto —Kunden, die Anspruch auf Citrix DaaS haben, erhalten standardmäßig die Aktivierung des Citrix Gateway-Dienstes. Kunden müssen keine separate Citrix Gateway Service-Testversion anfordern. Einzelheiten finden Sie unter [Registrierung für Service](#).

### Voraussetzungen

- Citrix Cloud-Konto. Einzelheiten finden Sie unter [Anmelden bei Citrix Cloud](#).

### Unterstützte Funktionen des Citrix Gateway Service

Im Folgenden sind einige der Funktionen aufgeführt, die vom Citrix Gateway Service für GCP unterstützt werden.

**TCP HDX Proxy** —Derzeit wird nur TCP HDX Proxy unterstützt. Der Start von Virtual Apps and Desktops wird nur über das TCP-Protokoll unterstützt.

**Rendezvous V1** —Mit Citrix Gateway Service ermöglicht das Rendezvous-Protokoll Version V1 VDAs, die Citrix Cloud Connectors zu umgehen, um eine direkte Verbindung zum Gateway-POP für Datenpfadverkehr herzustellen. Einzelheiten finden Sie unter [Rendezvous V1](#).

**Rendezvous V2** - Das Rendezvous-Protokoll Version V2 unterstützt das Umgehen der Citrix Cloud Connectors sowohl für den Steuerdatenverkehr als auch für den HDX-Sitzungsverkehr. Einzelheiten finden Sie unter [Rendezvous V2](#).

**Wichtig:**

EDT-Unterstützung ist für GCP noch nicht aktiviert.

## So aktivieren Sie den Citrix Gateway Service

Kunden, die Anspruch auf Citrix DaaS haben, erhalten standardmäßig den Citrix Gateway Service aktiviert. Kunden müssen keine separate Citrix Gateway Service-Testversion anfordern. Einzelheiten finden Sie unter [Registrierung für Service](#).

## Einschränkungen

Derzeit ist GCP nur in den Regionen USA und Europa verfügbar. GCP-Kunden aus anderen Regionen können Probleme mit hoher Latenz feststellen.

## Referenzen

- Konnektivitätsanforderungen für Citrix Cloud Connector —Weitere Informationen finden Sie unter [Allgemeine Anforderungen an die Cloud Connector-Konnektivität](#).
- Überlegungen zur Skalierung und Größe für Cloud Connectors. Einzelheiten finden Sie unter [Überlegungen zu Skalierung und Größe für Cloud Connectors](#).

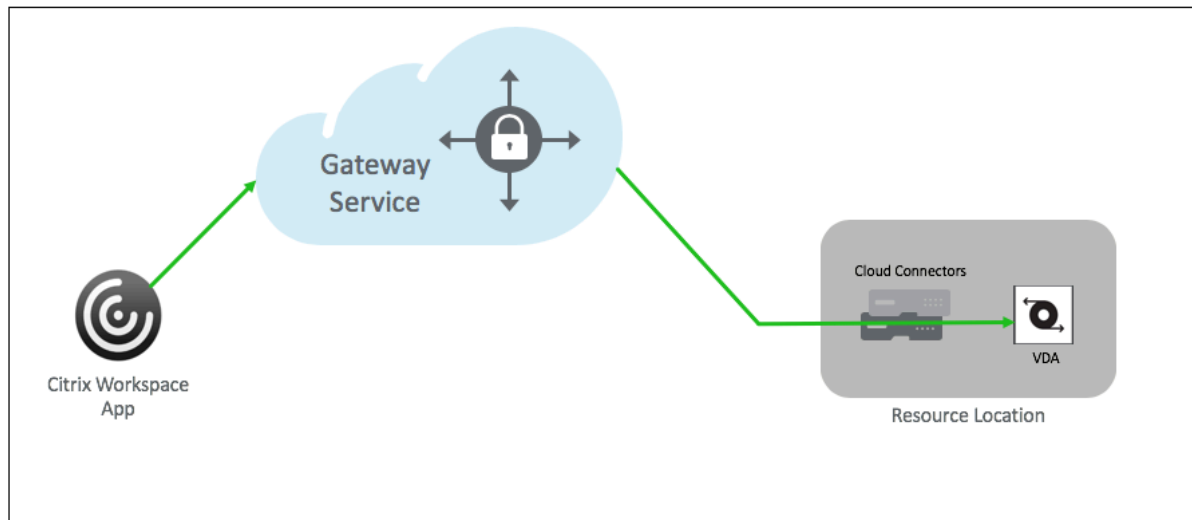
## Unterstützung für Citrix Virtual Apps and Desktops

June 6, 2023

Citrix Gateway Service bietet Benutzern sicheren Zugriff auf Citrix Virtual Apps and Desktops auf einer Reihe von Geräten, darunter Laptops, Desktops, Thin Clients, Tablets und Smartphones.

Citrix Gateway Service ermöglicht sicheren Remotezugriff auf Citrix Virtual Apps and Desktops, ohne dass Sie den Citrix Gateway Service in der DMZ bereitstellen oder Ihre Firewall neu konfigurieren müssen. Der gesamte Infrastrukturmehraufwand für die Verwendung von Citrix Gateway wird in die Cloud verlagert und von Citrix gehostet.

Sie aktivieren Citrix Gateway Service in Citrix Cloud. Nachdem Sie den Service aktivieren, können Benutzer von außerhalb des Netzwerks auf ihre VDAs zugreifen, wie in der folgenden Abbildung dargestellt.



### Funktionsweise

Die Endpoints der Benutzer und ihre on-premises gehosteten Ressourcen-VDAs sind über Citrix Cloud Connectors mit den jeweils nächstgelegenen POPs verbunden. Wenn Benutzer später eine virtuelle App oder einen Desktop auswählen, die aus ihrer Workspace-App gestartet werden soll, identifiziert das nächste POP-Hosting, mit dem die Verbindung verbunden ist, den entsprechenden Ressourcenstandort und leitet ihn an, eine Citrix Cloud Connector -Sitzung zu diesem POP zu erstellen, der eine End-to-End-Verbindung bildet, und dann ist eine virtuelle Sitzung etabliert.

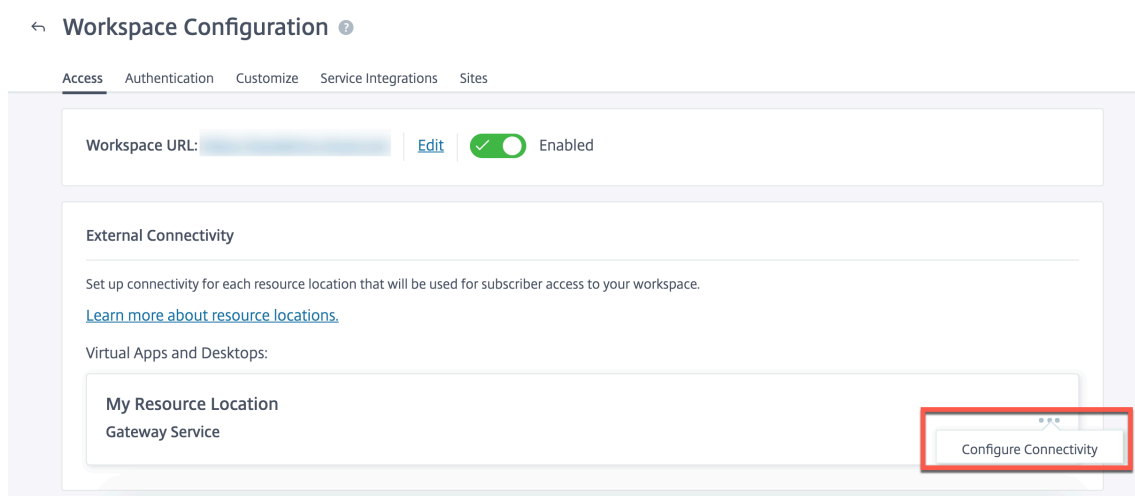
- Die Sitzungen werden über den Citrix Gateway Service über die WANs des Cloud-Partners miteinander verknüpft.
- VDAs und Workspace-Endpunkte treffen sich im Citrix Gateway Service POP, der dem Benutzer am nächsten ist.
- Sitzungen von hoher Qualität.

Weitere Informationen finden Sie unter [Citrix Gateway Service für HDX Proxy](#)

## Citrix Gateway Service aktivieren

Im Folgenden werden die Schritte zum Aktivieren von Citrix Gateway Service für Citrix Workspace-Benutzer aufgeführt.

1. Melden Sie sich bei Citrix Cloud Services als Administratorbenutzer an.
2. Klicken Sie auf das Hamburger-Symbol und wählen Sie Workspace-Konfiguration.
3. Suchen Sie **auf der Registerkarte Zugriff** im Abschnitt **Externe Konnektivität** Ellipsen neben **Mein Ressourcenstandort** unter **Citrix DaaS**. Klicken Sie auf die Ellipsen und dann auf **Konnektivität konfigurieren**.



4. Wählen Sie im Popup-Fenster Citrix Gateway Service und klicken Sie auf **Speichern**.

## Citrix Gateway Service für StoreFront – Preview

June 4, 2024

### Wichtige Informationen:

- In diesem Dokument werden die Schritte beschrieben, die Sie ausführen können, um Citrix Gateway Service für StoreFront in einem Szenario bereitzustellen, in dem Sie lieber das On-Premises NetScaler Gateway für die Authentifizierung und das on-premises StoreFront für die Enumeration verwenden.
- Die Citrix Gateway Service for StoreFront-Lösung befindet sich in der Vorschauversion und darf nicht in einer Produktionsumgebung verwendet werden. Es wird empfohlen, Funktionen in der Vorschauversion nur in Umgebungen zu verwenden, die nichts mit der

Produktion zu tun haben, um Kunden die Möglichkeit zu geben, Feedback zu geben. Die Cloud Software Group akzeptiert keine Supportanfragen für Funktionen in der Vorversion, freut sich aber über Feedback zu deren Verbesserung. Die Cloud Software Group kann auf Feedback basierend auf deren Schweregrad, Kritikalität und Wichtigkeit nach eigenem Ermessen reagieren.

- Für Test-, Vorschau-, Labor- oder Beta-Services wird keine Serviceverpflichtung angeboten.
- Citrix Gateway Service für StoreFront wird derzeit in [Citrix Cloud Japan](#)- und [Citrix Cloud Government](#)-Umgebungen nicht unterstützt.

### Übersicht

Citrix Gateway Service for StoreFront ist eine cloudbasierte HDX-Lösung, die sicheren Remotezugriff auf Ressourcen bietet, auf die über StoreFront on-premises zugegriffen wird. Sie können die Skalierbarkeit und Zuverlässigkeit von Citrix Cloud (für HDX-Proxy) nutzen, ohne Ihre on-premises StoreFront- und On-Premises NetScaler Gateway-Umgebungen zu ändern.

Bedenken Sie, dass Sie ein Citrix DaaS-Kunde sind und das on-premises StoreFront als Unternehmensanwendungsspeicher und das On-Premises NetScaler Gateway für den Remotezugriff verwenden. Wenn Sie nach einer Option suchen, um eine in der Cloud gehostete Remotezugriffslösung (HDX-Proxy) zu nutzen und gleichzeitig das on-premises StoreFront als Benutzerportal und das On-Premises NetScaler Gateway für die Authentifizierung beizubehalten, ist Citrix Gateway Service for StoreFront genau das Richtige für Sie.

Citrix Gateway Service verarbeitet die HDX-Proxystarts mithilfe eines Windows-basierten Cloud Connector an Ihrem Ressourcenstandort.

#### Hinweise:

- Sie können sich für die Vorschau anmelden unter <https://podio.com/webforms/28961380/2348524>.
- Sie können Ihr Feedback unter <https://podio.com/webforms/29573332/2436458> geben.

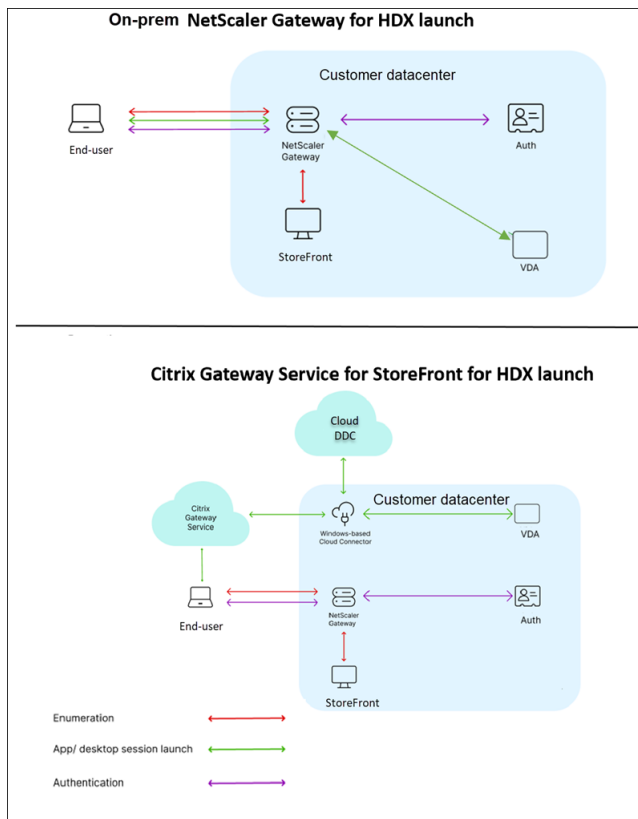
Citrix Gateway Service für StoreFront unterstützt die folgenden Anwendungsfälle:

- Authentifizierung und Sitzungsmanagement: Zwei-Faktor-Authentifizierung (LDAP, SAML) zusammen mit grundlegenden EPA-Scans
- HDX: HDX über TCP
- Smart Access

Die folgenden Anwendungsfälle werden nicht unterstützt:

- Nicht-HDX-Anwendungsfälle wie RDP-Proxy, VPN, PC over IP (PCoIP).

- Klassische Authentifizierungsrichtlinien



## Vorteile

- Das Citrix Cloud-Onboarding ist schneller und reibungsloser.
- Behält die Vorteile von on-premises StoreFront für die Enumeration und von On-Premises NetScaler Gateway für die Authentifizierung bei.
- Sorgt aufgrund der Multi-Cloud- und Multigeo-Architektur von Citrix Gateway Service für eine hohe Ausfallsicherheit.
- Die Leistungs- und Skalierungsanforderungen für HDX-Proxys werden jetzt vom Citrix Gateway Service verwaltet. Sie werden nicht mehr vom Kunden verwaltet.

## Voraussetzungen

- Verwenden Sie NetScaler 13.1 und höher. Einzelheiten finden Sie in der [NetScaler-Dokumentation](#).
- Verwenden Sie eine lokale StoreFront-Version 2311 oder höher mit konfigurierbarem Citrix DaaS. Einzelheiten finden Sie in den [StoreFront-Systemanforderungen](#).

- Onboarding von [Citrix Cloud](#) und Installation von [Citrix Cloud Connector](#). Cloud Connector in Ihrer on-premises Umgebung wird verwendet, um die Konnektivität mit Ihrem on-premises StoreFront über den Citrix Gateway Service herzustellen. Sie können einen vorhandenen Cloud Connector verwenden oder einen neuen bereitstellen. Wenn Ihr Connector-Upgrade deaktiviert ist, wenden Sie sich an den [Support](#), um es zu aktivieren.

Einzelheiten zu den Citrix Cloud Connector-Anforderungen finden Sie unter [Citrix Cloud Connector-Anforderungen](#). Einzelheiten zu den Größenanforderungen finden Sie unter [Überlegungen zu Größe und Skalierung für Cloud Connectors](#).

- Konfigurieren Sie einen NTP-Server (Network Time Protocol), um Zeitversatz zu vermeiden. Einzelheiten finden Sie unter [Synchronisieren der Systemuhr mit Servern im Netzwerk](#).

#### **Hinweis:**

Nur ein Windows-basierter Cloud Connector wird unterstützt. Connector Appliance wird nicht unterstützt.

## **Bereitstellen von Citrix Gateway Service für StoreFront**

Die Bereitstellung von Citrix Gateway Service für StoreFront umfasst die folgenden Schritte:

1. Lokales NetScaler Gateway für die Authentifizierung
2. Lokale StoreFront-Konfiguration für die Enumeration

### **1. Lokales NetScaler Gateway für die Authentifizierung**

Lokales NetScaler Gateway erleichtert direkt die Authentifizierung und stellt die Konnektivität mit dem on-premises StoreFront her. Mit diesem Ansatz können Sie die vorhandenen on-premises Ressourcen weiterhin für Authentifizierung, Enumeration und Pre-Launch verwenden.

Stellen Sie NetScaler Gateway on-premises am Rand des internen Netzwerks Ihrer Organisation bereit, um einen sicheren zentralen Zugriffspunkt auf Citrix Virtual Apps and Desktops bereitzustellen.

### **2. Lokale StoreFront-Konfiguration für die Enumeration**

In diesem Abschnitt werden die folgenden on-premises StoreFront-Konfigurationen beschrieben, die nach der Bereitstellung von Citrix Gateway Service für StoreFront ausgeführt werden müssen.

1. Remotezugriff auf den StoreFront-Store aktivieren
2. On-Premises NetScaler Gateway hinzufügen
3. Store für die Verwendung von Citrix Gateway Service für StoreFront konfigurieren

4. Startpfad einrichten

**1. Remotezugriff auf den StoreFront-Store aktivieren**

1. Wählen Sie **Stores** im rechten Bereich der on-premises StoreFront-GUI aus.
2. Wählen Sie im **Ergebnisbereich** einen Store aus und klicken Sie auf **RAS-Einstellungen konfigurieren**.
3. Wählen Sie die Option **Fernzugriff aktivieren**.

**2. On-Premises NetScaler Gateway hinzufügen** Dieser Schritt ermöglicht Benutzern, die eine Verbindung über öffentliche Netzwerke herstellen, den Zugriff auf die Stores von Citrix Gateway Service aus.

1. Klicken Sie im Abschnitt **Citrix Gateway-Appliances** auf **Hinzufügen**.

Configure Remote Access Settings - Store

Enabling remote access allows users outside the firewall to securely access resources. After you enable remote access, add a Citrix Gateway appliance.

Enable Remote Access

Select the permitted level of access to internal resources

Allow users to access only resources delivered through StoreFront (No VPN tunnel) ⓘ

Allow users to access all resources on the internal network (Full VPN tunnel) ⓘ  
Users may require the Citrix Gateway plug-in to establish a full VPN tunnel.

Citrix Gateway appliances:  ⓘ

Default appliance:

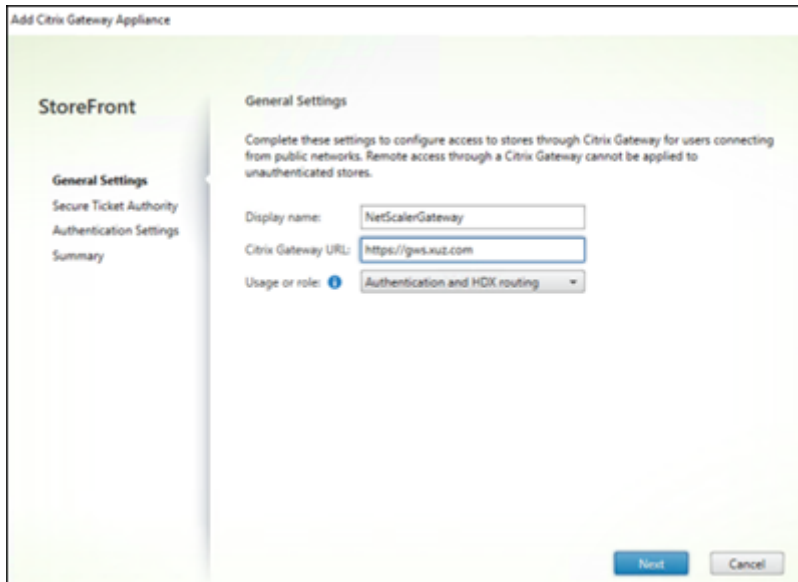
2. Konfigurieren Sie auf der Seite **Allgemeine Einstellungen** die folgenden Einstellungen:

- **Anzeigename:** Der Name des On-Premises NetScaler Gateway.
- **Citrix Gateway-URL:** FQDN des On-Premises NetScaler Gateway.
- **Verwendung oder Rolle:** Wählen Sie Authentifizierung und HDX-Routing aus.



**Hinweis:**

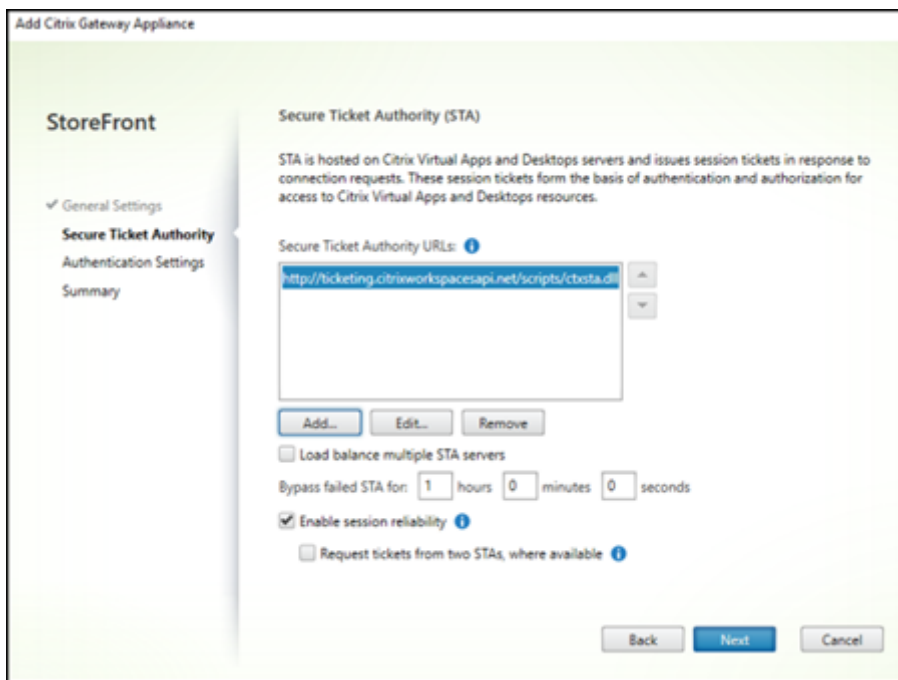
In diesem Abschnitt wird “NetScalerGateway” als Name des On-Premises NetScaler Gateway verwendet. Sie benötigen diesen Namen später, wenn Sie einen PowerShell-Befehl ausführen, um den Citrix Gateway Service für StoreFront zu aktivieren.



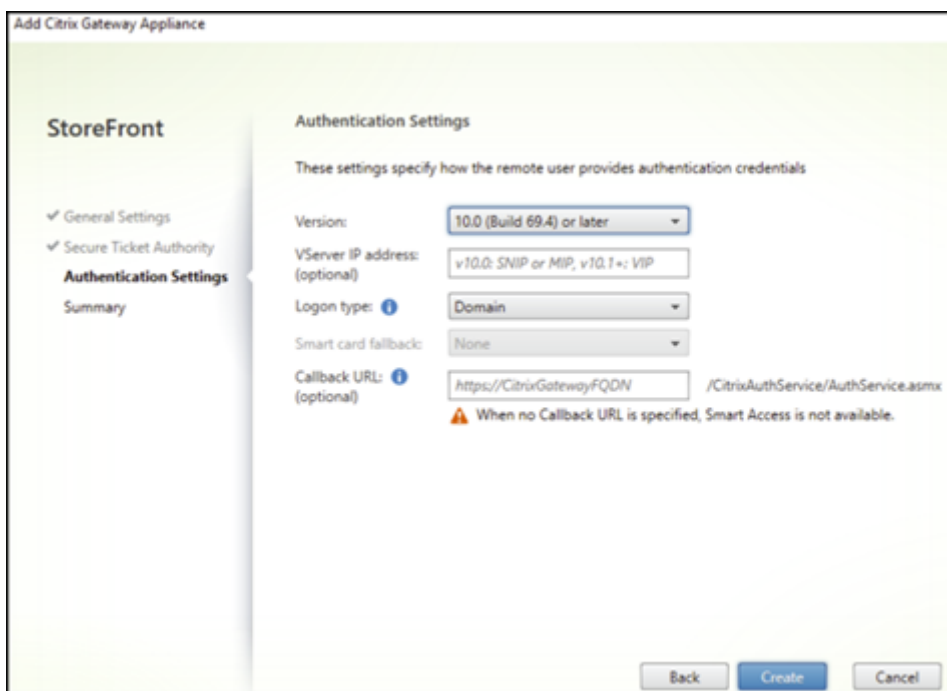
3. Fügen Sie auf der **Secure Ticket Authority (STA)**-Seite die STA-URL hinzu, die Sie zu dem Connector weiterleitet, der Ihre Anfragen an den Cloud STA-Dienst weiterleitet. Wählen Sie **Load Balancing für mehrere STA-Server** aus, wenn mehr als eine STA-URL konfiguriert ist.

**Hinweis:**

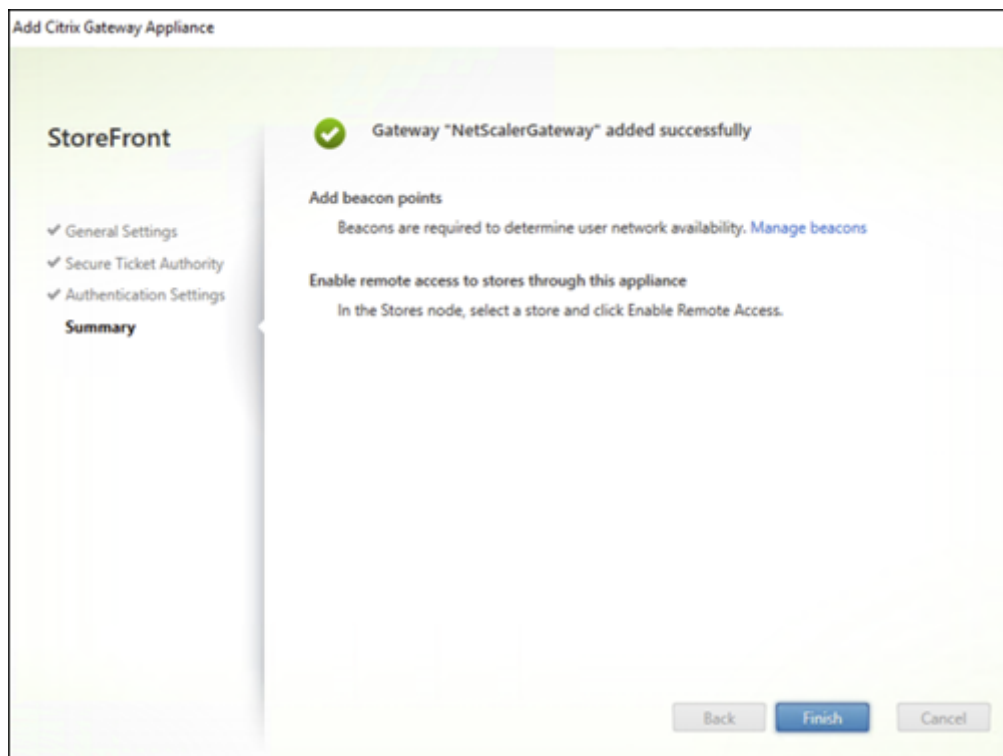
Stellen Sie sicher, dass das Kontrollkästchen **Sitzungszuverlässigkeit aktivieren** aktiviert ist.



4. Wählen Sie auf der Seite **Authentifizierungseinstellungen** die Version Ihres On-Premises NetScaler Gateway, den virtuellen Server und den Anmeldetyp aus und klicken Sie dann auf **Erstellen**.

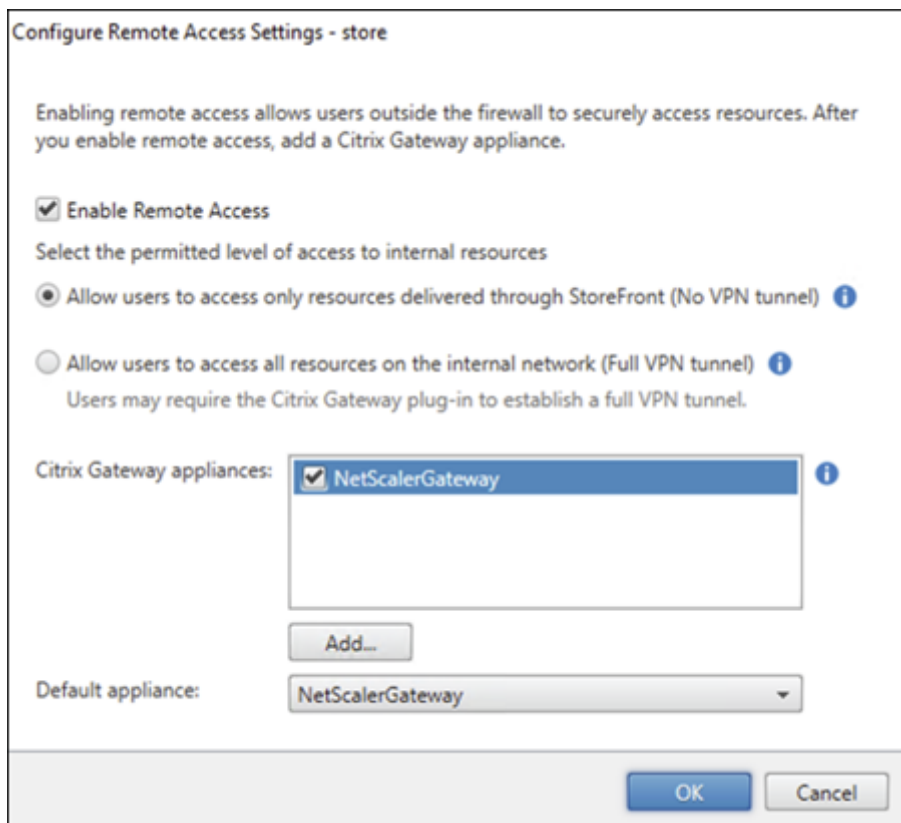


5. Auf der Seite **Zusammenfassung** wird eine Benachrichtigung angezeigt, dass das On-Premises NetScaler Gateway erfolgreich hinzugefügt wurde. Klicken Sie auf **Fertigstellen**.



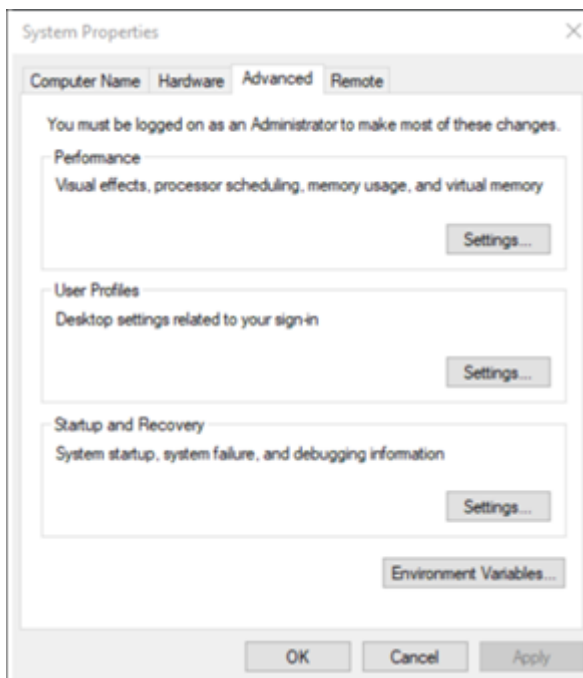
**3. Store für die Verwendung von Citrix Gateway Service für StoreFront konfigurieren** Mit diesem Schritt können Sie das On-Premises NetScaler Gateway Ihrem Store zuordnen.

1. Wählen Sie auf der Seite **Store > Remote Access-Einstellungen konfigurieren** Ihr lokales NetScaler Gateway aus und legen Sie es als Ihr Standardgerät fest.
2. Klicken Sie auf **OK**.

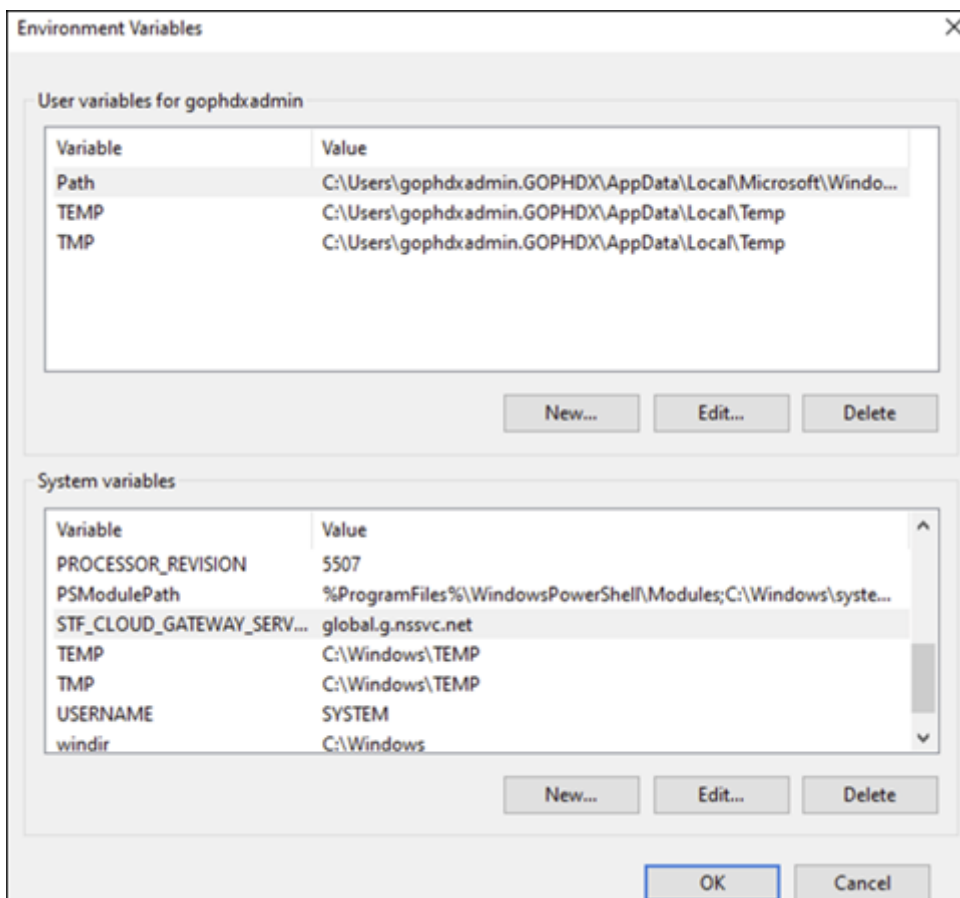


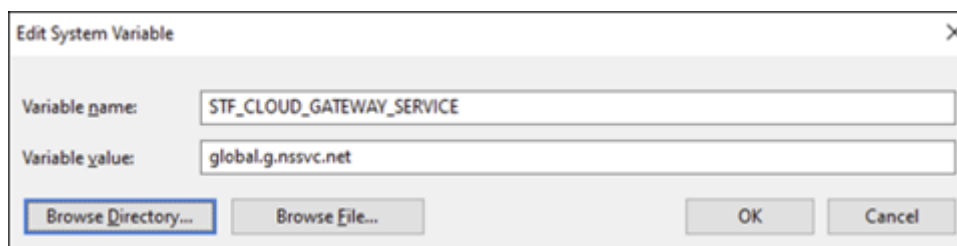
**4. Startpfad einrichten** Aktivieren Sie den Citrix Gateway Service-FQDN, um einen Pfad für den HDX-Start einzurichten.

1. Navigieren Sie auf Ihrem Gerät zu den **Systemeigenschaften** (führen Sie den Befehl `sysdm.cpl` in der Befehlszeile aus).
2. Gehen Sie zur Registerkarte **Erweitert** und klicken Sie auf **Umgebungsvariablen**.



3. Fügen Sie die Benutzer- und Systemvariablen hinzu. Weisen Sie den Variablen einen Namen und einen Wert zu und klicken Sie auf **OK**.





- Öffnen Sie Ihre Eingabeaufforderung als Administrator und führen Sie den Befehl `IISRESET` aus.

Verwenden Sie den folgenden PowerShell-Befehl, um die Cloud Gateway Service for StoreFront-Funktionalität für Ihre Bereitstellung zu aktivieren:

```
Set-STFRoamingGateway -Name "NetScalerGateway"-IsCloudGateway $true
```

Verwenden Sie den folgenden PowerShell-Befehl, um den Status Ihres Citrix Gateway Service für die On-Premises-StoreFront-Bereitstellung zu überprüfen.

```
1 Get-STFRoamingGateway | Format-Table Name, IsCloudGateway
2
3 Name          IsCloudGateway
4 # -----
5 # NetScalerGateway True
6 <!--NeedCopy-->
```

## Sicherheitsanforderungen

Bewährte Methoden zur NetScaler-Sicherheit finden Sie im [NetScaler Secure Deployment Guide](#).

## Problembehandlung

Stellen Sie sicher, dass Sie die Protokollebenen aktivieren, um die Citrix Gateway Service for StoreFront-Protokolle zu erfassen.

So aktivieren Sie Protokolle mit der NetScaler-GUI:

- Navigieren Sie zu **Konfiguration > System > Auditing**.
- Klicken Sie auf der Seite **Überwachung** unter **Einstellungen** auf **Auditing-Syslog-Einstellungen ändern**.
- Wählen **Sie unter Log Levels** die Option **ALLE** aus.

### Hinweis:

Stellen Sie sicher, dass Sie die Log-Level-Einstellungen nach der Fehlerbehebung wiederherstellen.

## Authentifizierung

- Informationen zur Behebung von Authentifizierungsproblemen finden Sie unter [Authentifizierungs-, Autorisierungs- und Auditprobleme beheben](#).
- Informationen zur Datenerfassung finden Sie unter [So sammeln Sie Daten für ADC Gateway-, Storefront- und VDA-Probleme](#).

## EPA

- **Problem:** Der EPA-Client ist bereits vorhanden, aber der Benutzer wird aufgefordert, ihn herunterzuladen:

**Mögliche Ursachen:** Versionskonflikt oder beschädigte Dateien

Führen Sie die Entwicklertools aus und überprüfen Sie, ob die Plug-in-Listendatei dieselbe Version wie die von NetScaler und Ihrem Client-Computer enthält. Stellen Sie sicher, dass die Citrix EPA-Clientversion mit der auf dem Client-Computer identisch ist.

**Problemumgehung:** Aktualisieren Sie den EPA-Client auf der On-Premises NetScaler Gateway-GUI, indem Sie zu **Citrix Gateway > Globale Einstellungen Clientbibliotheken aktualisieren** navigieren. Einzelheiten zu den EPA-Clientversionen finden Sie auf der Seite mit den [EPA-Plug-in-Bibliotheken](#) unter Citrix Downloads.

- Setzt die EPA-Einstellungen zurück (Immer, Ja, Nein), nachdem der Benutzer eine Option ausgewählt hat.

### Workaround:

- Navigieren Sie auf dem Client-Computer zu `C:\Users<user_name>\AppData\Local\Citrix\AGEE`.
- Öffnen Sie die Datei `config.js` und setzen Sie "trustAlways" auf "null". Zum Beispiel "trustAlways":null.

Anweisungen zu EPA-Konfigurationen finden Sie in den folgenden Artikeln:

- [Konfigurieren des EPA-Scans für die Vor- und Nachauthentifizierung als Faktor in der Multifaktorauthentifizierung \(nFactor\)](#)
- [Konfigurieren von NetScaler Gateway Vorauthentifizierung EPA-Scan für die Domänenprüfung](#)
- [Advanced Endpoint Analysis Scans](#)

## Sitzungsstart

Informationen zur Diagnose von Sitzungsstartfehlern finden Sie unter [Diagnose beim Sitzungsstart](#).

## Verfahren zur Erfassung von Protokollen für den allgemeinen Support

- **Technisches Support-Paket:** Einzelheiten finden Sie unter [So holen Sie das technische Support-Paket von VPX-Appliances zur Erkenntnisanalyse ab](#).
- **Trace-Dateien:** Einzelheiten finden Sie unter [So zeichnen Sie einen Paket-Trace auf NetScaler auf](#).
- Wenden Sie sich für weitere Informationen an den Support.

## Andere Referenzen

- [StoreFront-Always-On-Protokollierung](#)
- [EPA-Protokollsammlung](#)
- [Support](#)

## Bekannte Probleme und Einschränkungen

- Der HDX-Sitzungsstart schlägt fehl, wenn die Option Sitzungszuverlässigkeit aktivieren im on-premises StoreFront deaktiviert ist.
- Citrix Gateway Service für StoreFront unterstützt Dual-STA nicht.
- Über Citrix Workspace gestartete Anwendungen können nicht von iOS-Geräten geladen werden.

**Problemumgehung:** Führen Sie die folgenden CLI-Befehle über den Netscaler ADM-Konfigurationsjob aus, bevor Sie die Anwendungen über Citrix Workspace starten.

```
1  bind policy patset ns_aaa_relaystate_param_whitelist "
   citrixauthwebviewdone://" -index 1 -charset ASCII
2
3  bind policy patset ns_aaa_relaystate_param_whitelist "citrixsso
   ://" -index 2 -charset ASCII
4
5  bind policy patset ns_aaa_relaystate_param_whitelist "citrixng://
   " -index 3 -charset ASCII
6  <!--NeedCopy-->
```

## Kommende Verbesserungen

Die folgenden Verbesserungen sind in den kommenden Versionen geplant:

- HDX über EDT
- Unterstützung für lokalen Host-Cache



- Rendezvousprotokoll
- DDC (vor Ort)
- Multistore-Unterstützung

## Häufig gestellte Fragen

November 8, 2023

Dieser Abschnitt enthält die häufig gestellten Fragen zur Migration von Citrix ADC VPX zum Citrix Gateway Service für HDX-Proxy.

### **Kann ich meine On-Premises-Konfigurationen verwenden, um in Citrix Cloud zu portieren?**

Nein, die zugrundeliegende Infrastruktur und Mechanismen sind unterschiedlich. Siehe Abschnitt zur Aktivierung des Citrix Gateway Service.

### **Kann ich meine Portalanpassungen in Citrix Cloud hochladen?**

Das ist heute nicht möglich. Mit Citrix Cloud gibt es jedoch einige Anpassungsoptionen. Weitere Informationen finden Sie unter folgendem Link: <https://docs.citrix.com/en-us/xenapp-and-xendesktop/service/storefront.html>

### **Ich hatte die Multi-Faktor- oder Zwei-Faktor-Authentifizierung on-premises mit VPX aktiviert. Kann ich dies auch in der Cloud aktivieren?**

Das mit Citrix DaaS gelieferte VPX darf nur für HDX-Proxy (basierend auf EULA) und nicht für die Authentifizierung verwendet werden. Die Authentifizierung in der Cloud erfolgt mithilfe von on-premises AD über einen Cloud-Konnektor oder mithilfe von Azure Active Directory.

### **Kann ich SmartControl, SmartAccess mit Cloud-Services verwenden?**

Die Funktionen SmartAccess und SmartControl sind mit Citrix Gateway Service nicht verfügbar. Sie können diese Anforderungen jedoch mit dem [Citrix Device Posture Service](#) (für EPA-Scans) und dem [Citrix Adaptive Authentication Service](#) erfüllen.

## **Wie kann ich eine schrittweise Migration zum Citrix Gateway Service durchführen?**

Es gibt keine Konfiguration zur Unterstützung der Hybridbereitstellung (on-premises Citrix ADC VPX und Citrix Gateway Service). Es wird jedoch empfohlen, eine schrittweise Migration durchzuführen, indem Sie den Citrix Gateway Service mithilfe eines Testkontos (mit begrenztem Zeitraum) aktivieren und dieses für eine begrenzte Anzahl von Benutzern oder Vorschauenbenutzern verwenden.

## **Was ist die Mindestlizenz, die für den Citrix Gateway Service erforderlich ist?**

Jeder Kunde, der Citrix DaaS oder Citrix Workspace verwendet, ist berechtigt, Citrix Gateway Service for HDX Proxy zu verwenden.

## **Was passiert nachdem das Bandbreitenkontingent erschöpft ist?**

Sie können die Bandbreitennutzung im Dashboard zur Lizenzverwendung in Citrix Cloud überprüfen. Sobald das Bandbreitenkontingent erschöpft ist, läuft es wie gewohnt ohne Unterbrechungen. Kunden müssen jedoch mehr Bandbreite kaufen, für die sie sich an die Citrix Vertriebsvertreter wenden können.

Kunden von Citrix DaaS Advanced und Advanced Plus haben Anspruch auf die folgenden Lizenzen:

- Benutzerlizenzierung: 1 GB pro Benutzer und Monat
- Gleichzeitige Benutzerlizenzierung: 2 GB pro Benutzer und Monat

Citrix DaaS Premium- und Premium Plus-Kunden haben Anspruch auf die folgenden Lizenzen:

- Benutzerlizenzierung: 5 GB pro Benutzer und Monat
- Gleichzeitige Benutzerlizenzierung: 10 GB pro Benutzer und Monat

## **Wo kann ich die Metriken der Verbindungen einsehen, die über den Citrix Gateway Service hergestellt wurden?**

Das Connector-Statistik-Dashboard der Benutzeroberfläche von Citrix Analytics for Performance bietet einen umfassenden Überblick über den Ressourcenverbrauch des ausgewählten Connectors in den letzten 24 Stunden und eine Ansicht der synthetischen Latenz, die vom Connector zu den Citrix Gateway Service POPs in Ihrer virtuellen Apps- und Desktopumgebung berechnet wurde. Weitere Informationen finden Sie unter [Connector-Statistiken](#).



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).