# Citrix Gateway 13.0

**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



## Citrix Gateway Versionshinweise

March 27, 2024

Versionshinweise beschreiben, wie sich die Software in einem bestimmten Build geändert hat und welche Probleme in diesem Build bekannt sind.

Das Dokument mit den Versionshinweisen enthält alle oder einige der folgenden Abschnitte:

- **Was ist neu**: Die Verbesserungen und anderen Änderungen, die im Build veröffentlicht wurden.
- **Behobene Probleme**: Die Probleme, die im Build behoben wurden.
- **Bekannte Probleme**: Die Probleme, die im Build bestehen.
- **Zu beachtenswerte Punkte**: Die wichtigen Aspekte, die bei der Verwendung des Builds zu beachten sind.
- **Einschränkungen**: Die Einschränkungen, die im Build bestehen.

> **Wichtig:** Die Citrix Gateway Versionshinweise werden als Teil der Citrix ADC Versionshinweise behandelt.
> Ausführliche Informationen zu Verbesserungen von Citrix Gateway 13.0, bekannten Problemen und Fehlerbehebungen finden Sie auf der Seite mit Versionshinweisen.

**Hinweis:**

- Die [# XXXXXX]-Kennungen unter den Problembeschreibungen sind interne Tracking-IDs, die vom Citrix ADC-Team verwendet werden.
- Diese Versionshinweise dokumentieren keine sicherheitsrelevanten Korrekturen. Eine Liste mit sicherheitsrelevanten Fixes und Hinweisen finden Sie im Citrix Security Bulletin.

## Über Citrix Gateway

March 27, 2024

Citrix Gateway ist einfach bereitzustellen und einfach zu verwalten. Die typischste Bereitstellungskonfiguration besteht darin, das Citrix Gateway-Gerät in die DMZ zu platzieren. Sie können mehrere Citrix Gateway-Appliances für komplexere Bereitstellungen im Netzwerk installieren.

Wenn Sie Citrix Gateway zum ersten Mal starten, können Sie die Erstkonfiguration mithilfe einer seriellen Konsole, des Setup-Assistenten im Konfigurationsdienstprogramm oder dem Dynamic Host Configuration Protocol (DHCP) durchführen. Auf der MPX-Einheit können Sie die LCD-Tastatur an der Vorderseite des Geräts verwenden, um die Erstkonfiguration durchzuführen. Sie können

grundlegende Einstellungen konfigurieren, die für Ihr internes Netzwerk spezifisch sind, z. B. die IP-Adresse, die Subnetzmaske, die Standard-Gateway-IP-Adresse und die Domain Name System (DNS) -Adresse. Nachdem Sie die grundlegenden Netzwerkeinstellungen konfiguriert haben, konfigurieren Sie dann die für den Citrix Gateway-Vorgang spezifischen Einstellungen, z. B. die Optionen für Authentifizierung, Autorisierung, Netzwerkressourcen, virtuelle Server, Sitzungsrichtlinien und Endpunktrichtlinien.

Bevor Sie Citrix Gateway installieren und konfigurieren, lesen Sie die Themen in diesem Abschnitt, um Informationen zur Planung Ihrer Bereitstellung zu erhalten. Die Bereitstellungsplanung kann die Festlegung, wo die Appliance installiert werden soll, das Verständnis der Installation mehrerer Appliances in der DMZ und die Lizenzanforderungen umfassen. Sie können Citrix Gateway in jeder Netzwerkinfrastruktur installieren, ohne dass Änderungen an der vorhandenen Hardware oder Software erforderlich sind, die im sicheren Netzwerk ausgeführt wird. Citrix Gateway unterstützt andere Netzwerkprodukte wie Server-Load-Balancer, Cache-Engines, Firewalls, Router und IEEE 802.11-Wireless-Geräte.

Sie können Ihre Einstellungen in die Checkliste vor der Installation schreiben, die Sie zur Hand haben müssen, bevor Sie Citrix Gateway konfigurieren.

| | |
|---|---|
| Citrix Gateway-Geräte | Bietet Informationen zu Citrix Gateway-Geräten und Installationsanweisungen für das Gerät. |
| Checkliste vor der Installation | Bietet Planungsinformationen zur Überprüfung und eine Liste der Aufgaben, die vor der Installation von Citrix Gateway in Ihrem Netzwerk ausgeführt werden müssen. |
| Gemeinsame Bereitstellungen | Bietet Informationen zum Bereitstellen des Citrix Gateway in der Netzwerk-DMZ, in einem sicheren Netzwerk ohne DMZ und mit anderen Appliances zur Unterstützung von Lastenausgleich und Failover. Bietet auch Informationen zum Bereitstellen von Citrix Gateway mit Citrix Virtual Apps and Desktops. |
| Licensing | Bietet Informationen zur Installation von Lizenzen auf der Appliance. Bietet auch Informationen zum Installieren von Lizenzen auf mehreren Citrix Gateway-Appliances. |

### Citrix Gateway-Architektur

Die Kernkomponenten von Citrix Gateway sind:

- **Virtuelle Server**. Der virtuelle Citrix Gateway-Server ist eine interne Entität, die für alle konfigurierten Dienste repräsentativ ist, die Benutzern zur Verfügung stehen. Der virtuelle Server ist auch der Zugangspunkt, über den Benutzer auf diese Dienste zugreifen. Sie können mehrere virtuelle Server auf einer einzelnen Appliance konfigurieren, sodass eine Citrix Gateway-Appliance mehrere Benutzergemeinschaften mit unterschiedlichen Authentifizierungs- und Ressourcenzugriffsanforderungen bedienen kann.
- **Authentifizierung, Autorisierung und Prüfung**. Sie können Authentifizierung, Autorisierung und Buchhaltung so konfigurieren, dass Benutzer sich mit Anmeldeinformationen bei Citrix Gateway anmelden können, die entweder Citrix Gateway oder Authentifizierungsserver im sicheren Netzwerk wie LDAP oder RADIUS erkennen. Autorisierungsrichtlinien definieren Benutzerberechtigungen und legen fest, auf welche Ressourcen ein bestimmter Benutzer zugreifen darf. Weitere Informationen zur Authentifizierung und Autorisierung finden Sie unter Konfigurieren von Authentifizierung und Autorisierung. Audit-Server verwalten Daten über Citrix Gateway-Aktivitäten, einschließlich Benutzeranmeldeereignisse, Instanzen des Ressourcenzugriffs und Betriebsfehler. Diese Informationen werden auf Citrix Gateway oder auf einem externen Server gespeichert. Weitere Informationen zur Überwachung finden Sie unter Konfiguration der Überwachung auf Citrix Gateway
- **Benutzerverbindungen**. Benutzer können sich mithilfe der folgenden Zugriffsmethoden bei Citrix Gateway anmelden:
  - Das Citrix Gateway Plug-in für Windows ist Software, die auf einem Windows-basierten Computer installiert ist. Benutzer melden sich an, indem sie mit der rechten Maustaste auf ein Symbol im Infobereich eines Windows-basierten Computers klicken. Wenn Benutzer einen Computer verwenden, auf dem das Citrix Gateway-Plug-in nicht installiert ist, können sie sich mithilfe eines Webbrowsers anmelden, um das Plug-in herunterzuladen und zu installieren. Wenn Benutzer die Citrix Workspace-App installiert haben, melden sich Benutzer mit dem Citrix Gateway Plug-in über die Citrix Workspace-App an. Wenn die Citrix Workspace-App und das Citrix Gateway-Plug-In auf dem Benutzergerät installiert sind, fügt die Citrix Workspace-App das Citrix Gateway-Plug-In automatisch hinzu.
  - Das Citrix Gateway Plug-in für macOS X, mit dem Benutzer, die macOS X ausführen, sich anmelden können. Es hat dieselben Funktionen und Funktionen wie das Citrix Gateway Plug-in für Windows. Sie können Endpoint Analysis-Unterstützung für diese Plug-In-Version bereitstellen, indem Sie Citrix ADC Gateway 10.1, Build 120.1316.e installieren.
  - Citrix Workspace-App, die Benutzerverbindungen zu veröffentlichten Anwendungen und virtuellen Desktops in einer Serverfarm mithilfe des Webinterface oder Citrix StoreFront ermöglicht.

  - Citrix Workspace-App, Secure Hub, WorxMail und WorxWeb, die Benutzern den Zugriff auf Web- und SaaS-Anwendungen, iOS- und Android-Mobilanwendungen sowie ShareFile-Daten ermöglichen, die in Citrix Endpoint Management gehostet werden.
  - Benutzer können von einem Android-Gerät aus eine Verbindung herstellen, das die Citrix Gateway-Webadresse verwendet. Wenn Benutzer eine App starten, verwendet die Verbindung Micro VPN, um den Netzwerkverkehr an das interne Netzwerk weiterzuleiten. Wenn Benutzer von einem Android-Gerät aus eine Verbindung herstellen, müssen Sie DNS-Einstellungen auf Citrix Gateway konfigurieren. Weitere Informationen finden Sie unter Unterstützung von DNS-Abfragen mithilfe von DNS-Suffixen für Android-Geräte.
  - Benutzer können von einem iOS-Gerät aus eine Verbindung herstellen, das die Citrix Gateway-Webadresse verwendet. Sie konfigurieren Secure Browse entweder global oder in einem Sitzungsprofil. Wenn Benutzer eine App auf ihrem iOS-Gerät starten, wird eine VPN-Verbindung gestartet und die Verbindung wird über Citrix Gateway geleitet.
  - Clientloser Zugriff, der Benutzern den Zugriff bietet, den sie benötigen, ohne Software auf dem Benutzergerät zu installieren.

    Bei der Konfiguration von Citrix Gateway können Sie Richtlinien erstellen, um zu konfigurieren, wie sich Benutzer anmelden. Sie können die Benutzeranmeldung auch einschränken, indem Sie Sitzungs- und Endpoint Analysis-Richtlinien erstellen.

- **Netzwerkressourcen**. Dazu gehören alle Netzwerkdienste, auf die Benutzer über Citrix Gateway zugreifen, wie Dateiserver, Anwendungen und Websites.
- **Virtueller Adapter**. Der virtuelle Citrix Gateway-Adapter unterstützt Anwendungen, die IP-Spoofing erfordern. Der virtuelle Adapter wird auf dem Benutzergerät installiert, wenn das Citrix Gateway Plug-in installiert ist. Wenn Benutzer eine Verbindung zum internen Netzwerk herstellen, verwendet die ausgehende Verbindung zwischen Citrix Gateway und internen Servern die Intranet-IP-Adresse als Quell-IP-Adresse. Das Citrix Gateway Plug-in erhält diese IP-Adresse vom Server als Teil der Konfiguration.

  Wenn Sie Split-Tunneling auf Citrix Gateway aktivieren, wird der gesamte Intranet-Verkehr über den virtuellen Adapter geleitet. Beim Abfangen von intranetgebundenem Datenverkehr fängt der virtuelle Adapter DNS-Abfragen vom Typ A und AAAA ab, während alle anderen DNS-Abfragen intakt bleiben. Netzwerkverkehr, der nicht an das interne Netzwerk gebunden ist, wird über den auf dem Benutzergerät installierten Netzwerkadapter geleitet. Internet- und private LAN (LAN) -Verbindungen bleiben offen und verbunden. Wenn Sie das Split-Tunneling deaktivieren, werden alle Verbindungen über den virtuellen Adapter geroutet. Alle vorhandenen Verbindungen werden getrennt und der Benutzer muss die Sitzung erneut herstellen.

  Wenn Sie eine Intranet-IP-Adresse konfigurieren, wird der Datenverkehr zum internen Netzwerk über den virtuellen Adapter mit der Intranet-IP-Adresse gefälscht.

## So funktionieren Benutzerverbindungen

Benutzer können von einem Remote-Standort aus eine Verbindung zu ihren E-Mails, Dateifreigaben und anderen Netzwerkressourcen herstellen. Benutzer können mit der folgenden Software eine Verbindung zu internen Netzwerkressourcen herstellen:

- Citrix Gateway Plug-in
- Citrix Workspace-App
- WorxMail und WorxWeb
- Android- und iOS-Mobilgeräte

## Verbinden Sie sich mit dem Citrix Gateway Plug-in

Das Citrix Gateway Plug-in ermöglicht Benutzern den Zugriff auf Ressourcen im internen Netzwerk durch die folgenden Schritte:

1. Ein Benutzer stellt zum ersten Mal eine Verbindung zu Citrix Gateway her, indem er die Webadresse in einen Webbrowser eingibt. Die Anmeldeseite wird angezeigt und der Benutzer wird aufgefordert, einen Benutzernamen und ein Kennwort einzugeben. Wenn externe Authentifizierungsserver konfiguriert sind, kontaktiert Citrix Gateway den Server und die Authentifizierungsserver überprüfen die Anmeldeinformationen des Benutzers. Wenn die lokale Authentifizierung konfiguriert ist, führt Citrix Gateway die Benutzerauthentifizierung durch.
2. Wenn Sie eine Vorauthentifizierungsrichtlinie konfigurieren und der Benutzer die Citrix Gateway-Webadresse in einem Webbrowser auf einem Windows-basierten Computer oder einem macOS X-Computer eingibt, prüft Citrix Gateway, ob clientbasierte Sicherheitsrichtlinien vorhanden sind, bevor die Anmeldeseite angezeigt wird. Die Sicherheitsüberprüfungen stellen sicher, dass das Benutzergerät die sicherheitsrelevanten Bedingungen wie Betriebssystemupdates, Antivirenschutz und eine ordnungsgemäß konfigurierte Firewall erfüllt. Wenn das Benutzergerät die Sicherheitsüberprüfung nicht besteht, blockiert Citrix Gateway den Benutzer an der Anmeldung. Ein Benutzer, der sich nicht anmelden kann, muss die erforderlichen Updates oder Pakete herunterladen und auf dem Benutzergerät installieren. Wenn das Benutzergerät die Vorauthentifizierungsrichtlinie übergibt, wird die Anmeldeseite angezeigt und der Benutzer kann die Anmeldedaten eingeben. Sie können Advanced Endpoint Analysis auf einem macOS X-Computer verwenden, wenn Sie Citrix Gateway 10.1, Build 120.1316.e installieren.
3. Wenn Citrix Gateway den Benutzer erfolgreich authentifiziert, initiiert Citrix Gateway den VPN-Tunnel. Citrix Gateway fordert den Benutzer auf, das Citrix Gateway-Plug-In für Windows oder das Citrix Gateway-Plug-In für macOS X herunterzuladen und zu installieren.
4. Wenn Sie einen Scan nach der Authentifizierung konfigurieren, durchsucht Citrix Gateway nach der erfolgreichen Anmeldung eines Benutzers das Benutzergerät nach den erforder-

lichen Clientsicherheitsrichtlinien. Sie können dieselben sicherheitsrelevanten Bedingungen wie für eine Vorauthentifizierungsrichtlinie verlangen. Wenn das Benutzergerät den Scan nicht besteht, wird entweder die Richtlinie nicht angewendet oder der Benutzer wird in eine Quarantänegruppe versetzt und der Zugriff des Benutzers auf Netzwerkressourcen ist begrenzt.

5. Wenn die Sitzung eingerichtet ist, wird der Benutzer zu einer Citrix Gateway-Homepage weitergeleitet, auf der der Benutzer Ressourcen für den Zugriff auswählen kann. Die Homepage, die in Citrix Gateway enthalten ist, wird Access Interface genannt. Wenn sich der Benutzer mithilfe des Citrix Gateway-Plug-ins für Windows anmeldet, zeigt ein Symbol im Infobereich auf dem Windows-Desktop an, dass das Benutzergerät verbunden ist und der Benutzer eine Meldung erhält, dass die Verbindung hergestellt wurde. Der Benutzer kann auch auf Ressourcen im Netzwerk zugreifen, ohne das Access Interface zu verwenden, z. B. das Öffnen von Microsoft Outlook und das Abrufen von E-Mails.
6. Wenn die Benutzeranforderung sowohl Sicherheitschecks vor als auch nach der Authentifizierung besteht, kontaktiert Citrix Gateway dann die angeforderte Ressource und stellt eine sichere Verbindung zwischen dem Benutzergerät und dieser Ressource her.
7. Der Benutzer kann eine aktive Sitzung schließen, indem er im Infobereich eines Windows-basierten Computers mit der rechten Maustaste auf das Citrix Gateway-Symbol klickt und dann auf Abmelden klickt. Die Sitzung kann auch aufgrund von Inaktivität ausfallen. Wenn die Sitzung geschlossen wird, wird der Tunnel heruntergefahren und der Benutzer hat keinen Zugriff mehr auf interne Ressourcen. Der Benutzer kann die Citrix Gateway-Webadresse auch in einen Browser eingeben. Wenn der Benutzer die Eingabetaste drückt, wird das Access Interface angezeigt, von dem sich Benutzer abmelden können.

**Hinweis:** Wenn Sie Citrix Endpoint Management in Ihrem internen Netzwerk bereitstellen, muss ein Benutzer, der von außerhalb des internen Netzwerks eine Verbindung herstellt, zuerst eine Verbindung mit Citrix Gateway herstellen. Wenn der Benutzer die Verbindung herstellt, kann der Benutzer auf Web- und SaaS-Anwendungen, Android- und iOS-Mobilanwendungen sowie ShareFile-Daten zugreifen, die auf Citrix Endpoint Management gehostet werden. Ein Benutzer kann sich über clientlosen Zugriff oder mithilfe der Citrix Workspace-App oder Secure Hub mit dem Citrix Gateway-Plug-in verbinden.

### Verbinden Sie sich mit der Citrix Workspace-App

Benutzer können sich mit der Citrix Workspace-App verbinden, um auf ihre Windows-basierten Anwendungen und virtuellen Desktops zuzugreifen. Benutzer können auch von Endpoint Management aus auf Anwendungen zugreifen. Um von einem Remote-Standort aus eine Verbindung herzustellen, installieren Benutzer auch das Citrix Gateway-Plug-in auf ihrem Gerät. Die Citrix Workspace-App fügt das Citrix Gateway-Plug-in automatisch zu seiner Liste der Plug-Ins hinzu. Wenn sich Benutzer bei der Citrix Workspace-App anmelden, können sie sich auch am Citrix Gateway Plug-in anmelden. Sie können Citrix Gateway auch so konfigurieren, dass einmaliges Anmelden am Citrix Gateway Plug-in

durchgeführt wird, wenn sich Benutzer bei der Citrix Workspace-App anmelden.

### Verbinden Sie sich mit iOS- und Android-Geräten

Benutzer können mithilfe von Secure Hub eine Verbindung von einem iOS- oder Android-Gerät herstellen. Benutzer können mithilfe von Secure Mail auf ihre E-Mails zugreifen und mit WorxWeb eine Verbindung zu Websites herstellen.

Wenn Benutzer über das mobile Gerät eine Verbindung herstellen, werden die Verbindungen über Citrix Gateway geleitet, um auf interne Ressourcen zuzugreifen. Wenn Benutzer eine Verbindung mit iOS herstellen, aktivieren Sie Secure Browse als Teil des Sitzungsprofils. Wenn Benutzer eine Verbindung mit Android herstellen, verwendet die Verbindung das Micro-VPN automatisch. Darüber hinaus verwenden
Secure Mail und WorxWeb Micro VPN, um Verbindungen über Citrix Gateway herzustellen. Sie müssen Micro VPN nicht auf Citrix Gateway konfigurieren.

## Häufige Citrix Gateway-Bereitstellungen

March 27, 2024

Sie können Citrix Gateway am Umfang des internen Netzwerks (oder Intranets) Ihres Unternehmens bereitstellen, um einen sicheren zentralen Zugriffspunkt für die Server, Anwendungen und andere Netzwerkressourcen bereitzustellen, die sich im internen Netzwerk befinden. Alle Remote-Benutzer müssen eine Verbindung zu Citrix Gateway herstellen, bevor sie auf Ressourcen im internen Netzwerk zugreifen können.

Citrix Gateway wird am häufigsten an den folgenden Speicherorten in einem Netzwerk installiert:

- Im Netzwerk DMZ
- In einem sicheren Netzwerk, das kein DMZ besitzt

Sie können Citrix Gateway auch mit Citrix Virtual Apps, Citrix Virtual Desktops, StoreFront und Citrix Endpoint Management bereitstellen, um Benutzern den Zugriff auf ihre Windows-, Web-, Mobil- und SaaS-Anwendungen zu ermöglichen. Wenn Ihre Bereitstellung Citrix Virtual Apps, StoreFront und Desktops 7 umfasst, können Sie Citrix Gateway in einer Single-Hop- oder Double-Hop-DMZ-Konfiguration bereitstellen. Eine Double-Hop-Bereitstellung wird mit früheren Versionen von Citrix Virtual Desktops oder Citrix Endpoint Management nicht unterstützt.

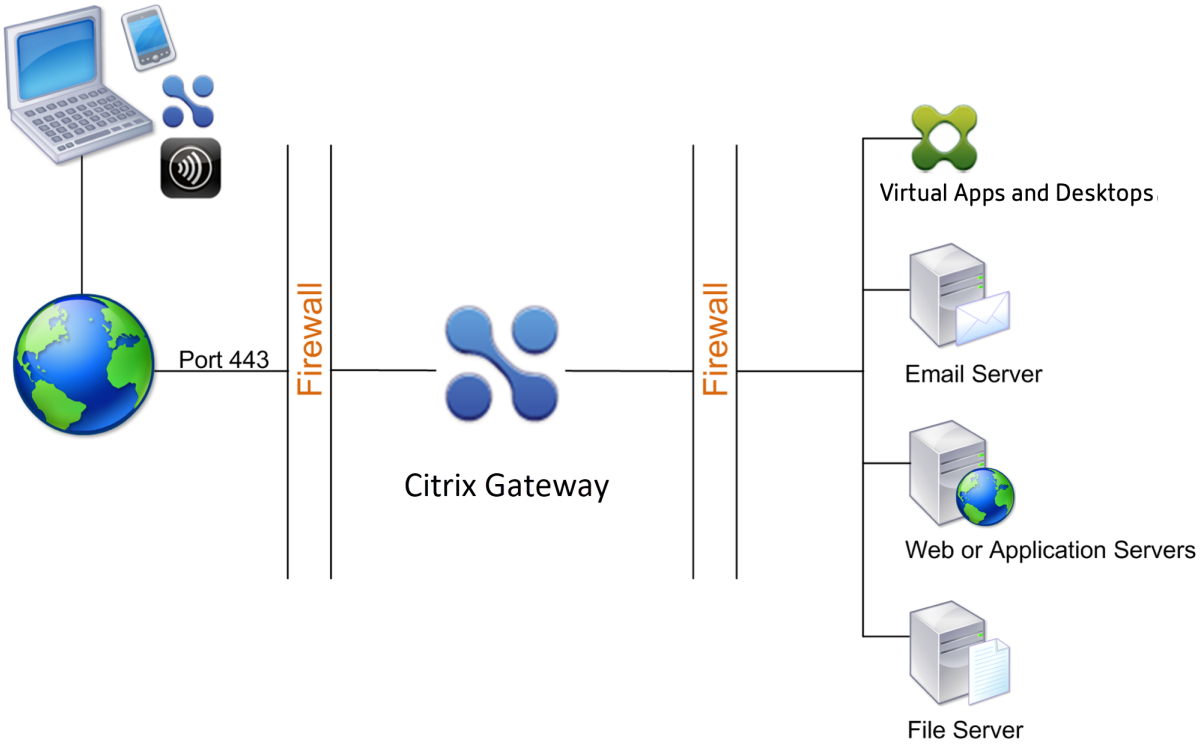
Weitere Informationen zum Erweitern Ihrer Citrix Gateway-Installation mit diesen und anderen unterstützten Citrix Lösungen finden Sie im Thema Integration mit Citrix Produkten.

## Bereitstellen von Citrix Gateway in einer DMZ

Viele Unternehmen schützen ihr internes Netzwerk mit einer DMZ. Eine DMZ ist ein Subnetz, das zwischen dem sicheren internen Netzwerk einer Organisation und dem Internet (oder einem externen Netzwerk) liegt. Wenn Sie Citrix Gateway in der DMZ bereitstellen, stellen Benutzer eine Verbindung mit dem Citrix Gateway Plug-In oder der Citrix Workspace-App her.

Abbildung 1. Citrix Gateway in der DMZ bereitgestellt




In der in der vorhergehenden Abbildung gezeigten Konfiguration installieren Sie Citrix Gateway in der DMZ und konfigurieren es so, dass eine Verbindung zum Internet und zum internen Netzwerk hergestellt wird.

## Citrix Gateway-Konnektivität in einer DMZ

Wenn Sie Citrix Gateway in der DMZ bereitstellen, müssen Benutzerverbindungen die erste Firewall durchqueren, um eine Verbindung zu Citrix Gateway herzustellen. Standardmäßig verwenden Benutzerverbindungen SSL an Port 443, um diese Verbindung herzustellen. Damit Benutzerverbindungen das interne Netzwerk erreichen können, müssen Sie SSL an Port 443 über die erste Firewall zulassen.

Citrix Gateway entschlüsselt die SSL-Verbindungen vom Benutzergerät und stellt im Namen des Benutzers eine Verbindung zu den Netzwerkressourcen hinter der zweiten Firewall her. Die Ports, die

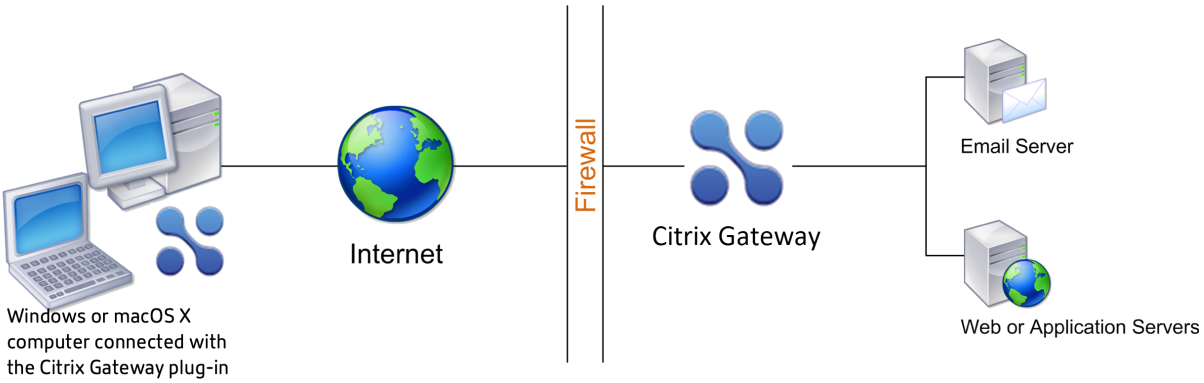
durch die zweite Firewall geöffnet sein müssen, sind von den Netzwerkressourcen abhängig, auf die Sie externen Benutzern Zugriff gewähren.

Wenn Sie beispielsweise externen Benutzern den Zugriff auf einen Webserver im internen Netzwerk autorisieren und dieser Server auf HTTP-Verbindungen an Port 80 wartet, müssen Sie HTTP auf Port 80 über die zweite Firewall zulassen. Citrix Gateway stellt die Verbindung über die zweite Firewall zum HTTP-Server im internen Netzwerk im Namen der externen Benutzergeräte her.

### Bereitstellen von Citrix Gateway in einem sicheren Netzwerk

Sie können Citrix Gateway im sicheren Netzwerk installieren. In diesem Szenario steht eine Firewall zwischen dem Internet und dem sicheren Netzwerk. Citrix Gateway ist in der Firewall, um den Zugriff auf die Netzwerkressourcen zu steuern.

Abbildung 1. Citrix Gateway wird im sicheren Netzwerk bereitgestellt




Wenn Sie Citrix Gateway im sicheren Netzwerk bereitstellen, verbinden Sie eine Schnittstelle auf Citrix Gateway mit dem Internet und die andere Schnittstelle mit Servern, die im sicheren Netzwerk ausgeführt werden. Das Einfügen von Citrix Gateway in das sichere Netzwerk bietet lokalen und Remote-Benutzern Zugriff. Da diese Konfiguration nur über eine Firewall verfügt, ist die Bereitstellung für Benutzer, die sich von einem Remote-Standort aus verbinden, weniger sicher. Obwohl Citrix Gateway Datenverkehr aus dem Internet abfängt, gelangt der Datenverkehr in das sichere Netzwerk, bevor Benutzer authentifiziert werden. Wenn Citrix Gateway in einer DMZ bereitgestellt wird, werden Benutzer authentifiziert, bevor der Netzwerkverkehr das sichere Netzwerk erreicht.

Wenn Citrix Gateway im sicheren Netzwerk bereitgestellt wird, müssen Citrix Gateway-Plug-In-Verbindungen die Firewall durchqueren, um eine Verbindung zu Citrix Gateway herzustellen. Standardmäßig verwenden Benutzerverbindungen das SSL-Protokoll an Port 443, um diese Verbindung herzustellen. Um diese Konnektivität zu unterstützen, müssen Sie Port 443 an der Firewall öffnen.

# Client-Softwareanforderungen

March 27, 2024

Citrix Gateway unterstützt Benutzerverbindungen mithilfe des Citrix Gateway Plug-Ins. Wenn sich Benutzer mit dem Plug-In anmelden, wird ein vollständiger VPN-Tunnel eingerichtet. Mit dem Citrix Gateway Plug-in können Benutzer eine Verbindung zu den Netzwerkressourcen herstellen, auf die Sie Zugriff gewähren.

Wenn Endpunktrichtlinien auf Citrix Gateway konfiguriert sind, lädt Citrix Gateway den Citrix EPA-Client automatisch herunter und installiert ihn auf dem Benutzergerät, wenn sich Benutzer anmelden.

## Systemanforderungen für das Citrix Gateway Plug-in

Das Citrix Gateway Plug-in stellt eine sichere Verbindung vom Clientcomputer zur Citrix Gateway-Appliance her.

Das Plug-In wird als Desktop-App für Microsoft Windows-, macOS X- und Linux-Betriebssysteme verteilt. Nachdem Sie sich mit Ihrem Webbrowser bei der sicheren URL des Citrix Gateway-Geräts authentifiziert haben, wird das Plug-In automatisch heruntergeladen und auf Ihrem Computer installiert.

Das Plug-In wird als mobile App für Android- und iOS-Geräte bereitgestellt.

> **Hinweis:**
>
> - Um das Plug-In zu installieren, sind Admin-/Root-Rechte für das Betriebssystem erforderlich.
> - Die Browser, die das Citrix Gateway Plug-in unterstützen, unterstützen auch clientloses VPN.

Das Citrix Gateway Plug-in als Desktop-App wird für die folgenden Betriebssysteme und Webbrowser unterstützt.

| Betriebssystem | Unterstützte Browser |
| --- | --- |
| macOS X (10.9 und höher) | Safari 7.1 oder höher; Google Chrome Release 30 oder höher; Mozilla Firefox Release 30 oder höher |

| Betriebssystem | Unterstützte Browser |
| --- | --- |
| Windows 10 (x86 und x64) | Internet Explorer 11; Google Chrome Release 30 oder höher; Mozilla Firefox Release 24 oder höher; Edge Chromium |
| Linux; Ubuntu 18.04 LTS 32-Bit- und 64-Bit-Betriebssysteme werden unterstützt. | Mozilla Firefox Release 44 und höher; Google Chrome 50 und höher |

Wenn die erforderlichen Abhängigkeitspakete fehlen, listet der Befehl sie auf und die Installation des Plug-Ins schlägt fehl. Diese Abhängigkeitspakete müssen manuell installiert werden. Administratoren können ein fehlendes Paket installieren, indem sie den folgenden Befehl über die Befehlszeilenschnittstelle eingeben.

```
apt-get install <dependency package>
<!--NeedCopy-->
```

Das Citrix Gateway Plug-in als mobile App wird für die folgenden Betriebssysteme unterstützt.

| VPN-App | Unterstützte Betriebssysteme |
| --- | --- |
| Android | Android 7.0 und höher |
| iOS | iOS 12.0 und höher |

> **Hinweis:**
>
> Wenn Sie die neuesten Apple OS-Versionen wie macOS 14/iOS 17 und höher verwenden, empfehlen wir Ihnen, auf Citrix Secure Access Client/Citrix SSO Version 23.09.1 oder höher zu aktualisieren.

### Anforderungen für Endpoint Analysis

Citrix Gateway installiert den Citrix EPA-Client auf dem Benutzergerät. Der Citrix EPA-Client durchsucht das Benutzergerät nach den Endpunktsicherheitsanforderungen, die Sie auf NetScaler Gateway konfiguriert haben. Zu den Anforderungen gehören Informationen wie das Betriebssystem, das Antivirenprogramm oder die Webbrowser-Versionen.

Wenn Benutzer zum ersten Mal über den Browser eine Verbindung zu Citrix Gateway herstellen, fordert das Portal die Installation des Citrix EPA-Clients an. Bei nachfolgenden Anmeldeversuchen überprüft der Citrix EPA-Client die Konfiguration der Upgradesteuerung, um zu bestätigen, ob das Citrix EPA-Client-Upgrade erforderlich ist. Falls erforderlich, wird der Benutzer aufgefordert, den neuesten Citrix EPA-Client herunterzuladen und zu installieren. Der Citrix EPA-Client für Windows wird als 32-Bit-

Anwendung für Windows installiert. Der Citrix EPA-Client für macOS wird als 64-Bit-Anwendung installiert. Für die Installation oder Verwendung des Citrix EPA-Clients sind keine besonderen Rechte erforderlich, außer wenn EPA für den Zugriff auf Gerätezertifikate verwendet wird. Einzelheiten zur Verwendung von EPA für die Authentifizierung von Gerätezertifikaten finden Sie unter Verwenden von Gerätezertifikaten für die Authentifizierung.

Die Tooltips auf der Admin-UI-Konsole erklären die Scans im Detail. Einzelheiten zu den EPA-Bibliotheken finden Sie unter https://www.citrix.com/en-in/downloads/citrix-gateway/epa-libraries/.

> **Wichtig:**
>
> - Die Browser, die EPA unterstützen, unterstützen auch clientloses VPN.
> - Bei der Endpunktanalyse vor der Authentifizierung kann sich der Benutzer nicht mit dem Citrix Gateway Plug-in anmelden, wenn der Benutzer das Endpoint Analysis-Plug-in nicht installiert oder den Scan überspringt.
> - Bei der Endpunktanalyse nach der Authentifizierung kann der Benutzer auf Ressourcen zugreifen, für die kein Scan erforderlich ist, indem er entweder clientlosen Zugriff verwendet oder die Citrix Workspace-App verwendet.
> - Für OPSWAT-bezogene Scans müssen Sie das Binärpaket `epaPackage.exe` auf dem Clientcomputer installieren.

Die folgende Software ist auf den Benutzergeräten erforderlich, um das Endpoint Analysis-Plug-In verwenden zu können:

| Betriebssystem | Unterstützte Browser |
|---|---|
| macOS (10.9 und höher) | Safari 7.1 oder höher; Google Chrome Release 30 oder höher; Mozilla Firefox Release 30 oder höher |
| Windows 10 | Internet Explorer 11; Google Chrome Release 30 oder höher; Mozilla Firefox Release 24 oder höher; Edge Chromium |
| Linux; Ubuntu 18.04 LTS. Sowohl 32-Bit- als auch 64-Bit-Betriebssysteme werden unterstützt. Sowohl 32-Bit- als auch 64-Bit-Betriebssysteme werden unterstützt. | Mozilla Firefox Release 44 und höher; Google Chrome 50 und höher |

**Hinweis:**

- Alle zuvor erwähnten Editionen der Betriebssystemvarianten werden unterstützt.

- Windows 10 und Windows 11 im S-Modus werden nicht unterstützt.
- Für Windows-Editionen müssen alle Service Packs und kritischen Updates installiert sein.
- Für Internet Explorer-Versionen müssen Cookies aktiviert sein. Die erforderliche Mindestversion ist 7.0.
- Für Mozilla Firefox-Versionen muss Endpoint Analysis Plug-in-aktiviert sein, die erforderliche Mindestversion ist 3.0.
- Derzeit unterstützen der Citrix Secure Access Client und der Citrix EPA-Client für Ubuntu nur den standardmäßigen GNOME-Display-Manager.

## Citrix Gateway-Kompatibilität mit Citrix Produkten

March 27, 2024

Die folgende Tabelle enthält die Citrix Produkte und Versionen, mit denen Citrix Gateway 13.0 kompatibel ist.

> **Hinweis:**
>
> Citrix Gateway-Funktionen sind auf Citrix ADC VPX verfügbar.

### Citrix Produkte und unterstützte Versionen

| Citrix Produkt | Version freigeben |
|---|---|
| Citrix SD-WAN | 10.2, 11.0 |
| Citrix ADC-Plattformen | Alle aktuellen MPX- und VPX-Modelle einschließlich FIPS-konformer Appliances. |
| StoreFront | Alle derzeit unterstützten StoreFront-Versionen. |
| Citrix Virtual Apps and Desktops | 7,15, 1808, 1811, 1903, 1906, 1909, 2003, 2009, 2112, 1912 LTSR, 2203 LTSR |
| XenMobile | 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12 |

### Citrix Workspace-Apps, mobile Produktivitätsapps von Citrix und Plug-Ins

*Der erste unterstützte Build für jede Softwareversion ist in der folgenden Tabelle aufgeführt. Alle nachfolgenden Builds werden unterstützt, sofern nicht anders angegeben. Weitere Informationen zum Release-Lebenszyklus finden Sie in derProduktmatrix.

| Citrix Workspace-App oder Plug-In | Unterstützte Mindestversion* |
|---|---|
| Citrix Gateway Plug-in für macOS X | 3.1.8 |
| Citrix Gateway Plug-in für Windows | 12.0 |
| Citrix Gateway Plug-in für iOS | 3.1.4 |
| Citrix Gateway Plug-in für Android | 2.0.14 |
| Citrix Workspace-App für Android | 3.11 |
| Citrix Workspace-App für iOS | 7.1.3 |
| Citrix Workspace-App für Mac | 12.4 |
| Citrix Workspace-App für Windows | 4.4 |
| Citrix Workspace-App für Linux | 13.4 |
| Citrix Workspace-App für HTML5 | 2.3 |
| Citrix Workspace-App für Chrome | 2.3 |
| Secure Hub für iOS | 10.5 |
| Secure Hub für Android | 10.5 |
| Secure Mail für iOS | 10.5 |
| SecureWeb für iOS | 10.5 |
| Secure Mail für Android | 10.5 |
| SecureWeb für Android | 10.5 |

**Hinweis:**

- Einzelheiten zu einigen der häufig verwendeten Funktionen, die für jeden VPN-Client unterstützt werden, finden Sie unter Citrix Gateway VPN-Clients und unterstützte Funktionen.

## Citrix Gateway-Lizenzierung

March 27, 2024

Nachdem Sie Citrix Gateway installiert haben, können Sie Ihre Platform- oder Universal-Lizenzdateien von Citrix beziehen. Sie melden sich auf der Citrix Website an, um auf Ihre verfügbaren Lizenzen zuzugreifen und eine Lizenzdatei zu generieren. Nachdem die Lizenzdatei generiert wurde, laden Sie sie auf einen Computer herunter. Wenn sich die Lizenzdatei auf dem Computer befindet, laden Sie sie

dann auf Citrix Gateway hoch. Weitere Informationen zur Citrix Lizenzierung finden Sie unter Citrix Licensing System.

Stellen Sie vor dem Abrufen Ihrer Lizenzdateien sicher, dass Sie den Hostnamen der Appliance mithilfe des Setup-Assistenten konfigurieren und dann die Appliance neu starten.

Um Ihre Lizenzen zu erhalten, rufen Sie die Webseite Citrix Lizenzen aktivieren, aktualisieren und verwalten auf. Auf dieser Seite können Sie Ihre neue Lizenz erhalten und Citrix Lizenzen aktivieren, aktualisieren und verwalten.

**Wichtig:**

> - Sie müssen Lizenzen auf Citrix Gateway installieren. Die Appliance erhält keine Lizenzen von Citrix License Server.
> - Citrix empfiehlt, eine lokale Kopie aller Lizenzdateien aufzubewahren, die Sie erhalten. Wenn Sie eine Backupkopie der Konfigurationsdatei speichern, sind alle hochgeladenen Lizenzdateien darin enthalten. Wenn Sie die Citrix Gateway-Appliance-Software neu installieren müssen und keine Backup der Konfiguration haben, benötigen Sie die ursprünglichen Lizenzdateien.

Bevor Sie Lizenzen auf Citrix Gateway installieren, legen Sie den Hostnamen des Geräts fest und starten Sie Citrix Gateway neu. Sie verwenden den Setup-Assistenten, um den Hostnamen zu konfigurieren. Wenn Sie die Universal-Lizenz für Citrix Gateway generieren, wird der Hostname in der Lizenz verwendet.

### Citrix Gateway-Lizenztypen

Citrix Gateway erfordert eine Plattformlizenz. Die Plattformlizenz ermöglicht eine unbegrenzte Anzahl von Verbindungen zu Citrix Virtual Apps, Citrix Virtual Desktops oder StoreFront mithilfe von ICA Proxy. Um VPN-Verbindungen zum Netzwerk über das Citrix Gateway-Plug-In, einen SmartAccess-Anmeldepunkt oder Secure Hub, WorxWeb oder Secure Mail zuzulassen, müssen Sie auch eine Universal-Lizenz hinzufügen. Citrix Gateway VPX wird mit der Plattformlizenz geliefert.

Die Plattformlizenz wird auf den folgenden Citrix Gateway-Versionen unterstützt:

- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- Citrix ADC VPX

> **Wichtig:** Citrix empfiehlt, eine lokale Kopie aller Lizenzdateien aufzubewahren, die Sie erhalten. Wenn Sie eine Sicherungskopie der Konfigurationsdatei speichern, werden alle hochgeladenen Lizenzdateien in das Backup aufgenommen. Wenn Sie die Citrix Gateway-Appliance-Software neu installieren müssen und keine Backup der Konfiguration haben, benötigen Sie die ursprünglichen Lizenzdateien.

### Die Plattformlizenz

Die Plattformlizenz ermöglicht unbegrenzte Benutzerverbindungen zu veröffentlichten Anwendungen auf Citrix Virtual Apps oder virtuellen Desktops von Citrix Virtual Desktops. Verbindungen mithilfe von Citrix Receiver verwenden keine Citrix Gateway Universal-Lizenz. Diese Verbindungen benötigen nur die Plattformlizenz. Die Plattformlizenz wird elektronisch mit allen neuen Citrix Gateway-Bestellungen geliefert, egal ob physisch oder virtuell. Wenn Sie bereits eine Appliance besitzen, die unter einen Garantie- oder Wartungsvertrag fällt, können Sie die Plattformlizenz von der Citrix Websitebeziehen.

### Die Universal-Lizenz

Die Universallizenz für Citrix Gateway beschränkt die Anzahl gleichzeitiger Benutzersitzungen auf die Anzahl der gekauften Lizenzen. Wenn Sie 100 Lizenzen erwerben, können Sie jederzeit 100 gleichzeitige Sitzungen abhalten. Wenn Sie eine Standard Edition-Lizenz erwerben, können Sie jederzeit 500 gleichzeitige Sitzungen abhalten. Wenn ein Benutzer eine Sitzung beendet, wird diese Lizenz für den nächsten Benutzer freigegeben. Ein Benutzer, der sich von mehr als einem Computer bei Citrix Gateway anmeldet, belegt eine Lizenz für jede Sitzung.

Wenn alle Lizenzen belegt sind, können keine zusätzlichen Verbindungen geöffnet werden, bis ein Benutzer eine Sitzung beendet oder der Administrator die Sitzung mithilfe des Konfigurationsdienstprogramms beendet. Wenn eine Verbindung geschlossen wird, wird die Lizenz freigegeben und kann für einen neuen Benutzer verwendet werden.

Wenn Sie Ihr Citrix Gateway-Gerät erhalten, erfolgt die Lizenzierung in der folgenden Reihenfolge:

- Sie erhalten den Lizenzzugangscode (Lizenzschlüssel) in einer E-Mail.
- Sie verwenden den Setup-Assistenten, um Citrix Gateway mit dem Hostnamen zu konfigurieren.
- Sie weisen die Citrix Gateway-Lizenzen von der Citrix Website zu. Verwenden Sie den Hostnamen, um die Lizenzen während des Zuweisungsvorgangs an die Appliance zu binden.
- Sie installieren die Lizenzdatei auf Citrix Gateway.

Die Universal-Lizenz unterstützt die folgenden Funktionen:

- Vollständiger VPN-Tunnel

- Micro VPN
- Endpunktanalyse
- Richtlinienbasierter SmartAccess
- Clientloser Zugriff auf Websites und Dateifreigaben

**Erhalt der Universal License** Sie benötigen die folgenden Informationen, bevor Sie auf die Citrix Website gehen, um die Universallizenz zu erhalten.

- Die Benutzer-ID und das Kennwort Ihres Citrix Kontos.

  Registrieren Sie sich auf der Citrix Website (https://www.citrix.com/welcome/create-account/), um Ihre Benutzer-ID und Ihr Kennwort zu erhalten.
  Hinweis: Wenn Sie weder den Lizenzcode noch Ihre Benutzer-ID und Ihr Kennwort finden können, wenden Sie sich an den Citrix Customer Service.

- Der Hostname des
  Citrix Gateway

  Im Eingabefeld für diesen Namen auf der Citrix Website wird zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie daher sicher, dass Sie den Hostnamen genau so kopieren, wie er auf der Citrix ADC Appliance konfiguriert ist.

- Die Anzahl der Lizenzen, die Sie in die Lizenzdatei aufnehmen möchten

  Sie müssen nicht alle Lizenzen, auf die Sie Anspruch haben, gleichzeitig herunterladen. Wenn Ihr Unternehmen beispielsweise 100 Lizenzen gekauft hat, können Sie 50 herunterladen. Den Rest können Sie später in einer anderen Lizenzdatei zuweisen. Auf dem
  Citrix Gateway können mehrere Lizenzdateien installiert werden.

  **Hinweis:** Stellen Sie vor dem Erhalt Ihrer Lizenzen sicher, dass Sie den Hostnamen der Citrix ADC Appliance mithilfe des Setup-Assistenten konfigurieren und dann die Appliance neu starten.

**Um Ihre Universallizenz zu erhalten**

1. Melden Sie sich mit Ihren Citrix Anmeldeinformationen bei der Citrix Website (https://www.citrix.com/en-in/account/) an.
2. Folgen Sie unter **Citrix Manage Licenses hier**den Anweisungen, um Ihre Lizenzdatei zu erhalten.

**Installieren der Universallizenz** Informationen zur Installation der Lizenz finden Sie unter "Installieren der Lizenz". Überprüfen Sie nach der Installation, ob die Lizenz korrekt installiert wurde.

**Überprüfung der Installation der Universal License** Bevor Sie fortfahren, überprüfen Sie, ob Ihre Universallizenz korrekt installiert ist.

#### So überprüfen Sie die Installation der Universallizenz über die CLI

1. Öffnen Sie mithilfe eines SSH-Clients wie PuTTY eine SSH-Verbindung zur Citrix ADC Appliance.
2. Melden Sie sich mithilfe der Administratoranmeldeinformationen bei der Citrix ADC Appliance an.
3. Verwenden Sie den Befehl show license, um zu überprüfen, ob "SSL VPN = JA"und dass Maximum Users von 5 auf die erwartete Anzahl gleichzeitiger Benutzer gestiegen ist.

#### So überprüfen Sie die Installation der Universallizenz über die GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der Citrix ADC Appliance ein, `http://192.168.100.1`z.
2. Geben Sie im Feld User Name und Password die Administratoranmeldeinformationen ein.
3. Erweitern Sie im Navigationsbereich System, und klicken Sie dann auf Lizenzen.
4. Im Bereich Lizenzen sehen Sie ein grünes Häkchen neben **NetScaler Gateway**. Das Feld Maximum zulässige Citrix Gateway Benutzer zeigt die Anzahl der gleichzeitigen Benutzersitzungen an, die auf der Citrix ADC Appliance lizenziert sind.

### Zugehörige Ressourcen

- Citrix Lizenzsystem
- Citrix ADC Datenblatt
- Arten von Citrix ADC- und Citrix Gateway-Lizenzen

## Lizenz auf Citrix Gateway installieren

March 27, 2024

Nachdem Sie die Lizenzdatei erfolgreich auf Ihren Computer heruntergeladen haben, können Sie die Lizenz auf Citrix Gateway installieren. Die Lizenz ist im Verzeichnis /nsconfig/license installiert.

Wenn Sie den Setup-Assistenten verwendet haben, um die Anfangseinstellungen auf Citrix Gateway zu konfigurieren, wird die Lizenzdatei beim Ausführen des Assistenten installiert. Wenn Sie einen Teil Ihrer Lizenzen zuweisen und später eine zusätzliche Nummer zuweisen, können Sie die Lizenzen ohne Verwendung des Setup-Assistenten installieren.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option **System** und klicken Sie dann auf **Lizenzen**.
2. Klicken Sie im Detailbereich auf **Manage Licenses**.
3. Klicken Sie auf **Neue Lizenz hinzufügen**, dann auf **Durchsuchen**, navigieren Sie zur Lizenzdatei und klicken Sie dann auf **OK**.

   Im Konfigurationsdienstprogramm wird eine Meldung angezeigt, dass Sie Citrix Gateway neu starten müssen. Klicken Sie auf Neustart.

### Legen Sie die maximale Anzahl von Benutzern fest

Nachdem Sie die Lizenz auf der Appliance installiert haben, müssen Sie die maximale Anzahl von Benutzern festlegen, die eine Verbindung zur Appliance herstellen dürfen. Sie legen die maximale Benutzeranzahl in der globalen Authentifizierungsrichtlinie fest.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter Einstellungen auf **AAA-Authentifizierungseinstellungen ändern**.
3. Geben Sie unter Maximale Anzahl an Benutzern die Gesamtzahl der Benutzer ein, und klicken Sie dann auf **OK**.

   Die Zahl in diesem Feld entspricht der Anzahl Lizenzen, die in der Lizenzdatei enthalten sind. Diese Zahl muss kleiner oder gleich der Gesamtzahl der auf der Appliance installierten Lizenzen sein. Beispiel: Sie installieren eine Lizenz mit 100 Benutzerlizenzen und eine zweite mit 400 Benutzerlizenzen. Die Gesamtzahl der Lizenzen beträgt 500. Die maximale Anzahl von Benutzern, die sich anmelden können, ist kleiner oder gleich 500. Wenn 500 Benutzer angemeldet sind, wird allen Benutzern, die versuchen, sich über diese Anzahl hinaus anzumelden, der Zugriff verweigert, bis sich ein Benutzer abmeldet oder Sie eine Sitzung beenden.

### Überprüfen Sie die Universal Lizenzinstallation

Bevor Sie fortfahren, überprüfen Sie, ob Ihre Universal-Lizenz korrekt installiert ist.

### So überprüfen Sie die Installation der Universal-Lizenz über die GUI

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System, und klicken Sie dann auf Lizenzen.

Im Bereich Lizenzen sehen Sie ein grünes Häkchen neben Citrix Gateway. Im Feld Maximal zulässige Citrix Gateway-Benutzer wird die Anzahl gleichzeitiger Benutzersitzungen angezeigt, die auf dem Gerät lizenziert sind.

### So überprüfen Sie die Installation der Universal-Lizenz über die CLI

1. Öffnen Sie mithilfe eines SSH-Clients wie PuTTY eine Secure Shell (SSH) -Verbindung zur Appliance.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.
3. Geben Sie an einer Eingabeaufforderung;

```
show license
<!--NeedCopy-->
```

Die Lizenz wird korrekt installiert, wenn der Parameter SSL VPN Ja entspricht und der Parameter für maximale Benutzer der Anzahl der Lizenzen entspricht.

## Häufig gestellte Fragen zur Citrix Gateway Lizenzierung

March 27, 2024

### Wie erhalte ich Unterstützung bei Test- oder Demo-Lizenzen?

Viele der Citrix Produkte werden jetzt als umfassende, private, von Experten geleitete 1:1 -Demo-Erlebnisse angeboten. Unsere Citrix Experten passen die Demo an Ihre Bedürfnisse, Anwendungsfälle und aktiven Projekte an. Keine Downloads, keine Lizenz oder Installation erforderlich. Sie benötigen ein minimales Setup, um eine sofortige Demo zu sehen. Wenden Sie sich nach der Demo an Citrix Experten, um mit einem Machbarkeitsnachweis oder einer Testversion einer Citrix Lösung fortzufahren, die für Ihre Dienste gilt. Für Demos klicken Sie auf https://demo.citrix.com/.

### Wie installiert man Lizenzen?

Einzelheiten zur Installation von Lizenzen finden Sie unter So installieren Sie eine Lizenz auf Citrix Gateway.

### Was sind die verschiedenen Arten von Gateway-Lizenzen?

Die Plattformlizenz ermöglicht eine unbegrenzte Anzahl von Verbindungen zu Citrix Virtual Apps, Citrix Virtual Desktops oder StoreFront mithilfe von ICA Proxy.
Die Universal License ist eine Add-On-Lizenz zusätzlich zu Citrix ADC-Plattformlizenzen. Dies ermöglicht VPN-Verbindungen zum Netzwerk über das Citrix Gateway Plug-in, einen SmartAccess-Anmeldepunkt oder Secure Hub, Secure Web oder Secure Mail. Weitere Einzelheiten finden Sie unter Citrix Gateway-Lizenztypen.

### Wie viele gleichzeitige Benutzersitzungen werden unterstützt?

Die unterstützten Sitzungen hängen vom Gateway-Lizenztyp ab. Einzelheiten finden Sie unter Citrix Gateway-Lizenztypen.

Ein weiterer zu berücksichtigender Faktor ist die Kapazität der zugrunde liegenden Hardware selbst. Informationen zur Leistung finden Sie im Citrix ADC MPX/SDX-Datenblatt oder im Citrix ADC VPX-Datenblatt.

### Wie überprüfe ich die aktuell lizenzierten gleichzeitigen Benutzersitzungen?

Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration den Knoten **System** und klicken Sie dann auf **Lizenzen**.
Im Bereich **Lizenzen** sehen Sie ein grünes Häkchen neben Citrix Gateway. Im Feld **Maximal zulässige Citrix Gateway-Benutzer** wird die Anzahl der gleichzeitigen Benutzersitzungen angezeigt, die auf dem Gerät lizenziert sind.

### Wie überprüft man, ob das lizenzierte Durchsatzlimit erreicht ist?

Sie können den Echtzeit-Durchsatz mit extrahieren `newnslog`. Wenn der Lizenzdurchsatz beispielsweise 500 Mbit/s beträgt, können Sie den Echtzeitdurchsatz über 500 mithilfe des folgenden Befehls extrahieren.

```
1 nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
     more
2 <!--NeedCopy-->
```

```
reltime:mili second between two records Mon Feb  5 13:47:13 2018
 Index   rtime totalcount-val      delta rate/sec symbol-name&device-no&time
    12    7000      801130681       3701      528 allnic_tot_rx_mbits  Mon Feb  5 13:47:55 2018
    13       0      460776045       3682      526 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:47:55 2018
    14    7000      801134437       3756      536 allnic_tot_rx_mbits  Mon Feb  5 13:48:02 2018
    15       0      460779784       3739      534 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:02 2018
    16    7000      801138166       3729      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:09 2018
    17       0      460783497       3713      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:09 2018
    18    7000      801141896       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:16 2018
    19       0      460787213       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:16 2018
    20    7000      801145623       3727      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:23 2018
    21       0      460790929       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:23 2018
    22    7000      801149353       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:30 2018
    23       0      460794646       3717      531 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:30 2018
    24    7000      801153067       3714      530 allnic_tot_rx_mbits  Mon Feb  5 13:48:37 2018
    25       0      460798342       3696      528 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:37 2018
```

### Wie kann überprüft werden, ob Pakete bei Erreichen des Lizenzdurchsatzes verworfen werden?

Mit dem folgenden Befehl können Sie überprüfen, ob Pakete verworfen werden.

```
1 nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
      more
2 <!--NeedCopy-->
```

```
reltime:mili second between two records Fri Feb  2 00:12:38 2018
 Index   rtime     totalcount-val      delta rate/sec symbol-name&device-no&time
     0 1966993       23723602        478       68 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:38 2018
     1       0       48048402        465       66 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:38 2018
     2       0     8307679782     145475    20782 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:38 2018
     3    7000       23723933        331       47 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:45 2018
     4       0       48048712        310       44 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:45 2018
     5       0     8307787105     107323    15331 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:45 2018
     6    7000       23723941          8        1 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:52 2018
     7       0       48048735         23        3 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:52 2018
     8       0     8307811163      24058     3436 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:52 2018
```

### Wie kann ich herausfinden, wie hoch der lizenzierte Durchsatz für eine Citrix ADC Appliance ist?

Führen Sie den Befehl `show license` von der CLI aus und verwenden Sie dann die Modellnummer, um den Durchsatz aus dem ADC- oder Gateway MPX-, SDX- und VPX-Datenblatt abzurufen.

```
> sh license
       License status:
                          Web Logging: YES
                     Surge Protection: YES
                       Load Balancing: YES
                    Content Switching: YES
                    Cache Redirection: YES
                         Sure Connect: YES
                  Compression Control: YES
                    Delta Compression: NO
                     Priority Queuing: YES
                       SSL Offloading: YES
           Global Server Load Balancing: YES
                       GSLB Proximity: YES
                  Http DoS Protection: YES
                      Dynamic Routing: YES
                    Content Filtering: YES
                   Integrated Caching: YES
                              SSL VPN: YES   (Maximum users = 5)   (Maximum ICA u
sers = 0)
                                  AAA: YES
                          OSPF Routing: YES
                           RIP Routing: YES
                           BGP Routing: YES
                              Rewrite: YES
              IPv6 protocol translation: YES
                   Application Firewall: YES
                             Responder: YES
                        HTML Injection: YES
                        NetScaler Push: YES
                  Web Interface on NS: YES
                              AppFlow: YES
                          CloudBridge: YES
                     Model Number ID: 5500
 Done
> 
```

CITRIX

Citrix NetScaler | Datasheet

| NetScaler platform | MPX 9500 | MPX 7500 | MPX 5500 | VPX 10/200/1000/3000 |
|---|---|---|---|---|
| **Platform attributes** | | | | |
| Processor | Intel Xeon L5410 (4 cores total) | Intel Xeon L5410 (4 cores total) | Intel Xeon E5205 (2 cores total) | Minimum Server Req.:[1] Dual core server with Intel® VTx or AMD-V™ |
| Memory | 8 GB | 8 GB | 4 GB | |
| Ethernet ports | 8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper) | 8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper) | 4x 10/100/1000 BASE-T | • Citrix® XenServer® 5 (update 3 or better)<br>• Windows Server 2008 R2 with Hyper-V role<br>• VMWare ESX/ESXi 3.5 or higher<br>• 4G RAM/20 GB hard drive<br>• Hypervisor supported NIC |
| Transceivers support | SX, LX | SX, LX | | |
| Software upgradable performance | | Upgrade option to MPX 9500 | | Upgrade options to VPX 200, VPX 1000 and VPX 3000 |
| **Platform performance** | | | | |
| System throughput, Gbps | 3 | 1 | 0.5 | Up to 3.0[2] |
| HTTP requests/sec | 200,000 | 100,000 | 50,000 | Up to 100,000 |
| SSL transactions/sec | 20,000 | 10,000 | 5,000 | Up to 500 |
| SSL throughput, Gbps | 3 | 1 | 0.5 | Up to 1.0 |
| Compression throughput, Gbps | 2 | 1 | 0.5 | Up to 0.75 |
| SSL VPN: concurrent users | 10,000 | 10,000 | 5,000 | Up to 300[3] |

### Wie fügt man mehr Benutzer zu bestehenden Gateway-Lizenzen hinzu?

Sie können eine zusätzliche Universallizenz installieren. Angenommen, Sie haben eine Universallizenz installiert, die 100 Benutzerlizenzen enthält. Wenn Sie die zweite Universallizenz installieren, die 400 Benutzerlizenzen enthält, entspricht die Gesamtzahl der Benutzerlizenzen 500.

## Vor dem Einstieg

March 27, 2024

Bevor Sie Citrix Gateway installieren, müssen Sie Ihre Infrastruktur bewerten und Informationen sammeln, um eine Zugriffsstrategie zu planen, die den spezifischen Anforderungen Ihres Unternehmens entspricht. Wenn Sie Ihre Zugriffsstrategie definieren, müssen Sie die Auswirkungen auf die Sicherheit berücksichtigen und eine Risikoanalyse durchführen. Sie müssen auch die Netzwerke festlegen, mit denen Benutzer eine Verbindung herstellen dürfen, und Richtlinien festlegen, die Benutzerverbindungen ermöglichen.

Neben der Planung der Ressourcen, die Benutzern zur Verfügung stehen, müssen Sie auch Ihr Bereitstellungsszenario planen. Citrix Gateway ist mit den folgenden Citrix Produkten kompatibel:

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Webinterface
- Citrix SD-WAN

Weitere Informationen zur Bereitstellung von Citrix Gateway finden Sie unter Gemeinsame Bereitstellungenund Integration mit Citrix Produkten

Führen Sie bei der Vorbereitung Ihrer Zugriffsstrategie die folgenden vorbereitenden Schritte aus:

- Identifizieren Sie Ressourcen. Listen Sie die Netzwerkressourcen auf, für die Sie Zugriff gewähren möchten, z. B. Web, SaaS, mobile oder veröffentlichte Anwendungen, virtuelle Desktops, Dienste und Daten, die Sie in Ihrer Risikoanalyse definiert haben.
- Entwickeln Sie Zugriffsszenarien. Erstellen Sie Zugriffsszenarien, die beschreiben, wie Benutzer auf Netzwerkressourcen zugreifen. Ein Zugriffsszenario wird durch den virtuellen Server definiert, der für den Zugriff auf das Netzwerk verwendet wird, Endpoint Analysis-Scanergebnisse, Authentifizierungstyp oder eine Kombination davon. Sie können auch festlegen, wie sich Benutzer am Netzwerk anmelden.

- Identifizieren Sie Clientsoftware. Sie können vollen VPN-Zugriff mit dem Citrix Gateway-Plug-in bereitstellen, sodass sich Benutzer mit der Citrix Workspace-App, Secure Hub oder mithilfe des clientlosen Zugriffs anmelden müssen. Sie können auch den E-Mail-Zugriff auf Outlook Web App oder WorxMail einschränken. Diese Zugriffsszenarien bestimmen auch die Aktionen, die Benutzer ausführen können, wenn sie Zugriff erhalten. Sie können beispielsweise angeben, ob Benutzer Dokumente mithilfe einer veröffentlichten Anwendung oder durch Herstellen einer Verbindung zu einer Dateifreigabe ändern können.
- Verknüpfen Sie Richtlinien Benutzern, Gruppen oder virtuellen Servern. Die Richtlinien, die Sie auf Citrix Gateway erstellen, werden durchgesetzt, wenn die Person oder die Gruppe von Benutzern bestimmte Bedingungen erfüllt. Sie legen die Bedingungen basierend auf den von Ihnen erstellten Zugriffsszenarien fest. Anschließend erstellen Sie Richtlinien, die die Sicherheit Ihres Netzwerks erhöhen, indem Sie die Ressourcen steuern, auf die Benutzer zugreifen können, und die Aktionen, die Benutzer für diese Ressourcen ausführen können. Sie verknüpfen die Richtlinien entsprechenden Benutzern, Gruppen, virtuellen Servern oder global.

Dieser Abschnitt enthält die folgenden Themen, die Ihnen bei der Planung Ihrer Zugriffsstrategie helfen sollen:

- Planning for Security beinhaltet Informationen über Authentifizierung und Zertifikate.
- Voraussetzungen, die Netzwerkhardware und -software definieren, die Sie möglicherweise benötigen.
- Die Checkliste vor der Installation, mit der Sie Ihre Einstellungen notieren können, bevor Sie Citrix Gateway konfigurieren.

### Voraussetzungen für die Installation von Citrix Gateway

Bevor Sie Einstellungen auf Citrix Gateway konfigurieren, überprüfen Sie die folgenden Voraussetzungen:

- Citrix Gateway ist physisch in Ihrem Netzwerk installiert und hat Zugriff auf das Netzwerk. Citrix Gateway wird in der DMZ oder im internen Netzwerk hinter einer Firewall bereitgestellt. Sie können Citrix Gateway auch in einer Double-Hop-DMZ konfigurieren und Verbindungen zu einer Serverfarm konfigurieren. Citrix empfiehlt, die Appliance in der DMZ bereitzustellen.
- Sie konfigurieren Citrix Gateway mit einem Standardgateway oder mit statischen Routen zum internen Netzwerk, damit Benutzer auf Ressourcen im Netzwerk zugreifen können. Citrix Gateway ist standardmäßig für die Verwendung statischer Routen konfiguriert.
- Die für die Authentifizierung und Autorisierung verwendeten externen Server werden konfiguriert und ausgeführt. Weitere Informationen finden Sie unter Authentifizierung und Autorisierung.
- Das Netzwerk verfügt über einen Domänennamenserver (DNS) oder Windows Internet

Naming Service (WINS) -Server zur Namensauflösung, um die korrekte Citrix Gateway-Benutzerfunktionalität bereitzustellen.

- Sie haben die Universal-Lizenzen für Benutzerverbindungen mit dem Citrix Gateway Plug-in von der Citrix Website heruntergeladen und die Lizenzen können auf Citrix Gateway installiert werden.
- Citrix Gateway verfügt über ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert ist. Weitere Informationen finden Sie unter Installieren und Verwalten von Zertifikaten.

Verwenden Sie vor der Installation von Citrix Gateway die Checkliste vor der Installation, um Ihre Einstellungen aufzuschreiben.

## Planen für Sicherheit

Bei der Planung Ihrer Citrix Gateway-Bereitstellung müssen Sie die grundlegenden Sicherheitsprobleme im Zusammenhang mit Zertifikaten sowie der Authentifizierung und Autorisierung verstehen.

### Konfiguration der sicheren Zertifikatsverwaltung

Standardmäßig enthält Citrix Gateway ein selbstsigniertes Secure Sockets Layer (SSL) -Serverzertifikat, mit dem die Appliance SSL-Handshakes abschließen kann. Selbstsignierte Zertifikate eignen sich zum Testen oder für Beispielbereitstellungen, aber Citrix empfiehlt nicht, sie für Produktionsumgebungen zu verwenden. Bevor Sie Citrix Gateway in einer Produktionsumgebung bereitstellen, empfiehlt Citrix, dass Sie ein signiertes SSL-Serverzertifikat von einer bekannten Zertifizierungsstelle (CA) anfordern, empfangen und auf Citrix Gateway hochladen.

Wenn Sie Citrix Gateway in einer Umgebung bereitstellen, in der Citrix Gateway als Client in einem SSL-Handshake arbeiten muss (verschlüsselte Verbindungen mit einem anderen Server initiieren), müssen Sie auch ein vertrauenswürdiges Stammzertifikat auf Citrix Gateway installieren. Wenn Sie beispielsweise Citrix Gateway mit Citrix Virtual Apps und dem Webinterface bereitstellen, können Sie Verbindungen von Citrix Gateway zum Webinterface mit SSL verschlüsseln. In dieser Konfiguration müssen Sie ein vertrauenswürdiges Stammzertifikat auf Citrix Gateway installieren.

### Unterstützung der Authentifizierung

Sie können Citrix Gateway so konfigurieren, dass Benutzer authentifiziert und die Zugriffsebene (oder Autorisierung) gesteuert werden, die Benutzer auf die Netzwerkressourcen im internen Netzwerk haben.

Vor der Bereitstellung von Citrix Gateway muss Ihre Netzwerkumgebung über die Verzeichnisse und Authentifizierungsserver verfügen, um einen der folgenden Authentifizierungstypen zu unterstützen:

- LDAP
- RADIUS
- TACACS+
- Clientzertifikat mit Auditing und Smartcard-Unterstützung
- RSA mit RADIUS-Konfiguration
- SAML-Authentifizierung

Wenn Ihre Umgebung keinen dieser Authentifizierungstypen unterstützt oder Sie eine kleine Anzahl von Remotebenutzern haben, können Sie eine Liste lokaler Benutzer auf Citrix Gateway erstellen. Sie können dann Citrix Gateway so konfigurieren, dass Benutzer anhand dieser lokalen Liste authentifiziert werden. Bei dieser Konfiguration müssen Sie keine Benutzerkonten in einem separaten, externen Verzeichnis verwalten.

#### Schützen Sie Ihre Citrix Gateway-Bereitstellung

Verschiedene Bereitstellungen können unterschiedliche Sicherheitsüberlegungen erfordern. Die Richtlinien zur sicheren Bereitstellung von Citrix ADC bieten allgemeine Sicherheitshinweise, die Ihnen bei der Entscheidung für eine geeignete sichere Bereitstellung basierend auf Ihren speziellen Sicherheitsanforderungen helfen.

Einzelheiten finden Sie unter Citrix ADC Richtlinien für sichere Bereitstellung.

## Checkliste für Gateway-Vorinstallation

March 27, 2024

Die Checkliste besteht aus einer Liste von Aufgaben und Planungsinformationen, die Sie vor der Installation von Citrix Gateway ausführen müssen.

Es ist Platz vorhanden, damit Sie jede Aufgabe abhaken und sich Notizen machen können. Citrix empfiehlt, dass Sie sich die Konfigurationswerte notieren, die Sie während des Installationsvorgangs und während der Konfiguration von Citrix Gateway eingeben müssen.

Schritte zum Installieren und Konfigurieren von Citrix Gateway finden Sie unter Installieren von Citrix Gateway.

### Benutzergeräte

- Stellen Sie sicher, dass Benutzergeräte die in den Systemanforderungen des Citrix Gateway Plug-ins beschriebenen Installationsvoraussetzungen erfüllen
- Identifizieren Sie die Mobilgeräte, mit denen sich Benutzer verbinden. **Hinweis**: Wenn Benutzer eine Verbindung mit einem iOS-Gerät herstellen, müssen Sie Secure Browse in einem Sitzungsprofil aktivieren.

### Citrix Gateway grundlegende Netzwerkkonnektivität

Citrix empfiehlt, Lizenzen und signierte Serverzertifikate zu beziehen, bevor Sie mit der Konfiguration der Appliance beginnen.

- Identifizieren und notieren Sie den Hostnamen von Citrix Gateway. **Hinweis**: Dies ist nicht der vollqualifizierte Domainname (FQDN). Der FQDN ist im signierten Serverzertifikat enthalten, das an den virtuellen Server gebunden ist.
- Beziehen Sie Universal-Lizenzen von der Citrix Website
- Generieren Sie eine Certificate Signing Request (CSR) und senden Sie sie an eine Zertifizierungsstelle (CA). Geben Sie das Datum ein, an dem Sie die CSR an die Zertifizierungsstelle senden.
- Notieren Sie die System-IP-Adresse und die Subnetzmaske.
- Notieren Sie die Subnetz-IP-Adresse und die Subnetzmaske.
- Notieren Sie sich das Administratorkennwort. Das Standardkennwort, das mit Citrix Gateway geliefert wird, lautet `nsroot`.
- Notieren Sie sich die Portnummer, auf der Citrix Gateway auf sichere Benutzerverbindungen wartet. Der Standardwert ist TCP-Port 443. Dieser Port muss an der Firewall zwischen dem ungesicherten Netzwerk (Internet) und der DMZ geöffnet sein.
- Notieren Sie sich die standardmäßige Gateway-IP-Adresse.
- Notieren Sie die IP-Adresse und Portnummer des DNS-Servers. Die Standardportnummer ist 53. Wenn Sie den DNS-Server direkt hinzufügen, müssen Sie außerdem ICMP (Ping) auf der Appliance konfigurieren.
- Notieren Sie die erste IP-Adresse und den Hostnamen des virtuellen Servers.
- Notieren Sie die IP-Adresse und den Hostnamen des zweiten virtuellen Servers (falls zutreffend).
- Notieren Sie die IP-Adresse des WINS-Servers (falls zutreffend).

### Interne Netzwerke, die über Citrix Gateway zugänglich sind

- Notieren Sie die internen Netzwerke, auf die Benutzer über Citrix Gateway zugreifen können. Beispiel: 10.10.0.0/24

- Geben Sie alle internen Netzwerke und Netzwerksegmente ein, auf die Benutzer Zugriff benötigen, wenn sie mithilfe des Citrix Gateway Plug-Ins eine Verbindung über Citrix Gateway herstellen.

### Hohe Verfügbarkeit

Wenn Sie über zwei Citrix Gateway-Appliances verfügen, können Sie sie in einer Hochverfügbarkeitskonfiguration bereitstellen, in der ein Citrix Gateway Verbindungen akzeptiert und verwaltet, während ein zweites Citrix Gateway das erste Gerät überwacht. Wenn das erste Citrix Gateway aus irgendeinem Grund keine Verbindungen mehr akzeptiert, übernimmt das zweite Citrix Gateway die Kontrolle und beginnt aktiv Verbindungen zu akzeptieren.

- Notieren Sie sich die Versionsnummer der Citrix Gateway-Software.
- Die Versionsnummer muss auf beiden Citrix Gateway-Appliances identisch sein.
- Notieren Sie sich das Administratorkennwort (`nsroot`). Das Kennwort muss auf beiden Geräten gleich sein.
- Notieren Sie die primäre Citrix Gateway-IP-Adresse und -ID. Die maximale ID-Nummer beträgt 64.
- Notieren Sie die sekundäre Citrix Gateway IP-Adresse und ID.
- Besorgen und installieren Sie die Universal-Lizenz auf beiden Geräten.
- Installieren Sie dieselbe Universal-Lizenz auf beiden Appliances.
- Notieren Sie sich das RPC-Knotenkennwort.

### Authentifizierung und Autorisierung

Citrix Gateway unterstützt verschiedene Authentifizierungs- und Autorisierungstypen, die in verschiedenen Kombinationen verwendet werden können. Ausführliche Informationen zur Authentifizierung und Autorisierung finden Sie unter Authentifizierung und Autorisierung.

#### LDAP-Authentifizierung

Wenn Ihre Umgebung einen LDAP-Server enthält, können Sie LDAP für die Authentifizierung verwenden.

- Notieren Sie die IP-Adresse und den Port des LDAP-Servers.

  Wenn Sie unsichere Verbindungen zum LDAP-Server zulassen, ist der Standardport 389. Wenn Sie Verbindungen zum LDAP-Server mit SSL verschlüsseln, ist der Standardport 636.

- Notieren Sie sich den Sicherheitstyp.

  Sie können die Sicherheit mit oder ohne Verschlüsselung konfigurieren.

- Notieren Sie den Administrator-Bind-DN.

  Wenn Ihr LDAP-Server eine Authentifizierung erfordert, geben Sie den Administrator-DN ein, den Citrix Gateway zur Authentifizierung verwenden muss, wenn Sie Abfragen an das LDAP-Verzeichnis stellen. Ein Beispiel ist cn=Administrator, CN=Users, dc=ace, dc=com.

- Notieren Sie sich das Administratorkennwort.

  Das Kennwort ist mit dem Administrator-Bind-DN verknüpft.

- Notieren Sie den Basis-DN.

  DN (oder Verzeichnisebene), unter dem sich Benutzer befinden; zum Beispiel ou=users, dc=ace, dc=com.

- Notieren Sie das Attribut für den Serveranmeldenamen.

  Geben Sie das LDAP-Verzeichnis Personenobjektattribut ein, das den Anmeldenamen eines Benutzers angibt. Der Standardwert ist sAMAccountName. Wenn Sie Active Directory nicht verwenden, lauten die üblichen Werte für diese Einstellung cn oder uid.
  Weitere Informationen zu LDAP-Verzeichniseinstellungen finden Sie unter Konfigurieren der LDAP-Authentifizierung

- Notieren Sie das Gruppenattribut.
  Geben Sie das LDAP-Verzeichnis Personenobjektattribut ein, das die Gruppen angibt, zu denen ein Benutzer gehört. Die Standardeinstellung ist MemberOf. Mit diesem Attribut kann Citrix Gateway die Verzeichnisgruppen identifizieren, zu denen ein Benutzer gehört.

- Notieren Sie den Namen des Unterattributs.

#### RADIUS-Authentifizierung und Autorisierung

Wenn Ihre Umgebung einen RADIUS-Server enthält, können Sie RADIUS für die Authentifizierung verwenden.
Die RADIUS-Authentifizierung umfasst RSA SecurID-, SafeWord- und Gemalto Protiva-Produkte.

- Notieren Sie die IP-Adresse und den Port des primären RADIUS-Servers. Der Standardport ist 1812.
- Notieren Sie das primäre RADIUS-Server-Secret (Shared Secret).
- Notieren Sie die IP-Adresse und den Port des sekundären RADIUS-Servers. Der Standardport ist 1812.
- Notieren Sie das sekundäre RADIUS-Server-Secret (Shared Secret)
- Notieren Sie sich die Art der Kennwortkodierung (PAP, CHAP, MS-CHAP v1, MSCHAP v2).

### SAML-Authentifizierung

Die Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für den Austausch von Authentifizierung und Autorisierung zwischen Identity Providern (IdP) und Service Providern.

- Besorgen und installieren Sie auf Citrix Gateway ein sicheres IdP-Zertifikat.
- Notieren Sie sich die Umleitungs-URL.
- Notieren Sie sich das Benutzerfeld.
- Notieren Sie den Namen des Signaturzertifikats.
- Notieren Sie den Namen des SAML-Ausstellers.
- Notieren Sie die Standardauthentifizierungsgruppe.

### Ports durch die Firewalls öffnen (Single-Hop-DMZ)

Wenn Ihre Organisation das interne Netzwerk mit einer einzigen DMZ schützt und Sie das Citrix Gateway in der DMZ bereitstellen, öffnen Sie die folgenden Ports durch die Firewalls. Wenn Sie zwei Citrix Gateway-Appliances in einer Double-Hop-DMZ-Bereitstellung installieren, lesen Sie Öffnen der entsprechenden Ports auf den Firewalls.

#### Auf der Firewall zwischen dem ungesicherten Netzwerk und der DMZ

- Öffnen Sie einen TCP/SSL-Port (Standard 443) auf der Firewall zwischen dem Internet und Citrix Gateway. Benutzergeräte stellen über diesen Port eine Verbindung zu Citrix Gateway her.

#### Auf der Firewall zwischen dem gesicherten Netzwerk

- Öffnen Sie einen oder mehrere geeignete Ports an der Firewall zwischen der DMZ und dem gesicherten Netzwerk. Citrix Gateway stellt eine Verbindung zu einem oder mehreren Authentifizierungsservern oder zu Computern her, auf denen Citrix Virtual Apps and Desktops im gesicherten Netzwerk an diesen Ports ausgeführt wird.
- Notieren Sie die Authentifizierungsports.

  Öffnen Sie nur den für Ihre Citrix Gateway-Konfiguration geeigneten Port.

  - Für LDAP-Verbindungen ist der Standardwert TCP-Port 389.
  - Für eine RADIUS-Verbindung ist der Standardwert der UDP-Port 1812. Notieren Sie die Ports für Citrix Virtual Apps and Desktops.
- Wenn Sie Citrix Gateway mit Citrix Virtual Apps and Desktops verwenden, öffnen Sie den TCP-Port 1494. Wenn Sie die Sitzungszuverlässigkeit aktivieren, öffnen Sie den TCP-Port 2598 anstelle von 1494. Citrix empfiehlt, diese beiden Ports offen zu halten.

### Citrix Virtual Desktops, Citrix Virtual Apps, das Webinterface oder StoreFront

Führen Sie die folgenden Aufgaben aus, wenn Sie Citrix Gateway bereitstellen, um Zugriff auf Citrix Virtual Apps and Desktops über das Webinterface oder StoreFront zu gewähren. Das Citrix Gateway Plug-in ist für diese Bereitstellung nicht erforderlich. Benutzer greifen über Citrix Gateway auf veröffentlichte Anwendungen und Desktops zu, indem sie nur Webbrowser und Citrix Receiver verwenden.

- Notieren Sie den FQDN oder die IP-Adresse des Servers, auf dem das Webinterface oder StoreFront ausgeführt wird.
- Notieren Sie den FQDN oder die IP-Adresse des Servers, auf dem die Secure Ticket Authority (STA) ausgeführt wird (nur für das Webinterface).

### Citrix Endpoint Management

Führen Sie die folgenden Aufgaben aus, wenn Sie Citrix Endpoint Management in Ihrem internen Netzwerk bereitstellen. Wenn Benutzer über ein externes Netzwerk wie das Internet eine Verbindung zu Endpoint Management herstellen, müssen Benutzer eine Verbindung zu Citrix Gateway herstellen, bevor sie auf Mobil-, Web- und SaaS-Apps zugreifen können.

- Notieren Sie den FQDN oder die IP-Adresse von Endpoint Management.
- Identifizieren Sie Web-, SaaS- und mobile iOS- oder Android-Anwendungen, auf die Benutzer zugreifen können.

### Double-Hop-DMZ-Bereitstellung mit Citrix Virtual Apps

Führen Sie die folgenden Aufgaben aus, wenn Sie zwei Citrix Gateway-Appliances in einer Double-Hop-DMZ-Konfiguration bereitstellen, um den Zugriff auf Server zu unterstützen, auf denen Citrix Virtual Apps ausgeführt wird.

#### Citrix Gateway in der ersten DMZ

Die erste DMZ ist die DMZ am äußersten Rand Ihres internen Netzwerks (am nächsten zum Internet oder unsicherem Netzwerk). Clients verbinden sich in der ersten DMZ über die Firewall, die das Internet von der DMZ trennt, mit Citrix Gateway. Sammeln Sie diese Informationen, bevor Sie Citrix Gateway in der ersten DMZ installieren.

- Füllen Sie die Elemente im Abschnitt Citrix Gateway Basic Network Connectivity dieser Checkliste für dieses Citrix Gateway aus.

  Wenn diese Elemente abgeschlossen sind, verbindet Interface 0 dieses Citrix Gateway mit dem Internet und Interface 1 verbindet dieses Citrix Gateway mit Citrix Gateway in der zweiten DMZ.

- Konfigurieren Sie die zweiten DMZ-Appliance-Informationen auf dem primären Gerät.

  Um Citrix Gateway als ersten Hop in der Double-Hop-DMZ zu konfigurieren, müssen Sie den Hostnamen oder die IP-Adresse von Citrix Gateway in der zweiten DMZ auf dem Gerät in der ersten DMZ angeben. Nachdem Sie im ersten Hop angegeben haben, wann der Citrix Gateway-Proxy auf dem Gerät konfiguriert ist, binden Sie ihn global an Citrix Gateway oder an einen virtuellen Server.

- Notieren Sie das Verbindungsprotokoll und den Port zwischen Geräten.

  Um Citrix Gateway als ersten Hop in der doppelten DMZ zu konfigurieren, müssen Sie das Verbindungsprotokoll und den Port angeben, auf dem Citrix Gateway in der zweiten DMZ auf Verbindungen wartet. Das Verbindungsprotokoll und der Port sind SOCKS mit SSL (Standardport 443). Das Protokoll und der Port müssen durch die Firewall geöffnet sein, die die erste DMZ und die zweite DMZ trennt.

#### Citrix Gateway in der zweiten DMZ

Die zweite DMZ ist die DMZ, die Ihrem internen, sicheren Netzwerk am nächsten liegt. Citrix Gateway, das in der zweiten DMZ bereitgestellt wird, dient als Proxy für ICA-Verkehr und durchquert die zweite DMZ zwischen den externen Benutzergeräten und den Servern im internen Netzwerk.

- Schließen Sie die Aufgaben im Abschnitt Citrix Gateway Basic Network Connectivity dieser Checkliste für dieses Citrix Gateway ab.

  Wenn diese Elemente fertiggestellt werden, verbindet Interface 0 dieses Citrix Gateway mit Citrix Gateway in der ersten DMZ. Schnittstelle 1 verbindet dieses Citrix Gateway mit dem gesicherten Netzwerk.

## Citrix Gateway-Appliance installieren und konfigurieren

March 27, 2024

Wenn Sie Ihr Citrix Gateway-Gerät erhalten, entpacken Sie das Gerät und bereiten die Site und das Rack vor. Nachdem Sie festgestellt haben, dass der Standort, an dem Sie Ihr Gerät installieren, den Umweltstandards entspricht und das Server-Rack gemäß den Anweisungen eingerichtet ist, installieren Sie die Hardware. Nachdem Sie das Gerät montiert haben, verbinden Sie es mit dem Netzwerk, an eine Stromquelle und an das Konsolenterminal, das Sie für die Erstkonfiguration verwenden. Nachdem Sie die Appliance eingeschaltet haben, führen Sie die Erstkonfiguration durch und weisen Verwaltungs- und Netzwerk-IP-Adressen zu. Achten Sie darauf, die in den Installationsanweisungen aufgeführten Warnhinweise und Warnhinweise zu beachten.

Bei der Installation einer virtuellen Citrix ADC VPX-Appliance müssen Sie zuerst das Image der virtuellen Appliance abrufen und auf einem Hypervisor oder einem anderen Monitor für virtuelle Maschinen installieren.

Citrix empfiehlt die Verwendung des Themas Citrix Gateway Pre-Installation Checklist, damit Sie Ihre Einstellungen notieren können, bevor Sie versuchen, ein Citrix Gateway-Gerät zu konfigurieren. Die Checkliste enthält Informationen zur Installation von Citrix Gateway und einer Appliance.

## Citrix Gateway-Appliance mit dem Assistenten konfigurieren

March 27, 2024

Citrix Gateway verfügt über die folgenden sechs Assistenten, mit denen Sie Einstellungen auf dem Gerät konfigurieren können:

- Der erstmalige Setup-Assistent wird angezeigt, wenn Sie sich zum ersten Mal bei der Citrix Gateway-Appliance anmelden.
- Der Schnellkonfigurationsassistent hilft Ihnen bei der Konfiguration der richtigen Richtlinien, Ausdrücke und Einstellungen für Verbindungen mit Citrix Endpoint Management, StoreFront und dem Webinterface.
- Der Citrix Gateway-Assistent hilft Ihnen bei der Konfiguration von Citrix Gateway-spezifischen Einstellungen.
- Der Setup-Assistent hilft Ihnen beim ersten Konfigurieren grundlegender Citrix Gateway-Einstellungen.
- Citrix Endpoint Management Integrated Configuration hilft Ihnen bei der Konfiguration Ihrer Citrix Gateway- und Citrix Endpoint Management-Umgebung.
- Der Assistent für veröffentlichte Anwendungen hilft Ihnen beim Konfigurieren von Einstellungen für Benutzerverbindungen mithilfe der Citrix Workspace-App.

### Erstmalige Einrichtung Wizard

Wenn Sie die Installation und Konfiguration der Anfangseinstellungen auf der Citrix Gateway-Appliance abgeschlossen haben und sich zum ersten Mal am Konfigurationsdienstprogramm anmelden, wird der Erst-Setup-Assistent angezeigt, wenn die folgenden Bedingungen nicht erfüllt sind:

- Sie haben keine Lizenz auf der Appliance installiert.
- Sie haben kein Subnetz oder eine zugeordnete IP-Adresse konfiguriert.
- Wenn die Standard-IP-Adresse der Appliances 192.168.100.1 lautet.

#### Konfigurieren Sie Citrix Gateway mit dem Erst-Setup-Assistenten

Um das Citrix Gateway (das physische Gerät oder das virtuelle VPX-Gerät) zum ersten Mal zu konfigurieren, benötigen Sie einen Verwaltungscomputer, der im selben Netzwerk wie das Gerät konfiguriert ist.

Weisen Sie eine Citrix Gateway IP (NSIP) -Adresse als Verwaltungs-IP-Adresse Ihres Geräts und eine Subnetz-IP-Adresse (SNIP) zu, mit der Ihre Server eine Verbindung herstellen können. Sie weisen eine Subnetzmaske zu, die sowohl für Citrix Gateway- als auch für SNIP-Adressen gilt. Konfigurieren Sie auch eine Zeitzone. Wenn Sie einen Hostnamen zuweisen, können Sie auf die Appliance zugreifen, indem Sie ihren Namen anstelle der NSIP-Adresse angeben.

Der Erst-Setup-Assistent besteht aus zwei Abschnitten. Im ersten Abschnitt konfigurieren Sie die grundlegenden Systemeinstellungen für das Citrix Gateway-Gerät, einschließlich:

NSIP-Adresse, SNIP-Adresse und Subnetzmaske
Appliance-Hostname
DNS-Server
Zeitzone
Administratorkennwort
Im zweiten Abschnitt installieren Sie Lizenzen. Wenn Sie die Adresse eines DNS-Servers angeben, können Sie die Hardware-Seriennummer (HSN) oder den Lizenzschlüssel verwenden, um Ihre Lizenzen zuzuweisen, anstatt Ihre Lizenzen von einem lokalen Computer auf die Appliance hochzuladen.

Hinweis: Citrix empfiehlt, Ihre Lizenzen auf Ihrem lokalen Computer zu speichern.

Wenn Sie die Konfiguration dieser Einstellungen abgeschlossen haben, fordert Citrix Gateway Sie auf, das Gerät neu zu starten. Wenn Sie sich erneut bei der Appliance anmelden, können Sie andere Assistenten und das Konfigurationsdienstprogramm verwenden, um andere Einstellungen zu konfigurieren.

### Schneller Konfigurationsassistent

Mit dem Schnellkonfigurationsassistenten können Sie mehrere virtuelle Server auf Citrix Gateway konfigurieren. Sie können virtuelle Server hinzufügen, bearbeiten und entfernen.

Der Schnellkonfigurationsassistent ermöglicht eine nahtlose Konfiguration für die folgenden Bereitstellungen:

- Webinterface-Verbindungen zu Citrix Virtual Apps and Desktops, mit der Möglichkeit, mehrere Instanzen der Secure Ticket Authority (STA) zu konfigurieren
- Nur Citrix Endpoint Management
- Nur StoreFront
- Citrix Endpoint Management und StoreFront zusammen

Mit dem Schnellkonfigurationsassistenten können Sie die folgenden Einstellungen auf der Appliance konfigurieren:

- Name, IP-Adresse und Port des virtuellen Servers
- Umleitung von einem unsicheren zu einem sicheren Port
- LDAP-Server
- RADIUS-Server
- Zertifikate
- DNS-Server
- Citrix Endpoint Management und Citrix Virtual Apps and Desktops

  **Hinweis**: Um SSO zu aktivieren, müssen Sie die Option **Single Sign-On bei Webanwendungen auf** der Registerkarte **Citrix Gateway-Sitzungsprofil erstellen > Clienterfahrung** für die Sitzungsaktion manuell aktivieren.

Citrix Gateway unterstützt Benutzerverbindungen direkt zu Citrix Endpoint Management, wodurch Benutzer Zugriff auf ihre Web-, SaaS- und mobilen Apps sowie Zugriff auf ShareFile erhalten. Sie können auch Einstellungen für StoreFront konfigurieren, wodurch Benutzer Zugriff auf ihre Windows-basierten Anwendungen und virtuellen Desktops erhalten.

Wenn Sie den Assistenten für die Schnellkonfiguration ausführen, werden die folgenden Richtlinien basierend auf Ihren Citrix Endpoint Management-, StoreFront- und Webinterface-Einstellungen erstellt:

- Sitzungsrichtlinien, einschließlich Richtlinien und Profile für Receiver, Receiver für Web, Citrix Gateway Plug-in und Program Neighborhood Agent
- Clientloser Zugriff
- LDAP- und RADIUS-Authentifizierung

#### Konfigurieren Sie die Einstellungen mit dem Schnellkonfigurationsassistenten

Sie können Einstellungen in Citrix Gateway konfigurieren, um die Kommunikation mit Citrix Endpoint Management, StoreFront oder Webinterface mithilfe des Schnellkonfigurationsassistenten zu ermöglichen. Wenn Sie die Konfiguration abgeschlossen haben, erstellt der Assistent die richtigen Richtlinien für die Kommunikation zwischen Citrix Gateway, Endpoint Management, StoreFront oder dem Webinterface. Zu diesen Richtlinien gehören Authentifizierungs-, Sitzungs- und clientlose Zugriffsrichtlinien. Wenn der Assistent abgeschlossen ist, sind die Richtlinien an den virtuellen Server gebunden.

Wenn Sie den Assistenten für die Schnellkonfiguration abgeschlossen haben, kann Citrix Gateway mit Endpoint Management oder StoreFront kommunizieren, und Benutzer können auf ihre Windows-basierten Anwendungen und virtuellen Desktops sowie Web-, SaaS- und mobilen Apps zugreifen. Benutzer können sich dann direkt mit Endpoint Management verbinden.

Während des Assistenten konfigurieren Sie die folgenden Einstellungen:

- Name, IP-Adresse und Port des virtuellen Servers
- Umleitung von einem unsicheren zu einem sicheren Port
- Zertifikate
- LDAP-Server
- RADIUS-Server
- Clientzertifikat für Authentifizierung (nur für Zwei-Faktor-Authentifizierung)
- Endpoint Management, StoreFront oder Webinterface

Der Schnellkonfigurationsassistent unterstützt LDAP-, RADIUS- und Clientzertifikatauthentifizierung. Sie können die Zwei-Faktor-Authentifizierung im Assistenten konfigurieren, indem Sie diese Richtlinien befolgen:

- Wenn Sie LDAP als primären Authentifizierungstyp auswählen, können Sie RADIUS als sekundären Authentifizierungstyp konfigurieren.
- Wenn Sie RADIUS als primären Authentifizierungstyp auswählen, können Sie LDAP als sekundären Authentifizierungstyp konfigurieren.
- Wenn Sie Clientzertifikate als primären Authentifizierungstyp auswählen, können Sie LDAP oder RADIUS als sekundären Authentifizierungstyp konfigurieren.

Sie können nicht mehrere LDAP-Authentifizierungsrichtlinien mithilfe des Schnellkonfigurationsassistenten erstellen. Sie möchten beispielsweise eine Richtlinie konfigurieren, die sAMAccountName im Feld **Serveranmeldungsnamenattribut** verwendet, und eine zweite LDAP-Richtlinie, die den Benutzerprinzipalnamen (UPN) im Feld **Serveranmeldungsnamenattribut** verwendet. Verwenden Sie zum Konfigurieren dieser separaten Richtlinien das Citrix Gateway-Konfigurationsdienstprogramm, um die Authentifizierungsrichtlinien zu erstellen. Weitere Informationen finden Sie unter Konfigurieren der LDAP-Authentifizierung.

Sie können Zertifikate für Citrix Gateway im Schnellkonfigurationsassistenten mithilfe der folgenden Methoden konfigurieren:

- Wählen Sie ein Zertifikat aus, das auf der Appliance installiert ist.
- Installieren Sie ein Zertifikat und einen privaten Schlüssel.
- Wählen Sie ein Testzertifikat aus.
  **Hinweis**: Wenn Sie ein Testzertifikat verwenden, müssen Sie den vollqualifizierten Domänennamen (FQDN) hinzufügen, der im Zertifikat enthalten ist.

Sie können den **Assistenten für die Schnellkonfiguration** auf eine der folgenden zwei Arten öffnen:

- Wenn Sie sich auf der Anmeldeseite von Citrix Gateway befinden und unter **BereitstellungstypCitrix Gateway**auswählen, wird die Registerkarte**Start**angezeigt. Wenn Sie eine andere Option im**Bereitstellungstyp**auswählen, wird die Registerkarte**Start** nicht angezeigt.
- Über den Link **Create/Monitor Citrix Gateway** im Citrix Gateway Detailbereich. Der Link wird angezeigt, wenn Sie eine Lizenz installieren, die Citrix ADC-Funktionen aktiviert. Wenn Sie das Gerät nur für Citrix Gateway lizenzieren, wird der Link nicht angezeigt.

Nachdem Sie den Assistenten zum ersten Mal ausgeführt haben, können Sie den Assistenten erneut ausführen, um weitere virtuelle Server und Einstellungen zu erstellen.

**Wichtig**: Wenn Sie den Assistenten für die Schnellkonfiguration verwenden, um einen zusätzlichen virtuellen Citrix Gateway-Server zu konfigurieren, müssen Sie eine eindeutige IP-Adresse verwenden. Sie können nicht dieselbe IP-Adresse verwenden, die auf einem vorhandenen virtuellen Server verwendet wird. Beispielsweise haben Sie einen virtuellen Server mit der IP-Adresse 192.168.10.5 mit einer Portnummer von 80. Sie führen den Schnellkonfigurations-Assistenten aus, um einen zweiten virtuellen Server mit der IP-Adresse 192.168.10.5 mit Portnummer 443 zu erstellen. Wenn Sie versuchen, die Konfiguration zu speichern, tritt ein Fehler auf.

**So konfigurieren Sie Einstellungen mit dem Schnellkonfigurations-Assistenten**

1. Führen Sie im Konfigurationsdienstprogramm einen der folgenden Schritte aus:
    a) Wenn das Gerät nur für Citrix Gateway lizenziert ist, klicken Sie auf die Registerkarte **Start**.
    b) Wenn die Appliance für die Aufnahme von Citrix ADC-Funktionen lizenziert ist, klicken Sie auf der Registerkarte Konfiguration im Navigationsbereich auf **Citrix Gateway**, und klicken Sie dann im Detailbereich unter **Erste Schritte**auf **Citrix Gateway for Enterprise Store konfigurieren**.
2. Klicken Sie im Dashboard auf **Neues Citrix Gateway erstellen**.
3. Konfigurieren Sie in den **Citrix Gateway-Einstellungen**Folgendes:
    a) Geben Sie **unter Name**einen Namen für den virtuellen Server ein.
    b) Geben Sie unter **IP-Adresse**die IP-Adresse für den virtuellen Server ein.
    c) Geben Sie unter **Port**die Portnummer ein. Die Standardportnummer ist 443.
    d) Wählen Sie Anfragen von Port 80 an sicheren Port umleiten, damit Benutzerverbindungen von Port 80 zu Port 443 wechseln können.
4. Klicken Sie auf **Weiter**.
5. Führen Sie auf der Seite Zertifikat einen der folgenden Schritte aus:
    a) Klicken Sie auf **Choose Certificate** und wählen Sie dann unter Zertifikat das Zertifikat aus.

b) Klicken Sie auf **Zertifikat installieren,** und klicken Sie dann unter **Zertifikat auswählen** und unter **Schlüssel auswählen**auf **Durchsuchen**, um zum Zertifikat und dem privaten Schlüssel zu navigieren.
c) Klicken Sie auf **Testzertifikat verwenden**, und geben Sie dann unter Certificate FQDN den vollqualifizierten Domainnamen (FQDN) ein, der im Testzertifikat enthalten ist

6. Klicken Sie auf **Weiter**.
7. Gehen Sie in den Authentifizierungseinstellungen wie folgt vor:

a) Wählen Sie unter **Primäre Authentifizierung**LDAP, RADIUS oder Cert aus.
b) Wählen Sie einen Authentifizierungsserver aus oder konfigurieren Sie die Einstellungen für den Authentifizierungstyp, den Sie im vorherigen Schritt ausgewählt haben. Wenn Sie Cert wählen, wählen Sie entweder das Clientzertifikat aus oder installieren Sie ein neues Clientzertifikat.
c) Wählen Sie unter **Sekundäre Authentifizierung**den Authentifizierungstyp aus und konfigurieren Sie dann die Einstellungen des Authentifizierungsservers.

8. Klicken Sie auf **Weiter**.

Wenn Sie die Konfiguration der Netzwerk- und Authentifizierungseinstellungen abgeschlossen haben, können Sie die Einstellungen für Citrix Endpoint Management oder Citrix Virtual Apps and Desktops (StoreFront oder Webinterface) konfigurieren.

**Konfigurieren von Enterprise Store-Einstellungen** Citrix Gateway unterstützt den Benutzerzugriff auf Web-, SaaS- und mobile Apps sowie ShareFile nur über Endpoint Management. Wenn Sie auch StoreFront oder das Webinterface bereitstellen, haben Benutzer Zugriff auf Windows-basierte Apps und virtuelle Desktops. Sie können Einstellungen für die folgenden Optionen konfigurieren:

- Nur Endpoint Management
- Nur StoreFront
- Endpoint Management und StoreFront zusammen
- Nur Webinterface

Wenn Sie im vorherigen Verfahren auf **Weiter** klicken, können Sie die Einstellungen für Ihr Bereitstellungsszenario konfigurieren. Die folgenden Verfahren beginnen auf der Seite Citrix Integrationseinstellungen.

Nachdem Sie den virtuellen Server erstellt haben, können Sie beim Bearbeiten des virtuellen Servers im Schnellkonfigurationsassistenten die Einstellungen für Citrix Endpoint Management oder Citrix Virtual Apps and Desktops nicht ändern.

Wenn Sie beispielsweise die Konfiguration eines virtuellen Servers zu einem beliebigen Zeitpunkt abbrechen, bevor Sie die **Citrix Enterprise Store-Einstellungen** konfigurieren, wählt der Assistent automatisch das Webinterface aus, ohne Einstellungen zu konfigurieren. In diesem Fall können Sie

die Details des virtuellen Servers für die Konfiguration des Webinterface bearbeiten, aber Sie können nicht zu Citrix Endpoint Management wechseln. Um zu wechseln, müssen Sie einen neuen virtuellen Server erstellen und dürfen den Assistenten während der Konfiguration zu keinem Zeitpunkt abbrechen. Wenn Sie den virtuellen Webinterface-Server nicht benötigen, können Sie ihn mithilfe des Assistenten für die Schnellkonfiguration löschen.

**So konfigurieren Sie Einstellungen nur für StoreFront**

1. Klicken Sie auf **Citrix Virtual Apps and Desktops**.
2. Wählen Sie unter **BereitstellungstypStoreFront**aus.
3. Geben Sie in **StoreFront FQDN**den vollqualifizierten Domänennamen (FQDN) des StoreFront-Servers ein.
4. Belassen Sie in **Receiver für Web Path** den Standardpfad, oder geben Sie Ihren eigenen Pfad ein.
5. Wählen Sie **HTTPS** für sichere Benutzerverbindungen.
6. Geben Sie unter **Single Sign-On Domain**die Domäne für StoreFront ein.
7. Geben Sie unter **STA-URL**die vollständige IP-Adresse oder den FQDN des Servers ein, auf dem die Secure Ticket Authority (STA) ausgeführt wird, wenn Sie StoreFront bereitstellen und Zugriff auf veröffentlichte Anwendungen von Citrix Virtual Apps oder virtuelle Desktops von Citrix Virtual Desktops aus gewähren.
8. Klicken Sie auf **Fertig**.

Wenn Benutzer über Citrix Gateway eine Verbindung zu StoreFront herstellen, können Benutzer ihre Apps und Desktops entweder von Receiver für Web oder Receiver aus starten.

**So konfigurieren Sie nur Einstellungen für Endpoint Management**

1. Klicken Sie auf **Citrix Endpoint Management**.
2. Geben Sie in **App Controller FQDN**den FQDN für Endpoint Management ein.
3. Klicken Sie auf **Fertig**.

**So konfigurieren Sie Webinterface-Einstellungen**

1. Klicken Sie im Schnellkonfigurationsassistenten auf **Citrix Virtual Apps and Desktops**.
2. Wählen Sie unter **BereitstellungstypWebinterface**aus, und konfigurieren Sie dann Folgendes:

    a) Geben Sie unter **Citrix Virtual Apps Site-URL**die vollständige IP-Adresse oder den FQDN des Webinterface ein.
    b) Geben **Sie in der URL der Citrix Virtual Apps Services-Site**die vollständige IP-Adresse oder den FQDN des Webinterface mit dem Citrix Workspace-App-Pfad ein. Sie können den Standardpfad eingeben oder Ihren eigenen Pfad eingeben.

c) Geben Sie unter **Single Sign-On Domain**die zu verwendende Domain ein.
d) Geben Sie unter **STA-URL**die vollständige IP-Adresse oder den FQDN des Servers ein, auf dem die STA ausgeführt wird.

3. Klicken Sie auf **Fertig**.

## Citrix Gateway Assistent

Sie verwenden den Citrix Gateway-Assistenten, um die folgenden Einstellungen auf dem Gerät zu konfigurieren:

- Virtuelle Server
- Zertifikate
- Nennen Sie Dienstleister
- Authentifizierung
- Autorisierung
- Port-Umleitung
- Clientloser Zugriff
- Clientloser Zugriff für SharePoint

### Konfigurieren von Einstellungen mithilfe des Citrix Gateway-Assistenten

Nachdem Sie den Setup-Assistenten ausgeführt haben, können Sie den Citrix Gateway-Assistenten ausführen, um andere Einstellungen auf Citrix Gateway zu konfigurieren. Sie führen den Citrix Gateway-Assistenten über das Konfigurationsdienstprogramm aus.

Citrix Gateway wird mit einem Testzertifikat geliefert. Wenn Sie kein signiertes Zertifikat von einer Zertifizierungsstelle (CA) haben, können Sie das Testzertifikat verwenden, wenn Sie den Citrix Gateway-Assistenten verwenden. Wenn Sie das signierte Zertifikat erhalten, können Sie das Testzertifikat entfernen und das signierte Zertifikat installieren. Citrix empfiehlt, das signierte Zertifikat zu erhalten, bevor Citrix Gateway für Benutzer öffentlich verfügbar gemacht wird.

Hinweis: Sie können eine Certificate Signing Request (CSR) aus dem Citrix Gateway-Assistenten heraus erstellen. Wenn Sie den Citrix Gateway-Assistenten zum Erstellen der CSR verwenden, müssen Sie den Assistenten beenden und den Assistenten erneut starten, wenn Sie das signierte Zertifikat von der Zertifizierungsstelle erhalten. Weitere Informationen zu Zertifikaten finden Sie unter Installieren und Verwalten von Zertifikaten.

Sie können Benutzerverbindungen für Internet Protocol Version 6 (IPv6) im Citrix Gateway-Assistenten konfigurieren, wenn Sie einen virtuellen Server konfigurieren. Weitere Informationen zur Verwendung von IPv6 für Benutzerverbindungen finden Sie unter Konfigurieren von IPv6 für Benutzerverbindungen.

**So starten Sie den Citrix Gateway-Assistenten**

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf Citrix Gateway.
2. Klicken Sie im Detailbereich unter Erste Schritte auf Citrix Gateway-Assistent.
3. Klicken Sie auf Weiter und folgen Sie dann den Anweisungen des Assistenten.

### Setup Assistent

Sie verwenden den Setup-Assistenten, um die folgenden Anfangseinstellungen auf der Appliance zu konfigurieren:

- System-IP-Adresse und Subnetzmaske
- Zugeordnete IP-Adresse und Subnetzmaske
- Hostname
- Standard-Gateway
- Lizenzen

Hinweis: Laden Sie Ihre Lizenzen von der Citrix Website herunter, bevor Sie den Setup-Assistenten ausführen. Weitere Informationen finden Sie unter
Citrix Gateway lizenzieren

### Assistent für veröffentlichte Anwendungen

Sie verwenden den Assistenten für veröffentlichte Anwendungen, um Citrix Gateway so zu konfigurieren, dass eine Verbindung zu Servern hergestellt wird, auf denen Citrix Virtual Apps and Desktops im internen Netzwerk ausgeführt wird. Mit dem Assistenten für veröffentlichte Anwendungen können Sie:

- Wählen Sie einen virtuellen Server für Verbindungen zur Serverfarm aus.
- Konfigurieren Sie die Einstellungen für Benutzerverbindungen für das Webinterface oder StoreFront, Single Sign-On und die Secure Ticket Authority.
- Erstellen oder wählen Sie Sitzungsrichtlinien für SmartAccess aus.

Innerhalb des Assistenten können Sie auch Ausdrücke für Sitzungsrichtlinien für Benutzerverbindungen erstellen. Weitere Informationen zum Konfigurieren von Citrix Gateway für die Verbindung mit einer Serverfarm finden Sie unter Bereitstellen des Zugriffs auf veröffentlichte Anwendungen und virtuelle Desktops über das Webinterface.

### Integrierte Citrix Endpoint Management-Konfiguration

Sie können Citrix Gateway mit Citrix Endpoint Management MDM bereitstellen, das die Möglichkeit bietet, zu skalieren, Hochverfügbarkeit für Apps sicherzustellen und die Sicherheit aufrechtzuerhalten. Um die Citrix Endpoint Management-Konfiguration verwenden zu können, müssen Sie Version 10.1, Build 120.1316.e installieren.

Die integrierte Citrix Endpoint Management-Konfiguration erstellt Folgendes:

- Load Balancing-Server für Device Manager.
- Lastausgleichsserver für Microsoft Exchange mit E-Mail-Filter.
- Lastausgleichsserver für ShareFile.

Weitere Informationen zum Erstellen von Einstellungen mit der integrierten Citrix Endpoint Management-Konfiguration finden Sie unter Konfigurieren von Einstellungen für Ihre Citrix Endpoint Management-Umgebung

## Konfigurieren von Citrix Gateway

March 27, 2024

Nachdem Sie die Basisnetzwerkeinstellungen auf Citrix Gateway konfiguriert haben, konfigurieren Sie die detaillierten Einstellungen, damit Benutzer eine Verbindung zu Netzwerkressourcen im sicheren Netzwerk herstellen können. Zu diesen Einstellungen gehören:

- Virtuelle Server. Sie können mehrere virtuelle Server auf Citrix Gateway konfigurieren, wodurch Sie je nach dem zu implementierenden Benutzerszenario unterschiedliche Richtlinien erstellen können. Jeder virtuelle Server hat seine eigene IP-Adresse, sein eigenes Zertifikat und einen eigenen Richtliniensatz. Sie können beispielsweise einen virtuellen Server konfigurieren und Benutzer auf Netzwerkressourcen im internen Netzwerk beschränken, abhängig von ihrer Mitgliedschaft in Gruppen und den Richtlinien, die Sie an die virtuellen Server binden. Sie können virtuelle Server mithilfe der folgenden Methoden erstellen:
  - Schneller Konfigurationsassistent
  - Citrix Gateway Assistent
  - Konfigurationsdienstprogramm
- Hohe Verfügbarkeit. Sie können Hochverfügbarkeit konfigurieren, wenn Sie zwei Citrix Gateway-Appliances in Ihrem Netzwerk bereitstellen. Wenn die primären Geräte ausfallen, kann das sekundäre Gerät die Kontrolle übernehmen, ohne die Benutzersitzungen zu beeinträchtigen.

- Zertifikate. Sie können Zertifikate verwenden, um Benutzerverbindungen zu Citrix Gateway zu sichern. Wenn Sie eine Certificate Signing Request (CSR) erstellen, fügen Sie dem Zertifikat den vollqualifizierten Domänennamen hinzu. Sie können Zertifikate an virtuelle Server binden.
- Authentifizierung. Citrix Gateway unterstützt verschiedene Authentifizierungstypen, darunter Lokales LDAP, RADIUS, SAML, Clientzertifikate und TACACS+. Darüber hinaus können Sie die Kaskadierung und die Zwei-Faktor-Authentifizierung konfigurieren.
  Hinweis: Wenn Sie RSA, Safeword oder Gemalto Protiva für die Authentifizierung verwenden, konfigurieren Sie diese Typen mithilfe von RADIUS.
- Benutzerverbindungen. Sie können Benutzerverbindungen mithilfe von Sitzungsprofilen konfigurieren. Innerhalb des Profils können Sie festlegen, mit welchen Plug-Ins sich Benutzer anmelden können, sowie alle Einschränkungen, die Benutzer möglicherweise benötigen. Dann können Sie eine Richtlinie mit einem Profil erstellen. Sie können Sitzungsrichtlinien an Benutzer, Gruppen und virtuelle Server binden.
- Startseite. Sie können das standardmäßige Access Interface als Ihre Homepage verwenden oder eine benutzerdefinierte Homepage erstellen. Die Homepage wird angezeigt, nachdem sich Benutzer erfolgreich bei Citrix Gateway angemeldet haben.
- Endpunktanalyse. Sie können Richtlinien auf Citrix Gateway konfigurieren, die das Benutzergerät bei der Benutzeranmeldung auf Software, Dateien, Registrierungseinträge, Prozesse und Betriebssysteme überprüfen. Mit der Endpunktanalyse können Sie die Sicherheit Ihres Netzwerks erhöhen, indem das Benutzergerät über die erforderliche Software verfügen muss.

## Verwenden des Konfigurationsdienstprogramms

Mit dem Konfigurationsdienstprogramm können Sie die meisten Citrix Gateway-Einstellungen konfigurieren. Sie verwenden einen Webbrowser, um auf das Konfigurationsdienstprogramm zuzugreifen.

### Melden Sie sich beim Konfigurationsdienstprogramm an

1. Geben Sie in einem Webbrowser die System-IP-Adresse von Citrix Gateway ein, `http://192.168.100.1`z.
   Hinweis: Citrix Gateway ist mit einer Standard-IP-Adresse von 192.168.100.1 und einer Subnetzmaske von 255.255.0.0 vorkonfiguriert.
2. Geben Sie unter Benutzername und Kennwort ein `nsroot`.
3. Wählen Sie unter Bereitstellungstyp Citrix Gateway aus und klicken Sie dann auf Anmelden.

Wenn Sie sich zum ersten Mal beim Konfigurationsdienstprogramm anmelden, wird das Dashboard standardmäßig auf der Registerkarte **Home** geöffnet. Auf der Registerkarte **Start** können Sie den Assistenten für die Schnellkonfiguration verwenden, um die Einstellungen für einen virtuellen Server,

Authentifizierung, Zertifikate und Citrix Endpoint Management zu konfigurieren. Sie können auch entweder StoreFront- oder Webinterface-Einstellungen im Schnellkonfigurationsassistenten konfigurieren.

Weitere Informationen zur Konfiguration von Citrix Gateway finden Sie unter:

- Konfigurieren der Anfangseinstellungen mithilfe des Setup-Assistenten.
- Configuring Settings with the Quick Configuration Wizard
- Konfigurieren von Einstellungen mithilfe des Citrix Gateway-Assistenten.

## Virtuelle Server erstellen

March 27, 2024

Ein virtueller Server ist ein Zugriffspunkt, an dem sich Benutzer anmelden. Jeder virtuelle Server hat seine eigene IP-Adresse, sein eigenes Zertifikat und einen eigenen Richtliniensatz. Ein virtueller Server besteht aus einer Kombination aus einer IP-Adresse, einem Port und einem Protokoll, das eingehenden Datenverkehr akzeptiert. Virtuelle Server enthalten die Verbindungseinstellungen für die Anmeldung von Benutzern an der Appliance. Sie können die folgenden Einstellungen auf virtuellen Servern konfigurieren:

- Zertifikate
- Authentifizierung
- Richtlinien
- Lesezeichen
- Adresspools (auch als IP-Pools oder Intranet-IPs bezeichnet)
- Double-Hop-DMZ-Bereitstellung mit Citrix Gateway
- Secure Ticket Authority
- SmartAccess ICA-Proxy-Sitzungsübertragung

Wenn Sie den Citrix Gateway-Assistenten ausführen, können Sie während des Assistenten einen virtuellen Server erstellen. Sie können mehr virtuelle Server auf folgende Weise konfigurieren:

- **Vom Knoten der virtuellen Server**. Dieser Knoten ist im Navigationsbereich des Konfigurationsdienstprogramms. Mithilfe des Konfigurationsdienstprogramms können Sie virtuelle Server hinzufügen, bearbeiten und entfernen.
- **Mit dem Schnellkonfigurations-Assistenten**. Wenn Sie Citrix Endpoint Management, StoreFront oder das Webinterface in Ihrer Umgebung bereitstellen, können Sie den Assistenten für die Schnellkonfiguration verwenden, um den virtuellen Server und alle für Ihre Bereitstellung erforderlichen Richtlinien zu erstellen.

Wenn Sie möchten, dass sich Benutzer anmelden und einen bestimmten Authentifizierungstyp wie RADIUS verwenden, können Sie einen virtuellen Server konfigurieren und dem Server eine eindeutige IP-Adresse zuweisen. Wenn sich Benutzer anmelden, werden sie zum virtuellen Server weitergeleitet und dann zur Eingabe ihrer RADIUS-Anmeldeinformationen aufgefordert.

Sie können auch konfigurieren, wie sich Benutzer bei Citrix Gateway anmelden. Sie können eine Sitzungsrichtlinie verwenden, um den Typ der Benutzersoftware, die Zugriffsmethode und die Homepage zu konfigurieren, die Benutzer nach dem Anmelden sehen.

## So erstellen Sie virtuelle Server

Sie können virtuelle Server mithilfe der Citrix Gateway GUI oder des Schnellkonfigurationsassistenten hinzufügen, ändern, aktivieren oder deaktivieren und entfernen. Weitere Informationen zum Konfigurieren eines virtuellen Servers mit dem Schnellkonfigurationsassistenten finden Sie unter Konfigurieren von Einstellungen mit dem Schnellkonfigurationsassistenten.

> **Hinweis:**
>
> Der virtuelle VPN-Server unterstützt standardmäßig DTLS Version 1.0. Informationen zum Aktivieren der DTLS-Version 1.2 finden Sie unter Konfigurieren des virtuellen DTLS-VPN-Servers mithilfe des virtuellen SSL-VPN-Servers.

### So erstellen Sie einen virtuellen Server über die GUI

1. Navigieren Sie zu **Citrix Gateway > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Konfigurieren Sie die Einstellungen gemäß Ihren Anforderungen.
4. Klicken Sie auf **Create** und dann auf **Close**.

### So erstellen Sie einen virtuellen Server über die CLI

Geben Sie an der Eingabeaufforderung;

```
add vpn vserver <name> <serviceType> [<IPAddress> [<port>]
<!--NeedCopy-->
```

**Beispiel:**

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
<!--NeedCopy-->
```

### Punkte, die beim Binden eines Netzprofils an den virtuellen VPN-Server zu beachten sind

Sie können Netzprofile (Netzwerkprofile) erstellen, um die Appliance für die Verwendung einer bestimmten Quell-IP-Adresse zu konfigurieren und das Netzprofil an den virtuellen VPN-Server zu binden. Beachten Sie jedoch Folgendes, wenn Sie ein Netzprofil an den virtuellen VPN-Server binden.

- Wenn Sie ein Netzprofil an einen virtuellen Citrix Gateway-Server binden, wählt das Netzprofil kein bestimmtes SNIP aus, das vom virtuellen Server oder Dienst für den Datenverkehr zu Back-End-Servern verwendet werden soll. Stattdessen ignoriert das Gateway-Gerät die Netzprofilbindung und verwendet die Round-Robin-Methode zur Auswahl der SNIPs.
- Das Netzprofil funktioniert nicht für dynamisch generierte Dienste (STA, SF-Monitor). Für STA und andere dynamisch generierte Dienste können Sie das Netzprofil direkt an diese Monitore binden, und diese Monitore werden zu diesem Zeitpunkt verwendet. Wenn Sie jedoch mehrere Gateways auf derselben Appliance haben, verwenden alle Gateways dasselbe Netzprofil für die konfigurierten Monitore.

Weitere Einzelheiten zum Netzprofil finden Sie unter Verwenden einer angegebenen Quell-IP für die Back-End-Kommunikation.

### Aktuelle Benutzer und insgesamt verbundene Benutzer auf dem virtuellen Server

**Aktuelle Benutzer:** Anzahl der Benutzer, die an einem bestimmten virtuellen Server angemeldet sind. Es wird empfohlen, dass Sie die aktuellen Benutzer für die Verfolgung von CCUs überwachen.

**Gesamtzahl der verbundenen Benutzer:** Anzahl der Benutzer, die eine oder mehrere aktive Verbindungen über den bestimmten virtuellen Server haben. Die Gesamtzahl der verbundenen Benutzer wird hauptsächlich im ICA-Proxy verwendet.

Sie können die Anzahl der Zähler für verbundene Benutzer insgesamt in den folgenden Szenarien verwenden:

- Bedenken Sie, dass eine ICA-Verbindung hergestellt wurde, aber keine entsprechende Authentifizierungs-, Autorisierungs- und Überwachungssitzung hergestellt wird. In diesem Szenario startet ein Benutzer eine Anwendung oder einen Desktop, schließt den Browser, arbeitet weiterhin an der gestarteten App oder dem gestarteten Desktop. Die Authentifizierungs-, Autorisierungs- und Überwachungssitzung läuft ab, aber die Verbindung ist immer noch aktiv. Die Gesamtzahl der verbundenen Benutzer kann verwendet werden, um die Benutzer zu identifizieren, die noch verbunden sind.
- Beim optimalen HDX-Routing können sich das Authentifizierungs-Gateway und das ICA-Gateway auf verschiedenen Geräten befinden. Die Gesamtzahl der verbundenen Benutzer

kann in diesem Fall verwendet werden, um die Anzahl der verbundenen Benutzer auf dem ICA-Gateway zu ermitteln.

**Zu beachtende Punkte:**

- Aktuelle Benutzer überschreiten die Gesamtzahl der verbundenen Benutzer, wenn es aktive Sitzungen gibt (noch nicht abgelaufen), aber es gibt keine aktiven Verbindungen in diesen Sitzungen. Beispielsweise startete ein Benutzer eine Anwendung oder einen Desktop und schloss sie sofort, meldete sich jedoch nicht von der Authentifizierungs-, Autorisierungs- und Überwachungssitzung ab.
- Die Gesamtzahl der verbundenen Benutzer übersteigt die aktuellen Benutzer, wenn das Timeout für Authentifizierungs-, Autorisierungs- und Überwachungssitzungen abläuft, ICA-
- In einem reinen VPN-Setup (keine ICA ist beteiligt) sind die Anzahl der aktuellen Benutzer und die Gesamtzahl der verbundenen Benutzer gleich.

## Konfigurieren von Verbindungstypen auf dem virtuellen Server

Wenn Sie einen virtuellen Server erstellen und konfigurieren, können Sie die folgenden Verbindungsoptionen konfigurieren:

- Verbindungen mit der Citrix Workspace-App nur mit Citrix Virtual Apps and Desktops ohne SmartAccess-, Endpunktanalyse- oder Netzwerkschicht-Tunneling-Funktionen.
- Verbindungen mit dem Citrix Gateway Plug-in und SmartAccess, die die Verwendung von SmartAccess-, Endpunktanalyse- und Netzwerkschicht-Tunneling-Funktionen ermöglichen.
- Verbindungen mit Secure Hub, der eine Micro-VPN-Verbindung von Mobilgeräten zu Citrix Gateway herstellt.
- Parallele Verbindungen, die von einem Benutzer über das ICA-Sitzungsprotokoll von mehreren Geräten hergestellt wurden. Die Verbindungen werden zu einer einzigen Sitzung migriert, um die Verwendung mehrerer Universal-Lizenzen zu verhindern.

Wenn Sie möchten, dass sich Benutzer ohne Benutzersoftware anmelden, können Sie eine clientlose Zugriffsrichtlinie konfigurieren und an den virtuellen Server binden.

### So konfigurieren Sie Basic- oder SmartAccess-Verbindungen auf einem virtuellen Server

1. Navigieren Sie zu **Citrix Gateway** und klicken Sie dann auf **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie **unter Name**einen Namen für den virtuellen Server ein.
4. Geben Sie unter **IP-Adresse** und **Port**die IP-Adresse und die Portnummer für den virtuellen Server ein.

5. Führen Sie einen der folgenden Schritte aus:
    - Um nur ICA-Verbindungen zuzulassen, klicken Sie auf **Grundmodus**.
    - Um die Benutzeranmeldung mit Secure Hub, dem Citrix Gateway Plug-in und SmartAccess zu ermöglichen, klicken Sie auf **SmartAccess-Modus**.
    - Damit SmartAccess ICA-Proxysitzungen für mehrere Benutzerverbindungen verwalten kann, klicken Sie auf **ICA-Proxysitzungsmigration**.
6. Konfigurieren Sie die anderen Einstellungen für den virtuellen Server, klicken Sie auf **Erstellen**und dann auf **Schließen**.

## Konfigurieren einer Listen-Richtlinie für virtuelle Platzhalter-Server

Sie können virtuelle Citrix Gateway-Server so konfigurieren, dass ein virtueller Server die Möglichkeit einschränkt, auf einem bestimmten VLAN zu hören. Sie können einen virtuellen Platzhalterserver mit einer Listen-Richtlinie erstellen, die ihn auf die Verarbeitung des Datenverkehrs im angegebenen VLAN beschränkt.

Die Konfigurationsparameter lauten:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name des virtuellen Servers. Der Name ist erforderlich und Sie können ihn nicht ändern, nachdem Sie den virtuellen Server erstellt haben. Der Name darf 127 Zeichen nicht überschreiten und das erste Zeichen muss eine Zahl oder ein Buchstabe sein. Sie können auch die folgenden Zeichen verwenden: bei Symbol (@), Unterstrich (_), Bindestrich (-), Punkt (.), Doppelpunkt (:), Pfundzeichen (#) und ein Leerzeichen. |
| IP | Die IP-Adresse des virtuellen Servers. Für einen virtuellen Platzhalterserver, der an das VLAN gebunden ist, ist der Wert immer *. |
| Typ | Das Verhalten des Dienstes. Sie haben die Wahl: HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP und RTSP. |

| Parameter | Beschreibung |
| --- | --- |
| Port | Der Port, auf dem der virtuelle Server auf Benutzerverbindungen wartet. Die Portnummer muss zwischen 0 und 65535 liegen. Für den virtuellen Platzhalterserver, der an ein VLAN gebunden ist, ist der Wert normalerweise *. |
| Hören Sie Priorität | Die Priorität, die der Listen-Richtlinie zugewiesen wird. Die Priorität wird in umgekehrter Reihenfolge ausgewertet; je niedriger die Zahl, desto höher ist die der Listen-Richtlinie zugewiesene Priorität. |
| Richtlinienregel hören | Die Richtlinienregel, die verwendet werden soll, um das VLAN zu identifizieren, auf das der virtuelle Server hören muss. Die Regel lautet: CLIENT.VLAN.ID.EQ (<ipaddressat>) Ersetzen Sie für <ipaddressat>die dem VLAN zugewiesene ID-Nummer. |

**So erstellen Sie einen virtuellen Platzhalterserver mit einer Listenrichtlinie**

1. Erweitern Sie im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie **unter Name**einen Namen für den virtuellen Server ein.
4. Wählen Sie unter **Protokoll**das Protokoll aus.
5. Geben Sie unter **IP-Adresse**die IP-Adresse für den virtuellen Server ein.
6. Geben Sie unter **Port**den Port für den virtuellen Server ein.
7. Geben Sie auf der Registerkarte **Erweitert** unter Listenrichtlinie unter **Listenpriorität**die Priorität für die Listen-Richtlinie ein.
8. Klicken Sie neben Listen-Richtlinienregel auf **Konfigurieren**.
9. Klicken **Sie im Dialogfeld Ausdruck erstellen** auf **Hinzufügen**, konfigurieren Sie den Ausdruck, und klicken Sie dann auf **OK**.
10. Klicken Sie auf **Create** und dann auf **Close**.

## IP-Adressen auf Citrix Gateway konfigurieren

March 27, 2024

Sie können IP-Adressen für die Anmeldung am Konfigurationsdienstprogramm und für Benutzerverbindungen konfigurieren. Citrix Gateway ist mit einer Standard-IP-Adresse von 192.168.100.1 und einer Subnetzmaske von 255.255.0.0 für den Verwaltungszugriff konfiguriert. Die Standard-IP-Adresse wird immer dann verwendet, wenn ein vom Benutzer konfigurierter Wert für die System-IP (NSIP) -Adresse fehlt.

- NSIP-Adresse. Die Management-IP-Adresse für Citrix Gateway, die für den gesamten verwaltungsbezogenen Zugriff auf das Gerät verwendet wird. Citrix Gateway verwendet auch die NSIP-Adresse für die Authentifizierung.
- **Standard-Gateway**. Der Router, der Datenverkehr von außerhalb des sicheren Netzwerks an Citrix Gateway weiterleitet.
- **Subnetz-IP-Adresse (SNIP)**. Die IP-Adresse, die das Benutzergerät durch Kommunikation mit einem Server in einem sekundären Netzwerk darstellt.

Die SNIP-Adresse verwendet die Ports 1024 bis 64000.

### So verwendet Citrix Gateway IP-Adressen

Citrix Gateway bezieht Datenverkehr von IP-Adressen basierend auf der auftretenden Funktion. In der folgenden Liste werden verschiedene Funktionen und die Art und Weise beschrieben, wie Citrix Gateway IP-Adressen für jede verwendet, als allgemeine Richtlinie:

- **Authentifizierung.** Die IP-Adresse, die Citrix Gateway verwendet, hängt vom Typ des Authentifizierungsservers ab.
  - LDAP-/RADIUS/TACACS-Server. Wenn AAAD direkt mit dem virtuellen Authentifizierungsserver kommuniziert, wird die NSIP-Adresse verwendet.
  - Wenn ein Load Balancer als Proxy verwendet wird, verwendet der Load Balancer die SNIP-Adresse für die Authentifizierung. AAAD verwendet die NSIP-Adresse für die Kommunikation mit dem Load Balancer. Die IP-Adresse, die der Citrix ADC verwendet, hängt von der Entität ab, die mit dem virtuellen Authentifizierungsserver kommuniziert.
  - SAML/OAUTH/WEBAUTH-Server: Diese Server kommunizieren über die SNIP-Adresse.
- **Dateiübertragungen von der Homepage.** Citrix Gateway verwendet die SNIP-Adresse.
- **DNS- und WINS-Abfragen.** Citrix Gateway verwendet die SNIP-Adresse.
- **Netzwerkverkehr zu Ressourcen im sicheren Netzwerk.** Citrix Gateway verwendet die SNIP-Adresse oder das IP-Pooling, abhängig von der Konfiguration auf Citrix Gateway.
- **ICA-Proxy-Einstellung.** Citrix Gateway verwendet die SNIP-Adresse.

## Subnetz-IP-Adressen

Die Subnetz-IP-Adresse ermöglicht es dem Benutzer, von einem externen Host, der sich in einem anderen Subnetz befindet, eine Verbindung zu Citrix Gateway herzustellen. Wenn Sie eine Subnetz-IP-Adresse hinzufügen, wird ein entsprechender Routeneintrag in der Routentabelle vorgenommen. Pro Subnetz wird nur ein Eintrag gemacht. Der Routeneintrag entspricht der ersten im Subnetz hinzugefügten IP-Adresse.

Im Gegensatz zur System-IP-Adresse und der zugeordneten IP-Adresse ist es nicht zwingend erforderlich, die Subnetz-IP-Adresse bei der Erstkonfiguration von Citrix Gateway anzugeben.

Die zugeordnete IP-Adresse und Subnetz-IP-Adressen verwenden die Ports 1024 bis 64000.

### So fügen Sie eine Subnetz-IP-Adresse hinzu

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **System\ > Netzwerk**, und klicken Sie dann auf **IPs**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld IP erstellen in das Feld IP-Adresse die IP-Adresse ein.
4. Geben Sie unter Netzwerkmaske die Subnetzmaske ein.
5. Wählen Sie unter IP-Typ Subnetz-IP aus, klicken Sie auf **Schließen** und dann auf **Erstellen**.

## Konfigurieren von IPv6 für Benutzerverbindungen

Sie können Citrix Gateway so konfigurieren, dass mithilfe von Internet Protocol Version 6 (IPv6) auf Benutzerverbindungen gehört wird. Wenn Sie eine der folgenden Einstellungen konfigurieren, können Sie das Kontrollkästchen IPv6 aktivieren und dann die IPv6-Adresse in das Dialogfeld eingeben:

- Globale Einstellungen —Veröffentlichte Anwendungen —ICA-Proxy
- Globale Authentifizierung —RADIUS
- Globale Authentifizierung —LDAP
- Globale Authentifizierung - TACACS
- Sitzungsprofil —Veröffentlichte Anwendungen —ICA-Proxy
- Virtuelle Citrix Gateway-Server
- Authentifizierungsserver erstellen —RADIUS
- Erstellen Sie einen Authentifizierungsserver - LDAP
- Erstellen Sie einen Authentifizierungsserver - TACACS
- Prüfungsserver erstellen
- Einrichtung für hohe Verfügbarkeit
- Binden/Entbinden von Routenmonitoren für Hochverfügbarkeit
- Virtueller Server (Load Balancing)

Wenn Sie den virtuellen Citrix Gateway-Server für das Abhören einer IPv6-Adresse konfigurieren, können Benutzer nur mit der Citrix Workspace-App eine Verbindung herstellen. Benutzerverbindungen mit dem Citrix Gateway Plug-in werden mit IPv6 nicht unterstützt.

Sie können die folgenden Richtlinien für die Konfiguration von IPv6 auf Citrix Gateway verwenden:

- Citrix Virtual Apps und Webinterface. Wenn Sie IPv6 für Benutzerverbindungen konfigurieren und eine zugeordnete IP-Adresse vorhanden ist, die IPv6 verwendet, können Citrix Virtual Apps und Webinterface-Server auch IPv6 verwenden. Das Webinterface muss hinter Citrix Gateway installiert sein. Wenn Benutzer eine Verbindung über Citrix Gateway herstellen, wird die IPv6-Adresse in IPv4 übersetzt. Wenn die Verbindung zurückkehrt, wird die IPv4-Adresse in IPv6 übersetzt.
- Virtuelle Server. Sie können IPv6 für einen virtuellen Server konfigurieren, wenn Sie den Citrix Gateway-Assistenten ausführen. Klicken Sie im Citrix Gateway-Assistenten auf der Seite Virtuelle Server auf IPv6 und geben Sie die IP-Adresse ein. Sie können nur mithilfe des Citrix Gateway-Assistenten eine IPv6-Adresse für einen virtuellen Server konfigurieren.
- Andere. Um IPv6 für ICA-Proxy, Authentifizierung, Überwachung und Hochverfügbarkeit zu konfigurieren, aktivieren Sie im Dialogfeld das Kontrollkästchen IPv6 und geben Sie dann die IP-Adresse ein.

## DNS-Server im sicheren Netzwerk auflösen

March 27, 2024

Wenn sich Ihr DNS-Server im sicheren Netzwerk hinter einer Firewall befindet und die Firewall ICMP-Verkehr blockiert, können Sie keine Verbindungen zum Server testen, da die Firewall die Anforderung blockiert. Sie können dieses Problem beheben, indem Sie die folgenden Schritte ausführen:

- Erstellen eines DNS-Dienstes mit einem benutzerdefinierten DNS-Monitor, der zu einem bekannten vollqualifizierten Domänennamen (FQDN) aufgelöst wird.
- Erstellen eines nicht direkt adressierbaren virtuellen DNS-Servers auf Citrix Gateway.
- Binden des Dienstes an den virtuellen Server.

Hinweis:

- Konfigurieren Sie einen virtuellen DNS-Server und einen DNS-Dienst nur, wenn sich Ihr DNS-Server hinter einer Firewall befindet.
- Wenn Sie eine Citrix ADC-Lastausgleichslizenz auf der Appliance installieren, wird der Knoten Virtuelle Server und Dienste nicht im Navigationsbereich angezeigt. Sie können dieses Verfahren ausführen, indem Sie Load Balancing erweitern und dann auf Virtuelle Server klicken.

### So konfigurieren Sie einen DNS-Dienst und einen DNS-Monitor

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich Virtuelle Server und Dienste, und klicken Sie dann auf Virtuelle Server.
2. Klicken Sie im Detailbereich auf "Hinzufügen".
3. Geben Sie unter Name einen Namen für den Dienst ein.
4. Wählen Sie unter Protokoll DNS aus.
5. Geben Sie unter IP-Adresse die IP-Adresse des DNS-Servers ein.
6. Geben Sie unter Portdie Portnummer ein.
7. Klicken Sie auf der Registerkarte Dienste auf Hinzufügen.
8. Wählen Sie auf der Registerkarte Monitore unter Verfügbar DNS aus, klicken Sie auf Hinzufügen, klicken Sie auf Erstellen und dann auf Schließen.
9. Klicken Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) auf Erstellen und dann auf Schließen.

Erstellen Sie als Nächstes den virtuellen DNS-Server mithilfe des Verfahrens So konfigurieren Sie einen virtuellen DNS-Server und binden Sie dann den DNS-Dienst an den virtuellen Server.

### So binden Sie einen DNS-Dienst an einen virtuellen DNS-Server

1. Klicken Sie im Dialogfeld Virtuellen Dienst konfigurieren (Load Balancing) auf der Registerkarte Dienste auf Hinzufügen, wählen Sie den DNS-Dienst aus, klicken Sie auf Erstellen und dann auf Schließen.

## Virtuelle DNS-Server konfigurieren

March 27, 2024

Um einen virtuellen DNS-Server zu konfigurieren, geben Sie einen Namen und eine IP-Adresse an. Wie beim virtuellen Citrix Gateway-Server müssen Sie dem virtuellen DNS-Server eine IP-Adresse zuweisen. Diese IP-Adresse muss sich jedoch auf der internen Seite des Zielnetzwerks befinden, damit Benutzergeräte alle internen Adressen auflösen. Geben Sie außerdem den DNS-Port an.

**Hinweis**: Wenn Sie eine Citrix ADC-Lastausgleichslizenz auf der Appliance installieren, wird der Knoten
Virtuelle Server und Dienste nicht im Navigationsbereich angezeigt. Sie können diese Funktion mithilfe des virtuellen Lastausgleichsservers konfigurieren. Weitere Informationen finden Sie in der Citrix ADC-Dokumentation in der Citrix Produktdokumentation.

### So konfigurieren Sie einen virtuellen DNS-Server

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich Virtuelle Server und Dienste, und klicken Sie dann auf Virtuelle Server.
2. Klicken Sie im Detailbereich auf "Hinzufügen".
3. Geben Sie unter Nameeinen Namen für den virtuellen Server ein.
4. Geben Sie unter IP-Adresse die IP-Adresse des DNS-Servers ein.
5. Geben Sie unter Port den Port ein, auf dem der DNS-Server lauscht.
6. Wählen Sie unter Protokoll DNS aus und klicken Sie dann auf Erstellen.

Verknüpfen Sie schließlich den virtuellen DNS-Server mit Citrix Gateway über eine der folgenden beiden Methoden, abhängig von den Anforderungen Ihrer Bereitstellung:

- Binden Sie den Server global an Citrix Gateway.
- Binden Sie den virtuellen DNS-Server auf einer pro-virtuellen Serverbasis.

Wenn Sie den virtuellen DNS-Server global bereitstellen, haben alle Benutzer Zugriff darauf. Dann können Sie Benutzer einschränken, indem Sie den virtuellen DNS-Server an den virtuellen Server binden.

## Namensdienstanbieter konfigurieren

March 27, 2024

Citrix Gateway verwendet Namensdienstanbieter, um Webadressen in IP-Adressen umzuwandeln.

Wenn Sie den Citrix Gateway-Assistenten ausführen, können Sie entweder einen DNS-Server oder einen WINS-Server konfigurieren. Sie können das Konfigurationsdienstprogramm verwenden, um auch andere DNS- oder WINS-Server zu konfigurieren.

### So fügen Sie Citrix Gateway einen DNS-Server hinzu

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte "Configuration"im Navigationsbereich "Citrix Gateway"und klicken Sie auf "Global Settings".
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Klicken Sie auf der Registerkarte Netzwerkkonfiguration auf Hinzufügen.
4. Geben Sie im Dialogfeld Namensserver einfügen unter IP-Adresse die IP-Adresse des DNS-Servers ein, klicken Sie auf Erstellen und dann auf Schließen.
5. Klicken Sie im Konfigurationsdienstprogramm auf OK.

### So fügen Sie Citrix Gateway einen WINS-Server hinzu

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Geben Sie auf der Registerkarte Netzwerkkonfiguration in WINS Server IP die IP-Adresse des WINS-Servers ein und klicken Sie dann auf OK.

Geben Sie als Nächstes den Namen und die IP-Adresse des virtuellen DNS-Servers an. Wie beim virtuellen Citrix Gateway-Server muss dem virtuellen Server eine IP-Adresse zugewiesen werden. Diese IP-Adresse muss sich jedoch auf der internen Seite des Zielnetzwerks befinden, damit Benutzergeräte alle internen Adressen ordnungsgemäß auflösen. Sie müssen auch den DNS-Port angeben.

Wenn Sie einen DNS-Server und einen WINS-Server für die Namensauflösung konfigurieren, können Sie dann mithilfe des Citrix Gateway-Assistenten auswählen, welcher Server zuerst die Namenssuche durchführt.

### So geben Sie die Priorität der Namenssuche an

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf Citrix Gateway.
2. Klicken Sie im Detailbereich unter Erste Schritte auf Citrix Gateway-Assistent.
3. Klicken Sie auf Weiter, um die aktuellen Einstellungen zu akzeptieren, bis Sie zur Seite Name Service Provider gelangen.
4. Wählen Sie unter Name Lookup Priority WINS oder DNS aus und fahren Sie dann bis zum Ende des Assistenten fort.

## Serverinitiierte Verbindungen konfigurieren

March 27, 2024

Für jeden Benutzer, der bei Citrix Gateway mit aktivierten IP-Adressen angemeldet ist, wird das DNS-Suffix an den Benutzernamen angehängt und ein DNS-Adressdatensatz wird zum DNS-Cache der Appliance hinzugefügt. Diese Technik hilft dabei, Benutzern einen DNS-Namen anstelle der IP-Adressen der Benutzer zur Verfügung zu stellen.

Wenn der Sitzung eines Benutzers eine IP-Adresse zugewiesen wird, ist es möglich, über das interne Netzwerk eine Verbindung zum Gerät des Benutzers herzustellen. Beispielsweise können Benutzer, die sich mit dem Remotedesktop oder einem Virtual Network Computing (VNC) -Client verbinden, auf

das Benutzergerät zugreifen, um eine Problemanwendung zu diagnostizieren. Es ist auch möglich, dass zwei Citrix Gateway-Benutzer mit internen Netzwerk-IP-Adressen, die remote angemeldet sind, über Citrix Gateway miteinander kommunizieren. Das Erkennen der internen Netzwerk-IP-Adressen der angemeldeten Benutzer auf der Appliance ermöglicht diese Kommunikation.

Ein Remotebenutzer kann dann den folgenden Ping-Befehl verwenden, um die interne Netzwerk-IP-Adresse eines Benutzers zu ermitteln, der bei Citrix Gateway angemeldet sein kann:

```
ping \<username.domainname\>
```

Ein Server kann auf folgende verschiedene Arten eine Verbindung zu einem Benutzergerät herstellen:

- TCP- oder UDP-Verbindungen. Die Verbindungen können von einem externen System im internen Netzwerk oder von einem anderen bei Citrix Gateway angemeldeten Computer stammen. Die interne Netzwerk-IP-Adresse, die jedem bei Citrix Gateway angemeldeten Benutzergerät zugewiesen wird, wird für diese Verbindungen verwendet. Die verschiedenen Arten von serverinitiierten Verbindungen, die Citrix Gateway unterstützt, werden beschrieben.
  Bei TCP- oder UDP-Server-initiierten Verbindungen verfügt der Server über Vorkenntnisse über die IP-Adresse und den Port des Benutzergeräts und stellt eine Verbindung zu diesem her. Citrix Gateway fängt diese Verbindung ab.

  Dann stellt das Benutzergerät eine erste Verbindung zum Server her und der Server stellt an einem Port eine Verbindung zum Benutzergerät her, der bekannt ist oder von dem ersten konfigurierten Port abgeleitet ist.

  In diesem Szenario stellt das Benutzergerät eine erste Verbindung zum Server her und tauscht dann Ports und IP-Adressen mit dem Server aus, indem ein anwendungsspezifisches Protokoll verwendet wird, in das diese Informationen eingebettet sind. Auf diese Weise kann das Citrix Gateway Anwendungen wie aktive FTP-Verbindungen unterstützen.
- Port-Befehl. Dies wird in einem aktiven FTP und in bestimmten Voice-over-IP-Protokollen verwendet.
- Verbindungen zwischen Plug-Ins. Citrix Gateway unterstützt Verbindungen zwischen Plug-Ins mithilfe der internen Netzwerk-IP-Adressen.

  Bei dieser Art von Verbindung können zwei Citrix Gateway-Benutzergeräte, die dasselbe Citrix Gateway verwenden, Verbindungen miteinander herstellen. Ein Beispiel für diesen Typ ist die Verwendung von Instant Messaging-Anwendungen wie Office Communicator oder Yahoo! Bote.

Wenn sich ein Benutzer von Citrix Gateway abmeldet und die Abmeldeanforderung das Gerät nicht erreicht hat, kann sich der Benutzer mithilfe eines beliebigen Geräts erneut anmelden und die vorherige Sitzung durch eine neue Sitzung ersetzen. Diese Funktion kann bei Bereitstellungen von Vorteil sein, bei denen pro Benutzer eine IP-Adresse zugewiesen wird.

Wenn sich ein Benutzer zum ersten Mal bei Citrix Gateway anmeldet, wird eine Sitzung erstellt und dem Benutzer eine IP-Adresse zugewiesen. Wenn sich der Benutzer abmeldet, die Abmeldeanforderung jedoch verloren geht oder das Benutzergerät keine saubere Abmeldung durchführt, wird die Sitzung auf dem System aufrechterhalten. Wenn der Benutzer versucht, sich von demselben Gerät oder einem anderen Gerät aus erneut anzumelden, wird nach erfolgreicher Authentifizierung ein Anmeldedialogfeld für die Übertragung angezeigt. Wenn der Benutzer die Anmeldung übertragen möchte, wird die vorherige Sitzung auf Citrix Gateway geschlossen und eine neue Sitzung erstellt. Die Übertragung der Anmeldung ist nach der Abmeldung nur zwei Minuten lang aktiv, und wenn die Anmeldung von mehreren Geräten gleichzeitig versucht wird, ersetzt der letzte Anmeldeversuch die ursprüngliche Sitzung.

## Routing auf Citrix Gateway konfigurieren

March 27, 2024

Um Zugriff auf interne Netzwerkressourcen zu ermöglichen, leitet Citrix Gateway Daten an Ihre internen, sicheren Netzwerke weiter. Standardmäßig verwendet Citrix Gateway eine statische Route.

Die Netzwerke, an die Citrix Gateway Daten weiterleiten kann, werden durch die Art und Weise bestimmt, wie Sie die Citrix Gateway-Routingtabelle und das Standardgateway konfigurieren, das Sie für Citrix Gateway angeben.

Die Citrix Gateway-Routingtabelle muss die Routen enthalten, die erforderlich sind, um Daten an eine interne Netzwerkressource weiterzuleiten, auf die ein Benutzer möglicherweise zugreifen muss.

Citrix Gateway unterstützt die folgenden Routingprotokolle:

- Routing-Informationsprotokoll (RIP v1 und v2)
- Öffnen Sie zuerst den kürzesten Pfad (OSPF)
- Grenz-Gateway-Protokoll (BGF)

### Konfigurieren einer statischen Route

Wenn Sie die Kommunikation mit einem anderen Host oder Netzwerk einrichten, müssen Sie eine statische Route von Citrix Gateway zum neuen Ziel konfigurieren, wenn Sie kein dynamisches Routing verwenden.

#### So konfigurieren Sie eine statische Route

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **System > Netzwerk > Erweitert**, und klicken Sie dann auf **Routen**.

2. Klicken Sie im Detailbereich auf der Registerkarte Einfach auf **Hinzufügen**.
3. Konfigurieren Sie die Einstellungen für die Route und klicken Sie dann auf **Erstellen**.

**So testen Sie eine statische Route**

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich **System,** und klicken Sie dann auf **Diagnose**.
2. Klicken Sie im Detailbereich unter Dienstprogramme auf **Ping**.
3. Geben Sie unter Parameter unter Host name den Namen des Geräts ein.
4. Geben Sie unter Erweitert unter Quell-IP-Adresse die IP-Adresse des Geräts ein, und klicken Sie dann auf **Ausführen**.

   Wenn Sie erfolgreich mit dem anderen Gerät kommunizieren, zeigen Nachrichten an, dass dieselbe Anzahl von Paketen übertragen und empfangen wurde und keine Pakete verloren gegangen sind.

   Wenn Sie nicht mit dem anderen Gerät kommunizieren, zeigen die Statusmeldungen an, dass keine Pakete empfangen wurden und alle Pakete verloren gegangen sind. Wiederholen Sie den Vorgang, um diesen Mangel an Kommunikation zu beheben, um eine statische Route hinzuzufügen.

Um den Test zu beenden, klicken Sie im **Ping-Dialogfeld** auf **Stopp** und dann auf **Schließen**.

## Automatische Aushandlung konfigurieren

March 27, 2024

Standardmäßig ist die Appliance für die Verwendung der automatischen Aushandlung konfiguriert, bei der Citrix Gateway den Netzwerkverkehr gleichzeitig in beide Richtungen überträgt und die entsprechende Adaptergeschwindigkeit bestimmt. Wenn Sie die Standardeinstellung auf
Auto Negotiation belassen, verwendet Citrix Gateway den Vollduplex-Betrieb, bei dem der Netzwerkadapter Daten gleichzeitig in beide Richtungen senden kann.

Wenn Sie die automatische Aushandlung deaktivieren, verwendet Citrix Gateway einen Halbduplex-Betrieb, bei dem der Adapter Daten in beide Richtungen zwischen zwei Knoten senden kann, der Adapter jedoch nur die eine oder andere Richtung gleichzeitig verwenden kann.

Für die Erstinstallation empfiehlt Citrix, Citrix Gateway so zu konfigurieren, dass die automatische Aushandlung für Ports verwendet wird, die mit der Appliance verbunden sind. Nachdem Sie sich anfänglich angemeldet und Citrix Gateway konfiguriert haben, können Sie die automatische Aushand-

lung deaktivieren. Sie können die automatische Aushandlung nicht global konfigurieren. Sie müssen die Einstellung für jede Schnittstelle aktivieren oder deaktivieren.

### So aktivieren oder deaktivieren Sie die automatische Aushandlung

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **System\ > Netzwerk,** und klicken Sie dann auf **Schnittstellen**.
2. Wählen Sie im Detailbereich die Schnittstelle aus, und klicken Sie dann auf **Öffnen**.
3. Führen Sie im Dialogfeld „ **Schnittstelle konfigurieren** “einen der folgenden Schritte aus:
    - Um die automatische Aushandlung zu aktivieren, klicken Sie neben Auto Negotiation auf **Ja** und dann auf **OK**.
    - Um die automatische Aushandlung zu deaktivieren, klicken Sie neben Auto Negotiation auf **Nein** und dann auf **OK**.

## Hostnamen und FQDN auf Citrix Gateway konfigurieren

March 27, 2024

Der Hostname ist der Name des Citrix Gateway-Geräts, das der Lizenzdatei zugeordnet ist. Der Hostname ist eindeutig für die Appliance und wird verwendet, wenn Sie die Universal-Lizenz herunterladen. Sie definieren den Hostnamen, wenn Sie den Setup-Assistenten ausführen, um Citrix Gateway zum ersten Mal zu konfigurieren.

Der vollqualifizierte Domänenname (FQDN) ist im signierten Zertifikat enthalten, das an einen virtuellen Server gebunden ist. Sie konfigurieren den FQDN nicht auf Citrix Gateway. Einer Appliance kann jedem virtuellen Server, der auf Citrix Gateway mithilfe von Zertifikaten konfiguriert ist, ein eindeutiger FQDN zugewiesen werden.

Den FQDN eines Zertifikats finden Sie, indem Sie die Details des Zertifikats anzeigen. Der FQDN ist Antragstellerfeld des Zertifikats.

### So zeigen Sie den FQDN eines Zertifikats an

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **SSL,** und klicken Sie dann auf **Zertifikate**.
2. Wählen Sie im Detailbereich ein Zertifikat aus, klicken Sie auf **Aktion** und dann auf **Details**.
3. Klicken Sie im Dialogfeld „Zertifikatsdetails“auf **Betreff**. Der FQDN des Zertifikats wird in der Liste angezeigt.

# Richtlinien und Profile auf Citrix Gateway

March 27, 2024

Mit Richtlinien und Profilen auf Citrix Gateway können Sie Konfigurationseinstellungen unter bestimmten Szenarien oder Bedingungen verwalten und implementieren. Eine einzelne Richtlinie gibt die Konfigurationseinstellungen an oder definiert sie, die in Kraft treten, wenn eine bestimmte Reihe von Bedingungen erfüllt ist. Jede Richtlinie hat einen eindeutigen Namen und kann ein an die Richtlinie gebundenes Profil haben.

## So funktionieren Richtlinien

Eine Richtlinie besteht aus einer booleschen Bedingung und einer Sammlung von Einstellungen, die als Profil bezeichnet werden. Die Bedingung wird zur Laufzeit ausgewertet, um festzustellen, ob die Richtlinie angewendet werden muss.

Ein Profil ist eine Sammlung von Einstellungen, die bestimmte Parameter verwenden. Das Profil kann einen beliebigen Namen haben und Sie können ihn in mehr als einer Richtlinie wiederverwenden. Sie können mehrere Einstellungen innerhalb des Profils konfigurieren, aber Sie können nur ein Profil pro Richtlinie einschließen.

Sie können Richtlinien mit den konfigurierten Bedingungen und Profilen an virtuelle Server, Gruppen, Benutzer oder global binden. Richtlinien werden durch die Art der Konfigurationseinstellungen bezeichnet, die sie steuern. In einer Sitzungsrichtlinie können Sie beispielsweise steuern, wie sich Benutzer anmelden und wie viele Benutzer angemeldet bleiben können.

Wenn Sie Citrix Gateway mit Citrix Virtual Apps verwenden, werden Citrix Gateway-Richtliniennamen als Filter an Citrix Virtual Apps gesendet. Wenn Sie Citrix Gateway so konfigurieren, dass es mit Citrix Virtual Apps und SmartAccess kompatibel ist, konfigurieren Sie die folgenden Einstellungen in Citrix Virtual Apps:

- Der Name des virtuellen Servers, der auf der Appliance konfiguriert ist. Der Name wird als Citrix Gateway-Farmname an Citrix Virtual Apps gesendet.
- Die Namen der Vorauthentifizierungs- oder Sitzungsrichtlinien werden als Filternamen gesendet.

Weitere Informationen zum Konfigurieren von Citrix Gateway für die Kompatibilität mit Citrix Endpoint Management finden Sie unterKonfigurieren von Einstellungen für Ihre Citrix Endpoint Management-Umgebung.

Weitere Informationen zum Konfigurieren von Citrix Gateway für die Kompatibilität mit Citrix Virtual Apps and Desktops finden Sie unterZugriff auf Citrix Virtual Apps und Citrix Virtual Desk-

tops Ressourcen mit dem Webinterfaceund Integration mit Citrix Endpoint Management oder StoreFront.

Weitere Informationen zu Vorauthentifizierungsrichtlinien finden Sie unter Konfigurieren von Endpunktrichtlinien.

### Bedingte Richtlinien

Beim Konfigurieren von Richtlinien können Sie einen beliebigen booleschen Ausdruck verwenden, um die Bedingung für die Anwendung der Richtlinie auszudrücken. Wenn Sie bedingte Richtlinien konfigurieren, können Sie einen der verfügbaren Systemausdrücke verwenden, z. B. den folgenden:

- Sicherheitszeichenfolgen für Kunden
- Informationen zum Netzwerk
- HTTP-Header und Cookies
- Uhrzeit des Tages
- Clientzertifikatwerte

Sie können auch Richtlinien erstellen, die nur angewendet werden, wenn das Benutzergerät bestimmte Kriterien erfüllt, z. B. eine Sitzungsrichtlinie für SmartAccess.

Ein weiteres Beispiel für die Konfiguration einer bedingten Richtlinie ist das Variieren der Authentifizierungsrichtlinie für Benutzer. Sie können beispielsweise verlangen, dass Benutzer, die sich von außerhalb des internen Netzwerks mit dem Citrix Gateway Plug-in verbinden, z. B. von ihrem Heimcomputer oder mithilfe von Micro VPN von einem mobilen Gerät aus, mithilfe von LDAP authentifiziert werden, und Benutzer, die sich über das WAN verbinden, mit RADIUS authentifiziert werden.

Hinweis : Sie können keine Richtlinienbedingungen verwenden, die auf Ergebnissen der Endpunktanalyse basieren, wenn die Richtlinienregel als Teil der Sicherheitseinstellungen in einem Sitzungsprofil konfiguriert ist.

### Prioritäten von Richtlinien

Richtlinien werden in der Reihenfolge priorisiert und bewertet, in der die Richtlinie gebunden ist.

Die folgenden beiden Methoden bestimmen die Priorität der Richtlinie:

- Die Ebene, an die die Richtlinie gebunden ist: global, virtueller Server, Gruppe oder Benutzer. Die Richtlinienebenen werden wie folgt vom höchsten zum niedrigsten eingestuft:
  - Benutzer (höchste Priorität)
  - Gruppe
  - Virtueller Server
  - Global (niedrigste Priorität)

- Die numerische Priorität hat unabhängig von der Ebene, an die die Richtlinie gebunden ist, Vorrang. Wenn eine global gebundene Richtlinie eine Prioritätsnummer von einer hat und eine andere an einen Benutzer gebundene Richtlinie eine Prioritätsnummer von zwei hat, hat die globale Richtlinie Vorrang. Eine niedrigere Prioritätszahl gibt der Richtlinie eine höhere Priorität.

### Erstellen von Richtlinien auf Citrix Gateway

Sie können das Konfigurationsdienstprogramm verwenden, um Richtlinien zu erstellen. Nachdem Sie eine Richtlinie erstellt haben, binden Sie die Richtlinie an die entsprechende Ebene: Benutzer, Gruppe, virtueller Server oder global. Wenn Sie eine Richtlinie an eine dieser Ebenen binden, erhalten Benutzer die Einstellungen innerhalb des Profils, wenn die Richtlinienbedingungen erfüllt sind. Jede Richtlinie und jedes Profil hat einen eindeutigen Namen.

Wenn Sie Citrix Endpoint Management oder StoreFront als Teil Ihrer Bereitstellung verwenden, können Sie den Assistenten für die Schnellkonfiguration verwenden, um die Einstellungen für diese Bereitstellung zu konfigurieren. Weitere Informationen zum Assistenten finden Sie unter Konfigurieren von Einstellungen mit dem Schnellkonfigurationsassistenten.

## Konfigurieren von Systemausdrücken

March 27, 2024

Ein Systemausdruck gibt die Bedingungen an, unter denen die Richtlinie durchgesetzt wird. Beispielsweise werden Ausdrücke in einer Vorauthentifizierungsrichtlinie durchgesetzt, während sich ein Benutzer anmeldet. Ausdrücke in einer Sitzungsrichtlinie werden ausgewertet und durchgesetzt, nachdem der Benutzer authentifiziert und bei Citrix Gateway angemeldet wurde.

Zu den Ausdrücken auf Citrix Gateway gehören:

- Allgemeine Ausdrücke, die die Objekte einschränken, die Benutzer beim Herstellen einer Verbindung zu Citrix Gateway verwenden können. Sehen Sie zum Beispiel:
  - Sitzungsrichtlinien
- Client-Sicherheitsausdrücke, die die Software, Dateien, Prozesse oder Registrierungswerte definieren, die auf dem Benutzergerät installiert und ausgeführt werden müssen. Sehen Sie zum Beispiel:
  - Endpunktrichtlinien

- Netzwerkbasierte Ausdrücke, die den Zugriff basierend auf Netzwerkeinstellungen einschränken. Sehen Sie zum Beispiel:
  - Datenverkehrsrichtlinien
  - Richtlinien zur Autorisierung

Citrix Gateway kann auch als Citrix ADC Appliance verwendet werden. Einige Ausdrücke auf der Appliance gelten eher für Citrix ADC. Allgemeine und netzwerkbasierte Ausdrücke werden üblicherweise mit Citrix ADC verwendet und im Allgemeinen nicht mit Citrix Gateway verwendet. Client-Sicherheitsausdrücke werden auf Citrix Gateway verwendet, um festzustellen, dass die richtigen Elemente auf dem Benutzergerät installiert sind.

### Konfigurieren von Client-Sicherheitsausdrücken

Ausdrücke sind Bestandteil einer Richtlinie. Ein Ausdruck stellt eine einzelne Bedingung dar, die anhand einer Anforderung oder einer Antwort ausgewertet wird. Sie können eine einfache Ausdruckssicherheitszeichenfolge erstellen, um nach Bedingungen zu suchen, wie zum Beispiel:

- Betriebssystem des Benutzergeräts einschließlich Service Packs
- Version der Antivirensoftware und Virendefinitionen
- Dateien
- Prozesse
- Registry-Werte
- Benutzer-Zertifikate

## Zertifikatsverwaltung auf Citrix Gateway

March 27, 2024

Auf Citrix Gateway verwenden Sie Zertifikate, um sichere Verbindungen herzustellen und Benutzer zu authentifizieren.

Um eine sichere Verbindung herzustellen, ist an einem Ende der Verbindung ein Serverzertifikat erforderlich. Am anderen Ende der Verbindung ist ein Stammzertifikat der Certificate Authority (CA) erforderlich, die das Serverzertifikat ausgestellt hat.

- Serverzertifikat. Ein Serverzertifikat bescheinigt die Identität des Servers. Citrix Gateway erfordert diese Art von digitalem Zertifikat.
- Root-Zertifikat. Ein Stammzertifikat dient zur Identifizierung der Zertifizierungsstelle, die das Serverzertifikat signiert hat. Das Stammzertifikat gehört der Certificate Authority. Ein Benutzergerät benötigt diese Art von digitalem Zertifikat, um das Serverzertifikat zu überprüfen.

Beim Herstellen einer sicheren Verbindung mit einem Webbrowser auf dem Benutzergerät sendet der Server sein Zertifikat an das Gerät.

Wenn das Benutzergerät ein Serverzertifikat erhält, prüft der Webbrowser wie Internet Explorer, welche CA das Zertifikat ausgestellt hat und ob das Benutzergerät der CA vertraut. Wenn der CA nicht vertraut wird oder wenn es sich um ein Testzertifikat handelt, fordert der Webbrowser den Benutzer auf, das Zertifikat zu akzeptieren oder abzulehnen (die Möglichkeit, auf die Website zuzugreifen, effektiv zu akzeptieren oder abzulehnen).

Citrix Gateway unterstützt die folgenden drei Arten von Zertifikaten:

- Ein Testzertifikat, das an einen virtuellen Server gebunden ist und auch für Verbindungen zu einer Serverfarm verwendet werden kann. Citrix Gateway wird mit einem vorinstallierten Testzertifikat geliefert.
- Ein Zertifikat im PEM- oder DER-Format, das von einer CA signiert und mit einem privaten Schlüssel gekoppelt ist.
- Ein Zertifikat im Format PKCS #12, das zum Speichern oder Transportieren des Zertifikats und des privaten Schlüssels verwendet wird. Das PKCS #12 -Zertifikat wird normalerweise aus einem vorhandenen Windows-Zertifikat als PFX-Datei exportiert und dann auf Citrix Gateway installiert.

Citrix empfiehlt die Verwendung eines Zertifikats, das von einer vertrauenswürdigen Zertifizierungsstelle wie Thawte oder Verisign signiert wurde.

## Zertifikatsignieranforderung erstellen

March 27, 2024

Um sichere Kommunikation über SSL oder TLS bereitzustellen, ist ein Serverzertifikat auf Citrix Gateway erforderlich. Bevor Sie ein Zertifikat auf Citrix Gateway hochladen können, müssen Sie eine Certificate Signing Request (CSR) und einen privaten Schlüssel generieren. Sie verwenden die im Citrix Gateway-Assistenten enthaltene Zertifikatsanforderung erstellen oder das Konfigurationsdienstprogramm, um die CSR zu erstellen. Die Zertifikatsanforderung erstellen erstellt eine CSR-Datei, die zur Signatur per E-Mail an die Zertifizierungsstelle (CA) gesendet wird, und einen privaten Schlüssel, der auf der Appliance verbleibt. Die CA signiert das Zertifikat und sendet es an die von Ihnen angegebene E-Mail-Adresse an Sie zurück. Wenn Sie das signierte Zertifikat erhalten, können Sie es auf Citrix Gateway installieren. Wenn Sie das Zertifikat von der CA zurückerhalten, koppeln Sie das Zertifikat mit dem privaten Schlüssel.

Wichtig: Wenn Sie den Citrix Gateway-Assistenten zum Erstellen der CSR verwenden, müssen Sie den Assistenten beenden und warten, bis die CA Ihnen das signierte Zertifikat sendet. Wenn Sie das Zertifikat erhalten, können Sie den Citrix Gateway-Assistenten erneut ausführen, um die Einstellungen

zu erstellen und das Zertifikat zu installieren. Weitere Informationen zum Citrix Gateway-Assistenten finden Sie unter
Konfigurieren von Einstellungen mithilfe des Citrix Gateway-Assistenten.

### Erstellen einer CSR mithilfe des Citrix Gateway-Assistenten

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf **Citrix ADC Gateway**.
2. Klicken Sie im Detailbereich unter Erste Schritte auf **Citrix ADC Gateway** Wizard.
3. Folgen Sie den Anweisungen des Assistenten, bis Sie zur Seite Serverzertifikat angeben gelangen.
4. Klicken Sie auf **Erstellen einer Zertifikatsignieranforderung** und füllen Sie die Felder aus.
   Hinweis: Der vollqualifizierte Domänenname (FQDN) muss nicht mit dem Citrix Gateway-Hostnamen übereinstimmen. Der FQDN wird für die Benutzeranmeldung verwendet.
5. Klicken Sie auf **Erstellen**, um das Zertifikat auf Ihrem Computer zu speichern, und klicken Sie dann auf **Schließen**.
6. Beenden Sie den Citrix Gateway Assistenten, ohne Ihre Einstellungen zu speichern.

### Erstellen Sie eine CSR mithilfe der Citrix ADC GUI

Sie können auch die Citrix ADC GUI verwenden, um eine CSR zu erstellen, ohne den Citrix Gateway-Assistenten auszuführen.

1. Navigieren Sie zu **Traffic Management** > **SSL > SSL-Dateien** und wählen Sie**Certificate Signing Request (CSR) erstellen**.
2. Füllen Sie die Einstellungen für das Zertifikat aus und klicken Sie dann auf **Erstellen**.

Nachdem Sie das Zertifikat und den privaten Schlüssel erstellt haben, senden Sie das Zertifikat per E-Mail an die CA wie Thawte oder Verisign.

Ausführliche Vorgehensweise finden Sie unter Erstellen einer Zertifikatsignieranforderung.

### Installieren Sie das signierte Zertifikat auf Citrix Gateway

Wenn Sie das signierte Zertifikat von der Certificate Authority (CA) erhalten, koppeln Sie es mit dem privaten Schlüssel auf dem Gerät und installieren Sie das Zertifikat dann auf Citrix Gateway.

#### Koppeln Sie das signierte Zertifikat über die GUI mit einem privaten Schlüssel

1. Kopieren Sie das Zertifikat mithilfe eines Secure Shell (SSH) -Programms wie WinSCP nach Citrix Gateway in den Ordner nsconfig/ssl.

2. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **SSL > Zertifikate**.
3. Klicken Sie auf der Seite **SSL-Zertifikat** auf **Erste Schritte**.
4. Klicken Sie im Detailbereich auf **Installieren**.
5. Geben Sie im Feld **Name des Zertifikatsschlüsselpaars** den Namen des Zertifikats ein.
6. Klicken Sie unter **Zertifikatsdateiname**auf **Appliance**
7. Navigieren Sie zum Zertifikat, klicken **Sie auf Auswählen**und dann auf **Öffnen**.
8. Klicken Sie unter **Schlüsseldateiname**auf **Appliance**. Der Name des privaten Schlüssels entspricht dem Namen der Certificate Signing Request (CSR). Der private Schlüssel befindet sich auf Citrix Gateway im Verzeichnis\ nsconfig\ ssl.
9. Wählen Sie den privaten Schlüssel aus und klicken Sie dann auf **Öffnen**.
10. Wenn das Zertifikat im PEM-Format ist, geben Sie unter **Passwort das Passwort**für den privaten Schlüssel ein.
11. Wenn Sie eine Benachrichtigung für den Ablauf des Zertifikats konfigurieren möchten, wählen Sie **Bei Ablauf benachrichtigen**.
12. Geben Sie im **Feld Benachrichtigungszeitraum**die Anzahl der Tage ein, klicken Sie auf **Erstellen**und dann auf **Schließen**.

#### Binden Sie das Zertifikat und den privaten Schlüssel über die GUI an einen virtuellen Server

Nachdem Sie ein Zertifikat und ein privates Schlüsselpaar erstellt und verknüpft haben, binden Sie es an einen virtuellen Server.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Wählen Sie auf der Registerkarte Zertifikate unter **Verfügbar**ein Zertifikat aus, klicken Sie auf **Hinzufügen**und dann auf **OK**.

#### Binden Sie das Zertifikat und den privaten Schlüssel über die CLI an einen virtuellen Server

Geben Sie an der Eingabeaufforderung;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
   Mandatory | Optional )
<!--NeedCopy-->
```

**Beispiel:**

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
   ocspCheck Mandatory
<!--NeedCopy-->
```

**Hinweis:** OSCPCheck ist optional, wenn für das Gerätezertifikat keine OCSP-Prüfung erforderlich ist.

#### Entbinden von Testzertifikaten über die GUI vom virtuellen Server

Nachdem Sie das signierte Zertifikat installiert haben, lösen Sie die Bindung aller Testzertifikate, die an den virtuellen Server gebunden sind. Sie können Testzertifikate mithilfe des Konfigurationsdienstprogramms aufheben.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Wählen Sie auf der Registerkarte Zertifikate unter **Konfiguriert**das Testzertifikat aus, und klicken Sie dann auf **Entfernen**.

## Zwischenzertifikate konfigurieren

March 27, 2024

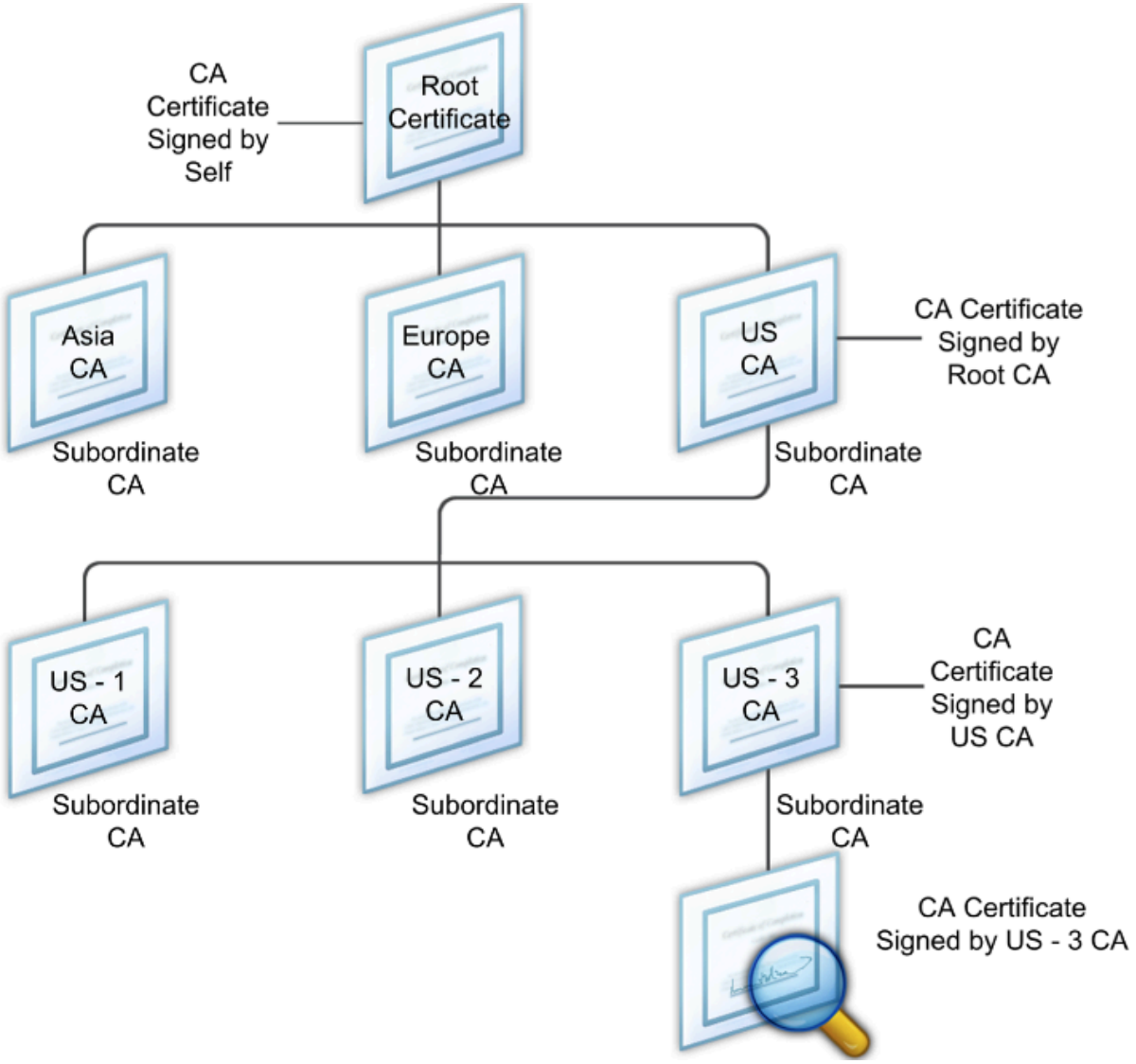
Ein Zwischenzertifikat ist ein Zertifikat, das zwischen Citrix Gateway (dem Serverzertifikat) und einem Stammzertifikat (auf dem Benutzergerät installiert) verläuft. Ein Zwischenzertifikat ist Teil einer Kette.

Einige Organisationen delegieren die Verantwortung für die Ausstellung von Zertifikaten, um das Problem der geografischen Trennung zwischen Organisationseinheiten zu lösen oder unterschiedliche Ausstellungsrichtlinien auf verschiedene Bereiche der Organisation anzuwenden.

Die Verantwortung für die Ausstellung von Zertifikaten kann durch die Einrichtung untergeordneter Zertifizierungsstellen (CAs) delegiert werden. Zertifizierungsstellen können ihre eigenen Zertifikate signieren (d. h. sie sind selbstsigniert) oder sie können von einer anderen Zertifizierungsstelle signiert werden. Der X.509-Standard beinhaltet ein Modell zum Einrichten einer Hierarchie von CAs. In diesem Modell befindet sich die Stamm-CA, wie in der folgenden Abbildung dargestellt, ganz oben in der Hierarchie und ist ein selbstsigniertes Zertifikat der Zertifizierungsstelle. Die CAs, die der Stamm-CA direkt untergeordnet sind, haben von der Stammzertifizierungsstelle signierte CA-Zertifikate. Zertifizierungsstellen unter den untergeordneten Zertifizierungsstellen in der Hierarchie lassen ihre CA-Zertifikate von den untergeordneten Zertifizierungsstellen signieren.

Abbildung 1. Das X.509-Modell zeigt die hierarchische Struktur einer typischen digitalen Zertifikatskette




Wenn ein Serverzertifikat von einer CA mit einem selbstsignierten Zertifikat signiert wird, besteht die Zertifikatskette aus genau zwei Zertifikaten: dem Entitätszertifikat und der Stammzertifizierungsstelle. Wenn ein Benutzer- oder Serverzertifikat von einer zwischengeschalteten Zertifizierungsstelle signiert wird, ist die Zertifikatskette länger.

Die folgende Abbildung zeigt, dass die ersten beiden Elemente das End-Entitätszertifikat (in diesem Fall gwy01.company.com) und das Zertifikat der zwischengeschalteten Zertifizierungsstelle in dieser Reihenfolge sind. Auf das Zertifikat der zwischengeschalteten Zertifizierungsstelle folgt das Zertifikat ihrer Zertifizierungsstelle. Diese Auflistung wird fortgesetzt, bis das letzte Zertifikat in der Liste für eine Stammzertifizierungsstelle gilt. Jedes Zertifikat in der Kette bestätigt die Identität des vorherigen Zertifikats.

Abbildung 2. Eine typische digitale Zertifikatskette


### Installieren Sie ein Zwischenzertifikat

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich SSL, und klicken Sie dann auf Zertifikate.
2. Klicken Sie im Detailbereich auf Installieren.
3. Geben Sie im Feld Name des Zertifikatsschlüsselpaars den Namen des Zertifikats ein.
4. Klicken Sie unter Details unter Certificate File Name auf Browse (Appliance) und wählen Sie in der Liste Local oder Appliance aus.
5. Navigieren Sie zum Zertifikat auf Ihrem Computer (lokal) oder auf Citrix Gateway (Appliance).
6. Wählen Sie im Zertifikatsformat PEM aus.
7. Klicken Sie auf Installieren und dann auf Schließen.

Wenn Sie ein Zwischenzertifikat auf Citrix Gateway installieren, müssen Sie weder den privaten Schlüssel noch ein Kennwort angeben.

Nachdem das Zertifikat auf der Appliance installiert wurde, muss das Zertifikat mit dem Serverzertifikat verknüpft werden.

### Verknüpfen eines Zwischenzertifikats mit einem Serverzertifikat

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich SSL, und klicken Sie dann auf Zertifikate.
2. Wählen Sie im Detailbereich das Serverzertifikat aus und klicken Sie dann unter Aktion auf Link.
3. Wählen Sie neben CA Certificate Name das Zwischenzertifikat aus der Liste aus und klicken Sie dann auf OK.

## Gerätezertifikate zur Authentifizierung verwenden

March 27, 2024

Citrix Gateway unterstützt die Überprüfung des Gerätezertifikats, mit der Sie die Geräte-Identität an den privaten Schlüssel eines Zertifikats binden können.  Die Gerätezertifikatsprüfung kann als Teil

klassischer oder erweiterter Endpoint Analysis (EPA) -Richtlinien konfiguriert werden. In klassischen EPA-Richtlinien kann das Gerätezertifikat nur für die Vorauthentifizierung von EPA konfiguriert werden.

Citrix Gateway überprüft das Gerätezertifikat, bevor der Endpoint Analysis-Scan ausgeführt wird oder bevor die Anmeldeseite angezeigt wird. Wenn Sie Endpoint Analysis konfigurieren, wird der Endpunkt-Scan ausgeführt, um das Benutzergerät zu überprüfen. Wenn das Gerät den Scan durchläuft und Citrix Gateway das Gerätezertifikat überprüft hat, können sich Benutzer dann am NetScaler Gateway anmelden.

> **Wichtig:**
>
> - Standardmäßig schreibt Windows Administratorrechte für den Zugriff auf Gerätezertifikate vor.
> - Um eine Gerätezertifikatsprüfung für Benutzer ohne Administratorrechte hinzuzufügen, müssen Sie das VPN-Plug-in installieren. Die VPN-Plug-In-Version muss dieselbe Version wie das EPA-Plug-In auf dem Gerät haben.
> - Sie können dem Gateway mehrere CA-Zertifikate hinzufügen und das Gerätezertifikat validieren.
> - Wenn Sie zwei oder mehr Gerätezertifikate auf Citrix Gateway installieren, müssen Benutzer das richtige Zertifikat auswählen, wenn sie sich bei Citrix Gateway anmelden oder bevor der Endpoint Analysis-Scan ausgeführt wird.
> - Wenn Sie das Gerätezertifikat erstellen, muss es sich um ein X.509-Zertifikat handeln.
> - Wenn Sie ein Gerätezertifikat haben, das von einer zwischengeschalteten CA ausgestellt wurde, müssen sowohl Zwischen- als auch Stamm-CA-Zertifikate gebunden sein.
> - Der EPA-Client benötigt den Benutzer lokale Administratorrechte, um auf den Maschinenzertifikatspeicher zugreifen zu können. Dies ist selten der Fall, daher besteht eine Problemumgehung darin, das vollständige NetScaler Gateway-Plug-In zu installieren, das auf den lokalen Speicher zugreifen kann.

Weitere Informationen zum Erstellen von Gerätezertifikaten finden Sie unter:

- Network Device Enrollment Service (NDES) in Active Directory-Zertifikatsdiensten (AD CS) auf der Microsoft-Website.
- So fordern Sie ein Zertifikat von einer Microsoft-Zertifizierungsstelle mithilfe von DCE/RPC und der Nutzdaten des Active Directory-Zertifikatprofils auf der Apple-Support-Website an.
- Ausstellung voniPad/iPhone-Zertifikaten im Microsoft-Support-Blog “Fragen Sie das Verzeichnisdienstteam”
- Einrichten des Netzwerkgeräte-Registrierungsdienstes auf der Windows IT Pro-Website.
- Beispiel für die schrittweise Bereitstellung der PKI-Zertifikate für Configuration Manager: Windows Server 2008-Zertifizierungsstelle auf der Microsoft System Center-Website.

### Schritte zum Konfigurieren von Gerätezertifikaten

Um ein Gerätezertifikat zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Installieren Sie das Zertifizierungsstellenzertifikat des Gerätezertifikatausstellers auf Citrix Gateway. Einzelheiten finden Sie unter Installieren des signierten Zertifikats auf Citrix Gateway.
- Binden Sie das Zertifikat der Zertifizierungsstelle des Gerätezertifikatausstellers an den virtuellen Citrix Gateway-Server und aktivieren Sie die OCSP-Prüfung. Einzelheiten finden Sie unter Installieren des signierten Zertifikats auf Citrix Gateway.
- Erstellen und binden Sie OCSP (Responder) auf dem Zertifikat der Zertifizierungsstelle des Gerätezertifikatausstellers. Einzelheiten finden Sie unter Überwachen des Zertifikatstatus mit OCSP.

Aktivieren Sie die Gerätezertifikatsprüfung auf dem virtuellen Server und fügen Sie das Zertifikat des Gerätezertifikatausstellers zur Checkliste für Gerätezertifikate hinzu. Einzelheiten finden Sie unter Aktivieren der Überprüfung von Gerätezertifikaten auf einem virtuellen Server für klassische EPA-Richtlinien.

Schließen Sie die clientseitige Konfiguration und Überprüfung des Gerätezertifikats auf dem Windows-Computer ab. Einzelheiten finden Sie unter Überprüfung des Gerätezertifikats auf einem Windows-Computer.

> **Hinweis:**
>
> Auf allen Clients, die das Gerätezertifikat EPA-Prüfung in Anspruch nehmen möchten, muss das Gerätezertifikat im Systemzertifikatspeicher des Computers installiert sein.

### Aktivieren der Gerätezertifikatsprüfung auf einem virtuellen Server für klassische EPA-Richtlinien

Nachdem Sie das Gerätezertifikat erstellt haben, installieren Sie das Zertifikat auf Citrix Gateway, indem Sie das Verfahren zum Importieren und Installieren eines vorhandenen Zertifikats in Citrix Gatewayverwenden.

1. Navigieren Sie auf der Registerkarte Konfiguration zu **Citrix Gateway > Virtuelle Server**.
2. Wählen Sie auf der Seite **Citrix Gateway Virtual Servers** einen vorhandenen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Virtuelle VPN-Server** im Abschnitt **Grundeinstellungen** auf **Bearbeiten**.
4. Deaktivieren Sie das Feld **Authentifizierung aktivieren**, um die Authentifizierung zu deaktivieren.
5. Wählen Sie das Feld **Gerätezertifikat** aktivieren, um das Gerätezertifikat

6. Klicken Sie auf **Hinzufügen**, um den Namen des CA-Zertifikats eines verfügbaren Gerätezertifikats zur Liste hinzuzufügen.
7. Um ein CA-Zertifikat an den virtuellen Server zu binden, klicken Sie im Abschnitt **CA for Device Certificateauf CA-Zertifikat**, klicken Sie auf**Hinzufügen**, wählen Sie das Zertifikat aus und klicken Sie dann auf**+**.

> **Hinweis:**
>
> Informationen zum Aktivieren und Binden von Gerätezertifikaten auf einem virtuellen Server für erweiterte EPA-Richtlinien finden Sie unter Gerätezertifikat in nFactor als EPA-Komponente.

### Überprüfung des Gerätezertifikats auf einem Windows-Computer

1. Öffnen Sie einen Browser und greifen Sie auf den Citrix Gateway FQDN zu.
2. Erlauben Sie dem Citrix End Point Analysis (EPA) -Client die Ausführung. Wenn noch nicht installiert, installieren Sie EPA.

   Citrix EPA führt das Gerätezertifikat aus und validiert es und leitet zur Authentifizierungsseite weiter, wenn die EPA-Prüfung des Gerätezertifikats erfolgreich ist, andernfalls werden Sie zur EPA-Fehlerseite weitergeleitet. Falls Sie andere EPA-Prüfungen haben, hängen die EPA-Scanergebnisse von den konfigurierten EPA-Prüfungen ab.

Überprüfen Sie zum weiteren Debuggen auf dem Client die folgenden EPA-Protokolle auf dem Client: C:\Users<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

**Hinweis:**

> Die Überprüfung des Gerätezertifikats mit CRL wird nicht unterstützt.

## Vorhandenes Zertifikat importieren und installieren

March 27, 2024

Sie können ein vorhandenes Zertifikat von einem Windows-basierten Computer mit Internetinformationsdiensten (IIS) oder von einem Computer importieren, auf dem Secure Gateway ausgeführt wird.

Achten Sie beim Exportieren des Zertifikats darauf, dass Sie auch den privaten Schlüssel exportieren. Manchmal können Sie den privaten Schlüssel nicht exportieren, was bedeutet, dass Sie das Zertifikat nicht auf Citrix Gateway installieren können. Verwenden Sie in diesem Fall die Certificate Signing Request (CSR), um ein Zertifikat zu erstellen. Einzelheiten finden Sie unter Erstellen einer Zertifikatsignieranforderung.

Wenn Sie ein Zertifikat und einen privaten Schlüssel aus Windows exportieren, erstellt der Computer eine Persönliche Informationsaustauschdatei (.pfx). Diese Datei wird dann auf Citrix Gateway als PKCS #12 -Zertifikat installiert.

Wenn Sie Secure Gateway durch Citrix Gateway ersetzen, können Sie das Zertifikat und den privaten Schlüssel vom Secure Gateway exportieren. Wenn Sie eine In-Place-Migration vom Secure Gateway zu Citrix Gateway durchführen, muss der vollqualifizierte Domänenname (FQDN) in der Anwendung und der Appliance identisch sein. Wenn Sie das Zertifikat vom Secure Gateway exportieren, setzen Sie das Secure Gateway sofort in den Ruhestand, installieren das Zertifikat auf Citrix Gateway und testen dann die Konfiguration. Secure Gateway und Citrix Gateway können nicht gleichzeitig in Ihrem Netzwerk ausgeführt werden, wenn sie denselben FQDN haben.

Wenn Sie Windows Server 2003 oder Windows Server 2008 verwenden, können Sie die Microsoft Management Console verwenden, um das Zertifikat zu exportieren. Weitere Informationen finden Sie in der Online-Hilfe von Windows.

Belassen Sie die Standardwerte für alle anderen Optionen, definieren Sie ein Kennwort und speichern Sie die PFX-Datei auf Ihrem Computer. Wenn das Zertifikat exportiert wird, installieren Sie es auf Citrix Gateway.

### So installieren Sie das Zertifikat und den privaten Schlüssel auf Citrix Gateway

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf **Citrix Gateway**.
2. Klicken Sie im Detailbereich unter Erste Schritte auf **Citrix Gateway-Assistent**.
3. Klicken Sie auf **Weiter**, wählen Sie einen vorhandenen virtuellen Server aus und klicken Sie dann auf **Weiter**.
4. Wählen Sie in den **Zertifikatsoptionen**die Option **Eine PKCS #12 -Datei (.pfx) installieren**aus.
5. Klicken Sie in **PKCS #12 File Name**auf **Durchsuchen**, navigieren Sie zum Zertifikat, und klicken Sie dann auf **Auswählen**.
6. Geben Sie in ((Kennwort)) das Kennwort für den privaten Schlüssel ein.

   Dies ist das Kennwort, das Sie bei der Konvertierung des Zertifikats in das PEM-Format verwendet haben.
7. Klicken Sie auf **Weiter**, um den Citrix Gateway-Assistenten zu beenden, ohne weitere Einstellungen zu ändern.

Wenn das Zertifikat auf Citrix Gateway installiert ist, wird das Zertifikat im Konfigurationsdienstprogramm im Knoten **SSL\ > Zertifikate** angezeigt.

**So erstellen Sie einen privaten Schlüssel**

1. Klicken Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich auf **SSL**.
2. Klicken Sie im Detailbereich unter **SSL-Schlüssel**auf **RSA-Schlüssel erstellen**.
3. Geben Sie unter**Key Filename**den Namen des privaten Schlüssels ein oder klicken Sie auf Durchsuchen, um zu einer vorhandenen Datei zu navigieren.
4. Geben Sie im**Feld Schlüsselgröße (Bits)**die Größe des privaten Schlüssels ein.
5. Wählen Sie unter**Public Exponent Value**F4 oder 3 aus.

   Der öffentliche Exponentenwert für den RSA-Schlüssel. Dies ist Teil des Verschlüsselungsalgorithmus und wird zum Erstellen des RSA-Schlüssels benötigt. Die Werte lauten F4 (Hex: 0x10001) oder 3 (Hex: 0x3). Die Standardeinstellung ist F4.
6. Wählen Sie im**Schlüsselformat**PEM oder DER aus.Citrix empfiehlt das PEM-Format für das Zertifikat.
7. Wählen Sie unter **PEM-Kodierungsalgorithmus**DES oder DES3 aus.
8. Geben Sie in**PEM Passphrase**und**Verify Passphrase**das Kennwort ein, klicken Sie auf **Erstellen**und dann auf **Schließen**.

   **Hinweis**: Um eine Passphrase zuzuweisen, muss das Schlüsselformat PEM sein und Sie müssen den Kodierungsalgorithmus auswählen.

Um einen privaten DSA-Schlüssel im Konfigurationsdienstprogramm zu**erstellen, klicken Sie auf DSA-Schlüssel** erstellen und befolgen Sie die Schritte zum Erstellen des privaten RSA-Schlüssels.

## Widerrufslisten für Zertifikate

March 27, 2024

Von Zeit zu Zeit stellen Zertifizierungsstellen (CAs) Zertifikatsperrlisten (CRLs) aus. CRLs enthalten Informationen über Zertifikate, denen nicht mehr vertraut werden kann. Angenommen, Ann verlässt die XYZ Corporation. Das Unternehmen kann Anns Zertifikat auf eine CRL legen, um zu verhindern, dass sie Nachrichten mit diesem Schlüssel signiert.

Ebenso können Sie ein Zertifikat widerrufen, wenn ein privater Schlüssel kompromittiert ist oder wenn dieses Zertifikat abgelaufen ist und ein neues verwendet wird. Bevor Sie einem öffentlichen Schlüssel vertrauen, stellen Sie sicher, dass das Zertifikat nicht in einer CRL angezeigt wird.

Citrix Gateway unterstützt die folgenden zwei CRL-Typen:

- CRLs, die die Zertifikate auflisten, die widerrufen wurden oder nicht mehr gültig sind
- Online Certificate Status Protocol (OSCP), ein Internetprotokoll, das zum Abrufen des Sperrstatus von X.509-Zertifikaten verwendet wird

**So fügen Sie eine CRL hinzu:**

Stellen Sie vor dem Konfigurieren der CRL auf dem Citrix Gateway-Gerät sicher, dass die CRL-Datei lokal auf dem Gerät gespeichert ist. Im Falle eines Hochverfügbarkeits-Setups muss die CRL-Datei auf beiden Citrix Gateway-Appliances vorhanden sein, und der Verzeichnispfad zur Datei muss auf beiden Appliances identisch sein.

Wenn Sie die CRL aktualisieren müssen, können Sie die folgenden Parameter verwenden:

- CRL-Name: Der Name der CRL, die auf dem Citrix ADC hinzugefügt wird. Maximal 31 Zeichen.
- CRL-Datei: Der Name der CRL-Datei, die auf dem Citrix ADC hinzugefügt wird. Der Citrix ADC sucht standardmäßig im Verzeichnis /var/netscaler/ssl nach der CRL-Datei. Maximal 63 Zeichen.
- URL: Maximal 127 Zeichen
- Basis-DN: Maximal 127 Zeichen
- Bind DN: Maximal 127 Zeichen
- Kennwort: Maximal 31 Zeichen
- Tage: Maximal 31

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration SSL und klicken Sie dann auf CRL.
2. Klicken Sie im Detailbereich auf "Hinzufügen".
3. Geben Sie im Dialogfeld CRL hinzufügen die Werte für Folgendes an:

    - CRL-Name
    - CRL Datei
    - Format (optional)
    - CA-Zertifikat (optional)

4. Klicken Sie auf **Create** und dann auf **Close**. Wählen Sie im Bereich CRL-Details die CRL aus, die Sie konfiguriert haben, und überprüfen Sie, ob die Einstellungen am unteren Bildschirmrand korrekt sind.

**So konfigurieren Sie CRL Autorefresh mithilfe von LDAP oder HTTP in der GUI:**

Eine CRL wird regelmäßig oder manchmal unmittelbar nach dem Widerruf eines bestimmten Zertifikats von einer CA generiert und veröffentlicht. Citrix empfiehlt, CRLs auf der Citrix Gateway-Appliance regelmäßig zu aktualisieren, um vor Clients zu schützen, die versuchen, eine Verbindung mit ungültigen Zertifikaten herzustellen.

Das Citrix Gateway-Gerät kann CRLs von einem Webspeicherort oder einem LDAP-Verzeichnis aus aktualisieren. Wenn Sie Aktualisierungsparameter und einen Webspeicherort oder einen LDAP-Server

angeben, muss die CRL zum Zeitpunkt der Ausführung des Befehls nicht auf dem lokalen Festplattenlaufwerk vorhanden sein. Bei der ersten Aktualisierung wird eine Kopie auf dem lokalen Festplattenlaufwerk in dem durch den Parameter CRL File angegebenen Pfad gespeichert. Der Standardpfad zum Speichern der CRL lautet /var/netscaler/ssl.

### CRL-Aktualisierungsparameter

- **CRL-Name**

  Der Name der CRL, die auf dem Citrix Gateway aktualisiert wird.

- **Aktivieren Sie die automatische Aktualisierung von CRL**

  Aktivieren oder deaktivieren Sie die automatische Aktualisierung von CRL.

- **CA-Zertifikat**

  Das Zertifikat der CA, die die CRL ausgestellt hat. Dieses CA-Zertifikat muss auf der Appliance installiert sein. Der Citrix ADC kann CRLs nur von CAs aktualisieren, deren Zertifikate darauf installiert sind.

- **Methode**

  Protokoll, in dem die CRL-Aktualisierung von einem Webserver (HTTP) oder einem LDAP-Server abgerufen werden soll. Mögliche Werte: HTTP, LDAP. Standard: HTTP.

- **Geltungsbereich**

  Das Ausmaß des Suchvorgangs auf dem LDAP-Server. Wenn der angegebene Bereich Base ist, erfolgt die Suche auf derselben Ebene wie der Basis-DN. Wenn der angegebene Bereich Eins ist, erstreckt sich die Suche auf eine Ebene unter dem Basis-DN.

- **Server-IP**

  Die IP-Adresse des LDAP-Servers, von dem die CRL abgerufen wird. Wählen Sie IPv6 aus, um eine IPv6-IP-Adresse zu verwenden.

- **Port**

  Die Portnummer, auf der der LDAP oder der HTTP-Server kommuniziert.

- **URL**

  Die URL für den Webstandort, von dem die CRL abgerufen wird.

- **Basis-DN**

  Der Basis-DN, der vom LDAP-Server für die Suche nach dem CRL-Attribut verwendet wird. Hinweis: Citrix empfiehlt, das Basis-DN-Attribut anstelle des Ausstellernamens aus dem CA-Zertifikat zu verwenden, um im LDAP-Server nach der CRL zu suchen. Das Feld "Ausstellername" stimmt möglicherweise nicht genau mit dem DN der LDAP-Verzeichnisstruktur überein.

- **Bind DN**

  Das bind-DN-Attribut wird verwendet, um auf das CRL-Objekt im LDAP-Repository zuzugreifen. Die Bind-DN-Attribute sind die Administratoranmeldeinformationen für den LDAP-Server. Konfigurieren Sie diesen Parameter, um den unbefugten Zugriff auf die LDAP-Server einzuschränken.

- **Kennwort**

  Das Administratorkennwort, das für den Zugriff auf das CRL-Objekt im LDAP-Repository verwendet wurde. Ein Kennwort ist erforderlich, wenn der Zugriff auf das LDAP-Repository eingeschränkt ist, das heißt, anonymer Zugriff ist nicht zulässig.

- **Intervall**

  Das Intervall, in dem die CRL-Aktualisierung durchgeführt werden muss. Geben Sie für eine sofortige CRL-Aktualisierung das Intervall als NOW an. Mögliche Werte: MONTHLY, DAILY, WEEKLY, NOW, NONE.

- **Tage**

  Der Tag, an dem die CRL-Aktualisierung durchgeführt werden muss. Die Option ist nicht verfügbar, wenn das Intervall auf DAILY eingestellt ist.

- **Zeit**

  Die genaue Uhrzeit im 24-Stunden-Format, zu der die CRL-Aktualisierung durchgeführt werden muss.

- **Binär**

  Stellen Sie den LDAP-basierten CRL-Abrufmodus auf binär ein. Mögliche Werte: YES, NO. Standard: NEIN.

1. Erweitern Sie im Navigationsbereich SSL und klicken Sie dann auf CRL.
2. Wählen Sie die konfigurierte CRL aus, für die Sie Aktualisierungsparameter aktualisieren möchten, und klicken Sie dann auf Öffnen.
3. Wählen Sie die Option "CRL Auto Refresh aktivieren".
4. Geben Sie in der Gruppe CRL Auto Refresh Parameters Werte für die folgenden Parameter an:
   Hinweis: Ein Sternchen (*) zeigt einen erforderlichen Parameter an.

   - Methode
   - Binär
   - Geltungsbereich
   - Server-IP
   - Port*
   - URL
   - Base DN*

- Bind DN
- Kennwort
- Intervall
- Tage
- Zeit

5. Klicken Sie auf Erstellen. Wählen Sie im CRL-Bereich die CRL aus, die Sie konfiguriert haben, und überprüfen Sie, ob die Einstellungen am unteren Bildschirmrand korrekt sind.

## Zertifikatsstatus mit OCSP überwachen

Online Certificate Status Protocol (OCSP) ist ein Internetprotokoll, das verwendet wird, um den Status eines Client-SSL-Zertifikats zu ermitteln. Citrix Gateway unterstützt OCSP wie in RFC 2560 definiert. OCSP bietet erhebliche Vorteile gegenüber Zertifikatsperrlisten (CRLs) in Bezug auf zeitnahe Informationen. Der aktuelle Widerrufsstatus eines Kundenzertifikats ist besonders nützlich bei Transaktionen mit hohen Geldsummen und hochwertigen Aktiengeschäften. Es verbraucht auch weniger System- und Netzwerkressourcen. Die Citrix Gateway-Implementierung von OCSP umfasst Anforderungs-Batching und Antwort-Caching.

### Citrix Gateway-Implementierung von OCSP

Die OCSP-Validierung auf einem Citrix Gateway-Gerät beginnt, wenn Citrix Gateway während eines SSL-Handshakes ein Clientzertifikat erhält. Um das Zertifikat zu validieren, erstellt Citrix Gateway eine OCSP-Anforderung und leitet sie an den OCSP-Responder weiter. Dazu extrahiert Citrix Gateway entweder die URL für den OCSP-Responder aus dem Clientzertifikat oder verwendet eine lokal konfigurierte URL. Die Transaktion befindet sich in einem angehaltenen Zustand, bis Citrix Gateway die Antwort des Servers auswertet und feststellt, ob die Transaktion zugelassen oder abgelehnt werden soll. Wenn sich die Antwort des Servers über die konfigurierte Zeit hinaus verzögert und keine anderen Responder konfiguriert sind, lässt Citrix Gateway die Transaktion zu oder zeigt einen Fehler an, je nachdem, ob Sie die OCSP-Prüfung auf optional oder obligatorisch festlegen. Citrix Gateway unterstützt das Stapeln von OCSP-Anfragen und das Zwischenspeichern von OCSP-Antworten, um die Belastung des OCSP-Responders zu reduzieren und schnellere Antworten zu ermöglichen.

### OCSP-Anforderungs-Batching

Jedes Mal, wenn Citrix Gateway ein Clientzertifikat erhält, sendet es eine Anfrage an den OCSP-Responder. Um eine Überlastung des OCSP-Responders zu vermeiden, kann Citrix Gateway den Status von mehr als einem Clientzertifikat in derselben Anforderung abfragen. Damit das Anforderungsbatching effizient funktioniert, müssen Sie ein Timeout definieren, damit die Verarbeitung eines einzelnen Zertifikats nicht verzögert wird, während Sie auf die Bildung eines Stapels warten.

#### OCSP-Antwort-Caching

Das Zwischenspeichern der vom OCSP-Responder empfangenen Antworten ermöglicht schnellere Antworten auf den Benutzer und reduziert die Belastung des OCSP-Responders. Nach Erhalt des Sperrstatus eines Clientzertifikats vom OCSP-Responder speichert Citrix Gateway die Antwort lokal für eine vordefinierte Zeitspanne. Wenn ein Clientzertifikat während eines SSL-Handshakes empfangen wird, überprüft Citrix Gateway zunächst seinen lokalen Cache auf einen Eintrag für dieses Zertifikat. Wenn ein Eintrag gefunden wird, der noch gültig ist (innerhalb des Cache-Timeout-Limits), wird der Eintrag ausgewertet und das Clientzertifikat wird akzeptiert oder abgelehnt. Wenn ein Zertifikat nicht gefunden wird, sendet Citrix Gateway eine Anforderung an den OCSP-Responder und speichert die Antwort für eine konfigurierte Zeitspanne in seinem lokalen Cache.

## Konfigurieren des OCSP-Zertifikats

Das Konfigurieren eines Online Certificate Status Protocol (OCSP) umfasst das Hinzufügen eines OCSP-Responders, das Binden des OCSP-Responders an ein signiertes Zertifikat von einer Certificate Authority (CA) und das Binden des Zertifikats und des privaten Schlüssels an einen virtuellen Secure Sockets Layer (SSL) -Server. Wenn Sie ein anderes Zertifikat und einen anderen privaten Schlüssel an einen bereits konfigurierten OCSP-Responder binden müssen, müssen Sie zuerst den Responder lösen und dann den Responder an ein anderes Zertifikat binden.

#### So konfigurieren Sie OCSP

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich SSL, und klicken Sie dann auf OCSP-Responder.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Feld Name einen Namen für das Profil ein.
4. Geben Sie unter URL die Webadresse des OCSP-Responders ein.

   Dieses Feld ist obligatorisch. Die Webadresse darf 32 Zeichen nicht überschreiten.
5. Um die OCSP-Antworten zwischenzuspeichern, klicken Sie auf Cache und geben Sie unter Timeout die Anzahl der Minuten ein, die Citrix Gateway die Antwort enthält.
6. Klicken Sie unter Batching anfordern auf Aktivieren.
7. Geben Sie in Batching Delay die Zeit in Millisekunden an, die für das Stapeln einer Gruppe von OCSP-Anfragen zulässig ist.

   Die Werte können zwischen 0 und 10000 liegen. Der Standardwert ist 1.

8. Geben Sie unter Produziert zur Zeitverzerrung ein, wie viel Zeit Citrix Gateway verwenden kann, wenn das Gerät die Antwort prüfen oder akzeptieren muss.
9. Wählen Sie unter Reaktionsüberprüfung Vertrauensantworten aus, wenn Sie Signaturprüfungen durch den OCSP-Responder deaktivieren möchten.

   Wenn Sie Trust Responses aktivieren, überspringen Sie Schritt 8 und Schritt 9.
10. Wählen Sie unter Certificate das Zertifikat aus, das zum Signieren der OCSP-Antworten verwendet wird.

    Wenn kein Zertifikat ausgewählt ist, wird die CA, an die der OCSP-Responder gebunden ist, zur Überprüfung der Antworten verwendet.
11. Geben Sie unter Request Timeout die Anzahl der Millisekunden ein, um auf eine OCSP-Antwort zu warten.

    Diese Zeit beinhaltet die Batching Delay-Zeit. Die Werte können zwischen 0 und 120000 liegen. Die Standardeinstellung ist 2000.
12. Wählen Sie unter Signaturzertifikat das Zertifikat und den privaten Schlüssel aus, mit denen OCSP-Anfragen signiert werden. Wenn Sie kein Zertifikat und keinen privaten Schlüssel angeben, werden die Anfragen nicht signiert.
13. Um die einmal verwendete Nummer zu aktivieren (`nonce`)`extension`, wählen Sie Nonce aus.
14. Um ein Clientzertifikat zu verwenden, klicken Sie auf Clientzertifikat einfügen
15. Klicken Sie auf Create und dann auf Close.

## Citrix Gateway-Konfigurationseinstellungen verwalten

March 27, 2024

Wenn Sie Konfigurationsänderungen an Citrix Gateway vornehmen, werden die Änderungen in Protokolldateien gespeichert. Sie können verschiedene Arten von Konfigurationseinstellungen anzeigen:

- Gespeicherte Konfiguration. Sie können die Einstellungen anzeigen, die Sie auf Citrix Gateway gespeichert haben.
- Laufende Konfiguration. Sie können aktive Einstellungen wie einen virtuellen Server oder eine Authentifizierungsrichtlinie anzeigen, die Sie konfiguriert, aber nicht als gespeicherte Konfiguration in Citrix Gateway gespeichert haben.

- Laufende versus gespeicherte Konfiguration. Sie können die laufende und gespeicherte Konfiguration auf Citrix Gateway nebeneinander vergleichen.

Sie können auch die Konfigurationseinstellungen auf Citrix Gateway löschen.

Wichtig: Wenn Sie Einstellungen auf Citrix Gateway löschen, werden Zertifikate, virtuelle Server und Richtlinien entfernt. Citrix empfiehlt, die Konfiguration nicht zu löschen.

## Speichern Sie die Citrix Gateway-Konfiguration

Sie können Ihre aktuelle Konfiguration auf Citrix Gateway auf einem Computer in Ihrem Netzwerk speichern, die aktuell ausgeführte Konfiguration anzeigen und die gespeicherten und ausgeführten Konfigurationen vergleichen.

### So speichern Sie die Konfiguration auf Citrix Gateway

1. Klicken Sie im Konfigurationsdienstprogramm über dem Detailbereich auf das Symbol Speichern und dann auf Ja.

### So zeigen Sie die Konfigurationsdatei auf Citrix Gateway an und speichern sie

Bei der gespeicherten Konfiguration handelt es sich um die Einstellungen, die in einer Protokolldatei auf Citrix Gateway gespeichert werden, z. B. Einstellungen für virtuelle Server, Richtlinien, IP-Adressen, Benutzer, Gruppen und Zertifikate.

Wenn Sie Einstellungen auf Citrix Gateway konfigurieren, können Sie die Einstellungen in einer Datei auf Ihrem Computer speichern. Wenn Sie die Citrix Gateway-Software neu installieren müssen oder versehentlich einige Einstellungen entfernen, können Sie diese Datei verwenden, um Ihre Konfiguration wiederherzustellen. Wenn Sie die Einstellungen wiederherstellen müssen, können Sie die Datei auf Citrix Gateway kopieren und das Gerät mithilfe der Befehlszeilenschnittstelle oder eines Programms wie WinSCP neu starten, um die Datei auf Citrix Gateway zu kopieren.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich System, und klicken Sie dann auf Diagnose.
2. Klicken Sie im Detailbereich unter Konfiguration anzeigen auf Gespeicherte Konfiguration.
3. Klicken Sie im Dialogfeld Gespeicherte Konfiguration auf Ausgabetext in einer Datei speichern, benennen Sie die Datei und klicken Sie dann auf Speichern.
   Hinweis: Citrix empfiehlt, die Datei unter dem Dateinamen ns.conf zu speichern.

#### So zeigen Sie die aktuelle laufende Konfiguration an

Alle Änderungen an Citrix Gateway, die ohne den Versuch, sie zu speichern, erfolgen, werden als laufende Konfiguration bezeichnet. Diese Einstellungen sind auf Citrix Gateway aktiv, werden jedoch nicht auf dem Gerät gespeichert. Wenn Sie zusätzliche Einstellungen wie eine Richtlinie, einen virtuellen Server, Benutzer oder Gruppen konfiguriert haben, können Sie diese Einstellungen in der laufenden Konfiguration anzeigen.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich System, und klicken Sie dann auf Diagnose.
2. Klicken Sie im Detailbereich unter Konfiguration anzeigen auf Konfiguration ausführen.

#### So vergleichen Sie die gespeicherte und laufende Konfiguration

Sie können sehen, welche Einstellungen auf der Appliance gespeichert sind, und diese Einstellungen mit der laufenden Konfiguration vergleichen. Sie können die laufende Konfiguration speichern oder Änderungen an der Konfiguration vornehmen.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich System, und klicken Sie dann auf Diagnose.
2. Klicken Sie im Detailbereich unter Konfiguration anzeigen auf Gespeichert v/s ausgeführt.

### Löschen Sie die Citrix Gateway-Konfiguration

Sie können die Konfigurationseinstellungen auf Citrix Gateway löschen. Sie können aus den folgenden drei Einstellungsebenen wählen, um sie zu löschen:

Wichtig: Citrix empfiehlt, Ihre Konfiguration zu speichern, bevor Sie die Citrix Gateway-Konfigurationseinstellungen löschen.

- Grundlegend. Löscht alle Einstellungen auf der Appliance mit Ausnahme der System-IP-Adresse, des Standard-Gateways, zugeordneten IP-Adressen, Subnetz-IP-Adressen, DNS-Einstellungen, Netzwerkeinstellungen, Hochverfügbarkeitseinstellungen, Administratorkennwort sowie Feature- und Moduseinstellungen.
- Verlängert. Löscht alle Einstellungen mit Ausnahme der System-IP-Adresse, zugeordneten IP-Adressen, Subnetz-IP-Adressen, DNS-Einstellungen und Hochverfügbarkeitsdefinitionen.
- Voll. Stellt die Konfiguration auf die ursprünglichen Werkseinstellungen zurück, mit Ausnahme der System-IP-Adresse (NSIP) und der Standardroute, die zur Aufrechterhaltung der Netzwerkkonnektivität zur Appliance erforderlich sind.

Wenn Sie die Konfiguration ganz oder teilweise löschen, werden die Funktionseinstellungen auf die werkseitigen Standardeinstellungen eingestellt.

Wenn Sie die Konfiguration löschen, werden Dateien, die auf Citrix Gateway gespeichert sind, wie Zertifikate und Lizenzen, nicht entfernt. Die Datei ns.conf wird nicht geändert. Wenn Sie die Konfiguration speichern möchten, bevor Sie die Konfiguration löschen, speichern Sie die Konfiguration zuerst auf Ihrem Computer. Wenn Sie die Konfiguration speichern, können Sie die Datei ns.conf auf Citrix Gateway wiederherstellen. Nachdem Sie die Datei auf der Appliance wiederhergestellt und Citrix Gateway neu gestartet haben, werden alle Konfigurationseinstellungen in ns.conf wiederhergestellt.

Änderungen an Konfigurationsdateien wie rc.conf werden nicht rückgängig gemacht.

Wenn Sie über ein Hochverfügbarkeitspaar verfügen, werden beide Citrix Gateway-Appliances identisch geändert. Wenn Sie beispielsweise die Grundkonfiguration auf einer Appliance löschen, werden die Änderungen an die zweite Appliance weitergegeben.

**So löschen Sie Citrix Gateway-Konfigurationseinstellungen**

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich System, und klicken Sie dann auf Diagnose.
2. Klicken Sie im Detailbereich unter Wartung auf Konfiguration löschen.
3. Wählen Sie unter Konfigurationsebene die Ebene aus, die Sie löschen möchten, und klicken Sie dann auf Ausführen.

## Zertifikatsverwaltung auf Citrix Gateway

March 27, 2024

Auf Citrix Gateway verwenden Sie Zertifikate, um sichere Verbindungen herzustellen und Benutzer zu authentifizieren.

Um eine sichere Verbindung herzustellen, ist an einem Ende der Verbindung ein Serverzertifikat erforderlich. Am anderen Ende der Verbindung ist ein Stammzertifikat der Certificate Authority (CA) erforderlich, die das Serverzertifikat ausgestellt hat.

- Serverzertifikat. Ein Serverzertifikat bescheinigt die Identität des Servers. Citrix Gateway erfordert diese Art von digitalem Zertifikat.
- Root-Zertifikat. Ein Stammzertifikat dient zur Identifizierung der Zertifizierungsstelle, die das Serverzertifikat signiert hat. Das Stammzertifikat gehört der Certificate Authority. Ein Benutzergerät benötigt diese Art von digitalem Zertifikat, um das Serverzertifikat zu überprüfen.

Beim Herstellen einer sicheren Verbindung mit einem Webbrowser auf dem Benutzergerät sendet der Server sein Zertifikat an das Gerät.

Wenn das Benutzergerät ein Serverzertifikat erhält, prüft der Webbrowser wie Internet Explorer, welche CA das Zertifikat ausgestellt hat und ob das Benutzergerät der CA vertraut. Wenn der CA nicht vertraut wird oder wenn es sich um ein Testzertifikat handelt, fordert der Webbrowser den Benutzer auf, das Zertifikat zu akzeptieren oder abzulehnen (die Möglichkeit, auf die Website zuzugreifen, effektiv zu akzeptieren oder abzulehnen).

Citrix Gateway unterstützt die folgenden drei Arten von Zertifikaten:

- Ein Testzertifikat, das an einen virtuellen Server gebunden ist und auch für Verbindungen zu einer Serverfarm verwendet werden kann. Citrix Gateway wird mit einem vorinstallierten Testzertifikat geliefert.
- Ein Zertifikat im PEM- oder DER-Format, das von einer CA signiert und mit einem privaten Schlüssel gekoppelt ist.
- Ein Zertifikat im Format PKCS #12, das zum Speichern oder Transportieren des Zertifikats und des privaten Schlüssels verwendet wird. Das PKCS #12 -Zertifikat wird normalerweise aus einem vorhandenen Windows-Zertifikat als PFX-Datei exportiert und dann auf Citrix Gateway installiert.

Citrix empfiehlt die Verwendung eines Zertifikats, das von einer vertrauenswürdigen Zertifizierungsstelle wie Thawte oder Verisign signiert wurde.

## Zertifikatsignieranforderung erstellen

March 27, 2024

Um sichere Kommunikation über SSL oder TLS bereitzustellen, ist ein Serverzertifikat auf Citrix Gateway erforderlich. Bevor Sie ein Zertifikat auf Citrix Gateway hochladen können, müssen Sie eine Certificate Signing Request (CSR) und einen privaten Schlüssel generieren. Sie verwenden die im Citrix Gateway-Assistenten enthaltene Zertifikatsanforderung erstellen oder das Konfigurationsdienstprogramm, um die CSR zu erstellen. Die Zertifikatsanforderung erstellen erstellt eine CSR-Datei, die zur Signatur per E-Mail an die Zertifizierungsstelle (CA) gesendet wird, und einen privaten Schlüssel, der auf der Appliance verbleibt. Die CA signiert das Zertifikat und sendet es an die von Ihnen angegebene E-Mail-Adresse an Sie zurück. Wenn Sie das signierte Zertifikat erhalten, können Sie es auf Citrix Gateway installieren. Wenn Sie das Zertifikat von der CA zurückerhalten, koppeln Sie das Zertifikat mit dem privaten Schlüssel.

Wichtig: Wenn Sie den Citrix Gateway-Assistenten zum Erstellen der CSR verwenden, müssen Sie den Assistenten beenden und warten, bis die CA Ihnen das signierte Zertifikat sendet. Wenn Sie das Zertifikat erhalten, können Sie den Citrix Gateway-Assistenten erneut ausführen, um die Einstellungen zu erstellen und das Zertifikat zu installieren. Weitere Informationen zum Citrix Gateway-Assistenten

finden Sie unter
Konfigurieren von Einstellungen mithilfe des Citrix Gateway-Assistenten.

### Erstellen einer CSR mithilfe des Citrix Gateway-Assistenten

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf **Citrix ADC Gateway**.
2. Klicken Sie im Detailbereich unter Erste Schritte auf **Citrix ADC Gateway** Wizard.
3. Folgen Sie den Anweisungen des Assistenten, bis Sie zur Seite Serverzertifikat angeben gelangen.
4. Klicken Sie auf **Erstellen einer Zertifikatsignieranforderung** und füllen Sie die Felder aus. Hinweis: Der vollqualifizierte Domänenname (FQDN) muss nicht mit dem Citrix Gateway-Hostnamen übereinstimmen. Der FQDN wird für die Benutzeranmeldung verwendet.
5. Klicken Sie auf **Erstellen**, um das Zertifikat auf Ihrem Computer zu speichern, und klicken Sie dann auf **Schließen**.
6. Beenden Sie den Citrix Gateway Assistenten, ohne Ihre Einstellungen zu speichern.

### Erstellen Sie eine CSR mithilfe der Citrix ADC GUI

Sie können auch die Citrix ADC GUI verwenden, um eine CSR zu erstellen, ohne den Citrix Gateway-Assistenten auszuführen.

1. Navigieren Sie zu **Traffic Management** > **SSL > SSL-Dateien** und wählen Sie**Certificate Signing Request (CSR) erstellen**.
2. Füllen Sie die Einstellungen für das Zertifikat aus und klicken Sie dann auf **Erstellen**.

Nachdem Sie das Zertifikat und den privaten Schlüssel erstellt haben, senden Sie das Zertifikat per E-Mail an die CA wie Thawte oder Verisign.

Ausführliche Vorgehensweise finden Sie unter Erstellen einer Zertifikatsignieranforderung.

### Installieren Sie das signierte Zertifikat auf Citrix Gateway

Wenn Sie das signierte Zertifikat von der Certificate Authority (CA) erhalten, koppeln Sie es mit dem privaten Schlüssel auf dem Gerät und installieren Sie das Zertifikat dann auf Citrix Gateway.

#### Koppeln Sie das signierte Zertifikat über die GUI mit einem privaten Schlüssel

1. Kopieren Sie das Zertifikat mithilfe eines Secure Shell (SSH) -Programms wie WinSCP nach Citrix Gateway in den Ordner nsconfig/ssl.

2. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **SSL > Zertifikate**.
3. Klicken Sie auf der Seite **SSL-Zertifikat** auf **Erste Schritte**.
4. Klicken Sie im Detailbereich auf **Installieren**.
5. Geben Sie im Feld **Name des Zertifikatsschlüsselpaars** den Namen des Zertifikats ein.
6. Klicken Sie unter **Zertifikatsdateiname**auf **Appliance**
7. Navigieren Sie zum Zertifikat, klicken **Sie auf Auswählen**und dann auf **Öffnen**.
8. Klicken Sie unter **Schlüsseldateiname**auf **Appliance**. Der Name des privaten Schlüssels entspricht dem Namen der Certificate Signing Request (CSR). Der private Schlüssel befindet sich auf Citrix Gateway im Verzeichnis\ nsconfig\ ssl.
9. Wählen Sie den privaten Schlüssel aus und klicken Sie dann auf **Öffnen**.
10. Wenn das Zertifikat im PEM-Format ist, geben Sie unter **Passwort das Passwort**für den privaten Schlüssel ein.
11. Wenn Sie eine Benachrichtigung für den Ablauf des Zertifikats konfigurieren möchten, wählen Sie **Bei Ablauf benachrichtigen**.
12. Geben Sie im **Feld Benachrichtigungszeitraum**die Anzahl der Tage ein, klicken Sie auf **Erstellen**und dann auf **Schließen**.

#### Binden Sie das Zertifikat und den privaten Schlüssel über die GUI an einen virtuellen Server

Nachdem Sie ein Zertifikat und ein privates Schlüsselpaar erstellt und verknüpft haben, binden Sie es an einen virtuellen Server.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Wählen Sie auf der Registerkarte Zertifikate unter **Verfügbar**ein Zertifikat aus, klicken Sie auf **Hinzufügen**und dann auf **OK**.

#### Binden Sie das Zertifikat und den privaten Schlüssel über die CLI an einen virtuellen Server

Geben Sie an der Eingabeaufforderung;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
   Mandatory | Optional )
<!--NeedCopy-->
```

**Beispiel:**

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
   ocspCheck Mandatory
<!--NeedCopy-->
```

**Hinweis:** OSCPCheck ist optional, wenn für das Gerätezertifikat keine OCSP-Prüfung erforderlich ist.

#### Entbinden von Testzertifikaten über die GUI vom virtuellen Server

Nachdem Sie das signierte Zertifikat installiert haben, lösen Sie die Bindung aller Testzertifikate, die an den virtuellen Server gebunden sind. Sie können Testzertifikate mithilfe des Konfigurationsdienstprogramms aufheben.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Wählen Sie auf der Registerkarte Zertifikate unter **Konfiguriert**das Testzertifikat aus, und klicken Sie dann auf **Entfernen**.

## Zwischenzertifikate konfigurieren

March 27, 2024

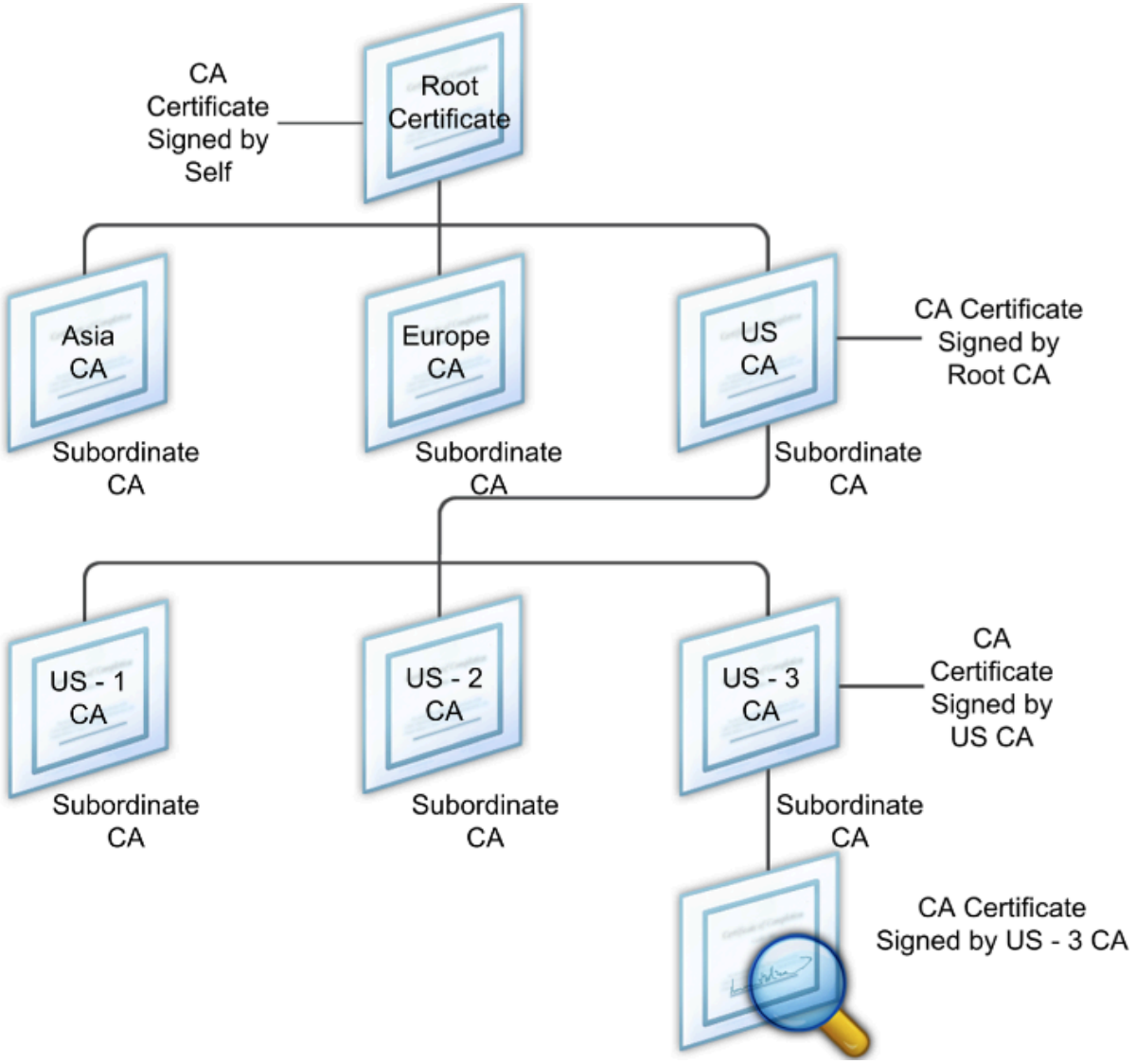
Ein Zwischenzertifikat ist ein Zertifikat, das zwischen Citrix Gateway (dem Serverzertifikat) und einem Stammzertifikat (auf dem Benutzergerät installiert) verläuft. Ein Zwischenzertifikat ist Teil einer Kette.

Einige Organisationen delegieren die Verantwortung für die Ausstellung von Zertifikaten, um das Problem der geografischen Trennung zwischen Organisationseinheiten zu lösen oder unterschiedliche Ausstellungsrichtlinien auf verschiedene Bereiche der Organisation anzuwenden.

Die Verantwortung für die Ausstellung von Zertifikaten kann durch die Einrichtung untergeordneter Zertifizierungsstellen (CAs) delegiert werden. Zertifizierungsstellen können ihre eigenen Zertifikate signieren (d. h. sie sind selbstsigniert) oder sie können von einer anderen Zertifizierungsstelle signiert werden. Der X.509-Standard beinhaltet ein Modell zum Einrichten einer Hierarchie von CAs. In diesem Modell befindet sich die Stamm-CA, wie in der folgenden Abbildung dargestellt, ganz oben in der Hierarchie und ist ein selbstsigniertes Zertifikat der Zertifizierungsstelle. Die CAs, die der Stamm-CA direkt untergeordnet sind, haben von der Stammzertifizierungsstelle signierte CA-Zertifikate. Zertifizierungsstellen unter den untergeordneten Zertifizierungsstellen in der Hierarchie lassen ihre CA-Zertifikate von den untergeordneten Zertifizierungsstellen signieren.

Abbildung 1. Das X.509-Modell zeigt die hierarchische Struktur einer typischen digitalen Zertifikatskette




Wenn ein Serverzertifikat von einer CA mit einem selbstsignierten Zertifikat signiert wird, besteht die Zertifikatskette aus genau zwei Zertifikaten: dem Entitätszertifikat und der Stammzertifizierungsstelle. Wenn ein Benutzer- oder Serverzertifikat von einer zwischengeschalteten Zertifizierungsstelle signiert wird, ist die Zertifikatskette länger.

Die folgende Abbildung zeigt, dass die ersten beiden Elemente das End-Entitätszertifikat (in diesem Fall gwy01.company.com) und das Zertifikat der zwischengeschalteten Zertifizierungsstelle in dieser Reihenfolge sind. Auf das Zertifikat der zwischengeschalteten Zertifizierungsstelle folgt das Zertifikat ihrer Zertifizierungsstelle. Diese Auflistung wird fortgesetzt, bis das letzte Zertifikat in der Liste für eine Stammzertifizierungsstelle gilt. Jedes Zertifikat in der Kette bestätigt die Identität des vorherigen Zertifikats.

Abbildung 2. Eine typische digitale Zertifikatskette


### Installieren Sie ein Zwischenzertifikat

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich SSL, und klicken Sie dann auf Zertifikate.
2. Klicken Sie im Detailbereich auf Installieren.
3. Geben Sie im Feld Name des Zertifikatsschlüsselpaars den Namen des Zertifikats ein.
4. Klicken Sie unter Details unter Certificate File Name auf Browse (Appliance) und wählen Sie in der Liste Local oder Appliance aus.
5. Navigieren Sie zum Zertifikat auf Ihrem Computer (lokal) oder auf Citrix Gateway (Appliance).
6. Wählen Sie im Zertifikatsformat PEM aus.
7. Klicken Sie auf Installieren und dann auf Schließen.

Wenn Sie ein Zwischenzertifikat auf Citrix Gateway installieren, müssen Sie weder den privaten Schlüssel noch ein Kennwort angeben.

Nachdem das Zertifikat auf der Appliance installiert wurde, muss das Zertifikat mit dem Serverzertifikat verknüpft werden.

### Verknüpfen eines Zwischenzertifikats mit einem Serverzertifikat

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich SSL, und klicken Sie dann auf Zertifikate.
2. Wählen Sie im Detailbereich das Serverzertifikat aus und klicken Sie dann unter Aktion auf Link.
3. Wählen Sie neben CA Certificate Name das Zwischenzertifikat aus der Liste aus und klicken Sie dann auf OK.

## Gerätezertifikate zur Authentifizierung verwenden

March 27, 2024

Citrix Gateway unterstützt die Überprüfung des Gerätezertifikats, mit der Sie die Geräte-Identität an den privaten Schlüssel eines Zertifikats binden können.  Die Gerätezertifikatsprüfung kann als Teil

klassischer oder erweiterter Endpoint Analysis (EPA) -Richtlinien konfiguriert werden. In klassischen EPA-Richtlinien kann das Gerätezertifikat nur für die Vorauthentifizierung von EPA konfiguriert werden.

Citrix Gateway überprüft das Gerätezertifikat, bevor der Endpoint Analysis-Scan ausgeführt wird oder bevor die Anmeldeseite angezeigt wird. Wenn Sie Endpoint Analysis konfigurieren, wird der Endpunkt-Scan ausgeführt, um das Benutzergerät zu überprüfen. Wenn das Gerät den Scan durchläuft und Citrix Gateway das Gerätezertifikat überprüft hat, können sich Benutzer dann am NetScaler Gateway anmelden.

> **Wichtig:**
>
> - Standardmäßig schreibt Windows Administratorrechte für den Zugriff auf Gerätezertifikate vor.
> - Um eine Gerätezertifikatsprüfung für Benutzer ohne Administratorrechte hinzuzufügen, müssen Sie das VPN-Plug-in installieren. Die VPN-Plug-In-Version muss dieselbe Version wie das EPA-Plug-In auf dem Gerät haben.
> - Sie können dem Gateway mehrere CA-Zertifikate hinzufügen und das Gerätezertifikat validieren.
> - Wenn Sie zwei oder mehr Gerätezertifikate auf Citrix Gateway installieren, müssen Benutzer das richtige Zertifikat auswählen, wenn sie sich bei Citrix Gateway anmelden oder bevor der Endpoint Analysis-Scan ausgeführt wird.
> - Wenn Sie das Gerätezertifikat erstellen, muss es sich um ein X.509-Zertifikat handeln.
> - Wenn Sie ein Gerätezertifikat haben, das von einer zwischengeschalteten CA ausgestellt wurde, müssen sowohl Zwischen- als auch Stamm-CA-Zertifikate gebunden sein.
> - Der EPA-Client benötigt den Benutzer lokale Administratorrechte, um auf den Maschinenzertifikatspeicher zugreifen zu können. Dies ist selten der Fall, daher besteht eine Problemumgehung darin, das vollständige NetScaler Gateway-Plug-In zu installieren, das auf den lokalen Speicher zugreifen kann.

Weitere Informationen zum Erstellen von Gerätezertifikaten finden Sie unter:

- Network Device Enrollment Service (NDES) in Active Directory-Zertifikatsdiensten (AD CS) auf der Microsoft-Website.
- So fordern Sie ein Zertifikat von einer Microsoft-Zertifizierungsstelle mithilfe von DCE/RPC und der Nutzdaten des Active Directory-Zertifikatprofils auf der Apple-Support-Website an.
- Ausstellung voniPad/iPhone-Zertifikaten im Microsoft-Support-Blog “Fragen Sie das Verzeichnisdienstteam”
- Einrichten des Netzwerkgeräte-Registrierungsdienstes auf der Windows IT Pro-Website.
- Beispiel für die schrittweise Bereitstellung der PKI-Zertifikate für Configuration Manager: Windows Server 2008-Zertifizierungsstelle auf der Microsoft System Center-Website.

### Schritte zum Konfigurieren von Gerätezertifikaten

Um ein Gerätezertifikat zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Installieren Sie das Zertifizierungsstellenzertifikat des Gerätezertifikatausstellers auf Citrix Gateway. Einzelheiten finden Sie unter Installieren des signierten Zertifikats auf Citrix Gateway.
- Binden Sie das Zertifikat der Zertifizierungsstelle des Gerätezertifikatausstellers an den virtuellen Citrix Gateway-Server und aktivieren Sie die OCSP-Prüfung. Einzelheiten finden Sie unter Installieren des signierten Zertifikats auf Citrix Gateway.
- Erstellen und binden Sie OCSP (Responder) auf dem Zertifikat der Zertifizierungsstelle des Gerätezertifikatausstellers. Einzelheiten finden Sie unter Überwachen des Zertifikatstatus mit OCSP.

Aktivieren Sie die Gerätezertifikatsprüfung auf dem virtuellen Server und fügen Sie das Zertifikat des Gerätezertifikatausstellers zur Checkliste für Gerätezertifikate hinzu. Einzelheiten finden Sie unter Aktivieren der Überprüfung von Gerätezertifikaten auf einem virtuellen Server für klassische EPA-Richtlinien.

Schließen Sie die clientseitige Konfiguration und Überprüfung des Gerätezertifikats auf dem Windows-Computer ab. Einzelheiten finden Sie unter Überprüfung des Gerätezertifikats auf einem Windows-Computer.

> **Hinweis:**
>
> Auf allen Clients, die das Gerätezertifikat EPA-Prüfung in Anspruch nehmen möchten, muss das Gerätezertifikat im Systemzertifikatspeicher des Computers installiert sein.

### Aktivieren der Gerätezertifikatsprüfung auf einem virtuellen Server für klassische EPA-Richtlinien

Nachdem Sie das Gerätezertifikat erstellt haben, installieren Sie das Zertifikat auf Citrix Gateway, indem Sie das Verfahren zum Importieren und Installieren eines vorhandenen Zertifikats in Citrix Gatewayverwenden.

1. Navigieren Sie auf der Registerkarte Konfiguration zu **Citrix Gateway > Virtuelle Server**.
2. Wählen Sie auf der Seite **Citrix Gateway Virtual Servers** einen vorhandenen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Virtuelle VPN-Server** im Abschnitt **Grundeinstellungen** auf **Bearbeiten**.
4. Deaktivieren Sie das Feld **Authentifizierung aktivieren**, um die Authentifizierung zu deaktivieren.
5. Wählen Sie das Feld **Gerätezertifikat** aktivieren, um das Gerätezertifikat

6. Klicken Sie auf **Hinzufügen**, um den Namen des CA-Zertifikats eines verfügbaren Gerätezertifikats zur Liste hinzuzufügen.
7. Um ein CA-Zertifikat an den virtuellen Server zu binden, klicken Sie im Abschnitt **CA for Device Certificateauf CA-Zertifikat**, klicken Sie auf**Hinzufügen**, wählen Sie das Zertifikat aus und klicken Sie dann auf**+**.

> **Hinweis:**
>
> Informationen zum Aktivieren und Binden von Gerätezertifikaten auf einem virtuellen Server für erweiterte EPA-Richtlinien finden Sie unter Gerätezertifikat in nFactor als EPA-Komponente.

### Überprüfung des Gerätezertifikats auf einem Windows-Computer

1. Öffnen Sie einen Browser und greifen Sie auf den Citrix Gateway FQDN zu.
2. Erlauben Sie dem Citrix End Point Analysis (EPA) -Client die Ausführung. Wenn noch nicht installiert, installieren Sie EPA.

   Citrix EPA führt das Gerätezertifikat aus und validiert es und leitet zur Authentifizierungsseite weiter, wenn die EPA-Prüfung des Gerätezertifikats erfolgreich ist, andernfalls werden Sie zur EPA-Fehlerseite weitergeleitet. Falls Sie andere EPA-Prüfungen haben, hängen die EPA-Scanergebnisse von den konfigurierten EPA-Prüfungen ab.

Überprüfen Sie zum weiteren Debuggen auf dem Client die folgenden EPA-Protokolle auf dem Client: C:\Users<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

**Hinweis:**

> Die Überprüfung des Gerätezertifikats mit CRL wird nicht unterstützt.

## Vorhandenes Zertifikat importieren und installieren

March 27, 2024

Sie können ein vorhandenes Zertifikat von einem Windows-basierten Computer mit Internetinformationsdiensten (IIS) oder von einem Computer importieren, auf dem Secure Gateway ausgeführt wird.

Achten Sie beim Exportieren des Zertifikats darauf, dass Sie auch den privaten Schlüssel exportieren. Manchmal können Sie den privaten Schlüssel nicht exportieren, was bedeutet, dass Sie das Zertifikat nicht auf Citrix Gateway installieren können. Verwenden Sie in diesem Fall die Certificate Signing Request (CSR), um ein Zertifikat zu erstellen. Einzelheiten finden Sie unter Erstellen einer Zertifikatsignieranforderung.

Wenn Sie ein Zertifikat und einen privaten Schlüssel aus Windows exportieren, erstellt der Computer eine Persönliche Informationsaustauschdatei (.pfx). Diese Datei wird dann auf Citrix Gateway als PKCS #12 -Zertifikat installiert.

Wenn Sie Secure Gateway durch Citrix Gateway ersetzen, können Sie das Zertifikat und den privaten Schlüssel vom Secure Gateway exportieren. Wenn Sie eine In-Place-Migration vom Secure Gateway zu Citrix Gateway durchführen, muss der vollqualifizierte Domänenname (FQDN) in der Anwendung und der Appliance identisch sein. Wenn Sie das Zertifikat vom Secure Gateway exportieren, setzen Sie das Secure Gateway sofort in den Ruhestand, installieren das Zertifikat auf Citrix Gateway und testen dann die Konfiguration. Secure Gateway und Citrix Gateway können nicht gleichzeitig in Ihrem Netzwerk ausgeführt werden, wenn sie denselben FQDN haben.

Wenn Sie Windows Server 2003 oder Windows Server 2008 verwenden, können Sie die Microsoft Management Console verwenden, um das Zertifikat zu exportieren. Weitere Informationen finden Sie in der Online-Hilfe von Windows.

Belassen Sie die Standardwerte für alle anderen Optionen, definieren Sie ein Kennwort und speichern Sie die PFX-Datei auf Ihrem Computer. Wenn das Zertifikat exportiert wird, installieren Sie es auf Citrix Gateway.

### So installieren Sie das Zertifikat und den privaten Schlüssel auf Citrix Gateway

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf **Citrix Gateway**.
2. Klicken Sie im Detailbereich unter Erste Schritte auf **Citrix Gateway-Assistent**.
3. Klicken Sie auf **Weiter**, wählen Sie einen vorhandenen virtuellen Server aus und klicken Sie dann auf **Weiter**.
4. Wählen Sie in den **Zertifikatsoptionen**die Option **Eine PKCS #12 -Datei (.pfx) installieren**aus.
5. Klicken Sie in **PKCS #12 File Name**auf **Durchsuchen**, navigieren Sie zum Zertifikat, und klicken Sie dann auf **Auswählen**.
6. Geben Sie in ((Kennwort)) das Kennwort für den privaten Schlüssel ein.

   Dies ist das Kennwort, das Sie bei der Konvertierung des Zertifikats in das PEM-Format verwendet haben.
7. Klicken Sie auf **Weiter**, um den Citrix Gateway-Assistenten zu beenden, ohne weitere Einstellungen zu ändern.

Wenn das Zertifikat auf Citrix Gateway installiert ist, wird das Zertifikat im Konfigurationsdienstprogramm im Knoten **SSL\ > Zertifikate** angezeigt.

**So erstellen Sie einen privaten Schlüssel**

1. Klicken Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich auf **SSL**.
2. Klicken Sie im Detailbereich unter **SSL-Schlüssel**auf **RSA-Schlüssel erstellen**.
3. Geben Sie unter**Key Filename**den Namen des privaten Schlüssels ein oder klicken Sie auf Durchsuchen, um zu einer vorhandenen Datei zu navigieren.
4. Geben Sie im**Feld Schlüsselgröße (Bits)**die Größe des privaten Schlüssels ein.
5. Wählen Sie unter**Public Exponent Value**F4 oder 3 aus.

   Der öffentliche Exponentenwert für den RSA-Schlüssel. Dies ist Teil des Verschlüsselungsalgorithmus und wird zum Erstellen des RSA-Schlüssels benötigt. Die Werte lauten F4 (Hex: 0x10001) oder 3 (Hex: 0x3). Die Standardeinstellung ist F4.
6. Wählen Sie im**Schlüsselformat**PEM oder DER aus.Citrix empfiehlt das PEM-Format für das Zertifikat.
7. Wählen Sie unter **PEM-Kodierungsalgorithmus**DES oder DES3 aus.
8. Geben Sie in**PEM Passphrase**und**Verify Passphrase**das Kennwort ein, klicken Sie auf **Erstellen**und dann auf **Schließen**.

   **Hinweis**: Um eine Passphrase zuzuweisen, muss das Schlüsselformat PEM sein und Sie müssen den Kodierungsalgorithmus auswählen.

Um einen privaten DSA-Schlüssel im Konfigurationsdienstprogramm zu**erstellen, klicken Sie auf DSA-Schlüssel** erstellen und befolgen Sie die Schritte zum Erstellen des privaten RSA-Schlüssels.

## Widerrufslisten für Zertifikate

March 27, 2024

Von Zeit zu Zeit stellen Zertifizierungsstellen (CAs) Zertifikatsperrlisten (CRLs) aus. CRLs enthalten Informationen über Zertifikate, denen nicht mehr vertraut werden kann. Angenommen, Ann verlässt die XYZ Corporation. Das Unternehmen kann Anns Zertifikat auf eine CRL legen, um zu verhindern, dass sie Nachrichten mit diesem Schlüssel signiert.

Ebenso können Sie ein Zertifikat widerrufen, wenn ein privater Schlüssel kompromittiert ist oder wenn dieses Zertifikat abgelaufen ist und ein neues verwendet wird. Bevor Sie einem öffentlichen Schlüssel vertrauen, stellen Sie sicher, dass das Zertifikat nicht in einer CRL angezeigt wird.

Citrix Gateway unterstützt die folgenden zwei CRL-Typen:

- CRLs, die die Zertifikate auflisten, die widerrufen wurden oder nicht mehr gültig sind
- Online Certificate Status Protocol (OSCP), ein Internetprotokoll, das zum Abrufen des Sperrstatus von X.509-Zertifikaten verwendet wird

**So fügen Sie eine CRL hinzu:**

Stellen Sie vor dem Konfigurieren der CRL auf dem Citrix Gateway-Gerät sicher, dass die CRL-Datei lokal auf dem Gerät gespeichert ist. Im Falle eines Hochverfügbarkeits-Setups muss die CRL-Datei auf beiden Citrix Gateway-Appliances vorhanden sein, und der Verzeichnispfad zur Datei muss auf beiden Appliances identisch sein.

Wenn Sie die CRL aktualisieren müssen, können Sie die folgenden Parameter verwenden:

- CRL-Name: Der Name der CRL, die auf dem Citrix ADC hinzugefügt wird. Maximal 31 Zeichen.
- CRL-Datei: Der Name der CRL-Datei, die auf dem Citrix ADC hinzugefügt wird. Der Citrix ADC sucht standardmäßig im Verzeichnis /var/netscaler/ssl nach der CRL-Datei. Maximal 63 Zeichen.
- URL: Maximal 127 Zeichen
- Basis-DN: Maximal 127 Zeichen
- Bind DN: Maximal 127 Zeichen
- Kennwort: Maximal 31 Zeichen
- Tage: Maximal 31

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration SSL und klicken Sie dann auf CRL.
2. Klicken Sie im Detailbereich auf "Hinzufügen".
3. Geben Sie im Dialogfeld CRL hinzufügen die Werte für Folgendes an:

    - CRL-Name
    - CRL Datei
    - Format (optional)
    - CA-Zertifikat (optional)

4. Klicken Sie auf **Create** und dann auf **Close**. Wählen Sie im Bereich CRL-Details die CRL aus, die Sie konfiguriert haben, und überprüfen Sie, ob die Einstellungen am unteren Bildschirmrand korrekt sind.

**So konfigurieren Sie CRL Autorefresh mithilfe von LDAP oder HTTP in der GUI:**

Eine CRL wird regelmäßig oder manchmal unmittelbar nach dem Widerruf eines bestimmten Zertifikats von einer CA generiert und veröffentlicht. Citrix empfiehlt, CRLs auf der Citrix Gateway-Appliance regelmäßig zu aktualisieren, um vor Clients zu schützen, die versuchen, eine Verbindung mit ungültigen Zertifikaten herzustellen.

Das Citrix Gateway-Gerät kann CRLs von einem Webspeicherort oder einem LDAP-Verzeichnis aus aktualisieren. Wenn Sie Aktualisierungsparameter und einen Webspeicherort oder einen LDAP-Server

angeben, muss die CRL zum Zeitpunkt der Ausführung des Befehls nicht auf dem lokalen Festplattenlaufwerk vorhanden sein. Bei der ersten Aktualisierung wird eine Kopie auf dem lokalen Festplattenlaufwerk in dem durch den Parameter CRL File angegebenen Pfad gespeichert. Der Standardpfad zum Speichern der CRL lautet /var/netscaler/ssl.

### CRL-Aktualisierungsparameter

- **CRL-Name**

  Der Name der CRL, die auf dem Citrix Gateway aktualisiert wird.

- **Aktivieren Sie die automatische Aktualisierung von CRL**

  Aktivieren oder deaktivieren Sie die automatische Aktualisierung von CRL.

- **CA-Zertifikat**

  Das Zertifikat der CA, die die CRL ausgestellt hat. Dieses CA-Zertifikat muss auf der Appliance installiert sein. Der Citrix ADC kann CRLs nur von CAs aktualisieren, deren Zertifikate darauf installiert sind.

- **Methode**

  Protokoll, in dem die CRL-Aktualisierung von einem Webserver (HTTP) oder einem LDAP-Server abgerufen werden soll. Mögliche Werte: HTTP, LDAP. Standard: HTTP.

- **Geltungsbereich**

  Das Ausmaß des Suchvorgangs auf dem LDAP-Server. Wenn der angegebene Bereich Base ist, erfolgt die Suche auf derselben Ebene wie der Basis-DN. Wenn der angegebene Bereich Eins ist, erstreckt sich die Suche auf eine Ebene unter dem Basis-DN.

- **Server-IP**

  Die IP-Adresse des LDAP-Servers, von dem die CRL abgerufen wird. Wählen Sie IPv6 aus, um eine IPv6-IP-Adresse zu verwenden.

- **Port**

  Die Portnummer, auf der der LDAP oder der HTTP-Server kommuniziert.

- **URL**

  Die URL für den Webstandort, von dem die CRL abgerufen wird.

- **Basis-DN**

  Der Basis-DN, der vom LDAP-Server für die Suche nach dem CRL-Attribut verwendet wird. Hinweis: Citrix empfiehlt, das Basis-DN-Attribut anstelle des Ausstellernamens aus dem CA-Zertifikat zu verwenden, um im LDAP-Server nach der CRL zu suchen. Das Feld "Ausstellername" stimmt möglicherweise nicht genau mit dem DN der LDAP-Verzeichnisstruktur überein.

- **Bind DN**

  Das bind-DN-Attribut wird verwendet, um auf das CRL-Objekt im LDAP-Repository zuzugreifen. Die Bind-DN-Attribute sind die Administratoranmeldeinformationen für den LDAP-Server. Konfigurieren Sie diesen Parameter, um den unbefugten Zugriff auf die LDAP-Server einzuschränken.

- **Kennwort**

  Das Administratorkennwort, das für den Zugriff auf das CRL-Objekt im LDAP-Repository verwendet wurde. Ein Kennwort ist erforderlich, wenn der Zugriff auf das LDAP-Repository eingeschränkt ist, das heißt, anonymer Zugriff ist nicht zulässig.

- **Intervall**

  Das Intervall, in dem die CRL-Aktualisierung durchgeführt werden muss. Geben Sie für eine sofortige CRL-Aktualisierung das Intervall als NOW an. Mögliche Werte: MONTHLY, DAILY, WEEKLY, NOW, NONE.

- **Tage**

  Der Tag, an dem die CRL-Aktualisierung durchgeführt werden muss. Die Option ist nicht verfügbar, wenn das Intervall auf DAILY eingestellt ist.

- **Zeit**

  Die genaue Uhrzeit im 24-Stunden-Format, zu der die CRL-Aktualisierung durchgeführt werden muss.

- **Binär**

  Stellen Sie den LDAP-basierten CRL-Abrufmodus auf binär ein. Mögliche Werte: YES, NO. Standard: NEIN.

1. Erweitern Sie im Navigationsbereich SSL und klicken Sie dann auf CRL.
2. Wählen Sie die konfigurierte CRL aus, für die Sie Aktualisierungsparameter aktualisieren möchten, und klicken Sie dann auf Öffnen.
3. Wählen Sie die Option "CRL Auto Refresh aktivieren".
4. Geben Sie in der Gruppe CRL Auto Refresh Parameters Werte für die folgenden Parameter an: Hinweis: Ein Sternchen (*) zeigt einen erforderlichen Parameter an.

   - Methode
   - Binär
   - Geltungsbereich
   - Server-IP
   - Port*
   - URL
   - Base DN*

- Bind DN
- Kennwort
- Intervall
- Tage
- Zeit

5. Klicken Sie auf Erstellen. Wählen Sie im CRL-Bereich die CRL aus, die Sie konfiguriert haben, und überprüfen Sie, ob die Einstellungen am unteren Bildschirmrand korrekt sind.

## Zertifikatsstatus mit OCSP überwachen

Online Certificate Status Protocol (OCSP) ist ein Internetprotokoll, das verwendet wird, um den Status eines Client-SSL-Zertifikats zu ermitteln. Citrix Gateway unterstützt OCSP wie in RFC 2560 definiert. OCSP bietet erhebliche Vorteile gegenüber Zertifikatsperrlisten (CRLs) in Bezug auf zeitnahe Informationen. Der aktuelle Widerrufsstatus eines Kundenzertifikats ist besonders nützlich bei Transaktionen mit hohen Geldsummen und hochwertigen Aktiengeschäften. Es verbraucht auch weniger System- und Netzwerkressourcen. Die Citrix Gateway-Implementierung von OCSP umfasst Anforderungs-Batching und Antwort-Caching.

### Citrix Gateway-Implementierung von OCSP

Die OCSP-Validierung auf einem Citrix Gateway-Gerät beginnt, wenn Citrix Gateway während eines SSL-Handshakes ein Clientzertifikat erhält. Um das Zertifikat zu validieren, erstellt Citrix Gateway eine OCSP-Anforderung und leitet sie an den OCSP-Responder weiter. Dazu extrahiert Citrix Gateway entweder die URL für den OCSP-Responder aus dem Clientzertifikat oder verwendet eine lokal konfigurierte URL. Die Transaktion befindet sich in einem angehaltenen Zustand, bis Citrix Gateway die Antwort des Servers auswertet und feststellt, ob die Transaktion zugelassen oder abgelehnt werden soll. Wenn sich die Antwort des Servers über die konfigurierte Zeit hinaus verzögert und keine anderen Responder konfiguriert sind, lässt Citrix Gateway die Transaktion zu oder zeigt einen Fehler an, je nachdem, ob Sie die OCSP-Prüfung auf optional oder obligatorisch festlegen. Citrix Gateway unterstützt das Stapeln von OCSP-Anfragen und das Zwischenspeichern von OCSP-Antworten, um die Belastung des OCSP-Responders zu reduzieren und schnellere Antworten zu ermöglichen.

### OCSP-Anforderungs-Batching

Jedes Mal, wenn Citrix Gateway ein Clientzertifikat erhält, sendet es eine Anfrage an den OCSP-Responder. Um eine Überlastung des OCSP-Responders zu vermeiden, kann Citrix Gateway den Status von mehr als einem Clientzertifikat in derselben Anforderung abfragen. Damit das Anforderungsbatching effizient funktioniert, müssen Sie ein Timeout definieren, damit die Verarbeitung eines einzelnen Zertifikats nicht verzögert wird, während Sie auf die Bildung eines Stapels warten.

#### OCSP-Antwort-Caching

Das Zwischenspeichern der vom OCSP-Responder empfangenen Antworten ermöglicht schnellere Antworten auf den Benutzer und reduziert die Belastung des OCSP-Responders. Nach Erhalt des Sperrstatus eines Clientzertifikats vom OCSP-Responder speichert Citrix Gateway die Antwort lokal für eine vordefinierte Zeitspanne. Wenn ein Clientzertifikat während eines SSL-Handshakes empfangen wird, überprüft Citrix Gateway zunächst seinen lokalen Cache auf einen Eintrag für dieses Zertifikat. Wenn ein Eintrag gefunden wird, der noch gültig ist (innerhalb des Cache-Timeout-Limits), wird der Eintrag ausgewertet und das Clientzertifikat wird akzeptiert oder abgelehnt. Wenn ein Zertifikat nicht gefunden wird, sendet Citrix Gateway eine Anforderung an den OCSP-Responder und speichert die Antwort für eine konfigurierte Zeitspanne in seinem lokalen Cache.

## Konfigurieren des OCSP-Zertifikats

Das Konfigurieren eines Online Certificate Status Protocol (OCSP) umfasst das Hinzufügen eines OCSP-Responders, das Binden des OCSP-Responders an ein signiertes Zertifikat von einer Certificate Authority (CA) und das Binden des Zertifikats und des privaten Schlüssels an einen virtuellen Secure Sockets Layer (SSL) -Server. Wenn Sie ein anderes Zertifikat und einen anderen privaten Schlüssel an einen bereits konfigurierten OCSP-Responder binden müssen, müssen Sie zuerst den Responder lösen und dann den Responder an ein anderes Zertifikat binden.

#### So konfigurieren Sie OCSP

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich SSL, und klicken Sie dann auf OCSP-Responder.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Feld Name einen Namen für das Profil ein.
4. Geben Sie unter URL die Webadresse des OCSP-Responders ein.

   Dieses Feld ist obligatorisch. Die Webadresse darf 32 Zeichen nicht überschreiten.
5. Um die OCSP-Antworten zwischenzuspeichern, klicken Sie auf Cache und geben Sie unter Timeout die Anzahl der Minuten ein, die Citrix Gateway die Antwort enthält.
6. Klicken Sie unter Batching anfordern auf Aktivieren.
7. Geben Sie in Batching Delay die Zeit in Millisekunden an, die für das Stapeln einer Gruppe von OCSP-Anfragen zulässig ist.

   Die Werte können zwischen 0 und 10000 liegen. Der Standardwert ist 1.

8. Geben Sie unter Produziert zur Zeitverzerrung ein, wie viel Zeit Citrix Gateway verwenden kann, wenn das Gerät die Antwort prüfen oder akzeptieren muss.
9. Wählen Sie unter Reaktionsüberprüfung Vertrauensantworten aus, wenn Sie Signaturprüfungen durch den OCSP-Responder deaktivieren möchten.

   Wenn Sie Trust Responses aktivieren, überspringen Sie Schritt 8 und Schritt 9.
10. Wählen Sie unter Certificate das Zertifikat aus, das zum Signieren der OCSP-Antworten verwendet wird.

    Wenn kein Zertifikat ausgewählt ist, wird die CA, an die der OCSP-Responder gebunden ist, zur Überprüfung der Antworten verwendet.
11. Geben Sie unter Request Timeout die Anzahl der Millisekunden ein, um auf eine OCSP-Antwort zu warten.

    Diese Zeit beinhaltet die Batching Delay-Zeit. Die Werte können zwischen 0 und 120000 liegen. Die Standardeinstellung ist 2000.
12. Wählen Sie unter Signaturzertifikat das Zertifikat und den privaten Schlüssel aus, mit denen OCSP-Anfragen signiert werden. Wenn Sie kein Zertifikat und keinen privaten Schlüssel angeben, werden die Anfragen nicht signiert.
13. Um die einmal verwendete Nummer zu aktivieren (`nonce`)`extension`, wählen Sie Nonce aus.
14. Um ein Clientzertifikat zu verwenden, klicken Sie auf Clientzertifikat einfügen
15. Klicken Sie auf Create und dann auf Close.

## Citrix Gateway-Konfiguration testen

March 27, 2024

Nachdem Sie die Anfangseinstellungen im Citrix Gateway konfiguriert haben, können Sie Ihre Einstellungen testen, indem Sie eine Verbindung zum Gerät herstellen.

Erstellen Sie ein lokales Benutzerkonto, um die Citrix Gateway-Einstellungen zu testen. Öffnen Sie dann mithilfe der IP-Adresse des virtuellen Servers oder des vollqualifizierten Domänennamens (FQDN) des Geräts einen Webbrowser und geben Sie die Webadresse ein. Beispiel: Geben Sie in die Adressleiste `https://my.company.com` oder `https://192.168.96.183` ein.

Geben Sie im Anmeldebildschirm den Benutzernamen und das Kennwort des zuvor erstellten Benutzerkontos ein. Nachdem Sie sich angemeldet haben, werden Sie aufgefordert, das Citrix Gateway Plug-in herunterzuladen und zu installieren.

Nachdem Sie das Citrix Gateway Plug-in installiert und anschließend erfolgreich mit dem Citrix Gateway verbunden haben, wird das Access Interface angezeigt. Das Access Interface ist die Standard-Homepage für Citrix Gateway.

### Erstellen Sie über die GUI ein Benutzerkonto

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway\ > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Benutzer**.
2. Klicken Sie im Detailbereich auf "Hinzufügen".
3. Geben Sie unter "Benutzername"den Benutzernamen ein.
4. Wenn Sie die lokale Authentifizierung verwenden, deaktivieren Sie das Kontrollkästchen "Externe Authentifizierung". Die Authentifizierung von Benutzern mit externen Authentifizierungstypen wie LDAP oder RADIUS ist die Standardeinstellung. Wenn Sie dieses Kontrollkästchen deaktivieren, werden Benutzer von Citrix Gateway authentifiziert.
5. Geben Sie unter Kennwort und Kennwort bestätigen das Kennwort für den Benutzer ein, klicken Sie auf Erstellen und dann auf Schließen.

Wenn Sie Benutzer mit dem Konfigurationsprogramm hinzufügen, können Sie die folgenden Richtlinien an den Benutzer binden:

- Autorisierung
- Datenverkehr, Sitzung und Überwachung
- Lesezeichen
- Intranetanwendungen
- Intranet-IP-Adressen

Wenn Sie Probleme beim Anmelden mit dem Testbenutzerkonto haben, überprüfen Sie Folgendes:

- Wenn eine Zertifikatwarnung angezeigt wird, ist auf Citrix Gateway entweder ein Testzertifikat oder ein ungültiges Zertifikat installiert. Wenn auf dem Gerät ein von einer Zertifizierungsstelle (ZS) signiertes Zertifikat installiert ist, stellen Sie sicher, dass auf dem Benutzergerät ein entsprechendes Stammzertifikat vorhanden ist.
- Vergewissern Sie sich bei Verwendung eines von einer Zertifizierungsstelle signierten Zertifikats, dass Sie das Site-Zertifikat ordnungsgemäß mithilfe der signierten Zertifikatsignieranforderung (CSR) generiert haben und dass die in die CSR eingegebenen Distinguished Name-Daten (DN) korrekt sind. Das Problem könnte auch darin bestehen, dass der Hostname nicht mit der IP-Adresse übereinstimmt, die sich auf dem signierten Zertifikat befindet. Überprüfen Sie, ob der allgemeine Name des konfigurierten Zertifikats den IP-Adressinformationen des konfigurierten virtuellen Servers entspricht.
- Wenn der Anmeldebildschirm nicht angezeigt oder eine andere Fehlermeldung angezeigt wird, überprüfen Sie den Setupvorgang und vergewissern Sie sich, dass Sie alle Schritte korrekt ausgeführt und alle Parameter korrekt eingegeben haben.

# Upgrade der Citrix Gateway-Software

March 27, 2024

Sie können die Software aktualisieren, die sich auf Citrix Gateway befindet, wenn neue Versionen verfügbar gemacht werden. Sie können auf der Citrix Website nach Updates suchen. Sie können nur auf eine neue Version upgraden, wenn Ihre Citrix Gateway-Lizenzen bei der Veröffentlichung des Updates unter dem Subscription Advantage-Programm stehen. Sie können Subscription Advantage jederzeit verlängern. Weitere Informationen finden Sie auf der Citrix Support-Website.

Der Upgrade-Pfad und die Informationen zu kompatiblen Produkten sind auch im Citrix Upgrade Guideverfügbar.

Informationen zur neuesten Citrix Gateway-Wartungsversion finden Sie im Citrix Knowledge Center.

## Suchen Sie nach Softwareupdates

1. Rufen Sie die Citrix Website auf.
2. Klicken Sie auf **My Account** und melden Sie sich an.
3. Klicken Sie auf **Downloads**.
4. Wählen Sie unter Downloads suchen **Citrix Gateway**aus.
5. Wählen Sie unter **Download-Typauswählen** die Option **Produktsoftware** aus und klicken Sie dann auf **Suchen**.
   Sie können auch **Virtual Appliances** auswählen, um Citrix ADC VPX herunterzuladen. Wenn Sie diese Option auswählen, sehen Sie eine Liste mit Software für die virtuellen Maschinen für jeden Hypervisor.
6. Erweitern Sie auf der Seite Citrix Gateway **Citrix ADC Gateway oder Access Gateway**.
7. Klicken Sie auf die Gerätesoftwareversion, die Sie herunterladen möchten.
8. Wählen Sie auf der Seite Appliance-Software für die Version, die Sie herunterladen möchten, die virtuelle Appliance aus, und klicken Sie dann auf **Herunterladen**.
9. Folgen Sie den Anweisungen auf dem Bildschirm, um die Software herunterzuladen.

Wenn die Software auf Ihren Computer heruntergeladen wird, können Sie den Upgrade-Assistenten oder die Eingabeaufforderung verwenden, um die Software zu installieren.

## Aktualisieren Sie das Citrix Gateway mithilfe des Upgrade-Assistenten

1. Klicken Sie im Konfigurationsdienstprogramm auf der **Registerkarte Konfiguration**im Navigationsbereich auf System.

2. Klicken Sie im Detailbereich auf **Upgrade-Assistent**.
3. Klicken Sie auf **Weiter** und folgen Sie dann den Anweisungen des Assistenten.

### Aktualisieren Sie das Citrix Gateway mithilfe einer Eingabeaufforderung

1. Um die Software auf Citrix Gateway hochzuladen, verwenden Sie einen sicheren FTP-Client wie WinSCP, um eine Verbindung zur Appliance herzustellen.
2. Kopieren Sie die Software von Ihrem Computer in das`nsinstall` Verzeichnis /var/ auf der Appliance.
3. Verwenden Sie einen Secure Shell (SSH) -Client wie PuTTY, um eine SSH-Verbindung zur Appliance zu öffnen.
4. Melden Sie sich bei Citrix Gateway an.
5. Geben Sie an einer Eingabeaufforderung Folgendes ein: `shell`
6. Um in das `nsinstall` Verzeichnis zu wechseln, geben Sie an einer Eingabeaufforderung Folgendes ein: `cd /var/nsinstall`
7. Um den Inhalt des Verzeichnisses anzuzeigen, geben Sie Folgendes ein: `ls`
8. Um die Software zu entpacken, geben Sie ein: tar —xvzf build_x_xx.tgz, wobei build_x_xx.tgz der Name des Builds ist, auf den Sie upgraden möchten.
9. Um die Installation zu starten, geben Sie an einer Eingabeaufforderung Folgendes ein: `./installns`
10. Wenn die Installation abgeschlossen ist, starten Sie Citrix Gateway neu.

Starten Sie nach dem Neustart von Citrix Gateway das Konfigurationsdienstprogramm, um die erfolgreiche Installation zu überprüfen. Die Citrix Gateway-Version, die sich auf dem Gerät befindet, wird in der oberen rechten Ecke angezeigt.

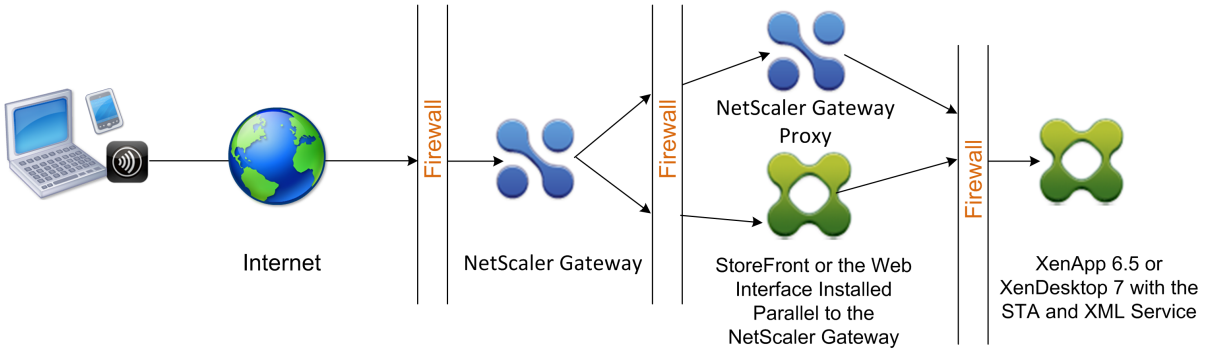
## Citrix Gateway in einer Double-Hop-DMZ bereitstellen

March 27, 2024

Einige Organisationen verwenden für den Schutz ihrer internen Netzwerke drei Firewalls. Diese drei Firewalls unterteilen die DMZ in zwei Stufen und bieten so zusätzliche Sicherheit für das interne Netzwerk. Diese Netzwerkkonfiguration nennt sich Double-Hop-DMZ.

Abbildung 1. Citrix Gateway-Appliances werden in einer Double-Hop-DMZ bereitgestellt




> **Hinweis:**
>
> Zur Veranschaulichung beschreibt das vorangegangene Beispiel eine Double-Hop-Konfiguration mit drei Firewalls mit StoreFront, dem Webinterface und Citrix Virtual Apps, aber Sie können auch eine Double-Hop-DMZ mit einer Appliance in der DMZ und einer Appliance im sicheren Netzwerk haben. Wenn Sie eine Double-Hop-Konfiguration mit einer Appliance in der DMZ und einer im sicheren Netzwerk konfigurieren, können Sie die Anweisungen zum Öffnen von Ports an der dritten Firewall ignorieren.

Sie können eine Double-Hop-DMZ für die Unterstützung von Citrix StoreFront oder das parallel zum Citrix Gateway-Proxy installierte Webinterface konfigurieren. Benutzer verbinden sich mithilfe der Citrix Workspace-App.

> **Hinweis:**
>
> Wenn Sie Citrix Gateway in einer Double-Hop-DMZ mit StoreFront bereitstellen, funktioniert die E-Mail-basierte AutoDiscovery für Citrix Workspace-App nicht.

### So funktioniert eine Double-Hop-Bereitstellung

Sie können Citrix Gateway-Appliances in einer Double-Hop-DMZ bereitstellen, um den Zugriff auf Server zu steuern, auf denen Citrix Virtual Apps ausgeführt wird. Die Verbindungen in einer Double-Hop-Bereitstellung erfolgen wie folgt:

- Benutzer stellen in der ersten DMZ eine Verbindung zu Citrix Gateway her, indem sie einen Webbrowser verwenden und mithilfe der Citrix Workspace-App eine veröffentlichte Anwendung auswählen.
- Die Citrix Workspace-App startet auf dem Benutzergerät. Der Benutzer stellt eine Verbindung zu Citrix Gateway her, um auf die veröffentlichte Anwendung zuzugreifen, die in der Serverfarm im sicheren Netzwerk ausgeführt wird.

  **Hinweis:** Secure Hub und das Citrix Gateway-Plug-in werden in einer Double-Hop-DMZ-Bereitstellung nicht unterstützt. Nur die Citrix Workspace-App wird für Benutzerverbindungen verwendet.

- Citrix Gateway in der ersten DMZ verarbeitet Benutzerverbindungen und führt die Sicherheitsfunktionen eines SSL-VPN aus. Dieses Citrix Gateway verschlüsselt Benutzerverbindungen, bestimmt, wie die Benutzer authentifiziert werden, und steuert den Zugriff auf die Server im internen Netzwerk.
- Citrix Gateway in der zweiten DMZ dient als Citrix Gateway-Proxy-Gerät. Dieses Citrix Gateway ermöglicht es dem ICA-Datenverkehr, die zweite DMZ zu durchqueren, um Benutzerverbindungen zur Serverfarm herzustellen. Die Kommunikation zwischen Citrix Gateway in der ersten DMZ und der Secure Ticket Authority (STA) im internen Netzwerk wird ebenfalls über Citrix Gateway in der zweiten DMZ weitergeleitet.

Citrix Gateway unterstützt IPv4- und IPv6-Verbindungen. Sie können das Konfigurationsdienstprogramm verwenden, um die IPv6-Adresse zu konfigurieren.

In der folgenden Tabelle wird die Unterstützung der Double-Hop-Bereitstellung für die verschiedenen ICA-Funktionen vorgeschlagen:

| ICA-Funktion | Double-Hop-Unterstützung |
|---|---|
| SmartAccess | Ja |
| SmartControl | Ja |
| Enlightened Data Transport (EDT) | Ja |
| HDX Insight | Ja |
| ICA-Sitzungszuverlässigkeit (Port 2598) | Ja |
| ICA-Sitzungsmigration | Ja |
| ICA-Sitzungszeitlimit | Ja |
| Multistream-ICA | Ja (nur TCP) |
| Framehawk | Nein |
| UDP-Audio | Nein |

### Bereiten Sie sich auf eine Double-Hop-DMZ-Bereitstellung vor

Um sich angemessen vorzubereiten und unnötige Probleme bei der Konfiguration einer Double-Hop-DMZ-Bereitstellung zu vermeiden, müssen Sie die folgenden Fragen beantworten:

- Möchte ich den Lastenausgleich unterstützen?
- Welche Ports muss ich an den Firewalls öffnen?
- Wie viele SSL-Zertifikate brauche ich?
- Welche Komponenten benötige ich, bevor ich mit der Bereitstellung beginne?

Die Themen in diesem Abschnitt enthalten Informationen, die Ihnen bei der Beantwortung dieser Fragen helfen, sofern dies für Ihre Umgebung angemessen ist.

**Komponenten, die für den Beginn der Bereitstellung erforderlich sind**

Bevor Sie mit einer Double-Hop-DMZ-Bereitstellung beginnen, stellen Sie sicher, dass Sie über die folgenden Komponenten verfügen:

- Mindestens zwei Citrix Gateway-Appliances müssen verfügbar sein (eine für jede DMZ).
- Server, auf denen Citrix Virtual Apps ausgeführt werden, müssen im internen Netzwerk installiert und betriebsbereit sein.
- Das Webinterface oder StoreFront muss in der zweiten DMZ installiert und für den Betrieb mit der Serverfarm im internen Netzwerk konfiguriert sein.
- Mindestens ein SSL-Serverzertifikat muss auf Citrix Gateway in der ersten DMZ installiert sein. Dieses Zertifikat stellt sicher, dass der Webbrowser und Benutzerverbindungen zu Citrix Gateway verschlüsselt sind.

  Sie benötigen zusätzliche Zertifikate, wenn Sie Verbindungen verschlüsseln möchten, die zwischen den anderen Komponenten in einer Double-Hop-DMZ-Bereitstellung auftreten.

## Kommunikationsfluss in einer Double-Hop-DMZ-Bereitstellung

March 27, 2024

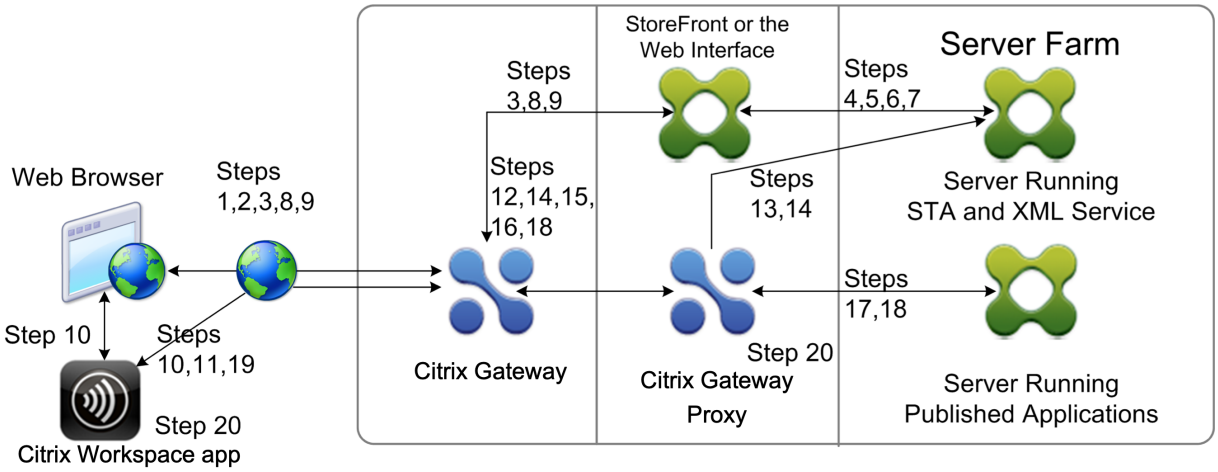
Um die Konfigurationsprobleme einer Double-Hop-DMZ-Bereitstellung zu verstehen, müssen Sie über ein grundlegendes Verständnis darüber verfügen, wie die verschiedenen Komponenten von Citrix Gateway und Citrix Virtual Apps in einer Double-Hop-DMZ-Bereitstellung kommunizieren, um eine Benutzerverbindung zu unterstützen. Der Verbindungsprozess für StoreFront und das Webinterface ist derselbe.

Obwohl der Benutzerverbindungsprozess in einem kontinuierlichen Fluss stattfindet, sind die folgenden Schritte auf hoher Ebene in den Prozess involviert.

- Benutzer authentifizieren
- Erstellen Sie ein Sitzungsticket
- Starten Sie die Citrix Workspace-App
- Schließen Sie die Verbindung ab

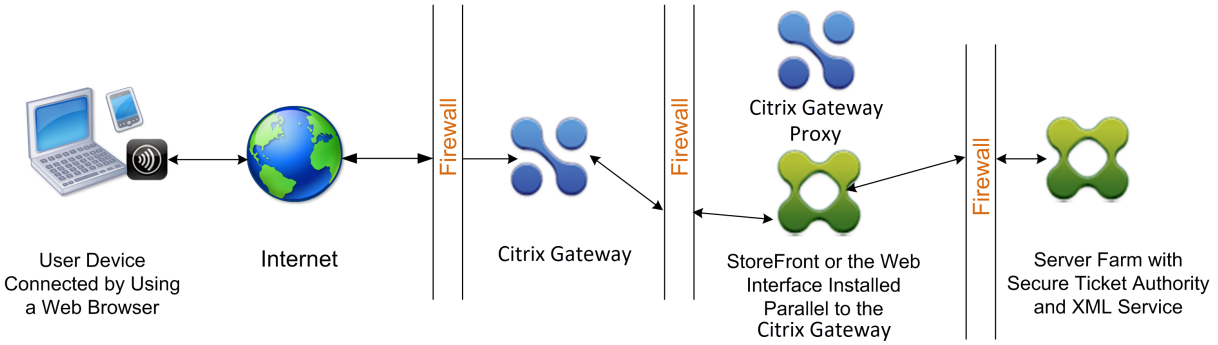
Die folgende Abbildung zeigt die Schritte, die bei der Benutzerverbindung mit StoreFront oder dem Webinterface auftreten. Im sicheren Netzwerk führen Computer, auf denen Citrix Virtual Apps ausgeführt werden, auch die Secure Ticket Authority (STA), den XML-Dienst und veröffentlichte Anwendungen aus.




## Prozess der Verbindung

**Die Authentifizierung von Benutzern ist der erste Schritt des Benutzerverbindungsprozesses in einer Double-Hop-DMZ-Bereitstellung.**

Die folgende Abbildung zeigt den Benutzerverbindungsprozess in dieser Bereitstellung.




Während der Benutzerauthentifizierungsphase findet der folgende grundlegende Prozess statt:

1. Ein Benutzer gibt die Adresse von Citrix Gateway ein, z. B. https://www.ng.wxyco.com in einem Webbrowser, um eine Verbindung zu Citrix Gateway in der ersten DMZ herzustellen. Wenn Sie die Authentifizierung der Anmeldeseite auf Citrix Gateway aktiviert haben, authentifiziert Citrix Gateway den Benutzer.
2. Citrix Gateway in der ersten DMZ erhält die Anfrage.
3. Citrix Gateway leitet die Webbrowser-Verbindung zum Webinterface um.

4. Das Webinterface sendet die Benutzeranmeldeinformationen an den Citrix XML-Dienst, der in der Serverfarm im internen Netzwerk ausgeführt wird.
5. Der Citrix XML-Dienst authentifiziert den Benutzer.
6. Der XML-Dienst erstellt eine Liste der veröffentlichten Anwendungen, auf die der Benutzer zugreifen darf, und sendet diese Liste an das Webinterface.

   **Hinweis:**

   - Wenn Sie die Authentifizierung auf Citrix Gateway aktivieren, sendet das Gerät die Citrix Gateway-Anmeldeseite an den Benutzer. Der Benutzer gibt die Authentifizierungsanmeldeinformationen auf der Anmeldeseite ein und die Appliance authentifiziert den Benutzer. Citrix Gateway gibt dann die Benutzeranmeldeinformationen an das Webinterface zurück.
   - Wenn Sie die Authentifizierung nicht aktivieren, führt Citrix Gateway keine Authentifizierung durch. Die Appliance stellt eine Verbindung zum Webinterface her, ruft die Webinterface-Anmeldeseite ab und sendet die Webinterface-Anmeldeseite an den Benutzer. Der Benutzer gibt die Authentifizierungsanmeldeinformationen auf der Webinterface-Anmeldeseite ein und Citrix Gateway übergibt die Benutzeranmeldeinformationen zurück an das Webinterface.

   **Das Erstellen des Sitzungsticket ist die zweite Phase des Benutzerverbindungsprozesses in einer Double-Hop-DMZ-Bereitstellung.**

   Während der Erstellungsphase des Sitzungsticket findet der folgende grundlegende Prozess statt:

7. Das Webinterface kommuniziert sowohl mit dem XML-Dienst als auch mit der Secure Ticket Authority (STA) im internen Netzwerk, um Sitzungstickets für jede der veröffentlichten Anwendungen zu erstellen, auf die der Benutzer zugreifen darf. Das Sitzungsticket enthält eine Aliasadresse für den Computer, auf dem Citrix Virtual Apps ausgeführt wird und der eine veröffentlichte Anwendung hostet.
8. Die STA speichert die IP-Adressen der Server, die die veröffentlichten Anwendungen hosten. Die STA sendet dann die angeforderten Sitzungstickets an das Webinterface. Jedes Sitzungsticket enthält einen Alias, der die IP-Adresse des Servers darstellt, der die veröffentlichte Anwendung hostet, jedoch nicht die tatsächliche IP-Adresse.
9. Das Webinterface generiert eine ICA-Datei für jede der veröffentlichten Anwendungen. Die ICA-Datei enthält das von der STA ausgestellte Ticket. Das Webinterface erstellt und füllt dann eine Webseite mit einer Liste von Links zu den veröffentlichten Anwendungen und sendet diese Webseite an den Webbrowser auf dem Benutzergerät.

   Das Starten der Citrix Workspace-App ist die dritte Stufe des Benutzerverbindungsprozesses in einer Double-Hop-DMZ-Bereitstellung. Der grundlegende Prozess ist wie folgt:

10. Der Benutzer klickt im Webinterface auf einen Link zu einer veröffentlichten Anwendung. Das Webinterface sendet die ICA-Datei für diese veröffentlichte Anwendung an den Browser für das Benutzergerät.

    Die ICA-Datei enthält Daten, die den Webbrowser anweisen, Receiver zu starten.

    Die ICA-Datei enthält auch den vollqualifizierten Domänennamen (FQDN) oder den Domänennamensystem (DNS) -Namen des Citrix Gateway in der ersten DMZ.

11. Der Webbrowser startet Receiver und der Benutzer stellt eine Verbindung zu Citrix Gateway in der ersten DMZ her, indem er den Namen Citrix Gateway in der ICA-Datei verwendet. Das anfängliche SSL/TLS-Handshaking erfolgt, um die Identität des Servers festzustellen, auf dem Citrix Gateway ausgeführt wird.

    **Das Herstellen der Verbindung ist die vierte und letzte Phase des Benutzerverbindungsprozesses in einer Double-Hop-DMZ-Bereitstellung.**

    Während der Verbindungsabschlussphase findet der folgende grundlegende Prozess statt:

    - Der Benutzer klickt im Webinterface auf einen Link zu einer veröffentlichten Anwendung.
    - Der Webbrowser erhält die vom Webinterface generierte ICA-Datei und startet die Citrix Workspace-App.
      Hinweis: Die ICA-Datei enthält Code, der den Webbrowser anweist, die Citrix Workspace-App zu starten.
    - Die Citrix Workspace-App initiiert in der ersten DMZ eine ICA-Verbindung zu Citrix Gateway.
    - Citrix Gateway in der ersten DMZ kommuniziert mit der Secure Ticket Authority (STA) im internen Netzwerk, um die Aliasadresse im Sitzungsticket auf die tatsächliche IP-Adresse eines Computers aufzulösen, auf dem Citrix Virtual Apps oder StoreFront ausgeführt wird. Diese Kommunikation wird vom Citrix Gateway-Proxy über die zweite DMZ geleitet.
    - Citrix Gateway in der ersten DMZ stellt die ICA-Verbindung zur Citrix Workspace-App her.
    - Die Citrix Workspace-App kann jetzt über beide Citrix Gateway-Appliances mit dem Computer kommunizieren, auf dem Citrix Virtual Apps im internen Netzwerk ausgeführt wird.

    Die detaillierten Schritte zum Abschließen des Benutzerverbindungsvorgangs lauten wie folgt:

12. Die Citrix Workspace-App sendet das STA-Ticket für die veröffentlichte Anwendung an Citrix Gateway in der ersten DMZ.

13. Citrix Gateway in der ersten DMZ kontaktiert die STA im internen Netzwerk zur Ticketvalidierung. Um die STA zu kontaktieren, baut Citrix Gateway eine SOCKS oder SOCKS mit SSL-Verbindung zum Citrix Gateway-Proxy in der zweiten DMZ auf.

14. Der Citrix Gateway-Proxy in der zweiten DMZ leitet die Anforderung zur Ticketvalidierung an die STA im internen Netzwerk weiter. Die STA validiert das Ticket und ordnet es dem Computer zu, auf dem Citrix Virtual Apps ausgeführt wird, auf dem die veröffentlichte Anwendung gehostet wird.

15. Die STA sendet eine Antwort an den Citrix Gateway-Proxy in der zweiten DMZ, die in der ersten DMZ an Citrix Gateway übergeben wird. Diese Antwort schließt die Ticketvalidierung ab und enthält die IP-Adresse des Computers, der die veröffentlichte Anwendung hostet.
16. Citrix Gateway in der ersten DMZ integriert die Adresse des Citrix Virtual Apps-Servers in das Benutzerverbindungspaket und sendet dieses Paket an den Citrix Gateway-Proxy in der zweiten DMZ.
17. Der Citrix Gateway-Proxy in der zweiten DMZ stellt eine Verbindungsanforderung an den im Verbindungspaket angegebenen Server.
18. Der Server reagiert auf den Citrix Gateway-Proxy in der zweiten DMZ. Der Citrix Gateway-Proxy in der zweiten DMZ übergibt diese Antwort an Citrix Gateway in der ersten DMZ, um die Verbindung zwischen dem Server und Citrix Gateway in der ersten DMZ herzustellen.
19. Citrix Gateway in der ersten DMZ vervollständigt den SSL/TLS-Handshake mit dem Benutzergerät, indem das endgültige Verbindungspaket an das Benutzergerät übergeben wird. Die Verbindung vom Benutzergerät zum Server wird hergestellt.
20. Der ICA-Verkehr fließt zwischen dem Benutzergerät und dem Server über Citrix Gateway in der ersten DMZ und den Citrix Gateway-Proxy in der zweiten DMZ.

## Citrix Gateway in einer Double-Hop-DMZ installieren und konfigurieren

March 27, 2024

Sie müssen mehrere Schritte ausführen, um Citrix Gateway in einer Double-Hop-DMZ bereitzustellen. Zu den Schritten gehören die Installation von Geräten in beiden DMZs und die Konfiguration der Appliances für Benutzergeräteverbindungen.

### Installieren Sie Citrix Gateway in der ersten DMZ

Folgen Sie den Anweisungen unter Installieren der Hardware, um Citrix Gateway in der ersten DMZ zu installieren.

Wenn Sie mehrere Citrix Gateway-Appliances in der ersten DMZ installieren, können Sie die Appliances hinter einem Load Balancer bereitstellen.

### Konfigurieren Sie Citrix Gateway in der ersten DMZ

In einer Double-Hop-DMZ-Bereitstellung ist es zwingend erforderlich, dass Sie jedes Citrix Gateway in der ersten DMZ so konfigurieren, dass Verbindungen entweder zu StoreFront oder zum Webinterface

in der zweiten DMZ umgeleitet werden.

Die Umleitung zu StoreFront oder dem Webinterface erfolgt auf Citrix Gateway Global- oder Virtual Server-Ebene. Um über Citrix Gateway eine Verbindung zum Webinterface herzustellen, muss ein Benutzer einer Citrix Gateway-Benutzergruppe zugeordnet sein, für die die Umleitung zum Webinterface aktiviert ist.

### Installieren Sie Citrix Gateway in der zweiten DMZ

Das Citrix Gateway-Gerät in der zweiten DMZ wird als Citrix Gateway-Proxy bezeichnet, da es den Datenverkehr von ICA und Secure Ticket Authority (STA) über die zweite DMZ weiterleitet. Installieren Sie die Hardware, um jedes Citrix Gateway-Gerät in der zweiten DMZ zu installieren.

Sie können dieses Installationsverfahren verwenden, um andere Geräte in der zweiten DMZ zu installieren.

Nachdem Sie Citrix Gateway-Geräte in der zweiten DMZ installiert haben, konfigurieren Sie die folgenden Einstellungen:

- Konfigurieren Sie einen virtuellen Server auf dem Citrix Gateway-Proxy.
- Konfigurieren Sie Citrix Gateway-Geräte in der ersten und zweiten DMZ für die Kommunikation miteinander.
- Binden Sie das Citrix Gateway in der zweiten DMZ global oder an einen virtuellen Server.
- Konfigurieren Sie die STA auf dem Gerät in der ersten DMZ.
- Öffnen Sie Ports in den Firewalls, die die DMZ unterteilen.
- Installieren Sie Zertifikate auf den Geräten.

## Einstellungen auf den virtuellen Servern im Citrix Gateway-Proxy konfigurieren

March 27, 2024

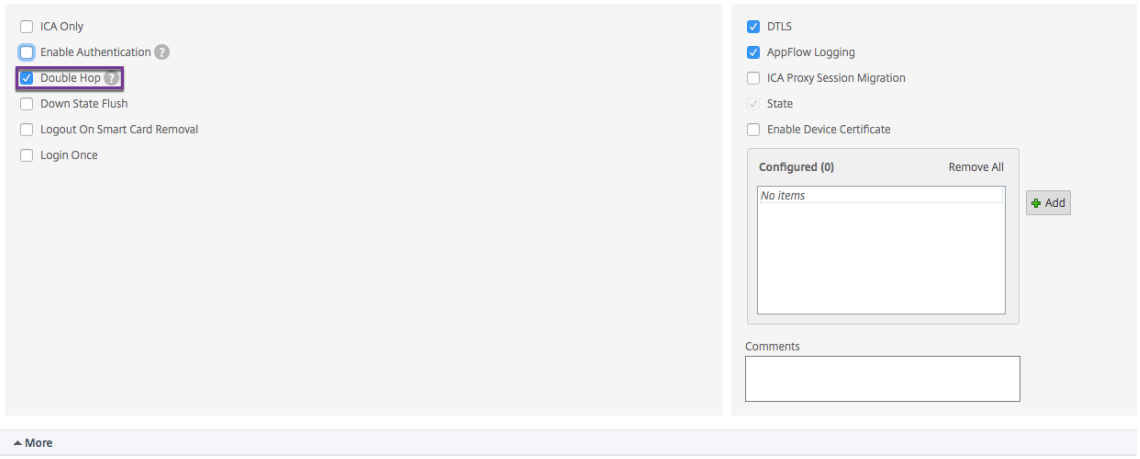
Um Verbindungen zwischen den Citrix Gateway-Appliances zuzulassen, aktivieren Sie Double-Hop auf dem virtuellen Server auf dem Citrix Gateway-Proxy.

Wenn Benutzer eine Verbindung herstellen, authentifiziert das Citrix Gateway-Gerät Benutzer und stellt dann die Verbindung zum Proxy-Gerät her. Konfigurieren Sie auf dem Citrix Gateway in der ersten DMZ den virtuellen Server für die Kommunikation mit Citrix Gateway in der zweiten DMZ. Konfigurieren Sie keine Authentifizierung oder Richtlinien für den Citrix Gateway-Proxy. Citrix empfiehlt, die Authentifizierung auf dem virtuellen Server zu deaktivieren.

### So aktivieren Sie Double-Hop auf dem virtuellen Server auf dem Citrix Gateway-Proxy über die GUI

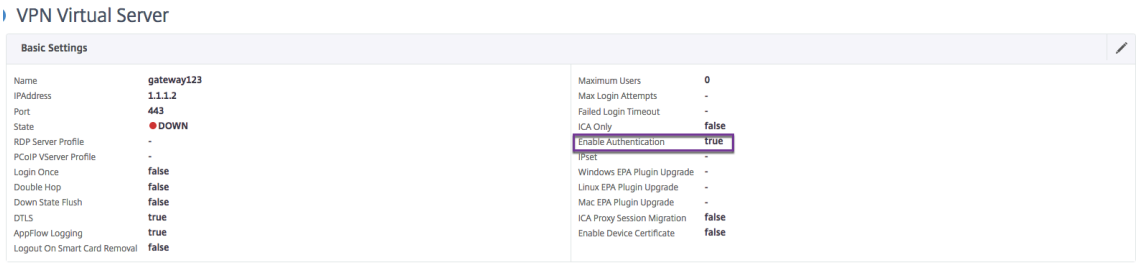
1. Navigieren Sie zu **Konfiguration > Citrix Gateway > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Grundeinstellungen** auf das Bearbeitungssymbol und dann auf **Mehr**.
4. Wählen Sie **Double Hop**.




5. Klicken Sie auf **OK**.

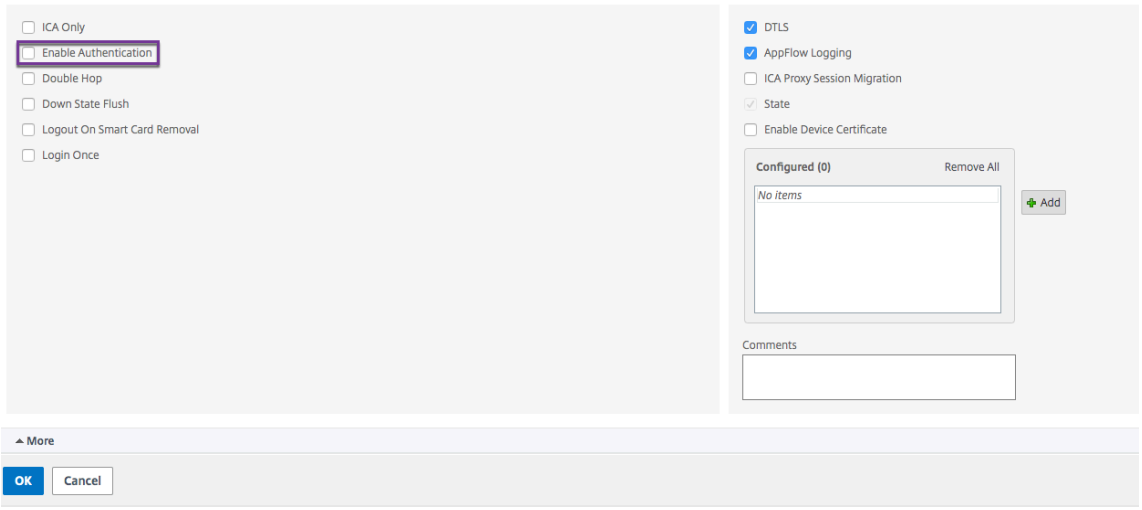
### So deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem Citrix Gateway-Proxy über die GUI

1. Navigieren Sie zu **Konfiguration > Citrix Gateway > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Grundeinstellungen** auf das Bearbeitungssymbol und dann auf **Mehr**.




4. Deaktivieren Sie das Kontrollkästchen **Authentifizierung aktivieren**.




5. Klicken Sie auf **OK**.

## Appliance für die Kommunikation mit dem Applianceproxy konfigurieren

March 27, 2024

Wenn Sie Citrix Gateway in einer Double-Hop-DMZ bereitstellen, müssen Sie Citrix Gateway in der ersten DMZ für die Kommunikation mit dem Citrix Gateway-Proxy in der zweiten DMZ konfigurieren.

Wenn Sie mehrere Appliances in der zweiten DMZ bereitstellen, konfigurieren Sie jede Appliance in der ersten DMZ für die Kommunikation mit jeder Proxy-Appliance in der zweiten DMZ.

Hinweis: Wenn Sie IPv6 verwenden möchten, konfigurieren Sie den nächsten Hop-Server mithilfe des Konfigurationsdienstprogramms. Erweitern Sie dazu
Citrix Gateway > Ressourcen und klicken Sie dann auf
Next Hop Server. Befolgen Sie die Schritte im folgenden Verfahren und aktivieren Sie dann das Kontrollkästchen
IPv6.

### So konfigurieren Sie Citrix Gateway für die Kommunikation mit dem Citrix Gateway Proxy

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration Citrix Gateway > Ressourcen, und klicken Sie dann auf Next Hop Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.

3. Geben Sie unter Name einen Namen für das erste Citrix Gateway ein.
4. Geben Sie unter IP-Adresse die IP-Adresse des virtuellen Servers des Citrix Gateway-Proxys in die zweite DMZ ein.
5. Geben Sie unter Port die Portnummer ein, klicken Sie auf Erstellen und dann auf Schließen. Wenn Sie einen sicheren Port wie 443 verwenden, wählen Sie Sicher.

Sie müssen jedes in der ersten DMZ installierte Citrix Gateway für die Kommunikation mit allen Citrix Gateway-Proxy-Appliances konfigurieren, die in der zweiten DMZ installiert sind.

Nachdem Sie die Einstellungen für den Citrix Gateway-Proxy konfiguriert haben, binden Sie die Richtlinie an Next Hop Server in Citrix Gateway Global oder an einen virtuellen Server.

### So binden Sie den Citrix Gateway Next-Hop-Server global

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration Citrix Gateway > Ressourcen, und klicken Sie dann auf Next Hop Server.
2. Wählen Sie im Detailbereich einen Next-Hop-Server aus und wählen Sie dann unter Aktion Globale Bindungen aus.
3. Wählen Sie im Dialogfeld Globale Bindung für den nächsten Hop Server konfigurieren unter Next Hop Server Name die Proxy-Appliance aus, und klicken Sie dann auf OK.

### So binden Sie den Citrix Gateway Next-Hop-Server an einen virtuellen Server

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration Citrix Gateway, und klicken Sie dann auf Virtuelle Server.
2. Wählen Sie im Detailbereich einen virtuellen Server aus und klicken Sie dann auf Öffnen.
3. Klicken Sie auf der Registerkarte Published Applications unter Next Hop Server auf ein Element und dann auf OK.

Sie können auch einen Next-Hop-Server über die Registerkarte Veröffentlichte Anwendungen hinzufügen.

## Citrix Gateway für den STA- und ICA-Verkehr konfigurieren

March 27, 2024

Wenn Sie Citrix Gateway in einer Double-Hop-DMZ bereitstellen, müssen Sie Citrix Gateway in der ersten DMZ so konfigurieren, dass die Kommunikation mit der Secure Ticket Authority (STA) und dem ICA-Verkehr angemessen verarbeitet wird. Der Server, auf dem die STA ausgeführt wird, kann entweder global oder an einen virtuellen Server gebunden sein.

Nachdem Sie die STA konfiguriert haben, können Sie die STA entweder global oder an einen virtuellen Server binden.

So konfigurieren und binden Sie die STA global:

1. Erweitern Sie in der GUI auf der Registerkarte Konfiguration **Citrix Gateway**, und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Server** auf **STA-Server binden/unbind, die von der Secure Ticket Authority verwendet werden sollen**.
3. Klicken Sie im Dialogfeld **STA-Server binden/aufheben** auf **Hinzufügen**.
4. Geben **Sie im Dialogfeld STA-Server konfigurieren** unter **URL**den Pfad zu dem Server ein, auf dem die STA ausgeführt wird, z. B. http://mycompany.com oder http://ipAddress, und klicken Sie dann auf **Erstellen**.

So konfigurieren und binden Sie die STA an einen virtuellen Server:

1. Erweitern Sie in der GUI auf der Registerkarte Konfiguration **Citrix Gateway**, und klicken Sie dann auf **Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen Server aus und klicken Sie dann auf **Öffnen**.
3. Klicken Sie auf der Registerkarte **Veröffentlichte Anwendungen** unter **Secure Ticket Authority** auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **STA-Server konfigurieren** unter URL den Pfad zu dem Server ein, auf dem die STA ausgeführt wird, z. B. http://mycompany.com oder http://ipAddress, und klicken Sie dann auf **Erstellen**.

**Hinweis:**

Wenn sich die virtuellen VPN-Server denselben virtuellen Next-Hop-Server und die STA-Server teilen, wird die Verbindung zurückgesetzt, wenn der gemeinsame STA-Server von einem virtuellen Server getrennt wird, der denselben virtuellen Server mit dem nächsten Hop teilt.

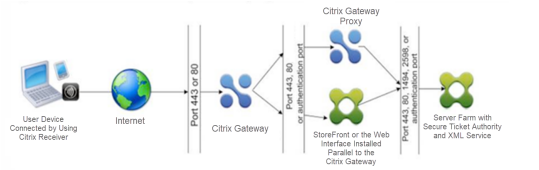
## Entsprechende Ports in Firewalls öffnen

March 27, 2024

Sie müssen sicherstellen, dass die entsprechenden Ports an den Firewalls geöffnet sind, um die verschiedenen Verbindungen zu unterstützen, die zwischen den verschiedenen Komponenten einer Double-Hop-DMZ-Bereitstellung auftreten. Weitere Informationen zum Verbindungsvorgang finden Sie unter Kommunikationsfluss in einer Double-Hop-DMZ-Bereitstellung.

Die folgende Abbildung zeigt gemeinsame Ports, die in einer Double-Hop-DMZ-Bereitstellung verwendet werden können.




Die folgende Tabelle zeigt die Verbindungen, die über die erste Firewall entstehen, und die Ports, die geöffnet sein müssen, um die Verbindungen zu unterstützen.

| Verbindungen durch die erste Firewall | Benutzte Ports |
|---|---|
| Der Webbrowser aus dem Internet stellt in der ersten DMZ eine Verbindung zu Citrix Gateway her. **Hinweis:** Citrix Gateway enthält eine Option zum Umleiten von Verbindungen, die an Port 80 hergestellt werden, an einen sicheren Port. Wenn Sie diese Option auf Citrix Gateway aktivieren, können Sie Port 80 über die erste Firewall öffnen. Wenn ein Benutzer eine unverschlüsselte Verbindung zu Citrix Gateway auf Port 80 herstellt, leitet Citrix Gateway die Verbindung automatisch an einen sicheren Port um. | Öffnen Sie den TCP-Port 443 durch die erste Firewall. |
| Die Citrix Workspace-App aus dem Internet stellt in der ersten DMZ eine Verbindung zu Citrix Gateway her. | Öffnen Sie den TCP-Port 443 durch die erste Firewall. |

Die folgende Tabelle zeigt die Verbindungen, die über die zweite Firewall entstehen, und die Ports, die geöffnet sein müssen, um die Verbindungen zu unterstützen.

| Verbindungen durch die zweite Firewall | Benutzte Ports |
|---|---|
| Citrix Gateway in der ersten DMZ stellt eine Verbindung zum Webinterface in der zweiten DMZ her. | Öffnen Sie entweder TCP-Port 80 für eine unsichere Verbindung oder TCP-Port 443 für eine sichere Verbindung durch die zweite Firewall. |
| Citrix Gateway in der ersten DMZ stellt eine Verbindung zu Citrix Gateway in der zweiten DMZ her. | Öffnen Sie den TCP-Port 443 für eine sichere SOCKS-Verbindung durch die zweite Firewall. |

| Verbindungen durch die zweite Firewall | Benutzte Ports |
| --- | --- |
| Wenn Sie die Authentifizierung auf Citrix Gateway in der ersten DMZ aktiviert haben, muss dieses Gerät möglicherweise eine Verbindung zu einem Authentifizierungsserver im internen Netzwerk herstellen. | Öffnen Sie den TCP-Port, an dem der Authentifizierungsserver auf Verbindungen wartet. Beispiele sind Port 1812 für RADIUS und Port 389 für LDAP. |

Die folgende Tabelle zeigt die Verbindungen, die über die dritte Firewall entstehen, und die Ports, die geöffnet sein müssen, um die Verbindungen zu unterstützen.

| Verbindungen durch die dritte Firewall | Benutzte Ports |
| --- | --- |
| StoreFront oder das Webinterface in der zweiten DMZ stellt eine Verbindung zum XML-Dienst her, der auf einem Server im internen Netzwerk gehostet wird. | Öffnen Sie entweder Port 80 für eine unsichere Verbindung oder Port 443 für eine sichere Verbindung durch die dritte Firewall. |
| StoreFront oder das Webinterface in der zweiten DMZ stellt eine Verbindung zur Secure Ticket Authority (STA) her, die auf einem Server im internen Netzwerk gehostet wird. | Öffnen Sie entweder Port 80 für eine unsichere Verbindung oder Port 443 für eine sichere Verbindung durch die dritte Firewall. |
| Citrix Gateway in der zweiten DMZ stellt eine Verbindung zur STA her, die sich im sicheren Netzwerk befindet. | Öffnen Sie entweder Port 80 für eine unsichere Verbindung oder Port 443 für eine sichere Verbindung durch die dritte Firewall. |
| Citrix Gateway stellt in der zweiten DMZ eine ICA-Verbindung zu einer veröffentlichten Anwendung oder einem virtuellen Desktop auf einem Server im internen Netzwerk her. | Öffnen Sie den TCP-Port 1494, um ICA-Verbindungen über die dritte Firewall zu unterstützen. Wenn Sie die Sitzungszuverlässigkeit in Citrix Virtual Apps aktiviert haben, öffnen Sie den TCP-Port 2598 anstelle von 1494. |
| Wenn Sie die Authentifizierung auf Citrix Gateway in der ersten DMZ aktiviert haben, muss dieses Gerät möglicherweise eine Verbindung zu einem Authentifizierungsserver im internen Netzwerk herstellen. | Öffnen Sie den TCP-Port, an dem der Authentifizierungsserver auf Verbindungen wartet. Beispiele sind Port 1812 für RADIUS und Port 389 für LDAP. |

## Pflege und Überwachung des Systems

March 27, 2024

Sobald Sie die Konfiguration Ihres Citrix Gateway abgeschlossen haben, müssen Sie das Gerät warten und überwachen. Sie können dies auf folgende Weise tun:

- Sie können Citrix Gateway auf die neueste Version der Software aktualisieren. Wenn Sie sich auf der Citrix Website anmelden, können Sie zur Citrix Gateway-Download-Site navigieren und die Software herunterladen. Die Readme für Wartungs-Builds finden Sie im Citrix Knowledge Center.
- Sie können Citrix Gateway-Konfigurations- und Verwaltungsaufgaben verschiedenen Mitgliedern Ihrer Gruppe zuweisen. Mit der delegierten Verwaltung können Sie Personen Zugriffsebenen zuweisen, die sie auf die Ausführung bestimmter Aufgaben auf Citrix Gateway beschränken.
- Sie können die Citrix Gateway-Konfiguration entweder auf dem Gerät oder in einer Datei auf Ihrem Computer speichern. Sie können die aktuell laufende und gespeicherte Konfiguration vergleichen. Sie können die Konfiguration auch von Citrix Gateway löschen.
- Sie können Benutzersitzungen im Citrix Gateway-Konfigurationsdienstprogramm anzeigen, aktualisieren und beenden.
- Sie können die Anmeldung auf Citrix Gateway konfigurieren. Die Protokolle enthalten wichtige Informationen über die Appliance und sind nützlich, falls Probleme auftreten.

## Delegierte Administratoren konfigurieren

March 27, 2024

Citrix Gateway hat einen Standardbenutzernamen und ein Standardkennwort für Administratoren. Der Standardbenutzername und das Standardkennwort lautet `nsroot`. Wenn Sie den Setup-Assistenten zum ersten Mal ausführen, können Sie das Administratorkennwort ändern.

Sie können weitere Administratorkonten erstellen und jedem Konto unterschiedliche Zugriffsebenen auf Citrix Gateway zuweisen. Diese zusätzlichen Konten werden als delegierte Administratoren bezeichnet. Beispielsweise haben Sie eine Person zur Überwachung von Citrix Gateway-Verbindungen und -Protokollen und eine andere Person, die für die Konfiguration bestimmter Einstellungen auf Citrix Gateway verantwortlich ist. Der erste Administrator hat schreibgeschützten Zugriff und der zweite Administrator hat eingeschränkten Zugriff auf die Appliance.

Um einen delegierten Administrator zu konfigurieren, verwenden Sie Befehlsrichtlinien sowie Systembenutzer und -gruppen.

Wenn Sie einen delegierten Administrator konfigurieren, lautet der Konfigurationsprozess wie folgt:

- Fügen Sie einen Systembenutzer hinzu. Ein Systembenutzer ist ein Administrator mit bestimmten Berechtigungen. Alle Administratoren erben die Richtlinien der Gruppen, zu denen sie gehören.
- Fügen Sie eine Systemgruppe hinzu. Eine Systemgruppe enthält Systembenutzer mit bestimmten Berechtigungen. Mitglieder der Systemgruppe erben die Richtlinien der Gruppe oder Gruppen, zu denen sie gehören.
- Erstellen Sie eine Befehlsrichtlinie. Mit Befehlsrichtlinien können Sie definieren, auf welche Teile der Citrix Gateway-Konfiguration ein Benutzer oder eine Gruppe zugreifen und diese ändern darf. Sie können auch festlegen, welche Befehle wie Befehlsgruppen, virtuelle Server und andere Elemente Administratoren und Gruppen konfigurieren dürfen.
- Binden Sie die Befehlsrichtlinie an den Benutzer oder die Gruppe, indem Sie die Priorität festlegen. Weisen Sie beim Konfigurieren der delegierten Verwaltung dem Administrator oder der Gruppe Prioritäten zu, damit Citrix Gateway bestimmen kann, welche Richtlinie Vorrang hat.

Citrix Gateway verfügt über eine standardmäßige Deny-Systembefehlsrichtlinie. Befehlsrichtlinien können nicht global gebunden werden. Binden Sie die Richtlinien direkt an Systemadministratoren (Benutzer) oder Gruppen. Wenn Benutzer und Gruppen keine zugeordnete Befehlsrichtlinie haben, wird die standardmäßige Verweigerungsrichtlinie angewendet, und Benutzer können keine Befehle ausführen oder Citrix Gateway konfigurieren.

Sie können benutzerdefinierte Befehlsrichtlinien konfigurieren, um eine größere Detailgenauigkeit für Benutzerrechtezuweisungen zu definieren. Beispielsweise können Sie einer Person die Möglichkeit geben, Sitzungsrichtlinien zu Citrix Gateway hinzuzufügen, dem Benutzer jedoch nicht erlauben, eine andere Konfiguration durchzuführen.

## Befehlsrichtlinien für delegierte Administratoren konfigurieren

March 27, 2024

Citrix Gateway verfügt über vier integrierte Befehlsrichtlinien, die Sie für die delegierte Verwaltung verwenden können:

- **Schreibgeschützt** ermöglicht den schreibgeschützten Zugriff, um alle Befehle mit Ausnahme der Systembefehlsgruppe und der Befehle `ns.conf show` anzuzeigen.
- **Der Bediener** ermöglicht den schreibgeschützten Zugriff und ermöglicht auch den Zugriff zum Aktivieren und Deaktivieren von Befehlen für Dienste. Diese Richtlinie ermöglicht auch den Zugriff, um Dienste und Server als "Zugriff nach unten"festzulegen.
- Das**Netzwerk** ermöglicht fast vollständigen Systemzugriff, ohne Systembefehle und den Shell-Befehl.

- **Superuser** gewährt vollständige Systemberechtigungen, wie die dem Standardadministrator gewährten Berechtigungen `nsroot`.

Befehlsrichtlinien enthalten integrierte Ausdrücke. Verwenden Sie das Konfigurationsdienstprogramm, um Systembenutzer, Systemgruppen, Befehlsrichtlinien zu erstellen und Berechtigungen zu definieren.

### So erstellen Sie einen Administratorbenutzer auf Citrix Gateway

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich auf der Registerkarte **KonfigurationSystem**>**Benutzerverwaltung**, und klicken Sie dann auf**Systembenutzer**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie **unter Benutzername**einen Benutzernamen ein.
4. Geben Sie in die Felder **Kennwortund Kennwort bestätigen** das Kennwort ein.
5. Um Benutzer zu einer Gruppe hinzuzufügen, klicken Sie **unter Mitglied von**auf **Hinzufügen**.
6. Wählen Sie unter **Verfügbar**eine Gruppe aus und klicken Sie dann auf den Pfeil nach rechts.
7. Klicken Sie auf **Befehlsrichtlinien > Aktion > Einfügen**.
8. Wählen Sie im Dialogfeld Befehlsrichtlinien einfügen den Befehl aus und klicken Sie auf **OK > Erstellen > Schließen**.

### Erstellen von Administratorgruppen

Administrative Gruppen enthalten Benutzer, die über Administratorrechte für Citrix Gateway verfügen. Sie können im Konfigurationsdienstprogramm Administratorgruppen erstellen.

#### So konfigurieren Sie eine Administratorgruppe mithilfe des Konfigurationsdienstprogramms

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich auf der Registerkarte **KonfigurationSystem**>**Benutzerverwaltung**, und klicken Sie dann auf**Systemgruppen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie **unter Gruppenname**einen Namen für die Gruppe ein.
4. Um einen vorhandenen Benutzer zur Gruppe hinzuzufügen, klicken Sie in **Mitglieder**auf **Hinzufügen**.
5. Wählen Sie unter **Verfügbar**einen Benutzer aus und klicken Sie dann auf den Pfeil nach rechts.
6. Klicken Sie unter **Befehlsrichtlinien**in **Aktion**auf **Einfügen**, wählen Sie eine Richtlinie oder Richtlinien aus, klicken Sie auf **OK**, klicken Sie auf **Erstellen** und dann auf **Schließen**.

# Benutzerdefinierte Befehlsrichtlinien für delegierte Administratoren konfigurieren

March 27, 2024

Beim Konfigurieren einer benutzerdefinierten Befehlsrichtlinie geben Sie einen Richtliniennamen an und konfigurieren dann die Richtlinienkomponenten, um die Befehlsspezifikation zu erstellen. Mit der Befehlsspezifikation können Sie die Befehle einschränken, die Administratoren verwenden dürfen. Beispielsweise möchten Sie Administratoren die Möglichkeit verweigern, den Befehl remove zu verwenden. Stellen Sie beim Konfigurieren der Richtlinie die Aktion auf Verweigern ein und konfigurieren Sie dann die Parameter.

Sie können eine einfache oder erweiterte Befehlsrichtlinie konfigurieren. Wenn Sie eine einfache Richtlinie konfigurieren, konfigurieren Sie eine Komponente auf der Appliance, wie Citrix Gateway und Authentifizierung. Wenn Sie eine erweiterte Richtlinie konfigurieren, wählen Sie die Komponente aus, die als Entitätsgruppe bezeichnet wird, und wählen dann die Befehle aus, die Administratoren in der Gruppe ausführen dürfen.

## So erstellen Sie eine einfache benutzerdefinierte Befehlsrichtlinie

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **System** > **Benutzerverwaltung**, und klicken Sie dann auf **Befehlsrichtlinien.**
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. Geben Sie **unter Richtlinienname**einen Namen für die Richtlinie ein.
4. Wählen Sie unter **Aktion** die Option **Zulassen** oder **Verweigern** aus.
5. Klicken Sie unter **Befehlsspezifikation**auf **Hinzufügen**.
6. Wählen **Sie im Dialogfeld Befehl hinzufügen** auf der Registerkarte **Einfach** unter Operation die Aktion aus, die delegierte Administratoren ausführen können.
7. Wählen Sie unter **Entity Group**eine oder mehrere Gruppen aus.

   Sie können die STRG-Taste drücken, um mehrere Gruppen auszuwählen.
8. Klicken Sie auf **Create** und dann auf **Close**.

## So erstellen Sie eine erweiterte benutzerdefinierte Befehlsrichtlinie

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich auf der Registerkarte **KonfigurationSystem**>**Benutzerverwaltung**, und klicken Sie dann auf**Befehlsrichtlinien**.

2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie **unter Richtlinienname**einen Namen für die Richtlinie ein.
4. Wählen Sie unter **Aktion** die Option **Zulassen** oder **Verweigern** aus.
5. Klicken Sie unter **Befehlsspezifikation**auf **Hinzufügen**.
6. Klicken **Sie im Dialogfeld Befehl hinzufügen** auf die Registerkarte **Erweitert**.
7. Wählen Sie in **Entity Group** die Gruppe aus, zu der der Befehl gehört, eine solche Authentifizierung oder Hochverfügbarkeit.
8. Wählen Sie unter **Entity**die Richtlinie aus.

   Sie können die STRG-Taste drücken, um mehrere Elemente in der Liste auszuwählen.
9. Wählen Sie unter **Operation**den Befehl aus, klicken Sie auf **Erstellen** und dann auf **Schließen**.

   Sie können die STRG-Taste drücken, um mehrere Elemente in der Liste auszuwählen.
10. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
11. Klicken **Sie im Dialogfeld Befehlsrichtlinieerstellen auf Erstellen**und dann auf**Schließen**.

Wenn Sie auf **Erstellen**klicken, wird der Ausdruck unter Befehlsspezifikation im Dialogfeld **Befehlsrichtlinie erstellen** angezeigt.

Nachdem Sie die benutzerdefinierte Befehlsrichtlinie erstellt haben, können Sie sie an einen Benutzer oder eine Gruppe binden.

> **Hinweis:** Sie können benutzerdefinierte Befehlsrichtlinien nur an die Benutzer oder Gruppen binden, die Sie erstellen. Sie können eine benutzerdefinierte Befehlsrichtlinie nicht an den Benutzer binden `nsroot`.

### So binden Sie eine benutzerdefinierte Befehlsrichtlinie an einen Benutzer oder eine Gruppe

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **System** > **Benutzerverwaltung**, und klicken Sie dann auf **Systembenutzer** oder klicken Sie auf **Systemgruppen**.
2. Wählen Sie im Detailbereich einen Benutzer oder eine Gruppe aus der Liste aus und klicken Sie dann auf **Öffnen**.
3. Wählen Sie unter **Befehlsrichtlinien**die Richtlinie aus und klicken Sie dann auf **OK**.

# Überwachung auf Citrix Gateway konfigurieren

March 27, 2024

Mit Citrix Gateway können Sie die Status- und Statusinformationen protokollieren, die das Gerät sammelt. Sie können die Audit-Protokolle verwenden, um den Ereignisverlauf in chronologischer Reihenfolge anzuzeigen. Die Nachrichten in den Protokollen enthalten Informationen über das Ereignis, das die Nachricht generiert hat, einen Zeitstempel, den Nachrichtentyp sowie vordefinierte Protokollierungen und Nachrichteninformationen. Sie können Einstellungen konfigurieren, die die protokollierten Informationen und den Speicherort der Nachrichten bestimmen.

Citrix Gateway unterstützt derzeit 2 Protokollformate: ein proprietäres Protokollformat für lokale Protokolle und das Syslog-Format für die Verwendung mit Syslog-Servern. Sie können die Überwachungsprotokolle so konfigurieren, dass sie die folgenden Informationen bereitstellen:

| Ebene | Beschreibung |
|---|---|
| EMERGENCY | Protokolliert nur größere Fehler. Einträge im Protokoll zeigen an, dass bei Citrix Gateway ein kritisches Problem auftritt, das dazu führt, dass es unbrauchbar wird. |
| ALERT | Protokolliert Probleme, die dazu führen können, dass Citrix Gateway falsch funktioniert, aber für seinen Betrieb nicht kritisch sind. Es können so schnell wie möglich Korrekturmaßnahmen ergriffen werden, um zu verhindern, dass bei Citrix Gateway ein kritisches Problem auftritt. |
| CRITICAL | Protokolliert kritische Bedingungen, die den Betrieb von Citrix Gateway nicht einschränken, aber möglicherweise zu einem größeren Problem eskalieren. |
| ERROR | Protokolliert Einträge, die aus einer fehlgeschlagenen Operation auf Citrix Gateway resultieren. |
| WARNING | Protokolliert potenzielle Probleme, die zu einem Fehler oder einem kritischen Fehler führen können. |
| NOTICE | Protokolliert ausführlichere Probleme als das Protokoll auf Informationsebene, dient jedoch demselben Zweck wie die Benachrichtigung. |

| Ebene | Beschreibung |
| --- | --- |
| INFORMATIONEN | Protokollieren Sie von Citrix Gateway durchgeführten Aktionen. Dieses Level ist nützlich für die Fehlerbehebung bei Problemen. |

Das Citrix Gateway-Überwachungsprotokoll speichert auch Komprimierungsstatistiken für Citrix Gateway, wenn Sie die TCP-Komprimierung konfigurieren. Das für verschiedene Daten erzielte Komprimierungsverhältnis wird für jede Benutzersitzung in der Protokolldatei gespeichert.

Citrix Gateway verwendet die Protokollsignatur sessionID. Auf diese Weise können Sie Protokolle pro Sitzung und nicht pro Benutzer verfolgen. Protokolle, die im Rahmen einer Sitzung generiert werden, haben dieselbe sessionID. Wenn ein Benutzer zwei Sitzungen von demselben Benutzergerät mit derselben IP-Adresse einrichtet, hat jede Sitzung eine eindeutige SessionID.

> **Wichtig:** Wenn Sie benutzerdefinierte Log-Parsing-Skripte geschrieben haben, müssen Sie diese Signaturänderung innerhalb der benutzerdefinierten Parsing-Skripte vornehmen.

## Protokolle auf Citrix Gateway konfigurieren

March 27, 2024

Wenn Sie die Anmeldung auf Citrix Gateway konfigurieren, können Sie die Überwachungsprotokolle auf Citrix Gateway speichern oder an einen Syslog-Server senden. Sie verwenden das Konfigurationsdienstprogramm, um Überwachungsrichtlinien zu erstellen und Einstellungen zum Speichern der Überwachungsprotokolle zu konfigurieren.

### So erstellen Sie eine Auditing-Richtlinie

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration **Citrix Gateway** > **Richtlinien** > **Überwachung**.
2. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
3. Wählen Sie eine Option aus:
    - Syslog, wenn Sie die Protokolle an einen Syslog-Server senden möchten.
    - `Nslog` um die Protokolle auf Citrix Gateway zu speichern.

> **Hinweis:** Wenn Sie diese Option wählen, werden Protokolle im Ordner /var/log auf der Appliance gespeichert.

4. Klicken Sie im Detailbereich auf **Hinzufügen**.
5. Geben Sie die folgenden Informationen für die Serverinformationen ein, auf denen die Protokolle gespeichert sind:
   - Geben Sie unter Name den Namen des Servers ein.
   - Geben Sie unter Server den Namen oder die IP-Adresse des Protokollservers ein.
6. Klicken Sie auf Erstellen und dann auf Schließen.

Nachdem Sie die Überwachungsrichtlinie erstellt haben, können Sie die Richtlinie an eine beliebige Kombination der folgenden Elemente binden:

- Weltweit
- Virtuelle Server
- Gruppen
- Benutzer

### So binden Sie eine Auditing-Richtlinie global

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration **Citrix Gateway** > **Richtlinien** > **Überwachung**.
2. Wählen Sie entweder **`Syslog`** oder **`Nslog`**.
3. Klicken Sie im Detailbereich auf **Aktion** und dann auf **Globale Bindungen**.
4. Klicken **Sie im Dialogfeld Überwachungsrichtlinien an**Global**binden/aufheben** unter **Details**auf **Richtlinie einfügen**.
5. Wählen Sie unter **Richtliniennameeine** Richtlinie aus und klicken Sie dann auf **OK**.

### So ändern Sie eine Auditing-Richtlinie

Sie können eine vorhandene Überwachungsrichtlinie ändern, um den Server zu ändern, an den die Protokolle gesendet werden.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte **KonfigurationCitrix Gateway**>**Richtlinien**>**Überwachung**
2. Wählen Sie entweder **`Syslog`** oder **`Nslog`**.
3. Klicken Sie im Detailbereich auf eine Richtlinie und dann auf **Öffnen**.
4. Wählen Sie unter Server den neuen Server aus, und klicken Sie dann auf **OK**.

### So entfernen Sie eine Auditing-Richtlinie

Sie können eine Überwachungsrichtlinie von Citrix Gateway entfernen. Wenn Sie eine Überwachungsrichtlinie entfernen, wird die Richtlinie automatisch ungebunden.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration **Citrix Gateway** > **Richtlinien** > **Überwachung**.
2. Wählen Sie entweder **Syslog** oder **Nslog**.
3. Klicken Sie im Detailbereich auf eine Richtlinie und dann auf **Entfernen**.

## ACL-Protokollierung konfigurieren

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass Details für Pakete protokolliert werden, die einer erweiterten Zugriffssteuerungsliste (ACL) entsprechen. Zusätzlich zum ACL-Namen enthalten die protokollierten Details paketspezifische Informationen wie die Quell- und Ziel-IP-Adressen. Die Informationen werden entweder in einem Syslog oder einer `nslog` Datei gespeichert, abhängig von der Art der Protokollierung (syslog oder `nslog`), die Sie aktivieren.

Sie können die Protokollierung sowohl auf globaler als auch auf ACL-Ebene aktivieren. Um die Protokollierung auf ACL-Ebene zu aktivieren, müssen Sie sie jedoch auch auf globaler Ebene aktivieren. Die globale Einstellung hat Vorrang.

Um die Protokollierung zu optimieren, werden nur die Details des ersten Pakets protokolliert, wenn mehrere Pakete aus demselben Fluss mit einer ACL übereinstimmen. Der Zähler wird für jedes andere Paket erhöht, das zum selben Flow gehört. Ein Flow ist definiert als eine Reihe von Paketen, die dieselben Werte für die folgenden Parameter haben:

- Quell-IP
- Ziel-IP
- Quell-Port
- Destination port
- Protokoll (TCP oder UDP)

Wenn das Paket nicht aus demselben Fluss stammt oder wenn die Zeitdauer die mittlere Zeit überschreitet, wird ein neuer Fluss erstellt. Die mittlere Zeit ist die Zeit, in der Pakete desselben Flusses keine zusätzlichen Nachrichten generieren (obwohl der Zähler erhöht wird).

> **Hinweis:** Die Gesamtzahl der verschiedenen Flows, die zu einem bestimmten Zeitpunkt protokolliert werden können, ist auf 10.000 begrenzt.

In der folgenden Tabelle werden die Parameter beschrieben, mit denen Sie die ACL-Protokollierung auf Regelebene für erweiterte ACLs konfigurieren können.

| Parametername | Beschreibung |
| --- | --- |
| `Logstate` | Status der Protokollierungsfunktion für die ACL. Mögliche Werte: ENABLED und DISABLED. Standard: DISABLED. |
| `Ratelimit` | Anzahl der Protokollmeldungen, die eine bestimmte ACL generieren kann. Standardwert: 100. |

### So konfigurieren Sie die ACL-Protokollierung mithilfe des Konfigurationsdienstprogramms

Sie können die Protokollierung für eine ACL konfigurieren und die Anzahl der Protokollmeldungen angeben, die die Regel generieren kann.

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich **System** > **Netzwerk** und klicken Sie dann auf ACLs.
2. Klicken Sie im Detailbereich auf die Registerkarte **Erweiterte ACLs** und dann auf Hinzufügen.
3. Geben Sie im Dialogfeld **Erweiterte ACL erstellen** in das Feld Name einen Namen für die Richtlinie ein.
4. Aktivieren Sie das Kontrollkästchen **Log State**.
5. Geben Sie im Textfeld **Log Rate Limit** die Ratenbegrenzung ein, die Sie für die Regel angeben möchten, und klicken Sie dann auf **Erstellen**.

Nachdem Sie die ACL-Protokollierung konfiguriert haben, können Sie sie auf Citrix Gateway aktivieren. Erstellen Sie eine Überwachungsrichtlinie und binden Sie sie dann an einen Benutzer, eine Gruppe, einen virtuellen Server oder global.

### So aktivieren Sie die ACL- oder TCP-Anmeldung auf Citrix Gateway

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich **Citrix Gateway** > **Richtlinien** > **Überwachung**.
2. Wählen Sie entweder syslog oder `nslog`.
3. Klicken Sie auf der Registerkarte **Server** auf **Hinzufügen**.
4. Geben **Sie im Dialogfeld Überwachungsserver erstellen** in das Feld **Name**einen Namen für den Server ein, und konfigurieren Sie dann die Servereinstellungen.
5. Klicken Sie auf **ACL-Protokollierung** oder **TCP-Protokollierung** und dann auf **Erstellen**.

# Aktivieren der Citrix Gateway Plug-in-Protokollierung

March 27, 2024

Sie können das Citrix Gateway-Plug-in so konfigurieren, dass alle Fehler in Textdateien protokolliert werden, die auf dem Benutzergerät gespeichert sind. Benutzer können das Citrix Gateway-Plug-in so konfigurieren, dass die Anmeldestufe auf dem Benutzergerät festgelegt wird, um bestimmte Benutzeraktivitäten aufzuzeichnen. Wenn Benutzer die Protokollierung konfigurieren, erstellt das Plug-In die folgenden zwei Dateien auf dem Benutzergerät:

- hooklog<num>.txt, das Abfangmeldungen protokolliert, die das Citrix Gateway Plug-in generiert.
- nssslvpn.txt, das Fehler mit dem Plug-In auflistet.

> **Hinweis:** Die Dateien hooklog.txt werden nicht automatisch gelöscht. Citrix empfiehlt, die Dateien regelmäßig zu löschen.

Benutzerprotokolle sind in den folgenden Verzeichnissen in Windows auf dem Benutzergerät:

- Windows XP (all users): %SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP (user-specific): %SystemDrive%:\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 7 (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7 (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8 (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 8 (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE

Sie können diese Protokolldateien verwenden, um das Citrix Gateway Plug-in zu beheben. Benutzer können die Protokolldateien per E-Mail an den Technischen Support senden.

Im Dialogfeld Konfiguration können Benutzer die Protokollierungsstufe für das Citrix Gateway Plug-in festlegen. Die Protokollierungsebenen sind:

- Aufzeichnen von Fehlermeldungen
- Aufzeichnen von Ereignisnachrichten
- Aufzeichnen von Citrix Gateway Plug-In-Statistiken
- Alle Fehler, Ereignismeldungen und Statistiken aufzeichnen

Weitere Informationen zur Protokollierungsfunktion des Citrix Secure Access Clients für Windows finden Sie unter Verbesserte Protokollerfassung für den Windows-Client.

## Überwachen von ICA-Verbindungen

March 27, 2024

Sie können aktive Benutzersitzungen auf Ihrer Serverfarm mithilfe des Dialogfelds ICA-Verbindungen überwachen. Dieses Dialogfeld enthält die folgenden Informationen:

- Benutzername der Person, die sich mit der Serverfarm verbindet
- Domänenname der Serverfarm
- IP-Adresse des Benutzergeräts
- Portnummer des Benutzergeräts
- IP-Adresse des Servers, auf dem Citrix Virtual Apps and Desktops ausgeführt wird
- Portnummer des Servers, auf dem Citrix Virtual Apps and Desktops ausgeführt wird

1. Klicken Sie im Konfigurationsdienstprogramm im Navigationsbereich auf Citrix ADC Gateway.
2. Klicken Sie im Detailbereich unter Verbindungen überwachen auf ICA-Verbindungen, um das Überwachungsdialogfeld anzuzeigen.

## Authentifizierung und Autorisierung

March 27, 2024

Citrix Gateway verwendet ein flexibles Authentifizierungsdesign, das eine umfassende Anpassung der Benutzerauthentifizierung für Citrix Gateway ermöglicht. Sie können Authentifizierungsserver nach Industriestandard verwenden und Citrix Gateway für die Authentifizierung von Benutzern bei den Servern konfigurieren. Citrix Gateway unterstützt auch die Authentifizierung basierend auf Attributen in einem Clientzertifikat. Die Citrix Gateway-Authentifizierung wurde entwickelt, um einfache Authentifizierungsverfahren zu ermöglichen, die eine einzige Quelle für die Benutzerauthentifizierung verwenden, und komplexere, kaskadierte Authentifizierungsverfahren, die auf mehreren Authentifizierungstypen basieren.

Die Citrix Gateway-Authentifizierung beinhaltet die lokale Authentifizierung für die Erstellung lokaler Benutzer und Gruppen. Bei diesem Entwurf geht es um die Verwendung von Richtlinien zur Steuerung der von Ihnen konfigurierten Authentifizierungsverfahren. Die von Ihnen erstellten Richtlinien können auf globalen oder virtuellen Serverebenen von Citrix Gateway angewendet werden und können verwendet werden, um Authentifizierungsserverparameter basierend auf dem Quellnetzwerk des Benutzers bedingt festzulegen.

Da Richtlinien entweder global oder an einen virtuellen Server gebunden sind, können Sie Ihren Richtlinien auch Prioritäten zuweisen, um im Rahmen der Authentifizierung eine Kaskade mehrerer

Authentifizierungsserver zu erstellen.

Citrix Gateway bietet Unterstützung für die folgenden Authentifizierungstypen.

- Lokal
- Lightweight Directory Access Protocol (LDAP)
- RADIUS
- SAML
- TACACS+
- Clientzertifikatauthentifizierung (einschließlich Smartcard-Authentifizierung)

Citrix Gateway unterstützt auch RSA SecurID, Gemalto Protiva und SafeWord. Sie verwenden einen RADIUS-Server, um diese Authentifizierungstypen zu konfigurieren.

Während die Authentifizierung es Benutzern ermöglicht, sich bei Citrix Gateway anzumelden und eine Verbindung zum internen Netzwerk herzustellen, definiert die Autorisierung die Ressourcen innerhalb des sicheren Netzwerks, auf die Benutzer Zugriff haben. Sie konfigurieren die Autorisierung mit LDAP- und RADIUS-Richtlinien.

## Globale Standardauthentifizierungstypen konfigurieren

March 27, 2024

Wenn Sie Citrix Gateway installiert und den Citrix Gateway-Assistenten ausgeführt haben, haben Sie die Authentifizierung innerhalb des Assistenten konfiguriert. Diese Authentifizierungsrichtlinie ist automatisch an die globale Ebene von Citrix Gateway gebunden. Der Authentifizierungstyp, den Sie im Citrix Gateway-Assistenten konfigurieren, ist der Standardauthentifizierungstyp. Sie können den Standardautorisierungstyp ändern, indem Sie den Citrix Gateway-Assistenten erneut ausführen, oder Sie können die globalen Authentifizierungseinstellungen im Konfigurationsdienstprogramm ändern.

Wenn Sie zusätzliche Authentifizierungstypen hinzufügen müssen, können Sie Authentifizierungsrichtlinien auf Citrix Gateway konfigurieren und die Richtlinien mithilfe des Konfigurationsdienstprogramms an Citrix Gateway binden. Wenn Sie die Authentifizierung global konfigurieren, definieren Sie die Art der Authentifizierung, konfigurieren die Einstellungen und legen die maximale Anzahl von Benutzern fest, die authentifiziert werden können.

Nachdem Sie die Richtlinie konfiguriert und gebunden haben, können Sie die Priorität festlegen, um zu definieren, welcher Authentifizierungstyp Vorrang hat. Beispielsweise konfigurieren Sie LDAP- und RADIUS-Authentifizierungsrichtlinien. Wenn die LDAP-Richtlinie eine Prioritätsnummer von 10 hat und die RADIUS-Richtlinie eine Prioritätsnummer von 15 hat, hat die LDAP-Richtlinie Vorrang, unab-

hängig davon, wo Sie die einzelnen Richtlinien binden. Dies wird als kaskadierende Authentifizierung bezeichnet.

Sie können Anmeldeseiten aus dem In-Memory-Cache von Citrix Gateway oder vom HTTP-Server bereitstellen, der auf Citrix Gateway ausgeführt wird. Wenn Sie die Anmeldeseite aus dem In-Memory-Cache bereitstellen, ist die Bereitstellung der Anmeldeseite von Citrix Gateway erheblich schneller als vom HTTP-Server. Die Entscheidung, die Anmeldeseite aus dem In-Memory-Cache bereitzustellen, reduziert die Wartezeit, wenn sich eine große Anzahl von Benutzern gleichzeitig anmeldet. Sie können die Bereitstellung von Anmeldeseiten aus dem Cache nur als Teil einer globalen Authentifizierungsrichtlinie konfigurieren.

Sie können auch die IP-Adresse der Netzwerkadressübersetzung (NAT) konfigurieren, bei der es sich um eine bestimmte IP-Adresse für die Authentifizierung handelt. Diese IP-Adresse ist für die Authentifizierung eindeutig und nicht das Citrix Gateway-Subnetz, zugeordnete oder virtuelle IP-Adressen. Dies ist eine optionale Einstellung.

**Hinweis**: Sie können den Citrix Gateway-Assistenten nicht zum Konfigurieren der SAML-Authentifizierung verwenden.

Sie können den Schnellkonfigurations-Assistenten verwenden, um die LDAP-, RADIUS- und Clientzertifikatauthentifizierung zu konfigurieren. Wenn Sie den Assistenten ausführen, können Sie aus einem vorhandenen LDAP- oder RADIUS-Server auswählen, der auf Citrix Gateway konfiguriert ist. Sie können die Einstellungen auch für LDAP oder RADIUS konfigurieren. Wenn Sie die Zwei-Faktor-Authentifizierung verwenden, empfiehlt Citrix die Verwendung von LDAP als primären Authentifizierungstyp.

### So konfigurieren Sie die Authentifizierung global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungen auf Authentifizierungseinstellungen ändern.
3. Geben Sie im Feld Maximale Anzahl an Benutzerndie Anzahl der Benutzer ein, die mit diesem Authentifizierungstyp authentifiziert werden können.
4. Geben Sie im Feld NAT-IP-Adressedie eindeutige IP-Adresse für die Authentifizierung ein.
5. Wählen SieStatisches Caching aktivieren aus, um Anmeldeseiten schneller bereitzustellen.
6. Wählen Sie Erweitertes Authentifizierungsfeedback aktivieren aus, um Benutzern eine Nachricht zu senden, falls die Authentifizierung fehlschlägt Die Nachricht, die Benutzer erhalten, enthält Kennwortfehler, Konto deaktiviert oder gesperrt, oder der Benutzer wurde nicht gefunden, um nur einige zu nennen.
7. Wählen Sie unter Standard-Authentifizierungstypden Authentifizierungstyp aus.
8. Konfigurieren Sie die Einstellungen für Ihren Authentifizierungstyp und klicken Sie dann auf OK.

## Authentifizierung ohne Autorisierung konfigurieren

March 27, 2024

Die Autorisierung definiert die Ressourcen, mit denen Benutzer über Citrix Gateway eine Verbindung herstellen dürfen. Sie konfigurieren Autorisierungsrichtlinien, indem Sie einen Ausdruck verwenden und dann festlegen, dass die Richtlinie zulässig oder verweigert wird. Sie können Citrix Gateway so konfigurieren, dass nur Authentifizierung ohne Autorisierung verwendet wird.

Wenn Sie die Authentifizierung ohne Autorisierung konfigurieren, führt Citrix Gateway keine Gruppenautorisierungsprüfung durch. Die Richtlinien, die Sie für den Benutzer oder die Gruppe konfigurieren, werden dem Benutzer zugewiesen.

Weitere Informationen zum Konfigurieren der Autorisierung finden Sie unter Konfigurieren der Autorisierung.

## Autorisierung konfigurieren

March 27, 2024

Die Autorisierung gibt die Netzwerkressourcen an, auf die Benutzer Zugriff haben, wenn sie sich bei Citrix Gateway anmelden. Die Standardeinstellung für die Autorisierung besteht darin, den Zugriff auf alle Netzwerkressourcen zu verweigern. Citrix empfiehlt, die globale Standardeinstellung zu verwenden und dann Autorisierungsrichtlinien zu erstellen, um die Netzwerkressourcen zu definieren, auf die Benutzer zugreifen können.

Sie konfigurieren die Autorisierung auf Citrix Gateway mithilfe einer Autorisierungsrichtlinie und Ausdrücken. Nachdem Sie eine Autorisierungsrichtlinie erstellt haben, können Sie sie an die Benutzer oder Gruppen binden, die Sie auf der Appliance konfiguriert haben.

## Autorisierungsrichtlinien konfigurieren

March 27, 2024

Wenn Sie eine Autorisierungsrichtlinie konfigurieren, können Sie festlegen, dass sie den Zugriff auf Netzwerkressourcen im internen Netzwerk erlaubt oder verweigert. Verwenden Sie beispielsweise den folgenden Ausdruck, um Benutzern Zugriff auf das 10.3.3.0-Netzwerk zu gewähren:

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Autorisierungsrichtlinien werden auf Benutzer und Gruppen angewendet. Nachdem ein Benutzer authentifiziert wurde, führt Citrix Gateway eine Gruppenautorisierungsprüfung durch, indem die Gruppeninformationen des Benutzers entweder von einem RADIUS-, LDAP- oder TACACS+-Server abgerufen werden. Wenn Gruppeninformationen für den Benutzer verfügbar sind, überprüft Citrix Gateway die für die Gruppe zulässigen Netzwerkressourcen.

Um zu steuern, auf welche Ressourcen Benutzer zugreifen können, müssen Sie Autorisierungsrichtlinien erstellen. Wenn Sie keine Autorisierungsrichtlinien erstellen müssen, können Sie die globale Standardermächtigung konfigurieren.

Wenn Sie innerhalb der Autorisierungsrichtlinie einen Ausdruck erstellen, der den Zugriff auf einen Dateipfad verweigert, können Sie nur den Pfad des Unterverzeichnisses und nicht das Stammverzeichnis verwenden. Verwenden Sie zum Beispiel fs.path enthält "\\ dir1\\ dir2"anstelle von fs.path enthält "\\ rootdir\\ dir1\\ dir2". Wenn Sie in diesem Beispiel die zweite Version verwenden, schlägt die Richtlinie fehl.

Nachdem Sie die Autorisierungsrichtlinie konfiguriert haben, binden Sie sie an einen Benutzer oder eine Gruppe, wie in den folgenden Aufgaben gezeigt.

Standardmäßig werden Autorisierungsrichtlinien zuerst anhand von Richtlinien validiert, die Sie an den virtuellen Server binden, und dann gegen global gebundene Richtlinien. Wenn Sie eine Richtlinie global binden und möchten, dass die globale Richtlinie Vorrang vor einer Richtlinie hat, die Sie an einen Benutzer, eine Gruppe oder einen virtuellen Server binden, können Sie die Prioritätsnummer der Richtlinie ändern. Prioritätszahlen beginnen bei Null. Eine niedrigere Prioritätszahl gibt der Richtlinie eine höhere Priorität.

Wenn die globale Richtlinie beispielsweise eine Prioritätsnummer von eins hat und der Benutzer eine Priorität von zwei hat, wird zuerst die globale Authentifizierungsrichtlinie angewendet.

> **Wichtig:**
>
> - Klassische Autorisierungsrichtlinien werden nur auf TCP-Verkehr angewendet.
> - Erweiterte Autorisierungsrichtlinie kann auf alle Arten von Datenverkehr (TCP/UDP/ICMP/DNS) angewendet werden.
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if "type"is not explicitly mentioned or "type"is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Weitere Einzelheiten zu erweiterten Autorisierungsrichtlinien finden Sie im Artikel https://support.ci

trix.com/article/CTX232237.

### Beispiele für Ausdrücke für Autorisierungsrichtlinien

Im Folgenden finden Sie Ausdrucksbeispiele für Autorisierungsrichtlinien:

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\" allowedGroup\")"ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(10.102.75.10,10.1 "DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\" portal-srv")|| CLIENT.IP.DST.IN_SUBNET(10.102.75.0/25)"ALLOW`

### So konfigurieren Sie eine Autorisierungsrichtlinie über die GUI

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Autorisierung.**
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Wählen Sie unter **Aktion** die Option **Zulassen** oder **Verweigern** aus.
5. Klicken Sie in **Expression** auf **Expression Editor**.
6. Um mit der Konfiguration des Ausdrucks zu beginnen, klicken Sie auf **Auswählen** und wählen Sie die erforderlichen Elemente aus.
7. Klicken Sie auf **Fertig**, wenn Ihr Ausdruck vollständig ist.
8. Klicken Sie auf **Erstellen**.

### So binden Sie eine Autorisierungsrichtlinie über die GUI an einen Benutzer

1. Navigieren Sie zu **Citrix Gateway > Benutzerverwaltung.**
2. Klicken Sie auf **AAA-Benutzer**.
3. Wählen Sie im Detailbereich einen Benutzer aus und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie in **Erweiterte Einstellungen**auf **Autorisierungsrichtlinien**.
5. Wählen Sie auf der Seite **Policy Binding** eine Richtlinie aus oder erstellen Sie eine Richtlinie.
6. Legen Sie unter **Priorität**die Prioritätsnummer fest.
7. Wählen Sie unter **Typ**den Anforderungstyp aus und klicken Sie dann auf **OK**.

### So binden Sie eine Autorisierungsrichtlinie über die GUI an eine Gruppe

1. Navigieren Sie zu **Citrix Gateway > Benutzerverwaltung**.

2. Klicken Sie auf **AAA-Gruppen**.
3. Wählen Sie im Detailbereich eine Gruppe aus und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie in **Erweiterte Einstellungen**auf **Autorisierungsrichtlinien**.
5. Wählen Sie auf der Seite **Policy Binding** eine Richtlinie aus oder erstellen Sie eine Richtlinie.
6. Legen Sie unter **Priorität**die Prioritätsnummer fest.
7. Wählen Sie unter **Typ**den Anforderungstyp aus und klicken Sie dann auf **OK**.

## Globale Standardermächtigung konfigurieren

January 29, 2024

Um die Ressourcen zu definieren, auf die Benutzer Zugriff im internen Netzwerk haben, können Sie die globale Standardermächtigung konfigurieren. Sie konfigurieren die globale Autorisierung, indem Sie den Zugriff auf Netzwerkressourcen global im internen Netzwerk zulassen oder verweigern.

Jede globale Autorisierungsaktion, die Sie erstellen, wird auf alle Benutzer angewendet, denen weder direkt noch über eine Gruppe eine Autorisierungsrichtlinie zugeordnet ist. Eine Benutzer- oder Gruppenautorisierungsrichtlinie überschreibt immer die globale Autorisierungsaktion. Wenn die Standardautorisierungsaktion auf Verweigern festgelegt ist, müssen Sie Autorisierungsrichtlinien für alle Benutzer oder Gruppen anwenden, um Netzwerkressourcen für diese Benutzer oder Gruppen zugänglich zu machen. Diese Anforderung trägt zur Verbesserung der Sicherheit bei.

So legen Sie die globale Standardermächtigung fest:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Wählen Sie auf der Registerkarte Sicherheit neben Standardermächtigungsaktion die Option Zulassen oder Verweigern aus und klicken Sie auf OK.

## Authentifizierung deaktivieren

March 27, 2024

Wenn für Ihre Bereitstellung keine Authentifizierung erforderlich ist, können Sie sie deaktivieren. Sie können die Authentifizierung für jeden virtuellen Server deaktivieren, für den keine Authentifizierung erforderlich ist.

Wichtig: Citrix empfiehlt, die Authentifizierung mit Vorsicht zu deaktivieren. Wenn Sie keinen externen Authentifizierungsserver verwenden, erstellen Sie lokale Benutzer und Gruppen, damit Citrix Gateway Benutzer authentifizieren kann. Durch das Deaktivieren der Authentifizierung wird die Verwendung von Authentifizierungs-, Autorisierungs- und Buchhaltungsfunktionen beendet, die Verbindungen zu Citrix Gateway steuern und überwachen. Wenn Benutzer eine Webadresse eingeben, um eine Verbindung zu Citrix Gateway herzustellen, wird die Anmeldeseite nicht angezeigt.

### Deaktivieren der Authentifizierung

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich Citrix Gateway, und klicken Sie dann auf Virtuelle Server.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf Öffnen.
3. Deaktivieren Sie auf der Registerkarte Authentifizierung unter Benutzerauthentifizierung die Option Authentifizierung aktivieren.

## Authentifizierung für bestimmte Zeiten konfigurieren

March 27, 2024

Sie können eine Authentifizierungsrichtlinie so konfigurieren, dass Benutzern zu bestimmten Zeiten Zugriff auf das interne Netzwerk gewährt wird, z. B. während der normalen Arbeitszeit. Wenn Benutzer versuchen, sich zu einem anderen Zeitpunkt anzumelden, wird die Anmeldung verweigert.

Um zu beschränken, wann sich Benutzer bei Citrix Gateway anmelden, erstellen Sie einen Ausdruck innerhalb der Authentifizierungsrichtlinie und binden ihn dann an einen virtuellen Server oder global.

### So konfigurieren Sie die Authentifizierung für Uhrzeit, Datum oder Wochentag

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Wählen Sie unter Authentifizierung den Authentifizierungstyp.
3. Klicken Sie im Detailbereich auf die Registerkarte Richtlinien, wählen Sie eine Authentifizierungsrichtlinie aus und klicken Sie dann auf Öffnen.
4. Klicken Sie im Dialogfeld Authentifizierungsrichtlinie konfigurieren unter Ausdruck neben Any Expression auf Hinzufügen.
5. Wählen Sie im Dialogfeld Ausdruck hinzufügen unter Ausdruckstyp Datum/Uhrzeit aus.

6. Wählen Sie in Qualifier eine der folgenden Optionen aus:

    - TIME, um die Zeit zu konfigurieren, zu der sich Benutzer nicht anmelden können.
    - DATE, um das Datum zu konfigurieren, an dem sich Benutzer nicht anmelden können.
    - DAYOFWEEK, um den Tag zu konfigurieren, an dem sich Benutzer nicht anmelden können.

    Example: TIME: 2020-10-12-02:30:00GMT DATE: 2020-10-12 DAYOFWEEK: Monday

7. Wählen Sie unter Operator den Wert aus.
8. Klicken Sie unter Wert auf den Kalender neben dem Textfeld und wählen Sie dann den Tag, das Datum oder die Uhrzeit aus.
9. Klicken Sie zweimal auf OK, klicken Sie auf Schließen und dann auf OK.

## Authentifizierungsrichtlinien

March 27, 2024

Wenn sich Benutzer bei Citrix Gateway anmelden, werden sie gemäß einer von Ihnen erstellten Richtlinie authentifiziert. Die Richtlinie definiert den Authentifizierungstyp. Eine einzige Authentifizierungsrichtlinie kann für einfache Authentifizierungsanforderungen verwendet werden und ist normalerweise auf globaler Ebene gebunden. Sie können auch den Standardauthentifizierungstyp verwenden, der lokal ist. Wenn Sie die lokale Authentifizierung konfigurieren, müssen Sie auch Benutzer und Gruppen auf Citrix Gateway konfigurieren.

Sie können mehrere Authentifizierungsrichtlinien konfigurieren und binden, um ein detailliertes Authentifizierungsverfahren und virtuelle Server zu erstellen. Sie können beispielsweise die Kaskadierung und die Zwei-Faktor-Authentifizierung konfigurieren, indem Sie mehrere Richtlinien konfigurieren. Sie können auch die Priorität der Authentifizierungsrichtlinien festlegen, um zu bestimmen, welche Server und die Reihenfolge, in der Citrix Gateway die Benutzeranmeldeinformationen überprüft. Eine Authentifizierungsrichtlinie beinhaltet einen Ausdruck und eine Aktion. Wenn Sie beispielsweise den Ausdruck auf True festlegen, wird bei der Benutzeranmeldung durch die Aktion die Benutzeranmeldung auf true ausgewertet, und Benutzer haben Zugriff auf Netzwerkressourcen.

Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie die Richtlinie entweder auf globaler Ebene oder an virtuelle Server. Wenn Sie mindestens eine Authentifizierungsrichtlinie an einen virtuellen Server binden, werden alle Authentifizierungsrichtlinien, die Sie an die globale Ebene gebunden haben, nicht verwendet, wenn sich Benutzer am virtuellen Server anmelden, es sei denn, der globale Authentifizierungstyp hat eine höhere Priorität als die an den virtuellen Server gebundene Richtlinie.

Wenn sich ein Benutzer bei Citrix Gateway anmeldet, wird die Authentifizierung in der folgenden Reihenfolge ausgewertet:

- Der virtuelle Server wird auf gebundene Authentifizierungsrichtlinien überprüft.
- Wenn Authentifizierungsrichtlinien nicht an den virtuellen Server gebunden sind, sucht Citrix Gateway nach globalen Authentifizierungsrichtlinien.
- Wenn eine Authentifizierungsrichtlinie nicht an einen virtuellen Server oder global gebunden ist, wird der Benutzer über den Standardauthentifizierungstyp authentifiziert.

Wenn Sie LDAP- und RADIUS-Authentifizierungsrichtlinien konfigurieren und die Richtlinien für die Zwei-Faktor-Authentifizierung global binden möchten, können Sie die Richtlinie im Konfigurationsdienstprogramm auswählen und dann auswählen, ob es sich bei der Richtlinie um den primären oder sekundären Authentifizierungstyp handelt. Sie können auch eine Gruppenextraktionsrichtlinie konfigurieren.

## Authentifizierungsprofile konfigurieren

March 27, 2024

Sie können ein Authentifizierungsprofil mithilfe des Citrix Gateway-Assistenten oder des Konfigurationsdienstprogramms erstellen. Das Profil enthält alle Einstellungen für die Authentifizierungsrichtlinie. Sie konfigurieren das Profil, wenn Sie die Authentifizierungsrichtlinie erstellen.

Mit dem Citrix Gateway-Assistenten können Sie den ausgewählten Authentifizierungstyp verwenden, um die Authentifizierung zu konfigurieren. Wenn Sie nach dem Ausführen des Assistenten zusätzliche Authentifizierungsrichtlinien konfigurieren möchten, können Sie das Konfigurationsdienstprogramm verwenden. Weitere Informationen zum Citrix Gateway-Assistenten finden Sie unter Konfigurieren von Einstellungen mithilfe des Citrix Gateway-Assistenten.

### So erstellen Sie mithilfe des Konfigurationsdienstprogramms eine Authentifizierungsrichtlinie

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Wählen Sie im Navigationsbereich unter Authentifizierung einen Authentifizierungstyp aus.
3. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
4. Wenn Sie einen externen Authentifizierungstyp verwenden, klicken Sie neben Server auf Neu.
5. Konfigurieren Sie im Dialogfeld Authentifizierungsserver erstellen die Einstellungen für Ihren Authentifizierungstyp, klicken Sie auf Erstellen und dann auf Schließen.

6. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie erstellen neben Benannte Ausdrücke den Wert True aus, klicken Sie auf Ausdruck hinzufügen, klicken Sie auf Erstellen und dann auf Schließen.
   Hinweis: Wenn Sie einen Authentifizierungstyp auswählen und das Authentifizierungsprofil speichern, können Sie den Authentifizierungstyp nicht ändern. Um einen anderen Authentifizierungstyp zu verwenden, müssen Sie eine neue Richtlinie erstellen.

### So ändern Sie eine Authentifizierungsrichtlinie mithilfe des Konfigurationsdienstprogramms

Sie können konfigurierte Authentifizierungsrichtlinien und -profile ändern, z. B. die IP-Adresse des Authentifizierungsservers oder den Ausdruck.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Wählen Sie im Navigationsbereich unter Authentifizierung einen Authentifizierungstyp aus.
3. Wählen Sie im Detailbereich auf der Registerkarte Server einen Server aus und klicken Sie dann auf Öffnen.

### So entfernen Sie eine Authentifizierungsrichtlinie

Wenn Sie einen Authentifizierungsserver aus Ihrem Netzwerk geändert oder entfernt haben, entfernen Sie die entsprechende Authentifizierungsrichtlinie aus Citrix Gateway.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Wählen Sie im Navigationsbereich unter Authentifizierung einen Authentifizierungstyp aus.
3. Wählen Sie im Detailbereich auf der Registerkarte Richtlinien eine Richtlinie aus und klicken Sie dann auf Entfernen.

## Authentifizierungsrichtlinien binden

March 27, 2024

Nachdem Sie die Authentifizierungsrichtlinien konfiguriert haben, binden Sie die Richtlinie entweder global oder an einen virtuellen Server. Sie können entweder das Konfigurationsdienstprogramm verwenden, um eine Authentifizierungsrichtlinie zu binden.

### So binden Sie eine Authentifizierungsrichtlinie über die GUI global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
2. Klicken Sie auf eine Authentifizierungsart.
3. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf einen Server, und klicken Sie dann unter **Aktion**auf **Globale Bindungen**.
4. Klicken Sie auf der Registerkarte **Primär oder Sekundär** unter **Details**auf **Richtlinie einfügen**.
5. Wählen Sie unter **Richtliniennam**edie Richtlinie aus, und klicken Sie dann auf **OK**.

   **Hinweis:** Wenn Sie die Richtlinie auswählen, setzt Citrix Gateway den Ausdruck automatisch auf den Wert True.

### So lösen Sie die Bindung einer globalen Authentifizierungsrichtlinie über die GUI

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
2. Klicken Sie auf der Registerkarte **Richtlinien** unter **Aktion** auf **Globale Bindungen**.
3. Wählen Sie im Dialogfeld **Authentifizierungsrichtlinien an global binden/entbinden** auf der Registerkarte **Primär oder Sekundär** unter **Richtlinienname** die Richtlinie aus, klicken Sie auf **Unbind policy** und dann auf **OK.**

## Prioritäten für Authentifizierungsrichtlinien festlegen

March 27, 2024

Standardmäßig werden Authentifizierungsrichtlinien zuerst anhand von Richtlinien validiert, die Sie an den virtuellen Server binden, und dann gegen global gebundene Richtlinien. Wenn Sie eine Authentifizierungsrichtlinie global binden und möchten, dass die globale Richtlinie Vorrang vor einer Richtlinie hat, die Sie an einen virtuellen Server binden, können Sie die Prioritätsnummer der Richtlinie ändern. Prioritätszahlen beginnen bei Null. Eine niedrigere Prioritätszahl gibt der Authentifizierungsrichtlinie eine höhere Priorität.

Wenn die globale Richtlinie beispielsweise die Prioritätsnummer eins hat und der virtuelle Server eine Priorität von zwei hat, wird zuerst die globale Authentifizierungsrichtlinie angewendet.

### So legen Sie die Priorität für globale Authentifizierungsrichtlinien fest oder ändern sie

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Klicken Sie auf der Registerkarte Richtlinien unter Aktion auf Globale Bindungen.
3. Geben Sie im Dialogfeld Globale Authentifizierungsrichtlinien binden/aufheben auf der Registerkarte Primär oder Sekundär unter Priorität die Zahl ein, und klicken Sie dann auf OK.

### So ändern Sie die Priorität für eine an einen virtuellen Server gebundene Authentifizierungsrichtlinie

Sie können auch eine Authentifizierungsrichtlinie ändern, die an einen virtuellen Server gebunden ist.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf Virtuelle Server.
2. Wählen Sie einen virtuellen Server aus und klicken Sie dann auf Öffnen.
3. Klicken Sie auf die Registerkarte Authentifizierung und wählen Sie dann entweder Primär oder Sekundär aus.
4. Wählen Sie die Richtlinie aus, geben Sie unter Priorität die Nummer der Priorität ein und klicken Sie dann auf OK.

## Lokale Benutzer konfigurieren

March 27, 2024

Sie können Benutzerkonten lokal auf Citrix Gateway erstellen, um die Benutzer auf Authentifizierungsservern zu ergänzen. Beispielsweise möchten Sie möglicherweise lokale Benutzerkonten für temporäre Benutzer wie Berater oder Besucher erstellen, ohne einen Eintrag für diese Benutzer auf dem Authentifizierungsserver zu erstellen.

Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen Sie sie dann Gruppen hinzu, die Sie auf Citrix Gateway erstellen. Nach der Konfiguration von Benutzern und Gruppen können Sie Autorisierungs- und Sitzungsrichtlinien anwenden, Lesezeichen erstellen, Anwendungen angeben und die IP-Adresse von Dateifreigaben und Servern angeben, auf die Benutzer Zugriff haben.

### So erstellen Sie lokale Benutzer

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte **Konfiguration** und erweitern Sie im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Benutzer**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Geben Sie im Feld Benutzername den Benutzernamen ein.**
4. Wenn Sie die lokale Authentifizierung verwenden, deaktivieren Sie **Externe Authentifizierung**. **Hinweis**: Wählen Sie **Externe Authentifizierung** aus, damit sich Benutzer bei einem externen Authentifizierungsserver wie LDAP oder RADIUS authentifizieren können. Deaktivieren Sie das Kontrollkästchen, damit sich Citrix Gateway bei der lokalen Benutzerdatenbank authentifiziert.
5. Geben **Sie unter**Passwort**und Passwort bestätigen** das Passwort für den Benutzer ein, klicken Sie auf **Erstellen**und dann auf **Schließen**.

### So ändern Sie ein Benutzerkennwort

Nachdem Sie einen lokalen Benutzer erstellt haben, können Sie das Kennwort des Benutzers ändern oder das Benutzerkonto für die Authentifizierung bei einem externen Authentifizierungsserver konfigurieren.

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte **Konfiguration** und erweitern Sie im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Benutzer**.
2. Wählen Sie im Detailbereich einen Benutzer aus und klicken Sie dann auf **Öffnen**.
3. Geben **Sie unter**Passwort**und Passwort bestätigen** das neue Passwort für den Benutzer ein, und klicken Sie dann auf **OK**.

### So ändern Sie die Authentifizierungsmethode eines Benutzers

Wenn Sie Benutzer haben, die für die lokale Authentifizierung konfiguriert sind, können Sie die Authentifizierung auf einen externen Authentifizierungsserver ändern. Aktivieren Sie dazu die externe Authentifizierung.

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte **Konfiguration** und erweitern Sie im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Benutzer**.
2. Wählen Sie im Detailbereich einen Benutzer aus und klicken Sie dann auf **Öffnen**.
3. Wählen Sie **Externe Authentifizierung**aus, und klicken Sie dann auf **OK**.

### So entfernen Sie einen Benutzer

Sie können einen Benutzer auch aus Citrix Gateway entfernen.

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte **Konfiguration** und erweitern Sie im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Benutzer**.
2. Wählen Sie im Detailbereich einen Benutzer aus, und klicken Sie dann auf **Entfernen**.

Wenn Sie einen Benutzer aus Citrix Gateway entfernen, werden alle zugehörigen Richtlinien auch aus dem Benutzerprofil entfernt.

## Gruppen konfigurieren

March 27, 2024

Sie können Gruppen auf Citrix Gateway haben, die lokale Gruppen sind und Benutzer mit lokaler Authentifizierung authentifizieren können. Wenn Sie externe Server für die Authentifizierung verwenden, werden Gruppen auf Citrix Gateway so konfiguriert, dass sie mit Gruppen übereinstimmen, die auf Authentifizierungsservern im internen Netzwerk konfiguriert sind. Wenn sich ein Benutzer anmeldet und authentifiziert wird und ein Gruppenname mit einer Gruppe auf einem Authentifizierungsserver übereinstimmt, erbt der Benutzer die Einstellungen für die Gruppe auf Citrix Gateway.

Nachdem Sie Gruppen konfiguriert haben, können Sie Autorisierungs- und Sitzungsrichtlinien anwenden, Lesezeichen erstellen, Anwendungen angeben und die IP-Adresse von Dateifreigaben und Servern angeben, auf die der Benutzer Zugriff hat.

Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen Sie sie Gruppen hinzu, die auf Citrix Gateway konfiguriert sind. Die Benutzer erben dann die Einstellungen für diese Gruppe.

**Wichtig**: Wenn Benutzer Mitglied einer Active Directory-Gruppe sind, muss der Name der Gruppe auf Citrix Gateway mit der Active Directory-Gruppe übereinstimmen.

### So erstellen Sie eine Gruppe

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte **Konfiguration** und erweitern Sie im Navigationsbereich **Citrix Gateway > Benutzerverwaltung** und klicken Sie dann auf **AAA-Gruppen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.

3. Geben Sie im **Feld Gruppenname**einen Namen für die Gruppe ein, klicken Sie auf **Erstellen**und dann auf **Schließen**.

### Löschen einer Gruppe

Sie können Benutzergruppen auch aus Citrix Gateway löschen.

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte **Konfiguration** und erweitern Sie im Navigationsbereich **Citrix Gateway > Benutzerverwaltung** und klicken Sie dann auf **AAA-Gruppen**.
2. Wählen Sie im Detailbereich die Gruppe aus, und klicken Sie dann auf **Entfernen**.

## Benutzer zu Gruppen hinzufügen

March 27, 2024

Sie können Benutzer entweder während der Erstellung der Gruppe oder später zu einer Gruppe hinzufügen. Sie können Benutzer mehreren Gruppen hinzufügen, damit Benutzer die an diese Gruppen gebundenen Richtlinien und Einstellungen erben können.

So fügen Sie Benutzer zu Gruppen hinzu:

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und erweitern Sie im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Benutzer**.
2. Wählen Sie im Detailbereich eine Gruppe aus, und klicken Sie dann auf **Öffnen**.
3. Wählen Sie auf der Registerkarte **Benutzer** unter **Verfügbare Benutzer**die Benutzer aus, klicken Sie auf **Hinzufügen**und dann auf **OK**.

## Richtlinien mit Gruppen konfigurieren

March 27, 2024

Nachdem Sie Gruppen konfiguriert haben, können Sie das Dialogfeld “Gruppe “verwenden, um Richtlinien und Einstellungen anzuwenden, die den Benutzerzugriff festlegen. Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen sie Gruppen hinzu, die auf Citrix Gateway konfiguriert sind. Die Benutzer erben dann die Einstellungen für diese Gruppe.

Im Dialogfeld Gruppe können Sie die folgenden Richtlinien oder Einstellungen für eine Gruppe von Benutzern konfigurieren:

- Benutzer
- Richtlinien zur Autorisierung
- Richtlinien für die Prüfung
- Sitzungsrichtlinien
- Datenverkehrsrichtlinien
- Lesezeichen
- Intranetanwendungen
- Intranet-IP-Adressen

In Ihrer Konfiguration haben Sie möglicherweise Benutzer, die zu mehr als einer Gruppe gehören. Darüber hinaus kann jede Gruppe über eine oder mehrere gebundene Sitzungsrichtlinien verfügen, wobei verschiedene Parameter konfiguriert sind. Benutzer, die zu mehr als einer Gruppe gehören, erben die Sitzungsrichtlinien, die allen Gruppen zugewiesen sind, zu denen der Benutzer gehört. Um sicherzustellen, welche Sitzungsrichtlinienbewertung Vorrang vor der anderen hat, müssen Sie die Priorität der Sitzungsrichtlinie festlegen.

Beispielsweise haben Sie Gruppe1, die an eine Sitzungsrichtlinie gebunden ist, die mit der Homepage www.homepage1.com konfiguriert ist. Group2 ist an eine Sitzungsrichtlinie gebunden, die mit der Homepage www.homepage2.com konfiguriert ist. Wenn diese Richtlinien ohne Prioritätsnummer oder mit derselben Prioritätsnummer an entsprechende Gruppen gebunden sind, hängt die Homepage, die Benutzern angezeigt wird, die beiden Gruppen angehören, davon ab, welche Richtlinie zuerst verarbeitet wird. Durch Festlegen einer niedrigeren Prioritätszahl, die höhere Priorität hat, für die Sitzungsrichtlinie mit Homepage www.homepage1.com können Sie sicherstellen, dass Benutzer, die beiden Gruppen angehören, die Homepage www.homepage1.com erhalten.

Wenn Sitzungsrichtlinien keine Prioritätsnummer zugewiesen wurde oder dieselbe Prioritätsnummer hat, wird die Priorität in der folgenden Reihenfolge ausgewertet:

- User
- Gruppe
- Virtueller Server
- Global

Wenn Richtlinien an dieselbe Ebene ohne Prioritätsnummer gebunden sind oder wenn die Richtlinien dieselbe Prioritätsnummer haben, entspricht die Reihenfolge der Bewertung der Richtlinienbindungsreihenfolge. Richtlinien, die zuerst an eine Ebene gebunden sind, haben Vorrang vor später gebundenen Richtlinien.

Wenn wir einen Benutzer haben, der an mehrere Gruppen gebunden ist, wobei jede Gruppe IIP gebunden ist, kann der Benutzer kostenlose IP von jeder der gebundenen Gruppen erhalten.

# LDAP-Authentifizierung konfigurieren

March 27, 2024

Sie können das Citrix Gateway so konfigurieren, dass der Benutzerzugriff mit einem oder mehreren LDAP-Servern authentifiziert wird.

Für die LDAP-Autorisierung sind identische Gruppennamen im Active Directory, auf dem LDAP-Server und auf dem Citrix Gateway erforderlich. Die Zeichen und der Fall müssen ebenfalls übereinstimmen.

Standardmäßig ist die LDAP-Authentifizierung mithilfe von Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) sicher. Es gibt zwei Arten von sicheren LDAP-Verbindungen. Bei einem Typ akzeptiert der LDAP-Server die SSL- oder TLS-Verbindungen an einem Port getrennt von dem Port, den der LDAP-Server verwendet, um klare LDAP-Verbindungen zu akzeptieren. Nachdem Benutzer die SSL- oder TLS-Verbindungen hergestellt haben, kann LDAP-Verkehr über die Verbindung gesendet werden.

Die Portnummern für LDAP-Verbindungen lauten:

- 389 für ungesicherte LDAP-Verbindungen
- 636 für sichere LDAP-Verbindungen
- 3268 für Microsoft unsichere LDAP-Verbindungen
- 3269 für sichere LDAP-Verbindungen von Microsoft

Die zweite Art von sicheren LDAP-Verbindungen verwendet den Befehl StartTLS und verwendet die Portnummer 389. Wenn Sie die Portnummern 389 oder 3268 auf Citrix Gateway konfigurieren, versucht der Server, StartTLS zum Herstellen der Verbindung zu verwenden. Wenn Sie eine andere Portnummer verwenden, versucht der Server, mithilfe von SSL oder TLS Verbindungen herzustellen. Wenn der Server StartTLS, SSL oder TLS nicht verwenden kann, schlägt die Verbindung fehl.

Wenn Sie das Stammverzeichnis des LDAP-Servers angeben, durchsucht Citrix Gateway alle Unterverzeichnisse, um das Benutzerattribut zu finden. In großen Verzeichnissen kann dieser Ansatz die Leistung beeinträchtigen. Aus diesem Grund empfiehlt Citrix, eine bestimmte Organisationseinheit (OU) zu verwenden.

Die folgende Tabelle enthält Beispiele für Benutzerattributfelder für LDAP-Server:

| LDAP-Server | Benutzer-Attribut | Case sensitiv |
|---|---|---|
| Microsoft Active Directory-Server | sAMAccountName | Nein |
| Novell eDirectory | ou | Ja |

| LDAP-Server | Benutzer-Attribut | Case sensitiv |
|---|---|---|
| IBM Verzeichnisserver | uid | Ja |
| Lotus-Domino | CN | Ja |
| Sun ONE Verzeichnis (ehemals iPlanet) | uid oder cn | Ja |

Diese Tabelle enthält Beispiele für den Basis-DN:

| LDAP-Server | Basis-DN |
|---|---|
| Microsoft Active Directory-Server | DC =citrix, DC = lokal |
| Novell eDirectory | ou=Benutzer, ou=dev |
| IBM Verzeichnisserver | cn=users |
| Lotus-Domino | OU=Stadt, O=Citrix, C=US |
| Sun ONE Verzeichnis (ehemals iPlanet) | ou = Menschen, dc =citrix, dc = com |

Die folgende Tabelle enthält Beispiele für Bind-DN:

| LDAP-Server | Bind DN |
|---|---|
| Microsoft Active Directory-Server | CN=Administrator, CN=Benutzer, DC=citrix, DC = lokal |
| Novell eDirectory | cn=admin, o=citrix |
| IBM Verzeichnisserver | LDAP_dn |
| Lotus-Domino | CN=Notes Administrator, O=Citrix, C=US |
| Sun ONE Verzeichnis (ehemals iPlanet) | uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot |

**Hinweis**: Weitere Informationen zu den LDAP-Servereinstellungen finden Sie unter Bestimmen von Attributen in Ihrem LDAP-Verzeichnis.

# LDAP-Authentifizierung mit dem Konfigurationsdienstprogramm konfigurieren

March 27, 2024

1. Navigieren Sie zu **Citrix Gateway** >**Richtlinien** > **Authentifizierung**.
2. Klicken Sie auf **LDAP**.
3. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Hinzufügen**.
4. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
5. Klicken Sie neben **Server** auf **Neu**.
6. Geben Sie unter **Name** den Namen des Servers ein.
7. Geben Sie unter **Server**unter **IP-Adresse und Port**die IP-Adresse und Portnummer des LDAP-Servers ein.
8. Wählen Sie unter **Typ**entweder **AD** für Active Directory oder **NDS** für Novell Directory Services aus.
9. Führen Sie unter **Verbindungseinstellungen**Folgendes aus:

   a) Geben Sie unter **Basis-DN (Standort der Benutzer)**den Basis-DN ein, unter dem sich Benutzer befinden. Basis-DN durchsucht die Benutzer, die sich unter dem ausgewählten Verzeichnis befinden (AD oder NDS).

   Der Basis-DN wird vom Bind-DN abgeleitet, indem der Benutzername entfernt und die Gruppe angegeben wird, in der sich Benutzer befinden. Beispiele für die Syntax für den Basis-DN sind:

   ```
   ou=users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   b) Geben Sie unter **Administrator Bind-DN**den Administratorbindungs-DN für Abfragen an das LDAP-Verzeichnis ein. Beispiele für die Syntax von Bind-DN sind:

   ```
   domain/user name
   ou=administrator,dc=ace,dc=com
   user@domain.name (for Active Directory)
   cn=Administrator,cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   Für Active Directory ist der als cn=groupname angegebene Gruppenname erforderlich. Der Gruppenname, den Sie in Citrix Gateway definieren, und der Gruppenname auf dem LDAP-Server müssen identisch sein.

Für andere LDAP-Verzeichnisse ist der Gruppenname entweder nicht erforderlich oder wird bei Bedarf als ou=groupname angegeben.

Citrix Gateway bindet mithilfe der Administratoranmeldeinformationen an den LDAP-Server und sucht dann nach dem Benutzer. Nach dem Auffinden des Benutzers entfernt Citrix Gateway die Administratoranmeldeinformationen und bindet die Benutzeranmeldeinformationen erneut.

c) Geben Sie unter **Administratorkennwort und Administratorkennwort bestätigen**das Administratorkennwort für den LDAP-Server ein.

10. Um automatisch weitere LDAP-Einstellungen abzurufen, klicken Sie auf **Attribute abrufen**.

    Wenn Sie auf **Attribute abrufen**klicken, werden die Felder unter Andere Einstellungen automatisch ausgefüllt. Wenn Sie diesen Schritt ignorieren möchten, fahren Sie mit den Schritten 12 und 13 fort. Ansonsten fahren Sie mit Schritt 14 fort.

11. Geben Sie unter **Andere Einstellungen**in Serveranmeldungsnamenattribut das Attribut ein, unter dem Citrix Gateway nach Benutzeranmeldenamen für den LDAP-Server suchen muss, den Sie konfigurieren. Der Standardwert ist `samAccountName`.

12. Geben Sie unter **Suchfilter**den Wert ein, um nach den Benutzern zu suchen, die einzelnen oder mehreren Active Directory-Gruppen zugeordnet sind.

    Zum Beispiel “Memberof=CN=GatewayAccess, OU=Groups, DC=Users, DC=Lab”.

    > **Hinweis**
    >
    > Sie können das vorangegangene Beispiel verwenden, um den Zugriff auf Citrix Gateway nur auf Mitglieder einer bestimmten AD-Gruppe zu beschränken.

13. Belassen Sie unter **Gruppenattribut**das standardmäßige MemberOf für Active Directory oder ändern Sie das Attribut in das Attribut des von Ihnen verwendeten LDAP-Servertyps. Mit diesem Attribut kann Citrix Gateway die Gruppen abrufen, die einem Benutzer während der Autorisierung zugeordnet sind.

14. Wählen Sie unter **Sicherheitstyp** den Sicherheitstyp aus und klicken Sie dann auf **Erstellen**.

15. Um Benutzern zu erlauben, ihr LDAP-Kennwort zu ändern, wählen Sie **Kennwortänderung zulassen**.

    **Hinweis:**

    - Wenn Sie **PLAINTEXT** als Sicherheitstyp auswählen, wird es nicht unterstützt, Benutzern das Ändern ihrer Kennwörter zu erlauben.
    - Wenn Sie aus Sicherheitsgründen **PLAINTEXT** oder **TLS** auswählen, verwenden Sie die Portnummer 389. Wenn Sie **SSL**wählen, verwenden Sie die Portnummer 636.

## Bestimmen der Attribute in Ihrem LDAP-Verzeichnis

March 27, 2024

Wenn Sie Hilfe bei der Bestimmung Ihrer LDAP-Verzeichnisattribute benötigen, damit Sie die Authentifizierungseinstellungen auf NetScaler Gateway konfigurieren können, können Sie diese ganz einfach mit dem kostenlosen LDAP-Browser von Softerra nachschlagen.

Sie können den LDAP-Browser von der Softerra LDAP Administrator-Websiteherunterladen. Legen Sie nach der Installation des Browsers die folgenden Attribute fest:

- Der Hostname oder die IP-Adresse Ihres LDAP-Servers.
- Der Port Ihres LDAP-Servers. Die Standardeinstellung ist 389.
- Das Basis-DN-Feld, das Sie leer lassen können. Die vom LDAP-Browser bereitgestellten Informationen können Ihnen bei der Bestimmung des Basis-DN helfen, den Sie diese Einstellung auf Citrix Gateway konfigurieren müssen.
- Die Überprüfung der anonymen Bindung bestimmt, ob der LDAP-Server Benutzeranmeldeinformationen benötigt, um eine Verbindung herzustellen. Wenn der LDAP-Server Anmeldeinformationen benötigt, lassen Sie das Kontrollkästchen deaktiviert.

Nach Abschluss der Einstellungen zeigt der LDAP-Browser den Profilnamen im linken Fensterbereich an und stellt eine Verbindung zum LDAP-Server her.

## LDAP-Gruppenextraktion konfigurieren

March 27, 2024

Wenn Sie die Zwei-Faktor-Authentifizierung verwenden, werden Gruppen, die sowohl aus der primären als auch aus der sekundären Authentifizierungsquelle extrahiert wurden, verkettet. Autorisierungsrichtlinien können auf die Gruppe angewendet werden, die vom primären oder sekundären Authentifizierungsserver extrahiert wird.

Die vom LDAP-Server erhaltenen Gruppennamen werden mit den lokal auf Citrix Gateway erstellten Gruppennamen verglichen. Wenn die beiden Gruppennamen übereinstimmen, gelten die Eigenschaften der lokalen Gruppe für die Gruppe, die von den LDAP-Servern bezogen wurde.

Wenn Benutzer zu mehr als einer LDAP-Gruppe gehören, extrahiert Citrix Gateway Benutzerinformationen aus allen Gruppen, zu denen Benutzer gehören. Wenn ein Benutzer Mitglied von zwei Gruppen in Citrix Gateway ist und jede Gruppe über eine gebundene Sitzungsrichtlinie verfügt, erbt der Benutzer die Sitzungsrichtlinien von beiden Gruppen. Um sicherzustellen, dass Benutzer die richtige Sitzungsrichtlinie erhalten, legen Sie die Priorität für die Sitzungsrichtlinie fest.

Weitere Informationen zu LDAP-Gruppenmitgliedschaftsattributen finden Sie im Folgenden:

- LDAP-Gruppenextraktion direkt aus dem Benutzerobjekt
- LDAP-Gruppenextraktion indirekt aus dem Gruppenobjekt

## LDAP-Gruppenextraktion direkt aus dem Benutzerobjekt

March 27, 2024

LDAP-Server, die Gruppenmitgliedschaften von Gruppenobjekten auswerten, unterstützen die Citrix Gateway-Autorisierung.

Bei einigen LDAP-Servern können Benutzerobjekte Informationen über Gruppen enthalten, zu denen die Objekte gehören, wie Active Directory (über das MemberOf-Attribut) oder IBM eDirectory (über das groupMembership-Attribut). Die Gruppenmitgliedschaft eines Benutzers kann Attribute aus dem Benutzerobjekt sein, z. B. IBM Directory Server (über ibm-allGroups) oder Sun ONE-Verzeichnisserver (über nsRole). Beide Arten von LDAP-Servern unterstützen die Extraktion von Citrix Gateway-Gruppen.

Beispielsweise können in IBM Directory Server alle Gruppenmitgliedschaften, einschließlich der statischen, dynamischen und verschachtelten Gruppen, mithilfe des IBM-AllGroups-Attributs zurückgegeben werden. In Sun ONE werden alle Rollen, einschließlich verwaltet, gefiltert und verschachtelt, mithilfe des NSRole-Attributs berechnet.

## LDAP-Gruppenextraktion indirekt aus dem Gruppenobjekt

March 27, 2024

LDAP-Server, die indirekt Gruppenmitgliedschaften von Gruppenobjekten auswerten, sind nicht mit der Citrix Gateway-Autorisierung kompatibel.

Einige LDAP-Server, wie Lotus Domino, ermöglichen es Gruppenobjekten, nur Informationen über Benutzer zu enthalten. Diese LDAP-Server ermöglichen es dem Benutzerobjekt nicht, Informationen über Gruppen zu enthalten, und sind daher nicht mit der Citrix Gateway-Gruppenextraktion kompatibel. Für diesen LDAP-Servertyp werden Gruppenmitgliedschaftssuchen durchgeführt, indem der Benutzer in der Mitgliederliste der Gruppen gesucht wird.

## LDAP-Berechtigungsgruppen-Attributfelder

January 29, 2024

Die folgende Tabelle enthält Beispiele für LDAP-Gruppen-Attributfelder:

| LDAP-Server | LDAP-Attribut |
|---|---|
| Microsoft Active Directory-Server | memberOf |
| Novell eDirectory | groupMembership |
| IBM Verzeichnisserver | ibm-allGroups |
| Sun ONE Verzeichnis (ehemals iPlanet) | nsRole |

## LDAP-Autorisierung konfigurieren

March 27, 2024

Sie konfigurieren die LDAP-Autorisierung in der Authentifizierungsrichtlinie, indem Sie den Namen des Gruppenattributs und das Unterattribut festlegen.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Klicken Sie unter Authentifizierung auf einen Authentifizierungstyp.
3. Klicken Sie im Detailbereich auf "Hinzufügen".
4. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
5. Klicken Sie neben Server auf Neu.
6. Geben Sie unter Name den Namen des Servers ein.
7. Geben Sie unter Server die IP-Adresse und den Port des LDAP-Servers ein.
8. Geben Sie im Feld GruppenattributMemberOf ein.
9. Geben Sie unter Unterattribut Name CN ein und klicken Sie dann auf Erstellen.
10. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie erstellen neben Benannte Ausdrücke den Ausdruck aus, klicken Sie auf Ausdruck hinzufügen, klicken Sie auf Erstellen und dann auf Schließen.

# Extraktion verschachtelter LDAP-Gruppen konfigurieren

March 27, 2024

Citrix Gateway kann LDAP-Gruppen abfragen und Gruppen- und Benutzerinformationen aus Vorfahrengruppen extrahieren, die Sie auf dem Authentifizierungsserver konfigurieren. Sie haben beispielsweise Gruppe1 erstellt und innerhalb dieser Gruppe haben Sie Gruppe2 und Gruppe3 erstellt. Wenn der Benutzer zu Gruppe3 gehört, extrahiert Citrix Gateway Informationen aus allen verschachtelten Vorfahrengruppen (Gruppe2, Gruppe1) bis zur angegebenen Ebene.

Sie können eine Authentifizierungsrichtlinie verwenden, um die Extraktion verschachtelter LDAP-Gruppen zu konfigurieren. Wenn die Abfrage ausgeführt wird, durchsucht Citrix Gateway die Gruppen, bis die maximale Verschachtelungsstufe erreicht ist oder bis alle verfügbaren Gruppen durchsucht werden.

## So konfigurieren Sie die Extraktion verschachtelter LDAP-Gruppen

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung > Authentifizierung > Authentifizierung > Authentifizierung** und klicken Sie dann auf **LDAP**.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Hinzufügen**.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Server auf **Neu**.
5. Geben Sie unter Name den Namen des Servers ein.
6. Konfigurieren Sie die Einstellungen für den LDAP-Server.
7. Erweitern Sie **Verschachtelte Gruppenextraktion**, und klicken Sie dann auf **Aktivieren**.
8. Geben Sie **unter Maximale Verschachtelungsstufe**die Anzahl der Ebenen ein, die Citrix Gateway prüft.
9. Geben **Sie unter Group Name Identifier**den LDAP-Attributnamen ein, der einen Gruppennamen auf dem LDAP-Server eindeutig identifiziert, z. `sAMAccountName`B.
10. Geben Sie unter **Gruppensuchattribut**den LDAP-Attributnamen ein, der in der Suchantwort abgerufen werden soll, um die übergeordneten Gruppen einer Gruppe zu bestimmen. Beispiel: `memberOf`.
11. Geben Sie unter **Gruppensuch-Unterattribut**den Namen des LDAP-Unterattributs ein, nach dem als Teil des Gruppensuchattributs gesucht werden soll, um die übergeordneten Gruppen einer Gruppe zu bestimmen. Geben Sie beispielsweise CN ein.
12. Geben Sie unter **Gruppensuchfilter**die Abfragezeichenfolge ein. Zum Beispiel kann der Filter sein `&(samaccountname=test)(objectClass=\*)`.
13. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

14. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie erstellen neben Benannte Ausdrücke den Ausdruck aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

## LDAP-Gruppenextraktion für mehrere Domänen konfigurieren

March 27, 2024

Wenn Sie über mehrere Domänen für die Authentifizierung verfügen und StoreFront oder das Webinterface verwenden, können Sie Citrix Gateway so konfigurieren, dass die Gruppenextraktion verwendet wird, um den richtigen Domänennamen an das Webinterface zu senden.

In Active Directory müssen Sie für jede Domäne in Ihrem Netzwerk eine Gruppe erstellen. Nachdem Sie die Gruppe erstellt haben, fügen Sie Benutzer hinzu, die zur Gruppe und der angegebenen Domäne gehören. Nachdem die Gruppen in Active Directory konfiguriert wurden, konfigurieren Sie die LDAP-Gruppenextraktion für mehrere Domänen auf Citrix Gateway.

Um Citrix Gateway für die Gruppenextraktion für mehrere Domänen zu konfigurieren, müssen Sie dieselbe Anzahl von Sitzungs- und Authentifizierungsrichtlinien erstellen wie die Anzahl der Domänen in Ihrem Netzwerk. Zum Beispiel haben Sie zwei Domänen namens `Sampa` und Child. Jede Domäne erhält eine Sitzungsrichtlinie und eine Authentifizierungsrichtlinie.

Nach dem Erstellen der Richtlinien erstellen Sie Gruppen auf Citrix Gateway und binden die Sitzungsrichtlinien an die Gruppe. Dann binden Sie die Authentifizierungsrichtlinien an einen virtuellen Server.

Wenn Sie StoreFront in mehreren Domänen bereitstellen, muss eine Vertrauensbeziehung zwischen Domänen bestehen.

Wenn Sie Citrix Endpoint Management oder das Webinterface in mehreren Domänen bereitstellen, müssen sich die Domänen nicht gegenseitig vertrauen.

## Sitzungsrichtlinien für die Gruppenextraktion konfigurieren

March 27, 2024

Der erste Schritt beim Erstellen von Sitzungsrichtlinien für die Gruppenextraktion besteht darin, zwei Sitzungsprofile zu erstellen und die folgenden Parameter festzulegen:

- Aktivieren Sie ICA-Proxy.
- Fügen Sie die Webinterface-Webadresse hinzu.

- Fügen Sie die Windows-Domäne hinzu.
- Fügen Sie das Profil zu einer Sitzungsrichtlinie hinzu und setzen Sie den Ausdruck auf true.

### So erstellen Sie die Sitzungsprofile für die Gruppenextraktion

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Profile** und dann auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für das Profil ein.** Geben Sie zum Beispiel ein `Sampa`.
4. Gehen Sie auf der Registerkarte **Veröffentlichte Anwendungen** wie folgt vor:
    a) Klicken Sie neben **ICA-Proxy**auf **Override Global** und wählen Sie dann **ON**aus.
    b) Klicken Sie neben **Webinterface-Adresse**auf **Override Global** und geben Sie dann die Webadresse des Webinterface ein.
    c) Klicken Sie neben **Single Sign-On Domäne aufOverride Global**, geben Sie den Namen der Windows-Domäne ein und klicken Sie dann auf**Erstellen**.
5. **Löschen Sie im Feld Name den Namen der ersten Domäne und geben Sie den Namen der zweiten Domäne ein, z. B. Kind.**
6. Löschen Sie neben **Single Sign-On Domain**den Namen der ersten Windows-Domäne, geben Sie den Namen der zweiten Domäne ein, klicken Sie auf **Erstellen** und dann auf **Schließen**.

Nachdem Sie die Sitzungsprofile erstellt haben, erstellen Sie zwei Sitzungsrichtlinien. Jede Sitzungsrichtlinie verwendet eines der Profile.

### So erstellen Sie eine Sitzungsrichtlinie

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Wählen Sie **unter Profil anfordern**das Profil für die erste Domain aus.
5. Klicken Sie neben **Benannte Ausdrücke**auf **Allgemein**, wählen Sie den **Wert True**aus, klicken Sie auf **Ausdruck hinzufügen,** und klicken Sie dann auf **Erstellen**.
6. Ändern Sie unter **Name**den Namen in die zweite Domain.
7. Wählen Sie unter **Profil anfordern**das Profil für die zweite Domäne aus, klicken Sie auf **Erstellen** und dann auf **Schließen**.

# LDAP-Authentifizierungsrichtlinien für mehrere Domänen erstellen

March 27, 2024

Nachdem Sie Sitzungsrichtlinien auf Citrix Gateway erstellt haben, erstellen Sie LDAP-Authentifizierungsrichtlinien die nahezu identisch sind. Bei der Konfiguration der Authentifizierungsrichtlinie ist das wichtige Feld Suchfilter. In dieses Feld müssen Sie den Namen der Gruppe eingeben, die Sie im Active Directory erstellt haben.

Erstellen Sie zuerst die Authentifizierungsprofile und erstellen Sie dann die Authentifizierungsrichtlinie.

## So erstellen Sie Authentifizierungsprofile für Extraktionen mehrerer Domänengruppen

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration Citrix **Gateway > Richtlinien > Authentifizierung**.
2. Klicken Sie im Navigationsbereich auf **LDAP**.
3. Klicken Sie im Detailbereich auf die Registerkarte **Server** und dann auf **Hinzufügen**.
4. Geben Sie **unter Name**den Namen der ersten Domäne ein, z. SampaB.
5. Konfigurieren Sie die Einstellungen für den LDAP-Server und klicken Sie dann auf **Erstellen**.
6. Wiederholen Sie die Schritte 3, 4 und 5, um das Authentifizierungsprofil der zweiten Domäne zu konfigurieren, und klicken Sie dann auf **Schließen**.

Nachdem Sie die Profile erstellt und gespeichert haben, erstellen Sie die Authentifizierungsrichtlinien.

## So erstellen Sie Authentifizierungsrichtlinien für Extraktionen mehrerer Domänengruppen

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Richtlinien** und dann auf **Hinzufügen**.
3. Geben Sie **unter Name**den Namen der ersten Domäne ein.
4. Wählen Sie unter **AuthentifizierungstypLDAP**aus.
5. Wählen Sie unter **Server**das Authentifizierungsprofil für die erste Domain aus.
6. Klicken Sie neben **Benannte Ausdrücke**auf **Allgemein**, wählen Sie den **Wert True**aus, klicken Sie auf **Ausdruck hinzufügen,** und klicken Sie dann auf **Erstellen**.
7. Geben Sie unter Name den Namen der zweiten Domäne ein.
8. Wählen Sie unter **Server**das Authentifizierungsprofil für die zweite Domäne aus, klicken Sie auf **Erstellen** und dann auf **Schließen**.

# Gruppen und Bindungsrichtlinien für die LDAP-Gruppenextraktion für mehrere Domänen erstellen

March 27, 2024

Nachdem Sie Authentifizierungsrichtlinien erstellt haben, erstellen Sie Gruppen auf Citrix Gateway. Nachdem Sie die Gruppen erstellt haben, binden Sie die Authentifizierungsrichtlinie an einen virtuellen Server.

## So erstellen Sie Gruppen auf Citrix Gateway

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Gruppen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im **Feld Gruppenname**den Namen der ersten Active Directory Directory-Gruppe ein. **Wichtig**: Beim Erstellen von Gruppen auf Citrix Gateway für die Gruppenextraktion aus mehreren Domänen müssen Gruppennamen mit den Gruppen übereinstimmen, die Sie im Active Directory definiert haben. Bei Gruppennamen wird auch zwischen Groß- und Kleinschreibung unterschieden, und die Groß-/Kleinschreibung muss mit der Groß-/Kleinschreibung übereinstimmen
4. Klicken Sie auf der Registerkarte **Richtlinien** auf **Sitzung**und dann auf **Richtlinie einfügen**.
5. Doppelklicken Sie unter **Richtliniennam**eauf die Richtlinie, und klicken Sie dann auf **Erstellen**.

## So binden Sie die Authentifizierungsrichtlinien an einen virtuellen Server

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Klicken Sie auf der Registerkarte Authentifizierung auf **Primär**, doppelklicken Sie unter **Richtliniennam**eauf **Richtlinie einfügen**, und wählen Sie dann die erste Authentifizierungsrichtlinie aus.
4. Klicken Sie unter **Richtliniennam**eauf **Richtlinie einfügen**, doppelklicken Sie auf die zweite Authentifizierungsrichtlinie, und klicken Sie dann auf **OK**.

## Benachrichtigung 14 Tage vor Kennwortablauf für LDAP-Authentifizierung

January 29, 2024

Das NetScaler Gateway-Gerät unterstützt eine Benachrichtigung 14 Tage vor Ablauf des Kennworts für die LDAP-basierte Authentifizierung. Mit dieser Funktion können Administratoren die Endbenutzer über den Ablauf des Kennworts informieren. Der Schwellenwert wird in Tagen angegeben. Weitere Einzelheiten finden Sie unter Benachrichtigung 14 Tage vor Kennwortablauf für LDAP-Authentifizierung.

## Clientzertifikatauthentifizierung konfigurieren

March 27, 2024

Benutzer, die sich bei einem virtuellen Citrix Gateway-Server anmelden, können auch basierend auf den Clientzertifikatattributen authentifiziert werden, die dem virtuellen Server angezeigt werden. Die Clientzertifikatauthentifizierung kann auch mit anderen Authentifizierungstypen wie LDAP oder RADIUS verwendet werden, um eine Zwei-Faktor-Authentifizierung bereitzustellen.

Um Benutzer basierend auf den clientseitigen Zertifikatattributen zu authentifizieren, muss die Clientauthentifizierung auf dem virtuellen Server aktiviert und das Clientzertifikat angefordert werden. Sie müssen ein Stammzertifikat an den virtuellen Server von Citrix Gateway binden.

Wenn sich Benutzer nach der Authentifizierung am virtuellen Citrix Gateway-Server anmelden, werden die Benutzernameninformationen aus dem angegebenen Feld des Zertifikats extrahiert. Üblicherweise ist es das Feld “Subject:CN”. Wurde der Benutzername erfolgreich extrahiert, wird der Benutzer authentifiziert. Die Authentifizierung schlägt in den folgenden Fällen fehl.

- Wenn der Benutzer während des Secure Sockets Layer (SSL) -Handshakes kein gültiges Zertifikat bereitstellt.
- Die Extraktion des Benutzernamens schlägt fehl, die Authentifizierung schlägt fehl.

Sie können Benutzer anhand des Clientzertifikats authentifizieren, indem Sie für den Standardauthentifizierungstyp die Verwendung des Clientzertifikats angeben. Sie können auch eine Zertifikataktion erstellen, mit der Sie definieren, was während der Authentifizierung basierend auf einem Client-SSL-Zertifikat geschehen soll.

### So konfigurieren Sie das Clientzertifikat über die GUI als Standardauthentifizierungstyp

1. Wechseln Sie zu **Konfiguration > Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Authentifizierungseinstellungen**auf **Authentifizierungs-CERT-Einstellungen ändern**.
3. Wählen Sie **ON** aus, um die Zwei-Faktor-Authentifizierung mithilfe des Zertifikats gemäß Ihrer Anforderung zu aktivieren.
4. Wählen Sie im **Feld Benutzername**das Feld für den Typ des Zertifikats aus, das die Benutzernamen enthält.
5. Wählen Sie im **Feld Gruppenname**den Typ des Zertifikatfelds aus, das den Gruppennamen enthält.
6. Geben Sie unter **Standardermächtigungsgruppe**den Namen der Standardgruppe ein, und klicken Sie dann auf **OK**.

### Extrahieren des Benutzernamens aus dem Clientzertifikat

Wenn die Clientzertifikatauthentifizierung in Citrix Gateway aktiviert ist, werden Benutzer basierend auf bestimmten Attributen des Clientzertifikats authentifiziert. Nach erfolgreicher Authentifizierung wird der Benutzername oder der Benutzer- und Gruppenname des Benutzers aus dem Zertifikat extrahiert. Außerdem werden die für diesen Benutzer angegebenen Richtlinien angewendet.

## Richtlinie für die Clientzertifikatauthentifizierung konfigurieren und binden

March 27, 2024

Sie können eine Clientzertifikatauthentifizierungsrichtlinie erstellen und an einen virtuellen Server binden. Sie können die Richtlinie verwenden, um den Zugriff auf bestimmte Gruppen oder Benutzer zu beschränken. Diese Richtlinie hat Vorrang vor der globalen Richtlinie.

So konfigurieren Sie eine Richtlinie zur Clientzertifikatauthentifizierung

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
2. Klicken Sie im Navigationsbereich unter **Authentifizierung** auf **CERT**.
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Geben Sie im Feld **Name** einen Namen für die Richtlinie ein.

5. Klicken Sie neben **Server** auf **Neu**.
6. **Geben Sie im Feld Name einen Namen für das Profil ein.**
7. Wählen Sie neben **Two FactorOFF aus**.
8. Wählen Sie im Feld **Benutzername** und im Feld **Gruppenname** die Werte aus und klicken Sie dann auf &**Erstellen**.
   Hinweis: Wenn Sie zuvor Clientzertifikate als Standardauthentifizierungstyp konfiguriert haben, verwenden Sie dieselben Namen, die Sie für die Richtlinie verwendet haben. Wenn Sie das Feld Benutzername und das Feld
   Gruppenname für den Standardauthentifizierungstyp ausgefüllt haben, verwenden Sie dieselben Werte für das Profil.
9. Wählen Sie im Dialogfeld **Authentifizierungsrichtlinie erstellen** neben **Benannte Ausdrücke** den Ausdruck aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen** und dann auf **Schließen**.

So binden Sie eine Clientzertifikatrichtlinie an einen virtuellen Server:

Nachdem Sie die Richtlinie für die Clientzertifikatauthentifizierung konfiguriert haben, können Sie sie an einen virtuellen Server binden.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Klicken Sie im Dialogfeld **Citrix Gateway Virtual Server** konfigurieren auf die Registerkarte **Authentifizierung**.
4. Klicken Sie **Primär** oder **Sekundär**.
5. Klicken Sie unter **Details**auf **Richtlinie einfügen**.
6. Wählen Sie unter **Richtlinienname**die Richtlinie aus, und klicken Sie dann auf **OK**.

So konfigurieren Sie einen virtuellen Server für die Anforderung des Clientzertifikats:

Wenn Sie ein Clientzertifikat für die Authentifizierung verwenden möchten, müssen Sie den virtuellen Server so konfigurieren, dass Clientzertifikate während des SSL-Handshakes angefordert werden.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen **virtuellen Server** und dann auf **Öffnen**.
3. Klicken Sie auf der Registerkarte **Zertifikate** auf **SSL-Parameter**.
4. Klicken Sie unter **Andere**auf **Clientauthentifizierung**.
5. Wählen Sie in **ClientzertifikatOptional**oder**Obligatorisch**und klicken Sie dann zweimal auf OK
   Wählen Sie**Optional** aus, wenn Sie andere Authentifizierungstypen auf demselben virtuellen Server zulassen möchten und keine Verwendung von Clientzertifikaten erfordern.

**Hinweis**

- Weitere Informationen zur Rückruf-URL finden Sie unter Importieren eines Citrix Gateway.
- Weitere Informationen zu Zertifikaten finden Sie unter Installieren, Verknüpfen und Aktualisieren von Zertifikaten.

## Zwei-Faktor-Zertifikatauthentifizierung konfigurieren

March 27, 2024

Sie können ein Clientzertifikat konfigurieren, um Benutzer zuerst zu authentifizieren, und dann von Benutzern verlangen, sich mit einem sekundären Authentifizierungstyp wie LDAP oder RADIUS anzumelden. In diesem Szenario authentifiziert das Clientzertifikat zuerst Benutzer. Dann erscheint eine Anmeldeseite, auf der sie ihren Benutzernamen und ihr Kennwort eingeben können. Wenn der Secure Sockets Layer (SSL) -Handshake abgeschlossen ist, kann die Anmeldesequenz einen der folgenden beiden Pfade annehmen:

- Weder der Benutzername noch die Gruppe werden aus dem Zertifikat extrahiert. Die Anmeldeseite wird dem Benutzer mit einer Aufforderung zur Eingabe gültiger Anmeldeinformationen angezeigt. Citrix Gateway authentifiziert die Benutzeranmeldeinformationen wie bei der normalen Kennwortauthentifizierung.
- Der Benutzername und der Gruppenname werden aus dem Clientzertifikat extrahiert. Wenn nur der Benutzername extrahiert wird, wird dem Benutzer eine Anmeldeseite angezeigt, auf der der Anmeldename vorhanden ist und der Benutzer den Namen nicht ändern kann. Nur das Kennwortfeld ist leer.

Gruppeninformationen, die Citrix Gateway während der zweiten Authentifizierungsrunde extrahiert, werden an die Gruppeninformationen angehängt, die Citrix Gateway aus dem Zertifikat extrahiert hat.

## Smartcardauthentifizierung konfigurieren

March 27, 2024

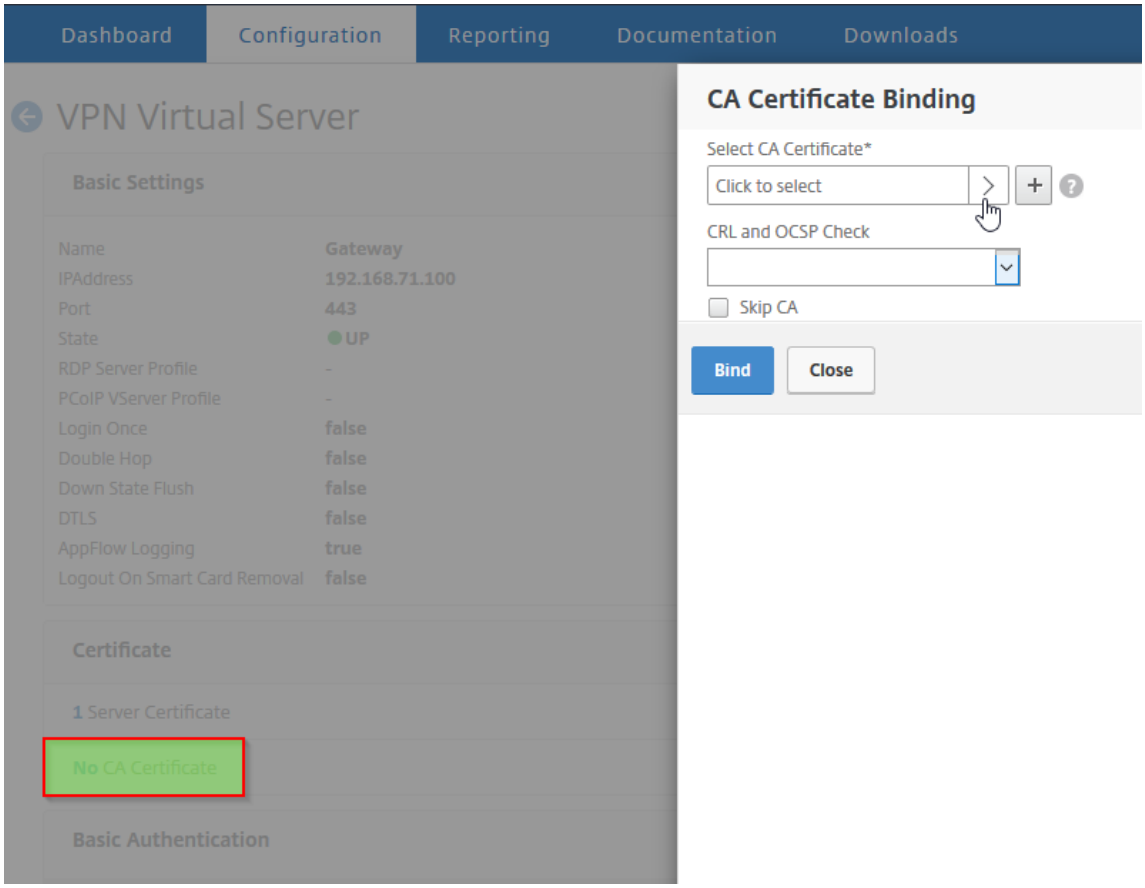
Sie können Citrix Gateway so konfigurieren, dass eine kryptografische Smartcard zur Authentifizierung von Benutzern verwendet wird.

Um eine Smartcard mit Citrix Gateway zu konfigurieren, müssen Sie Folgendes tun:

- Erstellen Sie eine Richtlinie zur Zertifikatauthentifizierung. Weitere Informationen finden Sie unter Konfigurieren der Clientzertifikatauthentifizierung.
- Binden Sie die Authentifizierungsrichtlinie an einen virtuellen Server.
- Fügen Sie das Stammzertifikat der Zertifizierungsstelle (CA), die die Clientzertifikate ausstellt, zu Citrix Gateway hinzu. Weitere Informationen finden Sie unter To install a root certificate on Citrix Gateway.

  **Wichtig**: Wenn Sie das Stammzertifikat für die Smartcard-Authentifizierung zum virtuellen Server hinzufügen, müssen Sie das Zertifikat aus der Liste **CA-Zertifikat auswählen auswählen**.




Nachdem Sie das Clientzertifikat erstellt haben, können Sie das als Flash bezeichnete Zertifikat auf die Smartcard schreiben. Wenn Sie diesen Schritt abgeschlossen haben, können Sie die Smartcard testen.

Wenn Sie das Webinterface für die Smartcard-Passthrough-Authentifizierung konfigurieren und eine der folgenden Bedingungen erfüllt ist, schlägt die einmalige Anmeldung am Webinterface fehl:

- Wenn Sie die Domäne stattdessen auf der Registerkarte **Veröffentlichte Anwendungen** als `mydomain`.com festlegen `mydomain`.

- Wenn Sie den Domänennamen nicht auf der Registerkarte **Veröffentlichte Anwendungen** festlegen und den Befehl `wi-sso-split-upn` ausführen, setzen Sie den Wert auf 1. In diesem Fall enthält der userPrincipalName den Domainnamen "`mydomain`.com. "

Sie können die Smartcard-Authentifizierung verwenden, um den Anmeldevorgang für Ihre Benutzer zu rationalisieren und gleichzeitig die Sicherheit des Benutzerzugriffs auf Ihre Infrastruktur zu verbessern. Der Zugriff auf das interne Unternehmensnetzwerk wird durch zertifikatbasierte Zwei-Faktor-Authentifizierung über die Public-Key-Infrastruktur geschützt. Private Schlüssel werden über die Hardware geschützt und verlassen nie die Smartcard. Die Benutzer können auf ihre Desktops und Anwendungen von unterschiedlichen Geräten des Unternehmens aus bequem mit Smartcard und PIN zugreifen.

Sie können Smartcards für die Benutzerauthentifizierung über StoreFront bei von Citrix Virtual Apps and Desktops bereitgestellten Desktops und Anwendungen verwenden. Smartcard-Benutzer, die sich bei StoreFront anmelden, können auch auf Anwendungen zugreifen, die von Citrix Endpoint Management bereitgestellt werden. Benutzer müssen sich jedoch erneut authentifizieren, um auf Endpoint Management-Webanwendungen zuzugreifen, die Clientzertifikatauthentifizierung verwenden.

Weitere Informationen finden Sie unter Konfigurieren der Smartcard-Authentifizierung in der StoreFront-Dokumentation.

### Konfigurieren der Smartcard-Authentifizierung mit sicheren ICA-Verbindungen

Benutzer, die sich mithilfe einer Smartcard mit auf Citrix Gateway konfigurierter Single Sign-On anmelden und eine sichere ICA-Verbindung herstellen, erhalten möglicherweise zweimal Aufforderungen zur Eingabe ihrer persönlichen Identifikationsnummer (PIN).

- Beim Anmelden und beim Versuch, eine veröffentlichte Ressource zu starten. Diese Situation tritt auf, wenn der Webbrowser und die Citrix Workspace-App denselben virtuellen Server verwenden, der für die Verwendung von Clientzertifikaten konfiguriert ist.
- Die Citrix Workspace-App teilt keinen Prozess oder eine Secure Sockets Layer (SSL) -Verbindung mit dem Webbrowser. Wenn die ICA-Verbindung den SSL-Handshake mit Citrix Gateway abschließt, ist das Clientzertifikat daher ein zweites Mal erforderlich.

Um zu verhindern, dass Benutzer die zweite PIN-Eingabeaufforderung erhalten, müssen Sie zwei Einstellungen ändern:

- Die Clientauthentifizierung auf dem virtuellen VPN-Server muss deaktiviert sein.
- SSL-Neuverhandlungen müssen aktiviert sein.

Binden Sie nach dem Konfigurieren des virtuellen Servers einen oder mehrere STA-Server an den virtuellen Server, wie unter Konfigurieren der Citrix Gateway-Einstellungen im Webinterface 5.3beschrieben.

Möglicherweise möchten Sie auch die Smartcard-Authentifizierung testen.

Deaktivieren der Clientauthentifizierung:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf Virtuelle Server.
2. Wählen Sie im Hauptdetailbereich den entsprechenden virtuellen Server aus, und klicken Sie dann auf Bearbeiten.
3. Klicken Sie im Bereich Erweiterte Optionen auf SSL-Parameter.
4. Deaktivieren Sie das Kontrollkästchen Clientauthentifizierung.
5. Klicken Sie auf Fertig.

So aktivieren Sie die SSL-Neuverhandlung:

1. Navigieren Sie mithilfe des Konfigurationsdienstprogramms auf der Registerkarte Konfiguration zu Traffic Management, und klicken Sie dann auf SSL.
2. Klicken Sie im Hauptbereich auf Erweiterte SSL-Einstellungen ändern.
3. Wählen Sie im Menü SSL-Neuverhandlung verweigern die Option NEIN aus.

So testen Sie die Smartcard-Authentifizierung:

1. Verbinden Sie die Smartcard mit dem Benutzergerät.
2. Öffnen Sie Ihren Webbrowser und melden Sie sich bei Citrix Gateway an.

## RADIUS-Authentifizierung konfigurieren

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass der Benutzerzugriff mit einem oder mehreren RADIUS-Servern authentifiziert wird. Wenn Sie RSA SecurID-, SafeWord- oder Gemalto Protiva-Produkte verwenden, wird jedes dieser Produkte mithilfe eines RADIUS-Servers konfiguriert.

Ihre Konfiguration erfordert möglicherweise die Verwendung einer Netzwerkzugriffsserver-IP-Adresse (NAS-IP) oder einer Netzwerkzugriffsserver-ID (NAS-ID). Beachten Sie beim Konfigurieren von Citrix Gateway für die Verwendung eines RADIUS-Authentifizierungsservers die folgenden Richtlinien:

- Wenn Sie die Verwendung der NAS-IP aktivieren, sendet die Appliance ihre konfigurierte IP-Adresse an den RADIUS-Server und nicht an die Quell-IP-Adresse, die für den Aufbau der RADIUS-Verbindung verwendet wurde.
- Wenn Sie die NAS-ID konfigurieren, sendet die Appliance den Bezeichner an den RADIUS-Server. Wenn Sie die NAS-ID nicht konfigurieren, sendet die Appliance ihren Hostnamen an den RADIUS-Server.

- Wenn Sie die NAS-IP aktivieren, ignoriert die Appliance alle NAS-IDs, die mithilfe der NAS-IP für die Kommunikation mit dem RADIUS-Server konfiguriert wurden.

### Konfigurieren von Gemalto Protiva

Protiva ist eine starke Authentifizierungsplattform, die Gemalto entwickelt hat, um die Stärken der Smartcard-Authentifizierung von Gemalto zu nutzen. Bei Protiva melden sich Benutzer mit einem Benutzernamen, einem Kennwort und einem Einmalkennwort an, das das Protiva-Gerät generiert. Ähnlich wie bei RSA SecurID wird die Authentifizierungsanforderung an den Protiva-Authentifizierungsserver gesendet, und der Server validiert oder lehnt das Kennwort ab. Verwenden Sie die folgenden Richtlinien, um Gemalto Protiva so zu konfigurieren, dass es mit Citrix Gateway kompatibel ist:

- Installieren Sie den Protiva-Server.
- Installieren Sie die Protiva SAS Agent Software, die den Internet Authentication Server (IAS) erweitert, auf einem Microsoft IAS RADIUS-Server. Vergewissern Sie sich, dass Sie die IP-Adresse und Portnummer des IAS-Servers notieren.
- Konfigurieren Sie ein RADIUS-Authentifizierungsprofil auf Citrix Gateway und geben Sie die Einstellungen des Protiva-Servers ein.

### Konfigurieren von SafeWord

Die SafeWord-Produktlinie bietet eine sichere Authentifizierung mit einem tokenbasierten Passcode. Nachdem der Benutzer den Passcode eingegeben hat, macht SafeWord den Passcode sofort ungültig und kann nicht erneut verwendet werden. Wenn Sie den SafeWord-Server konfigurieren, benötigen Sie die folgenden Informationen:

- Die IP-Adresse von Citrix Gateway. Die IP-Adresse muss dieselbe IP-Adresse sein, die Sie in der Konfiguration des RADIUS-Server-Clients konfiguriert haben. Citrix Gateway verwendet die interne IP-Adresse für die Kommunikation mit dem RADIUS-Server. Verwenden Sie bei der Konfiguration des Shared Secret die interne IP-Adresse. Wenn Sie zwei Appliances für Hochverfügbarkeit konfigurieren, verwenden Sie die virtuelle interne IP-Adresse.
- Ein gemeinsames Geheimnis.
- Die IP-Adresse und der Port des SafeWord-Servers. Die Standardportnummer ist 1812.

## So konfigurieren Sie die RADIUS-Authentifizierung

March 27, 2024

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Klicken Sie auf RADIUS, und klicken Sie dann im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Dialogfeld Authentifizierungsrichtlinie erstellen in das Feld Name einen Namen für die Richtlinie ein.
4. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
5. Klicken Sie neben Server auf Neu.
6. Geben Sie im Dialogfeld Authentifizierungsrichtlinie erstellen in das Feld Name einen Namen für den Server ein.
7. Geben Sie unter Server unter IP-Adresse die IP-Adresse des RADIUS-Servers ein.
8. Geben Sie in Port den Port ein. Die Standardeinstellung ist 1812.
9. Geben Sie unter Details unter Secret Key und Secret Key bestätigen das RADIUS-Servergeheimnis ein.
10. Geben Sie in NAS-ID die Identifikationsnummer ein und klicken Sie dann auf Erstellen.
11. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie erstellen neben Benannte Ausdrücke den Ausdruck aus, klicken Sie auf Ausdruck hinzufügen, klicken Sie auf Erstellen und dann auf Schließen.

## RADIUS-Authentifizierungsprotokoll wählen

March 27, 2024

Citrix Gateway unterstützt Implementierungen von RADIUS, die für die Verwendung mehrerer Protokolle für die Benutzerauthentifizierung konfiguriert sind, darunter:

- Kennwort Authentifizierungsprotokoll (PAP)
- Challenge-Handshake-Authentifizierungsprotokoll (CHAP)
- Microsoft Challenge-Handshake-Authentifizierungsprotokoll (MS-CHAP Version 1 und Version 2)

Wenn Ihre Bereitstellung des Citrix Gateway für die Verwendung der RADIUS-Authentifizierung konfiguriert ist und Ihr RADIUS-Server für die Verwendung von PAP konfiguriert ist, können Sie die Benutzerauthentifizierung verstärken, indem Sie dem RADIUS-Server ein starkes gemeinsames Geheimnis zuweisen. Starke gemeinsame RADIUS-Secrets bestehen aus zufälligen Sequenzen von Groß- und Kleinbuchstaben, Zahlen und Satzzeichen und sind mindestens 22 Zeichen lang. Verwenden Sie nach Möglichkeit ein Programm zur zufälligen Zeichengenerierung, um gemeinsam genutzte RADIUS-Geheimnisse zu ermitteln.

Weisen Sie jedem Citrix Gateway-Gerät oder virtuellen Server ein anderes gemeinsames Geheimnis zu, um den RADIUS-Verkehr weiter zu schützen. Wenn Sie Clients auf dem RADIUS-Server definieren, können Sie jedem Client auch ein separates Shared Secret zuweisen. In diesem Fall müssen Sie jede Citrix Gateway-Richtlinie, die die RADIUS-Authentifizierung verwendet, separat konfigurieren.

Wenn Sie eine RADIUS-Richtlinie erstellen, konfigurieren Sie freigegebene Geheimnisse auf Citrix Gateway als Teil der Richtlinie.

## IP-Adressextrahierung konfigurieren

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass die IP-Adresse von einem RADIUS-Server extrahiert wird. Wenn sich ein Benutzer beim RADIUS-Server authentifiziert, gibt der Server eine gerahmte IP-Adresse zurück, die dem Benutzer zugewiesen ist. Die gerahmte IP-Adresse wird in Zugriffsanfragen auch als RADIUS-Attribut 8-Frame-IP-Adresse bezeichnet.

Im Folgenden sind Komponenten für die Extraktion von IP-Adressen aufgeführt:

- Ermöglicht einem Remote-RADIUS-Server, eine IP-Adresse aus dem internen Netzwerk für einen bei Citrix Gateway angemeldeten Benutzer bereitzustellen.
- Ermöglicht die Konfiguration für jedes RADIUS-Attribut unter Verwendung der **Typ-IP-Adresse**, einschließlich herstellerkodierter Attribute.

Wenn Sie den RADIUS-Server für die IP-Adressenextraktion konfigurieren, konfigurieren Sie die Hersteller-ID und den Attributtyp. Die Hersteller-ID und die Attribute werden verwendet, um die Zuordnung zwischen dem RADIUS-Client und dem RADIUS-Server herzustellen.

- Die Hersteller-ID (ID) ermöglicht es dem RADIUS-Server, dem Client eine IP-Adresse aus einem Pool von IP-Adressen zuzuweisen, die auf dem RADIUS-Server konfiguriert sind. Die Hersteller-ID ist das Attribut in der RADIUS-Antwort, das die IP-Adresse des internen Netzwerks bereitstellt. Ein Wert von Null zeigt an, dass das Attribut nicht herstellercodiert ist
- Der Attributtyp ist das Remote-IP-Adressattribut in einer RADIUS-Antwort. Der Mindestwert ist 1 und der Maximalwert beträgt 255.

Eine übliche Konfiguration besteht darin, die **gerahmte IP-Adresse**des RADIUS-Attributs zu extrahieren. Die Lieferanten-ID ist auf 0 festgelegt oder nicht angegeben. Der Attributtyp ist auf 8 festgelegt.

**So konfigurieren Sie die IP-Adressextraktion von einem RADIUS-Server über die GUI:**

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Authentifizierung** und klicken Sie auf **RADIUS**.

2. Wählen Sie im Bereich **Details** auf der Registerkarte **Richtlinien** eine RADIUS-Richtlinie aus, und klicken Sie dann auf **Öffnen**.
3. Klicken **Sie im Dialogfeld Authentifizierungsrichtlinie konfigurieren** neben Server auf **Ändern**.
4. Geben **Sie unter Details**im Feld **Group Vendor Identifier**den Wert ein.
5. Geben Sie unter **Gruppenattributtyp**den Wert ein, und klicken Sie dann zweimal auf **OK**.

## RADIUS-Gruppen-Extraktion konfigurieren

March 27, 2024

Sie können die RADIUS-Autorisierung mithilfe einer Methode namens Gruppenextraktion konfigurieren. Durch die Konfiguration der Gruppenextraktion können Sie Benutzer auf Ihrem RADIUS-Server verwalten, anstatt sie zu Citrix Gateway hinzuzufügen.

Sie konfigurieren die RADIUS-Autorisierung mithilfe einer Authentifizierungsrichtlinie und Konfigurieren der Gruppen-Hersteller-ID (ID), des Gruppenattributtyps, des Gruppenpräfix und eines Gruppentrennzeichens. Wenn Sie die Richtlinie konfigurieren, fügen Sie einen Ausdruck hinzu und binden die Richtlinie dann entweder global oder an einen virtuellen Server.

### Konfigurieren von RADIUS auf Windows Server 2003

Wenn Sie Microsoft Internet Authentication Service (IAS) für die RADIUS-Autorisierung auf Windows Server 2003 verwenden, müssen Sie während der Konfiguration von Citrix Gateway die folgenden Informationen angeben:

- Die Lieferanten-ID ist der herstellerspezifische Code, den Sie in IAS eingegeben haben.
- Typ ist die vom Anbieter zugewiesene Attributnummer.
- Der Attributname ist der Typ des Attributnamens, den Sie in IAS definiert haben. Der Standardname ist CTXSUserGroups=

Wenn IAS nicht auf dem RADIUS-Server installiert ist, können Sie es über das Hinzufügen oder Entfernen von Programmen in der Systemsteuerung installieren. Weitere Informationen finden Sie in der Online-Hilfe von Windows.

Verwenden Sie zur Konfiguration von IAS die Microsoft Management Console (MMC) und installieren Sie das Snap-In für IAS. Folgen Sie dem Assistenten und stellen Sie sicher, dass Sie die folgenden Einstellungen auswählen:

- Wählen Sie den lokalen Computer aus.

- Wählen Sie RAS-Richtlinien aus und erstellen Sie eine benutzerdefinierte Richtlinie.
- Wählen Sie Windows-Gruppen für die Richtlinie aus.
- Wählen Sie eines der folgenden Protokolle aus:
  - Microsoft Challenge-Handshake-Authentifizierungsprotokoll Version 2 (MS-CHAP v2)
  - Microsoft Challenge-Handshake-Authentifizierungsprotokoll (MS-CHAP)
  - Challenge-Handshake-Authentifizierungsprotokoll (CHAP)
  - Unverschlüsselte Authentifizierung (PAP, SPAP)
- Wählen Sie das herstellerspezifische Attribut aus.

  Das herstellerspezifische Attribut muss die Benutzer, die Sie in der Gruppe auf dem Server definiert haben, mit den Benutzern auf Citrix Gateway abgleichen. Um diese Anforderung zu erfüllen, senden Sie die herstellerspezifischen Attribute an Citrix Gateway. Stellen Sie sicher, dass Sie Radius=Standard wählen.
- Der Radius-Standardwert ist 0. Verwenden Sie diese Nummer für den Lieferantencode.
- Die vom Anbieter zugewiesene Attributnummer ist 0.

  Dies ist die zugewiesene Nummer für das Attribut Benutzergruppe. Das Attribut ist im Zeichenfolgenformat.
- Wählen Sie Zeichenfolge für das Attributformat.

  Der Attributwert erfordert den Attributnamen und die Gruppen.

  Für das Access Gateway lautet der Attributwert ctxsUserGroups=groupName. Wenn zwei Gruppen definiert sind, wie Vertrieb und Finanzen, lautet der Attributwert ctxsUserGroups=Vertrieb; Finanzen. Trennen Sie jede Gruppe durch ein Semikolon.
- Entfernen Sie alle anderen Einträge im Dialogfeld “Einwählprofil bearbeiten”, wobei der Eintrag “Anbieterspezifisch”belassen wird.

Nachdem Sie die RAS-Richtlinie in IAS konfiguriert haben, konfigurieren Sie die RADIUS-Authentifizierung und -Autorisierung auf Citrix Gateway.

Verwenden Sie beim Konfigurieren der RADIUS-Authentifizierung die Einstellungen, die Sie auf dem IAS-Server konfiguriert haben.

### Konfigurieren von RADIUS für die Authentifizierung auf Windows Server 2008

Unter Windows Server 2008 konfigurieren Sie die RADIUS-Authentifizierung und -Autorisierung mithilfe des Netzwerkrichtlinienservers (NPS), der den Internetauthentifizierungsdienst (IAS) ersetzt. Sie verwenden Server-Manager und fügen NPS als Rolle hinzu, um ihn zu installieren.

Wenn Sie NPS installieren, wählen Sie den Netzwerkrichtliniendienst aus. Nach der Installation können Sie RADIUS-Einstellungen für Ihr Netzwerk konfigurieren, indem Sie den NPS über die Verwaltungsdienste im Startmenü starten. Wenn Sie den NPS öffnen, fügen Sie Citrix Gateway als RADIUS-Client hinzu und konfigurieren dann Servergruppen.

Stellen Sie bei der Konfiguration des RADIUS-Clients sicher, dass Sie die folgenden Einstellungen wählen:

- Wählen Sie für den Namen des Anbieters RADIUS Standard aus.
- Notieren Sie sich das Shared Secret, da Sie dasselbe freigegebene Geheimnis auf Citrix Gateway konfigurieren müssen.

Für die RADIUS-Gruppen benötigen Sie die IP-Adresse oder den Hostnamen des RADIUS-Servers. Ändern Sie die Standardeinstellungen nicht.

Nachdem Sie den RADIUS-Client und die Gruppen konfiguriert haben, konfigurieren Sie die Einstellungen in den folgenden beiden Richtlinien:

- Verbindungsanforderungsrichtlinien, in denen Sie die Einstellungen für die Citrix Gateway-Verbindung konfigurieren, einschließlich des Netzwerkservertyps, der Bedingungen für die Netzwerkrichtlinie und die Einstellungen für die Richtlinie.
- Netzwerkrichtlinien, in denen Sie die Authentifizierung des Extensible Authentication Protocol (EAP) und die herstellerspezifischen Attribute konfigurieren.

Wenn Sie die Verbindungsanforderungsrichtlinie konfigurieren, wählen Sie für den Typ des Netzwerkservers Nicht angegeben aus. Anschließend konfigurieren Sie Ihren Zustand, indem Sie den NAS-Port-Typ als Bedingung und Virtual (VPN) als Wert auswählen.

Wenn Sie eine Netzwerkrichtlinie konfigurieren, müssen Sie die folgenden Einstellungen konfigurieren:

- Wählen Sie Remote Access Server (VPN-DFÜ-Verbindung) als Typ des Netzwerkzugriffsservers aus.
- Wählen Sie Verschlüsselte Authentifizierung (CHAP) und Unverschlüsselte Authentifizierung (PAP und SPAP) für das EAP aus.
- Wählen Sie RADIUS-Standard für das herstellerspezifische Attribut aus.

  Die Standardattributnummer ist 26. Dieses Attribut wird für die RADIUS-Autorisierung verwendet.

  Citrix Gateway benötigt das herstellerspezifische Attribut, um die in der Gruppe auf dem Server definierten Benutzer mit denen auf Citrix Gateway abzugleichen. Dies erfolgt durch Senden der herstellerspezifischen Attribute an das Citrix Gateway.
- Wählen Sie String für das Attributformat.

Der Attributwert erfordert den Attributnamen und die Gruppen.

Für Citrix Gateway lautet der Attributwert ctxsUserGroups= groupname. Wenn zwei Gruppen definiert sind, wie Vertrieb und Finanzen, lautet der Attributwert ctxsUserGroups=Vertrieb; Finanzen. Trennen Sie jede Gruppe durch ein Semikolon.

- Das Trennzeichen ist das, das Sie im NPS verwendet haben, um Gruppen wie ein Semikolon, einen Doppelpunkt, ein Leerzeichen oder einen Punkt zu trennen.

Wenn Sie die Konfiguration der RAS-Richtlinie in IAS abgeschlossen haben, können Sie die RADIUS-Authentifizierung und -Autorisierung auf Citrix Gateway konfigurieren.

## RADIUS-Autorisierung konfigurieren

March 27, 2024

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Klicken Sie auf RADIUS.
3. Klicken Sie auf der Registerkarte Richtlinien auf Hinzufügen.
4. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
5. Unter dem Server* klicken Sie auf +
6. Geben Sie unter Name den Namen des RADIUS-Servers ein.
7. Geben Sie unter Server die IP-Adresse und den Port des RADIUS-Servers ein.
8. Geben Sie unter Details die Werte für Gruppen-Lieferanten-ID und Gruppenattributtyp ein.
9. Wählen Sie unter Password Encoding das Authentifizierungsprotokoll aus und klicken Sie dann auf Erstellen.
10. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie erstellen neben Benannte Ausdrücke den Ausdruck aus, klicken Sie auf Ausdruck hinzufügen, klicken Sie auf Erstellen und dann auf Schließen.

## RADIUS-Benutzerbuchhaltung konfigurieren

March 27, 2024

Citrix Gateway kann Nachrichten zum Start und Stoppen von Benutzersitzungen an Ihren RADIUS-Buchhaltungsserver senden. Die Nachrichten, die für jede Benutzersitzung gesendet werden, enthalten eine Teilmenge der in RFC2866 definierten Attribute. Tabelle 1 listet die unterstützten Attribute

und die Typen von RADIUS-Buchhaltungsnachrichten (RAD_START und RAD_STOP) auf, in denen sie gesendet werden. Tabelle 2 listet die vordefinierten Werte auf, die dem Attribut `Acct-Terminate-Cause` zugewiesen werden können, sowie die entsprechenden Citrix Gateway-Ereignisse.

Tabelle 1. Unterstützte RADIUS-Attribute

| Attribut | Bedeutung | RAD_START | RAD_STOP |
|---|---|---|---|
| Benutzername | Name des mit der Sitzung verknüpften Benutzers. | X | X |
| Sitzungs-ID | Die NetScaler-Sitzungs-ID. | X | X |
| Acct-Sitzungszeit | Sitzungsdauer Sekunden. | | X |
| Acct-Beendigung Ursache | Grund für die Kündigung des Kontos. | | X |

Tabelle 2. Ursachen für RADIUS-Kündigung

| NetScaler Logout-Methode | Ursache für RADIUS-Terminierung |
|---|---|
| LOGOUT_SESSN_TIMEDOUT | RAD_TERM_SESSION_TIMEOUT |
| LOGOUT_SESSN_INITIATEDBYUSER | RAD_TERM_USER_REQUEST |
| LOGOUT_SESSN_KILLEDBYADMIN | RAD_TERM_ADMIN_RESET |
| LOGOUT_SESSN_TLOGIN | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_MAXLICRCHD | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_CLISECCHK_FAILED | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_PREAUTH_CHANGED | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_COOKIE_MISMATCH | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSS_DHT | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSS_2FACTOR_FAIL | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_ICALIC | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_INTERNALERR | RAD_TERM_NAS_ERROR |
| Sonstiges | RAD_TERM_NAS_ERROR |

Die Konfiguration der RADIUS-Benutzerbuchhaltung erfordert die Erstellung eines Richtlinienpaars. Die erste Richtlinie ist eine RADIUS-Authentifizierungsrichtlinie, die einen RADIUS-Server angibt, an

den Buchhaltungsnachrichten gesendet werden sollen. Die zweite ist eine Sitzungsrichtlinie, die die RADIUS-Bilanzierungsrichtlinie als Aktion verwendet.

Um das RADIUS-Benutzerkonto zu konfigurieren, müssen Sie:

1. Erstellen Sie eine RADIUS-Richtlinie zur Definition des RADIUS-Buchhaltungsservers. Der Buchhaltungsserver kann derselbe Server sein, den Sie für die RADIUS-Authentifizierung verwenden.
2. Erstellen Sie eine Sitzungsrichtlinie, indem Sie die RADIUS-Richtlinie als Aktion verwenden, die den RADIUS-Benutzerbuchhaltungsserver angibt.
3. Binden Sie die Sitzungsrichtlinie entweder global, sodass sie für den gesamten Datenverkehr gilt, oder an einen virtuellen Citrix Gateway-Server, sodass sie nur für den Datenverkehr gilt, der durch diesen virtuellen Server fließt.

### So erstellen Sie eine RADIUS-Richtlinie

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich den Knoten Citrix Gateway und dann Richtlinien.
2. Erweitern Sie Authentifizierung und wählen Sie RADIUS
3. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
4. Geben Sie einen Namen für die Richtlinie ein.
5. Wählen Sie einen Server aus dem Server-Menü aus oder klicken Sie auf das Symbol + und folgen Sie den Anweisungen, um einen neuen RADIUS-Server hinzuzufügen.
6. Wählen Sie im Ausdrucksbereich aus dem Menü Gespeicherte Richtlinienausdrücke die Option ns_true aus.
7. Klicken Sie auf Erstellen.

### So erstellen Sie eine Sitzungsrichtlinie

Erstellen Sie nach dem Konfigurieren einer RADIUS-Richtlinie, die den RADIUS-Buchhaltungsserver angibt, wie folgt eine Sitzungsrichtlinie, die diesen Buchhaltungsserver in einer Aktion anwendet:

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich den Knoten Citrix Gateway und dann Richtlinien.
2. Wählen Sie Sitzung aus.
3. Wählen Sie im Hauptdetailbereich Hinzufügen aus.
4. Geben Sie einen Namen für die Richtlinie ein.
5. Klicken Sie im Menü Aktion auf das +-Symbol, um eine neue Sitzungsaktion hinzuzufügen.
6. Geben Sie einen Namen für die Sitzungsaktion ein.
7. Klicken Sie auf die Registerkarte Client Experience.
8. Wählen Sie im Menü Buchhaltungsrichtlinie die RADIUS-Richtlinie aus, die Sie zuvor erstellt haben.

9. Klicken Sie auf Erstellen.
10. Wählen Sie im Ausdrucksbereich aus dem Menü Gespeicherte Richtlinienausdrücke die Option ns_true aus.
11. Klicken Sie auf Erstellen.

### So binden Sie die Sitzungsrichtlinie global

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich den Knoten Citrix Gateway und dann Richtlinien.
2. Wählen Sie Sitzung aus.
3. Wählen Sie im Menü Aktion im Hauptdetailbereich Globale Bindungen aus.
4. Klicken Sie auf Bind.
5. Wählen Sie im Bereich Richtlinien die zuvor erstellte Sitzungsrichtlinie aus, und klicken Sie dann auf Einfügen.
6. Klicken Sie in den Listen Richtlinien auf den Eintrag Priorität für die Sitzungsrichtlinie und geben Sie einen Wert zwischen 0 und 64000 ein.
7. Klicken Sie auf OK.

### So binden Sie die Sitzungsrichtlinie an einen virtuellen Citrix Gateway-Server

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich den Knoten Citrix Gateway, und wählen Sie dann Virtuelle Server aus.
2. Wählen Sie im Hauptdetailbereich einen virtuellen Server aus, und klicken Sie dann auf Bearbeiten.
3. Klicken Sie im Bereich Richtlinien auf das Symbol +, um eine Richtlinie auszuwählen.
4. Wählen Sie im Menü Richtlinie wählen die Option Sitzung aus und stellen Sie sicher, dass Anforderung im Menü Typ wählen ausgewählt ist.
5. Klicken Sie auf Weiter.
6. Klicken Sie auf Bind.
7. Wählen Sie im Bereich Richtlinien die zuvor erstellte Sitzungsrichtlinie aus, und klicken Sie dann auf Einfügen.
8. Klicken Sie auf OK.

## SAML-Authentifizierung konfigurieren

March 27, 2024

Die Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für den Austausch von Authentifizierung und Autorisierung zwischen Identity Providern (IdP) und Service Providern. Citrix Gateway unterstützt SAML-Authentifizierung.

Wenn Sie die SAML-Authentifizierung konfigurieren, erstellen Sie die folgenden Einstellungen:

- IdP-Zertifikatsname. Dies ist der öffentliche Schlüssel, der dem privaten Schlüssel beim IdP entspricht.
- Umleitungs-URL. Dies ist die URL des Authentifizierungs-IdP. Benutzer, die nicht authentifiziert sind, werden auf diese URL umgeleitet.
- Benutzer-Feld. Sie können dieses Feld verwenden, um den Benutzernamen zu extrahieren, wenn der IdP den Benutzernamen in einem anderen Format als das NameIdentifier-Tag des Subject -Tags sendet. Dies ist eine optionale Einstellung.
- Name des signierenden Zertifikats. Dies ist der private Schlüssel des Citrix Gateway-Servers, mit dem die Authentifizierungsanforderung an den IdP signiert wird. Wenn Sie keinen Zertifikatnamen konfigurieren, wird die Assertion unsigniert gesendet oder die Authentifizierungsanforderung wird abgelehnt.
- Name des SAML-Ausstellers. Dieser Wert wird verwendet, wenn die Authentifizierungsanfrage gesendet wird. Das Feld des Emittenten muss einen eindeutigen Namen enthalten, um die Behörde anzugeben, von der die Assertion gesendet wird. Dies ist ein optionales Feld.
- Standard-Authentifizierungsgruppe. Dies ist die Gruppe auf dem Authentifizierungsserver, von der aus Benutzer authentifiziert werden.
- Zwei Faktor. Diese Einstellung aktiviert oder deaktiviert die Zwei-Faktor-Authentifizierung.
- Lehnen Sie eine unsignierte Assertion ab. Wenn aktiviert, lehnt Citrix Gateway die Benutzerauthentifizierung ab, wenn der Name des Signaturzertifikats nicht konfiguriert ist.

Citrix Gateway unterstützt die HTTP-Nachbindung. In dieser Bindung antwortet die sendende Partei dem Benutzer mit einem 200-OK, das einen form-automatischen Beitrag mit den erforderlichen Informationen enthält. Insbesondere muss das Standardformular zwei versteckte Felder mit dem Namen `SAMLRequest` und `SAMLResponse` enthalten, je nachdem, ob es sich bei dem Formular um eine Anfrage oder eine Antwort handelt. Das Formular enthält auch RelayState, bei dem es sich um einen Status oder Informationen handelt, die von der sendenden Partei verwendet wird, um willkürliche Informationen zu senden, die nicht von der versendenden Partei verarbeitet werden. Die vertrauende Partei sendet die Informationen zurück, sodass die sendende Partei weiß, was als Nächstes zu tun ist, wenn die sendende Partei die Assertion zusammen mit RelayState erhält. Es wird empfohlen, den RelayState zu verschlüsseln oder zu verschleiern.

> **Hinweis**
>
> - Wenn Citrix Gateway als IdP für Citrix Cloud verwendet wird, müssen Sie die **RelayState-Regel** auf Citrix Gateway nicht konfigurieren.

> - Im Falle einer IdP-Verkettung reicht es aus, die **RelayState-Regel** nur für die erste SAML-Richtlinie zu konfigurieren. In diesem Zusammenhang ist IdP-Ketten ein Szenario, in dem sich eine konfigurierte SAML-Aktion auf einen virtuellen Authentifizierungsserver-IdP bezieht, der eine weitere SAML-Aktion enthält.

### Konfigurieren der Active Directory-Verbunddienste 2.0

Sie können Active Directory-Verbunddienste (AD FS) 2.0 auf jedem Windows Server 2008- oder Windows Server 2012-Computer konfigurieren, den Sie in einer Verbundserverrolle verwenden. Wenn Sie den ADFS-Server so konfigurieren, dass er mit Citrix Gateway kompatibel ist, müssen Sie die folgenden Parameter mit dem Vertrauensassistenten für vertrauende Parteien in Windows Server 2008 oder Windows Server 2012 konfigurieren.

Windows Server 2008 Parameter:

- Vertrauen auf Partei vertrauen. Sie geben den Speicherort der Citrix Gateway-Metadatendatei an `https://vserver.fqdn.com/ns.metadata.xml`, z. B. wo vserver.fqdn.com der vollqualifizierte Domänenname (FQDN) des virtuellen Citrix Gateway-Servers ist. Sie finden den FQDN auf dem Serverzertifikat, das an den virtuellen Server gebunden ist.
- Autorisierungsregeln. Sie können Benutzern den Zugriff auf die verantwortende Partei gewähren oder verweigern.

Windows Server 2012 Parameter:

- Vertrauen auf Partei vertrauen. Sie geben den Speicherort der Citrix Gateway-Metadatendatei an `https://vserver.fqdn.com/ns.metadata.xml`, z. B. wo vserver.fqdn.com der vollqualifizierte Domänenname (FQDN) des virtuellen Citrix Gateway-Servers ist. Sie finden den FQDN auf dem Serverzertifikat, das an den virtuellen Server gebunden ist.
- ADFS-Profil. Wählen Sie das ADFS-Profil aus.
- Zertifikat. Citrix Gateway unterstützt keine Verschlüsselung. Sie müssen kein Zertifikat auswählen.
- Aktivieren Sie die Unterstützung für das SAML 2.0 WebSSO-Protokoll. Dies ermöglicht die Unterstützung von SAML 2.0 SSO. Sie geben die URL des virtuellen Citrix Gateway-Servers an, z. `https:netScaler.virtualServerName.com/cgi/samlauth`B.

  Diese URL ist die Assertion Consumer Service-URL auf dem Citrix Gateway-Gerät. Dies ist ein konstanter Parameter und Citrix Gateway erwartet eine SAML-Antwort auf diese URL.
- Vertrauenskennung der vertrauenden Partei. Geben Sie den Namen Citrix Gateway ein. Dies ist eine URL, die verlässt, die beteiligten Parteien identifiziert, wie z. B. `https://netscalerGateway.virtualServerName.com/adfs/services/trust`.

- Autorisierungsregeln. Sie können Benutzern den Zugriff auf die verantwortende Partei gewähren oder verweigern.
- Konfigurieren Sie Antragsregeln. Sie können die Werte für LDAP-Attribute mithilfe von Ausgabentransformationsregeln konfigurieren und die Vorlage LDAP-Attribute als Forderungen senden verwenden. Sie konfigurieren dann LDAP-Einstellungen, die Folgendes beinhalten:
  - Email-Adressen
  - sAMAccountName
  - User Principal Name (UPN)
  - MemberOf
- Signatur des Zertifikats. Sie können die Signaturüberprüfungszertifikate angeben, indem Sie die Eigenschaften einer weiterleitenden Partei auswählen und dann das Zertifikat hinzufügen.

  Wenn das Signaturzertifikat weniger als 2048 Bit beträgt, wird eine Warnmeldung angezeigt. Sie können die Warnung ignorieren, um fortzufahren. Wenn Sie eine Testbereitstellung konfigurieren, deaktivieren Sie die Zertifikatsperrliste (CRL) auf der weiterleiten Partei. Wenn Sie die Prüfung nicht deaktivieren, versucht AD FS die CRL, das Zertifikat zu validieren.

  Sie können die CRL deaktivieren, indem Sie den folgenden Befehl ausführen: Set-ADFWRelayingPartyTrust - SigningCertficateRevocatonCheck None-TargetName NetScaler

Nachdem Sie die Einstellungen konfiguriert haben, überprüfen Sie die Daten der vertrauenden Partei, bevor Sie den Relaying Party Trust Wizard abschließen. Sie überprüfen das Zertifikat des virtuellen Citrix Gateway-Servers mit der Endpunkt-URL, z. `https://vserver.fqdn.com/cgi/samlauth` B.

Nachdem Sie die Konfiguration der Einstellungen im Relaying Party Trust Wizard abgeschlossen haben, wählen Sie die konfigurierte Vertrauensstellung aus und bearbeiten Sie dann die Eigenschaften. Führen Sie folgende Schritte aus:

- Stellen Sie den sicheren Hash-Algorithmus auf SHA-1 ein.

  Hinweis: Citrix unterstützt nur SHA-1.
- Löschen Sie das Verschlüsselungszertifikat. Verschlüsselte Behauptungen werden nicht unterstützt.
- Bearbeiten Sie die Anspruchsregeln, einschließlich der folgenden:
  - Wählen Sie Transformationsregel
  - Anspruchsregel hinzufügen
  - Wählen Sie Vorlage für Anspruchsregeln: LDAP-Attribute als Ansprüche senden
  - Gib einen Namen
  - Attributspeicher wählen: Active Directory

- Wählen Sie das LDAP-Attribut: <Active Directory parameters>
- Wählen Sie Regel für ausgehende Ansprüche als "Namens-ID"

Hinweis: XML-Tags für Attributnamen werden nicht unterstützt.

- Konfigurieren Sie die Abmelde-URL für die einmalige Abmeldung. Die Anspruchsregel lautet Abmelde-URL senden. Die benutzerdefinierte Regel muss wie folgt lauten:

```
pre codeblock => issue(Type = "logoutURL", Value = "https://<adfs
.fqdn.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws
/2005/05/identity/claimproperties/attributename"] = "urn:oasis:
names:tc:SAML:2.0:attrname-format:unspecified"); <!--NeedCopy-->
```

Nachdem Sie die AD FS-Einstellungen konfiguriert haben, laden Sie das AD FS-Signaturzertifikat herunter und erstellen Sie dann einen Zertifikatschlüssel auf Citrix Gateway. Sie können dann die SAML-Authentifizierung auf Citrix Gateway mit Zertifikat und Schlüssel konfigurieren.

### Konfigurieren der SAML-Zwei-Faktor-Authentifizierung

Sie können die SAML-Zwei-Faktor-Authentifizierung konfigurieren. Wenn Sie die SAML-Authentifizierung mit LDAP-Authentifizierung konfigurieren, beachten Sie die folgenden Leitlinien:

- Wenn SAML der primäre Authentifizierungstyp ist, deaktivieren Sie die Authentifizierung in der LDAP-Richtlinie und konfigurieren Sie die Gruppenextraktion. Binden Sie dann die LDAP-Richtlinie als sekundären Authentifizierungstyp.
- Die SAML-Authentifizierung verwendet kein Kennwort und verwendet nur den Benutzernamen. Außerdem informiert die SAML-Authentifizierung Benutzer nur, wenn die Authentifizierung erfolgreich ist. Wenn die SAML-Authentifizierung fehlschlägt, werden Benutzer nicht benachrichtigt. Da keine Fehlerantwort gesendet wird, muss SAML entweder die letzte Richtlinie in der Kaskade oder die einzige Richtlinie sein.
- Es wird empfohlen, tatsächliche Benutzernamen anstelle von undurchsichtigen Zeichenfolgen zu konfigurieren.
- SAML kann nicht als sekundärer Authentifizierungstyp gebunden werden.

## So konfigurieren Sie die SAML-Authentifizierung

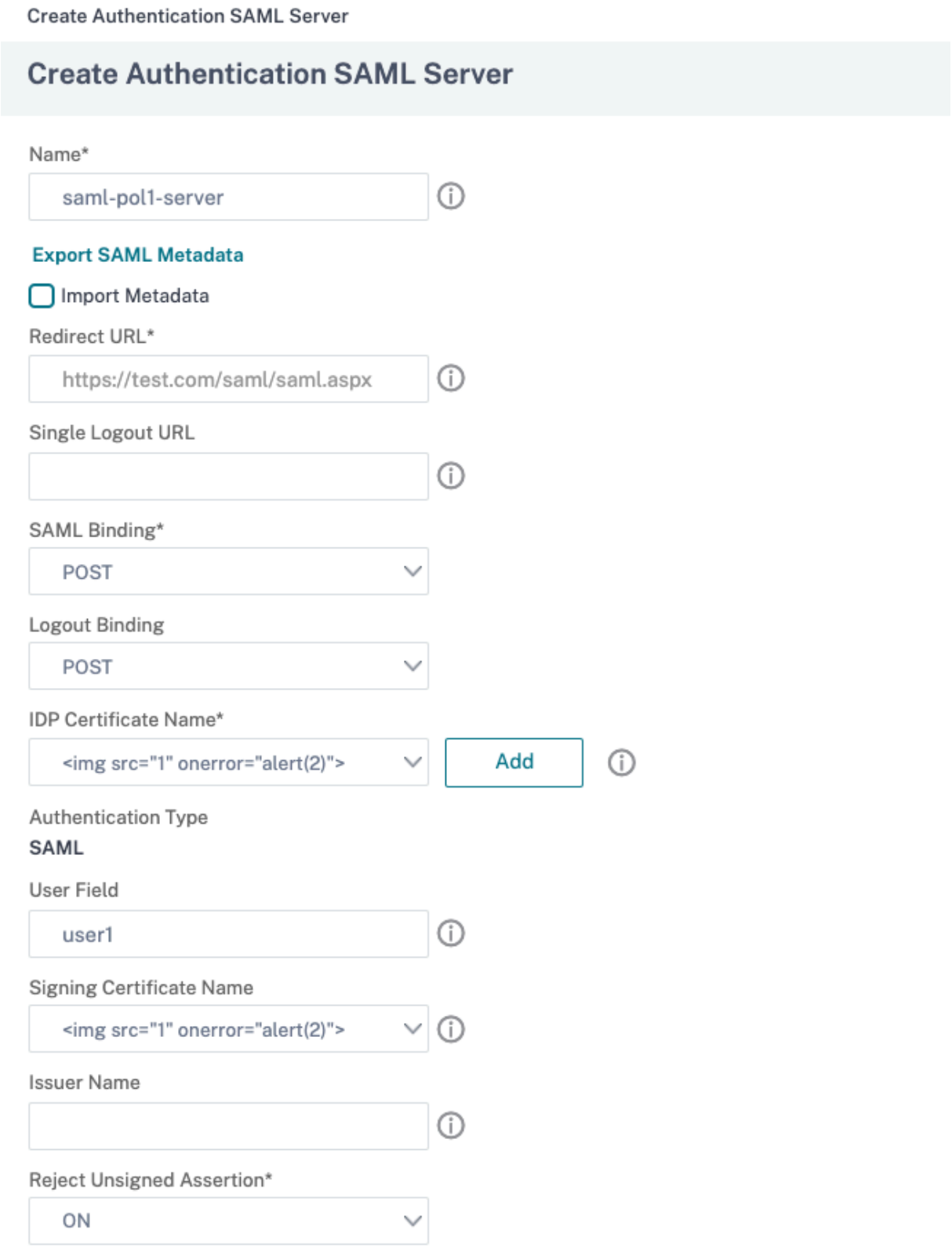
March 27, 2024

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.

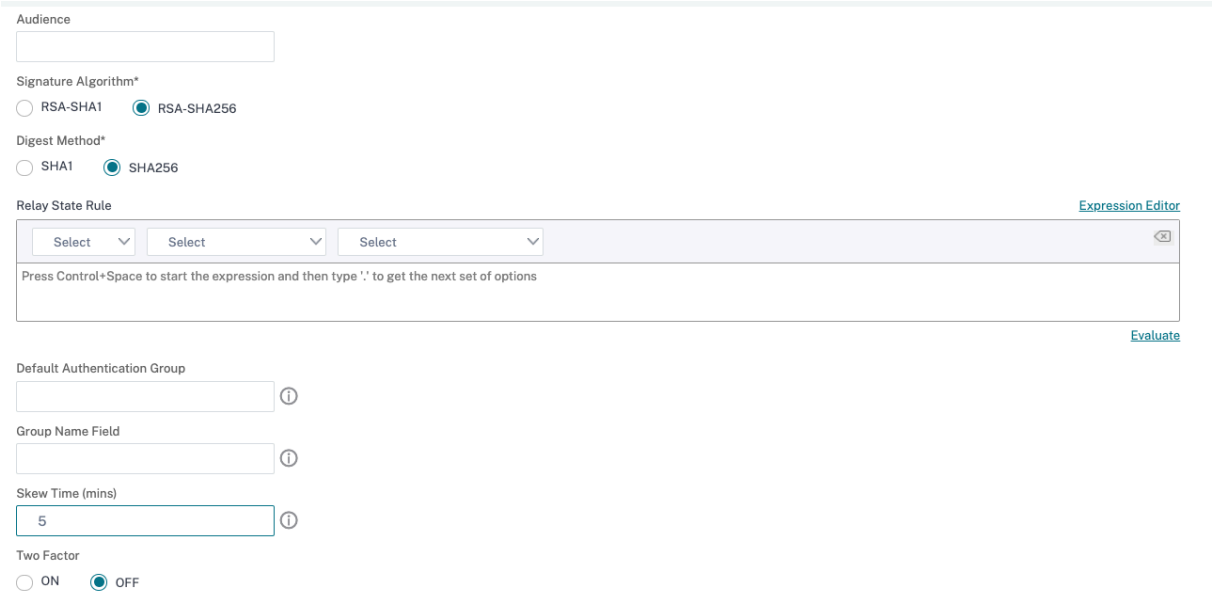
 

2. Klicken Sie im Navigationsbereich auf **SAML.**
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Geben Sie im Dialogfeld Authentifizierungsrichtlinie erstellen in das Feld **Name**einen Namen für die Richtlinie ein.






1. Klicken Sie neben Server auf **Neu**.
2. Geben Sie **unter Name**einen Namen für das Serverprofil ein.
3. Wählen Sie unter IdP Certificate Name ein Zertifikat aus oder klicken Sie auf **Installieren**. Dies ist das auf dem SAML- oder IdP-Server installierte Zertifikat.

   Wenn Sie auf Installieren klicken, fügen Sie das Zertifikat und den privaten Schlüssel hinzu. Weitere Informationen finden Sie unter Installieren und Verwalten von Zertifikaten.
4. Geben Sie unter **Umleitungs-URL**die URL des Identitätsanbieters für die Authentifizierung (IdP) ein.

   Dies ist die URL für die Benutzeranmeldung beim SAML-Server. Dies ist der Server, an den Citrix Gateway die erste Anfrage umleitet.
5. Geben Sie unter **Single Logout URL**die URL an, damit die Appliance erkennen kann, wann der Client an den IdP zurückgesendet werden muss, um den Abmeldevorgang abzuschließen.
6. Wählen Sie in **SAML-Bindung**die Methode aus, mit der der Client vom SP zum IdP verschoben werden soll. Dies muss beim IdP gleich sein, damit er versteht, wie sich der Client mit ihm verbindet. Wenn die Appliance als SP fungiert, unterstützt sie POST-, REDIRECT- und ARTIFACT-Bindungen.
7. Wählen Sie unter **Logout-Bindung**die Option **REDIRECT aus.**
8. Wählen Sie unter **IDP Certificate Name**das IDPcert Certificate (Base64) aus, das unter dem SAML-Signaturzertifikat vorhanden ist.

> **Hinweis:**
>
> Sie können auch auf **Metadaten importieren** klicken und die URL auswählen, unter der die Metadatenkonfiguration gespeichert wird.

9. Geben Sie im **Benutzerfeld**den zu extrahierenden Benutzernamen ein.
10. Wählen Sie unter **Signaturzertifikatname**das SAML SP-Zertifikat (mit privatem Schlüssel) aus, das die Appliance verwendet, um Authentifizierungsanforderungen an den IdP zu signieren. Das gleiche Zertifikat (ohne privaten Schlüssel) muss in den IdP importiert werden, damit der IdP die Signatur der Authentifizierungsanfrage überprüfen kann. Dieses Feld wird von den meisten IDPs nicht benötigt

    Dies ist das Zertifikat, das an die virtuelle IP-Adresse von Citrix Gateway gebunden ist. Der SAML-Ausstellername ist der vollqualifizierte Domainname (FQDN), bei dem sich Benutzer anmelden, z. B. lb.example.com oder ng.example.com.
11. Geben Sie **unter Name des Ausstellers**den FQDN der Lastenausgleich- oder Citrix Gateway-IP-Adresse ein, an die das Gerät die anfängliche Authentifizierungsanforderung (GET) sendet.
12. Geben Sie im Feld **Assertion ohne Vorzeichen ablehnen**an, ob die Assertions vom IdP signiert werden sollen. Sie können sicherstellen, dass nur die Assertion signiert werden muss (ON) oder dass sowohl die Behauptung als auch die Antwort des IdP signiert werden müssen (STRICT).
13. Geben Sie in **Audience**das Publikum ein, für das die vom IdP gesendete Assertion anwendbar ist. Dies ist normalerweise ein Entitätsname oder eine URL, die den Dienstanbieter darstellt.
14. Wählen Sie in **Signature Algorithm**RSA-SHA256
15. Wählen Sie in **Digest-Methode**SHA256
16. Geben Sie unter **Standardauthentifizierungsgruppe**zusätzlich zu den extrahierten Gruppen die Standardgruppe ein, die ausgewählt wird, wenn die Authentifizierung erfolgreich ist.
17. Geben Sie **unter Gruppenname**den Namen des Tags in der Assertion ein, die Benutzergruppen enthält.
18. Geben Sie im **Skew Time (Minuten)**den zulässigen Taktversatz in Minuten an, den der Dienstanbieter bei einer eingehenden Assertion zulässt.
19. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
20. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie erstellen neben Benannte Ausdrücke die Option Allgemein aus, wählen Sie Wahrer Wert aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

### Referenzen

- Citrix ADC als SAML SP
- Citrix ADC als SAML-IdP
- Zusätzliche Funktionen für SAML unterstützt

## SAML-Authentifizierung zum Anmelden bei Citrix Gateway verwenden

March 27, 2024

Sie können die SAML-Authentifizierung verwenden, um sich mit den Citrix VPN-Clients und der Workspace-App bei Citrix Gateway anzumelden. Das Plug-in unterstützt die SAML-Authentifizierung nur über erweiterte SAML-Richtlinien, die an den virtuellen Authentifizierungsserver gebunden sind, dh die nFactor-Authentifizierung.

**Wichtig**: Das Plug-in unterstützt keine SAML-Authentifizierung, wenn SAML-Richtlinien direkt an den virtuellen VPN-Server gebunden sind, dh Nicht-NFactor-Authentifizierung.

### Unterstützte Plattformen und Apps

In der folgenden Tabelle sind die Plattformen und Anwendungen aufgeführt, die SAML-Authentifizierung für die Anmeldung bei Citrix Gateway unterstützen.

| Product | Version |
|---|---|
| Citrix Gateway | Version 12.0 Build 41.16 und höher |
| VPN-Kunde | Version 12.1 Build 49.37 und höher.<br>**Unterstützte Plattformen**: Windows 7, Windows 8, Windows 8.1, Windows 10 |
| Versionen der Workspace-App | Windows: 1808; Mac: 1808 |

### Konfigurieren für die SAML-Authentifizierung mithilfe erweiterter SAML-Richtlinien

Einzelheiten zur Konfiguration der SAML-Authentifizierung mithilfe erweiterter SAML-Richtlinien finden Sie unter Citrix ADC als SAML-IdP.

# Verbesserungen bei der SAML-Authentifizierung

March 27, 2024

Diese Funktion erfordert SAML-Kenntnisse, grundlegende Authentifizierungskenntnisse und FIPS-Verständnis, um diese Informationen verwenden zu können.

Sie können die folgenden Citrix ADC-Funktionen mit Anwendungen und Servern von Drittanbietern verwenden, die mit der SAML 2.0-Spezifikation kompatibel sind:

- SAML-Dienstanbieter (SP)
- SAML Identity Provider (IdP)

SP und IdP ermöglichen einen Single Sign-On (SSO) zwischen Cloudservices. Die SAML SP-Funktion bietet eine Möglichkeit, Benutzeransprüche eines IdP zu adressieren. Der IdP kann ein Drittanbieterdienst oder eine andere Citrix ADC Appliance sein. Die SAML-IdP-Funktion wird verwendet, um Benutzeranmeldungen geltend zu machen und von SPs verbrauchte Ansprüche bereitzustellen.

Im Rahmen der SAML-Unterstützung signieren sowohl IdP- als auch SP-Module die Daten, die an Peers gesendet werden, digital. Die digitale Signatur umfasst eine Authentifizierungsanforderung von SP, Assertion von IdP und Abmeldungen zwischen diesen beiden Entitäten. Die digitale Signatur bestätigt die Echtheit der Nachricht.

Die aktuellen Implementierungen von SAML SP und IdP führen die Signaturberechnung in einer Paket-Engine durch. Diese Module verwenden SSL-Zertifikate, um die Daten zu signieren. In einem FIPS-konformen Citrix ADC ist der private Schlüssel des SSL-Zertifikats nicht in der Paket-Engine oder im Benutzerbereich verfügbar, sodass das SAML-Modul heute nicht für FIPS-Hardware bereit ist.

In diesem Dokument wird der Mechanismus zum Auslagern von Signaturberechnungen auf die FIPS-Karte beschrieben. Die Signaturüberprüfung erfolgt in der Software, da der öffentliche Schlüssel verfügbar ist.

## Lösung

Der SAML-Funktionssatz wurde erweitert, um eine SSL-API für den Signatur-Offload zu verwenden. Einzelheiten zu diesen betroffenen SAML-Unterfunktionen finden Sie in der Citrix Produktdokumentation:

1. SAML SP Post Binding —Signieren von AuthnRequest
2. SAML IdP Post Binding - Unterzeichnung der Assertion/Response/Both
3. SAML SP Single Logout Szenarien —Signieren von LogoutRequest im SP-initiierten Modell und Signieren von LogoutResponse im IdP-initiierten Modell

4. SAML SP Artefakt-Bindung —Signieren einer ArtifactResolve-Anfrage
5. SAML SP Redirect Binding —Signieren von AuthnRequest
6. SAML IdP Redirect Binding - Signieren von Response/Assertion/Both
7. Unterstützung von SAML SP Encryption —Entschlüsselung von Assertion

### Plattform

Die API kann nur auf eine FIPS-Plattform ausgelagert werden.

### Konfiguration

Die Offload-Konfiguration erfolgt automatisch auf der FIPS-Plattform.

Da private SSL-Schlüssel jedoch nicht für den Benutzerbereich in FIPS-Hardware verfügbar sind, ändert sich das Erstellen des SSL-Zertifikats auf FIPS-Hardware geringfügig an der Konfiguration.

Hier sind die Konfigurationsinformationen:

- `add ssl fipsKey fips-key`

  Erstellen Sie eine CSR und verwenden Sie sie auf dem CA-Server, um ein Zertifikat zu generieren. Sie können das Zertifikat dann in kopieren `/nsconfig/ssl`. Nehmen wir an, dass die Datei fips3cert.cerist.

- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  Geben Sie dann dieses Zertifikat in der SAML-Aktion für das SAML SP-Modul an.

- `set samlAction <name> -samlSigningCertName fips-cert`

  Ebenso verwenden Sie dies im Modul `samlIdpProfile` für das SAML-IdP-Modul.

- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

Beim ersten Mal haben Sie das im vorhergehenden Abschnitt `fips-key` beschriebene nicht. Wenn kein FIPS-Schlüssel vorhanden ist, erstellen Sie einen, wie unter Erstellen eines FIPS-Schlüssels beschrieben.

```
1 create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent
      (3 | F4)]
2
3 create certreq <reqFileName> -fipskeyName <string>
4 <!--NeedCopy-->
```

# TACACS+ Authentifizierung konfigurieren

March 27, 2024

Sie können einen TACACS+-Server für die Authentifizierung konfigurieren. Ähnlich wie bei der RADIUS-Authentifizierung verwendet TACACS+ einen geheimen Schlüssel, eine IP-Adresse und die Portnummer. Die Standardportnummer ist 49.

Um Citrix Gateway für die Verwendung eines TACACS+-Servers zu konfigurieren, geben Sie die Server-IP-Adresse und das TACACS+-Geheimnis an. Sie müssen den Port nur angeben, wenn die verwendete Server-Portnummer etwas anderes als die Standardportnummer 49 ist.

Führen Sie die folgenden Schritte aus, um die TACACS+-Authentifizierung über die Benutzeroberfläche zu konfigurieren.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
2. Klicken Sie auf **TACACS**.
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Geben Sie im Feld **Name** einen Namen für die Richtlinie ein.
5. Klicken Sie neben dem Feld **Server** auf **Hinzufügen**, um einen neuen TACACS-Server zu erstellen, oder klicken Sie auf **Bearbeiten**, um Änderungen an einem vorhandenen TACACS-Server vorzunehmen.
6. Geben Sie im Feld **Name** einen Namen für den Server ein.
7. Geben **Sie unter IP-Adresse**die IP-Adresse ein.
8. Verwenden Sie unter **Port**die Standardportnummer 49.
9. Geben Sie im Feld **TACACS Key** den Schlüssel ein. Geben **Sie im Feld TACACS-Schlüssel** bestätigen denselben Schlüssel zur Bestätigung ein.
10. Klicken Sie auf **Mehr**.
11. Wählen Sie unter **AutorisierungON**aus und klicken Sie dann auf**Erstellen**.
12. Wählen **Sie im Dialogfeld TACACS-Richtlinie für Authentifizierung erstellen** den Ausdruck aus, klicken Sie auf Erstellen und dann auf Schließen.

Um die TACACS+-Authentifizierung über die Befehlszeilenschnittstelle zu konfigurieren, geben Sie den folgenden Befehl ein.

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr
    |*>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -tacacsSecret  }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-
    auditFailedCmds ( ON | OFF )] [-groupAttrName <string>][-
    defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-
    Attribute2 <string>] [-Attribute3 <string>] [-Attribute4 <string>]
```

```
5 [-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
     Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]
6 [-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>]
      [-Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <
     string>]
7 <!--NeedCopy-->
```

Nachdem Sie die TACACS+-Servereinstellungen in Citrix Gateway konfiguriert haben, binden Sie die Richtlinie, damit sie aktiv wird. Sie können die Richtlinie entweder auf globaler oder auf virtueller Serverebene binden. Weitere Informationen zum Binden von Authentifizierungsrichtlinien finden Sie unter Binden von Authentifizierungsrichtlinien.

## Clear Config Basic Must Not Clear TACACS Config

March 27, 2024

Dieses Thema konzentriert sich darauf, nicht alle RBA-bezogenen Konfigurationen (Rollenbasierter Zugriff) zu löschen, wenn der Befehl clear config ausgeführt wird.

Der aktuelle Befehl clear config wird in einer von drei Ebenen ausgeführt:

- Einfach
- Verlängert
- Voll

Basierend auf der Ebene werden Citrix ADC-Konfigurationen gelöscht und auf die Werkseinstellungen zurückgesetzt.

Der verwendete Befehl lautet:

```
1 clear ns config [-force] <level>
2 <!--NeedCopy-->
```

Der neue Befehl fügt einen Knopf hinzu, um das Löschen aller RBA-bezogenen Konfigurationen zu erlauben/zu verweigern.

### Neuer Befehl

Beschrieben werden die Clear RBA-Konfigurationsfunktionen:

1. JA/NEIN-Regler mit Standard: JA.

   Der Administrator entscheidet, ob die RBA-Konfiguration beibehalten werden soll oder nicht.

2. NUR das BASIC LEVEL von clear config wird unterstützt.

3. Die folgenden Konfigurationen wurden nicht gelöscht:

    - Systembenutzer/-gruppe hinzufügen/binden.
    - Fügen Sie eine cmd-Richtlinie hinzu.
    - TACACS-Befehle (TACACS-Aktion/Richtlinie hinzufügen).
    - Bindesystem global

    **Hinweis:** TACACS-bezogene Konfiguration (Aktion/Richtlinie) wird beibehalten, wenn die Richtlinie an das System global gebunden ist oder gelöscht wird

### CLI-Konfiguration

Der verwendete Befehl lautet:

```
clear config [ – force] <level> [-RBAconfig]
<!--NeedCopy-->
```

Standardmäßig ist es auf YES eingestellt und löscht die Konfigurationen basierend auf der Ebene.

Wenn —auf NO gesetzt`RBAconfig` ist, wird die RBA-bezogene Konfiguration beibehalten. Folgendes ist enthalten:

- /bind Systembenutzer /group hinzufügen
- Bindesystem global
- TACACS-bezogene Befehle (TACACS-Aktion/Richtlinie hinzufügen)
- cmd-Richtlinie hinzufügen

## Multifaktor-Authentifizierung konfigurieren

March 27, 2024

Sie können zwei Arten der Multifaktor-Authentifizierung in Citrix Gateway konfigurieren:

- Kaskadierende Authentifizierung, die die Authentifizierungspriorität
- Zwei-Faktor-Authentifizierung, bei der sich Benutzer mithilfe von zwei Authentifizierungsarten anmelden müssen

Wenn Sie über mehrere Authentifizierungsserver verfügen, können Sie die Priorität Ihrer Authentifizierungsrichtlinien festlegen. Die von Ihnen festgelegten Prioritätsstufen bestimmen die Reihenfolge, in der der Authentifizierungsserver die Anmeldeinformationen der Benutzer validiert.

Eine Richtlinie mit einer niedrigeren Prioritätszahl hat Vorrang vor einer Richtlinie mit einer höheren Zahl.

Sie können Benutzer bei zwei verschiedenen Authentifizierungsservern authentifizieren lassen. Sie können beispielsweise eine LDAP-Authentifizierungsrichtlinie und eine RSA-Authentifizierungsrichtlinie konfigurieren. Wenn sich Benutzer anmelden, authentifizieren sie sich zuerst mit ihrem Benutzernamen und Kennwort. Dann authentifizieren sie sich mit einer persönlichen Identifikationsnummer (PIN) und dem Code aus dem RSA-Token.

## Kaskadierende Authentifizierung konfigurieren

March 27, 2024

Mit der Authentifizierung können Sie mithilfe der Richtlinienpriorisierung eine Kaskade mehrerer Authentifizierungsserver erstellen. Wenn Sie eine Kaskade konfigurieren, durchquert das System jeden Authentifizierungsserver, wie in den kaskadierten Richtlinien definiert, um die Anmeldeinformationen eines Benutzers zu überprüfen. Priorisierte Authentifizierungsrichtlinien werden in aufsteigender Reihenfolge kaskadiert und können Prioritätswerte im Bereich von 1—9999 aufweisen. Sie definieren diese Prioritäten, wenn Sie Ihre Richtlinien entweder auf globaler oder auf virtueller Serverebene binden.

Während der Authentifizierung, wenn sich ein Benutzer anmeldet, wird zuerst der virtuelle Server überprüft und dann werden globale Authentifizierungsrichtlinien überprüft. Wenn ein Benutzer sowohl auf dem virtuellen Server als auch global zu einer Authentifizierungsrichtlinie gehört, wird zuerst die Richtlinie vom virtuellen Server und dann die globale Authentifizierungsrichtlinie angewendet. Wenn Sie möchten, dass Benutzer die global gebundene Authentifizierungsrichtlinie erhalten, ändern Sie die Priorität der Richtlinie. Wenn eine globale Authentifizierungsrichtlinie die Prioritätsnummer eins hat und eine an einen virtuellen Server gebundene Authentifizierungsrichtlinie eine Priorität Nummer zwei hat, hat die globale Authentifizierungsrichtlinie Vorrang. Sie können beispielsweise drei Authentifizierungsrichtlinien an den virtuellen Server gebunden haben und die Priorität jeder Richtlinie festlegen.

Wenn es einem Benutzer nicht gelingt, sich gegen eine Richtlinie in der primären Kaskade zu authentifizieren, oder wenn es diesem Benutzer gelingt, sich gegen eine Richtlinie in der Primärkaskade zu authentifizieren, sich aber nicht gegen eine Richtlinie in der sekundären Kaskade authentifiziert, stoppt der Authentifizierungsprozess und der Benutzer wird auf eine Fehlerseite umgeleitet.

Hinweis: Citrix empfiehlt, dass Sie beim Binden mehrerer Richtlinien an einen virtuellen Server oder global eindeutige Prioritäten für alle Authentifizierungsrichtlinien definieren.

### So legen Sie die Priorität für globale Authentifizierungsrichtlinien fest

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
2. Wählen Sie die global gebundene Richtlinie aus, und klicken Sie dann **unter Aktion**auf **Globale Bindungen**.
3. Geben Sie im Dialogfeld **Globale Authentication Bind/Unbind Authentication Polices** unter Priorität die Nummer ein, und klicken Sie dann auf **OK**.

### So ändern Sie die Priorität für eine an einen virtuellen Server gebundene Authentifizierungsrichtlinie

Sie können auch eine Authentifizierungsrichtlinie ändern, die an einen virtuellen Server gebunden ist.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway**, und klicken Sie dann auf **Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen Server aus, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie auf die Registerkarte **Authentifizierung** und dann entweder auf **Primär** oder **Sekundär**.
4. Geben Sie neben der Authentifizierungsrichtlinie unter **Priorität**die Nummer ein, und klicken Sie dann auf **OK**.

## Zwei-Faktor-Authentifizierung konfigurieren

March 27, 2024

Citrix Gateway unterstützt die Zwei-Faktor-Authentifizierung. Normalerweise stoppt Citrix Gateway bei der Authentifizierung von Benutzern den Authentifizierungsprozess, sobald ein Benutzer über eine der konfigurierten Authentifizierungsmethoden erfolgreich authentifiziert wird. In bestimmten Fällen müssen Sie möglicherweise einen Benutzer bei einem Server authentifizieren, aber Gruppen von einem anderen Server extrahieren. Wenn Ihr Netzwerk beispielsweise Benutzer gegenüber einem RADIUS-Server authentifiziert, Sie aber auch die RSA SecurID-Token-Authentifizierung verwenden und Benutzergruppen auf diesem Server gespeichert sind, müssen Sie möglicherweise Benutzer bei diesem Server authentifizieren, damit Sie die Gruppen extrahieren können.

Wenn Benutzer mithilfe von zwei Authentifizierungstypen authentifiziert werden und einer dieser Typen die Clientzertifikatauthentifizierung ist, können Sie die Zertifikatauthentifizierungsrichtlinie als zweite Authentifizierungsmethode konfigurieren. Beispielsweise verwenden Sie LDAP als primären

Authentifizierungstyp und das Clientzertifikat als sekundäre Authentifizierung. Wenn sich Benutzer mit ihrem Benutzernamen und Kennwort anmelden, haben sie Zugriff auf Netzwerkressourcen.

Bei der Konfiguration der Zwei-Faktor-Authentifizierung wählen Sie aus, ob der Authentifizierungstyp der primäre oder sekundäre Typ ist.

### Konfigurieren der Zwei-Faktor-Authentifizierung

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte KonfigurationCitrix Gateway > Richtlinien > Authentifizierung.
2. Klicken Sie auf der Registerkarte Richtlinien auf Globale Bindungen.
3. Klicken Sie im Dialogfeld Authentifizierungsrichtlinien an Global binden/aufheben auf Primär.
4. Klicken Sie auf Richtlinie einfügen.
5. Wählen Sie unter Richtlinienname die Authentifizierungsrichtlinie aus.
6. Klicken Sie auf Sekundär, wiederholen Sie die Schritte 4 und 5 und klicken Sie dann auf OK.

## Auswählen des Authentifizierungstyps für Single Sign-On

March 27, 2024

Wenn Sie Single Sign-On und Zwei-Faktor-Authentifizierung auf Citrix Gateway konfiguriert haben, können Sie auswählen, welches Kennwort für das einmalige Anmelden verwendet werden soll. Beispielsweise haben Sie LDAP als primären Authentifizierungstyp konfiguriert und RADIUS als sekundärer Authentifizierungstyp konfiguriert. Wenn Benutzer auf Ressourcen zugreifen, die einmaliges Anmelden erfordern, werden der Benutzername und das primäre Kennwort standardmäßig gesendet. Sie legen fest, welches Kennwort für die einmalige Anmeldung bei Webanwendungen innerhalb eines Sitzungsprofils verwendet werden muss.

### So konfigurieren Sie die Authentifizierung für einmaliges Anmelden

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien > Sitzung**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Profile**, und führen Sie dann einen der folgenden Schritte aus:
   - Um ein neues Profil zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um ein vorhandenes Profil zu ändern, klicken Sie auf **Öffnen**.
3. Klicken Sie auf der Registerkarte Client Experience neben Credential Index auf **Override Global**und wählen Sie entweder **Primär** oder **Sekundär**aus.

4. Wenn es sich um ein neues Profil handelt, klicken Sie auf **Erstellen**und dann auf **Schließen**.
5. Wenn Sie ein vorhandenes Profil ändern, klicken Sie auf **OK**.

## Clientzertifikate und LDAP-Zwei-Faktor-Authentifizierung konfigurieren

March 27, 2024

Sie können ein sicheres Clientzertifikat mit LDAP-Authentifizierung und -Autorisierung verwenden, z. B. die Verwendung der Smartcard-Authentifizierung mit LDAP. Der Benutzer meldet sich an und dann wird der Benutzername aus dem Clientzertifikat extrahiert. Das Clientzertifikat ist die primäre Form der Authentifizierung und LDAP ist das sekundäre Formular. Die Clientzertifikatauthentifizierung muss Vorrang vor der LDAP-Authentifizierungsrichtlinie haben. Wenn Sie die Priorität der Richtlinien festlegen, weisen Sie der Clientzertifikatauthentifizierungsrichtlinie eine niedrigere Zahl zu als die Nummer, die Sie der LDAP-Authentifizierungsrichtlinie zuweisen.

Um ein Clientzertifikat verwenden zu können, benötigen Sie eine Unternehmenszertifizierungsstelle (CA), wie z. B. die Zertifikatsdienste in Windows Server 2008, die auf demselben Computer ausgeführt wird, auf dem Active Directory ausgeführt wird. Sie können die CA verwenden, um ein Clientzertifikat zu erstellen.

Um ein Clientzertifikat mit LDAP-Authentifizierung und -Autorisierung verwenden zu können, muss es sich um ein sicheres Zertifikat handeln, das Secure Sockets Layer (SSL) verwendet. Um sichere Clientzertifikate für LDAP zu verwenden, installieren Sie das Clientzertifikat auf dem Benutzergerät und installieren Sie ein entsprechendes Stammzertifikat auf Citrix Gateway.

Gehen Sie folgendermaßen vor, bevor Sie ein Clientzertifikat konfigurieren:

- Erstellen Sie einen virtuellen Server.
- Erstellen Sie eine LDAP-Authentifizierungsrichtlinie für den LDAP-Server.
- Setzen Sie den Ausdruck für die LDAP-Richtlinie auf den Wert True.

### So konfigurieren Sie die Clientzertifikatauthentifizierung mit LDAP

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien\ > Authentifizierung**.
2. Klicken Sie im Navigationsbereich unter Authentifizierung auf Cert.
3. Klicken Sie im Detailbereich auf “Hinzufügen”.
4. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
5. Wählen Sie unter Authentifizierungstyp Cert aus.

6. Klicken Sie neben Server auf Neu.
7. Geben Sie unter Name einen Namen für den Server ein, und klicken Sie dann auf Erstellen.
8. Geben Sie im Dialogfeld Authentifizierungsserver erstellen in das Feld Name den Namen des Servers ein.
9. Wählen Sie neben Two Factor ON aus.
10. Wählen Sie im Feld Benutzername Betreff:CN aus und klicken Sie dann auf Erstellen.
11. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie erstellen neben Benannte Ausdrücke den Wert True aus, klicken Sie auf Ausdruck hinzufügen, klicken Sie auf Erstellen und dann auf Schließen.

Binden Sie die Richtlinie nach dem Erstellen der Zertifikatauthentifizierungsrichtlinie an den virtuellen Server. Binden Sie nach dem Binden der Zertifikatauthentifizierungsrichtlinie die LDAP-Authentifizierungsrichtlinie an den virtuellen Server.

**Wichtig**: Sie müssen die Richtlinie zur Zertifikatauthentifizierung an den virtuellen Server binden, bevor Sie die LDAP-Authentifizierungsrichtlinie an den virtuellen Server binden.

### To install a root certificate on Citrix Gateway

Nachdem Sie die Zertifikatauthentifizierungsrichtlinie erstellt haben, laden Sie ein Stammzertifikat von Ihrer CA im Base64-Format herunter, installieren es und speichern es auf Ihrem Computer. Sie können dann das Stammzertifikat auf Citrix Gateway hochladen.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich SSL, und klicken Sie dann auf Zertifikate.
2. Klicken Sie im Detailbereich auf Installieren.
3. Geben Sie unter Zertifikat - Schlüsselpaarname einen Namen für das Zertifikat ein.
4. Klicken Sie unter Certificate File Name auf Durchsuchen und wählen Sie in der Liste entweder Appliance oder Local aus.
5. Navigieren Sie zum Stammzertifikat, klicken Sie auf Öffnen und dann auf Installieren.

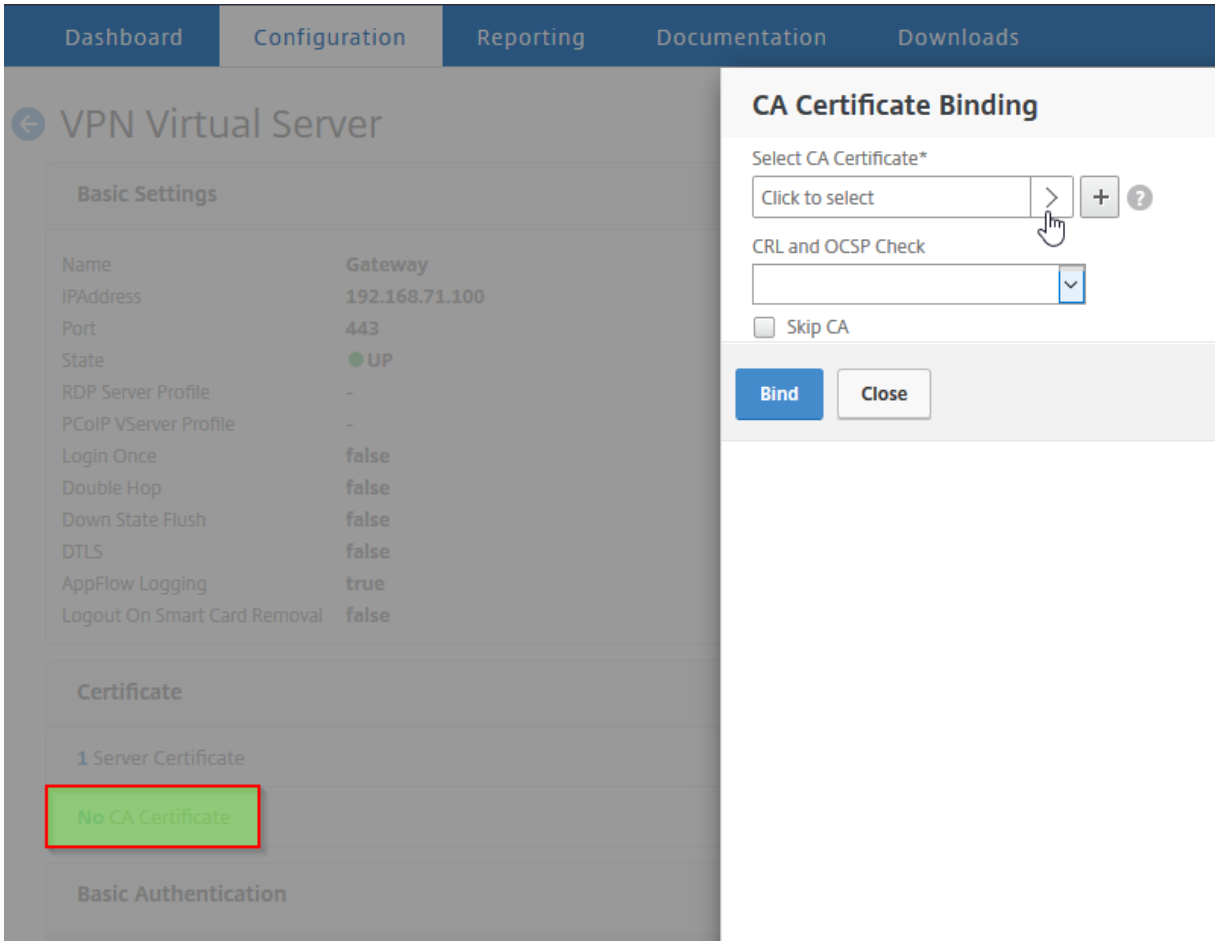
### To add a root certificate to a virtual server

Fügen Sie nach der Installation des Stammzertifikats auf Citrix Gateway das Zertifikat zum Zertifikatspeicher des virtuellen Servers hinzu.

**Wichtig**: Wenn Sie das Stammzertifikat für die Smartcard-Authentifizierung zum virtuellen Server hinzufügen, müssen Sie das Zertifikat aus dem Listenfeld
**CA-Zertifikat auswählen auswählen**, wie in der folgenden Abbildung dargestellt.

Abbildung 1. Hinzufügen eines Stammzertifikats als CA




1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf Virtuelle Server.
2. Wählen Sie im Detailbereich einen virtuellen Server aus und klicken Sie dann auf Öffnen.
3. Wählen Sie auf der Registerkarte Zertifikate unter Verfügbar das Zertifikat aus, neben Hinzufügen, klicken Sie in der Liste auf CA, und klicken Sie dann auf OK.
4. Wiederholen Sie Schritt 2.
5. Klicken Sie auf der Registerkarte Zertifikate auf SSL-Parameter.
6. Wählen Sie unter Andere die Option Clientauthentifizierung aus.
7. Wählen Sie unter Andere neben Clientzertifikat die Option Optional aus, und klicken Sie dann zweimal auf OK.
8. Testen Sie nach dem Konfigurieren des Clientzertifikats die Authentifizierung, indem Sie sich mit dem Citrix Gateway Plug-in bei Citrix Gateway anmelden. Wenn Sie mehr als ein Zertifikat installiert haben, werden Sie aufgefordert, das richtige Zertifikat auszuwählen. Nachdem Sie das Zertifikat ausgewählt haben, wird der Anmeldebildschirm mit dem Benutzernamen angezeigt,

der mit den aus dem Zertifikat erhaltenen Informationen gefüllt ist. Geben Sie das Kennwort ein und klicken Sie dann auf Anmelden.

Wenn Sie im Feld Benutzername auf dem Anmeldebildschirm nicht den richtigen Benutzernamen sehen, überprüfen Sie die Benutzerkonten und Gruppen in Ihrem LDAP-Verzeichnis. Die Gruppen, die auf Citrix Gateway definiert sind, müssen mit denen im LDAP-Verzeichnis identisch sein. Konfigurieren Sie in Active Directory Gruppen auf Domänen-Root-Ebene. Wenn Sie Active Directory-Gruppen erstellen, die sich nicht auf der Domänen-Root-Ebene befinden, kann ein falsches Lesen des Clientzertifikats zur Folge haben.

Wenn sich Benutzer und Gruppen nicht auf Domänen-Root-Ebene befinden, zeigt die Citrix Gateway-Anmeldeseite den in Active Directory konfigurierten Benutzernamen an. In Active Directory haben Sie beispielsweise einen Ordner mit dem Namen Benutzer und das Zertifikat lautet CN=Users. Auf der Anmeldeseite, in Benutzername, wird das Wort Benutzer angezeigt.

Wenn Sie Ihre Gruppen- und Benutzerkonten nicht auf die Stammdomänenebene verschieben möchten, lassen Sie bei der Konfiguration des Zertifikatauthentifizierungsservers auf Citrix Gateway das Feld Benutzernamen und das Feld für den Gruppennamen leer.

## Native OTP-Unterstützung für die Authentifizierung

March 27, 2024

Citrix Gateway unterstützt Einmalkennwörter (OTPs), ohne einen Server eines Drittanbieters verwenden zu müssen. Einmal-Kennwort ist eine hochsichere Option für die Authentifizierung bei sicheren Servern, da die generierte Nummer oder der Code zufällig ist. Zuvor boten spezialisierte Unternehmen wie RSA mit bestimmten Geräten, die Zufallszahlen generieren, die OTPs an. Dieses System muss in ständiger Kommunikation mit dem Client stehen, um eine vom Server erwartete Zahl zu generieren.

Diese Funktion reduziert nicht nur die Kapital- und Betriebskosten, sondern verbessert auch die Kontrolle des Administrators, indem die gesamte Konfiguration auf der Citrix ADC Appliance beibehalten wird.

> **Hinweis:**
>
> Da Server von Drittanbietern nicht mehr benötigt werden, muss der Citrix ADC Administrator eine Schnittstelle zum Verwalten und Überprüfen von Benutzergeräten konfigurieren.

Der Benutzer muss bei einem virtuellen Citrix Gateway-Server registriert sein, um die OTP-Lösung verwenden zu können. Die Registrierung ist nur einmal pro Gerät erforderlich und kann auf bestimmte Umgebungen beschränkt werden. Die Konfiguration und Validierung eines registrierten Benutzers ähnelt der Konfiguration einer zusätzlichen Authentifizierungsrichtlinie.

### Vorteile der nativen OTP-Unterstützung

- Senkt die Betriebskosten, da neben dem Active Directory keine zusätzliche Infrastruktur auf einem Authentifizierungsserver erforderlich ist.
- Konsolidiert die Konfiguration nur auf der Citrix ADC Appliance und bietet so Administratoren eine hervorragende Kontrolle.
- Beseitigt die Abhängigkeit des Clients von einem zusätzlichen Authentifizierungsserver zur Generierung einer von den Clients erwarteten Zahl.

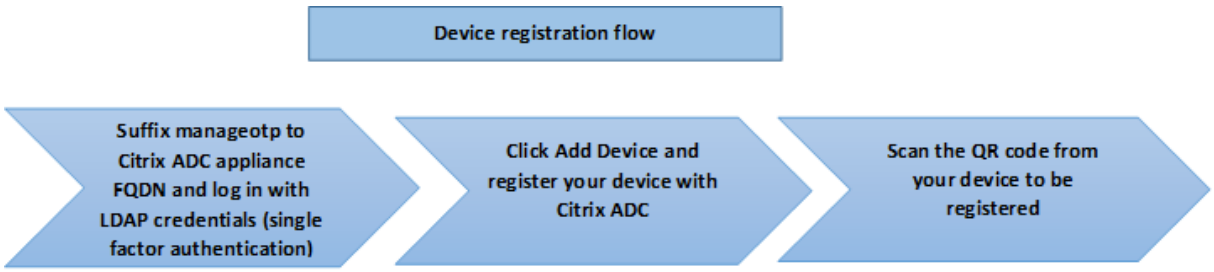
### Nativer OTP-Workflow

Bei der nativen OTP-Lösung handelt es sich um einen zweifachen Prozess, und der Arbeitsablauf wird wie folgt klassifiziert:

- Geräteregistrierung
- Anmeldung für Endbenutzer

**Wichtig:** Sie können den Registrierungsprozess überspringen, wenn Sie Lösungen von Drittanbietern verwenden oder andere Geräte außer der Citrix ADC-Appliance verwalten. Die letzte Zeichenfolge, die Sie hinzufügen, muss das von Citrix ADC angegebene Format haben.

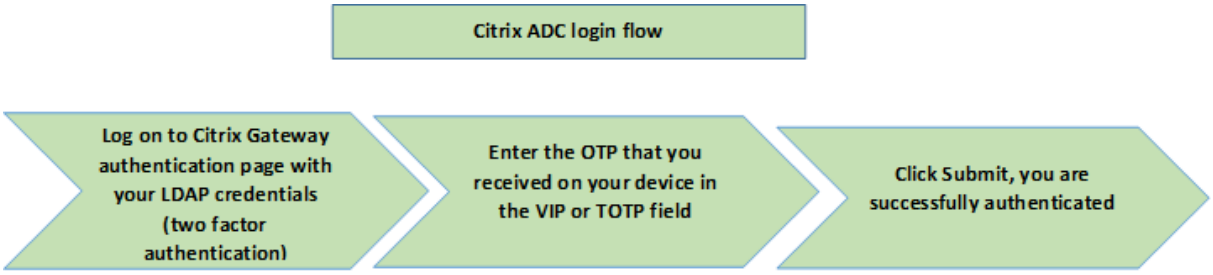
Die folgende Abbildung zeigt den Ablauf der Geräteregistrierung zur Registrierung eines neuen Geräts für den Empfang von OTP.




> **Hinweis:**
>
> Die Geräteregistrierung kann anhand einer Reihe von Faktoren erfolgen. Der Einzelfaktor (wie in der vorherigen Abbildung angegeben) wird als Beispiel verwendet, um den Prozess der Geräteregistrierung zu erläutern.

Die folgende Abbildung zeigt die Überprüfung von OTP durch das registrierte Gerät.




### Voraussetzungen

Um die native OTP-Funktion zu verwenden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Die Citrix ADC Feature Release-Version ist 12.0 Build 51.24 und höher.
- Die Advanced- oder Premium Edition-Lizenz ist auf Citrix Gateway installiert.
- Citrix Gateway ist mit Management-IP konfiguriert und auf die Verwaltungskonsole kann sowohl über einen Browser als auch über eine Befehlszeile zugegriffen werden.
- Citrix ADC ist mit einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver zur Authentifizierung von Benutzern konfiguriert.
- Die Citrix ADC Appliance ist mit Unified Gateway konfiguriert und das Authentifizierungs-, Autorisierungs- und Überwachungsprofil ist dem virtuellen Gateway-Server zugewiesen.
- Die native OTP-Lösung ist auf den nFactor-Authentifizierungsfluss beschränkt. Für die Konfiguration der Lösung sind erweiterte Richtlinien erforderlich. Weitere Einzelheiten finden Sie im Artikel CTX222713.

Stellen Sie außerdem Folgendes für Active Directory sicher:

- Eine minimale Attributlänge von 256 Zeichen.
- Der Attributtyp muss ‘DirectoryString’sein, z. B. UserParameters. Diese Attribute können Zeichenkettenwerte enthalten.
- Der Typ der Attributzeichenfolge muss Unicode sein, wenn der Gerätename aus nichtenglischen Zeichen besteht.
- Der Citrix ADC LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.
- Die Citrix ADC Appliance und der Client-Computer müssen mit einem gemeinsamen Network Time Server synchronisiert werden.

### Konfigurieren Sie Native OTP mit der GUI

Die native OTP-Registrierung ist nicht nur eine Ein-Faktor-Authentifizierung. Die folgenden Abschnitte helfen Ihnen bei der Konfiguration der Einzel- und Zwei-Faktor-Authentifizierung.

**Anmeldeschema für den ersten Faktor erstellen**

1. Navigieren Sie zu **Sicherheit AAA > Anwendungsverkehr > Anmeldeschema**.
2. Gehen Sie zu **Profile** und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Authentifizierungs-Login-Schema erstellen** unter dem Feld **Name***lschema_single_auth_manage_otp* ein und klicken Sie neben **noschema** auf **Bearbeiten**.
4. Klicken Sie auf den Ordner **LoginSchema**.
5. Scrolle nach unten, um **SingleAuth.xml** auszuwählen und klicke auf **Auswählen**
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Richtlinien** und dann auf **Hinzufügen**.
8. Geben Sie auf dem Bildschirm **Create Authentication Login-Schema Policy**die folgenden Werte ein.

   **Name:** `lpol_single_auth_manage_otp_by_url`
   **Profil:** wähle l`pol_single_auth_manage_otp_by_url` aus der Liste aus.
   **Regel:** `HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("`manageotp`")`

**Konfiguration des virtuellen Servers für Authentifizierung, Autorisierung und Überwachung**

1. Navigieren Sie zu **Sicherheit > AAA —Anwendungsverkehr > Virtuelle Authentifizierungsserver**. Klicken Sie hier, um den vorhandenen virtuellen Server zu bearbeiten.
2. Klicken Sie auf das **+**-Symbol neben **Anmeldeschemas** unter **Erweiterte Einstellungen** im rechten Fensterbereich.
3. Wählen Sie **Kein Anmeldeschema aus.**
4. Klicken Sie auf den Pfeil und wählen Sie die Richtlinie **lpol_single_auth_manage_otp_by_url** aus.
5. Wählen Sie die Richtlinie **lpol_single_auth_manage_otp_by_url** aus und klicken Sie auf **Auswählen**.
6. Klicken Sie auf **Bind**.
7. Scrollen Sie nach oben und wählen Sie unter **Erweiterte Authentifizierungsrichtlinie** die Option **1 Authentifizierungsrichtlinie** aus.
8. Klicken Sie mit der rechten Maustaste auf die **nFactor-Richtlinie**, und wählen Sie **Bindung bearbeiten** aus.

9. Klicken Sie auf das **+-Symbol** unter **Nächsten Faktor auswählen,** erstellen Sie einen Nächsten Faktor und klicken Sie auf **Binden**.
10. Geben Sie auf dem Bildschirm **Authentifizierung erstellen** `PolicyLabel` Folgendes ein und klicken Sie auf **Weiter**:

    **Vorname**: manage_otp_flow_label

    **Anmeldeschema**: Lschema_Int
11. Klicken Sie auf dem Bildschirm **Authentication PolicyLabel** auf das Symbol **+**, um eine Richtlinie zu erstellen.
12. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinie erstellen** Folgendes ein:

    **Vorname**: auth_pol_ldap_otp_action
13. Wählen Sie mithilfe der Liste Aktionstyp den **Aktionstyp** aus.
14. Klicken Sie im Feld **Aktion** auf das **+-Symbol**, um eine Aktion zu erstellen.
15. Aktivieren Sie auf der Seite **Authentifizierung LDAP-Server erstellen** das Optionsfeld **Server-IP**, deaktivieren Sie das Kontrollkästchen neben **Authentifizierung**, geben Sie die folgenden Werte ein und wählen Sie **Verbindung testen**aus.

    **Vorname**: ldap_otp_action

    **IP-Adresse**: 192.168.10.11

    **Base DN**: DC = Training, DC = Labor

    **Verwaltungsrätin**: Administrator@training.lab

    **Passwort**: xxxxx
16. Scrollen Sie nach unten zum Abschnitt **Andere Einstellungen**. Verwenden Sie das Dropdown-menü, um die folgenden Optionen auszuwählen.
    **Server-Anmeldename Attribut** als **Neu** und geben Sie **userprincipalname ein**.
17. Verwenden Sie das Dropdownmenü, um **SSO-Namensattribut** als **Neu** auszuwählen und **user-principalname**einzugeben.
18. Geben Sie “UserParameters”in das Feld **OTP Secret** ein und klicken Sie auf **Mehr**.
19. Geben Sie die folgenden Attribute ein.

    **Attribute 1** = mail
    **Attribute 2** = objectGUID
    **Attribute 3** = immutableID
20. Klicken Sie auf **OK**.
21. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** den Ausdruck auf **true** fest und klicken Sie auf **Erstellen**.

22. Klicken Sie auf der Seite **Create Authentication Policylabel** auf **Binden**und dann auf **Fertig.**
23. Klicken Sie auf der Seite **Policy Binding** auf **Bind**.
24. Klicken Sie auf der Seite **Authentifizierungsrichtlinie** auf **Schließen**, und klicken Sie auf **Fertig**.

> **Hinweis:**
>
> Der virtuelle Authentifizierungsserver muss an das RFWebUI-Portaldesign gebunden sein. Binden Sie ein Serverzertifikat an den Server. Die Server-IP '1.2.3.5'muss einen entsprechenden FQDN haben, nämlich otpauth.server.com, für die spätere Verwendung.

#### Anmeldeschema für OTP mit dem zweiten Faktor erstellen

1. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Virtuelle Server**. Wählen Sie den virtuellen Server aus, der bearbeitet werden soll.
2. Scrollen Sie nach unten und wählen Sie **1 Login**
3. Klicken Sie auf **Add binding**.
4. Klicken Sie im Abschnitt **Policy Binding** auf das Symbol **+**, um eine Richtlinie hinzuzufügen.
5. Geben Sie auf der Seite **Create Authentication Login Schema Policy** Name as OTP ein und klicken Sie auf das Symbol **+**, um ein Profil zu erstellen.
6. Geben Sie auf der Seite **Create Authentication Login Schema** Name as OTP ein, und klicken Sie auf das Symbol neben **noschema**.
7. Klicken Sie auf den Ordner **LoginSchema**, wählen Sie **DualAuthManageOTP.xml** aus, und klicken Sie dann auf **Auswählen**.
8. Klicken Sie auf **Erstellen**.
9. Geben Sie im Abschnitt **Regel** die Option **True** ein. Klicken Sie auf **Erstellen**.
10. Klicken Sie auf **Bind**.
11. Beachten Sie die beiden Authentifizierungsfaktoren. Klicken Sie auf **Schließen**, und klicken Sie auf **Fertig**.

#### Content Switching-Richtlinie für die Verwaltung von OTP konfigurieren

Die folgenden Konfigurationen sind erforderlich, wenn Sie Unified Gateway verwenden.

1. Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**. Wählen Sie die Richtlinie für den Content Switching aus, klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten**.
2. Bearbeiten Sie den Ausdruck, um die folgende OR-Anweisung auszuwerten, und klicken Sie auf **OK**:

is_vpn_url

### Konfigurieren Sie Native OTP mit der CLI

Sie benötigen die folgenden Informationen, um die OTP-Geräteverwaltungsseite zu konfigurieren:

- Dem virtuellen Authentifizierungsserver zugewiesene IP
- FQDN, der der zugewiesenen IP entspricht
- Serverzertifikat für den virtuellen Authentifizierungsserver

> **Hinweis:**
>
> Native OTP ist nur eine webbasierte Lösung.

#### So konfigurieren Sie die OTP-Geräteregistrierungs- und Verwaltungsseite

Virtuellen Authentifizierungsserver erstellen

```
add authentication vserver authvs SSL 1.2.3.5 443
bind authentication vserver authvs -portaltheme RFWebUI
bind ssl vserver authvs -certkeyname otpauthcert
<!--NeedCopy-->
```

> **Hinweis:**
>
> Der virtuelle Authentifizierungsserver muss an das RFWebUI-Portalthema gebunden sein. Binden Sie ein Serverzertifikat an den Server. Die Server-IP ‘1.2.3.5’muss einen entsprechenden FQDN haben, nämlich otpauth.server.com, für die spätere Verwendung.

#### So erstellen Sie eine LDAP-Anmeldeaktion

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -  serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
<!--NeedCopy-->
```

**Beispiel**:

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname
<!--NeedCopy-->
```

#### So fügen Sie eine Authentifizierungsrichtlinie für die LDAP-Anmeldung hinzu

```
1 add authentication Policy auth_pol_ldap_logon -rule true -action
     ldap_logon_action
2 <!--NeedCopy-->
```

#### Um die Benutzeroberfläche über LoginSchema zu präsentieren

Benutzernamenfeld und Kennwortfeld für Benutzer bei der Anmeldung anzeigen

```
1 add authentication loginSchema lschema_single_auth_manage_otp -
     authenticationSchema "/nsconfig/loginschema/LoginSchema/
     SingleAuthManageOTP.xml"
2 <!--NeedCopy-->
```

### Geräteregistrierungs- und Verwaltungsseite anzeigen

Citrix empfiehlt zwei Möglichkeiten, den Bildschirm für die Geräteregistrierung und -verwaltung anzuzeigen: URL oder Hostname.

- **Verwenden von URL**

  Wenn die URL '/manageotp'enthält

  ```
  - add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_ur
    -rule "http.req.cookie.value("NSC_TASS").contains("manageotp
  ")"-action lschema_single_auth_manage_otp
  - bind authentication vserver authvs -policy lpol_single_auth_manage_otp
    -priority 10 -gotoPriorityExpression END
  ```

- **Verwenden des Hostnamens**

  Wenn der Hostname 'alt.server.com'ist

  ```
  - add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_ho
    -rule "http.req.header("host").eq("alt.server.com")"-action
  lschema_single_auth_manage_otp
  - bind authentication vserver authvs -policy lpol_single_auth_manage_otp
    -priority 20 -gotoPriorityExpression END
  ```

#### So konfigurieren Sie die Benutzeranmeldeseite mit der CLI

Sie benötigen die folgenden Informationen, um die Benutzeranmeldeseite zu konfigurieren:

- IP für einen virtuellen Lastausgleichsserver
- Entsprechender FQDN für den virtuellen Lastausgleichsserver
- Serverzertifikat für den virtuellen Lastausgleichsserver

```
bind ssl vserver lbvs_https -certkeyname lbvs_server_cert
<!--NeedCopy-->
```

Der Back-End-Dienst im Load Balancing wird wie folgt dargestellt:

```
add service iis_backendsso_server_com 1.2.3.210 HTTP 80
bind lb vserver lbvs_https iis_backendsso_server_com
<!--NeedCopy-->
```

**So erstellen Sie eine Aktion zur OTP-Passcode-Validierung**

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
   -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
   ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
   authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>
<!--NeedCopy-->
```

**Beispiel:**

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
   serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
   administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
   ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
   userParameters
<!--NeedCopy-->
```

> **Wichtig:**
>
> Der Unterschied zwischen der LDAP-Anmeldung und der OTP-Aktion besteht darin, dass die Authentifizierung deaktiviert und ein neuer Parameter `OTPSecret` eingeführt werden muss. Verwenden Sie nicht den AD-Attributwert.

**So fügen Sie eine Authentifizierungsrichtlinie für die OTP-Passcode-Validierung hinzu**

```
add authentication Policy auth_pol_otp_validation -rule true -action
   ldap_otp_action
<!--NeedCopy-->
```

**Um die Zwei-Faktor-Authentifizierung über LoginSchema zu präsentieren** Fügen Sie die Benutzeroberfläche für die Zwei-Faktor-Authentifizierung hinzu.

```
add authentication loginSchema lscheme_dual_factor -
   authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml
   "
```

```
2 add authentication loginSchemaPolicy lpol_dual_factor -rule true -
    action lscheme_dual_factor
3 <!--NeedCopy-->
```

**Um einen Passcode-Validierungsfaktor über das Policy-Label zu erstellen** Erstellen Sie ein Richtlinienlabel zum Verwalten von OTP-Flows für den nächsten Faktor (der erste Faktor ist die LDAP-Anmeldung)

```
1 add authentication loginSchema lschema_noschema -authenticationSchema
    noschema
2 add authentication policylabel manage_otp_flow_label -loginSchema
    lschema_noschema
3 <!--NeedCopy-->
```

**Um die OTP-Richtlinie an das Richtlinienlabel zu binden**

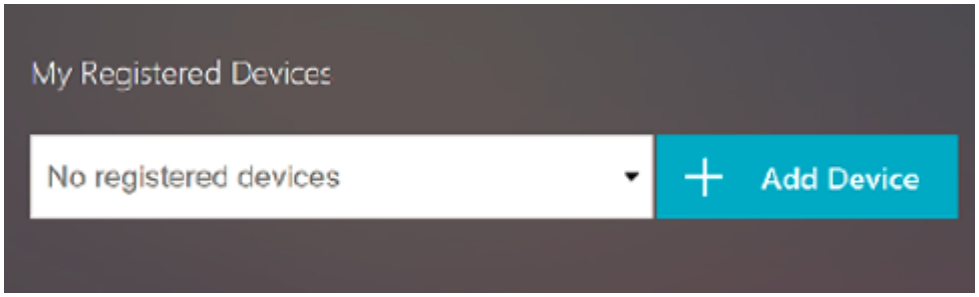
```
1 bind authentication policylabel manage_otp_flow_label -policyName
    auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
2 <!--NeedCopy-->
```

**Um den UI-Flow zu binden** Binden Sie die LDAP-Anmeldung gefolgt von der OTP-Validierung an den virtuellen Authentifizierungsserver.

```
1 bind authentication vserver authvs -policy auth_pol_ldap_logon -
    priority 10 -nextFactor  manage_otp_flow_label -
    gotoPriorityExpression NEXT
2 bind authentication vserver authvs -policy lpol_dual_factor -priority
    30 -gotoPriorityExpression END
3 <!--NeedCopy-->
```

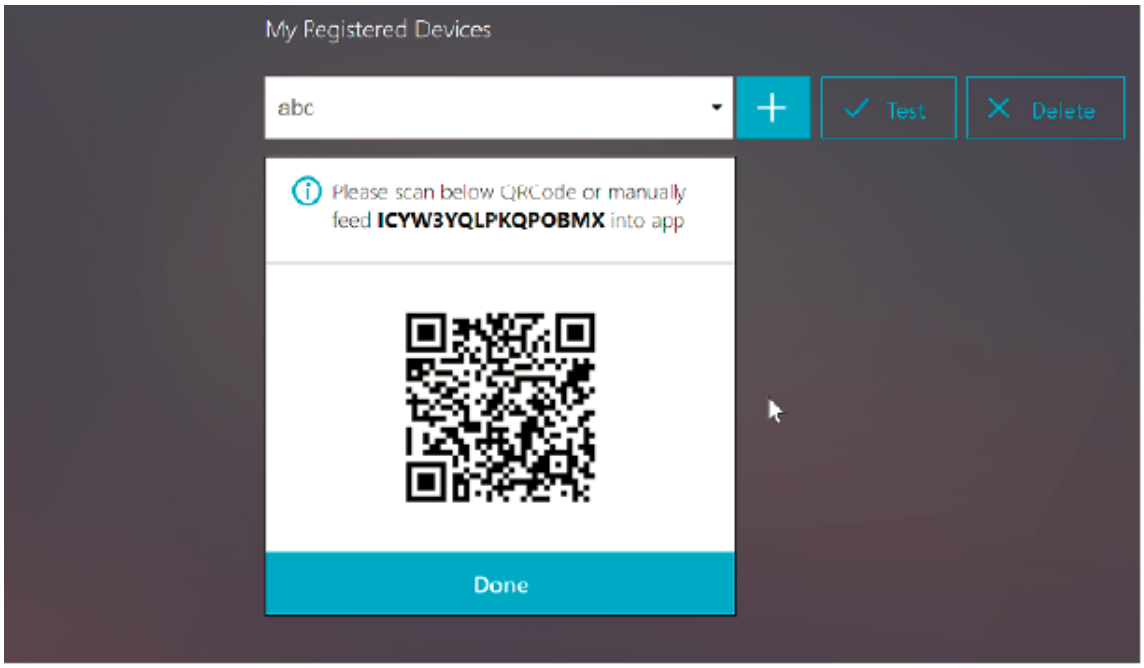
### Registrieren Sie Ihr Gerät bei Citrix ADC

1. Navigieren Sie mit dem Suffix /manageotp zu Ihrem Citrix ADC FQDN (erste öffentliche IP). Zum Beispiel Login bei https://otpauth.server.com/manageotp mit Benutzeranmeldeinformationen.
2. Klicken Sie auf das **+-Symbol**, um ein Gerät hinzuzufügen.



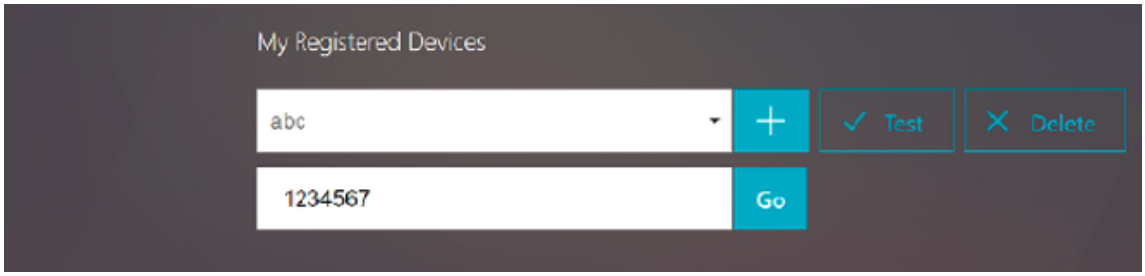

 

3. Geben Sie einen Gerätenamen ein und drücken Sie **Los**. Auf dem Bildschirm erscheint ein Barcode.
4. Klicken Sie auf **Setup beginnen** und dann auf **Barcode scannen**.
5. Bewegen Sie die Gerätekamera über den QR-Code. Sie können den Code optional eingeben.




> **Hinweis:**
>
> Der angezeigte QR-Code ist 3 Minuten gültig.

6. Nach erfolgreichem Scan wird Ihnen ein sechsstelliger zeitkritischer Code angezeigt, mit dem Sie sich anmelden können.

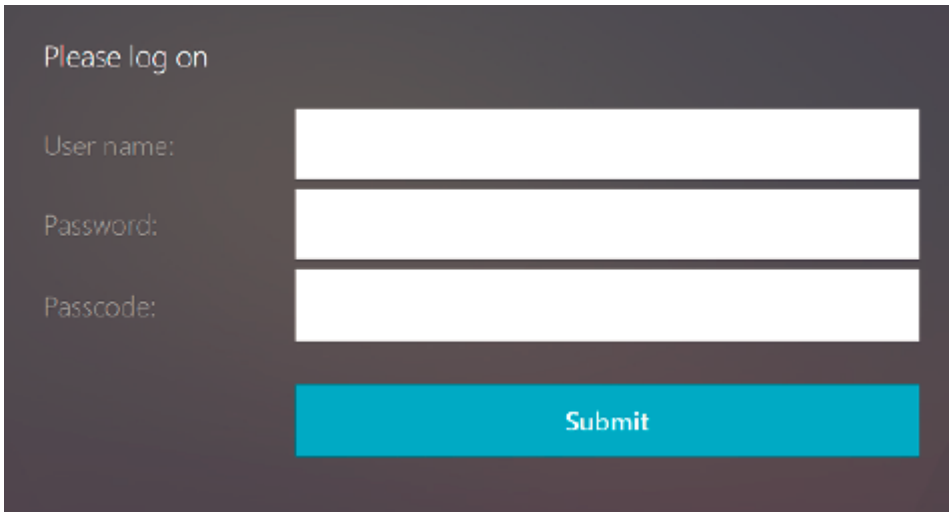



7. Klicken Sie zum Testen auf dem QR-Bildschirm auf **Fertig** und dann auf das grüne Häkchen rechts.
8. Wählen Sie Ihr Gerät aus dem Dropdownmenü aus, geben Sie den Code von Google Authenticator ein (muss blau und nicht rot sein) und klicken Sie auf **Los**.
9. Stellen Sie sicher, dass Sie sich über das Drop-down-Menü in der oberen rechten Ecke der Seite abmelden.

### Melden Sie sich mit dem OTP bei Citrix ADC an

1. Navigieren Sie zu Ihrer ersten öffentlich zugänglichen URL und geben Sie Ihr OTP über Google Authenticator ein, um sich anzumelden.
2. Authentifizieren Sie sich auf der Citrix ADC Splash-Seite.




## Push-Benachrichtigung für OTP

March 27, 2024

Citrix Gateway unterstützt Push-Benachrichtigungen für OTP. Benutzer müssen den auf ihren registrierten Geräten empfangenen OTP nicht manuell eingeben, um sich bei Citrix Gateway anzumelden. Administratoren können Citrix Gateway so konfigurieren, dass Anmeldebenachrichtigungen über Push-Benachrichtigungsdienste an registrierte Geräte gesendet werden. Wenn Benutzer die Benachrichtigung erhalten, müssen sie bei der Benachrichtigung einfach auf Zulassen tippen, um sich bei Citrix Gateway anzumelden. Wenn Gateway eine Bestätigung vom Benutzer erhält, identifiziert es die Quelle der Anforderung und sendet eine Antwort an diese Browserverbindung.

Wenn die Benachrichtigungsantwort nicht innerhalb des Zeitüberschreitungszeitraums (30 Sekunden) empfangen wird, werden Benutzer zur Citrix Gateway-Anmeldeseite weitergeleitet. Die Benutzer können dann den OTP manuell eingeben oder auf **Benachrichtigung erneut senden** klicken, um die Benachrichtigung erneut auf dem registrierten Gerät zu erhalten.

Administratoren können Push-Benachrichtigungsauthentifizierung als Standardauthentifizierung vornehmen, indem sie die Loginschemas verwenden, die für die Push-Benachrichtigung erstellt wurden.

> **Wichtig:** Die Push-Benachrichtigungsfunktion ist mit einer Citrix ADC Premium Edition Lizenz verfügbar.

### Vorteile von Push-Benachrichtigungen

- Push-Benachrichtigungen bieten einen sichereren Multi-Faktor-Authentifizierungsmechanismus. Die Authentifizierung bei Citrix Gateway ist erst erfolgreich, wenn der Benutzer den Anmeldeversuch genehmigt hat.
- Push-Benachrichtigung ist einfach zu verwalten und zu verwenden. Benutzer müssen die mobile Citrix SSO-App herunterladen und installieren, für die keine Administratorunterstützung erforderlich ist.
- Benutzer müssen den Code nicht kopieren oder merken. Sie müssen einfach auf das Gerät tippen, um authentifiziert zu werden.
- Benutzer können mehrere Geräte registrieren.

### Funktionsweise von Push-Benachrichtigungen

Der Workflow für Pushbenachrichtigungen kann in zwei Kategorien eingeteilt werden:

- Geräteregistrierung
- Endbenutzer-Anmeldung

### Voraussetzungen für die Verwendung von Push-Benachrichtigungen

- Schließen Sie den Citrix Cloud-Onboarding-Prozess ab.
    1. Erstellen Sie ein Citrix Cloud-Unternehmenskonto oder treten Sie einem vorhandenen Konto bei. Detaillierte Prozesse und Anweisungen zum Fortfahren finden Sie unter Registrieren für Citrix Cloud.
    2. Melden Sie sich bei anhttps://citrix.cloud.comund wählen Sie den Kunden aus.
    3. Wählen Sie im Menü die Option Identitäts- und Zugriffsverwaltung aus, und navigieren Sie dann zur Registerkarte API-Zugriff, um einen Client für den Kunden zu erstellen.
    4. Kopieren Sie die ID, die geheime und die Kunden-ID. Die ID und der geheime Schlüssel sind erforderlich, um den Push-Dienst in Citrix ADC als “ClientID”bzw. “ClientSecret”zu konfigurieren.

> **Wichtig:**
>
> - Gleiche API-Anmeldeinformationen können in mehreren Rechenzentren verwendet

werden.
- Citrix ADC-Appliances müssen in der Lage sein, die Serveradressen mfa.cloud.com und trust.citrixworkspacesapi.net aufzulösen und von der Appliance aus zu erreichen. Damit soll sichergestellt werden, dass keine Firewalls oder IP-Adressblöcke für diese Server über Port 443 vorhanden sind.

- Laden Sie die Citrix SSO mobile App aus dem App Store und dem Play Store für iOS-Geräte bzw. Android-Geräte herunter. Push-Benachrichtigung wird unter iOS ab Build 1.1.13 auf Android ab 2.3.5 unterstützt.
- Stellen Sie für Active Directory Folgendes sicher.
  - Die minimale Attributlänge muss mindestens 256 Zeichen lang sein.
  - Attributtyp muss "DirectoryString"sein, z. B. UserParameters. Diese Attribute können Zeichenfolgenwerte enthalten.
  - Der Typ der Attributzeichenfolge muss Unicode sein, wenn der Gerätename nicht englische Zeichen enthält.
  - Der Citrix ADC LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.
  - Citrix ADC und der Clientcomputer müssen mit einem gemeinsamen Netzwerkzeitserver synchronisiert werden.

## Konfiguration von Push-Benachrichtigungen

Im Folgenden werden die Schritte auf hoher Ebene aufgeführt, die ausgeführt werden müssen, um die Push-Benachrichtigungsfunktion zu verwenden.

- Der Citrix Gateway-Administrator muss die Schnittstelle konfigurieren, um Benutzer zu verwalten und zu validieren.
  1. Konfigurieren Sie einen Push-Service.
  2. Konfigurieren Sie Citrix Gateway für die OTP-Verwaltung und die Endbenutzeranmeldung.

     Benutzer müssen ihre Geräte beim Gateway registrieren, um sich bei Citrix Gateway anzumelden.
  3. Registrieren Sie Ihr Gerät bei Citrix Gateway.
  4. Melden Sie sich bei Citrix Gateway an.

### Erstellen eines Push-Service

1. Navigieren Sie zu **Sicherheit** > **AAA-Anwendungsdatenverkehr** > **Richtlinien** > **Authentifizierung** > **Erweiterte Richtlinien** > **Aktionen** > **Push-Dienst**, und klicken Sie auf **Hinzufü-**

**gen** .

2. Geben Sie **unter Name**den Namen des Push-Dienstes ein.
3. Geben Sie unter **Client-ID**die eindeutige Identität der vertrauenden Partei für die Kommunikation mit dem Citrix Push-Server in der Cloud ein.
4. Geben Sie unter **Client Secret**das eindeutige Geheimnis der vertrauenden Partei für die Kommunikation mit dem Citrix Push-Server in der Cloud ein.
5. Geben Sie unter **Kunden-ID**die Kunden-ID oder den Namen des Kontos in der Cloud ein, mit dem Client-ID und Client-geheimes Paar erstellt werden.

### Konfigurieren von Citrix Gateway für OTP-Verwaltung und Endbenutzeranmeldung

Führen Sie die folgenden Schritte für die OTP-Verwaltung und die Endbenutzeranmeldung aus.

- Anmeldeschema für die OTP-Verwaltung erstellen
- Konfigurieren der Authentifizierung, Autorisierung und Überwachung des virtuellen Servers
- Konfigurieren von VPN- oder Lastausgleichs-Servern
- Richtlinienlabel konfigurieren
- Anmeldeschema für Endbenutzer-Anmeldung erstellen

Weitere Informationen zur Konfiguration finden Sie unterNative OTP-Unterstützung.

**Wichtig**: Für Push-Benachrichtigungen müssen Administratoren Folgendes explizit konfigurieren:

- Erstellen Sie einen Push-Service.
- Wählen Sie beim Erstellen des Anmeldeschemas für die OTP-Verwaltung das Anmeldeschema SingleAuthManageOTP.xml oder ein Äquivalent gemäß der Notwendigkeit aus.
- Wählen Sie beim Erstellen des Anmeldeschemas für die Endbenutzeranmeldung das Anmeldeschema DualAuthOrPush.xml oder ein Äquivalent gemäß der Notwendigkeit aus.

### Registrieren Sie Ihr Gerät bei Citrix Gateway

Benutzer müssen ihre Geräte bei Citrix Gateway registrieren, um die Push-Benachrichtigungsfunktion nutzen zu können.

1. Navigieren Sie in Ihrem Webbrowser zu Ihrem Citrix Gateway-FQDN und Suffix **/manageotp** zum FQDN.

   Dadurch wird die Authentifizierungsseite geladen.
   Beispiel: https://gateway.company.com/manageotp
2. Melden Sie sich bei Bedarf mit Ihren LDAP-Anmeldeinformationen oder geeigneten Zwei-Faktor-Authentifizierungsmechanismen an.

3. Klicken Sie auf **Gerät hinzufügen**.
4. Geben Sie einen Namen für Ihr Gerät ein, und klicken Sie auf **Los**.

   Ein QR-Code wird auf der Citrix Gateway-Browserseite angezeigt.
5. Scannen Sie diesen QR-Code mit der Citrix SSO-App vom zu registrierenden Gerät aus.

   Citrix SSO überprüft den QR-Code und registriert sich dann beim Gateway für Push-Benachrichtigungen. Wenn bei der Registrierung keine Fehler auftreten, wird das Token erfolgreich zur Seite Kennworttokens hinzugefügt.
6. Wenn es keine zusätzlichen Geräte zum Hinzufügen/Verwalten gibt, melden Sie sich mit der Liste oben rechts auf der Seite ab.

**Testen der Einmalkennwortauthentifizierung**

1. Klicken Sie zum Testen des OTP in der Liste auf Ihr Gerät, und klicken Sie dann auf **Testen**.
2. Geben Sie den OTP ein, den Sie auf Ihrem Gerät erhalten haben, und klicken Sie auf Los.**

   Die Meldung OTP-Überprüfung erfolgreich wird angezeigt.
3. Melden Sie sich mit der Liste oben rechts auf der Seite ab.

Hinweis: Sie können das OTP-Verwaltungsportal jederzeit verwenden, um die Authentifizierung zu testen, registrierte Geräte zu entfernen oder weitere Geräte zu registrieren.**

**Anmelden bei Citrix Gateway**

Nach der Registrierung ihrer Geräte bei Citrix Gateway können Benutzer die Push-Benachrichtigungsfunktion für die Authentifizierung verwenden.

1. Navigieren Sie zu der Citrix Gateway-Authentifizierungsseite (Beispiel:https://gateway.company.com)

   Je nach Konfiguration des Anmeldeschemas werden Sie aufgefordert, nur Ihre LDAP-Anmeldeinformationen einzugeben.
2. Geben Sie Ihren LDAP-Benutzernamen und Ihr Kennwort ein, und wählen Sie **Absenden**aus.

   Eine Benachrichtigung wird an Ihr registriertes Gerät gesendet.

   **Hinweis:** Wenn Sie den OTP manuell eingeben möchten, müssen Sie **auf Klicken klicken**, um OTP manuell einzugeben, und den OTP in das Feld **TOTP** eingeben.
3. Öffnen Sie die Citrix SSO-App auf Ihrem registrierten Gerät und tippen Sie auf **Zulassen**.

**Hinweis**:

- Der Authentifizierungsserver wartet auf Push-Server-Benachrichtigungsantwort, bis der konfigurierte Zeitüberschreitungszeitraum abgelaufen ist. Nach dem Timeout zeigt Citrix Gateway die Anmeldeseite an. Die Benutzer können dann den OTP manuell eingeben oder auf **Benachrichtigung erneut senden** klicken, um die Benachrichtigung erneut auf dem registrierten Gerät zu erhalten. Basierend auf Ihrer ausgewählten Option validiert Gateway den von Ihnen eingegebenen OTP oder sendet die Benachrichtigung erneut auf Ihrem registrierten Gerät.
- Es wird keine Benachrichtigung an Ihr registriertes Gerät über einen Fehler bei der Anmeldung gesendet.

## Fehlerbedingungen

- Die Geräteregistrierung schlägt in den folgenden Fällen möglicherweise fehl.
  - Das Serverzertifikat wird vom Endbenutzergerät möglicherweise nicht vertrauenswürdig.
  - Citrix Gateway, das zur Registrierung für OTP verwendet wird, ist vom Client nicht erreichbar.
- Die Benachrichtigungen können in den folgenden Fällen fehlschlagen.
  - Benutzergerät ist nicht mit dem Internet verbunden
  - Benachrichtigungen auf dem Benutzergerät werden blockiert
  - Benutzer genehmigt die Benachrichtigung auf dem Gerät nicht

In diesen Fällen wartet der Authentifizierungsserver, bis der konfigurierte Zeitüberschreitungszeitraum abgelaufen ist. Nach dem Timeout zeigt Citrix Gateway eine Anmeldeseite mit den Optionen an, das OTP manuell einzugeben oder die Benachrichtigung erneut auf Ihrem registrierten Gerät erneut zu senden. Basierend auf der ausgewählten Option erfolgt eine weitere Validierung.

## Citrix SSO-App-Verhalten unter iOS —weist darauf hin

### Benachrichtigungsverknüpfungen

Citrix SSO iOS-App bietet Unterstützung für verwertbare Benachrichtigungen, um die Benutzerfreundlichkeit zu verbessern. Sobald eine Benachrichtigung auf einem iOS-Gerät empfangen wurde und das Gerät gesperrt ist oder sich die Citrix SSO-App nicht im Vordergrund befindet, können Benutzer die in der Benachrichtigung integrierten Verknüpfungen verwenden, um die Anmeldeanforderung entweder zu genehmigen oder zu verweigern.

Um auf Benachrichtigungsverknüpfungen zuzugreifen, müssen Benutzer entweder die Berührung erzwingen (3D-Touch) oder die Benachrichtigung je nach Hardware des Geräts lange drücken. Durch Auswahl der Aktion Verknüpfung zulassen wird eine Anmeldeanforderung an Citrix ADC gesendet.

Je nachdem, wie die Authentifizierungsrichtlinie auf dem virtuellen Server für Authentifizierung, Autorisierung und Überwachung konfiguriert ist;

- Die Anmeldeanforderung kann im Hintergrund gesendet werden, ohne die App in den Vordergrund zu starten oder das Gerät zu entsperren.
- Die App kann als zusätzlicher Faktor für Touch-ID/Face -ID/Passcode auffordern. In diesem Fall wird die App in den Vordergrund gestartet.

**Löschen von Kennwort-Token aus Citrix SSO**

1. Um ein Kennworttoken zu löschen, das für Push in der Citrix SSO-App registriert ist, müssen Benutzer die folgenden Schritte ausführen:
2. Heben Sie die Registrierung des iOS/Android -Geräts auf dem Gateway auf (entfernen) auf. QR-Code zum Entfernen der Registrierung vom Gerät wird angezeigt.
3. Öffnen Sie die Citrix SSO-App und tippen Sie auf die Info-Schaltfläche des zu löschenden Kennwort-Token.
4. Tippen **Sie auf Token löschen** und scannen Sie den QR-Code.

**Hinweis**:

- Wenn der QR-Code gültig ist, wird das Token erfolgreich aus der Citrix SSO-App entfernt.
- Benutzer können auf Löschen erzwingen tippen, um ein Kennwort-Token zu löschen, ohne den QR-Code scannen zu müssen, wenn das Gerät bereits vom Gateway entfernt wurde. Das Löschen erzwingen kann dazu führen, dass das Gerät weiterhin Benachrichtigungen erhält, wenn das Gerät nicht aus Citrix Gateway entfernt wurde.

## Konfigurieren von Single Sign-On

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass Single Sign-On mit Windows, Webanwendungen (wie SharePoint), Dateifreigaben und für das Webinterface unterstützt wird. Single Sign-On gilt auch für Dateifreigaben, auf die Benutzer über das Dateiübertragungsprogramm im Access Interface oder über das Citrix Gateway-Symbolmenü im Infobereich zugreifen können.

Wenn Sie Single Sign-On bei der Benutzeranmeldung konfigurieren, werden sie automatisch wieder angemeldet, ohne ihre Anmeldeinformationen ein zweites Mal eingeben zu müssen.

# Konfigurieren von Single Sign-On mit Windows

March 27, 2024

Benutzer öffnen eine Verbindung, indem sie das Citrix Gateway Plug-in vom Desktop aus starten. Sie können angeben, dass das Citrix Gateway Plug-in automatisch gestartet wird, wenn sich der Benutzer bei Windows anmeldet, indem Sie Single Sign-On aktivieren. Wenn Sie Single Sign-On konfigurieren, werden die Windows-Anmeldeinformationen der Benutzer zur Authentifizierung an Citrix Gateway übergeben. Das Aktivieren von Single Sign-On für das Citrix Gateway Plug-in erleichtert den Betrieb auf dem Benutzergerät, wie Installationsskripte und automatische Laufwerkszuordnung.

Aktivieren Sie Single Sign-On nur, wenn sich Benutzergeräte bei der Domäne Ihres Unternehmens anmelden. Wenn Single Sign-On aktiviert ist und ein Benutzer von einem Gerät aus eine Verbindung herstellt, das sich nicht in Ihrer Domäne befindet, wird der Benutzer aufgefordert, sich anzumelden.

Sie konfigurieren Single Sign-On mit Windows entweder global oder mithilfe eines Sitzungsprofils, das an eine Sitzungsrichtlinie angehängt ist.

## So konfigurieren Sie Single Sign-On mit Windows global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte **Client Experienceauf Single Sign-On with Windows**, und klicken Sie dann auf**OK**.

## So konfigurieren Sie Single Sign-On mit Windows über eine Sitzungsrichtlinie

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie**neben Profil anfordern**auf **Neu**.
5. **Geben Sie im Feld Name einen Namen für das Profil ein.**
6. Klicken Sie auf der Registerkarte **Client Experience** neben **Single Sign-On mit Windows** auf **Global überschreiben**, klicken Sie **auf Single Sign-On mit Windows**, und klicken Sie dann auf **OK**.
7. Wählen **Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben **Benannte Ausdrückedie Option Allgemein**aus, wählen Sie Wahrer Wert aus, klicken Sie auf**Ausdruck hinzufügen**, klicken Sie auf**Erstellen**und dann auf**Schließen**.

# Konfigurieren von Single Sign-On für Webanwendungen

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass einmaliges Anmelden für Server im internen Netzwerk bereitgestellt wird, die webbasierte Authentifizierung verwenden. Mit einmaliger Anmeldung können Sie den Benutzer zu einer benutzerdefinierten Homepage wie einer SharePoint-Website oder zum Webinterface umleiten. Sie können das einmalige Anmelden bei Ressourcen auch über das Citrix Gateway-Plug-in über ein auf der Homepage konfiguriertes Lesezeichen oder eine Webadresse konfigurieren, die Benutzer im Webbrowser eingeben.

Wenn Sie die Homepage auf eine SharePoint-Website oder ein Webinterface umleiten, geben Sie die Webadresse für die Website an. Wenn Benutzer entweder von Citrix Gateway oder einem externen Authentifizierungsserver authentifiziert werden, werden Benutzer auf die angegebene Homepage umgeleitet. Benutzeranmeldeinformationen werden transparent an den Webserver weitergegeben. Wenn der Webserver die Anmeldeinformationen akzeptiert, werden Benutzer automatisch angemeldet. Wenn der Webserver die Anmeldeinformationen verweigert, erhalten Benutzer eine Authentifizierungsaufforderung, in der sie nach ihrem Benutzernamen und Kennwort gefragt werden.

Sie können Single Sign-On für Webanwendungen global oder mithilfe einer Sitzungsrichtlinie konfigurieren.

## So konfigurieren Sie Single Sign-On für Webanwendungen global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Klicken Sie auf der Registerkarte Client Experience auf Single Sign-On to Web Applications und dann auf OK.

## So konfigurieren Sie Single Sign-On bei Webanwendungen mithilfe einer Sitzungsrichtlinie

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway > Richtlinien und klicken Sie dann auf Sitzung.
2. Wählen Sie im Detailbereich auf der Registerkarte Richtlinien eine Sitzungsrichtlinie aus und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld Sitzungsrichtlinie konfigurieren neben Anforderungsprofil auf Ändern.

4. Klicken Sie auf der Registerkarte Clienterfahrung neben Single Sign-On bei Webanwendungen auf Global Override, klicken Sie auf Single Sign-On to Web Applications und dann auf OK.

### Definieren des HTTP-Ports für Single Sign-On bei Webanwendungen

Single Sign-On wird nur für den Netzwerkverkehr versucht, bei dem der Zielport als HTTP-Port betrachtet wird. Um Single Sign-On für Anwendungen zu ermöglichen, die einen anderen Port als Port 80 für HTTP-Verkehr verwenden, fügen Sie eine oder mehrere Portnummern auf Citrix Gateway hinzu. Sie können mehrere Ports aktivieren. Die Ports sind global konfiguriert.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte "Configuration"im Navigationsbereich "Citrix Gateway"und klicken Sie auf "Global Settings".
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Klicken Sie auf der Registerkarte Netzwerkkonfiguration auf Erweiterte Einstellungen.
4. Geben Sie unter HTTP-Ports die Portnummer ein, klicken Sie auf Hinzufügen und dann zweimal auf OK.

   Sie können Schritt 4 für jeden Port wiederholen, den Sie hinzufügen möchten.

**Hinweis**: Wenn Webanwendungen im internen Netzwerk öffentliche IP-Adressen verwenden, funktioniert Single Sign-On nicht. Um Single Sign-On zu aktivieren, muss Split-Tunneling als Teil der globalen Richtlinieneinstellung aktiviert werden, unabhängig davon, ob der clientlose Zugriff oder das Citrix Gateway-Plug-in für Benutzergeräteverbindungen verwendet wird. Wenn es nicht möglich ist, Split-Tunneling auf globaler Ebene zu aktivieren, erstellen Sie einen virtuellen Server, der einen privaten Adressbereich verwendet.

## Single Sign-On bei Webanwendungen mit LDAP konfigurieren

March 27, 2024

Wenn Sie Single Sign-On konfigurieren und sich Benutzer mithilfe des Benutzerprinzipalnamens (UPN) mit dem Format
username@domain.com anmelden, schlägt das einmalige Anmelden standardmäßig fehl und die Benutzer müssen sich zweimal authentifizieren. Wenn Sie dieses Format für die Benutzeranmeldung verwenden müssen, ändern Sie die LDAP-Authentifizierungsrichtlinie, um diese Form des Benutzernamens zu akzeptieren.

### So konfigurieren Sie Single Sign-On für Webanwendungen

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **KonfigurationCitrix Gateway > Richtlinien > Authentifizierung**.
2. Wählen Sie im Detailbereich auf der Registerkarte **Richtlinien** eine LDAP-Richtlinie aus, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie im Dialogfeld **Authentifizierungsrichtlinie konfigurieren** neben **Server** auf **Ändern**.
4. Geben Sie unter **Verbindungseinstellungen**in Basis-DN (Standort der Benutzer) DC=Domainname, DC=com ein.
5. Geben Sie unter **Administrator Bind-DN**LDAPaccount@domainname.com ein, wobei Domainname.com der Name Ihrer Domain ist.
6. Geben Sie unter **Administratorkennwort** und **Administratorkennwort bestätigen**das Kennwort ein.
7. Geben Sie unter **Andere Einstellungen**in **Serveranmeldungsnamenattribut**userPrincipalName ein.
8. Geben Sie im **Feld Gruppenattribut**MemberOf ein.
9. Geben Sie unter **Name des Unterattributs**CN ein.
10. Geben Sie **unter SSO-Namensattribut**das Format ein, mit dem sich Benutzer anmelden, und klicken Sie dann zweimal auf **OK**. Dieser Wert ist entweder `SamAccountName` oder `UserPrincipalName`.

## Konfigurieren von Single Sign-On für eine Domäne

March 27, 2024

Wenn Benutzer eine Verbindung zu Servern herstellen, auf denen Citrix Virtual Apps ausgeführt wird, und SmartAccess verwenden, können Sie Single Sign-On für Benutzer konfigurieren, die eine Verbindung zur Serverfarm herstellen. Wenn Sie den Zugriff auf veröffentlichte Anwendungen mithilfe einer Sitzungsrichtlinie und eines Profils konfigurieren, verwenden Sie den Domänennamen für die Serverfarm.

Sie können auch Single Sign-On für Dateifreigaben in Ihrem Netzwerk konfigurieren.

### So konfigurieren Sie Single Sign-On für eine Domäne

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway > Richtlinien und klicken Sie dann auf Sitzung.

2. Wählen Sie im Detailbereich auf der Registerkarte Richtlinien eine Sitzungsrichtlinie aus und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld Sitzungsrichtlinie konfigurieren neben Anforderungsprofil auf Ändern.
4. Klicken Sie im Dialogfeld Sitzungsprofil konfigurieren auf der Registerkarte Veröffentlichte Anwendungen unter Single Sign-On-Domäne auf Global überschreiben, geben Sie den Domänennamen ein, und klicken Sie dann zweimal auf OK.

Weitere Informationen zum Konfigurieren von Citrix Gateway mit Citrix Virtual Apps finden Sie unter Integrieren von Citrix Gateway mit Citrix Virtual Apps and Desktops.

## Konfigurieren von Single Sign-On für Microsoft Exchange 2010

March 27, 2024

Im folgenden Abschnitt wird die Konfiguration von Single Sign-On (SSO) für Microsoft Exchange 2010 auf Citrix Gateway beschrieben. Das SSO für Outlook Web Access (OWA) 2010 funktioniert unter den folgenden Bedingungen nicht:

- Verwenden der formularbasierten Authentifizierung auf Microsoft Exchange 2010.
- Load Balancing virtueller Server mit Authentifizierungs-, Autorisierungs- und Überwachungsverkehrsmanag Richtlinie.

> **Hinweis:** Diese Konfiguration funktioniert nur für den Lastausgleich eines virtuellen Servers mit Authentifizierungs-, Autorisierungs- und Überwachungsverkehrsverwaltungsrichtlinien. Es funktioniert nicht für SSO in OWA 2010 mit clientlosem VPN.

Die folgenden Schritte sind Voraussetzungen, die Sie berücksichtigen müssen, bevor Sie SSO für Microsoft Exchange 2010 auf Citrix Gateway konfigurieren.

- Die Aktions-URL für das SSO-Formular ist in OWA 2010 anders. Ändern Sie die Verkehrsmanagement-Richtlinie entsprechend.
- Sie benötigen eine Richtlinie zum Umschreiben, um das Cookie `PBack` in der Anforderung logon.aspx zu setzen. In normalen Szenarien setzen Sie das `PBack` Cookie beim Client und klicken auf Senden.
- Wenn Sie SSO verwenden, wird die Antwort auf logon.aspx verbraucht und das Citrix Gateway generiert die Formularanforderung. Das Cookie ist nicht in der Anfrage zur Einreichung des Formulars angehängt.
- Der OWA-Server erwartet das Cookie `PBack` in der Anfrage zur Einreichung des Formulars. Die Richtlinie zum Umschreiben ist erforderlich, um das Cookie `PBack` in der Anfrage zur Einreichung des Formulars anzuhängen.

### Führen Sie Folgendes mit der CLI aus

1. Konfigurieren Sie die Authentifizierung, Autorisierung und Überwachung des Verkehrsmanagements

   ```
   add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.owa"-userField username -passwdField password -ssoSuccessRule "http.RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.GT(70"-responsesize 15000 -submitMethod POST
   ```

2. Konfigurieren Sie die Verkehrsverwaltungsrichtlinie und binden Sie die Richtlinie

   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
   - `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")"OWA_2010_Prof`
   - `bind tm global -policyName owa2k10_pol -priority 100`

### Rewrite-Konfiguration über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")""\";PBack=0\""-bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

#### Alternative Rewrite-Konfiguration

In seltenen Fällen gibt Microsoft Outlook möglicherweise keine OWA-Sitzungscookies aus und die `Pback` Cookies werden möglicherweise auch nicht eingefügt. Das Problem kann auftreten, nachdem Sie die vorhergehenden Befehle zur Implementierung der Rewrite-Konfiguration ausgeführt haben.

Um solche Szenarien zu überwinden und als Problemumgehung, können Sie anstelle der Umschreibkonfiguration die folgenden Befehle konfigurieren.

Geben Sie in der Befehlszeile Folgendes ein:

- `add rewrite action set_pback_cookie insert_http_header "Cookie"'" PBack=0"'`

- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\" logon.aspx\")"set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

## Verwendung von Einmalkennwörtern konfigurieren

March 27, 2024

Sie können Citrix Gateway für die Verwendung von Einmalkennwörtern wie einer persönlichen Identifikationsnummer (PIN) oder einem Passcode für Token konfigurieren. Nachdem ein Benutzer den Passcode oder die PIN eingegeben hat, macht der Authentifizierungsserver das Einmalkennwort sofort ungültig und der Benutzer kann dieselbe PIN oder dasselbe Kennwort nicht erneut eingeben.

Zu den Produkten, die die Verwendung eines Einmalkennworts beinhalten, gehören

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordischer SMS-PASSCODE

Um jedes dieser Produkte zu verwenden, konfigurieren Sie den Authentifizierungsserver im internen Netzwerk für die Verwendung von RADIUS. Weitere Informationen finden Sie unter Konfigurieren der RADIUS-Authentifizierung.

Wenn Sie die Authentifizierung auf Citrix Gateway so konfigurieren, dass ein Einmalkennwort mit RADIUS verwendet wird, wie es beispielsweise von einem RSA SecurID-Token bereitgestellt wird, versucht Citrix Gateway, Benutzer mithilfe des zwischengespeicherten Kennworts erneut zu authentifizieren. Diese erneute Authentifizierung erfolgt, wenn Sie Änderungen an Citrix Gateway vornehmen oder wenn die Verbindung zwischen dem Citrix Gateway Plug-in und Citrix Gateway unterbrochen und dann wiederhergestellt wird.

Ein Versuch einer erneuten Authentifizierung kann auch auftreten, wenn Verbindungen für die Verwendung der Citrix Workspace-App konfiguriert sind und Benutzer mithilfe von RADIUS oder LDAP eine Verbindung zum Webinterface herstellen. Wenn ein Benutzer eine Anwendung startet und die Anwendung verwendet und dann zu Receiver zurückkehrt, um eine andere Anwendung zu starten, verwendet Citrix Gateway zwischengespeicherte Informationen, um den Benutzer zu authentifizieren.

# RSA SecurID-Authentifizierung konfigurieren

March 27, 2024

Bei der Konfiguration des RSA/ACE-Servers für die RSA SecureID-Authentifizierung müssen Sie die folgenden Schritte ausführen:

Konfigurieren Sie den RADIUS-Client mit den folgenden Informationen:

- Geben Sie den Namen des Citrix Gateway-Geräts an.
- Geben Sie eine Beschreibung ein (nicht zwingend erforderlich).
- Geben Sie die System-IP-Adresse an.
- Stellen Sie das gemeinsame Geheimnis zwischen Citrix Gateway und dem RADIUS-Server bereit.
- Konfigurieren Sie die Marke/das Modell als Standard-RADIUS.

In der Konfiguration des Agent-Hosts benötigen Sie die folgenden Informationen:

- Geben Sie den vollqualifizierten Domänennamen (FQDN) von Citrix Gateway an (wie er auf dem an den virtuellen Server gebundenen Zertifikat angezeigt wird). Nachdem Sie den FQDN bereitgestellt haben, klicken Sie auf die Tabulatortaste und das Fenster Netzwerkadresse füllt sich selbst.

  Nachdem Sie den FQDN eingegeben haben, wird die Netzwerkadresse automatisch angezeigt. Wenn dies nicht der Fall ist, geben Sie die System-IP-Adresse ein.
- Geben Sie den Agententyp mithilfe von Communication Server an.
- Konfigurieren Sie den Import aller Benutzer oder einer Reihe von Benutzern, die sich über Citrix Gateway authentifizieren dürfen.

Wenn es noch nicht konfiguriert ist, erstellen Sie einen Agent-Host-Eintrag für den RADIUS-Server mit den folgenden Informationen:

- Stellen Sie den FQDN des RSA-Servers bereit.

  Nachdem Sie den FQDN eingegeben haben, wird die Netzwerkadresse automatisch angezeigt. Wenn dies nicht der Fall ist, geben Sie die IP-Adresse des RSA-Servers an.
- Geben Sie den Agent-Typ an, bei dem es sich um den RADIUS-Server handelt.

Weitere Informationen zur Konfiguration eines RSA RADIUS-Servers finden Sie in der Dokumentation des Herstellers.

Um RSA SecurID zu konfigurieren, erstellen Sie ein Authentifizierungsprofil und eine Richtlinie und binden Sie die Richtlinie dann global oder an einen virtuellen Server. Informationen zum Erstellen einer RADIUS-Richtlinie zur Verwendung von RSA SecurID finden Sie unter Konfigurieren der RADIUS-Authentifizierung.

Binden Sie die Authentifizierungsrichtlinie nach dem Erstellen an einen virtuellen Server oder global. Weitere Informationen finden Sie unter Binding Authentication Policies.

## Kennwortrückgabe mit RADIUS konfigurieren

March 27, 2024

Sie können Domain-Kennwörter durch ein Einmalkennwort ersetzen, das ein Token von einem RADIUS-Server generiert. Wenn sich Benutzer bei Citrix Gateway anmelden, geben sie eine persönliche Identifikationsnummer (PIN) und den Passcode aus dem Token ein. Nachdem Citrix Gateway seine Anmeldeinformationen überprüft hat, gibt der RADIUS-Server das Windows-Kennwort des Benutzers an Citrix Gateway zurück. Citrix Gateway akzeptiert die Antwort vom Server und verwendet dann das zurückgegebene Kennwort für die einmalige Anmeldung, anstatt den Passcode zu verwenden, den Benutzer während der Anmeldung eingegeben haben. Diese Kennwortrückgabe mit der RADIUS-Funktion ermöglicht es Ihnen, Single Sign-On zu konfigurieren, ohne dass Benutzer ihr Windows-Kennwort abrufen müssen.

Wenn sich Benutzer mithilfe der Kennwortrückgabe anmelden, können sie auf alle zulässigen Netzwerkressourcen im internen Netzwerk zugreifen, einschließlich Citrix Endpoint Management, StoreFront und dem Webinterface.

Um das einmalige Anmelden mithilfe von zurückgegebenen Kennwörtern zu aktivieren, konfigurieren Sie eine RADIUS-Authentifizierungsrichtlinie auf Citrix Gateway mithilfe der Parameter Password Vendor Identifier und Kennwortattributtyp. Diese beiden Parameter geben das Windows-Kennwort des Benutzers an Citrix Gateway zurück.

Citrix Gateway unterstützt Imprivata OneSign. Die erforderliche Mindestversion von Imprivata OneSign ist 4.0 mit Service Pack 3. Die standardmäßige Kennwort-Hersteller-ID für Imprivata OneSign ist 398. Der standardmäßige Kennwort-Attribut-Typcode für Imprivata OneSign ist 5.

Sie können andere RADIUS-Server für die Kennwortrückgabe verwenden, z. B. RSA, Cisco oder Microsoft. Konfigurieren Sie den RADIUS-Server so, dass das einmalige Anmeldekennwort des Benutzers in einem herstellerspezifischen Attributwert-Paar zurückgegeben wird. In einer Citrix Gateway-Authentifizierungsrichtlinie müssen Sie die Parameter **Kennwort Vendor Identifier und Kennwortattributtyp** für diese Server hinzufügen.

Eine vollständige Liste der Lieferantenkennungen finden Sie auf der Website der Internet Assigned Numbers Authority (IANA). Beispielsweise lautet die Hersteller-ID für RSA-Sicherheit 2197, für Microsoft 311 und für Cisco Systems ist sie 9. Das herstellerspezifische Attribut, das ein Anbieter unterstützt, muss mit dem Anbieter bestätigt werden. Beispielsweise hat Microsoft eine Liste herstellerspezifischer Attribute bei herstellerspezifischen MICROSOFT-RADIUS-Attributenveröffentlicht.

Sie können jedes der herstellerspezifischen Attribute auswählen, um das Single-Sign-On-Kennwort für Benutzer auf dem RADIUS-Server des Anbieters zu speichern. Wenn Sie Citrix Gateway mit der Hersteller-ID und dem Attribut konfigurieren, in dem das Benutzerkennwort auf dem RADIUS-Server gespeichert ist, fordert Citrix Gateway den Wert des Attributs im Zugriffsanforderungspaket an, das an den RADIUS-Server gesendet wird. Wenn der RADIUS-Server mit dem entsprechenden Attribut-Wert-Paar im Access-Accept-Paket antwortet, funktioniert die Kennwortrückgabe unabhängig vom verwendeten RADIUS-Server.

So konfigurieren Sie Single Sign-On mithilfe von zurückgegebenen Kennwörtern:

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien\ > Authentifizierung**.
2. Klicken Sie im Navigationsbereich auf **RADIUS**.
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **Authentifizierungsrichtlinie erstellen** in das Feld Name einen Namen für die Richtlinie ein.
5. Klicken Sie neben **Server** auf **Neu**.
6. Geben Sie unter **Name** den Namen des Servers ein.
7. Konfigurieren Sie die Einstellungen für den RADIUS-Server.
8. Geben Sie unter **Password Vendor Identifier** die Hersteller-ID ein, die vom RADIUS-Server zurückgegeben wird. Dieser Bezeichner muss einen Mindestwert von 1 haben.
9. Geben Sie unter **Kennwortattributtyp** den Attributtyp, der vom RADIUS-Server zurückgegeben wird, im herstellerspezifischen AVP-Code ein. Der Wert kann zwischen 1 und 255 liegen.
10. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie **erstellen** neben **Benannte Ausdrücke** den Ausdruck aus, klicken Sie auf **Ausdruck hinzufügen** , klicken Sie auf **Erstellen** und dann auf **Schließen**.

## SafeWord-Authentifizierung konfigurieren

January 29, 2024

Die SafeWord-Produktlinie hilft bei der Bereitstellung einer sicheren Authentifizierung mithilfe eines tokenbasierten Passcodes. Nachdem Benutzer einen Passcode eingegeben haben, wird dieser von SafeWord ungültig und kann nicht erneut verwendet werden.

Wenn Access Gateway Secure Gateway in einer Secure Gateway- und Webinterface-Bereitstellung ersetzt, können Sie die Authentifizierung auf dem Access Gateway nicht konfigurieren und dem Webinterface weiterhin erlauben, SafeWord-Authentifizierung für eingehenden HTTP-Verkehr bereitzustellen.

Access Gateway unterstützt die SafeWord-Authentifizierung für die folgenden Produkte:

- SafeWord 2008
- SafeWord PremierAccess
- SafeWord für Citrix
- SafeWord RemoteAccess

Sie können Access Gateway auf folgende Weise für die Authentifizierung mit SafeWord-Produkten konfigurieren:

- Konfigurieren Sie die Authentifizierung für die Verwendung eines PremierAccess RADIUS-Servers, der als Teil von SafeWord PremierAccess installiert wird, und erlauben Sie ihm, die Authentifizierung abzuwickeln.
- Konfigurieren Sie die Authentifizierung für die Verwendung des SafeWord IAS-Agenten, der eine Komponente von SafeWord RemoteAccess, SafeWord für Citrix und SafeWord PremierAccess 4.0 ist.
- Installieren Sie den SafeWord Webinterface Agent zur Unterstützung des Citrix Webinterface. Sie müssen die Authentifizierung auf Access Gateway nicht konfigurieren, und das Citrix Webinterface kann damit umgehen. Bei dieser Konfiguration werden weder der PremierAccess RADIUS-Server noch der SafeWord IAS-Agent verwendet.

Bei der Konfiguration des SafeWord RADIUS-Servers benötigen Sie folgende Informationen:

- Die IP-Adresse von Access Gateway. Wenn Sie Clienteinstellungen auf dem RADIUS-Server konfigurieren, verwenden Sie die Access Gateway-IP-Adresse.
- Ein gemeinsames Geheimnis.
- Die IP-Adresse und der Port des SafeWord-Servers.

## Gemalto Protiva-Authentifizierung konfigurieren

March 27, 2024

Protiva ist eine starke Authentifizierungsplattform, die entwickelt wurde, um die Stärken der Smartcard-Authentifizierung von Gemalto zu nutzen. Bei Protiva melden sich Benutzer mit einem Benutzernamen, einem Kennwort und einem Einmalkennwort an, die vom Protiva-Gerät generiert wurden. Ähnlich wie bei RSA SecurID wird die Authentifizierungsanforderung an den Protiva Authentication Server gesendet und das Kennwort wird entweder validiert oder abgelehnt.

Verwenden Sie die folgenden Richtlinien, um Gemalto Protiva für die Unterstützung von Citrix Gateway zu konfigurieren:

- Installieren Sie den Protiva-Server.

- Installieren Sie das Protiva Internet Authentication Server (IAS) -Agenten-Plug-in auf einem Microsoft IAS RADIUS-Server. Vergewissern Sie sich, dass Sie die IP-Adresse und Portnummer des IAS-Servers notieren.

# nFactor für Gateway Authentifizierung

March 27, 2024

Die nFactor-Authentifizierung ermöglicht eine ganze Reihe neuer Möglichkeiten für die Authentifizierung. Administratoren, die nFactor verwenden, profitieren von Authentifizierungs-, Autorisierungs- und Audit-Flexibilität bei der Konfiguration von Authentifizierungsfaktoren für virtuelle Server.

Zwei Richtlinienbanken oder zwei Faktoren schränken einen Administrator nicht mehr ein. Die Anzahl der Richtlinienbanken kann auf unterschiedliche Bedürfnisse ausgeweitet werden. Basierend auf früheren Faktoren bestimmt nFactor eine Authentifizierungsmethode. Dynamische Anmeldeformulare und Aktionen bei einem Fehler sind mithilfe von nFactor möglich.

> **Wichtig!**
>
> - Ab Version 13.0 Build 67.x wird die nFactor-Authentifizierung mit der Standardlizenz nur für den virtuellen Gateway-/VPN-Server und nicht für den virtuellen Authentifizierungsserver unterstützt. In der Standardlizenz kann die nFactor-Visualizer-GUI nicht verwendet werden, um die EPA im nFactor-Flow zu erstellen. Außerdem können Sie das Anmeldeschema nicht bearbeiten, sondern müssen das sofort einsatzbereite Anmeldeschema unverändert verwenden.
> - Damit Citrix ADC die nFactor-Authentifizierung unterstützt, ist eine Advanced-Lizenz oder eine Premium-Lizenz erforderlich. Weitere Informationen zur nFactor-Authentifizierung mit Citrix ADC finden Sie unter nFactor-Authentifizierung.

## Lizenzanforderungen für Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen

In der folgenden Tabelle sind die Lizenzanforderungen für die verfügbaren Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen aufgeführt.

| | Standardlizenz | Advanced Lizenz | Premium Lizenz |
|---|---|---|---|
| **LOKALE Authentifizierung** | Ja | Ja | Ja |
| **LDAP-Authentifizierung** | Ja | Ja | Ja |
| **RADIUS-Authentifizierung** | Ja | Ja | Ja |
| **TACACS-Authentifizierung** | Ja | Ja | Ja |
| **Web-Authentifizierung** | Ja | Ja | Ja |
| **Clientzertifikat-Authentifizierung** | Ja | Ja | Ja |
| **Authentifizierung aushandeln** | Ja | Ja | Ja |
| **SAML-Authentifizierung** | Ja | Ja | Ja |
| **OAuth-Authentifizierung** | Nein | Ja | Ja |
| **Natives OTP** | Nein | Ja | Ja |
| **E-Mail OTP** | Nein | Ja | Ja |
| **Pushbenachrichtigung für OTP** | Nein | Nein | Ja |
| **Wissensbasierte Frage und Antwort (KBA-Authentifizierung)** | Nein | Ja | Ja |
| **Self-Service-Kennwort-Reset (SSPR)** | Nein | Ja | Ja |
| **nFactor Visualizer** | Ja | Ja | Ja |

**Hinweis**

- Schritte zum Konfigurieren von nFactor für die Citrix ADC Standardlizenz finden Sie im Abschnitt Erstellen eines virtuellen Gateway-Servers für die nFactor-Authentifizierung in der Citrix ADC Standard-Lizenz.
- Nur ein nicht adressierbarer virtueller Authentifizierungs-, Autorisierungs- und Überwachungsserver kann in der Citrix ADC Standard-Lizenz an einen virtuellen Gateway-/VPN-Server gebunden werden.
- Die Anpassung von LoginSchema ist in der Citrix ADC Standard-Lizenz nicht zulässig. Die nFactor-Unterstützung ist einfach und bietet nur standardmäßige und bereits hinzugefügte Anmeldeschemas, die mit der Appliance geliefert werden. Der Administrator kann sie in seinen Konfigurationen verwenden, aber er kann kein Anmeldeschema hinzufügen. Daher ist die GUI-Option deaktiviert.

## Anwendungsfälle

nFactor-Authentifizierung ermöglicht dynamische Authentifizierungsflüsse basierend auf dem Benutzerprofil. Manchmal können die Abläufe für den Benutzer einfach und intuitiv sein. In anderen Fällen können sie mit der Sicherung von Active Directory oder anderen Authentifizierungsservern gekoppelt werden. Im Folgenden sind einige Gateway-spezifische Anforderungen aufgeführt:

1. **Dynamische Auswahl von Benutzernamen und Kennwort.** Traditionell verwenden die Citrix Clients (einschließlich Browser und Receiver) das Active Directory-Kennwort (AD) als erstes Kennwortfeld. Das zweite Kennwort ist für das Einmalkennwort (OTP) reserviert. Um AD-Server zu sichern, muss OTP jedoch zuerst validiert werden. nFactor kann dies tun, ohne dass Clientänderungen erforderlich sind.
2. **Endpunkt für mehrinstanzenfähige Authentifizierung.** Einige Organisationen verwenden unterschiedliche Gateway-Server für Benutzer von Zertifikaten und Nicht-Zertifikaten. Wenn Benutzer ihre eigenen Geräte zum Anmelden verwenden, variieren die Zugriffsebenen des Benutzers auf der Citrix ADC Appliance je nach verwendetem Gerät. Das Gateway kann unterschiedliche Authentifizierungsanforderungen erfüllen.
3. **Authentifizierung auf der Grundlage der Gruppenmitgliedschaft.** Einige Organisationen beziehen Benutzereigenschaften von AD-Servern, um Authentifizierungsanforderungen zu ermitteln. Die Authentifizierungsanforderungen können für einzelne Benutzer variiert werden.
4. **Kofaktoren für die Authentifizierung.** Manchmal werden verschiedene Paare von Authentifizierungsrichtlinien verwendet, um verschiedene Benutzersätze zu authentifizieren. Die Bereitstellung von Paarrichtlinien erhöht die effektive Authentifizierung Abhängige Richtlinien können aus einem Fluss erstellt werden. Auf diese Weise werden unabhängige Richtlinien zu eigenen Abläufen, die die Effizienz erhöhen und die Komplexität verringern.

### Behandlung der Antwort auf Authentifizierung

Die Citrix Gateway Callback-Register verarbeiten Authentifizierungsantworten. AAAD-Antworten (Authentication Daemon) und Erfolgs-/Fehler-/Dialogcodes werden an das Rückruf-Handle eingespeist. Die Erfolg/Misserfolg/Fehler-/Dialogcodes weisen Gateway an, die entsprechenden Maßnahmen zu ergreifen.

### Client-Support

In der folgenden Tabelle werden die Konfigurationsdetails beschrieben.

| Client | nFactor Unterstützung | Bindepunkt für Authentifizierungsrichtlinien | EPA |
|---|---|---|---|
| Browser | Ja | Authentifizierung | Ja |
| Citrix Workspace-App | Ja | VPN | Ja |
| Gateway Plug-In | Ja | VPN | Ja |

**Hinweis:**

- Die Citrix Workspace-App unterstützt die nFactor-Authentifizierung für die unterstützten Betriebssysteme aus den folgenden aufgelisteten Versionen.
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5: Unterstützt durch Store Web
  - Chrome: Unterstützt durch Store Web

### Konfiguration der Befehlszeile

Der virtuelle Gateway-Server benötigt einen virtuellen Authentifizierungsserver, der als Attribut benannt ist. Der Name des virtuellen Servers als Attribut ist die einzige Konfiguration, die für dieses Modell erforderlich ist.

```
add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
<!--NeedCopy-->
```

Der AuthNvsName ist der Name des virtuellen Authentifizierungsservers. Der virtuelle AuthNvsName-Server muss mit erweiterten Authentifizierungsrichtlinien konfiguriert werden und wird für die nFactor-Authentifizierung verwendet.

```
add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of
   -profile>
set vpn vserver <name> -authnProfile <name-of-profile>
<!--NeedCopy-->
```

Wobei AuthnProfile das zuvor erstellte Authentifizierungsprofil ist.

### Interop-Herausforderungen

Die meisten Legacy Gateway-Clients, zusätzlich zu den RFWeb-Clients, sind den von Gateway gesendeten Antworten nachempfunden. Beispielsweise wird für viele Clients eine 302-Antwort auf /vpn/index.html erwartet. Diese Clients sind auch auf verschiedene Gateway-Cookies wie ““pwcount, “NSC_CERT angewiesen. “

### Endpunktanalyse (EPA)

EPA in nFactor wird für das Citrix ADC-Authentifizierungs-, Autorisierungs- und Überwachungsmodul nicht unterstützt. Daher führt der virtuelle Citrix Gateway-Server EPA durch. Nach EPA werden die Anmeldeinformationen mithilfe der zuvor erwähnten API an den virtuellen Authentifizierungsserver gesendet. Sobald die Authentifizierung abgeschlossen ist, fährt Gateway mit dem Nachauthentifizierungsprozess fort und richtet die Benutzersitzung ein.

### Überlegungen zur Fehlkonfiguration

Der Gateway-Client sendet die Benutzeranmeldeinformationen nur einmal. Gateway erhält entweder eine oder zwei Anmeldeinformationen vom Client mit der Anmeldeanforderung. Im Legacy-Modus gibt es maximal zwei Faktoren. Die erhaltenen Kennwörter werden für diese Faktoren verwendet. Mit nFactor ist die Anzahl der konfigurierbaren Faktoren jedoch praktisch unbegrenzt. Die vom Gateway-Client erhaltenen Kennwörter werden (gemäß Konfiguration) für konfigurierte Faktoren wiederverwendet. Es muss darauf geachtet werden, dass das Einmalkennwort (OTP) nicht mehrfach wiederverwendet werden darf. Ebenso muss ein Administrator sicherstellen, dass das bei einem Faktor wiederverwendete Kennwort tatsächlich auf diesen Faktor anwendbar ist.

### Definieren von Citrix Clients

Die Konfigurationsoption hilft Citrix ADC dabei, Browserclients im Vergleich zu Thick-Clients wie Receiver zu ermitteln.

Ein Mustersatz, ns_vpn_client_useragents, wird für den Administrator bereitgestellt, um Muster für alle Citrix Clients zu konfigurieren.

Binden Sie die Zeichenfolge "Citrix Receiver"an das `patset` oben, um alle Citrix Clients zu ignorieren, die "Citrix Receiver"im User-Agent haben.

### Einschränkung von nFactor für Gateway

nFactor für die Gateway-Authentifizierung tritt nicht ein, wenn die folgenden Bedingungen erfüllt sind.

1. authnProfile ist nicht auf Citrix Gateway eingestellt.
2. Erweiterte Authentifizierungsrichtlinien sind nicht an den virtuellen Authentifizierungsserver gebunden, und derselbe virtuelle Authentifizierungsserver wird in `authnProfile` erwähnt.
3. Die User-Agent-Zeichenfolge in der HTTP-Anforderung entspricht den in `patset` ns_vpn_client_useragents konfigurierten User-Agents.

Wenn diese Bedingungen nicht erfüllt sind, wird die klassische Authentifizierungsrichtlinie verwendet, die an Gateway gebunden ist.

Wenn ein User-Agent oder ein Teil davon an das zuvor erwähnte `patset` gebunden ist, nehmen Anfragen von diesen Benutzeragenten nicht am nFactor-Flow teil. Der folgende Befehl schränkt beispielsweise die Konfiguration für alle Browser ein (vorausgesetzt, alle Browser enthalten "Mozilla"in der User-Agent-Zeichenfolge):

```
bind patset ns_vpn_client_useragents Mozilla
<!--NeedCopy-->
```

### LoginSchema

LoginSchema ist eine logische Darstellung des Anmeldeformulars. Die XML-Sprache definiert es. Die Syntax von loginSchema entspricht der Common Forms Protocol-Spezifikation von Citrix.

LoginSchema definiert die "Ansicht"des Produkts. Ein Administrator kann eine angepasste Beschreibung, einen Hilfstext usw. des Formulars bereitstellen. Das Anmeldeschema enthält die Beschriftungen des Formulars selbst. Ein Kunde kann die Erfolgs- oder Misserfolgsmeldung übermitteln, die das zu einem bestimmten Zeitpunkt vorgelegte Formular beschreibt.

Verwenden Sie den folgenden Befehl, um ein Anmeldeschema zu konfigurieren.

```
add authentication loginSchema <name> -authenticationSchema <string> [-
    userExpression <string>] [-passwdExpression <string>] [-
    userCredentialIndex <positive_integer>]
```

```
2 [-passwordCredentialIndex <positive_integer>] [-authenticationStrength
     <positive_integer>] [-SSOCredentials ( YES | NO )]
3 <!--NeedCopy-->
```

**Beschreibung des Parameters**

- name - Name für das neue Anmeldeschema. Dies ist ein obligatorisches Argument. Maximale Länge: 127
- authenticationSchema - Name der Datei zum Lesen des Authentifizierungsschemas, die für die Benutzeroberfläche der Anmeldeseite gesendet werden soll. Diese Datei enthält die xml-Definition der Elemente gemäß dem Citrix Forms Authentication Protocol, um das Anmeldeformular rendern zu können. Wenn der Administrator Benutzer nicht zur Eingabe anderer Anmeldeinformationen auffordern möchte, sondern mit zuvor erhaltenen Anmeldeinformationen fortfahren möchte, kann `noschema` als Argument angegeben werden. Dies gilt nur, wenn loginSchemas mit den benutzerdefinierten Faktoren verwendet wird und nicht für den Faktor des virtuellen Servers.

Dies ist ein obligatorisches Argument. Maximale Länge: 255

- userExpression - Ausdruck für die Extraktion von Benutzernamen während der Anmeldung. Dies kann jeder relevante erweiterte Richtlinienausdruck sein. Maximale Länge: 127
- passwdExpression - Ausdruck für die Kennwortextraktion während der Anmeldung. Dies kann jeder relevante erweiterte Richtlinienausdruck sein. Maximale Länge: 127
- userCredentialIndex - Der Index, bei dem der Benutzer den Benutzernamen eingegeben hat, muss in der Sitzung gespeichert werden. Mindestwert: 1, Maximalwert: 16
- PasswordCredentialIndex - Der Index, bei dem der Benutzer das Kennwort eingegeben hat, muss in der Sitzung gespeichert werden. Mindestwert: 1, Maximalwert: 16
- authenticationStrength - Gewicht der aktuellen Authentifizierung Mindestwert: 0, Maximalwert: 65535
- `SSOCredentials` - Diese Option gibt an, ob die Anmeldeinformationen für den aktuellen Faktor die Standardanmeldeinformationen für SSO (SingleSignon) sind. Mögliche Werte: YES, NO. Standardwert: NO

## LoginSchema und nFactor Wissen erforderlich

Vorgefertigte LoginSchema-Dateien sind im folgenden Citrix ADC-Speicherort **/NSConfig/loginSchema/loginSchema/**. Diese vorgefertigten LoginSchema-Dateien dienen gängigen Anwendungsfällen und können bei Bedarf für geringfügige Abweichungen modifiziert werden.

Außerdem benötigen die meisten Ein-Faktor-Anwendungsfälle mit wenigen Anpassungen die Konfiguration des Anmeldeschemas nicht.

Dem Administrator wird empfohlen, in der Dokumentation nach anderen Konfigurationsoptionen zu suchen, mit denen Citrix ADC die Faktoren ermitteln kann. Sobald der Benutzer die Anmeldeinformationen übermittelt hat, kann der Administrator mehr als einen Faktor konfigurieren, um die Authentifizierungsfaktoren flexibel auszuwählen und zu verarbeiten.

### Konfigurieren der Dual-Faktor-Authentifizierung ohne LoginSchema

Citrix ADC bestimmt automatisch die Dual-Faktor-Anforderungen basierend auf der Konfiguration. Sobald der Benutzer diese Anmeldeinformationen vorlegt, kann der Administrator den ersten Satz von Richtlinien auf dem virtuellen Server konfigurieren. Für jede Richtlinie kann ein "NextFactor"als "Passthrough"konfiguriert sein. Ein "Passthrough"bedeutet, dass der Citrix ADC die Anmeldung mit dem vorhandenen Berechtigungssatz verarbeiten muss, ohne an den Benutzer zu gehen. Durch die Verwendung von "Passthrough"-Faktoren kann ein Administrator den Authentifizierungsablauf programmatisch steuern. Administratoren wird empfohlen, die nFactor-Spezifikation oder die Bereitstellungshandbücher für weitere Details zu lesen. Siehe
Multi-Factor (nFactor) -Authentifizierung.

### Benutzername und Kennwortausdrücke

Um die Anmeldeinformationen zu verarbeiten, muss der Administrator das LoginSchema konfigurieren. Ein-Faktor- oder Dual-Faktor-Anwendungsfälle mit wenigen LoginSchema-Anpassungen benötigen keine angegebene XML-Definition. Das LoginSchema hat andere Eigenschaften wie UserExpression und PasswdExpression, die verwendet werden können, um den Benutzernamen oder das Kennwort zu ändern, das der Benutzer angibt.

Anmeldeschemas sind erweiterte Richtlinienausdrücke und können auch verwendet werden, um die Benutzereingaben zu überschreiben. Dies kann erreicht werden, indem eine Zeichenfolge für Parameter in **-authenticationSchema** angehängt wird, wie im folgenden Beispiel gezeigt.

Im Folgenden finden Sie Beispiele zum Ändern von Benutzereingaben für den Benutzernamen bzw. für das Kennwort.

- Ändern Sie die Benutzereingabe für den Benutzernamen von `username@citrix.com` auf `username@xyz.com`

```
1 add authentication loginSchema user_schema -authenticationSchema
     LoginSchema/DualAuth.xml -userExpression "AAA.LOGIN.USERNAME.
     BEFORE_STR("@").APPEND("@xyz.com")"
2 <!--NeedCopy-->
```

- Stellen Sie sich ein Szenario vor, in dem der Benutzer im ersten Faktor ein Kennwort und einen Passcode als Teil des konfigurierten Anmeldeschemas angibt. Um den vom Benutzer im ersten Faktor bereitgestellten **Passcode** und das **Kennwort** im zweiten Faktor zu verwenden, können Sie das vorhandene Anmeldeschema mithilfe der folgenden Befehle ändern.

```
1 add authentication loginSchema user_schema -authenticationSchema
    LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.
    PASSWORD2"
2 <!--NeedCopy-->
```

```
1 add authentication loginSchema user_schema_second -
    authenticationSchema noschema  -passwdExpression "AAA.LOGIN.
    PASSWORD"
2 <!--NeedCopy-->
```

### Schritte auf hoher Ebene in der nFactor-Konfiguration

Das folgende Diagramm veranschaulicht die Schritte auf hoher Ebene, die bei der Konfiguration von nFactor erforderlich sind.


### GUI-Konfiguration

Die folgenden Themen werden in diesem Abschnitt beschrieben:

- Erstellen Sie einen virtuellen Server

- Erstellen eines virtuellen Authentifizierungsservers
- Erstellen eines Authentifizierungs-CERT-Profils
- Erstellen einer Authentifizierungsrichtlinie
- Einen LDAP-Authentifizierungsserver hinzufügen
- Hinzufügen einer LDAP-Authentifizierungsrichtlinie
- Einen RADIUS-Authentifizierungsserver hinzufügen
- Hinzufügen einer RADIUS-Authentifizierungsrichtlinie
- Erstellen eines Authentifizierungs-Login-Schemas
- Erstellen eines Richtlinienlabels

### Erstellen Sie einen virtuellen Server

1. Navigieren Sie zu **Citrix Gateway -> Virtuelle Server.**
2. Klicken Sie auf die Schaltfläche **Hinzufügen**, um einen virtuellen Gateway-Server zu erstellen.
3. Geben Sie die folgenden Informationen ein und klicken Sie auf **OK**.

| Parametername | Beschreibung des Parameters |
|---|---|
| Geben Sie den Namen des virtuellen Servers ein. | Name für den virtuellen Citrix Gateway-Server. Muss mit einem ASCII-Zeichen oder einem Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), gleich (=) und Bindestrich (-) enthalten. Kann geändert werden, nachdem der virtuelle Server erstellt wurde. Die folgende Anforderung gilt nur für die Citrix ADC CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Server”oder “mein Server”). |
| Geben Sie den IP-Adresstyp für den virtuellen Server ein | Wählen Sie im Dropdownmenü eine Option für IP-Adresse oder nicht adressierbar aus. |

| Parametername | Beschreibung des Parameters |
| --- | --- |
| Geben Sie die IP-Adresse des virtuellen Servers ein. | Eine Internetprotokolladresse (IP-Adresse) ist ein numerisches Etikett, das jedem am Computernetzwerk teilnehmenden Gerät zugewiesen wird, das das Internetprotokoll für die Kommunikation verwendet. |
| Geben Sie die Portnummer für den virtuellen Server ein. | Geben Sie die Portnummer ein. |
| Gib das Authentifizierungsprofil ein. | Authentifizierungsprofilentität auf dem virtuellen Server. Diese Entität kann verwendet werden, um die Authentifizierung auf den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver für die Multi-Faktor (nFactor) -Authentifizierung |
| Geben Sie das RDP-Serverprofil ein. | Name des RDP-Serverprofils, das dem virtuellen Server zugeordnet ist. |
| Geben Sie die maximale Benutzerzahl ein. | Maximale Anzahl gleichzeitiger Benutzersitzungen, die auf diesem virtuellen Server zulässig sind. Die tatsächliche Anzahl der Benutzer, die sich an diesem virtuellen Server anmelden dürfen, hängt von der Gesamtzahl der Benutzerlizenzen ab. |
| Geben Sie die maximalen Anmeldeversuche ein. | Maximale Anzahl von Anmeldeversuchen. |
| Geben Sie das Zeitlimit für fehlgeschlagene Anmeldung ein | Anzahl der Minuten, die ein Konto gesperrt ist, wenn der Benutzer die maximal zulässigen Versuche überschreitet. |
| Rufen Sie das Windows EPA-Plug-In-Upgrade auf. | Option zum Festlegen des Plug-In-Upgrade-Verhaltens für Win. |
| Rufen Sie das Linux EPA-Plug-In-Upgrade auf. | Option zum Festlegen des Plug-In-Upgrade-Verhaltens für Linux. |
| Rufen Sie das MAC EPA-Plug-In-Upgrade auf | Option zum Festlegen des Plug-In-Upgrade-Verhaltens für Mac. |
| Einmal anmelden | Diese Option aktiviert/deaktiviert Seamless SSO für diesen virtuellen Server. |

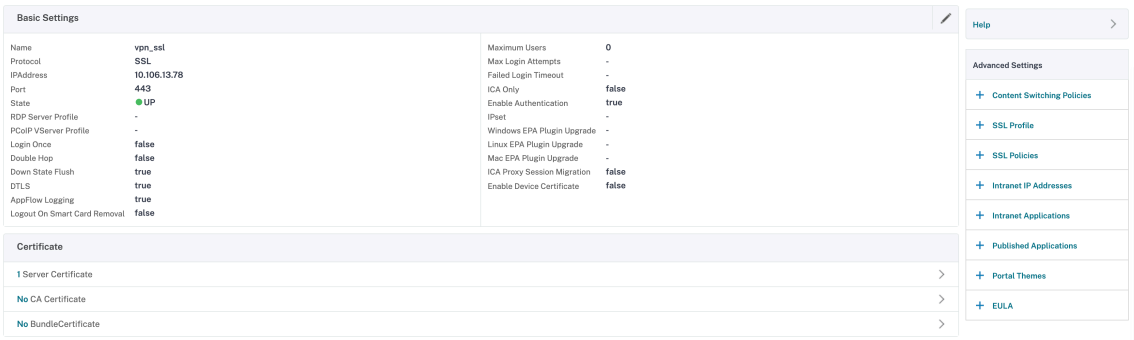
| Parametername | Beschreibung des Parameters |
| --- | --- |
| Nur ICA | Bei Einstellung auf ON bedeutet dies den Basismodus, in dem sich der Benutzer entweder mit der Citrix Workspace-App oder einem Browser anmelden und Zugriff auf die veröffentlichten Apps erhalten kann, die in der Citrix Virtual Apps and Desktops-Umgebung konfiguriert wurden, auf die der Parameter `Wihome` hinweist. Benutzer dürfen keine Verbindung über das Citrix Gateway-Plug-In herstellen, und Endpunktscans können nicht konfiguriert werden. Die Anzahl der Benutzer, die sich anmelden und auf die Apps zugreifen können, ist in diesem Modus nicht durch die Lizenz begrenzt. - Bei Einstellung auf OFF bedeutet dies den SmartAccess-Modus, in dem sich der Benutzer entweder mit der Citrix Workspace-App, einem Browser oder einem Citrix Gateway-Plug-in anmelden kann. Der Administrator kann Endpunkt-Scans so konfigurieren, dass sie auf den Client-Systemen ausgeführt werden, und dann die Ergebnisse verwenden, um den Zugriff auf die veröffentlichten Apps zu steuern. In diesem Modus kann der Client in anderen Clientmodi, nämlich VPN und clientloses VPN, eine Verbindung zum Gateway herstellen. Die Anzahl der Benutzer, die sich anmelden und auf die Ressourcen zugreifen können, ist durch die CCU-Lizenzen in diesem Modus begrenzt. |
| Authentifizierung aktivieren | Erfordert Authentifizierung für Benutzer, die sich mit Citrix Gateway verbinden. |

| Parametername | Beschreibung des Parameters |
| --- | --- |
| Doppel Hop | Verwenden Sie das Citrix Gateway-Gerät in einer Double-Hop-Konfiguration. Eine Double-Hop-Bereitstellung bietet eine zusätzliche Sicherheitsebene für das interne Netzwerk, indem drei Firewalls verwendet werden, um die DMZ in zwei Stufen zu unterteilen. Eine solche Bereitstellung kann eine Appliance in der DMZ und eine Appliance im sicheren Netzwerk haben. |
| State Flush nach unten | Schließen Sie bestehende Verbindungen, wenn der virtuelle Server als DOWN markiert ist, was bedeutet, dass der Server möglicherweise eine Zeitüberschreitung hat. Das Trennen vorhandener Verbindungen befreit Ressourcen und beschleunigt in bestimmten Fällen die Wiederherstellung überlasteter Lastausgleichseinrichtungen. Aktivieren Sie diese Einstellung auf Servern, auf denen die Verbindungen sicher geschlossen werden können, wenn sie als DOWN markiert sind. Aktivieren Sie nicht DOWN State Flush auf Servern, die ihre Transaktionen abschließen müssen. |
| DTLS | Diese Option start/stoppt den Turn Service auf dem virtuellen Server |
| AppFlow-Protokollierung | Protokollieren Sie AppFlow-Datensätze, die standardmäßige NetFlow- oder IPFIX-Informationen enthalten, wie Zeitstempel für den Beginn und das Ende eines Flusses, Paketanzahl und Byteanzahl. Protokollieren Sie auch Datensätze, die Informationen auf Anwendungsebene enthalten, wie HTTP-Webadressen, HTTP-Anforderungsmethoden und Antwortstatuscodes, Serverreaktionszeit und Latenz. |

| Parametername | Beschreibung des Parameters |
| --- | --- |
| ICA-Proxysitzungsmigration | Diese Option bestimmt, ob eine vorhandene ICA-Proxysitzung übertragen wird, wenn sich der Benutzer von einem anderen Gerät aus anmeldet. |
| Status | Der aktuelle Status des virtuellen Servers, wie UP, DOWN, BUSY usw. |
| Gerätezertifikat aktivieren | Zeigt an, ob die Gerätezertifikatsprüfung als Teil von EPA ein- oder ausgeschaltet ist. |




4. Wählen Sie den Abschnitt **Kein Serverzertifikat** auf der Seite.
5. Klicken Sie auf **>**, um das Serverzertifikat auszuwählen.
6. Wählen Sie das SSL-Zertifikat aus und klicken Sie auf die Schaltfläche **Auswählen**.
7. Klicken Sie auf **Bind**.
8. Wenn Sie eine Warnung über **Keine brauchbaren Chiffren** sehen, klicken Sie auf **OK**
9. Klicken Sie auf **Weiter**.
10. Klicken Sie im Abschnitt Authentifizierung oben rechts auf das **+-Symbol**.

## Erstellen Sie einen virtuellen Authentifizierungsserver

1. Navigieren Sie zu **Sicherheit -> Citrix ADC AAA —Anwendungsverkehr -> Virtuelle Server.**
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Füllen Sie die folgenden Grundeinstellungen aus, um den virtuellen Authentifizierungsserver zu erstellen.

   **Hinweis:** Das * -Zeichen rechts neben dem Einstellungsnamen weist auf Pflichtfelder hin.

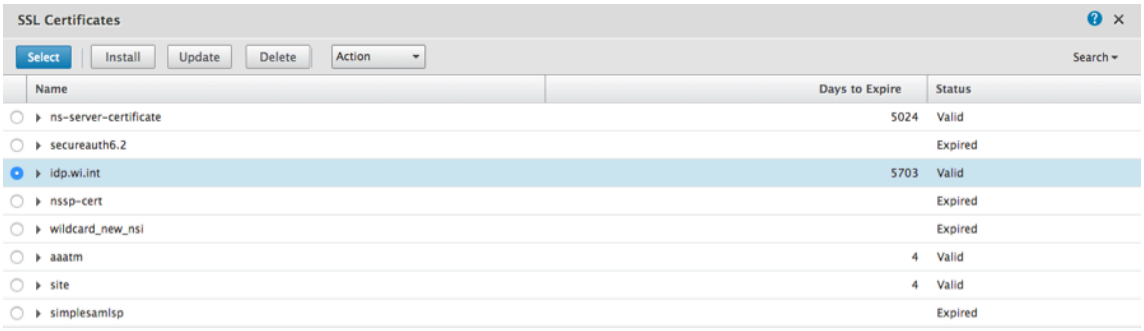
   - Geben Sie den **Namen** für den neuen virtuellen Authentifizierungsserver ein.

- Geben Sie den **IP-Adresstyp ein**. Der IP-Adresstyp kann als nicht adressierbar konfiguriert werden.
- Geben Sie die **IP-Adresse**ein. Die IP-Adresse kann Null sein.
- Geben Sie den **Protokolltyp** des virtuellen Authentifizierungsservers ein.
- Geben Sie den **TCP-Port** ein, auf dem der virtuelle Server Verbindungen akzeptiert.
- Geben Sie die **Domäne** des Authentifizierungs-Cookies ein, das vom virtuellen Authentifizierungsserver gesetzt wurde.

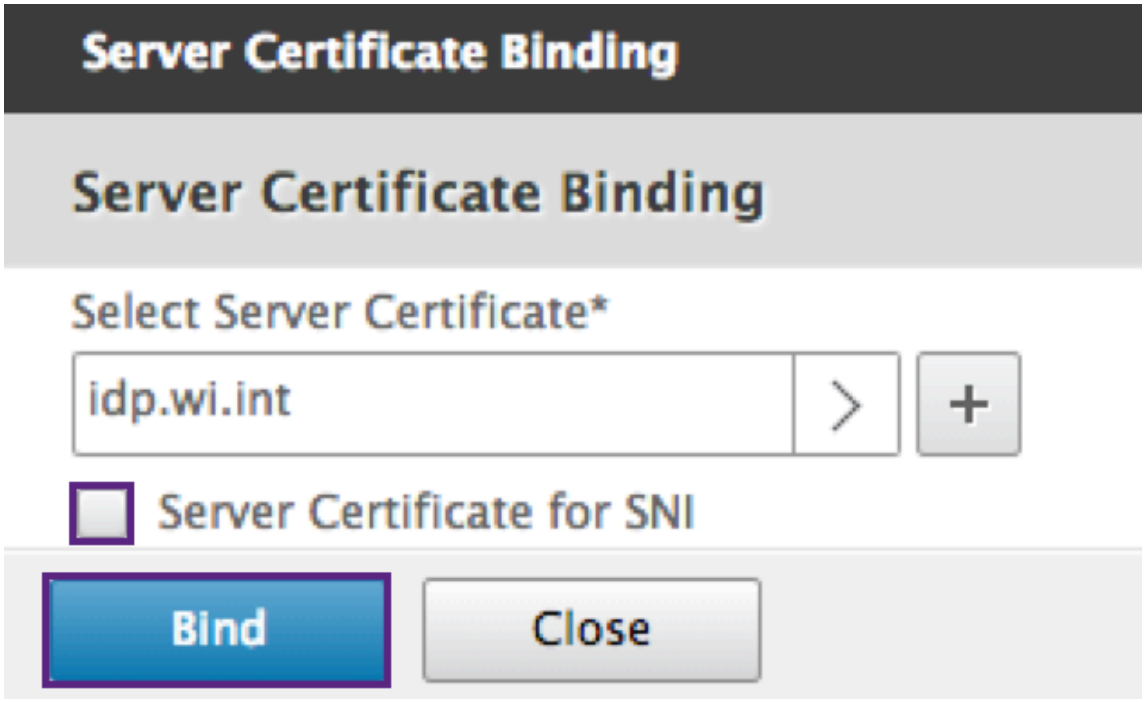
4. Klicken Sie auf **OK**.
5. Klicken Sie auf das **Kein Serverzertifikat**.
6. Wählen Sie das gewünschte Serverzertifikat aus der Liste aus.
7. Wählen Sie das gewünschte SSL-Zertifikat aus und klicken Sie auf die Schaltfläche **Auswählen**.

   **Hinweis**: Der virtuelle Authentifizierungsserver benötigt kein an ihn gebundenes Zertifikat.




8. Konfigurieren Sie die **Serverzertifikatbindung**
   - Aktivieren Sie das Kästchen **Serverzertifikat für SNI**, um einen oder mehrere Cert-Schlüssel zu binden, die für die SNI-Verarbeitung verwendet werden.
   - Klicken Sie auf die Schaltfläche **Binden**.




### Erstellen eines CERT-Authentifizierungsprofils

1. Navigieren Sie zu **Sicherheit -> Citrix ADC AAA —Anwendungsverkehr -> Richtlinien -> Authentifizierung -> Grundlegende Richtlinien -> CERT.**
2. Wählen Sie die Registerkarte Profile und dann **Hinzufügen**.
3. Füllen Sie die folgenden Felder aus, um das Authentifizierungs-CERT-Profil zu erstellen. Das * -Zeichen rechts neben dem Einstellungsnamen weist auf Pflichtfelder hin.
   - **Name** —Name für das Serverprofil für die Clientzertifikat Authentifizierung (Aktion).
   - **Zwei Faktoren** —In diesem Fall ist die Zwei-Faktor-Authentifizierungsoption NOOP.
   - **Benutzernamenfeld** —geben Sie das Client-Cert-Feld ein, aus dem der Benutzername extrahiert wird. Muss entweder auf “”Betreff “”oder “”Aussteller “”festgelegt sein (beide Sätze von doppelten Anführungszeichen enthalten).
   - **Gruppennamenfeld** - geben Sie das Client-Cert-Feld ein, aus dem die Gruppe extrahiert wird. Muss entweder auf “”Betreff “”oder “”Aussteller “”festgelegt sein (beide Sätze von doppelten Anführungszeichen enthalten).
   - **Standardauthentifizierungsgruppe** - Dies ist die Standardgruppe, die ausgewählt wird, wenn die Authentifizierung zusätzlich zu den extrahierten Gruppen erfolgreich ist.
4. Klicken Sie auf **Erstellen**.

### Erstellen einer Authentifizierungsrichtlinie

> **Hinweis**
>
> Wenn Sie eine Richtlinie für den ersten Faktor mit einer Richtlinienregel mithilfe von AAA.Login konfigurieren, muss der folgende Ausdruck mit der OR-Bedingung konfiguriert werden, damit die Citrix Workspace-App die nFactor-Bereitstellung unterstützt.
>
> ```
> || HTTP.REQ.URL.CONTAINS("/cgi/authenticate")
> ```

1. Navigieren Sie zu **Sicherheit -> Citrix ADC AAA —Anwendungsverkehr -> Richtlinien -> Authentifizierung -> Erweiterte Richtlinien -> Richtlinie.**
2. Wähle den Button "**Hinzufügen** "
3. Füllen Sie die folgenden Informationen aus, um eine Authentifizierungsrichtlinie zu erstellen. Das * -Zeichen rechts neben dem Einstellungsnamen weist auf Pflichtfelder hin.

   a) **Name** —geben Sie den Namen für die Richtlinie für die erweiterte AUTHENTIFIZIERUNG ein. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestriche (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann nicht geändert werden, nachdem die Authentifizierungsrichtlinie erstellt wurde.

   Die folgende Anforderung gilt nur für die Citrix ADC CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. "meine Authentifizierungsrichtlinie"oder "meine Authentifizierungsrichtlinie").

   b) **Aktionstyp** - geben Sie den Typ der Authentifizierungsaktion ein.

   c) **Aktion** - geben Sie den Namen der Authentifizierungsaktion ein, die ausgeführt werden soll, wenn die Richtlinie übereinstimmt.

   d) **Aktion protokollieren** - geben Sie den Namen der Nachrichtenprotokollaktion ein, die verwendet werden soll, wenn eine Anforderung dieser Richtlinie entspricht.

   e) **Ausdruck** - Geben Sie den Namen der benannten Citrix ADC-Regel oder einen Standardsyntaxausdruck ein, mit dem die Richtlinie bestimmt, ob versucht wird, den Benutzer beim AUTHENTICATION-Server zu authentifizieren.

   f) **Kommentare** —geben Sie Kommentare ein, um Informationen zu dieser Richtlinie aufzubewahren.
4. Klicken Sie auf **Erstellen**.

### Einen LDAP-Authentifizierungsserver hinzufügen

1. Navigieren Sie zu **Sicherheit -> Citrix ADC AAA —Anwendungsverkehr -> Richtlinien -> Authentifizierung -> Grundlegende Richtlinien -> LDAP.**

2. Fügen Sie einen LDAP-Server hinzu, indem Sie die Registerkarte **Server** auswählen und die Schaltfläche **Hinzufügen** auswählen.

### Hinzufügen einer LDAP-Authentifizierungsrichtlinie

1. Gehen Sie zu **Sicherheit > Citrix ADC AAA —Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie hinzuzufügen.
3. Füllen Sie die folgenden Informationen aus, um eine Authentifizierungsrichtlinie zu erstellen. Das * -Zeichen rechts neben dem Einstellungsnamen weist auf Pflichtfelder hin.

   a) **Name —Name** für die erweiterte AUTHENTIFIZIERUNGS-Richtlinie.
   Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestriche (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann nicht geändert werden, nachdem die Authentifizierungsrichtlinie erstellt wurde.

   Die folgende Anforderung gilt nur für die Citrix ADC CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Authentifizierungsrichtlinie”oder “meine Authentifizierungsrichtlinie”).

   b) **Aktionstyp** - Typ der Authentifizierungsaktion.

   c) **Aktion** - Name der Authentifizierungsaktion, die ausgeführt werden soll, wenn die Richtlinie übereinstimmt.

   d) **Aktion protokollieren** - Name der zu verwendenden Nachrichtenprotokollaktion, wenn eine Anforderung mit dieser Richtlinie übereinstimmt.

   e) **Ausdruck** - Name der benannten Citrix ADC-Regel oder eines Standardsyntaxausdrucks, mit dem die Richtlinie bestimmt, ob versucht wird, den Benutzer beim AUTHENTICATION-Server zu authentifizieren.

   f) **Kommentare** - Kommentare zur Aufbewahrung von Informationen zu dieser Richtlinie.
4. Klicken Sie auf **Erstellen.**

### Einen RADIUS-Authentifizierungsserver hinzufügen

1. Navigieren Sie zu **Sicherheit > Citrix ADC AAA —Anwendungsverkehr > Richtlinien Authentifizierung > Grundlegende Richtlinien > RADIUS**.
2. Um einen Server hinzuzufügen, wählen Sie die Registerkarte **Server** und wählen Sie die Schaltfläche **Hinzufügen**.

3. Geben Sie Folgendes ein, um einen Authentifizierungs-RADIUS-Server zu erstellen. Das * -Zeichen rechts neben dem Einstellungsnamen weist auf Pflichtfelder hin.

   a) Geben Sie einen **Namen** für die RADIUS-Aktion ein.

   b) Geben Sie den **Servernamen** oder die **Server-IP-Adresse** ein, die dem RADIUS-Server zugewiesen sind.

   c) Geben Sie die **Portnummer** ein, auf der der RADIUS-Server auf Verbindungen lauscht.

   d) Geben Sie den **Timeout-Wert** in wenigen Sekunden ein. Die Citrix ADC Appliance wartet auf eine Antwort vom RADIUS-Server, bis der konfigurierte Timeout-Wert abläuft.

   e) Geben Sie den **geheimen Schlüssel** ein, der zwischen dem RADIUS-Server und der Citrix ADC Appliance gemeinsam genutzt wird. Der geheime Schlüssel ist erforderlich, damit die Citrix ADC Appliance mit dem RADIUS-Server kommunizieren kann.

   f) **Bestätige den geheimen Schlüssel**.

4. Klicken Sie auf **Erstellen.**

### Hinzufügen einer RADIUS-Authentifizierungsrichtlinie

1. Navigieren Sie zu **Sicherheit > Citrix ADC AAA —Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie.**
2. Klicke auf **Hinzufügen**, um eine Authentifizierungsrichtlinie zu erstellen.
3. Füllen Sie die folgenden Informationen aus, um eine Authentifizierungsrichtlinie zu erstellen. Das * -Zeichen rechts neben dem Einstellungsnamen weist auf Pflichtfelder hin.

   a) **Name —Name** für die erweiterte AUTHENTIFIZIERUNGS-Richtlinie.
   Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestriche (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann nicht geändert werden, nachdem die AUTHENTICATION Richtlinie erstellt wurde.

   Die folgende Anforderung gilt nur für die Citrix ADC CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Authentifizierungsrichtlinie”oder “meine Authentifizierungsrichtlinie”).

   a) **Aktionstyp** —Typ der Authentifizierungsaktion.

   b) **Aktion** - Name der Authentifizierungsaktion, die ausgeführt werden soll, wenn die Richtlinie übereinstimmt.

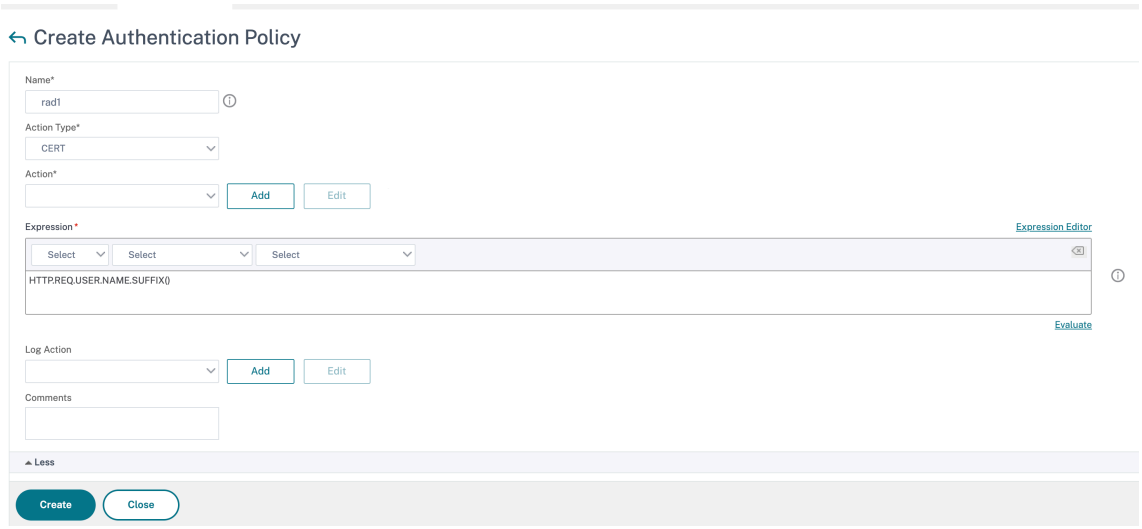
   c) **Aktion protokollieren** —Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anfrage dieser Richtlinie entspricht.

d) **Ausdruck** - Name der benannten Citrix ADC-Regel oder eines Standardsyntaxausdrucks, mit dem die Richtlinie bestimmt, ob versucht wird, den Benutzer beim AUTHENTICATION-Server zu authentifizieren.

e) **Kommentare** —Alle Kommentare zur Aufbewahrung von Informationen zu dieser Richtlinie.

4. Klicken Sie auf **OK.** Die von Ihnen erstellte Authentifizierungsrichtlinie ist in der Liste der Richtlinien aufgeführt.




## Erstellen eines Authentifizierungs-Login-Schemas

1. Navigieren Sie zu **Sicherheit > Citrix ADC AAA —Anwendungsverkehr > Anmeldeschema.**
2. Wählen Sie die Registerkarte Profile und klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Füllen Sie die folgenden Felder aus, um ein Authentifizierungs-Login-Schema zu erstellen

a) **Name** eingeben —Name für das neue Anmeldeschema.

b) Enter **Authentication Schema** - Name der Datei zum Lesen des Authentifizierungsschemas, das für die Benutzeroberfläche der Anmeldeseite gesendet werden soll. Diese Datei muss die XML-Definition der Elemente gemäß dem Citrix Forms Authentication Protocol enthalten, um ein Anmeldeformular rendern zu können. Wenn ein Administrator Benutzer nicht zur Eingabe weiterer Anmeldeinformationen auffordern möchte, sondern mit zuvor erhaltenen Anmeldeinformationen fortfahren möchte, kann`noschema`""als Argument angegeben werden. Dies gilt nur für LoginSchemas, die mit benutzerdefinierten Faktoren verwendet werden, und nicht für den Faktor des virtuellen Servers

c) **Benutzerausdruck** eingeben - Ausdruck für die Extraktion des Benutzernamens während der Anmeldung

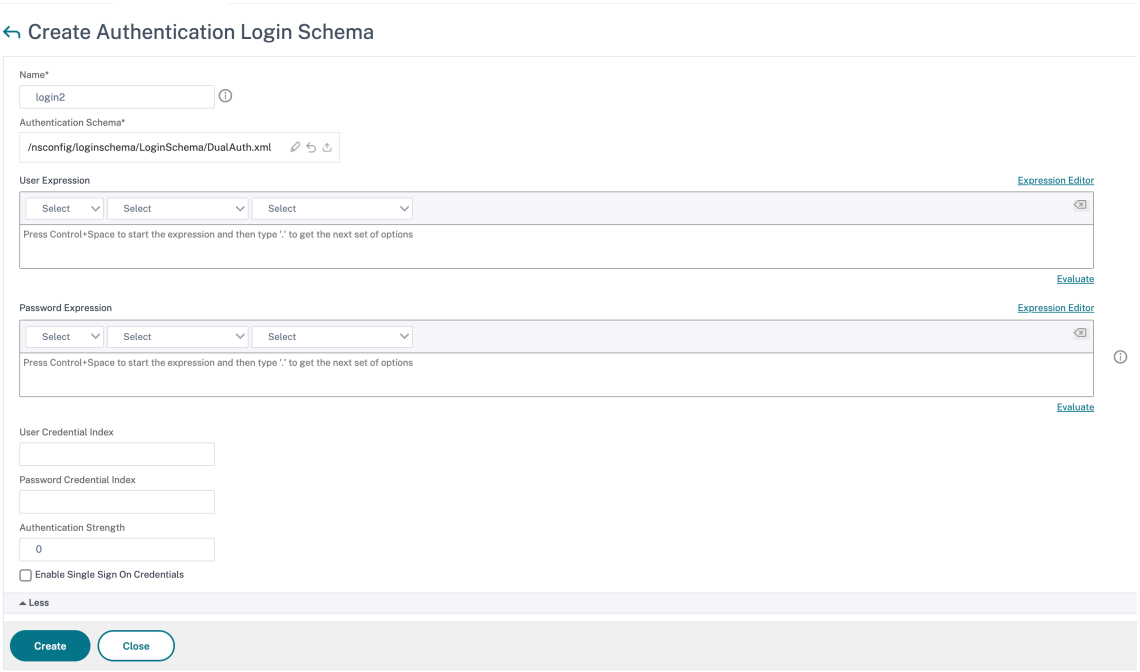
d) Enter **Password Expression** - Ausdruck für Kennwortextraktion während der Anmeldung

e) Geben Sie den **Benutzeranmeldeinformationsindex** ein - Ein Index, bei dem der vom Benutzer eingegebene Benutzername in der Sitzung gespeichert wird.

f) Enter **Password Credential Index** - Ein Index, bei dem das vom Benutzer eingegebene Kennwort in der Sitzung gespeichert werden muss.

g) Geben Sie die **Authentifizierungsstärke** ein - Gewicht der aktuellen Authentifizierung.

4. Klicken Sie auf **Erstellen.** Das Anmeldeschemaprofil, das Sie erstellt haben, muss in der Profilliste des Anmeldeschemas erscheinen.



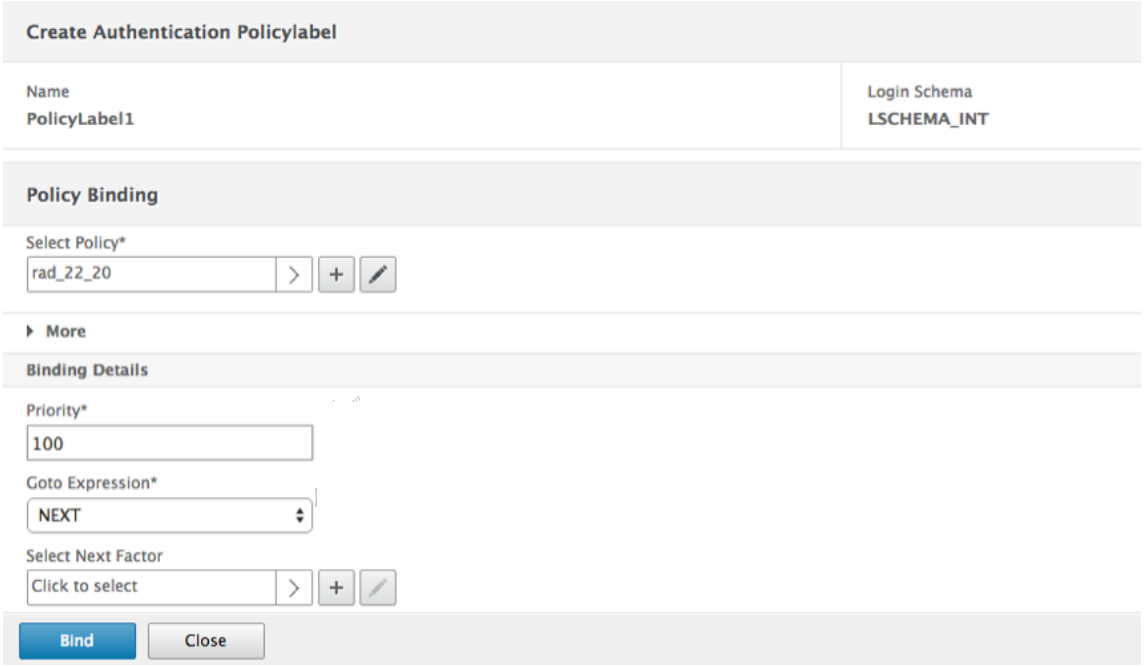

## Erstellen einer Policy Label

Ein Policy Label gibt die Authentifizierungsrichtlinien für einen bestimmten Faktor an. Jedes Policy Label entspricht einem einzelnen Faktor. Das Policy Label gibt das Anmeldeformular an, das dem Benutzer vorgelegt werden muss. Das Policy Label muss als nächster Faktor einer Authentifizierungsrichtlinie oder einer anderen Authentifizierungsrichtlinienbezeichnung gebunden sein. In der Regel enthält ein Policy Label Authentifizierungsrichtlinien für einen bestimmten Authentifizierungsmechanismus. Sie können jedoch auch ein Policy Label haben, das Authentifizierungsrichtlinien für verschiedene Authentifizierungsmechanismen enthält.

1. Navigieren Sie zu **Sicherheit > Citrix ADC AAA —Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinienbezeichnung.**
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Füllen Sie die folgenden Felder aus, um ein Authentifizierungsrichtlinienlabel zu erstellen:
   a) Geben Sie den **Namen** für die neue Bezeichnung der Authentifizierungsrichtlinie ein.
   b) Geben Sie das mit der Bezeichnung der Authentifizierungsrichtlinie verknüpfte **Login-Sch** ein.
   c) Klicken Sie auf **Weiter**.
4. **Wählen Sie eine Richtlinie** aus dem Dropdownmenü aus.
5. Wählen Sie die gewünschte **Authentifizierungsrichtlinie** und klicken Sie auf die Schaltfläche **Auswählen**.
6. Füllen Sie die folgenden Felder aus:
   a) Geben Sie die **Priorität** der Policy-Bindung ein.
   b) Geben Sie den **Gehe zu Ausdruck** ein —der Ausdruck gibt die Priorität der nächsten Richtlinie an, die ausgewertet wird, wenn die aktuelle Richtlinienregel mit TRUE ausgewertet wird.




7. Wählen Sie die gewünschte Authentifizierungsrichtlinie aus und klicken Sie auf die Schaltfläche **Auswählen**.
8. Klicken Sie auf die Schaltfläche **Binden**.
9. Klicken Sie auf **Fertig**.
10. Überprüfen Sie das Label der Authentifizierungsrichtlinie

## Re-Captcha-Konfiguration für die nFactor-Authentifizierung

Ab Citrix ADC Release 12.1 Build 50.x unterstützt Citrix Gateway eine neue erstklassige Aktion 'CaptchaAction', die die Captcha-Konfiguration vereinfacht. Da Captcha eine erstklassige Aktion ist, kann es ein eigener Faktor sein. Sie können Captcha an beliebiger Stelle im nFactor-Flow injizieren.

Zuvor mussten Sie benutzerdefinierte WebAuth Richtlinien mit Änderungen an der RFWebUI schreiben. Mit der Einführung von CaptchaAction müssen Sie das JavaScript nicht ändern.

> **Wichtig!**
>
> Wenn Captcha zusammen mit Benutzernamen- oder Kennwortfeldern im Schema verwendet wird, ist die Schaltfläche Senden deaktiviert, bis Captcha erreicht ist.

### Captcha-Konfiguration

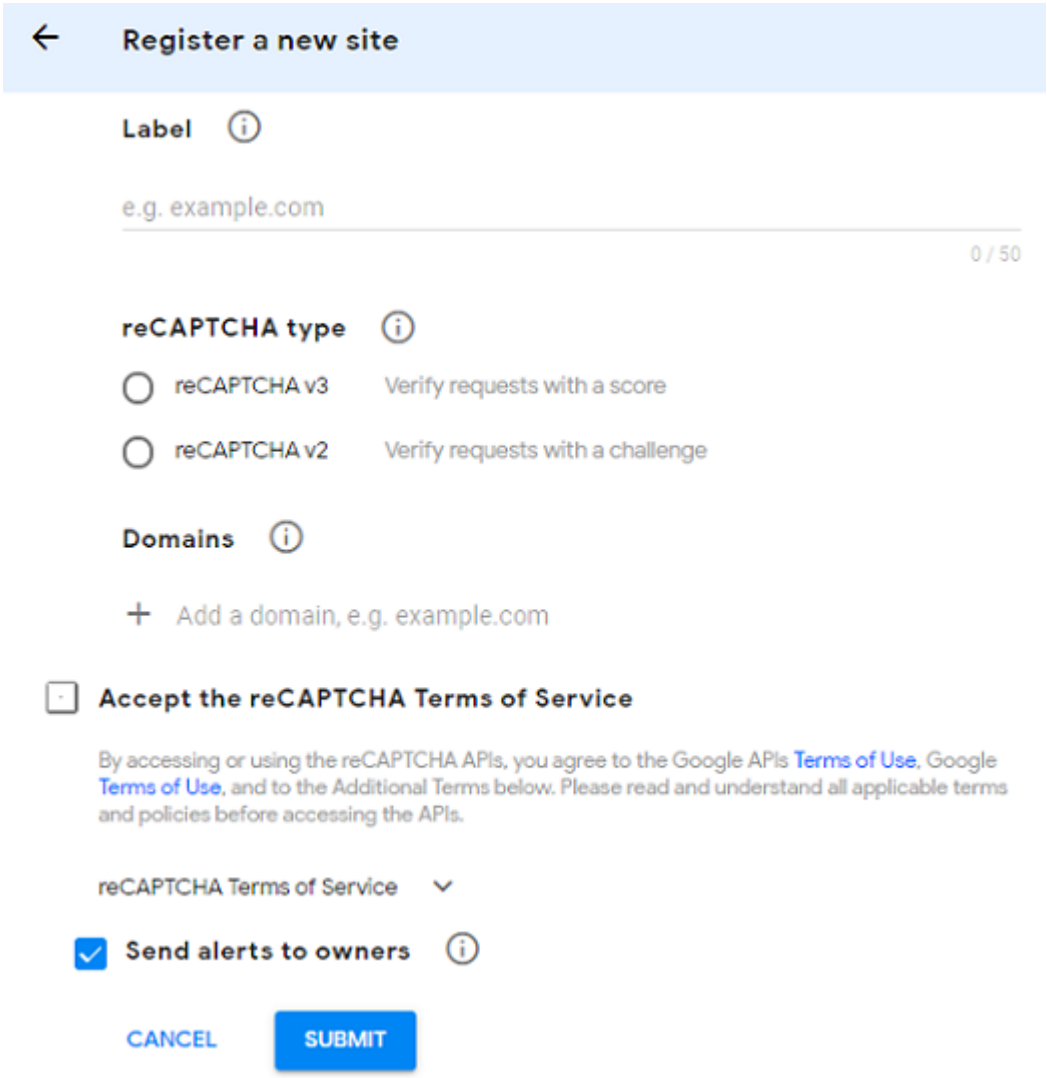
Die Captcha-Konfiguration umfasst zwei Teile.

1. Konfiguration bei Google für die Registrierung von Captcha.
2. Konfiguration auf der Citrix ADC Appliance zur Verwendung von Captcha als Teil des Anmeldeflusses.

**Captcha-Konfiguration bei Google** Registrieren Sie eine Domain für Captcha unter `https://www.google.com/recaptcha/admin#list`.

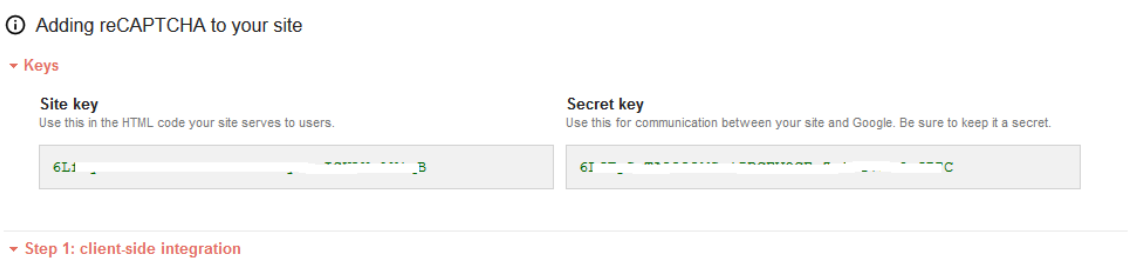
1. Wenn Sie zu dieser Seite navigieren, wird der folgende Bildschirm angezeigt.




> **Hinweis**
>
> Verwenden Sie nur `reCAPTCHA` v2. Unsichtbares `reCAPTCHA` ist immer noch in der Vorschau.

2. Nachdem eine Domain registriert wurde, werden der "SiteKey"und "SecretKey"angezeigt.



> **Hinweis**
>
> Der “SiteKey”und “SecretKey”sind aus Sicherheitsgründen ausgegraut. “SecretKey”muss sicher aufbewahrt werden.

**Captcha-Konfiguration auf der Citrix ADC Appliance** Die Captcha-Konfiguration auf der Citrix ADC Appliance kann in drei Teile unterteilt werden:

- Captcha-Bildschirm anzeigen
- Posten Sie die Captcha-Antwort auf dem Google-Server
- Die LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

**Captcha-Bildschirm anzeigen** Die Anpassung des Anmeldeformulars erfolgt über das Anmeldeschema SingleAuthCaptcha.xml. Diese Anpassung wird auf dem virtuellen Authentifizierungsserver angegeben und zum Rendern des Anmeldeformulars an die Benutzeroberfläche gesendet. Das integrierte Anmeldeschema SingleAuthCaptcha.xml ist im Verzeichnis /nsconfig/loginSchema /LoginSchema auf der Citrix ADC-Appliance.

> **Wichtig!**
>
> - Basierend auf Ihrem Anwendungsfall und verschiedenen Schemas können Sie das vorhandene Schema ändern. Zum Beispiel, wenn Sie nur Captcha-Faktor (ohne Benutzernamen oder Kennwort) oder doppelte Authentifizierung mit Captcha benötigen.
> - Wenn benutzerdefinierte Änderungen vorgenommen werden oder die Datei umbenannt wird, empfiehlt Citrix, alle Anmeldeschemas aus dem Verzeichnis /NSConfig/loginSchema/loginSchema in das übergeordnete Verzeichnis /nsconfig/loginschema zu kopieren.

**So konfigurieren Sie die Anzeige von Captcha mit CLI**

```
1  -  add authentication loginSchema singleauthcaptcha -
       authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml
2
3  -  add authentication loginSchemaPolicy singleauthcaptcha -rule true -
       action singleauthcaptcha
4
5  -  add authentication vserver auth SSL <IP> <Port>
6
7  -  add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to
       -key-file>
8  -  bind ssl vserver auth -certkey vserver-cert
9  -  bind authentication vserver auth -policy singleauthcaptcha -priority
        5 -gotoPriorityExpression END
10 <!--NeedCopy-->
```

**Posten Sie die Captcha-Antwort auf dem Google-Server** Nachdem Sie das Captcha konfiguriert haben, das den Benutzern angezeigt werden muss, veröffentlichen die Administratoren die Konfiguration auf dem Google-Server, um die Captcha-Antwort vom Browser zu überprüfen.

**So überprüfen Sie die Captcha-Antwort vom Browser**

```
1 - add authentication captchaAction myrecaptcha -sitekey <sitekey-
    copied-from-google> -secretkey <secretkey-from-google>
2
3 - add authentication policy myrecaptcha -rule true -action myrecaptcha
4 - bind authentication vserver auth -policy myrecaptcha -priority 1
5 <!--NeedCopy-->
```

Die folgenden Befehle sind erforderlich, um zu konfigurieren, ob AD-Authentifizierung gewünscht ist. Andernfalls können Sie diesen Schritt ignorieren.

```
1 - add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
     636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn
    adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -
    encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
     memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -
    defaultAuthenticationGroup ldapGroup
2
3 - add authenticationpolicy ldap-new -rule true -action ldap-new
4 <!--NeedCopy-->
```

**Die LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)** Die LDAP-Authentifizierung erfolgt nach Captcha, Sie fügen sie dem zweiten Faktor hinzu.

```
1 - add authentication policylabel second-factor
2 - bind authentication policylabel second-factor -policy ldap-new -
    priority 10
3 - bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
4 <!--NeedCopy-->
```

Der Administrator muss entsprechende virtuelle Server hinzufügen, je nachdem, ob der virtuelle Lastausgleichsserver oder das Citrix Gateway-Gerät für den Zugriff verwendet wird. Der Administrator muss den folgenden Befehl konfigurieren, wenn ein virtueller Lastausgleichsserver erforderlich ist:

```
1 add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com`
2 <!--NeedCopy-->
```

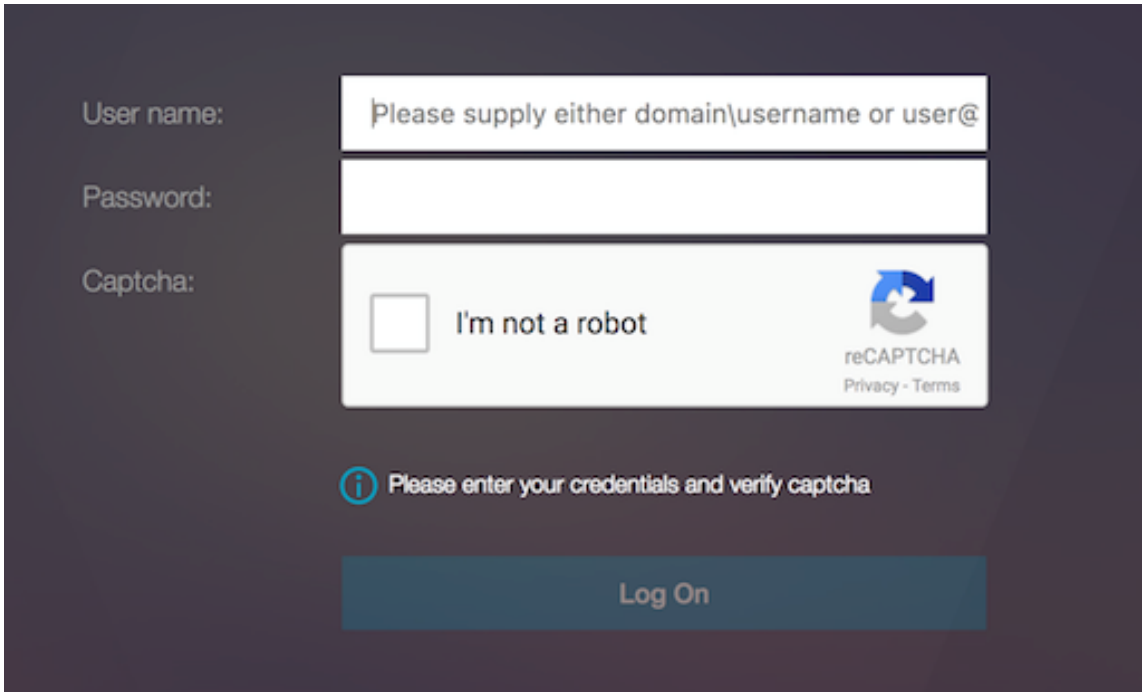
**nssp.aaatm.com** —Löst zum virtuellen Authentifizierungsserver auf.

**Benutzervalidierung von Captcha** Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, sehen Sie sich die vorherigen Bildschirmaufnahmen der Benutzerober-

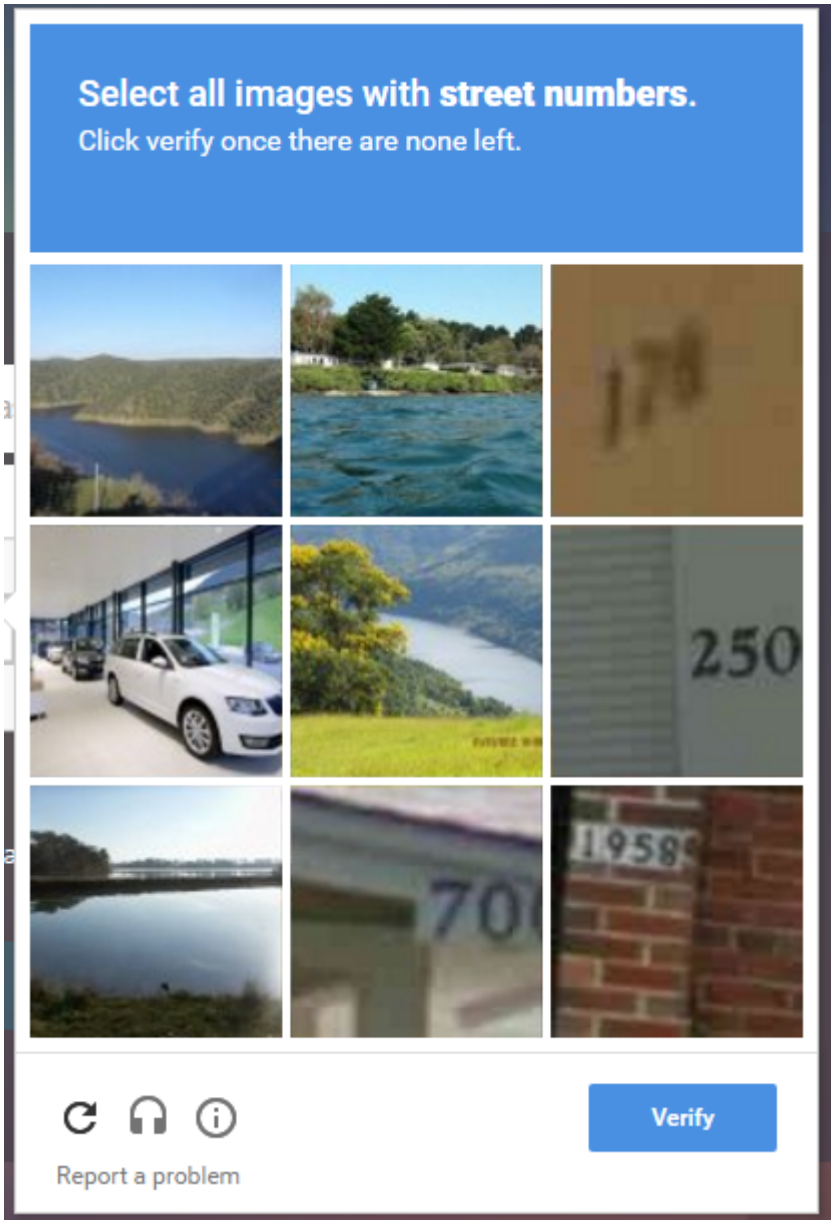
fläche an.

1. Sobald der virtuelle Authentifizierungsserver die Anmeldeseite geladen hat, wird der Anmeldebildschirm angezeigt. Die**Anmeldung ist deaktiviert**, bis Captcha abgeschlossen ist.



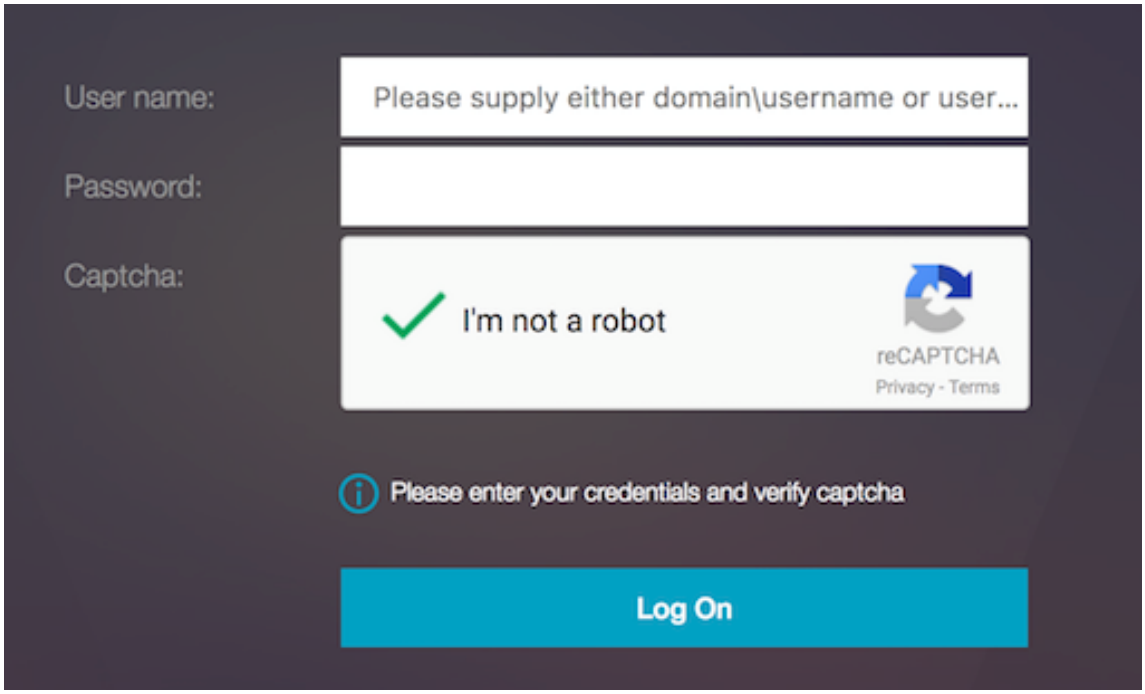

2. Wählen Sie “Ich bin kein Roboter”aus. Das Captcha-Widget wird angezeigt.




3. Sie werden durch eine Reihe von Captcha-Bildern navigiert, bevor die Fertigstellungsseite angezeigt wird.
4. Geben Sie die AD-Anmeldeinformationen ein, aktivieren Sie das Kontrollkästchen **Ich bin kein Roboter** und klicken Sie auf **Anmelden**. Wenn die Authentifizierung erfolgreich ist, werden Sie zur gewünschten Ressource weitergeleitet.

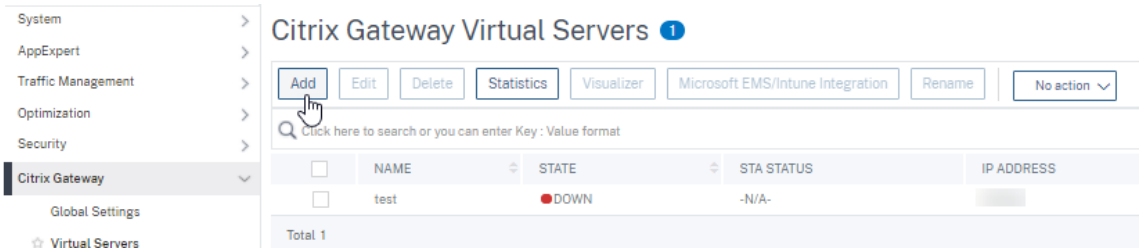



**Hinweis:**

- Wenn Captcha mit AD-Authentifizierung verwendet wird, ist die Schaltfläche Senden für Anmeldeinformationen deaktiviert, bis Captcha abgeschlossen ist.
- Das Captcha geschieht in einem eigenen Faktor. Daher müssen alle nachfolgenden Validierungen wie AD in `nextfactor` von Captcha erfolgen.

### Erstellen Sie einen virtuellen Gateway-Server für die nFactor-Authentifizierung in der Citrix ADC Standard-Lizenz

1. Navigieren Sie zu **Citrix Gateway> Virtuelle Server**.
2. Klicken Sie auf der Seite **Citrix Gateway Virtual Servers** auf **Hinzufügen**.

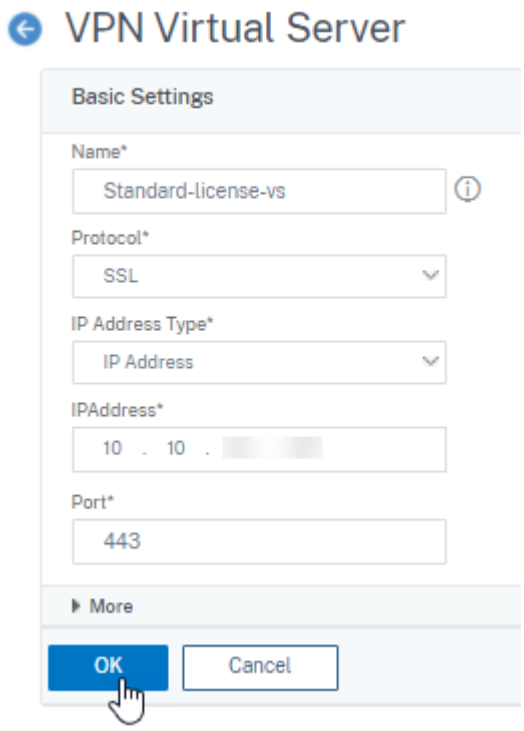



3. Geben Sie auf der Seite **VPN Virtual Server** die folgenden Details ein, klicken Sie auf **OK**und dann auf **Weiter**.

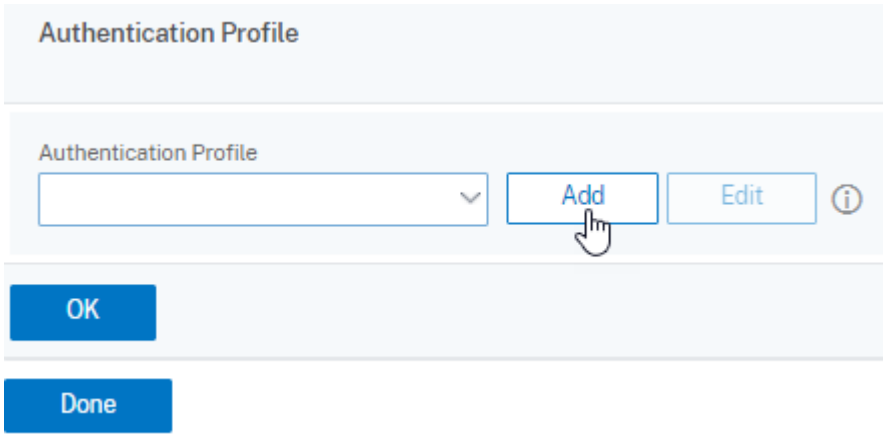
   - Name —Name des virtuellen Citrix Gateway-Servers
   - Protokoll - Wählen Sie **SSL**

- IP-Adresse —IP-Adresse des virtuellen Citrix Gateway-Servers
- Port - Geben Sie 443 ein

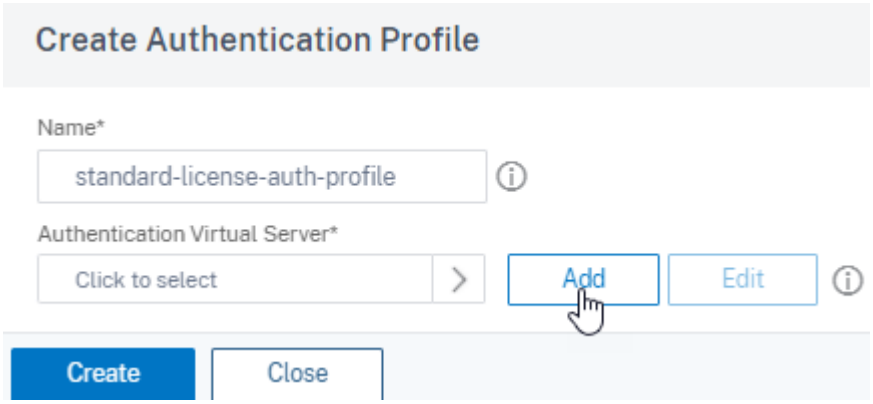



4. Klicken Sie auf der Seite **VPN Virtual Server** auf das Plus-Symbol neben **Authentifizierungsprofil**.
5. Klicken Sie auf **Hinzufügen**, um das Authentifizierungsprofil zu



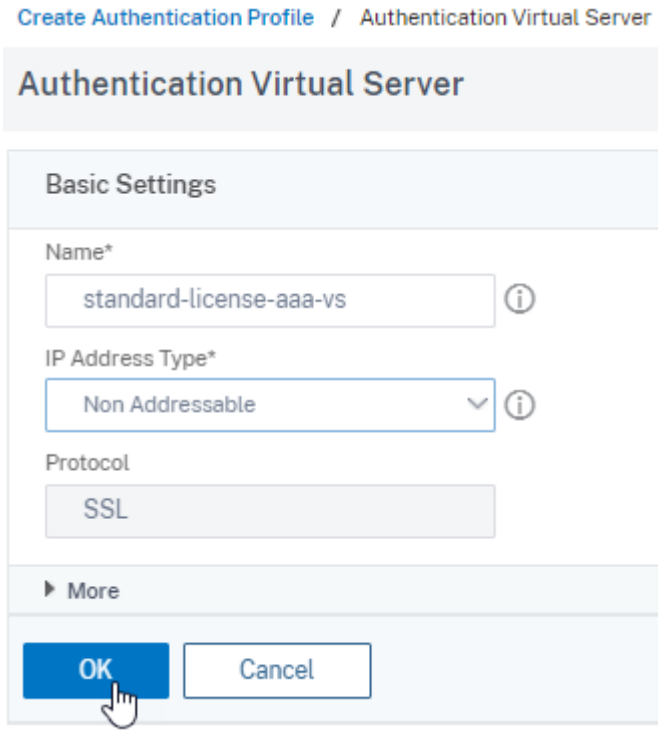

6. Geben Sie einen Namen für das Authentifizierungsprofil ein und klicken Sie auf **Hinzufügen**.




7. Geben Sie auf der Seite **VPN Virtual Server** die folgenden Details ein, klicken Sie auf **OK** und dann auf **Weiter**.

   - Name —Name des virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsservers
   - Protokoll - Wählen Sie **Nicht adressierbar**aus. Nur ein nicht adressierbarer virtueller Authentifizierungs-, Autorisierungs- und Überwachungsserver kann in der Citrix ADC Standard-Lizenz an einen virtuellen Gateway-/VPN-Server gebunden werden.




**Hinweis:**

- In der Citrix ADC Standard-Lizenz entsprechen die Schritte zum Erstellen einer Richtlinie mit der Premium-Lizenz für unterstützte Richtlinientypen.
- Die Citrix ADC Standard-Lizenz unterstützt kein Hinzufügen neuer Anmeldeschemas

> in der nFactor-Konfiguration.

### Referenzen

Ein Beispiel für eine Ende-zu-Ende-nFactor-Konfiguration finden Sie unter Konfigurieren der nFactor-Authentifizierung.

## Unified Gateway Visualizer

March 27, 2024

Der Unified Gateway Visualizer bietet eine visuelle Darstellung der Konfigurationen mithilfe des Unified Gateway-Assistenten. Der Unified Gateway Visualizer wird verwendet, um Konfiguration hinzuzufügen und zu bearbeiten und ein Back-End-Problem zu diagnostizieren.

Der Unified Gateway Visualizer zeigt Folgendes:

| Konfiguration | Konfiguration |
|---|---|
| Richtlinien vor der Authentifizierung | Authentifizierungsrichtlinien |
| Virtuelle CS-Server | Virtuelle VPN-Server |
| Virtuelle LB-Server | XA/XD-Apps |
| Web-Apps | SaaS-Apps |

Die Unified Gateway-Bereitstellung ermöglicht sicheren Remotezugriff über eine URL auf Ihre Enterprise- oder SaaS-Anwendungen, clientlosen Zugriffsanwendungen, Citrix Virtual Apps und Desktop-Ressourcen.

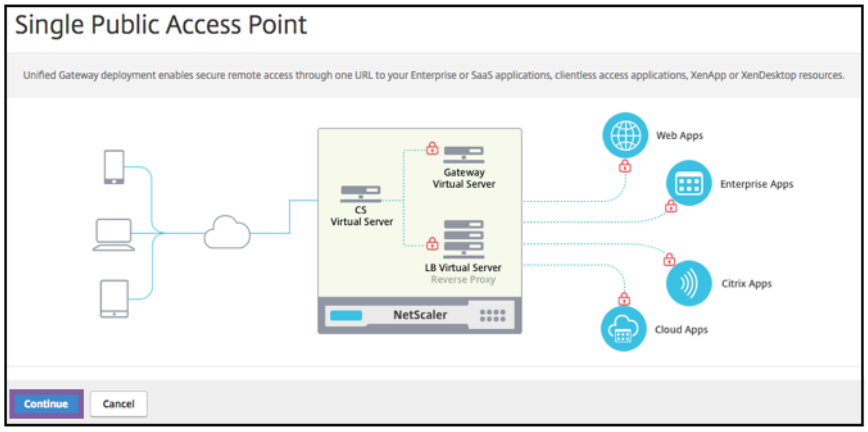
### Konfigurieren von Unified Gateway

1. Wählen Sie im Menü Unified Gateway aus.
2. Stellen Sie auf dem nächsten Bildschirm sicher, dass Sie über die folgenden Informationen verfügen, und klicken Sie dann auf **Erste Schritte**:
   - Öffentliche IP-Adresse für das Unified Gateway.
   - Serverzertifikatskette (.PFX oder.PEM) mit optionalem Root-CA-Zertifikat.
   - LDAP-/RADIUS-/Clientzertifikat-basierte Authentifizierungsdetails.

- Anwendungsdetails (URLs für SaaS-Anwendungen oder Citrix Virtual Apps and Desktops Serverdetails).

3. Klicken Sie auf **Weiter**.

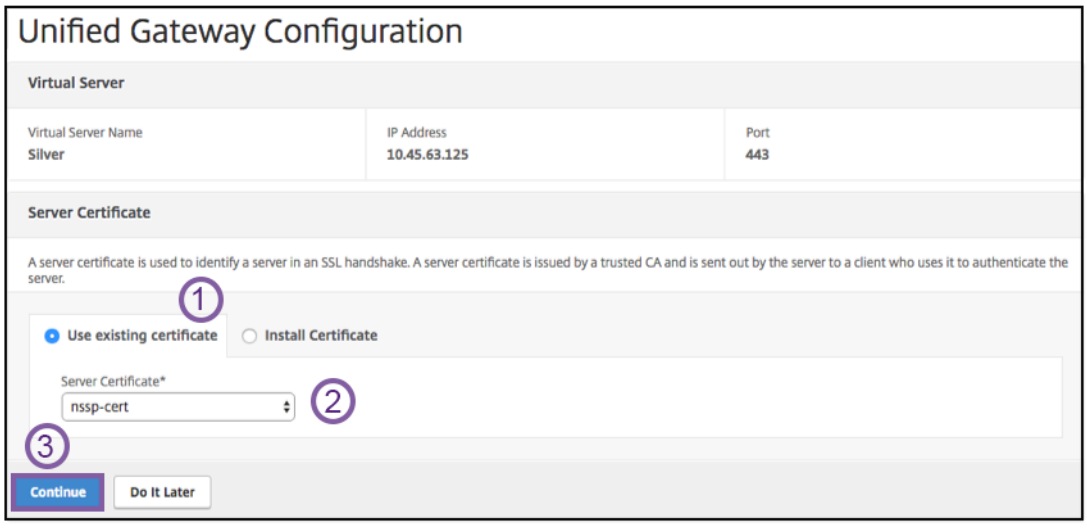



**Erstellen Sie einen virtuellen Server mit Unified Gateway-Konfiguration.**

1. Geben Sie den **Konfigurationsnamen** für den virtuellen Server ein.
2. Geben Sie die öffentlich zugängliche **Unified Gateway-IP-Adresse** für die Unified Gateway-Bereitstellung ein.
3. Geben Sie die **Portnummer** ein. Der Portnummernbereich ist 1—65535.
4. Klicken Sie auf **Weiter**.

**Füllen Sie die folgenden Informationen aus, um das Serverzertifikat anzugeben.**

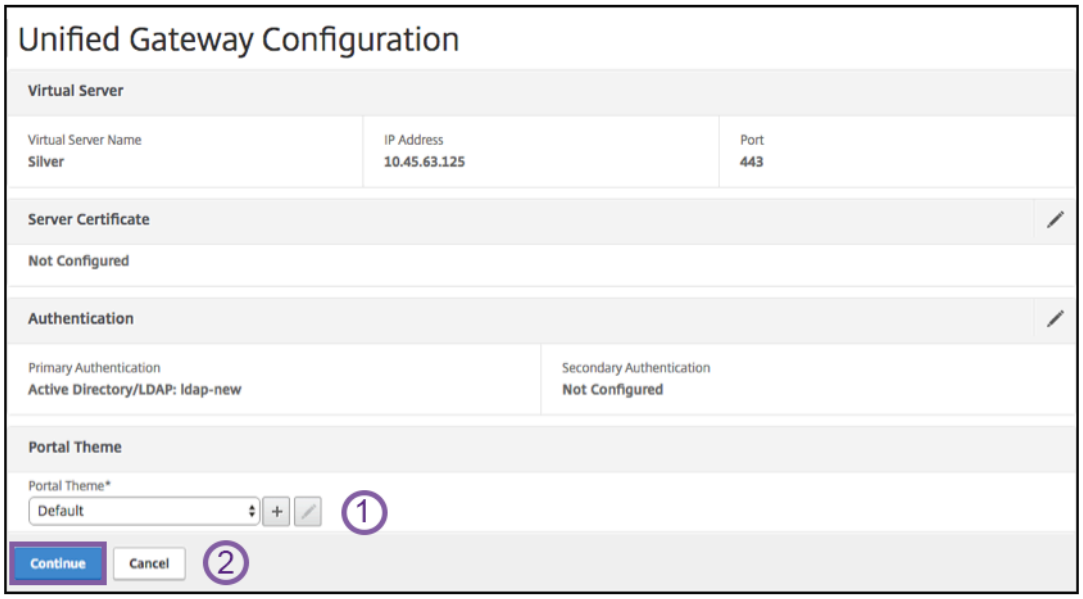
1. Wählen Sie entweder die Optionsfelder **Bestehendes Zertifikat verwendenoder Zertifikat installieren**.
2. Wählen Sie im Menü ein **Serverzertifikat** aus.
3. Klicken Sie auf **Weiter**.



**Füllen Sie die folgenden Informationen aus, um Authentifizierung anzugeben.**

1. Wählen Sie im Menü eine **primäre Authentifizierungsmethode** aus.
2. Wählen Sie entweder die Optionsfelder **Bestehenden Server verwenden** oder **Neuen Server hinzufügen** aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie im Menü das **Portal-Thema** aus.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie entweder die **Optionsfelder**Webanwendung**oder Citrix Virtual Apps Desktops** aus.
7. Klicken Sie auf **Weiter**.




## Anwendung wählen

**Füllen Sie die folgenden Informationen aus, um die Webanwendung anzugeben.**

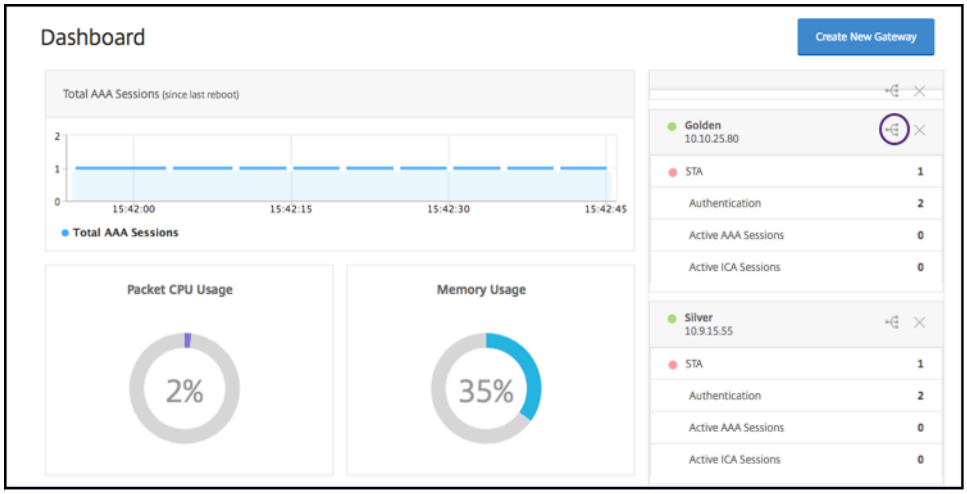
1. Geben Sie den Namen des Lesezeichen-Link ein.
2. Wählen Sie die Art der Anwendung aus, für die die VPN-URL steht. Die möglichen Werte sind:
   - Intranet-Anwendung
   - Clientloser Zugang
   - SaaS
   - Vorkonfigurierte Anwendung auf diesem Citrix ADC
3. Aktivieren Sie dieses Kästchen, um diese Anwendung über die Unified Gateway-URL zugänglich zu machen.
4. Geben Sie die URL für den Lesezeichen-Link ein.
5. Wählen Sie aus der Icon-URL eine Datei aus, um eine Icon-Datei abzurufen. Die MaxLength = 255

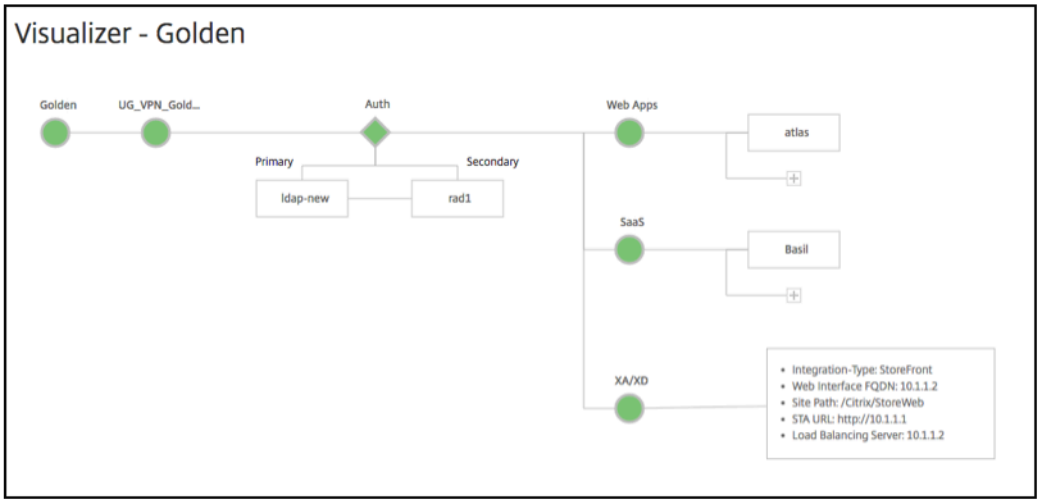
6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig**.
8. Klicken Sie auf **Weiter**.
9. Klicken Sie auf **Fertig**.

## GUI-Konfiguration

1. Wählen Sie im Menü Unified Gateway aus.
2. Klicken Sie auf das Symbol **Unified Gateway Visualizer**, um auf konfigurierte Gateway-Instanzen zuzugreifen



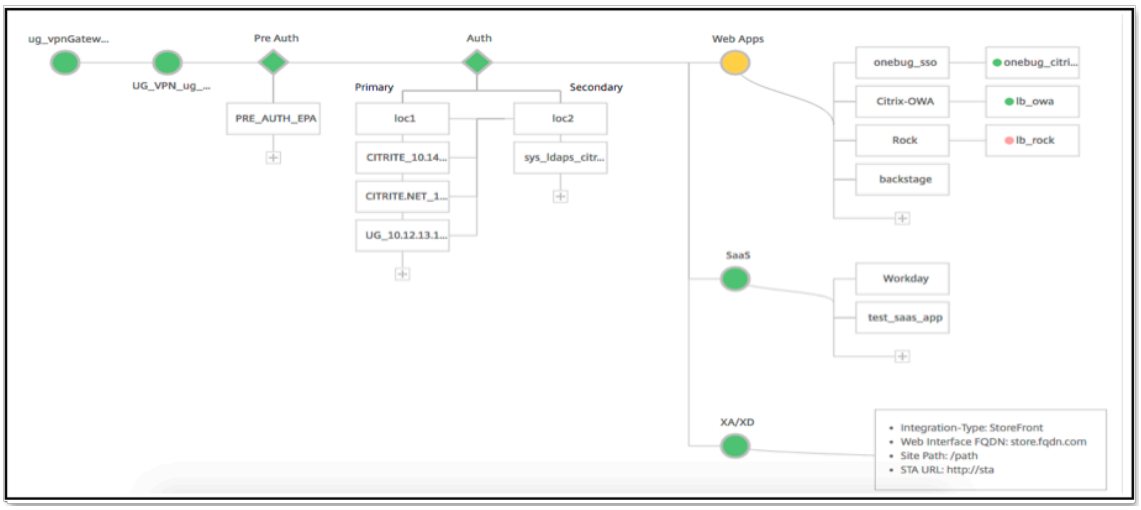

Der Unified Gateway Visualizer sieht aus wie ein Flussdiagramm, wie in der folgenden Abbildung gezeigt:




Der Unified Gateway Visualizer hat PreAuth und einen Apps-Bereich. `Auth` Wenn der virtuelle

VPN-Server über eine Vorauthentifizierungsrichtlinie verfügt, wird `pre-auth` im Unified Gateway Visualizer angezeigt.




Der Unified Gateway Visualizer verwendet ein Farbcodierungsschema für den Lastausgleich und virtuelle VPN-Server, um ihren Status anzuzeigen.

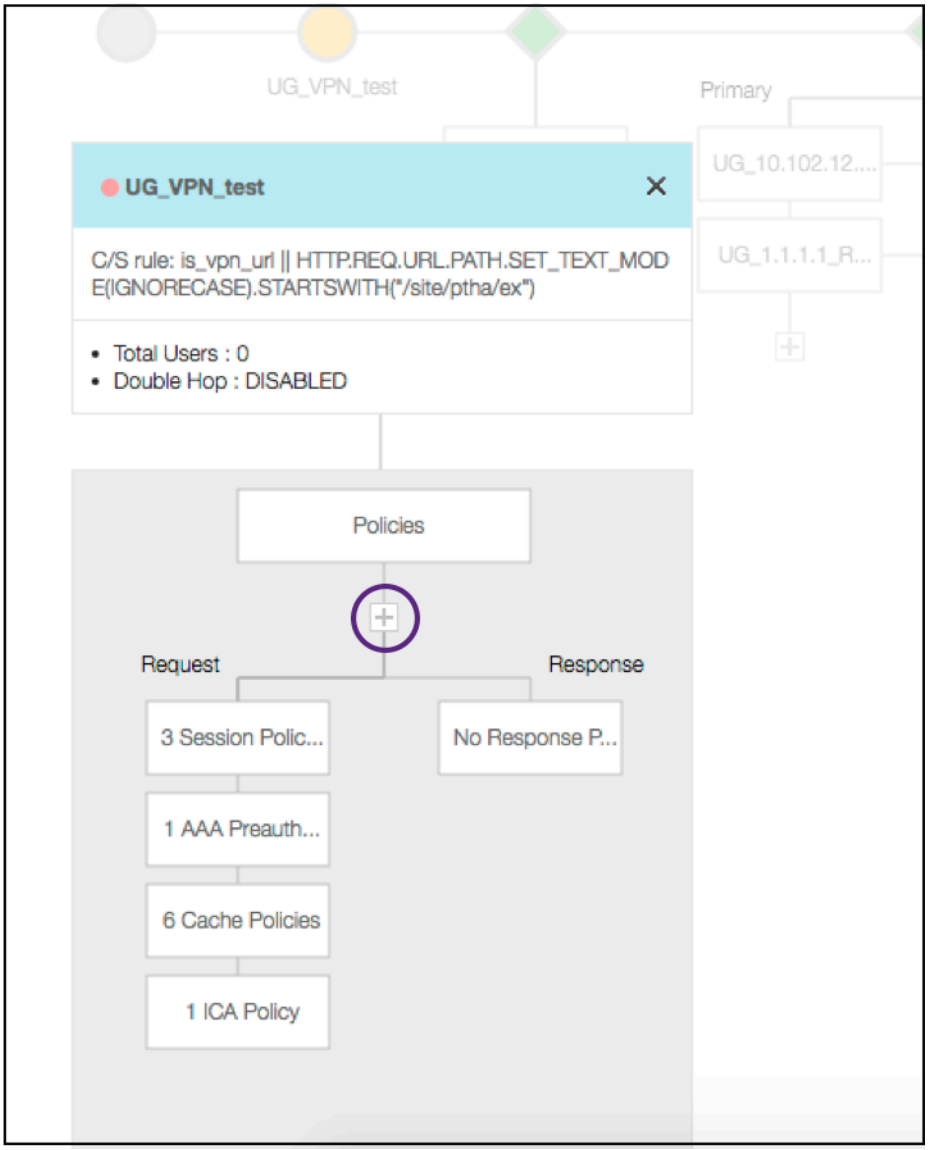
| Farbe | Beschreibung |
|---|---|
| Rot | bedeutet, dass der Server ausgefallen ist. |
| Grau | bedeutet, dass WebApps/Citrix Virtual Apps nicht konfiguriert wurden. |
| Grün | bedeutet, dass mit dem virtuellen Server alles in Ordnung ist. |
| Orangen | bedeutet, dass einer der virtuellen Serverdienste für den Lastausgleich ausgefallen ist, aber immer noch ordnungsgemäß funktioniert. |

### Details von virtuellen VPN-Servern

Um die Details der virtuellen VPN-Server abzurufen, klicken Sie auf den **Knoten Virtuelle VPN-Server**. Das Popup rendert Details wie die C/S-Regel und alle Richtlinien.

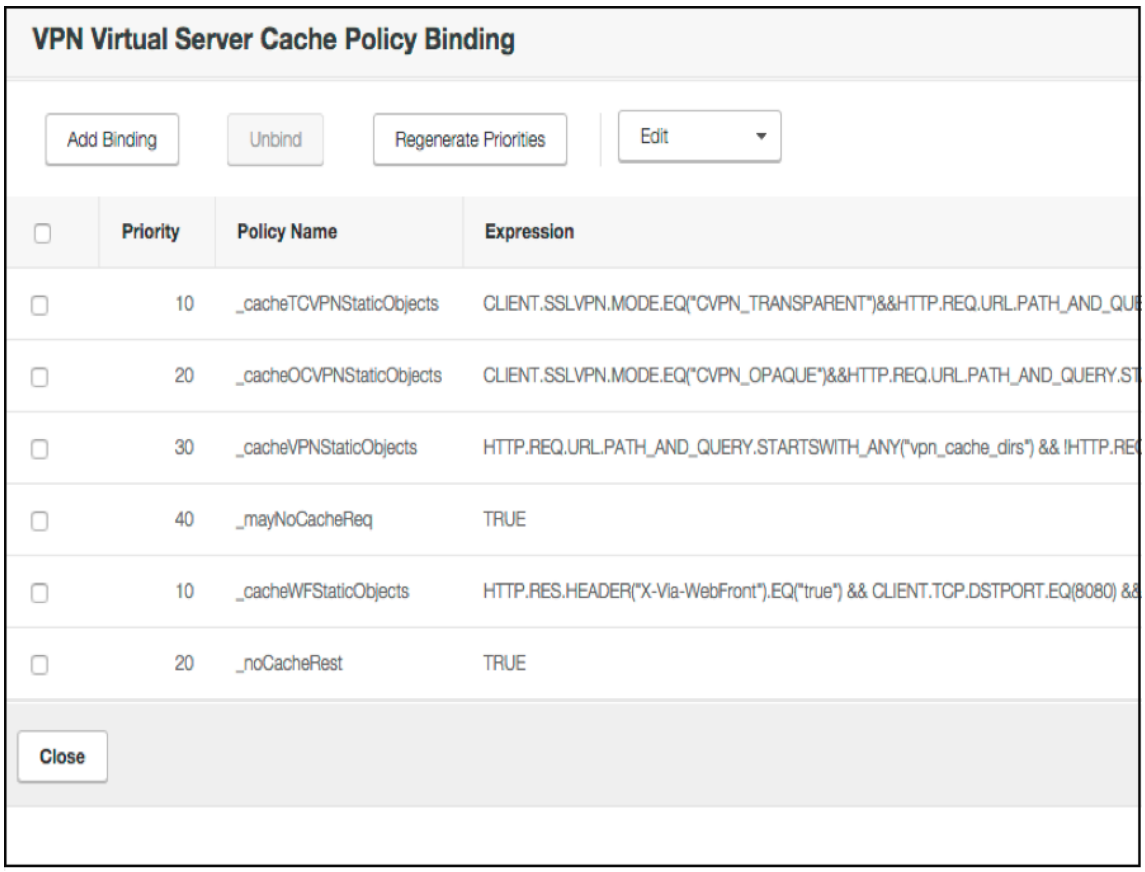
1. Fügen Sie der VPN-Entität Richtlinien hinzu, indem Sie auf das (+) -Symbol klicken.

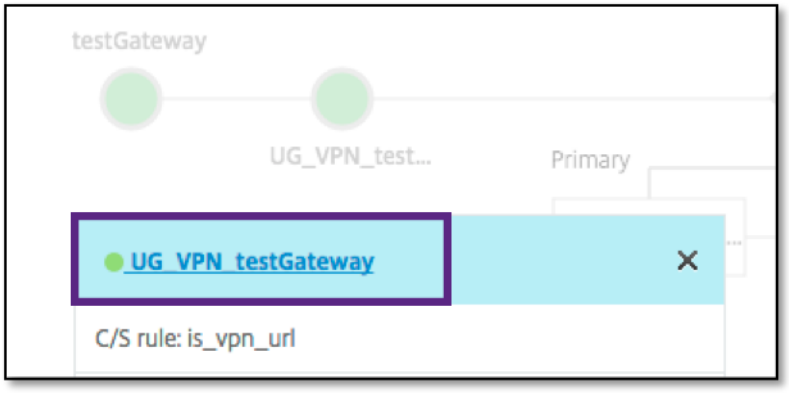



2. Klicken Sie auf den gewünschten Knoten, um Einzelheiten zu bereits konfigurierten Richtlinien anzuzeigen.

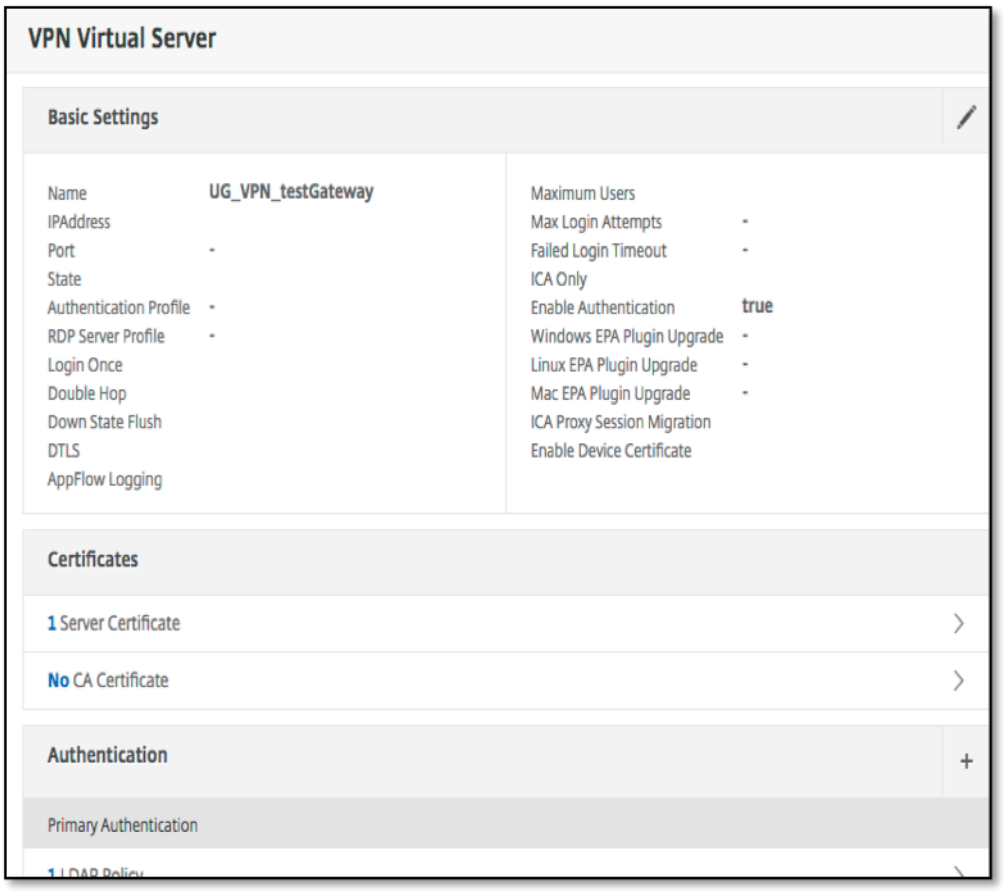



Für Informationen zum virtuellen VPN-Server ist der VPN-Titel im Popup eine anklickbare Entität, die zu einem Schieberegler wechselt, der den virtuellen VPN-Server angibt.




Die Details des VPN-Servers werden hier angezeigt.

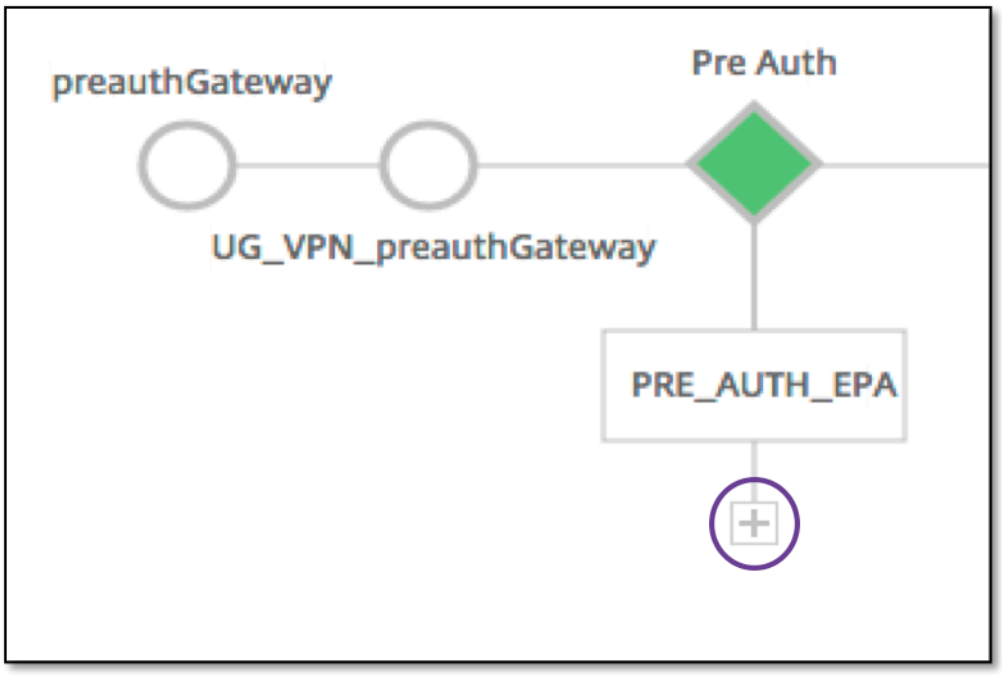



### The Pre Auth Block

Wenn einem virtuellen VPN-Server Vorauthentifizierungsrichtlinien zugeordnet sind, zeigt der Unified Gateway Visualizer einen `Pre Auth` Block an. Der `Pre Auth` Block zeigt die Richtlinien und bietet die Möglichkeit, dem VPN Vorauthentifizierungsrichtlinien hinzuzufügen.

1. Klicken Sie auf das **+**, um eine `preauth` Richtlinie hinzuzufügen.



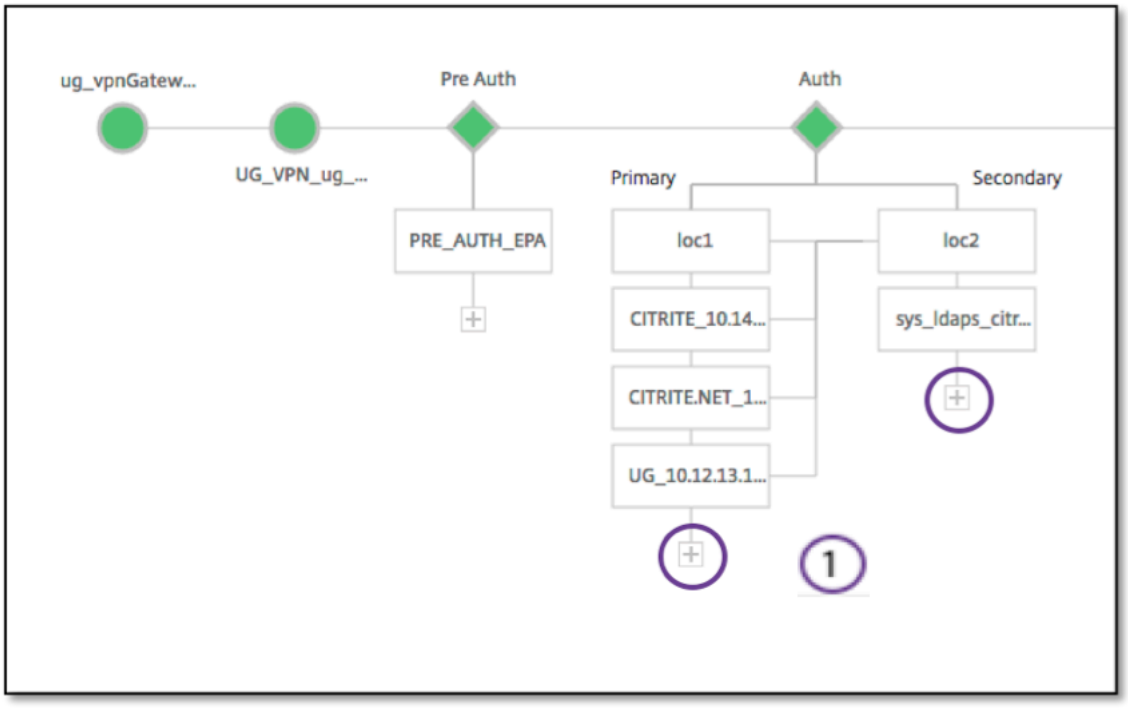

In einem Fall, in dem keine Vorauthentifizierungsrichtlinien zugeordnet sind, wäre dieser Block vor der Ansicht verborgen.

### The Auth Block

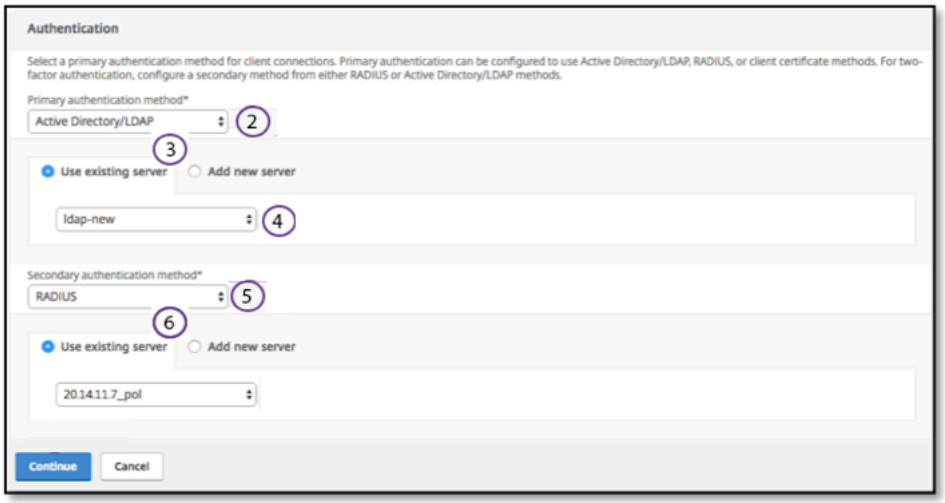
Der Auth Block listet die primären und sekundären Richtlinien auf. Der Auth Block bietet eine Option zum Hinzufügen von Richtlinien.

1. Klicken Sie in der Liste Primär auf **+**, um eine primäre Authentifizierungsbindung hinzuzufügen, oder klicken Sie in der Liste Sekundär auf +, um eine sekundäre Authentifizierungsbindung



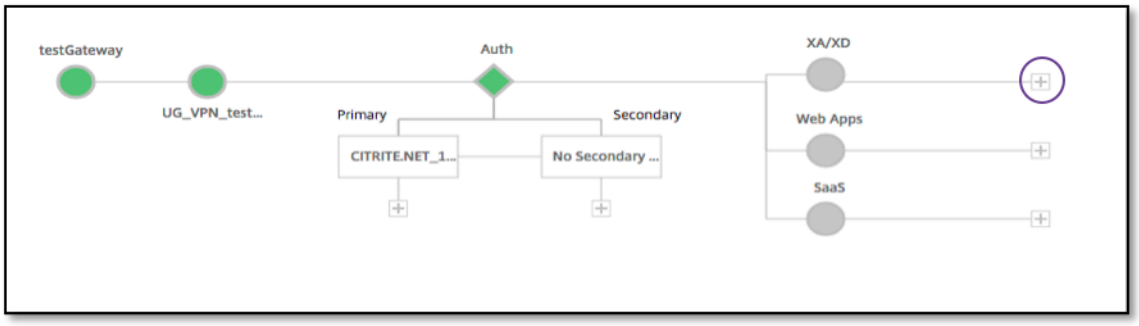

2. Wählen Sie im Menü **Primäre Authentifizierungsmethode eine** Option aus.
3. Geben Sie an, ob es sich um einen **vorhandenen Server** handelt oder **fügen Sie neuen Server** hinzu, indem Sie das Optionsfeld auswählen.
4. Wählen Sie im Menü **LDAP-Richtlinienname** eine Option aus.
5. Wählen Sie **RADIUS** aus dem Menü **Sekundäre Authentifizierungsmethode**.
6. Geben Sie an, ob Sie einen**vorhandenen Server verwenden** oder **neuen Server hinzufügen** möchten, indem Sie das Optionsfeld auswählen.
7. Klicken Sie auf **Weiter**.



### StoreFront hinzufügen

1. Klicken Sie in der Nähe des XA/XD auf **+** und Sie müssen "XA/XD"-Apps hinzufügen.




Sie können Ihren Integrationspunkt wählen. Die Optionen sind StoreFront, WI oder WionNS. Klicken Sie auf **Weiter**.

1. Füllen Sie die folgenden Felder aus, um StoreFront zu konfigurieren. Die Felder, die Pflichtangaben erfordern, sind mit dem * gekennzeichnet.

   |**Feld**|**Beschreibung**|
   |—|—|
   |StoreFront FQDN*|Geben Sie den FQDN des StoreFront-Servers ein. Maximale Länge: 255 char.Beispiel: //storefront.xendt.net|
   |Site-Pfad*|Geben Sie den Pfad zu Receiver für die bereits auf StoreFront konfigurierte Website ein.|
   |`Single Sign-on Domain`*|Geben Sie die Standarddomäne für die Benutzerauthentifizierung ein|
   |Storename*|Geben Sie den Namen für die StoreFront-Monitore ein.
   Der STORENAME ist ein Argument, das den Namen des StoreFront-Dienstspeichers definiert, um den Zustand von StoreFront-Servern zu prüfen. Gilt für StoreFront-Monitore. Maximale Länge: 31|
   |Secure Ticket Authority-Server|*Geben Sie die Secure Ticket Authority-URL ein, die normalerweise auf dem Delivery Controller vorhanden ist.*
   *Beispiel:*`http://sta`|
   |*StoreFront-Server*|Geben Sie die IP-Adresse des StoreFront-Servers ein|
   |Protokoll|*Geben Sie das vom Server verwendete Protokoll ein.* |
   |*Port*|Geben Sie den vom Server verwendeten Port ein. |
   |Load Balancing|Geben Sie die Lastausgleichskonfiguration für die StoreFront-Server ein. |
   |Virtueller Server*|Geben Sie die öffentlich zugängliche IP-Adresse für die Unified Gateway-Bereitstellung ein. |

2. Klicken Sie auf **Weiter.**

### SaaS hinzufügen

1. Klicken Sie auf **+**, um SaaS-Apps hinzuzufügen. Sie gelangen zur Seite SaaS hinzufügen. Füllen Sie die folgenden Felder aus, um SaaS zu konfigurieren. Die Felder, die Pflichtangaben erfordern, sind mit einem* gekennzeichnet.

| Feld | Beschreibung |
|---|---|
| Nome* | Geben Sie den Namen des Lesezeichen-Link ein. |
| Anwendungstyp | Geben Sie die Art der Anwendung ein, die diese VPN-URL repräsentiert.Mögliche Werte sind: Intranet-Anwendung/Clientloser Zugriff/Saas/vorkonfigurierte Anwendung auf diesem Citrix ADC |
| Geben Sie die URL ein* | Geben Sie die URL der Intranet-Anwendung ein. |
| Wählen Sie **Datei** | Geben Sie die URL ein, um die Icon-Datei für die Anzeige dieser Ressource abzurufen. Maximale Länge = 255 |

### Hinzufügen von WebApps

1. Klicken Sie auf **+**, um Web-Apps hinzuzufügen. Sie gelangen zur Seite Web-Apps hinzufügen. Füllen Sie die folgenden Felder aus, um eine Webanwendung zu konfigurieren. Die Felder, die Pflichtangaben erfordern, sind mit einem * gekennzeichnet.

| Feld | Beschreibung |
|---|---|
| Nome* | Geben Sie den Namen des Lesezeichen-Link ein. |
| Anwendungstyp | Geben Sie die Art der Anwendung ein, die diese VPN-URL repräsentiert.Mögliche Werte sind: Intranet-Anwendung/Clientloser Zugriff/Saas/vorkonfigurierte Anwendung auf diesem Citrix ADC |
| Geben Sie die URL ein* | Geben Sie die URL der Intranet-Anwendung ein. |
| Wählen Sie **Datei** | Geben Sie die URL ein, um die Icon-Datei zur Anzeige dieser Ressource abzurufen.MaxLength = 255 |

Wenn auf eine Anwendung über die Unified Gateway-URL zugegriffen werden kann, können Sie auf die Details des Load Balancing-Servers zugreifen, indem Sie auf die App klicken:


Neue Richtlinien können durch Klicken auf (+) hinzugefügt werden, und alle gebundenen Richtlinien können angezeigt werden, indem Sie auf den Knoten klicken, der Richtlinieninformationen anzeigt.

Die Anzahl der an den Load Balancer gebundenen Dienste wird ebenfalls angezeigt, zusammen mit den allgemeinen Statusinformationen. Ein weiterer Klick listet alle Dienste auf. Neue Dienste können zum Load Balancer hinzugefügt werden.

Für weitere Details des Load Balancers ist der Titel des Popups anklickbar, der auf der Detailseite des virtuellen Lastausgleichsservers landet.

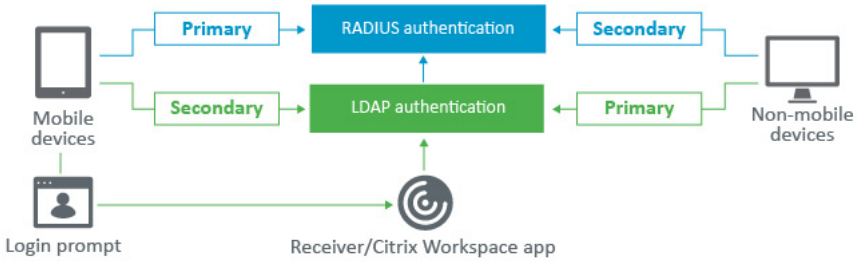
# Konfigurieren Sie Citrix Gateway für die Verwendung der RADIUS- und LDAP-Authentifizierung mit Mobil-/Tablet-Geräten

March 27, 2024

In diesem Abschnitt wird beschrieben, wie das Citrix Gateway-Gerät für die Verwendung der RADIUS-Authentifizierung als primäre und LDAP-Authentifizierung als sekundäre mit Mobil-/Tablet-Geräten konfiguriert wird.

Die in diesem Abschnitt demonstrierte Konfiguration ermöglicht weiterhin allen anderen Verbindungen, zuerst LDAP und dann RADIUS zu verwenden.

Wenn Sie die Zwei-Faktor-Authentifizierung in der Citrix Workspace-App für die Verwendung mit Mobil-/Tablet-Geräten konfigurieren, müssen Sie die RSA SecureID (RADIUS-Authentifizierung) als primäre Authentifizierung hinzufügen. Wenn die Benutzer jedoch die Aufforderung zur Eingabe von Benutzernamen und Kennwort, Passcode auf Receiver erhalten, setzen sie LDAP an die erste Stelle und RADIUS als zweite Anmeldeinformationen. Aus Sicht des Administrators handelt es sich um eine andere Konfiguration im Vergleich zu einer nicht-mobilen Konfiguration.



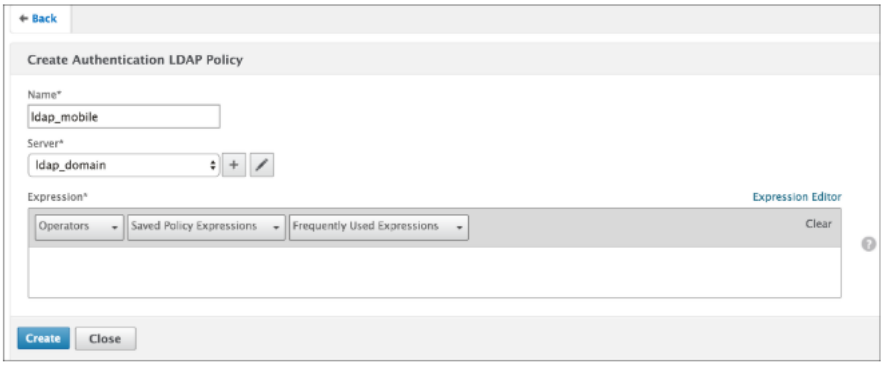

Führen Sie das folgende Verfahren aus, um das Citrix Gateway-Gerät für die Verwendung der RADIUS-Authentifizierung als primäre und LDAP-Authentifizierung als sekundäre mit Mobil-/Tablet-Geräten zu konfigurieren.

1. Wählen Sie im Konfigurationsprogramm **Citrix Gateway > Richtlinien > Authentifizierung** aus und erstellen Sie eine Authentifizierungsrichtlinie für LDAP und RSA für mobile Geräte und nicht mobile Geräte. Dies ist notwendig, um eine Logikbedingung zu vermeiden, die es Benutzern ermöglicht, die RADIUS-Authentifizierung zu Bypass.
2. Geben Sie LDAP-Serverdetails ein, nachdem Sie auf der Registerkarte **Server** für LDAP auf die Option **Hinzufügen** geklickt haben.
3. Erstellen Sie eine LDAP-Richtlinie für die Mobilgeräte, indem Sie den erforderlichen LDAP-Server auswählen.

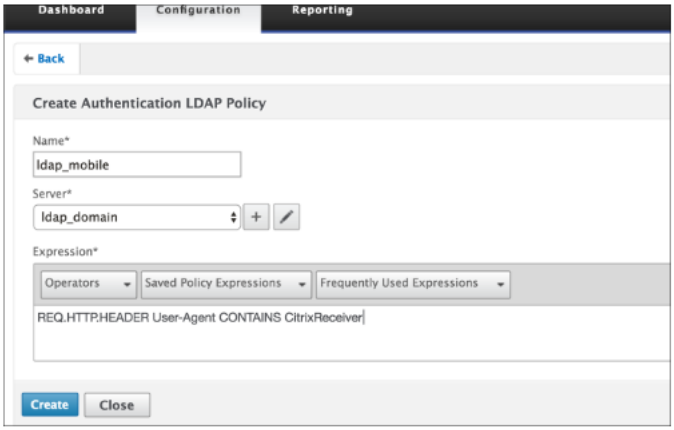
   Verwenden Sie den folgenden Ausdruck, um diese Richtlinie nur an mobile Geräte zu binden:

   ```
   1 REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```




4. Klicken Sie auf **Expression Editor**, um eine Richtlinie zu erstellen:

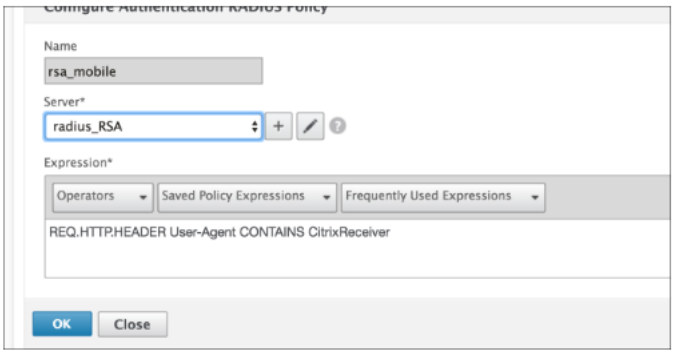

5. Erstellen Sie eine RADIUS-Richtlinie und einen RADIUS-Server für die Mobilgeräte.

   - Navigieren Sie über **Citrix Gateway > Richtlinien > Authentifizierung > RADIUS zur Option RADIUS**. Klicken Sie auf der Registerkarte Server auf **Hinzufügen**.

- Fügen Sie die erforderlichen Details hinzu. Der Standardport für die RADIUS-Authentifizierung ist 1812.

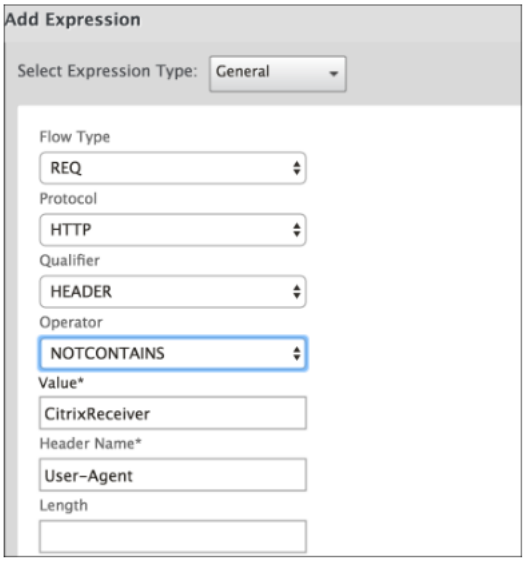

- Verwenden Sie den folgenden Ausdruck, um diese Richtlinie nur an mobile Geräte zu binden:

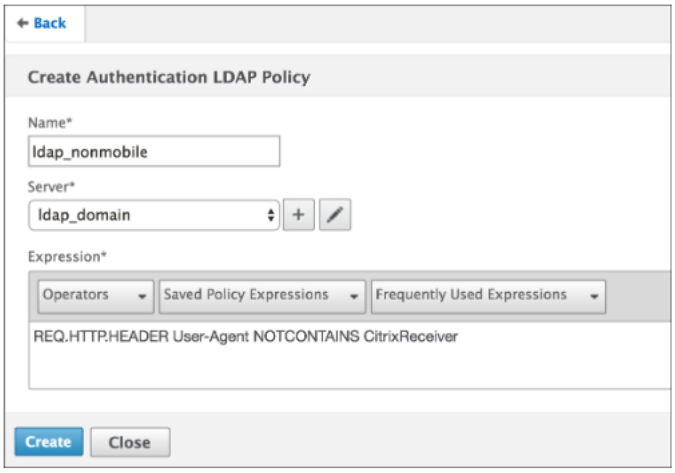



6. Befolgen Sie denselben Schritt, um eine LDAP-Richtlinie für nicht mobile Geräte zu erstellen. Verwenden Sie den folgenden Ausdruck, um diese Richtlinie nur an Nicht-Mobilgeräte zu binden:

```
1 REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

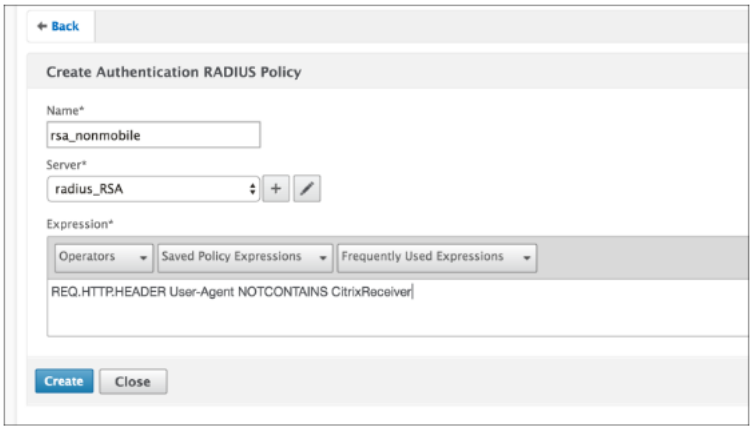
 



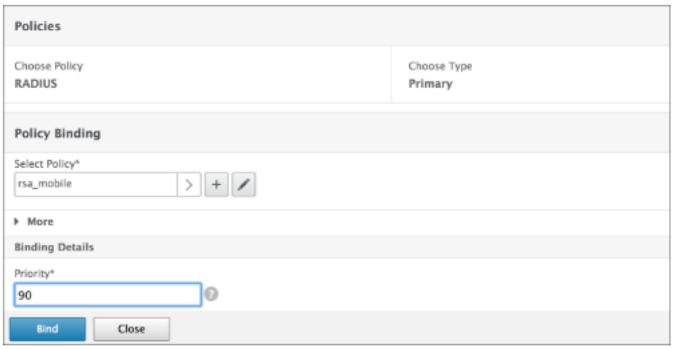

7. Erstellen Sie eine RADIUS-Richtlinie für nicht-mobile Geräte. Verwenden Sie den folgenden Ausdruck, um diese Richtlinie nur an Nicht-Mobilgeräte zu binden:

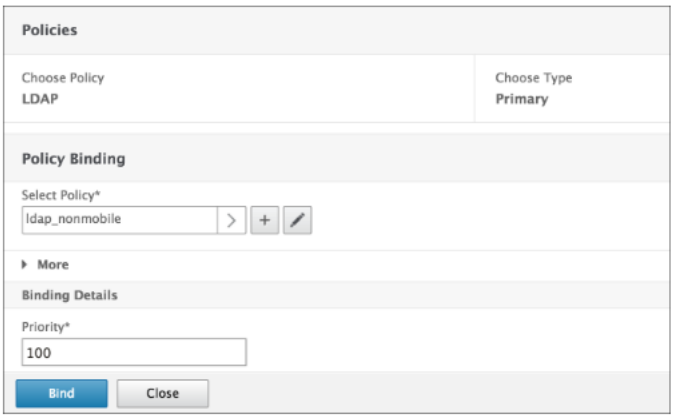
```
1 REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```



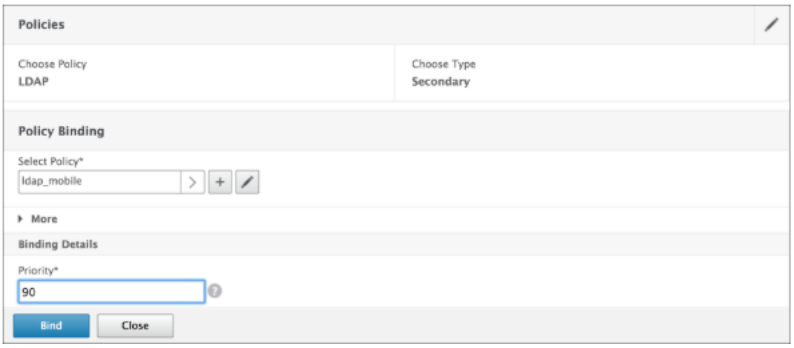

 

8. Gehen Sie zu den Eigenschaften des virtuellen Citrix Gateway-Servers und klicken Sie auf die Registerkarte **Authentifizierung**. Fügen Sie in den Primären Authentifizierungsrichtlinien die Richtlinie RSA_Mobile als oberste Priorität und die LDAP_NonMobile-Richtlinie als sekundäre Priorität hinzu:




9. Fügen Sie in den sekundären Authentifizierungsrichtlinien die Richtlinie LDAP_Mobile als oberste Priorität hinzu, gefolgt von der Richtlinie RSA_NonMobile als sekundäre Priorität:



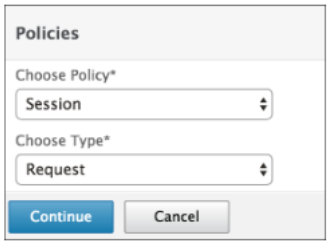

> Die Sitzungsrichtlinie muss über den richtigen Single Sign-On Credential Index verfügen, d. h. es müssen die LDAP-Anmeldeinformationen sein. Für mobile Geräte muss der **Anmeldeinformationsindex** unter **Sitzungsprofil > Client Experience** auf **Sekundär** festgelegt werden, was LDAP ist.

Daher benötigen Sie zwei Sitzungsrichtlinien, eine für mobile Geräte und die andere für nicht-

mobile Geräte.

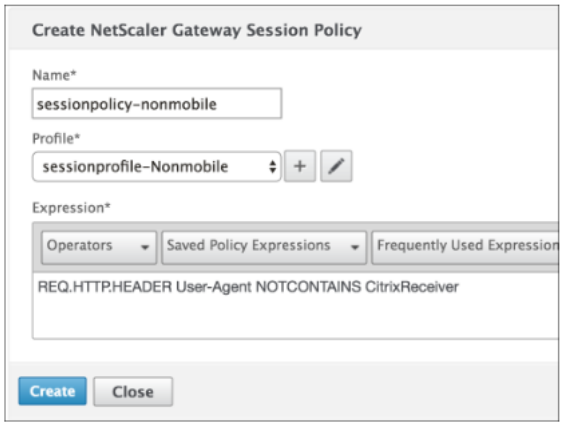
- Für mobile Geräte werden die Sitzungsrichtlinie und das Sitzungsprofil wie im folgenden Screenshot angezeigt.
  Um eine Sitzungsrichtlinie zu erstellen, navigieren Sie zum erforderlichen virtuellen Server, klicken Sie auf **Bearbeiten**, gehen Sie zum Abschnitt Richtlinie und klicken Sie auf + Zeichen:
- Wählen Sie die Option **Sitzung** aus dem Menü.




- Geben Sie den gewünschten Sitzungsrichtliniennamen ein und klicken Sie auf +, um ein Profil zu erstellen. Für mobile Geräte muss der **Anmeldeinformationsindex** unter **Sitzungsprofil > Client Experience** auf **Sekundär** festgelegt werden, was LDAP ist.
- Befolgen Sie für nicht mobile Geräte dieselben Schritte. **Der Anmeldeinformationsindex** unter **Sitzungsprofil > Client Experience** muss auf **Primär** festgelegt werden, was LDAP ist.

Der Ausdruck muss geändert werden in:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

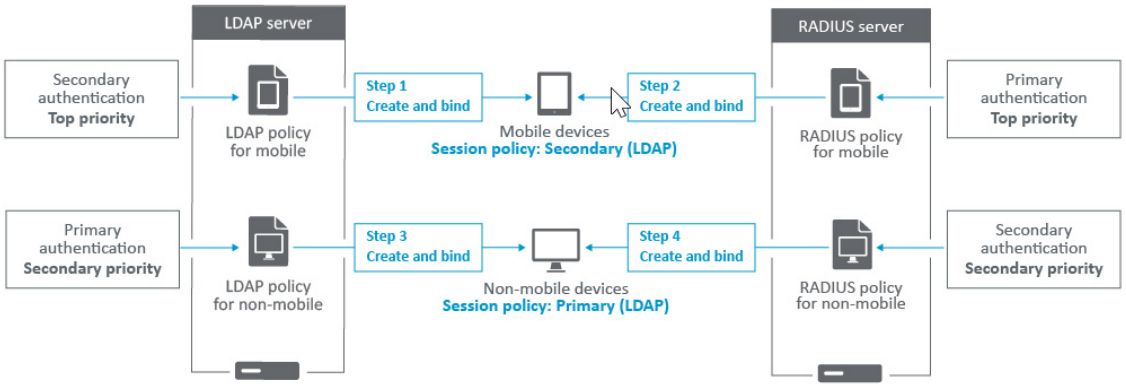



- Um ein Profil für nicht-mobile Benutzer zu erstellen, klicken Sie auf + Zeichen.

10. Die folgende Abbildung zeigt die Richtlinien und Profile unter dem erforderlichen virtuellen Server.

11. Ebenfalls auf der StoreFront, unter der Citrix Gateway-Konfiguration, um “Anmeldetyp”= “Domäne und Sicherheitstoken”zu verwenden




# Zugriff auf Citrix Gateway für Mitglieder einer Active Directory-Gruppe beschränken

March 27, 2024

Citrix Gateway unterstützt zwei Methoden zur Einschränkung des Anmeldezugriffs.

- LDAP-Suchfilter —Nur Benutzernamen, die dem LDAP-Suchfilter entsprechen (z. B. Active Directory-Gruppenmitgliedschaft), können sich bei Citrix Gateway anmelden.
- Gruppen, die sich an einer Citrix Gateway-Sitzungsrichtlinie oder einem Citrix Gateway-Sitzungsprofil anmelden dürfen —Diese Methode unterstützt mehrere Active Directory Einzelheiten finden Sie unter https://support.citrix.com/article/CTX125797.

In diesem Artikel wird die LDAP-Suchfilter-Methode beschrieben.

## Übersicht

Wenn ein Benutzer die Anmeldeinformationen auf der Anmeldeseite des virtuellen Citrix Gateway-Servers eingibt und die EINGABETASTE drückt, durchsucht das Gerät zuerst das Active Directory (LDAP) nach dem Benutzernamen. Wenn in der LDAP-Richtlinie oder auf dem Server kein LDAP-Suchfilter definiert ist, durchsucht die Appliance alle Active Directory-Benutzernamen nach einer Übereinstimmung. Sobald eine Übereinstimmung gefunden wurde, zieht die Appliance den vollständigen Distinguished Name (DN) des Benutzers und verwendet den DN und das Kennwort des Benutzers, um sich beim Active Directory zu authentifizieren.

Wenn ein LDAP-Suchfilter definiert ist, werden nur Benutzernamen gesucht, die dem LDAP-Suchfilter entsprechen, nach einer Übereinstimmung mit dem Benutzernamen. Wenn der LDAP-Suchfilter

beispielsweise so konstruiert ist, dass nur Mitglieder einer Active Directory-Gruppe gesucht werden, muss der vom Benutzer eingegebene Benutzername mit den Mitgliedern der Gruppe übereinstimmen.

### Voraussetzungen

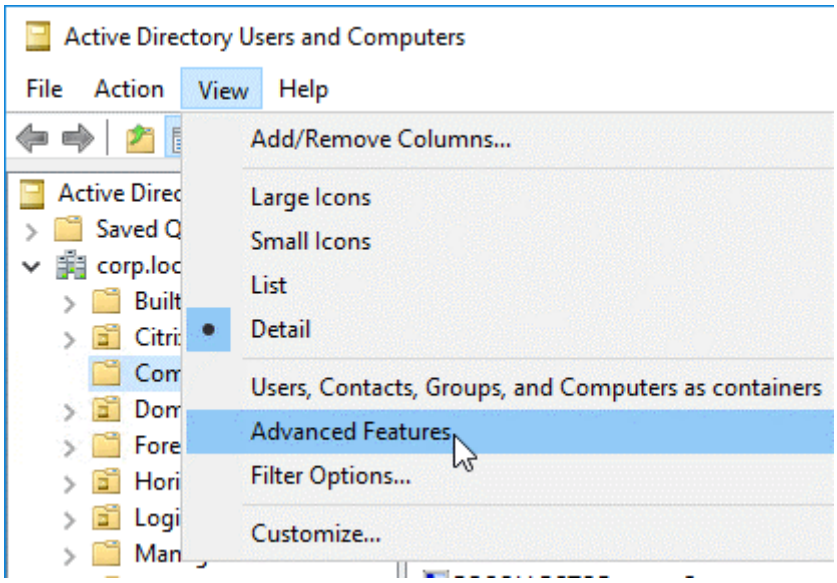
Der virtuelle Citrix Gateway-Server muss für die LDAP-Authentifizierung konfiguriert sein.

### Schritte zum Konfigurieren eines LDAP-Suchfilters für Mitglieder einer Active Directory-Gruppe

1. Bestimmen Sie die Active Directory-Gruppe, die Zugriffsberechtigung hat, und erhalten Sie den vollständigen Distinguished

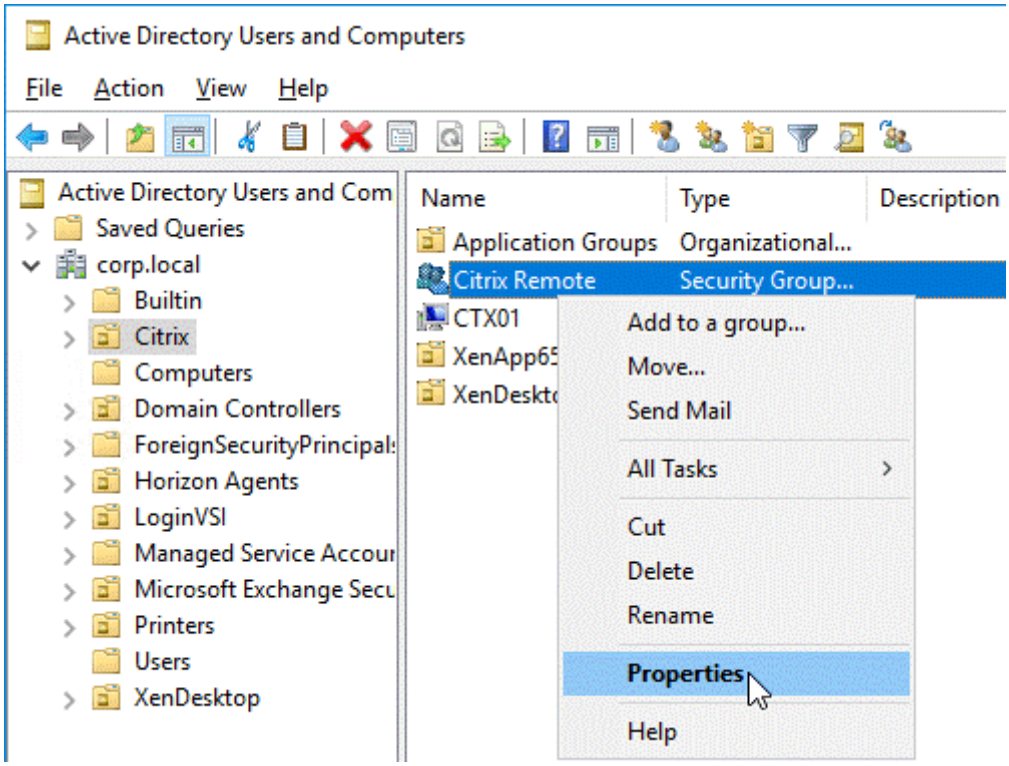
   Eine einfache Möglichkeit, den vollständigen Distinguished Name der Gruppe zu erhalten, sind Active Directory-Benutzer und -Computer.

2. Aktivieren Sie in Active Directory-Benutzer und -Computer im Menü **AnsichtErweiterte Funktionen**.

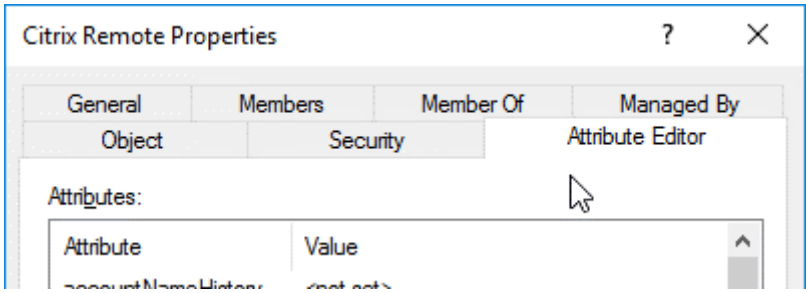



3. Blättern Sie in der Struktur zum Gruppenobjekt, klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Eigenschaften**.
   **Hinweis:** Sie können **Find**nicht verwenden. Stattdessen müssen Sie durch den Baum navigieren, um das Objekt zu finden.



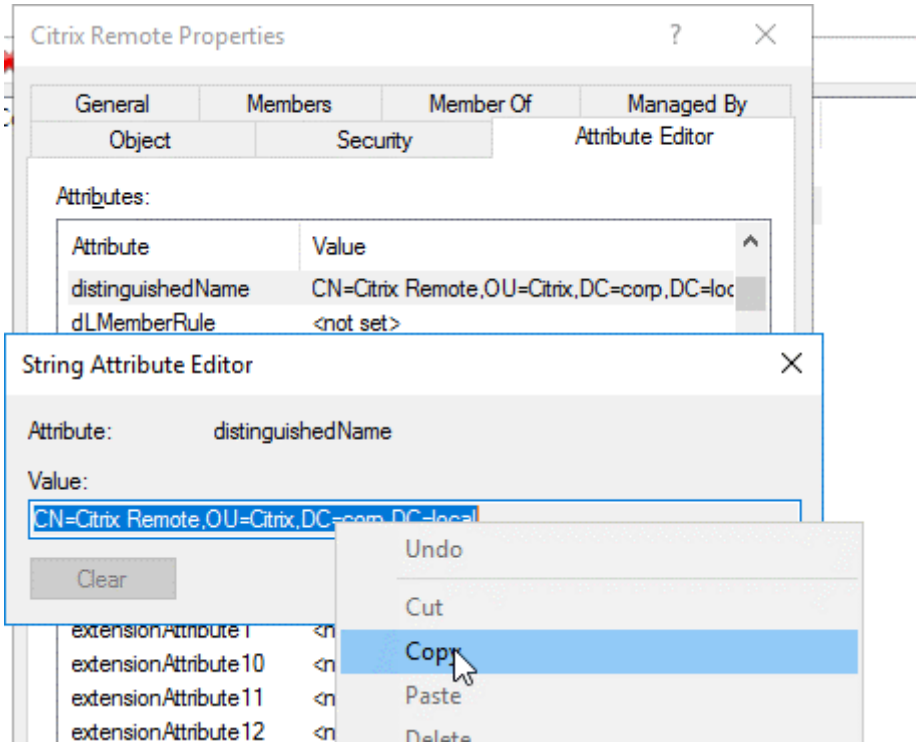

4. Wechseln Sie auf der rechten Seite zur Registerkarte **Attribut-Editor**.



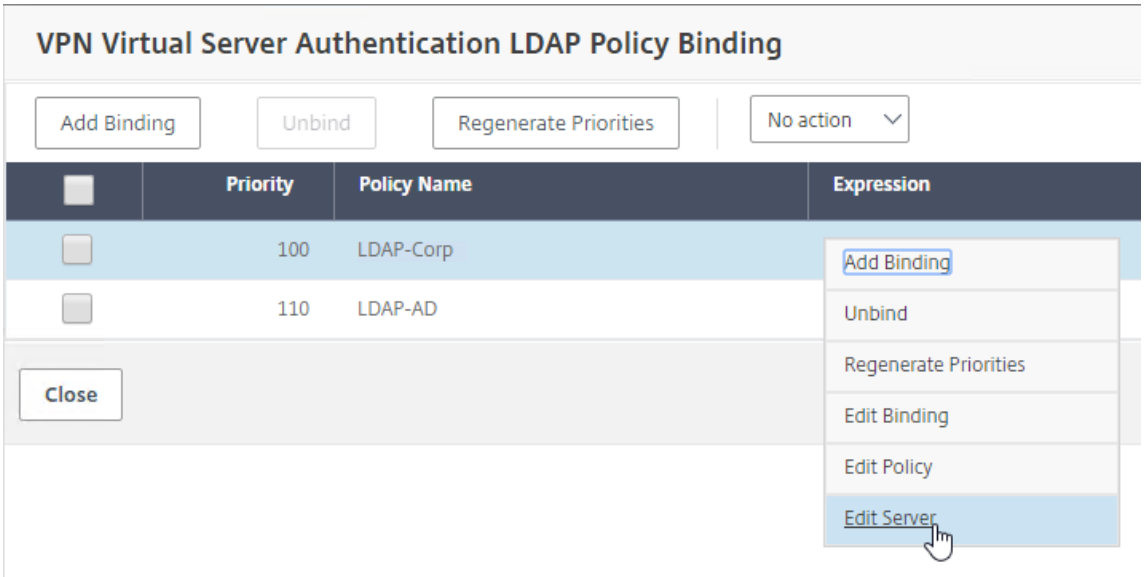

   Diese Registerkarte ist nur sichtbar, wenn **erweiterte Funktionen** aktiviert sind und Sie die **Suchfunktion** nicht verwendet haben.

5. Scrollen Sie nach unten zu **DistinguishedName**, doppelklicken Sie darauf und kopieren Sie es dann in die Zwischenablage.



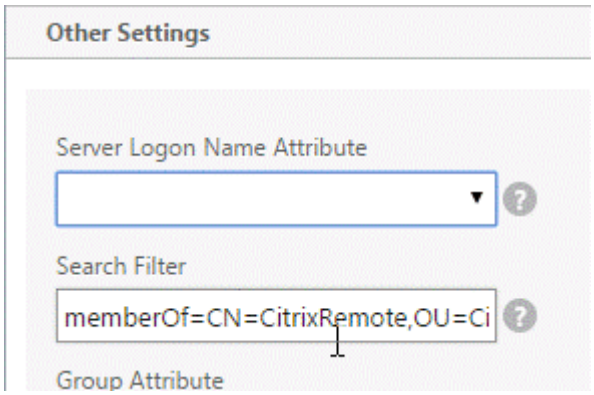

6. Navigieren Sie in der Citrix Gateway GUI zu **Citrix Gateway > Virtuelle Server**.
7. Wählen Sie einen vorhandenen virtuellen Citrix Gateway-Server aus und klicken Sie auf **Bearbeiten**.
8. Klicken Sie im Abschnitt Standardauthentifizierung auf **LDAP-Richtlinien**.
9. Klicken Sie mit der rechten Maustaste auf eine bestehende LDAP-Richtlinie, und klicken Sie auf **Server bearbeiten**.




10. Geben Sie im Abschnitt **Andere Einstellungen** im Feld **SuchfilterMemberOf=** ein und fügen

Sie dann den Distinguished Name der Active Directory-Gruppe nach dem Gleichheitszeichen (=) ein.




Ein Beispiel für einen Suchfilter ist der folgende:
Memberof=CN=Citrix Remote, OU=Citrix, DC=Corp, DC=Local
**Hinweis:** Standardmäßig sucht NetScaler nur nach Benutzernamen, die direkte Mitglieder der Active Directory-Gruppe sind. Wenn Sie verschachtelte Gruppen suchen möchten, fügen Sie Microsoft OID zum LDAP-Suchfilter hinzu. Die OID wird zwischen MemberOf und = eingefügt.

**Beispiel:** Memberof:1.2.840.113556.1.4.1941: =CN=Citrix Remote, OU=Citrix, DC=Corp, DC=Lokal

11. Klicken Sie auf **OK**.

## Verwenden von Hochverfügbarkeit

March 27, 2024

Eine Hochverfügbarkeitsbereitstellung von zwei Citrix Gateway-Appliances kann bei jeder Transaktion einen unterbrechungsfreien Betrieb ermöglichen. Wenn Sie eine Appliance als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server, während der sekundäre Knoten den primären Knoten überwacht. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten die Kontrolle.

Der sekundäre Knoten überwacht den primären Knoten, indem er regelmäßige Nachrichten (oft als Heartbeat-Nachrichten oder Zustandsprüfungen bezeichnet) sendet, um festzustellen, ob der primäre Knoten Verbindungen akzeptiert. Wenn eine Integritätsüberprüfung fehlschlägt, versucht der sekundäre Knoten die Verbindung für einen bestimmten Zeitraum erneut, woraufhin festgestellt wird, dass der primäre Knoten nicht normal funktioniert. Der sekundäre Knoten übernimmt dann die primäre (ein Prozess, der als Failover bezeichnet wird).

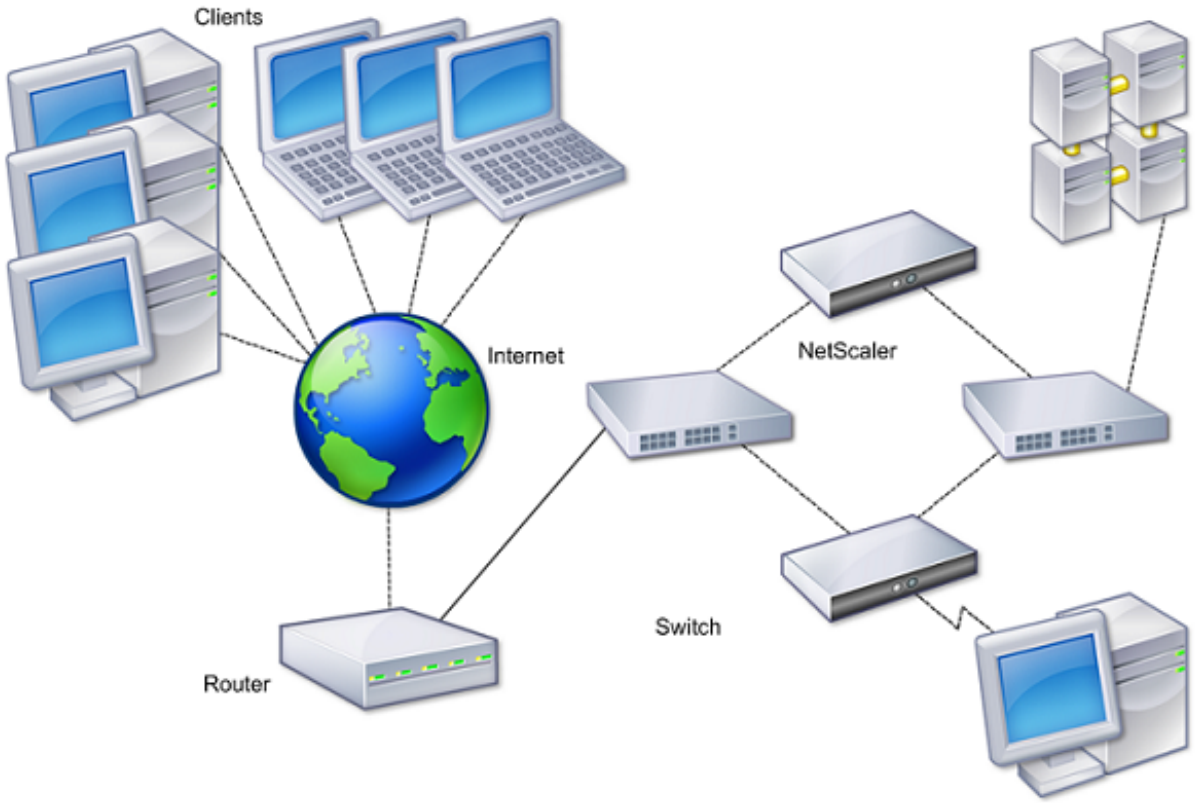
 

Nach einem Failover müssen alle Clients ihre Verbindungen zu den verwalteten Servern wiederherstellen, aber die Regeln für die Sitzungspersistenz werden wie vor dem Failover beibehalten.

Wenn die Webserver-Protokollierungspersistenz aktiviert ist, gehen aufgrund des Failovers keine Protokolldaten verloren. Damit die Protokollierungspersistenz aktiviert wird, muss die Konfiguration des Protokollservers Einträge für beide Systeme in der Datei log.conf enthalten.

Die folgende Abbildung zeigt eine Netzwerkkonfiguration mit einem Hochverfügbarkeitspaar.

Abbildung 1. Citrix Gateway Appliances in einer Hochverfügbarkeitskonfiguration




Die grundlegenden Schritte zur Konfiguration der Hochverfügbarkeit lauten wie folgt:

1. Erstellen Sie ein Basis-Setup, bei dem sich beide Knoten im selben Subnetz befinden.
2. Passen Sie die Intervalle an, in denen die Knoten Informationen zur Gesundheitscheck übermitteln.
3. Passen Sie den Prozess an, mit dem Knoten die Synchronisierung aufrecht halten.
4. Passen Sie die Weitergabe von Befehlen von der Primär- zur Sekundärseite an.
5. Konfigurieren Sie optional den ausfallsicheren Modus, um eine Situation zu verhindern, in der keiner der Knoten primär ist.
6. Konfigurieren Sie virtuelle MAC-Adressen, wenn Ihre Umgebung Geräte enthält, die keine kostenlosen ARP-Nachrichten von Citrix Gateway akzeptieren.

Wenn Sie für eine komplexere Konfiguration bereit sind, können Sie Hochverfügbarkeitsknoten in ver-

schiedenen Subnetzen konfigurieren.

Um die Zuverlässigkeit Ihres Hochverfügbarkeits-Setups zu verbessern, können Sie Routenmonitore konfigurieren und redundante Verbindungen erstellen. In einigen Situationen, z. B. bei der Fehlerbehebung oder Durchführung von Wartungsaufgaben, möchten Sie möglicherweise einen Knoten zum Failover zwingen (dem anderen Knoten den Primärstatus zuweisen), oder Sie möchten den sekundären Knoten zwingen, sekundär zu bleiben oder der primäre Knoten primär zu bleiben.

## Wie Hochverfügbarkeit funktioniert

March 27, 2024

Wenn Sie Citrix Gateway in einem Hochverfügbarkeitspaar konfigurieren, überwacht das sekundäre Citrix Gateway das erste Gerät, indem es regelmäßige Nachrichten sendet, die auch als Heartbeat-Meldung oder Zustandsprüfung bezeichnet werden, um festzustellen, ob das erste Gerät Verbindungen akzeptiert. Wenn eine Zustandsprüfung fehlschlägt, versucht das sekundäre Citrix Gateway die Verbindung für eine bestimmte Zeit erneut, bis festgestellt wird, dass das primäre Gerät nicht funktioniert. Wenn das sekundäre Gerät den Fehler bei der Integritätsprüfung bestätigt, übernimmt das sekundäre Citrix Gateway die Kontrolle für das primäre Citrix Gateway. Dies wird als Failover bezeichnet.

Die folgenden Ports werden verwendet, um Informationen zur Hochverfügbarkeit zwischen Citrix Gateway-Appliances auszutauschen:

- Der UDP-Port 3003 wird verwendet, um Hallo-Pakete für die Kommunikation des Status für Intervalle auszutauschen.
- Der TCP-Port 3010 wird für die Synchronisierung der Hochverfügbarkeitskonfiguration verwendet.
- Der TCP-Port 3011 wird zur Synchronisierung von Konfigurationseinstellungen verwendet.

### Richtlinien für die Konfiguration von Hochverfügbarkeit

Bevor Sie ein Hochverfügbarkeitspaar konfigurieren, müssen Sie diese Richtlinien lesen:

- Auf jedem Citrix Gateway-Gerät muss dieselbe Version der Citrix Gateway-Software ausgeführt werden. Die Versionsnummer finden Sie oben auf der Seite im Konfigurationsdienstprogramm.
- Citrix Gateway synchronisiert Kennwörter nicht automatisch zwischen zwei Appliances. Sie können jedes Citrix Gateway mit dem Benutzernamen und dem Kennwort des anderen Geräts im Paar konfigurieren.
- Einträge in der Konfigurationsdatei ns.conf sowohl auf dem primären als auch auf dem sekundären Citrix Gateway müssen übereinstimmen, mit den folgenden Ausnahmen:

  - Das primäre und sekundäre Citrix Gateway-Gerät muss jeweils mit einer eigenen eindeutigen System-IP-Adresse konfiguriert werden. Verwenden Sie den Setup-Assistenten, um die System-IP-Adresse auf einem Citrix Gateway zu konfigurieren oder zu ändern.
  - In einem Hochverfügbarkeitspaar müssen die Citrix Gateway-ID und die zugehörige IP-Adresse auf das andere Citrix Gateway verweisen.

    Wenn Sie beispielsweise über zwei Appliances mit dem Namen AG1 und AG2 verfügen, müssen Sie AG1 mit der eindeutigen Citrix Gateway-ID und IP-Adresse von AG2 konfigurieren. Sie müssen AG2 mit der eindeutigen Citrix Gateway-ID und IP-Adresse von AG1 konfigurieren.

    Hinweis: Jedes Citrix Gateway-Gerät wird immer als Knoten 0 identifiziert. Konfigurieren Sie jede Appliance mit einer eindeutigen Knoten-ID.

- Jede Appliance im Hochverfügbarkeitspaar muss dieselbe Lizenz besitzen. Weitere Informationen zur Lizenzierung finden Sie unter Lizenzierung.
- Wenn Sie eine Konfigurationsdatei auf einem Knoten erstellen, indem Sie eine Methode verwenden, die nicht direkt über das Konfigurationsdienstprogramm oder die Befehlszeilenschnittstelle geht (z. B. das Importieren von SSL-Zertifikaten oder das Wechseln zu Start-Skripten), müssen Sie die Konfigurationsdatei auf den anderen Knoten kopieren oder einen identischen erstellen Datei auf diesem Knoten.
- Stellen Sie bei der Konfiguration eines Hochverfügbarkeitspaars sicher, dass die zugeordneten IP-Adressen und die Standard-Gateway-Adresse sowohl der primären als auch der sekundären Appliances identisch sind. Bei Bedarf können Sie die zugeordnete IP-Adresse jederzeit ändern, indem Sie den Setup-Assistenten ausführen.

Sie können die Checkliste vor der Installation verwenden, um eine Liste der spezifischen Einstellungen anzuzeigen, die Sie in einer Hochverfügbarkeitsbereitstellung konfigurieren müssen. Einzelheiten finden Sie unter Checkliste vor der Installation.

## Konfigurieren von Einstellungen für Hochverfügbarkeit

March 27, 2024

Um eine Hochverfügbarkeitskonfiguration einzurichten, erstellen Sie zwei Knoten, von denen jeder die Citrix Gateway-IP-Adresse des anderen als Remote-Knoten definiert. Sie können beginnen, indem Sie sich bei einer der beiden Citrix ADC Appliances anmelden, die Sie für Hochverfügbarkeit konfigurieren möchten, und einen Knoten hinzufügen. Geben Sie die Citrix Gateway-IP-Adresse des anderen Geräts als Adresse des neuen Knotens an. Melden Sie sich dann bei der anderen Appliance an und fügen Sie einen Knoten hinzu, der die Citrix Gateway-IP-Adresse des ersten Geräts enthält. Ein Algorithmus bestimmt, welcher Knoten primär und welcher sekundär wird.

Bevor Sie die Appliances konfigurieren, fügen Sie einen Hochverfügbarkeitsknoten hinzu. Dieser Knoten repräsentiert entweder das erste oder das zweite Citrix Gateway im Hochverfügbarkeitspaar. Um die Hochverfügbarkeit zu konfigurieren, erstellen Sie zuerst den Knoten und konfigurieren dann die Hochverfügbarkeitseinstellungen.

### So fügen Sie einen Hochverfügbarkeitsknoten hinzu

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **System > Hochverfügbarkeit**.
2. Klicken Sie im Detailbereich auf der Registerkarte Knoten auf **Hinzufügen**.
3. Geben Sie auf der Seite **HA-Knoten erstellen** im Textfeld **Remote-Knoten-IP-Adresse** die NSIP-Adresse des Citrix ADC ein, die als Remote-Knoten hinzugefügt werden soll. Wenn es sich bei der Citrix Gateway-IP-Adresse um eine IPv6-Adresse handelt, aktivieren Sie das Kontrollkästchen **IPv6**, bevor Sie die Adresse eingeben.
4. Wenn Sie den lokalen Knoten automatisch zum Remote-Knoten hinzufügen möchten, wählen Sie Remote-System konfigurieren, um am Hochverfügbarkeits-Setup teilzunehmen. Wenn Sie diese Option nicht auswählen, müssen Sie sich bei der Appliance anmelden, die durch den Remote-Knoten dargestellt wird, und den Knoten hinzufügen, den Sie gerade konfigurieren.
5. Klicken Sie hier, um die Option "**Ausschalten von HA Monitor-Schnittstellen/-kanälen" zu**aktivieren.
6. Wenn die Remote-Appliance über einen anderen Benutzernamen und ein anderes Kennwort verfügt, klicken Sie in Remote-System-Anmeldedaten auf Anmeldeinformationen für das Remote-System unterscheiden sich vom Selbstknoten.
7. **Geben Sie im Feld Benutzername den Benutzernamen der Remote-Appliance ein.**
8. Geben Sie unter **Kennwort**das Kennwort der Remote-Appliance ein.
9. Klicken Sie auf **OK**.

### So aktivieren oder deaktivieren Sie den sekundären Knoten

Sie können nur den sekundären Knoten deaktivieren oder aktivieren. Wenn Sie einen sekundären Knoten deaktivieren, sendet er keine Heartbeat-Nachrichten mehr an den primären Knoten, und daher kann der primäre Knoten den Status des sekundären Knotens nicht mehr überprüfen. Wenn Sie einen Knoten aktivieren, nimmt der Knoten an der Hochverfügbarkeitskonfiguration teil.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten den lokalen Knoten aus und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld HA Configure Node unter Hochverfügbarkeitsstatus die Option ENABLED (Nicht an HA teilnehmen).

4. Klicken Sie auf OK. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass der Knoten erfolgreich konfiguriert wurde.

### So konfigurieren Sie Einstellungen für Hochverfügbarkeit

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **System > Hochverfügbarkeit**.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten einen Knoten aus, und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie im Dialogfeld **HA Configure Node** in das Feld ID die Nummer der Node-ID ein. ID gibt die eindeutige Knotennummer für die andere Appliance an.
4. Geben Sie unter **IP-Adresse**die System-IP-Adresse ein und klicken Sie dann auf OK. Die IP-Adresse gibt die IP-Adresse der anderen Appliance an.

**Hinweis**: Die maximale ID für Knoten in einem Hochverfügbarkeitspaar beträgt 64.

## Ändern eines RPC-Knotenkennworts

March 27, 2024

Um mit anderen Citrix Gateway-Appliances zu kommunizieren, benötigt jede Appliance Kenntnisse der anderen Appliances, einschließlich der Authentifizierung auf Citrix Gateway. RPC-Knoten sind interne Systementitäten, die für die System-zu-System-Kommunikation von Konfigurations- und Sitzungsinformationen verwendet werden. Ein RPC-Knoten ist auf jedem Citrix Gateway vorhanden und speichert Informationen wie die IP-Adressen des anderen Citrix Gateway-Geräts und die für die Authentifizierung verwendeten Kennwörter. Das Citrix Gateway, das Kontakt mit einem anderen Citrix Gateway aufnimmt, überprüft das Kennwort innerhalb des RPC-Knotens.

Citrix Gateway erfordert RPC-Knotenkennwörter auf beiden Appliances in einem Hochverfügbarkeitspaar. Die Kennwörter müssen auf beiden Appliances identisch sein. Die primäre Appliance muss das Kennwort des sekundären RPC-Knotens kennen, und die sekundäre muss das Kennwort des primären RPC-Knotens kennen. Zu Beginn ist jedes Citrix Gateway mit demselben RPC-Knotenkennwort konfiguriert. Um die Sicherheit zu erhöhen, müssen Sie die standardmäßigen RPC-Knotenkennwörter ändern. Sie können das Konfigurationsdienstprogramm verwenden, um RPC-Knoten zu konfigurieren und zu ändern.

RPC-Knoten werden implizit erstellt, wenn ein Knoten hinzugefügt oder eine Global Server Load Balancing (GSLB) -Site hinzugefügt wird. Sie können RPC-Knoten nicht manuell erstellen oder löschen.

> **Wichtig:**
>
> Sie müssen auch die Netzwerkverbindung zwischen den Appliances sichern. Sie können die Sicherheit konfigurieren, wenn Sie das RPC-Knotenkennwort konfigurieren, indem Sie das Kontrollkästchen **Sicher** aktivieren.

### So ändern Sie ein RPC-Knotenkennwort und aktivieren eine sichere Verbindung

1. Navigieren Sie zu **System > Netzwerk > RPC .**
2. Wählen Sie im Detailbereich den Knoten aus und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie unter **Kennwort** und **Kennwort bestätigen**das neue Kennwort ein.
4. Geben Sie unter **Quell-IP-Adresse**die System-IP-Adresse des anderen Citrix Gateway-Geräts ein.
5. Klicken Sie auf **Sichern** und dann auf **OK**.

> **Hinweis:**
>
> Wenn Sie die Option **Sicher** aktivieren, verschlüsselt die Appliance die gesamte Kommunikation, die vom Knoten zu anderen RPC-Knoten gesendet wird, und sichert so die RPC-Kommunikation.

### So ändern Sie ein RPC-Knotenkennwort über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]

show ns rpcNode
<!--NeedCopy-->
```

**Beispiel:**

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>
<!--NeedCopy-->
```

# Konfiguration der primären und sekundären Appliances für Hochverfügbarkeit

March 27, 2024

Nachdem Sie das RPC-Knotenkennwort geändert und die sichere Kommunikation aktiviert haben, verwenden Sie das Konfigurationsdienstprogramm, um die primären und sekundären Citrix Gateway High Availability Knoten zu konfigurieren.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten einen Knoten aus und klicken Sie dann auf Bearbeiten.
3. Klicken Sie unter Hochverfügbarkeitsstatus auf Aktiviert (Aktiv an HA teilnehmen) und dann auf OK.

# Konfigurieren von Kommunikationsintervallen

March 27, 2024

Wenn Sie Citrix Gateway als Hochverfügbarkeitspaar konfigurieren, können Sie das sekundäre Citrix Gateway so konfigurieren, dass es in bestimmten Intervallen abhört, gemessen in Millisekunden (ms). Diese Intervalle werden als Hallo-Intervalle und Totintervalle bezeichnet.

Das Hallo-Intervall ist das Intervall, in dem die Heartbeat-Nachrichten an den Peer-Knoten gesendet werden. Das tote Intervall ist das Zeitintervall, nach dem der Peer-Knoten als DOWN markiert wird, wenn Heartbeat-Pakete nicht empfangen werden. Die Heartbeat-Nachrichten sind UDP-Pakete, die in einem Hochverfügbarkeitspaar an Port 3003 des anderen Knotens gesendet werden.

Wenn Sie das Hallo-Intervall konfigurieren, können Sie die Werte 200 bis 1000 verwenden. Der Standardwert beträgt 200. Die Werte des toten Intervalls liegen zwischen 3 und 60. Der Standardwert ist 3.

> **Hinweis**
>
> Das Totintervall muss als Vielfaches des Hallo-Intervalls festgelegt werden.

## So konfigurieren Sie Kommunikationsintervalle für das sekundäre Citrix Gateway

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.

2. Wählen Sie im Detailbereich auf der Registerkarte Knoten einen Knoten aus und klicken Sie dann auf Bearbeiten.
3. Führen Sie unter Intervalle eine oder beide der folgenden Aktionen aus:

    - Geben Sie in Hello Interval (ms) den Wert ein und klicken Sie dann auf OK. Der Standardwert beträgt 200 Millisekunden.
    - Geben Sie unter Dead Interval (Sekunden) den Wert ein und klicken Sie dann auf OK. Die Standardeinstellung beträgt drei Sekunden.

## Citrix Gateway-Geräte synchronisieren

March 27, 2024

Die automatische Synchronisierung von Citrix Gateway-Appliances in einem Hochverfügbarkeitspaar ist standardmäßig aktiviert. Mit der automatischen Synchronisierung können Sie Änderungen an einer Appliance vornehmen und aktivieren, dass die Änderungen automatisch auf die zweite Appliance übertragen werden. Bei der Synchronisierung wird Port 3010 verwendet.

Die Synchronisierung beginnt, wenn Folgendes eintritt:

- Der sekundäre Knoten wird neu gestartet.
- Der primäre Knoten wird nach einem Failover sekundär.

Sie können die Synchronisierung deaktivieren, wodurch verhindert wird, dass das sekundäre Citrix Gateway seine Konfiguration mit dem primären Citrix Gateway synchronisiert, wenn eine Änderung auf dem primären Gerät auftritt. Sie können auch die Synchronisierung erzwingen.

Sie aktivieren oder deaktivieren die Hochverfügbarkeitssynchronisierung auf dem sekundären Knoten im Paar.

### So aktivieren oder deaktivieren Sie die Hochverfügbarkeitssynchronisierung

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten einen Knoten aus und klicken Sie dann auf Bearbeiten.
3. Führen Sie im Dialogfeld Knoten konfigurieren unter HA-Synchronisierung einen der folgenden Schritte aus:

    - Um die Synchronisierung zu deaktivieren, deaktivieren Sie das Kontrollkästchen Sekundärer Knoten ruft die Konfiguration von Primär ab.

- Um die Synchronisierung zu aktivieren, aktivieren Sie das Kontrollkästchen Sekundärer Knoten holt die Konfiguration von Primär ab.

4. Klicken Sie auf OK. In der Statusleiste wird eine Meldung angezeigt, dass die Knotenkonfiguration erfolgreich ist.

### So erzwingen Sie die Synchronisierung zwischen

Zusätzlich zur automatischen Synchronisierung unterstützt Citrix Gateway die erzwungene Synchronisierung zwischen den beiden Knoten in einem Hochverfügbarkeitspaar.

Sie können die Synchronisierung sowohl auf den primären als auch auf sekundären Citrix Gateway-Appliances Wenn die Synchronisierung jedoch bereits ausgeführt wird, schlägt der Befehl fehl und Citrix Gateway zeigt eine Warnung an. Die erzwungene Synchronisierung schlägt auch unter folgenden Umständen fehl:

- Sie erzwingen die Synchronisierung auf einem eigenständigen System.
- Der sekundäre Knoten ist deaktiviert.
- Sie deaktivieren die Hochverfügbarkeitssynchronisierung auf dem sekundären Knoten.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Klicken Sie auf der Registerkarte Knoten auf Synchronisierung erzwingen.

## Synchronisieren von Konfigurationsdateien in einer Hochverfügbarkeitseinrichtung

March 27, 2024

In einem Hochverfügbarkeits-Setup können Sie verschiedene Konfigurationsdateien vom primären Knoten bis zum sekundären Knoten synchronisieren.

### Parameter zum Synchronisieren von Dateien in einem Hochverfügbarkeits-Setup

- Modus

  Die Art der durchzuführenden Synchronisierung. Die folgenden Beschreibungen enthalten in Klammern das Befehlszeilenargument, das die Option angibt.

- **Alles außer Lizenzen und rc.conf** (alle). Synchronisiert Dateien im Zusammenhang mit der Systemkonfiguration, Citrix Gateway-Lesezeichen, SSL-Zertifikaten, SSL-CRL-Listen, HTML-Injection-Skripts und Anwendungsfirewall-XML-Objekten.
- **Lesezeichen** (Lesezeichen). Synchronisiert alle Citrix Gateway-Lesezeichen.
- **SSL-Zertifikate und Schlüssel** (`ssl`). Synchronisiert alle Zertifikate, Schlüssel und CRLs für die SSL-Funktion.
- **Lizenzen und rc.conf** (misc). Synchronisiert alle Lizenzdateien und die Datei rc.conf.
- **Alles einschließlich Lizenzen und rc.conf** (all_plus_misc). Synchronisiert Dateien im Zusammenhang mit der Systemkonfiguration, Citrix Gateway-Lesezeichen, SSL-Zertifikaten, SSL-CRL-Listen, HTML-Injection-Skripts, XML-Objekten der Anwendungsfirewall, Lizenzen und der Datei rc.conf.

Hinweis: Wenn Sie eine Citrix ADC-Lizenz auf der Appliance installieren, stehen weitere Optionen zur Verfügung.

### So synchronisieren Sie Dateien in einem Hochverfügbarkeits-Setup mithilfe des Konfigurationsdienstprogramms

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Diagnose**.
2. Klicken Sie im Detailbereich unter **Dienstprogramme**auf **HA-Dateisynchronisierung starten**.
3. Wählen Sie im Dialogfeld **Dateisynchronisierung starten** im Menü **Modus** den entsprechenden Synchronisationstyp aus (z. B. Alles außer Lizenzen und rc.conf), und klicken Sie dann auf **OK**.

## Konfigurieren der Befehlsausbreitung

March 27, 2024

In einem Hochverfügbarkeits-Setup wird jeder auf dem primären Knoten ausgegebene Befehl automatisch an den sekundären Knoten weitergegeben und auf diesem ausgeführt, bevor der Befehl auf dem primären Knoten ausgeführt wird. Wenn die Befehlsweitergabe fehlschlägt oder die Befehlsausführung auf dem sekundären Knoten fehlschlägt, führt der primäre Knoten den Befehl aus und protokolliert einen Fehler. Die Befehlsausbreitung verwendet Port 3011.

In einer Paarkonfiguration mit hoher Verfügbarkeit ist die Befehlsübertragung standardmäßig sowohl auf dem primären als auch auf dem sekundären Knoten aktiviert. Sie können die Befehlsweitergabe auf beiden Knoten in einem Hochverfügbarkeitspaar aktivieren oder deaktivieren. Wenn Sie die Befehlsübertragung auf dem primären Knoten deaktivieren, werden Befehle nicht an den sekundären Knoten weitergegeben. Wenn Sie die Befehlsübertragung auf dem sekundären Knoten deaktivieren,

werden Befehle, die vom primären Knoten weitergegeben werden, nicht auf dem sekundären Knoten ausgeführt.

Hinweis: Denken Sie nach dem erneuten Aktivieren der Weitergabe daran, die Synchronisierung zu erzwingen

Hinweis: Wenn die Synchronisierung stattfindet, während Sie die Propagierung deaktivieren, werden alle konfigurationsbezogenen Änderungen, die Sie vor dem Inkrafttreten der Deaktivierung der Propagierung vornehmen, mit dem sekundären Knoten synchronisiert. Dies gilt auch für Fälle, in denen die Propagierung während der laufenden Synchronisierung deaktiviert ist.

### So aktivieren oder deaktivieren Sie die Propagierung auf dem primären Knoten

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option **System** und klicken Sie dann auf **Hochverfügbarkeit**.
2. Wählen Sie im Detailbereich auf der Registerkarte **Knoten** einen Knoten aus, und klicken Sie dann auf **Bearbeiten**.
3. Führen Sie unter **HA-Propagierung**einen der folgenden Schritte aus:
    - Um die Weitergabe von Hochverfügbarkeit zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Primärer Knoten überträgt Konfiguration an Sekundär**.
    - Um die Hochverfügbarkeitsweitergabe zu aktivieren, aktivieren Sie das Kontrollkästchen **Primärer Knoten überträgt Konfiguration an Sekundär**.
4. Klicken Sie auf **OK**.

## Fehlerbehebung bei der Befehlsausbreitung

March 27, 2024

In der folgenden Liste werden die Gründe beschrieben, warum die Befehlsweitergabe fehlschlagen könnte, und Lösungen für die Wiederherstellung der Einstellung:

- Die Netzwerkkonnektivität ist nicht aktiv. Wenn eine Befehlsübertragung fehlschlägt, überprüfen Sie die Netzwerkverbindung zwischen den primären und sekundären Citrix Gateway-Geräten.
- Fehlende Ressourcen auf sekundärem Citrix Gateway. Wenn eine Befehlsausführung auf dem primären Citrix Gateway erfolgreich ist, sich jedoch nicht an das sekundäre Citrix Gateway weiterleitet, führen Sie den Befehl direkt auf dem sekundären Citrix Gateway aus, um die Fehlermeldung anzuzeigen. Der Fehler ist möglicherweise aufgetreten, weil die für den Befehl erforderlichen Ressourcen auf dem primären Citrix Gateway vorhanden sind und auf dem sekundären

Citrix Gateway nicht verfügbar sind. Stellen Sie außerdem sicher, dass die Lizenzdateien auf jeder Appliance übereinstimmen.

Stellen Sie beispielsweise sicher, dass alle Ihre Secure Sockets Layer (SSL) -Zertifikate auf jedem Citrix Gateway vorhanden sind. Stellen Sie sicher, dass auf beiden Citrix Gateway-Geräten eine Initialisierungsskriptanpassung vorhanden ist

- Die Authentifizierung schlägt fehl. Wenn Sie eine Fehlermeldung über einen Authentifizierungsfehler erhalten, überprüfen Sie die RPC-Knoteneinstellungen auf jeder Appliance.

## Konfigurieren des ausfallsicheren Modus

January 29, 2024

In einer Hochverfügbarkeitskonfiguration stellt der ausfallsichere Modus sicher, dass ein Knoten immer primär ist, wenn beide Knoten die Integritätsprüfung nicht bestehen. Der ausfallsichere Modus stellt sicher, dass Backup-Methoden Datenverkehr aktivieren und verarbeiten können, wenn ein Knoten nur teilweise verfügbar ist.

Sie konfigurieren den ausfallsicheren Hochverfügbarkeitsmodus unabhängig auf jedem Knoten.

Die folgende Tabelle zeigt einige der ausfallsicheren Fälle. Der Status NOT_UP bedeutet, dass der Knoten die Zustandsprüfung nicht bestanden hat und der Knoten dennoch teilweise verfügbar ist. Der UP-Status bedeutet, dass der Knoten die Zustandsprüfung bestanden hat.

Tabelle 1. Fälle im ausfallsicheren Modus

| Gesundheitszustand von Knoten A (primär) | Gesundheitszustand von Knoten B (sekundär) | Standardverhalten bei hoher Verfügbarkeit | Ausfallsicheres aktiviertes Hochverfügbarkeitsverhalten | Beschreibung |
|---|---|---|---|---|
| NOT_UP (zuletzt fehlgeschlagen) | NOT_UP (ist zuerst fehlgeschlagen) | A (Sekundär), B (Sekundär) | A (Primär), B (Sekundär) | Wenn beide Knoten nacheinander ausfallen, bleibt der Knoten, der der letzte primäre Knoten war, primär. |

| Gesundheitszustand von Knoten A (primär) | Gesundheitszustand von Knoten B (sekundär) | Standardverhalten bei hoher Verfügbarkeit | Ausfallsicheres aktiviertes Hochverfügbarkeitsverhalten | Beschreibung |
|---|---|---|---|---|
| NOT_UP (ist zuerst fehlgeschlagen) | NOT_UP (zuletzt fehlgeschlagen) | A (Sekundär), B (Sekundär) | A (Sekundär), B (Primär) | Wenn beide Knoten nacheinander ausfallen, bleibt der Knoten, der der letzte primäre Knoten war, primär. |
| UP | UP | A (Primär), B (Sekundär) | A (Primär), B (Sekundär) | Wenn beide Knoten die Integritätsprüfung bestehen, ändert sich das Verhalten bei aktiviertem Failsafe nicht. |
| UP | NOT_UP | A (Primär), B (Sekundär) | A (Primär), B (Sekundär) | Wenn nur der sekundäre Knoten ausfällt, ändert sich das Verhalten bei aktiviertem Failsafe nicht. |
| NOT_UP | UP | A (Sekundär), B (Primär) | A (Sekundär), B (Primär) | Wenn nur der Primärbereich ausfällt, ändert sich das Verhalten bei aktivierter Failsafe nicht. |

| Gesundheitszustand von Knoten A (primär) | Gesundheitszustand von Knoten B (sekundär) | Standardverhalten bei hoher Verfügbarkeit | Ausfallsicheres aktiviertes Hochverfügbarkeitsverhalten | Beschreibung |
|---|---|---|---|---|
| NOT_UP | UP (STAYSECONDARY) | A (Sekundär), B (Sekundär) | A (Primär), B (Sekundär) | Wenn die Sekundärstufe als STAYSECONDARY konfiguriert ist, bleibt die Primärstufe auch dann primär, wenn sie ausfällt. |

### So konfigurieren Sie den ausfallsicheren Modus

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten einen Knoten aus und klicken Sie dann auf Bearbeiten.
3. Wählen Sie im Dialogfeld Knoten konfigurieren unter Fail-Safe-Modus die Option Einen primären Knoten beibehalten, auch wenn beide Knoten ungesund sind, und klicken Sie dann auf OK.

## Konfigurieren der virtuellen MAC-Adresse

March 27, 2024

Die virtuelle MAC-Adresse wird von den primären und sekundären Citrix Gateway-Geräten in einem Hochverfügbarkeits-Setup gemeinsam genutzt.

In einem Hochverfügbarkeits-Setup besitzt das primäre Citrix Gateway alle Floating-IP-Adressen, z. B. die zugeordnete IP-Adresse oder die virtuelle IP-Adresse. Es reagiert auf Anfragen des Adressauflösungsprotokolls (ARP) für diese IP-Adressen mit einer eigenen MAC-Adresse. Infolgedessen wird die ARP-Tabelle eines externen Geräts (z. B. eines Routers) mit der Floating-IP und der primären Citrix Gateway MAC-Adresse aktualisiert. Wenn ein Failover auftritt, übernimmt das sekundäre Citrix Gateway die Kontrolle als neues primäres Citrix Gateway. Anschließend verwendet es das Gratuitous Address Resolution Protocol (GARP), um die Floating-IP-Adressen anzukündigen, die es von der primären

Appliance erworben hat. Die MAC-Adresse, die das neue primäre Gerät ankündigt, ist die seiner eigenen Schnittstelle.

Einige Geräte akzeptieren keine von Citrix Gateway generierten GARP-Nachrichten. Infolgedessen behalten einige der externen Geräte die alte IP-zu-Mac-Zuordnung bei, die vom alten primären Citrix Gateway angekündigt wurde. Diese Situation kann dazu führen, dass eine Website nicht mehr verfügbar ist. Um das Problem zu beheben, konfigurieren Sie eine virtuelle MAC-Adresse auf beiden Citrix Gateway-Appliances eines Hochverfügbarkeitspaars. Diese Konfiguration impliziert, dass beide Citrix Gateway-Appliances identische MAC-Adressen haben. Daher bleibt bei einem Failover die MAC-Adresse des sekundären Citrix Gateway unverändert und ARP-Tabellen auf den externen Geräten müssen nicht aktualisiert werden.

Um eine virtuelle MAC-Adresse zu erstellen, erstellen Sie eine virtuelle Router-ID (ID) und binden Sie sie an eine Schnittstelle. In einem Hochverfügbarkeits-Setup muss der Benutzer die ID an die Schnittstellen beider Appliances binden.

Wenn die ID des virtuellen Routers an eine Schnittstelle gebunden ist, generiert das System eine virtuelle MAC-Adresse mit der ID des virtuellen Routers als letztes Oktett. Ein Beispiel für die generische virtuelle MAC-Adresse ist 00:00:5e:00:01:<VRID>. Wenn Sie beispielsweise eine virtuelle Router-ID mit dem Wert 60 erstellt und an eine Schnittstelle gebunden haben, lautet die resultierende virtuelle MAC-Adresse 00:00:5 e: 00:01:3 c, wobei 3c die Hexadezimaldarstellung der virtuellen Router-ID ist. Sie können 255 virtuelle Router-IDs im Bereich von 1 bis 254 erstellen.

Sie können virtuelle MAC-Adressen für IPv4 und IPv6 konfigurieren.

## Konfigurieren virtueller IPv4-MAC-Adressen

January 29, 2024

Wenn Sie eine virtuelle IPv4-MAC-Adresse erstellen und an eine Schnittstelle binden, verwendet jedes IPv4-Paket, das von der Schnittstelle gesendet wird, die virtuelle MAC-Adresse, die an die Schnittstelle gebunden ist. Wenn keine virtuelle IPv4-MAC-Adresse an eine Schnittstelle gebunden ist, wird die physische MAC-Adresse der Schnittstelle verwendet.

Die generische virtuelle MAC-Adresse hat die Form 00:00:5e:00:01:<VRID>. Wenn Sie beispielsweise eine VRID mit einem Wert von 60 erstellen und an eine Schnittstelle binden, lautet die resultierende virtuelle MAC-Adresse 00:00:5e:00:01:3c, wobei 3c die Hexadezimaldarstellung der VRID ist. Sie können 255 VRIDs mit Werten von 1 bis 255 erstellen.

# Erstellen oder Ändern einer virtuellen IPv4-MAC-Adresse

March 27, 2024

Sie erstellen eine virtuelle IPv4-MAC-Adresse, indem Sie ihr eine virtuelle Router-ID zuweisen. Sie können dann die virtuelle MAC-Adresse an eine Schnittstelle binden. Sie können nicht mehrere virtuelle Router-IDs an dieselbe Schnittstelle binden. Um die Konfiguration der virtuellen MAC-Adresse zu überprüfen, müssen Sie die virtuelle MAC-Adresse und die an die virtuelle MAC-Adresse gebundenen Schnittstellen anzeigen und untersuchen.

## Parameter für die Konfiguration einer virtuellen MAC-Adresse

- VrID

  Die ID des virtuellen Routers, die die virtuelle MAC-Adresse identifiziert. Mögliche Werte: 1—255.

- `ifnum`

  Die Schnittstellennummer (Steckplatz/Portnotation), die an die virtuelle MAC-Adresse gebunden werden soll.

## So konfigurieren Sie eine virtuelle MAC-Adresse

1. Navigieren Sie zu **System > Netzwerk** und klicken Sie dann auf **VMAC**.
2. Klicken Sie im Detailbereich auf der Registerkarte **VMAC** auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Create VMAC unterVirtual Router ID**den Wert ein.
4. Wählen Sie unter **Zugehörige Schnittstellen** unter **Verfügbare Schnittstellen** eine Netzwerkschnittstelle aus, klicken Sie auf **Hinzufügen**, klicken Sie auf **Erstellen** und dann auf **Schließen**.

Nachdem Sie die virtuelle MAC-Adresse erstellt haben, wird sie im Konfigurationsdienstprogramm angezeigt. Wenn Sie eine Netzwerkschnittstelle ausgewählt haben, ist die ID des virtuellen Routers an diese Schnittstelle gebunden.

## So löschen Sie eine virtuelle MAC-Adresse

Um eine virtuelle MAC-Adresse zu löschen, müssen Sie die entsprechende virtuelle Router-ID löschen.

1. Navigieren Sie zu **System > Netzwerk,** und klicken Sie dann auf **VMAC**.
2. Wählen Sie im Detailbereich ein Element aus und klicken Sie dann auf **Entfernen**.

### So binden und lösen Sie eine virtuelle MAC-Adresse

Als Sie die ID des virtuellen Routers erstellt haben, haben Sie eine Netzwerkschnittstelle auf Citrix Gateway ausgewählt und dann die ID des virtuellen Routers an die Netzwerkschnittstelle gebunden. Sie können auch eine virtuelle MAC-Adresse von der Netzwerkschnittstelle trennen, aber die MAC-Adresse auf Citrix Gateway konfiguriert lassen.

1. Navigieren Sie zu **System > Netzwerk** und klicken Sie dann auf **VMAC**.
2. Wählen Sie im Detailbereich ein Element aus, und klicken Sie dann auf **Öffnen**.
3. Wählen Sie unter **Konfigurierte Schnittstellen** eine Netzwerkschnittstelle aus, klicken Sie auf **Entfernen**, klicken Sie auf **OK** und dann auf **Schließen**.

## Virtuelle IPv6-MAC-Adressen konfigurieren

March 27, 2024

Das Citrix Gateway unterstützt virtuelle MAC-Adressen für IPv6-Pakete. Sie können jede Schnittstelle an eine virtuelle MAC-Adresse für IPv6 binden, auch wenn eine virtuelle IPv4-MAC-Adresse an die Schnittstelle gebunden ist. Jedes IPv6-Paket, das von der Schnittstelle gesendet wird, verwendet die virtuelle MAC-Adresse, die an diese Schnittstelle gebunden ist. Wenn keine virtuelle MAC-Adresse an eine Schnittstelle gebunden ist, verwendet ein IPv6-Paket den physischen MAC.

## Erstellen oder Ändern einer virtuellen MAC-Adresse für IPv6

March 27, 2024

Erstellen Sie eine virtuelle IPv6-MAC-Adresse, indem Sie ihr eine virtuelle IPv6-Router-ID zuweisen. Binden Sie dann die virtuelle MAC-Adresse an eine Schnittstelle. Sie können nicht mehrere IPv6-IDs des virtuellen Routers an eine Schnittstelle binden. Um die Konfiguration der virtuellen MAC-Adresse zu überprüfen, zeigen und überprüfen Sie die virtuellen MAC-Adressen und die an die virtuelle MAC-Adresse gebundenen Schnittstellen.

### Parameter für die Konfiguration einer virtuellen MAC-Adresse für IPv6

- `Virtual Router ID`

  Die ID des virtuellen Routers, die die virtuelle MAC-Adresse identifiziert. Mögliche Werte: 1—255.

- `ifnum`

  Die Schnittstellennummer (Steckplatz/Portnotation), die an die virtuelle MAC-Adresse gebunden werden soll.

### So konfigurieren Sie eine virtuelle MAC-Adresse für IPv6

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **System > Netzwerk** und klicken Sie dann auf VMAC.
2. Führen Sie im Detailbereich auf der Registerkarte VMAC6 einen der folgenden Schritte aus:
   - Um eine neue virtuelle MAC-Adresse zu erstellen, klicken Sie auf Hinzufügen.
   - Um eine vorhandene virtuelle MAC-Adresse zu ändern, klicken Sie auf Öffnen.
3. Geben Sie im Dialogfeld VMAC6 erstellen oder VMAC6 konfigurieren unter Virtual Router ID den Wert ein, z. B. vRID6.
4. Klicken Sie in Verknüpfen von Schnittstellen auf **Hinzufügen > Erstellen > Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die virtuelle MAC-Adresse konfiguriert ist.

### So entfernen Sie eine virtuelle MAC-Adresse für IPv6

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **System > Netzwerk** und klicken Sie dann auf VMAC.
2. Wählen Sie im Detailbereich auf der Registerkarte VMAC6 die ID des virtuellen Routers aus, die Sie entfernen möchten, und klicken Sie dann auf Entfernen. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die virtuelle MAC-Adresse entfernt wurde.

## Konfigurieren von Hochverfügbarkeitspaaren in verschiedenen Subnetzen

March 27, 2024

Eine typische Bereitstellung mit hoher Verfügbarkeit liegt vor, wenn sich beide Appliances in einem Hochverfügbarkeitspaar im selben Subnetz befinden. Eine Hochverfügbarkeitsbereitstellung kann auch aus zwei Citrix Gateway-Appliances bestehen, in denen sich jedes Gerät in einem anderen Netzwerk befindet. In diesem Thema wird die letztere Konfiguration beschrieben und enthält Beispielkonfigurationen und eine Liste von Unterschieden zwischen den Hochverfügbarkeitskonfigurationen innerhalb eines Netzwerks und über Netzwerke hinweg.

Sie können auch Link-Redundanz und Routenmonitore konfigurieren. Diese Citrix Gateway-Funktionen sind in einer netzwerkübergreifenden Hochverfügbarkeitskonfiguration hilfreich. Die Funktionen decken auch den Prozess der Zustandsprüfung ab, der von jedem Citrix Gateway verwendet wird, um sicherzustellen, dass das Partnergerät aktiv ist.

### So funktioniert die unabhängige Netzwerkkonfiguration

Die Citrix Gateway-Geräte sind mit verschiedenen Routern, R3 und R4 genannt, in zwei verschiedenen Netzwerken verbunden. Die Appliances tauschen Heartbeat-Pakete über diese Router aus. Ein Heartbeat-Paket ist ein Signal, das in regelmäßigen Abständen auftritt und sicherstellt, dass die Verbindung weiterhin aktiv ist. Sie können diese Konfiguration erweitern, um Bereitstellungen mit einer beliebigen Anzahl von Schnittstellen zu ermöglichen.

Hinweis: Wenn Sie statisches Routing in Ihrem Netzwerk verwenden, müssen Sie statische Routen zwischen allen Systemen hinzufügen, um sicherzustellen, dass Heartbeat-Pakete erfolgreich gesendet und empfangen werden. (Wenn Sie dynamisches Routing auf Ihren Systemen verwenden, sind statische Routen nicht erforderlich.)

Wenn sich die Appliances in einem Hochverfügbarkeitspaar in zwei verschiedenen Netzwerken befinden, muss das sekundäre Citrix Gateway über eine unabhängige Netzwerkkonfiguration verfügen. Dies bedeutet, dass Citrix Gateway-Appliances in verschiedenen Netzwerken keine zugeordneten IP-Adressen, virtuellen LANs oder Netzwerkrouten gemeinsam nutzen können. Diese Art der Konfiguration, bei der die Citrix Gateway-Appliances in einem Hochverfügbarkeitspaar unterschiedliche konfigurierbare Parameter aufweisen, wird als unabhängige Netzwerkkonfiguration oder symmetrische Netzwerkkonfiguration bezeichnet.

Die folgende Tabelle fasst die konfigurierbaren Parameter für eine unabhängige Netzwerkkonfiguration zusammen und zeigt, wie Sie sie auf jedem Citrix Gateway festlegen müssen:

| Konfigurierbare Parameter | Ergebnis |
|---|---|
| IP-Adressen | Citrix Gateway spezifisch. Nur auf diesem Gerät aktiv. |
| Virtuelle IP-Adresse | Floating. |
| Virtuelles LAN | Citrix Gateway spezifisch. Nur auf diesem Gerät aktiv. |
| Routen | Citrix Gateway spezifisch. Nur auf diesem Gerät aktiv. Eine Route des Link-Lastausgleichs (LLB) ist floating. |
| Zugriffssteuerungslisten (ACLs) | Floating (üblich). Aktiv auf beiden Geräten. |

| Konfigurierbare Parameter | Ergebnis |
| --- | --- |
| Dynamisches Routing | Citrix Gateway spezifisch. Nur auf diesem Gerät aktiv. Das sekundäre Citrix Gateway muss auch die Routingprotokolle und Peer mit Upstream-Routern ausführen. |
| L2-Modus | Floating (üblich). Aktiv auf beiden Geräten. |
| L3-Modus | Floating (üblich). Aktiv auf beiden Geräten. |
| Umgekehrte Netzwerkadressübersetzung (NAT) | Citrix Gateway spezifisch. Reverse NAT mit einer virtuellen IP-Adresse, da die NAT-IP-Adresse variabel ist. |

> **Hinweis:**
>
> IPSET im INC-Modus wird mit öffentlichen IP-Adressen unterstützt. Einzelheiten finden Sie unter Citrix ADC Hochverfügbarkeit mit Azure Load Balancer Front-End-IP-validiertes Referenzdesign.

## Hinzufügen eines Remote-Knotens

March 27, 2024

Wenn sich zwei Knoten eines Hochverfügbarkeitspaars in verschiedenen Subnetzen befinden, muss jeder Knoten über eine andere Netzwerkkonfiguration verfügen. Um zwei unabhängige Systeme so zu konfigurieren, dass sie als Hochverfügbarkeitspaar fungieren, müssen Sie daher während des Konfigurationsvorgangs einen unabhängigen Netzwerk-Computing-Modus angeben.

Wenn Sie einen Hochverfügbarkeitsknoten hinzufügen, müssen Sie den Hochverfügbarkeitsmonitor für jede Schnittstelle deaktivieren, die nicht verbunden ist oder für den Verkehr verwendet wird.

### So fügen Sie einen Remote-Knoten für den unabhängigen Netzwerk-Rechenmodus hinzu

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **System > Hochverfügbarkeit**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Knoten** und dann auf **Hinzufügen**.
3. Geben Sie im Dialogfeld Hochverfügbarkeits-Setup im Textfeld **Remote-Knoten-IP-Adresse** die Citrix Gateway-IP-Adresse der Appliance ein, bei der es sich um den Remote-Knoten handelt.

Um eine IPv6-Adresse zu verwenden, aktivieren Sie das Kontrollkästchen **IPv6**, bevor Sie die IP-Adresse eingeben.

4. Wenn Sie den lokalen Knoten automatisch zum Remote-Knoten hinzufügen möchten, wählen Sie Remote-System konfigurieren, um am Hochverfügbarkeits-Setup teilzunehmen. Wenn Sie diese Option nicht auswählen, müssen Sie sich bei der Appliance anmelden, die durch den Remote-Knoten dargestellt wird, und den Knoten hinzufügen, den Sie gerade konfigurieren.
5. Klicken Sie hier, um einen klaren HA-Monitor auf ausfallenden Schnittstellen/Kanälen zu aktivieren.
6. Klicken Sie hier, um den Modus "INC einschalten"(Independent Network Configuration) im Selbstmodus zu aktivieren.
7. Klicken Sie auf **OK**. Auf der Seite **Knoten** werden die lokalen und Remote-Knoten in Ihrer Hochverfügbarkeitskonfiguration angezeigt.

### So entfernen Sie einen Remote-Knoten

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **System > Hochverfügbarkeit**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Knoten**.
3. Wählen Sie den Knoten aus, den Sie entfernen möchten, klicken Sie auf **Entfernen** und dann auf **Ja**.

## Konfigurieren von Routenmonitoren

March 27, 2024

Sie können Routenmonitore verwenden, um den Hochverfügbarkeitsstatus von der internen Routingtabelle abhängig zu machen, unabhängig davon, ob die Tabelle dynamisch erlernte oder statische Routen enthält. In einer Hochverfügbarkeitskonfiguration überprüft ein Routenmonitor auf jedem Knoten die interne Routingtabelle, um sicherzustellen, dass immer ein Routeneintrag zum Erreichen eines bestimmten Netzwerks vorhanden ist. Wenn der Routeneintrag nicht vorhanden ist, ändert sich der Status des Routenmonitors auf DOWN.

Wenn ein Citrix Gateway-Gerät nur über statische Routen zum Erreichen eines Netzwerks verfügt und Sie einen Routenmonitor für das Netzwerk erstellen möchten, müssen Sie überwachte statische Routen für die statischen Routen aktivieren. Die überwachte statische Route entfernt unerreichbare statische Routen aus der internen Routingtabelle. Wenn Sie überwachte statische Routen auf statischen Routen deaktivieren, kann eine nicht erreichbare statische Route in der internen Routingtabelle verbleiben, wodurch der Zweck der Routenüberwachung zunichte gemacht wird.

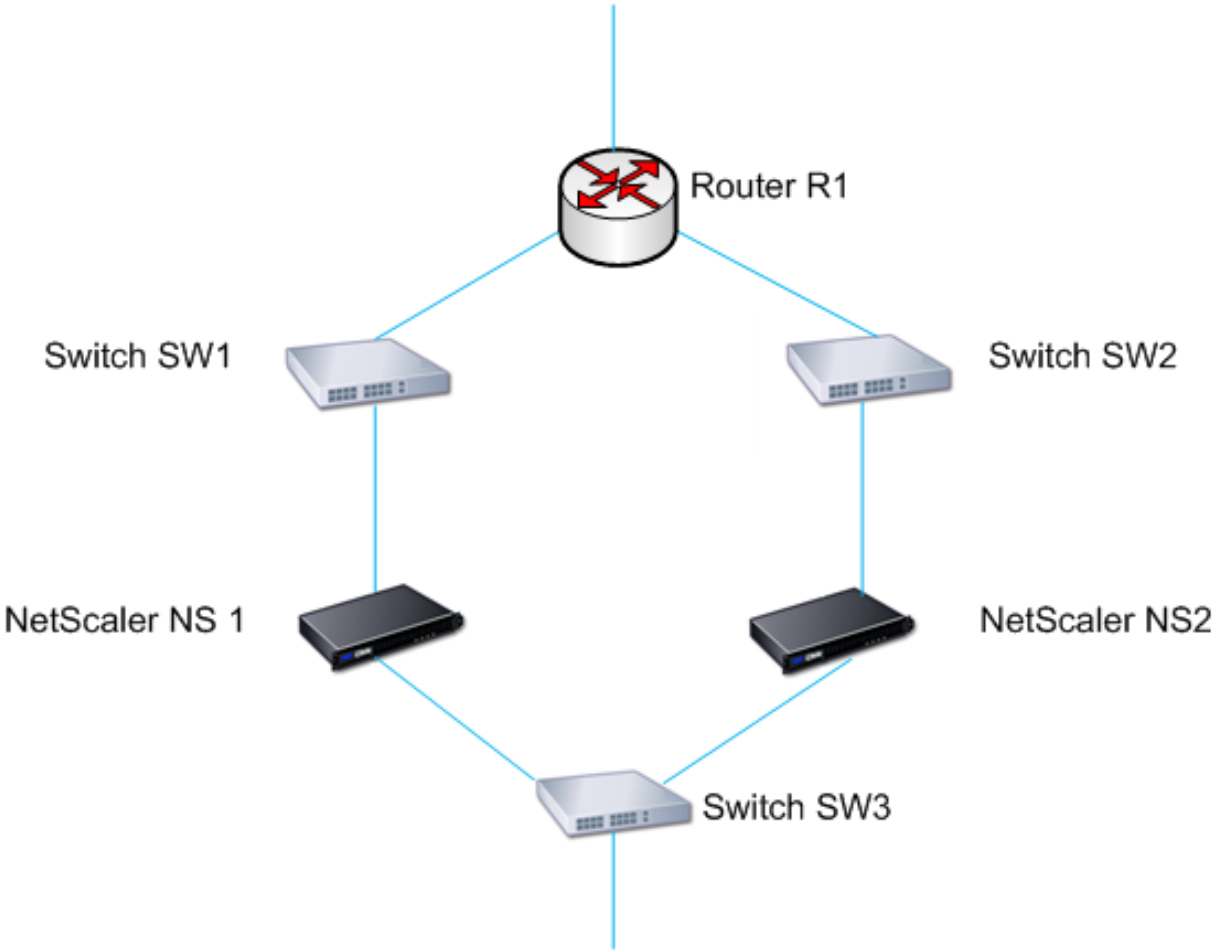
Routenmonitore werden entweder für aktivierte oder deaktivierte Einstellungen für unabhängige Netzwerkkonfiguration unterstützt. Die folgende Tabelle zeigt, was bei Routenmonitoren in einem Hochverfügbarkeits-Setup und bei aktivierter oder deaktivierter unabhängiger Netzwerkkonfiguration geschieht.

| Routing Monitore in Hochverfügbarkeit im deaktivierten unabhängigen Netzwerkkonfigurationsmodus | Routen von Monitoren in Hochverfügbarkeit im aktivierten unabhängigen Netzwerkkonfigurationsmodus |
|---|---|
| Routenmonitore werden von Knoten weitergegeben und während der Synchronisierung ausgetauscht. | Routenmonitore werden während der Synchronisation weder von Knoten weitergegeben noch ausgetauscht. |
| Routenmonitore sind nur im aktuellen primären Knoten aktiv. | Routenmonitore sind sowohl auf dem primären als auch auf dem sekundären Knoten aktiv. |
| Das Citrix Gateway-Gerät zeigt den Status eines Routenmonitors immer als UP an, unabhängig davon, ob der Routeneintrag in der internen Routingtabelle vorhanden ist oder nicht. | Das Citrix Gateway-Gerät zeigt den Status des Routenmonitors als DOWN an, wenn der entsprechende Routeneintrag nicht in der internen Routingtabelle vorhanden ist. |
| Ein Routenmonitor beginnt in den folgenden Fällen mit der Überwachung seiner Route, damit Citrix Gateway die dynamischen Routen erlernen kann, was bis zu 180 Sekunden dauern kann: Neustart, Failover, Festlegen des Befehls route6 für v6-Routen, Festlegen des Befehls zum `msr` Aktivieren/Deaktivieren von Route für v4-Routen, Hinzufügen eines neuen Routenmonitors | Nicht verfügbar |

Routenmonitore sind nützlich, wenn Sie den Modus “Unabhängige Netzwerkkonfiguration”deaktivieren und ein Gateway von einem primären Knoten wünschen, das so unerreichbar ist wie eine der Bedingungen für ein Failover mit hoher Verfügbarkeit.

Beispielsweise deaktivieren Sie die unabhängige Netzwerkkonfiguration in einem Hochverfügbarkeits-Setup in einer zweiarmigen Topologie, die Citrix Gateway-Appliances NS1 und NS2 im selben Subnetz hat, mit Router R1 und Switches SW1, SW2 und SW3, wie in der folgenden Abbildung dargestellt. Da R1 der einzige Router in diesem Setup ist, möchten Sie, dass das Hochverfügbarkeits-Setup immer dann ausfällt, wenn R1 vom aktuellen Primärknoten aus nicht erreichbar ist. Sie können einen Routenmonitor (z. B. RM1 bzw. RM2) auf jedem der Knoten konfigurieren, um die Erreichbarkeit von R1 von diesem Knoten aus zu überwachen.




Mit NS1 als aktuellem primären Knoten ist der Netzwerkfluss wie folgt:

1. Der Routenmonitor RM1 auf NS1 überwacht die interne Routingtabelle von NS1 auf das Vorhandensein eines Routeneintrags für Router R1. NS1 und NS2 tauschen in regelmäßigen Abständen Heartbeat-Nachrichten über den Switch SW1 oder SW3 aus.
2. Wenn Switch SW1 ausfällt, erkennt das Routingprotokoll auf NS1, dass R1 nicht erreichbar ist, und entfernt daher den Routeneintrag für R1 aus der internen Routingtabelle. NS1 und NS2 tauschen in regelmäßigen Abständen Heartbeat-Nachrichten über den Switch SW3 aus.
3. RM1 erkennt, dass der Routeneintrag für R1 in der internen Routingtabelle nicht vorhanden ist, und leitet ein Failover ein Failover ein. Wenn die Route zu R1 sowohl von NS1 als auch von NS2 nicht erreichbar ist, findet alle 180 Sekunden ein Failover statt, bis eine der Appliances R1 erreichen und die Verbindung wiederherstellen kann.

## Routenmonitore hinzufügen oder entfernen

March 27, 2024

Wenn sich die Appliances eines Hochverfügbarkeitspaars in verschiedenen Netzwerken befinden, hängt der Hochverfügbarkeitsstatus von Citrix Gateway davon ab, ob die Appliance erreicht werden kann oder nicht. In einer netzwerkübergreifenden Hochverfügbarkeitskonfiguration scannt ein Routenmonitor auf jedem Citrix Gateway die interne Routingtabelle, um sicherzustellen, dass immer ein Eintrag für das andere Citrix Gateway vorhanden ist.

### So fügen Sie einen Routenmonitor hinzu

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Klicken Sie im Dialogfeld Routenmonitore binden/unbind auf der Registerkarte Routenmonitore auf Aktion und dann auf Konfigurieren.
3. Geben Sie unter Routenmonitor angeben in Netzwerk die IP-Adresse des Netzwerks des anderen Citrix Gateway-Geräts ein.

   Um eine IPv6-Adresse zu konfigurieren, klicken Sie auf IPv6 und geben Sie dann die IP-Adresse ein.
4. Geben Sie unter Netzwerkmaske die Subnetzmaske des anderen Netzwerks ein, klicken Sie auf Hinzufügen und dann auf OK.

Wenn dieses Verfahren abgeschlossen ist, ist der Routenmonitor an Citrix Gateway gebunden.

Hinweis: Wenn ein Routenmonitor nicht an ein Citrix Gateway gebunden ist, wird der Hochverfügbarkeitsstatus einer der beiden Appliances durch den Status der Schnittstellen bestimmt.

### So entfernen Sie einen Routenmonitor

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Klicken Sie auf der Registerkarte Routenmonitore auf Aktion und dann auf Konfigurieren.
3. Wählen Sie unter Konfigurierte Routenmonitore den Monitor aus, klicken Sie auf Entfernen und dann auf OK.

## Konfigurieren der Link-Redundanz

March 27, 2024

Verknüpfen Sie Redundanz gruppiert Netzwerkschnittstellen, um ein Failover aufgrund eines Fehlers auf einer Netzwerkschnittstelle eines Citrix Gateway mit anderen funktionierenden Schnittstellen zu

verhindern. Der Ausfall der ersten Schnittstelle auf dem primären Citrix Gateway löst ein Failover aus, obwohl die erste Schnittstelle immer noch ihren zweiten Link verwenden kann, um Benutzeranforderungen zu bearbeiten. Wenn Sie die Link-Redundanz konfigurieren, können Sie die beiden Schnittstellen in einem Failover-Schnittstellensatz gruppieren, um zu verhindern, dass der Ausfall einer einzelnen Verbindung ein Failover auf das sekundäre Citrix Gateway verursacht, es sei denn, alle Schnittstellen auf dem primären Citrix Gateway sind nicht funktionsfähig.

Jede Schnittstelle in einem Failover-Schnittstellensatz verwaltet unabhängige Bridge-Einträge. Die aktivierten Monitorschnittstellen und die Hochverfügbarkeit auf einem Citrix Gateway, die nicht an einen ausgefallenen Schnittstellensatz gebunden sind, werden als kritische Schnittstellen bezeichnet, da bei einem Ausfall einer dieser Schnittstellen ein Failover ausgelöst wird.

### So konfigurieren Sie Link-Redundanz

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Klicken Sie auf der Registerkarte Failover-Schnittstellensatz auf Hinzufügen.
3. Geben Sie unter Name einen Namen für das Set ein.
4. Klicken Sie in Interfaces auf Hinzufügen.
5. Wählen Sie unter Verfügbare Schnittstellen eine Schnittstelle aus und klicken Sie dann auf den Pfeil, um die Schnittstelle nach Konfiguriert zu verschieben.
6. Wiederholen Sie die Schritte 4 und 5 für die zweite Oberfläche, und klicken Sie dann auf Erstellen.

Sie können so viele Schnittstellen hinzufügen, wie Sie für ein Failover zwischen den Schnittstellen benötigen.

### So entfernen Sie Schnittstellen aus dem Failover-Schnittstellensatz

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie auf der Registerkarte Failover-Schnittstellensatz einen Satz aus und klicken Sie dann auf Entfernen.

### So entfernen Sie einen Failover-Schnittstellensatz

Wenn Sie kein Failover-Schnittstellensatz mehr benötigen, können Sie es aus Citrix Gateway entfernen.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.

2. Wählen Sie auf der Registerkarte Failover-Schnittstellensatz einen Satz aus und klicken Sie dann auf Entfernen.

## Verstehen der Ursachen von Failovers

January 29, 2024

Die folgenden Ereignisse können in einer Hochverfügbarkeitskonfiguration zu einem Failover führen:

1. Wenn der sekundäre Knoten für einen Zeitraum, der das auf der Sekundärseite eingestellte Dead-Intervall überschreitet, kein Heartbeat-Paket vom primären Knoten empfängt. Weitere Informationen zum Einstellen des Totintervalls finden Sie unter Konfigurieren von Kommunikationsintervallen. Mögliche Ursachen für einen Knoten, der keine Heartbeat-Pakete von einem Peer-Knoten empfängt, sind:
    - Ein Netzwerkkonfigurationsproblem verhindert, dass Heartbeats das Netzwerk zwischen den Hochverfügbarkeitsknoten durchlaufen.
    - Der Peer-Knoten kommt es zu einem Hardware- oder Softwarefehler, der dazu führt, dass er einfriert (hängt), neu startet oder anderweitig die Verarbeitung und Weiterleitung von Heartbeat-Paketen stoppt.
2. Der primäre Knoten erlebt einen Hardwarefehler seiner SSL-Karte.
3. Der primäre Knoten erhält drei Sekunden lang keine Heartbeat-Pakete auf seinen Netzwerkschnittstellen.
4. Auf dem primären Knoten schlägt eine Netzwerkschnittstelle fehl, die nicht Teil eines Failover Interface Set (FIS) oder eines Link Aggregation (LA) -Kanals ist und den Hochverfügbarkeitsmonitor (HAMON) aktiviert hat. Die Schnittstellen sind aktiviert, gehen aber in einen DOWN-Zustand.
5. Auf dem primären Knoten schlagen alle Schnittstellen in einem FIS fehl. Die Schnittstellen sind aktiviert, gehen aber in einen DOWN-Zustand.
6. Auf dem primären Knoten schlägt ein LA-Kanal mit aktiviertem HAMON fehl. Die Schnittstellen sind aktiviert, gehen aber in einen DOWN-Zustand.
7. Auf dem primären Knoten schlagen alle Schnittstellen fehl. In diesem Fall tritt ein Failover unabhängig von der HAMON-Konfiguration auf.
8. Auf dem primären Knoten sind alle Schnittstellen manuell deaktiviert. In diesem Fall tritt ein Failover unabhängig von der HAMON-Konfiguration auf.
9. Sie erzwingen ein Failover, indem Sie den Befehl Force Failover auf beiden Knoten ausgeben.
10. Ein Routenmonitor, der an den primären Knoten gebunden ist, geht DOWN.

## Failover von einem Knoten erzwingen

March 27, 2024

Möglicherweise möchten Sie ein Failover erzwingen, wenn Sie beispielsweise den primären Knoten ersetzen oder aktualisieren müssen. Sie können ein Failover entweder vom primären oder vom sekundären Knoten erzwingen. Ein erzwungenes Failover wird nicht weitergegeben oder synchronisiert. Um den Synchronisationsstatus nach einem erzwungenen Failover anzuzeigen, können Sie den Status des Knotens anzeigen.

Ein erzwungenes Failover schlägt unter den folgenden Umständen fehl:

- Sie erzwingen ein Failover auf einem eigenständigen System.
- Der sekundäre Knoten ist deaktiviert.
- Der Sekundärknoten ist so konfiguriert, dass er sekundär bleibt.

Das Citrix Gateway-Gerät zeigt eine Warnmeldung an, wenn es beim Ausführen des Befehls Force Failover ein potenzielles Problem feststellt. Die Nachricht enthält die Informationen, die die Warnung ausgelöst haben, und fordert eine Bestätigung an, bevor Sie fortfahren.

## Failover auf dem primären oder sekundären Knoten erzwingen

January 29, 2024

Wenn Sie ein Failover auf dem primären Knoten erzwingen, wird der primäre Knoten zum sekundären und der sekundäre Knoten zum primären Knoten. Erzwungenes Failover ist nur möglich, wenn der primäre Knoten feststellen kann, dass der sekundäre Knoten UP ist.

Wenn der sekundäre Knoten DOWN ist, gibt der Befehl Force Failover die folgende Fehlermeldung zurück: “Der Betrieb ist aufgrund eines ungültigen Peer-Status nicht möglich. Behebung und Wiederholen.”

Wenn sich das sekundäre System im Anspruchszustand befindet oder inaktiv ist, gibt der Befehl die folgende Fehlermeldung zurück: `"Operation not possible now. Please wait for system to stabilize before retrying."`

Wenn Sie den Befehl Failover erzwingen vom sekundären Knoten ausführen, wird der sekundäre Knoten primär und der primäre Knoten wird sekundär. Ein Force-Failover kann nur auftreten, wenn der Zustand des sekundären Knotens gut ist und der Knoten nicht so konfiguriert ist, dass er sekundär bleibt.

Wenn der sekundäre Knoten nicht zum primären Knoten werden kann oder wenn der sekundäre Knoten so konfiguriert wurde, dass er sekundär bleibt (mit der Option STAYSECONDARY), zeigt der Knoten die folgende Fehlermeldung an: "Operation nicht möglich, da mein Status ungültig ist. Sehen Sie sich den Knoten für weitere Informationen an."

### So erzwingen Sie ein Failover auf dem primären oder sekundären Knoten

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten den primären Knoten aus, und klicken Sie dann unter Aktionen auf Failover erzwingen.
3. Klicken Sie im Dialogfeld Warnung auf Ja.

## Erzwingen des primären Knotens, primär zu bleiben

March 27, 2024

In einer Hochverfügbarkeitskonfiguration können Sie das primäre Citrix Gateway zwingen, auch nach dem Gerätefailover primär zu bleiben. Sie können diese Einstellung nur auf eigenständigen Citrix Gateway-Geräten und auf dem Citrix Gateway konfigurieren, das das primäre Gerät in einem Hochverfügbarkeitspaar ist.

### So zwingen Sie den primären Knoten, primär zu bleiben

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten einen Knoten aus und klicken Sie dann auf Bearbeiten.
3. Klicken Sie unter Hochverfügbarkeitsstatus auf Primär bleiben und dann auf OK.

Sie können diese Konfiguration nur mit dem folgenden Befehl löschen:

```
clear configuration full
```

Die folgenden Befehle ändern die Citrix Gateway-Hochverfügbarkeitskonfiguration nicht:

```
clear configuration basic
```

```
clear configuration extended
```

# Den sekundären Knoten zwingen, sekundär zu bleiben

March 27, 2024

In einem Hochverfügbarkeits-Setup können Sie das sekundäre Citrix Gateway zwingen, unabhängig vom Status des primären Citrix Gateway sekundär zu bleiben. Wenn Sie Citrix Gateway so konfigurieren, dass es sekundär bleibt, bleibt es sekundär, selbst wenn das primäre Citrix Gateway ausfällt.

Nehmen wir beispielsweise in einem vorhandenen Hochverfügbarkeits-Setup an, dass Sie das primäre Citrix Gateway aktualisieren müssen und dass dieser Prozess eine bestimmte Zeit in Anspruch nimmt. Während des Upgrades kann das primäre Citrix Gateway nicht verfügbar sein, aber Sie möchten nicht, dass das sekundäre Citrix Gateway die Kontrolle übernimmt. Sie möchten, dass es das sekundäre Citrix Gateway bleibt, auch wenn es einen Fehler im primären Citrix Gateway feststellt.

Wenn der Status eines Citrix Gateway in einem Hochverfügbarkeitspaar so konfiguriert ist, dass es sekundär bleibt, nimmt es nicht an Hochverfügbarkeitszustandsmaschinenübergängen teil. Sie können den Status des Citrix Gateway im Konfigurationsdienstprogramm auf der Registerkarte **Knoten** überprüfen.

Diese Einstellung funktioniert sowohl auf einem eigenständigen als auch auf einem sekundären Citrix Gateway.

Wenn Sie den Knoten für hohe Verfügbarkeit festlegen, wird er nicht weitergegeben oder synchronisiert und wirkt sich nur auf das Citrix Gateway aus, auf dem die Einstellung konfiguriert ist.

## Den sekundären Knoten zwingen, sekundär zu bleiben

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten einen Knoten aus, und klicken Sie dann auf Bearbeiten.
3. Klicken Sie unter Hochverfügbarkeitsstatus auf Sekundär bleiben (Im Hörmodus bleiben), und klicken Sie dann auf OK.

## So geben Sie Citrix Gateway als aktives Hochverfügbarkeitsgerät zurück

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich die Option System und klicken Sie dann auf Hochverfügbarkeit.
2. Wählen Sie im Detailbereich auf der Registerkarte Knoten die Appliance aus, die der primäre Knoten bleiben soll, und klicken Sie dann auf Öffnen.

3. Klicken Sie unter Hochverfügbarkeitsstatus auf Aktiviert (Aktiv an HA teilnehmen), und klicken Sie dann auf OK.

## Verwenden von Clustering

March 27, 2024

Citrix Gateway kann in Clusterkonfigurationen bereitgestellt werden, um einen hohen Durchsatz, hohe Verfügbarkeit und Skalierbarkeit für den VPN-Clientverkehr bereitzustellen. In einem Cluster fungiert eine Gruppe von Citrix Gateway-Appliances oder VMs als ein einziges Systemimage, um Benutzersitzungen zu koordinieren und den Datenverkehr zu Netzwerkressourcen zu verwalten. Ein Citrix Gateway-Cluster kann mit mindestens zwei und maximal 32 Citrix Gateway-Appliances oder VMs erstellt werden, die als Clusterknoten konfiguriert sind.

Lesen Sie die
Citrix ADC Clustering-Dokumentation, bevor Sie mit der Konfiguration Ihres Citrix Gateway-Clusters beginnen. Achten Sie besonders auf die folgenden Themen in dieser Dokumentation.

- Siehe Hardware- und Softwareanforderungen, um zu überprüfen, ob die Systeme, die Sie verwenden möchten, die Anforderungen erfüllen.
- Eine Beschreibung der Clustering-Konzepte finden Sie unter Funktionsweise von Clustering.
- Weitere Informationen finden Sie unter Einrichten der Kommunikation zwischen Knoten, um die Bereitstellung zu planen und eventuelle Vorbehalte zu ermitteln, die für Ihre Umgebung relevant sein könnten.

Ein Citrix Gateway-Cluster arbeitet als Citrix ADC-Cluster mit gepunktetem VIP-Konfigurationstyp.

> **Wichtig:**
>
> Der **XenApp und XenDesktop-Assistent** wird für das Clustering nicht unterstützt. Daher finden Sie den **XenApp- und XenDesktop-Assistenten** nicht im Abschnitt **GUI > Navigationsbereich > Integrate with Citrix Products**.

## Clustering konfigurieren

March 27, 2024

Die Hauptaufgaben beim Einrichten von Citrix Gateway-Clustering sind:

1. Entscheiden Sie, welches Citrix Gateway-Gerät oder die virtuelle Maschine der Konfigurationskoordinator ist, und erstellen Sie eine Clusterinstanz auf diesem System (falls noch keine vorhanden ist).
2. Verbinden Sie Citrix Gateway-Systeme als Knoten mit dem Cluster.
3. Erstellen Sie eine Knotengruppe auf der Clusterinstanz mit dem Optionssatz STICKY.
4. Binden Sie einen einzelnen Clusterknoten an die Cluster-Knotengruppe.
5. Konfigurieren Sie einen virtuellen Citrix Gateway-Server im Konfigurationskoordinator und binden Sie ihn an die Cluster-Knotengruppe.

Für die Konfiguration eines Citrix ADC-Clusters stehen mehrere Methoden zur Verfügung. Die folgenden Aufgaben verwenden die direkteste Methode, die im Konfigurationsdienstprogramm verfügbar ist.

### So erstellen Sie eine Citrix Gateway-Clusterinstanz mithilfe des Konfigurationsdienstprogramms

Sobald Sie die Bereitstellungsdetails in Ordnung haben, beginnen Sie mit der Konfiguration auf dem Citrix Gateway, dem Konfigurationskoordinator.

Vorsicht: Durch das Erstellen der Clusterinstanz wird die Konfiguration gelöscht. Wenn Sie die vorhandene Systemkonfiguration als Referenz speichern müssen, archivieren Sie eine Kopie, bevor Sie mit der Clusterkonfiguration fortfahren. Alle vorhandenen Einstellungen, die im Cluster verwendet werden sollen, können nach der Einrichtung des Clusters erneut auf den Konfigurationskoordinator angewendet werden.

1. Melden Sie sich unter der NSIP-Adresse beim Citrix ADC-Konfigurationsdienstprogramm an.
2. Erweitern Sie den Systemknoten und dann den Cluster-Unterknoten.
3. Klicken Sie im Detailbereich auf Cluster verwalten.
4. Legen Sie im Dialogfeld Clusterkonfiguration die Parameter fest, die zum Erstellen des Clusters erforderlich sind.

    a) Geben Sie eine Clusterinstanz-ID ein. Die Clusterinstanz-ID ist der numerische Bezeichner für die Clusterinstanz. Der Standardwert ist 1, aber Sie können ihn auf eine beliebige Zahl von 1 bis 16 setzen.
    b) Geben Sie die Cluster-IP-Adresse ein. Die Cluster-IP-Adresse ist die IP-Adresse des Clusters für den Konfigurationskoordinator, bei der es sich um die Verwaltungs-IP-Adresse für den Cluster handelt.
    c) Wählen Sie das bevorzugte Backplane-Interface aus. Dies ist diese Citrix Gateway-Schnittstelle, die für die Kommunikation zwischen den Clusterknoten verwendet werden soll.

5. Klicken Sie auf Erstellen.

6. Klicken Sie bei der Aufforderung zur Bestätigung des Systemneustarts auf Ja.
7. Nachdem der Knoten in Betrieb ist und die Synchronisierung erfolgreich war, ändern Sie von der Cluster-IP-Adresse die RPC-Anmeldeinformationen sowohl für den Knoten als auch für die Cluster-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.
8. Warten Sie, bis das System neu startet. Sobald verfügbar, melden Sie sich unter der in Schritt 4 (2) konfigurierten Cluster-IP-Adresse beim Konfigurationsdienstprogramm an.

**Hinweis:** Im **Detailbereich Systeminformationen** wird der lokale Knoten an der NSIP-Adresse als Konfigurationskoordinator gemeldet. Dies bestätigt, dass die Basisclusterinstanz jetzt in Betrieb ist.

Der lokale Knoten des Konfigurationskoordinators wird automatisch zum Cluster hinzugefügt. In der folgenden Aufgabe können weitere Knoten hinzugefügt werden.

### Hinzufügen von Knoten zu einem Citrix Gateway Cluster

Sobald die Clusterinstanz eingerichtet wurde, können Sie damit beginnen, dem Cluster weitere Citrix Gateway-Knoten hinzuzufügen.

Um dem Cluster weitere Citrix Gateway-Systeme hinzuzufügen, können Sie das Konfigurationsdienstprogramm verwenden, um die Cluster-Knoten-Erstellung und Join-Cluster-Einstellungen remote vorzunehmen.

**Hinweis**: Das Hinzufügen von Knoten zum Cluster muss abgeschlossen sein, bevor Sie Ihr Citrix Gateway-Setup konfigurieren. Auf diese Weise müssen Sie die Citrix Gateway-Konfiguration nicht wiederholen, wenn mit Ihrer Clusterkonfiguration etwas schief geht und Sie den Cluster entfernen und erneut beginnen möchten.

1. Melden Sie sich unter der Cluster-IP-Adresse beim Citrix ADC-Konfigurationsdienstprogramm an.
2. Erweitern Sie den **Systemknoten** und dann den Cluster-Unterknoten.
3. Klicken Sie im Detailbereich auf **Cluster verwalten**.
4. Klicken Sie im Detailbereich Clusterknoten auf **Hinzufügen**.
5. Geben **Sie im Bereich Clusterknoten erstellen** eine eindeutige Node-ID für diesen Knoten ein.
6. Geben Sie die Citrix ADC IP-Adresse des Systems ein, das als Clusterknoten hinzugefügt werden soll.
7. Geben Sie im Bereich **Cluster Node-Anmeldeinformationen** den Citrix Gateway-Benutzernamen und das Kennwort für das Remote-Citrix Gateway-System ein.
8. Geben Sie im Bereich Configuration Coordinator-Anmeldeinformationen das Kennwort für den lokal autorisierten Benutzer ein.
9. Klicken Sie auf **Erstellen**.

10. Wenn Sie dazu aufgefordert werden, klicken Sie auf **JA**, damit die Systemkonfiguration gespeichert werden kann, und führen Sie einen Warmstart des Remote-Citrix-Gateways durch.
11. Nachdem der Knoten in Betrieb ist und die Synchronisierung erfolgreich war, ändern Sie von der Cluster-IP-Adresse die RPC-Anmeldeinformationen sowohl für den Knoten als auch für die Cluster-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.

Wiederholen Sie die Schritte 4 bis 11 für jedes zusätzliche Citrix Gateway-Remote-System, das Sie als Clusterknoten konfigurieren möchten.

Stellen Sie sicher, dass die Clusterknoten in der Liste der aktiven Knoten im Detailbereich Clusterknoten enthalten sind. Wenn Knoten fehlen, wiederholen Sie die Schritte 4 bis 10, bis alle erforderlichen Knoten aufgeführt sind.

### Erstellen einer Cluster-Knoten-Gruppe

Sobald die Clusterknoten hinzugefügt wurden, kann eine Cluster-Knotengruppe erstellt werden.

1. Melden Sie sich unter der Cluster-IP-Adresse beim Citrix ADC-Konfigurationsdienstprogramm an.
2. Erweitern Sie den **Systemknoten** und dann den Cluster-Unterknoten.
3. Klicken Sie auf **Node-Gruppen**.
4. Klicken Sie im Detailbereich auf **Hinzufügen**.
5. Geben Sie einen Namen für die Cluster-Knoten-Gruppe ein.
6. Wählen Sie die Option **Sticky** aus, um den virtuellen Citrix Gateway-Servertyp zu unterstützen.
7. Klicken Sie auf **Weiter**.

Die Cluster-Knotengruppe ist jetzt eingerichtet. Bevor Sie diesen Bereich des Konfigurationsdienstprogramms verlassen, können Sie den lokalen Citrix Gateway-Knoten an die neue Cluster-Knotengruppe binden. Dies ist der einzige Knoten, der an die Clustergruppe gebunden ist.

### Binden Sie den lokalen Clusterknoten an die Cluster-Knotengruppe

Da es sich bei einer Citrix Gateway-Clusterkonfiguration um einen gepunkteten Typ handelt, kann nur ein Knoten an die Knotengruppe gebunden werden. Das folgende Verfahren bindet den lokalen Knoten im Konfigurationskoordinator an die Knotengruppe, aber jeder Knoten im Cluster kann für diese Bindung verwendet werden.

1. Erweitern Sie im Bereich Erweitert Clusterknoten.
2. Wählen Sie im mittleren Bereich Clusterknoten Kein Clusterknoten aus.
3. Klicken Sie auf dem Konfigurationsbildschirm für Cluster Node auf Bind.

4. Wählen Sie den lokalen Knoten aus, der durch die NSIP-Adresse für dieses Citrix Gateway-System dargestellt wird.
5. Klicken Sie auf Einfügen.
6. Klicken Sie auf OK.
7. Klicken Sie auf Fertig.

Der Cluster ist jetzt gefüllt und bereit, einen virtuellen Citrix Gateway-Server freizugeben, wie durch die folgende Aufgabe konfiguriert.

### Binden eines Citrix Gateway Virtual Servers an die Cluster-Knoten-Gruppe

Wenn ein Cluster eingerichtet ist, können Sie mit dem Erstellen der Citrix Gateway-Konfiguration fortfahren, die die Clusterbereitstellung bereitstellen soll. Um die Konfiguration an den Cluster zu binden, müssen Sie den virtuellen Citrix Gateway-Server erstellen und an eine Cluster-Knotengruppe binden, die auf den Typ Sticky eingestellt ist. Nachdem der virtuelle Server an die Clusterknotengruppe gebunden ist, können Sie das Citrix Gateway weiterhin konfigurieren.

Wenn mehrere virtuelle Citrix Gateway-Server konfiguriert sind, müssen diese ebenfalls an die Cluster-Knotengruppe gebunden sein.

**Hinweis:** Wenn virtuelle Citrix Gateway-Server noch nicht konfiguriert wurden, müssen Sie möglicherweise zuerst die Citrix Gateway- und Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen zuerst unter
**System > Einstellungen > Grundfunktionen konfigurieren**aktivieren.

1. Melden Sie sich unter der Cluster-IP-Adresse beim Citrix ADC-Konfigurationsdienstprogramm an.
2. Erweitern Sie den **Systemknoten** und dann den Cluster-Unterknoten.
3. Klicken Sie auf **Node-Gruppen**.
4. Wählen Sie im Bereich **Knotengruppe** den gewünschten Knotengruppennamen aus, und klicken Sie dann auf **Bearbeiten**.
5. Erweitern Sie im Bereich **Erweitert** auf der rechten Seite die Option **Virtuelle Server**, und klicken Sie dann auf das Symbol +, um einen virtuellen Server hinzuzufügen.
6. Wählen Sie den Typ des virtuellen VPN-Servers aus und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Bind**.
8. Wenn der benötigte virtuelle Server aufgeführt ist, wählen Sie ihn aus, klicken Sie auf **Einfügen**und dann auf **OK**.
9. Wenn Sie einen neuen virtuellen Server erstellen müssen, klicken Sie auf **Hinzufügen**. Fahren Sie mit der Citrix ADC Virtual Server-Konfiguration fort. Minimal muss lediglich der virtuelle Server erstellt werden, damit er an die Clusterknotengruppe gebunden werden kann.
10. Sobald der virtuelle Server in der Liste Citrix Gateway Virtual Servers verfügbar ist, wählen Sie ihn aus, und klicken Sie dann auf **Einfügen**.

11. Klicken Sie auf **OK**.
12. Klicken Sie auf **Fertig**.

**Hinweis**: Wenn mehrere virtuelle Citrix Gateway-Server konfiguriert sind, müssen diese ebenfalls mit derselben Methode an die Cluster-Knotengruppe gebunden werden.

## Unified Gateway

March 27, 2024

### Citrix ADC mit Unified Gateway: Eine URL

Citrix ADC mit Unified Gateway ermöglicht einen vereinfachten sicheren Zugriff auf jede Anwendung über eine einzige URL für Desktop- und mobile Benutzer. Hinter dieser einzigen URL haben Administratoren einen einzigen Punkt für Konfiguration, Sicherheit und Kontrolle des Fernzugriffs auf Anwendungen. Und Remote-Benutzer haben eine verbesserte Erfahrung mit nahtloser einmaliger Anmeldung für alle Anwendungen, die sie benötigen, zusammen mit dem Anmelden/Abmelden, sobald sie benutzerfreundlich sind.

Um dies zu erreichen, bietet Citrix ADC with Gateway zusammen mit den Content Switching-Kapazitäten und der umfangreichen Authentifizierungsinfrastruktur von Citrix ADC über diese einzige URL Zugriff auf Websites und Apps der Organisation. Remote-Benutzer können außerdem iOS- oder Android-Mobilgeräte sowie Linux-, PC- oder Mac-Systeme mit den Citrix Gateway-Client-Plug-Ins für einen einheitlichen Zugriff auf die Unified Gateway-URL verwenden, wo immer sie sich befinden.

Eine Unified Gateway-Bereitstellung ermöglicht den Zugriff mit einer einzigen URL auf die folgenden Anwendungskategorien:

- Intranet-Anwendungen.
- Clientlose Anwendungen
- Software als Serviceanwendung
- Vorkonfigurierte Anwendungen, die von Citrix ADC bereitgestellt werden
- Citrix Virtual Apps and Desktops veröffentlichte Anwendungen

**Intranet-Anwendungen** können jede webbasierte Anwendung sein, die sich innerhalb des sicheren Unternehmensnetzwerks befindet. Dies sind interne Ressourcen wie eine organisatorische Intranet-Site, eine Bug-Tracking-Anwendung oder ein Wiki.

Typischerweise sind die **clientlosen Anwendungen** Unified Gateway auch innerhalb des sicheren Unternehmensnetzwerks und bietet Zugriff auf eine einzige URL, zu denen Outlook Web Access und

SharePoint gehören. Diese Anwendungen bieten Zugriff auf Exchange-E-Mail- und Teamressourcen ohne dedizierte Clientsoftware, die Remote-Benutzern zur Verfügung stehen muss.

**SaaS-Anwendungen**, auch allgemein als Cloud Apps bekannt, sind externe, Cloud-basierte Anwendungen, auf die Unternehmen angewiesen sind, wie ShareFile, Salesforce oder NetSuite. SAML-basiertes Single Sign-On wird mit den SaaS-Anwendungen unterstützt, die es anbieten.

Einige Organisationen haben möglicherweise**Citrix ADC bereitgestellte Anwendungen vorkonfiguriert**, die in einer Citrix ADC-Konfiguration mit Lastausgleich bereitgestellt wurden. Oft wird dies auch als "Reverse-Proxy"-Anwendung bezeichnet. Unified Gateway unterstützt diese Anwendungen, wenn sich ein virtueller Server für die Bereitstellung auf derselben Citrix ADC Unified Gateway-Instanz oder Appliance befindet. Diese Anwendungen verfügen möglicherweise über eine eigene Authentifizierungskonfiguration, die unabhängig von der Unified Gateway-Konfiguration ist.

Alle veröffentlichten **Citrix Virtual Apps and Desktops veröffentlichten Anwendungen**können über eine Unified Gateway-URL verfügbar gemacht werden. SmartAccess- und SmartControl-Richtlinien können optional auf granulare Richtlinien und Zugriffssteuerung auf diese Ressourcen angewendet werden.

### Der Konfigurationsassistent für Unified Gateway

Die empfohlene Methode zum Konfigurieren eines Citrix ADC mit Unified Gateway-Bereitstellung ist die Verwendung des Unified Gateway-Konfigurationsassistenten.Der Assistent führt Sie durch die Konfiguration und erstellt alle erforderlichen virtuellen Server, Richtlinien und Ausdrücke und wendet Einstellungen basierend auf den bereitgestellten Details an. Nach der Ersteinrichtung kann der Assistent verwendet werden, um Ihre Bereitstellung zu verwalten und deren Betrieb zu überwachen.

> **Hinweis:**
>
> Der Unified Gateway-Konfigurationsassistent führt keine anfängliche Systemkonfiguration durch. Ihre Citrix Gateway-Appliance oder VPX-Instanz muss die Basisinstallation abgeschlossen haben, bevor Sie Unified Gateway konfigurieren. Lesen Sie die Installationsanweisungen zumKonfigurieren von Citrix Gateway mit dem Erst-Setup-Assistenten, um die Grundkonfiguration abzuschließen.

Die vom Assistenten konfigurierten Unified Gateway-Elemente sind:

- Der primäre virtuelle Unified Gateway-Server
- Ein SSL-Serverzertifikat für den virtuellen Unified Gateway-Server
- Eine primäre und optionale sekundäre Authentifizierungskonfiguration
- Eine Portal-Themenauswahl und optionale Anpassung
- Die Benutzeranwendungen, auf die über das Unified Gateway-Portal zugegriffen werden soll

Für jedes dieser Elemente müssen Sie Konfigurationsinformationen angeben. Für eine einfache Unified Gateway-Bereitstellung werden die folgenden Informationen benötigt.

- Für den primären virtuellen Unified Gateway-Server die öffentliche IP-Adresse und die IP-Portnummer für die Bereitstellung. Dies ist die IP-Adresse, die in DNS in den Hostnamen der Unified Gateway-URL aufgelöst wird. Wenn beispielsweise die URL Ihrer Unified Gateway-Bereitstellung lautet `https://mycompany.com/`, muss die IP-Adresse auf mycompany.com aufgelöst werden.
- Das signierte SSL-Serverzertifikat für die Bereitstellung. Citrix Gateway unterstützt PEM- oder PFX-formatierte Zertifikate.
- Informationen zum primären Authentifizierungsserver. Die für diese Authentifizierungskonfiguration unterstützten Authentifizierungssysteme basieren auf LDAP/Active Directory, RADIUS und Certificate. Eine sekundäre LDAP- oder RADIUS-Authentifizierungskonfiguration könnte ebenfalls erstellt werden. Die IP-Adresse des Authentifizierungsservers muss zusammen mit allen relevanten Administratoranmeldeinformationen oder Verzeichnisattributen angegeben werden. Für die Zertifikatauthentifizierung müssen die Gerätezertifikattribute und ein CA-Zertifikat bereitgestellt werden.
- Ein Portal-Thema könnte ausgewählt werden. Wenn ein benutzerdefiniertes oder gebrandetes Portaldesign gewünscht wird, können benutzerdefinierte Grafiken mit dem Assistenten auf das System hochgeladen werden.
- Für webbasierte Benutzeranwendungen müssen die URLs für die einzelnen Anwendungen angegeben werden. Für Webanwendungen, die die SAML-Single-Sign-On-Authentifizierung verwenden sollen, sammelt das Dienstprogramm die Assertion Consumer Service-URL zusammen mit anderen optionalen SAML-Parametern. Sammeln Sie im Voraus die Konfigurationsdetails für die Anwendungen, die ein SAML-Authentifizierungssystem verwenden.
- Damit veröffentlichte Ressourcen von Citrix Virtual Apps and Desktops über die Unified Gateway-Bereitstellung verfügbar gemacht werden, müssen Sie den Integrationspunkt angeben (StoreFront, das Webinterface oder das Webinterface auf Citrix ADC). Das Dienstprogramm benötigt je nach Art des Integrationspunkts den vollqualifizierten Domänennamen des Integrationspunkts, den Standortpfad, die Single Sign-On-Domäne, die Secure Ticket Authority (STA) -Server-URL und andere.

#### Zusätzliche Konfigurationsverwaltung

Für standortspezifische Einstellungen, die im Unified Gateway-Konfigurationsdienstprogramm nicht verfügbar sind, z. B. alternative SSL-Einstellungen oder Sitzungsrichtlinien, können Sie die erforderlichen Einstellungen im Citrix Gateway-Konfigurationsdienstprogramm verwalten. Sie können diese

Einstellungen auf den virtuellen Content Switching- oder VPN-Servern ändern, sobald sie vom Unified Gateway-Konfigurationsdienstprogramm erstellt wurden.

### Virtueller Content Switching-Server

Dies ist die Citrix ADC-Konfigurationseinheit hinter der Haupt-IP-Adresse und -URL der Bereitstellung. Die SSL-Serverzertifikate und -parameter werden auf diesem virtuellen Server verwaltet. Da dieser virtuelle Server der antwortende Netzwerkhost für die Bereitstellung ist, können die ICMP-Serverantwort und der RHI-Status bei Bedarf auf diesem virtuellen Server geändert werden. Den virtuellen Content Switching-Server finden Sie auf der Registerkarte **Konfiguration** unter **Traffic Management** > **Content Switching** > **Virtuelle Server**.

> **Wichtig:**
>
> Wenn Sie Ihre Unified Gateway-Umgebung auf Version 13.0 Build 58.x oder höher aktualisieren, ist der DTLS-Regler auf dem virtuellen Content Switching-Server deaktiviert, der vor dem Gateway oder dem virtuellen VPN-Server konfiguriert ist. Aktivieren Sie den DTLS-Regler im virtuellen Content Switching-Server nach dem Upgrade manuell. Aktivieren Sie den DTLS-Regler nicht, wenn Sie den Assistenten für die Konfiguration verwenden.

#### Virtueller VPN-Server

Alle anderen VPN-Parameter, Profile und Richtlinienbindungen für die Unified Gateway-Konfiguration werden auf diesem virtuellen Server verwaltet, einschließlich der Hauptauthentifizierungskonfiguration. Diese Entität wird auf der Registerkarte **Konfiguration** unter **Citrix Gateway** > **Virtuelle Server**verwaltet. Der Name des entsprechenden virtuellen VPN-Servers enthält den Namen, der dem virtuellen Content Switching-Server während der anfänglichen Unified Gateway-Konfiguration gegeben wurde.

> **Hinweis:**
>
> Die virtuellen VPN-Server, die für eine Unified Gateway-Bereitstellung erstellt wurden, sind nicht adressierbar und weisen die 0.0.0.0-IP-Adresse zu.

## Häufig gestellte Fragen zu Unified Gateway

March 27, 2024

### Was ist Unified Gateway?

Unified Gateway ist eine neue Funktion in der Citrix ADC 11.0 Version, die die Möglichkeit bietet, Datenverkehr auf einem einzelnen virtuellen Server (als virtueller Unified Gateway-Server bezeichnet) zu empfangen und diesen Datenverkehr dann gegebenenfalls intern an virtuelle Server weiterzuleiten, die an den virtuellen Unified Gateway-Server gebunden sind.

Mit der Unified Gateway-Funktion können Endbenutzer mithilfe einer einzigen IP-Adresse oder URL (verbunden mit dem virtuellen Unified Gateway-Server) auf mehrere Dienste zugreifen. Administratoren können IP-Adressen freigeben und die Konfiguration der Citrix Gateway-Bereitstellung vereinfachen.

Jeder virtuelle Unified Gateway-Server kann einen virtuellen Citrix Gateway-Server zusammen mit null oder mehr virtuellen Lastausgleichsservern als Teil einer Formation vorn beenden. Unified Gateway verwendet das Content Switching-Feature der Citrix ADC Appliance.

Einige Beispiele für Unified Gateway-Bereitstellungen:

- Virtueller Unified Gateway-Server -> [ein virtueller Citrix Gateway-Server]
- Virtueller Unified Gateway-Server -> [ein virtueller Citrix Gateway-Server, ein virtueller Lastausgleichsserver]
- Virtueller Unified Gateway-Server -> [ein virtueller Citrix Gateway-Server, zwei virtuelle Lastausgleichsserver]
- Virtueller Unified Gateway-Server -> [ein virtueller Citrix Gateway-Server, drei virtuelle Lastausgleichsserver]

Jeder der virtuellen Lastausgleichsserver kann jeder standardmäßige Lastausgleichsserver sein, auf dem ein Back-End-Dienst wie Microsoft Exchange oder Citrix ShareFile gehostet wird.

### Warum Unified Gateway verwenden?

Mit der Unified Gateway-Funktion können Endbenutzer mithilfe einer einzigen IP-Adresse oder URL (verknüpft mit dem virtuellen Unified Gateway-Server) auf mehrere Dienste zugreifen. Für Administratoren besteht der Vorteil darin, dass sie IP-Adressen freigeben und die Konfiguration der Citrix Gateway-Bereitstellung vereinfachen können.

### Kann es mehr als einen virtuellen Unified Gateway-Server geben?

Ja. Es kann so viele virtuelle Unified Gateway-Server geben, wie Sie benötigen.

### Warum ist Content Switching für Unified Gateway erforderlich?

Die Funktion zum Content Switching ist erforderlich, da der virtuelle Server für die Content Switching derjenige ist, der Datenverkehr empfängt und intern an den entsprechenden virtuellen Server weiterleitet. Der virtuelle Content Switching-Server ist die Hauptkomponente der Unified Gateway-Funktion.

### In Versionen vor 11.0 kann Content Switching verwendet werden, um Datenverkehr für mehrere virtuelle Server zu empfangen. Wird diese Verwendung auch Unified Gateway genannt?

Die Verwendung eines virtuellen Content Switching-Servers zum Empfangen von Datenverkehr für mehrere virtuelle Server wird in Versionen vor 11.0 unterstützt. Content Switching kann jedoch keinen Datenverkehr zu einem virtuellen Citrix Gateway-Server leiten.

Die Verbesserungen in 11.0 ermöglichen es einem virtuellen Content Switching-Server, den Datenverkehr an jeden virtuellen Server zu leiten, einschließlich eines virtuellen Citrix Gateway-Servers.

### Was hat sich bei den Richtlinien Content Switching in Unified Gateway geändert?

1. Ein neuer Befehlszeilenparameter "-TargetVServer"wird für die Content Switching-Aktion hinzugefügt. Der neue Parameter wird verwendet, um den virtuellen Citrix Gateway-Zielserver anzugeben. Beispiel:

   ```
   add cs action UG_CSACT_MyUG -targetVserver UG_VPN_MyUG
   ```

   Im Citrix Gateway-Konfigurationsdienstprogramm verfügt die Aktion zum Content Switching über eine neue Option, Target Virtual Server, die auf einen virtuellen Citrix Gateway-Server verweisen kann.

2. Ein neuer erweiterter Richtlinienausdruck, is_vpn_url, kann verwendet werden, um Citrix Gateway und authentifizierungsspezifische Anforderungen abzugleichen.

### Welche Citrix Gateway-Funktionen werden derzeit in Unified Gateway nicht unterstützt?

Alle Funktionen werden in Unified Gateway unterstützt. Bei der nativen Anmeldung über das VPN-Plug-in wurde jedoch ein geringfügiges Problem (Problemnummer 544325) gemeldet. In diesem Fall funktioniert Seamless Single Sign-On (SSO) nicht.

### Wie verhalten sich EPA-Scans bei Unified Gateway?

Bei Unified Gateway wird die Endpunktanalyse nur für die Citrix Gateway-Zugriffsmethoden ausgelöst, nicht für den Citrix ADC AAA TM-Zugriff. Wenn ein Benutzer versucht, auf einen virtuellen Citrix ADC AAA TM-Server zuzugreifen, obwohl die Authentifizierung auf dem virtuellen Citrix Gateway-Server erfolgt, wird der EPA-Scan nicht ausgelöst. Wenn der Benutzer jedoch versucht, clientlosen VPN/vollständigen VPN-Zugriff zu erhalten, wird der konfigurierte EPA-Scan ausgelöst. In diesem Fall erfolgt entweder eine Authentifizierung oder ein nahtloses SSO.

### Was sind die Lizenzanforderungen für Unified Gateway?

Unified Gateway wird nur für Advanced- und Premium-Lizenzen unterstützt. Es ist nicht nur für Citrix Gateway oder Standard-Lizenzeditionen verfügbar.

### Benötigt der virtuelle Citrix Gateway-Server, der mit Unified Gateway verwendet wird, eine IP/Port/SSL-Konfiguration?

Für einen virtuellen Citrix Gateway-Server, der mit dem virtuellen Unified Gateway-Server verwendet wird, ist auf dem virtuellen Citrix Gateway-Server keine IP/Port-/SSL-Konfiguration erforderlich. Für die RDP-Proxy-Funktionalität können Sie jedoch dasselbe SSL/TLS-Serverzertifikat an den virtuellen Citrix Gateway-Server binden.

### Muss ich SSL-/TLS-Zertifikate, die sich auf dem virtuellen Citrix Gateway-Server befinden, für die Verwendung mit einem virtuellen Unified Gateway-Server erneut bereitstellen?

Sie müssen keine Zertifikate erneut bereitstellen, die derzeit an Ihren virtuellen Citrix Gateway-Server gebunden sind. Es steht Ihnen frei, alle vorhandenen SSL-Zertifikate wiederzuverwenden und an den virtuellen Unified Gateway-Server zu binden.

### Was ist der Unterschied zwischen einer einzelnen URL und einer Multi-Host-Bereitstellung? Welches brauche ich?

Eine einzelne URL bezieht sich auf die Fähigkeit des virtuellen Unified Gateway-Servers, Datenverkehr für einen vollqualifizierten Domänennamen (FQDN) zu verarbeiten. Diese Einschränkung besteht, wenn Unified Gateway ein SSL/TLS-Serverzertifikat verwendet, bei dem der Betreff des Zertifikats mit dem FQDN gefüllt ist. Zum Beispiel: ug.citrix.com

Wenn Unified Gateway ein Platzhalterserverzertifikat verwendet, kann es den Datenverkehr für mehrere Unterdomänen verarbeiten. Zum Beispiel: *.citrix.com

Eine weitere Option ist die SSL/TLS-Konfiguration mit Server Name Indicator (SNI) -Funktionalität, um das Binden mehrerer SSL/TLS-Serverzertifikate zu ermöglichen. Beispiele: auth.citrix.com, auth.citrix.de, auth.citrix.co.uk, auth.citrix.co.jp

Ein einzelner Host im Vergleich zu mehreren Hosts entspricht der Art und Weise, wie Websites normalerweise auf einem Webserver gehostet werden (z. B. der Apache HTTP-Server oder Microsoft Internet Information Services (IIS)). Wenn es einen einzelnen Host gibt, können Sie einen Site-Pfad verwenden, um den Datenverkehr genauso zu wechseln wie Alias oder "virtuelles Verzeichnis"in Apache. Wenn es mehrere Hosts gibt, verwenden Sie einen Host-Header, um den Datenverkehr ähnlich wie bei der Verwendung von virtuellen Hosts in Apache zu wechseln.

### Welche Authentifizierungsmechanismen können mit Unified Gateway verwendet werden?

Alle vorhandenen Authentifizierungsmechanismen, die mit Citrix Gateway kompatibel sind, sind auch mit Unified Gateway kompatibel.

Dazu gehören LDAP, RADIUS, SAML, Kerberos, zertifikatbasierte Authentifizierung und so weiter.

Unabhängig davon, welcher Authentifizierungsmechanismus auf dem virtuellen Citrix Gateway-Server konfiguriert ist, bevor das Upgrade durchgeführt wird, wird automatisch verwendet, wenn der virtuelle Citrix Gateway-Server hinter dem virtuellen Unified Gateway-Server platziert wird. Es sind keine zusätzlichen Konfigurationsschritte erforderlich, außer dem virtuellen Citrix Gateway-Server eine nicht adressierbare IP-Adresse (0.0.0.0) zuzuweisen.

### Was ist "SelfAuth"*Authentifizierung?

SelfAuth ist an sich kein Authentifizierungstyp. SelfAUTH beschreibt, wie eine URL erstellt wird. Ein neuer Befehlszeilenparameter ist für die VPN-URL-Konfiguration verfügbar. `ssotype` Beispiel:

```
> add vpn url RGB RGB "http://blue.citrix.lab/"-vServerName Blue -
ssotype selfauth
```

SelfAUTH ist einer der Werte des `ssotype` Parameters. Diese Art von URL kann verwendet werden, um auf Ressourcen zuzugreifen, die sich nicht in derselben Domäne wie der virtuelle Unified Gateway-Server befinden. Die Einstellung ist im Konfigurationsdienstprogramm bei der Konfiguration eines Lesezeichens zu sehen.

### Was ist “StepUp”Authentication’?

Wenn zusätzliche, sicherere Authentifizierungsebenen für den Zugriff auf eine Citrix ADC AAA TM-Ressource erforderlich sind, können Sie die StepUp-Authentifizierung verwenden. Verwenden Sie in der Befehlszeile einen AuthnProfile-Befehl, um den AuthenticationLevel-Parameter festzulegen. Beispiel:

```
1 add authentication authnProfile AuthProfile -authnVsName AAATMVserver -
     AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab
     **-**AuthenticationLevel 100
2 <!--NeedCopy-->
```

Dieses Authentifizierungsprofil ist an den virtuellen Lastausgleichsserver gebunden.

### Wird die StepUp-Authentifizierung für virtuelle Citrix ADC AAA TM-Server unterstützt?

Ja, es wird unterstützt.

### Was ist `login once/logout once`?

`Login Once`: VPN-Benutzer melden sich einmal bei einem Citrix ADC AAA TM oder einem virtuellen Citrix Gateway-Server an. Und von da an haben VPN-Benutzer nahtlosen Zugriff auf alle Unternehmens-/Cloud-/Webanwendungen. Der Benutzer muss nicht erneut authentifiziert werden. Eine erneute Authentifizierung erfolgt jedoch für Sonderfälle wie Citrix ADC AAA TM StepUp.

`Logout Once`: Nachdem die erste Citrix ADC AAA TM- oder Citrix Gateway-Sitzung erstellt wurde, wird sie verwendet, um nachfolgende Citrix ADC AAA TM- oder Citrix Gateway-Sitzungen für diesen Benutzer zu erstellen. Wenn eine dieser Sitzungen abgemeldet ist, meldet die Citrix ADC Appliance auch die anderen Anwendungen oder Sitzungen des Benutzers ab.

### Können gemeinsame Authentifizierungsrichtlinien auf Unified Gateway-Ebene mit Citrix ADC AAA TM für den Lastausgleich für virtuelle Server spezifiziert authentifiziert auf Ebene des Lastausgleichs des virtuellen Servers festgelegt werden? Was sind die Konfigurationsschritte zur Unterstützung dieses Anwendungsfalls?

Wenn Sie separate Authentifizierungsrichtlinien für den virtuellen Citrix ADC AAA TM-Server hinter Unified Gateway angeben müssen, benötigen Sie einen separaten, unabhängig adressierbaren virtuellen Authentifizierungsserver (ähnlich der normalen Citrix ADC AAA TM-Konfiguration). Die Einstellung des Authentifizierungshosts auf dem virtuellen Lastausgleichsserver muss auf diesen virtuellen Authentifizierungsserver verweisen.

### Wie konfigurieren Sie Unified Gateway so, dass gebundene virtuelle Citrix ADC AAA TM-Server ihre eigenen Authentifizierungsrichtlinien haben?

In diesem Szenario muss für den Lastausgleichsserver die Option FQDN für die Authentifizierung so eingestellt sein, dass sie auf den virtuellen Citrix ADC AAA TM-Server zeigt. Der virtuelle Citrix ADC AAA TM Server muss über eine unabhängige IP-Adresse verfügen und von Citrix ADC und Clients aus erreichbar sein.

### Ist ein virtueller Citrix ADC AAA TM Authentication Server erforderlich, um Benutzer zu authentifizieren, die über einen virtuellen Unified Gateway-Server kommen?

Nein. Der virtuelle Citrix Gateway-Server authentifiziert sogar die Benutzer von Citrix ADC AAA TM.

### Wo geben Sie Citrix Gateway-Authentifizierungsrichtlinien an —auf dem virtuellen Unified Gateway-Server oder auf dem virtuellen Citrix Gateway-Server?

Authentifizierungsrichtlinien müssen an den virtuellen Citrix Gateway-Server gebunden sein.

### Wie aktivieren Sie die Authentifizierung auf den virtuellen Citrix ADC AAA TM Servern hinter einem virtuellen Unified Gateway-Content Switching-Server?

Aktivieren Sie die Authentifizierung auf dem Citrix ADC AAA TM und verweisen Sie den Authentifizierungshost auf den FQDN des Unified Gateway-Content Switching

### Wie füge ich virtuelle TM Server hinter Content Switching hinzu (einzelne URL im Vergleich zu mehreren Hosts)?

Es gibt keinen Unterschied zwischen dem Hinzufügen der virtuellen Citrix ADC AAA TM-Server für eine einzelne URL und dem Hinzufügen für mehrere Hosts. In beiden Fällen wird der virtuelle Server als Ziel in einer Content Switching-Aktion hinzugefügt. Der Unterschied zwischen einzelner URL und Multi-Host wird durch Content Switching-Richtlinien implementiert.

### Was passiert mit den Authentifizierungsrichtlinien, die an einen virtuellen Citrix ADC AAA TM-Lastausgleichsserver gebunden sind, wenn dieser virtuelle Server hinter einen virtuellen Unified Gateway-Server verschoben wird?

Authentifizierungsrichtlinien sind an den virtuellen Authentifizierungsserver gebunden, und der virtuelle Authentifizierungsserver ist an den virtuellen Lastausgleichsserver gebunden. Für den

virtuellen Unified Gateway-Server empfiehlt Citrix, den virtuellen Citrix Gateway-Server als einzelnen Authentifizierungspunkt zu verwenden, wodurch die Notwendigkeit der Authentifizierung auf einem virtuellen Authentifizierungsserver (oder sogar die Notwendigkeit eines bestimmten virtuellen Authentifizierungsservers) zunichte gemacht wird. Durch Verweisen des Authentifizierungshosts auf den virtuellen Unified Gateway-Server FQDN wird sichergestellt, dass die Authentifizierung vom virtuellen Citrix Gateway-Server erfolgt. Wenn Sie den Authentifizierungshost auf Content Switching für Unified Gateway verweisen und immer noch einen virtuellen Authentifizierungsserver gebunden haben, werden die an den virtuellen Authentifizierungsserver gebundenen Authentifizierungsrichtlinien ignoriert. Wenn Sie jedoch einen Authentifizierungshost auf einen unabhängigen virtuellen Server mit adressierbarer Authentifizierung verweisen, werden die gebundenen Authentifizierungsrichtlinien wirksam.

### Wie konfigurieren Sie Sitzungsrichtlinien für Citrix ADC AAA TM-Sitzungen?

Wenn in Unified Gateway kein virtueller Authentifizierungsserver für den virtuellen Citrix ADC AAA TM Server angegeben ist, erben die Citrix ADC AAA TM-Sitzungen die Citrix Gateway-Sitzungsrichtlinien. Wenn der virtuelle Authentifizierungsserver angegeben ist, werden die an diesen virtuellen Server gebundenen Citrix ADC AAA TM-Sitzungsrichtlinien angewendet.

### Was sind die Änderungen am Citrix Gateway-Portal in Citrix ADC 11.0?

In Citrix ADC-Versionen vor 11.0 kann eine einzelne Portalanpassung auf globaler Ebene eingerichtet werden. Jeder virtuelle Gateway-Server in einer bestimmten Citrix ADC Appliance verwendet die globale Portalanpassung.

In Citrix ADC 11.0 können Sie mit der Funktion Portal-Designs mehrere Portal-Designs einrichten. Themen können global oder an bestimmte virtuelle Server gebunden sein.

### Unterstützt Citrix ADC 11.0 die Anpassung des Citrix Gateway-Portals?

Mithilfe des Konfigurationsdienstprogramms können Sie die neue Funktion Portal-Designs verwenden, um die Portal-Themen vollständig anzupassen und zu erstellen. Sie können verschiedene Bilder hochladen, Farbschemata festlegen, Textbeschriftungen ändern und so weiter.

Die Portalseiten, die angepasst werden können, sind:

- Anmeldeseite
- Seite Endpoint Analysis
- Endpoint Analysis-Fehlerseite
- Seite Endpoint Analysis veröffentlichen

- Seite VPN-Verbindung
- Portal-Startseite

Mit dieser Version können Sie virtuelle Citrix Gateway-Server mit einzigartigen Portaldesigns anpassen.

### Werden Portal-Themen in Citrix ADC Hochverfügbarkeit oder Clusterbereitstellungen unterstützt?

Ja. Portal-Themes werden in Citrix ADC Hochverfügbarkeit und Clusterbereitstellungen unterstützt.

### Werden meine Anpassungen im Rahmen des Citrix ADC 11.0 Upgrade-Prozesses migriert?

Nein. Bestehende Anpassungen an der Citrix Gateway-Portalseite, die durch die Dateiänderung rc.conf/rc.netscaler oder mithilfe der benutzerdefinierten Designfunktionalität in 10.1/10.5 aufgerufen werden, werden beim Upgrade auf Citrix ADC 11.0 nicht automatisch migriert.

### Gibt es Schritte vor dem Upgrade, um für Portal-Themen in Citrix ADC 11.0 bereit zu sein?

Alle vorhandenen Anpassungen müssen aus den Dateien rc.conf oder rc.netscaler entfernt werden.

Die andere Option ist, dass, wenn benutzerdefinierte Designs verwendet werden, ihnen die Standardeinstellung zugewiesen werden muss:

1. Navigieren Sie zu **Konfiguration > Citrix Gateway > Globale Einstellungen**
2. Klicken Sie auf **Globale Einstellungen ändern**.
3. Klicken Sie auf **Client Experience** und wählen Sie **Standard** aus der Liste **UI-Thema**.

### Ich habe Anpassungen, die auf der Citrix ADC-Instanz gespeichert sind und von rc.conf oder rc.netscaler aufgerufen werden. Wie wechsle ich zu Portaldesigns?

Citrix Knowledge Center-Artikel CTX126206 beschreibt eine solche Konfiguration für Citrix ADC 9.3 und 10.0 Versionen bis zu 10.0 Build 73.5001.e. Seit Citrix ADC 10.0 Build 10.0 73.5002.e (einschließlich 10.1 und 10.5) steht der UITHEME CUSTOM-Parameter zur Verfügung, mit dem Kunden ihre Anpassungen über Neustarts hinweg beibehalten können. Wenn die Anpassungen auf der Citrix ADC-Festplatte

gespeichert sind und Sie diese Anpassungen weiterhin verwenden möchten, sichern Sie die 11.0 GUI-Dateien und fügen Sie sie in die vorhandene benutzerdefinierte Design-Datei ein. Wenn Sie zu Portaldesigns wechseln möchten, müssen Sie zuerst den UITHEME-Parameter in den globalen Einstellungen oder im Sitzungsprofil unter **Client**Experience deaktivieren. Oder Sie können es auf DEFAULT oder GREENBUBBLE setzen. Dann können Sie beginnen, ein Portaldesign zu erstellen und zu binden.

### Wie kann ich meine aktuellen Anpassungen exportieren und speichern, bevor ich auf Citrix ADC 11.0 upgrade? Kann ich die exportierten Dateien auf eine andere Citrix ADC Appliance verschieben?

Die angepassten Dateien, die in den Ordner **ns_gui_custom** hochgeladen wurden, sind auf dem Datenträger und bleiben über Upgrades hinweg bestehen. Diese Dateien sind jedoch möglicherweise nicht vollständig mit dem neuen Citrix ADC 11.0 Kernel und anderen GUI-Dateien kompatibel, die Teil des Kernels sind. Daher empfiehlt Citrix, ein Backup der 11.0 GUI-Dateien anzulegen und das Backup anzupassen.

Darüber hinaus enthält das Konfigurationsprogramm kein Hilfsprogramm, um den Ordner **ns_custom_gui auf eine andere Citrix ADC Appliance** zu exportieren. Verwenden Sie SSH oder ein Dateiübertragungsprogramm wie WinSCP, um die Dateien von der Citrix ADC-Instanz zu entfernen.

### Werden Portaldesigns für virtuelle Citrix ADC AAA TM Server unterstützt?

Ja. Portaldesigns werden für virtuelle Citrix ADC AAA TM-Server unterstützt.

### Was hat sich an der RDP-Proxy-Funktion für Citrix Gateway 11.0 geändert?

Seit der Erweiterungsversion von Citrix ADC 10.5.e wurden viele Verbesserungen an RDP Proxy vorgenommen. In Citrix ADC 11.0 ist diese Funktion ab dem ersten veröffentlichten Build verfügbar.

#### Änderungen an der Lizenzierung

Die RDP-Proxy-Funktion in Citrix ADC 11.0 kann nur mit Premium- und Advanced-Editionen verwendet werden. Citrix Concurrent User (CCU) -Lizenzen müssen für jeden Benutzer bezogen werden.

#### Befehl aktivieren

In Citrix ADC 10.5.e gab es keinen Befehl zum Aktivieren von RDP-Proxy. In Citrix ADC 11.0 wurde der Befehl enable hinzugefügt:

```
enable feature rdpproxy
<!--NeedCopy-->
```

Die Funktion muss lizenziert sein, um diesen Befehl ausführen zu können.

#### Andere RDP-Proxy-Änderungen

Ein Pre-Shared Key (PSK) -Attribut im Serverprofil wurde obligatorisch gemacht.

Um vorhandene Citrix ADC 10.5.e-Konfigurationen für RDP-Proxy auf Citrix ADC 11.0 zu migrieren, müssen die folgenden Details verstanden und angesprochen werden.

Wenn ein Administrator einer ausgewählten Unified Gateway-Bereitstellung eine vorhandene RDP-Proxy-Konfiguration hinzufügen möchte:

- Die IP-Adresse des virtuellen Citrix Gateway-Servers muss bearbeitet und auf eine nicht adressierbare IP-Adresse (0.0.0.0) festgelegt werden.
- Alle SSL-/TLS-Serverzertifikate und Authentifizierungsrichtlinien müssen an den virtuellen Citrix Gateway-Server gebunden sein, der Teil der ausgewählten Unified Gateway-Formation ist.

### Wie migrieren Sie eine Remote Desktop Protocol (RDP) -Proxy-Konfiguration basierend auf Citrix ADC 10.5.e auf Citrix ADC 11.0?

Option 1: Behalten Sie den vorhandenen virtuellen Citrix Gateway-Server mit RDP-Proxy-Konfiguration mit einer Premium- oder Advanced-Lizenz bei.

Option 2: Verschieben Sie den vorhandenen virtuellen Citrix Gateway-Server mit RDP-Proxy-Konfiguration und platzieren Sie ihn hinter einem virtuellen Unified Gateway-Server.

Option 3: Fügen Sie einem vorhandenen Standard Edition-Gerät einen eigenständigen virtuellen Citrix Gateway-Server mit RDP-Proxy-Konfiguration hinzu.

### Wie richten Sie Citrix Gateway für die RDP-Proxy-Konfiguration mithilfe der Citrix ADC 11.0 Version ein?

Es gibt zwei Möglichkeiten, RDP-Proxy mithilfe der Version NS 11.0 bereitzustellen:

1. Verwenden eines nach außen gerichteten virtuellen Citrix Gateway-Servers. Dies erfordert eine extern sichtbare IP-Adresse/FQDN für den virtuellen Citrix Gateway-Server.Diese Option ist in Citrix ADC 10.5.e verfügbar.
2. Verwenden eines virtuellen Unified Gateway-Servers, der den virtuellen Citrix Gateway-Server voranstellt.

Mit Option 2 benötigt der virtuelle Citrix Gateway-Server keine eigene IP-Adresse/FQDN, da er eine nicht adressierbare IP-Adresse (0.0.0.0) verwendet.

### Ist HDX Insight mit Unified Gateway kompatibel?

Wenn Citrix Gateway mit Unified Gateway bereitgestellt wird, müssen die folgenden Bedingungen erfüllt sein:

- Der virtuelle Citrix Gateway-Server muss über ein gültiges SSL-Zertifikat verfügen, das an ihn gebunden ist.
- Der virtuelle Citrix Gateway-Server muss sich in einem UP-Status befinden, um AppFlow-Datensätze auf Citrix ADM für die HDX Insight-Berichterstattung zu generieren.

### Wie migriere ich meine bestehende HDX Insight-Konfiguration?

Es ist keine Migration erforderlich. AppFlow-Richtlinien, die an einen virtuellen Citrix Gateway-Server gebunden sind, werden übernommen, wenn dieser virtuelle Citrix Gateway-Server hinter einen virtuellen Unified Gateway-Server gestellt wird.

Für vorhandene Daten auf Citrix ADM für den virtuellen Citrix Gateway-Server gibt es zwei Möglichkeiten:

- Wenn die IP-Adresse des virtuellen Citrix Gateway-Servers im Rahmen der Migration zu Unified Gateway einem virtuellen Unified Gateway-Server zugewiesen wird, bleiben die Daten mit dem virtuellen Citrix Gateway-Server verknüpft.
- Wenn dem virtuellen Unified Gateway-Server eine separate IP-Adresse zugewiesen wird, werden AppFlow-Daten vom virtuellen Citrix Gateway-Server mit dieser neuen IP-Adresse verknüpft. Daher sind vorhandene Daten nicht Teil neuer Daten.

## VPN-Konfiguration auf einem Citrix Gateway-Gerät

March 27, 2024

> **Wichtig:**
>
> Die Bildschirmaufnahmen in diesem Abschnitt werden aus folgenden Gründen in einem Graustufenschema verwaltet:
>
> - Helfen Sie sehbehinderten Lesern, insbesondere solchen mit Farbenblindheit oder Farbmangel.
> - Die Verwendung eines Graustufenbildes stellt das Bild in einer generischen Form dar, die keine Auswirkungen der Anpassung der Farbcodierung zeigt, die möglicherweise im Browser oder im Betriebssystem des Benutzers vorgenommen wurde.

Benutzer können die folgenden Methoden verwenden, um über Citrix Gateway eine Verbindung zu den Netzwerkressourcen Ihres Unternehmens herzustellen:

- Citrix Workspace-App, die alle auf dem Benutzergerät installierten Citrix Plug-Ins enthält.
- Citrix Workspace-App für das Web, die Benutzerverbindungen zu Anwendungen, Desktops und ShareFile mithilfe eines Webbrowsers ermöglicht.
- Secure Hub ermöglicht Benutzern den Zugriff auf Secure Mail, WorxWeb und mobile Apps von ihren iOS- und Android-Geräten aus.
- Citrix Gateway Plug-in für Windows, macOS X oder Linux.
- Citrix Gateway App für iOS und Android.
- Citrix Gateway Plug-in für Java.
- Clientloser Zugriff, der Benutzern den Zugriff bietet, den sie benötigen, ohne Benutzersoftware zu installieren.
- Interoperabilität mit dem Citrix SD-WAN SD-WAN-Plug-In.

Wenn Benutzer das Citrix Gateway Plug-in installieren und dann die Citrix Workspace-App von Citrix Virtual Apps 6.5 für Windows Server 2008 (einschließlich Feature Pack und Feature Pack 2), Citrix Virtual Desktops 7.0 oder neuer installieren, fügt die Citrix Workspace-App automatisch das Citrix Gateway-Plug-in hinzu. Benutzer können sich über einen Webbrowser oder über die Citrix Workspace-App mit dem Citrix Gateway-Plug-in verbinden.

SmartAccess bestimmt automatisch die Zugriffsmethoden, die für ein Benutzergerät zulässig sind, basierend auf den Ergebnissen eines Endpoint Analysis-Scans. Weitere Informationen zu SmartAccess finden Sie unter SmartAccess konfigurieren.

Citrix Gateway unterstützt Citrix Endpoint Management-Apps für mobile Produktivitätsanwendungen für iOS- und Android-Mobilgeräte. Citrix Gateway enthält Secure Browse, das Verbindungen zu Citrix Gateway von iOS-Mobilgeräten ermöglicht, die den Micro-VPN-Tunnel einrichten. Android-Geräte, die sich mit dem Secure Hub verbinden, richten außerdem automatisch einen Mikro-VPN-Tunnel ein, der sicheren Zugriff auf Web- und Mobilanwendungsebene auf Ressourcen in Ihrem internen Netzwerk bietet. Wenn Benutzer von einem Android-Gerät aus eine Verbindung mit mobilen Produktivitätsapps

herstellen, müssen Sie DNS-Einstellungen auf Citrix Gateway konfigurieren. Einzelheiten finden Sie unter Unterstützung von DNS-Abfragen mithilfe von DNS-Suffixen für Android-Geräte.

## So verbinden sich Benutzer mit dem Citrix Gateway Plug-in

March 27, 2024

Citrix Gateway funktioniert wie folgt:

- Wenn Benutzer versuchen, über den VPN-Tunnel auf Netzwerkressourcen zuzugreifen, verschlüsselt das Citrix Gateway Plug-in den gesamten Netzwerkverkehr, der für das interne Netzwerk der Organisation bestimmt ist, und leitet die Pakete an Citrix Gateway weiter.
- Citrix Gateway beendet den SSL-Tunnel, akzeptiert eingehenden Datenverkehr, der für das private Netzwerk bestimmt ist, und leitet den Datenverkehr an das private Netzwerk weiter. Citrix Gateway sendet den Datenverkehr über einen sicheren Tunnel zurück zum Remotecomputer.

Wenn Benutzer die Webadresse eingeben, erhalten sie eine Anmeldeseite, auf der sie ihre Anmeldeinformationen eingeben und sich anmelden. Wenn die Anmeldeinformationen korrekt sind, beendet Citrix Gateway den Handshake mit dem Benutzergerät.

Wenn Benutzer hinter einem Proxyserver sind, können sie den Proxyserver und die Authentifizierungsinformationen angeben. Weitere Informationen finden Sie unter Aktivieren der Proxy-Unterstützung für Benutzerverbindungen.

Das Citrix Gateway Plug-in ist auf dem Benutzergerät installiert. Wenn sich Benutzer nach der ersten Verbindung mit einem Windows-basierten Computer anmelden, können sie das Symbol im Infobereich verwenden, um die Verbindung herzustellen.

### Stellen Sie den sicheren Tunnel her

Wenn Benutzer eine Verbindung mit dem Citrix Gateway Plug-in, Secure Hub oder der Citrix Workspace-App herstellen, richtet die Clientsoftware einen sicheren Tunnel über Port 443 (oder einen konfigurierten Port auf Citrix Gateway) ein und sendet Authentifizierungsinformationen. Wenn der Tunnel eingerichtet ist, sendet Citrix Gateway Konfigurationsinformationen an das Citrix Gateway Plug-in, Secure Hub oder die Citrix Workspace-App, in denen die zu sichernden Netzwerke beschrieben werden und eine IP-Adresse enthalten, wenn Sie Adresspools aktivieren.

#### Tunnel des privaten Netzwerkverkehrs über sichere Verbindungen

Wenn das Citrix Gateway Plug-in gestartet wird und der Benutzer authentifiziert wird, wird der gesamte Netzwerkverkehr, der für bestimmte private Netzwerke bestimmt ist, erfasst und über den

sicheren Tunnel zu Citrix Gateway umgeleitet. Die Citrix Workspace-App muss das Citrix Gateway-Plug-in unterstützen, um die Verbindung über den sicheren Tunnel herzustellen, wenn sich Benutzer anmelden.

Secure Hub, Secure Mail und WorxWeb verwenden Micro VPN, um den sicheren Tunnel für iOS- und Android-Mobilgeräte einzurichten.

Citrix Gateway fängt alle Netzwerkverbindungen ab, die das Benutzergerät herstellt, und multiplext sie über Secure Sockets Layer (SSL) an Citrix Gateways, wo der Datenverkehr demultiplext wird und die Verbindungen an die richtige Host- und Port-Kombination weitergeleitet werden.

Die Verbindungen unterliegen administrativen Sicherheitsrichtlinien, die für eine einzelne Anwendung, eine Teilmenge von Anwendungen oder ein ganzes Intranet gelten. Sie geben die Ressourcen (Bereiche von IP-Adressen/Subnetzpaaren) an, auf die Remotebenutzer über die VPN-Verbindung zugreifen können.

Das Citrix Gateway Plug-In fängt und tunnelt die folgenden Protokolle für die definierten Intranet-Anwendungen:

- TCP (alle Ports)
- UDP (alle Ports)
- ICMP (Typen 8 und 0 - Echo Request/Reply)

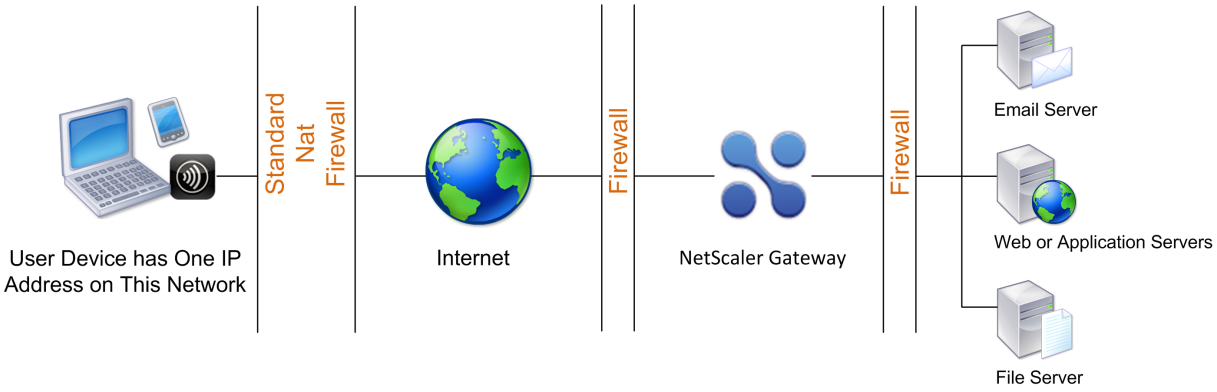
Verbindungen von lokalen Anwendungen auf dem Benutzergerät werden sicher an Citrix Gateway getunnelt, wodurch die Verbindungen zum Zielserver wiederhergestellt werden. Zielserver sehen Verbindungen als vom lokalen Citrix Gateway im privaten Netzwerk stammend an und verbergen so das Benutzergerät. Dies wird auch als umgekehrte Netzwerkadressübersetzung (NAT) bezeichnet. Das Ausblenden von IP-Adressen erhöht die Sicherheit der Quellspeicherorte.

Lokal auf dem Benutzergerät wird der gesamte verbindungsbezogene Datenverkehr wie SYN-ACK-, PUSH-, ACK- und FIN-Pakete vom Citrix Gateway-Plug-in neu erstellt, um vom privaten Server aus zu erscheinen.

### Verbinden Sie sich über Firewalls und Proxys

Benutzer des Citrix Gateway-Plug-Ins befinden sich manchmal in der Firewall einer anderen Organisation, wie in der folgenden Abbildung dargestellt:




NAT-Firewalls verwalten eine Tabelle, die es ihnen ermöglicht, sichere Pakete von Citrix Gateway zurück zum Benutzergerät zu leiten. Für leitungsorientierte Verbindungen verwaltet Citrix Gateway eine Port-zugeordnete, umgekehrte NAT-Übersetzungstabelle. Mit der umgekehrten NAT-Übersetzungstabelle kann Citrix Gateway Verbindungen abgleichen und Pakete mit den richtigen Portnummern über den Tunnel an das Benutzergerät zurücksenden, damit die Pakete zur richtigen Anwendung zurückkehren.

### Steuern des Upgrades von Citrix Gateway-Plug-Ins

Systemadministratoren steuern, wie das Citrix ADC-Plug-In funktioniert, wenn seine Version nicht mit der Citrix Gateway-Revision übereinstimmt. Die neuen Optionen steuern das Plug-In-Upgrade-Verhalten für Mac und Windows oder Betriebssysteme.

Für VPN-Plug-Ins kann die Upgrade-Option an zwei Stellen in der Benutzeroberfläche der Citrix ADC Appliance festgelegt werden:

- Bei den globalen Einstellungen
- Auf der Ebene des Sitzungsprofils

### Anforderungen

- Windows EPA- und VPN-Plug-In-Version muss größer als 11.0.0.0 sein
- Die Mac EPA-Plug-In-Version muss größer als 3.0.0.31 sein
- Die Mac-VPN-Plug-In-Version muss größer als 3.1.4 sein (357)

> **Hinweis:**
>
> Wenn die Citrix ADC Appliance auf die Version 11.0 aktualisiert wird, werden alle vorherigen VPN (und EPA) -Plug-Ins unabhängig von der Konfiguration der Upgrade-Steuerung auf die neueste

> Version aktualisiert. Bei nachfolgenden Upgrades respektieren sie die vorherige Konfiguration der Upgrade-Steuerung.

**Plug-In-Verhalten**

Für jeden Clienttyp ermöglicht Citrix Gateway die folgenden drei Optionen zur Steuerung des Plug-In-Upgrade-Verhaltens:

- **Immer**

Das Plug-In wird immer dann aktualisiert, wenn die Plug-In-Version des Endbenutzers nicht mit dem mit der Citrix ADC Appliance gelieferten Plug-In übereinstimmt. Dies ist das Standardverhalten. Wählen Sie diese Option, wenn Sie nicht möchten, dass mehrere Plug-In-Versionen in Ihrem Unternehmen ausgeführt werden.

- **Wesentlich** (und Sicherheit)

Das Plug-In wurde nur aktualisiert, wenn es für notwendig erachtet wird. Upgrades werden unter den folgenden beiden Umständen als notwendig erachtet:

- Das installierte Plug-In ist nicht mit der aktuellen Citrix ADC Appliance-Version kompatibel.
- Das installierte Plug-In muss für die notwendige Sicherheitskorrektur aktualisiert werden.

Wählen Sie diese Option, wenn Sie die Anzahl der Plug-In-Upgrades minimieren möchten, aber keine Plug-In-Sicherheitsupdates verpassen möchten

- **Nie**

Das Plug-In wird nicht aktualisiert.

**CLI-Parameter zur Steuerung des VPN-Plug-In-Upgrades**

Citrix Gateway unterstützt zwei Arten von Plug-Ins (EPA und VPN) für Windows- und Mac-Betriebssysteme. Um die Upgrade-Steuerung des VPN-Plug-Ins auf Sitzungsebene zu unterstützen, unterstützt Citrix Gateway zwei Sitzungsprofilparameter mit den Namen WindowsInPluginUpgrade und MacPluginUpgrade.

Diese Parameter sind auf globaler, virtueller Server-, Gruppen- und Benutzerebene verfügbar. Jeder Parameter kann den Wert Always, Essential oder Never haben. Eine Beschreibung dieser Parameter finden Sie unter Plug-In-Verhalten.

### CLI-Parameter zur Steuerung des EPA-Plug-In-Upgrades

Citrix Gateway unterstützt EPA-Plug-Ins für Windows- und Mac-Betriebssysteme. Zur Unterstützung der EPA-Plug-In-Upgrade-Steuerung auf virtueller Serverebene unterstützt Citrix Gateway zwei virtuelle Serverparameter mit den Namen windowsEPAPluginUpgrade und macEPAPluginUpgrade.

Die Parameter sind auf der Ebene des virtuellen Servers verfügbar. Jeder Parameter kann den Wert Always, Essential oder Never haben. Eine Beschreibung dieser Parameter finden Sie unter Plug-In-Verhalten.

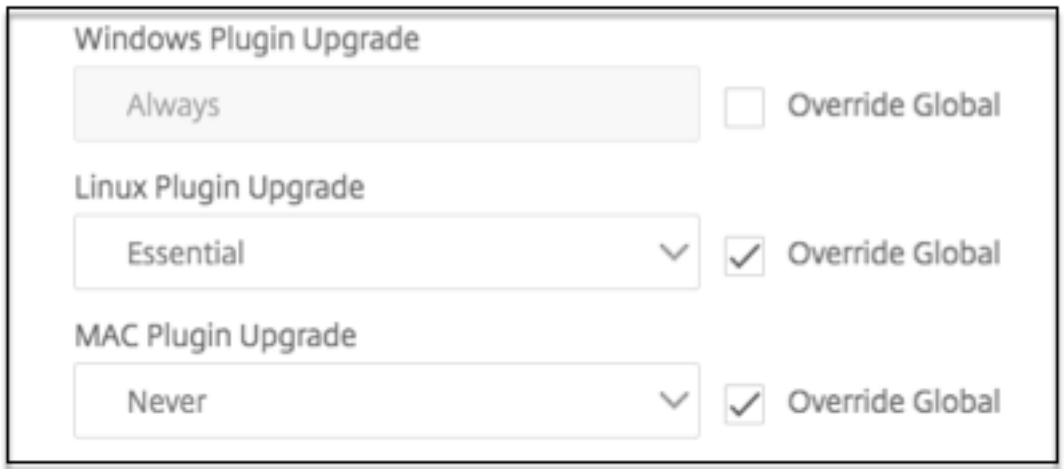
### VPN-Konfiguration

Folgen Sie diesen Schritten für die **VPN-Konfiguration von** Windows-, Linux- und Mac-Plug-ins.

1. Wechseln Sie zu **Citrix ADC > Richtlinien > Sitzung.**
2. Wählen Sie die gewünschte Sitzungsrichtlinie aus und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie die Registerkarte **Kundenerlebnis**
4. Diese Optionen in den Dialogfeldern beeinflussen das Upgrade-Verhalten.

   - Immer
   - Wesentlich
   - Nie

   Die Standardeinstellung ist Immer.
5. Aktivieren Sie das Kontrollkästchen rechts neben jeder Option. Wählen Sie die Häufigkeit für die Anwendung des Upgrade-Verhaltens



### EPA-Konfiguration

Befolgen Sie diese Schritte für die EPA-Konfiguration von Windows-, Linux- und Apple-Plug-Ins.

1. Wechseln Sie zu **Citrix Gateway > Virtuelle Server**.
2. Wählen Sie einen Server aus und klicken Sie auf die Schaltfläche **Bearbeiten**.
3. Klicken Sie auf das **Stiftsymbol**.


4. Klicken Sie auf **Mehr**
5. Die angezeigten Dialogfelder wirken sich auf das Upgrade-Verhalten aus. Es gibt folgende Optionen:

    - Immer
    - Wesentlich
    - Nie

## Setup des vollständigen VPNs in Citrix Gateway

March 27, 2024

In diesem Abschnitt wird beschrieben, wie Sie das vollständige VPN-Setup auf einem Citrix Gateway-Gerät konfigurieren. Es enthält Netzwerküberlegungen und den idealen Ansatz zur Lösung von Problemen aus Netzwerkperspektive.

### Voraussetzungen

- Installieren Sie ein SSL-Zertifikat und binden Sie es an den virtuellen VPN-Server.

  - CTX109260 - Generieren und Installieren eines öffentlichen SSL-Zertifikats auf einer NetScaler Appliance
  - CTX122521 - Ersetzen des Standardzertifikats einer NetScaler Appliance durch ein vertrauenswürdiges CA-Zertifikat, das dem Hostnamen der Appliance entspricht
  - Citrix Dokumentation - Binden des Zertifikatschlüsselpaars an den SSL-basierten virtuellen Server

- Erstellen Sie ein Authentifizierungsprofil für Citrix Gateway.
  - Weitere Informationen finden Sie in der Citrix Documentation - Configuring Externe Benutzerauthentifizierung
  - Weitere Informationen finden Sie in Checkliste: Verwenden Sie AD FS, um Single Sign-On zu implementieren und zu verwalten
- Laden Sie den Citrix VPN Clientherunter.
- Erstellen Sie eine Sitzungsrichtlinie, die vollständige VPN-Verbindungen ermöglicht.

Wenn Benutzer eine Verbindung mit dem Citrix Gateway Plug-in, Secure Hub oder der Citrix Workspace-App herstellen, richtet die Clientsoftware einen sicheren Tunnel über Port 443 (oder einen konfigurierten Port auf Citrix Gateway) ein und sendet Authentifizierungsinformationen. Sobald der Tunnel eingerichtet wurde, sendet Citrix Gateway Konfigurationsinformationen an das Citrix Gateway Plug-in, Citrix Secure Hub oder die Citrix Workspace-App, in denen die zu sichernden Netzwerke beschrieben werden. Diese Informationen enthalten auch eine IP-Adresse, wenn Sie Intranet-IPs aktivieren.

Sie konfigurieren Benutzergeräteverbindungen, indem Sie die Ressourcen definieren, auf die Benutzer im internen Netzwerk zugreifen können. Das Konfigurieren von Benutzergeräteverbindungen umfasst Folgendes:

- Split-Tunneling
- IP-Adressen für Benutzer, einschließlich Adresspools (Intranet-IPs)
- Verbindungen über einen Proxyserver
- Definieren der Domains, auf die Benutzer Zugriff haben
- Timeout-Einstellungen
- Single Sign-On
- Benutzersoftware, die über Citrix Gateway eine Verbindung herstellt
- Zugriff für mobile Geräte

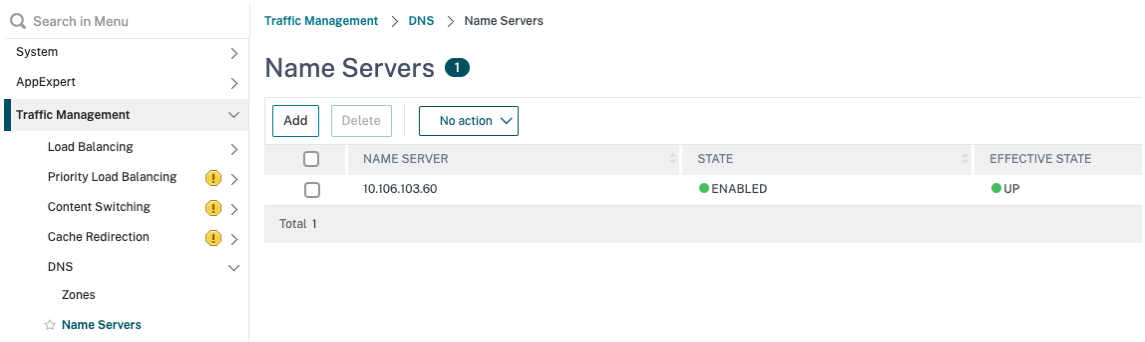
Sie konfigurieren die meisten Benutzergeräteverbindungen mithilfe eines Profils, das Teil einer Sitzungsrichtlinie ist. Sie können auch Verbindungseinstellungen für Benutzergeräte definieren, indem Sie Per-Authentifizierungs-, Traffic- und Autorisierungsrichtlinien verwenden. Sie können auch mithilfe von Intranet-Anwendungen konfiguriert werden.

## Konfigurieren eines vollständigen VPN-Setups auf einem Citrix Gateway-Gerät

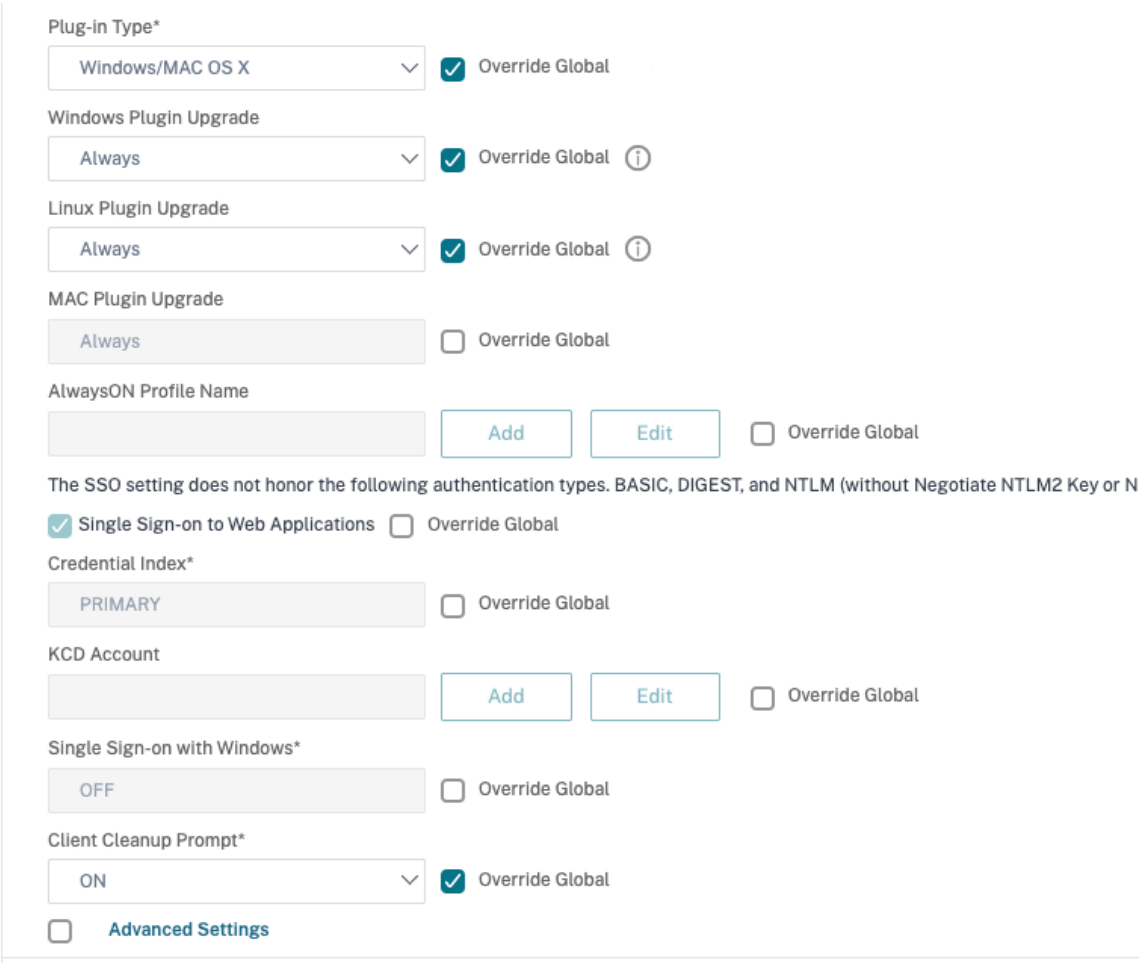
Führen Sie das folgende Verfahren aus, um ein VPN-Setup auf dem Citrix Gateway-Gerät zu konfigurieren:

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Wählen Sie den Knoten Nameserver aus, wie im folgenden Screenshot gezeigt. Stellen Sie sicher, dass der DNS-Nameserver aufgeführt ist. Wenn es nicht verfügbar ist, fügen Sie einen DNS-Nameserver hinzu.



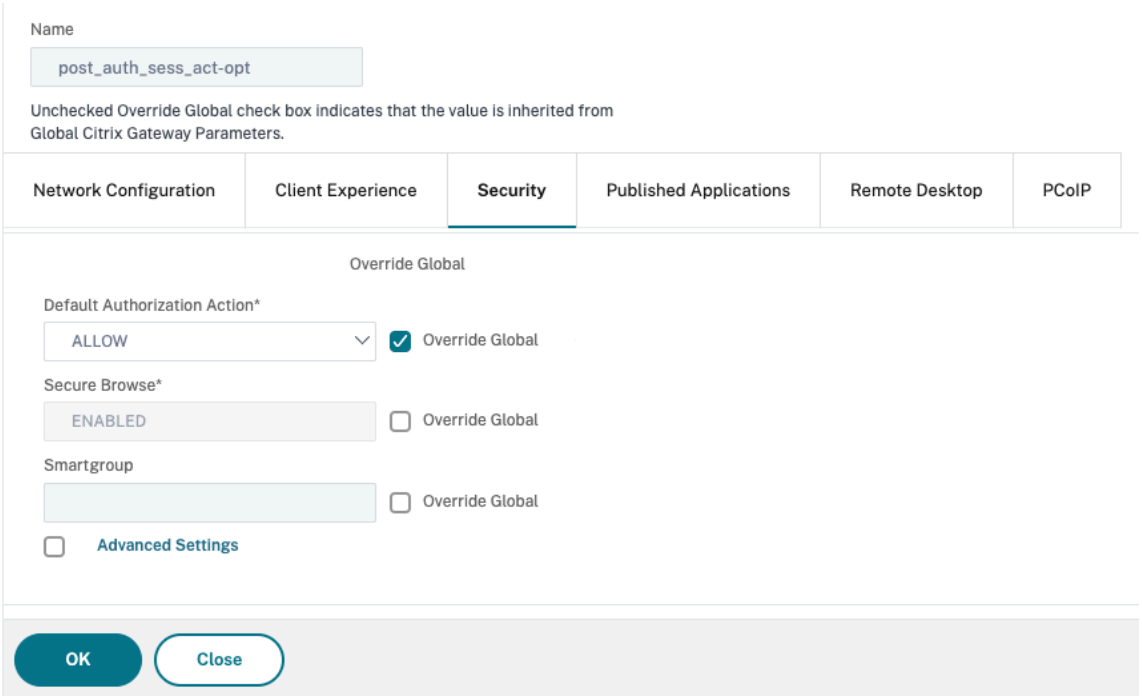

3. Erweitern Sie **Citrix Gateway > Richtlinien**.
4. Wählen Sie den Knoten **Session** aus.
5. Klicken Sie auf der Seite Citrix Gateway Sitzungsrichtlinien und -profile auf die Registerkarte **Profile** und klicken Sie auf **Hinzufügen**.
   Stellen Sie für jede Komponente, die Sie im Dialogfeld "Citrix Gateway-Sitzungsprofil konfigurieren"konfigurieren, sicher, dass Sie die Option **Override Global** für die entsprechende Komponente auswählen.
6. Klicken Sie auf den Tab „ **Kundenerlebnis** ".
7. Geben Sie die URL des Intranetportals in das Feld Startseite ein, wenn Sie eine URL angeben möchten, wenn sich der Benutzer beim VPN anmeldet. Wenn der Homepage-Parameter auf "nohomepage.html"eingestellt ist, wird die Homepage nicht angezeigt. Wenn das Plug-In startet, startet eine Browser-Instanz und wird automatisch getötet.
8. Stellen Sie sicher, dass Sie die gewünschte Einstellung aus der Liste Split-Tunnel auswählen.
9. Wählen Sie **OFF** aus der Liste **Clientless Access** aus, wenn Sie FullVPN wünschen.
10. Stellen Sie sicher, dass **Windows/Mac OS X** aus der Liste **Plug-In-Typ** ausgewählt ist.
11. Wählen Sie **bei Bedarf die Option Single Sign-On bei Webanwendungen**.
12. Stellen Sie sicher, dass die Option **Clientbereinigungsaufforderung** bei Bedarf ausgewählt ist, wie im folgenden Screenshot gezeigt:

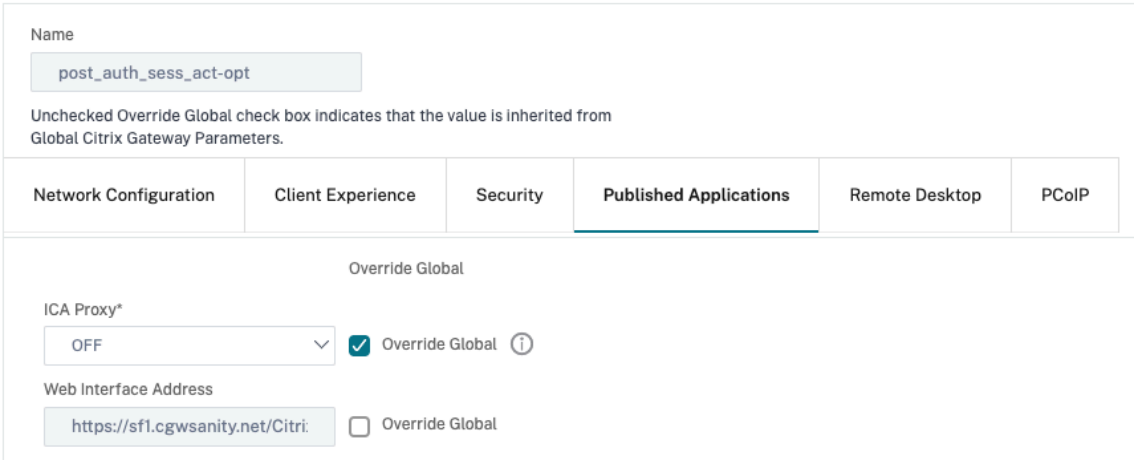



13. Klicken Sie auf die Registerkarte **Sicherheit**.
14. Stellen Sie sicher, **dass** ALLOW aus der Liste der **Standardautorisierungsaktionen** ausgewählt ist.

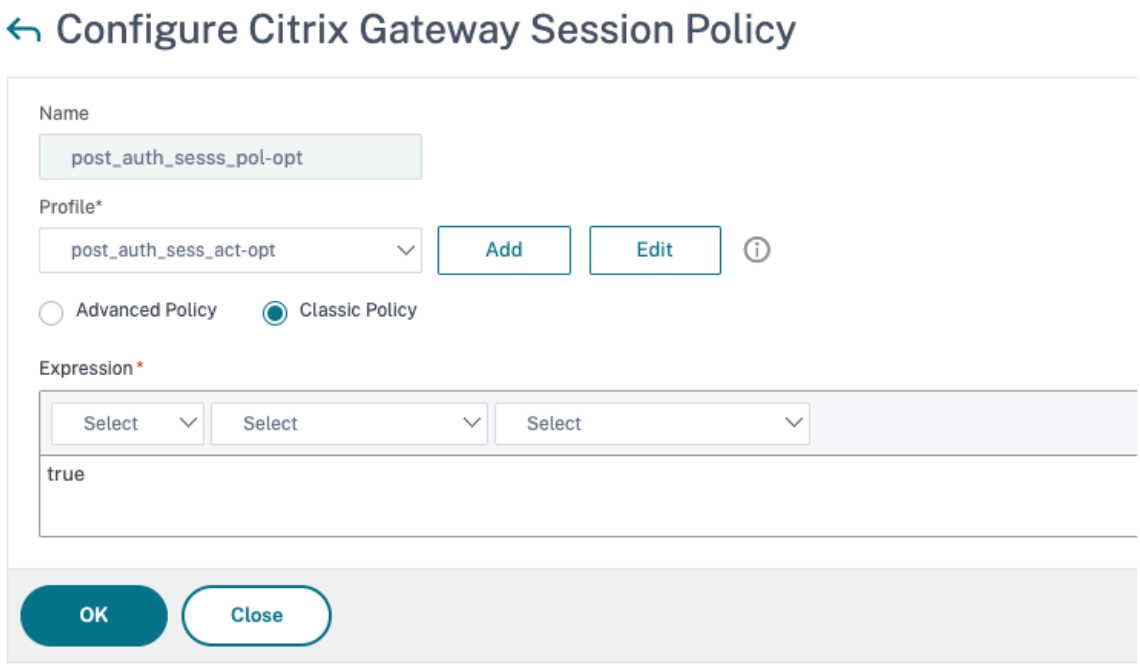



15. Klicken Sie auf die Registerkarte **Published Applications**.
16. Stellen Sie sicher, dass **OFF** aus der **ICA-Proxy-Liste** unter der Option **Veröffentlichte Anwendungen** ausgewählt ist.




17. Klicken Sie auf **Erstellen**.
18. Klicken Sie auf **Schließen**.
19. **Klicken Sie auf der Seite Citrix Gateway-Sitzungsrichtlinien und -profile im virtuellen Server auf die Registerkarte Richtlinien oder aktivieren Sie die Sitzungsrichtlinien nach Bedarf auf GRUPPE-/BENUTZER-Ebene.**
20. Erstellen Sie eine Sitzungsrichtlinie mit einem erforderlichen Ausdruck oder true, wie im folgenden Screenshot gezeigt:



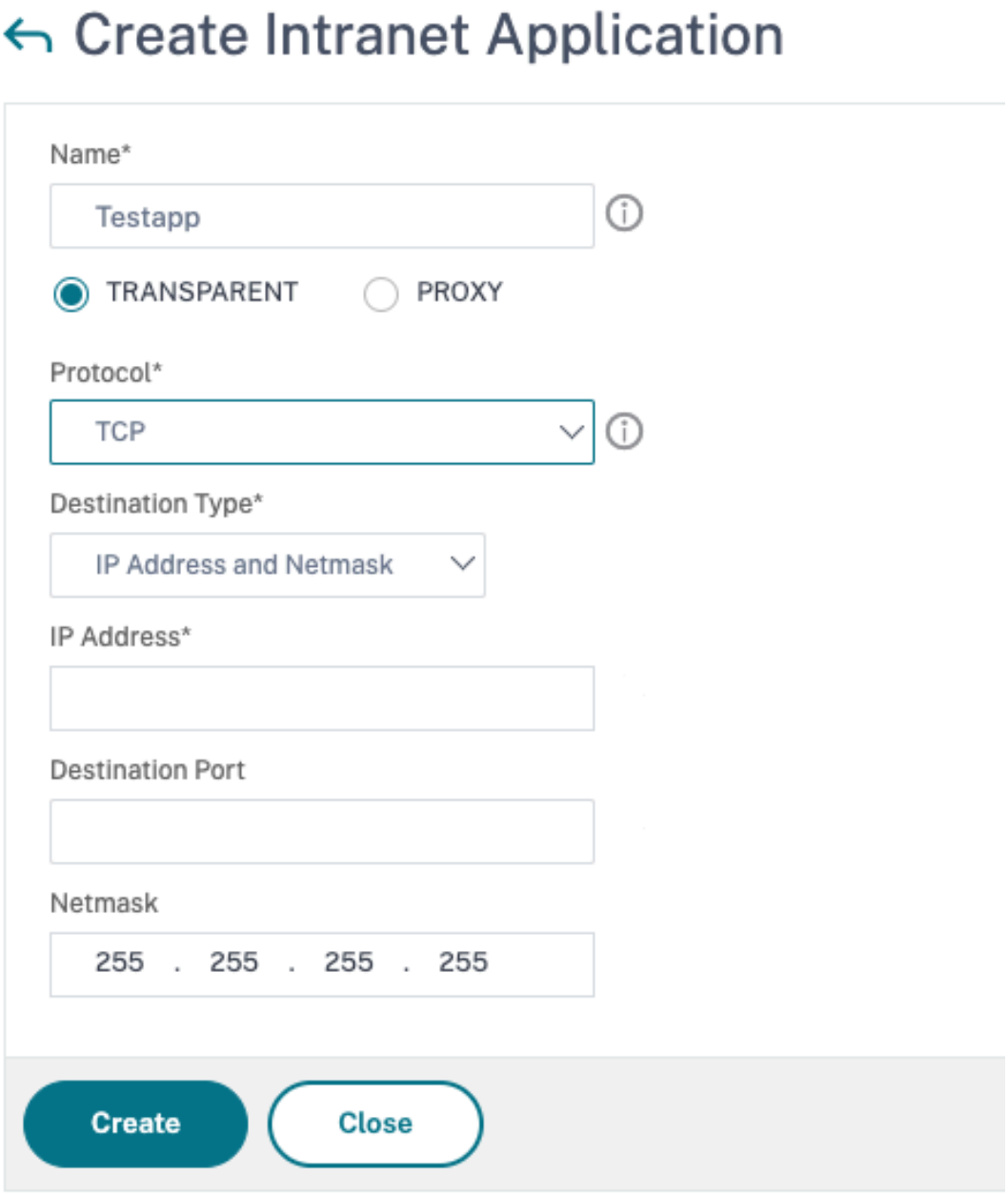

21. Binden Sie die Sitzungsrichtlinie an den virtuellen VPN-Server. Einzelheiten finden Sie unter Bind-Sitzungsrichtlinien.

    Wenn Split Tunnel auf ON konfiguriert wurde, müssen Sie die Intranet-Anwendungen konfigurieren, auf die die Benutzer zugreifen sollen, wenn sie mit dem VPN verbunden sind. Einzelheiten zu Intranetanwendungen finden Sie unter Konfigurieren von Intranetanwendungen für den Citrix Secure Access Client.

    a) Wechseln Sie zu **Citrix Gateway > Ressourcen > Intranet-Anwendungen**.

    b) Erstellen Sie eine Intranet-Anwendung. Wählen Sie Transparent für FullVPN mit Windows Client. Wählen Sie das Protokoll aus, das Sie zulassen möchten (TCP, UDP oder ANY), Zieltyp (IP-Adresse und Maske, IP-Adressbereich oder Hostname).



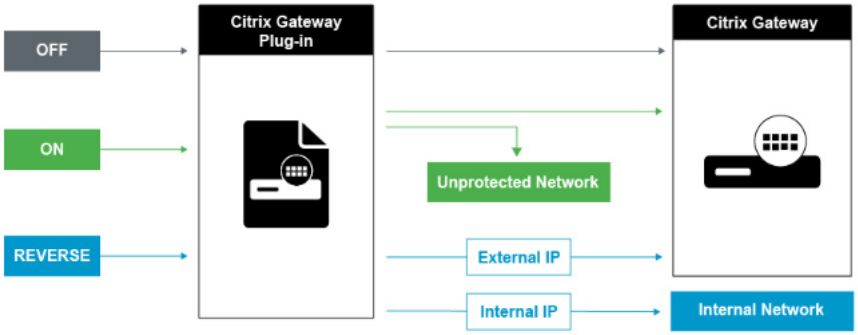

c) Legen Sie bei Bedarf eine neue Richtlinie für VPN unter iOS und Android mithilfe des folgenden Ausdrucks fest:
`HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")`

d) Binden Sie die auf USER/GROUP/VSERVER-Ebene erstellten Intranet-Anwendungen nach Bedarf.

### Andere Parameter

Im Folgenden sind einige der Parameter aufgeführt, die Sie konfigurieren können, und eine kurze Beschreibung der einzelnen Parameter:




**Split-Tunnel AUS** Wenn der Split-Tunnel auf Aus eingestellt ist, erfasst das Citrix Gateway Plug-in den gesamten Netzwerkverkehr, der von einem Benutzergerät stammt, und sendet den Datenverkehr durch den VPN-Tunnel an Citrix Gateway. Mit anderen Worten, der VPN-Client richtet eine Standardroute vom Client-PC ein, die auf den Citrix Gateway VIP zeigt, was bedeutet, dass der gesamte Datenverkehr durch den Tunnel gesendet werden muss, um zum Ziel zu gelangen. Da der gesamte Verkehr durch den Tunnel gesendet wird, müssen Autorisierungsrichtlinien festlegen, ob der Verkehr zu internen Netzwerkressourcen geleitet oder verweigert werden darf.

Während auf "Aus"gestellt, läuft der gesamte Datenverkehr durch den Tunnel, einschließlich des Standard-Webverkehrs zu Websites. Wenn das Ziel darin besteht, diesen Webverkehr zu überwachen und zu steuern, müssen Sie diese Anforderungen mithilfe der Citrix ADC Appliance an einen externen Proxy weiterleiten. Benutzergeräte können über einen Proxyserver eine Verbindung herstellen, um auch auf interne Netzwerke zuzugreifen.
Citrix Gateway unterstützt die Protokolle HTTP, SSL, FTP und SOCKS. Um die Proxy-Unterstützung für Benutzerverbindungen zu aktivieren, müssen Sie diese Einstellungen auf Citrix Gateway angeben. Sie können die IP-Adresse und den Port angeben, die vom Proxyserver auf Citrix Gateway verwendet werden. Der Proxyserver wird als Forward-Proxy für alle weiteren Verbindungen zum internen Netzwerk verwendet.

Weitere Informationen finden Sie unter Proxyunterstützung für Benutzerverbindungen aktivieren.

**Split-Tunnel EIN** Sie können Split-Tunneling aktivieren, um zu verhindern, dass das Citrix Gateway Plug-in unnötigen Netzwerkverkehr an Citrix Gateway sendet. Wenn der Split-Tunnel aktiviert ist, sendet das Citrix Gateway-Plug-in nur Datenverkehr, der für Netzwerke bestimmt ist, die von Citrix Gateway geschützt sind (Intranet-Anwendungen), durch den VPN-Tunnel. Das Citrix Gateway Plug-in sendet keinen Netzwerkverkehr, der für ungeschützte Netzwerke bestimmt ist, an Citrix Gateway. Wenn das Citrix Gateway-Plug-in gestartet wird, erhält es die Liste der Intranetanwendungen von

Citrix Gateway und legt eine Route für jedes Subnetz fest, das auf der Registerkarte Intranetanwendung auf dem Client-PC definiert ist. Das Citrix Gateway Plug-in untersucht alle vom Benutzergerät übertragenen Pakete und vergleicht die Adressen in den Paketen mit der Liste der Intranetanwendungen (Routingtabelle, die beim Start der VPN-Verbindung erstellt wurde). Wenn sich die Zieladresse im Paket in einer der Intranet-Anwendungen befindet, sendet das Citrix Gateway-Plug-in das Paket durch den VPN-Tunnel an Citrix Gateway. Wenn sich die Zieladresse nicht in einer definierten Intranet-Anwendung befindet, wird das Paket nicht verschlüsselt, und das Benutzergerät leitet das Paket dann entsprechend mithilfe des ursprünglich auf dem Client-PC definierten Standard-Routing weiter. “Wenn Sie Split-Tunneling aktivieren, definieren Intranet-Anwendungen den Netzwerkverkehr, der abgefangen und durch den Tunnel gesendet wird”.

**Rückwärtsgeteilter** Citrix Gateway unterstützt auch Reverse-Split-Tunneling, das den Netzwerkverkehr definiert, den Citrix Gateway nicht abfängt. Wenn Sie Split-Tunneling auf Rückwärtsgang einstellen, definieren Intranetanwendungen den Netzwerkverkehr, den Citrix Gateway nicht abfängt. Wenn Sie Reverse-Split-Tunneling aktivieren, umgeht der gesamte Netzwerkverkehr, der an interne IP-Adressen gerichtet ist, den VPN-Tunnel, während anderer Datenverkehr über Citrix Gateway fließt. Reverse-Split-Tunneling kann verwendet werden, um den gesamten nicht lokalen LAN-Verkehr zu protokollieren. Wenn Benutzer beispielsweise über ein drahtloses Heimnetzwerk verfügen und mit dem Citrix Gateway Plug-in angemeldet sind, fängt Citrix Gateway keinen Netzwerkverkehr ab, der für einen Drucker oder ein anderes Gerät im drahtlosen Netzwerk bestimmt ist.

### Split-Tunneling konfigurieren

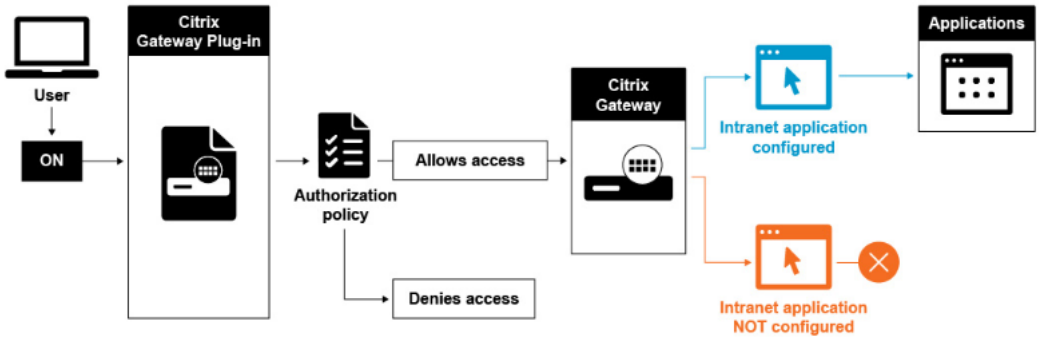
1. Navigieren Sie zu **Konfiguration** > **Citrix Gateway > Richtlinien > Sitzung**.
2. Wählen Sie im Detailbereich auf der Registerkarte Profile ein Profil aus und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie auf der Registerkarte **Client Experience** neben **Split Tunnel**die Option **Global Override**aus, wählen Sie eine Option aus, und klicken Sie dann auf **OK**.

   Konfigurieren von Split-Tunneling und Autorisierung

   Bei der Planung Ihrer Citrix Gateway-Bereitstellung ist es wichtig, Split-Tunneling sowie die Standard-Autorisierungsaktion und Autorisierungsrichtlinien in Betracht zu ziehen.

   Beispielsweise haben Sie eine Autorisierungsrichtlinie, die den Zugriff auf eine Netzwerkressource ermöglicht. Sie haben Split-Tunneling auf ON eingestellt und konfigurieren Intranet-Anwendungen nicht so, dass Netzwerkverkehr über Citrix Gateway gesendet wird. Wenn Citrix Gateway über diese Art von Konfiguration verfügt, ist der Zugriff auf die Ressource zulässig, Benutzer können jedoch nicht auf die Ressource zugreifen.




Wenn die Autorisierungsrichtlinie den Zugriff auf eine Netzwerkressource verweigert, sendet das Citrix Gateway Plug-in Datenverkehr an Citrix Gateway, aber der Zugriff auf die Ressource wird unter den folgenden Bedingungen verweigert.

- Sie haben Split-Tunneling auf ON eingestellt.
- Intranet-Anwendungen sind so konfiguriert, dass sie den Netzwerkverkehr über Citrix Gateway weiterleiten

Weitere Informationen zu Autorisierungsrichtlinien finden Sie im Folgenden:

- Autorisierung konfigurieren
- Autorisierungsrichtlinien konfigurieren
- Globale Standardermächtigung konfigurieren

So konfigurieren Sie den Netzwerkzugriff auf interne Netzwerkressourcen

1. Navigieren Sie zu **Konfiguration** > **Citrix Gateway > Ressourcen > Intranet-Anwendungen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Füllen Sie die Parameter für das Zulassen des Netzwerkzugriffs aus, klicken Sie auf **Erstellen**und dann auf **Schließen**.

Wenn wir die Intranet-IPs für die VPN-Benutzer nicht einrichten, sendet der Benutzer den Datenverkehr an das Citrix Gateway VIP, und von dort erstellt die Citrix ADC Appliance ein neues Paket an die Intranet-Anwendungsressource im internen LAN. Dieses neue Paket wird vom SNIP zur Intranet-Anwendung bezogen. Von hier aus erhält die Intranet-Anwendung das Paket, verarbeitet es und versucht dann, auf die Quelle dieses Pakets zu antworten (in diesem Fall das SNIP). Das SNIP erhält das Paket und sendet die Antwort an den Client, der die Anfrage gestellt hat.

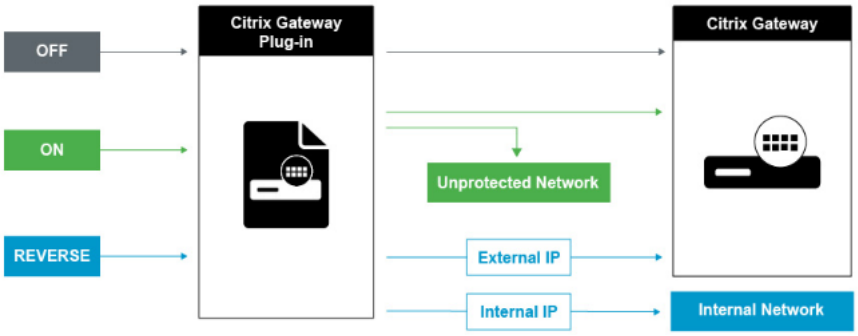
Wenn eine Intranet-IP-Adresse verwendet wird, sendet der Benutzer den Datenverkehr an das Citrix Gateway VIP, und von dort aus wird die Citrix ADC Appliance die Client-IP einer der konfigurierten INTRANET-IPs aus dem Pool zuordnen. Beachten Sie, dass die Citrix ADC Appliance den Intranet-IP-Pool besitzen wird und diese Bereiche aus diesem Grund nicht im internen Netzwerk verwendet werden dürfen. Die Citrix ADC Appliance weist eine Intranet-IP für die eingehenden VPN-Verbindungen

zu, wie es ein DHCP-Server tun würde. Die Citrix ADC Appliance erstellt ein neues Paket für die Intranetanwendung im LAN, auf das der Benutzer zugreifen würde. Dieses neue Paket wird von einem der Intranet-IPs für die Intranet-Anwendung bezogen. Von hier aus erhalten Intranet-Anwendungen das Paket, verarbeiten es und versuchen dann, auf die Quelle dieses Pakets (die INTRANET-IP) zu antworten. In diesem Fall muss das Antwortpaket an die Citrix ADC Appliance zurückgeleitet werden, wo sich die INTRANET-IPs befinden (Denken Sie daran, dass die Citrix ADC Appliance die Intranet-IPs-Subnetze besitzt). Um diese Aufgabe zu erfüllen, muss der Netzwerkadministrator über eine Route zur INTRANET-IP verfügen, die auf einen der SNIPs verweist. Es wird empfohlen, den Datenverkehr zurück auf das SNIP zu verweisen, das die Route enthält, von der aus das Paket die Citrix ADC Appliance zum ersten Mal verlässt, um asymmetrischen Datenverkehr zu vermeiden.

## Split-Tunneling-Optionen

Im Folgenden sind die verschiedenen Split-Tunneling-Optionen aufgeführt.




### Split-Tunnel AUS

Wenn der Split-Tunnel ausgeschaltet ist, erfasst der Citrix Secure Access Client den gesamten Netzwerkverkehr, der von einem Benutzergerät stammt, und sendet den Datenverkehr über den VPN-Tunnel an Citrix Gateway. Mit anderen Worten, der VPN-Client richtet eine Standardroute vom Client-PC ein, die auf den Citrix Gateway VIP zeigt, was bedeutet, dass der gesamte Datenverkehr durch den Tunnel gesendet werden muss, um zum Ziel zu gelangen. Da der gesamte Verkehr durch den Tunnel gesendet wird, müssen Autorisierungsrichtlinien festlegen, ob der Verkehr zu internen Netzwerkressourcen geleitet oder verweigert werden darf.

Während auf "Aus"gestellt, läuft der gesamte Datenverkehr durch den Tunnel, einschließlich des Standard-Webverkehrs zu Websites. Wenn das Ziel darin besteht, diesen Webverkehr zu überwachen und zu steuern, müssen Sie diese Anfragen mithilfe der Citrix Gateway-Appliance an einen externen Proxy weiterleiten. Benutzergeräte können über einen Proxyserver eine Verbindung herstellen, um auch auf interne Netzwerke zuzugreifen.
Citrix Gateway unterstützt die Protokolle HTTP, SSL, FTP und SOCKS. Um die Proxy-Unterstützung

für Benutzerverbindungen zu aktivieren, müssen Sie diese Einstellungen auf Citrix Gateway angeben. Sie können die IP-Adresse und den Port angeben, die vom Proxyserver auf Citrix Gateway verwendet werden. Der Proxyserver wird als Forward-Proxy für alle weiteren Verbindungen zum internen Netzwerk verwendet.

Weitere Informationen finden Sie unter den folgenden Links:

- Aktivieren der Proxy-Unterstützung für Benutzerverbindungen

**Split-Tunnel EIN**

Sie können Split-Tunneling aktivieren, um zu verhindern, dass der Citrix Secure Access Client unnötigen Netzwerkverkehr an Citrix Gateway sendet. Wenn der Split-Tunnel aktiviert ist, sendet der Citrix Secure Access Client nur Datenverkehr, der für Netzwerke bestimmt ist, die von Citrix Gateway geschützt sind (Intranetanwendungen), über den VPN-Tunnel. Der Citrix Secure Access Client sendet keinen Netzwerkverkehr, der für ungeschützte Netzwerke bestimmt ist, an Citrix Gateway. Wenn der Citrix Secure Access Client gestartet wird, ruft er die Liste der Intranetanwendungen von Citrix Gateway ab und richtet eine Route für jedes Subnetz ein, das auf der Registerkarte Intranetanwendung auf dem Client-PC definiert ist. Der Citrix Secure Access-Client untersucht alle vom Benutzergerät übertragenen Pakete und vergleicht die Adressen in den Paketen mit der Liste der Intranetanwendungen (Routingtabelle, die beim Starten der VPN-Verbindung erstellt wurde). Wenn sich die Zieladresse im Paket in einer der Intranetanwendungen befindet, sendet der Citrix Secure Access Client das Paket über den VPN-Tunnel an Citrix Gateway. Wenn sich die Zieladresse nicht in einer definierten Intranet-Anwendung befindet, wird das Paket nicht verschlüsselt, und das Benutzergerät leitet das Paket dann entsprechend mithilfe des ursprünglich auf dem Client-PC definierten Standard-Routing weiter. “Wenn Sie Split-Tunneling aktivieren, definieren Intranet-Anwendungen den Netzwerkverkehr, der abgefangen und durch den Tunnel gesendet wird”.

**Rückwärtsgeteilter**

Citrix Gateway unterstützt auch Reverse-Split-Tunneling, das den Netzwerkverkehr definiert, den Citrix Gateway nicht abfängt. Wenn Sie Split-Tunneling auf Rückwärtsgang einstellen, definieren Intranetanwendungen den Netzwerkverkehr, den Citrix Gateway nicht abfängt. Wenn Sie Reverse-Split-Tunneling aktivieren, umgeht der gesamte Netzwerkverkehr, der an interne IP-Adressen gerichtet ist, den VPN-Tunnel, während anderer Datenverkehr über Citrix Gateway fließt. Reverse-Split-Tunneling kann verwendet werden, um den gesamten nicht lokalen LAN-Verkehr zu protokollieren. Wenn Benutzer beispielsweise ein drahtloses Heimnetzwerk haben und mit dem Citrix Secure Access Client angemeldet sind, fängt Citrix Gateway keinen Netzwerkverkehr ab, der für einen Drucker oder ein anderes Gerät innerhalb des drahtlosen Netzwerks bestimmt ist.

> **Hinweis:**
>
> Der Citrix Secure Access-Client für Windows unterstützt auch einen FQDN-basierten Reverse-Split-Tunnel von Citrix Secure Access Version 22.6.1.5 und höher.

**Wichtige Hinweise IP-basiertes Reverse-Split-Tunneling:**

- Die Anzahl der auf IP-Adressen basierenden Regeln ist auf 1024 begrenzt.
- Wird sowohl von DNE- als auch von WFP-Treibern unterstützt.

**Auf Hostnamen basierendes Reverse-Split-Tunneling:**

- Die Anzahl der Hostnamen, auf die während einer VPN-Sitzung zugegriffen werden kann, ist durch die Anzahl der verwendbaren IP-Adressen begrenzt, die im FQDN-Spoofing-Bereich angegeben sind. Dies liegt daran, dass jeder Hostname eine IP-Adresse aus dem FQDN-Spoofing-Bereich belegt. Sobald der IP-Bereich erschöpft ist, wird die zuletzt zugewiesene IP-Adresse für den nächsten neuen Hostnamen wiederverwendet.
- DNS-Suffixe müssen konfiguriert werden.

  > **Hinweis:**
  >
  > Für Windows-Clients wird das auf Hostnamen basierende Reverse-Split-Tunneling nur mit dem WFP-Treiber unterstützt. Aktivieren Sie den WFP-Treibermodus und legen Sie „EnableWFP“als Registrierungswert fest. Weitere Informationen finden Sie unter Windows Citrix Secure Access Client mit Windows Filtering Platform.

**IP-basiertes und hostnamenbasiertes Reverse-Split-Tunneling:**

- Wird nur mit dem WFP-Treiber unterstützt. Alle anderen Richtlinien, die in IP-basiertem Reverse-Split-Tunneling und Hostnamen-basiertem Reverse-Split-Tunneling erwähnt werden, gelten.

## Name Service-Auflösung konfigurieren

Während der Installation von Citrix Gateway können Sie den Citrix Gateway-Assistenten verwenden, um andere Einstellungen zu konfigurieren, einschließlich Namensdienstanbieter. Die Namensdienstanbieter übersetzen den vollqualifizierten Domainnamen (FQDN) in eine IP-Adresse. Im Citrix Gateway-Assistenten können Sie auch Folgendes ausführen:

- Konfigurieren Sie einen DNS- oder WINS-Server
- Legen Sie die Priorität des DNS-Lookup fest
- Legen Sie fest, wie oft die Verbindung zum Server erneut versucht werden soll.

Wenn Sie den Citrix Gateway-Assistenten ausführen, können Sie dann einen DNS-Server hinzufügen. Sie können Citrix Gateway mithilfe eines Sitzungsprofils weitere DNS-Server und einen WINS-Server hinzufügen. Sie können dann Benutzer und Gruppen anweisen, eine Verbindung zu einem Namensauflösungsserver herzustellen, der sich von dem unterscheidet, den Sie ursprünglich mit dem Assistenten konfiguriert haben.

Erstellen Sie vor dem Konfigurieren eines anderen DNS-Servers auf Citrix Gateway einen virtuellen Server, der als DNS-Server für die Namensauflösung fungiert.

So fügen Sie einen DNS- oder WINS-Server innerhalb eines Sitzungsprofils hinzu

1. Im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration > **Citrix Gateway > Richtlinien > Sitzung**.
2. Wählen Sie im Detailbereich auf der Registerkarte Profile ein Profil aus und klicken Sie dann auf Öffnen.
3. Führen Sie auf der Registerkarte Netzwerkkonfiguration einen der folgenden Schritte aus:
    - Um einen DNS-Server zu konfigurieren, klicken Sie neben **Virtueller DNS-Server**auf **Override Global**, wählen Sie den Server aus, und klicken Sie dann auf **OK**.
    - Um einen WINS-Server zu konfigurieren, klicken Sie neben **WINS-Server-IP**auf **Override Global**, geben Sie die IP-Adresse ein und klicken Sie dann auf **OK**.

### Referenzen

- Split-Tunneling
- So verbinden sich Benutzer mit Citrix Secure Access Agent
- Über Citrix Gateway
- Benutzerzugriffsmethode wählen

## Benutzerzugriffsmethode wählen

March 27, 2024

Sie können Citrix Gateway für die Bereitstellung von Benutzerverbindungen in den folgenden Szenarien konfigurieren:

- Benutzerverbindungen mithilfe der Citrix Workspace-App. Die Citrix Workspace-App ist mit StoreFront oder dem Webinterface kompatibel, um Benutzern Zugriff auf veröffentlichte Anwendungen oder virtuelle Desktops in einer Serverfarm zu ermöglichen. Die Citrix Workspace-App

ist eine Software, die das ICA-Netzwerkprotokoll verwendet, um Benutzerverbindungen herzustellen. Benutzer installieren die Citrix Workspace-App auf dem Benutzergerät. Wenn Benutzer die Citrix Workspace-App auf ihrem Windows- oder Mac-basierten Computer installieren, subsumiert die Citrix Workspace-App alle Plug-Ins, einschließlich des Citrix Gateway-Plug-Ins für Benutzerverbindungen. Citrix Gateway unterstützt auch Verbindungen von der Citrix Workspace-App für Android und der Citrix Workspace-App für iOS. Benutzer können über Citrix Endpoint Management, StoreFront oder das Webinterface eine Verbindung zu ihren virtuellen Desktops und Windows-basierten, Web-, Mobil- und SaaS-Anwendungen herstellen.

- Benutzerverbindungen mit Secure Hub. Benutzer können eine Verbindung zu Mobil-, Web- und SaaS-Anwendungen herstellen, die in Endpoint Management konfiguriert sind. Benutzer installieren Secure Hub auf ihrem Mobilgerät (Android oder iOS). Wenn sich Benutzer bei Secure Hub anmelden, können sie WorxMail und WorxWeb zusammen mit jeder anderen mobilen App installieren, die Sie in Endpoint Management installiert haben. Secure Hub, Secure Mail und WorxWeb verwenden die Micro VPN-Technologie, um Verbindungen über Citrix Gateway herzustellen.
- Benutzerverbindungen mithilfe des Citrix Gateway-Plug-Ins als eigenständige Anwendung. Das Citrix Gateway Plug-in ist eine Software, die Benutzer herunterladen und auf einem Benutzergerät installieren können. Wenn sich Benutzer mit dem Plug-In anmelden, können Benutzer auf Ressourcen im sicheren Netzwerk zugreifen, als wären sie im Büro. Zu den Ressourcen gehören E-Mail-Server, Dateifreigaben und Intranet-Websites.
- Benutzerverbindungen durch Verwendung des clientlosen Zugriffs. Der clientlose Zugriff bietet Benutzern den Zugriff, den sie benötigen, ohne dass Software wie das Citrix Gateway Plug-in oder die Citrix Workspace-App auf dem Benutzergerät installiert werden muss. Der clientlose Zugriff ermöglicht Verbindungen zu einem begrenzten Satz von Webressourcen wie Outlook Web Access oder SharePoint, auf Citrix Virtual Apps veröffentlichten Anwendungen, virtuellen Desktops von Citrix Virtual Apps and Desktops sowie Dateifreigaben im sicheren Netzwerk über das Access Interface. Benutzer stellen eine Verbindung her, indem sie die Citrix Gateway-Webadresse in einen Webbrowser eingeben und dann auf der Auswahlseite clientlosen Zugriff auswählen.
- Benutzerverbindungen, wenn ein Scan vor oder nach der Authentifizierung fehlschlägt. Dieses Szenario wird als Fallback für Zugriffsszenarien bezeichnet. Mit dem Fallback für Zugriffsszenarien kann ein Benutzergerät mithilfe der Citrix Workspace-App vom Citrix Gateway-Plug-In auf StoreFront oder das Webinterface zurückgreifen, wenn das Benutzergerät den ersten Endpoint Analysis-Scan nicht durchläuft.

  Wenn sich Benutzer über die Citrix Workspace-App bei Citrix Gateway anmelden, funktioniert der Vorauthentifizierungsscan nicht. Scans nach der Authentifizierung funktionieren, wenn Citrix Gateway den VPN-Tunnel einrichtet.

Benutzer können das Citrix Gateway Plug-in mithilfe der folgenden Methoden herunterladen und installieren:

- Herstellen einer Verbindung zu Citrix Gateway mithilfe eines Webbrowsers.
- Verbinden mit StoreFront, das für das Akzeptieren von Citrix Gateway-Verbindungen konfiguriert ist.
- Installieren des Plug-Ins mithilfe eines Gruppenrichtlinienobjekts (GPO).
- Hochladen des Citrix ADC-Plug-Ins auf den Merchandising Server.

## Bereitstellen von Citrix Gateway-Plug-Ins für den Benutzerzugriff

March 27, 2024

Citrix Gateway enthält die folgenden Plug-Ins für den Benutzerzugriff:

- Citrix Gateway Plug-in für Windows
- Citrix Gateway Plug-in für Mac
- Citrix Gateway Plug-in für Java

Wenn sich Benutzer zum ersten Mal bei Citrix Gateway anmelden, laden sie das Citrix Gateway Plug-in von einer Webseite herunter und installieren es. Benutzer melden sich an, indem sie im Infobereich auf einem Windows-basierten Computer auf das Citrix Gateway-Symbol klicken. Auf einem macOS X-Computer können sich Benutzer über das **Dock oder das Anwendungsmenü** anmelden. Wenn Sie Citrix Gateway auf eine neue Softwareversion aktualisieren, wird das Citrix Gateway Plug-in automatisch auf dem Benutzergerät aktualisiert.

Das Citrix Gateway Plug-in für Java kann auf jedem Benutzergerät verwendet werden, das Java unterstützt. Das Citrix Gateway Plug-in für Java unterstützt die meisten TCP-basierten Anwendungen, bietet jedoch nur einige der Funktionen des Citrix Gateway Plug-Ins für Windows oder des Citrix Gateway-Plug-Ins für macOS X. Das Citrix Gateway Plug-In für Java bietet eingeschränkten Zugriff auf die von Ihnen definierten Netzwerkressourcen. Weitere Informationen zum Java-Plug-in finden Sie unter Citrix Gateway Plug-in für Java.

### Stellen Sie das Citrix Gateway Plug-in mithilfe des MSI-Installationspakets bereit

Sie können das Citrix Gateway-Plug-in mithilfe einer Microsoft Active Directory-Infrastruktur oder eines standardmäßigen MSI-Bereitstellungstools eines Drittanbieters wie Windows Server Update Services bereitstellen. Wenn Sie ein Tool verwenden, das Windows Installer-Pakete unterstützt, können Sie die Pakete mit jedem Tool bereitstellen, das MSI-Dateien unterstützt. Dann verwenden Sie Ihr Bereitstellungstool, um die Software auf den entsprechenden Benutzergeräten bereitzustellen und zu installieren.

**Vorteile der Verwendung eines zentralisierten Bereitstellungstools**

- Die Möglichkeit, die Sicherheitsanforderungen zu erfüllen: Beispielsweise können Sie Benutzersoftware installieren, ohne Softwareinstallationsberechtigungen für Benutzer ohne Administratorrechte zu aktivieren.
- Kontrolle über Softwareversionen. Sie können eine aktualisierte Version der Software für alle Benutzer gleichzeitig bereitstellen.
- Skalierbarkeit. Eine zentralisierte Bereitstellungsstrategie kann einfach skaliert werden, um mehr Benutzer zu unterstützen.
- Positive Benutzererfahrung. Sie können installationsbezogene Probleme bereitstellen, testen und beheben, ohne Benutzer in diesen Prozess einzubeziehen.

Citrix empfiehlt diese Option, wenn die administrative Kontrolle über die Installation von Benutzersoftware bevorzugt wird und der Zugriff auf Benutzergeräte leicht verfügbar ist.

Weitere Informationen finden Sie unter Bereitstellen des Citrix Gateway-Plug-ins aus Active Directory.

### Bestimmen Sie, welches Software-Plug-In bereitgestellt werden soll

Wenn für Ihre Citrix Gateway-Bereitstellung kein Software-Plug-In auf Benutzergeräten erforderlich ist, wird davon ausgegangen, dass Ihre Bereitstellung clientlosen Zugriff bietet. In diesem Szenario benötigen Benutzer nur einen Webbrowser, um auf Netzwerkressourcen zuzugreifen. Für bestimmte Funktionen ist jedoch die Plug-In-Software auf dem Gerät des Benutzers erforderlich.

## Wählen des Citrix Gateway Plug-ins für Benutzer

March 27, 2024

Wenn Sie Citrix Gateway konfigurieren, können Sie wählen, wie sich Benutzer anmelden. Benutzer können sich mit einem der folgenden Plug-Ins anmelden:

- Citrix Gateway Plug-in für Windows
- Citrix Gateway Plug-in für macOS
- Citrix Gateway Plug-in für Java

Sie schließen die Konfiguration ab, indem Sie eine Sitzungsrichtlinie erstellen und die Richtlinie dann an Benutzer, Gruppen oder virtuelle Server binden. Sie können Plug-Ins auch aktivieren, indem Sie globale Einstellungen konfigurieren. Innerhalb des globalen oder Sitzungsprofils wählen Sie entweder Windows/macOS X oder Java als Plug-in-Typ. Wenn sich Benutzer anmelden, erhalten sie

das Plug-In wie global oder im Sitzungsprofil und in der Richtlinie definiert. Erstellen Sie separate Profile für den Plug-In-Typ. Sie können im Sitzungsprofil nur entweder **Windows/macOS X oder Java** wählen. Informationen zum Konfigurieren des Citrix Gateway-Plug-ins für Java finden Sie unter Verbinden mit dem Citrix Gateway Plug-in für Java.

### Konfigurieren Sie das Plug-In global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte "Configuration"im Navigationsbereich "Citrix Gateway"und klicken Sie auf "Global Settings".
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Wählen Sie auf der Registerkarte Client Experience neben Plug-In-Typ Windows/macOS X aus und klicken Sie dann auf OK.

### Konfigurieren Sie den Plug-In-Typ für Windows oder macOS in einem Sitzungsprofil

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie eine neue Sitzungsrichtlinie erstellen, klicken Sie im Detailbereich auf **Hinzufügen**.
   - Wenn Sie eine bestehende Richtlinie ändern, wählen Sie eine Richtlinie aus, und klicken Sie dann auf **Öffnen**.
3. Erstellen Sie ein Profil oder ändern Sie ein vorhandenes Profil. Führen Sie dazu einen der folgenden Schritte aus:
   - Klicken Sie neben **Profil anfordern**auf **Neu**.
   - Klicken Sie neben **Profil anfordern** auf **Ändern**.
4. Klicken Sie auf der Registerkarte **Client Experience** neben **Plug-In-Typ**auf **Override Global** und wählen Sie dann **Windows/macOS X**aus.
5. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie ein neues Profil erstellen, klicken Sie auf **Erstellen**, legen Sie den Ausdruck im Richtliniendialogfeld fest, klicken Sie auf **Erstellen** und dann auf **Schließen**.
   - Wenn Sie ein vorhandenes Profil ändern, klicken Sie nach der Auswahl zweimal auf OK.

### Citrix Gateway Plug-in für Windows

Wenn sich Benutzer bei Citrix Gateway anmelden, laden sie das Citrix Gateway Plug-in herunter und installieren es auf dem Benutzergerät.

Um das Plug-In zu installieren, müssen Benutzer ein lokaler Administrator oder ein Mitglied der Gruppe Administratoren sein. Diese Einschränkung gilt nur für die Erstinstallation. Plug-In-Upgrades erfordern keinen Zugriff auf Administratorebene.

Damit Benutzer eine Verbindung zu Citrix Gateway herstellen und diese verwenden können, müssen Sie ihnen die folgenden Informationen bereitstellen:

- Citrix Gateway-Webadresse wie https://NetScalerGatewayFQDN/
- Alle Systemanforderungen für die Ausführung des Citrix Gateway-Plug-Ins, wenn Sie Endpunktressourcen und -richtlinien konfiguriert haben

Abhängig von der Konfiguration des Benutzergeräts müssen Sie möglicherweise auch die folgenden Informationen angeben:

- Wenn Benutzer eine Firewall auf ihrem Computer ausführen, müssen sie möglicherweise die Firewall-Einstellungen ändern, damit die Firewall keinen Datenverkehr zu oder von den IP-Adressen blockiert, die den Ressourcen entsprechen, für die Sie Zugriff gewährt haben. Das Citrix Gateway Plug-in verarbeitet automatisch die Internetverbindungsfirewall unter Windows XP und die Windows-Firewall in Windows XP Service Pack 2, Windows Vista, Windows 7, Windows 8 oder Windows 8.1.
- Benutzer, die Datenverkehr über eine Citrix Gateway-Verbindung an FTP senden möchten, müssen ihre FTP-Anwendung so einstellen, dass passive Übertragungen durchgeführt werden. Eine passive Übertragung bedeutet, dass der Remotecomputer die Datenverbindung zu Ihrem FTP-Server herstellt, anstatt die Datenverbindung durch den FTP-Server zum Remotecomputer herzustellen.
- Benutzer, die X-Clientanwendungen über die Verbindung ausführen möchten, müssen einen X-Server, z. B. `XManager`, auf ihren Computern ausführen.
- Benutzer, die Receiver für Windows oder Receiver für Mac installieren, können das Citrix Gateway Plug-in von Receiver oder mithilfe eines Webbrowsers starten. Geben Sie Benutzern Anweisungen zur Anmeldung mit dem Citrix Gateway Plug-in über Receiver oder einen Webbrowser.

Da Benutzer an Dateien und Anwendungen arbeiten, als wären sie lokal im Netzwerk der Organisation, müssen Sie Benutzer nicht umschulen oder Anwendungen konfigurieren.

Um zum ersten Mal eine sichere Verbindung herzustellen, melden Sie sich über die Webanmeldeseite bei Citrix Gateway an. Das typische Format einer Webadresse ist https://companyname.com. Wenn sich Benutzer anmelden, können sie das Citrix Gateway Plug-in herunterladen und auf ihrem Computer installieren.

#### Installieren Sie das Citrix Gateway Plug-in für Windows

1. Geben Sie in einem Webbrowser die Webadresse von Citrix Gateway ein.

2. Geben Sie den Benutzernamen und das Kennwort ein und klicken Sie dann auf Anmelden.
3. Wählen Sie Netzwerkzugriff und klicken Sie dann auf Herunterladen.
4. Folgen Sie den Anweisungen, um das Plug-In zu installieren.

Wenn der Download abgeschlossen ist, stellt das Citrix Gateway Plug-in eine Verbindung her und zeigt eine Meldung im Infobereich auf einem Windows-basierten Computer an.

Wenn Sie möchten, dass Benutzer eine Verbindung mit dem Citrix Gateway-Plug-In herstellen, ohne einen Webbrowser zu verwenden, können Sie das Plug-In so konfigurieren, dass das Anmeldedialogfeld angezeigt wird, wenn Benutzer auf einem Windows-basierten Computer mit der rechten Maustaste auf das **Citrix Gateway-Symbol** im Infobereich klicken oder das Plug-In über das Startmenü starten.

#### Konfigurieren Sie das Anmeldedialogfeld für das Citrix Gateway Plug-in für Windows

Um das Citrix Gateway Plug-in für die Verwendung des Anmeldedialogfelds zu konfigurieren, müssen Benutzer angemeldet sein, um dieses Verfahren abzuschließen.

1. Klicken Sie auf einem Windows-basierten Computer im Infobereich mit der rechten Maustaste auf das Citrix Gateway-Symbol, und klicken Sie dann auf Citrix Gateway konfigurieren.
2. Klicken Sie auf die Registerkarte Profil und dann auf Profil ändern.
3. Klicken Sie auf der Registerkarte Optionen auf Citrix Gateway Plug-in für die Anmeldung verwenden.
   Hinweis: Wenn Benutzer das Dialogfeld
   Citrix Gateway konfigurieren in Receiver öffnen, ist die Registerkarte
   Optionen nicht verfügbar.

#### Festlegen des Abfangmodus für das Citrix Gateway Plug-in für Windows

Wenn Sie das Citrix Gateway-Plug-In für Windows konfigurieren, müssen Sie auch den Abhörmodus konfigurieren und auf transparent einstellen.

1. Klicken Sie im Konfigurationsdienstprogramm auf die Registerkarte Konfiguration, erweitern Sie **Citrix Gateway > Ressourcen,** und klicken Sie dann auf **Intranet-Anwendungen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie auf **Transparent**.
5. Wählen Sie unter **Protokoll**die Option **BELIEBIG**aus.
6. Wählen Sie unter **Zieltyp**die Option **IP-Adresse und Netzwerkmaske**aus.
7. Geben Sie unter **IP-Adresse** die IP-Adresse ein.
8. Geben Sie unter **Netzwerkmaske**die Subnetzmaske ein, klicken Sie auf **Erstellen** und dann auf **Schließen**.

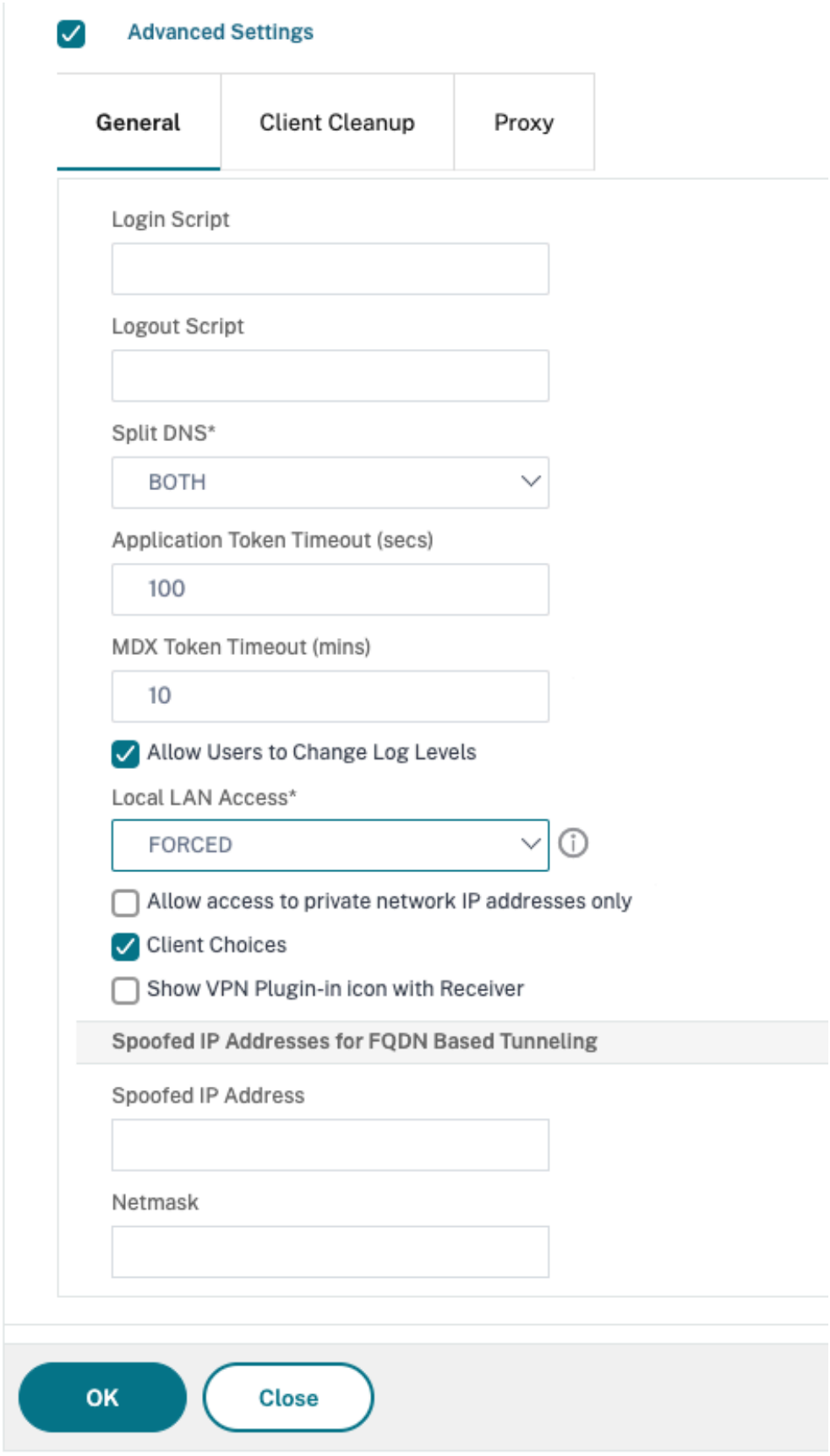
**Erzwingen des lokalen LAN-Zugriffs für Endbenutzer basierend auf der ADC-Konfiguration**

Ab Citrix ADC Version 13.0, Build 85.15, können Administratoren die Endbenutzer daran hindern, die lokale LAN-Zugriffsoption auf ihren Client-Computern zu deaktivieren. Eine neue Option, FORCED, wird zu den vorhandenen Parameterwerten für lokalen LAN-Zugriff hinzugefügt. Wenn der Wert Lokaler LAN-Zugriff auf FORCED gesetzt ist, ist der lokale LAN-Zugriff für Endbenutzer auf den Client-Computern immer aktiviert. Endbenutzer können die lokalen LAN-Einstellungen auf der Citrix Secure Access Client-Benutzeroberfläche nicht deaktivieren. Wenn Administratoren eine Option zum Aktivieren oder Deaktivieren des lokalen LAN-Zugriffs für den Endbenutzer bereitstellen möchten, müssen sie den lokalen LAN-Zugriffsparameter auf ON neu konfigurieren.

**So aktivieren Sie die Option Forced mithilfe der GUI:**

1. Navigieren Sie zu **Citrix Gateway > Globale Einstellungen > Globale Einstellungen ändern**.
2. Klicken Sie auf die Registerkarte **Clienterfahrung** und dann auf **Erweiterte Einstellungen**.
3. Wählen Sie unter **Lokaler LAN-Zugriff**die Option **FORCED**



**Führen Sie den folgenden Befehl aus, um die Option Forced mithilfe der CLI zu aktivieren:**

```
set vpn parameter -localLanAccess FORCED
<!--NeedCopy-->
```

## Citrix Gateway Plug-in für Java

Das Citrix Gateway Plug-in für Java kann auf jedem Benutzergerät verwendet werden, das Java unterstützt.

> **Hinweis:**
>
> Java Runtime Environment (JRE) Version 1.4.2 bis zur neuesten Version von JRE ist für die folgenden Betriebssysteme und Webbrowser erforderlich.

- macOS X
- Linux
- Windows XP (alle Versionen), Windows Vista, Windows 7 und Windows 8
- Internet Explorer
- Firefox
- Safari 1.2 bis zur aktuellsten Version des Webbrowsers

Das Citrix Gateway Plug-in für Java unterstützt die meisten TCP-basierten Anwendungen, bietet jedoch nur einige der Funktionen des Citrix Gateway Plug-Ins für Windows oder des Citrix Gateway Plug-Ins für macOS X.

Benutzer benötigen keine Administratorrechte auf dem Benutzergerät, um das Citrix Gateway Plug-in für Java verwenden zu können. Aus Sicherheitsgründen sollten Sie die Verwendung dieser Plug-in-Version für einen bestimmten virtuellen Server, eine Gruppe oder einen bestimmten Benutzer benötigen, unabhängig davon, welches Benutzergerät verwendet wird.

Um Citrix Gateway für die Installation des Citrix Gateway-Plug-ins für Java auf Benutzergeräten zu konfigurieren, konfigurieren Sie eine Sitzungsrichtlinie und binden Sie sie dann an den virtuellen Server, die Gruppe oder den Benutzer.

Wenn sich Benutzer von einem Computer aus anmelden, auf dem Windows 7 ausgeführt wird, werden die Proxy-Serverinformationen in Internet Explorer nicht automatisch festgelegt. Benutzer müssen den Proxyserver auf dem Computer, auf dem Windows 7 ausgeführt wird, manuell konfigurieren.

### Konfigurieren Sie Citrix Gateway-Plug-In für Java

1. Navigieren Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Profile**.
3. Wählen Sie ein Sitzungsprofil aus und klicken Sie dann auf **Öffnen**.

4. Klicken Sie auf der Registerkarte Client Experience neben Plug-in-Typ auf **Override Global** , wählen Sie **Java** aus, und klicken Sie dann auf **OK**.

#### So stellen Sie den Abfangmodus ein

Erstellen Sie nach dem Erstellen der Sitzungsrichtlinie eine Intranetanwendung, um den Abhörmodus für Benutzer zu definieren, die sich mit dem Citrix Gateway-Plug-in für Java anmelden.

1. Navigieren Sie zu **Citrix Gateway > Ressourcen** und klicken Sie dann auf **Intranetanwendungen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie unter Name einen Namen ein.
4. Klicken Sie auf **Proxy**.
5. Geben Sie unter Ziel-IP-Adresse die IP-Adresse ein.
6. Geben Sie unter Zielport die Portnummer ein.
7. Geben Sie unter Quell-IP-Adresse die IP-Adresse ein.
8. Geben Sie im Port Quellport die Portnummer ein, klicken Sie auf **Erstellen** und dann auf **Schließen**.

Wenn Sie keine Quell-IP-Adresse und Portnummer angeben, verwendet Citrix Gateway automatisch 127.0.0.1 für die IP-Adresse und 0 für den Port.

#### Aktualisieren Sie die HOSTS-Datei auf Windows-basierten Computern

Wenn sich Benutzer mit dem Citrix Gateway Plug-in für Java auf einem Computer anmelden, auf dem Windows Vista, Windows 7 oder Windows 8 ausgeführt wird, wird der Netzwerkverkehr für TCP-Intranetanwendungen nicht getunnelt. Die HOSTS-Datei wird auf Computern mit Vista und Windows 7 nicht automatisch aktualisiert. Fügen Sie die Intranet-Anwendungen manuell zur HOSTS-Datei hinzu.

Auf einem Windows-basierten Computer können Sie die HOSTS-Datei in Notepad oder einem anderen Texteditor bearbeiten. Wenn Sie die HOSTS-Datei in Notepad bearbeiten, müssen Sie Notepad als Administrator ausführen. Fügen Sie die Zuordnungseinträge für die Intranetanwendung für das Citrix Gateway Plug-in für Java hinzu und speichern Sie die Datei.

## Bereitstellen des Citrix Gateway Plug-ins mit Active Directory

March 27, 2024

Wenn Benutzer keine Administratorrechte zum Installieren des Citrix Gateway-Plug-Ins auf dem Benutzergerät haben, können Sie das Plug-in für Benutzer aus Active Directory bereitstellen. Wenn Sie diese Methode verwenden, um das Citrix Gateway Plug-In bereitzustellen, können Sie das Installationsprogramm extrahieren und dann eine Gruppenrichtlinie verwenden, um das Programm bereitzustellen. Die allgemeinen Schritte für diese Art der Bereitstellung sind:

- Extrahieren des MSI-Pakets.
- Verteilen des Plug-Ins mithilfe einer Gruppenrichtlinie.
- Erstellen eines Verteilungspunkts.
- Zuweisen des Citrix Gateway-Plug-in-Pakets mithilfe eines Gruppenrichtlinienobjekts.

  **Hinweis:** Die Verteilung des Citrix Gateway Plug-Ins aus Active Directory wird nur unter Windows 7, Windows 8 und Windows 10 unterstützt.

Sie können das MSI-Paket vom Konfigurationsdienstprogramm oder von der Citrix Website herunterladen.

### So laden Sie das Citrix Gateway Plug-in-MSI-Paket vom Konfigurationsdienstprogramm herunter

1. Klicken Sie im Konfigurationsdienstprogramm auf **Downloads**.
2. Klicken Sie unter Citrix Gateway Plug-in auf **Citrix Gateway Plugin für Windows herunterladen** und speichern Sie dann die Datei **nsvpnc_setup.exe** auf Ihrem Windows-Server.

   **Hinweis:**

   - Für 64-Bit-Computer müssen Sie die Datei Agee_setup.exe auf Ihrem Windows-Server speichern.
   - Wenn das Dialogfeld **Dateidownload** nicht angezeigt wird, drücken Sie die STRG-Taste, wenn Sie auf den Link **Citrix Gateway Plug-in für Windows herunterladen**klicken.
3. Navigieren Sie an einer Eingabeaufforderung zu dem Ordner, in dem Sie **nsvpnc_setup.exe** gespeichert haben, und geben Sie dann Folgendes ein:

   ```
   nsvpnc_setup /c
   <!--NeedCopy-->
   ```

   Dadurch wird die Datei agee.msi extrahiert.

   **Hinweis:** Navigieren Sie bei 64-Bit-Computern zu dem Ordner, in dem Sie **Agee_setup.exe** gespeichert haben, und geben Sie dann Folgendes ein:

   ```
   Agee_setup.exe /c
   <!--NeedCopy-->
   ```

Dadurch wird die Datei agee64.msi extrahiert.

4. Speichern Sie die extrahierte Datei in einem Ordner auf dem Windows-Server.

Verwenden Sie nach dem Extrahieren der Datei eine Gruppenrichtlinie auf Windows Server, um die Datei zu verteilen.

Installieren Sie vor dem Starten der Verteilung die Gruppenrichtlinienverwaltungskonsole unter Windows Server 2003, Windows Server 2008 oder Windows Server 2012. Weitere Informationen finden Sie in der Online-Hilfe von Windows.

**Hinweis:** Wenn Sie eine Gruppenrichtlinie verwenden, um das Citrix Gateway-Plug-In zu veröffentlichen, empfiehlt Citrix, das Paket dem Benutzergerät zuzuweisen. Das MSI-Paket wird pro Gerät installiert.

Bevor Sie die Software verteilen können, erstellen Sie einen Verteilungspunkt auf einer Netzwerkfreigabe auf einem Veröffentlichungsserver, z. B. dem Microsoft Internet Security and Acceleration (ISA) Server.

### So erstellen Sie einen Verteilungspunkt

1. Melden Sie sich als Administrator beim Publishing-Server an.
2. Erstellen Sie einen Ordner und teilen Sie ihn im Netzwerk mit Leseberechtigung für alle Konten, die Zugriff auf das Distributionspaket benötigen.
3. Navigieren Sie an der Eingabeaufforderung zu dem Ordner, in dem Sie die extrahierte Datei speichern, und geben Sie dann ein: msiexec -a agee.msi
4. Klicken Sie auf dem Bildschirm **Netzwerkspeicherort** auf **Ändern** und navigieren Sie dann zu dem freigegebenen Ordner, in dem Sie die Administratorinstallation des Citrix Gateway-Plug-Ins erstellen möchten.
5. Klicken Sie auf **OK** und dann auf **Installieren**.

Nachdem Sie das extrahierte Paket auf die Netzwerkfreigabe gelegt haben, weisen Sie das Paket einem Gruppenrichtlinienobjekt in Windows zu.

Nachdem Sie das Citrix Gateway Plug-in erfolgreich als verwaltetes Softwarepaket konfiguriert haben, wird das Plug-in beim nächsten Start des Benutzergeräts automatisch installiert.

> **Hinweis:** Wenn das Installationspaket einem Computer zugewiesen ist, muss der Benutzer den Computer neu starten.

Wenn die Installation beginnt, erhalten Benutzer eine Meldung, dass das Citrix Gateway Plug-in installiert wird.

# Verwalten des Citrix Gateway-Plug-ins mit Active Directory

March 27, 2024

Jede Version des Citrix Gateway-Plug-Ins wird als vollständige Produktinstallation statt als Patch verpackt. Wenn sich Benutzer anmelden und das Citrix Gateway-Plug-in eine neue Version des Plug-Ins erkennt, wird das Plug-in automatisch aktualisiert. Sie können das Citrix Gateway Plug-in auch mithilfe von Active Directory für ein Upgrade bereitstellen.

Erstellen Sie dazu einen Verteilungspunkt für das Citrix Gateway Plug-in. Erstellen Sie ein Gruppenrichtlinienobjekt und weisen Sie ihm die neue Version des Plug-Ins zu. Erstellen Sie dann eine Verbindung zwischen dem neuen Paket und dem vorhandenen Paket. Nachdem Sie den Link erstellt haben, wird das Citrix Gateway-Plug-in aktualisiert.

## Entfernen Sie das Citrix Gateway Plug-in von Benutzergeräten

Um das Citrix Gateway-Plug-In von Benutzergeräten zu entfernen, entfernen Sie das zugewiesene Paket aus dem Gruppenrichtlinienobjekt-Editor.

Wenn das Plug-In vom Benutzergerät entfernt wird, erhalten Benutzer eine Meldung, dass das Plug-In deinstalliert wird.

## Beheben Sie Fehler bei der Installation des Citrix Gateway-Plug-ins mithilfe von Active Directory

Wenn das zugewiesene Paket beim Start des Benutzergeräts nicht installiert werden kann, wird möglicherweise die folgende Warnung im Ereignisprotokoll der Anwendung angezeigt:

Änderungen an den Softwareinstallationseinstellungen konnten nicht übernommen werden. Die Anwendung der Softwareinstallationsrichtlinie wurde bis zur nächsten Anmeldung verzögert, da ein Administrator die Anmeldeoptimierung für Gruppenrichtlinien aktiviert hat. Der Fehler war: Das Gruppenrichtlinien-Framework muss die Erweiterung in der synchronen Vordergrundrichtlinienaktualisierung aufrufen.

Dieser Fehler wird durch die schnelle Anmeldeoptimierung in Windows XP verursacht, bei der sich Benutzer anmelden dürfen, bevor das Betriebssystem alle Netzwerkkomponenten einschließlich der Verarbeitung von Gruppenrichtlinienobjekten initialisiert hat. Einige Richtlinien erfordern möglicherweise mehr als einen Neustart, um wirksam zu werden. Deaktivieren Sie die Optimierung der Schnellanmeldung im Active Directory, um dieses Problem zu beheben.

Um andere Installationsprobleme für verwaltete Software zu beheben, empfiehlt Citrix die Verwendung einer Gruppenrichtlinie, um die Windows Installer-Protokollierung zu aktivieren.

# Integrieren des Citrix Gateway Plug-ins in die Citrix Workspace-App

March 27, 2024

Citrix Gateway unterstützt die Citrix Workspace-App. Das orchestrierte System besteht aus folgenden Komponenten:

- Citrix Workspace-App für Windows 3.4 oder neuer
- Citrix Workspace-App für Mac
- Citrix Workspace-App für Android
- Citrix Workspace-App für iOS
- StoreFront 2.1 oder neuer
- Endpoint Management 2.8 und neuer oder Citrix Endpoint Management 10
- Citrix Update Service, der auf der Citrix Websitegehostet wird

Weitere Informationen zur Kompatibilität von Citrix Gateway mit Citrix Produkten finden Sie unter Kompatibilität mit Citrix Produkten.

Sie können Citrix Gateway so konfigurieren, dass das Citrix Gateway Plug-In bei der Anmeldung von Benutzern an der Appliance einen Webbrowser öffnet, der einmaliges Anmelden auf der Homepage der Citrix Workspace-App ermöglicht. Benutzer können die Citrix Workspace-App von der Homepage herunterladen.

Wenn sich Benutzer mit der Citrix Workspace-App anmelden, können Benutzerverbindungen auf folgende Weise über Citrix Gateway geleitet werden:

- Direkt zu Endpoint Management
- Direkt zu StoreFront
- An StoreFront und dann Endpoint Management, wenn Sie keine mobilen MDX-Apps in Endpoint Management konfigurieren
- An Endpoint Management und dann StoreFront, wenn Sie mobile MDX-Apps in Endpoint Management konfigurieren

> **Hinweis:**
>
> Verbindungen, die direkt an Endpoint Management weitergeleitet werden, werden nur in Endpoint Management 2.0, Endpoint Management 2.5, Endpoint Management 2.6, Endpoint Management 2.8 und Endpoint Management 2.9 unterstützt. Wenn Sie Endpoint Management 1.1 in Ihrem Netzwerk bereitgestellt haben, müssen Benutzerverbindungen über StoreFront geleitet werden.

## So verbinden sich Benutzer mit der Citrix Workspace-App

January 29, 2024

Benutzer können über die Citrix Workspace-App eine Verbindung zu den folgenden Anwendungen, Desktops und Daten herstellen:

- Windows-basierte Anwendungen und virtuelle Desktops, die in StoreFront und im Webinterface veröffentlicht wurden
- ShareFile-Daten, auf die über Citrix Endpoint Management zugegriffen wird

Benutzer können sich mit einer der folgenden Citrix Workspace-Apps anmelden:

- Citrix Workspace-App für Web
- Citrix Workspace-App für Windows
- Citrix Workspace-App für Mac
- Citrix Workspace-App für iOS
- Citrix Workspace-App für Android

Benutzer können sich mit der Citrix Workspace-App für das Web mithilfe eines Webbrowsers oder über das Citrix Workspace-App-Symbol auf dem Benutzergerät anmelden.

Wenn sich Benutzer mit einer beliebigen Version der Citrix Workspace-App anmelden, werden Anwendungen, ShareFile-Daten und Desktops im Browser oder Citrix Workspace-App-Fenster angezeigt.

## Citrix Workspace-App-Symbol entkoppeln

March 27, 2024

Wenn eine Bereitstellung von Citrix Virtual Apps and Desktops mit dem in die Citrix Workspace-App integrierten Citrix Gateway-Plug-In konfiguriert ist, ist das Symbol des Plug-Ins für einen Benutzer, der mit dem VPN verbunden ist, nicht sichtbar. Das **Citrix Gateway Plug-in-Symbol** befindet sich normalerweise in der Windows-Taskleiste oder in der Menüleiste des macOS X Finders. Dieses Symbol ist die Schnittstelle zu den Einstellungen und Steuerelementen des Plug-Ins. Wenn für Windows-Benutzer die Citrix Workspace-App und das Citrix Gateway-Plug-In integriert sind, zeigt das Dialogfeld **Info** in der Citrix Workspace-App die Steuerelemente für das Citrix Gateway-Plug-In an. Für macOS X-Benutzer sind nach der Integration keine Steuerelemente für das Citrix Gateway Plug-in verfügbar.

Bei einigen integrierten Bereitstellungen müssen möglicherweise die Plug-In-Steuerelemente verfügbar gemacht werden, während die Integration der zugrunde liegenden Funktionalität beibehalten wird. Verwenden Sie dazu den folgenden CLI-Befehl oder die folgende Citrix ADC-Konfigurationsdienstprogrammaufgabe, um die Symbolintegration für VPN-Clients umzuschalten.

### Stellen Sie die Icon-Integration über die CLI ein

Geben Sie an der Eingabeaufforderung;

```
set vpn parameter [-iconWithReceiver (ON/OFF)]

<!--NeedCopy-->
```

### Stellen Sie die Icon-Integration über die GUI

1. Navigieren Sie auf der Registerkarte Konfiguration zu **Citrix Gateway > Globale Einstellungen**.
2. Klicken Sie auf **Globale Einstellungen ändern**und wählen Sie dann die Registerkarte **Clienterfahrung** aus.
3. Klicken Sie auf **Erweiterte Einstellungen.**
4. Wählen Sie **VPN-Plug-in-Symbol mit der Citrix Workspace-App anzeigen** aus.

## IPv6 für ICA-Verbindungen konfigurieren

March 27, 2024

Citrix Gateway unterstützt IPv6-Adressen für ICA-Verbindungen. Verbindungen mit IPv6 zum Webinterface oder StoreFront funktionieren genauso wie IPv4-Verbindungen. Wenn Benutzer mithilfe der Citrix Gateway-Webadresse eine Verbindung herstellen, stellt Citrix Gateway die Verbindung zum Webinterface oder StoreFront her.

Sie können IPv6 für Citrix Gateway konfigurieren, das in einer DMZ bereitgestellt oder in einer Double-Hop-DMZ bereitgestellt wird.

Sie aktivieren IPv6 auf Citrix Gateway mithilfe der Befehlszeile. Sie können die folgenden Richtlinien verwenden:

- Aktivieren Sie IPv6 auf der Appliance.
- Konfigurieren Sie Subnetz-IP-Adressen.
- Stellen Sie die Reihenfolge der DNS-Auflösung ein.
- Legen Sie die Webinterface- oder StoreFront-Webadresse fest.
- Binden Sie die Secure Ticket Authority (STA) an Citrix Gateway.

Standardmäßig unterstützt die zugeordnete IP-Adresse keine IPv6-Adressen. Um Benutzerkommunikation an das interne Netzwerk weiterzuleiten, müssen Sie Subnetz-IP-Adressen erstellen und dann Citrix Gateway für die Verwendung der Subnetz-IP-Adressen konfigurieren.

Wenn Sie mehrere IPv6-Subnetze in Ihrem Netzwerk bereitstellen, erstellen Sie mehrere IPv6-Subnetz-IP-Adressen auf Citrix Gateway für jedes Subnetz in Ihrem Netzwerk. Netzwerk-Routing sendet die IPv6-Pakete mithilfe der Subnetz-IP-Adressen an die jeweiligen Subnetze.

### So konfigurieren Sie IPv6 für ICA-Proxy über die CLI

1. Melden Sie sich mit einer Secure Shell (SSH) -Verbindung, z. B. von PuTTY, bei Citrix Gateway an. Geben Sie an der Eingabeaufforderung;

```
enable ns feature IPv6PT. This enables IPv6.

enable ns mode USNIP.

set dns parameter  – resolutionOrder AAAAThenAQuery AThenAAAAQuery
   OnlyAAAAQuery OnlyAQuery

set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`

<!--NeedCopy-->
```

Dabei ist ist entweder der Domainname oder die IP-Adresse von StoreFront.

**Beispiel:**

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb
   `.
<!--NeedCopy-->
```

Oder

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie die IPv6-Adresse zur Konfiguration dieses Parameters verwenden, muss die IP-Adresse in Klammern enthalten sein.

## Homepage der Citrix Workspace-App auf Citrix Gateway konfigurieren

March 27, 2024

Sie können die Homepage der Citrix Workspace-App entweder global oder als Teil eines Sitzungsprofils konfigurieren. Wenn Sie die Citrix Workspace-App für Web und frühere Citrix Workspace-App-Versionen konfigurieren möchten, die StoreFront nicht über Citrix Gateway erkennen, müssen Sie zwei separate Sitzungsprofile erstellen. Das Feld Citrix Workspace App Homepage muss die richtige Webadresse für jedes Profil haben, damit sich Benutzer erfolgreich anmelden können.

Für Citrix Workspace-Apps, die StoreFront über Citrix Gateway erkennen, können Sie die Citrix Workspace-App für Web und die Citrix Workspace-App ein Profil teilen lassen. Citrix empfiehlt jedoch, ein Sitzungsprofil für die Citrix Workspace-App für Web und ein separates Sitzungsprofil für alle anderen Citrix Workspace-Apps zu konfigurieren.

### So konfigurieren Sie die Homepage der Citrix Workspace-App global

So konfigurieren Sie die Homepage der Citrix Workspace-App global:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Klicken Sie im Dialogfeld Global Citrix Gateway Settings auf die Registerkarte Published Applications.
4. Geben Sie auf der Homepage der Citrix Workspace-App die Webadresse für die Citrix Workspace-App oder die Citrix Workspace-App für Web-Homepage ein, und klicken Sie dann auf OK.

### So konfigurieren Sie die Homepage der Citrix Workspace-App in einem Sitzungsprofil

So konfigurieren Sie die Homepage der Citrix Workspace-App in einem Sitzungsprofil:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte **Profile** auf **Hinzufügen**.
3. Klicken **Sie im Dialogfeld Citrix Gateway-Sitzungsprofil erstellen** auf der Registerkarte **Published Application** neben **Citrix Receiver-Homepage** auf **Override Global**.
4. Geben Sie auf der Homepage der Citrix Workspace-App die Webadresse für die Citrix Workspace-App oder die Citrix Workspace-App für Web-Homepage ein, und klicken Sie dann auf **Erstellen**.

## Citrix Workspace-App-Designs auf die Citrix Gateway-Anmeldeseite anwenden

March 27, 2024

Sie können die GUI verwenden, um das Citrix Workspace-App-Design auf die Anmeldeseite für Citrix Gateway anzuwenden. Sie können zwischen dem Citrix Workspace-App-Design, dem Standarddesign oder einem benutzerdefinierten Design wechseln, das Sie erstellen.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte "Configuration"im Navigationsbereich "Citrix Gateway"und klicken Sie auf "Global Settings".
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Klicken Sie im Dialogfeld Globale Citrix Gateway-Einstellungen auf die Registerkarte Clienterfahrung.
4. Klicken Sie neben UI Theme auf Green Bubble und dann auf OK.

   Dieser Befehl überschreibt die ursprüngliche Anmeldeseite mit dem Receiver-Design. Hinweis: Nachdem Sie ein anderes Thema angewendet haben, raten Sie den Benutzern, den Browser-Cache zu löschen, um zu verhindern, dass zwischengespeicherte Seiten angezeigt werden.

## Benutzerdefiniertes Designs für die Citrix Gateway-Anmeldeseite erstellen

March 27, 2024

Sie können die GUI verwenden, um ein benutzerdefiniertes Design für die Anmeldeseite für Citrix Gateway zu erstellen. Sie können auch das Standarddesign beibehalten oder das Citrix Workspace-App-Design verwenden. Wenn Sie ein benutzerdefiniertes Design auf die Anmeldeseite anwenden möchten, verwenden Sie die Citrix Gateway-Befehlszeile, um das Design zu erstellen und bereitzustellen. Sie verwenden dann die GUI, um die benutzerdefinierte Themenseite festzulegen.

Sie konfigurieren die Seite mit dem benutzerdefinierten Thema mithilfe der globalen Einstellungen von Citrix Gateway.

Sie können diese Funktion mit den folgenden Versionen von Citrix Gateway verwenden:

- Citrix Gateway 10.1
- Access Gateway 10, Build 73.5002.e (Sie müssen diesen Build nach Build 71.6104.e installieren, um diese Funktion mit Endpoint Management Versionen 2.5, 2.6 oder 2.8 zu verwenden)

- Access Gateway 10, Build 71.6104.e

### Erstellen und Bereitstellen des benutzerdefinierten Themas über die CLI

So erstellen und implementieren Sie das benutzerdefinierte Design mithilfe der Befehlszeile:

1. Melden Sie sich an der Citrix Gateway Befehlszeile an.
2. Geben Sie an der Eingabeaufforderung shell ein.
3. Geben Sie an der Eingabeaufforderung `mkdir /var/ns_gui_custom; cd /netscaler ; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*` ein.
4. Verwenden Sie das Konfigurationsdienstprogramm, um zum benutzerdefinierten Thema zu wechseln und dann unter /var/ns_gui_custom/ns_gui/VPN Anpassungsänderungen vorzunehmen. Sie haben folgende Möglichkeiten:
   - Nehmen Sie Änderungen an der Datei css/ctx.authentication.css vor.
   - Kopieren Sie ein benutzerdefiniertes Logo in den Ordner /var/ns_gui_custom/ns_gui/vpn/media. **Hinweis:** Sie können WinSCP verwenden, um die Dateien zu übertragen.
5. Wenn Sie über mehrere Citrix Gateway-Geräte verfügen, wiederholen Sie die Schritte 3 und 4 für alle Appliances.

## Registrierungsschlüssel für den Citrix Gateway Windows VPN-Client

March 27, 2024

Die VPN-Clientregistrierungsschlüssel sind unter **HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Client**verfügbar. In der folgenden Tabelle sind die Citrix Gateway VPN-Clientregistrierungsschlüssel, -werte und eine kurze Beschreibung der einzelnen Werte aufgeführt.

| Registrierungsschlüssel | Registrierungstyp | Werte und Beschreibung |
|---|---|---|
| AlwaysOnService | REG_DWORD | 1 => Richten Sie einen Tunnel auf Maschinenebene ein, aber keinen Tunnel auf Benutzerebene. 2 => Stellen Sie einen Tunnel auf Maschinenebene und einen Tunnel auf Benutzerebene |

| Registrierungsschlüssel | Registrierungstyp | Werte und Beschreibung |
|---|---|---|
| AlwaysOnURL | REG_SZ | URL des virtuellen Citrix Gateway-Servers, mit dem der Benutzer eine Verbindung herstellen möchte. Beispiel: *https://xyz.companyDomain.com* |
| AlwaysOn | REG_DWORD | 1 => Erlaubt Netzwerkzugriff bei VPN-Fehler. 2=> Blockieren Sie den Netzwerkzugriff bei VPN-Fehler. |
| locationDetection | REG_DWORD | 1 => Um die Standorterkennung zu aktivieren. 0 => Um die Standorterkennung zu deaktivieren. |
| suffixList | REG_SZ | Durch Semikolons getrennte Liste von Intranetdomänen. Wird verwendet, wenn die Standorterkennung aktiviert ist. |
| AlwaysOnWhitelist | REG_SZ | Durch Semikola getrennte Liste von IP-Adressen oder FQDNs, die vom Treiber im strikten Modus Always On auf die Positivliste gesetzt werden sollen. |
| ProductVersion | REG_SZ | Aktuelle installierte Version des Citrix Gateway Plug-ins. |
| InstallDir | REG_SZ | Speicherort, an dem das Citrix Gateway Plug-in installiert ist. |
| userCertCAList | REG_SZ | Wird im Kontext des Always On Service verwendet, bei dem ein Kunde die Liste der Zertifizierungsstellen angeben kann, aus denen das Clientzertifikat ausgewählt werden soll. |

| Registrierungsschlüssel | Registrierungstyp | Werte und Beschreibung |
|---|---|---|
| addedRoutes/modifiedRoutes | REG_SZ | Erstellt für die interne Plug-In-Kommunikation. Benutzer dürfen diesen Schlüssel nicht ändern. |
| ProductCode | REG_SZ | Dieser Schlüssel wird intern verwendet. Benutzer dürfen diesen Schlüssel nicht ändern |
| EnableAutoUpdate | REG_DWORD | Wird verwendet, um die Plug-In-Update-Funktionalität von der Clientseite aus zu steuern. Stellen Sie auf 0 ein, um die Funktion zur automatischen Aktualisierung zu deaktivieren Stellen Sie auf 1 ein, um die ADC-Konfiguration zu respektieren. |
| Connected | REG_DWORD | Bei erfolgreicher Verbindung wird dieser Schlüssel auf 1 und sonst auf 0 gesetzt. Dieser Schlüssel wird intern verwendet. Benutzer dürfen diesen Schlüssel nicht ändern. |
| EnableVA | REG_DWORD | Wenn der Citrix Virtual Adapter aktiviert sein muss, wenn IIP vorhanden ist. Dieser Schlüssel wird intern verwendet. Benutzer dürfen diesen Schlüssel nicht ändern. |
| DisableGA | REG_DWORD | Stellen Sie auf 1, um Google Analytics zu deaktivieren. |

| Registrierungsschlüssel | Registrierungstyp | Werte und Beschreibung |
|---|---|---|
| DisableCredProv | REG_DWORD | Wenn Always On vor der Benutzeranmeldung aktiviert ist, fügt das Windows VPN-Plug-In den Anmeldeinformationsanbieter hinzu, um den Tunnelstatus auf dem Anmeldebildschirm anzuzeigen. Wenn Sie diese zusätzliche Funktionalität nicht benötigen, erstellen Sie diese Registrierung und setzen Sie sie auf 1. |
| ClientControl | REG_DWORD | 1 => Ermöglicht Benutzern, sich abzumelden oder sich mit anderen Gateways zu verbinden. 0 => Blockiert Benutzer, sich abzumelden oder sich mit anderen Gateways zu verbinden. |
| ForcedLogging | REG_DWORD | Setzen Sie diesen Schlüssel auf 1, um die Debug-Protokollierung zu aktivieren. |
| NoDHCPRoute | REG_DWORD | Wenn auf 1 gesetzt, wird die DHCP-Serverroute nicht hinzugefügt. |
| DisableIntuneDeviceEnrollment | REG_DWORD | Wenn auf 1 gesetzt, wird die Intune-Geräteregistrierung nicht durchgeführt. |
| HttpTimeout | REG_DWORD | Das HTTP-Timeout ist in Sekunden konfiguriert. Wenn das Timeout nicht konfiguriert ist, wird das Standard-Timeout verwendet. Der standardmäßige Timeout-Wert beträgt 100 Sekunden, basierend auf Windows-Standards. |

| Registrierungsschlüssel | Registrierungstyp | Werte und Beschreibung |
|---|---|---|
| DisableIconHide | REG_DWORD | 1 => Die Citrix Workspace-App und das Gateway-Plug-In werden in der Taskleiste angezeigt. 0 => Das Gateway-Plug-In-Symbol ist in die Citrix Workspace-App für Windows integriert. Das Gateway-Plug-In ist in der Taskleiste nicht sichtbar, wenn eine vollständige VPN-Sitzung ausgeführt |
| EnableWFP | REG_DWORD | Standardwert 0 => Standardmäßig ist DNE aktiviert. 1 => Das VPN-Plug-In verwendet WFP. 0 => Das VPN-Plug-in verwendet DNE. |
| SecureAccessLogInScript | REG_SZ | Der Citrix Secure Access Service greift mit diesem Registrierungsschlüssel auf die Anmeldeskriptkonfiguration zu, wenn er eine Verbindung zum Citrix Secure Private Access Service herstellt. Einzelheiten finden Sie unter Registrierungen zur Konfiguration von Anmelde- und Abmeldeskripts. |

| Registrierungsschlüssel | Registrierungstyp | Werte und Beschreibung |
|---|---|---|
| SecureAccessLogOutScript | REG_SZ | Der Citrix Secure Access Service greift mit diesem Registrierungsschlüssel auf die Konfiguration des Abmeldeskripts zu, wenn er eine Verbindung zum Citrix Secure Private Access Service herstellt. Einzelheiten finden Sie unter Registrierungen zur Konfiguration von Anmelde- und Abmeldeskripts. |

> **Wichtig:**
>
> Sie können Registrierungsschlüssel basierend auf Ihren Bereitstellungen anwenden. Beispielsweise ist die AlwaysOnService-Registrierung nur für Always on Service anwendbar, während die ClientControl-Registrierung nicht für Always on Service gilt. Weitere Einzelheiten finden Sie in der einzelnen Bereitstellungsdokumentation.

## HttpOnly-Flag für Authentifizierungs-Cookies erzwingen

March 27, 2024

Ab Citrix Gateway Version 13.0-89.x und höher ist das HttpOnly-Flag für die Authentifizierungscookies von VPN-Szenarien verfügbar, d. h. NSC_AAAC- und NSC_TMAS-Cookies. Das NSC_TMAS-Authentifizierungscookie wird während der nFactor-Authentifizierung verwendet und das NSC_AAAC-Cookie wird für die authentifizierte Sitzung verwendet. Das HttpOnly-Flag in einem Cookie schränkt den Cookie-Zugriff mithilfe der Cookie-Option für JavaScript-Dokumente ein. Dies hilft dabei, Cookie-Diebstahl aufgrund von Cross-Site Scripting verhindern.

### Unterstütztes Szenario

Das HTTPOnly-Flag wird für die nFactor-Authentifizierung unterstützt.

**Verhalten, wenn der HttpOnlyCookie-Knopf des Citrix ADC AAA-Parameters zusammen mit dem HttpOnlyCookie-Knopf von tmsession verwendet wird:**

- Wenn der httpOnlyCookie-Knopf des Authentifizierungs-, Autorisierungs- und Audit-Parameters aktiviert ist und die nFactor-Authentifizierung verwendet wird, überschreibt der httpOnlyCookie-Knopf des Authentifizierungs-, Autorisierungs- und Auditing-Parameters den httpOnlyCookie-Knopf der TM-Sitzung. Außerdem sind sowohl NSC_TMAS als auch NSC_AAAC unabhängig vom Sitzungstyp als HttpOnly gekennzeichnet, unabhängig davon, ob es sich um eine VPN-Sitzung, TM-Sitzung oder während der nFactor-Authentifizierung handelt.
- Wenn der HttpOnlyCookie-Knopf deaktiviert ist, ist das HttpOnly-Flag für eine VPN-Sitzung nicht gesetzt. Für das Authentifizierungs-, Autorisierungs- und Auditszenario wird das HttpOnly-Flag auf der Grundlage des TM-Sitzungsknopfwerts gesetzt.

### HttpOnly-Funktion über die CLI konfigurieren

- HttpOnly-Flag aktivieren

```
set aaa parameter -httpOnlyCookie ENABLED
<!--NeedCopy-->
```

- Status der HttpOnly-Funktion überprüfen

```
show aaa parameter
<!--NeedCopy-->
```

### Einschränkungen

- Wenn die HttpOnly-Funktion aktiviert ist, funktioniert die Home-Page-Schaltfläche auf dem Citrix Secure Access-Client nicht.
- Das HttpOnly-Flag ist bei keiner klassischen Authentifizierung gesetzt.

## Benutzerportal für VPN-Benutzer anpassen

March 27, 2024

Citrix Gateway-Installationen, die das Portal für VPN-Benutzer bereitstellen, enthalten die Option, ein Portal-Design auszuwählen, um ein individuelles Erscheinungsbild für die Portalseiten zu erzielen. Sie können aus einem bereitgestellten Themensatz auswählen oder ein Thema als Vorlage verwenden, um ein benutzerdefiniertes oder gebrandetes Portal zu erstellen. Mit dem Konfigurationsdienstprogramm können Sie ein Thema ändern, indem Sie neue Logos, Hintergrundbilder, benutzerdefinierte Beschriftungen für Eingabefelder und verschiedene andere Attribute des CSS-basierten Portaldesigns

hinzufügen. Die integrierten Portal-Themen enthalten Inhalte für fünf Sprachen: Englisch, Französisch, Spanisch, Deutsch und Japanisch. Verschiedene Benutzer werden in verschiedenen Sprachen bedient, abhängig von den von ihren Webbrowsern gemeldeten Gebietsschemas.

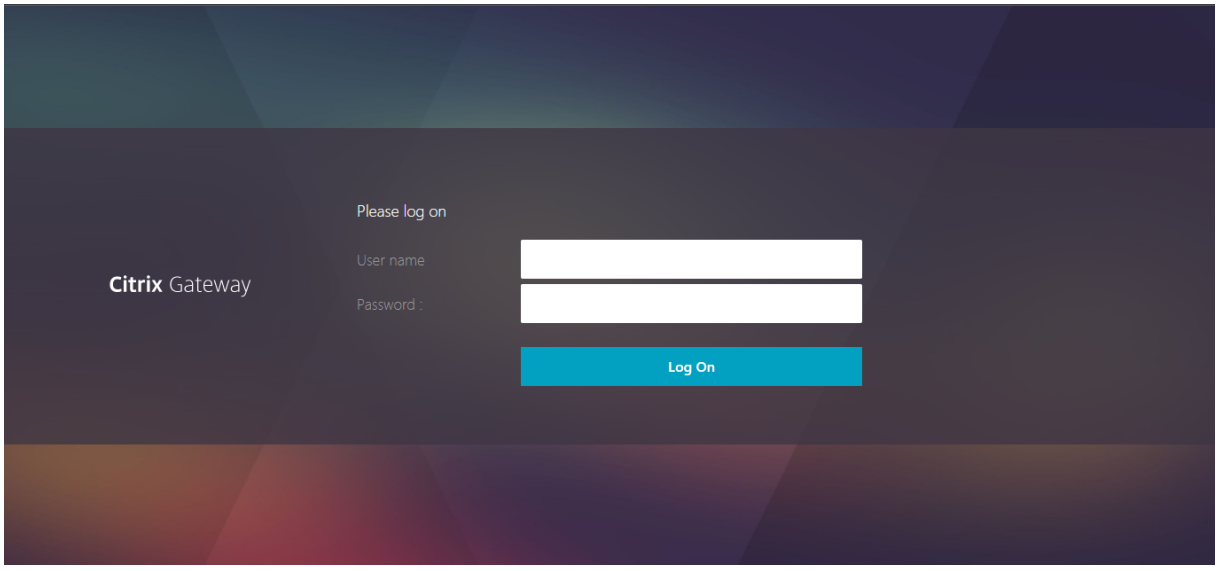
Sie können eine benutzerdefinierte EULA erstellen, die VPN-Benutzern präsentiert wird, bevor sie sich anmelden dürfen. Die EULA-Funktion unterstützt gebietsschemaspezifische Versionen einer EULA, die Benutzern basierend auf den von ihren Webbrowsern gemeldeten Gebietsschemas präsentiert werden.

Sowohl Portal-Themen als auch EULA-Konfigurationen können unabhängig voneinander auf der virtuellen VPN-Server- und VPN-Ebene gebunden werden.

> **Wichtig:**
>
> Citrix unterstützt keine Anpassung, die Codeänderungen erfordert, und bietet keine Unterstützung für die Lösung von Problemen, die über die Rückkehr zu einem Standarddesign hinausgehen.

### Wenden Sie ein Portalthema

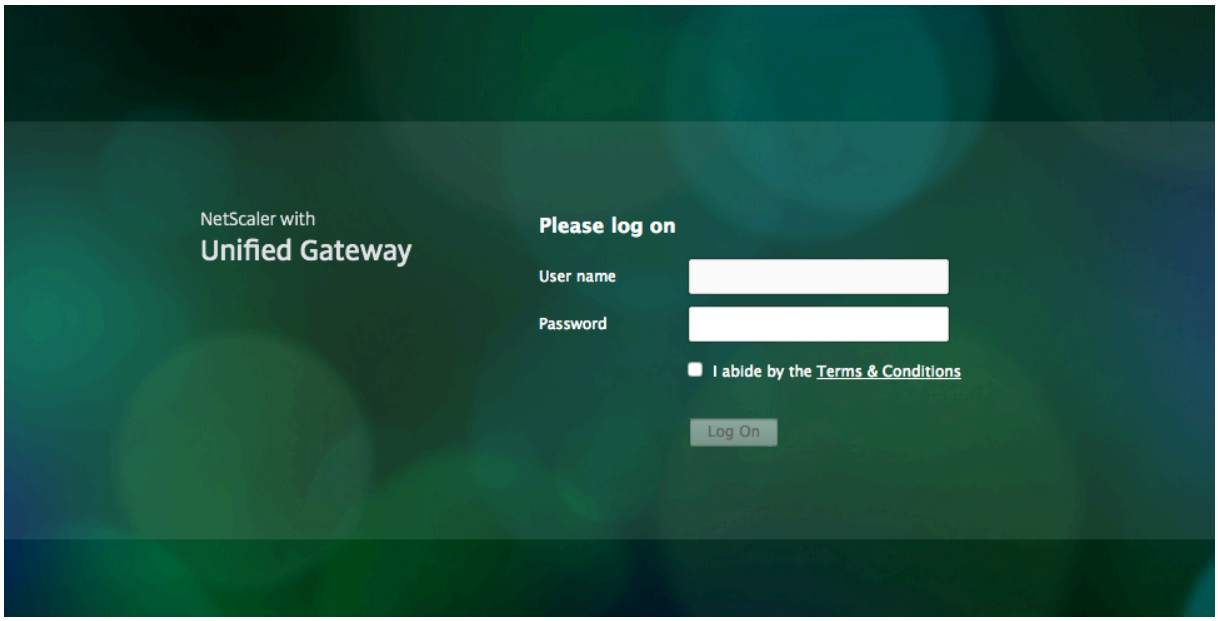
Ab Version 13.0 Build 67.43 ist das VPN-Portal standardmäßig für die Verwendung des RfWebUI-Themas konfiguriert. Zuvor `Caxton theme` war das das Standardthema. Sie können auch die Themen Green Bubble und X1 anwenden.



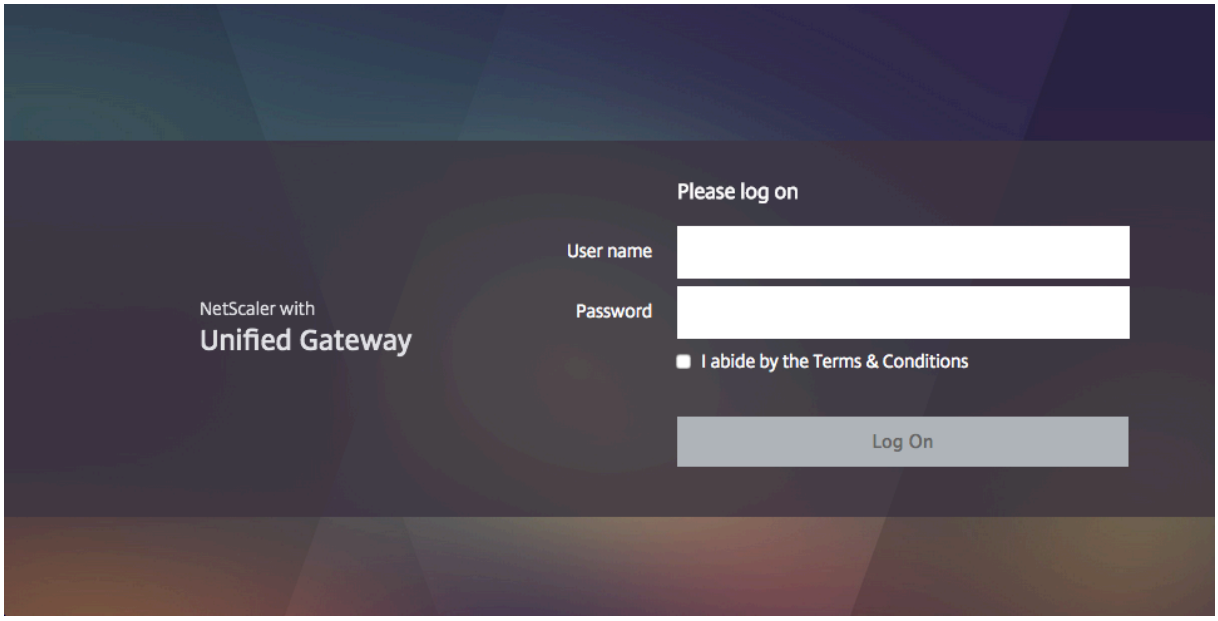
**Caxton-Thema**


**Thema Grüne Blase**



**X1-Thema**




Sie können jedes der bereitgestellten Themen direkt auf einen virtuellen VPN-Server oder als globale VPN-Bindung anwenden.

## Binden Sie ein Portal-Thema an einen virtuellen VPN-Server

Sie können ein Portal-Design an einen vorhandenen virtuellen Server oder beim Erstellen eines neuen virtuellen Servers binden.

### Binden Sie ein Portal-Thema über die CLI an einen virtuellen VPN-Server

Geben Sie an der Eingabeaufforderung;

```
bind vpn vserver <name> - portaltheme <name>
<!--NeedCopy-->
```

### Binden Sie ein Portal-Thema über die GUI an einen virtuellen VPN-Server

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Citrix Gateway** und klicken Sie auf **Virtuelle Server.**
2. Wählen Sie einen virtuellen Server aus und klicken Sie dann auf **Bearbeiten**.
3. Wenn ein Portal-Design noch nicht an den virtuellen Server gebunden ist, klicken Sie im Detailbereich unter **Erweiterte Einstellungen** auf **Portaldesign**. Andernfalls ist die Option **Portaldesign**bereits im Detailbereich erweitert.

4. Klicken Sie im Detailbereich unter **Portal-Designs**auf **Kein Portal-Design**, um das Bindungsfenster Portal-Design zu erweitern.
5. `Click` **Zum Auswählen klicken**.
6. Klicken Sie im Fenster **Portal-Designs** auf einen Themennamen und dann auf **Auswählen**.
7. Klicken Sie auf **Bind**.
8. Klicken Sie auf **Fertig**.

Wenn Sie einen virtuellen VPN-Server erstellen, können Sie die Schritte im vorherigen Verfahren ab Schritt 3 ausführen, während Sie sich im **Bearbeitungsbereich des virtuellen VPN-Servers** befinden, um ein Portal-Design zu binden.

## Binden Sie ein Portal-Thema an VPN global

### Binden Sie ein Portal-Thema über die CLI an VPN Global

Geben Sie in der Befehlszeile ein;

```
bind vpn global portaltheme <name>
<!--NeedCopy-->
```

### Binden Sie ein Portal-Thema über die GUI an VPN Global

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Citrix Gateway.**
2. Klicken Sie im Hauptdetailbereich auf **Citrix Gateway Policy Manager**.
3. Klicken Sie auf das Symbol "**+**".
4. Wählen Sie in der Liste **Bindepunkt** die Option **Ressourcen**aus.
5. Wählen Sie in der Liste**VerbindungstypPortal-Thema aus.**
6. Klicken Sie auf **Weiter**.
7. Klicken Sie im Bildschirm "**Bindepunkt**"auf "**Bindung hinzufügen**".
8. Klicken Sie auf **Klicken, um auszuwählen**.
9. Klicken Sie im Fenster **Portal-Designs** auf einen Themennamen und dann auf **Auswählen**.
10. Klicken Sie auf **Bind**.
11. Klicken Sie auf **Schließen**.
12. Klicken Sie auf **Fertig.**

> **Tipp:**
>
> Nachdem Sie die Änderungen vorgenommen haben, verwenden Sie den Befehl 'save ns config'in der Befehlszeile oder klicken Sie im Konfigurationsdienstprogramm auf das Speichersymbol, um sicherzustellen, dass Ihre Änderungen in der Citrix ADC-Konfigurationsdatei gespeichert werden.

## Erstellen eines Portal-Themas

Um ein benutzerdefiniertes Portaldesign zu erstellen, verwenden Sie eines der bereitgestellten Portal-Designs als Vorlage. Das System erstellt eine Kopie des ausgewählten Vorlagendesigns mit einem von Ihnen angegebenen Namen.

## Verwenden Sie ein Stockportal-Thema als Vorlage für ein benutzerdefiniertes Portal-Thema

Um ein Portal-Design zu erstellen, können Sie das Konfigurationsdienstprogramm oder die Befehlszeile verwenden, um die Themenentität zu erstellen. Die detaillierten Anpassungssteuerungen sind jedoch nur im Konfigurationsdienstprogramm verfügbar.

### Erstellen Sie über die CLI ein Portal-Thema

Geben Sie in der Befehlszeile ein;

```
add portaltheme <name> basetheme <name>
<!--NeedCopy-->
```

### Erstellen Sie über die GUI ein Portal-Thema

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Citrix Gateway** und klicken Sie auf **Portal Themes**.
2. Klicken Sie im Hauptdetailbereich auf **Hinzufügen**.
3. Geben Sie einen Namen für das Thema ein, wählen Sie eine Vorlage aus der Vorlagenliste aus und klicken Sie dann auf **OK**.
4. An dieser Stelle wird Ihnen die erste Ansicht des Bearbeitungsfensters des Portal-Themas angezeigt. Klicken Sie zum Beenden auf **OK**.

Sie können das neue Portal-Thema mit der Erstansicht anpassen.

Sobald ein neues Thema erstellt wurde, können Sie es an einen virtuellen VPN-Server oder an VPN global binden. Sie können ein neues Thema sofort nach der Erstellung oder nach Abschluss Ihrer Anpassungen binden.

## Anpassung des Portal-Themas

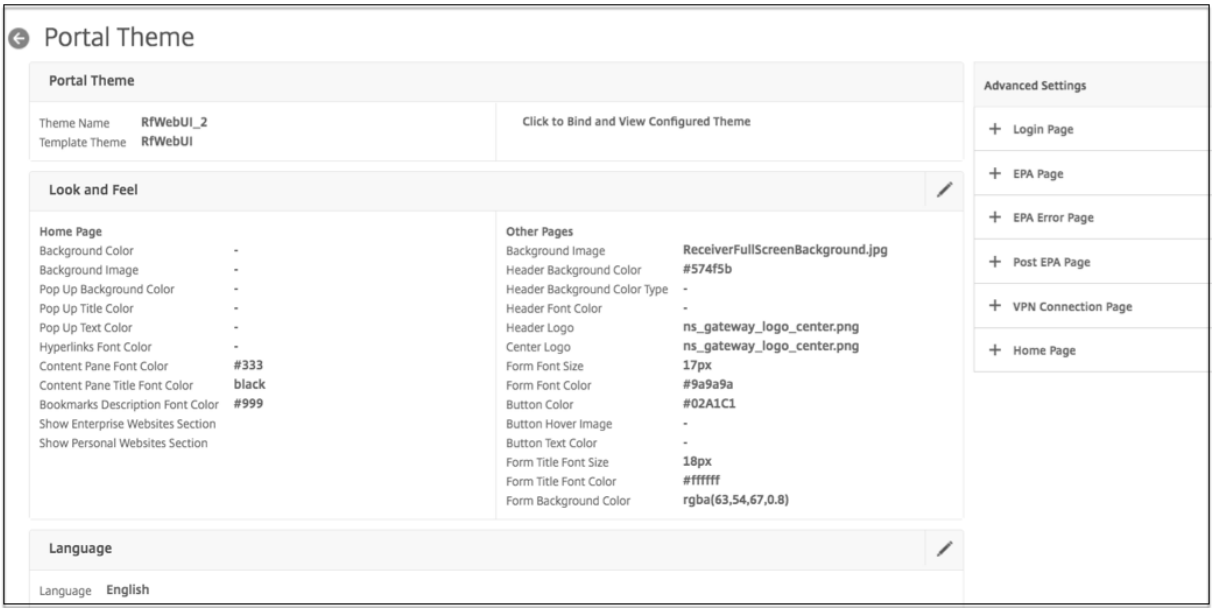
Um ein Portal-Design anzupassen, verwenden Sie die Oberfläche Portal Theme im Konfigurationsdienstprogramm. Um die besten Ergebnisse zu erzielen, müssen Sie die verschiedenen Elemente dieser Oberfläche verstehen, bevor Sie sie verwenden.

## Über die Oberfläche des Portal-Themas

Um die **Portal Theme-Oberfläche** im Citrix Gateway-Konfigurationsprogramm zu öffnen, navigieren Sie auf der Registerkarte **Konfiguration** zu **Citrix Gateway** und klicken Sie auf **Portal Themes**. Sie können entweder ein Theme erstellen, wie unter *Portal-Thema erstellen* beschrieben, oder ein vorhandenes Theme im Hauptdetailbereich auswählen und auf **Bearbeiten**klicken.

Die Seite zur Anpassung des Portaldesigns enthält vier Hauptkomponentenbereiche zum Ändern eines Portaldesigns: den Bereich **Portaldesign**, den Bereich Look & Feel, den Bereich **Erweiterte Einstellungen** und den Bereich **Sprache**.




Der Bereich **Portal-Thema** oben auf der Seite gibt an, welches Thema zur Bearbeitung geladen wird und auf welchem Vorlagenthema es basiert. Mit der Anzeigeoption hier können Sie Ihre Anpassungen anzeigen, ohne mit einer Benutzerverbindung auf das VPN zugreifen zu müssen. Bei Verwendung der Anzeigeoption muss das Thema an einen virtuellen VPN-Server gebunden werden, und die Bindung bleibt bestehen, nachdem das Anzeigefenster geschlossen wurde.

Mit dem Bereich "**Look & Feel** "in der Mitte der Seite konfigurieren Sie die allgemeinen Eigenschaften eines Themas, wie Überschriften, Hintergrundfarben und Bilder, Schrifteigenschaften und Logos. Wenn sich dieser Bereich im Bearbeitungsmodus befindet, stehen Attributlegenden zur Verfügung, um zu bestimmen, wo die Look & Feel Attribute auf Portalseiten verwendet werden.

Der Bereich **Erweiterte Einstellungen** enthält die Inhaltssteuerelemente auf dem Bildschirm für die einzelnen Portalseiten. Um den Inhalt einer Seite zur Bearbeitung zu laden, klicken Sie auf eine der aufgelisteten Seiten. Die Seitensteuerelemente werden dann unter den anderen Mittelfenstern geöffnet. Eine Seite bleibt im Bereich **Erweiterte Einstellungen** über Portal-Design-Bearbeitungen reduziert, solange die Seite nicht geändert wurde.

Im Bereich **Sprache** können Sie auswählen, welche der Sprachen geladen wird, wenn eine Seite zur

Bearbeitung im Bereich **Erweiterte Einstellungen** ausgewählt wird. Die englischsprachigen Seiten werden standardmäßig geladen.

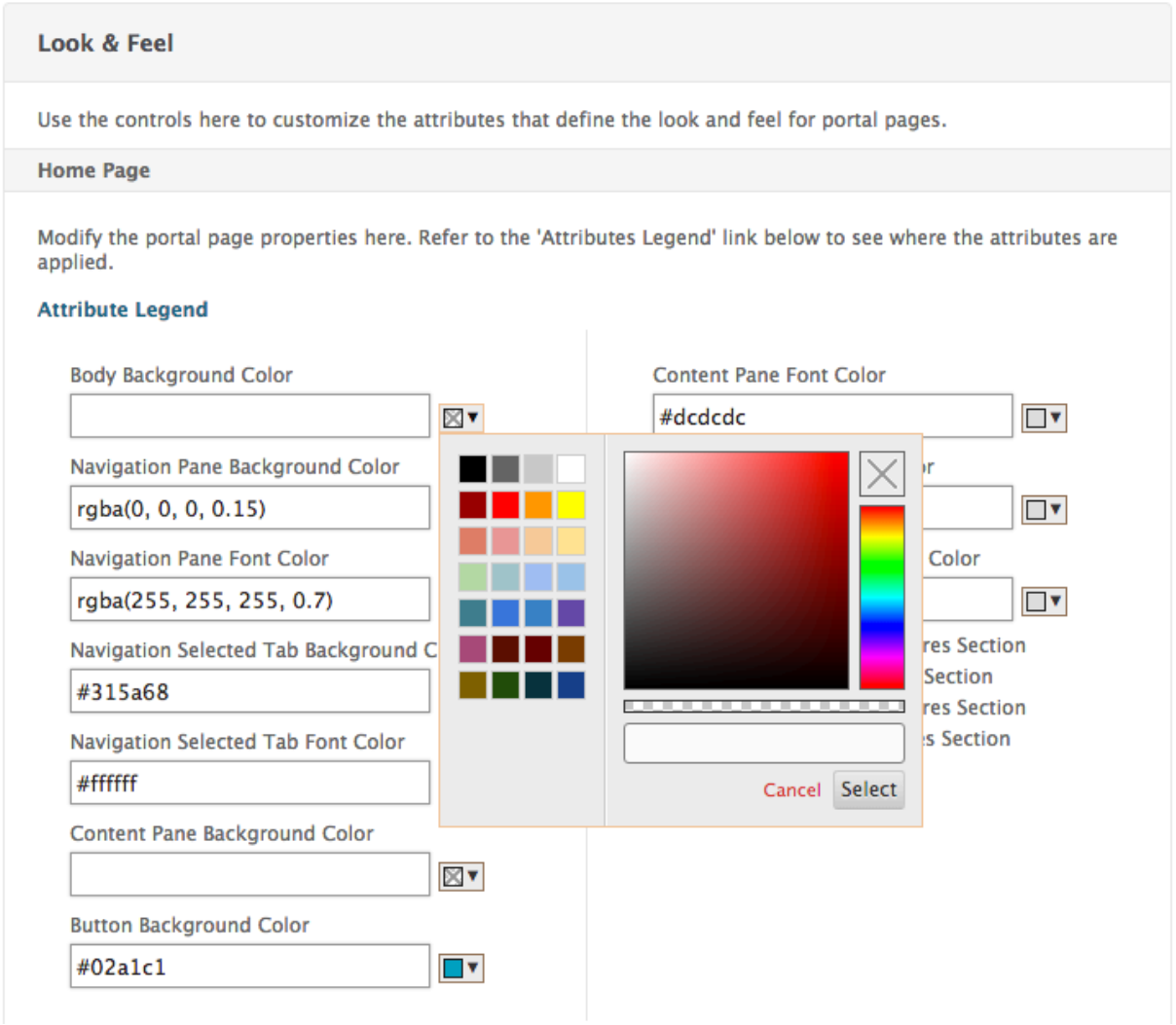
### Arten von anpassbaren Seitenattributen

Beim Anpassen eines Portal-Designs können Sie eine Reihe von Attributen in der Portal-Design-Oberfläche ändern. Zusammen mit dem Text und den unterstützten Sprachen, die bearbeitet werden können, können die grafischen Elemente des Layouts des Portals auf Ihre Bedürfnisse zugeschnitten werden. Jeder der Seitenelementtypen hat Parameter oder Empfehlungen, die vor dem Ändern berücksichtigt werden müssen.

#### *Farben*

Das Portaldesign legt die Farben für Attribute wie Seitenhintergründe, Highlights, Text für Titel und Textinhalt, Schaltflächensteuerelemente und Hover-Antworten fest. Um ein Farbattribut anzupassen, können Sie einen Farbwert direkt für ein ausgewähltes Element eingeben oder den mitgelieferten Farbwähler verwenden, um einen Farbwert zu generieren. Die Schnittstelle unterstützt die Eingabe gültiger HTML-Farbwerte im RGBA-Format, im HTML-Hexadezimal-Triplett-Format und X11-Farbnamen. Auf den Farbwähler kann für jedes zutreffende Farbattribut zugegriffen werden, indem Sie auf das Farbfeld neben dem Eingabefeld des Attributs klicken.




***Schriften***

Zusammen mit den Schriftfarben können Sie die Schriftgröße für einige Seitenattribute ändern. Für jedes dieser Attribute bietet ein Menü die für jedes Attribut verfügbaren Größen an, wie durch das Design des Portals festgelegt.

***Bilder***

Für Bilder, enthält eine Popup-Beschreibung, die für jedes Steuerelement verfügbar ist, Größenempfehlungen und andere Anforderungen. Die Beschreibungen variieren je nach Position eines Attributs auf der Seite und seiner Funktion. Sie können PNG- oder JPEG-Bilddateiformate verwenden. Sie können ein Bild zum Hochladen auswählen, indem Sie das Kontrollkästchen unter dem Dateinamen eines Elements aktivieren und dann zu dem Ort navigieren, an dem sich das Bild auf dem Laufwerk Ihres lokalen Computers befindet.

***Labels***

Im Abschnitt **Erweiterte Einstellungen** können Sie den Text einer bestimmten Portalseite auswählen,

den Sie ändern möchten. Wenn Sie den englischen Standardtext für eine Seite ändern, wird der Text für andere Sprachen nicht neu übersetzt. Der Inhalt der alternativen Sprachseite wird als Annehmlichkeit bereitgestellt, erfordert jedoch manuelle Aktualisierungen für etwaige Anpassungen. Um eine andere Sprachversion für eine Seite zu bearbeiten, reduzieren Sie zuerst das Fenster, falls es geöffnet ist, indem Sie auf das **X-Symbol** für die offene Portalseite klicken. Wählen Sie dann die Sprache im Bereich **Sprache** aus und klicken Sie auf **OK**. Alle Portalseiten, die im Bereich **Erweiterte Einstellungen** geöffnet werden, sind in dieser Sprache, bis Sie eine andere auswählen.

> **Wichtig!**
>
> In Hochverfügbarkeits- oder Clusterbereitstellungen werden Portal-Designs nur dann über die freigegebene Konfiguration verteilt, wenn die Einstellungen des Portal-Designs an den primären bzw. Konfigurationskoordinator-Citrix ADC-Entitäten vorgenommen werden.

## Ältere Portal-Anpassungen

Für Installationen mit manuell geändertem benutzerdefiniertem Portaldesign, die in Citrix Gateway- oder Access Gateway-Versionen vor 11.0 erstellt wurden, empfiehlt Citrix dringend, mit einem neuen Portal-Design in der Anpassungsoberfläche zu beginnen. Wenn Sie das nicht können, können Sie eine Anpassung manuell anwenden, aber direkte Unterstützung dafür wird nicht angeboten.

Wenn Sie ein manuell angepasstes Portal verwenden, müssen Sie das angepasste Portal als globale Portalkonfiguration festlegen. Dies bedeutet jedoch, dass eine angewendete globale Portalkonfiguration *nicht* mit VPN-Portal-Themenbindungen auf virtueller Serverebene außer Kraft gesetzt werden kann. Der Versuch, in diesem Fall eine Bindung des virtuellen VPN-Servers mit dem Konfigurationsdienstprogramm oder der Befehlszeile zu erstellen, gibt einen Fehler zurück.

Bei Hochverfügbarkeit und Clusterkonfigurationen müssen außerdem alle manuellen Anpassungen an jedem Knoten in der Bereitstellung durchgeführt werden, da die zugrunde liegenden Dateien auf dem Citrix ADC-Dateisystem nicht in der automatisch freigegebenen Konfiguration verteilt werden.

### Erstellen Sie manuell eine benutzerdefinierte Portalkonfiguration

Um eine ältere angepasste Portalkonfiguration nach dem Upgrade auf Citrix Gateway 11.0 manuell anzuwenden, müssen Sie eine Kopie einer vorhandenen Portalseite ändern, die **benutzerdefinierten Portaldateien in das Citrix ADC-Dateisystem einfügen und CUSTOM** als **UITHEME-Parameter** auswählen.

Sie können WinSCP oder ein anderes sicheres Kopierprogramm verwenden, um Dateien in das Citrix ADC-Dateisystem zu übertragen.

1. Melden Sie sich an der Citrix Gateway Befehlszeile an.
2. Geben Sie an der Eingabeaufforderung**shell**ein

3. Geben Sie an der Eingabeaufforderung **mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/* ein.**
4. Geben Sie an der Eingabeaufforderung **cd /var/netscaler/logon/themes/**ein

    - Wenn Sie das Design der grünen Blase anpassen möchten, geben Sie**cp -r** `Greenbubble` **Custom** ein, um eine Kopie des Green Bubble-Themas zu erstellen.
    - Wenn Sie das Standarddesign (`Caxton`) anpassen möchten, geben Sie **cp -r Default Custom ein.**
    - Um das X1-Design anzupassen, geben Sie**cp -r X1 Custom ein.**

5. Nehmen Sie die erforderlichen Änderungen an den kopierten Dateien unter**/var/netscaler/logon/themes/cu** vor, um das Theme manuell anzupassen.

    - Nehmen Sie die erforderlichen Änderungen an **css/base.css**vor.
    - Kopieren Sie alle benutzerdefinierten Images in das Verzeichnis **/var/ns_gui_custom/ns_gui/vpn/med**
    - Nehmen Sie Änderungen an Beschriftungen in den Dateien vor, die im Verzeichnis **ressources/** vorhanden sind. Diese Dateien entsprechen den vom Portal unterstützten Gebietsschemas.
    - Wenn auch Änderungen an HTML-Seiten oder Javascript-Dateien erforderlich sind, können Sie die relevanten Dateien in **/var/ns_gui_custom/ns_gui/**vornehmen.

6. Nachdem alle Anpassungsänderungen abgeschlossen sind, geben Sie an der Eingabeaufforderung Folgendes ein: **tar —cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gu**

> **Wichtig!**
>
> Beim Kopieren eines Themenverzeichnisses in den vorherigen Schritten muss der Name des kopierten Ordners genau als “Benutzerdefiniert”eingegeben werden, da bei Verzeichnisnamen innerhalb der Citrix ADC Shell-Oberfläche die Groß-/Kleinschreibung beachtet wird. Wenn der Verzeichnisname nicht genau eingegeben wird, wird der Ordner nicht erkannt, wenn die **UITHEME-Einstellung** auf **CUSTOM**konfiguriert ist.

#### Wählen Sie das angepasste Thema als globalen VPN-Parameter

Sobald die manuell angepasste Portalkonfiguration abgeschlossen und in das Citrix ADC-Dateisystem kopiert wurde, muss sie auf die Citrix Gateway-Konfiguration angewendet werden. Dies erfolgt durch Festlegen des UITHEME-Parameters auf CUSTOM und kann mit der Befehlszeile oder dem Konfigurationsdienstprogramm abgeschlossen werden.

Um die Befehlszeile zu verwenden, geben Sie den folgenden Befehl ein, um den **UITHEME-Parameter** festzulegen.

```
1 set vpn parameter UITHEME CUSTOM
2 <!--NeedCopy-->
```

Gehen Sie wie folgt vor, um den UITHEME-Parameter mithilfe des Konfigurationsdienstprogramms festzulegen.

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Citrix Gateway > Globale Einstellungen**.
2. Klicken Sie auf **Globale Einstellungen ändern**.
3. Klicken Sie auf den Tab „ **Kundenerlebnis** “.
4. Scrollen Sie zum unteren Bildschirmrand und wählen Sie dann im Listenmenü des **UI-Themas** die Option **CUSTOM**.
5. Klicken Sie auf **OK**.

Ihr manuell angepasstes Portal ist jetzt das Portaldesign, das VPN-Benutzern präsentiert wird.

## Erstellen Sie eine EULA

Das VPN-Portalsystem bietet die Möglichkeit, eine EULA auf eine Portalkonfiguration anzuwenden. Sobald eine EULA an die Citrix Gateway-Konfiguration gebunden ist, entweder im globalen VPN-Bereich oder an einen relevanten virtuellen VPN-Server, müssen VPN-Benutzer der EULA als Allgemeinen Geschäftsbedingungen zustimmen, bevor sie sich beim VPN authentifizieren dürfen.

Wie bei den Portal-Themen wird Benutzern eine sprachspezifische EULA basierend auf dem von ihrem Webbrowser gemeldeten Gebietsschema bereitgestellt. Bei einem Gebietsschema, das keiner der unterstützten Sprachen entspricht, ist die Standardsprache Englisch. Für jede EULA können Sie eine benutzerdefinierte Nachricht in jeder der unterstützten Sprachen eingeben. Vorübersetzte Inhalte werden für EULA-Konfigurationen nicht wie für die Portal-Themen bereitgestellt.Wenn das gemeldete Gebietsschema eines Benutzers mit einer Sprache übereinstimmt, in die kein EULA-Inhalt eingegeben wurde, wird dem Benutzer eine leere Seite zurückgegeben, wenn er auf der VPN-Anmeldeseite auf den Link “Allgemeine Geschäftsbedingungen”klickt.

Um eine EULA zu erstellen, können Sie eines der Steuerelemente im Konfigurationsdienstprogramm auf der Registerkarte **Konfiguration** unter **Citrix Gateway > Globale Einstellungen > EULA** oder **Citrix Gateway > Ressourcen > EULA**verwenden. Die Steuerelemente im Bereich **Globale Einstellungen** werden verwendet, um globale VPN-EULA-Bindungen zu verwalten, während das Steuerelement auf dem Knoten **Ressourcen > EULA** für allgemeine Vorgänge mit EULA-Konfigurationen vorgesehen ist. Sie können VPN-Bindungen für virtuelle Server verwalten, indem Sie einen virtuellen VPN-Server unter **Citrix Gateway > Virtuelle Server**bearbeiten. Einige Befehle sind auch über die Befehlszeile zur Verwaltung von EULA-Entitäten verfügbar. Die vollständigen EULA-Verwaltungssteuerungen sind jedoch nur im Konfigurationsdienstprogramm verfügbar.

### Erstellen einer EULA-Entität über die CLI

Geben Sie an der Eingabeaufforderung;

```
add vpn eula <name>
<!--NeedCopy-->
```

#### Erstellen Sie über die GUI eine EULA-Entität

1. Navigieren Sie zu **Citrix Gateway > Ressourcen > EULA**.
2. Klicken Sie auf **Hinzufügen**, um eine Entität zu erstellen
3. Geben Sie einen Namen für die Entität ein.
4. Fügen Sie für jede der Sprachen den Inhalt unter den entsprechenden Registerkarten ein. Sie können Nur-Text- oder HTML-Tags verwenden, um den Inhalt zu formatieren, einschließlich des Tags <br> zum Hinzufügen von Zeilenumbrüchen.
5. Klicken Sie auf **Erstellen**.

Sobald eine EULA-Entität erstellt wurde, kann sie global an die VPN-Konfiguration gebunden oder an einen virtuellen VPN-Server gebunden sein.

#### Binden Sie eine EULA über die CLI an VPN global

Geben Sie in der Befehlszeile ein;

```
bind vpn global eula <name>
<!--NeedCopy-->
```

#### Binden Sie eine EULA über die GUI an VPN global

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Citrix Gateway > Globale Einstellungen**.
2. Klicken Sie im Hauptdetailbereich auf **Endbenutzer-Lizenzvereinbarung konfigurieren**.
3. Klicken Sie auf **Add binding**.
4. Klicken Sie auf **Klicken, um auszuwählen**.
5. Wählen Sie eine EULA-Entität aus und **klicken Sie**dann auf
6. Klicken Sie auf **Bind**.
7. Klicken Sie auf **Schließen**.

#### Binden Sie eine EULA über die CLI an einen virtuellen VPN-Server

Geben Sie in der Befehlszeile ein;

```
bind vpn vserver <name> eula <name>
<!--NeedCopy-->
```

**Binden Sie eine EULA über die GUI an einen virtuellen VPN-Server**

1. Wechseln Sie auf der Registerkarte **Konfiguration** zu **Citrix Gateway > Virtuelle Server.**
2. Wählen Sie im Hauptdetailbereich einen virtuellen VPN-Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Bereich **Erweiterte Einstellungen** auf der rechten Seite der Seite auf **EULA**.
4. Klicken Sie im neu hinzugefügten EULA-Fenster auf **Keine EULA**.
5. `Click` **Zum Auswählen klicken**.
6. Wählen Sie eine EULA-Entität und klicken Sie auf **Auswählen**
7. Klicken Sie auf **Bind**.
8. Klicken Sie auf **Fertig**.

## Benutzer über eine benutzerdefinierte Seite zum Aktualisieren älterer oder nicht unterstützter Browser auffordern

January 29, 2024

Wenn ein Client mithilfe einer unsicheren Verschlüsselung wie SSLv3 eine Verbindung zu einer NetScaler VIP-Adresse herstellt, kann er auf eine benutzerdefinierte Seite umgeleitet werden, auf der er aufgefordert wird, auf die neueste Version von Internet Explorer, Firefox, Chrome oder Safari zu aktualisieren.

**Hinweis:** Laut RFC6176 der Internet Engineering Task Force (ITEF) dürfen TLS-Server SSLv2 nicht unterstützen. Daher unterstützt die NetScaler-Appliance SSLv2 ab Version 12.1 und höher nicht.

### So erstellen Sie eine benutzerdefinierte Seite, um Benutzer aufzufordern, ältere, nicht unterstützte Browser basierend auf SSL zu aktualisieren

- Erstellen Sie eine NetScaler-Responder-Richtlinie mit der Regel `client.ssl.version.eq()`. Die Version gibt die SSL-Protokollversion zurück.
  - Gibt 0 zurück, wenn die Transaktion nicht SSL-basiert ist.
  - Gibt 0x002 zurück, wenn die Transaktion SSLv2 ist.
  - Gibt 0x300 zurück, wenn die Transaktion SSLv3 ist.
  - Gibt 0x301 zurück, wenn die Transaktion TLSv1 ist.
- Sie müssen SSLv3 (oder eine andere frühere Version) aktivieren, um die Responder Policy auszulösen.

Wenn beispielsweise SSLv3 auf der NetScaler-Appliance deaktiviert ist und ein Client mit einem älteren Browser, der SSLv3 verwendet, versucht, eine Verbindung herzustellen, wird der Zugriff verweigert.

- Wenn für Ihre Bereitstellung SSLv3 oder eine frühere Version für einen bestimmten Zeitraum (ein oder zwei Monate) erforderlich ist, konfigurieren Sie Folgendes:
  - Aktivieren Sie das SSLv3-Protokoll.
  - Aktualisieren Sie die benutzerdefinierte Seite, um Informationen aufzunehmen, dass der Browser nach dem angegebenen Zeitraum keine Verbindung zur Appliance herstellen kann.

## Konfigurieren Sie den clientlosen VPN-Zugriff mit Citrix Gateway

March 27, 2024

Der clientlose Zugriff ermöglicht Benutzern den Zugriff, den sie benötigen, ohne dass sie Benutzersoftware wie das Citrix Gateway Plug-in oder Receiver installieren müssen. Benutzer können ihren Webbrowser verwenden, um eine Verbindung zu Webanwendungen wie Outlook Web Access herzustellen.

Sie verwenden die folgenden Schritte, um den clientlosen Zugriff zu konfigurieren:

- Aktivieren des clientlosen Zugriffs entweder global oder mithilfe einer Sitzungsrichtlinie, die an einen Benutzer, eine Gruppe oder einen virtuellen Server gebunden ist.
- Auswahl der Codierungsmethode für Webadresse.

Um den clientlosen Zugriff nur für einen bestimmten virtuellen Server zu ermöglichen, deaktivieren Sie den clientlosen Zugriff global und erstellen Sie dann eine Sitzungsrichtlinie, um ihn zu aktivieren.

Wenn Sie den Citrix Gateway-Assistenten zum Konfigurieren der Appliance verwenden, haben Sie die Wahl, den clientlosen Zugriff innerhalb des Assistenten zu konfigurieren. Die Einstellungen im Assistenten werden global angewendet. Im Citrix Gateway-Assistenten können Sie die folgenden Clientverbindungsmethoden konfigurieren:

- Citrix Gateway Plug-in. Benutzer dürfen sich nur mit dem Citrix Gateway Plug-in anmelden.
- Verwenden Sie das Citrix Gateway Plug-in und lassen Sie Fallback für Zugriffsszenarien zu. Benutzer melden sich mit dem Citrix Gateway Plug-in bei Citrix Gateway an. Wenn das Benutzergerät einen Endpoint Analysis-Scan nicht besteht, ist es Benutzern gestattet, sich mit clientlosem Zugriff anzumelden. In diesem Fall haben Benutzer eingeschränkten Zugriff auf Netzwerkressourcen.

- Ermöglichen Sie Benutzern, sich über einen Webbrowser und einen clientlosen Zugriff anzumelden. Benutzer können sich nur über den clientlosen Zugriff anmelden und erhalten eingeschränkten Zugriff auf Netzwerkressourcen.

## So funktionieren clientlose VPN-Zugriffsrichtlinien

Sie konfigurieren den clientlosen Zugriff auf Webanwendungen, indem Sie Richtlinien erstellen. Sie können die Einstellungen für eine clientlose Zugriffsrichtlinie im Konfigurationsdienstprogramm konfigurieren. Eine clientlose Zugriffsrichtlinie setzt sich aus einer Regel und einem Profil zusammen. Sie können die vorkonfigurierten clientlosen Zugriffsrichtlinien verwenden, die mit Citrix Gateway geliefert werden. Sie können auch Ihre eigenen benutzerdefinierten clientlosen Zugriffsrichtlinien erstellen.

Citrix Gateway bietet vorkonfigurierte Richtlinien für Folgendes:

- Outlook Web Access und Outlook Web App
- SharePoint 2007
- Alle anderen Webanwendungen

> **Hinweis:**
>
> OWA 2016 und SharePoint 2016 werden nur mit erweitertem clientlosem Zugriff unterstützt.

Beachten Sie die folgenden Merkmale der vorkonfigurierten clientlosen Zugriffsrichtlinien:

- Sie werden automatisch konfiguriert und können nicht geändert werden.
- Jede Richtlinie ist auf globaler Ebene gebunden.
- Jede Richtlinie wird nicht durchgesetzt, es sei denn, Sie aktivieren den clientlosen Zugriff entweder global oder durch Erstellen einer Sitzungsrichtlinie.
- Sie können globale Bindungen nicht entfernen oder ändern, auch wenn Sie keinen clientlosen Zugriff aktivieren.

Die Unterstützung für andere Webanwendungen hängt von den Umschreiberichtlinien ab, die Sie auf Citrix Gateway konfigurieren. Citrix empfiehlt, alle benutzerdefinierten Richtlinien zu testen, die Sie erstellen, um sicherzustellen, dass alle Komponenten der Anwendung erfolgreich neu geschrieben werden.

Wenn Sie Verbindungen von Receiver für Android, Receiver für iOS oder Citrix Secure Hub zulassen, müssen Sie den clientlosen Zugriff aktivieren. Für Citrix Secure Hub, der auf einem iOS-Gerät ausgeführt wird, müssen Sie auch Secure Browse innerhalb des Sitzungsprofils aktivieren. Secure Browse und clientloser Zugriff arbeiten zusammen, um Verbindungen von iOS-Geräten aus zu ermöglichen. Sie müssen Secure Browse nicht aktivieren, wenn Benutzer keine Verbindung zu iOS-Geräten herstellen.

Der Schnellkonfigurationsassistent konfiguriert die richtigen clientlosen Zugriffsrichtlinien und -einstellungen für mobile Geräte. Citrix empfiehlt, den Assistenten für die Schnellkonfiguration auszuführen, um die richtigen Richtlinien für Verbindungen mit StoreFront und Citrix Endpoint Management zu konfigurieren.

Sie können benutzerdefinierte clientlose Zugriffsrichtlinien entweder global oder an einen virtuellen Server binden. Wenn Sie clientlose Zugriffsrichtlinien an einen virtuellen Server binden möchten, müssen Sie eine benutzerdefinierte Richtlinie erstellen und diese dann binden. Um verschiedene Richtlinien für den clientlosen Zugriff entweder global oder für einen virtuellen Server durchzusetzen, ändern Sie die Prioritätsnummer der benutzerdefinierten Richtlinie so, dass sie eine niedrigere Zahl als die vorkonfigurierten Richtlinien hat, wodurch der benutzerdefinierten Richtlinie eine höhere Priorität eingeräumt wird. Wenn keine anderen clientlosen Zugriffsrichtlinien an den virtuellen Server gebunden sind, haben die vorkonfigurierten globalen Richtlinien Vorrang.

> **Hinweis:**
>
> Sie können die Prioritätsnummern der vorkonfigurierten clientlosen Zugriffsrichtlinien nicht ändern.

### Aktivieren Sie den clientlosen VPN-Zugriff

Wenn Sie den clientlosen Zugriff auf globaler Ebene aktivieren, erhalten alle Benutzer die Einstellungen für den clientlosen Zugriff. Sie können den Citrix Gateway-Assistenten, eine globale Richtlinie oder eine Sitzungsrichtlinie verwenden, um den clientlosen Zugriff zu ermöglichen.

In einer globalen Einstellung oder einem Sitzungsprofil hat der clientlose Zugriff die folgenden Einstellungen:

- **Auf**. Ermöglicht den clientlosen Zugriff. Wenn Sie die Clientauswahl deaktivieren und StoreFront nicht konfigurieren oder deaktivieren, melden sich Benutzer mithilfe des clientlosen Zugriffs an.
- **Aus** Der clientlose Zugriff ist standardmäßig nicht aktiviert. Der clientlose Zugriff wird aktiviert, nachdem sich Benutzer mit dem Citrix Gateway Plug-in angemeldet haben. Wenn Sie die Clientauswahl deaktivieren und StoreFront nicht konfigurieren oder deaktivieren, melden sich Benutzer mit dem Citrix Gateway Plug-in an. Wenn die Endpoint Analysis bei der Benutzeranmeldung fehlschlägt, erhalten Benutzer die Auswahlseite mit verfügbarem clientlosem Zugriff.
- **Deaktiviert**. Der clientlose Zugang ist deaktiviert. Wenn Sie **Deaktiviert**auswählen, können sich Benutzer nicht über den clientlosen Zugriff anmelden, und das Symbol für den clientlosen Zugriff wird nicht auf der Auswahlseite angezeigt.

Wenn Sie den clientlosen Zugriff nicht mithilfe des Citrix Gateway-Assistenten aktivieren, können Sie ihn mithilfe des Konfigurationsdienstprogramms global oder in einer Sitzungsrichtlinie aktivieren.

**Um den clientlosen Zugriff global zu ermöglichen**

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Wählen Sie auf der Registerkarte **Client Experience** neben **Clientless Access**die Option EIN aus **,** und klicken Sie dann auf **OK**.

**So aktivieren Sie den clientlosen Zugriff mithilfe einer Sitzungsrichtlinie**

Wenn Sie möchten, dass nur eine ausgewählte Gruppe von Benutzern, Gruppen oder virtuellen Servern clientlosen Zugriff verwendet, deaktivieren oder löschen Sie den clientlosen Zugriff global. Aktivieren Sie dann mithilfe einer Sitzungsrichtlinie den clientlosen Zugriff und binden Sie ihn an Benutzer, Gruppen oder virtuelle Server.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien > Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. **Geben Sie im Feld Name einen Namen für das Profil ein.**
6. Klicken Sie auf der Registerkarte **Client Experience** neben Clientless Access auf **Override Global**, wählen Sie **On** aus, und klicken Sie dann auf **Create**.
7. Wählen **Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben **Benannte Ausdrücke**die Option Allgemein aus, wählen Sie Wahrer Wert aus, klicken Sie auf Ausdruck hinzufügen, klicken Sie auf **Erstellen** und dann auf **Schließen**.
8. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

Nachdem Sie die Sitzungsrichtlinie erstellt haben, die clientlosen Zugriff ermöglicht, binden Sie sie an einen Benutzer, eine Gruppe oder einen virtuellen Server.

## Kodieren Sie die Webadresse

Wenn Sie den clientlosen Zugriff aktivieren, können Sie die Adressen interner Webanwendungen codieren oder die Adresse als Klartext belassen. Die Einstellungen lauten:

- Obskur. Dies verwendet Standardcodierungsmechanismen, um den Domäne- und Protokollteil der Ressource zu verschleiern.
- Klar. Die Webadresse ist nicht codiert und für Benutzer sichtbar.
- Verschlüsseln. Die Domäne und das Protokoll werden mithilfe eines Sitzungsschlüssels verschlüsselt. Wenn die Webadresse verschlüsselt ist, ist die URL für jede Benutzersitzung für

dieselbe Webressource unterschiedlich. Wenn Benutzer die codierte Webadresse mit einem Lesezeichen versehen, sie im Webbrowser speichern und sich dann abmelden. Wenn sich Benutzer anmelden und versuchen, mithilfe des Lesezeichens erneut eine Verbindung zur Webadresse herzustellen, können sie keine Verbindung zur Webadresse herstellen.
Hinweis: Wenn Benutzer das verschlüsselte Lesezeichen während ihrer Sitzung im Access Interface speichern, funktioniert das Lesezeichen jedes Mal, wenn sich der Benutzer anmeldet.

Sie können diese Einstellung entweder global oder als Teil einer Sitzungsrichtlinie konfigurieren. Wenn Sie die Kodierung als Teil einer Sitzungsrichtlinie konfigurieren, können Sie sie an die Benutzer, Gruppen oder einen virtuellen Server binden.

#### Konfigurieren Sie die Codierung von Webadressdaten global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte "Configuration"im Navigationsbereich "Citrix Gateway"und klicken Sie auf "Global Settings".
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Wählen Sie auf der Registerkarte Client Experience neben URL-Kodierung für clientlosen Zugriff die Kodierungsstufe aus, und klicken Sie dann auf OK.

### Konfigurieren der Webadressencodierung durch Erstellen einer Sitzungsrichtlinie

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf Sitzung.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf Neu.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Klicken Sie auf der Registerkarte Client Experience neben Clientless Access URL Encoding auf Override Global, wählen Sie die Codierungsstufe aus, und klicken Sie dann auf OK.
7. Wählen Sie im Dialogfeld Sitzungsrichtlinie erstellen neben Benannte Ausdrücke die Option Allgemein aus, wählen Sie Wahrer Wert aus, klicken Sie auf Ausdruck hinzufügen , klicken Sie auf Erstellen und dann auf Schließen.

### Erstellen Sie clientlose Zugriffsrichtlinien

Wenn Sie dieselben Einstellungen wie für die standardmäßigen clientlosen Zugriffsrichtlinien verwenden möchten, die Richtlinie jedoch an einen virtuellen Server binden möchten, können Sie die Standardrichtlinien kopieren und einen neuen Namen für die Richtlinie angeben. Sie können das Konfigurationsdienstprogramm verwenden, um die Standardrichtlinien zu kopieren.

Nachdem Sie die neue Richtlinie an den virtuellen Server gebunden haben, können Sie die Priorität der Richtlinie so festlegen, dass sie zuerst ausgeführt wird, wenn sich ein Benutzer anmeldet.

#### Erstellen einer clientlosen Zugriffsrichtlinie mithilfe von Standardeinstellungen

1. Erweitern Sie im Konfigurationsprogramm im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf Clientless Access.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf eine Standardrichtlinie und dann auf Hinzufügen.
3. Geben Sie unter Name einen neuen Namen für die Richtlinie ein, klicken Sie auf Erstellen und dann auf Schließen.

### Binden einer clientlosen Zugriffsrichtlinie an einen virtuellen Server

Nachdem Sie die Richtlinie erstellt haben, binden Sie sie an den virtuellen Server.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf Virtuelle Server.
2. Wählen Sie im Detailbereich einen virtuellen Server aus und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld Citrix Gateway Virtual Server konfigurieren auf die Registerkarte Richtlinien, und klicken Sie dann auf Clientlos.
4. Klicken Sie auf Richtlinie einfügen, wählen Sie eine Richtlinie aus der Liste aus, und klicken Sie dann auf OK.

#### Erstellen und Auswerten von Ausdrücken für clientlose Zugriffsrichtlinien

Wenn Sie eine Richtlinie für den clientlosen Zugriff erstellen, können Sie Ihren eigenen Ausdruck für die Richtlinie erstellen. Wenn Sie mit dem Erstellen des Ausdrucks fertig sind, können Sie den Ausdruck auf Genauigkeit prüfen.

1. Erweitern Sie im Konfigurationsprogramm im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf Clientless Access.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf eine Standardrichtlinie und dann auf Hinzufügen.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil auf Neu.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Konfigurieren Sie die Einstellungen für das Umschreiben und klicken Sie dann auf Erstellen.
7. Klicken Sie im Dialogfeld Clientlose Zugriffsrichtlinie erstellen unter Ausdruck auf Hinzufügen.
8. Erstellen Sie im Dialogfeld Ausdruck hinzufügen den Ausdruck, und klicken Sie dann auf OK.

9. Klicken Sie im Dialogfeld Clientlose Zugriffsrichtlinie erstellen auf Evaluieren, und wenn der Ausdruck als korrekt getestet wurde, klicken Sie auf Erstellen.

## Erweiterter clientloser VPN-Zugriff mit Citrix Gateway

March 27, 2024

Clientless VPN sieht eine Möglichkeit, Fernzugriff auf die Intranetressourcen des Unternehmens über Citrix Gateway ohne eine VPN-Clientanwendung auf dem Clientcomputer bereitzustellen. Clientless VPN bietet Remotezugriff auf Unternehmens-Webanwendungen, Portale und andere Ressourcen über einen Webbrowser am Ende des Kunden.
Die fortschrittliche clientlose VPN-Lösung beseitigt die folgenden Einschränkungen in Bezug auf clientloses VPN:

- Relative URLs können manchmal nicht identifiziert werden.
- Dynamisch generierte relative URLs können nicht identifiziert werden.

Das fortschrittliche clientlose VPN identifiziert die absolute URL und die Hostnamen und schreibt sie auf neue und einzigartige Weise um, anstatt zu versuchen, relative URLs auf den HTTP-Antworten/Webseiten neu zu schreiben. SharePoint muss den Standardordner nicht mehr zum Umschreiben von URLs verwenden, und ein benutzerdefinierter SharePoint-Zugriff wird unterstützt.

### Voraussetzungen

Im Folgenden sind die Voraussetzungen für die Konfiguration des erweiterten clientlosen VPN aufgeführt.

- **Wildcard-Serverzertifikat** —Das erweiterte clientlose VPN schreibt URLs auf einzigartige Weise um. Diese Eindeutigkeit wird für jede URL pro Benutzer beibehalten. Wenn beispielsweise die Webanwendung auf `https://webapp.customer.com`gehostet wird und der virtuelle VPN-Server gehostet wird `https://vpn.customer.com`, schreibt das erweiterte clientlose VPN sie als neu `https://cvpneqwerty.vpn.customer.com`. Das bedeutet, dass jede URL als Subdomain des virtuellen VPN-Servers umgeschrieben wird. In dieser neuen URL kann `cvpneqwerty` wieder zu `https://webapp.customer.com` entschlüsselt werden. Die Zeichenfolge `cvpneqwerty` ist dynamisch und daher müssen Sie für SSL den virtuellen VPN-Server mit einem Platzhalterzertifikat binden.

  Wenn der Server mit gehostet wird `https://vpn.customer.com`, muss das Serverzertifikat nun Einträge für (vpn.customer.com und.vpn.customer.com) als Teil der Zertifikate CN oder

SAN (wobei CN = allgemeiner Name, SAN = Subject Alternative Name) haben. Das Binden dieses Zertifikats bleibt auf Citrix Gateway gleich.
**Hinweis:** Platzhalterzertifikate unterstützen nur eine Ebene (d. *h.*.customer.com ist nicht erlaubt). Wenn Sie bereits ein Wildcard-Zertifikat (für*.customer.com) und Hosting verwenden `https://vpn.customer.com`, funktioniert dies nicht für das erweiterte clientlose VPN. Sie müssen ein neues Zertifikat mit bekommen `*.vpn.customer.com`.

- **WildCard-DNS-Eintrag** - Die Clients (Webbrowser) müssen den FQDN der erweiterten clientlosen VPN-App auflösen. Beim Einrichten des Citrix Gateway-Servers müssen Sie einen DNS-Eintrag konfiguriert haben, um vpn.customer.com aufzulösen. Auf diese Weise kann der Browser vpn.customer.com auf die IP-Adresse Ihres virtuellen VPN-Servers auflösen. Um URLs wie `https://cvpnqwerty.vpn.customer.com` dieselbe IP-Adresse aufzulösen (VPN virtueller Server), müssen Sie einen neuen Datensatz für die Domäne von `vpn.customer.com` hinzufügen. Finden Sie die Domain-Einstellung auf Ihrem DNS-Server und fügen Sie einen neuen Host-Eintrag für "*"mit derselben IP-Adresse wie zuvor hinzu. Nachdem Sie den Host-Datensatz hinzugefügt haben, müssen Sie erfolgreiche Ping-Antworten für sehen `https://cpvnanything.vpn.customer.com`.

### Konfigurieren des erweiterten clientlosen VPN-Zugriffs

**Um den erweiterten clientlosen VPN-Zugriff über die Befehlszeilenschnittstelle zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:**

```
set vpn parameter -clientlessVpnMode ON
set vpn parameter -advancedClientlessVpnMode ENABLED
<!--NeedCopy-->
```

Wenn eine Sitzungsaktion an den virtuellen Server gebunden ist, müssen Sie auch die erweiterte clientlose VPN-Modusoption für diese Sitzungsaktion aktivieren.

**Beispiel:**

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
<!--NeedCopy-->
```

**So konfigurieren Sie erweiterten clientlosen VPN-Zugriff mithilfe der Citrix ADC GUI:**

1. Navigieren Sie in der NetScaler GUI zu **Configuration> Citrix NetScaler> Globale Einstellungen.**
2. Klicken Sie auf der **Seite Globale Einstellungen**auf **Globale Einstellungen ändern**, und wählen Sie dann die Registerkarte **Clienterfahrung**aus.
3. Klicken Sie auf der Registerkarte **Client Experience** in der Liste **Clientless Accessauf An**.

4. Klicken Sie auf der Registerkarte **Client Experience** in der Liste **Erweiterter clientloser VPN-Modus** auf **Aktiviert**.
   Wenn Sie **STRICT** aus der Liste **Erweiterter clientloser VPN-Modus** auswählen, reagiert die Citrix ADC Appliance nur auf StoreFront-URLs in klassischer clientloser VPN-Form und blockiert alle anderen klassischen clientlosen VPN-Anfragen. Diese Option bietet eine sicherere Konfiguration auf der Appliance für die Bereitstellung interner Webressourcen.

> **Hinweis:**
>
> - Wenn eine Sitzungsaktion an den virtuellen Server gebunden ist, müssen Sie die Option **Erweiterter clientloser VPN-Modus** für diese Sitzungsaktion auch auf der Registerkarte **Clienterfahrung** auf der Seite **Citrix Gateway-Sitzungsprofil konfigurieren** aktivieren.
> - Sie können die Option **Global überschreiben** auswählen, um die globalen Einstellungen zu überschreiben.
> - Sie können die erweiterte clientlose VPN-Funktion auch auf Sitzungsebene konfigurieren.

### Vorbehalte

Das fortschrittliche clientlose VPN zielt darauf ab, Zugriff auf Enterprise Web Apps zu ermöglichen. Solche Apps haben nur einen FQDN für jede Art von Ressource, die sie benötigen (JavaScript, CSS, Bilder usw.). Da wir den kompletten FQDN interner Apps in ein einziges Oktett (clientloses VPN) codieren, verlieren wir die Subdomain-Beziehung. Wenn eine Enterprise WebApp mit CORS konfiguriert ist, kann es daher manchmal zu Problemen kommen, wenn Sie über das erweiterte clientlose VPN darauf zugreifen.

## Domänenzugriff für Benutzer konfigurieren

March 27, 2024

Wenn Benutzer mithilfe des clientlosen Zugriffs eine Verbindung herstellen, können Sie die Netzwerkressourcen, Domänen und Websites einschränken, auf die Benutzer zugreifen dürfen. Sie können den Citrix Gateway-Assistenten oder globale Einstellungen verwenden, um Listen zum Ein- oder Ausschließen des Zugriffs auf Domänen zu erstellen.

Sie können den Zugriff auf alle Netzwerkressourcen, Domänen und Websites zulassen und dann eine Ausschlussliste erstellen. Die Ausschlussliste nennt einen bestimmten Satz von Ressourcen, auf die Benutzer nicht zugreifen dürfen. Benutzer können nicht auf Domains zugreifen, die in der Ausschlussliste enthalten sind.

Sie können auch den Zugriff auf alle Netzwerkressourcen, Domänen und Websites verweigern und dann eine bestimmte Aufschlussliste erstellen. Die Aufnahmeliste nennt die Ressourcen, auf die Benutzer zugreifen können. Benutzer können nicht auf Domains zugreifen, die nicht in der Liste aufgeführt sind.

Hinweis: Wenn Sie clientlose Zugriffsrichtlinien für Citrix Endpoint Management oder StoreFront konfigurieren und Benutzer eine Verbindung mit Receiver for Web herstellen, müssen Sie die Domänen zulassen, auf die Receiver für Web zugreifen kann. Dies ist erforderlich, damit Citrix Gateway den Netzwerkverkehr für StoreFront und Endpoint Management umschreiben kann.

### Konfigurieren des Domänenzugriffs mithilfe des Citrix Gateway-Assistenten

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf Citrix Gateway.
2. Klicken Sie im Detailbereich unter Erste Schritte auf Citrix Gateway-Assistent.
3. Klicken Sie auf Weiter und folgen Sie dann den Anweisungen im Assistenten, bis Sie die Seite Clientlosen Zugriff konfigurieren erreichen.
4. Klicken Sie auf Domains für clientlosen Zugriff konfigurieren und führen Sie einen der folgenden Schritte aus:

    - Um eine Liste der ausgeschlossenen Domains zu erstellen, klicken Sie auf Domains ausschließen.
    - Um eine Liste der enthaltenen Domains zu erstellen, klicken Sie auf Domains zulassen.

5. Geben Sie unter Domainnamen den Domainnamen ein und klicken Sie dann auf Hinzufügen.
6. Wiederholen Sie Schritt 5 für jede Domäne, die Sie zur Liste hinzufügen möchten, und klicken Sie dann auf OK, wenn Sie fertig sind.
7. Konfigurieren Sie das Gerät mithilfe des Citrix Gateway-Assistenten weiter.

### So konfigurieren Sie Domäneneinstellungen mithilfe des Konfigurationsdienstprogramms

Sie können die Domänenliste auch mithilfe globaler Einstellungen im Konfigurationsdienstprogramm erstellen oder ändern.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Clientless Access auf Domains für clientlosen Zugriff konfigurieren.
3. Führen Sie einen der folgenden Schritte aus:

- Um eine Liste der ausgeschlossenen Domains zu erstellen, klicken Sie auf Domains ausschließen.
- Um eine Liste der enthaltenen Domains zu erstellen, klicken Sie auf Domains zulassen.

4. Geben Sie unter Domainnamen den Domainnamen ein und klicken Sie dann auf Hinzufügen.
5. Wiederholen Sie Schritt 4 für jede Domäne, die Sie zur Liste hinzufügen möchten, und klicken Sie dann auf OK, wenn Sie fertig sind.

## Clientloser VPN-Zugriff für SharePoint 2003, SharePoint 2007 und SharePoint 2013

March 27, 2024

Citrix Gateway kann Inhalte von einer oder mehreren SharePoint 2003- oder SharePoint 2007- oder SharePoint 2013-Websites umschreiben, sodass der Inhalt Benutzern zur Verfügung steht, ohne dass das Citrix Gateway-Plug-in erforderlich ist. Damit der Umschreibvorgang erfolgreich abgeschlossen werden kann, müssen Sie Citrix Gateway mit dem Hostnamen für jeden SharePoint-Server in Ihrem Netzwerk konfigurieren.

Sie können den Citrix Gateway-Assistenten oder das Konfigurationsdienstprogramm verwenden, um den Hostnamen für SharePoint-Websites zu konfigurieren.

Navigieren Sie im Citrix Gateway-Assistenten durch den Assistenten, um Ihre Einstellungen zu konfigurieren. Wenn Sie zur Seite Clientlosen Zugriff konfigurieren gelangen, geben Sie die Webadresse für die SharePoint-Website ein und klicken Sie dann auf **Hinzufügen**.

Um weitere Websites hinzuzufügen oder SharePoint zum ersten Mal nach dem Ausführen des Citrix Gateway-Assistenten zu konfigurieren, verwenden Sie das Konfigurationsdienstprogramm.

> **Wichtig:**
>
> Classic Clientless Access unterstützt Versionen bis SharePoint 2013 und OWA 2013. Advanced Clientless Access unterstützt SharePoint 2016 und OWA 2016 sowie spätere Versionen.

### Konfigurieren Sie den clientlosen Zugriff für SharePoint mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **Citrix Gateway** > **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter Clientless Access auf **Clientlosen Zugriff für SharePoint konfigurieren**.
3. Geben Sie unter Clientloser Zugriff für SharePoint unter Hostname des SharePoint-Servers den Hostnamen für die SharePoint-Website ein, und klicken Sie dann auf **Hinzufügen**.

4. Wiederholen Sie Schritt 3 für jede SharePoint-Website, die Sie der Liste hinzufügen möchten, und klicken Sie dann auf **OK**, wenn Sie fertig sind.

## Festlegen einer SharePoint-Website als Homepage

Wenn Sie eine SharePoint-Website als Homepage der Benutzer festlegen möchten, konfigurieren Sie ein Sitzungsprofil und geben Sie den Hostnamen der SharePoint-Website ein.

### So konfigurieren Sie eine SharePoint-Website als Homepage

1. Navigieren Sie zu **Citrix Gateway > Richtlinien,** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Klicken Sie auf der Registerkarte Clienterfahrung neben Homepage auf **Global überschreiben,** und geben Sie dann den Namen der SharePoint-Website ein.
7. Klicken Sie neben Clientless Access auf **Global überschreiben**, wählen Sie Ein aus **,** und klicken Sie dann auf **Erstellen**.
8. Wählen Sie im Dialogfeld Sitzungsrichtlinie erstellen neben Benannte Ausdrücke **die Option Allgemein**aus, wählen Sie **Wahrer Wert**aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

Binden Sie die Sitzungsrichtlinie nach Abschluss an Benutzer, Gruppen, virtuelle Server oder global. Wenn sich Benutzer anmelden, sehen sie die SharePoint-Website als ihre Homepage.

## Aktivieren der Namensauflösung für SharePoint 2007-Server

SharePoint 2007-Server senden den konfigurierten Servernamen als Hostnamen innerhalb verschiedener URLs als Teil der Antwort. Wenn ein konfigurierter SharePoint-Servername nicht der vollqualifizierte Domänenname (FQDN) ist, kann Citrix Gateway die IP-Adresse nicht mithilfe des SharePoint-Servernamens auflösen, und einige Benutzerfunktionen haben eine Zeitüberschreitung mit der Fehlermeldung "HTTP: 1.1 Gateway-Timeout". Diese Funktionen können das Einchecken und Auschecken von Dateien, das Anzeigen des Workspace und das Hochladen mehrerer Dateien umfassen, wenn Benutzer mit clientlosem Zugriff angemeldet sind.

Um dieses Problem zu beheben, können Sie eine der folgenden Möglichkeiten versuchen:

- Konfigurieren Sie ein DNS-Suffix auf Citrix Gateway, damit der SharePoint-Hostname vor der Namensauflösung in einen FQDN konvertiert wird.

- Konfigurieren Sie einen lokalen DNS-Eintrag auf Citrix Gateway für jeden SharePoint-Servernamen.
- Ändern Sie alle SharePoint-Servernamen, um den FQDN zu verwenden, z. B. SharePoint.IntranetDomain anstelle von SharePoint,

### DNS-Suffix konfigurieren

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **DNS** und klicken Sie dann auf **DNS-Suffix**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie unter **DNS-Suffix**den Intranet-Domänennamen als Suffix ein, klicken Sie auf **Erstellen**und dann auf **Schließen**.

Sie können Schritt 3 für jede Domain wiederholen, die Sie hinzufügen möchten.

#### So konfigurieren Sie einen lokalen DNS-Datensatz für jeden SharePoint-Servernamen auf Citrix Gateway

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich **DNS > Datensätze**, und klicken Sie dann auf **Adressdatensätze**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im **Feld Hostname**den SharePoint-Hostnamen für den DNS-Adressdatensatz ein.
4. Geben Sie unter **IP-Adresse**die IP-Adresse des SharePoint-Servers ein, klicken Sie auf **Hinzufügen**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

Der Hostname, für den ein A-Record hinzugefügt wird, darf keinen CNAME-Datensatz enthalten. Außerdem können keine doppelten A-Datensätze auf der Appliance vorhanden sein.

## Aktivieren Sie den clientlosen VPN-Zugriff dauerhafte Cookies

March 27, 2024

Dauerhafte Cookies sind erforderlich, um auf bestimmte Funktionen von SharePoint zuzugreifen, z. B. das Öffnen und Bearbeiten von Microsoft Word-, Excel- und PowerPoint-Dokumenten, die auf dem SharePoint-Server gehostet werden.

Ein dauerhaftes Cookie verbleibt auf dem Benutzergerät und wird mit jeder HTTP-Anforderung gesendet. Citrix Gateway verschlüsselt das dauerhafte Cookie, bevor es an das Plug-in auf dem Benutzergerät gesendet wird, und aktualisiert das Cookie regelmäßig, solange die Sitzung besteht. Das Cookie wird abgestanden, wenn die Sitzung endet.

Im Citrix Gateway-Assistenten können Administratoren dauerhafte Cookies global aktivieren. Sie können auch eine Sitzungsrichtlinie erstellen, um dauerhafte Cookies pro Benutzer, Gruppe oder virtuellem Server zu aktivieren.

Die folgenden Optionen sind für dauerhafte Cookies verfügbar:

- Zulassen ermöglicht dauerhafte Cookies und Benutzer können in SharePoint gespeicherte Microsoft-Dokumente öffnen und bearbeiten.
- Deny deaktiviert dauerhafte Cookies und Benutzer können in SharePoint gespeicherte Microsoft-Dokumente nicht öffnen und bearbeiten.
- Aufforderung fordert Benutzer auf, dauerhafte Cookies während der Sitzung zuzulassen oder abzulehnen.

Permanente Cookies sind für den clientlosen Zugriff nicht erforderlich, wenn Benutzer keine Verbindung zu SharePoint herstellen.

## Konfigurieren Sie dauerhafte Cookies für den clientlosen VPN-Zugriff für SharePoint

Sie können dauerhafte Cookies für den clientlosen Zugriff auf SharePoint entweder global oder als Teil einer Sitzungsrichtlinie konfigurieren.

### So konfigurieren Sie dauerhafte Cookies global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Wählen Sie auf der Registerkarte Clienterlebnis neben Persistente Cookies für den clientlosen Zugriff eine Option aus und klicken Sie dann auf OK.

### So konfigurieren Sie dauerhafte Cookies als Teil einer Sitzungsrichtlinie

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf Sitzung.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf Neu.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Klicken Sie auf der Registerkarte Client Experience neben Persistente Cookies für den clientlosen Zugriff auf Global überschreiben, wählen Sie eine Option aus, und klicken Sie dann auf Erstellen.

7. Wählen Sie im Dialogfeld Authentifizierungsrichtlinie erstellen neben Benannte Ausdrücke die Option Allgemein aus, wählen Sie den Wert True aus, klicken Sie auf Ausdruck hinzufügen, klicken Sie auf Erstellen und dann auf Schließen.

## Benutzereinstellungen für clientlosen Zugriff über das Webinterface speichern

March 27, 2024

Wenn sich Benutzer mithilfe des clientlosen Zugriffs am Webinterface anmelden und abmelden, leitet Citrix Gateway den vom Client verbrauchten Cookie-Satz aus der vorherigen Sitzung nicht weiter, selbst wenn die Cookies dauerhaft sind, wenn sich Benutzer mehrmals anmelden. Sie können die GUI oder die CLI verwenden, um Cookies an einen Mustersatz von Client-Cookies zu binden, um die Einstellungen des Webinterface zwischen den Sitzungen beizubehalten.

### So binden Sie Cookies für die Persistenz des Webinterface mithilfe des Konfigurationsdienstprogramms

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien**, und klicken Sie dann auf **Clientloser Zugriff**.
2. Klicken Sie im rechten Bereich auf der Registerkarte Richtlinien auf **Hinzufügen**.
3. Geben Sie im Dialogfeld Clientlose Zugriffsrichtlinie erstellen in das Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil auf **Neu**.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Wählen Sie auf der Registerkarte Client-Cookies unter Client-Cookies **ns_cvpn_default_client_cookies** aus und klicken Sie dann auf **Ändern**.
7. Geben Sie im Dialogfeld Mustersatz konfigurieren unter Muster angeben unter Muster die folgenden Parameter ein:

    - `WIUser` und klicken Sie dann auf **Hinzufügen**.
    - `WINGDevice` und klicken Sie dann auf **Hinzufügen**.
    - `WINGSession` und klicken Sie dann auf **Hinzufügen**.

8. Klicken Sie auf **OK** und dann auf **Erstellen**.
9. Geben Sie im Dialogfeld Clientlose Zugriffsrichtlinie erstellen unter Ausdruck den Wert true ein, klicken Sie auf **Erstellen** und dann auf **Schließen**.

### So binden Sie Cookies für die Persistenz des Webinterface mithilfe der Befehlszeile

1. Melden Sie sich mit einer Secure Shell (SSH) -Verbindung wie PuTTY an der Citrix Gateway-Befehlszeile an.
2. Geben Sie an der Eingabeaufforderung shell ein.
3. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
bind policy patset ns_cvpn_default_client_cookies WIUser
bind policy patset ns_cvpn_default_client_cookies WINGDevice
bind policy patset ns_cvpn_default_client_cookies WINGSession
<!--NeedCopy-->
```

4. Drücken Sie die **Eingabetaste**.

## Citrix SSO VPN-Client für mobile Geräte

March 27, 2024

Citrix SSO ist der VPN-Client für mobile Geräte (macOS, iOS und iOS). Citrix SSO bietet vollständige Unterstützung für Mobile Device Management (MDM) für macOS, iOS und Android. Mit einem MDM-Server kann ein Administrator VPN-Profile auf Geräteebene und Pro-App-VPN-Profile remote konfigurieren und verwalten.
Citrix SSO unterstützt auch die meisten der am häufigsten verwendeten Funktionen.

### Referenzen

- Citrix Gateway-Clients
- Citrix Gateway VPN-Clients und unterstützte Funktionen

## Seite “Clientauswahl”konfigurieren

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass Benutzern mehrere Anmeldeoptionen zur Verfügung gestellt werden. Durch die Konfiguration der Clientauswahlseite haben Benutzer die Möglichkeit, sich von einem Standort aus mit den folgenden Optionen anzumelden:

- Citrix Gateway Plug-in für Windows

- Citrix Gateway Plug-in für macOS X
- Citrix Gateway Plug-in für Java
- StoreFront
- Webinterface
- Clientloser Zugriff

Benutzer melden sich bei Citrix Gateway an, indem sie die Webadresse im an Citrix Gateway oder den virtuellen Server gebundenen Zertifikat verwenden. Durch Erstellen einer Sitzungsrichtlinie und eines Profils können Sie die Anmeldeoptionen festlegen, die Benutzer erhalten. Je nachdem, wie Sie Citrix Gateway konfigurieren, werden auf der Seite Clientoptionen bis zu drei Symbole angezeigt, die die folgenden Anmeldeoptionen darstellen:

- Netzwerkzugriff. Wenn sich Benutzer zum ersten Mal mit einem Webbrowser bei Citrix Gateway anmelden und dann Netzwerkzugriff auswählen, wird die Downloadseite angezeigt. Wenn Benutzer auf Herunterladen klicken, wird das Plug-In auf das Benutzergerät heruntergeladen und installiert. Wenn der Download und die Installation abgeschlossen sind, wird das Access Interface angezeigt. Wenn Sie eine neuere Version installieren oder zu einer älteren Version von Citrix Gateway zurückkehren, aktualisiert oder heruntergestuft das Citrix Gateway-Plug-in für Windows auf die Version auf der Appliance. Wenn Benutzer mithilfe des Citrix Gateway-Plug-ins für Mac eine Verbindung herstellen, wird das Plug-in stillschweigend aktualisiert, wenn bei der Benutzeranmeldung eine neue Appliance-Version erkannt wird. Diese Version des Plug-Ins wird nicht lautlos heruntergestuft.
- Webinterface oder StoreFront. Wenn Benutzer das Webinterface für die Anmeldung auswählen, wird die Seite Webinterface angezeigt. Benutzer können dann auf ihre veröffentlichten Anwendungen oder virtuellen Desktops zugreifen. Wenn Benutzer StoreFront für die Anmeldung auswählen, wird Receiver geöffnet, und Benutzer können auf Anwendungen und Desktops zugreifen.
  Hinweis: Wenn Sie StoreFront als Clientauswahl konfigurieren, werden Anwendungen und Desktops nicht im linken Bereich des Access Interface angezeigt.
- Clientloser Zugriff: Wenn Benutzer clientlosen Zugriff für die Anmeldung auswählen, wird das Access Interface oder Ihre angepasste Homepage angezeigt. Im Access Interface können Benutzer zu Dateifreigaben und Websites navigieren und Outlook Web Access verwenden.

Wenn Benutzer das **Citrix Gateway-Plug-In** für Java auswählen, wird das Plug-In gestartet und Benutzer werden angemeldet. Die Auswahlseite wird nicht angezeigt.

Mit Secure Browse können Benutzer von einem iOS-Gerät aus eine Verbindung über Citrix Gateway herstellen. Wenn Sie Secure Browse aktivieren und sich Benutzer mithilfe von Secure Hub anmelden, deaktiviert Secure Browse die Clientauswahlseite.

## Zeigen Sie die Seite Clientauswahl bei der Anmeldung an

Wenn Sie die Option Clientauswahl aktivieren, können sich Benutzer nach erfolgreicher Authentifizierung bei Citrix Gateway mit dem Citrix Gateway Plug-in, dem Webinterface, Receiver oder dem clientlosen Zugriff von einer Webseite aus anmelden. Wenn die Anmeldung erfolgreich ist, werden auf der Webseite Symbole angezeigt, von denen aus Benutzer die Methode zum Herstellen einer Verbindung auswählen können. Sie können das Citrix Gateway Plug-in für Java auch so konfigurieren, dass es auf der Auswahlseite angezeigt wird.

Sie können Clientauswahl aktivieren, ohne Endpoint Analysis zu verwenden oder Fallback für Zugriffsszenarien zu implementieren. Wenn Sie keinen Clientsicherheitsausdruck definieren, erhalten Benutzer Verbindungsoptionen für die Einstellungen, die auf Citrix Gateway konfiguriert sind. Wenn ein Client-Sicherheitsausdruck für die Benutzersitzung vorhanden ist und das Benutzergerät den Endpoint Analysis-Scan nicht besteht, bietet die Auswahlseite nur die Option, das Webinterface zu verwenden, wenn es konfiguriert ist. Andernfalls können Benutzer den clientlosen Zugriff verwenden, um sich anzumelden.

Sie konfigurieren Clientoptionen entweder global oder mithilfe eines Sitzungsprofils und einer Richtlinie.

> **Wichtig:**
>
> Konfigurieren Sie beim Konfigurieren von Clientoptionen keine Quarantänegruppen. Benutzergeräte, die den Endpoint Analysis-Scan nicht bestehen und unter Quarantäne gestellt und genauso behandelt werden wie Benutzergeräte, die den Endpunkt-Scan bestehen.

### Aktivieren Sie Optionen für Clientauswahl global

1. Erweitern Sie in der GUI auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway**, und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter Einstellungen auf **Globale Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte “Kundenerlebnis”auf **Erweiterte Einstellungen**.
4. Klicken Sie auf der Registerkarte Allgemein auf **Clientauswahl** und dann auf **OK**.

### Aktivieren von Clientoptionen als Teil einer Sitzungsrichtlinie

Sie können Clientoptionen auch als Teil einer Sitzungsrichtlinie konfigurieren und dann an Benutzer, Gruppen und virtuelle Server binden.

1. Erweitern Sie in der GUI auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien,** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Hinzufügen**.

3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf **Neu**.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Klicken Sie auf der Registerkarte „Kundenerlebnis“auf „ **Erweitert**“.
7. Klicken Sie auf der Registerkarte Allgemein neben Clientauswahl auf **Global überschreiben**, klicken Sie auf **Clientauswahl**, klicken Sie auf **OK**und dann auf **Erstellen**.
8. Wählen Sie im Dialogfeld Sitzungsrichtlinie erstellen neben Benannte Ausdrücke **die Option Allgemein**aus, wählen Sie **Wahrer Wert**aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

## Konfigurieren von Clientoptionen

Zusätzlich zur Aktivierung von Clientoptionen mithilfe eines Sitzungsprofils und einer Richtlinie müssen Sie die Einstellungen für die Benutzersoftware konfigurieren. Sie möchten beispielsweise, dass sich Benutzer entweder mit dem Citrix Gateway Plug-in, StoreFront oder dem Webinterface oder mit clientlosem Zugriff anmelden. Sie erstellen ein Sitzungsprofil, das alle drei Optionen und Clientoptionen ermöglicht. Anschließend erstellen Sie eine Sitzungsrichtlinie mit dem Ausdruck, der mit dem angehängten Profil auf True festgelegt ist. Als Nächstes binden Sie die Sitzungsrichtlinie an einen virtuellen Server.

Bevor Sie die Sitzungsrichtlinie und das Sitzungsprofil erstellen, müssen Sie eine Berechtigungsgruppe für Benutzer erstellen.

### Erstellen einer Berechtigungsgruppe

1. Klicken Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Gruppen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie **unter Gruppenname**den Namen der Gruppe ein.
4. Wählen Sie auf der Registerkarte **Benutzer** die Benutzer aus, klicken Sie für jeden Benutzer auf **Hinzufügen**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

Das folgende Verfahren ist ein Beispielsitzungsprofil für Clientoptionen mit dem Citrix Gateway Plug-In, StoreFront und clientlosem Zugriff.

## Erstellen Sie ein Sitzungsprofil für Clientauswahl

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien > Sitzung**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Profile** und dann auf **Hinzufügen**.

3. **Geben Sie im Feld Name einen Namen für das Profil ein.**
4. Gehen Sie auf der Registerkarte **Client Experience** wie folgt vor:

    a) Klicken Sie neben Startseite auf **Override Global** und deaktivieren Sie dann die **Option Startseite anzeigen**. Dadurch wird das Access Interface deaktiviert.
    b) Klicken Sie neben **Clientless Access**auf **Override Global**und wählen Sie dann **AUS**.
    c) Klicken Sie neben **Plug-In-Typ**auf **Override Global**und wählen Sie dann Windows/Mac OS X aus.
    d) Klicken Sie auf **Erweiterte Einstellungen** und klicken Sie neben **Clientauswahl**auf **Global überschreiben**und dann auf **Clientauswahl**.

5. Klicken Sie auf der Registerkarte **Sicherheit** neben **Standardautorisierungsaktion**auf **Override Global** und wählen Sie dann ALLOW **aus**.
6. Klicken Sie auf der Registerkarte **Sicherheit** auf **Erweiterte Einstellungen**.
7. Klicken Sie unter **Autorisierungsgruppen**auf **Override Global**, klicken Sie auf **Hinzufügen**, und wählen Sie dann die Gruppe aus.
8. Gehen Sie auf der Registerkarte **Veröffentlichte Anwendungen** wie folgt vor:

    a) Klicken Sie neben **ICA-Proxy**auf **Override Global**, und wählen Sie dann **AUS**.
    b) Klicken Sie neben **Webinterface-Adresse**auf **Override Global**, und geben Sie dann die Webadresse von StoreFront ein, z. B. http://ipAddress/Citrix/
    c) Klicken Sie neben **Webinterface Portal Mode**auf **Override Global** und wählen Sie dann **COMPACT**aus.
    d) Klicken Sie neben **Single Sign-On-Domain**auf **Override Global**und geben Sie dann den Namen der Domain ein.

9. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Wenn Sie das Citrix Gateway-Plug-In für Java als Clientauswahl verwenden möchten, wählen Sie auf der Registerkarte **Client Experience** unter Plug-in-Typ die Option **Java**aus. Wenn Sie diese Option wählen, müssen Sie eine Intranet-Anwendung konfigurieren und den Abfangmodus auf Proxy einstellen.

Erstellen Sie nach dem Erstellen des Sitzungsprofils eine Sitzungsrichtlinie. Wählen Sie innerhalb der Richtlinie das Profil aus und setzen Sie den Ausdruck auf True.

Um StoreFront als Clientauswahl zu verwenden, müssen Sie auch die Secure Ticket Authority (STA) auf dem Citrix Gateway konfigurieren. Die STA ist an den virtuellen Server gebunden.

> **Hinweis:**
>
> Wenn der Server, auf dem StoreFront ausgeführt wird, nicht verfügbar ist, wird die Auswahl Citrix Virtual Apps nicht auf der Auswahlseite angezeigt.

**Konfigurieren Sie den STA-Server global**

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway**, und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter Server auf **STA-Server binden/unbind**, die von der Secure Ticket Authority verwendet werden sollen.
3. Klicken Sie im Dialogfeld **STA-Server binden/aufheben** auf **Hinzufügen**.
4. Geben **Sie im Dialogfeld STA-Server konfigurieren** unter URL die Webadresse des STA-Servers ein, und klicken Sie dann auf **Create**.
5. Wiederholen Sie die Schritte 3 und 4, um weitere STA-Server hinzuzufügen, und klicken Sie dann auf **OK**.

**Binden Sie die STA an einen virtuellen Server**

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Wählen Sie auf der Registerkarte **Published Applications** unter **Secure Ticket Authority**unter **Aktiv**die STA-Server aus, und klicken Sie dann auf **OK**.

Sie können auch STA-Server auf der Registerkarte **Published Applications** hinzufügen.

## Konfigurieren des Zugriffsszenario-Fallbacks

March 27, 2024

Mit SmartAccess kann Citrix Gateway basierend auf den Ergebnissen eines Endpoint Analysis-Scans automatisch die Zugriffsmethoden ermitteln, die für ein Benutzergerät zulässig sind. Das Fallback des Zugriffsszenarios erweitert diese Funktion weiter, indem es einem Benutzergerät ermöglicht, mithilfe der Citrix Workspace-App vom Citrix Gateway Plug-In auf das Webinterface oder StoreFront zurückzugreifen, wenn das Benutzergerät den ersten Endpoint Analysis-Scan nicht durchläuft.

Um Fallback für Zugriffsszenarien zu aktivieren, konfigurieren Sie eine Richtlinie nach der Authentifizierung, die festlegt, ob Benutzer bei der Anmeldung bei Citrix Gateway eine alternative Zugriffsmethode erhalten. Diese Richtlinie nach der Authentifizierung ist als Client-Sicherheitsausdruck definiert, den Sie entweder global oder als Teil eines Sitzungsprofils konfigurieren. Wenn Sie ein Sitzungsprofil konfigurieren, wird das Profil einer Sitzungsrichtlinie zugeordnet, die Sie dann an Benutzer, Gruppen oder virtuelle Server binden. Wenn Sie Fallback für Zugriffsszenarien aktivieren,

initiiert Citrix Gateway nach der Benutzerauthentifizierung einen Endpoint Analysis-Scan. Die Ergebnisse für Benutzergeräte, die die Anforderungen eines Fallback-Scans nach der Authentifizierung nicht erfüllen, lauten wie folgt:

- Wenn die Clientauswahl aktiviert ist, können sich Benutzer nur mithilfe der Citrix Workspace-App am Webinterface oder StoreFront anmelden.
- Wenn clientloser Zugriff und Clientauswahl deaktiviert sind, können Benutzer in eine Gruppe isoliert werden, die nur Zugriff auf das Webinterface oder StoreFront bietet.
- Wenn der clientlose Zugriff und das Webinterface oder StoreFront auf Citrix Gateway aktiviert sind und der ICA-Proxy deaktiviert ist, greifen Benutzer auf den clientlosen Zugriff zurück.
- Wenn das Webinterface oder StoreFront nicht konfiguriert ist und der clientlose Zugriff auf Zulassen eingestellt ist, greifen Benutzer auf den clientlosen Zugriff zurück.

Wenn der clientlose Zugriff deaktiviert ist, muss die folgende Kombination von Einstellungen für das Fallback des Zugriffsszenarios konfiguriert werden:

- Definieren Sie Sicherheitsparameter für den Fallback-Scan nach der Authentifizierung.
- Definieren Sie die Webinterface-Homepage.
- Deaktivieren Sie Clientauswahl.
- Wenn Benutzergeräte die Client-Sicherheitsprüfung nicht bestehen, werden Benutzer in eine Quarantänegruppe eingeordnet, die nur Zugriff auf das Webinterface oder StoreFront und auf veröffentlichte Anwendungen ermöglicht.

### Erstellen von Richtlinien für Access Scenario Fallback

Um Citrix Gateway für das Fallback von Zugriffsszenarien zu konfigurieren, müssen Sie Richtlinien und Gruppen auf folgende Weise erstellen:

- Erstellen Sie eine Quarantänegruppe, in der Benutzer platziert werden, wenn der Endpoint Analysis-Scan fehlschlägt.
- Erstellen Sie eine globale Einstellung für das Webinterface oder StoreFront, die verwendet wird, wenn der Endpoint Analysis-Scan fehlschlägt.
- Erstellen Sie eine Sitzungsrichtlinie, die die globale Einstellung überschreibt, und binden Sie dann die Sitzungsrichtlinie an eine Gruppe.
- Erstellen Sie eine globale Client-Sicherheitsrichtlinie, die angewendet wird, wenn die Endpunktanalyse fehlschlägt.

Beachten Sie beim Konfigurieren des Fallbacks für das Zugriffsszenario die folgenden Richtlinien:

- Die Verwendung von Clientoptionen oder Fallbacks für Zugriffsszenarien erfordert das Endpoint Analysis-Plug-In für alle Benutzer. Wenn die Endpoint Analysis nicht ausgeführt werden kann

oder wenn Benutzer während des Scans Scan überspringen auswählen, wird Benutzern der Zugriff verweigert.
Hinweis: Die Option zum Überspringen des Scans wird in Citrix Gateway 10.1, Build 120.1316.e entfernt

- Wenn Sie die Clientauswahl aktivieren und das Benutzergerät den Endpoint Analysis-Scan nicht besteht, werden Benutzer in die Quarantänegruppe aufgenommen. Benutzer können sich weiterhin entweder mit dem Citrix Gateway Plug-in oder der Citrix Workspace-App am Webinterface oder StoreFront anmelden.
  Hinweis: Citrix empfiehlt, keine Quarantänegruppe zu erstellen, wenn Sie die Clientauswahl aktivieren. Benutzergeräte, die den Endpoint Analysis-Scan nicht bestehen, werden unter Quarantäne gestellt, werden genauso behandelt wie Benutzergeräte, die den Endpunkt-Scan bestehen.
- Wenn der Endpoint Analysis-Scan fehlschlägt und der Benutzer in die Quarantänegruppe aufgenommen wird, sind die an die Quarantänegruppe gebundenen Richtlinien nur wirksam, wenn keine direkt an den Benutzer gebundenen Richtlinien vorhanden sind, die eine gleiche oder niedrigere Prioritätszahl als die an die Quarantänegruppe gebundenen Richtlinien haben.
- Sie können verschiedene Webadressen für das Access Interface und das Webinterface oder StoreFront verwenden. Wenn Sie die Homepages konfigurieren, hat die Access Interface-Homepage Vorrang für das Citrix Gateway Plug-in, und die Webinterface-Homepage hat Vorrang für Webinterface-Benutzer. Die Homepage der Citrix Workspace-App hat Vorrang für StoreFront.

**Erstellen einer Quarantänegruppe**

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Gruppen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im **Feld Gruppenname**einen Namen für die Gruppe ein, klicken Sie auf **Erstellen** und dann auf **Schließen**.
   **Wichtig**: Der Name der Quarantänegruppe darf nicht mit dem Namen einer Domänengruppe übereinstimmen, zu der Benutzer gehören könnten. Wenn die Quarantänegruppe mit einem Active Directory-Gruppennamen übereinstimmt, werden Benutzer unter Quarantäne gestellt, selbst wenn das Benutzergerät den Endpoint Analysis-Sicherheitsscan durchläuft.

Konfigurieren Sie Citrix Gateway nach dem Erstellen der Gruppe so, dass auf das Webinterface zurückgekehrt wird, wenn das Benutzergerät den Endpoint Analysis-Scan nicht besteht.

**Konfigurieren von Einstellungen zur Quarantäne von Benutzerverbindungen**

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Wählen Sie im Dialogfeld **Globale Citrix Gateway-Einstellungen** auf der Registerkarte **Published Applications** neben **ICA-ProxyOFF**aus.
4. Geben Sie neben **Webinterface-Adresse**die Webadresse für StoreFront oder das Webinterface ein.
5. Geben Sie neben **Single Sign-On Domäne**den Namen Ihrer Active Directory-Domäne ein, und klicken Sie dann auf **OK**.

Erstellen Sie nach dem Konfigurieren der globalen Einstellungen eine Sitzungsrichtlinie, die die globale ICA-Proxy-Einstellung außer Kraft setzt, und binden Sie dann die Sitzungsrichtlinie an die Quarantänegruppe.

**Erstellen einer Sitzungsrichtlinie für Access Scenario Fallback**

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. Klicken Sie auf der Registerkarte **Veröffentlichte Anwendungen** neben **ICA-Proxy**auf **Global überschreiben**, wählen Sie Ein aus **,** und klicken Sie dann auf **Erstellen**.
6. Wählen **Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben **Benannte Ausdrückedie Option Allgemein**aus, wählen Sie**Wahrer Wert**aus, klicken Sie auf**Ausdruck hinzufügen**, klicken Sie auf**Erstellen**und dann auf**Schließen**.

Binden Sie die Richtlinie nach dem Erstellen der Sitzungsrichtlinie an eine Quarantänegruppe.

**Binden Sie die Sitzungsrichtlinie an die Quarantänegruppe**

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Gruppen**.
2. Wählen Sie im Detailbereich eine Gruppe aus, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie auf Sitzung.
4. Wählen Sie auf der Registerkarte **RichtlinienSitzung**aus, und klicken Sie dann auf**Richtlinie einfügen**.
5. Wählen Sie unter **Richtliniennam**die Richtlinie aus, und klicken Sie dann auf **OK**.

Erstellen Sie nach dem Erstellen der Sitzungsrichtlinie und des Profils, die das Webinterface oder StoreFront auf Citrix Gateway aktiviert haben, eine globale Client-Sicherheitsrichtlinie.

**Erstellen einer globalen Client-Sicherheitsrichtlinie**

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte **Sicherheit** auf **Erweiterte Einstellungen**.
4. Geben Sie unter **Client Security**den Ausdruck ein. Weitere Informationen zum Konfigurieren von Systemausdrücken finden Sie unter Konfigurieren von Systemausdrücken und Konfigurieren von Sicherheitsausdrücken für zusammengesetzte Clients
5. Wählen Sie in **Quarantänegruppe**die Gruppe aus, die Sie in der Gruppenprozedur konfiguriert haben, und klicken Sie dann auf **OK**.

## Konfigurieren von Verbindungen für das Citrix Gateway Plug-in

March 27, 2024

Sie konfigurieren Benutzergeräteverbindungen, indem Sie die Ressourcen definieren, auf die Benutzer im internen Netzwerk zugreifen können. Das Konfigurieren von Benutzergeräteverbindungen umfasst:

- Definieren der Domänen, auf die Benutzer Zugriff erhalten.
- Konfigurieren von IP-Adressen für Benutzer, einschließlich Adresspools (Intranet-IPs).
- Konfigurieren von Timeout-Einstellungen.
- Konfigurieren von einmaliger Anmeldung.
- Konfigurieren des Clientabfangs.
- Konfigurieren von Split-Tunneling.
- Konfigurieren von Verbindungen über einen Proxyserver.
- Konfigurieren von Benutzersoftware für die Verbindung über Citrix Gateway.
- Konfigurieren des Zugriffs für mobile Geräte.

Sie konfigurieren die meisten Benutzergeräteverbindungen mithilfe eines Profils, das Teil einer Sitzungsrichtlinie ist. Sie können Verbindungseinstellungen für Benutzergeräte auch mithilfe von Intranetanwendungen, Vorauthentifizierung und Verkehrsrichtlinien definieren.

> **Hinweis:**
>
> Das Windows VPN-Plug-In und die EPA-Plug-Ins sammeln Telemetriedaten für seine verschiedenen Vorgänge. Um die Funktion zu deaktivieren, gehen Sie auf dem Clientcomputer wie folgt vor.
>
> Stellen Sie die Registrierung "HKLM\ Software\ Citrix\ Secure Access Client\ DisableGA"vom Typ REG_DWORD auf 1.

## Anzahl der Benutzersitzungen konfigurieren

March 27, 2024

Sie können die maximale Anzahl von Benutzern konfigurieren, die zu einem bestimmten Zeitpunkt eine Verbindung zu Citrix Gateway herstellen dürfen, entweder auf globaler Ebene oder auf einer Ebene pro virtuellem Server. Sitzungen werden auf Citrix Gateway nicht erstellt, wenn die Anzahl der Benutzer, die eine Verbindung zur Appliance herstellen, den von Ihnen konfigurierten Wert überschreitet. Wenn die Anzahl der Benutzer die von Ihnen zugelassene Anzahl überschreitet, erhalten Benutzer eine Fehlermeldung.

### So legen Sie das globale Benutzerlimit fest

Wenn Sie das Benutzerlimit global konfigurieren, gilt die Einschränkung für alle Benutzer, die Sitzungen mit verschiedenen virtuellen Servern auf dem System einrichten. Wenn die Anzahl der Benutzersitzungen den von Ihnen festgelegten Wert erreicht, können auf keinem virtuellen Server auf Citrix Gateway neue Sitzungen eingerichtet werden.

Sie legen die maximale Anzahl von Benutzern auf globaler Ebene fest, wenn Sie den Standardauthentifizierungstyp für Citrix Gateway festlegen.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte "Configuration"im Navigationsbereich "Citrix Gateway"und klicken Sie auf "Global Settings".
2. Klicken Sie im Detailbereich unter Einstellungen auf Authentifizierungseinstellungen ändern.
3. Geben Sie im Dialogfeld Globale Authentifizierungseinstellungen in das Feld Maximale Anzahl an Benutzern die Anzahl der Benutzer ein, und klicken Sie dann auf OK.

### So legen Sie das Benutzerlimit pro virtuellem Server fest

Sie können das Benutzerlimit auch auf jeden virtuellen Server im System anwenden. Wenn Sie das Benutzerlimit pro virtuellem Server konfigurieren, gilt die Einschränkung nur für Benutzer, die Sitzun-

gen mit dem bestimmten virtuellen Server einrichten. Benutzer, die Sitzungen mit anderen virtuellen Servern einrichten, sind von diesem Limit nicht betroffen.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf Virtuelle Server.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf Öffnen.
3. Geben Sie unter Max Users die Anzahl der Benutzer ein und klicken Sie dann auf OK.

## Timeouteinstellungen konfigurieren

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass eine Trennung erzwungen wird, wenn die Verbindung für eine bestimmte Anzahl von Minuten nicht aktiv ist. Eine Minute bevor eine Sitzung abläuft (die Verbindung trennt), erhält der Benutzer eine Warnung, die darauf hinweist, dass die Sitzung geschlossen wird. Wenn die Sitzung geschlossen wird, muss sich der Benutzer erneut anmelden.

Die folgenden Timeout-Optionen sind verfügbar.

- **Erzwungene Auszeit.** Wenn Sie diese Einstellung aktivieren, trennt Citrix Gateway die Sitzung nach Ablauf des Timeout-Intervalls, unabhängig davon, was der Benutzer tut. Es gibt keine Aktion, die der Benutzer ergreifen kann, um zu verhindern, dass die Verbindung unterbrochen wird, wenn das Timeout-Intervall abgelaufen ist. Diese Einstellung wird für Benutzer erzwungen, die eine Verbindung mit dem Citrix Gateway Plug-in, der Citrix Workspace-App, Secure Hub oder über einen Webbrowser herstellen. Der Mindestwert ist 1, und der Maximalwert ist 65535.
- **Sitzungs-Zeitüberschreitung.** Wenn Sie diese Einstellung aktivieren, trennt Citrix Gateway die Sitzung, wenn für das angegebene Intervall keine Netzwerkaktivität festgestellt wird. Diese Einstellung wird für Benutzer erzwungen, die eine Verbindung mit dem Citrix Gateway Plug-in, der Citrix Workspace-App, Citrix Secure Hub oder über einen Webbrowser herstellen. Die Standard-Timeout-Einstellung beträgt 30 Minuten. Der Mindestwert ist 1, und der Maximalwert ist 65535.
- **Timeout für Sitzung im Leerlauf.** Die Dauer, nach der das Citrix Gateway-Plug-in eine Sitzung im Leerlauf beendet, wenn für das angegebene Intervall keine Benutzeraktivität stattfindet, z. B. über die Maus, die Tastatur oder die Berührung. Diese Einstellung wird nur für Benutzer erzwungen, die eine Verbindung mit dem Citrix Gateway Plug-in herstellen. Der Mindestwert ist 1 und der Maximalwert ist 9999.

Sie können jede der Timeout-Einstellungen aktivieren, indem Sie einen Wert zwischen 1 und 65536 eingeben, um die Minuten für das Timeout-Intervall anzugeben. Wenn Sie mehr als eine dieser Einstellungen aktivieren, schließt das erste verstrichene Timeoutintervall die Verbindung des Benutzergeräts.

Sie konfigurieren Timeout-Einstellungen, indem Sie globale Einstellungen konfigurieren oder ein Sitzungsprofil verwenden. Wenn Sie das Profil zu einer Sitzungsrichtlinie hinzufügen, ist die Richtlinie dann an einen Benutzer, eine Gruppe oder einen virtuellen Server gebunden. Wenn Sie die Timeout-Einstellungen global konfigurieren, werden die Einstellungen auf alle Benutzersitzungen angewendet.

> **Hinweis:**
>
> - In Always On (Dienstmodus oder Benutzermodus) ignoriert der VPN-Client alle Timeouts. Entscheidungen über erzwungenes Timeout und Sitzungstimeout treten auf der Citrix ADC Appliance auf, und daher funktionieren diese Timeouts wie vorgesehen. Wenn ein solches Timeout auftritt, versucht das VPN-Plug-In, eine automatische Authentifizierung durchzuführen.
>
>  Konfigurieren Sie in Always On, da das Benutzergerät ständig über den VPN-Tunnel verbunden sein muss, kein erzwungenes Timeout oder ein Timeout im Leerlauf des Clients. Das Sitzungstimeout kann jedoch so konfiguriert werden, dass veraltete Sitzungen entfernt werden.
> - Einige Anwendungen, wie Microsoft Outlook, senden automatisch Netzwerkverkehrssonden ohne Benutzereingriff an E-Mail-Server. Citrix empfiehlt, dass Sie das Timeout für Sitzungen im Leerlauf mit Sitzungstimeout konfigurieren, um sicherzustellen, dass eine unbeaufsichtigte Sitzung auf einem Benutzergerät innerhalb einer angemessenen Zeit abläuft.

## Konfigurieren erzwungener Tim

Ein erzwungenes Timeout trennt das Citrix Gateway Plug-in automatisch nach einer bestimmten Zeit. Sie können ein erzwungenes Timeout global oder als Teil einer Sitzungsrichtlinie konfigurieren.

### Konfigurieren eines globalen erzwungenen Zeitlimits

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich Citrix Gateway und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte **Netzwerkkonfiguration** auf **Erweiterte Einstellungen**.
4. Geben Sie unter Erzwungenes Timeout (Minuten) die Anzahl der Minuten ein, die Benutzer in Verbindung bleiben können.
5. Geben Sie unter Warnung für erzwungene Zeitüberschreitung (Minuten) die Anzahl der Minuten ein, bevor Benutzer gewarnt werden, dass die Verbindung getrennt werden soll, und klicken Sie dann auf **OK**.

#### Konfigurieren eines erzwungenen Zeitlimits innerhalb einer Sitzungsrichtlinie

Wenn Sie weitere Kontrolle darüber haben möchten, wer das erzwungene Timeout erhält, erstellen Sie eine Sitzungsrichtlinie und wenden Sie die Richtlinie dann auf einen Benutzer oder eine Gruppe an.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** > **Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf **Neu**.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Klicken Sie auf der Registerkarte **Netzwerkkonfiguration** auf **Erweitert**.
7. Klicken Sie unter Timeouts auf Global überschreiben und geben Sie unter Erzwungenes Timeout (Minuten) die Anzahl der Minuten ein, die Benutzer verbunden bleiben können
8. Klicken Sie neben **Erzwungener Timeout-Warnung (Minuten)**auf **Override Global** und geben Sie die Anzahl der Minuten ein, für die Benutzer gewarnt werden, dass die Verbindung getrennt werden soll. Klicken Sie zwei Mal auf **OK**.
9. Wählen **Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben **Benannte Ausdrücke**die Option Allgemein aus, wählen Sie **Wahrer Wert**aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen** und dann auf **Schließen**.

### Konfigurieren von Sitzungs- oder Leerlaufzeitpunkten

Sie können die Citrix ADC GUI verwenden, um Sitzungs- und Client-Timeouteinstellungen global zu konfigurieren oder eine Sitzungsrichtlinie zu erstellen. Wenn Sie eine Sitzungsrichtlinie und ein Profil erstellen, legen Sie den Ausdruck auf True fest.

> **Hinweis:**
>
> Wenn Sie die globale Einstellung nicht explizit außer Kraft setzen und das Sitzungstimeout unter **Clienterfahrung > Sitzungstimeout (Minuten)** festlegen, kann dies zu Authentifizierungsschleifen führen, die eine erneute Anmeldung erfordern. Dies tritt auch bei einem Standardsitzungs-Timeout von 30 Minuten auf.

### So konfigurieren Sie eine Sitzung oder ein Client-Timeout im Leerlauf global über die GUI

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.

3. Führen Sie auf der Registerkarte **Client Experience** eine oder beide der folgenden Aktionen aus:
    - Geben Sie unter **Sitzungstimeout (Minuten)**die Anzahl der Minuten ein.
    - Geben Sie unter **Client Idle Timeout (Minuten)**die Anzahl der Minuten ein, und klicken Sie dann auf **OK**.

### So konfigurieren Sie Sitzungs- oder Client-Timeouteinstellungen im Leerlauf mithilfe einer Sitzungsrichtlinie über die GUI

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** > **Richtlinien**, und klicken Sie dann auf **Sitzung**
2. Klicken Sie auf der Seite **Citrix Gateway-Sitzungsrichtlinien und-profile auf Sitzungsprofile**und dann auf**Hinzufügen**.
3. Geben Sie im Feld Name einen Namen für das Profil ein.
4. Führen Sie auf der Registerkarte **Client Experience** eine oder beide der folgenden Aktionen aus:
    - Klicken Sie neben **Sitzungstimeout (Minuten)**auf **Global überschreiben**, geben Sie dann die Anzahl der Minuten ein, und klicken Sie dann auf **Erstellen**.
    - Klicken Sie neben **Client Idle Timeout (Minuten)**auf **Override Global**, geben Sie die Anzahl der Minuten ein und klicken Sie dann auf **Erstellen**.
5. a) Klicken Sie auf der Seite **Citrix Gateway Sitzungsrichtlinien und -profile** auf **Sitzungsrichtlinien**und dann auf **Hinzufügen**.
6. In der **Sitzungsrichtlinie Create Citrix Gateway**
    - Geben Sie **unter Name**den Namen für die Richtlinie ein.
    - Wählen Sie unter **Profil**das Profil aus, das die Aktion angibt, die von der neuen Sitzungsrichtlinie angewendet werden soll, wenn die Regelkriterien erfüllt sind.
    - wählen Sie **Erweiterte Richtlinie**.
    - Fügen Sie im Feld **Ausdruck** Ihren Ausdruck oder Namen eines benannten Ausdrucks hinzu und geben Sie den Datenverkehr an, der der Richtlinie entspricht.
    - Klicken Sie auf **Erstellen**und dann auf **Schließen**.

## Mit internen Netzwerkressourcen verbinden

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass Benutzer auf Ressourcen im internen Netzwerk zugreifen können. Wenn Sie Split-Tunneling deaktivieren, wird der gesamte Netzwerkverkehr vom Benutzergerät an Citrix Gateway gesendet, und Autorisierungsrichtlinien bestimmen, ob der

Datenverkehr an interne Netzwerkressourcen übertragen werden darf. Wenn Sie Split-Tunneling aktivieren, wird nur der für das interne Netzwerk bestimmte Datenverkehr vom Benutzergerät abgefangen und an Citrix Gateway gesendet. Sie konfigurieren, welche IP-Adressen Citrix Gateway mithilfe von Intranetanwendungen abfängt.

Wenn Sie das Citrix Gateway Plug-in für Windows verwenden, stellen Sie den Abhörmodus auf transparent ein. Wenn Sie das Citrix Gateway Plug-in für Java verwenden, stellen Sie den Abfangmodus auf Proxy ein. Wenn Sie den Abfangmodus auf transparent einstellen, können Sie den Zugriff auf Netzwerkressourcen zulassen mit:

- Eine einzelne IP-Adresse und Subnetzmaske
- Ein Bereich von IP-Adressen

Wenn Sie den Abfangmodus auf Proxy einstellen, können Sie Ziel- und Quell-IP-Adressen und Portnummern konfigurieren.

### Konfigurieren des Netzwerkzugriffs auf interne Netzwerkressourcen

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich Citrix Gateway, erweitern Sie Ressourcen, und klicken Sie dann auf **Intranetanwendungen.**
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. Füllen Sie die Parameter für das Zulassen des Netzwerkzugriffs aus, klicken Sie auf **Erstellen** und dann auf **Schließen.**

## Split-Tunneling konfigurieren

March 27, 2024

Sie können Split-Tunneling aktivieren, um zu verhindern, dass das Citrix Gateway Plug-in unnötigen Netzwerkverkehr an Citrix Gateway sendet.

Wenn Sie das Split-Tunneling nicht aktivieren, erfasst das Citrix Gateway Plug-in den gesamten Netzwerkverkehr, der von einem Benutzergerät stammt, und sendet den Datenverkehr durch den VPN-Tunnel an Citrix Gateway.

Wenn Sie Split-Tunneling aktivieren, sendet das Citrix Gateway Plug-in nur Datenverkehr, der für Netzwerke bestimmt ist, die von Citrix Gateway geschützt sind, durch den VPN-Tunnel. Das Citrix Gateway Plug-in sendet keinen Netzwerkverkehr, der für ungeschützte Netzwerke bestimmt ist, an Citrix Gateway.

Wenn das Citrix Gateway Plug-in gestartet wird, erhält es die Liste der Intranet-Anwendungen von Citrix Gateway. Das Citrix Gateway Plug-in untersucht alle Pakete, die vom Benutzergerät im Netzwerk übertragen werden, und vergleicht die Adressen in den Paketen mit der Liste der Intranetanwendungen. Wenn sich die Zieladresse im Paket in einer der Intranet-Anwendungen befindet, sendet das Citrix Gateway-Plug-in das Paket durch den VPN-Tunnel an Citrix Gateway. Wenn sich die Zieladresse nicht in einer definierten Intranet-Anwendung befindet, wird das Paket nicht verschlüsselt und das Benutzergerät leitet das Paket entsprechend weiter. Wenn Sie Split-Tunneling aktivieren, definieren Intranet-Anwendungen den abgefangenen Netzwerkverkehr.

> **Hinweis:**
>
> Wenn Benutzer mithilfe der Citrix Workspace-App eine Verbindung zu veröffentlichten Anwendungen in einer Serverfarm herstellen, müssen Sie kein Split-Tunneling konfigurieren.

Citrix Gateway unterstützt auch Reverse-Split-Tunneling, das den Netzwerkverkehr definiert, den Citrix Gateway nicht abfängt. Wenn Sie Split-Tunneling auf Rückwärtsgang einstellen, definieren Intranetanwendungen den Netzwerkverkehr, den Citrix Gateway nicht abfängt. Wenn Sie Reverse-Split-Tunneling aktivieren, umgeht der gesamte Netzwerkverkehr, der an interne IP-Adressen gerichtet ist, den VPN-Tunnel, während anderer Datenverkehr über Citrix Gateway fließt. Reverse-Split-Tunneling kann verwendet werden, um den gesamten nicht lokalen LAN-Verkehr zu protokollieren. Wenn Benutzer beispielsweise über ein drahtloses Heimnetzwerk verfügen und mit dem Citrix Gateway Plug-in angemeldet sind, fängt Citrix Gateway keinen Netzwerkverkehr ab, der für einen Drucker oder ein anderes Gerät im drahtlosen Netzwerk bestimmt ist.

Weitere Informationen zu Intranet-Anwendungen finden Sie unter Configuring Client Interception.

Sie konfigurieren Split-Tunneling als Teil der Sitzungsrichtlinie.

### So konfigurieren Sie Split-Tunneling

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway-Richtlinien** und klicken Sie dann auf **Sitzung.**
2. Wählen Sie im Detailbereich auf der Registerkarte **Profile** ein Profil aus und klicken Sie dann auf **Öffnen.**
3. Wählen Sie auf der Registerkarte **Client Experience** neben **Split Tunnel**die Option **Global Override**aus, wählen Sie eine Option aus und klicken Sie dann zweimal auf **OK**.

### Konfigurieren von Split-Tunneling und Autorisierung

Bei der Planung Ihrer Citrix Gateway-Bereitstellung ist es wichtig, Split-Tunneling sowie die Standard-Autorisierungsaktion und Autorisierungsrichtlinien in Betracht zu ziehen.

Beispielsweise haben Sie eine Autorisierungsrichtlinie, die den Zugriff auf eine Netzwerkressource ermöglicht. Sie haben Split-Tunneling auf ON eingestellt und konfigurieren Intranet-Anwendungen nicht so, dass Netzwerkverkehr über Citrix Gateway gesendet wird. Wenn Citrix Gateway über diese Art von Konfiguration verfügt, ist der Zugriff auf die Ressource zulässig, Benutzer können jedoch nicht auf die Ressource zugreifen.

Wenn die Autorisierungsrichtlinie den Zugriff auf eine Netzwerkressource verweigert, haben Sie Split-Tunneling auf ON eingestellt, und Intranetanwendungen sind so konfiguriert, dass sie Netzwerkverkehr über Citrix Gateway weiterleiten. Das Citrix Gateway-Plug-in sendet Datenverkehr an Citrix Gateway, der Zugriff auf die Ressource wird jedoch verweigert.

Weitere Informationen zum Split-Tunneling finden Sie unter Split-Tunneling konfigurieren.

## Clientabfangs konfigurieren

March 27, 2024

Sie konfigurieren Abfangregeln für Benutzerverbindungen auf Citrix Gateway mithilfe von Intranet-Anwendungen. Standardmäßig werden Subnetz-Routen basierend auf diesen IP-Adressen erstellt, wenn Sie die System-IP-Adresse, eine zugeordnete IP-Adresse oder eine Subnetz-IP-Adresse auf der Appliance konfigurieren. Intranet-Anwendungen werden basierend auf diesen Routen automatisch erstellt und können an einen virtuellen Server gebunden werden. Wenn Sie Split-Tunneling aktivieren, müssen Sie Intranet-Anwendungen definieren, damit das Client-Abfangen erfolgen kann.

Sie können Intranet-Anwendungen mithilfe des Konfigurationsdienstprogramms konfigurieren. Sie können Intranet-Anwendungen an Benutzer, Gruppen oder virtuelle Server binden.

Wenn Sie Split-Tunneling aktivieren und Benutzer mithilfe von WorxWeb oder WorxMail eine Verbindung herstellen, müssen Sie beim Konfigurieren des Clientabfangs die IP-Adressen für Citrix Endpoint Management und Ihren Exchange-Server hinzufügen. Wenn Sie kein Split-Tunneling aktivieren, müssen Sie die Endpoint Management- und Exchange-IP-Adressen in Intranet-Anwendungen nicht konfigurieren.

Informationen zur Konfiguration von Split-Tunneling finden Sie unter Konfiguration von Split-Tunneling.

### Konfigurieren von Intranet-Anwendungen für das Citrix Gateway Plug-in

Sie erstellen Intranet-Anwendungen für den Benutzerzugriff auf Ressourcen, indem Sie Folgendes definieren:

- Eine IP-Adresse

- Ein Bereich von IP-Adressen
- Ein Hostname

Wenn Sie eine Intranetanwendung auf Citrix Gateway definieren, fängt Citrix Secure Access Agent für Windows Benutzerdatenverkehr ab, der für die Ressource bestimmt ist, und sendet den Datenverkehr über Citrix Gateway.

Beachten Sie bei der Konfiguration von Intranet-Anwendungen Folgendes:

- Wenn der Split-Tunnel ON ist,
  - Konfigurieren Sie die Intranetanwendungen.
  - Weisen Sie jeder Authentifizierungs-, Autorisierungs- und Überwachungsgruppe Intranetanwendungen zu.
- Wenn der Split-Tunnel OFF ist,
  - Der gesamte Verkehr wird durch den VPN-Tunnel abgefangen.
  - Intranetanwendungen müssen nicht konfiguriert werden.
- Wenn der Split-Tunnel REVERSE ist,
  - Konfigurieren Sie die Intranetanwendungen. Der Datenverkehr, der nicht von den Intranetanwendungen angegeben wird, durchläuft den VPN-Tunnel.
  - Weisen Sie jeder Authentifizierungs-, Autorisierungs- und Überwachungsgruppe die Intranetanwendungen zu, die vom VPN ausgeschlossen werden sollen.

> **Wichtig:**
>
> Interception muss unabhängig von der Konfiguration des Split-Tunnels auf **TRANSPARENT** gesetzt werden.

**Hinweis:**

- Bei der Konfiguration einer Intranet-Anwendung müssen Sie einen Abfangmodus auswählen, der dem Typ der Plug-In-Software entspricht, mit der Verbindungen hergestellt werden.
- Sie können eine Intranet-Anwendung nicht sowohl für Proxy- als auch für transparentes Abfangen konfigurieren.

### So erstellen Sie eine Intranet-Anwendung für eine IP-Adresse

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway-Ressourcen** und klicken Sie dann auf Intranetanwendungen **.**
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. **Geben Sie im Feld Name einen Namen für das Profil ein.**

4. Wählen **Sie im Dialogfeld Intranetanwendung erstellen** die Option **TRANSPARENT**aus.
5. Wählen Sie unter **Zieltyp** die Option **IP-Adresse** und **Netzwerkmaske** aus.
6. Wählen Sie unter **Protokoll** das Protokoll aus, das für die Netzwerkressource gilt.
7. Geben Sie unter **IP-Adresse**die IP-Adresse ein.
8. Geben Sie unter **Netzmaske**Subnetzmaske ein, klicken Sie auf **Erstellen** und dann auf **Schließen.**

### So konfigurieren Sie einen IP-Adressbereich

Wenn Sie mehrere Server in Ihrem Netzwerk haben, z. B. Web-, E-Mail- und Dateifreigaben, können Sie eine Netzwerkressource konfigurieren, die den IP-Bereich für Netzwerkressourcen umfasst. Diese Einstellung ermöglicht Benutzern den Zugriff auf die im IP-Adressbereich enthaltenen Netzwerkressourcen.

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway-Ressourcen** und klicken Sie dann auf **Intranetanwendungen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. **Geben Sie im Feld Name einen Namen für das Profil ein.**
4. Wählen Sie unter **Protokoll** das Protokoll aus, das für die Netzwerkressource gilt.
5. Wählen Sie im Dialogfeld Intranetanwendung **erstellen** die Option **TRANSPARENT** aus.
6. Wählen Sie unter **ZieltypIP-Adressbereich aus.**
7. Geben Sie unter **IP Start**die Start-IP-Adresse ein und geben Sie unter IP-Ende die End-IP-Adresse ein, klicken Sie auf **Erstellen** und dann auf **Schließen.**

### So erstellen Sie eine Intranet-Anwendung für einen Hostnamen

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway-Ressourcen** und klicken Sie dann auf Intranetanwendungen **.**
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. Geben Sie im Feld Name einen Namen für das Profil ein.
4. Wählen **Sie im Dialogfeld Intranetanwendung erstellen** die Option **TRANSPARENT**aus.
5. Wählen Sie unter **Zieltyp**den **Hostnamen**aus.
6. Wählen Sie unter Protokoll **ANY**aus, klicken Sie auf **Erstellen** und dann auf **Schließen.**

> **Wichtig:**
>
> - Ab Version 13.0 Build 36.27 und höher unterstützt das Windows VPN-Plug-In auf Hostnamen (FQDN) basierende Regeln für Split-Tunneling. Sie müssen sowohl die Citrix ADC Appliance als auch das Windows VPN-Plug-In aktualisieren, um 13.0 Build 36.27 oder höher zu veröffentlichen.

- Wildcard-Hostnamen werden ebenfalls unterstützt. Wenn beispielsweise eine Intranetanwendung mit dem Hostnamen "*.example.com"konfiguriert ist, `a1.example.com`, `b2.example.com` usw. werden getunnelt.
- Die auf dem Hostnamen basierende Intranetanwendung funktioniert nur, wenn Sie Split-Tunneling auf ON oder REVERSE eingestellt haben.
- Auf Hostnamen basierende Regeln werden für Reverse-Split-Tunneling nicht unterstützt.

### Konfigurieren von Intranet-Anwendungen für das Citrix Gateway Plug-in für Java

Wenn Benutzer eine Verbindung mit dem Citrix Gateway Plug-in für Java herstellen, müssen Sie eine Intranetanwendung konfigurieren und den Abfangmodus auf Proxy einstellen. Das Citrix Gateway-Plug-in für Java fängt den Datenverkehr mithilfe der im Profil angegebenen Loopback-IP-Adresse und Portnummer des Benutzergeräts ab.

Wenn Benutzer von einem Windows-basierten Gerät aus eine Verbindung herstellen, versucht das Citrix Gateway-Plug-in für Java, die Hostdatei zu ändern, indem der Hostname der Anwendung für den Zugriff auf die im Profil angegebene Loopback-IP-Adresse und den Port festgelegt wird. Benutzer müssen über Administratorrechte auf dem Benutzergerät für die Änderung der HOST-Datei verfügen.

Wenn Benutzer von einem Nicht-Windows-Gerät aus eine Verbindung herstellen, müssen Sie Anwendungen manuell mithilfe der Quell-IP-Adresse und der Portwerte konfigurieren, die im Intranet-Anwendungsprofil angegeben sind.

### So konfigurieren Sie eine Intranet-Anwendung für das Citrix Gateway Plug-in für Java

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway-Ressourcen** und klicken Sie dann auf **Intranetanwendungen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. **Geben Sie im Feld Name einen Namen für das Profil ein.**
4. Klicken Sie auf **Proxy.**
5. Geben Sie unter **Ziel-IP-Adresse** und **Zielport**die Ziel-IP-Adresse und den Zielport ein.
6. Geben Sie unter **Quell-IP-Adresse** und **Quellport**die Quell-IP-Adresse und den Port ein.

   **Hinweis:**

   Stellen Sie die Quell-IP-Adresse auf die Loopback-IP-Adresse 127.0.0.1 ein. Wenn Sie keine IP-Adresse angeben, wird die Loopback-IP-Adresse verwendet. Wenn Sie keinen Portwert eingeben, wird der Zielportwert verwendet.

# Name Service-Auflösung konfigurieren

March 27, 2024

Während der Installation von Citrix Gateway können Sie den Citrix Gateway-Assistenten verwenden, um andere Einstellungen zu konfigurieren, einschließlich Namensdienstanbieter. Die Namensdienstanbieter übersetzen den vollqualifizierten Domainnamen (FQDN) in eine IP-Adresse. Im Citrix Gateway-Assistenten können Sie einen DNS- oder WINS-Server konfigurieren, die Priorität der DNS-Suche festlegen und wie oft die Verbindung zum Server erneut versucht wird.

Wenn Sie den Citrix Gateway-Assistenten ausführen, können Sie dann einen DNS-Server hinzufügen. Mithilfe eines Sitzungsprofils können Sie Citrix Gateway weitere DNS-Server und einen WINS-Server hinzufügen. Sie können dann Benutzer und Gruppen anweisen, eine Verbindung zu einem Namensauflösungsserver herzustellen, der sich von dem unterscheidet, den Sie ursprünglich mit dem Assistenten konfiguriert haben.

Erstellen Sie vor dem Konfigurieren eines zusätzlichen DNS-Servers auf Citrix Gateway einen virtuellen Server, der als DNS-Server für die Namensauflösung fungiert.

### Hinzufügen eines DNS- oder WINS-Servers innerhalb eines Sitzungsprofils

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway-Richtlinien** und klicken Sie dann auf **Sitzung.**
2. Wählen Sie im Detailbereich auf der Registerkarte Profile ein Profil aus und klicken Sie dann auf Öffnen.
3. Führen Sie auf der Registerkarte Netzwerkkonfiguration einen der folgenden Schritte aus:
    - Um einen DNS-Server zu konfigurieren, klicken Sie neben Virtueller DNS-Server auf **Override Global** , wählen Sie den Server aus, und klicken Sie dann auf **OK**.
    - Um einen WINS-Server zu konfigurieren, klicken Sie neben WINS-Server-IP auf **Override Global** , geben Sie die IP-Adresse ein und klicken Sie dann auf **OK**.

> **Wichtig:**
>
> Responder-Richtlinien werden nicht für nicht adressierbare virtuelle DNS-Server ausgewertet, die an das VPN-Sitzungsprofil angeschlossen sind.

# Proxyunterstützung für Benutzerverbindungen aktivieren

March 27, 2024

Benutzergeräte können über einen Proxyserver eine Verbindung herstellen, um auf interne Netzwerke zuzugreifen. Citrix Gateway unterstützt die Protokolle HTTP, SSL, FTP und SOCKS. Um die Proxy-Unterstützung für Benutzerverbindungen zu aktivieren, geben Sie die Einstellungen auf Citrix Gateway an. Sie können die IP-Adresse und den Port angeben, die vom Proxyserver auf Citrix Gateway verwendet werden. Der Proxyserver wird als Forward-Proxy für alle weiteren Verbindungen zum internen Netzwerk verwendet.

### Proxy-Einstellungen

Sie können Proxy-Einstellungen im Browser oder auf der Citrix ADC Appliance konfigurieren. Um Proxy-Einstellungen im Browser oder auf der Appliance zu konfigurieren, navigieren Sie zu **Globale Citrix Gateway-Einstellungen > Registerkarte Clienterfahrung > Erweiterte Einstellungen > Proxy**, und wählen Sie dann **Browser** oder **NS** aus.

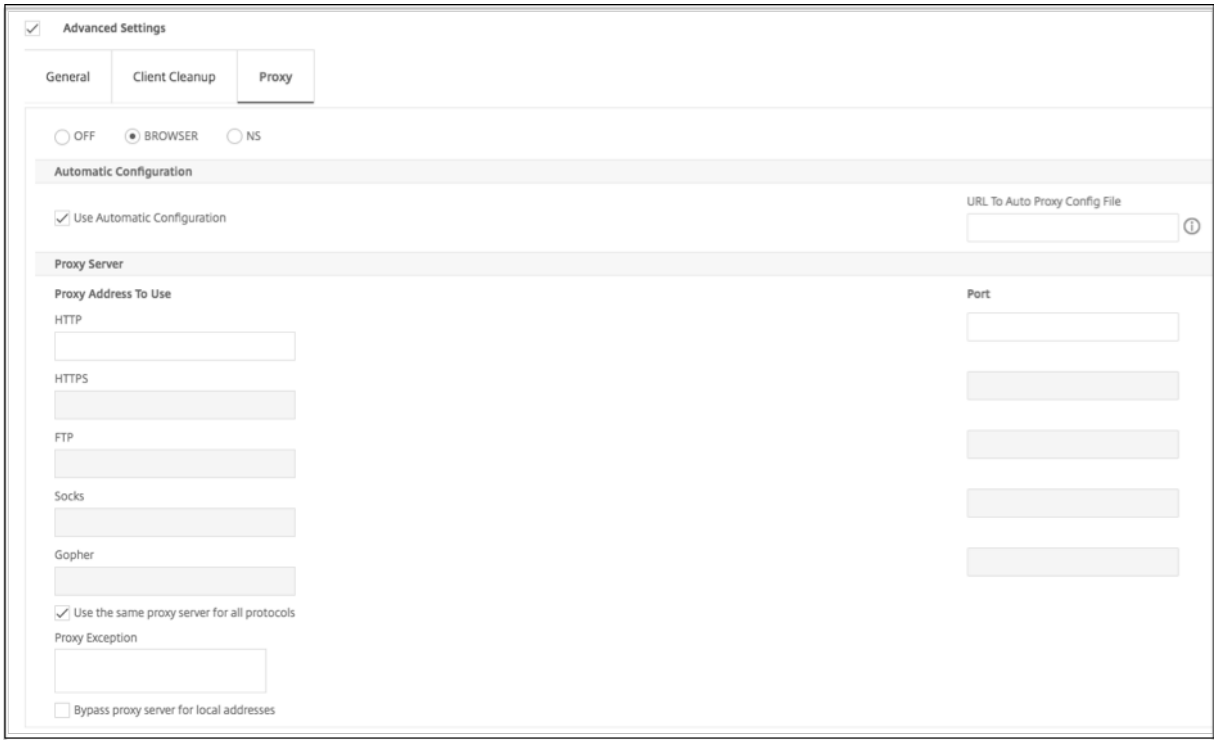
- **Browser**: Wenn Sie Proxy-Einstellungen im Browser konfigurieren, können Sie die automatische Konfigurationsoption verwenden, indem Sie einen Link zur automatischen Proxy-Konfigurationsdatei bereitstellen. Die automatische Konfiguration kann die manuellen Einstellungen überschreiben.

  Wenn Sie **Browser**auswählen, können Sie die zuvor konfigurierten Proxys Bypass, indem Sie die Proxy-Ausnahmeoption auswählen.

  **Hinweis:** Verschiedene Clienttypen verfügen über unterschiedliche Funktionen in Bezug auf die Konfiguration des **Browser-Proxys**. Einzelheiten finden Sie unter Citrix Gateway VPN-Clients und unterstützte Funktionen.

- **NS**: Sie können die automatische Konfigurationsoption nicht verwenden, wenn Sie Proxy-Einstellungen auf der Citrix ADC Appliance konfigurieren. Sie können die zuvor konfigurierten Proxys nicht Bypass, wenn Sie die Proxy-Einstellungen auf der Appliance konfigurieren.




### So konfigurieren Sie die Proxy-Unterstützung für Benutzerverbindungen

1. Erweitern Sie im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen.**
2. Klicken Sie im Detailbereich unter **Einstellungen**auf Globale Einstellungen ändern.
3. Klicken Sie auf der Registerkarte "Kundenerlebnis"auf **Erweiterte Einstellungen**.
4. Wählen Sie auf der Registerkarte **Proxy** unter **Proxyeinstellungen** die Option **Browser** aus.
5. Geben Sie für die Protokolle die IP-Adresse und die Portnummer ein und klicken Sie dann auf **OK.**

> **Hinweis:**
>
> - Wenn Sie **NS**wählen, können Sie Proxyserver konfigurieren, die nur sichere und unsichere HTTP-Verbindungen unterstützen.
> - Nachdem Sie die Proxy-Unterstützung auf Citrix Gateway aktiviert haben, geben Sie auf dem Benutzergerät Konfigurationsdetails für den Proxyserver an, die dem Protokoll entsprechen.
>
>   Nachdem Sie die Proxy-Unterstützung aktiviert haben, sendet Citrix Gateway die Proxy-Serverdetails an den Client-Webbrowser und ändert die Proxy-Konfiguration im Browser.
>
>   – When the user device connects to Citrix Gateway, the user device can communicate

with the proxy server directly for connection to the user's network.
- When the user device disconnects from Citrix Gateway, the proxy settings are restored to the previous default settings, that was present before connecting to the VPN plug-in.

## So konfigurieren Sie einen Proxyserver für die Verwendung aller Protokolle für Citrix Gateway

Sie können einen Proxyserver so konfigurieren, dass er alle Protokolle unterstützt, die Citrix Gateway verwendet. Diese Einstellung stellt eine Kombination aus IP-Adresse und Port für alle Protokolle bereit.

1. Erweitern Sie im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf Globale Einstellungen ändern.
3. Klicken Sie auf der Registerkarte „ **Kundenerlebnis** "auf **Erweiterte Einstellungen.**
4. Wählen Sie auf der Registerkarte **Proxyunter Proxyeinstellungen**die Option**Browser aus.**
5. Geben Sie für die Protokolle die IP-Adresse und die Portnummer ein.
6. Klicken Sie auf Dieselben Proxyserver für alle Protokolle verwenden und dann auf **OK.**

Wenn Sie das Split-Tunneling deaktivieren und alle Proxy-Einstellungen auf Ein setzen, werden die Proxy-Einstellungen an Benutzergeräte weitergegeben. Wenn die Proxy-Einstellungen auf Appliance festgelegt sind, werden die Einstellungen nicht an Benutzergeräte weitergegeben.

Citrix Gateway stellt im Namen des Benutzergeräts Verbindungen zum Proxyserver her. Die Proxy-Einstellungen werden nicht an den Browser des Benutzers weitergegeben, sodass keine direkte Kommunikation zwischen dem Benutzergerät und dem Proxyserver möglich ist.

## So konfigurieren Sie das Citrix Gateway als Proxyserver

Wenn Sie Citrix Gateway als Proxyserver konfigurieren, ist unsicheres und sicheres HTTP die einzigen unterstützten Protokolle.

1. Erweitern Sie im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen.**
2. Klicken Sie im Detailbereich unter **Einstellungen**auf Globale Einstellungen ändern.
3. Klicken Sie auf der Registerkarte „ **Kundenerlebnis** "auf **Erweiterte Einstellungen.**
4. Wählen Sie auf der Registerkarte **Proxy** unter **Proxy-Einstellungen** die Option **NS** aus.
5. Geben Sie für die Protokolle die IP-Adresse und die Portnummer ein und klicken Sie dann auf **OK.**

# Adresspools konfigurieren

March 27, 2024

In einigen Situationen benötigen Benutzer, die sich mit dem Citrix Gateway Plug-in verbinden, eine eindeutige IP-Adresse für Citrix Gateway. In einer Samba-Umgebung muss beispielsweise jeder Benutzer, der eine Verbindung zu einem zugeordneten Netzlaufwerk herstellt, scheinbar von einer anderen IP-Adresse stammen. Wenn Sie Adresspools (auch als IP-Pooling bezeichnet) für eine Gruppe aktivieren, kann Citrix Gateway jedem Benutzer einen eindeutigen IP-Adressalias zuweisen.

Sie konfigurieren Adresspools mit Intranet-IP-Adressen. Die folgenden Arten von Anwendungen müssen möglicherweise eine eindeutige IP-Adresse verwenden, die aus dem IP-Pool stammt:

- Voice-Over-IP
- Aktiv FTP
- Instant Messaging
- Sichere Shell (SSH)
- Virtual Network Computing (VNC) zur Verbindung mit einem Computerdesktop
- Remotedesktop (RDP), um eine Verbindung zu einem Clientdesktop herzustellen

Sie können Citrix Gateway so konfigurieren, dass Benutzern, die eine Verbindung zu Citrix Gateway herstellen, eine interne IP-Adresse zuweisen. Statische IP-Adressen können Benutzern zugewiesen werden oder ein Bereich von IP-Adressen kann einer Gruppe, einem virtuellen Server oder dem System global zugewiesen werden.

Mit Citrix Gateway können Sie Ihren Remote-Benutzern IP-Adressen aus Ihrem internen Netzwerk zuweisen. Eine IP-Adresse im internen Netzwerk kann einen Remote-Benutzer ansprechen. Wenn Sie sich für die Verwendung eines IP-Adressbereichs entscheiden, weist das System einem Remote-Benutzer bei Bedarf dynamisch eine IP-Adresse aus diesem Bereich zu.

Beachten Sie beim Konfigurieren von Adresspools Folgendes:

- Zugewiesene IP-Adressen müssen korrekt geroutet werden. Beachten Sie Folgendes, um das korrekte Routing sicherzustellen:
  - Wenn Sie kein Split-Tunneling aktivieren, stellen Sie sicher, dass die IP-Adressen über Geräte zur Netzwerkadressübersetzung (NAT) weitergeleitet werden können.
  - Auf allen Servern, auf die über Benutzerverbindungen mit Intranet-IP-Adressen zugegriffen wird, müssen die richtigen Gateways konfiguriert sein, um diese Netzwerke zu erreichen.
  - Konfigurieren Sie Gateways oder eine statische Route auf Citrix Gateway, damit der Netzwerkverkehr von der Benutzersoftware an das interne Netzwerk weitergeleitet wird.

- Bei der Zuweisung von IP-Adressbereichen können nur zusammenhängende Subnetzmasken verwendet werden. Eine Teilmenge eines Bereichs kann einer untergeordneten Entität zugewiesen werden. Wenn beispielsweise ein IP-Adressbereich an einen virtuellen Server gebunden ist, binden Sie eine Teilmenge des Bereichs an eine Gruppe.
- IP-Adressbereiche können nicht an mehrere Entitäten innerhalb einer Bindungsebene gebunden werden. Beispielsweise kann eine Teilmenge eines Adressbereichs, die an eine Gruppe gebunden ist, nicht an eine zweite Gruppe gebunden werden.
- Citrix Gateway erlaubt es Ihnen nicht, IP-Adressen zu entfernen oder zu lösen, während sie aktiv von einer Benutzersitzung verwendet werden.
- Interne Netzwerk-IP-Adressen werden Benutzern mithilfe der folgenden Hierarchie zugewiesen:
  - Direkte Bindung des Nutzers
  - Gruppe zugewiesener Adresspool
  - Dem virtuellen Server zugewiesener Adresspool
  - Globaler Adressbereich
- Bei der Zuweisung von Adressbereichen können nur zusammenhängende Subnetzmasken verwendet werden. Eine Teilmenge eines zugewiesenen Bereichs kann jedoch weiter einer untergeordneten Entität zugewiesen werden.
  Ein gebundener globaler Adressbereich kann einen Bereich haben, der an Folgendes gebunden ist:
  - Virtueller Server
  - Gruppe
  - User
- Ein gebundener Adressbereich eines virtuellen Servers kann eine Teilmenge haben, die an Folgendes gebunden ist:
  - Gruppe
  - User

Ein gebundener Gruppenadressbereich kann eine Teilmenge haben, die an einen Benutzer gebunden ist.

Wenn einem Benutzer eine IP-Adresse zugewiesen wird, ist die Adresse für die nächste Anmeldung des Benutzers reserviert, bis der Adresspoollbereich erschöpft ist. Wenn die Adressen erschöpft sind, fordert Citrix Gateway die IP-Adresse des Benutzers zurück, der am längsten von Citrix Gateway abgemeldet ist.

Wenn eine Adresse nicht zurückgewonnen werden kann und alle Adressen aktiv verwendet werden, erlaubt Citrix Gateway dem Benutzer nicht, sich anzumelden. Sie können diese Situation verhindern, indem Sie Citrix Gateway erlauben, die zugeordnete IP-Adresse als Intranet-IP-Adresse zu verwenden, wenn alle anderen IP-Adressen nicht verfügbar sind.

### Intranet-IP-DNS-Registrierung

Wenn eine Intranet-IP einem Clientcomputer zugewiesen wird und nach dem Aufbau eines VIP-Tunnels, prüft das VPN-Plug-In, ob dieser Clientcomputer einer Domäne beigetreten ist. Wenn es sich bei dem Clientcomputer um einen in die Domäne eingebundenen Computer handelt, initiiert das VPN-Plug-in den DNS-Registrierungsprozess, um das Intranet des Rechners mit der zugewiesenen Intranet-IP-Adresse zu verknüpfen. Diese Registrierung wird vor der Wiederherstellung des Tunnels rückgängig gemacht.

Stellen Sie für eine erfolgreiche DNS-Registrierung sicher, dass die folgenden `nsapimgr`-Regler eingestellt sind. Stellen Sie außerdem sicher, dass der autorisierende DNS-Server "nicht sichere" DNS-Updates zulässt.

- **`nsapimgr` -ys enable_vpn_dns_override=1**: Dieses Flag wird zusammen mit den anderen Konfigurationsparametern an den Citrix Gateway VPN-Client gesendet. Wenn dieses Flag nicht gesetzt ist und der VPN-Client eine DNS/WINS-Anforderung abfängt, sendet er eine entsprechende HTTP-Anforderung "GET /DNS"über den Tunnel an den virtuellen Citrix Gateway-Server, um die aufgelöste IP-Adresse abzurufen. Wenn jedoch das Flag 'enable_vpn_dnstruncate_fix'gesetzt ist, leitet der VPN-Client die DNS/WINS-Anfragen transparent an den virtuellen Citrix Gateway-Server weiter. In diesem Fall wird das DNS-Paket unverändert über den VPN-Tunnel an den virtuellen Citrix Gateway-Server gesendet. Dies hilft in Fällen, in denen die DNS-Einträge, die von den im Citrix Gateway konfigurierten Nameservern zurückkommen, riesig sind und nicht in das UPD-Antwortpaket passen. In diesem Fall erreicht dieses TCP-DNS-Paket unverändert den Citrix Gateway-Server, wenn der Client wieder TCP-DNS verwendet, und daher führt der Citrix Gateway-Server eine TCP-DNS-Abfrage an einen DNS-Server durch.
- **nsapimgr -ys enable_vpn_dnstruncate_fix=1**: Dieses Flag wird vom Citrix Gateway-Server selbst verwendet. Wenn dieses Flag gesetzt ist, überschreibt Citrix Gateway das Ziel für die „TCP-Verbindungen am DNS-Port"zu den auf Citrix Gateway konfigurierten DNS-Servern (anstatt zu versuchen, sie an die DNS-Server-IP zu senden, die ursprünglich im eingehenden TCP-DNS-Paket vorhanden war). Für UDP-DNS-Anfragen wird standardmäßig die konfigurierte DNS-Server für die DNS-Auflösung verwendet. Das Citrix Gateway Plug-In für Windows unterstützt sowohl sichere als auch nicht sichere DNS-Updates. Die Unterstützung für sichere DNS-Updates ist standardmäßig in Builds 21.7.1.1 oder höher verfügbar.

  Das sichere DNS-Update im Windows-Plug-In ist standardmäßig deaktiviert. Um es zu aktivieren, erstellen Sie einen Wert vom Typ REG_DWORD in `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access` und setzen Sie ihn auf 1.

  - Wenn Sie den Wert auf 1 setzen, versucht das VPN-Plug-In zuerst die unsichere DNS-Aktualisierung. Wenn das unsichere DNS-Update fehlschlägt, versucht das VPN-Plug-in das sichere DNS-Update.

- Um nur das sichere DNS-Update auszuprobieren, können Sie den Wert auf 2 setzen.

Weitere Informationen zum Einstellen dieser Regler finden Sie unter https://support.citrix.com/article/CTX200243.

### Konfigurieren von Adresspools für einen Benutzer, eine Gruppe oder einen virtuellen Server

1. Erweitern Sie im Konfigurationsdienstprogramm im Navigationsbereich **Citrix Gateway**und führen Sie eine der folgenden Aktionen aus:
   - Erweitern Sie Citrix Gateway User Administration und klicken Sie dann auf **AAA-Benutzer**.
   - Erweitern Sie **Citrix Gateway** > **Benutzerverwaltung** und klicken Sie dann auf **AAA-Gruppen**.
   - Erweitern Sie **Citrix Gateway** und klicken Sie dann auf **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen Benutzer, eine Gruppe oder einen virtuellen Server und dann auf **Öffnen**.
3. Geben Sie auf der Registerkarte **Intranet-IPs** unter IP-Adresse und Netzmaske die IP-Adresse und die Subnetzmaske ein und klicken Sie dann auf **Hinzufügen**.
4. Wiederholen Sie Schritt 3 für jede IP-Adresse, die Sie dem Pool hinzufügen möchten, und klicken Sie dann auf **OK**.

### Konfigurieren von Adresspools global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Intranet-IPs**auf Um eine eindeutige, statische IP-Adresse oder einen Pool von IP-Adressen für die Verwendung durch alle Citrix Gateway-Clientsitzungen zuzuweisen, konfigurieren Sie Intranet-IPs.
3. Klicken Sie im Dialogfeld **Intranet-IPs binden** auf **Aktion** und dann auf **Einfügen**.
4. Geben Sie unter IP-Adresse und Netzmaske die IP-Adresse und die Subnetzmaske ein und klicken Sie dann auf **Hinzufügen**.
5. Wiederholen Sie die Schritte 3 und 4 für jede IP-Adresse, die Sie dem Pool hinzufügen möchten, und klicken Sie dann auf **OK**.

### Definieren von Adresspools Optionen

Sie können eine Sitzungsrichtlinie oder die globalen Citrix Gateway-Einstellungen verwenden, um zu steuern, ob Intranet-IP-Adressen während einer Benutzersitzung zugewiesen werden. Durch das

Definieren von Adresspools können Sie Citrix Gateway Intranet-IP-Adressen zuweisen und gleichzeitig die Verwendung von Intranet-IP-Adressen für eine bestimmte Benutzergruppe deaktivieren.

Sie können Adresspools mithilfe einer Sitzungsrichtlinie auf eine der folgenden drei Arten konfigurieren:

- `Nospillover` - Wenn Sie Adresspools für die Intranet-IP-Adresse konfigurieren, erhalten Sie eine Sitzung mit einer verfügbaren IP aus dem Pool. Für Benutzer, die alle verfügbaren Intranet-IP-Adressen verwendet haben, wird die Seite Anmeldung übertragen angezeigt.
- **Überlauf** - Wenn Sie Adresspools konfigurieren und die zugeordnete IP als Intranet-IP-Adresse verwendet wird, wird die zugeordnete IP-Adresse für Benutzer verwendet, die alle verfügbaren Intranet-IP-Adressen verwendet haben.
- **Aus** —Adresspools sind nicht konfiguriert.

> **Hinweis:**
>
> Wenn die zugeordnete IP-Adresse nicht konfiguriert ist, wird SNIP verwendet.

### So definieren Sie Adresspools

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Klicken Sie auf der Registerkarte **Netzwerkkonfiguration** auf **Erweitert**.
7. Klicken Sie neben Intranet IP auf **Override Global** und wählen Sie dann eine Option aus.
8. Wenn Sie in Schritt 9 **SPILLOVER** auswählen, klicken Sie neben Zugeordnete IP auf **Global überschreiben**, wählen Sie den Hostnamen der Appliance aus, klicken Sie auf **OK,** und klicken Sie dann auf **Erstellen**.
9. Erstellen Sie im Dialogfeld **Sitzungsrichtlinie erstellen** einen Ausdruck, klicken Sie auf **Erstellen** und dann auf **Schließen**.

### Konfigurieren Sie die Anmeldeseite für die Übertragung

Wenn ein Benutzer keine Intranet-IP-Adresse verfügbar hat und dann versucht, eine weitere Sitzung mit Citrix Gateway aufzubauen, wird die Seite Anmeldung übertragen angezeigt. Auf der Seite Anmeldung übertragen können Benutzer ihre vorhandene Citrix Gateway-Sitzung durch eine neue Sitzung ersetzen.

Die Seite "Anmeldung übertragen"kann auch verwendet werden, wenn die Abmeldeanforderung verloren geht oder wenn der Benutzer keine saubere Abmeldung durchführt. Beispiel:

- Einem Benutzer wird eine statische Intranet-IP-Adresse zugewiesen und verfügt über eine vorhandene Citrix Gateway-Sitzung. Wenn der Benutzer versucht, eine zweite Sitzung von einem anderen Gerät aus aufzubauen, wird die Seite Anmeldung übertragen angezeigt, und der Benutzer kann die Sitzung auf das neue Gerät übertragen.
- Einem Benutzer werden fünf Intranet-IP-Adressen zugewiesen und hat fünf Sitzungen über Citrix Gateway. Wenn der Benutzer versucht, eine sechste Sitzung einzurichten, wird die Seite "Anmeldung übertragen"angezeigt, und der Benutzer kann wählen, ob er eine bestehende Sitzung durch eine neue Sitzung ersetzen möchte.

> **Hinweise:**
>
> - Wenn dem Benutzer keine zugewiesene IP-Adresse zur Verfügung steht, weshalb keine neue Sitzung eingerichtet werden kann, wird eine Fehlermeldung angezeigt.
> - Citrix Secure Access für Android 23.12.1 und höhere Versionen unterstützen die Übertragungsanmeldefunktion von NetScaler Gateway im Always-On-VPN-Modus.

Die Seite "Anmeldung übertragen"wird nur angezeigt, wenn Sie Adresspools konfigurieren und Spillover deaktivieren.

## DNS-Suffix konfigurieren

Wenn sich ein Benutzer bei Citrix Gateway anmeldet und eine IP-Adresse zugewiesen wird, wird dem Citrix Gateway DNS-Cache ein DNS-Datensatz für die Kombination aus Benutzernamen und IP-Adresse hinzugefügt. Sie können ein DNS-Suffix so konfigurieren, dass es an den Benutzernamen angehängt wird, wenn der DNS-Eintrag zum Cache hinzugefügt wird. Auf diese Weise können Benutzer mit dem DNS-Namen referenziert werden, der leichter zu merken ist als eine IP-Adresse. Wenn sich der Benutzer von Citrix Gateway abmeldet, wird der Datensatz aus dem DNS-Cache entfernt.

### So konfigurieren Sie ein DNS-Suffix

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Wählen Sie im Detailbereich auf der Registerkarte **Richtlinien** eine Sitzungsrichtlinie aus und klicken Sie dann auf **Öffnen**.
3. Klicken Sie neben Profil anfordern auf **Ändern**.
4. Klicken Sie auf der Registerkarte **Netzwerkkonfiguration** auf **Erweitert**.
5. Klicken Sie neben Intranet-IP-DNS-Suffix auf **Override Global**, geben Sie das DNS-Suffix ein und klicken Sie dann dreimal auf **OK**.

## Unterstützung für VoIP-Telefone

March 27, 2024

Wenn Sie Citrix Gateway als eigenständiges Gerät installieren und Benutzer eine Verbindung zum Citrix Gateway Plug-in herstellen, unterstützt Citrix Gateway die bidirektionale Kommunikation mit Voice over IP (VoIP) -Softphones.

Citrix Gateway unterstützt die folgenden VoIP-Softphones.

- Cisco Softphone
- Avaya IP-Softphone

Sicheres Tunneln wird zwischen der IP-PBX und der auf dem Benutzergerät laufenden Softphone-Software unterstützt. Damit der VoIP-Datenverkehr den sicheren Tunnel durchqueren kann, müssen Sie das Citrix Gateway-Plug-In und eines der unterstützten Softphones auf demselben Benutzergerät installieren. Wenn der VoIP-Verkehr über den sicheren Tunnel gesendet wird, werden die folgenden Softphone-Funktionen unterstützt:

- Ausgehende Anrufe, die vom IP-Softphone aus getätigt werden
- Eingehende Anrufe, die an das IP-Softphone getätigt werden
- Bidirektionaler Sprachverkehr

Die Unterstützung für VoIP-Softphones wird mithilfe von Intranet-IP-Adressen konfiguriert. Sie müssen für jeden Benutzer eine Intranet-IP-Adresse konfigurieren. Wenn Sie Cisco Softphone Communication verwenden, ist nach dem Konfigurieren der Intranet-IP-Adresse und der Bindung an einen Benutzer keine zusätzliche Konfiguration erforderlich. Weitere Informationen zum Konfigurieren einer Intranet-IP-Adresse finden Sie unter Konfigurieren von Adresspools.

Wenn Sie Split-Tunneling aktivieren, erstellen Sie eine Intranet-Anwendung und geben Sie die Avaya Softphone-Anwendung an. Darüber hinaus müssen Sie ein transparentes Abfangen aktivieren.

## Access Interface konfigurieren

March 27, 2024

Citrix Gateway enthält eine Standardstartseite, die nach der Benutzeranmeldung angezeigt wird. Die Standard-Homepage heißt Access Interface. Sie verwenden das Access Interface als Homepage oder konfigurieren das Webinterface als Homepage oder eine benutzerdefinierte Homepage.

Das Access Interface enthält drei Panels. Wenn Sie das Webinterface in Ihrer Bereitstellung haben, können sich Benutzer im linken Bereich des Access Interface bei Receiver anmelden. Wenn Sie Store-

Front in Ihrer Bereitstellung haben, können sich Benutzer nicht von der linken Seite aus bei Receiver anmelden.

Das Access Interface wird verwendet, um Links zu internen und externen Websites sowie Links zu Dateifreigaben im internen Netzwerk bereitzustellen. Sie können das Access Interface auf folgende Weise anpassen:

- Ändern des Access Interface.
- Erstellen von Access Interface-Links.

Benutzer können das Access Interface auch anpassen, indem sie ihre eigenen Links zu Websites und Dateifreigaben hinzufügen. Benutzer können die Homepage auch verwenden, um Dateien vom internen Netzwerk auf ihr Gerät zu übertragen.

> **Hinweis:**
>
> Wenn sich Benutzer anmelden und versuchen, Dateifreigaben über das Access Interface zu öffnen, wird die Dateifreigabe nicht geöffnet und Benutzer erhalten die Fehlermeldung "TCP-Verbindung zum Server konnte nicht hergestellt werden". Um dieses Problem zu beheben, konfigurieren Sie Ihre Firewall so, dass Datenverkehr von der Citrix Gateway-System-IP-Adresse zur Dateiserver-IP-Adresse an den TCP-Ports 445 und 139 zugelassen wird.

## Ändern Sie das Access Interface

Möglicherweise möchten Sie Benutzer zu einer angepassten Homepage leiten, anstatt sich auf das Access Interface zu verlassen. Installieren Sie dazu die Homepage auf Citrix Gateway und konfigurieren Sie dann die Sitzungsrichtlinie für die Verwendung der neuen Homepage.

### So installieren Sie eine angepasste Homepage

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte **Konfiguration** und dann im Navigationsbereich auf **Citrix Gateway.**
2. Klicken Sie im Detailbereich unter **Access Interface anpassen**auf **Access Interface**hochladen**.**
3. Um die Homepage von einer Datei auf einem Computer in Ihrem Netzwerk zu installieren, klicken Sie unter Lokale Datei auf **Durchsuchen**, navigieren Sie zur Datei und klicken Sie dann auf **Auswählen.**
4. Um eine Homepage zu verwenden, die auf Citrix Gateway installiert ist, klicken Sie in Remote Path auf **Durchsuchen**, wählen Sie die Datei aus, und klicken Sie dann auf **Auswählen.**
5. Klicken Sie auf **Hochladen** und dann auf **Schließen.**

### Ersetzen Sie das Access Interface durch eine benutzerdefinierte Homepage

Sie können entweder globale Einstellungen oder eine Sitzungsrichtlinie und ein Profil verwenden, um eine benutzerdefinierte Homepage zu konfigurieren, um die Standardstartseite, das Access Interface, zu ersetzen. Nachdem Sie die Richtlinie konfiguriert haben, können Sie die Richtlinie an einen Benutzer, eine Gruppe, einen virtuellen Server oder global binden. Wenn Sie eine benutzerdefinierte Homepage konfigurieren, wird das Access Interface nicht angezeigt, wenn sich Benutzer anmelden.

#### Konfigurieren Sie die benutzerdefinierte Homepage global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen.**
2. Klicken Sie im Detailbereich unter **Einstellungen**auf Globale Einstellungen ändern.
3. Klicken Sie auf der Registerkarte **Client Experience** unter **Homepage** auf **Homepage anzeigen** und geben Sie dann die Webadresse Ihrer benutzerdefinierten Homepage ein.
4. Klicken Sie auf **OK** und dann auf **Schließen**.

#### Konfigurieren einer benutzerdefinierten Homepage in einem Sitzungsprofil

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway-Richtlinien** und klicken Sie dann auf **Sitzung.**
2. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Hinzufügen.**
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben **Profil** anfordern auf **Neu.**
5. **Geben Sie im Feld Name einen Namen für das Profil ein.**
6. Klicken Sie auf der Registerkarte **Client Experience** neben **Homepage**auf **Global überschreiben**, klicken Sie auf **Homepage anzeigen,** und geben Sie dann die Webadresse der Homepage ein.
7. **Wählen Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben **Benannte Ausdrücke** die Option **Allgemein** aus, wählen Sie Wahrer Wert aus, klicken Sie auf **Ausdruck hinzufügen** , klicken Sie auf **Erstellen** und dann auf **Schließen.**

## Erstellen und Anwenden von Weblinks

March 27, 2024

Sie können das Access Interface so konfigurieren, dass eine Reihe von Links zu internen Ressourcen angezeigt wird, die Benutzern zur Verfügung stehen. Um diese Links zu erstellen, müssen Sie die Links

zuerst als Ressourcen definieren. Dann binden Sie sie an einen Benutzer, eine Gruppe, einen virtuellen Server oder global, um sie im Access Interface aktiv zu machen. Die von Ihnen erstellten Links werden in den **Websites-Fensten** unter **Unternehmenswebsites**angezeigt.

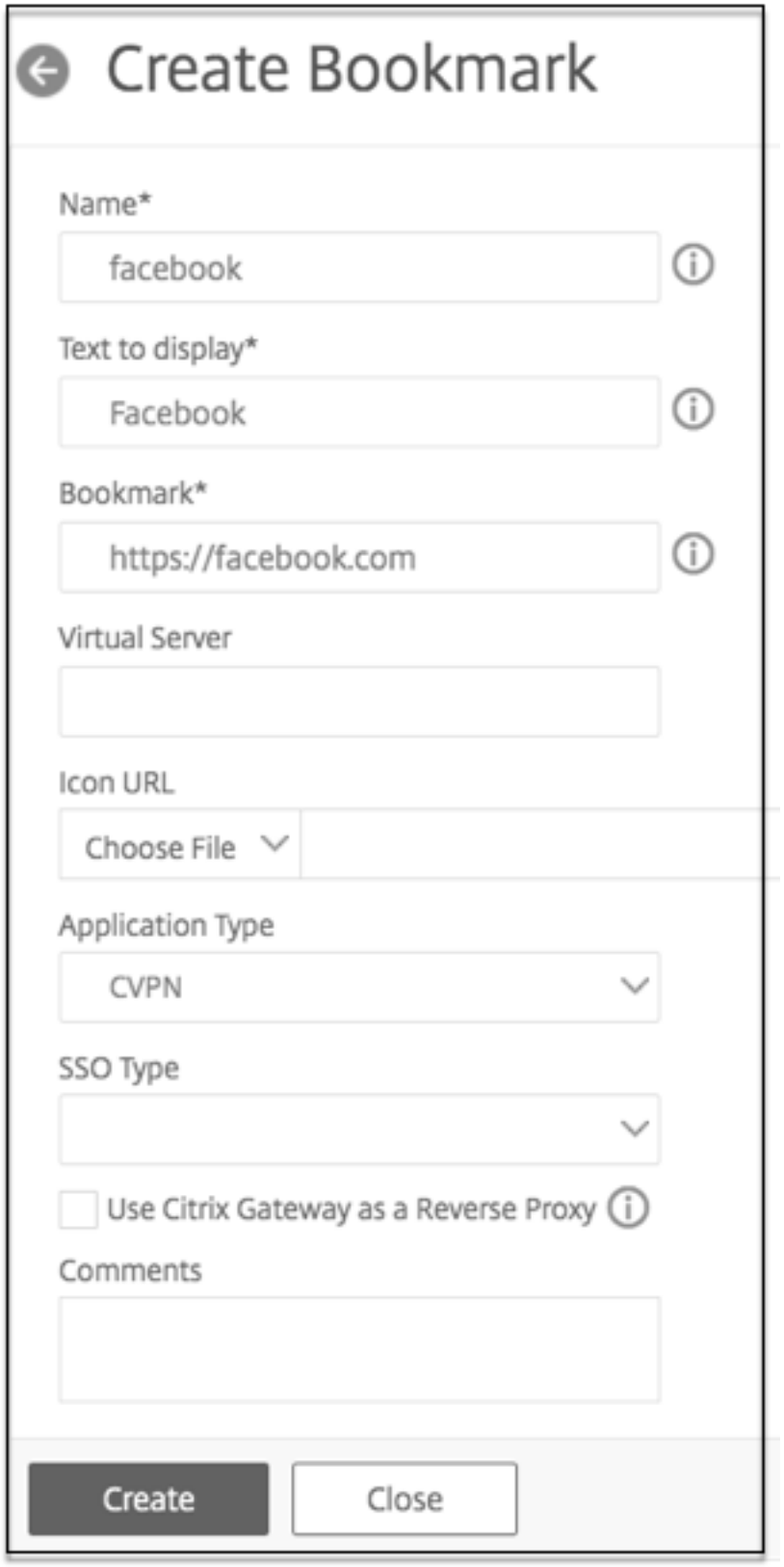
> **Wichtig:**
>
> Ab Citrix ADC Version 13.0 Build 64.xx werden Dateifreigaben über Citrix Gateway nicht unterstützt.

## Erstellen von Enterprise Lesezeichen

### So erstellen Sie einen Access Interface-Link in einer Sitzungsrichtlinie

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway > Ressourcen**, und klicken Sie dann auf **Portal-Lesezeichen.**
2. Klicken Sie im Detailbereich auf **Hinzufügen.**




3. Geben Sie **unter Name**einen Namen für das Lesezeichen ein.

4. Geben Sie im **Feld Anzuzeigender Text**die Beschreibung des Links ein. Die Beschreibung wird im **Access Interface angezeigt.**
5. Geben Sie im Feld **Lesezeichen**die Webadresse der Anwendung ein.
6. Geben Sie unter **Virtueller Server**den Namen des zugehörigen virtuellen Loadbalancing-/Content Switching-Servers ein. Das Feld ist optional.
7. In der **Icon-URL**werden die hochgeladenen Symbole für alle Designs außer dem Standarddesign unterstützt. Die empfohlene Maximalgröße beträgt 70x70 Pixel. Wir empfehlen die Verwendung transparenter Bilder. Das Feld ist optional.
8. Wählen Sie unter **Anwendungstyp**den Anwendungstyp (VPN, clientloses VPN oder SaaS) aus, für den die URL steht. Das Feld ist optional.
9. Wählen Sie unter **SSO-Typ** den SSO-Typ aus, den Sie für das Lesezeichen konfigurieren möchten. Wenn SSO konfiguriert ist, können Benutzer auf die Anwendungen zugreifen, ohne ihre Anmeldeinformationen bei den nachfolgenden Anmeldungen eingeben zu müssen. Die folgenden SSO-Typen werden unterstützt:

    - Unified Gateway: Diese SSO-Konfiguration ermöglicht den sicheren Remotezugriff auf mehrere Ressourcen einer Anwendung über eine einzige URL.
    - Selbstauthentifizierung: In dieser SSO-Konfiguration werden Citrix Gateway-Benutzer aufgefordert, die Anmeldeinformationen für den Zugriff auf die Anwendung einzugeben.
    - SAML-basierte Authentifizierung: In dieser SSO-Konfiguration verwendet Citrix Gateway einen IdP, um die Benutzerdetails zu validieren, generiert eine SAML-Assertion und sendet sie an den SP. Wenn die Validierung erfolgreich ist, ist das SSO erfolgreich.

    > **Hinweis:**
    >
    > Wenn Sie den clientlosen Zugriff aktivieren, können Sie sicherstellen, dass Anfragen an Websites über Citrix Gateway gesendet werden. Beispielsweise haben Sie ein Lesezeichen für Googlehinzugefügt. Aktivieren Sie das Kontrollkästchen **Citrix Gateway als Reverse-Proxy verwenden**. Wenn Sie dieses Kontrollkästchen aktivieren, werden Website-Anfragen vom Benutzergerät an Citrix Gateway und dann zur Website weitergeleitet. Wenn Sie das Kontrollkästchen deaktivieren, werden Anfragen vom Benutzergerät zur Website weitergeleitet. Dieses Kontrollkästchen ist nur verfügbar, wenn Sie den clientlosen Zugriff aktivieren.

10. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

#### So binden Sie einen Access Interface-Link

Sie können Access Interface-Links an die folgenden Speicherorte binden:

- Benutzer
- Gruppen
- Virtuelle Server

Nachdem Sie die Konfiguration gespeichert haben, stehen die Links Benutzern im Access Interface auf der Registerkarte **Home** zur Verfügung. Dies ist die erste Seite, die Benutzer sehen, nachdem sie sich erfolgreich angemeldet haben.

1. Führen Sie im Konfigurationsdienstprogramm im Navigationsbereich einen der folgenden Schritte aus:
    - Erweitern Sie **Citrix Gateway User Administration** und klicken Sie dann auf **AAA-Benutzer.**
    - Erweitern Sie **Citrix Gateway Benutzerverwaltung** und klicken Sie dann auf **AAA-Gruppen.**
    - Erweitern Sie **Citrix Gateway** und klicken Sie dann auf **Virtuelle Server.**
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
    - Wählen Sie einen Benutzer aus und klicken Sie dann auf Öffnen.
    - Wählen Sie eine Gruppe aus und klicken Sie dann auf Öffnen.
    - Wählen Sie einen virtuellen Server aus und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld auf die Registerkarte **Lesezeichen**.
4. Wählen Sie unter **Verfügbare Lesezeichen**ein oder mehrere Lesezeichen aus, klicken Sie auf den Pfeil nach rechts, um die Lesezeichen unter Konfigurierte Lesezeichen zu verschieben, und dann **auf OK.**

**So binden Sie Lesezeichen über die GUI global**

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen.**
2. Klicken Sie im Detailbereich unter **Lesezeichen**auf **Links zu den HTTP- und Windows-Dateifreigabe-Anwendungen erstellen, die Sie auf der Citrix Gateway-Portalseite zugänglich machen möchten**.


3. Klicken **Sie im Dialogfeld VPN Global Binding konfigurieren*** auf **Hinzufügen.**
4. Wählen Sie unter **Verfügbar**ein oder mehrere Lesezeichen aus, klicken Sie auf den Pfeil nach rechts, um die Lesezeichen unter Konfiguriert und dann **auf OK**zu verschieben.

#### So fügen Sie über die CLI ein Enterprise-Lesezeichen hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
<!--NeedCopy-->
```

**Beispiel:**

Web-Lesezeichen

```
add vpn url google google "https://www.google.com"
<!--NeedCopy-->
```

#### So binden Sie ein Enterprise-Lesezeichen über die CLI

Sie können Enterprise-Lesezeichen an Benutzer-, Gruppen-, virtuelle Server- und globale Ebene binden.

```
bind aaa user <userName> -urlName <string>
bind aaa group <groupName> -urlName <string>
bind vpn vserver <vserverName> -urlName <string>
bind vpn global  – urlName <string>
<!--NeedCopy-->
```

**Beispiel:**

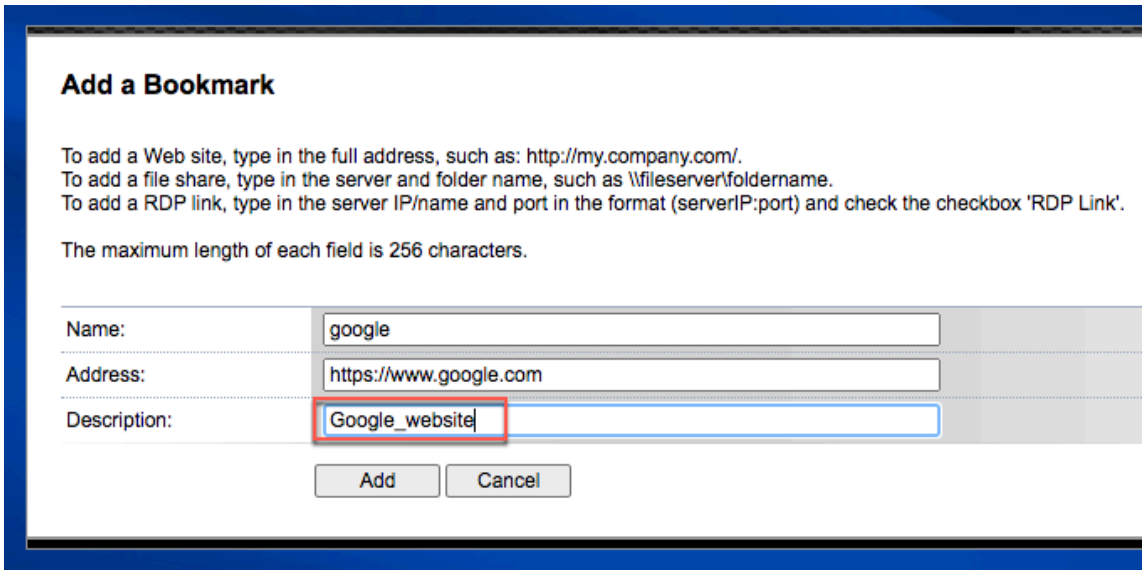
```
bind vpn global -urlName google
<!--NeedCopy-->
```

### Erstellen persönlicher Lesezeichen

Sie können persönliche Websites nur vom virtuellen VPN-Server aus erstellen. Es gibt keine Citrix Gateway-Administrator-GUI zum Hinzufügen persönlicher Lesezeichen.

1. Melden Sie sich bei einem virtuellen VPN-Server an.
2. Klicken Sie auf **Netzwerkzugriff** oder **Clientloser Zugriff**, um ein Lesezeichen hinzuzufügen.
3. Klicken Sie auf **Hinzufügen**.


4. Geben Sie die Details des Lesezeichens wie Name, Adresse und Beschreibung der Website ein.



5. Klicken Sie auf **Hinzufügen**.

Die Websites, die Sie hinzugefügt haben, werden unter den entsprechenden Registerkarten angezeigt.


### Konfigurieren von Benutzernamen-Token in Lesezeichen

Sie können Lesezeichen- und Dateifreigabe-URLs mit einem speziellen Token konfigurieren,%username%. Wenn sich Benutzer anmelden, wird das Token durch den Anmeldenamen jedes Benutzers ersetzt. Beispielsweise erstellen Sie ein Lesezeichen für einen Mitarbeiter namens Jack für einen Ordner als\\ EmployeeServer\%username%\. Wenn sich Jack anmeldet, wird die Dateifreigabe-URL\\ EmployeeServer\ Jack\ zugeordnet. Beachten Sie beim Konfigurieren von Benutzernamen-Token in Lesezeichen die folgenden Situationen:

- Wenn Sie einen Authentifizierungstyp verwenden, ersetzt der Benutzername das Token%username%.
- Wenn Sie die Zwei-Faktor-Authentifizierung verwenden, wird der Benutzername vom primären Authentifizierungstyp verwendet, um dasusername%% -Token zu ersetzen.
- Wenn Sie die Clientzertifikatauthentifizierung verwenden, wird das Feld Benutzername im Clientzertifikatauthentifizierungsprofil verwendet, um dasusername%% -Token zu ersetzen.

## Datenverkehrsrichtlinien

March 27, 2024

Mit Verkehrsrichtlinien können Sie die folgenden Einstellungen für Benutzerverbindungen konfigurieren:

- Erzwingen kürzerer Timeouts für sensible Anwendungen, auf die von nicht vertrauenswürdigen Netzwerken aus zugegriffen wird.
- Umschalten des Netzwerkverkehrs zur Verwendung von TCP für einige Anwendungen. Wenn Sie TCP auswählen, müssen Sie Single Sign-On für bestimmte Anwendungen aktivieren oder deaktivieren.
- Identifizieren von Situationen, in denen Sie andere HTTP-Funktionen für den Citrix Gateway-Plug-in-Verkehr verwenden möchten.
- Definieren der Dateinamenerweiterungen, die mit der Dateitypzuordnung verwendet werden.

### Erstellen Sie eine Verkehrsrichtlinie

Um eine Verkehrsrichtlinie zu konfigurieren, erstellen Sie ein Profil und konfigurieren die folgenden Parameter:

- Protokoll (HTTP oder TCP)
- Zeitüberschreitung der Anwendung
- Einmaliges Anmelden bei Webanwendungen
- Formular einmaliges Anmelden
- Dateitypzuordnungen
- Repeater-Plug-In
- Kerberos Constrained Delegierte (KCD) Konten

Nachdem Sie die Verkehrsrichtlinie erstellt haben, können Sie die Richtlinie an virtuelle Server, Benutzer, Gruppen oder global binden.

Beispielsweise haben Sie die Webanwendung PeopleSoft Human Resources auf einem Server im internen Netzwerk installiert. Sie können eine Verkehrsrichtlinie für diese Anwendung erstellen, die die Ziel-IP-Adresse und den Zielport definiert, und Sie können festlegen, wie lange ein Benutzer bei der Anwendung angemeldet bleiben kann, z. B. 15 Minuten.

Wenn Sie andere Funktionen wie die HTTP-Komprimierung für eine Anwendung konfigurieren möchten, können Sie eine Verkehrsrichtlinie verwenden, um die Einstellungen zu konfigurieren. Verwenden Sie beim Erstellen der Richtlinie den HTTP-Parameter für die Aktion. Erstellen Sie im Ausdruck die Zieladresse für den Server, auf dem die Anwendung ausgeführt wird.

#### Beispiele für Ausdrücke in Verkehrsrichtlinien

Im Folgenden sind die Ausdrucksbeispiele für Datenverkehrsrichtlinien aufgeführt:

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\")|| HTTP.REQ.URL.CONTAINS(\"10.102.\")")"trafAct1`
- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\")|| HTTP.REQ.URL.CONTAINS(\"homePage\"))"trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

#### Konfigurieren einer Verkehrsrichtlinie über die GUI

1. Erweitern Sie **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Verkehr**.
2. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Traffic Policy erstellen** in das Feld **Name** einen Namen für die Richtlinie ein.
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. **Geben Sie im Feld Name einen Namen für das Profil ein.**
6. Wählen Sie im **Protokoll**entweder **HTTP** oder **TCP**aus.

   **Hinweis:** Wenn Sie TCP als Protokoll auswählen, können Sie Single Sign-On nicht konfigurieren und die Einstellung ist im Profildialogfeld deaktiviert.
7. Geben Sie in **AppTimeout (Minuten)**die Anzahl der Minuten ein. Diese Einstellung begrenzt die Zeit, die Benutzer bei der Webanwendung angemeldet bleiben können.
8. Um Single Sign-on bei der Webanwendung zu aktivieren, wählen Sie unter **Single Sign-On** die Option **ON**aus.

Hinweis : Wenn Sie formularbasiertes Single Sign-On verwenden möchten, können Sie die Einstellungen im Verkehrsprofil konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von formularbasiertem Single Sign-On.

9. Um eine Dateitypzuordnung anzugeben, wählen Sie unter **Dateitypzuordnung** die Option **ON** aus.
10. Um das Repeater-Plug-In zur Optimierung des Netzwerkverkehrs zu verwenden, wählen Sie in Citrix SD-WAN **ON** aus, klicken Sie auf **Erstellen** und dann auf **Schließen**.
11. Wenn Sie KCD auf der Appliance konfigurieren, wählen Sie im KCD-Konto das Konto aus.

    Weitere Informationen zur Konfiguration von KCD auf der Appliance finden Sie unter Konfigurieren von Kerberos Constrained Delegation auf einer NetScaler Appliance.
12. Erstellen Sie im Dialogfeld Verkehrsrichtlinie erstellen einen Ausdruck, oder fügen Sie ihn hinzu, klicken Sie auf **Erstellen** und dann auf **Schließen**.

## Konfigurieren Sie formularbasiertes einmaliges Anmelden

Formularbasiertes Single Sign-On ermöglicht es Benutzern, sich einmalig bei allen geschützten Anwendungen in Ihrem Netzwerk anzumelden. Wenn Sie formularbasiertes Single Sign-On in Citrix Gateway konfigurieren, können Benutzer auf Webanwendungen zugreifen, die eine formularbasierte HTML-Anmeldung erfordern, ohne ihr Kennwort erneut eingeben zu müssen. Ohne einmaliges Anmelden müssen sich Benutzer separat anmelden, um auf jede Anwendung zugreifen zu können.

Nachdem Sie das Profil für einmaliges Anmelden des Formulars erstellt haben, erstellen Sie dann ein Verkehrsprofil und eine Richtlinie, die das Profil für einmaliges Anmelden des Formulars enthält. Weitere Informationen finden Sie unter Erstellen einer Verkehrsrichtlinie.

### Konfigurieren Sie formularbasiertes einmaliges Anmelden

1. Erweitern Sie **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Traffic**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Formular-SSO-Profile** und dann auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für das Profil ein.**
4. Geben Sie unter **Aktions-URL** die URL ein, an die das ausgefüllte Formular gesendet wird.

   **Hinweis:** Die URL ist die relative Stamm-URL.
5. Geben Sie unter **Benutzername**den Namen des Attributs für das Feld Benutzername ein.
6. Geben Sie unter **Kennwort**den Namen des Attributs für das Kennwortfeld ein.

7. Erstellen Sie in der **SSO-Erfolgsregel**einen Ausdruck, der die Aktion beschreibt, die dieses Profil ausführt, wenn es durch eine Richtlinie aufgerufen wird. Sie können den Ausdruck auch mithilfe der Schaltflächen Präfix, Hinzufügen und Operator unter diesem Feld erstellen.

   Diese Regel überprüft, ob das Single Sign-On erfolgreich ist oder nicht.

8. Geben Sie **unter Name Value Pair**den Wert des Benutzernamens ein, gefolgt von einem kaufmännischen Und (&) und dann dem Wert des Kennwortfelds.

   Wertnamen werden durch ein kaufmännisches und (&) getrennt, wie name1=Wert1&name2=Wert2.

9. Geben Sie unter **Response Size**die Anzahl Byte ein, um die vollständige Antwortgröße zu ermöglichen. Geben Sie die Anzahl der Byte in der Antwort ein, die für das Extrahieren der Formulare analysiert werden sollen.
10. Wählen Sie unter **Extraktion**aus, ob das Name/Wert-Paar statisch oder dynamisch ist. Die Standardeinstellung ist Dynamisch.
11. Wählen Sie unter **Submit Method**die HTTP-Methode aus, die vom Formular für einmaliges Anmelden verwendet wird, um die Anmeldeinformationen an den Anmeldeserver zu senden. Die Standardeinstellung ist "Hole".
12. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

## Konfigurieren von SAML-Single-Sign-On

Sie können ein SAML 1.1- oder SAML 2.0-Profil für Single Sign-On (SSO) erstellen. Benutzer können eine Verbindung zu Webanwendungen herstellen, die das SAML-Protokoll für einmaliges Anmelden unterstützen. Citrix Gateway unterstützt das einmalige Anmelden des Identitätsanbieters (IdP) für SAML-Webanwendungen.

### Konfigurieren von SAML-Single-Sign-On

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway\ > Richtlinien**, und klicken Sie dann auf Verkehr.
2. Klicken Sie im Detailbereich auf die Registerkarte SAML SSO-Profil.
3. Klicken Sie im Detailbereich auf "Hinzufügen".
4. Geben Sie im Feld Name einen Namen für das Profil ein.
5. Geben Sie unter Signaturzertifikatname den Namen des X.509-Zertifikats ein.
6. Geben Sie unter ACS-URL den Assertion-Verbraucherdienst des Identitätsanbieters oder Dienstanbieters ein. Die AssertionConsumerServiceURL (ACS-URL) bietet SSO-Funktionen für Benutzer.
7. Erstellen Sie in Relay State Rule den Ausdruck für die Richtlinie aus Gespeicherten Richtlinienausdrücken und häufig verwendeten Ausdrücken. Wählen Sie aus der Liste Operator aus, um

zu definieren, wie der Ausdruck ausgewertet wird. Um den Ausdruck zu testen, klicken Sie auf Evaluieren.
8. Wählen Sie unter Kennwort senden ON oder OFF.
9. Geben Sie unter Name des Ausstellers die Identität für die SAML-Anwendung ein.
10. Klicken Sie auf Erstellen und dann auf Schließen.

## Binden Sie eine Verkehrsrichtlinie

Sie können Verkehrsrichtlinien an virtuelle Server, Gruppen, Benutzer und an Citrix Gateway Global binden. Sie können das Konfigurationsdienstprogramm verwenden, um eine Verkehrsrichtlinie zu binden.

### Binden Sie eine Verkehrsrichtlinie global über die GUI

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf Traffic.
2. Wählen Sie im Detailbereich eine Richtlinie aus und klicken Sie dann unter Aktion auf Globale Bindungen.
3. Klicken Sie im Dialogfeld Traffic-Richtlinien binden/aufheben unter Details auf Richtlinie einfügen.
4. Wählen Sie unter Richtlinienname die Richtlinie aus, und klicken Sie dann auf OK.

## Verkehrsrichtlinien entfernen

Sie können entweder das Konfigurationsdienstprogramm verwenden, um Verkehrsrichtlinien von Citrix Gateway zu entfernen. Wenn Sie das Konfigurationsdienstprogramm verwenden, um eine Verkehrsrichtlinie zu entfernen, und die Richtlinie an die Benutzer-, Gruppen- oder virtuelle Serverebene gebunden ist, müssen Sie zuerst die Richtlinie aufheben. Dann können Sie die Richtlinie entfernen.

### Entbinden einer Verkehrsrichtlinie über die GUI

1. Erweitern Sie **Citrix Gateway,** und klicken Sie dann auf **Virtuelle Server**.
    - **Erweitern Sie Citrix Gateway > Benutzerverwaltung**und klicken Sie dann auf **AAA-Gruppen**.
    - Erweitern Sie **Citrix Gateway > Benutzerverwaltung** und klicken Sie dann auf **AAA-Benutzer**.

2. Wählen Sie im Detailbereich einen virtuellen Server, eine Gruppe oder einen Benutzer aus und klicken Sie dann auf **Öffnen**.
3. Klicken **Sie im Dialogfeld Citrix Gateway Virtual Server konfigurieren, AAA-Gruppekonfigurieren oder AAA-Benutzer**konfigurieren auf die Registerkarte**Richtlinien**.
4. Klicken Sie auf **Traffic**, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Richtlinie aufheben**.
5. Klicken Sie auf **OK** und dann auf **Schließen**.

Nachdem die Verkehrsrichtlinie nicht gebunden ist, können Sie die Richtlinie entfernen.

#### Entfernen einer Verkehrsrichtlinie über die GUI

1. Erweitern Sie **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Traffic**.
2. Wählen Sie im Detailbereich auf der Registerkarte Richtlinien die Verkehrsrichtlinie aus, und klicken Sie dann auf **Entfernen**.

## Sitzungsrichtlinien

March 27, 2024

Eine Sitzungsrichtlinie ist eine Sammlung von Ausdrücken und Einstellungen, die auf Benutzer, Gruppen, virtuelle Server und global angewendet werden.

Sie verwenden eine Sitzungsrichtlinie, um die Einstellungen für Benutzerverbindungen zu konfigurieren. Sie können Einstellungen definieren, um die Software zu konfigurieren, mit der sich Benutzer anmelden. Zum Beispiel das Citrix Gateway-Plug-In für Windows oder das Citrix Gateway-Plug-In für Mac. Sie können Einstellungen auch so konfigurieren, dass Benutzer sich mit der Citrix Workspace-App oder Secure Hub anmelden müssen. Nachdem der Benutzer authentifiziert wurde, werden die Sitzungsrichtlinien bewertet und angewendet.

Sitzungsrichtlinien werden gemäß den folgenden Regeln angewendet:

- Sitzungsrichtlinien überschreiben immer globale Einstellungen in der Konfiguration.
- Alle Attribute oder Parameter, die nicht mithilfe einer Sitzungsrichtlinie festgelegt wurden, werden für Richtlinien festgelegt, die für den virtuellen Server festgelegt wurden.
- Die globale Konfiguration legt andere Attribute fest, die nicht von einer Sitzungsrichtlinie oder dem virtuellen Server festgelegt werden.

> **Wichtig:**
>
> Die folgenden Anweisungen sind allgemeine Richtlinien zum Erstellen von Sitzungsrichtlinien.

> Es gibt spezielle Anweisungen zum Konfigurieren von Sitzungsrichtlinien für verschiedene Konfigurationen, wie zum Beispiel clientlosen Zugriff oder für den Zugriff auf veröffentlichte Anwendungen. Die Anweisungen können Anweisungen zum Konfigurieren einer bestimmten Einstellung enthalten. Diese Einstellung kann jedoch eine von vielen Einstellungen sein, die in einem Sitzungsprofil und einer Richtlinie enthalten sind.

Wenn Sie Citrix Endpoint Management oder StoreFront in Ihrem Netzwerk bereitstellen, empfiehlt Citrix, den Schnellkonfigurations-Assistenten zum Konfigurieren von Sitzungsrichtlinien und -profilen zu verwenden. Wenn Sie den Assistenten ausführen, definieren Sie die Einstellungen für Ihre Bereitstellung. Citrix Gateway erstellt dann die erforderlichen Authentifizierungs-, Sitzungs- und clientlosen Zugriffsrichtlinien.

## Erstellen einer Sitzungsrichtlinie

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf Sitzung.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf Neu.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Füllen Sie die Einstellungen für das Sitzungsprofil aus und klicken Sie dann auf Erstellen.
7. Fügen Sie im Dialogfeld Sitzungsprofil erstellen einen Ausdruck für die Richtlinie hinzu, klicken Sie auf Erstellen und dann auf Schließen.
   Hinweis: Wählen Sie im Ausdruck den Wert Wahr aus, damit die Richtlinie immer auf die Ebene angewendet wird, an die sie gebunden ist.

### Beispiel für Ausdrücke für Sitzungsrichtlinien

Im Folgenden finden Sie Ausdrucksbeispiele für Sitzungsrichtlinien:

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")|| HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")"sessAct1`
- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT"sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

## Binden von Sitzungsrichtlinien

Nachdem Sie eine Sitzungsrichtlinie erstellt haben, binden Sie sie an einen Benutzer, eine Gruppe, einen virtuellen Server oder global. Sitzungsrichtlinien werden in der folgenden Reihenfolge als Hierarchie angewendet:

- Benutzer
- Gruppen
- Virtuelle Server
- Weltweit

### Binden einer Sitzungsrichtlinie über die GUI an einen virtuellen Server

1. Navigieren Sie zu **Citrix Gateway > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**. Sie können auch einen neuen virtuellen Server erstellen.
3. Scrollen Sie nach unten zum Abschnitt **Richtlinien** und klicken Sie auf das Symbol **+**.
4. Wählen Sie unter **Richtlinie wählen** die Option **Sitzung** aus.
5. Wählen Sie unter **Typ wählen** die Option **Anforderung** aus und klicken Sie auf **Weiter**.
6. Wählen Sie unter **Richtlinie auswählen** die Richtlinie aus, die Sie an diesen virtuellen Server binden möchten.
7. Geben Sie unter **Priorität** die Prioritätsnummer der Richtlinie ein.
8. Klicken Sie auf **Bind**.

### Binden einer Sitzungsrichtlinie über die GUI an eine Authentifizierungs-, Autorisierungs- und Überwachungsgruppe

1. Navigieren Sie zu **Citrix Gateway > Benutzerverwaltung > AAA-Gruppen**.
2. Wählen Sie eine vorhandene Authentifizierungs-, Autorisierungs- und Überwachungsgruppe aus und klicken Sie auf **Bearbeiten**. Sie können auch eine Authentifizierungs-, Autorisierungs- und Überwachungsgruppe erstellen.
3. Klicken Sie in den **Erweiterten Einstellungen** auf **Richtlinien** und dann auf das Symbol **+**.
4. Wählen Sie unter **Richtlinie auswählen** die Option **Sitzung** aus und klicken Sie auf **Weiter**.
5. Wählen Sie unter **Richtlinie auswählen** die Richtlinie aus, die Sie an diese Authentifizierungs-, Autorisierungs- und Überwachungsgruppe binden möchten.
6. Geben Sie unter **Priorität** die Prioritätsnummer der Richtlinie ein.
7. Klicken Sie auf **Bind**.

#### Binden einer Sitzungsrichtlinie über die GUI an einen Authentifizierungs-, Autorisierungs- und Überwachungsbenutzer

1. Navigieren Sie zu **Citrix Gateway > Benutzerverwaltung > AAA-Benutzer**.
2. Wählen Sie einen vorhandenen Citrix ADC-Benutzer aus und klicken Sie auf **Bearbeiten**. Sie können auch einen Authentifizierungs-, Autorisierungs- und Überwachungsbenutzer erstellen.
3. Klicken Sie in den **Erweiterten Einstellungen** auf **Richtlinien** und dann auf das Symbol **+**.
4. Wählen Sie unter **Richtlinie auswählen** die Option **Sitzung** aus und klicken Sie auf **Weiter**.
5. Wählen Sie unter **Richtlinie auswählen** die Richtlinie aus, die Sie an diesen Authentifizierungs-, Autorisierungs- und Überwachungsbenutzer binden möchten.
6. Geben Sie unter **Priorität** die Prioritätsnummer der Richtlinie ein.
7. Klicken Sie auf **Bind**.

**Hinweis**: Einzelheiten zur Priorität finden Sie unter https://support.citrix.com/article/CTX214588.

### Erstellen Sie ein Sitzungsprofil

Ein Sitzungsprofil enthält die Einstellungen für Benutzerverbindungen.

Sitzungsprofile geben die Aktionen an, die auf eine Benutzersitzung angewendet werden, wenn das Benutzergerät die Bedingungen für den Richtlinienausdruck erfüllt. Profile werden mit Sitzungsrichtlinien verwendet. Sie können das Konfigurationsdienstprogramm verwenden, um Sitzungsprofile getrennt von einer Sitzungsrichtlinie zu erstellen und das Profil dann für mehrere Richtlinien zu verwenden. Sie können nur ein Profil mit einer Richtlinie verwenden.

#### Konfigurieren von Netzwerkeinstellungen für Benutzerverbindungen in einem Sitzungsprofil

Sie können die Registerkarte **Netzwerkkonfiguration** im Sitzungsprofil verwenden, um die folgenden Netzwerkeinstellungen für Benutzerverbindungen zu konfigurieren:

- DNS-Server
- WINS-Server-IP-Adresse
- Zugeordnete IP-Adresse, die Sie als Intranet-IP-Adresse verwenden können
- Spillover-Einstellungen für Adresspools (Intranet-IP-Adressen)
- Intranet-IP-DNS-Suffix
- HTTP-Anschlüsse
- Erzwungene Timeout-

### Konfigurieren von Verbindungseinstellungen in einem Sitzungsprofil

Sie können die Registerkarte „ **Kundenerlebnis** “im Sitzungsprofil verwenden, um die folgenden Verbindungseinstellungen zu konfigurieren:

- Access Interface oder angepasste Homepage
- Webadresse für webbasierte E-Mails wie Outlook Web Access
- Plug-in-Typ (Citrix Gateway Plug-in für Windows, Citrix Gateway Plug-in für macOS X oder Citrix Gateway Plug-in für Java)
- Split-Tunneling
- Einstellungen für Sitzung und Leerlauf-Timeout
- Clientloser Zugriff
- URL-Kodierung für clientlosen Zugriff
- Plug-in-Typ (Windows, Mac oder Java)
- Einmaliges Anmelden bei Webanwendungen
- Berechtigungsindex für die Authentifizierung
- Einmaliges Anmelden mit Windows
- Verhalten bei der Clientbereinigung
- Anmeldeskripts
- Client-Debug-Einstellungen
- Split DNS
- Zugriff auf private Netzwerk-IP-Adressen und lokalen LAN-Zugriff
- Wahlmöglichkeiten für Clients
- Proxy-Einstellungen

Weitere Informationen zum Konfigurieren von Einstellungen für Benutzerverbindungen finden Sie unter Konfigurieren von Verbindungen für das Citrix Gateway Plug-in.

### Konfigurieren von Sicherheitseinstellungen in einem Sitzungsprofil

Sie können die Registerkarte **Sicherheit** in einem Sitzungsprofil verwenden, um die folgenden Sicherheitseinstellungen zu konfigurieren:

- Standard-Autorisierungsaktion (erlauben oder verweigern)
- Secure Browse nach Verbindungen von iOS-Geräten
- Quarantäne-Gruppen
- Berechtigungsgruppen

Weitere Informationen zum Konfigurieren der Autorisierung auf Citrix Gateway finden Sie unter Konfigurieren der Autorisierung.

### Konfigurieren der Einstellungen für Citrix Virtual Apps and Desktops in einem Sitzungsprofil

Sie können die Registerkarte **Veröffentlichte Anwendungen** in einem Sitzungsprofil verwenden, um die folgenden Einstellungen für Verbindungen zu Servern zu konfigurieren, auf denen Citrix Virtual Apps and Desktops ausgeführt wird:

- ICA-Proxy, bei dem es sich um Clientverbindungen mit der Citrix Workspace-App handelt
- Webinterface-Adresse
- Webinterface-Portalmodus
- Einmaliges Anmelden bei der Serverfarmdomäne
- Homepage der Citrix Workspace-App
- Adresse der Kontodienste

  Weitere Informationen finden Sie unter Bereitstellen des Zugriffs auf veröffentlichte Anwendungen und virtuelle Desktops über das Webinterface.

Sie können Sitzungsprofile unabhängig von einer Sitzungsrichtlinie erstellen. Wenn Sie die Richtlinie erstellen, können Sie das Profil auswählen, das an die Richtlinie angehängt werden soll.

#### So erstellen Sie über die GUI ein Sitzungsprofil

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Profile** und dann auf **Hinzufügen**.
3. Konfigurieren Sie die Einstellungen für das Profil.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Nachdem Sie ein Profil erstellt haben, können Sie es in eine Sitzungsrichtlinie aufnehmen.

#### So fügen Sie über die GUI ein Profil zu einer Sitzungsrichtlinie hinzu

1. Erweitern Sie im Konfigurationsprogramm im Navigationsbereich **Access Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Führen Sie auf der Registerkarte **Richtlinien** eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, um eine Sitzungsrichtlinie zu erstellen
   - Wählen Sie eine Richtlinie aus und klicken Sie dann auf **Öffnen**.
3. Wählen Sie **unter Profil anfordern**ein Profil aus der Liste aus.
4. Beenden Sie die Konfiguration der Sitzungsrichtlinie und führen Sie dann einen der folgenden Schritte aus:

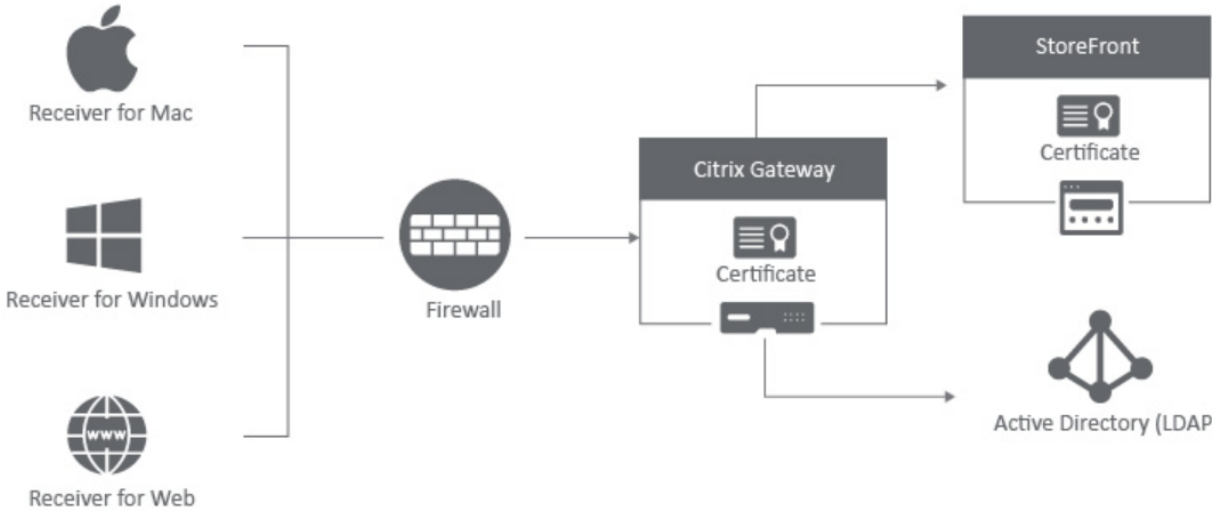
 

a) Klicken Sie auf **Erstellen** und dann auf **Schließen**, um die Richtlinie zu erstellen.
b) Klicken Sie auf **OK** und dann auf **Schließen**, um die Richtlinie zu ändern.

## Citrix Gateway-Sitzungsrichtlinien für StoreFront konfigurieren

March 27, 2024

In diesem Artikel wird beschrieben, wie Sie eine Authentifizierung nur für Citrix Gateway-Domäne mit StoreFront für Benutzer konfigurieren, die die Citrix Workspace-App oder einen Webbrowser verwenden.




### Mindestanforderungen

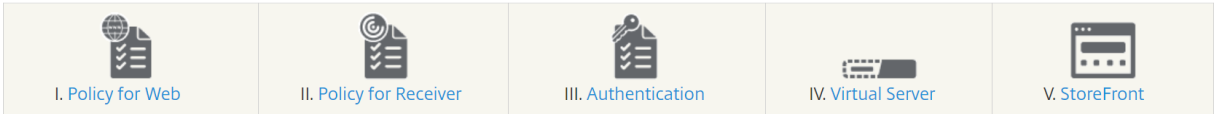
- Citrix StoreFront 2.x oder 3.0
- Citrix ADC 10.5 und höher
- Citrix Workspace-App für Windows 4.x
- Citrix Workspace-App für Mac 11.8
- Webbrowser (Citrix Workspace-App für Web)
- Auf der Citrix ADC Appliance konfigurierte Authentifizierung wie in CTX108876 beschrieben - Konfigurieren der LDAP-Authentifizierung auf einer Citrix ADC Appliance
- Für StoreFront Server und Citrix Gateway konfigurierte SSL-Zertifikate. Einzelheiten zu den folgenden Themen finden Sie unter StoreFront-Dokumentation.

  - Installation und Einrichtung für StoreFront 2.6

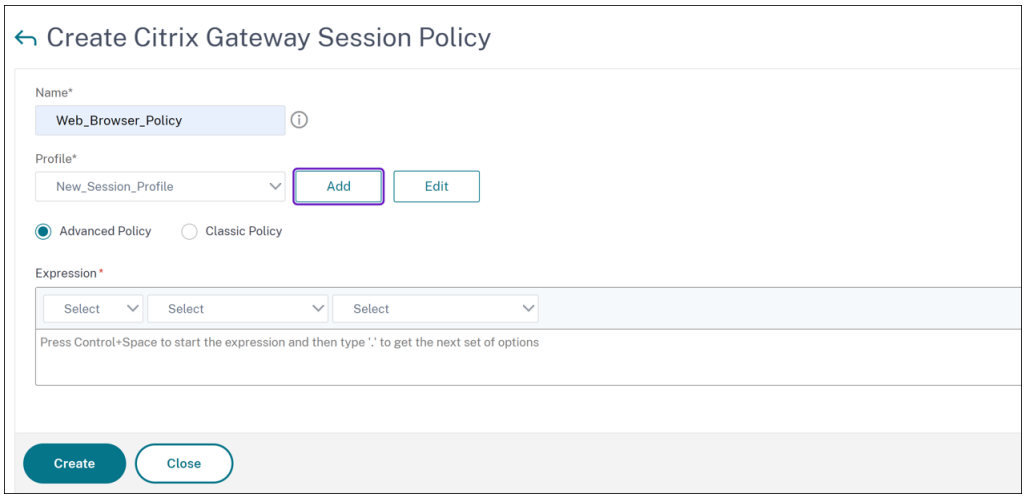
- Windows 2012 Serverzertifikate
- So fügen Sie eine SSL-Bindung zu einer Site hinzu
- Installieren und Verwalten von Zertifikaten für Citrix ADC Appliance 10.5

## Konfigurieren von Citrix Gateway mit StoreFront




### Sitzungsrichtlinie für den webbrowserbasierten Zugriff erstellen

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Sitzung**.
2. Klicken Sie auf der Registerkarte **Sitzungsrichtlinien** auf **Hinzufügen**.
3. Geben Sie **unter Name**den Namen der Sitzungsrichtlinie ein. Zum Beispiel Web_Browser_Policy.
4. Klicken Sie in **Profil**auf **Hinzufügen**. Die Seite **Citrix Gateway-Sitzungsrichtlinie erstellen** wird angezeigt.
5. Aktualisieren Sie die erforderlichen Felder und klicken Sie auf **Erstellen**.




6. Wählen Sie auf der Seite **Citrix Gateway-Sitzungsrichtlinien und Profile** die Sitzungsrichtlinie aus.
7. Um ein Sitzungsprofil hinzuzufügen, gehen Sie zum Feld **Profil** und klicken Sie auf **Hinzufügen**. Die Seite **Citrix Gateway-Sitzungsprofil erstellen** wird angezeigt.

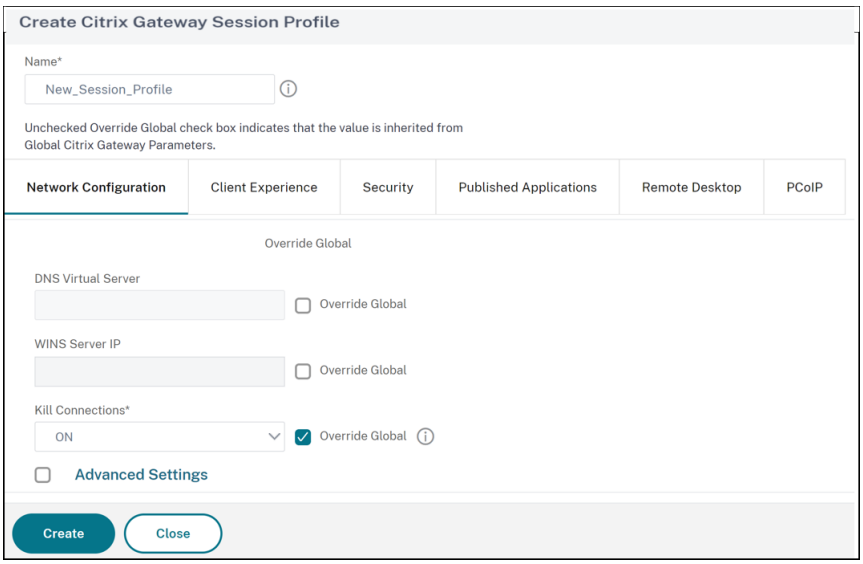
   Weisen Sie dem Sitzungsprofil einen Namen zu. Sie können die Kontrollkästchen **Override Global** auf allen Registerkarten aktivieren, um die geerbten Werte aus den globalen Citrix

Gateway-Parametern zu überschreiben.
Das folgende Konfigurationsbeispiel beschreibt die obligatorischen Parameter:

8. Konfigurieren Sie auf der Registerkarte **Netzwerkkonfiguration** die folgenden Einstellungen:

   - **Verbindungen**beenden : Geben Sie an, ob Citrix Gateway die Verbindungen trennen muss, die vor der Anmeldung des Benutzers bei Citrix Gateway bestanden, und eingehende Verbindungen verhindern muss, wenn der Benutzer verbunden ist und Split-Tunneling deaktiviert ist.



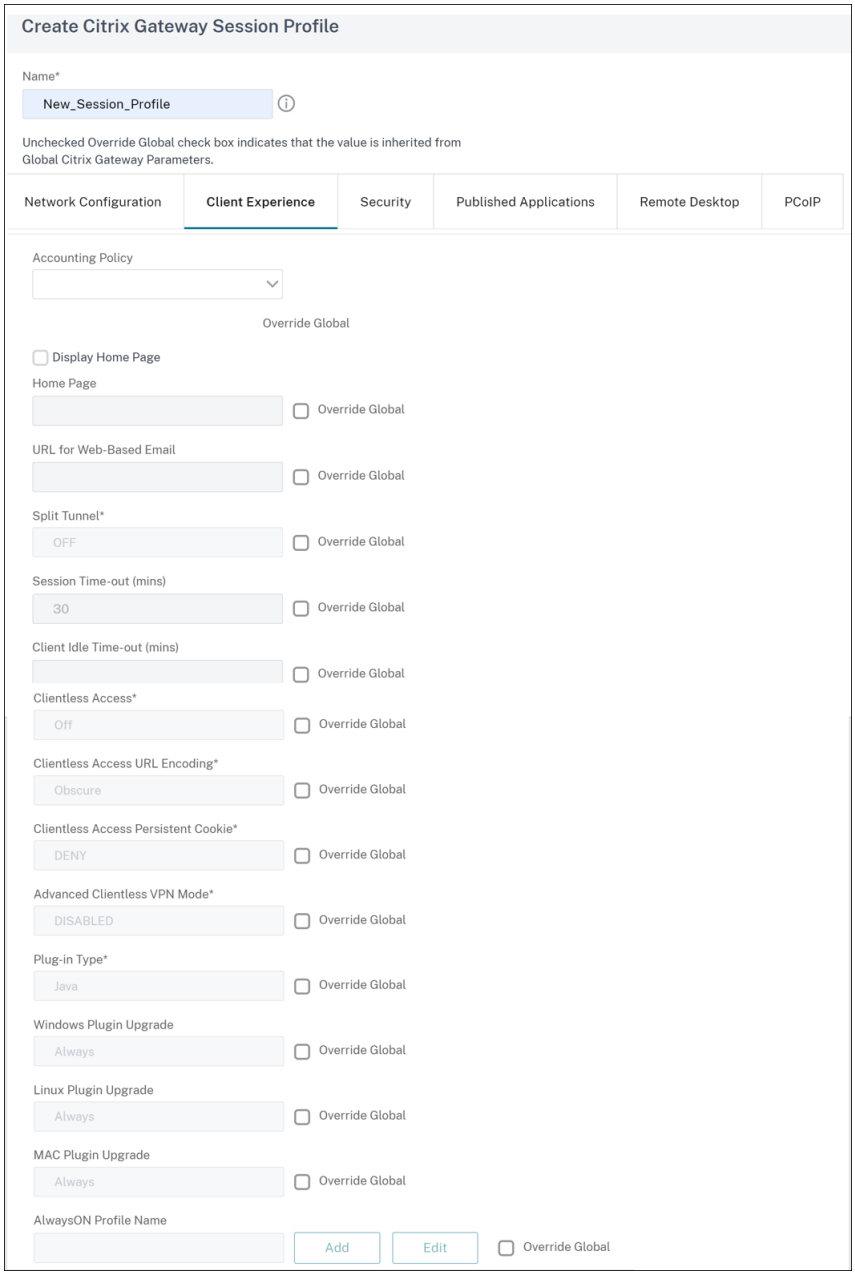

9. Konfigurieren Sie auf der Registerkarte **Client Experience** die folgenden Einstellungen:

   - **Split-Tunnel**: Tunnelt den Verkehr nur für Intranetanwendungen, die in Citrix Gateway definiert sind. Leitet den gesamten anderen Datenverkehr direkt ins Internet weiter.
   - **Clientloser Zugriff**: Wenn diese Option auf **ALLOW** gesetzt ist, können Sie auf Anwendungen zugreifen, ohne den Citrix Secure Access Client zu installieren.
   - **URL-Codierung für clientlosen Zugriff**: Wenn der clientlose Zugriff aktiviert ist, können Sie die Adressen interner Webanwendungen verschlüsseln oder die Adresse als Klartext belassen.
   - **Dauerhafter Cookie für clientlosen Zugriff**: Stellen Sie diese Option auf **Zulassen** ein, um den Status persistenter Cookies im clientlosen Zugriffsmodus anzuzeigen. Ein dauerhaftes Cookie verbleibt auf dem Benutzergerät und wird mit jeder HTTP-Anforderung gesendet.
   - **Erweiterter clientloser VPN-Modus**: Aktiviert oder deaktiviert den erweiterten clientlosen VPN-Modus. Die STRICT-Option blockiert den klassischen clientlosen VPN-Modus, wenn der erweiterte clientlose Modus verwendet wird.

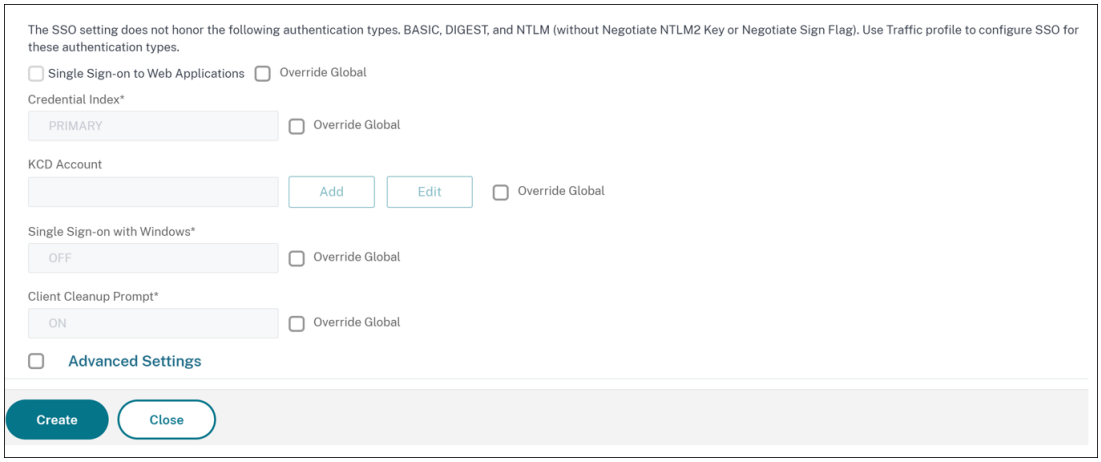
 

- **Plug-in-Typ**: Ermöglicht den Zugriff auf Netzwerkressourcen mithilfe einer einzigen IP-Adresse und Subnetzmaske oder mithilfe eines IP-Adressbereichs. Wenn diese Option deaktiviert ist, setzt Citrix Gateway den Modus auf Proxy, in dem Sie die Quell- und Ziel-IP-Adressen sowie die Portnummern konfigurieren.
- **Einmaliges Anmelden bei der Webanwendung**: Aktivieren Sie diese Option, um Single Sign-On (SSO) für eine Sitzung einzurichten. Wenn der Benutzer auf einen Server zugreift, werden die Anmeldeinformationen des Benutzers zur Authentifizierung an den Server umgeleitet.
- **Anmeldeinformationsindex**: Geben Sie an, ob Sie die primäre Authentifizierung oder die sekundären Anmeldeinformationen für die einmalige Anmeldung am Server verwenden möchten.
- **Single Sign-On mit Windows**: Aktiviert oder deaktiviert die automatische Windows-Anmeldung für eine Sitzung. Wenn nach der Aktivierung dieser Einstellung eine VPN-Sitzung eingerichtet wird, wird der Benutzer nach dem Neustart des Systems automatisch mit Windows-Anmeldeinformationen angemeldet.
- **Aufforderung**zur Clientbereinigung : Stellen Sie diese Option ein, wenn Citrix Gateway Sie zu einer clientseitigen Cache-Bereinigung auffordern soll, wenn eine vom Client initiierte Sitzung geschlossen wird.

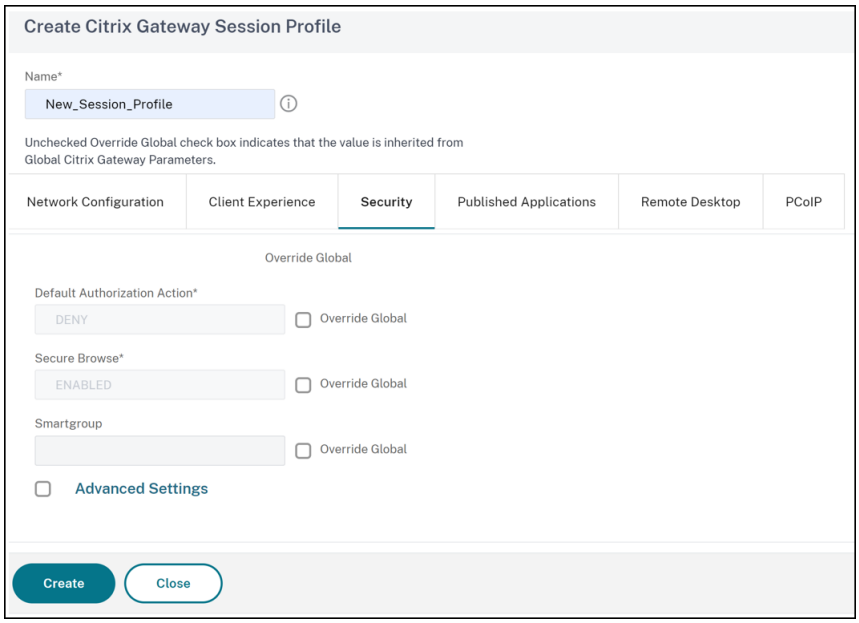





10. Konfigurieren Sie auf der Registerkarte **Sicherheit** die folgende Einstellung:

    - **Standardautorisierungsaktionen : Setzen Sie diese Option auf ZULASSEN**, damit Benutzer von iOS- und Android-Mobilgeräten aus eine Verbindung zu Netzwerkressourcen herstellen können. Benutzer müssen keinen vollständigen VPN-Tunnel einrichten, um auf Ressourcen im sicheren Netzwerk zuzugreifen.

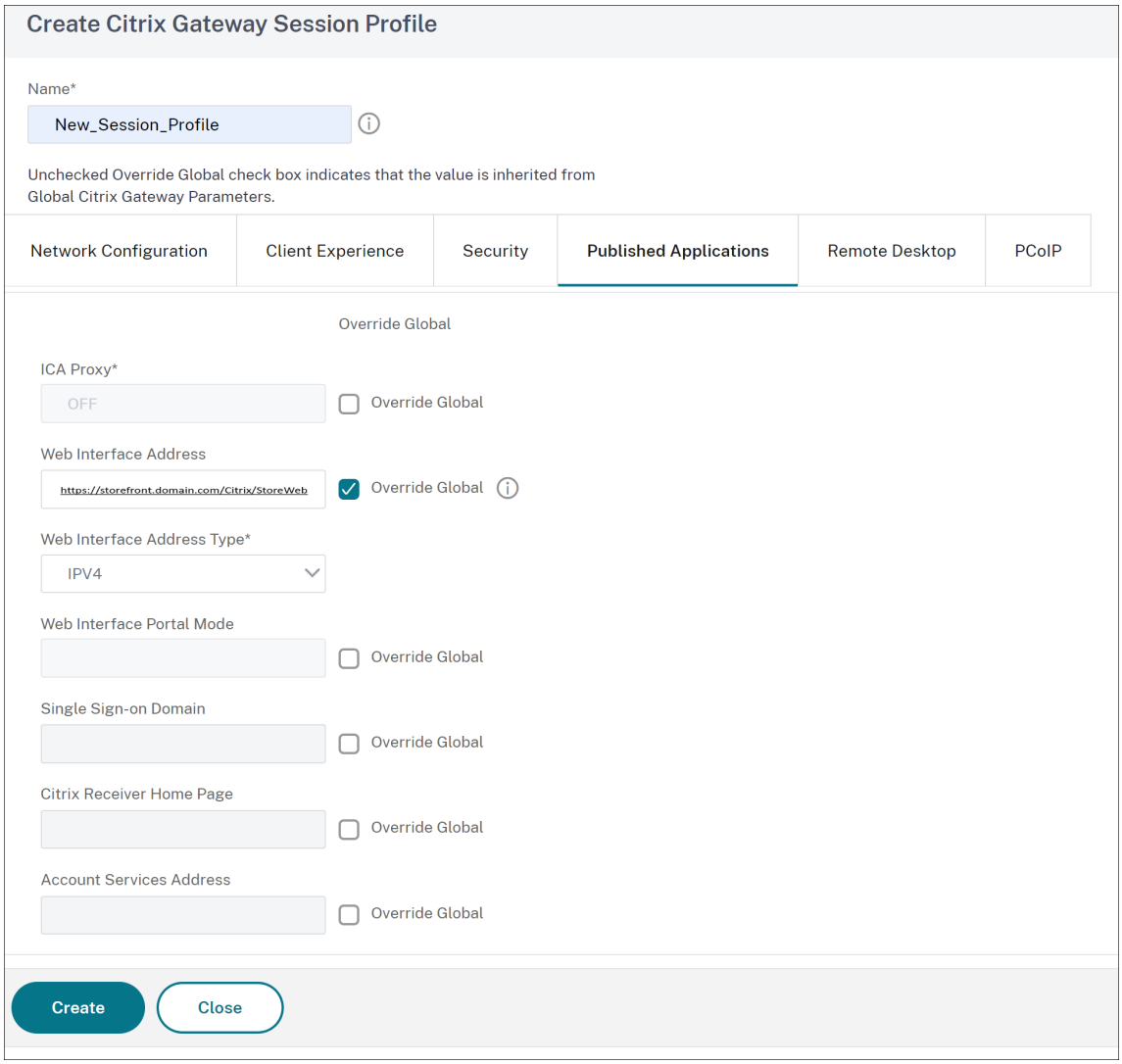



11. Aktivieren Sie auf der Registerkarte **Veröffentlichte Anwendungen** die folgenden Einstellungen:

    - **ICA-Proxy**: Auf ON gesetzt.
    - **Webinterface-Adresse**: FQDN des StoreFront-Servers, gefolgt vom Pfad zum Store für das Web.
    - **Webinterface-Typ**: Typ des Webinterface (IPv4/v6).

- **Single Sign-On-Domäne**: NetBIOS-Name für die Domäne.




12. Klicken Sie auf **Erstellen**.
13. Fügen Sie einen Ausdruck hinzu.

    a) Klicken Sie auf **Erweiterte Richtlinie** und dann auf **Ausdrucksеditor**.
    b) Wählen Sie im **AusdrucksеditorHTTP > REQ > HEADER** und geben Sie dann den Parameter ein, z. B. `**CitrixReceiver**` Beispiel:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

Diese Richtlinie ist erforderlich, damit der Citrix ADC zwischen webbrowserbasierten und Citrix Workspace-App-basierten Verbindungen unterscheiden kann. Diese Richtlinie wird auf Webbrowser-basierte Verbindungen angewendet.

**Erstellen einer Sitzungsrichtlinie für die Citrix Workspace-App für Windows oder Mac und für Mobilgeräte auf Citrix Gateway**

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Sitzung**.
2. Klicken Sie im Feld **Sitzungsrichtlinien** auf **Hinzufügen**.
3. Geben Sie im Feld **Name** den Namen der Sitzungsrichtlinie ein. Zum Beispiel Receiver_Policy.
4. Geben Sie den Namen des neuen Sitzungsprofils im Fenster **Citrix Gateway-Sitzungsprofil konfigurieren** ein.
5. Aktivieren Sie auf der Registerkarte **Client Experience** die folgenden Einstellungen:
   - **Homepage**: Auf **None** setzen
   - **Split-Tunnel**: Auf **AUS** setzen
   - **Clientloser Zugriff: Auf Ein gesetzt**
   - **Single Sign-On für die Webanwendung**: Aktivieren Sie das Kontrollkästchen
   - **Plug-In-Typ**: Auf **Java** festlegen
6. Legen Sie auf der Registerkarte **Sicherheit** die Option **Standardautorisierungsaktionen** auf **ZULASSEN** fest.
7. Aktivieren Sie auf der Registerkarte **Veröffentlichte Anwendungen** die folgenden Einstellungen:
   - **ICA-Proxy**: Auf ON gesetzt.
   - **Webinterface-Adresse:** FQDN des StoreFront-Servers, gefolgt vom Pfad zum Store
   - **Domäne für einmaliges Anmelden:** NetBIOS-Name für die Domäne
   - **Adresse der Kontodienste:**Geben Sie die Adresse der Kontodienste ein. Der letzte Backslash ist wichtig. Zum Beispiel `https://accounts.example.com/Citrix/Roaming/Accounts`
8. Klicken Sie auf **Erstellen**.
9. Wenn Sie einen klassischen Richtlinienausdruck verwenden, fügen Sie im Feld **Ausdruck** die folgenden Informationen hinzu und klicken Sie auf **Erstellen**.

   ```
   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```

10. Wenn Sie einen erweiterten Richtlinienausdruck verwenden, fügen Sie im Feld **Ausdruck** die folgenden Informationen hinzu und klicken Sie auf **Erstellen**.

    ```
    HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
    ```

Diese Richtlinie ist erforderlich, damit der Citrix ADC zwischen den webbrowserbasierten und den App-basierten Citrix Workspace-Verbindungen unterscheiden kann. Diese Richtlinie wird für Verbindungen auf Basis der Citrix Workspace-App angewendet.

#### Konfigurieren der Authentifizierung auf der Citrix ADC Appliance

Informationen zum Konfigurieren der LDAP-Authentifizierung auf einer Citrix ADC Appliance finden Sie unter Konfigurieren der LDAP-Authentifizierung.

#### Erstellen Sie einen virtuellen Citrix Gateway-Server und binden Sie die Sitzungsrichtlinien

1. Navigieren Sie zu **Citrix Gateway > Virtual Server** und klicken Sie auf **Hinzufügen**, um einen neuen virtuellen Server hinzuzufügen.
2. Binden Sie nach dem Erstellen des virtuellen Servers die spezifische Sitzungsrichtlinie basierend auf den Anforderungen Ihres Unternehmens an den virtuellen Server.

### Konfigurieren der Authentifizierung für StoreFront

1. Aktivieren Sie die Passthrough-Authentifizierung von Citrix Gateway auf StoreFront. Weitere Informationen finden Sie unter Erstellen und Konfigurieren des Authentifizierungsdiensts.

   StoreFront muss dem Aussteller des gebundenen Zertifikats des virtuellen Citrix Gateway-Servers (Stamm- und/oder Zwischenzertifikate) für den Authentifizierungsrückrufdienst vertrauen.
2. Fügen Sie Citrix Gateway zu StoreFront hinzu. Weitere Informationen finden Sie unter Hinzufügen einer Citrix Gateway-Verbindung.

   Die Gateway-URL muss genau mit dem übereinstimmen, was die Benutzer in die Adressleiste des Webbrowsers eingeben.
3. Aktivieren Sie den Remotezugriff im StoreFront-Store. Weitere Informationen finden Sie unter Verwalten des Remotezugriffs auf Stores über Citrix Gateway.

### Referenzen

- Timeouteinstellungen konfigurieren

# Erweiterte Richtlinienunterstützung für Unternehmens-Lesezeichen

March 27, 2024

Unternehmenslesezeichen (VPN-URLs) können als erweiterte Richtlinien konfiguriert werden.

> **Hinweise:**
>
> - Citrix Gateway unterstützt HTTP-, HTTPs- und RDP-Protokolle für die Unternehmens-Lesezeichen.
> - Citrix Gateway unterstützt nur absolute URLs für die Unternehmens-Lesezeichen.

## Konfigurieren Sie die VPN-URL als erweiterte Richtlinie

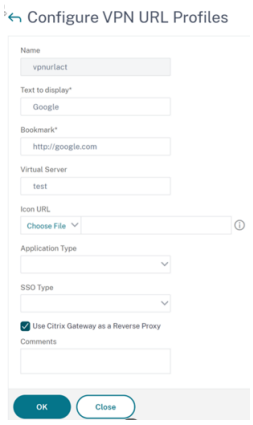
### Auf der GUI

1. Erstellen Sie ein VPN-URL-Profil.
   - Navigieren Sie zu **Konfiguration > Citrix Gateway > Richtlinien > VPN-URL**.
   - Wählen Sie auf der Seite **VPN-URL-Richtlinien und -Profile** die Registerkarte **VPN-URL-Profile** aus und klicken Sie auf **Hinzufügen**.
   - Aktualisieren Sie die erforderlichen Felder und klicken Sie auf **Erstellen**.
     - Name: Ein Name für das VPN-URL-Profil.
     - Anzuzeigender Text: Eine kurze Beschreibung des Links. Die Beschreibung wird auf der Zugriffsoberfläche angezeigt.
     - Lesezeichen: Webadresse der Anwendung.
     - Virtueller Server: Name des zugehörigen virtuellen Load-Balancing- oder Content-Switching-Servers, der konfiguriert ist. Das Feld ist optional.
     - Symbol-URL: Die in dieses Feld hochgeladenen Symbole werden für alle Designs außer dem Standarddesign unterstützt. Die empfohlene Maximalgröße beträgt 70x70 Pixel. Wir empfehlen die Verwendung transparenter Bilder. Das Feld ist optional.
     - Anwendungstyp: Wählen Sie den Anwendungstyp (VPN, clientloses VPN oder SaaS) aus, für den die URL steht. Das Feld ist optional.
     - SSO-Typ: SSO-Typ, den Sie für das Lesezeichen konfigurieren möchten. Wenn SSO konfiguriert ist, können Benutzer auf die Anwendungen zugreifen, ohne ihre Anmeldeinformationen bei den nachfolgenden Anmeldungen eingeben zu müssen. Die folgenden SSO-Typen werden unterstützt:

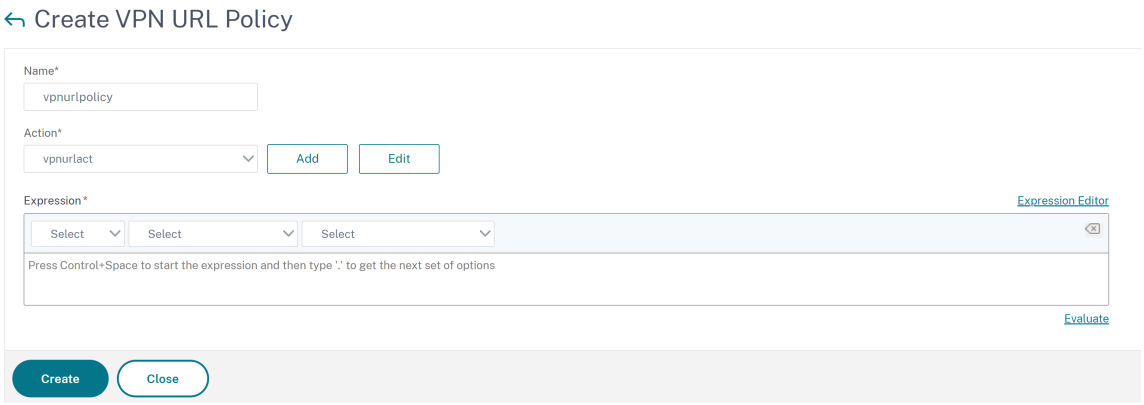
* Unified Gateway: Diese SSO-Konfiguration ermöglicht den sicheren Remotezugriff auf mehrere Ressourcen einer Anwendung über eine einzige URL.
* Selbstauthentifizierung: In dieser SSO-Konfiguration werden Citrix Gateway-Benutzer aufgefordert, die Anmeldeinformationen für den Zugriff auf die Anwendung einzugeben.
* SAML-basierte Authentifizierung: In dieser SSO-Konfiguration verwendet Citrix Gateway einen IdP, um die Benutzerdetails zu validieren, generiert eine SAML-Assertion und sendet sie an den SP. Wenn die Validierung erfolgreich ist, ist das SSO erfolgreich.

> **Note:**
>
> If you enable clientless access, you can make sure that requests to websites go through Citrix Gateway. For example, you added a bookmark for Google. Select the Use Citrix Gateway as a reverse proxy check box. When you select this check box, website requests go from the user device to Citrix Gateway and then to the website. When you clear the check box, requests go from the user device to the website. This check box is only available if you enable clientless access.



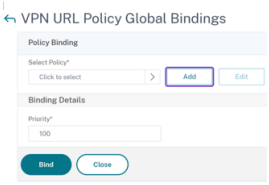

2. Erstellen Sie eine VPN-URL-Richtlinie.
   - Navigieren Sie zu **Konfiguration > Citrix Gateway > Richtlinien > VPN-URL**.
   - Wählen Sie auf der Seite **VPN-URL-Richtlinien und -Profile** die Registerkarte **VPN-URL-Richtlinie** aus und klicken Sie auf **Hinzufügen**.
   - Aktualisieren Sie die erforderlichen Felder und klicken Sie auf **Erstellen**.
     - Name: Ein Name für die VPN-URL-Richtlinie.
     - Aktion: Wählen Sie das konfigurierte VPN-URL-Profil aus. Wenn die Dropdownliste kein Profil enthält, klicken Sie auf Hinzufügen und wiederholen Sie Schritt 1.
     - Ausdruck: Informationen zu den erweiterten Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.




3. Binden Sie die VPN-URL-Richtlinie an einen Bindungspunkt.

   - Navigieren Sie zu **Konfiguration > Citrix Gateway > Richtlinien > VPN-URL**.
   - Wählen Sie auf der Seite **VPN-URL-Richtlinien und -Profile** die Registerkarte **VPN-URL-Richtlinie** aus.
   - Wählen Sie in der Dropdownliste **Aktion auswählen die OptionGlobale Bindungen** aus.
   - Wählen Sie die VPN-URL-Richtlinie aus. Wenn keine Richtlinie aufgeführt ist, klicken Sie auf **Hinzufügen** und wiederholen Sie Schritt 2.
   - Weisen Sie der VPN-URL-Richtlinie im Abschnitt **Bindungsdetails** eine Priorität zu.




### Über die Befehlszeilenschnittstelle

#### Erstellen Sie eine VPN-URL-Aktion:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add vpn urlAction <name> -linkName <string> -actualURL <string> \[-
    vServerName <string>] \[-clientlessAccess \( ON | OFF )] \[-comment
    <string>] \[-iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype
     <applicationtype>] \[-samlSSOProfile <string>]
```

Citrix Gateway unterstützt die folgenden Operationen für VPN-URL-Aktionen:

- **Konto**

```
add vpn urlAction <name> -linkName <string> -actualURL <string>
   \[-vServerName <string>] \[-clientlessAccess \( ON | OFF )]
   \[-comment <string>] \[-iconURL <URL>] \[-ssotype <ssotype>]
   \[-applicationtype <applicationtype>] \[-samlSSOProfile <
   string>]
```

- **einstellen**

```
set vpn urlAction <name> \[-vServerName <string>] \[-
   clientlessAccess \( ON | OFF )] \[-comment <string>] \[-
   iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype <
   applicationtype>] \[-samlSSOProfile <string>]
```

- **unset**

```
unset vpn urlAction <name> [-vServerName] [-clientlessAccess] [-
   comment] [-iconURL] [-ssotype] [-applicationtype] [-
   samlSSOProfile]
```

> **Hinweis:**
>
> Wenn Sie den clientlosen Zugriff auf ON setzen, können Sie sicherstellen, dass Anfragen an Websites vom Benutzergerät an Citrix Gateway und dann an die Website weitergeleitet werden.

- **show**

```
show vpn urlAction [<name>]
```

- **entfernen**

```
remove vpn urlAction <name>
```

- **umbenennen**

```
rename vpn urlAction <name>@ <newName>@
```

**Erstellen Sie eine VPN-URL-Richtlinie:**

Citrix Gateway unterstützt die folgenden Operationen für die VPN-URL-Richtlinie:

- **Konto**

```
add vpn urlPolicy <name> -rule <expression> -action <string> [-
   comment <string>] [-logAction <string>]
```

- **einstellen**

```
set vpn urlPolicy <name> [-rule <expression>] [-action <string>]
   [-comment <string>] [-logAction <string>]
```

- **unset**

```
unset vpn urlPolicy <name> [-comment] [-logAction]
```

- **show**

```
show vpn urlPolicy [<name>]
```

- **entfernen**

```
remove vpn urlPolicy <name>
```

- **umbenennen**

```
rename vpn urlpolicy <name>@ <newName>@
```

- **stat**

```
stat vpn urlpolicy \[<name>] \[-detail] \[-fullValues] \[-ntimes
   <positive\_integer>] \[-logFile <input\_filename>] \[-
   clearstats \( basic | full )]
```

**Binden Sie die VPN-URL-Richtlinie an einen Bindpunkt:**

Citrix Gateway unterstützt die folgenden Vorgänge für die VPN-URL-Richtlinienbindung:

- **binden**

```
bind vpn vserver <vserver name> -policy <string> -priority <
   positive_integer> [-gotoPriorityExpression <expression>]
bind vpn global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>]
bind aaa user <userName> -policy <string> [-priority <
   positive_integer>] [-type <type>] [-gotoPriorityExpression <
   expression>]
bind aaa group <groupName> -policy <string> [-priority <
   positive_integer>] [-type <type>] [-gotoPriorityExpression <
   expression>]
```

- **lösen**

```
unbind vpn vserver <name> -policy <string>
unbind vpn global -policyName <string>
unbind aaa user <name> -policy <string>
unbind aaa group <name> -policy <string>
```

> **Hinweis:**
>
> Bindungspunkte sind `aaauseraaagroup`, `vpnvserver`, und `vpnglobal`.

# Endpunktrichtlinien

March 27, 2024

Endpoint Analysis (EPA) ist ein Prozess, der das Gerät eines Benutzers scannt und Informationen wie das Vorhandensein und die Versionsstufe von Betriebssystemupdates, Antivirus-, Firewall- und Webbrowsersoftware erkennt. Mit Endpoint Analysis können Sie feststellen, ob das Gerät eines Benutzers Ihre Anforderungen erfüllt, bevor es eine Verbindung zu Ihrem Netzwerk herstellt. Es kann auch so konfiguriert werden, dass es regelmäßig nach Änderungen sucht, während der Benutzer verbunden bleibt. Sie können Dateien, Prozesse und Registrierungseinträge auf dem Benutzergerät während der Benutzersitzung überprüfen, um sicherzustellen, dass das Gerät weiterhin die Anforderungen erfüllt.

> **Wichtig:**
>
> - Endpoint Analysis dient zur Analyse des Benutzergeräts anhand vorab festgelegter Konformitätskriterien. Die Sicherheit von Endbenutzergeräten wird nicht validiert oder erzwungen. Es wird empfohlen, Endpunktsicherheitssysteme zu verwenden, um Geräte vor lokalen Administratorangriffen zu schützen.
> - Der EPA-Client ist als eigenständiger Client verfügbar und wird auch zusammen mit dem Citrix Secure Access Client gebündelt. Der Citrix EPA-Client und der Citrix Secure Access-Client sind voneinander unabhängig.

## So funktionieren Endpunkt-Richtlinien

Sie können Citrix Gateway so konfigurieren, dass überprüft wird, ob ein Benutzergerät bestimmte Anforderungen erfüllt, bevor sich ein Benutzer anmeldet. Dies wird als Vorauthentifizierungsrichtlinie bezeichnet. Sie können Citrix Gateway so konfigurieren, dass ein Benutzergerät auf Antivirenprogramme, Firewall, Antispam, Prozesse, Dateien, Registrierungseinträge, Internetsicherheit oder Betriebssysteme überprüft wird, die Sie in der Richtlinie angeben. Wenn das Benutzergerät den Scan vor der Authentifizierung fehlschlägt, dürfen sich Benutzer nicht anmelden.

Um andere Anforderungen zu überprüfen, die in einer Vorauthentifizierungsrichtlinie nicht verwendet werden, können Sie eine Sitzungsrichtlinie konfigurieren und sie an einen Benutzer oder eine Gruppe binden. Diese Art von Richtlinie wird als Nachauthentifizierungsrichtlinie bezeichnet, die während der Benutzersitzung ausgeführt wird, um sicherzustellen, dass die erforderlichen Kriterien, wie Antivirensoftware oder ein Prozess, konform bleiben.

Wenn Sie eine Richtlinie vor oder nach der Authentifizierung konfigurieren, lädt Citrix Gateway das Endpoint Analysis Plug-In herunter und führt den Scan dann auf dem Benutzergerät aus. Jedes Mal, wenn sich ein Benutzer anmeldet, wird das Endpoint Analysis-Plug-In automatisch ausgeführt.

Sie können die folgenden drei Richtlinientypen verwenden, um Endpunktrichtlinien zu konfigurieren:

- Vorauthentifizierungsrichtlinie, die einen Ja- oder Nein-Parameter verwendet. Der Scan bestimmt, ob das Benutzergerät die angegebenen Anforderungen erfüllt. Wenn der Scan fehlschlägt, kann der Benutzer keine Anmeldeinformationen auf der Anmeldeseite eingeben.
- Sitzungsrichtlinie, die bedingt ist und für SmartAccess verwendet werden kann.
- Ausdruck für die Überprüfung des Clientgeräts innerhalb einer Sitzungsrichtlinie. Wenn das Benutzergerät die Anforderungen des Client-Geräteprüfungsausdrucks nicht erfüllt, können Sie Benutzer so konfigurieren, dass sie in eine Quarantänegruppe aufgenommen werden. Wenn das Benutzergerät den Scan durchläuft, können Benutzer in eine andere Gruppe eingeordnet werden, für die möglicherweise andere Überprüfungen erforderlich sind.

Sie können die erkannten Informationen in Richtlinien integrieren, sodass Sie je nach Benutzergerät unterschiedliche Zugriffsebenen gewähren können. Beispielsweise können Sie Benutzern, die eine Remote-Verbindung von Benutzergeräten herstellen, die aktuelle Anforderungen an Antiviren- und Firewall-Software haben, vollen Zugriff mit Downloadberechtigung gewähren. Für Benutzer, die eine Verbindung von nicht konformen Geräten herstellen, können Sie eine eingeschränktere Zugriffsebene bereitstellen, mit der Benutzer Dokumente auf Remoteservern bearbeiten können, ohne sie herunterladen zu müssen. Alle Geräte, auf denen EPA läuft, gelten als nicht konforme Geräte.

Endpoint Analysis führt die folgenden grundlegenden Schritte aus:

- Untersucht einen ersten Satz von Informationen über das Benutzergerät, um festzustellen, welche Scans angewendet werden sollen.
- Führt alle anwendbaren Scans aus. Wenn Benutzer versuchen, eine Verbindung herzustellen, überprüft das Endpoint Analysis Plug-In das Benutzergerät auf die Anforderungen, die in der Vorauthentifizierungs- oder Sitzungsrichtlinie festgelegt sind Wenn das Benutzergerät den Scan besteht, können sich Benutzer anmelden. Wenn das Benutzergerät den Scan nicht besteht, dürfen sich Benutzer nicht anmelden.

  **Hinweis:** Endpoint Analysis-Scans werden abgeschlossen, bevor die Benutzersitzung eine Lizenz verwendet.
- Vergleicht die auf dem Benutzergerät erkannten Eigenschaftswerte mit den gewünschten Eigenschaftswerten, die in Ihren konfigurierten Scans aufgeführt sind.
- Erzeugt eine Ausgabe, die überprüft, ob die gewünschten Eigenschaftswerte gefunden wurden.

> **Achtung:**
>
> Die Anweisungen zum Erstellen von Endpoint Analysis-Richtlinien sind allgemeine Richtlinien. Sie können viele Einstellungen innerhalb einer Sitzungsrichtlinie vornehmen. Spezifische Anweisungen zum Konfigurieren von Sitzungsrichtlinien können Anweisungen zum Konfigurieren einer bestimmten Einstellung enthalten. Diese Einstellung kann jedoch eine von vielen Einstel-

> lungen sein, die in einem Sitzungsprofil und einer Richtlinie enthalten sind.

#### Beispiele für EPA-Ausdrücke

Im Folgenden finden Sie Ausdrucksbeispiele für einige EPA-Komponenten wie den Prozess beenden, Dateien löschen und das Gerätezertifikat:

- Windows:
  - Prozess beenden: `sys.client_expr(\“proc_0_perl\“)-killProcess processToKill.exe`
  - Gerätezertifikat:`sys.client_expr(“device-cert_0_0”)`
  - Dateien löschen:`sys.client_expr(\“proc_0_perl\“)-deletefiles “C:/removefile.txt”`
- MAC
  - Prozess beenden: `sys.client_expr(\“proc_0_perl\“)-killProcess processToKill.exe`
  - Gerätezertifikat:`sys.client_expr(“device-cert_0_0”)`
  - Dateien löschen:`sys.client_expr(\“proc_0_perl\“)-deletefiles “C:/removefile.txt”`

### Bewerten von Benutzeranmeldeoptionen

Wenn sich Benutzer anmelden, können sie den Endpoint Analysis-Scan überspringen. Wenn Benutzer den Scan überspringen, verarbeitet Citrix Gateway diese Aktion als fehlgeschlagene Endpoint Analysis. Wenn Benutzer den Scan nicht bestehen, können sie nur auf das Webinterface oder über clientlosen Zugriff zugreifen.

Sie möchten Benutzern beispielsweise mit Citrix Secure Access Agent Zugriff gewähren. Um sich mit dem Plug-In bei Citrix Gateway anzumelden, müssen Benutzer eine Antivirenanwendung wie Norton Antivirus ausführen. Wenn das Benutzergerät die Anwendung nicht ausführt, können sich Benutzer nur mit Receiver anmelden und veröffentlichte Anwendungen verwenden. Sie können auch den clientlosen Zugriff konfigurieren, der den Zugriff auf bestimmte Anwendungen wie Outlook Web Access einschränkt.

Um Citrix Gateway für dieses Anmeldeszenario zu konfigurieren, weisen Sie eine restriktive Sitzungsrichtlinie als Standardrichtlinie zu. Anschließend konfigurieren Sie die Einstellungen so, dass Benutzer auf eine privilegierte Sitzungsrichtlinie aktualisiert werden, wenn das Benutzergerät den Endpoint Analysis-Scan durchläuft. Zu diesem Zeitpunkt haben Benutzer Zugriff auf Netzwerkebene und können sich mit Citrix Secure Access Agent anmelden.

**Führen Sie die folgenden Schritte aus, um Citrix Gateway so zu konfigurieren, dass zuerst die Richtlinie für restriktive Sitzungen durchzusetzen ist:**

- Konfigurieren Sie die globalen Einstellungen mit aktiviertem ICA-Proxy und allen anderen erforderlichen Einstellungen, wenn die angegebene Anwendung nicht auf dem Benutzergerät ausgeführt wird.
- Erstellen Sie eine Sitzungsrichtlinie und ein Profil, das Citrix Secure Access Agent aktiviert
- Erstellen Sie einen Ausdruck innerhalb des Regelabschnitts der Sitzungsrichtlinie, um die Anwendung anzugeben, z. B. `(client.application.process(symantec.exe) exists)`

  Wenn sich Benutzer anmelden, wird zuerst die Sitzungsrichtlinie angewendet. Wenn Endpoint Analysis fehlschlägt oder der Benutzer den Scan überspringt, ignoriert Citrix Gateway die Einstellungen in der Sitzungsrichtlinie (der Ausdruck in der Sitzungsrichtlinie wird als falsch angesehen). Infolgedessen haben Benutzer über das Webinterface oder den clientlosen Zugriff eingeschränkt. Wenn Endpoint Analysis erfolgreich ist, wendet Citrix Gateway die Sitzungsrichtlinie an, und Benutzer haben vollen Zugriff auf Citrix Secure Access Agent.

### Überspringen Sie den EPA-Scan

Sie können den EPA-Scan nur zur Nachauthentifizierung und zur Vorabauthentifizierung überspringen. Skip EPA ist in Browsern aller unterstützten Betriebssysteme verfügbar. Benutzer müssen auf die Schaltfläche **EPA überspringen** klicken, die beim Zugriff auf das Gateway angezeigt wird. Wenn Benutzer den Scan überspringen, verarbeitet Citrix Gateway diese Aktion als fehlgeschlagene Endpoint Analysis. Wenn Benutzer den Scan nicht bestehen, können sie nur auf das Webinterface oder über clientlosen Zugriff zugreifen.

Siehe auch https://support.citrix.com/article/CTX200748.

### Endpunktanalyse-Scans, die für Ubuntu unterstützt werden

Die folgenden Endpoint Analysis (EPA) -Scans werden für das EPA-Plug-In unterstützt, das für das Ubuntu-Betriebssystem installiert ist. Ein Beispielausdruck zur Konfiguration der einzelnen Scans wird zusammen mit den EPA-Scans aufgeführt. Sie können diese Ausdrücke in den Authentifizierungsrichtlinien konfigurieren.

- **Datei**
  - **Existenz**: sys.client_expr(“file_0_/home/user/test.txt”)
  - **MD5-Prüfsumme**: sys.client_expr(“file_0*/home/user/test.txt_md5* ce780e271debcc29f551546e8db336
    )

  - **Text in einer Datei (Unterstützung für reguläre Ausdrücke)**: sys.client_expr( “file_0_/home/user/test.txt_search_cloud”)

- **Prozess**
  - **Existenz**: sys.client_expr(“proc_0_perl”)
  - **MD5-Prüfsumme**: sys.client_expr(“proc_0*perl_md5* c060d3a5f97e27066cef8c116785567a” )
  - **Pfad**: sys.client_expr(“proc_0*perl_path*/usr/bin/perl”)
- **Dateisystemgerät oder Mountpoint-Name**: sys.client_expr(“mountpoint_0_/sys”)

Wenn Sie erweiterte Richtlinien verwenden, können die Ausdrücke für jeden Scan über die GUI generiert werden (**Sicherheit > AAA > Richtlinien > Authentifizierung > Erweiterte Richtlinien > EPA**).

**Hinweis:** Auf der Seite Ausdruckseditor können Sie für den Linux-Client **Allgemein** auswählen und dann **Prozess, Datei** oder **Mount Point**auswählen.

## Richtlinien und Profile für die Vorauthentifizierung

March 27, 2024

> **Wichtig:**
>
> Die Endpunktanalyse dient dazu, das Benutzergerät anhand vorab festgelegter Konformitätskriterien zu analysieren. Die Sicherheit der Endbenutzergeräte wird nicht erzwungen oder validiert. Es wird empfohlen, Endpunktsicherheitssysteme zu verwenden, um Geräte vor lokalen Administratorangriffen zu schützen.

Sie können Citrix Gateway so konfigurieren, dass die Geräte eines Benutzers überprüft werden, bevor sie bei Citrix Gateway authentifiziert werden. Dies kann verwendet werden, um den Zugriff einzuschränken, wenn das Gerät des Benutzers die Anforderungen Ihres Unternehmens nicht erfüllt. Geräteprüfungen können mithilfe individueller Richtlinien implementiert werden, die für einen virtuellen Server spezifisch sind, oder global, wie in den folgenden beiden Verfahren beschrieben.

Vorauthentifizierungsrichtlinien bestehen aus einem Profil und einem Ausdruck. Sie konfigurieren das Profil so, dass ein Ausdruck verwendet wird, um die Ausführung eines Prozesses auf dem Benutzergerät zuzulassen oder zu verweigern. Beispielsweise wird die Textdatei clienttext.txt auf dem Gerät des Benutzers ausgeführt. Wenn sich der Benutzer bei Citrix Gateway anmeldet, können Sie den Zugriff zulassen oder verweigern, je nachdem, ob die Textdatei ausgeführt wird. Wenn Sie Benutzern nicht erlauben möchten, sich während der Ausführung des Prozesses anzumelden, können Sie ein Vorauthentifizierungsprofil so konfigurieren, dass der Prozess angehalten wird, bevor sich Benutzer anmelden.

**Sie können die folgenden Einstellungen für Richtlinien vor der Authentifizierung konfigurieren:**

- Expression. Beinhaltet die folgenden Einstellungen, die Ihnen beim Erstellen von Ausdrücken helfen:
  - Expression. Zeigt alle Ausdrücke an.
  - Entsprechen Sie einem beliebigen Ausdruck. Konfiguriert die Richtlinie so, dass sie mit einem der Ausdrücke übereinstimmt, die in der Liste der ausgewählten Ausdrücke enthalten sind.
  - Entspricht allen Ausdrücken. Konfiguriert die Richtlinie so, dass sie mit allen Ausdrücken übereinstimmt, die in der Liste der ausgewählten Ausdrücke enthalten sind.
  - Tabellarische Ausdrücke. Erstellt mithilfe der `OR (||)` `or AND (&&)` Operatoren einen zusammengesetzten Ausdruck mit den vorhandenen Ausdrücken.
  - Fortgeschrittene Freiform. Erstellt mithilfe der Ausdrucksnamen und der `OR (||)` `and AND (&&)` Operatoren benutzerdefinierte zusammengesetzte Ausdrücke. Wählen Sie nur die Ausdrücke aus, die Sie benötigen, und lassen Sie andere Ausdrücke aus der Liste der ausgewählten Ausdrücke aus.
  - Add. Erzeugt einen Ausdruck.
  - Modifizieren. Ändert einen vorhandenen Ausdruck.
  - Remove. Entfernt den ausgewählten Ausdruck aus der Liste zusammengesetzter Ausdrücke.
  - Benannte Ausdrücke. Wählen Sie einen konfigurierten benannten Ausdruck. Sie können benannte Ausdrücke aus dem Menü der Ausdrücke auswählen, die bereits auf Citrix Gateway vorhanden sind.
  - Ausdruck hinzufügen. Fügt der Richtlinie den ausgewählten benannten Ausdruck hinzu.
  - Ersetzen Sie den Ausdruck. Ersetzt den ausgewählten benannten Ausdruck durch die Richtlinie.
  - Vorschau des Ausdrucks. Zeigt die detaillierte Zeichenfolge an, die auf Citrix Gateway konfiguriert ist, wenn Sie einen benannten Ausdruck auswählen.

## Vorauthentifizierungsprofil konfigurieren

### So konfigurieren Sie ein Vorauthentifizierungsprofil global über die GUI

1. Klicken Sie auf der Registerkarte Konfiguration auf **Citrix Gateway** und dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Vorauthentifizierungseinstellungen ändern**.
3. Konfigurieren Sie im Dialogfeld **Globale Einstellungen für die Vorauthentifizierung** die Einstellungen:

a) Wählen Sie unter **Aktion**die Option **Zulassen oder Verweigern**aus.

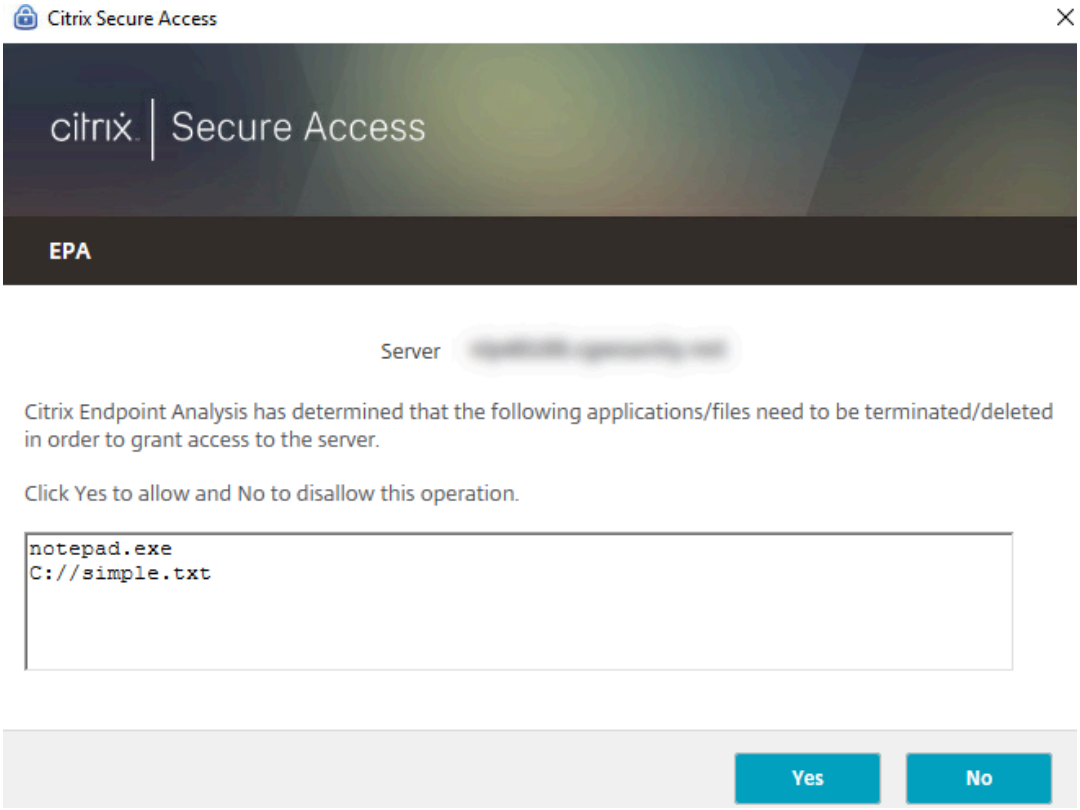
Verweigert oder ermöglicht Benutzern die Anmeldung nach dem Auftreten der Endpoint Analysis.

b) Geben Sie im Feld **Zu stornierende Prozesse**den Prozess ein.

Dies gibt die Prozesse an, die das Endpoint Analysis-Plug-in beenden muss.

c) Geben Sie im Feld **Zu löschende Dateien**den Dateinamen ein.

Dies gibt die Dateien an, die das Endpoint Analysis-Plug-in löschen muss. Wenn Sie einen Prozess löschen oder abbrechen, wird den Endbenutzern eine Benachrichtigung angezeigt.




4. In Ausdruck können Sie den Ausdruck ns_true beibehalten oder einen Ausdruck für eine bestimmte Anwendung erstellen, z. B. Antiviren- oder Sicherheitssoftware, und dann auf **OK**klicken.

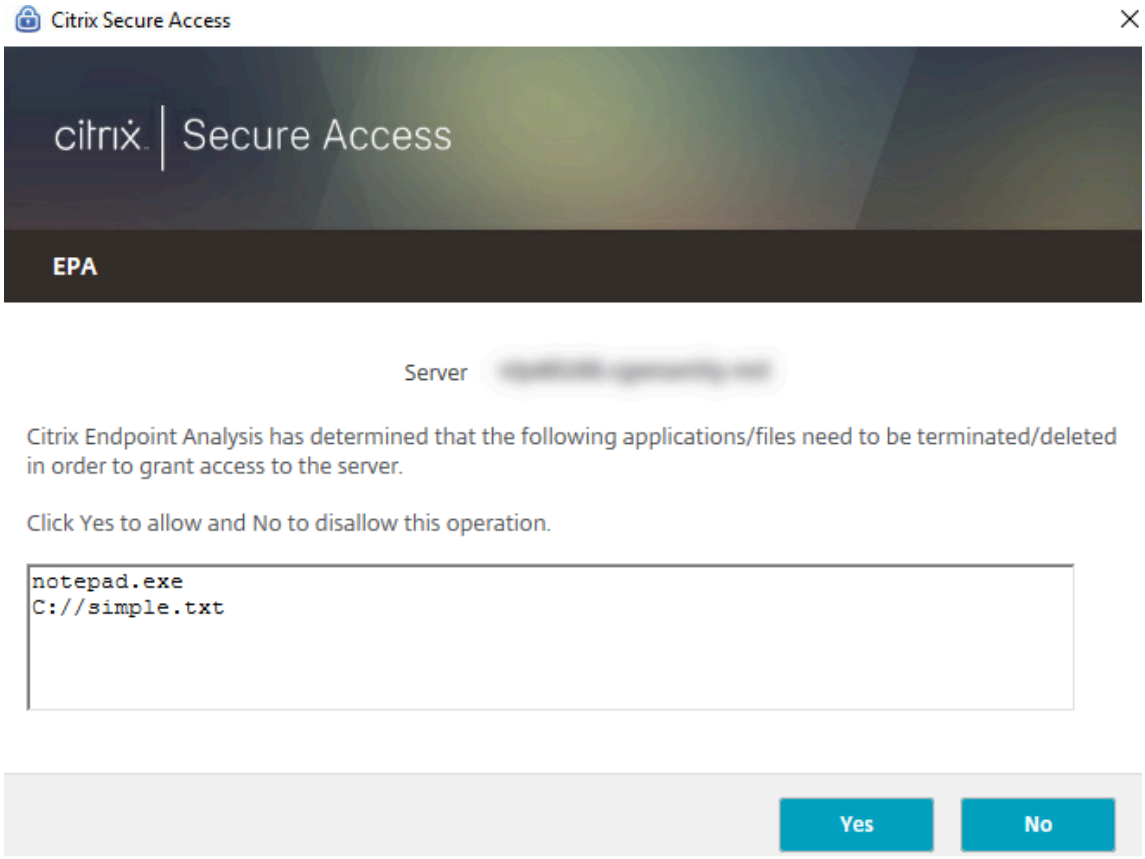
**So konfigurieren Sie ein Vorauthentifizierungsprofil über die GUI**

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung und klicken Sie dann auf**Pre-Authentication**EPA.
2. Klicken Sie im Detailbereich auf der Registerkarte **Profile** auf **Hinzufügen**.
3. Geben Sie **unter Name**den Namen der zu prüfenden Anwendung ein.

4. Wählen Sie in **Aktion** **ERLAUBEN** oder **VERWEIGERN**.
5. Geben Sie im **Feld Prozesse, die abgebrochen werden sollen**, den Namen des Prozesses ein, der gestoppt werden soll.
6. Geben **Sie unter Zu löschende Dateien** den Namen der zu löschenden Datei ein, z. B. c:\clientext.txt, klicken Sie auf **Erstellen** und dann auf **Schließen**.

   Dies gibt die Dateien an, die das Endpoint Analysis-Plug-in löschen muss. Wenn Sie einen Prozess löschen oder abbrechen, wird den Endbenutzern eine Benachrichtigung angezeigt.




Wenn Sie die GUI verwenden, um ein Vorauthentifizierungsprofil zu konfigurieren, erstellen Sie die Vorauthentifizierungsrichtlinie, indem Sie auf der Registerkarte **Richtlinien** auf **Hinzufügen** klicken. Wählen **Sie im Dialogfeld Vorauthentifizierungsrichtlinie erstellen** das Profil aus dem Menü **Profil anfordern** aus.

### Hinzufügen eines vorkonfigurierten Ausdrucks zu einer Vorauthentifizierungsrichtlinie

Citrix Gateway enthält vorkonfigurierte Ausdrücke, die als benannte Ausdrücke bezeichnet werden. Wenn Sie eine Richtlinie konfigurieren, können Sie einen benannten Ausdruck für die Richtlinie verwenden. Sie möchten beispielsweise, dass die Vorauthentifizierungsrichtlinie nach Symantec An-

tivirus 10 mit aktualisierten Virendefinitionen sucht. Erstellen Sie eine Vorauthentifizierungsrichtlinie und fügen Sie den Ausdruck wie im folgenden Verfahren beschrieben hinzu.

Wenn Sie eine Vorauthentifizierungs- oder Sitzungsrichtlinie erstellen, können Sie den Ausdruck beim Erstellen der Richtlinie erstellen. Sie können die Richtlinie dann mit dem Ausdruck auf virtuelle Server oder global anwenden.

Im folgenden Verfahren wird beschrieben, wie Sie mithilfe des Konfigurationsdienstprogramms einen vorkonfigurierten Antivirus-Ausdruck zu einer Richtlinie hinzufügen.

**Hinzufügen eines benannten Ausdrucks zu einer Vorauthentifizierungsrichtlinie**

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung und klicken Sie dann auf**Pre-Authentication**EPA.
2. Wählen Sie im Detailbereich eine Richtlinie aus und klicken Sie dann auf **Öffnen**.
3. Wählen Sie neben **Benannte AusdrückeAnti-Virus**und wählen Sie das Antivirenprodukt aus der Liste aus.
4. Klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen** und dann auf **Schließen**.

## Konfigurieren von benutzerdefinierten Ausdrücken

Ein benutzerdefinierter Ausdruck ist einer, den Sie innerhalb der Richtlinie erstellen. Wenn Sie einen Ausdruck erstellen, konfigurieren Sie die Parameter für den Ausdruck.

Sie können auch benutzerdefinierte Ausdrücke erstellen, um auf häufig verwendete Zeichenfolgen zu verweisen. Dies erleichtert die Konfiguration von Vorauthentifizierungsrichtlinien und auch die Pflege der konfigurierten Ausdrücke.

Sie möchten beispielsweise einen benutzerdefinierten Ausdruck für Symantec Antivirus 10 erstellen und sicherstellen, dass die Virendefinitionen nicht älter als drei Tage sind. Erstellen Sie eine Richtlinie und konfigurieren Sie dann den Ausdruck, um die Virusdefinitionen anzugeben.

Das folgende Verfahren zeigt, wie Sie einen Ausdruck in einer Vorauthentifizierungsrichtlinie erstellen. Sie können dieselben Schritte in einer Sitzungsrichtlinie verwenden.

**Erstellen einer Vorauthentifizierungsrichtlinie und eines benutzerdefinierten Ausdrucks**

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung** und klicken Sie dann auf **Pre-Authentication EPA**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.

5. Geben Sie im Dialogfeld Authentifizierungsprofil erstellen in das Feld **Name**einen Namen für das Profil ein, wählen Sie unter **Aktion**die Option **Zulassen**aus, und klicken Sie dann auf **Erstellen**.
6. Klicken Sie im Dialogfeld Vorauthentifizierungsrichtlinie erstellen neben My**Match Any Expression**auf **Hinzufügen**.
7. Wählen Sie unter **Ausdruckstyp** die Option **Clientsicherheit** aus.
8. Konfigurieren Sie Folgendes:

    a) Wählen Sie unter **KomponenteAntivirus**aus.
    b) Geben Sie **unter Name**einen Namen für die Anwendung ein.
    c) Wählen Sie unter **Qualifier** die Option **Version** aus.
    d) Wählen Sie unter **Operator==**aus.
    e) Geben Sie im Feld **Wert**den Wert ein.
    f) Geben Sie unter **Frische**3 ein, und klicken Sie dann auf **OK**.

9. Klicken Sie im Dialogfeld Pre-Authentication Policy **erstellen auf Erstellen**und dann auf **Schließen**.

Wenn Sie einen benutzerdefinierten Ausdruck konfigurieren, wird er dem Feld **Ausdruck** im Richtlinien-Dialogfeld hinzugefügt.

### Konfigurieren von zusammengesetzten Ausdrücken

Eine Vorauthentifizierungsrichtlinie kann ein Profil und mehrere Ausdrücke enthalten. Wenn Sie zusammengesetzte Ausdrücke konfigurieren, verwenden Sie Operatoren, um die Bedingungen des Ausdrucks anzugeben. Sie können beispielsweise zusammengesetzte Ausdrücke so konfigurieren, dass das Benutzergerät eine der folgenden Antivirenanwendungen ausführen muss:

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

Sie konfigurieren den Ausdruck mit dem ODER-Operator, um nach den drei vorhergehenden Anwendungen zu suchen. Wenn Citrix Gateway die richtige Version einer der Anwendungen auf dem Benutzergerät erkennt, können sich Benutzer anmelden. Der Ausdruck im Richtliniendialogfeld sieht wie folgt aus:

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

Weitere Hinweise zu zusammengesetzten Ausdrücken finden Sie unter Konfigurieren von zusammengesetzten Ausdrücken.

## Binden von Vorauthentifizierungsrichtlinien

Nachdem Sie die Vorauthentifizierungsrichtlinie erstellt haben, binden Sie die Richtlinie an die Ebene, für die sie gilt. Sie können die Vorauthentifizierungsrichtlinien an virtuelle Server oder global binden.

### Erstellen und binden Sie eine Vorauthentifizierungsrichtlinie global

1. Klicken Sie auf der Registerkarte Konfiguration auf **Citrix Gateway** und dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich auf **Einstellungen für die Vorauthentifizierung ändern**.
3. Wählen Sie im Dialogfeld Globale Einstellungen für die Vorauthentifizierung unter **Aktion**die Option **Zulassen** oder **Verweigern**aus.
4. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
5. Wählen Sie im Dialogfeld **Globale Einstellungen für die Vorauthentifizierung** neben **Benannte Ausdrücke**die Option **Allgemein**aus, wählen Sie den Wert **True** aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

### Binden einer Vorauthentifizierungsrichtlinie an einen virtuellen Server

1. Klicken Sie auf der Registerkarte Konfiguration auf **Citrix Gateway** und dann auf **Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen Server aus, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie im Dialogfeld Citrix Gateway Virtual Server konfigurieren auf die Registerkarte **Richtlinien** und dann auf **Vorauthentifizierung**.
4. Klicken Sie unter Details auf **Richtlinie einfügen**, und wählen Sie dann unter Richtlinienname die Vorauthentifizierungsrichtlinie aus.
5. Klicken Sie auf **OK**.

## Aufheben und Entfernen von Vorauthentifizierungsrichtlinien

Bei Bedarf können Sie eine Vorauthentifizierungsrichtlinie aus Citrix Gateway entfernen. Bevor Sie eine Vorauthentifizierungsrichtlinie entfernen, lösen Sie die Bindung vom virtuellen Server oder global.

### Aufheben der Bindung einer globalen Vorauthentifizierungsrichtlinie

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung und klicken Sie dann auf**Pre-Authentication**EPA.

2. Wählen Sie im Detailbereich eine Richtlinie aus und klicken Sie dann unter **Aktion** auf **Globale Bindungen**.
3. Wählen **Sie im Dialogfeld Vorauthentifizierungsrichtlinien an Global binden/aufheben** eine Richtlinie aus, klicken Sie auf **Richtlinie aufheben**, und klicken Sie dann auf **OK**.

#### Aufheben der Bindung einer Vorauthentifizierungsrichtlinie von einem virtuellen Server

1. Klicken Sie auf der Registerkarte Konfiguration auf **Citrix Gateway** und dann auf **Virtuelle Server**.
2. Klicken **Sie im Dialogfeld Citrix Gateway Virtual Server konfigurieren** auf die Registerkarte **Richtlinien**, und klicken Sie dann auf **Vorauthentifizierung**.
3. Wählen Sie die Richtlinie aus und klicken Sie dann auf **Richtlinie aufheben**.

Wenn die Vorauthentifizierungsrichtlinie nicht gebunden ist, können Sie die Richtlinie aus Citrix Gateway entfernen.

#### Entfernen einer Vorauthentifizierungsrichtlinie

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung** und klicken Sie dann auf **Pre-Authentication EPA**.
2. Wählen Sie im Detailbereich eine Richtlinie aus und klicken Sie dann auf **Entfernen**.

### Festlegen der Priorität von Vorauthentifizierungsrichtlinien

Sie können mehrere Vorauthentifizierungsrichtlinien haben, die an verschiedene Ebenen gebunden sind. Beispielsweise verfügen Sie über eine Richtlinie, die nach einer bestimmten global gebundenen Antivirenanwendung sucht, und eine Firewallrichtlinie, die an den virtuellen Server gebunden ist. Wenn sich Benutzer anmelden, wird zuerst die Richtlinie angewendet, die an den virtuellen Server gebunden ist. Die global gebundene Richtlinie wird an zweiter Stelle angewendet.

Sie können die Reihenfolge ändern, in der die Vorauthentifizierungsscans stattfinden. Damit Citrix Gateway zuerst die globale Richtlinie anwendet, ändern Sie die Prioritätsnummer der an den virtuellen Server gebundenen Richtlinie und geben Sie ihm eine höhere Prioritätsnummer als die global gebundene Richtlinie. Legen Sie beispielsweise die Prioritätsnummer für die globale Richtlinie auf eins und die Richtlinie für virtuelle Server auf zwei fest. Wenn sich Benutzer anmelden, führt Citrix Gateway zuerst den globalen Richtlinienscan und dann den Scan der virtuellen Serverrichtlinie aus.

**Ändern der Priorität einer Vorauthentifizierungsrichtlinie**

1. Klicken Sie auf der Registerkarte Konfiguration auf **Citrix Gateway** und dann auf **Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen Server aus, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie auf der Registerkarte Richtlinien auf **Vorauthentifizierung**.
4. Geben Sie unter Priorität die Prioritätsnummer für die Richtlinie ein, und klicken Sie dann auf **OK**.

## Richtlinien nach der Authentifizierung

March 27, 2024

> **Wichtig:**
>
> Die Endpunktanalyse dient dazu, das Benutzergerät anhand vorab festgelegter Konformitätskriterien zu analysieren. Die Sicherheit der Endbenutzergeräte wird nicht erzwungen oder validiert. Es wird empfohlen, Endpunktsicherheitssysteme zu verwenden, um Geräte vor lokalen Administratorangriffen zu schützen.

Eine Richtlinie nach der Authentifizierung ist ein Satz generischer Regeln, die das Benutzergerät erfüllen muss, um die Sitzung aktiv zu halten. Wenn die Richtlinie fehlschlägt, endet die Verbindung zu Citrix Gateway. Wenn Sie die Richtlinie nach der Authentifizierung konfigurieren, können Sie jede Einstellung für Benutzerverbindungen konfigurieren, die bedingt gemacht werden können.

Sie verwenden Sitzungsrichtlinien, um Richtlinien nach der Authentifizierung zu konfigurieren. Zunächst erstellen Sie die Benutzer, für die die Richtlinie gilt. Dann fügen Sie die Benutzer zu einer Gruppe hinzu. Als Nächstes binden Sie Sitzungen, Verkehrsrichtlinien und Intranet-Anwendungen an die Gruppe.

Sie können auch Gruppen als Berechtigungsgruppen angeben. Mit diesem Gruppentyp können Sie Benutzer Gruppen zuweisen, die auf einem Ausdruck zur Überprüfung des Client-Geräts innerhalb der Sitzungsrichtlinie basieren.

Sie können auch eine Richtlinie nach der Authentifizierung konfigurieren, um Benutzer in eine Quarantänegruppe zu versetzen, wenn das Benutzergerät die Anforderungen der Richtlinie nicht erfüllt. Eine einfache Richtlinie umfasst einen Ausdruck zur Überprüfung des Client-Geräts und eine Meldung. Wenn sich Benutzer in der Quarantänegruppe befinden, können sich Benutzer bei Citrix Gateway anmelden. Sie erhalten jedoch eingeschränkten Zugriff auf Netzwerkressourcen.

Sie können keine Autorisierungsgruppe und Quarantänegruppe erstellen, indem Sie dasselbe Sitzungsprofil und dieselbe Richtlinie verwenden. Die Schritte zum Erstellen der Richtlinie nach der Authen-

tifizierung sind dieselben. Wenn Sie die Sitzungsrichtlinie erstellen, wählen Sie entweder eine Autorisierungsgruppe oder eine Quarantänegruppe aus. Sie können zwei Sitzungsrichtlinien erstellen und jede Richtlinie an die Gruppe binden.

Richtlinien nach der Authentifizierung werden auch mit SmartAccess verwendet. Weitere Informationen zu SmartAccess finden Sie unter Konfigurieren von SmartAccess auf Citrix Gateway.

> **Hinweis:**
>
> Diese Funktion funktioniert nur mit Citrix Secure Access Agent. Wenn sich Benutzer mit der Citrix Workspace-App anmelden, wird der Endpoint Analysis-Scan nur bei der Anmeldung ausgeführt.

## Konfigurieren einer Richtlinie nach der Authentifizierung

Sie verwenden eine Sitzungsrichtlinie, um eine Richtlinie nach der Authentifizierung zu konfigurieren. Eine einfache Richtlinie umfasst einen Ausdruck zur Überprüfung des Client-Geräts und eine Meldung.

### So konfigurieren Sie eine Richtlinie nach der Authentifizierung über die GUI

1. Erweitern Sie **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. **Geben Sie im Feld Name einen Namen für das Profil ein.**
6. Klicken Sie auf der Registerkarte Sicherheit auf **Erweiterte Einstellungen**.
7. Klicken Sie unter **Client Security**auf **Override Global** und dann auf **New**.
8. Konfigurieren Sie den Ausdruck für die Überprüfung des Client-Geräts und klicken Sie dann auf **Erstellen**.
9. Wählen Sie unter **Client Security**unter Quarantänegruppe eine Gruppe aus.
10. Geben Sie im **Feld Fehlermeldung**die Meldung ein, die Benutzer erhalten sollen, wenn der Scan nach der Authentifizierung fehlschlägt.
11. Klicken Sie unter Autorisierungsgruppen auf **Global überschreiben**, wählen Sie eine Gruppe aus, klicken Sie auf **Hinzufügen**, klicken Sie auf **OK**und dann auf **Erstellen**.
12. Wählen **Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben Benannte Ausdrücke **die Option Allgemein**aus, wählen Sie **Wahrer Wert**aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

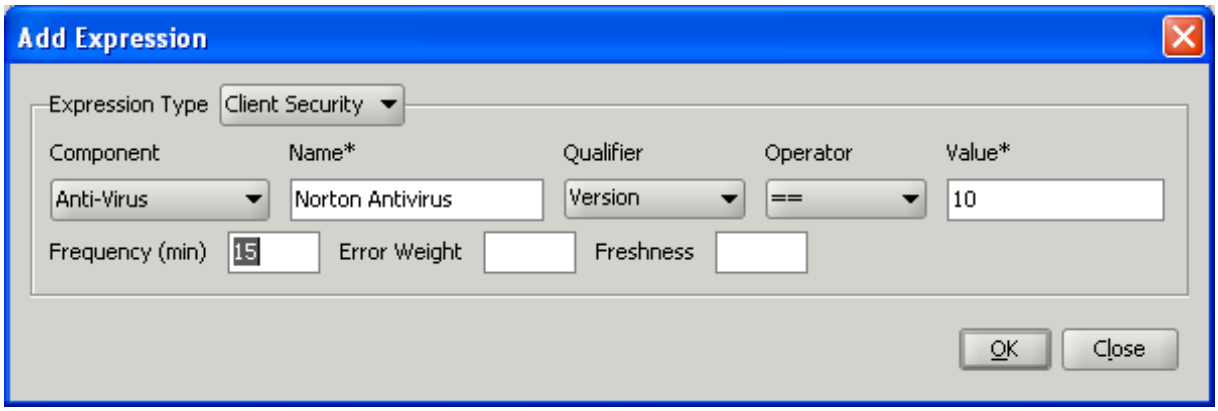
 

### Konfigurieren Sie die Häufigkeit von Scans nach der Authentifizierung

Sie können Citrix Gateway so konfigurieren, dass die Richtlinie nach der Authentifizierung in bestimmten Intervallen ausgeführt wird. Sie haben beispielsweise eine Richtlinie zur Überprüfung von Client-Geräten konfiguriert und möchten, dass sie alle 10 Minuten auf dem Benutzergerät ausgeführt wird. Sie können diese Häufigkeit konfigurieren, indem Sie einen benutzerdefinierten Ausdruck innerhalb der Richtlinie erstellen.

> **Hinweis:**
>
> Die Frequenzprüfungsfunktion für Richtlinien nach der Authentifizierung funktioniert nur mit Citrix Secure Access Agent. Wenn sich Benutzer mit der Citrix Workspace-App anmelden, wird der Endpoint Analysis-Scan nur bei der Anmeldung ausgeführt.

Sie können die Häufigkeit (in Minuten) festlegen, in der Sie die Richtlinie zur Überprüfung des Client-Geräts konfigurieren, indem Sie das Verfahren zur Konfiguration einer Richtlinie nach der Authentifizierung befolgen. Die folgende Abbildung zeigt, wo Sie im Dialogfeld **Ausdruck hinzufügen** einen Häufigkeitswert eingeben können.




### Quarantäne- und Berechtigungsgruppen

Wenn sich Benutzer bei Citrix Gateway anmelden, weisen Sie sie einer Gruppe zu, die Sie entweder auf Citrix Gateway oder auf einem Authentifizierungsserver im sicheren Netzwerk konfigurieren. Wenn ein Benutzer einen Scan nach der Authentifizierung nicht besteht, können Sie den Benutzer einer eingeschränkten Gruppe zuweisen, die als Quarantänegruppe bezeichnet wird und den Zugriff auf Netzwerkressourcen einschränkt.

Sie können auch Autorisierungsgruppen verwenden, um den Benutzerzugriff auf Netzwerkressourcen einzuschränken. Beispielsweise haben Sie möglicherweise eine Gruppe von Vertragspersonal, die nur Zugriff auf Ihren E-Mail-Server und eine Dateifreigabe haben. Wenn Benutzergeräte die Anforderungen für die Geräteüberprüfung erfüllen, die Sie auf Citrix Gateway definiert haben, können Benutzer dynamisch Mitglieder von Gruppen werden.

Sie verwenden entweder globale Einstellungen oder Sitzungsrichtlinien, um Quarantäne- und Autorisierungsgruppen zu konfigurieren, die an einen Benutzer, eine Gruppe oder einen virtuellen Server gebunden sind. Sie können Benutzer anhand eines Ausdrucks zur Überprüfung des Client-Geräts innerhalb der Sitzungsrichtlinie Gruppen zuweisen. Wenn der Benutzer Mitglied einer Gruppe ist, wendet Citrix Gateway die Sitzungsrichtlinie basierend auf der Gruppenmitgliedschaft an.

### Konfigurieren von Autorisierungsgruppen

Wenn Sie einen Endpoint Analysis-Scan konfigurieren, können Sie Benutzer dynamisch zu einer Autorisierungsgruppe hinzufügen, wenn das Benutzergerät den Scan durchläuft. Beispielsweise erstellen Sie einen Endpoint Analysis-Scan, der die Domänenmitgliedschaft des Benutzergeräts überprüft. Erstellen Sie auf Citrix Gateway eine lokale Gruppe namens Domain-Joined Computers und fügen Sie sie als Autorisierungsgruppe für alle hinzu, die den Scan bestanden haben. Wenn Benutzer der Gruppe beitreten, erben Benutzer die mit der Gruppe verknüpften Richtlinien.

Sie können Autorisierungsrichtlinien nicht global oder an einen virtuellen Server binden. Sie können Autorisierungsgruppen verwenden, um einen Standardsatz von Autorisierungsrichtlinien bereitzustellen, wenn Benutzer nicht als Mitglieder einer anderen Gruppe auf Citrix Gateway konfiguriert sind.

#### So konfigurieren Sie eine Autorisierungsgruppe mithilfe einer Sitzungsrichtlinie

1. Navigieren Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. **Geben Sie im Feld Name einen Namen für das Profil ein.**
6. Klicken Sie auf der Registerkarte Sicherheit auf **Erweiterte Einstellungen**.
7. Klicken Sie unter Autorisierungsgruppen auf **Global überschreiben** und wählen Sie eine Gruppe aus der Dropdownliste aus.
8. Klicken Sie auf **Hinzufügen**, klicken Sie auf **OK** und dann auf **Erstellen**.
9. Wählen **Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben Benannte Ausdrücke **die Option Allgemein**aus, wählen Sie **Wahrer Wert**aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen** und dann auf **Schließen**.

Nachdem Sie die Sitzungsrichtlinie erstellt haben, können Sie sie an einen Benutzer, eine Gruppe oder einen virtuellen Server binden.

#### So konfigurieren Sie eine globale Berechtigungsgruppe

1. Erweitern Sie **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.

2. Klicken Sie im Detailbereich unter Einstellungen auf **Globale Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte Sicherheit auf **Erweiterte Einstellungen**.
4. Wählen Sie unter Autorisierungsgruppe eine Gruppe aus der Dropdownliste aus.
5. Klicken Sie auf **Hinzufügen** und dann auf **OK**.

Wenn Sie eine Autorisierungsgruppe entweder global oder aus der Sitzungsrichtlinie entfernen möchten, wählen Sie im Dialogfeld Sicherheitseinstellungen —Erweitert die Autorisierungsgruppe aus der Liste aus und klicken Sie dann auf **Entfernen**.

### Quarantänegruppen konfigurieren

Wenn Sie eine Quarantänegruppe konfigurieren, konfigurieren Sie den Ausdruck für die Überprüfung des Client-Geräts mithilfe des Dialogfelds Sicherheitseinstellungen —Erweiterte Einstellungen in einem Sitzungsprofil.

**Um das Client-Gerät zu konfigurieren, überprüfen Sie den Ausdruck für eine Quarantänegruppe**

1. Navigieren Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. **Geben Sie im Feld Name einen Namen für das Profil ein.**
6. Klicken Sie auf der Registerkarte Sicherheit auf **Erweiterte Einstellungen**.
7. Klicken Sie unter **Client Security**auf **Override Global** und dann auf **New**.
8. Konfigurieren Sie im Dialogfeld **Client-Ausdruck** den Prüfausdruck für das Client-Gerät und klicken Sie dann auf **Erstellen**.
9. Wählen Sie unter **Quarantänegruppe**die Gruppe aus.
10. Geben Sie unter Fehlermeldung eine Meldung ein, die das Problem für Benutzer beschreibt, und klicken Sie dann auf **Erstellen**.
11. Wählen Sie im Dialogfeld **Sitzungsrichtlinie erstellen** neben "Benannte Ausdrücke"die Option **Allgemein**, wählen Sie **True** und klicken Sie auf **Ausdruck hinzufügen**.
12. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

Nachdem Sie die Sitzungsrichtlinie erstellt haben, binden Sie sie an einen Benutzer, eine Gruppe oder einen virtuellen Server.

> **Hinweis:**
>
> Wenn der Endpoint Analysis-Scan fehlschlägt und der Benutzer in die Quarantänegruppe aufgenommen wird, sind die an die Quarantänegruppe gebundenen Richtlinien nur wirksam, wenn keine direkt an den Benutzer gebundenen Richtlinien vorhanden sind, die eine gleiche

> oder niedrigere Prioritätszahl als die an die Quarantänegruppe gebundenen Richtlinien haben.

**So konfigurieren Sie eine globale Quarantänegruppe**

1. Erweitern Sie **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter Einstellungen auf **Globale Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte **Sicherheit** auf **Erweiterte Einstellungen**.
4. Konfigurieren Sie in **Client Security**den Ausdruck zur Überprüfung des Client-Geräts.
5. Wählen Sie unter **Quarantänegruppe**die Gruppe aus.
6. Geben Sie unter **Fehlermeldung**eine Meldung ein, die das Problem für Benutzer beschreibt, und klicken Sie dann auf **OK**.

## Ausdrücke für Geräteprüfungen vor der Authentifizierung für Benutzergeräte

March 27, 2024

> **Wichtig:**
>
> Die Endpunktanalyse dient dazu, das Benutzergerät anhand vorab festgelegter Konformitätskriterien zu analysieren. Die Sicherheit der Endbenutzergeräte wird nicht erzwungen oder validiert. Es wird empfohlen, Endpunktsicherheitssysteme zu verwenden, um Geräte vor lokalen Administratorangriffen zu schützen.

Citrix Gateway bietet verschiedene Endpunktkonformitätsprüfungen während der Benutzeranmeldung oder zu anderen konfigurierten Zeiten während einer Sitzung, die bei der Validierung der Benutzergeräte helfen. Nur die Benutzergeräte, die diese Prüfungen bestehen, dürfen eine Citrix Gateway-Sitzung einrichten.

Im Folgenden sind die Arten von Prüfungen auf Benutzergeräten aufgeführt, die Sie auf Citrix Gateway konfigurieren können:

- Spam-Antispam
- Antivirus
- Richtlinien für Dateien
- Sicherheit im Internet
- Betriebssystem
- Persönliche Firewall
- Prozess-Richtlinien
- Registry-Richtlinien

- Service-Richtlinien

Wenn eine Geräteüberprüfung auf dem Benutzergerät fehlschlägt, werden bis zu einer nachfolgenden Prüfung keine neuen Verbindungen hergestellt (bei Prüfungen, die in regelmäßigen Abständen durchgeführt werden). Der Datenverkehr, der über bestehende Verbindungen fließt, tunnelt jedoch weiterhin durch Citrix Gateway.

Sie können das Konfigurationsprogramm verwenden, um Vorauthentifizierungsrichtlinien oder Ausdrücke für Geräteprüfungen innerhalb von Sitzungsrichtlinien zu konfigurieren, die für die Durchführung von Prüfungen auf Benutzergeräten konzipiert sind.

## Konfigurieren von Antiviren-, Firewall-, Internetsicherheit- oder Antispam-Ausdrücken

Sie konfigurieren Einstellungen für Antiviren-, Firewall-, Internetsicherheits- und Antispam-Richtlinien im Dialogfeld **Ausdruck hinzufügen**. Die Einstellungen für jede Richtlinie sind dieselben: Die Unterschiede sind die Werte, die Sie auswählen. Wenn Sie beispielsweise das Benutzergerät auf Norton Antivirus-Version 10 und ZoneAlarm Pro überprüfen möchten, erstellen Sie zwei Ausdrücke innerhalb der Sitzungs- oder Vorauthentifizierungsrichtlinie, die den Namen und die Versionsnummer jeder Anwendung angeben.

Wenn Sie Client Security als Ausdruckstyp auswählen, können Sie Folgendes konfigurieren:

- Komponente: Die Art der Clientsicherheit, wie Antivirus, Firewall oder Registrierungseintrag.
- Name: Der Name der Anwendung, des Prozesses, der Datei, des Registrierungseintrags oder des Betriebssystems.
- Qualifier: Die Version oder der Wert der Komponente, auf die der Ausdruck prüft.
- Operator: Überprüft, ob der Wert existiert oder dem Wert entspricht.
- Wert: Die Anwendungsversion für Antiviren-, Firewall-, Internetsicherheit- oder Antispam-Software auf dem Benutzergerät.
- Frequenz: Häufigkeit, mit der ein Scan nach der Authentifizierung ausgeführt wird, in Minuten.
- Fehlergewicht: Eine Gewichtung, die jeder in einem verschachtelten Ausdruck enthaltenen Fehlermeldung zugewiesen wird, wenn mehrere Ausdrücke unterschiedliche Fehlerzeichenfolgen aufweisen. Das Gewicht bestimmt, welche Fehlermeldung angezeigt wird.
- Frische: Definiert, wie alt eine Virusdefinition sein kann. Sie können den Ausdruck beispielsweise so konfigurieren, dass Virendefinitionen nicht älter als drei Tage sind.

### So fügen Sie einer Vorauthentifizierungs- oder Sitzungsrichtlinie eine Richtlinie zur Überprüfung des Client-Geräts hinzu

1. Führen Sie im Konfigurationsdienstprogramm im Navigationsbereich einen der folgenden Schritte aus:

a) Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
b) Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung** und klicken Sie dann auf **Pre-Authentication EPA**.

2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Hinzufügen**.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Any Expression auf Hinzufügen.
5. Wählen Sie im Dialogfeld Ausdruck hinzufügen unter Ausdruckstyp die Option **Client-Sicherheit**aus.
6. Konfigurieren Sie die Einstellungen für Folgendes:

a) Wählen Sie unter Komponente das Element aus, nach dem gescannt werden soll.
b) Geben Sie unter Name den Namen der Anwendung ein.
c) Wählen Sie unter Qualifier die Option **Version**aus.
d) Wählen Sie unter Operator den Wert aus.
e) Geben Sie im Feld Wert die Prüfzeichenfolge für das Client-Gerät ein, klicken Sie auf **OK**, klicken Sie auf **Erstellen**und dann auf **Schließen**.

## Konfigurieren von Dienstrichtlinien

Ein Dienst ist ein Programm, das geräuschlos auf dem Benutzergerät läuft. Wenn Sie eine Sitzungs- oder Vorauthentifizierungsrichtlinie erstellen, können Sie einen Ausdruck erstellen, der sicherstellt, dass Benutzergeräte einen bestimmten Dienst ausführen, wenn die Sitzung eingerichtet wird.

### So konfigurieren Sie eine Dienstrichtlinie

1. Führen Sie im Konfigurationsdienstprogramm im Navigationsbereich einen der folgenden Schritte aus:

a) Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf Sitzung.
b) Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung und klicken Sie dann auf Pre-Authentication**EPA.

2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Any Expression auf Hinzufügen.
5. Wählen Sie im Dialogfeld Ausdruck hinzufügen unter Ausdruckstyp die Option Client-Sicherheitaus.

6. Konfigurieren Sie die Einstellungen für Folgendes:
    a) Wählen Sie unter Komponente Dienst aus.
    b) Geben Sie unter Name den Namen des Dienstes ein.
    c) Lassen Sie in Qualifier das Feld leer oder wählen Sie Version.
    d) Führen Sie abhängig von Ihrer Auswahl in Qualifier einen der folgenden Schritte aus:
        - Wenn leer gelassen, wählen Sie in Operator == oder! =
        - Wenn Sie Version ausgewählt haben, geben Sie in Operator unter Wert den Wert ein, klicken Sie auf OK, und klicken Sie dann auf Schließen.

Sie können eine Liste aller verfügbaren Dienste und den Status für jeden auf einem Windows-basierten Computer an folgender Stelle überprüfen:

**Systemsteuerung > Verwaltungstools > Dienste**

> **Hinweis:**
>
> Der Dienstname für jeden Dienst variiert von seinem aufgelisteten Namen. Suchen Sie im Dialogfeld
> Eigenschaften nach dem Namen des Dienstes.

## Konfigurieren von Prozessrichtlinien

Wenn Sie eine Sitzungs- oder Vorauthentifizierungsrichtlinie erstellen, können Sie eine Regel definieren, die erfordert, dass alle Benutzergeräte einen bestimmten Prozess ausführen müssen, wenn sich Benutzer anmelden. Der Prozess kann jede Anwendung sein und kundenspezifische Anwendungen beinhalten.

Hinweis: Die Liste aller Prozesse, die auf einem Windows-Computer ausgeführt werden, wird auf der Registerkarte
**Prozesse** des Windows Task-Managers angezeigt.

### So konfigurieren Sie eine Prozessrichtlinie

1. Führen Sie im Konfigurationsdienstprogramm im Navigationsbereich einen der folgenden Schritte aus:
    a) Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway\ > Richtlinien** und klicken Sie dann auf Sitzung.
    b) Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung**, und klicken Sie dann auf Pre-Authentication EPA.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.

3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Any Expression auf Hinzufügen.
5. Wählen Sie im Dialogfeld Ausdruck hinzufügen unter Ausdruckstyp die Option Client-Sicherheitaus.
6. Konfigurieren Sie die Einstellungen für Folgendes:

    a) Wählen Sie unter Komponente die Option Prozess aus.
    b) Geben Sie unter Name den Namen der Anwendung ein.
    c) Wählen Sie unter Operator EXISTS oder NOTEXISTS aus, klicken Sie auf OK und dann auf Schließen.

Wenn Sie eine Endpoint Analysis-Richtlinie (Vor- oder Nachauthentifizierung) konfigurieren, um nach einem Prozess zu suchen, können Sie eine MD5-Prüfsumme konfigurieren.

Wenn Sie den Ausdruck für die Richtlinie erstellen, können Sie die MD5-Prüfsumme zu dem Prozess hinzufügen, nach dem Sie suchen. Wenn Sie beispielsweise prüfen, ob notepad.exe auf dem Benutzergerät ausgeführt wird, lautet der Ausdruck:
CLIENT.APPLICATION.PROCESS (notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

### Konfigurieren von Betriebssystemrichtlinien

Wenn Sie eine Sitzungs- oder Vorauthentifizierungsrichtlinie erstellen, können Sie Prüfzeichenfolgen für das Client-Gerät konfigurieren, um festzustellen, ob auf dem Benutzergerät ein bestimmtes Betriebssystem ausgeführt wird, wenn sich Benutzer anmelden. Sie können den Ausdruck auch so konfigurieren, dass nach einem bestimmten Service Pack oder Hotfix gesucht wird.

Die Werte für Windows und Macintosh lauten:

| Betriebssystem | Wert |
|---|---|
| macOS X | macOS |
| Windows 8.1 | win8.1 |
| Windows 8 | win8 |
| Windows 7 | win7 |
| Windows Vista | vista |
| Windows XP | `winxp` |
| Windows Server 2008 | win2008 |
| Windows Server 2003 | win2003 |
| Windows 2000 Server | win2000 |

| Betriebssystem | Wert |
| --- | --- |
| Windows 64-Bit-Plattform | win64 |

**So konfigurieren Sie eine Betriebssystemrichtlinie über die GUI**

1. Führen Sie im Navigationsbereich einen der folgenden Schritte aus:
   a) Navigieren Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
   b) Navigieren Sie zu **Citrix Gateway > Richtlinien > Vorauthentifizierung**.
2. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Wählen Sie unter **Request Action** eine vorhandene Aktion aus oder erstellen Sie eine.
5. Klicken Sie auf **Expression Editor**.
6. Wählen Sie unter **Ausdruckstyp auswählen** die Option **Clientsicherheit** aus.
7. Konfigurieren Sie die Einstellungen für Folgendes:
   a) Wählen Sie unter **Komponente** die Option **Betriebssystem** aus.
   b) Geben Sie unter**Name** den Namen des Betriebssystems ein.
   c) Führen Sie in Qualifier einen der folgenden Schritte aus:
      - Lassen Sie das Feld leer
      - Wählen Sie **Service Pack**
      - Wählen Sie **Hotfix**
      - Wählen Sie **Version** (nur für macOS)
   d) Führen Sie abhängig von Ihrer Auswahl in Schritt 7 in Operator einen der folgenden Schritte aus:
      - Wenn Qualifier leer ist, wählen Sie in Operator EQUAL (= =), NOTEQUAL (! =), EXISTS oder NOTEXISTS.
      - Wenn Sie Service Pack oder Hotfix ausgewählt haben, wählen Sie den Operator aus und geben Sie unter Wert den Wert ein.
8. Klicken Sie auf **Fertig** und dann auf **Schließen**.

Wenn Sie ein Service Pack wie client.os (`winxp`) `.sp`konfigurieren und eine Zahl nicht im Feld **Wert** enthalten ist, gibt Citrix Gateway eine Fehlermeldung zurück, da der Ausdruck ungültig ist.

Wenn auf dem Betriebssystem Service Packs wie Service Pack 3 und Service Pack 4 vorhanden sind, können Sie eine Überprüfung nur für Service Pack 4 konfigurieren, da das Vorhandensein von Service Pack 4 automatisch darauf hinweist, dass frühere Service Packs vorhanden sind.

### Konfiguration von Registrierungsrichtlinien

Wenn Sie eine Sitzungs- oder Vorauthentifizierungsrichtlinie erstellen, können Sie auf dem Benutzergerät nach Existenz und Wert von Registrierungseinträgen suchen. Die Sitzung wird nur eingerichtet, wenn der bestimmte Eintrag existiert oder den konfigurierten oder höheren Wert hat.

Beachten Sie beim Konfigurieren eines Registrierungsausdrucks die folgenden Richtlinien:

- Vier umgekehrte Schrägstriche werden verwendet, um Schlüssel und Unterschlüssel zu trennen, wie z

  HKEY_LOCAL_MACHINE\\\\SOFTWARE

- Unterstriche werden verwendet, um den Unterschlüssel und den zugehörigen Wertnamen zu trennen, z. B.

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\VirusSoftware_Version

- Ein umgekehrter Schrägstrich (\) wird verwendet, um ein Leerzeichen zu bezeichnen, wie in den folgenden zwei Beispielen:

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\Citrix\\\\Secure\ Access\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\Software\\\\Symantec\\Norton\ AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5

Im Folgenden finden Sie einen Registrierungsausdruck, der bei der Benutzeranmeldung nach dem Registrierungsschlüssel von Citrix Secure Access Agent sucht:

CLIENT.REG(secureaccess).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client

> **Hinweis:**
>
> Wenn Sie nach Registrierungsschlüsseln und -werten suchen und im Dialogfeld Ausdruck Advanced Free-Form auswählen, muss der Ausdruck mit CLIENT.REG beginnen.

Registrierungsprüfungen werden unter den folgenden gängigsten fünf Typen unterstützt:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Zu überprüfende Registrierungswerte verwenden die folgenden Typen:

- Zeichenfolge

  Für den Zeichenfolgenwerttyp wird die Berücksichtigung von Groß- und Kleinschreibung geprüft.

- DWORD

  Für den DWORD-Typ wird der Wert verglichen und muss gleich sein.

- Erweiterter String

  Andere Typen, wie Binary und Multi-String, werden nicht unterstützt.

- Nur der Vergleichsoperator '==' wird unterstützt.
- Andere Vergleichsoperatoren wie <, > und Vergleiche mit Berücksichtigung der Groß-/Kleinschreibung werden nicht unterstützt.
- Die gesamte Länge der Registrierungszeichenfolge muss weniger als 256 Byte betragen.

Sie können dem Ausdruck einen Wert hinzufügen. Der Wert kann eine Softwareversion, eine Service Pack-Version oder ein anderer Wert sein, der in der Registrierung angezeigt wird. Wenn der Datenwert in der Registrierung nicht mit dem Wert übereinstimmt, mit dem Sie testen, wird Benutzern die Anmeldung verweigert.

> **Hinweis:**
>
> Sie können innerhalb eines Unterschlüssels nicht nach einem Wert suchen. Der Scan muss mit dem benannten Wert und dem zugehörigen Datenwert übereinstimmen.

**So konfigurieren Sie eine Registrierungsrichtlinie**

1. Führen Sie im Konfigurationsdienstprogramm im Navigationsbereich einen der folgenden Schritte aus:
   a) Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway\ > Richtlinien** und klicken Sie dann auf Sitzung.
   b) Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway > Richtlinien > Authentifizierung/Autorisierung**, und klicken Sie dann auf Pre-Authentication EPA.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Any Expression auf Hinzufügen.
5. Wählen Sie im Dialogfeld Ausdruck hinzufügen unter Ausdruckstyp die Option Client-Sicherheitaus.
6. Konfigurieren Sie die Einstellungen für Folgendes:
   a) Wählen Sie unter Component Registry aus.
   b) Geben Sie unter Name den Namen des Registrierungsschlüssels ein.
   c) Lassen Sie in Qualifier das Feld leer oder wählen Sie Wert.

d) Führen Sie unter Operator einen der folgenden Schritte aus:
   - Wenn Qualifier leer gelassen wird, wählen Sie EXISTS oder NOTEXISTS
   - Wenn Sie Wert in Qualifier gewählt haben, wählen Sie entweder == oder! ==

e) Geben Sie unter Wert den Wert so ein, wie er im Registrierungseditor angezeigt wird, klicken Sie auf OK und dann auf Schließen.

## Ausdrücke für die Geräteüberprüfung für zusammengesetzte Clients konfigurieren

Sie können Client-Geräte-Prüfzeichenfolgen kombinieren, um zusammengesetzte Client-Geräteprüfausdrücke zu bilden.

Die booleschen Operatoren, die in Citrix Gateway unterstützt werden, sind:

- Und (&&)

---

Oder (

---

-

- Nicht (!)

Für eine höhere Präzision können Sie die Zeichenfolgen in Klammern gruppieren.

> **Hinweis:**
>
> Wenn Sie die Befehlszeile zum Konfigurieren von Ausdrücken verwenden, verwenden Sie Klammern, um Geräteprüfausdrücke zu gruppieren, wenn Sie einen zusammengesetzten Ausdruck erstellen. Die Verwendung von Klammern verbessert das Verständnis und das Debuggen des Clientausdrucks.

### Konfigurieren Sie Richtlinien mit dem Operator UND (&&)

Der AND (&&)-Operator kombiniert zwei Prüfzeichenfolgen für das Client-Gerät, sodass die kombinierte Prüfung nur dann erfolgreich ist, wenn beide Prüfungen wahr sind. Der Ausdruck wird von links nach rechts ausgewertet und wenn die erste Prüfung fehlschlägt, wird die zweite Prüfung nicht durchgeführt.

Sie können den Operator AND (&&) mit dem Schlüsselwort ‘UND’oder den Symbolen ‘&&’konfigurieren.

Beispiel:

Im Folgenden finden Sie eine Überprüfung des Client-Geräts, bei der festgestellt wird, ob auf dem Benutzergerät Version 7.0 von Sophos Antivirus installiert ist und ausgeführt wird. Außerdem wird überprüft, ob der Net Logon-Dienst auf demselben Computer ausgeführt wird.

```
CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon)
EXISTS
```

Diese Zeichenfolge kann auch wie folgt konfiguriert werden:

```
CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon)
EXISTS
```

#### Konfigurieren Sie Richtlinien mit dem Operator ODER (||)

Der OR-Operator ( | | ) kombiniert zwei Geräteprüfzeichenfolgen. Die zusammengesetzte Prüfung ist erfolgreich, wenn eine der beiden Prüfungen wahr ist. Der Ausdruck wird von links nach rechts ausgewertet und wenn die erste Prüfung erfolgreich ist, wird die zweite Prüfung nicht durchgeführt. Wenn die erste Prüfung nicht bestanden wird, wird die zweite Prüfung durchgeführt.

Sie können den OR-Operator ( | | ) mit dem Schlüsselwort `OR` oder dem Symbol | | konfigurieren.

Beispiel:

Das Folgende ist eine Clientgeräteprüfung, mit der festgestellt wird, ob auf dem Benutzergerät die Datei `c:\\file.txt` ist oder ob der Prozess `putty.exe` darauf ausgeführt wird.

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)OR (client.proc(putty.exe)
EXISTS
```

Diese Zeichenfolge kann auch als konfiguriert werden

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)|| (client.proc(putty.exe)
EXISTS
```

### Konfigurieren Sie Richtlinien mit dem NOT (!) Operator

Der NOT (!) oder Negationsoperator negiert die Prüfzeichenfolge des Client-Geräts.

Beispiel:

Die folgende Client-Geräteüberprüfung ist erfolgreich, wenn die Datei c:\sophos_virus_defs.dat NICHT älter als zwei Tage ist:

```
\!(client.file(c:\\\\\\\\\\sophos\\_virus\\_defs.dat).timestamp==2dy)
```

# Gerätezertifikat in nFactor als EPA-Komponente

January 19, 2024

Device Certificate kann in nFactor als EPA-Komponente konfiguriert werden. Gerätezertifikat kann als beliebiger Faktor als Teil von EPA erscheinen.

Im Folgenden sind die Vorteile der Konfiguration Device Certificate in nFactor als EPA-Komponente.

- Der Fehler bei der Gerätezertifikatüberprüfung führt nicht zu einem Anmeldefehler. Basierend auf der Konfiguration kann die Anmeldung fortgesetzt werden und der Benutzer kann unter Gruppen mit eingeschränktem Zugriff platziert werden.
- Da die Gerätezertifikatprüfung richtliniengesteuert ist, können Sie den Zugriff auf Ihre Intranetressourcen Ihres Unternehmens basierend auf der Authentifizierung des Gerätezertifikats selektiv zulassen oder blockieren. Beispielsweise kann die Gerätezertifikatauthentifizierung verwendet werden, um bedingten Zugriff auf Office 365-Anwendung nur auf unternehmensverwalteten Laptops bereitzustellen.

Die Gerätezertifikatvalidierung kann nicht Teil eines periodischen EPA-Scans sein.

> **Wichtig:** Windows erteilt standardmäßig Administratorrechte für den Zugriff auf Gerätezertifikate. Um die Gerätezertifikatsprüfung für Benutzer ohne Administratoren hinzuzufügen, müssen Sie VPN-Plug-In der gleichen Version wie das EPA-Plug-on auf dem Gerät installieren.

## Gerätezertifikat in nFactor als EPA-Komponente konfigurieren

**Um Device Certificate in nFactor als EPA-Komponente über die Befehlszeilenschnittstelle zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:**

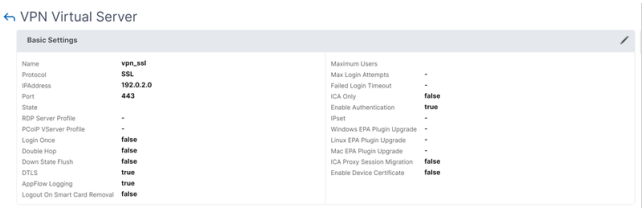
```
add authentication epaAction epa-act -csecexpr sys.client_expr("device-cert_0_0") -defaultgroup epa_pass -quarantine_group epa_fail

<!--NeedCopy-->
```

**So konfigurieren Sie Device Certificate in nFactor als EPA-Komponente für virtuellen VPN-Server mit der Citrix ADC-GUI:**

1. Navigieren Sie in der NetScaler GUI zu **Konfiguration > Citrix Gateway > Virtuelle Server**.
2. Wählen Sie auf der Seite **Virtuelle Citrix Gateway Server** den zu ändernden virtuellen Server aus, und klicken Sie auf **Bearbeiten** .
3. Klicken Sie auf der Seite **VPN Virtual Server** auf das Symbol Bearbeiten.

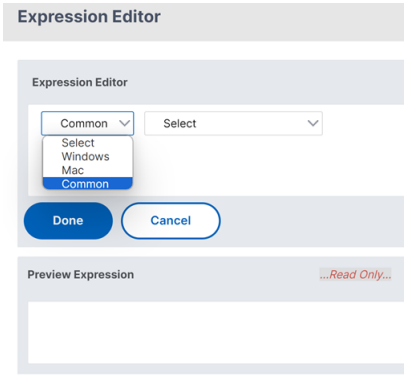



4. Klicken Sie auf **Mehr**.
5. Klicken Sie neben dem Abschnitt Zertifizierungsstelle für Gerätezertifikat auf **Hinzufügen**, und klicken Sie auf OK.

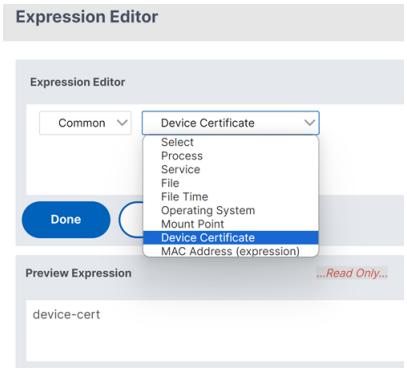

> Aktivieren Sie nicht das Kontrollkästchen Gerätezertifikat aktivieren. Wenn Sie es aktivieren, wird die Gerätezertifikatvalidierung im klassischen EPA aktiviert.

6. Navigieren Sie in der NetScaler GUI zu **Konfiguration > Sicherheit > AAA —Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > EPA >**.
7. Klicken Sie auf der Seite **Authentication EPA Action** auf **Hinzufügen**. Sie können auf **Bearbeiten** klicken, um eine vorhandene EPA-Aktion zu bearbeiten.
8. Geben Sie auf der Seite **Authentifizierungs-EPA-Aktion erstellen die Werte für die erforderlichen Felder ein**, um eine Authentifizierungs-EPA-Aktion zu erstellen, und klicken Sie auf den Link **EPA-Editor** .
9. Wählen Sie in der Liste **Ausdruckseditor** die Option **Gemeinsam** aus.




10. Wählen Sie **Gerätezertifikat** aus der nachfolgenden Liste, die angezeigt wird, und klicken Sie auf **Fertig**, um die Konfiguration abzuschließen.

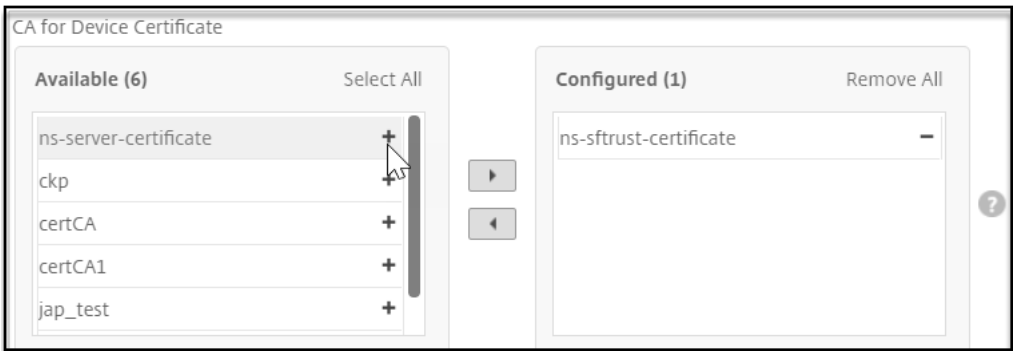



**So konfigurieren Sie Device Certificate in nFactor als EPA-Komponente für virtuellen AAA-Server mit der Citrix ADC-GUI:**

1. Navigieren Sie in der Citrix DC GUI zu **Sicherheit > AAA-Anwendungsdatenverkehr > Virtuelle Server**.
2. Wählen Sie auf der Seite **Virtuelle Citrix Gateway Server** den zu ändernden virtuellen Server aus, und klicken Sie auf Bearbeiten.
3. Klicken Sie auf der Seite **Virtueller Authentifizierungsserver** auf das Symbol Bearbeiten.
4. Klicken Sie auf **Mehr**.
5. Klicken **Sie** neben dem Abschnitt **Zertifizierungsstelle für Gerätezertifikat** auf Hinzufügen.

6. Wählen Sie das hinzuzufügende Zertifikat aus, und klicken Sie auf **OK**, um die Konfiguration abzuschließen.




7. Wiederholen Sie **Schritt 6 bis Schritt 10**, die im vorherigen Abschnitt aufgeführt ist, um die Konfiguration abzuschließen.

## EPA-Scan als Faktor bei der nFactor-Authentifizierung

March 27, 2024

> **Wichtig:**
>
> Die Endpunktanalyse dient dazu, das Benutzergerät anhand vorab festgelegter Konformitätskriterien zu analysieren. Die Sicherheit der Endbenutzergeräte wird nicht erzwungen oder validiert. Es wird empfohlen, Endpunktsicherheitssysteme zu verwenden, um Geräte vor lokalen Administratorangriffen zu schützen.

Im Folgenden sind einige der grundlegenden Einheiten von nFactor EPA aufgeführt.

**EPA-Aktion:** EPA Action ist ein Aktionstyp, der für nFactor EPA eingeführt wurde. Es enthält Folgendes:

- Ausdruck zur Überprüfung des Client-Geräts: Dieser Ausdruck wird zur Auswertung an das Gateway-EPA-Plug-In gesendet.
- Erfolgsgruppe: Diese Gruppe wird, sofern konfiguriert, an die Gateway-Sitzung vererbt, wenn das EPA-Ergebnis wahr ist.
- Quarantänegruppe: Diese Gruppe wird, sofern konfiguriert, an die Gateway-Sitzung vererbt, wenn das EPA-Ergebnis falsch ist.
- KillProcess: Dies ist der Name des Prozesses, den der EPA-Prozess beenden muss.
- DeleteFiles: Gibt durch Kommas getrennte Pfade zu Dateien an, die der EPA-Prozess löschen muss.

Gruppen können während der Dauer der Sitzung verwendet werden, um festzustellen, ob der Kunde bestimmte EPA-Bedingungen erfüllt.
Wenn bei einem bestimmten Faktor die EPA fehlschlägt und die letzte Aktion keine "Quarantänegruppe"enthält, wird die Authentifizierung für diesen Benutzer beendet.
Wenn "Quarantänegruppe"existiert, wird die Authentifizierung fortgesetzt und der Administrator kann prüfen, ob die Gruppe eingeschränkten Zugriff gewährt. Weitere Einzelheiten finden Sie unter EPA-Ausführung.

**EPA-Richtlinie:** In nFactor werden alle Richtlinien mit derselben Syntax „Authentifizierungsrichtlinie hinzufügen"hinzugefügt. Die Art der Maßnahme qualifiziert die Richtlinie jedoch als EPA-Richtlinie.

**EPA-Faktor:** Der EPA-Faktor ist ein reguläres Policy Label. Es gibt kein Unternehmen, das als EPA-Faktor bezeichnet wird. Sobald die EPA-Richtlinie an einen Faktor gebunden ist, erbt sie bestimmte Eigenschaften, die sie zu einem EPA-Faktor machen.

> **Hinweis:**
>
> Der Begriff "EPA-Faktor"wird in diesem Dokument häufig verwendet, um einen Faktor zu bezeichnen, der in den EPA-Richtlinien enthalten ist.

**EPA —Quarantäne:** Wenn bei einem bestimmten Faktor alle Prüfausdrücke aller Aktionen auf dem Client-Gerät fehlschlagen und wenn die letzte Aktion "Quarantänegruppe"enthält, wird diese Gruppe zur Sitzung hinzugefügt und der NextFactor wird untersucht. Das heißt, trotz des Scheiterns qualifiziert die Anwesenheit der "Quarantänegruppe"die Sitzung für die nächste Stufe. Aufgrund der Vererbung einer speziellen Gruppe kann der Administrator die Sitzung jedoch auf eingeschränkten Zugriff oder zusätzliche Authentifizierungsrichtlinien wie OTP oder SAML abweisen.

Wenn bei der letzten Aktion keine Quarantänegruppe vorhanden ist, wird die Authentifizierung bei einem Fehler beendet.

**EPA in nFactor verwendet auch die folgenden Entitäten:**

- **LoginSchema:** XML-Darstellung des Anmeldeformulars. Es definiert die "Ansicht"des Anmeldeformulars und hat auch Eigenschaften eines "Faktors".
- **Policy Label oder Richtlinienfaktor:** Es handelt sich um eine Sammlung von Richtlinien, die in einer bestimmten Authentifizierungsphase getestet werden.
- **Virtuelles Serverlabel:** Virtueller Server ist auch ein Richtlinienlabel, das heißt, man kann Richtlinien an den virtuellen Server binden. Der virtuelle Server ist jedoch die Sammlung verschiedener Policy Label, da er der Einstiegspunkt für den Benutzerzugriff ist.
- **nächster Faktor:** Er wird verwendet, um das Policylabel/den Policy-Faktor anzugeben, der angewendet werden soll, sobald die angegebene Authentifizierungsrichtlinie erfolgreich ist.
- **NO_AUTHN-Richtlinie:** spezielle Richtlinie, deren Aktion immer erfolgreich ist.
- **Passthrough-Faktor:** —Ist ein Policylabel/Faktor, dessen Anmeldeschema keine Ansicht enthält. Dies ist ein Hinweis für die Citrix ADC Appliance, die Authentifizierung mit dem angegebe-

nen Faktor ohne Benutzereingriff fortzusetzen.

Weitere Informationen finden Sie unter Konzepte, Entitäten und Terminologie von nFactor.

### gegenseitige Exklusivität des EPA-Faktors

EPA-Faktor enthält eine oder mehrere EPA-Richtlinien. Sobald die EPA-Richtlinien an einen Faktor gebunden sind, sind reguläre Authentifizierungsrichtlinien für diesen Faktor nicht zulässig. Diese Einschränkung soll die beste Benutzererfahrung und eine saubere Trennung der Endpunktanalyse bieten. Die einzige Ausnahme von dieser Regel ist die Richtlinie NO_AUTHN. Da es sich bei der NO_AUTHN-Richtlinie um eine spezielle Richtlinie handelt, die verwendet wird, um "bei einem Ausfallsprung"zu simulieren, ist sie im EPA-Faktor zulässig.

### EPA-Ausführung

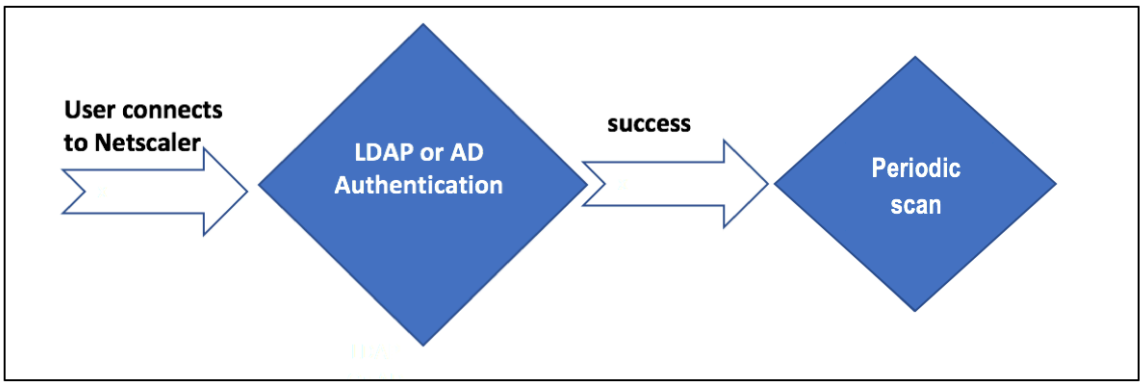
Bei jedem bestimmten Faktor (einschließlich des Faktors für virtuelle Server) prüft die Citrix ADC Appliance vor dem Ausfüllen des Anmeldeformulars, ob der Faktor für EPA konfiguriert ist. Wenn ja, sendet es eine bestimmte Antwort an den Client (UI), sodass die EPA-Sequenz ausgelöst wird. Diese Sequenz umfasst, dass der Client Ausdrücke zur Überprüfung des Client-Geräts anfordert und die Ergebnisse sendet.
Die Ausdrücke für die Überprüfung des Client-Geräts für alle Richtlinien in einem Faktor werden gleichzeitig an den Client gesendet. Sobald Ergebnisse auf der Citrix ADC Appliance erhalten wurden, wird jeder der Ausdrücke in allen Aktionen in einer Sequenz ausgewertet. Die erste Aktion, die zu einer erfolgreichen EPA führt, beendet diesen Faktor, und DefaultGroup wird, falls konfiguriert, in die Sitzung vererbt. Wenn eine NO_AUTHN-Richtlinie angetroffen wird, gilt dies als automatischer Erfolg. Wenn der NextFactor angegeben wird, fährt die Appliance mit diesem Faktor fort. Andernfalls endet die Authentifizierung.
Diese Bedingung gilt auch für den ersten Faktor. Wenn nach EPA auf dem virtuellen Server kein Authentifizierungsrichtlinienfaktor vorhanden ist, wird die Authentifizierung beendet. Dies unterscheidet sich vom klassischen Richtlinienverhalten, bei dem dem Benutzer immer die Anmeldeseite nach EPA angezeigt wird.
Falls jedoch keine erfolgreiche EPA-Richtlinie vorliegt, betrachtet Citrix Gateway die Quarantänegruppe, die für die letzte EPA-Richtlinie in diesem Faktor oder dieser Kaskade konfiguriert wurde. Wenn die letzte Richtlinie mit der Quarantänegruppe konfiguriert ist, wird diese Gruppe zur Sitzung hinzugefügt und der NextFactor wird überprüft. Wenn ein NextFactor existiert, geht die Authentifizierung zu diesem Faktor über. Andernfalls ist die Authentifizierung abgeschlossen.

## Konfigurieren Sie den regelmäßigen EPA-Scan als Faktor bei der nFactor-Authentifizierung

Sie können den regelmäßigen EPA-Scan mithilfe der erweiterten Richtlinieninfrastruktur als Faktor für die nFactor-Authentifizierung konfigurieren.

> **Hinweis:**
>
> In der klassischen Richtlinie wurde die periodische EPA als Teil der Sitzungsrichtlinie unter `vpn session action` konfiguriert.
> Die folgende Logik wird als Beispiel für die Implementierung des EPA-Scans als Faktor bei der nFactor-Authentifizierung verwendet.




- Der Benutzer versucht, eine Verbindung zu NetScaler Gateway Virtual IP herzustellen.
- Eine Anmeldeseite mit Benutzernamen und Kennwortfeld wird an den Benutzer gerendert, um Anmeldeinformationen anzugeben. Mit diesen Anmeldeinformationen wird eine LDAP- oder AD-basierte Authentifizierung im Back-End durchgeführt. Bei Erfolg wird dem Benutzer ein Popup angezeigt, um den EPA-Scan zu autorisieren.
- Sobald der Benutzer autorisiert hat, wird der EPA-Scan durchgeführt und basierend auf dem Erfolg oder Misserfolg der Benutzerclienteinstellungen wird Zugriff gewährt.
- Wenn der Scan erfolgreich ist, wird der EPA-Scan regelmäßig durchgeführt, um sicherzustellen, dass die konfigurierten Anforderungen für die Geräteüberprüfung weiterhin erfüllt sind.
- Wenn der EPA-Scan bei einer solchen Überprüfung fehlschlägt, wird die Sitzung beendet.

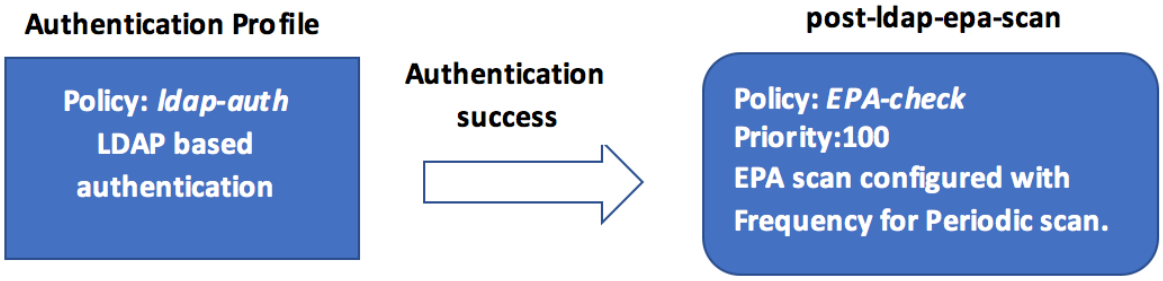
### Voraussetzungen

Es wird davon ausgegangen, dass die folgende Konfiguration vorhanden ist:

- Konfiguration des virtuellen VPN-Servers, des Gateway und der virtuellen Authentifizierungsserver
- LDAP-Serverkonfigurationen und zugehörige Richtlinien.

Im folgenden Abschnitt werden die erforderlichen Richtlinien und Policy Label-Konfigurationen sowie die Zuordnung von Richtlinien und Policy Label zu einem Authentifizierungsprofil beschrieben.




**Über die Befehlszeilenschnittstelle**

1. Erstellen Sie eine Aktion, um einen EPA-Scan vor der LDAP-Authentifizierung durchzuführen, und verknüpfen Sie sie mit einer EPA-Scanrichtlinie.

```
1 add authentication epaAction pre-ldap-epa-action -csecexpr "sys.
     client_expr ("proc_2_firefox")"
2
3 add authentication Policy pre-ldap-epa-pol -rule true -action pre-
     ldap-epa-action
4 <!--NeedCopy-->
```

   Der vorherige Ausdruck scannt, ob der Prozess ‘Firefox’läuft. Der EPA-Client überprüft alle 2 Minuten, ob der Prozess existiert, was durch die Ziffer „2“im Scanausdruck gekennzeichnet ist.

2. Konfigurieren Sie das Richtlinienlabel `pre-ldap-epa-label`, das die Richtlinie für den EPA-Scan hostet.

```
1 add authentication policylabel pre-ldap-epa-label -loginSchema
     LSCHEMA_INT
2 <!--NeedCopy-->
```

   > **Hinweis:**
   >
   > LSCHEMA_INT ist ein eingebautes Schema ohne Schema (noschema), was bedeutet, dass dem Benutzer in diesem Schritt keine zusätzliche Webseite präsentiert wird.

3. Ordnen Sie die in Schritt 1 konfigurierte Policy dem in Schritt 2 konfigurierten Policy Label zu. Dies vervollständigt den Authentifizierungsmechanismus.

```
1 bind authentication policylabel pre-ldap-epa-label -policyName pre
     -ldap-epa-pol -priority 100 -gotoPriorityExpression END
2 <!--NeedCopy-->
```

4. Konfigurieren Sie eine LDAP-Aktion und Richtlinie.

```
add authentication ldapAction ldap-act -serverIP 10.106.103.60 -
    ldapBase "dc=cgwsanity,dc=net" -ldapBindDn user1@example.net -
    ldapBindDnPassword 1.cloud -ldapLoginName samAccountName -
    groupAttrName memberOf -subAttributeName CN -passwdChange
    ENABLED

add authentication Policy ldap-pol -rule true -action ldap-act
<!--NeedCopy-->
```

5. Erstellen Sie ein Anmeldeschema mit aktiviertem SSO.

```
add authentication loginSchema ldap-schema -authenticationSchema "
    /nsconfig/loginschema/LoginSchema/SingleAuth.xml" -
    SSOCredentials Yes
<!--NeedCopy-->
```

6. Konfigurieren Sie das Richtlinienlabel `ldap-pol-label`, das die Richtlinie für die LDAP-Authentifizierung hostet.

```
add authentication policylabel ldap-pol-label -loginSchema ldap-
    schema
<!--NeedCopy-->
```

7. Binden Sie das in Schritt 5 konfigurierte Anmeldeschema an das in Schritt 6 konfigurierte Richtlinienlabel.

```
bind authentication policylabel ldap-pol-label -policyName ldap-
    pol -priority 100 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

8. Erstellen Sie eine Aktion, um einen EPA-Scan nach der LDAP-Authentifizierung durchzuführen, und verknüpfen Sie sie mit einer EPA-Scanrichtlinie.

```
add authentication epaAction post-ldap-epa-action -csecexpr "sys.
    client_expr ("proc_2_chrome")"

add authentication Policy post-ldap-epa-pol -rule true -action
    post-ldap-epa-action

add authentication policylabel post-ldap-epa-label -loginSchema
    LSCHEMA_INT

bind authentication policylabel post-ldap-epa-label -policyName
    post-ldap-epa-pol -priority 100 -gotoPriorityExpression
<!--NeedCopy-->
```

9. Wenn Sie alles zusammenfügen, ordnen Sie die Richtlinie dem virtuellen Authentifizierungsserver `pre-ldap-epa-pol` zu, wobei der nächste Schritt auf das Richtlinienlabel zeigt `ldap-pol-label`, um einen EPA-Scan durchzuführen.

```
bind authentication vserver user.auth.test -policy pre-ldap-epa-pol -priority 100 -nextFactor ldap-pol-label -gotoPriorityExpression NEXT

bind authentication policylabel ldap-pol-label -policyName ldap-pol -priority 100 -gotoPriorityExpression NEXT -nextFactor post-ldap-epa-label
<!--NeedCopy-->
```

**Hinweis:**

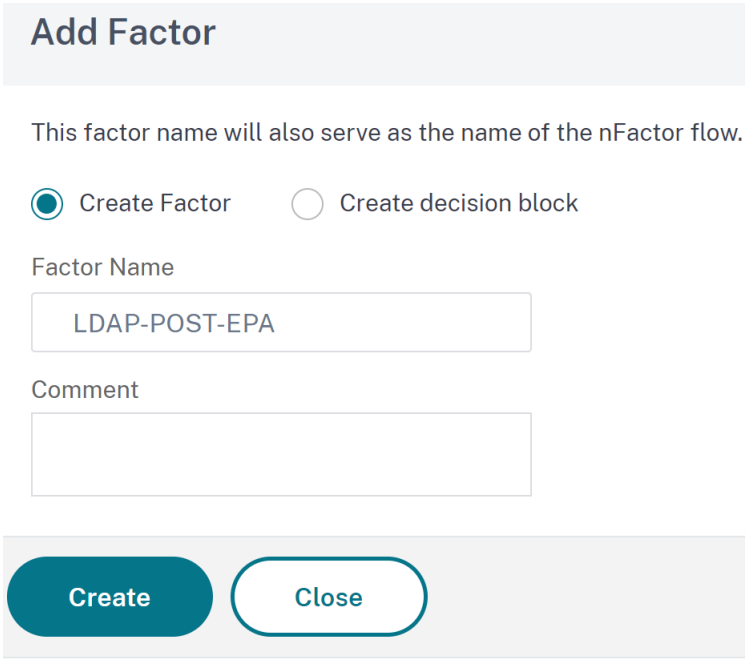
- Bei periodischen EPA, die als mehrere Faktoren konfiguriert sind, wird der neueste Faktor mit periodischer EPA-Konfiguration berücksichtigt.
- Regelmäßige Scans können nur mit dem EPA-Plug-In und nicht im Browser ausgeführt werden.
- Im ersten Beispiel ist EPA der erste Faktor, bei dem der Scan nach dem Prozess 'Firefox' sucht.
- Wenn der EPA-Scan erfolgreich ist, führt er zur LDAP-Authentifizierung, gefolgt vom nächsten EPA-Scan, der nach dem Prozess "Chrome"sucht.
- Wenn mehrere regelmäßige Scans als verschiedene Faktoren konfiguriert sind, hat der neueste Scan Vorrang. In diesem Fall sucht das EPA-Plug-in nach dem Prozess 'Chrome' alle 2 Minuten, nachdem die Anmeldung erfolgreich war.

#### Auf der GUI (mit nFactor Visualizer)

Mit dem nFactor-Visualizer auf der GUI können Sie den erweiterten EPA-Scan als Faktor konfigurieren. Im folgenden Beispiel haben wir LDAP als ersten Faktor und EPA als nächsten Faktor verwendet.

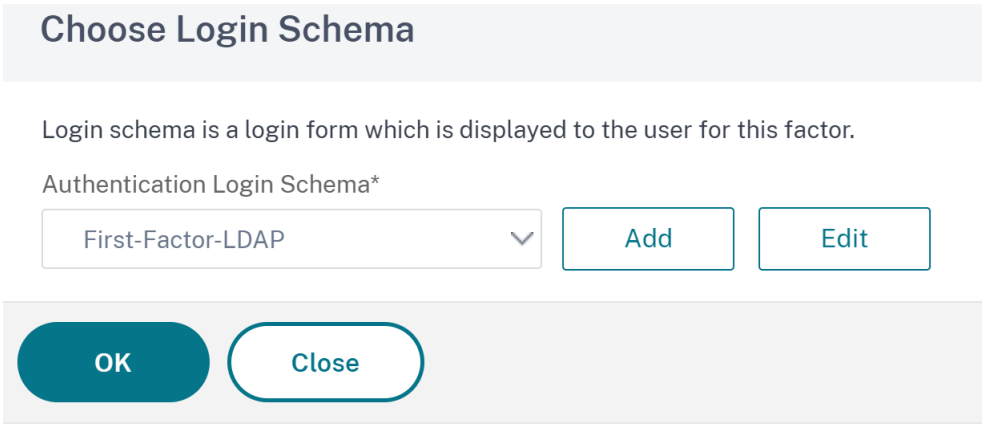
1. Erstellen Sie einen ersten Faktor für den nFactor-Flow.
   - Navigieren Sie zu **Sicherheit > AAA-Application Traffic > nFactor Visualizer > nFactor Flows** und klicken Sie auf **Hinzufügen**.
   - Klicken Sie auf **+**, um den nFactor-Flow hinzuzufügen.
   - Fügen Sie einen Faktor hinzu und klicken Sie auf **Erstellen**.




2. Erstellen Sie ein Anmeldeschema und eine Richtlinie für den ersten Faktor.

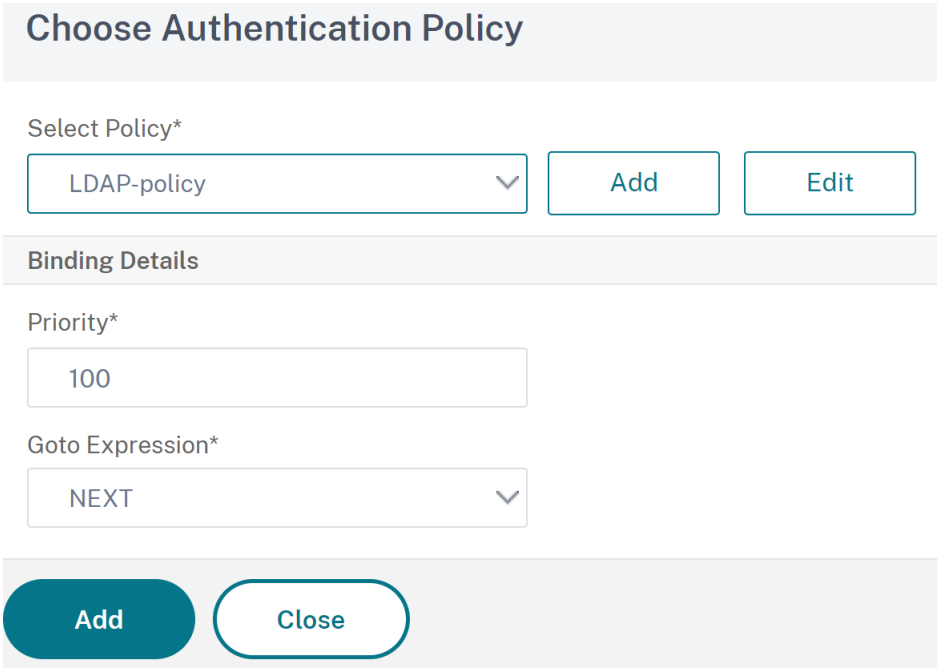
   - Klicken Sie auf der ersten Faktorkachel auf **Schema hinzufügen**, um ein Anmeldeschema hinzuzufügen. Sie können entweder ein vorhandenes Authentifizierungs-Anmeldeschema aus der Dropdownliste auswählen oder ein Anmeldeschema erstellen.
   - Um ein Authentifizierungs-Anmeldeschema zu erstellen, klicken Sie auf **Hinzufügen**. Ausführliche Informationen zum Anmeldeschema für die Authentifizierung finden Sie unter Konfiguration der nFactor-Authentifizierung.




   - Klicken Sie auf **Richtlinie hinzufügen**, um die LDAP-Richtlinie hinzuzufügen. Wenn die LDAP-Richtlinie bereits erstellt wurde, können Sie dieselbe auswählen. Klicken Sie auf **Hinzufügen**.

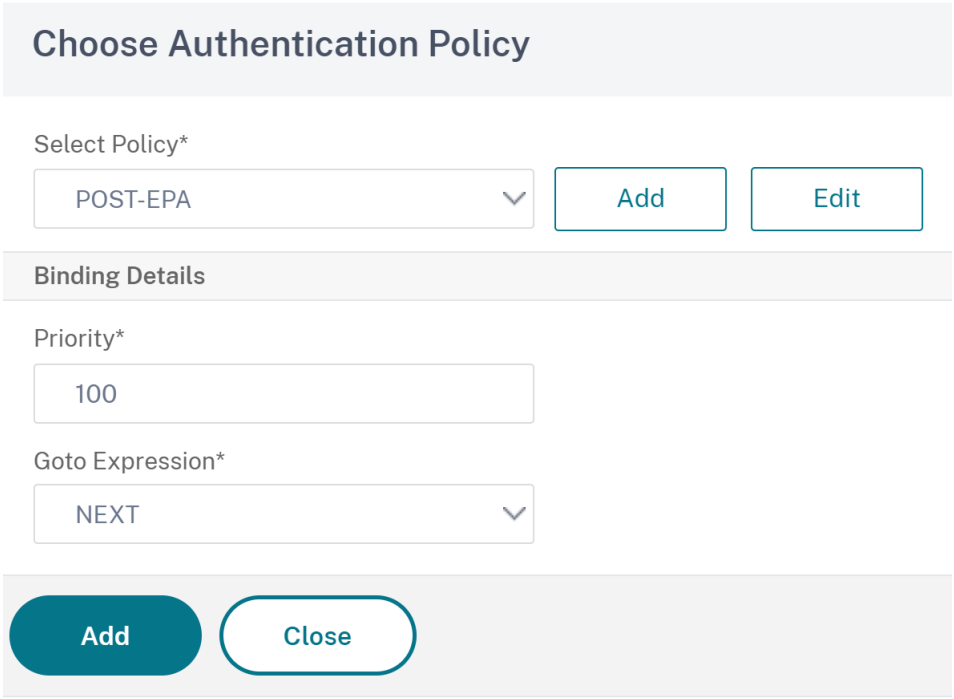
 

> **Hinweis:**
>
> Wenn keine LDAP-Richtlinie erstellt wurde, können Sie eine erstellen. Klicken Sie neben der Dropdownliste **Richtlinie auswählen** auf die Schaltfläche **Hinzufügen**. Wählen Sie im Feld **Aktion** die Option LDAP aus. Einzelheiten zum Hinzufügen eines Authentifizierungs-LDAP-Servers finden Sie unter `https://support.citrix.com/article/CTX123782`.

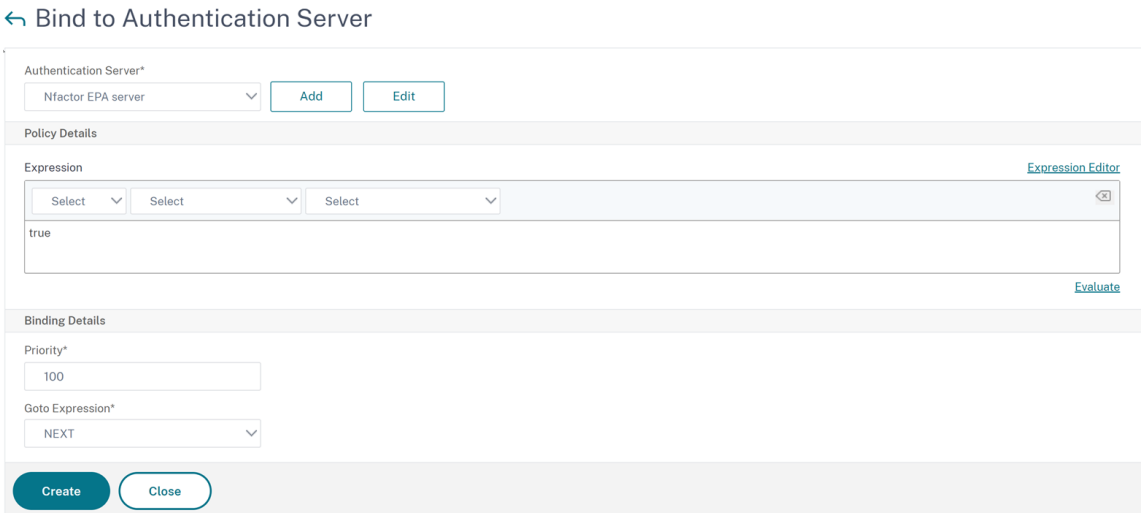



3. Erstellen Sie einen nächsten Faktor und verbinden Sie ihn mit dem ersten Faktor.
   - Klicken Sie auf das grüne oder rote **Plus-Symbol**, um EPA als nächsten Faktor hinzuzufügen.
   - Erstellen Sie den nächsten Faktor auf der Seite **Next Factor to Connect**.
   - Lassen **Sie den Abschnitt Schema hinzufügen** leer, wenn für diesen Faktor standardmäßig kein Schema angewendet werden soll.
4. Fügen Sie eine Richtlinie für den nächsten Faktor hinzu.
   - Klicken Sie auf **Richtlinie hinzufügen**, um die EPA-Richtlinie und Aktion nach der Authentifizierung hinzuzufügen.
   - Sie können entweder aus einer vorhandenen Liste von Richtlinien wählen oder eine Richtlinie erstellen. Um aus den vorhandenen Richtlinien auszuwählen, wählen Sie eine Richtlinie aus der Dropdownliste **Richtlinie auswählen** aus, geben Sie die verbindlichen Details ein und klicken Sie auf **Hinzufügen**.
   - Um eine Richtlinie zu erstellen, klicken Sie neben der Dropdownliste **Richtlinie auswählen** auf die Schaltfläche **Hinzufügen**.




5. Nachdem der nFactor-Flow abgeschlossen ist, klicken Sie auf **Fertig**.
6. Binden Sie den nFactor-Flow an einen Authentifizierungsserver.
   - Navigieren Sie zu **Security AAA - Application Traffic > nFactor Visualizer > nFactor Flows**.
   - Wählen Sie den nFactor aus und klicken Sie **auf An Authentifizierungsserver binden**.




## Referenzen

- nFactor Konzepte, Entitäten und Terminologie

- So konfigurieren Sie die LDAP-Authentifizierung auf Citrix Gateway
- LDAP-Authentifizierung
- Advanced Endpoint Analysis scans

# Advanced Endpoint Analysis scans

March 27, 2024

Advanced Endpoint Analysis (EPA) wird zum Scannen von Benutzergeräten nach den auf Citrix Gateway konfigurierten Endpunktsicherheitsanforderungen verwendet. Wenn ein Benutzergerät versucht, auf Citrix Gateway zuzugreifen, wird das Gerät nach Sicherheitsinformationen wie Betriebssystem, Virenschutz, Webbrowserversionen usw. durchsucht, bevor ein Administrator Zugriff auf Citrix Gateway gewähren kann. Weitere Informationen zu den Citrix EPA-Clientsystemanforderungen finden Sie unter Endpoint Analysis-Anforderungen.

Der Advanced EPA-Scan ist ein richtlinienbasierter Scan, den Sie auf Citrix Gateway für Authentifizierungssitzungen konfigurieren können. Die Richtlinie führt eine Registrierungsprüfung auf einem Benutzergerät durch und basierend auf der Auswertung ermöglicht oder verweigert die Richtlinie den Zugriff auf das Citrix ADC-Netzwerk.

Sie können den erweiterten EPA-Scan mithilfe der GUI oder der CLI konfigurieren.

## Auf der GUI

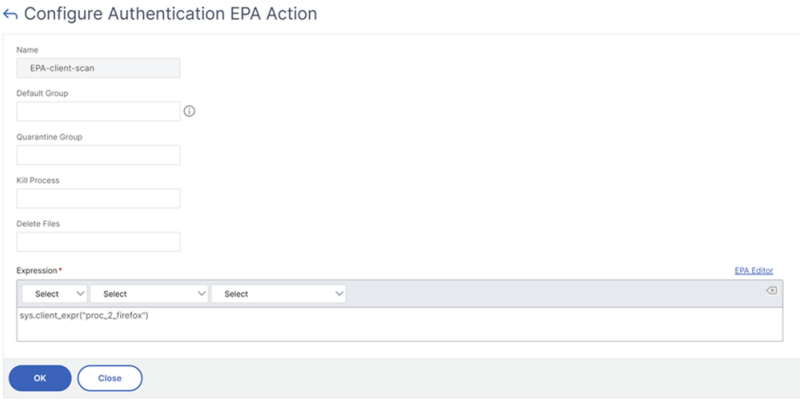
1. Erstellen Sie eine EPA-Aktion.

   Navigieren Sie zu **Sicherheit > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > EPA** und klicken Sie auf **Hinzufügen**. Aktualisieren Sie auf der Seite **EPA-Aktion für Authentifizierung erstellen** die folgenden Informationen und klicken Sie auf **Erstellen**.

   - Name: Name der EPA-Aktion.
   - Standardgruppe: Die Standardgruppe, die ausgewählt wird, wenn die EPA-Prüfung erfolgreich ist.
   - Quarantänegruppe: Die Quarantänegruppe, die ausgewählt wird, wenn die EPA-Prüfung fehlschlägt.
   - Prozess beenden: Zeichenfolge, die den Namen eines Prozesses angibt, der vom EPA-Plug-In beendet werden soll. Mehrere Prozesse müssen durch Kommas getrennt werden.
   - Dateien löschen: Zeichenfolge, die die Pfade und Namen der Dateien angibt, die vom EPA-Plug-in gelöscht werden sollen. Mehrere Dateien müssen durch Kommas getrennt werden.

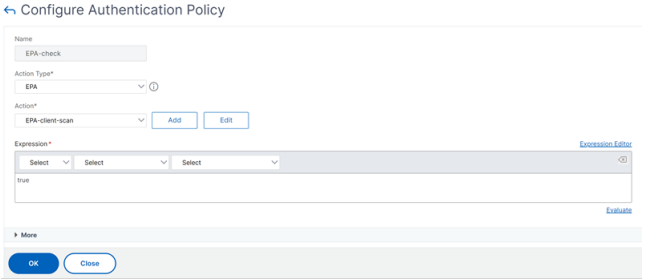
- Ausdruck: Informationen zum EPA-Ausdrucksformat finden Sie in der Richtlinienreferenz für Advanced Endpoint Analysis.




2. Erstellen Sie eine entsprechende EPA-Richtlinie.

   Navigieren Sie zu **Sicherheit > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policies** und klicken Sie auf **Hinzufügen**. Aktualisieren Sie auf der Seite **Authentifizierungsrichtlinie erstellen** die folgenden Informationen und klicken Sie auf **Erstellen**.

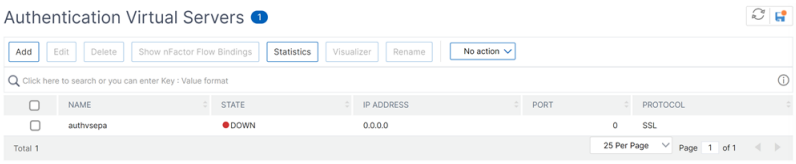
   - Name: Name der erweiterten EPA-Richtlinie.
   - Aktionstyp: Typ der Authentifizierungsaktion.
   - Aktion: Name der Authentifizierungsaktion, die ausgeführt werden soll, wenn die Richtlinie übereinstimmt.
   - Ausdruck: Informationen zum EPA-Ausdrucksformat finden Sie in der Richtlinienreferenz für Advanced Endpoint Analysis.
   - Protokollaktion: Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anfrage dieser Richtlinie entspricht. Die maximal zulässige Länge beträgt 127 Zeichen.



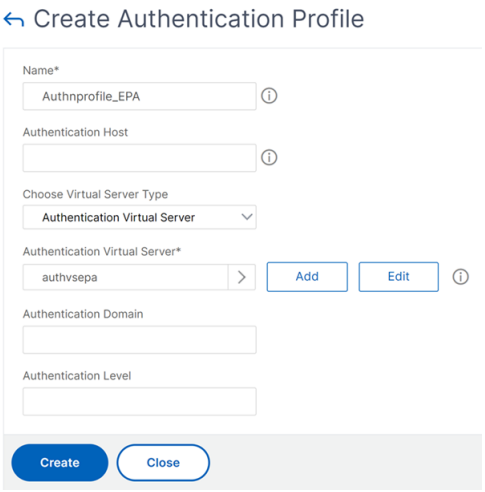

3. Konfigurieren Sie einen virtuellen Authentifizierungsserver und ein Authentifizierungsprofil.

   - Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Virtuelle Authentifizierungsserver** und klicken Sie auf **Hinzufügen**.

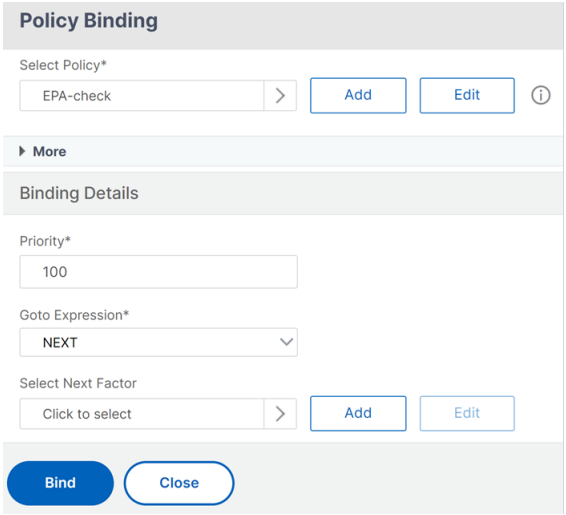



- Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Authentifizierungsprofil** und klicken Sie auf **Erstellen**.




4. Binden Sie die erweiterte EPA-Richtlinie an den virtuellen Authentifizierungsserver.

   - Navigieren Sie zu **Sicherheit > AAA —Anwendungsverkehr > Virtuelle Authentifizierungsserver** und wählen Sie den virtuellen Authentifizierungsserver aus.
   - Wählen Sie die Richtlinie im Abschnitt **Erweiterte Authentifizierungsrichtlinien** aus.
   - Klicken Sie im Abschnitt **Richtlinienbindung** auf **Binden**.




5. Binden Sie die EPA-Richtlinie an nFactor Flow.

   Einzelheiten zum Hinzufügen einer erweiterten EPA-Richtlinie als Faktor zum nFactor-Flow finden Sie unter EPA-Scan als Faktor bei der nFactor-Authentifizierung.

### Über die Befehlszeilenschnittstelle

1. Erstellen Sie eine Aktion, um den EPA-Scan durchzuführen.

```
add authentication epaAction EPA-client-scan -csecexpr "sys.
   client_expr ("proc_2_firefox")"
<!--NeedCopy-->
```

   Der vorhergehende Ausdruck scannt, ob der Prozess ‘Firefox’ausgeführt wird. Das EPA-Plug-in prüft alle 2 Minuten die Existenz des Prozesses, was durch die Ziffer ‘2’im Scan-Ausdruck gekennzeichnet ist.

2. Ordnen Sie die EPA-Aktion einer erweiterten EPA-Richtlinie zu.

```
add authentication Policy EPA-check -rule true -action EPA-client-
   scan
<!--NeedCopy-->
```

3. Konfigurieren Sie einen virtuellen Authentifizierungsserver und ein Authentifizierungsprofil.

```
add authentication vserver authnvsepa ssl -ip address
   10.104.130.129 -port 443
<!--NeedCopy-->
```

```
add Authnprofile_EPA -authnVsName authnvsepa
<!--NeedCopy-->
```

4. Binden Sie die erweiterte EPA-Richtlinie an den virtuellen Authentifizierungsserver.

```
bind authentication vs authnvsepa -policy EPA-check -pr 1
<!--NeedCopy-->
```

### Upgrade EPA-Bibliotheken

So verwenden Sie die Citrix ADC GUI zum Aktualisieren von EPA-Bibliotheken:

1. Navigieren Sie zu**Konfiguration > Citrix Gateway > Clientkomponenten aktualisieren**.
2. Klicken Sie unter **Clientkomponenten aktualisieren** auf den Link**EPA-Bibliotheken aktualisieren**.
3. Wählen Sie die erforderliche Datei aus und klicken Sie auf **Upgrade**.

> **Wichtig:**
>
> - Bei einer Citrix Gateway-Hochverfügbarkeit müssen die EPA-Bibliotheken sowohl auf dem primären als auch auf dem sekundären Knoten aktualisiert werden.
> - In einem Citrix Gateway-Clustering-Setup müssen die EPA-Bibliotheken auf allen Cluster-

> knoten aktualisiert werden.

Eine Liste der von Windows und MAC unterstützten Anwendungen von OPSWAT für Citrix ADC-Scans finden Sie unter https://support.citrix.com/article/CTX234466.

### Fehlerbehebung bei erweiterten Endpoint Analysis-Scans

Um bei der Fehlerbehebung bei Advanced Endpoint Analysis-Scans zu helfen, schreiben die Client-Plug-Ins Protokollinformationen in eine Datei auf Client-Endpunktsystemen. Diese Protokolldateien befinden sich je nach Betriebssystem des Benutzers in den folgenden Verzeichnissen.

**Windows Vista, Windows 7, Windows 8, Windows 8.1 und Windows 10:**

C:\Users\<username>\AppData\Local\Citrix\AGEE\nsepa.txt

**Windows XP:**

C:\Documents and Settings\All Users\Application Data\Citrix\AGEE\nsepa.txt

**Mac OS X-Systeme:**

~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

(Wobei das ~-Symbol den Home-Verzeichnispfad des entsprechenden macOS-Benutzers angibt.)
(Wobei das ~-Symbol den Home-Verzeichnispfad des entsprechenden macOS-Benutzers angibt.)

**Ubuntu:**

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

## Erweiterte Referenz für Richtlinienausdrücke für Endpoint

March 27, 2024

In diesem Thema werden das Format und die Konstruktion von Advanced Endpoint Analysis-Ausdrücken beschrieben. Das Citrix Gateway-Konfigurationsdienstprogramm erstellt automatisch die hier enthaltenen Ausdruckselemente und erfordert keine manuelle Konfiguration.

### Ausdruck-Format

Ein Ausdruck für erweiterte Endpoint Analysis hat das folgende Format:

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-
comparator_ Method-param _...)
```

Ort:

Der Scan-Typ ist die Art der zu analysierenden Anwendung.

Produkt-ID ist die Produktidentifikation für die analysierte Anwendung.

Methodenname ist das zu analysierende Produkt- oder Systemattribut.

Methoden-Komparator ist der gewählte Komparator für die Analyse.

Method-param ist der analysierte Attributwert oder die Werte.

Beispiel:

client.application (ANTIVIR_2600*RTP*==_TRUE)

> **Hinweis:**
>
> Für Scan-Typen ohne Anwendung lautet das Ausdruck-Präfix CLIENT.SYSTEM anstelle von CLIENT.APPLICATION.

### Expression-

Jeder der unterstützten Suchtypen in Advanced Endpoint Analysis verwendet einen eindeutigen Bezeichner in den Ausdrücken. In der folgenden Tabelle werden die Zeichenfolgen für jede Art von Scan aufgeführt.

| Scan-Typ | Zeichenfolge für Scan-Typ |
|---|---|
| Phishing-Schutz | ANTIPHI |
| Antispyware | ANTISPY |
| Antivirus | ANTIVIR |
| Backup Client | BACKUP |
| Gerätezugriffskontrolle | DEV-CONT |
| Verhindern von Datenverlust | DATA-PREV |
| Desktopfreigabe | DESK-SHARE |
| Firewall | FIREWALL |
| Gesundheits-Agent | HEALTH |
| Festplattenverschlüsselung | HD-ENC |

| Scan-Typ | Zeichenfolge für Scan-Typ |
|---|---|
| Sofortnachrichtendienst | IM |
| Webbrowser | BROWSER |
| P2P | P2P |
| Patch-Verwaltung | PATCH |
| URL-Filterung | URL-FILT |
| MAC-Adresse | MAC |
| Domänenüberprüfung | DOMAIN |
| Numerischer Registrierungsscan | REG-NUM |

> **Hinweis:**
>
> Für macOS X-spezifische Scans enthalten Ausdrücke das Präfix MAC- vor dem Methodentyp. Daher sind die Methoden für Antiviren- und Anti-Phishing-Scans MAC-ANTIVIR bzw. MAC-ANTIPHI.
>
> Zum Beispiel:
>
> client.application (MAC-ANTIVIR_2600*RTP*==_TRUE)

### Methoden zum Scannen von Anwendungen

Bei der Konfiguration von Advanced Endpoint Analysis-Ausdrücken werden Methoden verwendet, um die Parameter der Endpunkt-Scans zu definieren. Diese Methoden beinhalten einen Methodennamen, einen Komparator und einen Wert. In den folgenden Tabellen werden die Methoden aufgeführt, die für die Verwendung in Ausdrücken verfügbar sind.

**Gängige Scan-Methoden:**

Die folgenden Methoden werden für mehrere Arten von Anwendungsscans verwendet.

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| VERSION* | Gibt die Version der Anwendung an. | <, <=, >, >=, !=, == | Zeichenfolge der Version |
| AUTHENTIC** | Prüfen Sie, ob die Anwendung authentisch ist oder nicht. | == | TRUE |

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| AKTIVIERT | Prüfen Sie, ob die Anwendung aktiviert ist. | == | TRUE |
| RUNNING | Prüfen Sie, ob die Anwendung läuft. | == | TRUE |
| COMMENT | Kommentarfeld (vom Scan ignoriert). In Ausdrücken durch [] abgegrenzt. | == | Jeder Text |

* Die VERSION-Zeichenfolge kann eine Dezimalzeichenfolge mit bis zu vier Werten angeben, z. B. 1.2.3.4.

** Eine AUTHENTIC-Überprüfung überprüft die Echtheit der Binärdateien für die Anwendung.

> **Hinweis:**
>
> Sie können eine generische Version für Anwendungsscan-Typen auswählen. Wenn generische Scans ausgewählt sind, ist die Produkt-ID 0.

Gateway bietet eine Option, um generische Scans für jeden Softwaretyp zu konfigurieren. Mithilfe des generischen Scans kann ein Administrator den Clientcomputer scannen, ohne die Scanprüfung auf ein bestimmtes Produkt zu beschränken.

Bei generischen Scans funktionieren Scanmethoden nur, wenn das auf dem Benutzersystem installierte Produkt diese Scanmethode unterstützt. Wenden Sie sich an den Citrix Support, um zu erfahren, welche Produkte eine bestimmte Scanmethode unterstützen.

**Einzigartige Scanmethoden:**

Die folgenden Methoden sind für die angegebenen Scans eindeutig.

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| ENABLED-FOR | Prüfen Sie, ob Anti-Phishing-Software für die ausgewählte Anwendung aktiviert ist. | `allof`, `anyof`, `noneof` | **Für Windows**: Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Safari. **Für Mac:** Safari, Mozilla Firefox, Google, Chrome, Opera |

Tabelle 2. Antispyware und Antivirus

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| RTP | Prüfen Sie, ob der Echtzeitschutz eingeschaltet ist oder nicht. | == | TRUE |
| SCAN-TIME | Wie viele **Minuten** seit einem vollständigen Systemscan durchgeführt wurde. | <, <=, >, >=, !=, == | Jede positive Zahl |
| VIRDEF-FILE-TIME | Anzahl der **Minuten** seit der Aktualisierung der Virusdefinitionsdatei (d. h. Anzahl der Minuten zwischen dem Stempel der Virusdefinitionsdatei und dem aktuellen Zeitstempel). | <, <=, >, >=, !=, == | Jede positive Zahl |
| VIRDEF-FILE-VERSION | Version der Definitionsdatei. | <, <=, >, >=, !=, == | Zeichenfolge der Version |
| ENGINE-VERSION | Engineversion. | <, <=, >, >=, !=, == | Zeichenfolge der Version |

Tabelle 3. Backup Client

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| LAST-BK-ACTIVITY | Wie viele **Minuten** seit dem Abschluss der letzten Backup-Aktivität. | <, <=, >, >=, !=, == | Jede positive Zahl |

Tabelle 4. Schutz vor Datenverlusten

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| AKTIVIERT | Prüfen Sie, ob die Anwendung aktiviert ist oder nicht und der Zeitschutz aktiviert ist oder nicht. | == | TRUE |

Tabelle 5. Gesundheitscheck Agent

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| SYSTEM-COMPL | Prüfen Sie, ob das System konform ist. | == | TRUE |

Tabelle 6. Festplattenverschlüsselung

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| ENC-PATH | PATH zur Überprüfung des Verschlüs-selungsstatus. | NO OPERATOR | Jeder Text |
| ENC-TYPE | Überprüfen Sie, ob Verschlüsselungstyp für den angegebenen Pfad. | `allof`, `anyof`, `noneof` | **Liste mit den folgenden Optionen**: UNENCRYPTED, PARTIAL, ENCRYPTED, VIRTUAL, SUSPENDED, PENDING |

Tabelle 7. Webbrowser

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| DEFAULT | Prüfen Sie, ob als Standardbrowser festgelegt. | == | TRUE |

Tabelle 8. Patch-Verwaltung </caption>

|Methode|Beschreibung|Comparator|Mögliche Werte|
|—|—|—|—|
|SCAN-TIME|Wie viele Minuten seit dem letzten Patch-Scan durchgeführt wurde.|<, <=, >, >=, !=, ==|Jede positive Zahl|
|MISSED-PATCH|Dem Clientsystem fehlen keine Patches dieser Typen.|anyof, noneof|ALLE vorausgewählten (vorgewählte Patches auf dem Patch Manager-Server)
NON|

Tabelle 9. MAC-Adresse

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| ADDR | Prüfen Sie, ob die MAC-Adressen des Clientcomputers in der angegebenen Liste enthalten sind oder nicht. | anyof, noneof | Bearbeitbare Liste |

Tabelle 10. Domain-Mitgliedschaft

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| SUFFIX | Prüfen Sie, ob der Clientcomputer in der angegebenen Liste existiert oder nicht. | anyof, noneof | Bearbeitbare Liste |

Tabelle 11. Numerischer Registry-Eintrag

| Methode | Beschreibung | Comparator | Mögliche Werte |
| --- | --- | --- | --- |
| PATH | Pfad für die Überprüfung der Registrierung. Im Format: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate Es ist kein Entkommen von Sonderzeichen erforderlich. Alle Stammschlüssel der Registrierung: HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG | NO OPERATOR | Jeder Text |

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| REDIR-64 | Folgen Sie der 64-Bit-Umleitung. Wenn auf TRUE gesetzt, wird die WOW-Umleitung befolgt (das heißt, der Registrierungspfad wird auf 32-Bit-Systemen überprüft, aber der umgeleitete WOW-Pfad wird auf 64-Bit-Systeme überprüft.) Wenn nicht gesetzt, wird die WOW-Umleitung nicht befolgt (das heißt, derselbe Registrierungspfad wird für 32-Bit- und 64-Bit-Systeme überprüft). Für Registry-Einträge, die nicht umgeleitet werden, hat diese Einstellung keine Auswirkungen. Im folgenden Artikel finden Sie eine Liste der Registrierungss-chlüssel, die auf 64-Bit-Systemen umgeleitet werden: http://msdn.microsoft.com/en-us/library/aa384253%28v=vs.85%29.aspx | == | TRUE |

| Methode | Beschreibung | Comparator | Mögliche Werte |
|---|---|---|---|
| VALUE | Erwarteter Wert für den obigen Pfad. Dieser Scan funktioniert nur für Registry-Typen von REG_DWORD und REG_QWORD. | <, <=, >, >=, !=, == | Beliebige Zahl |

## EPA-Scan für MAC-Adressen

March 27, 2024

Ab Citrix ADC Version 13.0-88.x können Sie EPA-Scankonfigurationen für die zulässigen oder spezifischen MAC-Adressen konfigurieren. Citrix ADC verwendet Richtlinienausdrücke und Mustersätze, um die Liste der MAC-Adressen zu spezifizieren.

Vor der Citrix ADC-Version 13.0-88.x musste die Liste aller zulässigen MAC-Adressen als Teil eines EPA-Ausdrucks angegeben werden. Wenn die Kunden eine riesige Liste erlaubter MAC-Adressen hatten, war es umständlich, alle MAC-Adressen in einem Ausdruck hinzuzufügen. Außerdem gab es eine Beschränkung für die Anzahl der MAC-Adressen, die in einem einzigen Ausdruck hinzugefügt werden sollten.

Beispiel:

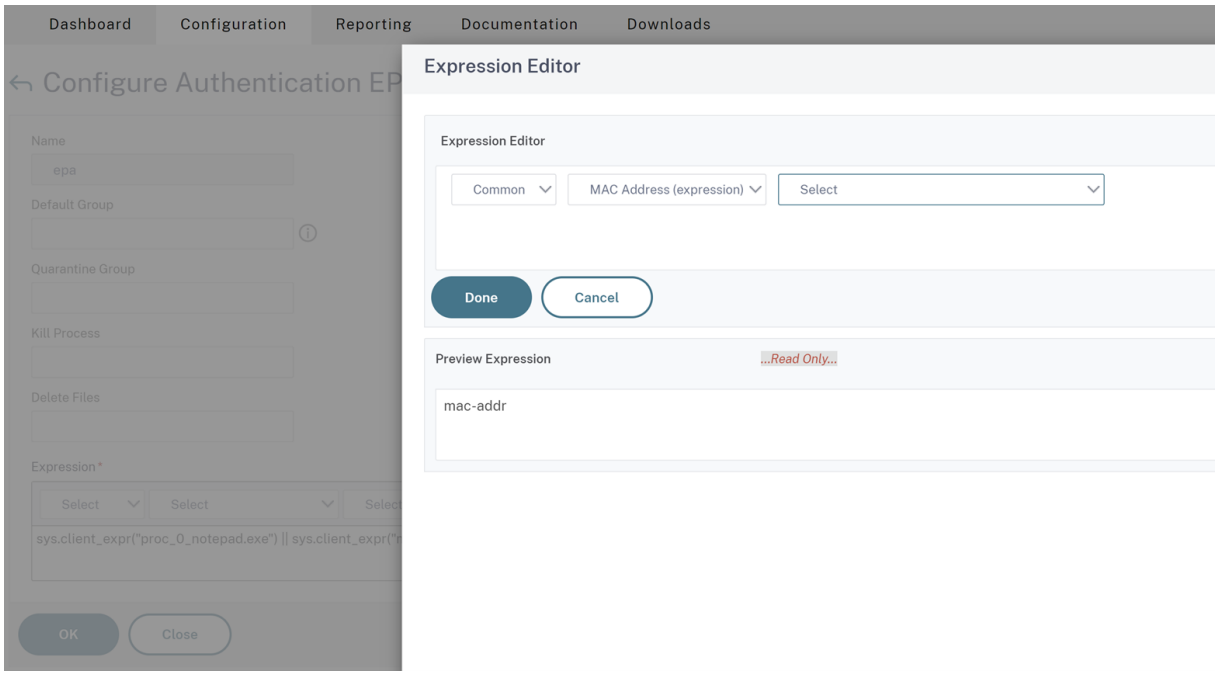
```
1 add authentication epaAction epa -csecexpr q/sys.client_expr("
    proc_0_notepad.exe") || sys.client_expr("proc_0_chrome") || sys.
    client_expr("proc_0_firefox") && sys.client_expr("
    sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT: MAC Address]
    ")/
2 <!--NeedCopy-->
```

### EPA-Scan für MAC-Adressen über die GUI konfigurieren

Die Option **MAC-Adressen (Ausdruck)**, die zuvor in der **Windows-Scankategorie** verfügbar war, ist jetzt in der Kategorie **Common** Scan der Citrix ADC GUI verfügbar. Mit dieser Option können Benutzer einen EPA-Scan für eine Liste zulässiger oder spezifischer MAC-Adressen konfigurieren.

> **Hinweis:**
>
> Der Citrix Secure Access-Client 22.10.1 und spätere Versionen unterstützen diese Methode, mit der Citrix ADC die EPA-Scankonfigurationen auf der GUI verarbeitet.




1. Mustersatz konfigurieren. Einzelheiten finden Sie unter Konfigurieren eines Mustersatzes.
2. Erstellen Sie für jeden Mustersatz einen entsprechenden Richtlinienausdruck.

   Wählen Sie beim Konfigurieren des Ausdrucks im Ausdruckseditor **AAA > LOGIN > CLIENT_MAC_ADDR > EQUAL_ANY (Zeichenfolge) > Mustersatz**aus.

   Einzelheiten zum Konfigurieren eines erweiterten Ausdrucks finden Sie unter Konfigurieren erweiterter Richtlinienausdrücke in einer Richtlinie.
3. Erstellen Sie einen EPA-Scan für den Ausdruck, der in den vorherigen Schritten konfiguriert wurde. Einzelheiten finden Sie unter Erweiterte Endpoint Analysis-Scans.

### Konfigurieren Sie den EPA-Scan für MAC-Adressen über die CLI

1. Speichern Sie die MAC-Adressen innerhalb von Mustersätzen.

   Geben Sie an der Eingabeaufforderung;

   ```
   add policy patset <name> [-comment <string>]
   <!--NeedCopy-->
   ```

   Example:

‘‘‘

add policy patset patset1

bind policy patset patset1 1A-C8-9C-83-BO-F7

bind policy patset patset1 02-50-F2-0A-77-7C …and so on up to 3K entries.

add policy patset patset2

bind policy patset patset2 1A-2B-3C-4D-5E-6A

bind policy patset patset2 1A-2B-3C-4D-5E-6B …and so on up to 3K entries.

‘‘‘

2. Erstellen Sie mit AAA.LOGIN.CLIENT_MAC_ADDR.equals_any() einen entsprechenden Richtlinienausdruck für jeden Mustersatz

   Geben Sie an der Eingabeaufforderung;

   ```
   Add policy expression <name> <value> [-comment <string>] [-
       clientSecurityMessage <string>]
   ```

   Beispiel:

   ```
   add policy expression exp1 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
       patset1")
   add policy expression exp2 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
       patset2")
   ```

3. Erstellen von EPA-Scans über konfigurierten Richtlinienausdrücke

   Geben Sie an der Eingabeaufforderung;

   ```
   add authentication epaAction <name>  -csecexpr <expression>
   ```

   Beispiel:

   ```
   add authentication epaAction epa -csecexpr q/sys.client_expr("
       proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")  ||
       sys.client_expr("mac-addr_0_exp1") || sys.client_expr("mac-
       addr_0_exp2") || sys.client_expr("proc_0_firefox")/
   ```

   Konfigurieren Sie eine Vorauthentifizierungsrichtlinie,

   ```
   add authentication Policy epapol -rule true -action epa
   ```

   Binden Sie die Vorauthentifizierungsrichtlinie,

   ```
   bind authentication vserver <name> -policy epapol -priority 10 -
       gotoPriorityExpression NEXT
   ```

### Wichtige Hinweise

- Das Konfigurieren eines EPA-Scans für eine zulässige Liste von MAC-Adressen gilt nur für die nFactor-Authentifizierungsabläufe.
- Es wird empfohlen, nicht mehr als 3000 Einträge in einem Mustersatz zu speichern.
- Die MAC-Adressen müssen im Format 1A-2B-3C-4D-5E-6F konfiguriert sein.
- Das Format für den EPA-Scan ist `mac-addr_0_<policy-expression-name>`. In diesem Format ist `mac-addr_0_` ein statischer Wert und Sie müssen den Richtlinienausdrucksnamen nach `mac-addr_0_` eingeben.
- Die EPA-Scans können mithilfe der Symbole entsprechend getrennt werden ( `||`, `&&`).
- Um viele MAC-Adressen zu einem Mustersatz hinzuzufügen, können Sie den dateibasierten Mustersatzimport verwenden. Es wird empfohlen, für eine optimale Leistung maximal 3000 Einträge/Mustersatz zu speichern.
- Wenn MAC-Adressen in einer Datei vorhanden sind, können Sie einen Mustersatz erstellen, indem Sie dateibasierte Mustersätze importieren und während des Imports das entsprechende Trennzeichen angeben.

### Referenzen

- Mustersatz konfigurieren.
- Mustersatz mit dateibasiertem Imports erstellen.
  “‘

## Benutzersitzungen verwalten

March 27, 2024

Sie können Benutzersitzungen in der Citrix ADC GUI über das Dialogfeld **Active Users Sessions** verwalten. In diesem Dialogfeld wird eine Liste aktiver Benutzersitzungen auf dem Citrix Gateway angezeigt. Sie können Endbenutzer- oder Gruppensitzungen mithilfe des Benutzernamens, des Gruppennamens oder der IP-Adresse anzeigen. In diesem Dialogfeld können Sie auch aktive Sessions anzeigen. Zu den Sitzungsinformationen gehören:

- Benutzername
- IP-Adresse des Benutzergeräts
- Portnummer des Benutzergeräts
- IP-Adresse des virtuellen Servers
- Portnummer des virtuellen Servers
- Dem Benutzer zugewiesene Intranet-IP-Adresse

## Verwalten von Benutzersitzungen über die GUI

### So zeigen Sie Benutzersitzungen an

1. Klicken Sie im Navigationsbereich der Citrix ADC GUI auf **Citrix Gateway**.
2. Klicken Sie im Detailbereich unter Verbindungen überwachen auf **Aktive Benutzersitzungen**.
3. Wählen Sie in **Aktive Benutzersitzungen**eine der folgenden Typen aus.
    - **Aktive Nutzer**
    - **Aktive Gruppen**
    - **Intranet-IP**- Wenn Sie Intranet-IP wählen, müssen Sie die Intranet-IP-Adresse und die Subnetzmaske eingeben.
4. Klicken Sie auf **Weiter**.

### So aktualisieren Sie die Sitzungsliste

Sie können aktualisierte Informationen über Sitzungen für Citrix Gateway abrufen.

1. Klicken Sie im Navigationsbereich der Citrix ADC GUI auf **Citrix Gateway**.
2. Klicken Sie im Detailbereich unter Verbindungen überwachen auf **Aktive Benutzersitzungen**.
3. Klicken Sie auf **Aktualisieren**.

### So beenden Sie Benutzer- oder Gruppensitzungen oder eine Sitzung mit einer bestimmten Intranet-IP-Adresse

Sie können Benutzer- und Gruppensitzungen beenden. Sie können auch eine Sitzung beenden, die eine bestimmte Intranet-IP-Adresse und Subnetzmaske hat.

1. Klicken Sie im Navigationsbereich der Citrix ADC GUI auf **Citrix Gateway**.
2. Klicken Sie im Detailbereich unter Verbindungen überwachen auf **Aktive Benutzersitzungen**.
3. Wählen Sie unter Sessions einen Benutzer, eine Gruppe oder eine Sitzung mit einer bestimmten Intranet-IP-Adresse aus, und klicken Sie dann auf **Beenden**.

## Verwalten von Benutzersitzungen über die CLI

Sie können die folgenden CLI-Befehle verwenden, um Benutzersitzungen, Endbenutzer- oder Gruppensitzungen anzuzeigen.

- `show aaa session`- Zeigt alle Citrix ADC-Authentifizierungs-, Autorisierungs- und Überwachungs- oder VPN-Verbindungen an, die an den angegebenen Benutzer, die Gruppe, die IP-Adresse oder den angegebenen IP-Bereich gebunden sind.

- `show vpn icaConnection` - Zeigt alle aktiven Verbindungen an, die den ICA-Proxy verwenden.
- `show system session` - Zeigt Informationen über alle aktuellen Systemsitzungen oder über die angegebene Sitzung an.

## Always On

March 27, 2024

Die Funktion Always On von Citrix Gateway stellt sicher, dass Benutzer immer mit dem Unternehmensnetzwerk verbunden sind. Diese dauerhafte VPN-Konnektivität wird durch die automatische Einrichtung eines VPN-Tunnels erreicht.

> **Hinweis**
>
> Always On-Funktion unterstützt Captive-Portale für Citrix ADC 12.0 Build 51.24 und höher.

### Wann sollte Always On verwendet werden

Verwenden Sie Always On, wenn Sie eine nahtlose VPN-Konnektivität basierend auf dem Benutzerstandort bereitstellen und den Netzwerkzugriff eines Benutzers verhindern müssen, der nicht mit einem VPN verbunden ist.

Die folgenden Szenarien veranschaulichen die Verwendung von Always On.

- Ein Mitarbeiter startet den Laptop außerhalb des Unternehmensnetzwerks und benötigt Unterstützung beim Aufbau der VPN-Konnektivität.
  **Lösung:** Wenn der Laptop außerhalb des Unternehmensnetzwerks gestartet wird, richtet Always On nahtlos einen Tunnel ein und bietet VPN-Konnektivität.
- Ein Mitarbeiter, der VPN-Konnektivität nutzt, wechselt ins Unternehmensnetzwerk. Der Mitarbeiter wird auf ein Unternehmensnetzwerk umgestellt, bleibt jedoch mit dem VPN-Tunnel verbunden, was kein wünschenswerter Zustand ist.
  **Lösung:** Wenn der Mitarbeiter in das Unternehmensnetzwerk wechselt, reißt Always On den VPN-Tunnel ab und schaltet den Mitarbeiter nahtlos in das Unternehmensnetzwerk um.
- Ein Mitarbeiter bewegt sich außerhalb des Unternehmensnetzwerks und schließt den Laptop (nicht heruntergefahren). Der Mitarbeiter benötigt Unterstützung beim Aufbau der VPN-Konnektivität, wenn er die Arbeit am Laptop wieder aufnimmt.
  **Lösung:** Wenn der Mitarbeiter das Unternehmensnetzwerk verlässt, baut Always On nahtlos einen Tunnel auf und stellt VPN-Konnektivität bereit.

- Ein Unternehmen möchte den Netzwerkzugriff regulieren, der seinen Benutzern gewährt wird, wenn sie nicht mit einem VPN-Tunnel verbunden sind.
  **Lösung:** Je nach Konfiguration schränkt Always On den Zugriff ein, sodass Benutzer nur auf das Gateway-Netzwerk zugreifen können.

## Das Always On Framework verstehen

Always On verbindet einen Benutzer automatisch mit einem VPN-Tunnel, den der Client zuvor eingerichtet hat. Das erste Mal, wenn der Benutzer einen VPN-Tunnel benötigt, muss der Benutzer eine Verbindung zur Citrix Gateway-URL herstellen und den Tunnel einrichten. Nachdem die Always On Konfiguration auf den Client heruntergeladen wurde, treibt diese Konfiguration den nachfolgenden Aufbau des Tunnels voran.

Die ausführbare Citrix Gateway-Clientdatei wird immer auf dem Clientcomputer ausgeführt. Wenn sich der Benutzer anmeldet oder sich das Netzwerk ändert, bestimmt der Citrix Gateway-Client, ob sich der Benutzerlaptop im Unternehmensnetzwerk befindet. Je nach Standort und Konfiguration richtet der Citrix Gateway-Client entweder einen Tunnel ein oder reißt einen vorhandenen Tunnel ab.

Der Tunnelaufbau wird erst eingeleitet, nachdem sich der Benutzer am Computer anmeldet. Der Citrix Gateway-Client verwendet die Anmeldeinformationen des Client-Computers, um sich beim Gateway-Server zu authentifizieren, und versucht, einen Tunnel einzurichten.

### Automatischer Wiedereinbau eines Tunnels

Die automatische Wiederherstellung eines Tunnels wird ausgelöst, wenn ein VPN-Tunnel von Citrix Gateway abgerissen wird.

> **Hinweis**
>
> Bei einem Fehler von Endpoint Analysis versucht der Citrix Gateway-Client nicht erneut den Tunnelaufbau, sondern zeigt eine Fehlermeldung an. Wenn ein Authentifizierungsfehler auftritt, fordert der Citrix Gateway-Client den Benutzer zur Eingabe von Anmeldeinformationen auf.

### Unterstützte Benutzerauthentifizierungsmethoden für nahtlosen Tunnelaufbau

Die unterstützten Benutzerauthentifizierungsmethoden lauten wie folgt:

- Benutzername + AD-Kennwort: Wenn der Windows-Benutzername und das Kennwort für die Authentifizierung verwendet werden, richtet der Citrix Gateway-Client den Tunnel mithilfe dieser Anmeldeinformationen nahtlos ein.

- Benutzerzertifikat: Wenn ein Benutzerzertifikat für die Authentifizierung verwendet wird und nur ein Zertifikat auf der Clientmaschine vorhanden ist, baut der Citrix Secure Access Client mithilfe dieses Zertifikats nahtlos einen Tunnel auf. Wenn mehrere Clientzertifikate installiert sind, wird der Tunnel eingerichtet, nachdem der Benutzer das bevorzugte Zertifikat ausgewählt hat. Der Citrix Secure Access Client verwendet dieses bevorzugte Zertifikat für spätere Tunnel.

  Wenn die Smartcards ein Benutzerzertifikat gemeinsam nutzen, kann die automatische Anmeldung nicht erreicht werden, wenn die Zertifikate im Speicher im Vergleich zu den im Speicher vorhandenen Zertifikaten dynamisch installiert werden.

- Benutzerzertifikat und Benutzername + AD-Kennwort: Diese Authentifizierungsmethode ist die Kombination zuvor beschriebener Authentifizierungsmethoden.

> **Hinweis**
>
> Alle anderen Authentifizierungsmechanismen werden unterstützt, aber der Tunnelaufbau ist für keine anderen Authentifizierungsmethoden nahtlos. Für alle anderen Authentifizierungsmethoden ist ein Benutzereingriff erforderlich.

#### Konfigurationsanforderungen für Always On

Der Unternehmensadministrator muss für die verwalteten Geräte Folgendes durchsetzen:

- Der Benutzer darf den Prozess/Dienst für eine bestimmte Konfiguration nicht beenden können
- Der Benutzer darf das Paket für eine bestimmte Konfiguration nicht deinstallieren können
- Der Benutzer darf bestimmte Registrierungseinträge nicht ändern können

> **Hinweis**
>
> Die Funktion funktioniert möglicherweise nicht wie erwartet, wenn der Benutzer über Administratorrechte verfügt, wie bei nicht verwalteten Geräten.

### Überlegungen beim Aktivieren der AlwaysOn Funktion

Lesen Sie den folgenden Abschnitt, bevor Sie die Funktion Always On aktivieren.

Primärer Netzwerkzugriff: Wenn der Tunnel eingerichtet ist, wird der Verkehr zum Unternehmensnetzwerk basierend auf der Split-Tunnelkonfiguration festgelegt. Andere Konfigurationen sind nicht vorgesehen, um dieses Verhalten außer Kraft zu setzen.

Proxy-Einstellungen des Clientcomputers: Proxy-Einstellungen des Clientcomputers werden für die Verbindung mit dem Gateway-Server ignoriert.

> **Hinweis**
>
> Die Proxykonfiguration der Citrix ADC Appliance wird nicht ignoriert. Nur die Proxy-Einstellungen des Clientcomputers werden ignoriert. Benutzer, die einen Proxy auf ihren Systemen konfiguriert haben, werden benachrichtigt, dass das VPN-Plug-In ihre Proxy-Einstellungen ignoriert hat.

Wenn der Konfigurationswert auf „Verweigern“gesetzt ist, gelten die folgenden Änderungen:

- Client-UI - Die Abmelde- und Exit-Optionen aus dem Kontextmenü des Plug-Ins und der Plug-In-Benutzeroberfläche sind deaktiviert. Benutzer dürfen die Gateway-URL nicht ändern.
- Browser-Anmeldung - Die Anmeldung des Browsers an einem anderen Gateway ist nicht zulässig. Client-Steuerelemente sind deaktiviert.

### Konfigurieren von Always On

Erstellen Sie zum Konfigurieren von Always On ein Alwayson-Profil auf dem Citrix Gateway-Gerät und wenden Sie das Profil an.

So erstellen Sie ein Alwayson-Profil:

1. Navigieren Sie in der Citrix ADC GUI zu **Konfiguration > Citrix Gateway > Richtlinien > AlwaysOn.**
2. Klicken Sie auf der Seite **AlwaysOn-Profile** auf **Hinzufügen**.
3. Geben Sie auf der Seite „ **AlwaysOn-Profil erstellen** “die folgenden Details ein:
    - **Name** —Der Name für Ihr Profil.
    - **Standortbasiertes VPN (clientseitiger Registrierungsname: LocationDetection) — Wählen Sie eine der folgenden Einstellungen aus:
        - **Remote**, damit ein Client erkennen kann, ob er sich im Unternehmensnetzwerk befindet, und den Tunnel einrichten kann, wenn nicht im Unternehmensnetzwerk. Remote ist die Standardeinstellung.
        - **Überall**, um einen Kunden die Standorterkennung überspringen zu lassen und den Tunnel einzurichten, unabhängig vom Standort des Kunden
    - **Clientsteuerung** —Wählen Sie eine der folgenden Einstellungen aus:
        - **Verweigern**, um zu verhindern, dass sich der Benutzer abmeldet und eine Verbindung zu einem anderen Gateway herstellt. Verweigern ist die Standardeinstellung.
        - **Ermöglicht es** dem Benutzer, sich abzumelden und eine Verbindung zu einem anderen Gateway herzustellen.
    - **Netzwerkzugriff bei VPN-Fehler (clientseitiger Registrierungsname: AlwaysOn)** — Wählen Sie eine der folgenden Einstellungen aus:

- **Voller Zugriff**, damit der Netzwerkverkehr zum und vom Client fließen kann, wenn der Tunnel nicht eingerichtet ist. Voller Zugriff ist die Standardeinstellung.
- **Nur zum Gateway**, um zu verhindern, dass Netzwerkverkehr zum oder vom Client fließt, wenn der Tunnel nicht eingerichtet ist. Der Verkehr zur oder von der Gateway-IP-Adresse ist jedoch zulässig.
  **Hinweis:** Im Modus **Nur zum Gateway** werden nur der virtuelle Server, das DNS und der DHCP-Verkehr entsperrt. Um andere Websites, IP-Adressbereiche oder IP-Adressen zu entsperren, müssen Sie die **AlwaysOnAllowList-Registrierung** mit einer durch Semikolons getrennten Liste von FQDNs, IP-Adressbereichen oder IP-Adressen festlegen.
  Zum Beispiel mycompany.com, mycdn.com, 10.120.67.0-10.120.67.255.67,67,67,67

4. Klicke auf **Erstellen**, um die Erstellung deines Profils abzuschließen.

So wenden Sie das Alwayson-Profil an:

1. Wählen Sie in der Citrix ADC-Schnittstelle **Konfiguration > Citrix Gateway > Globale Einstellungen**aus.
2. Klicken Sie auf der Seite Globale Einstellungen auf den Link **Globale Einstellungen ändern**, und wählen Sie dann die Registerkarte **Clienterfahrung** aus.
3. Wählen Sie im Dropdown-Menü **AlwaysON-Profilname** das neu erstellte Profil aus und klicken Sie auf **OK**.

> **Hinweis**
>
> Eine ähnliche Konfiguration kann im Sitzungsprofil vorgenommen werden, um die Richtlinien auf Gruppenebene, Serverhebel oder Benutzerebene anzuwenden.

## Hinweis zu IIPs

Der Tunnel auf Maschinenebene verwendet die zertifikatbasierte Authentifizierung, und die erstellte Sitzung hat den allgemeinen Namen des Zertifikats als Benutzernamen. Wenn Gerätezertifikate eindeutige gemeinsame Namen haben, haben die Sitzungen verschiedener Computer unterschiedliche Benutzernamen und damit unterschiedliche IIPs. Stellen Sie sicher, dass Sie ein Gerätezertifikat mit eindeutigen Namen generieren. Im Idealfall müssen Sie Maschinennamen als allgemeinen Namen des Gerätezertifikats verwenden.

### Verhaltensübersicht verschiedener Konfigurationen für Admin-Benutzer und Nicht-Admin-Benutzer

In der folgenden Tabelle wird das Verhalten für verschiedene Konfigurationen zusammengefasst. Es beschreibt auch die Möglichkeit bestimmter Benutzeraktionen, die sich auf die Always-On-

Funktionalität auswirken können.

| networkAccessONVPNFailure | Kontrolle durch den Kunden | Nicht-Admin-Benutzer | Admin-Benutzer |
|---|---|---|---|
| fullaccess | Allow | Der Tunnel wird automatisch eingerichtet. Der Benutzer kann sich abmelden und vom Netzwerk fernbleiben. Der Benutzer kann auch auf ein anderes Citrix Gateway verweisen. | Der Tunnel wird automatisch eingerichtet. Der Benutzer kann sich abmelden und vom Unternehmensnetzwerk fernhalten. Der Benutzer kann auch auf ein anderes Citrix Gateway verweisen. |
| fullaccess | Verweigern | Der Tunnel wird automatisch eingerichtet. Der Benutzer kann sich nicht abmelden oder auf ein anderes Citrix Gateway verweisen. | Der Tunnel wird automatisch eingerichtet. Der Benutzer kann den Citrix Gateway Client deinstallieren oder zu einem anderen Citrix Gateway wechseln. |
| onlyToGateway | Allow | Der Tunnel wird automatisch eingerichtet. Der Benutzer kann sich abmelden (kein Netzwerkzugriff). Der Benutzer kann auch auf ein anderes Citrix Gateway verweisen. In diesem Fall wird der Zugriff nur auf das neu gerichtete Citrix Gateway gewährt. | Der Tunnel wird automatisch eingerichtet. Der Benutzer kann den Citrix Gateway Client deinstallieren oder zu einem anderen Citrix Gateway wechseln. |

| networkAccessONVPNFailure | Kontrolle durch den Kunden | Nicht-Admin-Benutzer | Admin-Benutzer |
|---|---|---|---|
| onlyToGateway | Verweigern | Der Tunnel wird automatisch eingerichtet. Der Benutzer kann sich nicht abmelden oder auf ein anderes Citrix Gateway verweisen. | Der Tunnel wird automatisch eingerichtet. Der Benutzer kann den Citrix Gateway Client deinstallieren oder zu einem anderen Citrix Gateway wechseln. |

### Ausgewählte URLs zulassen, wenn “Immer ein”nicht aktiviert ist

Benutzer können auf einige Websites zugreifen, selbst wenn Always On nicht verfügbar ist und das Netzwerk gesperrt ist. Administratoren können die **AlwaysOnAllowList-Registrierung** verwenden, um die Websites hinzuzufügen, auf die Sie Zugriff gewähren möchten, wenn Always On nicht verfügbar ist.

> **Hinweis:**
>
> - Die **AlwaysOnAllowList-Registrierung** wird ab Version 13.0 Build 47.x und höher unterstützt.
> - Der **AlwaysOnAllowList-Registrierungsspeicherort** ist Computer\HKEY_LOCAL_MACHINE\SOFTWARE\C Access Client.
> - Platzhalter-URLs/FQDNs werden in der **AlwaysOnAllowList-Registrierung** nicht unterstützt.

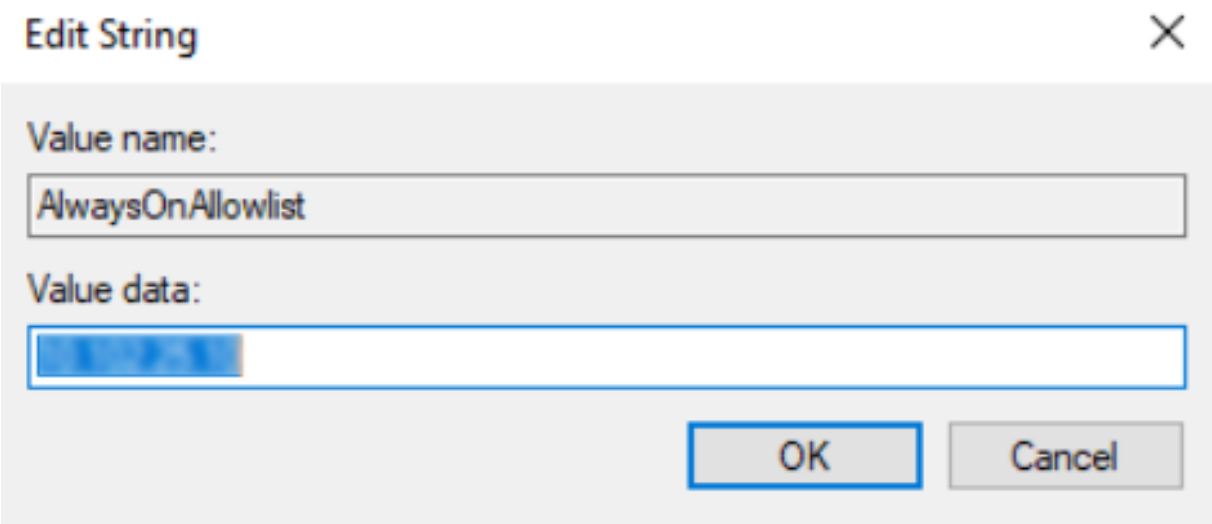
#### So legen Sie die AlwaysOnAllowlist-Registrierung fest

Legen Sie die **AlwaysOnAllowList-Registrierung** mit einer durch Semikolons getrennten Liste von FQDNs, IP-Adressbereichen oder IP-Adressen fest, auf die Sie Zugriff gewähren möchten.

**Beispiel:** example.citrix.com; 10.103.184.156; 10.102.0.0-10.102.255.100

Die folgende Abbildung zeigt ein Beispiel für eine **AlwaysOnAllowlist**-Registrierung.




## AlwaysON VPN vor der Windows-Anmeldung (früher Always On Service)

March 27, 2024

Die Funktion **AlwaysON VPN vor der Windows-Anmeldung** (früher Always On Service) ermöglicht es einem Benutzer, einen VPN-Tunnel auf Maschinenebene einzurichten, noch bevor sich ein Benutzer bei einem Windows-System anmeldet. Der Tunnel bleibt aktiv, bis die Maschine herunterfährt. Nachdem sich der Benutzer angemeldet hat, wird der VPN-Tunnel auf Computerebene von einem VPN-Tunnel auf Benutzerebene übernommen. Nachdem sich der Benutzer abmeldet, wird der Tunnel auf Benutzerebene zerrissen und ein Tunnel auf Maschinenebene eingerichtet. **Always On VPN vor der Windows-Anmeldung** kann nur mithilfe erweiterter Authentifizierungsrichtlinien konfiguriert werden. Einzelheiten finden Sie unter Konfigurieren von Always On VPN vor der Windows-Anmeldung.

### Immer im VPN vor Windows-Anmeldefunktionen

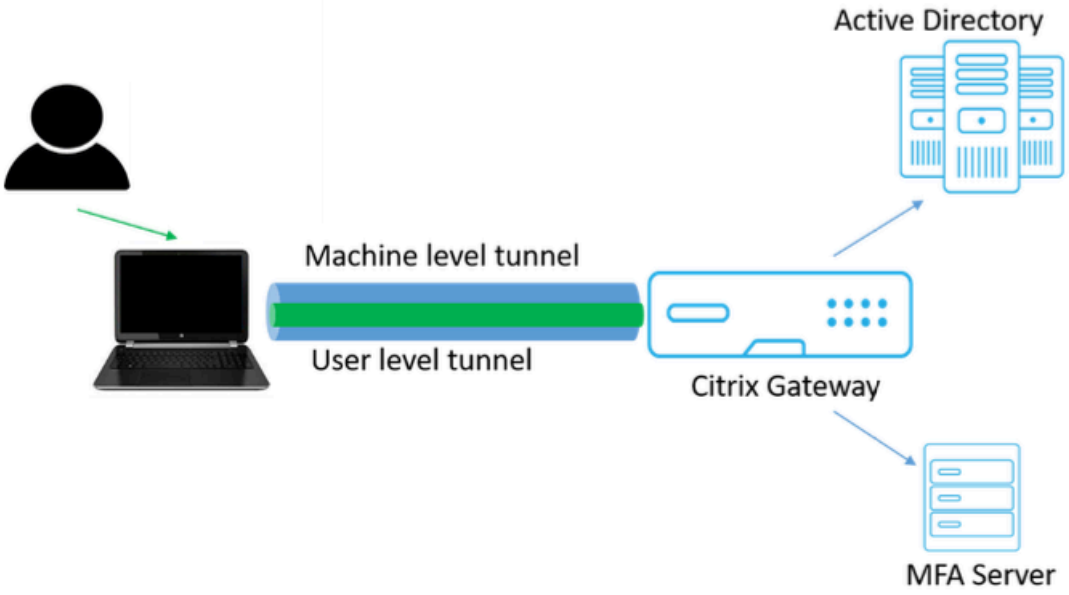
- Der Administrator kann Benutzern, die zum ersten Mal remote arbeiten, ein Einmalkennwort geben, mit dem Benutzer eine Verbindung zum Domänencontroller herstellen können, um ihr Kennwort zu ändern.
- Der Administrator kann AD-Richtlinien für das Gerät remote verwalten/durchsetzen, noch bevor sich der Benutzer anmeldet.
- Der Administrator kann Benutzern eine granulare Steuerung basierend auf der Benutzergruppe bieten, nachdem sich der Benutzer angemeldet hat. Beispielsweise können Sie mithilfe eines Tunnels auf Benutzerebene eine bestimmte Benutzergruppe einschränken oder Zugriff für eine Ressource gewähren.

- Der Benutzertunnel kann gemäß den Benutzeranforderungen für MFA konfiguriert werden.
- Mehrere Benutzer können dieselbe Maschine verwenden. Der Zugriff auf selektive Ressourcen erfolgt basierend auf dem Benutzerprofil. Beispielsweise können mehrere Benutzer eine Maschine problemlos in einem Kiosk verwenden.
- Benutzer, die remote arbeiten, stellen eine Verbindung zum Domänencontroller her, um ihr Kennwort zu ändern.
- Der Windows-Computer kann die Anmeldeinformationen des Benutzers mithilfe des Active Directorys (AD) des Unternehmens überprüfen, und die Windows-Anmeldeinformationen auf dem Computer werden nicht zwischengespeichert. Außerdem können sich neue AD-Benutzer des Unternehmens nahtlos an der Maschine anmelden.
- Der Windows-Computer wird bereits vor der Anmeldung von Benutzern Teil des Unternehmensintranets, sodass IT-Administratoren aus dem Unternehmensnetzwerk zu Debugging-Zwecken auf den Clientcomputer zugreifen können.
- Der VPN-Tunnel für einen Windows-Computer bleibt auch dann verbunden, wenn sich verschiedene Benutzer an der Maschine anmelden oder abmelden.

### Always On VPN vor der Windows-Anmeldung verstehen

Im Folgenden finden Sie den Ablauf der Ereignisse für die **AlwaysOn-VPN-Funktion vor der Windows-Anmeldung**.




- Der Benutzer schaltet den Laptop ein. Der Tunnel auf Maschinenebene wird mit dem Gerätezertifikat als Identität in Richtung Citrix Gateway eingerichtet.

- Der Benutzer meldet sich mit AD-Anmeldeinformationen am Laptop an.
- Nach der Anmeldung wird der Benutzer mit MFA herausgefordert.
- Nach einer erfolgreichen Authentifizierung wird der Tunnel auf Maschinenebene durch den Tunnel auf Benutzerebene ersetzt.
- Sobald sich der Benutzer abmeldet, wird der Tunnel auf Benutzerebene durch den Tunnel auf Maschinenebene ersetzt.

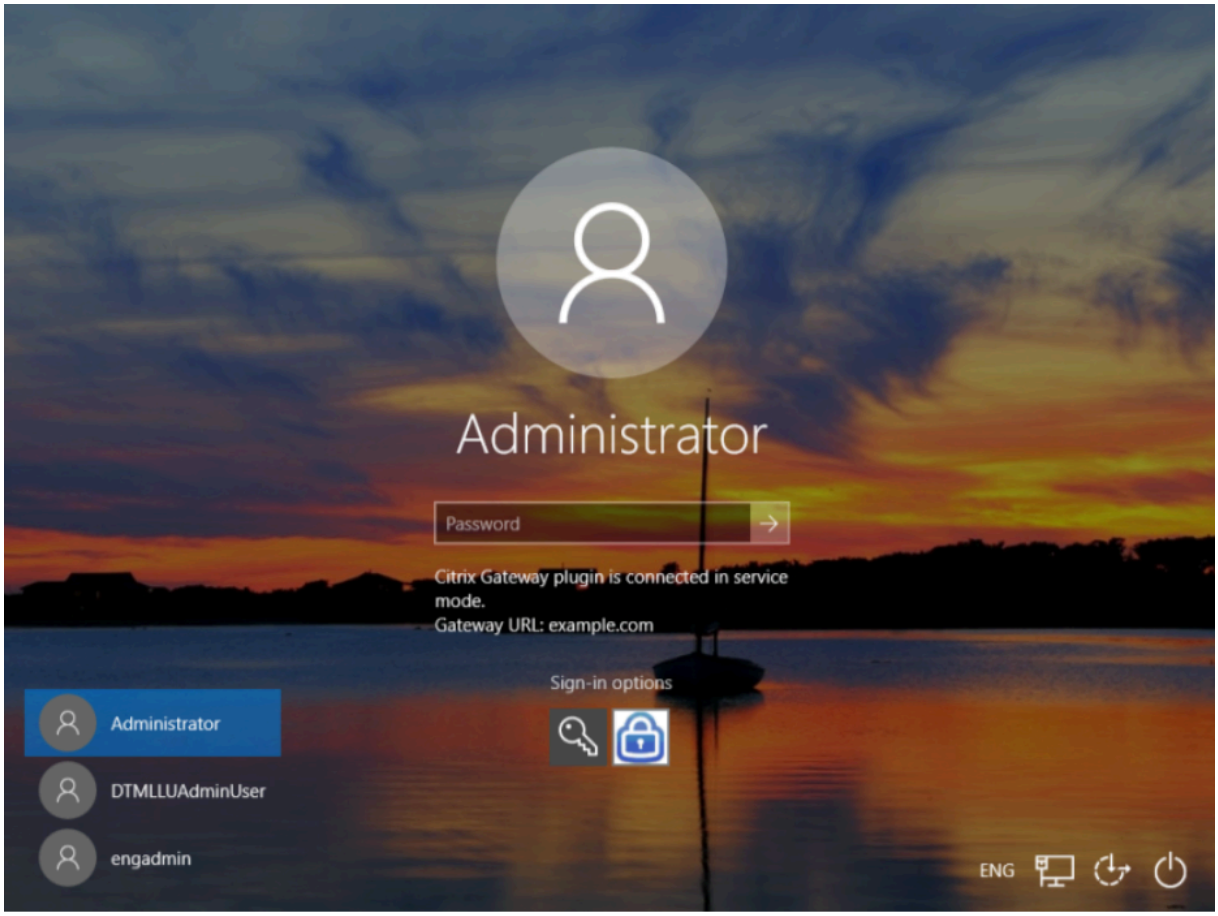
**Zu beachtende Punkte:**

- Citrix Gateway und VPN-Plug-In müssen Version 13.0.41.20 und höher sein.
- Wenn ein Clientcomputer keine Internetverbindung hat, wartet **Always On VPN vor der Windows-Anmeldung** darauf, dass die Internetverbindung verfügbar ist, bevor der VPN-Tunnel eingerichtet wird.
- Wenn ein Clientcomputer mit einem Captive-Portalnetzwerk verbunden ist, wartet **Always On VPN vor der Windows-Anmeldung** darauf, dass sich der Benutzer beim Captive-Portal authentifiziert. Nachdem sich der Benutzer anmeldet und der Internetzugang aktiviert ist, richtet **Always On VPN vor der Windows-Anmeldung** den VPN-Tunnel ein.
- Immer ein VPN vor der Windows-Anmeldung unterstützt Captive-Portale für Citrix ADC.
- Wenn die Option für zwischengespeicherte Anmeldeinformationen für Windows nicht aktiviert ist, können sich Benutzer in den folgenden Szenarien nicht anmelden:
  - Maschine hat keine Internetverbindung
  - Maschine ist mit einem Captive-Portal-Netzwerk verbunden
- Administratoren müssen den Status des Gerätezertifikats überprüfen, bevor sie den Endbenutzern die Anmeldeseite präsentieren.

## Bildschirm des Windows-Anmeldeinformationsmanagers nach Always On VPN vor der Konfiguration der Windows-

Nachdem die Funktion "**Immer ein VPN vor Windows-Anmeldung** "konfiguriert wurde, wird der Bildschirm des **Windows-Anmeldeinformations-Managers** wie folgt geändert.




Wenn Sie auf dem **Anmeldebildschirm auf Anmeldeoptionen** klicken, werden die folgenden Informationen angezeigt:

- Das Citrix Gateway-Symbol zeigt an, ob die Maschine mit Citrix Gateway verbunden ist oder nicht.
- Abhängig vom Benutzerkonfigurationsmodus wird eine der folgenden Anweisungen auf dem Anmeldebildschirm angezeigt.
  - Citrix Gateway ist im Dienstmodus verbunden
  - Citrix Gateway ist im Benutzermodus verbunden

## Always-On-VPN vor der Windows-Anmeldung konfigurieren

March 27, 2024

In diesem Abschnitt werden die Details zur Konfiguration von **Always On VPN vor der Windows-Anmeldung** mithilfe einer erweiterten Richtlinie erfasst.

### Voraussetzungen

- Citrix Gateway und VPN-Plug-In müssen Version 13.0.41.20 und höher sein.
- Citrix ADC Advanced Edition und höher ist erforderlich, damit die Lösung funktioniert.
- Sie können die Funktionalität nur mithilfe erweiterter Richtlinien konfigurieren.
- Der virtuelle VPN-Server muss betriebsbereit sein.

### Hochrangige Konfigurationsschritte

Die Konfiguration **Always On VPN vor der Windows-Anmeldung** umfasst die folgenden Schritte auf hoher Ebene:

1. Richten Sie einen Tunnel auf Maschinenebene ein
2. Richten Sie einen Tunnel auf Benutzerebene ein (optional)
3. Benutzerauthentifizierung aktivieren

    a) Konfigurieren Sie den virtuellen VPN-Server und binden Sie den Zertifikatsschlüssel an den virtuellen Server.
    b) Authentifizierungsprofil erstellen
    c) Erstellen Sie einen virtuellen Authentifizierungsserver
    d) Erstellen von Authentifizierungsrichtlinien
    e) Binden Sie die Richtlinien an das Authentifizierungsprofil

### Tunnel auf Maschinenebene

Der Tunnel auf Maschinenebene wird in Richtung Citrix Gateway mithilfe des Gerätezertifikats als Identität eingerichtet. Das Gerätezertifikat muss auf dem Clientcomputer unter dem Maschinenspeicher installiert sein. Dies gilt nur für den Dienst Always On vor dem Windows-Anmeldedienst.

Weitere Informationen zum Gerätezertifikat finden Sie unter Verwenden von Gerätezertifikaten für die Authentifizierung.

> **Wichtig:**
>
> Wenn der virtuelle VPN-Server auf der Citrix Gateway-Appliance auf einem nicht standardmäßigen Port (außer 443) konfiguriert ist, funktioniert der Tunnel auf Computerebene nicht wie vorgesehen.

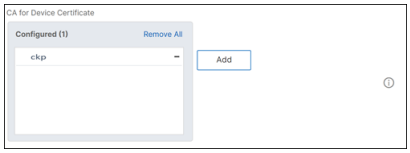
#### Richten Sie den Tunnel auf Maschinenebene mithilfe des Gerätezertifikats ein

#### Konfiguration der gerätezertifikatbasierten Authentifizierung über die GUI

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Citrix Gateway > Virtuelle Server**.

2. Wählen Sie auf der Seite Citrix Gateway Virtual Servers einen vorhandenen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite VPN Virtual Server auf das Bearbeitungssymbol.
4. Klicken Sie neben dem Abschnitt **CA for Device Certificate** auf **Hinzufügen** und dann auf **OK**.



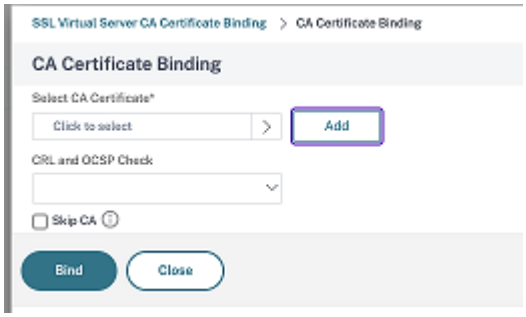

**Hinweis:** Aktivieren Sie nicht das Kontrollkästchen **Gerätezertifikat aktivieren**.

5. Um ein CA-Zertifikat an den virtuellen Server zu binden, klicken Sie im Abschnitt **Zertifikat** auf **CA-Zertifikat**. Klicken Sie auf der Seite **SSL Virtual Server CA Certificate Binding** auf **Bindung hinzufügen**.

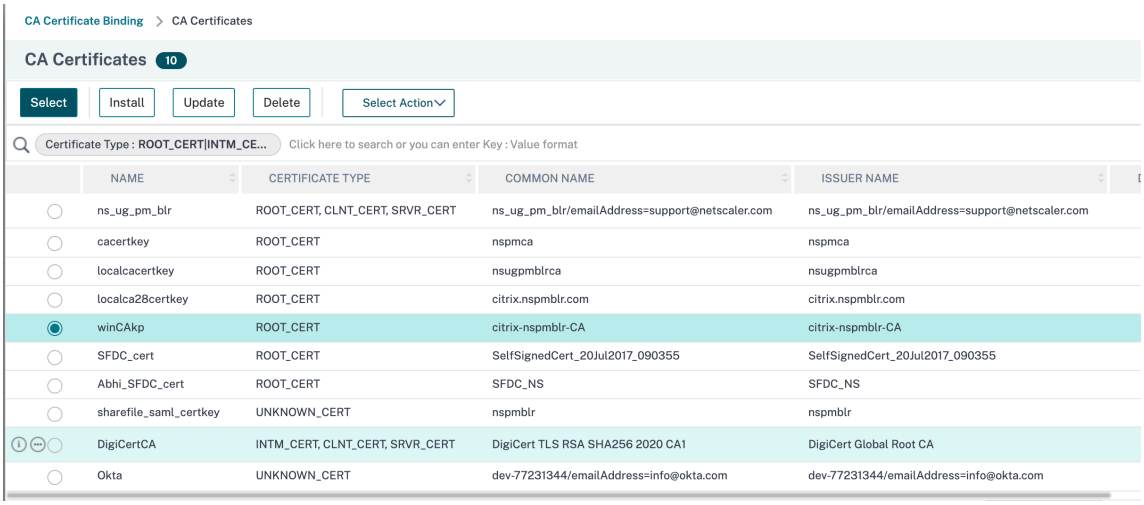
> **Hinweis:**
>
> - Das Feld Subject Common Name (CN) des Gerätezertifikats darf nicht leer sein. Wenn ein Gerät versucht, sich mit leeren CN-Gerätezertifikaten anzumelden, wird seine VPN-Sitzung mit dem Benutzernamen als “anonym”erstellt. Wenn in IIP mehrere Sitzungen denselben Benutzernamen haben, werden frühere Sitzungen getrennt. Wenn IIP aktiviert ist, bemerken Sie die Auswirkungen auf die Funktionalität aufgrund eines leeren gebräuchlichen Namens.
> - Alle CA-Zertifikate (Root und Intermediate), die das an Clients ausgestellte Gerätezertifikat möglicherweise signieren können, müssen an den Abschnitt **CA for Device Certificate** sowie an den Abschnitt **CA-Zertifikatbindung** für virtuelle Server in den Schritten 4 und 5 gebunden sein. Weitere Informationen zum Verknüpfen von CA-Zertifikaten mit Zwischen-/Untergeordneten finden Sie unter Installieren, Verknüpfen und Aktualisieren von Zertifikaten.
> - Wenn mehrere Gerätezertifikate konfiguriert sind, wird das Zertifikat mit dem längsten Ablaufdatum für die VPN-Verbindung versucht. Wenn dieses Zertifikat den EPA-Scan erfolgreich zulässt, wird die VPN-Verbindung hergestellt. Wenn dieses Zertifikat beim Scanvorgang fehlschlägt, wird das nächste Zertifikat verwendet. Dieser Vorgang wird solange fortgeführt, bis alle Zertifikate ausprobiert wurden.

6. Klicken Sie auf **Klicken zum Auswählen**, um das erforderliche Zertifikat auszuwählen.



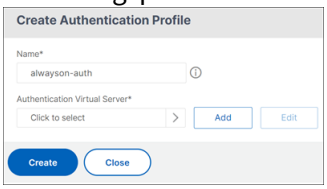

7. Wählen Sie das erforderliche CA-Zertifikat aus.




8. Klicken Sie auf **Bind**.
9. Erstellen Sie einen virtuellen Authentifizierungsserver.

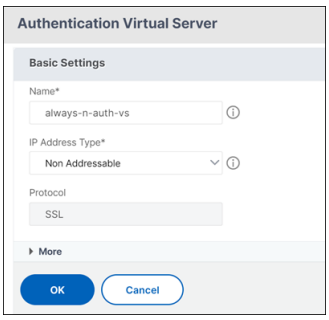
   a) Klicken Sie auf der Seite **Virtuelle VPN-Server** unter **Authentifizierungsprofil**auf **Hinzufügen**.

   b) Geben Sie auf der Seite **Authentifizierungsprofil erstellen** einen Namen für das Authentifizierungsprofil an und klicken Sie auf **Hinzufügen**.




   c) Geben Sie auf der Seite Virtueller Authentifizierungsserver einen Namen für den virtuellen Authentifizierungsserver an. Wählen Sie den IP-Adresstyp als **nicht adressierbar aus,** und klicken Sie auf **OK**.

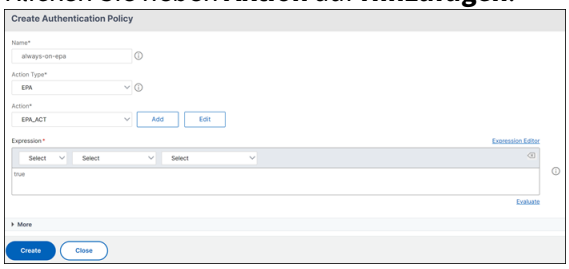
 



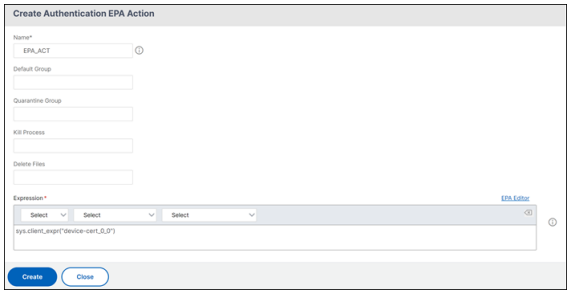

**Hinweis:** Der virtuelle Authentifizierungsserver bleibt immer im DOWN-Zustand.

10. Erstellen Sie eine Authentifizierungsrichtlinie.

    a) Klicken Sie unter "Erweiterte Authentifizierungsrichtlinien" in die Authentifizierungsrichtlinie.
    b) Klicken Sie auf der Seite Policy Binding neben **Richtlinie auswählen** auf **Hinzufügen**.
    c) Auf der Seite Authentifizierungsrichtlinie erstellen
        i. Geben Sie einen Namen für die erweiterte Authentifizierungsrichtlinie ein.
        ii. Wählen Sie **EPA** aus der Liste **Aktionstyp** aus.
        iii. Klicken Sie neben **Aktion** auf **Hinzufügen**.



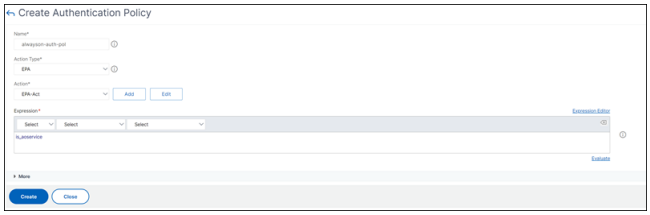

    d) Auf der Seite "EPA-Aktion für Authentifizierung erstellen";
        i. Geben Sie einen Namen für die zu erstellende EPA-Aktion ein.
        ii. Geben Sie `sys.client_expr("device-cert_0_0")` in das Feld **Ausdruck** ein.
        iii. Klicken Sie auf **Erstellen**.



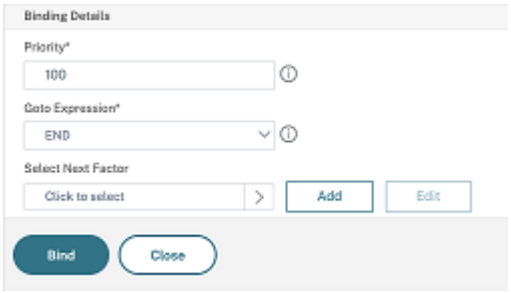

11. Auf der Seite Authentifizierungsrichtlinie erstellen

    a) Geben Sie einen Namen für die Authentifizierungsrichtlinie ein.
    b) Geben Sie **is_aoservice** in das Feld **Ausdruck** ein.
    c) Klicken Sie auf **Erstellen**.




12. Geben Sie auf der Seite Policy Binding **100** in **Priorität** ein und klicken Sie auf **Binden**.




### Konfiguration der gerätezertifikatbasierten Authentifizierung über die CLI

1. Binden Sie ein CA-Zertifikat an den virtuellen VPN-Server.

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```

Beispiel

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
    -ocspCheck Mandatory
<!--NeedCopy-->
```

2. Fügen Sie einen virtuellen Authentifizierungsserver hinzu.

```
add authentication authnProfile <name>  {
 -authnVsName <string> }

<!--NeedCopy-->
```

Beispiel

```
add authentication authnProfile always_on -authnVsName
    always_on_auth_server
<!--NeedCopy-->
```

3. Erstellen Sie eine EPA-Authentifizierungsaktion.

```
add authentication epaAction <name> -csecexpr <expression>
<!--NeedCopy-->
```

Example

“‘

add authentication epaAction epa-act -csecexpr `sys.client_expr("device-cert_0_0")` -defaultgroup epa_pass

“‘

4. Erstellen einer Authentifizierungsrichtlinie

```
add authentication Policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add authentication Policy always_on_epa_auth -rule is_aoservice -action epa_auth
```

**Wichtig:**

- Die Tunnelkonfiguration auf Maschinenebene ist jetzt abgeschlossen. Informationen zum Einrichten des Tunnels auf Benutzerebene nach der Windows-Anmeldung finden Sie im Abschnitt **Tunnel auf Benutzerebene**.
- Auf dem Clientcomputer ist das Gerätezertifikat im PFX-Format. Das PFX-Zertifikat ist auf dem Windows-Computer installiert, da Windows das PFX-Format versteht. Diese Datei enthält das Zertifikat und die Schlüsseldateien. Dieses Zertifikat muss derselben Domäne angehören, die an den virtuellen Server gebunden ist. Die PFX- und Serverzertifikate und -Schlüssel können mithilfe des Clientzertifikat-Assistenten generiert werden. Diese Zertifikate können zusammen mit der Zertifizierungsstelle verwendet werden, um die entsprechende PFX mit Serverzertifikat und Domäne zu generieren. Das Zertifikat .pfx ist im Computerkonto im persönlichen Ordner installiert. Der `show aaa session` Befehl zeigt den Gerätetunnel auf der Citrix ADC Appliance an.

## Tunnel auf Benutzerebene

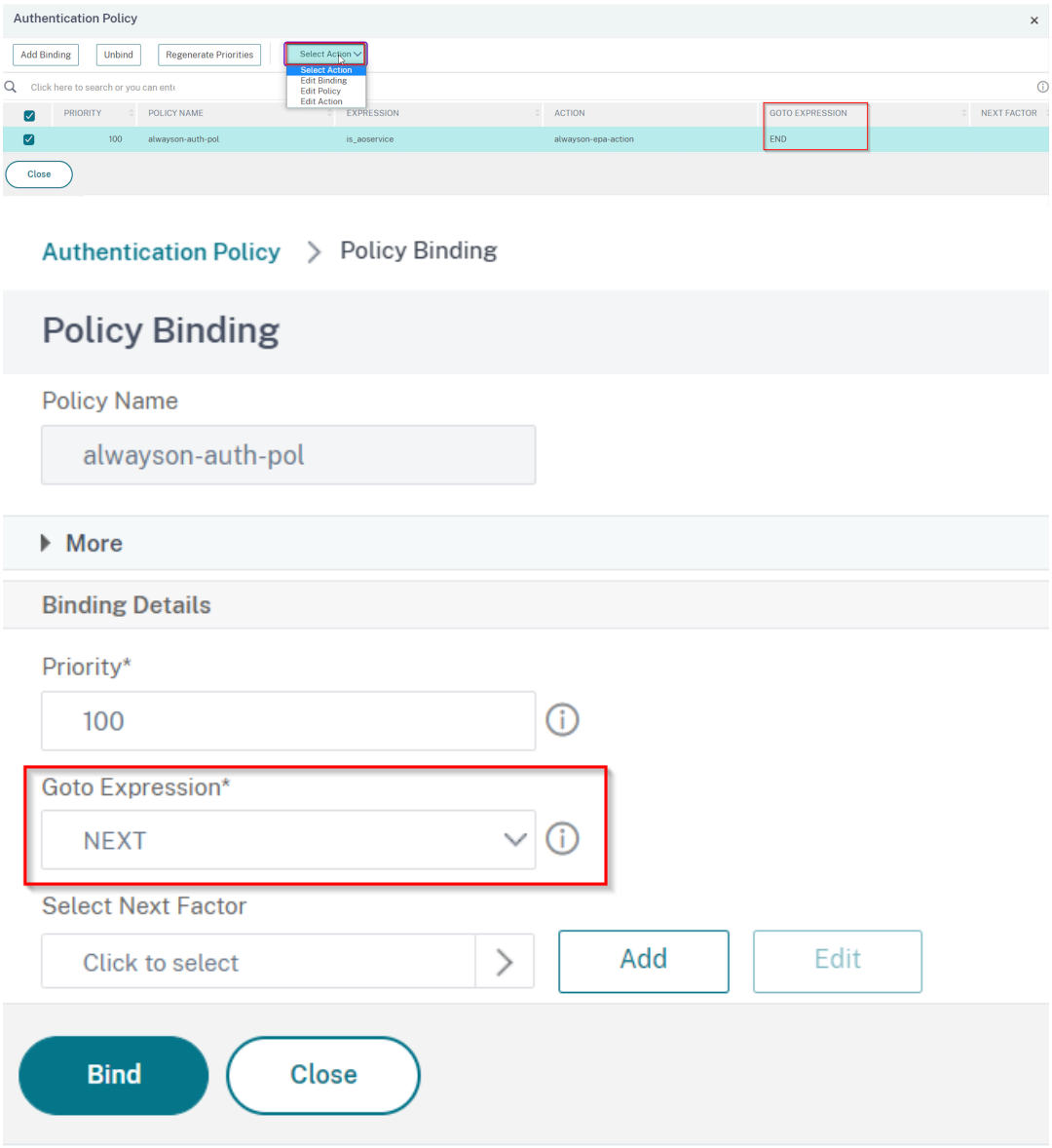
### Ersetzen eines Tunnels auf Maschinenebene durch einen Tunnel auf Benutzerebene über die GUI

**Hinweis:** Der Ausdruck `is_aoservice.not` gilt ab Citrix Gateway Version 13.0.41.20 und höher.

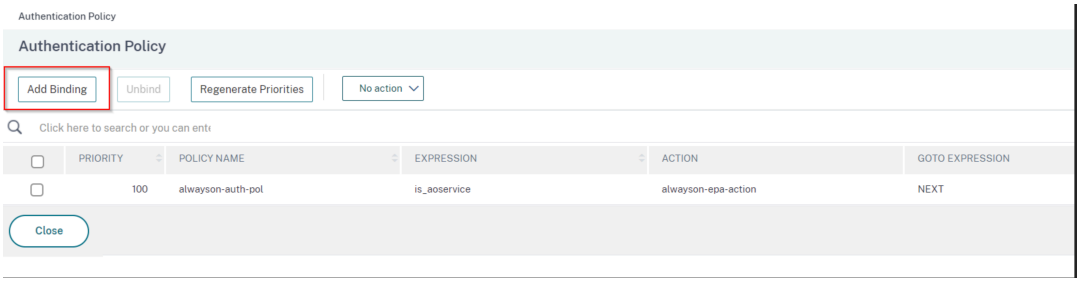
1. Konfigurieren Sie eine Richtlinie für die Benutzerauthentifizierung.
   a) Navigieren Sie zu **Citix Gateway > Virtuelle Server**, und klicken Sie in den **erweiterten Einstellungen**auf **Authentifizierungsprofil**.
   b) Konfigurieren Sie das Authentifizierungsprofil.
   c) Klicken Sie auf der Seite Virtueller Authentifizierungsserver in die Authentifizierungsrichtlinie.

d) Klicken **Sie unter Aktion auswählen**auf **Bindung bearbeiten**, und ändern Sie **GoTo-Ausdruck** für die Richtlinienbindung in **NEXT** anstelle von **END**.




e) Klicken Sie auf **Binden** und wählen Sie dann auf der Seite **Authentifizierungsrichtlinie** die Authentifizierungsrichtlinie aus und klicken Sie auf **Bindung hinzufügen**.

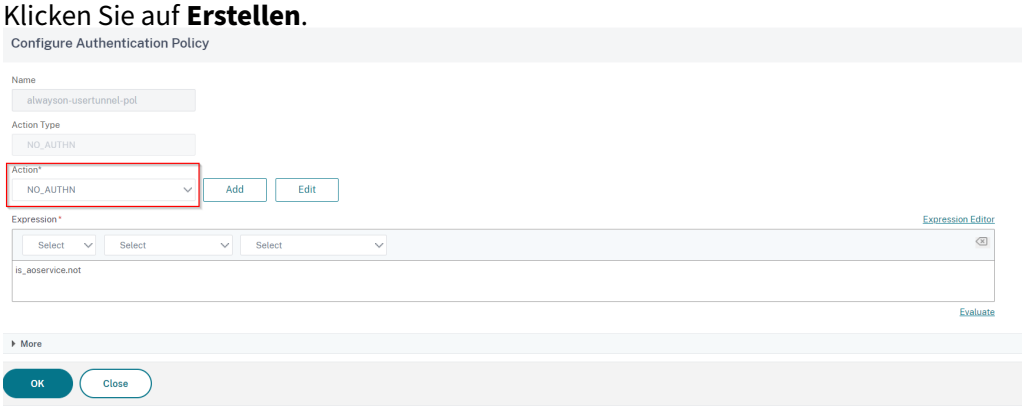


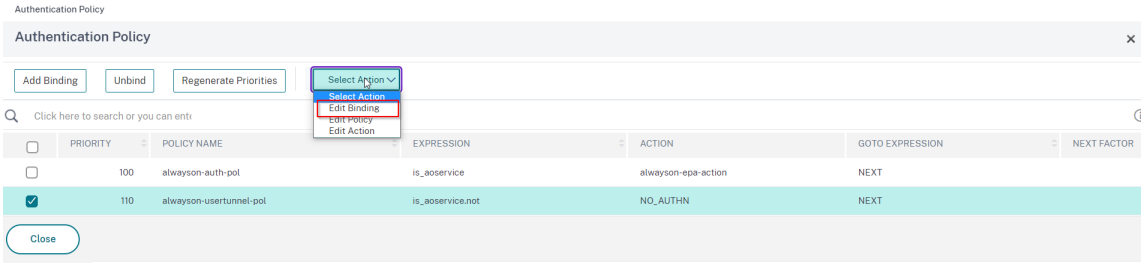
f) Klicken Sie auf der Seite Policy Binding neben **Richtlinie auswählen** auf **Hinzufügen**.

Auf der Seite Authentifizierungsrichtlinie erstellen

i. Geben Sie einen Namen für die Richtlinie “Keine Authentifizierung”ein, die erstellt werden soll.
ii. Wählen Sie den Aktionstyp als **NO_AuthN**.
iii. Geben Sie **is_aoservice.not** in das Feld **Ausdruck** ein.
iv. Klicken Sie auf **Erstellen**.




2. Klicken Sie unter **Aktion auswählen**auf **Bindung bearbeiten**.

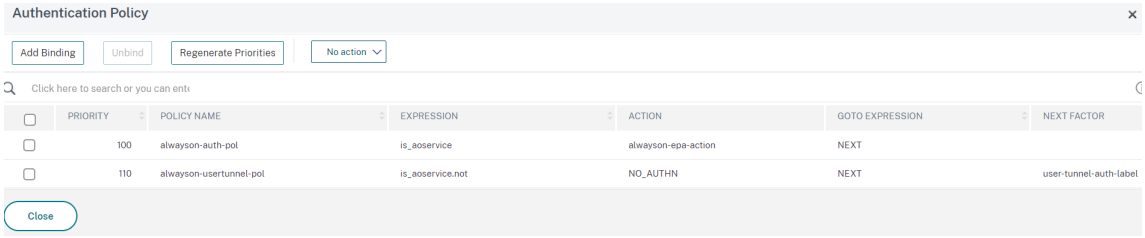



3. Geben Sie auf der Seite Policy Binding **110** in **Priorität**ein. Klicken Sie neben “Nächsten **Faktor auswählen”** auf **Hinzufügen**.

a) Geben Sie auf der Seite Authentifizierungsrichtlinienbezeichnung einen beschreibenden Namen für das Richtlinienlabel ein, wählen Sie das Anmeldeschema aus und klicken Sie auf **Weiter**.
b) Klicken Sie unter **Richtlinie auswählen**auf **Hinzufügen** und erstellen Sie eine LDAP-Authentifizierungsrichtlinie.
c) Klicken Sie auf **Erstellen** und dann auf **Binden.**
d) Klicken Sie auf **Fertig** und dann auf **Binden**.

Auf der Seite Authentifizierungsrichtlinie zeigt die Spalte **Nächster Faktor** die konfigurierte Richtlinie für den nächsten Faktor an.




4. Sie können die LDAP-Richtlinie als nächsten Faktor der Authentifizierungsrichtlinie konfigurieren.

   a) Geben Sie auf der Seite Authentifizierungsrichtlinie erstellen einen Namen für die LDAP-Richtlinie ein.
   b) Wählen Sie **Aktionstyp** als **LDAP**aus.
   c) Geben Sie **Action** als konfigurierte LDAP-Aktion ein.

> **Hinweis:**
>
> - Informationen zum Erstellen einer XML-Datei für das Anmeldeschema finden Sie unter XML-Dateifür das
> - Informationen zum Erstellen von Richtlinienbezeichnungen finden Sie unter Authentifizieren des Policy Label.
> - Informationen zum Erstellen einer LDAP-Authentifizierungsrichtlinie finden Sie unter So konfigurieren Sie die LDAP-Authentifizierung mithilfe des Konfigurationsdienstprogramms.

**Ersetzen eines Tunnels auf Maschinenebene durch einen Tunnel auf Benutzerebene über die CLI**

1. Binden einer Richtlinie an den virtuellen Authentifizierungsserver

```
bind authentication vserver <name> -policy <name> -priority  <
    positive_integer> -gotoPriorityExpression <expression>
```

   Beispiel

```
bind authentication vserver alwayson-auth-vserver -policy alwayson
    -auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. Fügen Sie eine Authentifizierungsrichtlinie mit dem Ausdruck Aktion als `NO_AUTH` und `is_aoservice.not`, und binden Sie sie an die Richtlinie.

```
add authentication Policy <name> -rule <expression> -action <
    string>

bind authentication vserver <name> -policy <name> -priority <
    positive_integer> -gotoPriorityExpression <expression>
```

Beispiel

```
add authentication Policy alwayson-usertunnel-pol -rule
    is_aoservice.not -action NO_AUTHN

bind authentication vserver alwayson-auth-vserver -policy alwayson
    -usertunnel-pol -priority 110
```

3. Fügen Sie einen nächsten Faktor hinzu und binden Sie die Policy Label an den nächsten Faktor.

```
add authentication policylabel <labelName> -loginSchema <string>

bind authentication  policylabel <string>  -policyName <string>  -
    priority <positive_integer> -gotoPriorityExpression <expression
    > -nextFactor <string>
```

Beispiel

```
add authentication policylabel user-tunnel-auth-label -loginSchema
     singleauth_alwayson

bind authentication policylabel user -policyName alwayson-
    usertunnel-pol -priority 100
```

4. Konfigurieren Sie eine LDAP-Richtlinie und binden Sie sie an die Policy Label des Benutzertunnels.

```
add authentication policy <name>  -rule <expression>  -action <
    string>

bind authentication vserver <vserver_name> -policy <string>  -
    priorit < positive integer>  gotoPriorityExpression <string>
```

Beispiel

```
add authentication Policy LDAP_new -rule true -action LDAP_new

bind authentication policylabel user-tunnel-auth-label -policyName
     LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

### Clientseitige Konfiguration

`AlwaysOn`, `locationDetection`, and `suffixList registries` sind optional und nur erforderlich, wenn die Standorterkennungsfunktion benötigt wird.

Um auf Registrierungsschlüsseleinträge zuzugreifen, navigieren Sie zu folgendem Pfad: **Computer>HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client**

| Registrierungsschlüssel | Registrierungstyp | Werte und Beschreibung |
|---|---|---|
| AlwaysOnService | REG_DWORD | 1 => Tunnel auf Maschinenebene einrichten, aber keinen Tunnel auf Benutzerebene; 2 => Tunnel auf Maschinenebene und Tunnel auf Benutzerebene einrichten |
| AlwaysOnURL | REG SZ | URL des virtuellen Citrix Gateway-Servers, mit dem der Benutzer eine Verbindung herstellen möchte. **Beispiel:** `https://xyz.companyDomain.com` **Wichtig:** Nur eine URL ist für den Tunnel auf Maschinenebene und den Tunnel auf Benutzerebene verantwortlich. Die AlwaysOnURL-Registrierung hilft sowohl der Service- als auch der Benutzerebenen-Komponente, einen separaten Tunnel zu arbeiten und zu verbinden, dh einen Tunnel auf Maschinenebene und einen auf dem Design basierenden Tunnel auf Benutzerebene |
| `AlwaysOn` | REG_DWORD | 1 => Netzwerkzugriff bei VPN-Fehler zulassen; 2=> Netzwerkzugriff bei VPN-Fehler blockieren |
| AlwaysOnAllowlist | REG_SZ | Semikolon-getrennte Liste von IP-Adressen oder FQDNs, die auf die Positivliste gesetzt werden müssen, während der Computer im strikten Modus läuft. **Beispiel:** `8.8.8.8;linkedin.com` |

| Registrierungsschlüssel | Registrierungstyp | Werte und Beschreibung |
|---|---|---|
| UserCertCAList | REG_SZ | Komma- oder Semikolon-getrennte Liste von Stamm-CA-Namen, das ist der Name des Ausstellers des Zertifikats. Wird im Kontext eines Always On Service verwendet, bei dem ein Kunde die Liste der Zertifizierungsstellen angeben kann, aus denen das Clientzertifikat ausgewählt werden soll. **Beispiel**: `cgwsanity.net;xyz.gov.in` |
| locationDetection | REG_DWORD | 1 => Um die Standorterkennung zu aktivieren; 0 => Um die Standorterkennung zu deaktivieren |
| suffixList | REG SZ | Die durch Semikolons getrennte Liste der Domänen ist dafür verantwortlich, zu überprüfen, ob sich das Gerät zu einem bestimmten Zeitpunkt im Intranet befindet oder nicht, wenn die Standorterkennung aktiviert ist. **Example:** `citrite.net`, `cgwsanity.net` |

Weitere Informationen zu diesen Registrierungseinträgen finden Sie unter Always On.

> **Hinweis:**
>
> Wenn der Always On-Dienst konfiguriert ist, wird das auf dem virtuellen Citrix Gateway-Server oder auf Citrix ADC konfigurierte Always On-Profil auf der Clientseite ignoriert. Stellen Sie daher sicher, dass Sie bei der Konfiguration des Always-On-Dienstes auch die VPN-Registrierungen

> `locationDetection` und `AlwaysOn` aktivieren.
> “‘

## VPN-Richtlinien über erweiterte Richtlinien erstellen

March 27, 2024

Classic Policy Engine (PE) und Advance Policy Infrastructure (PI) sind zwei verschiedene Frameworks für die Richtlinienkonfiguration und -bewertung, die Citrix ADC derzeit unterstützt.

Advance Policy Infrastructure besteht aus einer leistungsstarken Ausdruck Die Ausdruckssprache kann verwendet werden, um Regeln in Richtlinien zu definieren, verschiedene Teile von Action zu definieren und andere unterstützte Entitäten zu definieren. Die Ausdruckssprache kann jeden Teil der Anfrage oder Antwort analysieren und ermöglicht es Ihnen auch, die Header und die Nutzdaten genau zu durchsehen. Dieselbe Ausdruckssprache wird erweitert und funktioniert durch jedes logische Modul, das Citrix ADC unterstützt.

> **Hinweis:**
> Sie werden aufgefordert, erweiterte Richtlinien zum Erstellen von Richtlinien zu verwenden.

### Warum von Classic Policy zu Advance Policy migrieren?

Advanced Policy hat einen umfangreichen Ausdruckssatz und bietet eine viel größere Flexibilität als Classic Policy. Da Citrix ADC skaliert und für eine Vielzahl von Clients geeignet ist, ist es unerlässlich, Ausdrücke zu unterstützen, die die erweiterten Richtlinien bei weitem übertreffen. Weitere Informationen finden Sie unter Richtlinien und Ausdrücke.

Im Folgenden sind die zusätzlichen Funktionen für Advance-Richtlinien aufgeführt.

- Möglichkeit, auf den Hauptteil der Nachrichten zuzugreifen.
- Unterstützt viele andere Protokolle.
- Greift auf viele andere Funktionen des Systems zu.
- Hat mehr Grundfunktionen, Operatoren und Datentypen.
- Erreicht das Parsen von HTML-, JSON- und XML-Dateien.
- Erleichtert den schnellen parallelen Mehrsaiten-Abgleich (`patsets`usw.).

Jetzt können die folgenden VPN-Richtlinien mithilfe von Advance Policy konfiguriert werden.

- Sitzungsrichtlinie
- Autorisierungsrichtlinie
- Traffic Richtlinie

- Tunnel-Richtlinie
- Audit-Richtlinie

Außerdem kann Endpunktanalyse (EPA) als nFactor für die Authentifizierungsfunktion konfiguriert werden. EPA wird als Gatekeeper für Endpunktgeräte verwendet, die versuchen, eine Verbindung zum Gateway-Gerät herzustellen. Bevor die Gateway-Anmeldeseite auf einem Endpunktgerät angezeigt wird, wird das Gerät abhängig von den vom Gateway-Administrator konfigurierten Berechtigungskriterien auf minimale Hardware- und Softwareanforderungen überprüft. Der Zugriff auf das Gateway wird basierend auf dem Ergebnis der durchgeführten Überprüfungen gewährt. Zuvor wurde EPA als Teil der Sitzungsrichtlinie konfiguriert. Jetzt kann es mit nFactor verknüpft werden, was mehr Flexibilität bietet, wann es durchgeführt werden kann. Weitere Informationen zu EPA finden Sie unter Funktionsweise von Endpunkt-Richtlinien. Weitere Informationen zu nFactor finden Sie unter Thema nFactor-Authentifizierung.

**Anwendungsfälle:**

### Vorauthentifizierung EPA mit Advanced EPA

Der EPA-Scan vor der Authentifizierung erfolgt, bevor ein Benutzer die Anmeldeinformationen bereitstellt. Informationen zur Konfiguration von Citrix Gateway für die nFactor-Authentifizierung mit EPA-Scan vor der Authentifizierung als einem der Authentifizierungsfaktoren finden Sie im Thema CTX224268.

### Nach der Authentifizierung EPA mit Advanced EPA

Der EPA-Scan nach der Authentifizierung erfolgt, nachdem die Benutzeranmeldeinformationen überprüft wurden. Unter der klassischen Richtlinieninfrastruktur wurde EPA nach der Authentifizierung als Teil der Sitzungsrichtlinie oder Sitzungsaktion konfiguriert. Unter der erweiterten Richtlinieninfrastruktur soll der EPA-Scan als EPA-Faktor bei der nFactor-Authentifizierung konfiguriert werden. Informationen zur Konfiguration von Citrix Gateway für die nFactor-Authentifizierung mit EPA-Scan nach der Authentifizierung als einem der Authentifizierungsfaktoren finden Sie im Thema CTX224303.

### Vor- und Nachauthentifizierung EPA mithilfe erweiterter Richtlinien

EPA kann vor der Authentifizierung und nach der Authentifizierung durchgeführt werden. Informationen zur Konfiguration von Citrix Gateway für die nFactor-Authentifizierung mit EPA-Scans vor und nach der Authentifizierung finden Sie unter CTX231362 Thema.

### Periodischer EPA-Scan als Faktor bei der nFactor-Authentifizierung

Unter der klassischen Richtlinieninfrastruktur wurde der regelmäßige EPA-Scan als Teil der Sitzungsrichtlinienaktion konfiguriert. Unter der erweiterten Richtlinieninfrastruktur kann es als Teil des EPA-Faktors bei der nFactor-Authentifizierung konfiguriert werden.

Weitere Informationen zum Konfigurieren des periodischen EPA-Scans als Faktor bei der nFactor-Authentifizierung erhalten Sie, indem Sie aufCTX231361 Thema klicken.

**Problembehandlung:**

Die folgenden Punkte sind bei der Fehlerbehebung zu beachten.

- Klassische und Advance-Richtlinien desselben Typs (z. B. Sitzungsrichtlinie) können nicht an dieselbe Entität/denselben Bindungspunkt gebunden werden.
- Priorität ist für alle PI-Richtlinien obligatorisch.
- Die Vorab-Richtlinie für das VPN kann an alle Bindungspunkte gebunden werden.
- Advance Policy mit derselben Priorität kann an einen einzigen Bindepunkt gebunden werden.
- Wenn keine der konfigurierten Autorisierungsrichtlinien ausgewählt wird, wird die im VPN-Parameter konfigurierte globale Autorisierungsaktion angewendet.
- In der Autorisierungsrichtlinie wird die Autorisierungsaktion nicht rückgängig gemacht, wenn die Autorisierungsregel fehlschlägt.

**Häufig verwendete äquivalente Ausdrücke für erweiterte Richtlinien für klassische Richtlinien:**

| Klassische Richtlinienausdrücke | Erweiterte Richtlinienausdrücke |
|---|---|
| ns_true | wahr |
| ns_false | false |
| REQ.HTTP | HTTP.REQ |
| RES.HTTP | HTTP.RES |
| HEADER “foo” | HEADER(“foo”) |
| CONTAINS “bar” | .CONTAINS („bar“) [Beachten Sie die Verwendung von „..“] |
| REQ.IP | CLIENT.IP |
| RES.IP | SERVER.IP |
| SOURCEIP | SRC |
| DESTIP | DST |
| REQ.TCP | CLIENT.TCP |

| Klassische Richtlinienausdrücke | Erweiterte Richtlinienausdrücke |
|---|---|
| RES.TCP | SERVER.TCP |
| SOURCEPORT | SRCPORT |
| DESTPORT | DSTPORT |
| STATUSCODE | STATUS |
| REQ.SSL.CLIENT.CERT | CLIENT.SSL.CLIENT_CERT |

## Virtuellen DTLS-VPN-Server über den virtuellen SSL-VPN-Server konfigurieren

March 27, 2024

Sie können einen virtuellen DTLS-VPN-Server für NetScaler Gateway konfigurieren, indem Sie dieselbe IP-Adresse und Portnummer eines konfigurierten virtuellen SSL-VPN-Servers verwenden. Durch die Konfiguration virtueller DTLS-VPN-Server können Sie die erweiterten DTLS-Verschlüsselungen und -Zertifikate für eine erhöhte Sicherheit an den DTLS-Verkehr binden. Ab Version 13.0 Build 47.x wird das DTLS 1.2-Protokoll zusätzlich zum zuvor unterstützten DTLS 1.0-Protokoll unterstützt.

> **Wichtig:**
>
> - Standardmäßig ist die DTLS-Funktionalität für den vorhandenen virtuellen SSL-VPN-Server auf ON eingestellt. Deaktivieren Sie die Funktionalität für den Server, bevor Sie den virtuellen DTLS-VPN-Server erstellen.
> - Der virtuelle SNI für den virtuellen DTLS-Gateway-Server wird in NetScaler Gateway Version 13.0 Build 64.x und höher unterstützt.
> - Ab NetScaler Version 13.0 Build 79.x ist der `helloverifyrequest` Parameter standardmäßig aktiviert. Die Aktivierung des Parameters `helloverifyrequest` im DTLS-Profil hilft, das Risiko zu verringern, dass ein Angreifer oder Bots den Netzwerkdurchsatz überfordert, was möglicherweise zu einer Erschöpfung der ausgehenden Bandbreite führt. Das heißt, es hilft, den DTLS DDoS-Verstärkungsangriff zu mildern. Einzelheiten zum `helloverifyrequest` Parameter finden Sie unter DTLS-Profil.
> - Bei der Verarbeitung des UDP-Datenverkehrs steigt der Speicherverbrauch der NetScaler-Appliance, wenn die Back-End-Server viel Datenverkehr übertragen. Daher kann die

> NetScaler-Appliance diesen Datenverkehr aufgrund der TCP-MUX-Verbindung auf der Clientseite nicht an den Client übertragen. In solchen Fällen empfiehlt Citrix, das DTLS-Protokoll zu verwenden.

### Wichtige Hinweise

- Der virtuelle DTLS VPN-Server auf einer NetScaler Gateway-Appliance kann ab Version 13.0 Build 58.x konfiguriert werden.
- Bevor Sie einen virtuellen DTLS-VPN-Server auf einem NetScaler Gateway-Gerät konfigurieren, müssen Sie einen virtuellen SSL-VPN-Server auf der Appliance konfiguriert haben.
- Der virtuelle DTLS-VPN-Server verwendet die IP-Adresse und die Portnummer des konfigurierten virtuellen SSL-VPN-Servers.
- Wenn der DTLS-Handshake fehlschlägt, fällt die Verbindung auf TLS zurück.
- Um nur DTLS zu verwenden, können Sie TLS deaktivieren, indem Sie nur die DTLS-Chiffren an den DTLS-Verkehr binden.
- DTLS-Multiplexing wird nicht unterstützt, wenn TCP-Verkehr über VPN getunnelt wird.

### Virtuellen DTLS-VPN-Server mit der GUI konfigurieren

1. Navigieren Sie auf der Registerkarte Konfiguration zu **NetScaler Gateway > Virtuelle Server**.
2. Wählen Sie auf der Seite **Virtuelle NetScaler Gateway -Server** den vorhandenen virtuellen SSL-VPN-Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **VPN Virtual Server** auf das Bearbeitungssymbol, deaktivieren Sie das Kontrollkästchen **DTLS** und klicken Sie auf **OK**.
4. Navigieren Sie zurück zu **NetScaler Gateway > Virtuelle Server** und klicken Sie auf **Hinzufügen.**
5. Geben Sie unter **Grundeinstellungen**die Werte für die folgenden Felder ein und klicken Sie auf **OK**.
    - Name —Ein Name für den virtuellen DTLS-VPN-Server
    - Protokoll - Wählen Sie DTLS
    - IP-Adresse - Geben Sie die IP-Adresse des virtuellen SSL-VPN-Servers ein
    - Port - Geben Sie die Portnummer des virtuellen SSL-VPN-Servers ein
6. Wählen Sie auf der Seite **NetScaler Gateway Virtual Servers** den virtuellen Server aus, den Sie zuvor hinzugefügt haben, und klicken Sie auf **Bearbeiten.**

7. Klicken Sie unter **Zertifikate** auf das Pfeilsymbol, um den erforderlichen Zertifizierungsschlüssel auszuwählen.
8. Wählen Sie unter **Serverzertifikatbindung > Serverzertifikat auswählen** einen vorhandenen SSL-Zertifikatsschlüssel aus oder erstellen Sie einen.
9. Klicken Sie auf der Seite **Serverzertifikatbindung** auf **Binden**.

> **Hinweis:**
>
> - Um DTLS 1.2 zu verwenden, klicken Sie unter SSL-Parameter auf das Bearbeitungssymbol und aktivieren Sie das Kontrollkästchen **DTLS 1.2**.
> - Die Angabe des Servernamens (SNI) wird für virtuelle VPN-Server des Typs DTLS unterstützt.

### Virtuellen DTLS-VPN-Server mit der CLI konfigurieren

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
set vpn vserver <ssl vpnvserver name> -dtls off
add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl vpn vserver port>
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key>
<!--NeedCopy-->
```

DTLS 1.0 funktioniert wie gewohnt, um DTLS 1.2 zu verwenden, geben Sie den folgenden Befehl ein:

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
<!--NeedCopy-->
```

Beispiel

```
set vpn vserver vpnvserver  -dtls off
add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443
bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey
set ssl vserver vpnvserver_dtls -dtls12 ENABLED
<!--NeedCopy-->
```

**Um SNI für den virtuellen VPN-Server vom Typ DTLS zu aktivieren, geben Sie den folgenden Befehl ein:**

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key> <-SNICert>
<!--NeedCopy-->
```

Beispiel

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED
bind ssl vserver _XD_10.106.40.225_443_DTLS -certkeyName "Insight/*.
    insight.net.cer_CERT_" -snICert

<!--NeedCopy-->
```

#### Unterstützte virtuelle DTLS-VPN-Serverparameter

Nur die folgenden Parameter werden für den virtuellen VPN-Server vom Typ DTLS unterstützt.

- Ipaddress
- Port
- Status
- Double-Hop
- downstateflush
- Kommentar
- Appflowlog
- Icmpvsrresponse

#### Nicht unterstützte virtuelle DTLS-VPN-Serverparameter

Die folgenden Parameter werden für den virtuellen VPN-Server vom Typ DTLS nicht unterstützt.

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect
- logoutOnSmartcardRemoval
- l2Conn
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- failedLoginTimeout
- vserverFqdn
- deviceCert
- rdpServerProfileName
- pcoipVserverProfileName
- tcpProfileName

- netProfile
- authnProfile
- Listenpriority
- Listenpolicy
- ipset
- certkeyNames

### Virtuellen DTLS-Server mit dem XenApp- und XenDesktop-Assistenten konfigurieren

1. Klicken Sie unter **In Citrix-Produkte integrieren**auf **XenApp und XenDesktop**.
2. Wählen Sie im Setupassistenten für XenApp und XenDesktop **StoreFront** aus und klicken Sie auf **Weiter**.
3. Aktivieren Sie auf der Seite mit den **NetScaler Gateway-Einstellungen** das Kontrollkästchen **DTLS-Listener für diesen virtuellen VPN-Server konfigurieren** und klicken Sie auf **Weiter.**

   Der DTLS-Listener ist jetzt konfiguriert.
4. Klicken Sie unter Serverzertifikat auf **Datei auswählen**, um das Serverzertifikat auszuwählen, und klicken Sie auf **Weiter**.
5. Geben Sie die Zertifikatsdatei und den Namen der Schlüsseldatei an und klicken Sie auf **Weiter**.
6. Geben Sie im Abschnitt **StoreFront** die Werte für die erforderlichen Parameter wie folgt ein und klicken Sie auf **Weiter**.
7. Geben Sie im Abschnitt **Authentifizierung** die Werte für die erforderlichen Parameter wie folgt ein und klicken Sie auf **Verbindung testen**.

   Stellen Sie sicher, dass der Server erreichbar ist, geben Sie Timeout-Wert und Serveranmeldenamen-Attribut an, und klicken Sie auf **Continue**.
8. Klicken Sie auf **Fertig**, um die Konfiguration abzuschließen.

### Einschränkungen

- DTLS 1.2 wird nur auf Windows-Clients unterstützt.
- Der virtuelle VPN-Server mit DTLS unterstützt keine IPv6-Adressen.
- SSL-Richtlinie und SSL-Profil werden auf einem virtuellen DTLS-VPN-Server nicht unterstützt. Außerdem wird die Bindung der VPN-Server-Richtlinie nicht unterstützt.
- Der virtuelle NetScaler Gateway DTLS VPN-Server unterstützt die folgenden Funktionen nicht. Der virtuelle NetScaler Gateway SSL VPN-Server unterstützt jedoch diese Funktionen:
  - Unified Gateway mit virtuellen Content Switching-Server

  - UDP MUX
  - UDP-Video
  - UDP-Audio
  - PCOIP

- Der `stat vpn vserver` Befehl, der sich auf die Statistiken für den virtuellen DTLS-VPN-Server bezieht, wird nicht unterstützt.
- HSM-Schlüssel werden mit dem virtuellen DTLS-Server nicht unterstützt.
- Die Clusterkonfiguration wird nicht unterstützt.

## Integration mit Citrix Produkten

March 27, 2024

Wenn Sie ein Systemadministrator sind, der für die Installation und Konfiguration von Citrix Gateway verantwortlich ist, können Sie das Gerät so konfigurieren, dass es Citrix Endpoint Management, StoreFront und das Webinterface unterstützt.

Benutzer können direkt über das interne Netzwerk oder von einem Remote-Standort aus eine Verbindung zu Endpoint Management herstellen. Wenn Benutzer eine Verbindung herstellen, können sie auf ihr Web, SaaS und ihre mobilen Apps zugreifen. Sie können auch Dokumente in ShareFile von jedem Gerät aus unterstützen.

Um Benutzerverbindungen zu einer Serverfarm über Citrix Gateway zuzulassen, konfigurieren Sie Einstellungen entweder in StoreFront oder im Webinterface und auf Citrix Gateway. Wenn Benutzer eine Verbindung herstellen, haben sie Zugriff auf veröffentlichte Anwendungen und virtuelle Desktops.

Die Konfigurationsschritte für die Integration von Citrix Gateway in Endpoint Management, StoreFront und das Webinterface gehen von folgendem aus:

- Citrix Gateway befindet sich in der DMZ und ist mit einem vorhandenen Netzwerk verbunden.
- Citrix Gateway wird als eigenständiges Gerät bereitgestellt, und Remotebenutzer stellen eine direkte Verbindung zu Citrix Gateway her.
- StoreFront, Endpoint Management, Citrix Virtual Apps, Citrix Virtual Desktops und das Webinterface befinden sich im sicheren Netzwerk.
- ShareFile ist in Endpoint Management konfiguriert. Weitere Informationen zu ShareFile finden Sie unter ShareFile-Thema und Thema ShareFile für Benutzerzugriff konfigurieren.

Wie Sie StoreFront und Endpoint Management bereitstellen, hängt von den Apps ab, die Sie für mobile Geräte bereitstellen. Wenn Benutzer Zugriff auf MDX-Apps haben, die mit dem MDX Toolkit umschlossen sind, befindet sich Endpoint Management vor StoreFront im sicheren Netzwerk. Wenn

Sie keinen Zugriff auf MDX-Apps gewähren, befindet sich StoreFront vor Endpoint Management im sicheren Netzwerk.

## Wie Benutzer eine Verbindung zu Anwendungen, Desktops und ShareFile herstellen

January 19, 2024

Wenn Sie Citrix Endpoint Management in Ihrer Bereitstellung haben, können Benutzer auf folgende Weise eine Verbindung herstellen:

- Citrix Gateway-Plug-In, mit dem ein vollständiger VPN-Tunnel zu Ressourcen im internen Netzwerk eingerichtet wird. Sie erstellen ein Sitzungsprofil, um das Citrix Gateway-Plug-In für Windows oder das Citrix Gateway-Plug-In für Mac auszuwählen. Wenn sich Benutzer mit dem Plug-In anmelden, können Endpunktanalysescans auf dem Benutzergerät ausgeführt werden.

> **Hinweis**: Damit Endpunktanalysescans auf Mac-Computern ausgeführt werden können, müssen Sie Citrix Gateway 10.1, Build 120.1316.e oder neuer installieren.

- Citrix Workspace-App zum Herstellen einer Verbindung mit Web-, SaaS- und Enterprise-Anwendungen, Weblinks und Dokumenten von ShareFile über Endpoint Management. Wenn sich Benutzer mit der Citrix Workspace-App anmelden, leitet Citrix Gateway die Verbindung an Endpoint Management weiter. Wenn die Citrix Workspace-App die Verbindung aufbaut, werden die Anwendungen und Dokumente der Benutzer in der Citrix Workspace-App angezeigt. Wenn sich Benutzer mit der Citrix Workspace-App anmelden und sich direkt mit Endpoint Management verbinden, müssen Sie den clientlosen Zugriff in Citrix Gateway aktivieren. Für diese Bereitstellung ist StoreFront nicht erforderlich.
- Citrix Workspace-App zum Herstellen einer Verbindung mit veröffentlichten Anwendungen und virtuellen Desktops über StoreFront oder das Webinterface. Wenn sich Benutzer mit der Citrix Workspace-App anmelden, leitet Citrix Gateway die Verbindung an StoreFront oder das Webinterface weiter. Wenn die Citrix Workspace-App die Verbindung aufbaut, werden Benutzeranwendungen und Desktops in der Citrix Workspace-App angezeigt.
- Secure Hub zur Verbindung mit iOS- und Android-Apps, einschließlich WorxMail und WorxWeb, von mobilen Geräten über Endpoint Management. Wenn sich Benutzer bei Secure Hub anmelden, haben sie Zugriff auf die mobilen Apps, die Sie in Endpoint Management konfigurieren. Wenn Citrix Gateway die Micro-VPN-Verbindung herstellt, werden mobile Apps der Benutzer im Secure Hub-Fenster angezeigt. Benutzer können die Apps über Secure Hub starten. Einige Apps erfordern, dass Benutzer die App auf dem mobilen Gerät herunterladen und installieren.

Wenn Benutzer über Citrix Gateway eine Verbindung herstellen möchten, führen Sie in einem der vorhergehenden Szenarien folgende Schritte aus:

- Benutzer melden sich mit dem Citrix Gateway-Plug-In oder der Citrix Workspace-App an. Um sich zum ersten Mal anzumelden, öffnen Benutzer einen Webbrowser und geben den vollqualifizierten Domänennamen (FQDN) der Citrix Gateway oder der Citrix Workspace-App ein. Benutzer mit mobilen Geräten melden sich mit Secure Hub an.
- Auf der Anmeldeseite geben Benutzer ihre Anmeldeinformationen ein und werden authentifiziert.
- Nach der Authentifizierung leitet die Benutzersitzung je nach Bereitstellung zu StoreFront oder Endpoint Management um.
- Wenn Sie StoreFront und Endpoint Management bereitstellen, kontaktiert Citrix Gateway den ersten Server in der Bereitstellung. Wenn Sie beispielsweise mobile MDX-Apps in Endpoint Management konfigurieren, stellen Sie StoreFront hinter Endpoint Management bereit. Wenn Sie keinen Zugriff auf mobile MDX-Apps bereitstellen, stellen Sie Endpoint Management hinter StoreFront bereit.
- Alle Desktops, Dokumente und Webanwendungen der Benutzer, SaaS und Windows-basierte Anwendungen werden in der Citrix Workspace-App oder Secure Hub angezeigt.

Wenn Benutzer auf andere Ressourcen im internen Netzwerk zugreifen müssen, z. B. Exchange, Dateifreigaben oder interne Sites, können sie sich auch mit dem Citrix Gateway-Plug-In anmelden. Wenn Benutzer beispielsweise eine Verbindung zu einem Microsoft Exchange-Server im Netzwerk herstellen möchten, starten sie Microsoft Outlook auf ihrem Computer. Die sichere Verbindung wird mit dem Citrix Gateway-Plug-In hergestellt, das eine Verbindung mit Citrix Gateway herstellt. Der SSL-VPN-Tunnel wird für den Exchange Server erstellt und Benutzer können auf ihre E-Mails zugreifen.

> **Wichtig**: Citrix empfiehlt die Konfiguration der Authentifizierung auf dem virtuellen Citrix Gateway-Server. Wenn Sie die Authentifizierung in Citrix Gateway deaktivieren, werden nicht authentifizierte HTTP-Anforderungen direkt an die Server gesendet, auf denen das Webinterface, StoreFront oder Endpoint Management im internen Netzwerk ausgeführt wird.

## Citrix Gateway mit StoreFront integrieren

March 27, 2024

Der **Citrix Virtual Apps and Desktops**-Assistent wird verwendet, um StoreFront in Citrix Gateway zu integrieren. Die Integration erleichtert den Zugriff auf gehostete virtuelle Desktops (XenDesktop) und gehostete virtuelle Windows-Apps (XenApp) über Citrix Gateway.

Für die Citrix Gateway-Integration mit StoreFront wurde der Workflow des Citrix Virtual Apps and Desktops-Assistenten jetzt um die folgenden Funktionen erweitert.

- **Abruf der auf dem unterstützten StoreFront konfigurierten Stores:** Die auf unterstütztem StoreFront konfigurierten Stores können mit einem Klick abgerufen werden. Diese Abrufmethode hilft, manuelle Eingriffe zu vermeiden und somit menschliche Fehler (Tippfehler) zu vermeiden.
- **Exportunterstützung für StoreFront-Konfigurationsdatei:** Die StoreFront-Konfigurationsdateien können in Citrix Gateway exportiert werden. Die StoreFront-Konfigurationsdatei kann dann heruntergeladen und schließlich auf einen unterstützten StoreFront-Server importiert werden. Sobald die Datei importiert wurde, schließt StoreFront die NetScaler-Integration ab.
- **StoreFront** als Authentifizierungsserver: Die**Authentifizierung** wird durch die Einführung einer erweiterten Authentifizierungsaktion vereinfacht, um StoreFront als Authentifizierungsserver für Authentifizierungsdienste zu verwenden.

> **Hinweis:** Der Authentifizierungsserver kann auch für Nicht-Citrix Virtual Apps and Desktops-Bereitstellungen verwendet werden.

## So konfigurieren Sie Citrix Gateway für die Verwendung mit StoreFront

### Voraussetzungen

Sie benötigen die folgenden Informationen, um NetScaler in StoreFront zu integrieren:

- IP-Adresse des virtuellen Citrix Gateway-Servers
- Vollqualifizierter Domänenname (FQDN) des StoreFront-Servers
- Ein Serverzertifikat für das Citrix Gateway
- Details zum Authentifizierungsserver

Stellen Sie außerdem Folgendes sicher:

- Der Firewall-Port zwischen Citrix Gateway und StoreFront ist geöffnet
- StoreFront hat LAN-Zugriff

**So integrieren Sie StoreFront mithilfe der Citrix Gateway GUI in Citrix Gateway:**

1. Klicken Sie auf die Registerkarte **Konfiguration**.
2. Klicken **Sie in Integrate with Citrix Products**auf **XenApp und XenDesktop**.
3. Klicken Sie auf **Get Started.**
4. Wählen Sie **StoreFront** und klicken Sie auf **Weiter.**
5. Geben Sie die Werte für die folgenden Felder im Bereich Citrix Gateway ein und klicken Sie auf **Weiter.**

- **Gateway FQDN** —FQDN von Citrix Gateway
- **Gateway-IP-Adresse** —IP-Adresse von Citrix Gateway
- **Port** —Port von Citrix Gateway

6. Importieren Sie die folgenden Dateien im Bereich **Serverzertifikat** und klicken Sie auf **Weiter**. **Zertifikatsdatei** —Serverzertifikat für das Citrix Gateway.
7. Geben Sie im **StoreFront-Bereich** die folgenden Informationen ein und klicken Sie auf **Weiter**.

   - **StoreFront-URL** —URL des StoreFront-Servers
   - **Receiver für Web Path** - Pfad zu Receiver für Website, die bereits auf StoreFront konfiguriert ist
   - **Active Directory-Standarddomäne** - Single Sign-On-Domäne, die für Single-Sign-On-Anwendungen im internen Netzwerk verwendet werden soll
   - **Secure Ticket Authority URL** —Die Secure Ticket Authority URL, die normalerweise auf dem Zustellungscontroller vorhanden ist.

     > **Hinweis:**Bei Auswahl von "**Stores abrufen**"kontaktiert Citrix Gateway StoreFront und gibt alle Store-Informationen zurück, die in StoreFront konfiguriert sind. Sie können dann den bevorzugten Store aus dem Dropdownmenü auswählen. Die Option **Stores abrufen** funktioniert nur für den neuesten StoreFront-Server.

8. Mit den neuen Authentifizierungseinstellungen kann ein Benutzer eine Authentifizierungsrichtlinie erstellen oder Sie können eine vorhandene Authentifizierungsrichtlinie verwenden.

   Um eine domänenbasierte Authentifizierungsrichtlinie zu erstellen, geben Sie die Werte für die folgenden Felder in ein und klicken Sie auf **Weiter**.

9. **Wählen Sie Authentifizierungstyp -** Domäne wählen aus dem Dropdownmenü
10. Wählen Sie **Neuen Server hinzufügen** oder **Bestehenden Server verwenden** basierend auf Ihren Anforderungen

    - **IP-Adresse** —IP-Adresse für den Domain-Server
    - **Port** —Port des Domänenservers
    - **Basis-DN** - Der Basis-DN, unter dem sich die Benutzer befinden
    - **Dienstkonto** —Das für die Abfrage von Active Directory verwendete Konto
    - **Kennwort** - Das Kennwort, das für die Anmeldung am Domain-Server erforderlich ist
    - **Timeout** - Die Zeitdauer, für die das Domain-Verzeichnis nachgeschlagen wird
    - **Server-Anmeldenamen-Attribut** —Das Namensattribut, das von der NetScaler-Appliance zur Abfrage des externen Domänenservers oder eines Active Directory verwendet wird.

Sie können optional auf **Verbindung testen** klicken, um sicherzustellen, dass der Server erreichbar ist und gültige Anmeldeinformationen bereitgestellt werden.

> **Hinweis:**Um eine vorhandene Authentifizierungsrichtlinie zu verwenden, wählen Sie den erforderlichen **Authentifizierungstyp** aus der Liste **Authentifizierungstyp auswählen** aus und geben Sie die zuvor aufgeführten Informationen ein.

11. Klicken Sie auf der Seite Citrix Gateway-Einstellungen auf **Fertig.**
12. Klicken Sie auf **Datei herunterladen.**

**Im Folgenden sind die auf der StoreFront-GUI erforderlichen Konfigurationsschritte aufgeführt:**

1. Kopieren Sie die `Gatewayconfig.zip` Datei nach StoreFront.
2. Klicken Sie auf **Stores**.
3. Wählen Sie **Citrix Gateways verwalten** aus und klicken Sie im Fenster **Citrix Gateways verwalten** auf den Link **Aus Datei importieren**.
4. Klicken Sie im Fenster **NetScaler-Konfiguration importieren** unter **Datei auswählen** auf **Weiter**.
5. Geben Sie im Bereich **Anmeldetyp auswählen** optional eine **Rückruf-URL** an, damit StoreFront Citrix Gateway kontaktieren kann, und klicken Sie auf **Weiter**.
6. Klicken Sie unter Secure Ticket Authorities auf Weiter.
7. Klicken Sie unter **Änderungen überprüfen** auf **Weiter**.
8. Klicken Sie auf **Fertig stellen**.

## Citrix Gateway mit Citrix Virtual Apps and Desktops integrieren

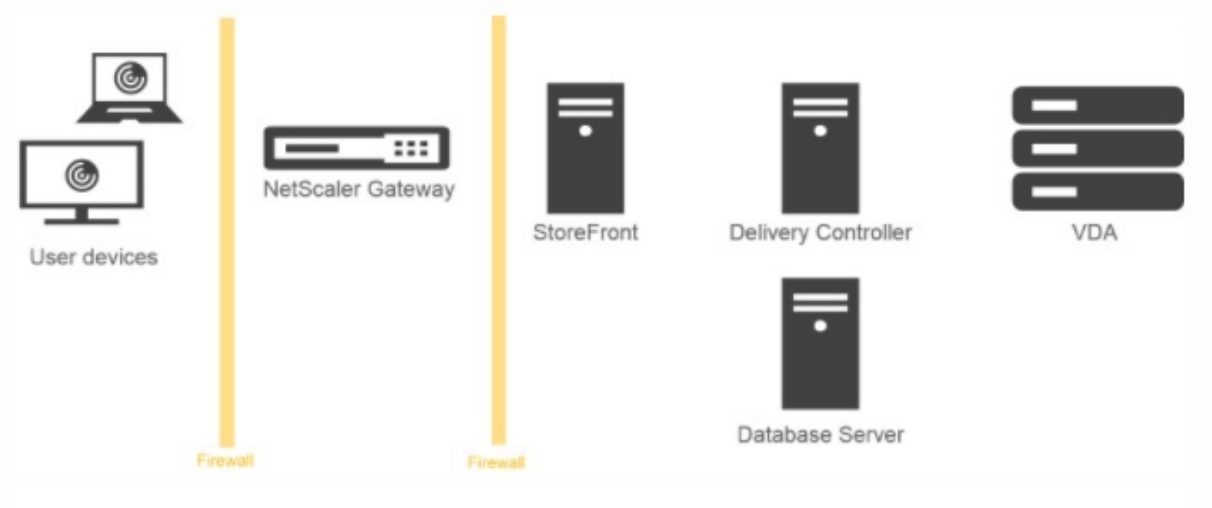
March 27, 2024

StoreFront-Server werden für die Zugriffsverwaltung auf veröffentlichte Ressourcen und Daten bereitgestellt und konfiguriert. Für den Remotezugriff wird das Hinzufügen von Citrix Gateway vor StoreFront empfohlen.

> **Hinweis**
>
> Ausführliche Konfigurationsschritte zur Integration von Citrix Virtual Apps and Desktops in Citrix Gateway finden Sie in derStoreFront-Dokumentation.

Das folgende Diagramm zeigt ein Beispiel für eine vereinfachte Citrix Bereitstellung, die Citrix Gateway enthält. Citrix Gateway kommuniziert mit StoreFront zum Schutz von Apps und Daten, die mit Citrix Virtual Apps and Desktops bereitgestellt werden. Die Benutzergeräte führen zum Herstellen einer sicheren Verbindung für den Zugriff auf Apps, Desktops und Dateien die Citrix Workspace-App aus.




Die Anmeldung und Authentifizierung von Benutzern erfolgt über Citrix Gateway. Citrix Gateway ist in der DMZ bereitgestellt und geschützt. Die zweistufige Authentifizierung ist konfiguriert. Anhand der Benutzeranmeldeinformationen werden Benutzern die relevanten Ressourcen und Anwendungen bereitgestellt. Die Anwendungen und Daten sind auf geeigneten Servern (nicht abgebildet). Separate Server werden für sicherheitskritische Anwendungen und Daten verwendet.

## Bereitstellung mit Citrix Endpoint Management, Citrix Virtual Apps und Desktop

March 27, 2024

Sie können Benutzer eine Verbindung zu Windows-, Web-, SaaS- und mobilen Anwendungen und virtuellen Desktops herstellen lassen, die in Ihrem Netzwerk gehostet werden. Mithilfe von Citrix Gateway, Citrix Endpoint Management und Citrix Virtual Apps and Desktops können Sie Remote- und internen Benutzern Zugriff auf Ihre Anwendungen und Desktops gewähren. Citrix Gateway authentifiziert Benutzer und ermöglicht ihnen dann den Zugriff auf ihre Anwendungen mithilfe der Citrix Workspace-App oder Secure Hub.

Benutzer stellen über die Citrix Workspace-App und StoreFront eine Verbindung zu ihren in Citrix Virtual Apps veröffentlichten Windows-basierten Apps und ihren in Citrix Virtual Desktops veröffentlichten virtuellen Desktops her.

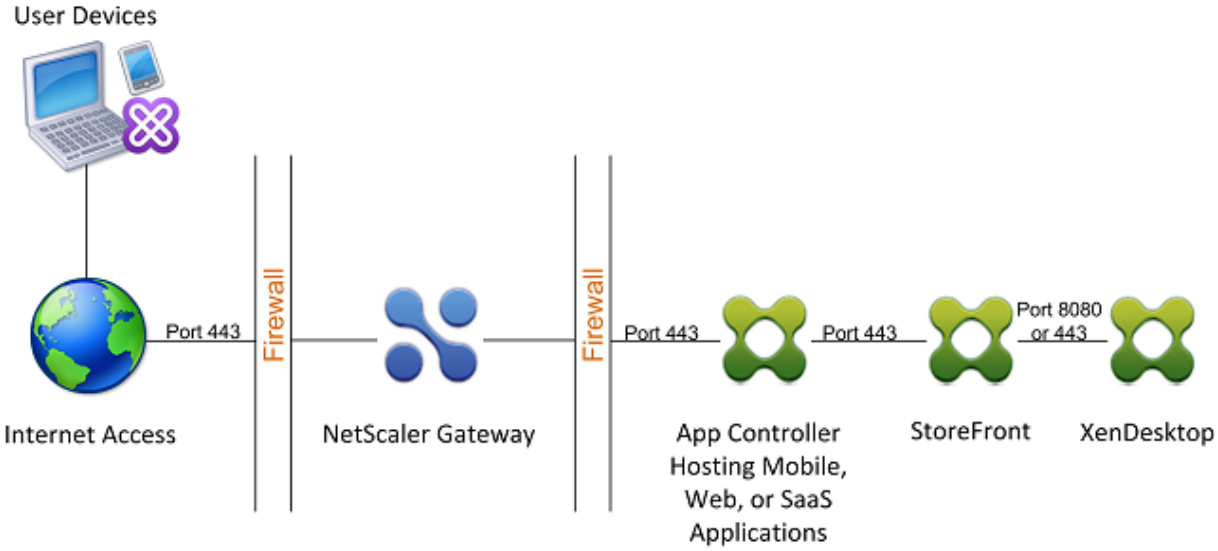
Citrix Endpoint Management enthält Citrix Endpoint Management, mit dem Benutzer eine Verbindung zu Web-, SaaS- und MDX-Anwendungen herstellen können. Mit Endpoint Management können Sie Web-, SaaS- und MDX-Anwendungen für Single Sign-On (SSO) zusammen mit ShareFile-Dokumenten verwalten. Sie installieren Endpoint Management im internen Netzwerk. Remote-Benutzer stellen über Citrix Gateway eine Verbindung zu Endpoint Management her, um auf ihre Anwendungen und

ShareFile-Daten zuzugreifen. Remote-Benutzer können sich entweder mit dem Citrix Gateway Plug-in, der Citrix Workspace-App oder Secure Hub verbinden, um auf Anwendungen und ShareFile zuzugreifen. Benutzer, die sich im internen Netzwerk befinden, können mithilfe der Citrix Workspace-App direkt eine Verbindung zu Endpoint Management herstellen. Die folgende Abbildung zeigt Citrix Gateway, das mit Endpoint Management und StoreFront bereitgestellt wurde.

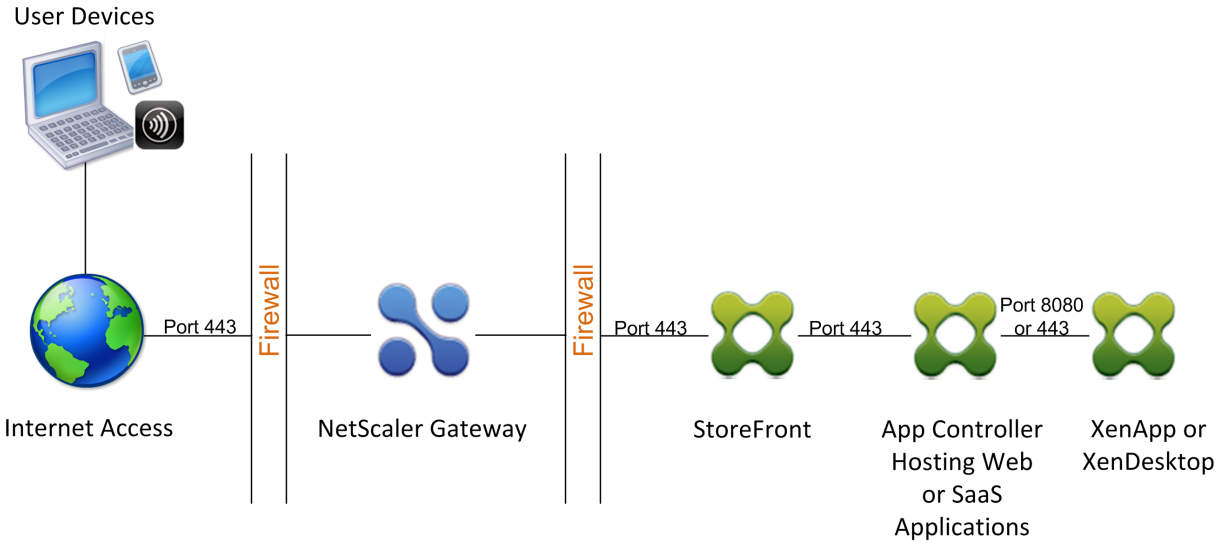
Wenn Ihre Bereitstellung Zugriff auf MDX-Anwendungen von Endpoint Management und Zugriff auf Windows-basierte Anwendungen von StoreFront aus bietet, stellen Sie Endpoint Management vor StoreFront bereit, wie in der folgenden Abbildung gezeigt:

Abbildung 1. Bereitstellen von Citrix Gateway mit Endpoint Management vor StoreFront




Wenn Ihre Bereitstellung keinen Zugriff auf MDX-Anwendungen bietet, ist StoreFront vor Endpoint Management, wie in der folgenden Abbildung gezeigt:

Abbildung 2. Bereitstellen von Citrix Gateway mit StoreFront vor Endpoint Management



Bei jeder Bereitstellung müssen sich StoreFront und Endpoint Management im internen Netzwerk befinden, und Citrix Gateway muss sich in der DMZ befinden. Weitere Informationen zum Bereitstellen von Endpoint Management finden Sie unter Installieren von Endpoint Management unter Installieren von Endpoint Management.
Weitere Informationen zur Bereitstellung von StoreFront finden Sie unter StoreFront-Thema.

## Einstellungen für Ihre Citrix Endpoint Management-Umgebungkonfigurieren

January 29, 2024

Der NetScaler für Citrix Endpoint Management-Assistent führt Sie durch die Konfiguration der NetScaler-Funktionen für Ihre Citrix Endpoint Management-Bereitstellung. Sie können den Assistenten verwenden, um:

- **Richten Sie ein Micro-VPN ein.** In diesem Szenario können Remote-Benutzer auf Apps und Desktops im internen Netzwerk zugreifen.
  - Für den Nur-MAM-Modus von Citrix Endpoint Management müssen Sie NetScaler Gateway für die Authentifizierung verwenden.
  - Für MDM-Bereitstellungen empfiehlt Citrix die Verwendung von NetScaler Gateway für VPNs für Mobilgeräte.
  - Wenn sich ein Benutzer bei ENT-Bereitstellungen von der MDM-Registrierung abmeldet, arbeitet das Gerät im Legacy-MAM-Modus und meldet sich mit dem NetScaler Gateway FQDN an.
- **Konfigurieren Sie die zertifikatbasierte Authentifizierung.** Die Standardkonfiguration für Citrix Endpoint Management ist Benutzernamen- und Kennwortauthentifizierung. Um eine weitere Sicherheitsebene für die Registrierung und den Zugriff auf die Citrix Endpoint Management-Umgebung hinzuzufügen, sollten Sie die Verwendung zertifikatbasierter Authentifizierung in Betracht ziehen.
- **Lastausgleich Citrix Endpoint Management-Server.** NetScaler-Lastausgleich ist für alle Citrix Endpoint Management-Gerätemodi erforderlich, wenn Sie über mehrere Citrix Endpoint Management-Server verfügen oder wenn sich Citrix Endpoint Management in Ihrer DMZ oder Ihrem internen Netzwerk befindet (und daher der Datenverkehr von Geräten zu NetScaler zu Citrix Endpoint Management fließt). In diesem Szenario befindet sich die NetScaler Appliance in der DMZ zwischen dem Benutzergerät und den Citrix Endpoint Management-Servern, um den Lastausgleich verschlüsselter Daten, die von Mobilgeräten an die Citrix Endpoint Management-Server gesendet werden, durchzuführen.

- **Lastausgleich von Microsoft Exchange-Servern mit E-Mail-Filter.** In diesem Szenario befindet sich die NetScaler Appliance zwischen dem Benutzergerät und dem Citrix Endpoint Management NetScaler Connector (XNC) sowie zwischen dem Benutzergerät und den Microsoft Exchange CAS-Servern. Alle Anfragen von Benutzergeräten gehen an das NetScaler Gateway-Gerät, das dann mit dem XNC kommuniziert, um Informationen über das Gerät abzurufen. Abhängig von der Antwort des XNC leitet die NetScaler Appliance die Anforderung entweder von einem Gerät auf der Positivliste an den Server im internen Netzwerk weiter oder löscht die Verbindung von einem Gerät auf der Sperrliste.
- **Lastausgleich ShareFile StorageZones Connectors basierend auf der Art des angeforderten Inhalts.** Dieses Szenario fordert Sie zur Eingabe grundlegender Informationen über Ihre StorageZones Controller-Umgebung auf und generiert dann eine Konfiguration, die Folgendes bewirkt:
  - Load gleicht den Datenverkehr über Storage Zones Controller aus.
  - Bietet Benutzerauthentifizierung für StorageZones Connectors.
  - Validiert URI-Signaturen für ShareFile-Uploads und -Downloads.
  - Beendet SSL-Verbindungen an der NetScaler Appliance.

Weitere Informationen zum Konfigurieren von ShareFile finden Sie unter Konfigurieren von NetScaler für StorageZones Controller.

> **Wichtig:**
>
> Bevor Sie den Citrix Endpoint Management-Assistenten verwenden, lesen Sie unbedingt diese Artikel zur Citrix Endpoint Management-Bereitstellung für Design- und Bereitstellungsinformationen und Empfehlungen:
>
> Citrix Endpoint Management-Integration
>
> Integration in NetScaler Gateway und NetScaler
>
> SSO- und Proxy-Überlegungen für MDX-Apps
>
> Authentifizierung
>
> Sie können den NetScaler für Citrix Endpoint Management-Assistenten nur einmal verwenden. Wenn Sie mehrere Citrix Endpoint Management-Instanzen benötigen, z. B. für Test-, Entwicklungs- und Produktionsumgebungen, müssen Sie NetScaler für die zusätzlichen Umgebungen manuell konfigurieren. In den folgenden Supportartikeln werden die Befehle aufgeführt, die vom Assistenten ausgeführt werden, und enthalten Anweisungen zum Ausführen dieser Befehle zum Erstellen einer NetScaler-Instanz:
>
> Vom Citrix Endpoint Management-Assistenten auf NetScaler generierte Befehle - SSL Bridge
>
> Befehle, die vom Citrix Endpoint Management-Assistenten auf NetScaler generiert wurden - SSL

> Offload

### Lizenzanforderungen für NetScaler-Funktionen

Sie müssen Lizenzen installieren, um die folgenden NetScaler-Funktionen zu aktivieren:

- Für den Citrix Endpoint Management MDM-Lastausgleich ist eine NetScaler-Standardlizenz erforderlich.
- Für den ShareFile-Lastenausgleich mit StorageZones ist eine NetScaler-Standardlizenz erforderlich.
- Für den Exchange-Lastausgleich ist eine NetScaler-Lizenz oder eine Advanced-Lizenz mit dem Zusatz einer Integrated Caching-Lizenz erforderlich.

### NetScaler für Citrix Endpoint Management-Assistent

Dieser Abschnitt enthält ein Beispiel für die Verwendung des NetScaler für Citrix Endpoint Management-Assistenten für:

- Richten Sie den Micro-VPN-Zugriff für Remote-Benutzerverbindungen zu von Citrix Endpoint Management verwalteten Ressourcen in Ihrem internen Netzwerk ein
- Konfigurieren Sie die zertifikatbasierte Authentifizierung. Informationen zum Abrufen und Installieren eines öffentlichen SSL-Zertifikats finden Sie unter Installieren und Verwalten von Zertifikaten.
- Konfigurieren Sie den Lastenausgleich für Citrix Endpoint Management-Server.

So verwenden Sie den Assistenten:

1. Klicken Sie in der NetScaler-GUI auf die Registerkarte **Configuration** und dann im Abschnitt **Integrate with Citrix Products** auf **XenMobile**.
2. Wählen Sie Ihre Citrix Endpoint Management-Version aus und klicken Sie dann auf **Erste Schritte**.
3. Wählen Sie die Funktionen aus, die Sie konfigurieren möchten. Sie können diesen Assistenten nur einmal verwenden und müssen die nachfolgende Konfiguration daher manuell durchführen. Bei diesen Anweisungen wird davon ausgegangen, dass Sie die folgenden Einstellungen auswählen: **Zugriff über NetScaler Gateway** (für Citrix Endpoint Management, das im ENT- oder MAM-Modus ausgeführt wird) und **Load Balance Citrix Endpoint Management Server**.
4. Geben Sie auf der Seite **NetScaler Gateway-Konfiguration** Werte für die externe NetScaler Gateway-IP-Adresse, den Port und den Namen des virtuellen Servers ein.
5. Wählen Sie auf der Seite **Serverzertifikat für NetScaler Gateway** unter **Zertifikatdatei** die Zertifikatdatei aus **Local** oder **Appliance** aus.

- Local: Wählen Sie das Zertifikat auf Ihrem Computer aus
- Appliance: Wählen Sie das Zertifikat auf NetScaler Gateway (Applicance) aus.

6. Wählen Sie auf der Seite **Authentifizierung** unter **Primäre Authentifizierungsmethode** die Option **Clientzertifikat** aus, und geben Sie dann einen Namen für das Zertifikatprofil ein.

   Bei den folgenden Schritten wird davon ausgegangen, dass Sie bereits eine Zertifikatrichtlinie haben.

   Wenn Sie eine Zertifikatrichtlinie erstellen müssen, klicken Sie auf Zertifikatrichtlinie erstellen. Wählen Sie auf dem Bildschirm Citrix Endpoint Management-Zertifikat ein vorhandenes Serverzertifikat aus, oder installieren Sie ein neues Zertifikat. Wenn Sie mehrere Citrix Endpoint Management-Server ausführen, fügen Sie für jeden ein Zertifikat hinzu. Geben Sie für das Serveranmeldenamenattribut je nach Ihren Anforderungen userPrincipalName oder sAMAccountName an.

7. Klicken Sie auf **Two Factor**, um die Zweifaktorauthentifizierung zu aktivieren, d. h. die Clientzertifikatauthentifizierung gefolgt von LDAP oder RADIUS als sekundären Authentifizierungstyp.

8. Wählen Sie unter **Sekundäre Authentifizierungsmethode** die sekundäre Authentifizierungsmethode aus.

   - Mit dem Clientzertifikat als primärer Authentifizierungstyp haben Sie die Möglichkeit, LDPA (oder RADIUS) als sekundären Authentifizierungstyp zu konfigurieren.

     Um nur die Clientzertifikatauthentifizierung zu verwenden, lassen Sie die **zweite Authentifizierungsmethode** als **Keine** und klicken Sie dann auf **Weiter**.

     Um die Authentifizierung mit Clientzertifikat und Domäne (LDAP) zu verwenden, ändern Sie die **Sekundäre Authentifizierungsmethode** in **LDAP** und konfigurieren Sie die Authentifizierungsservereinstellungen.

9. Konfigurieren Sie die **Citrix Endpoint Management App Management-Einstellungen**.

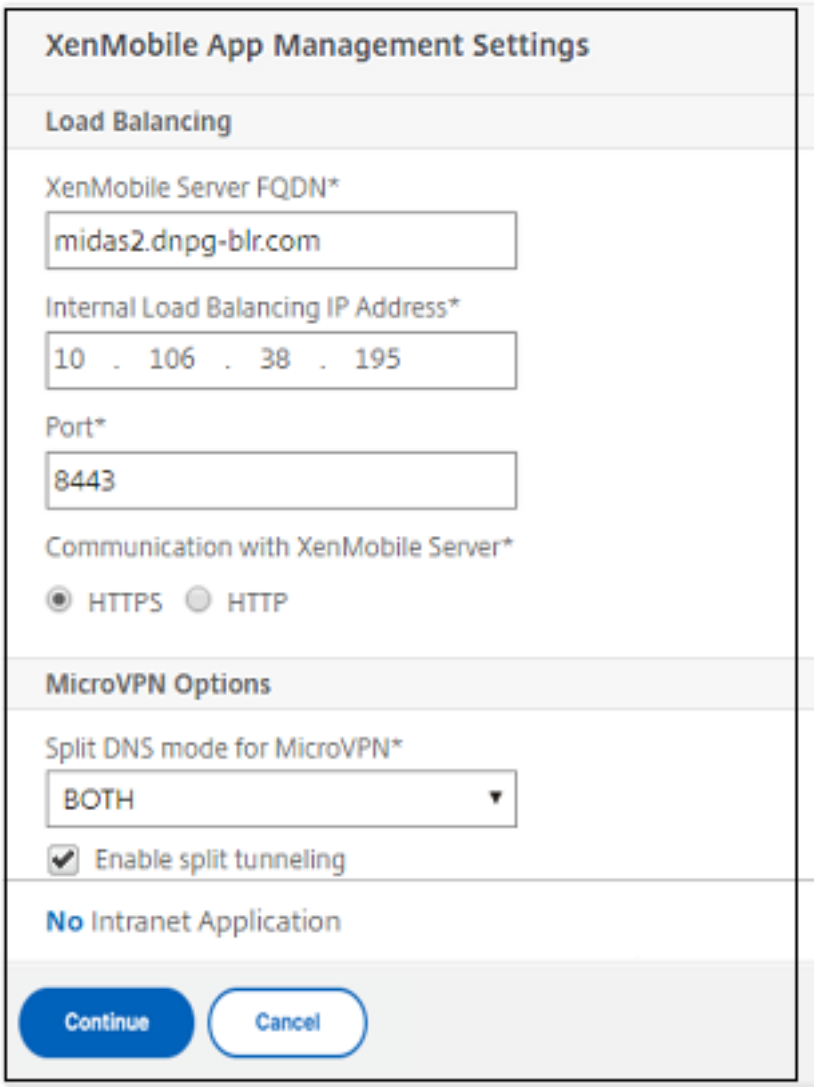
   - Geben Sie den **Citrix Endpoint Management-FQDN**ein.Dies ist der Lastausgleichs-FQDN für MAM.
   - Geben Sie eine **interne Lastausgleichs-IP-Adresse nur für MAM**für den virtuellen Server ein, der Citrix Endpoint Management-Server ausgleicht. NetScaler Gateway kommuniziert über diese virtuelle MAM-Lastausgleich-IP mit Citrix Endpoint Management.
   - Dies ist eine SSL-Offload-Bereitstellung. Wählen Sie daher**HTTP**in**Kommunikation mit Citrix Endpoint Management Server**aus.
   - Das Feld**Split-DNS-Modus für MicroVPN**wird automatisch auf**BEIDE**eingestellt.

   Wenn Ihre Bereitstellung Split-Tunneling erfordert, wählen Sie **Split-Tunneling aktivieren**. Konfigurieren Sie als Nächstes die Intranet-Anwendungsbindung, wenn Sie Split-Tunneling

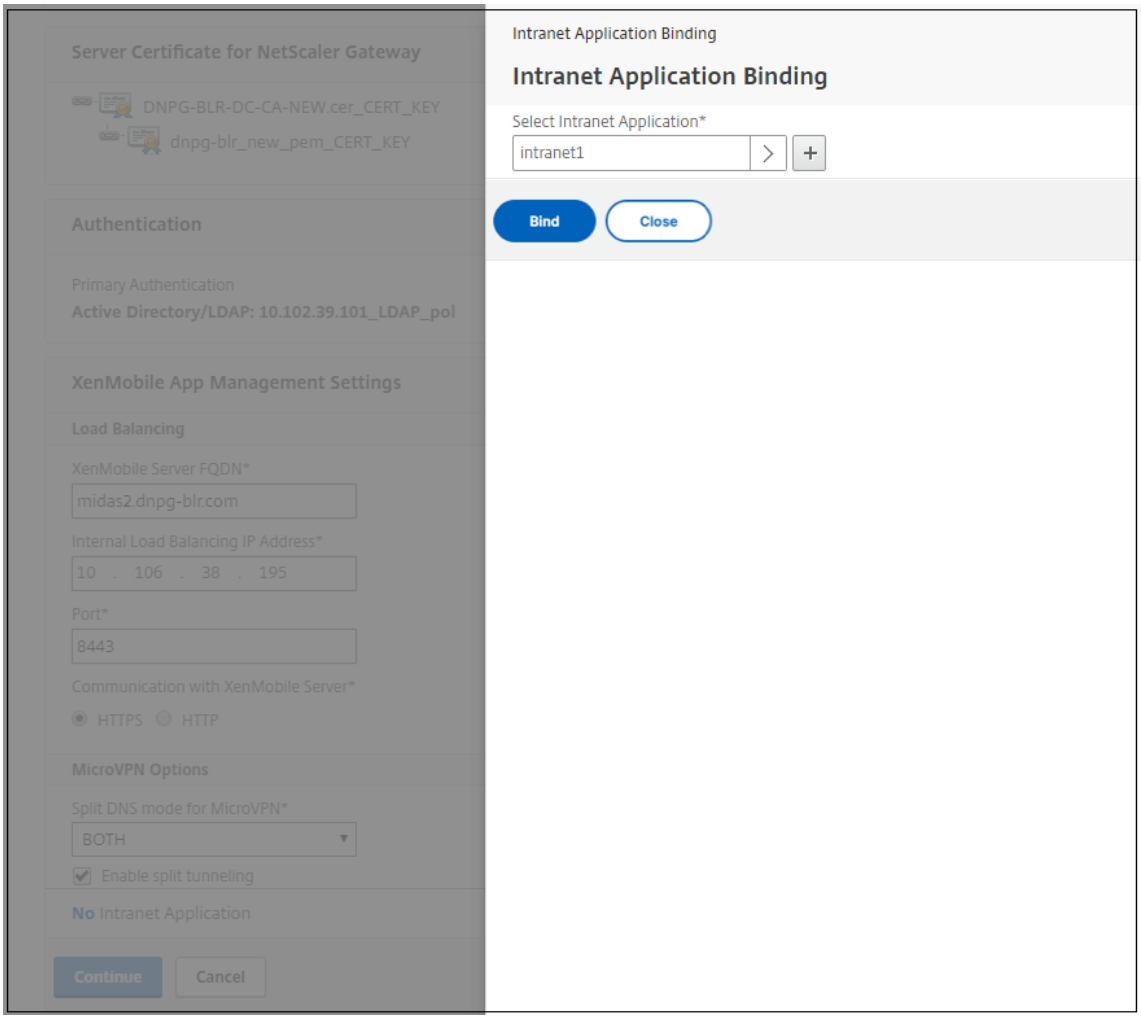
aktivieren.

Standardmäßig wird der sichere Webzugriff auf das interne Netzwerk getunnelt, was bedeutet, dass Secure Web einen anwendungsbezogenen VPN-Tunnel zurück zum internen Netzwerk für den gesamten Netzwerkzugriff verwendet und die NetScaler Appliance Split-Tunneleinstellungen verwendet.

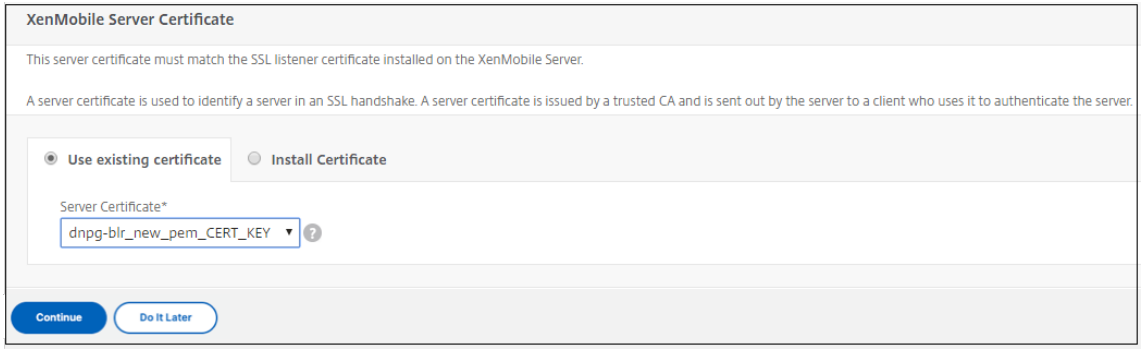



10. Um Abfangregeln für Benutzerverbindungen auf NetScaler Gateway zu konfigurieren, müssen Sie **Intranet-Anwendungsbindung**konfigurieren. Klicken Sie auf **+**, um eine Bindung hinzuzufügen.



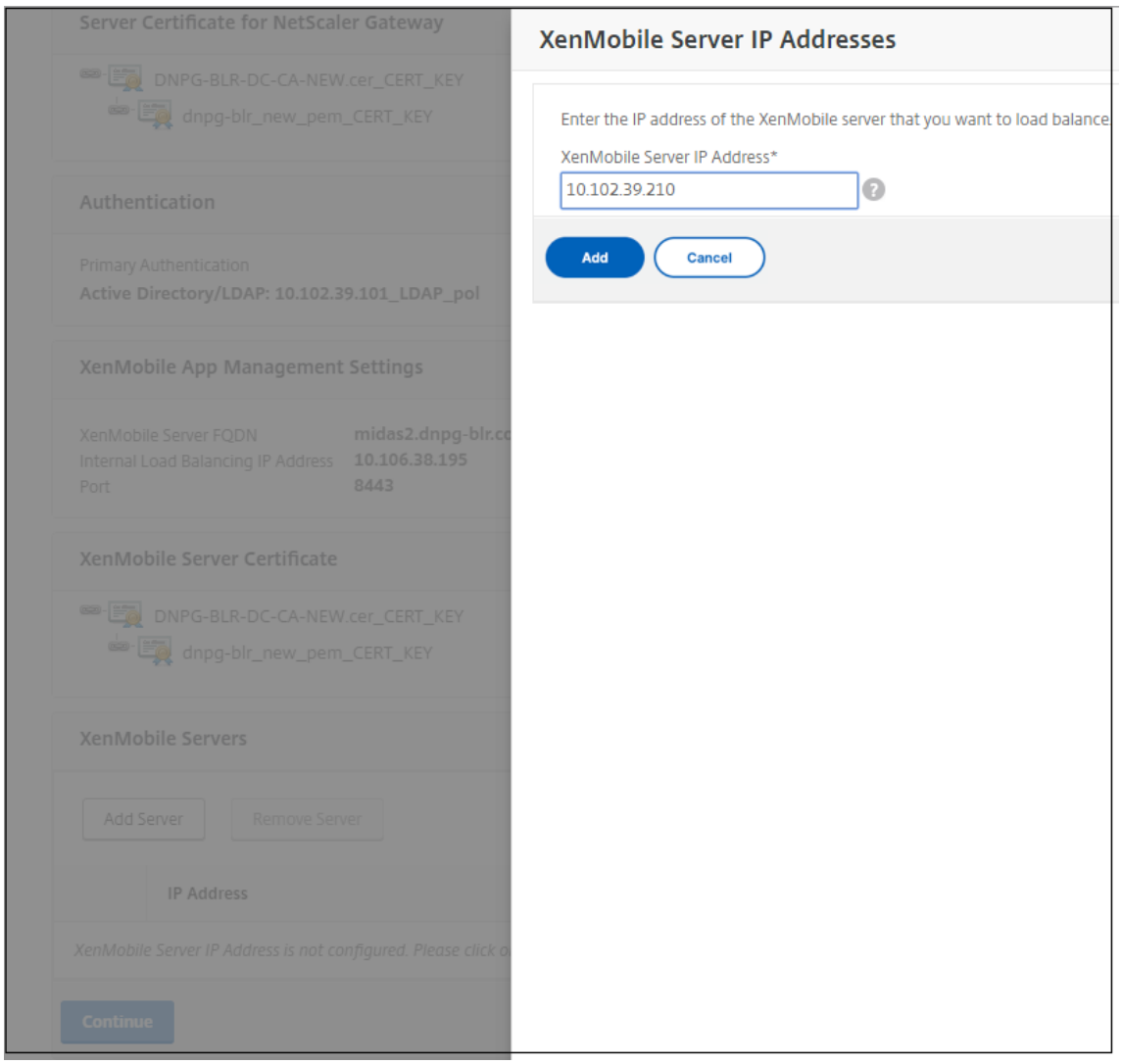

11. Füllen Sie die Parameter für das Zulassen des Netzwerkzugriffs aus und klicken Sie dann auf **Erstellen**.
12. Fügen Sie das Citrix Endpoint Management-Zertifikat hinzu. Dies wird für den virtuellen MAM-Lastausgleichsserver verwendet.




13. Klicken Sie unter **Citrix Endpoint Management**Servers auf **Server hinzufügen**, um die **Citrix Endpoint Management-IP-Adresse**hinzuzufügen, die an die virtuelle IP des Lastausgleichs

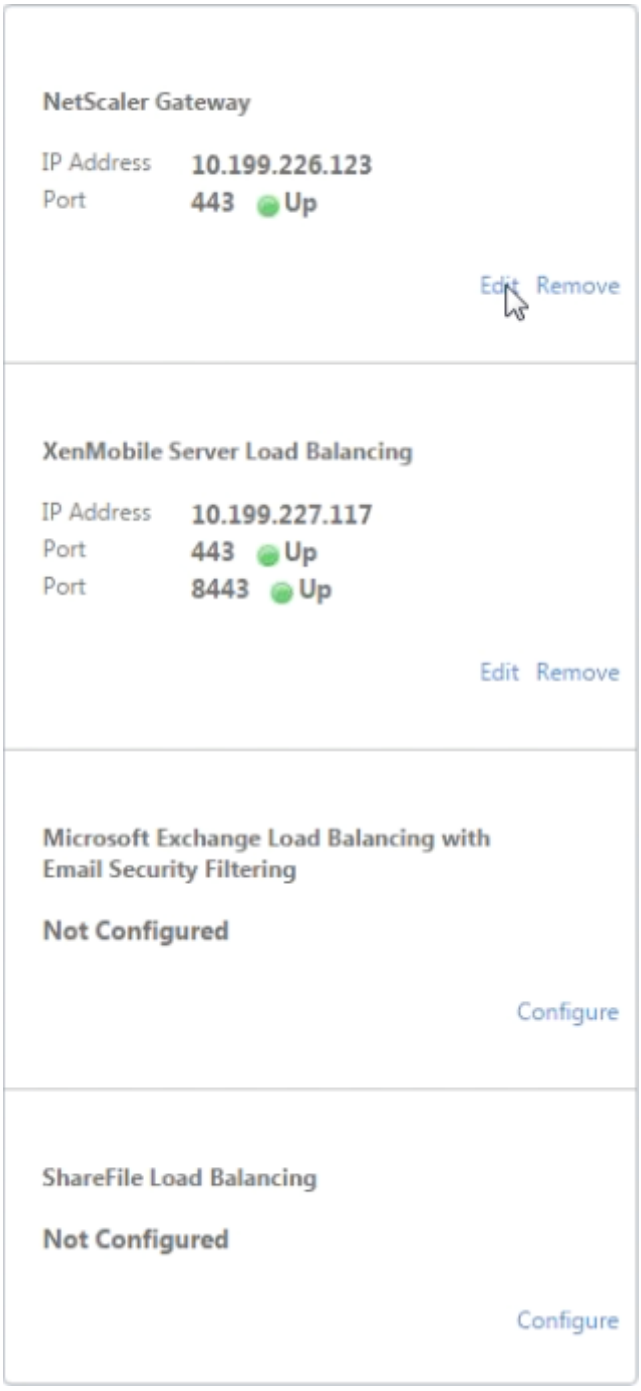
 

gebunden werden soll.




Vergewissern Sie sich im NetScaler-Dashboard, dass NetScaler Gateway und Citrix Endpoint Management-Lastausgleich konfiguriert sind.




Wenn Sie die sAMAccount-Attribute in den Benutzerzertifikaten als Alternative zum Benutzerprinzipalnamen (UPN) verwenden, konfigurieren Sie das Zertifikatprofil wie unter Manuelles Konfigurieren von NetScaler Gateway für die Clientzertifikatauthentifizierung beschrieben.

# Konfigurieren von Lastausgleichsservern für Citrix Endpoint Management oder Citrix XenMobile Server

March 27, 2024

Nachdem Sie den **Citrix ADC für Citrix Endpoint Management-Assistenten** für die Ersteinrichtung verwendet haben, verwenden Sie das Citrix Gateway-Konfigurationsdienstprogramm, um den Lastenausgleich zu konfigurieren, wie in diesem Abschnitt beschrieben. Verwenden Sie für Citrix Endpoint Management SSL Offload. Beachten Sie für Citrix Endpoint Management Server unbedingt die Empfehlungen für Lastausgleichsmodi unter "Deployment Summary"in Integration mit Citrix Gateway und Citrix ADC.

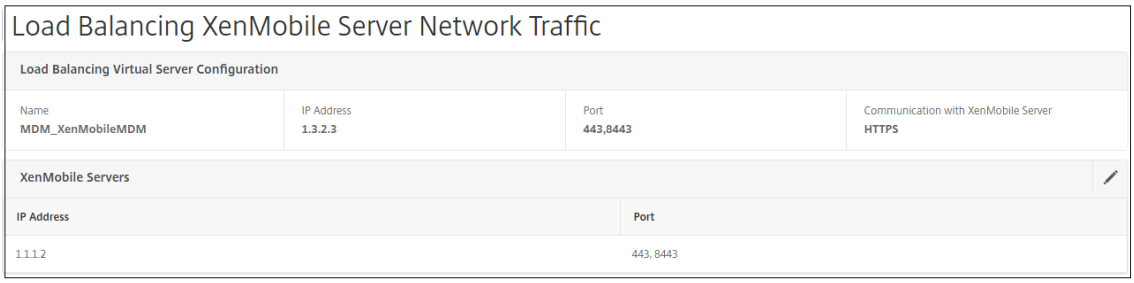
## So verwenden Sie den SSL-Bridge-Modus für Citrix ADC VIPs

Verwenden Sie den SSL Bridge-Modus, wenn sich Citrix Endpoint Management in der DMZ befindet. Wenn Sie Citrix Endpoint Management mit Citrix ADC VIPs im SSL Bridge-Modus laden, fließt der Internetverkehr direkt zum Citrix Endpoint Management-Server, wo Verbindungen beendet werden. Der SSL-Brückenmodus ist im Hinblick auf Einrichtung und Problembehandlung am einfachsten.

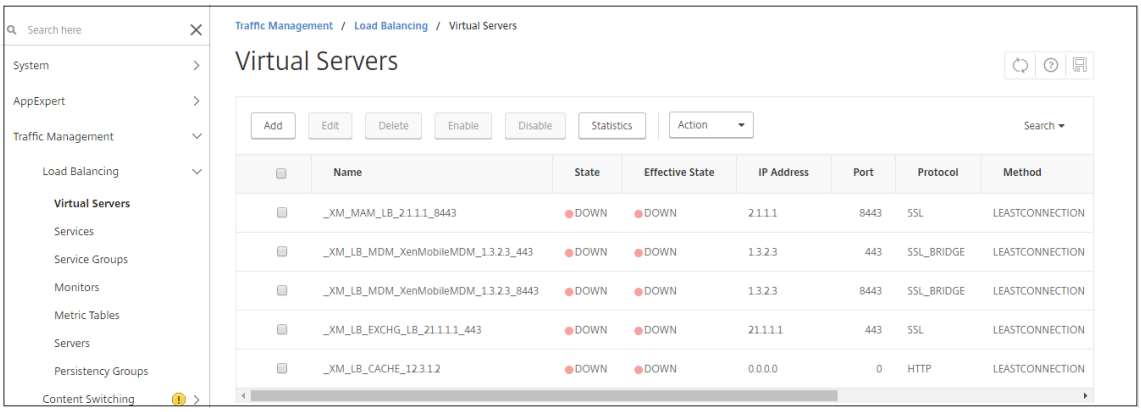
1. Gehen Sie vor dem Konfigurieren des SSL Bridge-Modus zu **Citrix Endpoint Management App Management-Einstellungen** und vergewissern Sie sich, dass für **Kommunikation mit Citrix Endpoint Management Server** die Option **HTTPS** ist.


2. Nachdem Sie sich beim Konfigurationsdienstprogramm angemeldet haben, klicken Sie auf der Registerkarte **Start** in **MDM Server LB**auf **Konfigurieren**.
3. Geben Sie unter **LB Virtual Server for Device Management**in das Feld **Name** einen Namen für den Server ein.
4. Geben Sie unter **IP-Adresse**die IP-Adresse für den virtuellen Server ein und klicken Sie dann auf **Weiter**.
5. Wiederholen Sie auf der Seite **Load Balance Citrix Endpoint Management MDM Servers** die Schritte 3 und 4, und klicken Sie dann auf **Erstellen**.
6. Stellen Sie sicher, dass die Einstellungen korrekt sind, und klicken Sie dann auf **Fertig**.




7. Um die Konfiguration des Lastenausgleichs zu überprüfen, gehen Sie zu **Traffic Management > Virtuelle Server**.




## Verwenden des SSL-Offload-Modus für Citrix ADC-VIPs

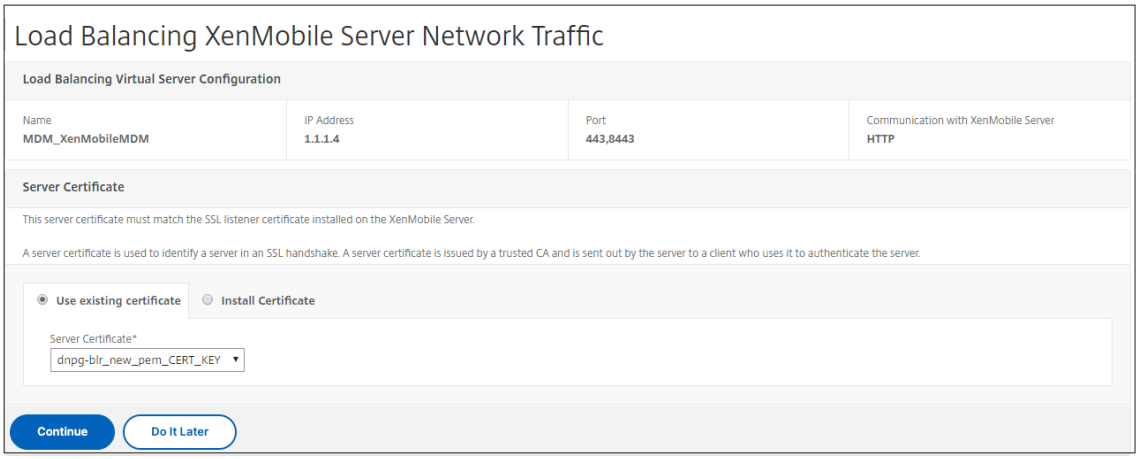
Verwenden Sie SSL-Offload für Citrix Endpoint Management. Verwenden Sie bei Bedarf auch SSL-Offload, um Sicherheitsstandards zu erfüllen, wenn sich das on-premises Citrix Endpoint Management im internen Netzwerk befindet. Wenn Sie Citrix Endpoint Management mit Citrix ADC VIPs im SSL-Offload-Modus laden, fließt der Internetverkehr direkt zur Citrix ADC Appliance, wo Verbindungen beendet werden. Citrix Gateway richtet dann neue Sitzungen von der Appliance zu Citrix Endpoint Management ein. Der SSL-Offload-Modus beinhaltet mehr Komplexität bei der Einrichtung und Fehlerbehebung.

1. Gehen Sie vor dem Konfigurieren des SSL-Offload-Modus zu **Citrix Endpoint Management App Management-Einstellungen** und vergewissern Sie sich, dass die **Kommunikation mit Citrix Endpoint Management ServerHTTP**ist.

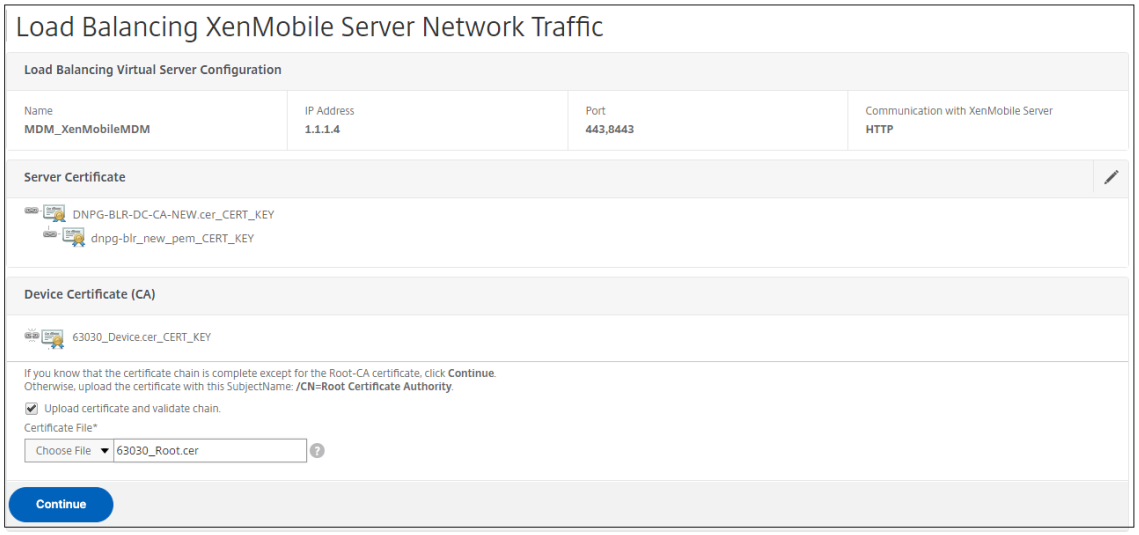

2. Melden Sie sich beim Konfigurationsdienstprogramm an. Klicken Sie auf der Registerkarte **Start** in **MDM Server LB**auf **Konfigurieren**.

3. Geben Sie unter **LB Virtual Server for Device Management**in das Feld **Name** einen Namen für den Server ein.
4. Geben Sie unter **IP-Adresse**die IP-Adresse für den virtuellen Server ein und klicken Sie dann auf **Weiter**.
5. Wiederholen Sie auf der Seite **Load Balance Citrix Endpoint Management MDM Servers** die Schritte 3 und 4, und klicken Sie dann auf **Erstellen**.
6. Überprüfen Sie die Einstellungen und klicken Sie dann auf **Fertig**.
7. Wenn Sie aufgefordert werden, ein Serverzertifikat hinzuzufügen, wählen Sie das Serverzertifikat aus und klicken Sie auf **Weiter**.

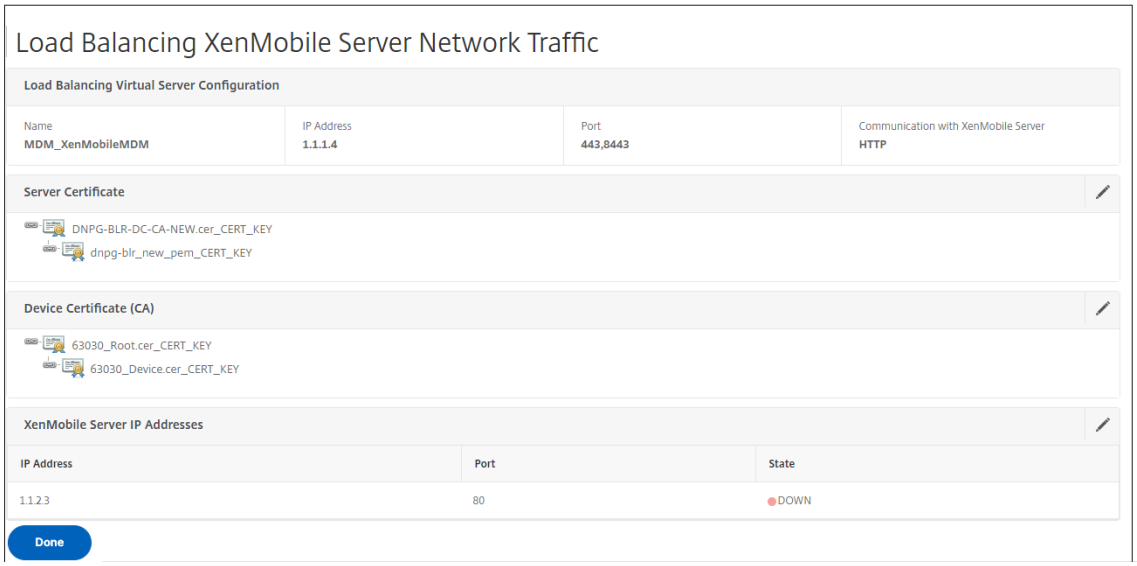



8. Geben Sie das CA-Zertifikat an und klicken Sie auf **Weiter**.

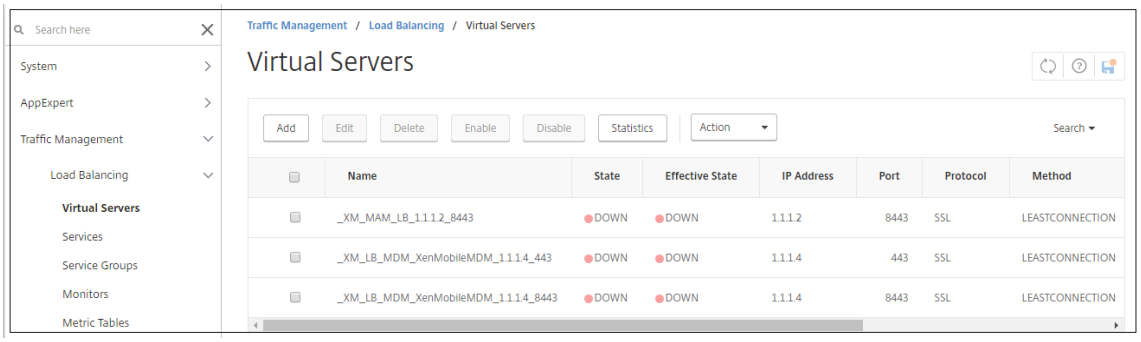



9. Behalten Sie dieselbe Citrix Endpoint Management-IP-Adresse bei. Klicken Sie auf **Fertig**.




10. Um die Konfiguration des Lastenausgleichs zu überprüfen, gehen Sie zu **Traffic Management > Virtuelle Server**.



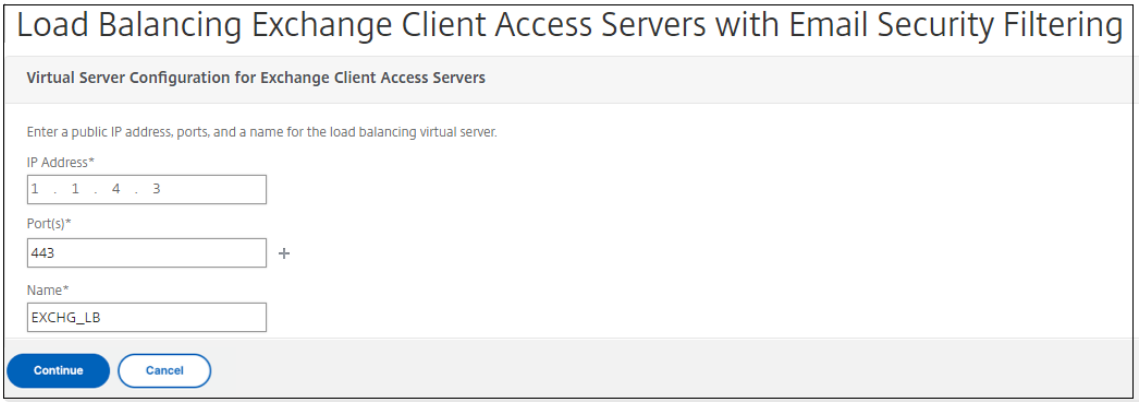

## Lastausgleichsserver für Microsoft Exchange mit Email Security-Filterung konfigurieren

March 27, 2024

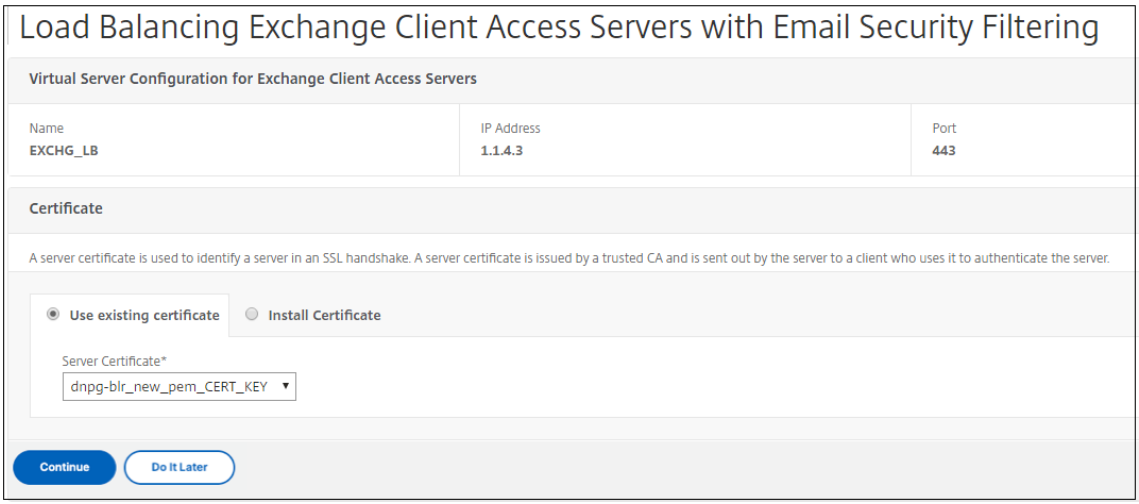
1. Klicken Sie auf der Registerkarte **Start** in **MDM Server LB**auf **Konfigurieren**.
2. Geben Sie unter **LB Virtual Server for Exchange CAS**unter **Name**einen Namen für den Server ein.
3. Geben Sie unter **IP-Adresse**die IP-Adresse für den virtuellen Server ein.
4. Geben Sie unter **Port**die Portnummer ein. Um weitere Ports hinzuzufügen, klicken Sie auf das Pluszeichen (**+**) und geben Sie dann die Portnummer ein.

5. Klicken Sie auf **Weiter**.

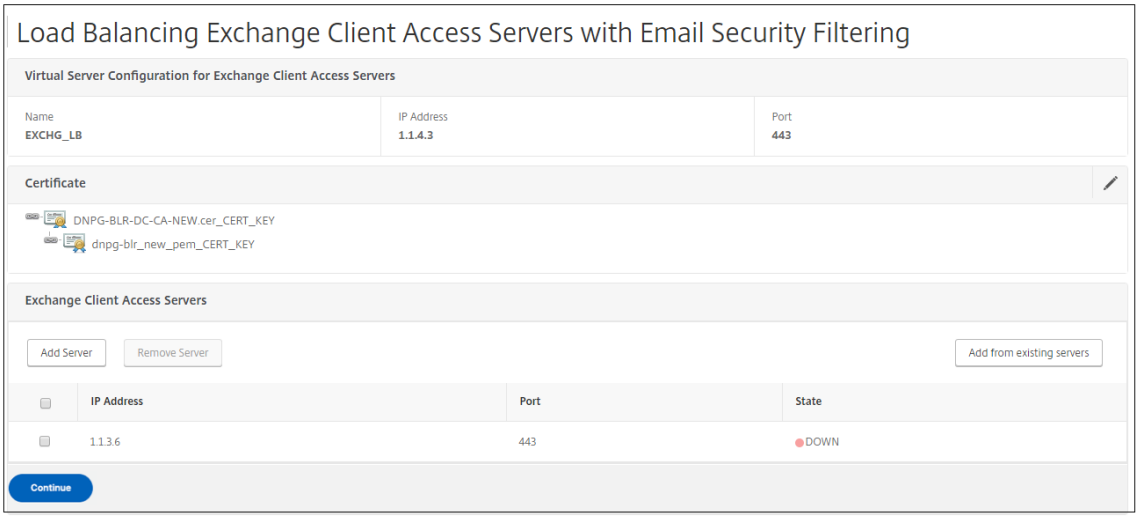



6. Wählen Sie unter **Zertifikate**entweder ein vorhandenes Zertifikat aus oder installieren Sie eines auf Ihrem Computer (**lokal**) oder auf der Citrix ADC Appliance (**Appliance**).
7. Klicken Sie auf **Weiter**.




8. Geben Sie unter **Exchange CAS-Dienstinstanzen**einen Namen, eine IP-Adresse und eine Portnummer für den virtuellen Server ein. Klicken Sie dann auf **Hinzufügen** und **Fortfahren**.




Wenn Sie auf **Fertig klicken, werden**die Felder zum Konfigurieren des Citrix Endpoint Management Citrix ADC Connector (XNC) ActiveSync-Filters angezeigt.

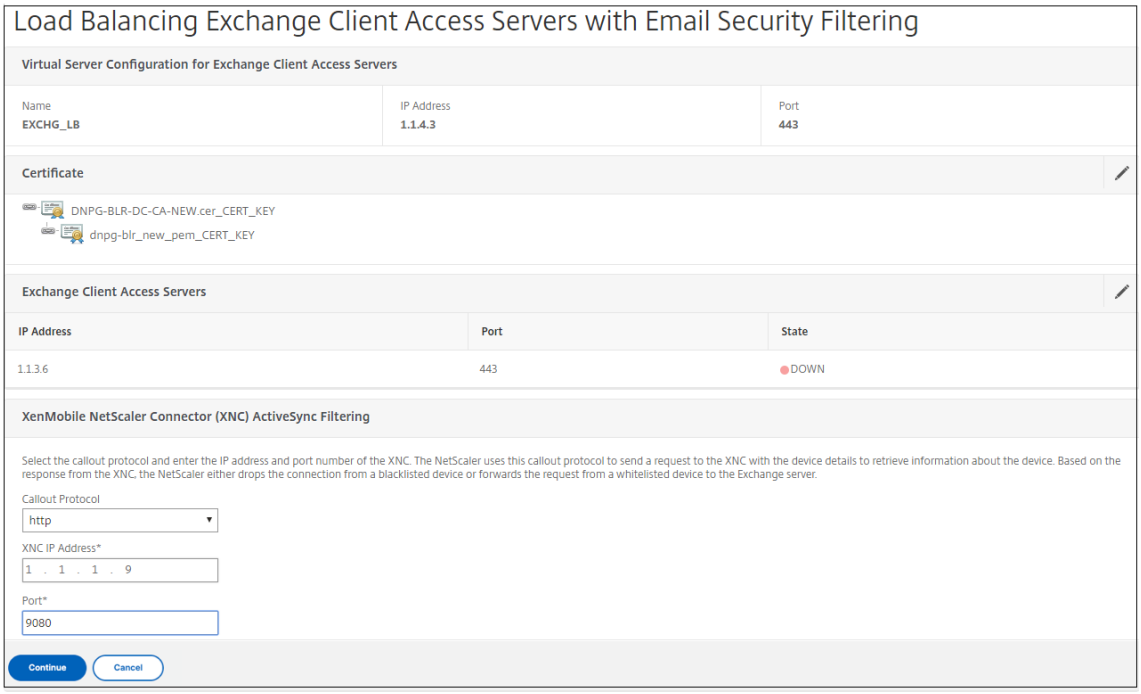
## Konfigurieren der Citrix Endpoint Management Citrix ADC Connector (XNC) ActiveSync-Filterung

March 27, 2024

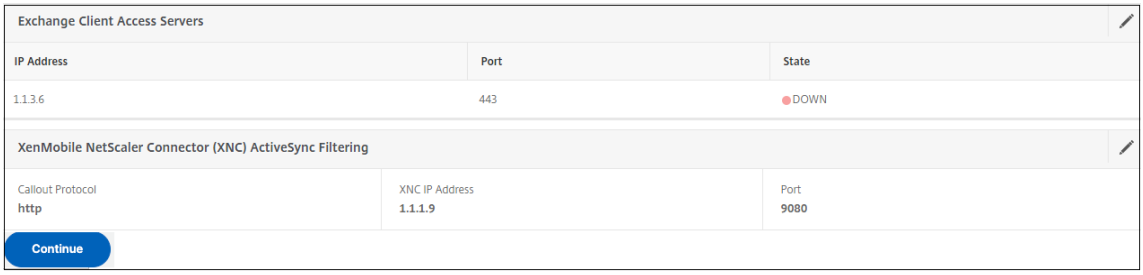
Der Citrix Endpoint Management Citrix ADC Connector (XNC) bietet Citrix ADC einen Autorisierungsdienst auf Geräteebene für ActiveSync-Clients, der als Reverseproxy für das Exchange ActiveSync-Protokoll fungiert. Die Kombination aus in Citrix Endpoint Management definierten Richtlinien und lokal von der XNC definierten Regeln steuert die Autorisierung.

1. Wählen Sie unter **Citrix Endpoint Management Citrix ADC Connector (XNC) ActiveSync-Filterung**für **Callout Protocolhttp**oder**https**aus.
2. Geben Sie unter **XNC-IP-Adresse**die IP-Adresse des Citrix Endpoint Management Citrix ADC Connectors ein.
3. Geben Sie unter **Port9080**für den HTTP-Netzwerkverkehr oder**9443**für HTTPS-Netzwerkverkehr ein, und klicken Sie dann auf**Weiter**.




Ihre Konfiguration wird angezeigt.




## Erlauben Sie den Zugriff von Mobilgeräten mit Citrix Mobile Productivity Apps

March 27, 2024

Der Citrix ADC für XenMobile-Assistent konfiguriert die Einstellungen, die erforderlich sind, damit Benutzer von unterstützten Geräten über Citrix Gateway eine Verbindung zu mobilen Apps und Ressourcen im internen Netzwerk herstellen können. Benutzer verbinden sich mithilfe von Secure Hub (zuvor Citrix Secure Hub), das einen Micro-VPN-Tunnel einrichtet. Wenn Benutzer eine Verbindung herstellen, öffnet sich ein VPN-Tunnel zu Citrix Gateway und wird dann im internen Netzwerk an XenMobile weitergeleitet. Benutzer können dann von XenMobile aus auf ihre Web-, Mobil- und SaaS-Apps zugreifen.

Um sicherzustellen, dass Benutzer eine einzige Universal-Lizenz verbrauchen, wenn sie mit mehreren Geräten gleichzeitig eine Verbindung zu Citrix Gateway herstellen, können Sie die Sitzungsübertragung auf dem virtuellen Server aktivieren. Einzelheiten finden Sie unter Konfigurieren von Verbindungstypen auf dem virtuellen Server.

Wenn Sie Ihre Konfiguration ändern müssen, nachdem Sie den Citrix ADC für XenMobile-Assistenten verwendet haben, verwenden Sie die Abschnitte in diesem Artikel als Anleitung. Stellen Sie vor dem Ändern der Einstellungen sicher, dass Sie die Auswirkungen Ihrer Änderungen verstehen. Weitere Informationen finden Sie in den Artikeln zur XenMobile-Bereitstellung.

### Konfigurieren von Secure Browse in Citrix Gateway

Sie können Secure Browse als Teil globaler Einstellungen oder als Teil eines Sitzungsprofils ändern. Sie können die Sitzungsrichtlinie an Benutzer, Gruppen oder virtuelle Server binden. Wenn Sie Secure Browse konfigurieren, müssen Sie auch den clientlosen Zugriff aktivieren. Für den clientlosen Zugriff müssen Sie jedoch nicht Secure Browse aktivieren. Wenn Sie den clientlosen Zugriff konfigurieren, legen Sie die **URL-Kodierung für den clientlosen Zugriff aufClear**fest.

So konfigurieren Sie Secure Browse global:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Klicken Sie im Dialogfeld **Globale Citrix Gateway-Einstellungen** auf der Registerkarte **Sicherheit** auf **Secure Browse** und dann auf **OK**.

So konfigurieren Sie Secure Browse in einer Sitzungsrichtlinie und einem Profil:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Wenn Sie eine neue Sitzungsrichtlinie erstellen, klicken Sie auf **Hinzufügen**.
   - Wenn Sie eine bestehende Richtlinie ändern, wählen Sie eine Richtlinie aus und klicken Sie dann auf **Öffnen**.
3. Erstellen Sie in der Richtlinie ein Profil oder ändern Sie ein vorhandenes Profil. Führen Sie dazu einen der folgenden Schritte aus:
   - Klicken Sie neben **Profil anfordern**auf **Neu**.
   - Klicken Sie neben **Profil anfordern** auf **Ändern**.
4. Klicken Sie auf der Registerkarte **Sicherheit** neben **Secure Browse**auf **Override Global** und wählen Sie dann **Secure Browse**aus.

5. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie ein neues Profil erstellen, klicken Sie auf **Erstellen**, legen Sie den Ausdruck im Richtliniendialogfeld fest, klicken Sie auf **Erstellen** und dann auf **Schließen**.
   - Wenn Sie ein vorhandenes Profil ändern, klicken Sie nach der Auswahl zweimal auf **OK**.

So konfigurieren Sie Verkehrsrichtlinien für Secure Web im Secure Browse-Modus:

Verwenden Sie die folgenden Schritte, um Verkehrsrichtlinien für die Weiterleitung von Secure Web Webverkehr über einen Proxyserver im Secure Browse-Modus zu konfigurieren.

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte **KonfigurationCitrix Gateway > Richtlinien**, und klicken Sie dann auf**Verkehr**.
2. Klicken Sie im rechten Bereich auf die Registerkarte **Verkehrsprofile** und dann auf **Hinzufügen**.
3. Geben Sie **unter Name**einen Namen für das Profil ein, wählen Sie **TCP** als **Protokoll**aus und lassen Sie den Rest der Einstellungen unverändert.
4. Klicken Sie auf **Erstellen**.
5. Klicken Sie auf die Registerkarte **Verkehrsprofile** und dann auf **Hinzufügen**.
6. Geben Sie **unter Name**einen Namen für das Profil ein und wählen Sie dann **HTTP** als **Protokoll**aus.
   Dieses Verkehrsprofil ist sowohl für HTTP als auch für SSL. Clientloser VPN-Verkehr ist vom Design her HTTP-Verkehr, unabhängig vom Zielport oder Diensttyp. Daher geben Sie sowohl SSL- als auch HTTP-Verkehr als **HTTP** im Verkehrsprofil an.
7. Geben Sie unter **Proxy**die IP-Adresse des Proxyservers ein. Geben Sie unter **Port**die Portnummer des Proxyservers ein.
8. Klicken Sie auf **Erstellen**.
9. Klicken Sie auf die Registerkarte **Verkehrsrichtlinien** und dann auf **Hinzufügen**.
10. Geben Sie den **Namen** der Verkehrsrichtlinie ein und wählen Sie für **Profil anfordern**das Verkehrsprofil aus, das Sie in Schritt 3 erstellt haben. Geben Sie den folgenden **Ausdruck** ein und klicken Sie dann auf **Erstellen**:

```
1 REQ.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER
     User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent
     CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS
     Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.
     HTTP.URL CONTAINS StoreWeb
2 <!--NeedCopy-->
```

    Diese Regel führt eine Überprüfung basierend auf dem Host-Header durch. Um den aktiven Sync-Verkehr vom Proxy zu umgehen, ersetzen Sie **`ActiveSyncServer`** durch den entsprechenden Active-Sync-Servernamen.

11. Klicken Sie auf die Registerkarte **Verkehrsrichtlinien** und dann auf **Hinzufügen**. Geben Sie den **Namen** der Verkehrsrichtlinie ein und wählen Sie für **Profil anfordern**das in Schritt 6 erstellte Verkehrsprofil aus. Geben Sie den folgenden **Ausdruck** ein und klicken Sie dann auf **Erstellen**:

| | |
|---|---|
| (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla | REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser |

12. Klicken Sie auf die Registerkarte **Verkehrsrichtlinien** und dann auf **Hinzufügen**. Geben Sie den **Namen** der Verkehrsrichtlinie ein und wählen Sie für **Profil anfordern**das in Schritt 6 erstellte Verkehrsprofil aus. Geben Sie den folgenden **Ausdruck** ein und klicken Sie dann auf **Erstellen**:

| | |
|---|---|
| (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla | REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser |

13. Navigieren Sie zu **Citrix Gateway > Virtuelle Server**, wählen Sie den virtuellen Server im rechten Bereich aus und klicken Sie dann auf **Bearbeiten**.
14. Klicken Sie in der Zeile **Richtlinien** auf **+**.
15. Wählen Sie im Menü **Richtlinie wählen** die Option **Traffic**aus.
16. Klicken Sie auf **Weiter**.
17. Klicken Sie unter **Policy Binding**gegenüber von **Richtlinie auswählen**auf **>**.
18. Wählen Sie die Richtlinie aus, die Sie in Schritt 10 erstellt haben, und klicken Sie dann auf **OK**.
19. Klicken Sie auf **Bind**.
20. Klicken Sie unter **Richtlinien**auf **Traffic Policy**.
21. Klicken Sie unter **VPN Virtual Server Traffic Policy Binding**auf **Bindung hinzufügen**
22. Klicken Sie unter **Richtlinienbindung**neben dem Menü **Richtlinie auswählen** auf **>**, um die Richtlinienliste anzuzeigen.
23. Wählen Sie die Richtlinie aus, die Sie in Schritt 11 erstellt haben, und klicken Sie dann auf **OK**.
24. Klicken Sie auf **Bind**.
25. Klicken Sie unter **Richtlinien**auf **Verkehrsrichtlinien**.
26. Klicken Sie unter **VPN Virtual Server Traffic Policy Binding**auf **Bindung hinzufügen**
27. Klicken Sie unter **Richtlinienbindung**neben dem Menü **Richtlinie auswählen** auf **>**, um die Richtlinienliste anzuzeigen.
28. Wählen Sie die Richtlinie aus, die Sie in Schritt 12 erstellt haben, und klicken Sie dann auf **OK**.

29. Klicken Sie auf **Bind**.
30. Klicken Sie auf **Schließen**.
31. Klicken Sie auf **Fertig**.

Konfigurieren Sie die Secure Web (WorxWeb) -App unbedingt in der XenMobile-Konsole. Gehen **Sie zu Konfigurieren > Apps**, wählen Sie die Secure Web App aus, klicken Sie auf **Bearbeiten**und nehmen Sie dann die folgenden Änderungen vor:

- Ändern Sie auf der **App-Informationsseite** den **ursprünglichen VPN-Modus** in **Secure Browse**.
- Ändern Sie auf der **iOS-Seite** den **anfänglichen VPN-Modus** in **Secure Browse**.
- Ändern Sie auf der **Android-Seite** den **bevorzugten VPN-Modus** in **Secure Browse**.

### Konfigurieren von Timeouts für Anwendungen und MDX-Token

Wenn sich Benutzer von einem iOS- oder Android-Gerät aus anmelden, wird ein Anwendungstoken oder ein MDX-Token ausgegeben. Das Token ähnelt der Secure Ticket Authority (STA).

Sie können die Anzahl der Sekunden oder Minuten festlegen, für die die Token aktiv sind. Wenn das Token abläuft, können Benutzer nicht auf die angeforderte Ressource zugreifen, z. B. auf eine Anwendung oder eine Webseite.

Token-Time-Outs sind globale Einstellungen. Wenn Sie die Einstellung konfigurieren, gilt sie für alle Benutzer, die sich bei Citrix Gateway anmelden.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Klicken Sie im Dialogfeld **Globale Citrix Gateway-Einstellungen** auf der Registerkarte **Client Experience** auf **Erweiterte Einstellungen**.
4. Geben Sie auf der Registerkarte **Allgemein** in **Application Token Timeout (Sek.)** die Anzahl der Sekunden ein, bevor das Token abläuft. Der Standardwert beträgt **100** Sekunden.
5. Geben Sie in **MDX Token Timeout (Minuten)**die Anzahl der Minuten ein, bevor das Token abläuft, und klicken Sie dann auf **OK**. Die Standardeinstellung beträgt **10** Minuten.

### Deaktivieren Sie Endpoint Analysis für mobile Geräte

Wenn Sie Endpoint Analysis konfigurieren, müssen Sie die Richtlinienausdrücke so konfigurieren, dass die Endpoint Analysis-Scans nicht auf Android- oder iOS-Mobilgeräten ausgeführt werden. Endpoint Analysis-Scans werden auf Mobilgeräten nicht unterstützt.

Wenn Sie eine Endpoint Analysis-Richtlinie an einen virtuellen Server binden, müssen Sie einen sekundären virtuellen Server für mobile Geräte erstellen. Binden Sie keine Vorauthentifizierungs- oder Nachauthentifizierungsrichtlinien an den virtuellen Server des Mobilgeräts.

Wenn Sie den Richtlinienausdruck in einer Vorauthentifizierungsrichtlinie konfigurieren, fügen Sie die User-Agent-Zeichenfolge hinzu, um Android oder iOS auszuschließen. Wenn sich Benutzer von einem dieser Geräte aus anmelden und Sie den Gerätetyp ausschließen, wird die Endpunktanalyse nicht ausgeführt.

Beispielsweise erstellen Sie den folgenden Richtlinienausdruck, um zu überprüfen, ob der User-Agent Android enthält, ob die Anwendung virus.exe nicht existiert, und um den Prozess keylogger.exe zu beenden, wenn er mithilfe des Vorauthentifizierungsprofils ausgeführt wird. Der Richtlinienausdruck könnte so aussehen:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS Android &&
CLIENT.APPLICATION.PROCESS(keylogger.exe) contains
```

Nachdem Sie die Vorauthentifizierungsrichtlinie und das Profil erstellt haben, binden Sie die Richtlinie an den virtuellen Server. Wenn sich Benutzer von einem Android- oder iOS-Gerät aus anmelden, wird der Scan nicht ausgeführt. Wenn sich Benutzer von einem Windows-basierten Gerät aus anmelden, wird der Scan ausgeführt.

Weitere Informationen zum Konfigurieren von Vorauthentifizierungsrichtlinien finden Sie unter Konfigurieren von Endpunktrichtlinien.

### Unterstützt DNS-Abfragen mithilfe von DNS-Suffixen für Android-Geräte

Wenn Benutzer eine Micro-VPN-Verbindung von einem Android-Gerät aus herstellen, sendet Citrix Gateway geteilte DNS-Einstellungen an das Benutzergerät. Citrix Gateway unterstützt geteilte DNS-Abfragen basierend auf den von Ihnen konfigurierten geteilten DNS-Einstellungen. Citrix Gateway kann auch geteilte DNS-Abfragen basierend auf DNS-Suffixen unterstützen, die Sie auf der Appliance konfigurieren. Wenn Benutzer von einem Android-Gerät aus eine Verbindung herstellen, müssen Sie DNS-Einstellungen auf Citrix Gateway konfigurieren.

Split DNS funktioniert auf folgende Weise:

- Wenn Sie Split-DNS auf "**Lokal**"setzen, sendet das Android-Gerät alle DNS-Anfragen an den lokalen DNS-Server.
- Wenn Sie geteiltes DNS auf **Remote**festlegen, werden alle DNS-Anforderungen zur Auflösung an die auf Citrix Gateway (Remote-DNS-Server) konfigurierten DNS-Server gesendet.
- Wenn Sie Split-DNS auf **Beide**festlegen, sucht das Android-Gerät nach dem DNS-Anforderungstyp.

- Wenn der DNS-Anforderungstyp nicht “A”ist, sendet er das DNS-Anforderungspaket sowohl an lokale als auch an Remote-DNS-Server.
- Wenn der DNS-Anforderungstyp “A”ist, extrahiert das Android-Plug-In den Abfrage-FQDN und vergleicht diesen FQDN mit der DNS-Suffixliste, die auf der Citrix ADC Appliance konfiguriert ist. Wenn der FQDN der DNS-Anforderung übereinstimmt, wird die DNS-Anforderung an den Remote-DNS-Server gesendet. Wenn der FQDN nicht übereinstimmt, wird die DNS-Anforderung an lokale DNS-Server gesendet.

In der folgenden Tabelle werden geteilte DNS-Arbeiten basierend auf dem Datensatz vom Typ A und der Suffix-Liste zusammengefasst.

| Geteilte DNS-Einstellung | Typ A-Datensatz? | Auf der Suffix-Liste? | Wohin die DNS-Anfrage gesendet wird |
|---|---|---|---|
| Lokal | beide Ja oder Nein | beide Ja oder Nein | Lokal |
| Remote | beide Ja oder Nein | beide Ja oder Nein | Remote |
| Beide | Nein | Nicht verfügbar | Beide |
| Beide | Ja | Ja | Remote |
| Beide | Ja | Nein | Lokal |

So konfigurieren Sie ein DNS-Suffix:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Wählen Sie im Detailbereich auf der Registerkarte **Richtlinien** eine Sitzungsrichtlinie aus und klicken Sie dann auf **Öffnen**.
3. Klicken Sie neben **Profil anfordern** auf **Ändern**.
4. Klicken Sie auf der Registerkarte **Netzwerkkonfiguration** auf **Erweitert**.
5. Klicken Sie neben **Intranet-IP-DNS-Suffix** auf **Override Global**, geben Sie das DNS-Suffix ein und klicken Sie dann dreimal auf **OK**.

So konfigurieren Sie geteiltes DNS global auf Citrix Gateway:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte „ **Kundenerlebnis** “auf **Erweiterte Einstellungen**.
4. Wählen Sie auf der Registerkarte **Allgemein** in **Split DNSBeide**,**Remote**oder**Lokal**aus und klicken Sie dann auf**OK**.

So konfigurieren Sie geteiltes DNS in einer Sitzungsrichtlinie auf Citrix Gateway:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway > Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Hinzufügen**.
3. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
4. Klicken Sie neben **Profil anfordern**auf **Neu**.
5. **Geben Sie im Feld Name einen Namen für das Profil ein.**
6. Klicken Sie auf der Registerkarte „ **Kundenerlebnis** “auf **Erweiterte Einstellungen**.
7. Klicken Sie auf der Registerkarte **Allgemein** neben **Split DNS**auf **Global überschreiben**, wählen Sie **Beide**, **Remote**oder **Lokal** aus und klicken Sie dann auf **OK**.
8. Wählen **Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben **Benannte Ausdrücke**die Option **Allgemein**aus, wählen Sie **True**aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen** und dann auf **Schließen**.

## Domänen- und Sicherheitstoken-Authentifizierung für Citrix Endpoint Management konfigurieren

March 27, 2024

Sie können Citrix Endpoint Management konfigurieren, sodass Benutzer sich mit ihren LDAP-Anmeldeinformationen und einem Einmalkennwort authentifizieren müssen. Dabei wird das RADIUS-Protokoll verwendet. Dieser Abschnitt beschreibt die erforderliche NetScaler Gateway-Konfiguration für diesen Zwei-Faktor-Authentifizierungstyp.

### Voraussetzungen

Wenn Sie den NetScaler für Citrix Endpoint Management-Assistenten noch nicht ausgeführt haben, lesen Sie den Abschnitt *NetScaler für Citrix Endpoint Management-Assistenten* unter Konfigurieren von Einstellungen für Ihre Citrix Endpoint Management-Umgebung. Stellen Sie sicher, dass Ihre NetScaler-Konfiguration Folgendes enthält:

- **LDAP-Portnummer** = **636** (was der Standardport für sichere LDAP-Verbindungen ist)
- **Server-Anmeldename Attribut** = **samAccountName** oder der **userPrincipalName** gemäß Ihren Anforderungen

### So konfigurieren Sie die Domänen- und Sicherheitstoken-Authentifizierung

1. Wechseln Sie zu **NetScaler Gateway > Virtuelle Server**. Wählen Sie den virtuellen Server aus und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie auf **Kein CA-Zertifikat.**
3. Wählen Sie unter **CA-Zertifikat auswählen** ein Zertifikat aus, klicken Sie auf **OK**, klicken Sie auf **Binden** und dann auf **Fertig**.
4. Gehen Sie zu **Richtlinien > Sitzung > Sitzungsprofile**, wählen Sie das Profil aus und klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf den Tab „ **Kundenerlebnis** “.
6. Wählen Sie unter **Credential Index** die Option **SECONDARY** aus.
7. Klicken Sie auf **OK**.
8. Wechseln Sie zu **Richtlinien > Authentifizierung > LDAP**, klicken Sie auf die Registerkarte **LDAP-Richtlinie** und dann auf **Bearbeiten**.
9. Verwenden Sie den folgenden Ausdruck, um separate NetScaler Gateway-VIPs für Citrix Endpoint Management und Citrix Virtual Apps and Desktops zu verwenden.

   REQ.HTTP.HEADER User-Agent CONTAINS `CitrixReceiver`
10. Wechseln Sie zu **Richtlinien > Authentifizierung > RADIUS** und klicken Sie dann auf die Registerkarte **Server**.
11. Klicken Sie auf **Hinzufügen**, geben Sie die Details des RADIUS-Servers ein und klicken Sie auf **Erstellen**.
12. Gehen Sie zu **Richtlinien** und klicken Sie dann auf **Hinzufügen**.
13. Geben Sie einen **Namen** für die Richtlinie ein. Wählen Sie im Dropdownmenü **Server** den RADIUS-Servernamen aus, den Sie erstellt haben.
14. Geben Sie im Feld **Ausdruck** Folgendes ein: **REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver**. Klicken Sie dann auf **Erstellen**.
15. Wählen Sie den virtuellen Server aus und klicken Sie dann auf **Bearbeiten**.
16. Klicken Sie unter **Primäre Authentifizierung**auf **LDAP-Richtlinie**.
17. Wählen Sie die Richtlinie aus, klicken Sie auf **Bindung aufheben**und dann auf **Schließen**.
18. Klicken Sie in der Zeile **Authentifizierung** auf **+**, um die RADIUS-Authentifizierung hinzuzufügen.
19. Wählen Sie unter **Typ wählen** unter **Richtlinie wählen** die Option **RADIUS** aus.
20. Klicken Sie auf **Bind**.

21. Wählen Sie die RADIUS-Authentifizierungsrichtlinie aus, die Sie zuvor erstellt haben, und klicken Sie dann auf **Einfügen**.
22. Klicken Sie auf **OK**.
23. Um LDAP als sekundäre Authentifizierungsrichtlinie hinzuzufügen: Klicken Sie in der Zeile **Authentifizierung** auf **+**.
24. Wählen Sie unter **Richtlinie auswählen** die Option **LDAP**.
25. Wählen Sie unter **Typ wählen** die Option **Sekundär**.
26. Wählen Sie unter **Richtlinie auswählen** die LDAP-Richtlinie aus.
27. Wählen Sie die Richtlinie aus und klicken Sie dann auf **OK**.
28. Klicken Sie auf **Bind**.
29. Klicken Sie auf **Fertig**.
30. Stellen Sie sicher, dass die von Ihnen erstellten Richtlinien die höchste Priorität haben. Dies stellt sicher, dass sie die höchste Priorität haben, auch wenn mehr Richtlinien für nicht-mobile Benutzer hinzugefügt werden. Weitere Informationen finden Sie unter Festlegen von Prioritäten für Authentifizierungsrichtlinien

## Clientzertifikat- oder Clientzertifikat und Domänenauthentifizierung konfigurieren

March 27, 2024

Sie können den Citrix ADC für Citrix Endpoint Management-Assistenten verwenden, um die für Citrix Endpoint Management erforderliche Konfiguration durchzuführen, wenn Sie die Citrix ADC-Authentifizierung oder das Zertifikat plus Domänenauthentifizierung verwenden. Sie können den Citrix ADC für Citrix Endpoint Management-Assistenten nur einmal ausführen. Informationen zur Verwendung des Assistenten finden Sie unter Konfigurieren von Einstellungen für Ihre Citrix Endpoint Management-Umgebung.

Wenn Sie den Assistenten bereits verwendet haben, verwenden Sie die Anweisungen in diesem Artikel für die zusätzliche Konfiguration, die für die Clientzertifikatauthentifizierung oder das Clientzertifikat plus Domänenauthentifizierung erforderlich ist.

Um sicherzustellen, dass sich der Benutzer eines Geräts im Nur-MAM-Modus nicht mit einem vorhandenen Zertifikat auf dem Gerät authentifizieren kann, lesen Sie “Citrix ADC Certificate Revocation List (CRL)”weiter unten in diesem Artikel.

### Konfigurieren von Citrix Gateway für die Clientzertifikatauthentifizierung über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den virtuellen Server vom Typ **SSL**aus und legen Sie im Abschnitt **SSL-Parameter** die **Option Sitzungswiederverwendung aktivieren** als **DISABLED**fest.
3. Navigieren Sie zu **Citrix Gateway > Virtuelle Server**.
4. Wählen Sie den virtuellen Server vom Typ **SSL** aus und klicken Sie auf **Bearbeiten**.
5. Klicken Sie im Abschnitt **SSL-Parameter** auf das Bearbeitungssymbol.
6. Wählen Sie **Clientauthentifizierung** aus und wählen Sie unter **Clientzertifikat**die Option **Mandatorry**.
7. Erstellen Sie eine Authentifizierungszertifikatrichtlinie, damit Citrix Endpoint Management den **Benutzerprinzipalnamen** oder den **sAMAccount** aus dem Clientzertifikat extrahieren kann, das von Secure Hub für Citrix Gateway bereitgestellt wird.
8. Navigieren Sie zu **Citrix Gateway> Richtlinien> Authentifizierung > CERT**.
9. Klicken Sie auf die Registerkarte **Profile** und dann auf **Hinzufügen**.
10. Stellen Sie die folgenden Parameter für das Zertifikatsprofil ein:

    Authentifizierungstyp: **CERT**

    Zwei-Faktor: **AUS** (nur für Authentifizierung mit Zertifikat)

    Feld Benutzername: Betreff: **CN**

    Feld für Gruppenname: **SubjectAltName:PrincipalName**
11. Binden Sie nur die Zertifikatauthentifizierungsrichtlinie als **Primäre Authentifizierung** im virtuellen Citrix Gateway-Server.
12. Binden Sie das Root-CA-Zertifikat, um das Vertrauen des Clientzertifikats zu überprüfen, das Citrix Gateway vorgelegt wird.

### Konfigurieren von Citrix Gateway für Clientzertifikat und Domänenauthentifizierung über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den virtuellen Server vom Typ **SSL**aus und legen Sie im Abschnitt **SSL-Parameter** die **Option Sitzungswiederverwendung aktivieren** als **DISABLED**fest.
3. Wechseln Sie zu **Citrix Gateway > Richtlinien > Authentifizierung > Cert**.

4. Klicken Sie auf die Registerkarte **Profile** und dann auf **Hinzufügen**.
5. Geben Sie den **Namen** des Profils ein, setzen Sie **Two Factorauf ON**und wählen Sie**unter Benutzername FieldSubjectAltNamePrincipalName**aus.
6. Klicken Sie auf die Registerkarte **Richtlinien** und dann auf **Hinzufügen**.
7. Geben Sie den **Namen** der Richtlinie ein, wählen Sie unter **Server** das Zertifikatsprofil aus, legen Sie den **Ausdruck** fest und klicken Sie auf **Erstellen**.
8. Wechseln Sie zu **Virtuelle Server**, wählen Sie den virtuellen Server vom Typ **SSL**aus und klicken Sie auf **Bearbeiten**.
9. Klicken Sie neben **Authentifizierung**auf **+**, um die Zertifikatauthentifizierung hinzuzufügen.
10. Um die Authentifizierungsmethode auszuwählen, wählen Sie unter **Richtlinie auswählen**die Option **Zertifikat** aus, und wählen Sie unter **Typ auswählen** die Option **Primär** aus. Dadurch wird die Zertifikatsauthentifizierung als primäre Authentifizierung mit derselben Priorität wie der LDAP-Authentifizierungstyp gebunden.
11. Klicken Sie unter **Richtlinienbindung**auf Zum **Auswählen klicken**, um die zuvor erstellte Zertifikatrichtlinie auszuwählen.
12. Wählen Sie die zuvor erstellte Zertifikatrichtlinie aus und klicken Sie auf **OK**
13. Stellen Sie die **Priorität** auf **100** ein und klicken Sie dann auf **Binden**. Verwenden Sie dieselbe Prioritätsnummer, wenn Sie die LDAP-Authentifizierungsrichtlinie in den folgenden Schritten konfigurieren.
14. Klicken Sie in der Zeile für **LDAP-Richtlinie**auf **.
15. Wählen Sie die Richtlinie aus und klicken **Sie** dann im Dropdownmenü Bearbeiten auf **Bindung bearbeiten**.
16. Geben Sie denselben **Prioritätswert** ein, den Sie für die Zertifikatsrichtlinie angegeben haben. Klicken Sie auf **Bind**.
17. Klicken Sie auf **Schließen**.
18. Klicken Sie im Abschnitt **SSL-Parameter** auf das Bearbeitungssymbol.
19. Markieren Sie das Kontrollkästchen **Clientauthentifizierung**, wählen Sie unter **Clientzertifikat** die Option **Obligatorisch** aus und klicken Sie auf **OK**.
20. Klicken Sie auf **Fertig**.

### Citrix ADC-Zertifikatsperrliste

Citrix Endpoint Management unterstützt Certificate Revocation List (CRL) nur für eine Drittanbieter-Zertifizierungsstelle. Wenn Sie eine Microsoft CA konfiguriert haben, verwendet Citrix Endpoint

Management Citrix ADC, um den Widerruf zu verwalten. Bedenken Sie beim Konfigurieren der Clientzertifikatauthentifizierung, ob Sie die Citrix ADC-Einstellung für Zertifikatsperrlisten (CRL) **Enable CRL Auto Refresh** konfigurieren müssen. Dadurch wird sichergestellt, dass Benutzer von Geräten im ausschließlichen MAM-Modus keine Authentifizierung mit einem existierenden Zertifikat am Gerät durchführen können. Citrix Endpoint Management stellt ein neues Zertifikat erneut aus, da es einen Benutzer nicht daran hindert, ein Benutzerzertifikat zu generieren, wenn eines widerrufen wird. Diese Einstellung erhöht die Sicherheit von PKI-Entitäten, wenn über die Zertifikatsperrliste auf abgelaufene PKI-Entitäten geprüft wird.

## Microsoft Intune-Integration

March 27, 2024

Die Integration von Microsoft Intune in Citrix Gateway bietet erstklassige Anwendungszugriffs- und Datenschutzlösung, die von Citrix Gateway und Intune angeboten wird.

Sie erhalten die umfassendste Palette an sicheren Produktivitäts-Apps, einschließlich E-Mail, Kalender, Kontakte, Notizen, Dokumentenbearbeitung und Fernzugriff, die alle zentral über verschiedene Plattformen hinweg verwaltet werden können. Die Integration von Intune und Citrix Gateway bietet erstklassige Funktionen zur Verwaltung mobiler Geräte (MDM), während die clientseitige Citrix Gateway-Technologie es diesen Intune-aufgeklärten Anwendungen ermöglicht, über das Citrix Gateway sicher auf Unternehmensdaten und -anwendungen zuzugreifen.

Die Integration ermöglicht es Citrix Gateway, Compliance-Daten aus Intune abzurufen und Richtlinien für bedingten Zugriff zu ermöglichen. Die Richtlinien für bedingten Zugriff geben Citrix Gateway eine feinere Kontrolle über die Regulierung des Zugriffs basierend auf Gerätefunktionalitäten usw. Beispielsweise kann ein Administrator eine Richtlinie erstellen, bei der nur den Geräten mit deaktivierter “Kamera”Zugriff gewährt wird.

Citrix Gateway unterstützt die Token-Authentifizierung von Azure Active Directory-Bibliotheken (ADAL), sobald der virtuelle Citrix Gateway-Server konfiguriert ist. Bei der Konfiguration greift eine mobile Anwendung, die mit dem Nur-Netzwerk-Wrapper oder SDK von Citrix umschlossen ist, auf Citrix Gateway zu, indem ein ADAL-Token verwendet wird, das die App direkt von AAD abrufen kann.

### Citrix Micro VPN-Integration mit Microsoft Endpoint Manager

Citrix Gateway-Kunden können Micro-VPN mit Microsoft Endpoint Manager (Intune) verwenden. Die Citrix Micro VPN-Integration in Microsoft Endpoint Management ermöglicht Ihren Apps den Zugriff auf on-premises Ressourcen.

Die Citrix Micro-VPN-Technologie bietet ein On-Demand-VPN, das die Datenübertragungskosten senkt und die Sicherheit vereinfacht, da der VPN-Tunnel nicht immer aktiv ist. Stattdessen ist es nur bei Bedarf aktiv, was das Risiko reduziert und die Leistung des Geräts für eine bessere Benutzererfahrung optimiert. Dies trägt auch zur Verbesserung der Akkulaufzeit von Mobilgeräten Die Micro-VPN-Technologie von Citrix bietet mobilen Benutzern sicheren Zugriff auf interne Geschäftsressourcen und bietet ihnen gleichzeitig die beste Benutzererfahrung.

Micro VPN wird nur für folgende Anwendungsfälle unterstützt:

- Nur Intune-Verwaltung für mobile Anwendungen (MAM)
- Intune-Verwaltung für mobile Geräte (MDM) und Verwaltung mobiler Anwendungen (MAM)

> **Wichtig:**
>
> Für die SSL-VPN-Funktionalität erfordert Micro-VPN eine NetScaler Gateway Advanced oder Premium Edition (VPX 3000 oder höher) und eine Citrix Endpoint Management-Berechtigung. Die Citrix Endpoint Management-Berechtigung gewährleistet die kontinuierliche Unterstützung des Micro-VPN-SDK in einem mobilen Microsoft Edge-Browser (iOS und Android). Weitere Informationen erhalten Sie von Ihrem Vertriebsmitarbeiter, Kundenbetreuer oder Partnervertreter.

Einzelheiten zum Einrichten der Citrix Micro VPN-Integration mit Microsoft Endpoint Manager finden Sie unter Einrichten von Citrix Gateway für die Verwendung von Micro VPN mit Microsoft Endpoint Manager.

## Wann sollte die integrierte Intune-MDM-Lösung verwendet werden?

March 27, 2024

Die folgenden Szenarien veranschaulichen die Verwendung der integrierten Intune MDM-Lösung:

- Ein neuer Kunde beschließt, Intune mit der lokalen Citrix Gateway-Bereitstellung zu verwenden
- Ein vorhandener Citrix Gateway-Benutzer möchte die Verwaltung mobiler Geräte mit Intune hinzufügen
- Ein vorhandener Intune-Benutzer möchte Mobilgeräten oder Anwendungen den Zugriff auf Daten ermöglichen, die sich im Unternehmensnetzwerk befinden, mit einer physischen oder virtuellen Citrix Gateway-Appliance in der Unternehmens-DMZ.

> **Hinweis**
>
> Nur iOS- und Android-Clients werden unterstützt.

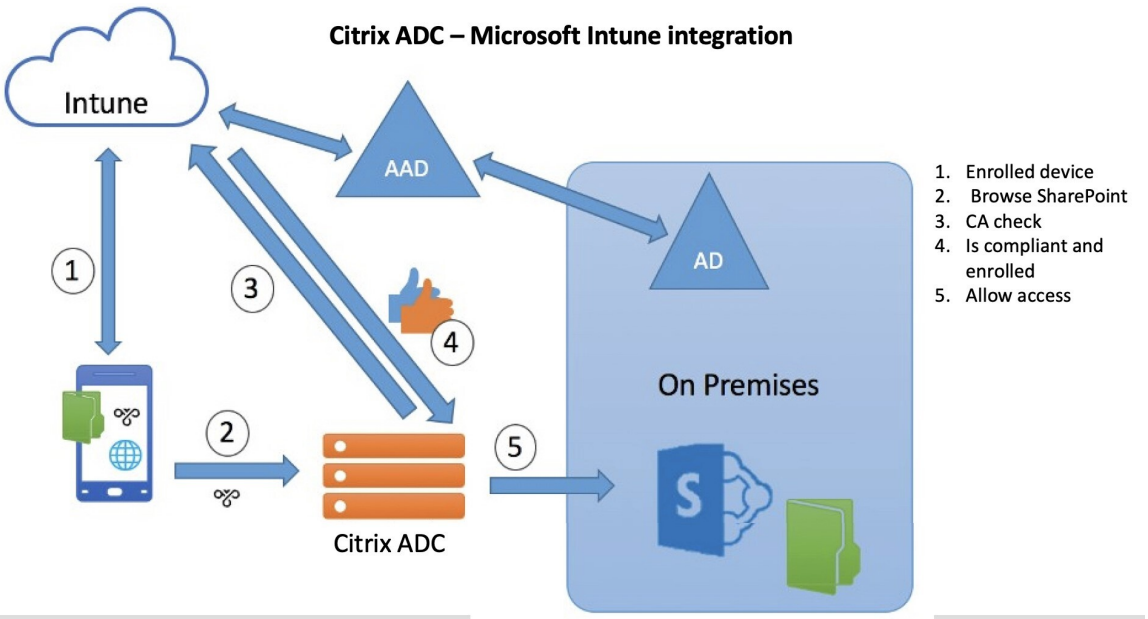
 

# Verstehen der Citrix Gateway MDM-Integration mit Intune

March 27, 2024

Im Folgenden finden Sie einen Beispielfluss von Ereignissen in einer typischen Citrix Gateway MDM-Integration mit Intune:

1. Melden Sie ein Mobilgerät bei Intune an.
2. Vom Unternehmen genehmigte Anwendungen und Geräterichtlinien werden auf das Gerät übertragen.
3. Durchsuchen Sie SharePoint (on-premises Anwendung) vom Gerät aus.
4. Die Browseranforderung geht an Citrix Gateway.
5. Das Citrix Gateway-Gerät prüft bei Intune den Registrierungsstatus des Geräts.
6. Wenn ein konformes Gerät erfolgreich registriert wurde, wird der SharePoint-Zugriff gewährt.




Wenn ein Gerät eine Richtlinie für bedingten Zugriff nicht erfüllt, zeigt der Citrix Gateway VPN-Client eine Fehlermeldung an. Die Nachricht enthält einen Link vom Gerät zu einer von Intune gehosteten Seite, die dem Benutzer die Möglichkeit gibt, sich zu registrieren oder den Konformitätsstatus des Geräts zu korrigieren.

> **Hinweis:**
>
> Administratoren müssen Folgendes sicherstellen, während sie die Zertifikate an Intune weitergeben, damit die Benutzer zwischen den verschiedenen Zertifikaten auf ihrem Gerät unterscheiden können.

- Zertifikate müssen eine Themenzusammenfassung haben.

- Die Themenzusammenfassungen für verschiedene Zertifikate müssen unterschiedlich sein.

## Konfigurieren der Überprüfung des Netzwerkzugriffssteuerungsgeräts für den virtuellen Citrix Gateway-Server für die Single

March 27, 2024

Dieses Thema enthält Informationen zum Konfigurieren von Citrix Gateway für die Verbindung mit einem internen Netzwerk von einem mobilen Gerät (iOS und Android) mit der von Microsoft Intune angebotenen Network Access Compliance (NAC) -Sicherheit. Wenn ein Benutzer versucht, von einem iOS- oder Android-VPN-Client aus eine Verbindung zu Citrix Gateway herzustellen, prüft das Gateway zunächst beim Intune-Dienst, ob das Gerät ein verwaltetes und ein kompatibles Gerät ist.

- Verwaltet: Das Gerät wird über den Intune Company Portal-Client registriert.
- Konform: Erforderliche Richtlinien, die vom Intune MDM-Server übertragen wurden, werden angewendet.

Nur wenn das Gerät sowohl verwaltet als auch konform ist, wird die VPN-Sitzung eingerichtet und der Benutzer erhält Zugriff auf die internen Ressourcen.

> **Hinweis:**
>
> - In diesem Setup spricht Citrix Gateway im Back-End mit dem Intune-Dienst. Die SSL-Profile verarbeiten die eingehenden Verbindungen zum Citrix Gateway. Die Citrix Gateway-Back-End-Kommunikation verarbeitet alle SNI-Anforderungen der Back-End-Cloud-Dienste (Intune).
> - Der virtuelle SNI für den virtuellen DTLS-Gateway-Server wird in Citrix Gateway Version 13.0 Build 64.x und höher unterstützt.
> - Intune NAC Check für das Pro-App-VPN oder sogar geräteweites VPN wird nur unterstützt, wenn das VPN-Profil vom Intune-Verwaltungsportal (jetzt als Microsoft Endpoint Manager bekannt) bereitgestellt wird. Diese Funktionen werden für vom Endbenutzer hinzugefügte VPN-Profile nicht unterstützt. Auf dem Endbenutzergerät muss das VPN-Profil von Microsoft Endpoint Manager von seinem Intune-Administrator auf seinem Gerät bereitgestellt werden, um die NAC-Prüfung verwenden zu können.

### Lizenzierung

Für diese Funktion ist eine Citrix Enterprise Edition-Lizenz erforderlich.

### Systemanforderungen

- Citrix Gateway Version 11.1 Build 51.21 oder höher
- iOS VPN —10.6 oder höher
- Android VPN —2.0.13 oder höher
- Microsoft
  - Azure AD-Zugriff (mit Mandanten- und Administratorrechten)
  - Mandant mit aktiviertem Intune
- Firewall
  Aktivieren Sie Firewall-Regeln für den gesamten DNS- und SSL-Verkehr von der Subnetz-IP-Adresse zu `https://login.microsoftonline.com` und `https://graph.windows.net` (Port 53 und Port 443)

### Voraussetzungen

- Alle bestehenden Authentifizierungsrichtlinien müssen von klassischen auf erweiterte Richtlinien umgestellt werden. Informationen zur Umstellung von klassischen Richtlinien auf erweiterte Richtlinien finden Sie unter https://support.citrix.com/article/CTX131024.
- Erstellen Sie eine Citrix Gateway-Anwendung im Azure-Portal. Einzelheiten finden Sie unter Konfigurieren einer Citrix Gateway-Anwendung im Azure-Portal.
- Konfigurieren Sie die OAuth-Richtlinie in der Citrix Gateway-Anwendung, die Sie mit den folgenden anwendungsspezifischen Informationen erstellt haben.
  - Client-ID/Anwendungs-ID
  - Client geheim/ Anwendungsschlüssel
  - Azure-Tenant-ID

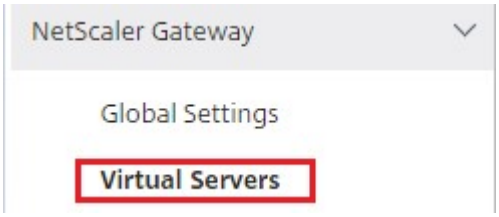
### Referenzen

- Dieses Dokument erfasst die Citrix Gateway-Setup-Konfiguration. Der größte Teil der Konfiguration des Citrix SSO-Clients (iOS/Android) erfolgt auf der Intune-Seite. Einzelheiten zur Intune-VPN-Konfiguration für NAC finden Sie unter https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate.
- Informationen zum Konfigurieren des VPN-Profils für eine iOS-App finden Sie unter https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios.
- Informationen zum Einrichten der Citrix Gateway-Anwendung im Azure-Portal finden Sie unter Konfigurieren einer Citrix Gateway-Anwendung im Azure-Portal.

### So fügen Sie einen virtuellen Citrix Gateway-Server mit nFactor für die Gateway-Bereitstellung hinzu

1. Navigieren Sie zu **Citrix Gateway > Virtuelle Server**.

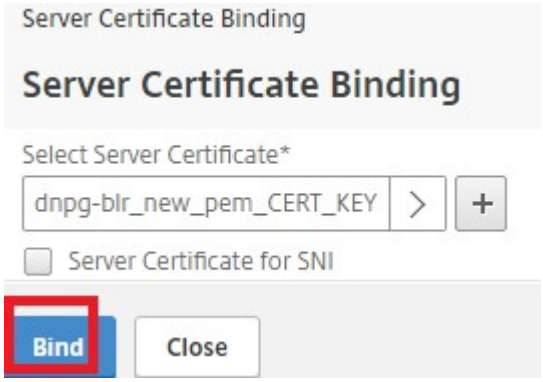



2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie die erforderlichen Informationen im Bereich **Grundeinstellungen** ein und klicken Sie auf **OK**.


4. Wählen Sie **Serverzertifikat**.


5. Wählen Sie das erforderliche Serverzertifikat und klicken Sie auf **Bind**.

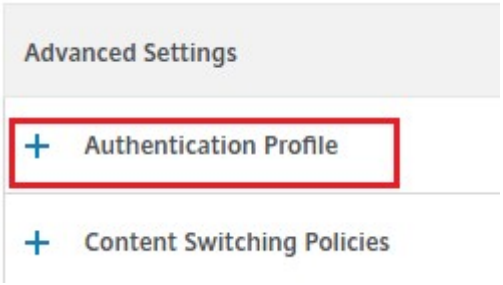
 



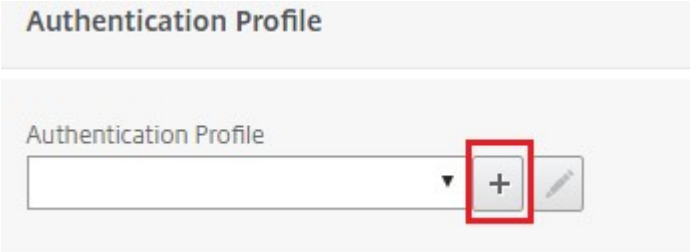

6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Weiter**.
9. Klicken Sie auf das Pluszeichen **[+]** neben **Richtlinien** und wählen Sie **Sitzung** aus der Liste **Richtlinie auswählen** aus. Wählen Sie in der Liste **Typ auswählen** die Option **Anforderung** aus und klicken Sie auf **Weiter**.
10. Klicken Sie auf das Plus-Symbol **[+]** neben **Richtlinie auswählen**.
11. Geben Sie auf der Seite **Create Citrix Gateway Sitzungsrichtlinie** einen Namen für die Sitzungsrichtlinie an.
12. Klicken Sie auf das Plus-Symbol [+] neben **Profil** und geben Sie auf der Seite **Citrix Gateway-Sitzungsprofil erstellen** einen Namen für das Sitzungsprofil an.
13. Klicken Sie auf der Registerkarte **Client Experience** auf das Kontrollkästchen neben **Clientless Access**, und wählen Sie aus der Liste **Aus**.
14. Klicken Sie auf das Kontrollkästchen neben **Plug-In-Typ** und wählen Sie Windows/Mac OS X aus der Liste aus.
15. Klicken Sie auf **Erweiterte Einstellungen**, aktivieren Sie das Kontrollkästchen neben **Clientauswahl** und setzen Sie den Wert auf **ON**.
16. Klicken Sie auf der Registerkarte **Sicherheit** auf das Kontrollkästchen neben **Standardermächtigungsaktion** und wählen Sie **Zulassen** aus der Liste aus.
17. Klicken Sie auf der Registerkarte **Published Applications** auf das Kontrollkästchen neben **ICA-Proxy**, und wählen Sie **AUS** in der Liste aus.
18. Klicken Sie auf **Erstellen.**
19. **Konfigurieren Sie auf der Seite Citrix Gateway-Sitzungsrichtlinie** erstellen im Bereich **Ausdruck** den qualifizierenden Ausdruck.
20. Klicken Sie auf **Erstellen**.

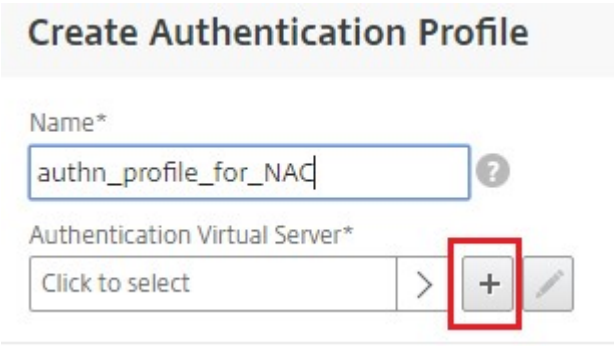
21. Klicken Sie auf **Bind**.
22. Wählen Sie unter **Erweiterte EinstellungenAuthentifizierungsprofil**.




23. Klicken Sie auf das Pluszeichen **[+]** und geben Sie einen Namen für das Authentifizierungsprofil ein.

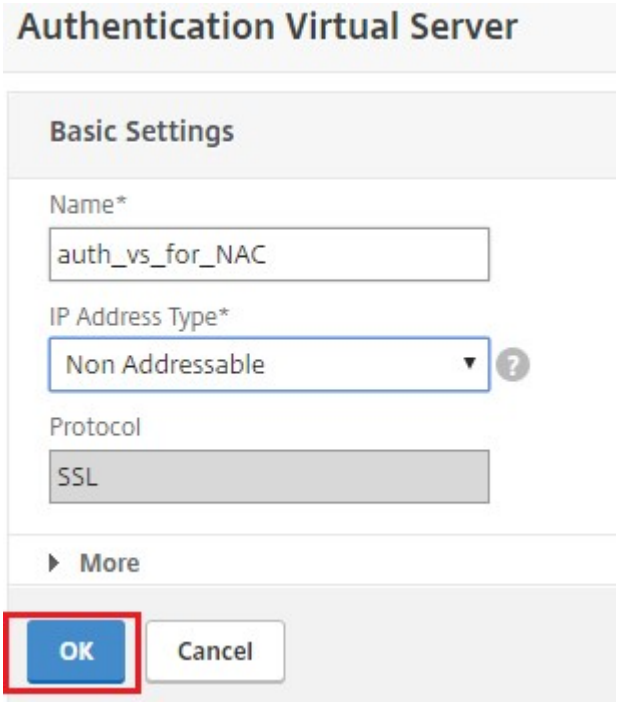



24. Klicken Sie auf das Pluszeichen **[+]**, um einen virtuellen Authentifizierungsserver zu erstellen.

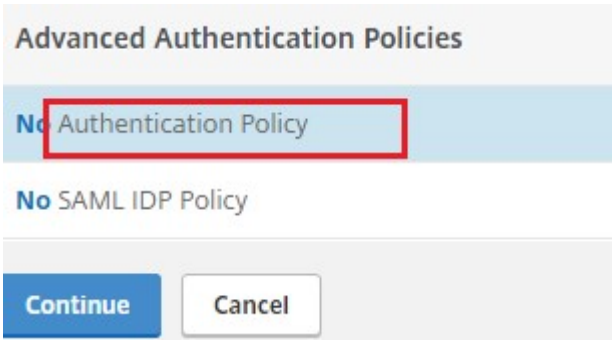



25. Geben Sie im Bereich **Grundeinstellungen** den Namen und den IP-Adresstyp für den virtuellen Authentifizierungsserver an und klicken Sie auf **OK**.Der IP-Adresstyp kann auch **nicht adressierbar** sein.

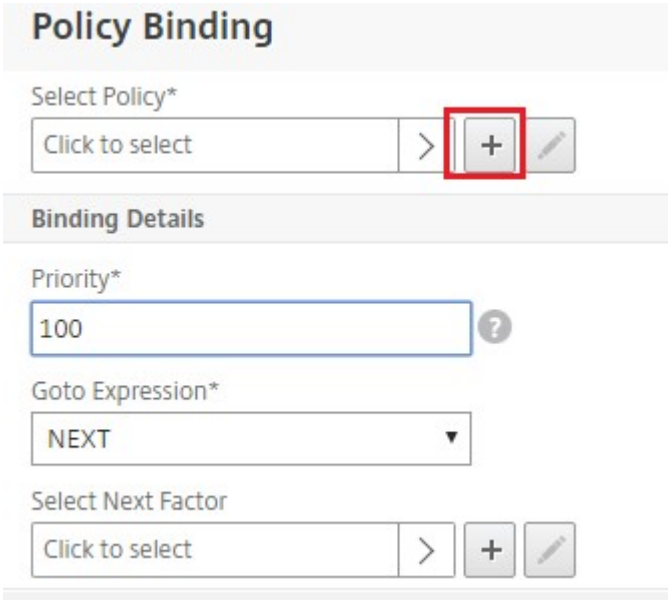



26. Klicke auf **Authentifizierungsrichtlinie**.

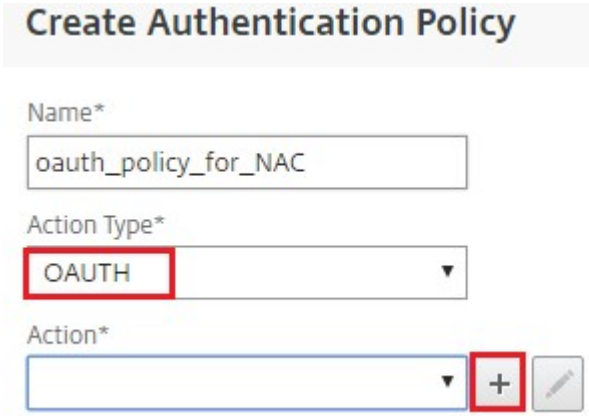



27. Klicken Sie in der Ansicht Richtlinienbindung auf das Pluszeichen **[+]**, um eine Authentifizierungsrichtlinie zu erstellen.




28. Wählen Sie **OAUTH** als **Aktionstyp** aus und klicken Sie auf das Plus-Symbol **[+]**, um eine OAuth-Aktion für NAC zu erstellen.



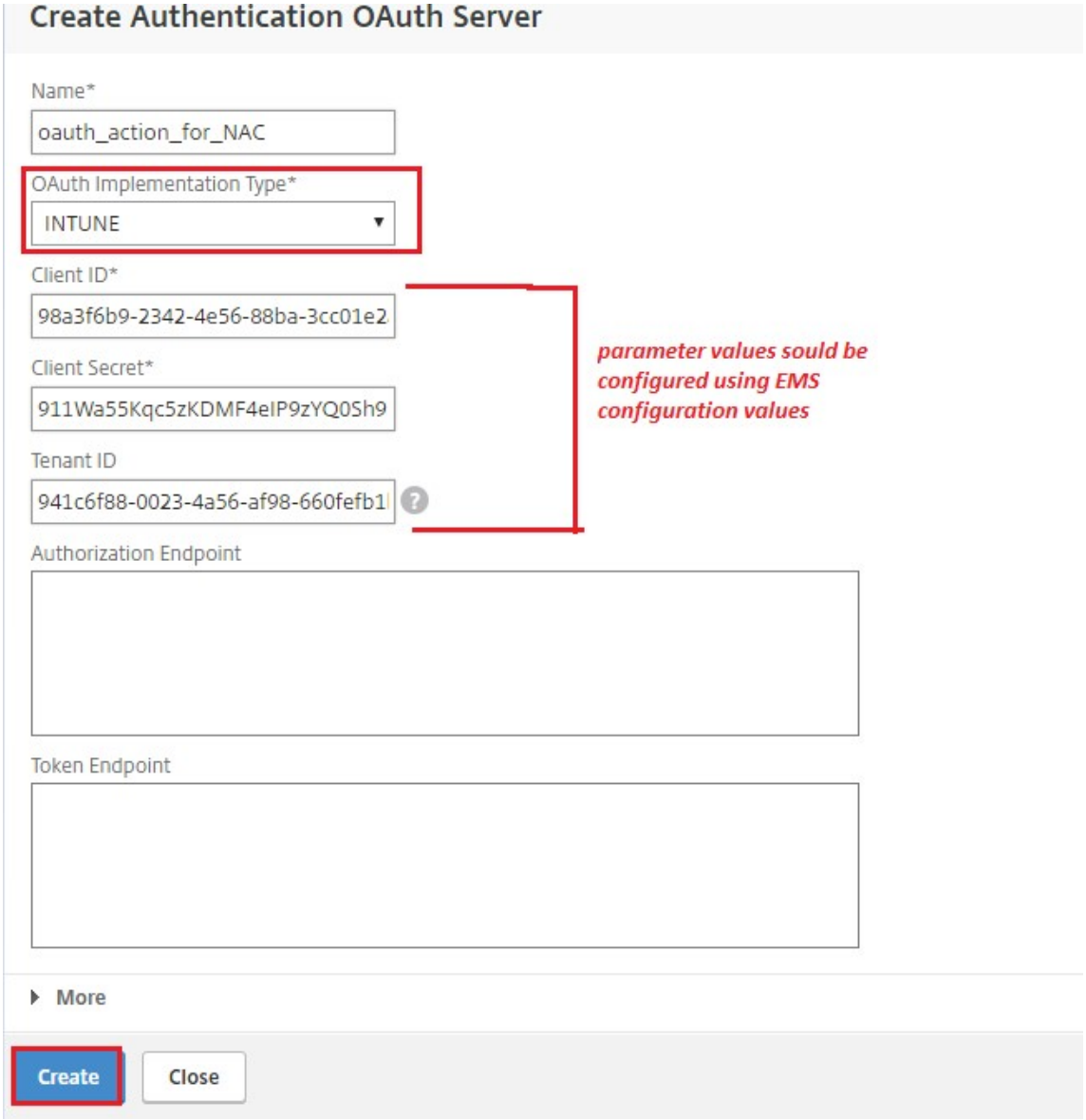

29. Erstellen Sie eine OAuth Aktion mit **Client-ID**, **Client Secret**und **Mandanten-ID**.

> **Hinweis:**
>
> - **Client-ID**, **Client Secret** und **Mandanten-ID** werden nach der Konfiguration der Citrix Gateway-Anwendung im Azure-Portal generiert.
> - Notieren Sie sich die Client-ID/Anwendungs-ID, Client Secret/Application Secret und Azure-Tenant-ID-Informationen, da sie beim späteren Erstellen einer OAuth-Aktion auf Citrix Gateway erforderlich sind.

Stellen Sie sicher, dass auf Ihrer Appliance ein geeigneter DNS-Nameserver konfiguriert ist, um aufzulösen und zu erreichen;
`https://login.microsoftonline.com/`,

```
1 \- - -  `https://graph.windows.net/`,  *.manage.microsoft.com.
```

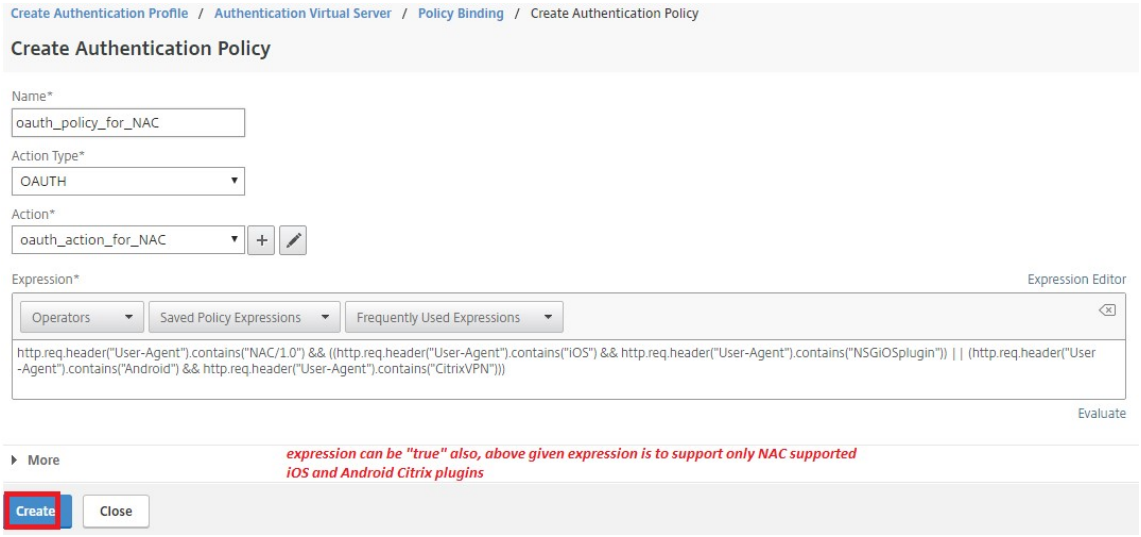



30. Erstellen Sie eine Authentifizierungsrichtlinie für **OAuth Action**.

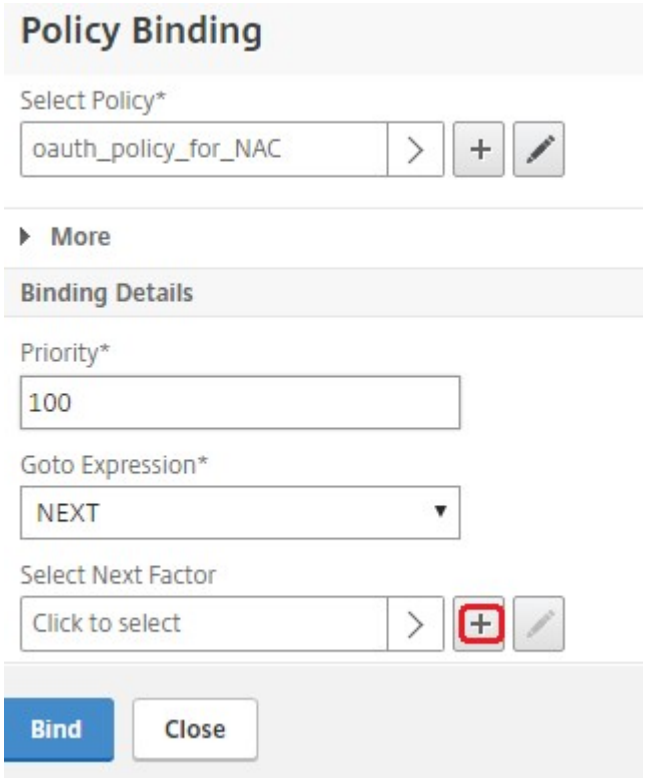
**Regel:**

```
http.req.header("User-Agent").contains("NAC/1.0")&& ((http.req.
    header("User-Agent").contains("iOS") && http.req.header("User-
    Agent").contains("NSGiOSplugin")) || (http.req.header("User-
    Agent").contains("Android") && http.req.header("User-Agent").
    contains("CitrixVPN")))
<!--NeedCopy-->
```

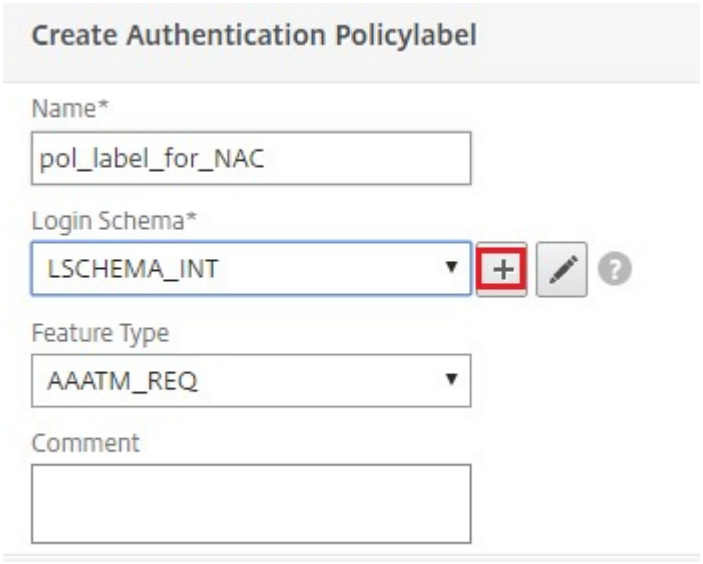



31. Klicken Sie auf das Plus-Symbol **[+]**, um eine NextFactor-Policy Label zu erstellen.

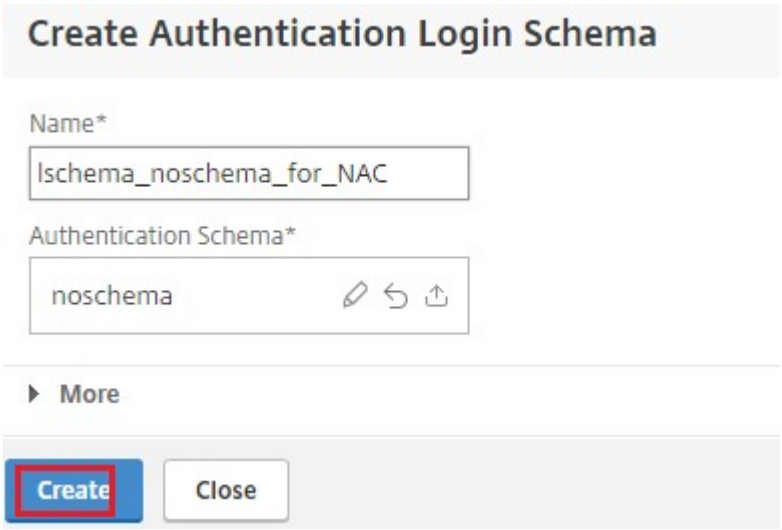



32. Klicken Sie auf das Plus-Symbol **[+]**, um ein Anmeldeschema zu erstellen.

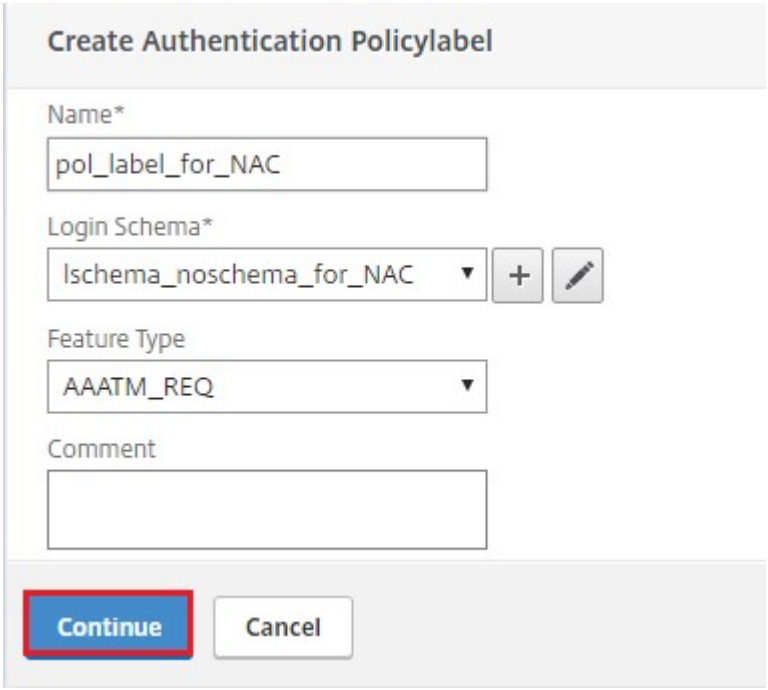



33. Wählen Sie **noschema** als Authentifizierungsschema aus und klicken Sie auf **Erstellen**.

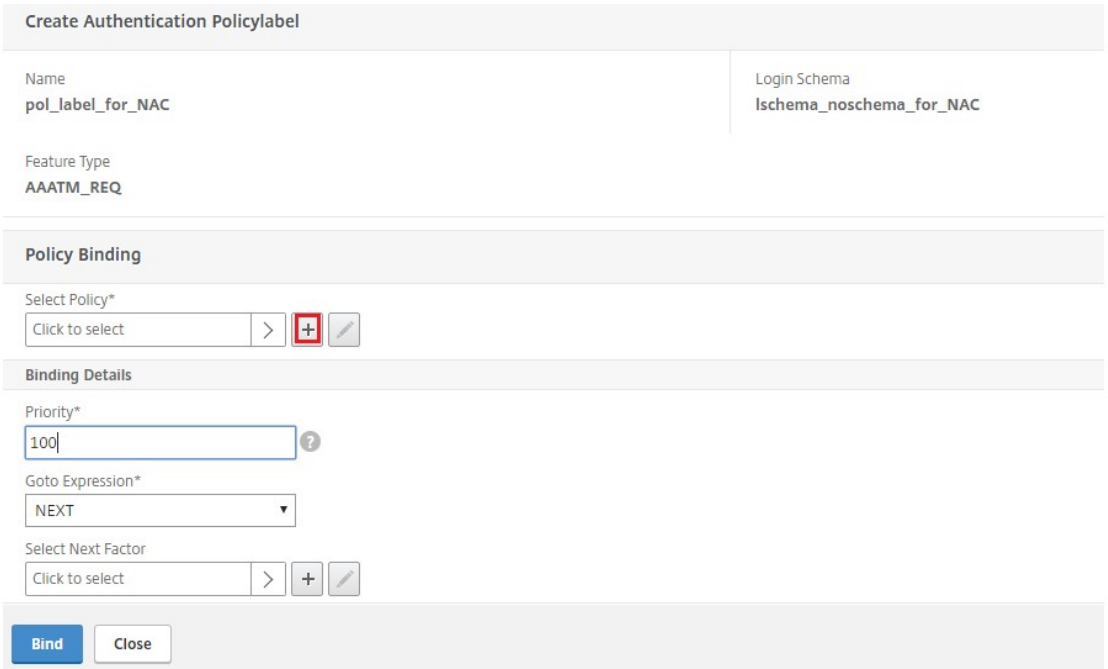



34. Klicken Sie nach Auswahl des erstellten Anmeldeschemas auf **Weiter**.

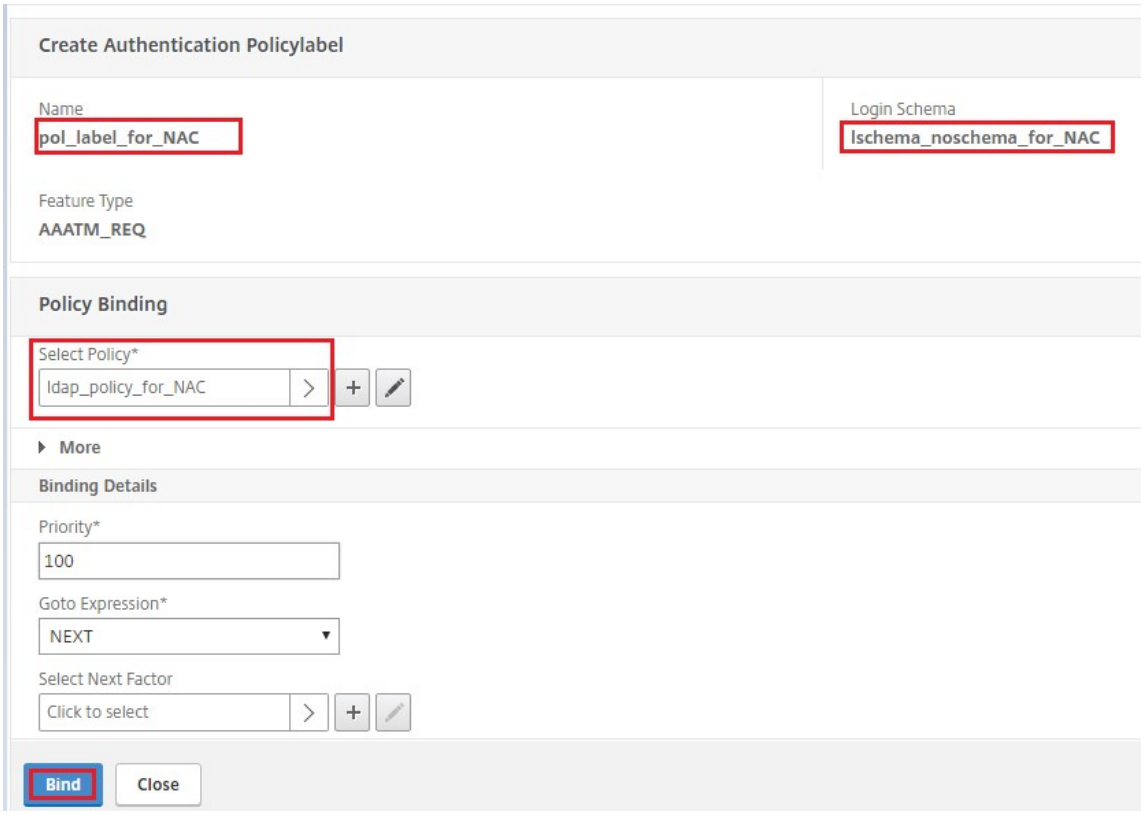



35. Wählen Sie unter **Richtlinie auswählen**eine bestehende Authentifizierungsrichtlinie für die Benutzeranmeldung aus oder klicken Sie auf das Plus-Symbol **+**, um eine Authentifizierungsrichtlinie zu erstellen.
    Einzelheiten zum Erstellen einer Authentifizierungsrichtlinie finden Sie unter Konfigurieren erweiterter Authentifizierungsrichtlinien und Konfigurieren der LDAP-Authentifizierung.

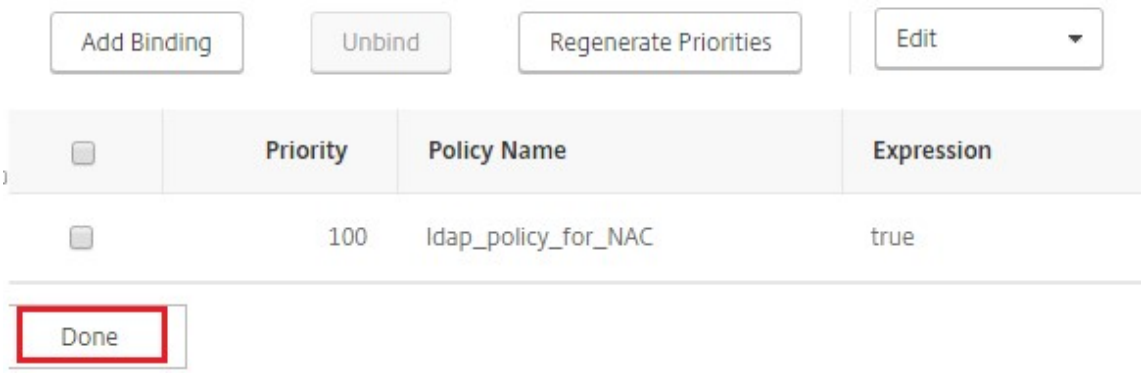



36. Klicken Sie auf **Bind**.

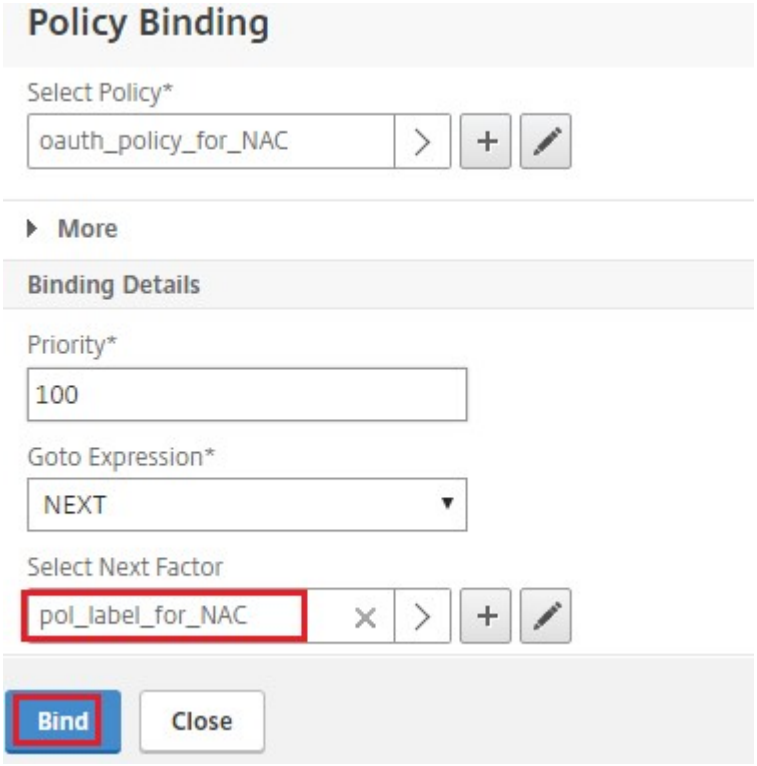



37. Klicken Sie auf **Fertig**.

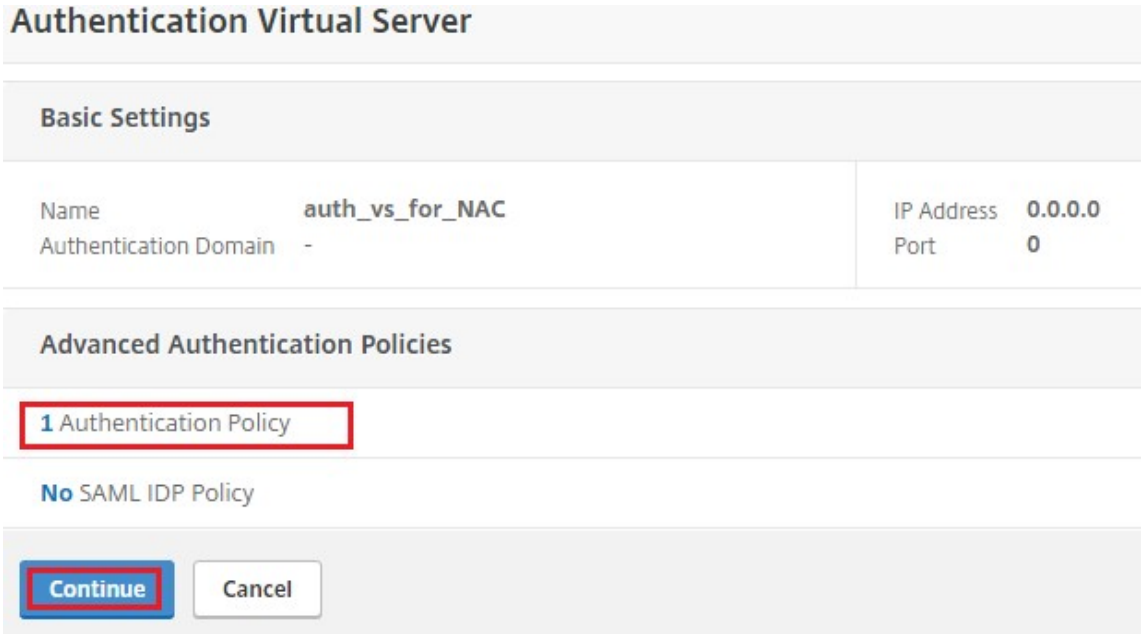



38. Klicken Sie auf **Bind**.

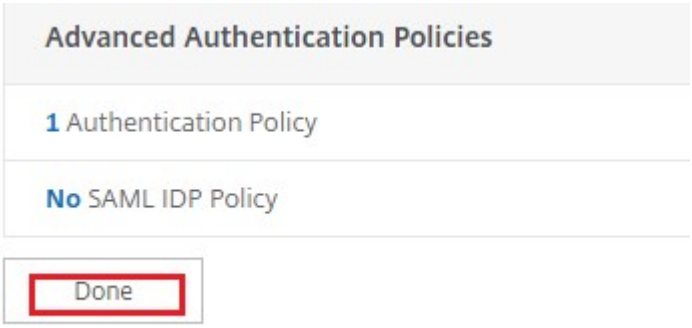



39. Klicken Sie auf **Weiter**.

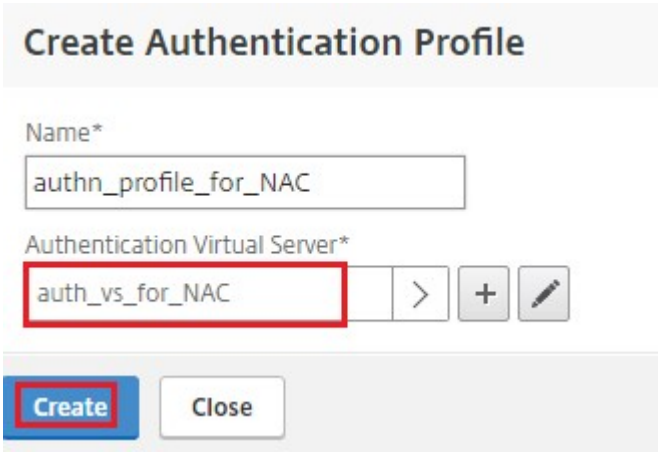



40. Klicken Sie auf **Fertig**.

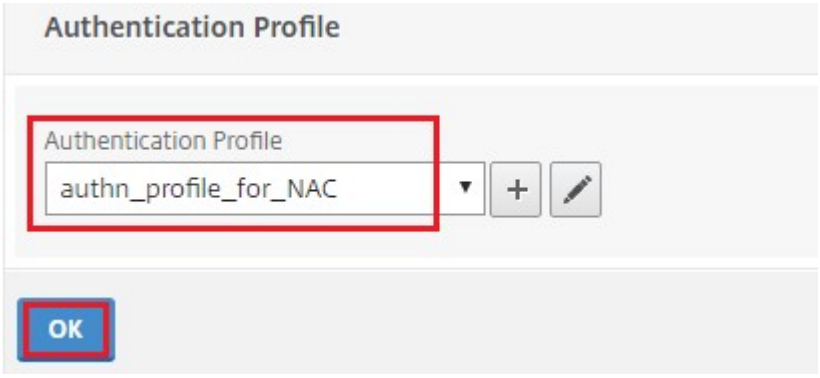
 



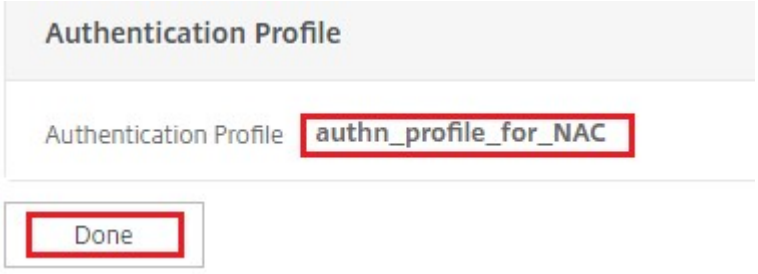

41. Klicken Sie auf **Erstellen**.




42. Klicken Sie auf **OK**.




43. Klicken Sie auf **Fertig**.

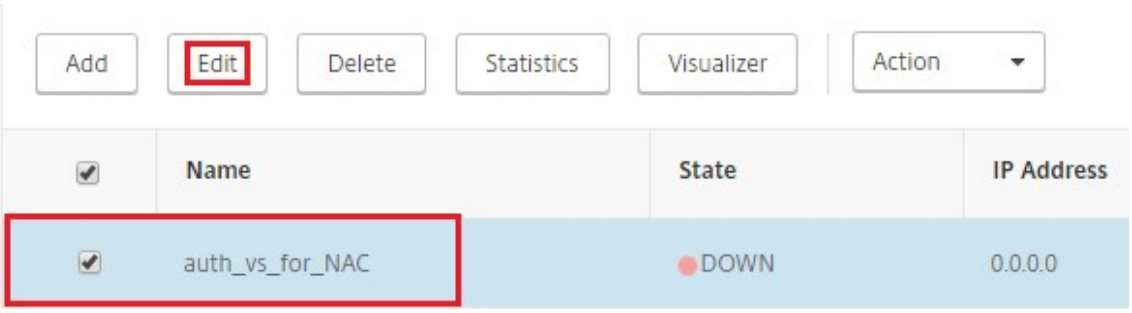


### So binden Sie das Authentifizierungsanmeldeschema an den virtuellen Authentifizierungsserver, um VPN-Plug-Ins anzugeben, um die Geräte-ID als Teil der /cgi/login-Anfrage zu senden

1. Navigieren Sie zu **Sicherheit** > **AAA —Anwendungsverkehr** > **Virtuelle Server**.


2. Wählen Sie den zuvor ausgewählten virtuellen Server aus und klicken Sie auf **Bearbeiten**.

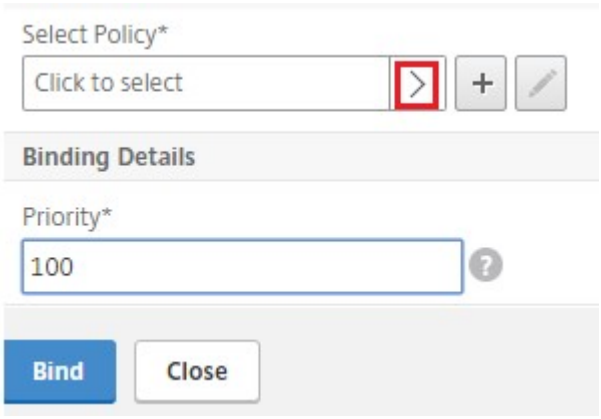



3. Klicken Sie unter **Erweiterte Einstellungen** auf **Anmeldeschemas**.


4. Klicken Sie auf **Login Schemas**, um zu binden.

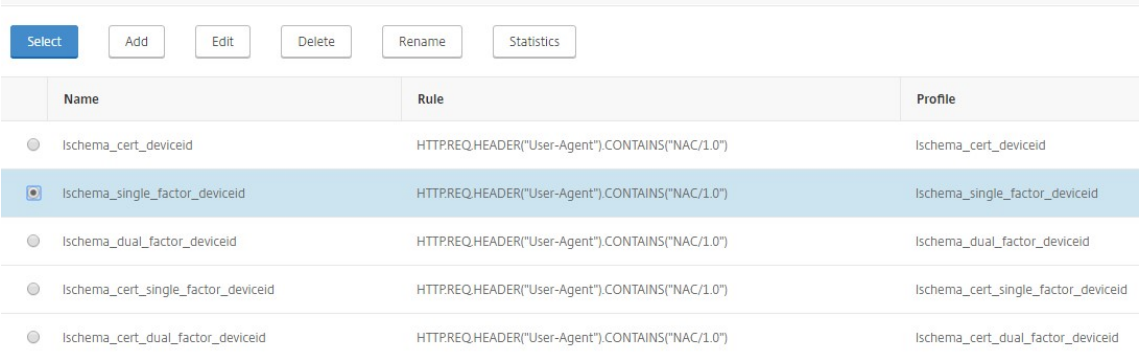

 

5. Klicken Sie auf **[>]**, um die vorhandenen Richtlinien für das Build-In-Anmeldeschema für die NAC-Geräteprüfung auszuwählen und zu binden.

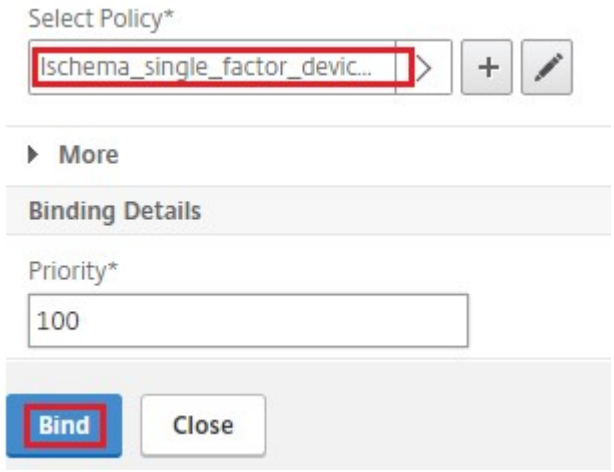



6. Wählen Sie die für Ihre Authentifizierungsbereitstellung geeignete Richtlinie für das Anmeldeschema aus und klicken Sie auf **Auswählen**

   In der zuvor erläuterten Bereitstellung wird eine Single-Faktor-Authentifizierung (LDAP) zusammen mit einer NAC OAuth Action-Richtlinie verwendet, daher wurde **lschema_single_factor_deviceid** ausgewählt.

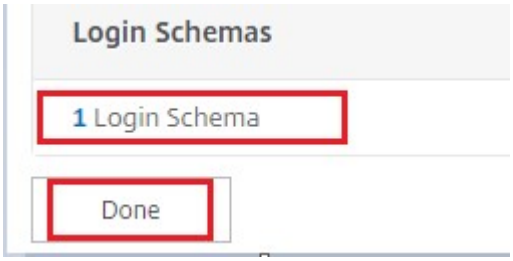



7. Klicken Sie auf **Bind**.



8. Klicken Sie auf **Fertig**.




## Problembehandlung

### Allgemeine Probleme

| Problem | Auflösung |
| --- | --- |
| Die Meldung “Richtlinie hinzufügen erforderlich” wird angezeigt, wenn Sie eine App öffnen<br>Es gibt Richtlinienkonflikte | Hinzufügen von Richtlinien in der Microsoft Graph-API<br>Es ist nur eine einzige Richtlinie pro App zulässig |
| Ihre App kann keine Verbindung zu internen Ressourcen herstellen | Stellen Sie sicher, dass die richtigen Firewall-Ports geöffnet sind, Sie die Mandanten-ID korrigieren und so weiter |

### Citrix Gateway-Probleme

| Problem | Auflösung |
| --- | --- |
| Die Berechtigungen, die für die Gateway-App auf Azure konfiguriert werden müssen, sind nicht verfügbar. | Überprüfen Sie, ob eine Intune-Lizenz verfügbar ist. Versuchen Sie, das Portal manage.windowsazure.com zu verwenden, um festzustellen, ob die Berechtigung hinzugefügt werden kann. Wenden Sie sich an den Microsoft-Support, wenn das Problem weiterhin besteht. |

| Problem | Auflösung |
| --- | --- |
| Citrix Gateway kann nicht erreichen `login.microsoftonline.comandgraph.windows.net`. | Prüfen Sie von NS Shell aus, ob Sie die folgende Microsoft-Website erreichen können: cURL -v -k https://login.microsoftonline.com. Überprüfen Sie dann, ob DNS auf Citrix Gateway konfiguriert ist. Vergewissern Sie sich auch, dass die Firewall-Einstellungen korrekt sind (falls DNS-Anfragen durch eine Firewall gespeichert sind). |
| Ein Fehler erscheint in ns.log nachdem Sie OAuthAction konfiguriert haben. | Überprüfen Sie, ob die Intune-Lizenzierung aktiviert ist und die Azure Gateway-App über die richtigen Berechtigungen verfügt. |
| Der Befehl "OAuthAction"zeigt den OAuth-Status nicht als abgeschlossen an. | Überprüfen Sie die DNS-Einstellungen und Berechtigungen für die Azure Gateway-App. |
| Auf dem Android- bzw. iOS-Gerät wird die Zweifaktor-Authentifizierungsaufforderung nicht angezeigt. | Überprüfen Sie, ob das Zweifaktor-Geräte-ID-LogonSchema an den virtuellen Authentifizierungsserver gebunden ist. |

**Status und Fehlerzustand von Citrix Gateway OAuth**

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

**Hinweis:** Wenn der OAuth Status erfolgreich ist, wird der Status als COMPLETE angezeigt.

**Intune-Konfigurationsprüfung**

Stellen Sie sicher, dass Sie das Kontrollkästchen **Ich stimme** zu **unter Basis-iOS-VPN-Konfiguration für Citrix SSO > Netzwerkzugriffskontrolle (NAC) aktivieren**. Sonst funktioniert der NAC-Check nicht.

## Citrix Gateway-Anwendung im Azure-Portal

March 27, 2024

Im folgenden Abschnitt werden Schritte zum Konfigurieren einer Citrix Gateway-Anwendung im Azure-Portal aufgeführt.

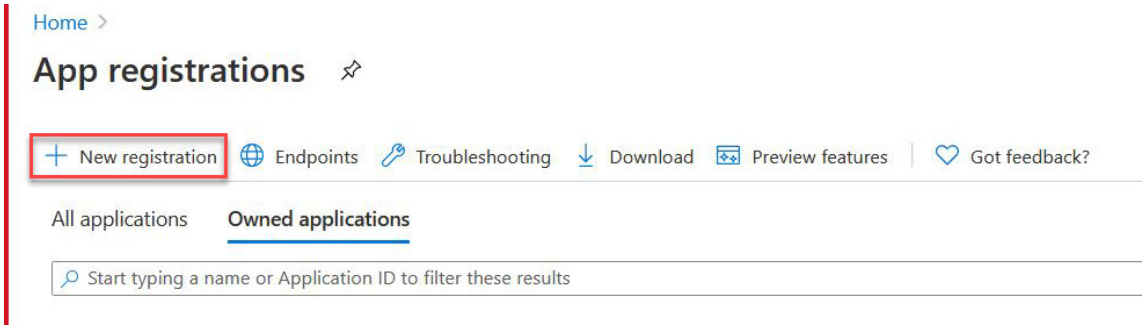
### Voraussetzung

- Globale Azure Admin-Anmeldeinformationen
- Intune-Lizenzierung ist aktiviert
- Für Intune Integration müssen Sie eine Citrix Gateway-Anwendung im Azure-Portal erstellen.
- Konfigurieren Sie nach dem Erstellen der Citrix Gateway-Anwendung die OAuth-Richtlinie auf Citrix Gateway mithilfe der folgenden anwendungsspezifischen Informationen:
  - Client-ID/Anwendungs-ID
  - Client Secret/Anwendungsschlüssel
  - Azure-Tenant-ID
- Citrix Gateway verwendet die App-Client-ID und das Clientgeheimnis, um mit Azure zu kommunizieren und die NAC-Konformität zu überprüfen.

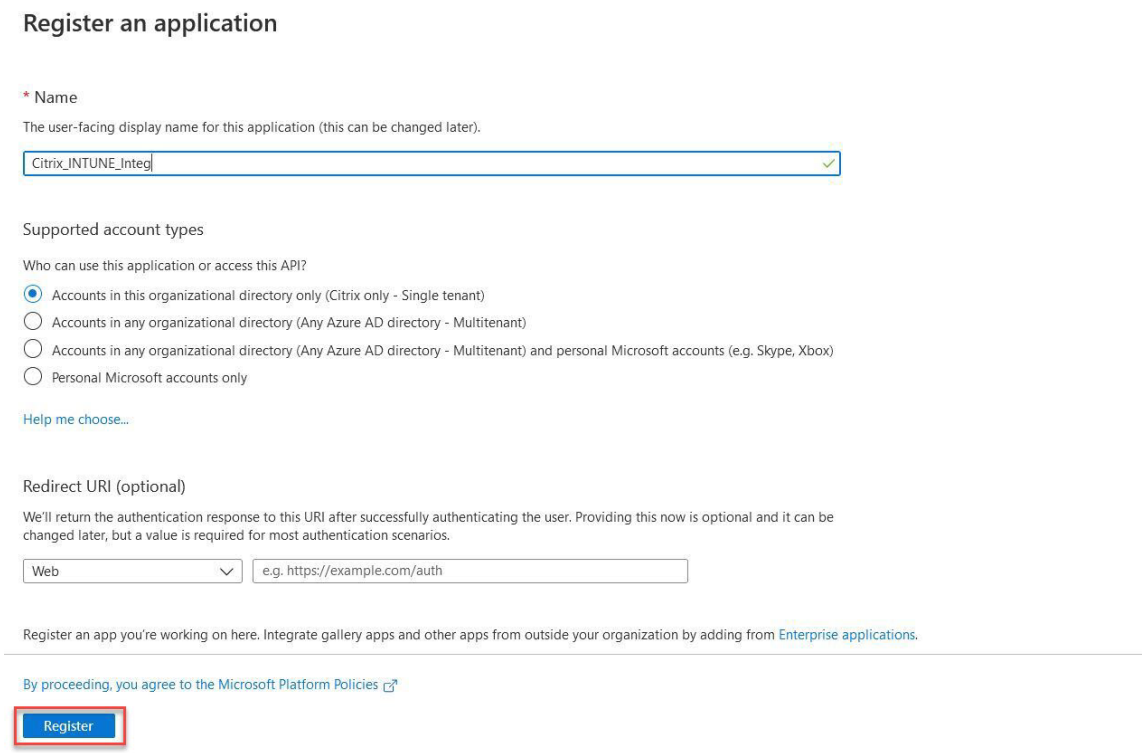
### So erstellen Sie eine Citrix Gateway App auf Azure

1. Loggen Sie sich auf portal.azure.com ein
2. Klicken Sie auf **Azure Active Directory**.
3. Klicken Sie auf **App-Registrierungen** und dann auf **Neue Registrierung**.

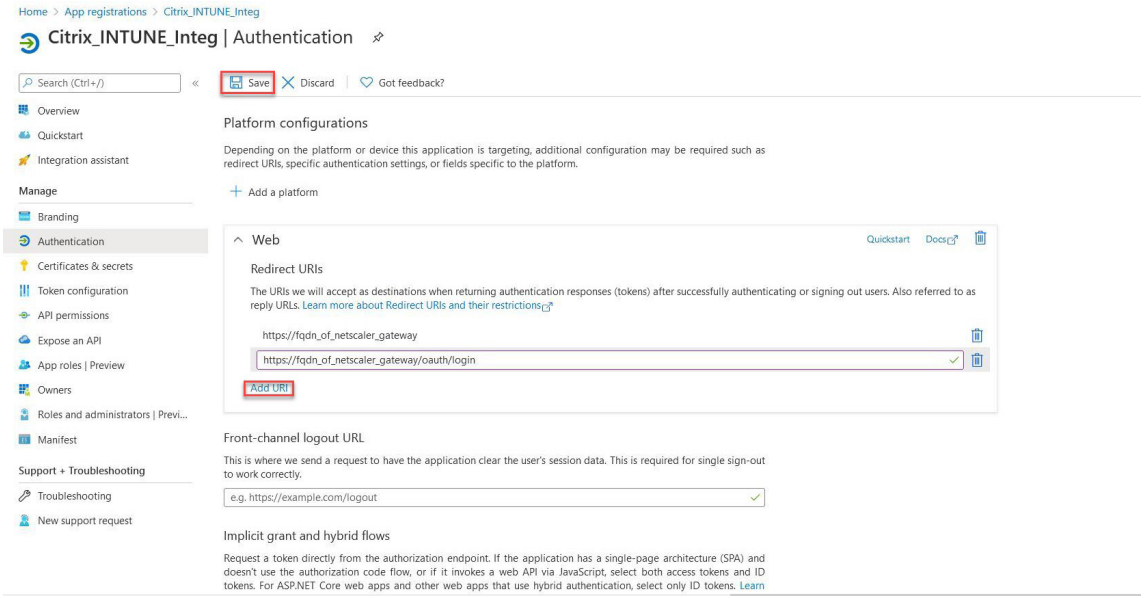



4. Geben Sie auf der Seite **Anwendung registrieren einen** App-Namen ein und klicken Sie auf **Registrieren**.

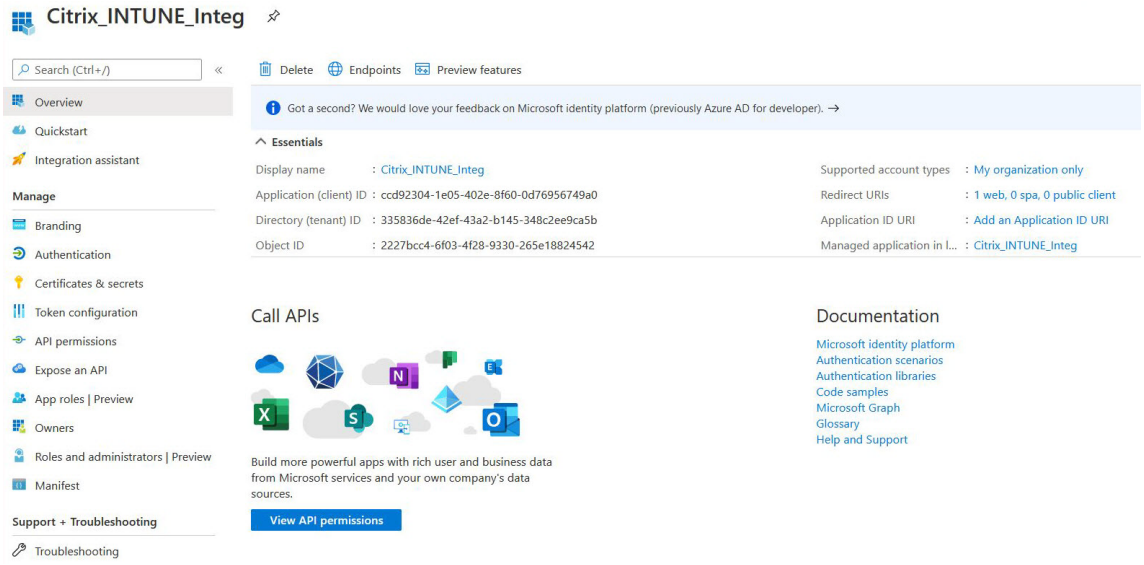



5. Navigieren Sie zu **Authentifizierung**, klicken Sie auf **URI hinzufügen**, geben Sie FDQN für Citrix Gateway ein und klicken Sie auf **Speichern**.

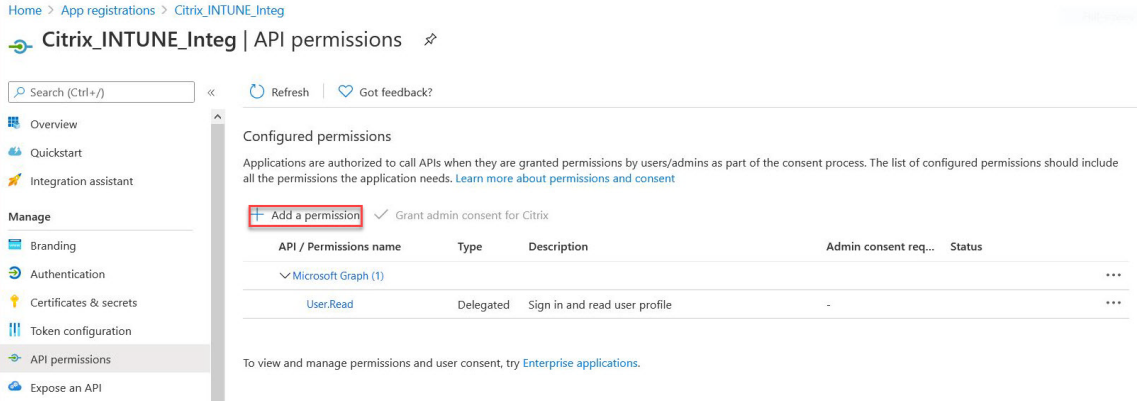



6. Navigieren Sie zur **Übersichtsseite**, um die Client-ID, die Mandanten-ID und die Objekt-ID abzurufen.




7. Navigieren Sie zu **API-Berechtigungen** und klicken Sie auf **Berechtigung hinzufügen**.




**Hinweis:**

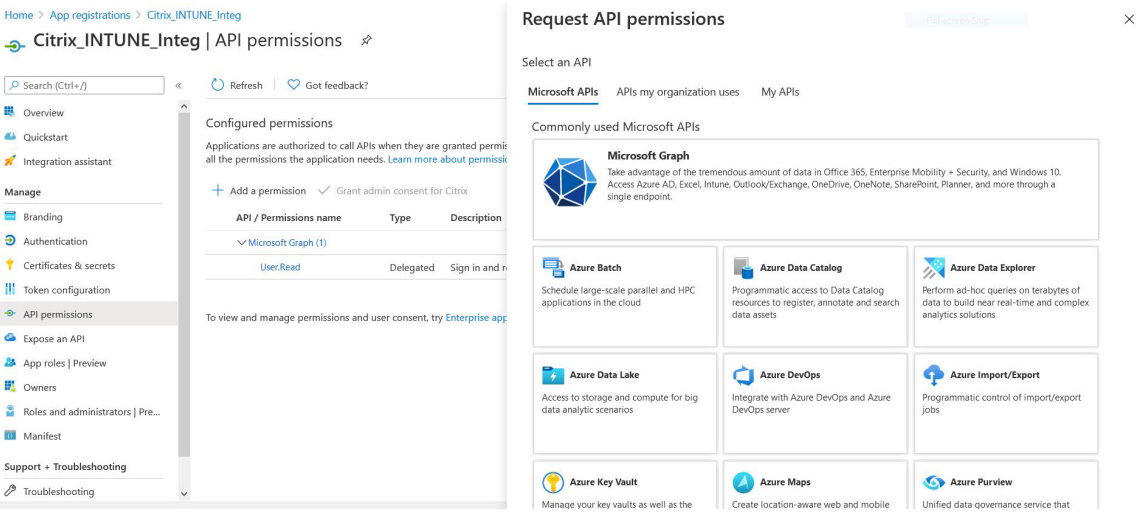
Alle Azure AD-Anwendungen, die die Dienstendpunkte `https://login.microsoftonline.com`, `https://graph.microsoft.com` oder `https://graph.windows.com` aufrufen, brauchen die API-Berechtigung, damit das Gateway die NAC-API aufrufen kann. Die verfügbaren API-Berechtigungen sind:

- Application.Read.All
- Application.ReadWrite.All
- Application.OwnedBy
- Directory.Read.All

Die bevorzugte Berechtigung ist **Application.Read.All**.

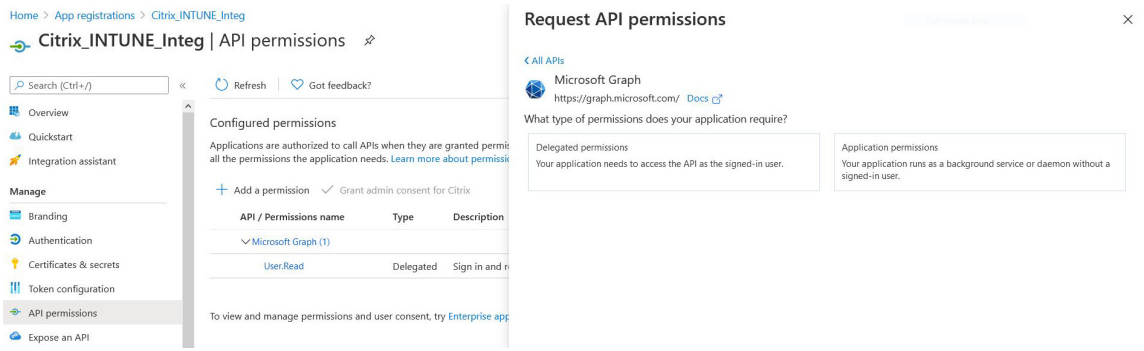
Weitere Einzelheiten finden Sie unter https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

8. Klicken Sie auf die **Microsoft Graph-Kachel**, um API-Berechtigungen für Microsoft Graph zu konfigurieren



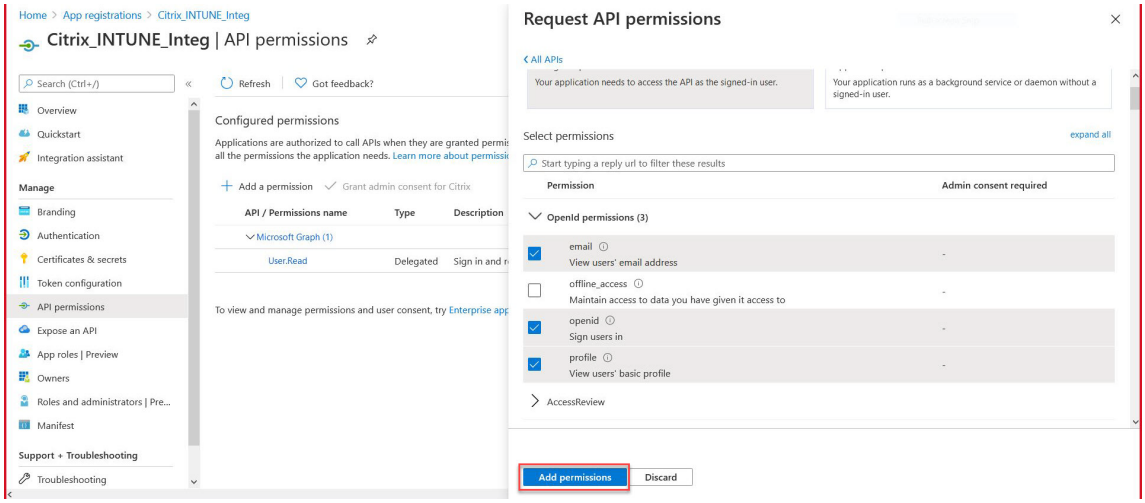

 

9. Klicken Sie auf die Kachel **Delegierte Berechtigungen**.

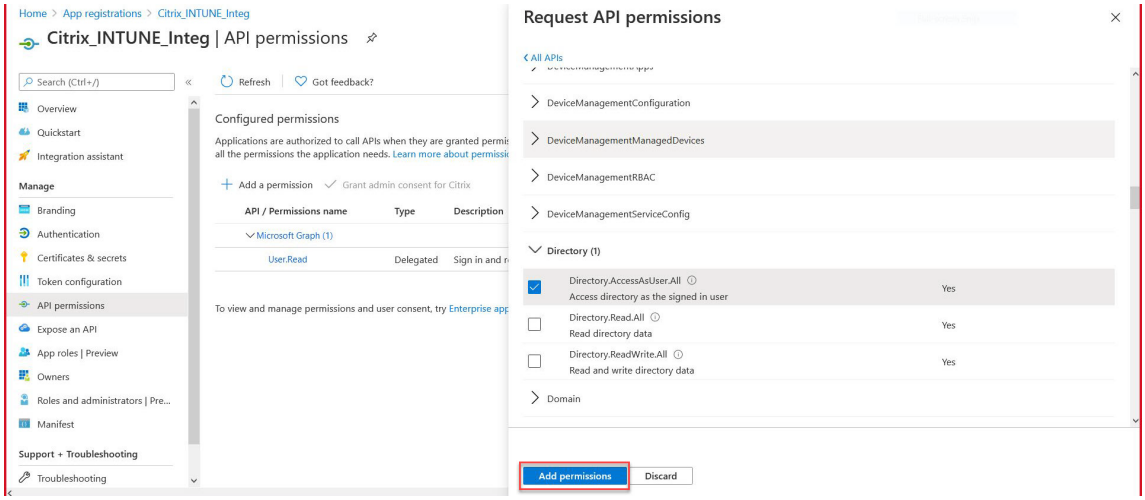


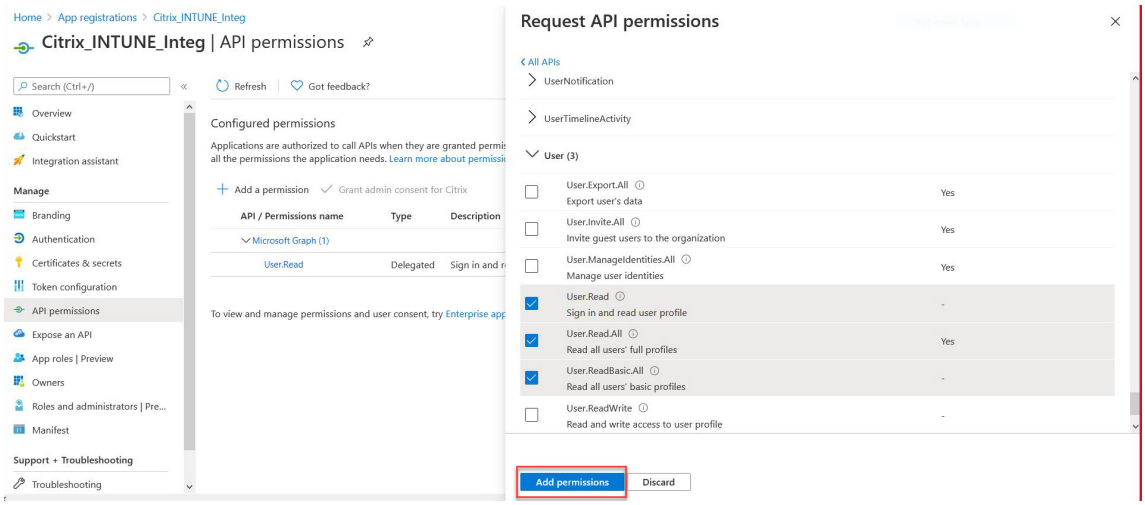

10. Wählen Sie die folgenden Berechtigungen aus und klicken Sie auf **Berechtigungen hinzufügen**.

- E-Mail
- openid
- Profil
- Directory.AccessAsUser.All
- User.Read
- User.Read.All
- User.ReadBasic.All






**Berechtigungen für die Intune-NAC-Prüfung:**

Für alle Azure AD-Anwendungen, die die Dienstendpunkte `https://login.microsoftonline.com`, `https://graph.microsoft.com` oder `https://graph.windows.com` aufrufen, muss die API-Berechtigung zugewiesen werden, damit das Gateway die NAC-API aufrufen kann. Die verfügbaren API-Berechtigungen sind:

- Application.Read.All
- Application.ReadWrite.All
- Application.OwnedBy
- Directory.Read.All

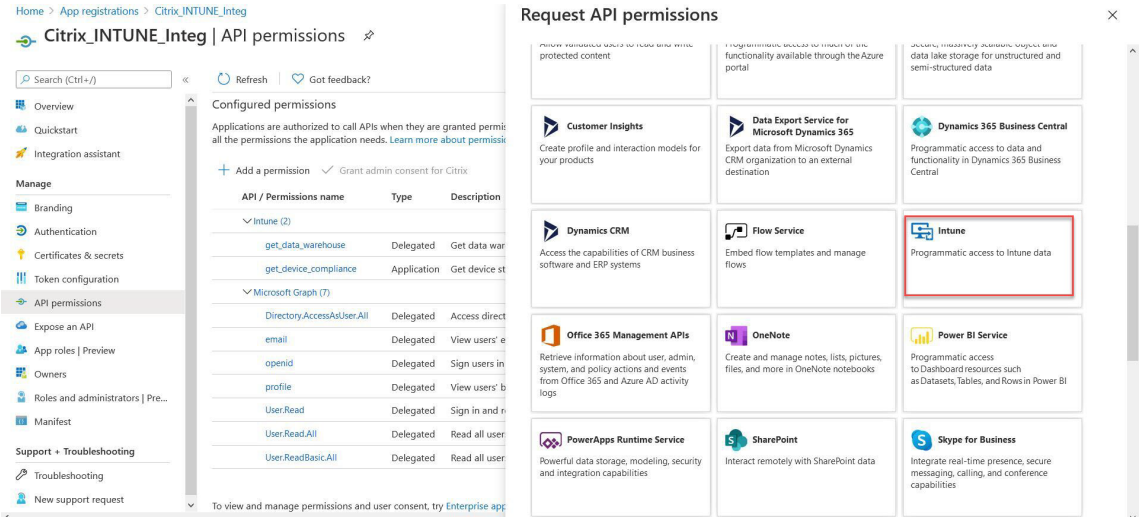
Die bevorzugte Berechtigung ist **Application.Read.All**.

Weitere Informationen finden https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

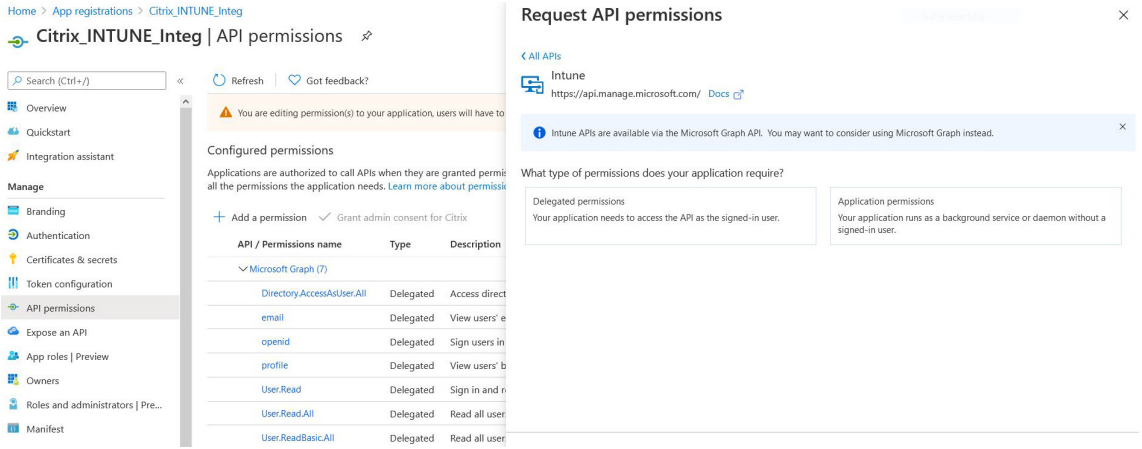
 

> **Sie unter Hinweis:**
>
> Wenn ein Kunde nur die Intune Action for NAC-Prüfung verwendet, ist **Application.Read.All** in Microsoft Graph die einzige erforderliche Berechtigung.

11. Klicken Sie auf die **Intune-Kachel**, um API-Berechtigungen für Intune zu konfigurieren.




12. Klicken Sie auf die Kachel **Anwendungsberechtigungen** und die Kachel **Delegierte Berechtigungen**, um Berechtigungen für get_device_Compliance bzw. get_Data_Warehouse hinzuzufügen.

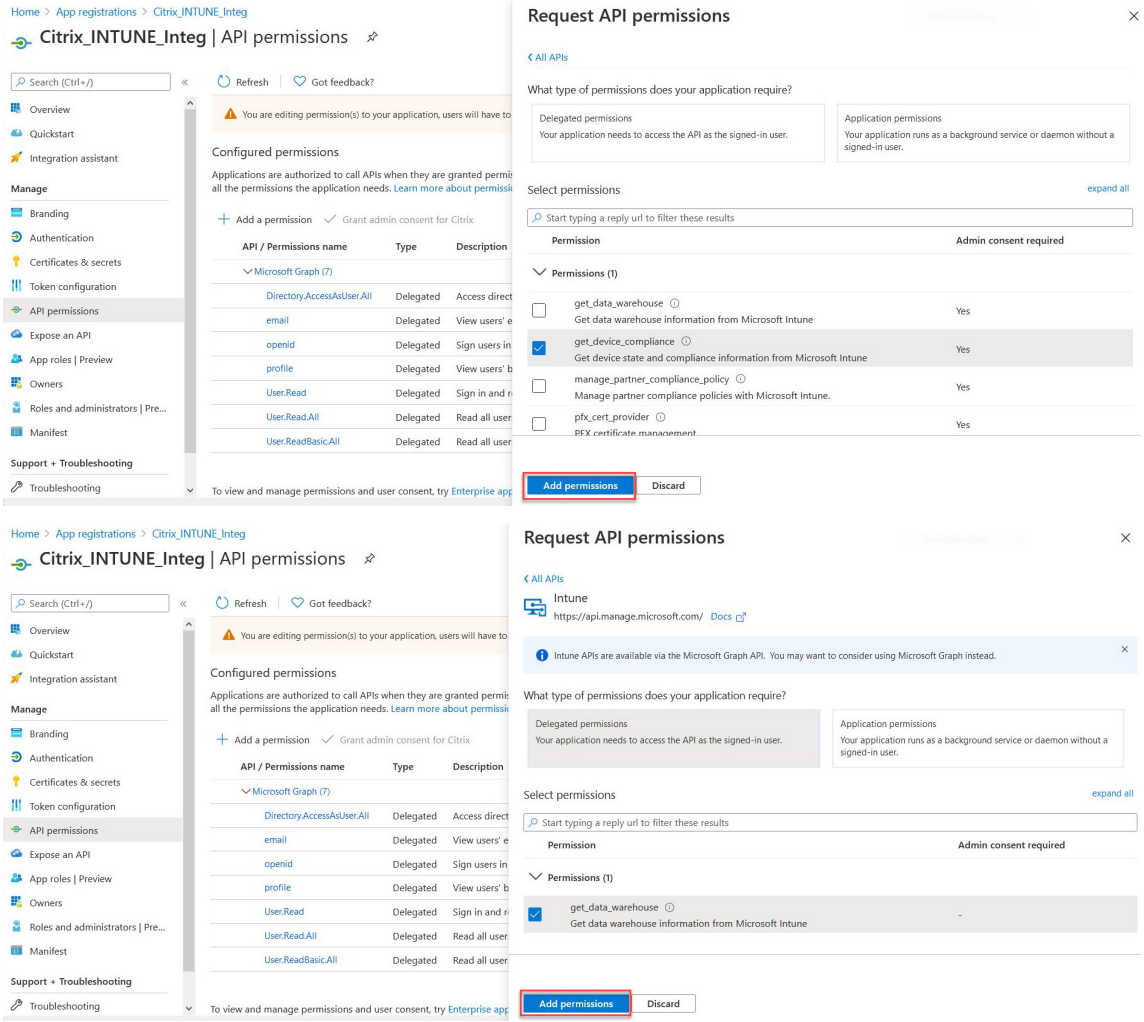



13. Wählen Sie die folgenden Berechtigungen aus und klicken Sie auf **Berechtigungen hinzufügen**.

    - get_device_Compliance - Anwendungsberechtigungen
    - get_data_Warehouse - Delegierte Berechtigungen

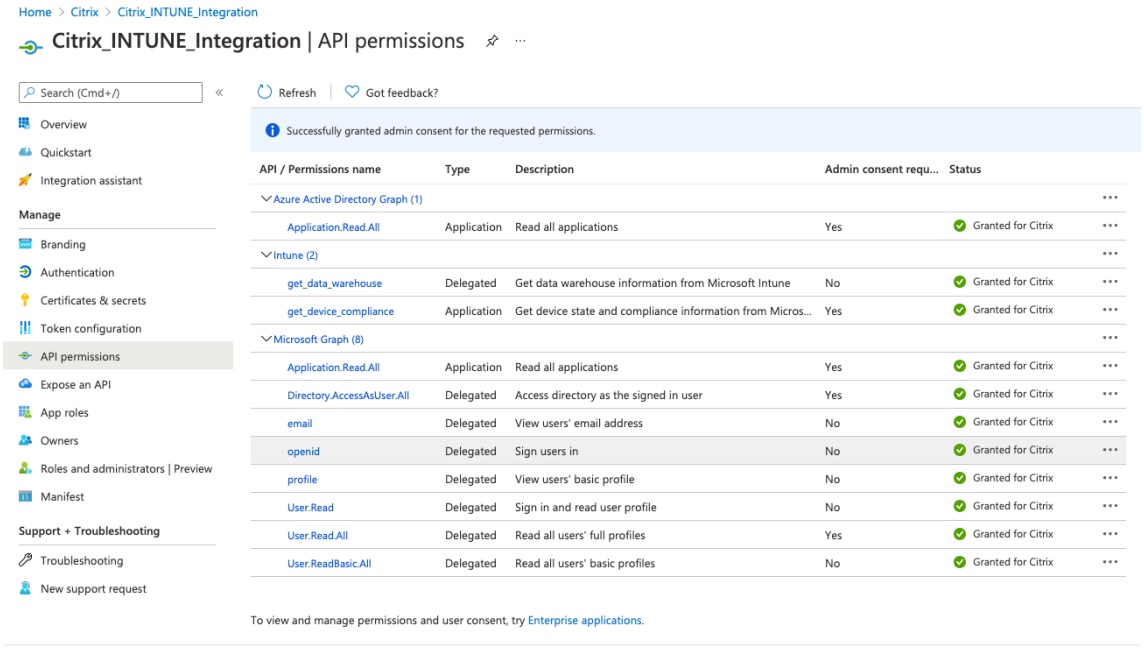
> **Hinweis:**
>
> Für die Intune-NAC-Prüfung ist die einzige erforderliche Berechtigung **get_device_Compliance**.

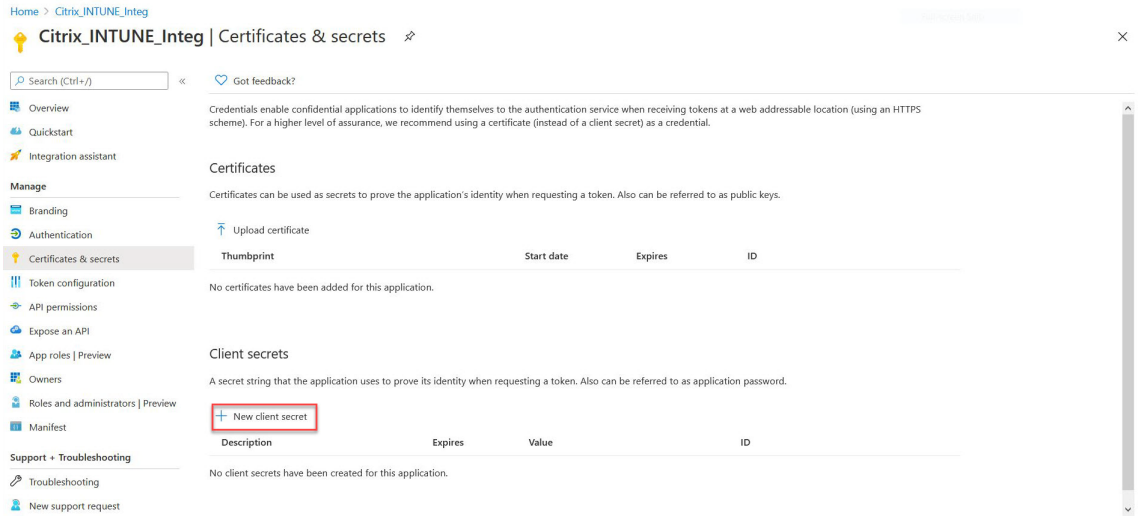



14. Auf der folgenden Seite sind die konfigurierten API-Berechtigungen aufgeführt.

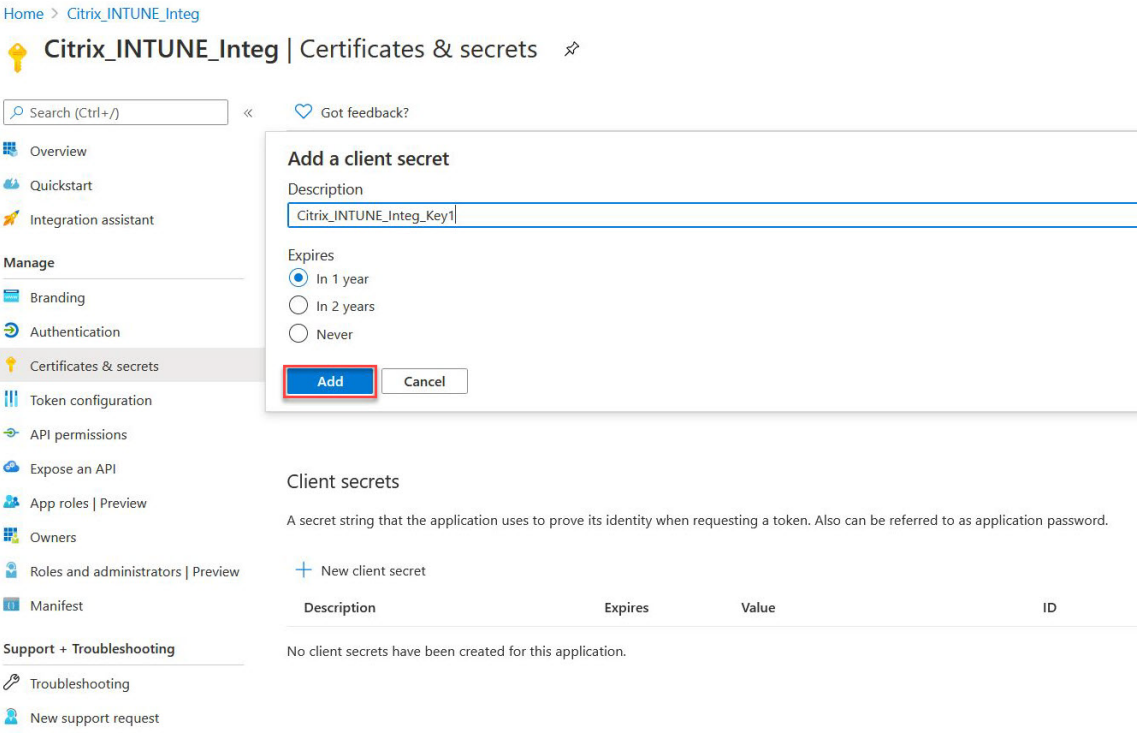



15. Navigieren Sie zu **Certificates & Secrets** und klicken Sie auf **Neuer**



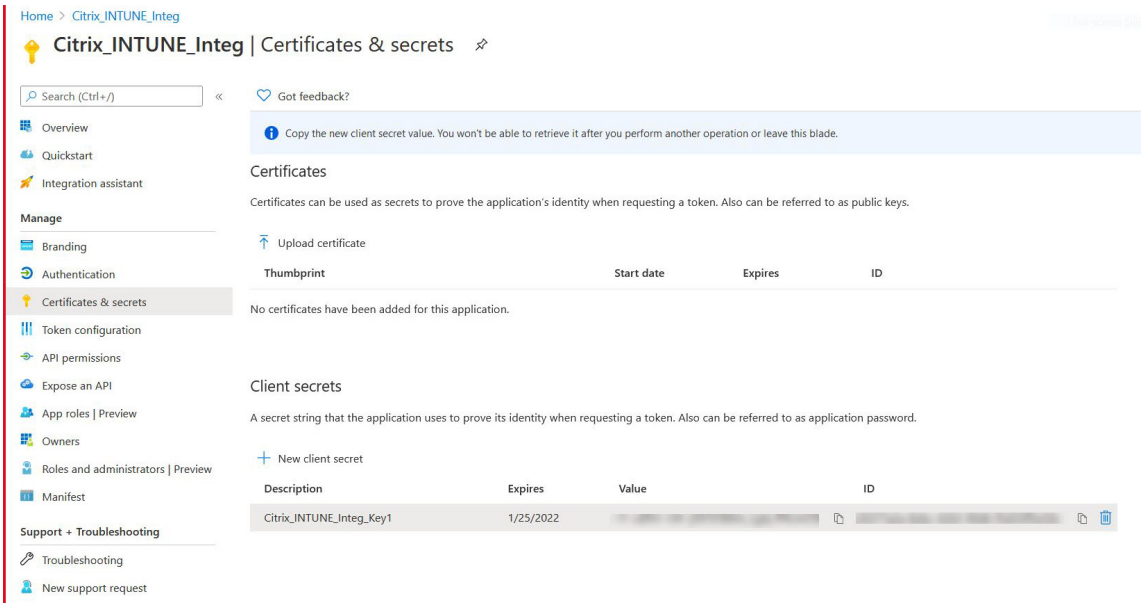

16. Geben Sie auf der Seite **Clientgeheimnis hinzufügen** eine Beschreibung ein, wählen Sie Ablauf aus und klicken Sie auf **Hinzufügen**.




17. Der folgende Bildschirm zeigt das konfigurierte Clientgeheimnis.

> **Hinweis**
>
> Das Client-Secret wird nur einmal angezeigt, wenn es generiert wird. Kopieren Sie das angezeigte Clientgeheimnis lokal. Verwenden Sie dasselbe Clientgeheimnis zusammen mit der Client-ID, die der neu registrierten App zugeordnet ist, während Sie die OAuth -Aktion auf der Citrix Gateway-Appliance für Intune konfigurieren.



Die Anwendungskonfiguration im Azure-Portal ist jetzt abgeschlossen.

## Azure ADAL-Token-Authentifizierung

March 27, 2024

Es folgt der Ablauf von Ereignissen in einer typischen Citrix Gateway-Microsoft-ADAL-Token-Authentifizierung:

1. Wenn eine App in iOS oder Android gestartet wird, kontaktiert die App Azure. Der Benutzer wird aufgefordert, sich mit Benutzeranmeldeinformationen anzumelden. Nach einer erfolgreichen Anmeldung erhält die App ein ADAL-Token.

2. Dieses ADAL-Token wird einem Citrix Gateway präsentiert, das zur Validierung des ADAL-Tokens konfiguriert wurde.

3. Citrix Gateway validiert die Signatur des ADAL-Tokens mit dem entsprechenden Zertifikat von Microsoft.

4. Nach einer erfolgreichen Validierung extrahiert Citrix Gateway den Principal Name (UPN) des Benutzers und gewährt der App VPN Zugriff auf die internen Ressourcen.

## Citrix Gateway Virtual Server für die Microsoft ADAL Token-Authentifizierung konfigurieren

March 27, 2024

Um einen virtuellen Citrix Gateway-Server für die Überwachung der Microsoft ADAL-Token-Authentifizierung zu konfigurieren, benötigen Sie die folgenden Informationen:

- **certEndpoint**: Die URL des Endpoints, der den JSON-Webschlüssel (JWK) für die ADAL-Token-Überprüfung enthält.
- **Zielgruppe**: FQDN des virtuellen Citrix ADC-Servers, an den die App das ADAL-Token sendet.
- **Issuer**: Name des AAD-Ausstellers. Wird standardmäßig aufgefüllt.
- **TenantID**: Mandanten-ID für die Azure ADAL Registrierung.
- **ClientID**: Eine eindeutige ID, die der Gateway-App im Rahmen der ADAL-Registrierung gegeben wurde.
- **clientSecret**: Ein geheimer Schlüssel, der der Gateway-App im Rahmen der ADAL-Registrierung gegeben wurde.

- **ResourceURI**: Ein optionaler Parameter zum Erfassen des Ressourcen-URI. Wenn nicht konfiguriert, verwendet Citrix ADC kommerzielle Azure-Ressourcen-URI.

Führen Sie über die Befehlszeilenschnittstelle die folgenden Schritte aus:

1. Erstellen Sie eine OAuth Aktion.

```
add authentication OAuthAction <oauth-action-name> -OAuthType <
    INTUNE>  – clientid <clientID> -clientsecret <client-secret> -
    audience <audience name> -tenantid <tenantID> -issuer <issuer-
    name> -userNameField <upn> -certEndpoint <certEndpoint-name> -
    resourceURI <name of resource URI>
<!--NeedCopy-->
```

2. Erstellen Sie eine Authentifizierungsrichtlinie, die mit der neu erstellten OAuth -Aktion verknüpft werden soll.

```
add authentication Policy <policy-name> -rule <true> -action <
    oauth intune action>
<!--NeedCopy-->
```

3. Binden Sie das neu erstellte OAuth an AuthVs.

```
bind authentication vserver <auth-vserver> -policy <oauth-intune-
    policy> -priority 2 -gotoPriorityExpression END
<!--NeedCopy-->
```

4. Erstellen Sie ein LoginSchema.

```
add authentication loginSchema <loginSchemaName> -
    authenticationSchema <authenticationSchema ” location ” >
add authentication loginSchemaPolicy <loginSchemaPolicyName> -rule
     true -action <loginSchemaName>
<!--NeedCopy-->
```

5. Binden Sie AuthVS mit LoginSchema.

```
bind authentication vserver <auth-vs> -policy <oauth-pol> -
    priority 2 -gotoPriorityExpression END
<!--NeedCopy-->
```

6. Fügen Sie ein Authentifizierungsprofil hinzu und weisen Sie es einem virtuellen VPN-Server zu.

```
add authnprofile <nfactor-profile-name> -authnvsName <authvserver>
set vpn vserver <vserver-name> -authnprofile <nfactor-profile-name
     >
<!--NeedCopy-->
```

Beispielkonfiguration

```
add authentication OAuthAction tmp-action -OAuthType INTUNE -clientid
    id 1204 -clientsecret a -audience "[http://hello](http://hello/)" -
```

```
    tenantid xxxx -issuer "[https://hello](https://hello/)" -
    userNameField upn -certEndpoint https://login.microsoftonline.com/
    common/discovery/v2.0/keys --resourceURI htpps://api.manage.
    microsoft.com
2
3 add authentication Policy oauth-intune-pol -rule true -action tmp-
    action
4 bind authentication vserver auth-vs-for-gw1-intune -policy oauth-pol -
    priority 2 -gotoPriorityExpression END
5
6 add authentication loginSchema oauth-loginschema -authenticationSchema
    "/nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml"
7
8 add authentication loginSchemaPolicy oauth-loginschema-pol -rule true -
    action oauth-loginschema `
9
10 bind authentication vserver auth-vs-for-gw1-intune -policy oauth-
    loginschema-pol -priority 2 -gotoPriorityExpression END
11
12 add authnprofile nfactor-prof-intune -authnvsName auth-vs-for-gw1-
    intune
13
14 set vpn vserver gw1-intune-authnprofile nfactor-prof-intune
15 <!--NeedCopy-->
```

## Citrix Gateway für Micro-VPN mit Microsoft Endpoint Manager einrichten

March 27, 2024

Die Citrix Micro VPN-Integration in Microsoft Endpoint Management ermöglicht Ihren Apps den Zugriff auf on-premises Ressourcen. Einzelheiten finden Sie unter Citrix Micro VPN-Integration mit Microsoft Endpoint Manager.

### Systemanforderungen

- Citrix Gateway Versionen
  - 13.0
  - 12.1.50.x oder höher
  - 12.0.59.x oder höher

  Sie können die neueste Version von Citrix Gateway von der Citrix Gateway-Downloadseite herunterladen.

- Windows-Desktop mit Windows 7 oder höher (nur für das Umschließen von Android-Apps)
- Microsoft
  - Azure AD-Zugriff (mit Mandantenadministratorberechtigung)
  - Intune-fähiger Mandant
- Firewallregeln
  - Aktivieren einer Firewallregel für SSL-Datenverkehr von einer Citrix Gateway-Subnetz-IP zu `*.manage.microsoft.comhttps://login.microsoftonline.com`, und `https://graph.windows.net` (Port 443)
  - Citrix Gateway muss in der Lage sein, die vorhergehenden URLs extern aufzulösen.

### Voraussetzungen

- **Intune-Umgebung:** Wenn Sie keine Intune-Umgebung haben, richten Sie eine ein. Anweisungen finden Sie in der Microsoft-Dokumentation.
- **Edge-Browser-App:** Das Micro VPN SDK ist in die Microsoft Edge-App und die Intune Managed Browser-App für iOS und Android integriert. Weitere Informationen zum Managed Browser finden Sie auf der Microsoft-Seite zum Managed Browser.
- **Citrix Endpoint Management-Berechtigung**: Stellen Sie sicher, dass Sie über eine aktive Citrix Endpoint Management-Berechtigung verfügen, um das Micro-VPN-SDK in einem mobilen Microsoft Edge-Browser (iOS und Android) weiterhin unterstützen zu können. Weitere Informationen erhalten Sie von Ihrem Vertriebsmitarbeiter, Kundenbetreuer oder Partnervertreter.

### Erteilen Sie Azure Active Directory (AAD) -Anwendungsberechtigungen

1. Zustimmung zur Mandantenanten-AAD-Anwendung von Citrix, Citrix Gateway die Authentifizierung bei der AAD-Domäne zu ermöglichen. Der Azure Global Administrator muss die folgende URL und Zustimmung aufrufen:

   https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent.

2. Zustimmung zur Mandantenanten-AAD-Anwendung von Citrix, um mobilen Anwendungen die Authentifizierung mit dem Citrix Gateway Micro VPN zu ermöglichen. Dieser Link ist nur erforderlich, wenn der Azure Global Admin den Standardwert für Benutzer geändert hat, die Anwendungen von Ja auf Nein registrieren können.
   Diese Einstellung finden Sie im Azure-Portal unter **Azure Active Directory > Benutzer > Benutzereinstellungen**.
   Der globale Azure Administrator muss die folgende URL und Zustimmung aufrufen (fügen Sie

Ihre
Mandanten-ID hinzu) https://login.microsoftonline.com/%5Btenant_id%5D/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7.

### Konfigurieren von Citrix Gateway für Micro-VPN

Zur Verwendung von Micro-VPN in Intune müssen Sie Citrix Gateway für die Authentifizierung bei Azure AD konfigurieren. Ein vorhandener virtueller Citrix Gateway-Server kann in diesem Anwendungsfall nicht verwendet werden.
Konfigurieren Sie Azure AD zunächst zur Synchronisierung mit dem On-Premises-Active Directory. Dieser Schritt ist erforderlich, um eine einwandfreie Authentifizierung zwischen Intune und Citrix Gateway sicherzustellen.

**Download-Skript:** Die ZIP-Datei enthält eine Readme-Datei mit Anweisungen zur Implementierung des Skripts. Sie müssen die Informationen, die die Skripte benötigen, manuell eingeben und das Skript auf dem Citrix Gateway ausführen, um den Dienst zu konfigurieren. Sie können die Skriptdatei von der Citrix Downloads-Seiteherunterladen.

> **Wichtig:** Nachdem Sie die Citrix Gateway-Konfiguration abgeschlossen haben und wenn Sie einen anderen OAuth-Status als COMPLETE sehen, lesen Sie den Abschnitt Fehlerbehebung.

### Konfigurieren des Microsoft Edge-Browsers

1. Melden Sie sich bei https://endpoint.microsoft.com/ an und navigieren Sie zu **Intune > Mobile Apps**.
2. Veröffentlichen Sie die Edge-App wie gewohnt und fügen Sie dann eine App-Konfigurationsrichtlinie hinzu.
3. Klicken Sie unter **Verwalten** auf **App-Konfigurationsrichtlinien**.
4. Klicken Sie auf **Hinzufügen** und geben Sie einen Namen für die Richtlinie ein, die Sie erstellen möchten. Wählen Sie unter **GeräteregistrierungstypVerwaltete Apps**aus.
5. Klicken Sie auf **Verknüpfte App**
6. Wählen Sie die Apps aus, auf die Sie die Richtlinie anwenden möchten (verwalteter Microsoft Edge- oder Intune-Browser), und klicken Sie dann auf **OK**.
7. Klicken Sie auf **Konfigurationseinstellungen**.
8. Geben Sie im Feld **Name** den Namen einer der in der folgenden Tabelle aufgeführten Richtlinien ein.
9. Geben Sie im Feld **Wert** den Wert ein, den Sie für diese Richtlinie anwenden möchten. Klicken Sie außerhalb des Felds, um die Richtlinie zur Liste hinzuzufügen. Sie können mehrere Richtlinien hinzufügen.
10. Klicken Sie auf **OK** und dann auf **Hinzufügen**.

Die Richtlinie wird der Liste hinzugefügt.

| Name (iOS/Android) | Wert | Beschreibung |
|---|---|---|
| MvpnGatewayAddress | `https://external.companyname.com` | Externe URL Ihres Citrix Gateway |
| MvpnNetworkAccess | MvpnNetworkAccessTunneledWebSSO oder Unrestricted | MvpnNetworkAccessTunneledWebSSO ist die Standardeinstellung für das Tunneln. |
| MvpnExcludeDomains | Kommagetrennte Liste der auszuschließenden Domainnamen | Optional. Default=blank |

> **Hinweis:** Web SSO ist der Name für Secure Browse in den Einstellungen. Das Verhalten ist dasselbe.

- **MvpnNetworkAccess** - MvpnNetworkAccessTunneledWebSSO ermöglicht die HTTP/HTTPS-Umleitung über das Citrix Gateway, auch bekannt als Tunneled-Web SSO. Das Gateway reagiert inline auf Herausforderungen bei der HTTP-Authentifizierung und bietet ein Single-Sign-On (SSO) -Erlebnis. Um Web SSO zu verwenden, legen Sie diese Richtlinie auf **MvpnNetworkAccessTunneledWebSSO**fest. Eine vollständige Tunnelumleitung wird derzeit nicht unterstützt. Verwenden Sie **Uneingeschränkt**, um das Micro-VPN-Tunneling ausgeschaltet zu lassen.
- **MvpnExcludeDomains** - Kommagetrennte Liste von Host- oder Domänennamen, die vom Routing durch den Citrix Gateway Reverse-Webproxy ausgeschlossen werden sollen. Die Host- oder Domänennamen werden ausgeschlossen, obwohl die von Citrix Gateway konfigurierten geteilten DNS-Einstellungen andernfalls die Domäne oder den Host auswählen könnten.

  > **Hinweis:**
  >
  > - Diese Richtlinie wird nur für **MvpnNetworkAccessTunneledWebSSO**-Verbindungen durchgesetzt. Wenn `MvpnNetworkAccess` auf **Unrestricted** gesetzt ist, wird diese Richtlinie ignoriert.
  > - Diese Richtlinie gilt nur für den getunnelten Web-SSO-Modus, bei dem NetScaler Gateway für Reverse-Split-Tunneling konfiguriert ist.

## Problembehandlung

### Allgemeine Probleme

| Problem | Auflösung |
| --- | --- |
| Die Meldung “Richtlinie hinzufügen erforderlich” wird angezeigt, wenn Sie eine App öffnen<br>Es gibt Richtlinienkonflikte | Hinzufügen von Richtlinien in der Microsoft Graph-API<br>Es ist nur eine einzige Richtlinie pro App zulässig |
| Die Meldung “App konnte nicht verpackt werden”wird beim Umschließen einer App angezeigt. Die vollständige Meldung finden Sie in der folgenden Tabelle | Die App ist in das Intune SDK integriert. Sie müssen die App nicht mit dem Intune umschließen |
| Ihre App kann keine Verbindung zu internen Ressourcen herstellen | Stellen Sie sicher, dass die richtigen Firewall-Ports geöffnet sind, Sie die Mandanten-ID korrigieren und so weiter |

**Fehler beim Packen der App-Fehlermeldung:**

*App konnte nicht verpackt werden. com.microsoft.intune.mam.apppackager.utils.AppPackagerException: Diese App hat das MAM*
*SDK bereits integriert.*
*com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113)*
*com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198)*
*com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56)*
*Die Anwendung darf nicht umschlossen sein.*

**Citrix Gateway-Probleme**

| Problem | Auflösung |
| --- | --- |
| Die Berechtigungen, die für die Gateway-App auf Azure konfiguriert werden müssen, sind nicht verfügbar. | Überprüfen Sie, ob eine Intune-Lizenz verfügbar ist. Versuchen Sie, das Portal manage.windowsazure.com zu verwenden, um festzustellen, ob die Berechtigung hinzugefügt werden kann. Wenden Sie sich an den Microsoft-Support, wenn das Problem weiterhin besteht. |

| Problem | Auflösung |
| --- | --- |
| Citrix Gateway kann nicht erreichen `login.microsoftonline.comandgraph.windows.net`. | Prüfen Sie von NS Shell aus, ob Sie die folgende Microsoft-Website erreichen können: cURL -v -k https://login.microsoftonline.com. Überprüfen Sie dann, ob DNS auf Citrix Gateway konfiguriert ist. Vergewissern Sie sich auch, dass die Firewall-Einstellungen korrekt sind (falls DNS-Anfragen durch eine Firewall gespeichert sind). |
| Ein Fehler erscheint in ns.log nachdem Sie OAuthAction konfiguriert haben. | Überprüfen Sie, ob die Intune-Lizenzierung aktiviert ist und die Azure Gateway-App über die richtigen Berechtigungen verfügt. |
| Der Befehl "OAuthAction"zeigt den OAuth-Status nicht als abgeschlossen an. | Überprüfen Sie die DNS-Einstellungen und Berechtigungen für die Azure Gateway-App. |
| Auf dem Android- bzw. iOS-Gerät wird die Zweifaktor-Authentifizierungsaufforderung nicht angezeigt. | Überprüfen Sie, ob das Zweifaktor-Geräte-ID-LogonSchema an den virtuellen Authentifizierungsserver gebunden ist. |

**Status und Fehlerzustand von Citrix Gateway OAuth**

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

**Hinweis:** Wenn der OAuth Status erfolgreich ist, wird der Status als COMPLETE angezeigt.

## Erweiterte Unterstützung für Azure AD Graph

March 27, 2024

Da Azure AD Graph veraltet ist, können Kunden, die eine neue Anwendung auslösen, die früheren Berechtigungen, die mit dem Azure AD-Diagramm verfügbar waren, nicht verwenden. Kunden mit vorhandenen Anwendungen, die die alten Berechtigungen von Azure AD Graph für einige Zeit verwenden möchten, können dies jedoch weiterhin tun, indem sie einige Konfigurationsänderungen auf der Gateway-Appliance vornehmen. Diese Konfiguration wird in Citrix Gateway Version 13.1-27.xx und höher unterstützt.

Führen Sie die folgenden Konfigurationsänderungen auf der Citrix Gateway-Appliance durch:

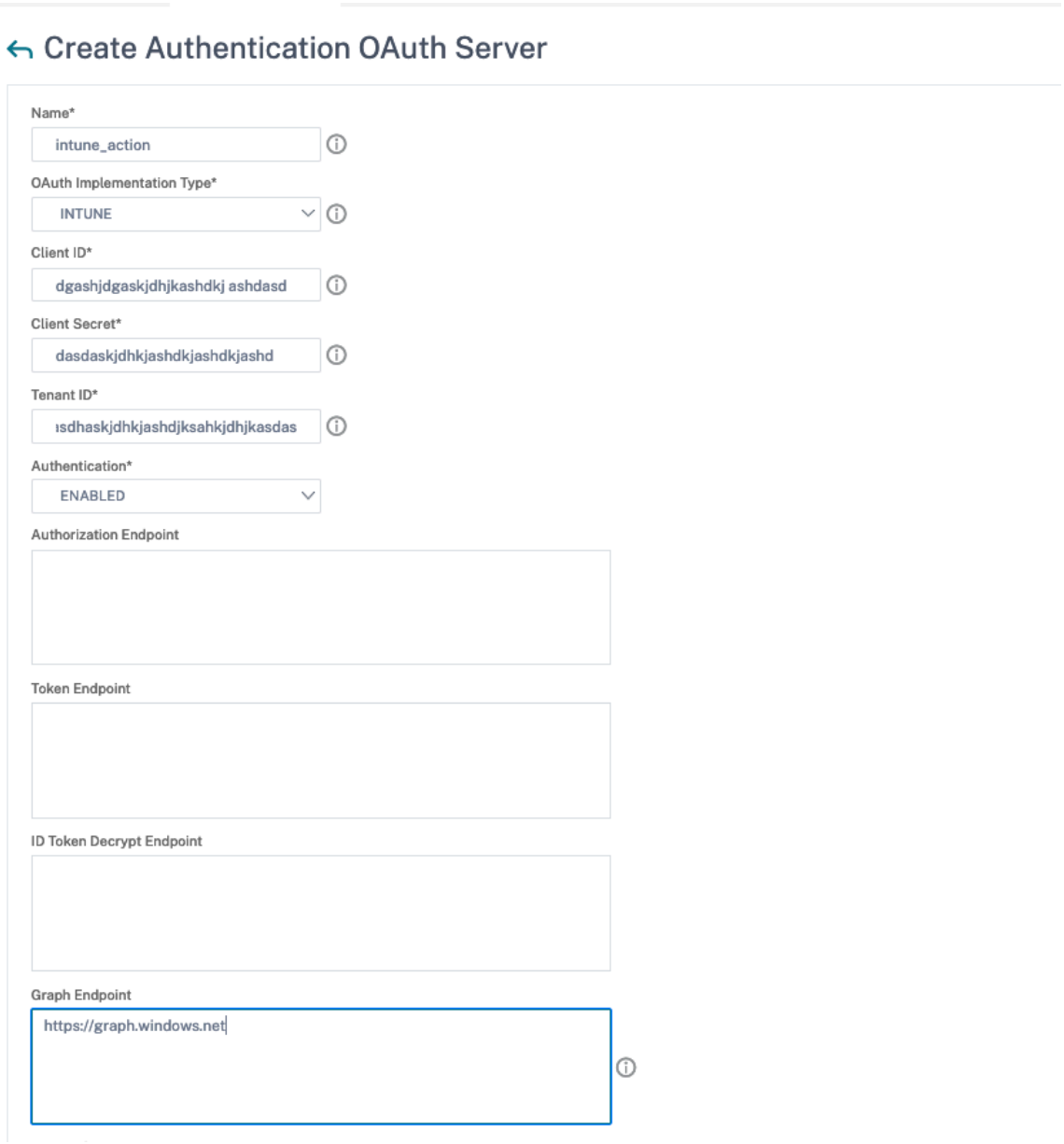
1. Führen Sie in der Eingabeaufforderung den folgenden Befehl aus.

```
shell nsapimgr_wr.sh -ys call=”ns_intune_enable_old_endpoints”
<!--NeedCopy-->
```

2. Navigieren Sie zu **Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > OAUTH-Aktionen**.

   a) Wählen Sie einen vorhandenen OAuth-Server aus.
   b) Klicken Sie auf **Mehr**.
   c) Stellen Sie in **Graph Endpoint**sicher, dass die URL wie die in der Abbildung angezeigte aussieht.




## HDX erleuchtete Unterstützung für Datentransport

March 27, 2024

Die Unterstützung von Enlightened Data Transport (EDT) für Citrix Gateway gewährleistet Benutzern, die die Citrix Workspace-App ausführen, eine hochauflösende Benutzererfahrung virtueller Desktops während der Sitzung.

Außerdem wird die Ende-zu-Ende-Verschlüsselung mit dem DTLS 1.0 für die EDT-Terminierung zwis-

chen der Citrix Workspace-App und VDA erleichtert. Weitere Informationen finden Sie unter Unterstützung für das DTLS-Protokoll.

EDT-fähiges Citrix Gateway bietet eine gute Benutzererfahrung sowohl unter LAN- als auch WAN-Bedingungen. Mit EDT benötigen Sie keine Verwaltungs- oder Benutzerkonfiguration, wenn Sie von einem zum anderen roamen. Der Vorteil zeigt sich am deutlichsten in Netzwerken mit hoher Latenz und moderatem Paketverlust, in denen die Benutzererfahrung im Allgemeinen bei Alternativen zurückbleibt.

## Wann sollte die Unterstützung für den Enlightened Data Transport verwendet werden

March 27, 2024

Die folgenden Szenarien veranschaulichen die Verwendung von EDT-fähiger Citrix Gateway.

- Ein Benutzer möchte ein Erlebnis so gut wie in einer LAN-Umgebung, während er remote auf Geschäftsressourcen zugreift.
- Ein Benutzer möchte eine reichhaltige virtuelle Anwendung und Desktop-Benutzererfahrung in Wi-Fi und Mobilfunknetzen, in denen die Netzwerkqualität aufgrund von Überlastung, hohem Paketverlust und hoher Latenz schlecht ist.

Die folgenden Punkte sind bei der Verwendung von EDT zu beachten.

- Der DTLS-Regler auf der Ebene des virtuellen Servers ist standardmäßig aktiviert.
- IPv6 mit DTLS wird nicht unterstützt.
- Die Appliance kann jetzt für Double-Hop-Funktionalität für EDT-Verkehr zwischen Receiver und VDA konfiguriert werden. Weitere Informationen erhalten Sie, indem Sie auf In einer Double-Hop-DMZ bereitstellenklicken.

**Hinweis:** EDT wird auf der MPX FIPS-Plattform in Version 12.1 Build 49.xx und höher unterstützt. Auf den Intel Coleto SSL-Chip-basierten MPX-Geräten wird EDT ab Version 12.1 Build 51.16 und höher unterstützt.

## Konfigurieren von Citrix Gateway zur Unterstützung von Enlightened Data Transport und HDX Insight

March 27, 2024

Der EDT-Verkehr durch Gateway ist jetzt durchgängig sichtbar. Die Verfügbarkeit von Echtzeit- und historischen Sichtbarkeitsdaten ermöglicht es Citrix ADM, eine Vielzahl von Anwendungsfällen zu unterstützen.

Die folgenden Szenarien werden unterstützt:

| Szenario | EDT Support |
|---|---|
| Citrix Gateway | Ja |
| Citrix Gateway mit Hochverfügbarkeit (HA) | Ja |
| Citrix Gateway mit Optimierung für Hochverfügbarkeit (HA) | Ja |
| Citrix ADC mit Unified Gateway | Ja |
| Citrix Gateway mit GSLB | Ja |
| Citrix Gateway mit Cluster | Ja |
| Citrix Workspace-App auf Citrix Gateway DTLS-Verschlüsselung | Ja |
| Dual Secure Ticket Authority (STA) auf Citrix Gateway | Ja |
| Citrix Gateway ICA-Sitzungstimeout | Ja |
| Citrix Gateway Multistream-ICA | Nein |
| Citrix Gateway-Sitzungszuverlässigkeit (Port 2598) | Ja |
| Citrix Gateway Doppel-Hop | Ja |
| Citrix ADC zu VDA DTLS-Verschlüsselung | Ja |
| HDX Insight | Ja |
| Citrix Gateway im IPv6-Modus | Nein |
| Citrix Gateway SOCKS (Port 1494) | Nein |
| Citrix ADC reiner LAN-Proxy (siehe Hinweis) | Nein |

> **Hinweis:**
>
> EDT wird nicht unterstützt, wenn der Citrix ADC LAN-Proxy im LAN-Benutzermodus oder im transparenten Modus konfiguriert ist. TCP wird jedoch unterstützt. Weitere Informationen:

- Konfigurieren des ausgehenden ICA-Proxy
- Erfassung von HDX Insight Analytics für LAN-Benutzer mit Citrix ADC mithilfe von SOCKS

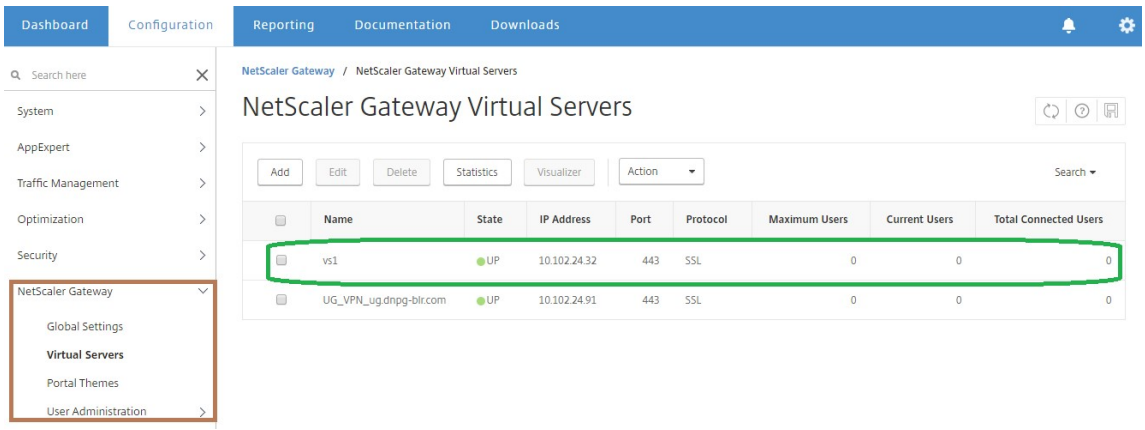
## Konfigurieren Sie Citrix Gateway für die Unterstützung von Enlightened Data Transport

Wenn Sie Enlightened Data Transport (EDT) verwenden, muss Datagram Transport Layer Security (DTLS) aktiviert sein, um die von EDT verwendete UDP-Verbindung zu verschlüsseln. Der DTLS-Parameter muss auf der Ebene des virtuellen Gateway-VPN-Servers aktiviert sein. Außerdem müssen die Komponenten von Citrix Virtual Apps and Desktops ordnungsgemäß aktualisiert und konfiguriert werden, um verschlüsselten Datenverkehr zwischen dem virtuellen Gateway-VPN-Server und dem Benutzergerät zu erreichen.

> **Hinweis:** Der für den virtuellen Citrix Gateway-Front-End-Server konfigurierte UDP-Port (z. B. Port 443) muss in der DMZ geöffnet werden, damit der virtuelle Server die DTLS-Verbindungen empfangen kann. DTLS und CGP sind Voraussetzungen dafür, dass EDT mit Citrix Gateway kompatibel ist.

### So konfigurieren Sie Citrix Gateway für die Unterstützung von EDT über die GUI

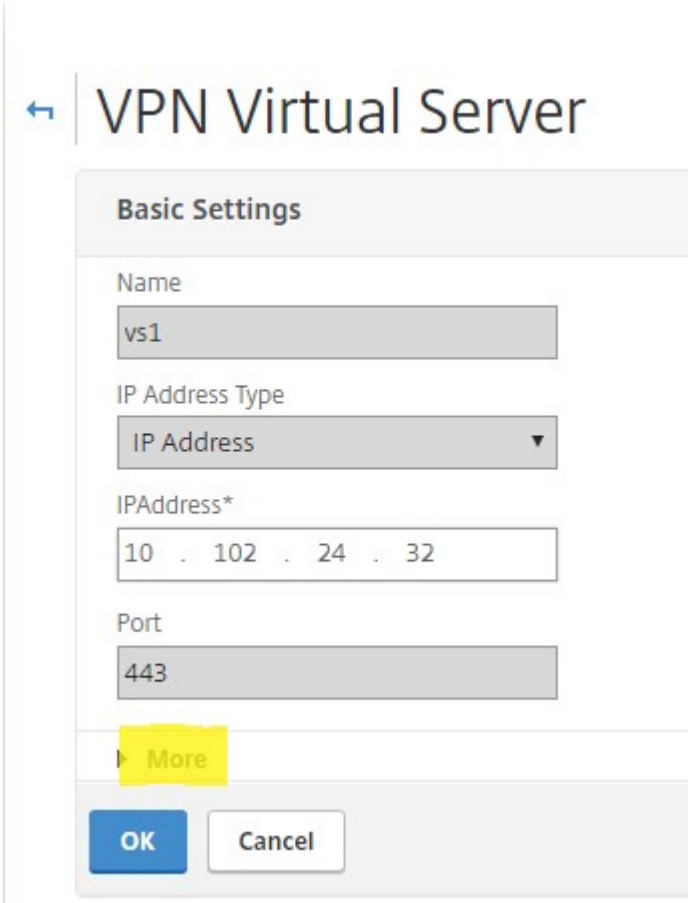
1. Stellen Sie Citrix Gateway bereit und konfigurieren Sie es für die Kommunikation mit StoreFront und zur Authentifizierung der Benutzer von Citrix Virtual Apps and Desktops.
2. Erweitern Sie auf der Registerkarte Konfiguration in der Citrix ADC GUI **Citrix Gateway** und wählen Sie **Virtuelle Server**aus.




3. Klicken Sie auf **Bearbeiten**, um die Grundeinstellungen für den virtuellen VPN-Server anzuzeigen, und überprüfen Sie dann den Status der DTLS-Einstellung.

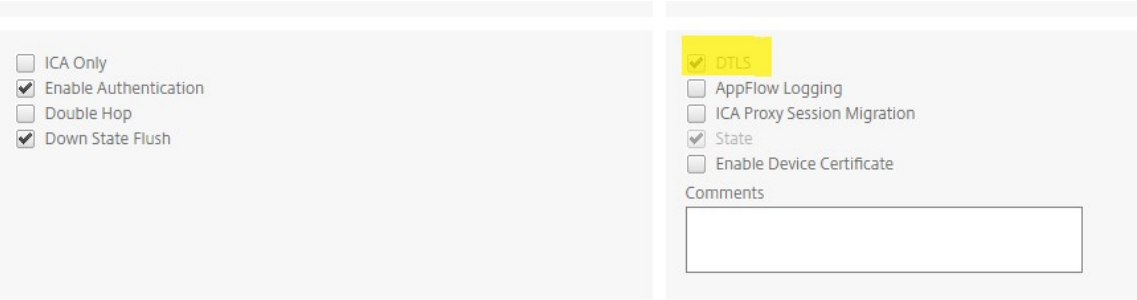
 


4. Klicken Sie auf **Mehr**, um weitere Konfigurationsoptionen anzuzeigen.



5. Wählen Sie **DTLS** aus, um Kommunikationssicherheit für Datagramm-Protokolle zu gewährleisten. Klicken Sie auf **OK**. Der Bereich **Grundeinstellungen** für den virtuellen VPN-Server zeigt, dass das DTLS-Flag auf **True**gesetzt ist.




#### So konfigurieren Sie Citrix Gateway für EDT-Unterstützung mithilfe von CLI

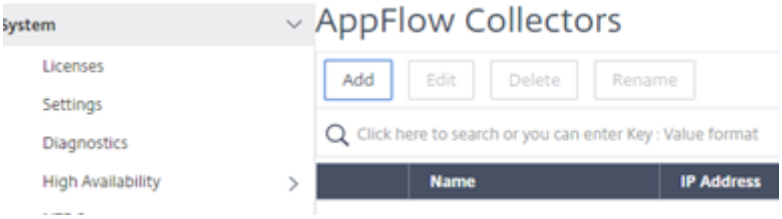
```
set vpn vserver vs1 -DTLS ON
```

### Konfigurieren Sie Citrix Gateway für die Unterstützung von HDX Insight

HDX Insight bietet End-to-End-Sichtbarkeit für HDX-Verkehr zu virtuellen Apps und Desktops, die Citrix ADC durchlaufen. Außerdem können Administratoren Client- und Netzwerklatenzmetriken in Echtzeit, historische Berichte, End-to-End-Leistungsdaten anzeigen und Leistungsprobleme beheben.

#### So konfigurieren Sie Citrix Gateway für die Unterstützung von HDX Insight über die GUI

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System> AppFlow> Collectors**und klicken Sie auf **Hinzufügen**.




2. Füllen Sie auf der Seite **AppFlow Collector erstellen** die folgenden Felder aus und klicken Sie auf **Erstellen**.
   Name —Name für den Sammler

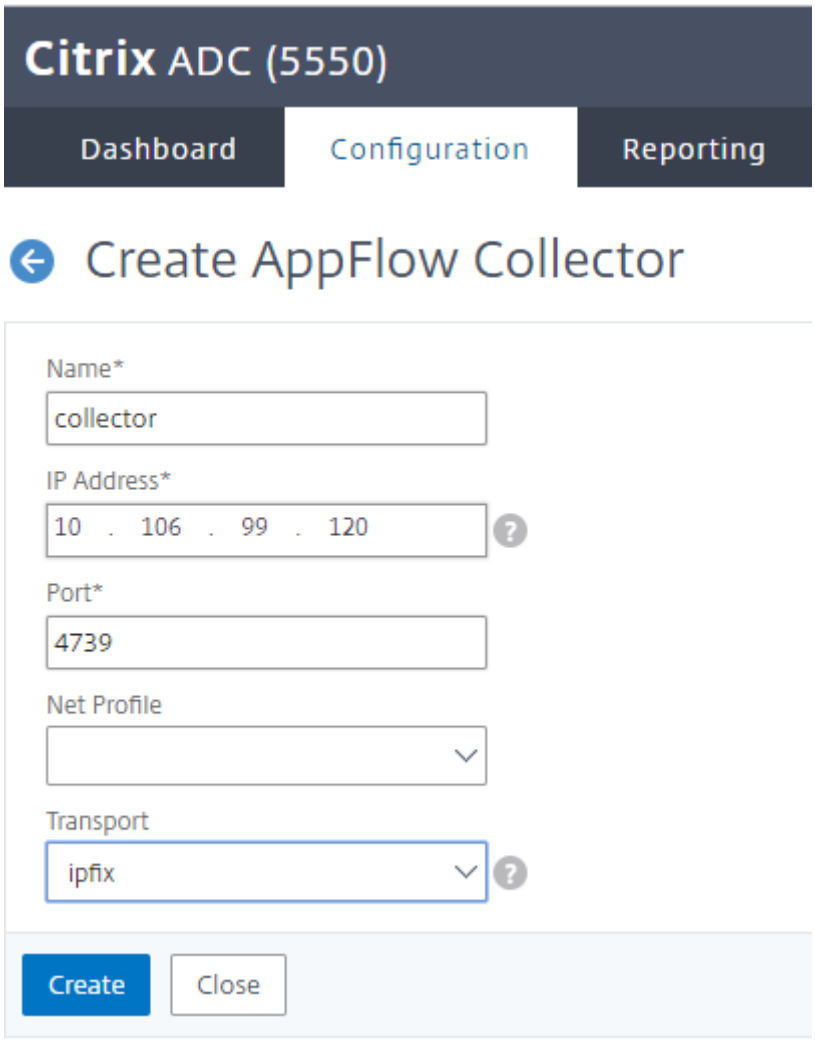
   IP-Adresse —IPv4-Adresse des Collectors

   Port —Port, den der Collector abhört

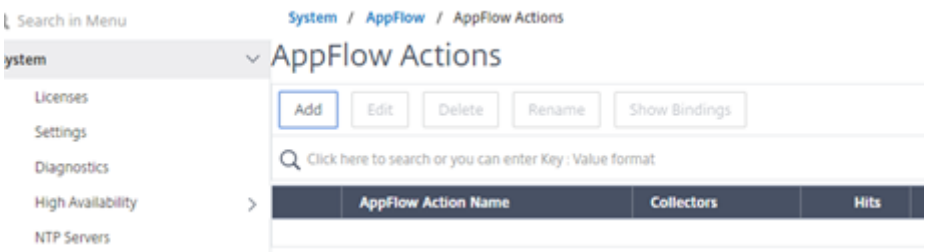
 

Netzprofil - Netzprofil, das mit dem Collector verknüpft werden soll. Die im Profil definierte IP-Adresse wird als Quell-IP-Adresse für den AppFlow-Verkehr für diesen Collector verwendet. Wenn Sie diesen Parameter nicht festlegen, wird die Citrix ADC IP (NSIP) -Adresse als Quell-IP-Adresse verwendet.

Transport —Transporttyp des Kollektors.




3. Navigieren Sie zu **System> AppFlow> Aktionen**und klicken Sie auf **Hinzufügen**.




4. Füllen Sie auf der Seite **AppFlow-Aktion erstellen** die folgenden Felder aus und klicken Sie auf

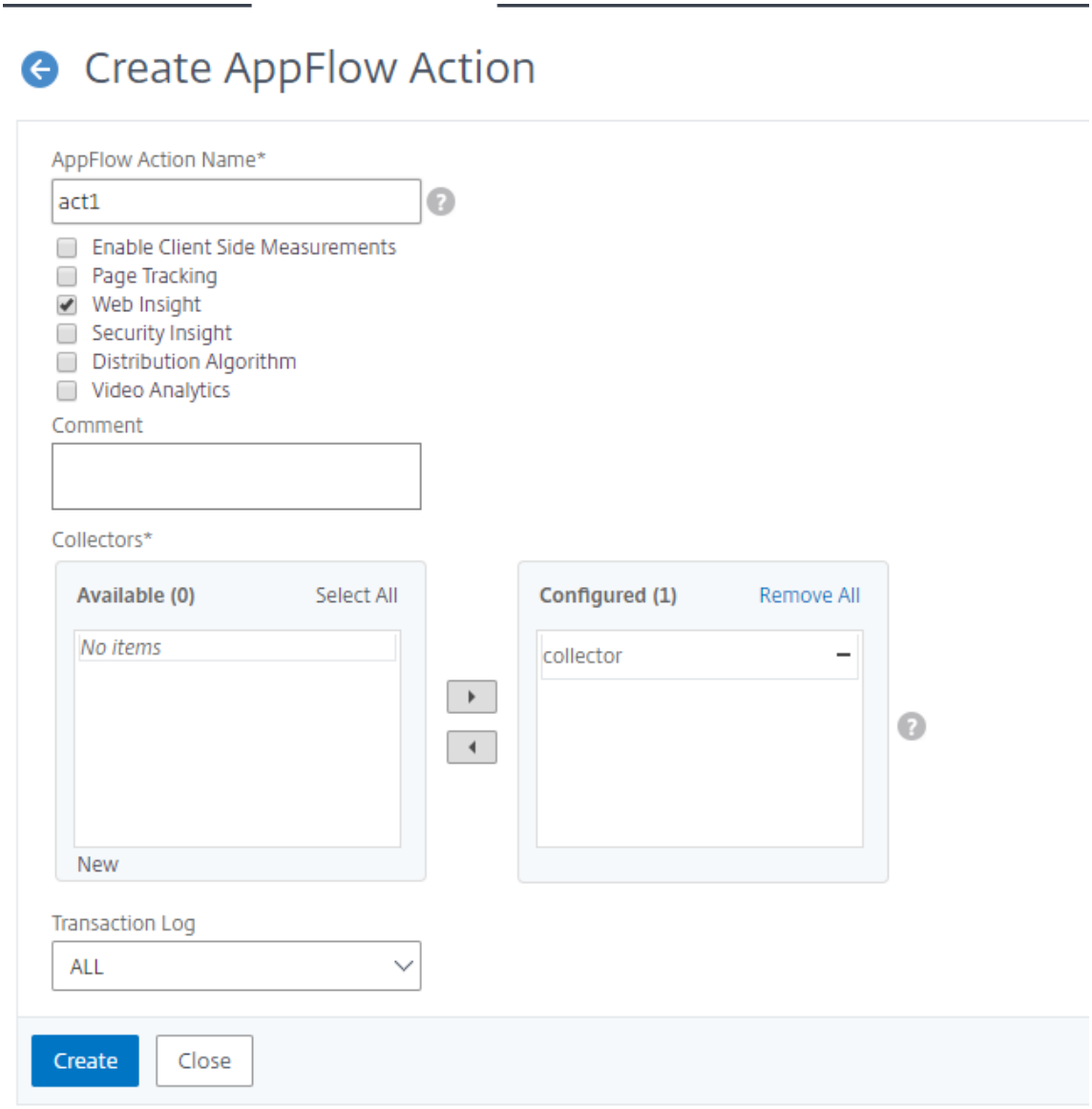
**Erstellen**.

AppFlow-Aktionsname —Name für die Aktion

Kommentar —Jeder Kommentar zur Aktion

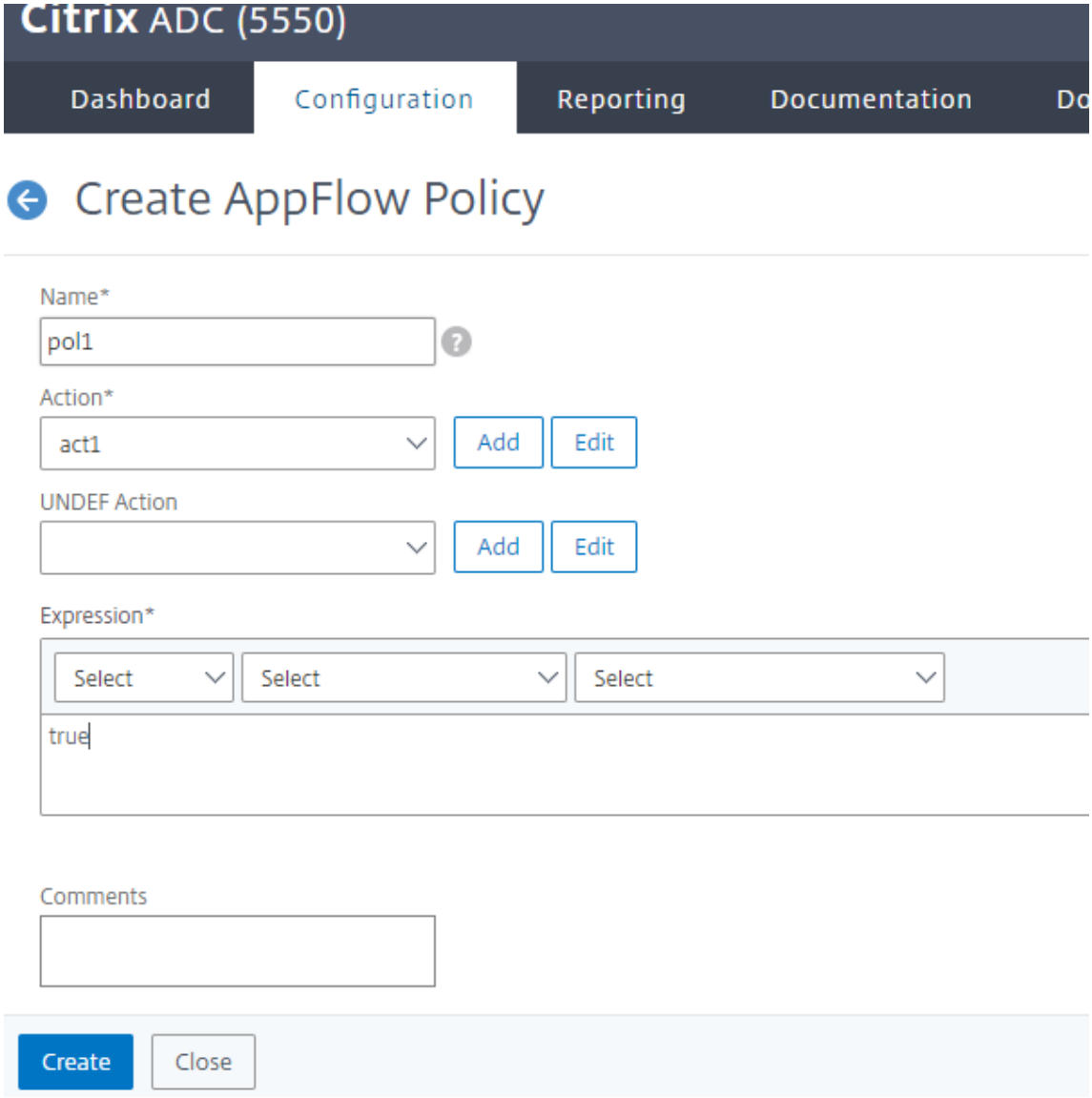
Collector —Wählen Sie die Namen der Collectors aus, die mit der AppFlow-Aktion verknüpft werden sollen.

Transaktionslog —Zu protokollierende Transaktionstyp.




5. Navigieren Sie zu **System > AppFlow> Richtlinien**und klicken Sie auf **Hinzufügen**.




6. Füllen Sie auf der Seite **AppFlow-Richtlinie erstellen** die folgenden Felder aus und klicken Sie auf **Erstellen**.

   Name —Name für die Richtlinie.

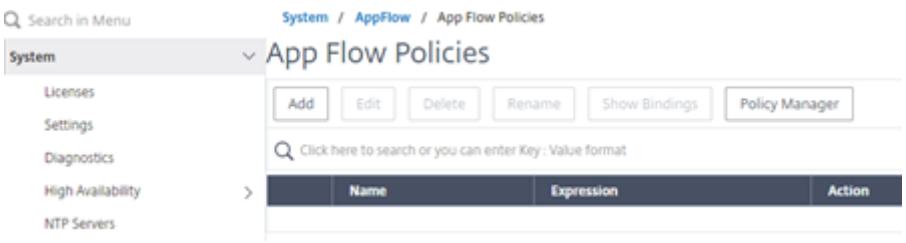
   Aktion —Name der Aktion, die mit der Richtlinie verknüpft werden soll.

   UNDEF - Name der AppFlow-Aktion, die dieser Richtlinie zugeordnet werden soll, wenn ein undefiniertes Ereignis eintritt.

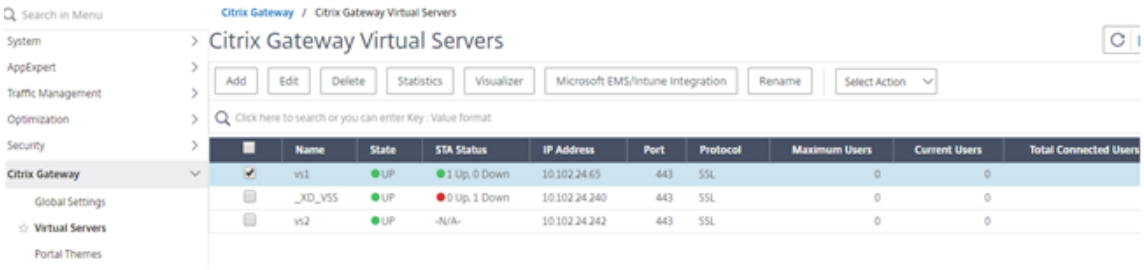
   Ausdruck - Ausdruck oder anderer Wert, für den der Verkehr ausgewertet wird. Muss ein boolescher Ausdruck sein.

   Kommentare - Irgendwelche Kommentare zu dieser Richtlinie.



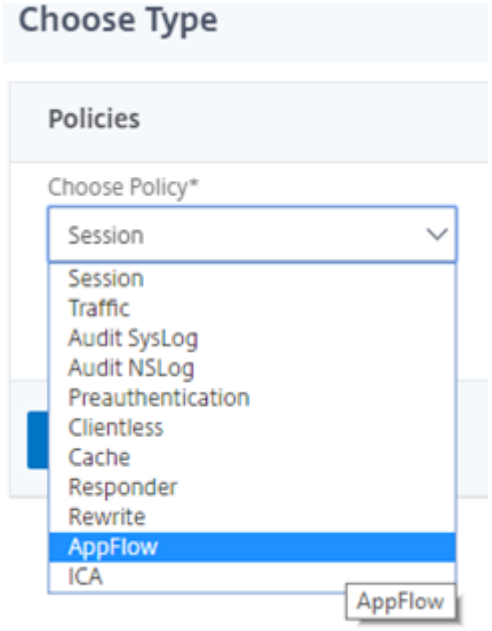

7. Navigieren Sie zu **Citrix Gateway> Virtuelle Server**, wählen Sie den virtuellen Server aus und klicken Sie auf **Bearbeiten**.



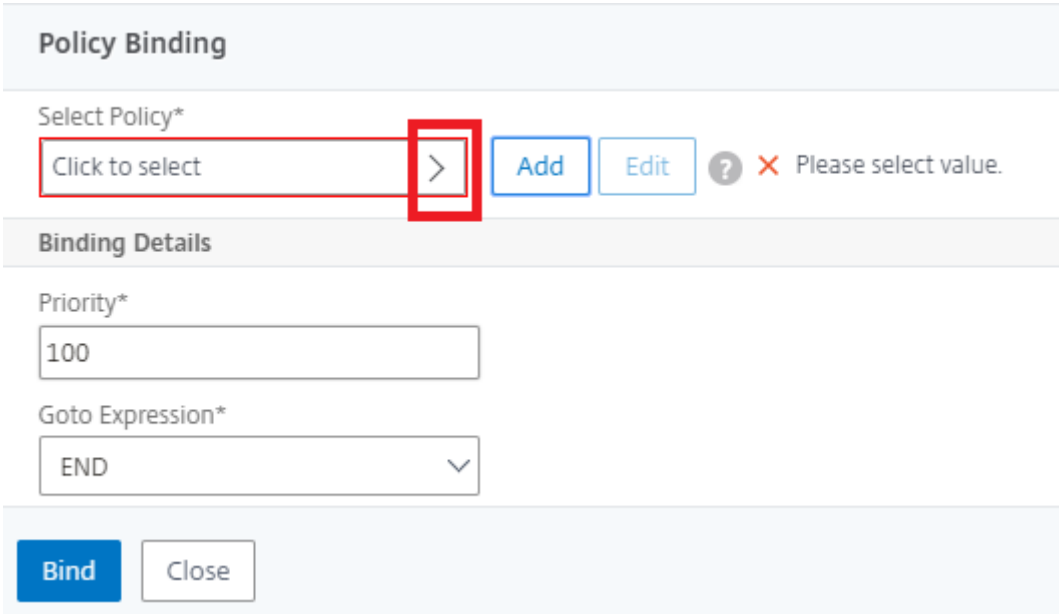

8. Scrollen Sie auf der Seite **VPN Virtual Server** nach unten und klicken Sie im Abschnitt **Richtlinien** auf **+**.


9. **Wählen Sie auf dem Bildschirm Typwählen im Dropdownmenü Richtlinie**wählen**AppFlow**aus.**Wählen Sie im Dropdownmenü Typ wählen**die Option**Request**oder**ICA-Anfrage**und klicken Sie auf**Weiter**.

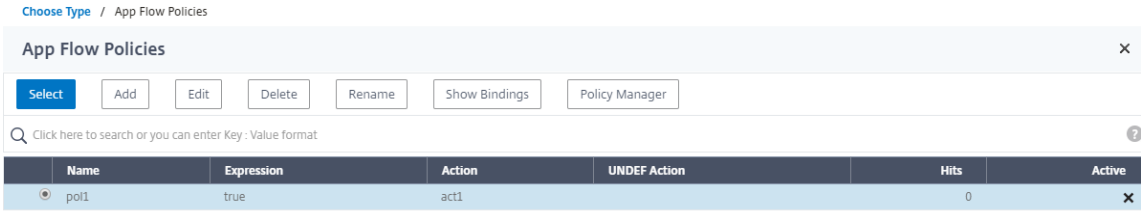
 




10. Klicken Sie unter **Richtlinie auswählen**auf den markierten Pfeil.

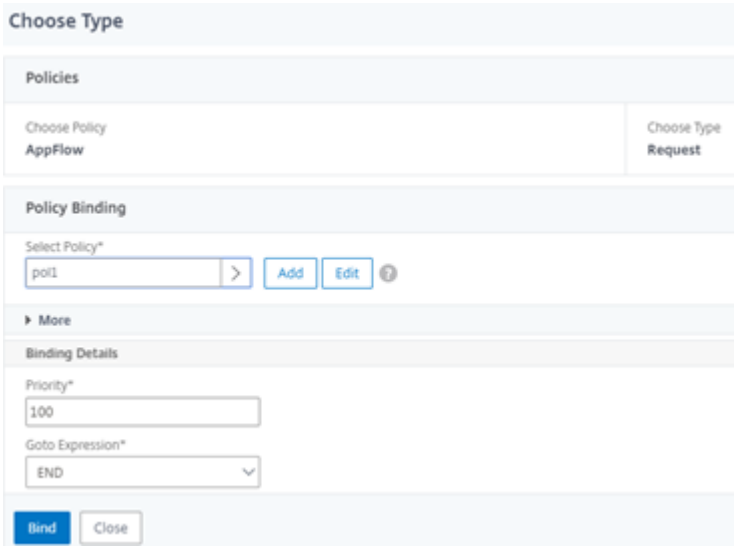



11. Wählen Sie die **AppFlow-Richtlinie** aus und klicken Sie auf **Auswählen**.




12. Klicken Sie abschließend auf **Bind**.




**Um Citrix Gateway für HDX Insight-Unterstützung über die CLI zu konfigurieren, geben Sie den folgenden Befehl ein**

```
add appflow collector col3 -IPAddress<ip_mas>
add appflow action act1 <action_name>
add appflow policy <policy_name> true <action_name>
bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END -
    type <ICA_Request>
```

### Deaktivieren Sie HDX Insight für Nicht-NSAP-HDX-Sitzung

In einer Citrix ADC Appliance können Sie HDX Insight jetzt für die Nicht-NSAP-HDX-Sitzungen deaktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
set ica parameter HDXInsightNonNSAP (YES | NO )
<!--NeedCopy-->
```

Standardmäßig ist HDX Insight für Nicht-NSAP-Sitzungen aktiviert.

## L7-Latenz-Schwellenwert

March 27, 2024

Die L7-Latenzgrenzwertfunktion in HDX Insight erkennt aktiv End-to-End-Probleme mit der Netzwerklatenz auf Anwendungsebene und ergreift proaktive Maßnahmen.  Die L7-Latenzgrenzwertfunktion

führt eine Live-Latenzüberwachung durch, um die Spitzen zu erkennen, und sendet Benachrichtigungen an HDX Insight, wenn die Latenz die minimal beobachtete Latenz überschreitet.

Zuvor wurden durchschnittliche clientseitige und serverseitige L7-Latenzwerte alle 60 Sekunden an HDX Insight gesendet. Alle innerhalb dieses Intervalls beobachteten Spitzen wurden gemittelt und blieben daher unentdeckt. Außerdem gab es keine Live-Latenzüberwachung, um diese Spitzen zu erkennen.

### Wie unterscheidet sich die L7-Latenz von der L4-Latenz

Netzwerklatenzen werden ebenfalls auf L4-Ebene erfasst und angezeigt. Diese Latenzen werden aus der TCP-Schicht berechnet und erfordern kein Parsen des ICA-Datenverkehrs. Daher sind sie relativ einfach zu beschaffen und weniger CPU-intensiv. Der Hauptnachteil der L4-Latenz besteht jedoch darin, die Ende-zu-Ende-Latenz zu verstehen. Wenn der Pfad TCP-Proxys enthält, erfasst die L4-Latenz nur die Latenz vom Citrix ADC zum TCP-Proxy. Dies kann zu unvollständigen Informationen führen und daher zu Schwierigkeiten beim Debuggen des Problems führen.

Die L7-Latenz wird durch Parsen des ICA-Datenverkehrs berechnet. Die L7-Latenzberechnung erfolgt auf der ICA-Schicht, und daher führen Zwischenproxys nicht zu unvollständigen Latenzwerten. Somit bietet eine Ende-zu-Ende-Latenzerkennung.

Die folgenden Abbildungen zeigen einen Bereitstellungstyp mit und ohne TCP-Proxys.

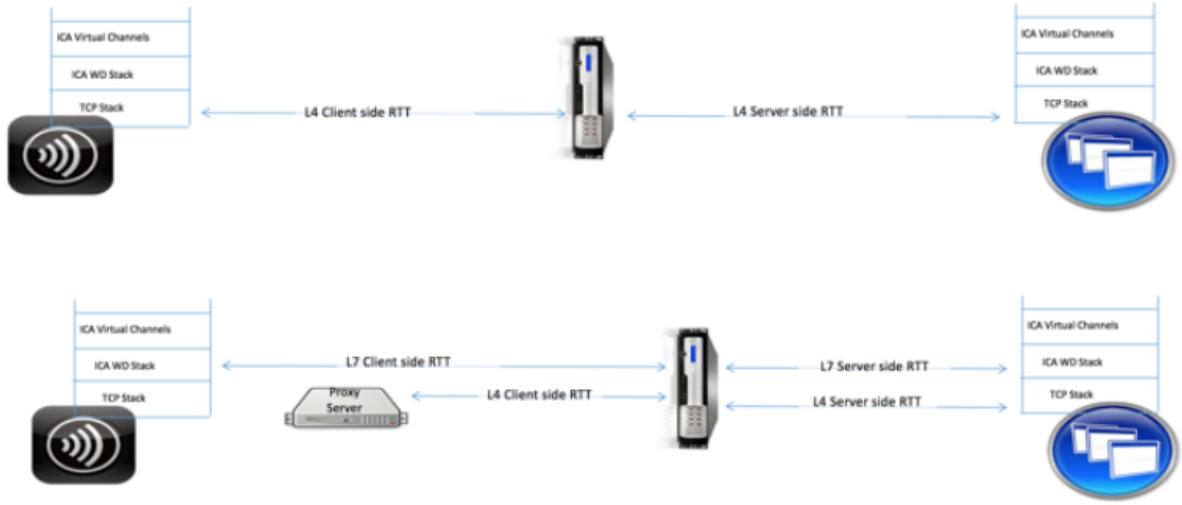



*Fig 2. Deployment with TCP Proxies*

### Unterschied zwischen ICA RTT- und L7-Latenzberechnungen

ICA RTT stellt die gesamte Roundtrip-Zeit von der Citrix Workspace-App zum Virtual Delivery Agent (VDA) dar. Die L7-Latenz liefert detaillierte Details zu Latenzen auf der Client- und Serverseite. Die L7-

Clientlatenz ist die Latenz zwischen der Citrix Workspace-App und Citrix Gateway. Die L7-Serverlatenz ist die Latenz zwischen Citrix Gateway und VDA.

> **Hinweis**: Die serverseitige L7-Latenzberechnung für den Server wird nur für die Citrix Virtual Apps and Desktops Version 7.13 und höher unterstützt.

### Konfigurieren Sie den L7-Latenzschwellenwert über die CLI

1. Fügen Sie ein ICA-Latenzprofil hinzu.

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
    DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
    l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
     <positive_integer>] [-l7LatencyMaxNotifyCount <
    positive_integer>]
<!--NeedCopy-->
```

2. Fügen Sie eine ICA-Aktion hinzu.

```
add ica action <name> [-latencyprofileName <string>]
<!--NeedCopy-->
```

3. Eine ICA-Richtlinie hinzufügen.

```
add ica policy <name> -rule <expression> -action <string> [-
    comment<string>] [-logAction <string>
<!--NeedCopy-->
```

4. Binden Sie die ICA-Richtlinie an den VPN-Server oder den globalen ICA-Bindpunkt

```
bind ica global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>] [-type (
    ICA_REQ_OVERRIDE | ICA_REQ_DEFAULT )]
<!--NeedCopy-->
```

Oder

```
bind vpn vserver <name> -policy <string>  [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Oder

```
bind cr vserver <name> -policy <string> [-priority <positive
    _integer>]
<!--NeedCopy-->
```

**Argumente**

- **Latenzüberwachung**: Parameter zum Aktivieren oder Deaktivieren der L7-Schwellenwertüberwachung. Wenn dieser Parameter aktiviert ist, werden Benachrichtigungen an HDX Insight gesendet, wenn die festgelegten Bedingungen erfüllt sind.

  Standardwert: DISABLED

- **LatencyThresholdFactor**: Faktor, um den die aktive Latenz größer als die beobachtete Mindestlatenz sein muss, um zu schließen, dass der Schwellenwert überschritten wird und daher eine Benachrichtigung an HDX Insight gesendet werden muss.

  Standardwert: 4

  Mindestwert: 2

  Maximaler Wert: 65535

- **LatencyWaitTime: Zeit**in Sekunden, die die Appliance warten muss, nachdem der Latenzschwellenwert überschritten wurde, um eine Benachrichtigung an HDX Insight zu senden.

  Standardwert: 20

  Mindestwert: 1

  Maximaler Wert: 65535

- **latencyNotifyInterval: Zeitintervall**in Sekunden, in dem die Appliance nach Ablauf der Wartezeit nachfolgende Benachrichtigungen an HDX Insight sendet.

  Standardwert: 20

  Mindestwert: 1

  Maximaler Wert: 65535

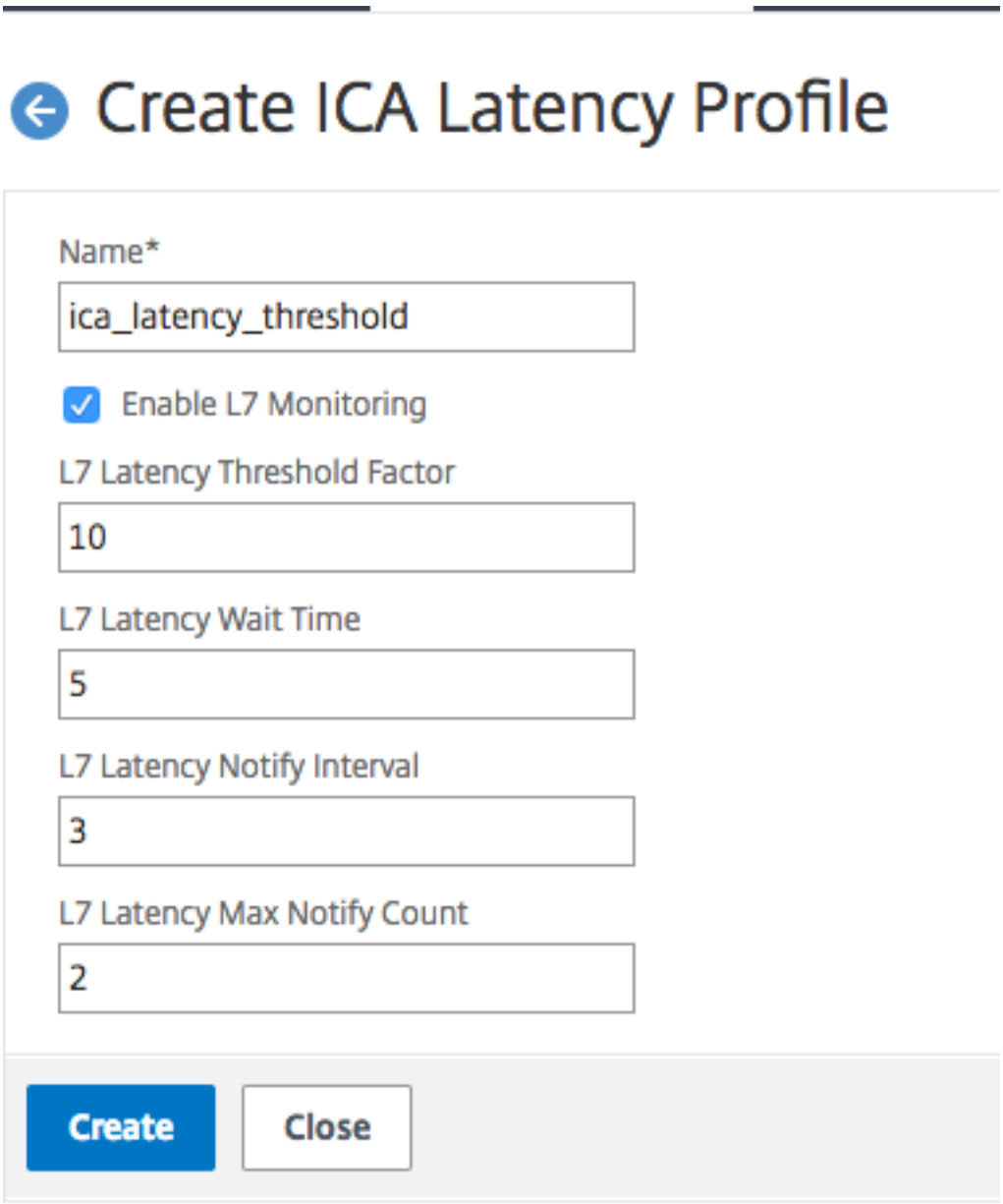
- **LatencyMaxNotifyCount**: Maximale Anzahl von Benachrichtigungen, die innerhalb eines Intervalls, in dem die Latenz über dem Schwellenwert liegt, an HDX Insight gesendet werden können.

  Standardwert: 5

## Konfigurieren Sie den L7-Latenzschwellenwert über die GUI

1. Navigieren Sie zu **Konfiguration** > **NetScaler Gateway** > **Richtlinien** > **ICA**.
2. Wählen Sie die Registerkarte **ICA-Latenzprofile** und klicken Sie auf **Hinzufügen**.
3. Führen **Sie auf der Seite ICA-Latenzprofil erstellen** die folgenden Schritte aus.




- Wählen Sie **L7-Latenzüberwachung**, um die L7-Schwellenwertüberwachung zu aktivieren.
- Geben Sie im Feld **L7-Schwellenwertfaktor**den Wert ein, um den die aktive Latenz die beobachtete Mindestlatenz überschreiten muss, um eine Benachrichtigung an HDX Insight zu senden.
- Geben Sie unter **L7-Latenzwartezeit**die Zeit in Sekunden ein, die die Appliance warten soll, nachdem der Schwellenwert überschritten wurde, um eine Benachrichtigung an HDX Insight zu senden.
- Geben Sie im **L7-Latenzbenachrichtigungsintervall**die Zeit in Sekunden ein, zu der die Appliance nach Ablauf der Wartezeit nachfolgende Benachrichtigungen an HDX Insight

senden soll.

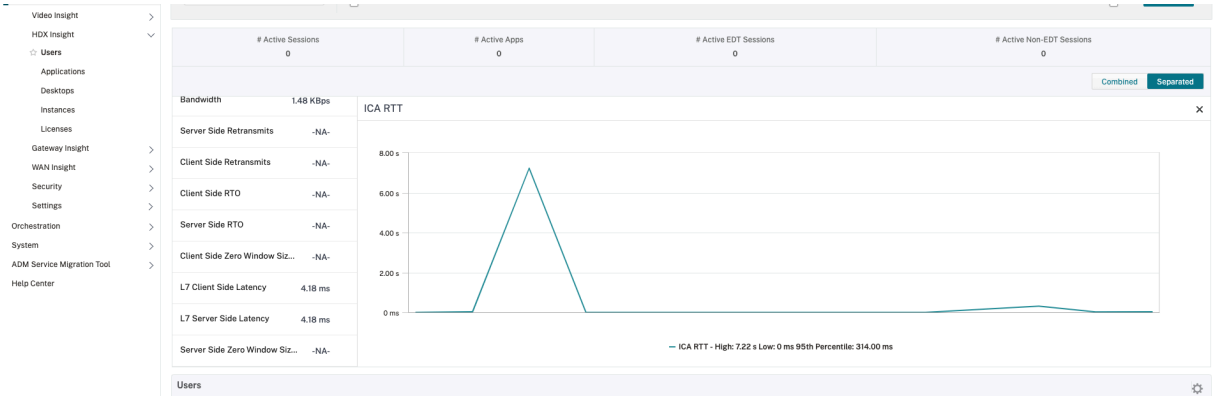
- Geben Sie im Feld **L7 Latency Maximum Notify Count**die maximale Anzahl von Benachrichtigungen ein, die innerhalb eines Intervalls, in dem die Latenz über dem Schwellenwert liegt, an HDX Insight gesendet werden können.
  **Hinweis:** Die Anzahl der maximalen Benachrichtigungen der L7-Latenz ist anwendbar, sobald der Schwellenwert überschritten wurde, und wird zurückgesetzt, wenn die aktive Latenz unter den Schwellenwert fällt. Die Periodizität dieser Benachrichtigungen wird durch das Benachrichtigungsintervall geregelt.

4. Klicken Sie auf **Erstellen**.

> **Wichtig:**
>
> Nachdem Sie die Parameter für den L7-Latenzschwellenwert konfiguriert haben, müssen Sie HDX Insight konfigurieren. Einzelheiten finden Sie unter Konfigurieren von Citrix Gateway für die Unterstützung von HDX Insight.

### Anzeigen von L7-Latenzparametern in Citrix ADM

Um die L7-Latenzparameter in Citrix ADM anzuzeigen, navigieren Sie zu **Analytics > HDX Insight > Anwendungen** oder **Analytics > HDX Insight > Benutzer**.




## Parameter zur Angabe eines Zeitintervalls für die Berechnung des L7-Client-Latenzwerts

Ab Citrix ADC Version 13.0 Build 83.17 und höher können Sie ein Zeitintervall in Sekunden angeben, für das der L7-Clientlatenzwert berechnet werden soll. Diese Konfiguration ist erforderlich, wenn Sie die L7-Latenz aktiviert haben und die ICA-Latenz einer Sitzung fälschlicherweise mit 64.000 ms aufgezeichnet wird.

### So legen Sie die Latenzfrequenz mit der CLI fest

Geben Sie an der Eingabeaufforderung;

```
set ica parameter -L7LatencyFrequency <positive_integer>
<!--NeedCopy-->
```

Beispiel:

```
set ica parameter -L7LatencyFrequency 5
<!--NeedCopy-->
```

Um die L7-Latenzfrequenz anzuzeigen, geben Sie in der Befehlszeile Folgendes ein:

```
show ica parameter
<!--NeedCopy-->
```

Um die L7-Latenzfrequenz zu deaktivieren oder zu deaktivieren, geben Sie in der Befehlszeile Folgendes ein:

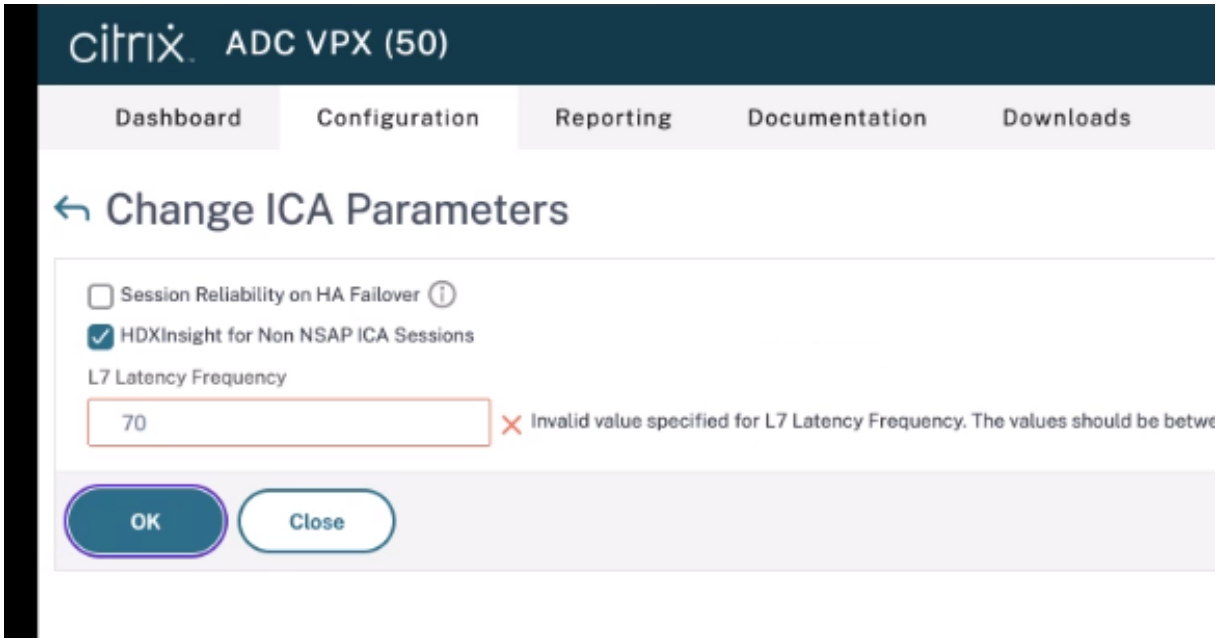
```
unset ica parameter -L7LatencyFrequency
<!--NeedCopy-->
```

**Hinweis:** Standardmäßig wird die L7-Client-Latenz für jedes Paket berechnet. Der Standardwert des Parameters `L7LatencyFrequency` ist 0, der Mindestwert 0 und der Höchstwert ist 60.

### So legen Sie die Latenzfrequenz mit der CLI fest

1. Navigieren Sie zu **System > Einstellungen > ICA-Parameter ändern**.
2. Geben Sie im Feld **L7-Latenzfrequenz** das Zeitintervall ein, für das der L7-Client-Latenzwert berechnet werden soll.



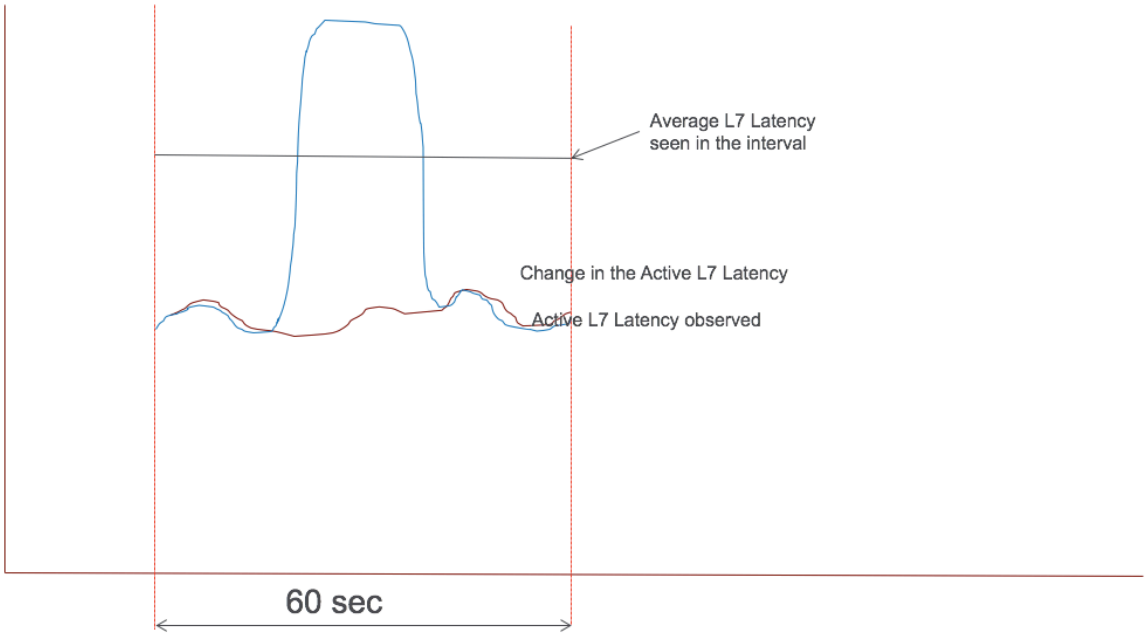

## Das L7-Latenzmessmodell im Vergleich zum Berichtsmodell für den L7-Latenzschwellenwert

### Das L7-Latenz-Messmodell

Im L7-Latenzmessmodul werden die durchschnittlichen clientseitigen und serverseitigen L7-Latenzwerte alle 60 Sekunden an HDX Insight gesendet. Infolgedessen werden die innerhalb dieses Intervalls beobachteten Spitzen gemittelt und bleiben daher unentdeckt. Außerdem verfügt das L7-Latenzmessmodul nicht über die Live-Latenzüberwachung.

Die folgende Abbildung zeigt ein Beispiel für ein L7-Latenzmessmodell.



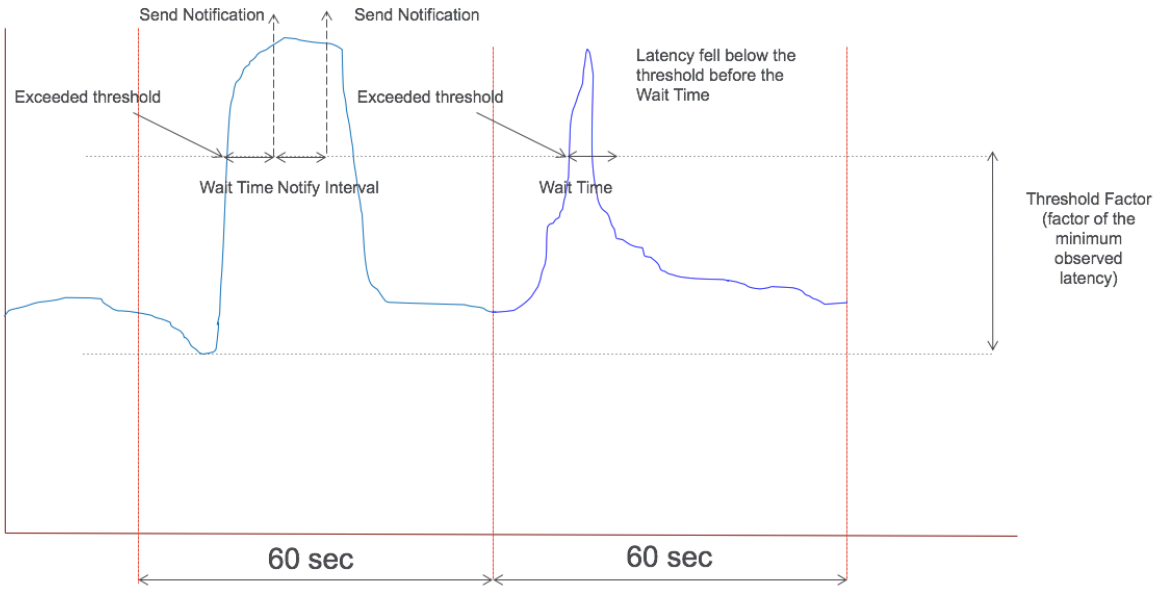

**L7-Latenz-Schwellenwert-Berichtsmodell**

Das L7-Latenzschwellenwert-Berichtsmodell verfügt über die Live-Latenzüberwachung, um Spitzen zu erkennen. Benachrichtigungen werden an HDX Insight gesendet, wenn die Latenz die beobachtete Mindestlatenz überschreitet.

Immer wenn ein Schwellwertfaktor überschritten wird, wird die Latenzerhöhung erkannt. Nachdem die konfigurierte Wartezeit für den Schwellenwert abgelaufen ist, wird eine Benachrichtigung an HDX Insight gesendet. Eine nachfolgende Benachrichtigung wird an HDX Insight gesendet, nachdem die Wartezeit abgelaufen ist und der Schwellenwertfaktor immer noch überschritten wurde.
Falls der Latenzwert vor Ablauf der Wartezeit unter den Schwellenwertfaktor fällt, wird keine Benachrichtigung an HDX Insight gesendet.

Die folgende Abbildung veranschaulicht ein Beispiel für ein Berichtsmodell für L7-Latenzschwellen.




Die folgenden Parameter können zur Laufzeit konfiguriert werden:

- Schwellenwertüberwachung (EIN/AUS)
- Schwellenwertfaktor
- Wartezeit für Schwellenwerte
- Intervall für Benachrichtigungen
- Maximale Anzahl von Benachrichtigungen

## RDP-Proxy

March 27, 2024

Die RDP-Proxy-Funktionalität wird als Teil des Citrix Gateway bereitgestellt. In einer typischen Bereitstellung wird der RDP-Client auf dem Computer eines Remote-Benutzers ausgeführt. Das Citrix Gateway-Gerät wird in der DMZ bereitgestellt, und die RDP-Serverfarm ist im internen Unternehmensnetzwerk.

Der Remote-Benutzer;

1. stellt eine Verbindung zur öffentlichen IP-Adresse von Citrix Gateway her
2. stellt eine SSL-VPN-Verbindung her
3. authentifiziert
4. greift über das Citrix Gateway-Gerät auf die Remote-Desktops zu

Die RDP-Proxy-Funktion wird im clientlosen VPN- und ICA-Proxy-Modus unterstützt.

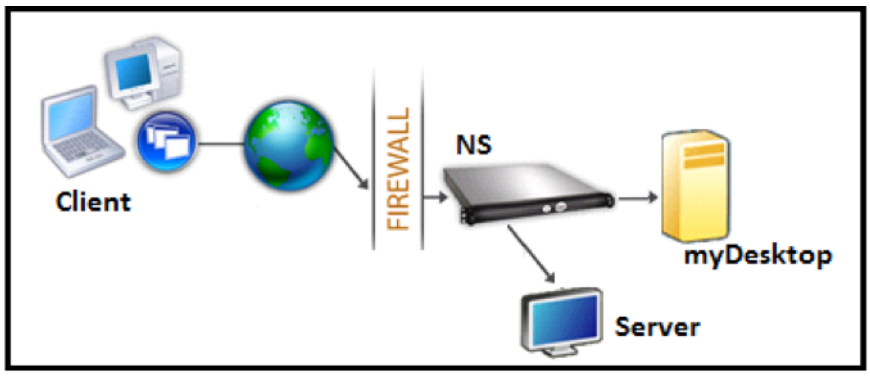
 

> **Hinweis:**
>
> Citrix Gateway unterstützt keine Remote Desktop Session Host (RDSH), Remote App, RDS-Multiuser, RDP-Sitzungen oder RDP-Apps.

Die folgenden RDP-Proxy-Funktionen bieten Zugriff auf eine Remote-Desktop-Farm über das Citrix Gateway.

- Sicherer RDP-Verkehr durch clientloses VPN oder ICA-Proxy-Modus (ohne Full Tunnel).
- SSO (Single Sign-On) zu RDP-Servern über Citrix Gateway. Bietet auch eine Option, SSO bei Bedarf zu deaktivieren.
- Durchsetzungsfunktion (SmartAccess), bei der die Citrix ADC-Administratoren bestimmte RDP-Funktionen über die Citrix Gateway-Konfiguration deaktivieren können.
- Single/Stateless (Dual) Gateway-Lösung für alle Anforderungen (VPN/ICA/RDP/Citrix Endpoint Management).
- Kompatibilität mit dem nativen Windows MSTSC-Client für RDP, ohne dass benutzerdefinierte Clients erforderlich sind.
- Verwendung eines vorhandenen von Microsoft bereitgestellten RDP-Clients auf MACOSX, iOS und Android.

Die folgende Abbildung zeigt einen Überblick über die Bereitstellung:




### Bereitstellung durch clientloses VPN

In diesem Modus werden die RDP-Links auf der Gateway-Homepage oder dem Portal als Lesezeichen, über die Konfiguration `add vpn url` oder über ein externes Portal veröffentlicht. Der Benutzer kann auf diese Links klicken, um Zugriff auf den Remotedesktop zu erhalten.

### Bereitstellung über ICA-Proxy

In diesem Modus wird mit dem Parameter `wihome` eine benutzerdefinierte Homepage für die Gateway-VIP konfiguriert. Diese Homepage kann mit der Liste der Remote-Desktop-Ressourcen angepasst werden, auf die der Benutzer zugreifen darf. Diese benutzerdefinierte Seite kann auf Citrix ADC gehostet werden, oder wenn sie extern ist, kann sie ein iFrame auf der vorhandenen Gateway-Portalseite sein.

In beiden Modi, nachdem der Benutzer auf den bereitgestellten RDP-Link oder das bereitgestellte RDP-Symbol geklickt hat, kommt eine HTTPS-Anforderung für die entsprechende Ressource beim Citrix Gateway an. Das Gateway generiert den Inhalt der RDP-Datei für die angeforderte Verbindung und sendet ihn an den Client. Der native RDP-Client wird aufgerufen und stellt eine Verbindung zu einem RDP-Listener auf dem Gateway her. Gateway führt SSO zum RDP-Server durch Unterstützung der Durchsetzung (SmartAccess) durch. Das Gateway blockiert den Clientzugriff auf bestimmte RDP-Funktionen basierend auf der Citrix ADC-Konfiguration und leitet dann den RDP-Verkehr zwischen dem RDP-Client und dem Server weiter.

### Einzelheiten zur Durchsetzung

Der Citrix ADC-Administrator kann bestimmte RDP-Funktionen über die Citrix Gateway-Konfiguration konfigurieren. Citrix Gateway bietet die Funktion “RDP-Durchsetzung”für wichtige RDP-Parameter. Citrix ADC stellt sicher, dass der Client blockierte Parameter nicht aktivieren kann. Wenn die blockierten Parameter aktiviert sind, ersetzt die RDP-Erzwingungsfunktion die clientfähigen Parameter und sie werden nicht berücksichtigt.

> **Wichtig:** Die Durchsetzungsfunktion ist nur anwendbar, wenn SSO aktiviert ist.

#### Unterstützte RDP-Parameter für die Durchsetzung

Durchsetzen des Folgens von Umleitungsparametern wird unterstützt Diese Parameter sind als Teil eines RDP-Clientprofils konfigurierbar.

- Umleitung der Zwischenablage
- Umleitung von Druckern
- Umleitung von Laufwerken
- Umleitung von COM-Ports
- Umleitung von PNP-Geräten

### Ablauf der Verbindung

Der Verbindungsfluss kann in zwei Schritte unterteilt werden:

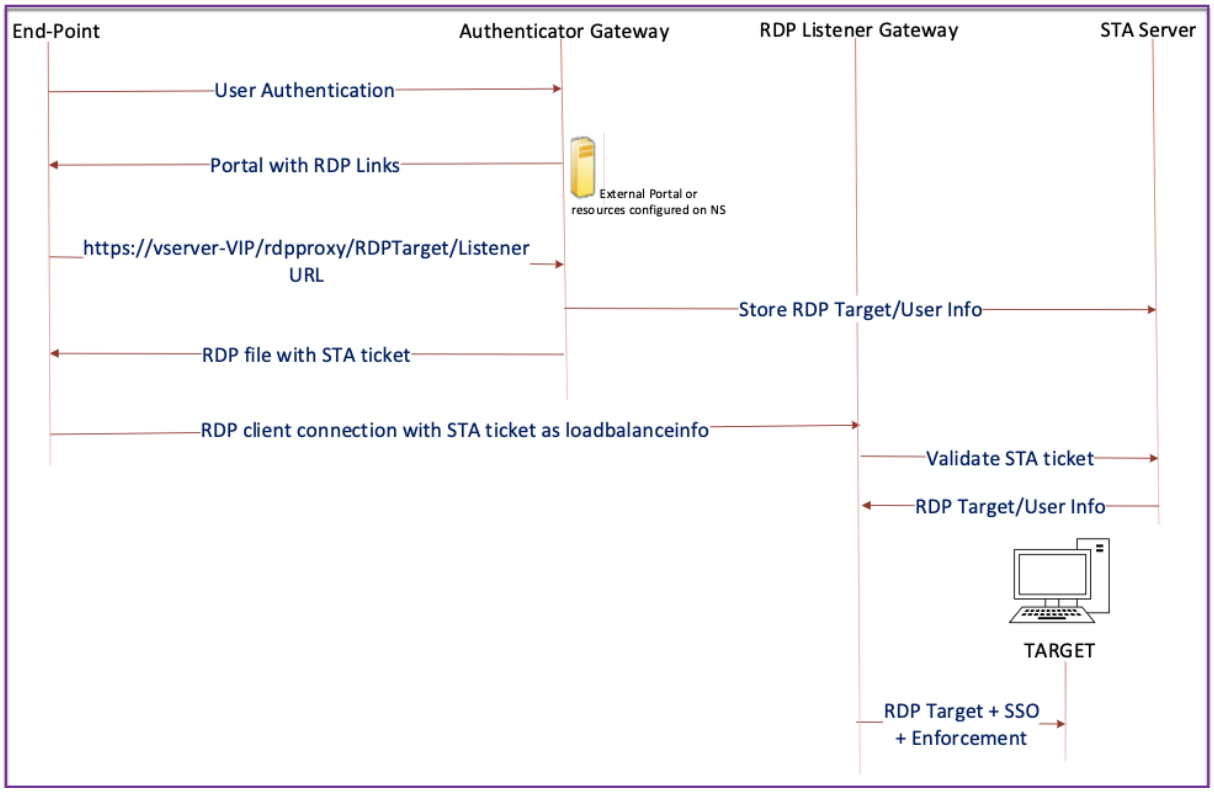
- RDP-Ressourcenaufzählung und RDP-Dateidownload.
- Start der RDP-Verbindung.

Basierend auf dem vorhergehenden Verbindungsablauf gibt es zwei Bereitstellungslösungen:

- Stateless (Dual) Gateway-Lösung - Die RDP-Ressourcenaufzählung und der RDP-Dateidownload erfolgt über das Authenticator-Gateway, aber der Start der RDP-Verbindung erfolgt über das RDP-Listener-Gateway.
- Einzel-Gateway-Lösung - Die RDP-Ressourcenaufzählung, der RDP-Dateidownload und der Start der RDP-Verbindung erfolgen über dasselbe Gateway.

## Stateless (duale) Gateway-Kompatibilität

Die folgende Abbildung zeigt die Bereitstellung:




- Ein Benutzer stellt eine Verbindung zum Authenticator Gateway VIP her und stellt die Anmeldeinformationen bereit.

- Nach einer erfolgreichen Anmeldung am Gateway wird der Benutzer zur Homepage oder zum externen Portal weitergeleitet, das die Remote-Desktop-Ressourcen aufzählt, auf die der Benutzer zugreifen kann.
- Sobald der Benutzer eine RDP-Ressource ausgewählt hat, erhält die Authenticator Gateway-VIP die Anforderung in dem Format, das die veröffentlichte Ressource `https://vserver-vip/rdpproxy/rdptarget/listener` angibt, auf die der Benutzer geklickt hat. Diese Anforderung enthält die Informationen über die IP-Adresse und den Port des RDP-Servers, die der Benutzer ausgewählt hat.
- Das Authenticator Gateway verarbeitet die /rdpproxy/ -Anforderung. Da der Benutzer bereits authentifiziert ist, enthält diese Anfrage ein gültiges Gateway-Cookie.
- Die Informationen `RDPTarget` und `RDPUser` werden auf dem STA-Server gespeichert und ein STA-Ticket wird generiert. Die auf dem STA-Server gespeicherten Informationen werden mithilfe des konfigurierten Pre-Shared-Schlüssels verschlüsselt. Das Authenticator Gateway verwendet einen der STA-Server, der auf dem virtuellen Gateway-Server konfiguriert ist.
- Die 'Listener'-Informationen aus der Anforderung /rdpproxy/ wird als "`fulladdress`"in die `.rdp file` gepeichert und das STA-Ticket (mit vorangestellter STA AuthID) wird als "`loadbalanceinfo`"in die `.rdp file` gepeichert.
- Die `.rdp file` wird an den Endpunkt des Clients zurückgesendet.
- Der native RDP-Client startet und stellt eine Verbindung zum her `RDPListener Gateway`. Es sendet das STA-Ticket im ersten Paket.

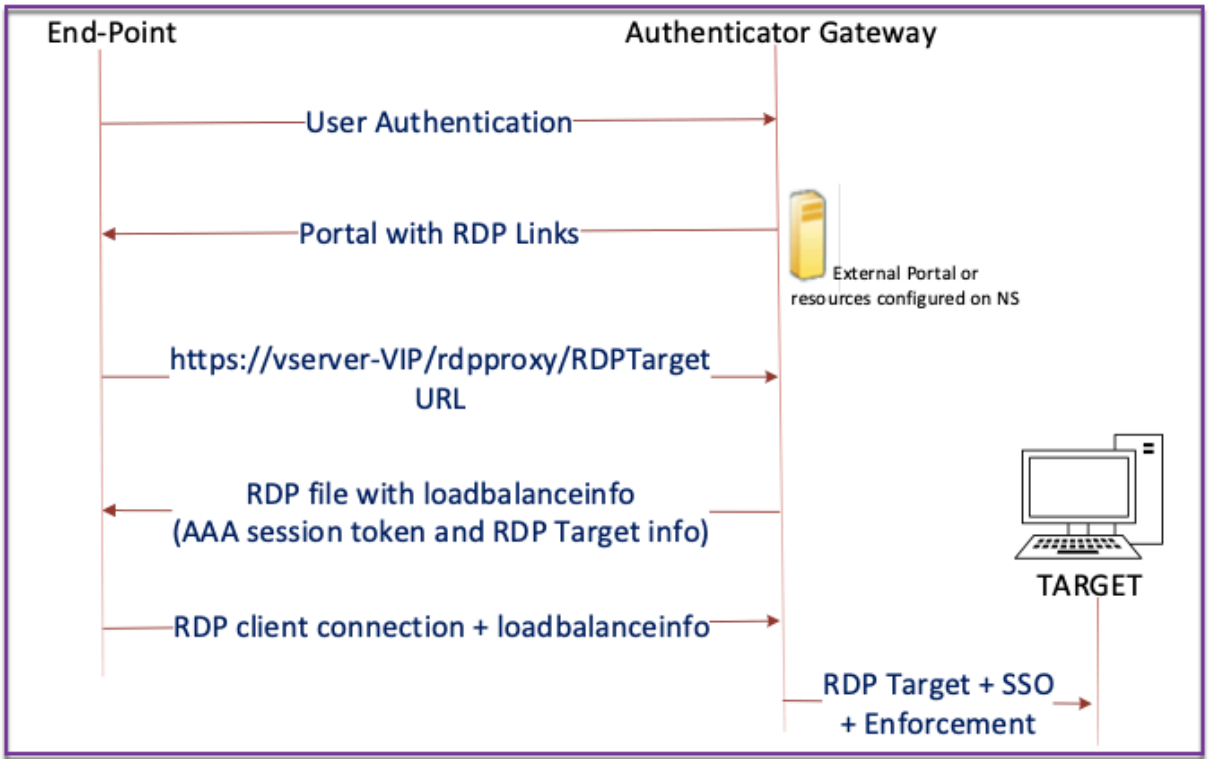
  Das `RDPListener`-Gateway validiert das STA-Ticket und erhält die Informationen `RDPTarget` und `RDPUser`. Der zu verwendende STA-Server wird mithilfe der in der vorhandenen 'AuthID'abgerufen `loadbalanceinfo`.
- Eine Gateway-Sitzung wird zum Speichern von Autorisierungs-/Überwachungsrichtlinien erstellt. Wenn eine Sitzung für den Benutzer existiert, wird sie wiederverwendet.
- Das `RDPListener`-Gateway verbindet sich mit `RDPTarget` und meldet sich mit CREDSSP an.

> **Wichtig:**
>
> - Für einen statuslosen RDP-Proxy validiert der STA-Server das vom RDP-Client gesendete STA-Ticket, um die Informationen `RDPTarget`/`RDPUser` zu erhalten. Sie müssen den STA-Server zusätzlich zum virtuellen VPN-Server binden.

### Single-Gateway Kompatibilität

Die folgende Abbildung zeigt die Bereitstellung:




> **Wichtig:**
>
> Im Fall einer einzelnen Gateway-Bereitstellung ist der STA-Server nicht erforderlich. Das Authenticator-Gateway codiert das `RDPTarget` und das Citrix Authentifizierungs-, Autorisierungs- und Überwachungssitzungscookie sicher und sendet sie als `loadbalanceinfo` in der `.rdp file`. Wenn der RDP-Client dieses Token im ursprünglichen Paket sendet, decodiert das Authenticator-Gateway die `RDPTarget`-Informationen, schlägt die Sitzung nach und stellt eine Verbindung zum `RDPTarget` her.

### Unterstützung für einen einzelnen Listener

- Single Listener für sowohl RDP- als auch SSL-Verkehr.
- Der RDP-Dateidownload und der RDP-Verkehr können über dasselbe 2-Tupel (dh IP und Port) auf der Citrix ADC Appliance verarbeitet werden.

### Lizenzanforderungen für RDP Proxy

Premium-Ausgabe, Advanced-Ausgabe

> **Hinweis:**
>
> Die RDP-Proxy-Funktion steht Kunden, die nur eine Gateway-Plattformlizenz oder nur die Stan-

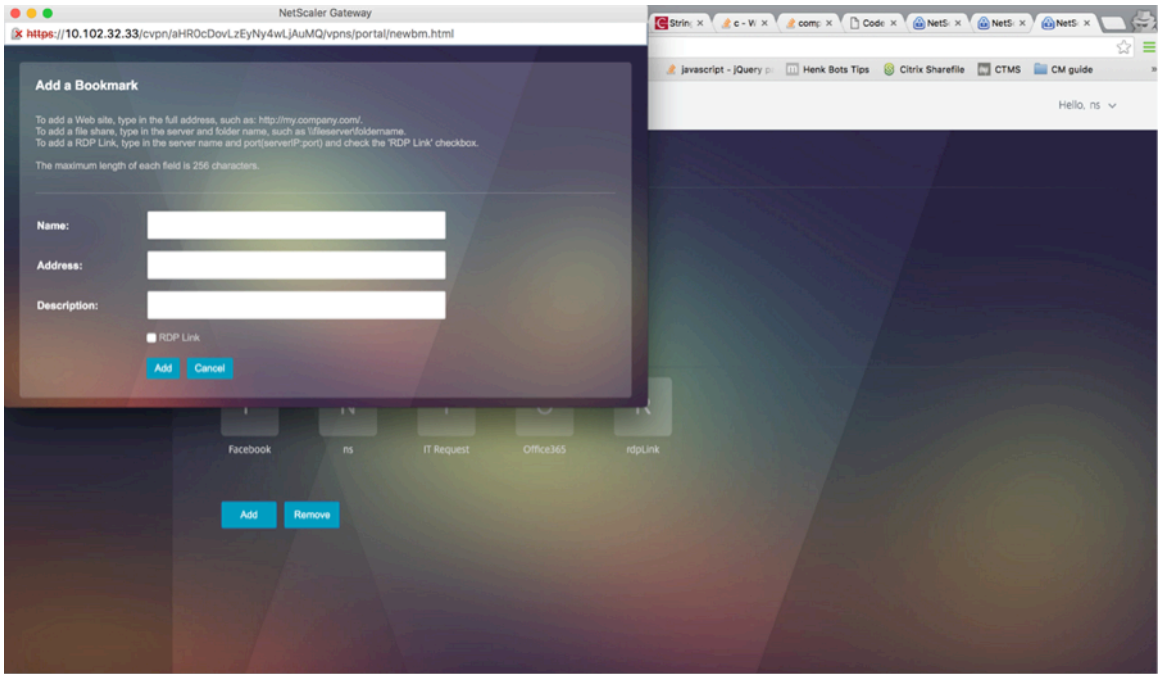
> dard Edition besitzen, nicht zur Verfügung.

Sie können den folgenden Befehl verwenden, um RDP-Proxy zu aktivieren.

```
enable feature rdpProxy
<!--NeedCopy-->
```

### Lesezeichen

**RDP-Linkgenerierung über Portal.** Anstatt die RDP-Links für den Benutzer zu konfigurieren oder die RDP-Links über ein externes Portal zu veröffentlichen, können Sie Benutzern die Möglichkeit geben, ihre eigenen URLs durch Bereitstellung zu generieren `targerIP:Port`. Für die zustandslose RDP-Proxy-Bereitstellung kann der Administrator RDP-Listener-Informationen im FQDN: Port-Format als Teil des RDP-Clientprofils einschließen. Dies erfolgt im Rahmen der Option `rdpListener`. Diese Konfiguration wird für die Generierung von RDP-Verbindungen über das Portal im Dual-Gateway-Modus verwendet.




#### Lesezeichen erstellen

1. Erstellen Sie Lesezeichen auf der Portalseite, um auf die RDP-Ressourcen zuzugreifen: (actualURL beginnt mit `rdp://`).
2. VPN-URL hinzufügen `<urlName> <linkName> <actualURL>`
   - Die URL muss das folgende Format haben: `rdp://<TargetIP:Port>`.

- Für den statuslosen RDP-Proxy-Modus muss die URL das folgende Format haben: `rdp://<TargetIP:Port>/<ListenerIP:Port>`
- Die URL wird im Portal im Format veröffentlicht:
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>`
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`

3. Binden Sie die Lesezeichen an den Benutzer oder die Gruppe oder den virtuellen VPN-Server oder VPN global.

#### Funktionen und Modi, die für RDP Proxy aktiviert werden sollen

```
1 -  enable ns feature ssl
2
3 -  enable ns feature sslvpn
4
5 -  enable ns feature rdpproxy
6
7 -  enable mode usnip
8 <!--NeedCopy-->
```

### RDP-Proxy-Konfigurationsschritte auf hoher Ebene

Die folgenden Schritte auf hoher Ebene sind an der statuslosen RDP-Proxy-Konfiguration beteiligt.

- Erstellen Sie ein RDP-Serverprofil
- Erstellen Sie ein RDP-Clientprofil
- Erstellen und binden Sie einen virtuellen Server
- Erstellen Sie ein Lesezeichen
- Erstellen oder Bearbeiten eines Sitzungsprofils oder einer Richtlinie
- Binden Sie ein Lesezeichen

#### Konfigurieren eines Clientprofils

Konfigurieren Sie das Clientprofil auf dem Authenticator-Gateway. Das Folgende ist eine Beispielkonfiguration:

```
1 add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
      audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook
      >] [-multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
      rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
      rdpFileName <string>] [-rdpHost <optional FQDN that will be put in
      the RDP file as ' fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE
      )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts (
```

```
      ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
      redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE
       | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]
<!--NeedCopy-->
```

Verknüpfen Sie das RDP-Clientprofil mit dem virtuellen VPN-Server.

Dies kann entweder durch Konfigurieren einer SessionAction+SessionPolicy oder durch Festlegen des globalen VPN-Parameters erfolgen.

Beispiel:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
   prioritynumber>
<!--NeedCopy-->
```

ODER

```
set vpn parameter  – rdpClientprofile <name>
<!--NeedCopy-->
```

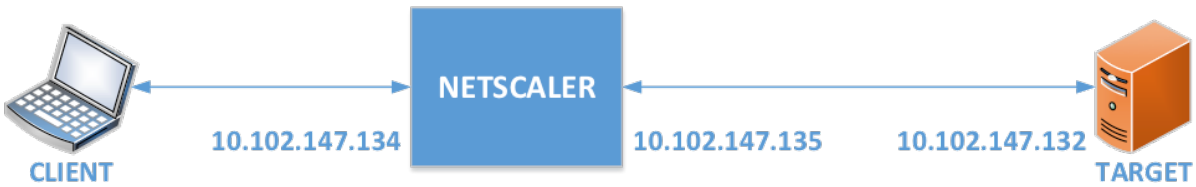
### Konfigurieren eines Serverprofils

Konfigurieren Sie das Serverprofil auf dem Listener-Gateway.

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
   listener> -rdpPort <port for terminating RDP client connections> -
   psk <key to decrypt RDPTarget/RDPUser information, needed while
   using STA>`
<!--NeedCopy-->
```

`rdp ServerProfile` muss auf dem virtuellen VPN-Server konfiguriert sein.

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -
   rdpServerProfile <rdpServer Profile>`
<!--NeedCopy-->
```



### RDP-Proxy-Konfiguration über die CLI

Das Folgende ist ein Beispiel für eine RDP-Proxy-Konfiguration über die CLI.

- Fügen Sie die VPN-URL für den Benutzer mit den Zielinformationen hinzu.

```
add aaa user Administrator –password freebsd123$%^

add vpn url rdp RdpLink rdp://rdpserverinfo

add dns addrec rdpserverinfo 10.102.147.132

bind aaa user Administrator  –urlName rdp
<!--NeedCopy-->
```

- Konfigurieren Sie das RDP-Client- und Serverprofil für die VPN-Verbindung.

```
add rdp clientprofile p1 –psk citrix -redirectClipboard ENABLE

add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix

add vpn vserver mygateway SSL  10.102.147.134 443 –
   rdpserverprofile p1

set vpn parameter -clientlessVpnMode ON -
   defaultAuthorizationAction ALLOW -rdpClientProfileName p1

add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key
   rdp_rootkey

bind ssl vserver mygateway -certkeyName gatewaykey
<!--NeedCopy-->
```

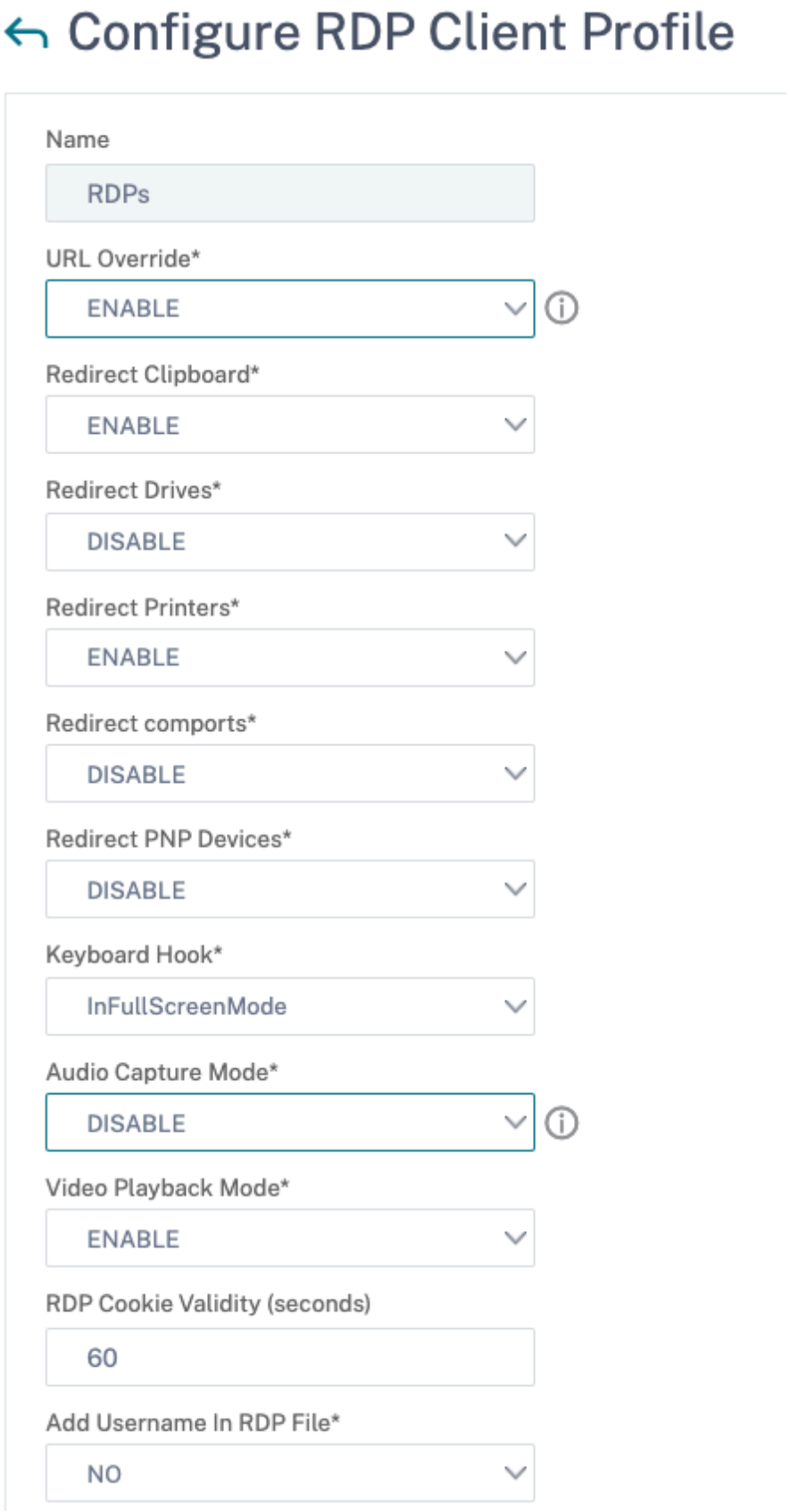
- Fügen Sie SNIP für die Verbindung von Citrix ADC zum Ziel hinzu.

```
add ns ip 10.102.147.135  255.255.255.0 –type SNIP
<!--NeedCopy-->
```

### RDP-Proxy-Konfiguration über die GUI

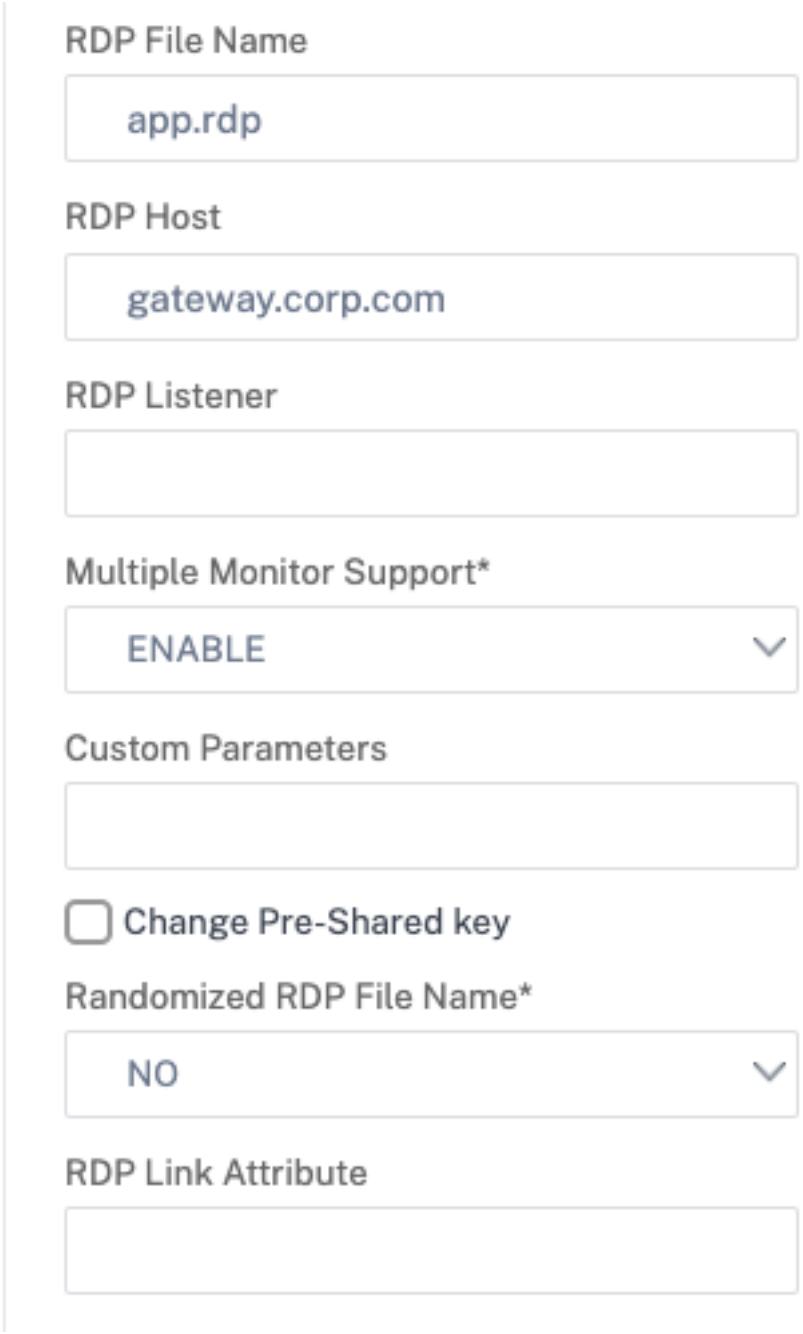
1. Navigieren Sie zu **Citrix Gateway > Richtlinien**, klicken Sie mit der rechten Maustaste auf **RDP**und klicken Sie auf **Funktion aktivieren**
2. Klicken Sie im Navigationsbereich auf RDP. Wählen Sie auf der rechten Seite die Registerkarte **Kundenprofile** aus und klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für das Clientprofil einen Namen ein und konfigurieren Sie ihn.



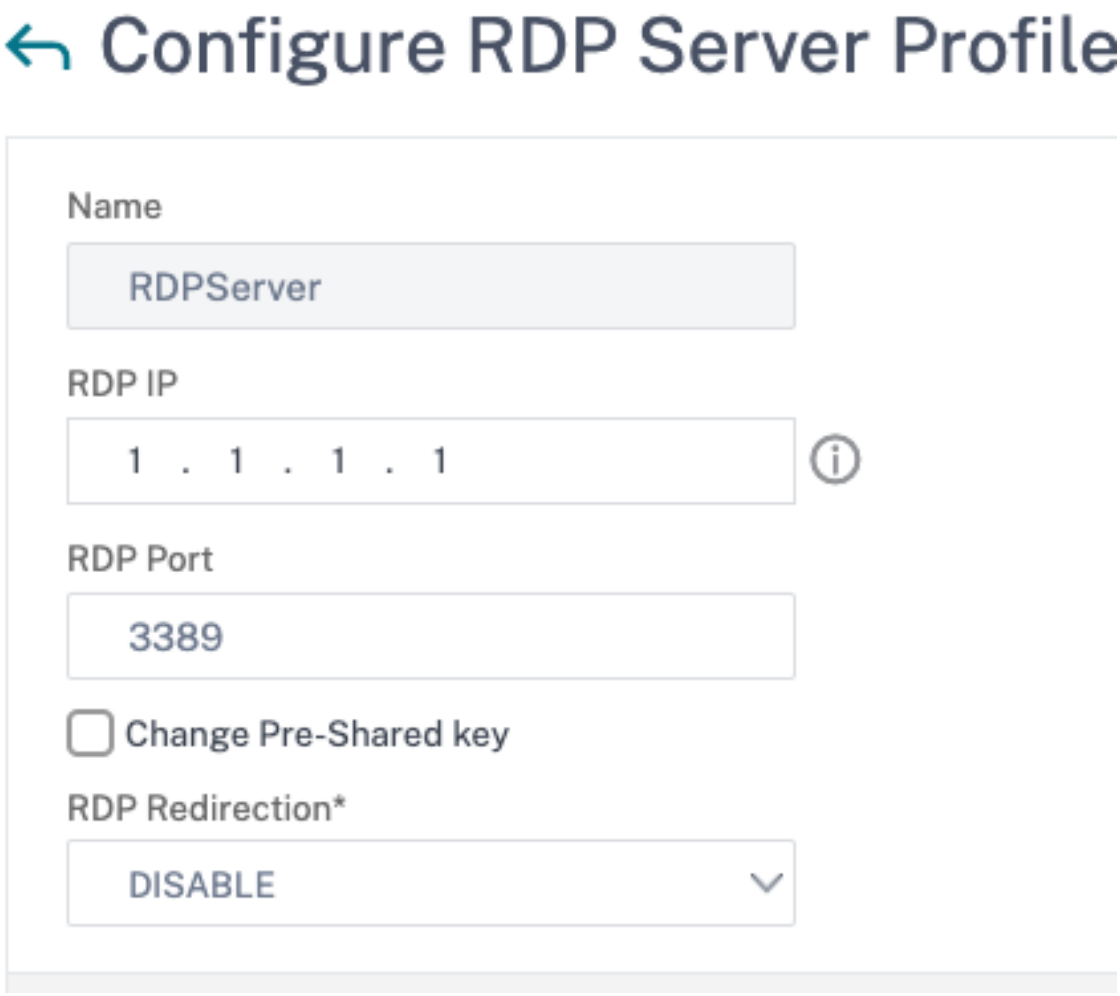
4. Geben Sie im Feld RDP-Host den FQDN ein, der in den RDP-Proxy-Listener aufgelöst wird. Dies ist normalerweise der gleiche FQDN wie der FDQN der Citrix Gateway-Appliance.
5. Geben Sie unter **Pre Shared Key**ein Kennwort ein und klicken Sie auf **OK**.




6. Geben Sie dem Serverprofil einen Namen ein.
7. Geben Sie die IP-Adresse des virtuellen Gateway-Servers ein, an den Sie dieses Profil binden möchten.
8. Geben Sie denselben Preshared Key ein, den Sie für das RDP-Clientprofil konfiguriert haben.

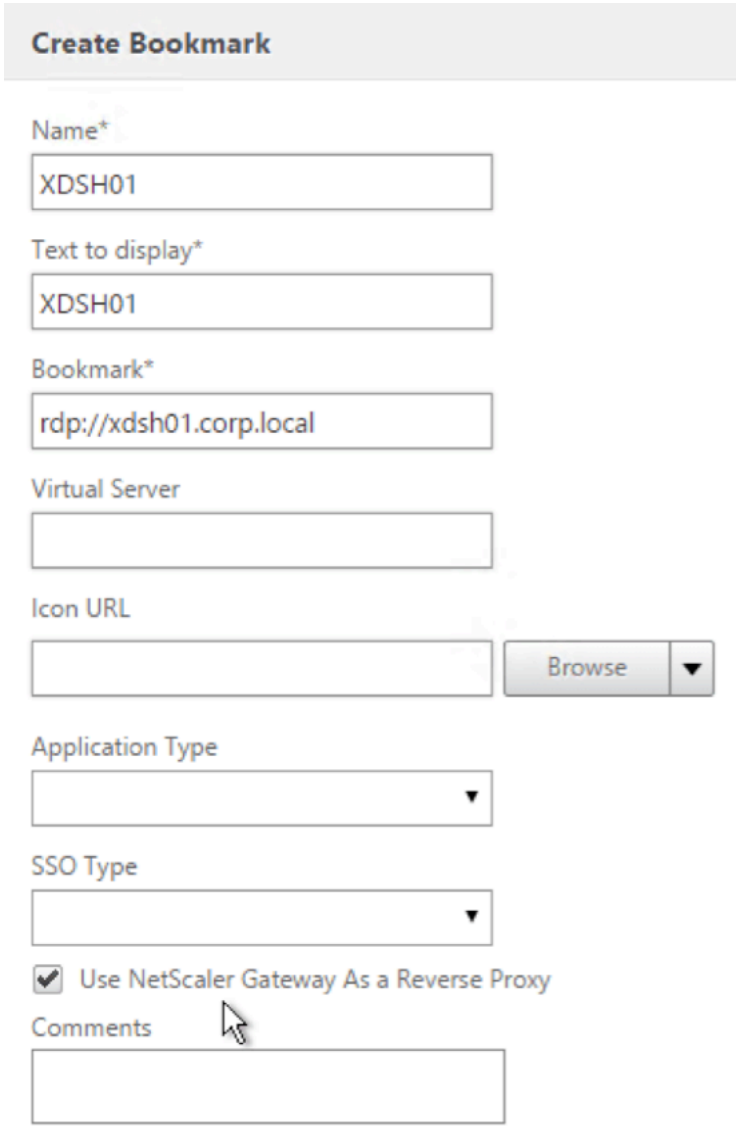
 

Klicken Sie auf **Erstellen**.



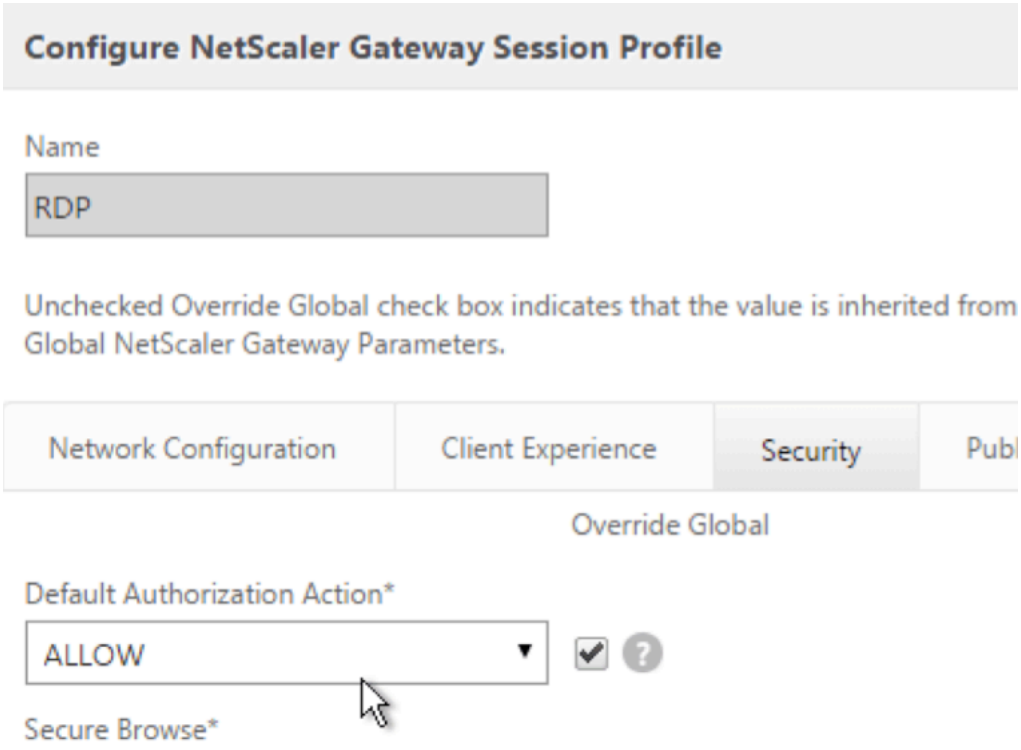

9. Wenn Sie RDP-Lesezeichen auf der Portalseite Clientless Access hinzufügen möchten, erweitern Sie auf der linken Seite **Citrix Gateway**, erweitern Sie **Ressourcen**, und klicken Sie auf **Lesezeichen**.
10. Klicken Sie rechts auf **Hinzufügen**.
11. Gib dem Lesezeichen einen Namen.
12. Geben Sie für die URL **rdp: //myRDPServer mit IP oder DNS**ein.
13. Wählen Sie **Citrix Gateway als Reverseproxy** verwenden und klicken Sie auf **Erstellen**.
14. Erstellen Sie Lesezeichen gemäß Ihren Anforderungen.

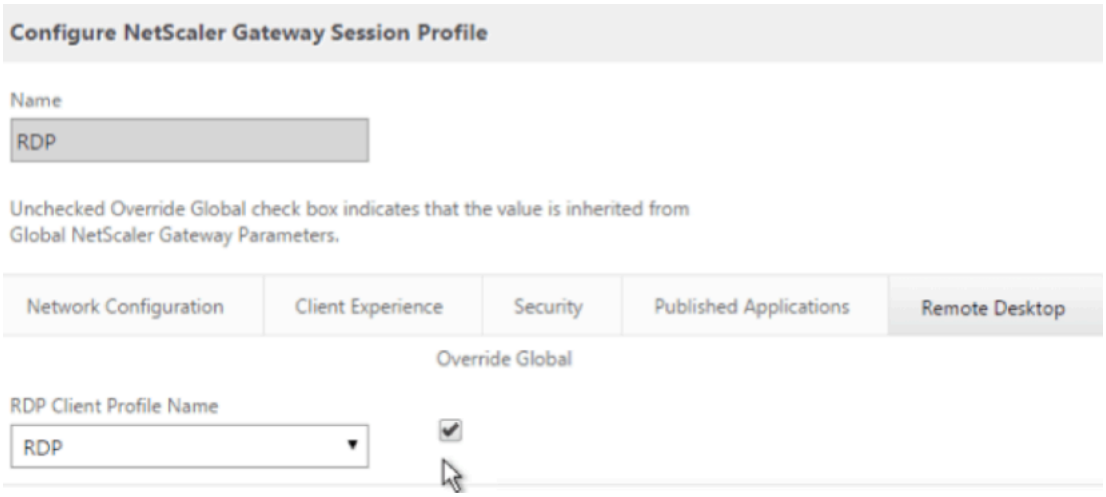



15. Erstellen oder bearbeiten Sie ein Sitzungsprofil. Navigieren Sie zu **Citrix Gateway > Richtlinien > Sitzung**.
16. Legen Sie auf der Registerkarte Sicherheit die **Standardautorisierungsaktion** auf **ZULASSEN**fest. Oder Sie können Autorisierungsrichtlinien verwenden, um den Zugriff zu steuern.

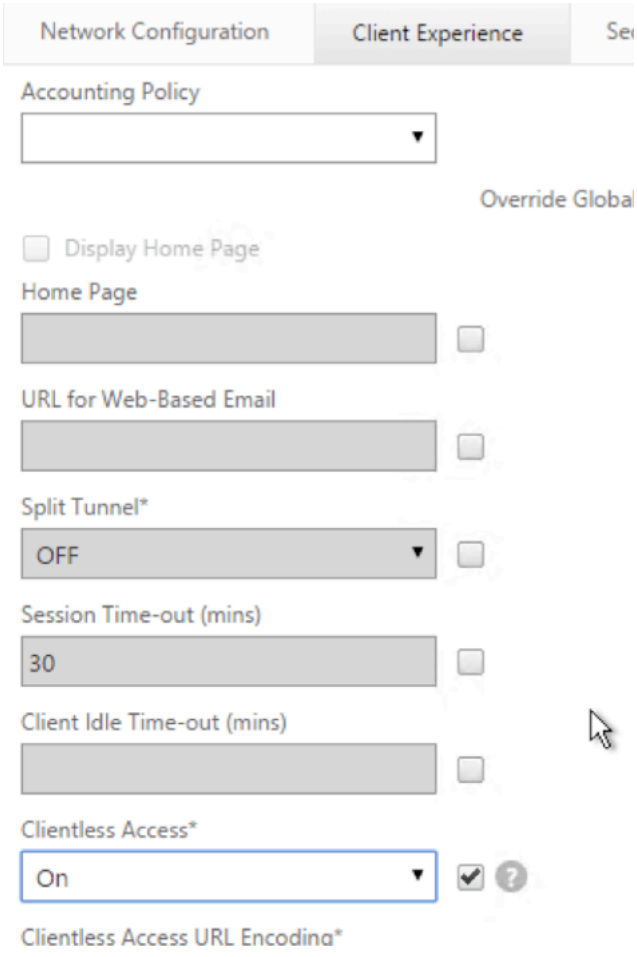



17. Wählen Sie auf der Registerkarte Remotedesktop das RDP-Clientprofil aus, das Sie zuvor erstellt haben.

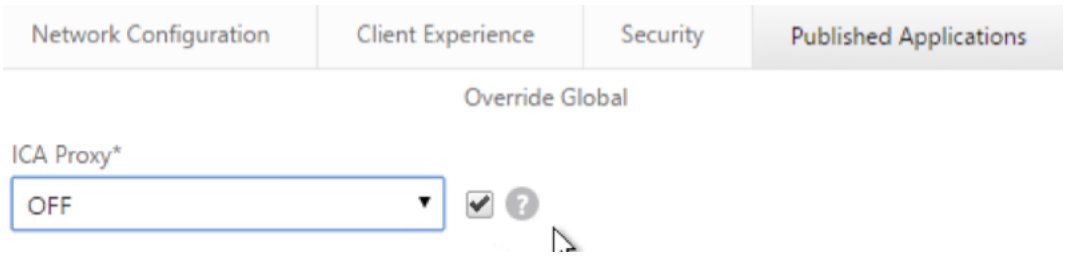



18. Wenn Sie Lesezeichen verwenden möchten, setzen Sie auf der Registerkarte **Client Experience-Clientless Accessauf On**.

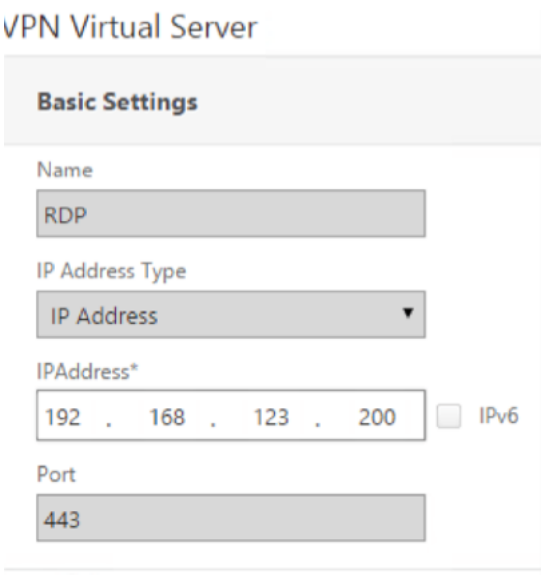



19. Stellen Sie auf der Registerkarte **Published Applications** sicher, dass der ICA-Proxy **AUS**ist.

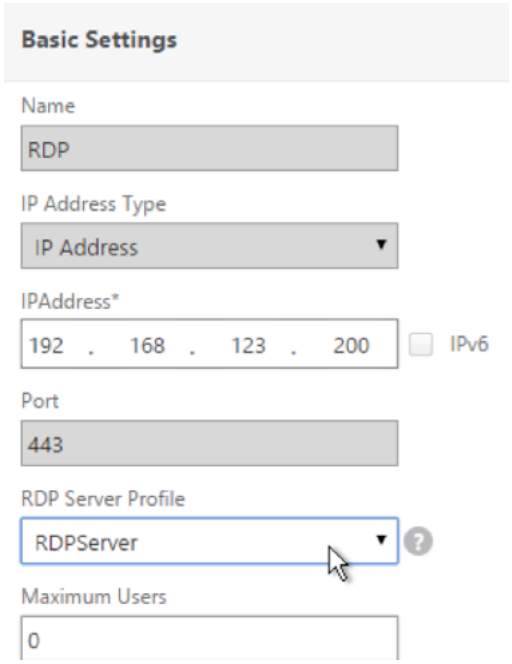



20. Ändern oder erstellen Sie Ihren virtuellen Gateway-Server.
21. Klicken Sie im Abschnitt **Grundeinstellungen** auf **Mehr**.

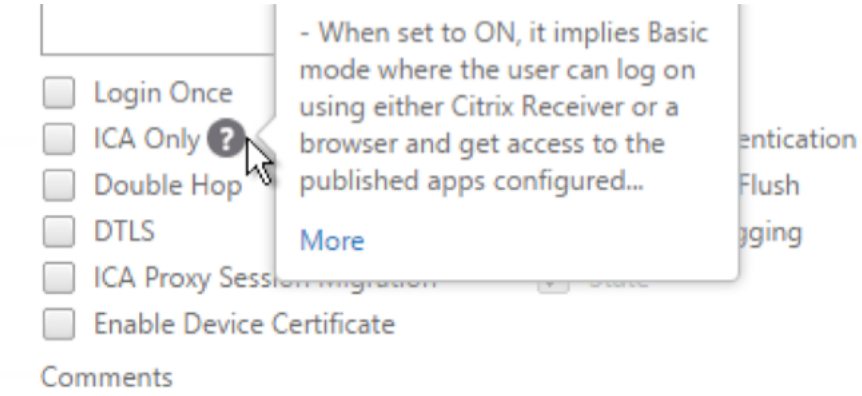



22. Verwenden Sie die RDP-Serverprofilliste, um das zuvor erstellte RDP-Serverprofil auszuwählen.

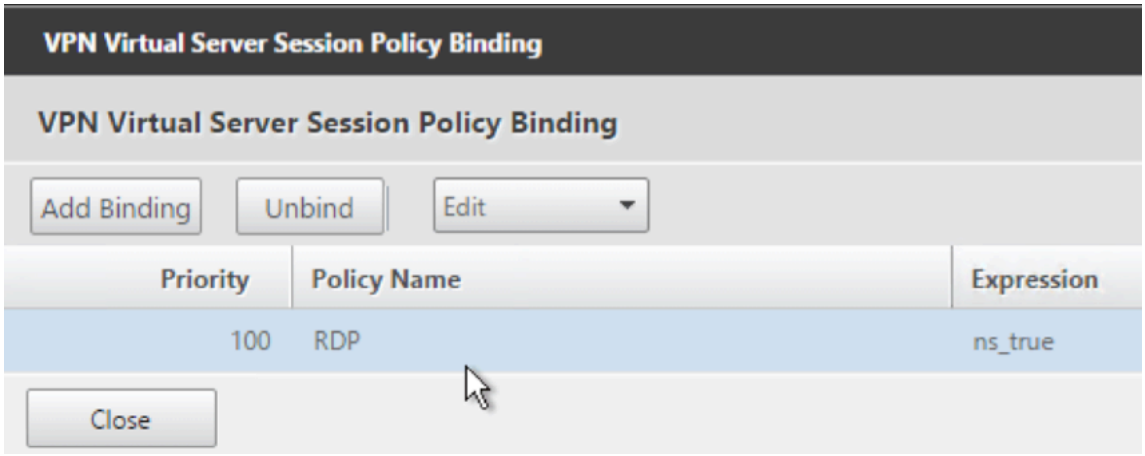



23. Scrolle nach unten. Stellen Sie sicher, dass “**Nur ICA** “nicht aktiviert ist.

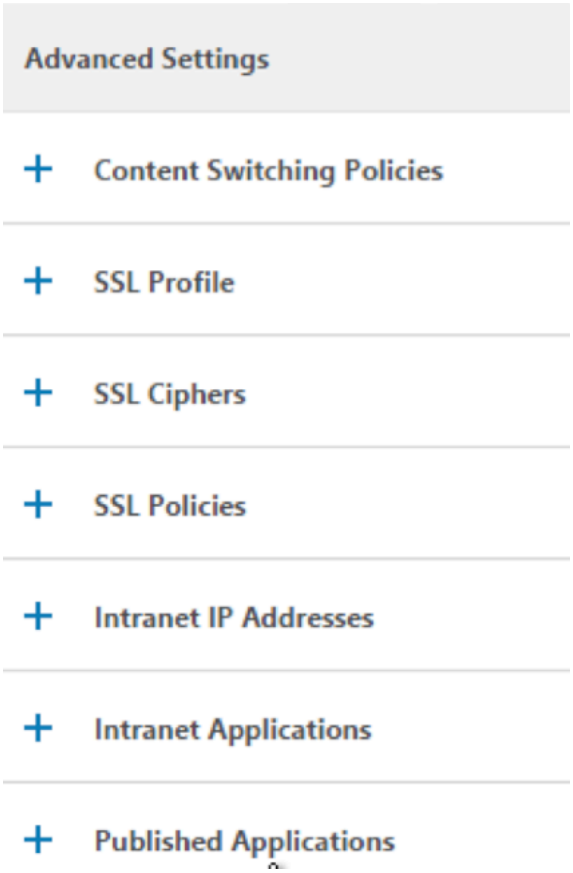



24. Binden Sie ein Zertifikat.
25. Binden Sie Authentifizierungsrichtlinien.
26. Binden Sie die Sitzungsrichtlinie/das Sitzungsprofil, für das das RDP-Clientprofil konfiguriert ist

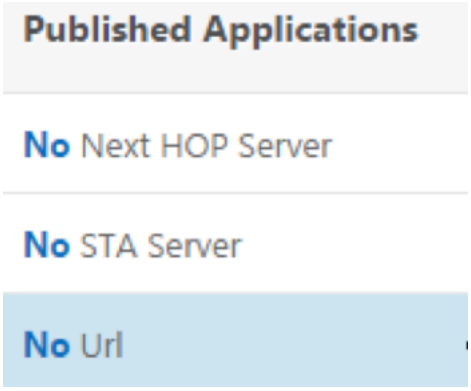



27. Sie können Lesezeichen entweder an den virtuellen Citrix Gateway-Server oder an eine Authentifizierungs-, Autorisierungs- und Überwachungsgruppe binden. Um an den virtuellen Citrix Gateway-Server zu binden, klicken Sie rechts im Abschnitt Erweiterte Einstellungen auf **Veröffentlichte Anwendungen**.

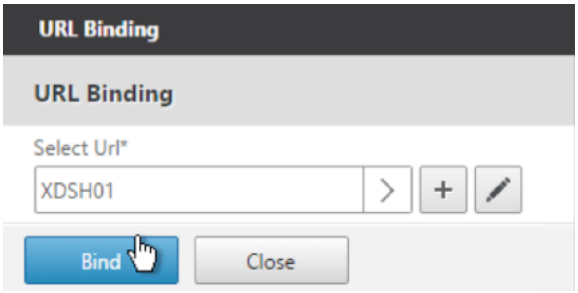
 




28. Klicken Sie links im Abschnitt **Veröffentlichte Anwendungen** auf **Keine URL**.

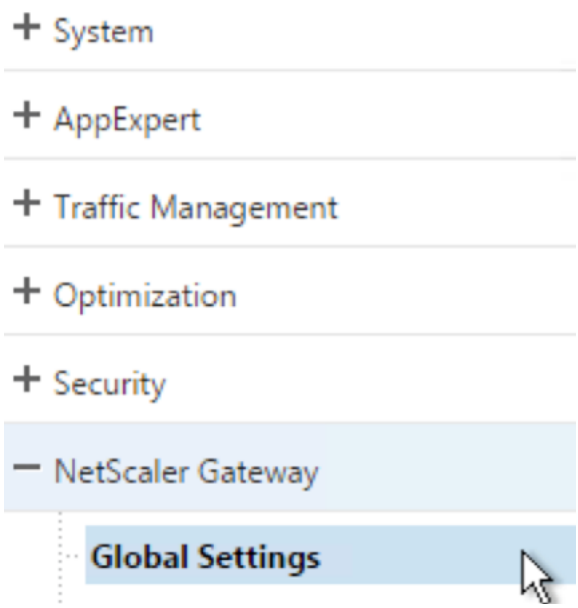



29. Binde deine Lesezeichen.

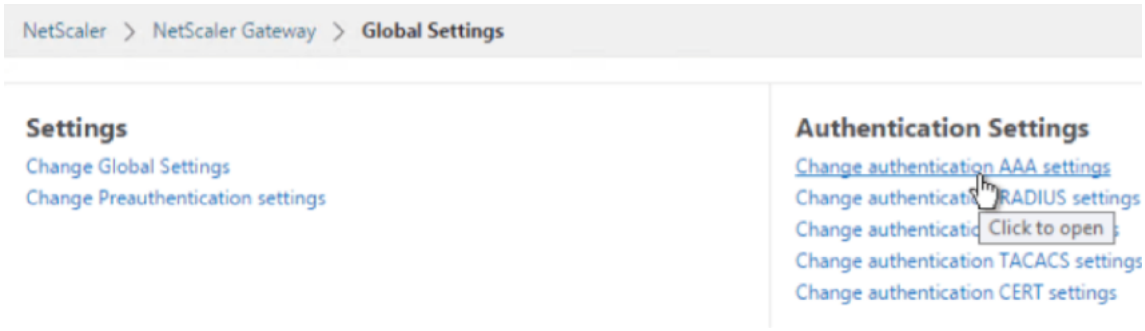


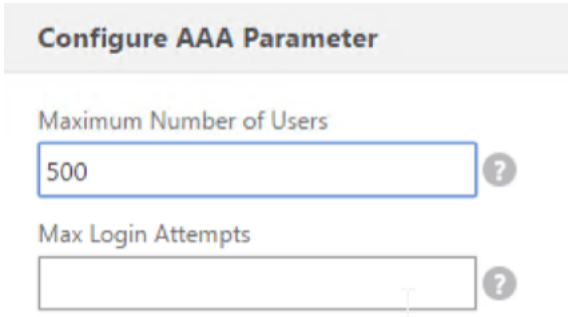
30. Da Only ICA für diesen virtuellen Citrix Gateway-Server nicht angegeben ist, stellen Sie sicher, dass Ihre Citrix Gateway Universal-Lizenzen korrekt konfiguriert sind. Erweitern Sie auf der linken Seite **Citrix Gateway** und klicken Sie auf **Globale Einstellungen**.




31. Klicken Sie rechts auf **AAA-Einstellungen für Authentifizierung ändern**.

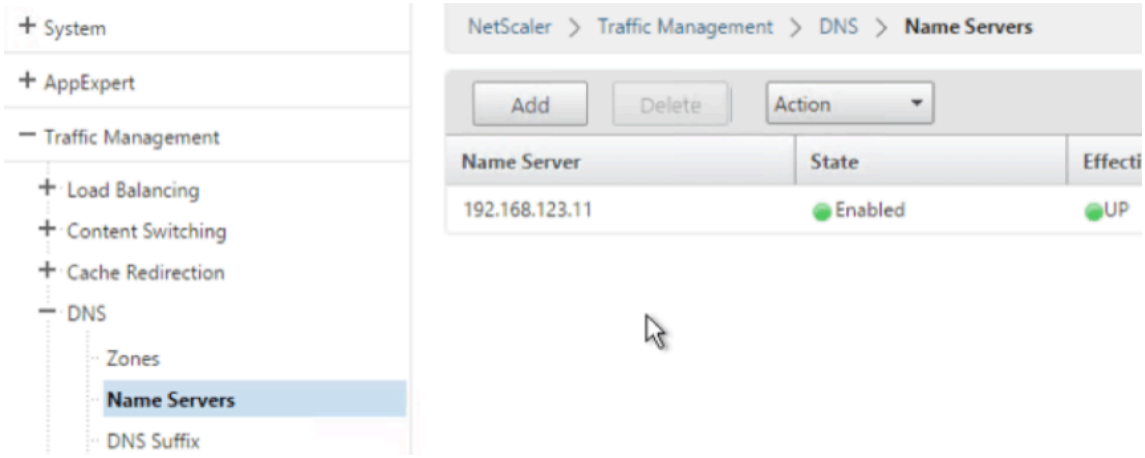



32. Ändern Sie die **maximale Anzahl von Benutzern** auf Ihr lizenziertes Limit.

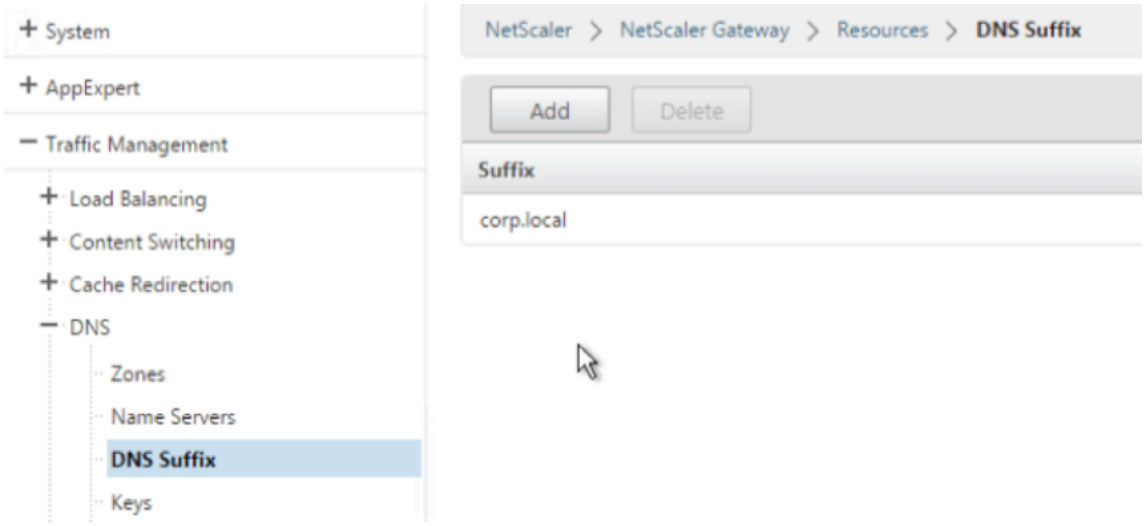



33. Wenn Sie mithilfe von DNS eine Verbindung zu RDP-Servern herstellen möchten, stellen Sie sicher, dass DNS-Server auf der Appliance konfiguriert sind (**Traffic Management > DNS > Nameserver)**.

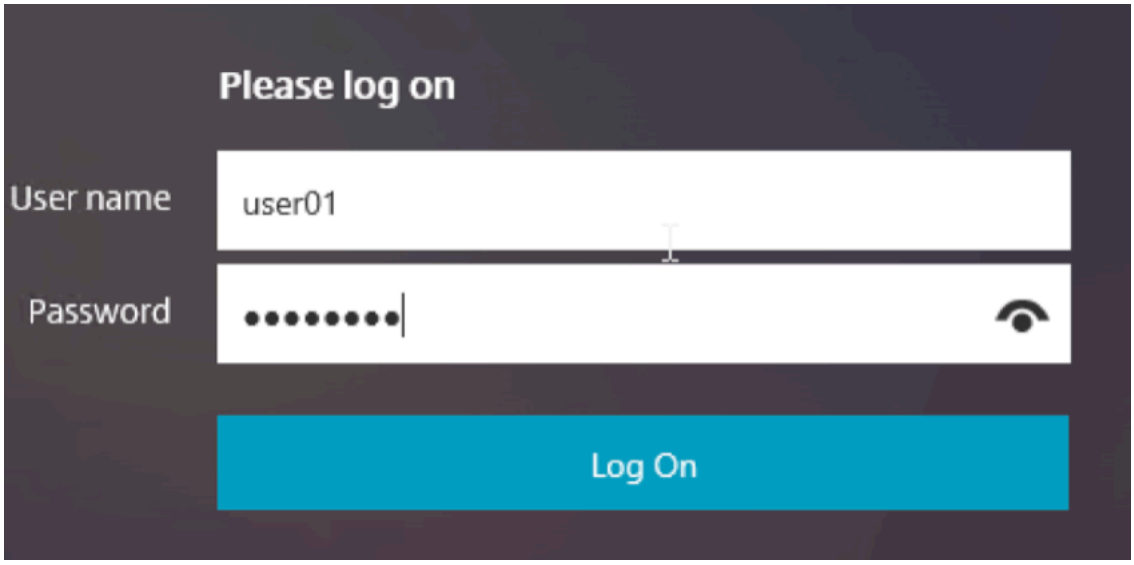



34. Wenn Sie die Kurznamen anstelle von FQDNs verwenden möchten, fügen Sie ein **DNS-Suffix hinzu (Traffic Management > DNS > DNS-Suffix)**.

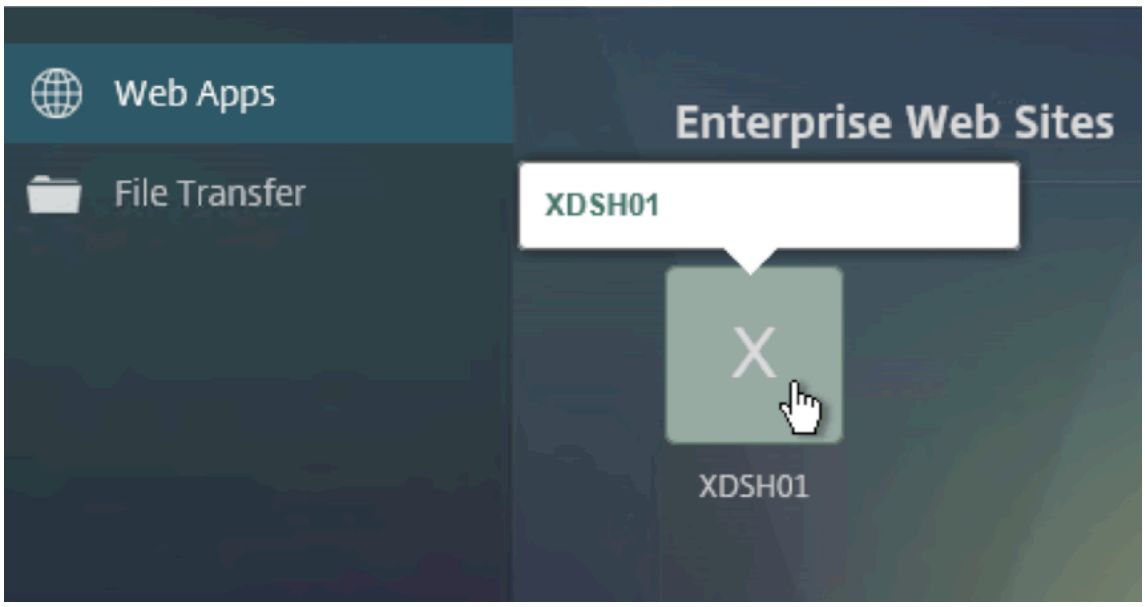



35. Verbinden Sie sich mit Ihrem Gateway und melden Sie sich an.

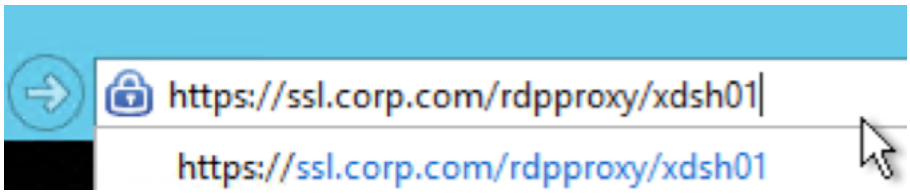
 




36. Wenn Sie **Lesezeichen**konfiguriert haben, klicken Sie auf das **Lesezeichen**.



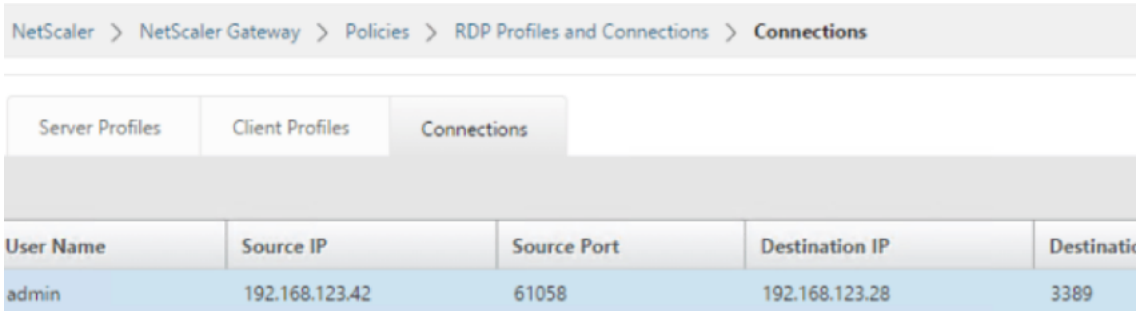

37. Sie können die Adressleiste in **/rdpProxy/myRDPServer**ändern. Sie können eine IP-Adresse (zum Beispiel rdpproxy/192.168.1.50) oder einen DNS-Namen (/rdpproxy/myserver) eingeben.




38. Öffne das `.rdp file`heruntergeladene

39. Sie können die derzeit verbundenen Benutzer anzeigen, indem Sie zu **Citrix Gateway Policies > RDP gehen.** Auf der rechten Seite ist die Registerkarte **Verbindungen**.




### Option zum Deaktivieren von SSO

Die SSO-Funktion (Single Sign-On) mit RDP-Proxy kann durch Konfigurieren von Citrix ADC-Verkehrsrichtlinien deaktiviert werden, sodass der Benutzer immer zur Eingabe von Anmeldeinformationen aufgefordert wird. Wenn SSO deaktiviert ist, funktioniert die RDP-Durchsetzung (SmartAccess) nicht.

Beispiel:

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
<!--NeedCopy-->
```

Die Verkehrsrichtlinie kann gemäß der Anforderung konfiguriert werden. Im Folgenden sind zwei Beispiele aufgeführt:

- So deaktivieren Sie SSO für den gesamten Verkehr:

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy
   " <TrafficActionName>
<!--NeedCopy-->
```

- So deaktivieren Sie SSO basierend auf Quell-/Ziel-IP/FQDN

```
add vpn trafficPolicy <TrafficPolicyName>  "HTTP.REQ.URL.CONTAINS
   ("rdpproxy") && CLIENT.IP.SRC.EQ(<IP>)" <TrafficActionName>
bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
<!--NeedCopy-->
```

## Zustandsloser RDP-Proxy

March 27, 2024

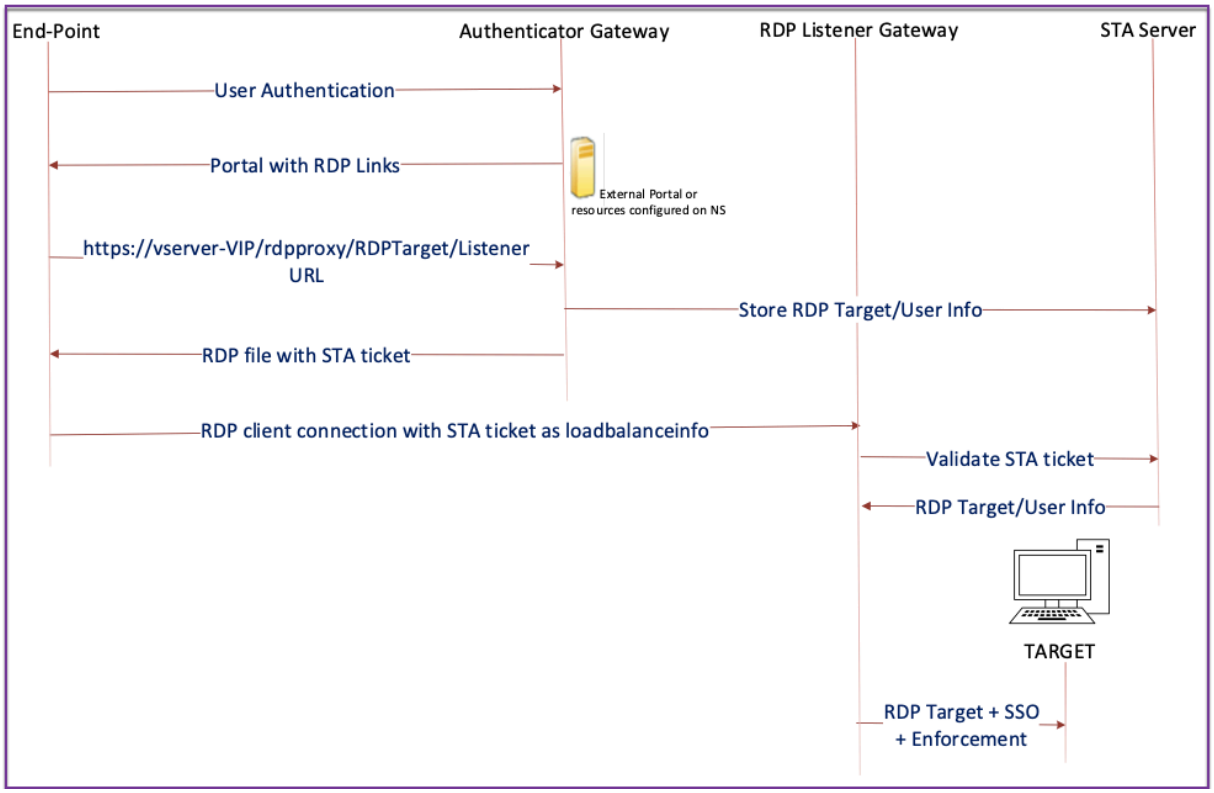
 

Der Stateless RDP-Proxy greift auf einen RDP-Host zu. Der Zugriff wird über `RDPListener` auf Citrix Gateway gewährt, wenn sich der Benutzer auf einem separaten Citrix Gateway Authenticator authentifiziert. Die vom `RDPListener` für Citrix Gateway benötigten Informationen werden sicher auf einem STA-Server gespeichert. Ein STA-Server kann überall platziert werden, solange das Citrix Gateway und die Anwendungsenumerationsserver ihn erreichen können. Einzelheiten finden Sie unter https://support.citrix.com/article/CTX101997.

### Ablauf der Verbindung

Am RDP-Proxyfluss sind zwei Verbindungen beteiligt. Die erste Verbindung ist die SSL-VPN-Verbindung des Benutzers zum Citrix Gateway VIP und die Aufzählung der RDP-Ressourcen.

Die zweite Verbindung ist die native RDP-Clientverbindung zum RDP-Listener (konfiguriert mit RDPip und RDPPort) auf dem Citrix Gateway und die anschließende sichere Weiterleitung des RDP-Clients an Serverpakete.




1. Der Benutzer stellt eine Verbindung zum Authenticator Gateway VIP her und stellt die Anmeldeinformationen bereit.
2. Nach erfolgreicher Anmeldung am Gateway wird der Benutzer zur Homepage/zum externen Portal weitergeleitet, das die Remote-Desktop-Ressourcen auflistet, auf die der Benutzer zugreifen kann.

3. Sobald der Benutzer eine RDP-Ressource ausgewählt hat, wird eine Anforderung vom Authenticator Gateway VIP in dem Format empfangen, das die veröffentlichte Ressource `https://AGVIP/rdpproxy/ip:port/rdptargetproxy` angibt, auf die der Benutzer geklickt hat. Diese Anforderung enthält die Informationen über die IP und den Port des RDP-Servers, die der Benutzer ausgewählt hat.
4. Das Authenticator-Gateway verarbeitet die /rdpproxy/ -Anforderung. Da der Benutzer bereits authentifiziert ist, enthält diese Anfrage ein gültiges Gateway-Cookie.
5. Die `RDPTarget` und `RDPUser` Informationen werden auf dem STA-Server gespeichert und ein STA-Ticket wird generiert. Die Informationen werden als XML-Blob gespeichert, das optional mit dem konfigurierten Pre-Shared-Schlüssel verschlüsselt wird. Wenn es verschlüsselt ist, wird das Blob base64-codiert und gespeichert. Das Authenticator Gateway verwendet einen der STA-Server, der auf dem virtuellen Gateway-Server konfiguriert ist.
6. Das XML-Blob hat das folgende Format

```
<Value name="IPAddress">ipaddr</Value>\n<Value name="Port">
    port</Value>n

<Value name="`Username`">username</Value>\n<Value name="
    Password">pwd</Value>
<!--NeedCopy-->
```

7. Das in der /rdpproxy/ -Anforderung `rdptargetproxy` erhaltene wird als '`fulladdress`' und das STA-Ticket (vorab mit der STA-AuthID angehängt) wird als `loadbalanceinfo` in der.rdp-Datei gesetzt.
8. Die `.rdp` Datei wird an den Client-Endpunkt zurückgesendet.
9. Der native RDP-Client startet und stellt eine Verbindung zum her `RDPListener Gateway`. Es sendet das STA-Ticket im ersten x.224-Paket.
10. Der `RDPListener Gateway` validiert das STA-Ticket und erhält die `RDPTarget` und `RDPUser` Informationen. Der zu verwendende STA-Server wird mit der in der vorhandenen 'AuthID'abgerufen `loadbalanceinfo`.
11. Eine Gateway-Sitzung wird zum Speichern von Autorisierungs-/Überwachungsrichtlinien erstellt. Wenn eine Sitzung für den Benutzer existiert, wird sie wiederverwendet.
12. Der `RDPListener Gateway` verbindet sich mit dem `RDPTarget` und meldet sich mit CREDSSP an.

### Voraussetzungen

- Der Benutzer wird im Citrix Gateway-Authentifikator authentifiziert.

- Die anfängliche /rdpproxy-URL und der RDP-Client sind mit einem anderen RDPListener Citrix Gateway verbunden.
- Das Authenticator Gateway, das einen STA-Server verwendet, übergibt die RDPListener Gateway Informationen sicher.

### Konfigurieren Sie den statuslosen RDP-Proxy über die CLI

- Fügen Sie ein rdpServer Profil hinzu. Das Serverprofil ist auf dem konfiguriert RDPListener Gateway.

  **Hinweis:**

  - Sobald das RDPServer-Profil auf dem virtuellen VPN-Server konfiguriert ist, kann es nicht geändert werden. Außerdem kann dasselbe rdpServerProfile nicht auf einem anderen virtuellen VPN-Server wiederverwendet werden.

```
add rdpServer Profile [profilename] -rdpIP [IPV4 address of the
   RDP listener] -rdpPort [port for terminating RDP client
   connections] -psk [key to decrypt RDPTarget/RDPUser
   information, needed while using STA].
<!--NeedCopy-->
```

  Konfigurieren Sie das RDP-Serverprofil auf dem virtuellen VPN-Server mit dem folgenden Befehl:

```
add vpn vserver v1 SSL [publicIP] [
   portforterminatingvpnconnections] -rdpServerProfile [rdpServer
    Profile]
<!--NeedCopy-->
```

  Beispiel

```
add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile
   rdp_server_prof
<!--NeedCopy-->
```

  **Wichtig:**

  - Derselbe STA-Server muss sowohl an das RDP-Authenticator-Gateway als auch an das Listener-Gateway gebunden sein.
  - Bei statusfreien RDP-Proxys validiert der STA-Server das vom RDP-Client gesendete STA-Ticket, um den RDP-Zielserver und die RDP-Benutzerinformationen abzurufen. Sie müssen den STA-Server zusätzlich zum virtuellen VPN-Server binden. Im folgenden Beispiel ist der RDP-Zielserver 1.1.1.0 und der virtuelle RDP-Listener-Gateway-Server 1.1.1.2.

```
1       add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
2   <!--NeedCopy-->
```

Konfigurieren Sie das Client-Profil auf dem Authenticator Gateway mit dem folgenden Befehl:

```
1 add rdpClient profile <name> -rdpHost <optional FQDN that will be put
     in the RDP file as ' fulladdress '> [-rdpUrlOverride ( ENABLE |
     DISABLE )] [-redirectClipboard ( ENABLE | DISABLE )] [-
     redirectDrives ( ENABLE | DISABLE )]
2
3          [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <
              keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
              videoPlaybackMode ( ENABLE | DISABLE )]
4
5          [-rdpCookieValidity <positive_integer>][-multiMonitorSupport (
              ENABLE | DISABLE )] [-rdpCustomParams <string>]
6 <!--NeedCopy-->
```

Die —rdphHost-Konfiguration wird in einer einzelnen Gateway-Bereitstellung verwendet. Nur `psk` ist ein obligatorisches Argument und es muss dasselbe psk sein, das im RDP-Serverprofil im RDP-Listener-Gateway hinzugefügt wurde.

- Verknüpfen Sie das RDP-Profil mit dem virtuellen VPN-Server.

Sie können ein RDP-Profil entweder durch Konfigurieren einer SessionAction+SessionPolicy oder durch Festlegen des globalen VPN-Parameters zuordnen.

**Beispiel:**

```
1 add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>
2
3 add vpn sessionpolicy <polname> NS_TRUE <actname>
4
5 bind vpn vserver <vservername> -policy <polname> -priority <
     prioritynumber>
6 <!--NeedCopy-->
```

ODER

```
1 set vpn parameter  – rdpClientprofile <name>
2 <!--NeedCopy-->
```

### Konfigurieren Sie den statuslosen RDP-Proxy über die GUI

Die folgenden Schritte auf hoher Ebene sind an der statuslosen RDP-Proxy-Konfiguration beteiligt. Die detaillierten Schritte finden Sie unter RDP-Proxy-Konfiguration.

- Erstellen Sie ein RDP-Serverprofil

- Erstellen Sie ein RDP-Clientprofil
- Erstellen Sie einen virtuellen Server
- Erstellen Sie ein Lesezeichen
- Erstellen oder Bearbeiten eines Sitzungsprofils oder einer Richtlinie
- Binden Sie ein Lesezeichen

> **Wichtig:**
>
> Für einen zustandslosen RDP-Proxy müssen Sie zusätzlich zum virtuellen VPN-Server einen STA-Server binden.

### Zähler für Verbindung

Ein neuer Verbindungszähler ns_rdp_tot_curr_active_conn wurde hinzugefügt, der die Anzahl der verwendeten aktiven Verbindungen aufzeichnet. Es kann als Teil des `nsconmsg` Befehls in der Citrix ADC-Shell angezeigt werden. Der CLI-Befehl zum Anzeigen dieser Zähler soll später hinzugefügt werden.

### Hinweise zu Upgrades

Der RDPIP und der RDPPort, die zuvor auf dem virtuellen VPN-Server konfiguriert wurden, sind Teil des rdpServerProfile. Der `rdp Profile` wird in umbenannt `rdp ClientProfile` und der Parameter clientSSL wird entfernt. Daher funktioniert die frühere Konfiguration nicht.

## RDP-Verbindungsumleitung

March 27, 2024

Ein Citrix Gateway-Gerät unterstützt jetzt die RDP-Verbindungsumleitung in Gegenwart eines Verbindungsbrokers oder Sitzungsverzeichnisses. Eine RDP-Proxy-Kommunikation erfordert nicht mehr eine exklusive URL für jede Verbindung vom Client zum Server. Stattdessen verwendet der Proxy eine einzige URL, um eine Verbindung zu einer RDP-Serverfarm herzustellen, wodurch der Wartungs- und Konfigurationsaufwand für einen Administrator reduziert wird.

**Bitte beachten Sie**:

- Die RDP-Verbindungsumleitung wird nur unterstützt, wenn SSO aktiviert ist und sowohl im Single Gateway- als auch im Stateless- oder Dual Gateway-Modus zusammen mit der Erzwingung (SmartAccess) unterstützt wird.

- Die RDP-Proxy-Funktion wird nur bei tokenbasierter Umleitung unterstützt, die IP-Cookies unterstützt. IP-basierte Routing-Token "msts="werden vom Windows-Sitzungsbroker oder Verbindungsbroker zurückgegeben, wenn die Funktion **IP-Adressumleitung verwenden** deaktiviert ist.
- Sie können die Einstellung **IP-Adressumleitung verwenden** deaktivieren, um die tokenbasierte Umleitung an der folgenden Stelle zu aktivieren.
  `Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker`.
- Deaktivieren Sie die Einstellung IP-Adressumleitung verwenden auf den RDSH-Computern und nicht auf dem Verbindungsbroker-Computer.
- Dedizierte Umleitungen für die RDP-Proxy-Verbindung können konfiguriert werden.

### Voraussetzungen

- Erstellen Sie ein RDP-Serverprofil, um den 3389-Listener auf dem virtuellen Citrix Gateway-Server zu aktivieren.
  Wenn der Computer, den Sie RDP verwenden möchten, kein Mitglied einer RDS-Verbindungsbroker-Infrastruktur ist, benötigen Sie den 3389-Listener nicht.
- Aktivieren Sie die RDP-Verbindungsumleitung auf der Citrix Gateway-Appliance, um RDP-Proxy in Anwesenheit eines Verbindungsbrokers zu unterstützen.

### Stellen Sie RDP-Proxy in Anwesenheit eines Verbindungsbrokers bereit

RDP-Proxy in Anwesenheit eines Verbindungsbrokers kann auf zwei Arten bereitgestellt werden.

- Mit Hostservern für Remotedesktopsitzungen, die am Lastenausgleich für Remotedesktopverbindungen
- Bei Vorhandensein der RDP-Lastausgleichsfunktion.

Bei**Servern mit Host für Remotedesktopsitzungen, die am Lastausgleich des Verbindungsbrokers**

In diesem Fall kann der RDP-URL-Link so konfiguriert werden, dass er auf einen der RDP-Server als Zielserver verweist, der als Redirector fungiert. Außerdem ist es möglich, einen der RDP-Server in der Farm als Zielserver zu haben (in diesem Fall akzeptiert der Server keine RDP-Sitzung).

**Bei Vorhandensein der RDP-Lastausgleichsfunktion**:

Wenn der Lastausgleich des Verbindungsbrokers nicht aktiviert ist, können wir die RDP-Lastausgleichsfunktion in Citrix ADC verfügbar machen, um den erforderlichen Lastausgleich der RDP-Sitzungen in Anwesenheit eines Verbindungsbrokers durchzuführen. In diesem Fall muss der RDP-URL-Link so konfiguriert werden, dass der RDP-Load Balancer als Zielserver verwendet wird. Der RDP-Lastausgleichsdienst kann sich auf derselben Citrix Gateway-Appliance wie der RDP-Proxy befinden. Weitere Informationen finden Sie unter Loading Balancing RDP-Server.

#### Konfigurieren Sie RDP-Proxy in Anwesenheit eines Verbindungsbrokers über die CLI

Geben Sie an der Eingabeaufforderung;

```
add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
    DISABLE )

add rdpserverprofile serverProfileName -psk " secretString " -
    rdpRedirection ENABLE
<!--NeedCopy-->
```

#### Konfigurieren Sie die RDP-Verbindungsumleitung mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > RDP**.
2. Rechtsklicken Sie auf **RDP**, um die RDP-Umleitungsfunktion zu **aktivieren** oder zu **deaktivieren**.

## RDP-URLs basierend auf dem LDAP-Attribut auffüllen

March 27, 2024

Sie können ein Citrix Gateway-Gerät so konfigurieren, dass eine Liste von RDP-Servern (IP/FQDN) von einem LDAP-Serverattribut abgerufen wird. Basierend auf der abgerufenen Liste zeigt die Appliance die RDP-URLs für die Server an, auf die ein Benutzer zugreifen kann.

### So füllen Sie RDP-URLs basierend auf dem LDAP-Attribut über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add rdpclientprofile <Name>  – rdpUrlLinkAttribute <string>

add rdpclientprofile clientProfileName  – rdpUrlLinkAttribute
    rdpServerAttribute

```

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

Im vorherigen Beispiel entspricht RdpServerAttribute den RDP-Serverdetails für einen bestimmten Benutzer auf dem LDAP-Server.

**Hinweis**: Um die LDAP-Attributdetails vom LDAP-Server abzurufen, muss die LDAP-Aktion mit derselben Zeichenfolge konfiguriert werden, die `pUrlLinkAttribute` wie folgt konfiguriert ist.

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
     <"domain name"> -ldapBindDn <username> -ldapLoginName
    sAMAccountName -ldapbindDnpassword <password>

add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
    ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -
    ldapLoginName sAMAccountName -ldapbindDnpassword xxxx

add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap

bind vpn vs vserver<name> -pol dnpg_ldap_pol

set ldapaction dnpg_ldap -attributes "rdpServerAttribute"

set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
<!--NeedCopy-->
```

### LDAP-Serverkonfiguration

Führen Sie auf dem LDAP-Server die folgenden Schritte aus:

1. Navigieren Sie zu einem bestimmten **Benutzer**.
2. Klicken Sie in **AD-Benutzer und -Computer** auf **Ansicht** und dann auf **Detail**.
3. Klicken Sie mit der rechten Maustaste auf den **Benutzernamen** und dann auf **Attribute Editor**.
4. Ändern Sie den erforderlichen Attributwert (DisplayName) und klicken Sie auf **OK**.

### So füllen Sie RDP-URLs basierend auf dem LDAP-Attribut über die GUI auf

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > RDP**.
2. Klicken Sie auf der Seite **RDP-Profile und Verbindungen** auf die Registerkarte **Clientprofile** und wählen Sie das Clientprofil aus, in dem Sie das RDP-Link-Attribut konfigurieren möchten.
3. Geben **Sie auf der Seite RDP-Clientprofil konfigurieren** unter **RDP-Linkattribut**den Namen des LDAP-Attributs ein.

   **Hinweis:** Der LDAP-Attributwert kann eine kommagetrennte Liste sein.

# RDP-Dateinamen mit RDP-Proxy randomisieren

March 27, 2024

Wenn Sie auf eine RDP-URL klicken, wird eine RDP-Datei heruntergeladen. Wenn Sie erneut auf die **RDP-URL** klicken, wird eine neue RDP-Datei mit demselben Namen heruntergeladen, was zu einem Popup führt, in dem die neue Datei durch die vorhandene Datei ersetzt werden kann. Um dies zu vermeiden, kann sich der Administrator für die Zufallsgenerierung des RDP-Dateinamens entscheiden. Der Dateiname wird nun randomisiert, indem die Ausgabe der Funktion time () im Format <rdpFileName>_<outputof time()>.rdp angehängt wird. Auf diese Weise generiert die Appliance jedes Mal, wenn Sie eine Datei herunterladen, einen eindeutigen RDP-Dateinamen.

### Konfigurieren Sie die Unterstützung für die zufällige RDP-Dateiname mit RDP-Proxy

**Um die Unterstützung für die Zufallsgenerierung des RDP-Dateinamens mit RDP-Proxy mithilfe der Befehlszeilenschnittstelle an der Eingabeaufforderung zu konfigurieren, geben**Sie Folgendes ein:

```
1     add rdpclientprofile <profileName> -rdpfileName <filename> -
          randomizeRDPFilename <YES/NO>
2
3     add rdpclientprofile clientProfileName -rdpfileName testRDP -
          randomizeRDPFilename YES
4  <!--NeedCopy-->
```

**So konfigurieren Sie die Unterstützung für die Zufallsgenerierung des RDP-Dateinamens mit RDP-Proxy mithilfe der Citrix ADC GUI:**

1. Navigieren Sie zu **Citrix Gateway** > **Richtlinien** > **RDP**.
2. Klicken Sie auf der Seite **RDP-Profile und Verbindungen** auf die Registerkarte **Clientprofile** und wählen Sie das Clientprofil aus, in dem Sie die Funktion für randomisierende RDP-Dateinamen konfigurieren möchten.
3. Wählen Sie auf der Seite **RDP-Clientprofil konfigurieren** im Menü neben dem Feld **Randomized RDP-Dateiname** die Option **JA** aus.

# Konfigurieren Sie den Namen für RDP-Dateien

March 27, 2024

Nach dem Herunterladen einer RDP-Datei kann diese lokal mit dem konfigurierten Dateinamen gespeichert werden.

### Einen Namen für RDP-Dateien konfigurieren

**Um mithilfe der CLI einen Namen für RDP-Dateien zu konfigurieren, geben Sie in der Befehlszeile Folgendes ein**:

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
<!--NeedCopy-->
```

**Um einen Namen für RDP-Dateien mit der GUI zu konfigurieren:**

1. Navigieren Sie zu **Citrix Gateway** > **Richtlinien** > **RDP**.
2. Klicken Sie auf der Seite **RDP-Profile und Verbindungen** auf die Registerkarte **Clientprofile**. Wählen Sie das Clientprofil aus, in dem Sie eine randomisierende RDP-Dateinamen-Funktionalität konfigurieren möchten.
3. Geben Sie auf der Seite **RDP-Clientprofil konfigurieren** einen Namen für das RDP-Profil in das Feld **RDP-Dateiname** ein. Der Name der Datei muss das folgende Format haben: . Für den Namen sind maximal 31 Zeichen zulässig.

## Unterstützung für den ausgehenden ICA-Proxy

March 27, 2024

Die Unterstützung für ausgehende ICA-Proxy für Citrix Gateway ermöglicht es den Netzwerkadministratoren, SmartControl-Funktionen auch dann zu nutzen, wenn Receiver und Citrix Gateway in verschiedenen Organisationen bereitgestellt werden.

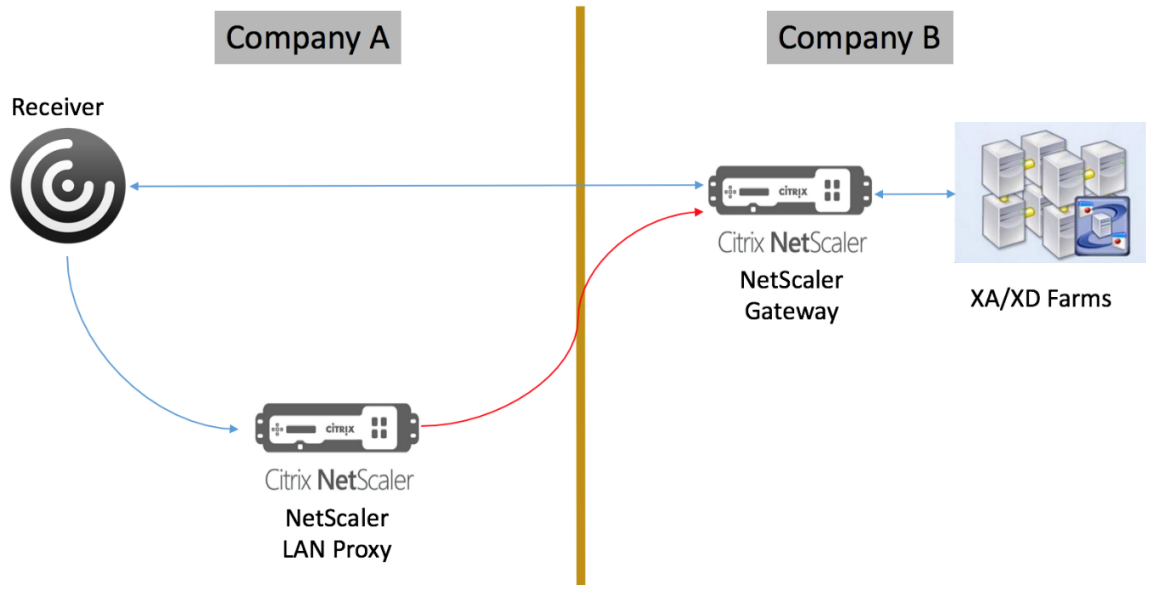
Das folgende Szenario veranschaulicht die Verwendung der Outbound-ICA-Proxy-Lösung:

Ein Netzwerkadministrator benötigt die Kontrolle über die ICA-Sitzungsfunktionen, wenn Receiver und Citrix Gateway in verschiedenen Organisationen bereitgestellt werden.

### Verstehen der Unterstützung für ausgehende ICA-Proxy

Um die SmartControl-Funktionalität in die Unternehmensorganisation, Unternehmen A, zu bringen, die über den Empfänger verfügt, müssen wir eine Citrix ADC Appliance hinzufügen, die als LAN-Proxy fungiert. Der Citrix ADC LAN Proxy erzwingt SmartControl und leitet den Datenverkehr an das Citrix Gateway von Unternehmen B weiter. In diesem Bereitstellungsszenario leitet der Receiver den Datenverkehr an den Citrix ADC LAN Proxy weiter, wodurch der Netzwerkadministrator von Unternehmen A SmartControl durchsetzen kann. Die Bereitstellung ist in der folgenden Abbildung dargestellt.




In diesem Szenario erfolgt der Datenverkehr zwischen dem LAN-Proxy und dem Citrix Gateway über SSL.

> **Hinweis:** Aktivieren Sie keine clientzertifikatbasierte Authentifizierung auf dem Citrix Gateway.

### SSL-Unterstützung auf Citrix ADC LAN-Proxy

Ab Version 13.0 Build xx.xx wird der Datenverkehr zwischen der Citrix Workspace-App und dem Citrix ADC LAN-Proxy auch über SSL unterstützt. Die Citrix Workspace-App verschlüsselt den Datenverkehr, den sie über SSL an den LAN-Proxy sendet. SSL-Unterstützung auf dem LAN-Proxy kann mit der vorhandenen Bereitstellung koexistieren.

Um die Verkehrsverschlüsselung über SSL zwischen der Citrix Workspace-App und dem Citrix ADC LAN-Proxy zu aktivieren, müssen Sie auf dem Citrix ADC LAN-Proxy Folgendes ausführen:

- Deaktivieren Sie die Authentifizierung und aktivieren Sie Double-Hop auf dem virtuellen VPN-Server.
- Stellen Sie den Host auf dem Windows-Client auf die IP-Adresse des virtuellen VPN-Servers ein.
- Aktivieren Sie die SNI- und Zertifikatvalidierung.
- Fügen Sie entsprechende CA-Zertifikate hinzu und aktivieren Sie sie global.

## Konfigurieren des ausgehenden ICA-Proxy

March 27, 2024

Die Konfiguration des ausgehenden ICA-Proxys umfasst die Konfiguration des Citrix ADC LAN-Proxys und des Citrix Gateway.

### Konfigurieren von Citrix ADC LAN Proxy für ausgehenden ICA-Proxy

Sie können die folgenden Schritte ausführen, um ausgehenden ICA-Proxy über die CLI zu konfigurieren.

- Fügen Sie einen virtuellen VPN-Server hinzu.

```
add vpn vserver <name> <serviceType> [<IPAddress> [-range <
   positive_integer>] [-ipset <string>]] [<port>] [-state (
   ENABLED | DISABLED )] [-authentication ( ON | OFF )] [-
   doubleHop ( ENABLED |DISABLED )]
<!--NeedCopy-->
```

- Stellen Sie die VPN-Parameter ein.

```
set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
   backendCertValidation ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

- Fügen Sie ein SSL-Zertifikatschlüsselpaar hinzu.

```
add ssl certKey ca_cert_verify -cert <certificate name>
<!--NeedCopy-->
```

- Binden Sie das SSL-Zertifikatschlüsselpaar global.

```
bind vpn global -cacert ca_cert_verify
<!--NeedCopy-->
```

**Beispiel:**

```
- add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication
   OFF - doubleHop ENABLED

- set vpn parameter backendserverSni ENABLED backendcertValidation
   ENABLED

- add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer

- bind vpn global -cacert dnpg_ca

<!--NeedCopy-->
```

### Konfigurieren von Citrix Gateway für ICA-Proxy

Einzelheiten zur Konfiguration von Citrix Gateway für ICA-Proxy finden Sie unter https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deploying-netscaler-gateway-in-ica-proxy-mode.pdf

**Hinweis:** Für die SSL-Unterstützung auf dem Citrix ADC LAN-Proxy sind keine Änderungen in der Citrix Gateway-Konfiguration erforderlich.

## Citrix Gateway aktiviert PCoIP-Proxy-Unterstützung für VMware Horizon View

March 27, 2024

Citrix Gateway 12.0 unterstützt das PC-over-IP (PCoIP) -Protokoll, das das Remote-Anzeigeprotokoll für mehrere Nicht-Citrix VDI-Lösungen ist, einschließlich VMware Horizon View. PCoIP entspricht dem Citrix HDX/ICA-Protokoll und dem Microsoft RDP-Protokoll. PCoIP verwendet den UDP-Port 4172.

Wenn PCoIP über Citrix Gateway weitergeleitet wird, kann Citrix Gateway die herkömmlichen PCoIP-Remotezugriffslösungen wie View Security Server oder VMware Access Point ersetzen.

**Die folgenden Szenarien veranschaulichen die Verwendung von Citrix Gateway-fähiger VMware Horizon View Solution.**

- Benutzer von VMware Horizon PCoIP, die über das Citrix Gateway remote auf VMware Horizon View-Desktop-Pools und Anwendungspools zugreifen müssen, ohne einen Horizon View Security Server oder VMware Access Point bereitzustellen.
- PCoIP-Benutzer, die über Citrix Gateway remote auf andere PCoIP-basierte virtuelle Desktop-Lösungen zugreifen.

> **Hinweis**
>
> Citrix Gateway wird als Remotezugriffslösung bereitgestellt.

## Citrix Gateway-fähigen PCoIP-Proxys für VMware Horizon View konfigurieren

March 27, 2024

### Voraussetzungen

**Version** - Citrix ADC 12.0 oder höher

**Universelle Lizenz** - PCoIP Proxy verwendet die Clientless Access-Funktion von Citrix Gateway, was bedeutet, dass jede Citrix Gateway-Verbindung für Citrix Gateway Universal lizenziert sein muss. Stellen Sie auf dem Citrix Gateway Virtual Server sicher, dass **Nur ICA** gelöscht ist.

**Horizon View-Infrastruktur** —Eine funktionale interne Horizon View-Infrastruktur. Stellen Sie sicher, dass Sie intern ohne Citrix Gateway eine Verbindung zu Horizon View Agents herstellen können. Stellen Sie sicher, dass Horizon View **HTTP (S) Secure Tunnel** und **PCoIP Secure Gateway** auf den View-Verbindungsservern, zu denen Citrix ADC Verbindungen herstellt, nicht aktiviert sind. Die folgenden Versionen von VMware Horizon View werden unterstützt.

- Verbindungsserver: 7.0.1 und höher
- Horizon Client: 4.2.0 und höher (Windows und Mac)

**Firewall-Ports**:

Stellen Sie dabei Folgendes sicher:

- UDP 4172 und TCP 443 müssen von Horizon View Clients zum Citrix Gateway VIP geöffnet sein.
- UDP 4172 muss vom Citrix ADC SNIP für alle internen Horizon View Agents geöffnet sein.
- PCoIP Proxy wird auf Citrix ADC unterstützt, das hinter NAT bereitgestellt wird. Im Folgenden sind die wichtigen Punkte zu beachten:
  - Die Unterstützung basiert auf der FQDN-Parametereinstellung des virtuellen VPN-Servers
  - Unterstützt nur öffentlich zugängliche FQDN und nicht IP
  - Unterstützt nur 443 und 4172 Ports
  - Muss ein statisches NAT sein

**Zertifikat** —Ein gültiges Zertifikat für den Citrix Gateway Virtual Server.

**Authentifizierung** —Eine LDAP-Authentifizierungsrichtlinie/ein Server mit Classic Syntax.

**Unified Gateway (optional)** —Wenn Unified Gateway, erstellen Sie das Unified Gateway, bevor Sie PCoIP-Funktionen hinzufügen.

**RfWebUI Portal Theme** —Für den Zugriff des Webbrowsers auf Horizon View muss der Citrix Gateway Virtual Server mit dem RfWebUI-Design konfiguriert werden.

**Horizon View Client** —Der Horizon View Client muss auf dem Clientgerät installiert sein, auch wenn über das Citrix ADC RfWebUI-Portal auf veröffentlichte Horizon-Symbole zugegriffen wird.

**So konfigurieren Sie Citrix Gateway für die Unterstützung von PCoIP-Proxy für VMware Horizon View:**

1. Navigieren Sie zu **Konfiguration > Citrix Gateway-Richtlinien > PCoIP**.

2. Erstellen Sie ein virtuelles Serverprofil und ein PCoIP-Profil auf der Seite **PCoIP-Profile und Verbindungen**.

   a) Um ein virtuelles Serverprofil zu erstellen, klicken Sie auf der Registerkarte **vServer-Profile** auf **Hinzufügen**.

   b) Geben Sie einen Namen für das virtuelle Serverprofil ein.

   c) Geben Sie einen Active Directory-Domänennamen ein, der für die einmalige Anmeldung bei View-Verbindungsserver verwendet wird, und klicken Sie dann auf **Erstellen.**
   **Hinweis:** Pro Citrix Gateway Virtual Server wird nur eine einzige Active Directory-Domäne unterstützt. Außerdem wird der hier angegebene Domainname im Horizon View Client angezeigt.

   d) Klicken Sie auf **Anmelden**.

   e) Um ein PCoIP-Profil zu erstellen, klicken Sie auf der Registerkarte **Profile** auf **Hinzufügen**.

      i. Geben Sie einen Namen für das PCoIP-Profil ein.

      ii. Geben Sie die Verbindungs-URL für den internen VMware Horizon View-Verbindungsserver ein, und klicken Sie dann auf **Erstellen**.

   f) Navigieren Sie zu **Konfiguration > Citrix Gateway > Richtlinien > Sitzung**.

   g) Klicken Sie auf der rechten Seite auf die Registerkarte **Sitzungsprofile**.

   h) Erstellen oder bearbeiten Sie auf der Seite **Citrix Gateway-Sitzungsrichtlinien und -profile** ein Citrix Gateway-Sitzungsprofil.

      i. Um ein Citrix Gateway-Sitzungsprofil zu erstellen, klicken Sie auf **Hinzufügen**und geben Sie einen Namen an.

      ii. Um ein Citrix Gateway-Sitzungsprofil zu bearbeiten, wählen Sie das Profil aus und klicken auf **Bearbeiten**.

   i) Stellen Sie auf der Registerkarte **Client Experience** sicher, dass der Wert für **clientlosen Zugriffauf**Ein festgelegt ist.

   j) Stellen Sie auf der Registerkarte **Sicherheit** sicher, dass der Wert **Standard-Autorisierungsaktion** auf **ZULASSEN**festgelegt ist.

   k) Wählen Sie auf der Registerkarte **PCoIP** das erforderliche PCoIP-Profil aus und klicken Sie dann auf **Erstellen**. Auf dieser Registerkarte können Sie auch PCoIP-Profile erstellen oder bearbeiten.

   l) Klicken Sie auf **Erstellen** oder auf **OK**, um das Erstellen oder Bearbeiten des Sitzungsprofils abzuschließen.

   m) Wenn Sie ein Sitzungsprofil erstellt haben, müssen Sie auch eine entsprechende Sitzungsrichtlinie erstellen.

i. Navigieren Sie zu **Konfiguration > Citrix Gateway > Richtlinien > Sitzung**.

ii. Klicken Sie auf der rechten Seite auf die Registerkarte **Sitzungsrichtlinien**.

iii. Klicken Sie auf **Hinzufügen**, geben Sie einen Namen für die Sitzungsrichtlinie ein und wählen Sie im Menü **Profil** den gewünschten Namen des Sitzungsprofils aus.

iv. Wenn Sie die Sitzungsrichtlinie mithilfe der Standardsyntax erstellen möchten, geben Sie im Bereich Ausdruck "wahr"(ohne die Anführungszeichen) ein, und klicken Sie dann auf **Erstellen**. Hinweis: Unified Gateway ist standardmäßig Classic Syntax.

v. Wenn Sie die Sitzungsrichtlinie mit klassischer Syntax erstellen möchten, klicken Sie zuerst auf **Zur klassischen Syntax wechseln**. Geben Sie dann im Bereich Ausdruck "ns_true"(ohne die Anführungszeichen) ein und klicken Sie dann auf **Erstellen**.

n) Binden Sie das erstellte Profil und die Sitzungsrichtlinie für virtuelle PCoIP-Server an einen Citrix Gateway Virtual Server.

i. Wechseln Sie zu **Citrix Gateway > Virtuelle Server**.

ii. Auf der rechten Seite **fügen Sie** entweder einen neuen Citrix Gateway Virtual Server hinzu oder **bearbeiten Sie** einen vorhandenen Citrix Gateway Virtual Server.

iii. Wenn Sie einen vorhandenen Citrix Gateway Virtual Server bearbeiten, klicken Sie im Abschnitt **Grundeinstellungen** auf das Stiftsymbol.

iv. Klicken Sie zum Hinzufügen und Bearbeiten im Abschnitt **Grundeinstellungen** auf **Mehr**.

v. Verwenden Sie das **PCoIP vServer Profilmenü**, um das erforderliche virtuelle PCoIP-Serverprofil auszuwählen.

vi. Scrollen Sie nach unten und stellen Sie sicher, dass nur ICA gelöscht ist Dann klick **OK** um den Abschnitt **Grundeinstellungen** zu schließen.

vii. Wenn Sie einen neuen Citrix Gateway Virtual Server erstellen, binden Sie ein **Zertifikat**und binden Sie eine LDAP-Authentifizierungsrichtlinie.

viii. Scrollen Sie zum Abschnitt **Richtlinien** und klicken Sie auf das Plus-Symbol.

ix. Auf der Seite **Typ wählen** wird standardmäßig **Sitzung** und **Anforderung verwendet**. Klicken Sie auf **Weiter**.

x. Klicken Sie im Abschnitt **Policy Binding** auf **Klicken, um auszuwählen**.

xi. Wählen Sie die erforderliche Sitzungsrichtlinie aus, für die das PCoIP-Profil konfiguriert ist, und klicken Sie auf **Auswählen**.

xii. Klicken Sie auf der Seite **Policy Binding** auf **Bind**.

xiii. Wenn Sie einen Webbrowser verwenden möchten, um eine Verbindung zu VMware Horizon View herzustellen, fügen Sie rechts unter **Erweiterte Einstellungen**den Abschnitt **Portal-Designs** hinzu. Wenn Sie den Horizon View Client nur für die Verbindung mit Citrix Gateway verwenden, müssen Sie diesen Schritt nicht ausführen.

xiv. Verwenden Sie das Menü **Portal Theme**, um **RfWebUI** auszuwählen, und klicken Sie auf **OK**.

xv. In Horizon View veröffentlichte Symbole werden dem RfWebUI-Portal hinzugefügt.

> **Hinweis:** VMware verwendet zwei oder mehr Protokolle, wenn ein anderes Protokoll als RDP verwendet wird. Dies kann dazu führen, dass die Anforderungen über zwei verschiedene Back-End-Server verteilt werden. Sie können dieses Problem beheben, indem Sie eine einzelne Persistenzgruppe für alle Protokolle einrichten, um sicherzustellen, dass alle Verbindungen auf demselben virtuellen Citrix Server verbleiben.

### Schritte zum Aktivieren der USB-Umleitung

Auf USB-Geräte, die mit dem Clientcomputer verbunden sind, kann von den virtuellen Desktops und Apps aus zugegriffen werden. Im Folgenden sind die Schritte zum Aktivieren der USB-Umleitung aufgeführt:

1. Melden Sie sich bei VMware Horizon Administrator Console an.
2. Navigieren Sie zu **Inventar > Konfigurationsserver anzeigen**.
3. Wählen Sie die Registerkarte **Verbindungsserver**.
4. Wählen Sie einen aufgelisteten Verbindungsserver aus und klicken Sie auf **Bearbeiten**.
5. Wählen Sie auf der Registerkarte **Allgemein** die Option **Sichere Tunnelverbindung zur Maschine verwenden** unter **HTTP (S) Secure Tunnel Tunnel**. Geben Sie die externe URL von Citrix Gateway im Feld **Externe URL** an.

### Content Switching-Ausdruck für Unified Gateway aktualisieren

Wenn sich Ihr Citrix Gateway Virtual Server hinter einem Unified Gateway (Content Switching Virtual Server) befindet, müssen Sie den Content Switching-Ausdruck aktualisieren, um die PCoIP-URL-Pfade einzuschließen.

1. Navigieren Sie in der Citrix ADC GUI zu **Konfiguration > Traffic Management > Content Switching > Richtlinien**.
2. Hängen Sie den folgenden Ausdruck im Bereich **Ausdruck** an, und klicken Sie dann auf **OK**.

| | | | |
|---|---|---|---|
| | http.req.url.path.eq(“/broker/xml”) | http.req.url.path.contains(“/broker/resources”) | http.req.url.path.eq(“/pcoip-client”) |

### Verwenden Sie PCoIP Gateway

1. Um eine Verbindung herzustellen, muss Horizon View Client auf dem Clientgerät installiert sein. Nach der Installation können Sie entweder die Benutzeroberfläche des Horizon View Clients verwenden, um eine Verbindung zu Citrix Gateway herzustellen, oder Sie können die Citrix Gateway RfWebUI-Portalseite verwenden, um die von Horizon veröffentlichten Symbole anzuzeigen.
2. Um die aktiven PCoIP-Verbindungen anzuzeigen, gehen Sie zu **Citrix Gateway > PCoIP.**
3. Wechseln Sie auf der rechten Seite zur Registerkarte **Verbindungen**. Die aktiven Sitzungen werden mit den folgenden Daten angezeigt: Benutzername, Horizon View Client-IP und Horizon View Agent-Ziel-IP.
4. Um eine Verbindung zu beenden, klicken Sie mit der rechten Maustaste auf die Registerkarte **Verbindung**, und klicken Sie auf **Verbindung beenden**. Oder klicken Sie auf **Alle Verbindungen** beenden, um alle PCoIP-Verbindungen zu beenden.

## VMware Horizon View-Verbindungsserver konfigurieren

March 27, 2024

So unterstützen Sie PCoIP Proxy über Citrix Gateway:

1.Melden Sie sich bei **VMware Horizon Administrator Console**an.

2.Navigieren Sie zu**Inventar** -> **Konfiguration anzeigen** -> **Server**.

3.Wählen Sie die Registerkarte **Verbindungsserver**.

4.Wählen Sie einen aufgelisteten Verbindungsserver aus und klicken Sie auf **Bearbeiten**.

5.Deaktivieren Sie auf der Registerkarte **Allgemein** die Option **Sichere Tunnelverbindung zur Maschine verwenden** unter HTTP (S) Secure Tunnel.

6.Klicken Sie auf **OK**, um das Fenster **Verbindungsserver-Einstellungen bearbeiten** zu schließen.

7.Führen Sie die Schritte 4 bis 6 auf allen aufgelisteten Verbindungsservern durch.

# Automatische Proxy-Konfiguration für ausgehende Proxy-Unterstützung für Citrix Gateway

March 27, 2024

Wenn Sie das Citrix Gateway-Gerät für die Unterstützung von Proxy Auto Configuration (PAC) konfigurieren, wird die URL einer PAC-Datei an den Clientbrowser übertragen. Der Traffic vom Client wird dann gemäß den in der PAC-Datei definierten Bedingungen zu den jeweiligen Proxys umgeleitet.

Im Folgenden sind einige gängige Anwendungsfälle für PAC für ausgehenden Proxy aufgeführt:

- Konfigurieren mehrerer Proxyserver, die den Clientverkehr verarbeiten.
- Zum Lastausgleich des Proxy-Datenverkehrs über Subnetze hinweg.

## Konfigurieren Sie globale Parameter von Citrix Gateway zur Unterstützung von PAC für ausgehenden Proxy über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

## Konfigurieren Sie Citrix Gateway für die Unterstützung von PAC in einem Sitzungsprofil über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

Wo;

- **URL** —URL für den Proxyserver
- **Name** —Name der VPN-Sitzungsaktion

## Konfigurieren Sie globale Parameter von Citrix Gateway zur Unterstützung von PAC für ausgehenden Proxy über die GUI

1. Navigieren Sie zu **Konfiguration > Citrix Gateway > Globale Einstellungen**.
2. Klicken Sie auf der Seite **Allgemeine Einstellungen** auf **Allgemeine Einstellungen ändern** und wählen Sie dann die Registerkarte **Kundenerlebnis** aus.

3. Wählen Sie auf der Registerkarte **Client Experience Erweiterte Einstellungenaus**, und wählen Sie dann die **Registerkarte Proxyaus**.
4. Wählen Sie auf der**Registerkarte Proxy Browser** und dann **Automatische Konfiguration verwenden** aus.
5. Geben Sie im Feld **URL zu Auto Proxy Config File** die URL für die erforderliche PAC-Datei ein.
6. Klicken Sie auf **Erstellen**.

### Konfigurieren Sie Citrix Gateway für die Unterstützung von PAC im Sitzungsprofil über die GUI

1. Navigieren Sie zu **Konfiguration > Citrix Gateway > Richtlinien > Sitzung**.
2. Erstellen Sie auf der Seite Citrix Gateway-**Sitzungsrichtlinien und -profile**ein Citrix Gateway-Sitzungsprofil.
3. Wählen Sie die Registerkarte **Sitzungsprofile** aus, klicken Sie auf **Hinzufügen**und geben Sie einen Namen ein.
4. Wählen Sie auf der Registerkarte**Client ExperienceErweiterte Einstellungen**und dann die Registerkarte**Proxy** aus.
5. Wählen Sie auf der Registerkarte**ProxyBrowser**und dann**Automatische Konfiguration verwenden**aus.
6. Geben Sie im Feld**URL zu Auto Proxy Config File**die URL für die erforderliche PAC-Datei ein.
7. Klicken Sie auf **Erstellen**.
8. Klicken Sie auf **Erstellen**.

## Konfigurationsunterstützung für SameSite-Cookie-Attribut

March 27, 2024

Das `SameSite` Attribut gibt dem Browser an, ob das Cookie für den standortübergreifenden Kontext oder nur für denselben Site-Kontext verwendet werden kann. Wenn auf eine Anwendung im standortübergreifenden Kontext zugegriffen werden soll, kann dies nur über die HTTPS-Verbindung erfolgen. Einzelheiten finden Sie unter RFC6265.

Bis Februar 2020 wurde das `SameSite` Attribut in der Citrix ADC Appliance nicht explizit festgelegt. Der Browser nahm den Standardwert (Keine). Die Nichteinstellung des `SameSite` Attributs hatte keine Auswirkungen auf die Bereitstellungen von Citrix Gateway und Citrix ADC AAA.

Bei bestimmten Browser-Upgrades wie Google Chrome 80 ändert sich das standardmäßige domänenübergreifende Verhalten von Cookies. Das `SameSite` Attribut kann auf einen der folgenden Werte festgelegt werden. Der Standardwert für Google Chrome ist auf Lax festgelegt. Für bestimmte

Versionen anderer Browser ist der Standardwert für das SameSite Attribut möglicherweise immer noch auf Keine festgelegt.

- **Keine**: Weist darauf hin, dass der Browser das Cookie im standortübergreifenden Kontext nur für sichere Verbindungen verwendet.
- **Lax**: Zeigt an, dass der Browser das Cookie für Anfragen im Kontext derselben Website verwendet. Im Cross-Site-Kontext können nur sichere HTTP-Methoden wie GET-Request das Cookie verwenden.
- **Streng**: Verwenden Sie das Cookie nur im selben Site-Kontext.

Wenn das Cookie kein SameSite Attribut enthält, übernimmt Google Chrome die Funktionalität von SameSite = Lax.
Daher teilt Google Chrome für Bereitstellungen innerhalb eines Iframes mit standortübergreifendem Kontext, bei denen Cookies vom Browser eingefügt werden müssen, keine standortübergreifenden Cookies. Infolgedessen wird der Iframe auf der Website möglicherweise nicht geladen.

## Konfiguration des SameSite Cookie-Attributs

Ein neues Cookie-Attribut mit dem Namen SameSite wird den virtuellen VPN- und Citrix ADC AAA-Servern hinzugefügt. Dieses Attribut kann auf globaler Ebene und auf virtueller Serverebene festgelegt werden.

Um das SameSite Attribut zu konfigurieren, müssen Sie Folgendes ausführen:

1. Legen Sie das SameSite Attribut für den virtuellen Server fest
2. Binden Sie Cookies an die patset (wenn der Browser siteübergreifende Cookies fallen lässt, werden sie vom Browser fallen gelassen)

### Festlegen des SameSite Attributs über die CLI

Verwenden Sie die folgenden Befehle, um das SameSite Attribut auf der Ebene des virtuellen Servers festzulegen.

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]
set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

Verwenden Sie die folgenden Befehle, um das SameSite Attribut auf globaler Ebene festzulegen.

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]
set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

**Hinweis**: Die Einstellung auf virtueller Serverebene nimmt den Vorzug gegenüber der Einstellung auf globaler Ebene vor. Citrix empfiehlt, das `SameSite` Cookie-Attribut auf der Ebene des virtuellen Servers festzulegen.

### Cookies `patset` über die CLI an die binden

Wenn der Browser Cross-Site-Cookies löscht, können Sie diese Cookie-Zeichenfolge an die vorhandene binden, `ns_cookies_SameSite patset` sodass das `SameSite` Attribut zum Cookie hinzugefügt wird.

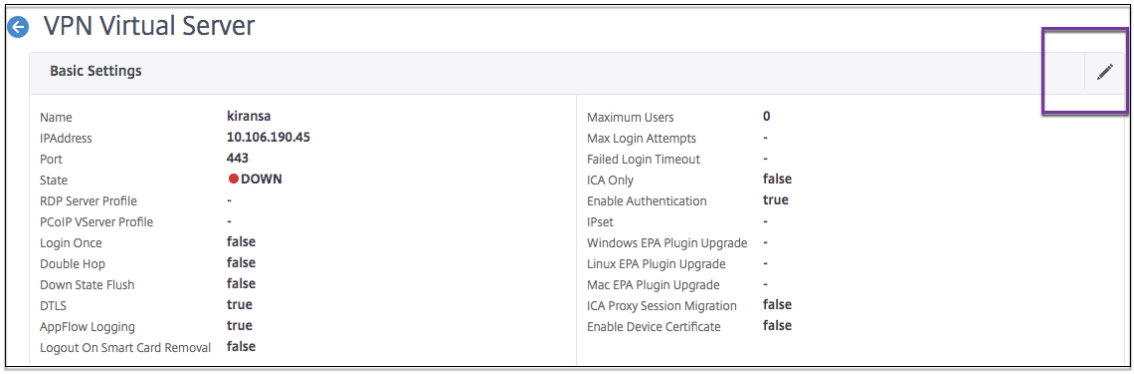
**Beispiel:**

```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```

### Festlegen des SameSite-Attributs über die GUI

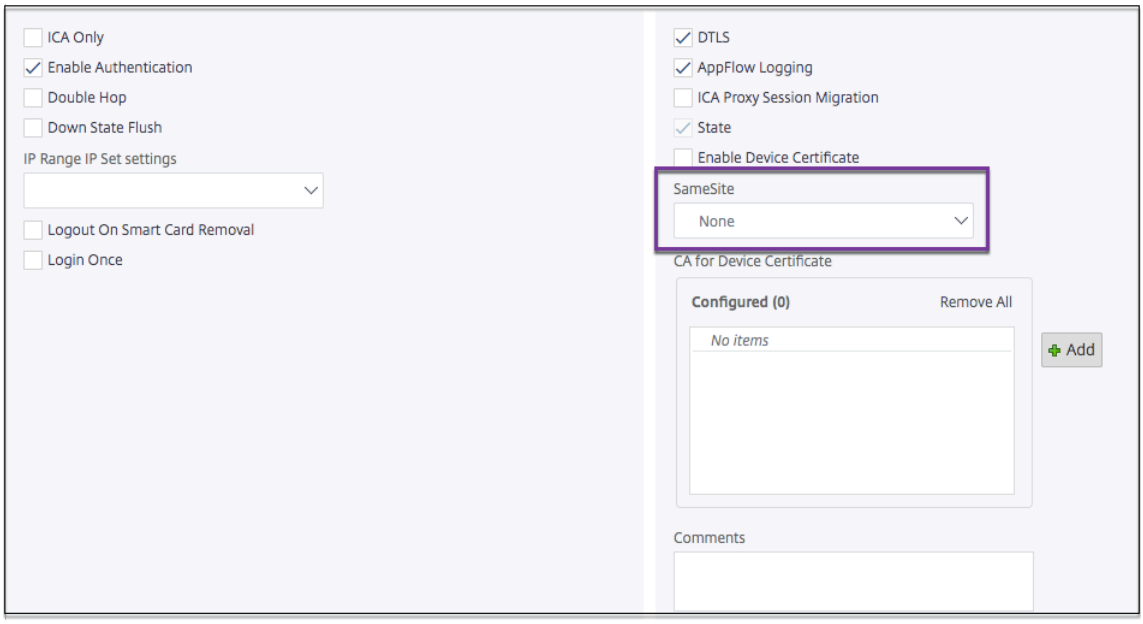
**So legen Sie das `SameSite` Attribut auf der Ebene des virtuellen Servers fest:**

1. Navigieren Sie zu **Citrix Gateway > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Wählen Sie das Bearbeitungssymbol im Abschnitt **Grundeinstellungen** aus und klicken Sie auf **Mehr**.



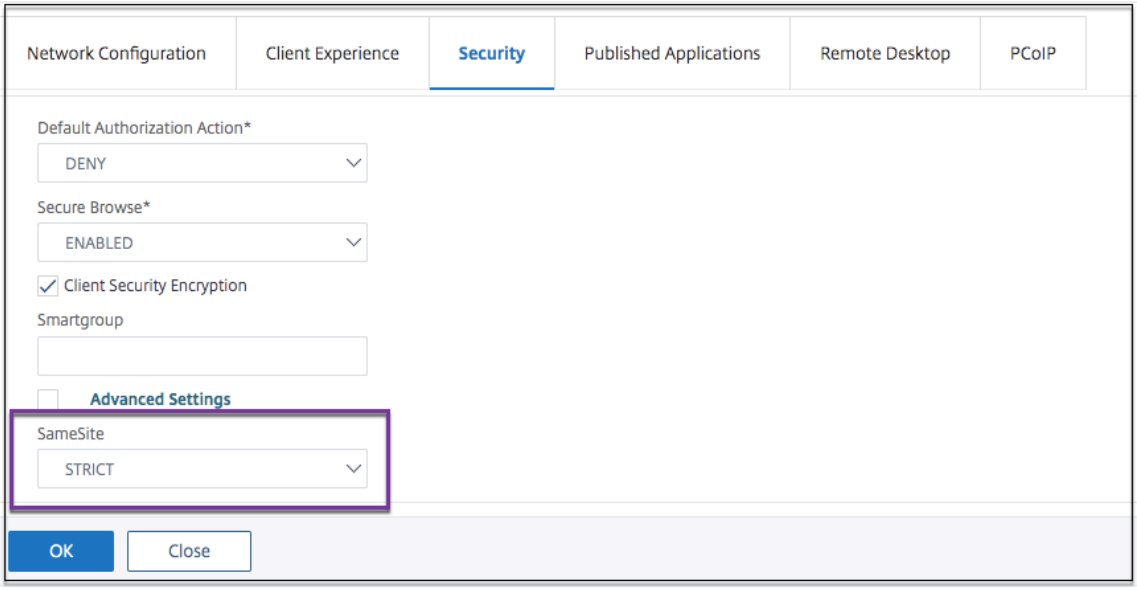

4. Wählen Sie in **SameSite**die Option nach Bedarf aus.




**So setzen Sie das `SameSite` Attribut auf globaler Ebene:**

1. Navigieren Sie zu **Citrix Gateway > Globale Einstellungen > Globale Einstellungen ändern.**
2. Klicken Sie auf die Registerkarte **Sicherheit**.
3. Wählen Sie in **`SameSite`**die Option nach Bedarf aus.



# Optimieren des Netzwerkverkehrs mit CloudBridge

January 28, 2024

Wenn sich Benutzer mit dem Citrix Gateway-Plug-In anmelden, kann die Verbindung mithilfe des CloudBridge-Plug-Ins optimiert werden, das von CloudBridge auf dem Benutzergerät installiert wird. Wenn die Verbindung mithilfe des CloudBridge-Plug-Ins optimiert wird, wird der Netzwerkverkehr über Citrix Gateway komprimiert und beschleunigt. Wenn CloudBridge für eine Verbindung aktiviert ist, werden TCP-Komprimierungsrichtlinien auf Citrix Gateway deaktiviert.

Das CloudBridge-Plug-In wird bereitgestellt und funktioniert mit dem Citrix Gateway-Plug-In.

Citrix Gateway unterstützt die Versionen 5.5 und 6.1 des Repeater-Plug-ins sowie die Versionen 6.2 und 7.0 des CloudBridge-Plug-Ins.

CloudBridge-Optimierung und Flusssteuerung haben Vorrang vor Citrix Gateway-Optimierungsfunktionen, die dynamische Inhaltsänderung erfordern. Wenn die CloudBridge-Optimierung für HTTP-Datenverkehr aktiviert ist, sind die folgenden Citrix Gateway-Features nicht verfügbar:

- Single Sign-On bei Webanwendungen
- Dateitypzuordnung
- HTTP-Autorisierung

Um Single Sign-On für Webanwendungen zu ermöglichen, können Sie die Beschleunigung auf HTTP deaktivieren. Dazu verwenden Sie die Befehlszeile. Melden Sie sich bei der seriellen Citrix Gateway-Konsole an, und geben Sie an der Eingabeaufforderung Folgendes ein:

add vpn trafficAction ssoact http -SSO ON

Netzwerkverkehr, der für einen konfigurierten HTTP-Port auf Citrix Gateway bestimmt ist, wird automatisch von der CloudBridge-Optimierung ausgeschlossen. Dies ist die Standardeinstellung. Wenn Sie eine Datenverkehrsrichtlinie für die CloudBridge-Optimierung auf einem HTTP-Port konfigurieren, wird die Datenverkehrsrichtlinie berücksichtigt und der Netzwerkverkehr von CloudBridge optimiert. Die Citrix Gateway-Optimierungsfunktionen sind jedoch für den gesamten Datenverkehr deaktiviert, der von dieser Richtlinie betroffen ist. CloudBridge kann den Netzwerkverkehr für Nicht-HTTP-Ports beschleunigen, ohne dass andere Citrix Gateway-Funktionen beeinträchtigt werden.

Sie verwenden eine Datenverkehrsrichtlinie, um Benutzerverbindungen für die Verwendung des CloudBridge-Plug-Ins zu konfigurieren. Anschließend können Sie die Richtlinie an Benutzer, Gruppen, virtuelle Server oder global binden. Die Richtlinie wird basierend auf der Bindung der Richtlinie oder der Prioritätsnummer, die Sie der Richtlinie geben, priorisiert.

### So erstellen Sie eine Verkehrsrichtlinie

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway-Richtlinien, und klicken Sie dann auf Datenverkehr.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie **unter Name** einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf **Neu**.
5. Geben Sie unter **Name** einen Namen für das Profil ein.
6. Wählen Sie im **Branch Repeater** EIN aus, und klicken Sie dann auf **Erstellen**.
7. Wählen **Sie im Dialogfeld Datenverkehrsrichtlinie erstellen** neben **Ausdruck hinzufügen einen Ausdruck** aus, der die Datenverkehrstypen darstellt, um die CloudBridge-Beschleunigung zu aktivieren, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen**, und klicken Sie dann auf **Schließen**.

Wählen Sie beim Hinzufügen eines Ausdrucks einen Netzwerkausdruck aus, um dieselben IP-Adressen und Portbereiche zu verwenden, für die CloudBridge zur Beschleunigung konfiguriert ist. Damit die CloudBridge-Beschleunigung erfolgt, müssen die in Citrix Gateway konfigurierten Datenverkehrstypen mit den in CloudBridge konfigurierten Service-Klassenrichtlinien übereinstimmen.

Der gesamte TCP-Datenverkehr profitiert von der CloudBridge-Beschleunigung. Wenn Sie die einmalige Anmeldung verwenden möchten, sollten Sie den HTTP-Datenverkehr nicht beschleunigen, da die Beschleunigung das einmalige Anmelden deaktiviert.

## RfWebUI Persona auf Gateway UX Konfiguration

March 27, 2024

RfWebUI Persona ist ein Thema, das eine neue Anmelde- und Portalseite für Citrix Gateway-Benutzer bereitstellt, die sich über Citrix Gateway anmelden. Das Portal bietet Benutzern von Receiver, StoreFront und Citrix Endpoint Management dieselbe Benutzeroberfläche wie beim direkten Zugriff auf eines dieser Produkte.

### Wann benutzt man RfWebUI Persona

Verwenden Sie die RFWebUI Persona in Citrix Gateway, wenn Sie eine Einzelfensteransicht aller Anwendungen benötigen, die von verschiedenen CITRIX Produkten bereitgestellt werden, wie Web- und Software as a Service (SaaS) -Anwendungen, virtuelle Windows-Anwendungen und Desktops.

Die folgenden Szenarien veranschaulichen die Verwendung von RfWebUI Persona.

- Ein Benutzer greift über Gateway auf StoreFront zu und findet eine andere GUI als die, die er beim Zugriff auf das Produkt ohne Gateway sieht.
  **Lösung:** Wenn der Benutzer über das Gateway auf StoreFront zugreift, bietet das RFWebUI-Design eine ähnliche Benutzeroberfläche, wie er beim Zugriff auf das Produkt ohne Verwendung des Gateway sieht.
- Ein Benutzer greift mit Gateway auf die Citrix Workspace-App, StoreFront- und Citrix Endpoint Management-Anwendungen zu und hat Schwierigkeiten, die gewünschten Anwendungen zu finden, da die Anwendungen nicht logisch gruppiert sind.
  **Lösung:** Die RfWebUI Persona bietet eine Benutzererfahrung in einem Bereich, indem eine logische Bündelung von Anwendungen erstellt wird, die von verschiedenen Produkten wie Receiver, StoreFront, Citrix Endpoint Management usw. bereitgestellt werden.

## Funktionalitäten von RFWebUI Persona

Die neue RFWebUI bietet folgende Funktionen:

- GO
- Aggregation von Anwendungen
- Benutzerkonfigurierte Proxylinks für Remotedesktopprotokoll (RDP)
- Lieblingsanwendungen

### GO

**GO:** Die Go-Funktion bietet Zugriff auf Webseiten über clientloses VPN. Der Benutzer gibt einfach die URL in den **URL-Bereich** auf der Registerkarte **Lesezeichen** ein und klickt auf **GO**.

Derzeit unterstützt die **GO-Funktion** nur Outlook Web Application (OWA) und SharePoint-URLs.

> **Hinweis**
> Die Registerkarte **GO** ist nur sichtbar, wenn der `clientlessAccessVPNMode` Parameter in der Sitzungsrichtlinie **Aktiviert**ist.

### Aggregation von Anwendungen

**Aggregation von Anwendungen:** Das Thema RfWebUI bietet eine einseitige Ansicht, indem die von verschiedenen Produkten bereitgestellten Anwendungen unter beschreibenden Bannern gebündelt werden. Beispielsweise befinden sich alle von einem Citrix ADC-Administrator konfigurierten VPN-URLs in einem Bundle mit dem Namen **Web- und SaaS-Anwendungen**, und benutzerspezifische Web-Lesezeichen befinden sich unter **Persönliche Lesezeichen**. Wenn Citrix Virtual Apps and Desktops Anwendungspakete in StoreFront konfiguriert sind, listet die Einzelfensteransicht in Citrix Gateway diese Bundles ebenfalls auf.

#### Benutzerkonfigurierte RDP-Proxy-Links

Benutzer können einen RDP-Proxy-Link als persönliche Lesezeichen hinzufügen. Die persönlichen Lesezeichen werden auf der Registerkarte **Desktops** angezeigt.

Die folgenden RDP-Modi werden unterstützt:

- Einzelnes Gateway
- Zustandsloses (duales) Gateway

> **Hinweis:** Ein Benutzer kann RDP-Proxy-Links nur hinzufügen, wenn ein `RDPclientprofile` konfiguriert ist. Weitere Informationen zu RDP-Konfigurationen finden Sie in der RDP-Proxy-Dokumentation.

#### Lieblingsanwendungen

Benutzer können die gewünschten Anwendungen, die unter **Web- und SaaS-Anwendung** und unter **Persönliche Lesezeichen** zu **FAVORITEN** aufgeführt sind, **hinzufügen, indem sie auf den Link Zu Favoriten** hinzufügen neben dem Anwendungsnamen klicken. Die einmal hinzugefügten Anwendungen können auf der Registerkarte **FAVORITEN** angezeigt werden. Dasselbe kann auch von der Registerkarte **FAVORITEN** entfernt werden, indem Sie auf den Link **ENTFERNEN** neben der Anwendung auf der Registerkarte **FAVORITEN** klicken.

### Überlegungen bei der Aktivierung der RfWebUI Persona

Die RfWebUI-Persona unterstützt Folgendes nicht vollständig:

**Fileshare-Funktion:** Die Fileshare-Funktion für den Zugriff auf SMB-Dateifreigaben wird nicht unterstützt.
**E-Mail Home:** Der **E-Mail Home** VPN-Parameter ist nicht als eingebettete Ansicht für das Citrix Gateway-Portal verfügbar. Auf sie kann als Anwendung im **Web- und SaaS** Apps-Bundle unter der Registerkarte **APPS** von RfWebUI zugegriffen werden.
**Java Client:** Der browserbasierte Java-Client zum Einrichten eines SSL-Tunnels ist in diesem Thema nicht verfügbar.

#### Konfigurieren von RfWebUI Persona

**So wenden Sie die RfWebUI Persona an**:

1. Navigieren Sie in der Citrix ADC-Oberfläche zu **Konfiguration > Citrix Gateway Portal Themes**.
2. Aktivieren Sie auf der Seite **Portal Themes** das Kontrollkästchen **RfWebUI**.
3. Klicken Sie oben rechts auf der Seite **Portal-Themes** auf das **Speichern-Symbol**.

4. Klicken Sie im Dialogfeld **Bestätigung speichern** auf **Ja**.

## RfWebUI Konfigurationsparameter

March 27, 2024

Das Gesamtverhalten des Citrix Gateway-Portals wird durch zwei Konfigurationsdateien beeinflusst: die lokale Citrix Gateway-Konfigurationsdatei und die StoreFront-Datei.

Abhängig von Ihrer Bereitstellung können Sie das Verhalten des Citrix Gateway-Portals ändern, indem Sie die Eigenschaften in der Datei "plugins.xml"ändern. Diese Datei wird als Konfigurationsdatei im Browser angezeigt, für die es sich um eine Anforderung handelt `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

Während der Anmeldung werden die Citrix Gateway-Konfigurationsdateien verwendet. Bei einer Verbindung mit StoreFront sendet StoreFront jedoch eine neue Konfiguration und die frühere Konfiguration wird überschrieben. Dieses Verhalten unterscheidet sich für clientloses VPN und ICA.

Für ICA hat die StoreFront-Konfiguration immer Vorrang, aber einige der Verhaltensweisen im clientlosen VPN, die von der Citrix Gateway-Konfiguration beeinflusst werden, bleiben auch nach der Aktualisierung der neuen Konfiguration von StoreFront erhalten.

In der folgenden Tabelle sind die Parameter aufgeführt, die die Konfiguration beschreiben, die Vorrang vor clientlosem VPN und ICA hat.

| Config-Typ | Sub-Konfigurationstyp | Parameter | Clientloses VPN | ICA | Beschreibung |
|---|---|---|---|---|---|
| Sitzung für clientloses VPN/AuthManager für ICA | - | loginFormTimeout | Citrix Gateway | - | Definiert die Zeit in Minuten für das Timeout der Anmeldeseite |
| Plug-In-Assistent | - | aktiviert | StoreFront | StoreFront | Den Plug-in-Assistenten aktivieren oder deaktivieren |

| Config-Typ | Sub-Konfigurationstyp | Parameter | Clientloses VPN | ICA | Beschreibung |
|---|---|---|---|---|---|
| Plug-In-Assistent | - | upgradeAtLogin | StoreFront | StoreFront | Fordert bei der Anmeldung zum Upgrade des Plug-ins auf |
| Plug-In-Assistent | - | showAfterLogin | Citrix Gateway | StoreFront | Zeigt die Aufforderung des Plug-ins nach der Anmeldung |
| Plug-In-Assistent | - | showOnlyIfRequiredByApps | Citrix Gateway | StoreFront | Zeigt die Aufforderung des Plug-ins nach der Anmeldung an, falls von den Apps gefordert |
| Plug-In-Assistent | macOS/win32 | path | Citrix Gateway | StoreFront | Definiert den Download-Pfad für die Plug-ins |
| Plug-In-Assistent | protocolHandler | aktiviert | Citrix Gateway | StoreFront | Vor dem Start des Plug-ins die Protokoll-handlerseite umschalten |
| Plug-In-Assistent | protocolHandler | platforms | Citrix Gateway | StoreFront | Identifiziert die unterstützte Plattform für das Plug-In |

| Config-Typ | Sub-Konfigurationstyp | Parameter | Clientloses VPN | ICA | Beschreibung |
|---|---|---|---|---|---|
| Plug-In-Assistent | - | skipDoubleHopCheckWithCitrixGateway | Disabled | StoreFront | Double-Hop-Citrix Gateway-Konfigurationsprüfung für ICA-Passthrough umschalten |
| Benutzeroberfläche | | frameOptions | Nicht verfügbar | Nicht verfügbar | - |
| Benutzeroberfläche | | autoLaunchDesktop | StoreFront | StoreFront | Aktivieren oder deaktivieren Sie den Desktop-Start |
| Benutzeroberfläche | workspaceControl | aktiviert | StoreFront | StoreFront | Workspace Control aktivieren oder deaktivieren |
| Benutzeroberfläche | workspaceControl | autoReconnectAtLogon | StoreFront | StoreFront | Umschalten, um vorherigen Sitzung automatisch wieder zu verbinden, falls verfügbar |
| Benutzeroberfläche | workspaceControl | logoffAction | StoreFront | StoreFront | Definiert das Abmeldeverhalten von Citrix Workspace |
| Benutzeroberfläche | workspaceControl | showReconnectButton | StoreFront | StoreFront | Die Schaltfläche **Wiederverbinden** ein- oder ausblenden |

| Config-Typ | Sub-Konfigurationstyp | Parameter | Clientloses VPN | ICA | Beschreibung |
|---|---|---|---|---|---|
| Benutzeroberfläche | workspaceControl | showDisconnectButton | StoreFront | StoreFront | **Disconnect** ein- oder ausblenden |
| Benutzeroberfläche | workspaceControl | showDesktopsView | StoreFront | StoreFront | Ein- oder Ausblenden der Desktops-Ansicht |
| Benutzeroberfläche | workspaceControl | showAppsView | StoreFront | StoreFront | Ein- oder Ausblenden der Apps-Ansicht |
| Benutzeroberfläche | workspaceControl | defaultView | StoreFront | StoreFront | Wählen Sie entweder die Desktop-Ansicht oder die App-Ansicht |
| Benutzeroberfläche | receiverConfiguration | aktiviert | StoreFront | StoreFront | Umschalten Receiver-Konfiguration |
| Benutzeroberfläche | receiverConfiguration | showOnlyIfRequiredByApps | CitrixGateway | Citrix Gateway | Receiver-Eingabeaufforderung anzeigen, falls für App erforderlich |
| Benutzeroberfläche | receiverConfiguration | downloadURL | StoreFront | StoreFront | Download-URL für Receiver |
| Benutzeroberfläche | appShortcuts | aktiviert | StoreFront | StoreFront | Aktivieren oder Deaktivieren der App-Verknüpfung |
| Benutzeroberfläche | appShortcuts | allowSessionReconnect | StoreFront | StoreFront | Sitzungswiederverbindung zulassen |

# Anpassung des Gateway-Portals mit benutzerdefinierten Plug-Ins

March 27, 2024

Citrix Gateway RfWebUI-Framework bietet die Möglichkeit, die benutzerdefinierten Plug-Ins hinzuzufügen, um ihr Gateway-Portal anzupassen. Diese benutzerdefinierten Plug-Ins können verwendet werden, um dem Gateway umfangreiche Funktionen hinzuzufügen, z. B. wenn Sie eine ganz neue Seite im Gateway-Flow hinzufügen möchten. Für andere Anwendungsfälle kann der Code zu der benutzerdefinierten Skriptdatei hinzugefügt werden, die für Gateway-Designs am Speicherort/bereitgestellt wird`var/netscaler/logon/themes/<custom_theme>/script.js`.

1. Um ein benutzerdefiniertes Plug-in hinzuzufügen, erstellen Sie die JavaScript-Datei am Speicherort `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`. Zum Beispiel finden Sie die folgenden Plug-Ins in `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`.

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   Es wird empfohlen, den Namen des Plugins im Format `<plugin_name>`.js einzugeben.

   Alle diese Plug-In-Dateien werden vom RfWebUI-Framework abgerufen, das für die Funktionalität erforderlich ist.

2. Verwenden Sie nach dem Erstellen der Plug-In-Datei den folgenden Code als Beispiel, um das Plug-in im RfWebUI-Framework zu registrieren.

```
1          (function ($) {
2
3                      CTXS.ExtensionAPI.addPlugin( {
4
5                                  Name : " plugin name " ,
6                                  initialize: function() {
7    }
8
9                       }
10  );
11              }
12  )(jQuery);
13 <!--NeedCopy-->
```

   Hierbei gilt:

   **name** ist der Name, der dem Plug-in gegeben wurde. Es wird als Identifikator für das Plug-in verwendet.

**initialize** nimmt die Funktion als den Parameter, mit dem das Plug-in initialisiert wird.

3. Geben Sie den Namen des Plugins und die Initialisierungsfunktion in die Funktion `CTXS.ExtensionAPI.addPlugin()` ein, um das Plug-in zu registrieren.
   Der hinzugefügte Plug-In-Name und -Speicherort muss an diesem Speicherort in der Datei plugins.xml registriert sein `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

4. Nach dem Schreiben des Plug-In-Codes müssen der neu hinzugefügte Plug-In-Name und -Speicherort bei der Datei `plugins.xml` am Speicherort `/var/netscaler/logon/themes/<custom_theme>/plugins.xml` registriert werden. Das Plug-in muss mit dem Tag `plug-in` registriert sein.

```
<plugins>
<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
    .js"/>
<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"
    />
</plugins>
<!--NeedCopy-->
```

5. Geben Sie einen Namen und src für das Plug-in ein, damit RfWebUI das Plug-in identifizieren und abrufen kann.

### Beispiel-Konfiguration

Die folgenden Beispielkonfigurationen können verwendet werden, um ein benutzerdefiniertes Plug-in hinzuzufügen, um der Citrix Gateway-Anmeldeseite eine Fußzeile hinzuzufügen.

1. Erstellen Sie die JavaScript-Plug-In-Datei am Speicherort, `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/.`

2. Nennen Sie das Plug-in als ns-footer.js
   `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js`

3. Fügen Sie dem registrierten Plug-in der RfWebUI den folgenden Code hinzu und fügen Sie in der Initialisierungsfunktion die Fußzeile zum Gateway hinzu.

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in
        configuration
    initialize: function () {

        CTXS.Extensions.beforeLogon = function (callback) {
```

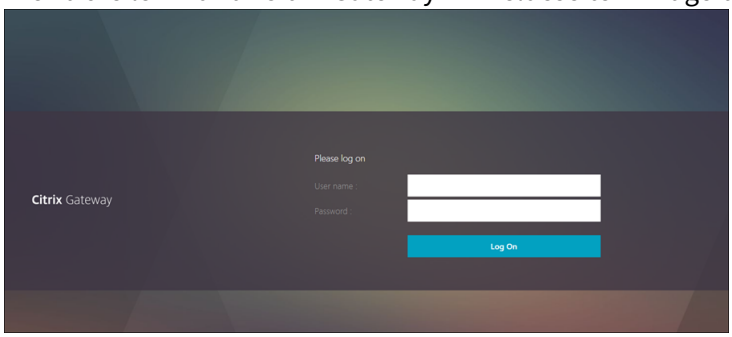
 

```
 9
10              $("#customExplicitAuthBottom").append("<div style='
                    text-align:center;color:white;font-size:15px;'><br>
                    Disclaimer<BR><BR>"+
11                   " Access to this website is restricted to
                        employees of Login Consultants<BR></div>");
12              callback();
13          }
14  ;
15      }
16
17  }
18  );
19  }
20  )(jQuery);
21  <!--NeedCopy-->
```

4. Speichern Sie die Datei.
5. Fügen Sie den Namen und src in der plugins.xml am Speicherort hinzu `var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

```
1  <plugins>
2  <plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />
3  <plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
       .js" />
4  <plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js"
       />
5  <plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />
6  </plugins>
7  <!--NeedCopy-->
```

6. Konfigurieren Sie das benutzerdefinierte Design, für das das Plug-in hinzugefügt wurde.
7. Spülen Sie den Cache mithilfe des Befehls `flush cache contentgroup loginstaticobjects` .
8. Laden Sie den Portalbildschirm neu.
   Die Fußzeile wird zur Citrix Gateway-Anmeldeseite hinzugefügt.



# Anmeldeschema erstellen und anpassen

March 27, 2024

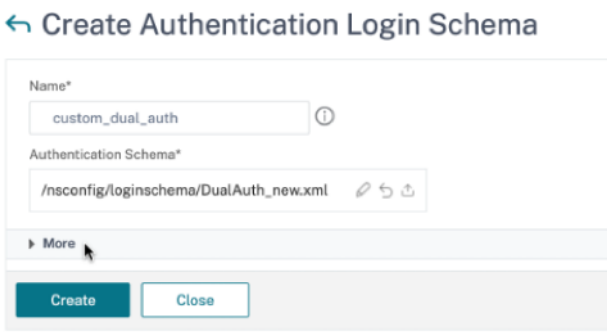
Das Anmeldeschema ist die XML-Datei, die die Struktur für die formularbasierte Authentifizierung bereitstellt.
Benutzer können eine Vielzahl von Authentifizierungsformularen verwenden, indem sie eine Reihe von Benutzeroberflächenkonstrukten verwenden, die einfachen HTML-Formularen ähneln.

Bei nFactor-Authentifizierungen werden Authentifizierungsfaktoren miteinander verkettet. Jeder Faktor kann unterschiedliche Anmeldeseiten oder -dateien haben. In einigen Authentifizierungsszenarien können Benutzern mehrere Anmeldebildschirme angezeigt werden. Sie können auch ein Anmeldeschema die Informationen sammeln lassen, die an mehrere Faktoren weitergegeben werden können, damit letztere Faktoren kein anderes Anmeldeschema anzeigen müssen.

Die XML-Dateien des Anmeldeschemas sind in der Citrix ADC Appliance in enthalten `/nsconfig/loginschema/LoginSchema`.

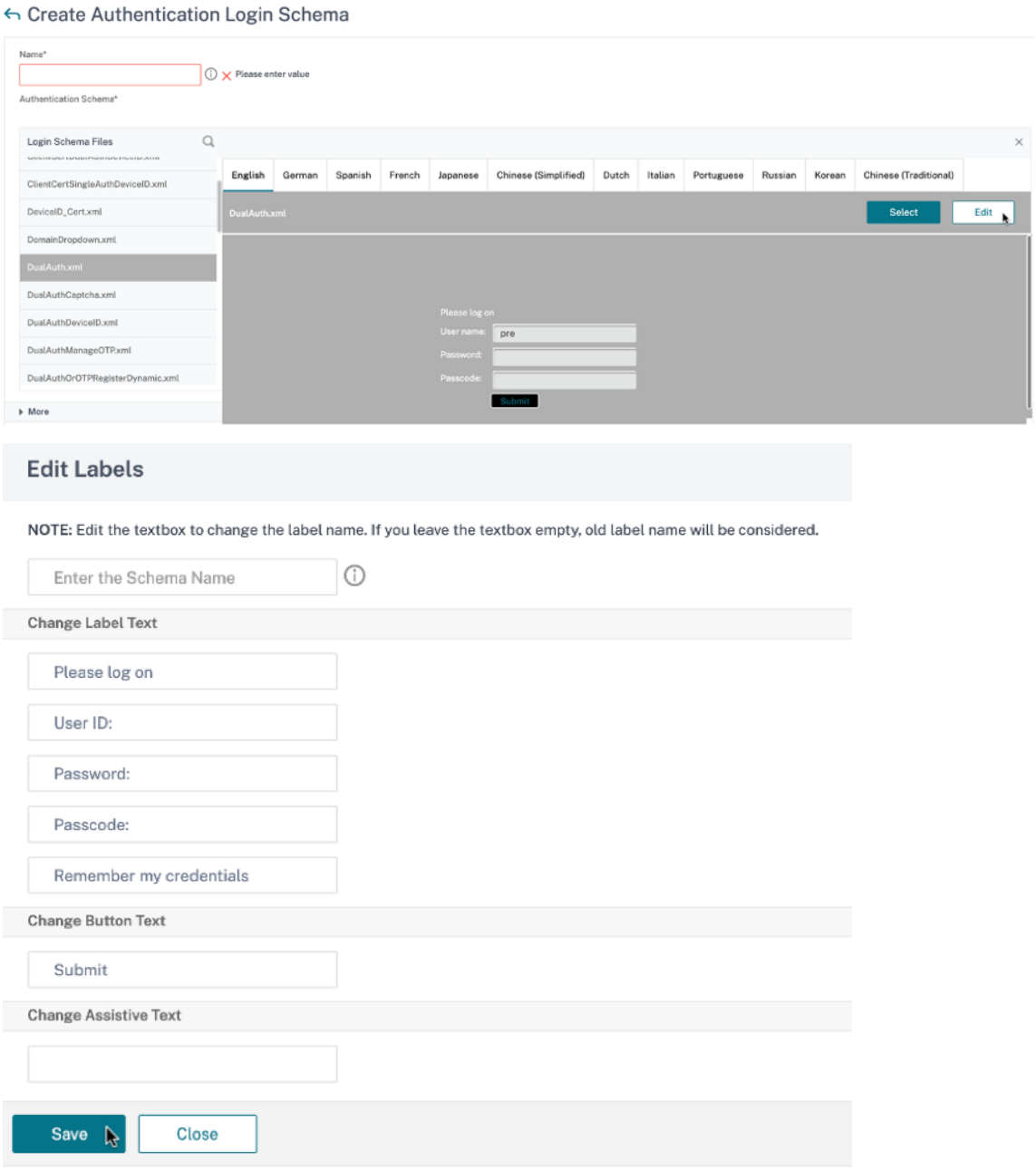
## Erstellen Sie ein Login-Schema-Profil

1. Navigieren Sie zu **Sicherheit > AAA > Anmeldeschema**.
2. Klicken Sie auf die Registerkarte **Profile** und dann auf **Hinzufügen**.
3. Klicken Sie im **Authentifizierungsschema**auf das Stiftsymbol.




4. Klicken Sie auf den Ordner **LoginSchema**, um die darin enthaltenen Dateien anzuzeigen.
5. Wählen Sie eine der Dateien aus und führen Sie die Änderungen nach Bedarf durch.
    - Ändern Sie die Beschriftungen, indem Sie oben rechts auf die Schaltfläche Bearbeiten klicken.
    - Bearbeiten Sie das Schema, indem Sie die Sprache auswählen.



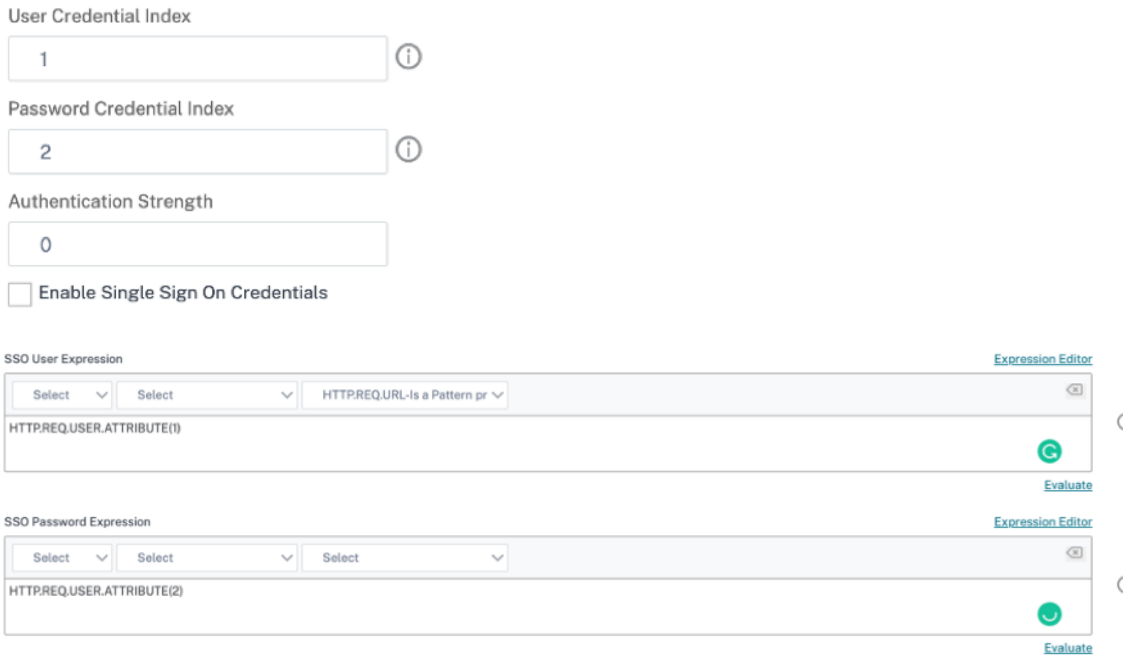

**Hinweis:** Wenn Sie die Änderungen nach der Änderung speichern, wird eine neue Schema-XML-Datei mit den Änderungen erstellt.

6. Klicken Sie rechts oben auf **Auswählen**, um das geänderte Schema-XML auszuwählen.
7. Geben Sie einen Namen für das Anmeldeschema ein und klicken Sie auf **Mehr**

   **Hinweis:** Sie können die bereits eingegebenen Anmeldeinformationen an anderer Stelle verwenden. Beispielsweise können Sie den Benutzernamen und eines der Kennwörter für die einmalige Anmeldung bei StoreFront verwenden. Sie können auf **Mehr** klicken und eindeutige Werte für die Indizes eingeben. Diese Werte können zwischen 1 und 16 liegen. Sie können in

einer Verkehrsrichtlinie oder einem Profil auf diese Indexwerte verweisen, indem Sie den Ausdruck REQ.USER.ATTRIBUTE (#) verwenden.




8. Klicken Sie auf **Erstellen**, um das Anmeldeschema-Profil zu erstellen.

### Binden eines Anmeldeschemaprofils an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver

Um ein Anmeldeschemaprofil an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver zu binden, müssen Sie zunächst eine Richtlinie für das Anmeldeschema erstellen. Richtlinien für Anmeldeschemas sind nicht erforderlich, wenn das Anmeldeschemaprofil an ein Authentifizierungsrichtlinienlabel gebunden wird.

So erstellen und binden Sie eine Richtlinie für das Login-Schema:

1. Navigieren Sie zu **Sicherheit > AAA > Anmeldeschema**.
2. Klicken Sie auf die Registerkarte **Richtlinien** und dann auf **Hinzufügen**.
3. Wählen Sie unter **Profil**das zuvor erstellte Anmeldeschema-Profil aus.
4. Geben Sie unter **Regel**den Standardsyntaxausdruck ein und klicken Sie auf **Erstellen**.

## Portalanpassungen über die Admin-Benutzeroberfläche

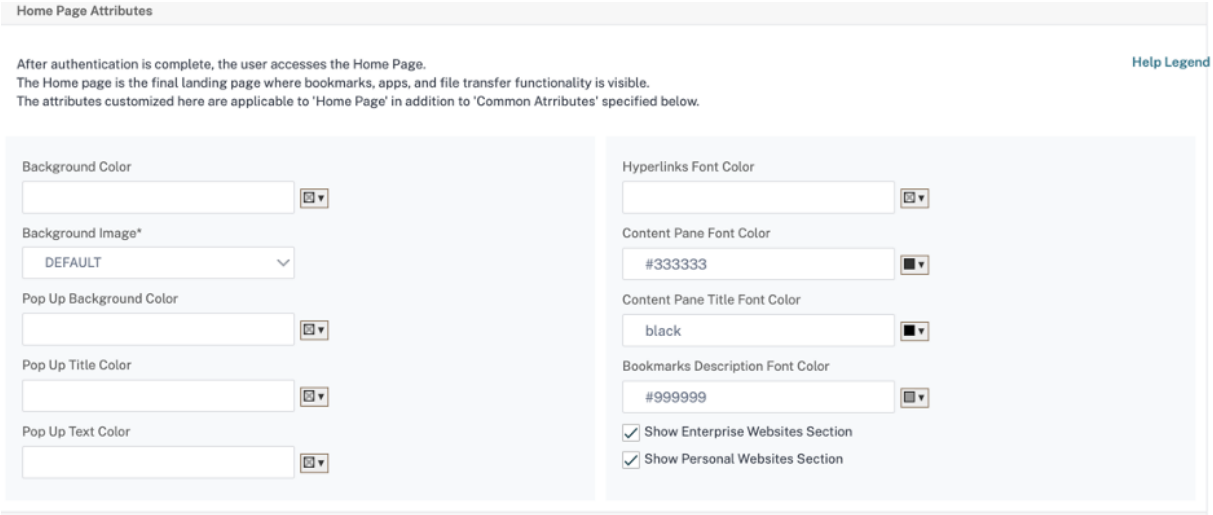
March 27, 2024

Administratoren können die Portalthemen anpassen, indem sie die benutzerdefinierten Themen erstellen, um das personalisierte Erscheinungsbild des Benutzerportals zu erreichen. Benutzerdefinierte Designs können basierend auf den Themen RfWebUI, Default, X1 und GreenBubble erstellt werden.

**So erstellen Sie die benutzerdefinierten Themen:**

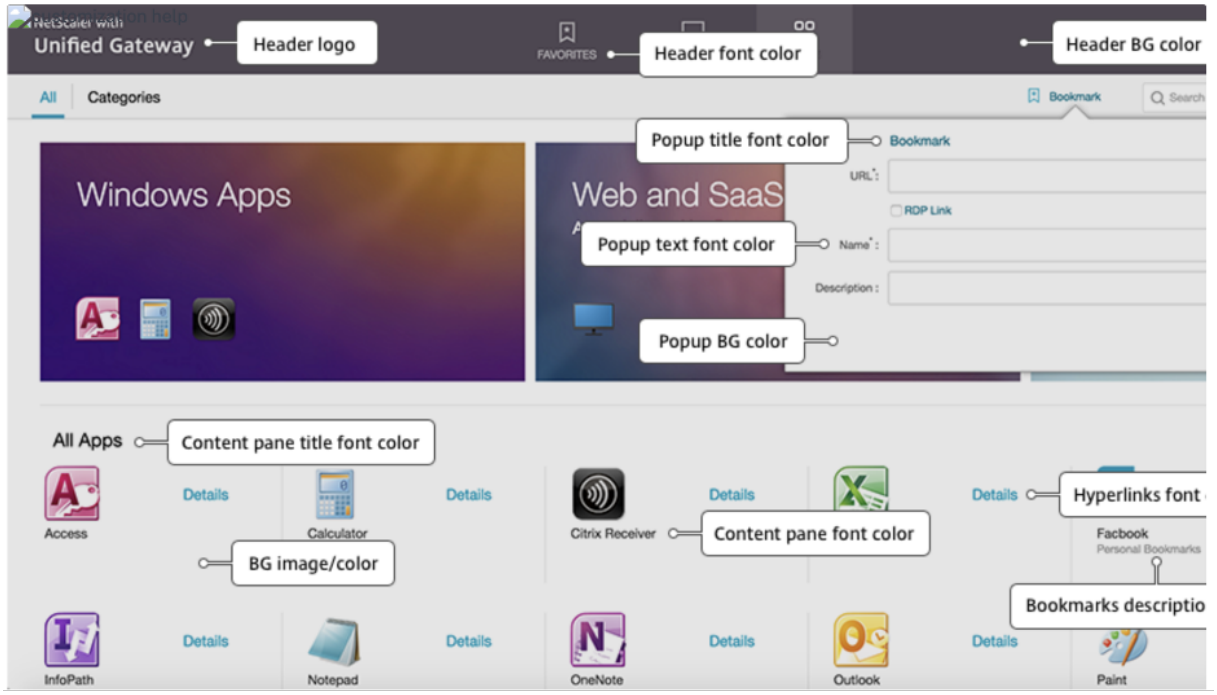
1. Navigieren Sie auf der Registerkarte Konfiguration zu **Citrix Gateway > Portal Themes** und klicken Sie auf **Hinzufügen**.
2. Geben Sie einen Namen für den Namen des benutzerdefinierten Themas ein.
3. Wählen Sie **unter Template Theme**das Basisthema gemäß Ihren Anforderungen aus. **RfWebUI** ist standardmäßig ausgewählt.
4. Klicken Sie auf **OK**.
5. Ändern **Sie im Abschnitt "Aussehen und** Verhalten"die Attribute gemäß Ihren Anforderungen für die Homepage und klicken Sie auf **OK**.




Die folgende Abbildung zeigt das auf RFWebUI basierende benutzerdefinierte Design.

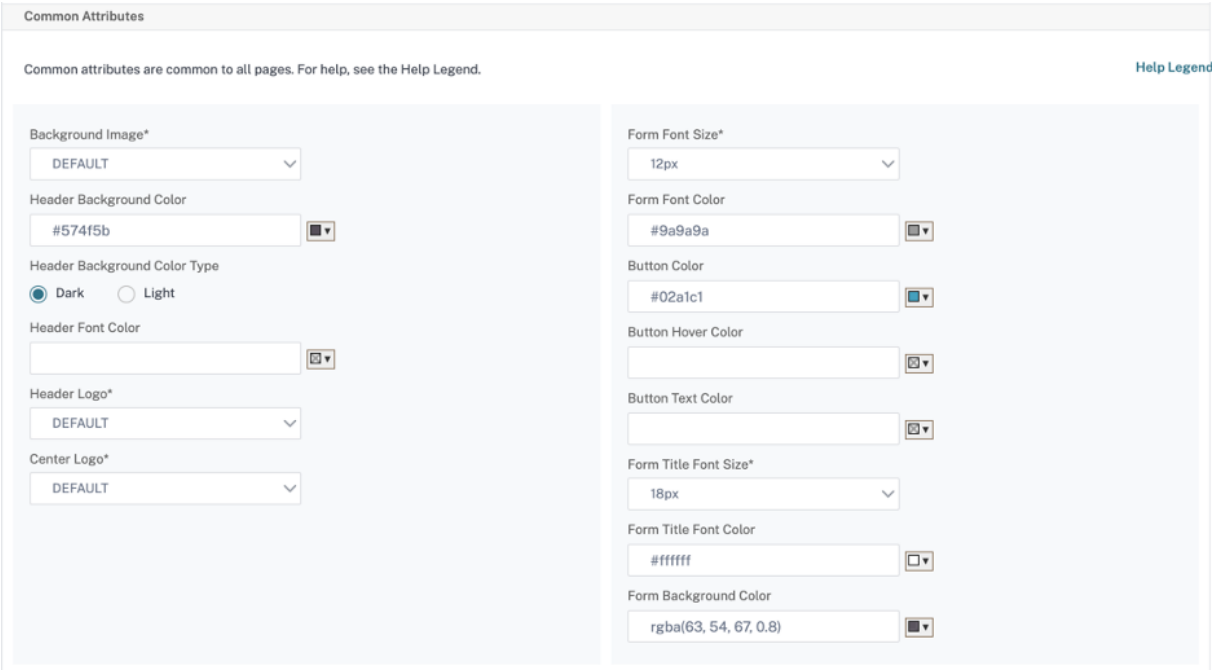
Der Link **Hilfelegende** zeigt die grafische Seitenanzeige mit den Abschnittsnamen an, damit Sie auswählen können, was Sie bearbeiten möchten.



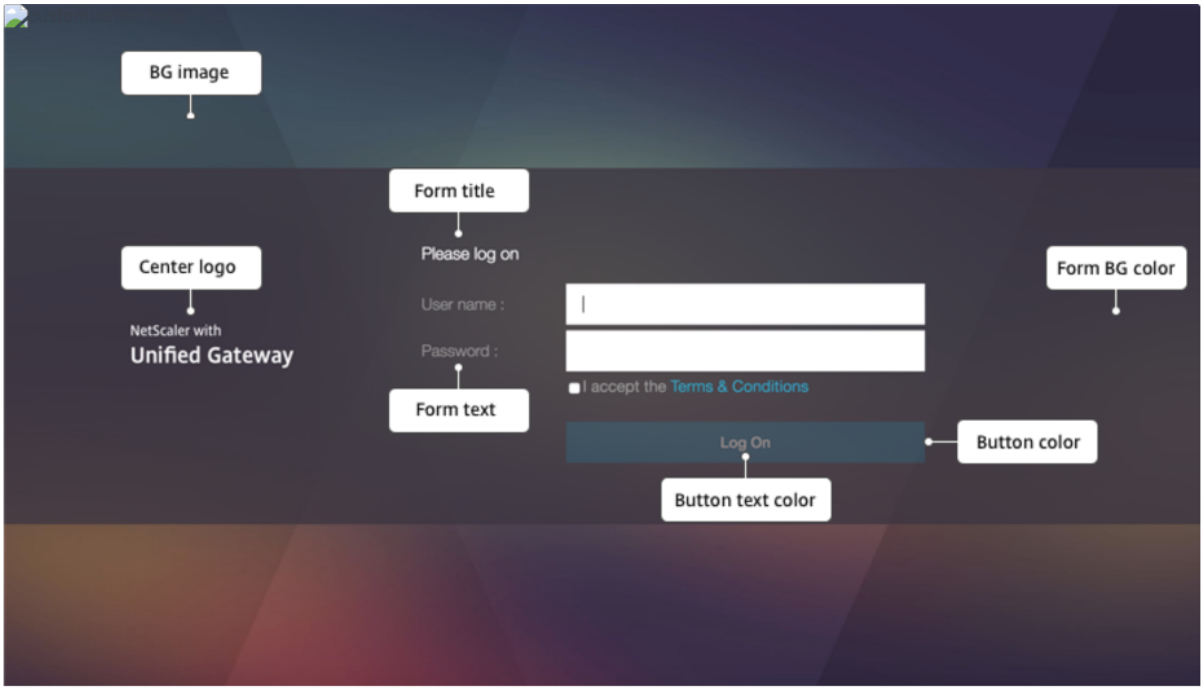

## Übliche Attribute

Der Abschnitt **Allgemeine Attribute** enthält die konfigurierbaren Einstellungen, die allen Citrix Gateway-Anmeldeseiten gemeinsam sind.



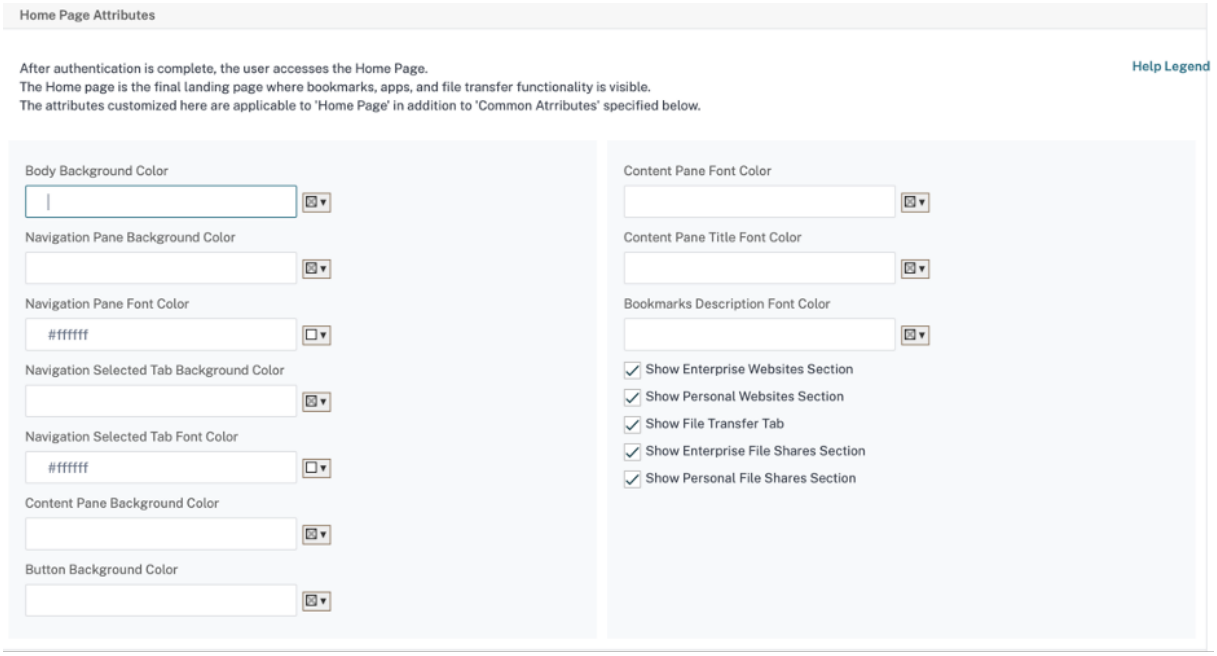

Klicken Sie auf den Link **Hilfelegende**, um alle gängigen konfigurierbaren Parameter anzuzeigen

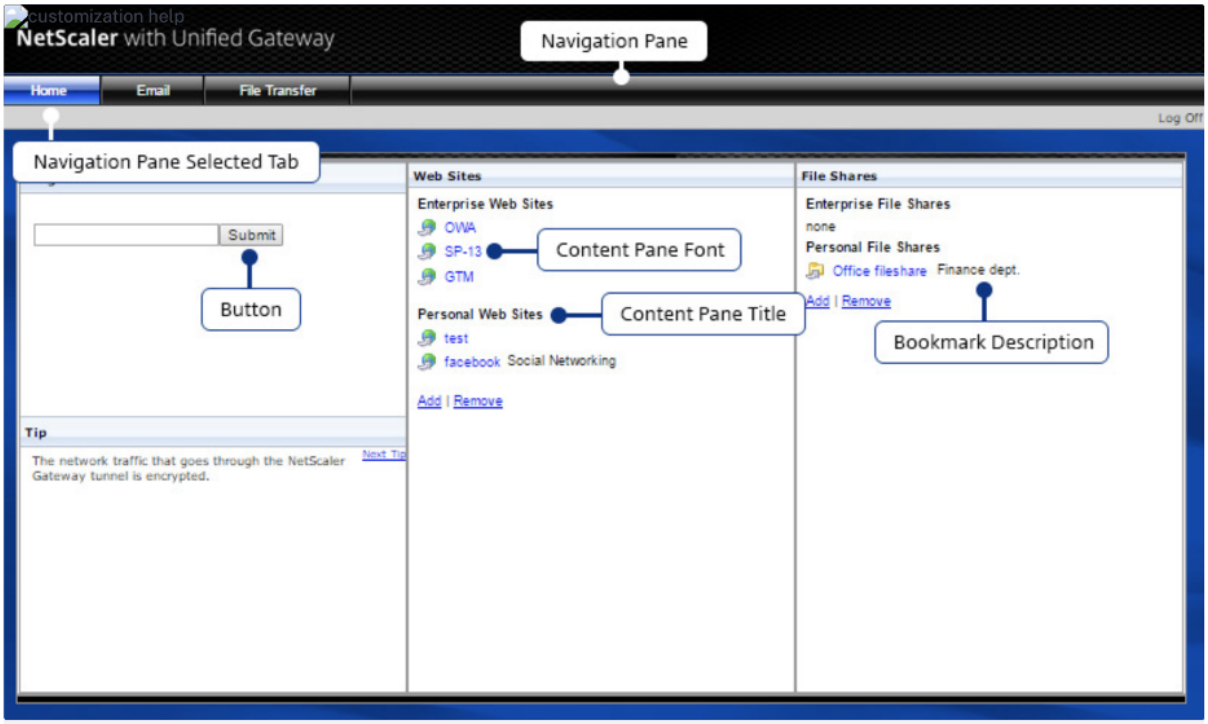


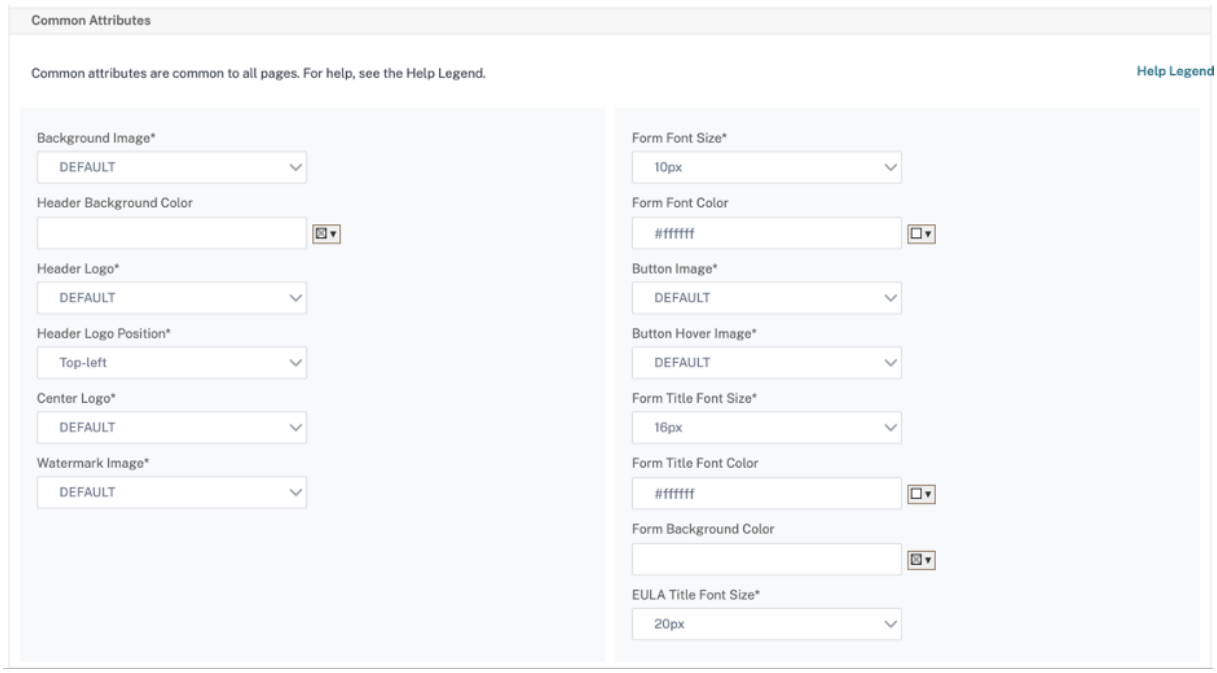

In ähnlicher Weise zeigt die folgende Abbildung für das benutzerdefinierte Design basierend auf **Default**die verfügbare Konfiguration für die Homepage.

**Hinweis:** Diese Konfiguration unterscheidet sich für x1 und GreenBubble.

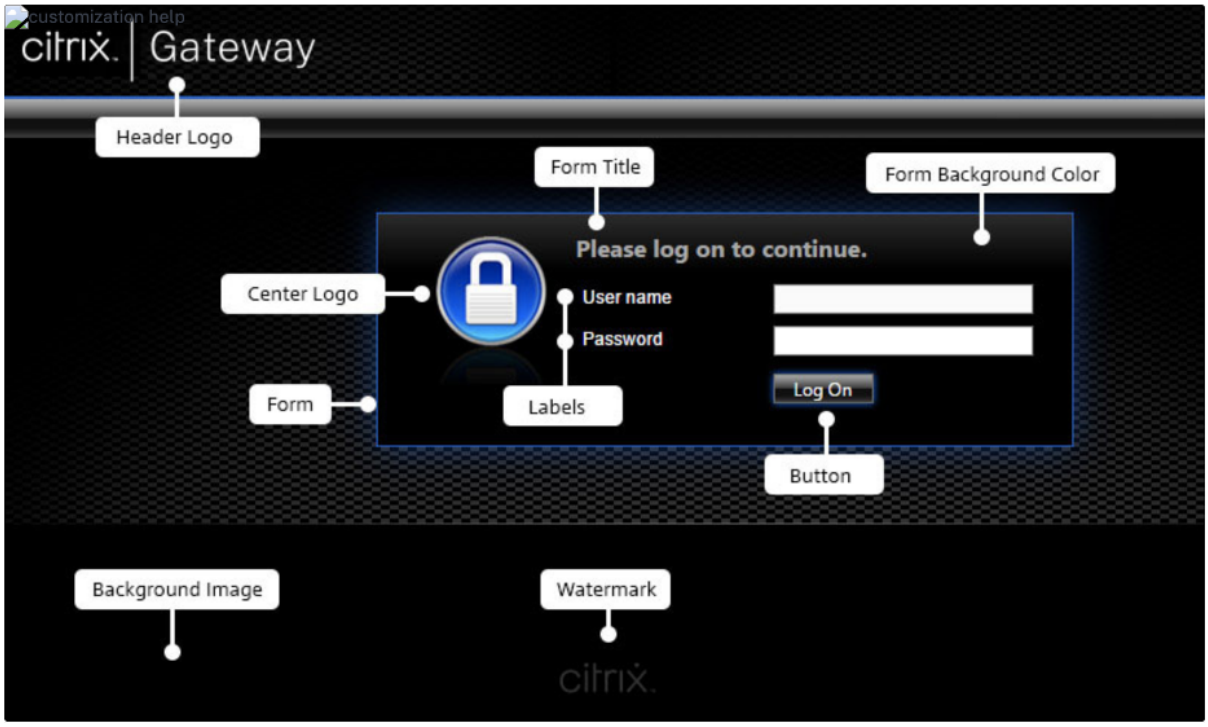




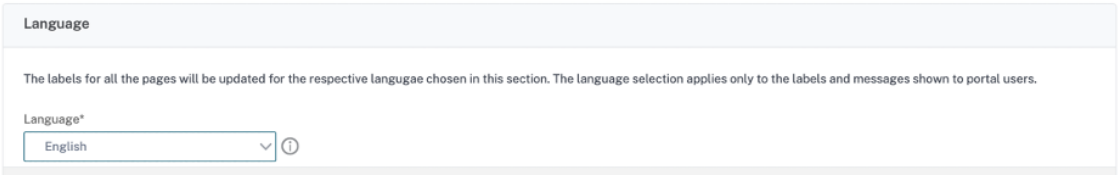



## String-Anpassungen

Neben dem Erscheinungsbild der Homepages des Gateway-Portals ermöglicht die Admin-Benutzeroberfläche auch die String-Anpassung auf allen Seiten.

**Führen Sie die folgenden Schritte aus, um die Zeichenfolgen anzupassen:**

1. Wählen Sie die Sprache aus, für die Sie die Zeichenfolge bearbeiten möchten. Die Zeichenfolgen werden in der ausgewählten Sprache angezeigt. Englisch ist standardmäßig ausgewählt.




   **Hinweis:** Die Sprache, die Sie auswählen, definiert nicht die Sprache des Portalthemas. Es ist die Sprache, für die die Zeichenfolgen angepasst werden.

2. Auf der rechten Seite werden in der **erweiterten Einstellung**die Seiten aufgeführt, die für die Zeichenfolgenanpassung verfügbar sind.

   - Anmeldeseite
   - EPA-Seite
   - EPA-Fehlerseite

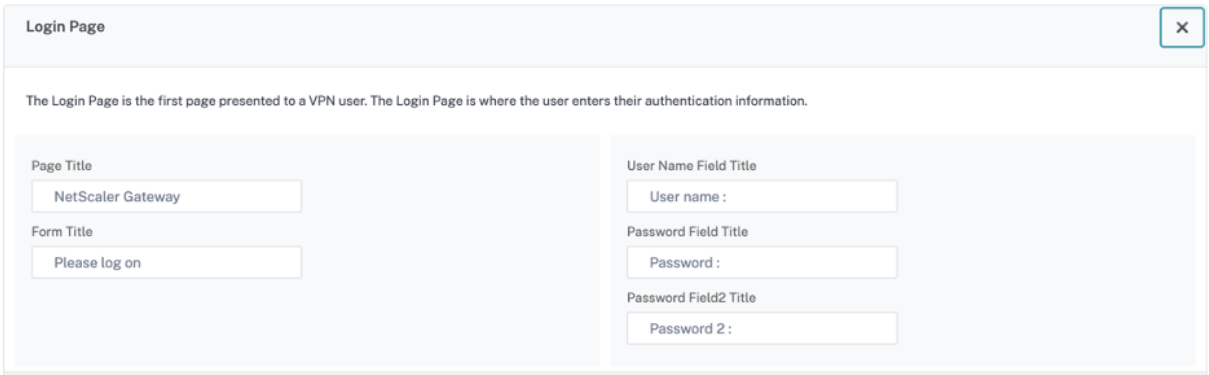
- Seite nach der EPA
- Seite VPN-Verbindung
- Startseite

3. Wählen Sie die Seite aus, für die Sie die Zeichenfolgen anpassen möchten, und klicken Sie auf das Symbol "Bearbeiten". Ein Formular mit vorausgefüllten Zeichenfolgenanpassungen wird angezeigt.
4. Wählen Sie das Feld aus und fügen Sie die Zeichenfolge gemäß Ihren Anforderungen hinzu oder bearbeiten Sie sie.
5. Klicken Sie auf **Fertig**, um die Erstellung des benutzerdefinierten Portalthemas abzuschließen Sie können die Themen später über **Citrix Gateway > Portal Themes**bearbeiten.

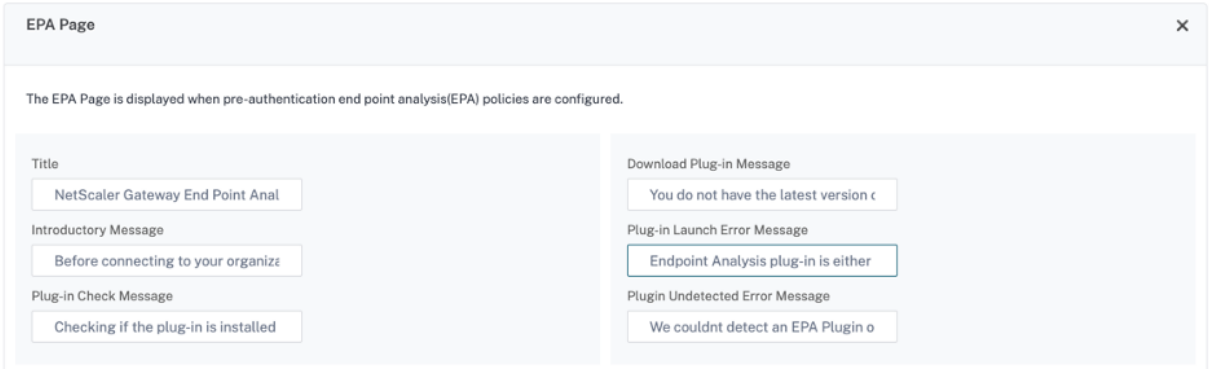
**Hinweis:** Wenn der Abschnitt die Zeichenfolgen immer noch in der zuvor ausgewählten Sprache anzeigt, war der Abschnitt möglicherweise bereits geöffnet, als die Sprache geändert wurde. Schließen Sie in diesem Fall den Abschnitt, wählen Sie die Sprache aus und öffnen Sie die Seite erneut über die **erweiterte Einstellung**.

Die folgenden Screenshots zeigen die verfügbaren anpassbaren Zeichenfolgen für jede Seite.

**Anmeldeseite:**

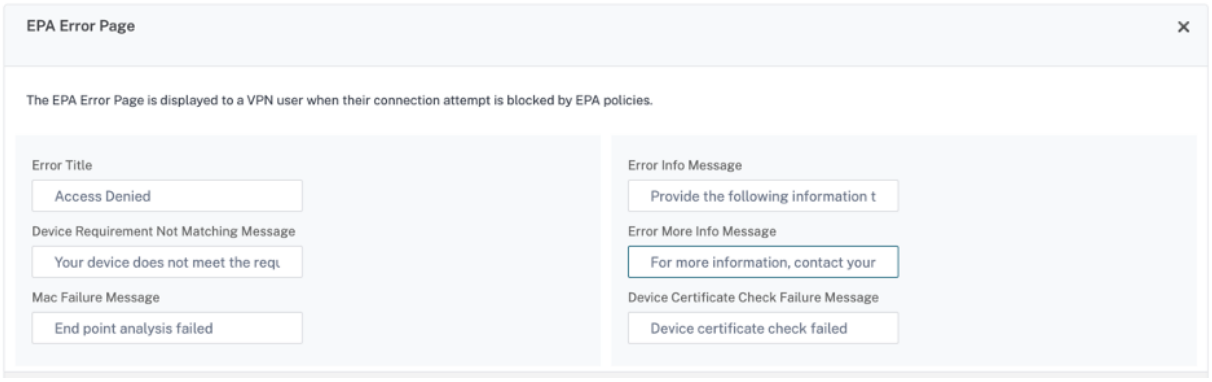



**EPA-Seite:**

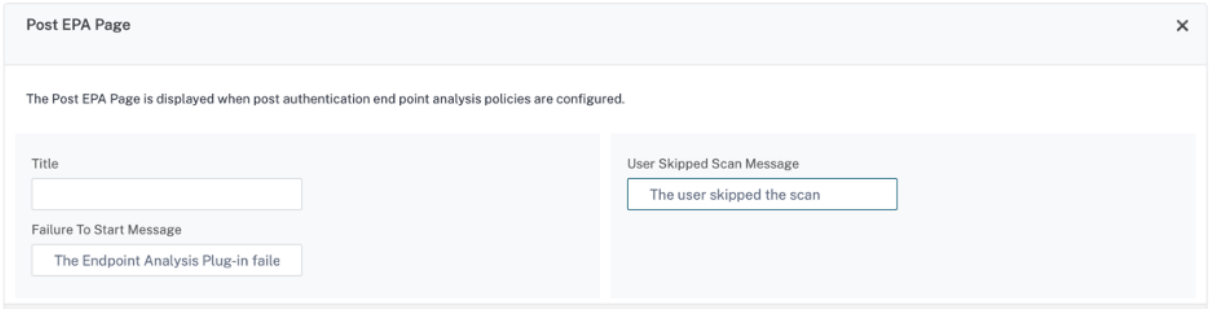



**EPA-Fehlerseite:**

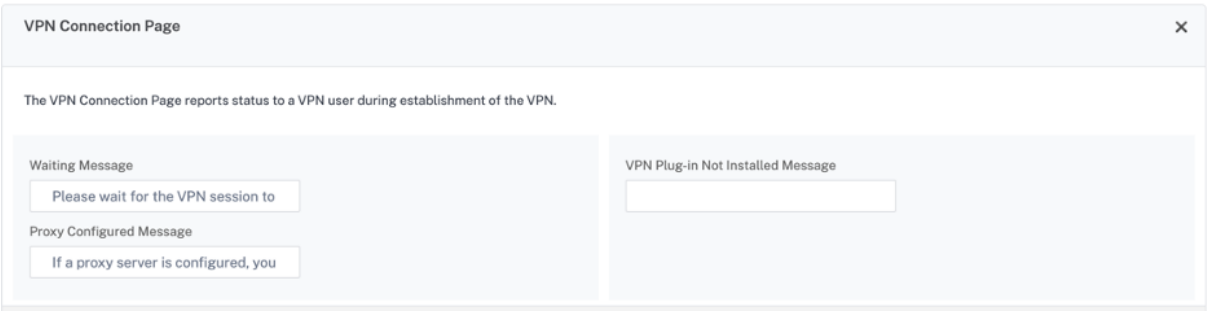
 




**Seite nach der EPA:**

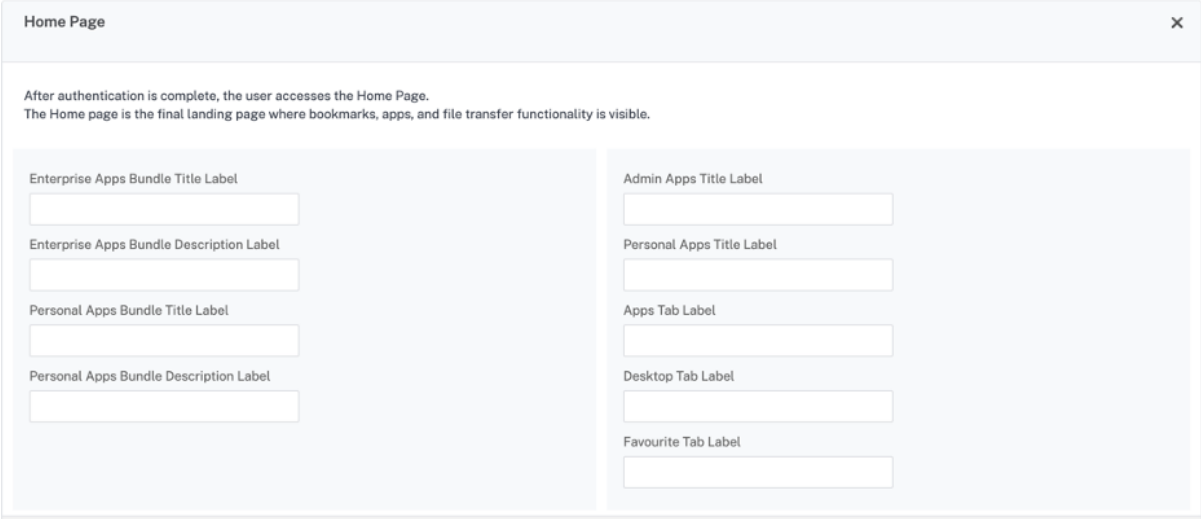



**Seite VPN-Verbindung:**




**Zuhause:**




## Citrix Gateway VPN-Split-Tunnel für Office365 optimieren

March 27, 2024

Da sich Unternehmen schneller als zuvor an die Remote-Arbeitsoptionen anpassen, muss die Fernzugriffsinfrastruktur optimiert werden, um eine nahtlose Konnektivität bei erhöhter Verkehrsbelastung zu ermöglichen.

> **Wichtig:**
>
> Microsoft empfiehlt, Datenverkehr, der für wichtige Office 365-Dienste bestimmt ist, vom Umfang der VPN-Verbindung auszuschließen, indem Split-Tunneling mithilfe veröffentlichter IPv4- und IPv6-Adressbereiche konfiguriert wird. Für eine optimale Leistung und die effizienteste Nutzung der VPN-Kapazität muss der Datenverkehr zu den dedizierten IP-Adressbereichen, die den folgenden Anwendungen zugeordnet sind, direkt außerhalb des VPN-Tunnels weitergeleitet werden:
>
> - Office 365 Exchange Online
> - SharePoint Online
> - Microsoft Teams (in der Microsoft-Dokumentation als Optimize-Kategorie bezeichnet)
>
> Weitere Informationen zu dieser Empfehlung finden Sie in den Microsoft-Anleitungen.

Die Empfehlung von Microsoft in Citrix Gateway wird erreicht, indem die von Microsoft bereitgestellte Liste der IP-Adressen mithilfe der Split-Tunnel-Reverse-Konfiguration direkt an das Internet für den O365-Verkehr weitergeleitet wird.

Die Konfiguration umfasst Folgendes, das manuell über die GUI oder die CLI durchgeführt werden kann:

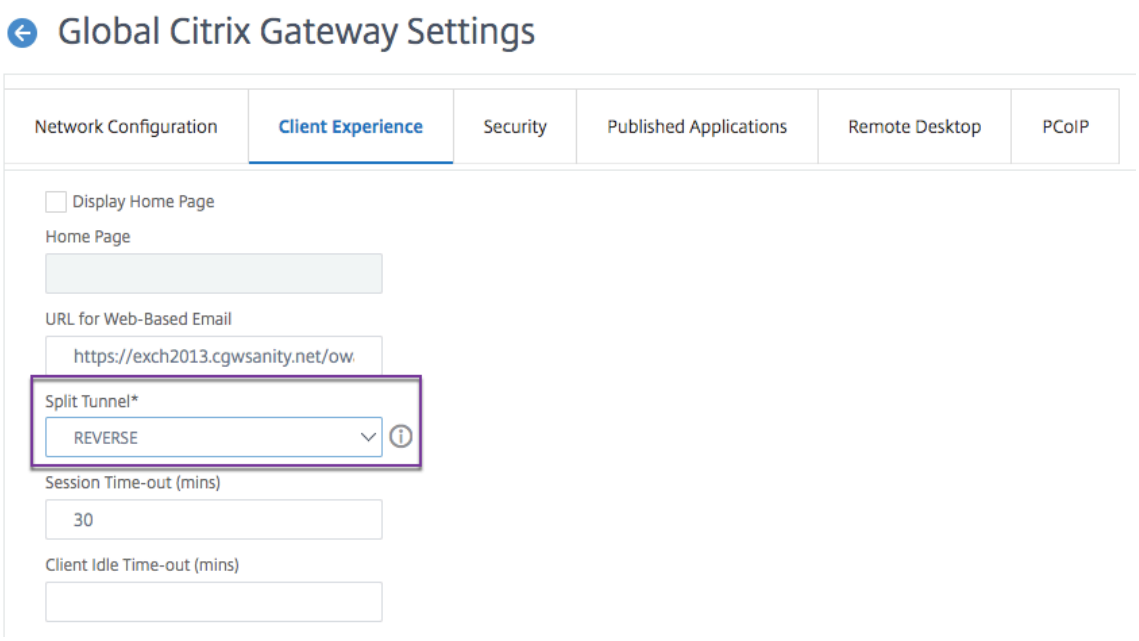
 

- Konfigurieren Sie den geteilten Tunnel für die umgekehrte Konfiguration. Einzelheiten finden Sie unter Split-Tunneling-Optionen.
- Konfigurieren Sie Intranetanwendungen für den Benutzerzugriff auf Ressourcen.

## Konfiguration über die GUI

### So konfigurieren Sie Split-Tunneling über die GUI

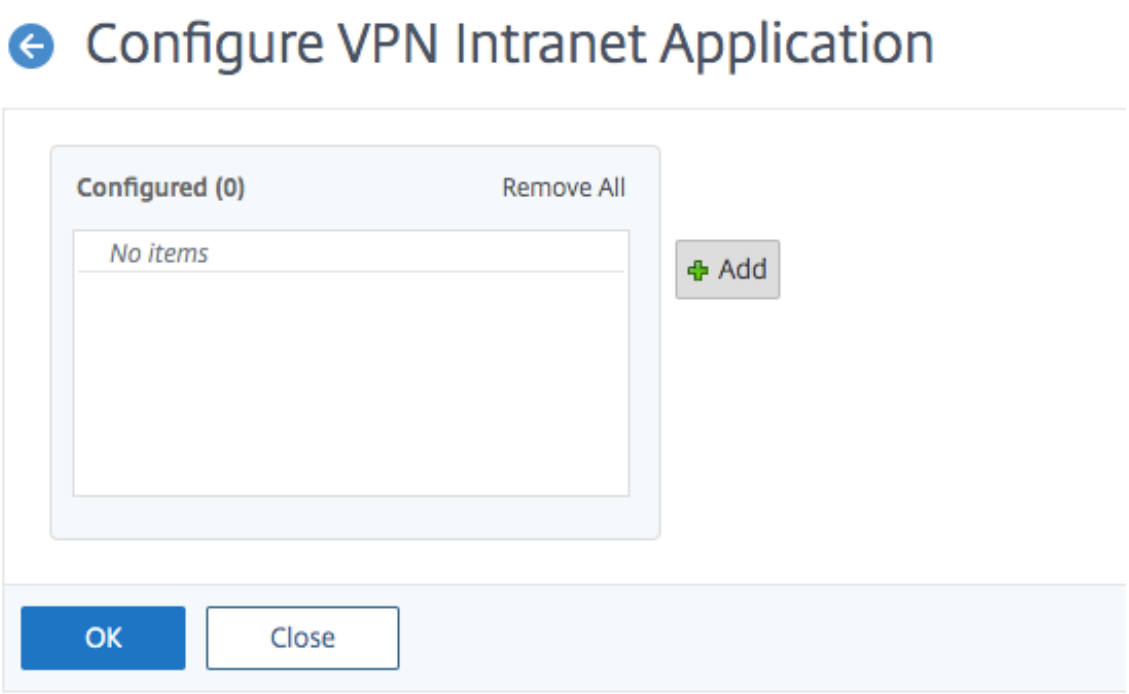
1. Navigieren Sie auf der Registerkarte Konfiguration zu **Citrix Gateway > Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Wählen Sie auf der Registerkarte **Client Experience** in **Split Tunnel**die Option **Umkehren**aus.
4. Klicken Sie auf **OK**.

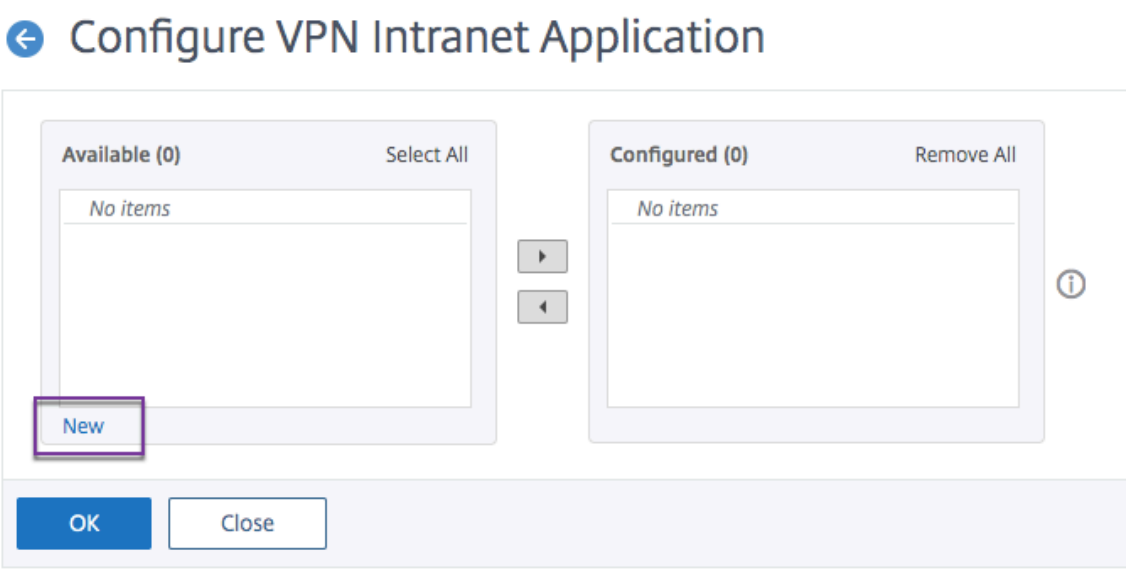



### So erstellen Sie eine VPN-Intranet-Anwendung über die GUI

1. Navigieren Sie auf der Registerkarte Konfiguration zu **Citrix Gateway > Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Intranet-Anwendungen**auf den Link.
3. Klicken Sie auf der Seite **VPN-Intranet-Anwendung konfigurieren** auf **Hinzufügen**und dann auf **Neu**.

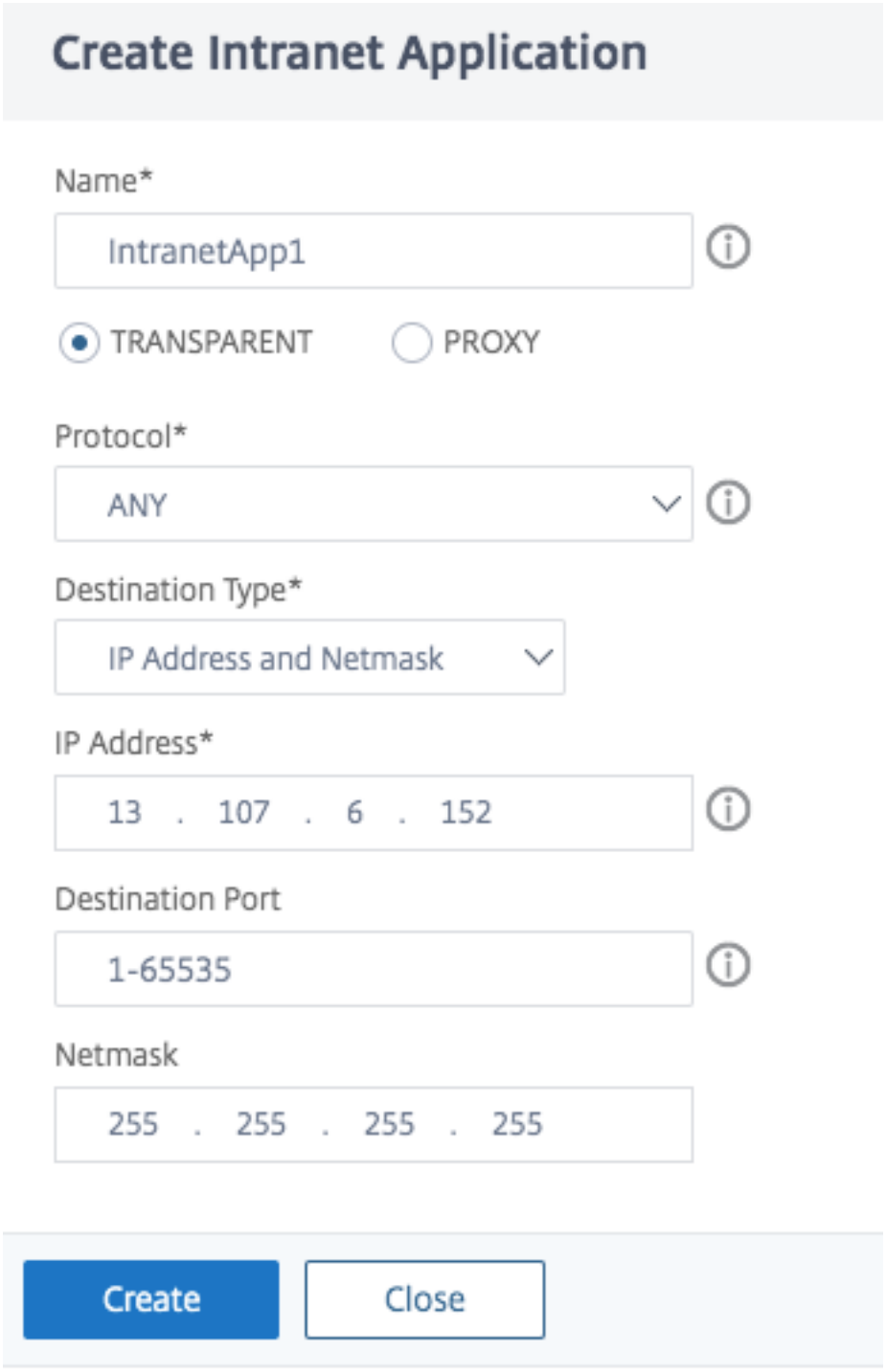
 




4. **Geben Sie im Feld Name einen Namen für das Profil ein.**
5. Wählen Sie unter **Protokoll** das Protokoll aus, das für die Netzwerkressource gilt.
6. Wählen Sie unter **Zieltyp**die Option **IP-Adresse und Netzwerkmaske**aus.
7. Geben Sie unter **IP-Adresse**die IP-Adresse ein, die für den O365-Verkehr direkt ins Internet geleitet werden muss. Eine Liste der IP-Adressen finden Sie unter Liste der IP-Adressen.
8. Geben Sie unter **Netzwerkmaske**die IP-Adresse der Netzmaske ein.




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

**Hinweis:** Wiederholen Sie diesen Vorgang für alle IP-Adressen.

### Konfiguration über die CLI

- Um den geteilten Tunnel auf Rückwärtsgang zu setzen, geben Sie an der Eingabeaufforderung;

```
set vpn parameter -splitTunnel REVERSE
<!--NeedCopy-->
```

- Um eine VPN-Intranet-Anwendung hinzuzufügen, geben Sie an der Eingabeaufforderung;

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
   255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
<!--NeedCopy-->
```

**Hinweis:** Wiederholen Sie diesen Vorgang für alle IP-Adressen.

- Um die Intranet-Anwendung zu binden, geben Sie an der Eingabeaufforderung ein;

```
bind vpn global -intranetApplication intranetapp1
<!--NeedCopy-->
```

### Liste der IP-Adressen der Office 365-Dienste (EXO, SPO und Microsoft Teams)

Referenz: https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

**Hinweis von Microsoft:**
*Als Teil der Reaktion von Microsoft auf die COVID-19-Situation hat Microsoft ein vorübergehendes Moratorium für einige geplante URL- und IP-Adressänderungen erklärt. Dieses Moratorium soll IT-Teams von Kunden Vertrauen und Einfachheit bei der Implementierung empfohlener Netzwerkoptimierungen für Office 365-Szenarien für das Homeoffice bieten. 24. März 2020 bis 30. Juni 2020 wird dieses Moratorium Änderungen für wichtige Office 365-Dienste (Exchange Online, SharePoint Online und Microsoft Teams) an IP-Bereichen und URLs in der Kategorie Optimize stoppen.*

#### IPv4-Adressbereich

104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32
132.245.0.0/16
150.171.32.0/22

150.171.40.0/22
191.234.140.0/22
204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.120.0.0/14

**IPv6-Adressbereich**

2603:1006::/40
2603:1016::/36
2603:1026::/36
2603:1036::/36
2603:1046::/36
2603:1056::/36
2603:1096::/38
2603:1096:400::/40
2603:1096:600::/40
2603:1096:a00::/39
2603:1096:c00::/40
2603:10a6:200::/40
2603:10a6:400::/40
2603:10a6:600::/40
2603:10a6:800::/40
2603:10d6:200::/40
2620:1ec:4::152/128
2620:1ec:4::153/128
2620:1ec:c::10/128
2620:1ec:c::11/128
2620:1ec:d::10/128
2620:1ec:d::11/128
2620:1ec:8f0::/46
2620:1ec:900::/46
2620:1ec:a92::152/128

2620:1ec:a92::153/128
2a01:111:f400::/48
2620:1ec:8f8::/46
2620:1ec:908::/46
2a01:111:f402::/48

## Art der Service-Unterstützung für UDP-Verkehr

March 27, 2024

Die Unterstützung von Type of Service (ToS) für UDP stellt sicher, dass Citrix Gateway den Wert beibehält, sobald ein ToS-Wert von einem Absender für ein UDP-Paket konfiguriert wurde, den Wert beibehält, bis das Paket sein Ziel erreicht. Auf der Grundlage des konfigurierten Werts und der Konfiguration des Zielnetzwerks stellt das Zielnetzwerk das UDP-Paket in eine priorisierte Ausgangsqueue.

> **Hinweis**
> Mithilfe von ToS-Informationen können Sie jedem IP-Paket eine Priorität zuweisen und eine bestimmte Behandlung wie hohen Durchsatz, hohe Zuverlässigkeit, niedrige Latenz usw. anfordern.

## Konfigurieren der Servernamenanzeigererweiterung

March 27, 2024

Ein Citrix Gateway-Gerät kann jetzt so konfiguriert werden, dass es eine Erweiterung für die Servernamenanzeige (SNI) in das SSL-Paket "Client Hello"enthält, das an den Backend-Server gesendet wird. Die SNI-Erweiterung hilft dem Backend-Server, den während des SSL-Handshakes angeforderten FQDN zu identifizieren und mit den entsprechenden Zertifikaten zu antworten.

> **Hinweis**
>
> Aktivieren Sie die SNI-Unterstützung, wenn mehrere SSL-Domains auf demselben Server gehostet werden.

**So konfigurieren Sie Citrix Gateway für die Unterstützung von SNI über die GUI:**

1. Navigieren Sie in der NetScaler GUI zu **Configuration> Citrix NetScaler> Globale Einstellungen.**

2. Klicken Sie auf den Link **Globale Einstellungen ändern** und wählen Sie im Menü **Backend-Server SNI** die Option **Aktiviert**aus.

**Um Citrix Gateway für die Unterstützung von SNI mithilfe der Befehlszeilenschnittstelle zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:**

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
<!--NeedCopy-->
```

## Serverzertifikat während eines SSL-Handshakes validieren

March 27, 2024

Das Citrix Gateway-Gerät kann jetzt so konfiguriert werden, dass das vom Back-End-Server bereitgestellte Serverzertifikat während eines SSL-Handshakes überprüft wird.

So konfigurieren Sie globale Parameter von Citrix Gateway zur Unterstützung von PAC für ausgehenden Proxy mithilfe des Konfigurationsdienstprogramms

Binden Sie das CA-Zertifikat

1. Navigieren Sie zu **Konfiguration** >**Citrix Gateway** > **Citrix Gateway Policy Manager** > **Zertifikatbindungen**.**
2. Klicken Sie auf dem Bildschirm **Certificate Bindings** auf das Symbol **+**.
3. Klicken Sie auf dem Bildschirm **Bindung von CA Certificate (s)** auf **Add Binding** und dann auf **Installieren**.
4. Wählen Sie im Feld Zertifikatsdateiname den **Namen der Zertifikatsdatei** aus und klicken Sie auf **Installieren**.
5. Wählen Sie auf dem Bildschirm **Bindung von CA Certificate (s)** das Zertifikat aus und klicken Sie auf **Bind**.
6. Klicken Sie auf **Fertig**.

**Aktivieren der Zertifikatvalidierung:**

1. Navigieren Sie zu **Citrix Gateway> Globale Einstellungen.**
2. Klicken Sie auf **Globale Einstellungen ändern**.**
3. Wählen Sie im Dropdownmenü **Backend-Serverzertifikatsprüfung** die Option **Aktiviert** aus und klicken Sie auf **OK**.

So konfigurieren Sie globale Parameter von Citrix Gateway für die Unterstützung von Serverzertifikaten mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
    bind vpn global cacert DNPGCA1

    set vpn parameter backendcertValidation ENABLED
<!--NeedCopy-->
```

## Vereinfachte SaaS-App-Konfiguration mit einer Vorlage

March 27, 2024

Die Konfiguration von SaaS-Apps mit Single Sign-On auf Citrix Gateway wird durch die Bereitstellung eines Dropdownmenüs für Vorlagen für beliebte SaaS-Apps vereinfacht. Die zu konfigurierende SaaS-App kann aus dem Menü ausgewählt werden. Die Vorlage enthält viele Informationen, die für die Konfiguration von Anwendungen erforderlich sind. Die für den Kunden spezifischen Informationen müssen jedoch noch zur Verfügung gestellt werden.

> **Hinweis:**
>
> Um SaaS-Apps zu konfigurieren und zu veröffentlichen, konfigurieren und veröffentlichen Sie sie auf dem Citrix Gateway und dann auf dem App-Server.
>
> Die Schritte im nächsten Abschnitt helfen Ihnen beim Konfigurieren und Veröffentlichen von Apps auf Citrix Gateway mithilfe einer Vorlage. Fahren Sie dann mit dem Abschnitt fort, in dem erklärt wird, wie Sie auf dem App-Server konfigurieren und veröffentlichen.

### Konfigurieren und Veröffentlichen von Apps mithilfe von Vorlagen - Citrix Gateway-spezifische Konfiguration

Die folgende Konfiguration verwendet die AWS Console-App als Beispiel für die Konfiguration und Veröffentlichung einer App mithilfe einer Vorlage.

Bevor Sie beginnen, benötigen Sie Folgendes:

- Ein Administratorkonto für die AWS-Konsole
- Ein Administratorkonto für Citrix Gateway

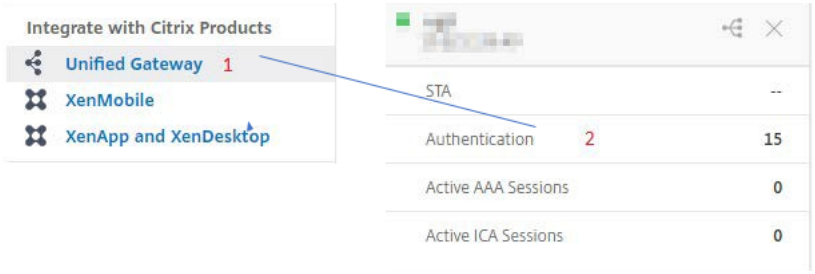
**Die Konfigurationsschritte der AWS-Konsole lauten wie folgt:**

1. Konfigurieren Sie die AWS-Konsole mit dem App-Katalog.
2. Exportieren Sie IdP-Metadaten der AWS-Konsole aus Citrix ADC.
3. Konfigurieren Sie IdP in AWS Console.

**SCHRITT 1:** Konfigurieren der AWS-Konsole mit App Catalog

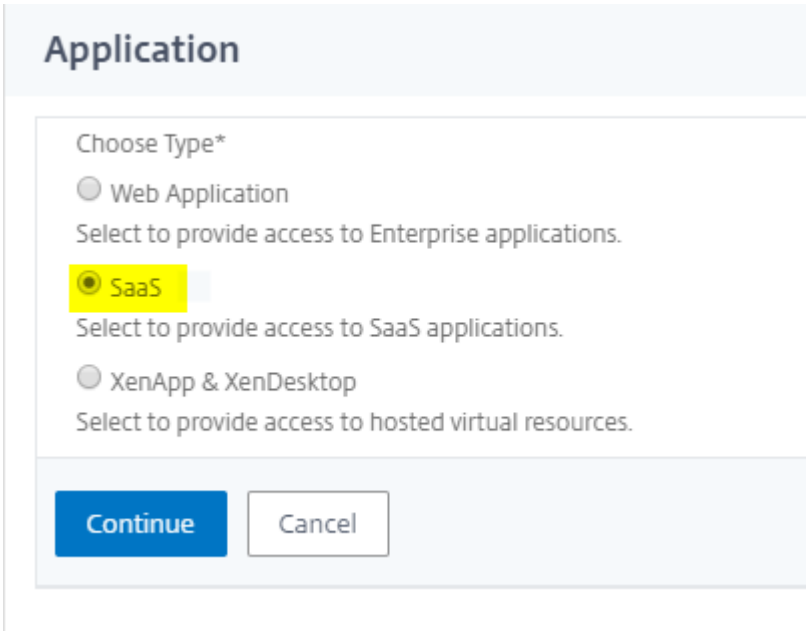
1. Klicken Sie auf **Unified Gateway > Authentifizierung**.




   Der Bildschirm Unified Gateway-Konfiguration wird angezeigt.

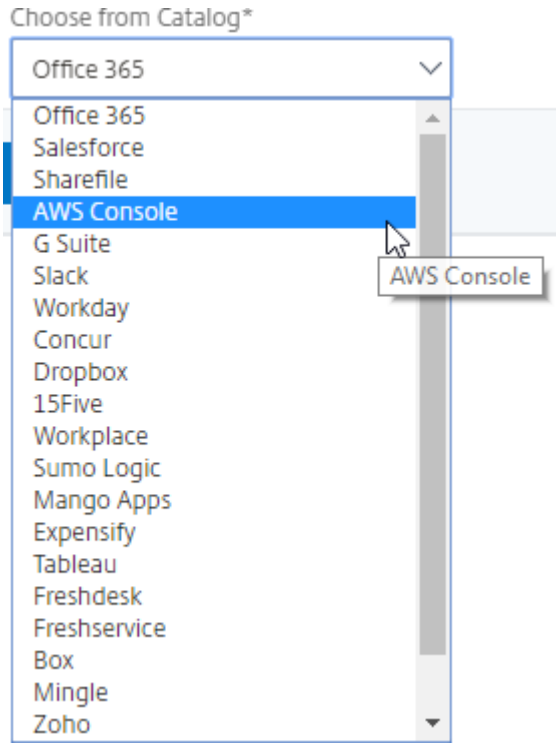
2. Klicken Sie im Abschnitt **Anwendungen** auf das Bearbeitungssymbol. Klicken Sie nun auf das Plus-Symbol. Das Anwendungsfenster wird angezeigt.


3. Wählen Sie **SaaS** aus dem Anwendungstyp aus.



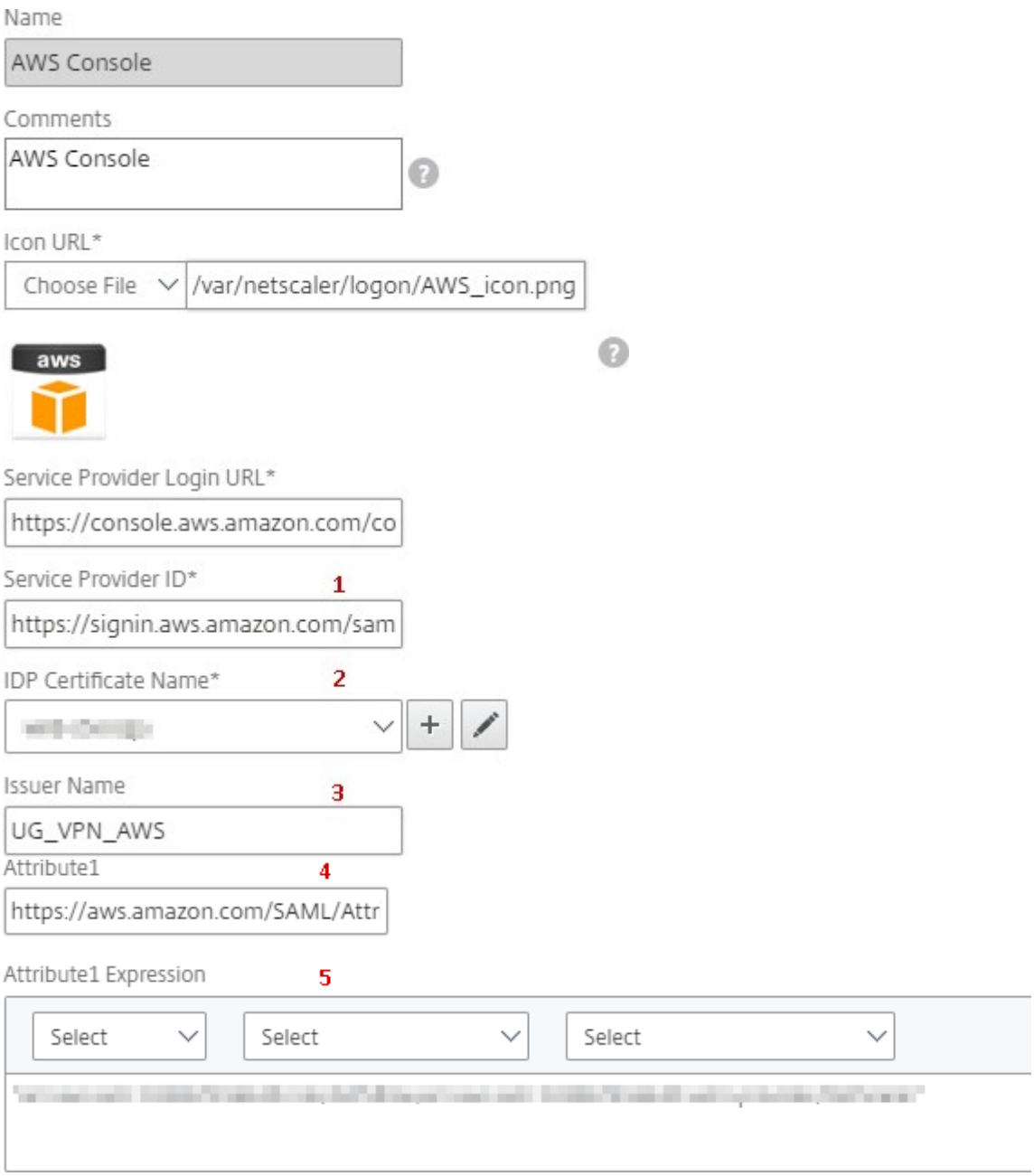

4. Wählen Sie in der Dropdown-Liste **AWS-Konsole** aus.




5. Füllen Sie die Anwendungsvorlage mit entsprechenden Werten.




6. Geben Sie die folgenden SAML-Konfigurationsdetails ein und klicken Sie auf **Weiter**.

   **ID des Dienstanbieters** —https://signin.aws.amazon.com/saml

   **Signaturzertifikatname** —IdP-Zertifikat muss ausgewählt sein

   **Name des Ausstellers** —Der Name des Ausstellers kann nach Ihrer Wahl ausgefüllt werden

   **Attribut 1** —`https://aws.amazon.com/SAML/Attributes/Role`

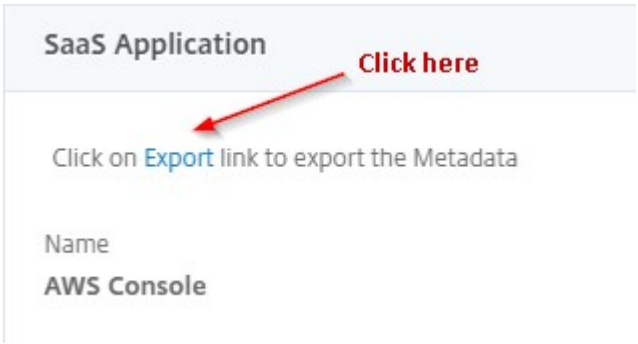
   **Attribute1 Ausdruck** – `Role ARN, IdP ARN`, wie in Schritt 3 gezeigt

7. Klicken Sie auf **Fertig**.

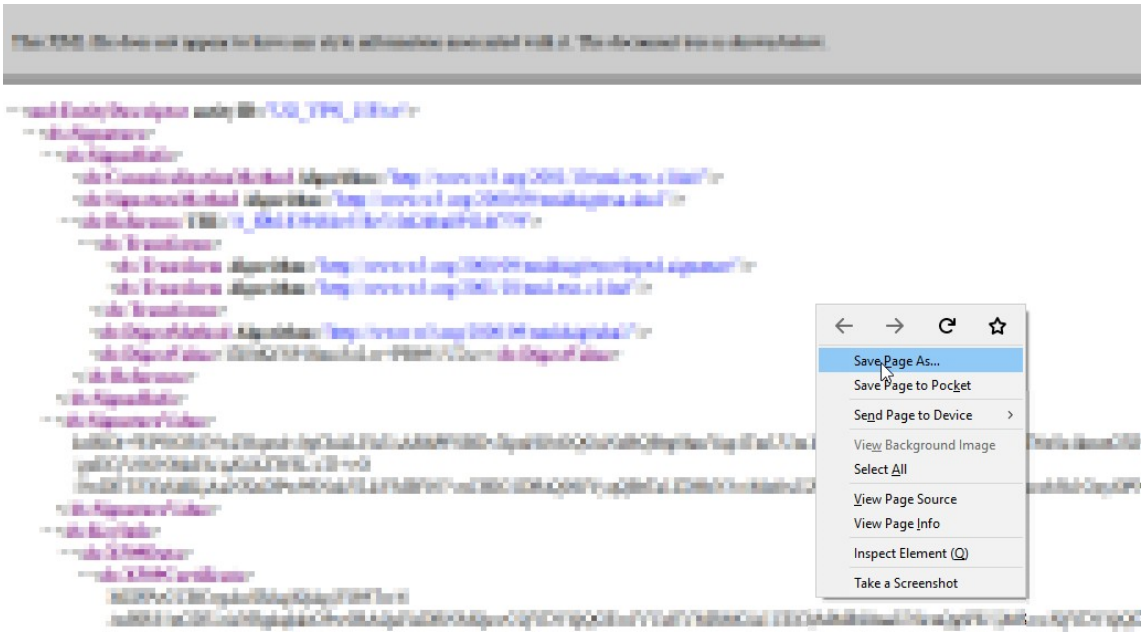
 

**SCHRITT 2:** Exportieren Sie IdP-Metadaten der AWS-Konsole von Citrix Gateway.

1. Klicken Sie auf **Unified Gateway > Authentifizierung**.
2. Scrollen Sie nach unten und klicken Sie auf **AWS Console Template**. Das SaaS-Anwendungsfenster wird angezeigt. Klicken Sie auf den Link **Exportieren**.




3. **Metadaten** werden in einem anderen Fenster geöffnet. Speichern Sie die **IdP-Metadatendatei**




**SCHRITT 3:** Konfigurieren Sie IdP in der AWS-Konsole.

## Konfigurieren und Veröffentlichen von Apps mithilfe von Vorlagen - App-Server-spezifische Konfiguration

Die folgenden Links öffnen PDF-Dokumente, die spezielle Anleitungen zum Konfigurieren und Veröffentlichen beliebter SaaS-Apps mithilfe von Vorlagen enthalten.

- 15Five

- Absorb
- Accompa
- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha
- AlertOps
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR
- Base CRM
- BitaBIZ
- BlueJeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence

- Contactzilla
- Convo
- Circonus
- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- DocuSign
- Domo
- Dropbox
- Duo
- eFront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk
- Front
- G-Suite
- GitHub

- GlassFrog
- GotoMeeting
- HappyFox
- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript

- Marketo
- Mingle
- Mixpanel
- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- PagerDuty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard

- Remedyforce
- Robin
- Rollbar
- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- StatusHub
- Statuspage
- Sumo Logic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria

- Testable
- TestFairy
- TextExpander
- TextMagic
- ThousandEyes
- Thycotic Secret server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- UniFi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- VIDIZMO
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- XMatters
- Yodeck

- Zendesk
- ZIVVER
- Zoho One
- ZIVVER
- Zoom

## Bereitstellen von Citrix Gateway mit dem Webinterface

March 27, 2024

Wenn Sie Citrix Gateway bereitstellen, um sicheren Remotezugriff auf Citrix Virtual Apps and Desktops bereitzustellen, ist Citrix Gateway mit dem Webinterface und der Secure Ticket Authority (STA) kompatibel, um Zugriff auf veröffentlichte Anwendungen und Desktops zu ermöglichen, die in einer Serverfarm gehostet werden.

Die Bereitstellung von Citrix Gateway in der DMZ ist die gebräuchlichste Konfiguration, wenn Citrix Gateway mit einer Serverfarm arbeitet. In dieser Konfiguration bietet Citrix Gateway einen sicheren einzigen Zugriffspunkt für die Webbrowser und die Citrix Workspace-App, die über das Webinterface auf die veröffentlichten Ressourcen zugreifen. In diesem Abschnitt werden die grundlegenden Aspekte dieser Bereitstellungsoption behandelt.

Die Konfiguration des Netzwerks Ihrer Organisation bestimmt, wo Sie Citrix Gateway bereitstellen, wenn es mit einer Serverfarm arbeitet. Die folgenden zwei Optionen sind verfügbar:

- Wenn Ihre Organisation das interne Netzwerk mit einer einzigen DMZ schützt, stellen Sie Citrix Gateway in der DMZ bereit.
- Wenn Ihre Organisation das interne Netzwerk mit zwei DMZs schützt, stellen Sie ein Citrix Gateway in jedem der beiden Netzwerksegmente in einer Double-Hop-DMZ-Konfiguration bereit. Weitere Informationen finden Sie unter Bereitstellen von Citrix Gateway in einer Double-Hop-DMZ.
  Hinweis: Sie können eine Double-Hop-DMZ auch mit der zweiten Citrix Gateway-Appliance im sicheren Netzwerk konfigurieren.

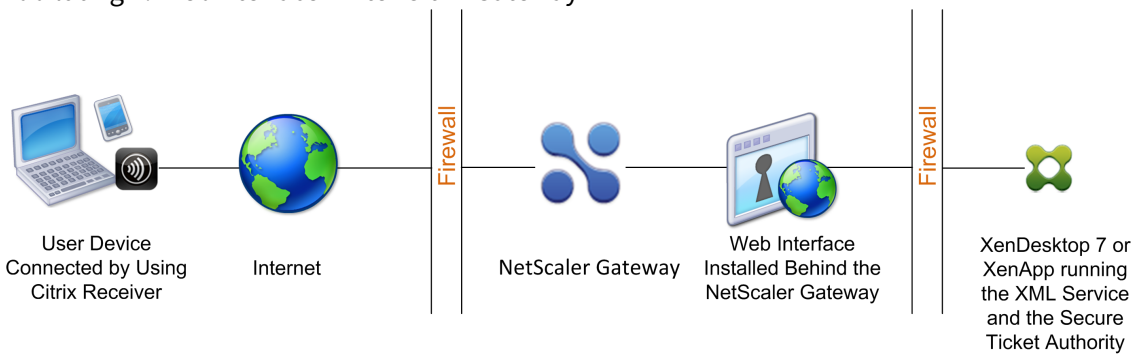
Wenn Sie Citrix Gateway in der DMZ bereitstellen, um Remotezugriff auf eine Serverfarm bereitzustellen, können Sie eine der folgenden drei Bereitstellungsoptionen implementieren:

- Stellen Sie das Webinterface hinter Citrix Gateway in der DMZ bereit. In dieser Konfiguration werden, wie in der folgenden Abbildung gezeigt, sowohl Citrix Gateway als auch das Webinterface in der DMZ bereitgestellt. Die erste Benutzerverbindung führt zu Citrix Gateway und wird

dann zum Webinterface umgeleitet.

Abbildung 1. Webinterface hinter Citrix Gateway im




- Stellen Sie Citrix Gateway parallel zum Webinterface in der DMZ bereit. In dieser Konfiguration werden sowohl Citrix Gateway als auch das Webinterface in der DMZ bereitgestellt, die anfängliche Benutzerverbindung wird jedoch anstelle von Citrix Gateway zum Webinterface hergestellt.
- Stellen Sie Citrix Gateway in der DMZ bereit und stellen Sie das Webinterface im internen Netzwerk bereit. In dieser Konfiguration authentifiziert Citrix Gateway Benutzeranforderungen, bevor die Anforderung an das Webinterface im sicheren Netzwerk weitergeleitet wird. Das Webinterface führt keine Authentifizierung durch, sondern interagiert mit der STA und generiert eine ICA-Datei, um sicherzustellen, dass der ICA-Verkehr über Citrix Gateway zur Serverfarm geleitet wird.

Der Ort, an dem Sie das Webinterface bereitstellen, hängt von verschiedenen Faktoren ab, darunter:

- Authentifizierung. Wenn sich Benutzer anmelden, können entweder Citrix Gateway oder das Webinterface Benutzeranmeldeinformationen authentifizieren. Wo Sie das Webinterface in Ihrem Netzwerk platzieren, ist ein Faktor, der teilweise bestimmt, wo sich Benutzer authentifizieren.
- Benutzer-Software. Benutzer können entweder mit dem Citrix Gateway Plug-in oder mit der Citrix Workspace-App eine Verbindung zum Webinterface herstellen. Sie können die Ressourcen einschränken, auf die Benutzer nur mithilfe der Citrix Workspace-App zugreifen können, oder Benutzern mit dem Citrix Gateway-Plug-In besseren Netzwerkzugriff gewähren. Wie Benutzer eine Verbindung herstellen und mit welchen Ressourcen Sie Benutzern eine Verbindung herstellen können, können Sie ermitteln, wo Sie das Webinterface in Ihrem Netzwerk bereitstellen.

### Stellen Sie das Webinterface in einem sicheren Netzwerk bereit

Bei dieser Bereitstellung ist das Webinterface im sicheren, internen Netzwerk. Citrix Gateway ist in der DMZ. Citrix Gateway authentifiziert Benutzeranfragen, bevor die Anfragen an das Webinterface gesendet werden.

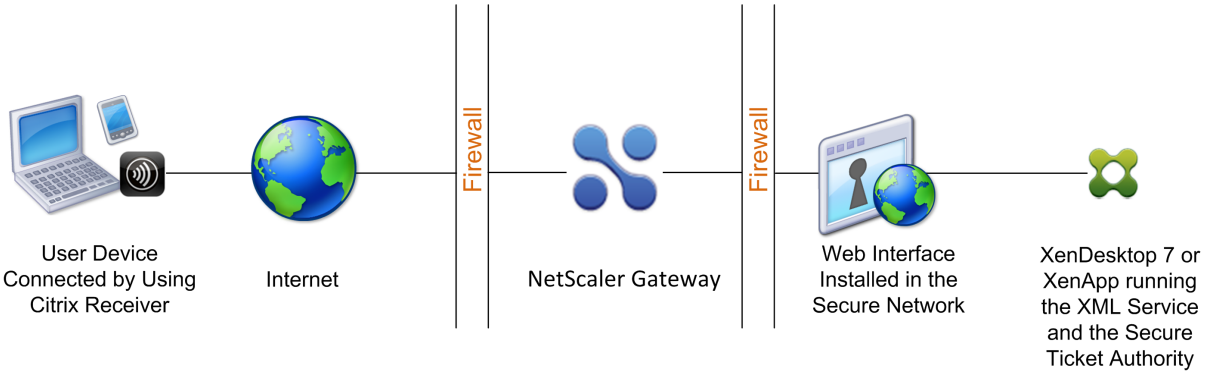
Wenn Sie das Webinterface im sicheren Netzwerk bereitstellen, müssen Sie die Authentifizierung auf Citrix Gateway konfigurieren.

Wenn Sie das Webinterface mit Citrix Virtual Apps and Desktops bereitstellen, ist die Bereitstellung des Webinterface im sicheren Netzwerk das Standardbereitstellungsszenario. Wenn der Desktop Delivery Controller installiert ist, wird auch eine benutzerdefinierte Version des Webinterface installiert.

> **Wichtig**:
> Wenn sich das Webinterface im sicheren Netzwerk befindet, müssen Sie die Authentifizierung auf Citrix Gateway aktivieren. Benutzer stellen eine Verbindung zu Citrix Gateway her, geben ihre Anmeldeinformationen ein und stellen dann eine Verbindung zum Webinterface her. Wenn Sie die Authentifizierung deaktivieren, werden nicht authentifizierte HTTP-Anfragen direkt an den Server gesendet, auf dem das Webinterface ausgeführt wird. Das Deaktivieren der Authentifizierung auf Citrix Gateway wird nur empfohlen, wenn sich das Webinterface in der DMZ befindet und Benutzer eine direkte Verbindung zum Webinterface herstellen.

Abbildung 1. Webinterface ist im sicheren Netzwerk



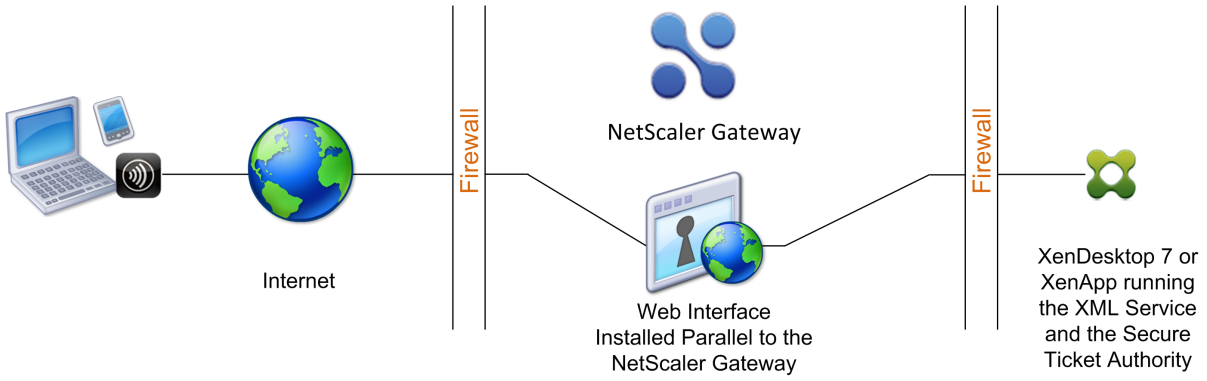

### Stellen Sie das Webinterface parallel zu Citrix Gateway in einer DMZ bereit

Bei dieser Bereitstellung sind das Webinterface und Citrix Gateway beide in der DMZ. Benutzer stellen mithilfe eines Webbrowsers oder einer Citrix Workspace-App eine direkte Verbindung zum Webinterface her. Benutzerverbindungen werden zuerst zur Authentifizierung an das Webinterface gesendet. Nach der Authentifizierung werden die Verbindungen über Citrix Gateway geroutet. Nachdem sich Benutzer erfolgreich am Webinterface angemeldet haben, können sie auf veröffentlichte Anwendungen oder Desktops in der Serverfarm zugreifen. Wenn Benutzer eine Anwendung oder einen Desktop starten, sendet das Webinterface eine ICA-Datei mit Anweisungen zum Weiterleiten des ICA-Datenverkehrs über Citrix Gateway, als wäre es ein Server, auf dem Secure Gateway ausgeführt wird. Die vom Webinterface gelieferte ICA-Datei enthält ein von der Secure Ticket Authority (STA) erstelltes Sitzungsticket.

Wenn die Citrix Workspace-App eine Verbindung zu Citrix Gateway herstellt, wird das Ticket angezeigt. Citrix Gateway kontaktiert die STA, um das Sitzungsticket zu validieren. Wenn das Ticket weiterhin gültig ist, wird der ICA-Verkehr des Benutzers an den Server in der Serverfarm weitergeleitet. Die folgende Abbildung zeigt diese Bereitstellung.

Abbildung 1. Das Webinterface wurde parallel zu Citrix Gateway installiert

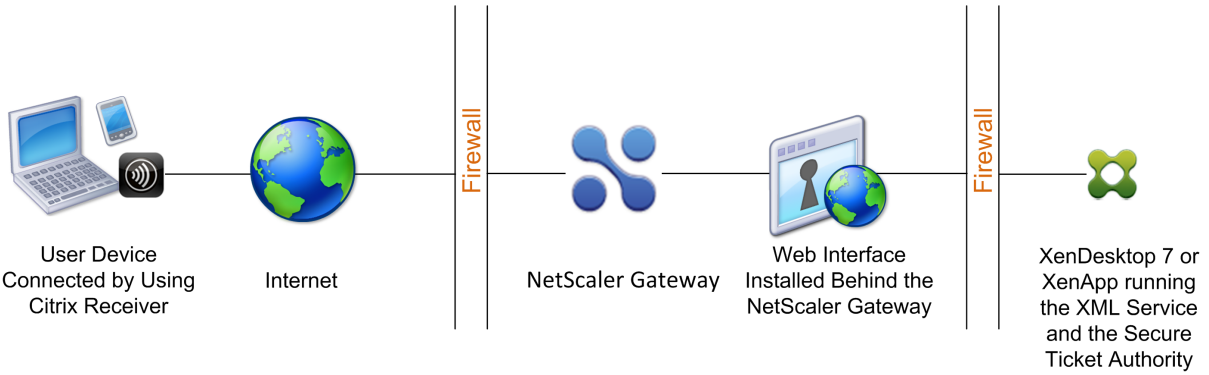



Wenn das Webinterface parallel zu Citrix Gateway in der DMZ ausgeführt wird, müssen Sie die Authentifizierung auf Citrix Gateway nicht konfigurieren. Das Webinterface authentifiziert Benutzer.

### Stellen Sie das Webinterface hinter Citrix Gateway in einer DMZ bereit

In dieser Konfiguration werden sowohl Citrix Gateway als auch das Webinterface in der DMZ bereitgestellt. Wenn sich Benutzer mit der Citrix Workspace-App anmelden, wird die erste Benutzerverbindung zu Citrix Gateway hergestellt und dann zum Webinterface umgeleitet. Um den gesamten HTTPS- und ICA-Datenverkehr über einen einzelnen externen Port weiterzuleiten und die Verwendung eines einzelnen SSL-Zertifikats zu erfordern, fungiert Citrix Gateway als Reverse-Webproxy für das Webinterface.

Abbildung 1. Webinterface ist hinter Citrix Gateway




Wenn das Webinterface hinter Citrix Gateway in der DMZ bereitgestellt wird, können Sie die Authentifizierung auf dem Gerät konfigurieren, dies ist jedoch nicht erforderlich. Sie können entweder Citrix Gateway oder das Webinterface Benutzer authentifizieren lassen, da sich beide in der DMZ befinden.

## Webinterface-Funktionen

March 27, 2024

Bevor Sie das Webinterface für Citrix Gateway konfigurieren, müssen Sie die Unterschiede zwischen Citrix Virtual Apps-Websites und Citrix Virtual Apps Services-Sites verstehen.

- **Citrix Virtual Apps-Websites.** Das Webinterface bietet Funktionen zum Erstellen und Verwalten von Citrix Virtual Apps-Websites. Benutzer greifen über einen Webbrowser und ein Plug-in remote auf veröffentlichte Ressourcen und gestreamte Anwendungen zu.
- **Websites für Citrix Virtual Apps Services.** Citrix Virtual Apps ist ein Plug-in, das auf Flexibilität und einfache Konfiguration ausgelegt ist. Durch die Verwendung von Citrix Virtual Apps mit Citrix Virtual Apps Services-Sites auf dem Webinterface können Sie veröffentlichte Ressourcen in die Desktops der Benutzer integrieren. Benutzer greifen auf Remote- und Streaming-Anwendungen sowie Remote-Desktops und -Inhalte zu, indem sie auf ihrem Desktop oder im Startmenü auf Symbole klicken oder in den Infobereich ihres Computerdesktops klicken. Sie können die Konfigurationsoptionen festlegen, auf die Ihre Benutzer zugreifen und diese ändern können, wie Audio-, Anzeige- und Anmeldeeinstellungen.

  > **Hinweis:**
  > Wenn Sie diese Option wählen, wird der Zugriff auf virtuelle Desktops nicht unterstützt.

Weitere Informationen finden Sie in der Citrix Produktdokumentation.

## Einrichten einer Webinterface-Site

March 27, 2024

Wenn Sie das Webinterface im sicheren Netzwerk bereitstellen und die Authentifizierung auf Citrix Gateway konfigurieren, authentifiziert das Gerät Benutzer, wenn Benutzer eine Verbindung zu Citrix Gateway herstellen.

> **Wichtig:**
>
> Installieren und konfigurieren Sie das Webinterface, bevor Sie Citrix Gateway konfigurieren. Weitere Informationen finden Sie in der Webinterface-Dokumentation in der Citrix Produktdokumentation.

Die Schritte zum Erstellen einer Webinterface-Site umfassen:

- Wählen Sie aus, wie sich Benutzer anmelden. Sie können sich über einen Webbrowser, das Citrix Gateway Plug-in oder die Citrix Workspace-App anmelden. Weitere Informationen finden Sie unter Webinterface-Funktionen.
- Identifizieren Sie, von wo aus sich Benutzer authentifizieren. Citrix Gateway oder das Webinterface.

> **Hinweis:**
>
> Wenn sich das Webinterface im sicheren Netzwerk befindet, aktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem Citrix Gateway. Wenn Sie die Authentifizierung deaktivieren, werden nicht authentifizierte HTTP-Anfragen direkt an den Server gesendet, auf dem das Webinterface ausgeführt wird. Das Deaktivieren der Authentifizierung auf dem Citrix Gateway wird nur empfohlen, wenn sich das Webinterface in der DMZ befindet und Benutzer eine direkte Verbindung zum Webinterface herstellen.

Stellen Sie sicher, dass Sie ein gültiges Serverzertifikat auf dem Citrix Gateway installieren. Weitere Informationen zum Arbeiten mit Zertifikaten finden Sie unter Installieren und Verwalten von Zertifikaten.

> **Wichtig:**
>
> Damit das Webinterface ordnungsgemäß mit Citrix Gateway 10.1 funktioniert, muss der Server, auf dem das Webinterface ausgeführt wird, dem Citrix Gateway-Zertifikat vertrauen und den vollqualifizierten Domänennamen (FQDN) des virtuellen Servers in die richtige IP-Adresse auflösen können.

## Erstellen einer Webinterface 5.4-Site

March 27, 2024

Die Citrix Webinterface Management-Konsole ist ein Microsoft Management Console (MMC) 3.0-Snap-In, mit dem Sie Citrix Virtual Apps Web- und Citrix Virtual Apps Services-Sites erstellen und konfigurieren können, die auf Microsoft Internet Information Services (IIS) gehostet werden. Webinterface-Sitetypen werden im linken Bereich angezeigt. Im zentralen Ergebnisbereich werden die Sites angezeigt, die innerhalb des im linken Bereich ausgewählten Site-Typ-Containers verfügbar sind.

Mit der Citrix Webinterface Management-Konsole können Sie alltägliche Verwaltungsaufgaben schnell und einfach ausführen. Im Aktionsbereich werden die derzeit verfügbaren Aufgaben aufgeführt. Aufgaben, die sich auf Elemente beziehen, die im linken Bereich ausgewählt wurden, werden oben und Aktionen angezeigt, die für im Ergebnisbereich ausgewählte Elemente verfügbar sind.

Wenn Sie die Konsole verwenden, wird Ihre Konfiguration wirksam, wenn Sie Ihre Änderungen über die Konsole festlegen. Infolgedessen können einige Webinterface-Einstellungen deaktiviert werden, wenn ihre Werte für die aktuelle Konfiguration nicht relevant sind und die entsprechenden Einstellungen in WebInterface.conf auf ihre Standardwerte zurückgesetzt werden. Citrix empfiehlt, dass Sie regelmäßige Backups der Dateien WebInterface.conf und config.xml für Ihre Sites erstellen.

Die Citrix Webinterface Management-Konsole wird automatisch installiert, wenn Sie das Webinterface für Microsoft Internet Information Services installieren. Führen Sie die Konsole aus, indem Sie auf Start > Alle Programme > Citrix > Management Consoles > Citrix Web Interface Management klicken.

> **Hinweis**: Stellen Sie sicher, dass MMC 3.0 auf dem Server vorhanden ist, auf dem Sie das Webinterface installieren, da dies eine Voraussetzung für die Installation der Citrix Webinterface Management-Konsole ist. MMC 3.0 ist standardmäßig auf allen Windows-Plattformen verfügbar, die für das Hosting des Webinterface unterstützt werden.

### Verwenden von Konfigurationsdateien

Sie können die folgenden Konfigurationsdateien bearbeiten, um Webinterface-Sites zu konfigurieren:

- Webinterface-Konfigurationsdatei: Die Webinterface-Konfigurationsdatei WebInterface.conf ermöglicht es Ihnen, viele Webinterface-Eigenschaften zu ändern. Es ist sowohl auf Microsoft Internet Information Services (IIS) als auch auf Java-Anwendungsservern verfügbar. Mit dieser Datei können Sie tägliche Verwaltungsaufgaben ausführen und viele weitere Einstellungen anpassen. Bearbeiten Sie die Werte in WebInterface.conf und speichern Sie die aktualisierte Datei, um die Änderungen zu übernehmen. Weitere Informationen zur Konfiguration des Webinterface mithilfe von WebInterface.conf finden Sie in der Webinterface-Dokumentation im Knoten Technologies in der Citrix Produktdokumentation.
- Citrix Online-Plug-in-Konfigurationsdatei. Sie können das Citrix Online Plug-in mithilfe der Datei config.xml auf dem Webinterface-Server konfigurieren.

## Konfigurieren von Sites über die Citrix Webinterface Management Console

March 27, 2024

Die Citrix Webinterface Management-Konsole ist ein Microsoft Management Console (MMC) 3.0-Snap-In, mit dem Sie Citrix Virtual Apps Web- und Citrix Virtual Apps Services-Sites erstellen und konfigurieren können, die auf Microsoft Internet Information Services (IIS) gehostet werden.

Webinterface-Sitetypen werden im linken Bereich angezeigt. Im zentralen Ergebnisbereich werden die Sites angezeigt, die innerhalb des im linken Bereich ausgewählten Site-Typ-Containers verfügbar sind.

Mit der Citrix Webinterface Management-Konsole können Sie alltägliche Verwaltungsaufgaben schnell und einfach ausführen. Im Aktionsbereich werden die derzeit verfügbaren Aufgaben aufgeführt. Aufgaben, die sich auf im linken Bereich ausgewählte Elemente beziehen, werden oben angezeigt, und die Aktionen, die für im Ergebnisbereich ausgewählte Elemente verfügbar sind, werden unten angezeigt.

Wenn Sie die Konsole verwenden, wird Ihre Konfiguration wirksam, wenn Sie Ihre Änderungen über die Konsole festlegen. Daher können einige Webinterface-Einstellungen deaktiviert werden, wenn ihre Werte für die aktuelle Konfiguration nicht relevant sind und die entsprechenden Einstellungen in WebInterface.conf auf ihre Standardwerte zurückgesetzt werden. Citrix empfiehlt, dass Sie regelmäßige Backups der Dateien WebInterface.conf und config.xml für Ihre Sites erstellen.

Die Citrix Webinterface Management Console wird automatisch installiert, wenn Sie das Webinterface für Microsoft IIS installieren. Führen Sie die Konsole aus, indem Sie auf Start > Alle Programme > Citrix > Management Consoles > Citrix Web Interface Management klicken.

Hinweis: Sie müssen sicherstellen, dass MMC 3.0 auf dem Server vorhanden ist, auf dem Sie das Webinterface installieren, da dies eine Voraussetzung für die Installation der Citrix Webinterface Management-Konsole ist. MMC 3.0 ist standardmäßig auf allen Windows-Plattformen verfügbar, die für das Hosting des Webinterface unterstützt werden.

## Konfigurieren von Citrix Gateway-Einstellungen im Webinterface 5.4

March 27, 2024

Um Citrix Gateway in Ihrer Bereitstellung zu verwenden, müssen Sie das Webinterface konfigurieren, das die Appliance unterstützt. Verwenden Sie dazu die Aufgabe Secure Access in der Citrix Webinterface Management-Konsole.

### So konfigurieren Sie Citrix Gateway-Einstellungen im Webinterface

1. Klicken Sie im **Windows-Startmenü** auf **Alle Programme > Citrix > Management Consoles > Citrix Web Interface Management**.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management-Konsole entweder auf **Citrix Virtual Apps-Websites oder auf Citrix Virtual Apps Services Sites,** und wählen Sie dann Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im **Aktionsbereich** auf **Secure Access**.
4. Führen Sie auf der Seite Zugriffsmethoden angeben einen der folgenden Schritte aus:
    - Klicken Sie auf **Hinzufügen**, um eine neue Zugriffsroute hinzuzufügen.
    - Wählen Sie eine bestehende Route aus der Liste aus und klicken Sie dann auf **Bearbeiten**.
5. Wählen Sie aus der Liste **Zugriffsmethode** eine der folgenden Optionen aus:
    - Wenn Sie die tatsächliche Adresse des Citrix Servers an Citrix Gateway senden möchten, wählen Sie **Gateway Direct**aus.
    - Wenn Sie die alternative Adresse des Citrix Virtual Apps-Servers an Citrix Gateway senden möchten, wählen Sie **Gateway alternate**aus.

    **Hinweis**: Auf virtuelle Desktops von Citrix Virtual Desktops kann nicht zugegriffen werden, wenn alternative Adressen verwendet werden.

    - Wenn die an Citrix Gateway angegebene Adresse durch die im Webinterface festgelegten Adressübersetzungszuordnungen bestimmt werden soll, wählen Sie **Gateway übersetzt**aus.
6. Geben Sie die Netzwerkadresse und die Subnetzmaske ein, die das Clientnetzwerk identifizieren. Verwenden Sie die Schaltflächen **Nach oben und Nach unten**, um die Zugriffswege in der Tabelle Benutzergeräte-Adressen in der Reihenfolge ihrer Priorität zu platzieren, und klicken Sie dann auf **Weiter**.
7. Wenn Sie keine Gateway-Adressübersetzung verwenden, fahren Sie mit Schritt 10 fort. Wenn Sie die Gateway-Adressübersetzung verwenden, führen Sie auf der Seite Adressübersetzungen angeben einen der folgenden Schritte aus:
    - Klicken Sie auf **Hinzufügen**, um eine neue Adressübersetzung hinzuzufügen.
    - Wählen Sie eine vorhandene Adressübersetzung aus der Liste aus und klicken Sie dann auf **Bearbeiten**.

    8. Wählen Sie im **Bereich Zugriffstyp**eine der folgenden Optionen aus:
        - Wenn Citrix Gateway die übersetzte Adresse verwendet, um eine Verbindung zum Citrix Server herzustellen, wählen Sie **Gateway-Routenübersetzung**aus.
        - Wenn Sie eine vom Client übersetzte Route in der Tabelle Benutzergeräteadressen konfiguriert haben und möchten, dass sowohl der Citrix Client als auch Citrix Gateway die übersetzte Adresse für die Verbindung mit dem Citrix Server verwenden, wählen Sie Benutzergerät- und Gateway-Routenübersetzung aus.

8. Geben Sie die internen und externen (übersetzten) Ports und Adressen für den Citrix Server ein, klicken Sie auf **OK** und dann auf **Weiter**.
   Wenn Citrix Gateway eine Verbindung zum Citrix Server herstellt, verwendet es die externe Portnummer und Adresse. Stellen Sie sicher, dass die von Ihnen erstellten Zuordnungen mit der Art der Adressierung übereinstimmen, die von der Serverfarm verwendet wird.
9. Geben Sie auf der Seite Gateway-Einstellungen angeben den vollqualifizierten Domänennamen (FQDN) und die Portnummer des Citrix Gateway-Geräts an, das Clients verwenden müssen. Der FQDN muss mit dem übereinstimmen, was sich auf dem auf dem Gateway installierten Zertifikat befindet.
10. Wählen Sie **Sitzungszuverlässigkeit aktivieren**, wenn der Citrix Server getrennte Sitzungen offen lassen soll, während der Client versucht, die Verbindung automatisch wiederherzustellen.
11. Wählen Sie **Tickets von zwei STAs anfordern** waren verfügbar, wenn Sie die Sitzungszuverlässigkeit aktiviert haben und gleichzeitiges Ticketing von zwei Secure Ticket Authority (STA) -Servern verwenden möchten. Wenn Sie diese Option aktivieren, erhält das Webinterface Tickets von zwei verschiedenen STAs, damit Benutzersitzungen nicht unterbrochen werden, wenn eine STA während der Sitzung nicht verfügbar ist. Wenn das Webinterface aus irgendeinem Grund nicht in der Lage ist, zwei STAs zu kontaktieren, greift es auf die Verwendung einer einzigen STA zurück. Klicken Sie auf **Weiter**.
12. Führen Sie auf der Seite Secure Ticket Authority Einstellungen angeben einen der folgenden Schritte aus:

    - Klicken Sie auf **Hinzufügen**, um die URL einer STA anzugeben, die das Webinterface verwenden kann.
    - Wählen Sie einen Eintrag aus der Liste aus und klicken Sie dann auf **Bearbeiten**.

    Verwenden Sie die Schaltflächen **Nach oben und Nach unten**, um die STAs in der Reihenfolge ihrer Priorität zu platzieren.
    STAs sind im Citrix XML-Dienst enthalten, `http\[s\]://servername.domain.com/scripts/ctxsta.dll`z. B.

    Sie können mehr als eine STA für die Fehlertoleranz angeben. Citrix empfiehlt jedoch, für diesen Zweck keinen externen Load Balancer zu verwenden.
13. Wählen Sie Für den Lastenausgleich **verwenden** aus, um zu wählen, ob der Lastausgleich zwischen STAs aktiviert werden soll.

    Durch die Aktivierung des Lastenausgleichs können Sie Verbindungen gleichmäßig auf Server verteilen, sodass kein Server überlastet wird.
14. Wählen Sie **Ausfallende Server umgehen** für aus, um anzugeben, wie lange nicht erreichbare STAs umgangen werden müssen.

Das Webinterface bietet Fehlertoleranz zwischen den Servern in der Liste der STA-URLs, sodass bei einem Kommunikationsfehler der ausgefallene Server für den angegebenen Zeitraum umgangen wird.

## Erstellen einer Webinterface 5.3-Site

March 27, 2024

Wenn Sie eine Webinterface 5.3-Site erstellen, können Sie Benutzer auffordern, sich entweder mit einem Webbrowser, der Citrix Workspace-App oder der Citrix Desktop Citrix Workspace-App anzumelden. Sie können die Citrix Webinterface Management-Konsole verwenden, um mehrere Webinterface-Sites zu erstellen.

Sie können das Single Sign-On nur mit einer Smartcard für das Webinterface mit dem Webinterface 5.3 aktivieren. Diese Version des Webinterface kann auf Citrix Virtual Apps 4.5, 5.0 und 6.0 ausgeführt werden.

Webinterface 5.3 läuft auf folgenden Betriebssystemen:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

> **Hinweis**:
> Citrix Virtual Apps 6.0 läuft nur unter Windows Server 2008 R2.

### So erstellen Sie eine Webinterface 5.3-Site

1. Klicken Sie auf **Start > Alle Programme > Citrix > Managementkonsolen > Citrix Web Interface Management**.
2. Wählen Sie im linken Bereich Citrix Virtual Apps-Websites aus. Benutzer melden sich mit einem Webbrowser am Webinterface an.
3. Klicken Sie im Menü **Aktion** auf **Site erstellen**.
4. Behalten Sie die standardmäßige Website und den Pfad der Internetinformationsdienste (IIS) bei und klicken Sie dann auf **Weiter**.

   Der standardmäßige Sitepfad lautet /Citrix/Citrix Virtual Apps oder Sie können einen Pfad angeben.

> **Hinweis**: Wenn es bereits Citrix Virtual Apps-Websites gibt, die den Standardpfad verwenden, wird ein entsprechendes Inkrement hinzugefügt, um die neue Site zu unterscheiden.

5. Wählen **Sie unter Geben Sie an, wo die Benutzerauthentifizierung stattfindet**, eine der folgenden Optionen aus:

   - Am Webinterface, um Benutzer über das Webinterface authentifizieren zu lassen.

     Wählen Sie diese Option aus, wenn das Webinterface als eigenständiger Server parallel zu Citrix Gateway in der entmilitarisierten Zone (DMZ) bereitgestellt wird.

   - Bei Access Gateway, damit Benutzer sich mit dem Citrix Gateway-Gerät authentifizieren können.

     Wenn Sie diese Option auswählen, authentifiziert Citrix Gateway Benutzer und initiiert Single Sign-On am Webinterface, wenn es auf dem Gerät konfiguriert ist.

   > **Hinweis**: Wenn SmartAccess auf Citrix Gateway konfiguriert ist, aktiviert diese Einstellung SmartAccess in Citrix Virtual Apps and Desktops.

6. Klicken Sie auf **Weiter**.
7. Geben Sie in Schritt 5 in der URL des Authentifizierungsdienstes die Webadresse für die URL des Citrix Gateway-Authentifizierungsdienstes ein, z. B. `https://access.company.com/CitrixAuthService/AuthService.asmx` und klicken Sie dann auf **Weiter**.
8. Wählen Sie unter **Authentifizierungsoptionen**aus, **wie sich Benutzer anmelden**.

   - **Explizit**. Benutzer melden sich mit einem Webbrowser an.
   - **Smartcard**. Benutzer melden sich mit einer Smartcard an.

9. Klicken Sie auf **Weiter**.
10. Wenn Sie in Schritt 8 **Smart Card** ausgewählt haben, wählen Sie eine der folgenden Optionen aus:

    - Fordern Sie Benutzer zur PIN auf. Benutzer geben ihre persönliche Identifikationsnummer (PIN) ein, wenn sie eine veröffentlichte Anwendung oder einen veröffentlichten Desktop starten.
    - Benutzer müssen ihre PIN nicht eingeben, wenn sie eine veröffentlichte Anwendung oder einen veröffentlichten Desktop starten.

    Auf dem Übersichtsbildschirm werden die Einstellungen angezeigt.

11. Klicken Sie auf **Weiter**, um die Webinterface-Site zu erstellen. Wenn die Site erfolgreich erstellt wurde, werden Sie aufgefordert, die verbleibenden Einstellungen im Webinterface zu konfigurieren. Folgen Sie den Anweisungen im Assistenten, um die Konfiguration abzuschließen.

# Konfigurieren von Citrix Gateway-Einstellungen im Webinterface 5.3

March 27, 2024

Nachdem Sie die Webinterface 5.3-Site erstellt haben, können Sie Citrix Webinterface Management verwenden, um Einstellungen für Citrix Gateway zu konfigurieren.

## So konfigurieren Sie Webinterface 5.3-Einstellungen für Citrix Gateway

1. Klicken Sie auf **Start > Alle Programme > Citrix > Managementkonsolen > Citrix Web Interface Management**.
2. Klicken Sie im linken Bereich von Citrix Webinterface Management auf **Citrix Virtual Apps-Websites**.
3. Klicken Sie im Aktionsbereich auf **Secure Access**.
4. Klicken **Sie im Dialogfeld „Secure Access-Einstellungen bearbeiten** “auf **Hinzufügen**.
5. Geben **Sie im Dialogfeld Zugangsroute hinzufügen** die Adresse des Benutzergeräts und die Subnetzmaske ein. Wählen Sie unter **Zugriffsmethode**die Option **Gateway direkt**aus, klicken Sie auf **OK**und dann auf **Weiter**. Wenn Sie die Adresse des Benutzergeräts und die Subnetzmaske nicht angeben, gilt die Option Gateway direct für alle Benutzergeräte. Die Option Gateway direct ist für Benutzergeräte geeignet, die sich von außerhalb des internen Netzwerks verbinden, wohingegen die Option Direct für Benutzergeräte geeignet ist, die sich aus dem internen Netzwerk verbinden.
6. Geben Sie unter **Adresse (FQDN)**den vollqualifizierten Domänennamen (FQDN) von Citrix Gateway ein. Dies muss derselbe FQDN sein, der für das Citrix Gateway-Zertifikat verwendet wird.
7. Geben Sie unter **Port**die Portnummer ein. Die Standardeinstellung ist 443.
8. Um die Sitzungszuverlässigkeit zu **aktivieren, klicken Sie auf Sitzungszuverlässigkeit**aktivieren und dann auf **Weiter**.
9. Klicken **Sie unter Secure Ticket Authority-URLs**auf **Hinzufügen**.
10. Geben Sie unter **Secure Ticket Authority-URL**den Namen des Masterservers ein, auf dem der XML-Dienst auf Citrix Virtual Apps ausgeführt wird, klicken Sie auf **OK**und dann auf **Fertig stellen**. Geben Sie zum Beispiel ein `http://Citrix Virtual Appssrv01/Scripts/CtxSta.dll`.

Nachdem Sie die Einstellungen im Webinterface konfiguriert haben, können Sie die Einstellungen auf Citrix Gateway konfigurieren.

## Hinzufügen von Citrix Virtual Apps and Desktops zu einer einzelnen Site

March 27, 2024

Wenn Sie Citrix Virtual Apps and Desktops ausführen, können Sie beide Anwendungen zu einer einzigen Webinterface-Site hinzufügen. Mit dieser Konfiguration können Sie denselben Secure Ticket Authority (STA) -Server von Citrix Virtual Apps and Desktops aus verwenden.

> **Hinweis**:
> Citrix Virtual Desktops unterstützt das Webinterface. Die erforderliche Mindestversion des Webinterface ist 5.0.

Wenn Sie Webinterface 5.3 oder 5.4 verwenden, kombinieren Sie die Sites Citrix Virtual Apps and Desktops mithilfe der Webinterface Management-Konsole.

> **Hinweis**:
> Wenn sich die Serverfarmen in verschiedenen Domänen befinden, müssen Sie eine bidirektionale Vertrauensstellung zwischen den Domänen herstellen.

### So fügen Sie Citrix Virtual Apps and Desktops mithilfe des Webinterface 5.3 oder 5.4 zu einer einzelnen Site hinzu

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Citrix Web Interface Management**.
2. Wählen Sie im linken Bereich **Citrix Virtual Apps Web Sites**aus.
3. Klicken Sie im **Aktionsbereich** mit der rechten Maustaste auf eine Site, und klicken Sie dann auf **Serverfarmen**.
4. Klicken **Sie im Dialogfeld Serverfarmen verwalten** auf **Hinzufügen**.
5. Füllen Sie die Einstellungen für die Serverfarm aus und klicken Sie dann zweimal auf **OK**.

Um die beste Erfahrung bei der Verwendung von Citrix Virtual Desktops zu erzielen, ändern Sie die Einstellung UserInterfaceBranding in Desktops in der Konfigurationsdatei WebInterface.conf.

## Routing von Benutzerverbindungen über Citrix Gateway

March 27, 2024

In Citrix Virtual Apps and Desktops können Sie die Server so konfigurieren, dass sie nur Verbindungen akzeptieren, die über Citrix Gateway geroutet werden. In Citrix XenApp 6.5 konfigurieren Sie eine

Richtlinie in Citrix AppCenter, um Verbindungen über Citrix Gateway weiterzuleiten. In Citrix Virtual Desktops 7.1 verwenden Sie Citrix Studio, um die Einstellungen zu konfigurieren.

### So konfigurieren Sie Citrix XenApp 6.5-Servereigenschaften so, dass Verbindungen akzeptiert werden, die nur über Citrix Gateway geroutet werden

1. Klicken Sie auf Start > Verwaltung > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie NetScaler-Ressourcen > Citrix Virtual Apps > FarmName, wobei FarmName der Name der Serverfarm ist.
3. Klicken Sie auf Richtlinien.
4. Klicken Sie im mittleren Bereich auf Computer oder Benutzer und dann auf Neu.
5. Geben Sie im Assistenten für neue Richtlinien unter Name einen Namen für die Richtlinie ein, und klicken Sie dann auf Weiter.
6. Klicken Sie unter **Kategorien**auf **Servereinstellungen**.
7. Klicken **Sie unter Einstellungen**neben Verbindungszugriffssteuerung auf **Hinzufügen**.
8. Wählen **Sie im Dialogfeld Einstellung hinzufügen - Verbindungszugriffssteuerung** unter **Wert die Option Nur Citrix Access Gateway-Verbindungen aus,** und klicken Sie dann auf **OK**.
9. Klicken Sie **zweimal auf Weiter** und dann auf **Erstellen**. Citrix Virtual Apps erstellt die Richtlinie.

### So konfigurieren Sie die Servereigenschaften von Citrix Virtual Desktops so, dass Verbindungen akzeptiert werden, die nur über Citrix Gateway geroutet werden

Sie können den Zugriff auf die Maschinen einer Bereitstellungsgruppe einschränken. Sie können den Zugriff für Benutzer einschränken, indem Sie SmartAccess verwenden, das Benutzerverbindungen filtert, die über Citrix Gateway hergestellt wurden. Sie können diese Aufgabe im Knoten Richtlinie in Studio oder über Richtlinieneinstellungen ausführen, wie in der Schnellreferenztabellebeschrieben.

1. Wählen Sie in Studio unter Bereitstellungsgruppen die Bereitstellungsgruppe aus, die Sie einschränken möchten.
2. Klicken Sie auf Bereitstellungsgruppe bearbeiten und dann auf Zugriffsrichtlinie.
3. Wählen Sie auf der Seite Zugriffsrichtlinie Verbindungen über Citrix Gateway aus. Es sind nur Verbindungen über das Citrix Gateway zulässig.
4. Um eine Teilmenge dieser Verbindungen auszuwählen, wählen Sie Verbindungen, die einen der folgenden Filter erfüllen:

    a) Definieren Sie die Citrix Gateway-Site.
    b) Fügen Sie die SmartAccess-Zeichenfolgen hinzu, bearbeiten oder entfernen Sie sie, die die erlaubten Benutzerzugriffsszenarien für die Bereitstellungsgruppe definieren. Weitere In-

formationen zur Konfiguration von SmartAccess finden Sie unter Konfigurieren von SmartAccess auf Citrix Gateway.

## Konfigurieren der Kommunikation mit dem Webinterface

March 27, 2024

Sie können Citrix Gateway für die Kommunikation mit dem Webinterface konfigurieren, das auf Citrix Virtual Apps and Desktops ausgeführt wird. Konfigurieren Sie dazu einen virtuellen Server auf Citrix Gateway. Binden Sie als Nächstes ein signiertes Serverzertifikat sowie Authentifizierungs-, Sitzungs-, Vorauthentifizierungs- und Nachauthentifizierungsrichtlinien an den virtuellen Server. Citrix Gateway verwendet die IP-Adresse des virtuellen Servers, um Benutzerverbindungen zum Webinterface weiterzuleiten.

Mit dem Assistenten für veröffentlichte Anwendungen können Sie Citrix Gateway so konfigurieren, dass Benutzerverbindungen an das Webinterface weitergeleitet werden. Citrix Gateway verwendet die Secure Ticket Authority (STA) für Benutzerverbindungen.

## Konfigurieren von Richtlinien für veröffentlichte Anwendungen und Desktops

March 27, 2024

Um die Kommunikation mit Citrix Virtual Apps and Desktops-Servern herzustellen, müssen Sie Citrix Gateway so konfigurieren, dass die Server erkannt werden. Sie können die Einstellungen global konfigurieren oder Richtlinien verwenden, die an Benutzer, Gruppen oder virtuelle Server gebunden sind.

### So konfigurieren Sie das Webinterface global auf Citrix Gateway

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Gehen Sie im Dialogfeld Globale Citrix Gateway-Einstellungen auf der Registerkarte Client Experience wie folgt vor:
    a) Wählen Sie im Plug-in-Typ Java aus.
    b) Wählen Sie in Clientless Access Zulassen aus.

> **Hinweis**: Führen Sie Schritt 3 aus, um die VPN-fähige Citrix Workspace-App wie die Citrix Workspace-App für iOS oder die Citrix Workspace-App für Android zu unterstützen. Um die mobile Citrix Workspace-App zu unterstützen, müssen Sie mindestens Access Gateway 10, Build 69.6 oder Access Gateway 10, Build 71.6014.e installieren. Wenn Sie Access Gateway 9.3 ausführen, müssen Sie diesen Schritt nicht ausführen.

4. Wählen Sie auf der Registerkarte Published Applications neben ICA-Proxy die Option ON aus.
5. Geben Sie neben Webinterface-Adresse die Webadresse des Webinterface ein und klicken Sie dann auf **OK**.

### So konfigurieren Sie eine Sitzungsrichtlinie für das Webinterface

Sie können eine Sitzungsrichtlinie konfigurieren und an einen virtuellen Server binden, um den Zugriff auf das Webinterface zu beschränken.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway-Richtlinien und klicken Sie dann auf Sitzung.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Dialogfeld Sitzungsrichtlinie erstellen in das Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf Neu.
5. Geben Sie im Dialogfeld Sitzungsprofil erstellen in das Feld Name einen Namen für das Profil ein.
6. Gehen Sie auf der Registerkarte Client Experience wie folgt vor:

    a) Wählen Sie neben dem Plug-in-Typ Override Global aus und wählen Sie dann Java aus.
    b) Wählen Sie neben Clientless Access die Option Global überschreiben aus und wählen Sie dann Zulassen aus.

7. Klicken Sie neben ICA-Proxy auf Override Global und wählen Sie ON aus.
8. Klicken Sie neben Webinterface-Adresse auf Override Global, geben Sie die Webadresse des Webinterface ein und klicken Sie dann auf Create.
9. Wählen Sie im Dialogfeld Sitzungsrichtlinie erstellen neben Benannte Ausdrücke die Option Allgemein aus, wählen Sie Wahrer Wert aus, klicken Sie auf Ausdruck hinzufügen , klicken Sie auf Erstellen und dann auf Schließen.

Nachdem Sie eine Sitzungsrichtlinie erstellt haben, binden Sie die Richtlinie an einen virtuellen Server.

### So binden Sie eine Sitzungsrichtlinie an einen virtuellen Server

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf Virtuelle Server.
2. Wählen Sie im Detailbereich einen virtuellen Server aus und klicken Sie dann auf Öffnen.
3. Klicken Sie auf der Registerkarte Richtlinien auf Sitzung und dann auf Richtlinie einfügen.
4. Wählen Sie eine Sitzungsrichtlinie aus der Liste aus, geben Sie die Prioritätsnummer ein (optional) und klicken Sie dann auf OK

## Konfigurieren von Einstellungen mit dem Assistenten für veröffentlichte Anwendungen

March 27, 2024

Um Citrix Gateway mit dem Webinterface zu konfigurieren, benötigen Sie die folgenden Informationen:

- IP-Adressen von Servern, auf denen Citrix Virtual Apps and Desktops ausgeführt werden.
- Vollqualifizierter Domänenname (FQDN) des Servers, auf dem das Webinterface ausgeführt wird.
- Virtueller Server, der auf Citrix Gateway konfiguriert ist.
- Für SmartAccess konfigurierte Sitzungsrichtlinie.
- IP-Adressen zusätzlicher Server, auf denen das Webinterface ausgeführt wird, wenn Sie das Webinterface-Failover konfigurieren.

### So konfigurieren Sie Webinterface-Einstellungen mithilfe des Assistenten für veröffentlichte Anwendungen

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf Citrix Gateway.
2. Klicken Sie im Detailbereich unter Erste Schritte auf Assistent für veröffentlichte Anwendungen.
3. Klicken Sie auf Weiter und folgen Sie dann den Anweisungen des Assistenten.

Sie können die Secure Ticket Authority (STA) im Assistenten für veröffentlichte Anwendungen konfigurieren und aktivieren. Wenn Sie den Assistenten für veröffentlichte Anwendungen abschließen, sind die Einstellungen global gebunden.

# Konfigurieren der Secure Ticket Authority auf Citrix Gateway

March 27, 2024

Die Secure Ticket Authority (STA) ist für die Ausstellung von Sitzungstickets als Reaktion auf Verbindungsanfragen für veröffentlichte Anwendungen auf Citrix Virtual Apps und veröffentlichte Desktops auf Citrix Virtual Desktops verantwortlich. Diese Sitzungstickets bilden die Grundlage für die Authentifizierung und Autorisierung für den Zugriff auf veröffentlichte Ressourcen.

Sie können die STA global oder an virtuelle Server binden. Sie können auch mehrere Server hinzufügen, auf denen die STA ausgeführt wird, wenn Sie einen virtuellen Server konfigurieren.

Wenn Sie die Kommunikation zwischen dem Citrix Gateway und der STA sichern, stellen Sie sicher, dass ein Serverzertifikat auf dem Server installiert ist, auf dem die STA ausgeführt wird.

In einer typischen Citrix Gateway GSLB-Bereitstellung müssen alle virtuellen Gateway-Server (an jedem Standort) mit denselben Back-End-STA-Servern konfiguriert werden, um Wiederverbindungsprobleme zu vermeiden.

## Um die STA global zu binden

1. Navigieren Sie zu **Citrix Gateway > Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter Server auf **STA-Server binden/unbind**, die von der Secure Ticket Authority verwendet werden sollen.
3. Klicken Sie im Dialogfeld **STA-Server binden/aufheben** auf **Hinzufügen**.
4. Geben **Sie im Dialogfeld STA-Server konfigurieren** die URL des STA-Servers ein, klicken Sie auf **Create**und dann auf **OK**.
5. Geben Sie im Dialogfeld **STA Server** unter URL die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Servers ein, auf dem die STA ausgeführt wird, und klicken Sie dann auf **Create**.

   > **Hinweis**:
   > Sie können mehr als einen Server, auf dem die STA ausgeführt wird, zur Liste hinzufügen. Die im Webinterface aufgeführten STAs müssen mit den STAs übereinstimmen, die auf Citrix Gateway konfiguriert sind. Wenn Sie mehrere STAs konfigurieren, verwenden Sie keinen Lastenausgleich zwischen Citrix Gateway und den Servern, auf denen die STA ausgeführt wird.

### So binden Sie eine STA an den virtuellen Server

1. Navigieren Sie zu **Citrix Gateway > Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen Server aus und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Veröffentlichte Anwendungen** unter Secure Ticket Authority auf **Hinzufügen**.
4. Geben **Sie im Dialogfeld STA-Server konfigurieren** die URL des STA-Servers ein und klicken Sie dann auf **Create**.
5. Wiederholen Sie Schritt 4, um weitere STA-Server hinzuzufügen, und klicken Sie dann auf **OK.**

### Referenzen

- Einzelheiten zu STA finden Sie im Artikel NetScaler Gateway Secure Ticket Authority.
- Einzelheiten zur Konfiguration Ihres Citrix Gateway für die Verwendung eines Cloud Connector als Secure Ticket Authority (STA) -Server finden Sie unter Wie konfiguriere ich Citrix Gateway für die Verwendung eines Cloud Connector als STA.

## Konfigurieren zusätzlicher Webinterface-Einstellungen auf Citrix Gateway

March 27, 2024

Wenn Sie Citrix Gateway in einer Webinterface-Umgebung bereitstellen, können Sie die folgenden optionalen Aufgaben ausführen:

- Konfigurieren von Webinterface-Failover Konfigurieren Sie Citrix Gateway für das Failover auf einen sekundären Server, auf dem das Webinterface ausgeführt
- Konfigurieren von Smart Card Access mit dem Webinterface Konfigurieren Sie Benutzersitzungen, um sich mithilfe der Citrix Workspace-App und der Smartcard-Authentifizierung direkt am Webinterface anzumelden.

## Konfigurieren von Webinterface-Failover

March 27, 2024

Sie können den Assistenten für veröffentlichte Anwendungen verwenden, um Citrix Gateway für das Failover auf einen sekundären Server zu konfigurieren, auf dem das Webinterface ausgeführt wird.

Durch das Webinterface-Failover können Benutzerverbindungen aktiv bleiben, wenn das primäre Webinterface ausfällt. Wenn Sie das Failover konfigurieren, definieren Sie zusätzlich zur System-IP-Adresse, der zugeordneten IP-Adresse oder der IP-Adresse des virtuellen Servers eine neue IP-Adresse. Die neue IP-Adresse muss sich im selben Subnetz wie das System oder die zugeordnete IP-Adresse befinden.

Wenn Sie das Webinterface-Failover auf Citrix Gateway konfigurieren, wird jeglicher Netzwerkverkehr, der an die neue IP-Adresse gesendet wird, an das primäre Webinterface weitergeleitet. Der virtuelle Server, den Sie im Assistenten für veröffentlichte Anwendungen auswählen, dient als IP-Adresse für die Netzwerkadressübersetzung (NAT). Die eigentliche IP-Adresse ist die des Webinterface. Wenn das primäre Webinterface ausfällt, wird der Netzwerkverkehr an das sekundäre Webinterface gesendet.

### So konfigurieren Sie Webinterface-Failover

1. Klicken Sie im Konfigurationsprogramm auf die Registerkarte Konfiguration und dann im Navigationsbereich auf Citrix Gateway.
2. Klicken Sie im Detailbereich unter Erste Schritte auf Assistent für veröffentlichte Anwendungen.
3. Klicken Sie auf Weiter, wählen Sie einen virtuellen Server aus und klicken Sie dann auf Weiter.
4. Klicken Sie auf der Seite Clientverbindungen konfigurieren auf Webinterface-Failover konfigurieren.
5. Geben Sie unter Primäres Webinterface in Webinterface Server die IP-Adresse des primären Webinterface ein.
6. Geben Sie unter Webinterface Server Port die Portnummer für das primäre Webinterface ein.
7. Geben Sie in Virtual Server IP die neue IP-Adresse für das Failover ein.
8. Geben Sie unter Virtueller Serverport die Portnummer für den virtuellen Server ein.
9. Geben Sie unter Backup Webinterface in Webinterface Server die IP-Adresse des Servers ein, auf dem das Webinterface ausgeführt wird, oder wählen Sie einen Server aus der Liste aus.
10. Geben Sie unter Webinterface Server Port die Portnummer des Webinterface ein und klicken Sie dann auf OK.
11. Klicken Sie auf Weiter und folgen Sie dann den Anweisungen, um den Assistenten abzuschließen.

## Konfigurieren des Smartcard-Zugriffs mit dem Webinterface

March 27, 2024

Wenn Sie das Webinterface für die Verwendung der Smartcard-Authentifizierung konfigurieren, können Sie die folgenden Bereitstellungsszenarien konfigurieren, um Citrix Gateway zu integrieren, je nachdem, wie sich Benutzer anmelden:

- Wenn sich Benutzer mithilfe der Citrix Workspace-App und der Smartcard-Authentifizierung direkt am Webinterface anmelden, muss das Webinterface parallel zu Citrix Gateway in der DMZ verlaufen. Der Server, auf dem das Webinterface ausgeführt wird, muss auch ein Domänenmitglied sein.

  In diesem Szenario führen sowohl Citrix Gateway als auch das Webinterface eine SSL-Terminierung durch. Das Webinterface beendet sicheren HTTP-Verkehr einschließlich Benutzerauthentifizierung, Anzeige veröffentlichter Anwendungen und Starten veröffentlichter Anwendungen. Citrix Gateway beendet SSL für eingehende ICA-Verbindungen.

- Wenn sich Benutzer mit dem Citrix Gateway Plug-in anmelden, führt Citrix Gateway die Erstauthentifizierung durch. Wenn Citrix Gateway den VPN-Tunnel einrichtet, können sich Benutzer mithilfe der Smartcard am Webinterface anmelden. In diesem Szenario können Sie das Webinterface hinter Citrix Gateway in der DMZ oder im sicheren Netzwerk installieren.

> **Hinweis**:
> Citrix Gateway kann die Smartcard auch mithilfe eines Clientzertifikats für die Authentifizierung verwenden.

Weitere Informationen finden Sie unter
Konfigurieren der Smartcard-Authentifizierung

## Konfigurieren des Zugriffs auf Anwendungen und virtuelle Desktops im Webinterface

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass Benutzern Zugriff auf veröffentlichte Anwendungen und virtuelle Desktops mit dem Citrix Gateway Plug-In statt mit Receiver gewährt wird. Um den Zugriff auf Anwendungen und Desktops zu konfigurieren, ändern Sie die Konfiguration auf Citrix Gateway von der Verwendung von Receiver nur für die Verbindung mit Citrix Gateway zu einer Konfiguration, die Verbindungen mithilfe des Citrix Gateway Plug-ins mit einmaliger Anmeldung am Webinterface ermöglicht. Sie konfigurieren beispielsweise Citrix Gateway so, dass sich alle Benutzer mit dem Citrix Gateway Plug-in verbinden und das Webinterface als Homepage verwenden. Dieses Szenario unterstützt Single Sign-On am Webinterface.

Zusätzlich zum Zugriff auf Anwendungen und Desktops können Benutzer auch auf dem Benutzergerät installierte Anwendungen ausführen, die Netzwerkverbindungen über den VPN-Tunnel herstellen.

Verwenden Sie die folgenden Richtlinien, um die Konfiguration zu starten:

- Erstellen Sie eine Webinterface-Site.

- Konfigurieren Sie die Einstellungen für erweiterte Zugriffssteuerung
- Konfigurieren Sie SmartAccess.
- Konfigurieren Sie die Endpunktanalyse auf Citrix Gateway.
- Konfigurieren Sie Richtlinien und Filter für Citrix Virtual Apps and Desktops.
- Konfigurieren Sie Citrix Gateway so, dass sich Benutzer mithilfe des Citrix Gateway-Plug-ins anmelden, um auf veröffentlichte Anwendungen und virtuelle Desktops zuzugreifen.

Weitere Informationen finden Sie in den folgenden Themen in der Citrix Produktdokumentation:

- Einrichten einer Webinterface-Site.
- So funktioniert SmartAccess für Citrix Virtual Apps and Desktops
- Konfigurieren von Endpunktrichtlinien
- Konfigurieren von Citrix Virtual Apps Richtlinien und Filtern
- Konfigurieren von Richtlinien und Filter in Citrix Virtual Desktops 5
- Konfigurieren von Citrix Gateway für die Kommunikation mit dem Webinterface

Wenn Sie die Benutzeranmeldung bei Citrix Virtual Apps and Desktops konfigurieren, erstellen Sie zunächst ein Sitzungsprofil, um das Citrix Gateway-Plug-in für Windows auszuwählen. Anschließend erstellen Sie ein Profil für Intranetanwendungen für den Zugriff auf Citrix Virtual Apps, Citrix Virtual Desktops und das Webinterface.

### So konfigurieren Sie globale Einstellungen für das Citrix Gateway Plug-in für den Zugriff auf Anwendungen und Desktops

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration”im Navigationsbereich “Citrix Gateway”und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungen auf Globale Einstellungen ändern.
3. Wählen Sie auf der Registerkarte Published Applications neben ICA-Proxy OFF aus.
4. Geben Sie unter Webinterface-Adresse die URL der Webinterface-Site ein. Dies wird zur Homepage für Benutzer.
5. Geben Sie unter Single Sign-On Domäne den Active Directory-Domänennamen ein.
6. Wählen Sie auf der Registerkarte Client Experience neben Plug-In-Typ Windows/Mac OS X aus und klicken Sie dann auf OK.

### So konfigurieren Sie die Intranet-Anwendung

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway\ > Ressourcen**, und klicken Sie dann auf Intranet-Anwendungen.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie unter Nameeinen Namen für die Anwendung ein.

4. Klicken Sie auf Transparent.
5. Wählen Sie unter Protokoll TCP, UDP oder Any aus.
6. Wählen Sie unter Zieltyp die Option IP-Adresse und Netzwerkmaske aus. Geben Sie beispielsweise 172.16.100.0 und die Subnetzmaske 255.255.255.0 ein, um alle Server im Subnetz 172.16.100.x darzustellen. Die IP-Adresse des Webinterface, Citrix Virtual Apps und aller anderen Server, mit denen Benutzer eine Verbindung herstellen, müssen sich in einem der Subnetze befinden, die als Intranetanwendung definiert sind.

   Nachdem Sie die Intranet-Anwendung erstellt haben, können Sie sie global oder an einen virtuellen Server binden.
7. Geben Sie unter IP-Adresse und NetMask die IP-Adresse und Subnetzmaske ein, die Ihr internes Netzwerk darstellen, klicken Sie auf Erstellen und dann auf Schließen.

   Nachdem Sie die Intranet-Anwendung erstellt haben, können Sie sie global oder an einen virtuellen Server binden.

### So binden Sie eine Intranet-Anwendung global

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte "Configuration"im Navigationsbereich "Citrix Gateway"und klicken Sie auf "Global Settings".
2. Klicken Sie im Detailbereich unter Intranetanwendungen auf Mappings zu TCP-Anwendungen im sicheren Netzwerk für das Citrix Gateway-Plug-In für Java erstellen.
3. Klicken Sie im Dialogfeld VPN-Intranetanwendungen konfigurieren auf Hinzufügen.
4. Wählen Sie unter Verfügbar eine oder mehrere Intranetanwendungen aus, klicken Sie auf den Pfeil, um die Intranetanwendungen nach Konfiguriert zu verschieben, und klicken Sie dann auf OK.

### So binden Sie eine Intranet-Anwendung an einen virtuellen Server

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf Virtuelle Server.
2. Wählen Sie im Detailbereich einen virtuellen Server aus und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld Citrix Gateway Virtual Server konfigurieren auf die Registerkarte Intranetanwendungen.
4. Wählen Sie unter Verfügbarer Anwendungsname die Intranetanwendungen aus, klicken Sie auf Hinzufügen und dann auf OK.

Wenn sich Benutzer mit dem Citrix Gateway Plug-in anmelden, wird der VPN-Tunnel eingerichtet und entweder der Empfänger oder das Webinterface wird als Homepage verwendet.

# Konfigurieren von SmartAccess

March 27, 2024

Sie können SmartAccess mit Citrix Virtual Apps and Desktops verwenden, um Benutzern intelligent veröffentlichte Anwendungen und virtuelle Desktops bereitzustellen.

Mit SmartAccess können Sie den Zugriff auf veröffentlichte Anwendungen und Desktops auf einem Server mithilfe von Citrix Gateway-Sitzungsrichtlinien steuern. Sie verwenden Vorauthentifizierungs- und Nachauthentifizierungsprüfungen zusammen mit anderen Bedingungen für den Zugriff auf veröffentlichte Ressourcen als Bedingung. Andere Bedingungen umfassen alles, was Sie mit einer Citrix Virtual Apps and Desktops-Richtlinie steuern können, wie Druckerbandbreitenbeschränkungen, Laufwerkszuordnung des Benutzergeräts, Zwischenablage, Audio und Druckerzuordnung. Sie können eine Richtlinie für Citrix Virtual Apps and Desktops basierend darauf anwenden, ob Benutzer eine Citrix Gateway-Prüfung bestehen.

Citrix Gateway kann Citrix Virtual Desktops mithilfe derselben Optionen bereitstellen, die mit Webinterface, ICA-Proxy-Zugriff, clientlosem Zugriff und Citrix Gateway-Zugriff verfügbar sind.

Diese Funktionalität wird durch die Integration von Citrix Gateway-Komponenten in das Webinterface und Citrix Virtual Apps and Desktops erreicht. Diese Integration bietet erweiterte Authentifizierung und Zugriffssteuerungsoptionen für das Webinterface. Weitere Informationen finden Sie in der Webinterface-Dokumentation im Knoten Technologies in der Citrix Produktdokumentation.

Für Remote-Konnektivität zu einer Serverfarm ist das Citrix Gateway-Plug-in nicht erforderlich. Benutzer können sich mit der Citrix Workspace-App verbinden. Benutzer können das Citrix Gateway Plug-in verwenden, um sich anzumelden und ihre veröffentlichten Anwendungen und virtuellen Desktops über das Access Interface zu empfangen, das die Standardstartseite für Citrix Gateway ist.

## So funktioniert SmartAccess für Citrix Virtual Apps and Desktops

March 27, 2024

Um SmartAccess zu konfigurieren, müssen Sie die Citrix Gateway-Einstellungen auf der Webinterface/-StoreFront konfigurieren und Sitzungsrichtlinien auf Citrix Gateway konfigurieren. Wenn Sie den Assistenten für veröffentlichte Anwendungen ausführen, können Sie die Sitzungsrichtlinien auswählen, die Sie für SmartAccess erstellt haben.

Nachdem Sie SmartAccess konfiguriert haben, funktioniert die Funktion wie folgt:

1. Wenn ein Benutzer die Webadresse eines virtuellen Servers in einem Webbrowser eingibt, werden alle von Ihnen konfigurierten Vorauthentifizierungsrichtlinien auf das Benutzergerät heruntergeladen.
2. Citrix Gateway sendet die Namen der Vorauthentifizierungs- und Sitzungsrichtlinien als Filter an die Webinterface/StoreFront. Wenn die Richtlinienbedingung auf true festgelegt ist, wird die Richtlinie immer als Filtername gesendet. Wenn die Richtlinienbedingung nicht erfüllt ist, wird der Filtername nicht gesendet. Auf diese Weise können Sie die Liste der veröffentlichten Anwendungen und Desktops und die effektiven Richtlinien auf einem Computer, auf dem Citrix Virtual Apps and Desktops ausgeführt wird, basierend auf den Ergebnissen der Endpunktanalyse unterscheiden.
3. Das Webinterface/StoreFront kontaktiert den Citrix Virtual Apps and Desktops-Server und gibt die veröffentlichte Ressourcenliste an den Benutzer zurück. Alle Ressourcen, auf die Filter angewendet wurden, werden nicht in der Liste des Benutzers angezeigt, es sei denn, die Bedingung des Filters ist erfüllt.

Sie können SmartAccess-Endpunktanalyse auf Citrix Gateway konfigurieren. Um Endpoint Analysis zu konfigurieren, erstellen Sie eine Sitzungsrichtlinie, die die **ICA-Proxy-Einstellung** aktiviert, und konfigurieren Sie dann eine Client-Sicherheitszeichenfolge.

Wenn sich der Benutzer anmeldet, führt die Endpoint Analysis-Richtlinie eine Sicherheitsüberprüfung des Benutzergeräts mit den Clientsicherheitszeichenfolgen durch, die Sie auf Citrix Gateway konfiguriert haben.

Sie möchten beispielsweise nach einer bestimmten Version von Sophos Antivirus suchen. Im Ausdrucksеditor erscheinen die Sicherheitszeichenfolgen des Clients wie folgt:

```
client.application.av(sophos).version == 10.0.2
<!--NeedCopy-->
```

Nachdem Sie die Sitzungsrichtlinie konfiguriert haben, binden Sie sie an einen Benutzer, eine Gruppe oder einen virtuellen Server. Wenn sich Benutzer anmelden, wird die SmartAccess-Richtlinienüberprüfung gestartet und überprüft, ob auf dem Benutzergerät Version 10.0.2 oder höher von Sophos Antivirus installiert ist.

Wenn die SmartAccess-Endpunktanalyseprüfung erfolgreich ist, wird das Webinterface/StoreFront-Portal in einer clientlosen Sitzung angezeigt. Andernfalls wird das Access Interface angezeigt.

Wenn Sie eine Sitzungsrichtlinie für SmartAccess erstellen, sind für das Sitzungsprofil keine Einstellungen konfiguriert, wodurch ein Nullprofil erstellt wird. In diesem Fall verwendet Citrix Gateway die global für SmartAccess konfigurierte Webinterface/StoreFront-URL.

## Konfigurieren von Citrix Virtual Apps Richtlinien und Filtern

March 27, 2024

Nachdem Sie die Sitzungsrichtlinie auf Citrix Gateway erstellt haben, konfigurieren Sie Richtlinien und Filter auf dem Computer, auf dem Citrix Virtual Apps ausgeführt wird. Die Richtlinien und Filter werden gemäß der Endpoint Analysis-Konfiguration auf Benutzer angewendet.

Einzelheiten zur Konfiguration von Citrix Virtual Apps Richtlinien und Filtern finden Sie unter Verwalten von Bereitstellungsgruppen.

## Konfigurieren einer Sitzungsrichtlinie für SmartAccess

March 27, 2024

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway > Richtlinien und klicken Sie dann auf Sitzung.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Dialogfeld Sitzungsrichtlinie erstellen in das Feld Name einen Namen für die Richtlinie ein, z. B. ValidEndpoint.
4. Klicken Sie unter Profil anfordern auf Neu und geben Sie unter Name einen Namen für das Profil ein, z. B. Null, und klicken Sie dann auf Erstellen.
5. Erstellen Sie im Dialogfeld Sitzungsrichtlinie erstellen einen Clientsicherheitsausdruck, klicken Sie auf Erstellen und dann auf Schließen.

Der Clientsicherheitsausdruck wird verwendet, um zwischen gültigen und ungültigen Endpunkten zu unterscheiden. Basierend auf den Ergebnissen der Endpunktanalyse können Sie verschiedene Zugriffsebenen auf veröffentlichte Anwendungen oder Desktops bereitstellen.

Nachdem Sie die Sitzungsrichtlinie erstellt haben, binden Sie sie entweder global oder an einen virtuellen Server.

## Konfigurieren der Benutzergerätezuordnung auf Citrix Virtual Apps

March 27, 2024

Sie können Citrix Gateway-Filter verwenden, die auf Richtlinien auf einem Computer angewendet werden, auf dem Citrix Virtual Apps ausgeführt werden. Filter bieten Benutzern Zugriff auf Citrix Vir-

tual Apps-Funktionen, wie z. B. die Laufwerkszuordnung von Benutzergeräten, die Druckerzuordnung oder die Zuordnung der Zwischenablage basierend auf den Ergebnissen der Endpunktanalyse.

Die Citrix Workspace-App unterstützt die Zuordnung von Geräten auf Benutzergeräten, damit Benutzer innerhalb von Benutzersitzungen auf externe Geräte zugreifen können. Die Zuordnung von Benutzergeräten bietet:

- Zugriff auf lokale Laufwerke und Ports
- Datenübertragung zwischen einer Benutzersitzung und der lokalen Zwischenablage ausschneiden und einfügen
- Audiowiedergabe (Systemsounds und .wav-Dateien) von der Benutzersitzung

Während der Anmeldung informiert das Benutzergerät den Server über die verfügbaren Benutzerlaufwerke und COM-Ports. In Citrix XenApp 6.5 werden Benutzerlaufwerke dem Server zugeordnet und verwenden den Laufwerksbuchstaben des Benutzergeräts. Diese Zuordnungen stehen nur dem aktuellen Benutzer während der aktuellen Sitzung zur Verfügung. Die Zuordnungen werden gelöscht, wenn sich der Benutzer abmeldet und bei der nächsten Anmeldung des Benutzers neu erstellt.

Nachdem Sie den XML-Dienst aktiviert haben, müssen Sie Richtlinien für die Zuordnung von Benutzergeräten konfigurieren.

Um Richtlinien für die Zuordnung von Benutzergeräten basierend auf SmartAccess-Filtern durchzusetzen, erstellen Sie die folgenden beiden Richtlinien auf dem Server:

- Eine restriktive ICA-Richtlinie, die die Zuordnung von Benutzergeräten deaktiviert und für alle Citrix Gateway-Benutzer gilt.
- Eine vollständige ICA-Richtlinie, die die Zuordnung von Benutzergeräten ermöglicht und nur für Benutzer gilt, die die Endpoint Analysis-Sitzungsrichtlinie erfüllen
  Hinweis: Die gefilterte, nicht restriktive ICA-Richtlinie muss eine höhere Priorität als die restriktive ICA-Richtlinie erhalten, damit, wenn sie für einen Benutzer gilt, die nicht einschränkende Richtlinie überschreibt die Richtlinie, die die Zuordnung von Benutzergeräten deaktiviert.

Sie konfigurieren restriktive und nicht restriktive Richtlinien für Citrix XenApp 6.5 mithilfe von Citrix AppCenter.

## Konfigurieren einer restriktiven Richtlinie in Citrix XenApp 6.5

March 27, 2024

1. Klicken Sie auf Start > Verwaltung > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie im linken Bereich Citrix Virtual Apps, erweitern Sie den Server und klicken Sie dann auf Richtlinien.

3. Klicken Sie im Bereich Richtlinien auf die Registerkarte Benutzer und dann auf Neu.
4. Geben Sie unter Name einen Namen für die Richtlinie ein und klicken Sie dann auf Weiter.
5. Klicken Sie unter Kategorien auf Alle Einstellungen.
6. Klicken Sie unter Einstellungen in Clientlaufwerke automatisch verbinden auf Hinzufügen.
7. Klicken Sie im Dialogfeld Einstellung hinzufügen auf Deaktiviert, klicken Sie auf OK und dann auf Weiter.
8. Klicken Sie unter Kategorien auf Alle Filter.
9. Klicken Sie unter Filter in der Zugriffssteuerung auf Hinzufügen.
10. Klicken Sie im Dialogfeld Neuer Filter auf Hinzufügen.
11. Klicken Sie im Modus auf Verweigern.
12. Wählen Sie unter Verbindungstyp With Access Gateway aus.
13. Geben Sie in AG Farm den Namen des virtuellen Servers ein.
14. Geben Sie unter Zugriffsbedingung den Namen der Sitzungsrichtlinie ein, der auf Citrix Gateway konfiguriert ist, klicken Sie zweimal auf OK, klicken Sie auf Weiter und dann auf Erstellen, um den Assistenten abzuschließen.

## Konfigurieren einer nicht restriktiven Richtlinie auf Citrix XenApp 6.5

March 27, 2024

1. Klicken Sie auf Start > Verwaltung > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie im linken Bereich Citrix Virtual Apps, erweitern Sie den Server und klicken Sie dann auf Richtlinien.
3. Klicken Sie im Bereich Richtlinien auf die Registerkarte Benutzer und dann auf Neu.
4. Geben Sie unter Name einen Namen für die Richtlinie ein und klicken Sie dann auf Weiter.
5. Klicken Sie unter Kategorien auf Alle Einstellungen.
6. Klicken Sie unter Einstellungen in Clientlaufwerke automatisch verbinden auf Hinzufügen.
7. Klicken Sie auf Aktiviert, klicken Sie auf OK und dann auf Weiter.
8. Klicken Sie unter Kategorien auf Alle Filter.
9. Klicken Sie unter Filter in der Zugriffssteuerung auf Hinzufügen.
10. Klicken Sie im Dialogfeld Neuer Filter auf Hinzufügen.
11. Klicken Sie im Modus auf Zulassen.
12. Wählen Sie unter Verbindungstyp With Access Gateway aus.
13. Geben Sie in AG Farm den Namen des virtuellen Servers ein.
14. Geben Sie unter Zugriffsbedingung den Namen der Sitzungsrichtlinie ein, der auf Citrix Gateway konfiguriert ist, klicken Sie zweimal auf OK, klicken Sie auf Weiter und dann auf Erstellen, um den Assistenten abzuschließen.

## Aktivieren von Citrix Virtual Apps als Quarantäne-Zugriffsmethode

March 27, 2024

Wenn Sie Endpoint Analysis auf Citrix Gateway konfiguriert haben, können Benutzer, die einen Endpunktscan bestehen, auf alle Ressourcen zugreifen, die Sie auf Citrix Gateway konfigurieren. Sie können Benutzer, die einen Endpunkt-Scan nicht bestehen, in eine Quarantänegruppe einfügen. Diese Benutzer können nur über Citrix Virtual Apps auf veröffentlichte Anwendungen zugreifen. Erfolg oder Misserfolg des Endpoint Analysis-Scans bestimmt die Zugriffsmethode, die Benutzern zur Verfügung steht.

Beispielsweise erstellen Sie einen Endpoint Analysis-Scan, um zu überprüfen, ob Notepad auf dem Benutzergerät ausgeführt wird, wenn sich Benutzer anmelden. Wenn Notepad ausgeführt wird, können sich Benutzer mit dem Citrix Gateway Plug-in anmelden. Wenn Notepad nicht ausgeführt wird, erhalten Benutzer nur die Liste der veröffentlichten Anwendungen.

Erstellen Sie eine Quarantänegruppe auf Citrix Gateway, um den eingeschränkten Benutzerzugriff zu konfigurieren. Sie erstellen die Quarantänegruppe innerhalb eines Sitzungsprofils und fügen das Profil dann einer Sitzungsrichtlinie hinzu.

## Erstellen einer Sitzungsrichtlinie und Endpoint Analysis-Scan für eine Quarantänegruppe

March 27, 2024

Um Citrix Virtual Apps als Quarantänezugriffsmethode zu aktivieren, erstellen Sie eine Gruppe auf Citrix Gateway, die Sie als Quarantänegruppe verwenden. Erstellen Sie dann eine Sitzungsrichtlinie, in der Sie die Gruppe auswählen.

Binden Sie die Richtlinie nach dem Erstellen der Sitzungsrichtlinie an die Quarantänegruppe. Nachdem Sie die Richtlinien konfiguriert und an die Gruppe gebunden haben, testen Sie die Ergebnisse. Damit sich Benutzer beispielsweise erfolgreich anmelden können, muss Notepad auf dem Benutzergerät ausgeführt werden. Wenn Notepad ausgeführt wird, können sich Benutzer mithilfe des Citrix Gateway-Plug-ins anmelden. Wenn Notepad nicht ausgeführt wird, können sich Benutzer mit der Citrix Workspace-App anmelden.

Weitere Informationen zum Konfigurieren von Endpoint Analysis-Richtlinien finden Sie unter Konfigurieren von Endpunktrichtlinien.

### So erstellen Sie einen Endpoint Analysis-Scan und fügen eine Quarantänegruppe hinzu

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway > Richtlinien und klicken Sie dann auf Sitzung.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Dialogfeld Sitzungsrichtlinie erstellen in das Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf Neu.
5. Geben Sie im Dialogfeld Sitzungsprofil erstellen in das Feld Name einen Namen für das Profil ein.
6. Klicken Sie auf der Registerkarte Sicherheit auf Erweitert.
7. Klicken Sie im Dialogfeld Sicherheitseinstellungen - Erweitert unter Client Security auf Global überschreiben und dann auf Neu.
8. Klicken Sie im Dialogfeld "Ausdruck erstellen"neben "Beliebiger Ausdruck anpassen"auf Hinzufügen.
9. Wählen Sie unter Ausdruckstyp die Option Clientsicherheit aus.
10. Wählen Sie unter Komponente die Option Prozess aus.
11. Geben Sie unter Name notepad.exe ein, klicken Sie auf OK und klicken Sie dann auf Create.
12. Wählen Sie im Dialogfeld Sicherheitseinstellungen - Erweitert in Quarantänegruppe die Quarantänegruppe aus, klicken Sie auf Erstellen, klicken Sie auf OK und dann auf Erstellen.
13. Wählen Sie im Dialogfeld Sitzungsrichtlinie erstellen neben Benannte Ausdrücke den Wert True aus, klicken Sie auf Ausdruck hinzufügen, klicken Sie auf Erstellen und dann auf Schließen.

## Konfigurieren von Citrix Virtual Desktops für SmartAccess

March 27, 2024

Mit Citrix Gateway können Citrix Virtual Desktops sichere Desktops für Remotebenutzer bereitstellen. Citrix Virtual Desktops können die SmartAccess-Funktionen von Citrix Gateway verwenden, um Desktops intelligent bereitzustellen. Wenn Sie die Delivery Services Console in Citrix Virtual Desktops zum Erstellen von Desktopgruppen verwenden, konfigurieren Sie dann Richtlinien und Filter für die Zugriffssteuerung.

Um Citrix Gateway für die Bereitstellung veröffentlichter Desktops zu konfigurieren, verwenden Sie dieselben Optionen, die für das Webinterface, den ICA-Proxy-Zugriff, den clientlosen Zugriff und den Citrix Gateway-Zugriff verfügbar sind.

Wenn Sie eine Sitzungsrichtlinie erstellen und Einstellungen auf der Registerkarte **Veröffentlichte Anwendungen** konfigurieren, verwenden Sie die Webadresse für die Citrix Virtual Desktops Webinterface-Site. Nachdem Sie die Richtlinie erstellt haben, binden Sie sie an einen virtuellen

Server. Erstellen Sie dann ein Nullsitzungsprofil, in dem Sie keine Einstellungen konfigurieren. Die Webinterface-Konfiguration wird von globalen Einstellungen geerbt.

## Konfigurieren einer Sitzungsrichtlinie für SmartAccess mit Citrix Virtual Desktops

March 27, 2024

Sie konfigurieren SmartAccess auf Citrix Gateway für den Zugriff auf Citrix Virtual Desktops, indem Sie eine an einen virtuellen Server gebundene Sitzungsrichtlinie erstellen.

**So konfigurieren Sie eine Sitzungsrichtlinie für SmartAccess mit Citrix Virtual Desktops über die GUI:**

1. Navigieren Sie auf der Registerkarte Konfiguration zu **Citrix Gateway > Richtlinien > Sitzung**.
2. Klicken Sie auf **die Registerkarte Sitzungsrichtlinien** und dann auf **Hinzufügen**.
3. Geben Sie auf der Seite **Create Citrix Gateway Sitzungsrichtlinie** einen Namen für die Richtlinie ein, z. B. Citrix Virtual DesktopsPolicy.
4. Klicken Sie in **Profil**auf **Hinzufügen**.
5. Geben Sie auf der Seite **Citrix Gateway-Sitzungsprofil erstellen** den Namen für das Profil ein, z. B. Citrix Virtual DesktopsProfile.
6. Klicken Sie auf der Registerkarte **Published Applications** neben **ICA-Proxy**auf **Override Global** und wählen Sie dann **ON**aus.
7. Klicken Sie unter **Webinterface-Adresse**auf **Override Global** und geben Sie dann die URL zur Citrix Virtual Desktops Webinterface-Site ein.
8. Klicken Sie in **Single Sign-On Domain aufOverride Global**, geben Sie den Domänennamen ein und klicken Sie dann auf**Erstellen**.
9. Fügen Sie auf der Seite **Citrix Sitzungsrichtlinie erstellen** unter **Ausdruck**den Ausdruck hinzu.

Sie müssen auch eine Nullsitzungsrichtlinie erstellen, die an den virtuellen Server gebunden ist. Das Sitzungsprofil enthält keine Konfiguration, was es zu einem Nullprofil macht. Fügen Sie in der Sitzungsrichtlinie den Ausdruck True Value hinzu und speichern Sie dann die Richtlinie.

Nachdem Sie beide Sitzungsrichtlinien erstellt haben, binden Sie beide Richtlinien an den virtuellen Server.

## Konfigurieren von Richtlinien und Filter in Citrix Virtual Desktops 5

March 27, 2024

Sie können Einstellungen in Citrix Virtual Desktops 5 mithilfe von Citrix Studio oder Gruppenrichtlinien-Editor konfigurieren. Wenn Sie Citrix Gateway-Einstellungen in Citrix Virtual Desktops konfigurieren, verwenden Sie den Namen des virtuellen Citrix Gateway-Servers und den Namen der Sitzungsrichtlinie. Konfigurieren Sie dann die Zugriffssteuerung, damit Verbindungen definierte Filter erfüllen können. Sie können auch SmartAccess-Richtlinien verwenden.

1. Klicken Sie auf dem Citrix Virtual Desktops-Server auf **Start > Alle Programme > Citrix > Citrix Studio**.
2. Klicken Sie im linken Bereich, um HDX-Richtlinie zu erweitern, und klicken Sie dann im mittleren Bereich auf die Registerkarte Benutzer.
3. Klicken Sie unter Benutzer auf Neu.
4. Geben Sie im Dialogfeld Neue Richtlinie unter Identifizieren Sie Ihre Richtlinie und dann in das Feld Name einen Namen ein.
5. Klicken Sie zweimal auf Weiter.
6. Klicken Sie im Dialogfeld Neue Richtlinie auf der Registerkarte Filter unter Filter auf Zugriffssteuerung und dann auf Hinzufügen.
7. Klicken Sie im Dialogfeld Neuer Filter auf Hinzufügen.
8. Wählen Sie im Dialogfeld Neues Filterelement unter Verbindungstyp die Option Mit Access Gateway aus.

   Um die Richtlinie auf Verbindungen anzuwenden, die über Citrix Gateway hergestellt wurden, ohne die Citrix Gateway-Richtlinien zu berücksichtigen, lassen Sie die Standardeinträge im AG-Farmnamen und in der Zugriffsbedingung
9. Wenn Sie die Richtlinie auf Verbindungen anwenden möchten, die über Citrix Gateway basierend auf vorhandenen Citrix Gateway-Richtlinien hergestellt werden, gehen Sie wie folgt vor:

   a) Geben Sie im Feld AG-Farmname den Namen des virtuellen Servers ein.
   b) Geben Sie unter Zugriffsbedingung den Namen der Endpoint Analysis Policy oder Session Policy ein.

   > **Wichtig:** Citrix Virtual Desktops validiert den Namen des virtuellen Citrix Gateway-Servers, der Endpoint Analysis-Richtlinie oder der Sitzungsrichtlinie nicht. Stellen Sie sicher, dass die Informationen korrekt sind.
10. Klicken Sie zweimal auf OK, klicken Sie auf Weiter und dann auf Erstellen.

## Hinzufügen des Desktop Delivery Controller als STA

March 27, 2024

Um ICA-Verbindungen mit Citrix Virtual Desktops herzustellen, fügen Sie die IP-Adresse des Desktop Delivery Controller als Secure Ticket Authority (STA) zum virtuellen Server hinzu.

**So fügen Sie über die GUI einen Desktop Delivery Controller als STA hinzu:**

1. Navigieren Sie auf der Registerkarte Konfiguration zu **Citrix Gateway > Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen Server aus und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Veröffentlichte Anwendungen** unter Secure Ticket Authority auf **Hinzufügen**.
4. Geben **Sie im Dialogfeld STA-Server konfigurieren** die URL des STA-Servers ein, und klicken Sie dann auf **Create**.
5. Wiederholen Sie Schritt 4, um weitere STA-Server hinzuzufügen, und klicken Sie dann auf **OK**.

## Konfigurieren von SmartControl

March 27, 2024

Mit SmartControl können Administratoren granulare Richtlinien definieren, um Benutzerumgebungsattribute für Citrix Virtual Apps and Desktops auf Citrix Gateway zu konfigurieren und durchzusetzen. SmartControl ermöglicht es Administratoren, diese Richtlinien von einem einzigen Standort aus zu verwalten, anstatt an jeder Instanz dieser Servertypen.

SmartControl wird durch ICA-Richtlinien auf Citrix Gateway implementiert. Jede ICA-Richtlinie ist eine Kombination aus Ausdruck und Zugriffsprofil, die auf Benutzer, Gruppen, virtuelle Server und global angewendet werden kann. ICA-Richtlinien werden ausgewertet, nachdem sich der Benutzer beim Sitzungsaufbau authentifiziert hat.

In der folgenden Tabelle sind die Attribute der Benutzerumgebung aufgeführt, die SmartControl erzwingen kann:

| | |
|---|---|
| ConnectClientDrives | Gibt die Standardverbindung zu den Clientlaufwerken an, wenn sich der Benutzer anmeldet. |
| ConnectClientLPTPorts | Gibt die automatische Verbindung von LPT-Ports vom Client an, wenn sich der Benutzer anmeldet. LPT-Ports sind die lokalen Druckeranschlüsse. |

|ClientAudioRedirection|Gibt die auf dem Server gehosteten Anwendungen an, um Audio über ein auf dem Clientcomputer installiertes Soundgerät zu übertragen.|
|ClientClipboardRedirection|Spezifiziert und konfiguriert den Zugriff auf die Zwischenablage auf dem Clientgerät und ordnet die Zwischenablage auf dem Server zu.|
|ClientCOMPortRedirection|Gibt die COM-Port-Umleitung zum und vom Client an. COM-Ports sind die Communication-Ports. COM-Ports sind serielle Ports.|
|ClientDriveRedirection|Gibt die Laufwerksumleitung zum und vom Client an.|
|Multistream|Gibt die Multistream-Funktion für bestimmte Benutzer an.|
|ClientUSBDeviceRedirection|Gibt die Umleitung von USB-Geräten zum und vom Client an (nur Workstation-Hosts).|
|`Localremotedata`|Gibt die Funktion zum Hochladen von HTML5-Dateien für die Citrix Workspace-App an.|
|ClientPrinterRedirection|Gibt die Clientdrucker an, die einem Server zugeordnet werden sollen, wenn sich ein Benutzer bei einer Sitzung anmeldet.|
|Richtlinien|Aktion|Zugriffsprofile |
|Hinzufügen|Bearbeiten|Löschen|
|Bindungen anzeigen|Policy Manager|Aktion|

## Richtlinien

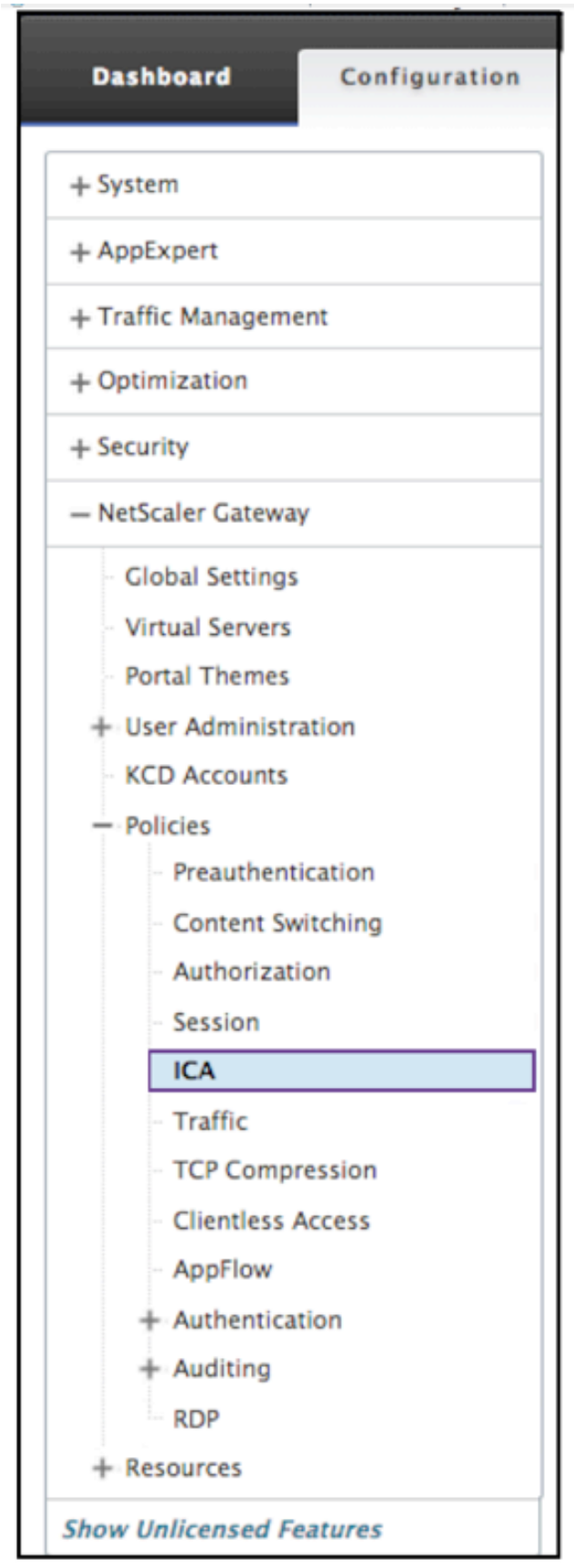
Eine ICA-Richtlinie legt eine Aktion, ein Zugriffsprofil, einen Ausdruck und optional eine Protokollaktion fest. Die folgenden Befehle sind auf der Registerkarte **Richtlinien** verfügbar:

- Hinzufügen
- Bearbeiten
- Löschen
- Bindungen anzeigen
- Policy Manager
- Aktion

### Hinzufügen

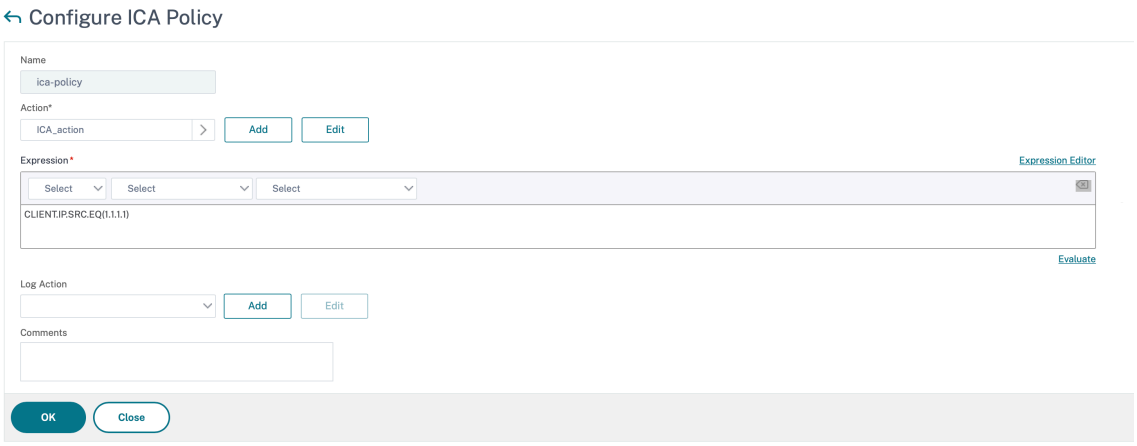
1. Wechseln Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **ICA**.



2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Hinzufügen**.
3. Geben Sie im Dialogfeld**Name**einen Namen für die Richtlinie ein.

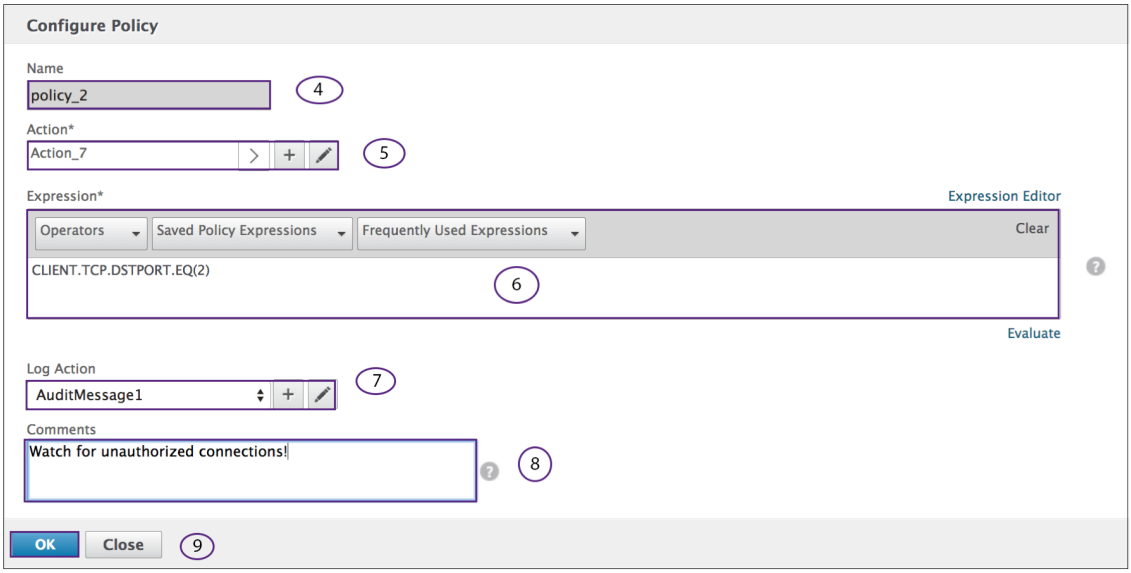



4. Führen Sie neben Action einen der folgenden Schritte aus:
   - Klicken Sie auf das Symbol **>**, um eine bestehende Aktion auszuwählen. Einzelheiten finden Sie unter [Wählen Sie eine Aktion] unter (#common -processes).
   - Klicken Sie auf das **+-Symbol**, um eine Aktion zu erstellen. Einzelheiten finden Sie unter [Neue Aktion erstellen] unter (#common -processes).
   - Das **Stiftsymbol** ist deaktiviert.
5. Erstellen Sie einen Ausdruck.
6. Erstellen Sie eine **Protokollaktion**. Weitere Einzelheiten finden Sie unter Erstellen einer Protokollaktion.
7. Geben Sie eine Nachricht in das Feld Kommentare ein. Der Kommentar schreibt in das Meldungslog. Das Feld ist optional.
8. Klicken Sie auf **Erstellen**.

### Bearbeiten

1. Wechseln Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **ICA**.
2. Wählen Sie die ICA-Richtlinie aus der Liste aus.
3. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Bearbeiten**.
4. Überprüfen Sie den Richtliniennamen.




5. Um die**Aktion**zu überarbeiten, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf das Symbol ****, um eine bestehende**Aktion**zu überarbeiten. Einzelheiten finden Sie unter [Wählen Sie eine Aktion] unter (#common -processes).
   - Klicken Sie auf das **+**, um eine**Aktion**zu erstellen. Einzelheiten finden Sie unter [Neue Aktion erstellen] unter (#common -processes).
   - Klicken Sie auf das **Stiftsymbol**, um das [Access-Profil] zu ändern.
6. Überarbeiten Sie den **Ausdruck** wie gewünscht. Einzelheiten finden Sie unter [Ausdrücke] unter (#common -processes).
7. Um die**Protokollaktion** zu überarbeiten, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf das +, um eine**Protokollaktion**zu erstellen.
   - Klicken Sie auf das **Stiftsymbol**, um eine Audit-Nachricht zu konfigurieren.
8. Überarbeiten Sie die Kommentare wie gewünscht.
9. Klicken Sie auf **OK**.

### Löschen

1. Wechseln Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **ICA**.
2. Wählen Sie die gewünschte ICA-Richtlinie aus der Liste aus.
3. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Löschen**.
4. Bestätigen Sie, dass Sie die Richtlinie löschen möchten, indem Sie auf**Ja**klicken.

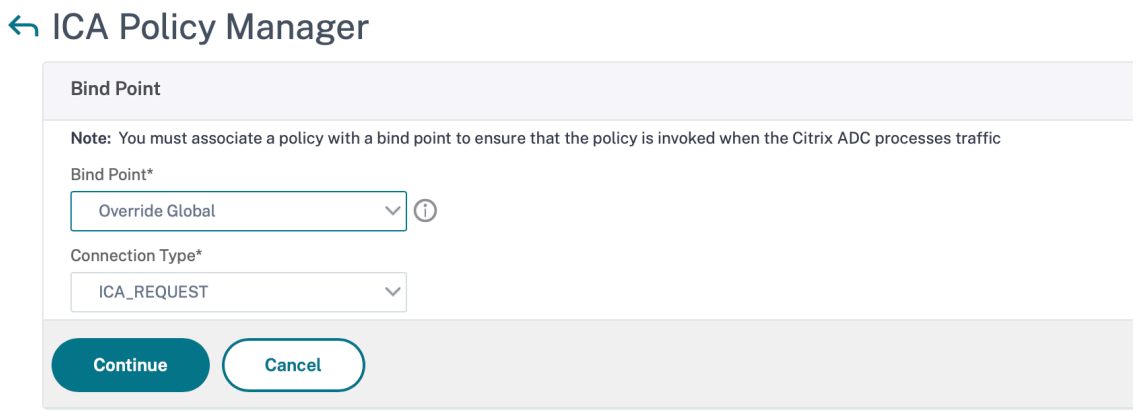
 

### Bindung anzeigen

1. Wechseln Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **ICA**.
2. Wählen Sie die ICA-Richtlinie aus der Liste aus.
3. Klicken Sie im Detailbereich auf der Registerkarte **Richtlinien** auf **Bindungen anzeigen**.

### Policy Manager

1. Wechseln Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **ICA**.
2. Wählen Sie die gewünschte ICA-Richtlinie aus der Liste aus.
3. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Richtlinien-Manager**
4. Wählen Sie im Dialogfeld "**Punkt binden** "eine der folgenden Richtlinien aus.
   - Global überschreiben
   - Virtueller VPN-Server
   - Virtueller Server für Cache-Umleitung
   - Standard Global
5. Wählen Sie im Dialogfeld Verbindungstyp eine Bindungsrichtlinie aus dem Menü aus.
6. Wenn Sie entweder den virtuellen VPN-Server oder den virtuellen Cache-Umleitungsserver auswählen, stellen Sie über das Menü eine Verbindung zum Server her.
7. Klicken Sie auf **Weiter**.

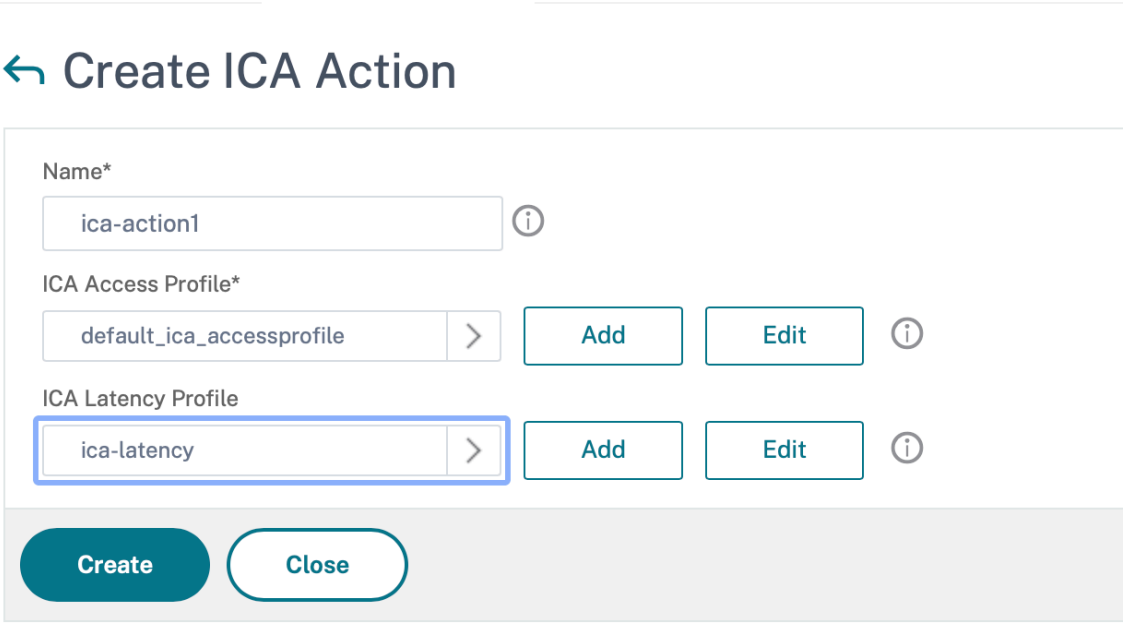



### Bindung hinzufügen

1. Nachdem Sie Weiter ausgewählt haben, wird dieser Bildschirm angezeigt.
2. Wählen Sie eine Richtlinie aus, um die Bindung anzuhängen.

3. Wählen Sie Bindung hinzufügen aus.

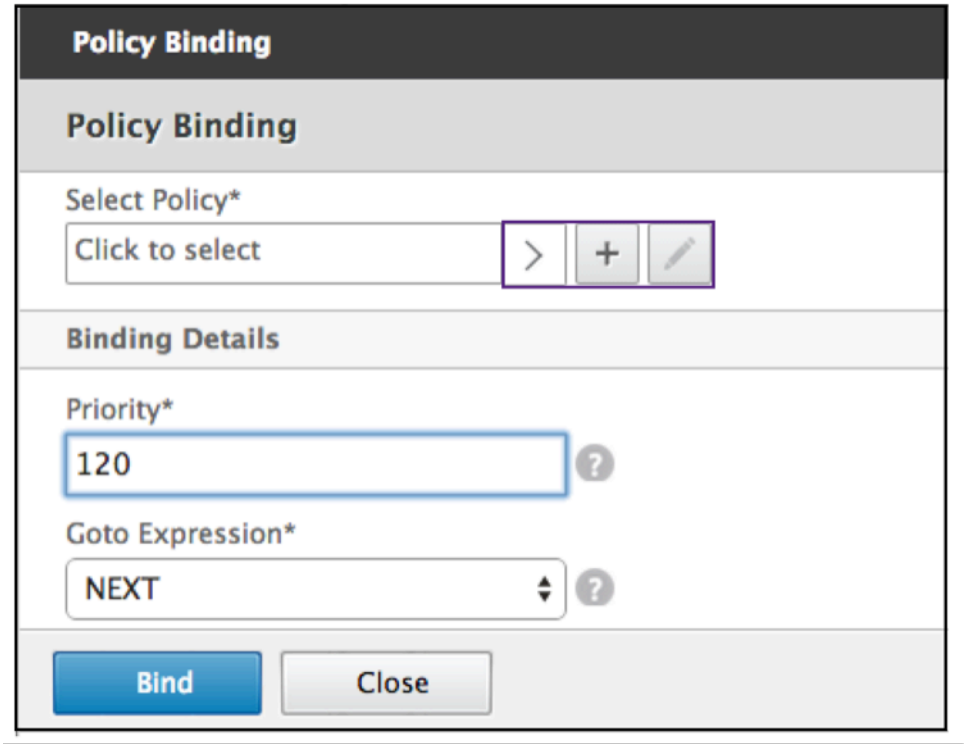



**Verbindliche Richtlinie**

1.Nach Auswahl von Fertig wird dieser Bildschirm angezeigt.

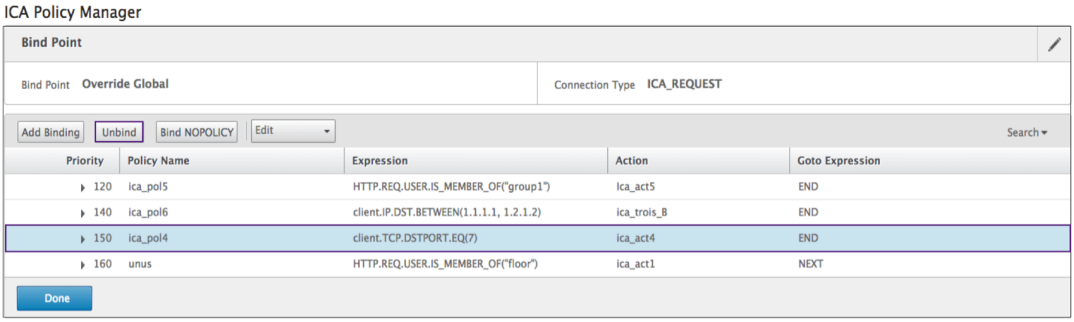
- Klicken Sie auf das Symbol**, um eine bestehende Richtlinie auszuwählen. Einzelheiten findenSie unter Auswählen einer bestehenden Richtlinie.
- Klicken Sie auf das+Symbol, um eine Richtlinie zu erstellen. Einzelheiten finden Sie unterErstellen einer Richtlinie.




**Richtlinie zur Entbindung aufheben**

1. Wählen Sie die Richtlinie aus, die Sie aufheben möchten, und klicken Sie auf die Schaltfläche "**Binden aufheben**".

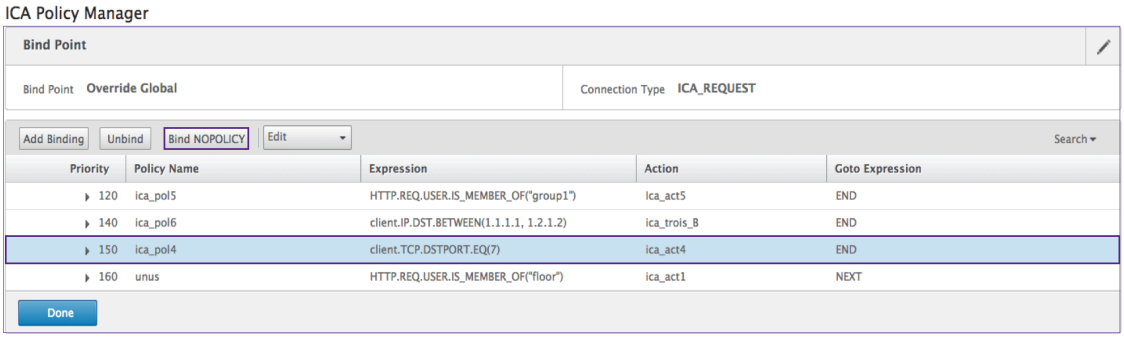



2. Klicken Sie auf **Fertig**.
3. Klicken Sie auf dem Popup-Bildschirm auf die Schaltfläche**Ja**, um zu bestätigen, dass Sie die ausgewählte Entität aufheben möchten.

### Binden Sie NOPOLICY

1. Wählen Sie eine Richtlinie aus, die NOPOLICY erfordert, und klicken Sie auf die Schaltfläche **NOPOLICY binden**.

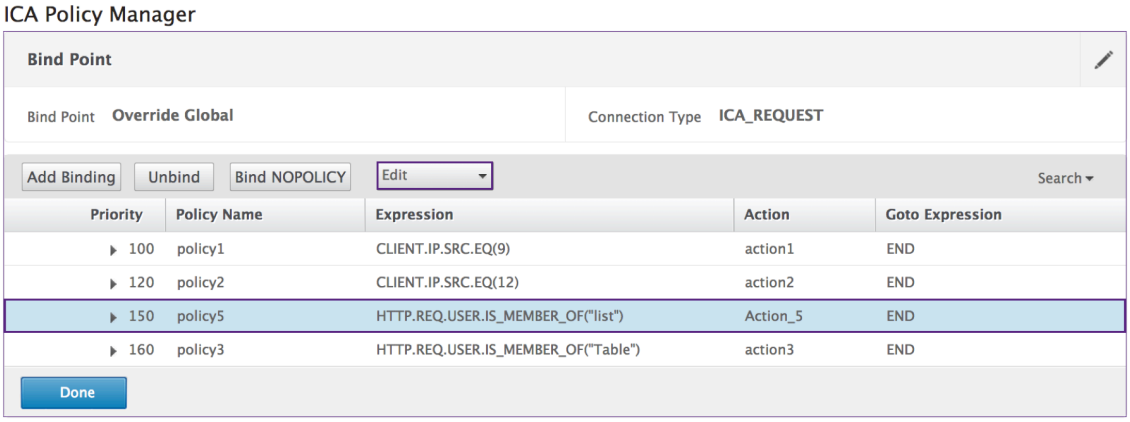



2. Klicken Sie auf **Fertig**.

### Bearbeiten

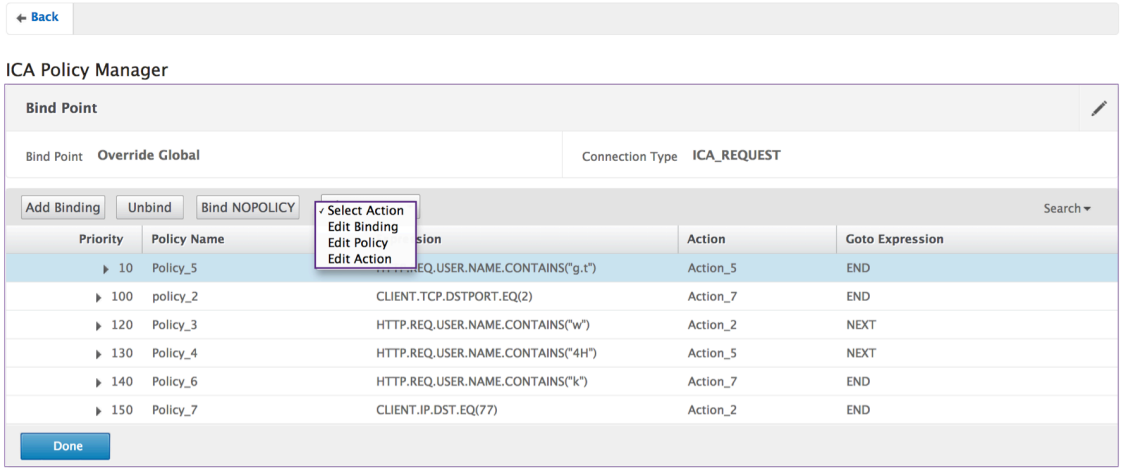
Sie können über den ICA-Richtlinien-Manager bearbeiten.

1. Wählen Sie die Richtlinie aus, die Sie bearbeiten möchten, und wählen Sie **Bearbeiten**aus.



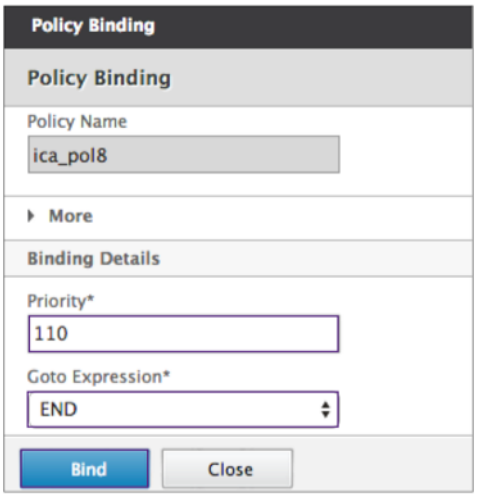

2. Sie können die folgenden Änderungen vornehmen: [Bindung**bearbeiten]**,**[Richtlinie bearbeiten]**,**[Aktion bearbeiten]**.




### Bindung bearbeiten

1. Klicken Sie bei ausgewählter Richtlinie auf **Bindung bearbeiten**.
2. Stellen Sie sicher, dass Sie die gewünschte Richtlinie bearbeiten. Dieser Richtlinienname ist nicht editierbar.



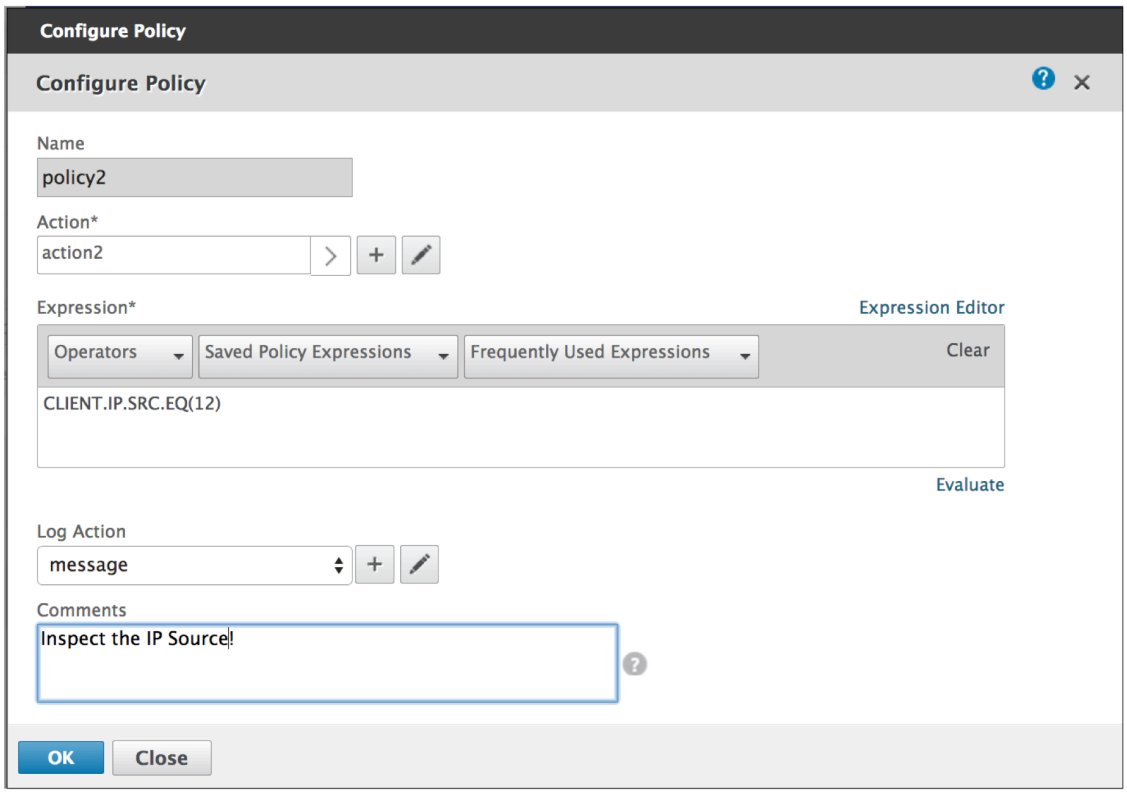

3. Stellen Sie die Priorität wie gewünscht ein.
4. Stellen Sie Gehe zu Ausdruck wie gewünscht ein.
5. Klicken Sie auf die Schaltfläche **Binden**.

### Richtlinie bearbeiten

1. Klicken Sie bei ausgewählter Richtlinie auf **Richtlinie bearbeiten**.

2. Überprüfen Sie den Namen der Richtlinie, um sicherzustellen, dass Sie die gewünschte Richtlinie bearbeiten. Dieses Feld ist nicht editierbar.




3. Führen Sie eine der folgenden Aktionen aus, um die Aktionsrichtlinie zu überarbeiten:

   - Klicken Sie auf das Symbol », um eine bestehende Aktion auszuwählen. Einzelheiten finden Sie unter [Wählen Sie eine Aktion] unter (#common -processes).
   - Klicken Sie auf das **+-Symbol**, um eine Aktion zu erstellen. Einzelheiten finden Sie unter [Neue Aktion erstellen] unter (#common -processes).
   - Klicken Sie auf das **Stiftsymbol**, um das Access-Profil zu überarbeiten. Einzelheiten finden Sie unter [Wählen Sie ein vorhandenes Zugriffsprofil aus] unter (#common -processes).

4. Überarbeiten Sie den Ausdruck wie gewünscht. Weitere Informationen finden Sie unter [Ausdrücke] unter (#common -processes).

5. Wählen Sie im Menü den gewünschten Nachrichtentyp aus. Um eine Protokollaktion zu erstellen, führen Sie einen der folgenden Schritte aus:

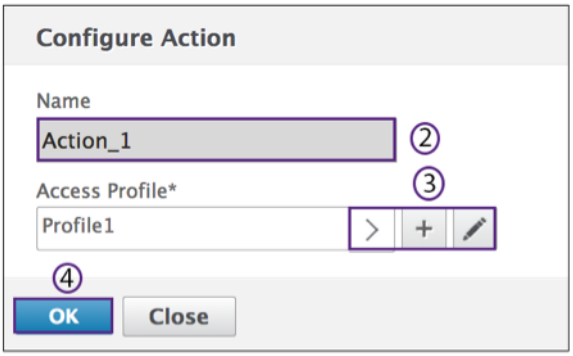
   - Klicken Sie auf das **+-Symbol**, um eine Aktion zu erstellen. Einzelheiten finden Sie unter Erstellen einer Protokollaktion.
   - Klicken Sie auf das **Stiftsymbol**, um die Aktion "Überwachungsnachricht konfigurieren" zu überarbeiten. Einzelheiten finden Sie unter Aktion "Überwachungsnachricht konfigurieren".

6. Geben Sie Kommentare zur ICA-Richtlinie ein.
7. Klicken Sie auf **OK**, wenn die Bearbeitung abgeschlossen ist.

### Aktion bearbeiten

1. Klicken Sie bei ausgewählter Richtlinie auf**Aktion bearbeiten**.
2. Überprüfen Sie den Aktionsnamen, um zu bestätigen, dass Sie die gewünschte Aktion bearbeiten. Dieses Feld ist nicht editierbar.
3. Führen Sie neben Zugriffsprofil einen der folgenden Schritte aus:
   - Klicken Sie auf das**-Symbol, um ein anderes Zugriffsprofil auszuwählen. Einzelheiten finden Sie unterAktion konfigurieren.
   - Klicken Sie auf das Symbol**+**, um ein neues Kanalprofil auszuwählen.Erstellen Sie ein Zugriffsprofil.
   - Klicken Sie auf das **Stiftsymbol**, um das Zugriffsprofil zu überarbeiten. Einzelheiten finden Sie unter [Wählen Sie ein vorhandenes Zugriffsprofil aus] unter (#common -processes).
4. Klicken Sie auf **OK**.

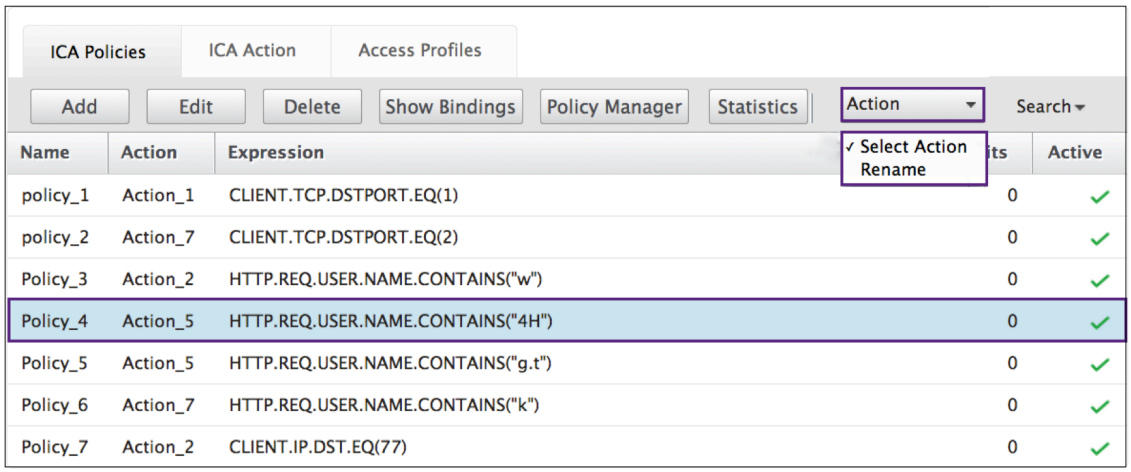



### Aktion

Die Befehle **Richtlinien > Aktion** werden verwendet, um die Aktion umzubenennen.

1. Wählen Sie die gewünschte ICA-Aktion aus der Liste aus.
2. Klicken Sie auf der Registerkarte ICA-Richtlinien auf **Aktion**. Wählen Sie im Menü **Umbenennen** aus.




3. Benennen Sie die Aktion um.
4. Klicken Sie auf **OK**.

### Aktion

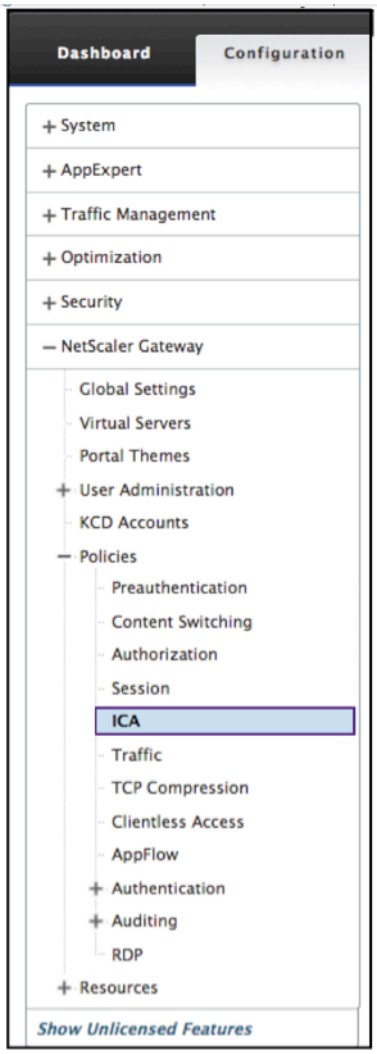
Eine Aktion verbindet eine Richtlinie mit einem Zugriffsprofil. Die folgenden Befehle sind auf der Registerkarte **Richtlinien** verfügbar:

- Hinzufügen
- Bearbeiten
- Löschen
- Aktion

### Hinzufügen

1. Wechseln Sie zu **Citrix Gateway > Aktion** und klicken Sie dann auf **ICA**.

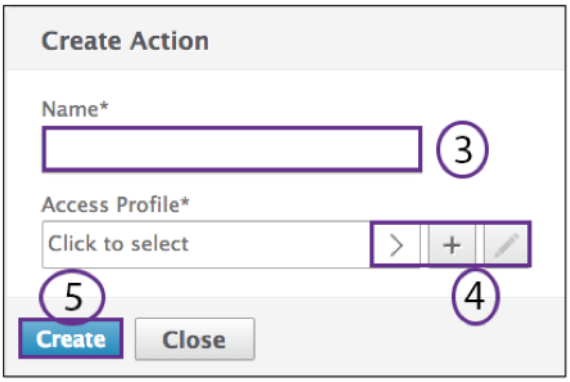



2. Klicken Sie im Detailbereich auf der Registerkarte Aktion auf **Hinzufügen**.

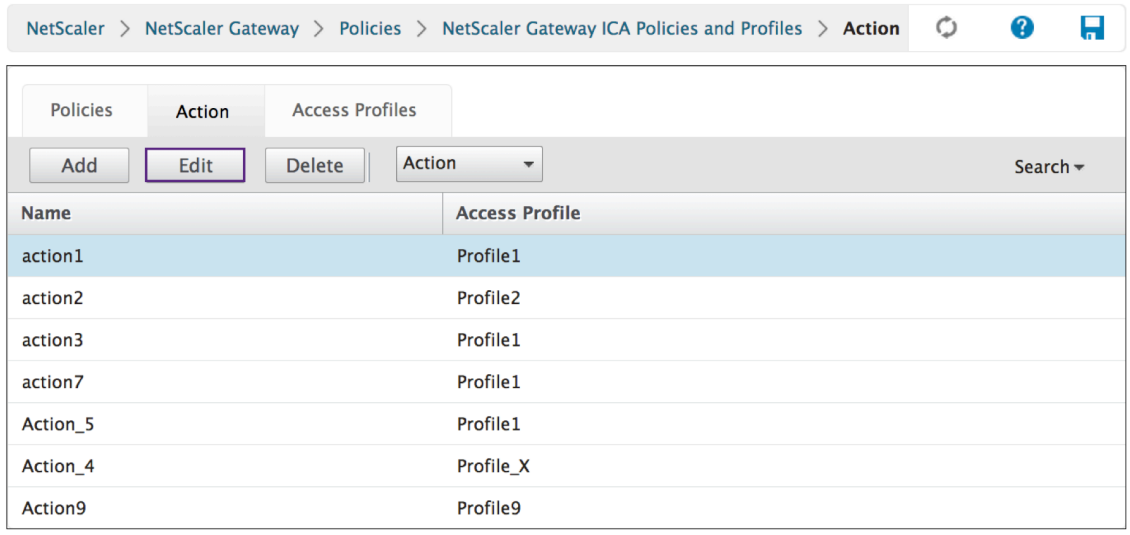
- Klicken Sie auf das Symbol **, um ein vorhandenes Access-Profil auszuwählen. Einzelheiten finden Sie unter [Wählen Sie ein vorhandenes Zugriffsprofil aus] unter (#common -processes).
- Klicken Sie auf das Symbol **+**, um ein Zugriffsprofil zu erstellen. Weitere Informationen finden Sie unter Erstellen eines Zugriffsprofils..
- Das **Stiftsymbol** ist für diesen Bildschirm deaktiviert.

3. Klicken Sie auf **Erstellen**.




### Bearbeiten

1. Wählen Sie die gewünschte ICA-Richtlinie aus der Liste aus.

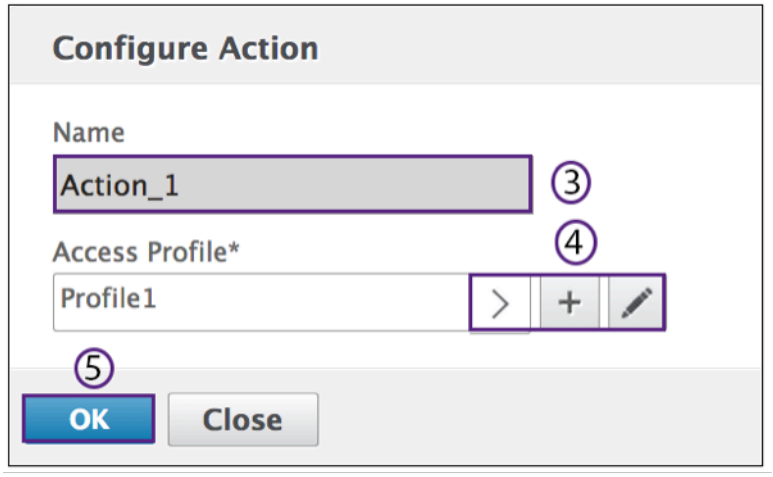



2. Klicken Sie im Detailbereich auf der Registerkarte Aktion auf **Bearbeiten**.

### Aktion konfigurieren

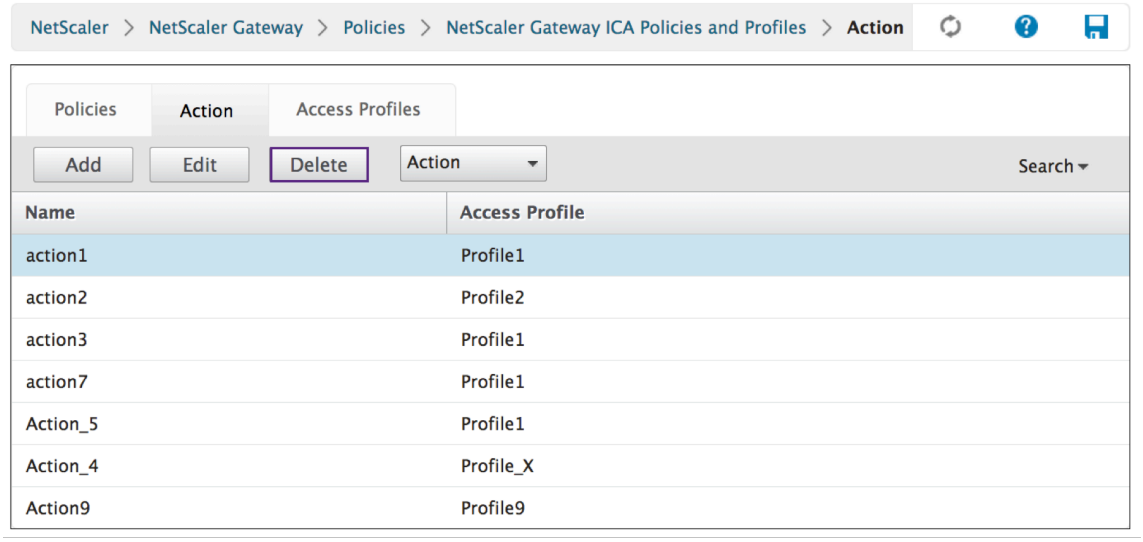
1. Überprüfen Sie den Aktionsnamen, um zu bestätigen, dass Sie die gewünschte Aktion bearbeiten. Dieses Feld ist nicht editierbar.
2. Führen Sie neben Zugriffsprofil einen der folgenden Schritte aus:
   - Klicken Sie auf **>**, um ein vorhandenes Zugriffsprofil auszuwählen. Einzelheiten finden Sie unter [Wählen Sie ein vorhandenes Zugriffsprofil aus] unter (#common -processes).
   - Klicken Sie auf das **+**, um ein Zugriffsprofil zu erstellen. Weitere Informationen finden Sie unter Erstellen eines Zugriffsprofils.
   - Klicken Sie auf das **Stiftsymbol**, um Zugriffsprofil zu konfigurieren
3. Klicken Sie auf **OK**.




### Löschen

1. Wechseln Sie zu **Citrix Gateway > Aktion** und klicken Sie dann auf **ICA**.
2. Wählen Sie die gewünschte ICA-Aktion aus der Liste aus.
3. Klicken Sie im Detailbereich auf der Registerkarte Aktion auf **Löschen**.

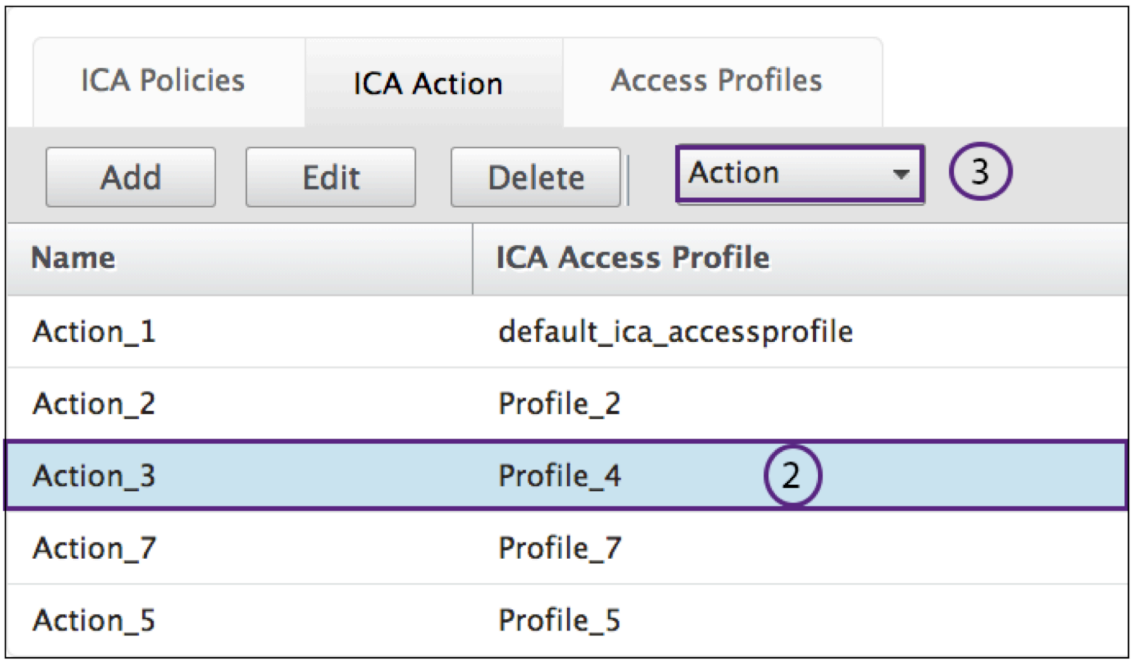



4. Bestätigen Sie die Aktion, mit der Sie die Richtlinie löschen möchten, indem Sie auf **Ja** klicken.

### Aktion

Die Befehle **ICA-Aktion > Aktion** werden verwendet, um die Aktion umzubenennen.

1. Wechseln Sie zu **Citrix Gateway > Aktion** und klicken Sie dann auf **ICA**.
2. Wählen Sie die gewünschte ICA-Aktion aus der Liste aus.
3. Klicken Sie im Detailbereich auf der Registerkarte Aktion auf **Aktion**.




4. Wählen Sie im Menü **Aktion > Umbenennen**.

5. Benennen Sie die Aktion um.
6. Klicken Sie auf **OK**.

#### Zugriff auf Profile

Ein ICA-Profil definiert die Einstellungen für Benutzerverbindungen.

Zugriffsprofile geben die Aktionen an, die auf die Citrix Virtual Apps and Desktops Umgebungs-ICA eines Benutzers angewendet werden, wenn das Benutzergerät die Bedingungen für den Richtlinienausdruck erfüllt. Sie können die GUI verwenden, um ICA-Profile getrennt von einer ICA-Richtlinie zu erstellen und das Profil dann für mehrere Richtlinien zu verwenden. Sie können nur ein Profil mit einer Richtlinie verwenden.

Sie können Zugriffsprofile unabhängig von einer ICA-Richtlinie erstellen. Wenn Sie die Richtlinie erstellen, können Sie das Zugriffsprofil auswählen, das an die Richtlinie angehängt werden soll. Ein Zugriffsprofil gibt die Ressourcen an, die einem Benutzer zur Verfügung stehen. Die folgenden Befehle sind auf der Registerkarte **Richtlinien** verfügbar:

- Hinzufügen
- Bearbeiten
- Löschen

### Erstellen eines Zugriffsprofils mit der GUI

1. Wechseln Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **ICA**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Zugriffsprofile** und dann auf **Hinzufügen**.
3. Konfigurieren Sie die Einstellungen für das Profil, klicken Sie auf Erstellen und dann auf **Schließen**. Nachdem Sie ein Profil erstellt haben, können Sie es in eine ICA-Richtlinie aufnehmen.

### Hinzufügen eines Zugriffsprofils zu einer Richtlinie über die GUI

1. Wechseln Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **ICA**.
2. Führen Sie auf der Registerkarte Richtlinien eine der folgenden Aktionen aus:
    - Klicke auf **Hinzufügen**, um eine ICA-Richtlinie zu erstellen
    - Wählen Sie eine Richtlinie aus und klicken Sie dann auf **Öffnen**.
3. Wählen Sie im Menü **Aktion** ein Zugriffsprofil aus der Liste aus.

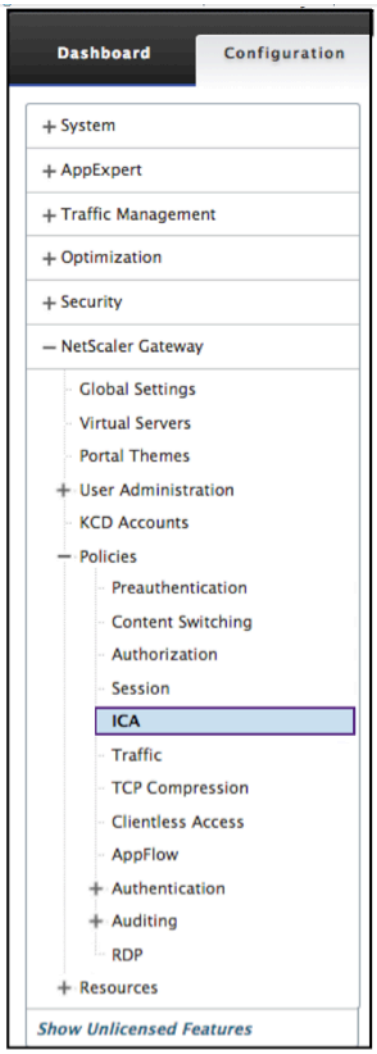
4. Beenden Sie die Konfiguration der ICA-Richtlinie und führen Sie dann einen der folgenden Schritte aus:

   a) Klicken Sie auf **Erstellen** und dann auf **Schließen**, um die Richtlinie zu erstellen.

   1.Klicken Sie auf **OK** und dann auf **Schließen**, um die Richtlinie zu ändern.

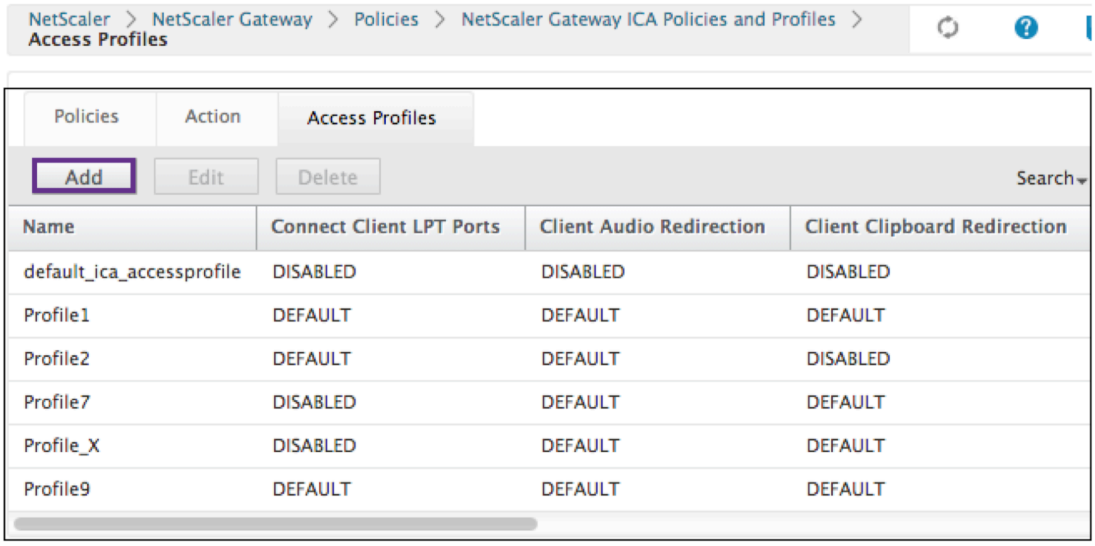
## Hinzufügen

1. Wechseln Sie zu **Citrix Gateway > Richtlinien** und klicken Sie dann auf **ICA**.

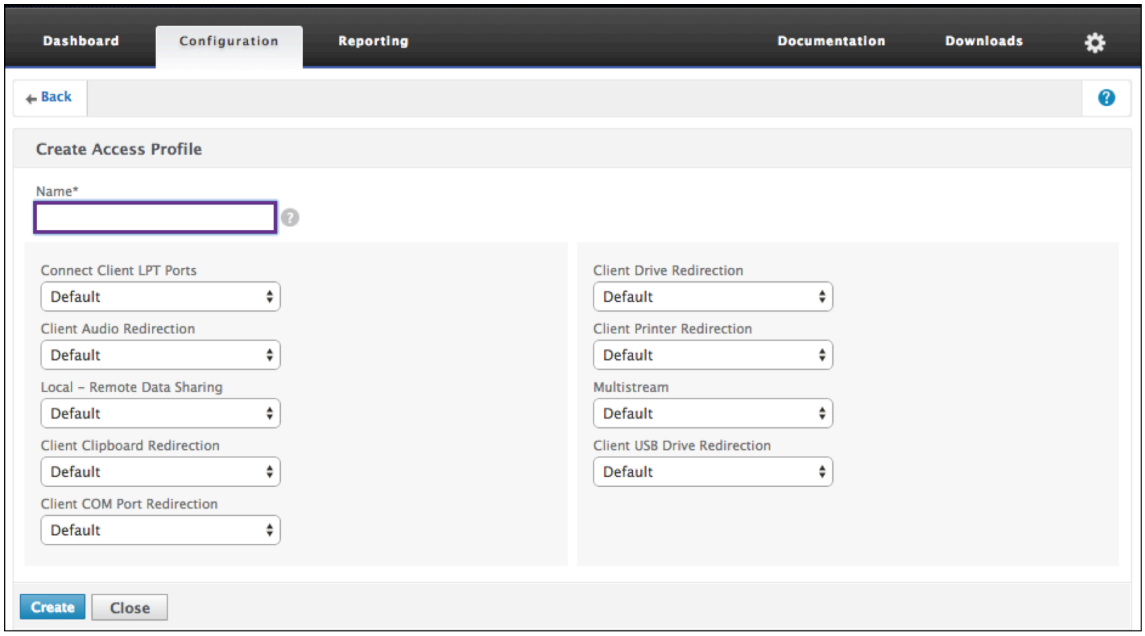



2. Klicken Sie im Detailbereich auf der Registerkarte Zugriffsprofile auf**Hinzufügen**.**




3. Geben Sie unter Name einen Namen für das Zugriffsprofil ein.

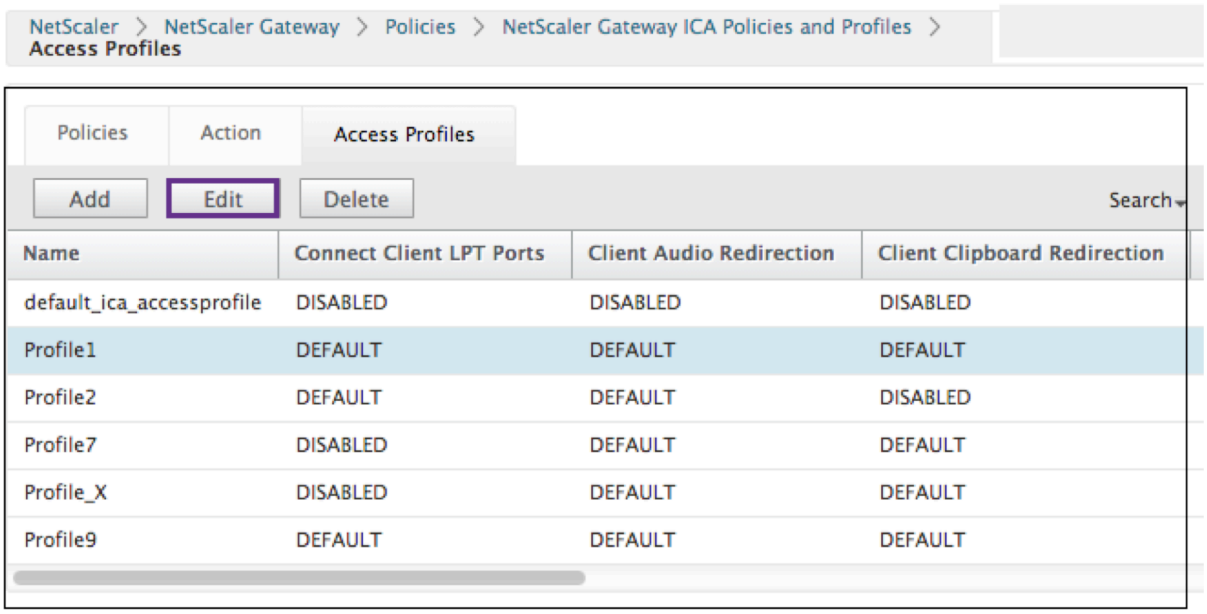



4. Wählen Sie in den angezeigten Menüs Standard oder Deaktivieren aus, um das Zugriffsprofil zu erstellen.
5. Klicken Sie auf **Erstellen**.

## Bearbeiten

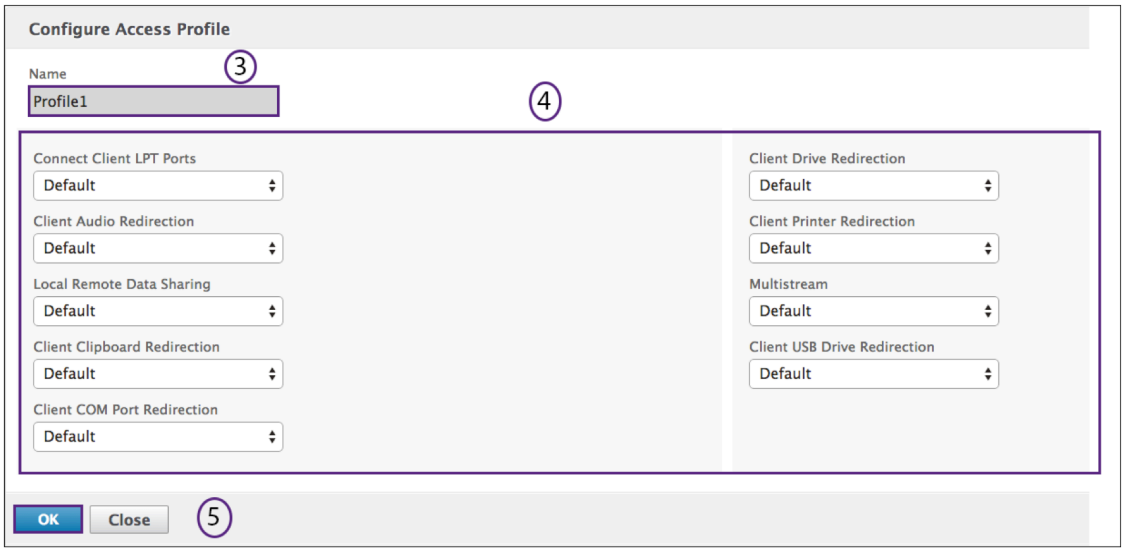
1. Wählen Sie das Zugriffsprofil aus, das Sie bearbeiten möchten.
2. Klicken Sie im Detailbereich auf der Registerkarte Zugriffsprofile auf **Bearbeiten**.




## Konfigurieren von Zugriffsprofil

1. Stellen Sie sicher, dass der **Name** derjenige ist, den Sie überarbeiten möchten.



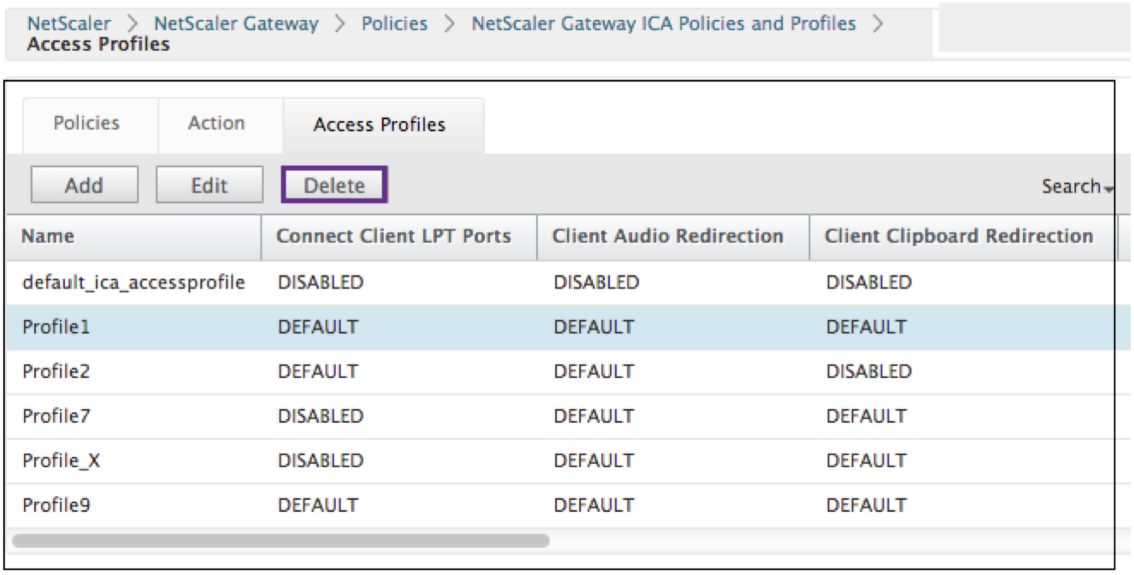

2. Wählen Sie im Menü **Standard** oder **Deaktivieren** aus, um nach Bedarf zu konfigurieren.
3. Klicken Sie auf **OK**.

## Löschen

1. Gehen Sie zu **Citrix Gateway > Action**, und klicken Sie dann auf **ICA**.

2. Wählen Sie die gewünschte ICA-Aktion aus der Liste aus.
3. Klicken Sie im Detailbereich auf der Registerkarte **Aktion** auf **Löschen**.



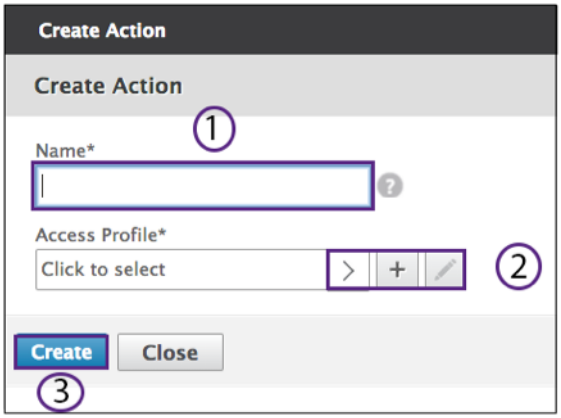

4. Bestätigen Sie das Zugriffsprofil, das Sie löschen möchten, indem Sie auf **Ja**klicken.

## Gängige Verfahren

### Erstellen Sie eine Aktion

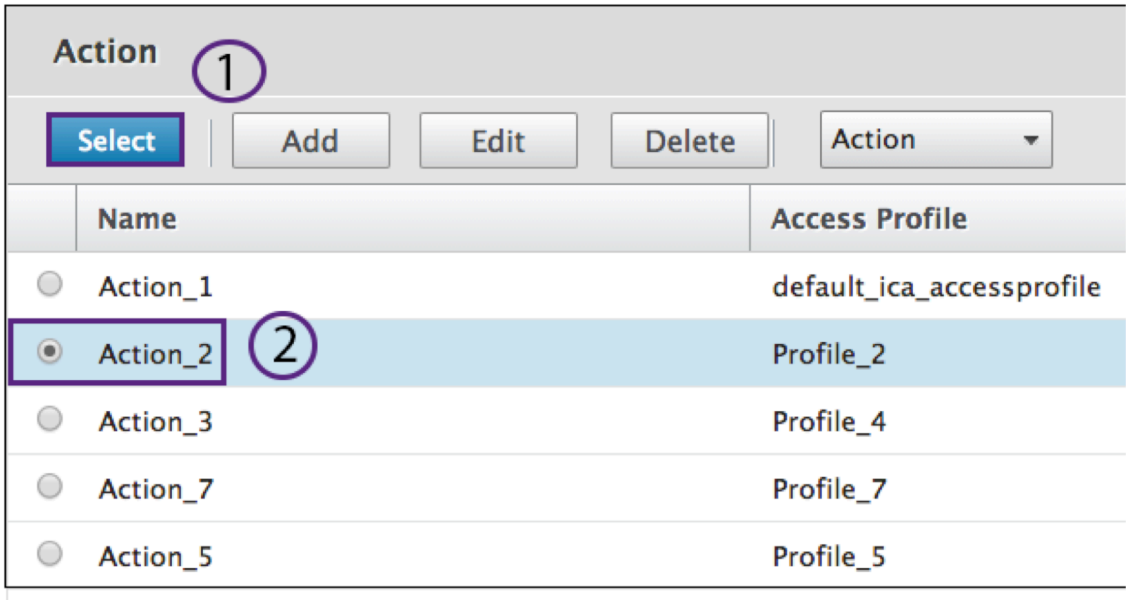
1. Geben Sie einen Namen für die Aktion ein.
2. Wählen Sie eine der folgenden Optionen aus, um das Zugriffsprofil bereitzustellen:
   - Klicken Sie auf >, um ein vorhandenes Zugriffsprofil auszuwählen. Einzelheiten finden Sie unter [Wählen Sie ein vorhandenes Zugriffsprofil aus] unter (#common -processes).
   - Klicken Sie auf +, um ein Zugriffsprofil zu erstellen. Einzelheiten finden Sie unter Erstellen eines Zugriffsprofils.
   - Das **Stiftsymbol** ist deaktiviert.
3. Klicken Sie auf **Erstellen**.




**Wählen Sie eine Aktion**

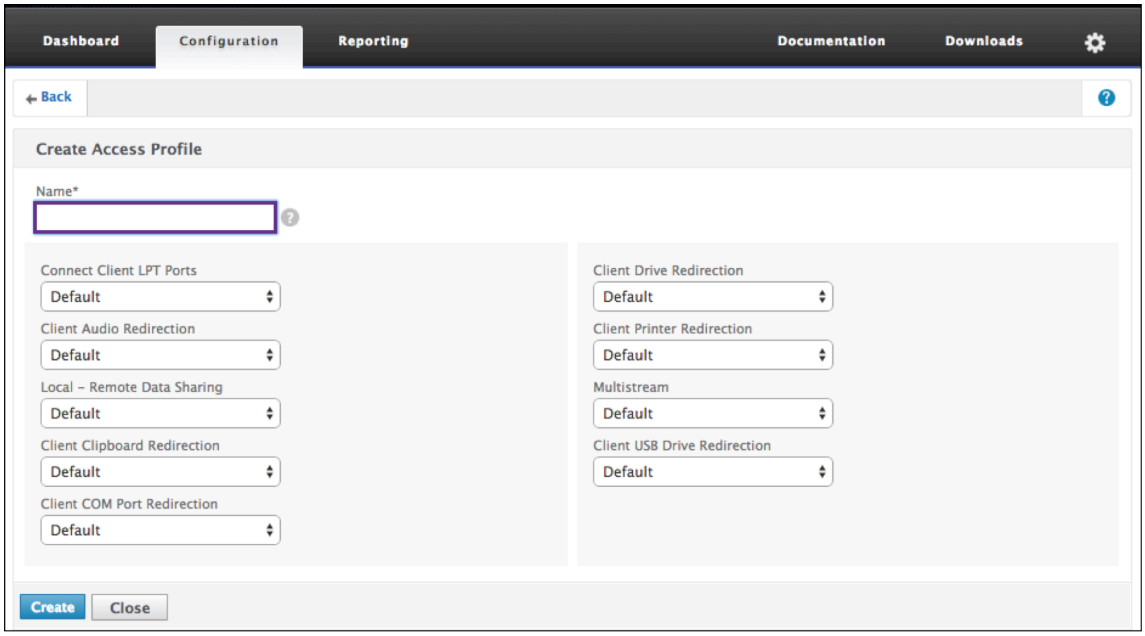
1. Wählen Sie eine Aktion aus, indem Sie auf das Optionsfeld links davon klicken.Das zugehörige Zugriffsprofil gibt die erlaubten Benutzerfunktionen an.
2. Klicken Sie auf die Schaltfläche **Auswählen**.




**Erstellen Sie ein Zugriffsprofil**

1. Nennen Sie das Zugriffsprofil.

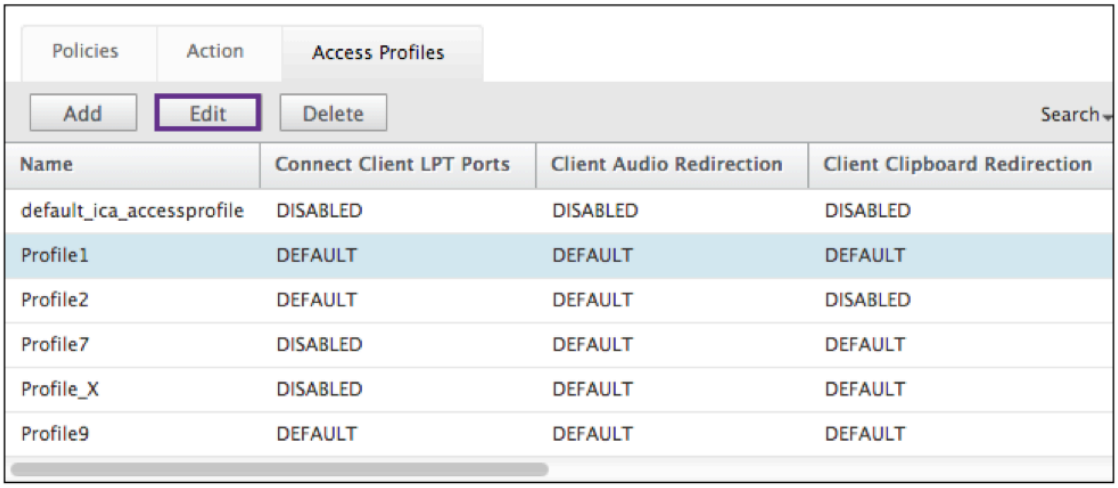
 




2. Sie können das Zugriffsprofil über dieses Menü konfigurieren.
3. Klicken Sie auf **Erstellen**.

### Wählen Sie ein vorhandenes Zugriffsprofil

1. Wählen Sie ein Zugriffsprofil aus, indem Sie darauf klicken.




2. Klicken Sie auf Bearbeiten.
3. Konfigurieren Sie das Zugriffsprofil. Einzelheiten finden Sie unter Konfigurieren des Zugriffsprofils.

**Ausdrücke**

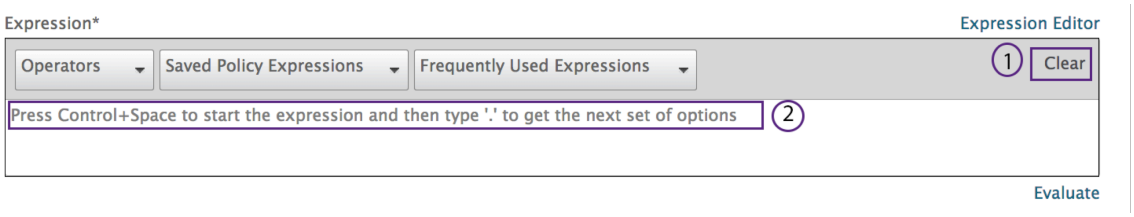
1. Um einen vorhandenen Ausdruck zu erstellen oder zu überarbeiten, wählen Sie **Löschen**aus.

   Die Ausdrücke sind die typischen ICA-Ausdrücke. Für die HTTP-Ausdrücke geben Sie den Namen mit dem “”ein und entfernen Sie die ().

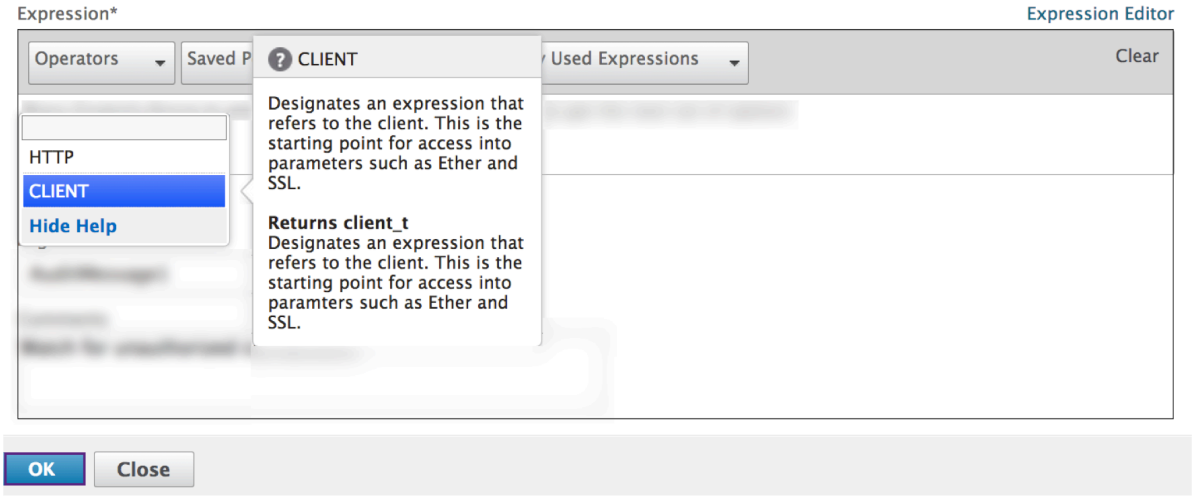
| | |
|---|---|
| ICA.SERVER.PORT | Dieser Ausdruck überprüft, ob der angegebene Port mit der Portnummer auf den Citrix Virtual Apps and Desktops übereinstimmt, die der Benutzer zu verbinden versucht. |
| ICA.SERVER.IP | Dieser Ausdruck überprüft, ob die angegebene IP mit der IP-Adresse auf den Citrix Virtual Apps and Desktops übereinstimmt, die der Benutzer zu verbinden versucht. |
| AAA.USER.IS_MEMBER_OF(“”).NOT | Dieser Ausdruck prüft, ob auf die aktuelle Verbindung von einem Benutzer zugegriffen wird, der KEIN Mitglied des angegebenen Gruppennamens ist. |
| AAA.USER.IS_MEMBER_OF(“group name”) | Dieser Ausdruck prüft, ob der Benutzer, der auf die aktuelle Verbindung zugreift, Mitglied der angegebenen Gruppe ist. |
| AAA.USER.NAME.CONTAINS(“”).NOT | Dieser Ausdruck prüft, ob der Benutzer, der auf die aktuelle Verbindung zugreift, KEIN Mitglied der angegebenen Gruppe ist. |
| AAA.USER.NAME.CONTAINS(“enter user name”) Gibt die Ressourcen für einen Benutzernamen an. | Dieser Ausdruck prüft, ob mit dem angegebenen Namen auf die aktuelle Verbindung zugegriffen wird. |
| CLIENT.IP.DST.EQ(geben Sie hier die IP-Adresse ein).NOT | Dieser Ausdruck prüft, ob die Ziel-IP des aktuellen Datenverkehrs NICHT der angegebenen IP-Adresse entspricht. |
| CLIENT.IP.DST.EQ(enter the IP address here) | Dieser Ausdruck prüft, ob die Ziel-IP des aktuellen Datenverkehrs der angegebenen IP-Adresse entspricht. |
| CLIENT.TCP.DSTPORT.EQ (enter port number).NOT | Dieser Ausdruck prüft, ob der Zielport NICHT der angegebenen Portnummer entspricht. |
| CLIENT.TCP.DSTPORT.EQ (enter port number) | Dieser Ausdruck prüft, ob der Zielport der angegebenen Portnummer entspricht. |

2. Gleichzeitig wählen Sie **Control** und die **Leertaste**. Dann sind Ihre Optionen sichtbar.




3. Geben Sie den Zeitraum ein. Treffen Sie Ihre Auswahl und drücken Sie die **Leertaste**.
4. Geben Sie für jede Periode des Ausdrucks in der vorherigen Tabelle den Zeitraum ein. Treffen Sie Ihre Auswahl und drücken Sie die Leertaste.
5. Klicken Sie auf **OK**.



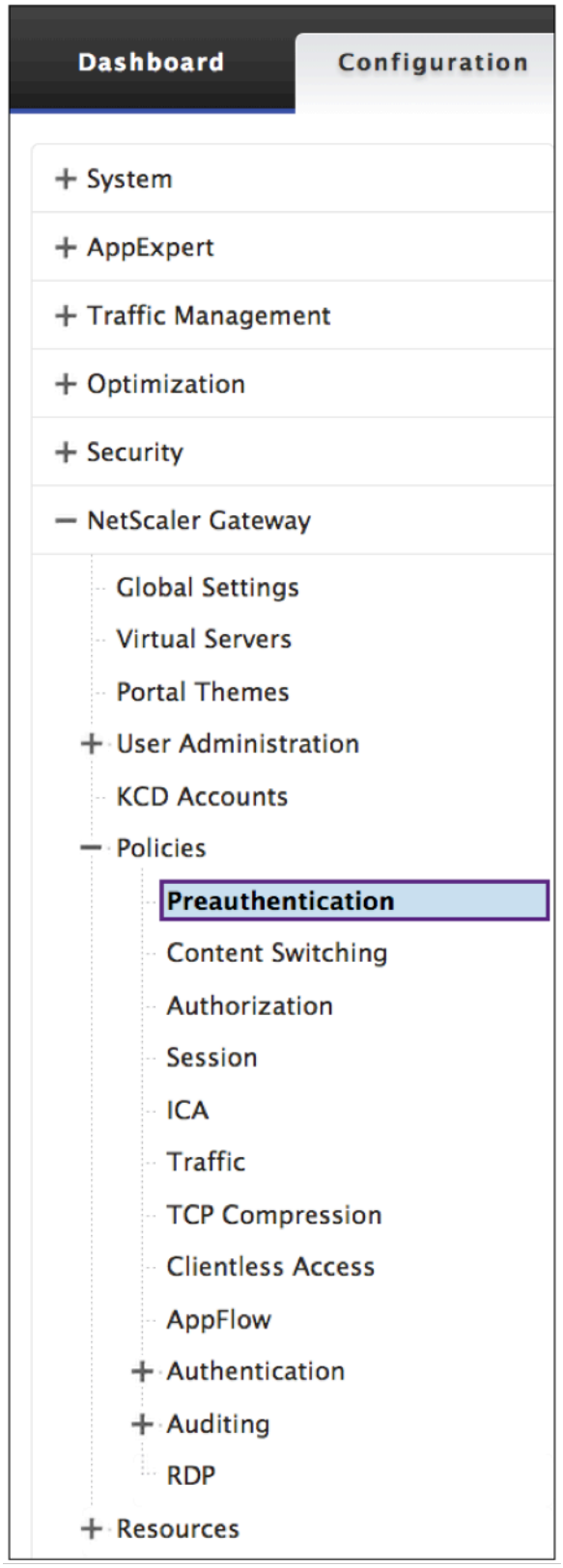

### Identifikation von Gruppen

Die Vorauthentisch- oder Sitzungsfunktionen definieren den Ausdruck mit einer Gruppennamenvariablen.

### Vorauthentifizierung

1. Wählen Sie im Konfigurationsbereich Vorauthentifizierung aus.

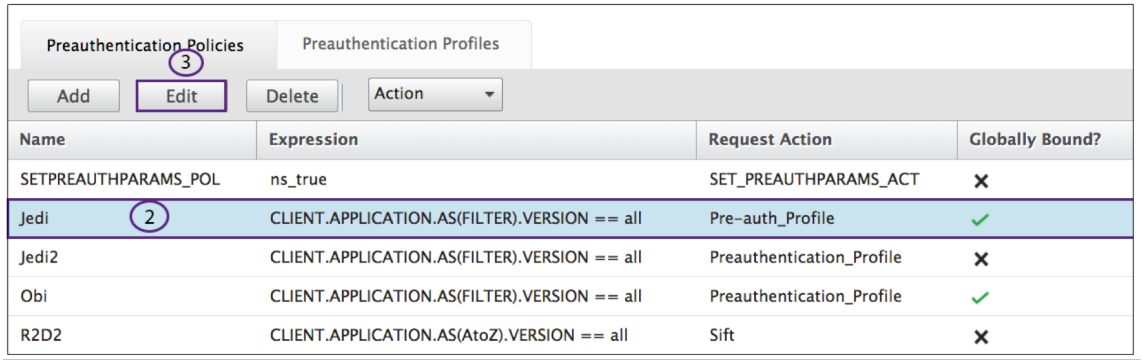
 



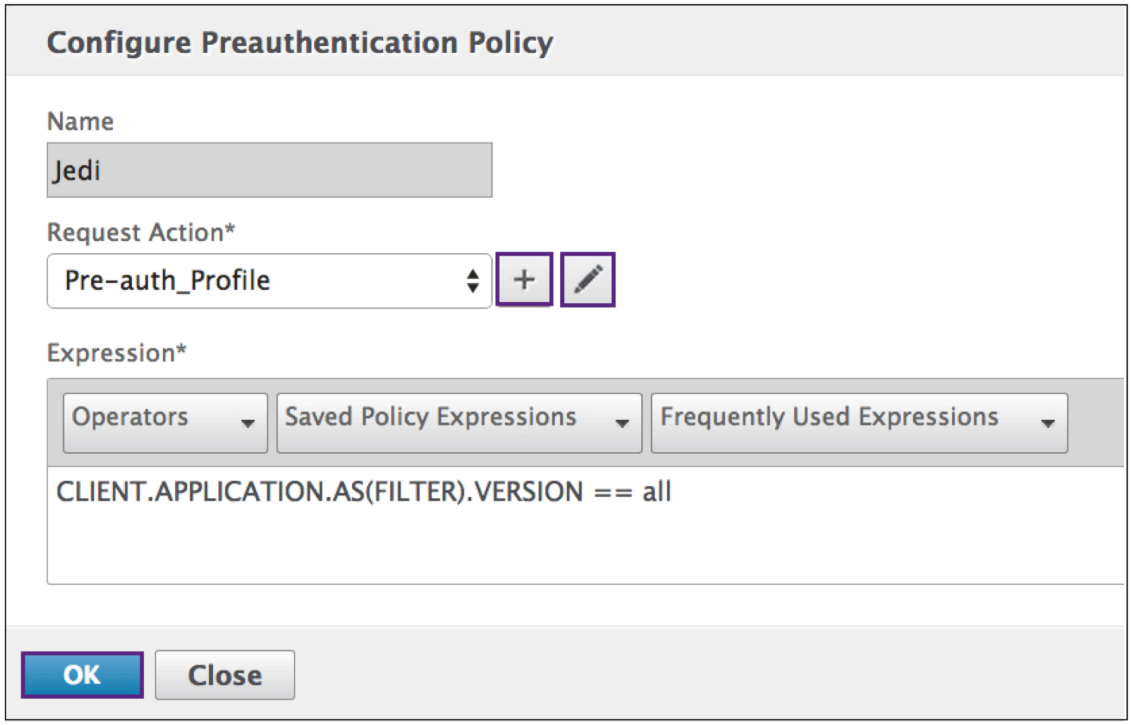

1. Wählen Sie einen Namen aus den Vorauthentifizierungsrichtlinien aus.

2. Wählen Sie auf der Registerkarte Vorauthentifizierungsrichtlinien die **Option Bearbeiten** aus.

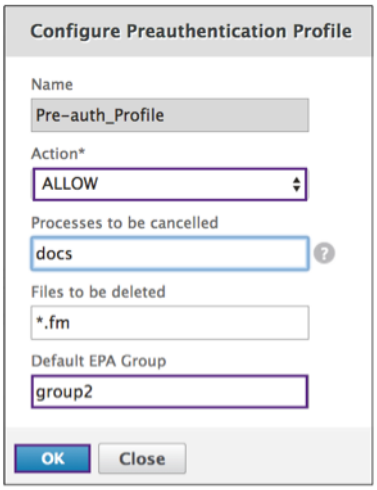



3. Wählen Sie das **Stiftsymbol** oder **+** neben dem Dialogfeld "Aktion anfordern".




4. Definieren Sie die ("<groupname>") im Dialogfeld Default EPA Group.

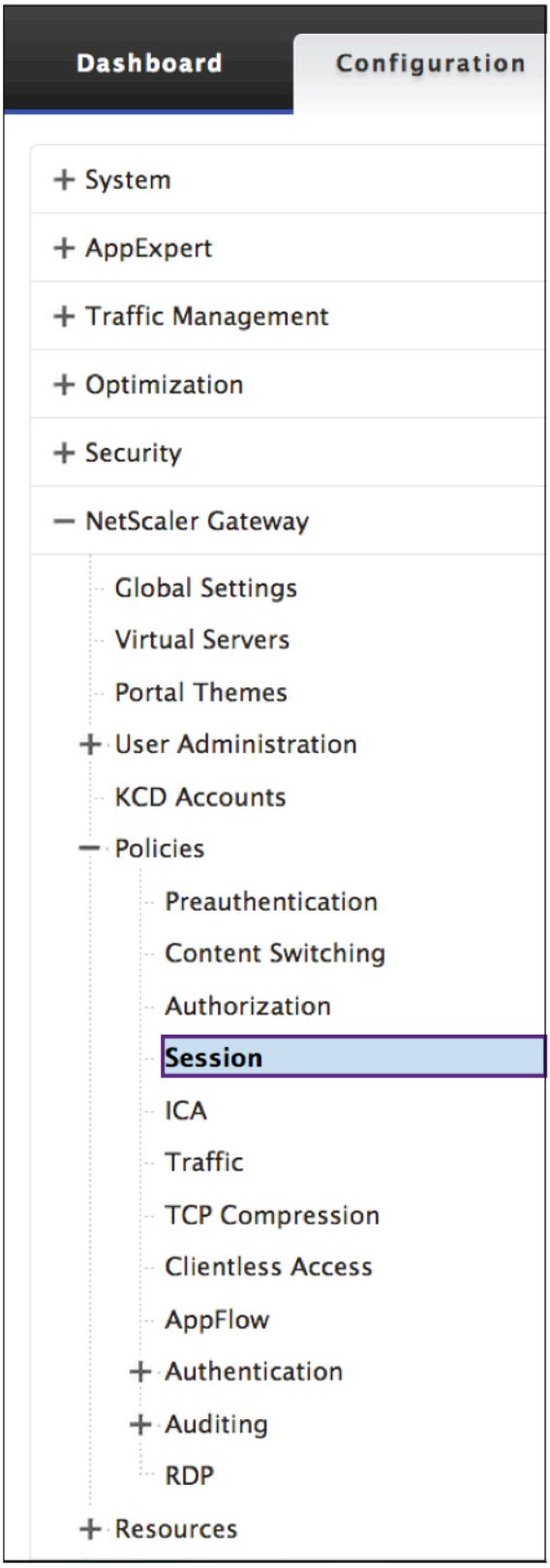
 




## Sitzungsfortbestehen

1. Wählen Sie im Konfigurationsbereich **Sitzung** aus.

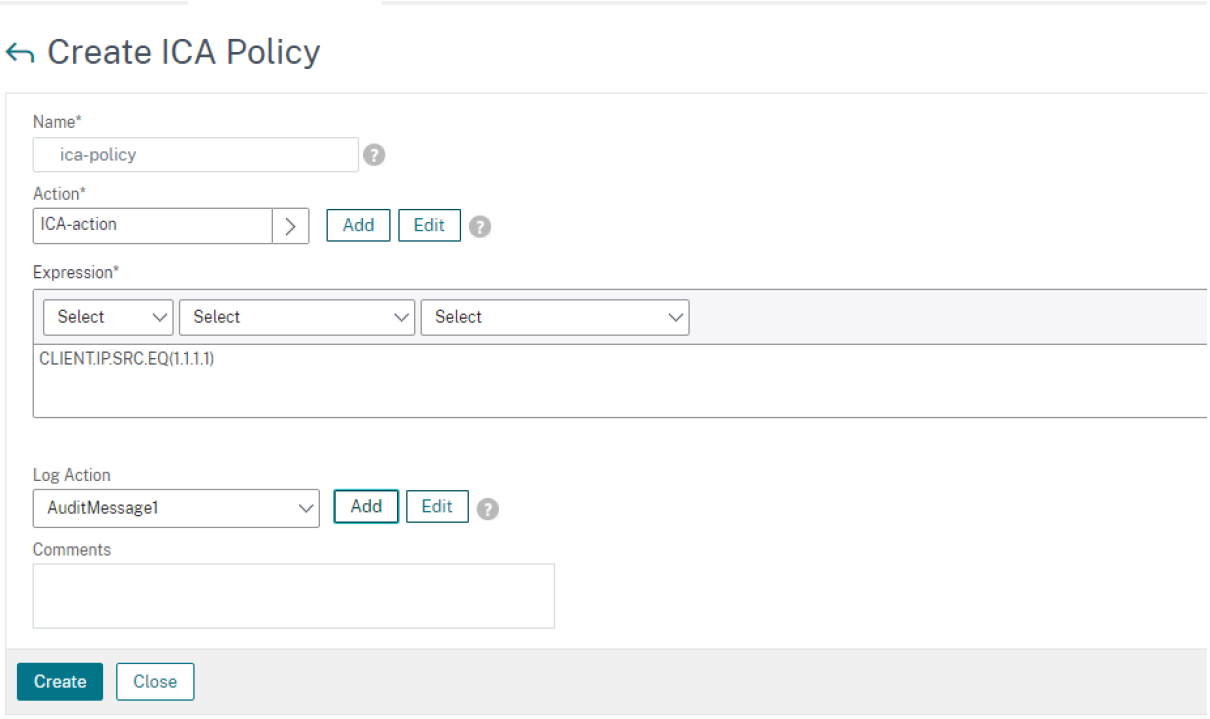
 



### Erstellen einer Protokollaktion

1. Wählen **Sie im Bildschirm "Richtlinie konfigurieren** "neben dem Dialogfeld "**Aktion protokollieren** "das Symbol **+**.




### Aktion "Überwachungsnachricht erstellen"

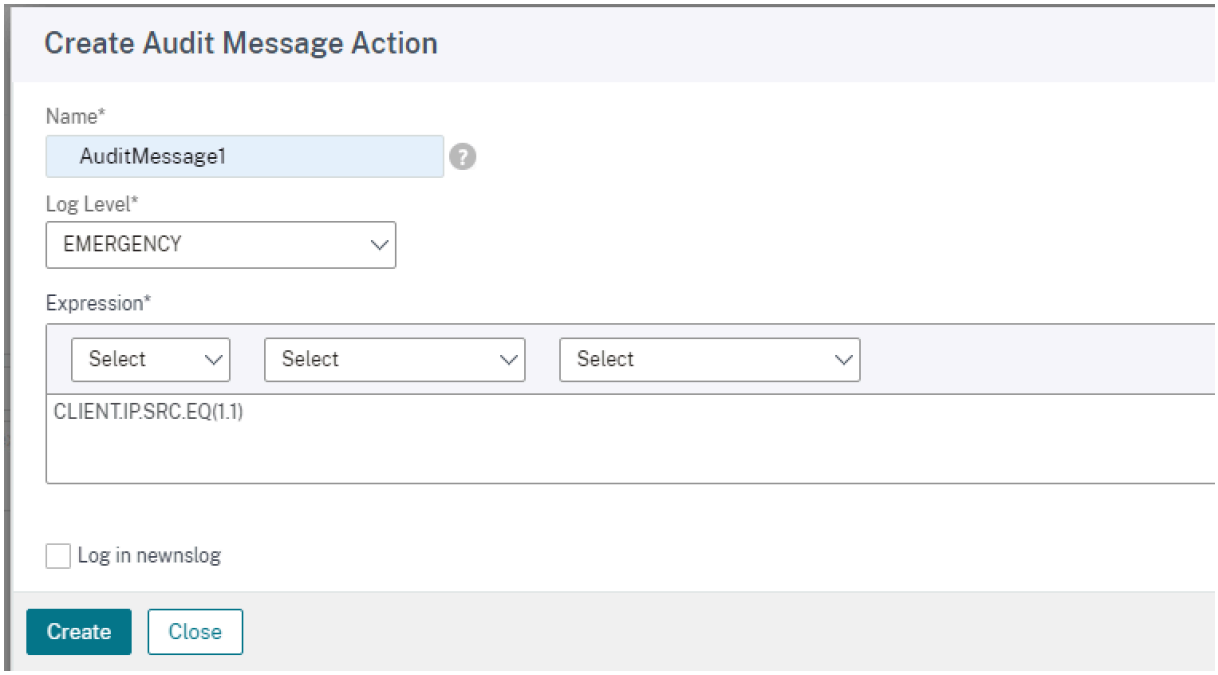
1. Der Bildschirm **Aktion "Audit-Nachricht erstellen** "wird angezeigt. Nennen Sie die Audit-Nachricht. Die Audit-Nachricht akzeptiert nur Zahlen, Buchstaben oder einen Unterstrich.
2. Geben Sie im Menü das Audit-Log Level an.

| | |
|---|---|
| Notfall | Ereignisse, die auf eine unmittelbare Krise auf dem Server hindeuten. |
| Warnung | Ereignisse, die möglicherweise Maßnahmen erfordern. |
| Kritisch | Ereignisse, die auf eine bevorstehende Serverkrise hindeuten. |
| Fehler | Ereignisse, die auf eine Art von Fehler hinweisen. |
| Warnung | Ereignisse, die bald Maßnahmen erfordern. |

| | |
|---|---|
| Beachten | Ereignisse, über die der Administrator Bescheid wissen muss. |
| Zur Information | Alle außer Low-Level-Events. |
| Debuggen | Alle Ereignisse bis ins kleinste Detail. |

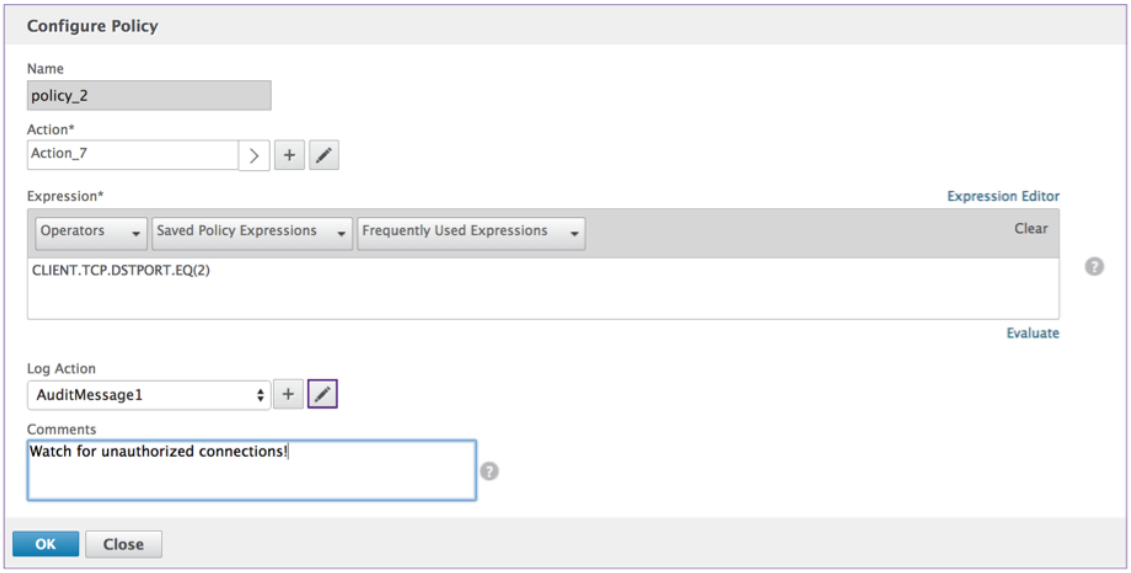
1. Geben Sie einen Ausdruck ein. Der Ausdruck definiert das Format und den Inhalt des Protokolls.
2. Die Kontrollkästchen.
   - Überprüfen Sie das Login `newnslog`, um die Nachricht an ein neues ns-Protokoll zu senden.
   - Wählen Sie **Sicherheitscheck** umgehen, um die Sicherheitsüberprüfung zu umgehen. Dies ermöglicht unsichere Ausdrücke.
3. Klicken Sie auf **Erstellen**.




### Überarbeiten einer Protokollaktion

1. Klicken Sie im Bildschirm Richtlinie konfigurieren neben dem Dialogfeld Aktion protokollieren auf das Symbol.

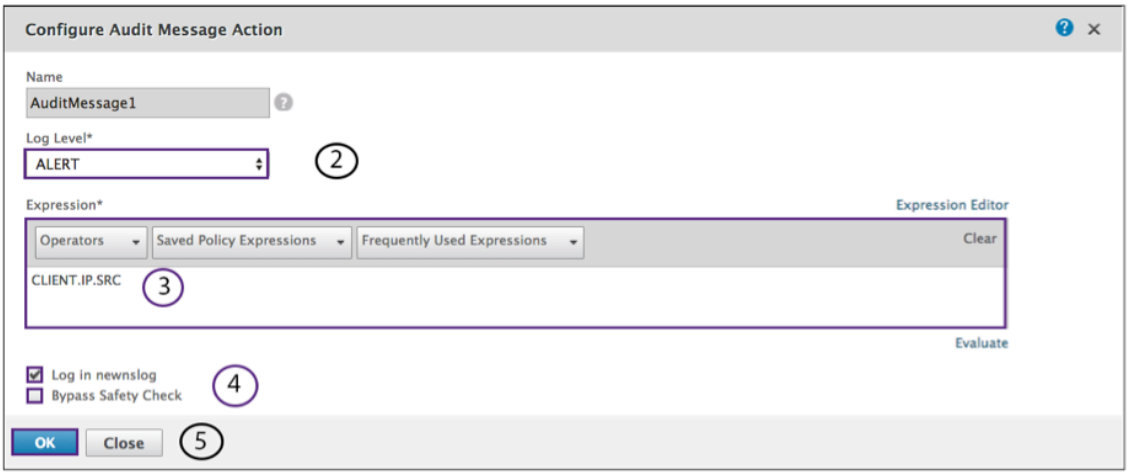
 




### Aktion "Überwachungsnachricht konfigurieren"

Das Folgende sind bearbeitbare Felder:

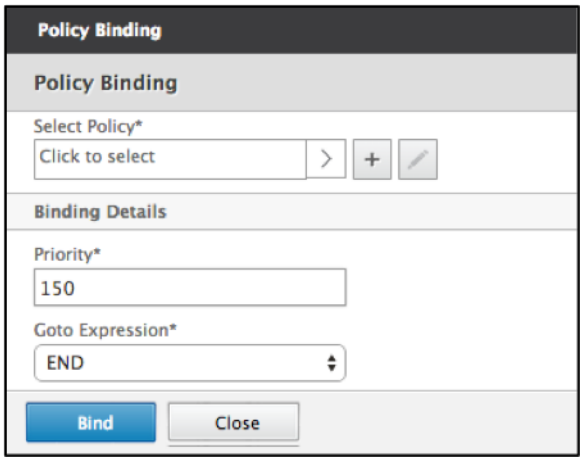
1. Geben Sie im Menü das Audit-Log Level an.
2. Geben Sie einen Ausdruck ein. Der Ausdruck definiert das Format und den Inhalt des Protokolls.
3. Die Kontrollkästchen:
   - Überprüfen Sie das Anmelden `newnslog`, um die Nachricht an ein neues ns-Protokoll zu senden.
   - Wählen Sie **Sicherheitscheck** umgehen, um die Sicherheitsüberprüfung zu umgehen. Dies ermöglicht unsichere Ausdrücke.
4. Klicken Sie auf **OK**.



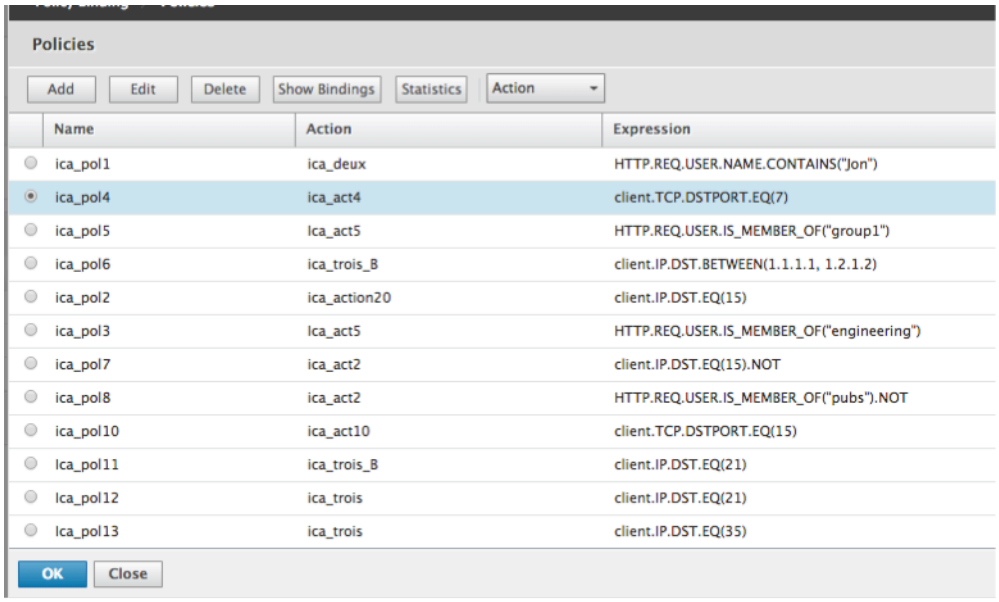

 

### Wählen Sie eine bestehende Richtlinie aus

1. Klicken Sie auf das Symbol >, um eine vorhandene Richtlinie auszuwählen.



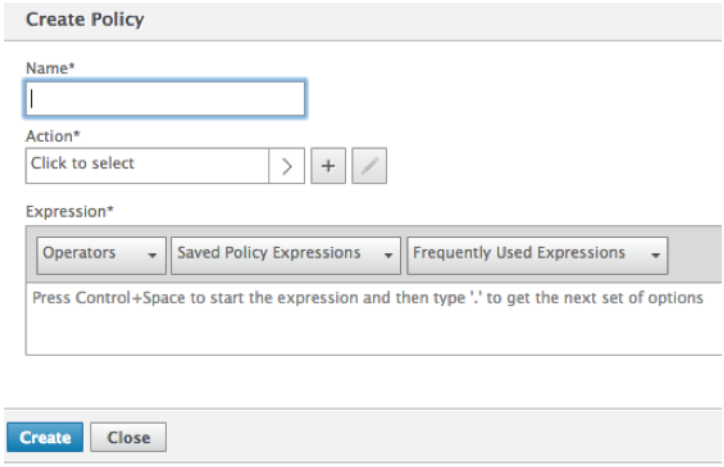

2. Wählen Sie das Optionsfeld der gewünschten Richtlinie aus.



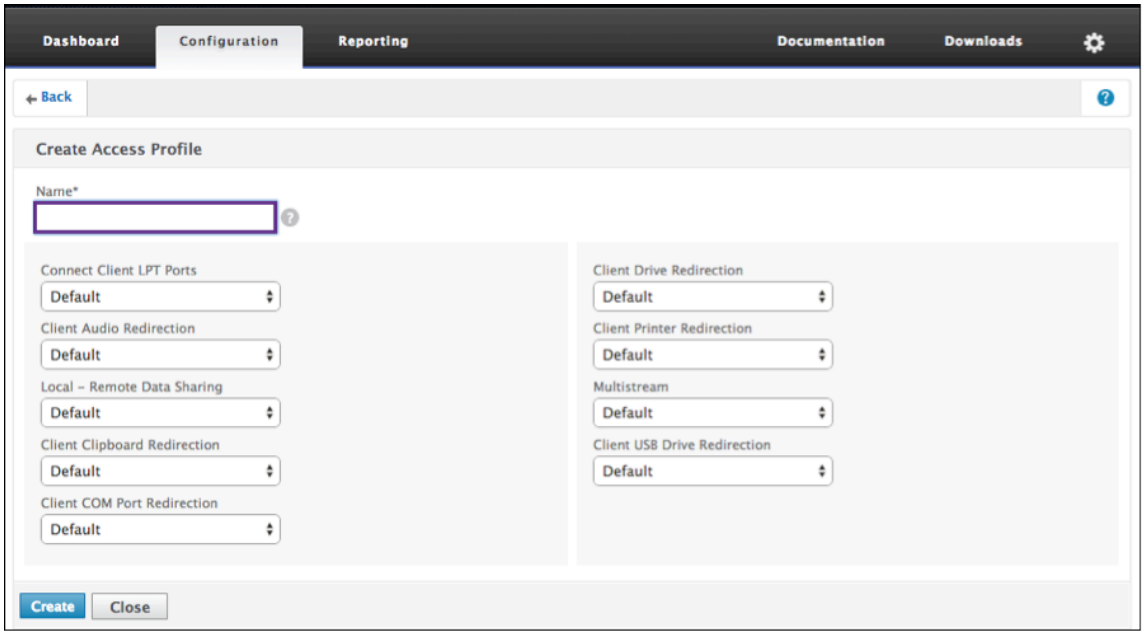

### Erstellen einer Richtlinie

1. **Geben Sie im Feld Name einen Namen für die Richtlinie ein.**
2. Klicken Sie auf +, um eine Richtlinie zu erstellen.

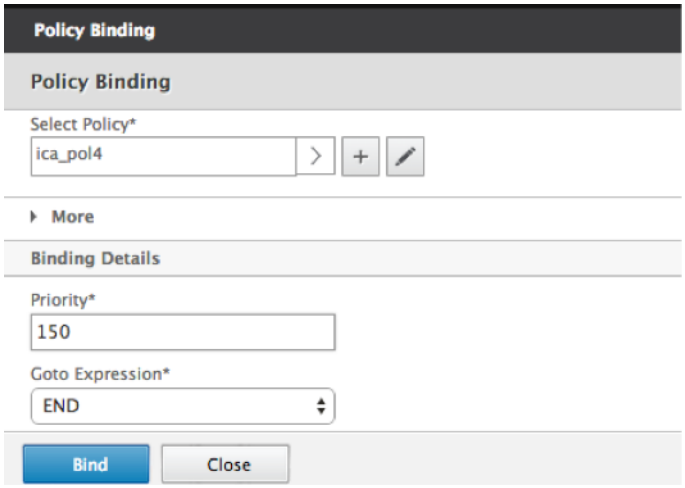



3. Erstellen Sie eine Aktion. Einzelheiten finden Sie unter **Erstellen einer neuen Aktion**.
4. Nennen Sie das Zugriffsprofil.




5. Konfigurieren Sie das Zugriffsprofil über dieses Menü.
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Bind**.




## Konfigurieren der Endpunktanalyse vor und nach der Authentifizierung

In diesem Abschnitt wird beschrieben, wie die Endpunktanalyse (EPA) nach der Authentifizierung und Vorauthentifizierung konfiguriert wird.

Um EPA nach der Authentifizierung mit SmartControl zu konfigurieren, verwenden Sie den Parameter `Smartgroup` aus der VPN-Sitzungsaktion. Der EPA-Ausdruck ist in der VPN-Sitzungsrichtlinie konfiguriert.

Sie können einen Gruppennamen für den Smartgroup-Parameter angeben. Dieser Gruppenname kann eine beliebige Zeichenfolge sein. Der Gruppenname muss keine existierende Gruppe im Active Directory sein.

Konfigurieren Sie die ICA-Richtlinie mit dem Ausdruck HTTP.REQ.IS_MEMBER_OF ("`groupname`"). Verwenden Sie den Gruppennamen, der zuvor für die Smartgroup angegeben wurde.

Um die Vorauthentifizierung von EPA mit SmartControl zu konfigurieren, verwenden Sie den Standard-EPA-Gruppenparameter aus dem Vorauthentifizierungsprofil. Der EPA-Ausdruck ist in der Vorauthentifizierungsrichtlinie konfiguriert.

Sie können einen Gruppennamen für den Standard-EPA-Gruppenparameter angeben. Dieser Gruppenname kann eine beliebige Zeichenfolge sein. Der Gruppenname muss keine existierende Gruppe im Active Directory sein.

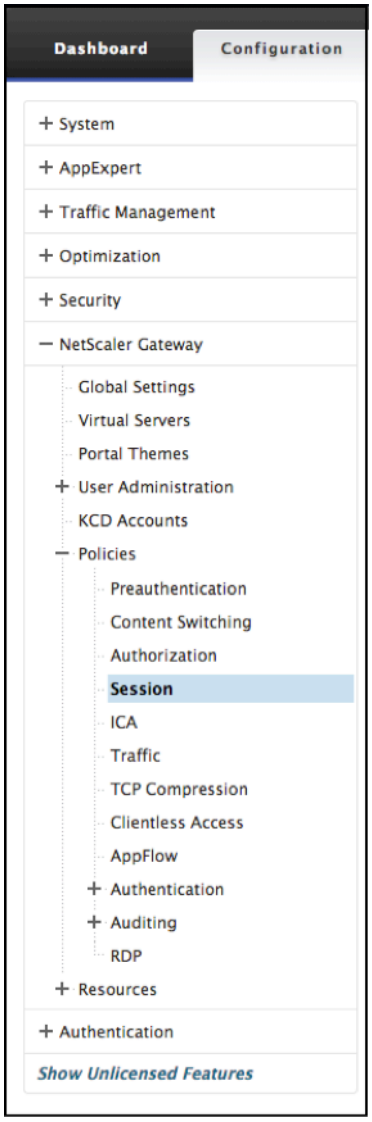
Konfigurieren Sie die ICA-Richtlinie mit dem Ausdruck HTTP.REQ.IS_MEMBER_OF ("`groupname`") und verwenden Sie den Gruppennamen, der zuvor für die Standard-EPA-Gruppe angegeben wurde.

### Konfiguration nach der Authentifizierung

**Gehen Sie wie folgt vor, um Smart Groups für die Konfiguration nach der Authentifizierung einzurichten.**

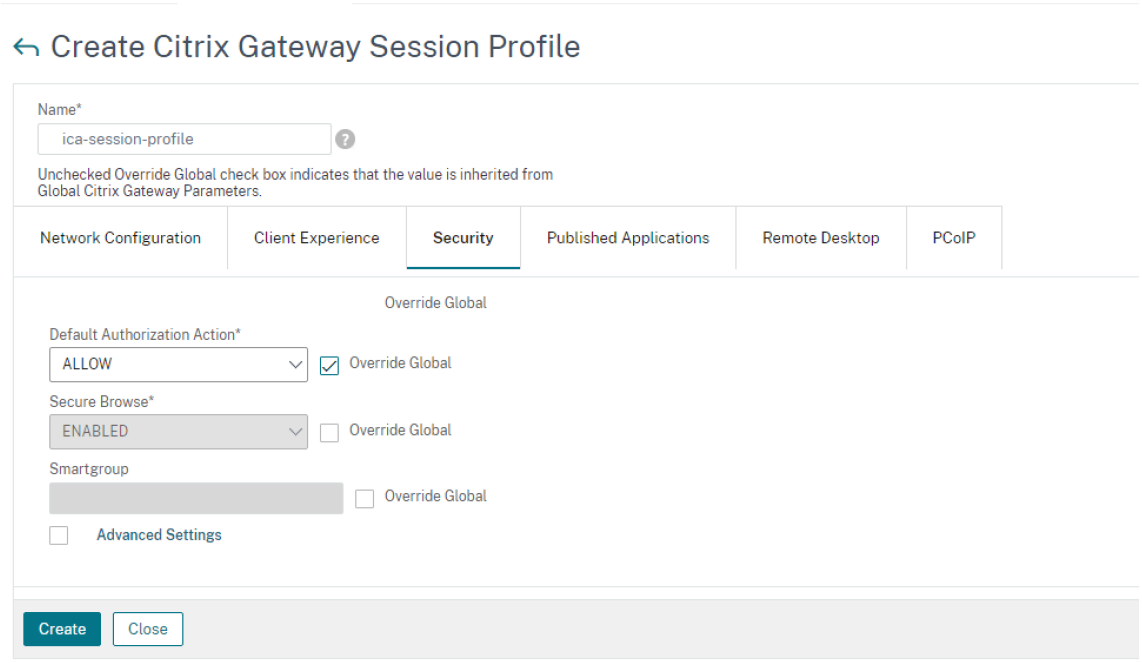
 

1. Wechseln Sie zu **Citrix Gateway > Richtlinien > Sitzung**.




2. Gehe zu **Sitzungsprofile> Hinzufügen**.




## Citrix Gateway-Sitzungsprofil erstellen

1. Klicken Sie auf die Registerkarte **Sicherheit**.
2. Geben Sie einen **Namen** für Ihr Citrix Gateway-Profil (Aktion) ein.
3. Markieren Sie das Kästchen rechts neben dem Menü und wählen Sie die gewünschte **Standard-Autorisierungsaktion**aus.

   Geben Sie die Netzwerkressourcen an, auf die Benutzer Zugriff haben, wenn sie sich am internen Netzwerk anmelden. Die Standardeinstellung für die Autorisierung besteht darin, den Zugriff auf alle Netzwerkressourcen zu verweigern. Citrix empfiehlt, die globale Standardeinstellung zu verwenden und dann Autorisierungsrichtlinien zu erstellen, um die Netzwerkressourcen zu definieren, auf die Benutzer zugreifen können. Wenn Sie die Standard-Autorisierungsrichtlinie auf DENY festlegen, müssen Sie den Zugriff auf jede Netzwerkressource explizit autorisieren, was die Sicherheit verbessert.
4. Markieren Sie das Kästchen rechts neben dem Menü und wählen Sie das gewünschte **Secure Browse aus.**

   Ermöglichen Sie Benutzern die Verbindung über Citrix Gateway mit Netzwerkressourcen von iOS- und Android-Mobilgeräten mit der Citrix Workspace-App. Benutzer müssen keinen vollständigen VPN-Tunnel einrichten, um auf Ressourcen im sicheren Netzwerk zuzugreifen.
5. Markieren Sie das Feld rechts neben dem Menü und geben Sie den Namen `Smartgroup` ein.

Dies ist die Gruppe, in die der Benutzer platziert wird, wenn die mit dieser Sitzungsaktion verknüpfte Sitzungsrichtlinie erfolgreich ist. Die VPN-Sitzungsrichtlinie führt die EPA-Prüfung nach der Authentifizierung durch, und wenn die Prüfung erfolgreich ist, wird der Benutzer in die Gruppe aufgenommen, die mit einer Smartgroup angegeben wurde. Der Ausdruck is_member_of (aaa.user.is_member_of) kann dann mit Richtlinien verwendet werden, um zu überprüfen, ob die EPA den zu dieser intelligenten Gruppe gehörenden Benutzer weitergegeben hat.

6. Klicken Sie auf **Erstellen**.
7. Wechseln Sie zu **Citrix Gateway > Richtlinien > Sitzung**.
8. Gehen Sie zu **Sitzungsrichtlinien > Hinzufügen**.
9. Geben Sie den **Namen** für die neue Sitzungsrichtlinie ein, die angewendet wird, nachdem sich der Benutzer bei Citrix Gateway angemeldet hat.
10. Wählen Sie über das Menü die Aktion **Profil** aus.

    Die Aktion, die von der neuen Sitzungsrichtlinie angewendet wird, wenn das Regelkriterium erfüllt ist.

    **Hinweis:** Wenn das gewünschte Profil erstellt werden muss, wählen Sie das + aus. Weitere Einzelheiten finden Sie unter Erstellen eines Citrix Gateway-Sitzungsprofils.

11. Geben Sie **Expression** in dieses Feld ein.

    Dieses Feld definiert den benannten Ausdruck, der den Verkehr angibt, der der Richtlinie entspricht. Der Ausdruck kann entweder in Standard- oder klassischer Syntax geschrieben werden. Die maximale Länge einer literalen Zeichenfolge für den Ausdruck beträgt 255 Zeichen. Eine längere Zeichenfolge kann in kleinere Zeichenfolgen mit jeweils bis zu 255 Zeichen aufgeteilt werden, und die kleineren Zeichenfolgen werden mit dem Operator + verkettet. Beispielsweise können Sie eine Zeichenfolge mit 500 Zeichen wie folgt erstellen: “”+ “”

    > Die folgenden Anforderungen gelten nur für die Citrix ADC CLI:

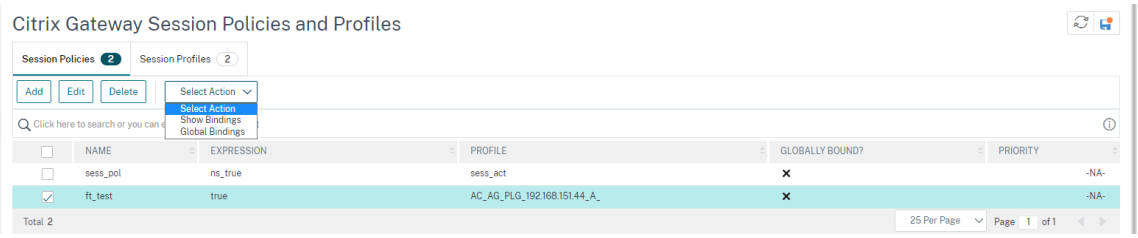
    - Wenn der Ausdruck ein oder mehrere Leerzeichen enthält, schließen Sie den gesamten Ausdruck in doppelte Anführungszeichen ein.
    - Wenn der Ausdruck selbst doppelte Anführungszeichen enthält, entkommen Sie den Anführungszeichen mithilfe des Zeichens.* Alternativ können Sie einfache Anführungszeichen verwenden, um die Regel einzuschließen. In diesem Fall müssen Sie die doppelten Anführungszeichen nicht entkommen.

12. Klicken Sie auf **Erstellen**.
13. Wechseln Sie zu **Sitzungsrichtlinien**.
14. Wählen Sie den **Namen** der Sitzungsrichtlinie aus.

15. Wählen Sie im Menü **Aktion** die Option **Globale Bindungen** aus.
16. Wählen Sie **Bindung hinzufügen** aus.
17. Wählen Sie ** aus, um eine bestehende Richtlinie auszuwählen.

    **Hinweis:** Wählen Sie +, um eine Richtlinie zu erstellen. Weitere Einzelheiten finden Sie im Abschnitt Erstellen eines Citrix Gateway-Sitzungsprofils.
18. Wähle einen Namen aus der Liste und drücke die Taste **Auswählen**.
19. Geben Sie die **Priorität** ein und klicken Sie auf **Binden**.
20. Klicken Sie auf **Fertig**
21. Die Prüfung zeigt, dass Ihre Auswahl global gebunden ist.

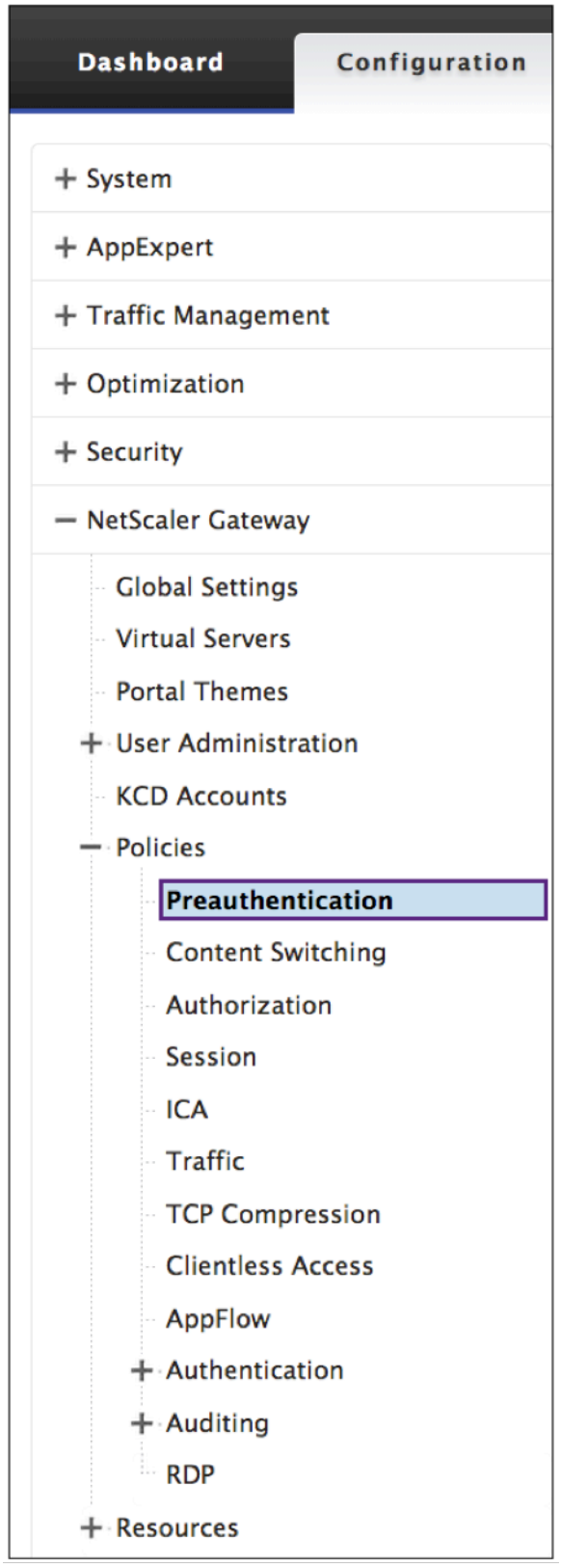



### Konfiguration vor der Authentifizierung

Gehen Sie wie folgt vor, um die Konfiguration vor der Authentifizierung einzurichten.

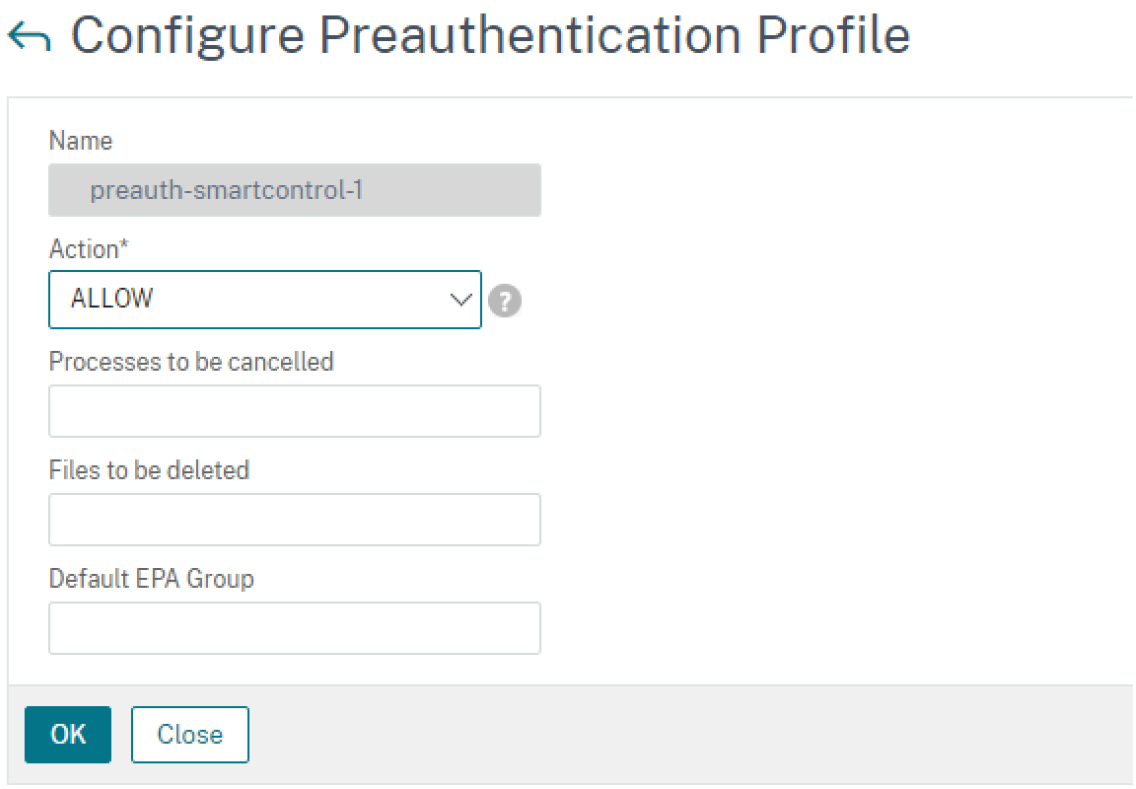
1. Wechseln Sie zu **Citrix Gateway > Richtlinien > Vorauthentifizierung**.




2. Wählen Sie die Registerkarte **Vorauthentifizierungsprofile** und wählen Sie **Hinzufügen**.




3. Geben Sie den **Namen** für die Vorauthentifizierungsaktion ein.

   Der Name muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur aus Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstrichen bestehen. Kann nicht geändert werden, nachdem eine Vorauthentifizierungsaktion erstellt wurde.

   **Hinweis:** Die folgende Anforderung gilt nur für die Citrix ADC CLI:
   Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein.

4. Wählen Sie eine **Anforderungsaktion** aus, die die Richtlinie aufrufen soll, wenn eine Verbindung mit der Richtlinie übereinstimmt.

   **Hinweis:** Wenn Sie ein Vorauthentifizierungsprofil erstellen oder erstellen möchten, wählen Sie das +. Weitere Informationen finden Sie unter Vorauthentifizierungsprofil erstellen.

5. Geben Sie einen **Ausdruck** ein, bei dem es sich um den Namen der benannten Citrix ADC-Regel oder einen Standardsyntaxausdruck handelt, der die Verbindungen definiert, die der Richtlinie entsprechen.

6. Klicken Sie auf **Erstellen**.

7. Wechseln Sie zur Registerkarte **Vorauthentifizierungsrichtlinien** und wählen Sie die gewünschte Richtlinie aus.

8. Wählen Sie im Menü **Aktion** die Option **Globale Bindung** aus.
9. Wählen Sie **Bindungen hinzufügen**aus.
10. Wählen Sie > aus, um eine bestehende Richtlinie auszuwählen.

    Wählen Sie + aus, um eine Richtlinie zu erstellen. Weitere Einzelheiten finden Sie unter Erstellen eines Citrix Gateway-Sitzungsprofils.
11. **Wählen Sie Richtlinie aus**.
12. Geben Sie die **Priorität** ein und klicken Sie auf **Binden**.
13. Klicken Sie auf **Fertig**.
14. Die Überprüfung zeigt, dass die **Vorauthentifizierungsrichtlinieglobal gebunden**ist.

## Vorauthentifizierungsprofil erstellen

1. Geben Sie den **Namen** für die Vorauthentifizierungsaktion ein

   Der Name muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur aus Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstrichen bestehen. Kann nicht geändert werden, nachdem eine Vorauthentifizierungsaktion erstellt wurde.

   **Hinweis:** Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen. Dies gilt nur für die Citrix ADC CLI.
2. Rufen Sie die **Aktion** aus dem Menü auf.

   Diese Option erlaubt oder verweigert die Anmeldung nach Endpoint Analysis (EPA) -Ergebnissen.
3. **Abgebrochene Prozesse**

   Diese Option identifiziert eine Reihe von Prozessen, die das Endpoint Analysis (EPA) -Tool beenden muss.
4. **Zu löschende Dateien**

   Diese Option identifiziert eine Zeichenfolge, die die Pfade und Namen der Dateien angibt, die das Endpoint Analysis (EPA) -Tool löschen muss.
5. **Standard-EPA-Gruppe**

   Die standardmäßige EPA-Gruppe ist die Gruppe, die ausgewählt wird, wenn die EPA-Überprüfung erfolgreich ist.
6. Klicken Sie auf **Erstellen**.

# Konfigurieren von Single Sign-On für das Webinterface

March 27, 2024

Sie können Citrix Gateway so konfigurieren, dass einmaliges Anmelden für Server im internen Netzwerk bereitgestellt wird, die webbasierte Authentifizierung verwenden. Mit einmaliger Anmeldung können Sie den Benutzer zu einer benutzerdefinierten Homepage wie einer SharePoint-Website oder zum Webinterface umleiten. Sie können das einmalige Anmelden bei Ressourcen auch über das Citrix Gateway Plug-in über ein im Access Interface konfiguriertes Lesezeichen oder eine Webadresse konfigurieren, die Benutzer im Webbrowser eingeben.

Wenn Sie das Access Interface auf eine SharePoint-Website oder das Webinterface umleiten, geben Sie die Webadresse für die Website an. Wenn Benutzer entweder von Citrix Gateway oder einem externen Authentifizierungsserver authentifiziert werden, werden Benutzer auf die angegebene Homepage umgeleitet und automatisch angemeldet. Benutzeranmeldeinformationen werden transparent an den Webserver weitergegeben. Wenn der Webserver die Anmeldeinformationen akzeptiert, werden Benutzer automatisch angemeldet. Wenn der Webserver die Anmeldeinformationen ablehnt, erhalten Benutzer eine Authentifizierungsaufforderung, in der sie nach ihrem Benutzernamen und Kennwort gefragt werden.

Sie können Single Sign-On für Webanwendungen global oder mithilfe einer Sitzungsrichtlinie konfigurieren.

Sie können auch Single Sign-On am Webinterface mithilfe einer Smartcard konfigurieren. Einzelheiten finden Sie unter Konfigurieren von Single Sign-On am Webinterface mithilfe einer Smartcard.

Citrix Gateway ist mit den folgenden Versionen des Webinterface kompatibel:

- Webinterface 4.5
- Webinterface 5.0
- Webinterface 5.1
- Webinterface 5.2
- Webinterface 5.3
- Webinterface 5.4

Stellen Sie vor dem Konfigurieren von Single Sign-On sicher, dass das Webinterface bereits konfiguriert ist und mit Citrix Gateway funktioniert.

## Konfigurieren von Single Sign-On für Webanwendungen global

March 27, 2024

Wenn Sie Single Sign-On global anwenden, kann ein Webdienst alle Webanwendungssitzungen authentifizieren, anstatt diese Sitzungen auf dem Citrix Gateway zu authentifizieren.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Klicken Sie im Dialogfeld **Globale Citrix Gateway-Einstellungen** auf der Registerkarte **Client Experienceauf Single Sign-On**to Web Applications und dann auf**OK**.

## Konfigurieren von Single Sign-On bei Webanwendungen über eine Sitzungsrichtlinie

March 27, 2024

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** > **Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Wählen Sie im Detailbereich auf der Registerkarte **Profile** eine Richtlinie aus und klicken Sie dann auf **Hinzufügen**.
3. Klicken **Sie im Dialogfeld Sitzungsrichtlinie konfigurieren** neben **Anforderungsprofil**auf **Ändern**.
4. Klicken **Sie im Dialogfeld Sitzungsprofil konfigurieren** auf der Registerkarte **Client Experience** neben Single Sign-On bei Webanwendungen auf **Global Override**, klicken Sie **auf Single Sign-On to Web Applications** und dann auf **OK**.

## Definieren des HTTP-Ports für Single Sign-On bei Webanwendungen

March 27, 2024

Single Sign-On wird nur für den Netzwerkverkehr versucht, bei dem der Zielport als HTTP-Port betrachtet wird. Um Single Sign-On für Anwendungen zu ermöglichen, die einen anderen Port als Port 80 für HTTP-Verkehr verwenden, fügen Sie eine oder mehrere Portnummern auf Citrix Gateway hinzu. Sie können mehrere Ports aktivieren. Sie konfigurieren die Ports global.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte **Netzwerkkonfiguration** auf **Erweiterte Einstellungen**.

4. Geben Sie unter HTTP-Ports die Portnummer ein, klicken Sie auf **Hinzufügen** und dann auf **OK**.

> **Hinweis**: Wenn Webanwendungen im internen Netzwerk unterschiedliche Portnummern verwenden, geben Sie die Portnummer ein und klicken Sie dann auf **Hinzufügen**. Sie müssen die HTTP-Portnummer definieren, um Single Sign-On für Webanwendungen, einschließlich des Webinterface, zu ermöglichen.

## Zusätzliche Konfigurationsrichtlinien

March 27, 2024

Beachten Sie beim Konfigurieren des Webinterface für einmaliges Anmelden die folgenden Richtlinien:

- Die URL des Authentifizierungsdienstes muss mit https beginnen.
- Der Server, auf dem das Webinterface ausgeführt wird, muss dem Citrix Gateway-Zertifikat vertrauen und in der Lage sein, den vollqualifizierten Domänennamen (FQDN) des Zertifikats auf die IP-Adresse des virtuellen Servers aufzulösen.
- Das Webinterface muss in der Lage sein, eine Verbindung zum virtuellen Citrix Gateway-Server herzustellen. Jeder virtuelle Citrix Gateway-Server kann für diesen Zweck verwendet werden. Es muss nicht der virtuelle Server sein, auf dem sich Benutzer anmelden.
- Wenn es eine Firewall zwischen dem Webinterface und Citrix Gateway gibt, können Firewallregeln den Benutzerzugriff verhindern, wodurch Single Sign-On am Webinterface deaktiviert wird. Um dieses Problem zu umgehen, lockern Sie entweder Ihre Firewallregeln oder erstellen Sie einen anderen virtuellen Server auf Citrix Gateway, mit dem das Webinterface eine Verbindung herstellen kann. Der virtuelle Server muss über eine IP-Adresse verfügen, die sich im internen Netzwerk befindet. Verwenden Sie beim Herstellen einer Verbindung zum Webinterface den sicheren Port 443 als Zielport.
- Wenn Sie ein Zertifikat einer privaten Zertifizierungsstelle (CA) für den virtuellen Server verwenden, verwenden Sie in der Microsoft Management Console (MMC) das Zertifikats-Snap-In, um das CA-Stammzertifikat im lokalen Computerzertifikatspeicher auf dem Server zu installieren, auf dem das Webinterface ausgeführt wird.
- Wenn sich Benutzer anmelden und eine Fehlermeldung "Zugriff verweigert"erhalten, überprüfen Sie die Webinterface-Ereignisanzeige für weitere Informationen.
- Für erfolgreiche Benutzerverbindungen zu veröffentlichten Anwendungen oder Desktops muss die Secure Ticket Authority (STA), die Sie auf Citrix Gateway konfiguriert haben, mit der STA übereinstimmen, die Sie auf dem Webinterface konfiguriert haben.

## Testen der Single Sign-On-Verbindung zum Webinterface

March 27, 2024

Nachdem Sie Single Sign-On für das Webinterface von einem Clientgerät aus konfiguriert haben, öffnen Sie einen Webbrowser und testen Sie, ob eine Verbindung erfolgreich ist.

1. Geben Sie in einem Webbrowser ein `https://NetScalerGatewayFQDN`, wobei NetscalerGatewayFQDN der vollqualifizierte Domänenname (FQDN) im an den virtuellen Server gebundenen Zertifikat ist.
2. Melden Sie sich bei einem Domänenbenutzerkonto in Active Directory an. Bei der Anmeldung werden Sie zum Webinterface weitergeleitet.

Anwendungen werden automatisch ohne zusätzliche Authentifizierung angezeigt. Wenn Benutzer eine veröffentlichte Anwendung starten, leitet die Citrix Workspace-App den Datenverkehr über das Citrix Gateway-Gerät an Server in der Farm weiter.

## Konfigurieren von Single Sign-On am Webinterface mithilfe einer Smartcard

March 27, 2024

Wenn Sie Smartcards für die Benutzeranmeldung verwenden, können Sie Single Sign-On am Webinterface konfigurieren. Sie konfigurieren Einstellungen auf Citrix Gateway und konfigurieren dann das Webinterface so, dass einmaliges Anmelden mit einer Smartcard akzeptiert wird. Einmaliges Anmelden wird auch als Passthrough-Authentifizierung bezeichnet.

Die Webinterface-Versionen 5.3 und 5.4 unterstützen einmaliges Anmelden am Webinterface mit einer Smartcard. Wenn Sie das Webinterface auf der Citrix ADC-Funktion aktivieren, die in NetScaler Version 10 verfügbar ist, können Sie auch Single Sign-On mit einer Smartcard verwenden. Weitere Informationen zum Konfigurieren dieser Funktion finden Sie unter Verwenden der Smartcard-Authentifizierung für das Webinterface über Citrix Gateway.

Benutzer können in mehreren CN-Gruppen im Active Directory sein, damit einmaliges Anmelden funktioniert, solange die Extraktion des Benutzernamens in der Zertifikataktion subjectAltName:PrincipalName lautet. Wenn Sie den Parameter Subject:CN verwenden, können Benutzer nicht Teil mehrerer CN-Gruppen sein.

Um Citrix Gateway für die einmalige Anmeldung am Webinterface mithilfe einer Smartcard zu konfigurieren, müssen Sie Folgendes tun:

- Installieren Sie ein signiertes Serverzertifikat von einer Zertifizierungsstelle (CA). Weitere Informationen finden Sie unter Installieren des signierten Zertifikats auf Citrix Gateway.
- Installieren Sie ein Stammzertifikat auf Citrix Gateway und dem Benutzergerät.
- Erstellen Sie einen virtuellen Server als Anmeldepunkt für das Webinterface. Wenn Sie den virtuellen Server konfigurieren, müssen Sie den SSL-Parameter des Clientzertifikats auf Optional festlegen. Weitere Informationen zum Konfigurieren eines virtuellen Servers finden Sie unter Erstellen virtueller Server.
- Erstellen Sie einen sekundären virtuellen Server, auf dem die Clientauthentifizierung in den SSL-Parametern deaktiviert ist. Diese Konfiguration verhindert, dass Benutzer eine sekundäre Anfrage nach ihrer persönlichen Identifikationsnummer (PIN) erhalten.
- Erstellen Sie eine Richtlinie zur Clientzertifikatauthentifizierung Verwenden Sie im Feld Benutzername den Parameter subjectAltName:PrincipalName, um Benutzer aus mehreren Gruppen zu extrahieren. Lassen Sie das Feld für den Gruppennamen leer.
- Erstellen Sie eine Sitzungsrichtlinie und ein Profil auf Citrix Gateway. Innerhalb des Sitzungsprofils aktivieren Sie den ICA-Proxy und geben das Webinterface und die Domäne an, die Sie für das einmalige Anmelden verwenden.

Sie können das folgende Verfahren verwenden, um ein Sitzungsprofil für die einmalige Anmeldung mit einer Smartcard zu erstellen.

### So erstellen Sie ein Sitzungsprofil für einmaliges Anmelden mithilfe einer Smartcard

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway-Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Profile** und dann auf **Hinzufügen**.
3. Klicken Sie auf der Registerkarte **Client Experience** neben Homepage auf **Global überschreiben,** und deaktivieren Sie dann **Homepage anzeigen**.
4. Klicken Sie neben **Single Sign-On bei Webanwendungen aufOverride Global,**und klicken Sie dann**auf Single Sign-On bei Webanwendungen**.
5. Klicken Sie auf die Registerkarte **Published Applications**.
6. Klicken Sie neben **ICA-Proxy**auf **Override Global** und wählen Sie dann **ON**aus.
7. Klicken Sie **unter Webinterface-Adresse**auf **Override Global** und geben Sie dann den vollqualifizierten Domänennamen (FQDN) oder das Webinterface ein.
8. Klicken Sie in **Single Sign-On Domäne aufOverride Global,**und geben Sie dann den Domänennamen ein.

> **Hinweis**: Verwenden Sie die Format-Domain und nicht das Format domain.com.

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

Nachdem Sie das Sitzungsprofil fertiggestellt haben, konfigurieren Sie die Sitzungsrichtlinie und verwenden Sie das Profil als Teil der Richtlinie. Sie können dann die Sitzungsrichtlinie an den virtuellen Server binden.

## Konfigurieren des Clientzertifikats für Single Sign-On mit einer Smartcard

March 27, 2024

Wenn Sie Single Sign-On am Webinterface mithilfe einer Smartcard konfigurieren, müssen Sie Clientauthentifizierung auf den
Zertifikaten im Dialogfeld des virtuellen Servers auswählen und dann das Clientzertifikat als Optional konfigurieren. Wenn Sie
Obligatorisch wählen, schlägt die einmalige Anmeldung am Webinterface fehl.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway und klicken Sie dann auf Virtuelle Server.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf Öffnen.
3. Klicken Sie im Dialogfeld Citrix Gateway Virtual Server konfigurieren auf der Registerkarte Zertifikate auf SSL-Parameter.
4. Klicken Sie im Dialogfeld SSL Params konfigurieren unter Andere auf Clientauthentifizierung.
5. Wählen Sie in Clientzertifikat Optional aus und klicken Sie dann zweimal auf OK.

## Konfigurieren von Single Sign-On für Citrix Virtual Apps und Dateifreigaben

March 27, 2024

Wenn Benutzer eine Verbindung zu Servern herstellen, auf denen Citrix Virtual Apps ausgeführt wird und SmartAccess verwendet wird, können Sie Single Sign-On für Benutzer konfigurieren, die eine Verbindung zur Serverfarm herstellen. Wenn Sie den Zugriff auf veröffentlichte Anwendungen mithilfe einer Sitzungsrichtlinie und eines Profils konfigurieren, verwenden Sie den Domänennamen für die Serverfarm.

Sie können auch Single Sign-On für Dateifreigaben in Ihrem Netzwerk konfigurieren.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich **Citrix Gateway** > **Richtlinien** und klicken Sie dann auf **Sitzung**.
2. Wählen Sie im Detailbereich auf der Registerkarte **Richtlinien** eine Sitzungsrichtlinie aus und klicken Sie dann auf **Öffnen**.
3. Klicken Sie im Dialogfeld **Sitzungsrichtlinie konfigurieren** neben **Anforderungsprofil** auf **Ändern**.
4. Klicken **Sie im Dialogfeld Sitzungsprofil konfigurieren** auf der Registerkarte **Veröffentlichte Anwendungen** unter Single Sign-On-Domäne auf **Global überschreiben**, geben Sie den Domänennamen ein, und klicken Sie dann zweimal auf **OK**.

## Dateitypzuordnung zulassen

March 27, 2024

Mit der Dateitypzuordnung können Benutzer Dokumente in Anwendungen öffnen, die über die Citrix Virtual Apps oder Desktops 7 veröffentlicht wurden. Sie können diese Berechtigung verwenden, um Benutzern das Öffnen und Bearbeiten von Dokumenten auf Servern in der vertrauenswürdigen Umgebung zu ermöglichen und das Senden des Dokuments an das Benutzergerät zu vermeiden. Sie können die Dateitypzuordnung nur für Dokumenttypen verwenden, die einer veröffentlichten Anwendung zugeordnet sind, und nur, wenn Sie die Eigenschaften des virtuellen Servers auf Citrix Gateway korrekt konfigurieren.

Die Bereitstellung der Dateitypzuordnung als einziges Mittel zum Bearbeiten von Ressourcendokumenten kann zur Erhöhung der Sicherheit beitragen, da die Bearbeitung auf dem Server und nicht auf dem Benutzergerät erfolgen muss. Beispielsweise können Sie eine Dateitypzuordnung für eine Dateifreigabe gewähren, in der Mitarbeiter Berichte über laufende Projektbesprechungen veröffentlichen, ohne sie herunterladen oder hochladen zu können.

Die Bereitstellung der Dateitypzuordnung erfordert Folgendes:

- Benutzer führen die Citrix Workspace-App auf dem Benutzergerät aus.
- Benutzer stellen eine Verbindung über einen virtuellen Server her, an den eine Verkehrsrichtlinie gebunden ist und an den Sie die Richtlinie für die Citrix Virtual Apps konfigurieren.
- Benutzer werden den gewünschten Anwendungen in Citrix Virtual Apps and Desktops 7 zugewiesen.
- Administratoren konfigurieren Citrix Virtual Apps so, dass sie mit Citrix Gateway kompatibel sind.

Zu den Schritten zum Erstellen einer Dateitypzuordnung gehören:

- Erstellen einer Webinterface-Site.

- Konfigurieren der Dateitypzuordnung mithilfe einer Verkehrsrichtlinie auf Citrix Gateway.
- Definieren von Dateinamenerweiterungen in Citrix Virtual Apps and Desktops 7.

## Erstellen einer Webinterface-Site

March 27, 2024

Um das Webinterface für die Unterstützung der Dateitypzuordnung zu konfigurieren, erstellen Sie zuerst die Webinterface-Site. Die Webinterface-Site kann sich in Direct oder Advanced Access Control befinden. Kopieren Sie die folgenden Verzeichnisse auf Ihre Webinterface-Site:

- app_data
- auth
- Website

Wenn Sie diese Verzeichnisse auf die Webinterface-Site kopieren, werden die vorhandenen Verzeichnisse überschrieben.

Wenn Sie das Webinterface 4.6 oder 5.0 verwenden, öffnen Sie die Datei web.config im Webinterface-Site-Verzeichnis und fügen Sie den folgenden Code hinzu. Sie können diesen Code von der Citrix Support-Site unter herunterladen http://support.citrix.com/article/ctx116253.

```
<location path="site/contentLaunch.ica">
<system.web>
<httpHandlers>
<add verb="*" path="*.ica" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
<location path="site/contentLaunch.rad">
<system.web>
<httpHandlers>
<add verb="*" path="*.rad" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
<!--NeedCopy-->
```

Dieser Code muss nach dem folgenden Abschnitt in der Datei web.config hinzugefügt werden:

```
<location path="site/launch.rad">
        <system.web>
            <httpHandlers>
                <add verb="*" path="*.rad" type="System.Web.UI.
                   PageHandlerFactory"/>
            </httpHandlers>
        </system.web>
```

```
    </location>
<!--NeedCopy-->
```

## Konfigurieren von Citrix Gateway für die Dateitypzuordnung

March 27, 2024

Bevor Sie die Dateitypzuordnung auf Citrix Gateway konfigurieren, konfigurieren Sie eine Webinterface-Site zur Unterstützung der Dateitypzuordnung. Nachdem Sie das Webinterface erstellt und konfiguriert haben, müssen Sie Einstellungen auf Citrix Gateway erstellen. Die Schritte beinhalten:

- Erstellen eines neuen virtuellen Servers oder Verwenden eines vorhandenen. Weitere Informationen zum Erstellen eines virtuellen Servers finden Sie unter Erstellen virtueller Server.
- Erstellen einer Sitzungsrichtlinie und eines Profils, für die das Webinterface konfiguriert ist.
- Binden der Sitzungsrichtlinie an den virtuellen Server.
- Erstellen einer Verkehrsrichtlinie.

Nachdem Sie die Sitzungsrichtlinie erstellt und an den virtuellen Server gebunden haben, erstellen Sie die Verkehrsrichtlinie und binden Sie sie auch an den virtuellen Server.

Wenn Sie eine Verkehrsrichtlinie für die Dateitypzuordnung konfigurieren, erstellen Sie einen Ausdruck, um die Dateinamenerweiterungen zu definieren. Beispielsweise möchten Sie die Dateitypzuordnung für Microsoft Word und Microsoft Excel aktivieren. Ein Beispielausdruck ist:

```
REQ.HTTP.URL == /\*.doc || REQ.HTTP.URL == /\*.xls
```

### So erstellen Sie eine Sitzungsrichtlinie und ein Profil für die Dateitypzuordnung

1. Klicken Sie im Konfigurationsdienstprogramm auf die Registerkarte **Konfiguration**, erweitern Sie dann im Navigationsbereich **Citrix Gateway** > **Richtlinien**, und klicken Sie dann auf **Sitzung**.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf **Hinzufügen**.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Klicken Sie neben Profil anfordern auf **Neu**.
5. Geben Sie im Feld Name einen Namen für das Profil ein.
6. Konfigurieren Sie auf der Registerkarte **Published Applications** die folgenden Einstellungen:

    a) Klicken Sie neben Webinterface-Adresse auf **Override Global** und geben Sie dann die Webadresse des Webinterface ein.

b) Klicken Sie neben Webinterface Portal Mode auf **Override Global** und wählen Sie dann entweder Normal oder Kompakt aus.
c) Klicken Sie neben Single Sign-On Domain auf **Override Global**, geben Sie den Namen der Domäne ein, in der sich die Benutzerkonten befinden, und klicken Sie dann auf **Erstellen**.

7. Wählen **Sie im Dialogfeld Sitzungsrichtlinie erstellen** neben **Benannter Ausdruck**den **Wert True**aus, klicken Sie auf **Ausdruck hinzufügen**, klicken Sie auf **Erstellen** und dann auf **Schließen**.

## So erstellen Sie ein Verkehrsprofil für die Dateitypzuordnung

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte **Konfiguration** im Navigationsbereich Citrix Gateway-Richtlinien und klicken Sie dann auf Traffic.
2. Klicken Sie im Detailbereich auf die Registerkarte Profile und dann auf Hinzufügen.
3. Geben Sie im Feld Name einen Namen für das Profil ein.
4. Wählen Sie unter Dateitypzuordnung ON aus, klicken Sie auf Erstellen und dann auf Schließen.

## So konfigurieren Sie die Dateitypzuordnung in einer Verkehrsrichtlinie

1. Erweitern Sie im Konfigurationsdienstprogramm auf der Registerkarte Konfiguration im Navigationsbereich Citrix Gateway-Richtlinien, und klicken Sie dann auf Verkehr.
2. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf Hinzufügen.
3. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
4. Wählen Sie unter Profil anfordern ein Profil aus.
5. Wählen **Sie im Dialogfeld Traffic Policy erstellen** unter Ausdrücke die Option Erweiterte Freiform aus, und klicken Sie dann auf **Hinzufügen**.
6. Gehen **Sie im Dialogfeld „Ausdruck hinzufügen** "wie folgt vor:

   a) Klicken Sie unter **Ausdruckstyp**auf **Allgemein**.
   b) Wählen Sie unter Flow Type die Option REQ aus.
   c) Wählen Sie unter Protocol die Option HTTP.
   d) Wählen Sie im Qualifier URL aus.
   e) Wählen Sie unter Operator = = aus.
   f) Geben Sie unter Wert /*.fileExtensionType ein, wobei FileExtensionType der Dateityp ist, z. B. .doc oder.xls, und klicken Sie dann auf **OK**.

7. Klicken **Sie im Dialogfeld Traffic Policy erstellen** unter **Ausdrücke**neben Erweiterte Freiform auf **ODER**.
8. Wiederholen Sie die Schritte 4, 5 und 6 für jede Dateinamenerweiterung, die Sie einschließen möchten, klicken Sie auf **Erstellen** und dann auf **Schließen**.