Citrix Secure Private Access — Legacy

Machine translated content

Disclaimer

Contents

Secure Private Access für On-Premises-Bereitstellungen konfigurieren —Legacy

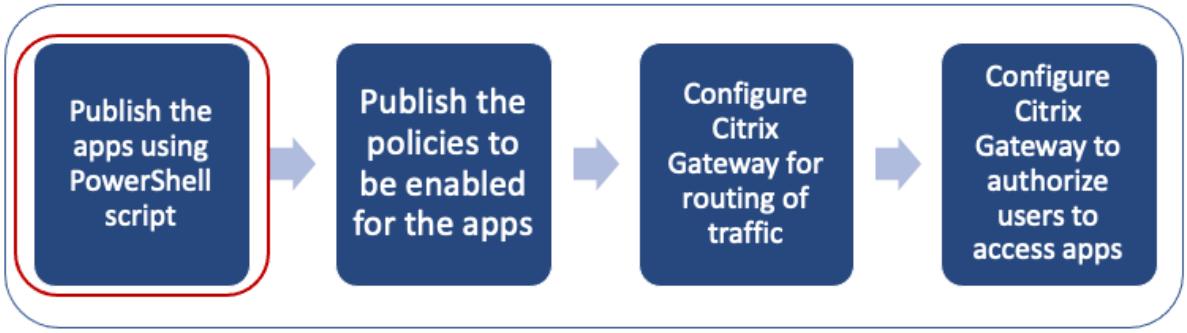
December 27, 2023

Die Konfiguration von Secure Private Access for on-premises ist ein vierstufiger Prozess.

1. Apps veröffentlichen
2. Richtlinien für die Apps veröffentlichen
3. Routing des Datenverkehrs über NetScaler Gateway aktivieren
4. Autorisierungsrichtlinien konfigurieren

> **Wichtig:**
>
> Ein Konfigurationstool ist verfügbar, um Apps und Richtlinien für die Apps schnell zu integrieren und auch die NetScaler Gateway- und StoreFront-Einstellungen zu konfigurieren. Beachten Sie jedoch Folgendes, bevor Sie das Tool verwenden.
>
> - Lesen Sie die Abschnitte Appsveröffentlichen und Richtlinien für die Apps veröffentlichen, um sicherzustellen, dass Sie die Konfigurationsanforderungen für die Konfiguration der on-premises Lösung vollständig verstehen.
> - Dieses Tool kann nur als Ergänzung zu den in diesem Thema dokumentierten bestehenden Verfahren verwendet werden und ersetzt nicht die Konfiguration, die manuell durchgeführt werden muss.
>
> Vollständige Informationen zum Tool finden Sie unter Konfigurieren von Apps und Richtlinien mit dem Secure Private Access-Konfigurationstool.

Schritt 1: Apps veröffentlichen



Sie müssen das PowerShell-Skript verwenden, um die URLs zu veröffentlichen. Sobald die App veröffentlicht ist, kann sie mit der Citrix Studio-Konsole verwaltet werden.

Sie können das PowerShell-Skript von https://www.citrix.com/downloads/workspace-app/powershell-module-for-configuring-secure-private-access-for-storefront/configure-secure-private-access-for-storefront.html herunterladen.

1. Öffnen Sie PowerShell auf der Maschine mit dem PowerShell-SDK.
2. Führen Sie den folgenden Befehl aus:

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

3. Definieren Sie die Variablen für die Web-App.

```
$citrixUrl: " <URL of the app> "
$appName: <app name as it must appear on Workspace>
$DesktopGroupId: 1
$desktopgroupname: <your desktop group name>
$AppIconFilePath:  <path of the image file>
```

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die mit eckigen Klammern (< >) markierten Platzhalter aktualisieren, bevor Sie den Befehl ausführen.

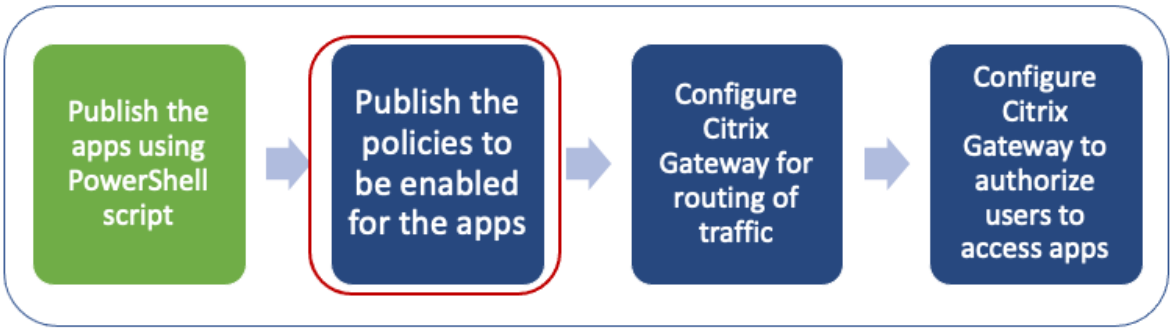
Nachdem Sie den Speicherort und den Anwendungsnamen zugewiesen haben, führen Sie den folgenden Befehl aus, um die Anwendung zu veröffentlichen.

```
New-BrokerApplication –ApplicationType PublishedContent –
    CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
    Uid
```

Die veröffentlichte App wird im Abschnitt **Anwendungen** in **Citrix Studio**angezeigt. Sie können die App-Details jetzt in der Citrix Studio-Konsole selbst ändern.

Weitere Informationen zum Veröffentlichen der App und zum Ändern des Standardsymbols der veröffentlichten App finden Sie unter Inhalt veröffentlichen.

Schritt 2: Richtlinien für die Apps veröffentlichen



Die Richtliniendatei definiert die Routing- und Sicherheitskontrollen jeder veröffentlichten App. Sie müssen die Richtliniendatei darüber aktualisieren, wie eine Web- oder SaaS-App weitergeleitet wird (über Gateway oder ohne Gateway).

Um Zugriffsrichtlinien für die Apps durchzusetzen, müssen Sie die Richtlinien für jede Web- oder SaaS-App veröffentlichen. Dazu müssen Sie die Richtlinien-JSON-Datei und die Datei Web.config aktualisieren.

- **Richtlinien-JSON-Datei:** Aktualisieren Sie die Richtlinien-JSON-Datei mit den App-Details und den Sicherheitsrichtlinien für die Apps. Die Richtlinien-JSON-Datei muss dann auf dem StoreFront-Server unter abgelegt werden `C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser`.

  > **Hinweis:**
  >
  > Sie müssen die Ordner **Resources** und **SecureBrowser** erstellen und dann die Richtlinien-JSON-Datei zum Ordner SecureBrowser hinzufügen.
  > Weitere Informationen zu den verschiedenen Richtlinienaktionen und ihren Werten finden Sie unter Details zu den Anwendungszugriffsrichtlinien.

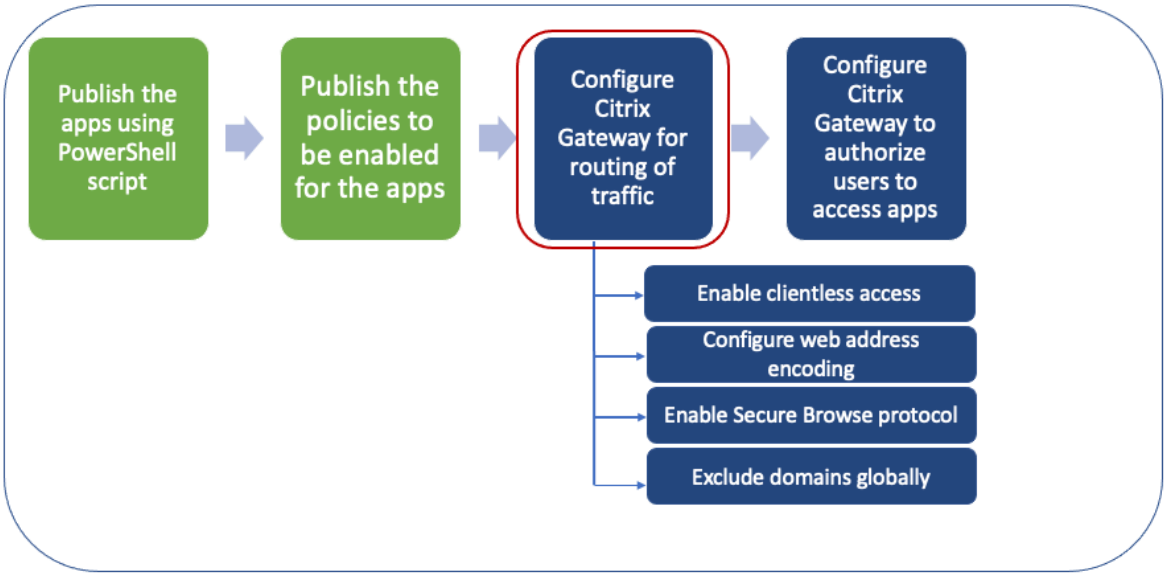
- **Web.config-Datei:** Um die neuen Richtliniendetails für die Citrix Workspace-App und den Citrix Enterprise Browser verfügbar zu machen, müssen Sie die Datei web.config im StoreFront Store-Verzeichnis ändern. Sie müssen die Datei bearbeiten, um ein neues XML-Tag mit dem Namen route hinzuzufügen. Die Datei Web.config muss dann im Verzeichnis C:\inetpub\wwwroot\Citrix\Store1 abgelegt werden.

  Eine Beispiel-XML-Datei finden Sie unter End-to-End-Beispielkonfiguration.

  > **Hinweis:**
  >
  > Im Pfad bezieht sich “Store1”auf den Namen, der für den Store angegeben wurde, als er erstellt wurde. Wenn ein anderer Geschäftsname verwendet wird, muss ein entsprechender Ordner erstellt werden.

  Es wird empfohlen, am Ende vorhandener Routen eine neue Route hinzuzufügen. Falls Sie in der Mitte eine Route hinzufügen, müssen Sie die Bestellnummer für alle nachfolgenden Routen manuell aktualisieren.

Schritt 3: Routing des Datenverkehrs über NetScaler Gateway aktivieren



Die Aktivierung des Routing von Datenverkehr über NetScaler Gateway umfasst die folgenden Schritte:

- Clientlosen Zugriff aktivieren
- URL-Codierung aktivieren
- Secure Browse aktivieren
- Domänen vom Umschreiben im clientlosen Zugriffsmodus ausschließen

Der clientlose Zugriff, die URL-Codierung und das sichere Surfen können global oder pro Sitzungsrichtlinie aktiviert werden.

- Die global aktivierte Einstellung gilt für alle konfigurierten virtuellen NetScaler Gateway-Server.
- Die Richtlinieneinstellung pro Sitzung gilt für Benutzer, Gruppen oder virtuelle Gatewayserver.

Clientlosen Zugriff aktivieren

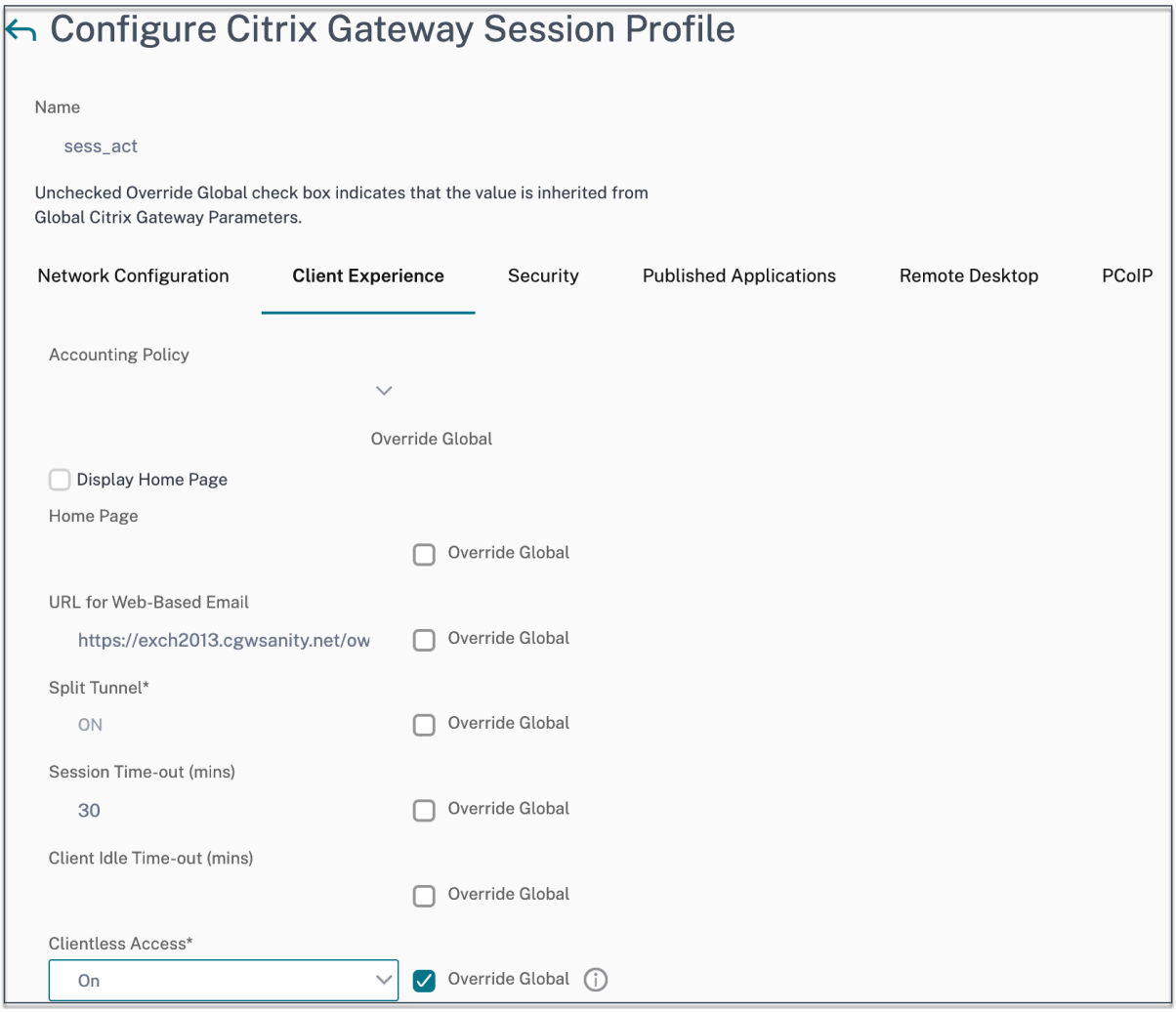
Um den clientlosen Zugriff global mithilfe der NetScaler Gateway-GUI zu aktivieren:

Erweitern Sie auf der Registerkarte **KonfigurationCitrix Gateway**und klicken Sie dann auf**Globale Einstellungen**.
Klicken Sie auf der Seite Allgemeine Einstellungen auf**Globale Einstellungen ändern**.
Wählen Sie auf der Registerkarte**Client Experience**unter Clientless Access die Option**ON**aus, und klicken Sie dann auf**OK**.

So aktivieren Sie den clientlosen Zugriff mithilfe einer Sitzungsrichtlinie mithilfe der NetScaler Gateway-GUI:

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 auf der Registerkarte **Konfiguration** den Eintrag **NetScaler Gateway** und klicken Sie dann auf **Richtlinien > Sitzung**.
2. Klicken Sie auf die Registerkarte **Sitzungsrichtlinie** 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. Klicken Sie auf der Registerkarte **Client Experience** neben Clientless Access auf **Override Global**, wählen Sie **On**aus und klicken Sie dann auf **Create**.
7. Geben Sie im Feld **Ausdruck** den Wert `true` ein. Wenn Sie den Wert `true` eingeben, wird die Richtlinie immer auf die Ebene angewendet, an die sie gebunden ist.
8. Klicken Sie auf **Erstellen** und dann auf **Schließen** .



Um den clientlosen Zugriff global mithilfe der NetScaler Gateway-CLI zu aktivieren:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
set vpn parameter -clientlessVpnMode On -icaProxy OFF
```

Um den clientlosen Zugriff pro Sitzungsrichtlinie mithilfe der NetScaler Gateway-CLI zu aktivieren:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
set vpn sessionAction <session-profile-name> -clientlessVpnMode On -
    icaProxy OFF
```

URL-Codierung aktivieren

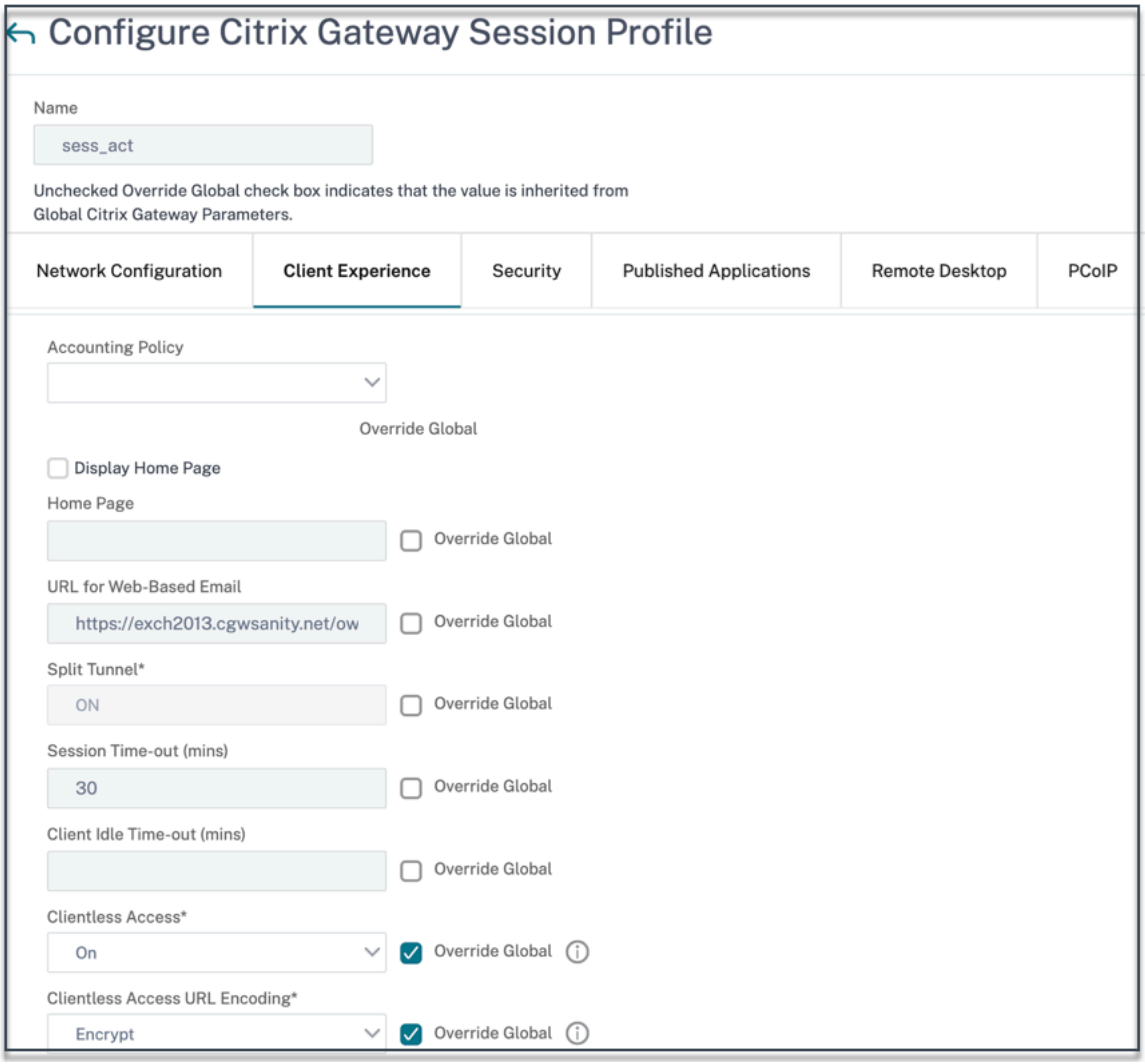
Wenn Sie den clientlosen Zugriff aktivieren, können Sie wählen, ob Sie die Adressen interner Webanwendungen codieren oder die Adresse als Klartext belassen möchten. Es wird empfohlen, die Webadresse als Klartext für den clientlosen Zugriff zu hinterlassen.

So aktivieren Sie die URL-Codierung global mithilfe der NetScaler Gateway-GUI:

1. Erweitern Sie auf der Registerkarte **KonfigurationCitrix Gateway**und klicken Sie dann auf**Globale Einstellungen**.
2. Klicken Sie auf der Seite **Globale Einstellungen** auf **Globale Einstellungen ändern**.
3. Wählen Sie auf der Registerkarte **Client Experience** unter **URL-Kodierung für den Clientless Access** die Einstellung für die Codierung Ihrer Web-URL aus, und klicken Sie dann auf **OK**.

So aktivieren Sie die URL-Codierung auf Sitzungsrichtlinienebene mithilfe der NetScaler Gateway-GUI:

1. Erweitern Sie auf der Registerkarte **Konfiguration** den Eintrag **NetScaler Gateway** und klicken Sie dann auf **Richtlinien > Sitzung**.
2. Klicken Sie auf die Registerkarte **Sitzungsrichtlinie** 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. 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. Geben Sie im Feld **Ausdruck** den Wert `true` ein. Wenn Sie den Wert `true` eingeben, wird die Richtlinie immer auf die Ebene angewendet, an die sie gebunden ist.



So aktivieren Sie die URL-Codierung global mithilfe der NetScaler Gateway-CLI:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
set vpn parameter -clientlessModeUrlEncoding TRANSPARENT
```

So aktivieren Sie die URL-Codierung pro Sitzungsrichtlinie mithilfe der NetScaler Gateway-CLI:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
set vpn sessionAction <session-profile-name> -clientlessModeUrlEncoding
    TRANSPARENT
```


Secure Browse aktivieren

Secure Browse und clientloser Zugriff ermöglichen zusammen Verbindungen im clientlosen VPN-Modus. Sie müssen sicheres Browsing aktivieren, damit der Citrix Enterprise Browser den sicheren Browsingmodus verwenden kann, um auf Apps ohne das Legacy-VPN zuzugreifen.

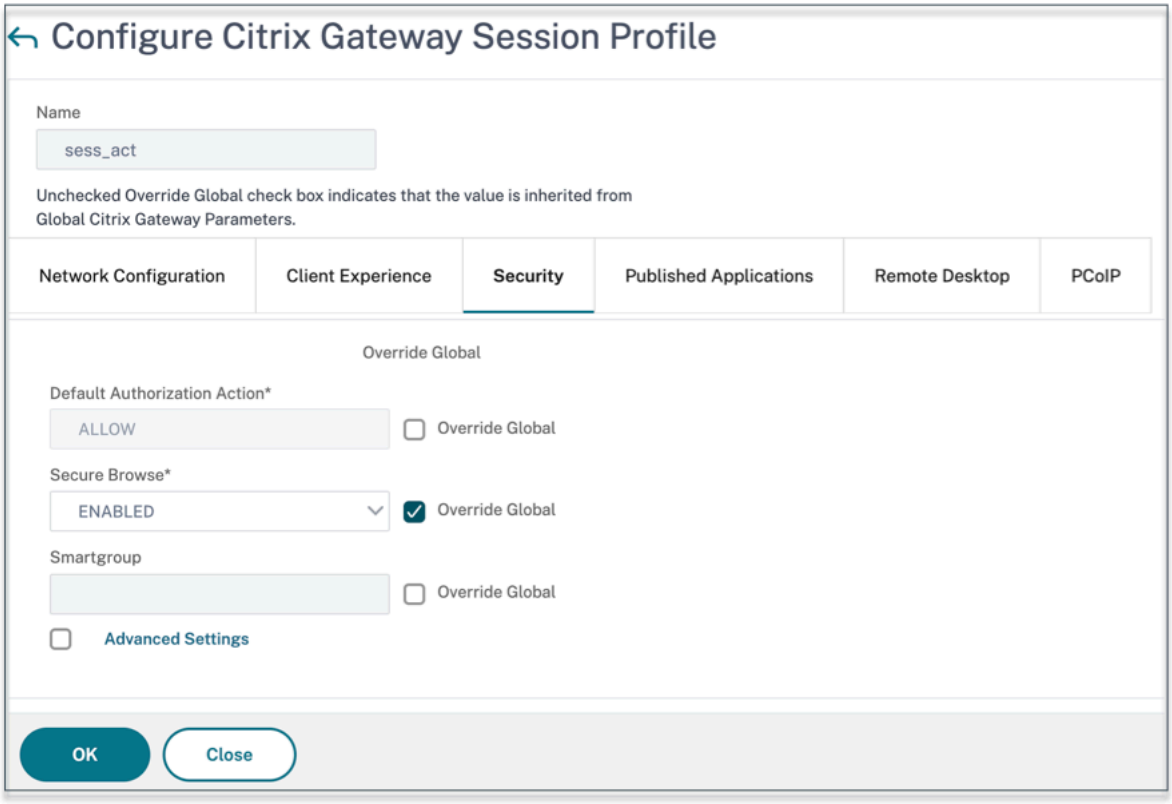
> **Hinweis:**
>
> Wenn der Endbenutzer den Citrix Enterprise Browser nicht installiert hat, werden die veröffentlichten URLs mit dem Tag **SPAEnabled** über den Standardbrowser des Geräts statt über den Citrix Enterprise Browser geöffnet. In einem solchen Fall gelten die Sicherheitsrichtlinien nicht. Das Problem tritt nur bei den StoreFront-Bereitstellungen auf.

So aktivieren Sie den sicheren Suchmodus global mithilfe der NetScaler Gateway-GUI:

1. Erweitern Sie auf der Registerkarte **KonfigurationCitrix Gateway**und klicken Sie dann auf**Globale Einstellungen**.
2. Klicken Sie auf der Seite Allgemeine Einstellungen auf **Globale Einstellungen ändern** .
3. Wählen Sie auf der Registerkarte **Sicherheit** in Secure Browse die Option **AKTIVIERT**aus, und klicken Sie dann auf **OK**.

So aktivieren Sie den sicheren Suchmodus auf Sitzungsrichtlinienebene mithilfe der NetScaler Gateway-GUI:

1. Erweitern Sie auf der Registerkarte **Konfiguration** den Eintrag **NetScaler Gateway** und klicken Sie dann auf **Richtlinien > Sitzung**.
2. Klicken Sie auf die Registerkarte **Sitzungsrichtlinie** 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. Klicken Sie auf der Registerkarte **Sicherheit** auf **Global überschreiben**und setzen **Sie Secure Browse** auf **AKTIVIERT**.



Um das sichere globale Durchsuchen mithilfe der NetScaler Gateway-CLI zu aktivieren:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
set vpn parameter -secureBrowse ENABLED
```

Um die Secure Browse per Session Policy mithilfe der NetScaler Gateway-CLI zu aktivieren, gehen Sie wie folgt vor:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

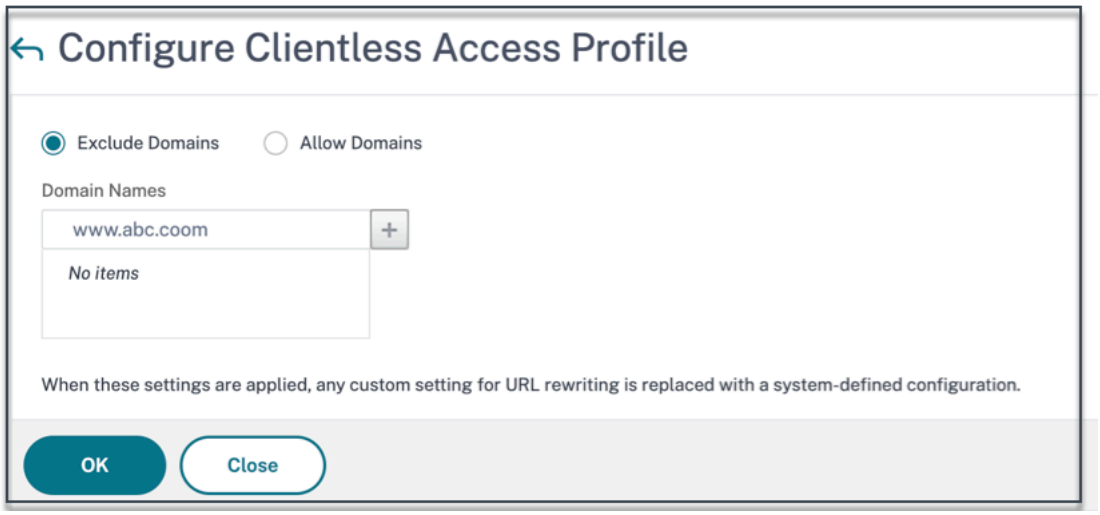
```
set vpn sessionAction <session-profile-name> -secureBrowse ENABLED
```

Domänen vom Umschreiben im clientlosen Zugriffsmodus ausschließen

Sie müssen die Domänen angeben, um zu verhindern, dass StoreFront die URLs im clientlosen Zugriffsmodus neu schreibt. Schließen Sie StoreFront-Server-FQDNs oder StoreFront-Loadbalancer-FQDNs und citrix.com aus. Diese Einstellung kann nur global angewendet werden.

1. Navigieren Sie zu **NetScaler Gateway > Globale Einstellungen**.
2. Klicken Sie unter **Clientless Access** auf **Configure Domains** for clientless Access.
3. Wählen Sie **Exclude Domain** aus.

4. Geben Sie im Feld **Domain Names** die Domänennamen ein (StoreFront-Server-FQDNs oder StoreFront-Loadbalancer-FQDNs).
5. Klicken Sie auf das **Pluszeichen** und geben Sie `citrix.com` ein.
6. Klicken Sie auf **OK**.

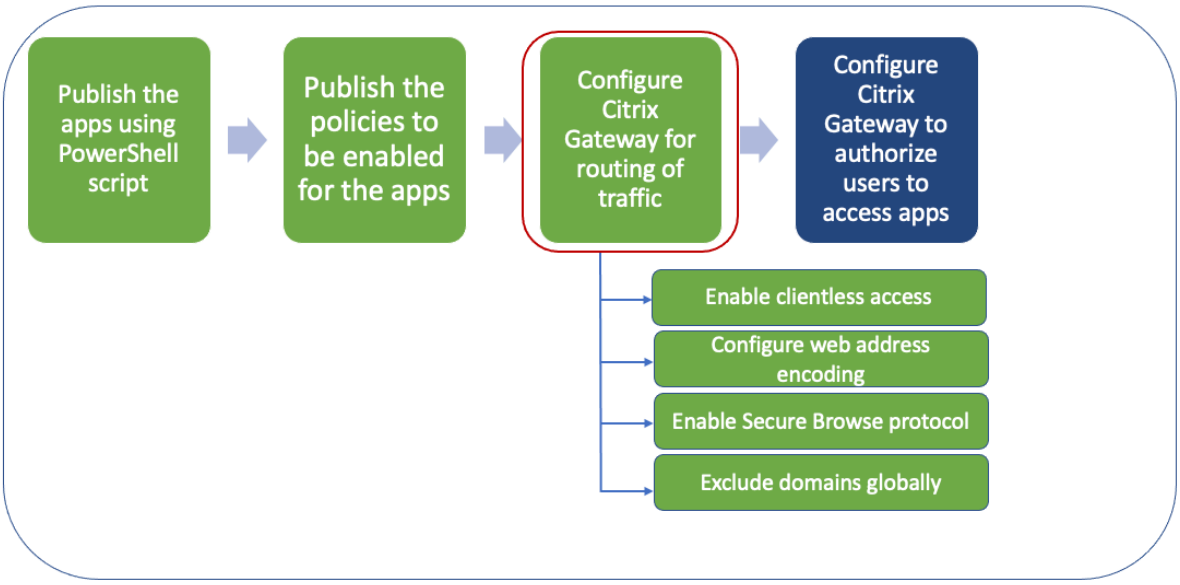


So schließen Sie Domänen mithilfe der NetScaler Gateway-CLI aus:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
bind policy patset ns_cvpn_default_bypass_domains <StoreFront-FQDN>
bind policy patset ns_cvpn_default_bypass_domains citrix.com
```

Schritt 4: Autorisierungsrichtlinien konfigurieren



Die Autorisierung gibt die Netzwerkressourcen an, auf die Benutzer zugreifen können, wenn sie sich bei NetScaler 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 NetScaler 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. Benutzerrichtlinien haben eine höhere Priorität als gruppengebundene Richtlinien.

Standard-Autorisierungsrichtlinien: Zwei Autorisierungsrichtlinien müssen erstellt werden, um den Zugriff auf den StoreFront-Server zu ermöglichen und den Zugriff auf alle veröffentlichten Web-Apps zu verweigern.

- Allow_StoreFront
- Deny_ALL

Autorisierungsrichtlinien für Web-Apps: Nachdem Sie die Standard-Autorisierungsrichtlinien erstellt haben, müssen Sie Autorisierungsrichtlinien für jede veröffentlichte Web-App erstellen.

- `Allow_<app1>`
- `Allow_<app2>`

So konfigurieren Sie eine Autorisierungsrichtlinie mithilfe der NetScaler Gateway-GUI:

1. Navigieren Sie zu **NetScaler 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 einen Ausdruck zu konfigurieren, klicken Sie auf **Auswählen** und wählen Sie die erforderlichen Elemente aus.
7. Klicken Sie auf **Fertig**.
8. Klicken Sie auf **Erstellen**.

So konfigurieren Sie eine Autorisierungsrichtlinie mithilfe der NetScaler Gateway-CLI:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
add authorization policy <policy-name> "HTTP.REQ.HOSTNAME.CONTAINS("<
    StoreFront-FQDN>")" ALLOW
```

So binden Sie eine Autorisierungsrichtlinie mithilfe der NetScaler Gateway-GUI an einen Benutzer/eine Gruppe:

1. Navigieren Sie zu **NetScaler Gateway > Benutzerverwaltung**.
2. Klicken Sie auf **AAA-Benutzer** oder **AAA-Gruppen**.
3. Wählen Sie im Detailbereich einen Benutzer/eine Gruppe aus und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie in **Erweiterte Einstellungen**auf **Autorisierungsrichtlinien**.
5. Wählen Sie auf der Seite "Richtlinienbindung"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 mithilfe der NetScaler Gateway-CLI:

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
bind aaa group <group-name> -policy <policy-name> -priority <priority>
    -gotoPriorityExpression END
```

Beispiel für eine End-to-End-Konfiguration

In diesem Beispiel wird eine App mit dem Namen "Docs"mit der URL https://docs.citrix.com in Citrix Workspace veröffentlicht.

1. Öffnen Sie PowerShell auf der Maschine mit dem PowerShell-SDK.
2. Führen Sie den folgenden Befehl aus:

   ```
   Add-PsSnapin Citrix*
   $dg = Get-BrokerDesktopGroup – Name PublishedContentApps
   ```

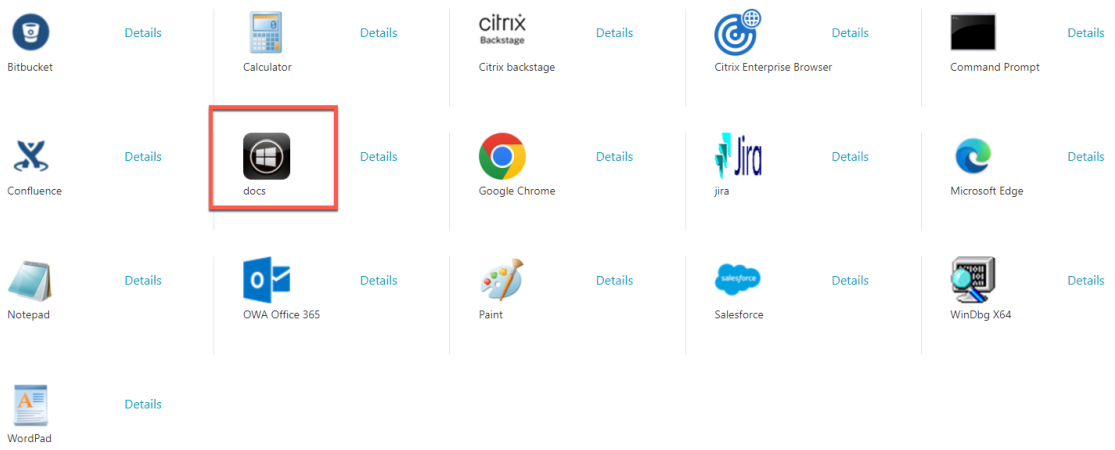
3. Fügen Sie dem Cmdlet die folgenden Details hinzu.

   ```
   $citrixUrl: " https://docs.citrix.com "
   $appName: docs
   $DesktopGroupId: 1
   $desktopgroupname: <mydesktop23>
   ```

4. Führen Sie den folgenden Befehl aus:

   ```
   New-BrokerApplication – ApplicationType PublishedContent –
       CommandLineExecutable $citrixURL – Name $appName – DesktopGroup
        $dg.Uid
   ```

   Die App ist jetzt auf Citrix Workspace veröffentlicht.



5. Aktualisieren Sie die JSON-Richtliniendatei mit den App-Details (“docs”). Stellen Sie dabei Folgendes sicher:

   - `proxytraffic_v1` Wert ist immer auf gesetzt `secureBrowse`. Diese Einstellung stellt sicher, dass der Citrix Enterprise Browser den Datenverkehr mithilfe des Secure Browse-Protokolls über NetScaler Gateway zur Webseite tunnelt.
   - `browser_v1` Wert ist immer auf gesetzt `embeddedBrowser`. Diese Einstellung gilt nur, wenn der Citrix Enterprise Browser (CEB) als Arbeitsbrowser konfiguriert ist. Wenn diese Option auf gesetzt ist `embeddedBrowser`, werden Links zu konfigurierten Secure Private Access-Domänen in CEB geöffnet.
   - `secureBrowseAddress` Wert ist Ihre NetScaler Gateway-URL.


```
{
  "policies": [
    {
      "name": "Docs",
      "patterns": ["*.docs.netscaler.com/*"],
      "policy": {
        "watermark_v1": "enabled",
        "clipboard_v1": "disabled",
        "printing_v1": "disabled",
        "download_v1": "disabled",
        "upload_v1": "disabled",
        "keylogging_v1": "disabled",
        "screencapture_v1": "enabled",
        "proxytraffic_v1": "secureBrowse",
        "browser_v1" : "embeddedBrowser"
      }

    }],
  "system": {
    "secureBrowseAddress": "https://yournetscalergateway.com"
  }
}
```

6. Platzieren Sie die JSON-Richtliniendatei unter C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser.
7. Ändern Sie die Datei Web.config so, dass sie auf die Richtliniendatei verweist, die Sie aktualisiert haben.

```
<route name="webSecurePolicy" order="22" url="Resources/SecureBrowser/policy.json">
        <defaults>
          <add param="controller" value="BrowserPolicy" />
          <add param="action" value="BrowserResources" />
        </defaults>
        <data>
          <add name="endpointId" value="WebSecurePolicy" />
          <add name="endpointCapabilities" value="webSecurePolicy" />
          <add name="CommonData" factory="Citrix.DeliveryServices.Configuration.ObjectCollectionFactory, Citrix.DeliveryServices.Configuration, Version=3.23.0.0, Culture=neutral,
PublicKeyToken=e8b77d454fa2a856" path="citrix.deliveryservices/dazzleResources" property="commonData" />
        </data>
      </route>
```

8. Gehen Sie auf Ihrer on-premises NetScaler Gateway-Appliance wie folgt vor:
   - Ermöglichen Sie den clientlosen Zugriff auf die Apps. Sie können den clientlosen Zugriff global oder auf Sitzungsebene aktivieren.
   - Webadressenkodierung aktivieren
   - Secure Browse-Modus aktivieren
   - Domänen vom Umschreiben im clientlosen Zugriffsmodus ausschließen

Einzelheiten finden Sie unter Schritt 3: Aktivieren der Authentifizierung und Autorisierung mit dem on-premises NetScaler Gateway.

Ablauf für Endbenutzer

- Melden Sie sich bei StoreFront als Benutzer an, der auf Anwendungen in der PublishedContentApps-Bereitstellungsgruppe zugreifen kann.
- Sobald Sie sich angemeldet haben, müssen Sie die neue Anwendung mit dem Standardsymbol sehen. Sie können das Symbol nach Bedarf anpassen. Einzelheiten finden Sie unter https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.
- Wenn Sie auf die App klicken, wird die App im Citrix Enterprise Browser geöffnet.

Einzelheiten der Anwendungszugriffsrichtlinie

In der folgenden Tabelle sind die verfügbaren Zugriffsrichtlinienoptionen und ihre Werte aufgeführt.

Schlüsselname	Beschreibung der Richtlinie	Value
—	—	—
Bildschirmaufnahme_v1	Screenshotschutzfunktion für die Webseite aktivieren oder deaktivieren	aktiviert oder deaktiviert
keylogging_v1	Keyloggingschutz für die Webseite aktivieren oder deaktivieren	aktiviert oder deaktiviert
Wasserzeichen_v1	Wasserzeichen auf der Webseite anzeigen oder nicht anzeigen	aktiviert oder deaktiviert
Upload_v1	Uploads auf die Webseite aktivieren oder deaktivieren	aktiviert oder deaktiviert
drucken_v1	Drucken von der Webseite aus aktivieren oder deaktivieren	aktiviert oder deaktiviert
v1 herunterladen	Downloads von der Webseite aktivieren oder deaktivieren	aktiviert oder deaktiviert
Zwischenablage v1	Aktivieren oder deaktivieren Sie die Zwischenablage auf der Webseite	aktiviert oder deaktiviert
proxytraffic_v1	Legt fest, ob der Citrix Enterprise Browser den Datenverkehr über NetScaler Gateway mithilfe von Secure Browse auf die Webseite tunnelt oder den direkten Zugriff ermöglicht	direct oder SecureBrowse
Browser_v1	Gilt nur, wenn der Citrix Enterprise Browser als Arbeitsbrowser konfiguriert ist. Wenn embeddedBrowser festgelegt ist, werden Links zu konfigurierten Secure Private Access-Domänen im Citrix Enterprise Browser geöffnet	systemBrowser oder embeddedBrowser
Name	Name der veröffentlichten Web- oder SaaS-App	Es wird empfohlen, dass Sie denselben Namen verwenden, den Sie bei der Veröffentlichung der App eingegeben haben. Muster	Durch

Kommas getrennte Liste von Domainnamen, die sich auf diese App beziehen. Sie können auch Platzhalter verwenden. Diese Domänennamen werden verwendet, um Richtlinien auf die Apps vom Citrix Enterprise Browser anzuwenden.|Beispiele: "*.office.com/*", "*.office.net/*", "*.microsoft.com/*", "*.sharepoint.com*"|

> **Hinweis:**
>
> Keyloggingschutz und Screenshotschutz erfordern die Installation der App-Schutzfunktion, die in der Citrix Workspace-App enthalten ist.

Apps und Richtlinien mit dem Secure Private Access-Konfigurationstool konfigurieren —Legacy

August 26, 2024

Sie können das Secure Private Access-Konfigurationstool auf einem Citrix Virtual Apps and Desktops Delivery Controller verwenden, um schnell eine SaaS- oder Webanwendung zu erstellen. Darüber hinaus können Sie dieses Tool verwenden, um Anwendungseinschränkungen und das Routing von Datenverkehr festzulegen und ein NetScaler Gateway zu erstellen. Das Tool generiert Skriptdateien als Ausgabe, die auf den jeweiligen Computern ausgeführt werden können, um die Konfiguration bereitzustellen.

Unterstützte Produktversionen

Stellen Sie sicher, dass Ihr Produkt die Mindestanforderungen an die Version erfüllt.

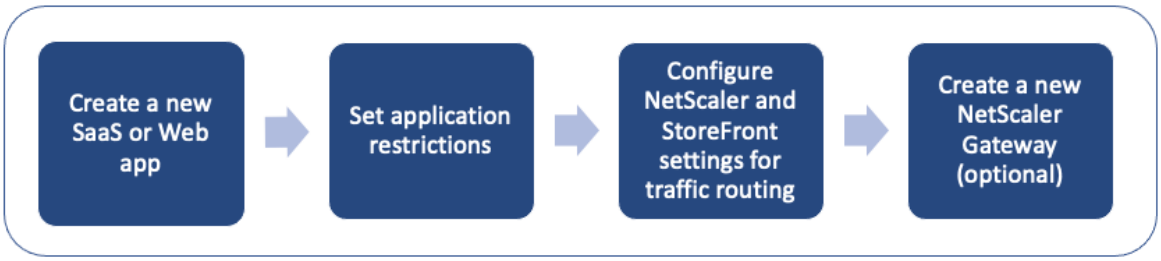
- Citrix Workspace-App
  - Windows - 2303 und höher
  - macOS - 2304 und höher
- Citrix Virtual Apps and Desktops —Unterstütztes LTSR und aktuelle Versionen
- StoreFront - LTSR 2203 oder Nicht-LTSR 2212 und höher
- NetScaler —12.1 und höher

Voraussetzungen für die Verwendung des Config-Tools

- Zugriff zum Herunterladen des Konfigurationstools von der Download-Seite.
- Administratorberechtigungen auf dem Citrix Virtual Apps and Desktops Controller zur Ausführung des Konfigurationstools.
- Auf dem Delivery Controller ist mindestens eine Bereitstellungsgruppe vorhanden.

Beginnen Sie mit dem Config-Tool

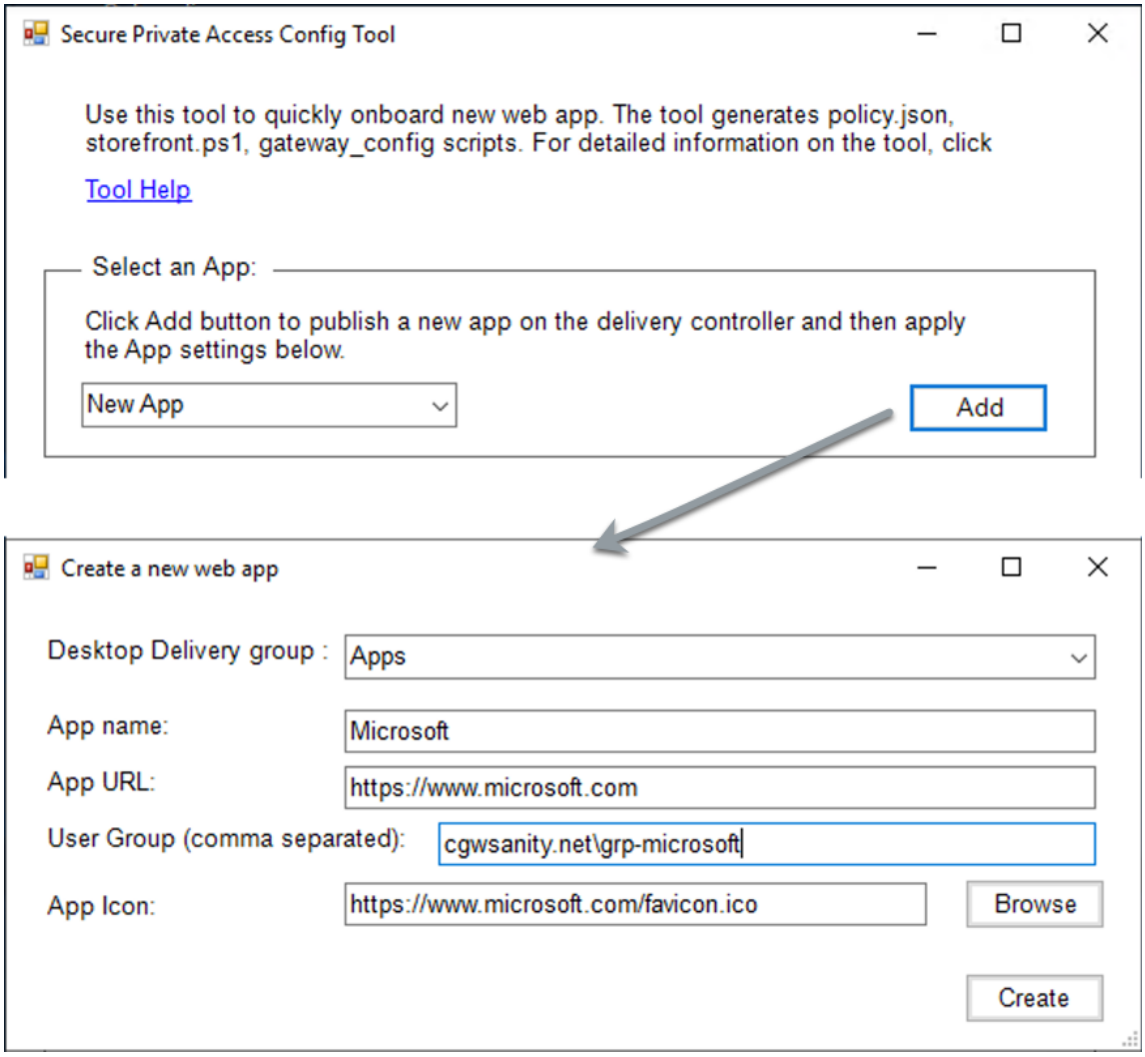
Sie können die folgenden Aufgaben mit dem Konfigurationstool ausführen.



- Veröffentlichen Sie eine neue Anwendung
- Legen Sie Anwendungseinschränkungen fest
- Konfiguration der StoreFront- und NetScaler Gateway-Einstellungen
- Neues NetScaler Gateway konfigurieren

Veröffentlichen Sie eine neue Anwendung

1. Führen Sie das Konfigurationstool aus.
2. Wählen Sie im Abschnitt **App auswählen** in der Dropdownliste die Option **Neue App** aus, und klicken Sie dann auf **Hinzufügen**.



3. Schließen Sie die App-Konfiguration ab.

   - **Desktop-Bereitstellungsgruppe**: Wählen Sie die Bereitstellungsgruppe aus, für die diese App zugänglich gemacht werden muss.
     Alle vorhandenen Bereitstellungsgruppen werden in der Desktop-Bereitstellungsgruppe aufgeführt.
   - **App-Name**: Geben Sie den App-Namen ein.
   - **App-URL**: Geben Sie die URL für die App an.
   - **Benutzergruppe**: Geben Sie sowohl den Domainnamen als auch den Gruppennamen im Format „Domäne\ Gruppe“ein. Benutzergruppen können Leerzeichen enthalten. Zum Beispiel „cgwsanity.net\ grp-microsoft“, „cgwsanity.net\ grp microsoft“.
     Diese Gruppen müssen bereits im Active Directory existieren.

> **Note:**
>
> – Built-in domain security groups such as “Domain Users”or “Domain Admins”are not supported. Only the manually created user groups must be used.
> – The user group is only used in NetScaler Gateway authorization policies and not for app assignments in Citrix Virtual Apps and Desktops. Hence, the user group that you enter here is not visible in Studio.

- **App-Symbol**: Das Tool verwendet favicon.ico der URL, falls es erkannt wird. Der Administrator kann die Symbole bei Bedarf auch anpassen. Wenn vom Administrator kein Symbol bereitgestellt wird, wird der App das Standardsymbol zugewiesen.

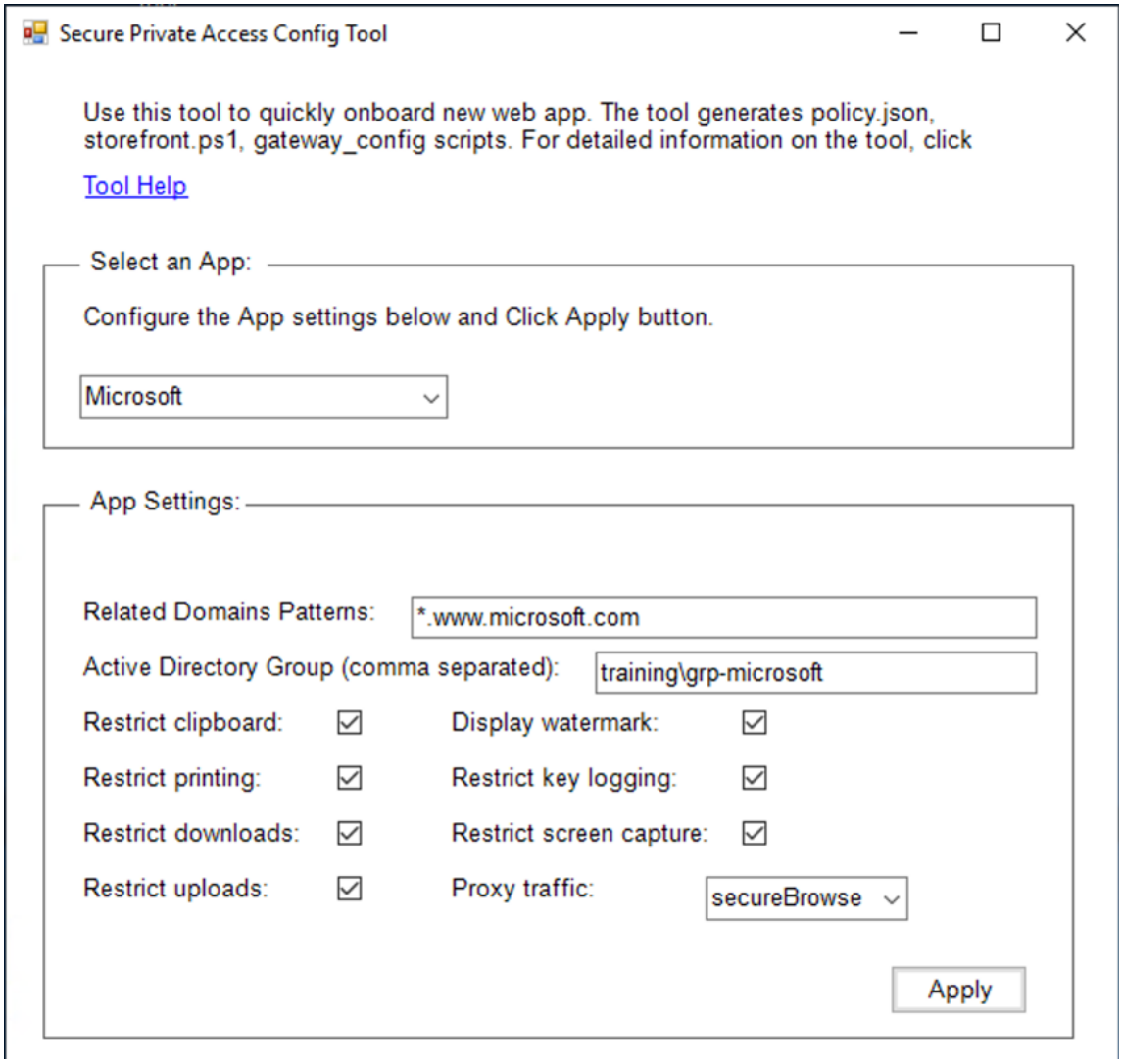
4. Klicken Sie auf **Erstellen**.

Die Anwendung wird auf dem Delivery Controller veröffentlicht und steht den Benutzern in den Benutzergruppen in StoreFront zur Verfügung.

Legen Sie Anwendungseinschränkungen fest

Nachdem Sie eine neue Anwendung veröffentlicht haben, können Sie Einschränkungen für diese App aktivieren oder deaktivieren.

1. Wählen Sie im Abschnitt **App auswählen** die App aus der Dropdown-Liste aus, für die Sie die Einstellungen erzwingen möchten.



2. Konfigurieren Sie die App-Einstellungen im Abschnitt **App-Einstellungen**.

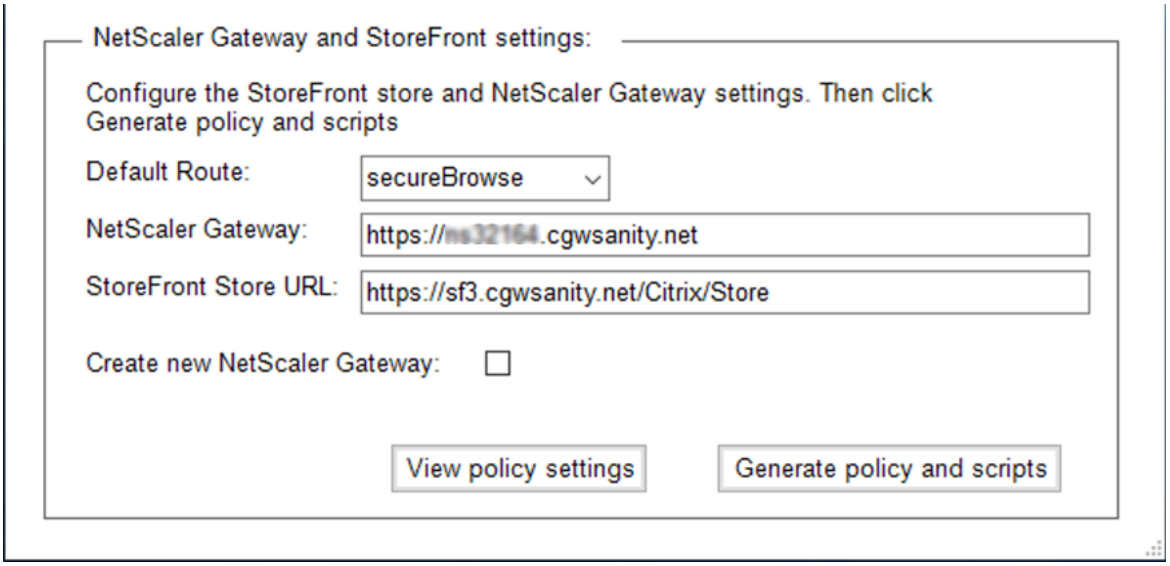
   - **Muster verwandter Domänen**: Die zugehörige Domänen-URL wird basierend auf der App-URL automatisch ausgefüllt. Admins können zusätzliche Domains hinzufügen, die durch ein Komma getrennt sind.
   - **Active Directory-Gruppe**: Geben Sie die Gruppen ein, für die diese Anwendung zugänglich sein muss. Dies ist ein Pflichtfeld.
     Sie können mehrere Gruppen eingeben, die durch ein Komma getrennt sind. Diese Gruppen müssen mit den im Active Directory verfügbaren Gruppen übereinstimmen. Die Gruppennamen, die Sie hier eingeben, wurden nicht überprüft. Daher ist es wichtig, dass Sie darauf achten, die Gruppennamen so einzugeben, dass sie mit dem übereinstimmen, was im Active Directory vorhanden ist.
   - **App-Einstellungen**: Alle App-Einstellungen sind standardmäßig eingeschränkt (ausgewählt). Sie können die entsprechenden Einstellungen, die Sie für die Benutzergruppen wünschen, auswählen oder deaktivieren.

- **Proxyverkehr**: Wählen Sie SecureBrowse aus. Diese Einstellung ermöglicht es dem Citrix Enterprise Browser, den Datenverkehr über NetScaler Gateway zur Webseite zu tunneln.

3. Klicken Sie auf **Anwenden**.

Konfiguration der StoreFront- und NetScaler Gateway-Einstellungen

Sie können Einstellungen für das Routing von Datenverkehr über NetScaler Gateway konfigurieren. Im Abschnitt Gateway- und StoreFront-Einstellungen können Sie ein vorhandenes NetScaler Gateway konfigurieren oder ein neues NetScaler **Gateway** erstellen.



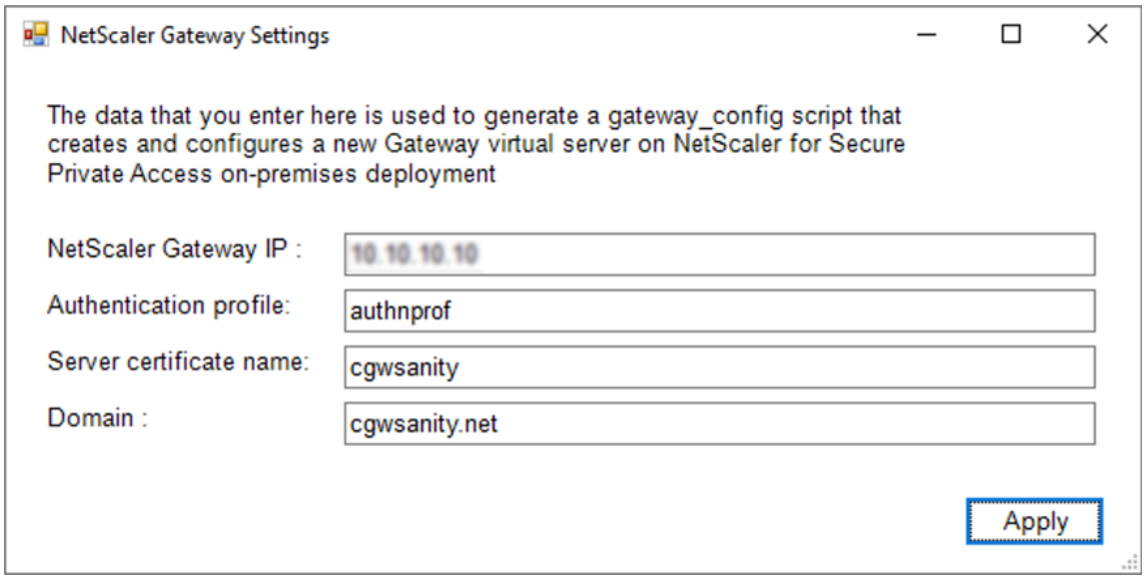
- **Standardroute**: Wenn keine Richtlinie für die App definiert ist, wird die Standardroute für die Apps angewendet.
  - **SecureBrowse**: Der Citrix Enterprise Browser tunnelt den Datenverkehr über NetScaler Gateway zur Webseite.
  - **Direkt**: Der Citrix Enterprise Browser ermöglicht den direkten Zugriff auf die Apps.
- **NetScaler Gateway**: Geben Sie die NetScaler Gateway-URL ein.
- **StoreFront-Store-URL**: Geben Sie die vollständige StoreFront-Store-URL ein. Beispiel: `http://<directory path>/Citrix/<StoreName>`. Sie können die URL von der StoreFront-Konsole abrufen.
- **(Optional)**Neues Gateway erstellen**: Aktivieren Sie das Kontrollkästchen, um ein neues NetScaler Gateway zu erstellen, und klicken Sie auf Erstellen.**

Neues NetScaler Gateway erstellen (optional)

Sie können ein neues NetScaler Gateway erstellen, wenn Sie die vorhandenen Gateway-Einstellungen nicht ändern möchten.

Wenn Sie bereits über ein NetScaler Gateway verfügen, können Sie die Autorisierungsrichtlinien und Bindungen für die Apps mithilfe des Konfigurationstools konfigurieren.

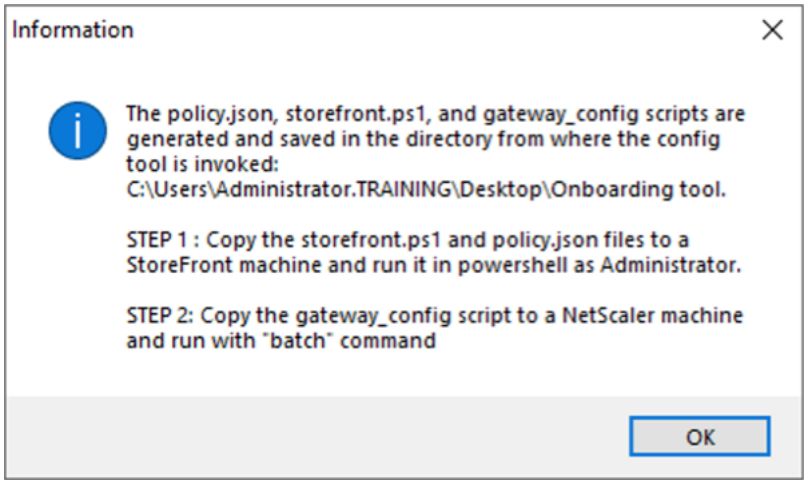
1. Sie müssen die folgenden Details für das neue NetScaler Gateway eingeben. Das Tool überprüft die Werte, die Sie beim Erstellen eines neuen Gateway eingeben, nicht. Daher ist es wichtig, dass Sie darauf achten, genaue Werte einzugeben.



   - **Gateway-IP**: IP-Adresse des NetScaler Gateway.
   - **Authentifizierungsprofil**: Geben Sie den Namen des Authentifizierungsprofils ein, der bereits auf NetScaler konfiguriert ist. Weitere Informationen finden Sie unter Authentifizierungsprofile.
   - **Name des Serverzertifikats**: Geben Sie den Namen des SSL-Zertifikats ein, der bereits auf NetScaler konfiguriert ist. Einzelheiten finden Sie unter SSL-Zertifikate.
   - **Domäne**: Wird für SSO für Apps im internen Netzwerk verwendet. Einzelheiten finden Sie unter VPN-Sitzungsaktion.

2. Klicken Sie auf **Anwenden**.
3. Klicken Sie auf **Richtlinie und Skripts generieren**.

   Die Dateien policy.json, storefront.ps1 und gateway_config werden generiert und an dem Ort gespeichert, von dem aus Sie das Konfigurationstool ausgeführt haben.



Wenn Sie die Datei gateway_config in einer unterstützten Anwendung öffnen, können Sie zwei Abschnitte in der Ausgabedatei sehen.

- Abschnitte zur NetScaler Gateway-Konfiguration (gilt nur, wenn ein neues Gateway erstellt wird)
- Abschnitte, die sich auf Autorisierungsrichtlinien, Benutzergruppen und verbindliche Richtlinien für die Benutzergruppen beziehen.

Die folgende Abbildung zeigt die Datei gateway_config einer neuen NetScaler Gateway-Konfiguration.


```
##################################################################################################
#1. Upload file to NetScaler (e.g. to /var/tmp)
#2. Run batch command (e.g. batch -fileName /var/tmp/gateway_config -outfile /var/tmp/gateway_config_output)
#3. Analyze output (e.g. cat /var/tmp/gateway_config_output)
##################################################################################################

# Enable NS features
enable ns feature SSL SSLVPN AAA

# Add Gateway
add vpn vserver _XD_SPAGateway_443 SSL [redacted] -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile
-deploymentType ICA_STOREFRONT -vserverFqdn gwalextest.spaopdev.local -authnProfile spaopdev_auth_prof -icaOnly OFF

# Add excluded domains
bind policy patset ns_cvpn_default_bypass_domains corealextest.spaopdev.local
bind policy patset ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_OS_SPAGateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF
-wihome "http://corealextest.spaopdev.local/Citrix/StoreWeb" -ClientChoices OFF -ntDomain spaopdev.local -clientlessVpnMode ON
-clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "http://corealextest.spaopdev.local" -sfGatewayAuthType domain

add vpn sessionAction AC_WB_SPAGateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF
-wihome "http://corealextest.spaopdev.local/Citrix/StoreWeb" -ClientChoices OFF -ntDomain spaopdev.local -clientlessVpnMode ON
-clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "http://corealextest.spaopdev.local" -sfGatewayAuthType domain

# Add session policies
add vpn sessionPolicy PL_OS_SPAGateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")" AC_OS_SPAGateway
add vpn sessionPolicy PL_WB_SPAGateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT" AC_WB_SPAGateway

# Bind policies to vserver
bind vpn vserver _XD_SPAGateway_443 -policy PL_OS_SPAGateway -priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _XD_SPAGateway_443 -policy PL_WB_SPAGateway -priority 110 -gotoPriorityExpression NEXT -type REQUEST

# Bind SSL cert to GW
bind ssl vserver _XD_SPAGateway_443 -certkeyName spaopdev

# Add default authorization policies
add authorization policy ALLOW_STOREFRONT "HTTP.REQ.HOSTNAME.CONTAINS(\"corealextest.spaopdev.local\")" ALLOW
add authorization policy DENY_ALL true DENY

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "SPAOP users"
bind aaa group "SPAOP users" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "SPAOP users" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.google.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.google.com\")" ALLOW

unbind aaa group "SPAOP users" -policy www.google.com
bind aaa group "SPAOP users" -policy www.google.com -priority 100 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupab"
bind aaa group "groupab" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupab" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

unbind aaa group "groupab" -policy www.google.com
bind aaa group "groupab" -policy www.google.com -priority 110 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupxy"
bind aaa group "groupxy" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupxy" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.microsoft.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.microsoft.com\")" ALLOW

unbind aaa group "groupxy" -policy www.microsoft.com
bind aaa group "groupxy" -policy www.microsoft.com -priority 120 -gotoPriorityExpression END

# Save
save ns config
```

Die folgende Abbildung zeigt die Datei gateway_config einer aktualisierten NetScaler Gateway-Konfiguration.


```
##########################################################################################
#1. Upload file to NetScaler (e.g. to /tmp)
#2. Run batch command (e.g. batch -fileName /tmp/Gateway_config -outfile /tmp/Gateway_config_output)
#3. Analyze output (e.g. cat /tmp/Gateway_config_output)
##########################################################################################

# Add default authorization policies
add  policy ALLOW_STOREFRONT "HTTP.REQ.HOSTNAME.CONTAINS(\"corealextest.spaopdev.local\")" ALLOW
add  policy DENY_ALL true DENY

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "SPAOP users"
bind aaa group "SPAOP users" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "SPAOP users" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.google.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.google.com\")" ALLOW

unbind aaa group "SPAOP users" -policy www.google.com
bind aaa group "SPAOP users" -policy www.google.com -priority 100 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupab"
bind aaa group "groupab" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupab" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

unbind aaa group "groupab" -policy www.google.com
bind aaa group "groupab" -policy www.google.com -priority 110 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupxy"
bind aaa group "groupxy" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupxy" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.microsoft.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.microsoft.com\")" ALLOW

unbind aaa group "groupxy" -policy www.microsoft.com
bind aaa group "groupxy" -policy www.microsoft.com -priority 120 -gotoPriorityExpression END

# Save
save ns config
```

Konfiguration von StoreFront mit dem neuen NetScaler Gateway

- Für die Konfiguration der StoreFront- und NetScaler Gateway-Einstellungen im Tool benötigen Sie Folgendes:
  - NetScaler Gateway-FQDN
  - StoreFront-Store-URL
- Anforderungen an die StoreFront-Konfiguration:
  - NetScaler Gateway: Der Remotezugriff ist aktiviert.
  - Die Passthrough-Authentifizierung von NetScaler Gateway ist aktiviert.
  - Active Directory: Administratorzugriff zum Hinzufügen oder Aktualisieren von Benutzern oder Gruppen sowie zum Konfigurieren von Authentifizierungsprofilen oder -richtlinien auf NetScaler.

Weitere Informationen finden Sie unter Integrieren von NetScaler Gatewayin StoreFront.

Verwenden Sie die Ausgabedateien des Konfigurationstools, um die Konfiguration von Apps und Richtlinien bereitzustellen

Das Config-Tool generiert die folgenden Dateien. Diese Dateien werden in dem Ort/Verzeichnis gespeichert, in dem das Tool hochgeladen und ausgeführt wird.

- policy.json
- storefront.ps1
- gateway_config

1. Kopieren Sie storefront.ps1-Dateien nach StoreFront.
2. Führen Sie das storefront.ps1-Skript auf PowerShell als Administrator aus.

   Das Skript erstellt einen Ordner Resources\ SecureBrowser, falls er nicht bereits im Pfad unter Store verfügbar ist.

   Das Skript aktualisiert auch die Datei web.config für die Route für die Datei policy.json.
3. Kopieren Sie die Datei policy.json in den Ordner Resources\ SecureBrowser, den storefront.ps1 unter dem Store erstellt.
4. Kopieren Sie die gateway_config in einen NetScaler und führen Sie das Skript mit dem folgenden Batch-Befehl auf der NetScaler-CLI aus.

   ```
   batch -fileName /var/tmp/gateway_config -outfile /var/tmp/gateway_config_o
   ```

> **Hinweis:**
>
> - Wenn eine Konfigurationsänderung im Tool vorgenommen wird, müssen die Skripts und Richtlinien neu generiert werden. Sie müssen die Datei policy.json erneut in den Ordner Resources\ SecureBrowser auf dem StoreFront-Computer kopieren und das gateway_config-Skript muss erneut auf dem NetScaler ausgeführt werden.
> - Sie müssen storefront.ps1 nicht erneut ausführen, wenn der Storename/die URL nicht geändert wird.

Zusätzliche Referenzen

Weitere Informationen finden Sie in der folgenden Dokumentation.

- Secure Private Access for on-premises
- Bereitstellungsleitfaden: Secure Private Access On-Premises