Citrix Secure Private Access — Vor Ort

Machine translated content

Disclaimer

Contents

Technische Übersicht

August 26, 2024

Citrix Secure Private Access für On-Premises ist eine vom Kunden verwaltete Zero Trust Network Access-(ZTNA)-Lösung, die VPN-freien Zugriff auf interne Web- und SaaS-Anwendungen mit den folgenden Funktionen sowie einer nahtlosen Endbenutzererfahrung bietet:

- Prinzip der geringsten Privilegien
- Single Sign-On (SSO)
- Multifaktorauthentifizierung
- Beurteilung des Gerätestatus
- Sicherheitskontrollen auf Anwendungsebene
- App Protection-Features

Die Lösung nutzt die on-premises StoreFront-App und die Citrix Workspace-App, um ein nahtloses und sicheres Zugriffserlebnis für den Zugriff auf Web- und SaaS-Apps innerhalb des Citrix Enterprise Browsers zu ermöglichen. Diese Lösung nutzt auch das 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 von StoreFront als einheitliches Zugangsportal für Web- und SaaS-Apps einfach Zero Trust Network Access für browserbasierte Apps (interne Web-Apps und SaaS-Apps) bereitzustellen, zusammen mit virtuellen Apps und Desktops als integriertem Bestandteil von Citrix Workspace.

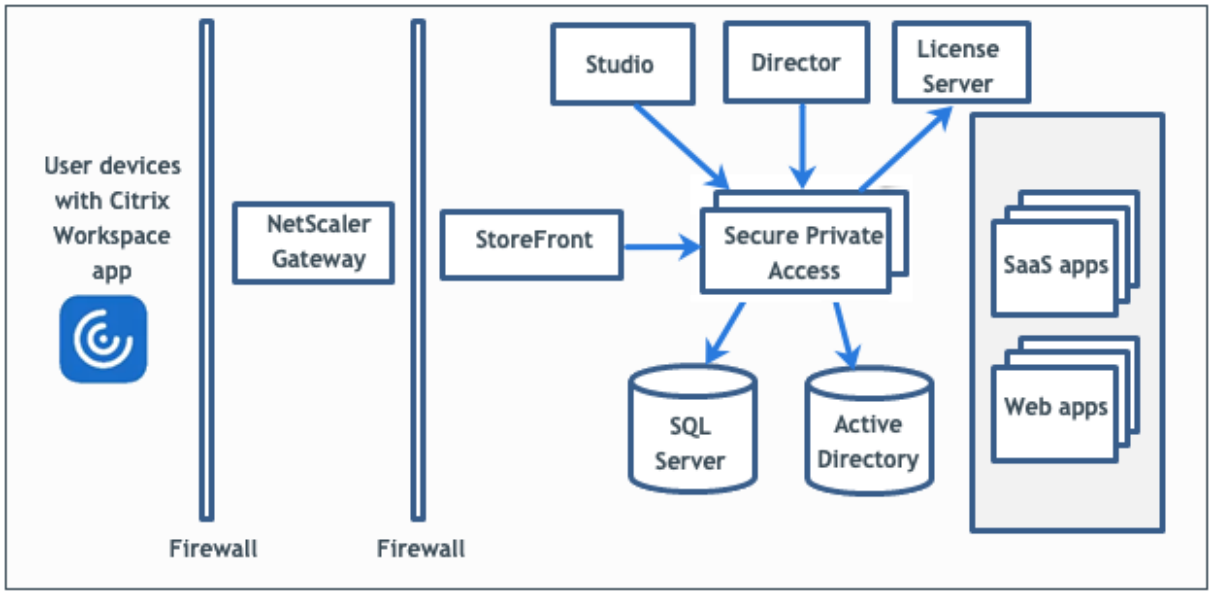
Citrix Secure Private Access kombiniert die Elemente von NetScaler Gateway und StoreFront, um Endbenutzern und Administratoren ein integriertes Erlebnis zu bieten.

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
Richtlinien zur Autorisierung	Secure Private Access

Funktionalität	Service/Komponente, die die Funktionalität bereitstellt
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

August 26, 2024

Juni 2024

Zusätzliche Zugriffsbeschränkungen für SaaS und interne Web-Apps

Zusätzliche Zugriffsbeschränkungen sind jetzt für SaaS und interne Web-Apps verfügbar. Administratoren können diese Einschränkungen über die Zugriffsrichtlinien durchsetzen. Einzelheiten finden Sie unter Verfügbare Zugriffsbeschränkungen.

Unterstützung für nicht genehmigte Websites

Der Zugriff auf nicht genehmigte Websites wird jetzt vom Secure Private Access Plug-In unterstützt. 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. Einzelheiten finden Sie unter Nicht genehmigte Websites.

Integration des Citrix Secure Private Access-Plug-Ins mit den SIEM-Diensten

Citrix Secure Private Access ist jetzt in das Security Information and Event Management (SIEM) integriert. Einzelheiten finden Sie unter SIEM-Integration.

Die Protokollebene zur Problembehandlung wurde von "Information"auf "Fehler"geändert

Die Protokollebene zur Problembehandlung wurde von "Information"auf "Fehler"geändert, um die Datenbanklast zu reduzieren. Einzelheiten zum Ändern der Protokollebene finden Sie unter Protokollebene für Problembehandlungsprotokolle ändern.

Behobene Probleme

August 26, 2024

Die folgenden Probleme wurden in Version 2402 behoben.

Konfiguration des Domänencontrollers

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

Verwaltung durch Administratoren

Die Änderungen der RBAC-Rolle des Administrators werden erst übernommen, wenn die aktuelle Sitzung ungültig wird (durch Abmelden oder Ablaufen des Tokens).

Start der Anwendung

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

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

Admin-Konsole

- Die Seite **App bearbeiten** wird nicht automatisch geschlossen, wenn die Seite **App bearbeiten** (**Secure Private Access > Anwendungen > Anwendung bearbeiten**) einer veröffentlichten Anwendung nicht geschlossen wird, nachdem ein verwandter Domäneeintrag geändert wurde.

  Zum Beispiel, wenn die verwandte Domäne, die Sie beim Erstellen einer App eingegeben haben, war `www.example.com`. Nachdem die App veröffentlicht wurde, ersetzen Sie die zugehörige Domäne `www.example.com` durch `abc.com` und klicken Sie 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 Routingdomänen-Tabelle (**Einstellungen > Anwendungsdomäne**) ohne das Präfix www gespeichert.

Upgrades

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

Bekannte Probleme

August 26, 2024

Die folgenden Probleme bestehen in Version 2402.

Domänencontroller-Konfigurationen

- Die unidirektionale oder bidirektionale Vertrauensstellung mit dem Vertrauenstyp “Gesamtstruktur“zwischen Domänen in verschiedenen AD-Gesamtstrukturen wird nicht unterstützt.

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

- Wenn sich die Domäne des Computers, auf der Secure Private Access for on-premises installiert ist, von der Domäne des Administrators unterscheidet, der bei Secure Private Access angemeldet ist, müssen Sie wie folgt vorgehen:

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

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

- Secure Private Access erfasst die Domain-Details in der Admin-Konsole oder im Dienst nicht. Daher hängt es vollständig von der Domain ab, die der Benutzer bereitgestellt hat. Wenn auf die entsprechende Domain nicht zugegriffen werden kann oder wenn der Domainname kein gültiger Name ist, wird diese Domain 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 Umschalten finden Sie unter Unterstützung für Smart Access-Tags.

RFWeb//Workspace für das Web

RFWeb/Workspace for Web wird nicht unterstützt und daher werden die Apps nicht aufgeführt. Einzelheiten finden Sie unter Bei Verwendung von StoreFront Version 2311 oder höher.

Start der Anwendung

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

StoreFront

- Unter **Stores > Unified Experience konfigurieren**muss der Standardempfänger für Website auf<StoreName>/Citrix/ Web konfiguriert sein. In früheren Versionen von StoreFront ist der Standardempfänger für Website auf einen leeren Wert festgelegt, der für Secure Private Access nicht funktioniert. Außerdem wird die frühere Version der Receiver-Benutzeroberfläche auf dem Client angezeigt. Informationen zur StoreFront-Konfiguration finden Sie unter StoreFront.
- Wenn Sie die StoreFront-Versionen 2308 oder früher verwenden, wird auf der Seite **Stores > Manage Delivery Controllers** der Secure Private Access Plug-In-Typ als **XenMobile** angezeigt. Dies hat keinen Einfluss auf die Funktionalität.

Protokollierung

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

Anzeige des Installationsprogramms auf der Seite Programm deinstallieren oder ändern

Wenn Sie Secure Private Access mithilfe der ISO-Datei von früheren Versionen auf 2405 aktualisieren, werden auf der Seite **Programm deinstallieren oder ändern** (**Systemsteuerung > Programme > Programme und Funktionen**) zwei Einträge für das Secure Private Access-Installationsprogramm angezeigt, anstatt den ursprünglichen Eintrag zu ersetzen.

Problemumgehung: Deinstallieren Sie das alte Build-Installationsprogramm.

> **Hinweis:**
>
> Dieses Problem tritt nicht auf, wenn das eigenständige Secure Private Access-Installationsprogramm mithilfe des Standalone-Installationsprogramms 2402 aktualisiert wird.

Upgrade

- Nachdem Sie ein Upgrade auf 2405 durchgeführt und eine vorhandene App bearbeitet haben, deren URL mit beginnt www, füllt das Feld **App Connectivity** den vorherigen Status nicht aus.

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.

- Nach dem Upgrade auf 2405 können Sie sich zwar an der Admin-Konsole anmelden, aber Sie können keine Anwendungen und Richtlinien verwalten. Es wird eine Fehlermeldung angezeigt.

  Problemumgehung: Sie müssen die Datenbank mithilfe der Skripts aktualisieren. Einzelheiten finden Sie unter Datenbank mithilfe von Skripten aktualisieren.

- Nach dem Upgrade auf 2405 schlagen die Anwendungsauflistung und der Anwendungsstart fehl.

  Problemumgehung: Sie müssen die Datenbank mithilfe der Skripts aktualisieren. Einzelheiten finden Sie unter Datenbank mithilfe von Skripten aktualisieren.

- Sie können das Secure Private Access-Plug-In nicht von Version 2402 auf 2405 aktualisieren, wenn das 2402-Plug-In mit dem Delivery Controller installiert wurde.

Systemanforderungen

August 26, 2024

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

- Citrix Workspace-App
  - Windows —2403 und höher
  - macOS —2402 und höher
- Betriebssystem für den Secure Private Access Plug-In-Server —Windows Server 2019 und höher
- StoreFront —LTSR 2203 oder CR 2212 und höher
- NetScaler —13.0, 13.1, 14.1 und höher. Für eine optimierte Leistung wird empfohlen, die neuesten Builds der NetScaler Gateway-Version 13.1 oder 14.1 zu verwenden.
- Director 2402 oder höher
- Kommunikationsports: Stellen Sie sicher, dass Sie die erforderlichen Ports für das Secure Private Access-Plug-In geöffnet haben. Einzelheiten finden Sie unter Kommunikationsports.

> **Hinweis:**
>
> Secure Private Access for on-premises wird in der Citrix Workspace-App für iOS und Android nicht unterstützt.

Voraussetzungen

Um ein vorhandenes NetScaler Gateway zu erstellen oder zu aktualisieren, stellen Sie 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 des Setups eingegeben werden müssen.
- Der Store auf StoreFront muss konfiguriert worden sein und die Store-Dienst-URL muss verfügbar sein. Das Format der Store-Dienst-URL ist `https://store.domain.com/Citrix/StoreSecureAccess`.
- NetScaler Gateway-IP-Adresse, FQDN und NetScaler Gateway-Rückruf-URL.
- IP-Adresse und FQDN der Hostmaschine des Secure Private Access-Plug-Ins (oder eines Load Balancers, wenn das Secure Private Access-Plug-In als Cluster bereitgestellt wird).
- Der Name des Authentifizierungsprofils wurde auf NetScaler konfiguriert.
- Auf NetScaler konfiguriertes SSL-Serverzertifikat.
- Domänename.
- Die Zertifikatskonfigurationen sind abgeschlossen. Administratoren müssen sicherstellen, dass die Zertifikatkonfigurationen vollständig sind. Das Secure Private Access-Installationsprogramm konfiguriert ein selbstsigniertes Zertifikat, wenn kein Zertifikat auf dem Computer 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 an das Administratorkonto

Die folgenden Administratorkonten sind für die Einrichtung von Secure Private Access erforderlich.

- 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 ein 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
Admin-Arbeitsstation	Plug-In für sicheren privaten Zugriff	HTTPS	4443	Secure Private Access-Plug-In — Admin-Konsole
Plug-In für sicheren privaten Zugriff	NTP-Dienst	TCP, UDP	123	Zeitsynchronisierung
	DNS-Dienst	TCP, UDP	53	DNS-Suche
	Active Directory	TCP, UDP	88	Kerberos
	Director	HTTP, HTTPS	80, 443	Kommunikation mit dem Director für Leistungsmanagement und verbesserte Problembehandlung
	Lizenzserver	TCP	8083	Kommunikation mit dem Lizenzserver zur Erfassung und Verarbeitung von Lizenzdaten
		TCP	389	LDAP über Klartext (LDAP)
		TCP	636	LDAP über SSL (LDAPS)
	Microsoft SQL Server	TCP	1433	Secure Private Access-Plug-In — Datenbankkommunikation
	StoreFront	HTTPS	443	Validierung der Authentifizierung
	NetScaler Gateway	HTTPS	443	NetScaler Gateway-Rückruf

Quelle	Ziel	Typ	Port	Details
StoreFront	NTP-Dienst	TCP, UDP	123	Zeitsynchronisierung
	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, mit dem Benutzer abgelaufene Kennwörter ändern können
	Plug-In für sicheren privaten Zugriff	HTTPS	443	Authentifizierung und Anwendungsaufzählung
	NetScaler Gateway	HTTPS	443	NetScaler Gateway-Rückruf
NetScaler Gateway	Plug-In für sicheren privaten Zugriff	HTTPS	443	Validierung der Anwendungsautorisierung
	StoreFront	HTTPS	443	Authentifizierung und Anwendungsaufzählung

Quelle	Ziel	Typ	Port	Details
	Webanwendungen	HTTP, HTTPS	80, 443	NetScaler Gateway-Kommunikation mit konfigurierten Secure Private Access-Anwendungen *(Ports können je nach Anwendungsanforderungen unterschiedlich sein*)
Benutzer-Gerät	NetScaler Gateway	HTTPS	443	Kommunikation zwischen Endbenutzergerät und NetScaler Gateway

Referenzen

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

Richtlinien zur Größenbestimmung

August 26, 2024

Anforderungen an den Datenbankspeicher

Der größte Teil des Datenbankspeichers wird von den Protokollen beansprucht. Der Speicherplatzverbrauch durch die Anwendungs- und Richtlinienkonfiguration ist im Vergleich zu den Protokollen vernachlässigbar.

Die folgende Abbildung zeigt die Serverspeicheranforderungen:

Number of users	Number of Secure Private Access server nodes	Secure Private Access node configuration			SQL Server (Secure Private Access Database only)			Active Directory		StoreFront	
		CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	CPU	Memory (GB)
1000	3	8	16	80	4	16	250	4	16	4	16
5000	8	8	16	80	16	16	750	16	16	4	16

Hinweis:

- Die Metriken werden auf der Grundlage der Annahme abgeleitet, dass die Protokollereignisbereinigung deaktiviert ist und die Protokollaufbewahrungsdauer auf 7 Tage festgelegt ist.
- Standardmäßig werden die Protokolle 90 Tage lang aufbewahrt, oder je nach den konfigurierten Einstellungen werden bis zu 100.000 Protokollereignisse aufbewahrt. Diese Einstellungen sind in der Datei appsettings.json des Secure Private Access Runtime Service verfügbar und können nach Bedarf geändert werden. Einzelheiten finden Sie unter Einstellungen zum Speichern von Ereignisprotokollen .

Serverkonfiguration

In der folgenden Tabelle werden die Serverkonfigurationsdetails angezeigt:

Konfiguration	Details
Gesamtzahl der Bewerbungen	250
Gesamtzahl der Richtlinien	50
Anzahl der Apps pro Benutzer	15
AD-Konfiguration	Benutzer sind Teil von 20 Gruppen mit bis zu 20 Verschachtelungsebenen
Problembehandlung bei der Protokollaufbewahrungsdauer	7 Tage (Standard)
Protokollebene zur Problembehandlung	Fehler (Standard)
Aufbewahrung von Secure Private Access-Serverprotokollen	90 Tage oder 600 Dateien

Verkehrsprofil

In der folgenden Tabelle werden die Details des Verkehrsprofils pro Tag und Benutzer angezeigt.

Profil	Details
Enumerationen	10
Synchronisierung der Unternehmensbrowserrichtlinien	20
App-Start über die Citrix Workspace-App	4
App-Zugriff über den Citrix Enterprise Browser	500
Helpdesk-Anfragen zur Problembehandlung (pro Tag) über Citrix Director	1000

Richtlinien für die Bereitstellung

Die folgende Tabelle zeigt die Anforderungen an die Datenbankgröße auf der Grundlage von Parametern wie Benutzersitzungen mit gleichzeitigem App-Zugriff, App-Enumeration pro Minute und CPUs, die von Secure Private Access verwendet werden:

Benutzersitzungen mit gleichzeitigem App-Zugriff	App-Aufzählung pro Minute	Secure Private Access-Speicher in GB	CPUs mit sicherem Privatzugriff	Speicherplatz in GB	Hinweise
< 20 (PoC-Zwecke)	2	4 GB	2	40 GB*	Für PoC-Zwecke kann SPA auf derselben Maschine wie StoreFront bereitgestellt werden, ohne dass die vorhandenen VM-Spezifikationen geändert werden.
20	5	8 GB	4	60 GB	-

Benutzersitzungen mit gleichzeitigem App-Zugriff	App-Aufzählung pro Minute	Secure Private Access-Speicher in GB	CPUs mit sicherem Privatzugriff	Speicherplatz in GB	Hinweise
160**	18	16 GB	4***	60 GB	Für eine bessere Leistung können 2 oder mehr SPA-Knoten bereitgestellt werden

Hinweis:

- * Der Speicher wird hauptsächlich von CDF-Protokollen verbraucht. Standardmäßig speichert Secure Private Access 600 Rollover-Protokolldateien, wobei jede Datei eine Größe von 10 MB hat. Wenn also sowohl der Secure Private Access-Administrator- als auch der Runtime-Dienst auf demselben Computer ausgeführt werden, beträgt die maximale Speichernutzung durch die Protokolle 12 GB. Außerdem kann SQL Express für PoC-Zwecke auf der lokalen VM installiert werden.
- ** Für dieses Lastprofil und höher wird empfohlen, Secure Private Access auf einem dedizierten Server bereitzustellen, anstatt gemeinsam mit StoreFront zu hosten, es sei denn, die NetScaler Gateway-Version ist niedriger als 13.0 oder kleiner als 13.1-48.47.
- *** Es wird empfohlen, mindestens 2 Secure Private Access-Knotencluster für solche Lasten zu verwenden, da einige bekannte Leistungsprobleme vorliegen. Diese Probleme sollen in den kommenden Versionen behoben werden.

Konfiguration anderer Komponenten

Komponente	vCPUs	Speicher
Plug-In für sicheren privaten Zugriff	8	16 GB
Secure Private Access SQL Server	8	16 GB
StoreFront	16	8 GB
Gateway	4	8 GB

Komponente	vCPUs	Speicher
Active Directory	8	14 GB
Client	4	8 GB

Installation

August 26, 2024

Das Secure Private Access-Installationsprogramm ist als eigenständiges Installationsprogramm oder als Teil des integrierten Citrix Virtual Apps and Desktops-Installationsprogramms verfügbar. Einzelheiten finden Sie unter Installieren von Kernkomponenten bzw. Installieren über die Befehlszeile.

Sobald die Installation abgeschlossen ist, wird die Admin-Konsole für die erstmalige Einrichtung automatisch im Standard-Browserfenster geöffnet. Sie können auf **Weiter** klicken, um Secure Private Access einzurichten. Sie können die Secure Private Access-Verknüpfung auch im Desktop-Startmenü sehen (**Citrix > Citrix Secure Private Access**).

Anforderungen an das Administratorkonto zur Installation und Verwaltung von Secure Private 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 ein lokaler Computeradministrator für den Computer ist, auf dem Secure Private Access installiert ist.
- Nach Abschluss der Einrichtung 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.

Secure Private Access einrichten

Sie können Secure Private Access einrichten, indem Sie die folgenden Schritte ausführen:

- Richten Sie Secure Private Access ein, indem Sie eine neue Site erstellen, oder richten Sie Secure Private Access ein, indem Sie einer vorhandenen Site beitreten

- Datenbanken konfigurieren
- StoreFront-, NetScaler Gateway-, Director- und Lizenzserver integrieren

Anwendungen und Zugriffsrichtlinien konfigurieren

Nachdem Sie die Secure Private Access-Umgebung eingerichtet haben, müssen Sie Anwendungen und Zugriffsrichtlinien für Anwendungen konfigurieren.

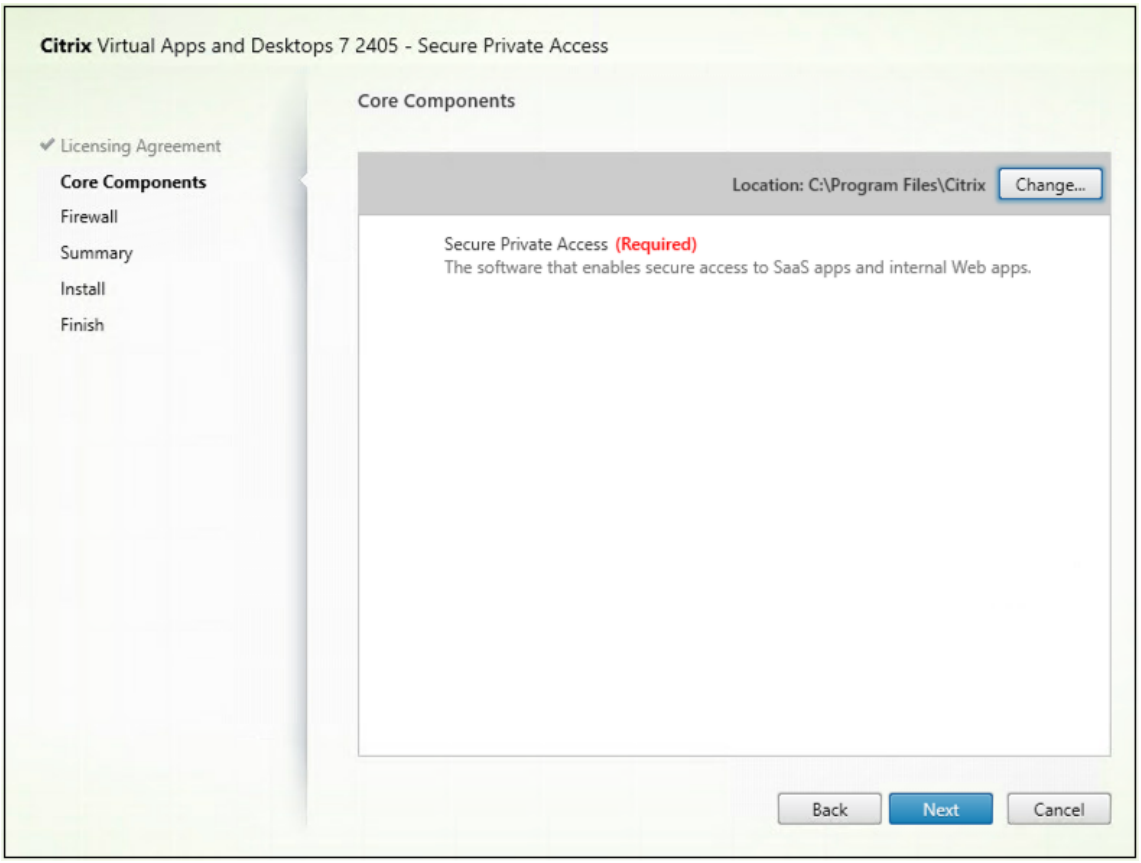
- Anwendungen konfigurieren
- Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen

Secure Private Access-Installationsprogramm

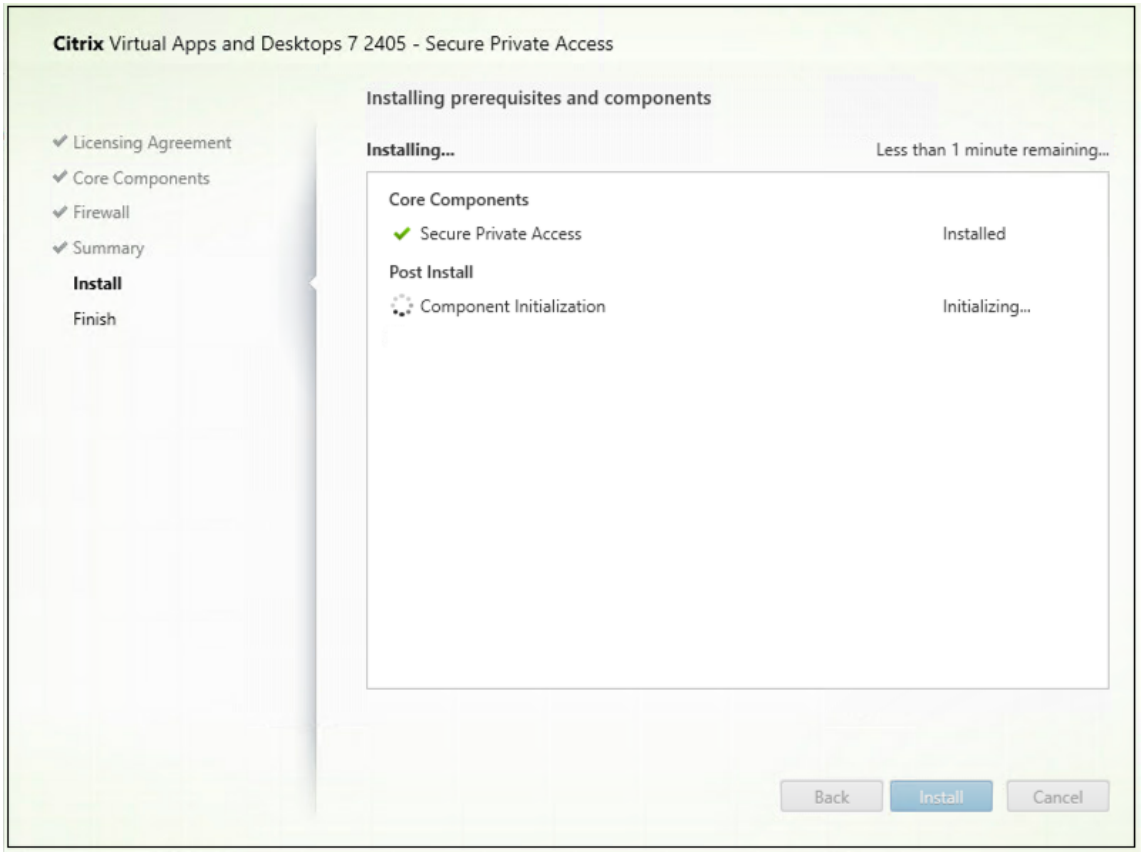
August 26, 2024

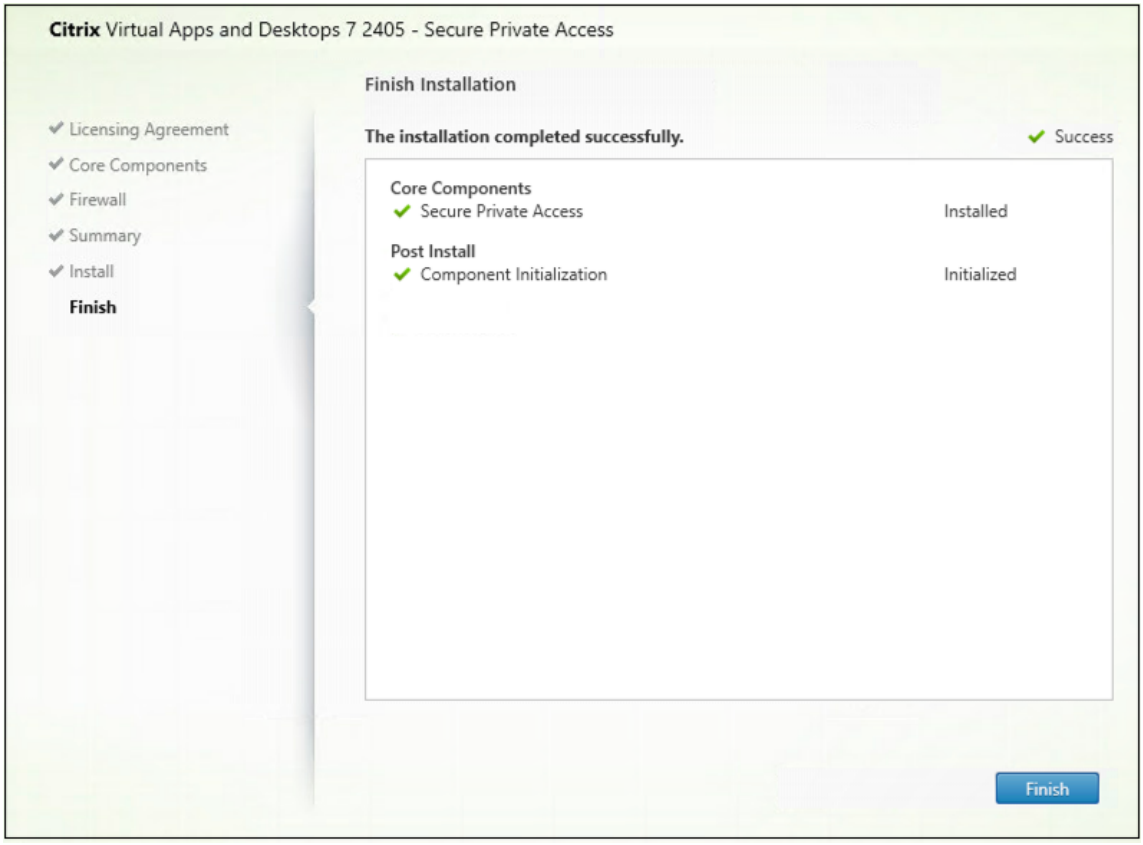
1. Laden Sie das Citrix Secure Private Access-Installationsprogramm von herunter https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/.
2. Führen Sie die EXE-Datei als Administrator auf einem Computer aus, der einer Domäne beigetreten ist.

   > **Hinweis:**
   >
   > Für POC-Zwecke wird empfohlen, Secure Private Access auf derselben Maschine zu installieren, auf der StoreFront installiert ist.

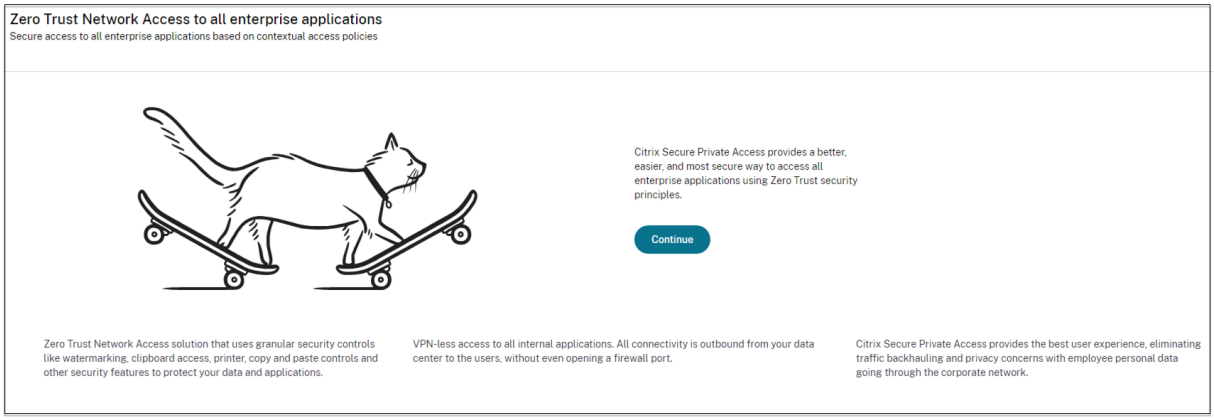


3. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen.

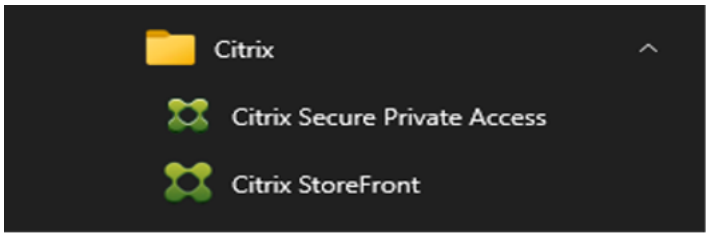




Sobald die Installation abgeschlossen ist, wird die Admin-Konsole für die erstmalige Einrichtung automatisch im Standard-Browserfenster geöffnet. Sie können auf **Weiter** klicken, um Secure Private Access einzurichten.



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



Weitere Informationen finden Sie in den folgenden Artikeln:

- Kernkomponenten installieren
- Installieren über die Befehlszeile

SSO zur Admin-Konsole

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

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

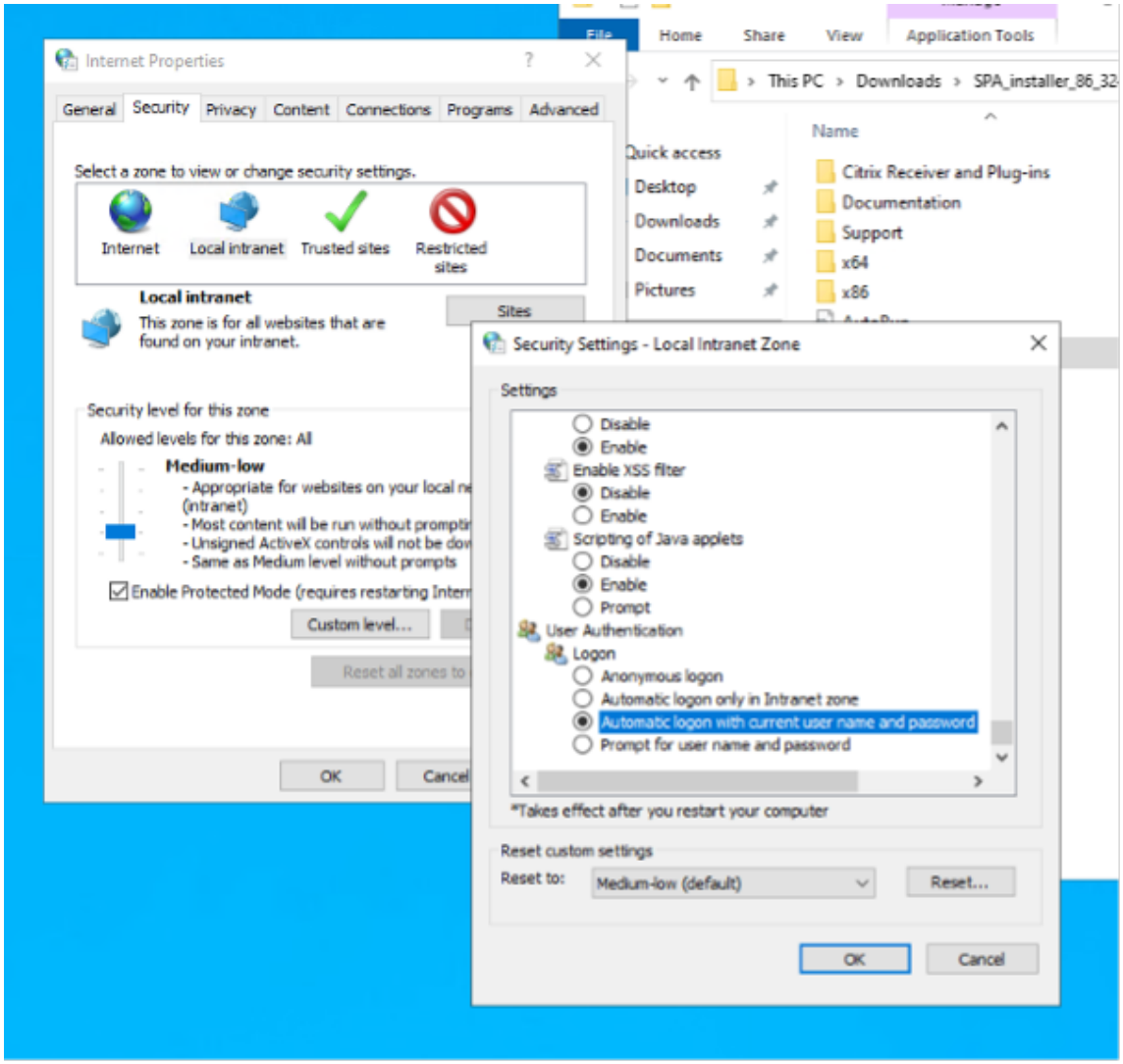
- Wenn Sie Ihre Anmeldeinformationen eingeben, aktivieren Sie die IWA-Anmeldung (Integrated Windows Authentication).
- Wenn Sie Ihre Anmeldeinformationen nicht eingeben, wird die Secure Private Access-Anmeldeseite angezeigt.

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

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

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

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



Hinweis:

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

Nächste Schritte

- Secure Private Access einrichten
- Konfigurieren von NetScaler Gateway

- Anwendungen konfigurieren
- Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen

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

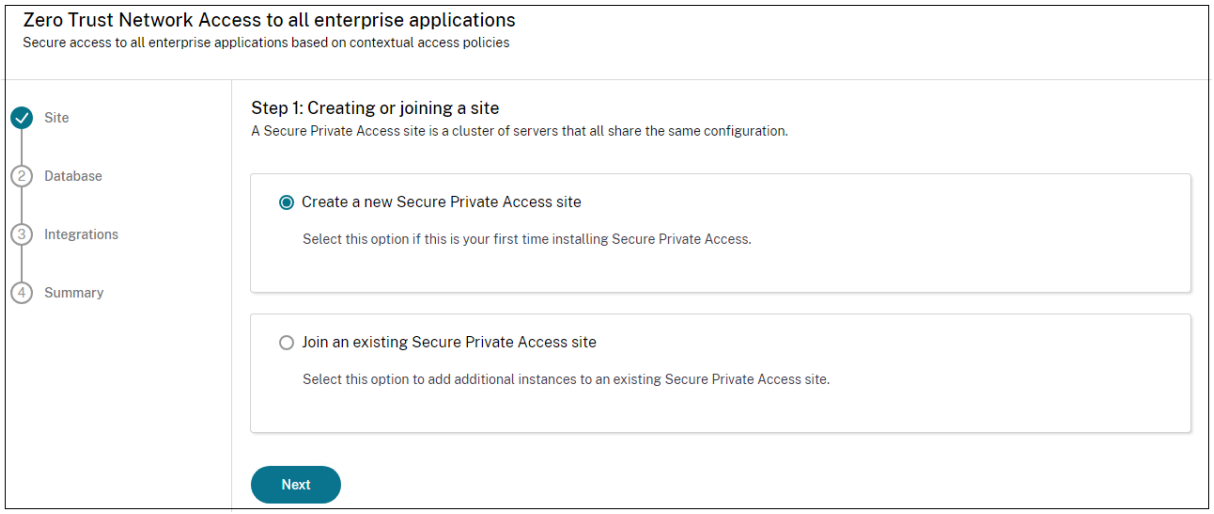
- Sie müssen sich bei der Secure Private Access-Administratorkonsole mit einem Domänenbenutzer anmelden, der auch ein lokaler Computeradministrator für den Computer ist, auf dem Secure Private Access installiert ist.
- Der SQL-Datenbankserver muss installiert werden, bevor eine Site erstellt wird.

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:

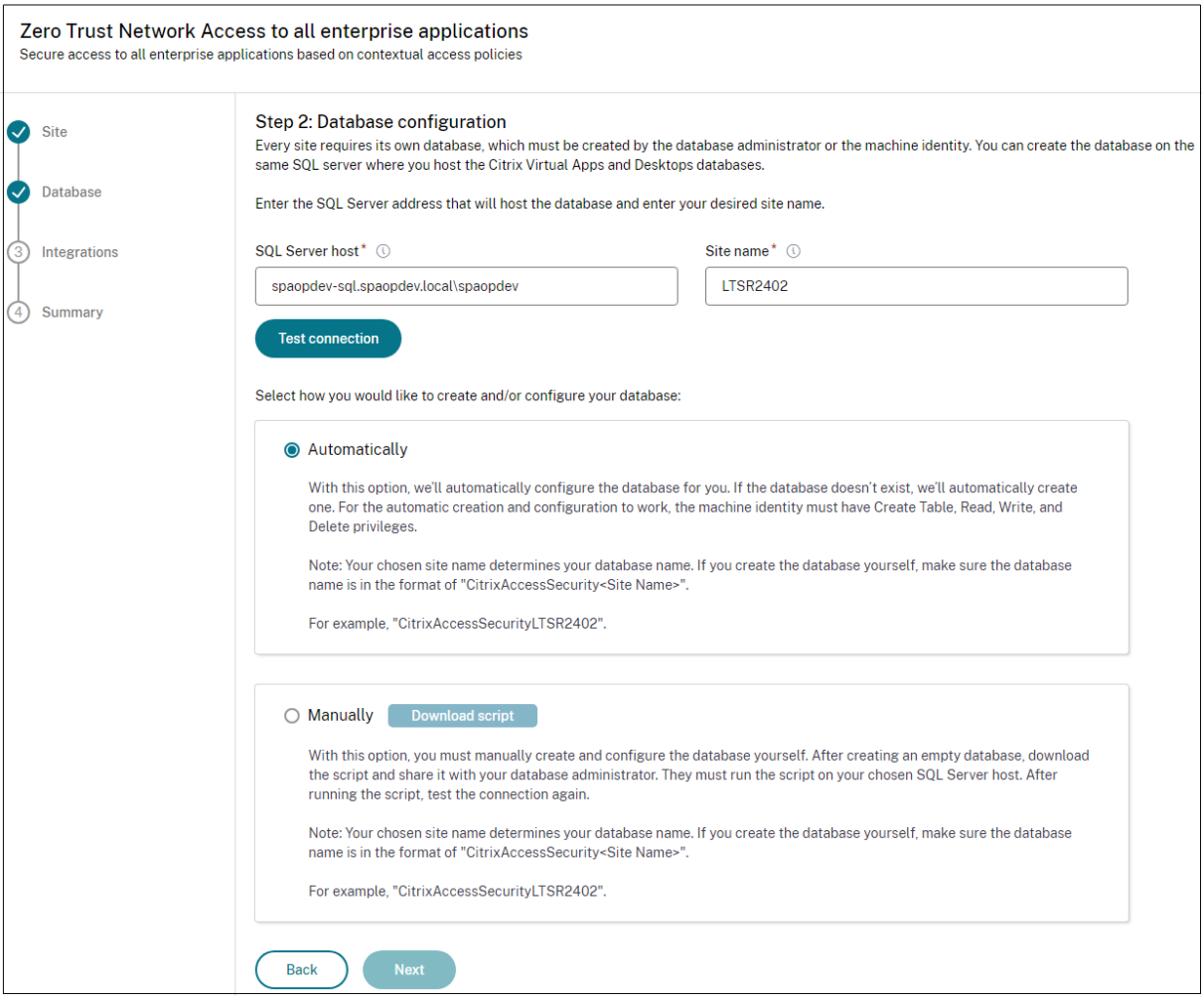
   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   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.

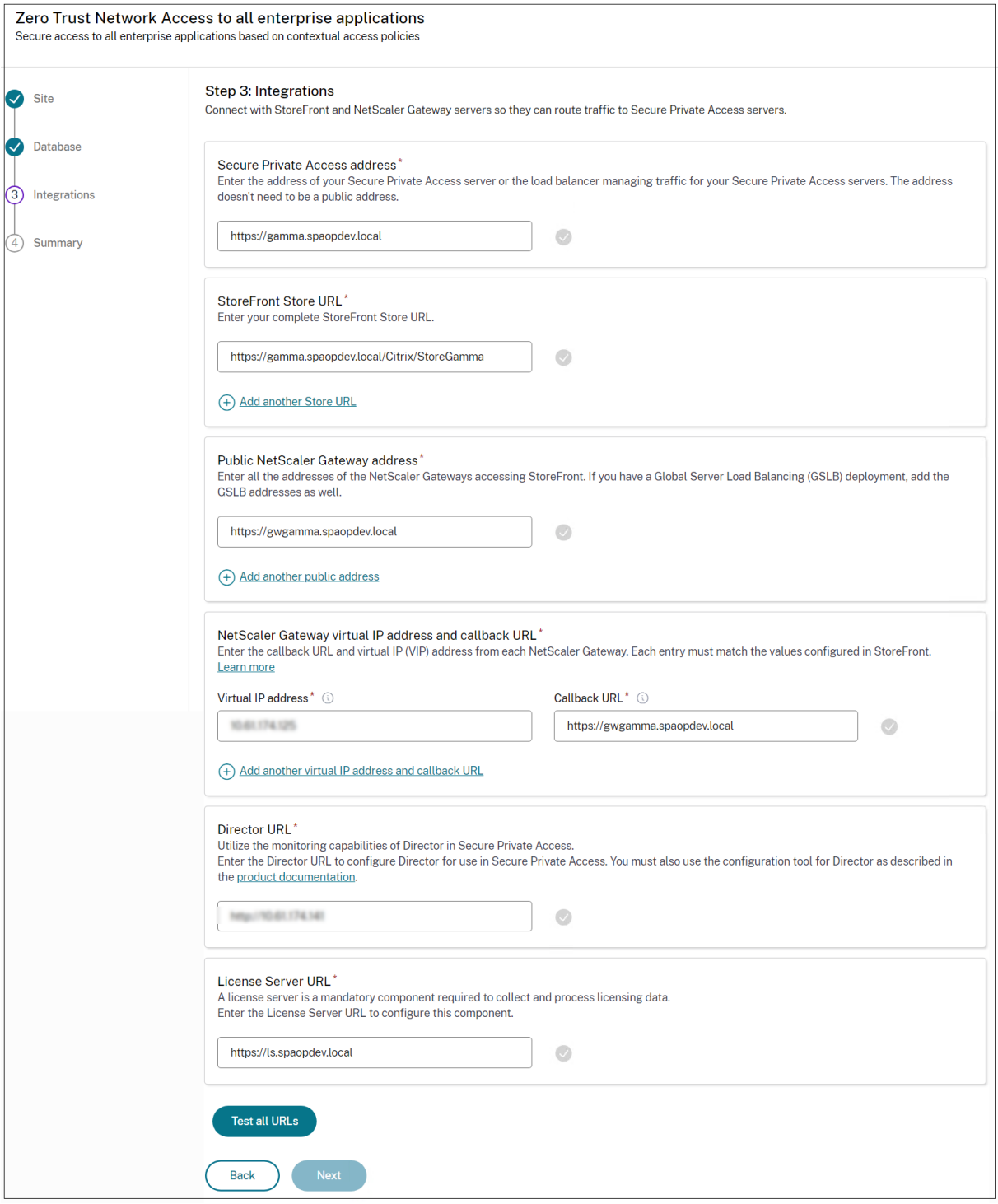
Bei der manuellen Konfiguration müssen Sie zuerst die Skripten herunterladen und dann die Skripten auf dem Datenbankserver ausführen, den Sie im Feld **SQL Server-Host** angegeben haben.

> **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**.

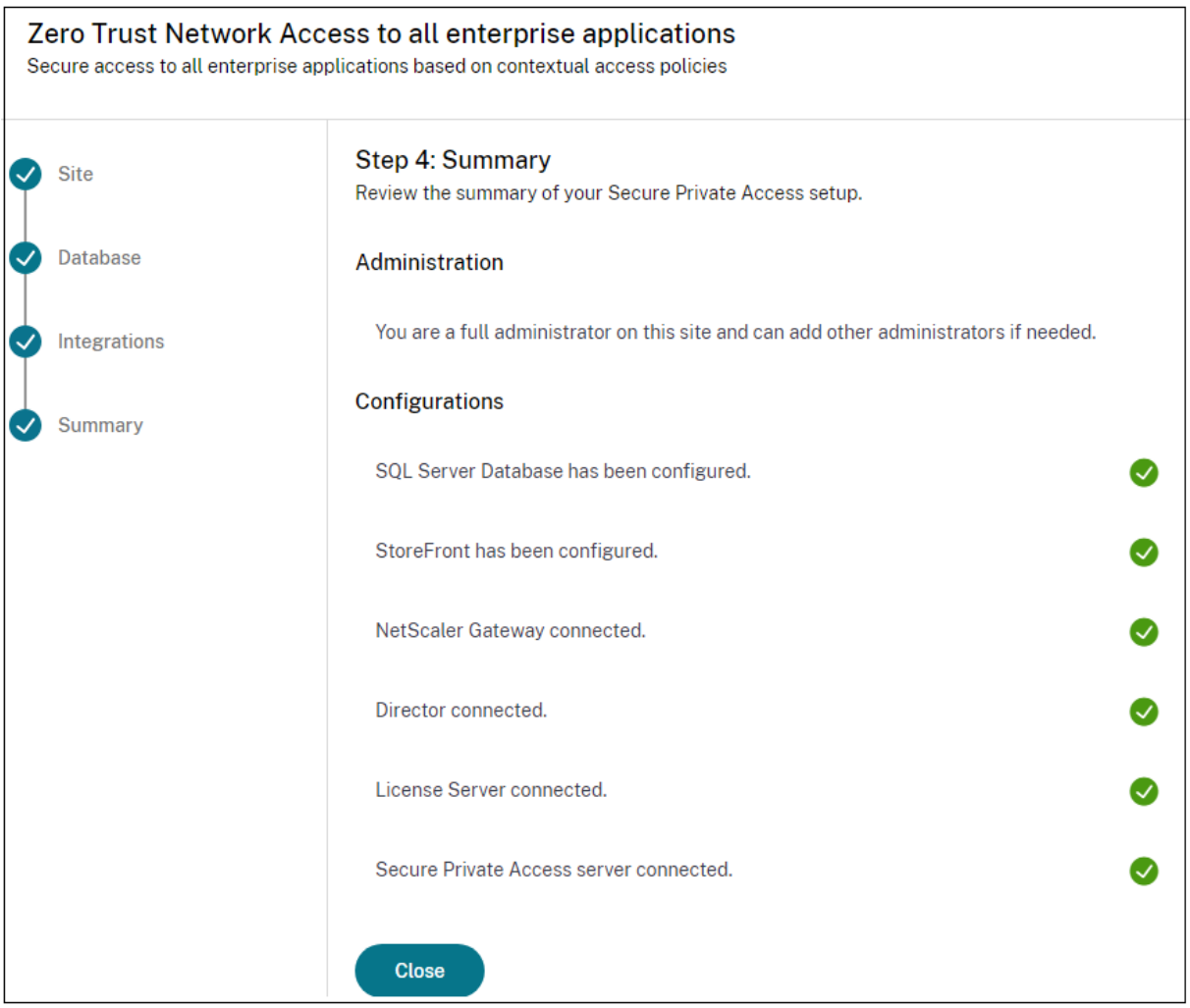


Schritt 4: Zusammenfassung der Konfiguration

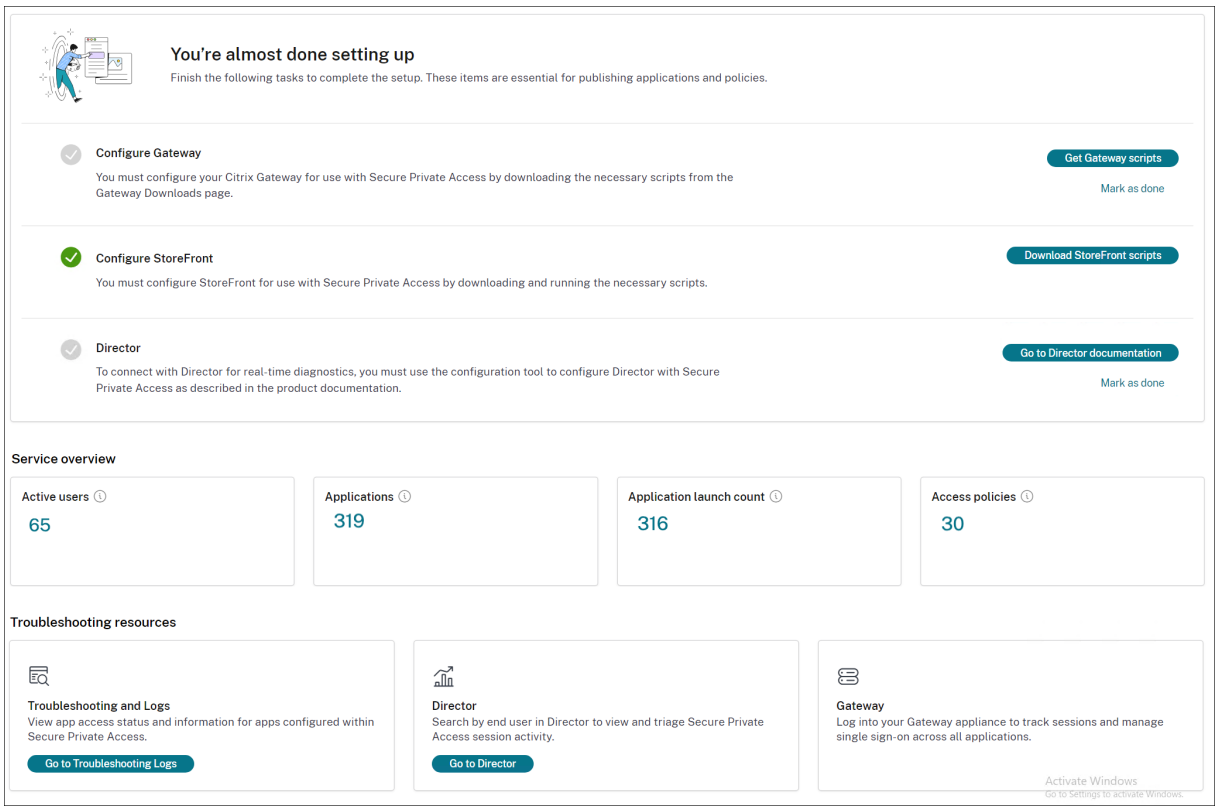
Nach Abschluss der Konfiguration erfolgt eine Überprüfung, um sicherzustellen, dass die konfigurierten Server erreichbar sind. Außerdem wird überprüft, ob der Secure Private Access-Server erreich-

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.



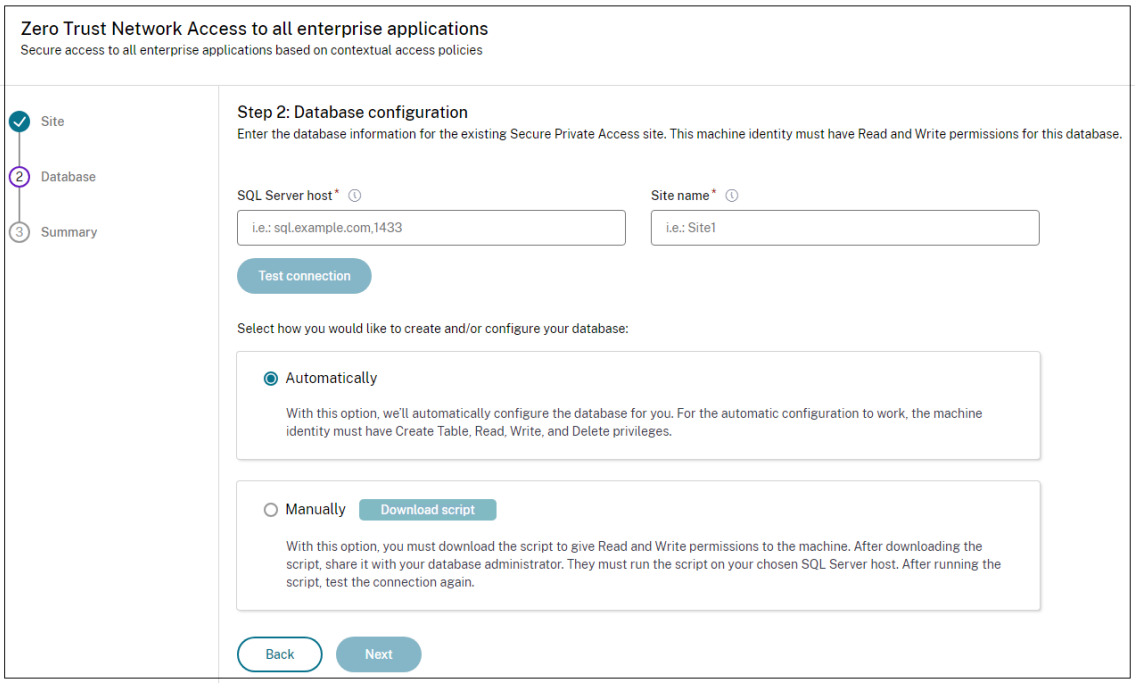
Hinweis:

- 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**.



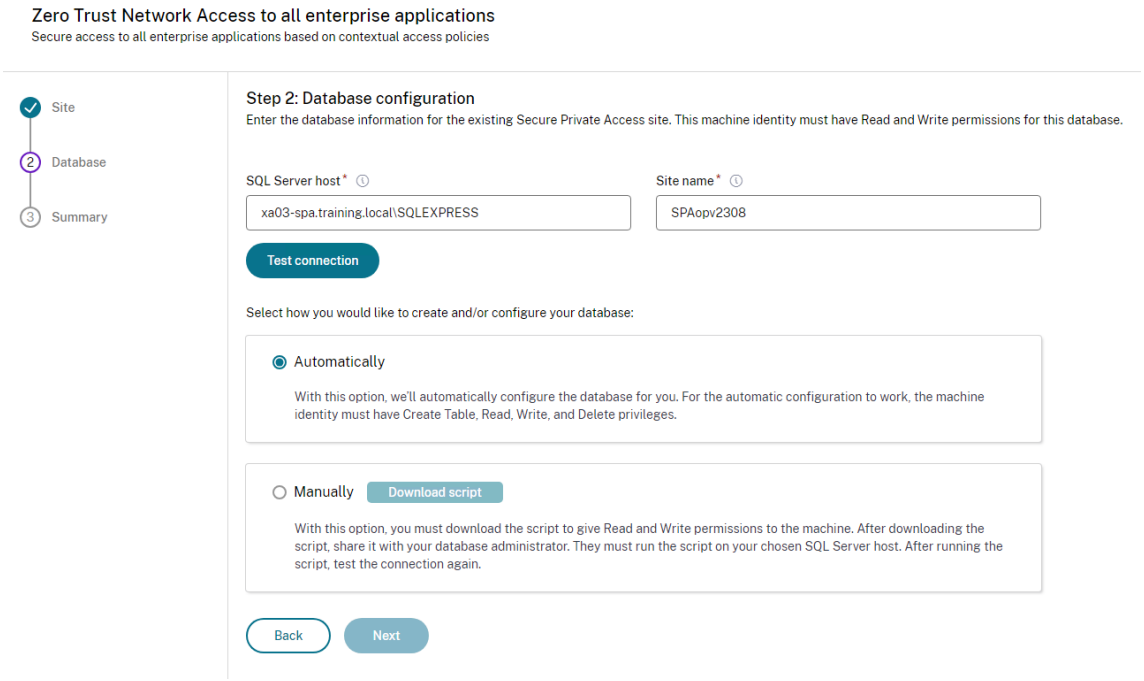
2. Geben Sie im Feld **SQL Server-Host** den Serverhostnamen ein. Stellen Sie sicher, dass eine Datenbank, die dem von Ihnen eingegebenen Site-Namen entspricht, bereits auf dem SQL-Server vorhanden ist, den Sie ausgewählt haben. Datenbankadressen können in einem der folgenden Formate angegeben werden:

   - 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

Komponenten

August 26, 2024

Im Folgenden sind die wichtigsten Komponenten einer typischen Secure Private Access-Bereitstellung für eine on-premises Bereitstellung aufgeführt.

- **StoreFront:** —StoreFront authentifiziert Benutzer und verwaltet Stores von 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 Anwendungsabonnements, Verknüpfungsnamen und andere Daten der Benutzer gespeichert. 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 Zugangspunkt über 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 Problembehandlung. 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 Secure Private Access-Integration mit Director.
- **Lizenzserver:** Der Lizenzserver sammelt und verarbeitet Lizenzdaten. Einzelheiten zur Integration des Lizenzservers mit Secure Private Access finden Sie unter Lizenzserverintegration mit Secure Private Access.
- **Web Studio:** Citrix Secure Private Access ist in die Web Studio-Konsole integriert, sodass Benutzer nahtlos über Web Studio auf den Dienst zugreifen können. Einzelheiten zur Secure Private Access-Integration mit Web Studio finden Sie unter Secure Private Access-Integration mit Web Studio.

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

NetScaler Gateway

August 26, 2024

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

1. Laden Sie das Skript von herunter https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.html.

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

   Verwenden Sie ns_gateway_secure_access_update.sh, um ein vorhandenes NetScaler Gateway zu aktualisieren.

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

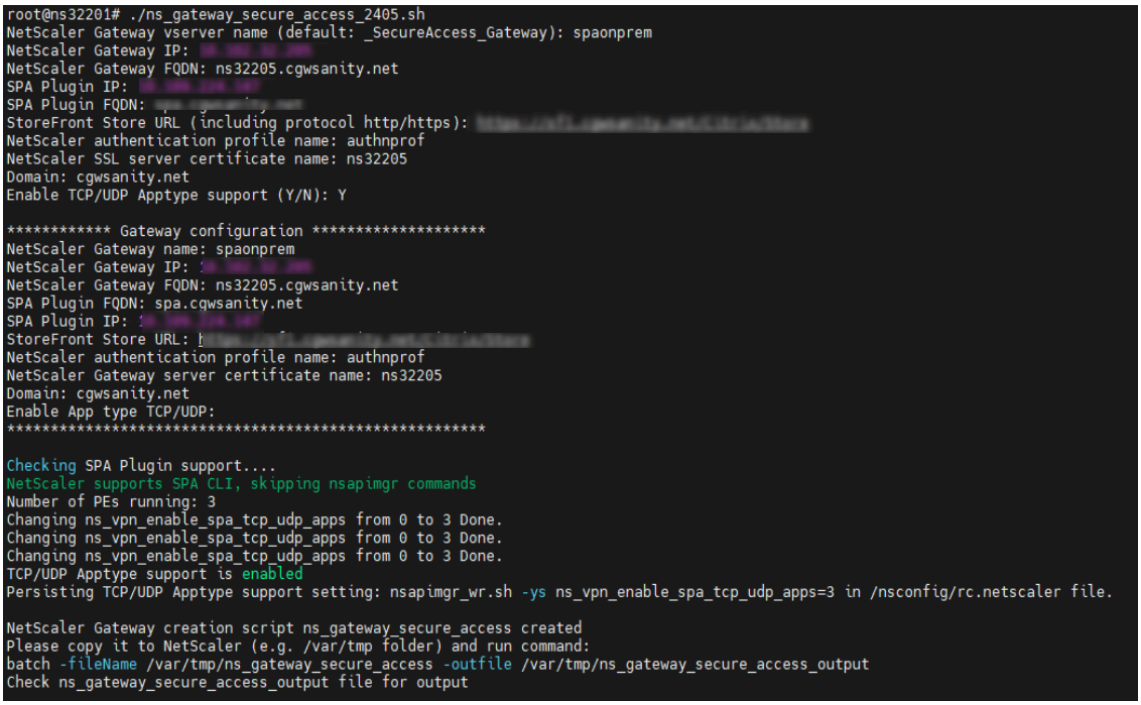
   Beispiel: *`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*

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

3. SSH zu NetScaler und wechseln Sie zur Shell (geben Sie ‘shell’in der NetScaler CLI ein).
4. Machen Sie das hochgeladene Skript ausführbar. Verwenden Sie dazu den Befehl chmod.

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

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

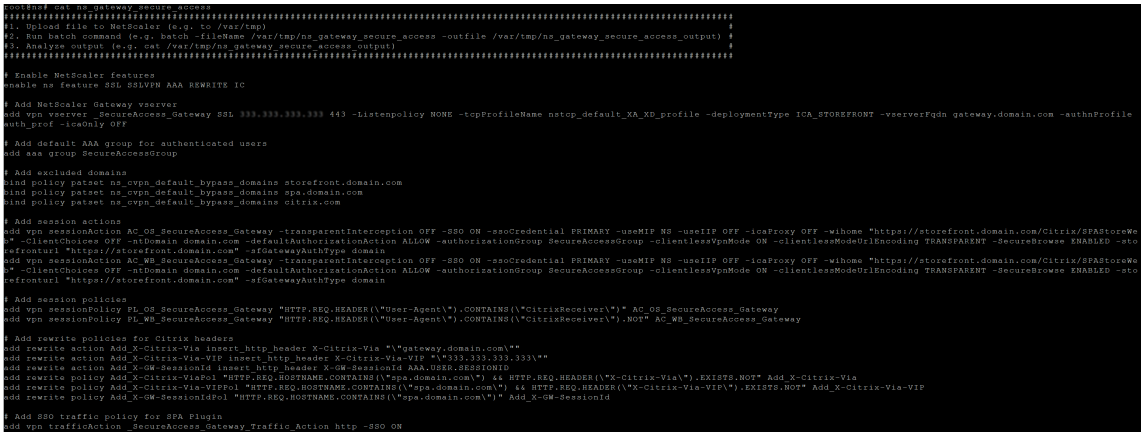


6. Geben Sie die erforderlichen Parameter ein. Eine Liste der Parameter finden Sie unter Voraussetzungen.

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

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

> **Hinweis:**
>
> Während der Skriptausführung wird die Kompatibilität des NetScaler- und Secure Private Access-Plug-Ins überprüft. Wenn NetScaler das Secure Private Access-Plug-In unterstützt, aktiviert das Skript die NetScaler-Funktionen zur Unterstützung von Smartaccess-Tags, das Senden von Verbesserungen und die Umleitung zu einer neuen Ablehnungsseite, wenn der Zugriff auf Ressourcen eingeschränkt ist. Einzelheiten zu Smarttags finden Sie unter Unterstützung für Smart Access-Tags.
>
> Die Funktionen des Secure Private Access-Plug-Ins, die in der Datei /nsconfig/rc.netscaler enthalten sind, ermöglichen es, sie auch nach dem Neustart von NetScaler aktiviert zu lassen.



7. 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. Schlägt ein Befehl fehl, 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.

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

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

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

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

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

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

Einstellungen auf dem virtuellen NetScaler Gateway-Server

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

Fügen Sie einen virtuellen Server hinzu:

- tcpProfileName: nstcp_default_XA_XD_profile
- deploymentType: ICA_STOREFRONT (nur mit dem Befehl `add vpn vserver` verfügbar)
- icaOnly: OFF

Aktualisieren Sie einen virtuellen Server:

- tcpProfileName: nstcp_default_XA_XD_profile
- icaOnly: OFF

Beispiele:

So fügen Sie einen virtuellen Server hinzu:

```
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
```


So aktualisieren Sie einen virtuellen Server:

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

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

NetScaler Gateway-Sitzungsaktionen

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

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

Beispiele:

So fügen Sie eine Sitzungsaktion hinzu:

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



```
storefronturl "https://storefront.mydomain.com"-sfGatewayAuthType
domain
```

So aktualisieren Sie eine Sitzungsaktion:

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

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

Kompatibilität mit den ICA-Apps

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

Einzelheiten finden Sie in den folgenden Themen:

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

Unterstützung für Smart Access-Tags

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

- 13.1-48.47 und höher
- 14.1—4.42 und höher

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

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

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

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

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

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


- Aktivieren Sie die Umleitung zur Seite "Zugriff eingeschränkt", wenn der Zugriff verweigert wird.

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

- Verwenden Sie die auf CDN gehostete Seite "Zugriffsbeschränkt".

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

- Führen Sie zum Deaktivieren 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-Plug-Ins auf NetScaler dauerhaft machen

Gehen Sie wie folgt vor, um die Einstellungen des Secure Private Access-Plug-Ins auf NetScaler beizubehalten:

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

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

   nsapimgr_wr.sh -ys call=toggle_vpn_redirect_to_access_restricted_page_on_d

   nsapimgr_wr.sh -ys call=toggle_vpn_use_cdn_for_access_restricted_page
   ```

3. Speichern Sie die Datei.

Die Einstellungen des Secure Private Access-Plug-Ins werden automatisch angewendet, wenn NetScaler neu gestartet wird.

Bekannte Einschränkungen

- Bestehendes NetScaler Gateway kann mit einem Skript aktualisiert werden, es kann jedoch eine unendliche Anzahl möglicher NetScaler-Konfigurationen geben, die nicht durch ein einziges Skript abgedeckt werden können.

- Verwenden Sie keinen ICA-Proxy auf NetScaler Gateway. Diese Funktion ist deaktiviert, wenn NetScaler Gateway konfiguriert ist.
- Wenn Sie NetScaler verwenden, das in der Cloud bereitgestellt wird, müssen Sie einige Änderungen im Netzwerk vornehmen. Erlauben Sie beispielsweise die Kommunikation zwischen NetScaler und anderen Komponenten an bestimmten Ports.
- Wenn Sie SSO auf NetScaler Gateway aktivieren, stellen Sie sicher, dass NetScaler über eine private IP-Adresse mit StoreFront kommuniziert. Möglicherweise müssen Sie NetScaler einen neuen StoreFront-DNS-Eintrag mit einer privaten StoreFront-IP-Adresse hinzufügen.

Laden Sie das öffentliche Gateway-Zertifikat hoch

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.

Gehen Sie wie folgt vor, um ein Public-Gateway-Zertifikat hochzuladen:

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

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

Kontexttags konfigurieren

August 26, 2024

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

Administratoren können der Zugriffsrichtlinie Bedingungen mit kontextbezogenen Tags hinzufügen. Das Kontext-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 Secure Private Access-Plug-In kann Smart Access-Tags als Header (neue Logik) oder durch Rückrufe an Gateway empfangen. Einzelheiten finden Sie unter Smart Access-Tags .

> **Hinweis:**
>
> Das Secure Private Access Plug-In unterstützt nur klassische Gateway-Vorauthentifizierungsrichtlinien, die auf NetScaler Gateway konfiguriert werden können.

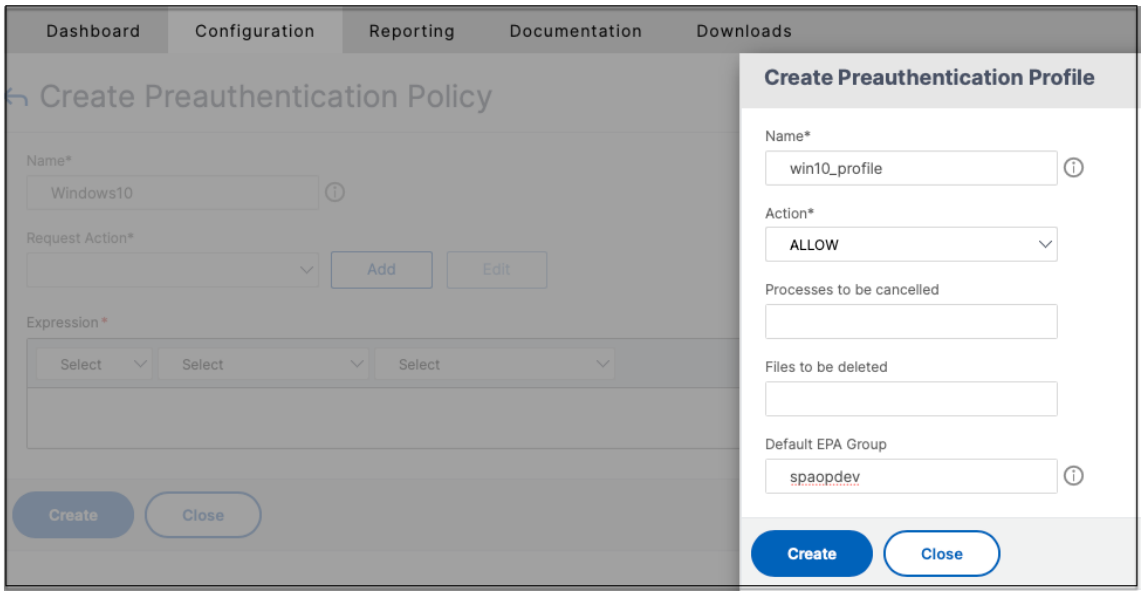
Konfigurieren Sie benutzerdefinierte Tags mit der GUI

Die folgenden allgemeinen Schritte sind für die Konfiguration von kontextbezogenen Tags erforderlich.

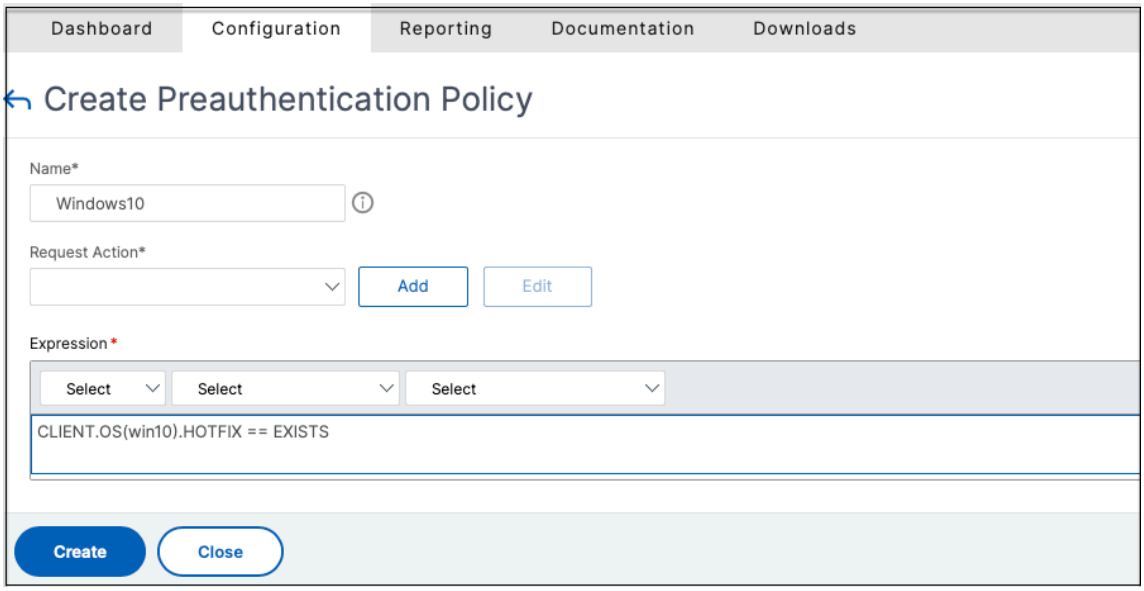
1. Konfigurieren Sie eine klassische Gateway-Vorauthentifizierungsrichtlinie
2. Binden Sie die klassische Vorauthentifizierungsrichtlinie an den virtuellen Gateway-Server

Konfigurieren Sie eine klassische Gateway-Vorauthentifizierungsrichtlinie

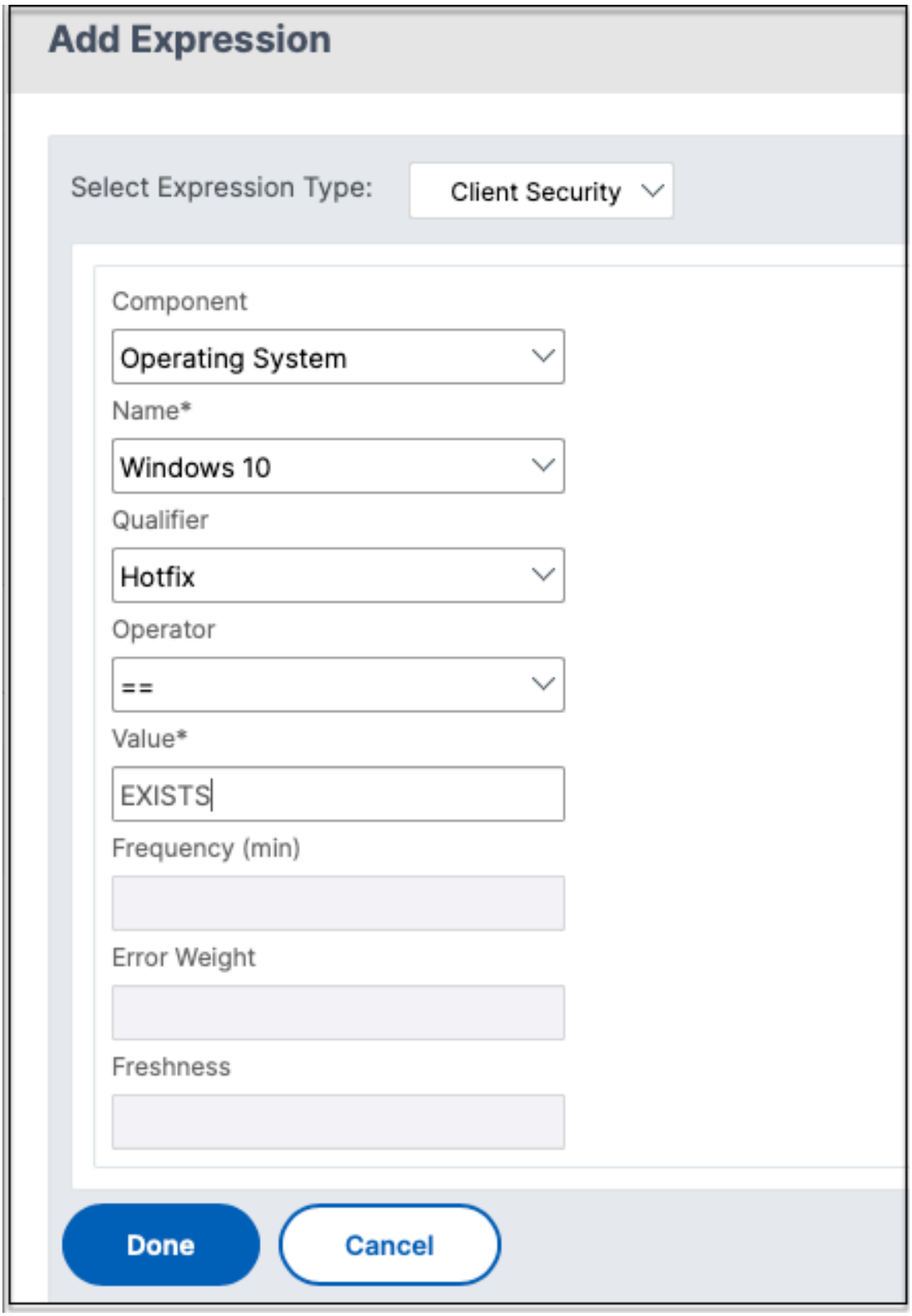
1. Navigieren Sie zu **NetScaler Gateway > Richtlinien > Vorauthentifizierung** und klicken Sie dann auf **Hinzufügen**.
2. Wählen Sie eine vorhandene Richtlinie aus oder fügen Sie einen Namen für die Richtlinie hinzu. Dieser Richtlinienname wird als benutzerdefinierter Tag-Wert verwendet.
3. Klicken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



4. Füllen Sie die erforderlichen Felder aus und klicken Sie auf **Erstellen**.
5. Geben Sie im Feld **Ausdruck** den Ausdruck manuell ein, oder verwenden Sie den Ausdrucksedditor, um einen Ausdruck für die Richtlinie zu erstellen.



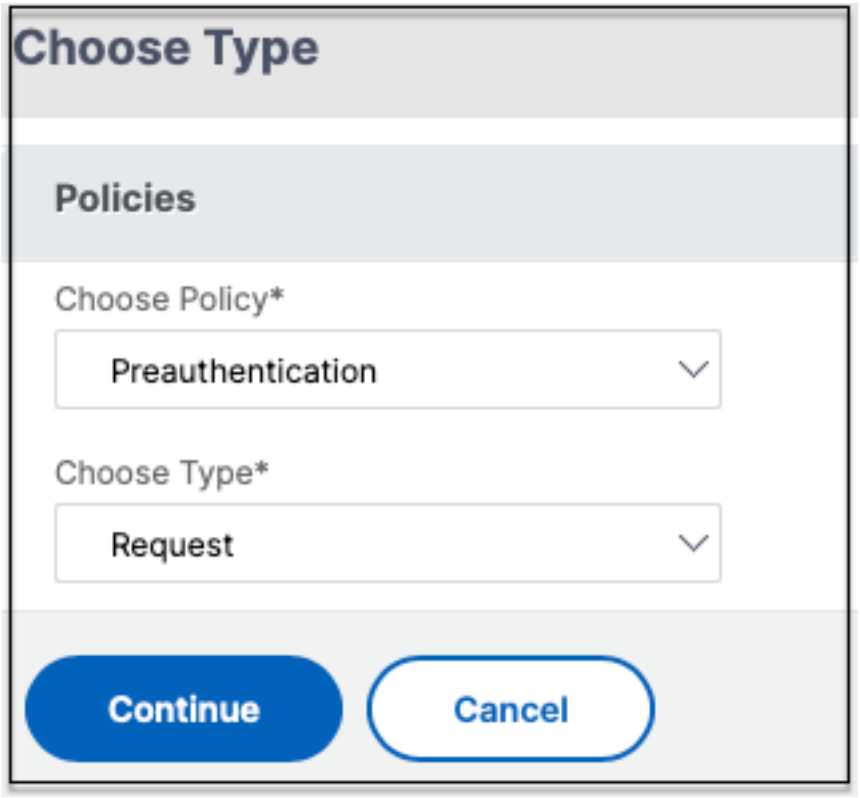
Die folgende Abbildung zeigt einen Beispielausdruck, der für die Überprüfung des Windows 10-Betriebssystems erstellt wurde.



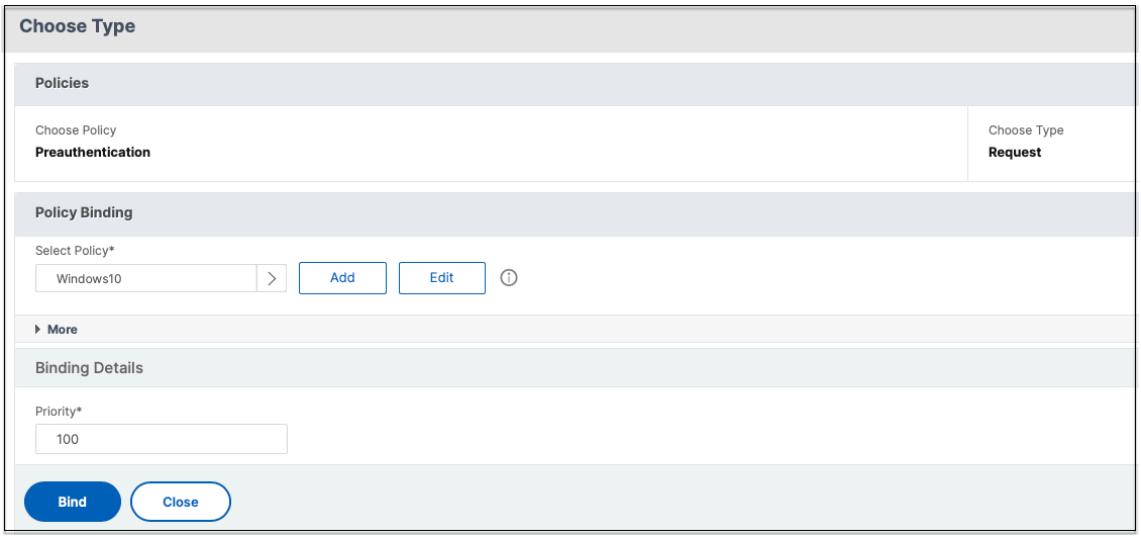
6. Klicken Sie auf **Erstellen**.

Binden Sie das benutzerdefinierte Tag an NetScaler Gateway

1. Navigieren Sie zu **NetScaler Gateway > Virtuelle Server**.
2. Wählen Sie den virtuellen Server aus, an 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 unter **Choose Policy** die Vorauthentifizierungsrichtlinie aus und wählen Sie unter **Choose Type** die Option **Request** aus.



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



Konfigurieren Sie benutzerdefinierte Tags mit der CLI

Führen Sie die folgenden Befehle in der NetScaler CLI aus, um eine Vorauthentifizierungsrichtlinie zu erstellen und zu binden:

Beispiel:

- `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`

Neues kontextbezogenes Tag hinzufügen

1. Öffnen Sie die Secure Private Access-Administratorkonsole und klicken Sie auf **Zugriffsrichtlinien**.
2. Erstellen Sie eine neue Richtlinie oder wählen Sie eine vorhandene Richtlinie aus.
3. Klicken Sie im Abschnitt **Wenn die folgende Bedingung erfüllt** ist auf **Bedingung hinzufügen** und wählen Sie **Kontextuelle Tags** , **Entspricht allen**, und geben Sie dann den Namen des kontextbezogenen Tags ein (z. B. `Windows10`).

Referenzen

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

StoreFront

August 26, 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-

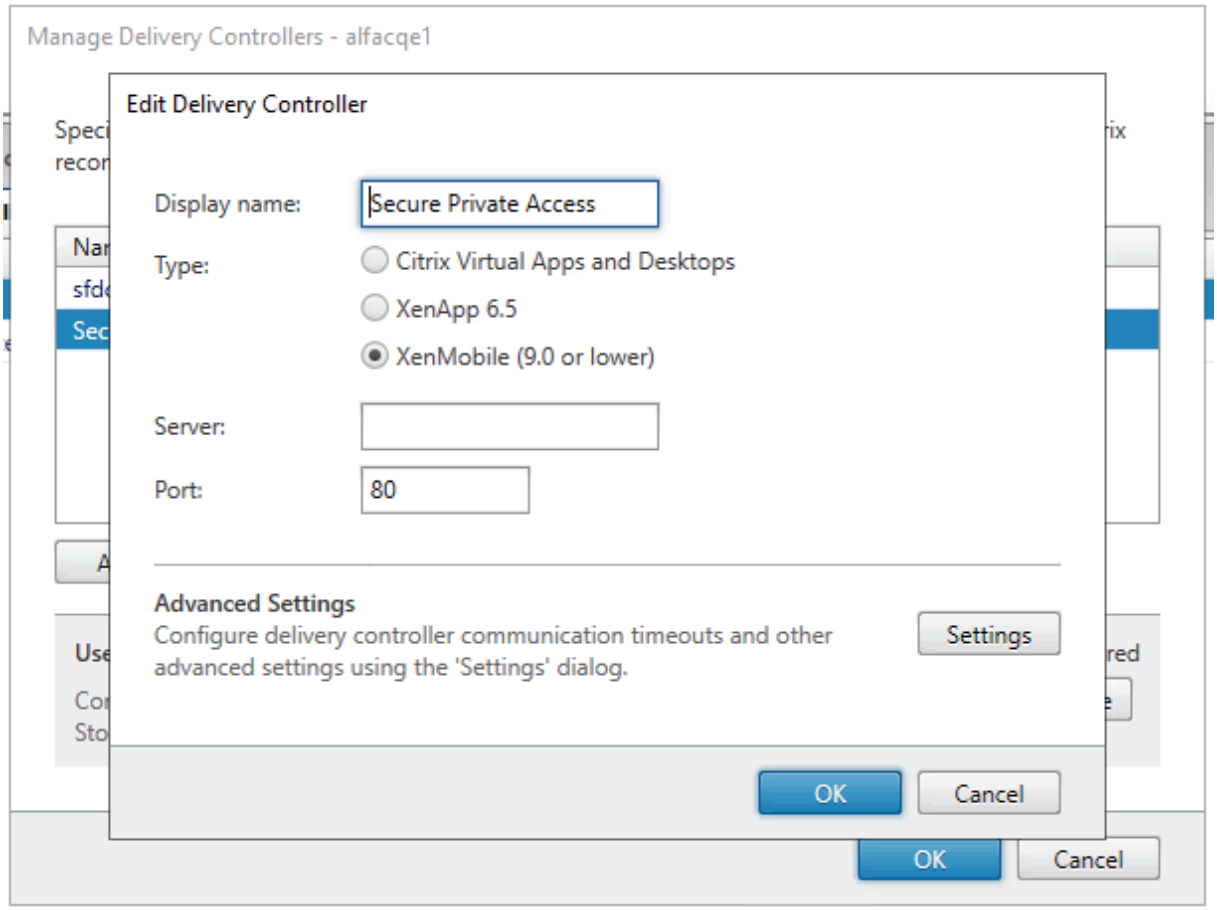
Benutzeroberfläche, da die Benutzeroberfläche nicht die gesamte erforderliche Konfiguration auf StoreFront abdeckt. Das Skript muss ausgeführt werden, um alle erforderlichen Konfigurationen abzuschließen.

- 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.

Director

August 26, 2024

Die Director-Integration mit Secure Private Access ermöglicht eine effektive Leistungsüberwachung und Problembehandlung. 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 on-premises 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 nicht abgeschlossen werden, ohne einen Director zu registrieren. Die Validierung schlägt auch in den folgenden Fällen fehl.

- Director ist nicht bei Secure Private Access registriert.
- Die Director-IP-Adresse oder der FQDN, die Sie eingegeben haben, existieren nicht.

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

> **Hinweis:**
>
> - Die Director-Registrierung oder -Anmeldung unterstützt die integrierte Windows-Authentifizierung (IWA) nicht. Wenn sich der Administrator mithilfe von IWA bei der Secure Private Access-Konsole angemeldet hat, wird der Administrator aufgefordert, die Anmeldeinformationen für die Director-Registrierung einzugeben.
> - Wenn der Administrator eine manuelle Anmeldung an der Secure Private Access-Konsole vorgenommen hat, werden diese Details für die Authentifizierung beim Director-Server verwendet. Gelingt dies nicht, 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**. Während die Director-Details nach der Einrichtung aktualisiert werden, müssen Administratoren die Anmeldeinformationen eingeben, um die Änderungen vorzunehmen. Single Sign-On wird für die Bearbeitung der Director-URL IPv6, SSLv3 nicht unterstützt.

Director mit Secure Private Access mithilfe des Director-Konfigurationstools konfigurieren

Die Konfiguration von Director mit Secure Private Access mithilfe des Config-Tools ist ein obligatorischer Schritt, damit die Integration abgeschlossen ist. Einzelheiten finden Sie unter Secure Private Access-Integration mit Director.

Secure Private Access-Benutzersitzungen in Director anzeigen

Sie können die View Secure Private Access-Benutzersitzungen in Director anzeigen. Einzelheiten finden Sie unter Eine Secure Private Access-Sitzung nach Benutzer anzeigen.

Lizenzserver

August 26, 2024

Ein Lizenzserver für das Secure Private Access Plug-In ist eine obligatorische Komponente, die für die Erfassung und Verarbeitung von Lizenzdaten erforderlich ist. Ein Lizenzserver kann bei der Ersteinrichtung bei Secure Private Access registriert werden oder er kann auch nach Abschluss der Installation konfiguriert oder aktualisiert werden. Einzelheiten zur Registrierung eines Lizenzservers bei Secure Private Access finden Sie unter StoreFront- und NetScaler Gateway-Server integrieren und Einstellungen nach der Installation verwalten.

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

> **Hinweis:**
>
> - Sie müssen mindestens eine Citrix Virtual Apps and Desktops Desktops-Brokerlizenz auf dem Lizenzserver installieren, um das Secure Private 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 und höher unterstützt. Wenn Sie bereits über einen Lizenzserver verfügen, müssen Sie den Lizenzserver auf Version 11.17.2 Build 45000 oder höher aktualisieren.

Weitere Informationen zum Lizenzserver finden Sie unter Lizenzserver.

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.

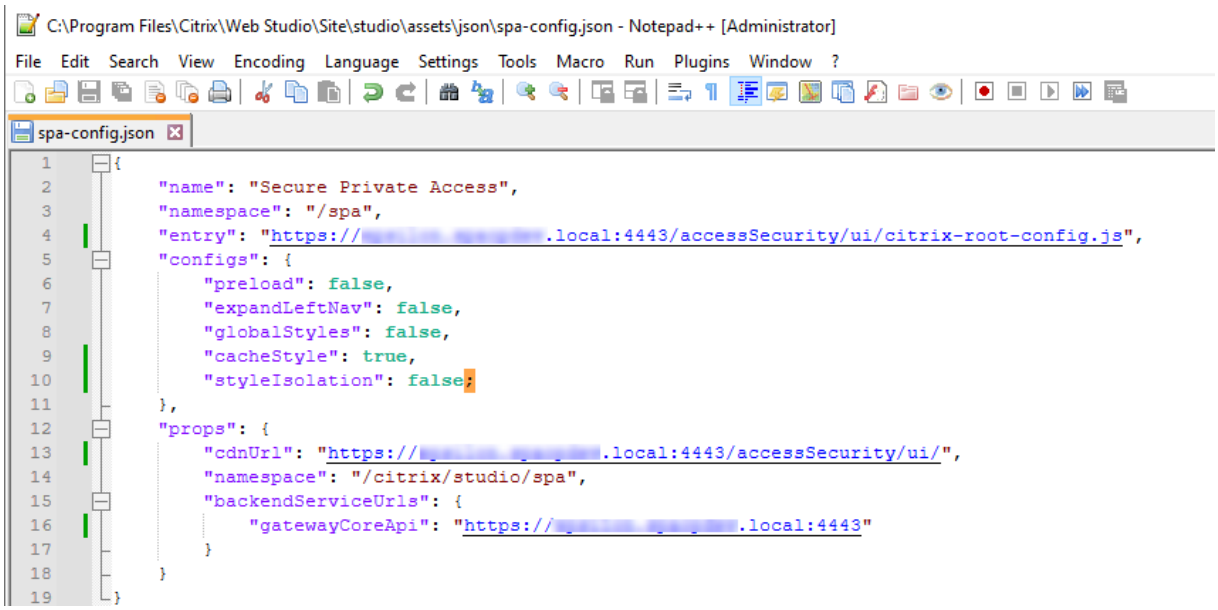
Sie müssen Web Studio Version 2308 oder höher installieren.

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

1. Installieren Sie Citrix Web Studio mit dem Citrix Virtual Apps and Desktops-Installationsprogramm oder dem integrierten DDC-Installationsprogramm.
2. Folgen Sie den Anweisungen auf dem Bildschirm und schließen Sie die Installation ab. Wenn Sie zur Eingabe einer Controller-Adresse aufgefordert werden, geben Sie den DDC-FQDN als Controller-Adresse ein.

3. Navigieren Sie nach erfolgreicher Installation zum Ordner C:\Program Files\Citrix\Web Studio\Site\studio\assets\json und ändern Sie den Inhalt der Datei spa-config.json.

   Wenn für die Web Studio-Installation ein anderer als der Standardspeicherort verwendet wurde, ersetzen Sie den Standardinstallationsort in C:\Program Files\Citrix durch den richtigen Speicherort.



1. Ersetzen Sie “SpaServer”durch den FQDN Ihres Secure Private Access-Plug-Ins.
2. Melden Sie sich bei Web Studio an.
3. Klicken Sie im linken Navigationsmenü auf **Secure Private Access**, um von Web Studio aus auf die Secure Private Access-Administratorkonsole zuzugreifen.

HTTP/HTTPS-Anwendungen konfigurieren

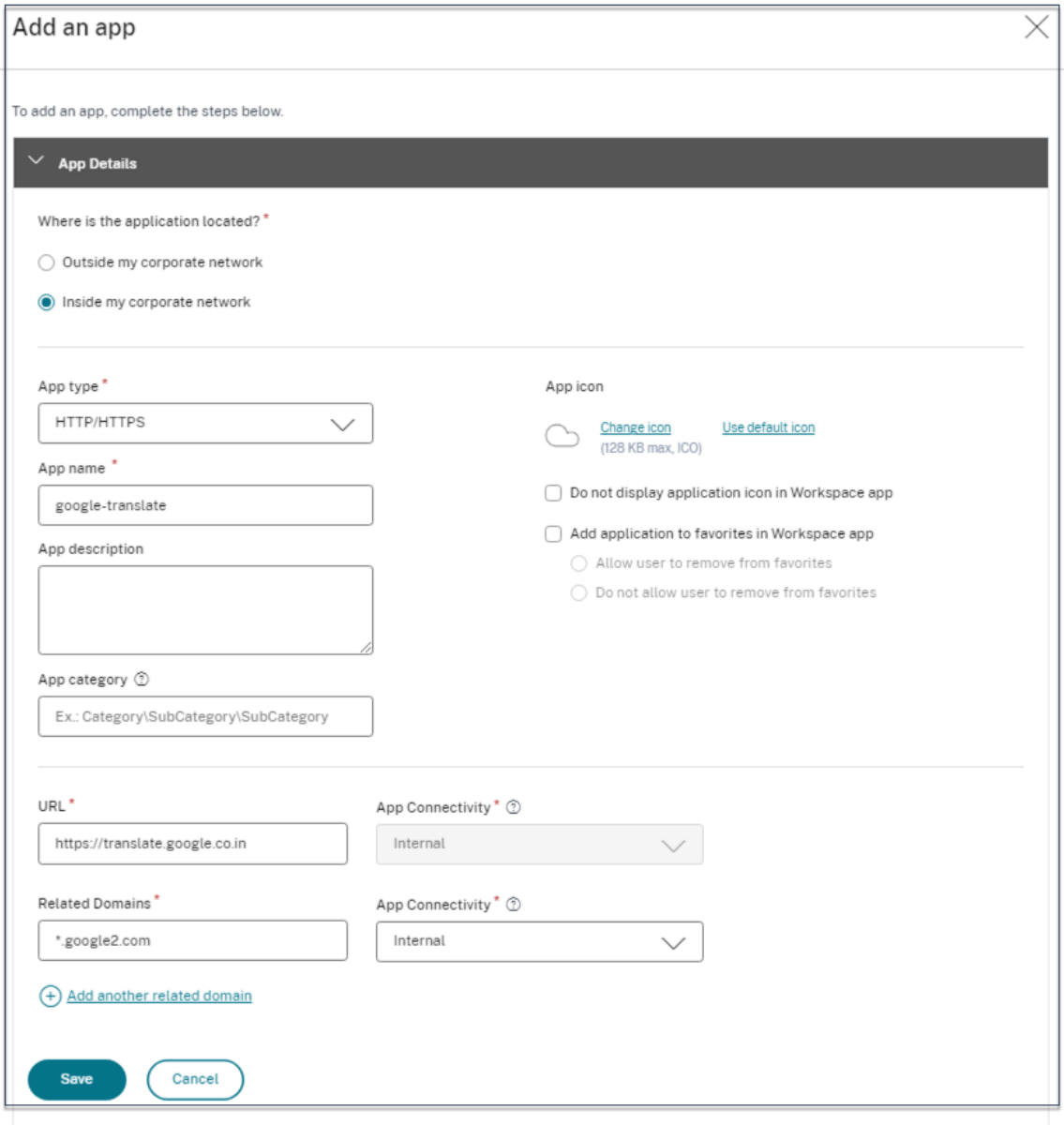
August 26, 2024

Nachdem Sie Secure Private Access eingerichtet haben, können Sie Apps und Zugriffsrichtlinien von der Admin-Konsole aus konfigurieren.

1. Klicken Sie in der Admin-Konsole auf **Anwendungen**.
2. Klicken Sie auf **App hinzufügen**.
3. Wählen Sie den Standort aus, an dem sich die App befindet.

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

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



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

hinzufügen oder vorhandene Kategorien über die Citrix Workspace-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angegeben haben, wird die App in der Workspace-Benutzeroberfläche unter der jeweiligen Kategorie angezeigt.

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

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

- **App-Symbol** —Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Größe der Symboldatei muss 128 x 128 Pixel betragen und nur das Ico-Format wird unterstützt. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.
- **Anwendung für Benutzer nicht anzeigen** —Wählen Sie diese Option, wenn Sie die App den Benutzern nicht anzeigen möchten.
- **URL** —URL der Anwendung.
- **Verwandte Domänen** —Die zugehörige Domäne wird basierend auf der Anwendungs-URL automatisch ausgefüllt. Administratoren können weitere verwandte interne oder externe Domänen hinzufügen.

  > **Hinweis:**
  >
  > - Stellen Sie sicher, dass sich die zugehörige Domäne einer App nicht mit der verwandten Domäne einer anderen App überschneidet. Wenn dies der Fall ist, entfernen Sie die zugehörige Domäne aus allen Apps und erstellen Sie eine neue App mit dieser Domäne. Legen Sie dann den Zugriff in der Zugriffsrichtlinie entsprechend fest. Sie können auch überlegen, ob Sie diese App in StoreFront anzeigen oder ausblenden möchten. Sie können die App in StoreFront mit der Option **Anwendung beim Veröffentlichen der App Benutzern nicht anzeigen** ausblenden.

> – Ebenso darf die URL einer veröffentlichten App nicht als zugehörige Domäne einer anderen App hinzugefügt werden.
> – Weitere Informationen finden Sie unter Bewährte Methoden für Web- und SaaS-Anwendungskonfigurationen.

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

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

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

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

Nächste Schritte

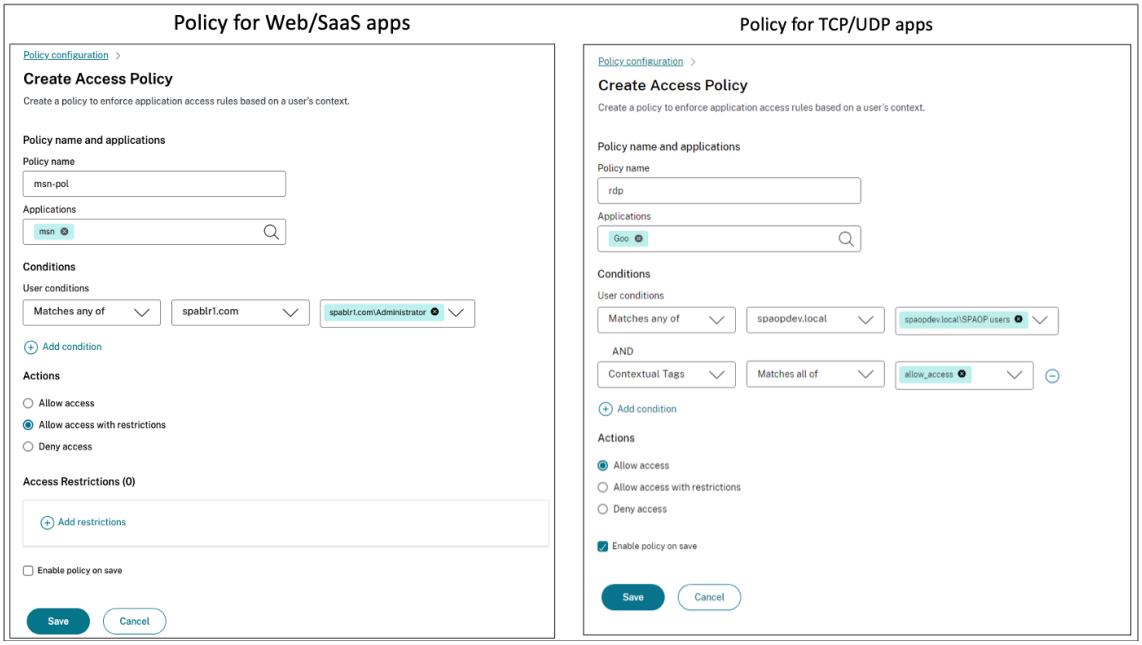
Konfigurieren Sie die Zugriffsrichtlinien für die Anwendungen

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) aktivieren, indem Sie die Sicherheitseinschränkungen hinzufügen.

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



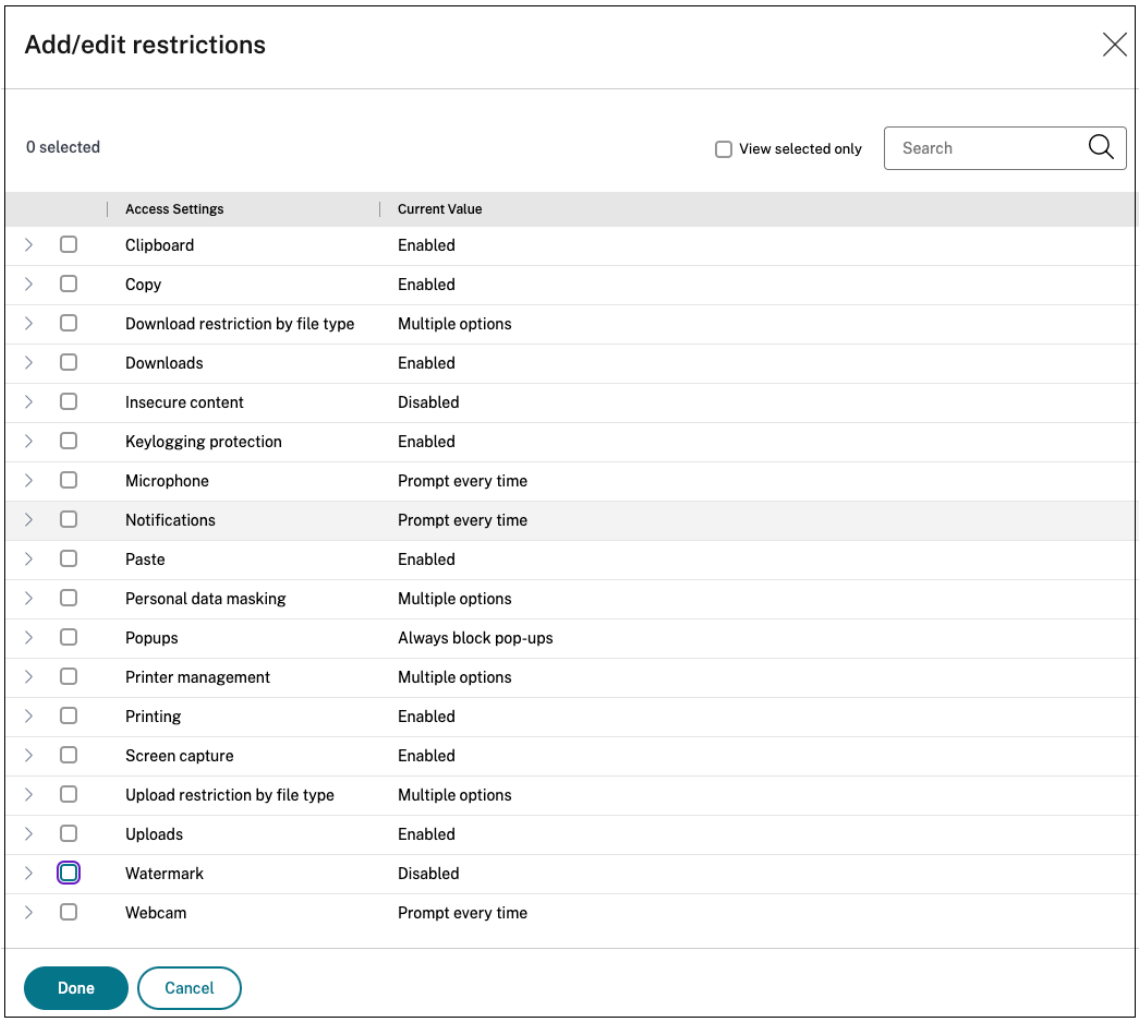
3. a) Geben Sie im Feld **Richtlinienname**einen Namen für die Richtlinie ein.
4. Wählen Sie unter **Anwendungen**die Apps aus, für die Sie die Zugriffsrichtlinien durchsetzen möchten.
5. Unter **Benutzerbedingungen**: Wählen Sie die Bedingungen und Benutzer oder Benutzergruppen aus, auf deren Grundlage 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**

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

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

> **Hinweis:**
>
> Die Aktion **Zugriff mit Einschränkungen zulassen** gilt nicht für die TCP/UDP-Apps.



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

Priorität der Zugriffsrichtlinie

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

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

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

Nächste Schritte

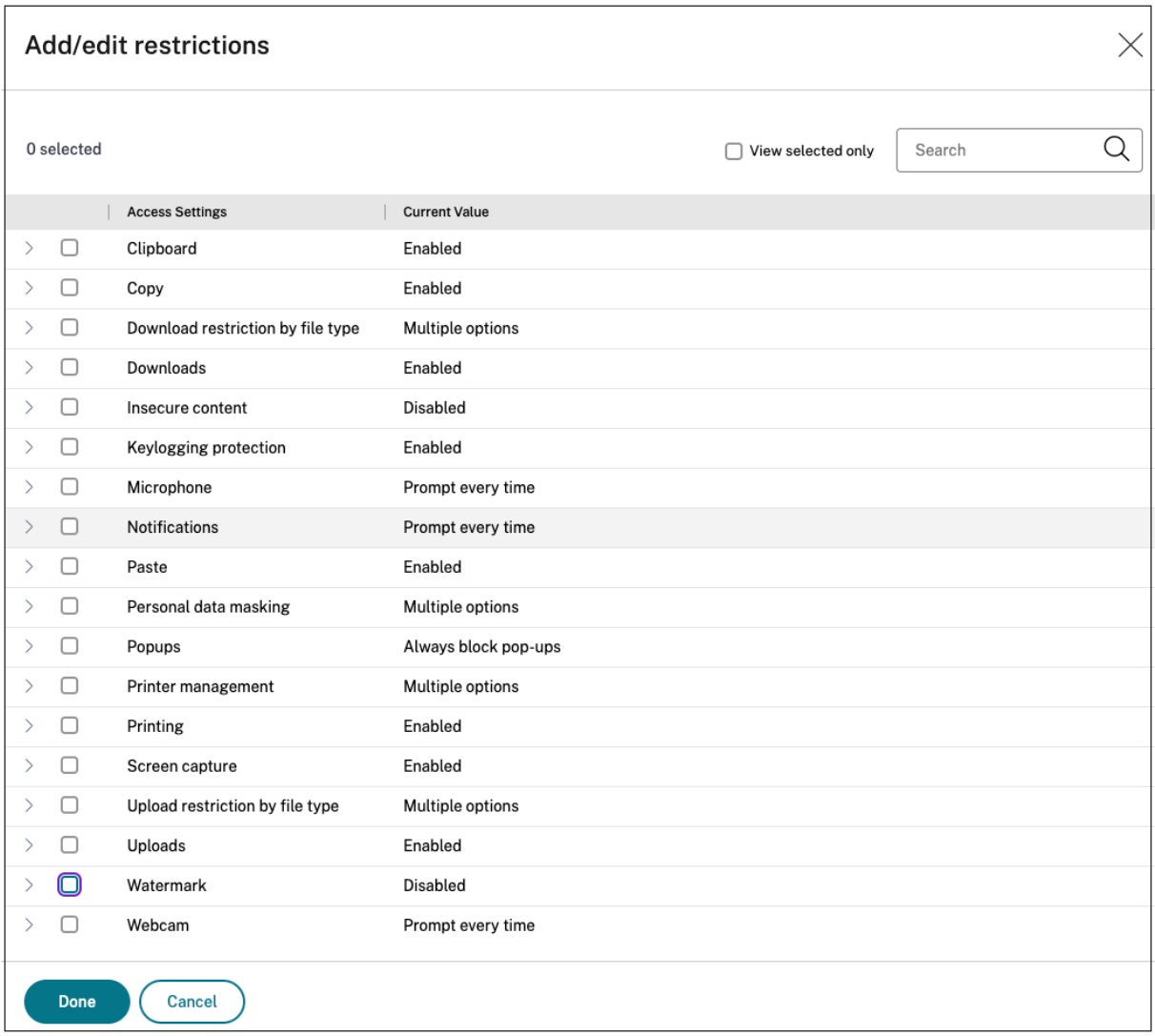
- Überprüfen Sie Ihre Konfiguration auf den Client-Computern (Windows und macOS).
- Überprüfen Sie für die TCP/UDP-Apps Ihre Konfiguration von den Client-Computern (Windows und macOS) aus, indem Sie sich beim Citrix Secure Access Client anmelden.

Validierung der Beispielkonfiguration

Optionen für Zugriffsbeschränkungen

August 27, 2024

Wenn Sie die Aktion **Zugriff mit Einschränkungen zulassen** auswählen, können Sie die Sicherheitseinschränkungen gemäß der Anforderung auswählen. Diese Sicherheitseinschränkungen sind im System vordefiniert. Administratoren können keine anderen Kombinationen ändern oder hinzufügen.



Zwischenablage

Aktivieren/deaktivieren Sie Ausschneiden/Kopieren/Einfügen in einer SaaS- oder internen Web-App mit dieser Zugriffsrichtlinie, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. Standardwert: Aktiviert.

Kopieren

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

> **Hinweis:**
>
> - Wenn sowohl die **Zwischenablage** als auch die **Kopiereinschränkungen** in einer Richtlinie aktiviert sind, hat die Einschränkung der **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.
> - Für eine granulare Steuerung der Kopiervorgänge innerhalb der Apps können Administratoren die Einschränkung **Sicherheitsgruppen** verwenden. Einzelheiten finden Sie unter Einschränkung der Zwischenablage für Sicherheitsgruppen.

Downloadbeschränkung nach Dateityp

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Fähigkeit des Benutzers, einen bestimmten MIME-Typ (Datei) aus der SaaS- oder internen Web-App herunterzuladen, wenn über den Citrix Enterprise Browser darauf zugegriffen wird.

> **Hinweis:**
>
> - Die **Download-Beschränkung nach Dateityp** ist zusätzlich zur **Download**-Beschränkung verfügbar.
> - Wenn sowohl **Downloads** als auch **Download-Beschränkung durch Dateitypeinschränkungen** in einer Richtlinie aktiviert sind, hat die **Download**-Beschränkung Vorrang vor der **Download-Beschränkung durch Dateitypeinschränkung**.
> - 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.

Gehen Sie wie folgt vor, um das Herunterladen von MIME-Typen zu aktivieren:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten zum Erstellen einer Zugriffsrichtlinie finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen** die Option **Mit Einschränkungen zulassen** aus.
3. Klicken Sie auf **Download-Beschränkung nach Dateityp** und dann auf **Bearbeiten**.
4. Wählen Sie auf der **Einstellungsseite Download-Beschränkung nach Dateityp** 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.

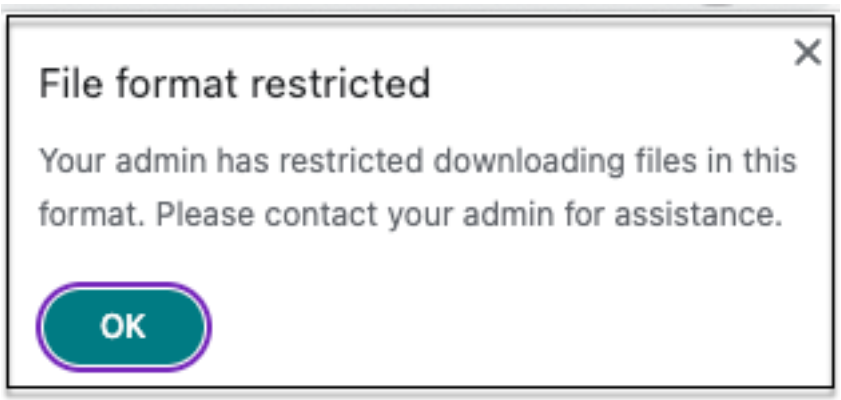
- **Alle Downloads mit Ausnahmen blockieren** —Wählen Sie nur die Typen aus, die hochgeladen werden können, und blockieren Sie alle anderen Typen.

5. Wenn der Dateityp in der Liste nicht vorhanden ist, gehen Sie wie folgt vor:

   a) Klicken Sie auf **Benutzerdefinierte MIME-Typen hinzufügen**.
   b) Geben Sie im Feld **MIME-Typen hinzufügen** den MIME-Typ im Format `category/subcategory<extension>` ein. Zum Beispiel image/png.
   c) Klicken Sie auf **Fertig**.

   Der MIME-Typ erscheint jetzt in der Liste der Ausnahmen.

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



Downloads

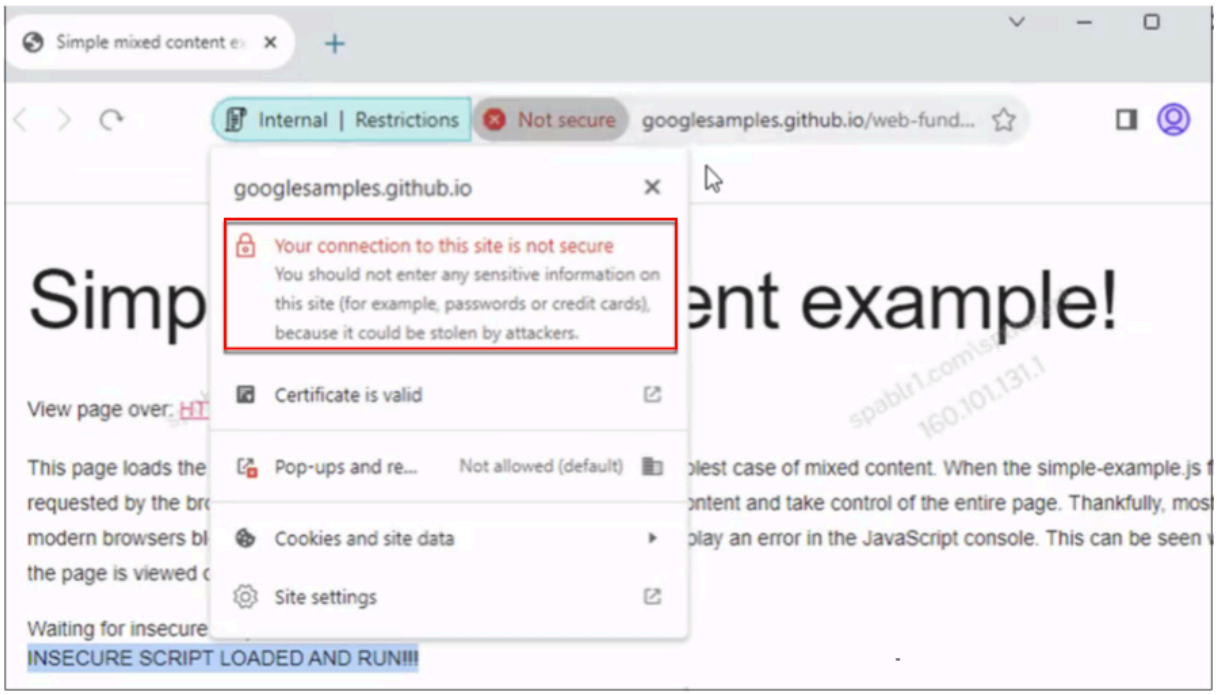
Aktivieren/deaktivieren Sie mit dieser Richtlinie die Fähigkeit des Benutzers, aus der SaaS- oder internen Web-App herunterzuladen, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. Standardwert: Aktiviert.

> **Hinweis:**
>
> Wenn sowohl **Downloads** als auch **Download-Beschränkung nach Dateityp** in einer Richtlinie aktiviert sind, hat die **Download**-Beschränkung Vorrang vor der **Download-Beschränkung nach Dateityp**.

Unsicherer Inhalt

Aktivieren/deaktivieren Sie den Zugriff von Endbenutzern auf unsichere Inhalte innerhalb der SaaS- oder internen Web-App, die mit dieser Richtlinie konfiguriert ist, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. Unsicherer Inhalt ist jede Datei, auf die von einer Webseite aus über einen HTTP-Link und nicht über einen HTTPS-Link verwiesen wird. Standardwert: Aktiviert.

Die folgende Abbildung zeigt ein Beispiel für eine Benachrichtigung, wenn Sie auf unsichere Inhalte zugreifen.



Keyloggingschutz

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

Mikrofon

Fordere Benutzer auf oder fordere sie nicht jedes Mal auf, innerhalb der SaaS- oder internen Web-App, die mit dieser Richtlinie konfiguriert ist, auf das Mikrofon zuzugreifen, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. Standardwert: Jedes Mal auffordern.

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

Gehen Sie wie folgt vor, um das Mikrofon jedes Mal zuzulassen, ohne dass Sie dazu aufgefordert werden:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen** die Option **Mit Einschränkungen zulassen** aus.

3. Klicken Sie auf **Mikrofon** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite mit den **Mikrofoneinstellungen** auf **Immer Zugriff zulassen**.
5. Klicken Sie auf **Speichern** und dann auf **Fertig**.

> **Hinweis:**
>
> - Wenn die **Mikrofonbeschränkung** in der Secure Private Access-Richtlinie aktiviert ist, zeigt Citrix Enterprise Browser die Einstellungen **Zulassen** an.
> - Wenn die Option **Jedes Mal auffordern** in der Secure Private Access-Richtlinie aktiviert ist, variiert die im Citrix Enterprise Browser angewendete Einstellung, je nachdem, ob der Global App Configuration Service (GACS) zur Verwaltung des Citrix Enterprise Browsers verwendet wird.
>
>   > – Wenn GACS verwendet wird, wird die GACS-Einstellung auf den Citrix Enterprise Browser angewendet.
>   > – Wenn GACS nicht verwendet wird, zeigt Citrix Enterprise Browser die Einstellung **Fragen** an.
>
> - Derzeit unterstützt Secure Private Access das Blockieren des Mikrofons nicht. Wenn Sie das Mikrofon blockieren müssen, müssen Sie dies über GACS tun.

Weitere Informationen zu GACS finden Sie unter Citrix Enterprise Browser über den Global App Configuration Service verwalten.

Benachrichtigungen

Erlauben/fordern Sie Benutzer jedes Mal auf, die Benachrichtigungen in der SaaS- oder internen Web-App anzuzeigen, die mit dieser Richtlinie konfiguriert ist, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. Standardwert: Jedes Mal auffordern.

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

Gehen Sie wie folgt vor, um die Anzeige von Benachrichtigungen ohne Aufforderung zu blockieren.

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen** die Option **Mit Einschränkungen zulassen** aus.
3. Klicken Sie auf **Benachrichtigungen** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite mit den **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 über den Citrix Enterprise Browser darauf zugegriffen wird. Standardwert: Aktiviert.

> **Hinweis:**
>
> - Wenn sowohl die Einschränkungen für die **Zwischenablage** als auch für das **Einfügen** in einer Richtlinie aktiviert sind, hat die Einschränkung für die **Zwischenablage** Vorrang vor der Beschränkung **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.
> - Für eine granulare Steuerung der Einfügevorgänge innerhalb der Apps können Administratoren die Einschränkung **Sicherheitsgruppen** verwenden. Einzelheiten finden Sie unter Einschränkung der Zwischenablage für Sicherheitsgruppen.

Maskierung personenbezogener Daten

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

> **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.

Gehen Sie wie folgt vor, 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 **Mit Einschränkungen zulassen** aus.
3. Klicken Sie auf **Maskierung persönlicher Daten** und dann auf **Bearbeiten**.
4. Wählen Sie den Informationstyp aus, den Sie verdecken oder maskieren möchten, und klicken Sie dann auf **Hinzufügen**.

   Wenn der Informationstyp nicht in der vordefinierten Liste erscheint, 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** —Verdeckt teilweise die vertraulichen Informationen. Nur die relevanten Abschnitte werden abgedeckt, der Rest bleibt erhalten.

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

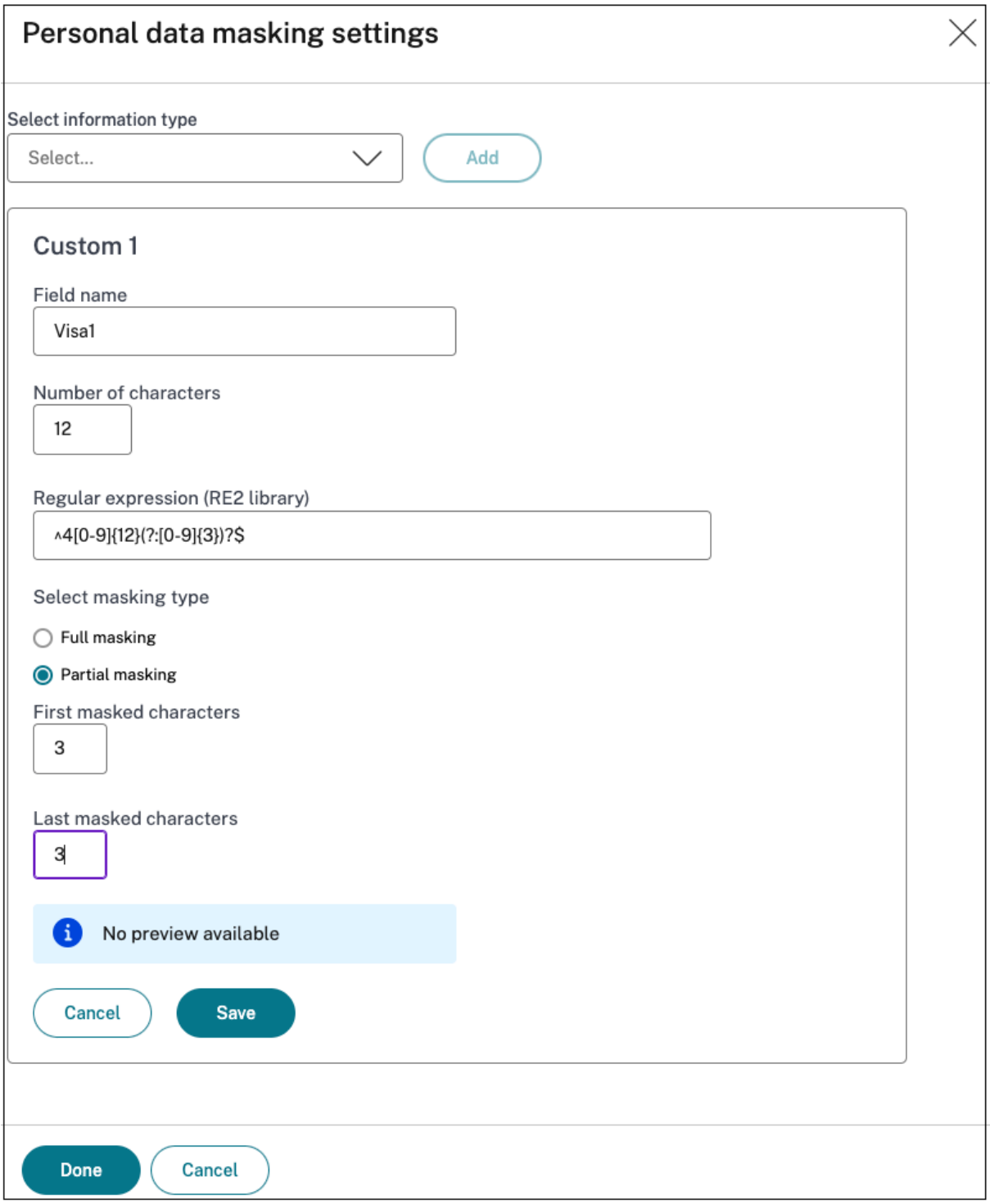
      Das **Vorschaufeld** zeigt das Maskierungsformat an. Diese Vorschau ist für benutzerdefinierte Richtlinien nicht verfügbar.

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

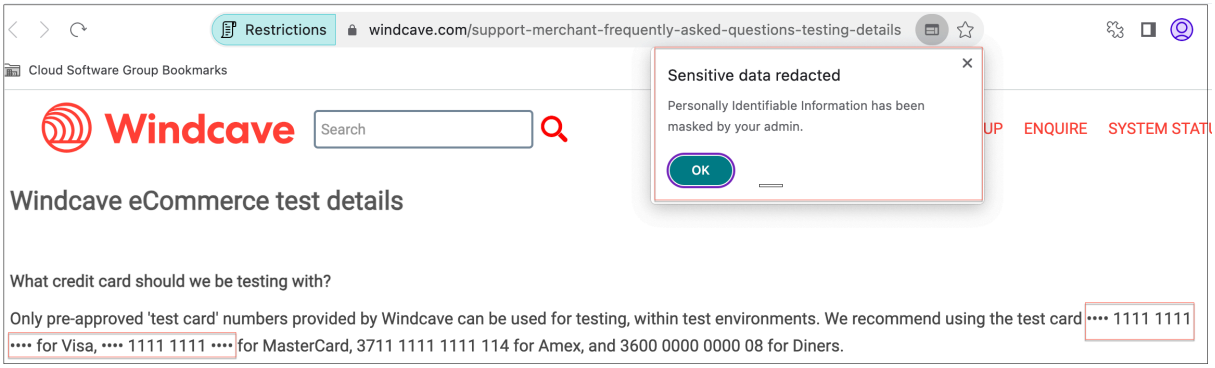
Benutzerdefinierten Informationstyp hinzufügen

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

1. Wählen Sie unter **Informationstyp auswählen** die Option **Benutzerdefiniert** aus und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie unter **Feldname** den Namen für den Informationstyp ein, den Sie maskieren möchten.
3. Geben Sie unter **Anzahl der Zeichen** die Anzahl der Zeichen des Informationstyps ein.
4. Geben Sie unter **Regulärer Ausdruck (RE2-Bibliothek)** den Ausdruck für den benutzerdefinierten Informationstyp ein. Beispiel: `^4[0-9]{ 12 } (?:[0-9]{ 3 } )?$`.
5. Wählen Sie den Maskierungstyp, wenn Sie die vollständigen Informationen oder die ersten oder 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. Die Abbildung zeigt auch die Benachrichtigung im Zusammenhang mit der Maskierung der personenbezogenen Informationen.



Popups

Aktivieren/deaktivieren Sie die Anzeige von Popups in der SaaS- oder internen Web-App, die mit dieser Richtlinie konfiguriert ist, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. 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.

Gehen Sie wie folgt vor, um die Anzeige von Popups zu aktivieren:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen** die Option **Mit Einschränkungen zulassen** 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 Druckdaten aus den konfigurierten SaaS- oder internen Web-Apps mit dieser Richtlinie, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. 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 sowohl **Druck** als auch Einschränkungen der **Druckerverwaltung** in einer Richtlinie aktiviert sind, hat die **Druckeinschränkung** Vorrang vor der **Druckerverwaltungseinschränkung**.

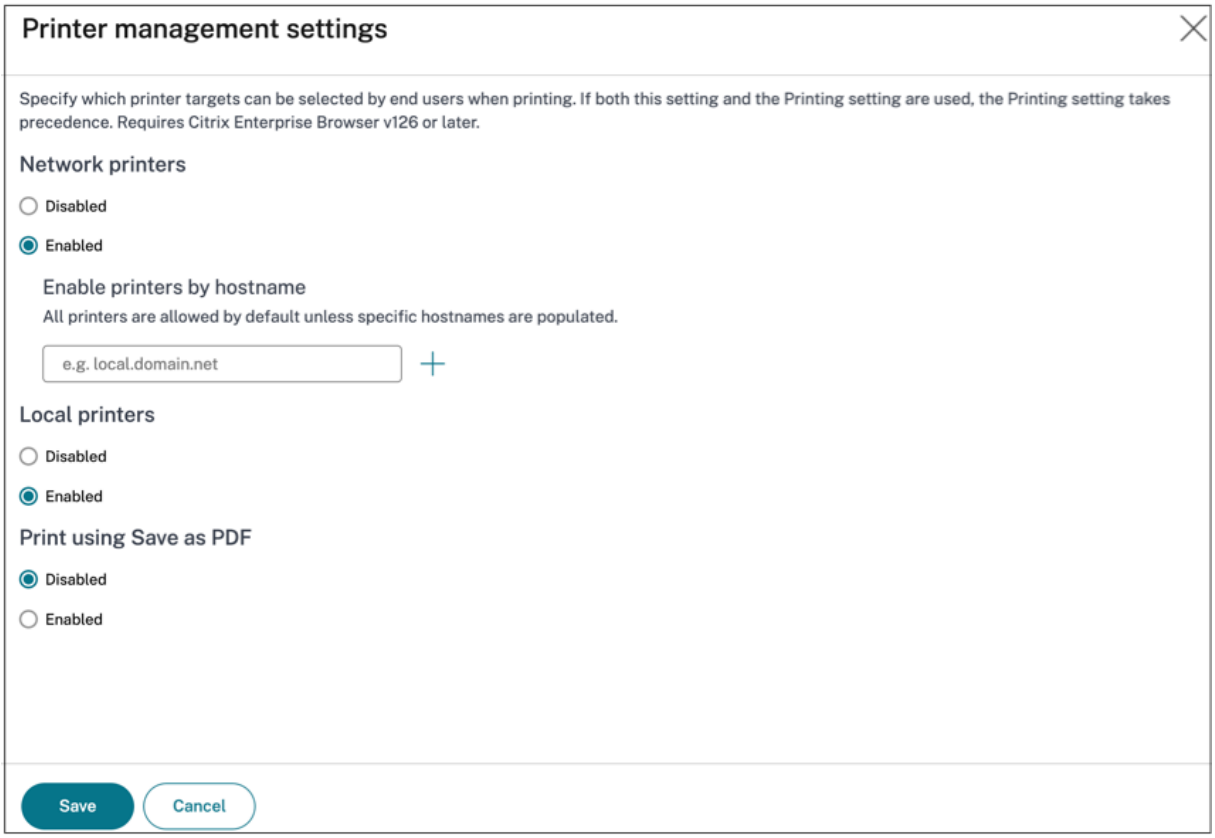
Druckerverwaltung

Aktivieren/deaktivieren Sie Druckdaten, indem Sie die vom Administrator konfigurierten Drucker aus den konfigurierten SaaS- oder internen Web-Apps mit dieser Richtlinie verwenden, wenn über den Citrix Enterprise Browser darauf zugegriffen wird.

> **Hinweis:**
>
> - Die Einschränkung für die **Druckerverwaltung** ist zusätzlich zur **Druckeinschränkung** verfügbar, bei der das Drucken entweder aktiviert oder deaktiviert ist.
>   Wenn sowohl **Druck**- als auch **Druckerverwaltungseinschränkungen** in einer Zugriffsrichtlinie aktiviert sind, hat die **Druckeinschränkung** Vorrang vor der **Druckerverwaltungseinschränkung**.
> - 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.

Gehen Sie wie folgt vor, um Druckeinschränkungen zu aktivieren/deaktivieren:

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



1. Wählen Sie die Ausnahmen gemäß Ihren Anforderungen 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 sind, werden alle anderen Netzwerkdrucker außer den angegebenen gesperrt.

     Hinweis: Netzwerkdrucker werden anhand ihrer Hostnamen identifiziert.

   - **Lokale Drucker:** Ein lokaler Drucker ist ein Gerät, das über eine Kabelverbindung direkt mit einem einzelnen Computer verbunden ist. Diese Verbindung wird in der Regel über USB, parallele Anschlüsse oder andere direkte Schnittstellen ermöglicht.

     - **Deaktiviert:** Das Drucken von allen lokalen Druckern ist deaktiviert.
     - **Aktiviert:** Das Drucken von allen lokalen Druckern ist aktiviert.

   - **Drucken mit Als PDF speichern**

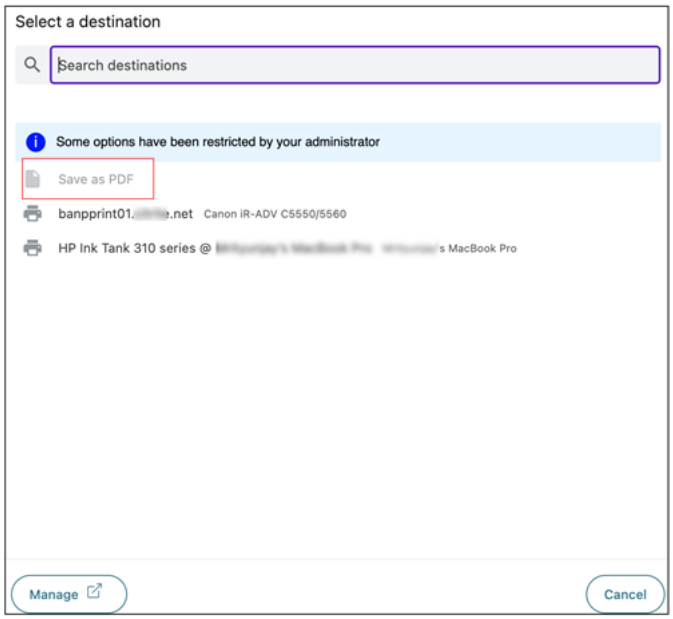
     - **Deaktiviert**: Das Speichern des Inhalts der Anwendung in einem PDF-Format ist deaktiviert.

- **Aktiviert:** Das Speichern der Inhalte aus der Anwendung in einem PDF-Format ist aktiviert.

2. Klicken Sie auf **Speichern**.

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

Wenn **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 die Möglichkeit, die Bildschirme von der SaaS- oder internen Web-App mit dieser Richtlinie zu erfassen, wenn über den Citrix Enterprise Browser mit einem der Bildschirmaufnahmeprogramme oder Apps zugegriffen wird. Wenn ein Benutzer versucht, den Bildschirm zu erfassen, wird ein leerer Bildschirm aufgenommen. Standardwert: Aktiviert.

Uploadbeschränkung nach Dateityp

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Fähigkeit des Benutzers, einen bestimmten MIME-Typ (Datei) aus der SaaS- oder internen Web-App herunterzuladen, wenn über den Citrix Enterprise Browser darauf zugegriffen wird.

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

Gehen Sie wie folgt vor, um das Hochladen von MIME-Typen zu aktivieren/deaktivieren:

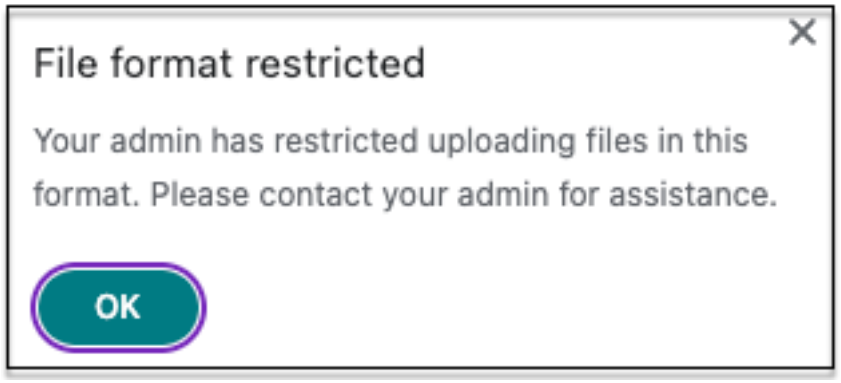
1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie unter **Aktionen** die Option **Mit Einschränkungen zulassen** aus.
3. Klicken Sie auf **Uploadbeschränkung nach Dateityp** und dann auf **Bearbeiten**.
4. Wählen Sie auf der Seite **Einstellungen für die Uploadbeschränkung nach Dateityp** eine der folgenden Optionen aus:

   Alle Uploads mit Ausnahmen zulassen: Laden Sie alle Dateien mit Ausnahme der ausgewählten Typen hoch.
   Alle Uploads mit Ausnahmen blockieren: Blockiert das Hochladen aller Dateitypen mit Ausnahme der ausgewählten Dateitypen.
5. Wenn der Dateityp in der Liste nicht vorhanden ist, gehen Sie wie folgt vor:

   a) Klicken Sie auf **Benutzerdefinierte MIME-Typen hinzufügen**.
   b) Geben Sie im Feld **MIME-Typen hinzufügen** den MIME-Typ im Format `category/subcategory<extension>` ein. Zum Beispiel image/png.
   c) Klicken Sie auf **Fertig**.

   Der MIME-Typ erscheint jetzt in der Liste der Ausnahmen.

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



Uploads

Aktivieren/deaktivieren Sie die Fähigkeit des Benutzers, innerhalb der SaaS- oder internen Web-App hochzuladen, die mit dieser Richtlinie konfiguriert ist, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. Standardwert: Aktiviert.

> **Hinweis:**
>
> Wenn sowohl **Uploads** als auch **Upload-Beschränkung durch Dateitypeinschränkungen** in einer Richtlinie aktiviert sind, hat die **Upload-Beschränkung** Vorrang vor der **Upload-Beschränkung durch Dateitypeinschränkung**.

Wasserzeichen

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

Webcam

Fordere Benutzer auf oder fordere sie nicht jedes Mal auf, innerhalb der SaaS- oder internen Web-App, die mit dieser Richtlinie konfiguriert ist, auf die Webcam zuzugreifen, wenn über den Citrix Enterprise Browser darauf zugegriffen wird. Standardwert: Jedes Mal auffordern.

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

Gehen Sie wie folgt vor, um die Webcam jedes Mal ohne Aufforderung zuzulassen:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen** die Option **Mit Einschränkungen zulassen** aus.

3. Klicken Sie auf **Webcam** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite mit den **Webcam-Einstellungen** auf **Immer Zugriff zulassen**.
5. Klicken Sie auf **Speichern** und dann auf **Fertig**.

> **Hinweis:**
>
> - Wenn die Webcam-Beschränkung in der Secure Private Access-Richtlinie aktiviert ist, zeigt Citrix Enterprise Browser die Einstellungen **Zulassen** an.
> - Wenn die Option **Jedes Mal auffordern** in der Secure Private Access-Richtlinie aktiviert ist, variiert die im Citrix Enterprise Browser angewendete Einstellung, je nachdem, ob der Global App Configuration Service (GACS) zur Verwaltung des Citrix Enterprise Browsers verwendet wird.
>
>   > – Wenn GACS verwendet wird, wird die GACS-Einstellung auf den Citrix Enterprise Browser angewendet.
>   > – Wenn GACS nicht verwendet wird, zeigt Citrix Enterprise Browser die Einstellung **Fragen** an.
>
> - Derzeit unterstützt Secure Private Access das Blockieren von Webcams nicht. Wenn Sie die Webcam blockieren müssen, müssen Sie dies über GACS tun.

Weitere Informationen zu GACS finden Sie unter Citrix Enterprise Browser über den Global App Configuration Service verwalten.

Einschränkung der Zwischenablage für Sicherheitsgruppen

Sie können den Zugriff auf die Zwischenablage für eine bestimmte Gruppe von Apps aktivieren, indem Sie die **Sicherheitsgruppeneinschränkung** verwenden **(Anwendungen > Sicherheitsgruppen)**. Sicherheitsgruppen wird eine Reihe von Apps zugewiesen, in denen die Kopier- und Einfügevorgänge ausgeführt 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.

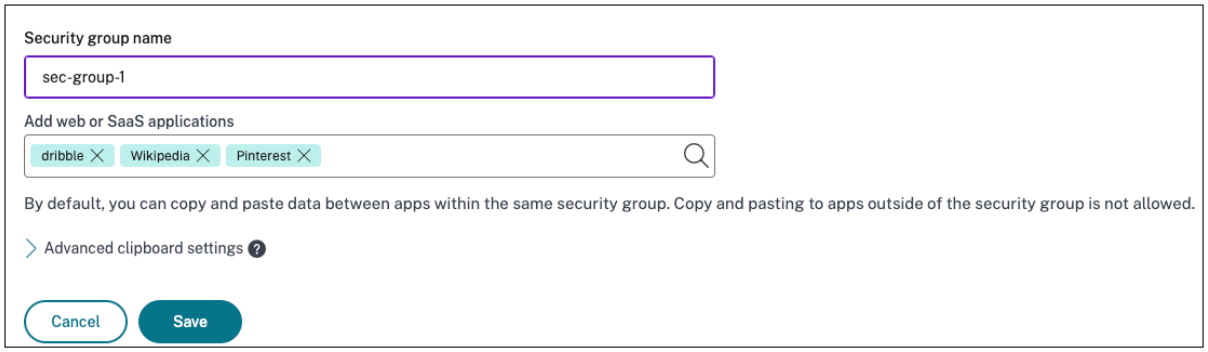
- Wenn die **Sicherheitsgruppeneinschränkung** aktiviert ist, können Sie keine Daten zwischen Anwendungen in verschiedenen Sicherheitsgruppen kopieren/einfügen. Wenn beispielsweise die App “ProdDocs”zur Sicherheitsgruppe “SG1”gehört und die App “Edocs”zur Sicherheitsgruppe “SG2”gehört, können Sie Inhalte von “Edocs”nicht nach “ProdDocs”kopieren/einfügen, selbst wenn die **Kopieren**/**Einfügen**-Beschränkung für beide Gruppen aktiviert ist.
- Für Apps, die nicht Teil einer Sicherheitsgruppe sind, können Sie eine Zugriffsrichtlinie mit der Aktion **Mit Einschränkungen zulassen** 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 Zugriff auf die Zwischenablage für Apps, auf die über den Citrix Enterprise Browser zugegriffen wird, auch über den Global App Configuration Service (GACS) einschränken. Wenn Sie GACS zur Verwaltung von Citrix Enterprise Browser verwenden, verwenden Sie die Option Zwischenablage in **Sandbox aktivieren, um den Zugriff auf die Zwischenablage** zu verwalten. Wenn Sie den Zugriff auf die Zwischenablage über GACS einschränken, gilt dies für alle Apps, auf die über den Citrix Enterprise Browser zugegriffen wird. Weitere Informationen zu GACS finden Sie unter Citrix Enterprise Browser über den Global App Configuration Service verwalten.

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe zu erstellen:

1. Klicken Sie in der Secure Private Access-Konsole auf **Anwendungen** und dann auf **Sicherheitsgruppen**.
2. Klicken Sie auf **Neue Sicherheitsgruppe hinzufügen**.

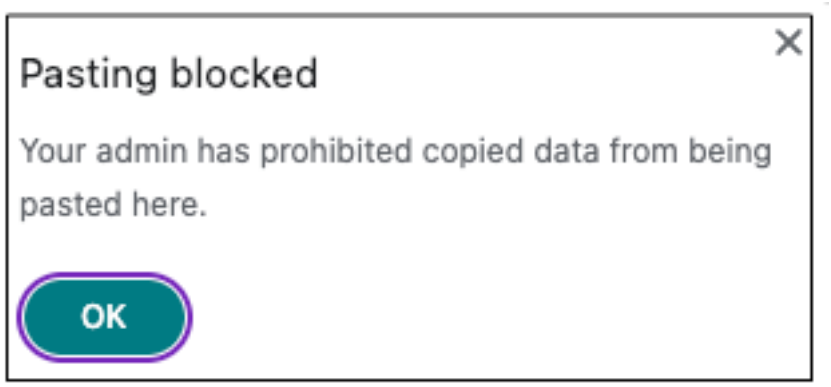


1. Geben Sie einen Namen für die Sicherheitsgruppe ein.
2. Wählen Sie unter **Web- oder SaaS-Anwendungen hinzufügen** die Anwendungen aus, die Sie gruppieren möchten, um das Kopieren und Einfügen zu aktivieren. Zum Beispiel Wikipedia, Pinterest und Dribble.
3. Klicken Sie auf **Speichern**.

Einzelheiten zu den erweiterten Einstellungen für die Zwischenablage finden Sie unter Steuerelemente zum Kopieren und Einfügen für native und unveröffentlichte Apps aktivieren.

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

Endbenutzer können jedoch keine Inhalte aus ihren lokalen Anwendungen auf ihren Computern oder aus unveröffentlichten Anwendungen in diese vorgesehenen Anwendungen kopieren und einfügen und umgekehrt. Die folgende Benachrichtigung wird angezeigt, wenn Inhalt aus den angegebenen Anwendungen in eine andere Anwendung kopiert wird:



> **Hinweis:**
>
> Mit den Optionen im Abschnitt **Erweiterte Einstellungen für die Zwischenablage** können Sie das Kopieren/Einfügen von Inhalten aus lokalen Anwendungen auf Benutzercomputern oder Steuerelemente für unveröffentlichte Anwendungen aktivieren. Einzelheiten finden Sie unter Steuerelemente zum Kopieren und Einfügen für native Anwendungen und unveröffentlichte Apps aktivieren.

Kopieren/Einfügen auf granularer Ebene aktivieren

Sie können den granularen Zugriff auf die Zwischenablage innerhalb der Anwendungen in einer bestimmten Gruppe aktivieren. Sie können dies tun, indem Sie Zugriffsrichtlinien für die Anwendungen erstellen und die Einschränkung **Kopieren**/**Einfügen** gemäß Ihren Anforderungen aktivieren.

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

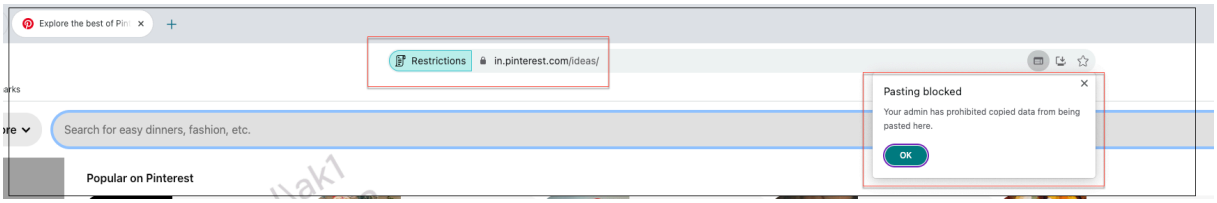
Beispiel:

Bedenken Sie, dass Sie eine Sicherheitsgruppe mit drei Anwendungen erstellt haben, nämlich Wikipedia, Pinterest und Dribble.

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

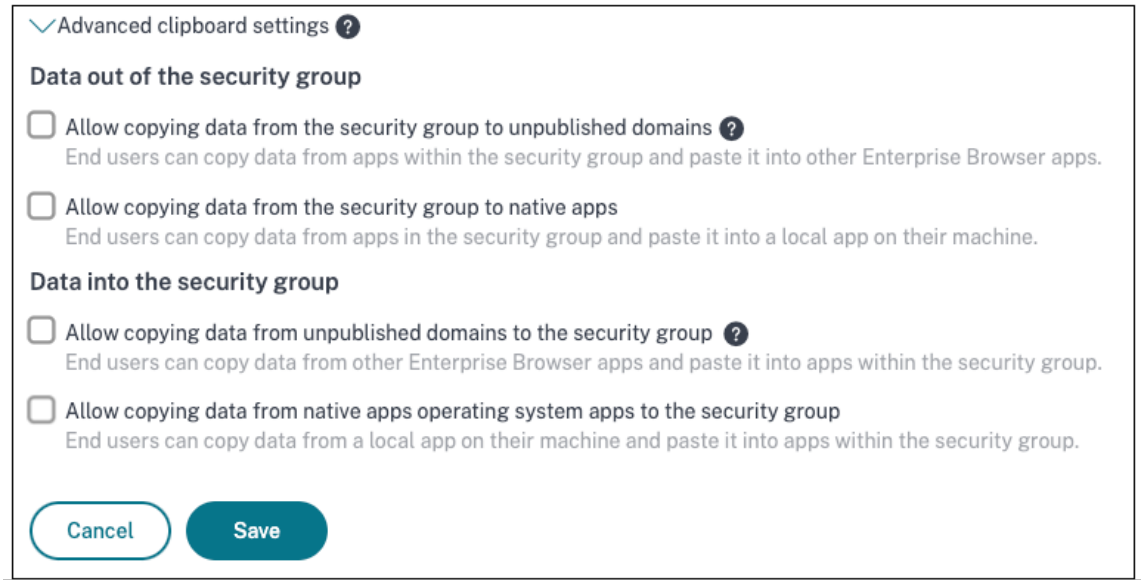
1. Erstellen oder bearbeiten Sie eine der Anwendung `Pinterest` zugewiesene Zugriffsrichtlinie. Einzelheiten zum Erstellen einer Zugriffsrichtlinie finden Sie unter Zugriffsrichtlinien konfigurieren.
2. Wählen Sie unter **Aktionen** die Option **Mit Einschränkungen zulassen** aus.
3. Wählen Sie **Einfügen** aus.

Obwohl Pinterest Teil einer Sicherheitsgruppe ist, zu der auch Wikipedia und Dribble gehören, können Nutzer aufgrund der mit Pinterest verbundenen Zugriffsrichtlinie, in der die Beschränkung zum **Einfügen** aktiviert ist, keine Inhalte von Wikipedia oder Dribble in Pinterest kopieren.



Steuerelemente zum Kopieren und Einfügen für native Anwendungen und unveröffentlichte Apps aktivieren

1. Erstellen Sie eine Sicherheitsgruppe. Einzelheiten finden Sie unter Sicherheitsgruppen in der Zwischenablage für Einschränkungen beim Kopieren und Einfügen.
2. Erweitern Sie **Erweiterte Einstellungen für die Zwischenablage**.



3. Wählen Sie die folgenden Optionen gemäß Ihren Anforderungen aus:

   - **Kopieren von Daten aus der Sicherheitsgruppe in unveröffentlichte Domänen zulassen**; Ermöglicht das Kopieren von Daten aus Anwendungen in den Sicherheitsgruppen in Apps, 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 den unveröffentlichten Domänen in die Sicherheitsgruppe zulassen**: Ermöglicht das Kopieren von Daten aus Apps, die nicht über Secure Private Access veröffentlicht wurden, in die Anwendungen in den Sicherheitsgruppen.
- **Kopieren von Daten aus nativen Apps, Betriebssystem und Sicherheitsgruppe zulassen**: Ermöglicht das Kopieren von Daten aus lokalen Anwendungen auf den Computern in die Anwendungen.

Bekannte Probleme

- Die Routing-Tabelle in (**Einstellungen > Anwendungsdomäne**) behält die Domänen einer gelöschten Anwendung bei. Daher werden diese Anwendungen in Secure Private Access auch als veröffentlichte Anwendungen betrachtet. Wenn direkt über den Citrix Enterprise Browser auf diese Domänen zugegriffen wird, ist das Kopieren/Einfügen in diesen Anwendungen deaktiviert, unabhängig von den Optionen, die Sie in den **erweiterten Zwischenablageeinstellungen** ausgewählt haben.

  Nehmen wir zum Beispiel das folgende Szenario an:

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

  In diesem Szenario ist das Steuerelement zum Einfügen deaktiviert, wenn der Benutzer versucht, Daten aus dieser Anwendung in eine andere Anwendung derselben Sicherheitsgruppe zu kopieren. 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. Wenn die Anwendung Teil der Sicherheitsgruppe ist, werden die Sicherheitsgruppeneinstellungen außerdem nicht berücksichtigt, sodass Sie keine Inhalte aus der Anwendung kopieren/einfügen können.

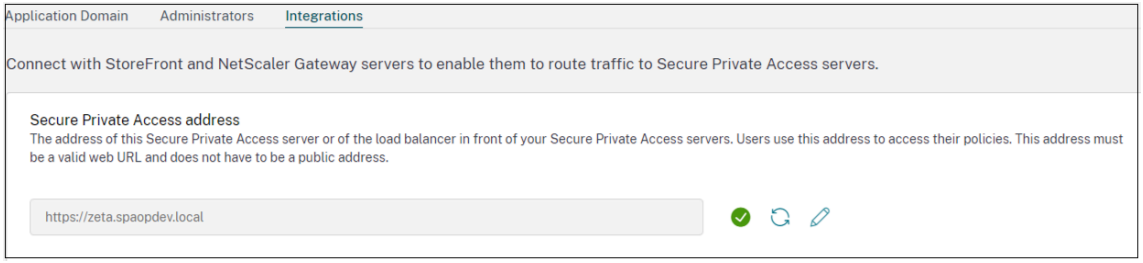
Stellen Sie Secure Private Access als Cluster bereit

August 26, 2024

Die Secure Private Access-Lösung on-premises kann als Cluster bereitgestellt werden, um Hochverfügbarkeit, hohen Durchsatz und Skalierbarkeit zu gewährleisten. Es wird empfohlen, eigenständige Secure Private Access-Knoten für große Bereitstellungen (z. B. mehr als 5000 Benutzer) bereitzustellen.

Secure Private Access-Knoten erstellen

- Erstellen Sie eine neue Secure Private Access-Site. Einzelheiten finden Sie unter Eine Secure Private Access-Site einrichten .
- Fügen Sie der Secure Private Access-Site die erforderliche Anzahl von Clusterknoten hinzu. Einzelheiten finden Sie unter Secure Private Access einrichten, indem Sie einer vorhandenen Site beitreten .
- Konfigurieren Sie auf jedem Secure Private Access-Knoten dieselben Serverzertifikate. Der allgemeine Name des Zertifikatantragstellers oder der alternative Name des Antragstellers muss mit dem FQDN des Load Balancers übereinstimmen.
- Verwenden Sie bei der Konfiguration des ersten Knotens in Secure Private Access die Namen des Load Balancers. Um die nachfolgenden Knoten hinzuzufügen, geben Sie die Datenbankadresse auf der Registerkarte Integrationen an und führen Sie das Datenbankskript manuell aus. Einzelheiten zum Upgrade der Datenbank mithilfe von Skripten finden Sie unter Datenbank mithilfe von Skripten aktualisieren.



Load Balancer-Konfiguration

Für das Secure Private Access-Cluster-Setup gibt es keine spezifischen Load Balancing-Konfigurationsanforderunge
Wenn Sie NetScaler als Load Balancer verwenden, beachten Sie Folgendes:

- Die FQDNs, die für den Zugriff auf StoreFront verwendet werden, sind im DNS-Feld als Subject Alternative Name (SAN) enthalten. Wenn Sie einen Load Balancer verwenden, geben Sie sowohl den FQDN des einzelnen Servers als auch den FQDN des Load Balancers an. Dies gilt für SSL-Zertifikate. Für Secure Private Access ist die Konfiguration des Load Balancers ausreichend. Einzelheiten finden Sie unter Load Balancing 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. Einzelheiten finden Sie unter StoreFront mit HTTPS sichern.

- 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 Load Balancer-Konfiguration verwendet werden kann. Wenn Sie die SSL-Bridge verwenden, stellen Sie sicher, dass auf jedem Secure Private Access-Knoten dieselben Serverzertifikate konfiguriert sind. Außerdem muss der allgemeine Name des Zertifikatssubjekts oder der alternative Antragstellername (SAN) 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 Admin- als auch Runtime-Dienste) sind zustandslos, sodass keine Persistenz erforderlich ist.
- Load Balancer (z. B. NetScaler) verfügen standardmäßig über integrierte Monitore (Probes) für Backend-Server. Wenn Sie einen benutzerdefinierten HTTP-basierten Monitor (Probe) für onpremises Secure Private Access-Server konfigurieren müssen, kann der folgende Endpunkt verwendet werden:

  `/secureAccess/health`

  Erwartete Antwort:

```
Http status code: 200 OK

Payload:

{
"status":"OK","details":{
"duration":"00:00:00.0084206","status":"OK" }
 }
```

  Einzelheiten zur Konfiguration eines NetScaler Load Balancers finden Sie unter Basic Load Balancing einrichten .

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
```

Binden Sie nach dem Erstellen eines Monitors das Zertifikat an den Monitor.

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

Secure Private Access deinstallieren

August 26, 2024

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

1. Wählen Sie **Citrix Virtual Apps and Desktops 7 2405 —Secure Private Access**.
2. Klicken Sie auf **Deinstallieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm und schließen Sie die Deinstallation ab.

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

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

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

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

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

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
```

Upgrade

August 26, 2024

Sie können Ihre Secure Private Access-Bereitstellungen auf eine neuere Version aktualisieren, ohne zuerst neue Computer oder Websites 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-Sequenz ist wie folgt:

1. Sie können Secure Private Access über den Delivery Controller oder über die spezielle Secure Private Access-Kachel in der Benutzeroberfläche des Installationsprogramms aktualisieren, je nachdem, wie Sie Secure Private Access ursprünglich installiert haben.
    - Wenn Sie Secure Private Access über Delivery Controller installiert haben, können Sie die Secure Private Access-Komponente nicht alleine aktualisieren. Stattdessen müssen Sie alle Komponenten aktualisieren. Informationen finden Sie unter Upgrade einer Bereitstellung.
    - Wenn Sie Secure Private Access über die spezielle Secure Private Access-Kachel installiert haben, können Sie es unabhängig aktualisieren. Einzelheiten finden Sie unter Aktualisieren Sie Ihr Secure Private Access-Installationsprogramm.

    > **Hinweis:**
    >
    > Wir empfehlen, Secure Private Access über den Delivery Controller für POC-Umgebungen zu installieren. Für Produktionsumgebungen empfehlen wir jedoch, das dedizierte Installationsprogramm zu verwenden, damit Sie neue Features oder Funktionen anpassen können.

2. Führen Sie die Datenbankskripten aus. Einzelheiten finden Sie unter Datenbank mithilfe von Skripten aktualisieren.

3. Führen Sie die StoreFront-Konfiguration erneut aus. Laden Sie die StoreFront-Skripts unter **Einstellungen > Konfiguration**herunter und führen Sie die Skripts auf den entsprechenden StoreFront-Maschinen aus. Einzelheiten finden Sie unter Integrationseinstellungen ändern.

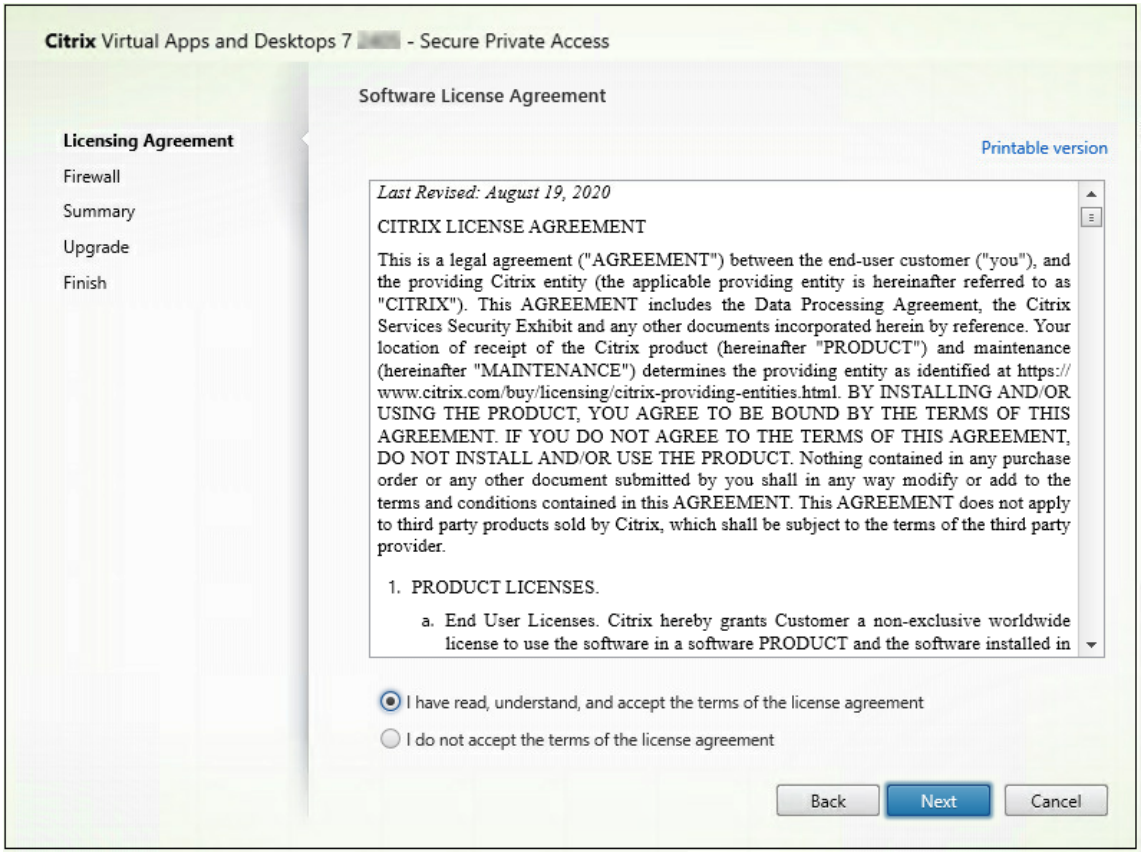
   > **Hinweis:**
   >
   > Wenn Sie die Skripts nicht ausführen, werden die Endpunkte nicht ausgelöst.

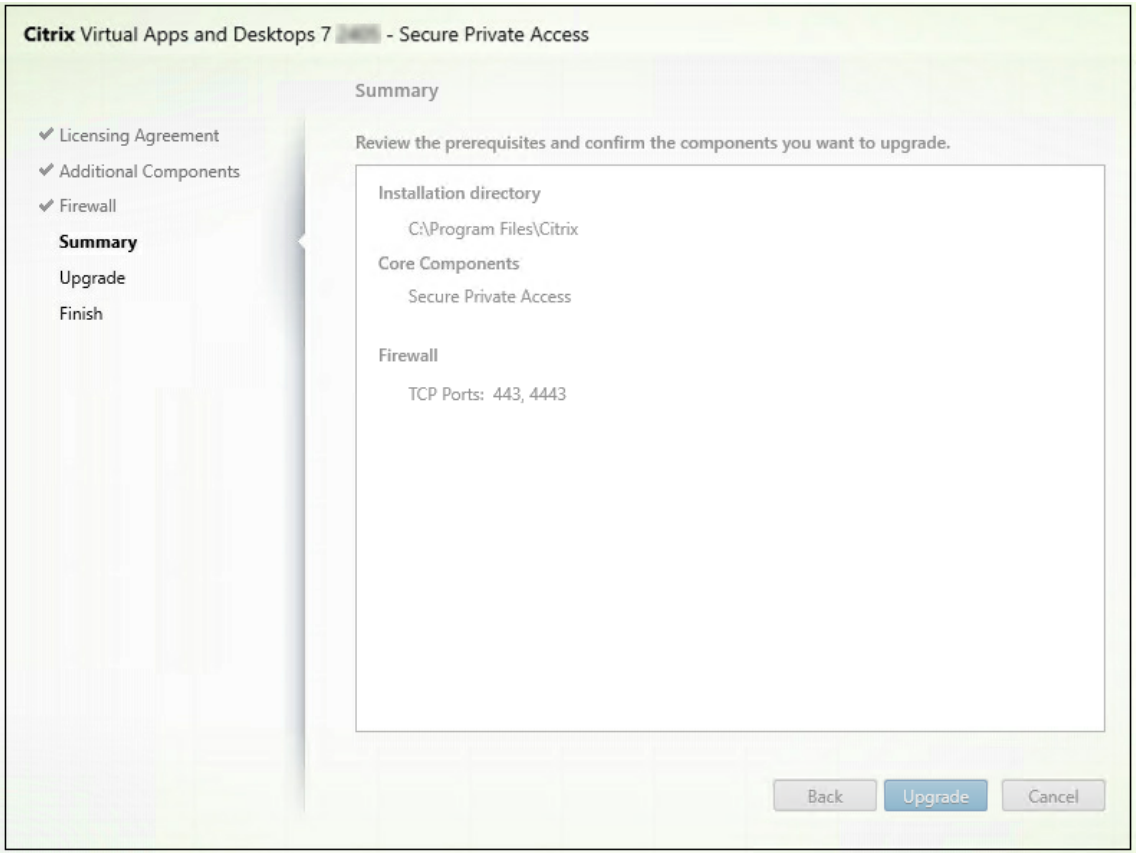
4. (Optional) Führen Sie das NetScaler Gateway-Skript aus. Einzelheiten finden Sie unter NetScaler Gateway.

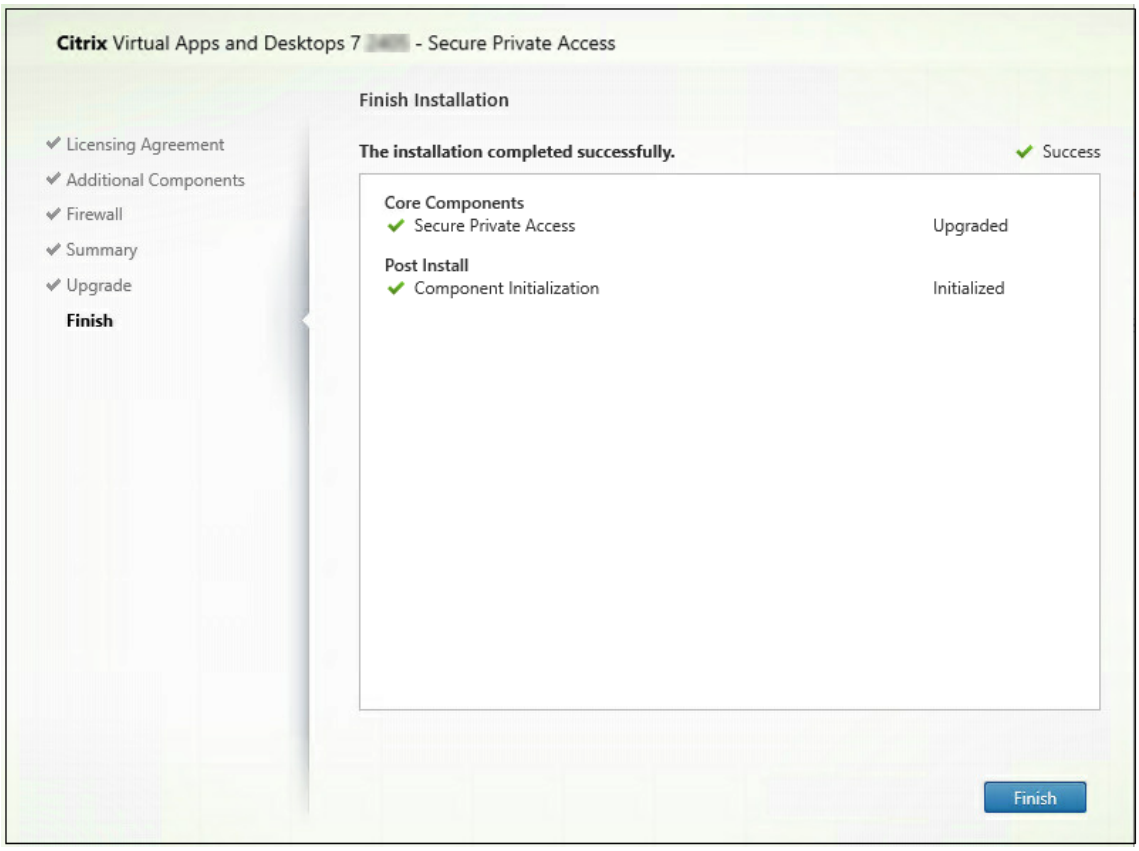
Secure Private Access-Installationsprogramm aktualisieren

August 26, 2024

1. Laden Sie das Installationsprogramm für Citrix Secure Private Access 2405 von https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/herunter.
2. Führen Sie die EXE-Datei als Administrator auf einem Computer aus, der einer Domäne beigetreten ist.
3. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen.







> **Wichtig:**
>
> Nachdem Sie das Installationsprogramm auf Version 2405 aktualisiert haben, müssen Sie das StoreFront-Skript erneut ausführen, damit die neuen Endpunktdetails verfügbar sind.

Nächste Schritte

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

Aktualisieren Sie die Datenbank mithilfe von Skripten

August 26, 2024

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

August 26, 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.

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

- Routing von Anwendungsdomänen verwalten
- Administratoren verwalten
- Integrationseinstellungen ändern

Einstellungen nach der Installation verwalten

August 26, 2024

Routing von Anwendungsdomänen verwalten

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

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

Administratoren verwalten

Auf der Seite "**Einstellungen"> "Administratoren"können Sie die Liste der Administratoren anzeigen und Administratoren** hinzufügen. Dem Administrator, der Secure Private Access zum ersten Mal installiert, wird die volle Berechtigung erteilt. Dieser Admin kann dann weitere Administratoren zum Setup hinzufügen.

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

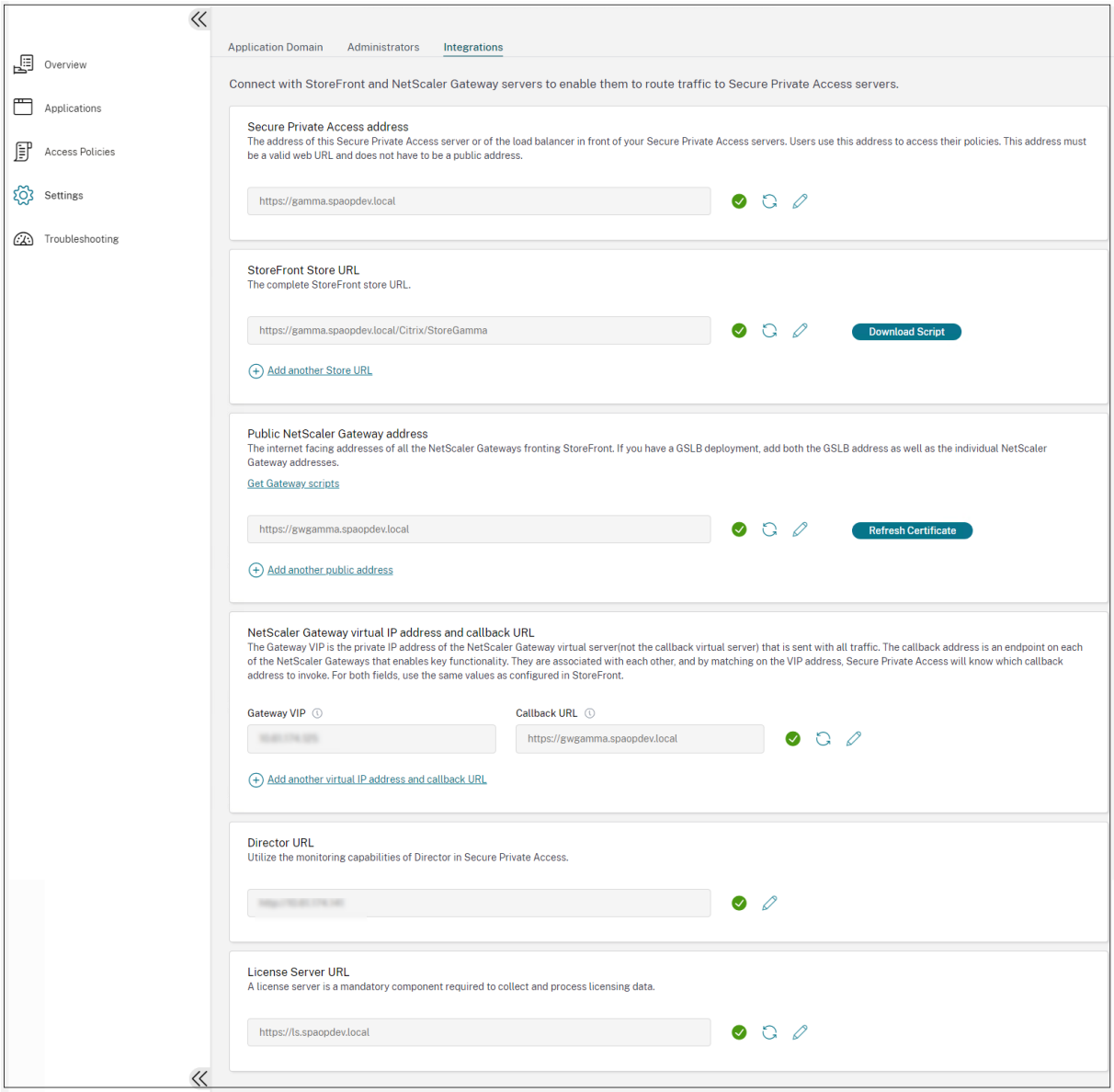
1. Klicken Sie auf der Seite **Administratoren** auf **Hinzufügen**.
2. Wählen Sie unter **Domäne** die Domäne aus, zu der dieser Administrator hinzugefügt werden muss.
3. Wählen Sie unter **Benutzer oder Benutzergruppe** den Benutzer oder eine Gruppe aus, zu der dieser Benutzer gehört.
4. Wählen Sie **unter Admin-Typ**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 Bearbeitungssymbol neben der Einstellung, die Sie ändern und den Eintrag aktualisieren möchten.
3. Klicken Sie auf das Aktualisierungssymbol, um sicherzustellen, dass die Einstellungen gültig sind.

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



Anwendungen und Richtlinien verwalten

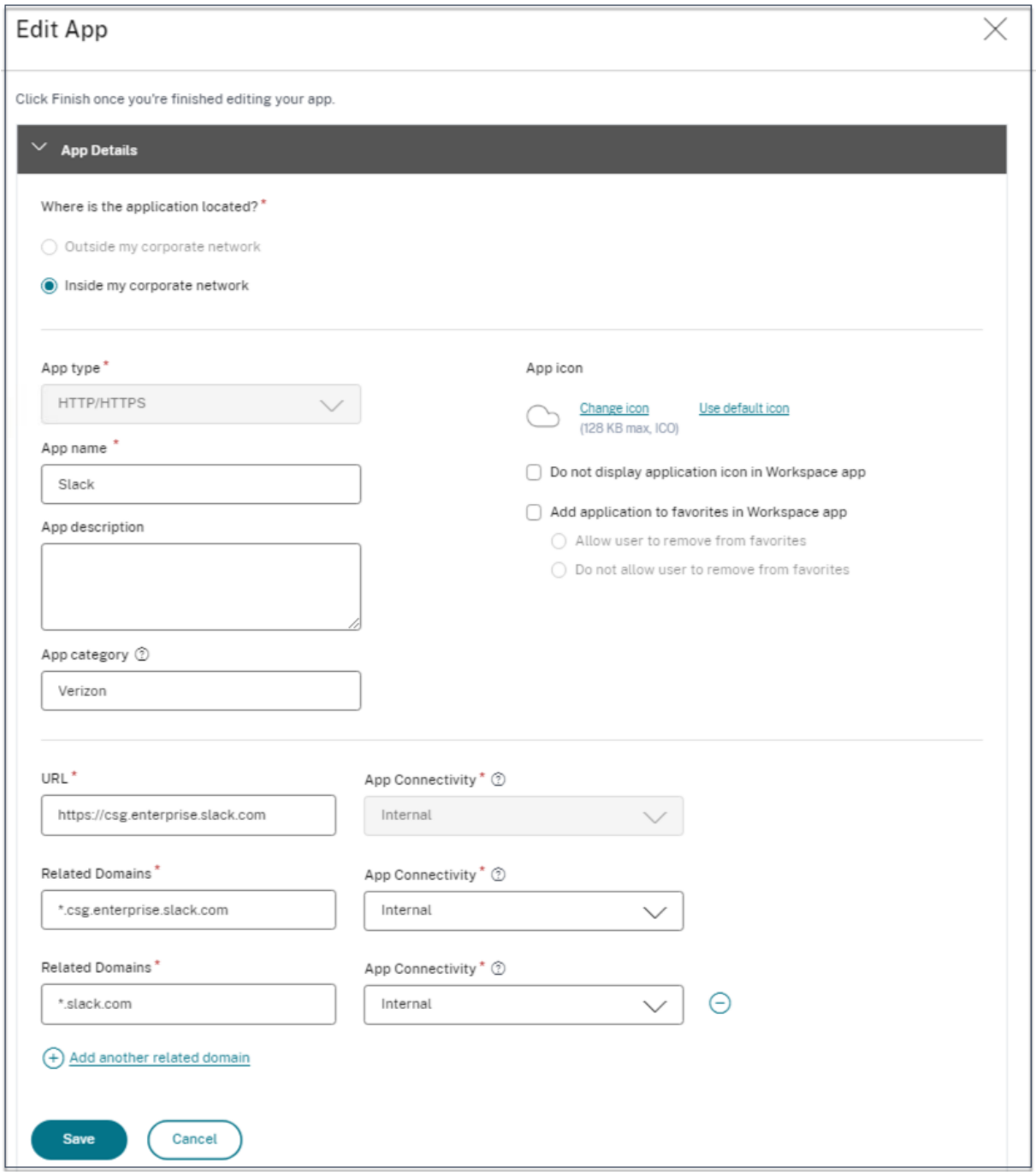
August 26, 2024

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

Eine Anwendung bearbeiten

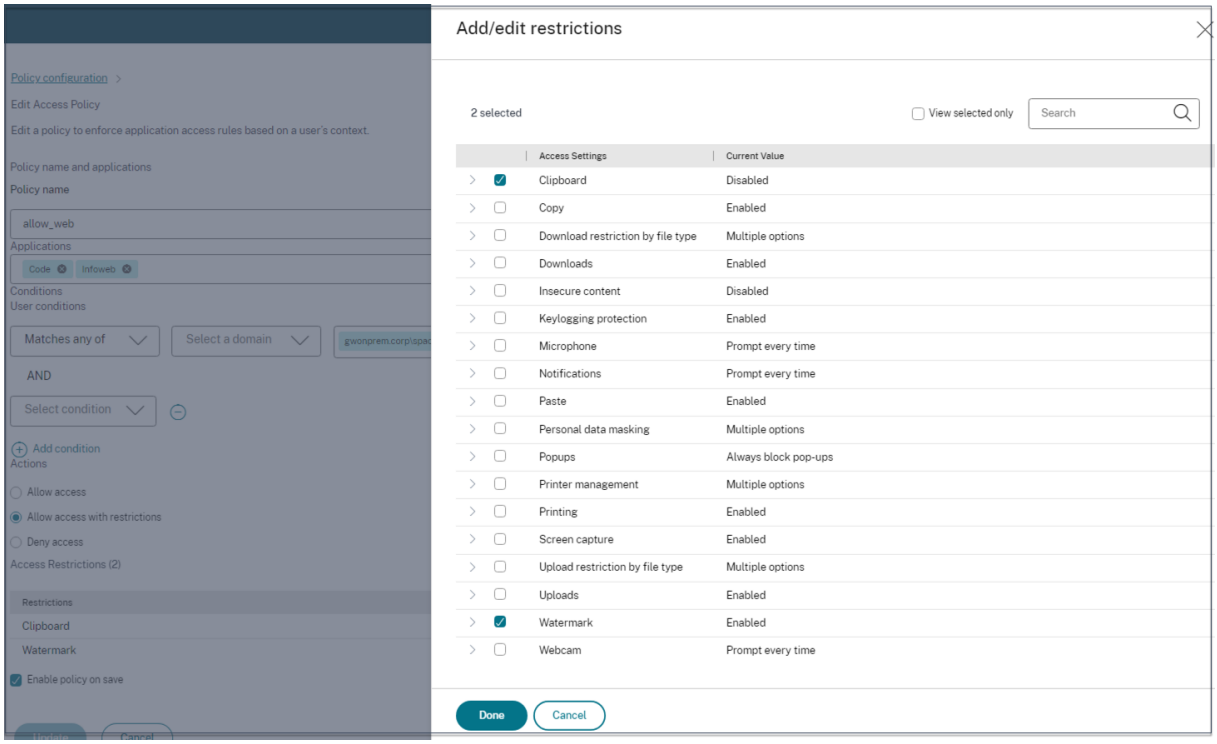
1. Klicken Sie in der Secure Private Access-Administrationskonsole auf **Anwendungen**.

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**.



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.

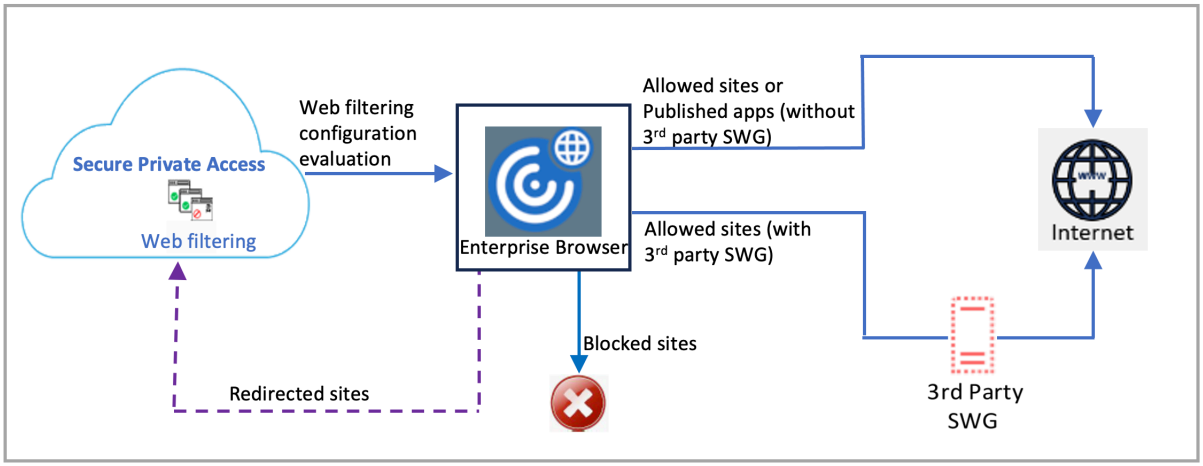
Für alle anderen Internet-URLs oder SaaS-Anwendungen, für die keine App konfiguriert ist, können Administratoren den Tab **Einstellungen > Unsanktionierte Websites** in der Admin-Konsole verwenden, um den Zugriff über den Citrix Enterprise Browser zuzulassen oder zu verweigern.

> **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.



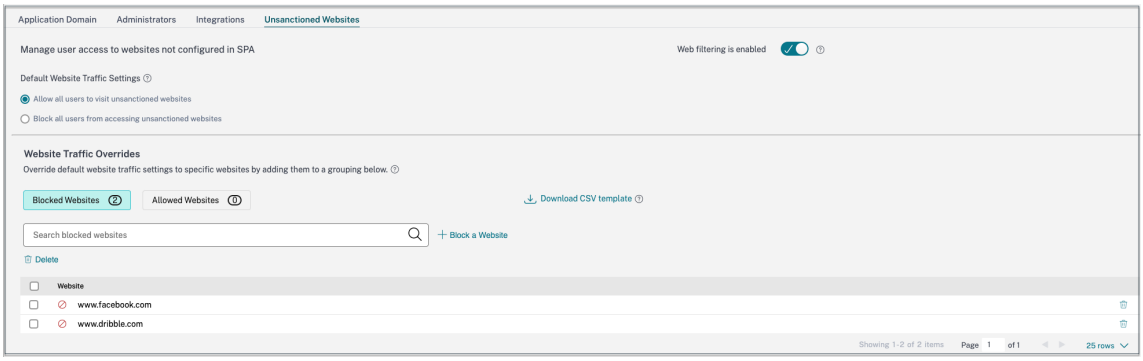
Nach dem Empfang einer Anfrage werden folgende Prüfungen und zugehörige Aktionen ausgeführt:

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.

Ablauf für Endbenutzer

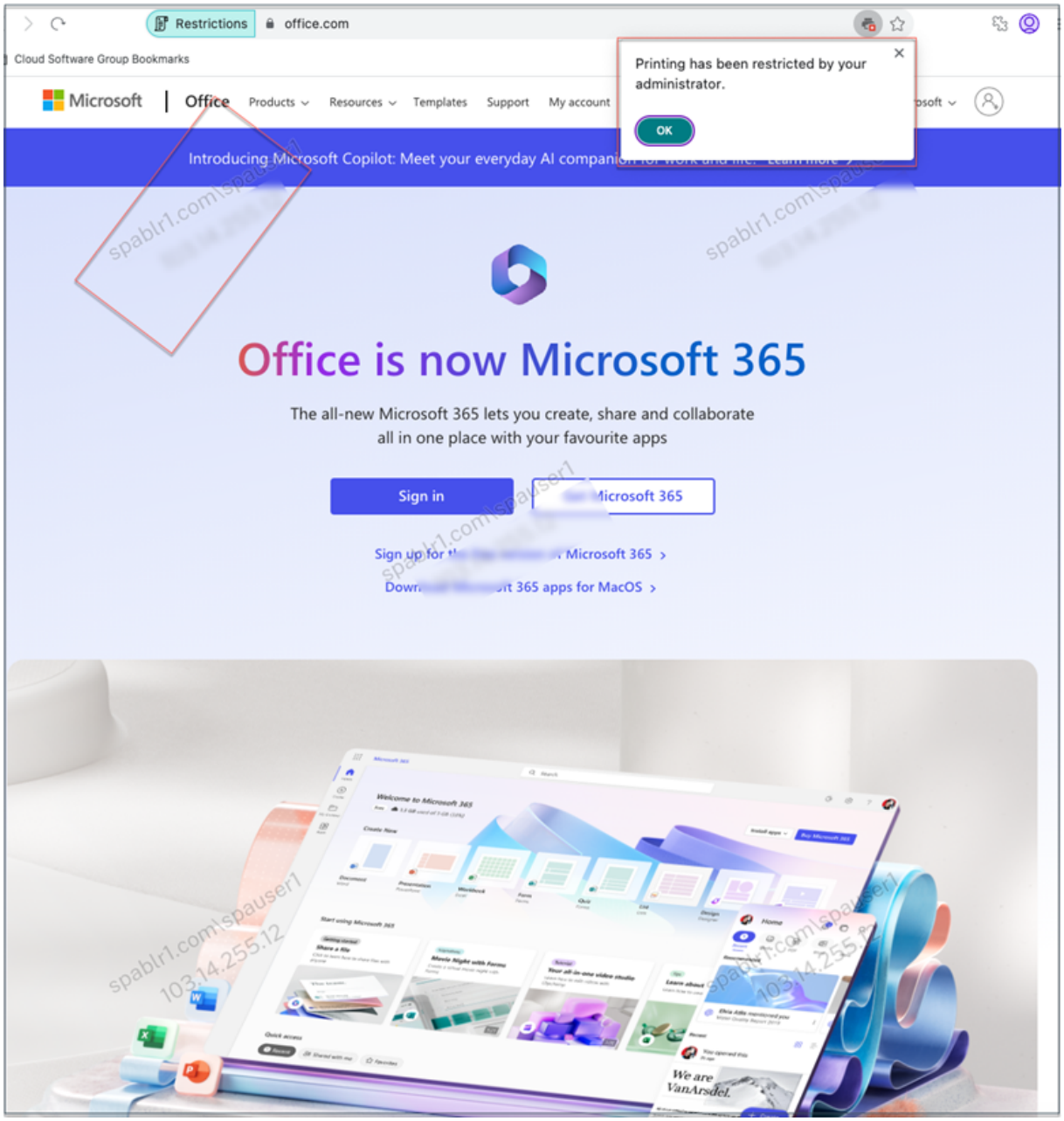
August 26, 2024

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.

Überwachen und Problembehandlung

August 26, 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

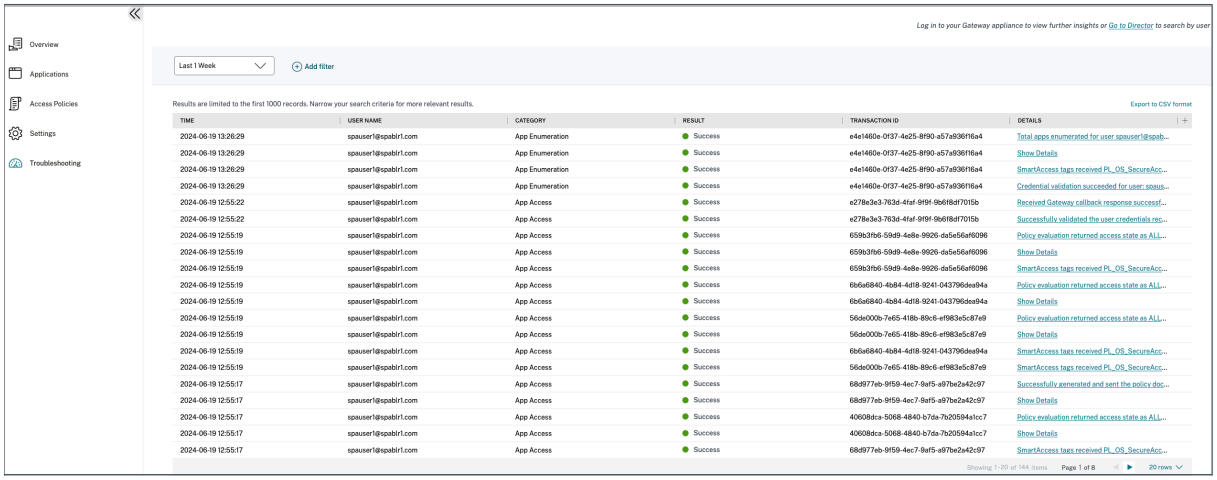
- Director mit Secure Private Access konfigurieren
- Eine Secure Private Access-Sitzung in Director anzeigen
- Liste der Secure Private Access-Sitzungscodes in Director.
- Director.

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 usw. 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.

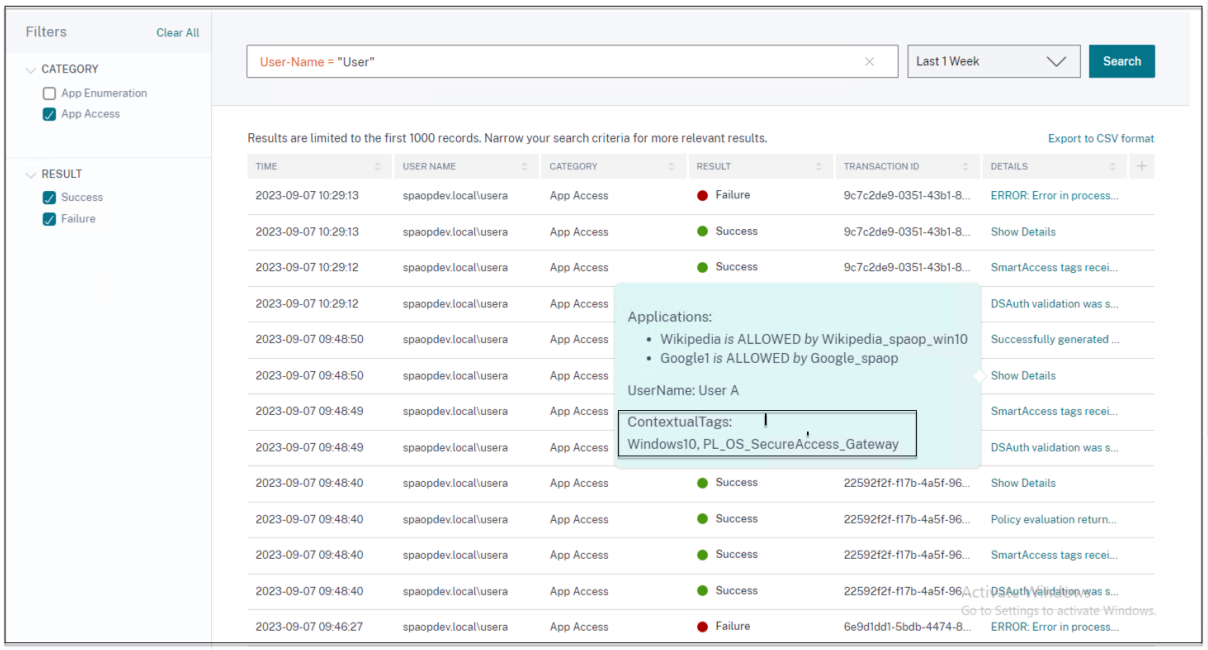
Sie können beispielsweise nach dem Ereignistyp “Enumeration”suchen, indem Sie im Suchfeld die Zeichenfolge **Event-Type > = (entspricht einem bestimmten Wert) > Enumeration** verwenden.

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.



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

  Auflösung:

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

StoreFront-Fehler

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

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

  Auflösung:

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

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

  Auflösung:

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

  Auflösung:

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

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

Auflösung:

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

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

Secure Private Access Server ist nicht erreichbar

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

Auflösung:

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 fehl mit der Meldung "Gateway-Konnektivitätsprüfung fehlgeschlagen. 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 Domäne1 ist, dann lautet die Maschinenidentität "Domäne1\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
 }
```

Problembehandlung mit Director

August 26, 2024

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. In den folgenden Tabellen sind die verschiedenen Fehlercodes und die zugehörigen Bedingungen aufgeführt, die in Director angezeigt werden.

Weitere Informationen finden Sie in den folgenden Artikeln.

- Director mit Secure Private Access konfigurieren
- Eine Secure Private Access-Sitzung in Director anzeigen

> **Hinweis:**
>
> - Codes, die in der zweiten Ziffer “0”enthalten, stellen einen normalen Ausführungsablauf dar. 1000 steht beispielsweise für eine erfolgreiche App-Enumeration.
> - Codes, die in der zweiten Ziffer “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 zu beheben, indem Sie die Protokolle überprüfen. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Support.

Aufzählungsbezogene Codes

Code	Status	Beschreibung
1101	Ausfall	Bei der Aufzählung ist ein interner Fehler aufgetreten.
1102	Ausfall	Einige Apps wurden aufgelistet, aber mindestens eine App-Bewertung ist fehlgeschlagen.
1103	Ausfall	Es wurden keine Apps aufgeführt und mindestens eine App-Bewertung ist fehlgeschlagen.
1000	Erfolg	Die Enumeration war erfolgreich. Mindestens eine App wurde aufgeführt.
1001	Erfolg	Es wurden keine Apps aufgeführt, da sie alle aufgrund von Richtlinien abgelehnt wurden.
1002	Erfolg	Es wurden keine Apps aufgeführt, da keine Richtlinien übereinstimmten.
1003	Erfolg	Es wurden keine Apps aufgeführt, da einige abgelehnt wurden und bei anderen keine Richtlinien übereinstimmten.
1004	Erfolg	Es wurden keine Apps aufgeführt, da keine Richtlinien bewertet werden mussten.

Sitzungsbezogene Codes

Code	Status	Beschreibung
2101	Misserfolg	Sitzungsfehler.
2102	aktiv/inaktiv/ausgefallen	Die Sitzung ist aktiv oder wurde beendet oder mindestens ein App-Start in der Sitzung ist fehlgeschlagen.
2000	Aktiv	Die Sitzung ist aktiv.
2001	Inaktiv	Die Sitzung ist terminiert/inaktiv.

Nachrichtencodes für die App-Aufzählung

Code	Status	Beschreibung
3101	Misserfolg	App-Enumeration —Ein interner Fehler ist aufgetreten (derzeit nicht verwendet).
3102	Misserfolg	Die App wurde nicht aufgeführt, da bei der Bewertung der Richtlinie eine Ausnahme aufgetreten ist.
3103	Misserfolg	Der App-Enumerationsstatus ist Null —Bei der Richtlinienauswertung ist ein interner Fehler aufgetreten.
3104	Erlauben/Ablehnen/Versagen	Fehler beim Abrufen der Richtliniendetails für die App.
3000	Allow	Die Aufzählung von Apps ist zulässig.
3001	Verweigern	Die App-Aufzählung wird durch eine Richtlinie verweigert.
3002	Verweigern	Die App wurde nicht aufgeführt, da keine Richtlinien übereinstimmten.
3003	Unbekannt	Der Status der App-Aufzählung ist unbekannt.

Code	Status	Beschreibung
3004	App-Start von CEB	Versuch, die App vom Citrix Enterprise Browser aus zu starten.

Nachrichtencodes zum Start der App

Code	Status	Beschreibung
4101	Misserfolg	Fehler beim Start der Anwendung —Beim Start der Anwendung ist ein interner Fehler aufgetreten
4102	Misserfolg	Fehler beim Starten der Anwendung (intern)
4103	Erlauben/Ablehnen/Versagen	Fehler beim Abrufen der Richtliniendetails für die App
4000	Allow	App Launch ist erlaubt.
4001	Verweigern	Der Start der Anwendung wurde aufgrund einer Richtlinie verweigert.
4002	Verweigern	Der Start der Anwendung wurde verweigert, da keine Richtlinie entsprach.

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 für SIEM-Lösungen

Einstellungen zur Aufbewahrung von Protokollen

August 26, 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

August 26, 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

August 26, 2024

Citrix Secure Private Access for on-premises