Citrix Secure Private Access –Vor Ort

Machine translated content

Disclaimer

Contents

Technische Übersicht

August 26, 2024

Citrix Secure Private Access on-premises ist eine vom Kunden verwaltete Zero Trust Network Access (ZTNA) -Lösung, die sicheren Zugriff auf interne Web-/SaaS- und TCP/UDP-Anwendungen mit den folgenden Funktionen sowie einer nahtlosen Endbenutzererfahrung bietet:

- VPN ohne Zugriff für SaaS und interne Web-Apps
- Prinzip der geringsten Privilegien
- Single Sign-On (SSO)
- Multifaktorauthentifizierung
- Beurteilung des Gerätestatus
- Sicherheitskontrollen auf Anwendungsebene
- App Protection-Features

Die Lösung verwendet die on-premises StoreFront-App und die Citrix Workspace-App, um einen nahtlosen und sicheren Zugriff auf interne Web-/SaaS- und TCP/UDP-Apps im Citrix Enterprise Browser zu ermöglichen. Diese Lösung verwendet auch NetScaler Gateway, um Authentifizierungs- und Autorisierungskontrollen durchzusetzen.

Die lokale Citrix Secure Private Access-Lösung verbessert die allgemeine Sicherheits- und Compliance-Situation eines Unternehmens durch die Möglichkeit, mithilfe des on-premises StoreFront-Portals als einheitliches Zugriffsportal für interne Web-/SaaS- und TCP/UDP-Apps sowie virtuelle Apps und Desktops als integrierten Bestandteil von Citrix Workspace auf einfache Weise Zero-Trust-Zugriff auf browserbasierte Apps (interne Web-/SaaS-Apps) und Client-Server-Apps (TCP/UDP-Apps) bereitzustellen.

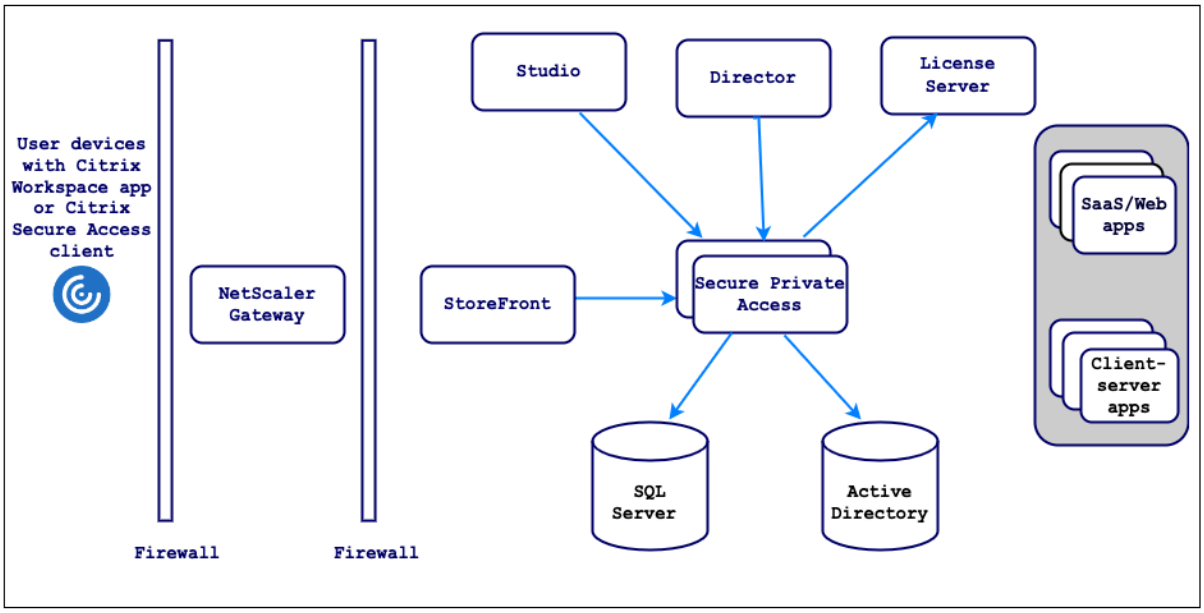
Citrix Secure Private Access kombiniert die Elemente von NetScaler Gateway und StoreFront, um Endbenutzern und Administratoren ein integriertes Erlebnis zu bieten.

Funktionalität	Service/Komponente, die die Funktionalität bereitstellt
Konsistente Benutzeroberfläche zum Zugriff auf Apps	StoreFront vor Ort/Citrix Workspace-App
SSO zu SaaS und Web-Apps	NetScaler Gateway
Multifaktor-Authentifizierung (MFA) und Gerätestatus (auch bekannt als Endpunktanalyse)	NetScaler Gateway
Sicherheitskontrollen und App-Schutzkontrollen für Web- und SaaS-Apps	Citrix Enterprise Browser

Funktionalität	Service/Komponente, die die Funktionalität bereitstellt
Richtlinien zur Autorisierung	Secure Private Access
Durchsetzung des Zugriffs	NetScaler Gateway- und Citrix Secure Access-Clients
Konfiguration und Management	Secure Private Access
Sichtbarkeit, Überwachung und Fehlerbehebung	Secure Private Access, NetScaler Console (früher ADM) und Citrix Director

Komponenten

Diese Abbildung zeigt die Komponenten einer typischen Secure Private Access-Bereitstellung.



Informationen zu den einzelnen Komponenten finden Sie unter Hauptkomponenten.

Was ist neu

October 21, 2024

August 2024

Anwendungserkennung

Mithilfe der Anwendungserkennungsfunktion erhält ein Administrator Einblick in die internen privaten Anwendungen wie Webanwendungen und Client-Server-Anwendungen (TCP- und UDP-basierte Anwendungen) in seiner Organisation und in die Benutzer, die auf diese Anwendungen zugreifen. Administratoren können die Apps ermitteln, indem sie den Umfang der Domänen (Platzhalterdomänen) oder IP-Subnetze angeben. Weitere Einzelheiten finden Sie unter Ermitteln von Domänen oder IP-Adressen, auf die Endbenutzer zugreifen.

Tool zur Richtlinienmodellierung

Das Tool zur Richtlinienmodellierung (**Zugriffsrichtlinien > Richtlinienmodellierung**) unterstützt Administratoren bei der Analyse und Behebung von Konfigurationsproblemen innerhalb der Administratorkonsole. Einzelheiten finden Sie unter Richtlinienmodellierungstool.

Neuer App-Typ für TCP/UDP-Server-zu-Client-Verbindungen hinzugefügt

Secure Private Access unterstützt jetzt einen neuen App-Typ **TCP/UDP** –**Server zu Client** , der für die folgenden Anwendungsfälle verwendet werden kann.

- **Unterstützung für Intranet-IP-Adressen:** –Intranet-IP-Adressen können verwendet werden, um Benutzer für Sicherheitsprüfungen, Netzwerksegmentierung und Compliance IP-Adressen zuzuordnen. Weitere Informationen zu Intranet-IP-Adressen finden Sie unter Adresspools konfigurieren.
- **Server-zu-Client-Verbindungen:** - Server-zu-Client-Verbindungen können zum Verwalten und Warten einer Netzwerkumgebung wie der folgenden verwendet werden:
  - Domänenbasiertes Richtlinien-Push mithilfe der Gruppenrichtlinie.
  - Softwareverteilung mithilfe von Microsoft Endpoint Configuration Manager oder ähnlichen Lösungen.
  - Fernunterstützung zur Fehlerbehebung und Fehlerbehebung bei Benutzerarbeitsplätzen.
- **Client-zu-Client-Verbindungen:** –Client-zu-Client-Verbindungen ermöglichen zwei Remotecomputern die direkte Kommunikation miteinander, um Daten in einem privaten, gemeinsam genutzten oder öffentlichen Netzwerk zu teilen und zu empfangen, ohne die Sicherheit und Flexibilität zu beeinträchtigen.

Einzelheiten zum Konfigurieren einer TCP/UDP-Server-zu-Client-App finden Sie unter TCP/UDP-Server-Client-Apps konfigurieren.

Behobene Probleme

October 21, 2024

Die folgenden Probleme werden in Version 2408 behoben.

Domänencontrollerkonfiguration

Das alternative UPN-Suffix wird von Secure Private Access für die Intranet-Anmeldung (StoreFront) und die Internet-/Extranet-App-Aufzählung (Gateway) nicht unterstützt.

Administratorverwaltung

Änderungen der RBAC-Rolle des Administrators werden erst angezeigt, nachdem die aktuelle Sitzung ungültig gemacht wurde (durch Abmeldung oder Ablauf des Tokens).

Anwendungsstart

Der Anwendungsstart schlägt fehl, wenn alle der folgenden Bedingungen erfüllt sind:

- Es werden Netscaler-Versionen 13.0.x, 13.1 vor 13.1-48.47 und 14.1 vor 14.1–4.42 verwendet.
- LDAP-UPNs werden mit einem anderen Suffix als die eigentliche Domäne konfiguriert.

Admin-Konsole

- Die Seite **App bearbeiten** wird nicht automatisch geschlossen, nachdem die Seite **App bearbeiten** (**Sicherer privater Zugriff> Anwendungen > Anwendung bearbeiten**) einer veröffentlichten Anwendung nicht geschlossen wird, nachdem ein zugehöriger Domäneneintrag geändert wurde.

  Wenn die zugehörige Domäne, die Sie beim Erstellen einer App eingegeben haben, beispielsweise `www.example.com`war. Nachdem die App veröffentlicht wurde, ersetzen Sie die zugehörige Domäne `www.example.com` durch `abc.com`und klicken auf **Speichern**. Die Seite **App bearbeiten** wird nicht geschlossen, obwohl die App erfolgreich aktualisiert wurde.
- Wenn beim Hinzufügen einer App der App-Name ein Komma enthält, wird eine Warnung angezeigt. Die App wird jedoch erstellt.
- Wenn eine App-URL `www`enthält, wird die URL in der Routing-Domänentabelle (**Einstellungen > Anwendungsdomäne**) ohne das Präfix `www`gespeichert.

Upgrades

Wenn für den Secure Workspace Access-Verwaltungsdienst ein benutzerdefiniertes SSL-Zertifikat verwendet wird, muss das Zertifikat erneut an die Site „Citrix Access Security Admin“im Internet Information Service (IIS) gebunden werden.

Bekannte Probleme

October 21, 2024

In Version 2408 treten die folgenden Probleme auf.

> **Hinweis:**
>
> Einigen Problemen wird eine Tracking-ID nur zur internen Referenz zugewiesen und diese hat keine Auswirkungen auf den Kunden.

Domänencontrollerkonfigurationen

- Die unidirektionale oder bidirektionale Vertrauensstellung mit dem Vertrauenstyp „Forest“zwischen Domänen in verschiedenen AD-Forests wird nicht unterstützt.

  Wenn sich beispielsweise die Domänen a.com und b.com in zwei unterschiedlichen AD-Gesamtstrukturen befinden und SPA auf einem Computer installiert ist, auf dem die Domäne mit a.com / b.com verbunden ist, können andere Domänenbenutzer nicht auf die von SPA veröffentlichten Apps zugreifen.

  [SPAOP-2031]

- Wenn die Domäne des Computers, auf dem Secure Private Access für vor Ort installiert ist, nicht mit der Domäne des bei Secure Private Access angemeldeten Administrators übereinstimmt, müssen Sie Folgendes tun:

  Fügen Sie sowohl für den Secure Private Access-Administrator als auch für den Laufzeitdienst ein anderes Domänendienstkonto als Identität im IIS-Anwendungspool hinzu.

  [SPAOP-1558]

- Verteilergruppen werden in Secure Workspace Access nicht unterstützt. Daher können Richtlinien nicht nach Verteilergruppen suchen, um Benutzer- und Gruppenbedingungen hinzuzufügen.

- Secure Private Access erfasst die Domänendetails nicht in der Administratorkonsole oder im Dienst. Es hängt daher vollständig von der vom Benutzer angegebenen Domäne ab. Wenn

die entsprechende Domäne nicht erreichbar ist oder der Domänenname kein gültiger Name ist, wird diese Domäne daher nicht unterstützt.

NetScaler Gateway

- Der virtuelle SSL-Server mit SSL-Profilkonfiguration wird im folgenden Szenario nicht unterstützt:
  - 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 Umschalter finden Sie unter Unterstützung für Smart-Access-Tags.

RfWeb / Arbeitsbereich für das Web

- RfWeb/Workspace für das Web wird nicht unterstützt und daher werden die Apps nicht aufgelistet. Einzelheiten finden Sie unter Bei Verwendung von StoreFront Version 2311 oder höher.

  [SPAOP-2487]

Anwendungsstart

- Wenn die Regler `ns_vpn_enable_spa_onprem` und `toggle_vpn_enable_securebrowse_clien` nicht aktiviert sind oder wenn diese Regler in Ihrem NetScaler Gateway nicht unterstützt werden, schlägt der App-Start nach der Rotation `CustomHeaderCryptoKey` fehl. Die `CustomHeaderCryptoKey` -Rotation erfolgt automatisch nach 30 Tagen.

  [SPAOP-4528]

- Der Anwendungsstart schlägt fehl, wenn LDAP-UPN und sAMAccountName unterschiedlich sind.

  [SPAOP-1412]

StoreFront

- In **Stores > Unified Experience konfigurieren**muss der Standardempfänger für die Website auf /Citrix/<`StoreName`>Web konfiguriert werden. In früheren Versionen von StoreFront ist

der Standardempfänger für die Website auf einen leeren Wert eingestellt und das funktioniert nicht für Secure Private Access. Außerdem wird auf dem Client die frühere Version der Receiver-Benutzeroberfläche angezeigt. Informationen zur StoreFront-Konfiguration finden Sie unter StoreFront.

- Wenn Sie StoreFront-Version 2308 oder früher verwenden, wird auf der Seite „ **Stores > Manage Delivery Controllers** “der Secure Private Access-Plug-In-Typ als **XenMobile**angezeigt. Die Funktionalität wird dadurch nicht beeinträchtigt.

Protokollieren

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

TCP/UDP-Überwachung

- Das Feature-Flag **SPAOP-3315-EnableZTNAApplications** ist in 2408 standardmäßig deaktiviert. Dies hat zur Folge, dass die TCP/UDP-Überwachungsdaten nicht gespeichert werden und die Director-Integration daher fehlschlägt.

  Problemumgehung: Wenn Sie TCP/UDP-Apps verwenden und die Director-Integration aktivieren möchten, aktualisieren Sie die Datenbank manuell, um dieses Feature-Flag zu aktivieren.

  [SPAOP-5587]

Upgrade

- Nach dem Datenbank-Upgrade werden die Modul-/Abschnittsregisterkarten in der Benutzeroberfläche für einige Zeit (ungefähr eine Stunde) nicht angezeigt.

  Problemumgehung: Starten Sie den IIS-Dienst manuell neu, wenn die Registerkarten in der Benutzeroberfläche unmittelbar nach dem Datenbankupgrade sichtbar sein sollen.

  [SPAOP-5331]

- Beim Versuch, die Versionen 2402 oder 2407 durch Ersetzen des MSI auf 2408 zu aktualisieren, wird auf der Kachel „Secure Private Access“im Citrix Virtual Apps and Desktops-Installationsprogramm **Upgrade verfügbar**angezeigt. Wenn Sie jedoch auf die Kachel „Secure Private Access“klicken, um mit dem Upgrade fortzufahren, wird Secure Private Access deinstalliert und nicht aktualisiert. Auf der Seite **Kernkomponenten** wird die Meldung „**Secure Private Access wird entfernt**“angezeigt.

[SPAOP-5495]

- Beim Upgrade von Version 2405 oder 2407 auf 2408 können Sie Secure Private Access nicht einrichten, wenn es nicht in den Versionen 2405 oder 2407 konfiguriert wurde. Der Vorgang zum Erstellen der Datenbank kann nicht fortgesetzt werden, da die Schaltfläche **Weiter** auf der Seite **Datenbankkonfiguration** ausgegraut ist.

  [SPAOP-5595]

- Wenn Sie auf 2408 aktualisieren und eine vorhandene App bearbeiten, deren URL mit www beginnt, wird im Feld **App-Konnektivität** nicht der vorherige Status angezeigt. Sie müssen den App-Konnektivitätstyp erneut auswählen. Dies ist eine einmalige Aktion nach dem Upgrade, nach der die Konfiguration gespeichert wird und weiterhin bestehen bleibt.

  [SPAOP-4216]

- Nach dem Upgrade auf 2408 können Sie sich zwar bei der Administratorkonsole anmelden, jedoch keine Anwendungen und Richtlinien verwalten. Es wird eine Fehlermeldung angezeigt.

  Problemumgehung: Sie müssen die Datenbank mithilfe der Skripts aktualisieren. Weitere Einzelheiten finden Sie unter Aktualisieren Sie die Datenbank mithilfe der Skripts.

  [SPAOP-5255]

- Nach dem Upgrade auf 2408 schlagen die Anwendungsaufzählung und der Anwendungsstart fehl.

  Problemumgehung: Sie müssen die Datenbank mithilfe der Skripts aktualisieren. Weitere Einzelheiten finden Sie unter Aktualisieren Sie die Datenbank mithilfe der Skripts.

  [SPAOP-5255]

- Sie können das Secure Private Access-Plug-In nicht von früheren Versionen auf 2408 aktualisieren, wenn das Plug-In mit dem Delivery Controller installiert wurde.

  [SPAOP-4505]

Benutzeroberfläche

- Das **Anzahl der Anwendungsstarts** Zähler im Feld **Sicherer privater Zugang > Überblick** wird für TCP/UDP-Apps nicht inkrementiert.

  [SPAOP-4201]

Systemanforderungen

October 21, 2024

Stellen Sie sicher, dass Ihr Produkt die Mindestversionsanforderungen erfüllt.

Produkt	Mindestversion
Citrix Workspace-App	Windows –2403 und höher macOS –2402 und höher
StoreFront	LTSR 2203 oder CR 2212 und höher
NetScaler	13.1, 14.1 und höher. Für eine optimierte Leistung wird empfohlen, die neuesten Builds von NetScaler Gateway, Version 13.1 oder 14.1, zu verwenden. Für TCP/UDP-Apps –14.1–25.56 und höher
Citrix Secure Access-Client	Windows-Client –24.6.1.17 und höher macOS-Client –24.06.2 und höher
Director	2402 oder höher
Betriebssystem für den Secure Private Access-Plug-in-Server	Windows Server 2019 und höher

Kommunikationsports: Stellen Sie sicher, dass Sie die erforderlichen Ports für das Secure Private Access-Plug-In geöffnet haben. Einzelheiten finden Sie unter Kommunikationsports.

Datenbanken: Nachfolgend finden Sie die Liste der unterstützten Microsoft SQL Server-Versionen für die Site-Konfiguration, die Konfigurationsprotokollierung und die Überwachungsdatenbanken:

```
- SQL Server 2022, Express, Standard und Enterprise Edition.
- SQL Server 2019, Express, Standard und Enterprise Edition.
- SQL Server 2017, Express, Standard und Enterprise Edition.

Neue Installationen: Standardmäßig wird SQL Server Express 2017 mit
   Cumulative Update 16 zusammen mit dem Controller installiert, wenn
   keine vorhandene unterstützte SQL Server-Installation erkannt wird.

Bei Upgrades werden vorhandene SQL Server Express-Versionen nicht
   aktualisiert.

Die folgenden Lösungen für hohe Verfügbarkeit der Datenbank werden
   unterstützt (außer bei SQL Server Express, das nur den eigenstä
   ndigen Modus unterstützt):
```



```
10
11  -  SQL Server Always On-Failoverclusterinstanzen
12  -  SQL Server AlwaysOn-Verfügbarkeitsgruppen (einschließlich Basisverfü
       gbarkeitsgruppen)
13  -  SQL Server-Datenbankspiegelung
14
15  Die Windows-Authentifizierung ist für Verbindungen zwischen dem
       Controller und der SQL Server-Sitedatenbank erforderlich.
16
17  Weitere Informationen zu den Datenbanken finden Sie unter [Datenbanken
       ](/de-de/citrix-virtual-apps-desktops/technical-overview/databases).
        > **Hinweis:** > > -  Secure Private Access für lokale Anwendungen
       wird in der Citrix Workspace-App für iOS und Android nicht unterstü
       tzt. > -  Der Citrix Secure Access-Client für Linux, iOS und Android
        unterstützt keine lokalen TCP/UDP-Apps von Secure Private Access.
```

Voraussetzungen

Stellen Sie zum Erstellen oder Aktualisieren eines vorhandenen NetScaler Gateways sicher, dass Sie über die folgenden Details verfügen:

- Ein Windows-Servercomputer mit laufendem IIS, konfiguriert mit einem SSL/TLS-Zertifikat, auf dem das Secure Private Access-Plug-In installiert wird.
- StoreFront-Store-URLs, die während der Einrichtung eingegeben werden müssen.
- Der Store auf StoreFront muss konfiguriert sein und die Store-Dienst-URL muss verfügbar sein. Das Format der Store-Dienst-URL ist `https://store.domain.com/Citrix/StoreSecureAccess`.
- IP-Adresse, FQDN und Rückruf-URL des NetScaler Gateways.
- IP-Adresse und FQDN des Hostcomputers des Secure Private Access-Plugins (oder eines Load Balancers, wenn das Secure Private Access-Plugin als Cluster bereitgestellt wird).
- Auf NetScaler konfigurierter Name des Authentifizierungsprofils.
- Auf NetScaler konfiguriertes SSL-Serverzertifikat.
- Domänenname.
- Die Zertifikatskonfigurationen sind abgeschlossen. Administratoren müssen sicherstellen, dass die Zertifikatskonfigurationen vollständig sind. Das Secure Private Access-Installationsprogramm konfiguriert ein selbstsigniertes Zertifikat, wenn auf dem Computer kein Zertifikat gefunden wird. Dies funktioniert jedoch möglicherweise nicht immer.

> **Hinweis:**
>
> Für den Runtime-Dienst (SecureAccess-Anwendung auf der IIS-Standardwebsite) muss die anonyme Authentifizierung aktiviert sein, da er die Windows-Authentifizierung nicht unterstützt.

> Diese Einstellungen werden standardmäßig vom Secure Private Access-Installationsprogramm festgelegt und dürfen nicht manuell geändert werden.

Anforderungen für Administratorkonten

Beim Einrichten von Secure Private Access werden die folgenden Administratorkonten benötigt.

- Installieren Sie Secure Private Access: Sie müssen mit einem lokalen Computeradministratorkonto angemeldet sein.
- Secure Private Access einrichten: Sie müssen sich bei der Secure Private Access-Administratorkonsole mit einem Domänenbenutzer anmelden, der auch lokaler Computeradministrator für den Computer ist, auf dem Secure Private Access installiert ist.
- Secure Private Access verwalten: Sie müssen sich mit einem Secure Private Access-Administratorkonto bei der Secure Private Access-Administratorkonsole anmelden.

Kommunikationsanschlüsse

In der folgenden Tabelle sind die Kommunikationsports aufgeführt, die vom Secure Private Access-Plug-In verwendet werden.

Quelle	Ziel	Typ	Port	Details
Administrator-Arbeitsstation	Plugin „Sicherer privater Zugriff“	HTTPS	4443	Secure Private Access-Plug-in – Administratorkonsole
Plugin „Sicherer privater Zugriff“	NTP-Dienst	TCP, UDP	123	Zeitsynchronisation
	DNS-Dienst	TCP, UDP	53	DNS-Suche
	Active Directory	TCP, UDP	88	Kerberos
	Director	HTTP, HTTPS	80, 443	Kommunikation mit dem Direktor zum Leistungsmanagement und zur verbesserten Fehlerbehebung

Quelle	Ziel	Typ	Port	Details
	Lizenzserver	TCP	8083	Kommunikation mit dem Lizenzserver zur Erfassung und Verarbeitung der Lizenzdaten
		TCP	389	LDAP über Klartext (LDAP)
		TCP	636	LDAP über SSL (LDAPS)
	Microsoft SQL Server	TCP	1433	Secure Private Access-Plugin – Datenbankkommunikation
	StoreFront	HTTPS	443	Authentifizierungsüberprüfung
	NetScaler Gateway	HTTPS	443	NetScaler Gateway-Rückruf
StoreFront	NTP-Dienst	TCP, UDP	123	Zeitsynchronisation
	DNS-Dienst	TCP, UDP	53	DNS-Suche
	Active Directory	TCP, UDP	88	Kerberos
		TCP	389	LDAP über Klartext (LDAP)
		TCP	636	LDAP über SSL (LDAPS)
		TCP, UDP	464	Natives Windows-Authentifizierungsprotokoll, das es Benutzern ermöglicht, abgelaufene Passwörter zu ändern
	Plugin „Sicherer privater Zugriff“	HTTPS	443	Authentifizierung und Anwendungsenumeration

Quelle	Ziel	Typ	Port	Details
	NetScaler Gateway	HTTPS	443	NetScaler Gateway-Rückruf
NetScaler Gateway	Plugin „Sicherer privater Zugriff“	HTTPS	443	Validierung der Anwendungsautorisierung
	StoreFront	HTTPS	443	Authentifizierung und Anwendungsenumeration
	Webanwendungen	HTTP, HTTPS	80, 443	NetScaler Gateway-Kommunikation mit konfigurierten Secure Private Access-Anwendungen *(Ports können je nach Anwendungsanforderungen unterschiedlich sein)*
Benutzergerät	NetScaler Gateway	HTTPS	443	Kommunikation zwischen Endgerät und NetScaler Gateway

Referenzen

- Authentifizierungsprofile.
- Funktionsweise von Authentifizierungsrichtlinien.
- Binden Sie ein SSL-Zertifikat an einen virtuellen Server (SSL) auf NetScaler.

Größenrichtlinien

October 21, 2024

Sicherer privater Zugriff auf lokale Datenbanken

Die lokale Secure Private Access-Datenbank enthält Informationen zu den Anwendungen, Richtlinien und zugehörigen Grafiken. Es enthält auch Informationen zur Fehlerbehebung und Telemetrie.

Aufgrund ihrer dynamischen Natur unterliegen die Aufzeichnungen zur Telemetrie und Fehlerbehebung häufigen Änderungen und werden nur für einen kurzen Zeitraum aufbewahrt. Daher muss eine Secure Private Access-Datenbank vor Ort konfiguriert werden, die den Bedarf an häufigen Updates berücksichtigt.

Bei internen Skalierbarkeitstests konnte die folgende Konfiguration der lokalen Secure Private Access-Datenbank eine Benutzerlast von 5.000 Benutzern bewältigen.

Komponente	Spezifikation
Prozessor	8 vCPUs
Speicher	16 GB
Netzwerk	10 GBP Netzwerk
Hostspeicher	Größe: 127 GB
^^	IOPS: 500
^^	Maximaler Durchsatz: 100
Betriebssystem	Windows Server 2022
SQL Server	SQL Server 2022 CU12
Täglicher Datenbankspeicherplatz für 5000 Benutzer	5 GB

> **Hinweis:**
>
> - Die Metriken werden unter der Annahme abgeleitet, dass die Bereinigung von Protokollereignissen deaktiviert und die Protokollaufbewahrungsdauer auf 7 Tage eingestellt ist.
> - Standardmäßig werden die Protokolle 90 Tage lang aufbewahrt, oder es werden, abhängig von den konfigurierten Einstellungen, bis zu 100.000 Protokollereignisse aufbewahrt. Diese Einstellungen sind in der Datei appsettings.json des Secure Private Access Runtime-Dienstes verfügbar und können nach Bedarf geändert werden. Einzelheiten finden Sie unter Einstellungen zum Aufbewahren von Ereignisprotokollen.

Dimensionierung des Entscheidungsservers

Die Skalierbarkeit des lokalen Secure Private Access-Servers hängt von der verwendeten Datenbank ab. In der Datenbank werden Telemetrie- und Fehlerbehebungsinformationen gespeichert. Der Umfang der Datenbank hängt vom Arbeitsspeicher, der Festplattengeschwindigkeit und der Anzahl der zur Verarbeitung der Last verwendeten CPUs ab.

Während der internen Skalierbarkeitstests wurde bestätigt, dass die folgende Konfiguration aus 3 lokalen Secure Private Access-Knoten eine Benutzerlast von 5.000 Benutzern bewältigen konnte.

Komponente	Spezifikation
Prozessor	4 vCPUs
Speicher	8 GB
Netzwerk	10 GBP
Hostspeicher	Premium SSD LRS Größe: 127 GB IOPS: 500 Maximaler Durchsatz: 100
Betriebssystem	Windows Server 2022

Installieren Sie Secure Private Access

October 21, 2024

Das sichere Private Access-Installationsprogramm ist als eigenständiges Installationsprogramm oder als Teil des integrierten Citrix Virtual Apps and Desktops-Installationsprogramms verfügbar.

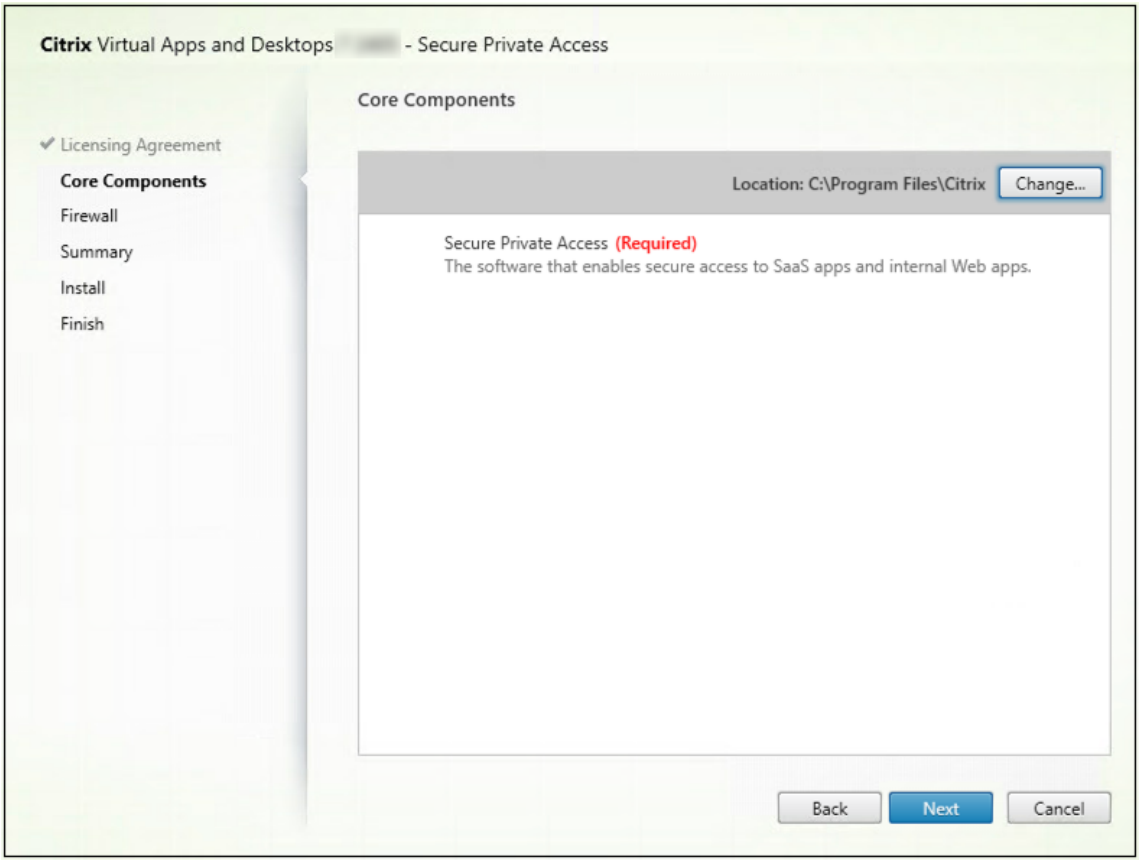
Anforderungen an das Administratorkonto zum Installieren und Verwalten von Secure Workspace Access

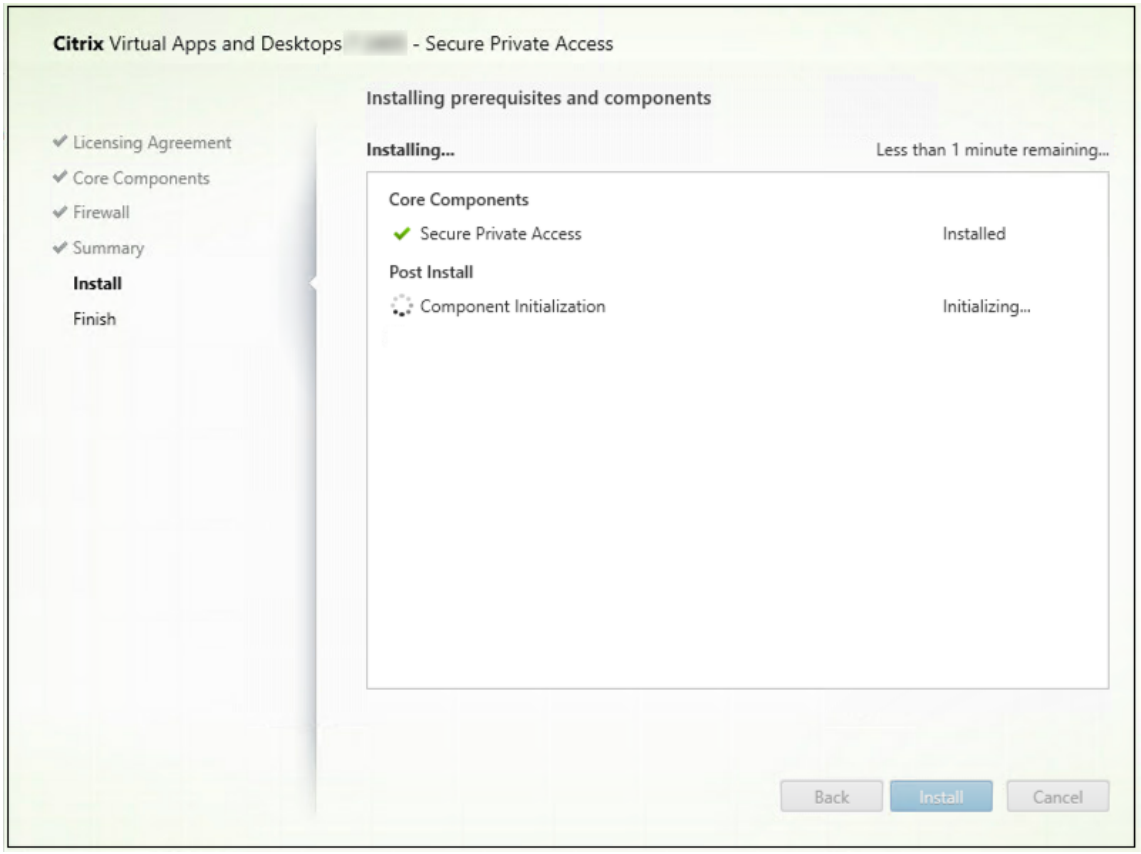
- Um Secure Private Access zu installieren, müssen Sie mit einem lokalen Computeradministratorkonto angemeldet sein.
- Um Secure Private Access einzurichten, müssen Sie sich bei der Secure Private Access-Administratorkonsole mit einem Domänenbenutzer anmelden, der auch lokaler Computeradministrator für den Computer ist, auf dem Secure Private Access installiert ist.

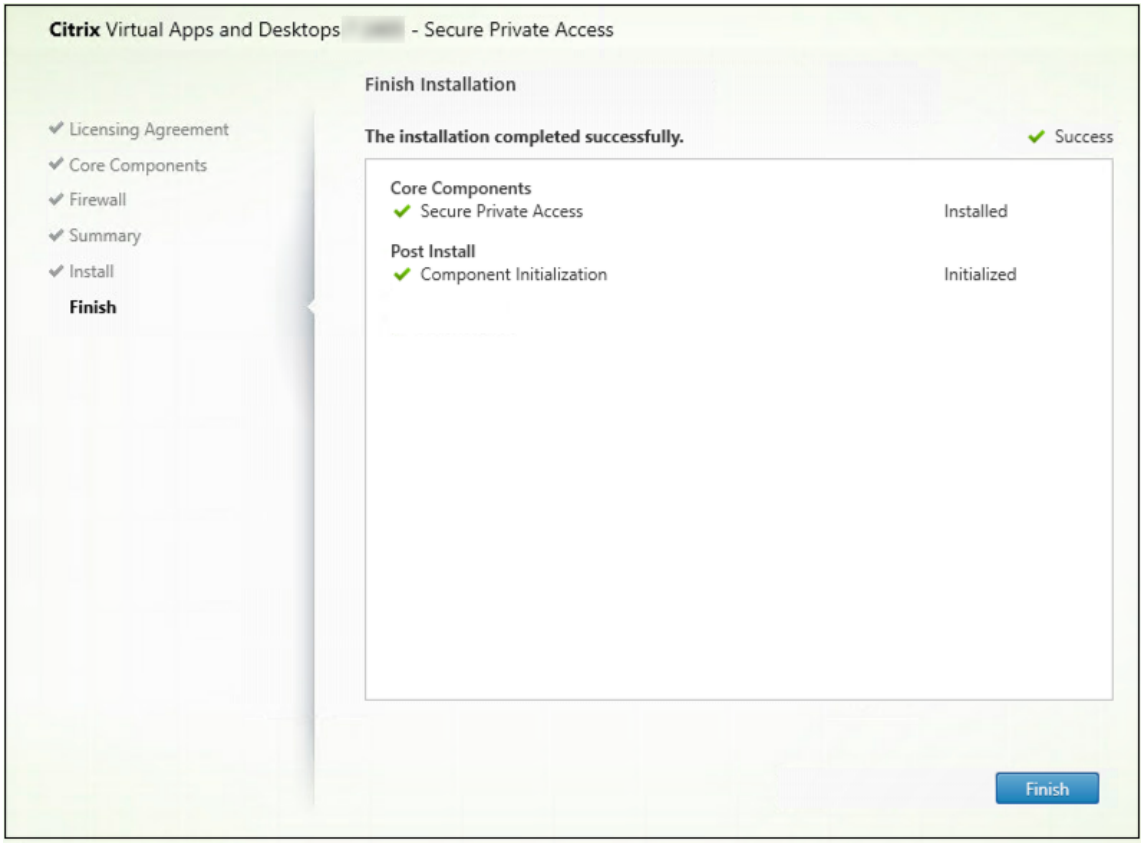
- Nachdem die Einrichtung abgeschlossen ist, wird dieser Benutzer der erste Secure Private Access-Administrator und kann dann weitere Administratoren hinzufügen.
- Um Secure Private Access nach der Einrichtung zu verwalten, müssen Sie sich mit einem Secure Private Access-Administratorkonto bei der Secure Private Access-Administratorkonsole anmelden.

Führen Sie die folgenden Schritte aus, um Secure Workspace Access zu installieren:

1. Laden Sie die Produktsoftware Citrix Virtual Apps and Desktops von https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/ herunter und starten Sie den Assistenten.
2. Klicken Sie auf **Start** neben dem zu installierenden Produkt: Virtual Apps oder Virtual Apps and Desktops.
3. Wählen Sie **Secure Private Access** und folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen.

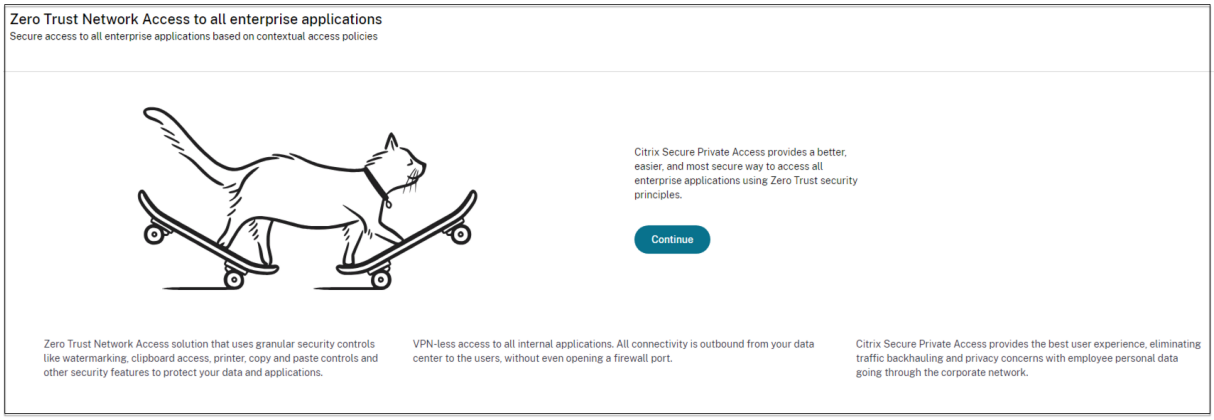




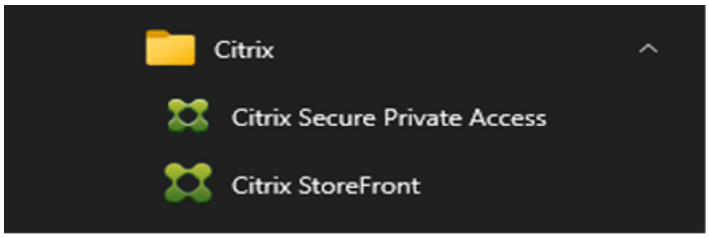


Ausführliche Schritt-für-Schritt-Anleitungen finden Sie unter Installieren der Kernkomponenten und . Installieren Sie mithilfe der Befehlszeile.

Sobald die Installation abgeschlossen ist, wird die Administratorkonsole für die Ersteinrichtung automatisch im Standardbrowserfenster geöffnet. Sie können auf **Weiter** klicken, um Secure Private Access einzurichten.



Sie können die Verknüpfung „Secure Private Access“auch im Startmenü des Desktops sehen (**Citrix > Citrix Secure Private Access)**.



SSO zur Administratorkonsole

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 für die Administratorauthentifizierung die Integrierte Windows-Authentifizierung (IWA) verwendet.

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

- Wenn Sie Ihre Anmeldeinformationen eingeben, aktivieren Sie die Anmeldung mit der integrierten Windows-Authentifizierung (IWA).
- Wenn Sie Ihre Anmeldeinformationen nicht eingeben, wird Ihnen die Anmeldeseite von Secure Private Access angezeigt.

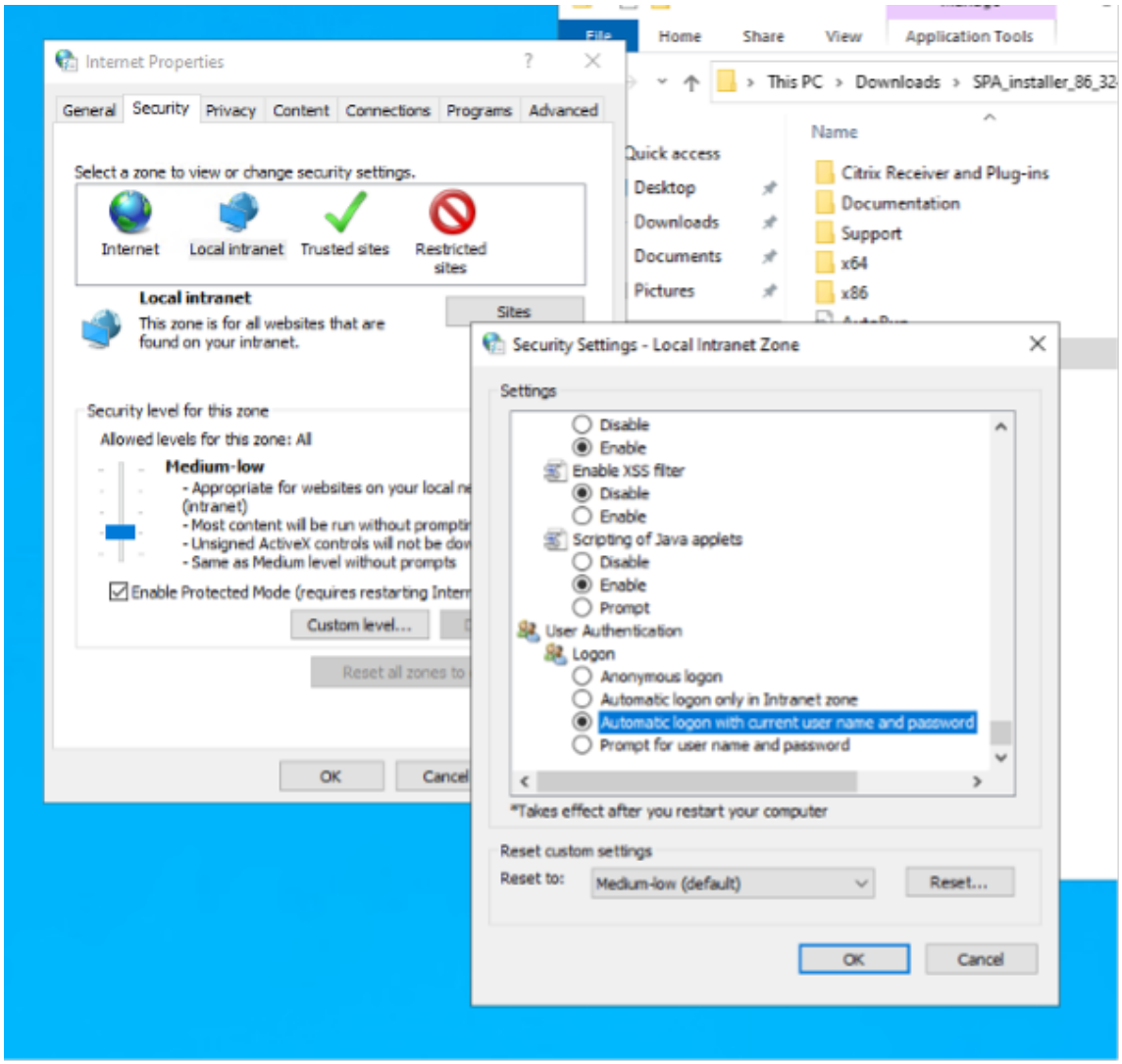
Sie müssen sich bei der Administratorkonsole anmelden, um mit der Einrichtung von Secure Private Access fortzufahren. Sie können Secure Private Access mit jedem Benutzer einrichten, der zur selben

Domäne wie der Installationscomputer gehört, sofern der Benutzer über lokale Administratorrechte auf dem Installationscomputer verfügt.

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

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

   Sie können auch ein Platzhalterzeichen verwenden, wenn Sie Secure Private Access auf mehreren Computern installieren möchten. Beispiel: `"https://*.fabrikam.local"`.
4. Klicken Sie auf **Benutzerdefinierte Ebene**.
5. Wählen Sie unter **Benutzerauthentifizierung > Anmeldung**die Option **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort**aus.



> **Hinweis:**

- Wenn Sie Inkognito-Sitzungen in Chrome 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.
- Lesen Sie bei anderen Browsern die Dokumentation des jeweiligen Browsers zur Kerberos-Authentifizierung.

Nächste Schritte

- Einrichten von Secure Private Access
- Konfigurieren von NetScaler Gateway
- Konfigurieren Sie Anwendungen
- Konfigurieren Sie Zugriffsrichtlinien für die Anwendungen

Komponenten

October 21, 2024

Im Folgenden sind die Schlüsselkomponenten eines typischen Secure Private Access für die Bereitstellung vor Ort aufgeführt.

- **StoreFront:** –StoreFront authentifiziert Benutzer und verwaltet Stores mit Desktops und Anwendungen, auf die Benutzer zugreifen. Es kann den Unternehmensanwendungsstore hosten, über den Sie Benutzern Self-Service-Zugriff auf Desktops und Anwendungen gewähren. Außerdem werden die Anwendungsabonnements, Verknüpfungsnamen und andere Daten der Benutzer verfolgt. Auf diese Weise wird eine konsistente Benutzererfahrung über mehrere Geräte sichergestellt. Einzelheiten zur Integration von StoreFront mit Secure Private Access finden Sie unter StoreFront.
- **NetScaler Gateway:** –NetScaler Gateway bietet einen einzigen sicheren Zugriffspunkt durch die Unternehmensfirewall. Einzelheiten zur Integration von NetScaler Gateway mit Secure Private Access finden Sie unter NetScaler Gateway.
- **Director:** (Optional) Director ermöglicht Ihnen eine effektive Leistungsüberwachung und Fehlerbehebung. Um Director in Secure Private Access zu integrieren, müssen Sie die IP-Adresse des FQDN des Director-Servers eingeben, der bei Secure Private Access registriert sein muss. Einzelheiten zur Integration von Director mit Secure Private Access finden Sie unter Integration von Secure Private Access mit Director.

- **Lizenzserver:** Der Lizenzserver sammelt und verarbeitet Lizenzdaten. Einzelheiten zur Integration des Lizenzservers mit Secure Private Access finden Sie unter Integration des Lizenzservers mit Secure Private Access.
- **Web Studio:** Citrix Secure Private Access ist in die Web Studio-Konsole integriert, um Benutzern einen nahtlosen Zugriff auf den Dienst über Web Studio zu ermöglichen. Einzelheiten zur Integration von Secure Private Access in Web Studio finden Sie unter Integration von Secure Private Access in Web Studio.

Informationen zu den Mindestversionsanforderungen dieser Produkte finden Sie unter Systemanforderungen.

> **Hinweis:**
>
> Director und License Server sind ab Version 2402 in Secure Private Access integriert.

StoreFront

June 19, 2024

Wenn Secure Private Access zusammen mit StoreFront gehostet wird, erfolgt die Secure Private Access-Konfiguration in StoreFront automatisch durch den Assistenten für die Erstinstallation.

Wenn Secure Private Access jedoch nicht gemeinsam mit StoreFront gehostet wird, müssen bestimmte Konfigurationsänderungen manuell vorgenommen werden.

Führen Sie die folgenden Schritte aus, um StoreFront manuell zu konfigurieren.

1. Laden Sie das Skript von der Secure Private Access-Administratorkonsole herunter (**Einstellungen > Integrationen**).
2. Klicken Sie auf **Skript herunterladen** , das dem StoreFront-Eintrag entspricht, für den die Konfigurationsänderungen vorgenommen werden müssen.

   Die heruntergeladene ZIP-Datei enthält ein Konfigurationsskript, eine README-Datei und ein Konfigurationsbereinigungsskript. Das Bereinigungsskript kann verwendet werden, falls die Integration zwischen StoreFront und Secure Private Access entfernt werden soll.
3. Führen Sie das Skript als Administrator auf einer PowerShell-64-Bit-Instanz aus, indem Sie den Befehl verwenden `./ConfigureStorefront.ps1`.

   - Es sind keine weiteren Parameter erforderlich.
   - Die PowerShell-Skriptausführungsrichtlinie muss **auf Uneingeschränkt** oder **Bypass** gesetzt sein, um das StoreFront-Skript auszuführen.

- Das Skript gibt die Konfiguration auch an andere StoreFront-Server weiter, wenn StoreFront als Cluster konfiguriert ist.

Sobald StoreFront mit den Secure Private Access-Einstellungen konfiguriert ist, kann die Secure Private Access-Plug-in-Konfiguration in der StoreFront-Admin-Benutzeroberfläche (Bildschirm "**Delivery Controller verwalten** ") angezeigt werden.

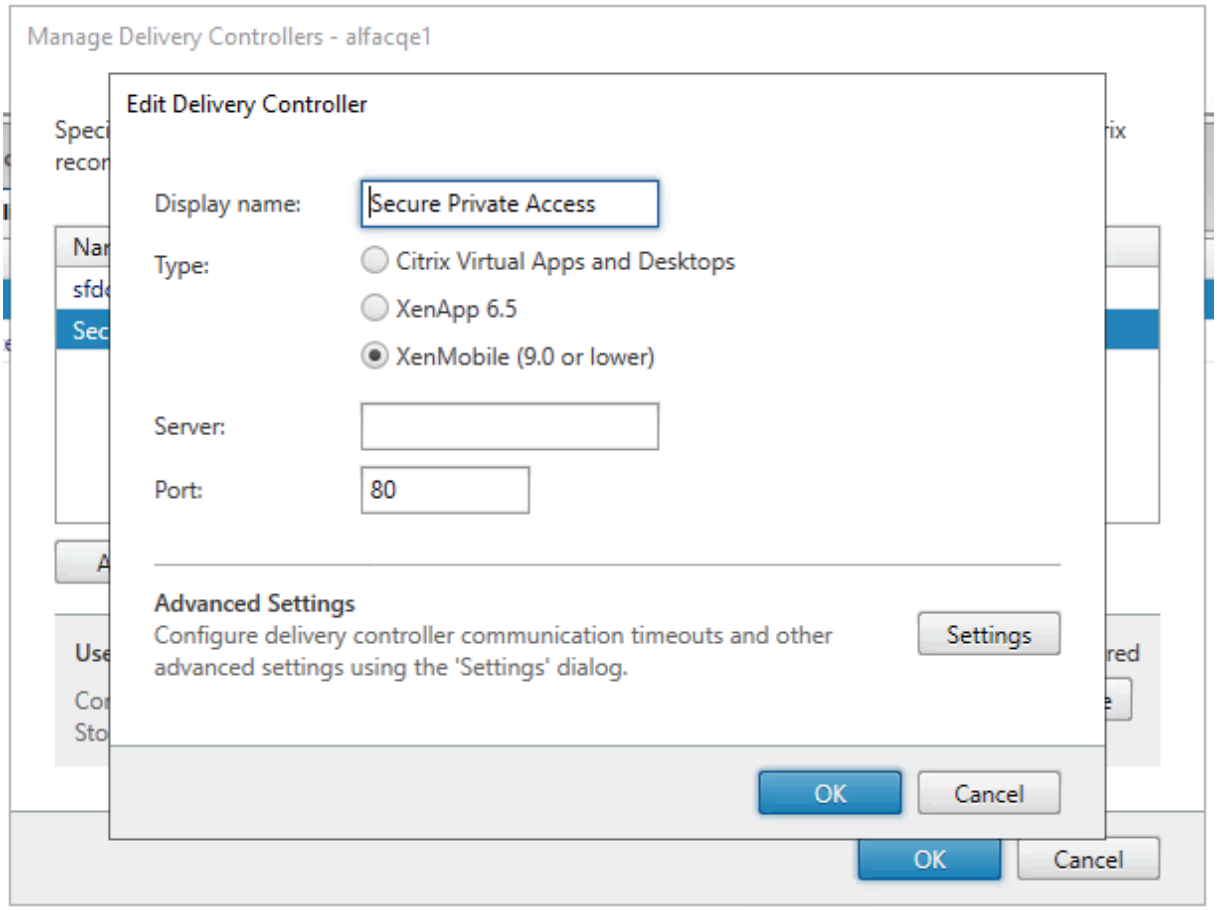
Das StoreFront-Skript konfiguriert automatisch die Aggregationsgruppeneinstellung für Secure Private Access, wenn diese für den Citrix Virtual Apps and Desktops Delivery Controller konfiguriert ist. Standardmäßig konfiguriert das Skript Secure Private Access für alle (**Konfiguration von Benutzerzuordnung und Aggregation mehrerer Websites > Konfiguriert**).

> **Wichtig:**
>
> - Es wird empfohlen, das von der Secure Private Access-Administratorschnittstelle heruntergeladene StoreFront-Skript zu verwenden, um StoreFront nur für Secure Private Access zu konfigurieren. Konfigurieren Sie Secure Private Access nicht über die StoreFront-Admin-Benutzeroberfläche, da die Benutzeroberfläche nicht die gesamte erforderliche Konfiguration auf StoreFront abdeckt. Das Skript muss ausgeführt werden, um alle erforderlichen Konfigurationen abzuschließen.
> - Eine Secure Private Access-Site kann auch in mehreren StoreFront-Bereitstellungen konfiguriert werden (entweder in einem anderen Store auf derselben StoreFront-Bereitstellung oder in einer anderen StoreFront-Bereitstellung).
>   StoreFront kann über die Seite **Einstellungen > Integrationen** hinzugefügt werden.
> - Die automatische StoreFront-Konfiguration funktioniert nicht auf der Seite **Einstellungen > Integration** , auch wenn Secure Private Access gemeinsam mit StoreFront gehostet wird. Die Autokonfiguration erfolgt nur bei der Ersteinrichtung. Wenn auf der Seite "**Einstellungen**"eine neue Storekonfiguration hinzugefügt wird, muss das StoreFront-Skript heruntergeladen und auf der entsprechenden StoreFront-Maschine ausgeführt werden.

Bei Verwendung von StoreFront Version 2308 oder früher

Wenn Sie StoreFront Version 2308 oder früher verwenden, hat die StoreFront-Admin-Benutzeroberfläche die folgenden bekannten Probleme:

- Der Secure Private Access Plug-in-Typ wird als XenMobile angezeigt.
- Die Secure Private Access-Server-URL wird nicht angezeigt.
- Der Secure Private Access-Port wird immer als 80 angezeigt.



Bei Verwendung von StoreFront Version 2311 oder höher

In StoreFront Version 2311 und höher listet der Citrix Workspace für Web Client die Secure Private Access-Apps nicht auf. Das liegt daran, dass Secure Private Access den Start der Secure Private Access-App auf der Workspace for Web-Plattform nicht unterstützt.

NetScaler Gateway

October 21, 2024

Die NetScaler Gateway-Konfiguration wird sowohl für Web-/SaaS- als auch für TCP/UDP-Anwendungen unterstützt. Sie können ein NetScaler Gateway erstellen oder eine vorhandene NetScaler Gateway-Konfiguration für Secure Private Access aktualisieren. Es wird empfohlen, dass Sie NetScaler-Snapshots erstellen oder die NetScaler-Konfiguration speichern, bevor Sie diese Änderungen anwenden.

Ausführliche Informationen zu NetScaler Gateway-Konfigurationen für Web-/SaaS- und TCP/UDP-Anwendungen finden Sie in den folgenden Themen:

- NetScaler Gateway-Konfiguration für Web-/SaaS-Anwendungen
- NetScaler Gateway-Konfiguration für TCP/UDP-Anwendungen

Kompatibilität mit den ICA-Apps

Zur Unterstützung des Secure Private Access-Plug-Ins erstelltes oder aktualisiertes NetScaler Gateway kann auch zum Aufzählen 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 Bereitstellung von Citrix Virtual Apps and Desktops.

Ausführliche Informationen 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

> **Hinweis:**
>
> - Die in diesem Abschnitt bereitgestellten Informationen sind nur anwendbar, wenn Ihre NetScaler Gateway-Version vor 14.1-25.56 liegt.
> - Wenn Ihre NetScaler Gateway-Version 14.1–25.56 oder höher ist, können Sie das Secure Private Access-Plug-In auf NetScaler Gateway mithilfe der CLI oder GUI aktivieren. Weitere Einzelheiten finden Sie unter Secure Private Access-Plug-in auf NetScaler Gateway aktivieren.

In den folgenden Versionen sendet NetScaler Gateway die Tags automatisch. Sie müssen die Gateway-Rückrufadresse 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-Plugin-Anforderung 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 (FreeBSD-Shell) umschalten:

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

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

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

- Aktivieren Sie die Umleitung auf die Seite „Zugriff eingeschränkt“, wenn der Zugriff verweigert wird.

  ```
  nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny
  ```

- Verwenden Sie die auf CDN gehostete Seite „Zugriff eingeschränkt“.

  ```
  nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
  ```

- Zum Deaktivieren führen Sie denselben Befehl erneut aus.
- Um zu überprüfen, ob der Schalter ein- oder ausgeschaltet ist, führen Sie den Befehl `nsconmsg` aus.
- Informationen zum Konfigurieren von Smart Access-Tags auf NetScaler Gateway finden Sie unter Kontextbezogene Tags konfigurieren.

Einstellungen des Secure Private Access-Plugins auf NetScaler beibehalten

Gehen Sie wie folgt vor, um die Einstellungen des Secure Workspace Access-Plugins auf NetScaler beizubehalten:

1. Erstellen oder aktualisieren Sie die Datei /nsconfig/rc.netscaler.
2. Fügen Sie der Datei die folgenden Befehle hinzu.

   ```
   nsapimgr -ys call=ns_vpn_enable_spa_onprem
   nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode
   nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny

   nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
   ```

3. Speichern Sie die Datei.

Die Einstellungen des Secure Private Access-Plugins werden beim Neustart von NetScaler automatisch angewendet.

Aktivieren Sie das Secure Private Access-Plugin auf NetScaler Gateway

Ab NetScaler Gateway 14.1–25.56 und höher können Sie das Secure Private Access-Plug-In auf NetScaler Gateway mithilfe der NetScaler Gateway-CLI oder der GUI aktivieren. Diese Konfiguration ersetzt den Knopf `nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem` , der in Versionen vor 2407 verwendet wurde.

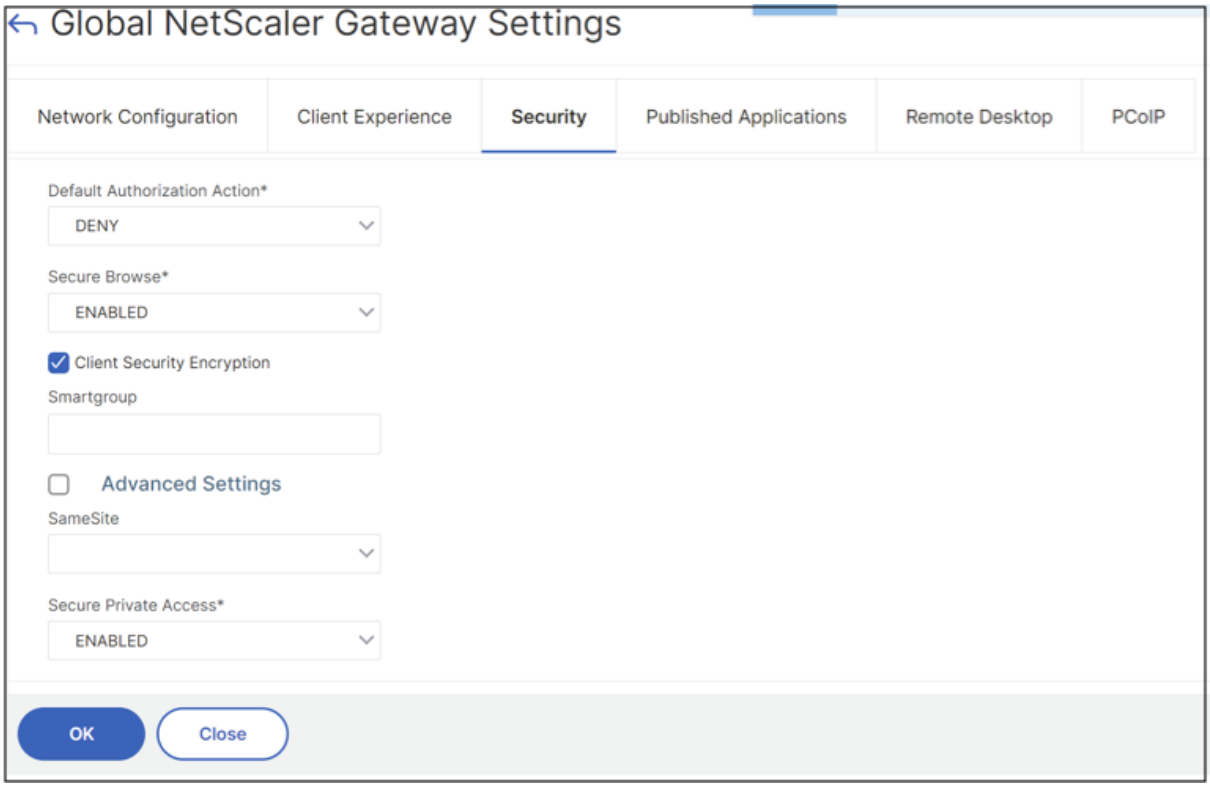
CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set vpn parameter -securePrivateAccess ENABLED
```

Benutzeroberfläche (GUI):

1. Navigieren Sie zu **NetScaler Gateway > Globale Einstellungen > Globale NetScaler Gateway-Einstellungen ändern**.
2. Klicken Sie auf die Registerkarte **Sicherheit** .
3. Wählen Sie unter **Sicherer privater Zugriff**die Option **AKTIVIERT aus.**



Öffentliches Gateway-Zertifikat hochladen

Wenn das öffentliche Gateway vom Secure Private Access-Computer aus nicht erreichbar ist, müssen Sie ein öffentliches Gateway-Zertifikat in die Secure Private Access-Datenbank hochladen.

Führen Sie die folgenden Schritte aus, um ein öffentliches Gateway-Zertifikat hochzuladen:

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

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

Bekannte Einschränkungen

- Vorhandene NetScaler Gateways können per Skript aktualisiert werden, es kann jedoch eine unendliche Zahl möglicher NetScaler-Konfigurationen geben, die nicht durch ein einzelnes Skript abgedeckt werden können.
- Verwenden Sie keinen ICA-Proxy auf dem NetScaler Gateway. Diese Funktion ist deaktiviert, wenn NetScaler Gateway konfiguriert ist.
- Wenn Sie in der Cloud bereitgestellten NetScaler verwenden, müssen Sie Änderungen im Netzwerk vornehmen. Erlauben Sie beispielsweise die Kommunikation zwischen NetScaler und anderen Komponenten auf 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 StoreFront-DNS-Eintrag mit einer privaten StoreFront-IP-Adresse hinzufügen.

NetScaler Gateway-Konfiguration für Web-/SaaS-Anwendungen

October 21, 2024

Führen Sie die folgenden Schritte aus, um NetScaler Gateway für Web-/SaaS-Anwendungen zu erstellen:

1. Laden Sie das neueste Skript *ns_gateway_secure_access.sh* herunter. von https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/.
2. Laden Sie diese Skripte auf die NetScaler-Maschine hoch. Sie können die WinSCP-App oder den SCP-Befehl verwenden. Zum Beispiel *scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp*.

   Beispiel: *scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp*

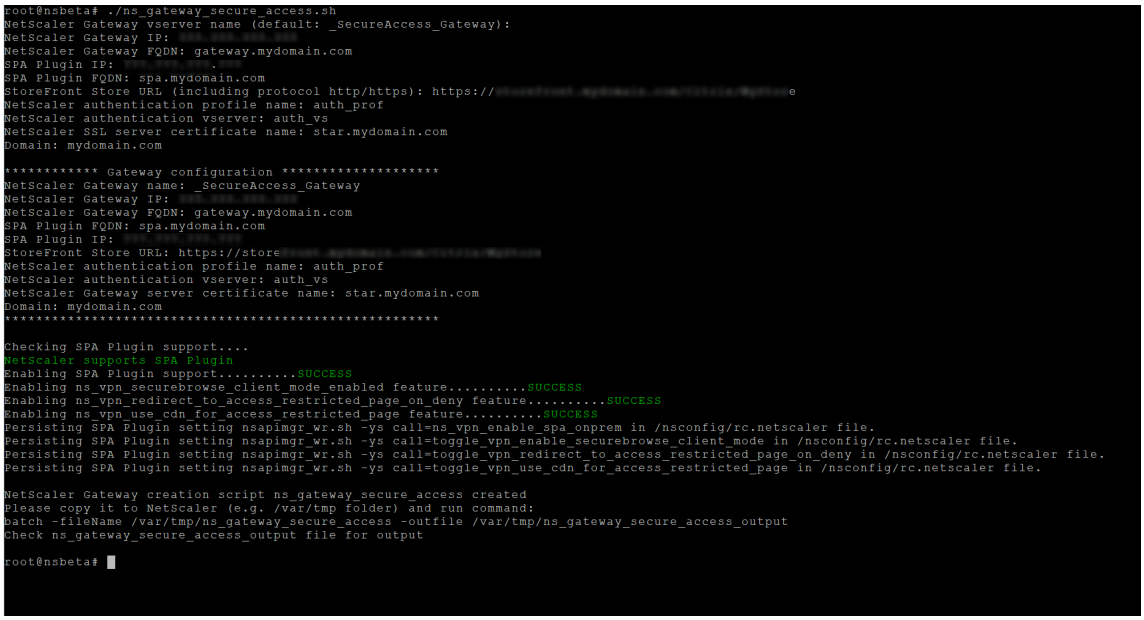
Hinweis:

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

1. Stellen Sie per SSH eine Verbindung zu NetScaler her und wechseln Sie zur Shell (geben Sie „Shell“in die NetScaler-CLI ein).
2. Machen Sie das hochgeladene Skript ausführbar. Verwenden Sie dazu den Befehl chmod.

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

3. Führen Sie das hochgeladene Skript auf der NetScaler-Shell aus.



4. Geben Sie **N** für den Parameter **TCP/UDP-App-Typ-Unterstützung aktivieren** ein, wenn Sie das Gateway nur für Web- und SaaS-Anwendungen konfigurieren möchten.
5. Geben Sie die erforderlichen Parameter ein. Die Liste der Parameter finden Sie unter Voraussetzungen.

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

   Es wird eine neue Datei mit mehreren NetScaler-Befehlen (der Standard ist var/tmp/ns_gateway_secure_access) generiert.

> **Hinweis:**
>
> Während der Skriptausführung wird die Kompatibilität der Plug-Ins NetScaler und Secure Private Access überprüft. Wenn NetScaler das Plug-In „Secure Private Access“unterstützt, aktiviert das Skript die NetScaler-Funktionen zur Unterstützung von Smart Access-Tags, die Verbesserungen senden und auf eine neue Deny-Page umleiten, wenn der Zugriff auf eine Ressource eingeschränkt ist. Einzelheiten zu Smarttags finden Sie unter Unterstützung für Smart Access-Tags.
>
> Die in der Datei /nsconfig/rc.netscaler gespeicherten Funktionen des Secure Private Access-Plugins ermöglichen es, sie nach dem Neustart von NetScaler aktiviert zu halten.

```
1 ![NetScaler-Konfiguration 2](/en-us/citrix-secure-private-access/media/
     spaop-configure-netscaler2-old.png)
```

1. Wechseln Sie zur NetScaler-CLI und führen Sie die resultierenden NetScaler-Befehle aus der neuen Datei mit dem Batch-Befehl aus. Zum 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. Wenn ein Befehl fehlschlägt, wird mit dem nächsten Befehl fortgefahren.

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

2. Stellen Sie sicher, dass alle Befehle erfolgreich ausgeführt werden.

> **Hinweis:**
>
> Wenn ein Fehler auftritt, führt NetScaler dennoch die verbleibenden Befehle aus und erstellt/aktualisiert/bindet teilweise Ressourcen. Wenn daher aufgrund eines falschen Parameters ein unerwarteter Fehler auftritt, wird empfohlen, die Konfiguration von Anfang an zu wiederholen.

Aktualisieren Sie die vorhandene NetScaler Gateway-Konfiguration für Web- und SaaS-Apps

Sie können das Skript `ns_gateway_secure_access_update.sh`auf einem vorhandenen NetScaler Gateway verwenden, um die Konfiguration für Web- und SaaS-Apps zu aktualisieren. Wenn Sie jedoch die vorhandene Konfiguration (NetScaler Gateway Version 14.1–4.42 und höher) manuell aktualisieren möchten, verwenden Sie die Beispielbefehle , um eine vorhandene NetScaler Gateway-Konfigurationzu aktualisieren. Außerdem müssen Sie den virtuellen Server und die Sitzungsaktionseinstellungen von NetScaler Gateway aktualisieren.

> **Hinweis:**
>
> Ab NetScaler Gateway 14.1–25.56 und höher können Sie das Secure Private Access-Plug-In auf NetScaler Gateway mithilfe der NetScaler Gateway-CLI oder der GUI aktivieren. Weitere Einzelheiten finden Sie unter Secure Private Access-Plug-in auf NetScaler Gateway aktivieren.

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

- Vorhandener virtueller NetScaler Gateway-Server
- Vorhandene 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 des virtuellen NetScaler Gateway-Servers

Wenn Sie den vorhandenen virtuellen NetScaler Gateway-Server hinzufügen oder aktualisieren, stellen Sie sicher, dass die folgenden Parameter auf die definierten Werte eingestellt sind. Beispielbefehle finden Sie unter Beispielbefehle zum Aktualisieren einer vorhandenen NetScaler Gateway-Konfiguration.

Einen virtuellen Server hinzufügen:

- TCPProfileName: nstcp_default_XA_XD_profile
- Bereitstellungstyp: ICA_STOREFRONT (nur mit dem Befehl `add vpn vserver` verfügbar)
- icaOnly: AUS

Aktualisieren Sie einen virtuellen Server:

- TCPProfileName: nstcp_default_XA_XD_profile
- icaOnly: AUS

Einstellungen für NetScaler Gateway-Sitzungsaktionen

Die Sitzungsaktion ist an einen virtuellen Gateway-Server mit Sitzungsrichtlinien gebunden. Wenn Sie eine Sitzungsaktion erstellen oder aktualisieren, stellen Sie sicher, dass die folgenden Parameter auf die definierten Werte eingestellt sind. Beispielbefehle finden Sie unter Beispielbefehle zum Aktualisieren einer vorhandenen NetScaler Gateway-Konfiguration.

- `transparenteInterception`: AUS
- SSO: EIN

- `ssoCredential`: PRIMÄR
- `verwendenMIP`: NS
- `useIIP`: AUS
- `icaProxy`: AUS
- `wihome`: `"https://storefront.mydomain.com/Citrix/MyStoreWeb"` –durch die echte Store-URL ersetzen. Der Pfad zum Store `/Citrix/MyStoreWeb` ist optional.
- `ClientChoices`: AUS
- `ntDomain`: mydomain.com –wird für SSO verwendet (optional)
- `Standardautorisierungsaktion`: ERLAUBEN
- `authorizationGroup`: SecureAccessGroup (Stellen Sie sicher, dass diese Gruppe erstellt wird, sie wird verwendet, um Secure Private Access-spezifische Autorisierungsrichtlinien zu binden)
- `clientlessVpnMode`: EIN
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: AKTIVIERT
- `Storefronturl`: `"https://storefront.mydomain.com"`
- `sfGatewayAuthType`: Domäne

Beispielbefehle zum Aktualisieren einer vorhandenen NetScaler Gateway-Konfiguration

Einen virtuellen Server hinzufügen/aktualisieren.

- `add vpn vserver SecureAccess_Gateway SSL 999.999.999.999 443 -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -authnProfile auth_prof_name -icaOnly OFF`
- `set vpn vserver SecureAccess_Gateway -icaOnly OFF`

Fügen Sie eine Sitzungsaktion hinzu.

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


```
useIIP OFF -icaProxy OFF -wihome "https://storefront.example.
corp/Citrix/SPAWeb"-ClientChoices OFF -ntDomain example.corp -
clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -
SecureBrowse ENABLED -storefronturl "https://storefront.example.
corp"-sfGatewayAuthType domain
```

Fügen Sie eine Sitzungsrichtlinie hinzu.

- `add vpn sessionPolicy PL_OSspaonprem "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")"AC_OSspaonprem`
- `add vpn sessionPolicy PL_WBspaonprem "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"plugin\").NOT"AC_WBspaonprem`

Binden Sie die Sitzungsrichtlinie an den virtuellen VPN-Server.

- `bind vpn vserver SecureAccess_Gateway -policy PL_OSspaonprem -priority 111 -gotoPriorityExpression NEXT -type REQUEST`
- `bind vpn vserver SecureAccess_Gateway -policy PL_WBspaonprem -priority 110 -gotoPriorityExpression NEXT -type REQUEST`

Binden Sie das Secure Private Access-Plug-In an den virtuellen VPN-Server.

- `bind vpn vserver spaonprem -appController "https://spa.example.corp"`

Einzelheiten zu den Sitzungsaktionsparametern finden Sie unter vpn-sessionAction.

Weitere Informationen

Weitere Informationen zu NetScaler Gateway für Secure Private Access finden Sie in den folgenden Themen:

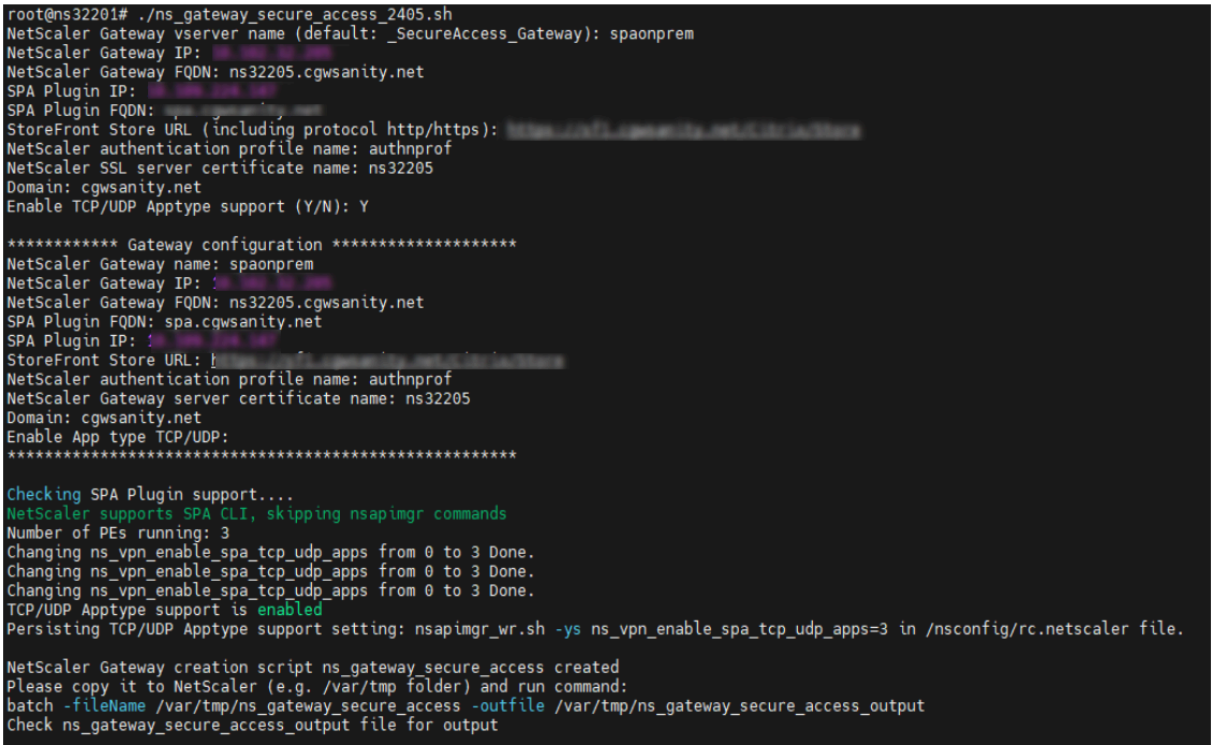
- Kompatibilität mit den ICA-Apps
- Unterstützung für Smart Access-Tags
- Einstellungen des Secure Private Access-Plugins auf NetScaler beibehalten
- Aktivieren Sie das Secure Private Access-Plugin auf NetScaler Gateway
- Öffentliches Gateway-Zertifikat hochladen
- Bekannte Einschränkungen

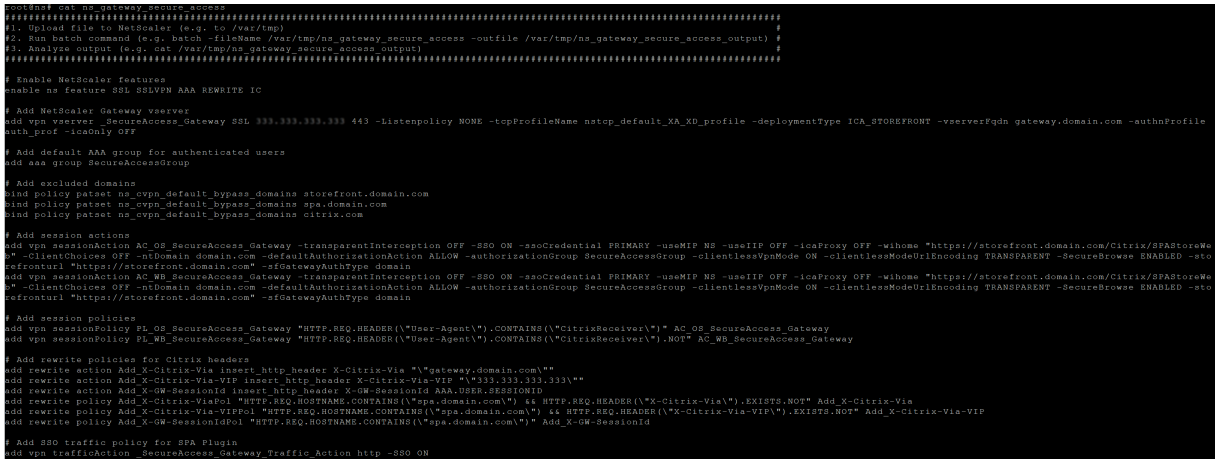
NetScaler Gateway-Konfiguration für TCP/UDP-Anwendungen

October 21, 2024

Sie können das in NetScaler Gateway-Konfiguration für Web-/SaaS-Anwendungen beschriebene Verfahren verwenden, um TCP/UDP-Anwendungen zu konfigurieren. Um das Gateway für TCP/UDP-Anwendungen zu konfigurieren, müssen Sie die TCP/UDP-Unterstützung aktivieren, indem Sie **Y** fürs **Aktivieren der Unterstützung von TCP/UDP-App-Typen** im Skript ein.

Die folgende Abbildung zeigt den für die TCP/UDP-Unterstützung aktivierten Parameter **„TCP/UDP-App-Typ-Unterstützung aktivieren“** .





Aktualisieren Sie die vorhandene NetScaler Gateway-Konfiguration für TCP/UDP-Apps

Wenn Sie die Konfiguration von früheren Versionen auf 2407 aktualisieren, wird empfohlen, die Konfiguration manuell zu aktualisieren. Einzelheiten finden Sie unter Beispielbefehle zum Aktualisieren einer vorhandenen NetScaler Gateway-Konfiguration. Außerdem müssen Sie den virtuellen Server und die Sitzungsaktionseinstellungen von NetScaler Gateway aktualisieren.

Einstellungen des virtuellen NetScaler Gateway-Servers

Wenn Sie den vorhandenen virtuellen NetScaler Gateway-Server hinzufügen oder aktualisieren, stellen Sie sicher, dass die folgenden Parameter auf die definierten Werte eingestellt sind. Beispielbefehle finden Sie unter Beispielbefehle zum Aktualisieren einer vorhandenen NetScaler Gateway-Konfiguration. Außerdem müssen Sie den virtuellen Server und die Sitzungsaktionseinstellungen von NetScaler Gateway aktualisieren.

Einen virtuellen Server hinzufügen:

- TCPProfileName: nstcp_default_XA_XD_profile
- Bereitstellungstyp: ICA_STOREFRONT (nur mit dem Befehl `add vpn vserver` verfügbar)
- icaOnly: AUS

Aktualisieren Sie einen virtuellen Server:

- TCPProfileName: nstcp_default_XA_XD_profile
- icaOnly: AUS

Einzelheiten zu den Parametern des virtuellen Servers finden Sie unter vpn-sessionAction.

NetScaler Gateway-Sitzungsrichtlinieneinstellungen

Die Sitzungsaktion ist an einen virtuellen Gateway-Server mit Sitzungsrichtlinien gebunden. Wenn Sie eine Sitzungsaktion erstellen oder aktualisieren, stellen Sie sicher, dass die folgenden Parameter auf die definierten Werte eingestellt sind. Beispielbefehle finden Sie unter Beispielbefehle zum Aktualisieren einer vorhandenen NetScaler Gateway-Konfiguration. Außerdem müssen Sie den virtuellen Server und die Sitzungsaktionseinstellungen von NetScaler Gateway aktualisieren.

- `transparenteInterception`: EIN
- `SSO`: EIN
- `ssoCredential`: PRIMÄR
- `verwendenMIP`: NS
- `useIIP`: AUS
- `icaProxy`: AUS

- ClientChoices: EIN
- ntDomain: mydomain.com –wird für SSO verwendet (optional)
- Standardautorisierungsaktion: ERLAUBEN
- Autorisierungsgruppe: Sichere Zugriffsgruppe
- clientlessVpnMode: AUS
- clientlessModeUrlEncoding: TRANSPARENT
- SecureBrowse: AKTIVIERT

Beispielbefehle zum Aktualisieren einer vorhandenen NetScaler Gateway-Konfiguration

> **Hinweis:**
>
> Wenn Sie die vorhandene Konfiguration manuell aktualisieren, müssen Sie zusätzlich zu den folgenden Befehlen die Datei /nsconfig/rc.netscaler mit dem Befehl `nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3`aktualisieren.

- Fügen Sie eine VPN-Sitzungsaktion hinzu, um Citrix Secure Access-basierte Verbindungen zu unterstützen.

```
add vpn sessionAction AC_AG_PLGspaonprem -splitDns BOTH -splitTunnel
 ON -transparentInterception ON -defaultAuthorizationAction ALLOW
 -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential
PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -ClientChoices ON -
ntDomain example.corp -clientlessVpnMode OFF -clientlessModeUrlEncoding
 TRANSPARENT -SecureBrowse ENABLED
```

- Fügen Sie eine VPN-Sitzungsrichtlinie hinzu, um Citrix Secure Access-basierte Verbindungen zu unterstützen.

```
add vpn sessionPolicy PL_AG_PLUGINspaonprem "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && (HTTP.REQ
.HEADER(\"User-Agent\").CONTAINS(\"plugin\")|| HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"CitrixSecureAccess\"))"AC_AG_PLGspaonprem
```

- Binden Sie die Sitzungsrichtlinie an den virtuellen VPN-Server, um Citrix Secure Access-basierte Verbindungen zu unterstützen.

```
bind vpn vserver spaonprem -policy PL_AG_PLUGINspaonprem -priority
 105 -gotoPriorityExpression NEXT -type REQUEST
```

- Fügen Sie eine HTTP-Callout-Richtlinie hinzu, um die Autorisierungsvalidierung für TCP/UDP-basierte Verbindungen zu unterstützen.

> **Hinweis:**
>
> Dieser Schritt ist nur erforderlich, wenn Ihre NetScaler Gateway-Version niedriger als 14.1-29.x ist.

```
`add policy httpCallout SecureAccess_httpCallout_TCP -IPAddress
   192.0.2.24 -port 443  -returnType BOOL -httpMethod POST -hostExpr "
   \"spa.example.corp\"" -urlStemExpr "\"/secureAccess/authorize\"" -
   headers Content-Type("application/json") X-Citrix-SecureAccess-Cache
   ("dstip="+HTTP.REQ.HEADER("CSIP").VALUE(0)+"&sessid="+aaa.user.
   sessionid) -bodyExpr q/"{
 "+"\"userName\":\""+aaa.USER.NAME.REGEX_REPLACE(re#\\#,"\\\\",ALL)+"
    \","+"\"domain\":\""+aaa.USER.DOMAIN+"\","+"\"customTags\":\""+http
    .REQ.HEADER("X-Citrix-AccessSecurity").VALUE(0)+"\","+"\"
    gatewayAddress\":\"ns224158.example.corp\","+"\"userAgent\":\"
    CitrixSecureAccess\","+"\"applicationDomain\":\""+http.REQ.HEADER("
    CSHOST").VALUE(0)+"\","+"\"smartAccessTags\":\""+aaa.user.attribute
    ("smartaccess_tags")+"\",\"applicationType\":\"ztna\",\"
    applicationDetails\":{
 \"destinationIp\":\""+HTTP.REQ.HEADER("CSIP").VALUE(0)+"\",\"
    destinationPort\":\""+HTTP.REQ.HEADER("PORT").VALUE(0)+"\",\"
    protocol\":\"TCP\" }
  }
 "/ -scheme https -resultExpr "http.RES.HEADER(\"X-Citrix-SecureAccess-
    Decision\").contains(\"ALLOW\")"`

wobei
-  **192.0.2.24** ist die IP-Adresse des Secure Private Access-Plugins
-  **spa.example.corp** ist der FQDN des Secure Private Access-Plugins
-  **ns224158.example.corp** ist der FQDN des virtuellen Gateway-VPN-
   Servers
```

- Fügen Sie eine Autorisierungsrichtlinie hinzu, um TCP/UDP-basierte Verbindungen zu unterstützen.

  ```
  add authorization policy SECUREACCESS_AUTHORIZATION_TCP "HTTP.REQ
  .URL.EQ(\"/cs\")&& HTTP.REQ.HEADER(\"PRTCL\").EQ(\"TCP\")&& sys.
  HTTP_CALLOUT(SecureAccess_httpCallout_TCP)"ALLOW
  ```

- Binden Sie die Autorisierungsrichtlinie an die Authentifizierungs- und Autorisierungsgruppe, um TCP/UDP-basierte Anwendungen zu unterstützen.

  ```
  bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION_TCP
   -priority 1010 -gotoPriorityExpression END
  ```

- Binden Sie das Secure Private Access-Plug-In an den virtuellen VPN-Server.

  ```
  bind vpn vserver spaonprem -appController "https://spa.example.
  corp"
  ```


Weitere Informationen

Weitere Informationen zum NetScaler Gateway für Secure Private Access finden Sie in den folgenden Themen:

- Kompatibilität mit den ICA-Apps
- Unterstützung für Smart Access-Tags
- Einstellungen des Secure Private Access-Plugins auf NetScaler beibehalten
- Aktivieren Sie das Secure Private Access-Plugin auf NetScaler Gateway
- Öffentliches Gateway-Zertifikat hochladen
- Bekannte Einschränkungen

Kontextbezogene Tags

October 21, 2024

Das Plug-In „Secure Private Access“bietet kontextbezogenen Zugriff (Smart Access) auf Web- oder SaaS-Anwendungen basierend auf dem Kontext der Benutzersitzung wie Geräteplattform und Betriebssystem, installierte Software und Geolokalisierung.

Administratoren können der Zugriffsrichtlinie Bedingungen mit kontextbezogenen Tags hinzufügen. Das kontextbezogene Tag auf dem Secure Private Access-Plug-In ist der Name einer NetScaler Gateway-Richtlinie (Sitzung, Vorauthentifizierung, EPA), die auf die Sitzungen der authentifizierten Benutzer angewendet wird.

Das Plug-In „Secure Private Access“kann Smart Access-Tags als Header (neue Logik) oder durch Rückrufe an das Gateway empfangen. Einzelheiten finden Sie unter Smart-Access-Tags.

> **Hinweis:**
>
> - Ab NetScaler Gateway 14.1-25.x werden nFactor EPA-Richtlinien unterstützt.
> - Wenn Ihre NetScaler Gateway-Version niedriger als 14.1-25.x ist, können auf NetScaler Gateway nur klassische Gateway-Vorauthentifizierungsrichtlinien konfiguriert werden.

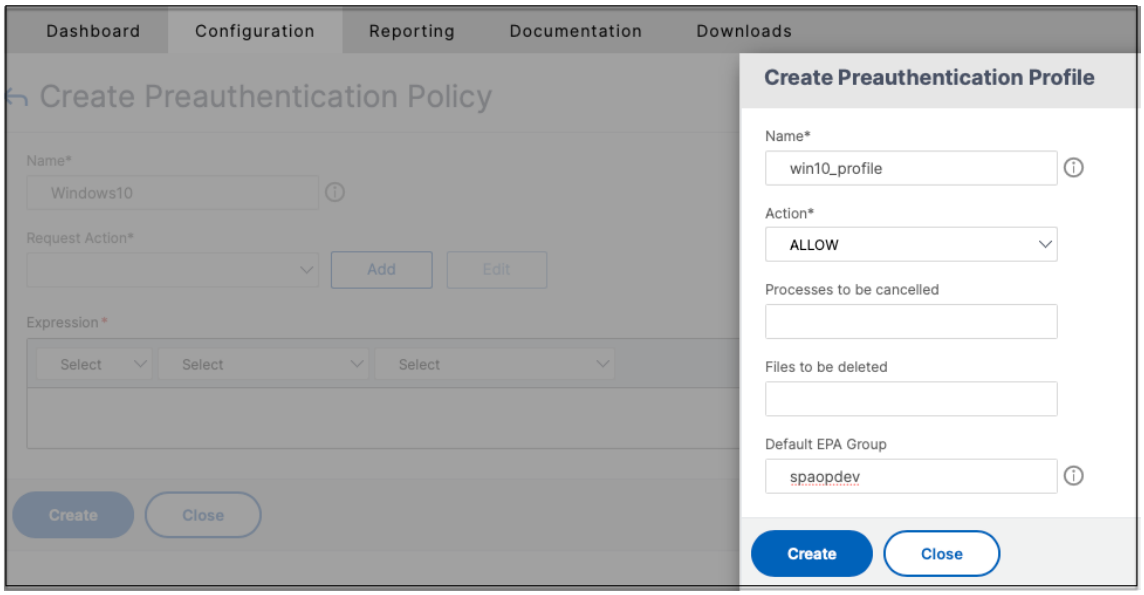
Konfigurieren Sie benutzerdefinierte Tags mithilfe der GUI

Die Konfiguration kontextbezogener Tags umfasst die folgenden allgemeinen Schritte.

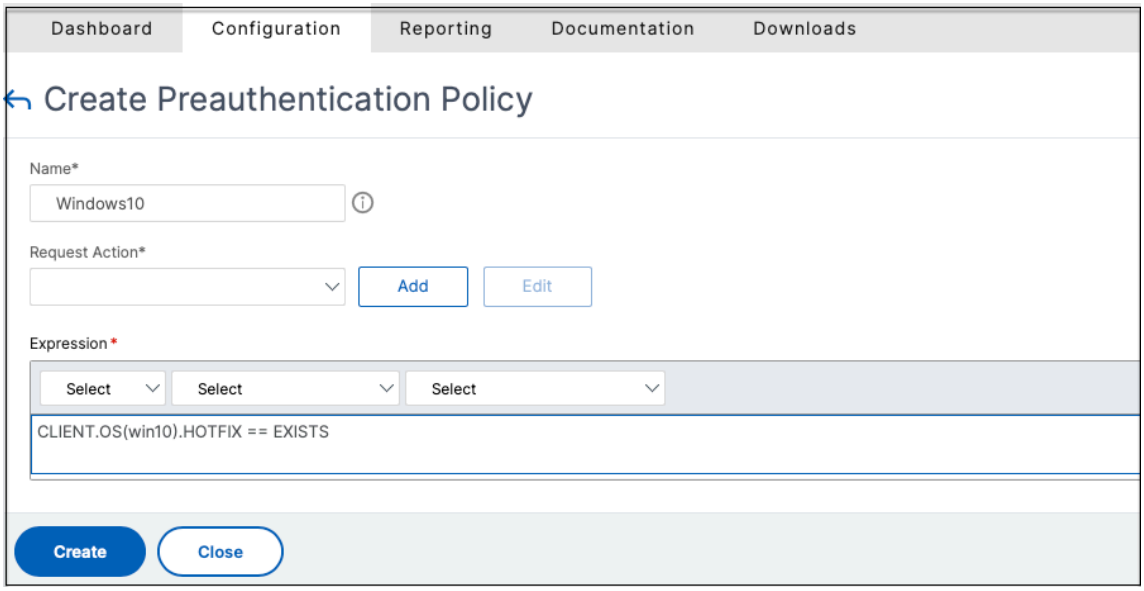
1. Konfigurieren einer klassischen Gateway-Vorauthentifizierungsrichtlinie
2. Binden Sie die klassische Vorauthentifizierungsrichtlinie an den virtuellen Gatewayserver

Konfigurieren einer klassischen Gateway-Vorauthentifizierungsrichtlinie

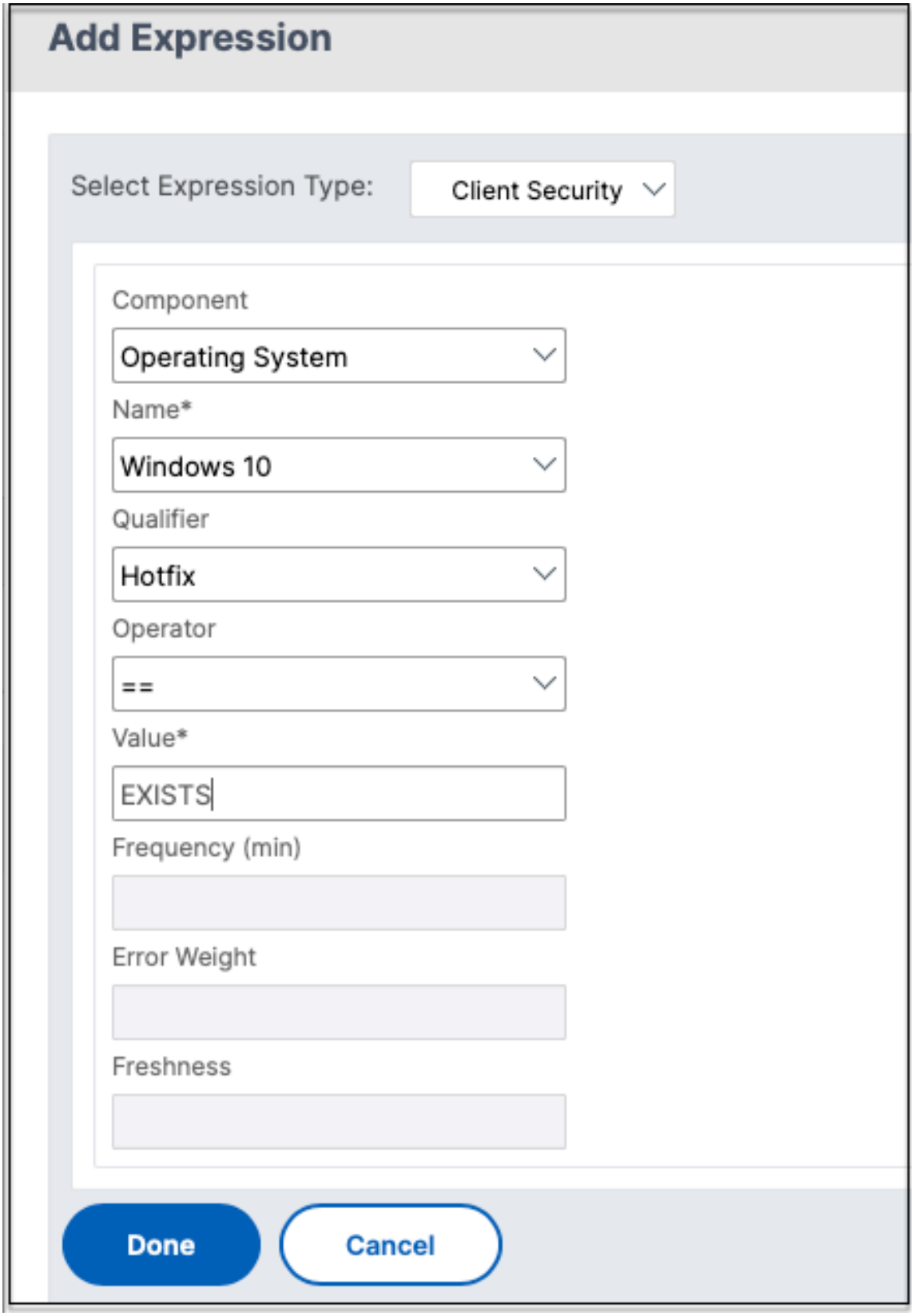
1. Navigieren Sie zu **NetScaler Gateway > Richtlinien > Vorauthentifizierung** und klicken Sie dann auf **Hinzufügen**.
2. Wählen Sie eine vorhandene Richtlinie aus oder fügen Sie einen Namen für die Richtlinie hinzu. Dieser Richtlinienname wird als benutzerdefinierter Tag-Wert verwendet.
3. Klicken Sie in **Aktion anfordern**auf **Hinzufügen** , um eine Aktion zu erstellen. Sie können diese Aktion für mehrere Richtlinien wiederverwenden; beispielsweise können Sie eine Aktion verwenden, um den Zugriff zu erlauben, und eine andere, um den Zugriff zu verweigern.



4. Geben Sie die Details in die erforderlichen Felder ein und klicken Sie auf **Erstellen**.
5. Geben Sie in **Ausdruck**den Ausdruck manuell ein oder verwenden Sie den Ausdruckseditor, um einen Ausdruck für die Richtlinie zu erstellen.



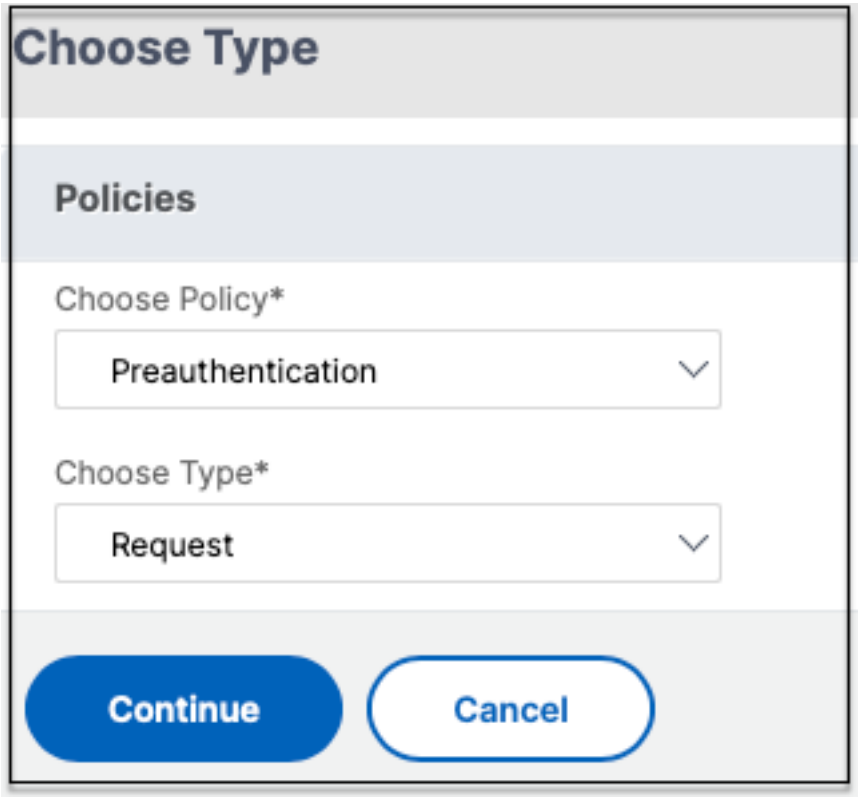
Die folgende Abbildung zeigt einen Beispielausdruck, der zum Überprüfen des Windows 10-Betriebssystems erstellt wurde.



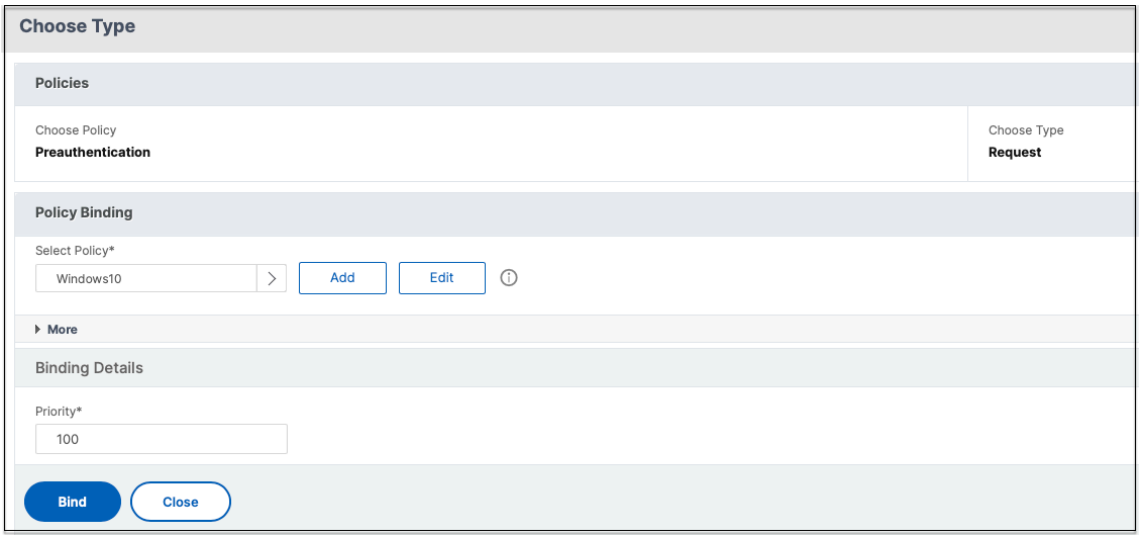
6. Klicken Sie auf **Erstellen**.

Binden Sie das benutzerdefinierte Tag an NetScaler Gateway

1. Navigieren Sie zu **NetScaler Gateway > Virtuelle Server**.
2. Wählen Sie den virtuellen Server aus, für den die Vorauthentifizierungsrichtlinie gebunden werden soll, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Richtlinien** auf **+** , um die Richtlinie zu binden.
4. Wählen Sie in **Richtlinie auswählen**die Vorauthentifizierungsrichtlinie aus und wählen Sie **Anforderung** in **Typ auswählen**aus.



5. Wählen Sie den Richtliniennamen und die Priorität für die Richtlinienauswertung aus.
6. Klicken Sie auf **Bind**.



Konfigurieren von benutzerdefinierten Tags mithilfe der CLI

Führen Sie die folgenden Beispielbefehle auf der NetScaler-CLI aus, um eine Vorauthentifizierungsrichtlinie zu erstellen und zu binden:

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10)EXISTS "win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

Führen Sie den folgenden Beispielbefehl in der NetScaler-CLI aus, um die nFactor EPA-Richtlinie zu konfigurieren:

- `add authentication epaAction epaallowact -csecexpr "sys.client_expr (\"proc_0_notepad.exe\")"-defaultEPAGroup allow_app -quarantineGroup deny_app`
- `add authentication Policy epaallow -rule true -action epaallowact`

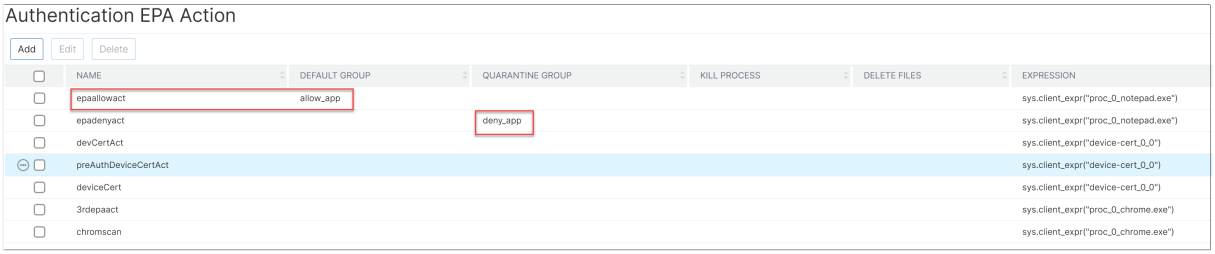
Hinzufügen eines neuen Kontexttags

1. Öffnen Sie die Secure Private Access-Administratorkonsole und klicken Sie auf **Zugriffsrichtlinien**.
2. Erstellen Sie eine neue Richtlinie oder bearbeiten Sie eine vorhandene Richtlinie.
3. Klicken Sie im Abschnitt **Bedingung** auf **Bedingung hinzufügen** und wählen Sie **Kontextbezogene Tags**, **Stimmt mit allem überein**aus und geben Sie dann den Namen des kontextbezogenen Tags ein (z. B. `Windows10`).

Hinweis zu EPA-Tags, die an das Secure Private Access-Plugin gesendet werden

Der in der nFactor EPA-Richtlinie konfigurierte EPA-Aktionsname und der zugehörige Gruppenname als Smart Access-Tags für das Secure Private Access-Plug-In. Welche Tags versendet werden, hängt jedoch vom Ergebnis der Maßnahmenbewertung der EPA ab.

- Wenn alle EPA-Aktionen in einer nFactor EPA-Richtlinie zur Aktion **DENY** führen und in der letzten Aktion eine Quarantänegruppe konfiguriert ist, wird der Name der Quarantänegruppe als Smart Access gesendet.
- Wenn eine EPA-Aktion in einer nFactor EPA-Richtlinie zur Aktion **ALLOW**führt, werden die mit der Aktion verknüpften EPA-Richtliniennamen und der Standardgruppenname (sofern konfiguriert) als Smart Access-Tags gesendet.



In diesem Beispiel wird, wenn die Aktion abgelehnt wird, *deny_app* als Smart Access-Tag an das Secure Private Access-Plug-In gesendet. Wenn die Aktion zulässig ist, werden *epaallowact* und *allow_app*als Smart Access-Tags an das Secure Private Access-Plug-In gesendet.

Referenzen

- Konfigurieren Sie Zugriffsrichtlinien für die Anwendungen.
- Unterstützung für Smart-Access-Tags.

Lizenzserver

October 21, 2024

Ein Lizenzserver für das Secure Private Access-Plug-In ist eine obligatorische Komponente, die zum Sammeln und Verarbeiten von Lizenzdaten erforderlich ist. Ein Lizenzserver kann während der Ersteinrichtung bei Secure Private Access registriert oder auch nach Abschluss der Einrichtung konfiguriert oder aktualisiert werden. Einzelheiten zum Registrieren eines Lizenzservers bei Secure Private Access finden Sie unter StoreFront- und NetScaler Gateway-Server integrieren.

Sie müssen die URL des Lizenzservers angeben, um Secure Private Access mit dem Lizenzserver zu verbinden. Das Secure Private Access-Plugin registriert sich automatisch auf dem Lizenzserver.

> **Hinweis:**
>
> - Sie müssen mindestens eine Citrix Virtual Apps and Desktops-Brokerlizenz auf dem Lizenzserver installieren, um das Secure Workspace Access-Plug-In auf dem Lizenzserver zu registrieren.
> - Der Lizenzserver für das Secure Private Access-Plug-In wird ab Version 11.17.2 Build 45000 unterstützt. Wenn Sie bereits über einen Lizenzserver verfügen, müssen Sie den Lizenzserver auf Version 11.17.2 Build 45000 oder höher aktualisieren.

Parameter des Konfigurationstools

Für den Lizenzserver stehen folgende Konfigurationstool-Parameter zur Verfügung:

- Hashing - `.\AdminConfigTool.exe LICENSE_SERVER_ENABLE_HASHING <true|false>`
- PII-Daten werden heruntergeladen - `.\AdminConfigTool.exe DOWNLOAD_PII_DATA <filename>`

Weitere Informationen zum Lizenzierungsserver finden Sie unter Lizenzierungsserver.

Citrix Secure Access-Client

October 21, 2024

Mit dem Citrix Secure Private Access-Client können Sie jetzt über einen nativen Browser oder eine native Clientanwendung über den auf Ihrem Computer ausgeführten Citrix Secure Access-Client auf alle privaten Apps zugreifen, einschließlich TCP/UDP- und HTTPS/HTTP-Apps.

Mit der zusätzlichen Unterstützung von TCP/UDP-Anwendungen innerhalb von Citrix Secure Private Access können Sie jetzt die Abhängigkeit von einer herkömmlichen VPN-Lösung beseitigen, um Remotebenutzern Zugriff auf alle privaten Apps zu gewähren.

Funktionsweise

Endbenutzer können problemlos auf alle ihre genehmigten privaten Apps zugreifen, indem sie einfach den Citrix Secure Access-Client auf ihren Clientgeräten installieren.

- Für Windows kann die Clientversion (24.6.1.17 und höher) von https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.htmlheruntergeladen werden.

- Für macOS kann die Client-Version (24.06.2 und höher) von der App heruntergeladen werden

Installieren des Citrix Secure Access-Clients auf einem Windows-Computer

Unterstützte Betriebssystemversionen:

Windows –Windows 11, Windows 10, Windows Server 2016 und Windows Server 2019.

Im Folgenden finden Sie die Schritte zur Installation des Citrix Secure Access-Clients auf einem Windows-Computer.

1. Laden Sie den Citrix Secure Access-Client von https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.htmlherunter.
2. Klicken Sie auf **Installieren** , um den Client auf Ihrem Windows-Computer zu installieren. Wenn Sie über einen vorhandenen Citrix Gateway-Client verfügen, wird dieser aktualisiert.

3. Klicken Sie auf **Fertig stellen** , um die Installation abzuschließen.

> **Hinweis:**
>
> Mehrbenutzersitzungen unter Windows werden nicht unterstützt.

Installieren des Citrix Secure Access-Clients auf einem macOS-Computer

1. Laden Sie den Citrix Secure Access-Client für macOS aus dem App Store herunter.
2. Klicken Sie auf **und öffnen Sie** , sobald der Download abgeschlossen ist.

> **Hinweis:**
>
> - Der Citrix Secure Access-Client für macOS ist ab macOS 10.15 (Catalina) verfügbar.
> - Vorschau-Builds sind in der TestFlight-App nur für macOS Monterey (12.x) verfügbar.
> - Wenn Sie zwischen der App Store-App und der TestFlight-Vorschau-App wechseln, müssen Sie das Profil, das Sie mit der Citrix Secure Access-App verwenden möchten, neu erstellen. Wenn Sie beispielsweise ein Verbindungsprofil mit `blr.abc.company.com`verwendet haben, löschen Sie das VPN-Profil und erstellen Sie dasselbe Profil erneut.

Unterstützte Betriebssystemversionen:

macOS –14.x (Sonoma), 13.x (Ventura), 12.x (Monterey)

Nicht unterstützte Features

Die folgenden Funktionen werden von der Lösung „Secure Workspace Access für vor Ort“nicht unterstützt.

- Always On vor der Windows-Anmeldung (Maschinentunnel)
- DNS-TCP

Nicht unterstützte Clientplattformen

Die folgenden Plattformen werden von der Lösung „Secure Private Access for On-Premises“nicht unterstützt.

- Linux
- iOS
- Android

Director

October 21, 2024

Die Director-Integration mit Secure Private Access ermöglicht eine effektive Leistungsüberwachung und Fehlerbehebung. Um Director in Secure Private Access zu integrieren, müssen Sie die IP-Adresse des FQDN des Director-Servers eingeben, der bei Secure Private Access registriert sein muss. Einzelheiten finden Sie unter Server integrieren.

Die Registrierung von Director bei Secure Private Access ist eine obligatorische Konfiguration für Secure Private Access für Kunden der lokalen Version 2402. Wenn Sie Director nicht konfiguriert haben, müssen Sie die neueste Version von Director, LTSR 2402 oder höher, installieren. Wenn Sie Director bereits konfiguriert haben, müssen Sie es auf die neueste Version, LTSR 2402 oder höher, aktualisieren. Die Einrichtung von Secure Private Access kann ohne die Registrierung eines Directors nicht abgeschlossen werden. Die Validierung schlägt auch in den folgenden Fällen fehl.

- Director ist nicht bei Secure Private Access registriert.
- Die von Ihnen eingegebene Director-IP-Adresse oder der FQDN existiert nicht.

Einzelheiten zum Registrieren von Director bei Secure Private Access finden Sie unter StoreFront- und NetScaler Gateway-Server integrieren und Einstellungen nach der Installation verwalten.

Hinweis:

- Ab Secure Private Access 2407 oder höher werden neben den Web-/SaaS-Apps auch die TCP/UDP-Sitzungen im Director-Dashboard angezeigt.
- Die Director-Registrierung oder -Anmeldung unterstützt die Integrierte Windows-Authentifizierung (IWA) nicht. Wenn sich der Administrator über IWA bei der Secure Private Access-Konsole angemeldet hat, wird er aufgefordert, die Anmeldeinformationen für die Director-Registrierung einzugeben.
- Wenn der Administrator sich manuell bei der Secure Private Access-Konsole angemeldet hat, werden diese Details zur Authentifizierung beim Director-Server genutzt. Wenn dies nicht gelingt, wird der Administrator aufgefordert, die Anmeldeinformationen einzugeben.
- Wenn der Administrator nach Abschluss der Einrichtung einen anderen Director hinzufügen muss, registrieren Sie den neuen Director auf der Seite **Einstellungen verwalten** . Beim Aktualisieren der Director-Details nach der Einrichtung müssen Administratoren die Anmeldeinformationen eingeben, um die Änderungen vorzunehmen. Single Sign-On wird zum Bearbeiten der Director-URL IPv6, SSLv3 nicht unterstützt.

Konfigurieren Sie Director mit Secure Private Access mithilfe des Director-Konfigurationstools

Die Konfiguration von Director mit Secure Private Access mithilfe des Konfigurationstools ist ein obligatorischer Schritt für die vollständige Integration. Einzelheiten finden Sie unter Secure Private Access-Integration mit Director.

Anzeigen von Secure Workspace Access-Benutzersitzungen in Director

Sie können die View Secure Private Access-Benutzersitzungen in Director anzeigen. Weitere Einzelheiten finden Sie unter Anzeigen einer Secure Private Access-Sitzung des Benutzers.

Web Studio

August 26, 2024

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

Um diese Integration zu aktivieren, müssen Sie Web Studio Version 2308 oder höher installieren.

Einzelheiten finden Sie unter Integration von Secure Private Access mit Web Studio.

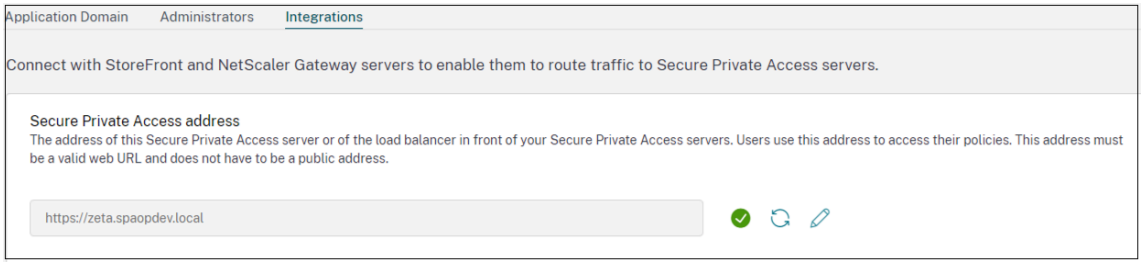
Bereitstellen von Secure Workspace Access als Cluster

October 21, 2024

Die lokale Lösung Secure Private Access kann als Cluster für hohe Verfügbarkeit, hohen Durchsatz und Skalierbarkeit bereitgestellt werden. Bei großen Bereitstellungen (z. B. über 5.000 Benutzer) können mehrere separate Secure Private Access-Knoten bereitgestellt werden, um die Arbeitslast zu verteilen und die Skalierbarkeit zu verbessern.

Erstellen Sie Secure Private Access-Knoten

- Erstellen Sie eine neue Secure Private Access-Site. Weitere Einzelheiten finden Sie unter Einrichten einer sicheren privaten Zugriffssite.
- Fügen Sie der Secure Private Access-Site die erforderliche Anzahl Clusterknoten hinzu. Weitere Einzelheiten finden Sie unter Einrichten eines sicheren privaten Zugriffs durch Beitritt zu einer vorhandenen Site.
- Konfigurieren Sie in jedem Secure Private Access-Knoten dieselben Serverzertifikate. Der allgemeine Name oder der alternative Name des Zertifikatsbetreffs muss mit dem FQDN des Load Balancers übereinstimmen.
- Verwenden Sie beim Konfigurieren des ersten Knotens in Secure Private Access die Namen der Lastenausgleichsmodule. Um die nachfolgenden Knoten hinzuzufügen, geben Sie die Datenbankadresse auf der Registerkarte „Integrationen“an und führen Sie das Datenbankskript manuell aus. Einzelheiten zum Aktualisieren der Datenbank mithilfe von Skripts finden Sie unter Aktualisieren der Datenbank mithilfe von Skripts.



Load Balancer-Konfiguration

Für die Einrichtung des Secure Private Access-Clusters gibt es keine spezifischen Konfigurationsanforderungen für den Lastausgleich. Wenn Sie NetScaler als Load Balancer verwenden, beachten Sie Folgendes:

- Die für den Zugriff auf StoreFront verwendeten FQDNs sind im DNS-Feld als Subject Alternative Name (SAN) enthalten. Wenn Sie einen Lastenausgleich verwenden, geben Sie sowohl den FQDN des einzelnen Servers als auch den FQDN des Lastenausgleichs an. Dies gilt für SSL-Zertifikate. Für Secure Private Access ist die Konfiguration eines Load Balancers ausreichend. Einzelheiten finden Sie unter Lastenausgleich mit NetScaler. Vor der Konfiguration von Secure Private Access muss der StoreFront Store konfiguriert werden. Wenn Sie einen Load Balancer verwenden, konfigurieren Sie die Basis-URL mit dem Namen des Load Balancers und verwenden Sie HTTPS für die sichere Kommunikation. Weitere Einzelheiten finden Sie unter Sichern von StoreFront mit HTTPS.
- Es wird empfohlen, Secure Private Access-Dienste als HTTPS auszuführen, dies ist jedoch keine zwingende Voraussetzung. Secure Private Access-Dienste können auch als HTTP bereitgestellt werden.
- SSL-Offload oder SSL-Bridge werden unterstützt, sodass jede beliebige Load Balancer-Konfiguration verwendet werden kann. Achten Sie bei Verwendung einer SSL-Brücke darauf, in jedem Secure Private Access-Knoten dieselben Serverzertifikate zu konfigurieren. Darüber hinaus muss der allgemeine Name oder der alternative Antragstellername (SAN) des Zertifikats mit dem FQDN des Load Balancers übereinstimmen. Außerdem muss SAN im Load Balancer-Dienst konfiguriert werden.
- Das richtige SSL-Zertifikat ist an den IIS-Server und NetScaler gebunden.
- Es werden sichere Chiffren verwendet.
- Secure Private Access-Dienste (sowohl Administrator- als auch Laufzeitdienste) sind zustandslos und daher ist keine Persistenz erforderlich.
- Load Balancer (z. B. NetScaler) verfügen standardmäßig über integrierte Monitore (Sonden) für Back-End-Server. Wenn Sie einen benutzerdefinierten HTTP-basierten Monitor (Sonde) für lokale Secure Workspace Access-Server konfigurieren müssen, kann der folgende Endpunkt verwendet werden:

  `/secureAccess/health`

  Erwartete Antwort:

  ```
  1    Http status code: 200 OK
  2
  3    Payload:
  4
  5    {
  6  "status":"OK","details":{
  7  "duration":"00:00:00.0084206","status":"OK" }
  8   }
  ```

  Einzelheiten zum Konfigurieren eines NetScaler-Load Balancers finden Sie unter Einrichten des grundlegenden Load Balancing.

Monitor für Secure Private Access erstellen

Verwenden Sie den folgenden CLI-Befehl, um einen Monitor für Secure Private Access zu erstellen.

```
add lb monitor SPAHealth HTTP -respCode 200 -httpRequest "GET /
secureAccess/health"-secure YES
```

Nachdem Sie einen Monitor erstellt haben, binden Sie das Zertifikat an den Monitor.

Einzelheiten zum Erstellen von Monitoren mit der NetScaler-Benutzeroberfläche finden Sie unter Monitore erstellen.

Konfigurieren des Secure Workspace Access-Plugins

October 21, 2024

Nachdem Sie das Citrix Secure Access-Plug-In installiert haben, können Sie die Secure Private Access-Umgebung einrichten und dann Anwendungen und Zugriffsrichtlinien für Anwendungen konfigurieren. Secure Private Access unterstützt Web-/SaaS- und TCP/UDP-Apps. Mithilfe von Zugriffsrichtlinien können Sie den Zugriff auf die Apps basierend auf Benutzern oder Benutzergruppen aktivieren oder deaktivieren. Darüber hinaus können Sie den eingeschränkten Zugriff auf die Apps (HTTP/HTTPS und TCP/UDP) ermöglichen, indem Sie die entsprechenden Sicherheitsbeschränkungen aktivieren.

- Konfigurieren von HTTP/HTTPS-Anwendungen
- Konfigurieren von TCP/UDP-Apps
- TCP/UDP konfigurieren –Server-zu-Client-Apps
- Konfigurieren Sie Zugriffsrichtlinien für die Anwendungen
- Optionen zur Zugriffsbeschränkung

Secure Private Access einrichten

August 26, 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.

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

Voraussetzungen

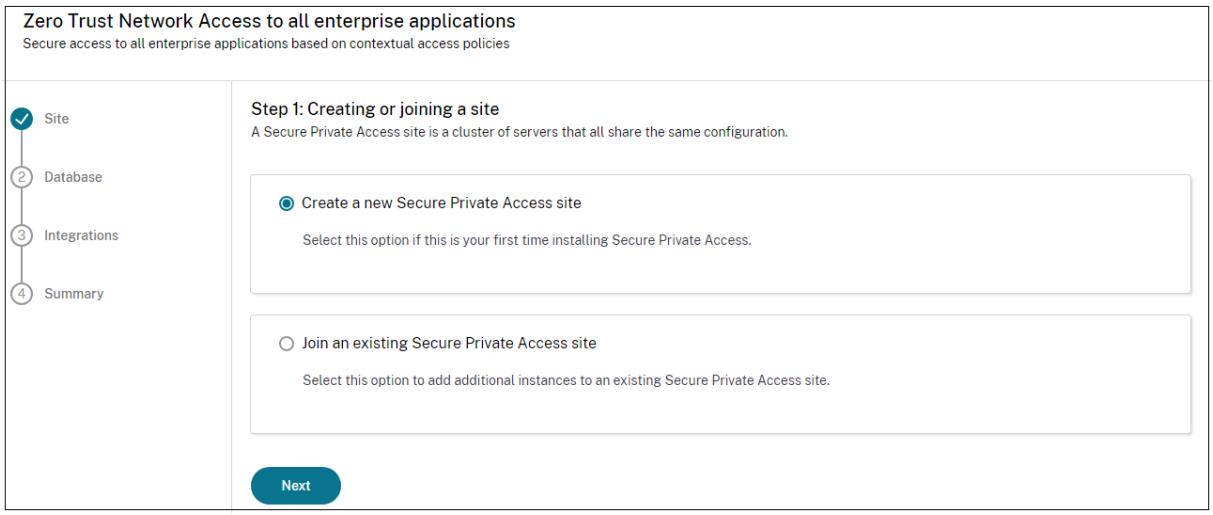
- Sie müssen sich bei der Secure Private Access-Administratorkonsole mit einem Domänenbenutzer anmelden, der auch ein lokaler Computeradministrator für den Computer ist, auf dem Secure Private Access installiert ist.
- Der SQL-Datenbankserver muss installiert werden, bevor eine Site erstellt wird.

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.

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:

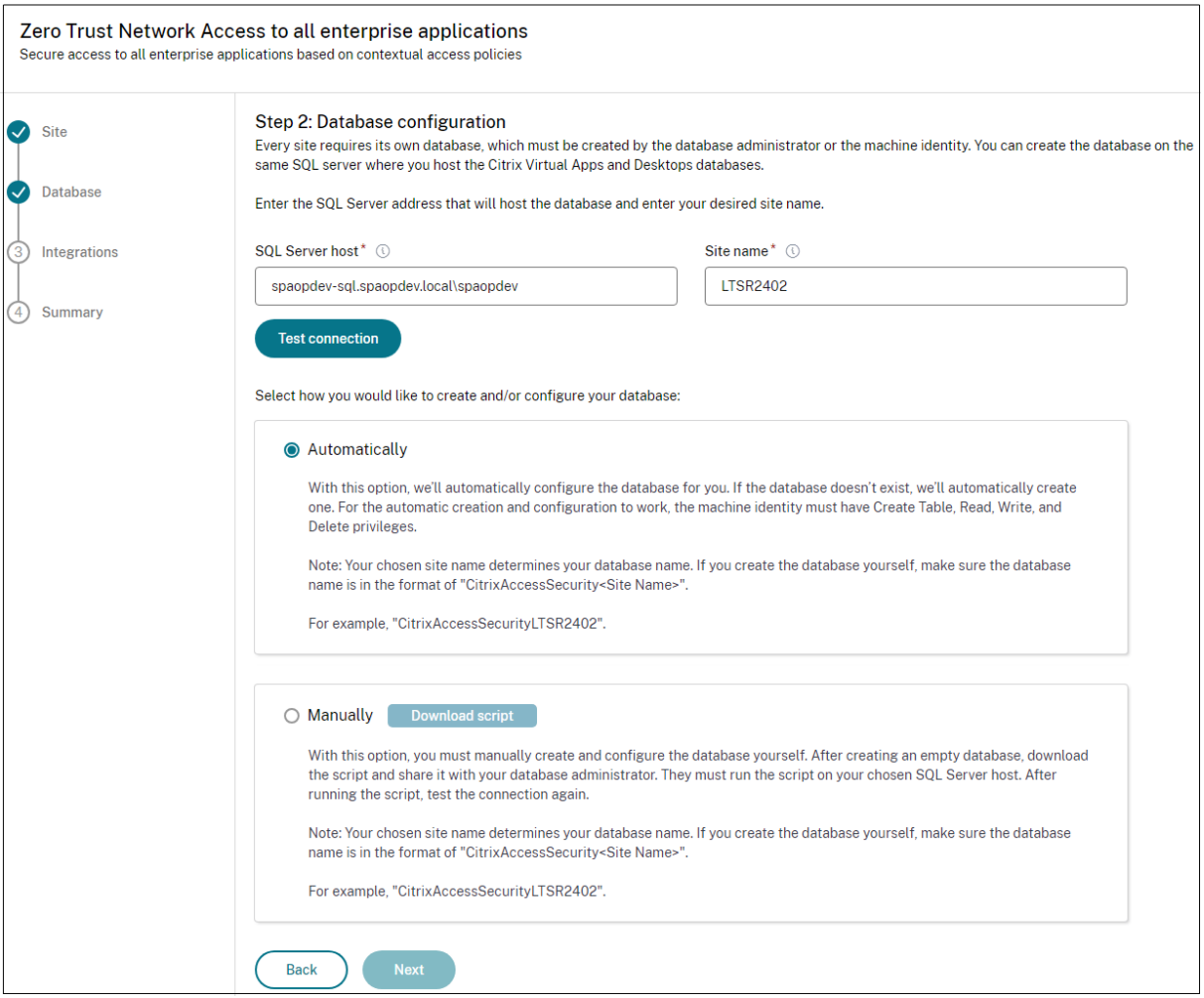
   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   Weitere Informationen finden Sie unter Datenbanken.

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

   > **Hinweis:**
   >
   > Der von Ihnen eingegebene Sitename wird an den Datenbanknamen angehängt. Das Format des Datenbanknamens ist `CitrixAccessSecurity<sitename>` und kann nicht geändert werden. Wenn Sie den Datenbanknamen anpassen müssen, wenden Sie sich an den Citrix Support.

3. Klicken Sie auf **Verbindung 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.
- 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.

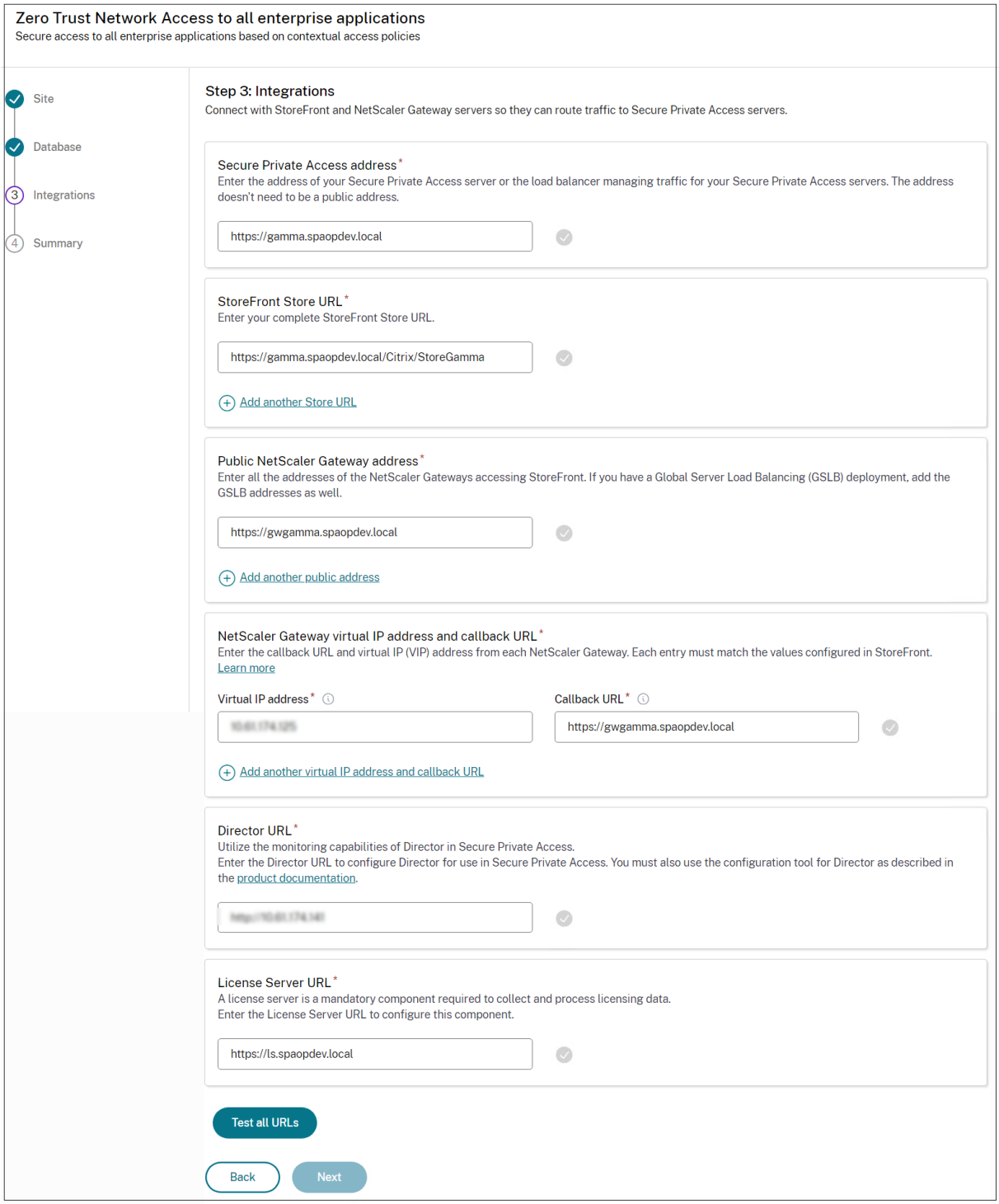
Bei der manuellen Konfiguration müssen Sie zuerst die Skripten herunterladen und dann die Skripten auf dem Datenbankserver ausführen, den Sie im Feld **SQL Server-Host** angegeben haben.

> **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: 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. Sie müssen auch den Director-Server und die Lizenzserverdetails angeben.

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`.
    - **Öffentliche NetScaler Gateway-Adresse** —URL des NetScaler Gateway. Beispiel: `https://gateway.domain.com`.
    - **Virtuelle IP-Adresse** —Diese virtuelle IP-Adresse muss mit der in StoreFront für Rückrufe konfigurierten übereinstimmen.
    - **Rückruf-URL** - Diese URL muss mit der in StoreFront konfigurierten URL übereinstimmen. Beispiel: `https://gateway.domain.com`.
    - **Director-URL:** - (Optional) Die Director-Server-IP-Adresse oder der FQDN, um Secure Private Access mit Citrix Director zu verbinden.
    - **Lizenzserver-URL:** - Die IP-Adresse des Lizenzservers zur Erfassung und Verarbeitung von Lizenzdaten.
2. Klicken Sie auf **Alle URLs überprüfen**
3. Klicken Sie auf **Weiter** und dann auf **Speichern**.

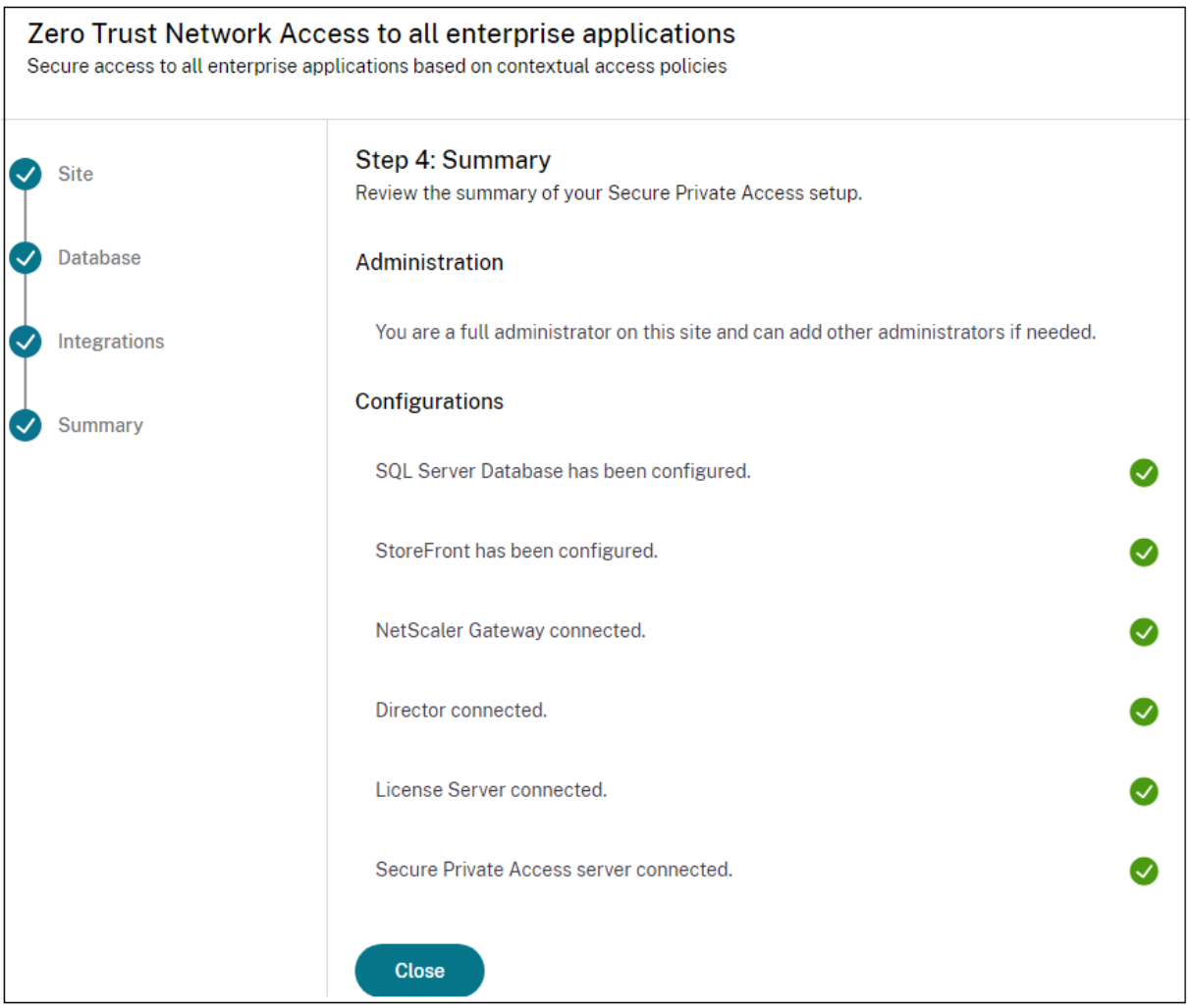


Schritt 4: Zusammenfassung der Konfiguration

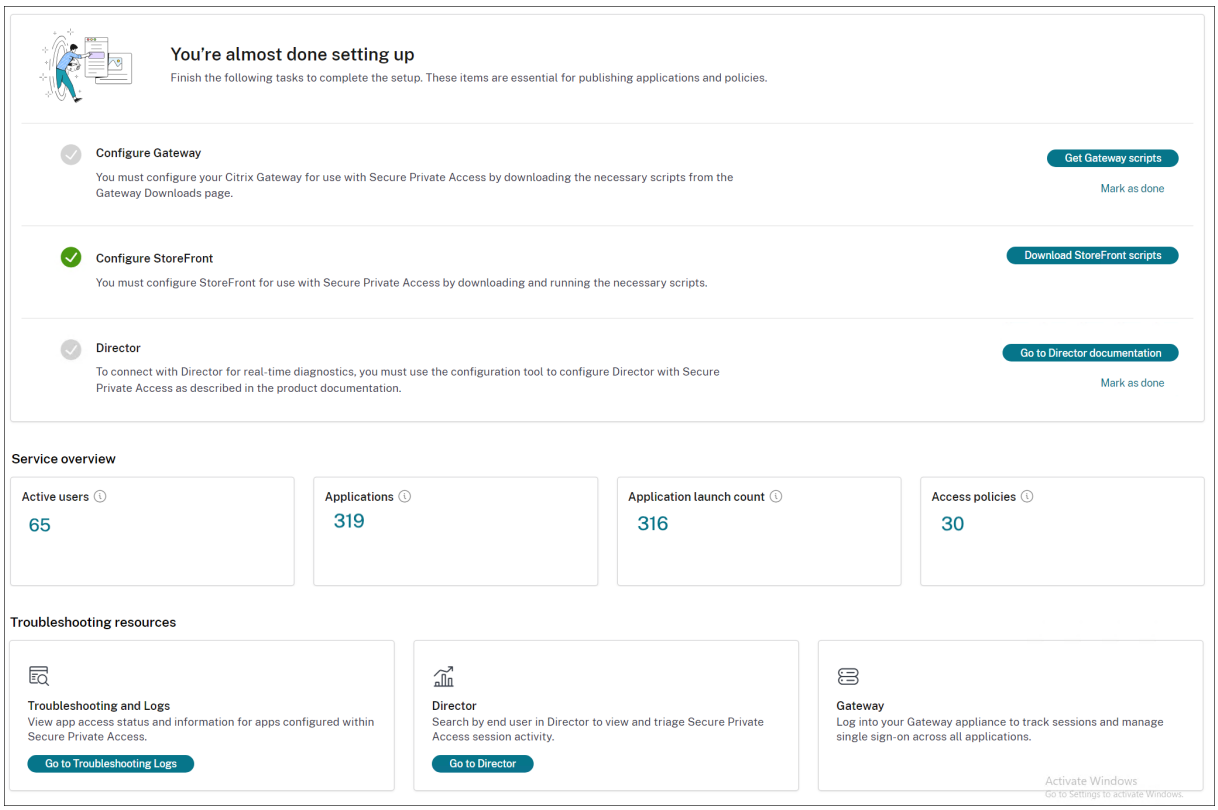
Nach Abschluss der Konfiguration erfolgt eine Überprüfung, um sicherzustellen, dass die konfigurierten Server erreichbar sind. Außerdem wird überprüft, ob der Secure Private Access-Server erreich-

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.



Nach Abschluss der Einrichtung wird die folgende Seite angezeigt, sobald Sie auf der **Übersichtsseite** auf **Schließen** klicken.



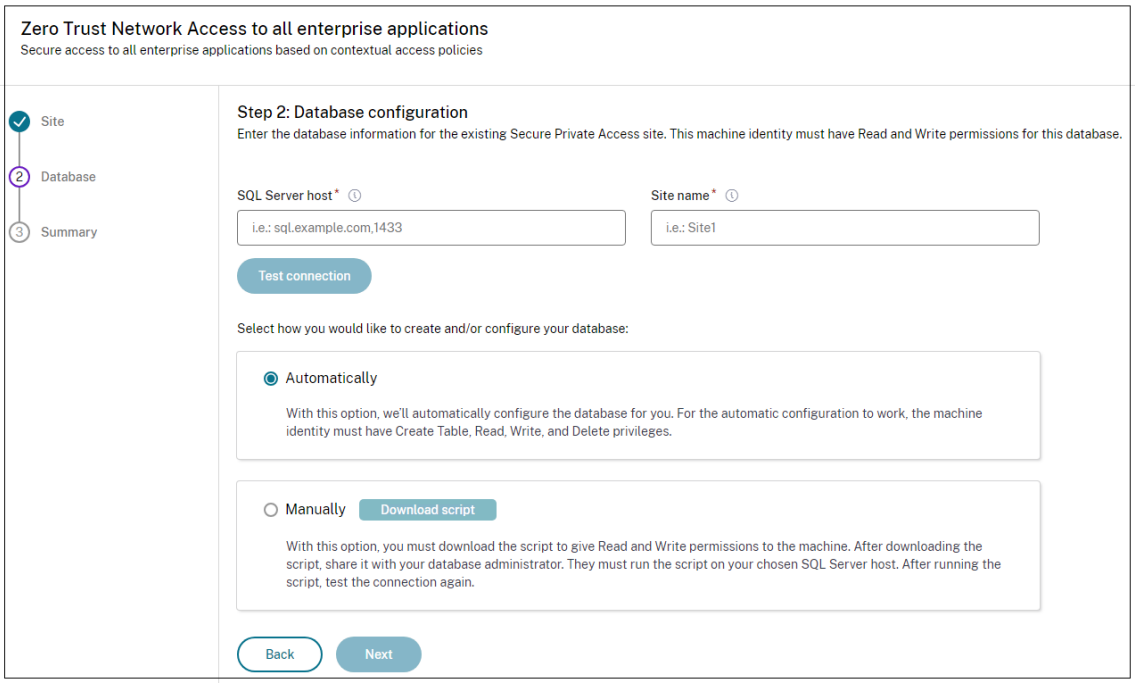
Hinweis:

- 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.

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**.



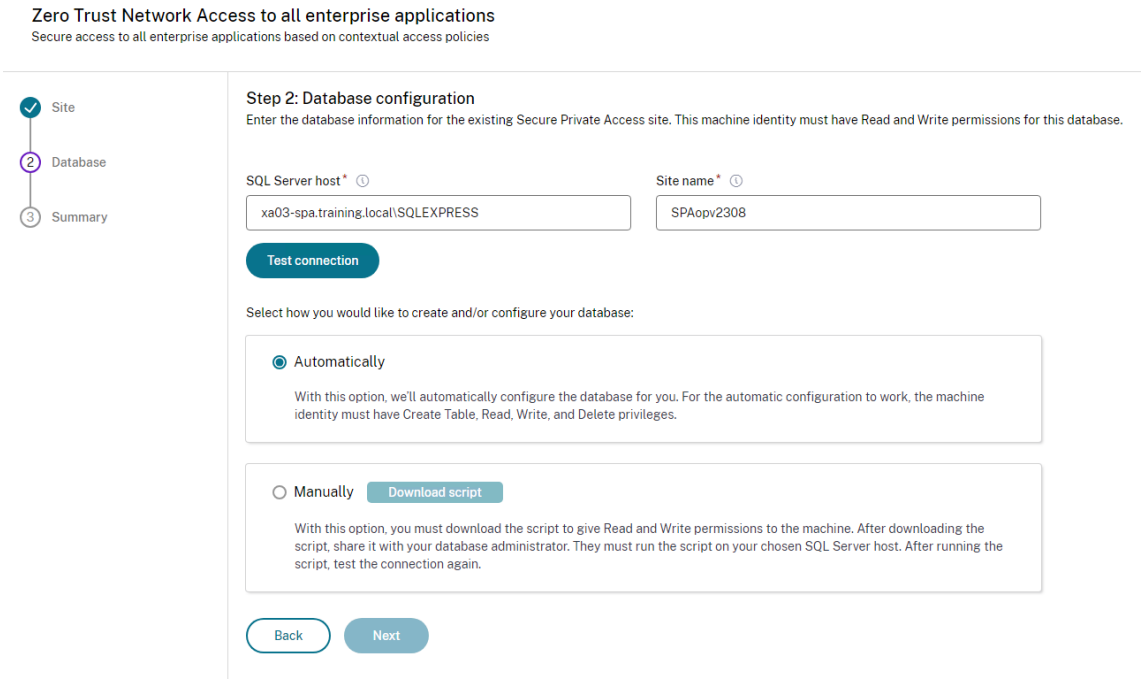
2. Geben Sie im Feld **SQL Server-Host** den Serverhostnamen ein. Stellen Sie sicher, dass eine Datenbank, die dem von Ihnen eingegebenen Site-Namen entspricht, bereits auf dem SQL-Server vorhanden ist, den Sie ausgewählt haben. Datenbankadressen können in einem der folgenden Formate angegeben werden:

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



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.

Nächste Schritte

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

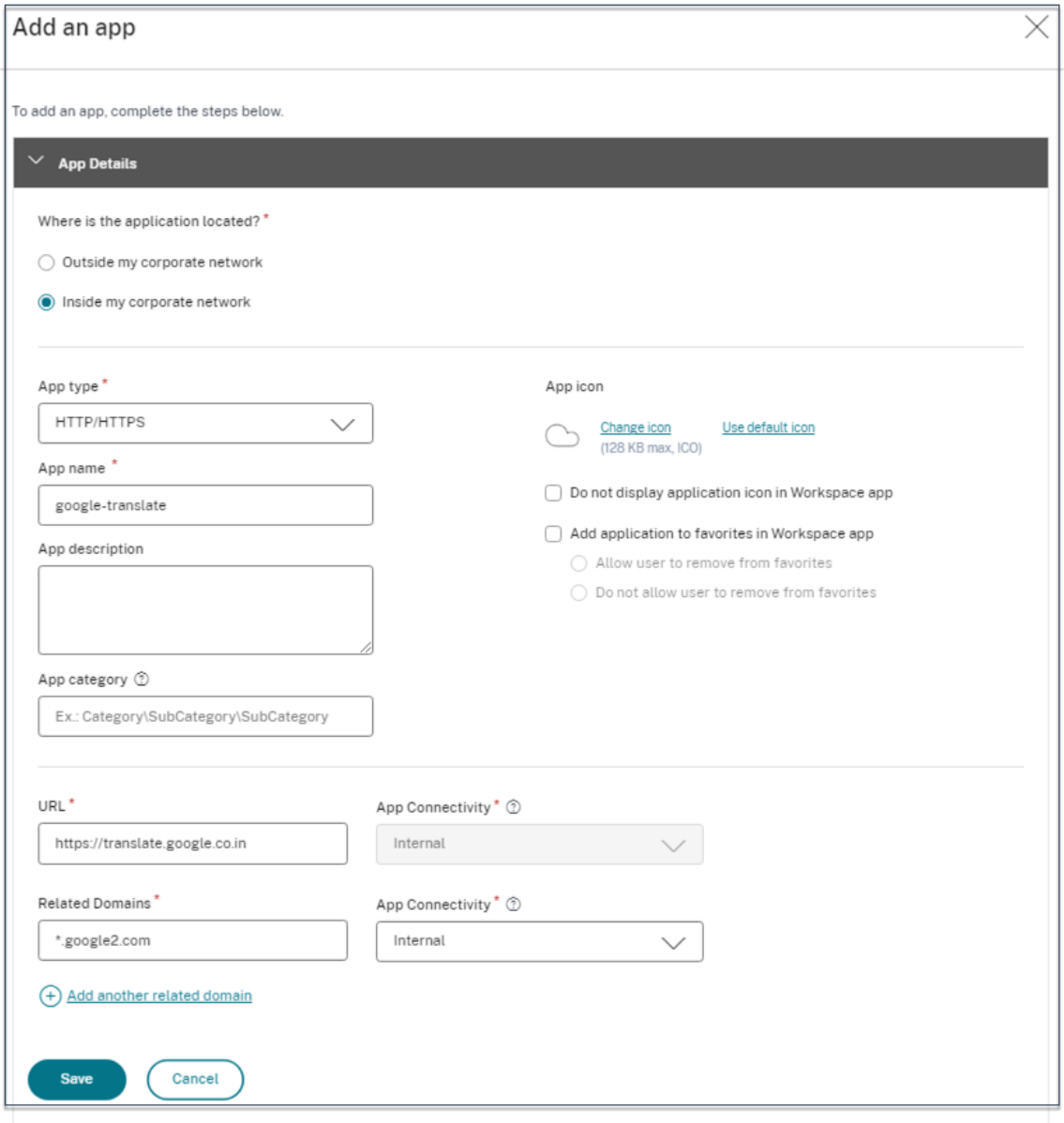
Konfigurieren von Web-/SaaS-Anwendungen

October 21, 2024

Nachdem Sie Secure Workspace Access eingerichtet haben, können Sie Apps und Zugriffsrichtlinien über die Administratorkonsole konfigurieren.

1. Klicken Sie in der Administratorkonsole auf **Anwendungen**.

2. Klicken Sie auf **App hinzufügen**.
3. Wählen Sie den Speicherort der App aus.
   - **Außerhalb meines Unternehmensnetzwerks** für externe Anwendungen.
   - **Innerhalb meines Unternehmensnetzwerks** für interne Anwendungen.
4. Geben Sie die folgenden Details im Abschnitt „App-Details“ein und klicken Sie auf **Weiter**.



   - **App-Name** –Name der Anwendung.
   - **App-Beschreibung** –Eine kurze Beschreibung der App. Diese Beschreibung wird Ihren Benutzern im Arbeitsbereich angezeigt. Sie können für die Anwendungen auch Schlüsselwörter im Format `SCHLÜSSELWÖRTER: <keyword_name>`eingeben. Mithilfe der

Schlagworte können Sie die Bewerbungen filtern. Weitere Einzelheiten finden Sie unter Filtern von Ressourcen nach enthaltenen Schlüsselwörtern.

- **App-Kategorie** –Fügen Sie die Kategorie und den Unterkategorienamen (falls zutreffend) hinzu, unter dem die von Ihnen veröffentlichte App in der Citrix Workspace-Benutzeroberfläche angezeigt werden muss. Sie können für jede App eine neue Kategorie hinzufügen oder vorhandene Kategorien aus der Citrix Workspace-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angeben, wird die App in der Workspace-Benutzeroberfläche unter der jeweiligen Kategorie angezeigt.
  - Die Kategorie/Unterkategorie kann vom Administrator konfiguriert werden und Administratoren können für jede App eine neue Kategorie hinzufügen.
  - Die Kategorie-/Unterkategorienamen müssen durch einen Backslash getrennt sein. Beispielsweise „Geschäft und Produktivität\Engineering“. Außerdem muss in diesem Feld die Groß- und Kleinschreibung beachtet werden. Administratoren müssen sicherstellen, dass sie die richtige Kategorie definieren. Wenn der Name in der Citrix Workspace-Benutzeroberfläche nicht mit dem im Feld „App-Kategorie“eingegebenen Kategorienamen übereinstimmt, wird die Kategorie als neue Kategorie aufgeführt.

    Wenn Sie beispielsweise die Kategorie „Business und Produktivität“im Feld „App-Kategorie“fälschlicherweise als „Business und Produktivität“eingeben, wird in der Citrix Workspace-Benutzeroberfläche zusätzlich zur Kategorie „Business und Produktivität“eine neue Kategorie mit dem Namen „Business und Produktivität “aufgeführt.
- **App-Symbol** –Klicken Sie auf **Symbol ändern** , um das App-Symbol zu ändern. Die Symboldateigröße muss 128 x 128 Pixel betragen und es wird nur das Ico-Format unterstützt. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.
- **Anwendung den Benutzern nicht anzeigen** –Wählen Sie diese Option, wenn Sie den Benutzern die App nicht anzeigen möchten.
- **URL** –URL der Anwendung.
- **Zugehörige Domänen** –Die zugehörige Domäne wird automatisch anhand der Anwendungs-URL ausgefüllt. Administratoren können weitere verwandte interne oder externe Domänen hinzufügen.

  > **Hinweis:**
  >
  > –Stellen Sie sicher, dass sich die zugehörige Domäne einer App nicht mit der zugehörigen Domäne einer anderen App überschneidet. If this occurs, remove the related domain from all apps and create a new app with this domain and then set access accordingly in the access policy. You can also consider if you want to display this app

> in StoreFront or hide it. You can hide the app in StoreFront using the option **Do not display application to users** while publishing the app.
>
> –Ebenso darf die URL einer veröffentlichten App nicht als zugehörige Domäne einer anderen App hinzugefügt werden.
>
> –Weitere Einzelheiten finden Sie unter Best Practices für Web- und SaaS-Anwendungskonfigurationen.

- **Anwendung automatisch zu Favoriten hinzufügen** –Klicken Sie auf diese Option, um die App als Favoriten-App in der Citrix Workspace-App hinzuzufügen. Wenn Sie diese Option auswählen, wird in der oberen linken Ecke der App in der Citrix Workspace-App ein Sternsymbol mit einem Vorhängeschloss angezeigt.
  - **Benutzer das Entfernen aus Favoriten erlauben** –Klicken Sie auf diese Option, um App-Abonnenten das Entfernen der App aus der Liste der Favoriten-Apps in der Citrix Workspace-App zu erlauben. Wenn Sie diese Option auswählen, wird in der oberen linken Ecke der App in der Citrix Workspace-App ein gelbes Sternsymbol angezeigt.
  - **Benutzer darf die App nicht aus den Favoriten entfernen** –Klicken Sie auf diese Option, um zu verhindern, dass Abonnenten die App aus der Liste der Favoriten-Apps in der Citrix Workspace-App entfernen.

  Wenn Sie die als Favoriten markierten Apps aus der Secure Workspace 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 Workspace Access-Konsole entfernt werden.
- **App-Konnektivität** - Wählen Sie **Intern** für Web-Apps und **Extern** für SaaS-Apps.

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

Sie können alle Anwendungsdomänen anzeigen, die in **Einstellungen > Anwendungsdomäne**konfiguriert sind. Weitere Einzelheiten finden Sie unter Einstellungen nach der Installation verwalten.

Nächste Schritte

Konfigurieren Sie Zugriffsrichtlinien für die Anwendungen

Konfigurieren von TCP/UDP-Apps

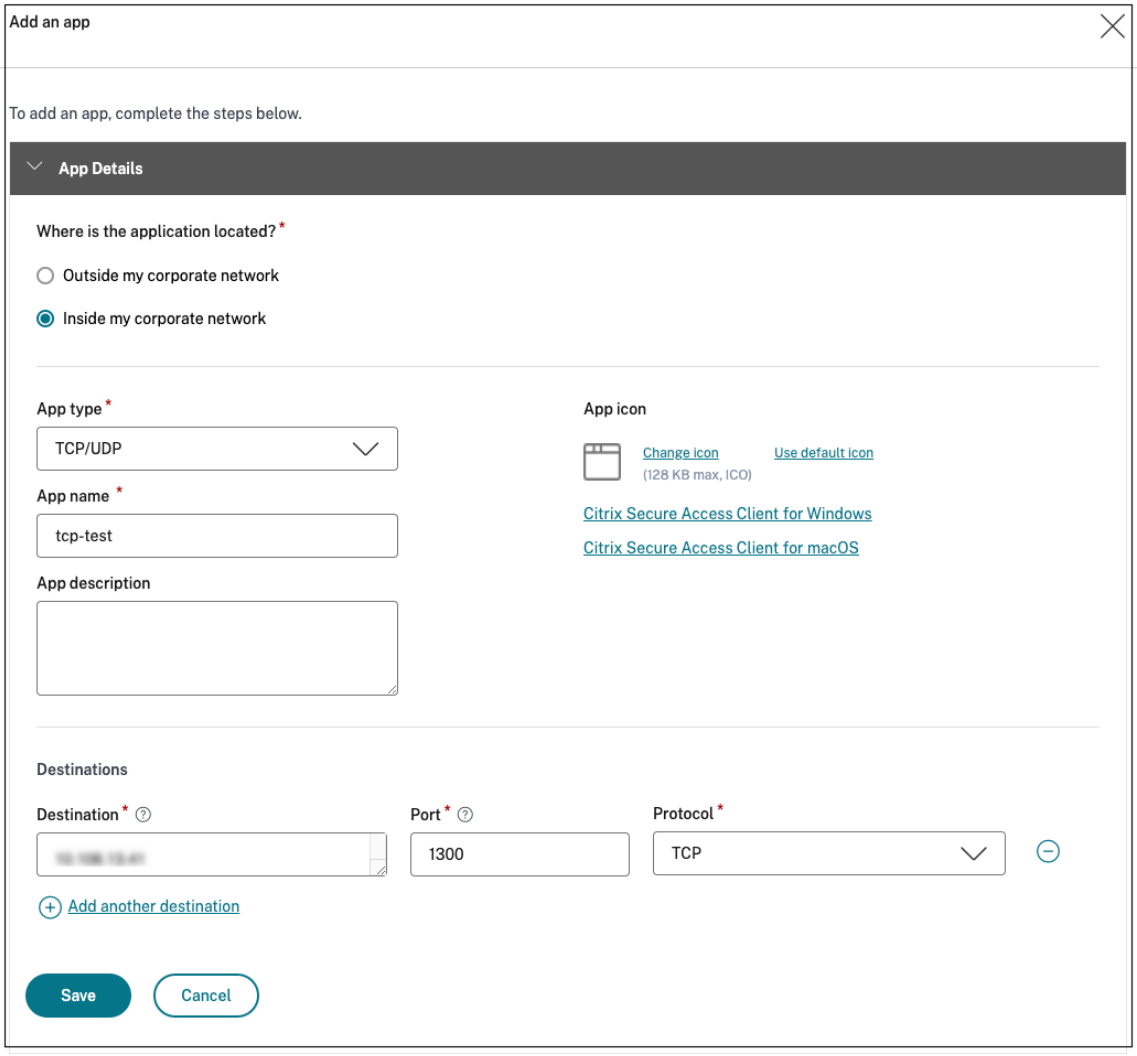
October 21, 2024

Voraussetzungen:

- Die Einrichtung von Secure Private Access ist abgeschlossen.
- Clientversionen erfüllen die folgenden Anforderungen:
  - Windows –24.6.1.17 und höher
  - macOS –24.06.2 und höher

Führen Sie die folgenden Schritte aus, um TCP/UDP-Apps von der Administratorkonsole aus zu konfigurieren:

1. Klicken Sie in der Administratorkonsole auf **Anwendungen** und dann auf **App hinzufügen**.
2. Wählen Sie den Standort **Innerhalb meines Unternehmensnetzwerks**aus.



3. Geben Sie folgende Details ein:
   - **App-Typ** –Wählen Sie **TCP/UDP** zum Herstellen von Verbindungen mit den Back-End-Servern im Rechenzentrum.

> **Hinweis:**
>
> Die TCP/UDP-Option wird ausgegraut angezeigt, wenn das Feature-Flag SPAOP-3315-EnableZTNAApplications deaktiviert ist. Sie müssen die Datenbank manuell aktualisieren, um dieses Feature-Flag zu aktivieren.

```
1  -  **App-Name** – Name der Anwendung.
2  -  **App-Beschreibung** – Beschreibung der App, die Sie hinzufügen.
   Das Feld ist optional.
3  -  **Ziele** – IP-Adressen oder FQDNs der Back-End-Maschinen im
   Rechenzentrum. Wie folgt können ein oder mehrere Ziele angegeben
   werden.
4     -  **IP-Adresse v4**
5     -  **IP-Adressbereich** – Beispiel: 10.68.90.10-10.68.90.99
6     -  **CIDR** – Beispiel: 10.106.90.0/24
7     -  **FQDN der Maschinen oder Domänenname** – Einzelne oder
         Platzhalterdomäne. Beispiel: ex.ziel.domain.com, *.domain.com >
         **Hinweis:** > > -  Endbenutzer können per FQDN auf die Apps
         zugreifen, auch wenn der Administrator die Apps mit der IP-
         Adresse konfiguriert hat. Dies ist möglich, weil der Citrix
         Secure Access-Client einen FQDN in die echte IP-Adresse auflösen
          kann.
8
9     In der folgenden Tabelle finden Sie Beispiele für verschiedene
         Ziele und wie Sie über diese Ziele auf die Apps zugreifen können
         :
10
11    | Zieleingabe             | So greifen Sie auf die App zu

         |
12    | ----------------------- |
         ------------------------------------------------------------------------
          |
13    | 10.10.10.1-10.10.10.100 | Es wird erwartet, dass der Endbenutzer
         nur über IP-Adressen in diesem Bereich auf die App zugreift.

         |
14    | 10.10.10.0/24           | Vom Endbenutzer wird erwartet, dass er
         auf die App nur über im IP CIDR konfigurierte IP-Adressen
         zugreift.

         |
15    | 10.10.10.101            | Der Endbenutzer kann die App
         voraussichtlich nur über 10.10.10.101 aufrufen.

         |
16    | `*.info.citrix.com`     | Vom Endbenutzer wird erwartet, dass er
         auf die Subdomänen `info.citrix.com` und auch `info.citrix.com`
         \(die übergeordnete Domäne) zugreift. Zum Beispiel `info.citrix.
         com, sub1.info.citrix.com, level1.sub1.info.citrix.com` \*\*
         Hinweis:\*\* Das Platzhalterzeichen muss immer das Startzeichen
         der Domäne und darf nur ein \* sein. ist erlaubt. |
```



```
17      | info.citrix.com          | Vom Endbenutzer wird erwartet, dass er
           nur auf `info.citrix.com` und keine Subdomänen zugreift.
           Beispielsweise ist `sub1.info.citrix.com` nicht zugänglich.

           |
18
19      Die Ziel-IP-Adresse muss für alle Ressourcenstandorte eindeutig
           sein. Wenn eine widersprüchliche Konfiguration vorliegt, wird
           neben der jeweiligen IP-Adresse in der Anwendungsdomänentabelle
           ein Warnsymbol angezeigt (**Einstellungen > Anwendungsdomäne**).
20
21      ![Konflikt](/en-us/citrix-secure-private-access/media/spaop-warning
           -conflict-config.png)
22
23  -         **Port** – The destination port on which the app is running.
          Admins can configure multiple ports or port ranges per
       destination.
24
25            The following table provides examples of ports that can be
                 configured for a destination.
26
27            |Port input|Description|
28            |---|---|
29            |\*|By default, the port field is set to `“*”` \(any port).
                    The port numbers from 1 to 65535 are supported for the
                 destination.|
30            |1300 – 2400|The port numbers from 1300 to 2400 are supported
                 for the destination.|
31            |38389|Only the port number 38389 is supported for the
                 destination.|
32            |22,345,5678|The ports 22, 345, 5678 are supported for the
                 destination.|
33            |1300 – 2400, 42000-43000,22,443|The port number range from
                 1300 to 2400, 42000 – 43000, and ports 22 and 443 are
                 supported for the destination.|
34
35          >**Hinweis:**
36          >
37          >Der Platzhalterport (*) kann nicht gleichzeitig mit
               Portnummern oder -bereichen verwendet werden.
38
39  -         **Protocol** – TCP/UDP
```

1. Klicken Sie auf **Hinzufügen** , um entsprechend weitere Ziele oder Server hinzuzufügen.
2. Klicken Sie auf **Speichern**. Die App wird der Seite **App-Konfiguration** hinzugefügt. Sie können eine App auf der Seite **Anwendungen** bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie hierzu auf die Auslassungspunkte-Schaltfläche neben der App und wählen Sie die entsprechenden Aktionen aus.

   - **Anwendung bearbeiten**
   - **Löschen**

Konfigurieren von Zugriffsrichtlinien für TCP/UDP-Apps

Um den Benutzern den Zugriff auf die Apps zu ermöglichen, müssen Administratoren Zugriffsrichtlinien erstellen. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.

Referenzen

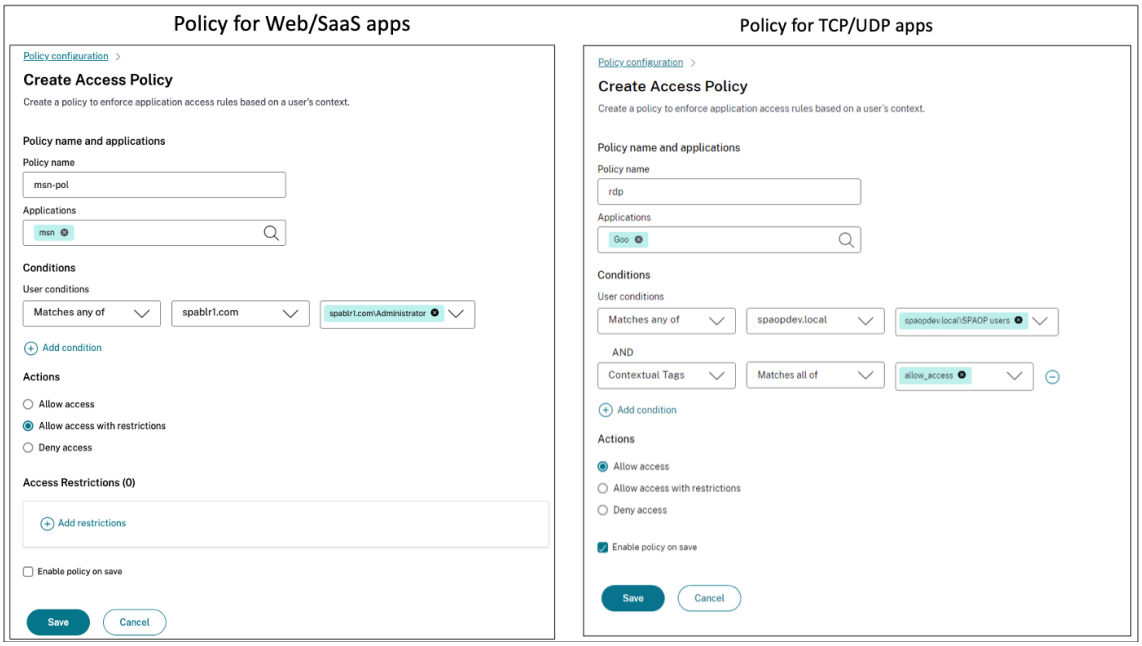
Citrix Secure Access-Client.

Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen

August 26, 2024

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 (HTTP/HTTPS und TCP/UDP) aktivieren, indem Sie die Sicherheitseinschränkungen hinzufügen.

1. Klicken Sie in der Admin-Konsole auf **Zugriffsrichtlinien**.
2. Klicken Sie auf **Richtlinie erstellen**.



3. a) Geben Sie im Feld **Richtlinienname**einen Namen für die Richtlinie ein.
4. Wählen Sie unter **Anwendungen**die Apps aus, für die Sie die Zugriffsrichtlinien durchsetzen möchten.

5. Unter **Benutzerbedingungen**: Wählen Sie die Bedingungen und Benutzer oder Benutzergruppen aus, auf deren Grundlage der App-Zugriff erlaubt oder verweigert werden muss.

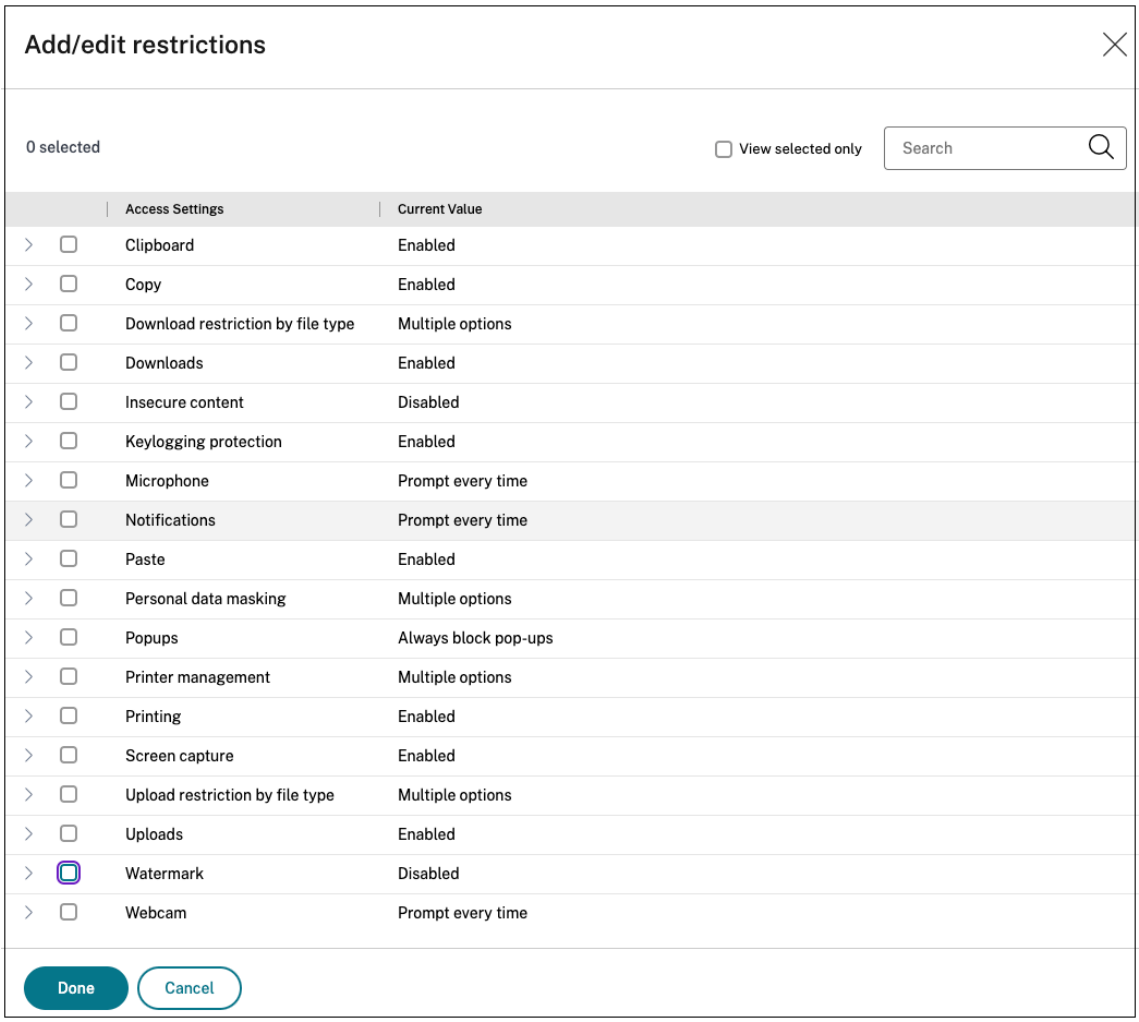
    - **Entspricht einem von**: Nur die Benutzer oder Gruppen, die einem der im Feld aufgeführten Namen entsprechen, dürfen darauf zugreifen.
    - **Stimmt mit keinem überein**: Allen Benutzern oder Gruppen außer den im Feld aufgeführten Benutzern oder Gruppen wird der Zugriff gewährt.

6. Klicken Sie auf **Bedingung hinzufügen**, um eine weitere Bedingung hinzuzufügen, die auf kontextuellen Tags basiert. Diese Tags werden vom NetScaler Gateway abgeleitet.

7. Wählen Sie unter **Aktionen** eine der folgenden Aktionen aus, die auf der Grundlage der Zustandsbewertung in der App durchgesetzt werden müssen.

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

    > **Hinweis:**
    >
    > - Die Aktion **Zugriff mit Einschränkungen zulassen** gilt nicht für die TCP/UDP-Apps.
    > - Wenn Sie **Zugriff mit Einschränkungen zulassen** auswählen, müssen Sie auf **Einschränkungen hinzufügen** klicken, um die Einschränkungen auszuwählen. Weitere Informationen zu den einzelnen Einschränkungen finden Sie unter Verfügbare Zugriffsbeschränkungen.



8. Wählen Sie die Einschränkungen aus und klicken Sie dann auf **Fertig**.
9. 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

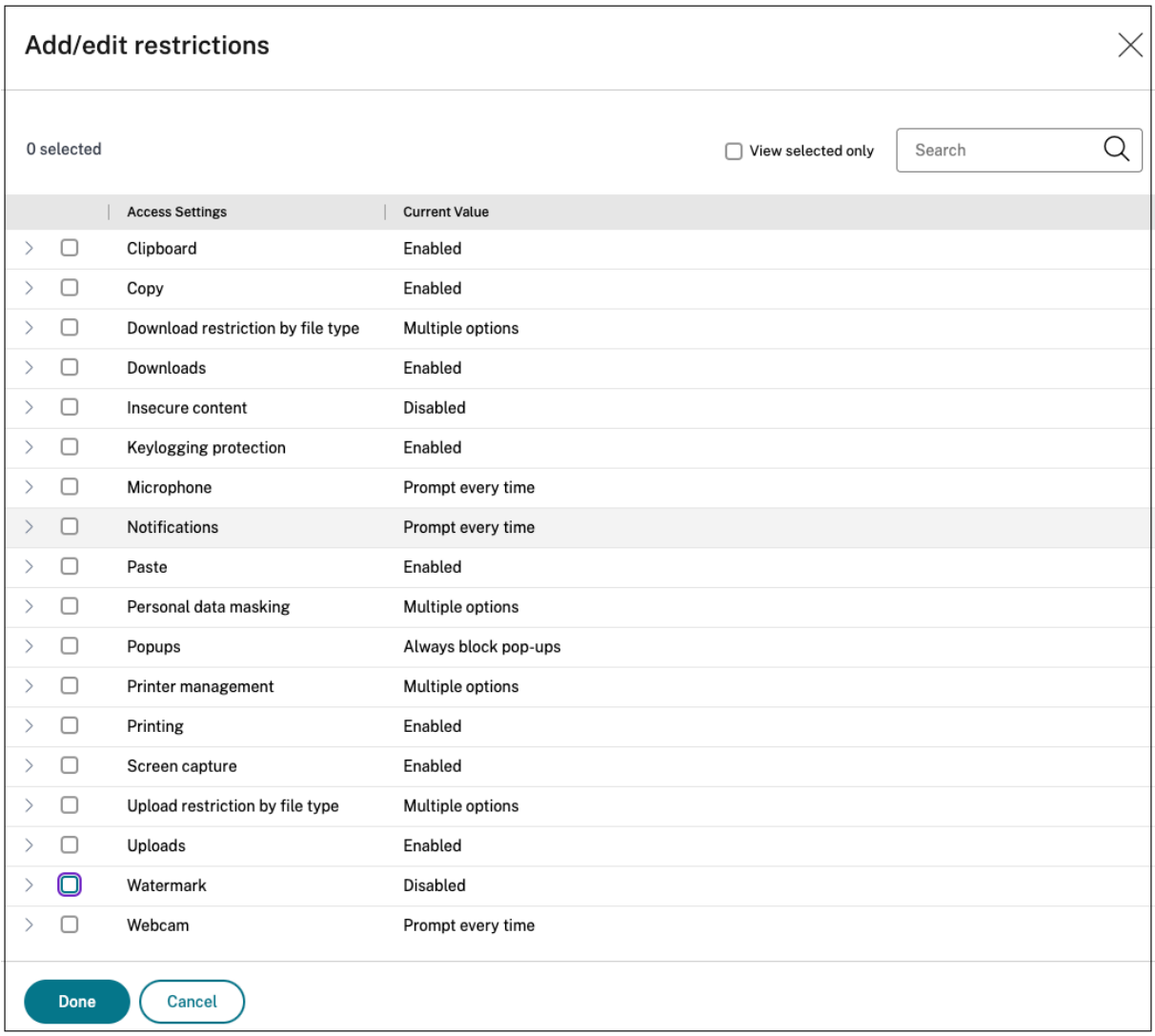
- Überprüfen Sie Ihre Konfiguration auf den Client-Computern (Windows und macOS).
- Überprüfen Sie für die TCP/UDP-Apps Ihre Konfiguration von den Client-Computern (Windows und macOS) aus, indem Sie sich beim Citrix Secure Access Client anmelden.

Validierung der Beispielkonfiguration

Optionen zur Zugriffsbeschränkung

October 21, 2024

Wenn Sie die Aktion **Zugriff mit Einschränkungen zulassen**auswählen, können Sie die Sicherheitsbeschränkungen je nach Bedarf auswählen. Diese Sicherheitsbeschränkungen sind im System vordefiniert. Administratoren können keine anderen Kombinationen ändern oder hinzufügen.



Zwischenablage

Aktivieren/deaktivieren Sie Ausschneide-/Kopieren-/Einfügevorgänge für eine SaaS- oder interne Web-App mit dieser Zugriffsrichtlinie, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

Kopieren

Aktivieren/deaktivieren Sie das Kopieren von Daten aus einer SaaS- oder internen Web-App mit dieser Zugriffsrichtlinie, wenn der Zugriff über den Citrix Enterprise-Browser erfolgt. Standardwert: Aktiviert.

Hinweis:

- Wenn in einer Richtlinie sowohl die Einschränkung **Zwischenablage** als auch **Kopieren** aktiviert sind, hat die Einschränkung **Zwischenablage** Vorrang vor der Einschränkung **Kopieren** .
- Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.
- Zur detaillierten Kontrolle von Kopiervorgängen innerhalb der Apps können Administratoren die Einschränkung **Sicherheitsgruppen** verwenden. Einzelheiten finden Sie unter Zwischenablageeinschränkung für Sicherheitsgruppen.

Downloads

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Möglichkeit des Benutzers, Downloads aus der SaaS- oder internen Web-App heraus durchzuführen, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

Hinweis:

- Wenn Sie die Einschränkung **Download** für den Endbenutzer deaktiviert haben, können die Endbenutzer beim Zugriff über den Citrix Enterprise Browser innerhalb der App Download-Zugriff anfordern. Einzelheiten finden Sie unter Download-Zugriff auf Anfrage.
- Wenn in einer Richtlinie sowohl die Beschränkungen **Downloads** als auch **Downloadbeschränkung nach Dateityp** aktiviert sind, hat die Beschränkung **Downloads** Vorrang vor der Beschränkung **Downloadbeschränkung nach Dateityp**.

Downloadbeschränkung nach Dateityp

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Möglichkeit des Benutzers, bestimmte MIME-Typen (Dateien) aus der SaaS- oder internen Web-App herunterzuladen, wenn der Zugriff über den Citrix Enterprise Browser erfolgt.

Hinweis:

- Die Download-Beschränkung **nach Dateityp** ist zusätzlich zur Download-Beschränkung ** verfügbar.
- Wenn in einer Richtlinie sowohl die Einschränkung **Downloads** als auch die Einschränkung **Downloadbeschränkung nach Dateityp** aktiviert sind, hat die Einschränkung **Downloads** Vorrang vor der Einschränkung **Downloadbeschränkung nach Dateityp** .

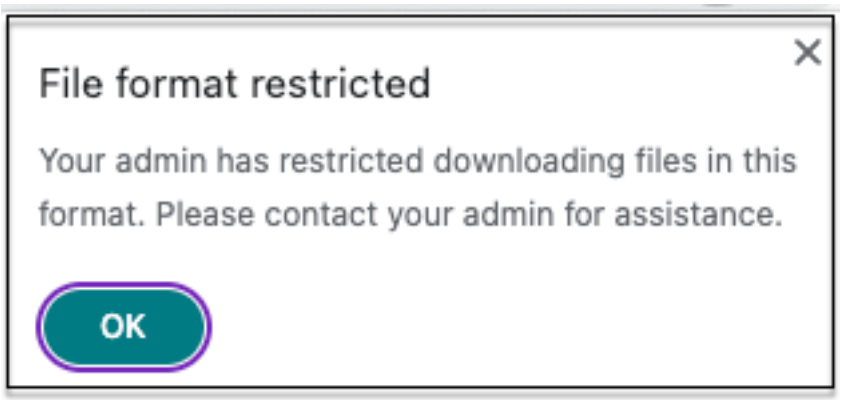
> - Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.

Um das Herunterladen von MIME-Typen zu aktivieren, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten zum Erstellen einer Zugriffsrichtlinie finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Downloadbeschränkung nach Dateityp** und dann auf **Bearbeiten**.
4. Wählen Sie auf der Seite „Downloadbeschränkung nach Dateitypeinstellungen“ eine der folgenden Optionen aus:
   - **Alle Downloads mit Ausnahmen zulassen** –Wählen Sie die Typen aus, die blockiert werden müssen, und lassen Sie alle anderen Typen zu.
   - **Alle Downloads mit Ausnahmen blockieren.** –Nur die Typen auswählen, die hochgeladen werden können, und alle anderen Typen blockieren.
5. Wenn der Dateityp nicht in der Liste vorhanden ist, gehen Sie wie folgt vor:
   a) Klicken Sie auf **Benutzerdefinierte MIME-Typen hinzufügen**.
   b) Geben Sie in **MIME-Typen hinzufügen**den MIME-Typ im Format `Kategorie/Unterkategorie<extension>`ein. Beispiel: `image/png`.
   c) Klicken Sie auf **Fertig**.

   Der MIME-Typ wird jetzt in der Liste der Ausnahmen angezeigt.

Wenn ein Endbenutzer versucht, einen eingeschränkten Dateityp herunterzuladen, zeigt Citrix Enterprise Browser die folgende Warnmeldung an:



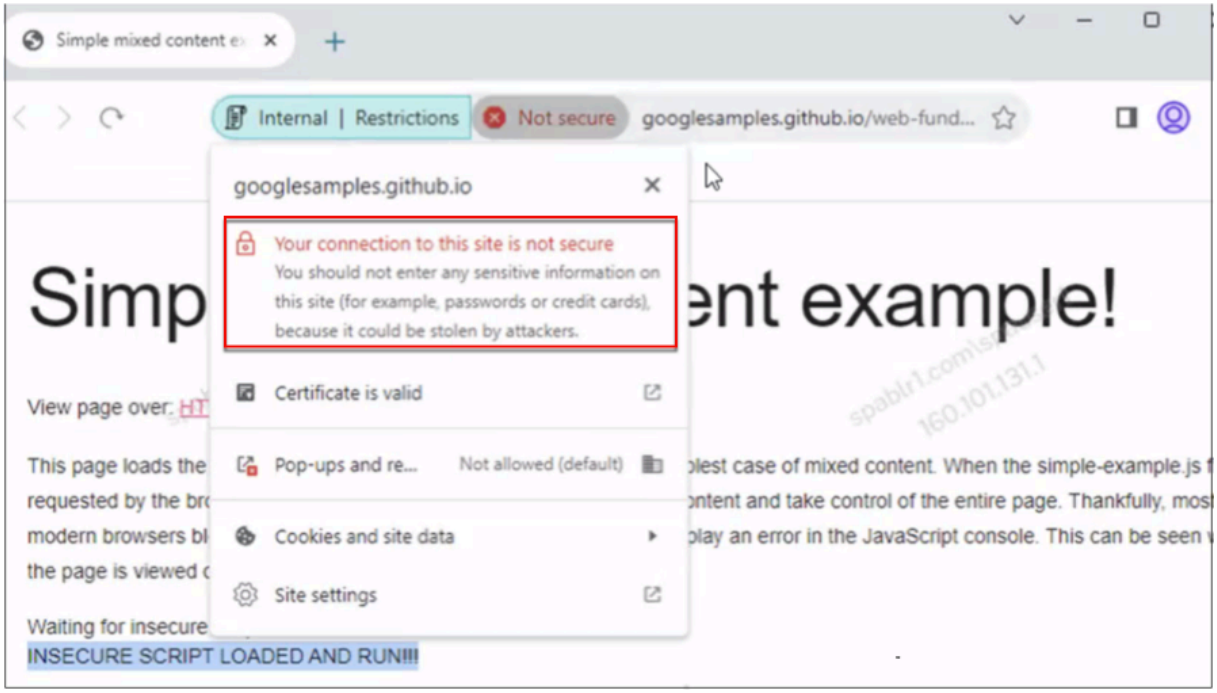
Unsicherer Inhalt

Aktivieren/deaktivieren Sie den Zugriff von Endbenutzern auf unsichere Inhalte innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Als unsicherer Inhalt gelten alle Dateien, auf die von einer Webseite aus über einen HTTP-Link und nicht über einen HTTPS-Link verwiesen wird. Standardwert: Deaktiviert.

Um die Anzeige unsicherer Inhalte zu ermöglichen, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten zum Erstellen einer Zugriffsrichtlinie finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Unsicherer Inhalt**.
4. Klicken Sie auf **Speichern**und dann auf **Fertig**.

Die folgende Abbildung zeigt eine Beispielbenachrichtigung, wenn Sie auf unsichere Inhalte zugreifen.



Keylogging-Schutz

Aktivieren/deaktivieren Sie mit dieser Zugriffsrichtlinie die Erfassung von Tastatureingaben durch Keylogger aus der SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

Mikrofon

Fordern Sie Benutzer bei jedem Zugriff auf das Mikrofon innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App auf/fordern Sie sie nicht auf, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Jedes Mal nachfragen.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die die Einschränkung **Mikrofon** aktiviert ist.

Um das Mikrofon jederzeit ohne Nachfrage zuzulassen, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Mikrofon** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite **Mikrofoneinstellungen** auf **Zugriff immer erlauben**.
5. Klicken Sie auf **Speichern**und dann auf **Fertig**.

> **Hinweis:**
>
> - Wenn die Einschränkung **Mikrofon** in der Secure Workspace-Richtlinie aktiviert ist, zeigt Citrix Enterprise Browser die Einstellungen **Zulassen**an.
> - Wenn die Option **Jedes Mal nachfragen** in der Secure Workspace-Richtlinie festgelegt ist, variiert die auf Citrix Enterprise Browser angewendete Einstellung je nachdem, ob der Global App Configuration Service (GACS) zum Verwalten von Citrix Enterprise Browser verwendet wird.
> - Wenn GACS verwendet wird, wird die GACS-Einstellung auf den Citrix Enterprise Browser angewendet.
> - Wenn GACS nicht verwendet wird, zeigt der Citrix Enterprise Browser die Einstellung **Ask**an.
> - Derzeit unterstützt Secure Private Access die Blockierung des Mikrofons nicht. Wenn Sie ein Mikrofon blockieren müssen, müssen Sie dies über GACS tun.

Weitere Informationen zu GACS finden Sie unter Verwalten des Citrix Enterprise Browsers über den Global App Configuration-Dienst.

Benachrichtigungen

Erlauben/fordern Sie Benutzer jedes Mal auf, die Benachrichtigungen innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App anzuzeigen, wenn auf sie über den Citrix Enterprise Browser zugegriffen wird. Standardwert: Jedes Mal nachfragen.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist.

Um die Anzeige von Benachrichtigungen ohne Aufforderung zu blockieren, führen Sie die folgenden Schritte aus.

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Benachrichtigungen** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite „ **Benachrichtigungseinstellungen** “auf **Benachrichtigungen immer blockieren**.
5. Klicken Sie auf **Speichern**und dann auf **Fertig**.

Einfügen

Aktivieren/deaktivieren Sie das Einfügen kopierter Daten in die SaaS- oder interne Web-App mit dieser Zugriffsrichtlinie, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

> **Hinweis:**
>
> - Wenn in einer Richtlinie sowohl die Einschränkung **Zwischenablage** als auch **Einfügen** aktiviert sind, hat die Einschränkung **Zwischenablage** Vorrang vor der Einschränkung **Einfügen** .
> - Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.
> - Zur detaillierten Steuerung von Einfügevorgängen innerhalb der Apps können Administratoren die Einschränkung **Sicherheitsgruppen** verwenden. Einzelheiten finden Sie unter Zwischenablageeinschränkung für Sicherheitsgruppen.

Maskierung personenbezogener Daten

Aktivieren/deaktivieren Sie mit dieser Richtlinie das Redigieren oder Maskieren personenbezogener Daten (PII) in der SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser erfolgt.

> **Hinweis:**
>
> Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.

Führen Sie die folgenden Schritte aus, um personenbezogene Daten zu redigieren oder zu maskieren:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Maskierung personenbezogener Daten** und anschließend auf **Bearbeiten**.
4. Wählen Sie den Informationstyp aus, den Sie verschleiern oder maskieren möchten, und klicken Sie dann auf **Hinzufügen**.

   Wenn der Informationstyp nicht in der vordefinierten Liste angezeigt wird, können Sie einen benutzerdefinierten Informationstyp hinzufügen. Einzelheiten finden Sie unter Benutzerdefinierten Informationstyp hinzufügen.
5. Wählen Sie den Maskierungstyp aus.

   - **Vollständige Maskierung** –Verdecken Sie die vertraulichen Informationen vollständig, um sie unlesbar zu machen.
   - **Teilweise Maskierung** –Verdecken Sie die vertraulichen Informationen teilweise. Es werden nur die relevanten Abschnitte behandelt, der Rest bleibt unverändert.

     Wenn Sie **Teilmarkierung**auswählen, müssen Sie Zeichen auswählen, die am Anfang oder am Ende des Dokuments beginnen. Sie müssen die Zahlen in die Felder **Erste maskierte Zeichen** und **Letzte maskierte Zeichen** eingeben.

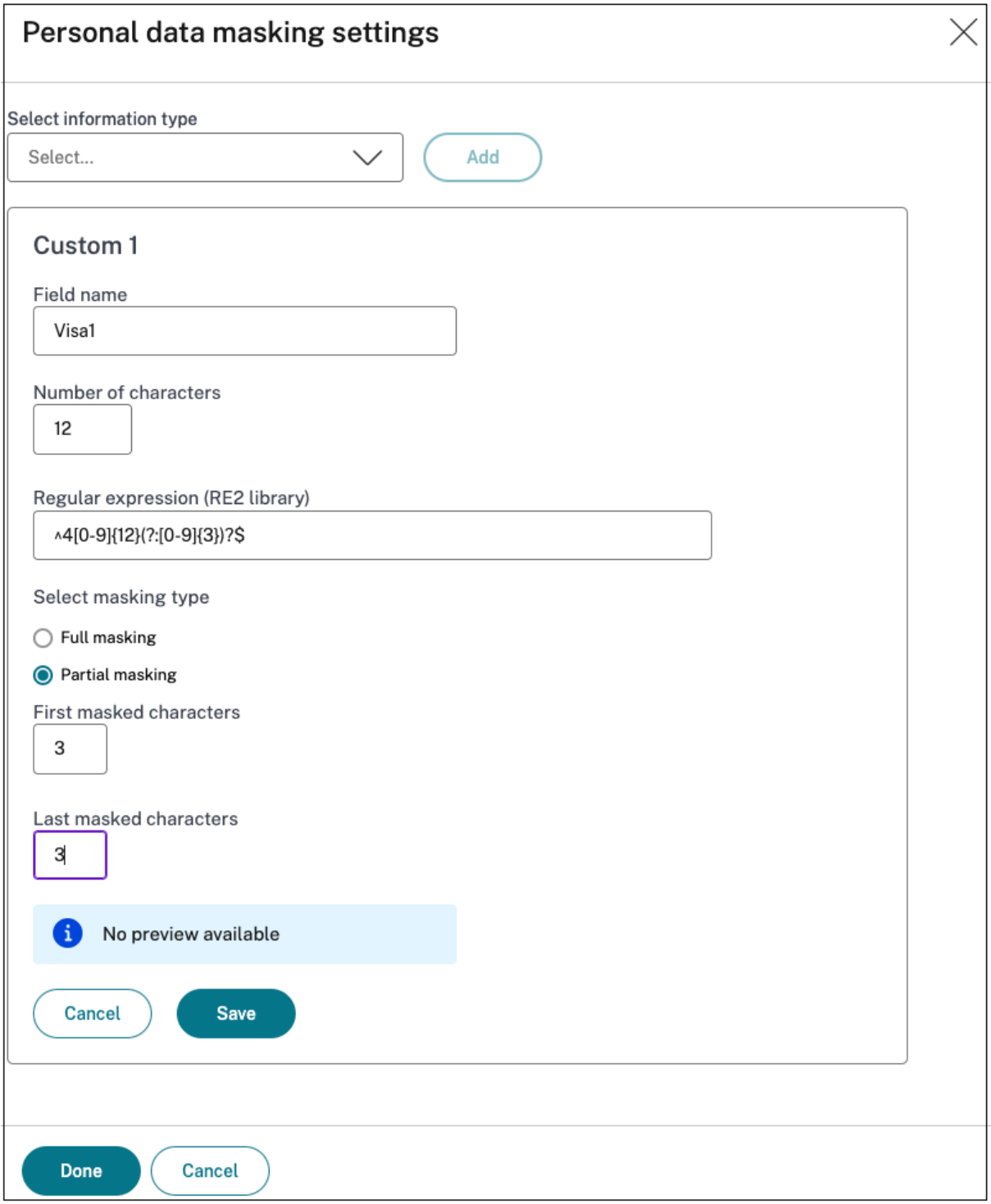
     Das Feld **Vorschau** zeigt das Maskierungsformat an. Diese Vorschau ist für benutzerdefinierte Richtlinien nicht verfügbar.
6. Klicken Sie auf **Speichern** und dann auf **Fertig**.

Benutzerdefinierten Informationstyp hinzufügen

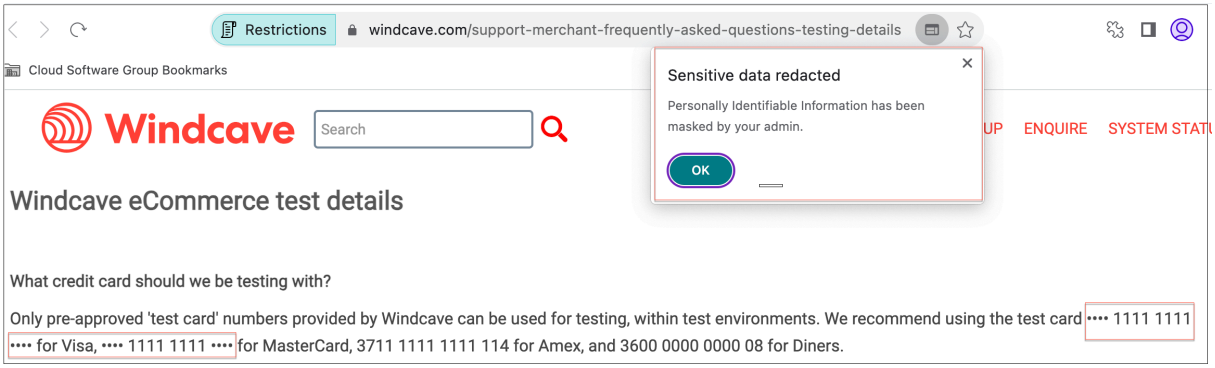
Sie können einen benutzerdefinierten Informationstyp hinzufügen, indem Sie den regulären Ausdruck des Informationstyps hinzufügen.

1. Wählen Sie in **Informationstyp**aus, wählen Sie **Benutzerdefiniert**aus und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie in **Feldname**den Namen für den Informationstyp ein, den Sie maskieren möchten.
3. Geben Sie in **Anzahl der Zeichen**die Anzahl der Zeichen des Informationstyps ein.
4. Geben Sie in **Regulärer Ausdruck (RE2-Bibliothek)**den Ausdruck für den benutzerdefinierten Informationstyp ein. Beispiel: `^4[0-9]{ 12 } (?:[0-9]{ 3 } )?$`.
5. Wählen Sie einen Maskierungstyp aus, wenn Sie die gesamten Informationen oder die ersten bzw. letzten Zeichen maskieren möchten.

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



Die folgende Abbildung zeigt eine Beispiel-App, in der die PII maskiert sind. In der Abbildung wird auch die Benachrichtigung zur Maskierung der PII angezeigt.



Popups

Aktivieren/deaktivieren Sie die Anzeige von Popups innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App beim Zugriff über den Citrix Enterprise Browser. Standardmäßig sind Popups auf Webseiten deaktiviert. Standardwert: Popups immer blockieren.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist.

Um die Anzeige von Popups zu aktivieren, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Popups** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite „ **Popup-Einstellungen** “auf **Popups immer zulassen**.
5. Klicken Sie auf **Speichern**und dann auf **Fertig**.

Drucken

Aktivieren/deaktivieren Sie mit dieser Richtlinie das Drucken von Daten aus den konfigurierten SaaS- oder internen Web-Apps beim Zugriff über den Citrix Enterprise Browser. Standardwert: Aktiviert.

Die folgende Meldung wird angezeigt, wenn ein Endbenutzer versucht, Inhalte aus der Anwendung zu drucken, für die die Druckbeschränkung aktiviert ist.

> **Hinweis:**
>
> - Wenn Sie die Druckoption für Endbenutzer deaktiviert haben, können die Endbenutzer beim Zugriff über den Citrix Enterprise Browser innerhalb der App Druckzugriff anfordern. Einzelheiten finden Sie unter Druckzugriff auf Anfrage.
> - Wenn in einer Richtlinie sowohl die Einschränkungen **Drucken** als auch **Druckerverwaltung** aktiviert sind, hat die Einschränkung **Drucken** Vorrang vor der Einschränkung **Druckerverwaltung** .

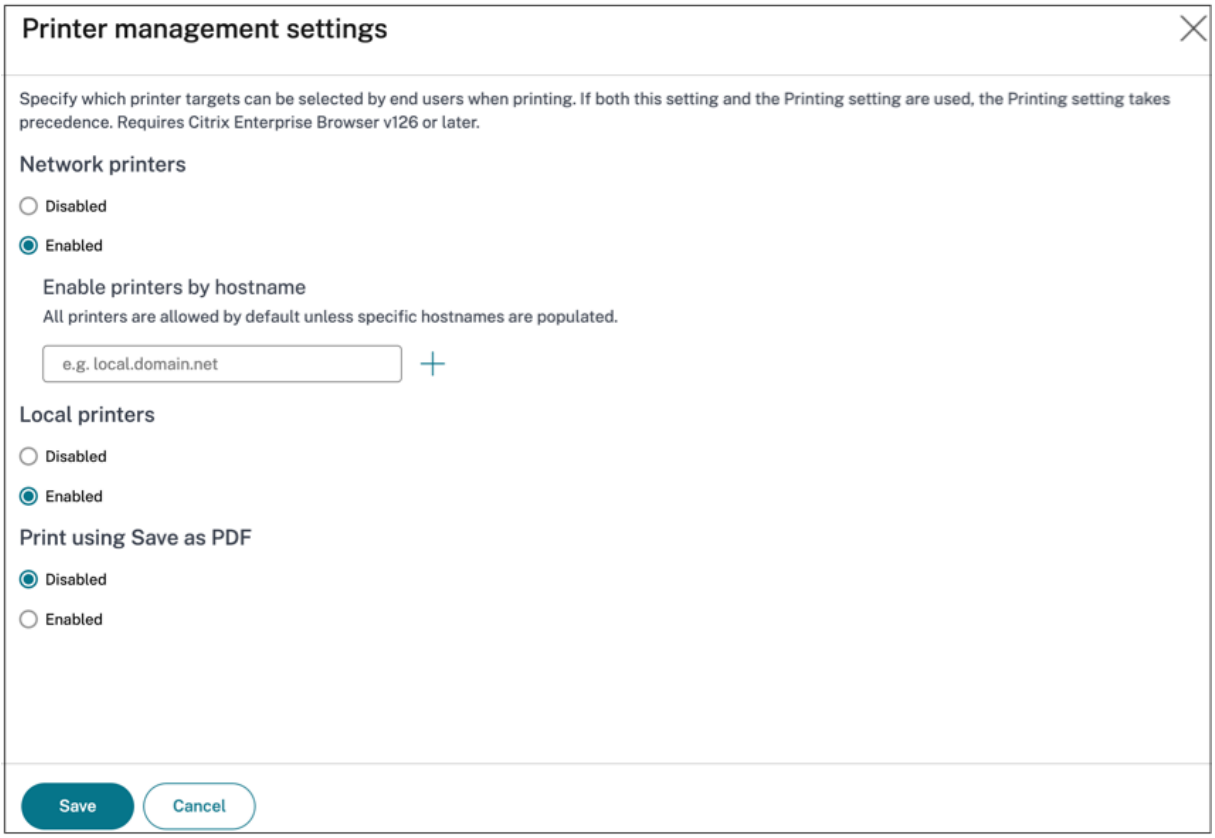
Druckerverwaltung

Aktivieren/deaktivieren Sie das Drucken von Daten mithilfe der vom Administrator konfigurierten Drucker aus den konfigurierten SaaS- oder internen Web-Apps mit dieser Richtlinie, wenn der Zugriff über den Citrix Enterprise Browser erfolgt.

> **Hinweis:**
>
> - Die Einschränkung **Druckerverwaltung** ist zusätzlich zur Einschränkung **Drucken** verfügbar, bei der das Drucken entweder aktiviert oder deaktiviert wird. Wenn in einer Zugriffsrichtlinie sowohl die Einschränkungen **Drucken** als auch **Druckerverwaltung** aktiviert sind, hat die Einschränkung **Drucken** Vorrang vor der Einschränkung **Druckerverwaltung** .
> - Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.

Um Druckbeschränkungen zu aktivieren/deaktivieren, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten zum Erstellen einer Zugriffsrichtlinie finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Druckerverwaltung** und anschließend auf **Bearbeiten**.



1. Wählen Sie die Ausnahmen entsprechend Ihrem Bedarf aus.

   - **Netzwerkdrucker** - Ein Netzwerkdrucker ist ein Drucker, der an ein Netzwerk angeschlossen und von mehreren Benutzern verwendet werden kann.
     - **Deaktiviert:** Das Drucken von allen Druckern im Netzwerk ist deaktiviert.
     - **Aktiviert:** Das Drucken von allen Netzwerkdruckern ist aktiviert. Wenn Drucker-Hostnamen angegeben werden, werden alle anderen Netzwerkdrucker außer den angegebenen blockiert.

     Hinweis: Netzwerkdrucker werden anhand ihres Hostnamens identifiziert.

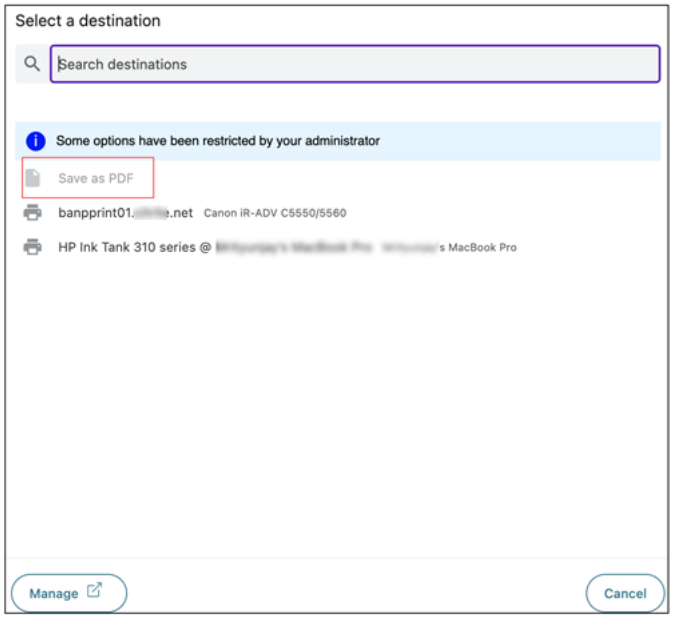
   - **Lokale Drucker** –Ein lokaler Drucker ist ein Gerät, das über eine Kabelverbindung direkt mit einem einzelnen Computer verbunden ist. Diese Verbindung wird normalerweise über USB, parallele Anschlüsse oder andere direkte Schnittstellen hergestellt.
     - **Deaktiviert:** Das Drucken von allen lokalen Druckern ist deaktiviert.
     - **Aktiviert:** Das Drucken von allen lokalen Druckern ist aktiviert.

   - **Drucken mit Als PDF speichern**
     - **Deaktiviert**: Das Speichern des Inhalts der Anwendung im PDF-Format ist deaktiviert.
     - **Aktiviert:** Das Speichern des Inhalts der Anwendung im PDF-Format ist aktiviert.

2. Klicken Sie auf **Speichern**.

Wenn ein Netzwerkdrucker deaktiviert ist, wird der jeweilige Druckername ausgegraut angezeigt, wenn Sie versuchen, den Drucker im Feld **Ziel** auszuwählen.

Wenn außerdem **Drucken mit „Als PDF speichern“** deaktiviert ist, wird die Option **Als PDF speichern** ausgegraut angezeigt, wenn Sie im Feld **Ziel** auf den Link **Mehr anzeigen** klicken.



Bildschirmaufnahme

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Möglichkeit zum Erfassen der Bildschirme der SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser mithilfe eines der Bildschirmerfassungsprogramme oder -apps erfolgt. Wenn ein Benutzer versucht, den Bildschirm zu erfassen, wird ein leerer Bildschirm erfasst. Standardwert: Aktiviert.

Uploadbeschränkung nach Dateityp

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Möglichkeit des Benutzers, bestimmte MIME-Typen (Dateien) aus der SaaS- oder internen Web-App herunterzuladen, wenn der Zugriff über den Citrix Enterprise Browser erfolgt.

> **Hinweis:**
>
> - Die Upload-Beschränkung **nach Dateityp** ist zusätzlich zur Upload-Beschränkung **verfügbar.
> - Wenn in einer Richtlinie sowohl die Beschränkungen **Upload** als auch **Uploadbeschränkung nach Dateityp** aktiviert sind, hat die Einschränkung **Uploads** Vorrang vor der Ein-

> schränkung **Uploadbeschränkung nach Dateityp** .
> - Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.

Um das Hochladen von MIME-Typen zu aktivieren/deaktivieren, führen Sie die folgenden Schritte aus:

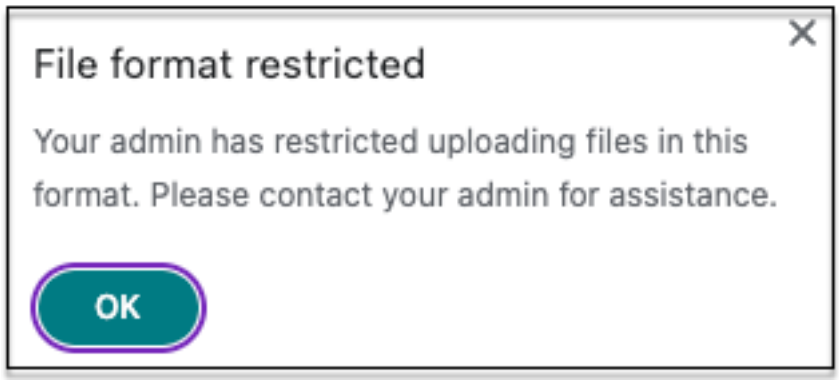
1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Upload-Beschränkung nach Dateityp** und dann auf **Bearbeiten**.
4. Wählen Sie auf der Seite „Uploadbeschränkung nach Dateitypeinstellungen “ eine der folgenden Optionen aus:

   Alle Uploads mit Ausnahmen zulassen. –Alle Dateien außer den ausgewählten Typen hochladen. **Alle Uploads mit Ausnahmen blockieren.** –Blockiert das Hochladen aller Dateitypen außer den ausgewählten Typen.
5. Wenn der Dateityp nicht in der Liste vorhanden ist, gehen Sie wie folgt vor:

   a) Klicken Sie auf **Benutzerdefinierte MIME-Typen hinzufügen**.
   b) Geben Sie in **MIME-Typen hinzufügen**den MIME-Typ im Format `Kategorie/Unterkategorie<extension>`ein. Beispiel: `image/png`.
   c) Klicken Sie auf **Fertig**.

   Der MIME-Typ wird jetzt in der Liste der Ausnahmen angezeigt.

Wenn ein Endbenutzer versucht, einen eingeschränkten Dateityp hochzuladen, zeigt Citrix Enterprise Browser eine Warnmeldung an.



Uploads

Aktivieren/deaktivieren Sie die Möglichkeit des Benutzers zum Hochladen innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

> **Hinweis:**
>
> Wenn in einer Richtlinie sowohl die Einschränkung **Uploads** als auch die Einschränkung **Uploadbeschränkung nach Dateityp** aktiviert sind, hat die Einschränkung **Uploads** Vorrang vor der Einschränkung **Uploadbeschränkung nach Dateityp** .

Wasserzeichen

Aktivieren/deaktivieren Sie das Wasserzeichen auf dem Benutzerbildschirm, das den Benutzernamen und die IP-Adresse des Computers des Benutzers anzeigt. Standardwert: Deaktiviert.

Webcam

Fordern Sie Benutzer bei jedem Zugriff auf die Webcam innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App auf/fordern Sie sie nicht auf, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Jedes Mal nachfragen.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die die Einschränkung **Webcam** aktiviert ist.

Um die Webcam jedes Mal ohne Nachfrage zuzulassen, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Webcam** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite „ **Webcam-Einstellungen** “auf **Zugriff immer erlauben**.
5. Klicken Sie auf **Speichern**und dann auf **Fertig**.

> **Hinweis:**
>
> - Wenn die Webcam-Einschränkung in der Secure Workspace-Richtlinie aktiviert ist, zeigt Citrix Enterprise Browser die Einstellungen **Zulassen**an.
> - Wenn die Option **Jedes Mal nachfragen** in der Secure Workspace-Richtlinie ist, variiert die auf Citrix Enterprise Browser angewendete Einstellung je nachdem, ob der Global App Configuration Service (GACS) zum Verwalten von Citrix Enterprise Browser verwendet wird.
> - Wenn GACS verwendet wird, wird die GACS-Einstellung auf den Citrix Enterprise Browser

> angewendet.
> - Wenn GACS nicht verwendet wird, zeigt der Citrix Enterprise Browser die Einstellung **Ask**an.
> - Derzeit unterstützt Secure Private Access das Blockieren der Webcam nicht. Wenn Sie die Webcam blockieren müssen, müssen Sie dies über GACS tun.

Weitere Informationen zu GACS finden Sie unter Verwalten des Citrix Enterprise Browsers über den Global App Configuration-Dienst.

Zwischenablagebeschränkung für Sicherheitsgruppen

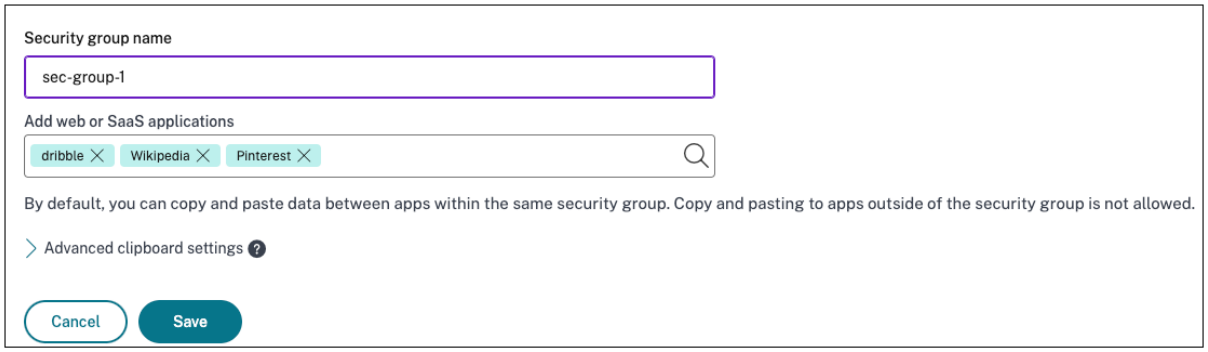
Sie können den Zugriff auf die Zwischenablage für eine bestimmte Gruppe von Apps aktivieren, indem Sie die Einschränkung **Sicherheitsgruppen (Anwendungen > Sicherheitsgruppen)**verwenden. Sicherheitsgruppen wird eine Reihe von Apps zugewiesen, innerhalb derer Kopier- und Einfügevorgänge durchgeführt werden können. Um den Zugriff auf die Zwischenablage innerhalb der Apps in einer Sicherheitsgruppe zu aktivieren, müssen Sie lediglich eine Zugriffsrichtlinie mit der Aktion **Zulassen** oder **Zulassen mit Einschränkungen** konfigurieren, ohne eine Zugriffseinstellung auszuwählen.

- Wenn die Einschränkung **Sicherheitsgruppen** aktiviert ist, können Sie keine Daten zwischen Anwendungen in verschiedenen Sicherheitsgruppen kopieren/einfügen. Wenn beispielsweise die App „ProdDocs“zur Sicherheitsgruppe „SG1“und die App „Edocs“zur Sicherheitsgruppe „SG2 “gehört, können Sie Inhalte nicht von „Edocs“nach „ProdDocs“kopieren/einfügen, selbst wenn die Einschränkung **Kopieren** / **Einfügen** für beide Gruppen aktiviert ist.
- Für Apps, die nicht Teil einer Sicherheitsgruppe sind, können Sie eine Zugriffsrichtlinie mit der Aktion **Zulassen mit Einschränkungen** erstellen und die Einschränkungen auswählen (**Kopieren**, **Einfügen**oder **Zwischenablage**). In diesem Fall ist die App nicht Teil einer Sicherheitsgruppe und daher kann die Einschränkung **Kopieren** / **Einfügen** auf diese App angewendet werden.

> **Hinweis:**
>
> Sie können den Zwischenablagezugriff für Apps, auf die über Citrix Enterprise Browser zugegriffen wird, auch über den Global App Configuration Service (GACS) einschränken. Wenn Sie GACS zum Verwalten des Citrix Enterprise Browsers verwenden, verwalten Sie den Zugriff auf die Zwischenablage mit der Option **Sandboxed Clipboard aktivieren** . Wenn Sie den Zwischenablagezugriff über GACS einschränken, gilt dies für alle Apps, auf die über den Citrix Enterprise Browser zugegriffen wird. Weitere Informationen zu GACS finden Sie unter Verwalten des Citrix Enterprise Browsers über den Global App Configuration-Dienst.

Führen Sie die folgenden Schritte aus, um eine Sicherheitsgruppe zu erstellen:

1. Klicken Sie in der Secure Private Access-Konsole auf **Anwendungen** und dann auf **Sicherheitsgruppen**.
2. Klicken Sie auf **. Fügen Sie eine neue Sicherheitsgruppe hinzu**.

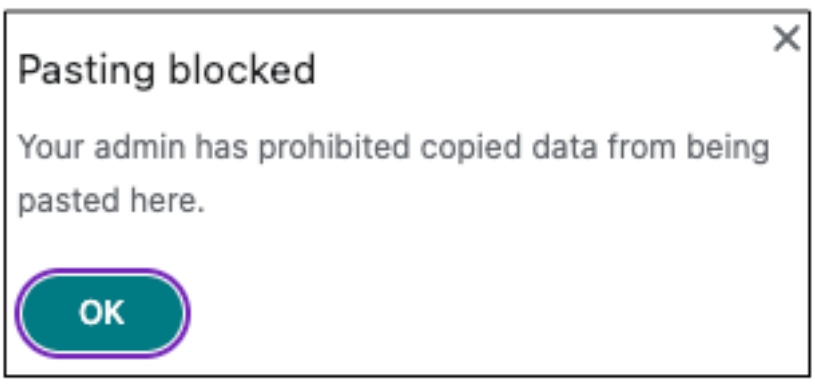


1. Geben Sie einen Namen für die Sicherheitsgruppe ein.
2. Wählen Sie unter **Web- oder SaaS-Anwendungen hinzufügen**die Anwendungen aus, die Sie gruppieren möchten, um die Kopier- und Einfügesteuerung zu aktivieren. Zum Beispiel Wikipedia, Pinterest und Dribble.
3. Klicken Sie auf **Speichern**.

Einzelheiten zu den erweiterten Zwischenablageeinstellungen finden Sie unter Kopier-/Einfügesteuerelemente für native Anwendungen und unveröffentlichte Apps aktivieren.

Wenn Endbenutzer diese Anwendungen (Wikipedia, Pinterest und Dribble) von Citrix Workspace aus starten, müssen sie Daten (Kopieren/Einfügen) von einer Anwendung mit den anderen Anwendungen innerhalb der Sicherheitsgruppe teilen können. Das Kopieren/Einfügen erfolgt unabhängig von anderen Sicherheitsbeschränkungen, die für die Anwendungen bereits aktiviert sind.

Endbenutzer können jedoch keine Inhalte aus den lokalen Anwendungen auf ihren Computern oder aus unveröffentlichten Anwendungen in diese bestimmten Anwendungen kopieren und einfügen und umgekehrt. Beim Kopieren des Inhalts aus der angegebenen Anwendung in eine andere Anwendung wird folgende Meldung angezeigt:



> **Hinweis:**
>
> Sie können das Kopieren/Einfügen von Inhalten aus lokalen Anwendungen auf Benutzercomputern oder aus nicht veröffentlichten Anwendungssteuerungen aktivieren, indem Sie die Optionen im Abschnitt **Erweiterte Zwischenablageeinstellungen** verwenden. Einzelheiten hierzu finden Sie unter Aktivieren von Kopier-/Einfügesteuerelementen für native Anwendungen und unveröffentlichte Apps.

Aktivieren Sie Kopieren/Einfügen auf granularer Ebene

Sie können den Zugriff auf die Zwischenablage in detaillierten Stufen innerhalb der Anwendungen einer bestimmten Gruppe aktivieren. Sie können dies tun, indem Sie Zugriffsrichtlinien für die Anwendungen erstellen und die Einschränkung **Kopieren** / **Einfügen** entsprechend Ihrem Bedarf aktivieren.

> **Hinweis:**
>
> Stellen Sie sicher, dass die spezifische Zugriffsrichtlinie, die Sie für den granularen Zwischenablagezugriff erstellt haben, eine höhere Priorität hat als die Richtlinie, die Sie für die Sicherheitsgruppen erstellt haben.

Beispiel:

Nehmen wir an, Sie haben eine Sicherheitsgruppe mit drei Anwendungen erstellt, nämlich Wikipedia, Pinterest und Dribble.

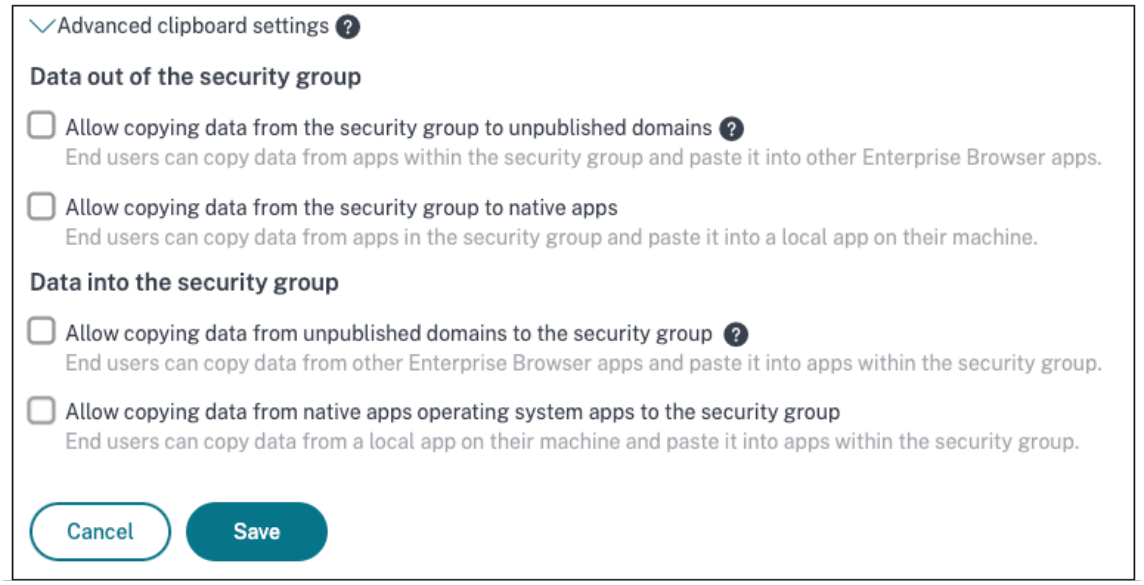
Jetzt möchten Sie das Einfügen von Inhalten aus Wikipedia oder Dribble in Pinterest einschränken. Führen Sie dazu die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine der Anwendung `Pinterest`zugewiesene Zugriffsrichtlinie. Einzelheiten zum Erstellen einer Zugriffsrichtlinie finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen**die Option **Zulassen mit Einschränkungen**aus.
3. Wählen Sie **und fügen Sie**ein.

Obwohl Pinterest Teil einer Sicherheitsgruppe ist, die auch Wikipedia und Dribble enthält, können Benutzer aufgrund der mit Pinterest verknüpften Zugriffsrichtlinie, in der die Einschränkung **Einfügen** aktiviert ist, keine Inhalte von Wikipedia oder Dribble nach Pinterest kopieren.

Aktivieren Sie Kopier-/Einfügekontrollen für native Anwendungen und unveröffentlichte Apps

1. Erstellen Sie eine Sicherheitsgruppe. Weitere Einzelheiten finden Sie unter Zwischenablage-Sicherheitsgruppen für Kopier- und Einfügebeschränkungen.
2. Erweitern Sie **Erweiterte Zwischenablageeinstellungen**.



3. Wählen Sie je nach Bedarf die folgenden Optionen aus:

   - **Kopieren von Daten aus der Sicherheitsgruppe in nicht veröffentlichte Domänen zulassen.** –Kopieren von Daten aus Anwendungen in den Sicherheitsgruppen in die Apps aktivieren, die nicht in Secure Private Access veröffentlicht sind.
   - **Kopieren von Daten aus der Sicherheitsgruppe in native Apps zulassen.** –Aktivieren Sie das Kopieren von Daten aus den Anwendungen in den Sicherheitsgruppen in die lokalen Anwendungen auf Ihren Computern.
   - **Kopieren von Daten aus nicht veröffentlichten Domänen in die Sicherheitsgruppe zulassen.** –Kopieren von Daten aus nicht über Secure Private Access veröffentlichten Apps in die Anwendungen in den Sicherheitsgruppen aktivieren.
   - **Erlaubt das Kopieren von Daten aus nativen Apps des Betriebssystems. Die Sicherheitsgruppe** - Aktiviert das Kopieren von Daten aus lokalen Anwendungen auf den Maschinen in die Anwendungen.

Bekannte Probleme

- Die Routing-Tabelle in (**Einstellungen > Anwendungsdomäne**) behält die Domänen einer gelöschten Anwendung bei. Daher werden diese Anwendungen auch im Secure Private Access als veröffentlichte Anwendungen betrachtet. Wenn auf diese Domänen direkt über den

Citrix Enterprise Browser zugegriffen wird, ist Kopieren/Einfügen aus diesen Anwendungen deaktiviert, unabhängig von den Optionen, die Sie in **Erweiterte Zwischenablageeinstellungen**ausgewählt haben.

Nehmen wir beispielsweise das folgende Szenario an:

- Sie haben eine Anwendung namens Jira2 (`https://test.citrite.net`) gelöscht, die Teil einer Sicherheitsgruppe war.
- Sie haben die Option **Kopieren von Daten aus der Sicherheitsgruppe in nicht veröffentlichte Domänen zulassen**aktiviert.

Wenn der Benutzer in diesem Szenario versucht, Daten aus dieser Anwendung in eine andere Anwendung in derselben Sicherheitsgruppe zu kopieren, wird die Einfügesteuerung deaktiviert. Dem Benutzer wird eine entsprechende Benachrichtigung angezeigt.

- Bei einer SaaS-App kann der App-Zugriff verweigert werden, wenn die Anwendung mit einer Zugriffsrichtlinie mit der Aktion **Zugriff verweigern konfiguriert ist.** Die Endbenutzer können weiterhin auf die App zugreifen, da der App-Verkehr nicht über Secure Private Access getunnelt wird. Auch wenn die Anwendung Teil der Sicherheitsgruppe ist, werden die Einstellungen der Sicherheitsgruppe nicht berücksichtigt und Sie können daher keine Inhalte aus der Anwendung kopieren/einfügen.

Ablauf für Endbenutzer

August 26, 2024

SaaS-App

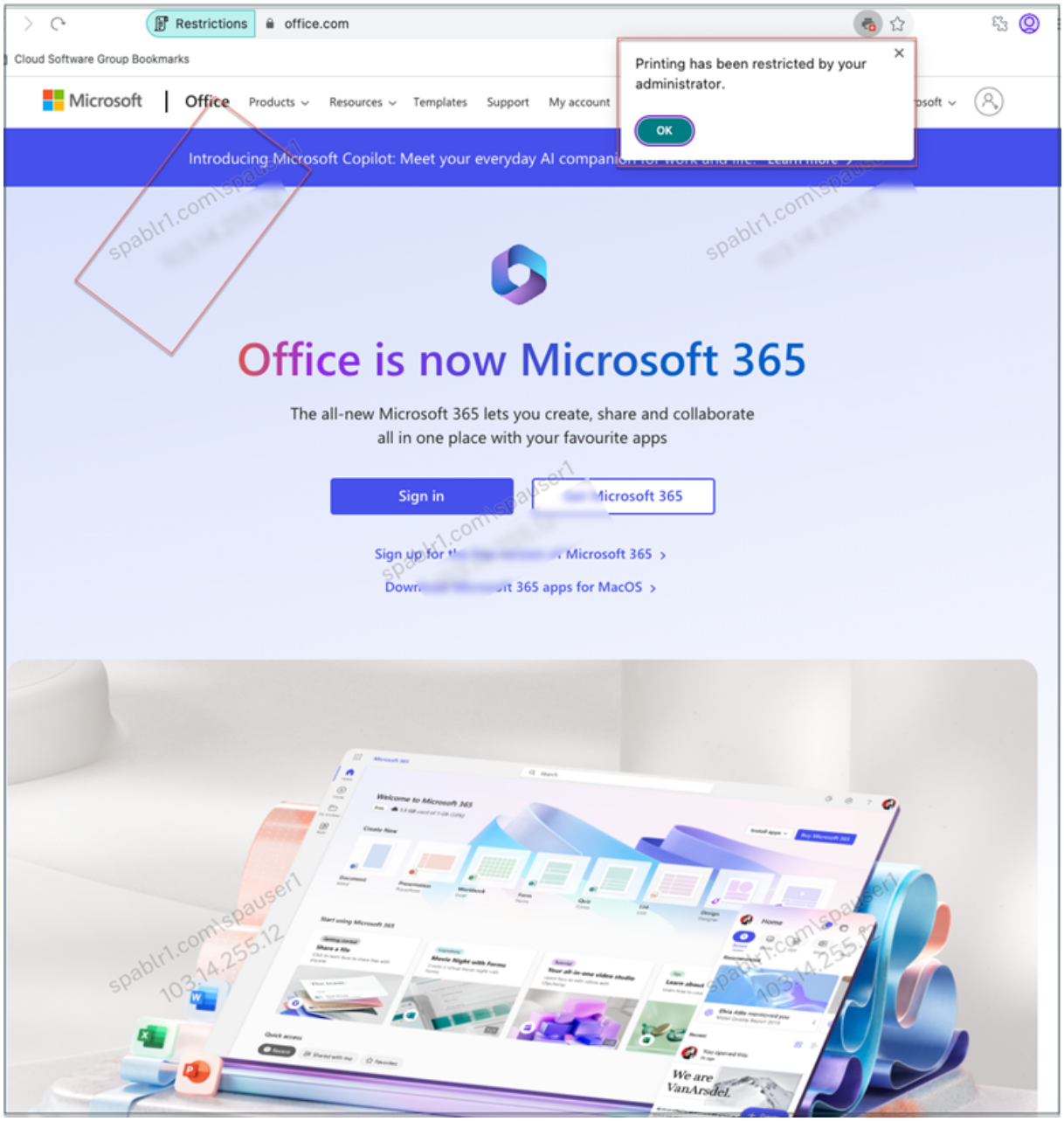
Angenommen, ein Administrator hat die Office365-App mit der Wasserzeichen- und Druckbeschränkung für den Endbenutzer konfiguriert. Wenn der Endbenutzer nun auf die Office365-App zugreift, müssen die Wasserzeichen- und Druckbeschränkungen auf die App angewendet werden.

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.



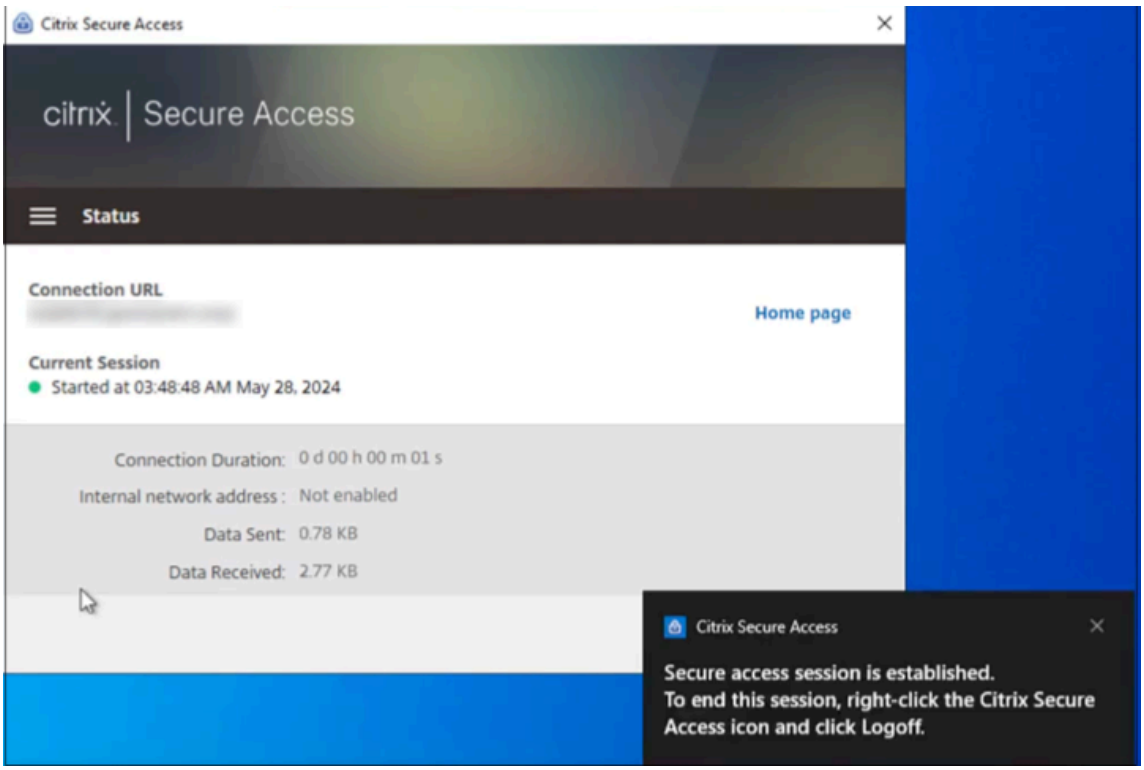
Hinweis:

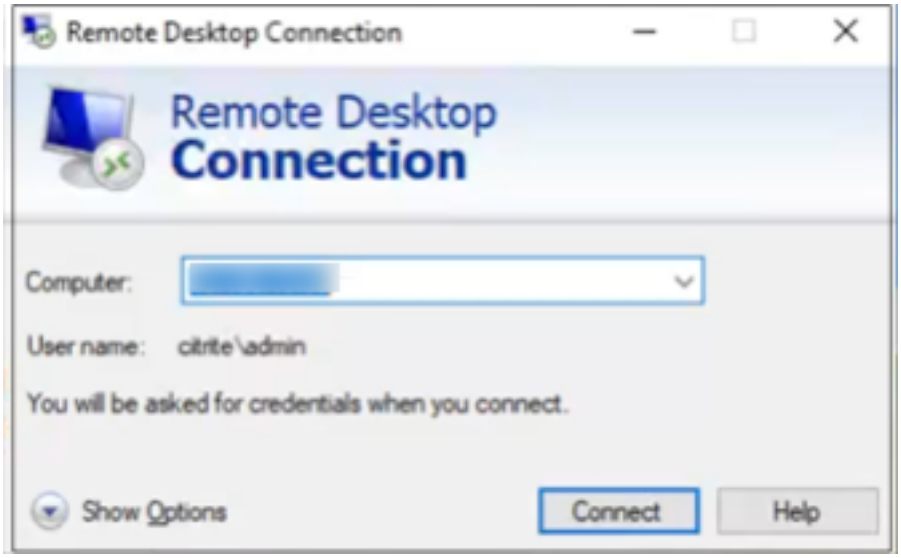
Administratoren müssen Benutzern die Kontoinformationen zur Verfügung stellen, die sie für den Zugriff auf virtuelle Desktops und Anwendungen benötigen. Einzelheiten finden Sie unter Hinzufügen einer Store-URL zur Citrix Workspace-App.

TCP/UDP-App

Wenn RDP konfiguriert ist, müssen Endbenutzer die folgenden Schritte ausführen, um auf die TCP/UDP-App zuzugreifen.

1. Melden Sie sich beim Citrix Secure Access Client an.
2. Nachdem die Secure Access-Sitzung eingerichtet wurde, starten Sie eine Remote-Desktop-Verbindung.





a) Drücken Sie die **Windows-Taste**, geben Sie **Remote Desktop Connection** ein und drücken Sie die **Eingabetaste**.
b) Geben Sie die IP-Adresse oder den Hostnamen des Computers ein, mit dem Sie eine Verbindung herstellen möchten.
c) Klicken Sie auf **Verbinden**. Möglicherweise werden Sie aufgefordert, die Anmeldeinformationen einzugeben.
d) Geben Sie den Benutzernamen und das Kennwort für den Remotecomputer ein und klicken Sie dann auf **OK**.

Eine Remote-Desktop-Verbindung ist jetzt hergestellt und der Endbenutzer kann mit dem Remote-Computer interagieren.

Upgrade

October 21, 2024

Sie können Ihre Secure Private Access-Bereitstellungen auf eine neuere Version aktualisieren, ohne zuerst neue Maschinen oder Sites einrichten zu müssen. Wir empfehlen Ihnen, vor dem Upgrade die Snapshots zu erstellen oder die Konfigurationen zu speichern. Um ein Upgrade zu starten, führen Sie das Installationsprogramm der neuen Version aus, um das zuvor installierte Secure Private Access-Plug-In zu aktualisieren.

Aktualisierungsreihenfolge

Die Upgrade-Reihenfolge ist wie folgt:

1. Sie können Secure Private Access über den Delivery Controller oder über die dedizierte Kachel „Secure Private Access“in der Benutzeroberfläche des Installationsprogramms aktualisieren, je nachdem, wie Sie Secure Private Access ursprünglich installiert haben.

   - Wenn Sie Secure Private Access über den Delivery Controller installiert haben, können Sie die Komponente Secure Private Access nicht alleine aktualisieren. Stattdessen müssen Sie alle Komponenten aktualisieren. Weitere Einzelheiten finden Sie unter Aktualisieren einer Bereitstellung.
   - Wenn Sie Secure Private Access über die dedizierte Kachel „Secure Private Access“installiert haben, können Sie es unabhängig davon aktualisieren. Weitere Einzelheiten finden Sie unter Aktualisieren Sie Ihr Secure Private Access-Installationsprogramm.

> **Hinweis:**
>
> Wir empfehlen, Secure Private Access für POC-Umgebungen über den Delivery Controller zu installieren. Für Produktionsumgebungen empfehlen wir jedoch die Verwendung des dedizierten Installationsprogramms, damit Sie neue Features oder Funktionen anpassen können.

1. Führen Sie die Datenbankskripte aus. Weitere Einzelheiten finden Sie unter Aktualisieren Sie die Datenbank mithilfe der Skripts.
2. Starten Sie die **Standardwebsite** und **Citrix Access Security Admin Site** auf der **Internet Information Service (IIS) Manager** -Konsole neu, um die Änderungen zu übernehmen.
3. Führen Sie die StoreFront-Konfiguration erneut aus. Laden Sie die StoreFront-Skripte von **Einstellungen > Konfiguration**herunter und führen Sie die Skripte auf den entsprechenden StoreFront-Computern aus. Einzelheiten finden Sie unter Integrationseinstellungen ändern.

> **Hinweis:**
>
> Wenn Sie die Skripte nicht ausführen, werden die Endpunkte nicht ausgelöst.

1. (Optional) Führen Sie das NetScaler Gateway-Skript aus. Einzelheiten finden Sie unter NetScaler Gateway.

Komponenten-Upgrade

Informationen zum Upgrade der Komponenten, die an der lokalen Bereitstellung von Secure Workspace Access beteiligt sind, finden Sie in den folgenden Themen.

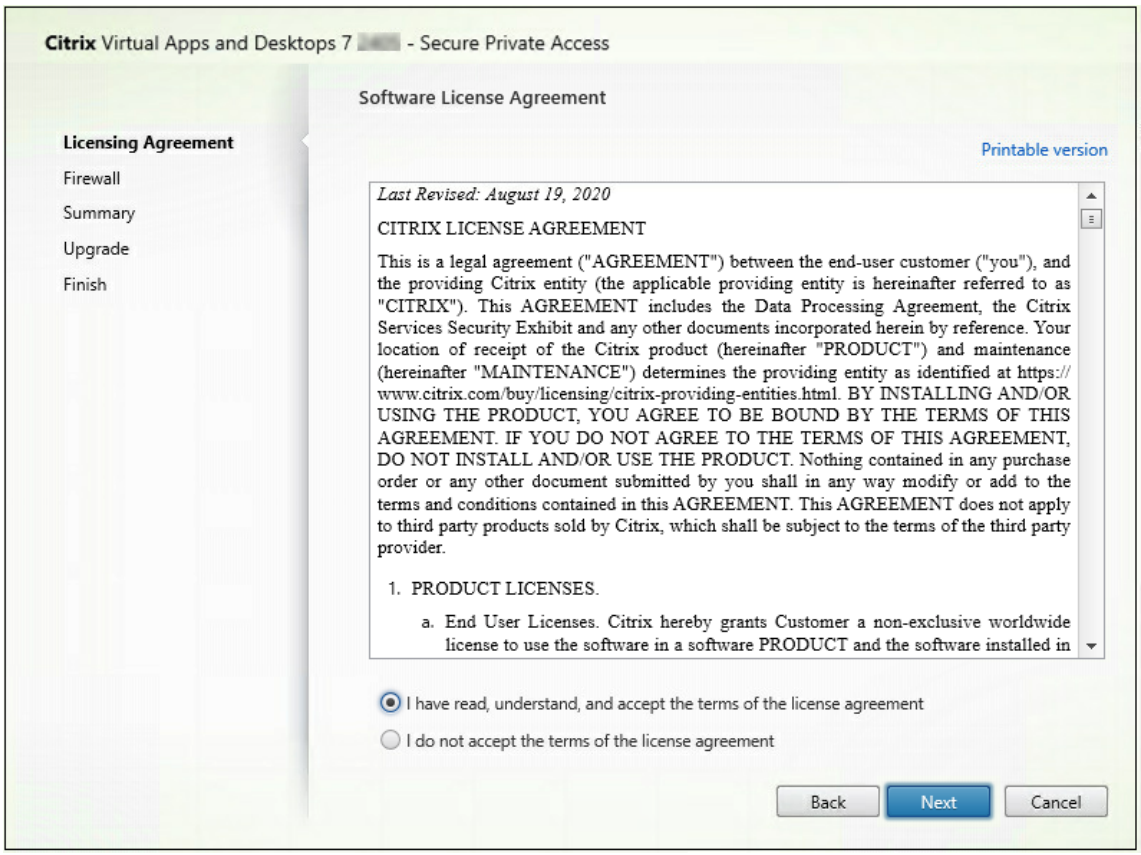
- Cloud Connector
- StoreFront
- NetScaler Gateway
- Lizenzserver
- Web Studio
- Director

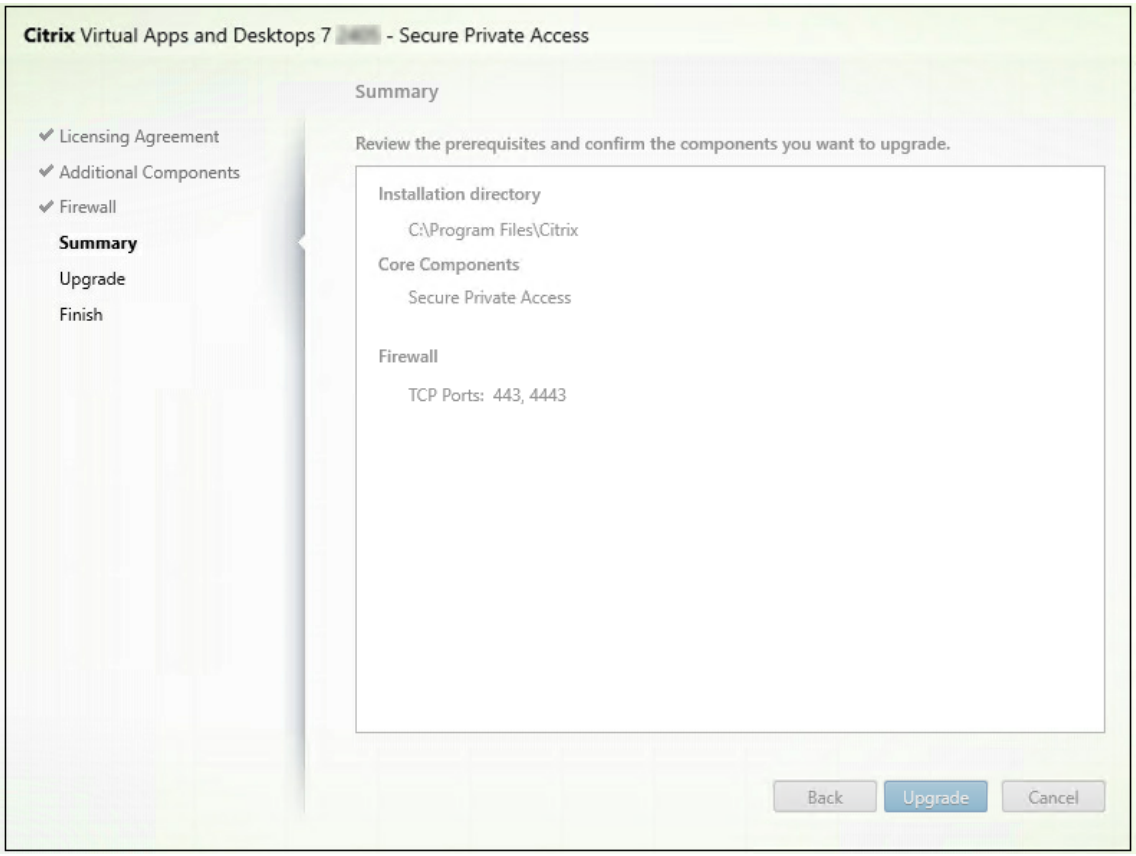
Aktualisieren Sie Ihr Secure Private Access-Installationsprogramm

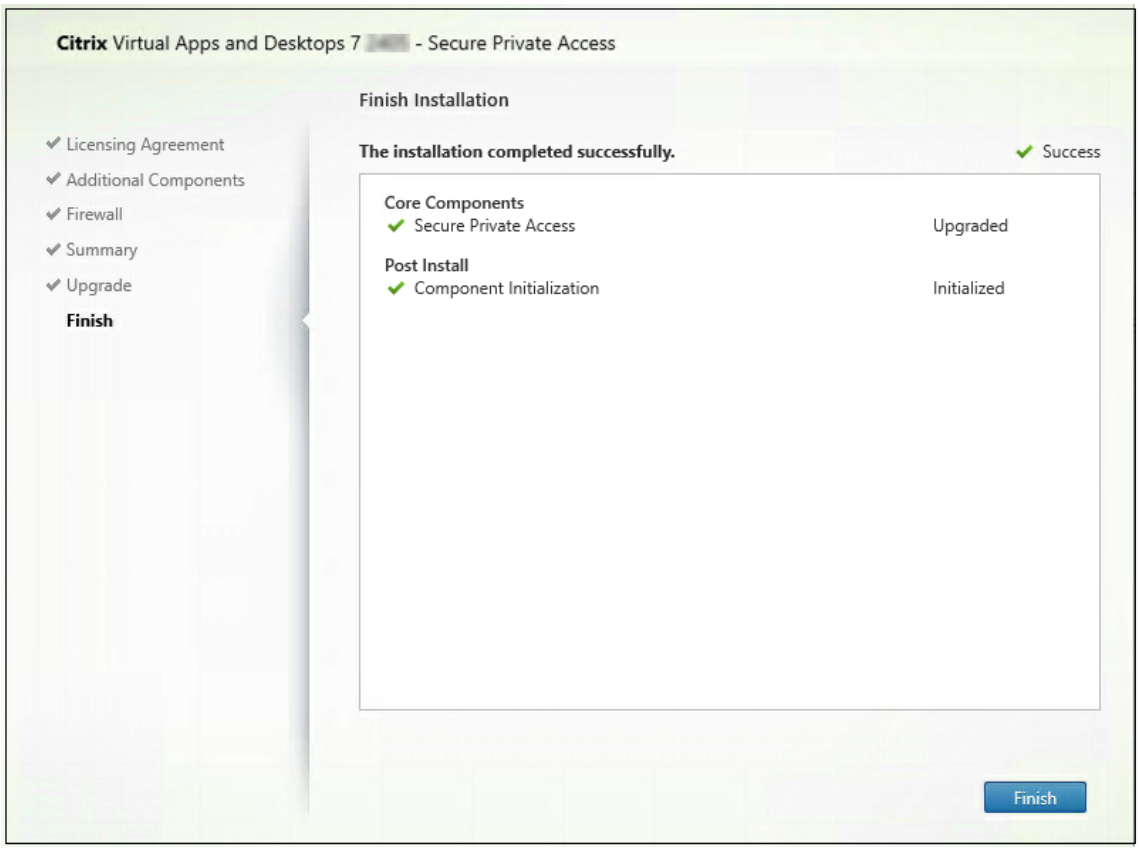
October 21, 2024

1. Laden Sie das Citrix Secure Private Access-Installationsprogramm von https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/herunter.
2. Führen Sie die EXE-Datei als Administrator auf einem der Domäne beigetretenen Computer aus.

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







> **Wichtig:**
>
> Nachdem Sie das Installationsprogramm aktualisiert haben, um die neueste Version freizugeben, müssen Sie das StoreFront-Skript erneut ausführen, damit die neuen Endpunktdetails verfügbar sind.

Nächste Schritte

- Einrichten von Secure Private Access
- Konfigurieren von NetScaler Gateway
- Konfigurieren Sie Anwendungen
- Konfigurieren Sie 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
   >
   ```

Verwalten von Konfigurationen

October 21, 2024

Nachdem Sie Secure Private Access installiert haben, können Sie die Einstellungen auf der Seite **Einstellungen** ändern. Sie können das Routing von Anwendungsdomänen und Administratoren verwalten und die Integrationseinstellungen ändern.

Um die Einstellungen zu ändern, müssen Sie sich mit einem Secure Private Access-Administratorkonto bei der Secure Private Access-Administratorkonsole anmelden.

Ausführliche Informationen zum Aktualisieren oder Ändern der Einstellungen finden Sie in den folgenden Themen:

- Routing von Anwendungsdomänen verwalten
- Administratoren verwalten
- Integrationseinstellungen ändern

Nicht genehmigte Websites verwalten

Sie können auch Regeln für nicht genehmigte Websites konfigurieren. Anwendungen (Intranet oder Internet), die nicht in Secure Private Access konfiguriert sind, gelten als „nicht genehmigte Websites“. Einzelheiten finden Sie unter Nicht genehmigte Websites.

Tool zur Richtlinienmodellierung

Das Tool zur Richtlinienmodellierung bietet Einblick in das Ergebnis des Anwendungszugriffs (zugelassen, mit Einschränkung zugelassen oder verweigert). Administratoren können die Zugriffsergebnisse für bestimmte Benutzer und Benutzerbedingungen überprüfen. Einzelheiten finden Sie unter Richtlinienmodellierungstool.

Nicht genehmigte Websites

August 26, 2024

Anwendungen (Intranet oder Internet), die nicht in Secure Private Access konfiguriert sind, werden als “nicht genehmigte Websites”betrachtet. Standardmäßig verweigert Secure Private Access den Zugriff auf alle Intranet-Webanwendungen, wenn für diese Anwendungen keine Anwendungen und Zugriffsrichtlinien konfiguriert sind.

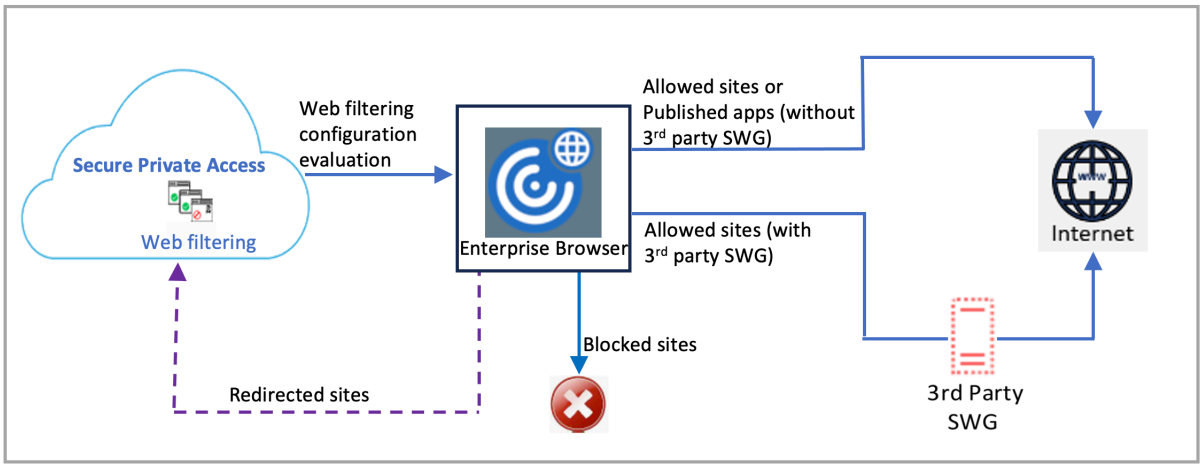
Für alle anderen Internet-URLs oder SaaS-Anwendungen, für die keine App konfiguriert ist, können Administratoren den Tab **Einstellungen > Unsanktionierte Websites** in der Admin-Konsole verwenden, um den Zugriff über den Citrix Enterprise Browser zuzulassen oder zu verweigern.

> **Hinweis:**
>
> Standardmäßig sind die Einstellungen so konfiguriert, dass der Zugriff auf alle Internet-URLs oder SaaS-Apps über den Citrix Enterprise Browser ZUGELASSEN wird.

So funktionieren nicht genehmigte Websites

1. Die URL-Analyse wird durchgeführt, um festzustellen, ob die URL eine Citrix Dienst-URL ist.
2. Die URL wird dann überprüft, um festzustellen, ob es sich um eine Enterprise Web- oder SaaS-App-URL handelt.
3. Die URL wird dann überprüft, um festzustellen, ob sie als blockierte URL identifiziert wurde oder ob auf die URL zugegriffen werden kann.

Die folgende Abbildung erläutert den Datenfluss für Endbenutzer.



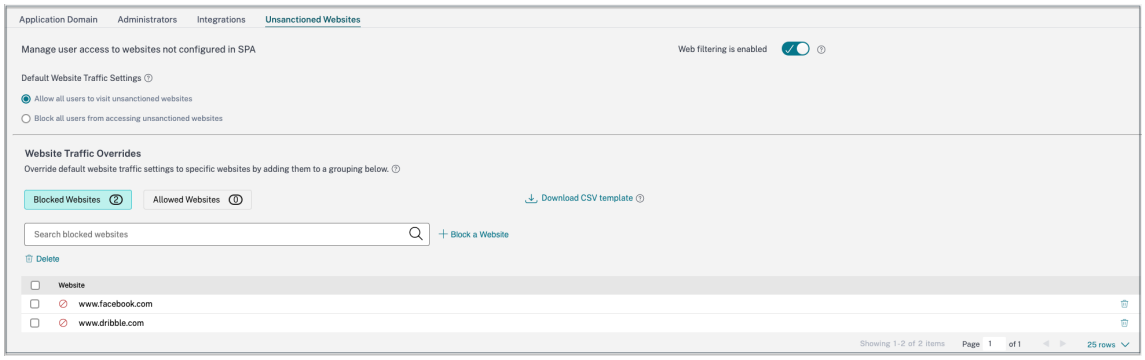
Nach dem Empfang einer Anfrage werden folgende Prüfungen und zugehörige Aktionen ausgeführt:

1. Stimmt die Anfrage mit der Liste global zugelassener Sites überein?
    a) Wenn ja, kann der Benutzer auf die angeforderte Website zugreifen.
    b) Wenn nicht, werden Websitelisten überprüft.
2. Stimmt die Anfrage mit der konfigurierten Websiteliste überein?
    a) Wenn ja, wird die Aktion durch folgende Sequenz festgelegt.
        i. Blockieren
        ii. Allow
    b) Wenn nicht, wird die Standardaktion (ZULASSEN) angewendet. Die Standardaktion kann nicht geändert werden.

Regeln für nicht genehmigte Websites konfigurieren

1. Klicken Sie in der Secure Private Access-Administratorkonsole auf **Einstellungen > Nicht genehmigte Websites**.

> **Hinweis:**
>
> - Die Webfilterfunktion ist standardmäßig aktiviert und der Zugriff auf alle nicht genehmigten Internet-URLs ist zulässig.
> - Sie können die Einstellung auf **Blockieren aller Benutzer am Zugriff auf nicht genehmigte Websites** ändern, um den Zugriff auf jede Internet-URL über den Citrix Enterprise Browser für alle Benutzer zu blockieren.



Sie können auch die Einstellungen für bestimmte URLs ändern, indem Sie sie zu blockierten oder erlaubten Websites hinzufügen.

Wenn Sie beispielsweise standardmäßig den Zugriff auf alle nicht sanktionierten URLs blockiert haben und den Zugriff auf nur einige bestimmte Internet-URLs zulassen möchten, können Sie dies tun, indem Sie die folgenden Schritte ausführen:

a) Klicken Sie auf den Tab **Zulässige Websites** und dann auf **Website zulassen**.

b) Fügen Sie die Adresse der Website hinzu, der der Zugriff gewährt werden muss. Sie können die Website-Adresse entweder manuell hinzufügen oder eine CSV-Datei mit der Website-Adresse per Drag-and-Drop ziehen.

c) Klicken **Sie auf URL hinzufügen** und dann auf **Speichern**.

   Die URL wird zur Liste der erlaubten Websites hinzugefügt.

Verwalten der Einstellungen nach der Installation

October 21, 2024

Routing von Anwendungsdomänen verwalten

Sie können eine Liste der Anwendungsdomänen anzeigen, die Ihrem Secure Private Access-Setup hinzugefügt wurden. In der Anwendungsdomänentabelle sind alle zugehörigen Domänen aufgeführt

und es wird angegeben, wie der App-Datenverkehr weitergeleitet wird (extern oder intern).

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

Administratoren verwalten

Sie können die Liste der Administratoren anzeigen und auch Administratoren von der Seite **Einstellungen > Administratoren** hinzufügen. Der Administrator, der Secure Private Access zum ersten Mal installiert, erhält die volle Berechtigung. Dieser Administrator kann dann weitere Administratoren zum Setup hinzufügen.

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

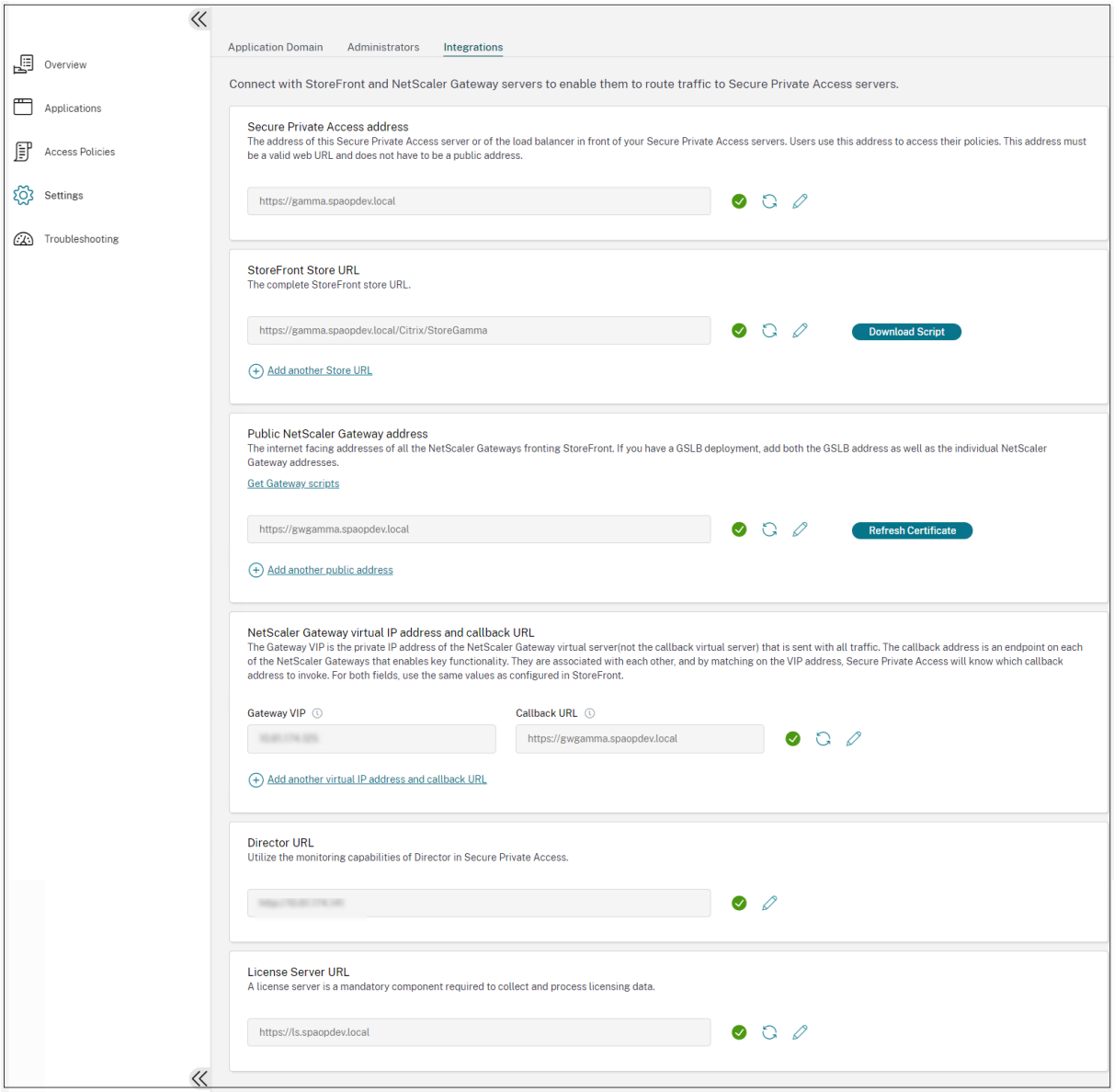
1. Klicken Sie auf der Seite **Administratoren** auf **Hinzufügen**.
2. Wählen Sie in **Domäne**die Domäne aus, zu der dieser Administrator hinzugefügt werden muss.
3. Wählen Sie unter **Benutzer oder Benutzergruppe**den Benutzer oder eine Gruppe aus, zu der dieser Benutzer gehört.
4. Wählen Sie unter **Administratortyp**den Berechtigungstyp aus, der diesem Benutzer zugewiesen werden muss.

Integrationseinstellungen ändern

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 Bearbeiten-Symbol neben der Einstellung, die Sie ändern möchten, und aktualisieren Sie den Eintrag.
3. Klicken Sie auf das Aktualisierungssymbol, um sicherzustellen, dass die Einstellungen gültig sind.

> **Hinweis:**
>
> - Wenn die Secure Private Access-Adresse geändert wird, laden Sie das StoreFront-Skript herunter und führen Sie es auf dem StoreFront-Host aus.
> - Wenn Secure Private Access auf einem anderen Computer als StoreFront installiert ist, laden Sie das StoreFront-Skript herunter und führen Sie es auf StoreFront aus.



Anwendungen und Richtlinien verwalten

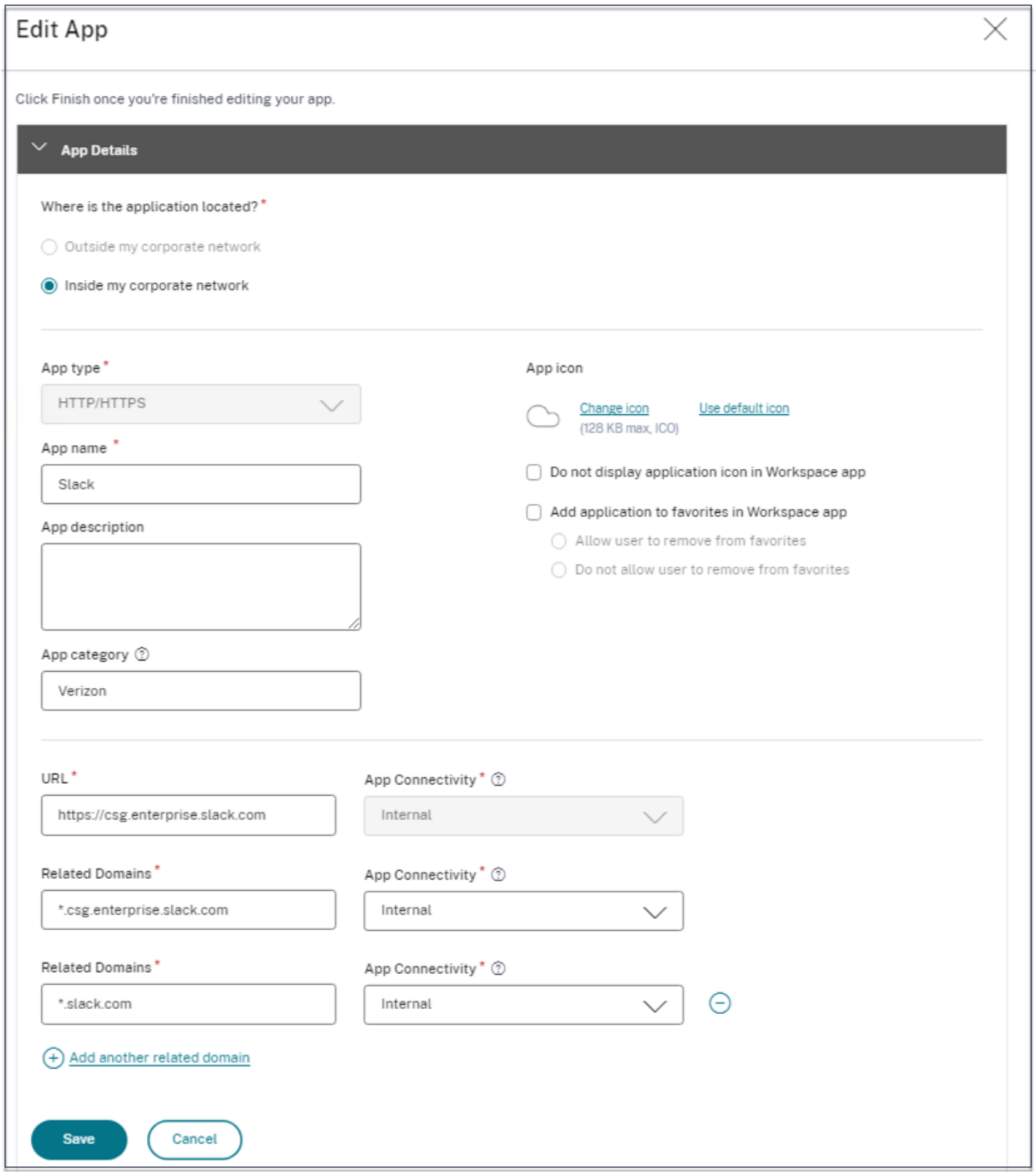
June 19, 2024

Nachdem Sie die Anwendungen und Zugriffsrichtlinien konfiguriert haben, können Sie sie bei Bedarf bearbeiten.

Eine Anwendung bearbeiten

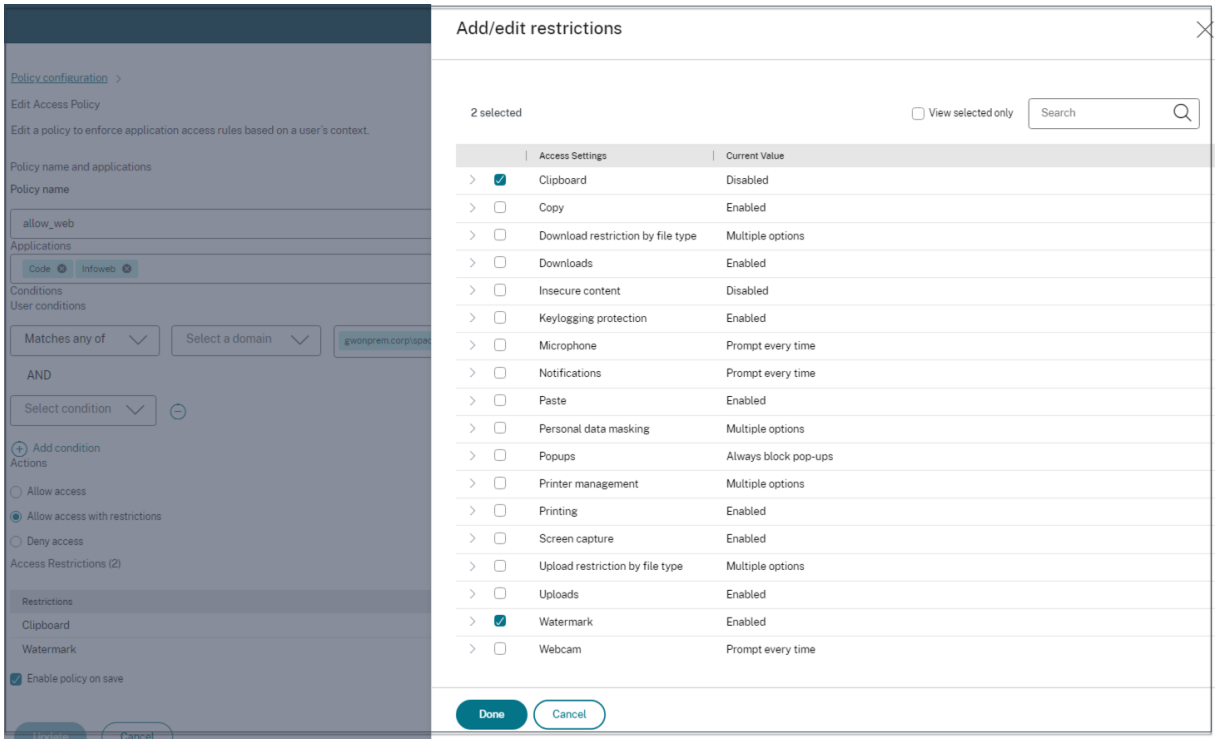
1. Klicken Sie in der Secure Private Access-Administrationskonsole auf **Anwendungen**.

2. Klicken Sie auf die Ellipsenschaltfläche neben der Anwendung, die Sie ändern möchten, und klicken Sie dann auf **Anwendung bearbeiten**.
3. Bearbeiten Sie die App-Details.
4. Klicken Sie auf **Speichern**.



Eine Zugriffsrichtlinie bearbeiten

1. Klicken Sie in der Secure Private Access-Administratorkonsole auf **Zugriffsrichtlinien**.
2. Klicken Sie auf die Ellipsenschaltfläche neben der Richtlinie, die Sie ändern möchten, und klicken Sie dann auf **Zugriffsrichtlinie bearbeiten**.
3. Bearbeiten Sie die Richtliniendetails.
4. Klicken Sie auf **Update**.



Deinstallieren Sie Secure Private Access

October 21, 2024

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

1. Wählen Sie **Citrix Virtual Apps and Desktops 7 2408 –Secure Private Access**.
2. Klicken Sie auf **Deinstallieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm und schließen Sie die Deinstallation ab.

> **Hinweis:**
>
> Wenn die Einrichtung von Secure Private Access nach der Installation abgeschlossen ist, laden

> Sie vor der Deinstallation von Secure Private Access die Datei StoreFrontScripts.zip von der Administratorkonsole herunter, um das Secure Private Access-Plug-In aus der StoreFront-Store-Konfiguration zu entfernen.

Um die StoreFrontScripts-ZIP-Datei herunterzuladen, folgen Sie diesen Schritten:

1. Melden Sie sich bei der Secure Private Access-Administratorkonsole an.
2. Klicken Sie auf **Einstellungen** und dann auf die Registerkarte **Integrationen** .
3. Klicken Sie im Abschnitt „StoreFront Store-URL“auf **Download-Skript** .

Entfernen Sie das Secure Private Access-Plugin aus der StoreFront-Storekonfiguration

Nachdem Sie Secure Private Access deinstalliert haben, müssen Sie das Secure Private Access-Plug-In aus der StoreFront-Storekonfiguration entfernen.

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
   ```

Überwachen und Problembehandlung

June 19, 2024

Das Secure Private Access **Troubleshooting** Dashboard zeigt die Protokolle zum Anwendungsstart, zur App-Enumeration und zu deren Status an. Einzelheiten finden Sie unter Dashboard-Übersicht.

Problembehandlung

Möglicherweise stoßen Sie während oder nach der Einrichtung von Secure Private Access auf Probleme im Zusammenhang mit den folgenden Themen:

- Fehler im Zertifikat
- Fehler bei der Datenbankerstellung
- StoreFront-Fehler

- Ausfall des öffentlichen Gateways/Callback-Gateways
- Secure Private Access Server ist nicht erreichbar

Einzelheiten zur Behebung dieser Probleme finden Sie unter Grundlegende Problembehandlung.

Sitzungsbezogene Codes in Director

Die Integration von Director in Secure Private Access ermöglicht eine effektive Leistungsüberwachung und Problembehandlung, da Probleme aus allen Komponenten einer Secure Private Access-Konfiguration in Director erfasst werden. Es wird empfohlen, die Fehler- oder Ausnahmeprobleme zu beheben, indem Sie die Protokolle überprüfen. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Support.

Referenzen

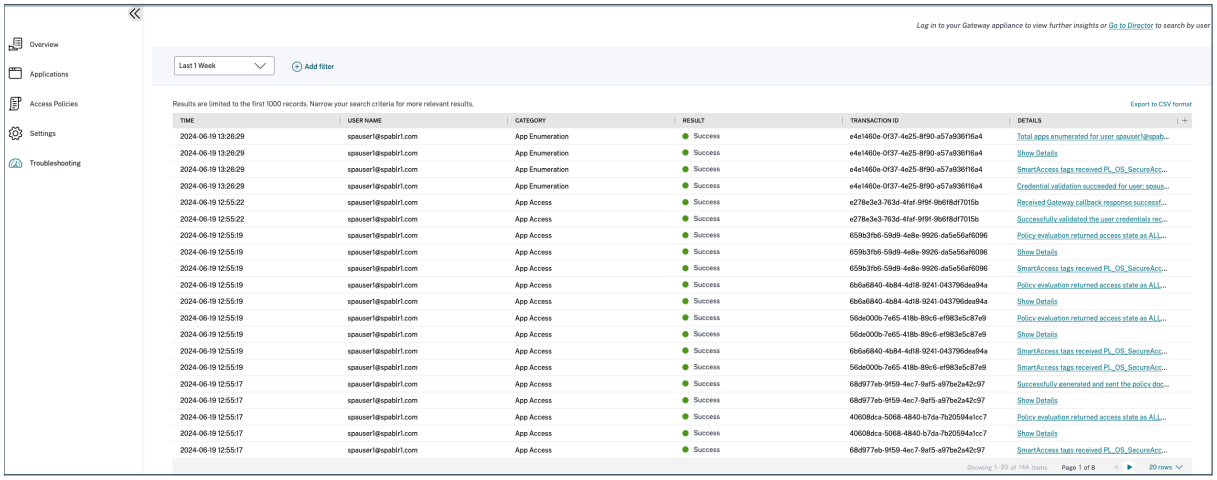
- Director mit Secure Private Access konfigurieren
- Eine Secure Private Access-Sitzung in Director anzeigen
- Liste der Secure Private Access-Sitzungscodes in Director.
- Director.

Dashboard-Übersicht

August 26, 2024

Das Dashboard zur Fehlerbehebung zeigt die Protokolle zum Anwendungsstart, zur App-Aufzählung und zum Status an. Sie können die Protokolle für die voreingestellte Zeit oder für eine benutzerdefinierte Zeitleiste anzeigen. Sie können die Option **Filter hinzufügen** verwenden, um Ihre Suche anhand der verschiedenen Kriterien wie App-Kategorie, Benutzername, Transaktions-ID zu verfeinern. In den Suchfeldern können Sie beispielsweise Transaction-ID, = (entspricht einem Wert) auswählen und in dieser Reihenfolge 7456c0fb-a60d-4bb9-a2a2-edab8340bb15 eingeben, um nach allen Logs zu suchen, die sich auf diese Transaktions-ID beziehen.

Sie können dem Diagramm Spalten hinzufügen, indem Sie auf das Pluszeichen klicken, je nachdem, welche Informationen Sie im Dashboard sehen möchten. Sie können die Benutzerprotokolle in das CSV-Format exportieren.



Sie können die folgenden Suchoperatoren verwenden, um Ihre Suche zu verfeinern, indem Sie die Option **Filter hinzufügen** verwenden:

- **= (entspricht einem bestimmten Wert)**: Um nach den Protokollen/Richtlinien zu suchen, die genau den Suchkriterien entsprechen.
- **! = (entspricht nicht einem bestimmten Wert)**: Um nach Protokollen/Richtlinien zu suchen, die die angegebenen Kriterien nicht enthalten.
- **~ (enthält einen Wert): Um nach den Protokollen/Richtlinien zu suchen, die den Suchkriterien teilweise**entsprechen.
- **! ~ (enthält keinen Wert)**: Um nach Protokollen/Richtlinien zu suchen, die einige der angegebenen Kriterien nicht enthalten.

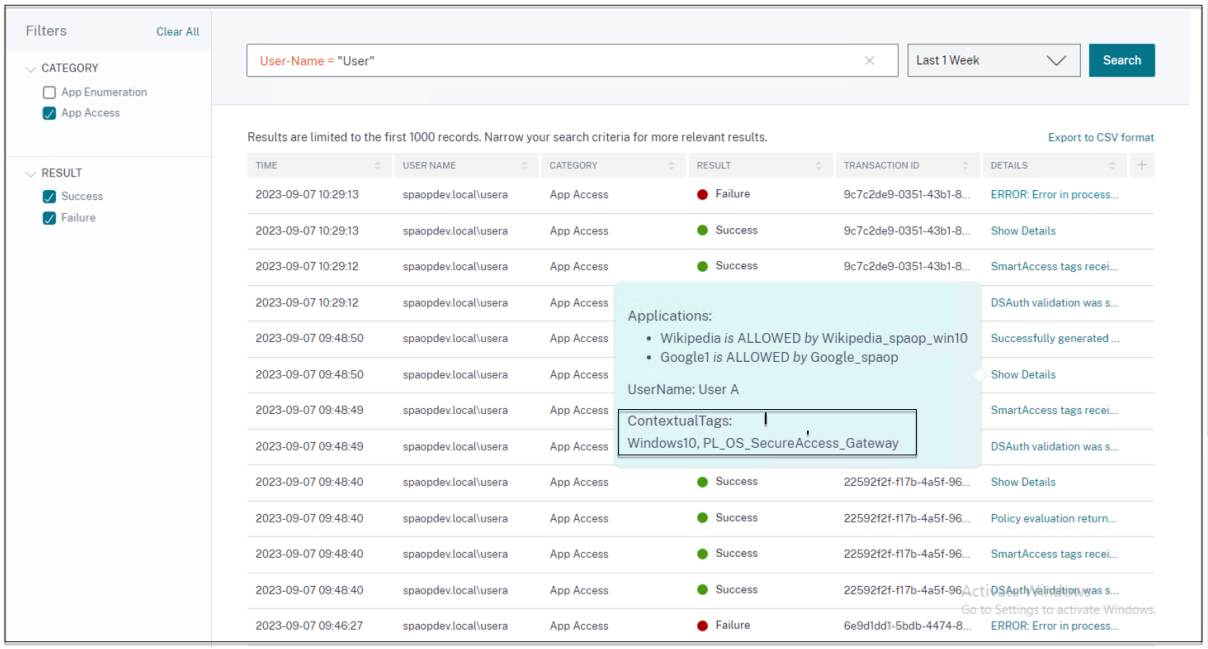
Sie können beispielsweise nach dem Ereignistyp “Enumeration”suchen, indem Sie im Suchfeld die Zeichenfolge **Event-Type > = (entspricht einem bestimmten Wert) > Enumeration** verwenden.

Verwenden Sie auf ähnliche Weise die Zeichenfolge **User-Name > ~ (enthält einen bestimmten Wert) > “operator”**, um nach Benutzern zu suchen, die teilweise den Begriff Operator enthalten. Diese Suche listet alle Benutzernamen auf, die den Begriff “operator”enthalten. Zum Beispiel “Local Operator”, “Admin Operator”.

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 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. Wenn die nFactor-Authentifizierung konfiguriert ist, werden die nFactor EPA-Aktionsnamen, die für die aktuellen Benutzer validiert werden, ebenfalls als Teil der kontextbezogenen Tags erfasst.



Grundlegende Problembehandlung

August 26, 2024

In diesem Thema sind einige der Fehler aufgeführt, auf die Sie während oder nach der Einrichtung von Secure Private Access stoßen könnten.

Fehler im Zertifikat

Fehler bei der Datenbankerstellung

StoreFront-Fehler

Ausfall des öffentlichen Gateways/Callback-Gateways

Secure Private Access Server ist nicht erreichbar

Fehler im Zertifikat

Fehlermeldung: Die Zertifikate konnten nicht automatisch von einem oder mehreren Gatewayservern abgerufen werden.

Diese Fehlermeldung wird angezeigt, wenn Sie versuchen, eine öffentliche NetScaler Gateway-Adresse hinzuzufügen, und beim Abrufen des Zertifikats ein Problem auftritt. Dieses Problem kann auftreten, wenn Secure Private Access eingerichtet oder die Einstellungen nach Abschluss der Einrichtung aktualisiert werden.

** Problemumgehung : Aktualisieren Sie das Gateway-Zertifikat auf dieselbe Weise 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.

  - 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

  Lösung:

  - 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.

  Lösung:

  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`>

  Lösung:

  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.

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. Dieses Skript muss auf allen StoreFront-Maschinen ausgeführt werden.

> **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.

  Lösung:

  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 dem Computer aus, auf dem die entsprechende StoreFront-Installation vorhanden ist. Dieses Skript muss auf allen StoreFront-Maschinen ausgeführt werden.

  > **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.

- **Fehlermeldung**: "Get-STFStoreService : Exception of type 'Citrix.DeliveryServices.Framework.Feature.Excep was thrown."beim Ausführen des StoreFront-Skripts mit PowerShell.

  Dieser Fehler tritt auf, wenn das StoreFront-Skript in einem x86-kompatiblen PowerShell-Fenster ausgeführt wird.

  Auflösung:

  Um das StoreFront PowerShell-Skript auszuführen, öffnen Sie das Windows x64-kompatible PowerShell-Fenster mit Administratorrechten und führen Sie dann `ConfigureStorefront.ps1` aus.

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>`

Lösung:

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

Lösung:

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.

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>
```

Fehler bei der Anwendungsaufzählung

Die Anwendungsaufzählung wird unterbrochen, wenn die StoreFront-URL oder die NetScaler Gateway-URL einen abschließenden Schrägstrich (/) enthält.

Auflösung:

Löschen Sie den abschließenden Schrägstrich in der StoreFront-Store-URL oder der NetScaler Gateway-URL. Einzelheiten finden Sie unter Aktualisieren von StoreFront- oder NetScaler Gateway-Serverdetails nach dem Setup.

Sonstiges

Die erstmalige Einrichtung kann nicht abgeschlossen werden

Sie können den Lizenzserver möglicherweise nicht neu konfigurieren, wenn die Director-Konfiguration bei der Erstinstallation fehlgeschlagen ist.

Auflösung:

Bereinigen Sie die Tabelle license_server manuell.

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>
  ```

SQL-Datenbankberechtigungen für Secure Private Access

Für die automatische Datenbankerstellung muss der Hostcomputer des Secure Private Access Plug-ins über die Berechtigungen verfügen, um eine Verbindung mit der Datenbank herzustellen und das 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>
```

2. Erstellen Sie ein SQL-Server-Login 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.

Protokollebene für Problembehandlungsprotokolle ändern

Problembehandlungsprotokolle sind die Standardstufe für Fehlerprotokolle.

Um die Protokollebene für die Problembehandlungsprotokolle zu ändern, aktualisieren Sie im Runtime Service appsettings.json (C:\Program Files\ Citrix\ Citrix Access Security\ Runtime\ RuntimeService) auf einen der folgenden `restrictedToMinimumLevel` Werte `TroubleshootingSql`:


```
-  Information
-  Debug
-  Warning
-  Error

"TroubleshootingSql": {

  "restrictedToMinimumLevel": "Error",
  "batchPostingLimit": 50,
  "batchPeriod": "00:00:05" // 5 seconds
 }
```

Fehlerbehebung bei Sitzungen mit Director

October 21, 2024

Die Integration von Director mit Secure Private Access ermöglicht eine effektive Leistungsüberwachung und Fehlerbehebung, da Probleme aller Komponenten in einer Secure Private Access-Konfiguration in Director erfasst werden. In den folgenden Tabellen sind die verschiedenen Fehlercodes und die damit verbundenen Bedingungen aufgeführt, die in Director angezeigt werden.

Weitere Informationen finden Sie in den folgenden Artikeln.

- Director mit Secure Private Access konfigurieren
- Anzeigen einer Secure Private Access-Sitzung in Director

> **Hinweis:**
>
> - Codes, die in der zweiten Ziffer eine „0“enthalten, stellen einen normalen Ausführungsfluss dar. Beispielsweise steht 1000 für eine erfolgreiche App-Enumeration.
> - Codes, die in der zweiten Ziffer eine „1“enthalten, stellen einen Fehler oder eine Ausnahme dar. Beispielsweise steht 2101 für einen Sitzungsfehler. Bei einem Fehler oder einer Ausnahme wird empfohlen, solche Probleme durch Untersuchen der Protokolle zu beheben. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Support.

Aufzählungsbezogene Codes

Code	Status	Beschreibung
1101	misserfolg	Während der Aufzählung ist ein interner Fehler aufgetreten.

Code	Status	Beschreibung
1102	misserfolg	Einige Apps wurden aufgelistet, aber die Bewertung von mindestens einer App ist fehlgeschlagen.
1103	misserfolg	Es wurden keine Apps aufgelistet und die Bewertung von mindestens einer App ist fehlgeschlagen.
1000	Erfolg	Die Aufzählung war erfolgreich. Mindestens eine App wurde aufgezählt.
1001	Erfolg	Es wurden keine Apps aufgelistet, da sie alle durch Richtlinien abgelehnt wurden.
1002	Erfolg	Es wurden keine Apps aufgelistet, da keine Richtlinien übereinstimmten.
1003	Erfolg	Es wurden keine Apps aufgelistet, da einige abgelehnt wurden und für andere keine Richtlinien übereinstimmten.
1004	Erfolg	Es wurden keine Apps aufgelistet, da keine Richtlinien zum Auswerten vorhanden sind.

Sitzungsbezogene Codes

Code	Status	Beschreibung
2101	Misserfolg	Sitzungsfehler.
2102	aktiv/inaktiv/Fehler	Die Sitzung ist aktiv oder beendet oder mindestens ein App-Start in der Sitzung ist fehlgeschlagen.
2000	Aktiv	Die Sitzung ist aktiv.

Code	Status	Beschreibung
2001	Inaktiv	Sitzung ist beendet/inaktiv.

Nachrichtencodes für die App-Aufzählung

Code	Status	Beschreibung
3101	Misserfolg	App-Aufzählung –Ein interner Fehler ist aufgetreten (derzeit nicht verwendet).
3102	Misserfolg	Die App wurde nicht aufgelistet, da bei der Richtlinienauswertung eine Ausnahme aufgetreten ist.
3103	Misserfolg	Der App-Aufzählungsstatus ist null –Während der Richtlinienauswertung ist ein interner Fehler aufgetreten.
3104	Zulassen/Ablehnen/Fehler	Fehler beim Abrufen der Richtliniendetails für die App.
3000	Zulassen	App-Aufzählung ist zulässig.
3001	Leugnen	Die App-Aufzählung wird durch die Richtlinie verweigert.
3002	Leugnen	Die App wurde nicht aufgelistet, da keine Richtlinien übereinstimmten.
3003	Unbekannt	Der App-Aufzählungsstatus ist unbekannt.
3004	App-Start von CEB	App-Startversuch vom Citrix Enterprise Browser aus.

Nachrichtencodes zum App-Start

Code	Status	Beschreibung
4101	Misserfolg	Fehler beim Starten der Anwendung –Beim Starten der Anwendung ist ein interner Fehler aufgetreten
4102	Misserfolg	Fehler beim Starten der Anwendung (intern)
4103	Zulassen/Ablehnen/Fehler	Fehler beim Abrufen der Richtliniendetails für die App
4000	Zulassen	App-Start ist erlaubt.
4001	Leugnen	Der Anwendungsstart wurde aufgrund einer Richtlinie verweigert.
4002	Leugnen	Der Start der Anwendung wurde verweigert, da keine Richtlinie übereinstimmte.

SIEM-Integration

August 26, 2024

Das Secure Private Access-Plug-In unterstützt die Integration mit SIEM-Diensten (Security Information and Event Management). Sicherheitsereignisse werden in Echtzeit im Windows-Ereignisprotokoll (Event Viewer\ Applications and Services Logs\ Citrix Access Security) gespeichert und können von Drittanbietertools erfasst und analysiert werden.

In der folgenden Tabelle sind die Sicherheitsereignisse des Secure Private Access Plug-Ins aufgeführt:

Ereignis-ID	Zusammenfassung	Beschreibung	Quelle
4624	Ein Konto wurde erfolgreich angemeldet	Ereignis, das erstellt wurde, als sich der Secure Private Access-Administrator an der Secure Private Access-Administratorkonsole anmeldete	Citrix Access Security-Verwaltungsdienst
4625	Ein Konto konnte sich nicht anmelden	Ereignis, das erstellt wurde, wenn sich der Secure Private Access-Administrator nicht an der Secure Private Access-Administratorkonsole anmelden konnte	Citrix Access Security-Verwaltungsdienst
4634	Ein Konto wurde abgemeldet	Ereignis, das erstellt wurde, als sich der Secure Private Access-Administrator von der Secure Private Access-Administratorkonsole abmeldete	Citrix Access Security-Verwaltungsdienst
4720	Ein Benutzerkonto wurde erstellt	Ereignis wurde erstellt, wenn ein neuer Secure Private Access-Administrator hinzugefügt wurde	Citrix Access Security-Verwaltungsdienst
4738	Ein Benutzerkonto wurde geändert	Ereignis wurde erstellt, als der neue Secure Private Access-Administrator aktualisiert wurde	Citrix Access Security-Verwaltungsdienst

Ereignis-ID	Zusammenfassung	Beschreibung	Quelle
4726	Ein Benutzerkonto wurde gelöscht	Ereignis wurde erstellt, als der neue Secure Private Access-Administrator entfernt wurde	Citrix Access Security-Verwaltungsdienst
8001	Sitzung mit sicherem Benutzerzugriff	Ereignis, das erstellt wird, wenn die Benutzersitzung auf dem Endpunkt initiiert oder beendet wurde. Enthält Benutzer-, Sitzungs- und Gerätedetails sowie besuchte interne und externe Domänen während der Sitzung	Citrix Access Security-Verwaltungsdienst
8002	Anfrage zur Autorisierung des Benutzerzugriffs	Ereignis, das erstellt wird, wenn das Secure Private Access-Plugin den Zugriff auf eine Ressource autorisiert. Enthält den Ressourcen-FQDN und die Autorisierungsentscheidung	Citrix Access Security-Verwaltungsdienst

Referenzen

- Integration von Sicherheitsinformationen und Ereignismanagement (SIEM)
- Über das Teilen von Protokollen mit SIEM-Lösungen

Scout-Integration

August 26, 2024

Citrix Scout ist in Secure Private Access integriert, sodass Administratoren Protokolle und Metriken zur Problembehandlung sammeln können. Informationen darüber, welche Informationen gesammelt werden, finden Sie unter Was wird gesammelt.

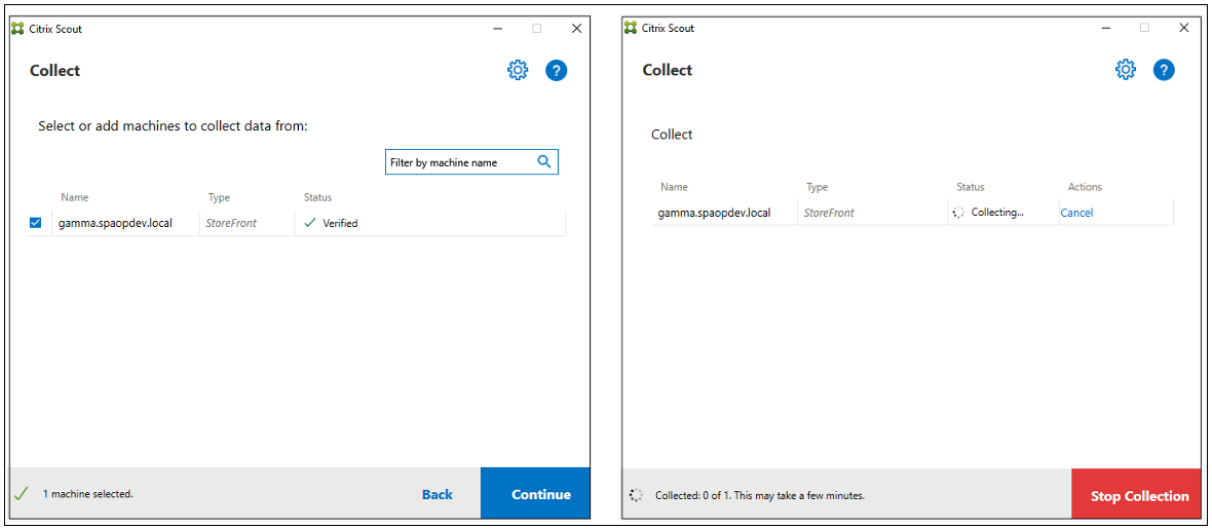
Gehen Sie wie folgt vor, um mit der Erfassung der Secure Private Access-Protokolle zu beginnen:

1. Wählen Sie einen Secure Private Access-Computer aus, um die Erfassung zu starten.
2. Klicken Sie auf **Weiter**.

Sie können jederzeit auf **Sammlung beenden** klicken, um die Erfassung zu beenden.

Citrix Scout ruft auch die folgenden Protokolle ab. Diese Protokolle werden in einem Paket auf dem lokalen Computer gespeichert und können in Citrix Cloud hochgeladen werden.

- C:\Program Files\Citrix\Citrix Access Security\Admin\AdminService\logs\spa-admin
- C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService\logs\spa-runtime



Einstellungen zur Aufbewahrung von Protokollen

June 19, 2024

Die Protokolle werden sieben Tage lang in der Secure Private Access-Datenbank gespeichert. Wenn die Gesamtzahl der Logs zu groß wird, beispielsweise über 100.000, können Sie die ältesten Logs vor 90 Tagen löschen. Die Bereinigungsaufgabe wird standardmäßig alle 12 Stunden ausgeführt. Der Job wird auch ausgeführt, wenn der Runtime-Dienst neu gestartet wird.

Anpassen der Aufbewahrungseinstellungen für Problembehandlungsprotokolle

Die Bereinigung der Protokolle ist über die Datei appsettings.json im Installationsordner des Runtime-Dienstes konfigurierbar. Sie können die Bereinigung auf der Grundlage des Alters der Protokolle und der Anzahl der Protokolle, die in der Datenbank gespeichert werden können, festlegen. Ändern Sie nach Bedarf die folgenden Einträge in der Datei appsettings.json:

Beispiel für eine appsettings.json-Datei:

```
1   "TroubleshootingLogs": {
2
3     "CleanupPeriodInHours": 12,
4     "CleanupDataOlderThanDays": 7,
5     "CleanupOldestDataIfEntriesCountAbove": 0
6    }
```

Um die Bereinigung zu deaktivieren, konfigurieren Sie die folgenden Einstellungen nach Bedarf:

- Um Protokolle nur 7 Tage lang aufzubewahren, setzen `CleanupDataOlderThanDays`Sie den Wert auf 7.
- Um die tageleitige Bereinigung zu deaktivieren, setzen `CleanupDataOlderThanDays`Sie den Wert auf 0.
- Um die zählbasierte Bereinigung zu deaktivieren, setzen `CleanupOldestDataIfEntriesCountAbove` Sie den Wert auf 0.
- Wenn beide Einstellungen auf 0 oder auf `CleanupPeriodInHours`0 gesetzt sind, werden die Protokolle für immer aufbewahrt.
  - Es wird nicht `CleanupDataOlderThanDays`empfohlen`CleanupOldestDataIfEntriesCour` , beide oder auf 0 oder auf 0 zu setzen`CleanupPeriodInHours`, da dies zu Problemen bei der Festplattennutzung von 100% führen kann.
  - Die Häufigkeit der Protokollbereinigung kann auch geändert werden, indem der `CleanupPeriodInHours`Eintrag geändert wird.

> **Hinweis:**
>
> Wenn Secure Private Access als Cluster bereitgestellt wird, müssen diese Einstellungen in jedem Clusterknoten geändert werden. Wenn die Knoteneinstellungen nicht übereinstimmen, hat die Instanz, die am häufigsten bereinigt wird, Vorrang.

Bereinigung von Protokollen und Telemetrie

June 19, 2024

Bereinigung von Telemetriedaten

Telemetriedaten werden 3 Monate lang in der Secure Private Access-Datenbank gespeichert. Die Prüfungen zur Identifizierung der Telemetriedaten, die bereinigt werden müssen, werden alle 30 Sekunden durchgeführt.

> **Hinweis:**
>
> Der Runtime-Dienst muss ausgeführt werden, um die Telemetriedatenbereinigung auszulösen.

Bereinigung von CDF-Protokollen

CDF-Protokolle werden auf dem Secure Private Access-Installationscomputer in den Installationsordnern für den Admin- und den Runtime-Dienst gespeichert. Die CDF-Protokolle werden in CSV-Dateien gespeichert, wobei für jede Datei eine Größenbeschränkung von 10 MB gilt.
Der Admin-Service kann bis zu 90 CDF-Protokolldateien gleichzeitig speichern. Danach löscht er die ältesten Dateien, um Speicherplatz für die neuen CDF-Protokolldateien freizugeben, die erstellt werden sollen.
Der Runtime-Dienst funktioniert genauso wie der Admin-Dienst, kann jedoch eine größere Anzahl von Dateien gleichzeitig speichern, bis zu 600.

Benutzerdefinierte Bereinigung von CDF-Protokollen

Die CDF-Protokollbereinigung kann über die appsettings.json-Dateien in den Installationsordnern der Admin- und Runtime-Dienste konfiguriert werden. Um die Dateigröße und das Zähllimit für die Dateien zu ändern, aktualisieren Sie die folgenden Einträge in der Datei appsettings.json:

```
"CdfFile": {

       "fileSizeLimitBytes": 10485760, // 10 MB
       "retainedFileCountLimit": 600
      }
```

> **Hinweis:**
>
> Wenn mehrere Instanzen von Secure Private Access für die Site eingerichtet sind, aktualisieren Sie die appsettings.json-Dateien für die CDF-Bereinigung auf jedem Secure Private Access-Installationscomputer.

Benachrichtigungen von Drittanbietern

December 27, 2023

Citrix Secure Private Access for on-premises