# Citrix Secure Private Access — Vor Ort

**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

**Was ist neu** 2

**Bekannte Probleme** 2

**Secure Private Access-Installationsprogramm** 4

**Aktualisieren Sie die Datenbank mithilfe von Skripten** 9

**Secure Private Access einrichten** 9

**Konfigurieren von NetScaler Gateway** 17

**Konfigurieren Sie Anwendungen** 23

**Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen** 26

**Ablauf für Endbenutzer** 29

**Sichere Private Access-Integration mit Web Studio-Integration** 32

**Einstellungen nach der Installation verwalten** 33

**Dashboard-Übersicht** 35

**Behebung von Fehlern** 37

**Secure Private Access deinstallieren** 44

**Secure Private Access 2308-Kompatibilität mit älteren Versionen** 45

**Benachrichtigungen von Drittanbietern** 48

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Was ist neu

December 27, 2023

### Oktober 2023

#### Citrix Secure Private Access for on-premises –Preview

Citrix Secure Private Access for on-premises ist jetzt als Vorschauversion verfügbar. Die lokale Secure Private Access-Lösung umfasst eine Benutzeroberfläche für die Administratorkonsole mit vollem Funktionsumfang, die dem Secure Private Access Service ähnelt. Einzelheiten finden Sie unter Secure Private Access for on-premises - Preview.

# Bekannte Probleme

February 16, 2024

Für Citrix Secure Private Access for on-premises sind die folgenden Probleme bekannt:

### Domänencontroller-Konfigurationen

- Die unidirektionale Vertrauensstellung zwischen Domänen innerhalb derselben Gesamtstruktur oder zwischen verschiedenen Gesamtstrukturen wird nicht unterstützt. Die Secure Private Access for On-Premises-Lösung funktioniert nicht, wenn die beiden folgenden Bedingungen erfüllt sind.
  - Die Domäne der Maschine, in der Secure Private Access for on-premises installiert ist, unterscheidet sich von der Domäne des Administrators, der bei Secure Private Access angemeldet ist.
  - Zwischen der Domäne der Maschine und der Domäne des Benutzers ist kein Vertrauen konfiguriert.
- Wenn sAMAccountName und UPN unterschiedlich sind, schlägt die Aufzählung fehl.

### NetScaler Gateway

Der virtuelle SSL-Server mit SSL-Profilkonfiguration wird im folgenden Szenario nicht unterstützt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Der Kunde verwendet NetScaler Gateway 13.1-48.47 und höher oder 14.1-4.42 und höher.
- Der Schalter `ns_vpn_enable_spa_onprem` ist aktiviert.

Workaround:

Binden Sie die im SSL-Profil konfigurierten SSL-Parameter direkt an den virtuellen SSL-Server oder deaktivieren Sie den Schalter `ns_vpn_enable_spa_onprem`.

Einzelheiten zum Umschalten finden Sie unter Unterstützung für Smart Access-Tags.

### RFWeb//Workspace für das Web

RfWeb / Workspace für Web wird nicht unterstützt. Obwohl die Apps aufgelistet sind, schlägt der Start einer App möglicherweise fehl.

### Anwendungssymbole

Nur das ICO-Symbolformat wird unterstützt. PNG, JPEG und andere Formate werden nicht unterstützt.

### Verwaltung durch Administratoren

- Die Änderungen der RBAC-Rolle des Administrators werden erst übernommen, wenn die aktuelle Sitzung ungültig wird (durch Abmelden oder Ablaufen des Tokens).
- Admin-Benutzer dürfen nicht Teil der Standard-AD-Gruppe „Domain-Benutzer“sein, da die Authentifizierung für diese Benutzer fehlschlägt.

### Upgrades

Ein Build-to-Build-Upgrade wird nicht unterstützt. Secure Private Access for on-premises fordert Sie auf, die vorhandene Installation zu entfernen und im Build-to-Build-Upgrade erneut zu installieren.

### StoreFront

- Unter **Stores > Unified Experience konfigurieren**muss der Standardempfänger für Website auf<`StoreName`>/Citrix/ Web konfiguriert sein. In früheren Versionen von StoreFront ist der Standardempfänger für Website auf einen leeren Wert festgelegt, der für Secure Private Access nicht funktioniert. Außerdem wird die frühere Version der Receiver-Benutzeroberfläche auf dem Client angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Wenn Sie die StoreFront-Versionen 2308 oder früher verwenden, wird auf der Seite **Stores > Manage Delivery Controllers** der Secure Private Access Plug-in-Typ als **XenMobile** angezeigt. Dies hat keinen Einfluss auf die Funktionalität.

### Protokollierung

- Die Generierung von Supportpaketen für den Cluster wird nicht unterstützt.
- Die Log-Ordner für Admin- und Runtime-Dienste dürfen nicht gelöscht werden. Secure Private Access kann nicht neu erstellt werden, wenn diese Ordner gelöscht werden.

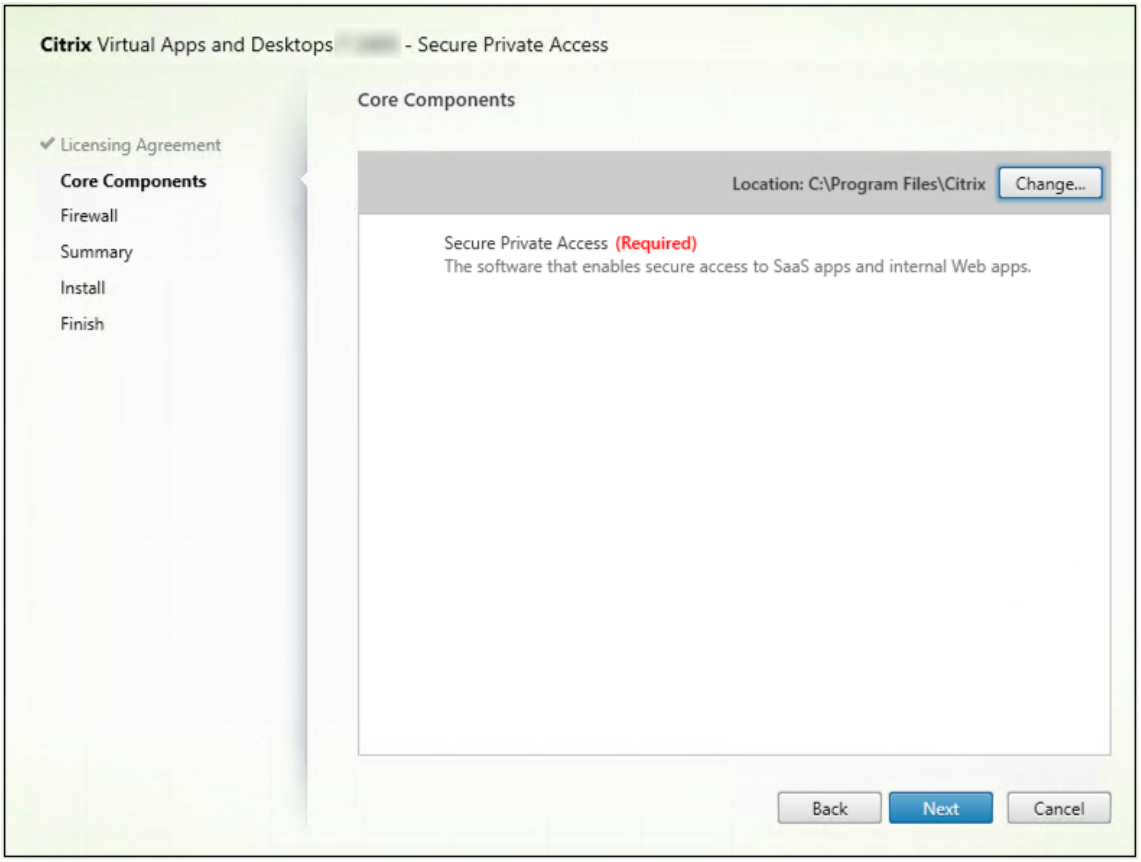
## Secure Private Access-Installationsprogramm

February 16, 2024

Sie können Secure Private Access mithilfe von SecurePrivateAccessSetup_2308.exe installieren.

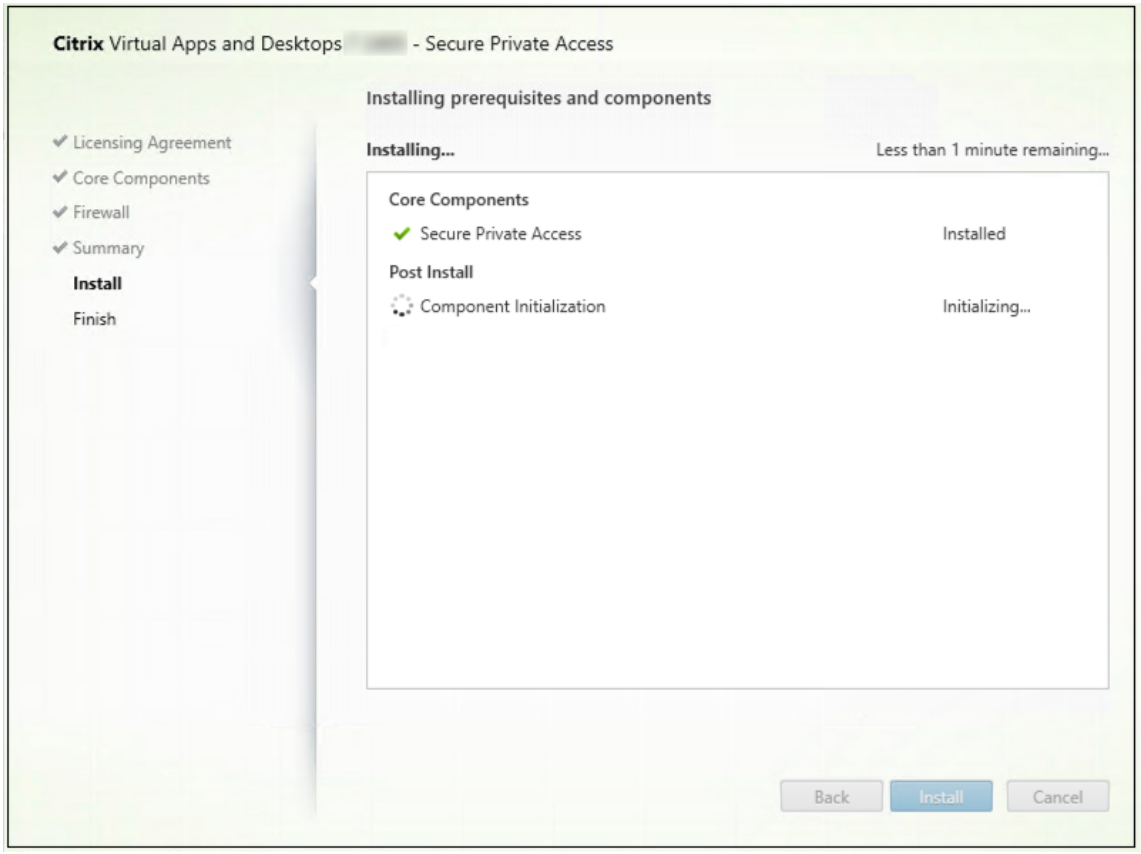
1. Laden Sie das Citrix Secure Private Access-Installationsprogramm von herunter https://www.citrix.com/downloads/citrix-early-access-release/.
2. Führen Sie die EXE-Datei als Administrator auf einer Maschine aus, die der Domäne beigetreten ist, vorzugsweise auf derselben Maschine, auf der StoreFront installiert ist.

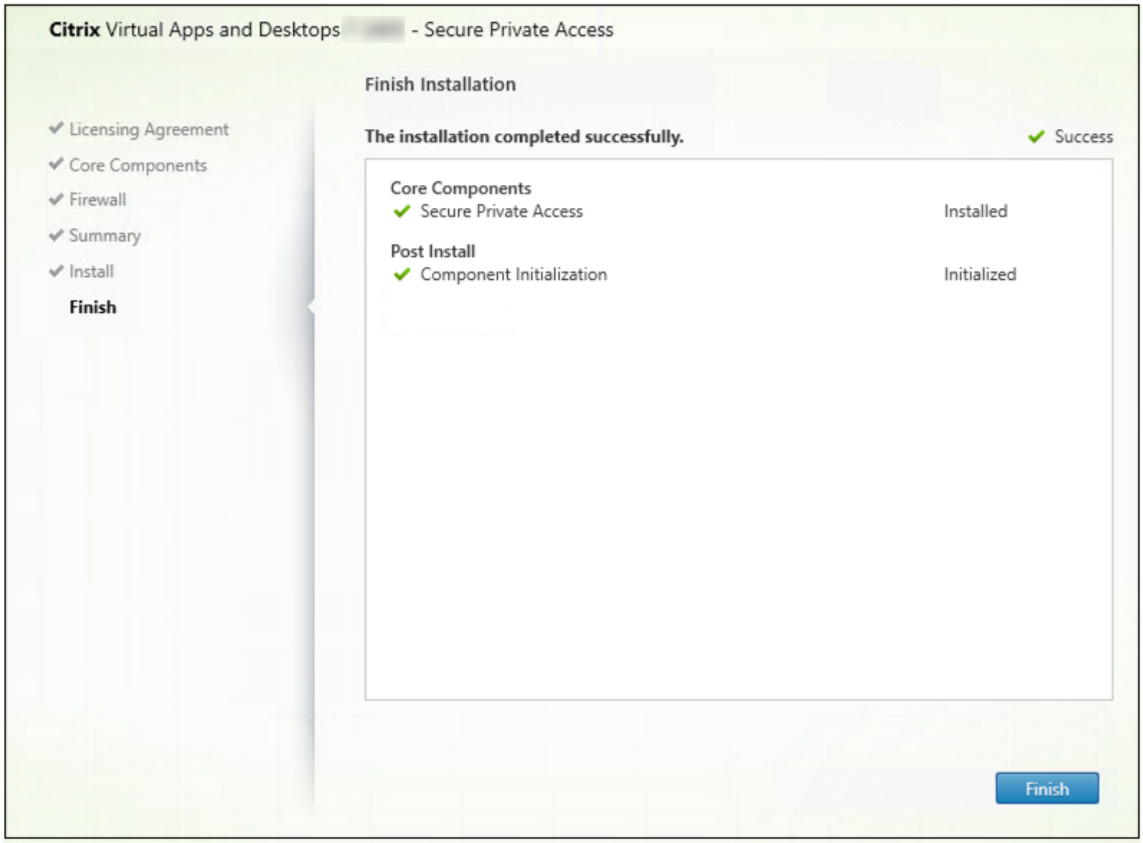
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




3. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen.

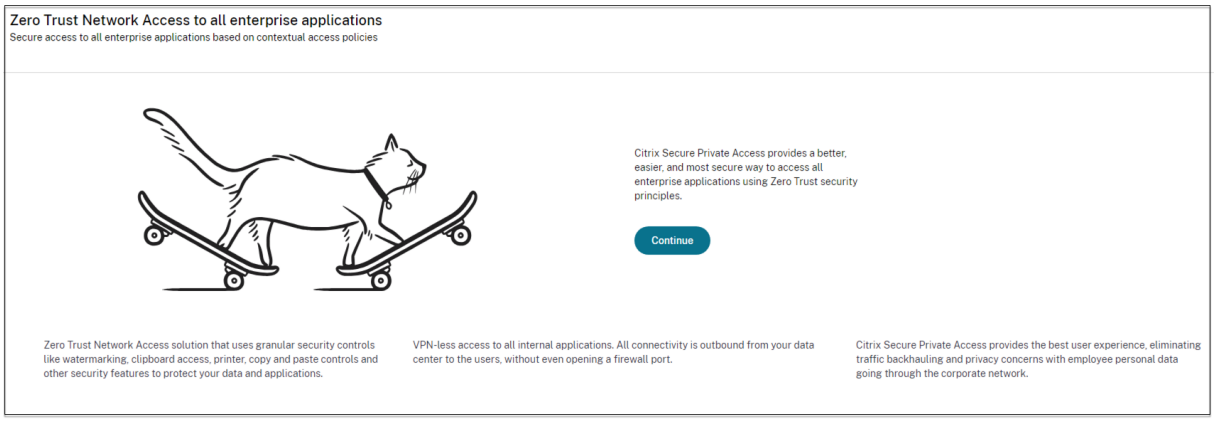
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



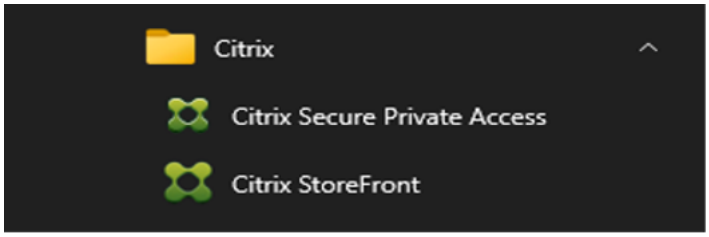




© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Sobald die Installation abgeschlossen ist, wird die Admin-Konsole für die erstmalige Einrichtung automatisch im Standard-Browserfenster geöffnet. Sie können auf **Weiter** klicken, um Secure Private Access einzurichten.




Sie können die Secure Private Access-Verknüpfung auch im Desktop-Startmenü sehen (**Citrix > Citrix Secure Private Access)**.




## SSO zur Admin-Konsole

Es wird empfohlen, die Kerberos-Authentifizierung für den Browser zu konfigurieren, den Sie für die Secure Private Access-Administratorkonsole verwenden. Dies liegt daran, dass Secure Private Access die integrierte Windows-Authentifizierung (IWA) für die Administratorauthentifizierung verwendet.

Wenn die Kerberos-Authentifizierung nicht eingerichtet ist, werden Sie vom Browser aufgefordert, Ihre Anmeldeinformationen einzugeben, wenn Sie auf die Secure Private Access-Administratorkonsole zugreifen.

- Wenn Sie Ihre Anmeldeinformationen eingeben, aktivieren Sie die IWA-Anmeldung (Integrated Windows Authentication).
- Wenn Sie Ihre Anmeldeinformationen nicht eingeben, wird die Secure Private Access-Anmeldeseite angezeigt.

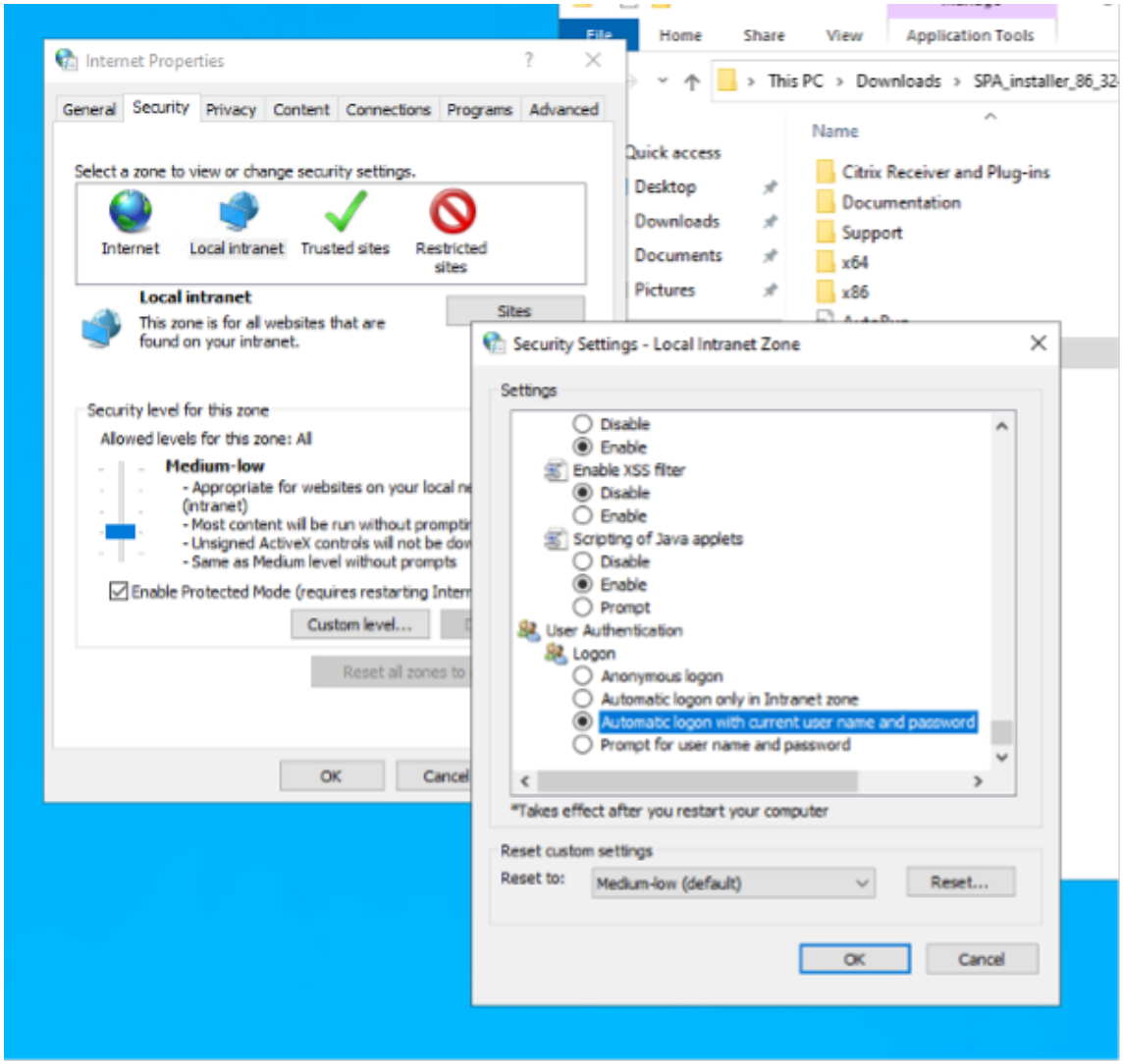
Sie müssen sich in der Admin-Konsole anmelden, um mit der Einrichtung von Secure Private Access fortzufahren. Sie können Secure Private Access mit jedem Benutzer einrichten, der derselben Domäne wie der Installationscomputer angehört, vorausgesetzt, der Benutzer verfügt über lokale Administratorrechte auf dem Installationscomputer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Führen Sie für die Google Chrome- und Microsoft Edge-Browser die folgenden Schritte aus, um Kerberos zu aktivieren.

1. Öffnen Sie die **Internetoptionen**.
2. Wählen Sie die Registerkarte **Sicherheit** und klicken Sie auf **Lokale Intranetzone**.
3. Klicken Sie auf **Websites** und fügen Sie die Secure Private Access-URL hinzu.

   Sie können auch einen Platzhalter verwenden, wenn Sie Secure Private Access auf mehreren Maschinen installieren möchten. Zum Beispiel “https://*.fabrikam.local”.
4. Klicken Sie auf **Stufe anpassen** und wählen Sie unter **Benutzerauthentifizierung > Anmeldung** die Option **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort** aus.




> **Hinweis:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Wenn Sie Chrome-Inkognito-Sitzungen verwenden, erstellen Sie einen DWORD-Registrierungsschlüssel Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AmbientAuthenticationInPrivateM und legen Sie ihn auf den Wert 1 fest.
- Sie müssen alle Chrome-Fenster (einschließlich Nicht-Inkognito-Fenster) neu starten, bevor Kerberos für den Inkognito-Modus aktiviert wird.
- Informationen zu anderen Browsern finden Sie in der Dokumentation des jeweiligen Browsers zur Kerberos-Authentifizierung.

### Nächste Schritte

- Secure Private Access einrichten
- NetScaler Gateway konfigurieren
- Anwendungen konfigurieren
- Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen

## Aktualisieren Sie die Datenbank mithilfe von Skripten

December 27, 2023

Sie können das Admin-Konfigurationstool verwenden, um die Datenbank-Upgrade-Skripts für das Secure Private Access-Plug-in herunterzuladen.

1. Öffnen Sie die PowerShell oder das Eingabeaufforderungsfenster mit Administratorrechten.
2. Ändern Sie das Verzeichnis in den Ordner Admin\ AdminConfigTool im Secure Private Access-Installationsordner (z. B. cd “C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ AdminConfigTool“).
3. Führen Sie den folgenden Befehl aus:

   ```
   .\AdminConfigTool.exe /DOWNLOAD_UPGRADE_DB_SCRIPTS <output folder
   >
   ```

## Secure Private Access einrichten

February 16, 2024

Sie können Secure Private Access einrichten, indem Sie eine neue Site erstellen oder einer vorhandenen Site beitreten. In beiden Szenarien können Sie die Web-Admin-Konsole verwenden, um die Secure Private Access-Umgebung einzurichten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Secure Private Access durch Erstellen einer neuen Site einrichten
- Secure Private Access durch Beitreten zu einer vorhandenen Site einrichten

### Voraussetzungen

Der SQL-Datenbankserver muss installiert werden, bevor eine Site erstellt wird.

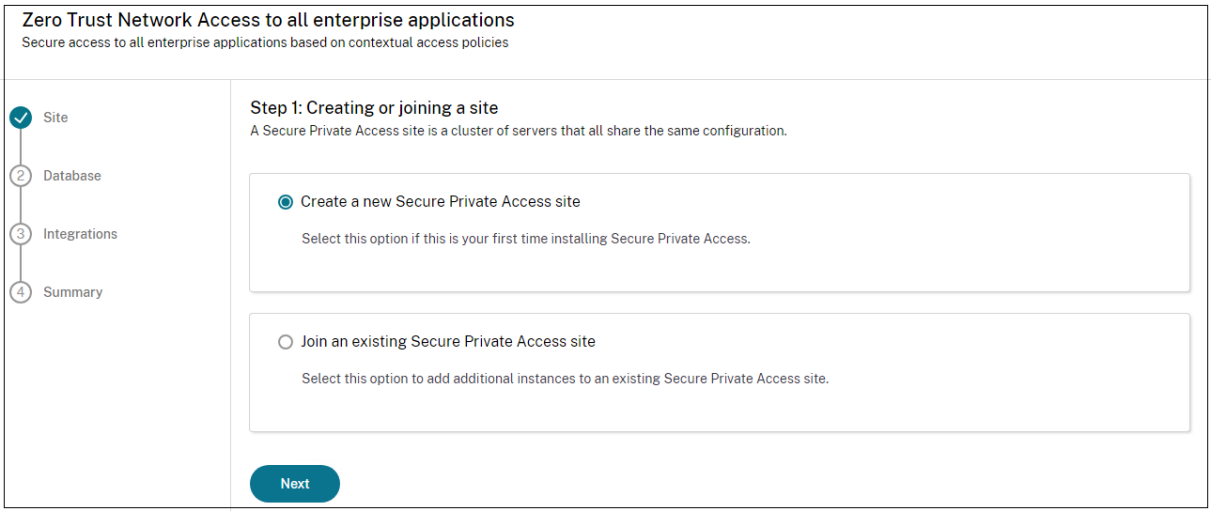
Secure Private Access durch Erstellen einer neuen Site einrichten

## Secure Private Access durch Erstellen einer neuen Site einrichten

### Schritt 1: Richten Sie eine Secure Private Access-Site ein

Eine Site ist der Name Ihrer Secure Private Access-Bereitstellung. Sie können entweder eine Site erstellen oder einer vorhandenen Site beitreten.

1. Starten Sie die Web-Admin-Konsole für sicheren privaten Zugriff.
2. Auf der Seite **Website erstellen oder einer Site beitretenist die Option Neue Secure Private Access-Site** erstellen standardmäßig ausgewählt.
3. Klicken Sie auf **Weiter**.




Wenn Sie eine Site erstellen möchten, müssen Sie automatisch oder manuell eine Datenbank für die neue Site konfigurieren, da die dem Site-Namen entsprechende Datenbank im Setup möglicherweise nicht verfügbar ist.

### Schritt 2: Datenbanken konfigurieren

Sie müssen eine Datenbank für die neue Secure Private Access-Site erstellen. Dies kann manuell oder automatisch erfolgen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

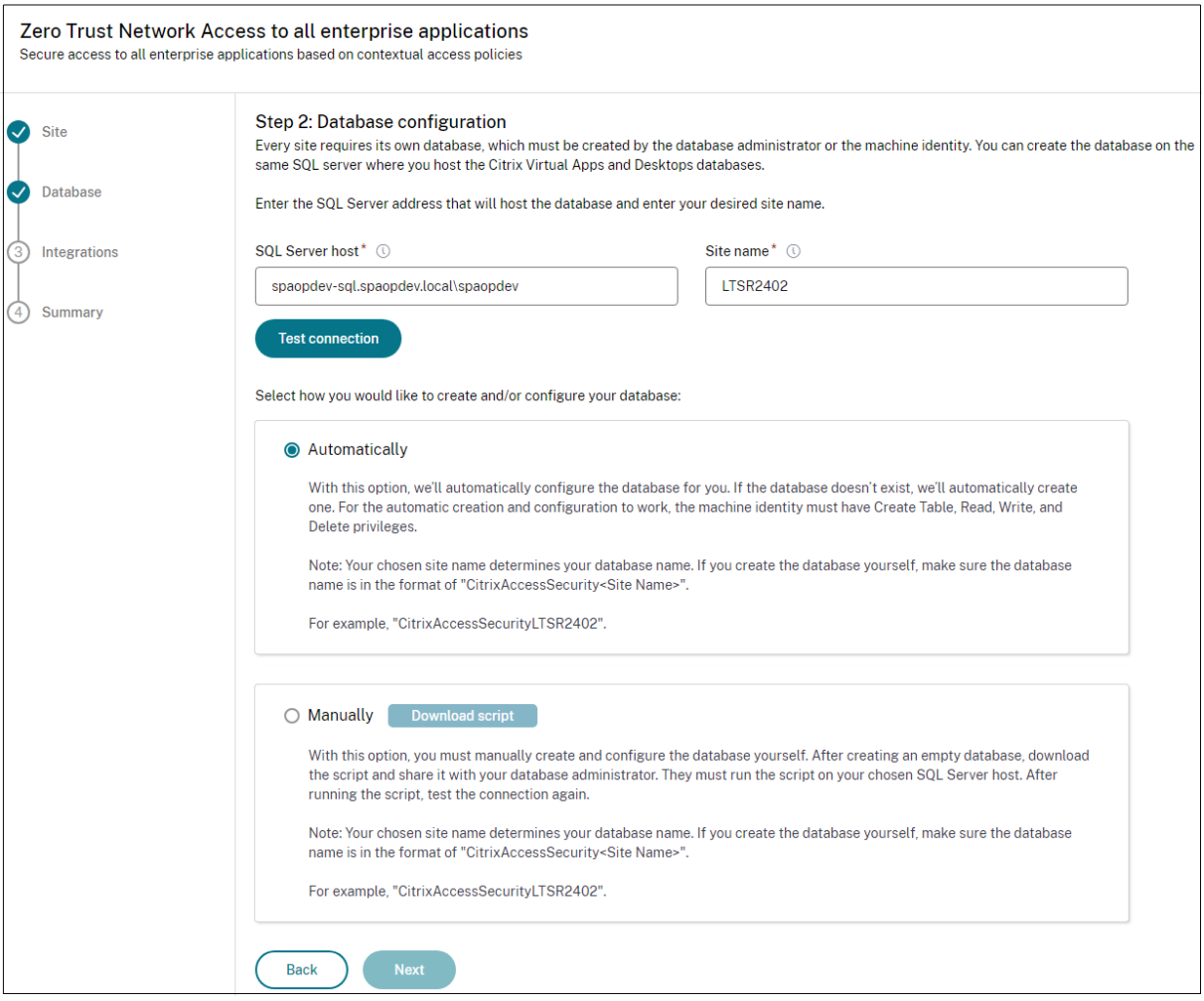
1. Geben Sie im Feld **SQL Server-Host** den Serverhostnamen ein. Beispiel: `sql1.fabrikam.local\citrix`.

   Datenbankadressen können in einem der folgenden Formate angegeben werden:

   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   Weitere Informationen finden Sie unter Datenbanken.

2. Geben Sie im Feld **Site** einen Namen für die Secure Private Access-Site ein.
3. Klicken Sie auf **Konnektivität testen**, um zu überprüfen, ob die SQL Server-Instanz gültig ist, und um zu bestätigen, dass die angegebene Datenbank für die Site existiert.




**Hinweis:**

- Wenn ein SQL-Server für die Site nicht verfügbar ist, schlägt die Konnektivitätsprüfung fehl.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Wenn ein SQL-Server verfügbar ist, die Datenbank jedoch nicht existiert, ist die Konnektivitätsprüfung erfolgreich. Es wird jedoch eine Warnmeldung angezeigt.
- Secure Private Access verwendet die Windows-Authentifizierung mithilfe der Computeridentität, um sich bei einem SQL-Server zu authentifizieren.

**Automatische Konfiguration**:

- Sie können die Option **Automatische Konfiguration** nur verwenden, wenn die Maschinenidentität über die erforderlichen Datenbankberechtigungen verfügt.
- Wenn eine Datenbank an der angegebenen Adresse nicht existiert, wird automatisch eine Datenbank erstellt.
- Wenn Sie eine Datenbank erstellen, stellen Sie sicher, dass sie leer ist, aber über die erforderlichen Datenbankberechtigungen verfügt. Einzelheiten zu den Rechten finden Sie unter Zum Einrichten von Datenbanken erforderliche Berechtigungen.

**Manuelle Konfiguration**:

Sie können die Option **Manuelle Konfiguration** verwenden, um die Datenbanken einzurichten.

Bei der manuellen Konfiguration müssen Sie zuerst die Skripten herunterladen und dann die Skripten auf dem Datenbankserver ausführen, den Sie im Feld **SQL Server-Host** angegeben haben.

> **Hinweis:**
>
> Die Datenbankerstellung schlägt möglicherweise fehl, wenn der Computer nicht über die READ-, WRITE- und UPDATE-Berechtigungen zum Erstellen von Tabellen innerhalb der Datenbank auf dem SQL-Server verfügt. Sie müssen die entsprechenden Berechtigungen auf dem Computer aktivieren. Einzelheiten finden Sie unter Zum Einrichten von Datenbanken erforderliche Berechtigungen.

#### Schritt 3: StoreFront- und NetScaler Gateway-Server integrieren

Sie müssen StoreFront- und NetScaler Gateway-Serverdetails angeben, um Secure Private Access mit StoreFront- und NetScaler Gateway-Servern zu verbinden. Diese Verbindung muss hergestellt werden, damit StoreFront und NetScaler Gateway den Datenverkehr an Secure Private Access weiterleiten können.

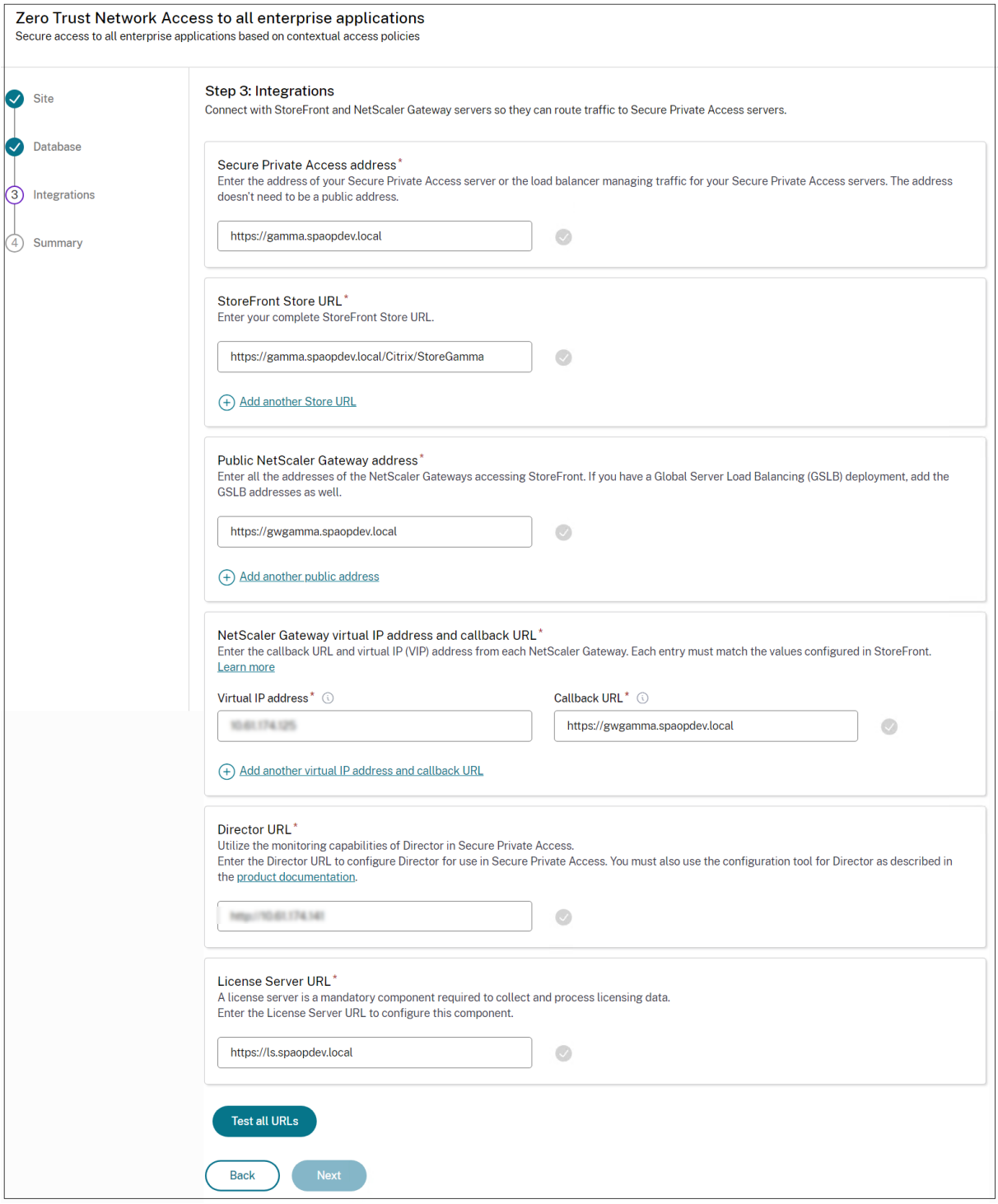
1. Geben Sie die folgenden Details ein.
    - **Secure Private Access-Serveradresse**. Beispiel: `https://secureaccess.domain.com`.
    - **StoreFront-Store-URL**. Beispiel: `https://storefront.domain.com/Citrix/StoreMain`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **Öffentliche Gateway-Adresse** —URL des NetScaler Gateway. Beispiel: `https://gateway.domain.com`.
- **Gateway-Rückrufadresse** —Diese URL muss mit der in StoreFront konfigurierten URL übereinstimmen. Beispiel: `https://gateway.domain.com`.
- **Gateway VIP** —Diese virtuelle IP-Adresse muss mit der in StoreFront für Rückrufe konfigurierten IP-Adresse übereinstimmen.

2. Klicken Sie auf **Alle URLs validieren**.
3. Klicken Sie auf **Weiter** und dann auf **Speichern**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 



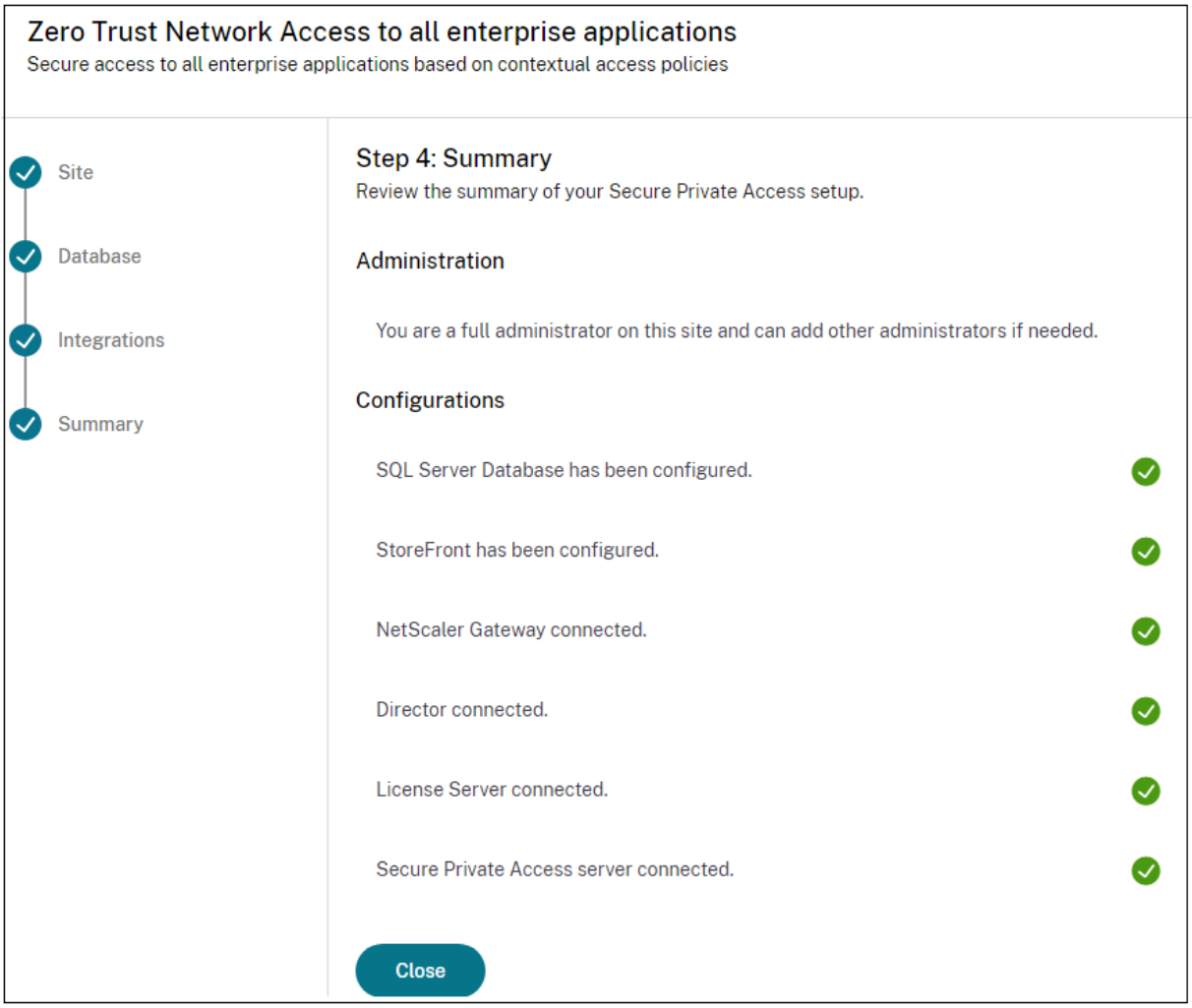

### Schritt 4: Zusammenfassung der Konfiguration

Nach Abschluss der Konfiguration erfolgt eine Überprüfung, um sicherzustellen, dass die konfigurierten Server erreichbar sind. Außerdem wird überprüft, ob der Secure Private Access-Server erreich-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

bar ist.

Wenn auf der Seite mit der Konfigurationszusammenfassung Fehler angezeigt werden, finden Sie weitere Informationen unter Problembehandlung . Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.




**Hinweis:**

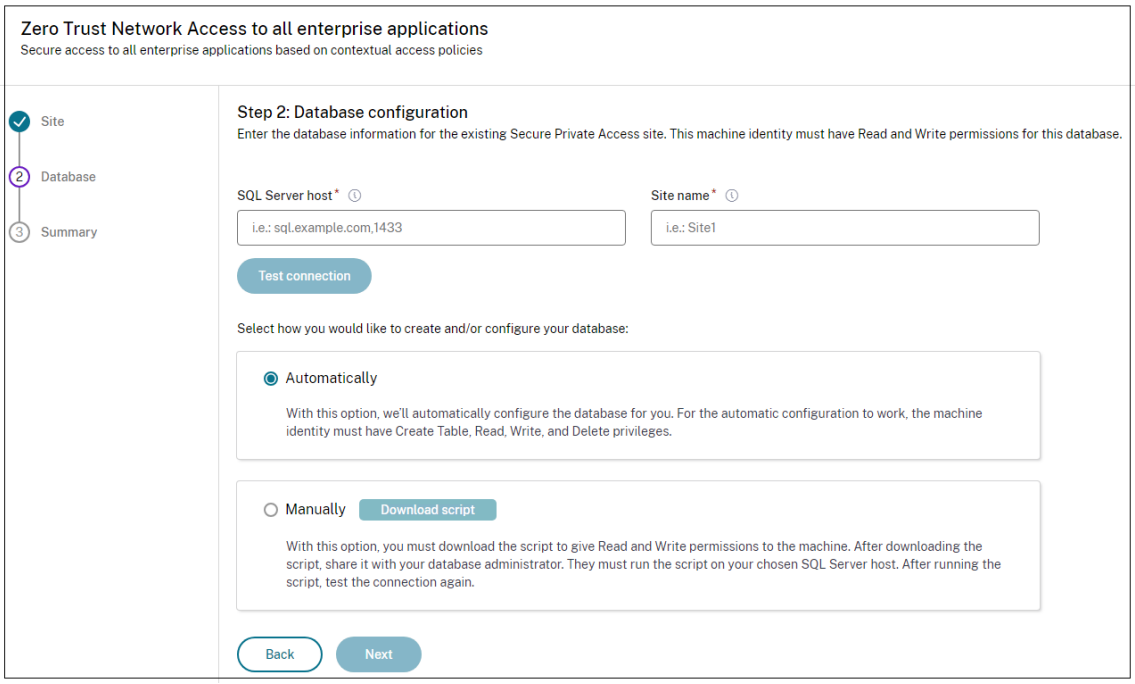
- Nachdem Sie die Umgebung eingerichtet haben, können Sie die Einstellungen in der Web-Admin-Konsole unter Einstellungen > Integrationen ändern.
- Dem Administrator, der Secure Private Access zum ersten Mal installiert, wird die volle Berechtigung erteilt. Dieser Administrator kann dann weitere Administratoren zum Setup hinzufügen. Sie können die Liste der Administratoren unter **Einstellungen > Administratoren**anzeigen.
- Sie können auch Administratorgruppen hinzufügen, sodass der Zugriff für alle Administratoren in dieser Gruppe aktiviert ist.

Einzelheiten finden Sie unter Einstellungen nach der Installation verwalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Secure Private Access durch Beitreten zu einer vorhandenen Site einrichten

1. Wählen Sie auf der Seite **Website erstellen oder einer Site beitreten** die Option **Einer vorhandenen Site beitreten** aus, und klicken Sie dann auf **Weiter**.




2. Geben Sie im Feld **SQL Server-Host** den Serverhostnamen ein. Stellen Sie sicher, dass eine Datenbank, die dem von Ihnen eingegebenen Site-Namen entspricht, bereits auf dem SQL-Server vorhanden ist, den Sie ausgewählt haben. Datenbankadressen können in einem der folgenden Formate angegeben werden:

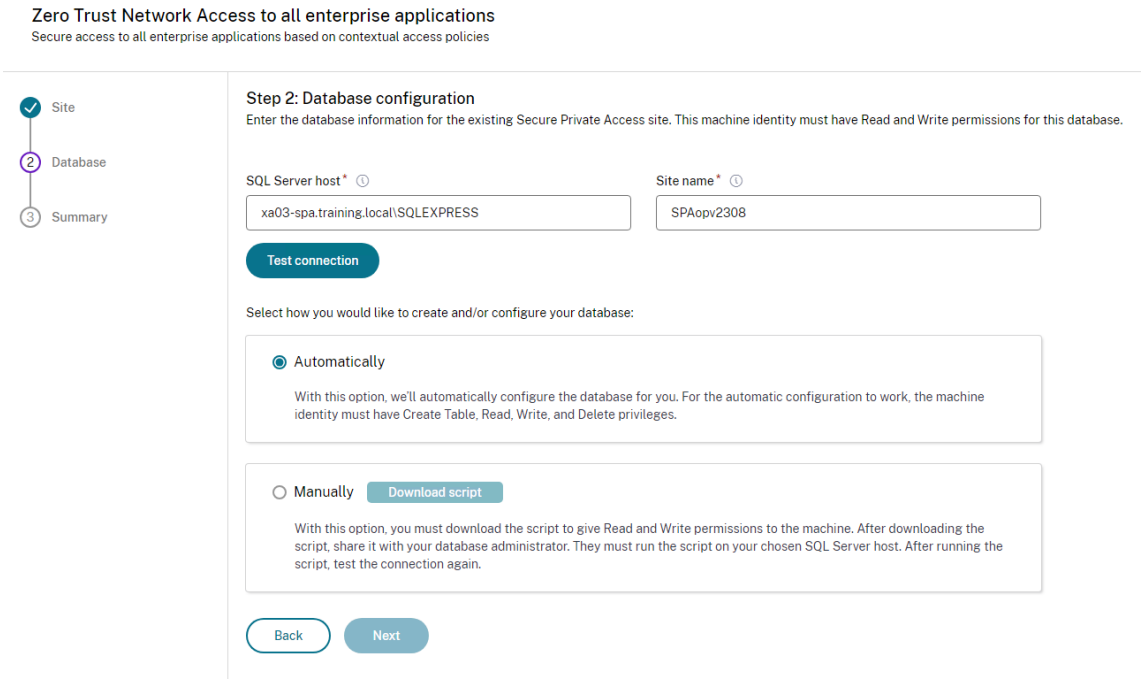
   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   Weitere Informationen finden Sie unter Datenbanken.

3. Geben Sie im Feld **Site** einen Namen für die Secure Private Access-Site ein.

4. Klicken Sie auf **Konnektivität testen**, um zu überprüfen, ob die SQL Server-Instanz gültig ist, und um zu bestätigen, dass die angegebene Site in der Datenbank vorhanden ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




Wenn es keine entsprechende Datenbank für die Site gibt, schlägt die Konnektivitätsprüfung fehl.

5. Klicken Sie auf **Speichern**.

Die Überprüfung der Konfiguration erfolgt, um sicherzustellen, dass der SQL-Datenbankserver konfiguriert ist, und um zu überprüfen, ob der Secure Private Access-Server erreichbar ist.

### Die nächsten Schritte

- NetScaler Gateway konfigurieren
- Anwendungen konfigurieren
- Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen

## Konfigurieren von NetScaler Gateway

August 26, 2024

> **Wichtig:**
>
> Wir empfehlen, NetScaler-Snapshots zu erstellen oder die NetScaler-Konfiguration zu speichern, bevor Sie diese Änderungen anwenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Laden Sie das Skript von herunter https://www.citrix.com/downloads/citrix-early-access-release/.

   Verwenden Sie *ns_gateway_secure_access.sh*, um ein neues NetScaler Gateway zu erstellen. Verwenden Sie *ns_gateway_secure_access_update.sh*, um ein vorhandenes NetScaler Gateway zu aktualisieren.

2. Laden Sie diese Skripts auf den NetScaler-Computer hoch. Sie können die WinSCP-App oder den SCP-Befehl verwenden. Beispiel: `*scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp*`.

   > **Hinweis:**
   >
   > - Es wird empfohlen, den NetScaler-Ordner /var/tmp zum Speichern temporärer Daten zu verwenden.
   > - Stellen Sie sicher, dass die Datei mit LF-Zeilenenden gespeichert ist. FreeBSD unterstützt CRLF nicht.
   > - Wenn Sie den Fehler sehen `-bash: /var/tmp/ns_gateway_secure_access.sh: /bin/sh^M: bad interpreter: No such file or directory`, bedeutet dies, dass die Zeilenenden falsch sind. Sie können das Skript mit einem beliebigen Rich-Text-Editor wie Notepad++ konvertieren.

3. SSH zu NetScaler und wechseln Sie zur Shell (geben Sie ‘shell’in der NetScaler CLI ein).

4. Machen Sie das hochgeladene Skript ausführbar. Verwenden Sie dazu den Befehl chmod.

   ```
   chmod +x /var/tmp/ns_gateway_secure_access.sh
   ```

5. Führen Sie das hochgeladene Skript in der NetScaler-Shell aus.

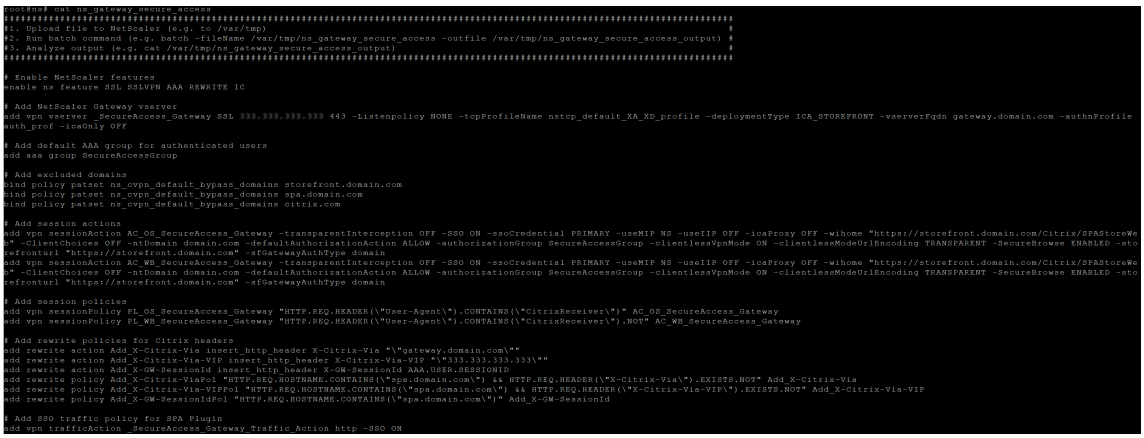
© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
root@ns32201# ./ns_gateway_secure_access_2405.sh
NetScaler Gateway vserver name (default: _SecureAccess_Gateway): spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin IP:
SPA Plugin FQDN:
StoreFront Store URL (including protocol http/https):
NetScaler authentication profile name: authnprof
NetScaler SSL server certificate name: ns32205
Domain: cgwsanity.net
Enable TCP/UDP Apptype support (Y/N): Y

************ Gateway configuration ********************
NetScaler Gateway name: spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin FQDN: spa.cgwsanity.net
SPA Plugin IP:
StoreFront Store URL:
NetScaler authentication profile name: authnprof
NetScaler Gateway server certificate name: ns32205
Domain: cgwsanity.net
Enable App type TCP/UDP:
*****************************************************

Checking SPA Plugin support....
NetScaler supports SPA CLI, skipping nsapimgr commands
Number of PEs running: 3
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
TCP/UDP Apptype support is enabled
Persisting TCP/UDP Apptype support setting: nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3 in /nsconfig/rc.netscaler file.

NetScaler Gateway creation script ns_gateway_secure_access created
Please copy it to NetScaler (e.g. /var/tmp folder) and run command:
batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output
Check ns_gateway_secure_access_output file for output
```

6. Geben Sie die erforderlichen Parameter ein. Eine Liste der Parameter finden Sie unter Voraussetzungen.

   Für das Authentifizierungsprofil und das SSL-Zertifikat müssen Sie Namen auf NetScaler angeben.

   Eine neue Datei mit mehreren NetScaler-Befehlen (die Standardeinstellung ist var/tmp/ns_gateway_secure_access) wird generiert.



7. Wechseln Sie zur NetScaler-CLI und führen Sie die resultierenden NetScaler-Befehle aus der neuen Datei mit dem Batch-Befehl aus. Beispiel:
   `batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output`

   NetScaler führt die Befehle aus der Datei nacheinander aus. Schlägt ein Befehl fehl, wird mit

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

dem nächsten Befehl fortgefahren.

Ein Befehl kann fehlschlagen, wenn eine Ressource vorhanden ist oder einer der in Schritt 6 eingegebenen Parameter falsch ist.

8. Stellen Sie sicher, dass alle Befehle erfolgreich ausgeführt wurden.

> **Hinweis:**
>
> Wenn ein Fehler auftritt, führt NetScaler immer noch die verbleibenden Befehle aus und erstellt/aktualisiert/bindet Ressourcen teilweise. Wenn Sie also einen unerwarteten Fehler sehen, weil einer der Parameter falsch ist, wird empfohlen, die Konfiguration von Anfang an zu wiederholen.

## Konfigurieren von Secure Private Access auf einem NetScaler Gateway mit vorhandener Konfiguration

Sie können die Skripts auch auf einem vorhandenen NetScaler Gateway verwenden, um Secure Private Access zu unterstützen. Das Skript aktualisiert jedoch nicht Folgendes:

- Bestehender virtueller NetScaler Gateway-Server
- Bestehende Sitzungsaktionen und Sitzungsrichtlinien, die an NetScaler Gateway gebunden sind

Stellen Sie sicher, dass Sie jeden Befehl vor der Ausführung überprüfen und Backups der Gateway-Konfiguration erstellen.

### Einstellungen auf dem virtuellen NetScaler Gateway-Server

Wenn Sie den vorhandenen virtuellen NetScaler Gateway-Server hinzufügen oder aktualisieren, stellen Sie sicher, dass die folgenden Parameter auf die definierten Werte festgelegt sind.

tcpProfileName: nstcp_default_XA_XD_profile
deploymentType: ICA_STOREFRONT
icaOnly: OFF

Beispiele:

So fügen Sie einen virtuellen Server hinzu:

```
`add vpn vserver _SecureAccess_Gateway SSL 333.333.333.333 443 -
   Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -
   deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -
   authnProfile auth_prof_name -icaOnly OFF`
```

So aktualisieren Sie einen virtuellen Server:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

```
`set vpn vserver  _SecureAccess_Gateway -icaOnly OFF`
```

Einzelheiten zu den virtuellen Serverparametern finden Sie unter vpn-sessionAction.

#### NetScaler Gateway-Sitzungsaktionen

Die Sitzungsaktion ist an einen virtuellen Gateway-Server mit Sitzungsrichtlinien gebunden. Wenn Sie eine Sitzungsaktion erstellen, stellen Sie sicher, dass die folgenden Parameter auf die definierten Werte gesetzt sind.

- transparentInterception: AUS
- SSO: AN
- ssoCredential: PRIMÄR
- useMIP: NS
- useIIP: AUS
- icaProxy: AUS
- wihome: "https://storefront.mydomain.com/Citrix/MyStoreWeb" - durch echte Store-URL ersetzen
- ClientChoices: AUS
- ntDomain: mydomain.com - wird für SSO verwendet
- defaultAuthorizationAction: ERLAUBEN
- authorizationGroup: SecureAccessGroup (Stellen Sie sicher, dass diese Gruppe erstellt wurde. Sie wird verwendet, um Secure Private Access-spezifische Autorisierungsrichtlinien zu binden)
- clientlessVpnMode: AN
- clientlessModeUrlEncoding: TRANSPARENT
- SecureBrowse: AKTIVIERT
- Storefronturl: "https://storefront.mydomain.com"
- sfGatewayAuthType: Domäne

Beispiele:

So fügen Sie eine Sitzungsaktion hinzu:

```
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy
 OFF -wihome "https://storefront.mydomain.com/Citrix/MyStoreWeb"-
ClientChoices OFF -ntDomain mydomain.com -defaultAuthorizationAction
 ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode
ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -
storefronturl "https://storefront.mydomain.com"-sfGatewayAuthType
domain
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

So aktualisieren Sie eine Sitzungsaktion:

```
set vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON
```

Einzelheiten zu den Parametern für Sitzungsaktionen finden Sie unter https://developer-docs.netscaler.com/en-us/adc-command-reference-int/13-1/vpn/vpn-sessionaction.

### Kompatibilität mit den ICA-Apps

NetScaler Gateway, das zur Unterstützung des Secure Private Access-Plug-Ins erstellt oder aktualisiert wurde, kann auch zum Auflisten und Starten von ICA-Apps verwendet werden. In diesem Fall müssen Sie Secure Ticket Authority (STA) konfigurieren und an das NetScaler Gateway binden.
Hinweis: Der STA-Server ist normalerweise Teil der DDC-Bereitstellung von Citrix Virtual Apps and Desktops.

Einzelheiten finden Sie in den folgenden Themen:

- Konfigurieren der Secure Ticket Authority auf NetScaler Gateway
- Häufig gestellte Fragen: Citrix Secure Gateway/NetScaler Gateway Secure Ticket Authority

### Unterstützung für Smart Access-Tags

In den folgenden Versionen sendet NetScaler Gateway die Tags automatisch. Sie müssen die Gateway-Callback-Adresse nicht verwenden, um die Smart Access-Tags abzurufen.

- 13.1.48.47 und höher
- 14.1—4.42 und höher

Smart Access-Tags werden als Header in der Secure Private Access-Plug-In-Anfrage hinzugefügt.

Verwenden Sie den Schalter `ns_vpn_enable_spa_onprem` oder `ns_vpn_disable_spa_onprem`, um diese Funktion in diesen NetScaler-Versionen zu aktivieren/deaktivieren.

- Sie können mit dem Befehl umschalten (FreeBSD-Shell):

  ```
  nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem
  ```

- Aktivieren Sie den SecureBrowse-Client-Modus für die HTTP-Callout-Konfiguration, indem Sie den folgenden Befehl ausführen (FreeBSD-Shell).

  ```
  nsapimgr_wr.sh -ys call=toggle_vpn_enable_securebrowse_client_mode
  ```

- Führen Sie zum Deaktivieren denselben Befehl erneut aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- Um zu überprüfen, ob der Schalter ein- oder ausgeschaltet ist, führen Sie den Befehl `nsconmsg` aus.
- Informationen zur Konfiguration von Smart Access-Tags auf NetScaler Gateway finden Sie unter Configuring Custom Tags (SmartAccess Tags) auf NetScaler Gateway.

### Bekannte Einschränkungen

- Bestehendes NetScaler Gateway kann mit einem Skript aktualisiert werden, es kann jedoch eine unendliche Anzahl möglicher NetScaler-Konfigurationen geben, die nicht durch ein einziges Skript abgedeckt werden können.
- Verwenden Sie keinen ICA-Proxy auf NetScaler Gateway. Diese Funktion ist deaktiviert, wenn NetScaler Gateway konfiguriert ist.
- Wenn Sie NetScaler verwenden, das in der Cloud bereitgestellt wird, müssen Sie einige Änderungen im Netzwerk vornehmen. Erlauben Sie beispielsweise die Kommunikation zwischen NetScaler und anderen Komponenten an bestimmten Ports.
- Wenn Sie SSO auf NetScaler Gateway aktivieren, stellen Sie sicher, dass NetScaler über eine private IP-Adresse mit StoreFront kommuniziert. Möglicherweise müssen Sie NetScaler einen neuen StoreFront-DNS-Eintrag mit einer privaten StoreFront-IP-Adresse hinzufügen.

### Laden Sie das öffentliche Gateway-Zertifikat hoch

Gehen Sie wie folgt vor, um ein öffentliches Gateway-Zertifikat in die Secure Private Access-Datenbank hochzuladen:

1. Öffnen Sie PowerShell oder das Eingabeaufforderungsfenster mit den Administratorrechten.
2. Ändern Sie das Verzeichnis in den Ordner Admin\AdminConfigTool im Secure Private Access-Installationsordner (z. B. cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool" )
3. Führen Sie den folgenden Befehl aus:

   ```
   \AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
   > <PublicGatewayCertificatePath>
   ```

## Konfigurieren Sie Anwendungen

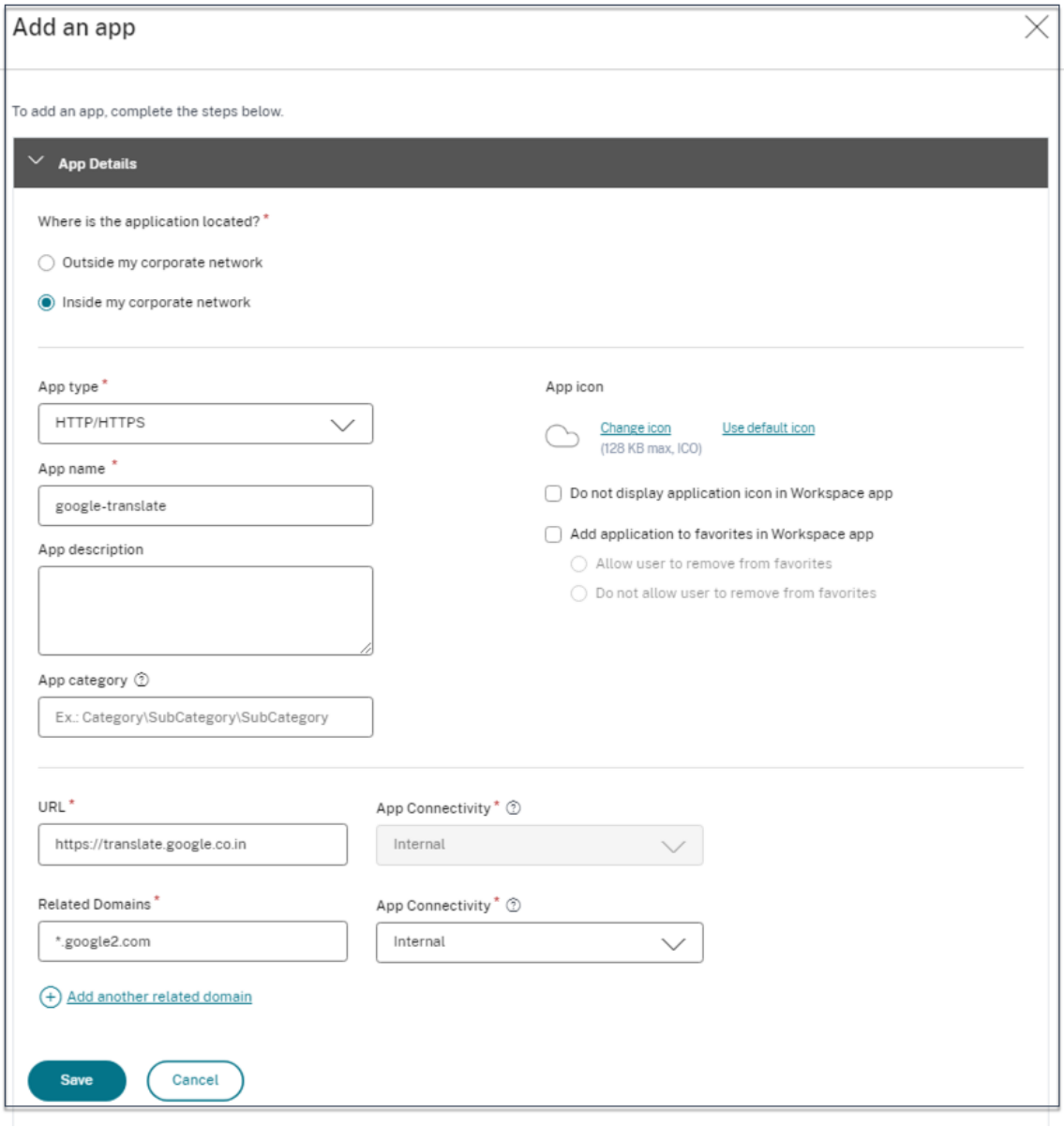
February 16, 2024

1. Wählen Sie den Standort aus, an dem sich die App befindet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

- **Außerhalb meines Unternehmensnetzwerks** für externe Anwendungen.
- **In meinem Unternehmensnetzwerk** für interne Anwendungen.

2. Geben Sie im Abschnitt App-Details die folgenden Details ein und klicken Sie auf **Weiter**.




- **Appname** —Name der Anwendung.
- **App-Beschreibung** —Eine kurze Beschreibung der App. Diese Beschreibung wird Ihren Benutzern im Workspace angezeigt. Sie können im Format `KEYWORDS: <keyword_name>` auch Schlüsselwörter für die Anwendungen eingeben. Sie können die Schlüsselwörter verwenden, um die Anwendungen zu filtern. Einzelheiten finden Sie unter Filtern von Ressourcen nach eingeschlossenen Schlüsselwörtern.
- **App-Kategorie** —Fügen Sie die Kategorie und den Namen der Unterkategorie (falls

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

zutreffend) hinzu, unter denen die App, die Sie veröffentlichen, auf der Citrix Workspace-Benutzeroberfläche angezeigt werden muss. Sie können für jede App eine neue Kategorie hinzufügen oder vorhandene Kategorien über die Citrix Workspace-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angegeben haben, wird die App in der Workspace-Benutzeroberfläche unter der jeweiligen Kategorie angezeigt.

- Die Kategorie/Unterkategorie ist vom Administrator konfigurierbar und Administratoren können für jede App eine neue Kategorie hinzufügen.
- Die Namen der Kategorie/Unterkategorien müssen durch einen umgekehrten Schrägstrich getrennt werden. Zum Beispiel Business And Productivity\ Engineering . Außerdem unterscheidet dieses Feld zwischen Groß- und Kleinschreibung. Administratoren müssen sicherstellen, dass sie die richtige Kategorie definieren. Wenn der Name in der Citrix Workspace-Benutzeroberfläche und der im Feld App-Kategorie eingegebene Kategoriename nicht übereinstimmen, wird die Kategorie als neue Kategorie aufgeführt.

  Wenn Sie beispielsweise die Kategorie Geschäft und Produktivität falsch als Geschäft und Produktivität in das Feld App-Kategorie eingeben, wird in der Citrix Workspace-Benutzeroberfläche zusätzlich zur Kategorie Geschäft und Produktivität eine neue Kategorie mit dem Namen Geschäft und Produktivität aufgeführt.

- **App-Symbol** —Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Größe der Symboldatei muss 128 x 128 Pixel betragen und nur das Ico-Format wird unterstützt. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.
- **Anwendung für Benutzer nicht anzeigen** —Wählen Sie diese Option, wenn Sie die App den Benutzern nicht anzeigen möchten.
- **URL** —URL der Anwendung.
- **Verwandte Domains** —Die zugehörige Domain wird basierend auf der Anwendungs-URL automatisch ausgefüllt. Administratoren können weitere verwandte interne oder externe Domänen hinzufügen.
  **Anwendung automatisch zu Favoriten hinzufügen** —Klicken Sie auf diese Option, um diese App als Lieblings-App in der Citrix Workspace-App hinzuzufügen.
- **Benutzern erlauben, aus Favoriten zu entfernen** —Klicken Sie auf diese Option, um App-Abonnenten zu erlauben, die App aus der Liste der Favoriten-Apps in der Citrix Workspace-App zu entfernen.
  Wenn Sie diese Option auswählen, wird in der Citrix Workspace-App oben links in der App ein gelbes Sternsymbol angezeigt.
- **Benutzern nicht erlauben, aus den Favoriten zu entfernen** —Klicken Sie auf diese Option, um zu verhindern, dass Abonnenten die App aus der Liste der Favoriten-Apps in der

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Citrix Workspace-App entfernen.

Wenn Sie diese Option auswählen, wird in der Citrix Workspace-App oben links in der App ein Sternsymbol mit einem Vorhängeschloss angezeigt.

Wenn Sie die als Favoriten markierten Apps aus der Secure Private Access-Konsole entfernen, müssen diese Apps manuell aus der Favoritenliste in Citrix Workspace entfernt werden. Die Apps werden nicht automatisch aus StoreFront gelöscht, wenn die Apps aus der Secure Private Access-Konsole entfernt werden.
App-Konnektivität: Wählen Sie Intern für Web-Apps und Extern für SaaS-Apps aus.

3. Klicken Sie auf **Speichern**und dann auf **Fertig stellen**.

Sie können alle Anwendungsdomänen anzeigen, die **unter Einstellungen > Anwendungs-domäne**konfiguriert sind. Weitere Informationen finden Sie unter Einstellungen nach der Installation verwalten.

### Die nächsten Schritte

Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen

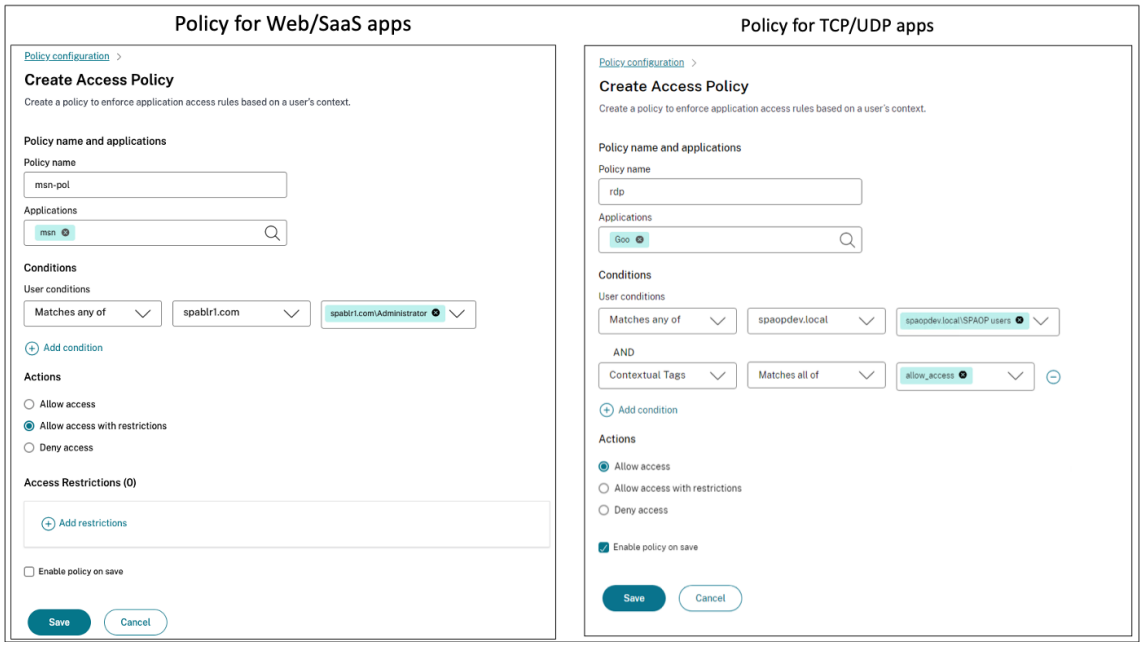
## Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen

December 27, 2023

Mithilfe von Zugriffsrichtlinien können Sie den Zugriff auf die Apps basierend auf dem Benutzer oder den Benutzergruppen aktivieren oder deaktivieren. Darüber hinaus können Sie den eingeschränkten Zugriff auf die Apps aktivieren, indem Sie die Sicherheitseinschränkungen hinzufügen.

1. Klicken Sie auf **Richtlinie erstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




2. Wählen Sie unter **Anwendungen**die Apps aus, für die Sie die Zugriffsrichtlinien durchsetzen möchten.
3. Unter **Benutzer/Benutzergruppen** —Wählen Sie die Bedingungen und Benutzer oder Benutzergruppen aus, auf deren Grundlage der App-Zugriff gewährt oder verweigert werden muss.

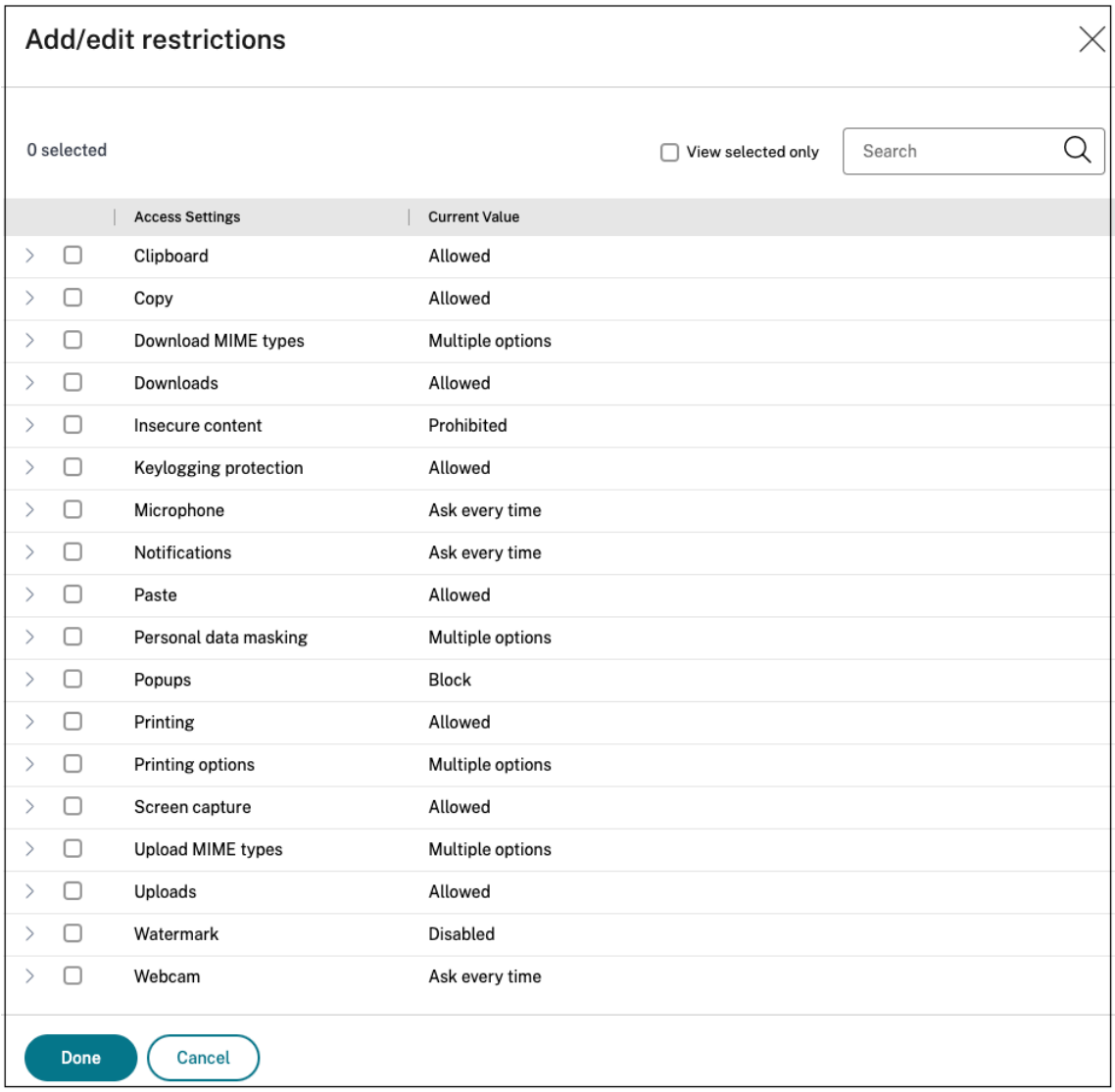
    - **Entspricht einem von**: Nur die Benutzer oder Gruppen, die einem der im Feld aufgeführten Namen entsprechen, dürfen darauf zugreifen.
    - **Stimmt mit keinem überein**: Allen Benutzern oder Gruppen außer den im Feld aufgeführten Benutzern oder Gruppen wird der Zugriff gewährt.

4. Klicken Sie auf **Bedingung hinzufügen**, um eine weitere Bedingung hinzuzufügen, die auf kontextuellen Tags basiert. Diese Tags werden vom NetScaler Gateway abgeleitet.
5. Wählen Sie **Bedingte Tags** und dann die Bedingungen aus, auf deren Grundlage der App-Zugriff erlaubt oder verweigert werden muss.
6. Wählen Sie unter **Dann gehen Sie wie folgt**vor eine der folgenden Aktionen aus, die auf der Grundlage der Zustandsbewertung für die App erzwungen werden müssen.

    - **Zugriff erlauben**
    - **Zugriff mit Einschränkungen erlauben**
    - **Zugriff verweigern**

    Wenn Sie **Zugriff mit Einschränkungen zulassen**auswählen, können Sie die folgenden Einschränkungen auswählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




- **Zugriff auf die Zwischenablage einschränken**: Deaktiviert das Ausschneiden/Kopieren/E-infügen zwischen der App und der Systemzwischenablage.
- **Drucken einschränken**: Deaktiviert das Drucken im Citrix Enterprise Browser.
- **Downloads einschränken**: Deaktiviert die Fähigkeit des Benutzers, aus der App herunterzuladen.
- **Uploads einschränken**: Deaktiviert die Fähigkeit des Benutzers, innerhalb der App hochzuladen.
- **Wasserzeichen anzeigen**: Zeigt ein Wasserzeichen auf dem Bildschirm des Benutzers an, das den Benutzernamen und die IP-Adresse des Computers des Benutzers anzeigt.
- **Beschränken Sie die Schlüsselprotokollierung**: Schützt vor Keyloggern. Wenn ein Benutzer versucht, sich mit dem Benutzernamen und dem Kennwort bei der App anzumelden, werden alle Schlüssel auf den Keyloggern verschlüsselt. Außerdem sind alle Aktivitäten, die der Benutzer in der App ausführt, vor Key-Logging geschützt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Wenn beispielsweise App-Schutzrichtlinien für Office 365 aktiviert sind und der Benutzer ein Office 365-Word-Dokument bearbeitet, werden alle Tastenanschläge auf Keyloggern verschlüsselt.

- **Bildschirmaufnahme einschränken**: Deaktiviert die Möglichkeit, die Bildschirme mit einem der Bildschirmaufnahmeprogramme oder Apps aufzunehmen. Wenn ein Benutzer versucht, den Bildschirm zu erfassen, wird ein leerer Bildschirm aufgenommen.

> **Hinweis:**
>
> Einschränkungen bei der Schlüsselprotokollierung und Bildschirmaufnahme gelten nur für Citrix Workspace-Desktopclients.

7. Geben Sie im Feld **Richtlinienname**einen Namen für die Richtlinie ein.
8. Wählen Sie **Richtlinie beim Speichern aktivieren**aus. Wenn Sie diese Option nicht auswählen, wird die Richtlinie nur erstellt und nicht für die Anwendungen durchgesetzt. Alternativ können Sie die Richtlinie auch von der Seite Zugriffsrichtlinien aus aktivieren, indem Sie den Kippschalter verwenden.

### Priorität der Zugriffsrichtlinie

Nachdem eine Zugriffsrichtlinie erstellt wurde, wird der Zugriffsrichtlinie standardmäßig eine Prioritätsnummer zugewiesen. Sie können die Priorität auf der Startseite der Zugriffsrichtlinien einsehen.

Eine Priorität mit einem niedrigeren Wert hat die höchste Priorität und wird zuerst ausgewertet. Wenn diese Richtlinie nicht den definierten Bedingungen entspricht, wird die nächste Richtlinie mit der niedrigeren Prioritätsnummer bewertet und so weiter.

Sie können die Prioritätsreihenfolge ändern, indem Sie die Richtlinien mithilfe des Auf-Abwärt-Symbols in der Spalte **Priorität** nach oben oder unten verschieben.

### Nächste Schritte

Überprüfen Sie Ihre Konfiguration auf den Client-Computern (Windows und macOS).

Example

## Ablauf für Endbenutzer

August 26, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

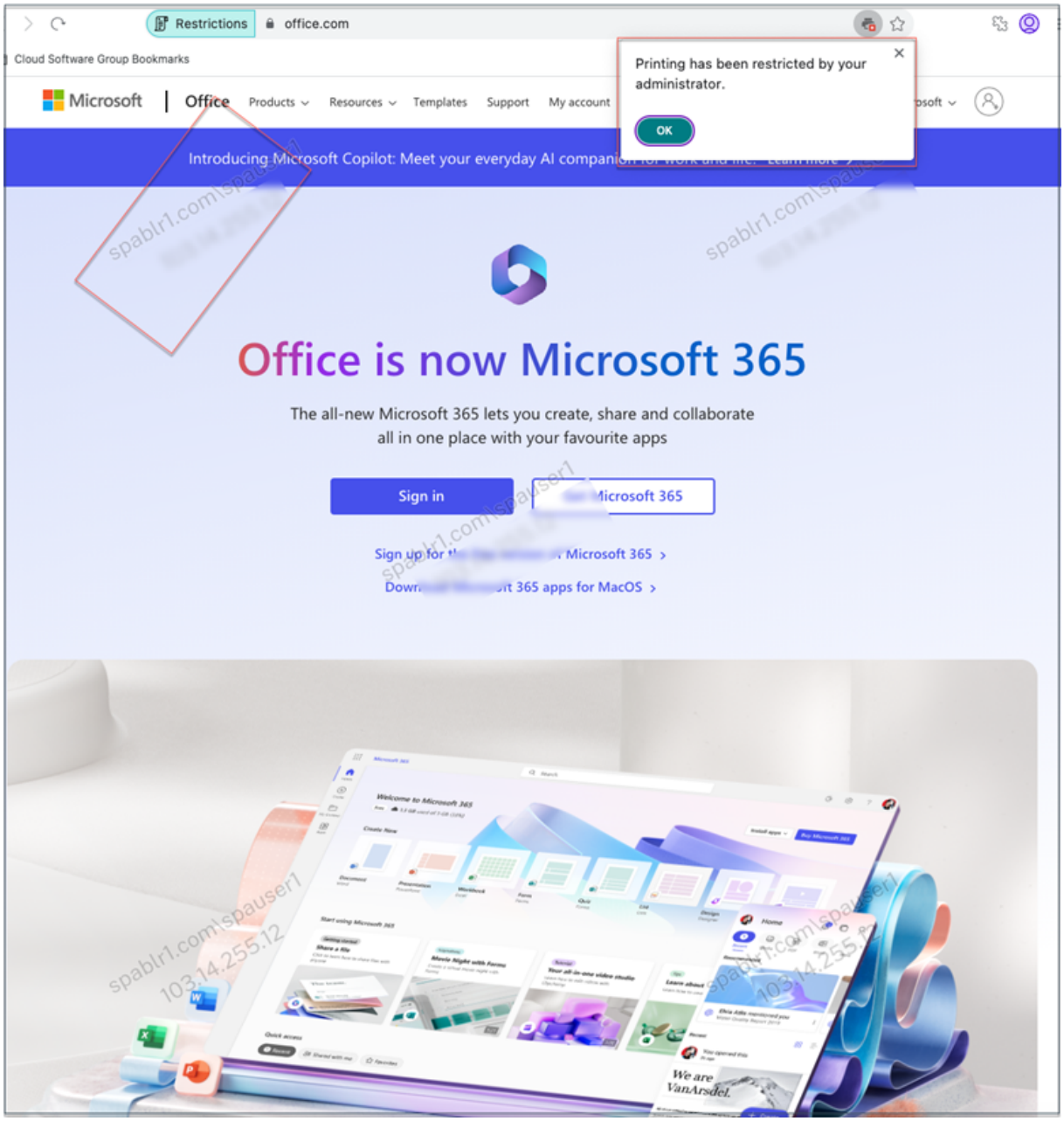
Angenommen, ein Administrator hat die Office365-App mit der Wasserzeichen- und Druckbeschränkung für den Endbenutzer konfiguriert. Wenn der Endbenutzer nun auf die Office365-App zugreift, müssen die Wasserzeichen- und Druckbeschränkungen auf die App angewendet werden.

Der Endbenutzer muss die folgenden Schritte ausführen, um auf die Office365-App zuzugreifen:

1. Greifen Sie über die Citrix Workspace-App auf den StoreFront Store zu.
2. Melden Sie sich im Store an.
3. Klicken Sie auf die Registerkarte **Apps** und dann auf die **Office365**-Anwendung.

   Der Endbenutzer muss nun feststellen, dass die Office365-Anwendung gestartet wird und das Wasserzeichen enthält. Wenn der Endbenutzer versucht, einige Daten aus der Office365-Anwendung zu drucken, muss dem Benutzer außerdem die Meldung zur Druckbeschränkung angezeigt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




**Hinweis:**

Administratoren müssen Benutzern die Kontoinformationen zur Verfügung stellen, die sie für den Zugriff auf virtuelle Desktops und Anwendungen benötigen. Einzelheiten finden Sie unter Hinzufügen einer Store-URL zur Citrix Workspace-App.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Sichere Private Access-Integration mit Web Studio-Integration

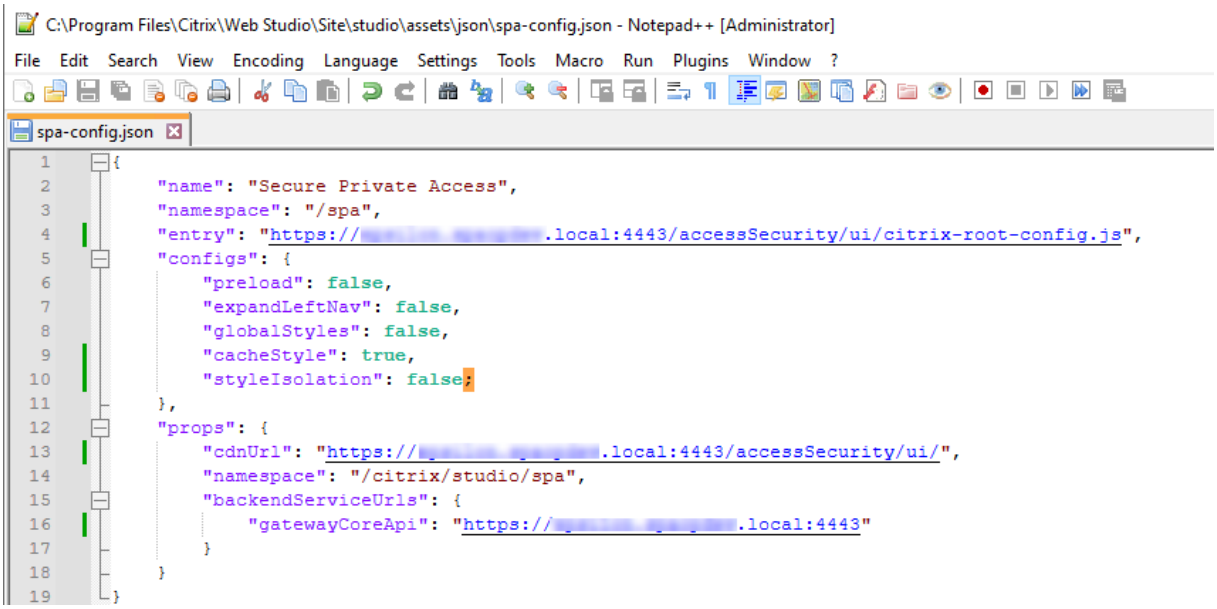
June 19, 2024

Citrix Secure Private Access ist auch in die Web Studio-Konsole integriert, sodass Benutzer problemlos über Web Studio auf den Dienst zugreifen können.

Sie müssen Web Studio Version 2308 oder höher installieren.

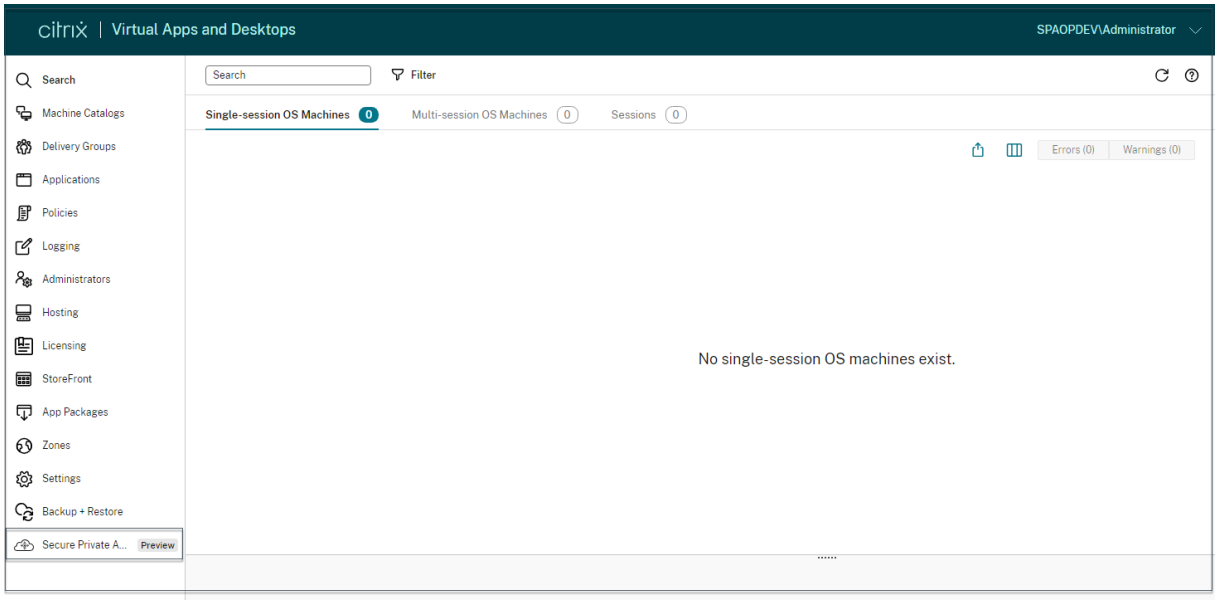
Führen Sie die folgenden Schritte aus, um die Web Studio-Integration zu aktivieren:

1. Installieren Sie Citrix Web Studio mit dem Citrix Virtual Apps and Desktops-Installationsprogramm oder dem integrierten DDC-Installationsprogramm.
2. Folgen Sie den Anweisungen auf dem Bildschirm und schließen Sie die Installation ab. Wenn Sie zur Eingabe einer Controller-Adresse aufgefordert werden, geben Sie den DDC-FQDN als Controller-Adresse ein.
3. Navigieren Sie nach erfolgreicher Installation zum Ordner C:\Program Files\Citrix\Web Studio\Site\assets\json und ändern Sie den Inhalt der Datei spa-config.json.
   Wenn für die Web Studio-Installation ein anderer als der Standardspeicherort verwendet wurde, ersetzen Sie den Standardinstallationsort in C:\Program Files\Citrix durch den richtigen Speicherort.




1. Ersetzen Sie “SpaServer”durch den FQDN Ihres Secure Private Access-Plug-Ins.
2. Melden Sie sich bei Web Studio an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




1. Klicken Sie im linken Navigationsmenü auf **Secure Private Access<Preview>**, um von Web Studio aus auf die Secure Private Access-Administratorkonsole zuzugreifen.

## Einstellungen nach der Installation verwalten

December 27, 2023

Nachdem Sie Secure Private Access installiert haben, können Sie die Einstellungen auf der Seite Einstellungen ändern.

### Routing von Anwendungsdomänen verwalten

Sie können eine Liste der Anwendungsdomänen anzeigen, die in Ihrem Secure Private Access-Setup hinzugefügt wurden. In der Tabelle mit den Anwendungsdomänen werden alle zugehörigen Domänen und die Art und Weise aufgeführt, wie der App-Verkehr weitergeleitet wird (extern oder intern).

1. Klicken Sie auf **Einstellungen > Anwendungsdomäne**.
2. Sie können auf das Bearbeitungssymbol klicken und bei Bedarf den Routingtyp ändern.

### Administratoren für Secure Private Access verwalten

Auf der Seite „ **Einstellungen“> „Administratoren“können Sie die Liste der Administratoren anzeigen und Administratoren** hinzufügen. Dem Administrator, der Secure Private Access zum

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

ersten Mal installiert, wird die volle Berechtigung erteilt. Dieser Admin kann dann weitere Administratoren zum Setup hinzufügen.

Sie können auch Admingruppen hinzufügen, sodass der Zugriff für alle Admins in dieser Gruppe aktiviert ist.

1. Klicken Sie auf der Seite **Administratoren** auf **Hinzufügen**.
2. Wählen Sie unter **Domain**die Domain aus, zu der dieser Administrator hinzugefügt werden muss.
3. Wählen Sie **unter Benutzer oder Benutzergruppe**den Benutzer oder die Gruppen aus, zu denen dieser Benutzer gehört.
4. Wählen Sie **unter Admin-Typ**den Berechtigungstyp aus, der diesem Benutzer zugewiesen werden muss.

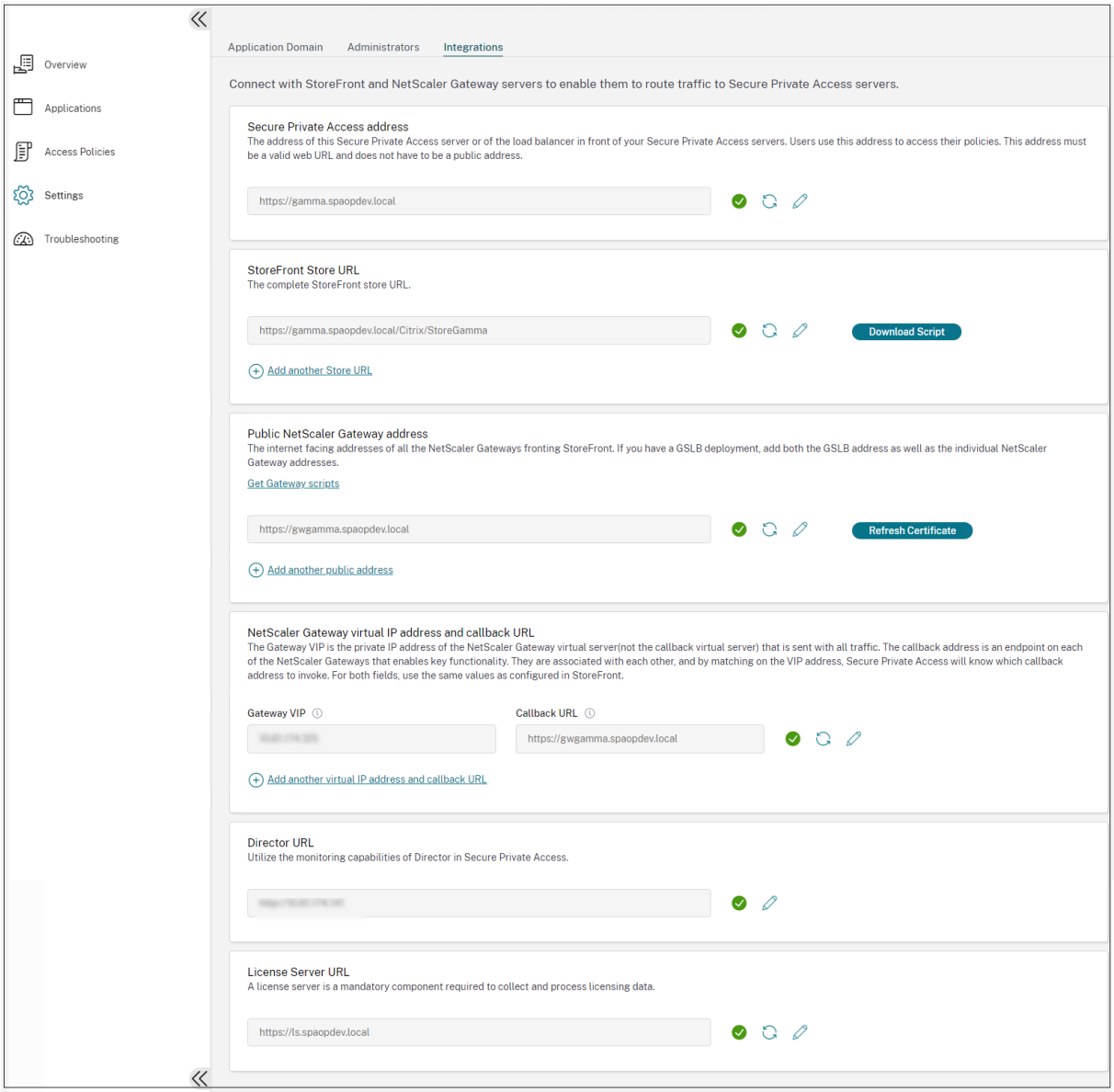
## Aktualisieren Sie die StoreFront- oder NetScaler Gateway-Serverdetails nach dem Setup

Nachdem Sie Secure Private Access eingerichtet haben, können Sie die StoreFront- und NetScaler Gateway-Einträge auf der Registerkarte **Integrationen** ändern oder aktualisieren.

1. Klicken Sie auf **Einstellungen > Integrationen.**
2. Klicken Sie auf das Bearbeitungssymbol neben der Einstellung, die Sie ändern und den Eintrag aktualisieren möchten.
3. Klicken Sie auf das Aktualisierungssymbol, um sicherzustellen, dass die Einstellungen gültig sind.

> **Hinweis:**
>
> Wenn Secure Private Access auf einer anderen Maschine als StoreFront installiert ist, laden Sie das StoreFront-Skript herunter und führen Sie es auf StoreFront aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 




## Dashboard-Übersicht

December 27, 2023

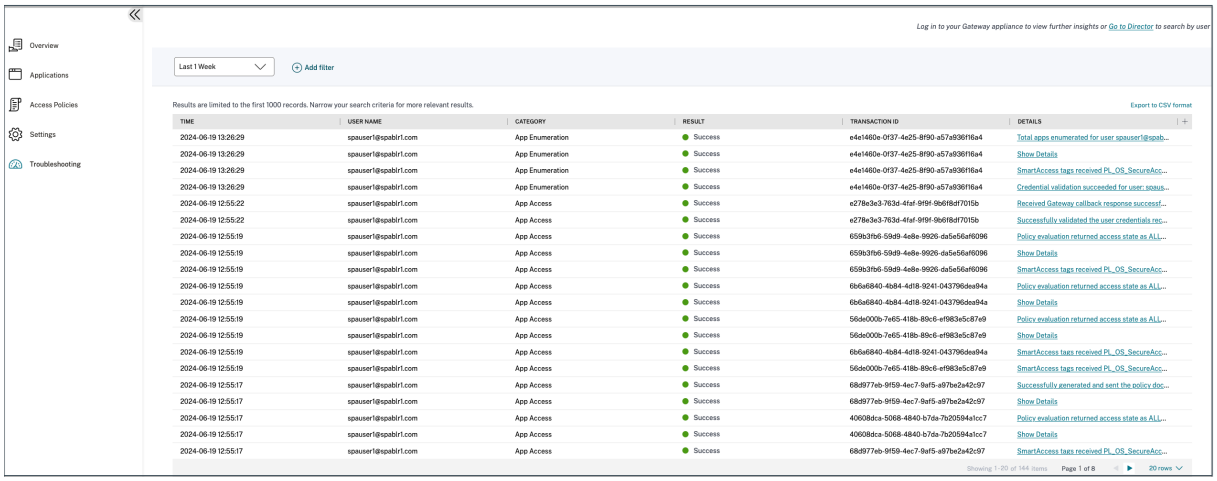
Das Dashboard für Secure Private Access-Problembehandlungsprotokolle zeigt die Protokolle zum Anwendungsstart, zur App-Aufzählung und deren Status an.

Sie können die Protokolle für die voreingestellte Zeit oder für eine benutzerdefinierte Zeitleiste anzeigen. Sie können dem Diagramm Spalten hinzufügen, indem Sie auf das Pluszeichen klicken, je nachdem, welche Informationen Sie im Dashboard sehen möchten. Sie können die Benutzerpro-

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

tokolle in das CSV-Format exportieren.

Sie können die Filter (KATEGORIE und ERGEBNIS) verwenden, um Ihre Suchergebnisse zu verfeinern.




Sie können Ihre Suche auch anhand der folgenden Parameter zusammen mit den Operatoren im Suchfeld verfeinern.

- Benutzername
- Kategorie
- Event-Typ
- Ergebnis
- Transaktions-ID
- Details

Im Folgenden finden Sie die Suchoperatoren, mit denen Sie Ihre Suche in den Benutzerprotokollen und den wichtigsten Zugriffsrichtlinien anhand von Durchsetzungsdiagrammen verfeinern können.

- =: Um nach den Protokollen/Richtlinien zu suchen, die genau den Suchkriterien entsprechen.
- !=: Um nach den Protokollen/Richtlinien zu suchen, die die angegebenen Kriterien nicht enthalten.
- ~: Um nach den Protokollen/Richtlinien zu suchen, die teilweise den Suchkriterien entsprechen.
- !~: Um nach den Protokollen/Richtlinien zu suchen, die einige der angegebenen Kriterien nicht enthalten.

Sie können beispielsweise nach einem Ereignistyp “DSAuth”suchen, indem Sie die Zeichenfolge **Event-Type = DSAuth** im Suchfeld verwenden.

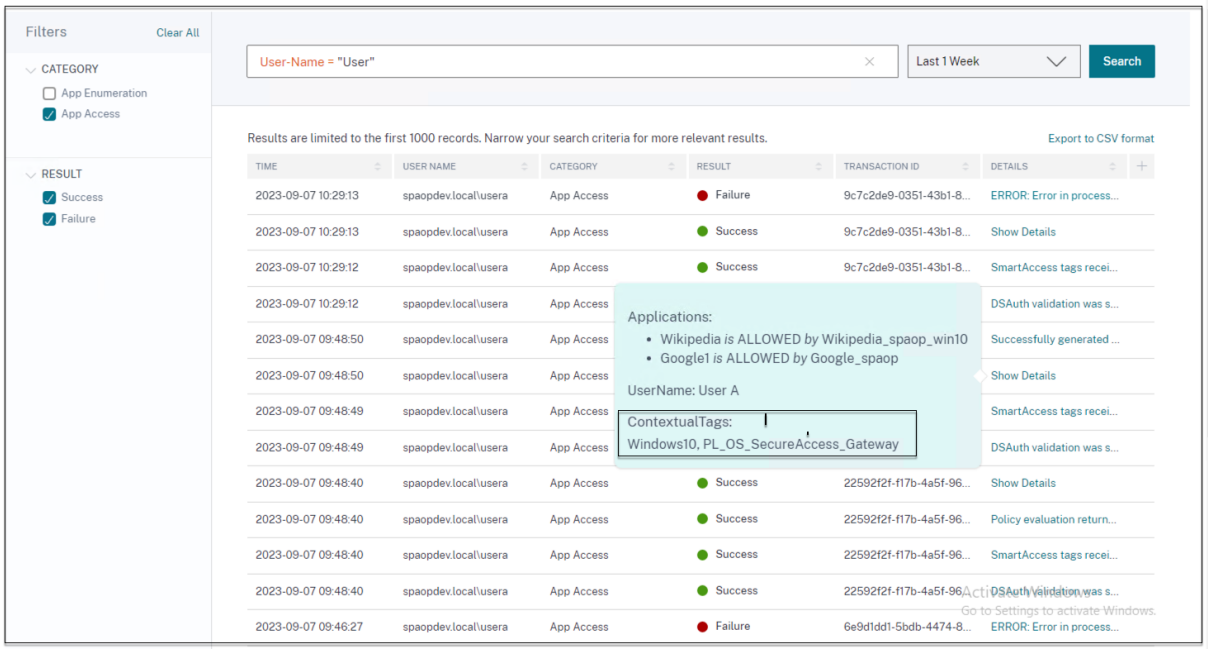
Verwenden Sie in ähnlicher Weise die Zeichenfolge **User-Name ~ operator**, um nach Benutzern zu suchen, die den Begriff “operator”teilweise enthalten. Diese Suche listet alle Benutzernamen auf, die den Begriff “operator”enthalten. Zum Beispiel “lokaler Operator”, “Admin-Operator”

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Mithilfe der Transaktions-ID können Sie nach allen Protokollen suchen, die sich auf ein einzelnes Ereignis beziehen. Die Transaktions-ID korreliert alle Secure Private Access-Protokolle für eine Zugriffsanforderung. Für eine App-Zugriffsanforderung können mehrere Protokolle generiert werden, beginnend mit der Authentifizierung, dann der App-Enumeration und dann dem App-Zugriff selbst. All diese Ereignisse generieren ihre eigenen Protokolle. Die Transaktions-ID wird verwendet, um all diese Protokolle zu korrelieren. Sie können die Protokolle zur Fehlerbehebung anhand der Transaktions-ID filtern, um alle Protokolle zu finden, die sich auf eine bestimmte App-Zugriffsanforderung beziehen.

### Kontextuelle Tags aus Protokollen anzeigen

Der Link **Details anzeigen** in der Spalte **Details** zeigt die Liste der Anwendungen an, die mit der jeweiligen Zugriffsrichtlinie verknüpft sind, sowie die mit der Richtlinie verknüpften kontextuellen Tags.




## Behebung von Fehlern

February 16, 2024

In diesem Thema werden einige der Fehler aufgeführt, auf die Sie beim Einrichten von Secure Private Access stoßen können.

Zertifikatsfehler Fehler bei
derDatenbankerstellung
StoreFront-Ausfälle

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

Öffentliche Gateway-/Callback-Gateway-Ausfälle
SecurePrivate Access Server nicht erreichbar

### Fehler im Zertifikat

**Fehlermeldung**: Die Zertifikate konnten nicht automatisch von einem oder mehreren Gatewayservern abgerufen werden.
**Problemumgehung**: Aktualisieren Sie das Gateway-Zertifikat genauso wie für Citrix Virtual Apps and Desktops.

### Fehler bei der Datenbankerstellung

- **Fehlermeldung**: Datenbank konnte nicht erstellt werden

  **Lösung**: Für den automatischen Fall —Die Maschine muss über READ-, WRITE- und UPDATE-Berechtigungen verfügen, um Tabellen in der Datenbank auf dem SQL-Server zu erstellen.

- **Fehlermeldung**: Datenbank konnte nicht erstellt werden: Eine Datenbank ist bereits vorhanden.

  Diese Fehlermeldung kann in einem der folgenden Szenarien auftreten.

  - Wenn bei der **Konfiguration der Datenbanken die Option Automatische** Konfiguration ausgewählt ist.
  - Wenn der Administrator eine Datenbank erstellt, muss es sich um eine leere Datenbank handeln. Diese Fehlermeldung kann erscheinen, wenn es sich bei der Datenbank um eine nicht leere Datenbank handelt.

    **Lösung**: Sie müssen eine leere Datenbank erstellen.
  - Sie deinstallieren Secure Private Access und wiederholen das Setup mit demselben Site-Namen. In diesem Fall wäre die Datenbank aus der vorherigen Installation nicht gelöscht worden.

    **Lösung**: Sie müssen die Datenbank manuell löschen.
  - Sie entscheiden, die Datenbank mithilfe des Skripts manuell einzurichten (indem Sie auf der Seite „Datenbanken konfigurieren“die Option Manuelle Konfiguration auswählen) und wechseln dann zur Option Automatische Konfiguration, verwenden jedoch denselben Site-Namen. In diesem Fall wird beim Ausführen des Skripts bereits eine Datenbank mit demselben Namen erstellt.

    **Lösung**: Sie müssen die Site umbenennen und dann das Skript erneut ausführen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

  - Die Maschine verfügt nicht über die READ-, WRITE- und UPDATE-Berechtigungen, um Tabellen in der Datenbank auf dem SQL-Server zu erstellen.

    **Lösung**: Aktivieren Sie die entsprechenden Berechtigungen auf dem Computer. Einzelheiten finden Sie unter Zum Einrichten von Datenbanken erforderliche Berechtigungen.

- **Fehlermeldung**: Datenbank konnte nicht erstellt werden: Verbindung fehlgeschlagen

  **Auflösung**:

  - Überprüfen Sie die Datenbank-Netzwerkkonnektivität von Ihrem Computer aus. Stellen Sie sicher, dass der SQL-Server-Port an der Firewall geöffnet ist.
  - Wenn Sie einen Remote-SQL-Server verwenden, überprüfen Sie, ob für den SQL-Server eine Anmeldung mit der Secure Private Access-Maschinenidentität Domain\ hostname$ erstellt wurde.
  - Wenn Sie einen Remote-SQL-Server verwenden, stellen Sie sicher, dass der Computeridentität die richtige Rolle zugewiesen wurde, die Systemadministratorrolle.
  - Wenn Sie einen lokalen SQL-Server verwenden (nicht vom Installationsprogramm), überprüfen Sie, ob für den Benutzer NT AUTHORITY\ SYSTEM ein Login erstellt werden muss.

### StoreFront-Fehler

- **Fehlermeldung**: StoreFront-Eintrag konnte nicht erstellt werden für: <`Store URL`>

  Aktualisieren Sie die StoreFront-Einträge auf der Registerkarte **Einstellungen**, falls sie nicht sichtbar sind. Nachdem Sie Secure Private Access mithilfe des Assistenten eingerichtet haben, können Sie StoreFront-Einträge auf der Registerkarte **Einstellungen** bearbeiten. Notieren Sie sich die StoreFront-Store-URL, für die dieser Fehler aufgetreten ist.

  **Auflösung**:

  1. Klicken Sie auf **Einstellungen** und dann auf den Tab **Integrationen**.
  2. Fügen Sie unter **StoreFront Store-URL** den StoreFront-Eintrag hinzu, falls er nicht sichtbar ist.

- **Fehlermeldung**: StoreFront-Eintrag konnte nicht konfiguriert werden für: <`Store URL`>

  **Auflösung**:

  1. Möglicherweise besteht eine Einschränkung der PowerShell-Ausführungsrichtlinie. Führen Sie den PowerShell-Skriptbefehl aus, `Get-ExecutionPolicy` um weitere Informationen zu erhalten.
  2. Wenn es eingeschränkt ist, müssen Sie dies Bypass und ein StoreFront-Konfigurationsskript manuell ausführen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

3. Klicken Sie auf **Einstellungen** und dann auf den Tab **Integrationen**.
4. Identifizieren Sie unter **StoreFront Store URL**den StoreFront-URL-Eintrag, für den der Fehler aufgetreten ist.
5. Klicken Sie neben dieser Store-URL auf die Schaltfläche Skript **herunterladen** und führen Sie dieses PowerShell-Skript mit Administratorrechten auf dem Computer aus, auf dem die entsprechende StoreFront-Installation vorhanden ist.

> **Hinweis:**
>
> Wenn Sie die Installation nach der Deinstallation erneut versuchen, stellen Sie sicher, dass Sie in der StoreFront-Konfiguration keinen Eintrag mit dem Namen „Secure Private Access "haben (**StoreFront > store> Delivery Controller -**Secure Private Access). Wenn Secure Private Access vorhanden ist, löschen Sie diesen Eintrag. Laden Sie das Skript manuell von der Seite Einstellungen > Integrationen herunter und führen Sie es aus.

- **Fehlermeldung**: Die StoreFront-Konfiguration ist nicht lokal für: <`Store URL`>

  Nachdem Sie Secure Private Access mithilfe des Assistenten eingerichtet haben, können Sie die Gateway-Einträge auf der Registerkarte Einstellungen bearbeiten. Notieren Sie sich die StoreFront-Store-URL, für die dieser Fehler aufgetreten ist.

  **Auflösung**:

  Dieses Problem tritt auf, wenn StoreFront nicht auf derselben Maschine wie Secure Private Access installiert ist. Sie müssen die StoreFront-Konfiguration manuell auf der Maschine ausführen, auf der Sie StoreFront installiert haben.

  1. Klicken Sie auf **Einstellungen** und dann auf den Tab **Integrationen**.
  2. Identifizieren Sie unter **StoreFront Store URL**den StoreFront-URL-Eintrag, für den der Fehler aufgetreten ist.
  3. Klicken Sie neben dieser Store-URL auf die Schaltfläche Skript herunterladen und führen Sie dieses PowerShell-Skript mit Administratorrechten auf der Maschine aus, auf der sich die entsprechende StoreFront-Installation befindet.

  > **Hinweis:**
  >
  > Um das StoreFront PowerShell-Skript auszuführen, öffnen Sie das Windows x64-kompatible PowerShell-Fenster mit Administratorrechten und führen Sie dann ConfigureStoreFront.ps1 aus. Das StoreFront-Skript ist nicht mit Windows PowerShell (x86) kompatibel.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Ausfall des öffentlichen Gateways/Callback-Gateways

**Fehlermeldung**: Gateway-Eintrag konnte nicht erstellt werden für: `<Gateway URL>` ODER Callback-Gateway-Eintrag konnte nicht erstellt werden für: `<Callback Gateway URL>`

**Auflösung**:

Notieren Sie sich die öffentliche Gateway- oder Callback-Gateway-URL, für die der Fehler aufgetreten ist. Nachdem Sie Secure Private Access mithilfe des Assistenten eingerichtet haben, können Sie die Gateway-Einträge auf der Registerkarte **Einstellungen** bearbeiten.

1. Klicken Sie auf **Einstellungen** und dann auf den Tab **Integrationen**.
2. Aktualisieren Sie die öffentliche Gateway-Adresse oder die Callback-Gateway-Adresse und die virtuelle IP-Adresse, für die der Fehler aufgetreten ist.

### Secure Private Access Server ist nicht erreichbar

**Fehlermeldung**: Der IIS-Pool konnte nicht aktualisiert werden. IIS-Pool konnte nicht neu gestartet werden

**Auflösung**:

1. Gehen Sie in den Internetinformationsdiensten (IIS) zu Anwendungspools und überprüfen Sie, ob die folgenden Anwendungspools gestartet wurden und ausgeführt werden:

- Sicherer privater Zugriffs-Laufzeitpool
- Administratorpool für sicheren privaten Zugriff

Stellen Sie außerdem sicher, dass die Standard-IIS-Website `"Default Web Site"` aktiv ist.

### Fehler bei der Überprüfung der Datenbankkonnektivität

**Fehlermeldung:** Konnektivitätsprüfung fehlgeschlagen

Die Überprüfung der Datenbankkonnektivität kann aus mehreren Gründen fehlschlagen:

- Der Datenbankserver ist aufgrund einer Firewall nicht vom Hostcomputer des Secure Private Access-Plug-ins aus erreichbar.

  **Lösung:** Überprüfen Sie, ob der Datenbankport (Standardport 1433) auf der Firewall geöffnet ist.

- Der Hostcomputer des Secure Private Access Plug-ins ist nicht berechtigt, eine Verbindung zur Datenbank herzustellen.

  **Lösung:** Siehe SQL-Datenbankberechtigungen für Secure Private Access.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### Die Gateway-Konnektivitätsprüfung ist fehlgeschlagen. Das öffentliche Zertifikat kann nicht abgerufen werden

**Fehlermeldung:** Die Konfiguration nach der Installation schlägt mit dem Fehler „Gateway-Konnektivitätsprüfung fehlgeschlagen“fehl. Ein öffentliches Zertifikat kann nicht abgerufen werden …”

**Auflösung:**

- Laden Sie das öffentliche Gateway-Zertifikat mithilfe des Konfigurationstools manuell in die Secure Private Access-Datenbank hoch.
- Öffnen Sie die PowerShell oder das Eingabeaufforderungsfenster mit Administratorrechten.
- Ändern Sie das Verzeichnis in den Ordner Admin\AdminConfigTool im Secure Private Access-Installationsordner (z. B. cd “C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool” )
- Führen Sie den folgenden Befehl aus:

```
.\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```

### Probleme mit der Authentifizierung

Die IIS-Authentifizierungskonfiguration des Secure Private Access-Laufzeitdienstes funktioniert möglicherweise nicht, da die integrierte Windows-Authentifizierung (IWA) nicht unterstützt wird.

### Sonstiges

#### Supportpaket für Secure Private Access-Diagnosen erstellen

Gehen Sie wie folgt vor, um ein Secure Private Access-Diagnosesupportpaket zu erstellen:

- Öffnen Sie die PowerShell oder das Eingabeaufforderungsfenster mit Administratorrechten.
- Ändern Sie das Verzeichnis in den Ordner Admin\ AdminConfigTool im Secure Private Access-Installationsordner (z. B. cd “C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ AdminConfigTool“).
- Führen Sie den folgenden Befehl aus:

```
.\AdminConfigTool.exe /SUPPORTBUNDLE <output folder>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

### SQL-Datenbankberechtigungen für Secure Private Access

Für die automatische Datenbankerstellung muss der Secure Private Access-Plug-in-Hostcomputer über die Berechtigungen verfügen, eine Verbindung mit der Datenbank herzustellen und ein Datenbankschema zu erstellen.

**Entfernte Datenbank:**

Führen Sie die folgenden Schritte aus, um die Berechtigungen für eine entfernte Datenbank einzurichten.

1. Erstellen Sie eine leere Datenbank mit der Namenssyntax `CitrixAccessSecurity<Site Name>`. `<Site Name>` ist hier der Name der Secure Private Access-Site. (zum Beispiel CitrixAccessSecuritySPA).

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. Erstellen Sie eine SQL-Serveranmeldung für die Maschinenidentität für die virtuelle Secure Private Access-Maschine. Wenn Ihr Secure Private Access Broker-Maschinenname beispielsweise HOST1 ist und die Maschinendomäne DOMAIN1 ist, dann lautet die Maschinenidentität "DOMAIN1\HOST1$". Wenn die Anmeldung bereits erstellt wurde, können Sie diesen Schritt ignorieren.

   ```
   USE CitrixAccessSecurity<SiteName>
   ```

   ```
   CREATE LOGIN [DOMAIN1\HOST1$] FROM WINDOWS
   ```

   Der Domänenname kann mit der folgenden Abfrage gefunden werden:

   ```
   SELECT DEFAULT_DOMAIN()[DomainName]
   ```

3. Weisen Sie der Maschinenidentität die Rolle db_owner zu.

   ```
   USE CitrixAccessSecurity<SiteName>
   ```

   ```
   EXEC sys.sp_addrolemember [db_owner], 'DOMAIN1\HOST1$'
   ```

   ```
   ALTER USER [DOMAIN1\HOST1$] WITH DEFAULT_SCHEMA = dbo;
   ```

**Lokale Datenbank:**

Führen Sie die folgenden Schritte aus, um die Berechtigungen für eine lokale Datenbank einzurichten.

1. Erstellen Sie eine leere Datenbank mit der Namenssyntax `CitrixAccessSecurity<Site Name>`. `<Site Name>` ist hier der Name der Secure Private Access-Site. (z. B. CitrixAccessSecuritySpa).

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

2. Erstellen Sie eine SQL-Serveranmeldung für den Benutzer `NT AUTHORITY\SYSTEM`. Wenn die Anmeldung bereits erstellt wurde, können Sie diesen Schritt ignorieren.

   ```
   USE CitrixAccessSecurity<SiteName>
   CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS
   ```

3. Weisen Sie dem Benutzer "NT AUTHORITY\SYSTEM"die Rolle db_owner zu.

   ```
   USE CitrixAccessSecurity<SiteName>
   EXEC sys.sp_addrolemember [db_owner], 'NT AUTHORITY\SYSTEM'
   ALTER USER [NT AUTHORITY\SYSTEM] WITH DEFAULT_SCHEMA = dbo;
   ```

Wenn Sie die Datenbank manuell erstellen, fügt das heruntergeladene Datenbankskript der Maschinenidentität die Berechtigungen hinzu.

## Secure Private Access deinstallieren

December 27, 2023

Sie können Secure Private Access über **Systemsteuerung > Programme > Programme und Funktionen**deinstallieren.

1. Wählen Sie **Citrix Virtual Apps and Desktops 7 2308 - Secure Private Access**.
2. Klicken Sie auf **Deinstallieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm und schließen Sie die Deinstallation ab.

> **Hinweis:**
>
> Wenn das Secure Private Access-Setup nach der Installation abgeschlossen ist, laden Sie vor der Deinstallation von Secure Private Access die Datei StoreFrontScripts.zip von der Admin-Konsole herunter, um das Secure Private Access-Plug-In aus der StoreFront-Store-Konfiguration zu entfernen.

Gehen Sie wie folgt vor, um die Datei StorefrontScripts.zip herunterzuladen:

1. Melden Sie sich bei der Secure Private Access-Administrationskonsole an.
2. Klicken Sie auf **Einstellungen** und dann auf den Tab **Integrationen**.
3. Klicken Sie im Abschnitt StoreFront-Store-URL auf **Skript herunterladen**.

### Secure Private Access-Plug-In aus der StoreFront-Storekonfiguration entfernen

Nach der Deinstallation von Secure Private Access müssen Sie das Secure Private Access-Plug-In aus der StoreFront-Storekonfiguration entfernen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Melden Sie sich bei der StoreFront-Maschine an.
2. Laden Sie die Datei StoreFrontScripts.zip herunter.
3. Entpacken Sie StoreFrontScripts.zip in einen Ordner.
4. Öffnen Sie ein PowerShell-Fenster mit Administratorrechten.
5. Führen Sie den folgenden Befehl aus:

```
cd <unzipped folder>
.\RemoveStorefrontConfiguration.ps1
```

## Secure Private Access 2308-Kompatibilität mit älteren Versionen

February 16, 2024

Secure Private Access 2308 ist nicht mit den älteren Versionen (Secure Private Access for on-premises V1.0 und V1.5) kompatibel. NetScaler Gateway muss mit dem neuen Skript konfiguriert werden, wie weiter oben unter NetScaler Gateway konfigurierenbeschrieben. Im Citrix Virtual Apps and Desktops Delivery Controller für Secure Private Access 2308 ist keine Konfiguration erforderlich.

Die beste Methode zur Migration von lokalen Secure Private Access-Legacy-Versionen (1.0 und 1.5) auf 2308 besteht darin, Folgendes zu bereinigen:

- Citrix Virtual Apps and Desktops Delivery Controller aus Web-/SaaS-Apps
- Aktualisieren Sie Citrix StoreFront auf die Standardkonfiguration oder erstellen Sie einen neuen Store auf StoreFront
- NetScaler Gateway

### Bereinigung des Delivery Controller Citrix Virtual Apps and Desktops

Die Secure Private Access-Anwendungen, die auf dem Citrix Virtual Apps and Desktops Delivery Controller erstellt wurden, können manuell oder mithilfe des PowerShell-Skripts entfernt werden.

**Manuell**:

1. Öffnen Sie Citrix Studio oder Citrix WebStudio.
2. Klicken Sie auf **Anwendungen**.
3. Wählen Sie die App aus, klicken Sie mit der rechten Maustaste und wählen Sie dann **Löschen**.

**Mithilfe eines Skripts**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

1. Rufen Sie die aktuellen Secure Private Access-Apps ab, indem Sie den folgenden Befehl ausführen:

   ```
   Get-BrokerApplication -Description "KEYWORDS:SPAENABLED"
   ```

   Einzelheiten finden Sie unter Remove-BrokerApplication.

2. Führen Sie nach der Überprüfung der Apps den folgenden Befehl aus, um sie zu entfernen:

   ```
   Get-BrokerApplication -Description "KEYWORDS:SPAENABLED"| Remove-BrokerApplication
   ```

### Citrix StoreFront-Bereinigung

Sie können entweder einen neuen StoreFront-Store erstellen oder den vorhandenen Store bereinigen.

- Neuen StoreFront-Store erstellen: Sie müssen einen neuen StoreFront-Store für Secure Private Access 2308 erstellen, da die vorhandenen StoreFront-Stores, die für die älteren Versionen erstellt wurden, nicht mit 2308 kompatibel sind. Dies ist die empfohlene Option, um Probleme im Zusammenhang mit der Konfiguration zu vermeiden.
- Vorhandenen StoreFront-Store bereinigen: Der vorhandene Store auf StoreFront kann manuell oder mithilfe des Skripts bereinigt werden. Die beste Option für die on-premises Migration von Secure Private Access auf 2308 besteht jedoch darin, einen neuen Store auf StoreFront zu erstellen.

**Manuell**:

1. Suchen und entfernen Sie policy.json (z. B. C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser\pol
2. Suchen und entfernen Sie die Ordner SecureBrowser (z. B. C:\inetpub\wwwroot\Citrix\Store\Resources\Secu und Resources (z. B. C:\inetpub\wwwroot\Citrix\Store\Resources)
3. Entfernen Sie den Knoten “route”aus web.config (Sie finden ihn in C:\inetpub\wwwroot\Citrix\Store) mit dem Namen “WebSecurePolicy”, das an die URL “Resources\SecureBrowser\policy.json” weiterleitet.
4. Starten Sie die **Standardwebsite in der Internet Information Service (IIS) -Manager-Konsole** neu, um die Änderungen zu übernehmen.

**Mithilfe eines Skripts**:

1. Laden Sie das Skript von der https://www.citrix.com/downloads/citrix-secure-private-access/herunter .
2. Laden Sie das Skript auf eine StoreFront-Maschine hoch.
3. Führen Sie das Skript als Administrator auf PowerShell aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

4. Geben Sie den Store-Namen ein.

   Das Skript entfernt den Ordner, den Unterordner und die Dateien C:\inetpub\wwwroot\Citrix\Store\Resource
   und aktualisiert die Datei web.config.

5. Starten Sie die **Standardwebsite in der Internet Information Service (IIS) -Manager-Konsole** neu, um die Änderungen zu übernehmen.

## NetScaler Gateway-Bereinigung

### Virtueller NetScaler Gateway-Server

Der virtuelle NetScaler Gateway-Server, der für ältere Versionen (1.0 und 1.5) erstellt wurde, kann für Secure Private Access 2308 wiederverwendet werden.

- Informationen zum Aktualisieren eines vorhandenen NetScaler Gateways finden Sie unter [Ein vorhandenes NetScaler Gateway aktualisieren].
- Informationen zur Konfiguration eines neuen NetScaler Gateway finden Sie unter [NetScaler Gateway konfigurieren].

### Sitzungsrichtlinien und Aktionen

Sitzungsrichtlinien und Aktionen, die für ältere Versionen (1.0 und 1.5) erstellt wurden, können von Secure Private Access 2308 wiederverwendet werden.

- Informationen zum Aktualisieren vorhandener NetScaler Gateway-Sitzungsrichtlinien/Aktionen finden Sie unter NetScaler Gateway-Sitzungsaktionen.
- Informationen zur Konfiguration eines neuen NetScaler Gateway finden Sie unter NetScaler Gateway konfigurieren

Das Skript erstellt auch vollständig konfigurierte Sitzungsrichtlinien/Aktionen.

### Richtlinien zur Autorisierung

Autorisierungsrichtlinien, die auf NetScaler Gateway für ältere Versionen (1.0 und 1.5) erstellt wurden, können Secure Private Access 2308-Richtlinien stören und den Datenfluss unterbrechen.

Sie können wie folgt vorgehen, um die Autorisierungsrichtlinien zu bereinigen.

- Trennen Sie manuell die Autorisierungsrichtlinien von Authentifizierungs- und Autorisierungsgruppen, die als Standardgruppen auf NetScaler Gateway verwendet werden. In diesem Fall können die Richtlinien wiederverwendet werden.
- Entfernen Sie die Autorisierungsrichtlinien.

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 

# Benachrichtigungen von Drittanbietern

December 27, 2023

Citrix Secure Private Access for on-premises

© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.