StoreFront 2203

Contents

StoreFront 2203 LTSR im Überblick

February 28, 2024

StoreFront ist ein Unternehmensappstore, der Anwendungen und Desktops von Citrix Virtual Apps and Desktops-Sites und Citrix DaaS in einem einzigen benutzerfreundlichen Store für Benutzer zusammenfasst.

In StoreFront können Sie einen oder mehrere Stores konfigurieren. Jeder Store hat seine eigene Konfiguration, einschließlich:

- Liste der Ressourcenfeeds, die StoreFront abfragt, um die Apps und Desktops für den jeweiligen Benutzer aufzulisten.
- Erscheinungsbild der Website, die für den Zugriff auf den Store verwendet wird.
- Welche Authentifizierungsmethoden die Benutzer verwenden, um sich anzumelden.
- Externer Zugriff über ein NetScaler Gateway.

Benutzer können die lokal installierte Citrix Workspace-App oder die Citrix Workspace-App für HTML5 in einem Webbrowser verwenden, um auf StoreFront-Stores zuzugreifen. Weitere Informationen finden Sie unter Benutzerzugriffsoptionen.

Planen Sie zunächst Ihre StoreFront-Bereitstellung, informieren Sie sich über die Systemanforderungen und installieren Sie StoreFront.

Neue Features

Cumulative Update 4 (CU4) ist das neueste Update für StoreFront 2203 LTSR. Siehe Neue Features.

Ab CU4 können Sie bei der Anmeldung bei StoreFront aktuelle und relevante Informationen zum Startstatus der Citrix Workspace-App für HTML5 sehen. Weitere Informationen finden Sie unter Verbesserter Start von virtuellen Apps und Desktops.

Frühere Releases

Dokumentation zu anderen aktuell verfügbaren Releases finden Sie hier.

Schritte zum Upgrade von einer früheren Version finden Sie unter Upgrade.

Lebenszyklus des Supports

Informationen zur Produktlebenszyklusstrategie für aktuelle Releases (CR) und Long Term Service Releases (LTSR) von StoreFront finden Sie unter Lifecycle Milestones. Zusätzliche Lebenszyklusinformationen für StoreFront finden Sie in CTX200356.

Neue Features

December 5, 2023

- 2203 LTSR CU4
- 2203 LITSR CU3
- 2203 LITSR CU2
- 2203 LITSR CU1
- 2203 LTSR (Erstrelease)
- Einstellung von Features und Plattformen
- Bekannte Probleme

Cumulative Update 4 (CU4)

May 31, 2024

Veröffentlichungsdatum: 16. November 2023

Citrix Workspace-App für HTML5

Diese Version enthält die Citrix Workspace-App für HTML5 2310.

Behobene Probleme in 2203 LTSR CU4 Cumulative Update 4 (CU4) Update 1

- Der Versuch, die Ressourcen- oder App-Auflistung zu starten, schlägt möglicherweise fehl, wenn Sie StoreFront auf Version 2203 LTSR CU4 aktualisieren. [CVADHELP-24175]
- Dieser Fix behebt ein Sicherheitsrisiko in einer Hintergrundkomponente. Weitere Informationen finden Sie unter CTX583759. [CVADHELP-23724]

Behobene Probleme im 2203 LTSR Cumulative Update 4 (CU4)

StoreFront 2203 LTSR CU4 enthält alle in CU3 enthaltenen Fixes sowie die folgenden neuen Fixes:

- Die neuen Anwendungen werden möglicherweise mit HTML5 statt mit der nativen Workspace-App gestartet, wenn der Benutzer die native Workspace-App als Startmethode bevorzugt. [CVADHELP-22435]

- Mit diesem Fix wird der Tippfehler in der deutschen Fehlermeldung korrigiert. [CVADHELP-23088]
- Wenn Sie eine Desktopsitzung mit On-Premises-Bereitstellungen starten, zeigt die Benutzeroberfläche der Citrix Workspace-App möglicherweise positive Startstatusmeldungen an. Innerhalb kürzester Zeit wird jedoch die folgende Fehlermeldung angezeigt:

  <Desktop name>Fehler beim Desktopstart

  Das Problem tritt auf, wenn die Citrix Workspace-App für HTML5 versucht, auf einen ausgeschalteten Desktop zuzugreifen. Die Citrix Workspace-App wartet, bis der Desktop eingeschaltet ist, anstatt das Fehlerdialogfeld anzuzeigen. [CVADHELP-23140]
- Die App-Auflistung auf StoreFront-Servern schlägt möglicherweise zeitweise fehl. [CVADHELP-23196]
- Die Citrix Workspace-App für Mac friert nach dem Umschalten aus dem Ruhezustand möglicherweise ein, wenn eine Verbindung zu einem StoreFront Store besteht. [CVADHELP-23217]
- Eine Race Condition kann dazu führen, dass der Citrix Abonnementstoredienst auf dem StoreFront-Server unerwartet mit Warnmeldungen beendet wird. [CVADHELP-23326]

Cumulative Update 3 (CU3)

February 28, 2024

Veröffentlichungsdatum: 1. Juni 2023

Citrix Workspace-App für HTML5

Diese Version enthält die Citrix Workspace-App für HTML5 2304.

Behobene Probleme

StoreFront 2203 LTSR CU3 enthält alle in CU2 enthaltenen Fixes sowie die folgenden neuen Fixes:

- [CVADHELP-15544] Die StoreFront-MMC-Konsole wird möglicherweise unerwartet beendet, wenn Sie die Verwendung oder Rolle für das Citrix Gateway von **Nur HDX-Routing** auf **Authentifizierung und HDX-Routing** oder **Nur Authentifizierung** ändern.
- [CVADHELP-19879] Wenn Siteaggregation oder Bereitstellungsgruppen mit bestimmten Brokerrichtlinien aktiviert sind, wird beim Starten einer Anwendung oder eines Desktops eine neue

Sitzung erstellt, anstatt sich erneut mit der bestehenden Anwendung bzw. dem Desktop zu verbinden.

- [CVADHELP-21886] Wenn Audio und Drucker in einer Sitzung auf **AUS** festgelegt sind, gilt die Einstellung **AUS** möglicherweise auch für anschließend geöffneten Sitzungen.
- [CVADHELP-22114] Wenn Sie Konfigurationsänderungen von einem StoreFront-Server auf einen anderen übertragen, wird nach der Übertragung möglicherweise die folgende Fehlermeldung angezeigt:

  Server ist nicht erreichbar. Die Konfigurationseinstellungen sind möglicherweise nicht aktuell.

Cumulative Update 2 (CU2)

February 28, 2024

Releasedatum: 08. Dezember 2022

Citrix Workspace-App für HTML5

Diese Version enthält die Citrix Workspace-App für HTML5 2211.

Browsererweiterung (tech preview)

Die Citrix Workspace-Browsererweiterung kann für die nahtlose Clienterkennung und den Sitzungsstart vom Webclient aus verwendet werden. Diese Funktion ist standardmäßig deaktiviert. Administratoren können dieses Feature mit dem folgenden PowerShell-Skript auf einem StoreFront-Server aktivieren:

```
`Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension "
   -IsEnabled $True`
```

Weitere Informationen finden Sie unter Browsererweiterungsbasierte(r) Clienterkennung und Sitzungsstart.

Behobene Probleme

StoreFront 2203 LTSR CU2 enthält alle in CU1 enthaltenen Fixes sowie die folgenden neuen Fixes:

- [CVADHELP-18949] Die SAML-Authentifizierung funktioniert nicht mit den vom ZA-Server ausgestellten Zertifikaten.
- [CVADHELP-21048] Nach dem Upgrade des StoreFront-Servers werden die konfigurierten **FeatureState**-Werte möglicherweise nicht beibehalten.

  > **Hinweis:**
  >
  > Dieser Fix muss sowohl auf die Basis- als auch auf der Upgrade-Version des StoreFront-Servers angewendet werden.

- [CVADHELP-20769] Mit diesem Fix können Sie HTML5-Early Access- und Backup-Releases mit der Standardkonfiguration verwenden. Auf den StoreFront-Servern ist keine zusätzliche Konfiguration erforderlich.
- [CVADHELP-20780] Wenn Sie die Citrix Gateway-Details in der Citrix StoreFront-Verwaltungskonsole ändern, werden möglicherweise zwei Nullparameter, **clusternodes** und **silentauthenticationurls** zur Datei **Roaming\web.config** auf dem StoreFront-Server hinzugefügt.
- [CVADHELP-21037] Nach dem Upgrade von StoreFront von früheren Versionen hat die Einstellung **Receiver für Web-Sites verwalten > Citrix Receiver/Workspace-App bereitstellen > Benutzern können HDX-Engine herunterladen > Quelle für Receiver/Workspace-App** möglicherweise standardmäßig den Wert **Citrix-Website** zugewiesen.

Cumulative Update 1 (CU1)

April 17, 2024

Releasedatum: 03. August 2022

Info zu diesem Release

StoreFront (Erstrelease)

Bekannte Probleme in diesem Release

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Citrix Workspace-App für HTML5

Diese Version enthält die Citrix Workspace-App für HTML5 2205.

Behobene Probleme

StoreFront 2203 LTSR CU1 enthält die folgenden Fixes:

- Wenn Sie versuchen, eine Anwendung oder einen Desktop in der Citrix Workspace-App zu starten, wobei die Siteaggregation für den Client-IP-Adressfilter konfiguriert ist, wird möglicherweise die folgende Fehlermeldung angezeigt:

  Ihre Sitzung wurde wegen des Fehlers 3500 nicht erfolgreich gestartet. Wenden Sie sich an Ihren Administrator, um weitere Informationen zu dem Fehler zu erhalten.

  [CVADHELP-19435]

- Dieser Fix bietet eine verbesserte Warnung, dass einige Features auf der StoreFront-Clienterkennungsseite verloren gehen können, wenn Benutzer während des Clienterkennungsprozesses auf den Link "Bereits installiert"klicken. [CVADHELP-19714]
- Die Authentifizierung delegierter Benutzer oder die Anwendungsenumerierung in Citrix Application Delivery Controller (ADC) schlägt nach dem Upgrade von StoreFront auf Version 2203 möglicherweise fehl. Das Problem tritt auf, wenn TLS1.0 auf dem ADC oder einem Delivery Controller, der für Secure XML Traffic konfiguriert ist, vor dem StoreFront-Upgrade deaktiviert wird. [CVADHELP-19774]

Neue Features

February 28, 2024

Neue Features in 2203 LTSR

Version 2203 von StoreFront enthält die folgenden neuen Features und Verbesserungen:

Unterstützung für TLS 1.0 und TLS 1.1 wurde beendet

Ab diesem Release unterstützt StoreFront die Protokolle TLS 1.0 und TLS 1.1 nicht mehr zwischen Citrix Virtual Apps and Desktops (früher XenApp und XenDesktop) und Citrix Receiver und Workspace Hub.

Citrix Workspace-App für HTML5

Diese Version enthält die Citrix Workspace-App für HTML5 2202.

Behobene Probleme

Die folgenden Probleme wurden seit Version 1912 LTSR CU4 behoben:

- [CVADHELP-16834] Beim Starten einer Benutzersitzung mit der Citrix StoreFront-Dienste-API sind die an die Startanforderung übergebenen Parameter möglicherweise falsch.
- [CVADHELP-17295] Die SAML-Authentifizierung schlägt möglicherweise in der Citrix Workspace-App fehl, die intern mit einem StoreFront verbunden ist.
- [CVADHELP-17385] Dieser Fix ist eine Erweiterung von StoreFront, die den lokalen Hostcache in der Citrix DaaS-Bereitstellung unterstützt. Durch diese Erweiterung können Benutzer Ressourcen von Standorten aus starten, an denen Connectors nicht als Delivery Controller StoreFront hinzugefügt wurden, wenn der Dienst nicht im Cloudausfallmodus ist.
- [CVADHELP-17671] StoreFront enthält ein CSRF-Token (Cross Site Request Forgery) in die Abfragezeichenfolge einiger URLs. Ein Sicherheitsproblem kann auftreten, weil die Token im Browserverlauf oder in den Protokollen von Zwischengeräten wie Proxyservern beibehalten werden können.

  Mit diesem Fix können Sie die CSRF-Token-Verwendung für die folgende URL-Anforderung deaktivieren.

  ```
  Add-STFFeatureState -Name "Citrix.DeliveryServices.WebUI.CsrfValidation
  .IgnoreOnSpecificRequests"-IsEnabled $True
  ```

  > **Hinweis:**
  >
  > Wenn das Feature Toggle auf **ON** gesetzt ist, müssen Sie CSRF-Token aus den URLs in allen WebAPI-basierten benutzerdefinierten Umgebungen entfernen.

- [CVADHELP-18083] Wenn Sie mit der Option “Citrix Receiver/Workspace-App bereitstellen” die “Quelle für Receiver/Workspace-App “als Citrix Website auswählen, wird die Citrix Receiver/Workspace-App von einer unsicheren Site heruntergeladen. Daher blockieren die neuesten Google Chrome-Browserupdates den Download.
- [CVADHELP-18221] Wenn Sie Konten wechseln, um sich auf dem gleichen Client bei Citrix Workspace-App anzumelden, starten Symbole von App-Gruppen mit Highlights möglicherweise falsche Anwendungen. Beispiel: Wenn Benutzer in Citrix Workspace App auf das Symbol von Anwendung **A** klicken, wird möglicherweise die Anwendung **B** gestartet. Außerdem werden im Detailfeld von Anwendung A die Informationen zur Anwendung B angezeigt.
- [LCM-9536] Hervorgehobene Registerkarten in Citrix Receiver für Web-Sites ignorieren den Wert “Linkfarbe”, der im Dialogfeld “Receiver für Web-Site bearbeiten”auf der Registerkarte **Benutzeroberfläche anpassen** angegeben ist. Stattdessen werden hervorgehobene Registerkarten violett angezeigt.

Einstellung von Features und Plattformen

February 28, 2024

Die Ankündigungen in diesem Artikel bieten Ihnen frühzeitige Informationen über Plattformen, Citrix Produkte und Features, die ausgemustert werden, sodass Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Nutzung von Features und Feedback, um den geeigneten Zeitpunkt für eine Außerbetriebnahme zu wählen. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element. Informationen zum Produktlebenszyklussupport finden Sie unter Product Lifecycle Support Policy. Hinweise zur Wartungsoption für Long Term Service Release (LTSR) finden Sie unter https://support.citrix.com/article/CTX205549.

Veraltete und entfernte Produkte und Features

Die in der folgenden Tabelle aufgeführten Plattformen, Citrix Produkte und Features sind veraltet oder wurden entfernt: Die **fett** formatierten Datumsangaben weisen auf Änderungen in diesem Release hin. Veraltete Elemente werden nicht sofort entfernt. Citrix unterstützt sie bis zu dem Release weiter, aus dem sie entfernt werden.

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
Unterstützung für benutzerseitige Kennwortzurücksetzung (SSPR)	2203	2203	-
Unterstützung für TLS 1.0- und TLS 1.1-Protokolle zwischen Citrix Virtual Apps and Desktops (zuvor XenApp und XenDesktop) und der Citrix Workspace-App.	3.14	2203	Aktualisieren Sie Citrix Receiver auf eine Citrix Workspace-App-Version, die TLS 1.2 unterstützt

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
Installation von StoreFront auf Windows Server 2012 R2	2203	2203	Installieren Sie StoreFront auf einem unterstützten Betriebssystem.
Unterstützung für Microsoft.NET Framework-Versionen vor 4.7.2.	2203	2203	Upgrade auf .NET Framework Version 4.7.2 oder höher (Das Installationsprogramm installiert .NET Framework 4.7.2 automatisch, wenn es nicht bereits installiert ist.)
Entfernen der Delivery Controller-Optionen für die folgenden veralteten Produkte: VDI-in-a-Box und XenMobile (9.0 oder früher).	1903	1903	—
Internet Explorer 9 und 10	1903	1903	—
Installation von StoreFront auf Windows Server 2012	1903	1903	Installieren Sie StoreFront auf einem unterstützten Betriebssystem.
Unterstützung für den Benutzerzugriff auf Desktops auf Desktopgerätewebsites	1811	1912	Verwenden Sie Desktop Lock für Anwendungsfälle ohne Domänenanbindung.
Klassisches Citrix-Design mit “grünen Blasen”	3.12	1903	Neue Benutzeroberfläche verwenden

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
Installation von StoreFront auf Windows Server 2012 und Windows Server 2008 R2 (einschließlich Service Packs).	3.12 LTSR	3.15	Installation von Komponenten auf einem unterstützten Betriebssystem.
Citrix Online-Integration (GoTo-Produkt)	3.11	3.12	—
Direkte Upgrades aus StoreFront 2.0, 2.1, 2.5 und 2.5.2	3.9	1818	Upgrade von einer dieser Versionen auf 3.12 und dann auf eine neuere Version
Installieren von StoreFront auf 32-Bit-Maschinen (x86).	3.8	3.13	Installation unter einem unterstützten x64-Betriebssystem.

Informationen zu veralteten Versionen in der Citrix Workspace-App für HTML5 finden Sie auf der Seite Veraltete Versionen.

Bekannte Probleme in Release 2203

May 31, 2024

> **Hinweis:**
>
> Bekannte Probleme, die im Erstrelease von 2203 in diesem Artikel beschrieben werden, sind auch in den CU-Updates vorhanden, sofern sie nicht in der Liste der behobenen Probleme aufgeführt sind.

Bekannte Probleme in StoreFront 2203 CU4

- Der Versuch, die Ressourcen- oder App-Auflistung zu starten, schlägt möglicherweise fehl, wenn Sie StoreFront auf Version 2203 LTSR CU4 aktualisieren.

  > **Hinweis:**
  >
  > Das Problem wurde in 2203 LTSR CU4 Update 1 behoben.

  [CVADHELP-24175]

- Benutzernamen mit Sonderzeichen werden möglicherweise beschädigt angezeigt. [CVADHELP-24499]

Bekannte Probleme in StoreFront 2203 CU3

Es gibt keine neuen bekannten Probleme im kumulativen Update 3.

Bekannte Probleme in StoreFront 2203 CU2

Im Cumulative Update 2 gibt es keine neuen bekannten Probleme.

Bekannte Probleme in StoreFront 2203 CU1

Im Cumulative Update 1 gibt es keine neuen bekannten Probleme.

Bekannte Probleme in StoreFront 2203

- Die StoreFront-Installation kann fehlschlagen, wenn die Datei TelemetryService.exe "Framework.xml"sperrt. Beenden Sie als Workaround den Citrix Telemetriedienst und wiederholen Sie die Installation. [LCM-12147]
- Die Authentifizierung delegierter Benutzer oder die Anwendungsenumerierung in Citrix Application Delivery Controller (ADC) schlägt nach dem Upgrade von StoreFront auf Version 2203 möglicherweise fehl. Das Problem tritt auf, wenn TLS1.0 auf dem ADC oder einem Delivery Controller, der für Secure XML Traffic konfiguriert ist, vor dem StoreFront-Upgrade deaktiviert wird. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX457757. [CVADHELP-19774]. Dieses Problem wurde in Release 2203 LTSR CU1 behoben.

Installieren, Einrichten, Upgrade durchführen und Deinstallieren

January 25, 2024

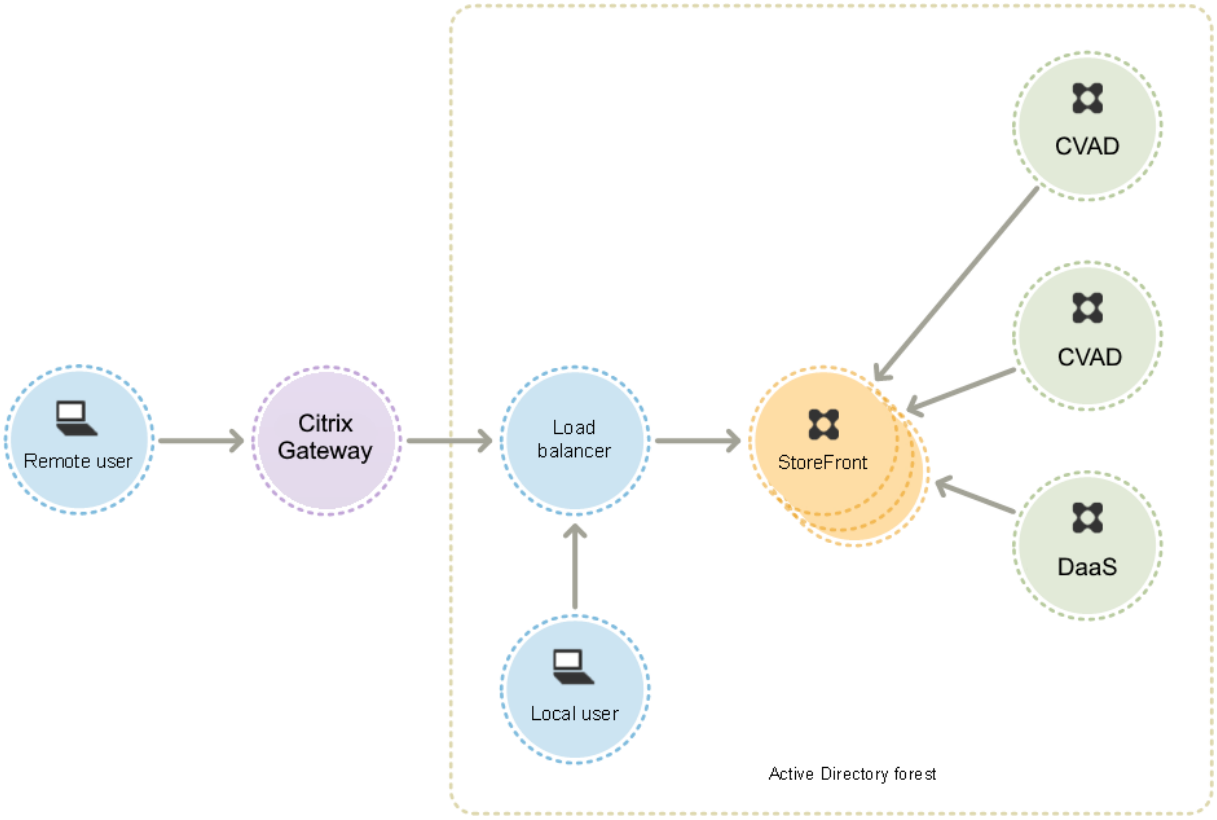
Aufgabe	Detail
StoreFront-Bereitstellung planen	Übersicht über die Komponenten einer StoreFront-Bereitstellung
Benutzerzugriffsoptionen	Übersicht darüber, wie Benutzer auf Ihre Stores zugreifen können
Systemanforderungen	Vergewissern Sie sich, dass Sie über die Voraussetzungen für die Installation von StoreFront verfügen.
Installieren von StoreFront	StoreFront auf einem neuen Server installieren
StoreFront mit HTTPS schützen	Clientzugriff auf StoreFront mit HTTPS verschlüsseln
Sichern der StoreFront-Bereitstellung	StoreFront für mehr Sicherheit konfigurieren
Neue Bereitstellung erstellen	Neuen StoreFront-Server mit einem neuen Store konfigurieren
Vorhandener Servergruppe beitreten	Neuen StoreFront-Server für vorhandenen Servergruppe konfigurieren
Aktualisieren von StoreFront	StoreFront-Server, auf dem eine ältere Version ausgeführt wird, aktualisieren
CEIP	Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) –teilnehmen oder abmelden
Citrix Analytics-Dienst	StoreFront für das Senden von Daten an den Citrix Analytics Service konfigurieren
Deinstallieren Sie StoreFront	StoreFront vom Server entfernen
Server auf die Werkseinstellungen zurücksetzen	Alle StoreFront-Einstellungen löschen, damit es neu konfiguriert werden kann

StoreFront-Bereitstellung planen

May 31, 2024

StoreFront kann in Ihre Citrix Virtual Apps and Desktops-Bereitstellungen integriert werden und bietet Benutzern einen zentralen Self-Service-Zugriffspunkt für ihre Desktops und Anwendungen.

Die Abbildung zeigt eine typische StoreFront-Bereitstellung.



Active Directory

StoreFront nutzt Active Directory zur Authentifizierung von Benutzern, für die Suche von Gruppenmitgliedschaften und anderen Details und zum Synchronisieren von Daten zwischen StoreFront-Servern.

Für Einzelserverbereitstellungen können Sie StoreFront auf einem Server installieren, der nicht in einer Domäne ist, bestimmte Funktionen stehen dann aber nicht zur Verfügung. Sonst müssen StoreFront-Server in der Active Directory-Domäne mit den Benutzerkonten residieren oder in einer Domäne, die mit dieser eine Vertrauensstellung hat, außer Sie aktivieren die Delegierung der Authentifizierung an die Citrix Virtual Apps and Desktops-Sites bzw. -Farmen. Alle StoreFront-Server einer Gruppe müssen in der gleichen Domäne sein.

StoreFront-Servergruppen

StoreFront kann auf einem einzelnen Server oder als Multiserverbereitstellung ("StoreFront-Servergruppe") konfiguriert werden. Servergruppen bieten nicht nur zusätzliche Kapazität, sondern auch eine höhere Verfügbarkeit. StoreFront stellt sicher, dass die Konfigurationsinformationen und Details zu den Anwendungsabonnements der Benutzer auf allen Servern in einer Servergruppe gespeichert und repliziert werden. Wenn ein StoreFront-Server aus irgendeinem Grund nicht verfügbar ist, können Benutzer weiter auf ihre Stores auf den übrigen Servern zugreifen. Die Konfigurations- und Abonnementsdaten auf dem ausgefallenen Server werden automatisch aktualisiert, wenn er wieder mit der Servergruppe verbunden wird. Abonnementdaten werden aktualisiert, wenn der Server wieder online geht, Sie müssen jedoch Konfigurationsänderungen verteilen, die vom Server verpasst wurden. Falls aufgrund eines Hardwarefehlers der Server ersetzt werden muss, installieren Sie StoreFront auf einem neuen Server und fügen ihn der vorhandenen Servergruppe hinzu. Der neue Server wird automatisch konfiguriert und mit den Anwendungsabonnements der Benutzer aktualisiert, wenn er der Servergruppe beitritt.

Citrix empfiehlt ein Maximum von sechs Servern pro Servergruppe. Bei mehr als sechs Servern überwiegt der Mehraufwand für die Datensynchronisierung den Nutzen der zusätzlichen Server und die Leistung fällt ab.

StoreFront-Servergruppenbereitstellungen werden nur unterstützt, wenn die Verbindungen zwischen Servern in einer Servergruppe eine Latenz von weniger als 40 ms (bei deaktivierten Abonnements) oder weniger als 3 ms (bei aktivierten Abonnements) haben. Idealerweise sollten alle Server in einer Servergruppe an demselben Standort sein (Rechenzentrum, Availability Zone). Servergruppen können aber über Standorte innerhalb derselben Region verteilt sein, vorausgesetzt, dass Verbindungen zwischen Servern in der Gruppe diese Latenzkriterien erfüllen. Beispiele hierfür sind Servergruppen, die Availability Zones innerhalb einer Cloudregion oder Rechenzentren in einer Metropolregion umfassen. Beachten Sie, dass die Latenz zwischen den Zonen je nach Cloudanbieter unterschiedlich ist. Citrix empfiehlt nicht, für die Notfallwiederherstellung standortübergreifende Konfigurationen zu verwenden, sie kann jedoch für eine hohe Verfügbarkeit geeignet sein.

Lastausgleich

Für mehrere Server in einer StoreFront-Servergruppe müssen Sie den externen Lastausgleich konfigurieren. Verwenden Sie einen Load Balancer mit integrierten Monitoren und Sitzungspersistenz, z. B. Citrix ADC. Weitere Informationen zum Lastausgleich mit Citrix ADC finden Sie unter Lastausgleich.

Citrix Gateway für Remotezugriff

Wenn Sie beabsichtigen, Zugriff auf StoreFront von außerhalb des Unternehmensnetzwerks zu ermöglichen, ist ein Citrix Gateway erforderlich, um sichere Verbindungen für Remotebenutzer

zu gewährleisten. Stellen Sie Citrix Gateway außerhalb des Unternehmensnetzwerks bereit und trennen Sie es vom öffentlichen und internen Netzwerk durch Firewalls. Stellen Sie sicher, dass Citrix Gateway auf die Active Directory-Gesamtstruktur mit den StoreFront-Servern zugreifen kann.

Global Server Load Balancing

In großen Citrix-Bereitstellungen befinden sich StoreFront- und NetScaler-Bereitstellungen möglicherweise in mehreren Datencentern. Mit Global Server Load Balancing (GSLB) können Sie eine einzelne globale URL konfigurieren, die der GSLB an die spezifische URL eines Gateways in einer der Regionen weiterleitet. In der Regel wählt GSLB auf der Grundlage eines Lastausgleichsalgorithmus wie Round Trip Time (RTT) oder Static Proximity das nächstgelegene Gateway.

Beispiel für drei regionale Gateways:

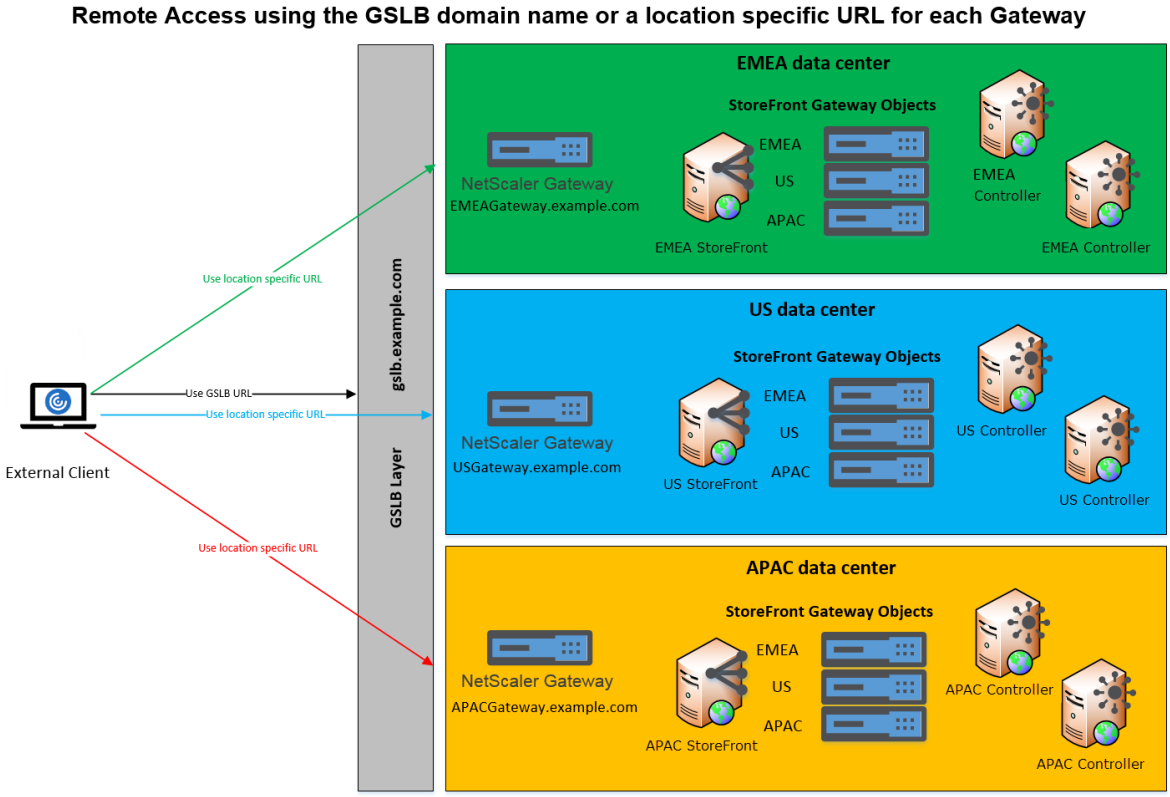
`emeagateway.example.com` –Gateway Europa

`usgateway.example.com` –Gateway USA

`apacgateway.example.com` –Gateway Asien-Pazifik

Plus GSLB

`gslb.example.com`



Bevor Sie GSLB konfigurieren, prüfen Sie, welche Serverzertifikate installiert sind und wie die DNS-Auflösung in Ihrem Unternehmen erfolgt. Alle URLs, die Sie in der Citrix Gateway- und StoreFront-Bereitstellung verwenden möchten, müssen in den Serverzertifikaten aufgelistet sein.

StoreFront besitzt keinen integrierten Mechanismus zum Synchronisieren der Konfiguration zwischen Servergruppen. Der Administrator muss stattdessen jede StoreFront-Servergruppe gleich konfigurieren, damit die Benutzer unabhängig von der Servergruppe, mit der sie verbunden sind, ein einheitliches Erlebnis erhalten.

StoreFront kann Abonnements (Favoriten) zwischen Servergruppen regelmäßig synchronisieren, siehe Abonnementsynchronisierung.

Benutzerzugriff

Siehe Benutzerzugriffsoptionen.

Benutzerzugriffsoptionen

May 31, 2024

Es gibt drei verschiedene Methoden, wie Benutzer auf StoreFront-Stores zugreifen können.

- Lokal installierte Citrix Workspace-App: Benutzer mit kompatiblen Versionen von Citrix Receiver bzw. der Citrix Workspace-App können direkt von der Citrix Workspace-App-Benutzeroberfläche auf StoreFront-Stores zugreifen. Dies bietet die beste Benutzererfahrung und den größten Funktionsumfang.
- Citrix Workspace-App für HTML5: Benutzer mit kompatiblen Webbrowsern können auf StoreFront-Stores zugreifen, indem sie zur Website des Stores gehen. Die Benutzer benötigen standardmäßig außerdem eine kompatible Version der Citrix Workspace-App, um auf ihre Desktops und Anwendungen zuzugreifen (Hybridstart). Sie können Ihre Website jedoch so konfigurieren, dass die Benutzer über ihren Browser und ohne installierte Citrix Workspace-App auf ihre Ressourcen zugreifen können.
- XenApp Services-URLs: Benutzer mit älteren Citrix Clients, die nicht aktualisiert werden können, können über die XenApp Services-URL auf Stores zugreifen. Wenn Sie einen neuen Store erstellen, wird die XenApp Services-URL standardmäßig aktiviert.

Lokal installierte Citrix Workspace-App

Der Zugriff auf Stores über die lokal installierte Citrix Workspace-App bietet die beste Benutzererfahrung. Informationen dazu, mit welchen Citrix Workspace-App-Versionen Sie so auf Stores

zugreifen können, finden Sie unter Systemanforderungen.

Die Citrix Workspace-App verwendet interne und externe URLs als Beacons. Anhand des Versuchs, diese Beacons zu kontaktieren, kann die Citrix Workspace-App ermitteln, ob ein Benutzer mit dem lokalen oder einem öffentlichen Netzwerk verbunden ist. Wenn ein Benutzer auf einen Desktop oder eine Anwendung zugreift, werden die Standortinformationen an den Server mit der Ressource weitergegeben, sodass die entsprechenden Verbindungsinformationen an die Citrix Workspace-App zurückgegeben werden können. Dadurch wird sichergestellt, dass die Benutzer nicht aufgefordert werden, sich neu anzumelden, wenn sie auf einen Desktop oder eine Anwendung zugreifen. Weitere Informationen finden Sie unter Konfigurieren von Beacons.

Store zur Workspace-App hinzufügen

Nach der Installation müssen in der Citrix Workspace-App die Verbindungsinformationen für die Stores konfiguriert werden, über die Benutzern Desktops und Anwendungen bereitgestellt werden. Sie können Benutzern die Konfiguration erleichtern, indem Sie die erforderlichen Informationen über eine der folgenden Methoden bereitstellen.

> **Wichtig:**
>
> Standardmäßig erfordert die Citrix Workspace-App HTTPS-Verbindungen zu Stores. Wenn StoreFront nicht für HTTPS konfiguriert ist, müssen Benutzer zusätzliche Konfigurationsschritte ausführen, um HTTP-Verbindungen zu verwenden. Citrix empfiehlt dringend, keine ungeschützten Benutzerverbindungen mit StoreFront in einer Produktionsumgebung zu aktivieren. Weitere Informationen finden Sie unter Store-Konfigurationsparameter in der Dokumentation der Citrix Workspace-App für Windows.

Manuelle Konfiguration Benutzer können die Citrix Workspace-App mit ihrem Store verbinden, indem sie Store-URLs in die Citrix Workspace-App eingeben. Weitere Informationen finden Sie in der Dokumentation zur Citrix Workspace-App.

Provisioningdateien Sie können Provisioningdateien mit den Verbindungsinformationen für die Stores der Benutzer bereitstellen. Nach der Installation der Citrix Workspace-App öffnen die Benutzer die CR-Datei, um Konten für die Stores automatisch zu konfigurieren. Die Website bietet den Benutzern standardmäßig eine Provisioningdatei für den einen Store, für den die Site konfiguriert ist. Sie könnten die Benutzer auffordern, die Websites für die Stores zu besuchen, auf die sie zugreifen möchten, und von dort Provisioningdateien herunterzuladen. Für eine größere Kontrolle können Sie alternativ die Citrix StoreFront-Verwaltungskonsole zum Generieren von Provisioningdateien verwenden, die Verbindungsdetails für einen oder mehrere Stores enthalten. Sie können dann diese Dateien an die entsprechenden Benutzer verteilen. Weitere Informationen finden Sie unter Exportieren der Store-Provisioningdateien für Benutzer.

Automatisch generierte Setup-URLs Für macOS-Benutzer können Sie mit dem Setup URL Generator der Citrix Workspace-App für Mac eine URL mit den Verbindungsinformationen für einen Store erstellen. Nach der Installation der Citrix Workspace-App klicken die Benutzer auf die URL, um ein Konto für den Store automatisch zu konfigurieren. Geben Sie die Bereitstellungsinformationen in das Tool ein und generieren Sie eine URL, die Sie an die Benutzer senden können.

E-Mail-basierte Kontenermittlung Bei der E-Mail-basierten Kontenermittlung müssen die Benutzer die Zugriffsinformationen für ihre Stores nicht kennen. Stattdessen geben sie während der Citrix Workspace-App-Erstkonfiguration ihre E-Mail-Adresse an. Einzelheiten zur Einrichtung finden Sie unter E-Mail-basierte Kontenermittlung.

Global App Configuration Service

Verwenden Sie den Global App Config Service, um die Citrix Workspace-App für Ihre StoreFront-Stores zu konfigurieren. Siehe Einstellungen für On-Premises-Stores konfigurieren.

Citrix Workspace-App für HTML5

Alternativ zur lokal installierten Workspace-App können Benutzer mit der Workspace-App für HTML5 über einen Webbrowser auf den Store zugreifen. Benutzer können ihre Ressourcen auf zweierlei Art starten.

1. Ressourcen werden in der lokal installierten Citrix Workspace-App gestartet. Dies wird als Hybrid-Launch bezeichnet. Er bietet den Benutzern die beste Erfahrung, da die vollständige Betriebssystemintegration genutzt werden kann. Weitere Informationen finden Sie unter Hybridstart
2. Im Browser. Auf diese Weise können Benutzer auf Ressourcen zugreifen, ohne lokale Software installieren zu müssen.

Die Standardkonfiguration erfordert die lokale Installation der Citrix Workspace-App für den Hybridstart. Sie können die Konfiguration so ändern, dass Ressourcen entweder immer im Browser gestartet werden oder dass der Benutzer die Wahl hat. Siehe Workspace-App bereitstellen.

Wenn der Administrator **Receiver für HTML5 verwenden, wenn lokaler Receiver nicht verfügbar ist** ausgewählt hat, kann der Benutzer beim ersten Öffnen der Store-Website in seinem Browser auf **Lightversion verwenden** klicken, um Ressourcen in seinem Webbrowser zu starten.

Voraussetzungen für das Öffnen von Ressourcen im Browser

Für Benutzer im internen Netzwerk ist der Zugriff über die Citrix Workspace-App für HTML5 auf Ressourcen, die von Citrix Virtual Apps and Desktops bereitgestellt werden, standardmäßig deaktiviert. Sie aktivieren den lokalen Zugriff auf Desktops und Anwendungen über die Citrix Workspace-App für HTML5, indem Sie die Richtlinie für ICA-WebSockets-Verbindungen auf den Citrix Virtual Apps and Desktops-Servern aktivieren. Citrix Virtual Apps and Desktops verwendet Port 8008 für Verbindungen mit der Citrix Workspace-App für HTML5. Stellen Sie sicher, dass Firewalls und andere Netzwerkgeräte den Zugriff auf diesen Port zulassen. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "WebSockets".

Damit Ressourcen von Citrix Virtual Apps and Desktops gestartet werden können, konfigurieren Sie TLS-Verbindungen mit den VDAs, auf denen die Apps und Desktops gehostet werden. Bei Remoteverbindungen über ein Citrix Gateway können Ressourcen über die Citrix Workspace-App für HTML5 ohne Konfiguration von TLS-Verbindungen mit dem VDA gestartet werden.

Hybridstart

Wenn Benutzer die Citrix Workspace für HTML5 zunächst über ihren Browser öffnen, Apps dann aber in der lokal installierten Citrix Workspace-App starten, wird dies als "Hybridstart"bezeichnet. Es gibt eine Reihe von Möglichkeiten, wie die Website mit der lokal installierten Workspace-App kommunizieren kann, um Ressourcen zu starten.

Citrix Workspace Launcher

Wenn ein Benutzer mit einem unterstützten Betriebssystem und Browser eine StoreFront-Website aufruft, versucht die Citrix Workspace-App für HTML5, den Citrix Workspace Launcher aufzurufen. Wenn eine unterstützte Version der Citrix Workspace-App installiert ist, benachrichtigt die App StoreFront. Die Citrix Workspace-App für HTML5 speichert dies und verwendet Citrix Workspace Launcher für App-Starts.

Die Store-Website ruft Citrix Workspace Launcher unter Windows, Mac und Linux auf, wenn die folgenden Browser verwendet werden:

- Firefox 52 oder höher
- Chrome 42 oder höher
- Safari 12 oder höher
- Edge 25 oder höher

Citrix Workspace Launcher erfordert die folgenden Mindestversionen von Citrix Receiver bzw. der Citrix Workspace-App.

- Receiver für Windows 4.3 oder höher
- Receiver für Mac 12.0 oder höher
- Workspace-App für Linux 2003 oder höher

Wenn der Workspace App Launcher nicht verfügbar ist oder der Benutzer sein Öffnen nicht zulässt, kann er die lokal installierte Citrix Workspace-App nicht erkennen. Der Benutzer kann es erneut versuchen oder auf **Bereits installiert** klicken. Im letzteren Fall werden Apps dann wieder mithilfe von ICA-Dateien gestartet. Der Benutzer kann es später erneut versuchen, indem im Einstellungsfenster auf **Citrix Workspace-App ändern** klickt.

Wenn Sie mehrere aktive StoreFront-Servergruppen hinter einem globalen Serverlastenausgleich verwenden, schlägt der Citrix Workspace Launcher möglicherweise zeitweise fehl. Um dies zu vermeiden, müssen Sie das Global Server Load Balancing so konfigurieren, dass die Benutzerwebsitzung für eine StoreFront-Servergruppe während der gesamten Lebensdauer des Clienterkennungsprozesses persistent ist, siehe CTX460312. Stellen Sie alternativ Citrix Workspace-Weberweiterungen bereit.

Wenn Sie über ein Citrix Gateway eine Verbindung zur Website herstellen, verwendet der Citrix Workspace Launcher das HDX-Routing des Gateways, um Anfragen von der Citrix Workspace-App zurück an den StoreFront-Server weiterzuleiten. Wenn das Gateway **nur für Authentifizierung** konfiguriert ist (nicht für HDX-Routing), funktioniert Citrix Workspace Launcher nicht. Aktivieren Sie entweder HDX-Routing oder stellen Sie Citrix Workspace-Weberweiterungen bereit.

Citrix Workspace-Weberweiterungen (Tech Preview)

Die Citrix Workspace-Weberweiterungen sind Erweiterungen für gebräuchliche Browser, die die Benutzererfahrung beim Erkennen einer lokal installierten Citrix Workspace-App und beim Starten virtueller Apps und Desktops verbessern. Im Vergleich zum Citrix Workspace Launcher bietet dies eine bessere Benutzererfahrung und vermeidet Probleme mit Global Server Load Balancing.

Gehen Sie wie folgt vor, um die browsererweiterungsbasierte Clienterkennung zu aktivieren:

- Aktivieren Sie das Feature auf dem StoreFront-Server.
- Stellen Sie die Browsererweiterung auf den Clientgeräten bereit.
- Stellen Sie die Citrix Workspace-App für Windows 2303, Mac 2304 oder Linux 2302 oder höher bereit.

Wenn ein Benutzer zum ersten Mal eine Storewebsite auf einer unterstützten Plattform aufruft, wird der Benutzer aufgefordert, die lokal installierte Workspace-App zu erkennen. Zuerst wird versucht, die Weberweiterung zu verwenden, und wenn dies fehlschlägt, wird Citrix Workspace Launcher versucht. Bestehende Benutzer, die die Workspace-App-Erkennung bereits abgeschlossen haben, können zu den **Kontoeinstellungen**gehen und auf **Citrix Workspace-App ändern** klicken, um die Workspace-App erneut zu erkennen.

Diese Funktion ist standardmäßig deaktiviert. Administratoren können dieses Feature mit dem folgenden PowerShell-Skript auf einem StoreFront-Server aktivieren: `Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension" -IsEnabled $True`.

Internet Explorer

Wenn ein Benutzer die Store-Website erstmals über Internet Explorer öffnet, wird er aufgefordert, die Citrix Workspace-App zu installieren. Diese enthält das Citrix ICA-Client-Add-On für Internet Explorer. Sobald dieses installiert ist, wird es verwendet, um Apps und Desktops über die lokal installierte Citrix Workspace-App zu starten.

ICA-Dateidownload

Erkennt die Citrix Workspace-App für HTML5 eine lokal installierte Citrix Workspace-App nicht auf eine andere Weise, lädt sie beim Starten einer App oder eines Desktops eine ICA-Datei herunter. Der Benutzer kann diese mit der lokal installierten Citrix Workspace-App öffnen.

Ressourcenverknüpfungen

Sie können URLs generieren, die den Zugriff auf Desktops und Anwendungen im Store ermöglichen. Betten Sie diese Links in Websites ein, die im internen Netzwerk gehostet werden, damit Benutzer schnell auf Ressourcen zugreifen können. Die Benutzer klicken auf einen Link und werden an die Store-Website weitergeleitet, wo sie sich anmelden, wenn sie dies nicht bereits getan haben. Die Store-Website startet die Ressource automatisch. Weitere Informationen zum Erstellen von Ressourcenverknüpfungen finden Sie unter Websiteverknüpfungen.

Wenn Sie eine Anwendungsverknüpfung erstellen, stellen Sie sicher, dass keine andere Anwendung im Store denselben Namen hat. Verknüpfungen können nicht zwischen mehreren Instanzen einer Anwendung mit dem gleichen Namen unterscheiden. Gleichermaßen können Sie, wenn Sie mehrere Instanzen eines Desktops in einer Desktopgruppe im Store zur Verfügung stellen, keine separate Verknüpfung für jede Instanz erstellen. Verknüpfungen können keine Befehlszeilenparameter an Anwendungen weitergeben.

Zum Erstellen von Anwendungsverknüpfungen konfigurieren Sie StoreFront mit den URLs der internen Websites, von denen die Verknüpfungen gehostet werden. Wenn ein Benutzer auf eine Anwendungsverknüpfung auf einer Website klickt, prüft StoreFront diese Website anhand der von Ihnen eingegebenen Liste der URLs, um sicherzustellen, dass die Anforderung von einer vertrauenswürdigen Website stammt.

Benutzeroberfläche anpassen

Citrix StoreFront bietet einen Mechanismus zum Anpassen der Benutzeroberfläche. Dies gilt unabhängig davon, ob über die Citrix Workspace-App oder einen Webbrowser auf einen Store zugegriffen wird. Sie können Zeichenfolgen anpassen, das Cascading Stylesheet und die JavaScript-Dateien. Sie können außerdem einen benutzerdefinierten Bildschirm vor oder nach der Anmeldung hinzufügen, ebenso wie Sprachpakete. Weitere Informationen finden Sie unter Benutzeroberfläche anpassen.

XenApp Services-URLs

Benutzer älterer Citrix Clients, die nicht aktualisiert werden können, können auf Stores zugreifen, indem sie ihren Client mit der XenApp Services-URL für den Store konfigurieren. Sie können auch Zugriff auf Stores über XenApp Services-URLs von domänengebundenen Desktopgeräten und umfunktionierten PCs, auf denen Citrix Desktop Lock ausgeführt wird, aktivieren. In diesem Zusammenhang ist die Einbindung der Geräte in eine Domäne in der Active Directory-Gesamtstruktur gemeint, die die StoreFront-Server enthält.

StoreFront unterstützt die Passthrough-Authentifizierung mit Proximitykarten über die Citrix Workspace-App bei XenApp Services-URLs. Citrix Ready-Partnerprodukte verwenden die Citrix Fast Connect-API zur Leitung von Benutzeranmeldungen über Citrix Receiver bzw. die Citrix Workspace-App für Windows für die Verbindung mit Stores mit der XenApp Services-URL. Die Benutzer authentifizieren sich bei Arbeitsstationen mit Proximitykarten und werden schnell mit per Citrix Virtual Apps and Desktops bereitgestellten Desktops und Anwendungen verbunden. Weitere Informationen finden Sie in der aktuellen Dokumentation zu Citrix Workspace.

Wenn Sie einen neuen Store erstellen, wird die XenApp Services-URL für den Store standardmäßig aktiviert. Die XenApp Services-URL für den Store hat das Format http[s]://serveraddress/Citrix/storename/PNAgent/c wobei “serveraddress”der vollqualifizierte Domänenname des Servers oder der Lastausgleichsumgebung für die StoreFront-Bereitstellung ist und “storename”der Name, den Sie beim Erstellen des Stores angegeben haben. Dies ermöglicht die Verwendung von Citrix Workspace-App-Instanzen, die nur über das PNAgent-Protokoll eine Verbindung mit StoreFront herstellen können. Eine Liste der Clients, mit denen Sie über XenApp Services-URLs auf Stores zugreifen können, finden Sie unter Anforderungen für Benutzergeräte.

Wichtige Überlegungen

XenApp Services-URLs dienen zur Unterstützung von Benutzern, die nicht auf die Citrix Workspace-App aktualisieren können, und für Szenarien, in denen alternative Zugriffsmethoden nicht verfügbar sind. Bei der Entscheidung, ob Sie Benutzern Zugriff auf Stores über XenApp Services-URLs gewähren möchten, sollten Sie die folgenden Einschränkungen berücksichtigen.

- Die XenApp Services-URL für einen Store kann nicht geändert werden.
- Sie können die Einstellungen einer XenApp Services-URL nicht durch Bearbeiten der Konfigurationsdatei config.xml ändern.
- XenApp Services-URLs unterstützen die explizite, Domänen-Passthrough-Authentifizierung mit Smartcards und die Passthrough-Authentifizierung mit Smartcards. Die explizite Authentifizierung ist standardmäßig aktiviert. Nur eine Authentifizierungsmethode kann für jede XenApp Services-URL konfiguriert werden und pro Store ist nur eine URL verfügbar. Wenn Sie mehrere Authentifizierungsmethoden benötigen, müssen Sie separate Stores mit einer XenApp Services-URL für jede Authentifizierungsmethode erstellen. Die Benutzer müssen dann eine Verbindung mit dem für ihre Authentifizierungsmethode geeigneten Store herstellen. Weitere Informationen finden Sie unter XML-basierte Authentifizierung.
- Workspace Control ist standardmäßig für XenApp Services-URLs aktiviert und kann nicht konfiguriert oder deaktiviert werden.
- Benutzeranforderungen zum Ändern von Kennwörtern werden direkt über die Citrix Virtual Apps and Desktops-Server, die Desktops und Anwendungen für den Store bereitstellen, an den Domänencontroller geleitet. Der StoreFront-Authentifizierungsdienst wird dabei umgangen.

Systemanforderungen

May 31, 2024

Lesen Sie vor der Installation von StoreFront den Artikel StoreFront-Bereitstellung planen.

StoreFront-Serveranforderungen

Software

Nach entsprechenden Tests bietet Citrix nun Unterstützung für StoreFront auf folgenden Plattformen:

- Windows Server 2022 (Standard- und Datacenter-Editionen)
- Windows Server 2019 (Standard- und Datacenter-Editionen)
- Windows Server 2016 (Standard- und Datacenter-Editionen)

> **Hinweis:**
>
> StoreFront erfordert die Windows-Desktoperfahrung und kann daher nicht auf Windows Server Core installiert werden.

Alle StoreFront-Server in einer Servergruppe müssen dieselbe Betriebssystemversion, Sprache und dasselbe Gebietsschema verwenden.

Das Aktualisieren des Betriebssystems eines Servers, auf dem StoreFront ausgeführt wird, wird nicht unterstützt. Citrix empfiehlt die Installation von StoreFront auf einer neuen Installation des Betriebssystems.

Bevor Sie StoreFront installieren können, müssen die folgenden Windows-Funktionen auf dem Webserver aktiviert sein. Diese Komponenten sind standardmäßig bei Windows-Neuinstallationen aktiviert, es ist also nur dann eine Aktion erforderlich, wenn sie explizit deinstalliert wurden.

- NET-Framework-45-Features
  - NET-Framework-45-Core
- PowerShellRoot
  - PowerShell

Wenn die installierte Version von .NET Framework älter als 4.7.2 ist, wird .NET Framework 4.7.2 automatisch vom Installationsprogramm installiert. Beachten Sie, dass hierfür die Windows-Funktion NET-Framework-45-Core bereits installiert sein muss.

Wenn das StoreFront-Installationsprogramm erkennt, dass eines der folgenden Windows-Features fehlt, werden sie automatisch installiert:

- Web-Server
  - Web-WebServer
    - Web-Common-Http
      - Web-Default-Doc
      - Web-Http-Errors
      - Web-Static-Content
      - Web-Http-Redirect
    - Web-Health
      - Web-Http-Logging
    - Web-Security
      - Web-Filtering
      - Web-Basic-Auth
      - Web-Windows-Auth
    - Web-App-Dev
      - Web-Net-Ext45
      - Web-AppInit
      - Web-Asp-Net45

        - Web-ISAPI-Ext
        - Web-ISAPI-Filter
    - Web-Mgmt-Tools
        - Web-Mgmt-Console
    - Web-Scripting-Tools
- NET-Framework-45-Features
    - NET-Framework-45-ASPNET
    - NET-WCF-Services45
        - NET-WCF-TCP-PortSharing45

Es ist möglich, die IIS-Website vor der Installation von StoreFront in ein anderes Verzeichnis oder Laufwerk zu verschieben. Der relative Pfad zu StoreFront in IIS muss auf allen Servern in einer Servergruppe identisch sein.

Hardware

StoreFront-Server müssen die folgenden Anforderungen erfüllen:

- Prozessor: Mindestens 2 virtuelle CPUs, empfohlen 4 virtuelle CPUs
- RAM: 4 GB plus 700 Byte pro verfügbarer Ressource pro Benutzer.
- Speicher:
    - 250 MB für StoreFront selbst.
    - 30 MB für jeden Store (sofern eine Website pro Store).
    - Für jeden Store mit aktivierten Favoriten 5 MB plus 8 MB für jeweils 1000 Favoriten.
    - Ausreichend Speicherplatz für IIS-Protokolldateien gemäß Ihren Anforderungen (siehe Microsoft-Dokumentation zur Verwaltung des IIS-Protokolldateispeicher).
    - Ausreichend Speicherplatz für StoreFront-Diagnoseprotokolle. Standardmäßig speichert StoreFront 1 GB an Protokollen pro Dienst. Eine StoreFront-Bereitstellung umfasst in der Regel einen Roamingdienst plus 3 Dienste pro Store (Store Service, Auth Service und Receiver für Webdienst). Siehe Problembehandlung bei StoreFront.

Netzwerk

StoreFront verwendet die folgenden Ports für die Kommunikation. Stellen Sie sicher, dass Firewalls und andere Netzwerkgeräte den Zugriff auf diese Ports zulassen.

- Die TCP-Ports 80 und 443 werden von Clients verwendet, um über HTTP- bzw. HTTPS-Kommunikation eine Verbindung zu StoreFront herzustellen.

- TCP-Port 808 wird für die Kommunikation zwischen StoreFront-Servern in einer Servergruppe verwendet.
- Ein nach dem Zufallsprinzip unter allen nicht reservierten Ports ausgewählter TCP-Port wird für die Kommunikation zwischen den StoreFront-Servern in eine Servergruppe verwendet. Wenn Sie StoreFront installieren, wird eine Windows-Firewallregel konfiguriert, die den Zugriff auf die ausführbare StoreFront-Datei gestattet. Da der Port jedoch nach dem Zufallsprinzip zugewiesen wird, müssen Sie sicherstellen, dass Firewalls oder andere Geräte im internen Netzwerk keinen Datenverkehr an einen der nicht zugewiesenen TCP-Ports blockieren.
- TCP-Port 8008 wird (wo aktiviert) von der Citrix Workspace-App für HTML5 bzw. unterstützten Versionen der Citrix Workspace-App für die Kommunikation zwischen lokalen Benutzern im internen Netzwerk und den Servern verwendet, die die Desktops und Anwendungen bereitstellen.

StoreFront unterstützt reine IPv6-Netzwerke und Umgebungen mit dualem Stapel (IPv4 und IPv6).

Active Directory

Für viele StoreFront-Features muss der Windows-Server, auf dem StoreFront installiert ist, einer Active Directory-Domäne beitreten.

Wenn Sie StoreFront auf einem Server installieren, der nicht in eine Domäne eingebunden ist, sind die folgenden Features nicht verfügbar:

- Servergruppen
- Favoriten
- Andere Authentifizierungsmethoden als expliziter Benutzername und Kennwort, entweder direkt an StoreFront oder über ein Gateway. Sie müssen StoreFront so konfigurieren, dass die Authentifizierung an den Delivery Controller delegiert wird.

Speichern von Abonnementdaten mit Microsoft SQL Server

Optional können Sie Abonnementdaten mit Microsoft SQL Server speichern. StoreFront unterstützt hierfür dieselben Microsoft SQL Server-Versionen wie die Datenbanken von Citrix Virtual Apps and Desktops. Informationen zu den Systemanforderungen für Citrix Virtual Apps and Desktops finden Sie unter Datenbanken.

Anforderungen an die Infrastruktur

Citrix hat StoreFront mit den folgenden Citrix Produktversionen getestet und unterstützt sie.

Citrix Virtual Apps and Desktops

StoreFront unterstützt die folgenden Versionen von Citrix Virtual Apps and Desktops:

- Citrix Virtual Apps and Desktops 7 2203 LTSR
- Citrix Virtual Apps and Desktops 7 2112
- Citrix Virtual Apps and Desktops 7 2109
- Citrix Virtual Apps and Desktops 7 2106
- Citrix Virtual Apps and Desktops 7 2103
- Citrix Virtual Apps and Desktops 7 2012
- Citrix Virtual Apps and Desktops 7 1912 LTSR
- XenApp and XenDesktop 7.15 LTSR

Weitere Informationen zur Verwendung des Release in einer LTSR-Umgebung (Long Term Service) und zu anderen häufig gestellten Fragen finden Sie in diesem Knowledge Center-Artikel.

Citrix Gateway

Die folgenden Versionen von Citrix Gateway können verwendet werden, um Benutzern in öffentlichen Netzwerken Zugriff auf StoreFront zu geben.

- Citrix Gateway 14.1 (unterstützt ab 2203 LTSR CU4)
- Citrix Gateway 13.1
- Citrix Gateway 13.0
- Citrix Gateway 12.1

Verbindungen über Citrix Gateway können per ICA-Proxy, Citrix Gateway-Plug-In oder clientloses VPN hergestellt werden.

Anforderungen für Benutzergeräte

StoreFront bietet Benutzern verschiedene Optionen für den Zugriff auf Desktops und Anwendungen. Citrix Benutzer können über eine lokal installierte Citrix Workspace-App auf Stores zugreifen oder die Citrix Workspace-App für HTML5 in ihrem Browser verwenden.

Lokal installierte Citrix Workspace-App

Sie können alle derzeit unterstützten Versionen der Citrix Workspace-App für den Zugriff auf StoreFront-Stores über interne Netzwerkverbindungen und über ein Citrix Gateway verwenden. Lebenszyklusdaten der Citrix Workspace-App finden Sie unter https://www.citrix.com/support/product-lifecycle/workspace-app.html.

Citrix Workspace-App für HTML5 in einem Browser

Sie können die Citrix Workspace-App für HTML5 verwenden, um über einen Webbrowser auf Ihren Store zuzugreifen. Apps und Desktops können über eine nativ installierte Citrix Workspace-App (bekannt als Hybridstart) oder im Webbrowser gestartet werden. Je nach Konfiguration Ihrer Website können Endbenutzer zwischen den beiden Startmethoden wechseln.

Verwenden Sie die neuesten Versionen der folgenden Browser.

Unter Windows:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Internet Explorer 11: Ab CU2 kann dies nur zum Durchsuchen des Stores verwendet werden, nicht zum Herstellen einer Verbindung zu Ressourcen.

Mac:

- Safari
- Google Chrome
- Mozilla Firefox

Unter Linux:

- Google Chrome
- Mozilla Firefox

Weitere Informationen zu den Anforderungen für die Verwendung der Citrix Workspace-App für HTML5 zum Herstellen einer Verbindung zu Ressourcen über einen Webbrowser finden Sie in der Dokumentation zur Citrix Workspace-App für HTML5.

Legacygeräte

Legacy Citrix Clients können XenApp Services-URLs verwenden, um auf StoreFront-Stores mit eingeschränkter Funktionalität zuzugreifen. XenApp Services-URLs bieten abwärtskompatible Legacyunterstützung für Verbindungen von Citrix Receiver 3.4 Enterprise und älteren Clients, die nur Verbindungen über PNAgent unterstützen.

Anforderungen für Smartcards

Citrix Workspace-App mit Smartcards verwenden

Citrix testet die Kompatibilität mit folgenden Smartcards: CAC (Common Access Card, US-Behörden), NIST PIV (National Institute of Standards and Technology Personal Identity Verification, USA) und diverse USB-Smartcardtoken. Sie können Kontaktkartenleser verwenden, die mit der Spezifikation "USB Chip/Smart Card Interface Devices"(CCID) übereinstimmen und vom deutschen Zentralen Kreditausschuss (ZKA) als Klasse 1-Smartcardleser klassifiziert wurden. Bei ZKA Klasse 1-Kontaktkartenlesern müssen Benutzer die Smartcards in den Leser einlegen. Andere Smartcardleser, einschließlich Klasse 2-Leser (mit Tastatur für die PIN-Eingabe), kontaktlose Leser und virtuelle TPM-Chip-basierte (Trusted Platform Module) Smartcards werden nicht unterstützt.

Für Windows-Geräte basiert die Smartcard-Unterstützung auf dem PC/SC-Standard (Personal Computer/Smart Card) von Microsoft. Als Mindestanforderung müssen Smartcards und Smartcardleser vom Betriebssystem unterstützt werden und über die Windows-Hardwarezertifizierung verfügen.

Weitere Informationen über Citrix-kompatible Smartcards und Middleware finden Sie unter Smartcards in der Citrix Virtual Apps and Desktops-Dokumentation und unter http://www.citrix.com/ready.

Anforderungen für Citrix Analytics

Sie können Citrix StoreFront so konfigurieren, dass die Citrix Workspace-App Daten an Citrix Analytics senden kann. Konfigurationsdetails werden unter Citrix Analytics Service beschrieben. Diese Funktionalität wird für die folgenden Szenarien unterstützt:

- Stores, auf die über Webbrowser zugegriffen wird.
- Stores, auf die über die Citrix Workspace-App 1903 für Windows oder höher zugegriffen wird.
- Stores, auf die über die Citrix Workspace-App 1901 für Linux oder höher zugegriffen wird.

Installieren von StoreFront

April 17, 2024

Vorbereiten der Installation

Führen Sie die nachfolgend beschriebenen Schritte aus, um StoreFront zu installieren und zu konfigurieren:

1. Lesen Sie die Informationen zu den Systemanforderungen.
2. Wenn Sie mit StoreFront Citrix Virtual Apps and Desktops-Ressourcen für Benutzer bereitstellen möchten, muss der StoreFront-Server Mitglied der Microsoft Active Directory-Domäne sein, in der Konten der Benutzer sind, oder in einer Domäne, die eine Vertrauensstellung mit der Domäne mit den Benutzerkonten hat.

   > **Wichtig:**
   >
   > - – Für Einzelserverbereitstellungen können Sie StoreFront auf einem Server installieren, der nicht in einer Domäne ist.
   > - StoreFront kann nicht auf einem Domänencontroller installiert werden.

3. Wenn Sie eine Multiserverbereitstellung konfigurieren möchten, können Sie optional auch eine Lastausgleichsumgebung für Ihre StoreFront-Server einrichten.

   Um Citrix ADC zum Lastausgleich zu verwenden, müssen Sie einen virtuellen Server als Proxyserver für die StoreFront-Server definieren. Weitere Informationen zum Konfigurieren von Citrix ADC für den Lastausgleich finden Sie unter Lastausgleich mit Citrix ADC.

4. Stellen Sie sicher, dass Firewalls und andere Netzwerkgeräte Zugriff auf den TCP-Port 80 oder 443 von innerhalb und außerhalb des Unternehmensnetzwerks gestatten. Stellen Sie außerdem sicher, dass Firewalls oder andere Geräte im internen Netzwerk keinen Datenverkehr an nicht zugewiesene TCP-Ports blockieren.

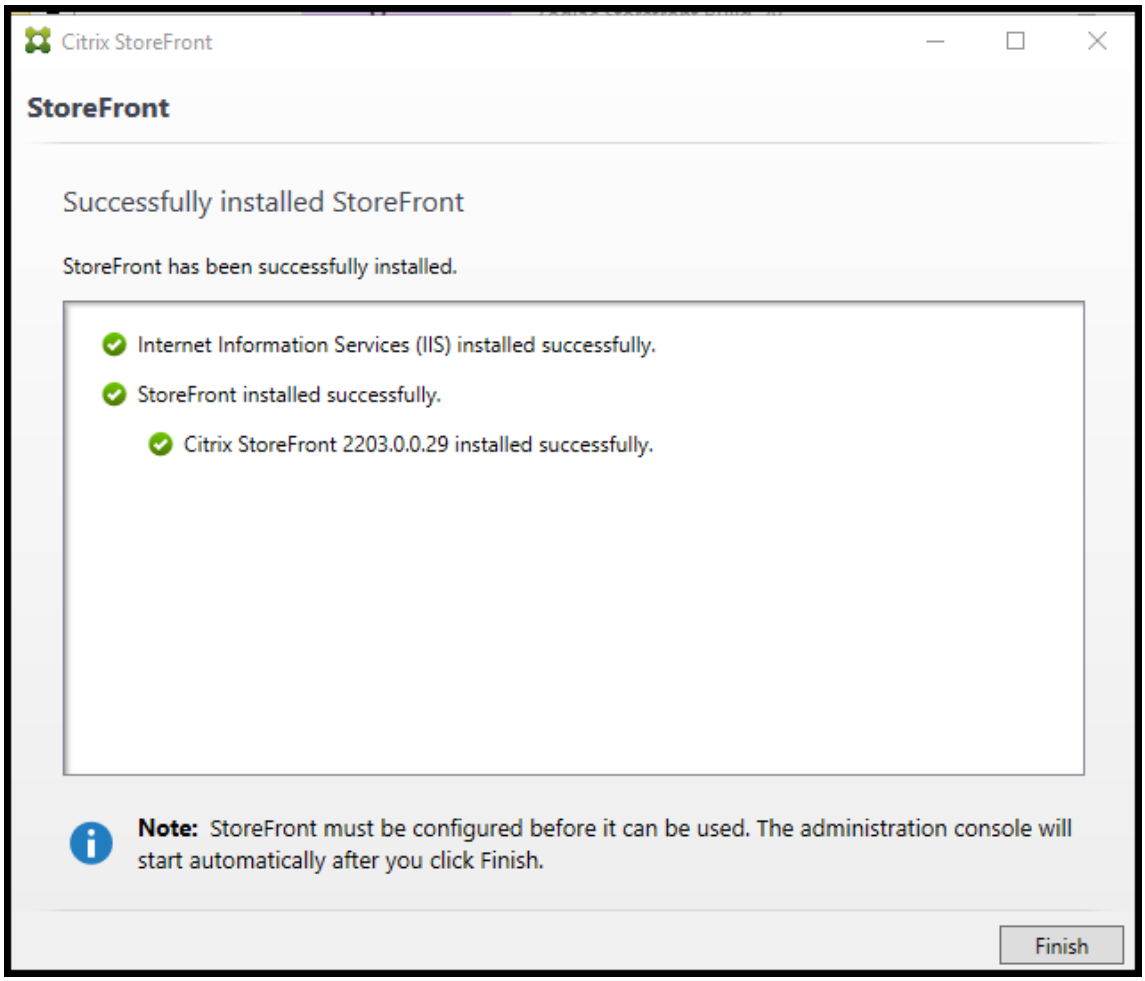
   Wenn Sie StoreFront installieren, wird eine Windows-Firewallregel konfiguriert, die den Zugriff auf die ausführbare StoreFront-Datei über einen zufällig unter allen nicht reservierten Ports ausgewählten TCP-Port ermöglicht. Dieser Port wird für die Kommunikation zwischen den StoreFront-Servern in einer Servergruppe verwendet.

Installieren von StoreFront

> **Wichtig!**
>
> Um potenzielle Fehler und Datenverlust beim Installieren von StoreFront zu vermeiden, müssen Sie sicherstellen, dass alle Anwendungen geschlossen sind und keine anderen Aufgaben oder Vorgänge auf dem Zielsystem ausgeführt werden.

1. Laden Sie das Installationsprogramm von der Downloadseite herunter.
2. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen bei StoreFront an.
3. Bei Verwendung von Windows 2016 installieren Sie dann .NET Framework 4.7.2 oder höher. Unter Windows Server 2019 und höher ist diese Windows-Funktion standardmäßig aktiviert.
4. Suchen Sie die Datei CitrixStoreFront-x64.exe und führen Sie sie als Administrator aus.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

6. Wenn die Seite “Voraussetzungen prüfen”angezeigt wird, klicken Sie auf **Weiter**.
7. Prüfen Sie auf der Seite “Bereit zur Installation”die Voraussetzungen und StoreFront-Komponenten für die Installation und klicken Sie auf **Installieren**.
8. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**.



9. StoreFront fordert möglicherweise einen Neustart an, um die Installation abzuschließen. Klicken Sie auf **Ja**, um den Computer jetzt neu zu starten.
10. Konfigurieren Sie Microsoft Internetinformationsdienste (IIS) für HTTPS. Anweisungen hierzu finden Sie unter StoreFront mit HTTPS schützen.

Installieren von StoreFront über eine Eingabeaufforderung

1. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen bei StoreFront an.
2. Stellen Sie sicher, dass die Voraussetzungen für die Installation von StoreFront erfüllt sind, bevor Sie StoreFront installieren. Weitere Informationen finden Sie unter Vorbereiten der Installation.

3. Navigieren Sie im Installationsmedium oder Downloadpaket zu der Datei CitrixStoreFront-x64.exe und kopieren Sie die Datei an einen temporären Speicherort auf dem Server.
4. Navigieren Sie in der Befehlszeile zu dem Ordner, der die Installationsdatei enthält, und geben Sie den folgenden Befehl ein:

```
CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR
    installationlocation] [-WINDOWS_CLIENT filelocation\filename.
    exe] [-MAC_CLIENT filelocation\filename.dmg]
<!--NeedCopy-->
```

   Verwenden Sie das Argument **-silent**, um eine automatische Installation von StoreFront und seiner Voraussetzungen durchzuführen. Standardmäßig wird StoreFront unter C:\Programme\Citrix\Receiver StoreFront\ installiert. Sie können einen anderen Speicherort für die Installation mit dem Argument **-INSTALLDIR** angeben, wobei *installationlocation* das Verzeichnis ist, in dem StoreFront installiert werden soll. Soll der Server Teil einer Servergruppe werden, müssen StoreFront-Installationsort und IIS-Websiteeinstellungen, physischer Pfad und Site-IDs in der Gruppe überall identisch sein.

   Wenn ein Benutzer einen Store in einem Webbrowser unter Windows oder macOS öffnet und dieser die Citrix Workspace-App nicht erkennt, wird der Benutzer standardmäßig aufgefordert, die für seine Plattform geeignete Version der Citrix Workspace-App von der Citrix-Website herunterzuladen und zu installieren. Sie können dieses Verhalten insofern ändern, dass Benutzer die Citrix Workspace-App-Installationsdateien von dem StoreFront-Server herunterladen. Weitere Informationen finden Sie unter Konfigurieren der Anzeige von Ressourcen für Benutzer.

   Wenn Sie eine solche Konfigurationsänderung beabsichtigen, geben Sie die Argumente **-WINDOWS_CLIENT** und **-MAC_CLIENT** an, um die Installationsdateien für Citrix Receiver bzw. die Citrix Workspace-App für Windows und Receiver bzw. die Citrix Workspace-App für Mac an den entsprechenden Speicherort in der StoreFront-Bereitstellung zu kopieren. Ersetzen Sie *filelocation* durch das Verzeichnis, das die zu kopierende Installationsdatei enthält, und *filename* durch den Namen der Installationsdatei. Die Installationsdateien für die Citrix Workspace-App für Windows und Citrix Receiver für Mac oder Citrix Workspace-App für Mac sind auf dem Installationsmedium für Citrix Virtual Apps and Desktops enthalten.

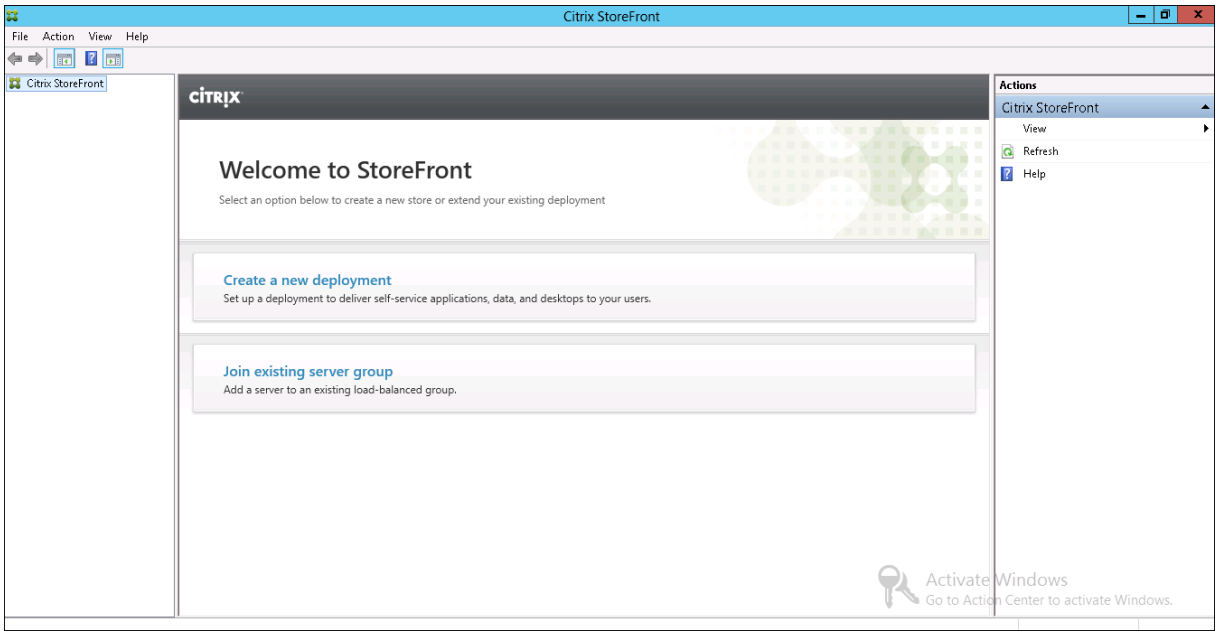
Installationsprotokolle

Weitere Informationen zu Protokolldateien finden Sie unter Installationsprotokolle.

Konfigurieren von StoreFront

Wenn Sie die Installation abgeschlossen haben, wird die Citrix StoreFront-Verwaltungskonsole automatisch gestartet. Sie können StoreFront auch über das Startmenü öffnen. Beim ersten Start der

Citrix StoreFront-Verwaltungskonsole sind drei Optionen verfügbar.



- Erstellen einer Bereitstellung. Konfigurieren Sie den ersten Server in einer neuen StoreFront-Bereitstellung. Bereitstellungen mit einem Server sind ideal für die Evaluierung von StoreFront oder für kleine Produktionsbereitstellungen. Nachdem Sie den ersten StoreFront-Server konfiguriert haben, können Sie jederzeit weitere Server zur Gruppe hinzufügen, um die Kapazität der Bereitstellung zu erhöhen.
- Vorhandener Servergruppe beitreten: Fügen Sie einer vorhandenen StoreFront-Bereitstellung einen Server hinzu. Wählen Sie diese Option aus, um die Kapazität der StoreFront-Bereitstellung schnell zu erhöhen. Für Bereitstellungen mit mehreren Servern ist ein externer Lastausgleich erforderlich. Sie müssen auf einen vorhandenen Server in der Bereitstellung zugreifen, um einen neuen Server hinzuzufügen.

Der Store steht den Benutzern jetzt über einen Browser oder die Citrix Workspace-App zur Verfügung. Siehe Benutzerhandbuch.

Citrix Programm zur Verbesserung der Benutzerfreundlichkeit

January 25, 2024

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, damit die Qualität und Leistung der Citrix Produkte verbessert wird.

Sie werden standardmäßig automatisch beim CEIP registriert, wenn Sie StoreFront installieren. Der erste Datenupload erfolgt ca. sieben Tage nach der Installation von StoreFront. Sie können die Standardeinstellung über eine Registrierungseinstellung ändern. Wenn Sie die Registrierungseinstellung ändern, bevor Sie StoreFront installieren, wird der neue Wert verwendet. Wenn Sie die Registrierungseinstellung ändern, bevor Sie StoreFront aktualisieren, wird der neue Wert verwendet.

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungseditors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungseditors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Registrierungseinstellung zur Steuerung des automatischen Uploads von Analysedaten (Standard = 1):

```
Location: HKLM:\Software\Citrix\Telemetry\CEIP
Name: Enabled
Type: REG_DWORD
Value: 0 = disabled, 1 = enabled
<!--NeedCopy-->
```

Standardmäßig ist die Eigenschaft **Enabled** in der Registrierung verborgen. Wird sie nicht festgelegt, dann ist der automatische Upload aktiviert.

Mit dem folgenden PowerShell-Cmdlet wird die Registrierung beim CEIP deaktiviert:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
Enabled -PropertyType DWORD -Value 0
```

> **Hinweis:**
>
> Die Registrierungseinstellung steuert den automatischen Upload anonymer Statistiken und Nutzungsinformationen für alle Komponenten auf einem Server. Wenn Sie StoreFront beispielsweise auf demselben Server wie den Delivery Controller installiert haben und die Teilnahme am CEIP per Registrierungseinstellung beenden, gilt dies für beide Komponenten.

Vom CEIP gesammelte StoreFront-Daten

In der folgende Tabelle sehen Sie Beispiele für die Art der anonymen Informationen, die gesammelt werden. Die Daten enthalten keine Informationen, die Sie als Kunden identifizieren.

Einstellung	Beschreibung
StoreFront-Version	Die Zeichenfolge steht für die installierte Version von StoreFront. Beispiel: “3.8.0.0”
Anzahl der Stores	Anzahl der Stores in der Bereitstellung
Anzahl der Server in der Servergruppe	Die Anzahl der Server in der Servergruppe
Delivery Controller pro Store	Liste numerischer Werte mit der Anzahl der für jeden Store in der Bereitstellung verfügbaren Delivery Controller
HTTPS aktiviert	Zeichenfolge, die angibt, ob HTTPS für die Bereitstellung aktiviert ist (“True”oder “False”).
HTML5-Einstellung für Citrix Receiver für Web	Liste von Zeichenfolgen, die die HTML5-Einstellung für Web Receiver angeben (“Always”, “Fallback”oder “Off”).
Workspace Control für Citrix Receiver bzw. die Citrix Workspace-App aktiviert	Liste boolescher Werte, die angeben, ob Workspace Control für jeden Web Receiver aktiviert ist (“True”oder “False”).
Remotezugriff für den Store aktiviert	Liste von Zeichenfolgen, die angeben, ob Remotezugriff für die Stores in der Bereitstellung aktiviert ist (“ENABLED”oder “DISABLED”).
Gateways	Anzahl der in der Bereitstellung konfigurierten Citrix Gateways.

Citrix Analytics-Dienst

April 17, 2024

Monitor-Kunden mit einer StoreFront-Bereitstellung im eigenen Rechenzentrum können StoreFront so konfigurieren, dass Daten an Citrix Analytics in Monitor gesendet werden. Bei entsprechender Konfiguration senden die Citrix Workspace-App und Webbrowser Benutzerereignisse zur Verarbeitung an Citrix Analytics. Citrix Analytics aggregiert Kennzahlen zu Benutzern, Anwendungen, Endpunkten, Netzwerken und Daten für detaillierte Einblicke in das Benutzerverhalten. Informationen zu dieser Funktion in der Citrix Analytics-Dokumentation finden Sie unter Onboarding von Virtual Apps and Desktops-Sites mit StoreFront.

Führen Sie zum Konfigurieren dieses Verhaltens folgende Schritte aus:

- Laden Sie eine Konfigurationsdatei von Citrix Analytics herunter.

- Importieren Sie Citrix Analytics-Daten per PowerShell in Ihre StoreFront-Bereitstellung.

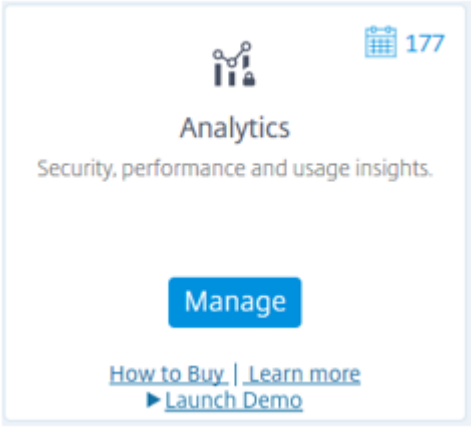
Nach dem Konfigurieren von StoreFront kann die Citrix Workspace-App Daten aus StoreFront-Stores senden, wenn dies von Citrix Analytics angefordert wird.

> **Wichtig:**
>
> Ihre StoreFront-Bereitstellung muss in der Lage sein, die folgenden Adressen über Port 443 zu kontaktieren, damit dieses Feature ordnungsgemäß funktioniert und Monitor-Dienste nutzen kann:
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

Herunterladen der Konfigurationsdatei von Citrix Analytics

> **Wichtig:**
>
> Für die Erstkonfiguration ist eine Konfigurationsdatei mit vertraulichen Informationen erforderlich. Schützen Sie die Datei nach dem Herunterladen vor unbefugtem Zugriff. Geben Sie die Datei nicht an Personen außerhalb Ihrer Organisation weiter. Nach der Konfiguration können Sie die Datei löschen. Wenn Sie die Konfiguration auf einem anderen Computer neu anwenden müssen, können Sie die Datei erneut über die Citrix Analytics-Dienstverwaltungskonsole herunterladen.

1. Melden Sie sich mit einem Administratorkonto bei Monitor (`https://citrix.cloud.com/`) an.
2. Wählen Sie einen Monitor-Kunden aus.
3. Öffnen Sie die Citrix Analytics-Verwaltungskonsole, indem Sie auf **Manage** klicken.



4. Wählen Sie in der Citrix Analytics-Verwaltungskonsole **Settings > Data Source**.
5. Wählen Sie auf der Karte “Virtual App and Desktops”das Menüsymbol (⋮) und dann **Connect StoreFront deployment**.

6. Wählen Sie auf der Seite "Connect StoreFront Deployment"**Download File**, um die Datei *StoreFrontConfigurationFile.json* herunterzuladen.

Beispiel einer Konfigurationsdatei

```
{

  "customerId": "<yourcloudcustomer>",
  "enablementService": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
     deviceid>/dsconfigdata",
  "cwsServiceKey": "PFJTPn…… T4=",
  "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/storefront/config",
  "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",
  "name": "CASSingleTenant"
 }

<!--NeedCopy-->
```

wobei

customerId ist die eindeutige ID des Monitor-Kunden.

cwsServiceKey ist ein eindeutiger Schlüssel zur Identifizierung des Monitor-Kundenkontos.

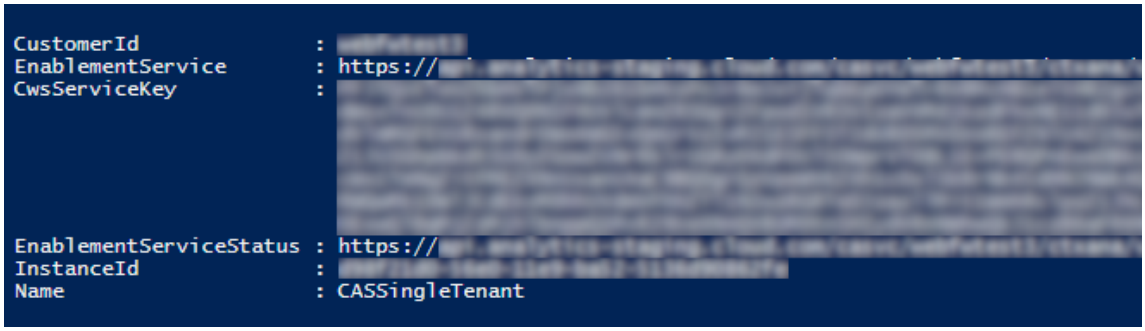
instanceID ist eine generierte ID, die zum Signieren von (sicheren) Anforderungen aus der Citrix Workspace-App an Citrix Analytics verwendet wird. Wenn Sie mehrere StoreFront-Server oder -Servergruppen bei Monitor registrieren, verfügt jeder/jede über eine eigene instanceID.

Importieren von Citrix Analytics-Daten in Ihre StoreFront-Bereitstellung

1. Kopieren Sie die Datei *StoreFrontConfigurationFile.json* in einen geeigneten Ordner auf dem lokalen StoreFront-Server (bzw. einem Server in einer StoreFront-Servergruppe). Die folgenden Befehle basieren auf einer Datei, die auf dem Desktop gespeichert ist.
2. Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.
3. Führen Sie die folgenden Befehle aus:

   ```
   Import-STFCasConfiguration -Path "$Env:UserProfile\Desktop\
      StoreFrontConfigurationFile.json"
   Get-STFCasConfiguration
   <!--NeedCopy-->
   ```

4. Dieser Befehl gibt eine Kopie der importierten Daten zurück und zeigt sie in der PowerShell-Konsole an.



> **Hinweis:**
>
> Für On-Premises-StoreFront-Server mit Windows Server 2012 R2 müssen die C++-Laufzeit-Softwarekomponenten evtl. manuell installiert werden, damit sie sich bei der ZS registrieren können. Wird StoreFront im Rahmen der Citrix Virtual Apps and Desktops-Installation installiert, ist dieser Schritt nicht erforderlich, da der Citrix Virtual Apps and Desktops-Metainstaller die C++-Laufzeitkomponenten installiert. Wird StoreFront nur mit dem CitrixStoreFront-x64.exe-Metainstaller ohne C++-Laufzeitumgebung installiert, kann es sich möglicherweise nicht bei Monitor registrieren, nachdem Sie die ZS-Konfigurationsdatei importiert haben.

Verteilen von Citrix Analytics-Daten an eine StoreFront-Servergruppe

Wenn Sie diese Aktionen an einer StoreFront-Servergruppe ausführen, müssen Sie die importierten Citrix Analytics-Daten an alle Mitglieder der Gruppe verteilen. Dieser Schritt ist bei Bereitstellungen mit nur einem StoreFront-Server nicht erforderlich.

Zur Verteilung der Daten gibt es folgende Möglichkeiten:

- Verwenden Sie die StoreFront-Verwaltungskonsole.
- Verwenden Sie das PowerShell-Cmdlet **Publish-STFServerGroupConfiguration**.

Prüfen der StoreFront-Servergruppen-ID

Um zu überprüfen, ob Ihre Bereitstellung erfolgreich bei Citrix Analytics registriert wurde, können Sie mithilfe von PowerShell die “ServerGroupID”für Ihre Bereitstellung erkennen lassen.

1. Melden Sie sich bei Ihrem StoreFront-Server oder bei einem StoreFront-Server in der Servergruppe an.
2. Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.
3. Führen Sie die folgenden Befehle aus:

```
1 $WebConfigPath = "C:\Program Files\Citrix\Receiver StoreFront\
    Framework\FrameworkData\Framework.xml"
```



```
$XMLObject = (Get-Content $WebConfigPath) -as [Xml]
$XMLObject.framework.properties.property
<!--NeedCopy-->
```

Diese Befehle erzeugen eine Ausgabe, die in etwa so aussieht:

```
name value
---- -----
ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432
HostBaseUrl https://storefront.example.com/
SelectedIISWebSiteId 1
AdminConsoleOperationMode Full
<!--NeedCopy-->
```

Beenden der Datenübertragung aus StoreFront an Citrix Analytics

1. Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.
2. Führen Sie die folgenden Befehle aus:

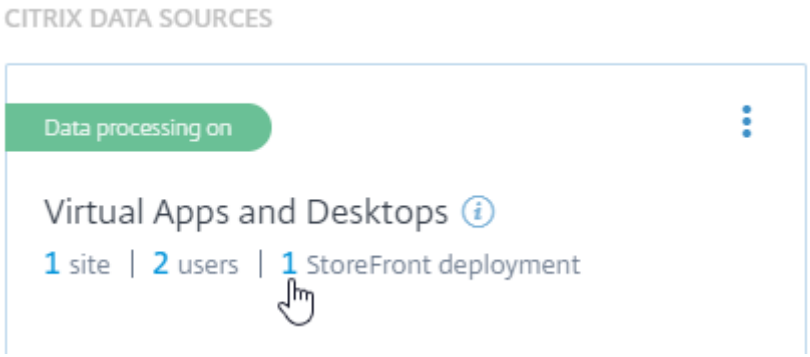
   ```
   Remove-STFCasConfiguration
   ```

   ```
   Get-STFCasConfiguration
   ```

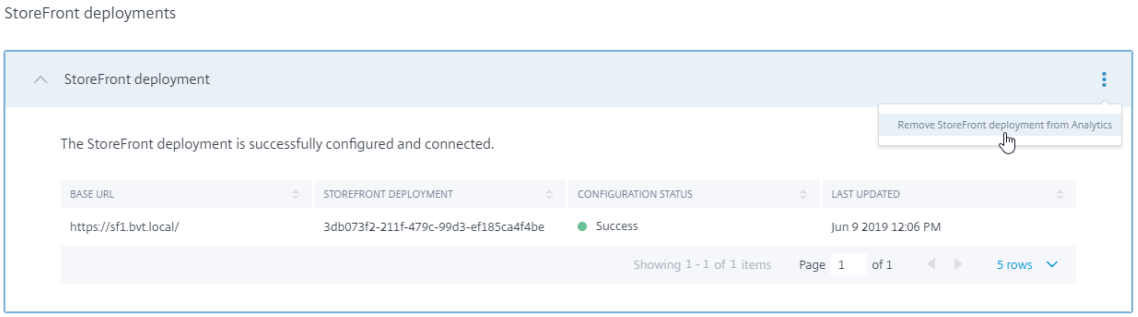
   Get-STFCasConfiguration gibt nichts zurück, wenn die zuvor importierten Citrix Analytics-Daten erfolgreich entfernt wurden.
3. Wenn Sie diese Aktionen an einer StoreFront-Servergruppe ausführen, verteilen Sie die Änderung zum Entfernen der Citrix Analytics-Daten von allen Mitgliedern der Gruppe. Führen Sie auf einem Server in der Servergruppe den folgenden Befehl aus:

   ```
   Publish-STFServerGroupConfiguration
   ```
4. Führen Sie auf den anderen Mitgliedern der Servergruppe den folgenden Befehl aus, um zu prüfen, ob die Citrix Analytics-Konfiguration erfolgreich entfernt wurde:

   ```
   Get-STFCasConfiguration
   ```
5. Melden Sie sich mit einem Administratorkonto bei Monitor (`https://citrix.cloud.com/`) an.
6. Wählen Sie einen Monitor-Kunden aus.
7. Öffnen Sie die Citrix Analytics-Verwaltungskonsole, indem Sie auf **Manage** klicken.
8. Wählen Sie in der Citrix Analytics-Verwaltungskonsole **Settings > Data Source**.
9. Wählen Sie auf der Karte “Virtual Apps and Desktops”die Anzahl der StoreFront-Bereitstellungen aus:



10. Identifizieren Sie die StoreFront-Bereitstellung, die Sie entfernen möchten, anhand der Host-Basis-URL und der ServerGroupID.
11. Wählen Sie im Menü (⊠) die Option **Remove StoreFront deployment from Analytics**.



> **Hinweis:**
>
> Wenn Sie die Konfiguration serverseitig entfernen, jedoch nicht aus Citrix Analytics, bleibt der StoreFront-Serverbereitstellungseintrag in Citrix Analytics, es werden jedoch keine Daten von StoreFront empfangen. Wenn Sie die Konfiguration nur aus Citrix Analytics entfernen, wird der StoreFront-Serverbereitstellungseintrag beim nächsten App-Pool-Recycle wieder hinzugefügt (bei einer IIS-Zurücksetzung oder automatisch alle 24 Stunden).

Konfigurieren von StoreFront für die Verwendung eines Webproxys zur Verbindung mit Monitor und Registrierung bei Citrix Analytics

Wenn StoreFront auf einem Hostwebserver hinter einem Webproxy ausgeführt wird, schlägt die Registrierung bei Citrix Analytics fehl. Wenn StoreFront-Administratoren einen HTTP-Proxy in ihrer Citrix Bereitstellung verwenden, muss der StoreFront-Datenverkehr in das Internet den Webproxy durchlaufen, bevor er Citrix Analytics in der Cloud erreicht. StoreFront verwendet nicht automatisch die Proxyeinstellungen des Hostbetriebssystems. Zusätzliche Konfiguration ist erforderlich, um den Store anzuweisen, ausgehenden Datenverkehr über den Webproxy zu senden. Sie können eine <system.net>-Proxykonfiguration erstellen, indem Sie der Datei web.config einen neuen

Abschnitt hinzufügen. Tun Sie dies für jeden Store auf dem StoreFront-Server, der zum Senden von Daten an Citrix Analytics verwendet wird.

Methode 1: Festlegen der Proxykonfiguration über PowerShell für einen oder mehrere Stores (empfohlen)

Das Powershell-Skript "Config-StoreProxy.ps1"automatisiert diesen Prozess für einen oder mehrere Stores und fügt automatisch einen gültigen XML-Eintrag zum Konfigurieren von `<system.net>` ein. Das Skript sichert auch die web.config-Datei des Stores auf dem Desktop des aktuellen Benutzers, sodass sie bei Bedarf wiederhergestellt werden kann.

> **Hinweis:**
>
> Das mehrfache Ausführen des Skripts kann dazu führen, dass mehrere `<system.net`-XML-Einträge hinzugefügt werden. Jeder Store darf nur einen Eintrag für `<system.net>` haben. Das Hinzufügen mehrerer Einträge führt zur Fehlfunktion der Store-Proxykonfiguration.

1. Öffnen Sie die PowerShell ISE und wählen Sie **Als Administrator ausführen**.
2. Legen Sie `$Stores = @("Store","Store2")` fest, um die Stores einzuschließen, die Sie mit einem Webproxy konfigurieren möchten.
3. Geben Sie den Webproxy an über:
   - eine IP-Adresse ODER
   - einen FQDN
4. Führen Sie folgendes PowerShell-Skript aus:

```
$Stores = @("Store","Store2")
$ProxyIP = "10.0.0.1"
$ProxyFQDN = "proxyserver.example.com"
$ProxyPort = 8888

# Set this for every Store using Stores array
function Set-StoreProxyServer() # Tested with both IP and FQDN
{

    [CmdletBinding()]
    param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
        Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
        array]$Stores,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
            string]$ProxyIP,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
            string]$ProxyFQDN,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
            Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")
            ][int]$ProxyPort)
```



```
15
16      foreach($Store in $Stores)
17      {
18
19          Write-Host "Backing up the Store web.config file for store
                $Store before making changes..." -ForegroundColor "
               Yellow"
20          Write-Host "`n"
21
22          if(!(Test-Path "$env:UserProfile\desktop$Store"))
23          {
24
25              Write-Host "Creating $env:UserProfile\desktop$Store\
                   directory for backup..." -ForegroundColor "Yellow"
26              New-Item -Path "$env:UserProfile\desktop$Store" -
                   ItemType "Directory" | Out-Null
27              Write-Host "`n"
28           }
29
30
31          Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
               config to $env:UserProfile\desktop$Store..." -
               ForegroundColor "Yellow"
32          Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
               config" -Destination "$env:UserProfile\desktop$Store" -
               Force | Out-Null
33
34          if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35          {
36
37              Write-Host "$env:UserProfile\desktop$Store\web.config
                   file backed up" -ForegroundColor "Green"
38           }
39
40          else
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                   file NOT found!" -ForegroundColor "Red"
44           }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
               Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
50
51          $StoreConfigPath = "c:\inetpub\wwwroot\Citrix$Store\web.
               config"
52          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54          if([string]::IsNullOrEmpty($ProxyFQDN))
55          {
```



```
56
57              $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
58           }
59
60          else
61          {
62
63              $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
64           }
65
66
67          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69          # Create 3 elements
70          $SystemNet = $XMLObject.CreateNode("element","system.net",
                ")
71          $DefaultProxy = $XMLObject.CreateNode("element","
                defaultProxy","")
72          $Proxy = $XMLObject.CreateNode("element","proxy","")
73          $Proxy.SetAttribute("proxyaddress","$ProxyServer")
74          $Proxy.SetAttribute("bypassonlocal","true")
75
76          # Move back up the XML tree appending new child items in
                reverse order
77          $DefaultProxy.AppendChild($Proxy)
78          $SystemNet.AppendChild($DefaultProxy)
79          $XMLObject.configuration.AppendChild($SystemNet)
80
81          # Save the modified XML document to disk
82          $XMLObject.Save($StoreConfigPath)
83
84          Write-Host "Getting the proxy configuration for c:\inetpub
                \wwwroot\Citrix$Store..." -ForegroundColor "Yellow"
85          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
86          $ConfiguredProxyServer = $XMLObject.configuration.'system.
                net'.defaultProxy.proxy.proxyaddress | Out-Null
87          Write-Host ("Configured proxy server for Store $Store"+":
                "+ $ConfiguredProxyServer) -ForegroundColor "Green"
88          Write-Host "`n"
89       }
90
91      Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
92      IISReset /RESTART
93   }
94
95
96  Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
        ProxyPort $ProxyPort
97  # OR
98  Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
        $ProxyPort
99  <!--NeedCopy-->
```


5. Überprüfen Sie, ob C:\inetpub\wwwroot\Citrix < Store>\web.config einen neuen<system.net>-Abschnitt am Dateiende enthält.

```
        </dependentAssembly>
    </assemblyBinding>
</runtime>
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
       bypassonlocal="true" />
    </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

6. Importieren Sie die Citrix Analytics-Daten wie unter Importieren von Citrix Analytics-Daten in Ihre StoreFront-Bereitstellung beschrieben.

Methode 2: Manuelles Hinzufügen eines <system.net>-Abschnitts zur web.config-Datei

Dieses Verfahren muss für jeden Store auf dem StoreFront-Server ausgeführt werden, der zum Senden von Daten an Citrix Analytics verwendet wird.

1. Sichern Sie die Datei web.config für den Store und kopieren Sie sie an einen anderen Speicherort außerhalb von C:\inetpub\wwwroot\Citrix< Store>\web.config.
2. Ändern Sie den folgenden XML-Eintrag unter Verwendung Ihrer Proxyeinstellungen entweder unter Angabe von FQDN-und-Port oder von IP-und-Port.

   Für FQDN-und-Port verwenden Sie beispielsweise das folgende <system.net>-Element:

```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
       bypassonlocal="true" />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

   Für IP-und-Port verwenden Sie beispielsweise das folgende <system.net>-Element:

```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true
       " />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

3. Fügen Sie am Ende der Datei web.config das <system.net>-Element wie hier gezeigt ein:


```
<runtime>
<gcServer enabled="true" />
<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
    <assemblyIdentity name="System.Web.MVC" publicKeyToken="31
       BF3856AD364E35" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="
       5.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
    <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30
       ad4fe6b2a6aeed" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="
       9.0.0.0" />
    </dependentAssembly>
</assemblyBinding>
</runtime>

Insert the <system.net> element here

</configuration>
<!--NeedCopy-->
```

4. Importieren Sie die Citrix Analytics-Daten wie unter Importieren von Citrix Analytics-Daten in Ihre StoreFront-Bereitstellung beschrieben.

StoreFront mit HTTPS schützen

April 17, 2024

Citrix empfiehlt dringend, die Kommunikation zwischen StoreFront und Benutzergeräten mit HTTPS zu schützen. Dadurch werden Kennwörter und andere Daten, die zwischen dem Client und StoreFront gesendet werden, verschlüsselt. Zudem können einfache HTTP-Verbindungen durch verschiedene Angriffe beeinträchtigt werden, z. B. durch Man-in-the-Middle-Angriffe, insbesondere wenn Verbindungen von unsicheren Orten wie öffentlichen Wi-Fi-Hotspots aus hergestellt werden. Wenn die entsprechende IIS-Konfiguration nicht verfügbar ist, verwendet StoreFront HTTP für die Kommunikation.

Abhängig von Ihrer Konfiguration greifen die Benutzer über ein Gateway oder einen Load Balancer auf StoreFront zu. Sie können die HTTPS-Verbindung am Gateway oder Load Balancer beenden. In diesem Fall empfiehlt Citrix dennoch, die Verbindungen zwischen dem Gateway und StoreFront mit HTTPS zu schützen.

Wenn StoreFront nicht für HTTPS konfiguriert ist, wird die folgende Warnung angezeigt:

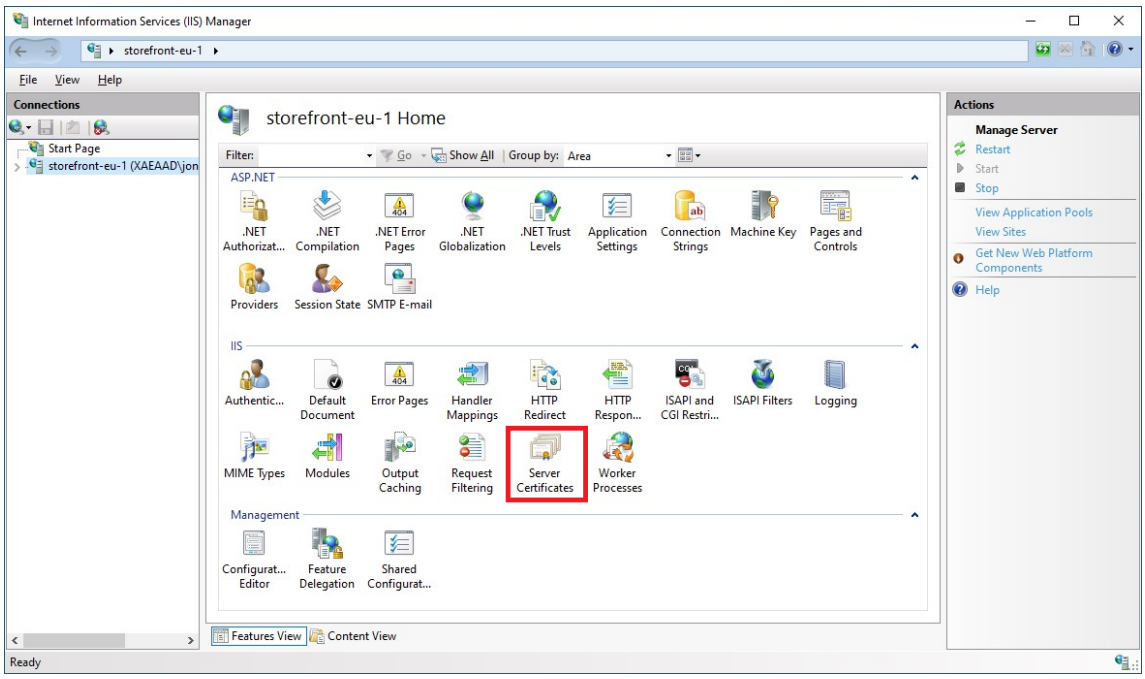
Zertifikate erstellen

- Stellen Sie sicher, dass für den Zugriff auf StoreFront verwendeten FQDNs im DNS-Feld als alternativer Antragstellernamen enthalten sind. Wenn Sie einen Load Balancer verwenden, geben Sie sowohl den FQDN des Servers als auch den Load Balancer-FQDN an.
- Unterzeichnen Sie das Zertifikat mit einer Drittanbieterzertifizierungsstelle, z. B. Verisign, oder einer Unternehmensstammzertifizierungsstelle für Ihre Organisation.
- Exportieren Sie das Zertifikat im PFX-Format einschließlich des privaten Schlüssels.

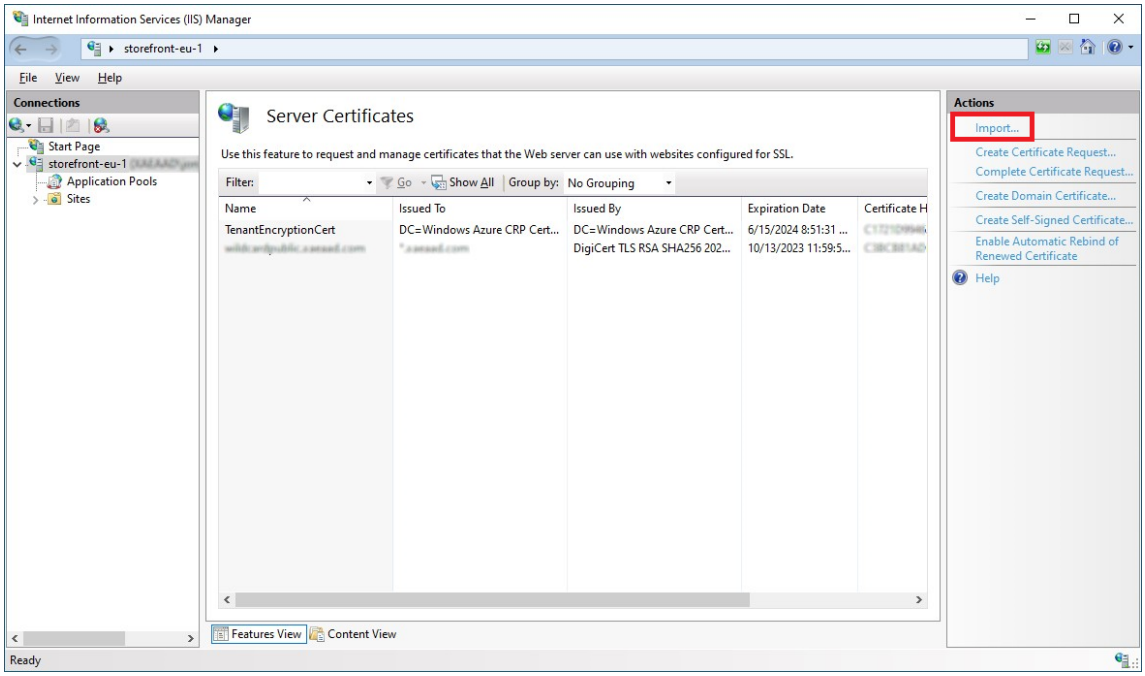
IIS für HTTPS konfigurieren

Konfigurieren von Microsoft Internetinformationsdienste (IIS) für HTTPS auf dem StoreFront-Server:

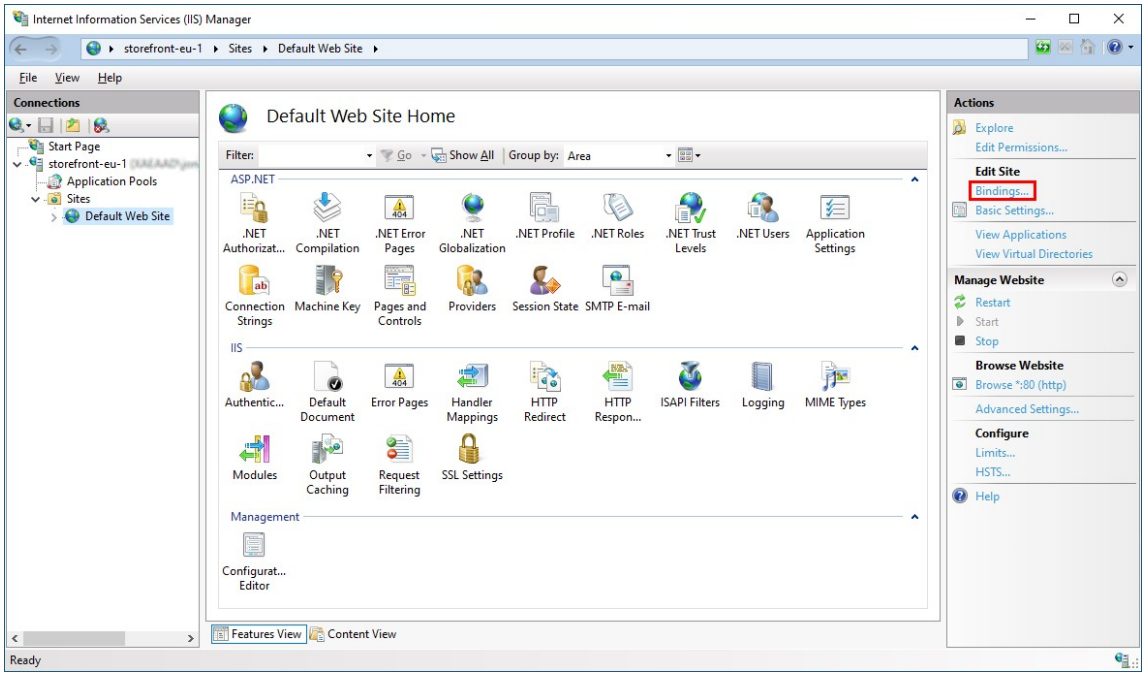
1. Öffnen Sie die IIS-Verwaltungskonsole.
2. Wählen Sie in der Baumstrukturansicht links den Server aus.
3. Doppelklicken Sie im rechten Bereich auf **Serverzertifikate**.



4. Im Fenster "Serverzertifikate"können Sie ein vorhandenes Zertifikat importieren oder ein neues Zertifikat erstellen.



5. Wählen Sie in der Baumstrukturansicht auf der linken Seite die Option **Standardwebsite** (oder die entsprechende Website).
6. Klicken Sie im Aktionsbereich auf **Bindungen**.

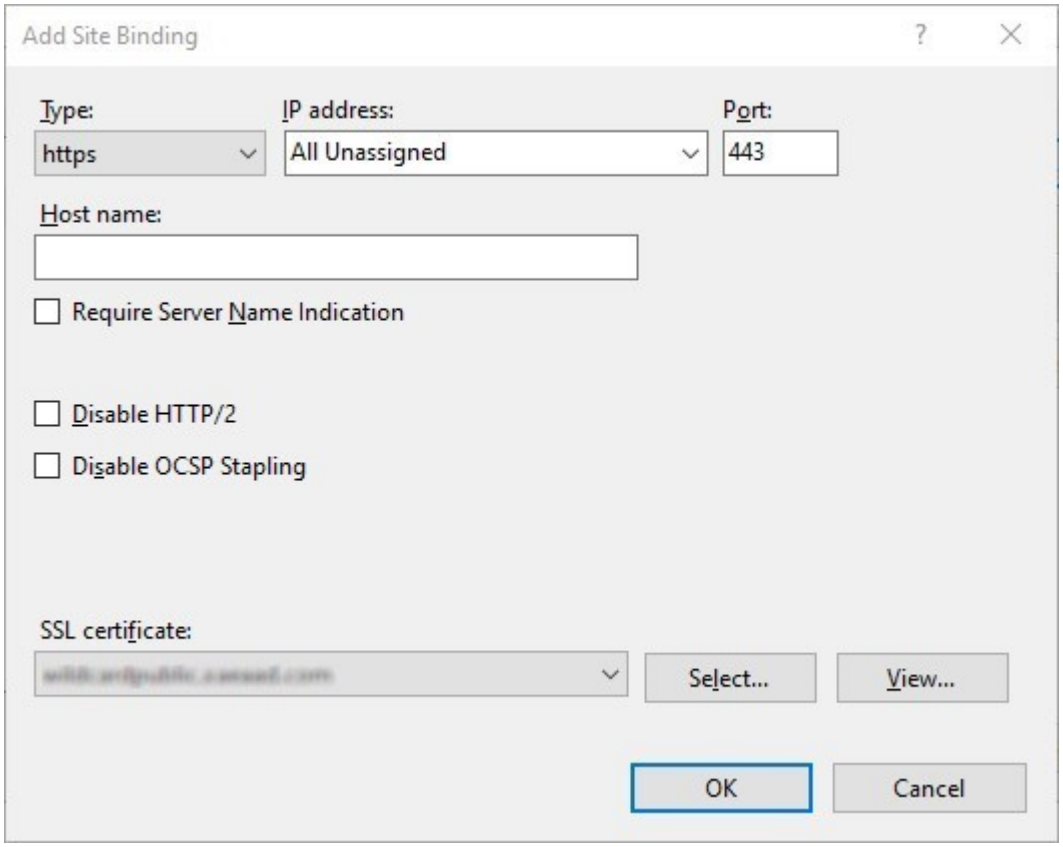


7. Klicken Sie im Bindungsfenster auf **Hinzufügen**.
8. Wählen Sie in der Dropdownliste **Typ** die Option **https**.
9. Klicken Sie unter Windows Server 2022 oder höher auf **Legacy-TLS deaktivieren**, um

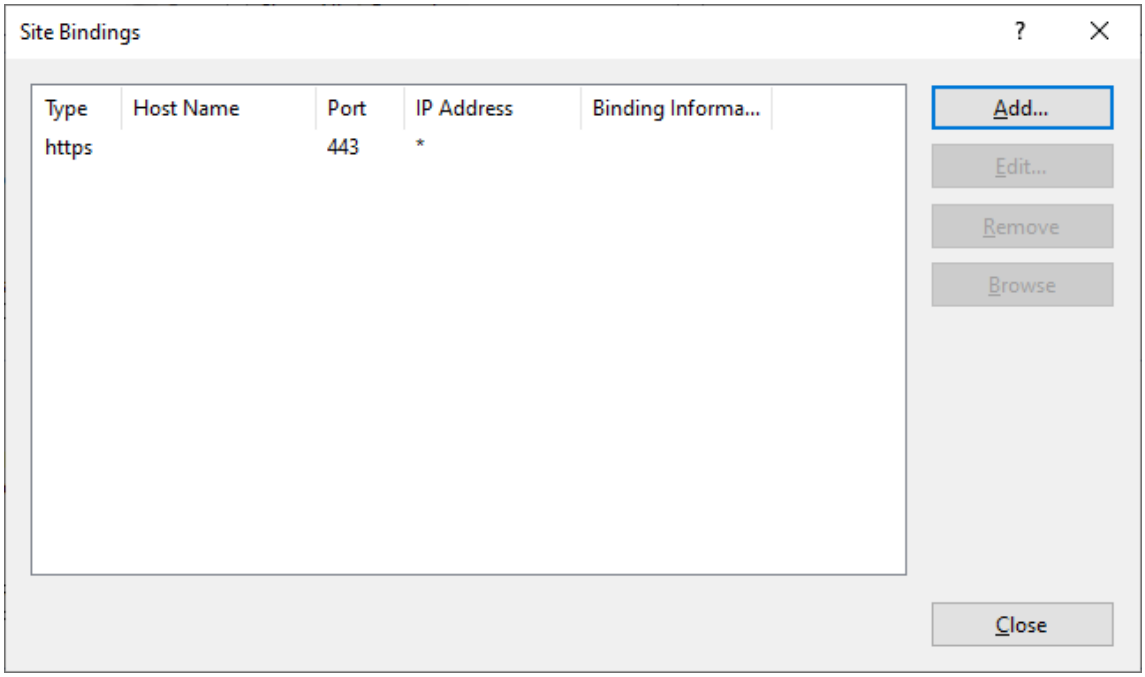
TLS-Versionen zu deaktivieren, die älter als 1.2 sind.

In älteren Windows Server-Versionen können Sie Legacy-TLS-Versionen über die Windows-Registrierung deaktivieren (siehe Windows Server-Dokumentation).

10. Wählen Sie das zuvor importierte Zertifikat aus. Klicken Sie auf OK.



11. Um den HTTP-Zugriff zu entfernen, wählen Sie HTTP und klicken Sie auf **Entfernen**.

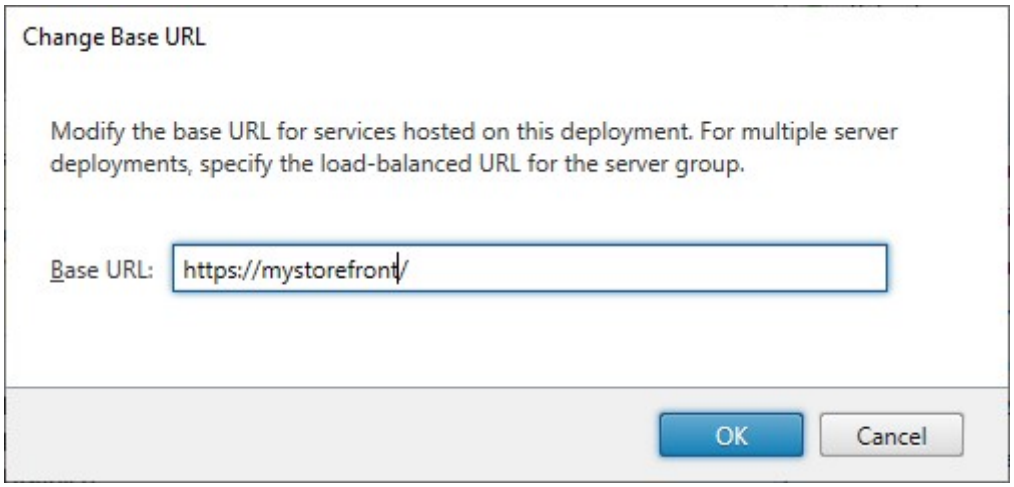


Ändern der Basis-URL des StoreFront-Servers von HTTP in HTTPS

Wenn Sie Citrix StoreFront installieren und konfigurieren, ohne zuvor ein SSL-Zertifikat zu installieren und zu konfigurieren, verwendet StoreFront HTTP für die Kommunikation.

Wenn Sie später ein SSL-Zertifikat installieren und konfigurieren, verwenden Sie das folgende Verfahren, um sicherzustellen, dass StoreFront und StoreFront-Dienste HTTPS-Verbindungen verwenden.

1. Klicken Sie in der Citrix StoreFront-Verwaltungskonsole links auf **Servergruppe**.
2. Klicken Sie im Aktionsbereich auf **Basis-URL ändern**.
3. Aktualisieren Sie die Basis-URL, um `https:` zu starten, und klicken Sie auf **OK**.



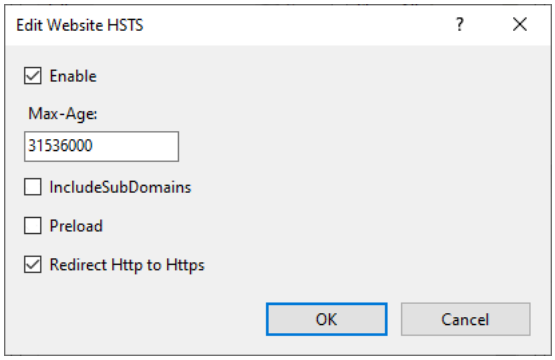
HSTS

Das Clientgerät des Benutzers ist anfällig, auch wenn Sie HTTPS auf der Serverseite aktiviert haben. Ein Man-in-the-Middle-Angreifer könnte beispielsweise den StoreFront-Server fälschen und den Benutzer dazu verleiten, über einfaches HTTP eine Verbindung zum Spoof-Server herzustellen. Die Angreifer könnten dann Zugriff auf vertrauliche Informationen wie die Anmeldeinformationen des Benutzers erhalten. Die Lösung besteht darin, sicherzustellen, dass der Browser des Benutzers nicht versucht, über HTTP auf den RfWeb-Server zuzugreifen. Sie können dies mit HTTP Strict Transport Security (HSTS) erreichen.

Wenn HSTS aktiviert ist, teilt der Server den Webbrowsern mit, dass Anfragen an die Website immer nur über HTTPS gestellt werden sollten. Wenn ein Benutzer versucht, über HTTP auf die URL zuzugreifen, wechselt der Browser automatisch zur Verwendung von HTTPS. Dies gewährleistet die clientseitige Validierung einer sicheren Verbindung sowie die serverseitige Validierung in IIS. Der Webbrowser behält diese Validierung für einen konfigurierten Zeitraum bei.

Auf Windows Server 2019 und höher:

1. Öffnen Sie den **Internetinformationsdienste (IIS)-Manager**.
2. Wählen Sie **Standardwebsite** (oder die entsprechende Website).
3. Klicken Sie im Aktionsbereich auf der rechten Seite auf **HSTS...**
4. Aktivieren Sie das Kontrollkästchen für **Aktivieren**, geben Sie eine Höchstdauer ein (z. B. 31536000 für ein Jahr), und aktivieren Sie **HTTP auf HTTPS umleiten**.
5. Klicken Sie auf **OK**.



> **Hinweis:**
>
> Die Aktivierung von HSTS wirkt sich auf alle Websites einer Domäne aus. Wenn die Website beispielsweise unter https://www.company.com/Citrix/StoreWeb aufgerufen werden kann, gilt die HSTS-Richtlinie für alle Websites unter https://www.company.com, was möglicherweise nicht erwünscht ist.

Sichern der StoreFront-Bereitstellung

May 31, 2024

In diesem Artikel werden Bereiche behandelt, die sich bei der Bereitstellung und Konfiguration von StoreFront auf die Systemsicherheit auswirken können.

Kommunikation zwischen Endbenutzern und StoreFront

Citrix empfiehlt, die Kommunikation zwischen Benutzergeräten und StoreFront mit HTTPS zu schützen. Dadurch werden Kennwörter und andere Daten, die zwischen dem Client und StoreFront gesendet werden, verschlüsselt. Zudem können einfache HTTP-Verbindungen durch verschiedene Angriffe beeinträchtigt werden, z. B. durch Man-in-the-Middle-Angriffe, insbesondere wenn Verbindungen von unsicheren Orten wie öffentlichen Wi-Fi-Hotspots aus hergestellt werden. Wenn die entsprechende IIS-Konfiguration nicht verfügbar ist, verwendet StoreFront HTTP für die Kommunikation.

Abhängig von Ihrer Konfiguration greifen die Benutzer über ein Gateway oder einen Load Balancer auf StoreFront zu. Sie können die HTTPS-Verbindung am Gateway oder Load Balancer beenden. In diesem Fall empfiehlt Citrix dennoch, die Verbindungen zwischen dem Gateway oder Load Balancer und StoreFront mit HTTPS zu schützen.

Informationen zum Aktivieren von HTTPS, Deaktivieren von HTTP und Aktivieren von HSTS finden Sie unter StoreFront mit HTTPS schützen.

StoreFront-Kommunikation mit Citrix Virtual Apps and Desktops-Servern

Citrix empfiehlt die Verwendung von HTTPS, um den Datenaustausch zwischen StoreFront und den Citrix Virtual Apps and Desktops Delivery Controllern zu schützen. Siehe Installieren von TLS-Serverzertifikaten auf Controllern. StoreFront unterstützt weder TLS 1.0 noch TLS 1.1 zwischen StoreFront und dem Delivery Controller. Alternativ können Sie Windows zum Schützen der Kommunikation zwischen den Servern mit von IPSec konfigurieren.

Sie können den Delivery Controller und StoreFront so konfigurieren, dass nur vertrauenswürdige StoreFront-Server mit dem Delivery Controller kommunizieren können (siehe Sicherheitsschlüssel verwalten).

StoreFront-Kommunikation mit Cloud Connectors

Citrix empfiehlt, das HTTPS-Protokoll zu verwenden, um den Datenaustausch zwischen StoreFront und Cloud Connectors zu schützen. Weitere Informationen finden Sie unter How to Enable SSL on

Cloud Connectors to Secure XML Traffic. StoreFront unterstützt weder TLS 1.0 noch TLS 1.1 zwischen StoreFront und den Cloud Connectors. Alternativ können Sie Windows zum Schützen der Kommunikation zwischen den Servern mit von IPSec konfigurieren.

Remotezugriff

Citrix rät davon ab, den StoreFront-Server direkt dem Internet zugänglich zu machen. Citrix empfiehlt die Verwendung eines Citrix Gateways für die Authentifizierung und den Zugriff für Remotebenutzer.

Microsoft IIS härten

Sie können StoreFront mit einer eingeschränkten IIS-Konfiguration konfigurieren. Dies ist jedoch nicht die IIS-Standardkonfiguration.

Dateinamenerweiterungen

Mit der Anforderungsfilterung können Sie eine Liste zulässiger Dateinamenerweiterungen konfigurieren und nicht aufgeführte Dateinamenerweiterungen verbieten. Siehe IIS-Dokumentation.

StoreFront benötigt die folgenden Dateinamenerweiterungen:

- . (leere Erweiterung)
- .appcache
- .aspx
- .cr
- .css
- .dtd
- .png
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

Ist Download oder Upgrade der Citrix Workspace-App für eine Store-Website aktiviert, sind für StoreFront außerdem diese Dateinamenerweiterungen erforderlich:

- .dmg
- .exe

Ist die Citrix Workspace-App für HTML5 aktiviert, sind für StoreFront zusätzlich diese Dateinamenerweiterung erforderlich:

- .eot
- .ttf
- .woff
- .wasm

Verben

Mit der Anforderungsfilterung können Sie eine Liste zulässiger Verben konfigurieren und nicht aufgeführte Verben verbieten. Siehe IIS-Dokumentation.

- GET
- POST
- HEAD

Nicht-ASCII-Zeichen in URLs

Wenn Sie sicherstellen, dass Storenamen und Websitenamen nur ASCII-Zeichen enthalten, enthalten StoreFront-URLs keine Nicht-ASCII-Zeichen. Sie können Nicht-ASCII-Zeichen mithilfe der Anforderungsfilterung verbieten. Siehe IIS-Dokumentation.

MIME-Typen

Sie können die OS-Shell-MIME-Typen für die folgenden Dateinamenerweiterungen entfernen:

- .exe
- .dll
- .com
- .bat
- .csh

Siehe IIS-Dokumentation.

X-Powered-By-Header entfernen

Standardmäßig meldet IIS, dass es ASP.NET verwendet, indem es den Header `X-Powered-By` mit Wert `ASP.NET` hinzufügt. Sie können IIS so konfigurieren, dass dieser Header entfernt wird. Weitere Informationen finden Sie in der IIS-Dokumentation zu CustomHeaders.

Serverheader mit IIS-Version entfernen

Standardmäßig meldet IIS die IIS-Version, indem es den Header `Server` hinzufügt. Sie können IIS so konfigurieren, dass dieser Header entfernt wird. Siehe IIS-Dokumentation zur Anforderungsfilterung.

StoreFront-Website in eine eigene Partition verschieben

Sie können StoreFront-Websites auf einer eigenen, von den Systemdateien getrennten Partition hosten. In IIS müssen Sie die **Standardwebsite**verschieben oder eine separate Website in der gewünschten Partition erstellen, bevor Sie die StoreFront-Bereitstellung erstellen.

IIS-Features

Eine Liste der IIS-Features, die von StoreFront installiert und verwendet werden, finden Sie unter Systemanforderungen. Sie können andere IIS-Features entfernen.

StoreFront verwendet ISAPI-Filter zwar nicht direkt, doch das Feature ist für ASP.NET erforderlich und kann daher nicht deinstalliert werden.

Handler-Zuordnungen

StoreFront erfordert die folgenden Handler-Zuordnungen. Sie können andere Handler-Zuordnungen entfernen.

- ExtensionlessUrlHandler-Integrated-4.0
- PageHandlerFactory-Integrated-4.0
- StaticFile

Weitere Informationen finden Sie in der IIS-Dokumentation zu Handlern.

ISAPI-Filter

StoreFront benötigt keine ISAPI-Filter. Sie können alle ISAPI-Filter entfernen. Siehe IIS-Dokumentation zu ISAPI-Filtern.

.NET-Autorisierungsregeln

Standardmäßig ist auf IIS-Servern die .NET-Autorisierungsregel auf "Alle Benutzer zulassen"festgelegt. Standardmäßig erbt die von StoreFront verwendete Website diese Konfiguration.

Wenn Sie die .NET-Autorisierungsregel auf Serverebene entfernen oder ändern, müssen Sie die Regeln der von StoreFront verwendeten Website außer Kraft setzen, um eine Zulassungsregel für "Alle Benutzer"hinzuzufügen, und alle anderen Regeln zu entfernen.

Retail Mode

Sie können den Retail Mode aktivieren, siehe IIS-Dokumentation.

Anwendungspools

StoreFront erstellt die folgenden Anwendungspools:

- Citrix-Konfigurations-API
- Citrix Delivery Services-Authentifizierung
- Ressourcen für Citrix Delivery Services
- und Citrix Receiver für Web

Ändern Sie nicht die von den einzelnen IIS-Anwendungen verwendeten Anwendungspools bzw. die Identität der Pools. Wenn Sie mehrere Sites verwenden, ist es nicht möglich, jede Site für die Verwendung eigener Anwendungspools zu konfigurieren.

In den Recycling-Einstellungen können Sie das Leerlauftimeout und die Menge des virtuellen Speichers für jeden Anwendungspool festlegen. Hinweis: Über einen Browser angemeldete Benutzer werden beim Recycling des Anwendungspools "Citrix Receiver für Web"abgemeldet. Daher ist für diesen standardmäßig ein tägliches Recycling für 02:00 Uhr festgelegt, um Störungen zu minimieren. Wenn Sie eine Recyclingeinstellung ändern, kann dies dazu führen, dass die Benutzer zu anderen Tageszeiten abgemeldet werden.

Erforderliche Einstellungen

- Ändern Sie die IIS-Authentifizierungseinstellungen nicht. StoreFront verwaltet die Authentifizierung und konfiguriert die benötigten Verzeichnisse der StoreFront-Site mit den erforderlichen Authentifizierungseinstellungen.
- Wählen Sie für den StoreFront-Server unter **SSL-Einstellungen** nicht die Option **Clientzertifikate: Erforderlich**. Die StoreFront-Installation konfiguriert die entsprechenden Seiten der StoreFront-Site mit dieser Einstellung.

- StoreFront erfordert Cookies für den Sitzungsstatus und andere Funktionen. In bestimmten Verzeichnissen muss unter **Sitzungszustand**, **Cookie-Einstellungen**, **Modus** auf **Cookies verwenden** festgelegt sein.
- Für StoreFront erfordert für die **.NET-Vertrauensebene** die Einstellung auf **Volles Vertrauen**. Legen Sie für die .NET-Vertrauensstufe keinen anderen Wert fest.

Services

Bei der StoreFront-Installation werden die folgenden Windows-Dienste erstellt:

- Citrix Konfigurationsreplikationsdienst (NT SERVICE\CitrixConfigurationReplication)
- Citrix Clusterbeitrittsdienst (NT SERVICE\CitrixClusterService)
- Citrix Peerauflösungsdienst (NT SERVICE\Citrix Peer Resolution Service)
- Citrix Credential Wallet-Dienst (NT SERVICE\CitrixCredentialWallet)
- Citrix Abonnementstoredienst (NT SERVICE\CitrixSubscriptionsStore)
- Citrix Standarddomänendienste (NT SERVICE\CitrixDefaultDomainService)

Diese Konten melden sich als `Network Service` an. Ändern Sie diese Konfiguration nicht.

Wenn Sie die eingeschränkte StoreFront-Kerberos-Delegierung für XenApp 6.5 konfigurieren, wird dadurch zusätzlich der Citrix StoreFront-Protokollübergangsdienst (NT SERVICE\ CitrixStoreFront-ProtocolTransition) erstellt. Dieser Dienst läuft als `NT AUTHORITY\SYSTEM`. Ändern Sie diese Konfiguration nicht.

Zuweisung von Benutzerrechten

Das Ändern der Standardwerte für die Zuweisung von Benutzerrechten kann zu Problemen mit StoreFront führen. Insbesondere gilt:

- Microsoft IIS wird im Rahmen der StoreFront-Installation aktiviert. Microsoft IIS gewährt die Anmeldeberechtigung **Als Batchauftrag anmelden** und das Privileg **Annehmen der Clientidentität nach Authentifizierung** für die integrierte Gruppe "IIS_IUSRS". Dies ist normales Microsoft IIS-Installationsverhalten. Ändern Sie diese Benutzerrechte nicht. Weitere Informationen finden Sie in der Microsoft-Dokumentation.
- Wenn Sie StoreFront installieren, werden Anwendungspools erstellt, denen IIS Benutzerrechte gewährt: **Als Dienst anmelden**, **Speicherkontingente für einen Prozess anpassen**, **Sicherheitsüberwachungen generieren** und **Token auf Prozessebene ersetzen**.
- Um eine Bereitstellung zu erstellen oder zu ändern, muss der Administrator über die Rechte **Dateien und Verzeichnisse wiederherstellen** verfügen.

- Damit ein Server einer Servergruppe beitreten kann, muss die Administratorgruppe die Rechte **Dateien und Verzeichnisse wiederherstellen**, **Auf diesen Computer vom Netzwerk aus zugreifen** und **Überwachungs- und Sicherheitsprotokoll verwalten** haben.
- Damit sich Benutzer mit einer Benutzernamen- und Kennwortauthentifizierung (direkt oder über ein Gateway) anmelden können, müssen sie über die Rechte "Lokale Anmeldung zulassen" verfügen, es sei denn, Sie haben StoreFront so konfiguriert, dass Kennwörter über den Delivery Controller überprüft werden.

Dies ist keine vollständige Liste und andere Benutzerzugriffsrechte können erforderlich sein.

Konfigurieren der Gruppenmitgliedschaften

Wenn Sie eine StoreFront-Servergruppe konfigurieren, werden der Sicherheitsgruppe "Administratoren"die folgenden Dienste hinzugefügt:

- Citrix Konfigurationsreplikationsdienst (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService) . Dieser Dienst wird nur auf Servern angezeigt, die Teil einer Gruppe sind, und wird nur während des Beitritts ausgeführt.

Diese Gruppenmitgliedschaften sind erforderlich damit StoreFront korrekt funktioniert:

- Erstellen, Exportieren, Importieren, Löschen und Festlegen der Zugriffsberechtigungen von Zertifikaten
- Lesen und Schreiben der Windows-Registrierung
- Hinzufügen und Entfernen von Microsoft .NET Framework-Assemblys im globalen Assemblycache (GAC)
- Zugriff auf den Ordner **Programme\Citrix**<*StoreFrontSpeicherort*>
- Hinzufügen, Bearbeiten und Entfernen von App-Poolidentitäten und IIS-Webanwendungen
- Hinzufügen, Bearbeiten und Entfernen von lokalen Sicherheitsgruppen und Firewallregeln
- Hinzufügen und Entfernen von Windows-Diensten und PowerShell-Snap-Ins
- Registrieren von Microsoft Windows Communication Framework (WCF)-Endpunkten

Bei Updates zu StoreFront kann sich diese Liste der Operationen ohne Ankündigung ändern.

Die StoreFront-Installation erstellt außerdem die folgenden lokalen Sicherheitsgruppen:

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSReplicators

- CitrixPNRSUsers
- CitrixStoreFrontAdministrators
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront verwaltet die Mitgliedschaft in diesen Sicherheitsgruppen. Sie werden für die Zugriffssteuerung in StoreFront verwendet und nicht auf Windows-Ressourcen wie Ordner und Dateien angewendet. Bearbeiten Sie diese Gruppenmitgliedschaften nicht.

NTLM

StoreFront verwendet NTLM, um sich zwischen Servern in einer Servergruppe zu authentifizieren. Wenn Sie NTLM deaktivieren, kann StoreFront keine Daten zwischen StoreFront-Servern in einer Servergruppe synchronisieren.

Sie können den Server so konfigurieren, dass er nur NTLMv2 verwendet und NTLMv1 ablehnt. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

Zertifikate in StoreFront

Serverzertifikate

Serverzertifikate werden zur Identifikation der Maschinen und für die TLS-Transportsicherheit in StoreFront verwendet. Wenn Sie die ICA-Dateisignierung aktivieren, kann StoreFront auch Zertifikate verwenden, um ICA-Dateien digital zu signieren.

Weitere Informationen finden Sie unter Kommunikation zwischen Endbenutzern und StoreFront und ICA-Dateisignierung.

Tokenverwaltungszertifikate

Sowohl die Authentifizierungsdienste als auch Stores benötigen Zertifikate für die Tokenverwaltung. StoreFront generiert ein selbstsigniertes Zertifikat, wenn ein Authentifizierungsdienst oder Store erstellt wird. Von StoreFront generierte, selbstsignierte Zertifikate sollten für keinen anderen Zweck verwendet werden.

Citrix Delivery Services-Zertifikate

StoreFront hält eine Reihe von Zertifikaten in einem benutzerdefinierten Windows-Zertifikatspeicher (Citrix Delivery Services). Der Citrix Konfigurationsreplikationsdienst, der Citrix Credential Wallet-

Dienst und der Citrix Abonnementstoredienst verwenden diese Zertifikate. Jeder StoreFront-Server in einem Cluster hat eine Kopie dieser Zertifikate. Diese Dienste verwenden nicht TLS für die sichere Kommunikation und diese Zertifikate werden nicht als TLS-Serverzertifikate verwendet. Diese Zertifikate werden erstellt, wenn ein StoreFront-Store erstellt oder wenn StoreFront installiert wird. Ändern Sie den Inhalt dieses Windows-Zertifikatspeichers nicht.

Codesignaturzertifikate

StoreFront enthält eine Reihe von PowerShell-Skripts (.ps1) im Ordner <*Installationsverzeichnis*>\Scripts. Die Standardinstallation von StoreFront verwendet diese Skripts nicht. Sie vereinfachen Konfigurationsschritte für bestimmte, seltene Aufgaben. Diese Skripts sind signiert, so dass StoreFront eine PowerShell-Ausführungsrichtlinie unterstützen kann. Wir empfehlen die Richtlinie **AllSigned**. (Die Richtlinie **Eingeschränkt** wird nicht unterstützt, da sie das Ausführen von PowerShell-Skripts verhindert.) StoreFront ändert die PowerShell-Ausführungsrichtlinie nicht.

Obwohl StoreFront kein Codesignaturzertifikat in der Aufstellung der vertrauenswürdigen Herausgeber installiert, kann Windows dort automatisch das Codesignaturzertifikat hinzufügen. Dies geschieht, wenn das PowerShell-Skript mit der Option **Immer ausführen** ausgeführt wird. (Wenn Sie die Option **Nie ausführen** wählen, wird das Zertifikat der Aufstellung der nicht vertrauenswürdigen Zertifikate hinzugefügt, und die PowerShell-Skripts von StoreFront werden nicht ausgeführt.) Nachdem das Codesignaturzertifikat der Aufstellung der vertrauenswürdigen Herausgeber hinzugefügt wurde, wird das Ablaufen nicht mehr von Windows geprüft. Sie können dieses Zertifikat aus der Aufstellung der vertrauenswürdigen Herausgeber entfernen, nachdem die StoreFront-Aufgaben abgeschlossen wurden.

Legacy-TLS-Versionen deaktivieren

Citrix empfiehlt, TLS 1.0 und 1.1 sowohl für die Client- als auch für die Serverkommunikation auf dem Windows-Server zu deaktivieren. Dies ist über die Gruppenrichtlinie oder die Windows-Registrierung möglich. Siehe Microsoft-Dokumentation.

Isolierung der StoreFront-Sicherheit

Falls Sie Webanwendungen in derselben Webdomäne (Domänenname und Port) wie StoreFront bereitstellen, können die mit diesen Webanwendungen verbundenen Sicherheitsrisiken eventuell auch die Sicherheit der StoreFront-Bereitstellung negativ beeinflussen. Ist höhere Sicherheit erforderlich, empfiehlt Citrix die Bereitstellung von StoreFront in einer getrennten Webdomäne.

ICA-Dateisignierung

In StoreFront können ICA-Dateien digital mit einem auf dem Server angegebenen Zertifikat signiert werden, damit Citrix Workspace-App-Versionen, die dieses Feature unterstützen, sicherstellen können, dass die Datei aus einer vertrauenswürdigen Quelle stammt. ICA-Dateien können mit einem Hashalgorithmus signiert werden, der von dem auf dem StoreFront-Server ausgeführten Betriebssystem unterstützt wird, z. B. SHA-1 und SHA-256. Weitere Informationen finden Sie unter Aktivieren der ICA-Dateisignierung.

Benutzerseitige Kennwortänderung

Sie können Benutzern, die sich über einen Webbrowser mit Active Directory-Domänenanmeldeinformationen anmelden, gestatten, ihre Kennwörter zu ändern, und zwar entweder jederzeit oder nur, wenn sie abgelaufen sind. Dadurch werden jedoch vertrauliche Sicherheitsfunktionen für alle Personen offengelegt, die auf einen der Stores, die diesen Authentifizierungsdienst verwenden, zugreifen können. Wenn Ihr Unternehmen eine Sicherheitsrichtlinie hat, die Funktionen zur Änderung des Kennworts nur zur internen Verwendung reserviert, stellen Sie sicher, dass auf keinen der Stores von außerhalb des Unternehmensnetzwerks zugegriffen werden kann. Beim Erstellen des Authentifizierungsdiensts verhindert die Standardkonfiguration, dass die Benutzer ihre Kennwörter ändern, selbst wenn die Kennwörter abgelaufen sind. Weitere Informationen finden Sie unter Kennwortänderung durch Benutzer zulassen.

Anpassungen

Erstellen Sie aus Sicherheitsgründen keine Anpassungen, mit denen Inhalte oder Skripts von Servern geladen werden, die nicht Ihrer Kontrolle unterstehen. Kopieren Sie den Inhalt bzw. das Skript in den benutzerdefinierten Websiteordner, wo Sie die Anpassungen vornehmen. Wenn StoreFront für HTTPS-Verbindungen konfiguriert ist, müssen alle Links zu benutzerdefinierten Inhalten und Skripts ebenfalls HTTPS verwenden.

Sicherheitsheader

Wenn Sie eine Store-Website über einen Webbrowser aufrufen, gibt StoreFront die folgenden Sicherheitsheader zurück, die Einschränkungen für den Webbrowser festlegen.

Headername	Wert	Beschreibung
`content-security-policy`	`frame-ancestors 'none'`	Dies verhindert Clickjacking-Angriffe, da andere Sites keine StoreFront-Websites in einen Frame einbetten können. StoreFront verwendet Inline-Skripts und -Stile, sodass diese nicht mit einer Inhaltsicherheitsrichtlinie (Content Security Policy) blockiert werden können. StoreFront-Websites zeigen nur von Administratoren konfigurierte Inhalte und keine Benutzereingaben an, sodass Inlineskripts nicht blockiert werden müssen.
`X-Content-Type-Options`	`nosniff`	Dadurch wird MIME-Sniffing vermieden.
`X-Frame-Options`	`deny`	Dies verhindert Clickjacking-Angriffe, da andere Sites keine StoreFront-Websites in einen Frame einbetten können. `content-security-policy` ersetzt es durch `frame-ancestors 'none'`, es wird jedoch von einigen älteren Browsern, die `content-security-policy` nicht unterstützen, verstanden.
`X-XSS-Protection`	`1; mode=block`	Wird von einigen Browsern zur Abwehr von XSS-Angriffen (Cross-Site-Scripting) verwendet

Cookies

StoreFront verwendet mehrere Cookies. Beispiele für zum Betrieb der Website verwendeten Cookies:

Cookie	Beschreibung
`ASP.NET_SessionId`	Verfolgt die Sitzung des Benutzers einschließlich des Authentifizierungsstatus. Hat `HttpOnly` aktiviert.
`CtxsAuthId`	Um Session Fixation-Angriffe zu verhindern, verfolgt StoreFront außerdem, ob der Benutzer mithilfe dieses Cookie authentifiziert wurde. Es hat `HttpOnly` festgelegt.
`CsrfToken`	Verhindert CSRF-Angriffe über das standardmäßige Cookie-to-Header-Token. Der Server setzt ein Token im Cookie. Der Client liest das Token aus dem Cookie und fügt es in die Abfragezeichenfolge oder einen Header in nachfolgenden Anforderungen ein. Für das Cookie darf `HttpOnly` nicht festgelegt sein, damit das Client-JavaScript es lesen kann.
`CtxsDeviceId`	Identifiziert das Gerät. Hat `HttpOnly` aktiviert.

StoreFront platziert eine Reihe weiterer Cookies, um den Benutzerzustand zu verfolgen. Einige müssen von JavaScript gelesen werden, daher ist `HttpOnly` für sie nicht gesetzt. Diese Cookies enthalten keine Informationen zur Authentifizierung oder andere vertrauliche Informationen.

Weitere Sicherheitsinformationen

> **Hinweis:**
>
> Diese Informationen können jederzeit und ohne vorherige Ankündigung geändert werden.

Sicherheitsprüfungen an StoreFront können zur Erfüllung gesetzlicher oder anderer Auflagen erforderlich sein. Die o. g. Konfigurationsoptionen können zu dazu beitragen, dass einige Sicherheitsprobleme vermieden werden.

Gibt es ein Gateway zwischen der Sicherheitsprüfung und StoreFront, können sich bestimmte Befunde im Prüfbericht auf das Gateway anstelle von StoreFront beziehen. Sicherheitsprüfberichte unterscheiden hier normalerweise nicht (Beispiel: TLS-Konfiguration). Aus diesem Grund können technische Beschreibungen in Sicherheitsprüfberichten irreführend sein.

E-Mail-basierte Kontenermittlung

September 27, 2023

Konfigurieren Sie die e-mail-basierte Kontenermittlung, sodass Benutzer, die die Citrix Workspace-App auf einem Gerät zum ersten Mal installieren, ihr Konto durch Eingabe ihrer E-Mail-Adresse einrichten können, ohne die Store-URL kennen zu müssen.

Während der Erstkonfiguration fordert die Citrix Workspace-App die Benutzer auf, eine E-Mail-Adresse oder eine Store-URL einzugeben. Wenn ein Benutzer eine E-Mail-Adresse eingibt, sucht die Citrix Workspace-App an verschiedenen Orten nach der E-Mail-Domäne, um den StoreFront-Server zu ermitteln. Anschließend werden alle sichtbaren Stores aufgelistet, aus denen der Benutzer auswählen kann.

Citrix empfiehlt, die E-Mail-Erkennung mithilfe des Global App Config Service zu konfigurieren. Alternativ können Sie die E-Mail-Erkennung mithilfe von DNS-SVR-Datensätzen oder eines DNS-Alias konfigurieren.

Global App Configuration Service

Informationen zur Konfiguration der E-Mail-Erkennung mithilfe des Global App Config Service finden Sie unter E-Mail-basierte Erkennung einrichten.

DNS-SVR-Datensätze

Als Alternative zum Global App Config Service können Sie DNS-SVR-Datensätze verwenden, um den StoreFront-Server zu konfigurieren, den die Citrix Workspace-App für eine E-Mail-Domäne verwenden soll.

Fügen Sie auf dem DNS-Server für Ihre E-Mail-Domäne einen **SRV**-Datensatz mit den folgenden Eigenschaften hinzu:

Eigenschaft	Wert
Service	_citrixreceiver
Proto	TCP

Eigenschaft	Wert
Ziel	Den vollqualifizierten Domänennamen (FQDN) und den Port für das Citrix Gateway-Gerät (Unterstützung lokaler und Remotebenutzer) oder den StoreFront-Server (nur Unterstützung von Benutzern im lokalen Netzwerk) im Format *servername.domäne:port*.

Wenn Ihre Umgebung sowohl interne als auch externe DNS-Server enthält, können Sie einen SRV-Eintrag mit dem StoreFront-Server-FQDN auf Ihrem internen DNS-Server und einen weiteren Eintrag auf dem externen Server mit dem FQDN von Citrix Gateway hinzufügen. Mit dieser Konfiguration erhalten lokale Benutzer die StoreFront-Details, Remotebenutzer dagegen Citrix Gateway-Verbindungsinformationen.

DNS-discoverReceiver-Datensatz

Als Fallback zu den anderen Methoden können Sie ein DNS-Alias für den StoreFront-Server `discoverReceiver` für die E-Mail-Domäne erstellen. Beispiel: Für die E-Mail-Domäne `example.com` erstellen Sie das DNS-Alias `discoverReceiver.example.com`. Wenn kein SRV-Eintrag in der angegebene Domäne gefunden wird, sucht die Citrix Workspace-App nach einer Maschine mit dem Namen "discoverReceiver", um einen StoreFront-Server zu finden.

Wenn Sie diesen Mechanismus verwenden, stellen Sie sicher, dass `discoverReceiver` als alternativer Antragstellername im HTTPS-Zertifikat für den StoreFront-Server enthalten ist.

Neue Bereitstellung erstellen

December 5, 2023

1. Wenn die Citrix StoreFront-Verwaltungskonsole nach der Installation von StoreFront nicht bereits geöffnet ist, klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel "Citrix StoreFront".
2. Klicken Sie im Ergebnisbereich der Citrix StoreFront-Verwaltungskonsole auf **Neue Bereitstellung erstellen**.
3. Wenn es mehrere IIS-Sites gibt, wählen Sie aus der Dropdownliste **IIS-Site** die zu verwendende Site.

4. Wenn Sie einen einzelnen StoreFront-Server verwenden, geben Sie die **Basis-URL**der Server-URL ein. Wenn Sie mehrere StoreFront-Server hinter einem Load Balancer konfigurieren, geben Sie die Load Balancing-URL als **Basis-URL** ein.

   Wenn Sie noch keine Lastausgleichsumgebung eingerichtet haben, geben Sie die Server-URL an. Sie können die URL für Ihre Bereitstellung später jederzeit ändern.

5. Klicken Sie auf **Weiter** und konfigurieren Sie den ersten Store (siehe Store erstellen).
6. Wenn alle Konfigurationsschritte ausgeführt sind, klicken Sie auf **Erstellen**, um die Bereitstellung und den Store zu erstellen.
7. StoreFront zeigt eine Zusammenfassung des erstellten Stores an. Klicken Sie auf **Fertig stellen**.

Bereitstellung mit dem PowerShell-SDK erstellen

Um eine Bereitstellung mit dem PowerShell-SDK zu erstellen, rufen Sie das Cmdlet Add-STFDeployment auf.

Mehrere Internetinformationsdienste- (IIS)-Websites

StoreFront ermöglicht das Bereitstellen von unterschiedlichen Stores in verschiedenen IIS-Websites per Windows-Server, sodass jeder Store einen anderen Hostnamen und eine Zertifikatbindung haben kann.

Informationen zum Erstellen mehrerer Websites finden Sie in der Microsoft-IIS-Dokumentation.

Es ist nicht möglich, mehrere StoreFront-Bereitstellungen mit der Verwaltungskonsole zu erstellen. Sie müssen das PowerShell-SDK verwenden. Um beispielsweise zwei IIS-Websitebereitstellungen – eine für Anwendungen und eine für Desktops –zu erstellen, verwenden Sie folgende Befehle:

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"
Add-STFDeployment -SiteID 2 -HostBaseURL "https://desktops.example.com"
<!--NeedCopy-->
```

Sobald Sie mehrere Sites aktiviert haben, deaktiviert StoreFront die Verwaltungskonsole und kann nicht wieder in den Einzelsitemodus versetzt werden. Sie müssen die Sites mit dem StoreFront-SDK konfigurieren und in jedem Befehl die `SiteID` angeben.

Vorhandener Servergruppe beitreten

April 17, 2024

Bevor Sie StoreFront auf einem Server installieren, den Sie der Gruppe hinzufügen möchten, stellen Sie Folgendes sicher:

- Auf dem Server, den Sie der Gruppe hinzufügen, muss die gleiche Betriebssystemversion mit dem gleichen Gebietsschema ausgeführt werden, wie auf den anderen Servern in der Gruppe. StoreFront-Servergruppen mit unterschiedlichen Betriebssystemversionen und Gebietsschemas werden nicht unterstützt.
- Der relative Pfad zu StoreFront in IIS auf dem Server, den Sie hinzufügen, muss mit dem auf den anderen Servern in der Gruppe identisch sein.

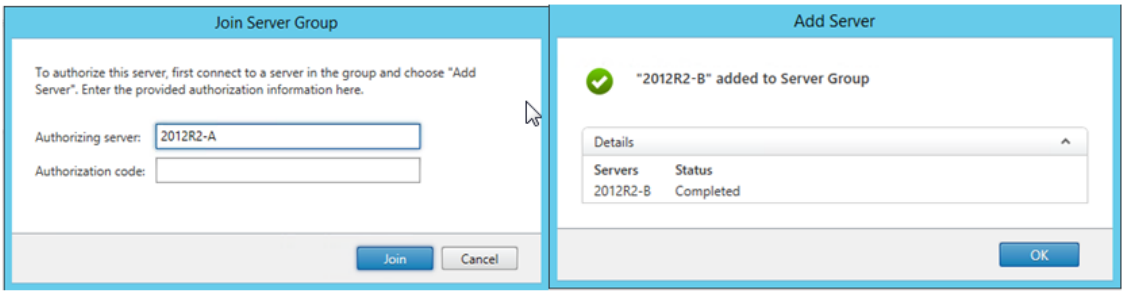
> **Hinweis:**
>
> Empfehlungen zur Größe der Servergruppen finden Sie unter StoreFront-Servergruppen.

Wurde der StoreFront-Server zuvor aus einer Servergruppe entfernt, kann er erst dann wieder zur gleichen oder einer anderen Servergruppe hinzugefügt werden, wenn Sie ihn auf die werkseitigen Standardeinstellungen zurückgesetzt haben. Siehe Zurücksetzen eines Servers auf die Werkseinstellungen.

> **Wichtig:**
>
> Wenn Sie einer Servergruppe einen neuen Server hinzufügen, werden StoreFront-Dienstkonten als Mitglieder der lokalen Administratorgruppe auf dem neuen Server hinzugefügt. Für diese Dienste sind lokalen Administratorberechtigungen erforderlich, um der Servergruppe beizutreten und für die Synchronisierung. Wenn Sie eine Gruppenrichtlinie verwenden, die verhindert, dass der lokalen Administratorgruppe neue Mitglieder hinzugefügt werden können, bzw. wenn Sie die Berechtigungen der lokalen Administratorgruppe auf den Servern einschränken, kann StoreFront nicht der Servergruppe beitreten.

1. Wenn die Citrix StoreFront-Verwaltungskonsole nach der Installation von StoreFront nicht bereits geöffnet ist, klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel "Citrix StoreFront".
2. Klicken Sie im Ergebnisbereich der Citrix StoreFront-Verwaltungskonsole auf **Vorhandener Servergruppe beitreten**.
3. Melden Sie sich bei einem Server in der StoreFront-Bereitstellung an, der Sie beitreten möchten, und öffnen Sie die Citrix StoreFront-Verwaltungskonsole. Wählen Sie im linken Bereich der Konsole den Knoten "Servergruppe"aus und klicken Sie im Bereich "Aktionen"auf **Server hinzufügen**. Notieren Sie sich den angezeigten Autorisierungscode.
4. Kehren Sie zum neuen Server zurück und geben Sie im Dialogfeld Servergruppe beitreten den Namen des vorhandenen Servers im Feld Autorisierungsserver an. Geben Sie den vom primären Server erhaltenen Autorisierungscode ein und klicken Sie auf **Beitreten**.

Nach dem Beitritt zu der Gruppe wird die Konfiguration des neuen Servers aktualisiert, damit sie mit der des vorhandenen Servers identisch ist. Alle anderen Server in der Gruppe werden mit den Informationen des neuen Servers aktualisiert.



Verwenden Sie zur Verwaltung einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Alle vorgenommenen Konfigurationsänderungen müssen an die anderen Server der Gruppe weitergegeben werden, damit eine konsistente Konfiguration der gesamten Bereitstellung gewährleistet ist.

StoreFront aktualisieren

February 28, 2024

Beim Upgrade bleibt Ihre StoreFront-Konfiguration erhalten, die Favoriten der Benutzer ebenso. Im Gegensatz dazu werden beim Deinstallieren von StoreFront neben StoreFront auch die zugehörigen Dienste, Sites, Favoriten (auf eigenständigen Servern) und die zugehörige Konfiguration entfernt.

Unterstützte Upgrade-Pfade

Sie können ein Upgrade auf die neueste CU von StoreFront 2203 durchführen von:

- StoreFront 2203 LTSR (Erstrelease oder eine beliebige CU)
- StoreFront 1912 LTSR (jedes CU)
- StoreFront 3.12 LTSR CU9

Um ein Upgrade von Versionen vor 3.12 CU9 durchzuführen, müssen Sie zuerst ein Upgrade auf StoreFront 3.12 CU9 durchführen.

> **Warnung:**
>
> Wenn Sie ein Upgrade von Versionen vor 1912 ausführen, werden alle Desktopgerätesites in der

> Bereitstellung automatisch entfernt. Als Alternative empfiehlt Citrix, den Citrix Workspace-App Desktop Lock für alle Anwendungsfälle ohne Domänenbindung zu verwenden.

Nützliche Info

- StoreFront unterstützt keine Multiserverbereitstellung mit mehreren Produktversionen. Daher müssen alle Server einer Gruppe auf dieselbe Version aktualisiert werden, bevor Zugriff auf die Bereitstellung erteilt wird.
- StoreFront unterstützt keine Bereitstellung mit mehreren Servern, auf denen unterschiedliche Betriebssysteme ausgeführt werden. Auf allen Servern in einer Servergruppe muss dasselbe Windows Server-Betriebssystem ausgeführt werden.
- Ein Upgrade aller Server in Bereitstellungen mit mehreren Servern in einem Arbeitsgang wird nicht unterstützt. Die Server müssen nacheinander aktualisiert werden.
- Bevor das StoreFront-Upgrade ausgeführt wird, erfolgen mehrere Prüfungen. Wird eine nicht bestanden, dann wird das Upgrade nicht gestartet und Sie werden über den Fehler benachrichtigt. Die StoreFront-Installation bleibt unverändert. Führen Sie nach dem Beheben des Fehlers das Upgrade erneut aus.
- Wenn das StoreFront-Upgrade selbst fehlschlägt, geht die ursprüngliche Konfiguration der StoreFront-Installation u. U. verloren. Stellen Sie die StoreFront-Installation in einen funktionierenden Zustand wieder her und führen Sie das Upgrade erneut aus. Zum Wiederherstellen von StoreFront gibt es folgende Möglichkeiten:
  - Wiederherstellen des VM-Snapshots, den Sie vor dem Upgrade erstellt haben
  - Importieren der StoreFront-Konfiguration, die Sie vor dem Upgrade exportiert haben, siehe Exportieren und Importieren der StoreFront-Konfiguration.
  - Durchführen der Problembehandlung wie unter Problembehandlung bei StoreFront-Upgradeproblemen beschrieben.
- Alle StoreFront-Upgradefehler im Citrix Virtual Apps and Desktops-Metainstaller werden in einem Dialogfeld mit einem Link zum entsprechenden Fehlerprotokoll gemeldet.

Vorbereitung des Upgrades

Citrix empfiehlt die Durchführung folgender Schritte vor einem Upgrade, um Fehlern beim Upgrade vorzubeugen:

- Planen Sie die Sicherung vor dem Upgrade.
- Stellen Sie sicher, dass Sie kein Upgrade von einer End-of-Life-StoreFront-Version versuchen. Weitere Informationen finden Sie unter CTX200356.
- Stellen Sie sicher, dass Sie ausschließlich ein Upgrade von einer unterstützten StoreFront-Version auf die aktuelle Version durchführen.

- Laden Sie das StoreFront-Installationsprogramm von der Citrix Website herunter.

Einzelnen StoreFront-Server aktualisieren

1. Sichern Sie den Server, indem Sie einen VM-Snapshot erstellen.
2. StoreFront-Konfiguration exportieren Wenn Sie mehrere Server in einer Servergruppe haben, exportieren Sie die Servergruppenkonfiguration von nur einem Server. Sofern Sie alle Änderungen zwischen den Servern einer Gruppe verteilt haben, ist die Konfiguration auf allen identisch. Mit diesem Backup können Sie mühelos eine neue Servergruppe erstellen, sodass Sie die Konfiguration bei Problemen leicht wiederherstellen können. Sie können das Backup nur auf einem Server derselben Version wiederherstellen, von der es exportiert wurde.
3. Wenn Sie Änderungen an Dateien in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` gemacht haben , z. B. default.ica und usernamepassword.tfrm, legen Sie für jeden Store ein Backup an. Nach dem Upgrade können Sie sie wiederherstellen, um Ihre Änderungen wieder anzuwenden.
4. Verhindern Sie, dass Benutzer eine Verbindung herstellen, indem Sie den Server aus dem Lastausgleich entfernen oder Verbindungen auf andere Weise blockieren.
5. Starten Sie den Server neu.
6. Stellen Sie sicher, dass keine Anwendungen (einschl. StoreFront-Verwaltungskonsole, Befehlszeilen- und PowerShell-Fenster) ausgeführt werden, die StoreFront-Dateien sperren könnten. So wird sichergestellt, dass das Installationsprogramm während des Upgrades auf alle StoreFront-Dateien zugreifen kann. Kann das Installationsprogramm auf eine Datei nicht zugreifen, dann wird diese nicht ersetzt und das Upgrade schlägt fehl, wodurch die vorhandene StoreFront-Konfiguration entfernt wird.
7. Stellen Sie sicher, dass weder Windows Explorer noch eine Befehlszeile für Verzeichnisse mit StoreFront-Dateien geöffnet sind.
8. Deaktivieren Sie alle Antivirus-Anwendungen.
9. Führen Sie die Installationsdatei der benötigten Version von StoreFront aus.

Upgrade einer StoreFront-Servergruppe

Beim Upgrade von StoreFront-Servergruppen wird ein Server verwendet, um die anderen Server aus der Gruppe zu entfernen. Die entfernten Server behalten die mit der Gruppe zusammenhängende Konfiguration bei, wodurch verhindert werden kann, dass sie einer neuen Servergruppe hinzugefügt werden. Bevor sie zum Erstellen neuer Servergruppen oder als eigenständige StoreFront-Server wiederverwendet werden können, müssen sie auf die Werkseinstellungen zurückgesetzt oder StoreFront muss neu auf ihnen installiert werden. Das gleichzeitige Aktualisieren der Server in einer StoreFront-Servergruppe wird nicht unterstützt.

Beispiel 1: Upgrade einer StoreFront-Servergruppe mit drei Knoten während der geplanten Wartung

Beschrieben wird das Upgrade einer StoreFront-Servergruppe mit den Servern A, B und C während einer geplanten Wartungsdowntime.

1. Deaktivieren Sie den Benutzerzugriff auf die Servergruppe, indem Sie die Lastausgleichs-URL deaktivieren. Dadurch wird verhindert, dass Benutzer während des Upgrades eine Verbindung mit der Bereitstellung herstellen.
2. Verwenden Sie Server A, um Server B und C aus der Gruppe zu entfernen.

   Server B und C sind nun kein Teil der Servergruppe mehr.
3. Aktualisieren Sie Server A gemäß den Anweisungen unter Einzelnen StoreFront-Server aktualisieren.
4. Stellen Sie sicher, dass Server A erfolgreich aktualisiert wurde.
5. Deinstallieren Sie auf den Servern B und C StoreFront und installieren Sie die neue StoreFront-Version.
6. Verbinden Sie die Server B und C mit Server A, um eine aktualisierte Servergruppe zu erstellen. Die Servergruppe besteht aus einem aktualisierten Server (A) und zwei neu installierten Servern (B und C).

   Der Prozess Beitreten zu einer vorhandenen Servergruppe verteilt automatisch alle Konfigurationsdaten und Abonnementdaten auf die neuen Server B und C.
7. Überprüfen Sie, ob alle Server ordnungsgemäß funktionieren.
8. Aktivieren Sie den Benutzerzugriff auf die aktualisierte Servergruppe, indem Sie die Lastausgleichs-URL aktivieren.

Beispiel 2: Upgrade einer StoreFront-Servergruppe mit drei Knoten ohne geplante Wartung

Beschrieben wird das Upgrade einer StoreFront-Servergruppe mit den Servern A, B und C ohne geplante Wartungsdowntime.

Vor dem Upgrade einer Servergruppe:

1. Exportieren Sie die StoreFront-Konfiguration unter Verwendung von **Export-STFConfiguration**. Diese Sicherung ist notwendig, da die Server später auf die Werkseinstellungen zurückgesetzt werden, wodurch Konfigurationsdaten gelöscht werden.
2. Exportieren Sie Abonnementdaten von Server A unter Verwendung von **Export-STFStoreSubscriptions**. Diese Sicherung ist notwendig, da die Server später auf die Werkseinstellungen zurückgesetzt

werden, wodurch Konfigurationsdaten gelöscht werden. Siehe Verwalten von Abonnementdaten für einen Store.

3. Deaktivieren Sie den Benutzerzugriff auf Server C, indem Sie ihn aus dem Load Balancer entfernen. Benutzer können sich dann während des Upgrades nicht mit Server C verbinden. Der Load Balancer sendet weiterhin Anforderungen an die Server A und B.
4. Verwenden Sie Server A, um Server C aus der Gruppe zu entfernen.
   Server A und B bieten weiterhin Zugriff auf die Ressourcen für die Benutzer. Server C ist nun aus der Servergruppe entfernt und wird auf die Werkseinstellungen zurückgesetzt.
5. Zurücksetzen von Server C auf die Werkseinstellungen mit **Clear-STFDeployment**.
6. Importieren Sie die StoreFront-Konfiguration, die Sie mit **Import-STFConfiguration** in Server C exportiert haben. Server C hat nun dieselbe Konfiguration wie die alte Servergruppe. Es ist *nicht* notwendig, diesen Schritt später zu wiederholen. Die Konfigurationsdaten müssen nur auf einem Server vorliegen, von wo aus sie auf andere Server verteilt werden, die der Gruppe beitreten.
7. Aktualisieren sie Server C gemäß den Anweisungen unter Einzelnen StoreFront-Server aktualisieren. Server C hat nun dieselbe Konfiguration wie die alte Servergruppe und wurde auf die neue StoreFront-Version aktualisiert.
8. Importieren Sie die Abonnementdaten, die Sie zuvor exportiert hatten, auf Server C. Dieser Schritt muss später *nicht* wiederholt werden. Die Abonnementdaten müssen nur auf einem Server vorliegen, von wo aus sie auf andere Server verteilt werden, die der Gruppe beitreten.
9. Wiederholen Sie die Schritte 3, 4, 5 und 7 für Server B (wiederholen Sie nicht Schritt 6). Während dieser Zeit können Benutzer nur über Server A auf Ressourcen zugreifen. Es empfiehlt sich daher, diesen Schritt zu einer Zeit auszuführen, zu der die StoreFront-Servergruppe nur minimal ausgelastet ist.
10. Fügen Sie Server A den Servergruppen B und C mit dem Prozess unter Vorhandener Servergruppe beitreten hinzu. Damit erhalten Sie eine Einzelserverbereitstellung für die aktuelle StoreFront-Version (Server A) und eine neue Servergruppe mit zwei Knoten in der neuen StoreFront-Version (Server B und C).
11. Fügen Sie die Server B und C zum Lastausgleich hinzu, damit sie die Funktion von Server A übernehmen können.
12. Entfernen Sie Server A aus dem Load Balancer, sodass Benutzer zu den neu aktualisierten Servern B und C weitergeleitet werden.
13. Wiederholen Sie die Schritte 3, 4, 5 und 7 für Server A (wiederholen Sie nicht Schritt 6). Das Upgrade der Servergruppe ist damit abgeschlossen. Server A, B und C verfügen über identische Konfigurations- und Abonnementdaten aus der ursprünglichen Gruppe.

> **Hinweis:**
>
> Während des kurzen Zeitraums, in dem Server A der einzige zugängliche Server ist, können Abonnementdaten verloren gehen (Schritt 9). Dies kann dazu führen, dass die neue Server-

> gruppe nach dem Upgrade eine leicht veraltete Kopie der Abonnementdatenbank hat und jegliche neuen Abonnementdatensätze verloren gehen.
>
> Dies hat keine Auswirkungen auf die Funktion, da Abonnementdaten nicht unbedingt benötigt werden, damit die Benutzer sich anmelden und Ressourcen starten können. Die Benutzer müssen in diesem Fall jedoch eine Ressource erneut abonnieren, wenn Server A auf die Werkseinstellungen zurückgesetzt und der neu aktualisierten Gruppe hinzugefügt wurde. Es gehen zwar in den allermeisten Fällen nur wenige Abonnementdatensätze verloren, dies ist jedoch als mögliche Folge eines Upgrades in einer aktiven StoreFront-Produktionsumgebung zu bedenken.

Vorgehen bei einem Upgradefehler

1. Öffnen Sie im Ordner *C:\Windows\Temp\StoreFront* das neueste *CitrixMsi*.log* und suchen Sie nach Ausnahmefehlern.

   Ausnahmen mit **Thumbs.db Access**: Verursacht durch *thumbs.db*-Dateien in *C:\inetpup\wwwroot\citrix* oder Unterverzeichnissen. Löschen Sie alle gefundenen Dateien *thumbs.db*-Dateien.

   Cannot get exclusive file access \in use: Stellen Sie den Snapshot/die Sicherung, falls verfügbar, wieder her oder starten Sie den Server neu und beenden Sie alle StoreFront-Dienste manuell.

   Service cannot be started: Stellen Sie den Snapshot/die Sicherung, falls verfügbar, wieder her oder installieren Sie die Vollversion von .NET Framework 4.5 (nicht Client Profile).

2. Enthält *CitrixMsi*.log* keine Ausnahmen, überprüfen Sie die Ereignisanzeige des Servers unter **Delivery Services** auf die o. a. Fehlermeldungen. Folgen Sie den entsprechenden Anweisungen.
3. Enthält die Ereignisanzeige keine Ausnahmefehler, überprüfen Sie die Admin-Protokolle unter *C:\Programme\Citrix\Receiver StoreFront\logs* auf die o. a. Fehlermeldungen. Folgen Sie den entsprechenden Anweisungen.

Weitere Informationen zu Protokolldateien finden Sie unter Installationsprotokolle.

Server auf die Werkseinstellungen zurücksetzen

April 17, 2024

Es kann notwendig werden, eine StoreFront-Installation auf den ursprünglichen Installationsstatus zurückzusetzen. Das ist beispielsweise dann erforderlich, wenn Sie einen StoreFront-Server einer Servergruppe erneut hinzufügen möchten.

Eine manuelle Deinstallation und Neuinstallation ist zwar möglich, dies ist jedoch zeitaufwändiger und kann unvorhergesehene Probleme verursachen. Stattdessen können Sie das PowerShell-Cmdlet **Clear-STFDeployment** ausführen, um den StoreFront-Server auf die werkseitigen Standardeinstellungen zurückzusetzen.

1. Stellen Sie sicher, dass die StoreFront-Verwaltungskonsole geschlossen ist.
2. Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.
3. Legen Sie den PowerShell-Pfad fest:

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('
    PSModulePath','Machine')
<!--NeedCopy-->
```

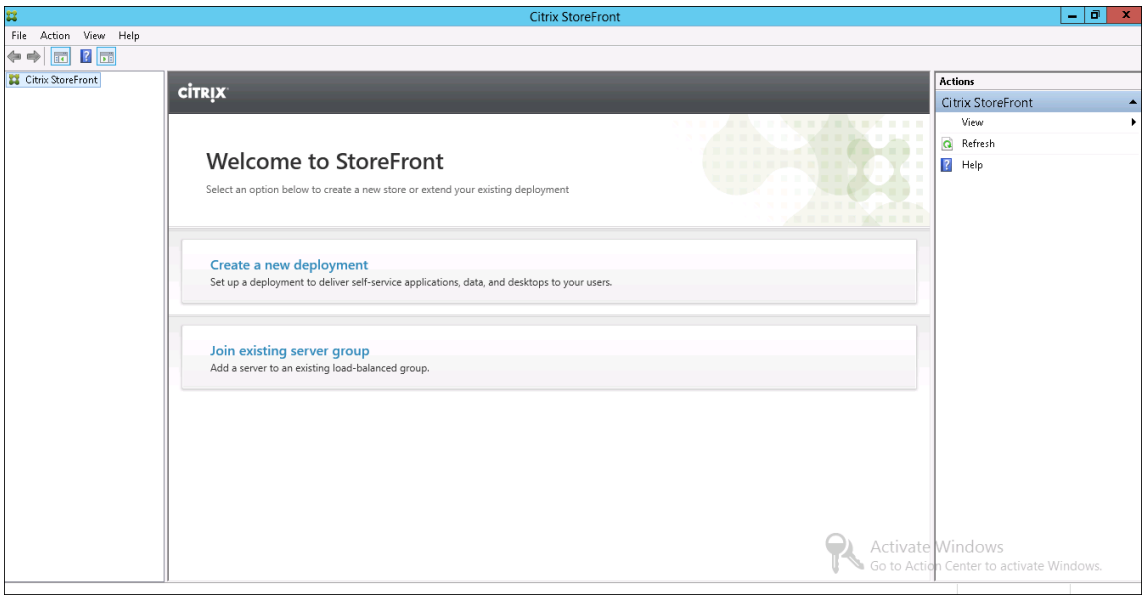
4. Importieren Sie das Citrix StoreFront-Modul.

```
Import-Module citrix.storefront -verbose
<!--NeedCopy-->
```

5. Führen Sie nach dem Importieren des Moduls den Befehl **Clear-STFDeployment** aus, um den StoreFront-Server auf die Standardeinstellungen zurückzusetzen:

```
Clear-STFDeployment -Confirm $False
<!--NeedCopy-->
```

6. Wenn der Befehl erfolgreich ausgeführt wurde, öffnen Sie die StoreFront-Verwaltungskonsole, und stellen Sie sicher, dass alle Einstellungen zurückgesetzt wurden. Die Optionen **Neue Bereitstellung erstellen** bzw. **Vorhandener Servergruppe beitreten** stehen zur Verfügung.



StoreFront deinstallieren

February 28, 2024

Neben dem Produkt selbst werden bei der Deinstallation von StoreFront der Authentifizierungsdienst, die Stores, Citrix Receiver für Web-Sites sowie XenApp Services-URLs und die zugeordneten Konfigurationen entfernt. Der Abonnementstoredienst, der die Anwendungsabonnementdaten der Benutzer enthält, wird ebenfalls gelöscht. Bei Einzelserverbereitstellungen gehen die Details zu den Anwendungsabonnements der Benutzer daher verloren. Bei Multiserverbereitstellungen werden diese Daten jedoch auf den anderen Servern der Gruppe beibehalten. Erforderliche Komponenten, die vom StoreFront-Installationsprogramm aktiviert werden, z. B. .NET Framework-Features und die Webserver (IIS)-Rollendienste, werden nicht vom Server entfernt, wenn StoreFront deinstalliert wird.

1. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen bei StoreFront an.
2. Schließen Sie die StoreFront-Verwaltungskonsole, falls sie geöffnet ist.
3. Schließen Sie alle PowerShell-Sitzungen, mit denen Sie ggf. StoreFront über das PowerShell SDK verwaltet haben.
4. Öffnen Sie das **Startmenü**, wählen Sie **Einstellungen** (Zahnradsymbol) und gehen Sie zu **Apps**.
5. Wählen Sie im Fenster **Programme und Funktionen Citrix StoreFront** aus und klicken Sie auf **Deinstallieren**, um alle StoreFront-Komponenten vom Server zu entfernen.
6. Klicken Sie im Dialogfeld **Citrix StoreFront deinstallieren** auf **Ja**. Wenn die Deinstallation abgeschlossen ist, klicken Sie auf **OK**.

Manuelles Entfernen von StoreFront

Vergewissern Sie sich nach der Deinstallation von StoreFront, dass es vollständig entfernt wurde:

1. Entfernen Sie die Webserverrolle.
2. Löschen Sie den Ordner *C: Programme\Citrix\Receiver StoreFront*.
3. Löschen Sie alle Unterverzeichnisse unter *C:\Programme\Citrix\StoreFront Install*.
4. Löschen Sie den Ordner *C:\Inetpub*.

Sie können StoreFront jetzt neu installieren.

Installationsprotokolle

Weitere Informationen zu Protokolldateien finden Sie unter Installationsprotokolle.

Authentifizierung und Delegierung konfigurieren

February 28, 2024

Es gibt mehrere Methoden für die Authentifizierung und Delegierung, die je nach den Anforderungen gewählt werden können.

Methode	Detail
Authentifizierung konfigurieren	Konfigurieren Sie die Methoden, mit denen die Benutzer sich über die Citrix Workspace-App bei StoreFront anmelden können.
Smartcardauthentifizierung	Richten Sie die Smartcardauthentifizierung ein.
Authentifizierung mit Benutzernamen und Kennwort	Erlauben Sie Benutzern, sich mit ihrem Active Directory-Benutzernamen und -Kennwort zu authentifizieren und konfigurieren Sie Optionen zum Ändern von Kennwörtern und Benachrichtigungen zum Ablauf von Kennwörtern.
Domänen-Passthrough-Authentifizierung	Erlauben Sie Windows-Geräten das Single Sign-On mit ihren Windows-Anmeldeinformationen.
SAML-Authentifizierung	Delegieren Sie die Authentifizierung mit SAML an externe Identitätsanbieter.
Verbundauthentifizierungsdienst konfigurieren	StoreFront zur Integration mit dem Verbundauthentifizierungsdienst für das Single Sign-On bei VDAs konfigurieren

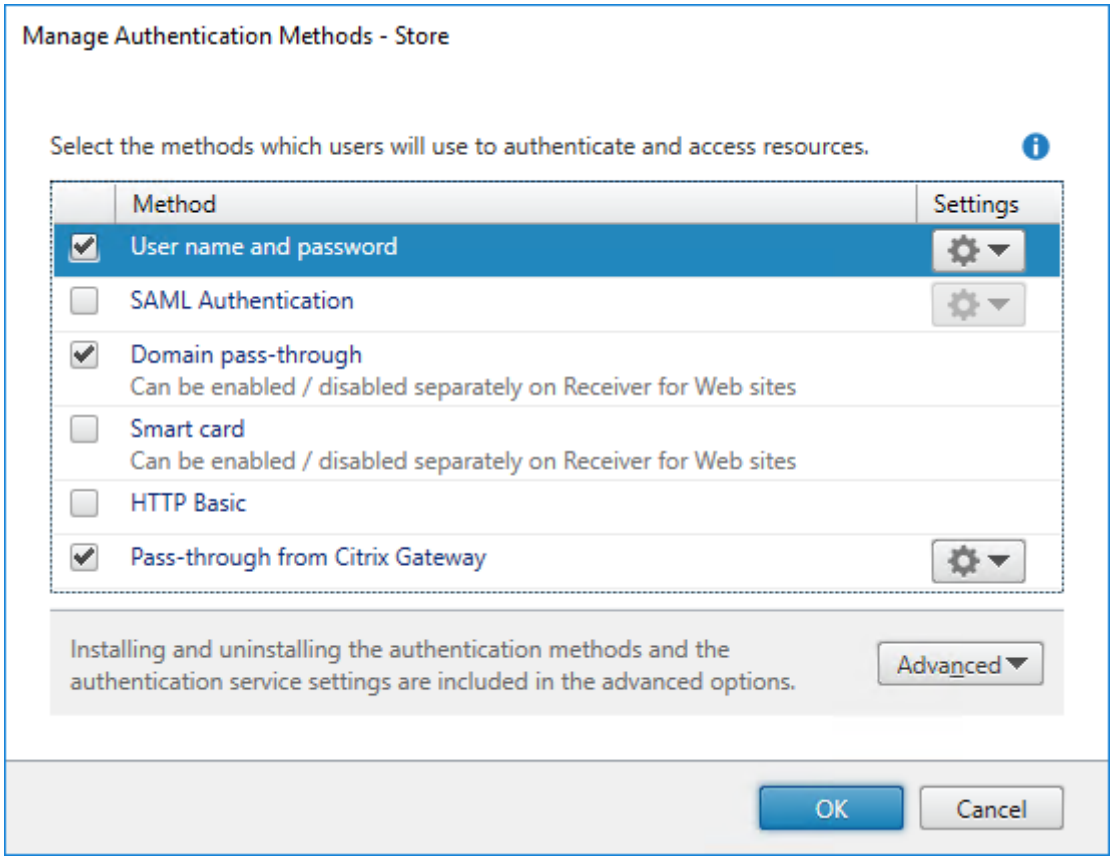
Authentifizierung konfigurieren

April 17, 2024

Authentifizierungsmethoden verwalten

Für jeden Store können Sie eine oder mehrere Authentifizierungsmethoden auswählen, die bei der Anmeldung beim Store über die Citrix Workspace-App verfügbar sind.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
2. Geben Sie an, welche Zugriffsmethoden für die Benutzer aktiviert werden sollen.



- Aktivieren Sie das Kontrollkästchen **Benutzername und Kennwort**, um die explizite Authentifizierung über den AD-Benutzernamen und das Kennwort zu aktivieren. Weitere Informationen finden Sie unter Authentifizierung mit Benutzernamen und Kennwort.
- Wählen Sie das Kontrollkästchen **SAML-Authentifizierung**, um die Integration eines SAML-Identitätsanbieters zu ermöglichen. Weitere Informationen finden Sie unter SAML-Authentifizierung.
- Aktivieren Sie **Domänen-Passthrough**, um Passthrough für Active Directory-Domänenanmeldeinformationen von Benutzergeräten zu aktivieren. Weitere Informationen finden Sie unter Domänen-Passthrough-Authentifizierung.
- Aktivieren Sie **Smartcard**, um die Smartcardauthentifizierung zu aktivieren. Weitere Informationen finden Sie unter Smartcardauthentifizierung.
- Aktivieren Sie **HTTP Basic**, um die HTTP Basic-Authentifizierung zu aktivieren. Benutzer authentifizieren sich über den IIS-Webserver des StoreFront-Servers.
- Aktivieren Sie **Passthrough-Authentifizierung von Citrix Gateway** zum Aktivieren der Passthrough-Authentifizierung von Citrix Gateway. Aktivieren Sie diese Option, wenn die Benutzer über ein Citrix Gateway mit aktivierter Authentifizierung auf StoreFront zugreifen.

Weitere Informationen finden Sie unter Passthrough-Authentifizierung von Citrix Gateway.

Das Ändern der Authentifizierungsmethoden für einen Store aktualisiert auch die Authentifizierungsmethoden für den Zugriff auf den Store über einen Webbrowser. Informationen zum Ändern der Authentifizierungsmethoden für die Anmeldung über einen Webbrowser finden Sie unter Authentifizierungsmethoden.

Authentifizierungsmethoden mithilfe des PowerShell-SDKs verwalten

Gehen Sie zum Konfigurieren der Authentifizierung mit dem PowerShell-SDK folgendermaßen vor:

1. Rufen Sie Get-STFAuthenticationService auf, um den Authentifizierungsdienst für einen Store oder ein virtuelles Verzeichnis aufzurufen und dessen aktuelle Konfiguration anzuzeigen.
2. Aktivieren bzw. deaktivieren Sie für den Authentifizierungsdienst die Authentifizierungsprotokolle nach Bedarf. Führen Sie Get-STFAuthenticationServiceProtocol aus, um eine Liste der verfügbaren Protokolle aufzurufen. Um die Protokolle zu aktivieren, führen Sie Enable-STFAuthenticationServiceProtocol mit einer Liste der zu aktivierenden Protokolle aus. Um die Protokolle zu deaktivieren, führen Sie Disable-STFAuthenticationServiceProtocol mit der Liste der zu deaktivierenden Protokolle aus.
3. Konfigurieren Sie die Authentifizierungsprotokolle, die Sie aktiviert haben. Einzelheiten finden Sie in der Dokumentation zu den einzelnen Protokollen.

Einstellungen für gemeinsam genutzte Authentifizierung

Verwenden Sie die Aufgabe zur Einstellung des gemeinsam genutzten Authentifizierungsdiensts zum Angeben von Stores, die den Authentifizierungsdienst gemeinsam verwenden, sodass Single Sign-On möglich ist.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
2. Wählen Sie im Dropdownmenü **Erweitert** die Option **Freigegebener Authentifizierungsdienst - Einstellungen** aus.
3. Klicken Sie auf das Kontrollkästchen **Freigegebenen Authentifizierungsdienst verwenden** und wählen Sie einen Store aus dem Dropdownmenü **Store** aus.

> **Hinweis:**
>
> Es gibt keinen funktionalen Unterschied zwischen einem gemeinsam genutzten und einem dedizierten Authentifizierungsdienst. Ein von mehreren Stores genutzter Authentifizierungsdienst wird als gemeinsam verwendeter Authentifizierungsdienst behandelt und alle Konfigurationsän-

> derungen gelten für alle Stores, die den Authentifizierungsdienst gemeinsam nutzen.

Smartcardauthentifizierung

April 17, 2024

Benutzer authentifizieren sich mit Smartcards und PINs beim Zugriff auf ihre Stores. Wenn Sie StoreFront installieren, wird die Smartcardauthentifizierung standardmäßig deaktiviert. Die Smartcardauthentifizierung kann für Benutzer aktiviert werden, die über die Citrix Workspace-App, Webbrowser und XenApp Services-URLs eine Verbindung mit Stores herstellen.

Verwenden Sie die Smartcardauthentifizierung, um den Anmeldeprozess für Ihre Benutzer zu optimieren und gleichzeitig die Sicherheit des Benutzerzugriffs auf Ihre Infrastruktur zu erhöhen. Der Zugriff auf das interne Unternehmensnetzwerk ist durch die zertifikatbasierte Zweifaktorauthentifizierung mit der Public Key-Infrastruktur geschützt. Private Schlüssel werden über die Hardware geschützt und verlassen nie die Smartcard. Die Benutzer können auf ihre Desktops und Anwendungen von unterschiedlichen Geräten des Unternehmens aus bequem mit Smartcard und PIN zugreifen.

Sie können Smartcards für die Benutzerauthentifizierung über StoreFront bei von Citrix Virtual Apps and Desktops bereitgestellten Desktops und Anwendungen verwenden. Benutzer von Smartcards, die sich bei StoreFront anmelden, können auch auf von Endpoint Management bereitgestellte Anwendungen zugreifen. Für den Zugriff auf Endpoint Management-Webanwendungen, für die Clientzertifikatauthentifizierung verwendet wird, müssen sich Benutzer jedoch neu authentifizieren.

Zum Aktivieren der Smartcardauthentifizierung müssen Benutzerkonten entweder in der Microsoft Active Directory-Domäne der StoreFront-Server konfiguriert werden oder in einer Domäne, die über eine direkte bidirektionale Vertrauensstellung mit der StoreFront-Serverdomäne verfügt. Bereitstellungen mit mehreren Gesamtstrukturen und bidirektionalen Vertrauensstellungen werden unterstützt.

Die Konfiguration der Smartcardauthentifizierung bei StoreFront hängt von den Benutzergeräten, den installierten Clients und davon ab, ob die Geräte in die Domäne eingebunden sind. In diesem Zusammenhang bedeutet in die Domäne eingebunden, das die Geräte in eine Domäne in der Active Directory-Gesamtstruktur eingebunden sind, die die StoreFront-Server enthält.

Das Dokument Smart card configuration for Citrix environments beschreibt, wie eine Citrix-Bereitstellung für eine bestimmte Art von Smartcards konfiguriert wird. Bei Smartcards anderer Hersteller sind die Arbeitsschritte ähnlich.

Voraussetzungen

- Stellen Sie sicher, dass die Konten für alle Benutzer entweder in der Microsoft Active Directory-Domäne konfiguriert werden, in der Sie die StoreFront-Server bereitstellen, oder in einer Domäne, die eine direkte bidirektionale Vertrauensstellung mit der StoreFront-Serverdomäne hat.
- Wenn Sie die Passthrough-Authentifizierung mit Smartcards aktivieren möchten, müssen Sie sicherstellen, dass die Smartcardleser, die Art und Konfiguration der Middleware und die Richtlinie für das Zwischenspeichern von Middleware-PINs dies gestatten.
- Installieren Sie die Smartcard-Middleware des Herstellers auf den virtuellen oder physischen Maschinen, auf denen Virtual Delivery Agent zur Bereitstellung von Desktops und Anwendungen ausgeführt wird. Weitere Informationen zur Verwendung von Smartcards mit Citrix Virtual Desktops finden Sie unter Smartcards.
- Stellen Sie sicher, dass die Public Key-Infrastruktur entsprechend konfiguriert ist. Prüfen Sie die ordnungsgemäße Konfiguration der Zertifikat-/Kontenzuordnung für die Active Directory-Umgebung und ob die Zertifikatüberprüfung erfolgreich ausgeführt werden kann.

Konfigurieren von StoreFront

- Sie müssen HTTPS für die Kommunikation zwischen StoreFront und Benutzergeräten verwenden, um die Smartcardauthentifizierung zu aktivieren. Siehe Secure StoreFront using HTTPS.
- Zur Aktivierung von Smartcardauthentifizierung für den Zugriff auf Stores über die Citrix Workspace-App aktivieren Sie **Smartcard** unter Authentifizierungsmethoden.
- Wenn Sie die Smartcardauthentifizierung für einen Store standardmäßig aktivieren, wird sie auch für alle Websites für diesen Store aktiviert. Sie können die Smartcardauthentifizierung für einzelne Websites auf der Registerkarte Authentifizierungsmethoden unter “Receiver für Web-Sites verwalten”separat aktivieren oder deaktivieren.
- Wenn Sie die Smartcardauthentifizierung und die Authentifizierung mit Benutzernamen und Kennwort konfigurieren, werden die Benutzer zunächst aufgefordert, sich mit der Smartcard und PIN anzumelden, können aber bei Problemen mit der Smartcard die explizite Authentifizierung auswählen.

Delivery Controller so konfigurieren, dass er StoreFront vertraut

Bei Verwendung der Smartcardauthentifizierung hat StoreFront keinen Zugriff auf die Anmeldeinformationen des Benutzers und kann sich daher nicht bei Citrix Virtual Apps and Desktops authentifizieren. Sie müssen den Delivery Controller daher so konfigurieren, dass er Anfragen von

StoreFront vertraut. Weitere Informationen finden Sie unter Überlegungen und Best Practices zur Sicherheit von Citrix Virtual Apps and Desktops.

Remotezugriff über Citrix Gateway

Für den Remotezugriff können Sie Smartcards auf dem Citrix Gateway und die Passthrough-Authentifizierung für StoreFront mit delegierter Authentifizierung aktivieren. Weitere Informationen finden Sie unter Gateway-Passthrough.

Sie können sicherstellen, dass die Benutzer beim Herstellen einer Verbindung zu ihren Ressourcen nicht ein weiteres Mal vom virtuellen Server aufgefordert werden, ihre Anmeldeinformationen einzugeben, indem Sie ein zweites Gateway erstellen und die Clientauthentifizierung in den SSL-Parametern deaktivieren. Weitere Informationen finden Sie unter Konfigurieren der Smartcardauthentifizierung. Beim Zugriff auf StoreFront über ein Citrix Gateway mit Smartcardauthentifizierung. Konfigurieren Sie das optimale Gatewayrouting über diesen virtuellen Server für Verbindungen mit den Bereitstellungen von Desktops und Anwendungen für den Store. Weitere Informationen finden Sie unter Konfigurieren des optimalen HDX-Routings für einen Store.

Single Sign-On auf VDAs

Sie können Single Sign-On für die VDAs aktivieren, indem Sie die Smartcardanmeldeinformationen der Benutzer weitergeben. Auf den Store kann über einen Webbrowser oder die Citrix Workspace-App für Windows zugegriffen werden, die Ressource muss jedoch in der Citrix Workspace-App für Windows geöffnet werden. Auf anderen Betriebssystemen oder beim Zugriff auf die Ressourcen über einen Browser müssen Benutzer ihre Anmeldeinformationen erneut eingeben, wenn sie eine Verbindung zu einem VDA herstellen.

1. Schließen Sie bei der Installation von Citrix Workspace für Windows die Single Sign On-Komponente ein und konfigurieren Sie sie für Single Sign On. Siehe Konfigurieren von Domänen-Passthrough-Authentifizierung.
2. Verwenden Sie einen Texteditor, um die Datei default.ica für den Store zu öffnen. Siehe Default ICA.
3. Für Passthrough von Smartcardanmeldeinformationen für Benutzer, die ohne Citrix Gateway auf Stores zugreifen, fügen Sie die folgende Einstellung im Bereich [Application] hinzu.

   ```
   DisableCtrlAltDel=Off
   ```

   Diese Einstellung gilt für alle Benutzer des Stores. Um die Passthrough-Authentifizierung für Domänen und mit Smartcards für Desktops und Anwendungen zu aktivieren, müssen Sie für jede Authentifizierungsmethode separate Stores erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.

4. Für Passthrough von Smartcardanmeldeinformationen für Benutzer, die mit Citrix Gateway auf Stores zugreifen, fügen Sie die folgende Einstellung im Bereich [Application] hinzu.

   ```
   UseLocalUserAndPassword=On
   ```

   Diese Einstellung gilt für alle Benutzer des Stores. Um die Passthrough-Authentifizierung für bestimmte Benutzer zu aktivieren, während andere sich anmelden müssen, um auf ihre Desktops und Anwendungen zuzugreifen, müssen Sie für jede Gruppe von Benutzern verschiedenen Stores erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.

Single Sign-On bei VDAs mit FAS

Alternativ können Sie den Verbundauthentifizierungsdienst für Single Sign-On auf VDAs konfigurieren, wenn Sie die lokal installierte Citrix Workspace-App verwenden, aber nicht die Citrix Workspace-App für HTML5.

Wichtige Überlegungen

Die Verwendung von Smartcards für die Benutzerauthentifizierung bei StoreFront unterliegt den folgenden Anforderungen und Einschränkungen.

- Zur Verwendung eines VPN-Tunnels mit Smartcardauthentifizierung müssen die Benutzer das Citrix Gateway-Plug-In installieren und sich über eine Webseite anmelden, wobei sie sich für jeden Schritt mit Smartcard und PIN authentifizieren. Die Passthrough-Authentifizierung bei StoreFront mit dem Citrix Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.
- Auf einem Benutzergerät können mehrere Smartcards und mehrere Smartcardleser verwendet werden. Wenn Sie jedoch die Passthrough-Authentifizierung mit Smartcard aktivieren, müssen Benutzer darauf achten, dass beim Zugriff auf einen Desktop oder eine Anwendung nur eine Smartcard eingeführt ist.
- Wird eine Smartcard innerhalb einer Anwendung verwendet (z. B. zur digitalen Signierung oder zur Verschlüsselung), werden möglicherweise zusätzliche Aufforderungen zum Einführen einer Smartcard oder zur Eingabe einer PIN angezeigt. Dieser Fall kann eintreten, wenn eine oder mehrere Smartcards gleichzeitig eingelegt wurden. Er kann auch aufgrund von Konfigurationseinstellungen eintreten, z. B. bei Middleware-Einstellungen wie PIN-Zwischenspeicherung, die in der Regel mit der Gruppenrichtlinie konfiguriert werden. Wenn Benutzer zum Einlegen einer Smartcard aufgefordert werden und die Smartcard bereits im Leser ist, müssen sie auf "Abbrechen"klicken. Wenn Benutzer aufgefordert werden, eine PIN einzugeben, müssen sie die PIN neu eingeben.

- Wenn Sie die Passthrough-Authentifizierung mit Smartcards bei Citrix Virtual Apps and Desktops für Benutzer der Citrix Workspace-App für Windows aktivieren, die domänengebundene Geräte verwenden und nicht über Citrix Gateway auf Stores zugreifen, gilt diese Einstellung für alle Benutzer des Stores. Um die Passthrough-Authentifizierung für Domänen und mit Smartcards für Desktops und Anwendungen zu aktivieren, müssen Sie für jede Authentifizierungsmethode separate Stores erstellen. Die Benutzer müssen dann eine Verbindung mit dem für ihre Authentifizierungsmethode geeigneten Store herstellen.
- Wenn Sie die Passthrough-Authentifizierung mit Smartcards bei Citrix Virtual Apps and Desktops für Benutzer der Citrix Workspace-App für Windows aktivieren, die domänengebundene Geräte verwenden und über Citrix Gateway auf Stores zugreifen, gilt diese Einstellung für alle Benutzer des Stores. Wenn Sie die Passthrough-Authentifizierung für bestimmte Benutzer aktivieren und für andere die Anmeldung an Desktops und Anwendungen erzwingen möchten, müssen Sie separate Stores für jede Benutzergruppe erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.
- Nur eine Authentifizierungsmethode kann für jede XenApp Services-URL konfiguriert werden und pro Store ist nur eine URL verfügbar. Wenn Sie zusätzlich zur Smartcardauthentifizierung weitere Authentifizierungsmethoden aktivieren möchten, müssen Sie für jede Authentifizierungsmethode einen eigenen Store mit einer XenApp Services-URL erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.
- Wenn StoreFront installiert ist, erfordert die Standardkonfiguration in Microsoft Internetinformationsdienste (IIS) nur, dass Clientzertifikate für HTTPS-Verbindungen mit der URL für die Zertifikatauthentifizierung des StoreFront-Authentifizierungsdiensts präsentiert werden. IIS fordert keine Clientzertifikate für andere StoreFront-URLs an. Dank dieser Konfiguration können Sie Smartcardbenutzern die Option des Fallbacks auf die explizite Authentifizierung gewähren, wenn diese Probleme mit ihren Smartcards haben. Abhängig von den entsprechenden Windows-Richtlinieneinstellungen können Benutzer auch ihre Smartcard entfernen, ohne sich neu authentifizieren zu müssen.

  Wenn Sie IIS für die Anforderung von Clientzertifikaten für alle HTTPS-Verbindungen mit allen StoreFront-URLs konfigurieren, müssen Authentifizierungsdienst und Stores auf demselben Server sein. Sie müssen ein Clientzertifikat verwenden, das für alle Stores gültig ist. Innerhalb dieser IIS-Sitekonfiguration können Smartcardbenutzer keine Verbindung über Citrix Gateway herstellen und nicht auf die explizite Authentifizierung zurückgreifen. Sie müssen sich dann neu anmelden, wenn sie ihre Smartcards aus Geräten entfernen.

Domänen-Passthrough-Authentifizierung

April 17, 2024

Die Benutzer authentifizieren sich bei ihrem domänengebundenen Computer und ihre Anmeldeinformationen werden für die automatische Anmeldung bei der Citrix Workspace-App verwendet. Dies wird von der Citrix Workspace-App für Windows und den folgenden Webbrowsern unter Windows unterstützt:

- Internet Explorer
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

StoreFront-Konfiguration

Um Domänen-Passthrough für Citrix Workspace-Apps für Windows zu aktivieren, wählen Sie unter Authentifizierungsmethoden die Option **Domänen-Passthrough** aus.

Wenn Sie die Passthrough-Authentifizierung für einen Store standardmäßig aktivieren, wird sie auch für alle Sites dieses Stores für Citrix Workspace-App für HTML5 aktiviert. Sie können die Passthrough-Authentifizierung für einzelne Websites auf der Registerkarte Authentifizierungsmethoden unter "Receiver für Web-Sites verwalten"separat aktivieren oder deaktivieren.

Delivery Controller so konfigurieren, dass er StoreFront vertraut

Bei Verwendung der Domänen-Passthrough-Authentifizierung hat StoreFront keinen Zugriff auf die Anmeldeinformationen des Benutzers und kann sich daher nicht bei Citrix Virtual Apps and Desktops authentifizieren. Sie müssen den Delivery Controller daher so konfigurieren, dass er Anfragen von StoreFront vertraut. Weitere Informationen finden Sie unter Überlegungen und Best Practices zur Sicherheit von Citrix Virtual Apps and Desktops.

Single Sign-On auf VDAs

Für das Single Sign-On bei VDAs müssen Sie die Citrix Workspace-App für Windows mit der Komponente **Single Sign-On aktivieren** verwenden (siehe Domänen-Passthrough-Authentifizierung konfigurieren). Wenn Sie die Citrix Workspace-App für HTML5 verwenden, muss sie so konfiguriert werden, dass sie eine Verbindung zu Ressourcen in der Citrix Workspace-App für Windows und nicht im Browser herstellt.

Konfiguration der Citrix Workspace-App für Windows

Informationen zum Aktivieren des Domänen-Passthrough für Single Sign-On für den Store und die VDAs mit der Citrix Workspace-App für Windows finden Sie in der Dokumentation zur Citrix Workspace-App für Windows.

Konfiguration der Citrix Workspace-App für HTML5

Möglicherweise müssen Sie die Webbrowserkonfiguration der Benutzer aktualisieren, um die Domänen-Passthrough-Authentifizierung zu ermöglichen. Sie können Domänen-Passthrough verwenden, um sich über einen Webbrowser bei einem Store anzumelden. Für Single Sign-On bei den VDAs müssen Benutzer Ressourcen in der Citrix Workspace-App für Windows und nicht im Webbrowser öffnen.

Internet Explorer, Edge und Chrome Die Workspace-App und die meisten Webbrowser verwenden die Konfiguration von Windows Explorer-Zonen, um zu entscheiden, ob Single Sign-On aktiviert werden soll. Standardmäßig ist es nur für Sites in der lokalen Intranetzone aktiviert. So fügen Sie Ihre Site zur Intranetzone hinzu:

1. Öffnen Sie die Systemsteuerung.
2. Öffnen Sie die Internetoptionen.
3. Gehen Sie zur Registerkarte **Sicherheit**.
4. Wählen Sie **Lokales Intranet**.
5. Klicken Sie auf **Sites**.
6. Klicken Sie auf **Erweitert**.
7. Fügen Sie Ihre StoreFront-Website hinzu.

Diese Einstellungen können mithilfe der Gruppenrichtlinie bereitgestellt werden.

Firefox Ändern Sie die erweiterten Browsereinstellungen so, dass dem StoreFront-Website-URI für Single Sign-On vertraut wird.

> **Warnung:**
>
> Fehlerhafte Änderungen an den erweiterten Einstellungen können zu schwerwiegenden Problemen führen. Änderungen machen Sie auf eigene Gefahr.

1. Öffnen Sie Firefox auf dem Computer, der sich mit Domänen-Passthrough authentifizieren wird.
2. Geben Sie in der Adressleiste “about:config”ein.
3. Klicken Sie auf “Ich akzeptiere das Risiko!”.
4. Geben Sie in der Suchleiste “negotiate”ein.

5. Doppelklicken Sie auf "network.negotiate-auth.delegation-uris".
6. Geben Sie den Namen Ihrer Windows-Unternehmensdomäne ein (z. B. "mydomain.com").
7. Klicken Sie auf OK.
8. Doppelklicken Sie auf "network.negotiate-auth.trusted-uris".
9. Geben Sie den Namen Ihrer Windows-Unternehmensdomäne ein (z. B. "mydomain.com").
10. Klicken Sie auf OK.
11. Schließen Sie Firefox und starten Sie ihn neu.

Single Sign-On bei VDAs mit FAS

Alternativ können Sie den Verbundauthentifizierungsdienst für Single Sign-On auf VDAs konfigurieren, wenn Sie die lokal installierte Citrix Workspace-App verwenden, aber nicht die Citrix Workspace-App für HTML5.

Passthrough-Authentifizierung von Citrix Gateway

April 17, 2024

Die Benutzer authentifizieren sich bei Citrix Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet. Die Passthrough-Authentifizierung von Citrix Gateway ist standardmäßig aktiviert, wenn Sie eine erste Konfiguration des Remotezugriffs auf den Store durchführen. Die Benutzer können mithilfe der Citrix Workspace-App oder eines Webbrowsers über Citrix Gateway eine Verbindung mit Stores herstellen. Weitere Informationen zum Konfigurieren von StoreFront für Citrix Gateway finden Sie unter Citrix Gateway konfigurieren.

StoreFront unterstützt Passthrough mit den folgenden Citrix Gateway-Authentifizierungsmethoden.

- **Domäne:** Die Benutzer melden sich mit ihrem Active Directory-Benutzernamen und -Kennwort an.
- **RSA:** Die Benutzer melden sich bei Citrix Gateway mit Passcodes an, die von mit Sicherheitstoken generierten Tokencodes abgeleitet werden, in einigen Fällen in Kombination mit persönlichen Identifikationsnummern. Wenn Sie zur Passthrough-Authentifizierung ausschließlich Sicherheitstoken aktivieren, stellen Sie sicher, dass die von Ihnen bereitgestellten Ressourcen keine zusätzlichen oder alternativen Authentifizierungsformen erfordern, wie Microsoft Active Directory-Domänenanmeldeinformationen.
- **Smartcard:** Die Benutzer melden sich mit Smartcards an
- **RSA + Domäne:** Benutzer, die sich an Citrix Gateway anmelden, müssen ihre Domänenanmeldeinformationen und ihre Sicherheitstoken-Passcodes eingeben.

Wenn Sie für das Citrix Gateway die Authentifizierung oder Single Sign-On deaktiviert haben, wird Passthrough nicht verwendet und Sie müssen eine der anderen Authentifizierungsmethoden konfigurieren.

Wenn Sie die Zweiquellenauthentifizierung bei Citrix Gateway für Remotebenutzer konfigurieren, die von der Citrix Workspace-App aus auf Stores zugreifen, müssen Sie zwei Authentifizierungsrichtlinien für Citrix Gateway erstellen. Konfigurieren Sie RADIUS (Remote Authentication Dial-In User Service) als primäre Authentifizierungsmethode und LDAP (Lightweight Directory Access Protocol) als sekundäre Methode. Ändern Sie den Anmeldeinformationsindex zur Verwendung der sekundären Authentifizierungsmethode im Sitzungsprofil, sodass LDAP-Anmeldeinformationen an StoreFront übergeben werden. Wenn Sie das Citrix Gateway-Gerät zu Ihrer StoreFront-Konfiguration hinzufügen, legen Sie den Anmeldetyp auf "Domäne und Sicherheitstoken"fest. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX125364

Um die Multidomänenauthentifizierung über Citrix Gateway zu StoreFront zu aktivieren, setzen Sie in der Citrix Gateway-LDAP-Authentifizierungsrichtlinie für jede Domäne das SSO-Namensattribut auf "userPrincipalName". Sie können festlegen, dass die Benutzer auf der Citrix Gateway-Anmeldeseite eine Domäne angeben müssen, sodass die richtige zu verwendende LDAP Richtlinie ermittelt werden kann. Geben Sie beim Konfigurieren der Citrix Gateway-Sitzungsprofile für Verbindungen mit StoreFront keine Single Sign-On-Domäne an. Sie müssen Vertrauensstellungen zwischen allen Domänen konfigurieren. Stellen Sie sicher, dass Benutzer sich von allen Domänen aus an StoreFront anmelden können, indem Sie den Zugriff nicht auf explizit vertrauenswürdige Domänen beschränken.

Wenn die Citrix Gateway-Bereitstellung dies unterstützt, können Sie SmartAccess zur Steuerung des Benutzerzugriffs auf Citrix Virtual Apps and Desktops-Ressourcen auf der Basis von Citrix Gateway-Sitzungsrichtlinien verwenden.

Gateway-Passthrough-Authentifizierung aktivieren

Um die Gateway-Passthrough-Authentifizierung für den Storezugriff über die Workspace-App zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie im Fenster Authentifizierungsmethoden das Kontrollkästchen **Passthrough-Authentifizierung von Citrix Gateway**.

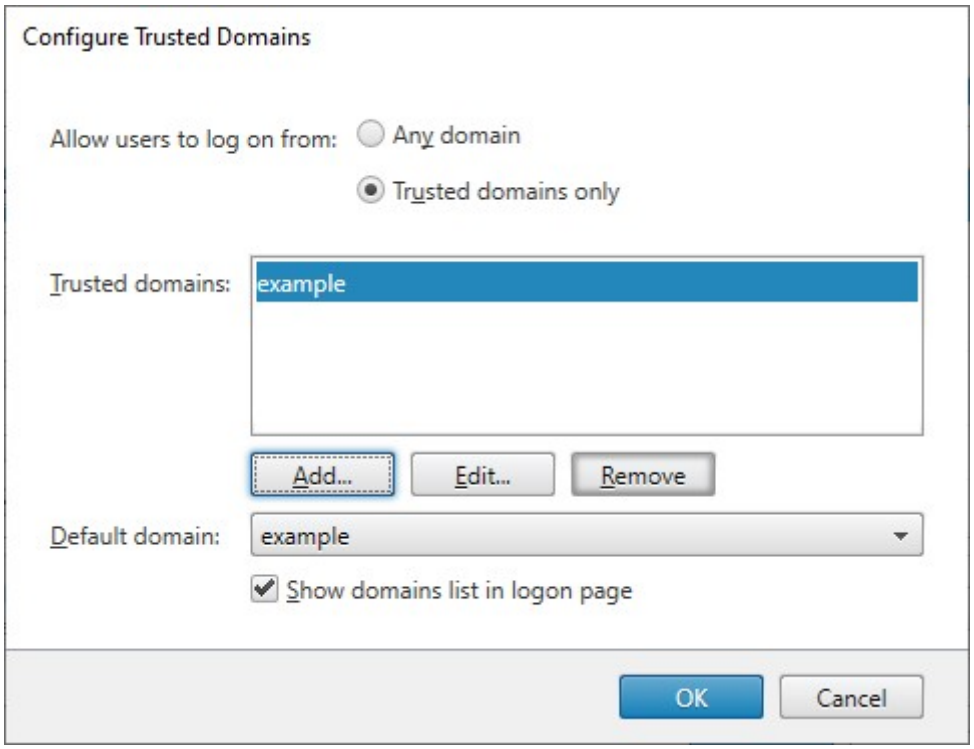
Wenn Sie die Citrix Gateway-Passthrough-Authentifizierung für einen Store standardmäßig aktivieren, wird sie auch für alle Websites für diesen Store aktiviert. Sie können die Authentifizierung mit Benutzernamen und Kennwort für einzelne Websites auf der Registerkarte Authentifizierungsmethoden separat aktivieren oder deaktivieren.

Konfigurieren vertrauenswürdiger Benutzerdomänen

Wenn Ihr Citrix Gateway für die Verwendung der LDAP-Authentifizierung konfiguriert ist, können Sie den Zugriff auf bestimmte Domänen einschränken.

1. Wählen Sie im Fenster "Authentifizierungsmethoden verwalten"im Dropdownmenü **Passthrough von Citrix Gateway** > **Einstellungen** die Option **Vertrauenswürdige Domänen konfigurieren** aus.
2. Wählen Sie **Nur vertrauenswürdige Domänen** aus und klicken Sie auf **Hinzufügen**, um den Namen einer vertrauenswürdigen Domäne einzugeben. Benutzer mit Konten in der Domäne können sich an allen Stores anmelden, die diesen Authentifizierungsdienst verwenden. Zum Ändern eines Domänennamens wählen Sie den Eintrag in der Liste "Vertrauenswürdige Domänen"aus und klicken Sie auf **Bearbeiten**. Um den Zugriff auf Stores für Benutzerkonten in der Domäne zu entfernen, wählen Sie eine Domäne in der Liste aus und klicken Sie auf **Entfernen**.

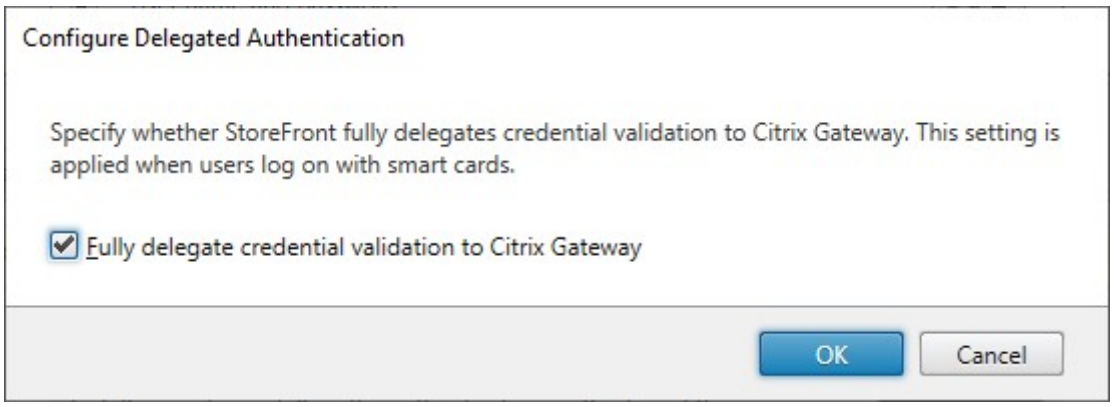
   Die Art, in der Sie den Domänennamen angeben, bestimmt das Format, in dem Benutzer ihre Anmeldeinformationen eingeben müssen. Wenn Benutzer ihre Anmeldeinformationen im Format des Domänenbenutzernamens eingeben sollen, fügen Sie der Liste den NetBIOS-Namen hinzu. Sollen die Benutzer ihre Anmeldeinformationen im Format des Benutzerprinzipalnamens eingeben, fügen Sie der Liste den vollqualifizierten Domänennamen hinzu. Wenn Benutzern ermöglicht werden soll, ihre Anmeldeinformationen sowohl im Format des Domänenbenutzernamens als auch im Format des Benutzerprinzipalnamens einzugeben, müssen Sie der Liste den NetBIOS-Namen und den vollqualifizierten Domänennamen hinzufügen.
3. Wenn Sie mehrere vertrauenswürdige Domänen konfigurieren, wählen Sie in der Liste Standarddomäne die Domäne aus, die standardmäßig ausgewählt wird, wenn Benutzer sich anmelden.
4. Sollen die vertrauenswürdigen Domänen auf der Anmeldeseite aufgelistet werden, klicken Sie auf das Kontrollkästchen "Domänenliste auf Anmeldeseite anzeigen".



Delegieren der Anmeldeinformationsvalidierung an Citrix Gateway

Standardmäßig überprüft StoreFront den vom Gateway empfangenen Benutzernamen und das Kennwort. Wenn das Citrix Gateway für kennwortlose Authentifizierungsmethoden wie Smartcard konfiguriert ist, müssen Sie StoreFront so konfigurieren, dass es die Anmeldeinformationen nicht prüft und von der Authentifizierung durch das Gateway abhängig ist. In diesem Fall wird empfohlen, bei der Konfiguration des Gateways eine Rückruf-URL einzugeben, damit StoreFront die Herkunft der Anforderung überprüfen kann (siehe Citrix Gateways verwalten).

1. Wählen Sie im Fenster **Authentifizierungsmethoden verwalten** im Dropdownmenü **Passthrough-Authentifizierung von Citrix Gateway** > **Einstellungen** die Option **Delegierte Authentifizierung konfigurieren**.
2. Aktivieren Sie **Anmeldeinformationenvalidierung vollständig an Citrix Gateway delegieren**.



PowerShell SDK

Um den Store so zu konfigurieren, dass er die Authentifizierung mithilfe des PowerShell SDK an das Gateway delegiert, verwenden Sie das Cmdlet Set-STFCitrixAGBasicOptions, um `CredentialValidationMode` auf `Auto` festzulegen. Um StoreFront für die Überprüfung der Anmeldeinformationen zu konfigurieren, setzen Sie `CredentialValidationMode` auf `Password`.

Zulassen, dass Benutzer abgelaufene Kennwörter ändern

Wenn Ihr Citrix Gateway für die Verwendung der LDAP-Authentifizierung (Benutzername und Kennwort) konfiguriert ist, können Sie NetScaler so konfigurieren, dass abgelaufene Kennwörter bei der Anmeldung geändert werden können.

1. Melden Sie sich auf der Website für die NetScaler-Verwaltung an
2. Gehen Sie im Seitenmenü **Authentication** > **Dashboard**.
3. Klicken Sie auf den Authentifizierungsserver.
4. Aktivieren Sie unter **Other Settings** die Option **Allow Password Change**.

Zulassen, dass Benutzer abgelaufene Kennwörter ändern

Bei aktivierter **Passthrough-Authentifizierung von Citrix Gateway** ist das Citrix Gateway für die Authentifizierung verantwortlich. Sie können StoreFront so konfigurieren, dass die Benutzer ihr Kennwort nach der Anmeldung ändern können. Dies ist nur möglich, wenn der Zugriff auf StoreFront-Stores über einen Browser erfolgt, nicht aber über lokal installierte Workspace-Apps.

Die StoreFront-Standardkonfiguration verhindert, dass die Benutzer ihre Kennwörter ändern, selbst wenn die Kennwörter abgelaufen sind. Wenn Sie diese Funktion aktivieren, vergewissern Sie sich, dass die Richtlinien für die Domänen mit Ihren Servern nicht die Benutzer davon abhalten, ihre Kennwörter zu ändern. Wenn Benutzer Kennwörter ändern können, werden vertrauliche Sicherheitsfunktionen für alle Personen offengelegt, die auf einen der Stores, die diesen Authentifizierungsdienst verwenden, zugreifen können. Wenn Ihr Unternehmen eine Sicherheitsrichtlinie hat, die Funktionen zur Änderung des Kennworts nur zur internen Verwendung reserviert, stellen Sie sicher, dass auf keinen der Stores von außerhalb des Unternehmensnetzwerks zugegriffen werden kann.

1. Wählen Sie im Fenster **Authentifizierungsmethoden verwalten** im Dropdownmenü **Passthrough-Authentifizierung von Citrix Gateway** > **Einstellungen** die Option **Kennwortoptionen verwalten**.
2. Damit die Benutzer ihre Kennwörter ändern können, aktivieren Sie das Kontrollkästchen **Benutzer dürfen Kennwort ändern**.

> **Hinweis:**
>
> Wenn Sie **Benutzer dürfen Kennwort ändern** aktivieren oder deaktivieren, wirkt sich dies auch auf die Einstellungen unter **Kennwortoptionen verwalten** für die Authentifizierung mit Benutzername und Kennwort aus.

PowerShell SDK

Verwenden Sie das Cmdlet Set-STFExplicitCommonOptions, um die Optionen zum Ändern von Kennwörtern über das PowerShell-SDK zu ändern.

Delivery Controller so konfigurieren, dass er StoreFront vertraut

Wenn das Gateway mit LDAP-Authentifizierung konfiguriert ist, leitet es die Anmeldeinformationen an StoreFront weiter. Bei anderen Authentifizierungsmethoden hat StoreFront keinen Zugriff auf die Anmeldeinformationen und kann sich daher nicht bei Citrix Virtual Apps and Desktops authentifizieren. Sie müssen den Delivery Controller daher so konfigurieren, dass er Anfragen von StoreFront vertraut. Weitere Informationen finden Sie unter Überlegungen und Best Practices zur Sicherheit von Citrix Virtual Apps and Desktops.

Single Sign-On zu VDAs mit dem Verbundauthentifizierungsdienst

Wenn das Gateway mit LDAP-Authentifizierung konfiguriert ist, leitet es die Anmeldeinformationen an StoreFront weiter, sodass ein Single Sign-On bei VDAs erfolgen kann. Bei anderen Authentifizierungsmethoden hat StoreFront keinen Zugriff auf die Anmeldeinformationen, sodass Single Sign-On nicht standardmäßig verfügbar ist. Sie können den Verbundauthentifizierungsdienst verwenden, um Single Sign-On bereitzustellen.

SAML-Authentifizierung

April 17, 2024

SAML (Security Assertion Markup Language) ist ein offener Standard, der von Identitäts- und Authentifizierungsprodukten verwendet wird. Über SAML können Sie StoreFront so konfigurieren, dass Benutzer zur Authentifizierung an einen externen Identitätsanbieter umgeleitet werden.

> **Hinweis:**
>
> Konfigurieren Sie StoreFront mit der SAML-Authentifizierung für den internen Zugriff. Für externen Zugriff konfigurieren Sie Citrix Gateway mit der SAML-Authentifizierung und dann StoreFront mit der Gateway-Passthrough-Authentifizierung.

StoreFront erfordert einen SAML 2.0-kompatiblen Identitätsanbieter (IdP). Dazu gehören:

- Microsoft AD Verbunddienste unter Nutzung von SAML-Bindungen (keine WS-Verbundbindungen) Weitere Informationen finden Sie unter AD FS Deployment und AD FS Operations.
- Citrix Gateway (als IdP konfiguriert)
- Microsoft Entra ID Weitere Informationen finden Sie unter CTX237490.

Die SAML-Assertion muss das Attribut `saml:Subject` enthalten, das den UPN des Benutzers enthält.

Um die SAML-Authentifizierung für einen Store zu aktivieren oder zu deaktivieren, wenn Sie eine Verbindung über die Workspace-App herstellen, aktivieren Sie im Fenster Authentifizierungsmethoden die Option **SAML-Authentifizierung**. Wenn Sie die SAML-Authentifizierung für einen Store standardmäßig aktivieren, wird sie auch für alle Websites für diesen Store aktiviert. Sie können SAML auf der Registerkarte Authentifizierungsmethoden für einzelne Websites separat konfigurieren.

SAML-Endpunkte für StoreFront

Für die Konfiguration von SAML benötigt Ihr Identitätsanbieter möglicherweise die folgenden Endpunkte:

- URL der Entitäts-ID. Das ist der Pfad zum Authentifizierungsdienst des Stores, normalerweise https://[storefront host]/Citrix/[StoreName]Auth
- URL des Assertion Consumer Service, normalerweise https://[storefront host]/Citrix/[StoreName]Auth/Saml
- Metadatendienst, normalerweise https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/ServiceProv

Zusätzlich gibt es einen Testendpunkt, normalerweise https://[storefront host]/Citrix/[StoreName]Auth/SamlTest

Sie können das folgende PowerShell-Skript verwenden, um die Endpunkte für einen Store aufzulisten.

```
# Change this value for your Store
$storeVirtualPath = "/Citrix/Store"

$auth = Get-STFAuthenticationService -Store (Get-STFStoreService -
    VirtualPath $storeVirtualPath)
$spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.
    ServiceProvider.Uri.AbsoluteUri
$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/AssertionConsumerService")
$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/ServiceProvider/Metadata")
$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlTest")
Write-Host "SAML Service Provider information:
Entity ID: $spId
Assertion Consumer Service: $acs
Metadata: $md
Test Page: $samlTest
<!--NeedCopy-->
```

Beispiel für die Ausgabe:

```
SAML Service Provider information:
Entity ID: https://storefront.example.com/Citrix/StoreAuth
Assertion Consumer Service: https://storefront.example.com/Citrix/
    StoreAuth/SamlForms/AssertionConsumerService
Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/
    ServiceProvider/Metadata
```



```
Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest
<!--NeedCopy-->
```

Konfiguration per Metadatenaustausch

Zur Vereinfachung der Konfiguration können Sie Metadaten (IDs, Zertifikate, Endpunkte und andere Konfigurationselemente) zwischen Identitäts- und Dienstanbieter, in diesem Fall StoreFront, austauschen.

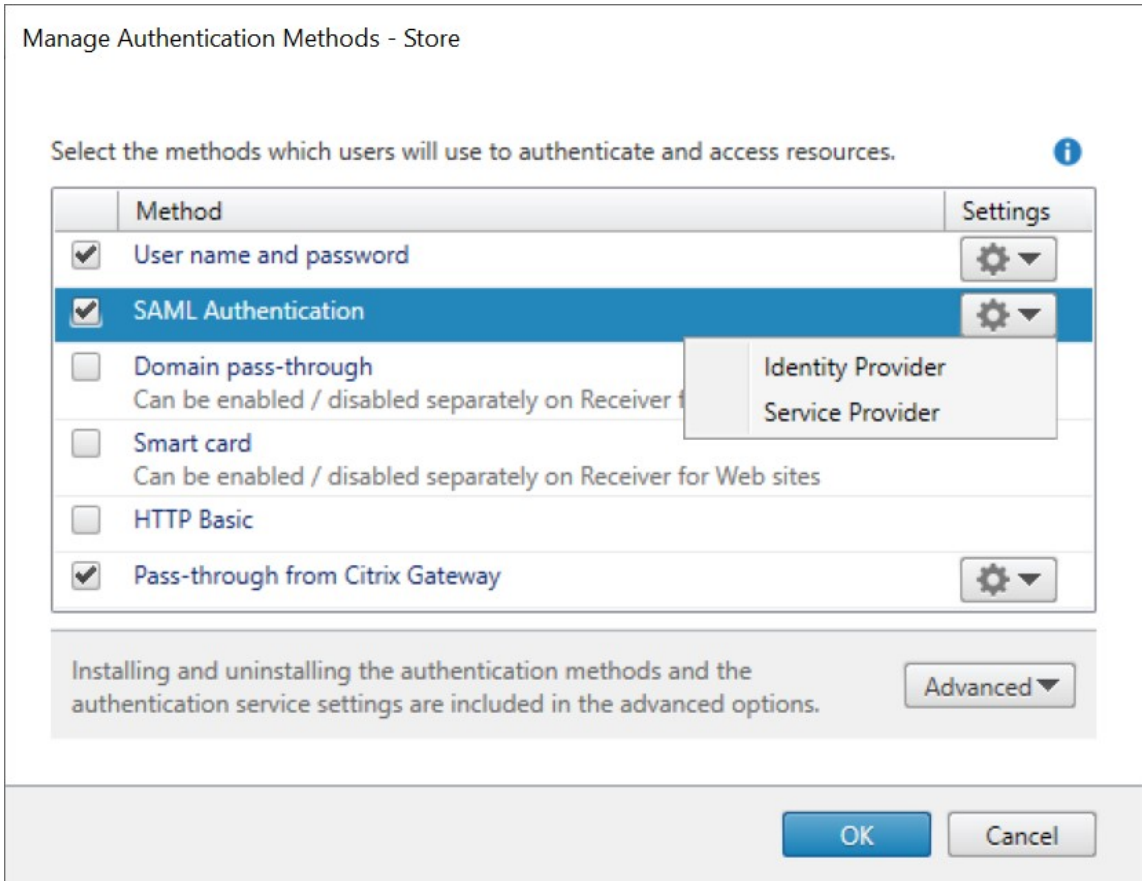
Wenn Ihr Identitätsanbieter den Metadatenimport unterstützt, können Sie ihn an den StoreFront-Metadaten-Endpunkt verweisen. **Hinweis:** Dies muss über HTTPS erfolgen.

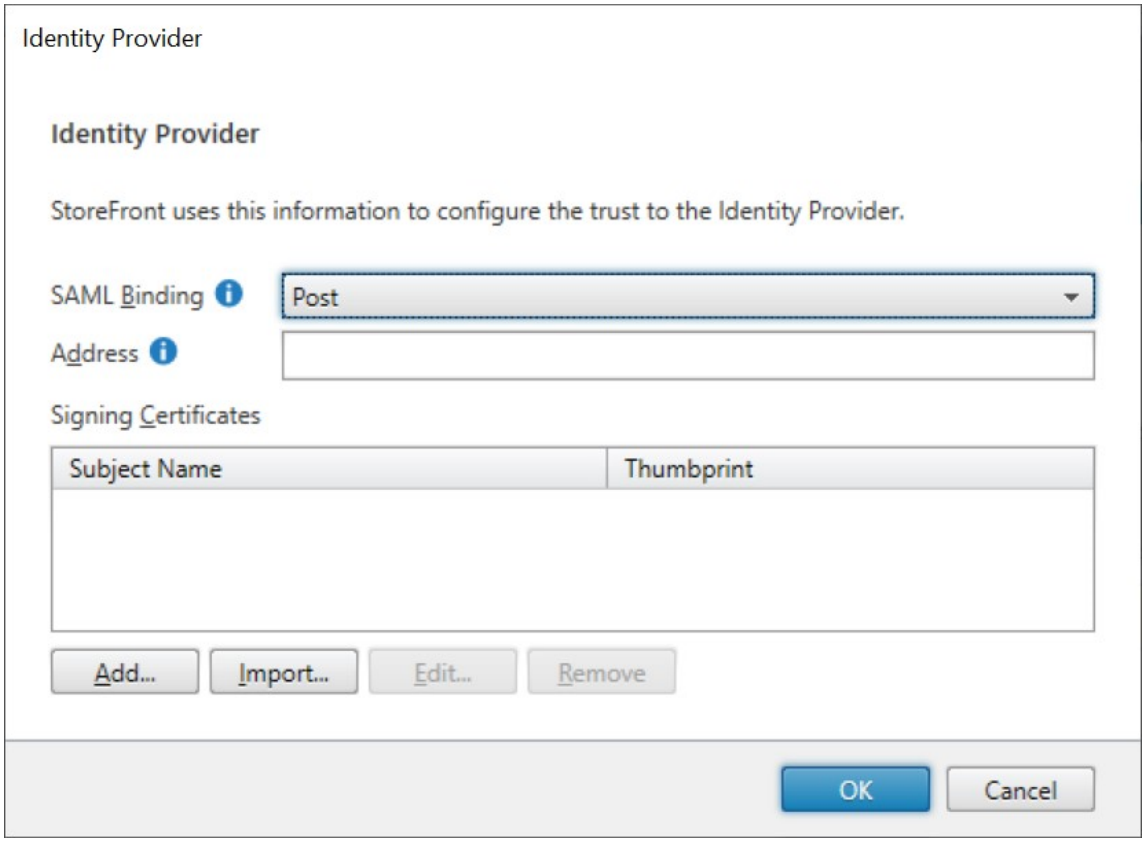
Um StoreFront mithilfe der Metadaten eines Identitätsanbieters zu konfigurieren, verwenden Sie das Cmdlet Update-STFSamlIdPFromMetadata. Beispiel:

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module

# Remember to change this with the virtual path of your Store.
$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store

# To read the metadata directly from the Identity Provider, use the following:
# Note again this is only allowed for https endpoints
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://example.com/FederationMetadata/2007-06/FederationMetadata.xml

# If the metadata has already been download, use the following:
# Note: Ensure that the file is encoded as UTF-8
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata.xml"
<!--NeedCopy-->
```

Identitätsanbieter konfigurieren

1. Klicken Sie in der Zeile **SAML-Authentifizierung** auf das Dropdownmenü “Einstellungen”und dann auf **Identitätsanbieter**.

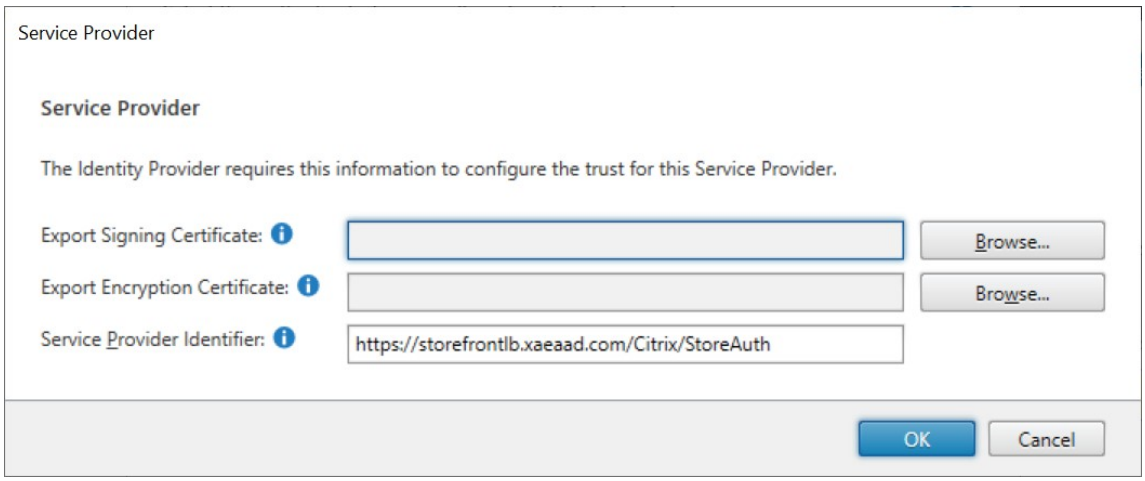




2. Wählen Sie für **SAML-Bindung** die Option **Posten** oder **Umleiten**.
3. Geben Sie die **Adresse** des Identitätsanbieters ein.
4. Importieren Sie das zum Signieren der SAML-Token verwendete Zertifikat.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Dienstanbieter konfigurieren

1. Klicken Sie in der Zeile **SAML-Authentifizierung** auf das Dropdownmenü “Einstellungen”und dann auf **Dienstanbieter**.



2. Wählen Sie optional ein Zertifikat unter **Signaturzertifikat exportieren**, das zum Signieren von Meldungen an den Identitätsanbieter verwendet wird.
3. Wählen Sie optional ein Zertifikat unter **Verschlüsselungszertifikat exportieren**, das zum Entschlüsseln von Meldungen vom Identitätsanbieter verwendet wird.
4. Für die **Dienstanbieter-ID** wird automatisch der Authentifizierungsdienst für den Store eingetragen.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

PowerShell SDK

Verwenden des PowerShell-SDKs:

- Um ein Signaturzertifikat zu importieren, rufen Sie das Cmdlet Import-STFSamlSigningCertificate auf.
- Um ein Verschlüsselungszertifikat zu importieren, rufen Sie das Cmdlet Import-STFSamlEncryptionCertificat auf.

Testen

SAML-Integration testen:

1. Gehen Sie zur SAML-Testseite (siehe SAML-Endpunkte für StoreFront).
2. Dadurch werden Sie zum Identitätsanbieter weitergeleitet. Geben Sie Ihre Anmeldeinformationen ein.
3. Sie werden zurück zur Testseite zurückgeleitet, auf der die Identitätsansprüche und Assertions angezeigt werden.

Delivery Controller so konfigurieren, dass er StoreFront vertraut

Bei Verwendung der SAML-Authentifizierung hat StoreFront keinen Zugriff auf die Anmeldeinformationen des Benutzers und kann sich daher nicht bei Citrix Virtual Apps and Desktops authentifizieren. Sie müssen den Delivery Controller daher so konfigurieren, dass er Anfragen von StoreFront vertraut. Weitere Informationen finden Sie unter Überlegungen und Best Practices zur Sicherheit von Citrix Virtual Apps and Desktops.

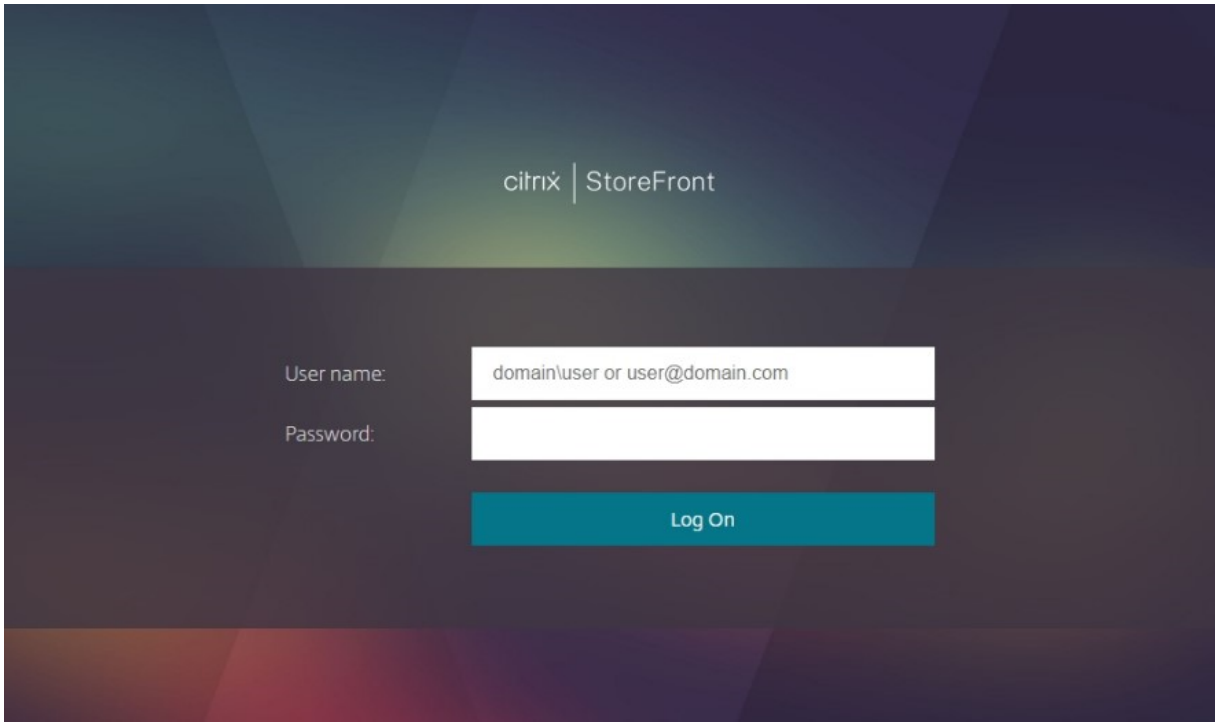
Single Sign-On zu VDAs mit dem Verbundauthentifizierungsdienst

Bei Verwendung der SAML-Authentifizierung hat StoreFront keinen Zugriff auf die Anmeldeinformationen des Benutzers, sodass Single Sign-On bei VDAs nicht standardmäßig verfügbar ist. Sie können den Verbundauthentifizierungsdienst verwenden, um Single Sign-On bereitzustellen.

Authentifizierung mit Benutzernamen und Kennwort

April 17, 2024

Bei der Authentifizierung mit Benutzernamen und Kennwort geben die Benutzer ihre Active Directory-Anmeldeinformationen ein.



Um die Authentifizierung mit Benutzernamen und Kennwort für einen Store beim Zugriff über die Workspace-App zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie im Fenster Authentifizierungsmethoden das Häkchen bei **Benutzername und Kennwort**.

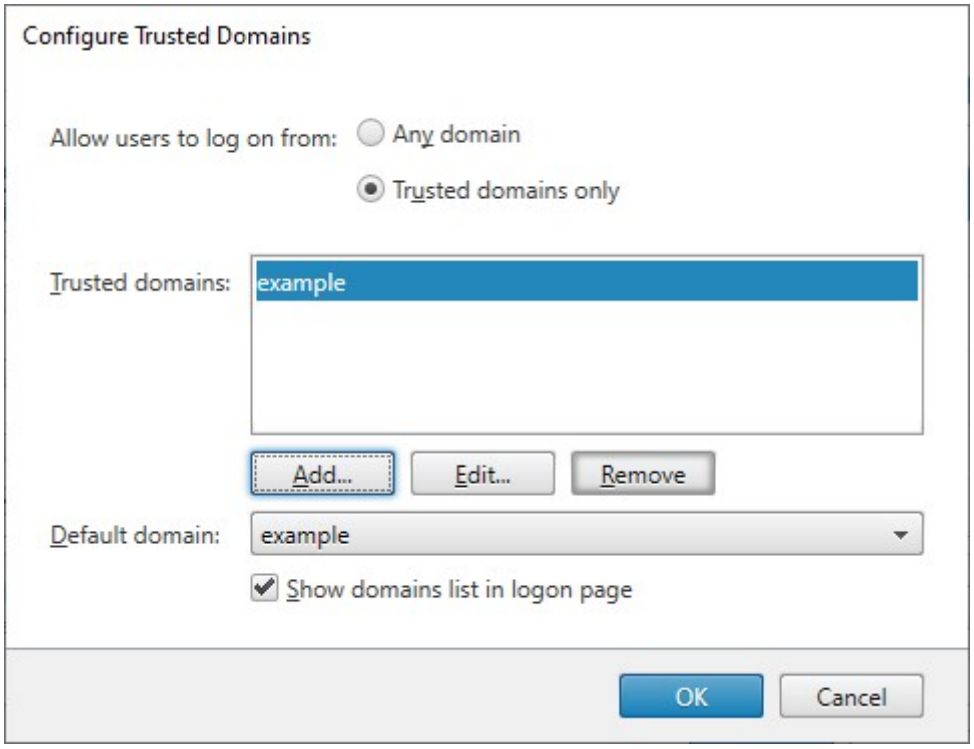
Wenn Sie standardmäßig die Authentifizierung mit Benutzernamen und Kennwort für einen Store aktivieren, wird sie auch für alle Websites dieses Stores aktiviert. Sie können die Authentifizierung mit Benutzernamen und Kennwort für einzelne Websites auf der Registerkarte Receiver für Web-Sites verwalten > Authentifizierungsmethoden separat aktivieren oder deaktivieren.

Konfigurieren vertrauenswürdiger Benutzerdomänen

Sie können den Zugriff auf Stores auf Benutzer beschränken, die sich mit Anmeldeinformationen von bestimmten vertrauenswürdigen Domänen anmelden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten "Stores"und im Ergebnisbereich die gewünschte Authentifizierungsmethode aus. Klicken Sie im Aktionsbereich auf **Authentifizierungsmethoden verwalten**.
2. Wählen Sie im Dropdownmenü **Benutzername und Kennwort > Einstellungen** die Option **Vertrauenswürdige Domänen konfigurieren** aus.
3. Wählen Sie **Nur vertrauenswürdige Domänen** aus und klicken Sie auf **Hinzufügen**, um den Namen einer vertrauenswürdigen Domäne einzugeben. Benutzer mit Konten in der Domäne können sich an allen Stores anmelden, die diesen Authentifizierungsdienst verwenden. Zum Ändern eines Domänennamens wählen Sie den Eintrag in der Liste "Vertrauenswürdige Domänen"aus und klicken Sie auf **Bearbeiten**. Um den Zugriff auf Stores für Benutzerkonten in der Domäne zu entfernen, wählen Sie eine Domäne in der Liste aus und klicken Sie auf **Entfernen**.

   Die Art, in der Sie den Domänennamen angeben, bestimmt das Format, in dem Benutzer ihre Anmeldeinformationen eingeben müssen. Wenn Benutzer ihre Anmeldeinformationen im Format des Domänenbenutzernamens eingeben sollen, fügen Sie der Liste den NetBIOS-Namen hinzu. Sollen die Benutzer ihre Anmeldeinformationen im Format des Benutzerprinzipalnamens eingeben, fügen Sie der Liste den vollqualifizierten Domänennamen hinzu. Wenn Benutzern ermöglicht werden soll, ihre Anmeldeinformationen sowohl im Format des Domänenbenutzernamens als auch im Format des Benutzerprinzipalnamens einzugeben, müssen Sie der Liste den NetBIOS-Namen und den vollqualifizierten Domänennamen hinzufügen.
4. Wenn Sie mehrere vertrauenswürdige Domänen konfigurieren, wählen Sie in der Liste Standarddomäne die Domäne aus, die standardmäßig ausgewählt wird, wenn Benutzer sich anmelden.
5. Sollen die vertrauenswürdigen Domänen auf der Anmeldeseite aufgelistet werden, klicken Sie auf das Kontrollkästchen "Domänenliste auf Anmeldeseite anzeigen".



Kennwortänderung durch Benutzer zulassen

Sie können zulassen, dass die Benutzer ihre Kennwörter zu einer beliebigen Zeit ändern. Alternativ können Sie die Kennwortänderung auf Benutzer beschränken, deren Kennwort abgelaufen ist. So können Sie sicherstellen, dass Benutzern nie der Zugriff auf ihre Desktops und Anwendungen verweigert wird, weil ein Kennwort abgelaufen ist.

Die Funktion zum Ändern des Kennworts ist in den folgenden Clients verfügbar:

Citrix Workspace-App	Benutzer kann ein abgelaufenes Kennwort ändern, sofern in StoreFront aktiviert	Benutzer wird benachrichtigt, dass das Kennwort abläuft	Benutzer kann das Kennwort vor Ablaufen ändern, sofern in StoreFront aktiviert
Windows	Ja		
Mac	Ja		
Android			
iOS			
Linux	Ja		
Web	Ja	Ja	Ja

Citrix Workspace-App	Benutzer kann ein abgelaufenes Kennwort ändern, sofern in StoreFront aktiviert	Benutzer wird benachrichtigt, dass das Kennwort abläuft	Benutzer kann das Kennwort vor Ablaufen ändern, sofern in StoreFront aktiviert

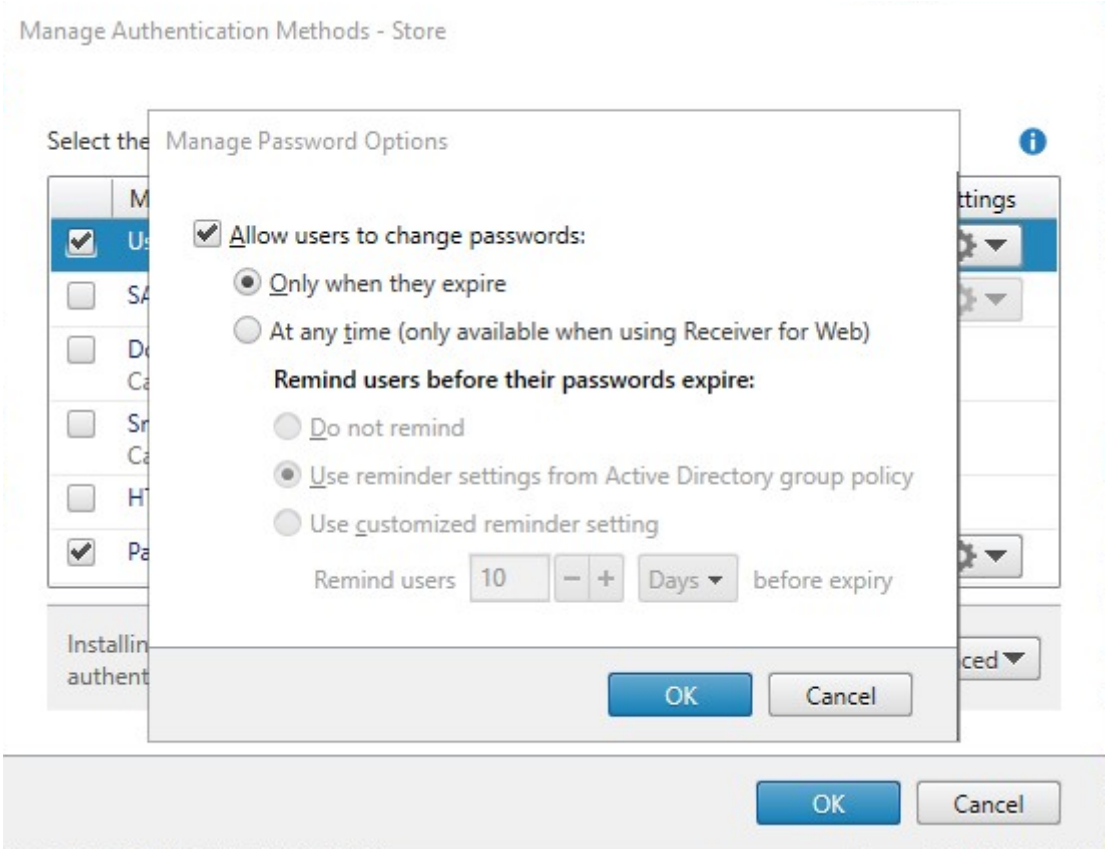
Die Standardkonfiguration verhindert, dass Benutzer der Citrix Workspace-App bzw. eines Webbrowsers ihre Kennwörter ändern, selbst wenn die Kennwörter abgelaufen sind. Wenn Sie diese Funktion aktivieren, vergewissern Sie sich, dass die Richtlinien für die Domänen mit Ihren Servern nicht die Benutzer davon abhalten, ihre Kennwörter zu ändern. Wenn Benutzer Kennwörter ändern können, werden vertrauliche Sicherheitsfunktionen für alle Personen offengelegt, die auf einen der Stores, die diesen Authentifizierungsdienst verwenden, zugreifen können. Wenn Ihr Unternehmen eine Sicherheitsrichtlinie hat, die Funktionen zur Änderung des Kennworts nur zur internen Verwendung reserviert, stellen Sie sicher, dass auf keinen der Stores von außerhalb des Unternehmensnetzwerks zugegriffen werden kann.

Wenn Sie zulassen, dass die Benutzer ihre Kennwörter jederzeit ändern können, wird lokalen Benutzern, deren Kennwörter bald ablaufen, beim Anmelden eine Warnung angezeigt. Standardmäßig hängt der Benachrichtigungszeitraum von der entsprechenden Windows-Richtlinieneinstellung ab. Alternativ können Sie einen eigenen Benachrichtigungszeitraum konfigurieren.

1. Wählen Sie im Fenster **Authentifizierungsmethoden verwalten** im Dropdownmenü **Benutzername und Kennwort** > **Einstellungen** die Option **Kennwortoptionen verwalten**.
2. Damit die Benutzer ihre Kennwörter ändern können, aktivieren Sie das Kontrollkästchen **Benutzer dürfen Kennwort ändern**.

   > **Hinweis:**
   > Wenn Sie diese Option nicht auswählen, müssen Sie Benutzern unterstützen, die keinen Zugriff auf ihre Desktops und Anwendungen haben, weil das Kennwort abgelaufen ist.

3. Wählen Sie aus, ob die Benutzer Kennwörter **Nur beim Ablaufen** oder **Jeder Zeit** ändern können sollen.
4. Wählen Sie aus, ob die Benutzer vor Ablauf des Kennworts erinnert werden sollen.



Hinweis 1:

StoreFront unterstützt keine differenzierte Kennwortrichtlinie in Active Directory.

Hinweis 2:

Stellen Sie sicher, dass auf den StoreFront-Servern ausreichend Speicherplatz zum Speichern aller Benutzerprofile vorhanden ist. Um zu prüfen, ob das Kennwort eines Benutzers bald abläuft, erstellt StoreFront ein lokales Profil für den Benutzer auf dem Server. StoreFront muss eine Verbindung mit dem Domänencontroller herstellen können, um die Kennwörter der Benutzer zu ändern.

Hinweis 3:

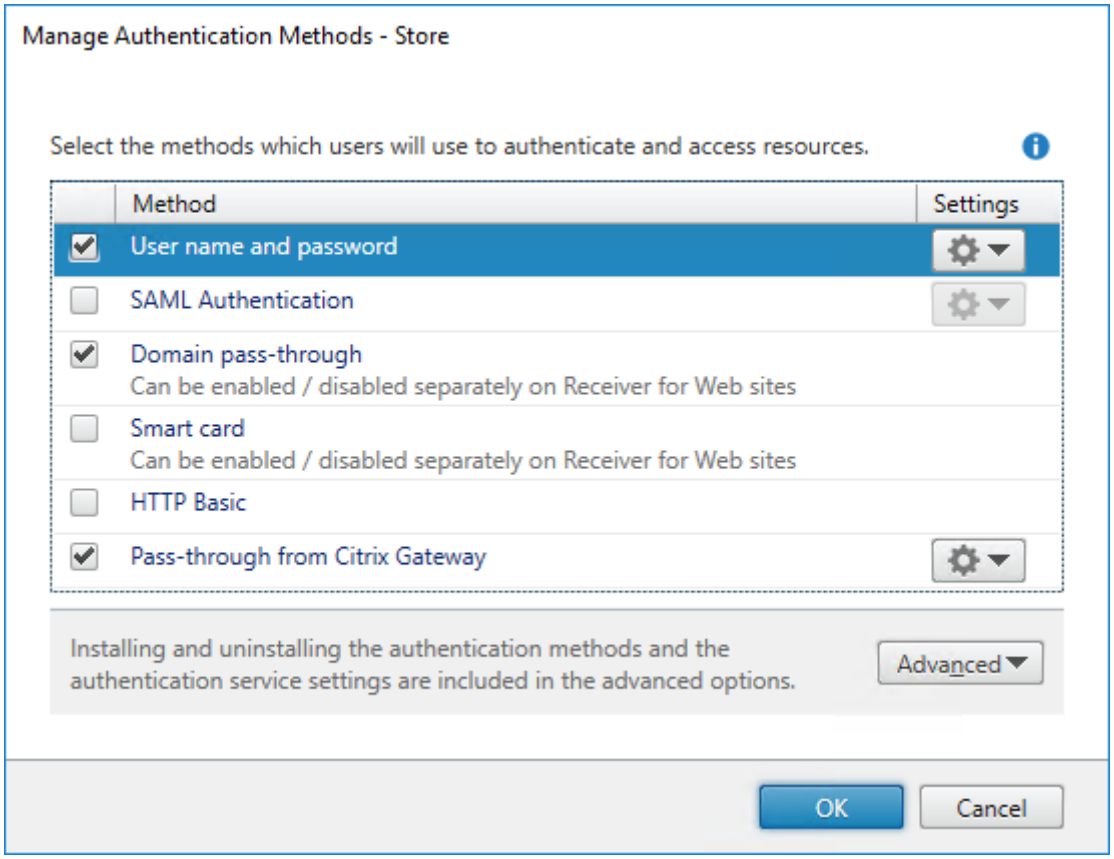
Wenn Sie das jederzeit mögliche Ändern von Kennwörtern aktivieren oder deaktivieren, wirkt sich dies auch auf die Einstellungen unter **Kennwortoptionen verwalten** für die Passthrough-Authentifizierung von Citrix Gateway aus.

Kennwort der Anmeldeinformationen überprüfen

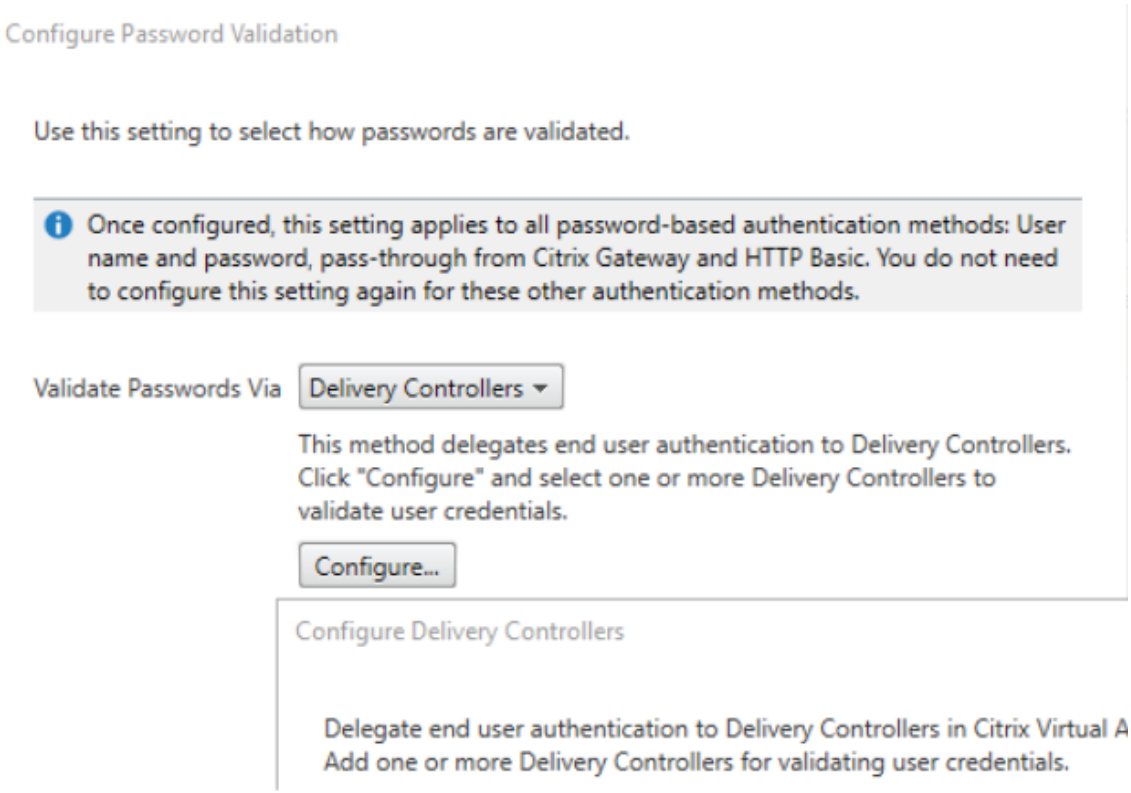
Normalerweise kommuniziert StoreFront direkt mit Active Directory, um Anmeldeinformationen zu überprüfen.

Wenn StoreFront nicht in der gleichen Domäne wie Citrix Virtual Apps and Desktops ist und keine Active Directory-Vertrauensstellungen eingerichtet werden können, können Sie StoreFront zur Verwendung der Delivery Controller von Citrix Virtual Apps and Desktops für die Authentifizierung der Anmeldeinformationen konfigurieren:

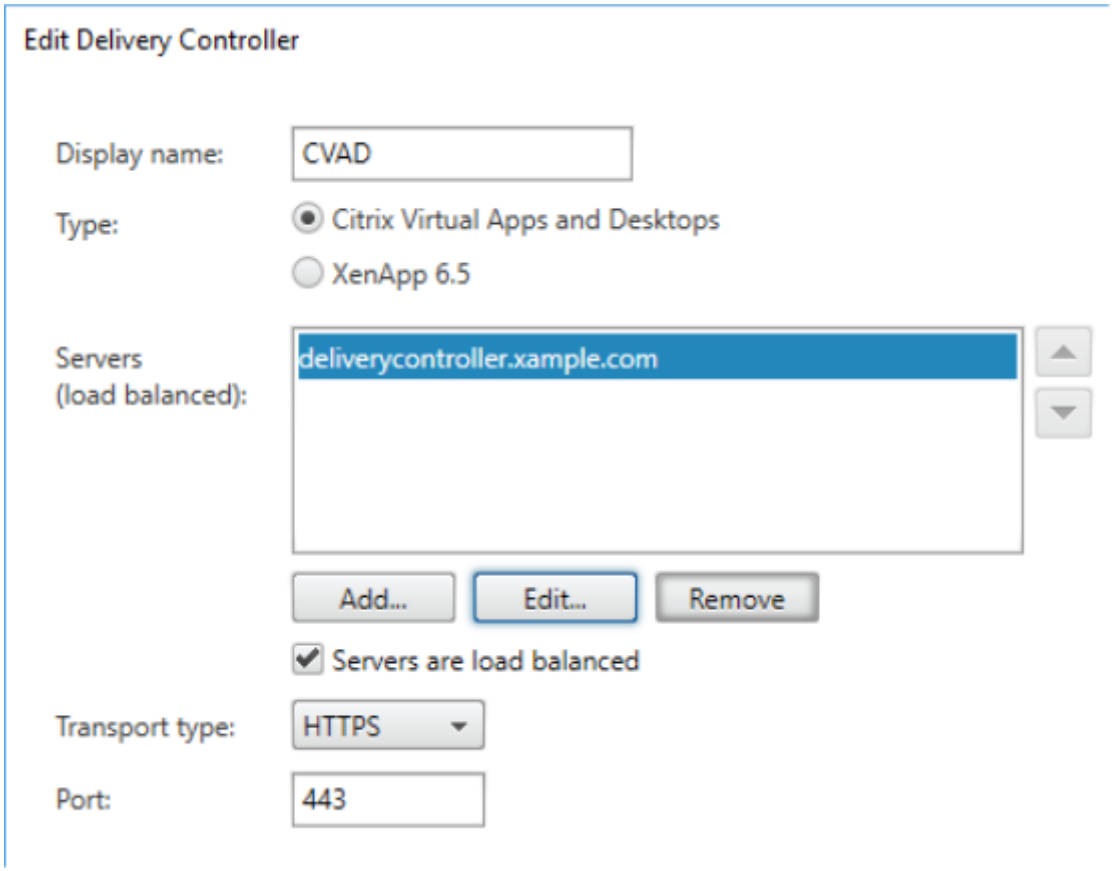
1. Wählen Sie im Fenster **Authentifizierungsmethoden verwalten** im Dropdownmenü **Benutzername und Kennwort > Einstellungen** die Option **Kennwortvalidierung konfigurieren**.



2. Wählen Sie in der Liste **Kennwörter validieren mit** die Option **Delivery Controller** und klicken Sie auf **Konfigurieren**.



3. Folgen Sie den Anweisungen auf den Seiten **Delivery Controller konfigurieren**, um mindestens einen **Delivery Controller** zum Validieren der Benutzeranmeldeinformationen hinzuzufügen und klicken Sie auf **OK**.



Active Directory verwenden

1. Wählen Sie auf der Seite **Authentifizierungsmethoden verwalten** in der Liste **Benutzername und Kennwort** > **Einstellungen** die Option **Kennwortvalidierung konfigurieren**.
2. Wählen Sie im Dropdownmenü **Kennwörter validieren mit** die Option **Active Directory** und klicken Sie auf **Konfigurieren**.

Single Sign-On auf VDAs

Wenn Benutzer eine Ressource starten, verwendet StoreFront die Anmeldeinformationen, mit denen sich der Benutzer am Store angemeldet hat, für Single Sign-On bei den VDAs.

Anmeldebildschirm anpassen

Der Anmeldebildschirm wird aus einer Vorlage generiert, die sich normalerweise unter C:\inetpub\wwwroot\Citrix\name]Auth\App_Data\Templates\UsernamePassword.tfrm befindet. Sie können den Bildschirm anpassen.

Titeltext

Wenn sich Benutzer der Citrix Workspace-App an einem Store anmelden, wird standardmäßig kein Titeltext im Anmeldedialogfeld angezeigt. Sie können den Text "Melden Sie sich an"oder eine eigene benutzerdefinierte Meldung anzeigen.

1. Verwenden Sie einen Texteditor, um die Datei UsernamePassword.tfrm für den Authentifizierungsdienst zu öffnen.
2. Suchen Sie die folgenden Zeilen in der Datei.

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
<!--NeedCopy-->
```

3. Heben Sie die Auskommentierung auf für die Anweisung auf, indem Sie an Anfang und Ende **@*** entfernen und am Ende ***@**.

```
@Heading("ExplicitAuth:AuthenticateHeadingText")
<!--NeedCopy-->
```

   Citrix Workspace-App-Benutzern wird der Titeltext "Melden Sie sich an"oder die entsprechende lokalisierte Version dieses Texts angezeigt, wenn sie sich an Stores anmelden, die diesen Authentifizierungsdienst verwenden.

4. Um den Titeltext zu ändern, öffnen Sie mit einem Texteditor die Datei *ExplicitFormsCommon.xx.resx* für den Authentifizierungsdienst (normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\resources\).
5. Suchen Sie die folgenden Elemente in der Datei. Bearbeiten Sie den vom <value>-Element umschlossenen Text, um den Titeltext zu ändern, der Benutzern im Citrix Workspace-App-Anmeldedialogfeld angezeigt wird, wenn sie auf Stores zugreifen, die diesen Authentifizierungsdienst verwenden.

```
<data name="AuthenticateHeadingText" xml:space="preserve">
    <value>My Company Name</value>
</data>
<!--NeedCopy-->
```

   Um den Titeltext des Anmeldedialogfelds für Benutzer mit einem anderen Gebietsschema zu ändern, bearbeiten Sie die lokalisierten Dateien *ExplicitAuth.languagecode.resx*, wobei **languagecode** die Gebietsschema-ID ist.

Zwischenspeicherung von Kennwörtern und Benutzernamen in Citrix Workspace-App für Windows deaktivieren

Standardmäßig speichert die Citrix Workspace-App für Windows die Kennwörter von Benutzern, wenn sie sich bei StoreFront-Stores anmelden. Um zu verhindern, dass die Citrix Workspace-App für Win-

dows Benutzerkennwörter zwischenspeichert, bearbeiten Sie die Dateien für den Authentifizierungsdienst.

1. Verwenden Sie einen Texteditor, um die Datei inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\Templat zu öffnen.
2. Suchen Sie die folgende Zeile in der Datei.

```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
<!--NeedCopy-->
```

3. Kommentieren Sie die Anweisung wie unten gezeigt.

```
<!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",
    initiallyChecked: ControlValue("SaveCredentials")) -->
<!--NeedCopy-->
```

   Die Benutzer müssen ihre Kennwörter jedes Mal eingeben, wenn sie sich bei einem Store mit diesem Authentifizierungsdienst anmelden.

   Standardmäßig verwendet Citrix Workspace für Windows automatisch den zuletzt eingegebenen Benutzernamen. Informationen zum Unterdrücken des Ausfüllens des Benutzernamenfelds bzw. zu einer alternativen Methode zum Unterdrücken der Kennwortzwischenspeicherung finden Sie unter Zwischenspeicherung von Kennwörtern und Benutzernamen in Citrix Workspace-App für Windows deaktivieren.

Remotezugriff über Citrix Gateway

Sie können Ihr Citrix Gateway so konfigurieren, dass sich Benutzer mit ihrem Domänenbenutzernamen und Kennwort am Gateway anmelden. Diese Anmeldeinformationen werden an StoreFront weitergeleitet, um sich beim Store anzumelden. Informationen zur Konfiguration Ihres Citrix-Gateways für die Authentifizierung mit LDAP-Benutzernamen und -Kennwort finden Sie in der NetScaler-Dokumentation – LDAP-Authentifizierung. Informationen zur Konfiguration von StoreFront finden Sie unter Passthrough von Citrix Gateway.

Konfiguration des Verbundauthentifizierungsdiensts

April 17, 2024

Bei Verwendung von Authentifizierungsmethoden wie SAML, bei denen der Benutzer seine Anmeldeinformationen nicht direkt in die Citrix Workspace-App eingibt, ist Single Sign-On bei VDAs standardmäßig nicht möglich. In diesen Fällen können Sie den Verbundauthentifizierungsdienst (FAS) verwenden, um Single Sign-On für VDAs per Zertifikatauthentifizierung bereitzustellen.

Um den FAS für StoreFront zu verwenden, müssen Sie StoreFront mit dem PowerShell-SDK konfigurieren. Verwenden Sie Set-STFClaimsFactoryNames, um die Claims Factory auf `FASClaimsFactory` festzulegen, und Set-STFStoreLaunchOptions, um den VDA-Anmeldedatenanbieter auf `FASLogonDataProvide` festzulegen.

Um beispielsweise FAS für einen Store zu aktivieren:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "FASClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
    FASLogonDataProvider"
<!--NeedCopy-->
```

Gehen Sie zum Deaktivieren des FAS für einen Store folgendermaßen vor:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "standardClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
<!--NeedCopy-->
```

Ersetzen Sie `[VirtualPath]` durch den entsprechenden virtuellen Pfad, z. B. `/Citrix/Store`.

Um die Liste der FAS-Server und andere Einstellungen zu konfigurieren, müssen Sie eine Gruppenrichtlinie verwenden. Weitere Informationen finden Sie in der FAS-Dokumentation.

FAS wird nicht verwendet, wenn Sie sich mithilfe von Domänen-Passthrough oder Smartcard über einen Browser authentifizieren.

Stores konfigurieren und verwalten

February 28, 2024

Citrix StoreFront ermöglicht das Erstellen und Verwalten von Stores für Anwendungen und Desktops aus Citrix Virtual Apps and Desktops, in denen sich die Benutzer nach Bedarf selbst bedienen können.

Aufgabe	Detail
Store erstellen	Sie können beliebig viele zusätzliche Stores konfigurieren.
Store konfigurieren	Store-Einstellungen konfigurieren
Store entfernen	Entfernen Sie einen nicht benötigten Store.
Store-Provisioningdateien für Benutzer exportieren	Generieren Sie Dateien mit Verbindungsinformationen für Stores, einschließlich Citrix Gateway-Bereitstellungen und Beacons, die für Stores konfiguriert wurden.
Stores für Benutzer ankündigen und ausblenden	Verhindern Sie, dass Stores den Benutzern zum Hinzufügen zu ihrem Konto angezeigt werden, wenn diese die Citrix Workspace-App über die e-mail-basierte Kontenermittlung oder den vollqualifizierten Domänennamen (FQDN) konfigurieren.
Kerberos-Delegierung konfigurieren	Geben Sie vor, ob StoreFront die Kerberos-Delegierung zur Authentifizierung bei Delivery Controllern verwenden soll.
Durch Stores zur Verfügung gestellte Ressourcen verwalten	Fügen Sie Ressourcen in Stores hinzu oder entfernen Sie Ressourcen daraus.
Remotezugriff auf Stores über Citrix Gateway verwalten	Konfigurieren Sie den Zugriff auf Stores über Citrix Gateway für Benutzer in öffentlichen Netzwerken.
Zertifikatsperrlisten überprüfen	Konfigurieren Sie StoreFront so, dass der Status der von Citrix Virtual Apps and Desktops-Delivery Controllern verwendeten TLS-Zertifikate anhand einer veröffentlichten Zertifikatssperrliste überprüft wird.
Zwei StoreFront-Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers konfigurieren	Konfigurieren Sie zwei StoreFront-Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers.
Favoriten aktivieren oder deaktivieren	Aktivieren oder deaktivieren Sie Favoriten für den Store.
Abonnementdaten für einen Store verwalten	Abonnementdaten (Favoriten) anzeigen, importieren, exportieren und löschen.

Aufgabe	Detail
Zwei StoreFront-Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers konfigurieren	Konfigurieren Sie zwei Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers.
Favoritendaten mit Microsoft SQL Server speichern	Verwenden Sie eine externe SQL Server-Datenbank zum Speichern von Abonnementdaten (Favoriten).
Citrix Virtual Apps and Desktops konfigurieren	Anzeige von Ressourcen auf Storewebsites in Citrix Virtual Apps and Desktops konfigurieren
Erweiterte Storeeinstellungen	Konfigurieren erweiterter Storeeinstellungen
Optimales HDX-Routing	Konfigurieren Sie, welches Gateway zur Verbindung mit einzelnen Ressourcen verwendet wird.
Standard-ICA-Einstellungen	Konfigurieren Sie HDX-Einstellungen, indem Sie sie zu default.ica hinzufügen.
ICA-Dateisignierung	ICA-Dateisignierung konfigurieren
Windows-Verknüpfungen	Konfigurieren Sie, wie die Citrix Workspace-App für Windows Startmenü- und Desktopverknüpfungen für bevorzugte und obligatorische Apps erstellt.

Store erstellen

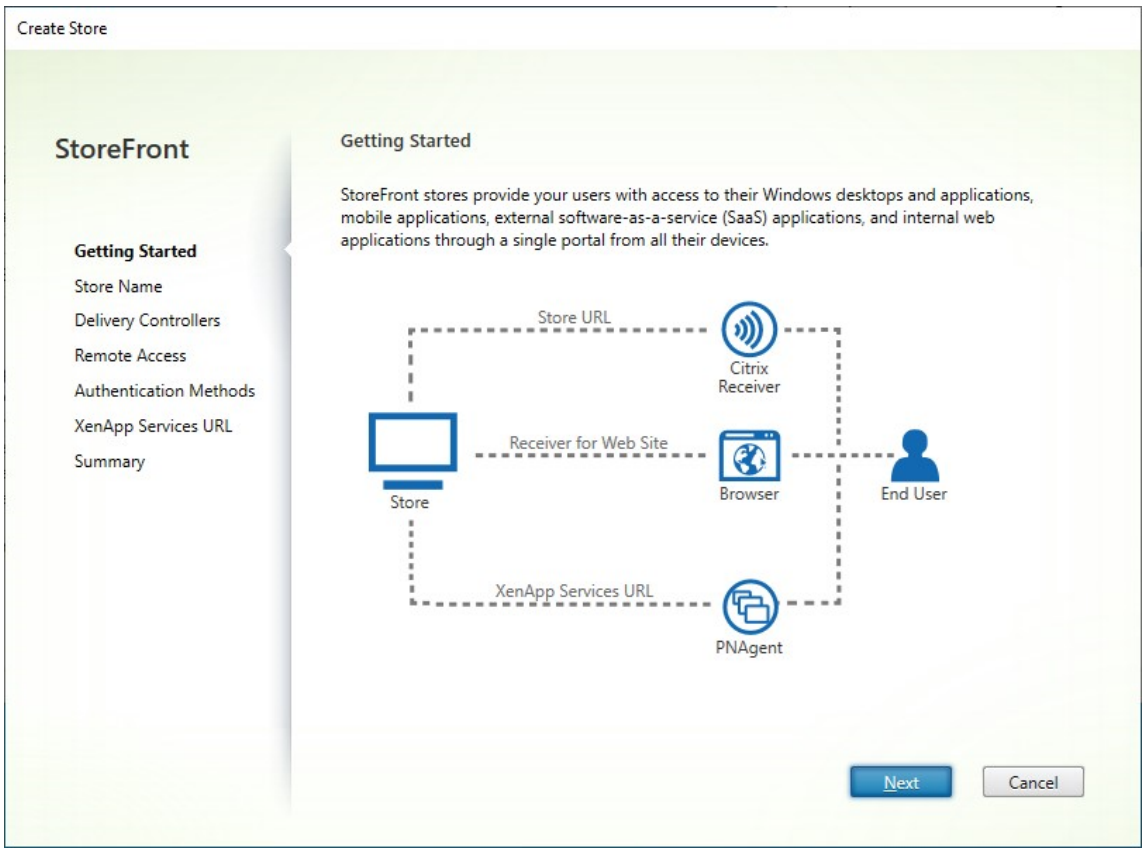
April 17, 2024

Sie können beliebig viele Stores erstellen. Beispielsweise kann es empfehlenswert sein, einen Store für eine bestimmte Benutzergruppe zu erstellen oder bestimmte Ressourcen zusammenzufassen.

> Wichtig:
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss
> übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Zum Erstellen eines Stores identifizieren und konfigurieren Sie die Kommunikation mit den Servern, auf denen die Ressourcen, die Sie im Store zur Verfügung stellen möchten, bereitgestellt werden. Anschließend konfigurieren Sie optional Remotezugriff auf den Store über Citrix Gateway.

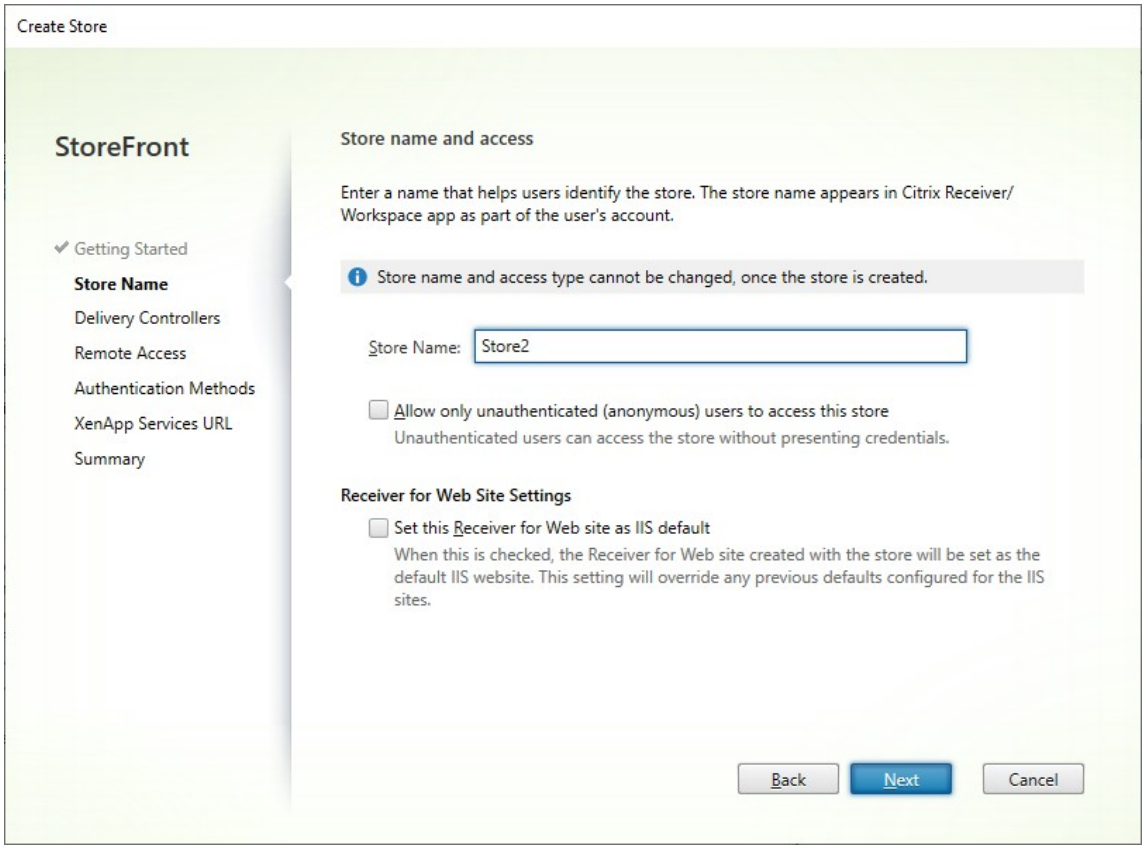
1. Klicken Sie im Aktionsbereich auf **Store erstellen**.



   Klicken Sie auf **Weiter**.

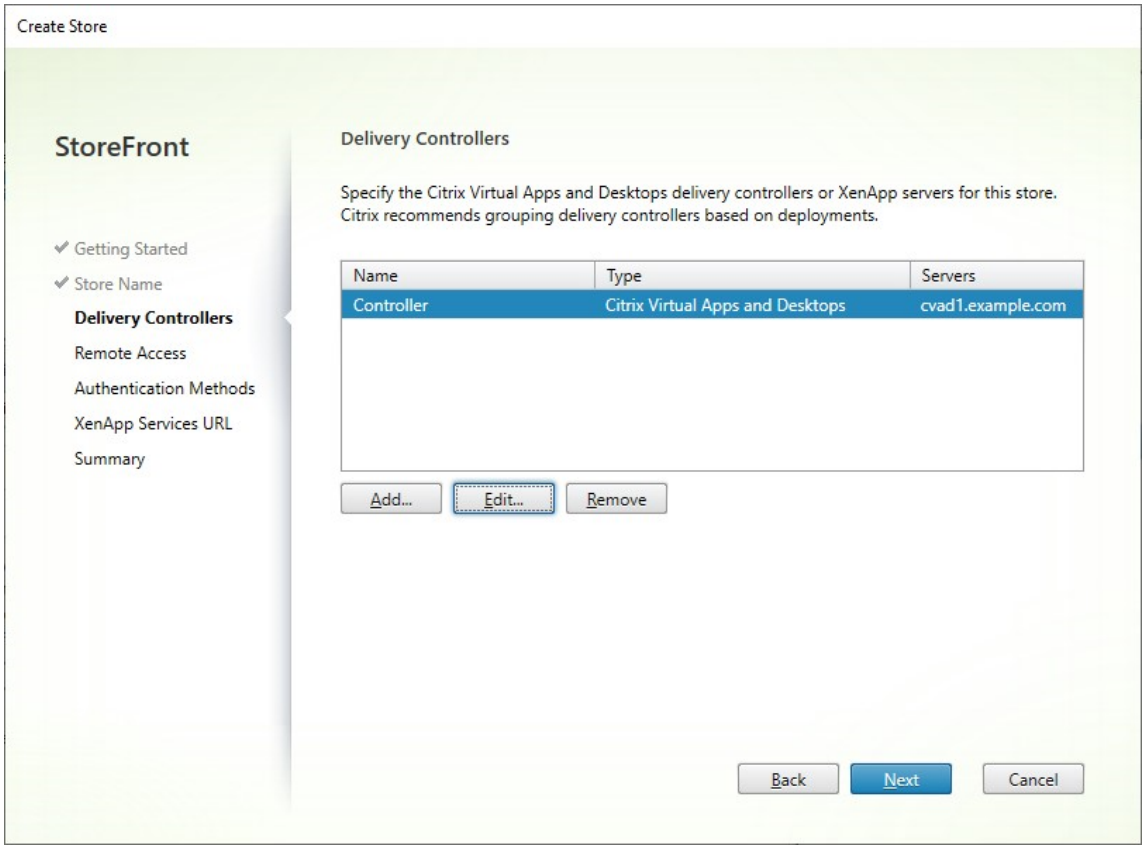
2. Führen Sie auf der Registerkarte **Storename** die folgenden Schritte aus:

   - Geben Sie einen Storenamen ein.
   - Wenn Sie Benutzern den anonymen bzw. nicht authentifizierten Zugriff auf den Store ermöglichen möchten, aktivieren Sie das Kontrollkästchen **Nur nicht authentifizierte (anonyme) Benutzer dürfen auf diesen Store zugreifen**. Wenn Sie einen Store ohne Authentifizierung erstellen, sind die Seiten **Authentifizierungsmethoden** und **Remotezugriff** nicht verfügbar und der **Servergruppenknoten** links und der Bereich "Aktion"wird durch **Basis-URL ändern** ersetzt. (Es ist nur diese Option verfügbar, weil Servergruppen für Server, die nicht in einer Domäne sind, nicht zur Verfügung stehen.)



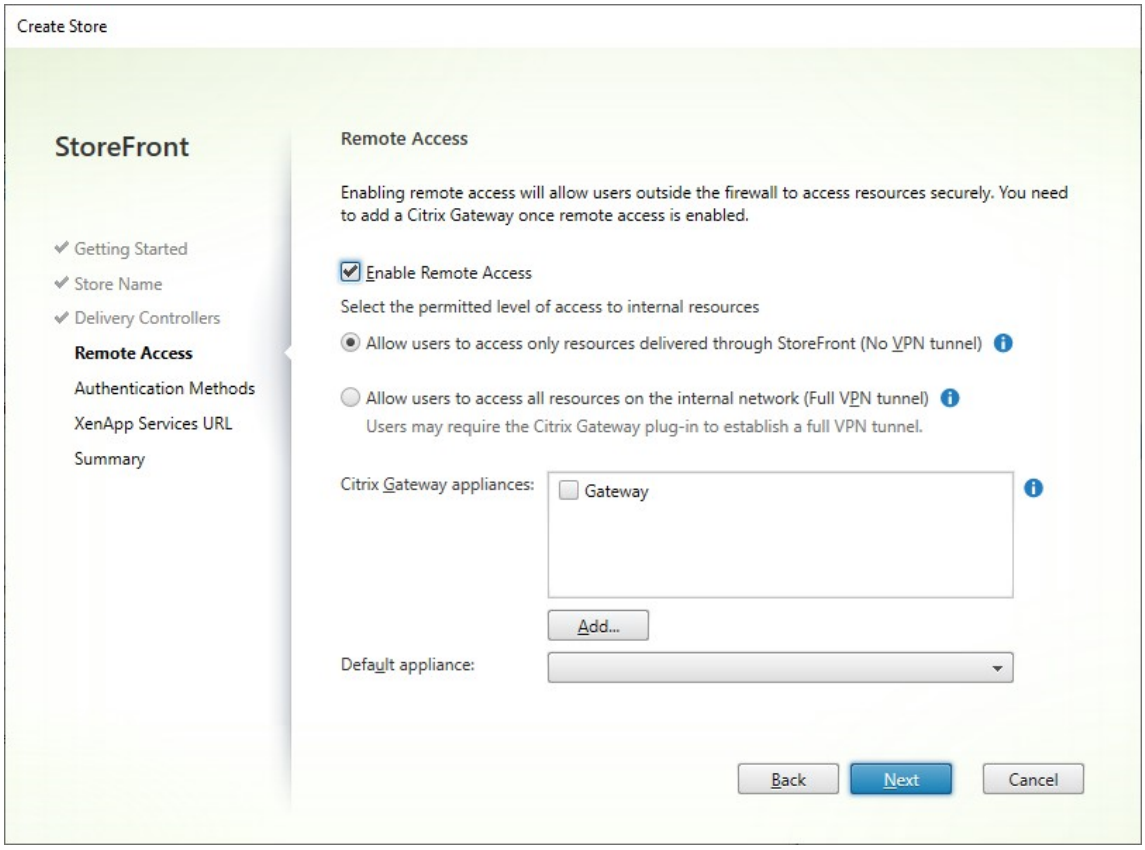
Klicken Sie auf **Weiter**.

3. Fügen Sie auf der Registerkarte **Delivery Controller** Ressourcenfeeds für die virtuellen Desktops und Anwendungen hinzu. Weitere Informationen finden Sie unter Durch Stores zur Verfügung gestellte Ressourcen verwalten.



Klicken Sie auf **Weiter**.

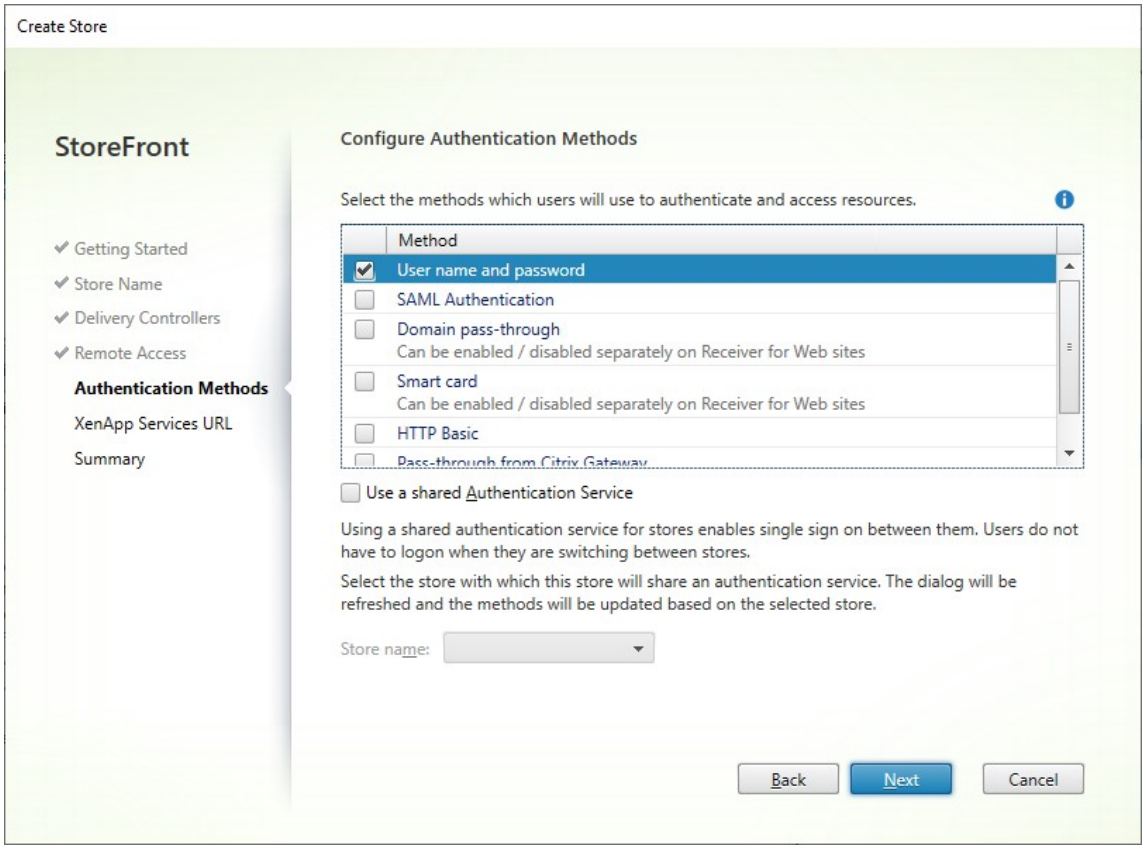
4. Wählen Sie auf der Registerkarte **Remotezugriff** aus, ob der Store über ein Citrix Gateway verfügbar sein soll. Weitere Informationen finden Sie unter Remotezugriff auf Stores über Citrix Gateway verwalten.



5. Wählen Sie auf der Registerkarte **Authentifizierungsmethoden** die Methoden, die Benutzer zum Authentifizieren und Zugreifen auf den Store verwenden, und klicken Sie auf **Weiter**.

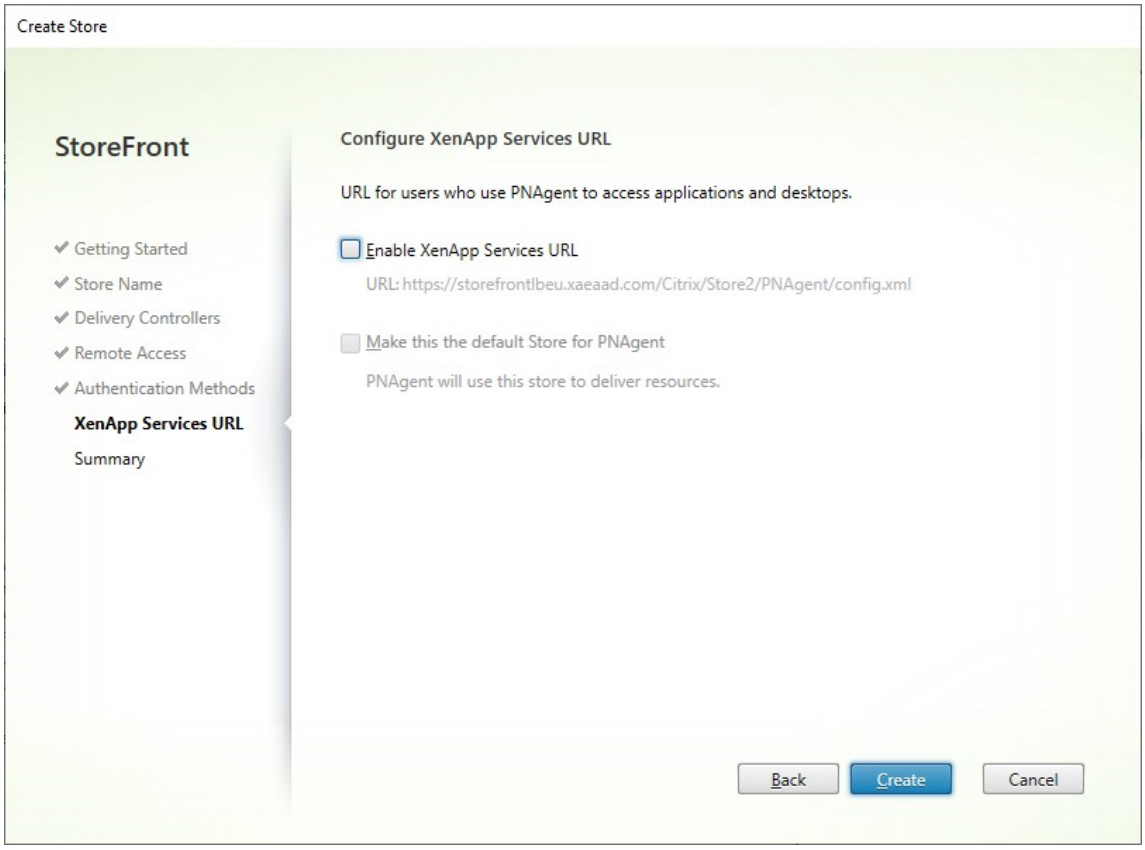
   Weitere Informationen zu den verfügbaren Authentifizierungsmethoden finden Sie unter Authentifizierungsdienst konfigurieren.

   Anstatt die Authentifizierungsmethoden für den Store separat zu konfigurieren, ist es möglich, die Authentifizierungskonfiguration mit einem anderen Store zu teilen. Aktivieren Sie hierfür **Gemeinsamen Authentifizierungsdienst verwenden** und wählen Sie einen Store aus.



Klicken Sie auf **Weiter**.

6. Wenn Sie ältere Geräte haben, die PNAgent benötigen, lassen Sie auf der Registerkarte **XenApp-Dienste-URL** das Kontrollkästchen **XenApp-Dienste-URL aktivieren** aktiviert. Andernfalls deaktivieren Sie es.



Klicken Sie auf **Erstellen**.

7. Nach dem Erstellen des Stores klicken Sie auf **Fertig stellen**.

Wenn ein neuer Store erstellt wird, wird auch eine neue Website erstellt, über die die Benutzer auf den Store zugreifen können. Sie können diese Website konfigurieren oder zusätzliche Websites erstellen.

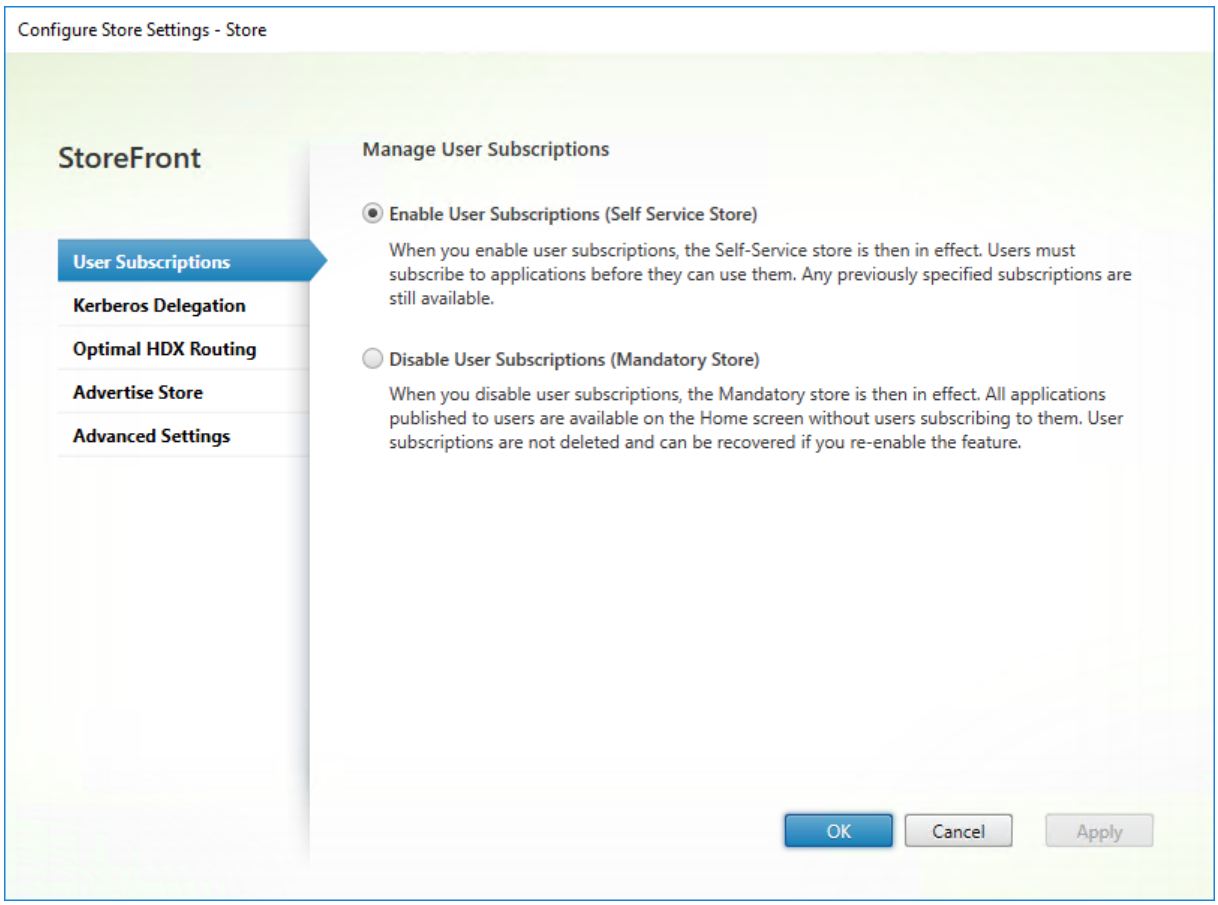
Store konfigurieren

April 17, 2024

Store ändern:

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren**.
2. Gehen Sie zur Registerkarte Benutzerabonnements, um vorzugeben, ob Favoriten aktiviert werden sollen.
3. Gehen Sie zur Registerkarte Kerberos-Delegierung, um vorzugeben, ob der Store die Kerberos-Delegierung zur Authentifizierung beim Delivery Controller verwendet.

4. Gehen Sie zur Registerkarte Optimales HDX-Routing, um vorzugeben, welches Gateway zum Starten von Apps und Desktops entsprechend ihrem Standort verwendet werden soll.
5. Gehen Sie zur Registerkarte Store ankündigen, um vorzugeben, ob der Store in der Workspace-App angezeigt werden soll, wenn der Benutzer den FQDN oder die E-Mail-Adresse eingibt.

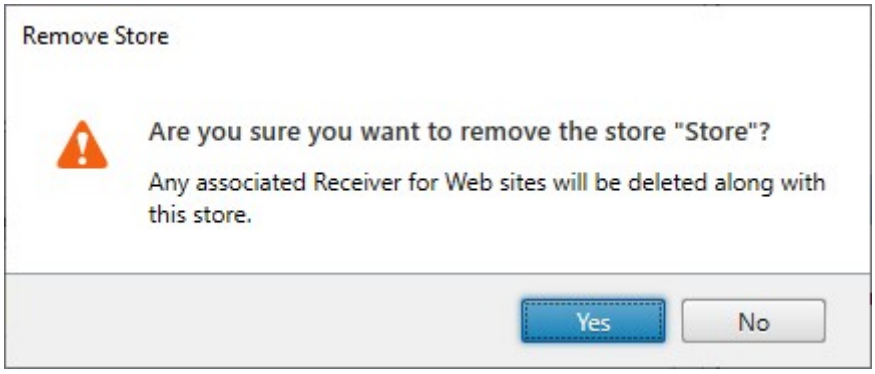


Store entfernen

April 17, 2024

Store entfernen:

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores**.
2. Klicken Sie im **Aktionsbereich** auf **Store entfernen**.
3. Klicken Sie im Bestätigungsfenster auf **Ja**.



Wenn Sie einen Store entfernen, werden alle diesem zugeordneten Websites ebenfalls gelöscht.

Store-Provisioningdateien für Benutzer exportieren

September 27, 2023

Sie können Dateien mit Verbindungsinformationen für Stores, einschließlich Citrix Gateway-Bereitstellungen und Beacons, die für Stores konfiguriert wurden, generieren. Stellen Sie diese Dateien Benutzern zur Verfügung, damit diese die Citrix Workspace-App automatisch mit den Details der Stores konfigurieren können. Die Benutzer können auch Citrix Workspace-App-Provisioningdateien herunterladen, wenn sie über einen Webbrowser auf einen Store zugreifen.

> Wichtig:
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss
> übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Um eine Provisioningdatei mit Details für mehrere Stores zu generieren, klicken Sie im Bereich “Aktionen”auf **Multistore-Provisioningdatei exportieren** und wählen Sie die Stores aus, die der Datei hinzugefügt werden sollen.
2. Klicken Sie auf **Exportieren** und speichern Sie die Provisioningdatei mit der Erweiterung **.cr** an einem geeigneten Speicherort im Netzwerk.

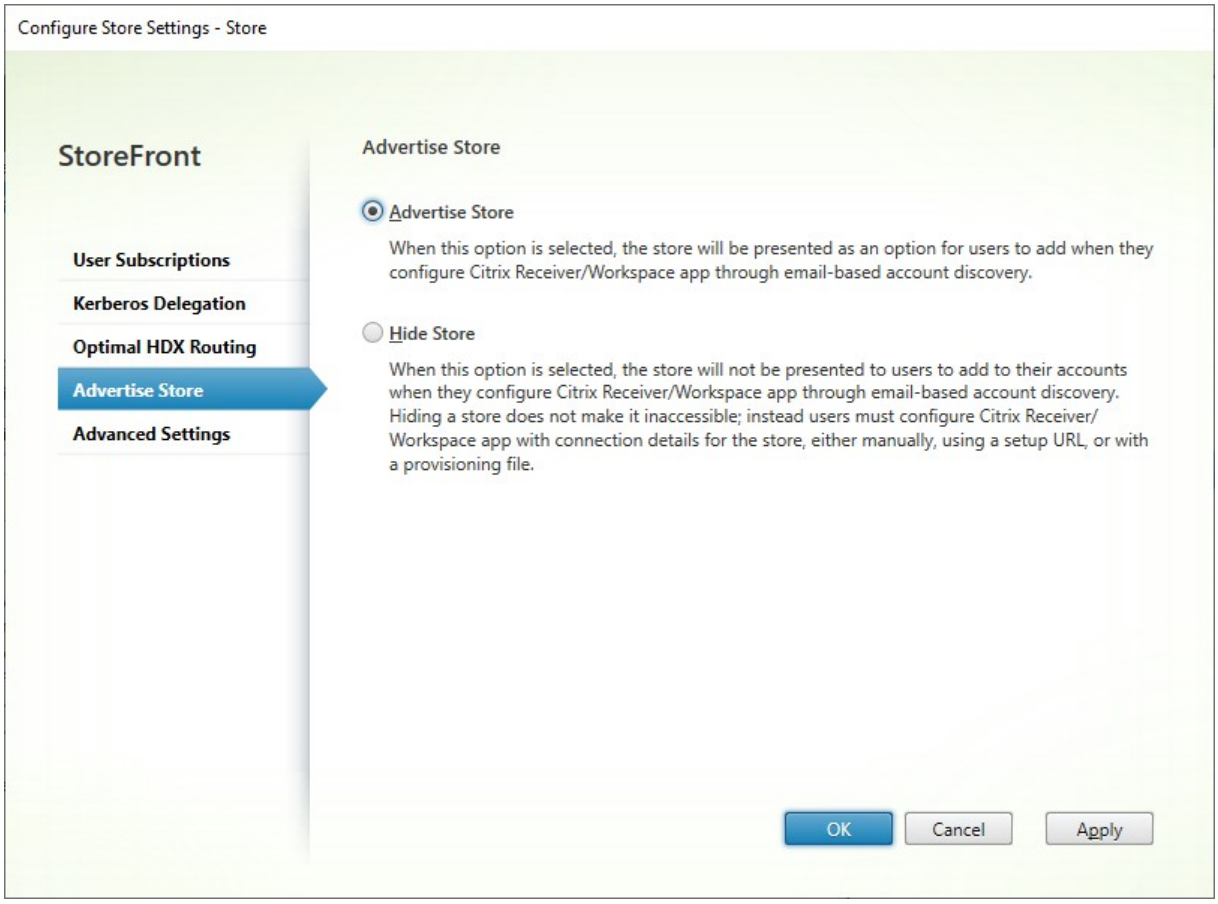
Stores für Benutzer ankündigen und ausblenden

April 17, 2024

Sie können auswählen, ob Stores den Benutzern zum Hinzufügen zu ihrem Konto angezeigt werden, wenn diese die Citrix Workspace-App über die E-Mail-basierte Kontenermittlung oder den vollqualifizierten Domänennamen (FQDN) konfigurieren. Wenn Benutzer die StoreFront-Bereitstellung, die einen Store hostet, ermitteln, werden erstellte Stores standardmäßig als Option zum Hinzufügen in Citrix Receiver angezeigt. Wenn Sie einen Store ausblenden, wird dieser dadurch nicht unzugänglich, doch die Benutzer müssen die Citrix Workspace-App mit den Verbindungsinformationen für den Store konfigurieren und zwar entweder manuell mit einer Setup-URL oder mit einer Provisioningdatei.

> Wichtig:
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss
> übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren** > **Store ankündigen**.
2. Wählen Sie auf der Seite **Store ankündigen** die Option **Store ankündigen** oder **Store ausblenden**.



Kerberos-Delegierung

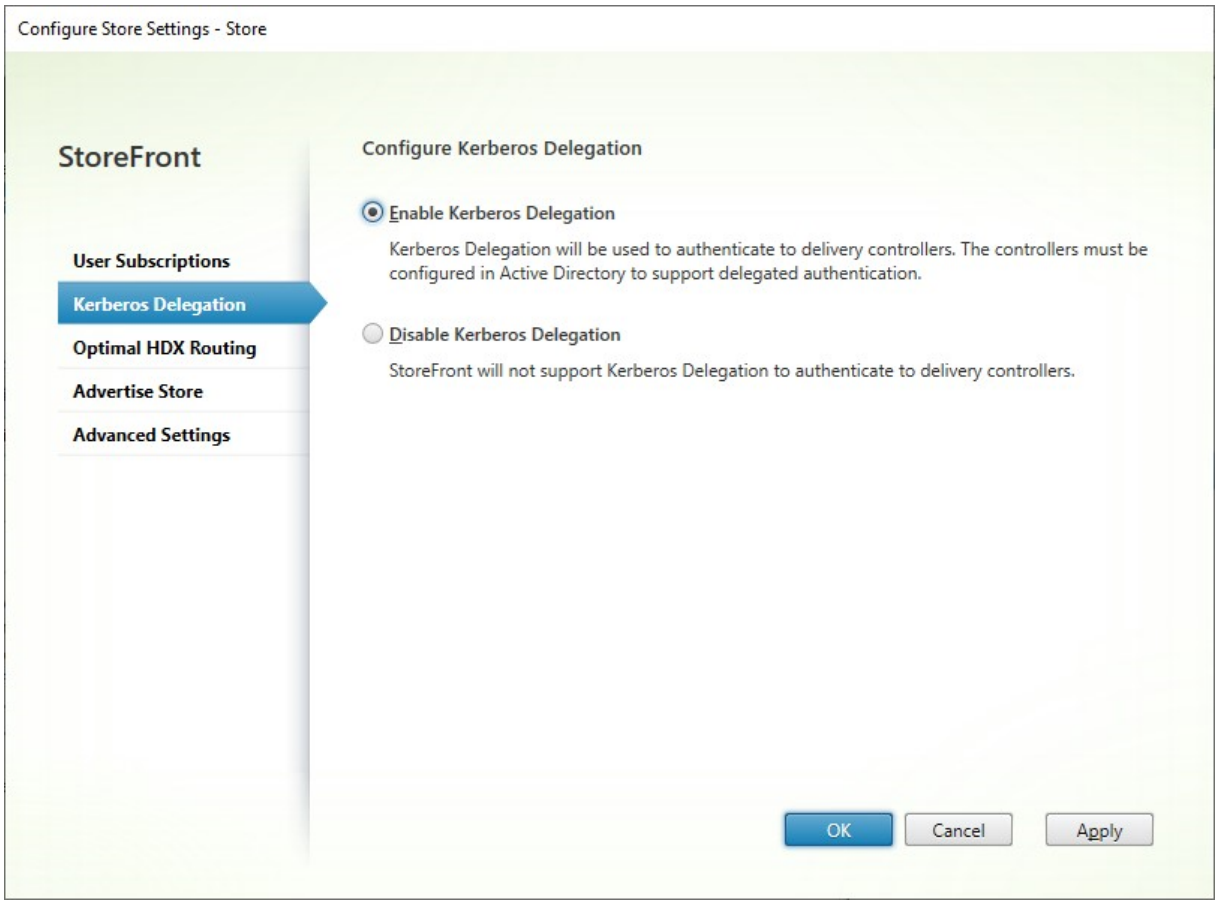
April 17, 2024

> **Hinweis:**
>
> Kerberos kann nur mit XenApp 6.5 und früheren Versionen verwendet werden.

Bei Verwendung der Domänen-Passthrough- oder Smartcard-Authentifizierung, entweder direkt oder über ein Citrix Gateway, verfügt StoreFront nicht über die Anmeldeinformationen des Benutzers und kann sich daher nicht mit den Anmeldeinformationen des Benutzers beim Delivery Controller authentifizieren. Wenn Sie XenApp 6.5 und früher verwenden, können Sie die Kerberos-Delegierung aktivieren, damit StoreFront die Identität des Benutzers annehmen kann, um sich beim Delivery Controller zu authentifizieren. Dazu muss die Delegierung in Active Directory konfiguriert werden.

1. Wählen Sie einen Store und klicken Sie im Aktionsbereich auf **Storeeinstellungen konfigurieren**.

2. Wählen Sie die Registerkarte **Kerberos-Delegierung**.
3. Wählen Sie **Kerberos-Delegierung aktivieren** oder **Kerberos-Delegierung deaktivieren**.
4. Klicken Sie auf **Anwenden** bzw. **OK**, um die Änderungen zu speichern.



PowerShell SDK

Um die Kerberos-Delegierung zu konfigurieren, verwenden Sie das Cmdlet Set-STFStoreService mit dem Parameter `-KerberosDelegation`.

Durch Stores zur Verfügung gestellte Ressourcen verwalten

April 17, 2024

Im Fenster **Delivery Controller verwalten** können Sie von Citrix Virtual Apps and Desktops, Citrix Desktops as a Service und Citrix Secure Private Access bereitgestellte Ressourcenfeeds hinzufügen, ändern und löschen.

Ressourcenfeeds anzeigen

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores**.
2. Wählen Sie im Ergebnisbereich einen Store.
3. Klicken Sie im Bereich **Aktionen** auf **Delivery Controller verwalten**.

Ressourcenfeeds mit dem PowerShell-SDK anzeigen

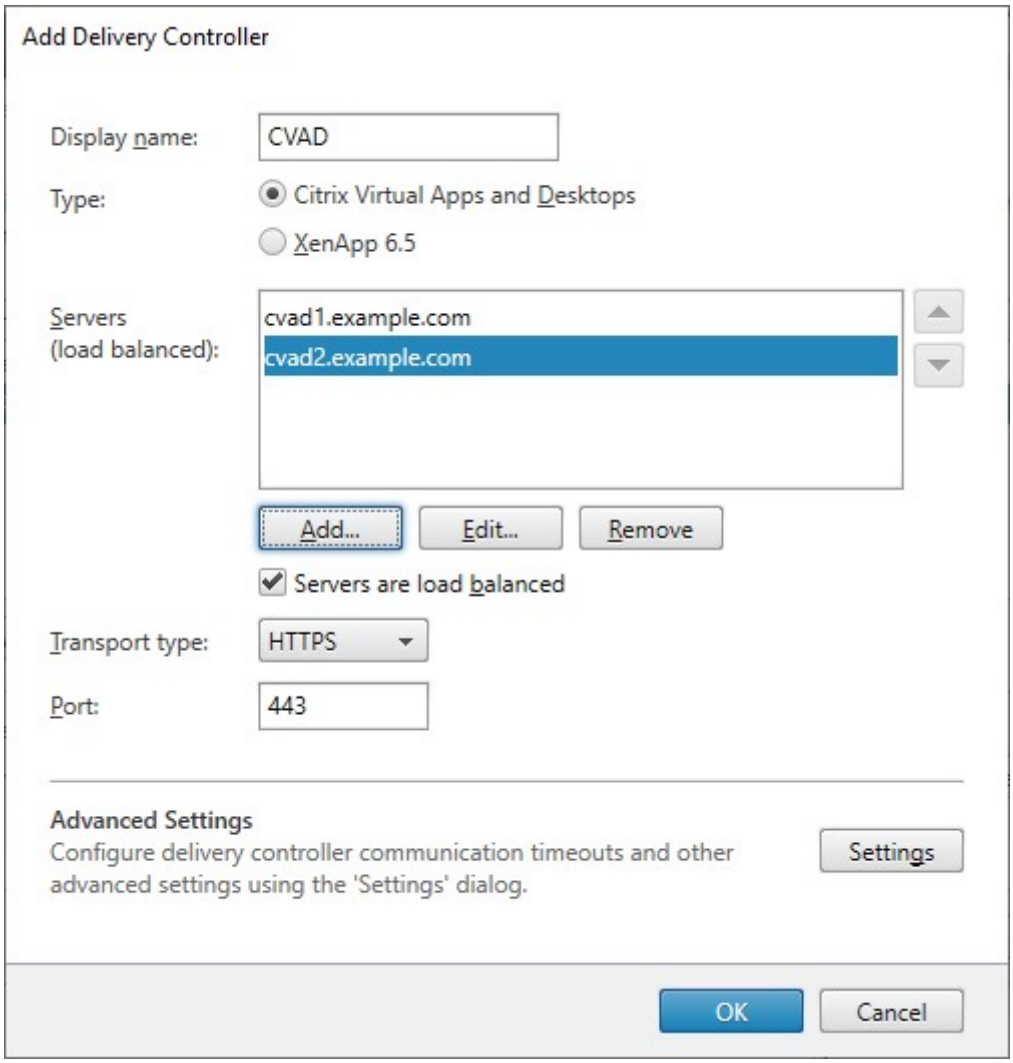
Verwenden Sie im PowerShell-SDK den Befehl Get-STFStoreFarm, um alle Ressourcenfeeds oder einen einzelnen Ressourcenfeed aufzulisten.

Ressourcenfeeds hinzufügen

Ressourcenfeeds für Citrix Virtual Apps and Desktops hinzufügen

1. Klicken Sie im Fenster **Delivery Controller verwalten** auf **Hinzufügen**.
2. Geben Sie einen **Anzeigenamen** zur Identifizierung des Feeds ein.
3. Wählen Sie für **Typ** die Option **Citrix Virtual Apps and Desktops**.
4. Klicken Sie unter **Server** auf **Hinzufügen** und geben Sie den Namen des Delivery Controllers ein. Wiederholen Sie diesen Schritt für jeden Delivery Controller. Citrix empfiehlt, mindestens zwei Server für den Lastenausgleich bzw. ein Failover zu verwenden.
5. Citrix empfiehlt die Auswahl der Option für **Server mit Lastenausgleich**. Dadurch verteilt StoreFront die Last auf alle Delivery Controller oder Connectors, indem bei jedem Start ein Server nach dem Zufallsprinzip aus der Liste ausgewählt wird. Wenn diese Option nicht ausgewählt ist, wird die Serverliste wie eine Failoverliste mit Prioritätsreihenfolge behandelt. In diesem Fall erfolgen 100 % der Starts auf dem ersten aktiven Delivery Controller oder Connector in der Liste. Wenn dieser Server offline geht, werden 100 % der Starts mit dem zweiten Server in der Liste ausgeführt usw.
6. Wählen Sie aus der Liste **Transporttyp** die Verbindungstypen für StoreFront, die für die Kommunikation mit den Servern verwendet werden sollen.
   - Wählen Sie **HTTP** aus, wenn Daten über unverschlüsselte Verbindungen gesendet werden sollen. Bei Auswahl dieser Option müssen Sie eigene Maßnahmen treffen, um die Verbindungen zwischen StoreFront und den Servern zu sichern.
   - Um Daten über TLS-Verbindungen zu senden, wählen Sie **HTTPS** (empfohlen). Wenn Sie diese Option für Citrix Virtual Apps and Desktops-Server auswählen, vergewissern Sie sich, dass der Citrix XML-Dienst so konfiguriert ist, dass der Port gemeinsam mit Internetinformationsdienste (IIS) verwendet wird und in der IIS-Konfiguration HTTPS-Unterstützung festgelegt wurde.

> **Hinweis:**
>
> Wenn Sie die Verbindungen zwischen StoreFront und den Servern mit HTTPS sichern, achten Sie darauf, dass die in der Liste "Server" eingegebenen Servernamen genau mit den Namen in den Zertifikaten für die Server übereinstimmen. Die Groß- und Kleinschreibung wird berücksichtigt.



1. Geben Sie den Port an, den StoreFront für Verbindungen mit dem Server verwenden soll. Der Standardport ist 80 für HTTP-Verbindungen und 443 für HTTPS-Verbindungen. Der angegebene Port muss der vom Citrix XML-Dienst verwendete Port sein.

Ressourcenfeeds für Citrix Desktops as a Service hinzufügen

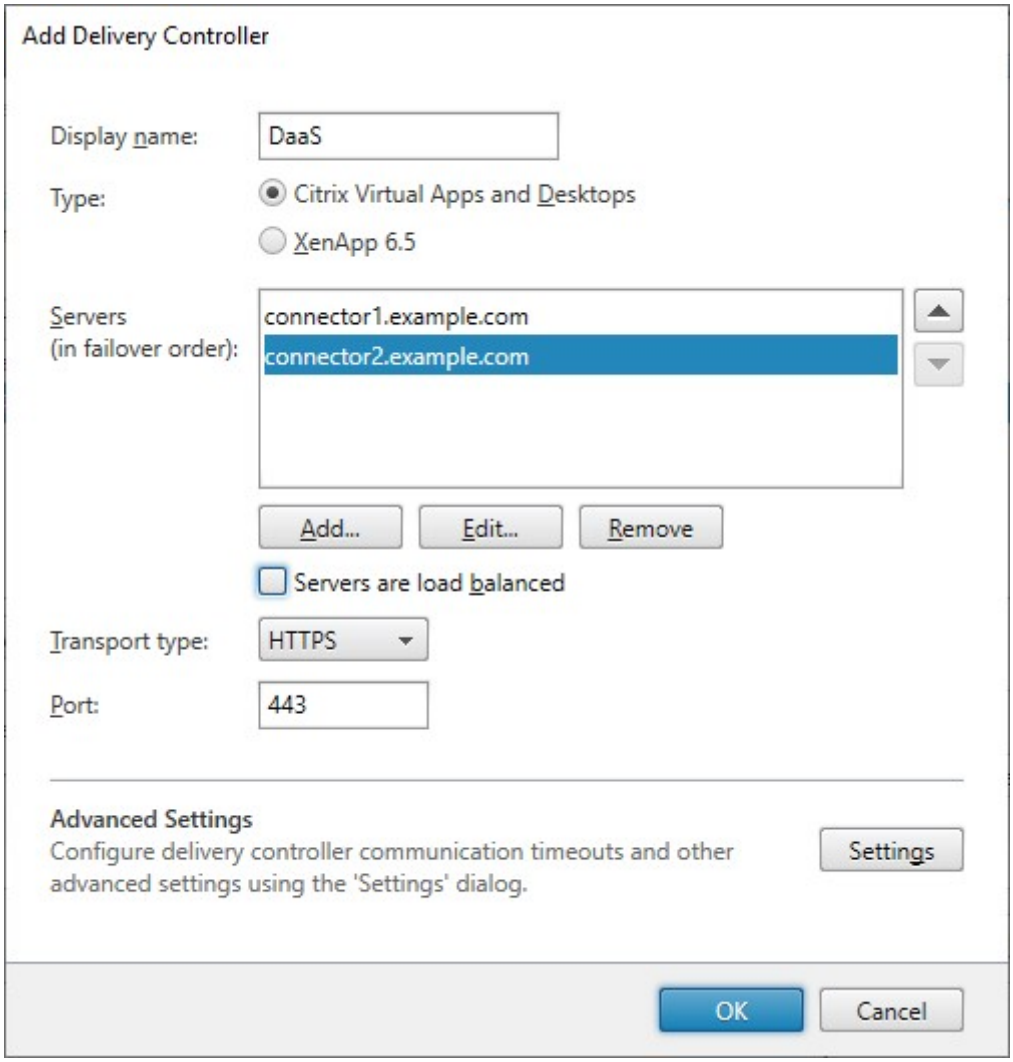
1. Klicken Sie im Fenster **Delivery Controller verwalten** auf **Hinzufügen**.

2. Geben Sie einen **Anzeigenamen** zur Identifizierung des Feeds ein.
3. Wählen Sie für **Typ** die Option **Citrix Virtual Apps and Desktops**.
4. Klicken Sie unter **Server** auf **Hinzufügen** und geben Sie den Namen eines Cloud Connectors ein. Wiederholen Sie diesen Vorgang für jeden Server bzw. Connector. Citrix empfiehlt aus Redundanzgründen mindestens zwei Connectors zu konfigurieren. Wenn Sie mehrere Ressourcenstandorte haben, empfiehlt Citrix, die Cloud Connectors von allen Ressourcenstandorten hinzuzufügen und die erweiterte Integritätsprüfung zu aktivieren. Dadurch wird sichergestellt, dass StoreFront während eines Ausfalls den lokalen Hostcache verwenden kann, um VDAs am entsprechenden Standort zu starten.
5. Wenn Sie Connectors aus mehreren Standorten haben, empfiehlt Citrix, die Connectors mit der niedrigsten Latenz zum StoreFront-Server ganz oben in der Liste zu platzieren und die Option für **Server mit Lastenausgleich** zu deaktivieren. Da die Connectors Informationen an DaaS-Delivery Controller nur per Proxy darstellen, hat Verwendung des Lastausgleichs nur begrenzte Vorteile.
6. Wählen Sie aus der Liste **Transporttyp** die Verbindungstypen für StoreFront, die für die Kommunikation mit den Servern verwendet werden sollen.

    - Wählen Sie **HTTP** aus, wenn Daten über unverschlüsselte Verbindungen gesendet werden sollen. Bei Auswahl dieser Option müssen Sie eigene Maßnahmen treffen, um die Verbindungen zwischen StoreFront und den Cloud Connectors zu sichern.
    - Um Daten über sichere HTTPS-Verbindungen zu senden, wählen Sie **HTTPS**aus. Wenn Sie diese Option auswählen, müssen Sie sicherstellen, dass die Cloud Connectors für HTTPS konfiguriert sind.

    > **Hinweis:**
    >
    > Wenn Sie die Verbindungen zwischen StoreFront und den Servern mit HTTPS sichern, achten Sie darauf, dass die in der Liste "Server"eingegebenen Servernamen genau mit den Namen in den Zertifikaten für die Server übereinstimmen. Die Groß- und Kleinschreibung wird berücksichtigt.

7. Geben Sie den Port an, den StoreFront für Verbindungen mit dem Server verwenden soll. Der Standardport ist 80 für HTTP-Verbindungen und 443 für HTTPS-Verbindungen.



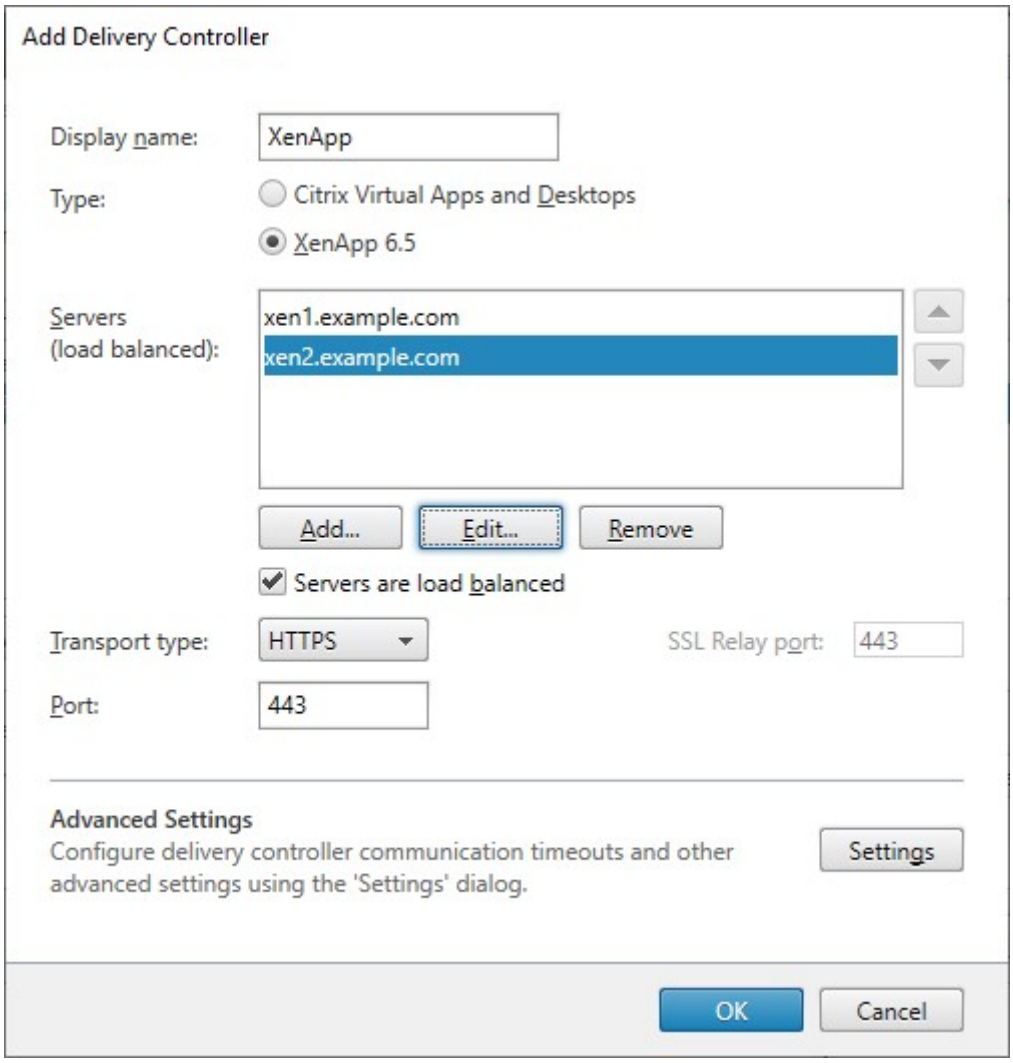
Ressourcenfeeds für XenApp 6.5 hinzufügen

1. Geben Sie einen **Anzeigenamen** zur Identifizierung des Feeds ein.
2. Wählen Sie als **Typ** die Option **Citrix Secure Private Access**.
3. Geben Sie den Namen des **Citrix Secure Private Access-Servers** ein.
4. Wählen Sie aus der Liste **Transporttyp** die Verbindungstypen für StoreFront, die für die Kommunikation mit den Servern verwendet werden sollen.

    - Wählen Sie **HTTP** aus, wenn Daten über unverschlüsselte Verbindungen gesendet werden sollen. Bei Auswahl dieser Option müssen Sie eigene Maßnahmen treffen, um die Verbindungen zwischen StoreFront und den Servern zu sichern.
    - Wählen Sie **HTTPS** aus, um Daten über sichere HTTP-Verbindungen mit SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) zu senden.
    - Wählen Sie SSL-Relay aus, um Daten über sichere Verbindungen an Citrix Virtual Apps-

Server zu senden. SSL-Relay übernimmt die Hostauthentifizierung und Datenverschlüsselung. Sie müssen auch einen SSL-Relay-Port eingeben.

5. Geben Sie den Port an, den StoreFront für Verbindungen mit dem Server verwenden soll. Der Standardport ist 80 für HTTP- oder SSL-Relay-Verbindungen und 443 für HTTPS-Verbindungen.



Ressourcenfeed mit dem PowerShell-SDK erstellen

Um einen Ressourcenfeed hinzuzufügen, verwenden Sie den Befehl Add-STFStoreFarm

- Stellen Sie für Citrix Virtual Apps and Desktops oder Citrix Desktops as a Service `FarmType` auf `XenDesktop` ein.
- Für XenApp 6.5 setzen Sie `FarmType` auf `XenApp`.

Ressourcenfeed ändern

Wählen Sie im Fenster **Delivery Controller verwalten** einen Ressourcenfeed und klicken Sie auf **Bearbeiten**.

Ressourcenfeed mit dem PowerShell-SDK ändern

Um einen Ressourcenfeed mithilfe von PowerShell zu ändern, verwenden Sie den Befehl Set-STFStoreFarm.

Ressourcenfeed löschen

Wählen Sie im Fenster **Delivery Controller verwalten** einen Ressourcenfeed und klicken Sie auf **Entfernen**.

Ressourcenfeed mit dem PowerShell-SDK löschen

Um einen Ressourcenfeed mithilfe von PowerShell zu löschen, verwenden Sie den Befehl Remove-STFStoreFarm.

Konfigurieren der Serverumgehung

Zur Verbesserung der Leistung bei Ausfall eines Servers, auf dem Ressourcen bereitgestellt werden, umgeht StoreFront vorübergehend Server, die nicht antworten. Bei einer Serverumgehung ignoriert StoreFront den Server und greift nicht auf dessen Ressourcen zu. Verwenden Sie folgende Parameter, um die Dauer der Umgehung festzulegen:

- **Umgehungsdauer bei Ausfall aller Server** ist eine reduzierte Dauer in Minuten, die StoreFront anstelle von **Umgehungsdauer** verwendet, wenn alle Server eines bestimmten Delivery Controllers umgangen werden. Der Standardwert ist 0 Minuten.
- **Umgehungsdauer** ist die Zeit in Minuten, die StoreFront einen einzelnen Server nach einem fehlgeschlagenen Kommunikationsversuch umgeht. Die Standarddauer für die Umgehung ist 60 Minuten.

Überlegungen beim Angeben der "Umgehungsdauer bei Ausfall aller Server"

Die Wahl eines höheren Werts für **Umgehungsdauer bei Ausfall aller Server** vermindert die Auswirkungen eines Ausfalls eines bestimmten Delivery Controllers, jedoch stehen die Ressourcen auf diesem Delivery Controller nach einem temporären Netzwerk- oder Serverausfall Benutzern für

die angegebene Dauer nicht zur Verfügung. Verwenden Sie ggf. einen höheren Wert für **Umgehungsdauer bei Ausfall aller Server**, wenn viele Delivery Controller für einen Store konfiguriert sind, insbesondere für nicht geschäftskritische Delivery Controller.

Die Wahl eines niedrigeren Werts für **Umgehungsdauer bei Ausfall aller Server** erhöht die Verfügbarkeit von Ressourcen auf dem Delivery Controller, gleichzeitig jedoch auch das Risiko clientseitiger Timeouts, wenn viele Delivery Controller konfiguriert sind und mehrere ausfallen. Es empfiehlt sich, den Standardwert von 0 Minuten für geschäftskritische Delivery Controller, bzw. wenn nur wenige Farmen konfiguriert sind, beizubehalten.

Bypass-Parameter ändern

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores**.
2. Wählen Sie im Ergebnisbereich einen Store.
3. Klicken Sie im Bereich **Aktionen** auf **Delivery Controller verwalten**.
4. Wählen Sie einen Controller aus, klicken Sie auf **Bearbeiten** und dann auf **Einstellungen** auf dem Bildschirm **Delivery Controller bearbeiten**.
5. Klicken Sie unter "Erweiterte Einstellungen"auf **Einstellungen**.
6. Gehen Sie im Dialogfeld "Erweiterte Einstellungen"vor:

    a) Klicken Sie in der Zeile **Umgehungsdauer bei Ausfall aller Server** in die zweite Spalte und geben Sie eine Zeit in Minuten ein, für die ein Delivery Controller als offline betrachtet wird, nachdem alle seine Server nicht geantwortet haben.
    b) Klicken Sie in der Zeile **Umgehungsdauer** in die zweite Spalte und geben Sie eine Zeit in Minuten ein, für die ein einzelner Server als offline betrachtet wird, wenn er nicht antwortet.

Benutzer zu Ressourcenfeeds zuordnen

Standardmäßig wird Benutzern beim Zugriff auf einen Store ein Aggregat aller für sie verfügbaren Ressourcen aus allen für den Store konfigurierten Ressourcenfeeds angezeigt. Um unterschiedlichen Benutzern eigene Ressourcen bereitzustellen, können Sie separate Stores oder sogar separate StoreFront-Bereitstellungen konfigurieren. Alternativ können Sie den Zugriff auf bestimmte Bereitstellungen auf Basis der Mitgliedschaft der Benutzer in Microsoft Active Directory-Gruppen gewähren. So können Sie für verschiedene Benutzergruppen verschiedene Benutzererfahrungen über einen einzelnen Store konfigurieren.

Sie können z. B. allgemeine Ressourcen für alle Benutzer in einer Bereitstellung gruppieren und Finanzanwendungen für die Buchhaltungsabteilung in einer anderen. In einer solchen Konfiguration sieht ein Benutzer, der kein Mitglied der Benutzergruppe "Buchhaltung"ist, nur die allgemeinen

Ressourcen, wenn er auf den Store zugreift. Ein Mitglied der Gruppe "Buchhaltung"sieht neben den allgemeinen Ressourcen auch die Finanzanwendungen.

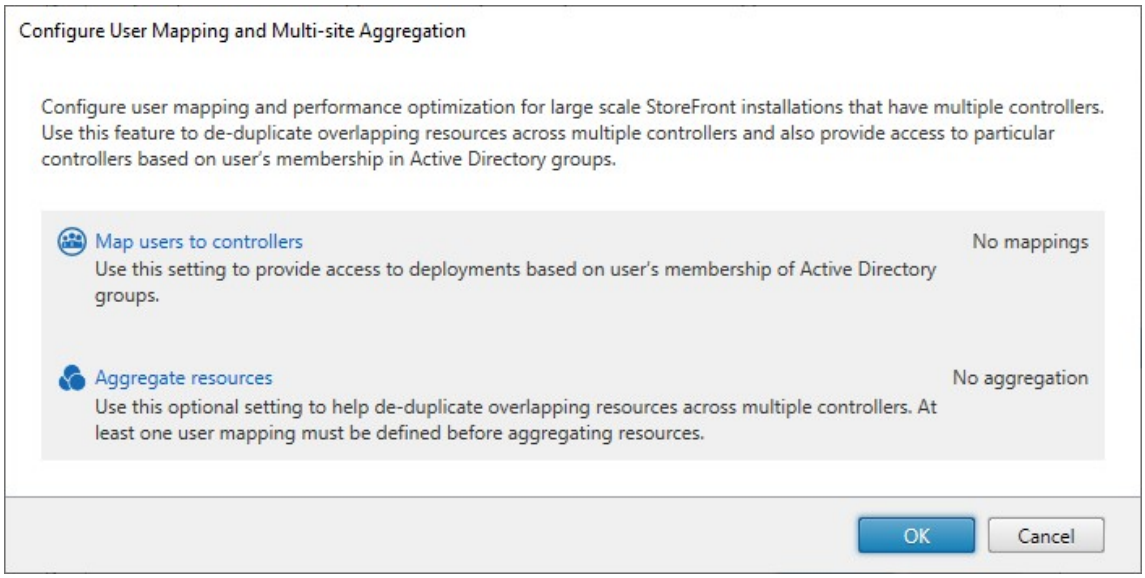
Für Poweruser können Sie auch eine Bereitstellung erstellen, die dieselben Ressourcen wie die anderen Bereitstellungen enthält, jedoch auf schnellerer und leistungsfähigerer Hardware beruht. So können Sie eine verbesserte Benutzererfahrung für wichtige Benutzer, wie etwa Führungskräfte, bereitstellen. Alle Benutzer sehen bei der Anmeldung bei einem Store die gleichen Desktops und Anwendungen, die Mitglieder der Gruppe "Führungskräfte"werden jedoch bevorzugt mit den Ressourcen der Bereitstellung für Poweruser verbunden.

> Hinweis:
>
> Dabei werden vollständige Ressourcenfeeds gefiltert. Darüber hinaus können Anwendungen innerhalb eines Ressourcenfeeds nach Benutzergruppen in der Citrix Virtual Apps and Desktops Studio-Konfiguration gefiltert werden.

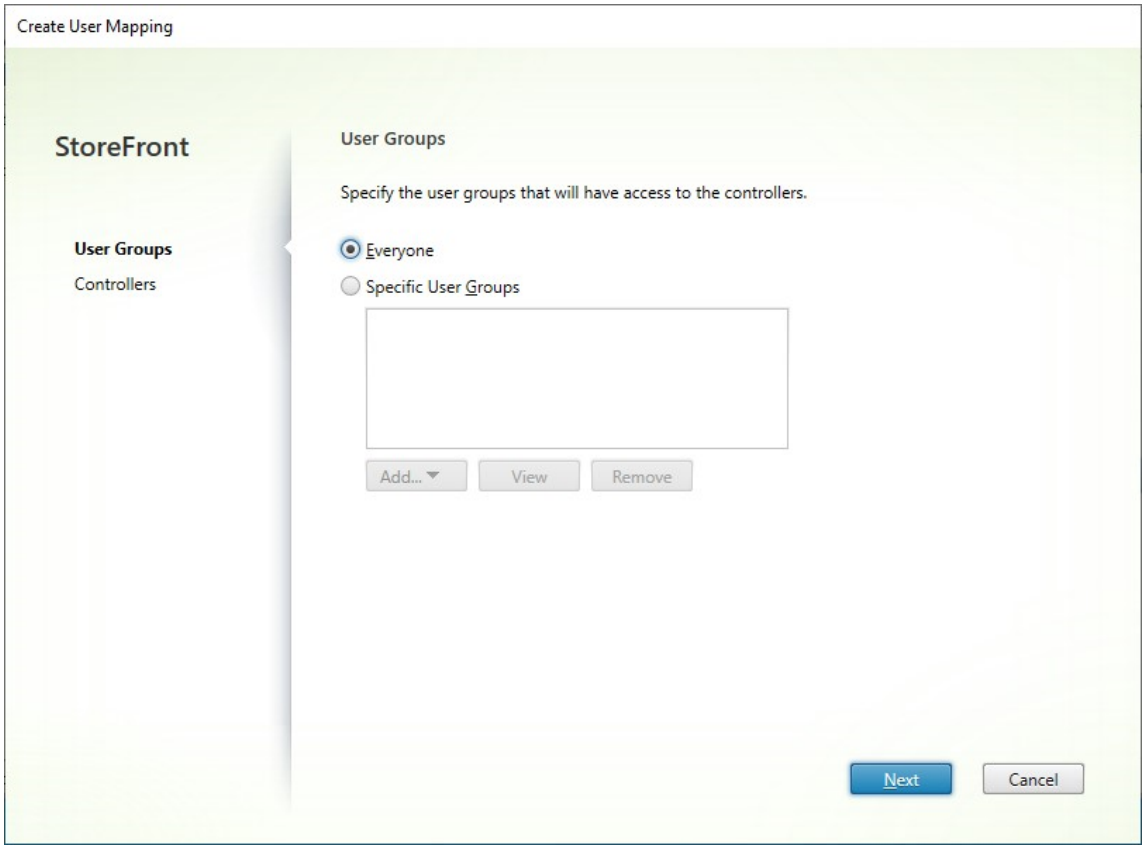
Gehen Sie wie folgt vor, um spezifische Ressourcenfeeds für eine Benutzergruppe zu konfigurieren:

1. Klicken Sie im Fenster **Delivery Controller verwalten** unter **Benutzerzuordnung und Multisiteaggregation konfigurieren** auf **Konfigurieren**. Diese Option ist nur verfügbar, wenn mindestens zwei Ressourcenfeeds konfiguriert sind.

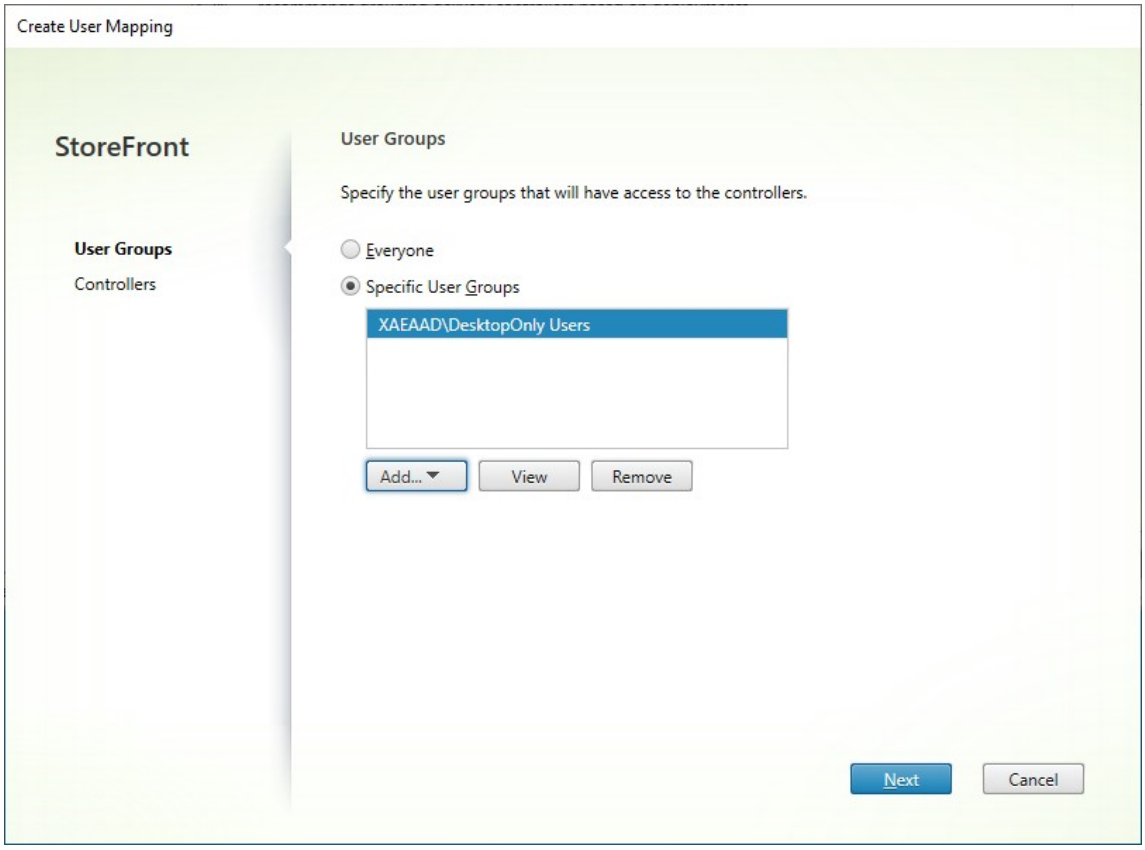
   Dadurch wird das Fenster **Benutzerzuordnung und Multisiteaggregation konfigurieren** geöffnet.



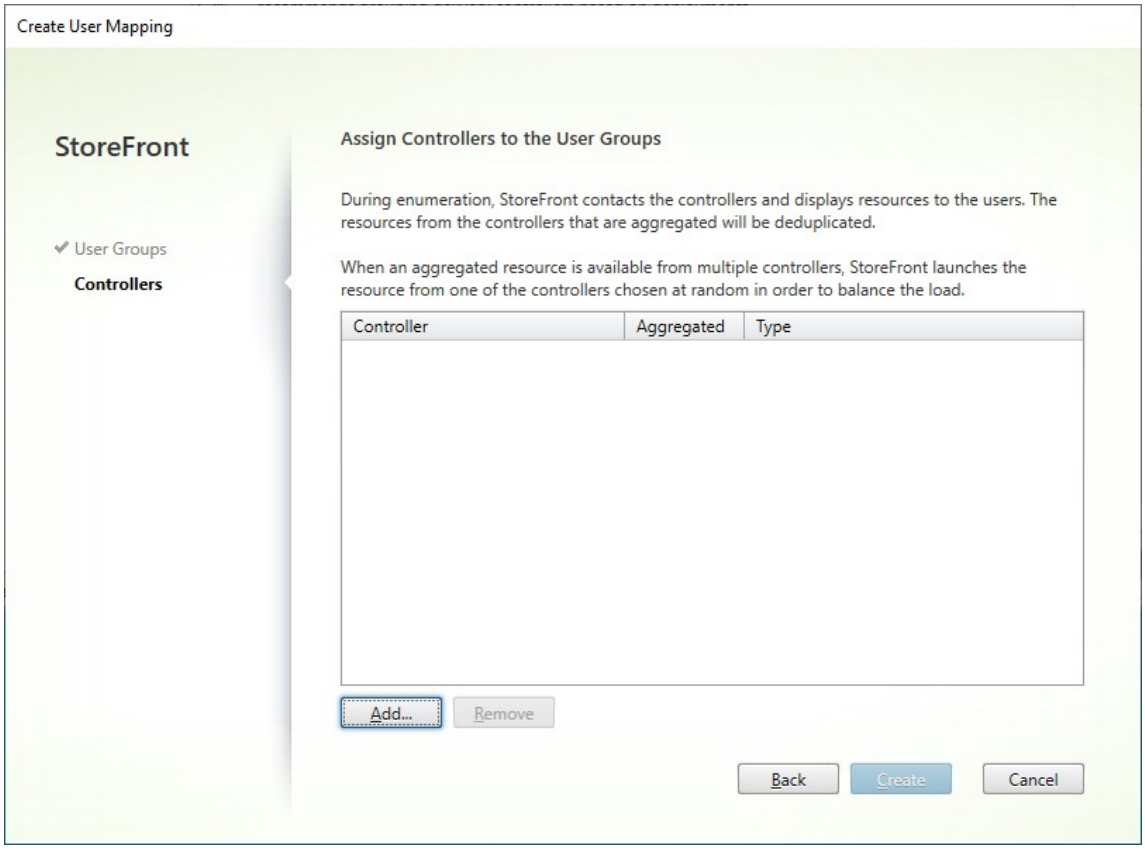
2. Klicken Sie auf **Benutzer Controllern zuordnen**. Dadurch wird das Fenster **Benutzerzuordnung erstellen** geöffnet, in dem Sie die erste Zuordnung erstellen können. Sie können später weitere Zuordnungen erstellen.



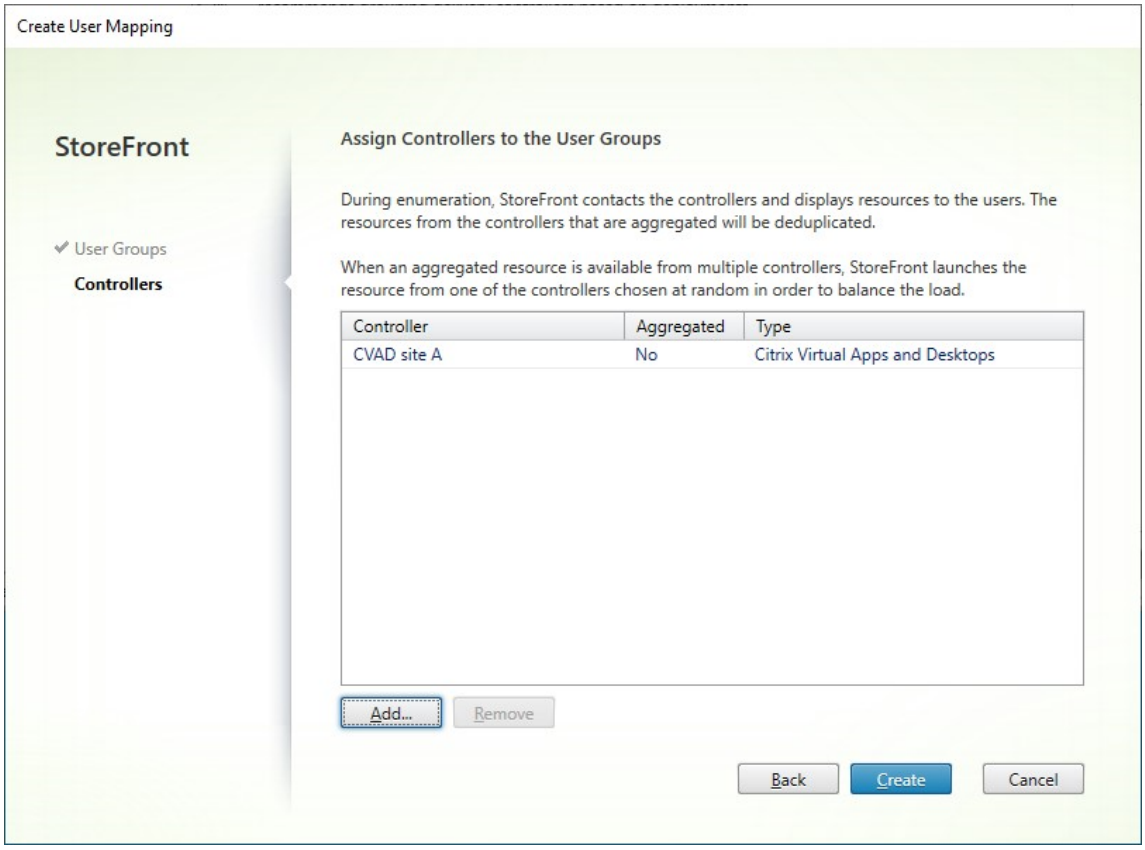
3. Wählen Sie **Jeder** oder **Spezifische Benutzergruppen** und fügen Sie eine oder mehrere Gruppen hinzu.



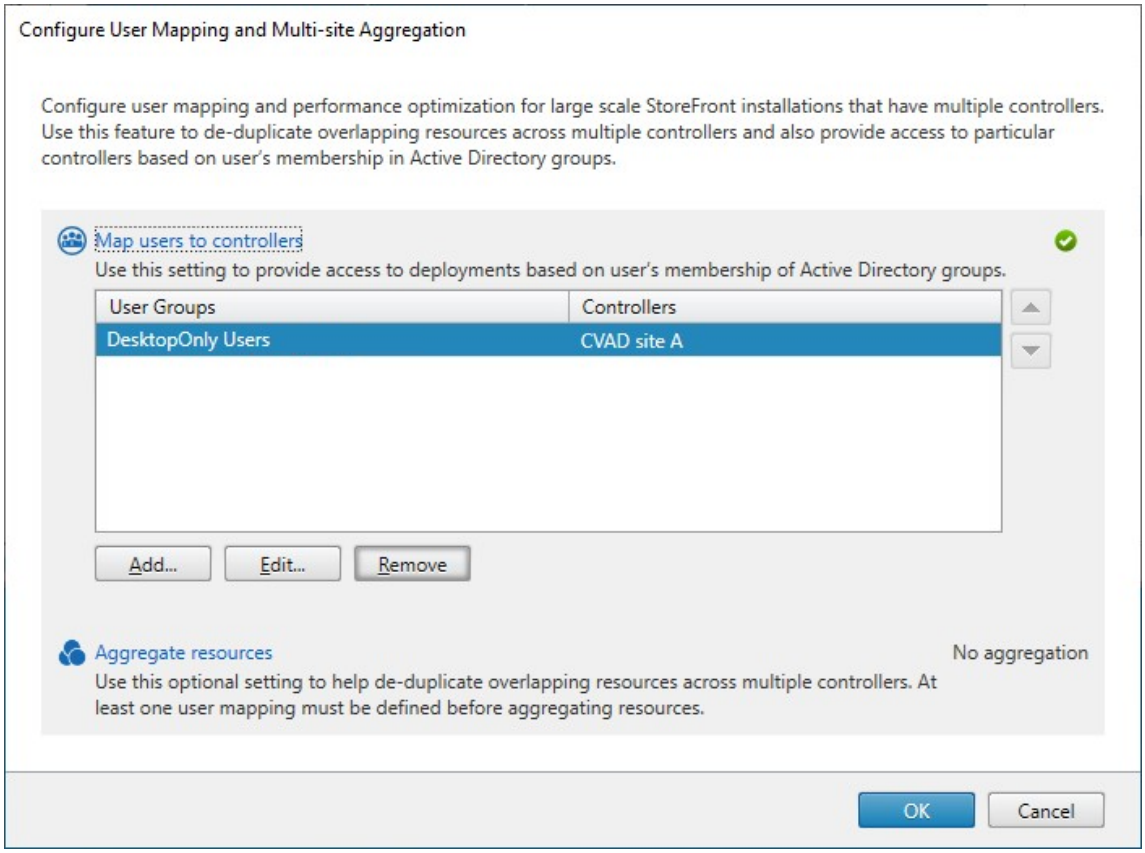
4. Klicken Sie auf **Weiter**. Dadurch gelangen Sie zur Registerkarte **Controller**.



5. Klicken Sie auf **Hinzufügen** und fügen Sie einen oder mehrere Controller hinzu.



6. Klicken Sie auf **Erstellen**.



7. Klicken Sie auf **Hinzufügen...** um nach Bedarf weitere Zuordnungen zu erstellen.

Ressourcen mithilfe des PowerShell-SDK Benutzer zuordnen

Sie können Ressourcen Benutzer mit dem PowerShell-SDK zuordnen.

1. Erstellen Sie für jeden Ressourcenfeed ein EquivalentFarmSet. Alle Ressourcenfeeds müssen Teil eines Farmsets sein, andernfalls stehen sie keinem Benutzer zur Verfügung. Rufen Sie New-STFEquivalentFarmset mit den folgenden Parametern auf:

   - `Name`: eindeutiger Name für das EquivalentFarmSet
   - `PrimaryFarms`: Name des nicht aggregierten Ressourcenfeeds (Farm).

2. Erstellen Sie für jede Benutzergruppe, die Zugriff auf einen spezifischen Ressourcenfeedsatz benötigt, Zuordnungen zwischen den Benutzern und den EquivalentFarmSets. Um das User-FarmMapping zu erstellen, rufen Sie Add-STFUserFarmMapping mit den folgenden Parametern auf:

   - `StoreService`: Storedienst, dem UserFarmMapping hinzugefügt werden soll.
   - `Name`: eindeutiger Name für die Zuordnung.

- `GroupMembers`: Hashtabelle mit den Namen und SIDs der Benutzergruppen, die Teil der Zuordnung sind. Der Name wird nur zur Anzeige verwendet; die SID definiert die Gruppe. Um alle Benutzer hinzuzufügen, erstellen Sie einen einzelnen Eintrag in der Hashtabelle mit dem Namen `Everyone` und dem Wert `Everyone`.
- `EquivalentFarmSet`: EquivalentFarmSet, das im vorherigen Schritt erstellt wurde.

Sie müssen sicherstellen, dass jeder Ressourcenfeed (Farm) in mindestens einer UserFarmMapping enthalten ist, da sonst keine Benutzer auf diese Ressourcen zugreifen können.

Multisiteaggregation

Standardmäßig werden in StoreFront alle Bereitstellungen, die Desktops und Anwendungen für einen Store bieten, aufgelistet und alle entsprechenden Ressourcen als separat behandelt. Wenn die gleiche Ressource aus mehreren Bereitstellungen verfügbar ist, sehen Benutzer daher ein Symbol für jede Ressource, was verwirrend sein kann, wenn die Ressourcen den gleichen Namen haben. Wenn Sie hoch verfügbare Multisitekonfigurationen einrichten, können Sie Citrix Virtual Apps and Desktops-Bereitstellungen, die den gleichen Desktop oder die gleiche Anwendung anbieten, so gruppieren, dass identische Ressourcen für Benutzer aggregiert werden können. Gruppierte Bereitstellungen müssen nicht identisch sein, aber Ressourcen müssen für die Aggregation den gleichen Namen und Pfad auf jedem Server haben.

Wenn bei Verwendung der Multisiteaggregation ein Desktop oder eine Anwendung aus mehreren, für einen bestimmten Store konfigurierten Citrix Virtual Apps and Desktops-Bereitstellungen verfügbar ist, werden alle Instanzen der Ressource in StoreFront aggregiert und den Benutzern wird ein einzelnes Symbol angezeigt. Wenn ein Benutzer eine aggregierte Ressource startet, bestimmt StoreFront die für den Benutzer am besten geeignete Instanz der Ressource auf der Grundlage der Serververfügbarkeit, der Tatsache, ob der Benutzer bereits eine aktive Sitzung hat, und der Reihenfolge, die Sie in der Konfiguration angegeben haben.

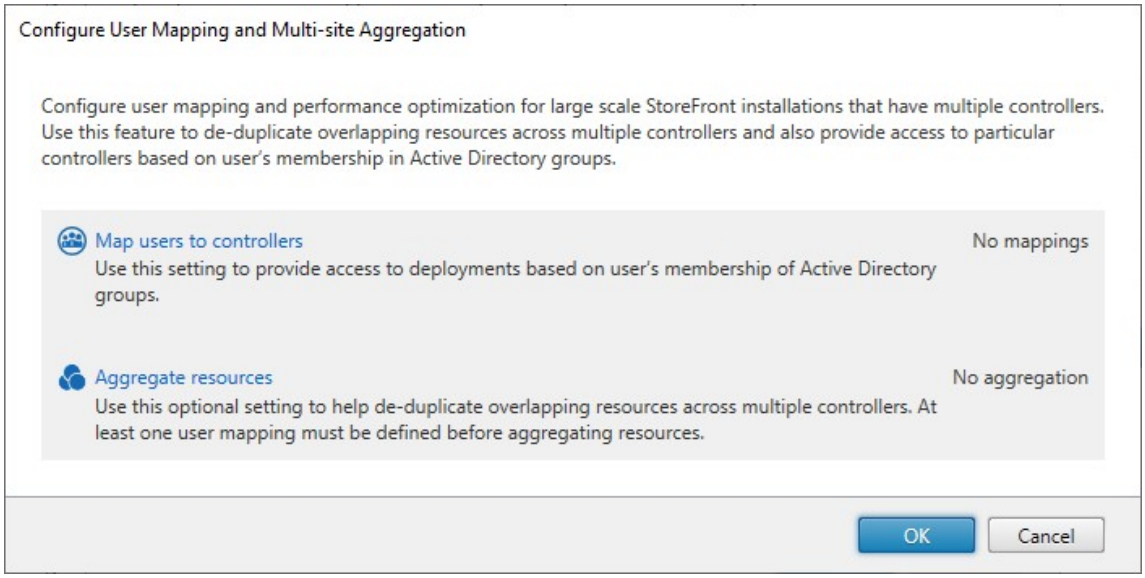
StoreFront überwacht dynamisch Server, die nicht auf Anforderungen reagieren, auf der Basis, dass solche Server entweder überlastet oder vorübergehend nicht verfügbar sind. Benutzer werden zu Ressourceninstanzen auf anderen Servern umgeleitet, bis die Kommunikation wiederhergestellt ist. Wenn die Server, auf denen die Ressourcen bereitgestellt werden, dies unterstützen, versucht StoreFront eine Wiederverwendung vorhandener Sitzungen, um zusätzliche Ressourcen zu liefern. Wenn ein Benutzer bereits eine aktive Sitzung auf einer Bereitstellung hat, die auch die angeforderte Ressource umfasst, verwendet StoreFront diese Sitzung, wenn sie mit der Ressource kompatibel ist. Durch Minimieren der Anzahl Sitzungen für jeden Benutzer wird die Zeit zum Starten zusätzlicher Desktops oder Anwendungen reduziert und ggf. eine effizientere Verwendung von Produktlizenzen ermöglicht.

Nach der Überprüfung auf Verfügbarkeit und vorhandene Benutzersitzungen verwendet StoreFront die in der Konfiguration angegebene Reihenfolge zur Bestimmung der Bereitstellung, mit der der Be-

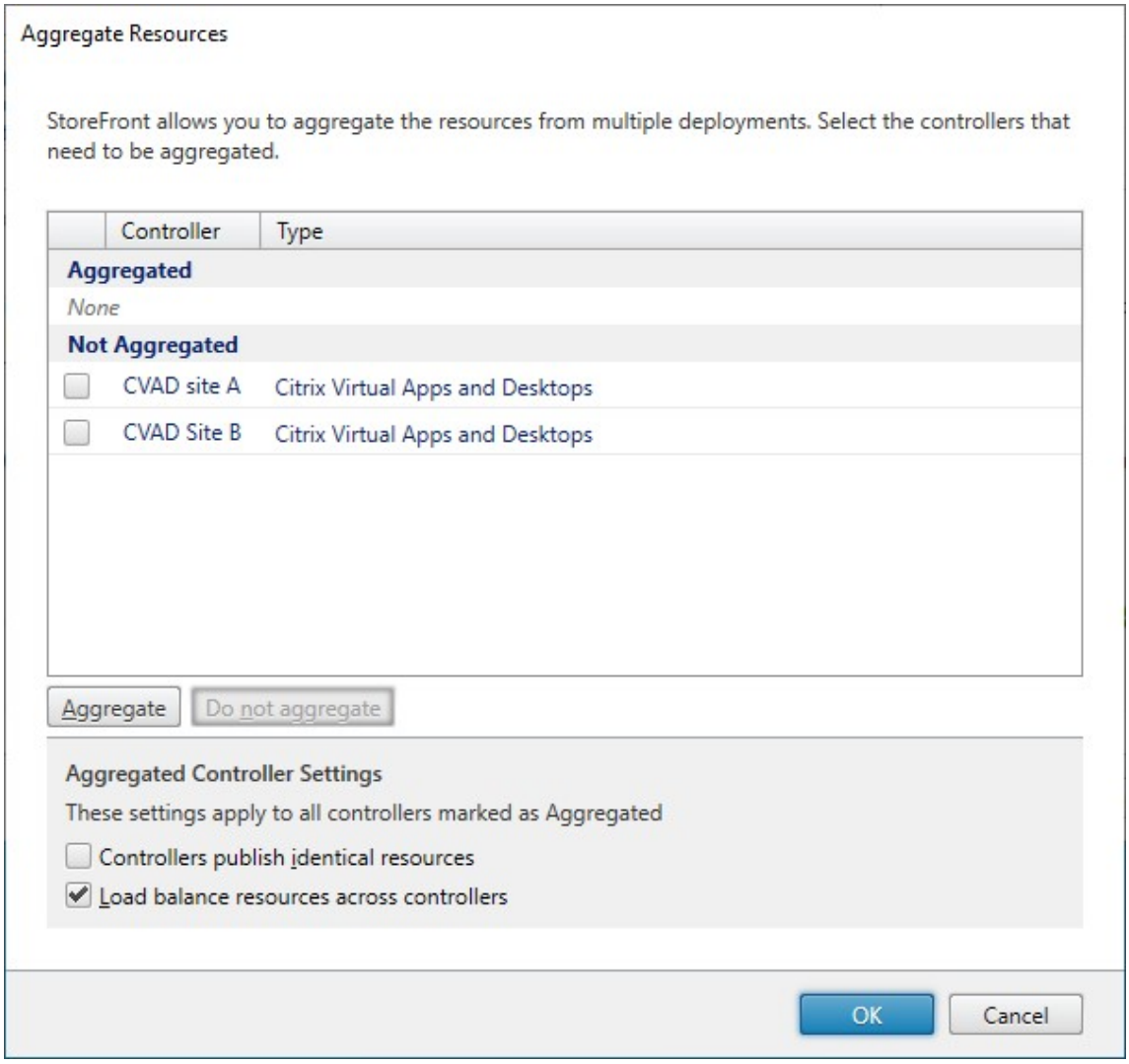
nutzer verbunden wird. Wenn dem Benutzer mehrere äquivalente Bereitstellungen zur Verfügung stehen, können Sie festlegen, dass eine Verbindung mit der ersten verfügbaren Bereitstellung oder per Zufallsprinzip mit einer beliebigen Bereitstellung in der Liste erfolgt. Die Verbindung von Benutzern mit der ersten verfügbaren Bereitstellung ermöglicht eine Minimierung der Anzahl der von den aktuellen Benutzern verwendeten Bereitstellungen. Die Verbindung per Zufallsprinzip erzielt eine gleichmäßigere Verteilung der Benutzer über alle verfügbaren Bereitstellungen.

Sie können die angegebene Reihenfolge der Bereitstellungen für einzelne Citrix Virtual Apps and Desktops-Ressourcen außer Kraft setzen und bevorzugte Bereitstellungen definieren, mit denen Benutzer bei Zugriff auf einen bestimmten Desktop oder eine bestimmte Anwendung verbunden werden. Damit können Sie z. B. festlegen, dass Benutzer bevorzugt mit einer speziell für einen bestimmten Desktop oder eine bestimmte Anwendung angepassten Bereitstellung verbunden werden, für andere Ressourcen jedoch andere Bereitstellungen verwenden. Fügen Sie zu diesem Zweck die Zeichenfolge `KEYWORDS:Primary` an die Beschreibung des Desktops oder der Anwendung in der bevorzugten Bereitstellung an und `KEYWORDS:Secondary` an die Ressource in anderen Bereitstellungen. Soweit möglich, werden Benutzer unabhängig von der Reihenfolge der Bereitstellungen in der Konfiguration mit der Bereitstellung mit der primären Ressource verbunden. Benutzer werden mit Bereitstellungen mit sekundären Ressourcen verbunden, wenn die bevorzugte Bereitstellung nicht verfügbar ist.

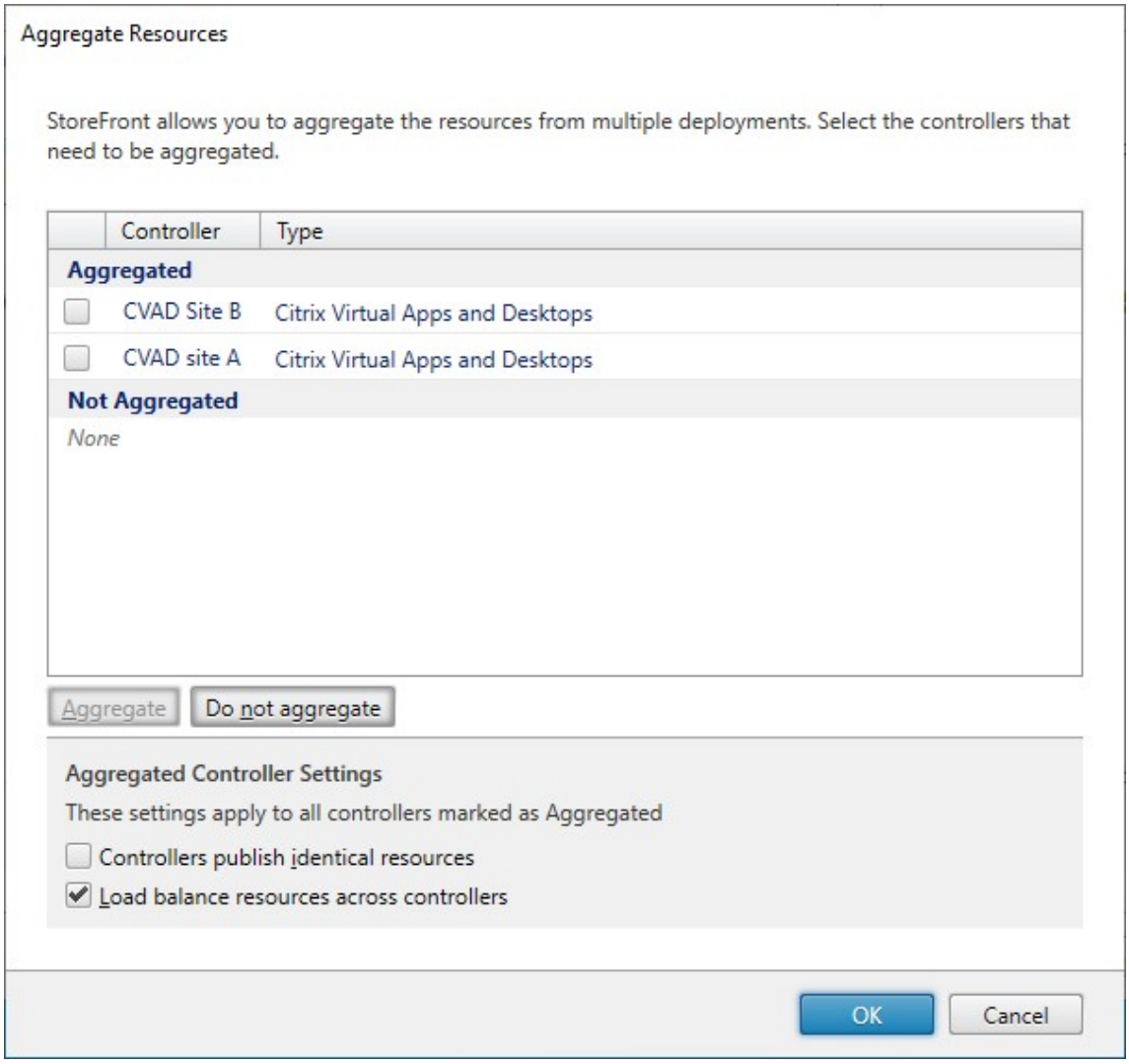
1. Klicken Sie im Fenster **Delivery Controller verwalten** unter **Benutzerzuordnung und Multi-siteaggregation konfigurieren** auf **Konfigurieren**. Diese Option ist nur verfügbar, wenn mindestens zwei Ressourcenfeeds konfiguriert sind.



2. Klicken Sie auf **Ressourcen aggregieren**. Dadurch wird das Fenster **Ressourcen aggregieren** geöffnet.



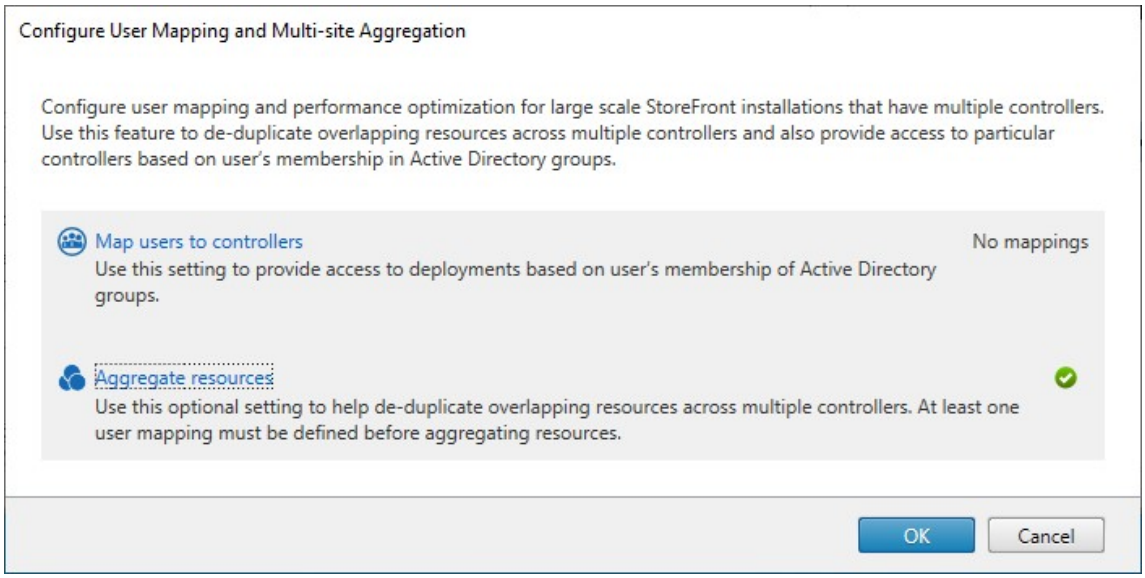
3. Wählen Sie die Ressourcenfeeds, die dieselben Ressourcen umfassen, und klicken Sie auf **Aggregieren**.



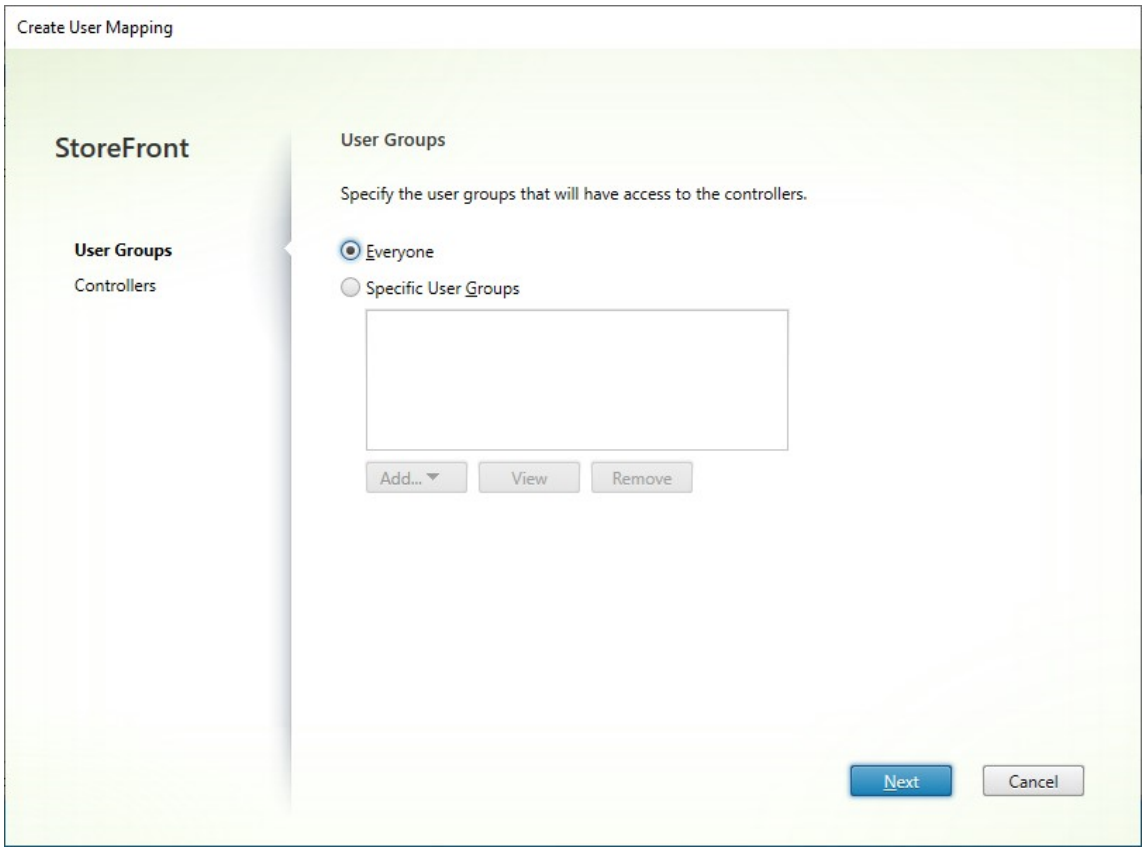
4. Wählen Sie nach Bedarf Optionen für **Aggregierte Controllereinstellungen** aus:

   - **Controller veröffentlichen identische Ressourcen** - Wenn aktiviert, enumeriert StoreFront nur die Ressourcen von einem der Controller in dem aggregierten Satz. Ist diese Option deaktiviert, enumeriert StoreFront die Ressourcen von allen Controllern im aggregierten Satz (sodass alle für den Benutzer verfügbaren Ressourcen angesammelt werden). Aktivieren dieser Option führt zu einer verbesserten Leistung beim Enumerieren der Ressourcen. Wir empfehlen sie aber nur, wenn Sie sind ganz sicher sind, dass die Ressourcenliste über alle aggregierten Ressourcen hinweg identisch ist.
   - **Lastausgleich für Ressourcen über Controller hinweg** - Wenn aktiviert, werden Starts gleichmäßig auf die verfügbaren Controller verteilt. Ist diese Option deaktiviert, werden Starts an den ersten Controller geleitet, der im Benutzerzuordnungsdialogfeld angegeben wurde. Es wird ein Failover auf weitere Controller durchgeführt, wenn der Start fehlschlägt.

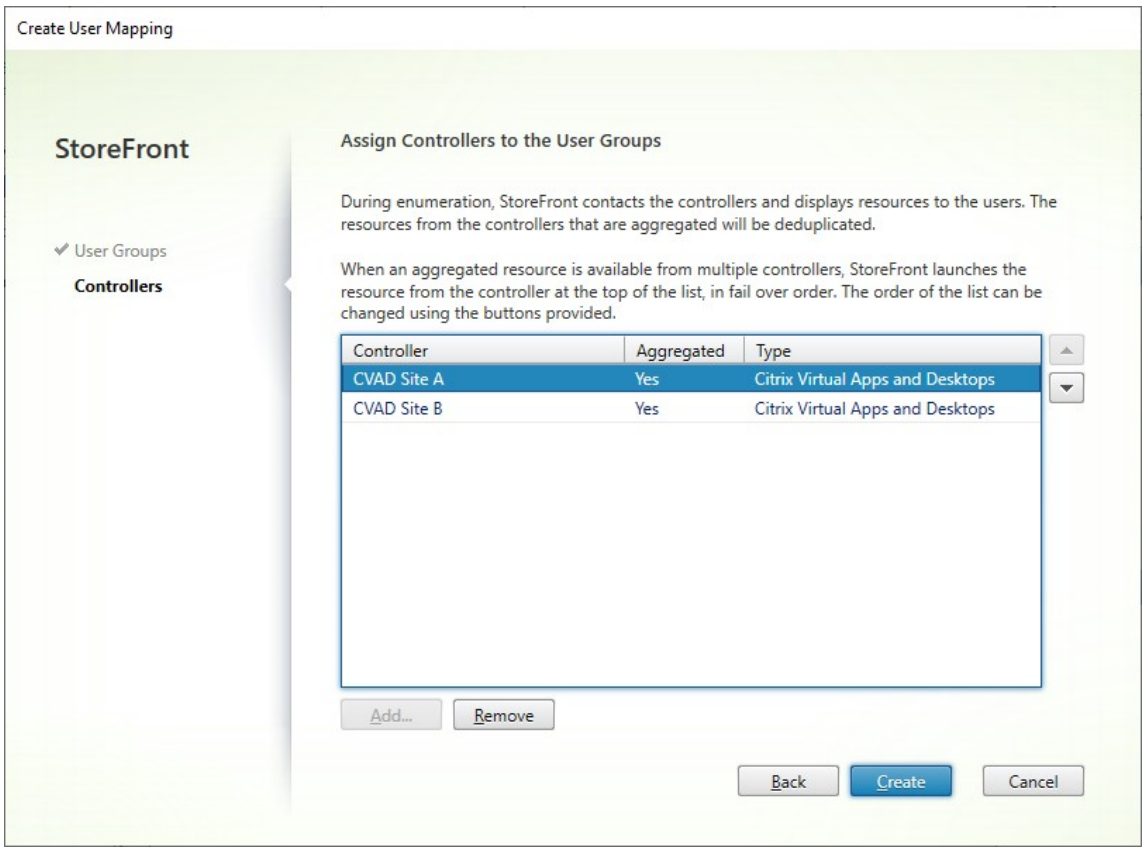
5. Klicken Sie auf **OK**, um zum Fenster **Benutzerzuordnung und Multisiteaggregation konfigurieren** zurückzukehren. **Ressourcen aggregieren** ist jetzt aktiviert.



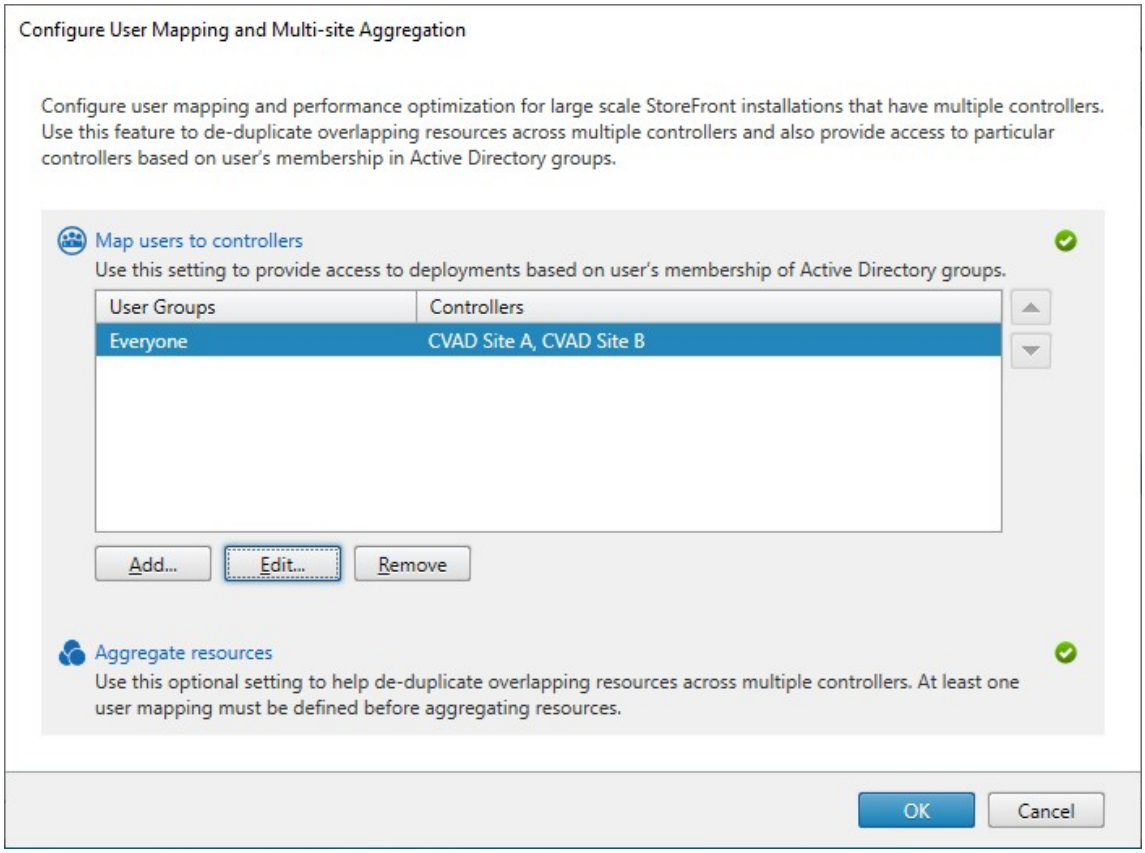
6. Wenn Ressourcen aggregiert wurden, haben standardmäßig keine Benutzer Zugriff auf die Ressourcen. Sie müssen also Benutzerzuordnungen hinzufügen. Klicken Sie auf **Benutzer Controllern zuordnen**. Dadurch wird das Fenster **Benutzerzuordnung erstellen** geöffnet.



7. Wählen Sie **Jeder** oder **Spezifische Benutzergruppen** und fügen Sie eine oder mehrere Gruppen hinzu. Beispiel: Auswahl einer Gruppe von Benutzern an einem bestimmten Standort.
8. Fügen Sie die aggregierten Ressourcenfeeds hinzu. Sie müssen alle aggregierten Ressourcenfeeds hinzufügen. Nicht hinzugefügte Ressourcenfeeds gelten als "Nicht aggregiert". Sie können auch nicht aggregierte Ressourcen einbeziehen.
9. Wenn Sie das Kontrollkästchen **Lastausgleich für Ressourcen über Controller hinweg** nicht aktiviert haben, können Sie die Reihenfolge auswählen, in der StoreFront Ressourcen starten soll.



10. Klicken Sie auf **Erstellen**, um zum Fenster **Benutzerzuordnung und Multisiteaggregation konfigurieren** zurückzukehren.



11. Fügen Sie nach Bedarf weitere Zuordnungen hinzu. Vergewissern Sie sich, dass jeder Ressourcenfeed einer Benutzergruppe zugeordnet ist, da nicht zugeordnete Ressourcen von niemandem verwendet werden können.
12. Klicken Sie auf **OK**.

Erweiterte Konfigurationen mit dem PowerShell-SDK

Sie können viele gängige Einstellungen für Multisitebereitstellungen und Hochverfügbarkeit mit der StoreFront-Verwaltungskonsole konfigurieren. Sie können StoreFront auch mit dem PowerShell-SDK konfigurieren, wodurch sich folgende zusätzliche Möglichkeiten bieten:

- Angeben mehrerer Gruppierungen von Bereitstellungen für die Aggregation.
  - Die Verwaltungskonsole lässt nur eine einzige Gruppierung von Bereitstellungen zu. Dies reicht in den meisten Fällen.
  - Für Stores mit vielen Bereitstellungen mit ungleichen Ressourcensätzen, verbessern mehrere Gruppierungen möglicherweise die Leistung.
- Angeben komplexer Prioritätsreihenfolgen für aggregierte Bereitstellungen. Die Verwaltungskonsole ermöglicht den Lastausgleich für aggregierte Bereitstellungen oder ein einzelne

Failoverliste. Mit PowerShell können Sie mehrere Gruppen von Feeds mit Lastenausgleich und Failover konfigurieren.

> **Warnung:**
>
> Nach der Konfiguration erweiterter Optionen für mehrere Sites mithilfe von PowerShell können die Optionen nicht über die Verwaltungskonsole geändert werden.

1. Entscheiden Sie, welche Aggregationsgruppen Sie verwenden möchten. In einer Aggregationsgruppe werden Anwendungen mit demselben Anzeigenamen zu einem Symbol zusammengefasst. Jede Aggregationsgruppe benötigt einen Namen. Mit der Verwaltungskonsole können Sie nur eine Aggregationsgruppe erstellen. Über PowerShell können Sie mehrere Aggregationsgruppen definieren.
2. Erstellen Sie für jede Aggregationsgruppe mindestens ein EquivalentFarmSet , in dem die Ressourcenfeeds (im SDK "farms") aufgeführt sind, die Sie aggregieren möchten. Wenn verschiedene Ressourcenfeeds der Aggregationsgruppe verschiedenen Benutzern zugewiesen werden, müssen Sie für jede dieser Benutzergruppen ein eigenes EquivalentFarmSet, erstellen, das den gleichen `AggregationGroupName` verwendet. Um das EquivalentFarmSet zu erstellen, rufen Sie New-STFEquivalentFarmset mit den folgenden Parametern auf:
   - `Name`: eindeutiger Name für das EquivalentFarmSet
   - `AggregationGroupName`: Name der Aggregationsgruppe, zu der das Farmset gehört.
   - `LoadBalanceMode`: `LoadBalanced` oder `Failover`.
   - `PrimaryFarms`: die Farmen, die Sie aggregieren möchten. Wenn `LoadBalanceMode` = `Failover` stellen Sie sicher, dass die Farmen in der erforderlichen Reihenfolge aufgeführt sind. Gibt es mehrere EquivalentFarmSets für eine Aggregationsgruppe, bestimmen diese Reihenfolge und die im UserFarmMapping definierte IndexNumber, welcher Ressourcenfeed zum Starten einer Ressource verwendet werden soll.
   - `BackupFarms`: Liste von Farmen, die verwendet werden können, falls keine der primären Farmen verfügbar ist. Diese Funktion ist veraltet. Fügen Sie stattdessen zusätzliche EquivalentFarmSets mit einer höheren IndexNumber hinzu.
3. Erstellen Sie für jeden Ressourcenfeed, der nicht Teil einer Aggregationsgruppe ist, ein EquivalentFarmSet, ohne Angaben von `AggregationGroupName`. Alle Ressourcenfeeds müssen Teil eines Farmsets sein. Rufen Sie New-STFEquivalentFarmset mit den folgenden Parametern auf:
   - `Name`: eindeutiger Name für das EquivalentFarmSet
   - `PrimaryFarms`: Name der nicht aggregierten Farm.
4. Erstellen Sie für jede Benutzergruppe, die Zugriff auf einen spezifischen Ressourcenfeedsatz benötigt, Zuordnungen zwischen den Benutzern und den EquivalentFarmSets. Um das User-

FarmMapping zu erstellen, rufen Sie Add-STFUserFarmMapping mit den folgenden Parametern auf:

- `StoreService`: Storedienst, dem UserFarmMapping hinzugefügt werden soll.
- `Name`: eindeutiger Name für die Zuordnung.
- `GroupMembers`: Hashtabelle mit den Namen und SIDs der Benutzergruppen, die Teil der Zuordnung sind. Der Name wird nur zur Anzeige verwendet; die SID definiert die Gruppe. Um alle Benutzer hinzuzufügen, erstellen Sie einen einzelnen Eintrag in der Hashtabelle mit dem Namen `Everyone` und dem Wert `Everyone`.
- `EquivalentFarmSet`: EquivalentFarmSet, das im vorherigen Schritt erstellt wurde.
- `IndexNumber`: Reihenfolge, in der Ressourcenfeeds ausgewertet werden. Dadurch wird die Reihenfolge festgelegt, in der Ressourcenfeeds zum Starten einer Ressource verwendet werden.

Sie müssen sicherstellen, dass jeder Ressourcenfeed (Farm) in mindestens einer UserFarmMapping enthalten ist, da sonst keine Benutzer auf diese Ressourcen zugreifen können.

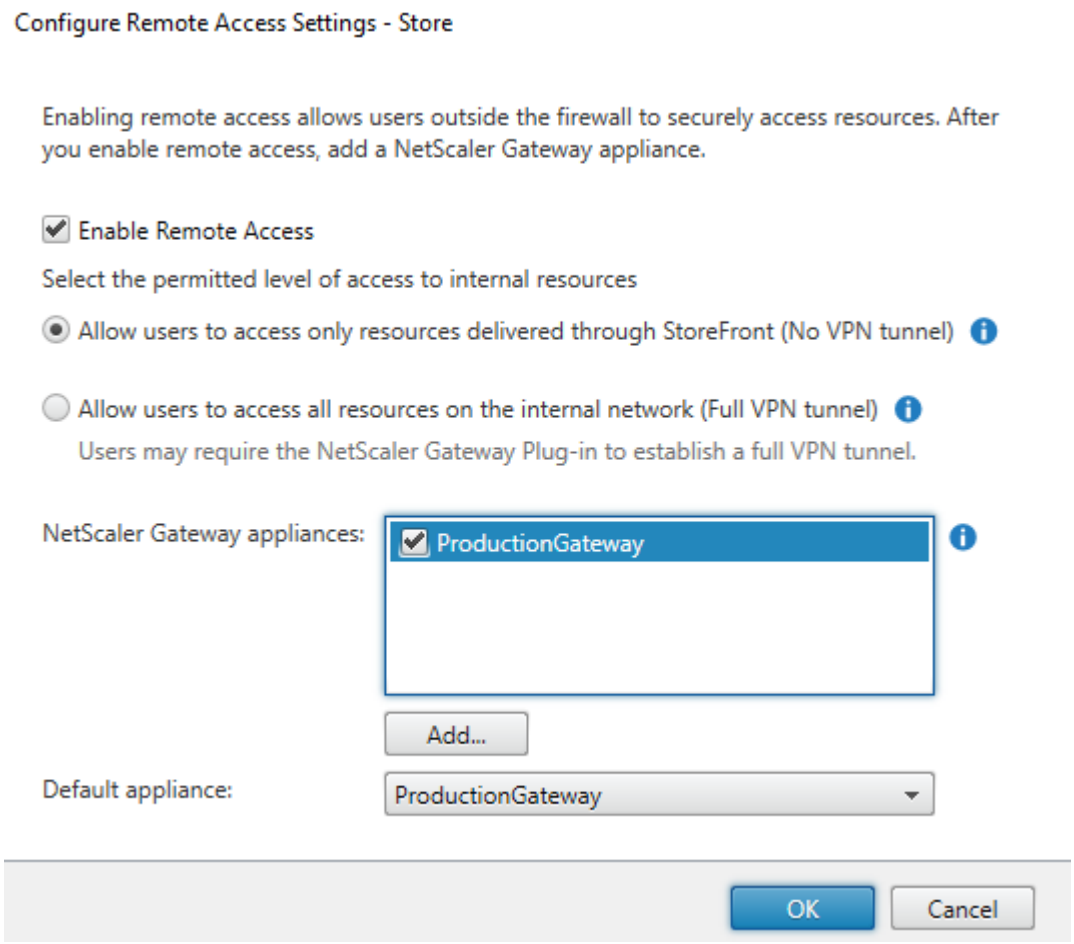
Remotezugriff auf Stores über Citrix Gateway verwalten

April 17, 2024

Mit der Aufgabe "Remotezugriffeinstellungen"können Sie den Zugriff auf Stores über Citrix Gateway für Benutzer in öffentlichen Netzwerken konfigurieren. Remotezugriff über Citrix Gateway ist nicht für Stores ohne Authentifizierung möglich.

> Wichtig:
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss
> übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Wählen Sie im rechten Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten "Stores" und im Ergebnisbereich einen Store aus. Klicken Sie im Aktionsbereich auf **Remotezugriffeinstellungen konfigurieren**.



2. Geben Sie im Dialogfeld "Remotezugriffeinstellungen konfigurieren"an, ob und wie Benutzer, die eine Verbindung von öffentlichen Netzwerken aus herstellen, über Citrix Gateway auf den Store zugreifen können.

   - Soll der Store Benutzern in öffentlichen Netzwerken nicht zur Verfügung stehen, deaktivieren Sie die Option **Remotezugriff aktivieren**. Nur lokale Benutzer im internen Netzwerk können dann auf den Store zugreifen.
   - Um den Remotezugriff zu ermöglichen, aktivieren Sie **Remotezugriff aktivieren**.
     - Wenn Sie Ressourcen, die über den Store angeboten werden, über Citrix Gateway verfügbar machen möchten, wählen Sie **Kein VPN-Tunnel** aus. Die Benutzer melden sich entweder über ICAProxy oder ein clientloses VPN (CVPN) bei Citrix Gateway an und benötigen das Citrix Gateway-Plug-In nicht für ein vollständiges VPN.
     - Wählen Sie **Vollständiger VPN-Tunnel** aus, um den Store und andere Ressourcen im internen Netzwerk über einen SSL-VPN-Tunnel (SSL = Secure Sockets Layer, VPN = virtuelles privates Netzwerk) verfügbar zu machen. Die Benutzer benötigen das Citrix Gateway-Plug-In für das Erstellen des VPN-Tunnels.

   Wenn Sie Remotezugriff auf den Store konfigurieren, wird automatisch die **Passthrough-**

Authentifizierung von Citrix Gateway aktiviert. Die Benutzer authentifizieren sich bei Citrix Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.

3. Wenn Sie Remotezugriff aktiviert haben, wählen Sie in der Liste **Citrix Gateway-Geräte** die Bereitstellungen aus, über die die Benutzer auf den Store zugreifen können. Die Liste enthält alle Bereitstellungen, die zuvor für diesen und andere Stores konfiguriert wurden. Wenn Sie weitere Bereitstellungen hinzufügen möchten, klicken Sie auf **Hinzufügen** und folgen Sie den Anweisungen unter Citrix Gateway hinzufügen.
4. Wenn Sie Zugriff über mehrere Geräte aktivieren, indem Sie mehr als einen Eintrag in der Liste auswählen, geben Sie das **Standardgerät** für den Zugriff auf den Store über die Citrix Workspace-App an.
5. Klicken Sie auf **OK**, um die Konfiguration zu speichern und das Dialogfeld "Remotezugriff konfigurieren"zu schließen.

Die Citrix Workspace-App verwendet Beacons, um zu ermitteln, ob Benutzer mit einem lokalen oder öffentlichen Netzwerk verbunden sind, und wählt daraufhin die richtige Zugriffsmethode aus. Weitere Informationen zum Ändern der Beacons finden Sie unter Konfigurieren von Beacons.

Standardmäßig verwendet StoreFront das Gateway, über das der Benutzer mit dem Store verbunden ist, um Ressourcen zu starten. Informationen zur Konfiguration von StoreFront zum Starten von Ressourcen mit einem anderen Gateway oder ohne Gateway finden Sie unter Optimales HDX-Routing.

Überprüfung von Zertifikatsperrlisten

April 17, 2024

Einführung

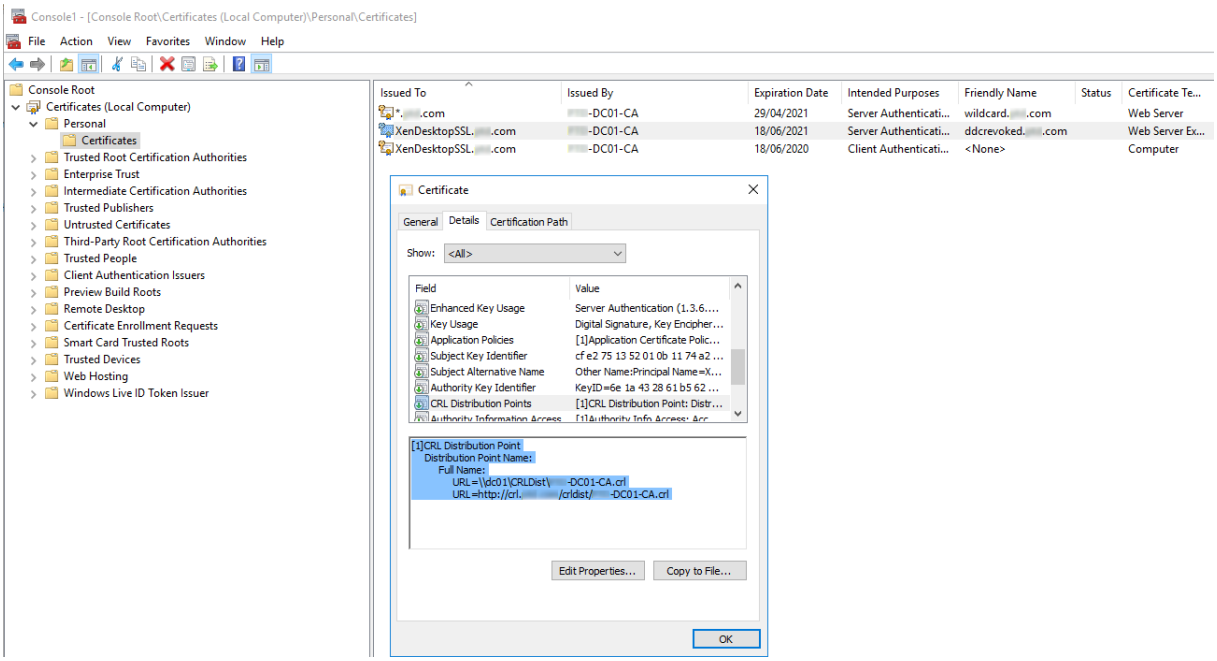
Sie können StoreFront so konfigurieren, dass der Status der von Citrix Virtual Apps and Desktops-Delivery Controllern verwendeten TLS-Zertifikate anhand einer veröffentlichten Zertifikatssperrliste überprüft wird. Sie müssen ggf. den Zugriff auf ein Zertifikat aus folgenden Gründen widerrufen:

- Sie vermuten, dass der private Schlüssel kompromittiert wurde.
- Die Zertifizierungsstelle wurde kompromittiert.
- Die Zugehörigkeit hat sich geändert.
- Das Zertifikat wurde ersetzt.

> **Hinweis:**
>
> Dieses Thema ist nur relevant, wenn zwischen StoreFront und Citrix Virtual Apps and Desktops-Delivery Controllern HTTPS-Verbindungen verwendet werden. HTTP-Verbindungen zu Delivery Controllern erfordern kein Zertifikat. Daher hat die hier beschriebene Einstellung -CertRevocationPolicy für den Store keine Auswirkungen.
>
> StoreFront unterstützt die Zertifikatsperrprüfung mithilfe von CDP-Erweiterungen und lokal installierten Zertifikatsperrlisten. StoreFront unterstützt keine Delta-Sperrlisten, sondern nur vollständige Zertifikatsperrlisten.

CDP-Erweiterungen

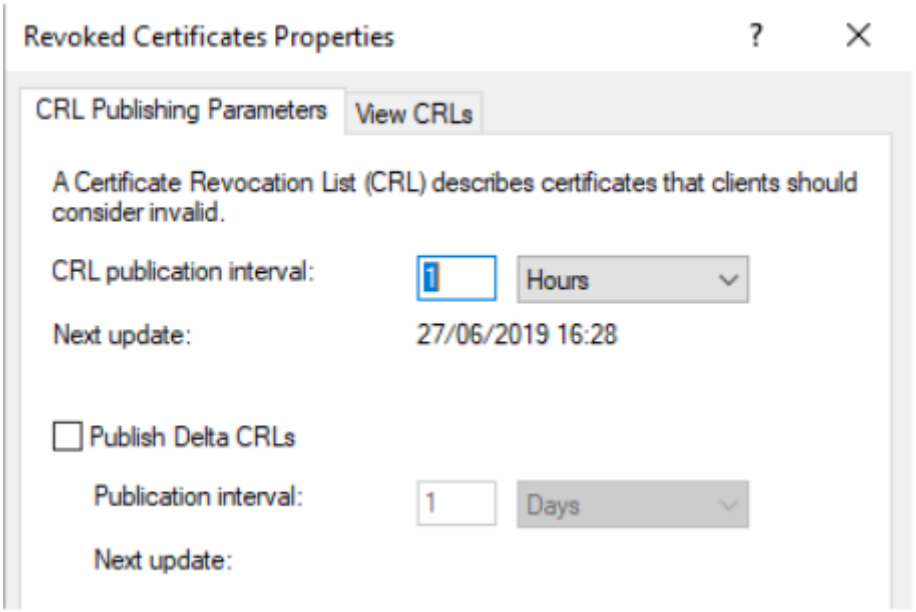
StoreFront listet keine Ressourcen von Citrix Virtual Apps and Desktops-Delivery Controllern auf, die gesperrte Zertifikate verwenden, deren Seriennummern in der veröffentlichten Zertifikatsperrliste aufgeführt sind. Um zu erkennen, welche Zertifikate gesperrt wurden, muss StoreFront über eine der in den CDP-Zertifikaterweiterungen definierten URLs auf die veröffentlichte Zertifikatsperrliste zugreifen können.



Zertifikatsperrlisten-Veröffentlichungsintervall

Damit StoreFront gesperrte Zertifikate auf Delivery Controllern schneller erkennt, verringern Sie das Veröffentlichungsintervall der Zertifizierungsstelle für die Zertifikatsperrliste. Legen Sie in

den Eigenschaften der CDP-Erweiterung einen niedrigeren, für Ihre PKI geeigneten Wert für das Zertifikatsperrlisten-Veröffentlichungsintervall fest.



Caching der Zertifikatsperrliste auf Clients

Der Windows-PKI-Client speichert Zertifikatsperrlisten lokal zwischen. Eine neue Zertifikatsperrliste wird erst heruntergeladen, wenn die lokal zwischengespeicherte abgelaufen ist.

StoreFront-Zugriff auf Zertifikatsperrlisten

Zur Überprüfung auf Zertifikatsperrungen muss StoreFront auf Zertifikatsperrlisten zugreifen können. Überlegen Sie, wie StoreFront den Webserver oder die Zertifizierungsstelle, die die Zertifikatsperrliste veröffentlicht, kontaktieren soll und wie StoreFront Zertifikatsperrlistenupdates erhalten soll.

Interne Unternehmenszertifizierungsstellen und private Zertifikate auf Delivery Controllern
Zur Verwendung privater Zertifizierungsstellen und Zertifikate benötigt StoreFront eine ordnungsgemäß konfigurierte Unternehmenszertifizierungsstelle und eine veröffentlichte Zertifikatsperrliste, auf die es innerhalb der Organisation im internen Netzwerk zugreifen kann. Informationen zum Konfigurieren einer Unternehmenszertifizierungsstelle zum Veröffentlichen von CDP-Erweiterungen finden Sie in der Microsoft-Dokumentation. Zertifikate auf Delivery Controllern, die vorhanden waren, bevor die Zertifizierungsstelle für
CDP-Erweiterungen konfiguriert wurde, müssen möglicherweise neu ausgestellt werden.

StoreFront- und Citrix Virtual Apps and Desktops-Server sind normalerweise in isolierten privaten Netzwerken ohne Zugriff auf das Internet. In einem solchen Szenario sollten private Zertifizierungsstellen

verwendet werden.

Externe öffentliche Zertifizierungsstellen und öffentliche Zertifikate auf Delivery Controllern
StoreFront-Server und Citrix Virtual Apps and Desktops-Delivery Controller können Zertifikate verwenden, die von öffentlichen Zertifizierungsstellen ausgestellt wurden. StoreFront muss Zugang zu dem Webserver der öffentlichen Zertifizierungsstelle über das Internet unter Verwendung der in den CDP-Erweiterungen referenzierten URLs haben. Wenn StoreFront keine Kopie der Zertifikatsperrliste anhand einer CDP-URL herunterladen kann, nachdem ein öffentliches Zertifikat gesperrt wurde, kann StoreFront die Zertifikatsperrprüfung nicht durchführen.

Einstellungen der Richtlinie "Zertifikatsperrüberprüfung"

Verwenden Sie die Citrix StoreFront-PowerShell-Cmdlets **Get-STFStoreFarmConfiguration** und **Set-STFStoreFarmConfiguration** zum Festlegen der Richtlinie "Zertifikatsperrüberprüfung"für einen Store. Mit **Get-Help Set-STFStoreFarmConfiguration -detailed** werden die PowerShell-Hilfe und Beispiele mit der Option -CertRevocationPolicy angezeigt. Weitere Informationen über diese StoreFront PowerShell-Cmdlets finden Sie unter Citrix StoreFront SDK PowerShell Modules.

Die Option **-CertRevocationPolicy** kann auf die folgenden Werte eingestellt werden:

Einstellung	Beschreibung
NoCheck	StoreFront überprüft das Zertifikat auf dem Delivery Controller nicht auf seinen Sperrstatus. StoreFront listet weiterhin Ressourcen von Delivery Controllern auf, die gesperrte Zertifikate verwenden. Dies ist die Standardeinstellung.

Einstellung	Beschreibung
MustCheck	Dies ist die sicherste Option. StoreFront versucht, eine Zertifikatsperrliste abzurufen, indem es die URLs aufruft, auf die in den CDP-Erweiterungen des Zertifikats auf dem Delivery Controller verwiesen wird. StoreFront kann nichts von dem Delivery Controller auflisten, wenn die Zertifikatsperrliste nicht verfügbar ist oder das auf dem Delivery Controller verwendete Zertifikat gesperrt ist. Die URL kann auf einen internen Webserver verweisen, wenn das Zertifikat privat ist, oder auf einen öffentlichen Internet-Webserver, wenn das Zertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt wurde.
FullCheck	StoreFront versucht die URLs aufzurufen, die in den CDP-Erweiterungen des Zertifikats auf dem Delivery Controller veröffentlicht sind. Kann StoreFront keine Kopie der Zertifikatsperrliste von den URLs abrufen, gestattet es weiterhin die Auflistung der Ressourcen von dem Delivery Controller. Ruft StoreFront die Zertifikatsperrliste erfolgreich ab und wurde das Zertifikat des Delivery Controllers gesperrt, listet StoreFront keine Ressourcen auf. Die URL kann auf einen internen Webserver verweisen, wenn das Zertifikat privat ist, oder auf einen öffentlichen Internet-Webserver, wenn das Zertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt wurde.

Einstellung	Beschreibung
NoNetworkAccess	Es werden nur Zertifikatsperrlisten geprüft, die lokal in den Citrix Delivery Controller-Zertifikatspeicher auf dem StoreFront-Server importiert wurden. StoreFront versucht nicht, die in den CDP-Erweiterungen angegebenen URLs aufzurufen. Kann StoreFront keine lokale Kopie der Zertifikatsperrliste abrufen, gestattet es weiterhin die Auflistung der Ressourcen von dem Delivery Controller. Ruft StoreFront die lokale Zertifikatsperrliste erfolgreich aus dem Citrix Delivery Controller-Zertifikatspeicher ab und wurde das Zertifikat des Delivery Controllers gesperrt, listet StoreFront keine Ressourcen auf.

Konfigurieren eines Stores für die Überprüfung der Zertifikatsperrlisten

Um die Richtlinie "Zertifikatsperrüberprüfung"für einen Store festzulegen, öffnen Sie die PowerShell ISE mit dem Befehl **Als Administrator ausführen** und führen Sie dann die folgenden PowerShell-Cmdlets aus. Wenn Sie mehrere Stores haben, wiederholen Sie diesen Vorgang für alle. -CertRevocationPolicy ist eine Einstellung auf Storeebene, die sich auf alle Delivery Controller auswirkt, die für den in $StoreVirtualPath angegebenen Store konfiguriert wurden.

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath
Set-STFStoreFarmConfiguration -StoreService $StoreObject -
    CertRevocationPolicy "MustCheck"
<!--NeedCopy-->
```

Führen Sie folgenden Befehl aus, um zu überprüfen, ob die Einstellung richtig angewendet wurde oder um die aktuelle
-CertRevocationPolicy-Konfiguration anzuzeigen:

```
(Get-STFStoreFarmConfiguration -StoreService $StoreObject).
    CertRevocationPolicy
<!--NeedCopy-->
```


Verwenden lokal importierter Zertifikatsperrlisten auf dem StoreFront-Server

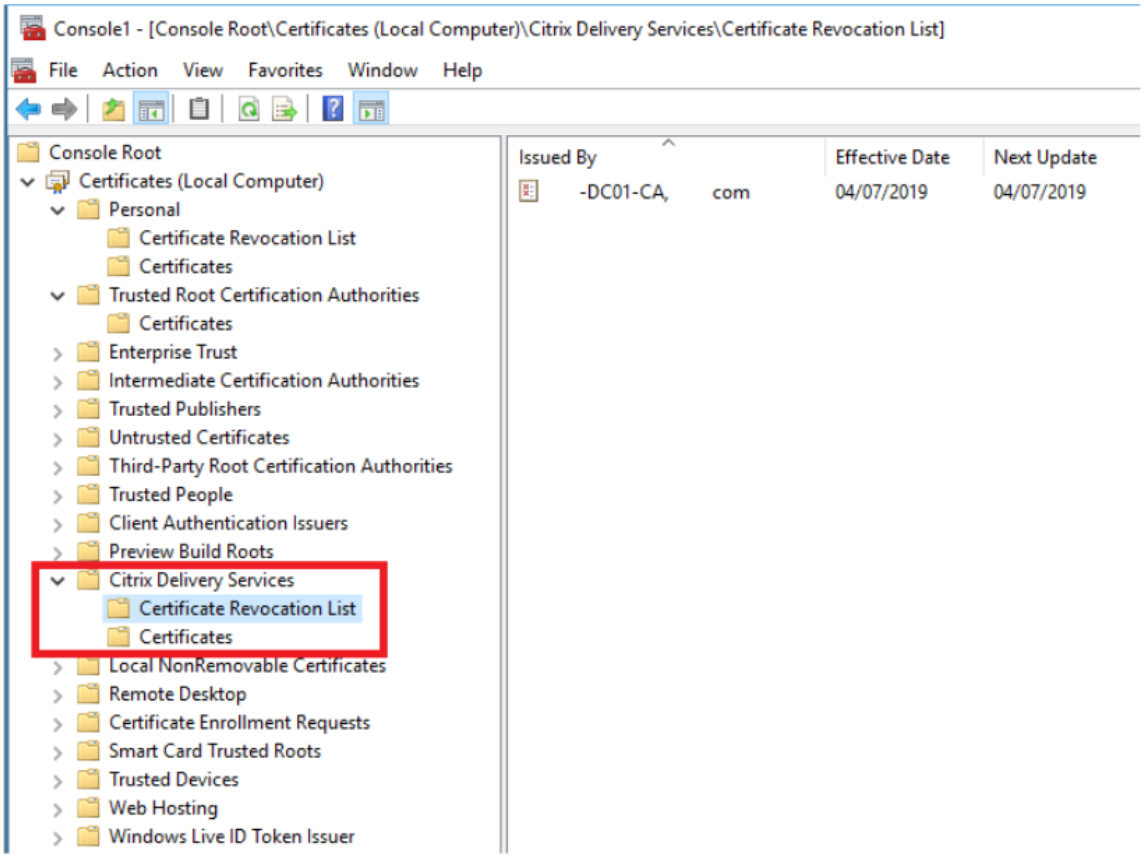
Die Verwendung lokal importierter Zertifikatsperrlisten wird unterstützt, von Citrix jedoch aus folgenden
Gründen nicht empfohlen:

- Die Verwaltung und Aktualisierung ist in großen Bereitstellungen schwierig, in denen möglicherweise mehrere StoreFront-Servergruppen vorliegen.
- Das manuelle Aktualisieren von Zertifikatsperrlisten auf jedem StoreFront-Server bei jeder Sperrung eines Zertifikats ist viel weniger effizient als die Verwendung von CDP-Erweiterungen und veröffentlichten Zertifikatsperrlisten in der gesamten Active Directory-Domäne.

Lokal installierte oder aktualisierte Zertifikatsperrlisten können verwendet werden, wenn -CertRevocationPolicy auf "NoNetworkAccess"festgelegt ist und Sie die Zertifikatsperrliste effizient an alle StoreFront-Server verteilen können.

Verwenden lokal importierter Zertifikatsperrlisten

1. Kopieren Sie die Zertifikatsperrliste auf den Desktop des StoreFront-Servers. Wenn der StoreFront-Server Teil einer Servergruppe ist, kopieren Sie sie auf alle Server in der Gruppe.
2. Öffnen Sie das MMC-Snap-In und wählen Sie **Datei > Snap-In hinzufügen/entfernen > Zertifikate > Computerkonto > Citrix Delivery Services certificate store**.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Alle Tasks > Importieren**, gehen Sie zur Zertifikatsperrlistendatei und wählen Sie **Alle Dateien auswählen > Öffnen > Alle Zertifikate in folgendem Speicher speichern > Citrix Delivery Services**.



Hinzufügen der Zertifikatsperrliste zum Citrix Delivery Services-Zertifikatspeicher per PowerShell oder Befehlszeile

1. Melden Sie sich bei StoreFront an und kopieren Sie die Zertifikatsperrlistendatei auf den Desktop des aktuellen
   Benutzers.
2. Öffnen Sie die PowerShell ISE und wählen Sie **Als Administrator ausführen**.
3. Führen Sie folgenden Befehl aus:

```
certutil -addstore "Citrix Delivery Services" "$env:UserProfile\
    Desktop\Example-DC01-CA.crl"
```

Bei Erfolg wird Folgendes zurückgegeben:

```
Citrix Delivery Services
CRL "CN=Example-DC01-CA, DC=example, DC=com" added to store.
CertUtil: -addstore command completed successfully.
```

Sie können diesen Befehl als Grundlage verwenden, um die Zertifikatsperrliste automatisch per Skript an alle
StoreFront-Server in Ihrer Bereitstellung zu verteilen.

XML-Authentifizierung mit Delivery Controllern

Sie können StoreFront so konfigurieren, dass die Benutzerauthentifizierung an Citrix Virtual Apps and Desktops-Delivery Controller delegiert wird. Die Benutzer werden daran gehindert, sich bei StoreFront anzumelden, wenn das Zertifikat auf dem Delivery Controller gesperrt wurde. Dieses Verhalten ist wünschenswert, da Active Directory-Benutzer sich nicht bei StoreFront anmelden können sollten, wenn das Zertifikat auf dem Citrix Virtual Apps and Desktops-Delivery Controller, das für ihre Authentifizierung verantwortlich ist, gesperrt wurde.

Delegieren der Benutzerauthentifizierung an Delivery Controller

1. Konfigurieren Sie den Store für die Zertifikatsperrung, wie im vorherigen Abschnitt Konfigurieren eines Stores für die Überprüfung der Zertifikatsperrlisten beschrieben.
2. Konfigurieren Sie den Delivery Controller für die Verwendung von HTTPS, wie im Verfahren Authentifizierung auf Basis des XML-Diensts beschrieben.

Konfigurieren des XML-Authentifizierungsdiensts für die Überprüfung der Zertifikatsperrlisten

Diese Schritte sind nur erforderlich, wenn Sie XML-Authentifizierung in Ihrer Bereitstellung verwenden.

> **Hinweis:**
>
> StoreFront unterstützt zwei Modelle zum Zuordnen von Stores zu einem Authentifizierungsdienst. Der empfohlene Ansatz ist die Eins-zu-Eins-Zuordnung zwischen Store und Authentifizierungsdienst. In diesem Fall müssen Sie die Schritte in diesem Abschnitt für alle Stores und zugehörigen Authentifizierungsdienste ausführen.
>
> Stellen Sie sicher, dass Sie den Zertifikatsperrmodus für Store und Authentifizierungsdienst auf denselben Wert festlegen. Ist die Authentifizierungskonfiguration für alle Stores identisch, können mehrere Stores zur gemeinsamen Verwendung eines einzelnen Authentifizierungsdiensts konfiguriert werden.

Die PowerShell-Cmdlets für Authentifizierungsdienste besitzen kein Äquivalent zu **Set-STFStoreFarmConfiguratio** Daher ist ein etwas anderer PowerShell-Ansatz erforderlich. Verwenden Sie dieselben Richtlinieneinstellungen für die Zertifikatsperre, die im vorherigen Abschnitt beschrieben wurden.

1. Öffnen Sie die PowerShell ISE und wählen Sie **Als Administrator ausführen**.

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
```



```
$AuthVirtualPath = "/Citrix/StoreAuth"
<!--NeedCopy-->
```

2. Wählen Sie den Storedienst, den Authentifizierungsdienst und den Delivery Controller für die XML-Authentifizierung aus. Stellen Sie sicher, dass der Delivery Controller bereits für den Store konfiguriert ist.

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
    $StoreVirtualPath
$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -
    FarmName "CVAD"
$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -
    VirtualPath $AuthVirtualPath
<!--NeedCopy-->
```

3. Ändern Sie direkt die CertRevocationPolicy-Eigenschaft des Authentifizierungsdiensts.

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"
$AuthObject.Save()
Enable-STFXmlServiceAuthentication -AuthenticationService
    $AuthObject -Farm $FarmObject
<!--NeedCopy-->
```

4. Prüfen Sie, ob Sie den richtigen Zertifikatsperrmodus festgelegt haben.

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
    $AuthVirtualPath
$AuthObject.FarmsConfiguration.CertRevocationPolicy
<!--NeedCopy-->
```

Erwartungsgemäße Fehler in der Windows-Ereignisanzeige

Wenn die Zertifikatsperrlisten-Überprüfung aktiviert ist, werden Fehler in der Windows-Ereignisanzeige auf dem StoreFront-Server gemeldet.

Öffnen der Ereignisanzeige:

- Geben Sie auf dem StoreFront-Server **run** ein.
- Geben Sie **eventvwr** ein und drücken Sie die Eingabetaste.
- Suchen Sie unter “Anwendungen und Dienste”nach Citrix Delivery Services-Ereignissen.

Beispiel: Store cannot contact a delivery controller with a revoked certificate

```
An SSL connection could not be established: An error occurred during
    SSL crytography: Access is denied.

```



```
This message was reported from the Citrix XML Service at address https://deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.

The specified Citrix XML Service could not be contacted and has been temporarily removed from the list of active services.
<!--NeedCopy-->
```

Beispiel für einen Fehler von Receiver für Web, wenn sich ein Benutzer aufgrund fehlgeschlagener XML-Authentifizierung nicht anmelden kann

```
An unexpected response was received during the authentication process.

Citrix.DeliveryServicesClients.Authentication.Exceptions.ExplicitAuthenticationFailure,
Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
Culture=neutral, PublicKeyToken=null

General Authentication Failure

ExplicitResult.State: 5

AuthenticationControllerRequestUrl:
https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/LoginAttempt

ActionType: LoginAttempt

at
Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.GetExplicitAuthResult(ActionType
type, Dictionary`2 postParams)
<!--NeedCopy-->
```

Zwei StoreFront-Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers konfigurieren

September 27, 2023

Bei der StoreFront-Installation wird lokal auf jedem StoreFront-Server ein Windows-Datenspeicher für die Abonnementdaten installiert. In Umgebungen mit StoreFront-Servergruppen hat jeder Server zudem eine Kopie der Abonnementdaten des Stores. Diese Daten werden an andere Servern verteilt, damit Benutzerabonnements gruppenweit gepflegt werden. Standardmäßig erstellt StoreFront einen Datenspeicher für jeden Store. Jeder Abonnementdatenspeicher wird separat aktualisiert.

Wenn unterschiedliche Konfigurationseinstellungen erforderlich sind, konfigurieren Administratoren StoreFront häufig mit zwei separaten Stores: einem für den externen Zugriff auf Ressourcen über Citrix Gateway und einem für den internen Zugriff über das Unternehmens-LAN. Sie können den externen und den internen Store so konfigurieren, dass beide einen Abonnementdatenspeicher gemeinsam nutzen, indem Sie eine einfache Änderung an der Datei web.config des Stores vornehmen.

Im Standardszenario mit zwei Stores und den entsprechenden Abonnementdatenspeichern muss ein Benutzer dieselbe Ressource zweimal abonnieren. Das Konfigurieren der beiden Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers verbessert und vereinfacht die Roamingerfahrung beim Zugriff auf die gleiche Ressource von innerhalb und außerhalb des Unternehmensnetzwerks. Bei einem gemeinsam genutzten Abonnementdatenspeicher ist es egal, ob der Benutzer beim ersten Abonnement einer neuen Ressource extern oder intern auf sie zugreift.

- Jeder Store hat eine web.config-Datei in C:\inetpub\wwwroot\citrix<storename>.
- Jede web.config-Datei hat einen Clientendpunkt für den Abonnementstoredienst.

```
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
__Citrix_<StoreName>"authenticationMode="windows"transferMode="
Streamed">
```

Die Abonnementdaten für jeden Store sind in:

```
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\
SubscriptionsStore\1__Citrix_<StoreName>
```

Damit zwei Stores einen Abonnementdatenspeicher verwenden, müssen Sie nur einen Store auf den Abonnementdienst-Endpunkt des anderen Speichers verweisen. Bei einer Servergruppenbereitstellung sind für alle Server identische Storepaare und identische Kopien von deren gemeinsam genutzten Datenspeichern definiert.

> Hinweis:
>
> Die für die einzelnen Stores konfigurierten Citrix Virtual Apps and Desktops-Controller müssen genau übereinstimmen, da ansonsten u. U. ein inkonsistenter Satz Ressourcenabonnements zwischen Stores auftritt. Die gemeinsame Datenspeichernutzung wird nur unterstützt, wenn die beiden Stores auf demselben StoreFront-Server bzw. in derselben Servergruppenbereitstellung residieren.

Endpunkte der StoreFront-Abonnementdatenspeicher

1. Öffnen Sie bei einer einzelnen StoreFront-Bereitstellung die externe Store-web.config-Datei in Editor und suchen Sie “clientEndpoint”. Beispiel:

```
1 <subscriptionsStoreClient enabled="true">
```



```
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_External" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
<!--NeedCopy-->
```

2. Ändern Sie extern so, dass es dem internen Storeendpunkt entspricht:

```
<subscriptionsStoreClient enabled="true">
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_Internal" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
<!--NeedCopy-->
```

3. Wenn Sie eine StoreFront-Servergruppe verwenden, übertragen Sie die an der Datei web.config des primären Knotens vorgenommenen Änderungen auf alle anderen Knoten.

Beide Stores verwenden nun den internen Abonnementdatenspeicher gemeinsam.

Favoriten für einen Store verwalten

May 31, 2024

Sie können Abonnementdaten (Favoriten) für einen Store mithilfe von PowerShell-Cmdlets verwalten.

> **Hinweis:**
>
> Verwenden Sie entweder die StoreFront-Verwaltungskonsole oder PowerShell zum Verwalten von StoreFront. Verwenden Sie nicht beide Methoden zur gleichen Zeit. Schließen Sie immer erst die StoreFront-Verwaltungskonsole, bevor Sie PowerShell zum Ändern der StoreFront-Konfiguration öffnen. Citrix empfiehlt zudem, ein Backup aller Abonnementdaten zu erstellen, bevor Sie Änderungen vornehmen, damit bei Bedarf ein Rollback auf einen früheren Zustand möglich ist.

Löschen von Abonnementdaten

Für jeden Store in der Bereitstellung gibt es einen Ordner und Datenspeicher mit den Abonnementdaten.

1. Halten Sie den Citrix Abonnementstoredienst auf dem StoreFront-Server an. Solange der Citrix Abonnementstoredienst ausgeführt wird, können keine Abonnementdaten für einen Store gelöscht werden.
2. Navigieren Sie auf jedem StoreFront-Server zum Abonnementstoreordner: `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>`
3. Löschen Sie den Inhalt des Ordners für den Abonnementstore, jedoch nicht den Ordner selbst.
4. Starten Sie den Citrix Abonnementstoredienst auf dem StoreFront-Server neu.

In StoreFront 3.5 oder höher können Sie mit dem folgenden PowerShell-Skript Abonnementdaten für einen Store löschen. Zum Ausführen dieser PowerShell-Funktion benötigen Sie Administratorrechte zum Beenden oder Starten von Diensten und zum Löschen von Dateien. Diese PowerShell-Funktion führt zum selben Ergebnis wie die oben beschriebene manuelle Schrittfolge.

Um die Cmdlets erfolgreich auszuführen, muss der Citrix Abonnementstoredienst auf dem Server ausgeführt werden.

```
function Remove-SubscriptionData
{

    [CmdletBinding()]

    [Parameter(Mandatory=$False)][String]$Store = "Store"

    $SubsService = "Citrix Subscriptions Store"

    # Path to Subscription Data in StoreFront version 2.6 or later

    $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\
       Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store*"

    Stop-Service -displayname $SubsService

    Remove-Item $SubsPath -Force -Verbose

    Start-Service -displayname $SubsService

    Get-Service -displayname $SubsService
 }


Remove-SubscriptionData -Store "YourStore"
<!--NeedCopy-->
```

Exportieren von Abonnementdaten

Mit dem folgenden PowerShell-Cmdlet können Sie Storeabonnementdaten in einer tabulatorgetrennten TXT-Backupdatei sichern.


```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"

Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
    :USERPROFILE\Desktop\Subscriptions.txt"
```

In einer Multiserverbereitstellung können Sie dieses PowerShell-Cmdlet auf einem beliebigen Server in der StoreFront-Servergruppe ausführen. Auf jedem Server in der Servergruppe ist eine identische synchronisierte Kopie der Abonnementdaten aller Peers gespeichert. Bei eventuellen Problemen mit der Abonnementsynchronisierung zwischen StoreFront-Servern können Sie die Daten aller Server in der Gruppe exportieren und auf Unterschiede überprüfen.

Wiederherstellen von Abonnementdaten

Mit Restore-STFStoreSubscriptions können Sie vorhandene Abonnementdaten überschreiben. Sie können die Abonnementdaten eines Stores mit der tabulatorgetrennten TXT-Backupdatei wiederherstellen, die Sie zuvor mit Export-STFStoreSubscriptions erstellt haben.

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "
    $env:USERPROFILE\Desktop\Subscriptions.txt"
<!--NeedCopy-->
```

Weitere Informationen zu Restore-STFStoreSubscriptions finden Sie unter https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2203/Restore-STFStoreSubscriptions/

Wiederherstellen von Daten auf einem einzelnen StoreFront-Server

In einer Einzelserverbereitstellung ist nicht erforderlich, den Abonnementstoredienst herunterzufahren. Sie müssen auch nicht die vorhandenen Abonnementdaten löschen, bevor Sie die Abonnementdaten wiederherstellen.

Wiederherstellen von Daten in einer StoreFront-Servergruppe

Zum Wiederherstellen von Abonnementdaten in einer Servergruppe sind folgende Schritte erforderlich.

Beispiel einer Servergruppenbereitstellung mit drei StoreFront-Servern.

- StoreFrontA
- StoreFrontB
- StoreFrontC

1. Erstellen Sie ein Backup der vorhandenen Abonnementdaten von einem der drei Server.
2. Beenden Sie den Abonnementstoredienst auf den Servern StoreFrontB und C, damit diese Server während der Aktualisierung von StoreFrontA keine Abonnementdaten senden oder empfangen.
3. Löschen Sie die Abonnementdaten der Server StoreFrontB und C, um Unterschiede zu den wiederhergestellten Abonnementdaten zu vermeiden.
4. Stellen Sie die Daten auf StoreFrontA mit dem Cmdlet **Restore-STFStoreSubscriptions** wieder her. Hierfür ist es nicht erforderlich, den Abonnementstoredienst anzuhalten oder Abonnementdaten auf StoreFrontA zu löschen, da diese beim Wiederherstellen überschrieben werden.
5. Starten Sie den Abonnementstoredienst auf den Servern StoreFrontB und StoreFrontC neu. Die Server können dann eine Kopie der Daten von StoreFrontA erhalten.
6. Warten Sie, bis die Synchronisierung zwischen allen Servern erfolgt. Die erforderliche Zeit hängt von der Anzahl der Datensätze auf StoreFrontA ab. Wenn alle Server in einem lokalen Netzwerk sind, geschieht die Synchronisierung normalerweise schnell. Die Synchronisierung von Abonnements über eine WAN-Verbindung kann länger dauern.
7. Exportieren Sie die Daten von StoreFrontB und C, um den Abschluss der Synchronisierung zu bestätigen oder die Gesamtanzahl an Storeabonnements anzuzeigen.

Importieren von Abonnementdaten

Verwenden Sie **Import-STFStoreSubscriptions**, wenn keine Abonnementdaten für den Store vorhanden sind. Mit diesem Cmdlet können Sie Abonnementdaten auch von einem Store auf einen anderen übertragen oder auf neu bereitgestellte StoreFront-Server importieren.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
     yourstore>"
2 Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
     :USERPROFILE\Desktop\Subscriptions.txt"
3 <!--NeedCopy-->
```

Weitere Informationen zu Import-STFStoreSubscriptions finden Sie unter https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2203/Import-STFStoreSubscriptions/

Details in der Abonnementdatendatei

Die Abonnementdatendatei ist eine Textdatei mit einer Zeile für jedes Benutzerabonnement. Jede Zeile besteht aus einer Reihe tabulatorgetrennter Werte:

```
<user-identifier> <resource-id> <subscription-id> <subscription-
status> <property-name> <property-value> <property-name> <property
-value> ...
```


Wobei:

- <user-identifier> - Erforderlich. Zeichenfolge zur Identifizierung des Benutzers. Dies ist die Windows-Sicherheits-ID des Benutzers.
- <resource-id> - Erforderlich. Zeichenfolge zur Identifizierung der abonnierten Ressource.
- <subscription-id> - Erforderlich. Zeichenfolge zur eindeutigen Identifizierung des Abonnements. Dieser Wert wird nicht verwendet (er muss jedoch in der Datendatei vorhanden sein).
- <subscription-status> - Erforderlich. Status des Abonnements: abonniert/nicht abonniert.
- <property-name> und <property-value> - Optional. Null oder mehr property-name-/property-value-Wertepaare. Diese repräsentieren Eigenschaften eines Abonnements durch einen StoreFront-Client (normalerweise eine Citrix Workspace-App). Eine Eigenschaft mit mehreren Werten, die durch mehrere Namen-/Wert-Paare mit dem gleichen Namen dargestellt wird (z. B. "…MyProp A MyProp B ….”stellt die Eigenschaft "MyProp”mit den Werten "A", "B" dar).

Beispiel

S-0-0-00-0000000000-0000000000-0000000000-0000 XenApp.Excel 21EC2020-3AEA-4069-A2DD-08002B30309D Subscribed dazzle:position 1

Größe der Abonnementdaten auf dem Datenträger des StoreFront-Servers

Anzahl Datensätze	Größe (MB)
0	6,02
1.000	7,02
10.000	40,00
100.000	219,00
200.000	358,00
500.000	784,00
800.000	1213,02
1.000.000	1597,15
1.300.000	1919,15
1.500.000	2205,15
2.000.000	2915,15

Größe der TXT-Dateien für den Import und Export

Anzahl Datensätze	Größe (MB)
0	0,00
1.000	0,13
10.000	1,30
100.000	12,80
200.000	25,60
500.000	64,10
800.000	102,00
1.000.000	128,00
1.300.000	166,00
1.500.000	192,00
1.700.000	218,00
2.000.000	256,00

Leistungsindikatoren für Storeabonnements

Mit dem Systemmonitor von Microsoft Windows (**Start > Ausführen > Perfmon**) können Sie die Gesamtanzahl aller Abonnementsdatensätze auf einem Server oder die Zahl der zwischen StoreFront-Servergruppen synchronisierten Datensätze anzeigen.

Anzeige der Abonnementzähler mit PowerShell

```
Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)\
    Subscription Entries Count (including unpurged deleted records)"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\
    Subscriptions Store Synchronizing"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
     Subscriptions Synchronized"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
     Subscriptions Transferred"
<!--NeedCopy-->
```


Abonnementdaten mit Microsoft SQL Server speichern

April 17, 2024

> **Hinweis:**
>
> Dieses Dokument setzt Grundkenntnisse in MS SQL Server und T-SQL-Abfragen voraus. Administratoren müssen mit der Konfiguration, Verwendung und Verwaltung von SQL Server vertraut sein, bevor sie die Informationen dieses Dokuments nutzen.

Einführung

ESENT ist eine einbettbare transaktionale Datenbankengine, die von Windows verwendet werden kann. Alle Versionen von StoreFront unterstützen standardmäßig die Verwendung einer integrierten ESENT-Datenbank. Sie können auch eine Verbindung zu einer Microsoft SQL Server-Instanz herstellen, wenn der Store zur Verwendung einer SQL-Verbindungszeichenfolge konfiguriert ist.

Der Hauptvorteil des Umstiegs von ESENT auf SQL in StoreFront besteht darin, dass Abonnementdatensätze mit T-SQL-Update-Anweisungen verwaltet, geändert und gelöscht werden können. Wenn Sie SQL verwenden, müssen Sie für geringfügige Änderungen an den Abonnementdaten nicht die gesamten ESENT-Abonnementdaten exportieren, ändern und wieder importieren.

Um Abonnementdaten von ESENT nach Microsoft SQL Server zu migrieren, müssen die aus StoreFront exportierten ESENT-Flat-Daten in ein SQL-freundliches Format für den Massenimport umgewandelt werden. Bei neuen Bereitstellungen ohne neue Abonnementdaten ist dieser Schritt nicht erforderlich. Die Datentransformation ist nur einmal erforderlich. In diesem Artikel wird die für StoreFront-Versionen ab Version 3.5 (mit der das hier genannte PowerShell-SDK -STF eingeführt wurde) unterstützte Konfiguration beschrieben.

> **Hinweis:**
>
> Fehler beim Herstellen der Verbindung mit der zum Speichern der Abonnementdaten verwendeten SQL Server-Instanz aufgrund von Netzwerkausfällen machen die StoreFront-Bereitstellung nicht unbrauchbar. Ausfälle führen lediglich zu einer vorübergehend verschlechterten Benutzererfahrung: Die Benutzer können keine bevorzugten Ressourcen hinzufügen, entfernen oder anzeigen, bis die Verbindung zu SQL Server wiederhergestellt wurde. Ressourcen können während eines Ausfalls weiterhin angezeigt und gestartet werden. Das erwartete Verhalten ist mit dem identisch, wenn bei Verwendung von ESENT der Citrix Subscription Store-Dienst beendet wird.
>
> **Tipp:**
>
> Mit KEYWORDS:Auto oder KEYWORDS:Mandatory konfigurierte Ressourcen verhalten sich bei

> Verwendung von ESENT und SQL gleich. Neue SQL-Abonnementdatensätze werden automatisch erstellt, wenn sich ein Benutzer zum ersten Mal anmeldet, wenn ein KEYWORD in den Ressourcen des Benutzers enthalten ist.

Vorteile von ESENT und SQL Server

ESENT	SQL
Standard, erfordert keine zusätzliche Konfiguration zur direkten Verwendung von StoreFront.	Wesentlich besser verwaltbar, Abonnementdaten können mühelos mit T-SQL-Abfragen bearbeitet oder aktualisiert werden. Ermöglicht das Löschen oder Aktualisieren von Datensätzen pro Benutzer. Ermöglicht das einfache Zählen von Datensätzen pro Anwendung, Delivery Controller oder Benutzer. Bietet einfaches Verfahren zum Löschen unnötiger Benutzerdaten, wenn Benutzer das Unternehmen verlassen. Einfache Möglichkeit zur Aktualisierung von Delivery Controller-Referenzen, z. B. wenn der Administrator auf Aggregation umstellt oder neue Delivery Controller bereitgestellt werden.
Einfachere Konfiguration der Replikation zwischen verschiedenen Servergruppen mithilfe von Abonnement-Synchronisierungs- und Pull-Zeitplänen. Siehe Konfigurieren der Abonnementsynchronisierung	Von StoreFront entkoppelt, sodass kein Backup der Abonnementdaten vor StoreFront-Upgrades erforderlich ist, da die Daten auf einem separaten SQL Server-Rechner verwaltet werden. Abonnementbackups sind unabhängig von StoreFront und verwenden SQL-Backupstrategien und -mechanismen.
SQL ist nicht nötig, wenn keine Abonnementverwaltung erforderlich ist. Wenn die Abonnementdaten nie aktualisiert werden müssen, erfüllt ESENT wahrscheinlich die Kundenanforderungen.	Eine Kopie der Abonnementdaten wird von allen Mitgliedern der Servergruppe gemeinsam genutzt, sodass die Wahrscheinlichkeit von Unterschieden bei Daten auf den Servern und von Synchronisierungsproblemen geringer ist.

Nachteile von ESENT und SQL Server

ESENT	SQL
Keine einfache Möglichkeit, Abonnementdaten detailliert zu verwalten. Bearbeitung der Abonnementdaten in exportierten TXT-Dateien erforderlich. Die gesamte Abonnementdatenbank muss exportiert und wieder importiert werden. Möglicherweise müssen Tausende von Datensätzen per Suche und Ersetzen geändert werden, was arbeitsintensiv und fehleranfällig ist.	Erfordert grundlegende SQL-Kenntnis und -Infrastruktur. Erfordert evtl. den Erwerb einer SQL-Lizenz, was die Gesamtbetriebskosten für die StoreFront Bereitstellung erhöht. Allerdings kann eine Citrix Virtual Apps and Desktops Datenbankinstanz auch für StoreFront verwendet werden, um Kosten zu senken.
Eine Kopie der ESENT-Datenbank muss auf jedem StoreFront-Server einer Servergruppe verwaltet werden. In seltenen Fällen kann diese Datenbank innerhalb einer Servergruppe oder zwischen verschiedenen Servergruppen asynchron werden.	Das Replizieren von Abonnementdaten zwischen Servergruppen ist eine nicht ganz einfache Bereitstellungsaufgabe. Es erfordert pro Datencenter mehrere SQL-Instanzen und die Transaktionsreplikation zwischen diesen. Hierfür ist MS SQL-Fachwissen erforderlich. Datenmigration aus ESENT und Umwandlung in SQL-freundliches Format erforderlich. Dieser Vorgang ist nur einmal erforderlich. Zusätzliche Windows-Server und -Lizenzen möglicherweise erforderlich. Zusätzliche Schritte zum Bereitstellen von StoreFront.

Bereitstellungsszenarios

> **Hinweis:**
>
> Jeder in StoreFront konfigurierte Store erfordert entweder eine ESENT-Datenbank oder eine Microsoft SQL-Datenbank, wenn Sie Benutzerabonnements unterstützen möchten. Die Methode zum Speichern der Abonnementdaten wird in StoreFront auf Store-Ebene festgelegt.

Citrix empfiehlt, alle Store-Datenbanken in derselben Microsoft SQL Server-Instanz zu führen, um die Verwaltung zu vereinfachen und das Potenzial von Fehlkonfigurationen zu verringern.

Stores können dieselbe Datenbank gemeinsam nutzen, vorausgesetzt, sie sind zur Verwendung derselben Verbindungszeichenfolge konfiguriert. Es spielt keine Rolle, ob sie unterschiedliche Delivery Controller verwenden. Der Nachteil der Verwendung einer Datenbank durch mehrere Stores besteht darin, dass nicht erkennbar ist, welchem Store die einzelnen Abonnementdatensätze entsprechen.

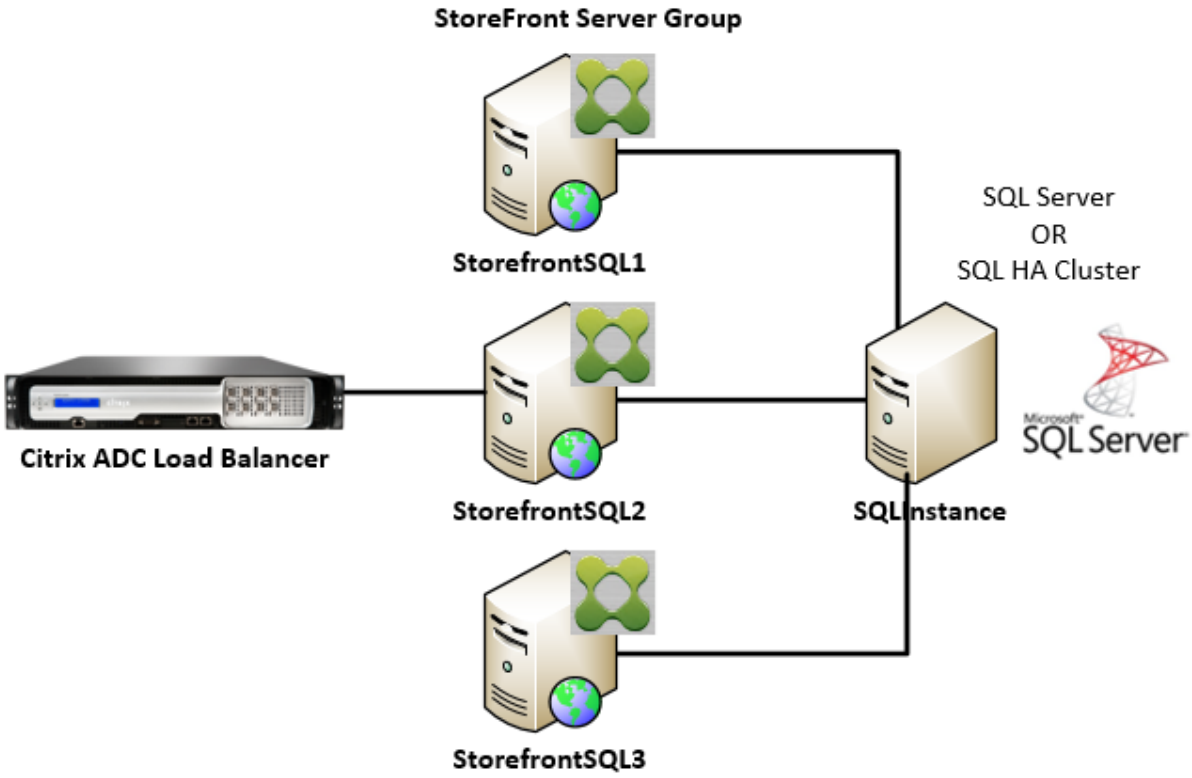
Eine Kombination beider Datenspeichermethoden in einer einzelnen StoreFront-Bereitstellung mit mehreren Stores ist technisch möglich. Ein Speicher kann für ESENT und ein zweiter für SQL konfiguriert werden. Das wird aufgrund der komplexeren Verwaltung und des Potenzials für Fehlkonfigurationen nicht empfohlen.

Zum Speichern von Abonnementdaten in SQL
Server gibt es vier Szenarien:

Szenario 1: Einzelner StoreFront -Server oder Servergruppe mit ESENT (Standard) Standardmäßig verwenden alle Versionen von StoreFront ab 2.0 eine ESENT-Flat-Datenbank, um Abonnementdaten einer Servergruppe zu speichern und zu replizieren. Auf jedem Mitglied der Servergruppe wird eine identische Kopie der Abonnementdatenbank geführt und mit allen anderen Mitgliedern der Servergruppe synchronisiert. Dieses Szenario erfordert keine zusätzliche Konfiguration. Das Szenario eignet sich für die meisten Kunden, bei denen keine häufigen Änderungen an Delivery Controller-Namen und keine häufigen Verwaltungsaufgaben an Abonnementdaten (Entfernen oder Aktualisieren alter Benutzerabonnements) zu erwarten sind.

Szenario 2: Einzelner StoreFront-Server und lokal installierte Microsoft SQL Server-Instanz StoreFront verwendet eine lokal installierte SQL Server-Instanz und beide Komponenten befinden sich auf demselben Server. Dieses Szenario eignet sich für eine einfache StoreFront-Bereitstellung, bei der häufig Änderungen an Delivery Controller-Namen oder Verwaltungsschritte wie Entfernen oder Aktualisieren von Abonnementdaten nötig sind, jedoch keine hohe Verfügbarkeit der StoreFront-Bereitstellung erforderlich ist. Citrix empfiehlt dieses Szenario nicht für Servergruppen, da damit ein zentraler Ausfallpunkt auf dem Servergruppenmitglied entsteht, das die Microsoft SQL-Datenbankinstanz hostet. Das Szenario ist nicht für große Enterprise-Bereitstellungen geeignet.

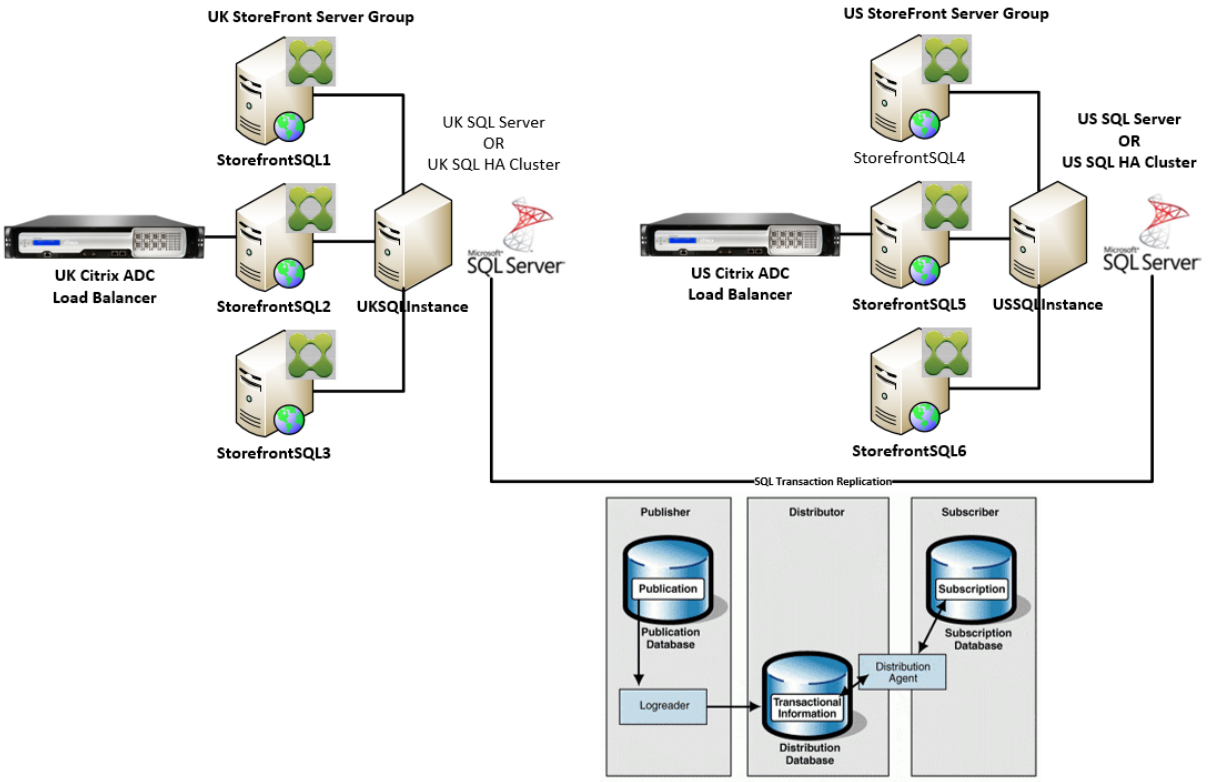
Szenario 3: StoreFront-Servergruppe und eine dedizierte, für hohe Verfügbarkeit konfigurierte Microsoft SQL Server-Instanz (empfohlen) Alle Mitglieder der StoreFront-Servergruppe stellen eine Verbindung mit derselben dedizierten Microsoft SQL Server-Instanz bzw. einem SQL-Failovercluster her. Dies ist das am besten geeignete Modell für große Enterprise-Bereitstellungen, in denen Citrix Administratoren häufig Änderungen an Delivery Controller-Namen vornehmen oder häufig Verwaltungsaufgaben an Abonnementdaten ausgeführt werden (z. B. Entfernen oder Aktualisieren) und die hohe Verfügbarkeit erfordern.



Szenario 4: Mehrere StoreFront-Servergruppen und eine dedizierte Microsoft SQL Server-Instanz für jede Servergruppe in jedem Datencenter

> **Hinweis:**
>
> Dies ist eine fortgeschrittene Konfiguration. Sie sollte nur von erfahrenen SQL Server-Administratoren erstellt werden, die mit der Transaktionsreplikation vertraut sind und über die erforderlichen Kenntnisse verfügen.

Das Szenario ähnelt Szenario 3, erweitert auf Umgebungen, in denen mehrere StoreFront-Servergruppen in verschiedenen Datencentern erforderlich sind. Citrix Administratoren können die Abonnementdaten zwischen verschiedenen Servergruppen in denselben oder verschiedenen Datencentern synchronisieren. Für Redundanz- und Failoverzwecke und eine hohe Leistung stellt jede Servergruppe im Datencenter eine Verbindung zu einer dedizierten Microsoft SQL Server-Instanz her. Das Szenario erfordert eine erhebliche zusätzliche Microsoft SQL Server-Konfiguration und -Infrastruktur. Sie nutzt für die Replikation von Abonnementdaten und für SQL-Transaktionen ausschließlich Microsoft SQL-Technologie.



Ressourcen

Sie können die folgenden hilfreichen Skripts von https://github.com/citrix/sample-scripts/tree/master/storefront herunterladen:

Konfigurationsskripts

- **Set-STFDatabase.ps1** –Legt die MS SQL-Verbindungszeichenfolge für jeden Store fest. Führen Sie das Skript auf dem StoreFront-Server aus.
- **Add-LocalAppPoolAccounts.ps1** –Gewährt den App-Pools des lokalen StoreFront-Servers Lese- und Schreibzugriff auf die SQL-Datenbank. Führen Sie das Skript für Szenario 2 auf dem SQL-Server aus.
- **Add-RemoteSFAccounts.ps1** –Gewährt allen StoreFront-Servern in einer Servergruppe Lese- und Schreibzugriff auf die SQL-Datenbank. Führen Sie das Skript für Szenario 3 auf dem SQL-Server aus.
- **Create-StoreSubscriptionsDB-2016.sql** –Erstellt die SQL-Datenbank und das Schema. Führen Sie das Skript auf dem SQL-Server aus.

Skripts für Datentransformation und Import

- **Transform-SubscriptionDataForStore.ps1** –Exportiert Abonnementdaten aus ESENT und wandelt sie in ein SQL-freundliches Format für den Import um.
- **Create-ImportSubscriptionDatasp.sql** –Erstellt eine gespeicherte Prozedur zum Importieren der von Transform-SubscriptionDataForStore.ps1 umgewandelten Daten. Führen Sie das Skript einmal auf dem SQL-Server aus, nachdem Sie das Datenbankschema mit Create-StoreSubscriptionsDB-2016.sql erstellt haben.

Konfigurieren der lokalen Sicherheitsgruppe des StoreFront-Servers auf dem SQL-Server

Szenario 2: Einzelner StoreFront-Server und lokal installierte Microsoft SQL Server-Instanz

Erstellen Sie eine lokale Sicherheitsgruppe unter dem Namen <SQLServer>\StoreFrontServers auf dem Microsoft SQL-Server und fügen Sie die virtuellen Konten für IIS APPPOOL\DefaultAppPool und IIS APPPOOL\Citrix Receiver for Web hinzu, damit das lokal installierte StoreFront Lese- und Schreibvorgänge an SQL ausführen kann. Auf diese Sicherheitsgruppe wird in dem SQL-Skript verwiesen, das das Schema für die Store-Abonnementdatenbank erstellt. Stellen Sie daher sicher, dass die Gruppennamen übereinstimmen.

Sie können hierfür das Skript Add-LocalAppPoolAccounts.ps1 herunterladen.

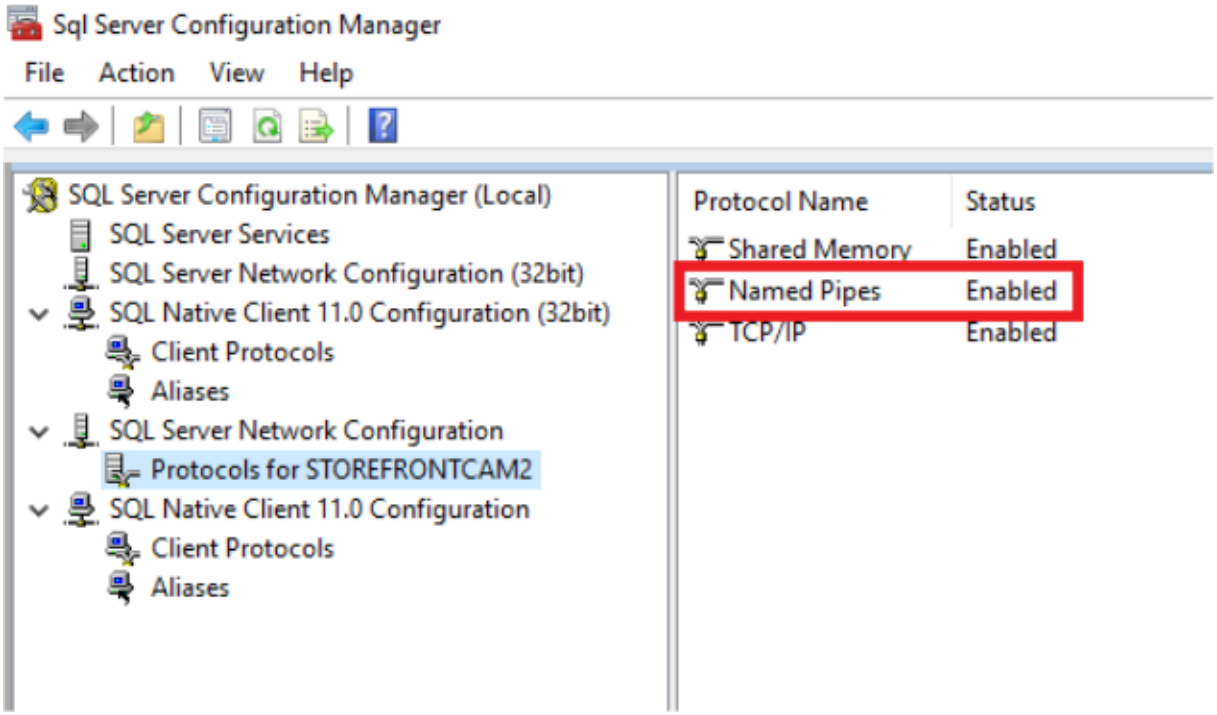
Installieren Sie StoreFront, bevor Sie das Skript *Add-LocalAppPoolAccounts.ps1* ausführen. Das Skript erfordert, dass das virtuelle IIS-Konto von IIS APPPOOL\Citrix Receiver for Web gefunden werden kann, welches erst nach der Installation und Konfiguration von StoreFront vorhanden ist. IIS APPPOOL\DefaultAppPool wird automatisch durch die Installation der IIS-Webserverrolle erstellt.

```
# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool Virtual Accounts"

# Check whether the Local Group Exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "
        Yellow"
 }

else
{

Write-Host "Creating $LocalGroupName local security group" -
    ForegroundColor "Yellow"

```



```
# Create Local User Group
$Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
$LocalGroup = $Computer.Create("group",$LocalGroupName)
$LocalGroup.setinfo()
$LocalGroup.description = $Description
$Localgroup.SetInfo()
Write-Host "$LocalGroupName local security group created" -
    ForegroundColor "Green"
 }

$Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"

# Add IIS APPPOOL\DefaultAppPool
$objAccount = New-Object System.Security.Principal.NTAccount("IIS
    APPPOOL\DefaultAppPool")
$StrSID = $objAccount.Translate([System.Security.Principal.
    SecurityIdentifier])
$DefaultSID = $StrSID.Value

$Account = [ADSI]"WinNT://$DefaultSID"
$Group.Add($Account.Path)

# Add IIS APPPOOL\Citrix Receiver for Web
$objAccount = New-Object System.Security.Principal.NTAccount("IIS
    APPPOOL\Citrix Receiver for Web")
$StrSID = $objAccount.Translate([System.Security.Principal.
    SecurityIdentifier])
$WebRSID = $StrSID.Value

$Account = [ADSI]"WinNT://$WebRSID"
$Group.Add($Account.Path)

Write-Host "AppPools added to $LocalGroupName local group" -
    ForegroundColor "Green"
<!--NeedCopy-->
```

Aktivieren Sie mithilfe von SQL Server-Konfigurations-Manager Named Pipes in Ihrer lokalen SQL-Instanz. Named Pipes sind für die Kommunikation zwischen StoreFront- und SQL Server-Prozessen erforderlich.

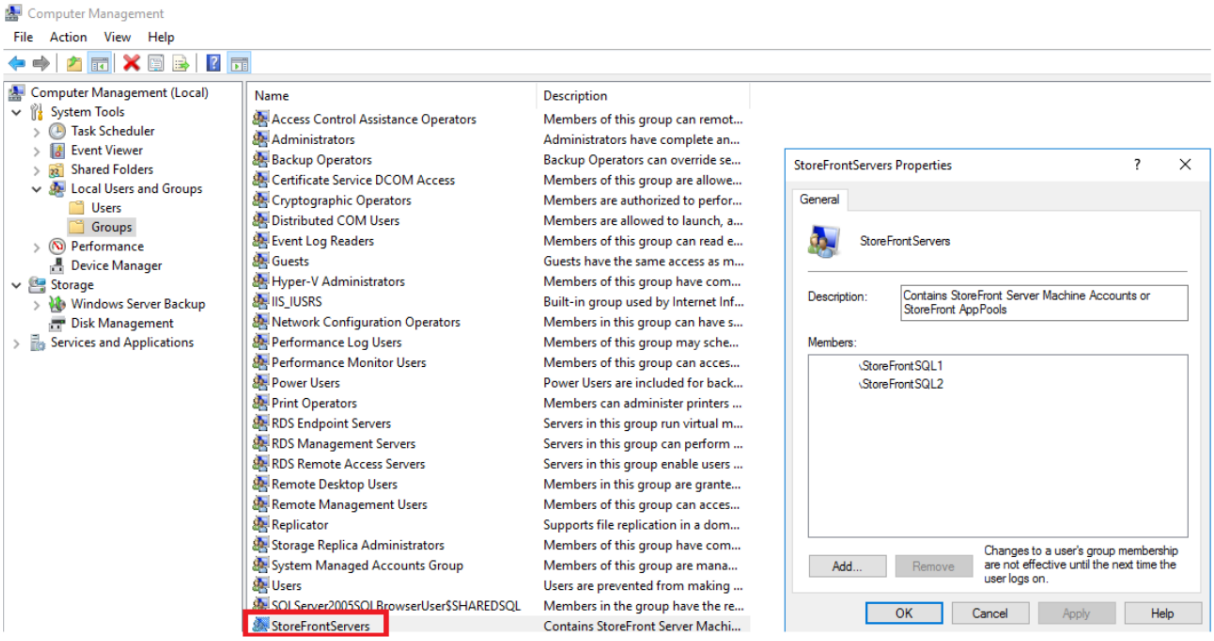


Stellen Sie sicher, dass die Windows-Firewallregeln korrekt konfiguriert sind, sodass SQL Server-Verbindungen über einen bestimmten Port oder dynamische Ports zugelassen sind. Spezifische Informationen hierzu für Ihre Umgebung finden Sie in der Microsoft-Dokumentation.

> **Tipp:**
>
> Wenn die Verbindung zur lokalen SQL-Instanz fehlschlägt, überprüfen Sie, ob localhost bzw. die Angabe `<hostname>` in der Verbindungszeichenfolge in die richtige IPv4-Adresse aufgelöst wird. Windows versucht möglicherweise, IPv6 anstelle von IPv4 zu verwenden, und die DNS-Auflösung von localhost kann ::1 anstelle der richtigen IPv4-Adresse des StoreFront- und SQL-Servers zurückgeben. Möglicherweise ist das vollständige Deaktivieren des IPv6-Netzwerkstapels auf dem Hostserver erforderlich, um dieses Problem zu beheben.

Szenario 3: StoreFront-Servergruppe und eine dedizierte Microsoft SQL Server-Instanz

Erstellen Sie eine lokale Sicherheitsgruppe unter dem Namen `<SQLServer>\StoreFrontServers` auf dem Microsoft SQL-Server und fügen Sie alle Mitglieder der StoreFront-Servergruppe hinzu. Auf diese Sicherheitsgruppe wird später im Skript **Create-StoreSubscriptionsDB-2016.SQL** verwiesen, das das Schema der Abonnementdatenbank in SQL erstellt.



Fügen Sie der Gruppe alle Domänencomputerkonten der StoreFront-Servergruppe <SQLServer>\StoreFrontServers hinzu. Nur in der Gruppe aufgelistete StoreFront-Server-Domänenkonten können Abonnementdatensätze in SQL lesen und schreiben, wenn die Windows-Authentifizierung von SQL Server verwendet wird. Die folgende PowerShell-Funktion in Skript Add-RemoteSFAccounts.ps1 erstellt die lokale Sicherheitsgruppe und fügt ihr zwei StoreFront-Server mit dem Namen "StoreFrontSQL1"und "StoreFrontSQL2"hinzu.

```
function Add-RemoteSTFMachineAccounts
{

[CmdletBinding()]
param([Parameter(Mandatory=$True)][string]$Domain,
[Parameter(Mandatory=$True)][array]$StoreFrontServers)

# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool virtual accounts"

# Check whether the Local Security Group already exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "
        Yellow"
 }

else
{

    Write-Host "Creating $LocalGroupName local group" -ForegroundColor
```

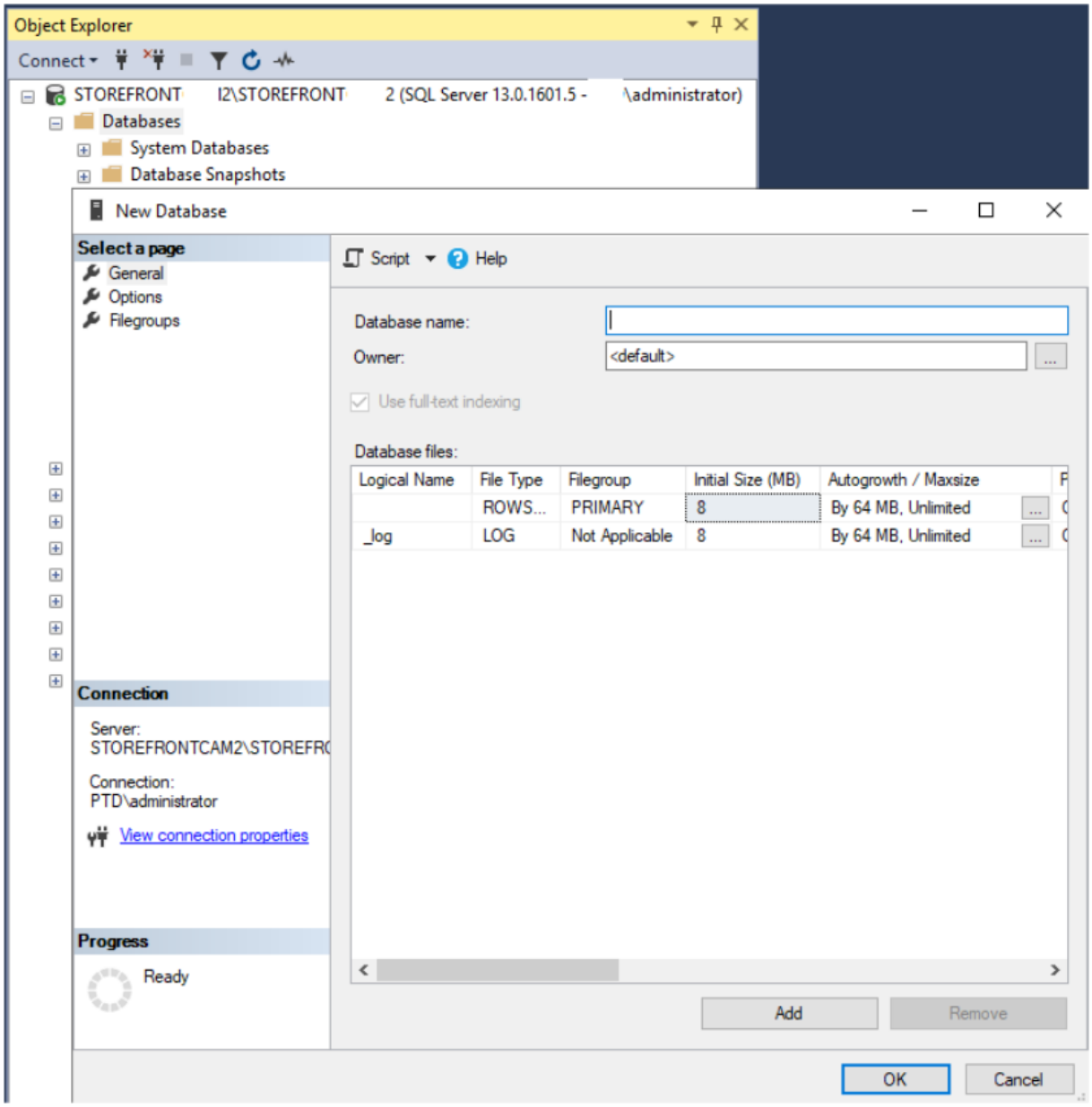


```
          "Yellow"
23
24      # Create Local Security Group
25      $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
26      $LocalGroup = $Computer.Create("group",$LocalGroupName)
27      $LocalGroup.setinfo()
28      $LocalGroup.description = $Description
29      $Localgroup.SetInfo()
30  Write-Host "$LocalGroupName local group created" -ForegroundColor "
        Green"
31   }
32
33  Write-Host "Adding $StoreFrontServers to $LocalGroupName local group" -
        ForegroundColor "Yellow"
34
35  foreach ($StoreFrontServer in $StoreFrontServers)
36  {
37
38      $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
39      $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"
40      $Group.Add($Computer.Path)
41   }
42
43  Write-Host "$StoreFrontServers added to $LocalGroupName" -
        ForegroundColor "Green"
44   }
45
46  Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers @("
        StoreFrontSQL1","StoreFrontSQL2")
47  <!--NeedCopy-->
```

Konfigurieren des Abonnementdatenbankschemas in Microsoft SQL Server für jeden Store

Erstellen Sie eine benannte Instanz auf Ihrem Microsoft SQL-Server zur Verwendung durch StoreFront. Legen Sie den Pfad innerhalb des .SQL-Skripts auf den Installationsort der SQL-Version oder den Speicherort der Datenbankdateien fest. Das Beispielskript Create-StoreSubscriptionsDB-2016.sql verwendet SQL Server 2016 Enterprise.

Erstellen Sie mit SQL Server Management Studio (SSMS) eine leere Datenbank, indem Sie mit der rechten Maustaste auf **Datenbanken** klicken und **Neue Datenbank** auswählen.



Geben Sie einen **Datenbanknamen** ein, der Ihrem Store entspricht, oder wählen Sie einen anderen Namen, etwa *STFSubscriptions*.

Ändern Sie vor dem Ausführen des Skripts für jeden Store in Ihrer StoreFront Bereitstellung die Verweise im Beispielskript so, dass sie Ihren StoreFront- und SQL-Bereitstellungen entsprechen. Beispiel:

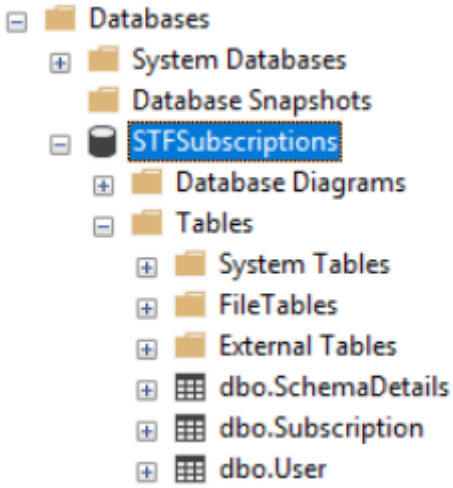
- Benennen Sie jede von Ihnen erstellte Datenbank so, dass sie mit dem Storenamen in StoreFront unter `USE [STFSubscriptions]` übereinstimmt.
- Legen Sie den Pfad der MDF- und LDF-Datenbankdateien auf den Pfad fest, an dem die Datenbank gespeichert werden soll.


```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.mdf

C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.ldf
```

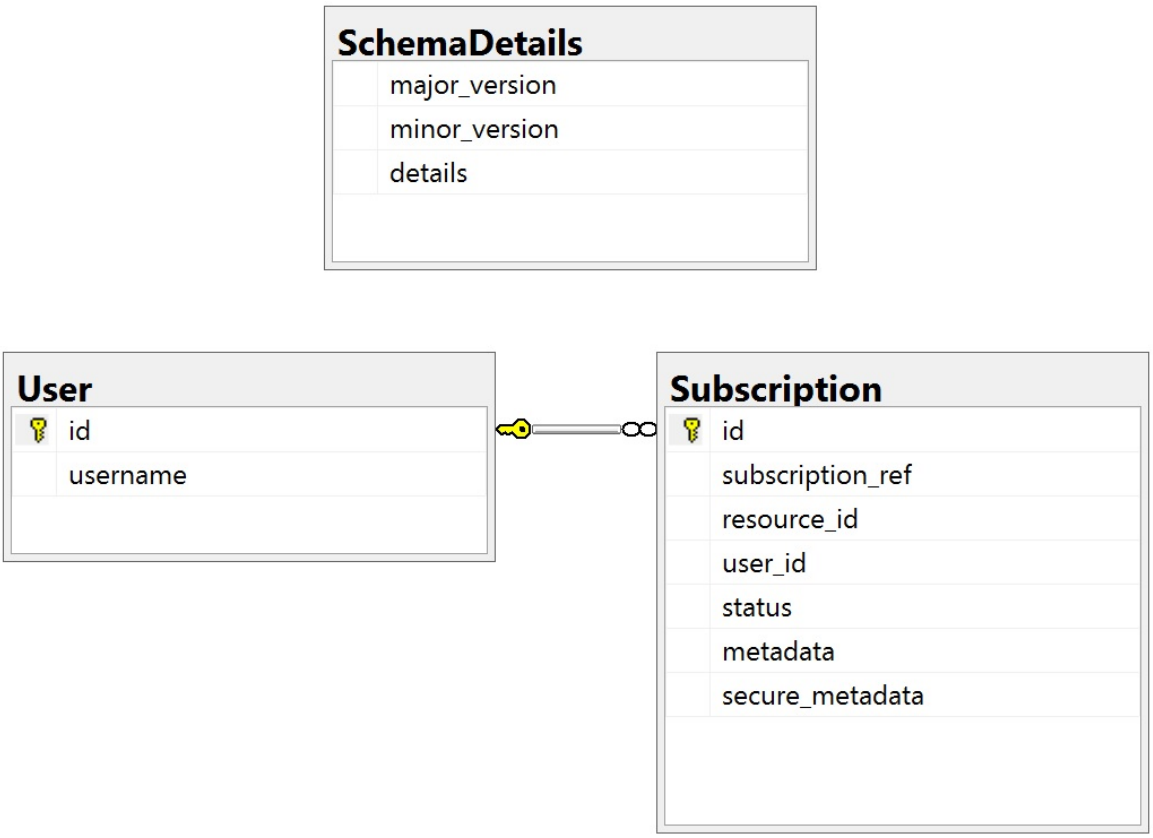
- Legen Sie den Verweis auf den Namen Ihres SQL-Servers innerhalb des Skripts fest:

```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;

ALTER LOGIN [SQL2016\StoreFrontServers]
```

Führen Sie das Skript aus. Nach erfolgreicher Konfiguration des Schemas werden drei Datenbanktabellen erstellt: *SchemaDetails*, *Subscription* und *User*.



Die folgende Abbildung zeigt das Schema der mit dem Skript *Create-StoreSubscriptionsDB-2016.SQL* erstellten Abonnementdatenbank:



Konfigurieren der SQL Server-Verbindungszeichenfolge für jeden StoreFront-Store

Szenario 1

> **Tipp:**
>
> Die auf dem Datenträger gespeicherten ursprünglichen Abonnementdaten der ESENT-Datenbank werden nicht gelöscht. Wenn Sie von Microsoft SQL Server wieder auf ESENT umsteigen möchten, können Sie die Store-Verbindungszeichenfolge entfernen und einfach wieder die ursprünglichen Daten verwenden. Abonnements, die während der Verwendung von SQL für den Store erstellt wurden, sind in ESENT nicht vorhanden und die Benutzer sehen diese neuen Abonnementdatensätze nicht. Alle ursprünglichen Abonnementdatensätze sind weiterhin vorhanden.

Erneutes Aktivieren von ESENT-Abonnements in einem Store Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.

Verwenden Sie die Option **-UseLocalStorage**, um den Store anzugeben, für den Sie ESENT-Abonnements erneut aktivieren möchten:


```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store1"

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
    $StoreVirtualPath

# Removes the SQL DB Connection string and reverts back to using ESENT
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    UseLocalStorage
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

Szenarios 2, 3 und 4

Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.

Geben Sie mit **$StoreVirtualPath** den Store an, für den Sie eine Verbindungszeichenfolge festlegen möchten.

```
$SiteID = 1
$VirtualPath= "/Citrix/Store1"
$DBName = "Store1"
$DBServer = "SQL2016Ent"
$DBLocalServer = "localhost"
$SQLInstance = "StoreFrontInstance"

# For a remote database instance
$ConnectionString = "Server=$DBServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"
<!--NeedCopy-->
```

ODER

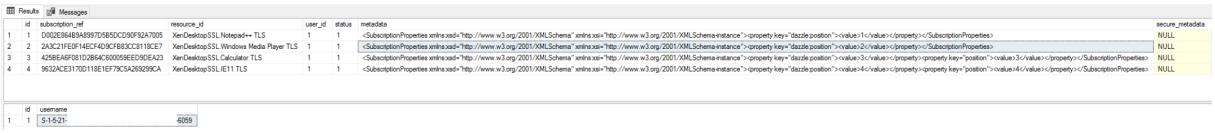
```
# For a locally installed database instance
$ConnectionString = "$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath "/
    Citrix/Store"
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

Wiederholen Sie den Vorgang für jeden Store in der Bereitstellung, wenn Sie alle Stores für die Verwendung einer SQL-Verbindungszeichenfolge konfigurieren möchten.

Migrieren von Daten von ESENT nach Microsoft SQL Server

Zur Migration vorhandener ESENT-Daten nach SQL ist ein zweistufiger Datentransformationsprozess erforderlich. Zwei Skripts stehen zur Verfügung, die bei der Ausführung dieser einmaligen Operation helfen. Wenn die Verbindungszeichenfolge in StoreFront und der SQL-Instanz korrekt konfiguriert ist, werden alle neuen Abonnements automatisch in SQL im richtigen Format erstellt. Nach der Migration werden die ESENT-Abonnementdaten in ein SQL-Format umgewandelt und die Benutzer sehen auch ihre zuvor abonnierten Ressourcen.

Beispiel: vier SQL-Abonnements für einen Domänenbenutzer



Schritt 1: Konvertieren der ESENT-Daten in ein SQL-Format für den Massenimport mit Transform-SubscriptionDataForStore.ps1 Melden Sie sich bei dem StoreFront-Server an, dessen ESENT-Daten Sie umwandeln möchten.

Jedes Mitglied einer Servergruppe ist geeignet, sofern alle die gleiche Anzahl Abonnementdatensätze enthalten.

Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.

Führen Sie das Skript Transform-SubscriptionDataForStore.ps1 aus, das eine `<StoreName>.txt`-Datei aus der ESENT-Datenbank auf den Desktop des aktuellen Benutzers exportiert.

Das PowerShell-Skript bietet ausführliches Feedback zu jeder verarbeiteten Abonnementzeile, um das Debuggen und die Prüfung des Erfolgs des Vorgangs zu unterstützen. Die Verarbeitung kann lange dauern.

Die umgewandelten Daten werden nach Abschluss des Skripts in die Datei `<StoreName>SQL.txt` auf dem Desktop des aktuellen Benutzers geschrieben. Das Skript fasst die Anzahl der eindeutigen Benutzerdatensätze und die Gesamtzahl der verarbeiteten Abonnements zusammen.

Wiederholen Sie diesen Vorgang für jeden Store, den Sie nach SQL Server migrieren möchten.

Schritt 2: Massenimport der umgewandelten Daten mit einer gespeicherten T-SQL-Prozedur Die Daten müssen für jeden Stores gesondert importiert werden.

Kopieren Sie die in Schritt 1 erstellte Datei `<StoreName>SQL.txt` vom Desktop des StoreFront-Servers`C:\` auf den Computer mit Microsoft SQL Server und benennen Sie sie in SubscriptionsSQL.txt um.

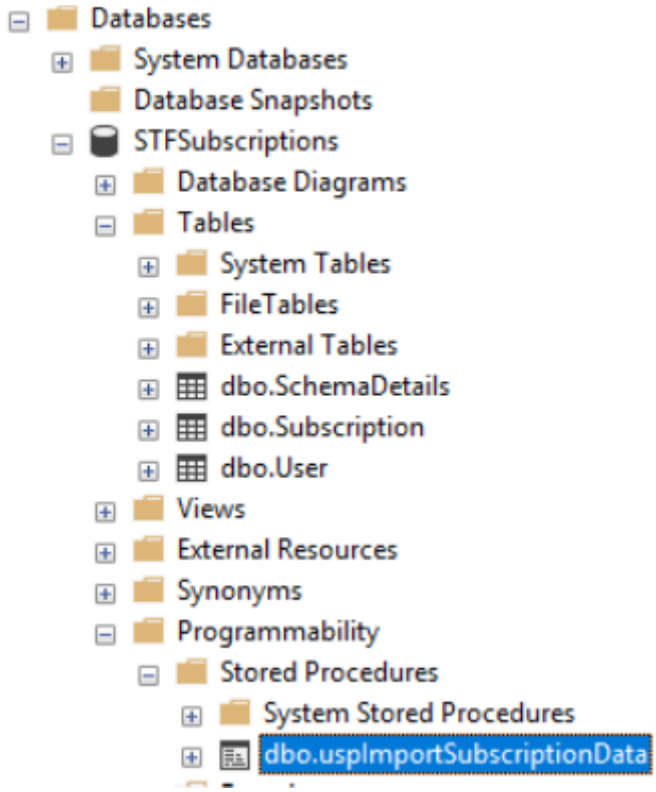
Das Skript Create-ImportSubscriptionDataSP.sql erstellt eine gespeicherte T-SQL-Prozedur zum Massenimport der Abonnementdaten. Es entfernt doppelte Einträge für eindeutige Benutzer, sodass die resultierenden SQL-Daten korrekt normalisiert und in die richtigen Tabellen aufgeteilt werden.

Bevor Sie *Create-ImportSubscriptionDatasp.sql* ausführen, ändern Sie `USE [STFSubscriptions]` auf die Datenbank, in der Sie die gespeicherte Prozedur erstellen möchten.

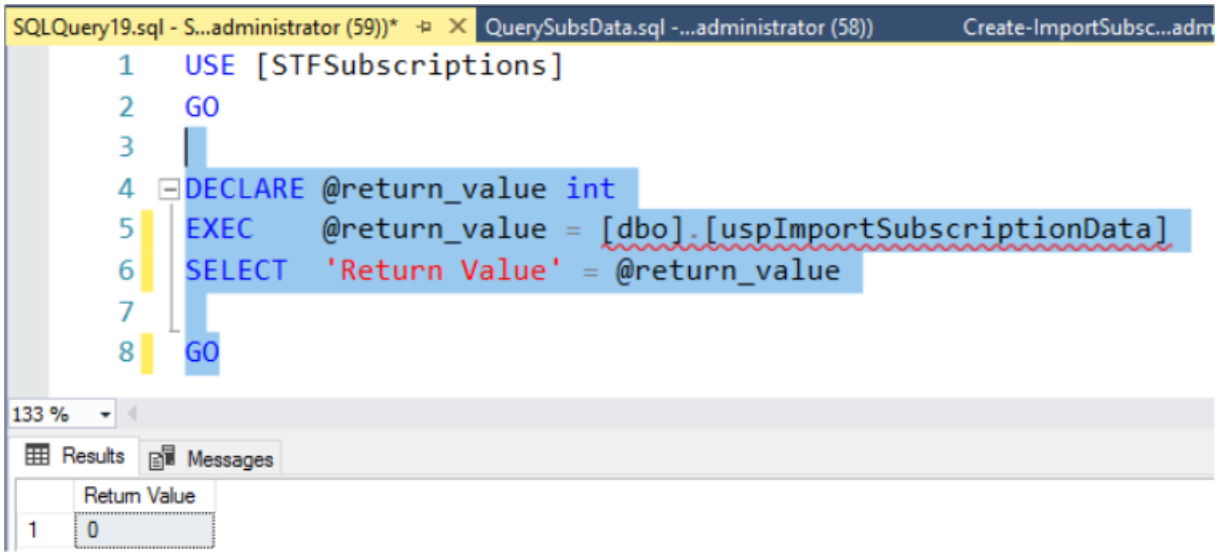
Öffnen Sie die Datei *Create-ImportSubscriptionDatasp.sql* mit SQL Server Management Studio und führen Sie den enthaltenen Code aus. Das Skript fügt der zuvor erstellten Datenbank die gespeicherte Prozedur *ImportSubscriptionDatasp* hinzu.

Nach Erstellung der gespeicherten Prozedur wird in der SQL-Konsole die folgende Meldung angezeigt und die gespeicherte Prozedur ImportSubscriptionDatasp wird der Datenbank hinzugefügt:

```
Commands completed successfully.
```



Führen Sie die gespeicherte Prozedur aus, indem Sie mit der rechten Maustaste darauf klicken, **Gespeicherte Prozedur ausführen** wählen und auf **OK** klicken.



Der Rückgabewert 0 zeigt an, dass alle Daten erfolgreich importiert wurden. Jegliche Probleme beim Import werden in der SQL-Konsole protokolliert. Nach dem erfolgreichen Ausführen der gespeicherten Prozedur vergleichen Sie die von Transform-SubscriptionDataForStore.ps1 zurückgegebene Gesamtzahl der Abonnementdatensätze und eindeutigen Benutzer mit dem Ergebnis der beiden SQL-Abfragen unten. Die beiden Summen müssen übereinstimmen.

Die Gesamtanzahl der Abonnements aus dem Transformationsskript muss mit der Gesamtzahl übereinstimmen, die von folgender SQL-Abfrage zurückgegeben wird:

```
SELECT COUNT(*) AS TotalSubscriptions
FROM [Subscription]
<!--NeedCopy-->
```

Die Anzahl der eindeutigen Benutzer aus dem Transformationsskript muss mit der Anzahl übereinstimmen, die von folgender SQL-Abfrage aus der Tabelle “User”zurückgegeben wird:

```
SELECT COUNT(*) AS TotalUsers
FROM [User]
<!--NeedCopy-->
```

Wenn das Transformationsskript 100 eindeutige Benutzer und 1000 Abonnementdatensätze insgesamt anzeigt, muss SQL nach erfolgreicher Migration dieselben Zahlen anzeigen.

Melden Sie sich bei StoreFront an, um zu überprüfen, ob bestehende Benutzer ihre Abonnementdaten sehen können. Bestehende Abonnementdatensätze werden in SQL aktualisiert, wenn Benutzer Ressourcen abonnieren oder abbestellen. Neue Benutzer- und Abonnementdatensätze werden ebenfalls in SQL erstellt.

Schritt 3: Ausführen der T-SQL-Abfragen an importierten Daten

> **Hinweis:**
>
> Bei allen Delivery Controller-Namen wird zwischen Groß- und Kleinschreibung unterschieden. Die Schreibung muss mit der in StoreFront verwendeten Groß- und Kleinschreibung übereinstimmen.

```
-- Get all SQL subscription records
Use [STFSubscriptions]
SELECT * FROM [Subscription]
SELECT * FROM [User]
<!--NeedCopy-->
```

```
-- Get all subscription records for a particular user SID
Use [STFSubscriptions]
SELECT * FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'

-- Get total number of Subscription records for a particular user SID
Use [STFSubscriptions]
SELECT COUNT(Subscription.id)
FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
<!--NeedCopy-->
```

```
-- Get all subscription records for a particular delivery controller
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'

-- Get all subscription records for a particular application
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] = ' DeliveryController.Application'
<!--NeedCopy-->
```

Aktualisieren oder Löschen von Abonnementdatensätzen mit T-SQL

> **Haftungsausschluss:**
>
> Sie verwenden alle SQL-Anweisungen zum Aktualisieren und Löschen ausschließlich auf eigenes Risiko. Citrix ist nicht haftbar bei einem Verlust oder einer versehentlichen Änderung Ihrer Abonnementdaten durch die falsche Anwendung der angegebenen Beispiele. Die folgenden T-SQL-Anweisungen sollen als Leitfaden für einfache Aktualisierungen dienen. Führen Sie für alle Abonnementdaten in der SQL-Datenbank ein vollständiges Backup aus, bevor Sie versuchen, Abonnements zu aktualisieren oder veraltete Datensätze zu entfernen. Wenn Sie diese erforderlichen Backups nicht ausführen, kann dies zu Datenverlust oder -beschädigung führen. Bevor Sie eigene T-SQL-UPDATE- oder DELETE-Anweisungen an der Produktionsdatenbank ausführen, testen Sie diese an Testdaten oder einer redundanten Kopie der Produktionsdaten außerhalb der Live-Produktionsdatenbank.
>
> **Hinweis:**
>
> Bei allen Delivery Controller-Namen wird zwischen Groß- und Kleinschreibung unterschieden. Die Schreibung muss mit der in StoreFront verwendeten Groß- und Kleinschreibung übereinstimmen.

```
-- Update the delivery controller used in all subscriptions.
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
   NewDeliveryController.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
<!--NeedCopy-->
```

```
-- After enabling multi-site aggregation, update the resource_id
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
   DefaultAggregationGroup.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular Delivery Controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'
<!--NeedCopy-->
```

```
-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
<!--NeedCopy-->
```



```
-- Delete all subscription records for a particular application
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE '%.Application'
<!--NeedCopy-->
```

```
-- Delete all subscription records for an application published via a
    specific delivery controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] = 'DeliveryController.Application'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular user SID
-- relies on cascade to delete records from [Subscription]
Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
<!--NeedCopy-->
```

```
-- Delete ALL subscription data from a particular database and reset
    the primary key clustered index to start numbering from 0.
-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
-- Can be useful whilst debugging data import issues to start with a
    clean database.

Use [STFSubscriptions]
DELETE FROM [Subscription]
DBCC CHECKIDENT ([Subscription], RESEED, 0)
DELETE FROM [User]
DBCC CHECKIDENT ([User], RESEED, 0)
<!--NeedCopy-->
```

Favoriten aktivieren oder deaktivieren

April 17, 2024

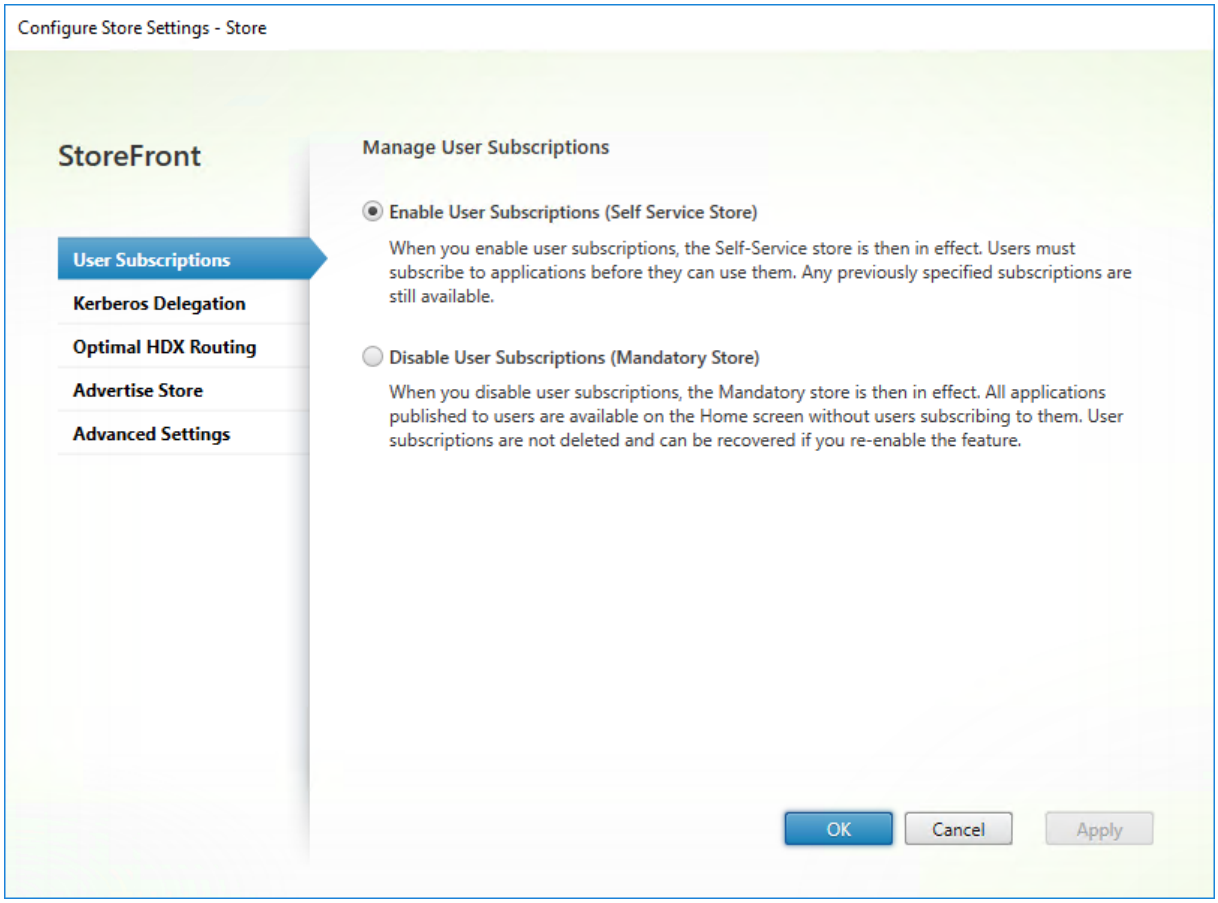
Im Fenster “Benutzerabonnements”können Sie eine der folgenden Optionen auswählen:

- Zulassen, dass Benutzer Favoriten erstellen und entfernen (Self-Service-Store). Die Benutzer können eine App als Favoriten markieren, indem sie auf den Stern auf der App-Kachel klicken. Die Benutzer können erneut auf den Stern klicken und die App als Favoriten abzuwählen. Favorisierte Apps werden auf der Registerkarte **Home** angezeigt.

- Favoriten deaktivieren (vorgegebener Store). Die Benutzer können Apps nicht als Favoriten markieren oder abwählen. Die Registerkarte “Home”wird nicht angezeigt.

Die Abonnementdaten im Store werden beim Deaktivieren von Abonnements nicht gelöscht. Werden Abonnements für den Store reaktiviert, können Benutzer ihre Favoriten anzeigen, sobald sie sich das nächste Mal anmelden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren**.
2. Klicken Sie auf die Registerkarte **Benutzerabonnements**, um das Favoritenfeature ein- oder auszuschalten.
3. Wählen Sie **Benutzerabonnements aktivieren (Self-Service-Store)**, um Favoriten zu aktivieren.
4. Wählen Sie **Benutzerabonnements deaktivieren**, um Favoriten zu deaktivieren.



Alternativ können Sie Benutzerabonnements für einen Store mit dem PowerShell-Cmdlet Get-STFStoreService konfigurieren. Beispiel:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
```



```
Set-STFStoreService -StoreService $StoreObject -LockedDown $True -
    Confirm:$False
<!--NeedCopy-->
```

Citrix Virtual Apps and Desktops konfigurieren

April 17, 2024

Berücksichtigen Sie die folgenden Optionen bei der Bereitstellung von Anwendungen mit Citrix Virtual Apps and Desktops oder Citrix Desktops as a Service, um die Benutzerfreundlichkeit beim Zugreifen auf Anwendungen über Ihre Stores zu erhöhen. Weitere Informationen zur Bereitstellung von Anwendungen finden Sie unter Anwendungen.

- Geben Sie im Feld **Anwendungsname (Benutzer)** den Namen der Anwendung so ein, wie er auf der Store-Website angezeigt werden soll.
- Geben Sie im Feld **Beschreibung und Schlüsselwörter** die Beschreibung ein, die auf der Store-Website beim Erweitern der App-Details angezeigt werden soll, sowie zusätzliche Schlüsselwörter.
- Wählen Sie das **Anwendungssymbol**, damit Benutzer eine Anwendung auf der StoreFront-Website visuell identifizieren können.
- Geben Sie im Feld **Anwendungskategorie** optional eine Kategorie ein. Fügen Sie dem Kategorienamen \ hinzu, um eine Ordnerhierarchie zu erstellen. Sie können beispielsweise Anwendungen nach Typ gruppieren oder alternativ Ordner für verschiedene Benutzerrollen in Ihrer Organisation erstellen. Auf der Registerkarte **Apps** der Store-Website werden unter **Kategorie** die einzelnen Kategorien und die Apps in jeder Kategorie aufgelistet.

Schlüsselwörter

Sie können Schlüsselwörter für eine App oder einen Desktop hinzufügen, indem Sie die Zeichenfolge `KEYWORDS:[keywordname]` an die Anwendungsbeschreibung anhängen. Mehrere Schlüsselwörter müssen ausschließlich durch Leerzeichen voneinander getrennt werden, z. B. `KEYWORDS:Accounts Featured`. Schlüsselwörter können auf verschiedene Weise verwendet werden:

- Zum Filtern von Anwendungen (siehe Erweiterte Storeeinstellungen).
- Zum Erstellen von App-Gruppen mit Highlights.
- Manche Schlüsselwörter haben spezielle Bedeutungen.

Schlüsselwortname	Beschreibung
Erforderlich	Fügt der Registerkarte “Home”eine Anwendung hinzu. Anders als bei Favoriten können Benutzer erforderliche Anwendungen nicht von der Registerkarte “Home”entfernen. Unwirksam, wenn Favoriten für den Store deaktiviert sind.
Automatisch	Wenn sich die Benutzer beim Store anmelden, wird die Anwendung automatisch als Favorit markiert und ihrer Home-Registerkarte hinzugefügt. Die Benutzer können solche Anwendungen als Favoriten abwählen. Unwirksam, wenn Favoriten für den Store deaktiviert sind.
TreatAsApp	Hiermit wird festgelegt, dass StoreFront den Desktop als App behandelt. Er wird dann auf der Registerkarte **Apps** und nicht auf der Registerkarte **Desktops** angezeigt. Außerdem wird der Desktop nicht automatisch gestartet, wenn sich der Benutzer an der Store-Website anmeldet, und er wird nicht mit Desktop Viewer aufgerufen, selbst wenn die Site so konfiguriert wurde, dass dies bei anderen Desktops der Fall ist.
prefer=”*application*“	*application* steht hierbei für eine lokal installierte Anwendung. Gilt nur für die Citrix Workspace-App unter Windows. Hiermit können Sie festlegen, dass die lokal installierte Version einer Anwendung bevorzugt vor einer übermittelten Instanz verwendet wird, wenn beide verfügbar sind. Weitere Informationen finden Sie unter Konfigurieren von lokalem App-Zugriff für Anwendungen.
Primary und **Secondary**	Bei Verwendung der Multisiteaggregation werden Ressourcen mit angehängtem Schlüsselwort **primary** der Version mit dem Schlüsselwort **secondary** vorgezogen.

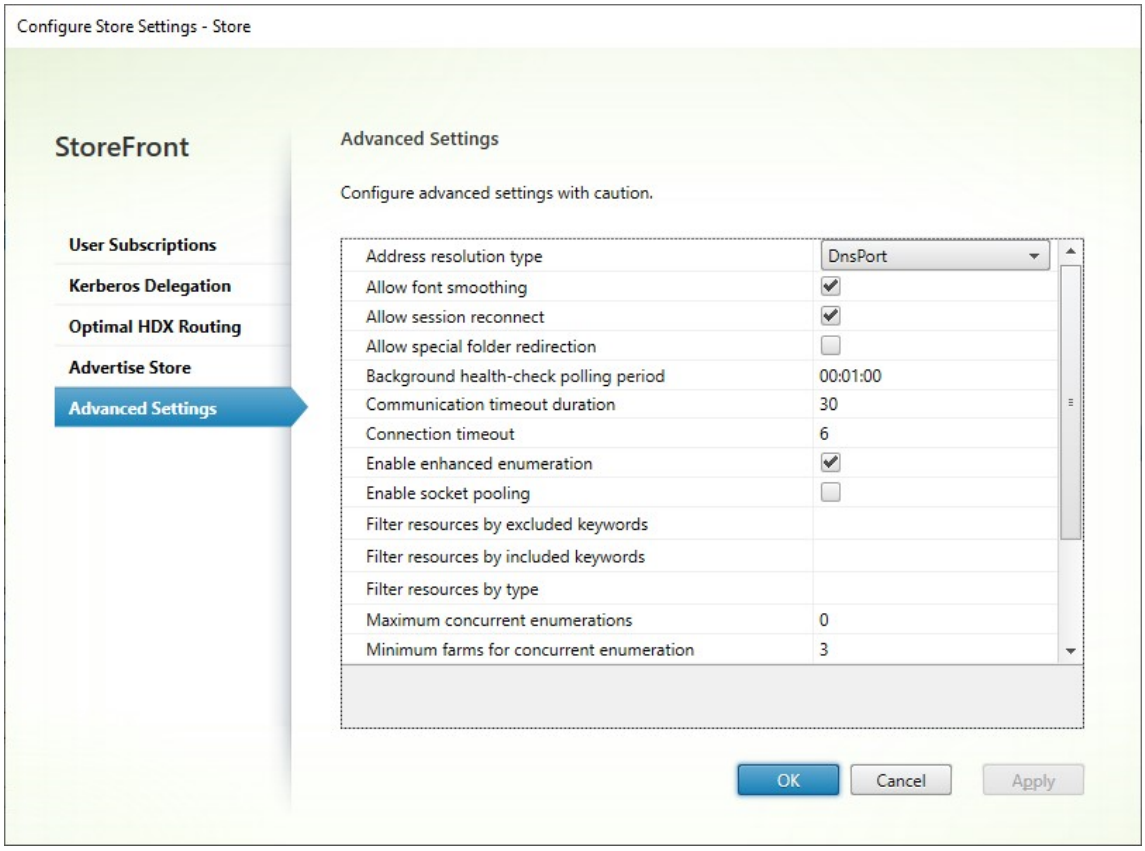
Erweiterte Storeeinstellungen

April 17, 2024

Sie können die meisten erweiterten Storeeigenschaften über “Erweiterte Einstellungen”auf der Seite “Storeeinstellungen konfigurieren”festlegen. Einige Einstellungen können nur mit PowerShell geändert werden.

> **Wichtig:**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss verteilen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten “Stores”und im mittleren Bereich den Store aus und wählen Sie dann im Aktionsbereich **Storeeinstellungen konfigurieren** aus.
2. Wählen Sie auf der Seite **Storeeinstellungen konfigurieren** die Option **Erweiterte Einstellungen** und nehmen Sie die erforderlichen Änderungen vor.



3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Adressauflösungstyp

Sie können den Adresstyp angeben, der vom Server angefordert werden soll. Der Standardwert ist "DnsPort".

Wählen Sie im Fenster **Erweiterte Einstellungen** eine Option in der Dropdownliste **Adressauflösungstyp**.

- Dns
- DnsPort
- IPV4
- IPV4Port
- Dot
- DotPort
- Uri
- NoChange

Schriftartenglättung zulassen

Sie können festlegen, ob bei HDX-Sitzungen die Schriftglättung verwendet werden soll. Die Standardeinstellung ist Ein.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Schriftglättung zulassen** und klicken Sie auf **OK**.

Sitzungswiederverbindung zulassen

Sie können festlegen, ob HDX-Sitzungen wieder verbunden werden sollen. Die Standardeinstellung ist Ein.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Sitzungswiederverbindung zulassen**.

Umleitung spezieller Ordner zulassen

Wenn die Umleitung spezieller Ordner konfiguriert ist, können Benutzer spezielle Windows-Ordner auf dem Server den Ordnern auf ihrem lokalen Computer zuordnen. Unter speziellen Ordner versteht man Windows-Standardordner, z. B. *Dokumente* oder *Desktop*, die unabhängig vom Betriebssystem immer gleich angezeigt werden.

Aktivieren oder deaktivieren Sie im Fenster **Erweiterte Einstellungen** die Option **Umleitung spezieller Ordner zulassen** und klicken Sie auf **OK**.

Erweiterte Integritätsprüfung

StoreFront führt regelmäßig Systemdiagnosen an jedem Delivery Controller und Cloud Connector von Citrix Virtual Apps and Desktops durch, um Probleme durch zeitweilige Serverausfälle zu vermindern. Die erweiterte Integritätsprüfung in StoreFront ist eine eingehendere Prüfung, bei der Probleme mit größerer Wahrscheinlichkeit erkannt werden.

Wenn Sie über einen Cloud Connector eine Verbindung zu Citrix Desktops as a Service herstellen, bietet die erweiterte Integritätsprüfung den zusätzlichen Vorteil, dass sie Informationen darüber abruft, welche VDAs sich am selben Ort wie der Cloud Connector befinden. Falls die Cloud Connectors Citrix Desktops as a Service nicht kontaktieren können, verwenden sie ihren lokalen Hostcache, um Verbindungen zu VDAs am selben Ort zu ermöglichen. StoreFront verwendet die zusätzlichen Informationen aus den Ergebnissen der erweiterten Integritätsprüfung, um den bestgeeigneten Online-Connector zum Starten von Apps und Desktops zu kontaktieren.

Um die Ressourcenverfügbarkeit während eines Ausfalls sicherzustellen, ohne Ressourcen in jeder Zone (Ressourcenstandort) veröffentlichen zu müssen, konfigurieren Sie auf allen StoreFront-Servern den Ressourcenfeed so, dass er alle Cloud Connectors an allen Ressourcenstandorten einschließt, und aktivieren Sie die erweiterte Integritätsprüfung.

Die erweiterte Integritätsprüfung standardmäßig aktiviert Citrix empfiehlt, dass Sie die erweiterte Integritätsprüfung in allen StoreFront-Bereitstellungen aktivieren. Um die erweiterte Systemintegritätsprüfung zu aktivieren, verwenden Sie den PowerShell-Befehl Set-STFStoreFarmConfiguration. Beispiel:

```
$storeService = Get-STFStoreService –VirtualPath '/Citrix/Store'
Set-STFStoreFarmConfiguration $storeService -AdvancedHealthCheck $true
<!--NeedCopy-->
```

Intervall für Hintergrundsystemdiagnose

StoreFront führt regelmäßig Systemdiagnosen an jedem Delivery Controller und Cloud Connector von Citrix Virtual Apps and Desktops durch, um Probleme durch zeitweilige Serverausfälle zu vermindern. Die Standardeinstellung ist jede Minute (00:01:00). Geben Sie im Fenster **Erweiterte Einstellungen** eine Zeit für Abfragezeit für **Systemdiagnose im Hintergrund** ein und klicken Sie auf **OK**, um die Häufigkeit der Diagnosen zu steuern. Es wird nicht empfohlen, den Abfragezeitraum auf einen niedrigen Wert einzustellen, wenn die Erweiterte Integritätsprüfung aktiviert ist, da dies Auswirkungen auf die Leistung haben kann.

Kommunikationstimeoutdauer

Standardmäßig ist das Timeout für Anforderungen von StoreFront an den Server, der die Ressourcen für einen Store bereitstellt, 30 Sekunden. Der Server gilt als nicht verfügbar, wenn 1 Kommunikationsversuch gescheitert ist. Ändern Sie im Fenster **Erweiterte Einstellungen** die Standardzeit nach Bedarf und klicken Sie auf **OK**.

Verbindungstimeout

Sie können die Zeit in Sekunden festlegen, die beim Herstellen einer ersten Verbindung mit einem Delivery Controller gewartet werden soll. Die Standardeinstellung ist 6.

Geben Sie im Fenster **Erweiterte Einstellungen** die Zeitdauer in Sekunden ein, die beim Herstellen der ersten Verbindung gewartet werden soll, und klicken Sie auf **OK**.

Erweiterte Enumeration aktivieren

Diese Option steuert, ob StoreFront die Delivery Controller gleichzeitig oder sequentiell abfragt, wenn Apps und Desktops über mehrere Citrix Virtual Apps and Desktops-Sites hinweg enumeriert werden. Die gleichzeitige Enumerierung bietet schnellere Antworten auf Benutzerabfragen, wenn Ressourcen über mehrere Sites hinweg aggregiert werden. Wenn diese Option ausgewählt ist (Standardeinstellung), sendet StoreFront gleichzeitig Enumerierungsanforderungen an alle Delivery Controller und aggregiert Antworten, wenn sie alle geantwortet haben. Sie können die Optionen **Maximum gleichzeitiger Enumerationen** und **Minimum Farmen für gleichzeitige Enumeration** verwenden, um dieses Verhalten zu optimieren.

Aktivieren oder deaktivieren Sie im Fenster **Erweiterte Einstellungen** die Option **Erweiterte Enumeration aktivieren** und klicken Sie auf **OK**.

Socketpooling aktivieren

Socketpooling ist in Stores standardmäßig deaktiviert. Ist Socketpooling aktiviert, verwaltet StoreFront einen Socketpool, anstatt Sockets jedes Mal neu zu erstellen und die Sockets beim Trennen der Verbindung an das Betriebssystem zurückzugeben. Das Aktivieren von Socketpooling verbessert die Leistung, besonders für SSL-Verbindungen (Secure Sockets Layer). Bearbeiten Sie die Storekonfigurationsdatei, um Socketpooling zu aktivieren. Aktivieren Sie im Fenster **Erweiterte Einstellungen** die Option **Socketpooling aktivieren** und klicken Sie auf **OK**.

Dateitypzuordnungen

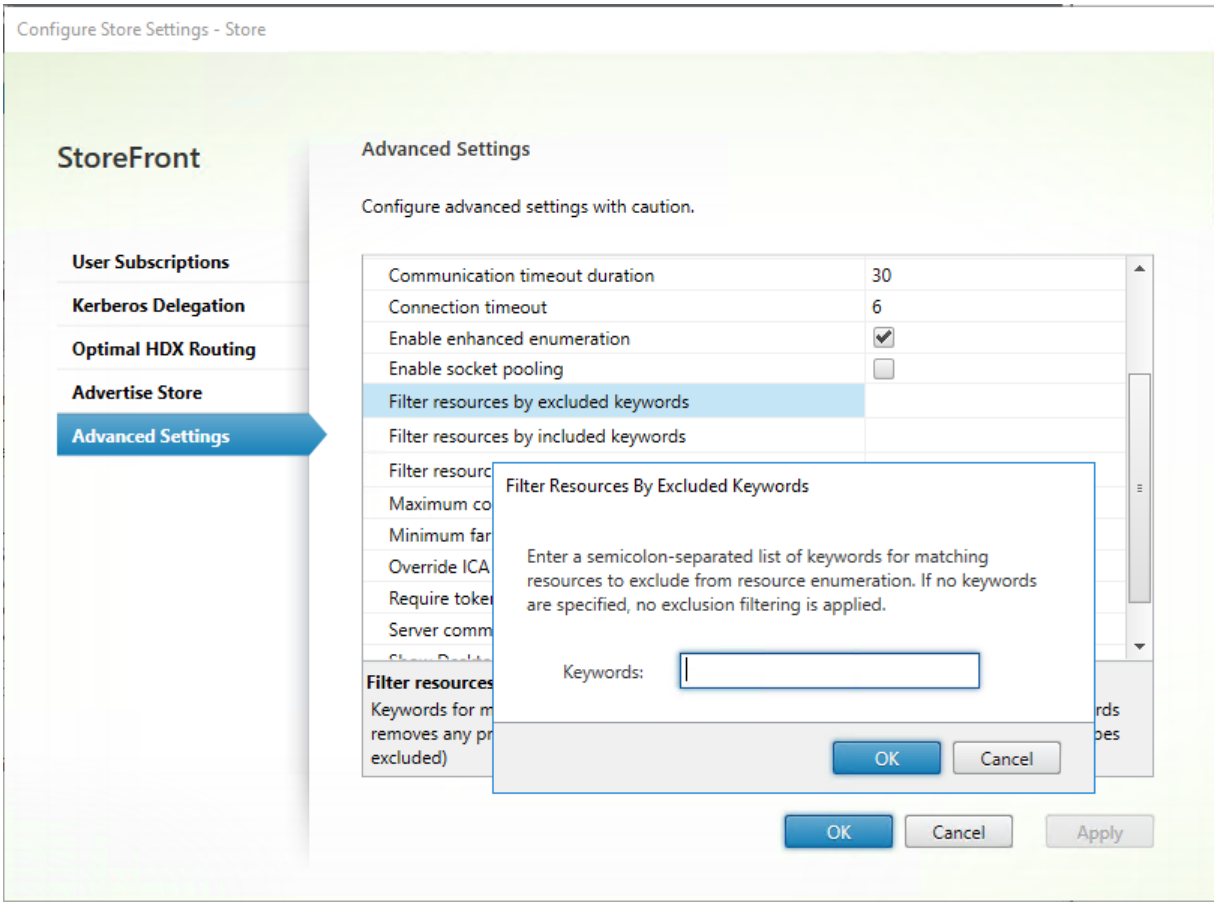
Standardmäßig ist die Dateitypzuordnung in Stores aktiviert, damit Inhalte nahtlos an die abonnierten Anwendungen der Benutzer umgeleitet werden, wenn sie lokale Dateien der entsprechenden Typen öffnen. Verwenden Sie den PowerShell-Befehl Set-STFStoreFarmConfiguration, um die Dateitypzuordnung zu aktivieren oder zu deaktivieren. Beispiel:

```
1 $storeService = Get-STFStoreService –VirtualPath '/Citrix/Store'
2 Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
     $false
3 <!--NeedCopy-->
```

Ressourcen nach Ausschlussschlüsselwörtern filtern

Sie können Ressourcen nach Ausschlussschlüsselwörtern filtern. Durch das Festlegen von Ausschlussschlüsselwörtern werden zuvor konfigurierte Einschlussschlüsselwörter entfernt. Der Standardwert ist “Kein Filtern (alle Ressourcentypen eingeschlossen)”.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Ressourcen nach Ausschlussschlüsselwörtern filtern**, klicken Sie rechts daneben, geben Sie die Schlüsselwörter durch Semikola getrennt ein und klicken Sie auf **OK**.



Um die Einstellung mithilfe von PowerShell zu ändern, verwenden Sie das Cmdlet Set-STFStoreEnumerationOption mit dem Parameter `-FilterByKeywordsExclude`.

Die folgenden Schlüsselwörter sind reserviert und dürfen nicht zum Filtern verwendet werden:

- Automatisch
- Erforderlich

Ressourcen nach Einschlussschlüsselwörtern filtern

Sie können Ressourcen nach Einschlussschlüsselwörtern filtern. Durch das Festlegen von Einschlussschlüsselwörtern werden zuvor konfigurierte Ausschlussschlüsselwörter entfernt. Der Standardwert ist "Kein Filtern (alle Ressourcentypen eingeschlossen)".

1. Suchen Sie im Fenster **Erweiterte Einstellungen** nach der Zeile **Ressourcen nach Einschlussschlüsselwörtern filtern**.
2. Klicken Sie in die rechte Spalte, um das Fenster **Ressourcen nach Einschlussschlüsselwörtern filtern** aufzurufen.
3. Geben Sie eine durch Semikolons getrennte Liste von Schlüsselwörtern ein.
4. Klicken Sie auf **OK**.

Um die Einstellung mithilfe von PowerShell zu ändern, verwenden Sie das Cmdlet Set-STFStoreEnumerationOption mit dem Parameter `-FilterByKeywordsInclude`.

Die folgenden Schlüsselwörter sind reserviert und dürfen nicht zum Filtern verwendet werden:

- Automatisch
- Erforderlich

Ressourcen nach Typ filtern

Wählen Sie die Ressourcentypen, die bei der Enumeration der Ressourcen berücksichtigt werden sollen. Der Standardwert ist "Kein Filtern (alle Ressourcentypen eingeschlossen)".

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Ressourcen nach Typ filtern**, klicken Sie rechts daneben, wählen Sie die Ressourcentypen für die Enumeration aus und klicken Sie auf **OK**.

Um die Einstellung mithilfe von PowerShell zu ändern, verwenden Sie das Cmdlet Set-STFStoreEnumerationOption mit dem Parameter `-FilterByTypesInclude` unter Angabe eines Ressourcentypenarrays (Anwendungen, Desktops oder Dokumente).

Maximum gleichzeitiger Enumerationen

Legen Sie fest, wie viele Anforderungen gleichzeitig an alle Delivery Controller gesendet werden sollen. Diese Option wird wirksam, wenn die Option **Erweiterte Enumeration aktivieren** aktiviert ist. Der Standardwert ist 0 (kein Maximum).

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Maximum gleichzeitiger Enumerationen**, geben Sie einen Zahlenwert ein und klicken Sie auf **OK**.

Minimum Farmen für gleichzeitige Enumeration

Geben Sie die Mindestanzahl von Delivery Controllern an, die erforderlich sind, um die gleichzeitige Enumeration auszulösen. Diese Option wird wirksam, wenn die Option **Erweiterte Enumeration aktivieren** aktiviert ist. Der Standardwert ist 3.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Minimum Farmen für gleichzeitige Enumeration**, geben Sie einen Zahlenwert ein und klicken Sie auf **OK**.

ICA-Clientnamen überschreiben

Durch diese Option wird der Clientname in der ICA-Startdatei durch eine vom Webbrowser generierte eindeutige ID ersetzt. Wenn die Option deaktiviert ist, wird der Clientname der Citrix Workspace-App festgelegt. Die Standardeinstellung ist "Aus".

Aktivieren Sie im Fenster **Erweiterte Einstellungen** die Option **ICA-Clientnamen überschreiben** und klicken Sie auf **OK**.

Tokenkonsistenz erforderlich

Ist diese Option aktiviert, erzwingt StoreFront Konsistenz zwischen dem für die Authentifizierung verwendeten Gateway und dem für den Zugriff auf den Store verwendeten Gateway. Sind diese Werte nicht konsistent, müssen die Benutzer eine erneute Authentifizierung durchführen. Sie müssen diese Option für Smart Access aktivieren. Sie müssen sie deaktivieren, wenn die Benutzer über ein Gateway mit deaktivierter Authentifizierung auf den Store zugreifen. Die Standardeinstellung ist Ein.

Aktivieren Sie im Fenster **Erweiterte Einstellungen** die Option **Tokenkonsistenz erforderlich** und klicken Sie auf **OK**.

Serverkommunikationsversuche

Legen Sie die Anzahl der Kommunikationsversuche mit Delivery Controllern fest, bevor diese als nicht verfügbar markiert werden. Der Standardwert ist 1.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Serverkommunikationsversuche**, geben Sie einen Zahlenwert ein und klicken Sie auf **OK**.

Desktop Viewer für Legacyclients anzeigen

Legen Sie fest, ob Fenster und Symbolleiste von Citrix Desktop Viewer angezeigt werden sollen, wenn Benutzer von Legacyclients aus auf ihre Desktops zugreifen. Die Standardeinstellung ist "Aus".

Aktivieren Sie im Fenster **Erweiterte Einstellungen** die Option **Desktop Viewer für Legacyclients anzeigen** und klicken Sie auf **OK**.

Desktops wie Apps behandeln

Geben Sie an, ob Desktops beim Zugriff auf den Store in der Ansicht "Apps"und nicht in der Ansicht "Desktops"angezeigt werden. Die Standardeinstellung ist "Aus".

Aktivieren Sie im Fenster **Erweiterte Einstellungen** die Option **Desktops wie Apps behandeln** und klicken Sie auf **OK**.

Konfigurieren des optimalen HDX-Routings für einen Store

April 17, 2024

Konfigurieren Sie mit StoreFront das optimale Citrix Gateway-Routing zum Optimieren der Handhabung von ICA-Verbindungsrouting von der HDX Engine mit per Citrix Virtual Apps and Desktops veröffentlichten Anwendungen. In der Regel ist das optimale Gateway für eine Site am selben geografischen Standort.

Sie müssen optimale Citrix Gateway-Geräte für Bereitstellungen nur definieren, wenn das Gerät, über das die Benutzer auf StoreFront zugreifen, nicht das optimale Gateway ist. Wenn Starts über das Gateway, das die Startanforderung durchführt, zurückgeleitet werden sollen, macht StoreFront das automatisch.

Sie können Gateways Delivery Controllern oder Zonen zuordnen. Eine Zone ist eine Gruppierung von Delivery Controllern und repräsentiert normalerweise ein Datencenter an einem geografischen Standort. Zonen werden in StoreFront definiert und müssen genau mit den in Citrix Virtual Apps and Desktops definierten Zonennamen übereinstimmen. Ein optimales Gateway kann mehr als einer Zone zugeordnet werden, aber es empfiehlt sich, nur eine Zone zu verwenden. Eine Zone repräsentiert normalerweise ein Datencenter an einem geografischen Standort. Es wird erwartet, dass jede Zone mindestens ein optimales Citrix Gateway hat, das für HDX-Verbindungen mit Ressourcen in der Zone verwendet wird.

Weitere Informationen zu Zonen finden Sie unter Zonen.

Beispielszenario mit Farmen

1 x UK-Gateway –> 1 x UK-StoreFront

- UK-lokale Apps und Desktops
- US Apps und Desktops ausschließlich für UK-Failover

1 x US-Gateway–> 1 x US-StoreFront

- US-lokale Apps und Desktops
- UK Apps und Desktops ausschließlich für US-Failover

Ein UK-Gateway bietet Remotezugriff auf gehostete Ressourcen wie Apps und Desktops über UK-StoreFront.

UK-StoreFront hat ein UK-basiertes und ein US-basiertes Citrix Gateway definiert und UK- und US-Controller in der Delivery Controller-Liste. UK-Benutzer greifen über den Gateway, StoreFront und die Farmen, die sich am selben Standort befinden, auf Remoteressourcen zu. Wenn kein Zugriff auf die UK-Ressourcen möglich ist, können sie als temporäre Failoverlösung auf US-Ressourcen zugreifen.

Ohne optimales Gatewayrouting würden alle ICA-Starts über das UK-Gateway geleitet, das die Startanforderung stellte, unabhängig vom geografischen Standort der Ressourcen. Standardmäßig werden die für die Startanforderungen verwendeten Gateways dynamisch von StoreFront identifiziert, wenn die Anforderung gestellt wird. Das optimale Gateway-Routing überschreibt die Standardeinstellung und erzwingt die Leitung von US-Verbindungen über das Gateway, das den US-Farmen, die die Apps und Desktops verfügbar machen, am nächsten ist.

> **Hinweis:**
>
> Sie können für einen StoreFront-Store nur einen optimalen Gateway pro Site zuordnen.

Beispielszenario mit Zonen

1 x CAMZone -> 2 x UK-StoreFronts

- Cambridge, UK: Apps und Desktops
- Fort Lauderdale, US-Osten: Apps und Desktops
- Bangalore, Indien: Apps und Desktops

1 x FTLZone -> 2 x USA-StoreFronts

- Fort Lauderdale, US-Osten: Apps und Desktops
- Cambridge, UK: Apps und Desktops
- Bangalore, Indien: Apps und Desktops

1 x BGLZone -> 2 x IN-StoreFronts

- Bangalore, Indien: Apps und Desktops
- Cambridge, UK: Apps und Desktops
- Fort Lauderdale, US-Osten: Apps und Desktops

Abbildung 1. Suboptimales Gatewayrouting

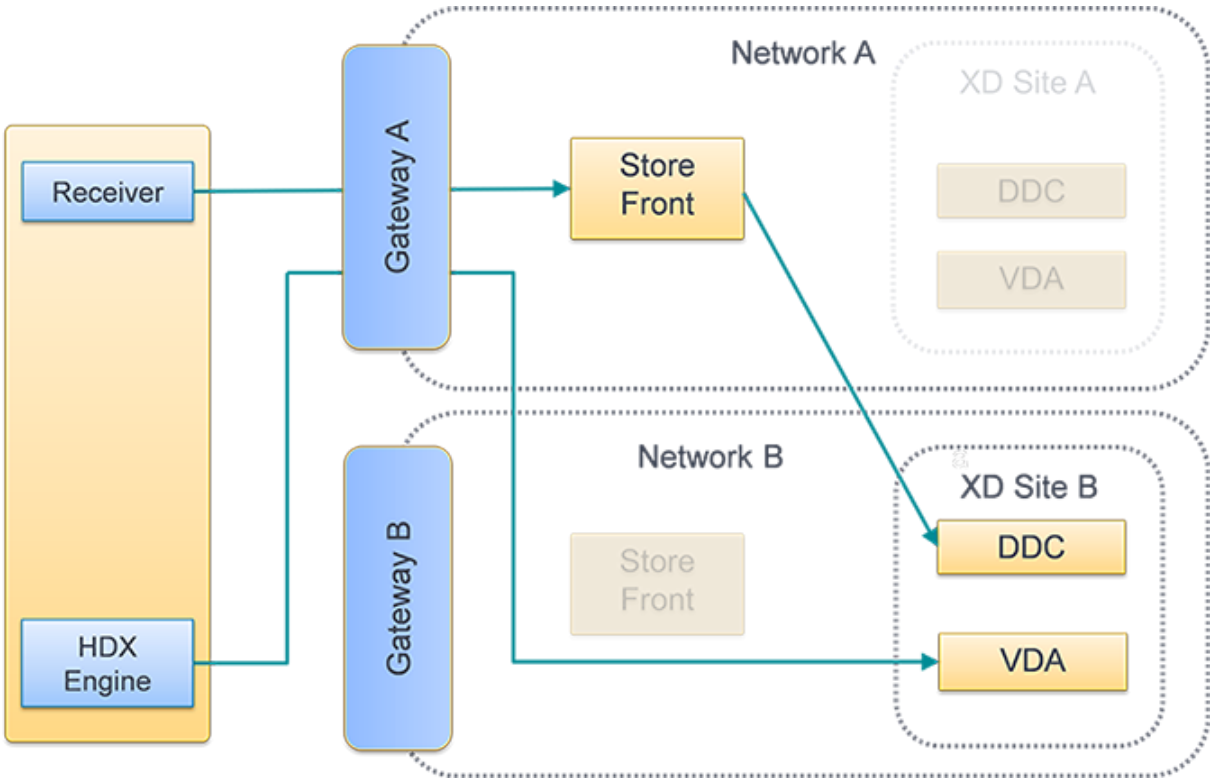
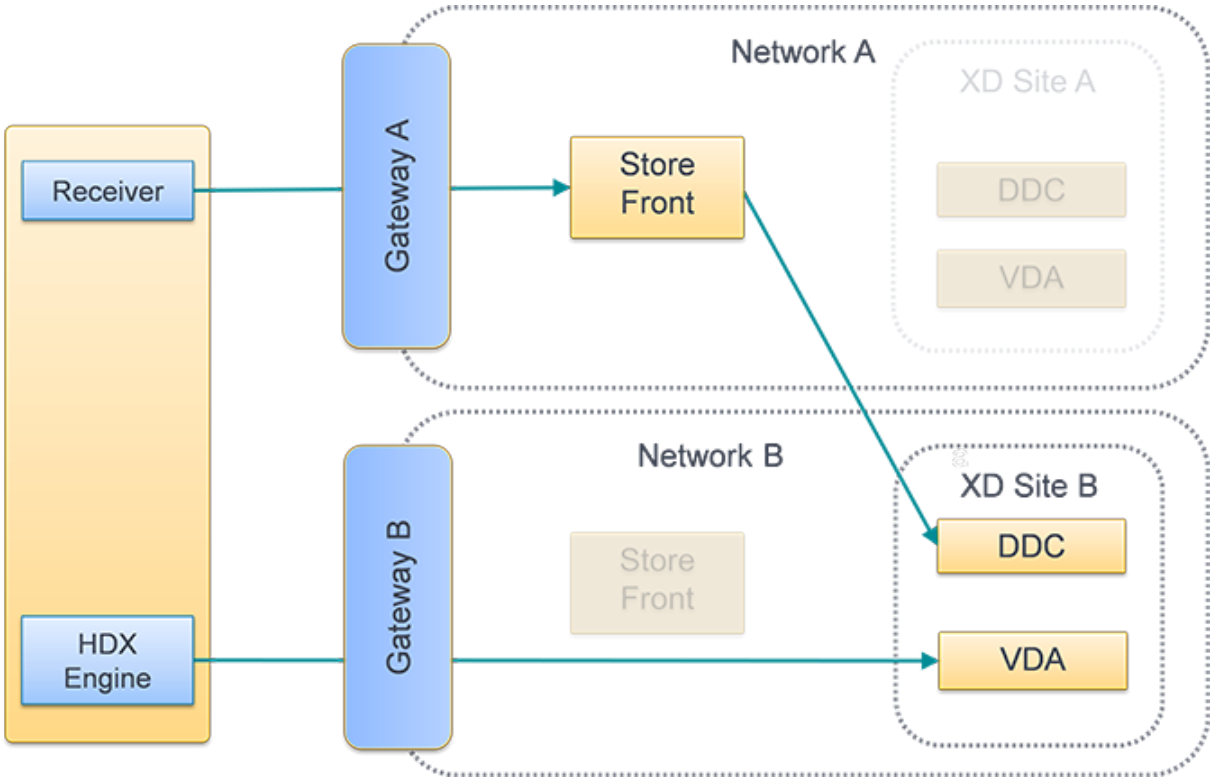


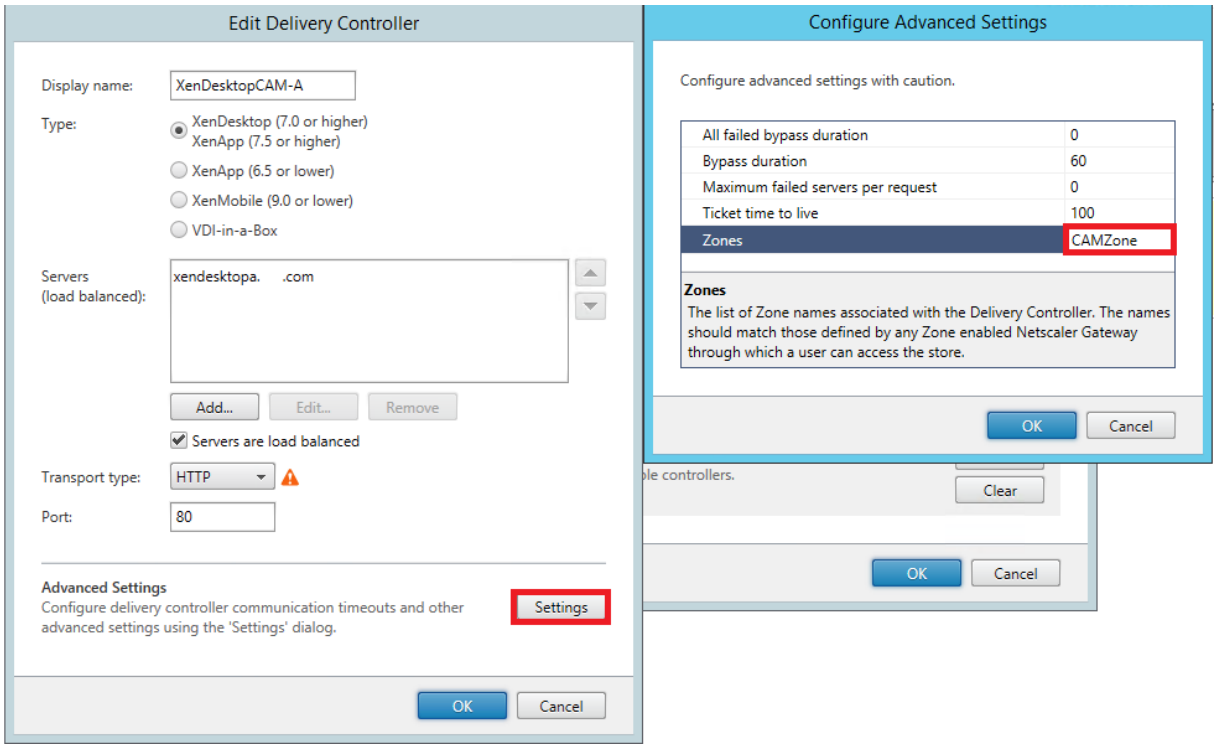
Abbildung 2. Optimales Gatewayrouting



Platzieren eines Delivery Controllers in einer Zone

Legen Sie das Zonenattribut auf jedem Delivery Controller fest, den Sie in einer Zone platzieren.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie auf **Delivery Controller verwalten** im Bereich **Aktionen**.
2. Wählen Sie einen Controller aus, klicken Sie auf **Bearbeiten** und dann auf **Einstellungen** auf dem Bildschirm **Delivery Controller bearbeiten**.
3. Klicken Sie in der Zeile **Zonen** auf die zweite Spalte.
4. Klicken Sie im Bildschirm **Delivery Controller-Zonennamen** auf **Hinzufügen** und fügen Sie einen Zonennamen hinzu.



Optimales HDX-Routing konfigurieren

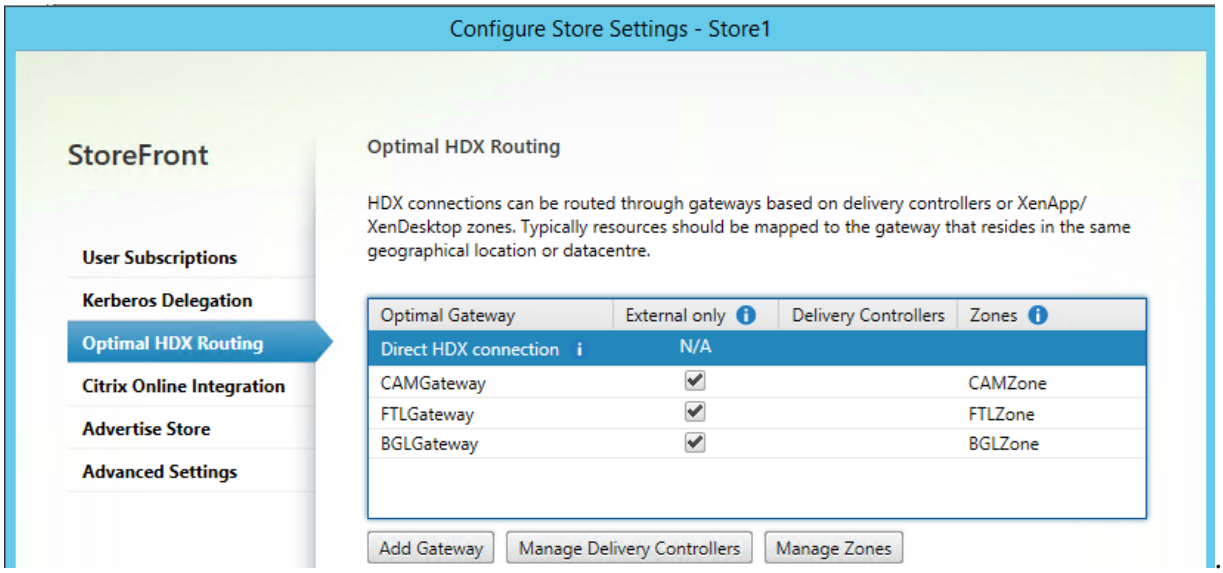
1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren**.
2. Wählen Sie die Registerkarte **Optimales HDX-Routing**.
3. Wählen Sie ein Gateway aus.

    a) Um das Gateway beim Zugriff auf Ressourcen von bestimmten Delivery Controllern zu verwenden, klicken Sie auf **Delivery Controller verwalten** und markieren Sie einen oder mehrere Delivery Controller.

b) Um das Gateway beim Zugriff auf Ressourcen von einer Gruppe von Delivery Controllern in einer Zone zu verwenden, klicken Sie auf **Zonen verwalten** und geben Sie eine oder mehrere Zonen ein.

c) Sobald Sie einen Delivery Controller oder eine Zone hinzufügen, wird standardmäßig **Nur externe** aktiviert, sodass StoreFront das Gateway nur zum Starten von StoreFront für Benutzer verwendet, die über ein Gateway mit StoreFront verbunden sind. Wenn Sie das Gateway auch zum Starten von Ressourcen für Benutzer verwenden möchten, die eine direkte Verbindung mit StoreFront ein Gateway hergestellt haben, deaktivieren Sie das Kontrollkästchen **Nur externe**.

4. Wenn Sie selbst für Benutzer, die remote über ein Gateway auf StoreFront zugreifen, immer eine direkte Verbindung zu bestimmten Ressourcen ohne Gateway hergestellt werden soll, wählen Sie **Direkte HDX-Verbindung** und dann einige Delivery Controller oder Zonen.



Konfigurieren des optimalen Citrix Gateway-Routings für einen Store mit PowerShell

- Um das optimale Gateway-Routing für einen Store zu konfigurieren, verwenden Sie Register-STFStoreOptimalLaunchGateway.
- Um das optimale Gateway-Routing für einen Store zu entfernen verwenden Sie Unregister-STFStoreOptimalLaunchGateway.
- Um das optimale Routing für einen Store anzuzeigen, verwenden Sie Get-STFStoreRegisteredOptimalLaunch

Abonnementsynchronisierung

April 17, 2024

StoreFront synchronisiert automatisch Abonnements zwischen Servern in StoreFront-Servergruppen. Wenn Sie über mehrere Servergruppen verfügen (in der Regel an unterschiedlichen geografischen Standorten), können Sie die regelmäßige Pullsynchronisierung von Benutzerabonnements aus Stores in verschiedenen StoreFront-Bereitstellungen konfigurieren. Dafür muss PowerShell verwendet werden.

> **Hinweis:**
>
> Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer zuerst die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zum Verwalten der StoreFront-Konfiguration öffnen. Schließen Sie gleichermaßen immer alle Instanzen von PowerShell, bevor Sie die StoreFront-Konsole öffnen.

Für die Abonnementsynchronisierung müssen die konfigurierten Delivery Controller der synchronisierten Stores identische Namen (einschl. Groß- und Kleinschreibung) haben. Wenn die Namen der Delivery Controller nicht identisch sind, haben Benutzer in den synchronisierten Stores möglicherweise unterschiedliche Abonnements. Wenn Sie Abonnements aus aggregierten Ressourcen synchronisieren, müssen auch die von beiden Stores verwendeten Name der Aggregationsgruppen übereinstimmen. Bei Namen von Delivery Controllern und Aggregationsgruppen wird zwischen Groß- und Kleinschreibung unterschieden. Beispiel: *CVAD_US* wird von *Cvad_Us* unterschieden.

1. Verwenden Sie ein Konto mit lokalen Administratorberechtigungen, um Windows PowerShell ISE zu starten.
2. Verwenden Sie den Befehl Publish-STFServerGroupConfiguration, um die Synchronisierung zu konfigurieren. Sie können entweder eine Startzeit und ein Wiederholintervall oder eine Liste von Zeiten angeben. Beispiel, um die Synchronisierung um 08:00 Uhr zu beginnen und alle 30 Minuten zu wiederholen:

   ```
   Add-STFSubscriptionSynchronizationSchedule -RecurringStartTime
      08:00:00 -RecurringInterval 30
   <!--NeedCopy-->
   ```

   Es wird empfohlen, Abrufzeitpläne zu staffeln, um zu vermeiden, dass zwei Servergruppen gleichzeitig Abonnementdaten voneinander abrufen. Beispielsweise würde ein Zeitplan zum Abrufen von Daten aus jeder Servergruppe alle 60 Minuten wie folgt konfiguriert. Servergruppe 1 ruft Daten aus Servergruppe 2 um 01:00, 02:00, 03:00 usw. ab. Servergruppe 2 ruft Daten aus Servergruppe 1 um 01:30, 02:30, 03:30 usw. ab.

3. Geben Sie den folgenden Befehl ein, um die Remoteimplementierung von StoreFront anzugeben, die den zu synchronisierenden Store enthält. Sie müssen dies für jedes Datencenter konfigurieren, in dem sich eine StoreFront-Servergruppe befindet, damit Abonnementdaten aus anderen Remotedatencentern abgerufen werden können. Siehe folgende Beispiele für Datencenter in den USA und Großbritannien:

   - Befehl für StoreFront-Server im US-Datencenter, um Daten von den britischen Servern abzurufen:

     ```
     $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
         Citrix/Store"
     Add-STFSubscriptionSynchronizationSource -FriendlyName "
         SyncFromUKStore" -StoreService $StoreObject -
         RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.
         com"
     <!--NeedCopy-->
     ```

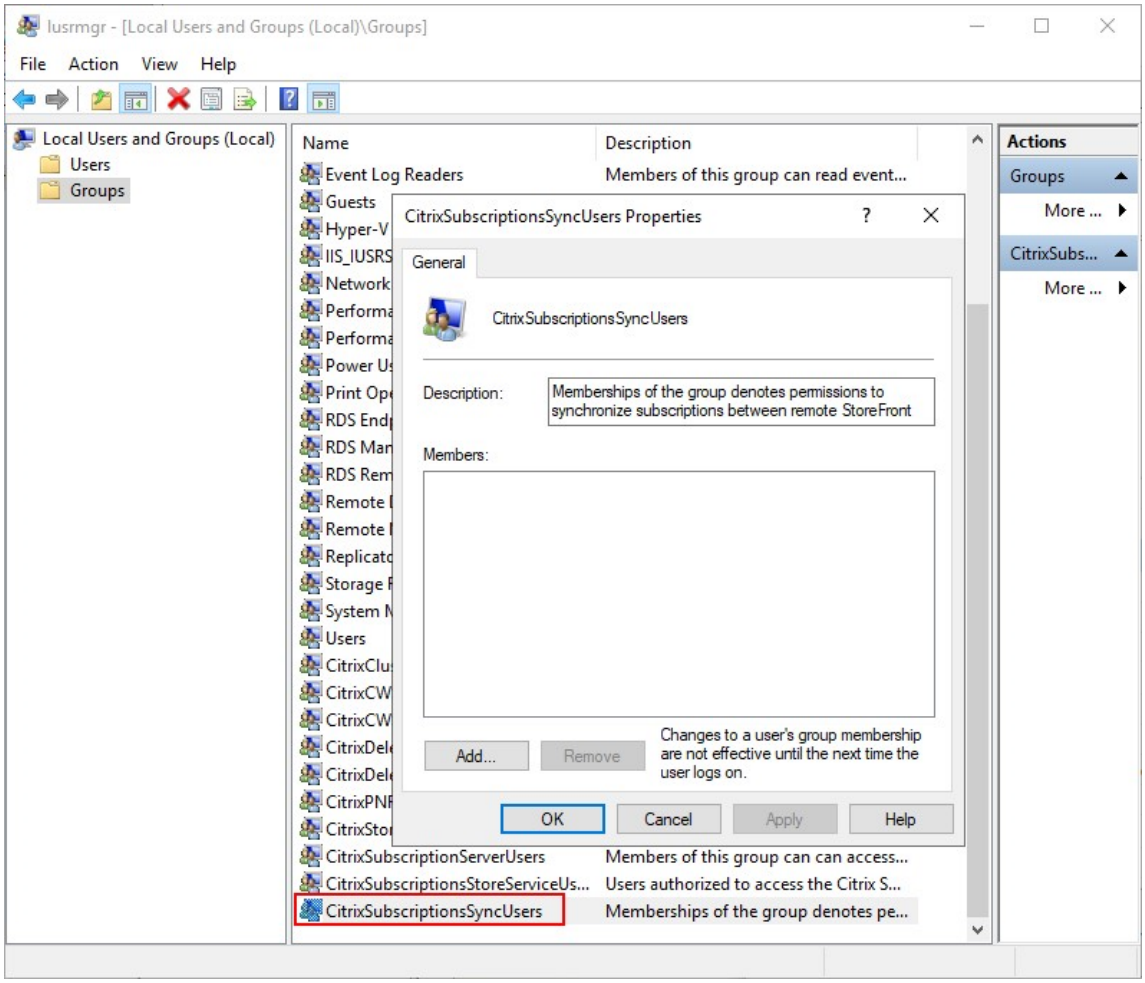
   - Befehl für StoreFront-Server im britischen Datencenter, um Daten von den US-Servern abzurufen:

     ```
     $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
         Citrix/Store"
     Add-STFSubscriptionSynchronizationSource -FriendlyName "
         SyncFromUSStore" -StoreService $StoreObject -
         RemoteStoreFrontAddress "USloadbalancedStoreFront.example.
         com"
     <!--NeedCopy-->
     ```

   FriendlyName ist ein Name zum Identifizieren der Remotebereitstellung und *RemoteStoreFrontAddress* ist der FQDN des StoreFront-Servers oder der Lastausgleichsservergruppe für die Remotebereitstellung. Anwendungsabonnements zwischen zwei oder mehr Stores können nur synchronisiert werden, wenn die Namen aller Stores in den jeweiligen StoreFront-Bereitstellungen übereinstimmen.

4. Fügen Sie die Microsoft Active Directory-Domänencomputerkonten für jeden StoreFront-Server in der Remotebereitstellung der lokalen Windows-Benutzergruppe CitrixSubscriptionSyncUsers auf dem aktuellen Server hinzu.

   So können die aktuellen Server neue oder aktualisierte Abonnementdaten von den in CitrixSubscriptionSyncUsers aufgeführten Remoteservern abrufen, sobald Sie einen Synchronisierungszeitplan konfiguriert haben. Weitere Informationen zum Ändern lokaler Benutzergruppen finden Sie unter https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11).



5. Wenn Sie den Zeitplan wie gewünscht konfiguriert haben, verwenden Sie die Citrix StoreFront-Verwaltungskonsole oder das PowerShell-Skript unten, um die Synchronisierungszeitpläne und -quellen auf alle anderen Server in der Gruppe zu verteilen.

```
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

   Weitere Informationen über die Übertragung von Änderungen in einer StoreFront-Multiserverbereitstellung finden Sie unter Konfigurieren von Servergruppen.

6. Um einen vorhandenen Abonnementsynchronisierungszeitplan zu entfernen, führen Sie den folgenden Befehl aus und verteilen Sie dann die Konfigurationsänderungen auf die anderen StoreFront-Server in der Bereitstellung.

```
Clear-STFSubscriptionSynchronizationSchedule
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

7. Um eine spezifische Abonnementsynchronisierungsquelle zu entfernen, führen Sie den folgenden Befehl aus und verteilen Sie dann die Konfigurationsänderungen auf die anderen

StoreFront-Server in der Bereitstellung.

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUKStore"
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

8. Um alle Abonnementsynchronisierungsquellen zu entfernen, führen Sie den folgenden Befehl aus und verteilen Sie dann die Konfigurationsänderungen auf die anderen StoreFront-Server in der Bereitstellung.

```
Clear-STFSubscriptionSynchronizationSource
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

9. Führen Sie den folgenden Befehl aus, um die derzeit für Ihre StoreFront-Bereitstellung konfigurierten Abonnementsynchronisierungszeitpläne aufzulisten.

```
Get-STFSubscriptionSynchronizationSchedule
<!--NeedCopy-->
```

10. Führen Sie den folgenden Befehl aus, um die derzeit für Ihre StoreFront-Bereitstellung konfigurierten Abonnementsynchronisierungsquellen aufzulisten.

```
Get-STFSubscriptionSynchronizationSource
<!--NeedCopy-->
```

Sitzungseinstellungen konfigurieren

April 17, 2024

Wenn ein Benutzer eine Anwendung startet, generiert StoreFront ein Dokument (eine sogenannte ICA-Datei), das alle Einstellungen enthält, die die Citrix Workspace-App zum Starten und Konfigurieren der Sitzung benötigt.

In den meisten Fällen wird empfohlen, die Sitzungseinstellungen mit Citrix Virtual Apps and Desktops-Richtlinien oder Citrix DaaS-Richtlinien zu ändern. In einigen Fällen ist es jedoch sinnvoll, diese Einstellungen für einen bestimmten Store zu überschreiben. Dies kann nützlich sein, wenn ein Store Ressourcen von mehreren Standorten aggregiert und Sie dieselben Einstellungen auf alle Ressourcen für diesen Store anwenden möchten.

Um Sitzungseinstellungen für einen Store zu definieren, haben Sie zwei Möglichkeiten:

- Verwenden Sie den Global App Config Service. Dies ist ein Dienst in Citrix Cloud. Weitere Informationen finden Sie unter Citrix Workspace-App mit dem Global App Configuration Service

konfigurieren.

- Fügen Sie auf dem StoreFront-Server der Datei default.ica des Stores Einstellungen hinzu.

Sie finden default.ica auf dem StoreFront-Server im Verzeichnis `\inetpub\wwwroot\Citrix\[StoreName]\App_Data`.

Eine Liste der verfügbaren Einstellungen finden Sie in der Referenz für ICA-Einstellungen. Einige Einstellungen gelten global. Sie können auch Abschnitte für spezifische Apps hinzufügen, indem Sie dem jeweiligen Abschnitt als Namen den in Studio konfigurierten Anwendungsnamen geben.

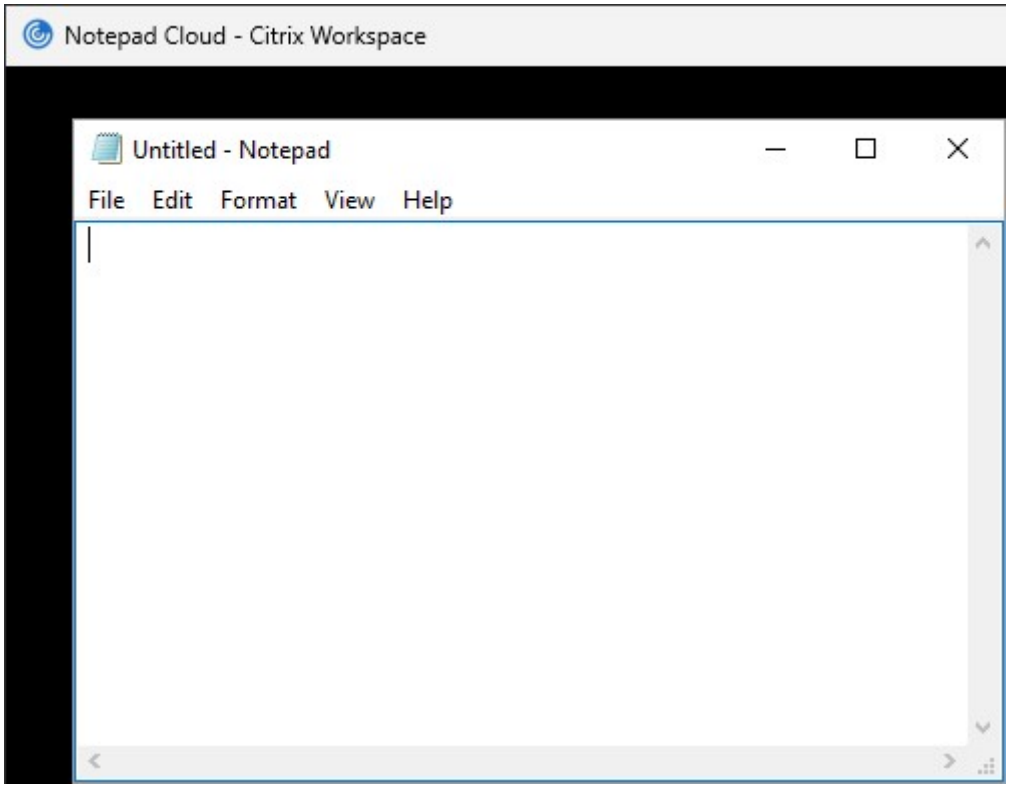
Beispiel: Editor im Fenstermodus starten

Um eine Anwendung so zu konfigurieren, dass sie im Fenstermodus gestartet wird, fügen Sie default.ica einen Abschnitt für die Anwendung mit folgenden Einstellungen hinzu:

- TWIMode: Auf "Off", um den Fenstermodus zu aktivieren.
- DesiredHRES: optional für die Anzahl horizontaler Pixel.
- DesiredVRES : optional für die Anzahl vertikaler Pixel.

Beispiel:

```
[Notepad]
TWIMode=Off
DesiredHRES=1024
DesiredVRES=768
<!--NeedCopy-->
```

ICA-Dateisignierung

April 17, 2024

StoreFront bietet die Option, ICA-Dateien digital zu signieren, damit die Versionen der Citrix Workspace-App, die dieses Feature unterstützen, prüfen können, ob eine Datei aus einer vertrauenswürdigen Quelle stammt. Wenn die Dateisignierung in StoreFront aktiviert ist, wird die beim Starten einer Anwendung durch einen Benutzer generierte ICA-Datei mit einem Zertifikat aus dem persönlichen Zertifikatspeicher des StoreFront-Servers signiert. ICA-Dateien können mit einem Hashalgorithmus signiert werden, der von dem auf dem StoreFront-Server ausgeführten Betriebssystem unterstützt wird. Die digitale Signatur wird von Clients, die dieses Feature nicht unterstützen oder nicht für die ICA-Dateisignierung konfiguriert sind, ignoriert. Wenn die Signierung fehlschlägt, wird die ICA-Datei ohne digitale Signatur generiert und an die Citrix Workspace-App gesendet. Anhand der Konfiguration wird daraufhin bestimmt, ob die unsignierte Datei akzeptiert wird.

Damit die ICA-Dateisignierung im Zusammenhang mit StoreFront verwendet werden kann, müssen die Zertifikate den privaten Schlüssel enthalten und im zulässigen Gültigkeitszeitraum liegen. Wenn das Zertifikat eine Schlüsselnutzungserweiterung enthält, muss der Schlüssel für die digitalen Signaturen verwendet werden. Falls eine erweiterte Schlüsselnutzungserweiterung enthalten ist, muss

dafür Codesignierung oder Serverauthentifizierung festgelegt worden sein.

Citrix empfiehlt bei ICA-Dateisignierung, ein Codesignierungs- oder SSL-Signierungszertifikat von einer öffentlichen Zertifizierungsstelle oder von der privaten Zertifizierungsstelle Ihrer Organisation zu verwenden. Wenn es Ihnen nicht möglich ist, ein geeignetes Zertifikat von einer Zertifizierungsstelle zu beziehen, können Sie entweder ein vorhandenes SSL-Zertifikat (z. B. ein Serverzertifikat) verwenden oder ein neues Zertifikat von der Stammzertifizierungsstelle erstellen und an die Benutzergeräte verteilen.

ICA-Dateisignierung ist in Stores standardmäßig deaktiviert. Zum Aktivieren der ICA-Dateisignierung bearbeiten Sie die Storekonfigurationsdatei und führen Windows PowerShell-Befehle aus. Weitere Informationen zum Aktivieren der ICA-Dateisignierung in der Citrix Workspace-App für Windows finden Sie unter ICA-Dateisignierung.

> Hinweis:
>
> Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer zuerst die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zum Verwalten der StoreFront-Konfiguration öffnen. Schließen Sie gleichermaßen immer alle Instanzen von PowerShell, bevor Sie die StoreFront-Konsole öffnen.

1. Stellen Sie sicher, dass das Zertifikat, das Sie zum Signieren von ICA-Dateien verwenden möchten, im Citrix Delivery Services-Zertifikatspeicher auf dem StoreFront-Server verfügbar ist und nicht im Zertifikatspeicher des aktuellen Benutzers.
2. Signieren mit dem PowerShell-Cmdlet `Set-STFStoreService` aktivieren:

   ```
   $storeService = Get-STFStoreService
   Set-STFStoreService $storeService -IcaFileSigning $true -
       IcaFileSigningCertificateThumbprint [certificatethumbprint]
   <!--NeedCopy-->
   ```

   Dabei ist **certificatethumbprint** der Digest (bzw. Fingerabdruck) der vom Hashalgorithmus generierten Zertifikatdaten.

   Wenn Sie einen anderen Hashalgorithmus als SHA-1 verwenden möchten, fügen Sie den Parameter **-IcaFileSigningHashAlgorithm** hinzu und setzen Sie den Wert nach Bedarf auf sha256, sha384 oder sha512.

Konfiguration der Citrix Workspace-App

February 28, 2024

Global App Configuration Service

Der Global App Config Service ist ein Clouddienst zur Verwaltung der Citrix Workspace-App-Konfiguration. In Ihrem Citrix Cloud-Konto können Sie Ihre Store-URLs beanspruchen und die Konfiguration für jeden Ihrer Stores definieren. Weitere Informationen finden Sie unter Einstellungen für On-Premises-Stores konfigurieren.

Storekontoeinstellungen

Als Alternative zum Global App Config Service können Sie die Citrix Workspace-App über die Storekontoeinstellungen konfigurieren. Wenn ein Benutzer einer lokal installierten Citrix Workspace-App einen Store hinzufügt, ruft er die StoreFront-Kontoeinstellungen ab. Dies kann Konfigurationseigenschaften beinhalten, um beispielsweise der Citrix Workspace-App für Windows mitzuteilen, ob sie Startmenüverknüpfungen für Apps erstellen soll. Einzelheiten zu den Eigenschaften finden Sie in der Dokumentation zur Workspace-App, z. B. Speicherorte für App-Verknüpfungen mit StoreFront-Kontoeinstellungen anpassen.

Schrittfolge zum Anpassen der Einstellungen:

1. Öffnen Sie die Datei web.config in `C:\inetpub\wwwroot\Citrix\Roaming`.
2. Suchen Sie im Abschnitt <Accounts> das Element <account ... name="Store"... > für den Store, den Sie ändern möchten.
3. Suchen Sie im Abschnitt Account den Abschnitt <annotatedServices>/<annotatedServiceRec >/<metadata>/<properties>.
4. Fügen Sie nach dem Element <clear/> die Eigenschaften in der Form <property name= "[name]"value="[value]"/> hinzu: Beispiel:

```
<properties>
    <clear/>
    <property name="PutShortcutsOnDesktop" value="true"/>
    <property name="DesktopDir" value="Citrix Applications"/>
</properties>
<!--NeedCopy-->
```

> **Wichtig!**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Webseite der Workspace-App

Informationen zur Konfiguration, welche Websitekonfiguration von der lokal installierten Citrix Workspace-App verwendet wird, finden Sie unter Workspace-App-Website konfigurieren.

Website verwalten

September 27, 2023

Für jeden Store können Sie eine oder mehrere Websites für den Zugriff durch die Benutzer über einen Browser oder über die Citrix Workspace-App konfigurieren.

Verwenden Sie die StoreFront-Verwaltungskonsole zur Ausführung folgender Aufgaben:

Aufgabe	Detail
Website erstellen	Erstellen Sie Websites, damit Benutzer über eine Webseite oder die Workspace-App auf Stores zugreifen können.
Website konfigurieren	Einstellungen für Ihre Website ändern
Website entfernen	Entfernen von Citrix Receiver für Web-Sites.
Workspace-App-Website konfigurieren	Wählen Sie aus, welche Website von der Citrix Workspace-App aus verwendet werden soll.

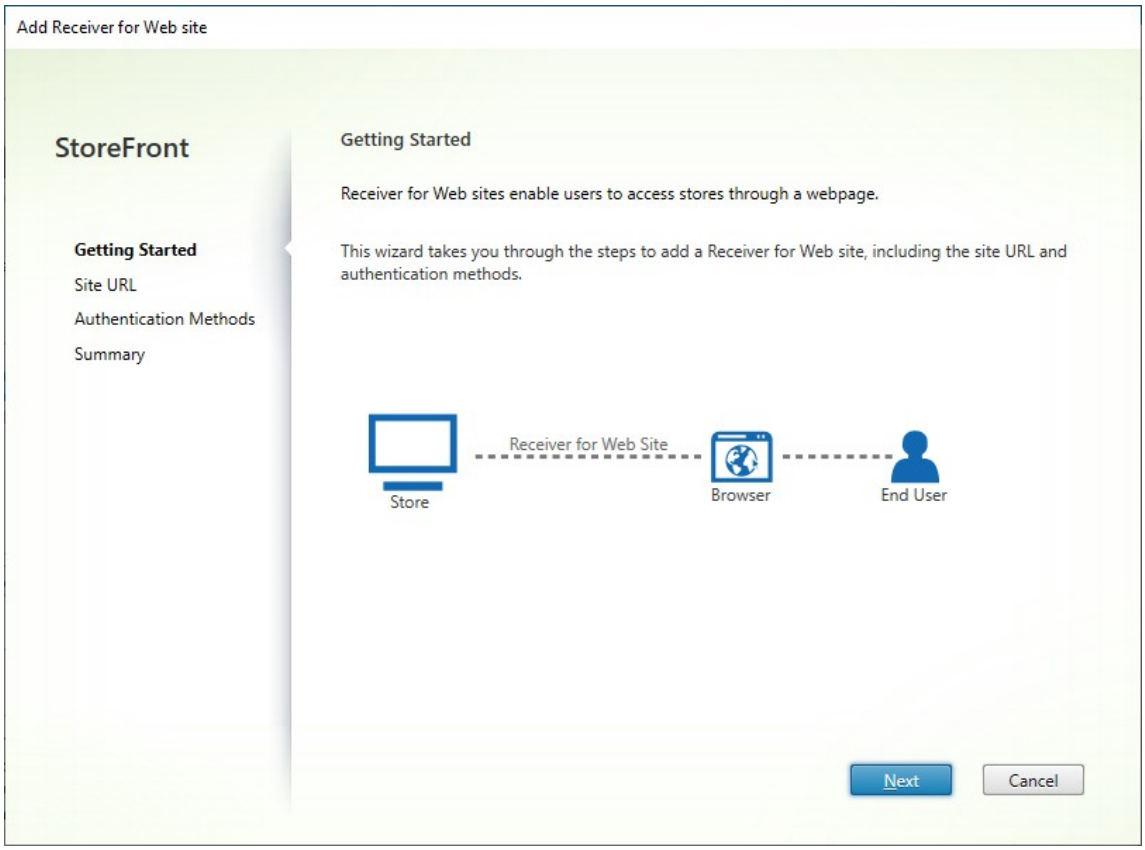
Website erstellen

April 17, 2024

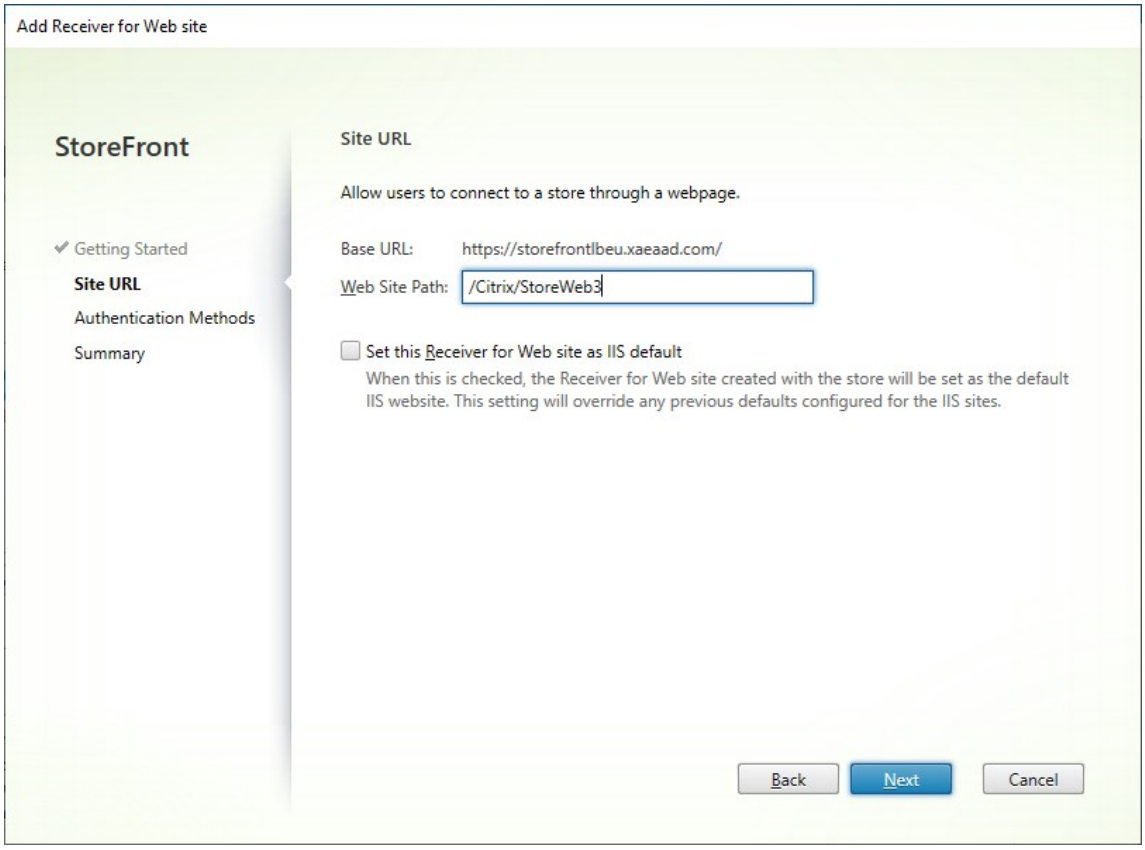
Bei der Erstellung eines Stores wird standardmäßig eine Website für den Store erstellt. Sie können zusätzliche Websites zu bestehenden Stores hinzufügen. Auf diese Weise können Sie für die Benutzer verschiedene URLs mit unterschiedlichen Konfigurationen zur Verfügung stellen. Auf mehrere Websites kann jedoch nur über einen Webbrowser zugegriffen werden, da die Citrix Workspace-App so konfiguriert ist, dass sie eine bestimmte Website für einen Store verwendet (siehe Workspace-App-Website konfigurieren).

> Wichtig:
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss
> übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

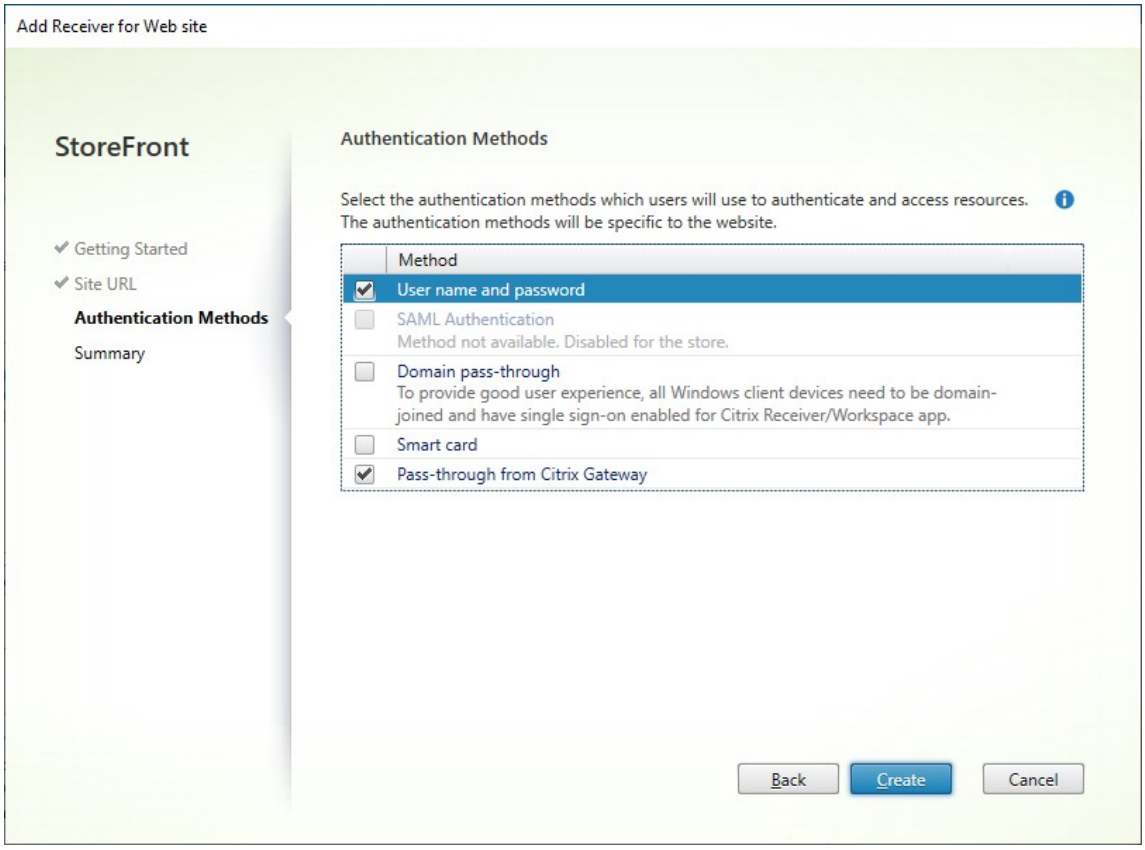
1. Wählen Sie in der Verwaltungskonsole den Store, für den Sie die Website erstellen möchten, und klicken Sie auf **Receiver für Web-Sites verwalten**.
2. Klicken Sie auf **Hinzufügen** und dann auf **Weiter**.



3. Geben Sie den gewünschten **Websitepfad** ein, wählen Sie aus, ob dies die Standardwebsite für die Basis-URL sein soll, und klicken Sie auf **Weiter**.



4. Aktivieren oder deaktivieren Sie die Authentifizierungsmethoden nach Bedarf. Manche Methoden sind nur verfügbar, wenn sie für den Store konfiguriert wurden. Klicken Sie auf **Weiter**.



5. Nach dem Erstellen der Site klicken Sie auf **Fertig stellen**.
6. Wählen Sie die neu erstellte Site und klicken Sie auf **Bearbeiten**, um die Website nach Bedarf zu konfigurieren. Weitere Informationen finden Sie unter Websites konfigurieren.

Website mit dem PowerShell-SDK erstellen

Um eine Website mit dem PowerShell-SDK zu erstellen, rufen Sie das Cmdlet Add-STFWebReceiverService auf.

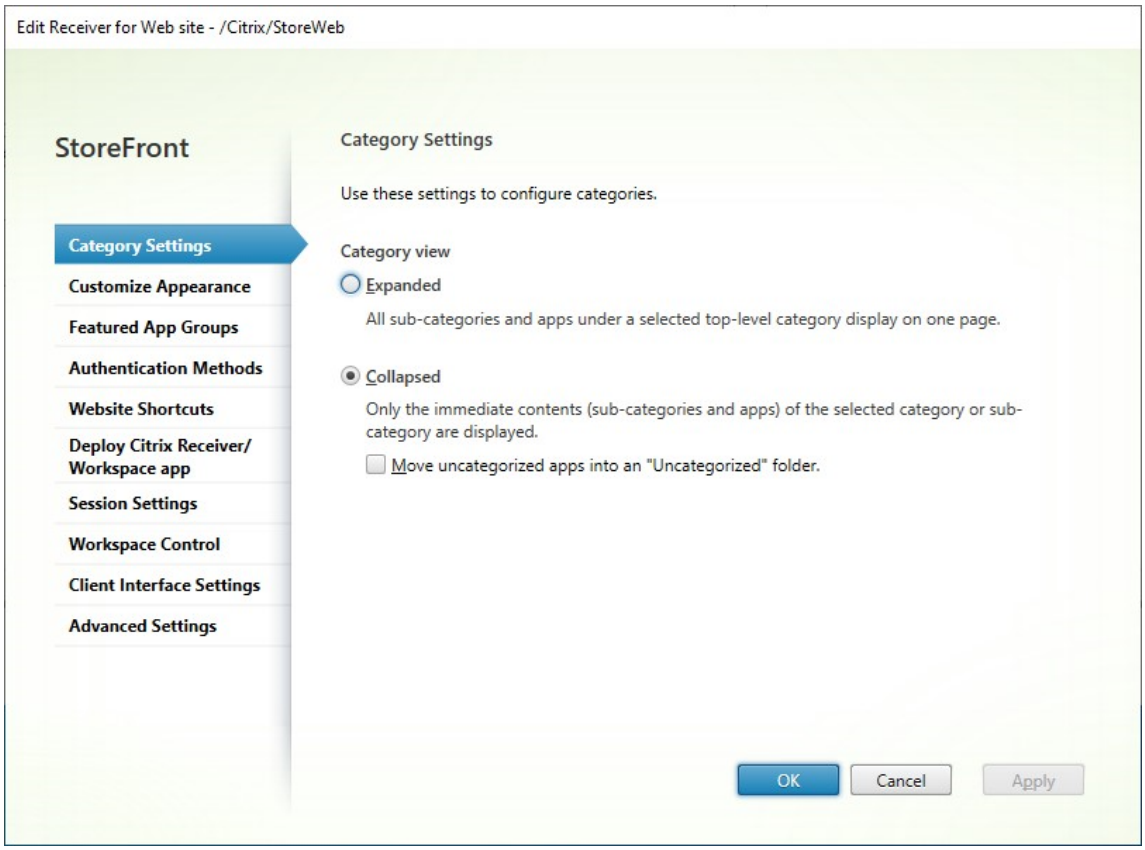
Website konfigurieren

April 17, 2024

Website konfigurieren:

1. Wählen Sie im linken Bereich den Knoten **Stores**, klicken Sie im Bereich **Aktionen**auf **Receiver für Web-Sites verwalten**.

2. Wählen Sie eine Website aus und klicken Sie auf **Konfigurieren...**



3. Ändern Sie die Einstellungen auf den entsprechenden Registerkarten.

   - Kategorieeinstellungen
   - Benutzeroberfläche anpassen
   - App-Gruppen mit Highlights
   - Authentifizierungsmethoden
   - Websiteverknüpfungen
   - Citrix Receiver/Workspace-App bereitstellen
   - Sitzungseinstellungen
   - Workspace Control
   - Einstellungen für die Clientoberfläche
   - Erweiterte Einstellungen

4. Wenn Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **OK**.

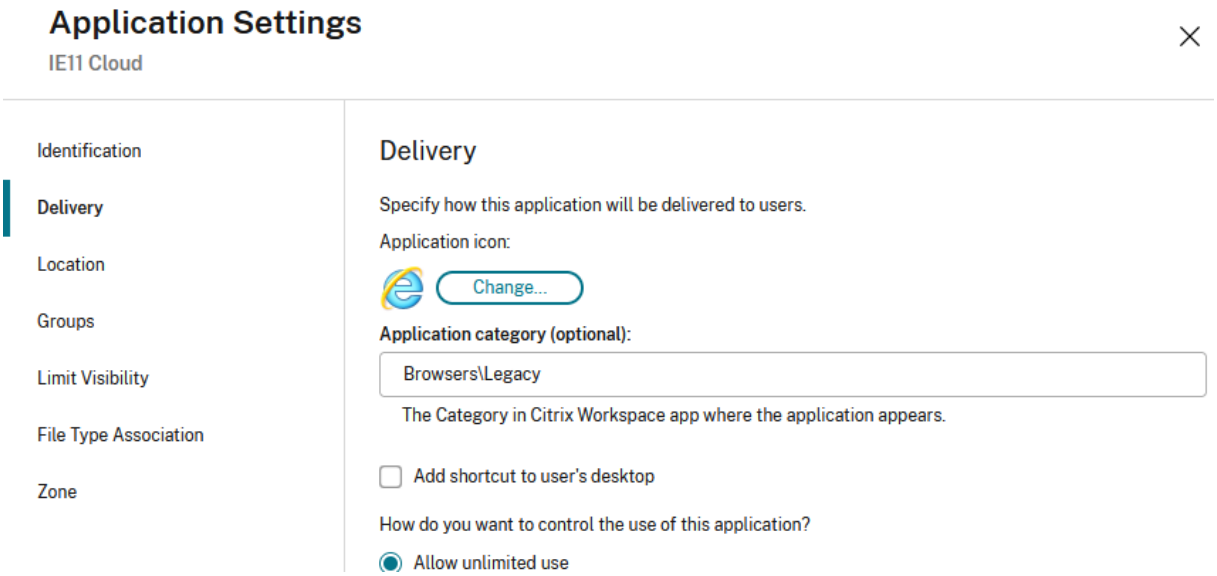
> **Wichtig:**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Ab-

> schluss
> übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

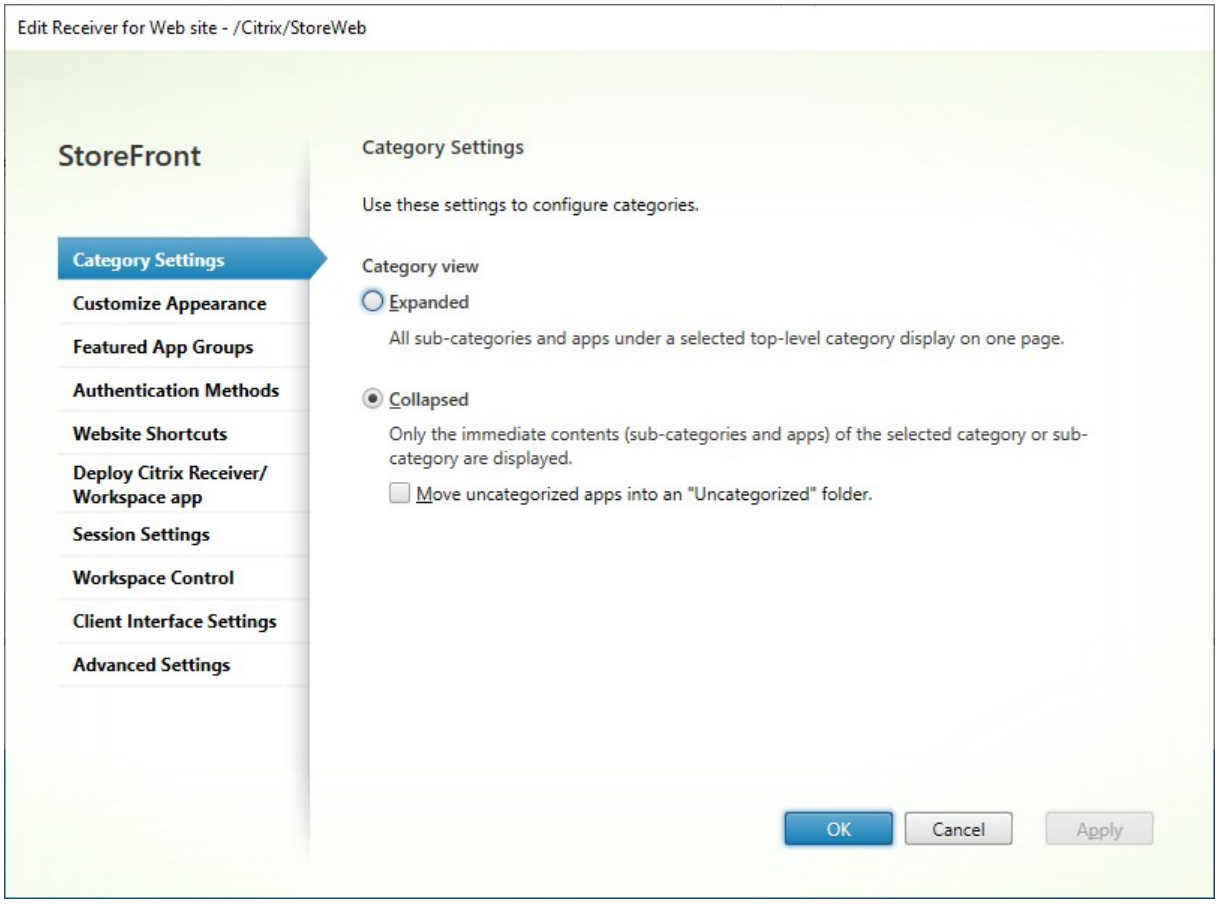
Kategorieeinstellungen

April 17, 2024

In Citrix Virtual Apps and Desktops können Sie jede Anwendung einer Kategorie zuweisen (siehe Anwendungen). Verwenden Sie das Symbol \, um eine Ordnerhierarchie der Kategorien zu erstellen. In StoreFront können Sie konfigurieren, wie diese Ordnerhierarchie angezeigt wird.



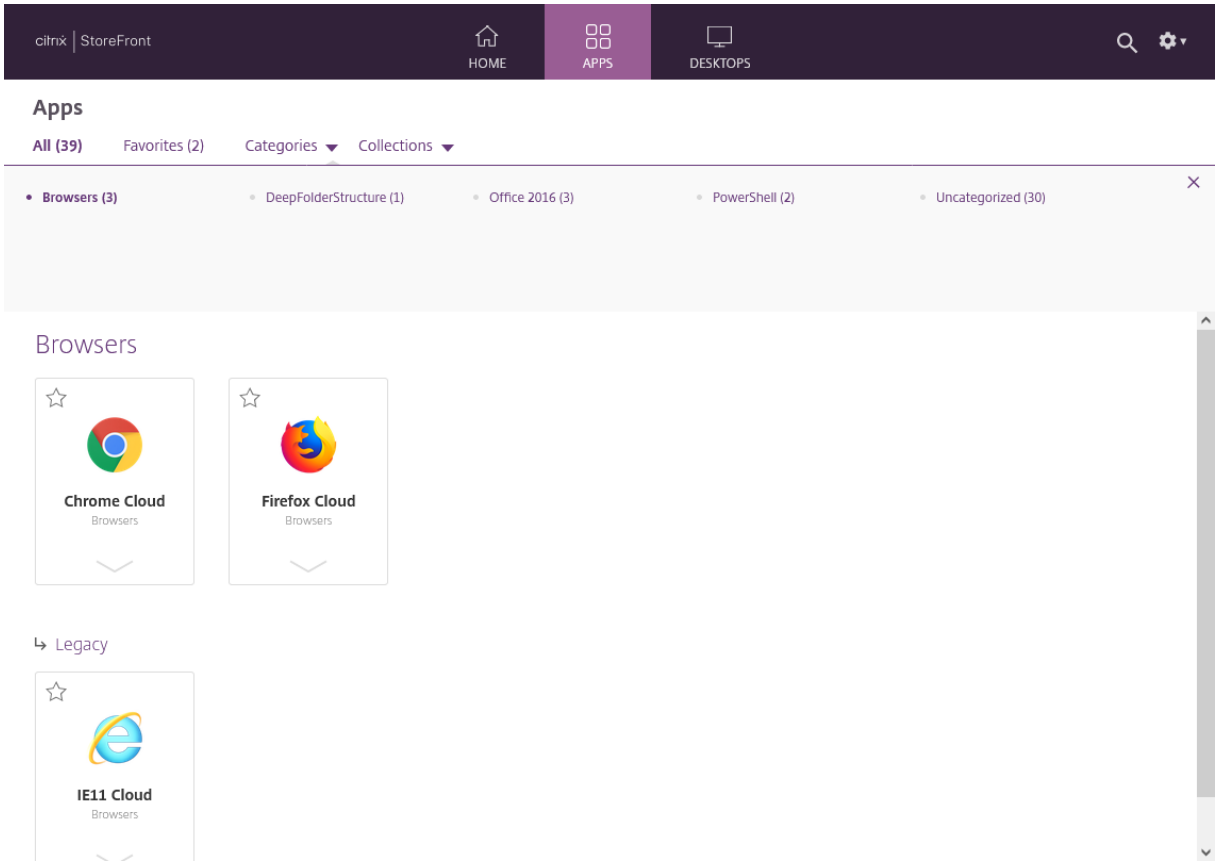
Um die Kategorieeinstellungen zu ändern, gehen Sie zu Receiver für Web-Site bearbeiten und wählen Sie die Registerkarte **Kategorieeinstellungen**.



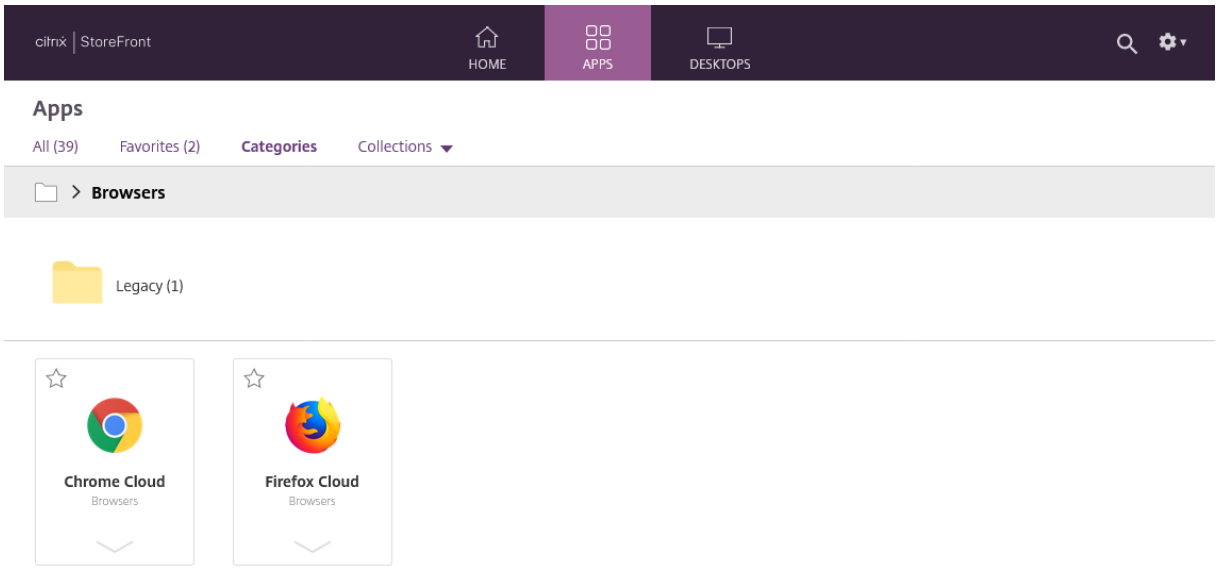
Kategorieansicht

In der erweiterten Ansicht zeigt StoreFront eine Liste der Kategorien der obersten Ebene an. Wenn der Benutzer auf eine Kategorie der obersten Ebene klickt, zeigt werden in StoreFront alle Apps in allen Unterkategorien auf einer Seite angezeigt.

Wenn Sie beispielsweise eine Kategorie "Browser" mit der Unterkategorie "Legacy" haben, werden alle Browser einschließlich derjenigen unter "Legacy" auf einer Seite angezeigt:

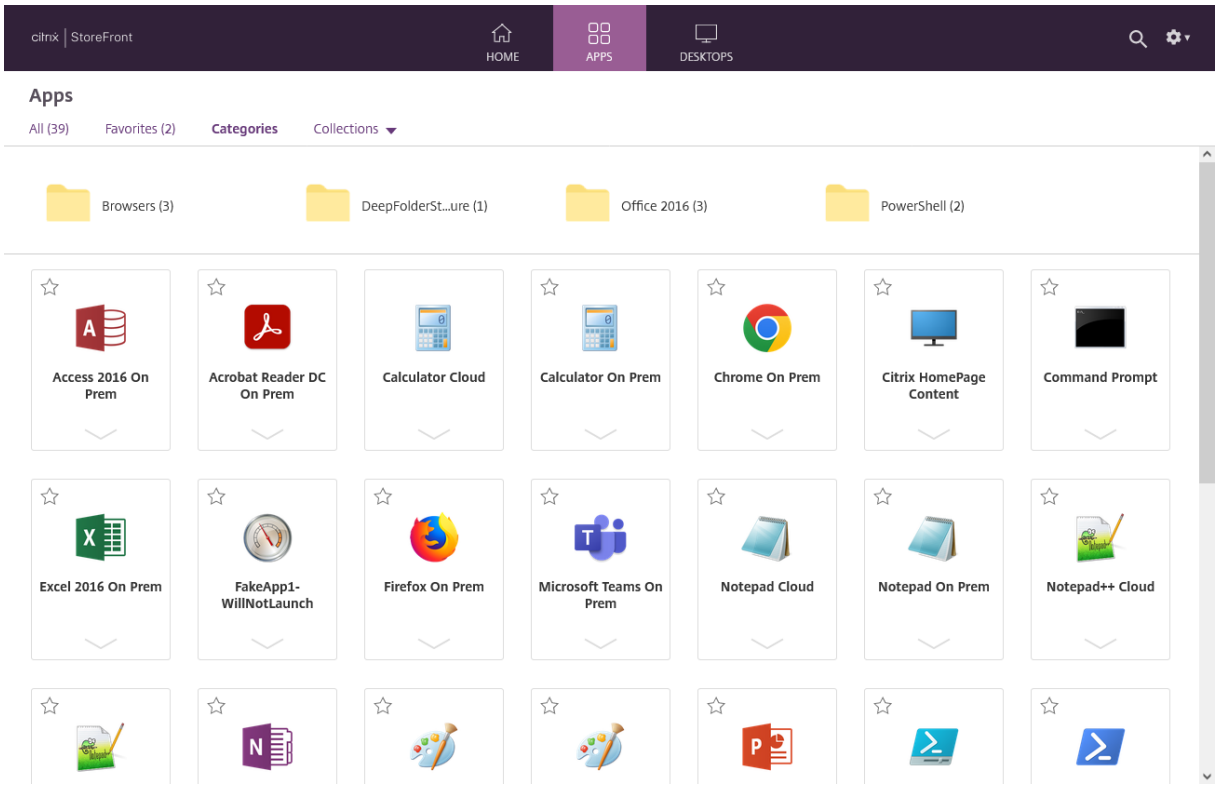


In der reduzierten Ansicht zeigt StoreFront eine Liste der Kategorien der obersten Ebene und optional alle nicht kategorisierten Apps an. Wenn der Benutzer auf eine Kategorie klickt, wird in StoreFront nur der direkte Inhalt (Unterkategorien und Apps) der ausgewählten Kategorie angezeigt. Der Benutzer kann auf die Unterkategorien klicken, um deren Inhalt anzuzeigen.

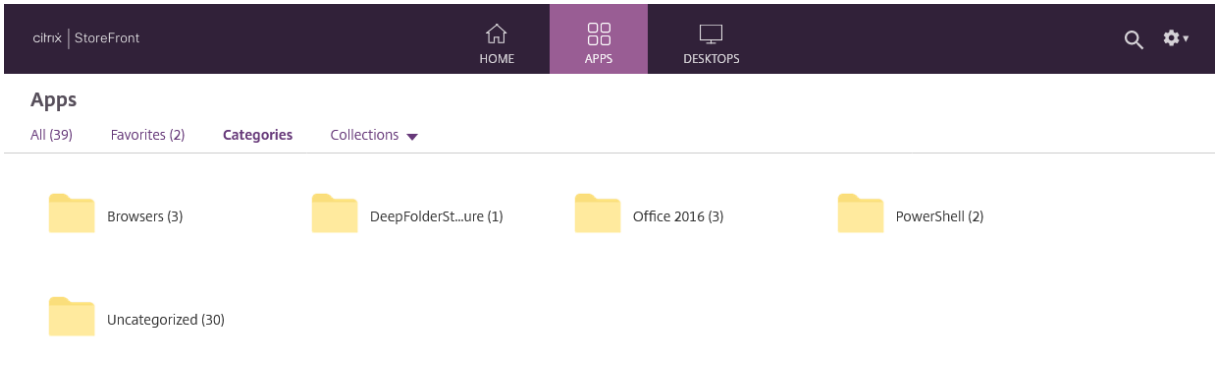


Nicht kategorisierte Apps

Deaktivieren Sie in der reduzierten Ansicht die Option **Nicht kategorisierte Apps in einen Ordner namens 'Nicht kategorisiert'verschieben**, um alle Apps und Desktops ohne Kategoriezuweisung in der ersten Ansicht anzuzeigen. Dieses Verhalten ähnelt dem früherer StoreFront-Versionen.



Aktivieren Sie in der reduzierten Ansicht die Option **Nicht kategorisierte Apps in einen Ordner namens 'Nicht kategorisiert'verschieben**, um alle Apps und Desktops ohne Kategoriezuweisung in einen eigenen Ordner unter dem Namen **Nicht kategorisiert** zu verschieben.



Kategorieeinstellungen mit dem PowerShell-SDK konfigurieren

Um die Kategorieansicht mit dem PowerShell-SDK zu aktivieren oder zu deaktivieren, rufen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `EnableAppsFolderView` auf.

Um die Kategorieansicht mit dem PowerShell-SDK zu ändern, rufen Sie das Cmdlet Set-STFWebReceiverUserInterfa mit dem Parameter `CategoryViewCollapsed` auf.

Benutzeroberfläche anpassen

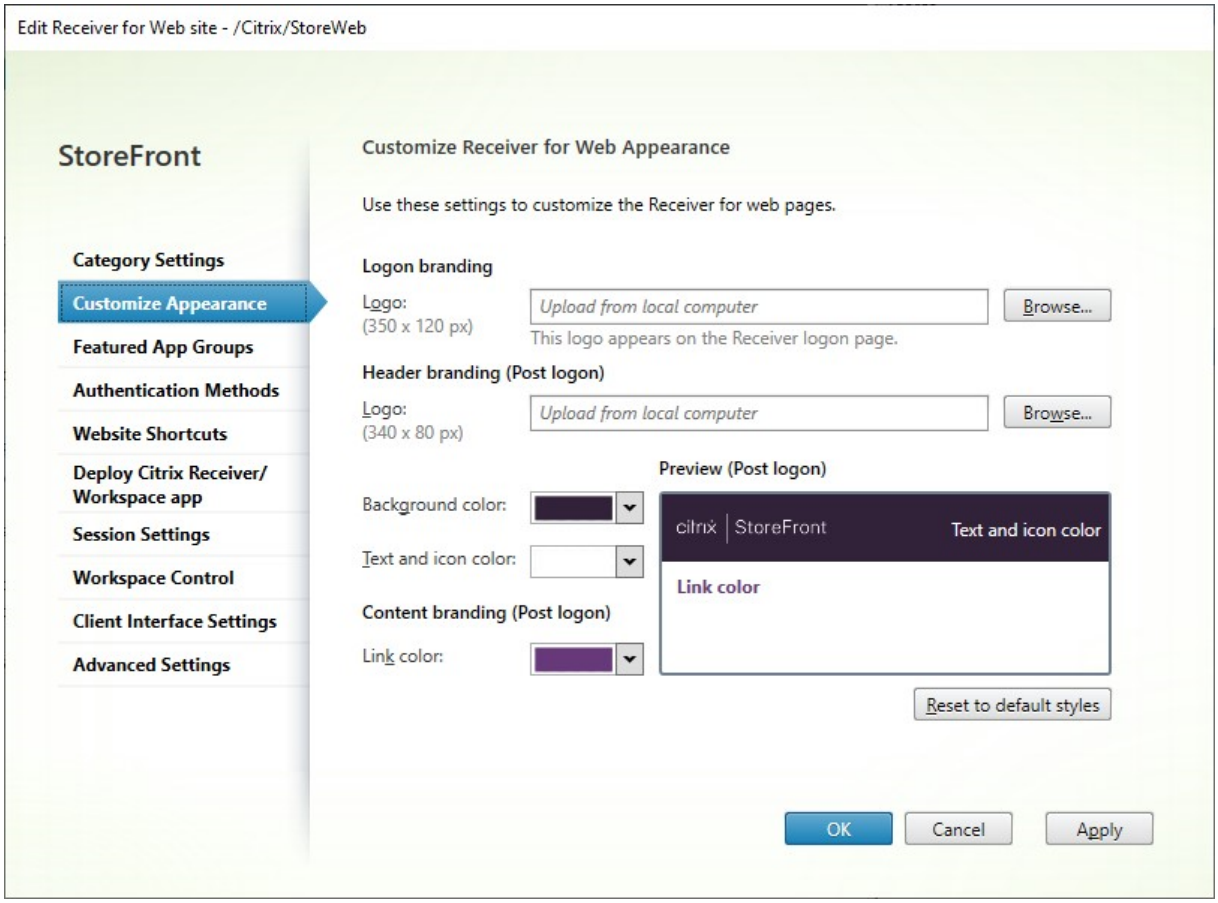
April 17, 2024

Sie können das auf Ihrer Store-Website verwendete Logo und die verwendeten Farben ändern.

Logo und Farben bearbeiten

Um das Erscheinungsbild anzupassen, gehen Sie zu Receiver für Website bearbeiten und wählen Sie die Registerkarte **Benutzeroberfläche anpassen**. Sie können Folgendes ändern:

- **Unternehmenslogo bei Anmeldung:** Logo, das auf dem Anmeldebildschirm angezeigt wird. Bei der Anmeldung über ein Citrix Gateway wird es nicht angezeigt. Klicken Sie auf **Durchsuchen...** und wählen Sie eine Datei vom Typ .jpg, .jpeg, .png, .png oder .bmp aus. Es wird empfohlen, ein Bild der Größe 350 x 120 px zu verwenden.
- **Unternehmenslogo im Header:** Das Logo wird nach dem Anmelden oben links angezeigt. Klicken Sie auf **Durchsuchen...** und wählen Sie eine Datei vom Typ .jpg, .jpeg, .png, .png oder .bmp aus. Es wird empfohlen, ein Bild der Größe 340 x 80 px zu verwenden.
- **Hintergrundfarbe:** Hintergrundfarbe des Navigationsbereichs oben auf der Seite.
- **Text- und Symbolfarbe:** Text- und Symbolfarbe im Navigationsbereich oben auf der Seite.
- **Linkfarbe:** Farbe, mit der das aktuell ausgewählte Element hervorgehoben wird.



Logo und Farben mit dem PowerShell-SDK bearbeiten

Rufen Sie mit dem PowerShell-SDK das Cmdlet Set-STFWebReceiverSiteStyle auf.

Darstellung auf die Standardeinstellungen zurücksetzen

Klicken Sie auf **Zurücksetzen auf Standardstil**, um die Logos und Farben auf die Standardeinstellung zurückzusetzen.

Darstellung mithilfe des PowerShell-SDKs auf die Standardeinstellungen zurücksetzen

Rufen Sie mit dem PowerShell-SDK das Cmdlet Clear-STFWebReceiverSiteStyle auf.

Anpassung mit JavaScript und CSS

Sie können die Website mithilfe der StoreFront Client UI Customization API weiter anpassen.

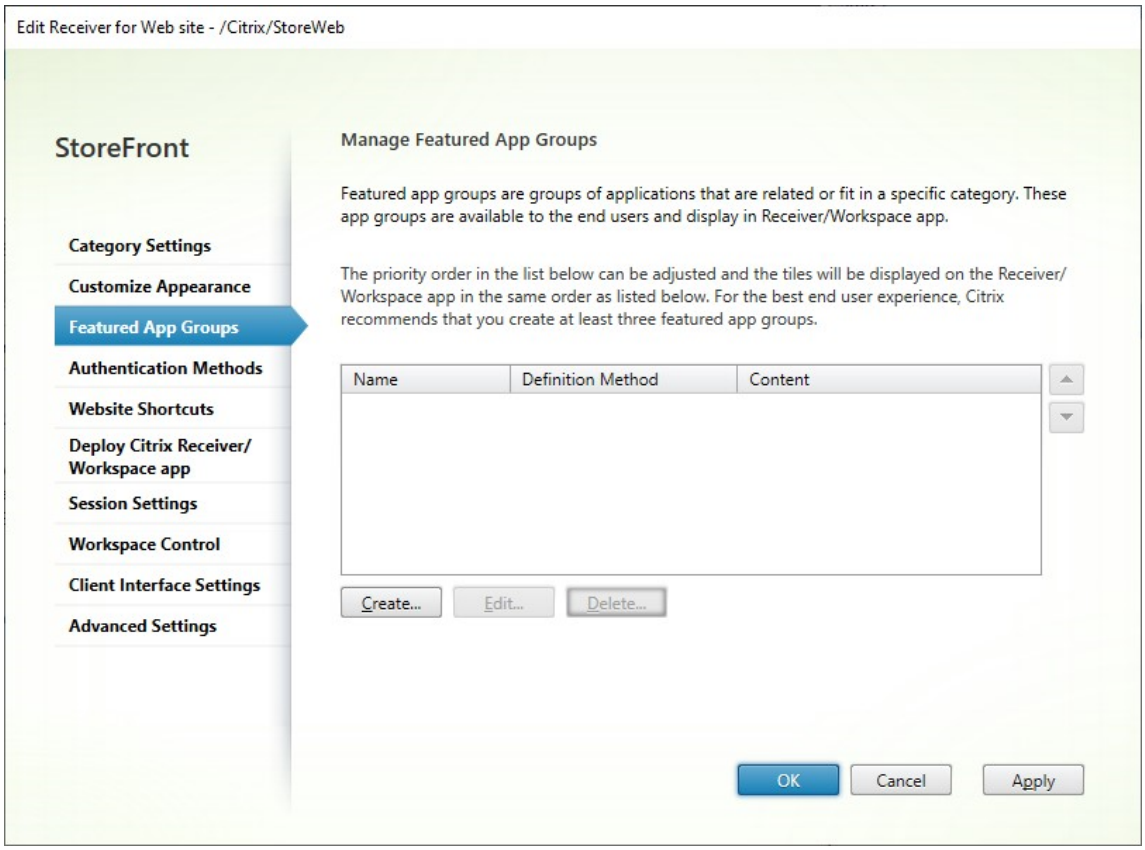
App-Gruppen mit Highlights

April 17, 2024

Sie können App-Gruppen mit empfohlenen Apps (sogenannte Highlights) für die Benutzer erstellen, die einer bestimmten Kategorie angehören oder zu ihr passen. Beispielsweise können Sie eine App-Gruppe mit Highlights unter dem Namen "Vertriebsabteilung"für Apps erstellen, die von dieser Abteilung verwendet werden. Sie können empfohlene Apps in der StoreFront-Verwaltungskonsole über Anwendungsnamen definieren oder mit Schlüsselwörtern oder Anwendungskategorien, die in der Studio-Konsole festgelegt wurden.

App-Gruppe mit Highlights erstellen

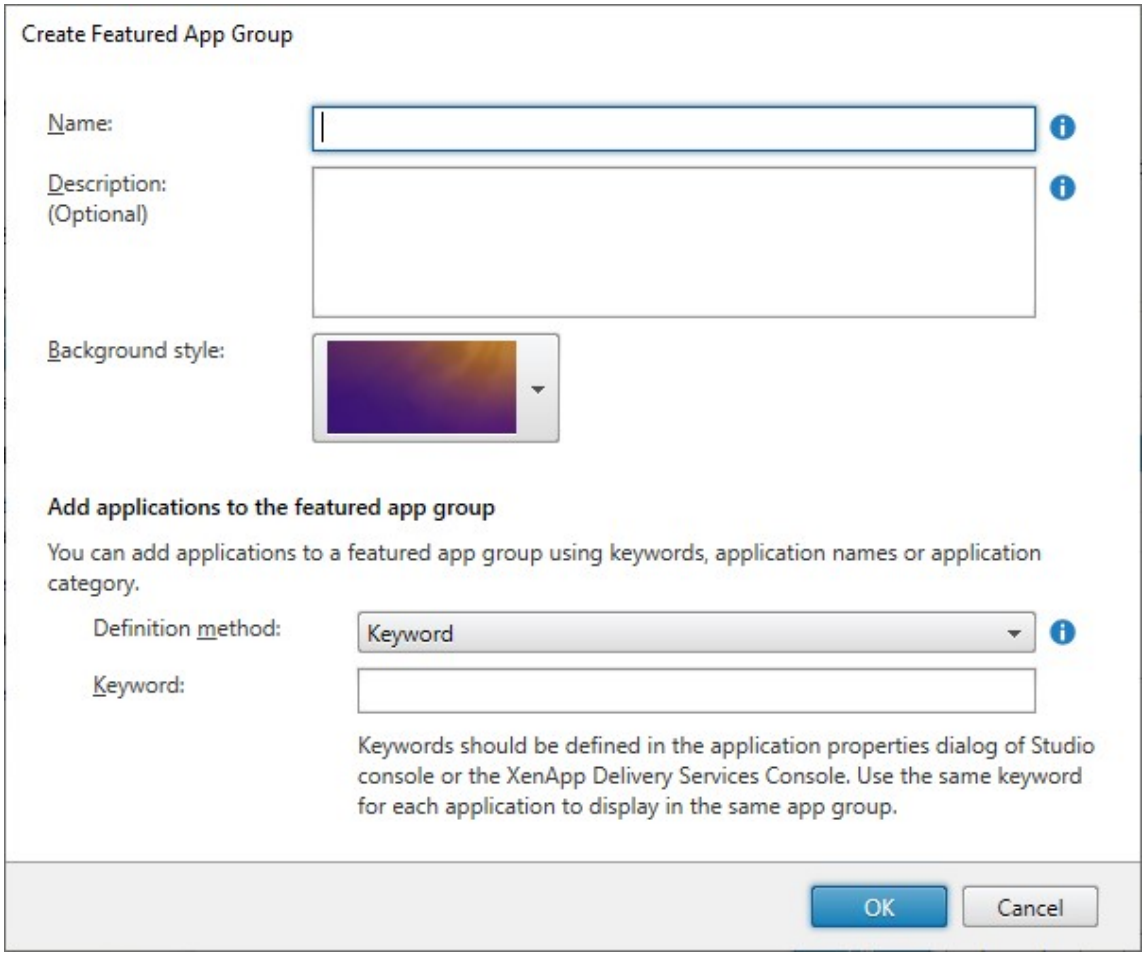
1. Wählen Sie im Bildschirm Receiver für Web-Site bearbeiten die Registerkarte **App-Gruppen mit Highlights**.



2. Klicken Sie auf **Erstellen**, um eine neue App-Gruppe mit Highlights zu erstellen.
3. Geben Sie einen Namen, eine Beschreibung (optional), einen Hintergrund und die Methode an, mit der Sie die App-Gruppen mit Highlights definieren. Sie können Schlüsselwörter, Anwen-

dungsnamen oder Anwendungskategorien auswählen.

Option	Beschreibung
Schlüsselwörter	Ordnet Apps nach dem in Studio festgelegten Schlüsselwort zu, indem Schlüsselwörter in die App-Beschreibung aufgenommen werden. Beispiel: "Zum Senden und Empfangen von E-Mails verwenden SCHLÜSSELWÖRTER: Zusammenarbeit".
Anwendungskategorie	Ordnet Apps in einer bestimmten Anwendungskategorie zu, die in Studio eingegeben wurde.
Anwendungsnamen	Verwenden Sie den Anwendungsnamen zum Definieren der App-Gruppe mit Highlights. Alle Anwendungen, deren Name dem in diesem Dialogfeld angegebenen Namen entsprechen, werden in die App-Gruppe mit Highlights aufgenommen. StoreFront unterstützt keine Platzhalter in Anwendungsnamen. Bei den Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, es werden jedoch vollständige Wörter gesucht. Wenn Sie beispielsweise "Excel"eingeben, wird in StoreFront die veröffentlichte Anwendung Microsoft Excel 2013 gefunden, doch bei Eingabe von Exc wird keine Übereinstimmung gefunden.

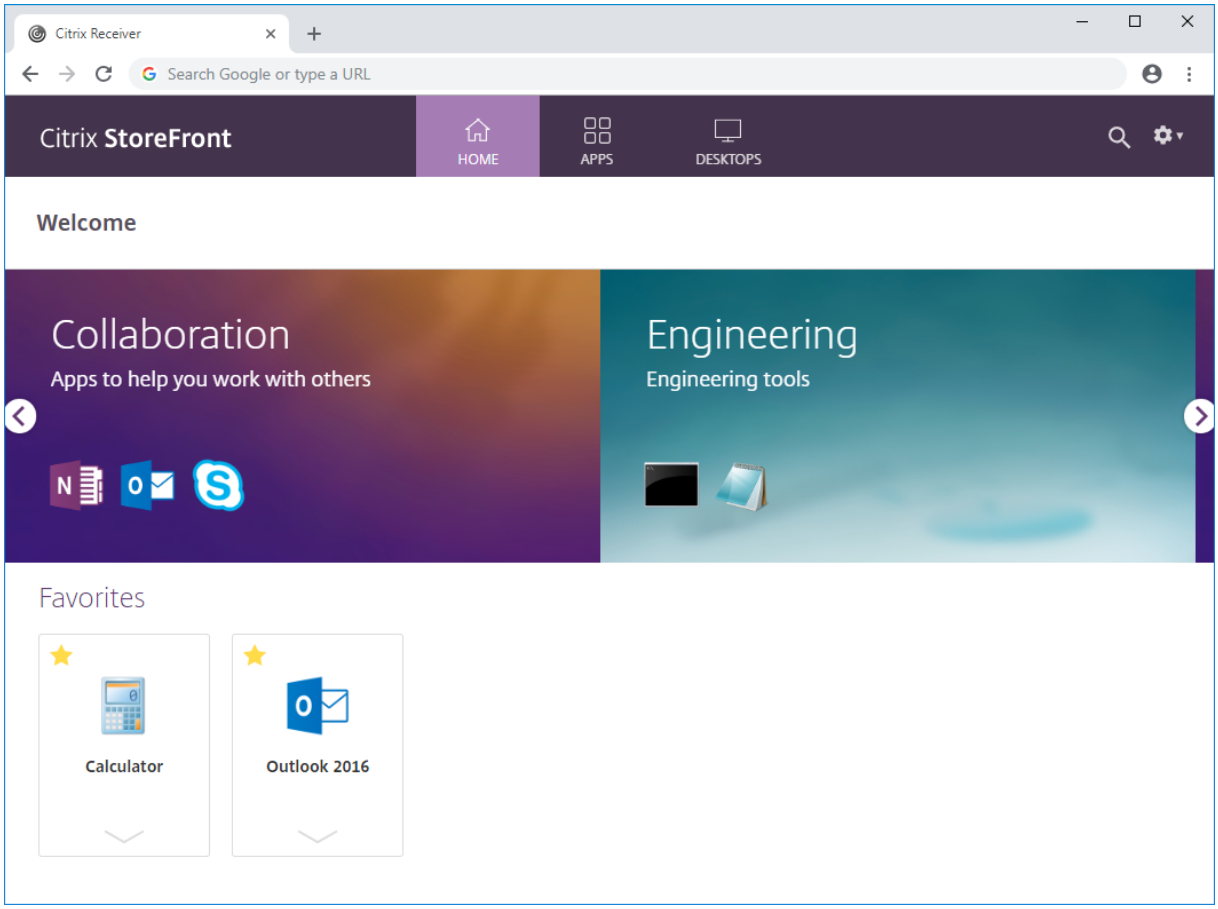


4. Klicken Sie auf **OK**.

Beispiel:

Wir haben zwei App-Gruppen mit Highlights erstellt:

- Collaboration: Erstellt durch Zuordnung von Apps der Kategorie **Collaboration** in Studio.
- Engineering: Erstellt unter Benennung der App-Gruppe und Angabe einer App-Sammlung.



App-Gruppen mit Highlights mithilfe des PowerShell-SDKs erstellen

Verwenden Sie zum Hinzufügen von App-Gruppen mit Highlights mit dem PowerShell-SDK das Cmdlet New-STFWebReceiverFeaturedAppGroup.

App-Gruppe mit Highlights bearbeiten

Wählen Sie im Bildschirm Receiver für Web-Site bearbeiten die Registerkarte **App-Gruppen mit Highlights**. Wählen Sie die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten...**.

App-Gruppen mit Highlights mithilfe des PowerShell-SDKs bearbeiten

Verwenden Sie zum Bearbeiten von App-Gruppen mit Highlights mit dem PowerShell-SDK das Cmdlet Set-STFWebReceiverFeaturedAppGroup.

App-Gruppe mit Highlights löschen

Wählen Sie im Bildschirm Receiver für Web-Site bearbeiten die Registerkarte **App-Gruppen mit Highlights**. Wählen Sie die gewünschte Gruppe aus und klicken Sie auf **Löschen…**.

App-Gruppen mit Highlights mithilfe des PowerShell-SDKs löschen

Verwenden Sie zum Löschen von App-Gruppen mit Highlights mit dem PowerShell-SDK das Cmdlet Remove-STFWebReceiverFeaturedAppGroup und zum Löschen aller App-Gruppen mit Highlights das Cmdlet Clear-STFWebReceiverFeaturedAppGroup.

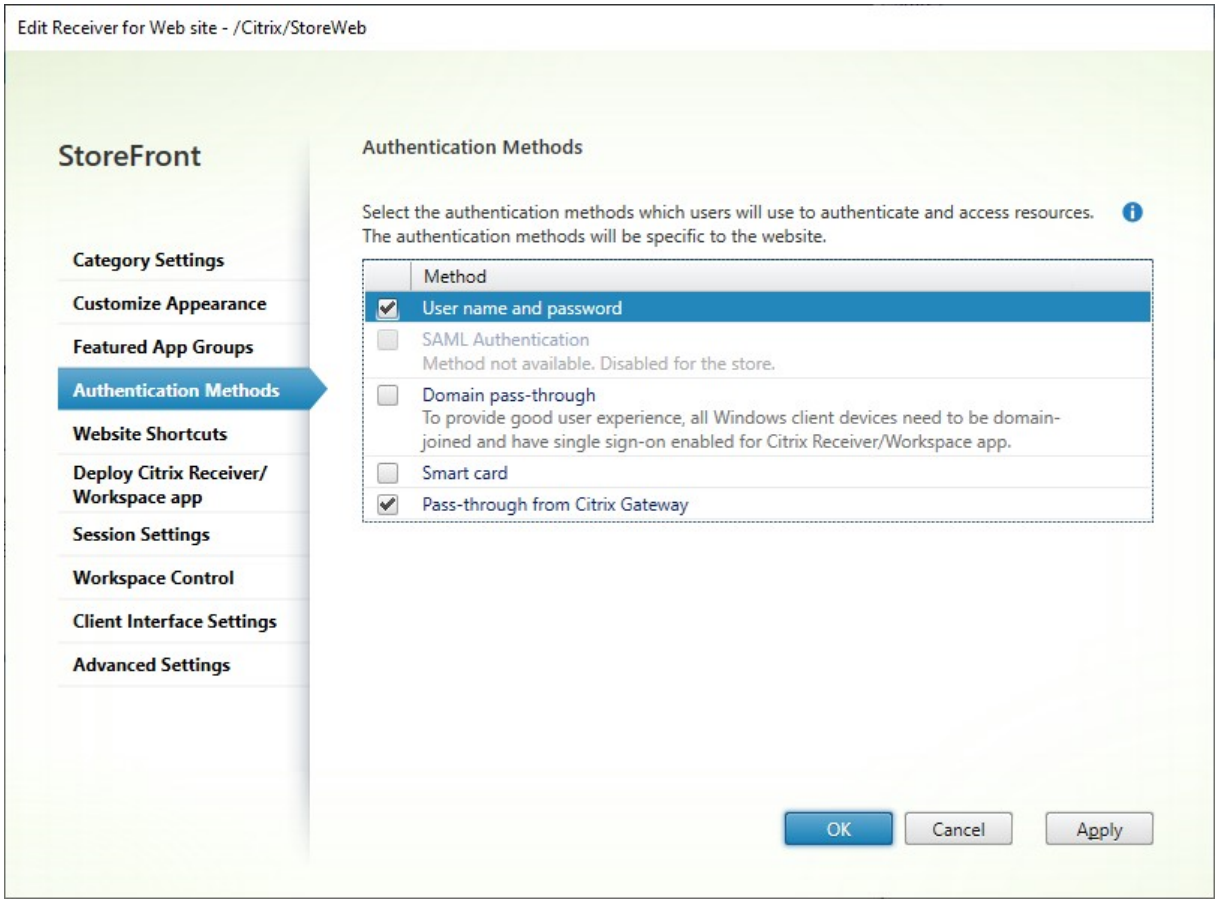
Authentifizierungsmethoden

April 17, 2024

Informationen zum Konfigurieren der für einen Store verfügbaren Authentifizierungsmethoden finden Sie unter Authentifizierung konfigurieren. Sie können einige dieser Einstellungen für eine spezifische Website außer Kraft setzen. Die Außerkraftsetzungen gelten nur für die Verwendung der Citrix Workspace-App für HTML5 über einen Browser. Die lokal installierte Citrix Workspace-App verwendet die Einstellungen aus dem Store und nicht die Website.

> **Warnung:**
> Wenn Sie die Authentifizierungsmethoden für einen Store ändern, werden die Einstellungen für alle Websites für diesen Store außer Kraft gesetzt, weshalb jegliche Änderungen erneut angewendet werden müssen.

Um die Authentifizierungsmethoden zu ändern, gehen Sie zu Receiver für Web-Site bearbeiten und wählen Sie die Registerkarte **Authentifizierungsmethoden**.



- Aktivieren Sie das Kontrollkästchen **Benutzername und Kennwort**, um die explizite Authentifizierung zu aktivieren. Siehe Authentifizierung mit Benutzernamen und Kennwort. Diese Option ist nur verfügbar, wenn sie für den Store aktiviert ist.
- Wählen Sie das Kontrollkästchen **SAML-Authentifizierung**, um die Integration eines SAML-Identitätsanbieters zu ermöglichen. Siehe SAML-Authentifizierung. Diese Option ist nur verfügbar, wenn sie für den Store aktiviert wurde.
- Aktivieren Sie **Domänen-Passthrough**, um Passthrough für Active Directory-Domänenanmeldeinformationen von Benutzergeräten zu aktivieren. Siehe Domänen-Passthrough-Authentifizierung. Diese Option ist nur verfügbar, wenn sie für den Store aktiviert wurde.
- Aktivieren Sie **Smartcard**, um die Smartcardauthentifizierung zu aktivieren. Siehe Smartcardauthentifizierung.
- Aktivieren Sie **Passthrough-Authentifizierung von Citrix Gateway** zum Aktivieren der Passthrough-Authentifizierung von Citrix Gateway. Aktivieren Sie diese Option, wenn die Benutzer über ein Citrix Gateway mit aktivierter Authentifizierung auf StoreFront zugreifen. Siehe Passthrough-Authentifizierung von Citrix Gateway.

Konfiguration mit dem PowerShell-SDK

Zum Konfigurieren der Authentifizierungsmethoden mithilfe des PowerShell-SDKs verwenden Sie das Cmdlet Set-STFWebReceiverAuthenticationMethods.

Websiteverknüpfungen

April 17, 2024

Verwenden Sie Websiteverknüpfungen, um Benutzern schnellen Zugriff auf Desktops und Anwendungen über vertrauenswürdige Websites, die im internen Netzwerk gehostet werden, zu gestatten. Dafür generieren Sie URLs für Ressourcen, die über eine Citrix Receiver für Web-Site verfügbar sind, und betten diese Links in die Websites ein. Die Benutzer klicken auf einen Link und werden an die Receiver für Web-Site weitergeleitet, wo sie sich anmelden, wenn sie dies nicht bereits getan haben. Die Receiver für Web-Site startet automatisch die Ressource. Im Fall von Anwendungen wird zudem ein Abonnement für die Benutzer erstellt, wenn diese eine Anwendung noch nicht abonniert haben.

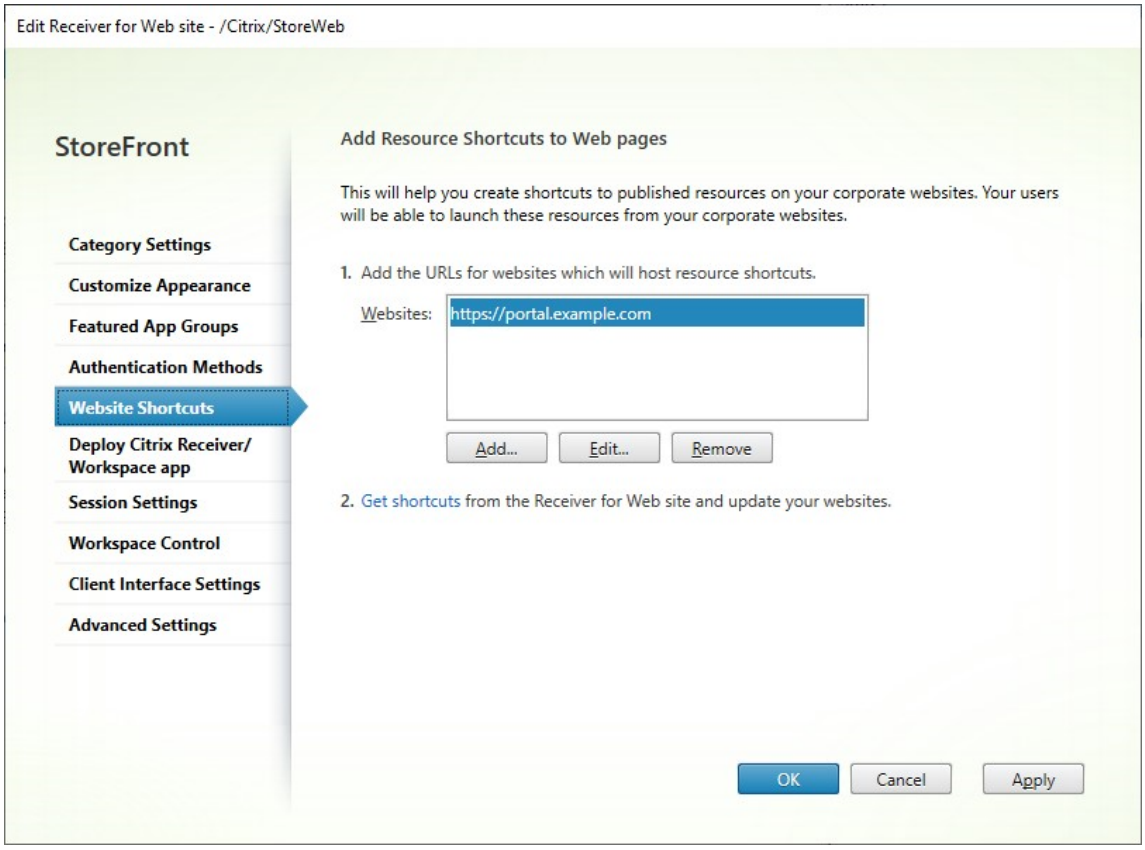
Bevor Sie Ressourcenverknüpfungen generieren können, müssen Sie die URLs von Hostwebsites mit der Citrix StoreFront-Verwaltungskonsole oder PowerShell der Liste *Vertrauenswürdige URLs* hinzufügen.

Standardmäßig warnt StoreFront Benutzer, wenn sie versuchen, Ressourcenverknüpfungen von nicht vertrauenswürdigen Websites zu starten, Benutzer können die Ressource jedoch weiterhin starten. Um die Anzeige der Warnungen zu stoppen, klicken Sie im Bereich **Stores** auf **Receiver für Web-Sites verwalten**, klicken Sie auf **Konfigurieren**, wählen Sie **Erweiterte Einstellungen** und deaktivieren Sie die Option **Aufforderung für nicht vertrauenswürdige Verknüpfungen**.

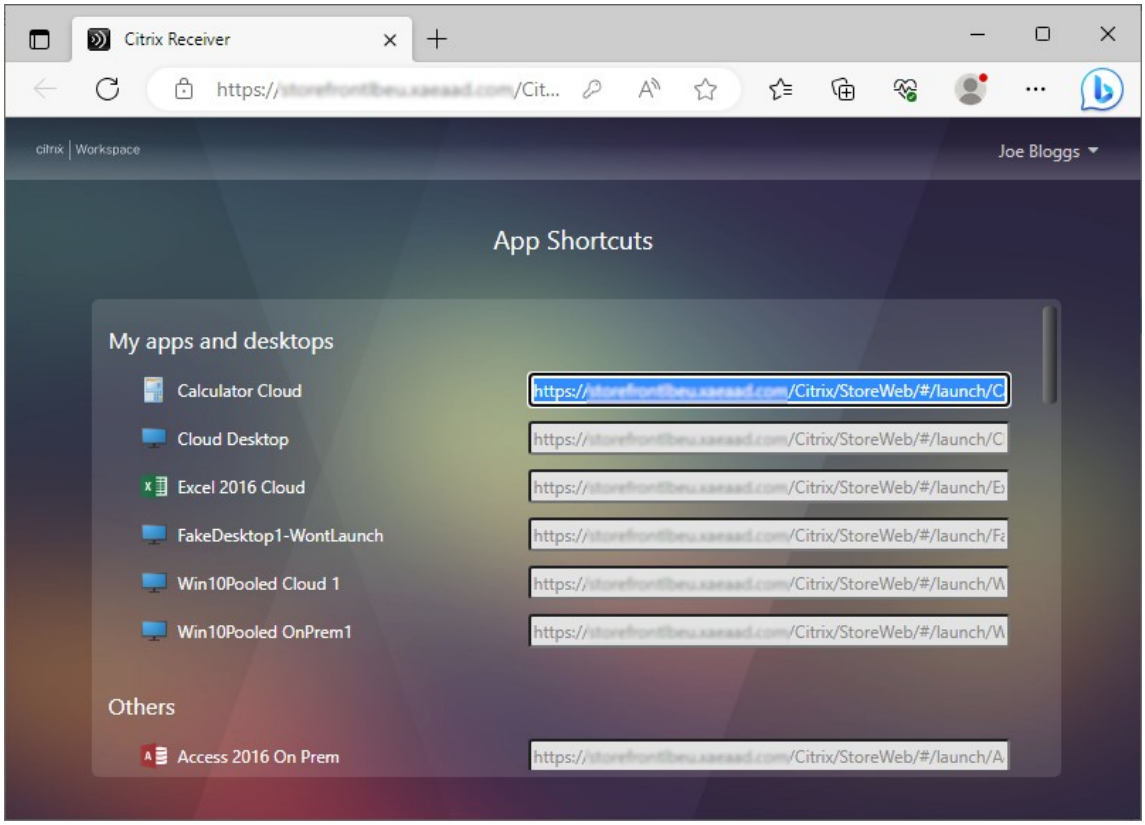
Aus Sicherheitsgründen werden Benutzer von Internet Explorer möglicherweise aufgefordert, zu bestätigen, dass sie Ressourcen über Verknüpfungen starten möchten. Weisen Sie die Benutzer an, den StoreFront-Server-FQDN in die Zone “Lokales Intranet”oder “Vertrauenswürdige Sites”in Internet Explorer einzufügen, um diesen zusätzlichen Schritt zu vermeiden.

Hinzufügen vertrauenswürdiger Websites über die Verwaltungskonsole

1. Wählen Sie auf dem Bildschirm Receiver für Web-Site bearbeiten die Registerkarte **Websiteverknüpfungen**.



2. Klicken Sie auf **Hinzufügen**, um die URL für eine Website hinzuzufügen, auf der Sie Verknüpfungen hosten möchten. URLs müssen in dem Format *http[s]://hostname[:port]* angegeben werden, wobei "hostname"der vollqualifizierte Domänenname des Websitehosts und "port"der Port ist, der für die Kommunikation mit dem Host verwendet wird, wenn der Standardport für das Protokoll nicht verfügbar ist. Pfade zu spezifischen Seiten auf der Website sind nicht erforderlich. Wenn Sie eine URL ändern möchten, wählen Sie den Eintrag in der Liste "Websites"aus und klicken Sie auf **Bearbeiten**. Wählen Sie einen Eintrag in der Liste aus und klicken Sie auf **Entfernen**, wenn Sie die URL einer Website löschen möchten, auf der Sie keine Verknüpfungen zu über Citrix Receiver für Web-Site verfügbaren Ressourcen mehr hosten möchten.
3. Klicken Sie auf **Anwendungsverknüpfungen abrufen** und kopieren Sie die URLs, die Sie für Ihre Website benötigen.



Vertrauenswürdige Websites mit dem PowerShell-SDK hinzufügen

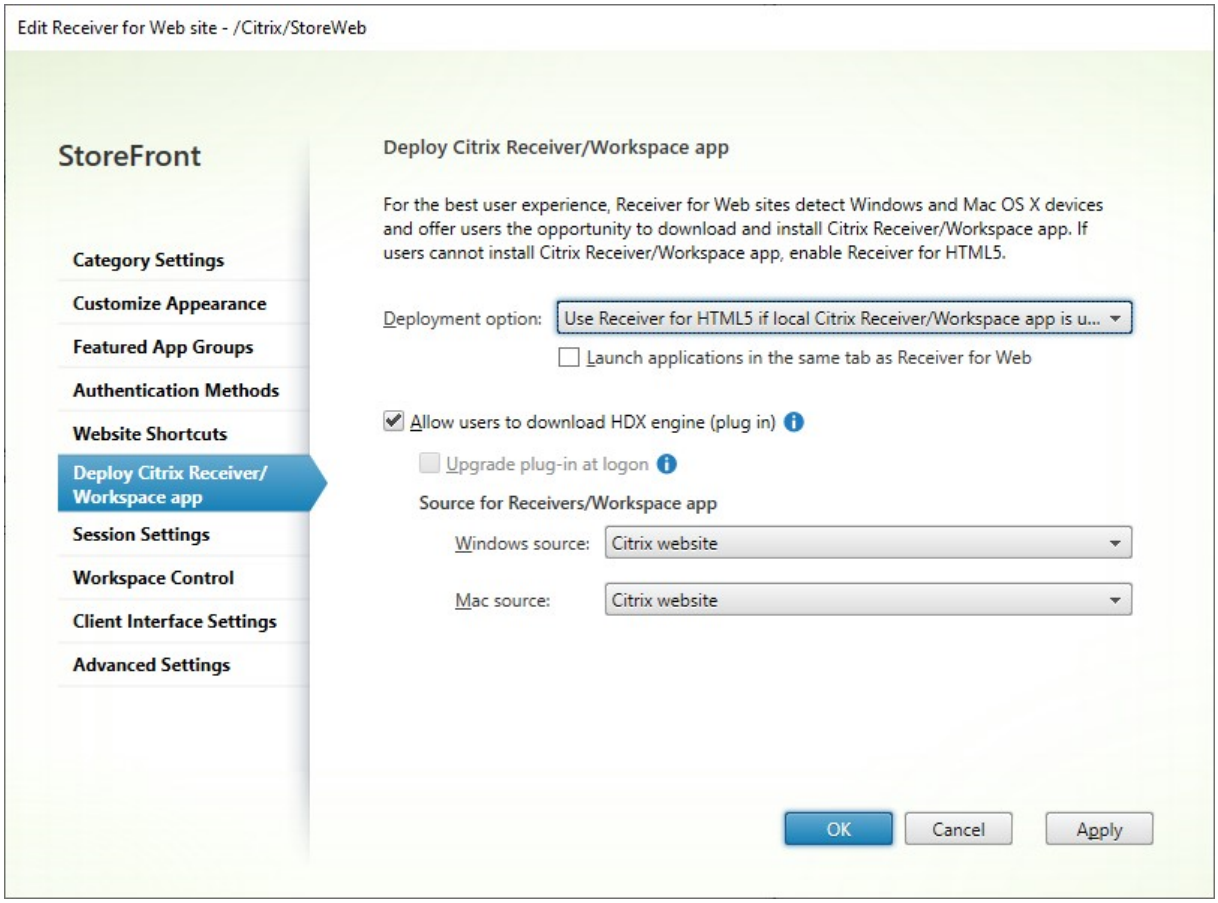
Sie können vertrauenswürdige URLs mit dem PowerShell Cmdlet Set-STFWebReceiverApplicationShortcuts hinzufügen.

Bereitstellung der Citrix Workspace-App

April 17, 2024

Wenn ein Benutzer erstmalig mit einem Browser unter Windows, macOS oder Linux auf einen Store zugreift, versucht StoreFront automatisch festzustellen, ob die Citrix Workspace-App lokal installiert ist.

Wenn eine lokal bereitgestellte Citrix Workspace-App nicht erkannt wird, wird der Benutzer aufgefordert, die App herunterzuladen und zu installieren. Der Standardort für den Download ist die Citrix Website, aber Sie können die Installationsprogramme auch auf dem StoreFront-Server oder an einem anderen Ort hosten. Benutzer, die die Citrix Workspace-App nicht lokal installieren können, können die Citrix Workspace-App für HTML5 über ihren Webbrowser verwenden.



Um die Bereitstellungsoptionen zu ändern, gehen Sie zu Receiver für Website bearbeiten und wählen Sie die Registerkarte **Citrix Receiver/Workspace-App bereitstellen**.

Bereitstellungsoption

- Wählen Sie **Immer Receiver für HTML5 verwenden**, wenn die Benutzer ohne Erscheinen der Aufforderung, die Citrix Workspace-App lokal herunterzuladen und zu installieren, immer über einen Webbrowser auf Ressourcen zugreifen sollen. Wenn diese Option ausgewählt ist, greifen Workspace für HTML5-Benutzer immer direkt über ihren Browser auf Ressourcen zu.
- Wählen Sie **Receiver für HTML5 verwenden, wenn lokaler Receiver nicht verfügbar ist**, wenn die Benutzer von der Store-Website aufgefordert werden sollen, die Citrix Workspace-App herunterzuladen und lokal zu installieren, aber auf den Zugriff auf Ressourcen über einen Browser zurückgegriffen wird, wenn eine Installation der Citrix Workspace-App nicht möglich ist. Benutzer ohne Citrix Workspace-App werden dann bei jeder Anmeldung an der Site aufgefordert, die App herunterzuladen und zu installieren.
- Wählen Sie **Lokal installieren**, wenn immer über eine lokal installierte Citrix Workspace-App auf Ressourcen zugegriffen werden soll. Die Benutzer werden aufgefordert, die Citrix Workspace-App für ihre Plattform herunterzuladen und zu installieren. Die Benutzer können weiterhin über

einen Browser auf den Store zugreifen, aber wenn sie eine Ressource starten, wird diese in der lokal installierten Workspace-App geöffnet.

Anwendungen auf derselben Registerkarte starten

Wenn Sie **Immer Receiver für HTML5 verwenden** oder **Receiver für HTML5 verwenden, wenn lokaler Receiver nicht verfügbar ist** ausgewählt haben, wird für im Browser gestartete Ressourcen standardmäßig eine neue Registerkarte geöffnet. Sollen Ressourcen auf derselben Registerkarte geöffnet werden, wählen Sie **Anwendungen auf der gleichen Registerkarte starten wie Receiver für Web**.

Benutzern erlauben, die Citrix Workspace-App für Windows oder Mac herunterzuladen

Wenn Sie **Lokal installieren** oder **Receiver für HTML5 verwenden, wenn lokaler Receiver nicht verfügbar ist** wählen und die Option **Benutzer können HDX Engine (Plug-In) herunterladen** aktivieren, erhalten die Benutzer die Möglichkeit, die Citrix Workspace-App für Windows oder Mac herunterzuladen, wenn die Workspace-App für HTML5 keine lokal installierte Workspace-App erkennt.

Workspace-App bei der Anmeldung aktualisieren

Wenn Sie **Plug-In beim Anmelden aktualisieren** auswählen, bietet die Workspace-App für HTML5 den Benutzern die Möglichkeit, den lokal installierten Client der Citrix Workspace-App bei der Anmeldung zu aktualisieren. Die Benutzer können das Upgrade überspringen und werden nur dann erneut zum Upgrade aufgefordert, es sei denn, ihre Browser-Cookies werden gelöscht. Zur Verwendung dieses Features müssen Sie sicherstellen, dass die Citrix Workspace-App-Dateien auf dem StoreFront-Server verfügbar sind.

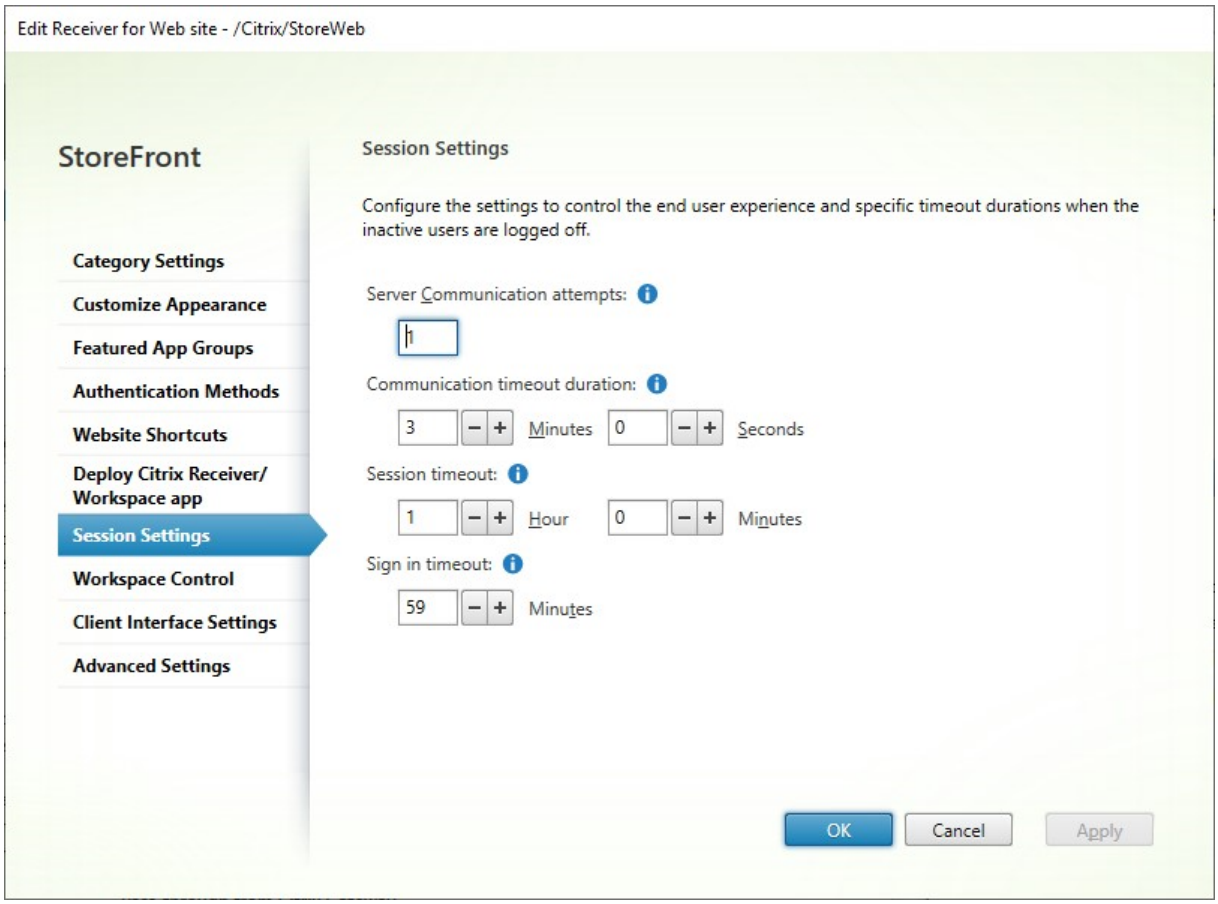
Downloadquelle

Sie können auswählen, ob Benutzer beim Klicken auf die Download-Schaltfläche zur Citrix-Website umgeleitet werden oder Dateien direkt vom Server herunterladen. Die verfügbaren Optionen sind **Citrix Website**, **Lokale Dateien auf dem StoreFront-Server** und **Dateien auf dem Remoteserver (per URL)**.

Sitzungseinstellungen konfigurieren

April 17, 2024

Um Sitzungseinstellungen zu ändern, gehen Sie zum Bildschirm Receiver für Web-Site bearbeiten und wählen Sie die Registerkarte **Sitzungseinstellungen**.



Serverkommunikationsversuche

Anzahl der Aufrufe zwischen dem Webproxy und den StoreFront-internen Store-Diensten. Normalerweise muss diese Einstellung nicht geändert werden.

Dauer für Kommunikationstimeout

Die für Aufrufe zwischen dem Webproxy und den StoreFront-internen Store-Diensten zulässige Zeitdauer. Normalerweise muss diese Einstellung nicht geändert werden.

Timeout bei Sitzungsinaktivität

Beim Zugriff auf einen StoreFront-Store über einen Browser wird nach einer festgelegten Zeit der Inaktivität die Meldung **Sitzungstimeout aufgrund von Inaktivität** angezeigt. Sie können das

Sitzungstimeout an das Nutzungsmuster der Benutzer anpassen. Dies hat keine Auswirkungen auf Citrix Workspace-Apps.

Alternativ können Sie PowerShell verwenden. Um zum Beispiel das Timeout für die Website "/Citrix/-StoreWeb"auf 30 Minuten festzulegen, gehen Sie folgendermaßen vor:

```
$rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'
Set-STFWebReceiverService $rfw -SessionStateTimeout 30
<!--NeedCopy-->
```

Wenn Sie das Sitzungstimeout auf eine längere Dauer als die Lebensdauer des Authentifizierungstokens oder die maximale Tokenlebensdauer ändern, wird dessen Lebensdauer entsprechend aktualisiert.

Lebensdauer des Authentifizierungstokens

Beim Zugriff auf einen StoreFront-Store über einen Browser erfolgt standardmäßig nach acht Stunden eine Abmeldung, unabhängig von jedweder Aktivität. Dies hat keine Auswirkungen auf Citrix Workspace-Apps. Um dieses Timeout zu verlängern gehen Sie folgendermaßen vor:

1. Navigieren Sie in StoreFront zu **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Öffnen Sie die Datei `web.config`.
3. Gehen Sie zu dem Eintrag: **<authentication tokenLifeTime="08:00:00"method ="Auto"/>**
4. Ändern Sie **tokenLifeTime** auf den gewünschten Wert. Verwenden Sie das Format `d.h:m:s`, um einen Wert von einem Tag oder mehr einzugeben.

Wenn Sie das Sitzungstimeout auf mehr als 20 Stunden erhöhen, müssen Sie auch die maximale Token-Lebensdauer des Authentifizierungsdiensts erhöhen.

Maximale Tokenlebensdauer des Authentifizierungsdiensts

Der Authentifizierungsdienst gibt Tokens aus, die beim Zugriff auf einen Store über einen Webbrowser oder die Citrix Workspace-Apps verwendet werden. Bei Citrix Workspace-Apps ist dies das einzige Anmeldetimeout, das aktualisiert werden muss. Beim Zugriff auf StoreFront über einen Browser wird dieses Timeout zusammen mit den anderen Timeouts verwendet. Im Gegensatz zu anderen auf dieser Seite beschriebenen Einstellungen gilt dies für alle Websites des Stores.

Wenn StoreFront Citrix Gateway vorgeschaltet ist, verfügt das Citrix Gateway über die Benutzeranmeldeinformationen und führt das Single Sign-On für StoreFront durch. Wenn das StoreFront-Token abläuft, gibt StoreFront eine CitrixAG Basic-Herausforderung aus und Citrix Gateway stellt die Anmeldeinformationen für die Anmeldung bei StoreFront bereit. Wenn Sie Citrix Gateway verwenden, müssen Sie daher auch dessen Sitzungstimeout konfigurieren.

1. Gehen Sie für die auf dem StoreFront-Server installierte Citrix Workspace-App zum Pfad des Authentifizierungsdiensts Ihres Stores **`c:\inetpub\wwwroot\Citrix\<Store>Auth`**. (Es kann sich, je nachdem, wie viele Stores Sie haben, um einen von mehreren Authentifizierungsdiensten handeln.)
2. Suchen Sie in der Datei `web.config` den Dienst **Authentication Token Producer** und darin das Element `add`, dessen `id` dem von **Authentication Token Producer** entspricht. Im folgenden Beispiel benötigen Sie das Element `add` mit `id="f7cac185-57c1-4629-a33c-88a89dd4295d"encipherId="2948f7ad-735e-4e03-8e01-8d4f5d3ca75b"`:

```
<service id="f7cac185-57c1-4629-a33c-88a89dd4295d" displayName="
    Authentication Token Producer">
     <relyingParties signingId="2948f7ad-735e-4e03-8e01-8
        d4f5d3ca75b" defaultLifetime="01:00:00" maxLifetime="
        01:00:00">
     <clear />
     <add id="f7cac185-57c1-4629-a33c-88a89dd4295d" encipherId="
        2948f7ad-735e-4e03-8e01-8d4f5d3ca75b" defaultLifetime="
        01:00:00" maxLifetime="20:00:00" />
<!--NeedCopy-->
```

3. Ändern Sie **`maxLifetime`** auf den gewünschten Wert. Der Standardwert ist `20:00:00`. Verwenden Sie das Format `dd.hh:mm:ss`, um einen Wert von einem Tag oder mehr einzugeben.
4. Führen Sie den Befehl **`iisreset`** aus, um die Änderungen anzuwenden. Wenn Sie diesen Befehl ausführen, werden die Benutzer von Citrix StoreFront Web abgemeldet, dies hat jedoch keine Auswirkungen auf ihre aktuelle ICA-Sitzung.

Workspace Control

May 31, 2024

Wenn Benutzer zwischen Geräten wechseln, wird von Workspace Control sichergestellt, dass die benutzten Anwendungen ihnen folgen. Benutzer können mit den gleichen Anwendungsinstanzen über mehrere Geräte hinweg arbeiten anstatt alle Anwendungen neu starten zu müssen, wenn sie sich an einem neuen Gerät anmelden. So können etwa Krankenhausärzte Zeit sparen, wenn sie sich von Arbeitsstation zu Arbeitsstation bewegen und auf Patientendaten zugreifen.

Wenn Benutzer sich anmelden, werden sie automatisch mit allen Anwendungen wieder verbunden, die sie nicht beendet haben. Beispiel: Ein Benutzer meldet sich bei einem Store an und startet einige Anwendungen. Wenn der Benutzer sich anschließend bei dem gleichen Store mit der gleichen Zugriffsmethode aber auf einem anderen Gerät anmeldet, werden die ausgeführten Anwendungen automatisch auf das neue Gerät übertragen. Alle Anwendungen, die ein Benutzer über einen bestimmten

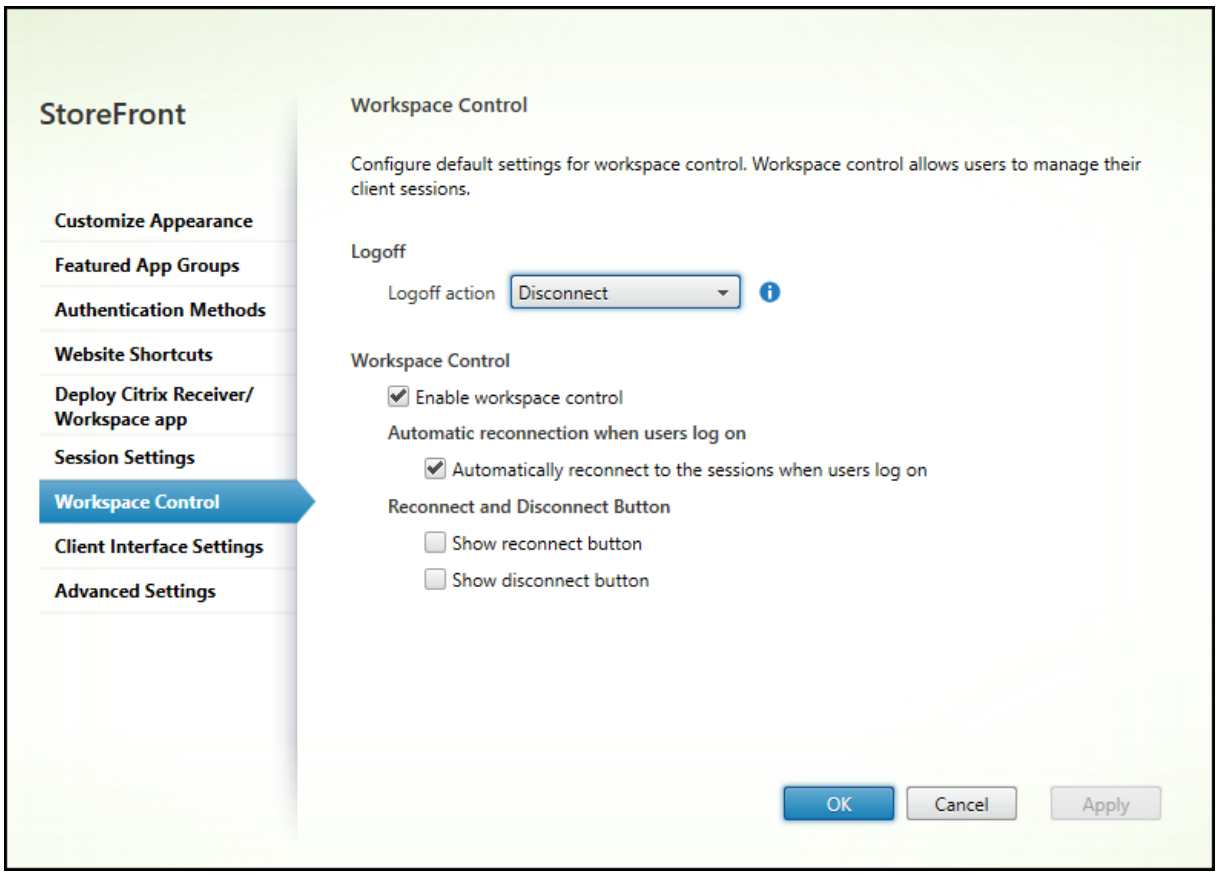
Store startet, werden bei Abmeldung des Benutzers von dem Store automatisch getrennt, jedoch nicht heruntergefahren. Beim Zugriff über einen Webbrowser muss für Anmeldung, Anwendungsstart und Abmeldung der gleiche Browser verwendet werden.

Workspace Control für die Workspace-App für HTML5 konfigurieren

Die Workspace Control-Einstellungen in der StoreFront-Verwaltungskonsole gelten nur für den Zugriff auf Stores über einen Webbrowser. Es gelten folgende Anforderungen und Einschränkungen:

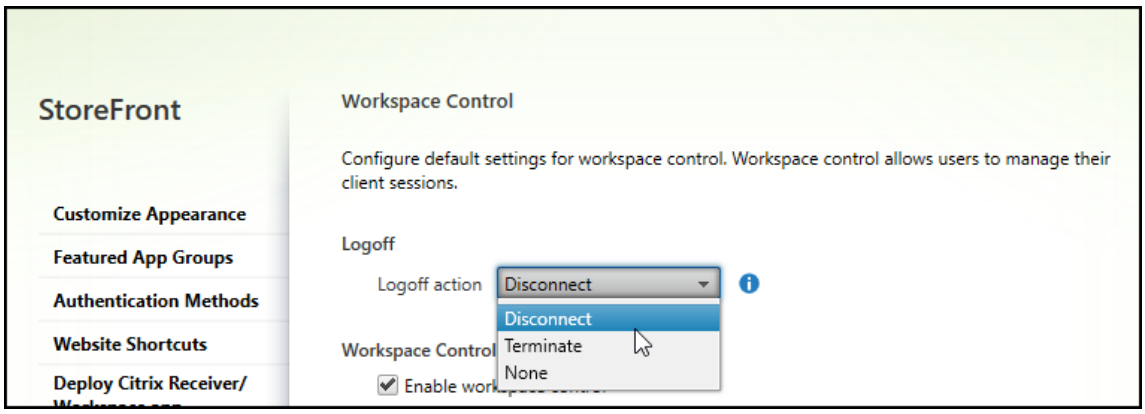
- Workspace Control ist nicht verfügbar, wenn die Workspace-App für HTML innerhalb eines gehosteten Desktops oder einer gehosteten Anwendung ausgeführt wird.
- Bei Benutzern, die über Windows-Geräte auf Websites zugreifen, ist Workspace Control nur dann aktiviert, wenn die Site feststellen kann, dass die Citrix Workspace-App für Windows auf den Geräten der Benutzer installiert ist oder wenn die Citrix Workspace-App für HTML5 für den Zugriff auf Ressourcen verwendet wird.
- Um eine Verbindung zu getrennten Anwendungen wiederherzustellen, müssen Benutzer, die über Internet Explorer auf Websites zugreifen, die Site den Zonen "Lokales Intranet"oder "Vertrauenswürdige Sites"hinzufügen.
- Wenn nur ein Desktop für einen Benutzer auf einer Website verfügbar ist, die so konfiguriert ist, dass einzelne Desktops bei Anmeldung automatisch gestartet werden, erfolgt unabhängig von der Workspace Control-Konfiguration keine Wiederverbindung der Anwendungen des Benutzers.
- Benutzer müssen die Verbindung zu ihren Anwendungen mit demselben Browser trennen, den sie ursprünglich zum Starten der Anwendungen verwendet haben. Verbindungen mit Ressourcen, die mit einem anderen Browser oder lokal vom Desktop bzw. über das Startmenü mit der Citrix Workspace-App gestartet wurden, können nicht mit Citrix Workspace-App für HTML5 getrennt oder heruntergefahren werden.
- Workspace Control ist nicht verfügbar, wenn Ressourcen in derselben Registerkarte eines Browsers geöffnet werden. Informationen zur Konfiguration finden Sie unter Bereitstellung der Citrix Workspace-App.

Um die Workspace Control-Einstellungen für den Zugriff auf einen Store über einen Webbrowser zu ändern, wählen Sie auf dem Bildschirm Receiver für Web-Site bearbeiten die Option **Workspace Control**.



Konfigurieren Sie die Einstellungen für Workspace Control wie folgt:

- Geben Sie die **Abmeldeaktion** an. Abmeldeaktionen:
  - **Trennen**: Wenn Sie sich von der Site abmelden, werden die App- und Desktopsitzungen automatisch vom Clientgerät getrennt.
  - **Beenden**: Wenn Sie sich von der Site abmelden, werden App- und Desktopsitzungen automatisch auf dem Server beendet.
  - **Ohne**: Wenn Sie sich von der Site abmelden, werden App- und Desktopsitzungen weiter ausgeführt.



- Aktivieren Sie das Kontrollkästchen **Workspace Control aktivieren**.
- Aktivieren Sie das Kontrollkästchen **Automatisch beim Anmelden der Benutzer mit der Sitzung wieder verbinden** unter **Automatische Wiederverbindung bei Benutzeranmeldung**.

Workspace Control mithilfe des PowerShell-SDKs konfigurieren

Sie können Workspace Control mit dem PowerShell-Cmdlet Set-STFWebReceiverUserInterface konfigurieren.

Workspace Control für die Workspace-App für Windows konfigurieren

Informationen zur Konfiguration von Workspace Control in Workspace für Windows finden Sie unter Wiederverbindung über Workspace Control verwalten.

Workspace Control für die Workspace-App für Mac konfigurieren

Informationen zur Konfiguration von Workspace Control für die Workspace-App für Mac finden Sie unter Workspace Control-Einstellungen konfigurieren.

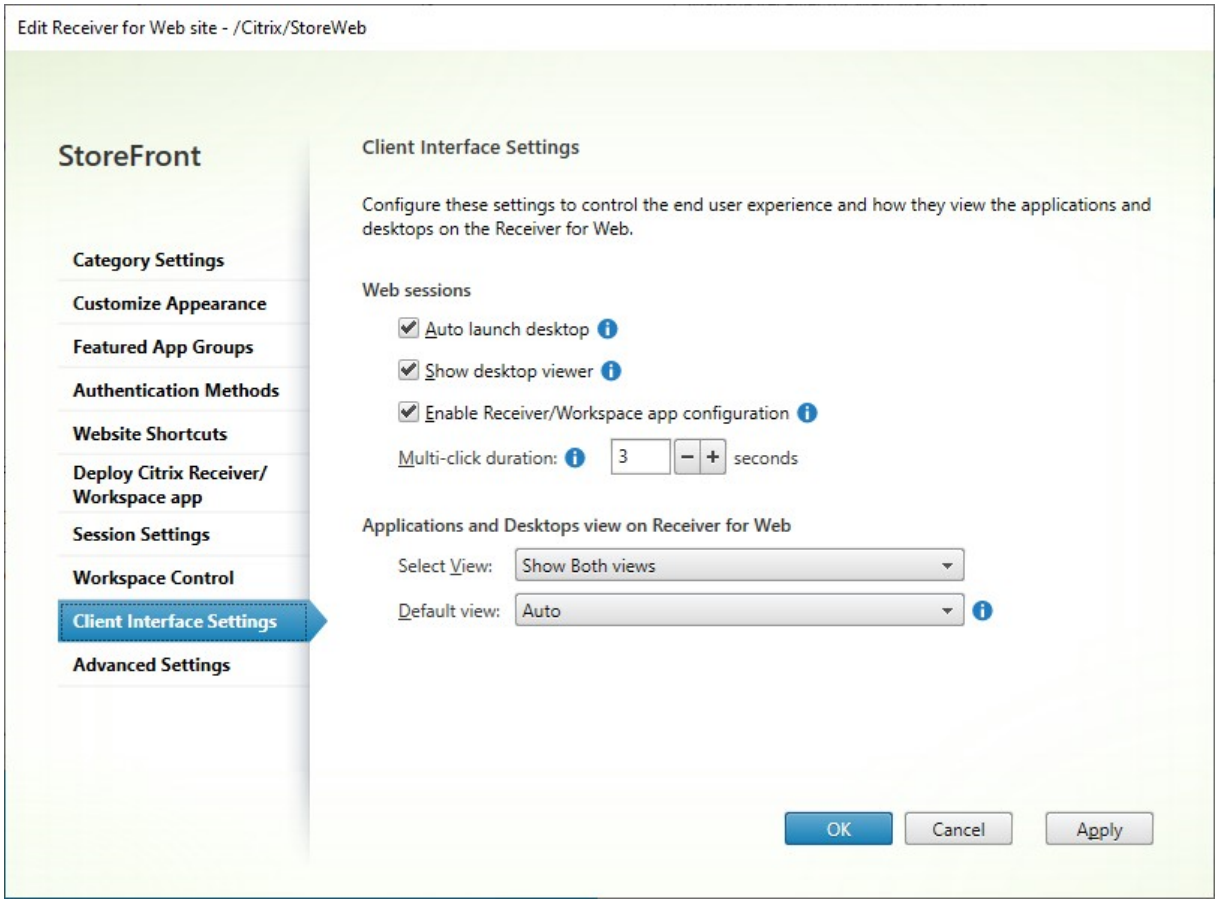
Workspace Control für alle Apps deaktivieren

Um die Sitzungswiederverbindung in StoreFront für alle Workspace-Apps unabhängig von deren Konfiguration zu deaktivieren, gehen Sie zur Registerkarte **Erweiterte Einstellungen** und deaktivieren Sie die Option **Sitzungswiederverbindung zulassen**.

Einstellungen für die Clientoberfläche

May 31, 2024

Um die Einstellungen der Clientbenutzeroberfläche im Fenster Receiver für Web-Site bearbeiten zu ändern, wählen Sie die Registerkarte **Einstellungen für die Clientoberfläche** aus.



Desktop automatisch starten

Wenn diese Einstellung aktiviert ist und ein Benutzer nur über einen Desktop verfügt, wird dieser gestartet, wenn sich der Benutzer anmeldet.

Um die Einstellung "Desktop automatisch starten"mit dem PowerShell-SDK zu ändern, rufen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `AutoLaunchDesktop` auf.

Diese Einstellung gilt nur, wenn Sie auf Citrix Receiver für Websites zugreifen. Sie gilt nicht, wenn Sie über lokal installierte Citrix Workspace-Apps auf Stores zugreifen.

Desktop Viewer anzeigen

Der Desktop Viewer ist die Symbolleiste, die einfachen Zugriff auf die HDX-Einstellungen bietet. Verwenden Sie diese Einstellung, um auszuwählen, ob sie angezeigt wird.

Multiklickdauer

Verhindert, dass Benutzer dieselbe Anwendung innerhalb der konfigurierten Dauer mehrmals starten. Die Einstellung gilt nur für die Citrix Workspace-App für HTML5 (nicht für die native Citrix Workspace-App).

Um die Multiklickdauer mit dem PowerShell-SDK zu ändern, rufen Sie das Cmdlet Set-STFWebReceiverUserInterfac mit dem Parameter `MultiClickTimeout` auf.
Diese Einstellung gilt nur für die Citrix Workspace-App für HTML5. Sie gilt nicht für lokal installierte Citrix Workspace-Apps.

Receiver-/Workspace-App-Konfiguration aktivieren

Wenn diese Option aktiviert ist, bietet die Citrix Workspace-App für HTML5 Provisioning-Dateien, mit denen die Benutzer die native Citrix Workspace-App automatisch für den zugehörigen Store konfigurieren können. Die Provisioningdateien enthalten Verbindungsinformationen für den Store, über den die Ressourcen auf der Website bereitgestellt werden, einschließlich Details jeglicher für den Store konfigurierter Citrix Gateway-Bereitstellungen und Beacons.

Um die Option mit dem PowerShell-SDK zu ändern, rufen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `ReceiverConfigurationEnabled` auf.

Anwendungs- und Desktopansicht

Wenn sowohl Desktops als auch Anwendungen verfügbar sind, werden in der Citrix Workspace-App standardmäßig separate Ansichten für Desktops und Anwendungen angezeigt. Favoriten werden in der **Home**-Ansicht angezeigt. Den Benutzern wird nach der Anmeldung an der Site zuerst die **Home**-Ansicht angezeigt.

Wählen Sie in der Dropdownliste **Ansicht auswählen** aus, ob Apps oder Desktops oder beides angezeigt werden sollen.

Wählen Sie in der Dropdownliste **Standardansicht** aus, welche Ansicht angezeigt wird, wenn sich der Benutzer anmeldet.

Option	Beschreibung
Automatisch	Home-Ansicht anzeigen
Apps	App-Ansicht anzeigen
Desktops	Desktopansicht anzeigen

Um diese Optionen mit dem PowerShell-SDK zu ändern, rufen Sie das Cmdlet Set-STFWebReceiverUserInterface mit den Parametern `ShowAppsView`, `ShowDesktopsView` und `DefaultView` auf.

Website entfernen

September 27, 2023

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Store**, wählen Sie im Bereich **Aktionen** den Store, für den Sie die Citrix Receiver für Web-Site erstellen möchten, und klicken Sie auf **Receiver für Web-Sites verwalten**.
2. Wählen Sie eine Site und klicken Sie auf **Entfernen**. Wenn Sie eine Site entfernen, können Benutzer diese nicht mehr für den Zugriff auf den Store verwenden.

Workspace-App-Website konfigurieren

September 27, 2023

Wenn Sie einen Store mit StoreFront erstellen, wird automatisch eine Website erstellt und dem Store zugewiesen. Wenn ein Store über mehrere Websites verfügt, wählen Sie diejenige aus, die angezeigt werden soll, wenn die Benutzer mit der Citrix Workspace-App auf den Store zugreifen.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores**.
2. Wählen Sie im mittleren Bereich einen Store aus und klicken Sie im **Aktionsbereich** auf **Einheitliche Benutzeroberfläche konfigurieren**. Wenn Sie keine Citrix Receiver für Web-Site erstellt haben, wird eine entsprechende Meldung mit einem Link zum Assistenten zum Hinzufügen einer solchen Site angezeigt.
3. Wählen Sie die Website aus, die von den Citrix Workspace-App-Clients angezeigt werden soll, wenn Benutzer auf diesen Store zugreifen.
4. Klicken Sie auf **OK**.

Servergruppen konfigurieren

April 17, 2024

Mit den folgenden Anleitungen können Sie die Einstellungen von StoreFront-Multiserverbereitstellungen ändern. Verwenden Sie zur Verwaltung einer Multiserverbereitstellung jeweils nur einen Server, um

Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Alle vorgenommenen Konfigurationsänderungen müssen an die anderen Server der Gruppe weitergegeben werden, damit eine konsistente Konfiguration der gesamten Bereitstellung gewährleistet ist.

Sie müssen den StoreFront-Installationsort und die IIS-Website-Einstellungen (z. B. physischer Pfad und Site-IDs) auf den Servern einer StoreFront-Servergruppe identisch konfigurieren.

Hinzufügen eines Servers zu einer Servergruppe

Mit der Aufgabe Server hinzufügen können Sie einen Autorisierungscode abrufen, der es Ihnen ermöglicht, der vorhandenen Bereitstellung einen neu installierten StoreFront-Server hinzuzufügen. Weitere Informationen zum Hinzufügen neuer Server zu vorhandenen StoreFront-Bereitstellungen finden Sie unter Vorhandener Servergruppe beitreten. Informationen zur Einschätzung der Zahl der in der Gruppe benötigten Server finden Sie unter *Planen der StoreFront- Bereitstellung* im Abschnitt Skalierbarkeit.

Entfernen von Servern aus einer Servergruppe

Mit der Aufgabe **Server entfernen** können Sie Server aus einer StoreFront-Multiserverbereitstellung löschen. Sie können jeden Server in der Gruppe mit Ausnahme des Servers, auf dem Sie die Aufgabe ausführen, entfernen. Entfernen Sie den Server zuerst aus der Lastausgleichsumgebung und dann aus der Multiserverbereitstellung.

Bevor ein entfernter StoreFront-Server wieder zur gleichen oder einer anderen Servergruppe hinzugefügt werden kann, müssen Sie ihn auf die werkseitigen Standardeinstellungen zurücksetzen. Siehe Zurücksetzen eines Servers auf die Werkseinstellungen.

Weitergeben lokaler Änderungen an eine Servergruppe

Mit der Aufgabe Änderungen verteilen können Sie die Konfiguration aller anderen Server in einer StoreFront-Multiserverbereitstellung aktualisieren, damit sie mit der Konfiguration des aktuellen Servers übereinstimmt. Die Verteilung von Konfigurationsinformationen wird manuell initiiert, sodass Sie die Kontrolle darüber behalten, ob und wann die Server in der Gruppe mit Konfigurationsänderungen aktualisiert werden. Beachten Sie bei dieser Aufgabe, dass Sie erst dann weitere Änderungen machen, wenn alle Server in der Gruppe aktualisiert wurden.

> **Wichtig:**
>
> Alle Änderungen, die auf anderen Servern in der Gruppe vorgenommen wurden, werden bei der

> Verteilung verworfen. Wenn Sie die Konfiguration eines Servers aktualisieren, verteilen Sie die Änderungen auf die anderen Server in der Gruppe, um zu vermeiden, dass die Änderungen verloren gehen, falls Sie anschließend Änderungen von einem anderen Server in der Bereitstellung übernehmen.

Die Informationen, die zwischen Servern in der Gruppe übertragen werden, umfassen Folgendes:

- Inhalt aller web.config-Dateien, die die StoreFront Konfiguration enthalten
- Inhalt von `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`, z. B. `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` und `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`
- Inhalt von `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`
- Inhalt von `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`, z. B. kopierte Bilder und benutzerdefinierte JS-Dateien
- Inhalt des Citrix Delivery Services-Zertifikatspeichers, ausgenommen manuell importierte Zertifikatsperrlisten. (Informationen zum Verteilen lokaler Zertifikatsperrlisten (CRLs) finden Sie unter Überprüfung von Zertifikatsperrlisten.

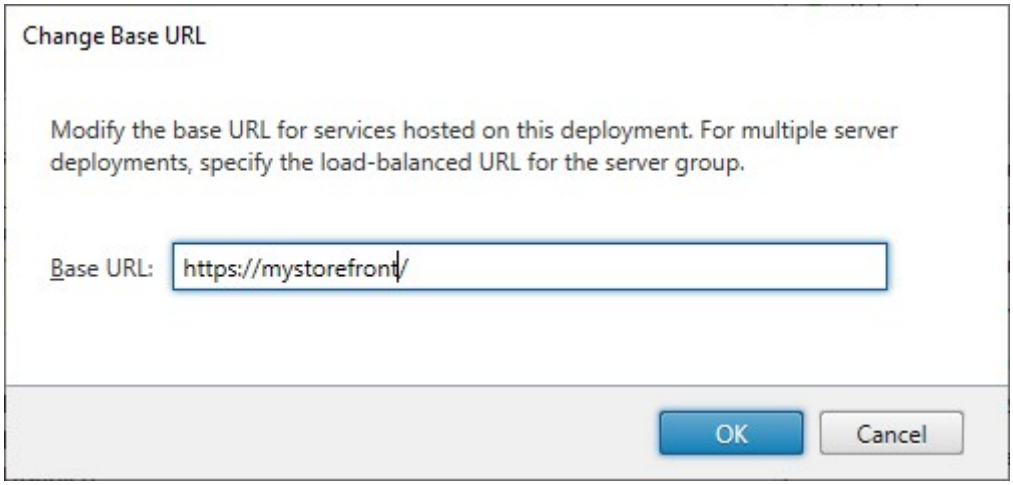
> **Hinweis:**
>
> Abonnementdaten werden unabhängig vom Mechanismus “Änderungen verteilen”mit den anderen Servern synchronisiert. Dies geschieht automatisch, ohne dass der Task “Änderungen verteilen”gestartet wird.

Ändern der Basis-URL für eine Bereitstellung

Die Basis-URL wird als Stamm der URLs für die einer Bereitstellung gehosteten Stores und StoreFront-Dienste verwendet. Geben Sie bei Bereitstellungen mit mehreren Servern die Lastausgleichs-URL an.

Basis-URL ändern:

1. Klicken Sie in der Citrix StoreFront-Verwaltungskonsole links auf den Knoten **Servergruppe**.
2. Klicken Sie im Aktionsbereich auf **Basis-URL ändern...**.
3. Geben Sie die neue URL ein.
4. Klicken Sie auf **OK**.



Integration mit Citrix Gateway und Citrix ADC

May 31, 2024

Durch Verwenden von Citrix Gateway mit StoreFront können Sie Benutzern außerhalb des Unternehmensnetzwerks einen sicheren Remotezugriff ermöglichen, während Citrix ADC für den Lastausgleich eingesetzt werden kann.

Aufgabe	Detail
Citrix Gateway importieren	Konfiguration aus dem Citrix Gateway exportieren und in StoreFront importieren
Citrix Gateways verwalten	Citrix Gateway-Verbindungseinstellungen hinzufügen, entfernen und bearbeiten
Lastausgleich mit Citrix ADC	Citrix als Load Balancer vor einer StoreFront-Servergruppe konfigurieren
Citrix ADC und StoreFront für die delegierte Formularauthentifizierung (DFA) konfigurieren	
Authentifizierung mit andere Domänen	StoreFront und Citrix Gateway so konfigurieren, dass die Benutzer sich zuerst beim Gateway in einer Domäne und dann bei StoreFront in einer anderen Domäne authentifizieren
Beacons konfigurieren	Beacon-URLs konfigurieren, anhand derer die Citrix Workspace-App ermitteln kann, ob sie sich innerhalb oder außerhalb Ihres Unternehmensnetzwerks befindet

Aufgabe	Detail
Einzelnen FQDN für die interne und externe Verwendung erstellen	Einzelnen vollqualifizierten Domänennamen (FQDN) erstellen, der direkt von Ihrem Unternehmensnetzwerk aus und remote über das Citrix Gateway auf einen Store zugreifen kann

Citrix Gateway importieren

April 17, 2024

Die Remotezugriffeinstellungen in der Citrix Gateway-Verwaltungskonsole müssen mit denen in StoreFront identisch sein. In diesem Artikel wird erläutert, wie Sie die Details eines virtuellen Citrix Gateway-Servers importieren, sodass Citrix Gateway und StoreFront richtig für die Zusammenarbeit konfiguriert sind.

Anforderungen

- Zum Exportieren mehrerer virtueller Gateway-Server in eine ZIP-Datei ist NetScaler 11.1.51.21 oder später erforderlich.

  > **Hinweis:**
  >
  > Citrix ADC-Geräte können nur virtuelle Gateway-Server exportieren, die mit dem Citrix Virtual Apps and Desktops-Assistenten erstellt wurden.

- Die Server-URLs aller STAs (Secure Ticket Authority) in der Datei GatewayConfig.json in der von dem Citrix ADC-Gerät generierten ZIP-Datei müssen von DNS aufgelöst und von StoreFront kontaktiert werden können.
- Die Datei GatewayConfig.json in der von dem Citrix ADC-Gerät generierten ZIP-Datei muss die URL einer Citrix Receiver für Web-Site auf dem StoreFront-Server enthalten. Ab Citrix ADC 11.1 wird dies gewährleistet, indem der StoreFront-Server kontaktiert und alle vorhandenen Stores und Citrix Receiver für Web-Sites aufgelistet werden, bevor die ZIP-Datei generiert wird.
- StoreFront muss unter Einsatz des importierten Gateways die Rückruf-URL in DNS in die IP-Adresse des virtuellen Gateway-VPN-Servers zur Authentifizierung auflösen können.

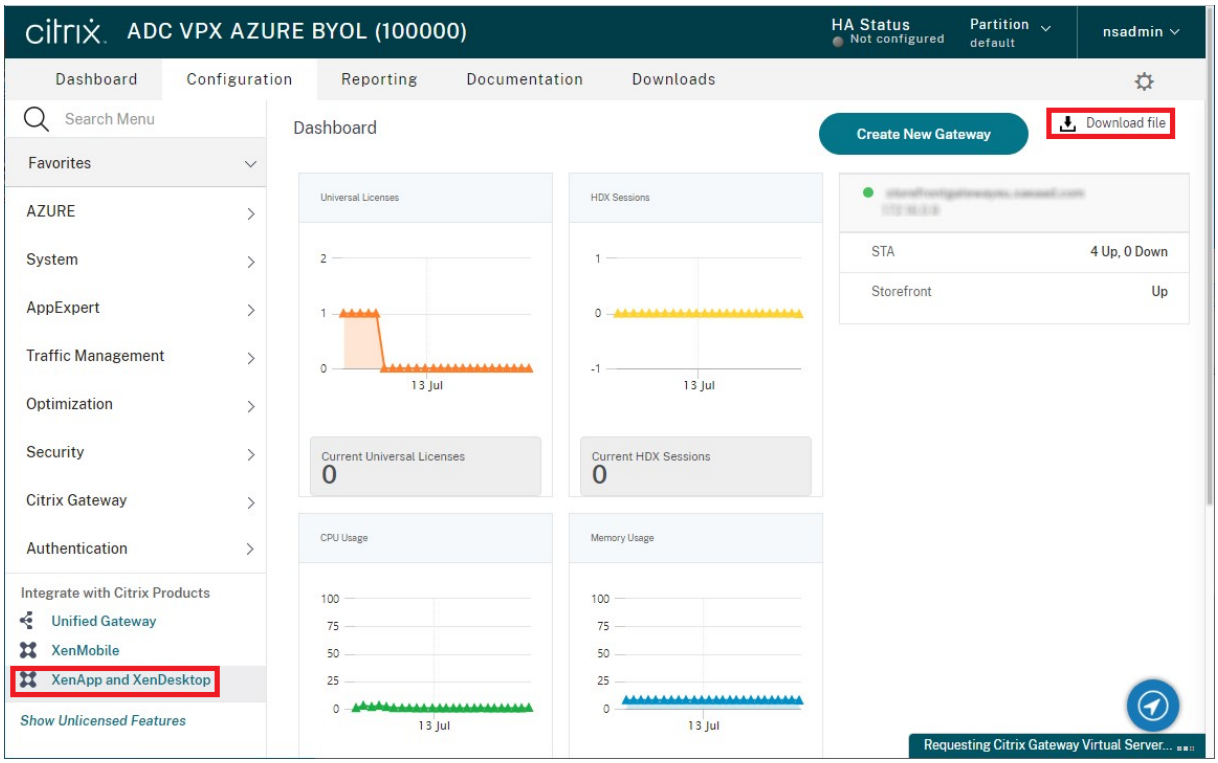
  Normalerweise wird für den Rückruf die gleiche Kombination aus URL und Port verwendet wie für das Gateway, vorausgesetzt, StoreFront kann diese URL auflösen.

Oder

Die Kombination aus URL und Port für den Rückruf darf sich von der für das Gateway unterscheiden, wenn Sie verschiedene externe und interne DNS-Namespaces in Ihrer Umgebung verwenden. Ist das Gateway in einer DMZ und hat eine <example.com>-URL und StoreFront ist im privaten Unternehmensnetzwerk und hat eine <example.local>-URL, können Sie eine <example.local>-Rückruf-URL verwenden, die auf den virtuellen Gateway-Server in der DMZ verweist.

Konfiguration aus Citrix Gateway exportieren

1. Melden Sie sich bei Citrix ADC an.
2. Gehen Sie zur Registerkarte "Konfiguration".
3. Klicken Sie unter "Integrate with Citrix Products"auf "XenApp and XenDesktop".
4. Klicken Sie oben rechts auf "Datei herunterladen".



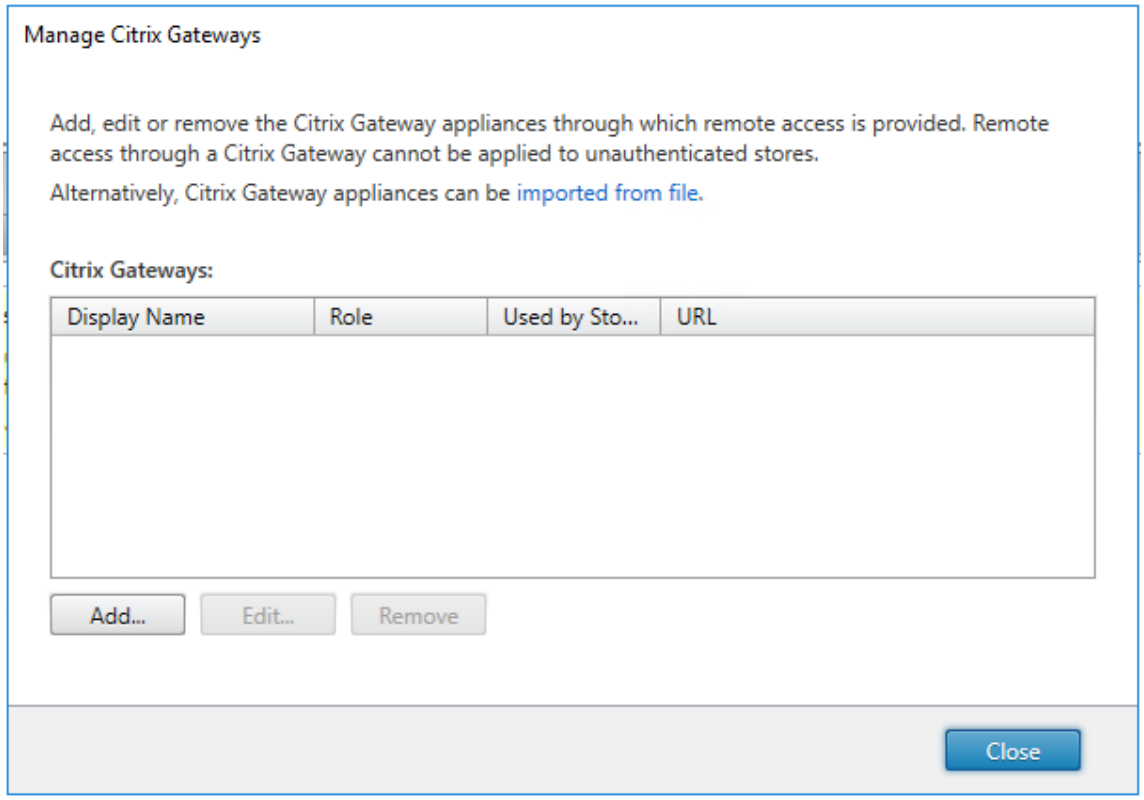
1. Wählen Sie aus, ob Sie die Konfiguration für alle Gateways oder ein bestimmtes Gateway herunterladen möchten.

Importieren eines Citrix Gateways mit der Konsole

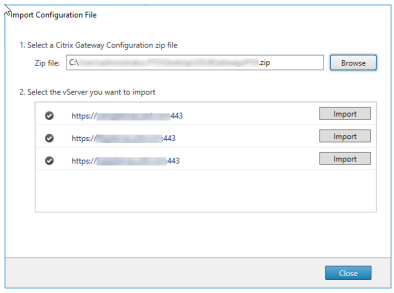
Sie können die Konfiguration eines oder mehrerer virtueller Citrix Gateway-Server mit derselben Importdatei importieren. Für mehrere virtuelle Gateway-Server von verschiedenen Citrix ADC-Geräten müssen Sie mehrere Importdateien verwenden.

> Wichtig:
>
> Manuelles Bearbeiten der Konfigurationsdatei, die aus Citrix Gateway exportiert wurde, wird nicht unterstützt.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** und klicken Sie im Bereich **Aktionen** auf **Citrix Gateways verwalten**.
2. Klicken Sie auf dem Bildschirm **Citrix Gateways verwalten** auf den Importiert-aus-Datei-Link.

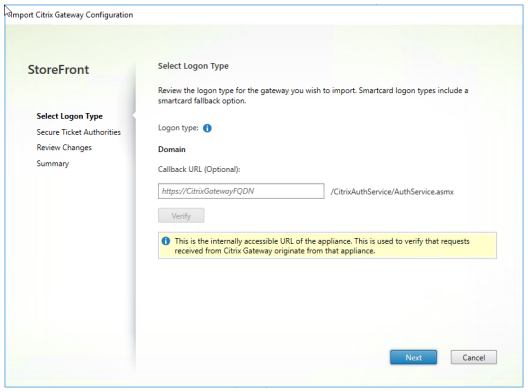


3. Navigieren Sie zu der Konfigurationsdatei des virtuellen Citrix Gateway-Servers.
4. Eine Liste der virtuellen Gateway-Server aus der ausgewählten ZIP-Datei wird angezeigt. Wählen Sie den gewünschten virtuellen Gateway-Server und klicken Sie auf **Importieren**. Wenn Sie den Import eines virtuellen Servers wiederholen, heißt die Schaltfläche “Update” . Mit **Update** erhalten Sie später die Option, das Gateway zu überschreiben oder ein neues Gateway zu erstellen.



5. Überprüfen Sie den **Anmeldetyp** für das ausgewählte Gateway und geben Sie bei Bedarf eine **Rückruf-URL** an. Der Anmeldetyp ist die Authentifizierungsmethode, die Sie auf dem Citrix Gateway-Gerät für Benutzer der Citrix Workspace-App konfiguriert haben. Einige Anmeldetypen erfordern Rückruf-URLs (siehe Tabelle).

    - Klicken Sie auf **Überprüfen**, um zu prüfen, ob die Rückruf-URL gültig und vom StoreFront-Server erreichbar ist.

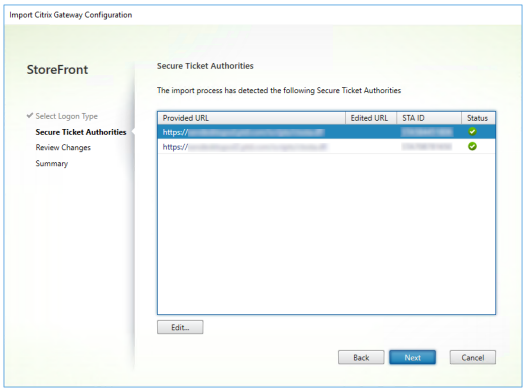


Anmeldeart in der Konsole	LogonType in der JSON-Datei	Rückruf-URL erforderlich
Domäne	Domäne	Nein
Domäne und Sicherheitstoken	DomainAndRSA	Nein
Sicherheitstoken	RSA	Ja
Smartcard - Kein Fallback	SmartCard	Ja
Smartcard - Domäne	SmartCardDomain	Ja
Smartcard - Domäne und Sicherheitstoken	SmartCardDomainAndRSA	Ja
Smartcard - Sicherheitstoken	SmartCardRSA	Ja
Smartcard - SMS-Authentifizierung	SmartCardSMS	Ja
SMS-Authentifizierung	SMS	Ja

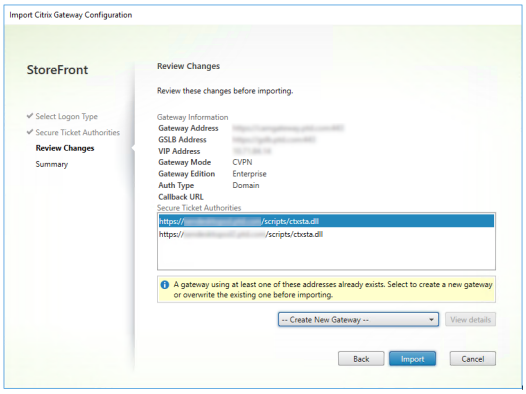
Wenn eine Rückruf-URL erforderlich ist, wird sie von StoreFront automatisch basierend auf der Gateway-URL in der ZIP-Datei eingetragen. Sie können sie in eine beliebige gültige URL ändern, die auf die korrekte virtuelle Citrix Gateway-IP-Adresse verweist. Bei GSLB-Gateways ist für jedes importierte Gateway eine eindeutige Rückruf-URL erforderlich.

Für die Verwendung von Smart Access bzw. der kennwortlosen Authentifizierung ist eine Rückruf-URL erforderlich.

6. Klicken Sie auf **Weiter**.
7. StoreFront kontaktiert über DNS alle STA-Server-URLs (Secure Ticket Authority), die in die ZIP-Datei aufgelistet sind, und prüft, ob es sich um funktionierende STA-Ticketing-Server handelt. Der Import wird nicht fortgesetzt, wenn eine STA-URL ungültig ist.



8. Klicken Sie auf **Weiter**.
9. Überprüfen Sie die Details für den Import. Wenn ein Gateway mit der gleichen URL-/Portkombination (GatewayURL:port) vorhanden ist, verwenden Sie das Dropdownmenü zur Auswahl eines Gateways zum Überschreiben oder Erstellen eines neuen Gateways.



StoreFront prüft anhand der GatewayURL:port-Kombination, ob ein Gateway, das Sie importieren möchten, einem vorhandenen Gateway entspricht, das aktualisiert werden soll. Hat ein Gateway eine andere GatewayURL:port-Kombination, wird es von StoreFront als neues Gateway behandelt. Die folgende Tabelle zeigt, welche Gateway-Einstellungen Sie aktualisieren können.

Gateway-Einstellungen	Aktualisierbar
Gateway-URL:Port-Kombination	Nein
GSLB-URL	Ja
Zertifikat und Fingerabdruck der Netscaler-Vertrauensstellung	Ja
Rückruf-URL	Ja
URL der Receiver für Web-Site	Ja
Gatewayadresse/-VIP	Ja
URL und ID der Secure Ticket Authority	Ja
Alle Anmeldetypen	Ja

10. Klicken Sie auf **Importieren**. Wenn der StoreFront-Server Teil einer Servergruppe ist, erinnert Sie eine Meldung daran, die importierten Gateway-Einstellungen auf die anderen Server in der Gruppe zu übertragen.
11. Klicken Sie auf **Fertig stellen**.

Zum Importieren einer weiteren Konfiguration eines virtuellen Servers wiederholen Sie die Schritte oben.

> **Hinweis:**
>
> Das Standardgateway eines Stores ist das Gateway, über das die Citrix Workspace-App eine Verbindung herstellt, es sei denn, sie ist zur Verwendung eines anderen Gateways konfiguriert. Wenn keine Gateways für den Store konfiguriert sind, wird das erste aus der ZIP-Datei importierte Gateway zum Standardgateway für die Citrix Workspace-App. Durch den Import nachfolgender Gateways ändert sich nichts an dem für den Store festgelegten Standardgateway.

Importieren mehrerer Citrix Gateways mit PowerShell

Read-STFNetScalerConfiguration

- Kopieren Sie die ZIP-Datei auf den Desktop des aktuell angemeldeten StoreFront-Administrators.
- Lesen Sie den Inhalt der ZIP-Datei mit der Konfiguration des virtuellen Citrix Gateway-Servers in den Speicher ein und suchen Sie die drei Gateways anhand ihrer Indexwerte.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
     USERPROFILE\desktop\GatewayConfig.zip"
2 <!--NeedCopy-->
```


Zeigen Sie die drei Gateway-Objekte aus dem Netscaler-ZIP-Importpaket mit dem Cmdlet **STFNetScalerConfiguration** im Speicher an.

```
$ImportedGateways.Document.Gateways[0]
$ImportedGateways.Document.Gateways[1]
$ImportedGateways.Document.Gateways[2]

GatewayMode            : CVPN
CallbackUrl            :
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:443
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.1
Stas                   : {
 STA298854503, STA909374257 }

StaLoadBalance         : True
CertificateThumbprints : {
 F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType        : Domain
GatewayEdition         : Enterprise
ReceiverForWebSites    : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }


GatewayMode            : CVPN
CallbackUrl            :
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:444
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.2
Stas                   : {
 STA298854503, STA909374257 }

StaLoadBalance         : True
CertificateThumbprints : {
 F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType        : DomainAndRSA
GatewayEdition         : Enterprise
ReceiverForWebSites    : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }


GatewayMode            : CVPN
CallbackUrl            : https://emeagateway.example.com:445
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
```



```
49 Address                : https://emeagateway.example.com:445
50 GslbAddress            : https://gslb.example.com:443
51 VipAddress             : 10.0.0.2
52 Stas                   : {
53  STA298854503, STA909374257 }
54
55 StaLoadBalance         : True
56 CertificateThumbprints : {
57  F549AFAA29EBF61E8709F2316B3981AD503AF387 }
58
59 GatewayAuthType        :SmartCard
60 GatewayEdition         : Enterprise
61 ReceiverForWebSites    : {
62  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
       ReceiverForWebSite }
63
64 <!--NeedCopy-->
```

Import-STFNetScalerConfiguration ohne eine CallbackURL

Kopieren Sie die ZIP-Datei auf den Desktop des aktuell angemeldeten StoreFront-Administrators. Lesen Sie das ZIP-Importpaket mit der Citrix Gateway-Konfiguration in den Speicher ein und suchen Sie die drei Gateways anhand ihrer Indexwerte.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
     USERPROFILE\desktop\GatewayConfig.zip"
2 <!--NeedCopy-->
```

Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet **Import-STFNetScalerConfiguration** und geben Sie die erforderlichen Gateway-Indizes an. Der Parameter **-Confirm:$False** verhindert, dass Sie von der Powershell GUI zum Zulassen jedes einzelnen zu importierenden Gateways aufgefordert werden. Entfernen Sie den Parameter, wenn Sie Gateways sorgfältig einzeln importieren möchten.

```
1 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 0 -Confirm:$False
2 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 1 -Confirm:$False
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 2 -Confirm:$False
4 <!--NeedCopy-->
```

Import-STFNetScalerConfiguration mit einer eigenen CallbackURL

Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet **Import-STFNetScalerConfiguration** und geben Sie mit dem Parameter “-callbackURL”eine Rückruf-URL Ihrer Wahl an.


```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
    Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -
    Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -
    Confirm:$False
<!--NeedCopy-->
```

Import-STFNetScalerConfiguration überschreibt die Authentifizierungsmethode, die in der Importdatei gespeichert ist, und lässt Sie ein eine eigene CallbackURL angeben

Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet **Import-STFNetScalerConfiguration** und geben Sie mit dem Parameter "-callbackURL"eine Rückruf-URL Ihrer Wahl an.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:443" -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:444" -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:445" -Confirm:$False
<!--NeedCopy-->
```

Citrix Gateway konfigurieren

April 17, 2024

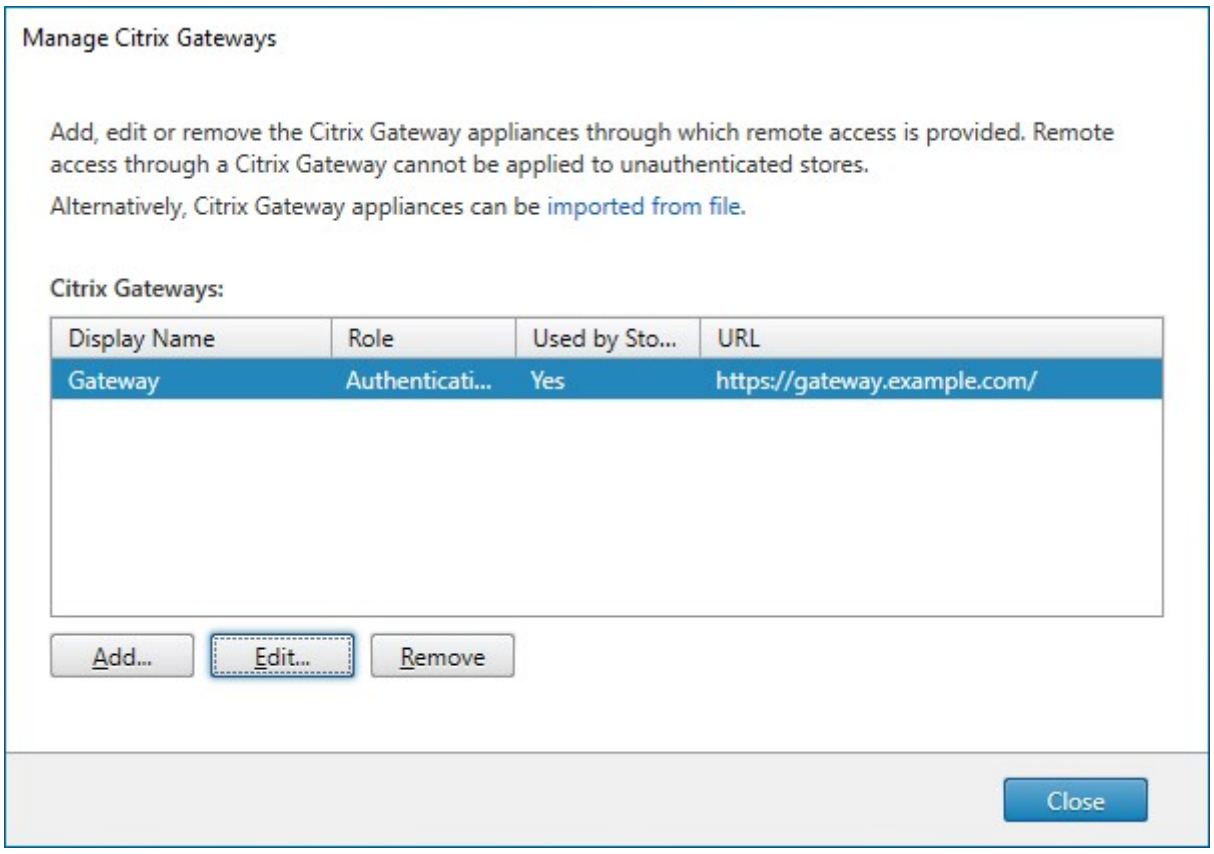
Verwenden Sie Citrix Gateways, um den Remotezugriff auf StoreFront bereitzustellen. Citrix Gateways werden auf einer Hardware- oder Software-Citrix ADC- oder Citrix Gateway-Appliance ausgeführt.

Weitere Informationen zur Konfiguration Ihres Gateways finden Sie unter NetScaler Gateway in StoreFront integrieren.

Sie müssen Ihr Gateway in StoreFront konfigurieren, bevor StoreFront den Zugriff über dieses Gateway zulässt.

Gateways anzeigen

Um die in StoreFront konfigurierten Gateways anzuzeigen, wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores aus und klicken Sie auf **Citrix Gateways verwalten**. Dadurch wird das Fenster **Citrix Gateways verwalten** angezeigt.



PowerShell

Rufen Sie Get-STFRoamingGateway auf, um eine Liste der Gateways und ihrer Konfiguration abzurufen.

Citrix Gateway hinzufügen

> **Wichtig:**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss
> übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie im Fenster **Citrix Gateways verwalten** auf **Hinzufügen**.
2. Geben Sie auf der Registerkarte "Allgemeine Einstellungen"die Einstellungen ein und klicken Sie auf **Weiter**.

   - Geben Sie einen **Anzeigenamen** für die Citrix Gateway-Bereitstellung an, über den die Benutzer sie erkennen können.

     Den Benutzern wird der Anzeigename angezeigt, den Sie in der Citrix Workspace-App angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit die Benutzer leichter entscheiden können, ob sie die Bereitstellung verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der Citrix Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.

   - Geben Sie die URL des Gateways ein.

     Der vollqualifizierte Domänenname (FQDN) für die StoreFront-Bereitstellung muss eindeutig sein und darf nicht dem vollqualifizierten Domänennamen des virtuellen Citrix Gateway-Servers entsprechen. Das Verwenden desselben FQDN für StoreFront und den virtuellen Citrix Gateway-Server wird nicht unterstützt. Das Gateway fügt die URL zum HTTP-Header `X-Citrix-Via` hinzu. StoreFront ermittelt anhand des Headers, welches Gateway verwendet wird.

     Mit der GUI kann nur eine Gateway-URL hinzugefügt werden. Wenn auf ein Gateway über mehrere URLs zugegriffen werden kann, müssen Sie dasselbe Gateway zweimal mit bis auf die URL identischer Konfiguration hinzufügen. Um die Konfiguration zu vereinfachen, können Sie eine sekundäre URL für den Zugriff auf das Gateway konfigurieren. Diese Option ist über die GUI nicht verfügbar, daher müssen Sie PowerShell verwenden. Schließen Sie die Verwaltungskonsole, bevor Sie PowerShell-Befehle ausführen. Wenn Sie beispielsweise mehrere Gateways hinter einem Global Server Load Balancing haben, ist es in der Regel nützlich, sowohl die GSLB-URL als auch eine URL hinzuzufügen, die für den Zugriff auf jedes regionale Gateway verwendet werden kann, beispielsweise zu Test- oder Fehlerbehebungszwecken. Nachdem Sie das Gateway erstellt haben, können Sie mithilfe von `Set-STFRoamingGateway` umd dem Parameter `-GSLBurl` für die sekundäre URL eine

zusätzliche URL hinzufügen. Der Parameter heißt zwar `GSLBurl`, kann jedoch für jede Situation verwendet werden, in der Sie eine zweite URL hinzufügen möchten. Beispiel:

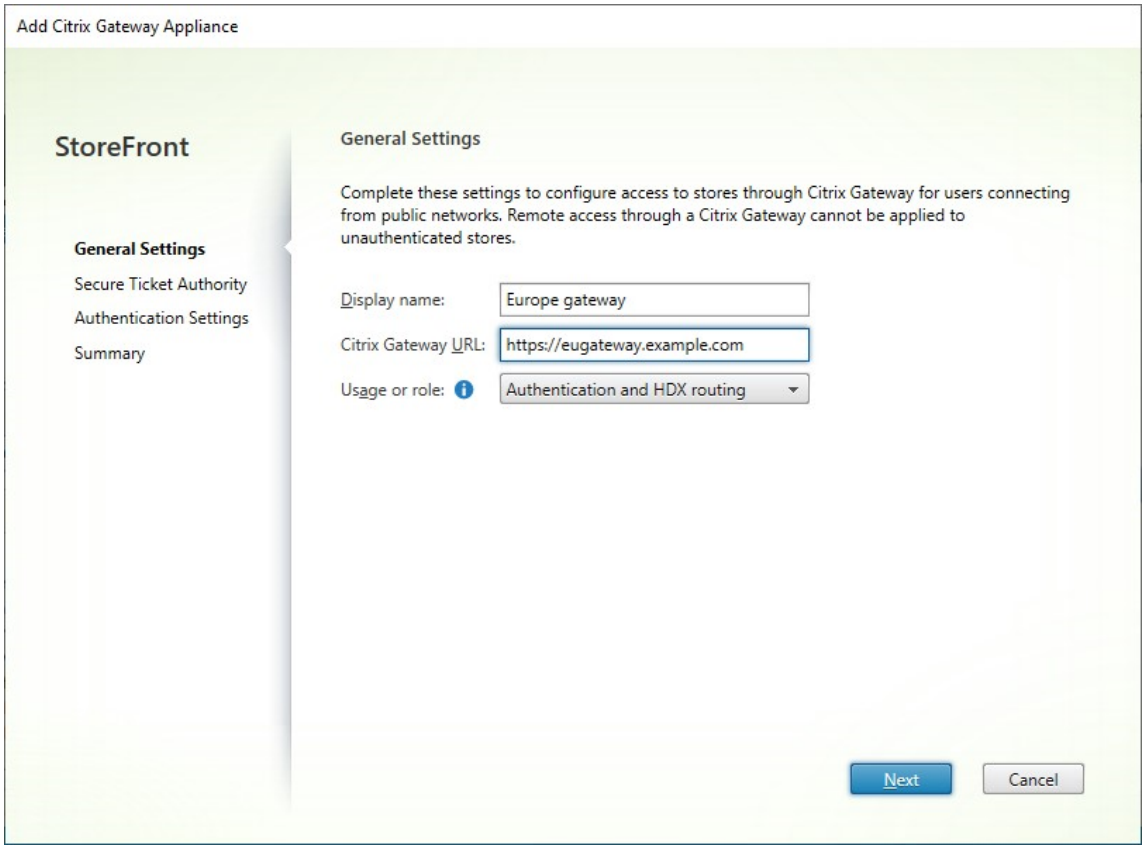
```
1  Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl "
       eugateway.example.com" -GatewayUrl "gslb.example.com"
2  <!--NeedCopy-->
```

> Hinweis:
>
> Unlogischerweise enthält der Parameter `GSLBurl` in diesem Beispiel die regionale URL und der Parameter `GatewayUrl` die GSLB-URL. Für die meisten Zwecke werden die URLs identisch behandelt, und wenn der Store nur über einen Webbrowser aufgerufen wird, können sie auf beiderlei Weise konfiguriert werden. Wenn Sie jedoch über die Citrix Workspace-App auf StoreFront zugreifen, liest die App `GatewayUrl` von StoreFront und verwendet dies für den Remotezugriff. Es ist empfehlenswert, die Konfiguration so zu wählen, dass die App immer eine Verbindung mit der GSLB-URL herstellt.

Wenn Sie mehr als zwei URLs benötigen, müssen Sie dies als separates Gateway konfigurieren.

- Wählen Sie die Verwendung oder Rolle aus:

Verwendung oder Rolle	Beschreibung
Authentifizierung und HDX-Routing	Gateway wird sowohl für den Remotezugriff auf StoreFront als auch für den Zugriff auf die VDAs verwendet.
Nur Authentifizierung	Gateway wird nur für den Remotezugriff auf StoreFront verwendet
Nur HDX-Routing	Gateway wird nur für die Bereitstellung von HDX-Zugriff auf VDAs verwendet (z. B. bei einer Site ohne StoreFront-Instanz)



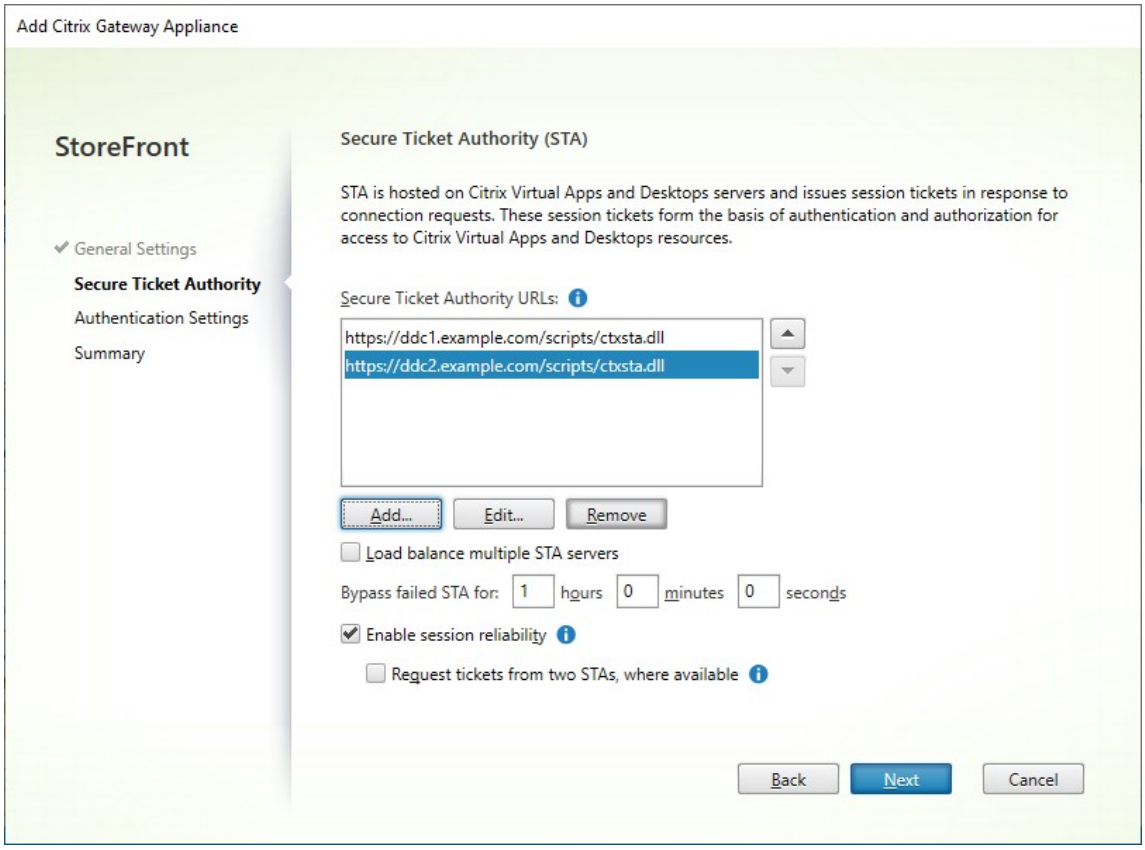
3. Geben Sie die Einstellungen auf der Registerkarte **Secure Ticket Authority** an.

   Die Secure Ticket Authority stellt Sitzungstickets als Antwort auf Verbindungsanfragen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf Citrix Virtual Apps and Desktops-Ressourcen.

   - Geben Sie mindestens eine URL für "Secure Ticket Authority-URL"ein. Wenn Sie Citrix Virtual Apps and Desktops verwenden, können Sie den Delivery Controller als STA verwenden. Wenn Sie Citrix Desktop as a Service verwenden, können Sie die Cloud Connectors angeben, die als Proxy für Anforderungen an die Citrix Cloud Ticket Authority dienen. Die Einträge dieser Liste müssen exakt mit der im Citrix Gateway konfigurierten Liste übereinstimmen.
   - Aktivieren Sie **Lastausgleich von mehreren STA-Servern**, um die Anforderungen über die STA-Server zu verteilen. Wird die Option nicht aktiviert, probiert StoreFront die Server in der Reihenfolge aus, in der sie aufgeführt sind.
   - Wenn StoreFront einen STA-Server nicht erreichen kann, wird dieser Server für einen bestimmten Zeitraum nicht verwendet. Standardmäßig ist dies 1 Stunde, aber Sie können diesen Wert anpassen.
   - Wenn Citrix Virtual Apps and Desktops getrennte Sitzungen aufrechterhalten soll, während die Citrix Workspace-App eine automatische Wiederverbindung versucht,

wählen Sie das Kontrollkästchen "Sitzungszuverlässigkeit aktivieren". Aktivieren Sie das Kontrollkästchen **Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar)**, wenn Sie mehrere STAs konfiguriert haben und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist.

Wenn das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar) aktiviert ist, ruft StoreFront Tickets von zwei verschiedenen Secure Ticket Authoritys ab, damit Benutzersitzungen nicht unterbrochen werden, wenn eine Secure Ticket Authority während der Sitzung ausfällt. Wenn StoreFront aus irgendeinem Grund keine Verbindung zu zwei Secure Ticket Authoritys herstellen kann, wird automatisch nur eine Secure Ticket Authority verwendet.



Wenn Sie die Einstellungen angegeben haben, klicken Sie auf **Weiter**.

4. Geben Sie die Einstellungen auf der Registerkarte **Authentifizierungseinstellungen** an.

   - Wählen Sie die NetScaler-Version.
   - Gibt es mehrere Gateways mit derselben URL (normalerweise bei Verwendung von Global Server Load Balancing) und Sie eine Rückruf-URL eingegeben haben, müssen Sie die VIP des Gateways eingeben. So kann StoreFront anhand der Rückruf-URL ermitteln, von welchem Gateway die Anforderung stammt und welcher Server kontaktiert werden muss. Andernfalls können Sie dieses Feld leer lassen.

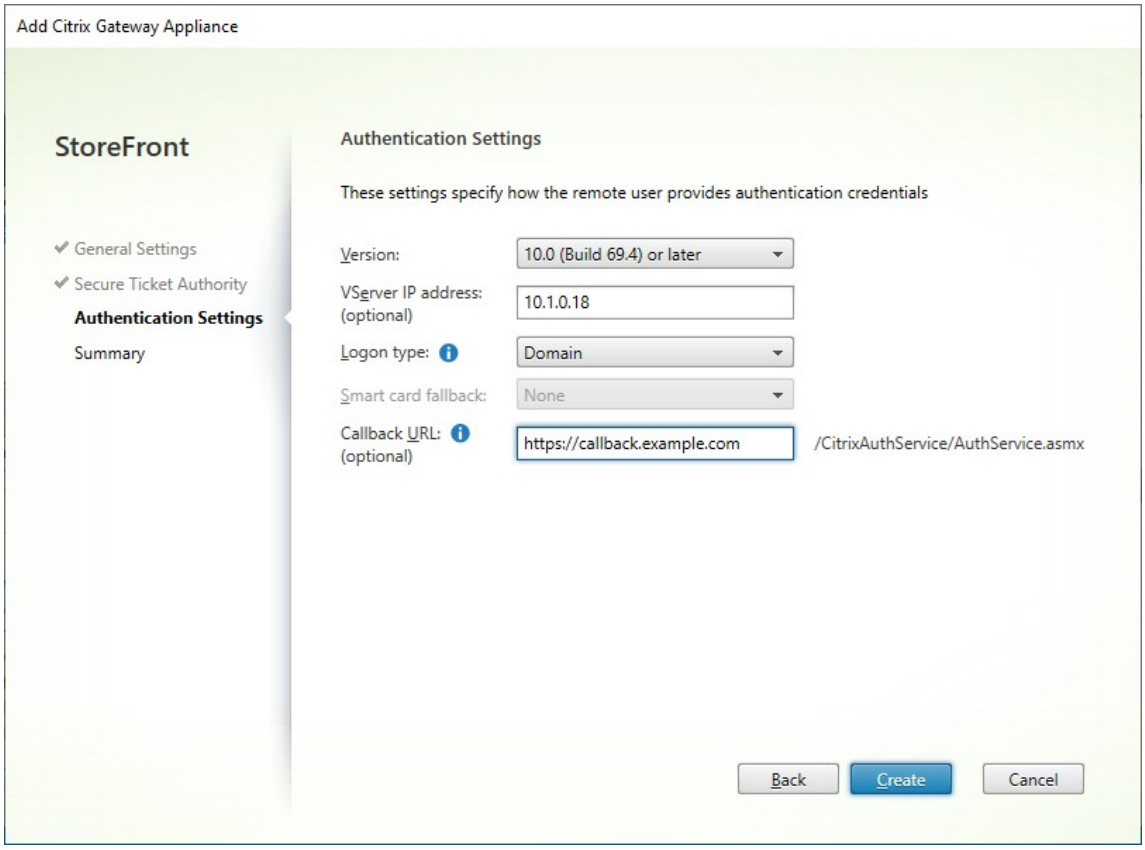
- Wählen Sie aus der Liste **Anmeldetyp** die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer der Citrix Workspace-App konfiguriert haben.

Die von Ihnen angegebenen Informationen über die Konfiguration des Citrix Gateway-Geräts werden der Provisioningdatei für den Store hinzugefügt. Dadurch kann die Citrix Workspace-App die richtige Verbindungsanforderung senden, wenn ein Gerät zum ersten Mal kontaktiert wird.

- Wenn Benutzer die Domänenanmeldeinformationen für Microsoft Active Directory eingeben müssen, wählen Sie Domäne.
- Wählen Sie Sicherheitstoken, wenn Benutzer einen Tokencode von einem Sicherheitstoken eingeben müssen.
- Wählen Sie "Domäne und Sicherheitstoken", wenn Benutzer ihre Domänenanmeldeinformationen und einen Tokencode von einem Sicherheitstoken eingeben müssen.
- Wählen Sie SMS-Authentifizierung, wenn Benutzer ein in einer Textnachricht gesendetes Einmalkennwort eingeben müssen.
- Wenn Benutzer eine Smartcard vorlegen und eine PIN eingeben müssen, wählen Sie Smartcard.

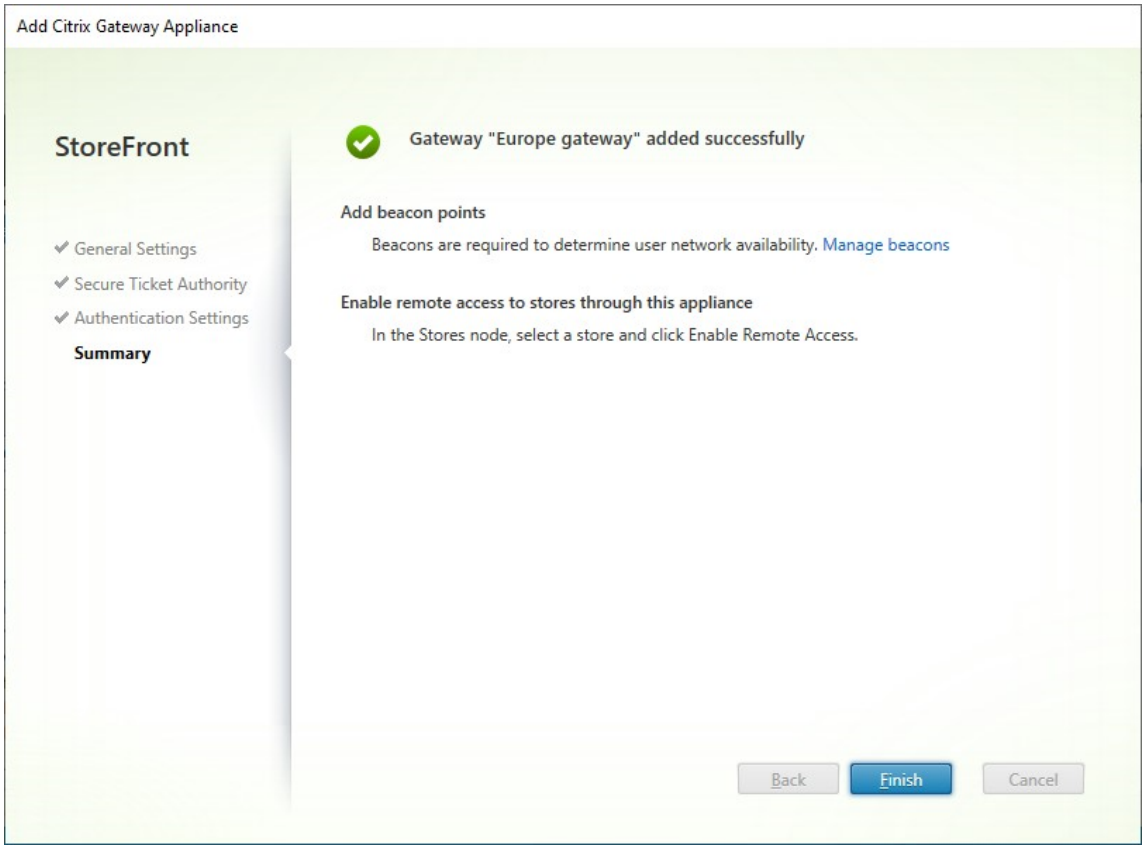
Wenn Sie die Smartcardauthentifizierung mit einer sekundären Authentifizierungsmethode konfigurieren, auf die Benutzer zurückgreifen können, wenn es Probleme mit den Smartcards gibt, wählen Sie die sekundäre Authentifizierungsmethode aus der Liste Smartcard-Fallback.

- Geben Sie optional die intern zugängliche URL des Gateways in das Feld "Callback-URL" ein. Damit kann StoreFront den Citrix Gateway-Authentifizierungsdienst kontaktieren, um zu überprüfen, ob von Citrix Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen. Sie ist für Smart Access und für die Authentifizierung ohne Kennwort (Smart Card oder SAML) erforderlich, andernfalls können Sie das Feld leer lassen. Wenn Sie mehrere Citrix Gateways mit derselben URL haben, muss diese URL für den spezifischen Gateway-Server gelten.



Wenn Sie die Einstellungen angegeben haben, klicken Sie auf **Weiter**.

5. Klicken Sie auf **Erstellen**, um die Konfiguration zu übernehmen.



6. Wenn die Bereitstellung angewendet wurde, klicken Sie auf **Fertig stellen**.
7. Damit die Benutzer über das Gateway auf Stores zugreifen können, konfigurieren Sie den Remotebenutzerzugriff.

PowerShell SDK

Um ein Gateway mit dem PowerShell SDK hinzuzufügen, rufen Sie das Cmdlet New-STFRoamingGateway auf.

Citrix Gateway bearbeiten

1. Klicken Sie im Fenster **Citrix Gateways verwalten** auf das Gateway, das Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

   Eine Beschreibung der Parameter finden Sie unter Citrix Gateway hinzufügen.
2. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

PowerShell SDK

Um die Gatewaykonfiguration mit dem PowerShell SDK zu ändern, rufen Sie das Cmdlet Set-STFRoamingGateway auf.

Citrix Gateway entfernen

1. Klicken Sie im Fenster **Citrix Gateways verwalten** auf das Gateway, das Sie ändern möchten, und klicken Sie auf **Entfernen**.
2. Klicken Sie im Bestätigungsfenster auf **Ja**.

PowerShell SDK

Um das Gateway mithilfe des PowerShell-SDK zu entfernen, rufen Sie Remove-STFRoamingGateway auf.

Lastausgleich mit Citrix ADC

April 17, 2024

Dieser Artikel enthält Informationen zum Bereitstellen einer StoreFront-Servergruppe mit mindestens zwei StoreFront-Servern in einer aktiven Konfiguration mit Lastausgleich. Der Artikel enthält Angaben zum Konfigurieren eines Citrix ADC-Geräts für den Lastausgleich für von der Citrix Workspace-App bzw. Webbrowsern eingehende Anforderungen über die StoreFront-Server in der Servergruppe hinweg.

Serverzertifikatanforderungen für die Bereitstellung mit Lastausgleich

Ziehen Sie die folgenden Optionen in Betracht, bevor Sie ein Zertifikat von einer kommerziellen Zertifizierungsstelle erwerben oder von der Zertifizierungsstelle Ihres Unternehmens ausstellen lassen.

- **Option 1:** Verwenden Sie ein Platzhalterzertifikat **.example.com* auf dem Citrix ADC virtuellen Lastausgleichsserver und den Knoten der StoreFront-Servergruppe. Dies vereinfacht die Konfiguration und ermöglicht das künftige Hinzufügen weiterer StoreFront-Server, ohne dass das Zertifikat ersetzt werden muss.
- **Option 2**: Verwenden Sie ein Zertifikat mit alternativem Antragstellernamen (SANs) auf dem virtuellen Citrix ADC-Lastausgleichsserver und den Knoten der StoreFront-Servergruppe. Zusätzliche SANs in dem Zertifikat, die allen vollqualifizierten Domänennamen der StoreFront-Server

entsprechen, sind zwar optional, jedoch empfehlenswert, da sie eine größere Flexibilität bei der StoreFront-Bereitstellung bieten.

Erstellen von DNS-Datensätzen für den Load Balancer der StoreFront-Servergruppe

Erstellen Sie einen DNS Alias- und einen PTR-Datensatz für den ausgewählten freigegebenen FQDN. Clients im Netzwerk verwenden diesen FQDN für den Zugriff auf die StoreFront-Servergruppe unter Verwendung des Citrix ADC-Load Balancers.

Beispiel: `storefront.example.com` wird in die virtuelle IP (VIP) des virtuellen Lastausgleichservers aufgelöst.

StoreFront-Server konfigurieren

Alle StoreFront-Server, die Sie in einen Lastausgleich einschließen möchten, müssen als StoreFront-Servergruppe konfiguriert werden, bei der die Konfiguration zwischen den Servern synchronisiert wird, um sicherzustellen, dass alle Server identisch konfiguriert sind. Weitere Informationen zum Hinzufügen von Servern zu einer Servergruppe finden Sie unter Vorhandener Servergruppe beitreten.

Jeder Server sollte für HTTPS konfiguriert sein, damit die Kommunikation zwischen dem Load Balancer und den StoreFront-Servern verschlüsselt ist. Siehe StoreFront mit HTTPS schützen. Das Zertifikat muss den FQDN mit Lastausgleich als allgemeinen Namen (CN) oder als alternativen Antragstellernamen (Subject Alternative Name, SAN) enthalten.

Legen Sie als Basis-URL der Servergruppe die URL des Load Balancers fest. Um die Basis-URL zu ändern, klicken Sie in der Citrix StoreFront-Verwaltungskonsole links mit der rechten Maustaste auf **Servergruppe** und dann auf **Basis-URL ändern**. Geben Sie die URL des virtuellen Load Balancer-Servers ein.

Optional: Citrix Service Monitor für HTTPS konfigurieren

StoreFront-Installationen beinhalten den Windows-Dienst **Citrix Service Monitor**. Dieser Dienst ist von keinem anderen Dienst abhängig und überwacht wichtige StoreFront-Dienste auf Fehler. Dadurch können Citrix ADC und andere Drittanbieteranwendungen die relative Integrität einer StoreFront-Serverbereitstellung überwachen.

Standardmäßig verwendet der Monitor HTTP auf Port 8000. Sie können dies optional auf HTTPS an Port 443 ändern.

1. Öffnen Sie PowerShell Integrated Scripting Environment (ISE) auf dem primären StoreFront-Server und führen Sie folgende Befehle aus, um den Standardmonitor auf HTTPS 443 zu ändern:


```
$ServiceUrl = "https://localhost:443/StorefrontMonitor"
Set-STFServiceMonitor -ServiceUrl $ServiceUrl
Get-STFServiceMonitor
<!--NeedCopy-->
```

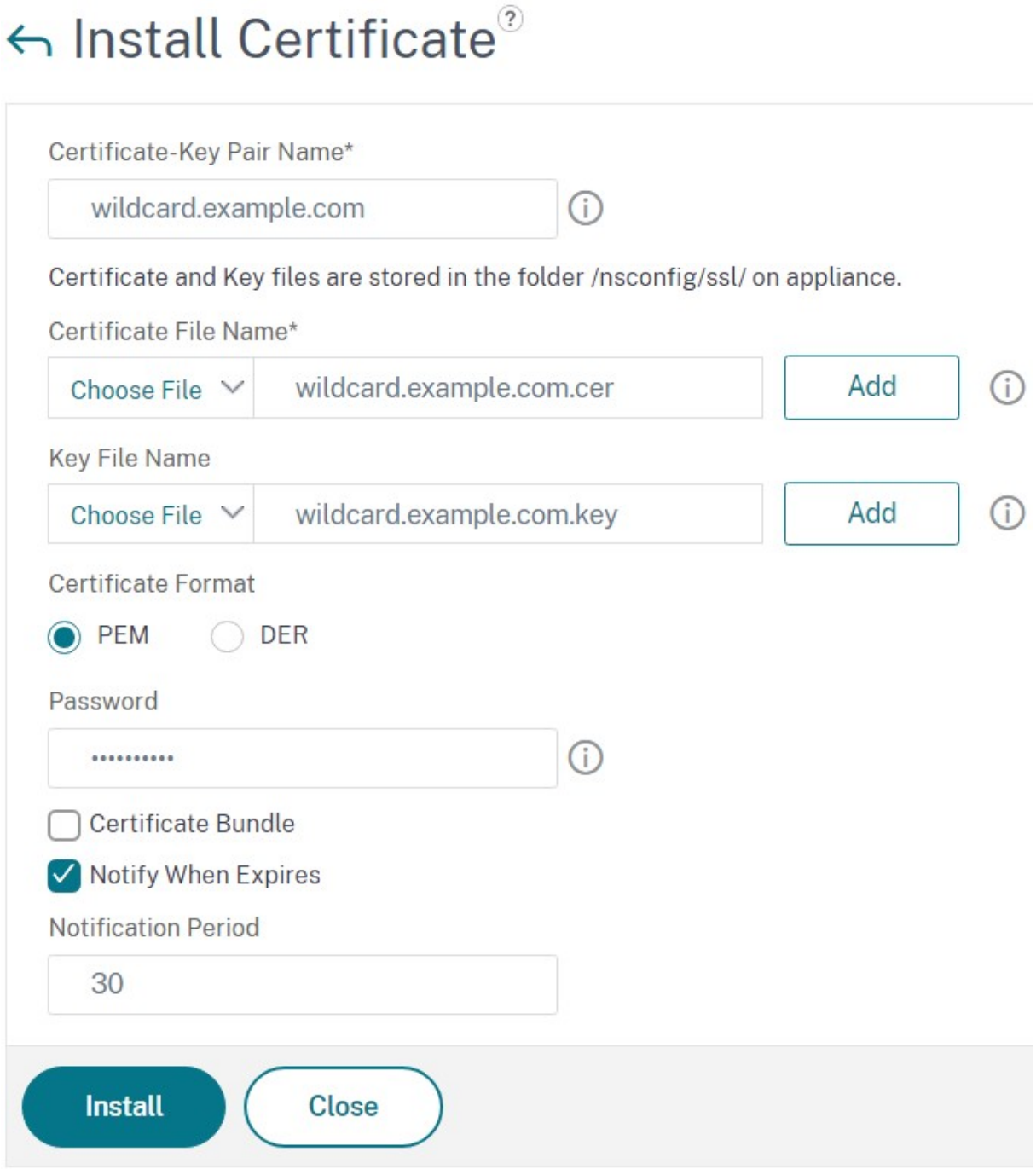
2. Nach Abschluss verteilen Sie die Änderungen auf alle anderen Server in der StoreFront-Servergruppe.
3. Für einen kurzen Test des Monitors geben Sie die folgende URL im Browser auf dem StoreFront-Server oder auf einem anderen Computer mit Netzwerkzugriff auf den StoreFront-Server ein. Der Browser gibt eine XML-Zusammenfassung des Status jedes StoreFront-Diensts zurück.

   ```
   https://<loadbalancingFQDN>/StoreFrontMonitor/GetSFServicesStatus
   ```

Citrix ADC Load Balancer konfigurieren

Serverzertifikat auf dem Citrix ADC konfigurieren

1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts an.
2. Wählen Sie **Traffic Management > SSL > Certificates > Server Certificates**.
3. Klicken Sie auf **Installieren**.
4. Geben Sie auf der Seite **Install Server Certificate** einen Namen für das Zertifikatsschlüsselpaar ein, klicken Sie auf **Choose File** und steuern Sie die Zertifikatdatei an. Wenn die Zertifikatdatei den privaten Schlüssel nicht enthält, müssen Sie zusätzlich eine **Schlüsseldatei** auswählen.

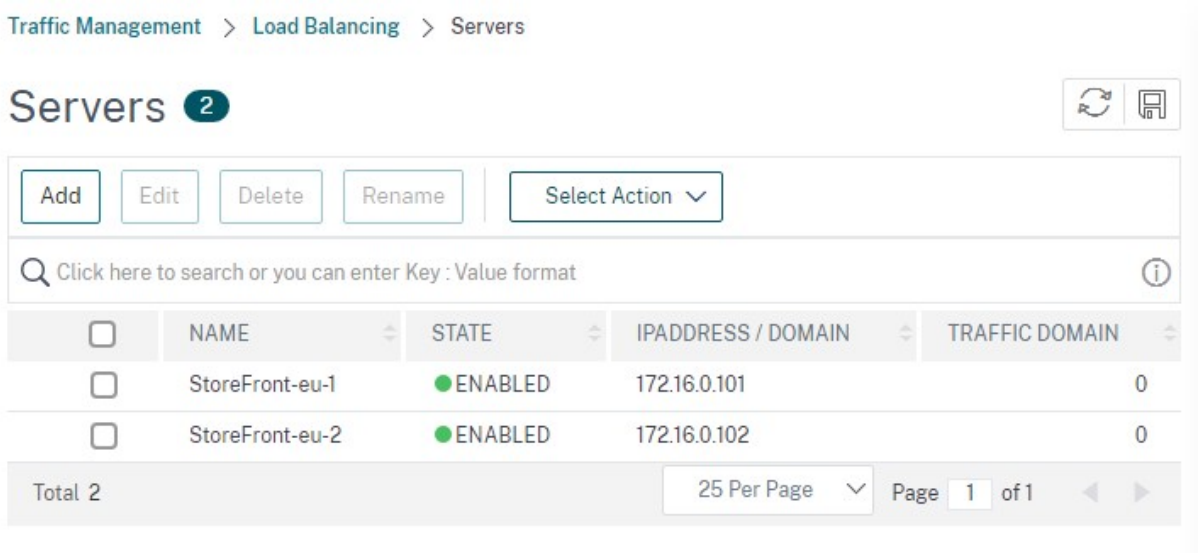


Hinzufügen einzelner StoreFront-Serverknoten zum Citrix ADC-Load Balancer

1. Navigieren Sie zu **Traffic Management > Load Balancing > Servers**. Klicken Sie auf **Hinzufügen** und fügen Sie jeden StoreFront-Server hinzu, für den der Lastenausgleich erfolgen soll.

   Beispiel = 2 StoreFront-Server mit den Namen “StoreFront-EU-1”und “StoreFront-EU-2”

2. Verwenden Sie die IP-basierte Serverkonfiguration und geben Sie die Server-IP-Adresse für jeden StoreFront-Knoten ein.



Definieren eines StoreFront-Monitors zur Prüfung des Status aller StoreFront-Knoten in der Servergruppe

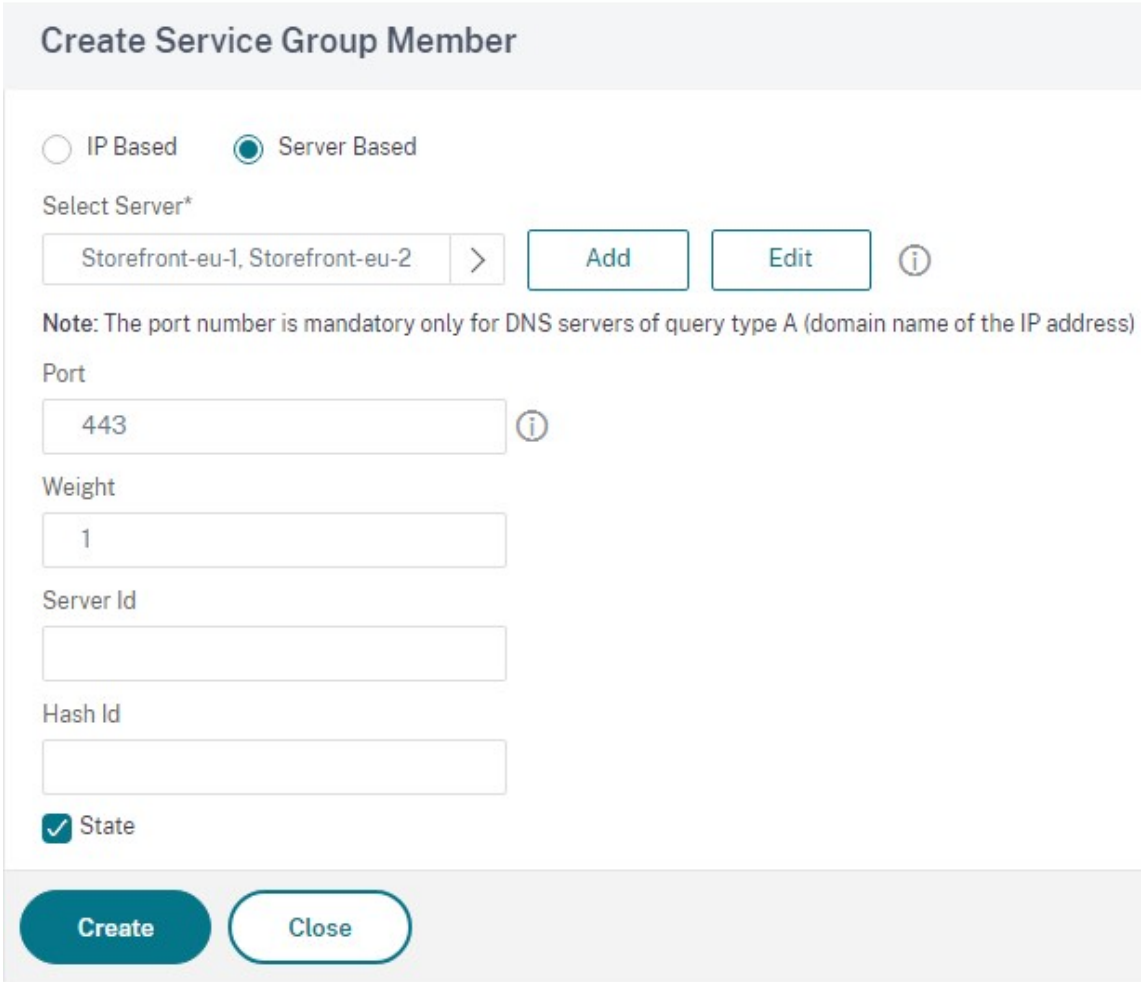
1. Melden Sie sich an der Verwaltungsbenutzeroberfläche des Citrix ADC-Geräts an.
2. Wählen Sie **Traffic Management > Load Balancing > Monitors > Add** und fügen Sie einen neuen Monitor unter dem Namen *StoreFront* hinzu. Akzeptieren Sie alle Standardeinstellungen.
3. Wählen Sie im Dropdownmenü **Type** die Option **StoreFront**.
4. Wenn Sie den StoreFront-Monitor für HTTPS konfiguriert haben, stellen Sie sicher, dass die Option **Sicher** ausgewählt ist. Andernfalls lassen Sie diese Option deaktiviert und geben Sie als Portnummer 8000 ein.
5. Wählen Sie die Option **Check Backend Services**. Damit wird die Überwachung von auf dem StoreFront-Server ausgeführten Diensten aktiviert. StoreFront-Dienste werden durch Sondieren eines Windows-Diensts auf dem StoreFront-Server überwacht, der den Status der folgenden Dienste zurückgibt:

   - W3SVC (IIS)
   - WAS (Aktivierungsdienst für Windows-Prozesse)
   - CitrixCredentialWallet
   - CitrixDefaultDomainService

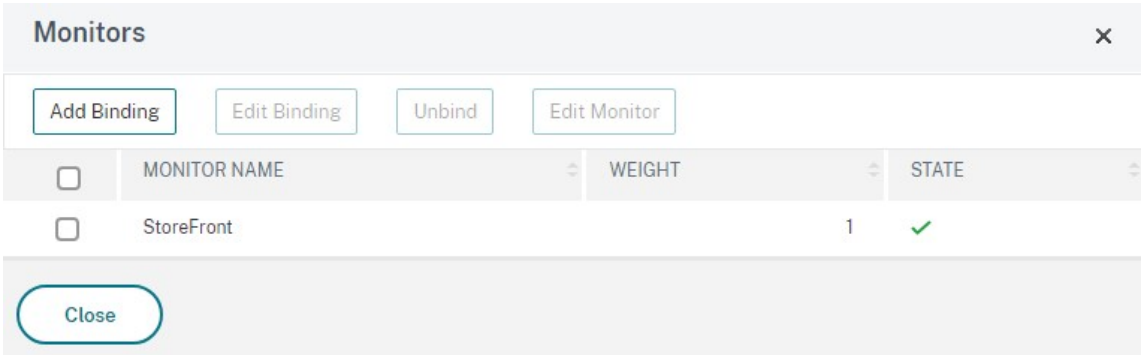
Dienstgruppe für alle StoreFront-Server erstellen

1. Gehen Sie zu **Traffic Management > Load Balancing > Service Groups**. Klicken Sie auf **Add**. Um über HTTPS eine Verbindung zu den StoreFront-Servern herzustellen, wählen Sie als Protokoll SSL. Übernehmen Sie bei den anderen Einstellungen den Standardwert. Klicken Sie auf **OK**.
2. Klicken Sie in Ihrer Dienstgruppe unter **Service Group Members** auf **No Service Group Member**.

   a) Klicken Sie auf **Service Based**.
   b) Wählen Sie alle Server aus, die Sie zuvor definiert haben.
   c) Zur Verwendung von SSL zwischen dem Load Balancer und dem StoreFront-Server geben Sie Port 443 ein. Andernfalls geben Sie Port 80 ein.

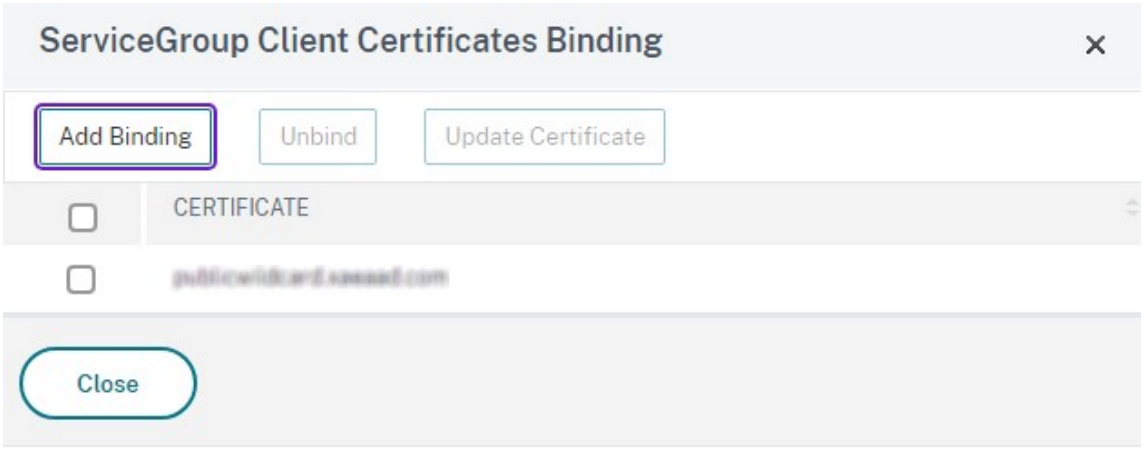


3. Fügen Sie den Bereich **Monitors** hinzu und wählen Sie den zuvor erstellten StoreFront-Monitor aus.



4. Fügen Sie den Bereich **Certificates** hinzu.

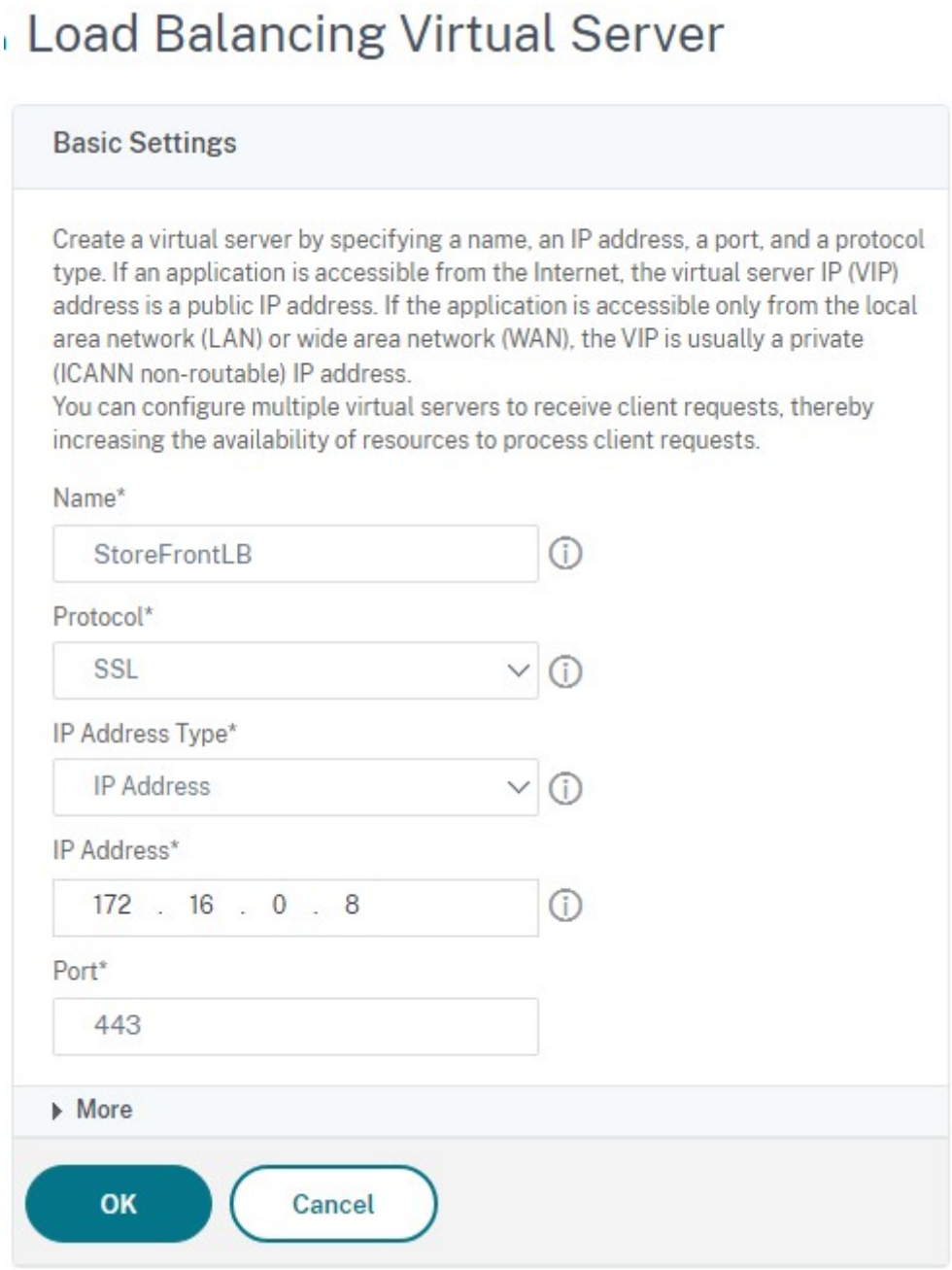
   a) Binden Sie das Clientzertifikat.
   b) Binden Sie das Zertifizierungsstellenzertifikat, das zum Signieren des zuvor importierten Serverzertifikats verwendet wurde, sowie jegliche Zertifizierungsstellen, die Teil der PKI-Vertrauenskette sind.



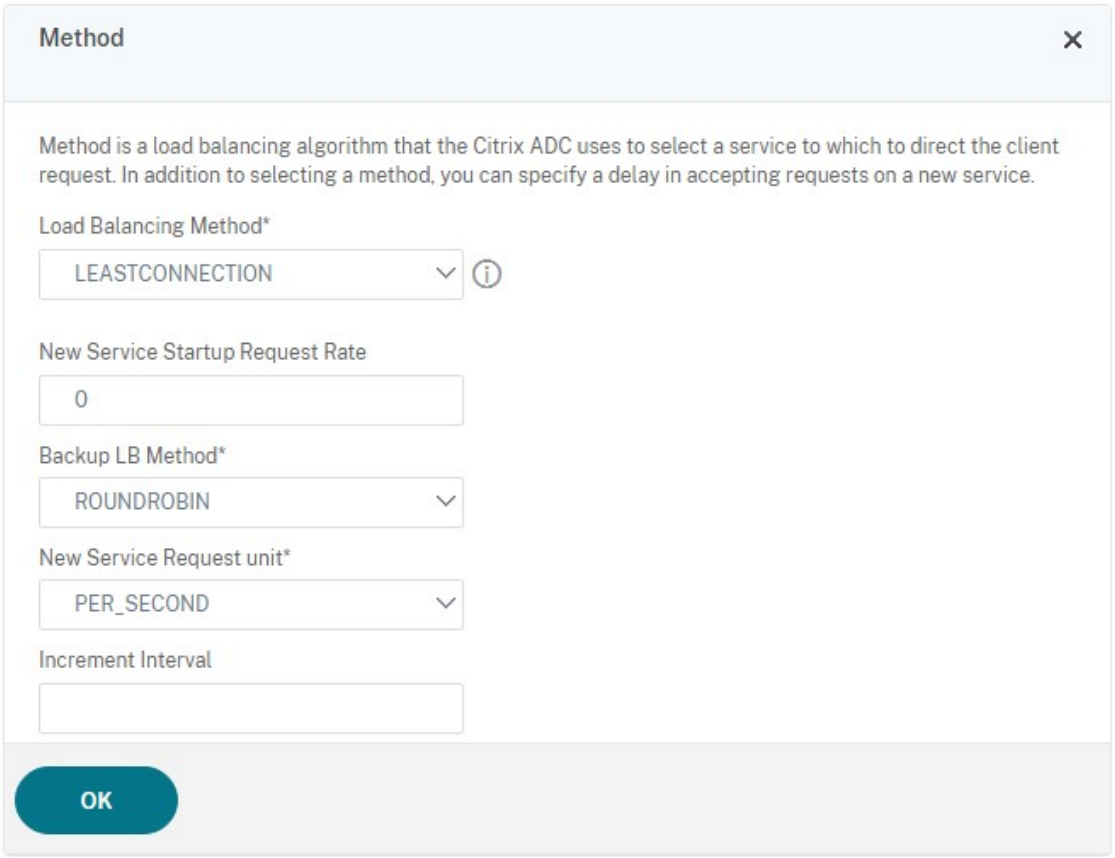
5. Fügen Sie den Bereich **Settings** hinzu. Wählen Sie **Insert Client IP Header** und geben Sie als Header-Namen **X-Forwarded-For** ein. Dadurch kann die Client-IP-Adresse in Citrix Virtual Apps and Desktops-Richtlinien verwendet werden.

Erstellen eines virtuellen Lastausgleichservers für den Benutzerdatenverkehr

1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts an.
2. Wählen Sie **Traffic Management > Load Balancing > Virtual Servers > Add** zum Erstellen eines neuen virtuellen Servers aus.
3. Geben Sie einen Namen ein, wählen Sie SSL als Protokoll und geben Sie dann den **Port** ein. Klicken Sie auf “OK”, um den virtuellen Server zu erstellen.



4. Binden Sie die zuvor erstellte **Dienstgruppe** an den virtuellen Lastenausgleichserver.
5. Binden Sie den Server und das ZS-Zertifikat, die Sie zuvor an die Dienstgruppe gebunden haben.
6. Fügen Sie den Bereich **Method** hinzu und wählen Sie die Lastausgleichmethode. Für den Lastausgleich in StoreFront wird in der Regel **round robin** oder **least connection** verwendet.



7. Fügen Sie den Bereich **Persistence** hinzu.

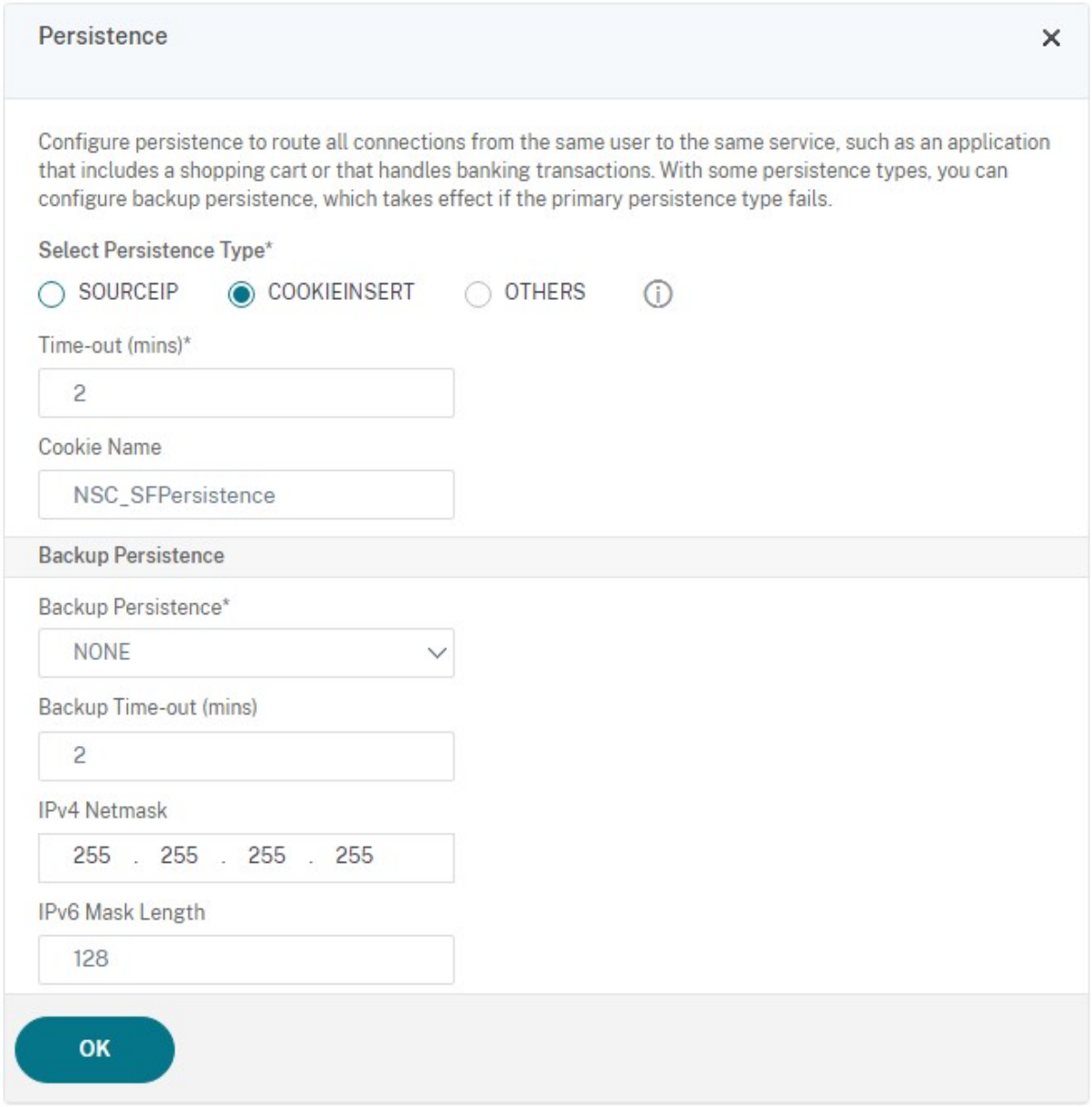
   a) Legen Sie die Persistenzmethode auf **COOKIEINSERT** fest.

   b) Legen Sie für das Timeout denselben Wert wie für "Sitzungstimeout"in StoreFront fest (standardmäßig 20 Minuten).

   c) Benennen Sie das Cookie. Beispielsweise, **NSC_SFPersistence**, da dies das Identifizieren während des Debuggens erleichtert.

   d) Legen Sie für "Backup persistence"**NONE** fest.

> **Hinweis:**
>
> Wenn der Client kein HTTP-Cookie speichern darf, enthalten nachfolgende Anforderungen kein HTTP-Cookie und "Persistence"wird nicht verwendet.

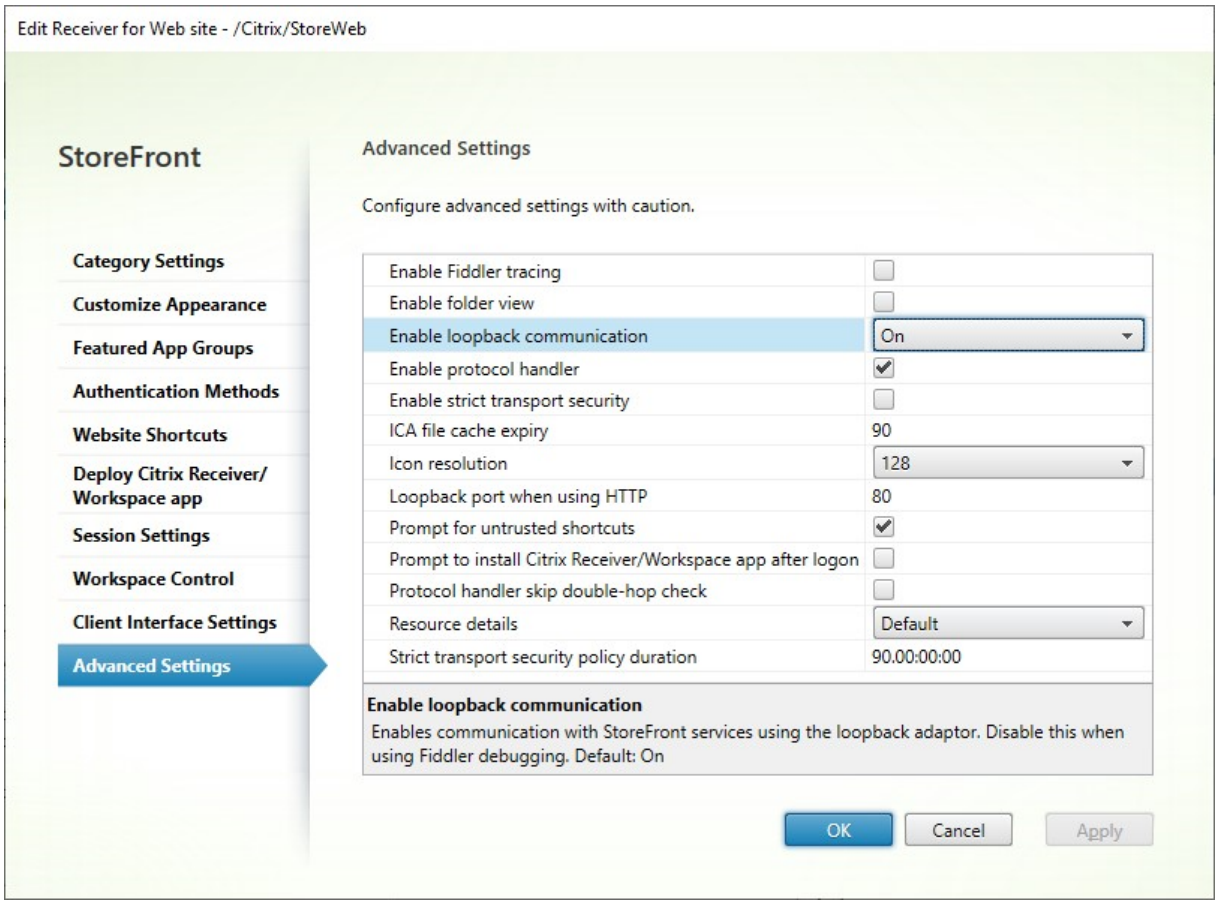


StoreFront-Loopback konfigurieren

Wenn es sich bei der Basisadresse um einen Load Balancer handelt, kann der Datenverkehr der internen Kommunikation zwischen StoreFront-Diensten an den Load Balancer und möglicherweise an einen weiteren Server weitergeleitet werden. Dies führt zu schlechter Leistung und unerwartetem Verhalten. Verwenden Sie die StoreFront-Einstellung **Loopbackkommunikation aktivieren**, um dies zu vermeiden. Standardmäßig ist dies auf **On** festgelegt, sodass der Hostteil der Dienstadresse durch die Loopback-IP-Adresse 127.0.0.1 ersetzt wird, während das Schema (HTTP oder HTTPS) unverändert bleibt. Dies kann bei Einzelserverbereitstellungen und bei Bereitstellungen mit einem Load Balancer ohne SSL-Terminierung eingesetzt werden.

Kommuniziert ein Load Balancer mit SSL-Terminierung über HTTP mit StoreFront (nicht empfohlen), muss die StoreFront-Loopbackkommunikation auf **OnUsingHttp** festgelegt werden, sodass StoreFront auch das Schema von HTTPS auf HTTP ändert.

1. Öffnen Sie Citrix StoreFront.
2. Gehen Sie für jeden Store zu **Receiver für Websites verwalten**. Gehen Sie für jede Website zu **Konfigurieren**.
3. Gehen Sie zu **Erweiterte Einstellungen**.
4. Ändern Sie die Einstellung **Loopbackkommunikation aktivieren** aktivieren in **OnUsingHttp**.



Kommuniziert ein Load Balancer mit SSL-Terminierung über HTTP mit StoreFront (nicht empfohlen), muss die StoreFront-Loopbackkommunikation auf **OnUsingHttp** festgelegt werden, sodass StoreFront auch das Schema von HTTPS auf HTTP ändert.

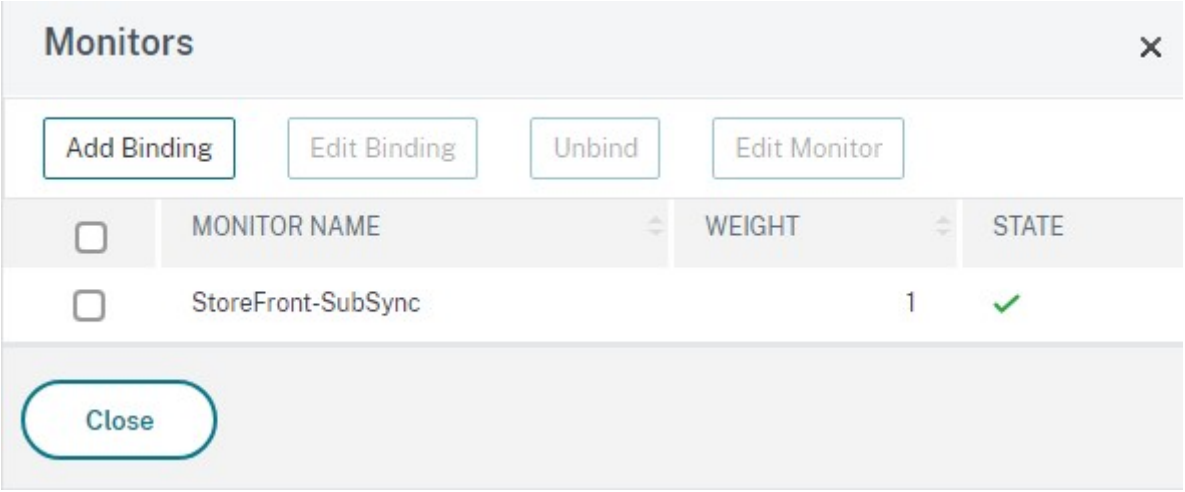
Citrix ADC Load Balancer für die Abonnementsynchronisierung zwischen Servergruppen konfigurieren

Wenn Sie über mehrere Sites mit zwei oder mehr StoreFront-Servergruppen verfügen, können Sie Abonnementdaten zwischen diesen über regelmäßige Pull-Aktionen nach Zeitplan replizieren. Für

die StoreFront-Abonnementreplikation wird TCP-Port 808 verwendet, die Verwendung eines vorhandenen virtuellen Lastausgleichsservers an HTTP-Port 80 oder HTTPS-Port 443 schlägt daher fehl. Zur Bereitstellung hoher Dienstverfügbarkeit erstellen Sie einen zweiten virtuellen Server auf jedem Citrix ADC-Gerät in der Bereitstellung zum Durchführen eines Lastausgleichs an TCP-Port 808 für jede der StoreFront-Servergruppen.

Konfigurieren einer Dienstgruppe für die Synchronisierung von Abonnements

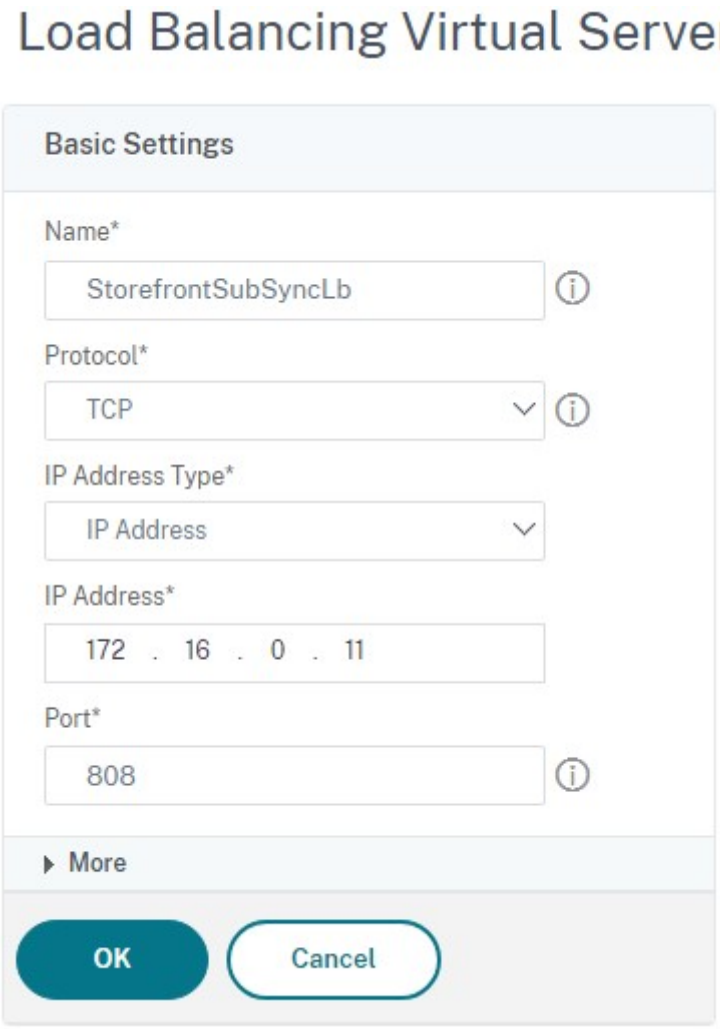
1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts an.
2. Wählen Sie **Traffic Management > Load Balancing > Service Groups > Add**.
3. Geben Sie einen Dienstgruppennamen ein, ändern Sie das Protokoll in **TCP** und klicken Sie zum Speichern auf **OK**.
4. Fügen Sie im Bereich **Service Group Members** alle StoreFront-Serverknoten hinzu, die Sie zuvor im Bereich "Server"definiert haben, und geben Sie als **Port** die Nummer **808** an.
5. Fügen Sie den Bereich **Monitors** hinzu.
    a) Klicken Sie auf **No Service Group to Monitor Binding**.
    b) Klicken Sie auf Hinzufügen. Geben Sie einen **Monitornamen** ein und legen Sie **Type** auf **TCP** fest. Klicken Sie auf **Erstellen**.
    c) Klicken Sie auf **Bind**.



Virtuellen Lastausgleichsserver für die Abonnementsynchronisierung erstellen

1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts an.
2. Wählen Sie **Traffic Management> Load Balancing > Virtual Servers > Add** und fügen Sie eine neue Dienstgruppe hinzu.
3. Geben Sie einen **Namen** ein.

4. Ändern Sie das Protokoll in **TCP**.
5. Geben Sie eine IP-Adresse ein.
6. Geben Sie als **Port** die Nummer **808** ein.



7. Klicken Sie auf **OK**.
8. Klicken Sie auf **No Load Balancing Virtual Server ServiceGroup Binding**, wählen Sie die zuvor erstellte Dienstgruppe aus und klicken Sie auf **Bind**.
9. Fügen Sie den Bereich **Method** hinzu und legen Sie **Load Balancing Method** auf **ROUNDROBIN** fest.
10. Klicken Sie auf **Done**, um die Bearbeitung abzuschließen.

StoreFront für den Abruf von Abonnementdaten über den Load Balancer konfigurieren

Siehe Abonnementsynchronisierung konfigurieren.

Legen Sie beim Konfigurieren des Replikationszeitplans für die Servergruppe eine Adresse fest, die der virtuellen IP-Adresse des Load Balancers des virtuellen Servers für die Abonnementsynchronisierung entspricht.

Citrix ADC und StoreFront für die delegierte Formularauthentifizierung (DFA) konfigurieren

February 28, 2024

Die erweiterbare Authentifizierung (extensible authentication) bietet einen einzelnen Anpassungspunkt zur Erweiterung der formularbasierten Authentifizierung des Citrix ADC-Geräts und von StoreFront. Zum Erstellen einer Authentifizierungslösung mit dem Extensible Authentication-SDK müssen Sie die delegierte Formularauthentifizierung (DFA) zwischen dem Citrix ADC-Gerät und StoreFront konfigurieren. Das Protokoll der delegierten Formularauthentifizierung ermöglicht die Erstellung und Verarbeitung von Authentifizierungsformularen, einschließlich Validierung der Anmeldeinformationen, zur Delegierung an eine andere Komponente. Beispiel: Citrix Gateway delegiert seine Authentifizierung an StoreFront und StoreFront interagiert dann mit einem Drittanbieter-Authentifizierungsserver oder -dienst.

Das Konfigurieren der delegierten Formularauthentifizierung in Citrix Gateway wird in CTX200383 beschrieben.

Installationsempfehlungen

- Zum Schützen der Kommunikation zwischen dem Citrix ADC-Gerät und StoreFront verwenden Sie HTTPS anstelle von HTTP.
- Bei Clusterbereitstellungen stellen Sie sicher, dass auf allen Knoten das gleiche Serverzertifikat installiert und in der IIS HTTPS-Bindung konfiguriert ist, bevor Sie mit der Konfiguration beginnen.
- Stellen Sie sicher, dass auf dem Citrix ADC-Gerät der Aussteller des StoreFront-Serverzertifikats als vertrauenswürdige Zertifizierungsstelle eingerichtet ist, wenn in StoreFront HTTPS konfiguriert ist.

Überlegungen zur StoreFront-Clusterinstallation

- Installieren Sie das Authentifizierungs-Plug-In eines Drittanbieters auf allen Knoten bevor Sie diese gruppieren.

- Konfigurieren Sie alle Einstellungen für die delegierte Formularauthentifizierung auf einem Knoten und verteilen Sie die Änderungen auf die anderen. Weitere Informationen finden Sie unter "Aktivieren der delegierten Formularauthentifizierung".

Aktivieren der delegierten Formularauthentifizierung

Da es in StoreFront keine GUI-Option zur Einrichtung des vorinstallierten Schlüssels für Citrix gibt, installieren die delegierte Formularauthentifizierung mit der PowerShell-Konsole.

1. Installieren Sie die delegierte Formularauthentifizierung. Sie wird nicht standardmäßig installiert und muss mit der PowerShell-Konsole installiert werden.

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts'
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1
Adding snapins
Importing modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-DSDFAServer
Id                              : bf694fbc-ae0a-4d56-8749-c945559e897a
ClassType                       : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc
FrameworkController             : Citrix.DeliveryServices.Framework.FileBased.FrameworkController
ParentInstance                  : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId                        : 860e9401-39c8-4f2c-928d-34251102b840
Data                            : {
  }

ReadOnlyData                    : {
 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                                   vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
```



```
                                    970-466c-ad4c-27a5980f716c], [
                                       TenantId, 860e9401-39c8-4f2c
                                       -928d-34251102b840] }

AdditionalInstanceDependencies : {
 b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }

IsDeployed                     : True
FeatureClass                   : Citrix.DeliveryServices.Framework
    .Feature.FeatureClass
<!--NeedCopy-->
```

2. Fügen Sie Citrix Trusted Client hinzu. Konfigurieren Sie den gemeinsamen geheimen Schlüssel (Passphrase) zwischen StoreFront und dem Citrix ADC-Gerät. Passphrase und Client-ID müssen mit denen auf dem Citrix ADC-Gerät identisch sein.

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-
    DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -
    passphrase secret
<!--NeedCopy-->
```

3. Richten Sie die Formularkonversationsfactory für die delegierte Formularauthentifizierung für die Leitung des gesamten Datenverkehrs an das benutzerdefinierte Formular ein. Sie finden ConversationFactory unter C:\inetpub\wwwroot\Citrix\Authentication\web.config. Dies ist ein Beispiel für das, was Sie sehen.

```
<example connectorURL="http://Example.connector.url:8080/adapters-
    sf-aaconnector-webapp">
       <routeTable order="1000">
         <routes>
           <route name="StartExampleAuthentication" url="Example-
               Bridge-Forms/Start">
             <defaults>
               <add param="controller" value="
                   ExplicitFormsAuthentication" />
               <add param="action" value="AuthenticateStart" />
               <add param="postbackAction" value="Authenticate" />
               <add param="cancelAction" value="CancelAuthenticate"
                    />
               <add param="conversationFactory" value="
                   ExampleBridgeAuthentication" />
               <add param="changePasswordAction" value="
                   StartChangePassword" />
               <add param="changePasswordController" value="
                   ChangePassword" />
               <add param="protocol" value="CustomForms" />
             </defaults>
           </route>
<!--NeedCopy-->
```

4. Legen Sie die Formularkonversationsfactory für die delegierte Formularauthentifizierung in

PowerShell fest. In diesem Beispiel auf ExampleBridgeAuthentication.

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
    DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
<!--NeedCopy-->
```

Bei den Argumenten in PowerShell wird nicht zwischen Groß- und Kleinschreibung unterschieden: **-ConversationFactory** ist identisch mit **-conversationfactory**.

StoreFront deinstallieren

Bevor Sie StoreFront deinstallieren, deinstallieren Sie jegliche Authentifizierungs-Plug-Ins von Drittanbietern, da diese sich auf die Funktionalität von StoreFront auswirken.

Authentifizierung mit andere Domänen

April 17, 2024

Einige Organisationen nutzen Richtlinien, die es nicht gestatten, externen Entwicklern oder Auftragnehmern Zugriff auf veröffentlichte Ressourcen in einer Produktionsumgebung zu geben. In diesem Artikel wird erläutert, wie Sie Zugriff auf veröffentlichte Ressourcen in einer Testumgebung geben, indem Sie die Authentifizierung über Citrix Gateway mit einer Domäne ermöglichen. Die Authentifizierung bei StoreFront und die Receiver für Web-Site kann dann über eine andere Domäne erfolgen. Die in diesem Artikel beschriebene Authentifizierung über Citrix Gateway wird für Benutzer unterstützt, die sich über die Receiver für Web-Site anmelden. Diese Authentifizierungsmethode wird nicht für Citrix Receiver für native Desktops oder mobile Geräte oder die Citrix Workspace-App unterstützt.

Einrichten einer Testumgebung

In diesem Beispiel werden die Produktionsdomäne “production.com”und die Testdomäne “development.com”verwendet.

`production.com`-Domäne

Die Domäne `production.com` ist im Beispiel wie folgt eingerichtet:

- Citrix Gateway mit konfigurierter LDAP-Authentifizierungsrichtlinie für `production.com`.
- Die Authentifizierung über das Gateway erfolgt mit einem Konto vom Typ production\testuser1 plus Kennwort.

`development.com`-Domäne

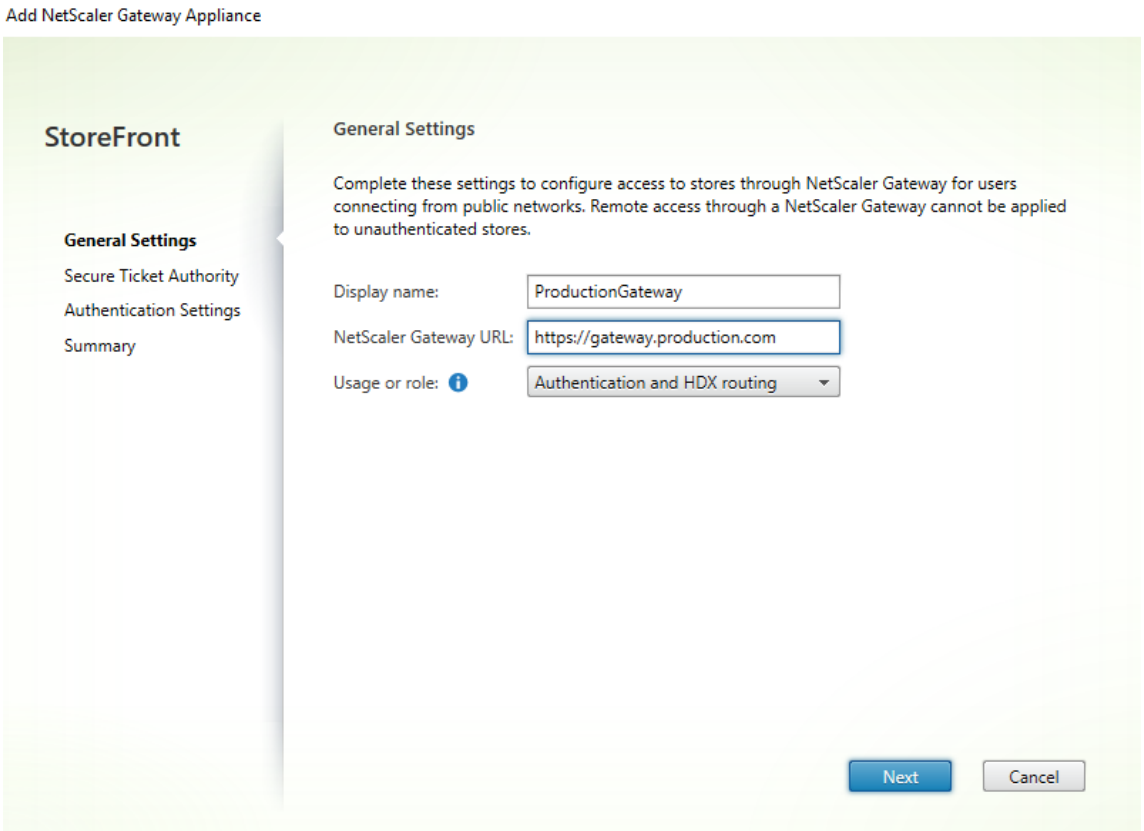
Die Domäne `development.com` ist im Beispiel wie folgt eingerichtet:

- StoreFront, Citrix Virtual Apps and Desktops und VDAs befinden sich alle in der`development.com` Domäne.
- Die Authentifizierung bei der Citrix Receiver für Web-Site erfolgt mit einem Konto vom Typ development\testuser1 plus Kennwort.
- Es besteht keine Vertrauensstellung zwischen den beiden Domänen.

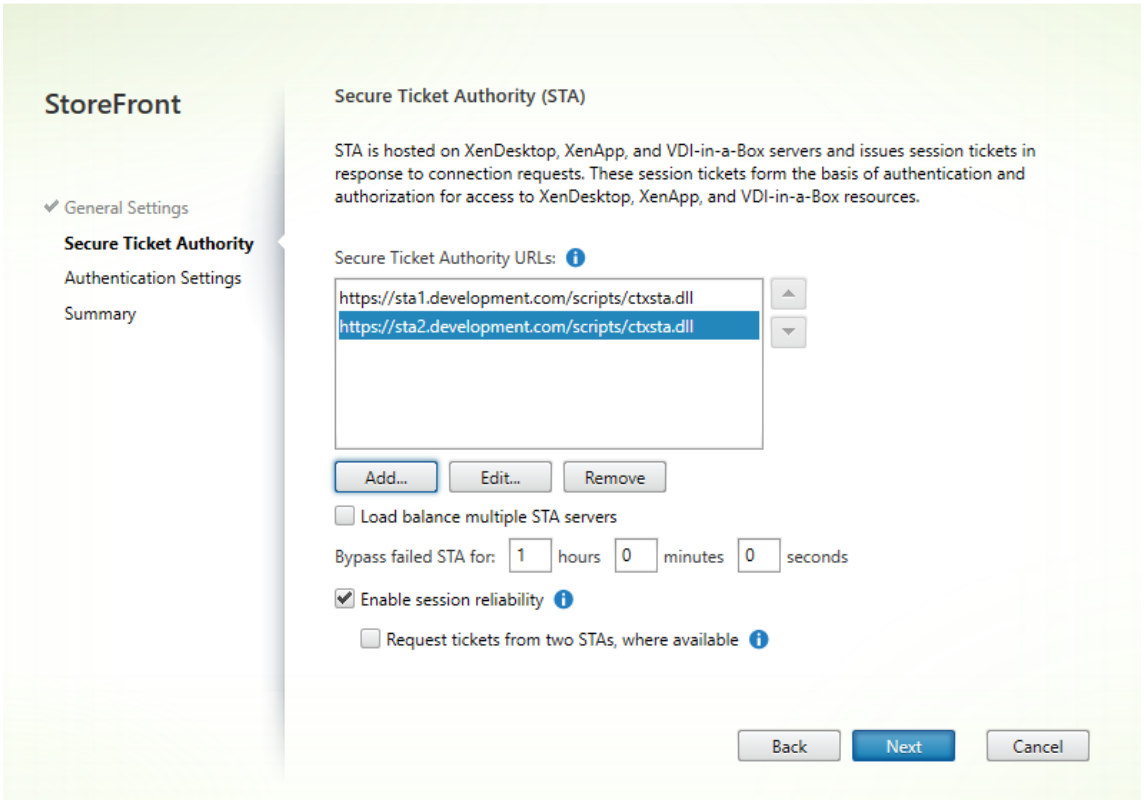
Konfigurieren eines Citrix Gateways für den Store

Gehen Sie zum Konfigurieren eines Citrix Gateways für den Store folgendermaßen vor:

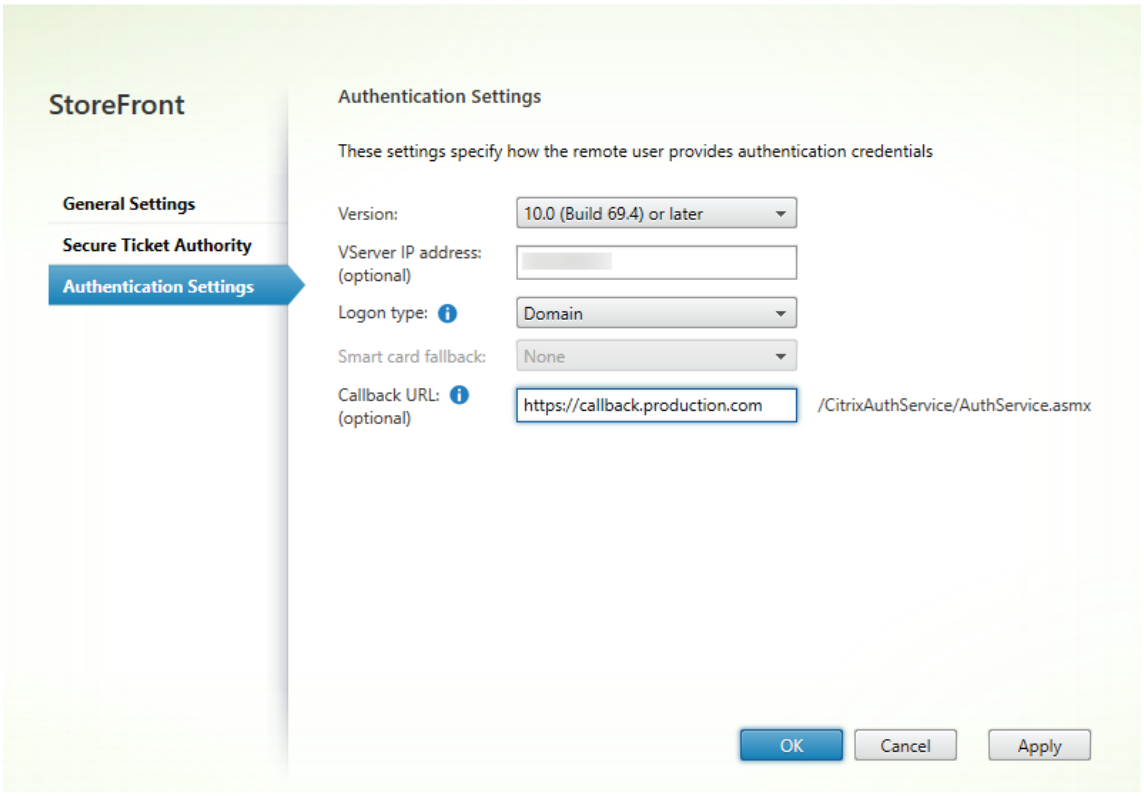
1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** und klicken Sie im Bereich **Aktionen** auf **Citrix Gateways verwalten**.
2. Klicken Sie auf dem Bildschirm “Citrix Gateways verwalten”auf die Schaltfläche **Hinzufügen**.
3. Legen Sie die Einstellungen für “Allgemeine Einstellungen”, “Secure Ticket Authority”und “Authentifizierung”fest.



Add NetScaler Gateway Appliance



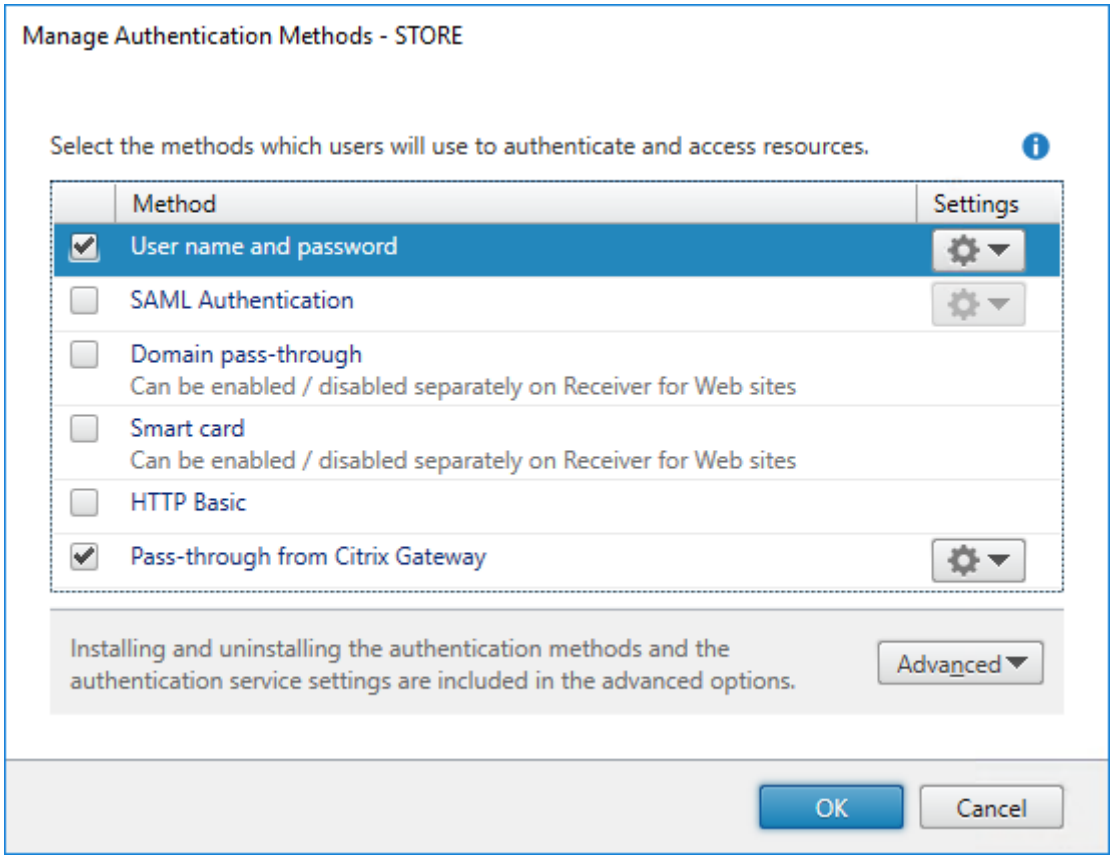
Edit NetScaler Gateway appliance - ProductionGateway



> **Hinweis:**
>
> Bedingte DNS-Weiterleitungen müssen ggf. hinzugefügt werden, damit DNS-Server in beiden Domänen FQDNs in der anderen Domäne auflösen können. Das Citrix ADC-Gerät muss die FQDNs des STA-Servers in der Domäne `development.com` auflösen können, indem es den DNS-Server von `production.com` verwendet. StoreFront muss außerdem die Rückruf-URL in der Domäne `production.com` auflösen können, indem es den DNS-Server von `development.com` verwendet. Als Alternative kann ein FQDN von `development.com` verwendet werden, der in die virtuelle IP-Adresse (VIP) des virtuellen Citrix Gateway-Servers aufgelöst wird.

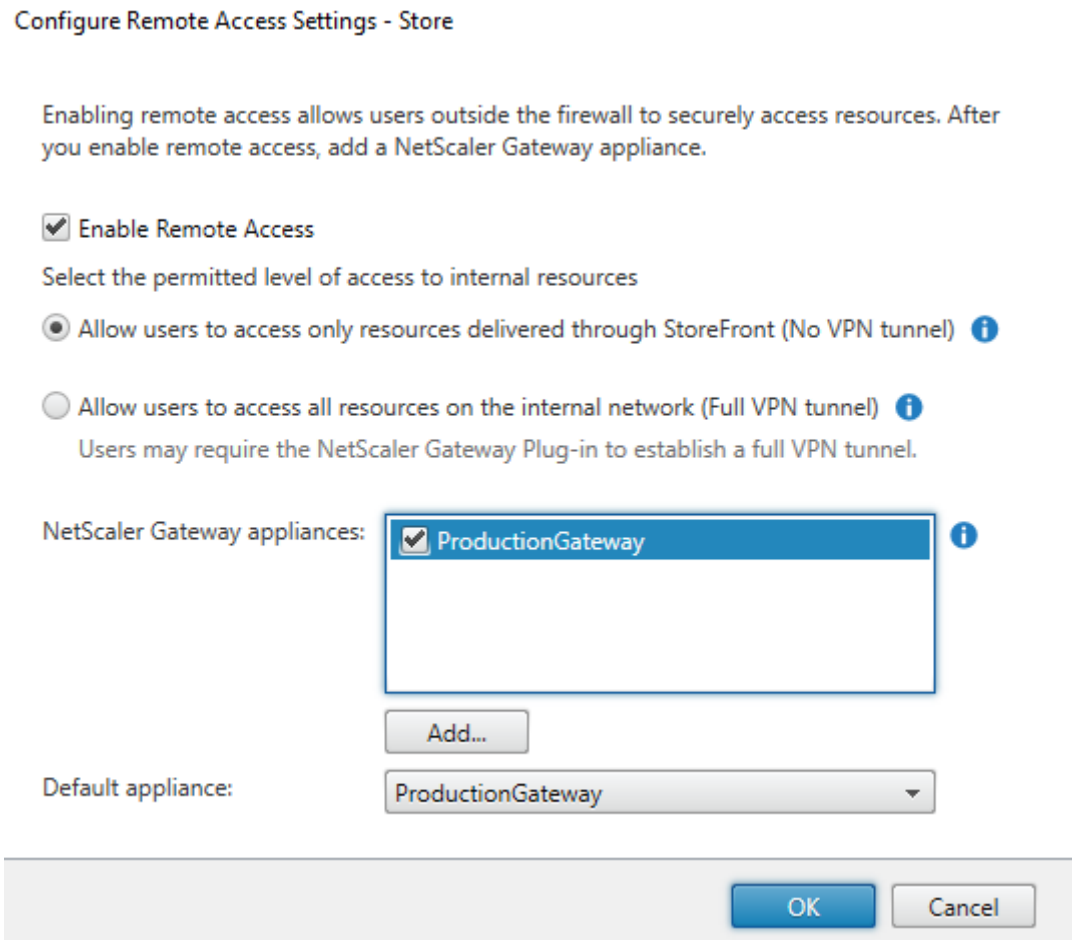
Aktivieren von Passthrough von Citrix Gateway

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus und klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
2. Aktivieren Sie auf dem Bildschirm "Authentifizierungsmethoden verwalten"die Option **Passthrough-Authentifizierung von Citrix Gateway**.
3. Klicken Sie auf **OK**.



Konfigurieren des Stores für einen Remotezugriff über Gateway

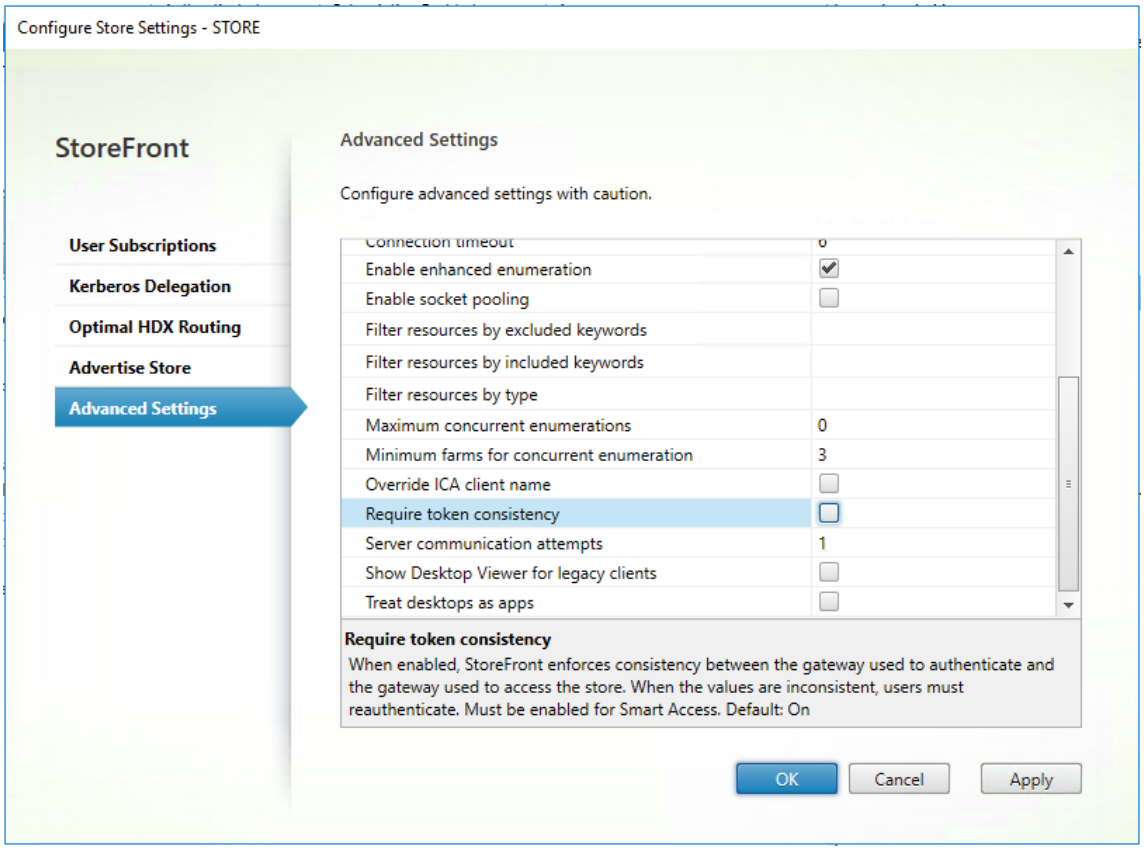
1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich einen Store aus. Klicken Sie im **Aktionsbereich** auf **Remotezugriffeinstellungen konfigurieren**.
2. Wählen Sie **Remotezugriff aktivieren**.
3. Stellen Sie sicher, dass Sie Citrix Gateway beim Store registriert haben. Wenn Citrix Gateway nicht registriert ist, können keine STA-Sitzungstickets erstellt werden.



Deaktivieren der Tokenkonsistenz

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren**.
2. Wählen Sie auf der Seite “Storeeinstellungen konfigurieren”die Option **Erweiterte Einstellungen** aus.

3. Deaktivieren Sie das Kontrollkästchen **Tokenkonsistenz erforderlich**. Weitere Informationen finden Sie unter Erweiterte Storeeinstellungen.



4. Klicken Sie auf **OK**.

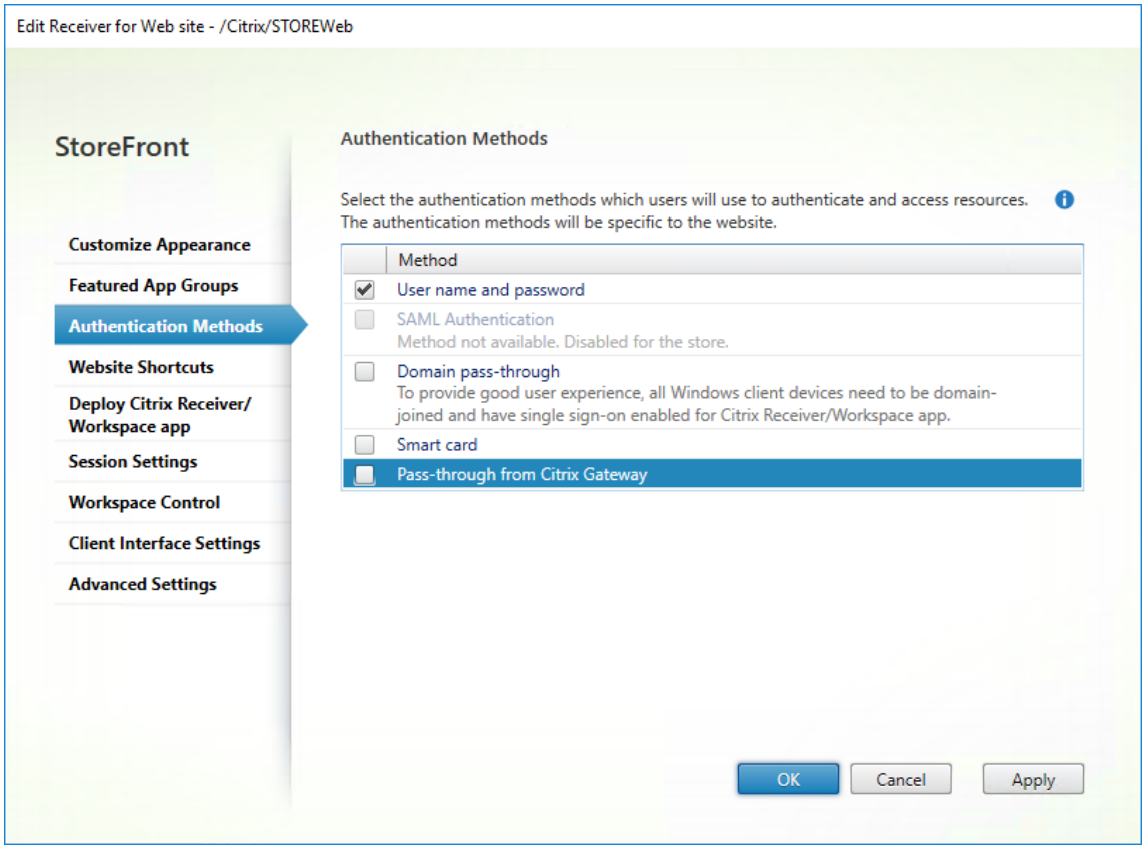
> Hinweis:
>
> Die Einstellung "Tokenkonsistenz erforderlich"ist standardmäßig aktiviert. Wenn Sie diese Einstellung deaktivieren, funktionieren SmartAccess-Features für die Citrix ADC-Endpunktanalyse (EPA) nicht mehr. Weitere Informationen zu SmartAccess finden Sie unter CTX138110.

Deaktivieren der Passthrough-Authentifizierung von Citrix Gateway für die Receiver für Web-Site

> **Wichtig:**
>
> Durch Deaktivieren der Passthrough-Authentifizierung von Citrix Gateway wird verhindert, dass Receiver für Web die falschen Anmeldeinformationen der Domäne `production.com` verwendet, die vom Citrix ADC-Gerät weitergegeben werden. Bei deaktivierter Passthrough-Authentifizierung von Citrix Gateway wird der Benutzer von Receiver für Web zur Eingabe der Anmeldeinformationen aufgefordert. Diese Anmeldeinformationen unterscheiden sich von den

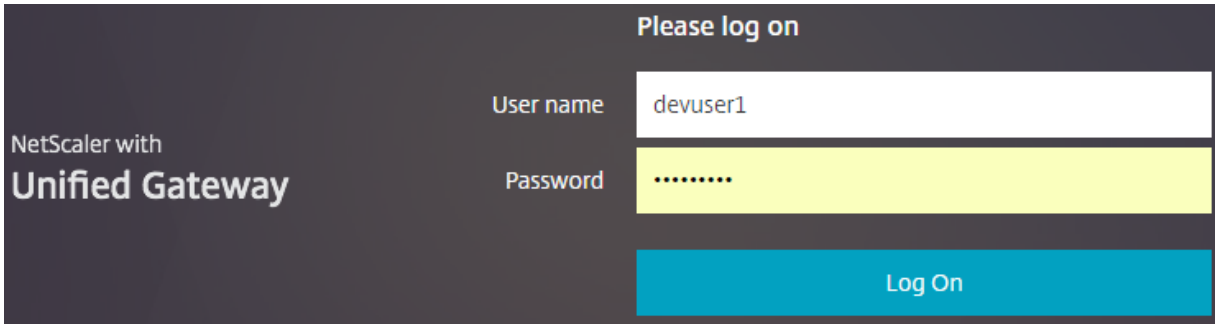
> Anmeldeinformationen, die zur Anmeldung über Citrix Gateway verwendet werden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores**.
2. Wählen Sie den **Store** aus, den Sie ändern möchten.
3. Klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten**.
4. Deaktivieren Sie unter "Authentifizierungsmethoden"**Passthrough-Authentifizierung von Citrix Gateway**.
5. Klicken Sie auf **OK**.

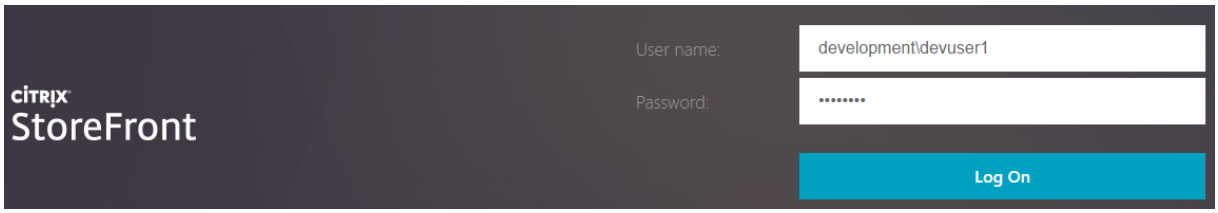


Melden Sie sich beim Gateway mit einem Benutzerkonto und Anmeldeinformationen von `production.com` an

Zum Testen melden Sie sich beim Gateway mit einem Benutzerkonto und Anmeldeinformationen von `production.com` an.



Nach der Anmeldung wird der Benutzer aufgefordert, die Anmeldeinformationen von `development.com` einzugeben.

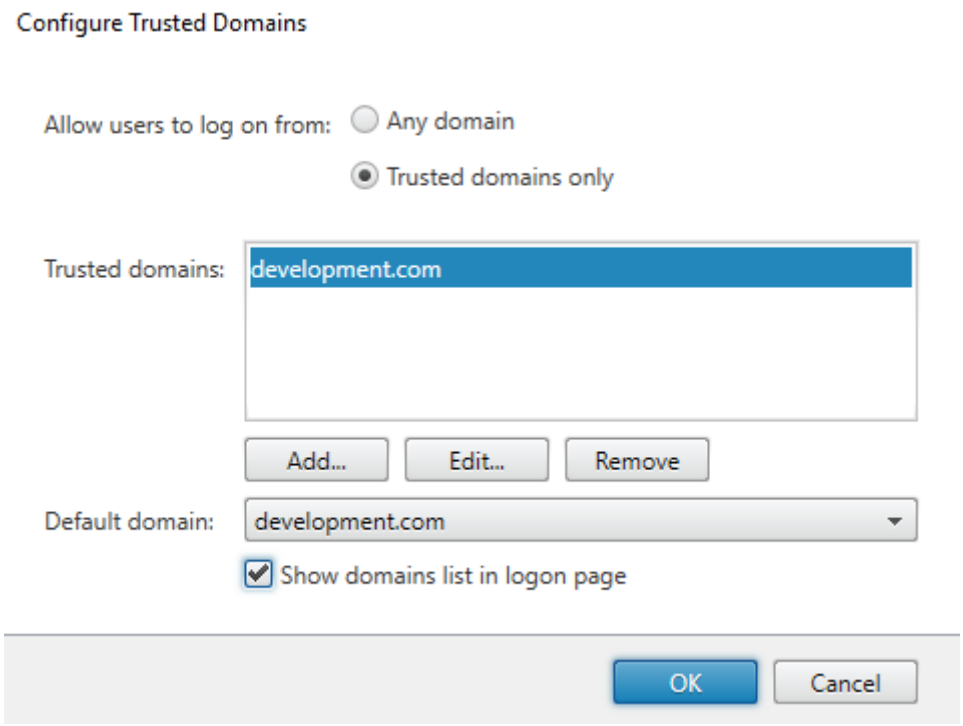


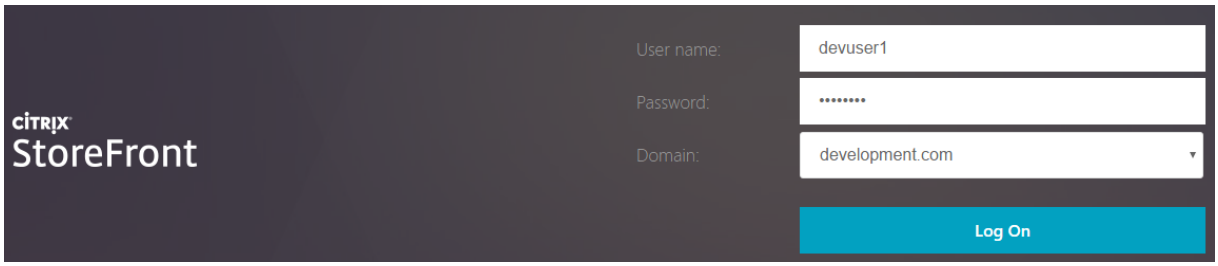
Hinzufügen einer Dropdownliste vertrauenswürdiger Domänen in StoreFront (optional)

Mit dieser optionalen Einstellung kann verhindert werden, dass Benutzer versehentlich die falsche Domäne zur Authentifizierung über Citrix Gateway eingeben.

Wenn der Benutzername für beide Domänen gleich ist, ist die Eingabe der falschen Domäne wahrscheinlicher. Neue Benutzer sind außerdem evtl. gewohnt, bei der Anmeldung über Citrix Gateway keine Domäne anzugeben. Benutzer können dann vergessen, domäne\benutzername für die zweite Domäne einzugeben, wenn sie aufgefordert werden, sich bei der Receiver für Web-Site anzumelden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus und klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
2. Klicken Sie auf den Dropdownpfeil neben **Benutzername und Kennwort**.
3. Klicken Sie auf **Hinzufügen**, um `development.com` als vertrauenswürdige Domäne hinzuzufügen, und aktivieren Sie das Kontrollkästchen **Domänenliste auf Anmeldeseite anzeigen**.
4. Klicken Sie auf **OK**.

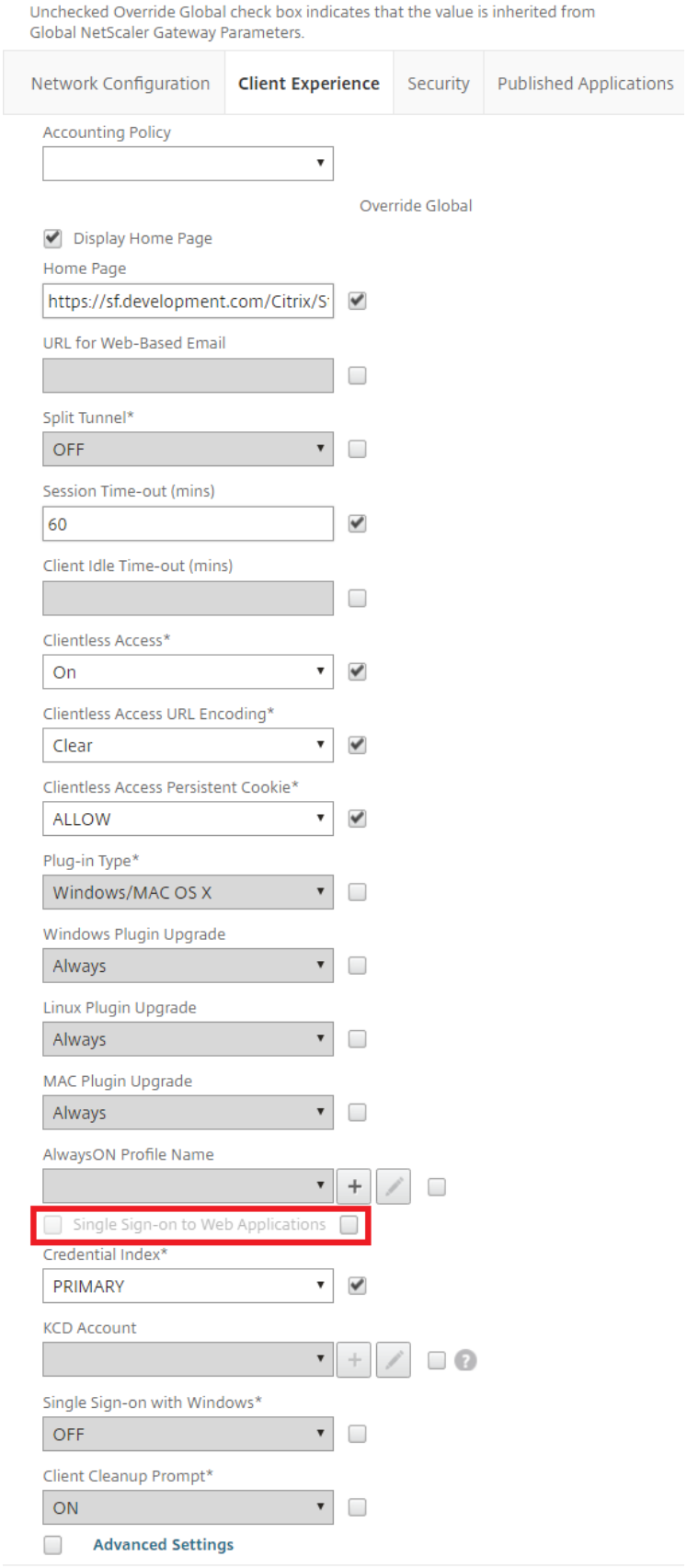


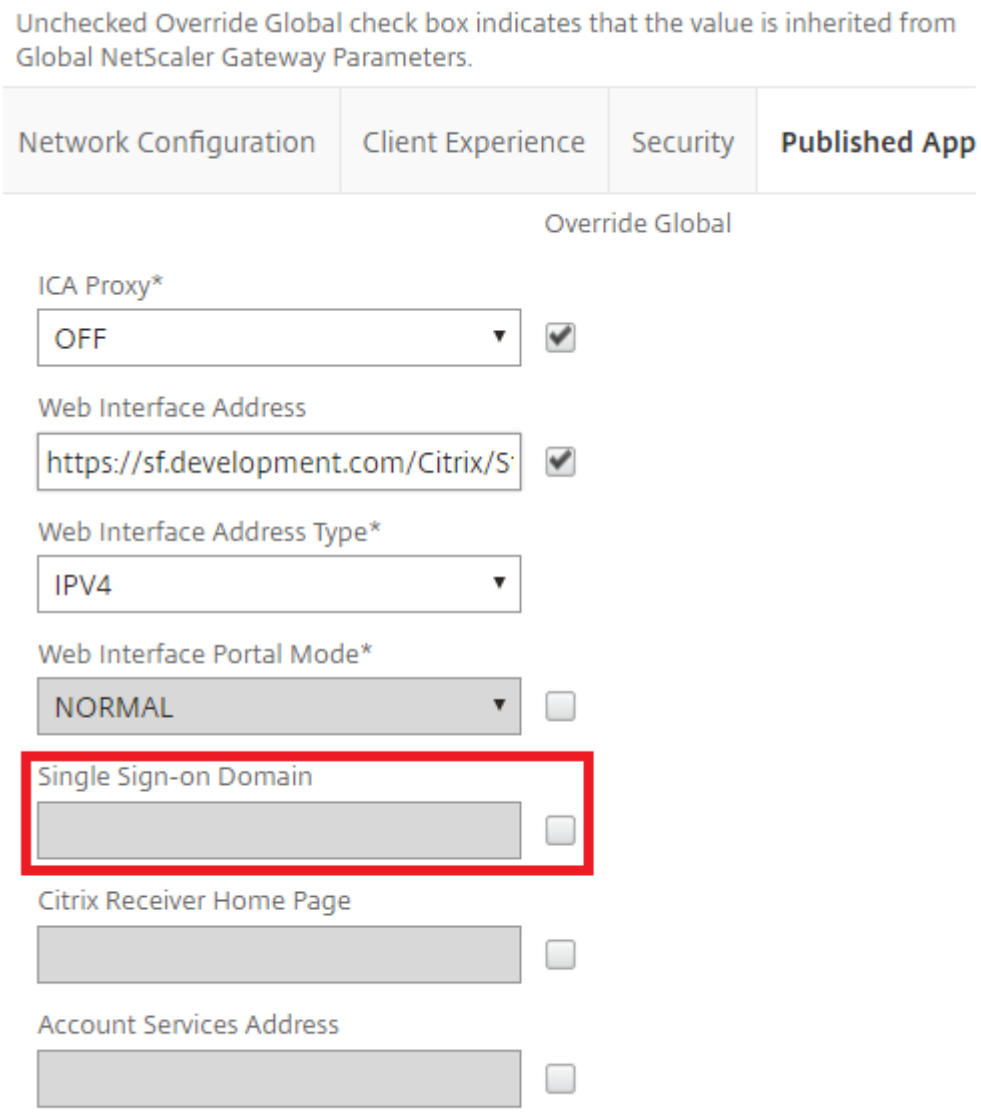


> **Hinweis:**
>
> Die Kennwortzwischenspeicherung im Browser wird für dieses Authentifizierungsszenario nicht empfohlen. Wenn Benutzer unterschiedliche Kennwörter für die beiden Domänenkonten verwenden, kann die Kennwortzwischenspeicherung zu Fehlern führen.

Aktionsrichtlinie für Citrix Gateway-Sitzungen mit clientlosem VPN (CVPN)

- Wenn Single Sign-On für Webanwendungen in der Citrix Gateway-Sitzungsrichtlinie aktiviert ist, ignoriert Receiver für Web falsche Anmeldeinformationen, die vom Citrix ADC-Gerät gesendet wurden, da die Authentifizierungsmethode **Passthrough-Authentifizierung von Citrix Gateway** auf der Receiver für Web-Site deaktiviert ist. Receiver für Web fordert Benutzer zur Eingabe der Anmeldeinformationen auf, unabhängig von der gewählten Einstellung für diese Option.
- Das Ausfüllen der Single Sign-On-Einträge auf den Registerkarten "Client Experience"und "Published Apps"auf dem Citrix ADC-Gerät ändert nicht das in diesem Artikel beschriebene Verhalten.





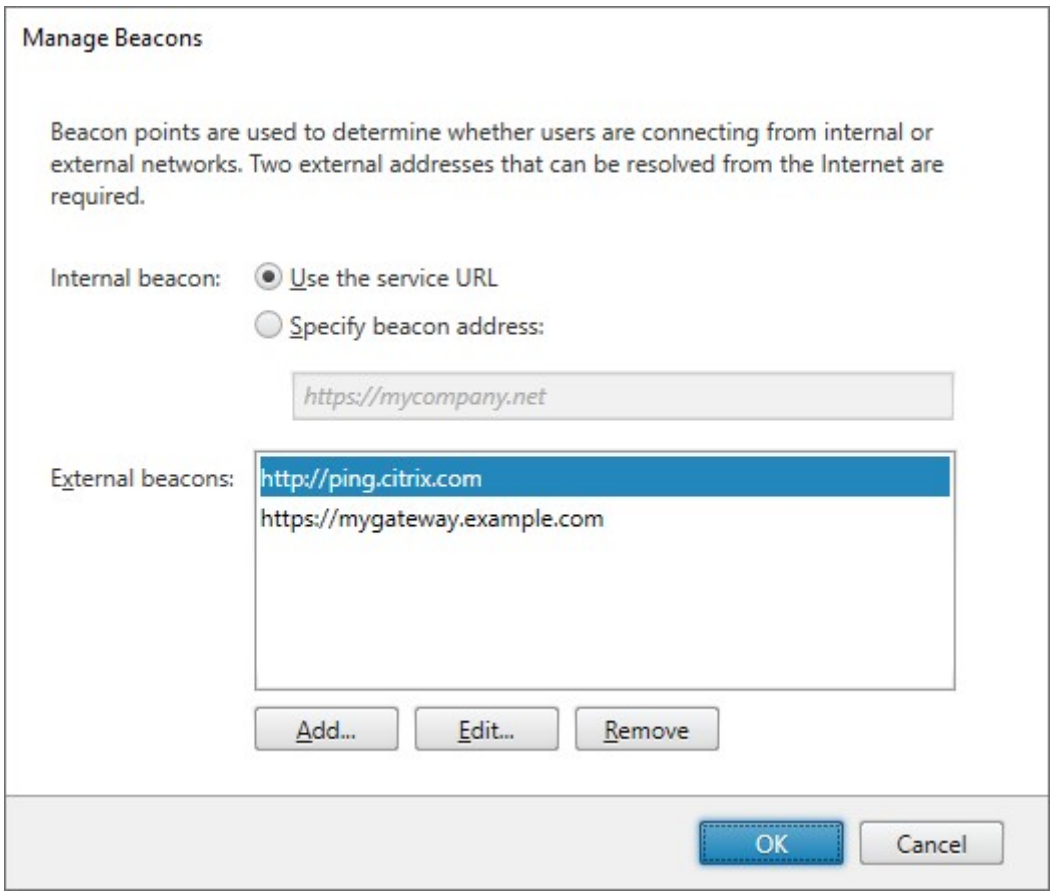
Beacons konfigurieren

May 31, 2024

> **Wichtig:**
>
> `http://ping.citrix.com` ist derzeit nicht verfügbar, daher müssen Sie einen alternativen Beacon einrichten.
>
> Verwenden Sie keine Websites Dritter, die Sie nicht besitzen, als externen Beacon. Verwenden

> Sie stattdessen Websites, die von Ihrer Organisation kontrolliert werden.

Auf der Seite"Beacons verwalten"können Sie URLs innerhalb und außerhalb des internen Netzwerks angeben, die als Beacons verwendet werden sollen. Die lokale installierte Citrix Workspace-App versucht eine Kontaktaufnahme mit den Beacons und ermittelt anhand der Antworten, ob Benutzer mit lokalen oder öffentlichen Netzwerken verbunden sind. Wenn ein Benutzer auf einen Desktop oder eine Anwendung zugreift, werden die Standortinformationen an den Server mit der Ressource weitergegeben, sodass die entsprechenden Verbindungsinformationen an die Citrix Workspace-App zurückgegeben werden können. Dadurch wird sichergestellt, dass die Benutzer nicht aufgefordert werden, sich neu anzumelden, wenn sie auf einen Desktop oder eine Anwendung zugreifen. Beacons werden von der Citrix Workspace-App für HTML5 nicht verwendet.



Beispiel: Wenn der interne Beacon zugänglich ist, ist der Benutzer mit dem lokalen Netzwerk verbunden. Wenn die Citrix Workspace-App den internen Beacon nicht kontaktieren kann und Antworten von beiden externen Beacons empfängt, hat der Benutzer eine Internetverbindung, ist jedoch außerhalb des Unternehmensnetzwerks. Daher muss sich der Benutzer über Citrix Gateway mit Desktops und Anwendungen verbinden. Wenn ein Benutzer auf einen Desktop oder eine Anwendung zugreift, wird der Server mit der Ressource benachrichtigt, um Details zum Citrix Gateway-Gerät, über das die Verbindung geleitet werden muss, bereitzustellen. Dies bedeutet, dass der Benutzer sich beim Zugriff auf den Desktop oder die Anwendung nicht am Gerät anmelden muss.

Standardmäßig legt StoreFront Folgendes fest:

- Den internen Beacon zur Basis-URL Ihrer Bereitstellung.
- Externe Beacons zu `http://ping.citrix.com` und der URL der ersten Citrix Gateway-Bereitstellung, die Sie hinzufügen.

So konfigurieren Sie Beacons:

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und klicken Sie im Bereich "Aktionen"auf **Beacons verwalten**.
2. Geben Sie die URL an, die als interner Beacon verwendet werden soll.
   - Zum Verwenden der Server-URL oder der Lastausgleichs-URL der StoreFront-Bereitstellung, wählen Sie **Dienst-URL verwenden**.
   - Zum Verwenden einer anderen URL wählen Sie **Beaconadresse angeben** und geben Sie eine hoch verfügbare URL im internen Netzwerk an.
3. Klicken Sie auf **Hinzufügen**, um die URL eines externen Beacons hinzuzufügen. Zum Ändern eines Beacons wählen Sie die URL in der Liste "Externe Beacons"aus und klicken Sie auf **Bearbeiten**. Wählen Sie eine URL in der Liste aus und klicken Sie auf **Entfernen**, um die Verwendung der Adresse als Beacon zu beenden.

   Sie müssen mindestens zwei hoch verfügbare externe Beacons, die von öffentlichen Netzwerken aus aufgelöst werden können, angeben. Die Beacon-URLs müssen vollqualifizierte Domänennamen sein (`http://example.com`), verwenden Sie keine abgekürzten NetBIOS-Namen (`http://example`). So kann die Citrix Workspace-App ermitteln, ob Benutzer hinter einer Internetpaywall sind, z. B. in einem Hotel oder Internetcafé. In solchen Fällen stellen alle externen Beacons eine Verbindung mit demselben Proxy her. Verwenden Sie URLs, die von Ihrer Organisation kontrolliert werden, nicht Websites Dritter.

Wenn Sie Beacons ändern, müssen Sie sicherstellen, dass die Benutzer die Citrix Workspace-App mit den geänderten Beaconinformationen aktualisieren. Benutzer können eine aktualisierte Citrix Workspace-App-Provisioningdatei von der Citrix Workspace-App für HTML5 abrufen. Andernfalls können Sie eine Provisioningdatei für den Store exportieren und diese Datei für die Benutzer verfügbar machen.

PowerShell SDK

Mit Get-STFRoamingBeacon können Sie die aktuellen Beacons abrufen.

Mit Set-STFRoamingBeacon können Sie einen Beacon hinzufügen.

Mit Clear-STFRoamingBeacon setzen Sie Beacons auf ihre Standardwerte zurück.

Einzelnen FQDN für die interne und externe Verwendung erstellen

February 28, 2024

Sie können einen einzelnen vollqualifizierten Domänennamen (FQDN) erstellen, der direkt von Ihrem Unternehmensnetzwerk aus und remote über ein Citrix Gateway auf einen Store zugreifen kann.

Nachfolgend gelten folgende Beispiele:

- `https://storefront.example.com` ist die Einzel-URL für den Zugriff der Benutzer auf StoreFront. Innerhalb des Netzwerks wird sie in den StoreFront-Server oder Load Balancer aufgelöst. Außerhalb des Netzwerks wird sie in das Gateway aufgelöst.
- `https://storefrontcb.example.com` ist die Rückruf-URL. Diese wird intern in das Gateway aufgelöst. Sie ist nur für Smart Access oder die kennwortlose Authentifizierung erforderlich.

Basis-URL der Servergruppe

Ändern Sie die Basis-URL zur Verwendung als Einzel-URL. Siehe Basis-URL für eine Bereitstellung ändern.

StoreFront-Beacons für die Citrix Workspace-App

Die lokale installierte Citrix Workspace-App versucht eine Kontaktaufnahme mit den Beacons und ermittelt anhand der Antworten, ob Benutzer mit lokalen oder öffentlichen Netzwerken verbunden sind.

Standardmäßig verwendet StoreFront die Basis-URL der Servergruppe als interne Beacon URL. In dieser Konfiguration ist dieselbe URL sowohl intern als auch extern gültig und kann daher nicht als Beacon verwendet werden. Daher müssen Sie den internen Beacon auf eine URL festlegen, von der Sie wissen, dass sie nur intern zugänglich ist.

Siehe Beacon konfigurieren.

Externes DNS

- storefront.example.com wird in die nach außen gerichtete IP des virtuellen Citrix Gateway-Servers aufgelöst.

Internes DNS

- storefront.example.com wird in den StoreFront-Load Balancer bzw. die IP des einzelnen StoreFront-Servers aufgelöst.
- storefrontcb.example.com wird in die VIP des virtuellen Gateway-Servers aufgelöst. Gibt es eine Firewall zwischen der DMZ und dem lokalen Unternehmensnetzwerk, müssen Sie dies berücksichtigen.

StoreFront-Konfiguration exportieren und importieren

April 17, 2024

> Hinweis:
>
> Sie können nur StoreFront-Konfigurationen von StoreFront-Versionen importieren, welche mit der StoreFront-Zielinstallation identisch sind. Jedes kumulative Update wird aufgrund dieser Einschränkung als eine andere Produktversion betrachtet.

Sie können die gesamte Konfiguration einer StoreFront-Bereitstellung exportieren. Dies schließt Einzelserverbereitstellungen und Servergruppenkonfigurationen ein. Wenn eine vorhandene Bereitstellung bereits auf dem importierenden Server besteht, wird die aktuelle Konfiguration gelöscht und durch die im Backuparchiv enthaltene Konfiguration ersetzt. Wenn der Zielserver eine saubere Werkstandardinstallation ist, wird mit der aus dem Backup importierten Konfiguration eine neue Bereitstellung erstellt. Das exportierte Konfigurationsbackup ist im unverschlüsselten Zustand ein ZIP-Archiv oder eine CTXZIP-Datei, wenn Sie die Backupdatei bei ihrer Erstellung verschlüsseln.

Szenarios, in denen Konfigurationsexport und -import verwendet werden kann

- Führen Sie nur ein Backup von StoreFront-Bereitstellungen in einem funktionierenden und vertrauenswürdigen Zustand aus. Bei jeder Änderung an der Konfiguration ist ein neues Backup erforderlich, welches das alte ersetzt. Sie können vorhandene Backups nicht ändern, da ein Datei-Hash der Datei backup.zip Änderungen verhindert.
- Führen Sie zum Zweck der Notfallwiederherstellung ein Backup VOR dem Upgrade von StoreFront aus.
- Klonen bestehender StoreFront-Testbereitstellungen für die Produktion
- Erstellen von Benutzerakzeptanzumgebungen durch Klonen von Produktionsbereitstellungen in eine Testumgebung

- Verschieben von StoreFront bei einer Betriebssystemmigration, z. B. beim Upgrade des Hostings von Windows Server 2019 auf Windows 2022. Direkte Betriebssystem-Upgrades werden nicht unterstützt.
- Aufbau zusätzlicher Servergruppen in Bereitstellungen mit mehreren Standorten, z. B. in großen Unternehmen mit mehreren Datencentern

Punkte, die beim Exportieren und Importieren einer StoreFront-Konfiguration zu berücksichtigen sind

- Verwenden Sie zurzeit von Citrix veröffentlichte Authentifizierungs-SDKs, wie Magic Word-Authentifizierung oder Authentifizierungsanpassungen von Drittanbietern? In diesem Fall müssen Sie diese Pakete auf ALLEN importierenden Servern installieren, BEVOR Sie eine Konfiguration importieren, die spezielle Authentifizierungsmethoden enthält. Wenn erforderliche Authentifizierungs-SDKs nicht auf den importierenden Servern installiert sind, schlägt der Import der Konfiguration fehl. Beim Importieren einer Konfiguration in eine Servergruppe müssen Sie die Authentifizierungspakete auf allen Mitgliedern der Gruppe installieren.
- Sie können die Konfigurationsbackups ver- und entschlüsseln. Die exportierenden und importierenden PowerShell-Cmdlets unterstützen beide Anwendungsfälle.
- Sie können verschlüsselte Backups (.ctxzip) später entschlüsseln; StoreFront kann unverschlüsselte Backupdateien (.zip) jedoch nicht erneut verschlüsseln. Wenn ein verschlüsseltes Backup erforderlich ist, führen Sie den Export erneut durch und verwenden Sie dabei ein PowerShell-Anmeldeinformationenobjekt mit einem Kennwort Ihrer Wahl.
- Die Site-ID der Website in IIS, in der StoreFront installiert ist (exportierender Server), muss mit der Site-ID der Zielwebsite in IIS (importierender Server) übereinstimmen, für die Sie das Backup der StoreFront-Konfiguration wiederherstellen möchten.

PowerShell-Cmdlets

Export-STFConfiguration

Parameter	Beschreibung
-TargetFolder (String)	Der Exportpfad für das Backuparchiv. Beispiel: “$env:userprofile\desktop\”

Parameter	Beschreibung
-Credential (PSCredential Object)	Geben Sie ein Anmeldeinformationsobjekt an, um während des Exports ein verschlüsseltes CTXZIP-Backuparchiv zu erstellen. Das PowerShell-Anmeldeinformationsobjekt muss das Kennwort für die Ver- und Entschlüsselung enthalten. Verwenden Sie nicht **-Credential** gleichzeitig mit dem Parameter **-NoEncryption**. Beispiel: $CredObject
-NoEncryption (Switch)	Geben Sie an, dass das Backuparchiv eine unverschlüsselte ZIP-Datei ist. Verwenden Sie nicht **-NoEncryption** gleichzeitig mit dem Parameter **-Credential**.
-ZipFileName (Zeichenfolge)	Der Name des StoreFront-Konfigurationsbackuparchivs. Fügen Sie keine Dateierweiterung wie .zip oder .ctxzip hinzu. Die Dateierweiterung wird automatisch hinzugefügt und hängt davon ab, ob beim Export der Parameter **-Credential** oder **-NoEncryption** angegeben wird. Beispiel: “backup”
-Force (Boolean)	Dieser Parameter überschreibt automatisch Backuparchive mit demselben Dateinamen, die bereits im angegebenen Speicherort vorhanden sind.

> **Wichtig:**
>
> Der Parameter **-SiteID** aus StoreFront 3.5 ist seit Version 3.6 veraltet. Beim Import muss **SiteID** nicht mehr angegeben werden, da immer die Site-ID aus dem Backuparchiv verwendet wird. Stellen Sie sicher, dass die Site-ID mit der vorhandenen StoreFront-Website übereinstimmt, die bereits in IIS auf dem importierenden Server konfiguriert ist.Konfigurationsimports von **SiteID 1** zu **SiteID 2** werden NICHT unterstützt.

Import-STFConfiguration

Parameter	Beschreibung
-ConfigurationZip (Zeichenfolge)	Der vollständige Pfad für das Backuparchiv, das Sie importieren. Er muss die Dateierweiterung enthalten. Verwenden Sie .zip für unverschlüsselte und .ctxzip für verschlüsselte Backuparchive. Beispiel:`$env:userprofile\desktop\backup.ctxzip`
-Credential (PSCredential Object)	Geben Sie ein Anmeldeinformationsobjekt an, um während des Imports eine verschlüsselte Backupdatei zu entschlüsseln. Beispiel:`$CredObject`
-HostBaseURL (Zeichenfolge)	Wenn dieser Parameter enthalten ist, wird die von Ihnen angegebene Host-Basis-URL statt der Host-Basis-URL des exportierenden Servers verwendet. Beispiel:`https://<importingserver>.example.com`

Unprotect-STFConfigurationBackup

Parameter	Beschreibung
-TargetFolder (String) -Credential (PSCredential Object)	Der Exportpfad für das Backuparchiv. Beispiel:$env:userprofile\desktop Erstellen Sie mit diesem Parameter eine unverschlüsselte Kopie des verschlüsselten Backuparchivs. Geben Sie das PowerShell-Anmeldeinformationsobjekt an, das das Kennwort für die Entschlüsselung enthält. Beispiel:`$CredObject`
-EncryptedConfigurationZip (Zeichenfolge)	Der vollständige Pfad für das verschlüsselte Backuparchiv, das Sie entschlüsseln möchten. Sie müssen die Dateierweiterung CTXZIP angeben. Beispiel:`$env:userprofile\\desktop\\backup.ctxzip`

Parameter	Beschreibung
-OutputFolder (Zeichenfolge) -Force (Boolean)	Der Pfad für eine unverschlüsselte Kopie des verschlüsselten Backuparchivs (.ctxzip). Die ursprüngliche verschlüsselte Kopie des Backups bleibt erhalten, sodass sie wiederverwendet werden kann. Geben Sie für die unverschlüsselte Kopie keinen Dateinamen und keine Dateierweiterung an. Beispiel:$env:userprofile\desktop Dieser Parameter überschreibt automatisch Backuparchive mit demselben Dateinamen, die bereits im angegebenen Speicherort vorhanden sind.

Beispiele für Konfigurationsexporte und -importe

Importieren der StoreFront-Cmdlets in die aktuelle PowerShell-Sitzung

Öffnen Sie PowerShell Integrated Scripting Environment (ISE) auf dem StoreFront-Server und führen Sie Folgendes aus:

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath
    ','Machine')
2 $SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\
    PowerShellSDK\Modules\Citrix.StoreFront'
3 Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
4 Import-Module "$SDKModules.Authentication\Citrix.StoreFront.
    Authentication.psd1" -verbose
5 Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -
    verbose
6 Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -
    verbose
7 Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.
    psd1" -verbose
8 <!--NeedCopy-->
```

Einzelserverszenarios

Erstellen Sie ein unverschlüsseltes Backup einer vorhandenen Konfiguration auf Server A und stellen Sie es auf derselben Bereitstellung wieder her Exportieren Sie die Konfiguration des Servers, den Sie sichern möchten.


```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

Kopieren Sie die Datei backup.zip an einen sicheren Speicherort. Sie können das Backup im Rahmen einer Notfallwiederherstellung dazu verwenden, den Server im vorherigen Zustand wiederherzustellen.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.example.com"
<!--NeedCopy-->
```

Serverklonerstellung durch Sichern der Konfiguration auf Server A und Wiederherstellen auf Server B Exportieren Sie die Konfiguration des Servers, den Sie sichern möchten.

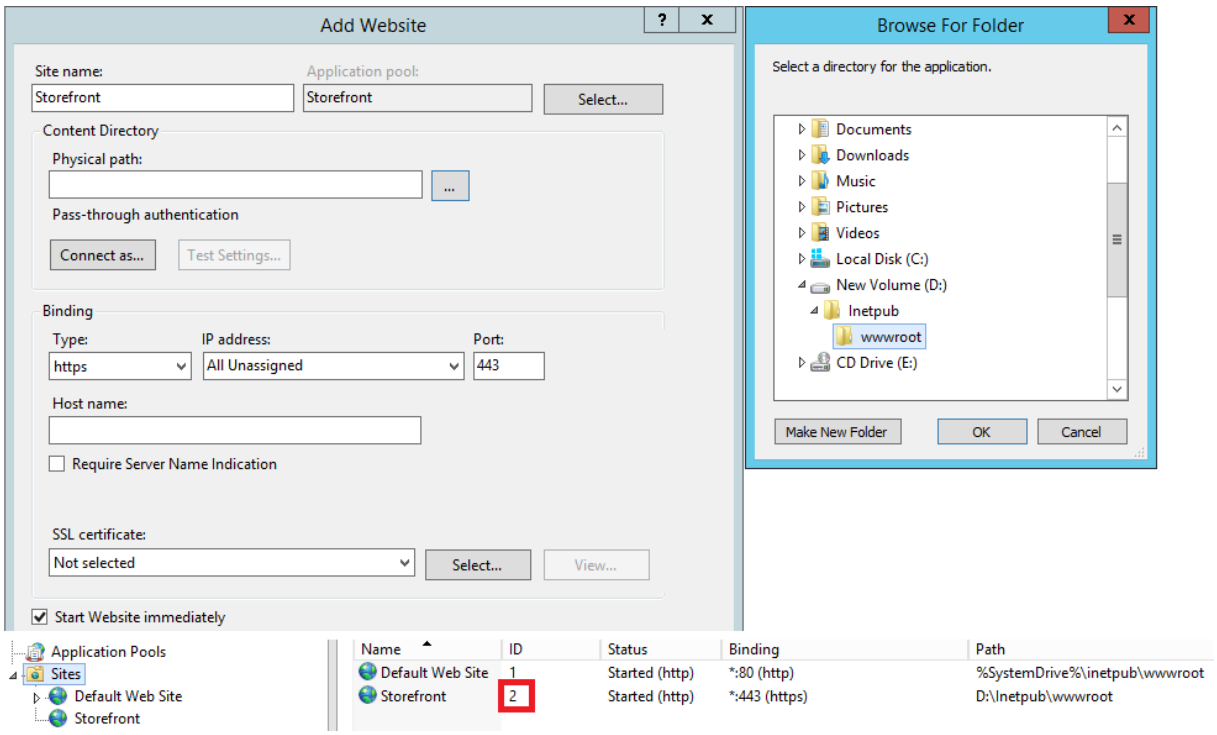
```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

Kopieren Sie die Datei backup.zip auf den Desktop des Servers B.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://serverB.example.com"
<!--NeedCopy-->
```

StoreFront ist bereits auf einer benutzerdefinierten Website in IIS bereitgestellt. Stellen Sie die Konfiguration auf einer anderen benutzerdefinierten Websitebereitstellung wieder her Bei Server A ist StoreFront auf einer benutzerdefinierten Website bereitgestellt statt der gewohnten Standardwebsite in IIS. Die IIS Site-ID für die zweite in IIS erstellte Website ist 2. Der physische Pfad der StoreFront-Website kann auf einem anderen Laufwerk sein, das nicht zum System gehört, wie d:\ oder auf dem standardmäßigen Systemlaufwerk c:\. Er sollte jedoch eine IIS Site-ID verwenden, die größer als 1 ist.

Eine neue Website mit dem Namen “StoreFront”wurde in IIS konfiguriert, die **SiteID = 2** verwendet. StoreFront wurde bereits auf der benutzerdefinierten Website in IIS bereitgestellt und der physische Pfad auf dem Laufwerk ist `d:\inetpub\wwwrooot`.



1. Exportieren Sie eine Kopie der Konfiguration von Server-A.
2. Konfigurieren Sie IIS auf Server B mit einer neuen Website namens **StoreFront**, die auch **SiteID 2** verwendet.
3. Importieren Sie die Server A-Konfiguration auf Server B. Die Site-ID im Backup wird verwendet und muss mit der Zielwebsite übereinstimmen, in die Sie die StoreFront-Konfiguration importieren.

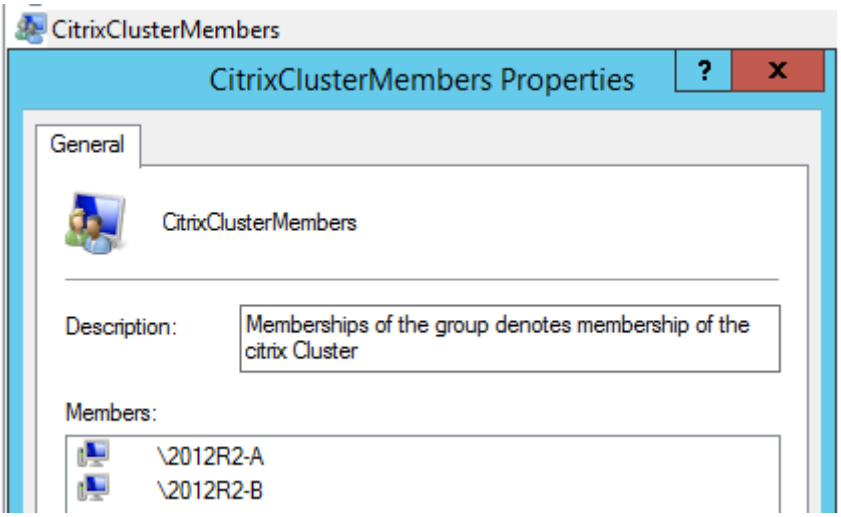
```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://serverB.example.
    com"
2 <!--NeedCopy-->
```

Servergruppenszenarios

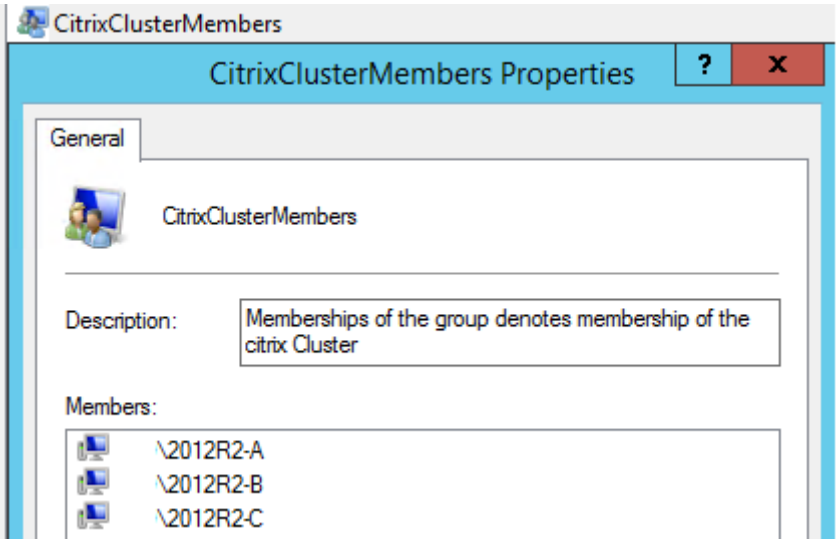
Szenario 1: Erstellen Sie ein Backup einer vorhandenen Servergruppenkonfiguration und stellen Sie die Konfiguration in derselben Servergruppenbereitstellung später wieder her Zu einem früheren Zeitpunkt, als die Servergruppe nur zwei StoreFront-Server, 2012R2-A und 2012R2-B, enthielt, wurde ein Backup der Konfiguration erstellt. Das Backuparchiv enthält einen Datensatz der **CitrixClusterMembership**, die zur Zeit des Backups nur die beiden ursprünglichen Server 2012R2-A und 2012R2-B enthielt. Die Größe der StoreFront-Servergruppenbereitstellung ist seit dem ursprünglichen Backup aufgrund des Unternehmensbedarfs angestiegen und ein zusätzlicher Knoten, 2012R2-C, wurde der Servergruppe hinzugefügt. Die zugrunde liegende StoreFront-Konfiguration

der Servergruppe im Backup hat sich nicht geändert. Die aktuelle CitrixClusterMembership von drei Servern muss erhalten bleiben, auch wenn ein altes Backup mit nur den zwei ursprünglichen Servergruppenknoten importiert wird. Während des Imports wird die aktuelle Clustermitgliedschaft beibehalten und zurückgeschrieben, wenn die Konfiguration erfolgreich auf den primären Server importiert wurde. Beim Import wird auch die aktuelle CitrixClusterMembership beibehalten, wenn Servergruppenknoten seit dem Erstellen des ursprünglichen Backups entfernt wurden.

1. Exportieren Sie die Konfiguration der Servergruppe 1 aus 2012R2-A, dem primären Server, der die gesamte Servergruppe verwaltet.



2. Fügen Sie der vorhandenen Servergruppe dann einen weiteren Server, 2012R2-C, hinzu.



3. Stellen Sie die Konfiguration der Servergruppe auf einen früheren funktionierenden Zustand wieder her. Während des Importvorgangs erstellt StoreFront ein Backup der aktuellen Citrix-ClusterMembership der drei Server und stellt sie nach dem Abschluss des Imports wieder her.
4. Importieren Sie die Konfiguration der Servergruppe 1 zurück auf den Knoten 2012R2-A.


```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://servergroup1.
    example.com"
<!--NeedCopy-->
```

5. Übertragen Sie die importierte Konfiguration auf die gesamte Servergruppe, sodass alle Server nach dem Import eine konsistente Konfiguration aufweisen.

Szenario 2: Erstellen Sie ein Backup einer vorhandenen Konfiguration von Servergruppe 1 und erstellen Sie damit eine neue Servergruppe auf einer anderen Werkstandardinstallation. Sie können dem primären Server dann andere neue Servergruppenmitglieder hinzufügen Servergruppe 2 wird mit zwei neuen Servern erstellt: 2012R2-C und 2012R2-D. Die Konfiguration von Servergruppe 2 basiert auf der Konfiguration einer vorhandenen Bereitstellung, Servergruppe 1, die ebenfalls zwei Server enthält: 2012R2-A und 2012R2-B. Die im Backuparchiv enthaltene CitrixClusterMembership wird beim Erstellen einer neuen Servergruppe nicht verwendet. Von der aktuellen CitrixClusterMembership wird immer ein Backup erstellt und sie wird nach dem Abschluss des Imports wiederhergestellt. Wenn Sie mit einer importierten Konfiguration eine neue Bereitstellung erstellen, enthält die Sicherheitsgruppe CitrixClusterMembership nur den importierenden Server, bis weitere Server der neuen Gruppe hinzugefügt werden. Servergruppe 2 ist eine neue Bereitstellung und soll neben Servergruppe 1 bestehen. Geben Sie den Parameter -HostBaseURL an. Servergruppe 2 wird mit einer neuen StoreFront-Werkstandardinstallation erstellt.

1. Exportieren Sie die Konfiguration der Servergruppe 1 aus 2012R2-A, dem primären Server, der die gesamte Servergruppe verwaltet.
2. Importieren Sie die Konfiguration der Servergruppe 1 auf den Knoten 2012R2-C, der der primäre Server zum Verwalten der neu erstellten Servergruppe 2 ist.

   ```
   Import-STFConfiguration -configurationZip "$env:userprofile\
       desktop\backup.ctxzip" -HostBaseURL "https://servergroup2.
       example.com"
   <!--NeedCopy-->
   ```

3. Verknüpfen Sie alle weiteren Server, die zur neuen Bereitstellung “Servergruppe 2”gehören sollen. Die neu aus Servergruppe 1 importierte Konfiguration wird automatisch auf alle neuen Mitglieder der Servergruppe 2 übertragen, da dies Teil des normalen Verknüpfungsvorgangs ist, wenn ein neuer Server hinzugefügt wird.

Szenario 3: Erstellen Sie ein Backup einer vorhandenen Konfiguration von Servergruppe A und überschreiben Sie damit die vorhandene Konfiguration der Servergruppe B Servergruppe 1 und Servergruppe 2 sind bereits in zwei verschiedenen Datencentern vorhanden. An Servergruppe 1 werden viele StoreFront-Konfigurationsänderungen vorgenommen, die Sie auf Servergruppe 2 im

anderen Datencenter übertragen müssen. Sie können die Änderungen von Servergruppe 1 auf Servergruppe 2 per Port übertragen. Verwenden Sie **CitrixClusterMembership** nicht im Backuparchiv auf der Servergruppe 2. Legen Sie den Parameter **-HostBaseURL** während des Imports fest, da die Host-Basis-URL für Servergruppe 2 nicht in den gleichen vollqualifizierten Domänennamen (FQDN) geändert werden sollte, den die Servergruppe 1 zurzeit verwendet. Servergruppe 2 ist eine vorhandene Bereitstellung.

1. Exportieren Sie die Konfiguration der Servergruppe 1 aus 2012R2-A, dem primären Server, der die gesamte Servergruppe verwaltet.
2. Importieren Sie die Konfiguration der Servergruppe 1 auf die Werkstandardinstallation auf Knoten 2012R2-C, der der primäre Server der neu erstellten Servergruppe 2 ist.

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.zip" -NoEncryption -HostBaseURL "https://
    servergroup2.example.com"
<!--NeedCopy-->
```

Erstellen eines verschlüsselte Backups der Serverkonfiguration

Ein PowerShell-Anmeldeinformationenobjekt enthält den Benutzernamen und das Kennwort für ein Windows-Konto. PowerShell-Anmeldeinformationsobjekte gewährleisten, dass Ihr Kennwort im Speicher geschützt ist.

> **Hinweis:**
>
> Zum Verschlüsseln und Entschlüsseln eines Konfigurationsbackuparchivs benötigen Sie nur das Kennwort. Der im Anmeldeinformationsobjekt gespeicherte Benutzername wird nicht verwendet. Sie müssen in der PowerShell-Sitzung ein Anmeldeinformationsobjekt mit demselben Kennwort erstellen, das auf den exportierenden und importierenden Servern verwendet wird. Sie können im Anmeldeinformationsobjekt einen beliebigen Benutzer angeben.

PowerShell erfordert die Angabe eines Benutzers beim Erstellen eines neuen Anmeldeinformationsobjekts. Der folgende Beispielcode enthält den zurzeit angemeldeten Windows-Benutzer.

Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt in der Powershell-Sitzung auf dem exportierenden Server.

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
<!--NeedCopy-->
```

Exportieren Sie die Konfiguration in backup.ctxzip (eine verschlüsselte ZIP-Datei).


```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -Credential $CredObject
<!--NeedCopy-->
```

Erstellen Sie ein identisches PowerShell-Anmeldeinformationsobjekt in der Powershell-Sitzung auf dem importierenden Server.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.ctxzip" -Credential $CredObject -HostBaseURL "https://
    storefront.example.com"
<!--NeedCopy-->
```

Aufheben des Schutzes eines vorhandenen verschlüsselten Backuparchivs

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)

Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:
    userprofile\desktop\backup.ctxzip" -credential $CredObject -
    outputFolder "c:\StoreFrontBackups" -Force
<!--NeedCopy-->
```

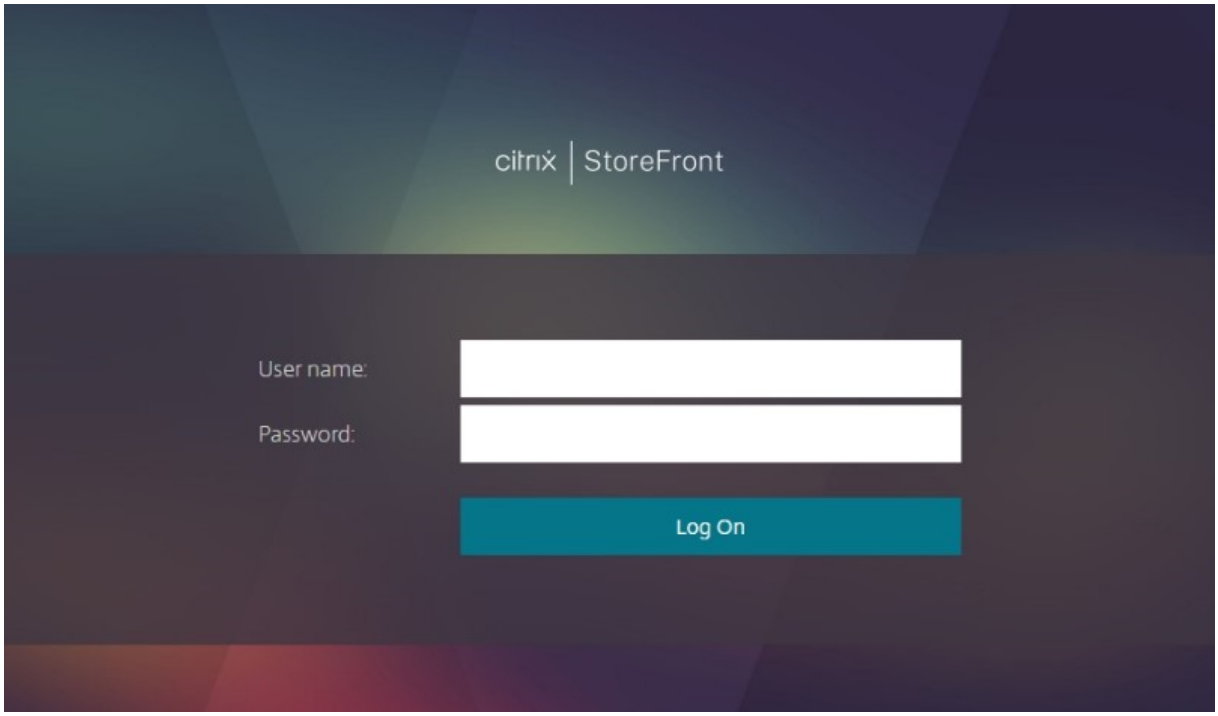
Endanwender-Dokumentation

April 17, 2024

In diesem Abschnitt werden die Features und die Oberfläche von Stores beim Zugriff über einen Webbrowser und über die Citrix Workspace-App beschrieben.

Anmelden

Abhängig von der Authentifizierungsmethode und davon, ob Single Sign-On aktiviert ist, müssen Sie sich möglicherweise anmelden.

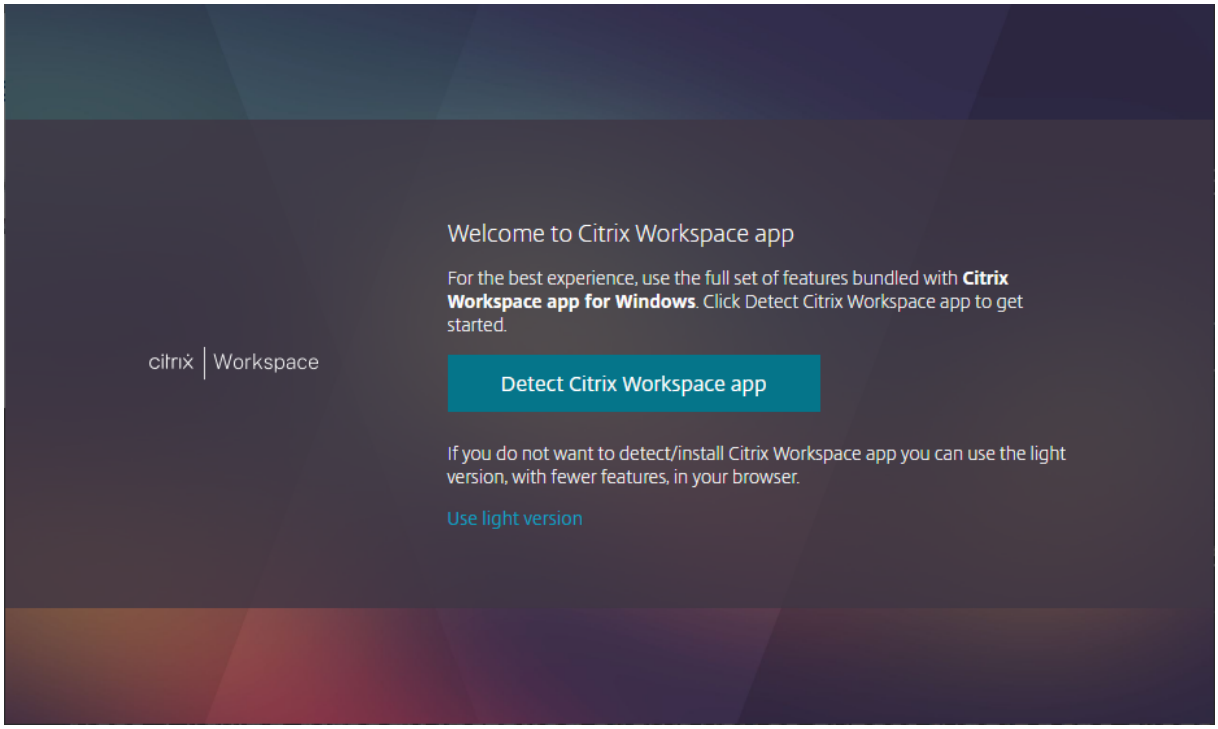


Citrix Workspace-App-Erkennung

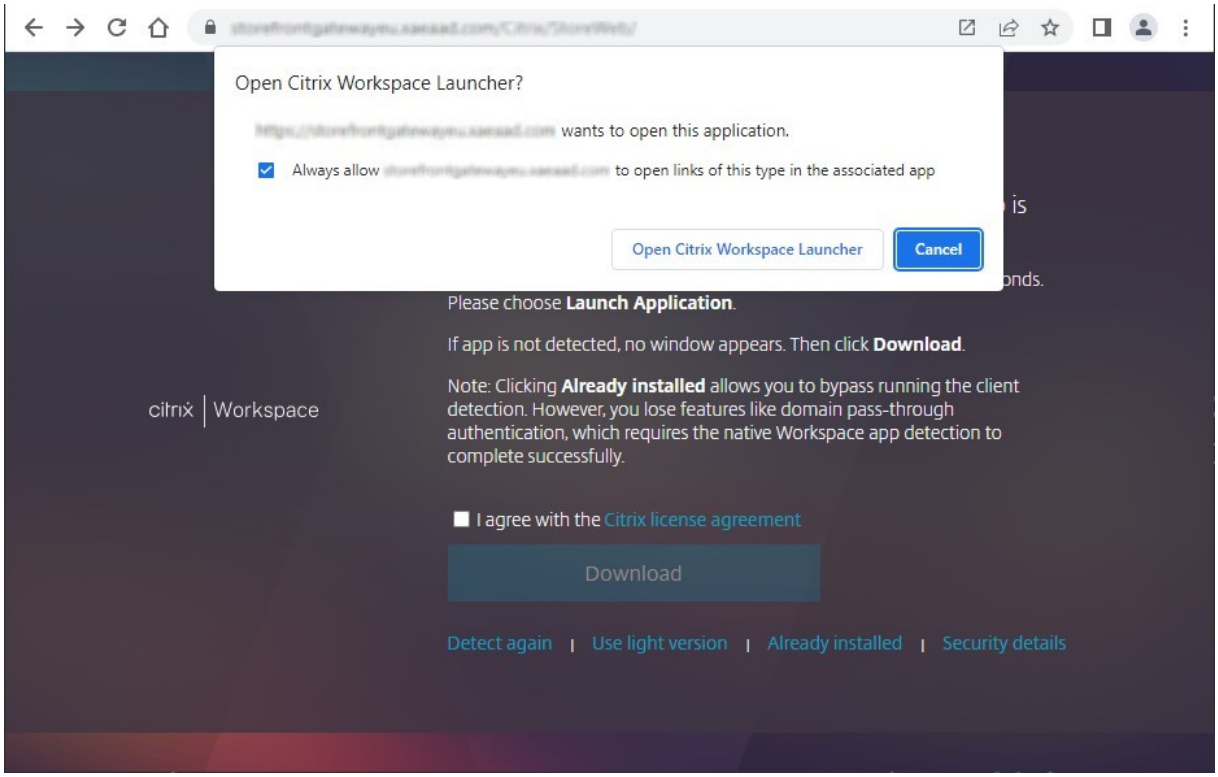
> **Hinweis:**
>
> Dieser Schritt gilt nur für den Zugriff auf Stores über einen Webbrowser, nicht aber für die lokal installierte Citrix Workspace-App. Er kann je nach Konfiguration vor oder nach der Anmeldung erfolgen.

Je nach Konfiguration wird beim ersten Zugriff auf den Store über einen Webbrowser bzw. nach dem Löschen der Cookies ggf. **Willkommen bei der Citrix Workspace-App** angezeigt. Sie haben folgende Möglichkeiten:

- Klicken Sie auf **Citrix Workspace-App erkennen**, wenn Ressourcen in der lokal installierten Citrix Workspace-App gestartet werden sollen. Dies wird für ein optimales Erlebnis empfohlen.
- Klicken Sie auf **Lightversion verwenden** (falls verfügbar), um Ressourcen immer im Browser zu starten.



Wenn Sie auf **Citrix Workspace-App erkennen** klicken, wird versucht, eine lokal installierte Citrix Workspace-App zu erkennen. Zuerst geschieht dies unter Verwendung der Citrix Workspace-Weberweiterungen. Sind diese nicht installiert oder wird die lokal installierte Citrix Workspace-App nicht erkannt, wird versucht, **Citrix Workspace Launcher** (eine Komponente der Citrix Workspace-App) zu öffnen. Wenn die Citrix Workspace-App installiert ist, wird ein Browserfenster geöffnet, in dem Sie aufgefordert werden, **Citrix Workspace Launcher** auszuführen. Klicken Sie (je nach Browser) auf **Citrix Workspace Launcher öffnen** oder auf **Link öffnen**. Es wird empfohlen, ***Domain immer erlauben, Links dieser Art in der zugehörigen App zu öffnen*** zu aktivieren, damit dieses Fenster nicht bei jedem Start einer Ressource angezeigt wird.



Wenn eine lokal installierte Citrix Workspace-App erkannt wird, wird nach einigen Sekunden mit dem nächsten Fenster fortgefahren. Wenn Sie anschließend eine Ressource starten, wird je nachdem, was erkannt worden war, entweder die Komponente Citrix Workspace-Weberweiterungen oder Citrix Workspace Launcher verwendet, um die Ressource in der lokal installierten Citrix Workspace-App zu öffnen.

Ist die Citrix Workspace-App nicht installiert oder der Launcher wird abgebrochen, haben Sie je nach Konfiguration die folgenden Möglichkeiten:

- **Herunterladen**: Die Citrix Workspace-App wird von der Citrix Website oder vom StoreFront-Server heruntergeladen. Klicken Sie nach der Installation der Citrix Workspace-App auf **Erneut erkennen**.
- **Erneut erkennen:** Der Versuch, die lokal installierte Citrix Workspace-App zu erkennen, wird wiederholt.
- **Lightversion verwenden:** Die Erkennung der Workspace-App wird übersprungen und alle Ressourcen werden im Browser geöffnet.
- **Bereits installiert**: Verwenden Sie diese Option, wenn eine ältere Version von Citrix Receiver installiert ist, die Citrix Workspace Launcher bzw. Citrix Workspace-Weberweiterungen nicht unterstützt. Wenn Sie diese Option auswählen und eine virtuelle App oder einen virtuellen Desktop starten, lädt Ihr Browser eine Datei **launch.ica** herunter, die Sie mit Citrix Receiver öffnen können. Die Funktionalität ist bei Verwendung dieser Option eingeschränkt, sie wird daher nicht empfohlen.

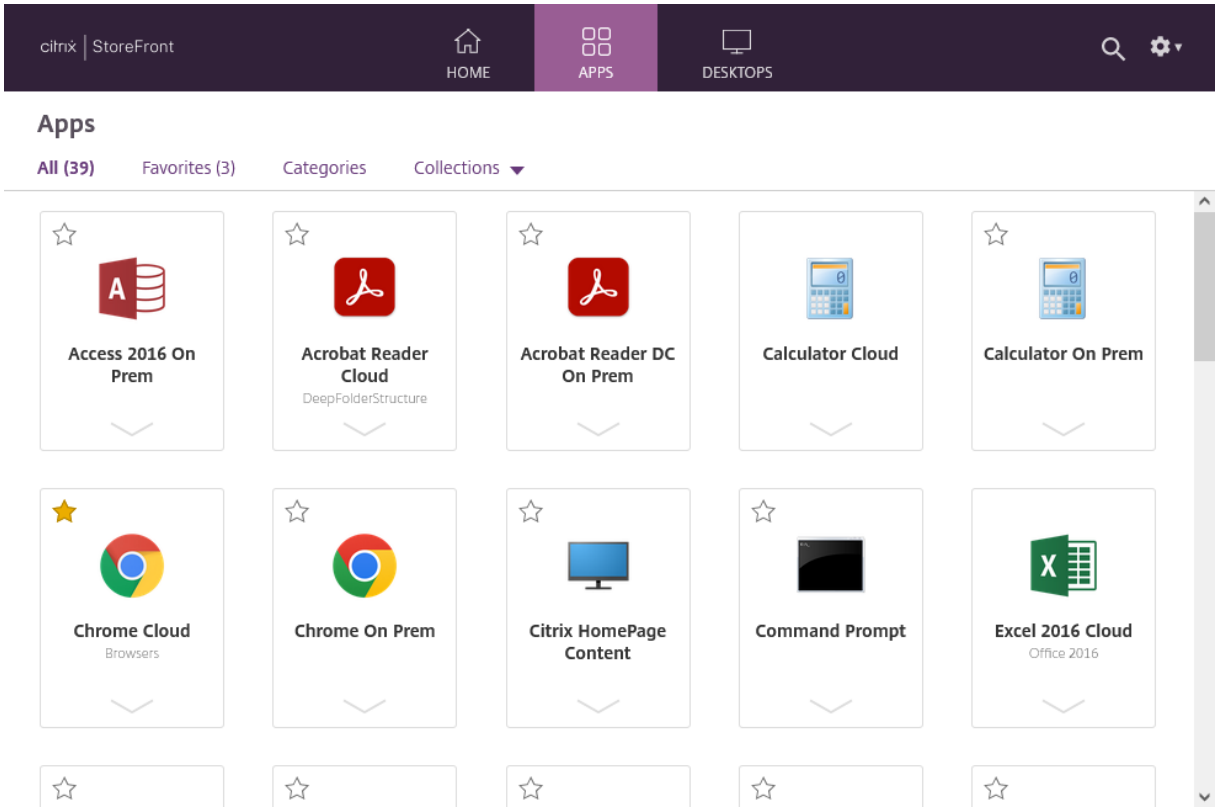
Registerkarte “Home”

Auf der Registerkarte **Home** werden alle App-Gruppen mit Highlights sowie alle bevorzugten und vorgegebenen Apps und Desktops angezeigt. Die Registerkarte **Home** wird nur angezeigt, wenn Favoriten für den Store aktiviert sind.

Registerkarte “Apps”

Die Registerkarte **Apps** enthält eine Reihe von Unteransichten:

- **Alle** zeigt alle Apps an.
- **Favoriten:** zeigt alle Favoriten-Apps an.
- **Kategorien** zeigt Kategorien und die Apps innerhalb dieser Kategorien an. Wie Kategorien angezeigt werden, hängt von den Kategorieeinstellungen ab.
- **Sammlungen** zeigt die App-Gruppen mit Highlights an.



Registerkarte “Desktops”

Die Registerkarte **Desktops** hat zwei Unteransichten:

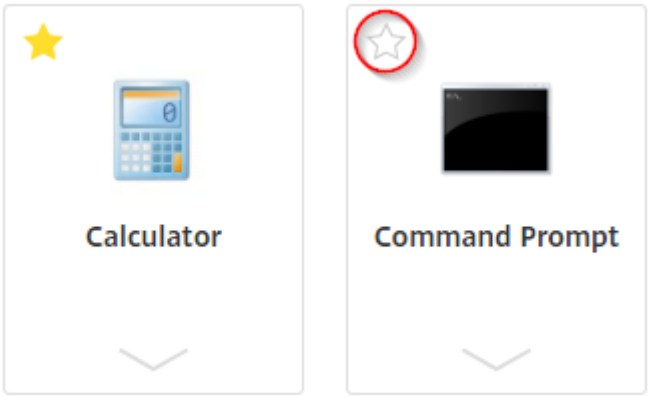
- **Alle** zeigt alle Desktops an.
- **Favoriten:** zeigt die Favoriten-Desktops an.

Kacheln für Apps und Desktops

Klicken Sie auf ein Symbol, um die App oder den Desktop zu starten.

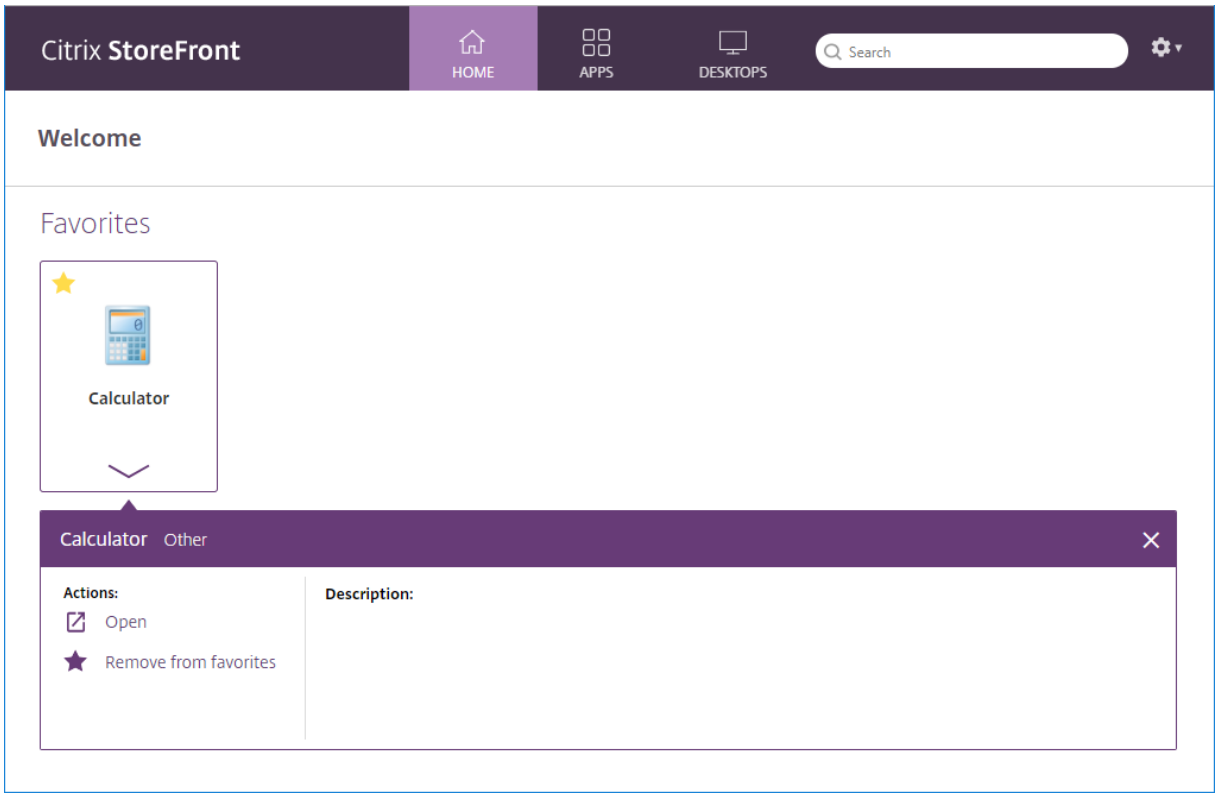
Favoriten

Klicken oder tippen Sie auf den Stern, um ein Element zu einem Favoriten zu machen:



Details und Aktionen anzeigen

Sie können ein Feld unter jedem Symbol öffnen, um die App-Beschreibung und die Aktionen anzuzeigen.



Die folgenden Aktionen sind ggf. verfügbar:

- **Öffnen** startet die App oder den Desktop bzw. stellt erneut eine Verbindung her.
- **Zu Favoriten hinzufügen:** Ist die Ressource weder Favorit noch obligatorisch und Favoriten sind für den Store aktiviert, wird sie zu den Favoriten hinzugefügt.

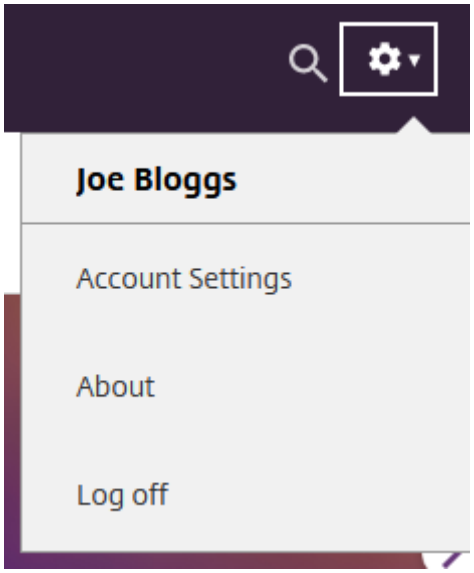
- **Aus Favoriten entfernen:** Ist die Ressource weder Favorit noch obligatorisch und Favoriten sind für den Store aktiviert, wird sie aus den Favoriten entfernt.
- **Neustart:** startet zugewiesene Desktops neu, bei denen ein Neustart verfügbar ist.

Suche

Klicken Sie auf das Lupensymbol, um das Suchfeld aufzurufen. Alle Apps, Desktops und Kategorien durchsuchen:

Einstellungen

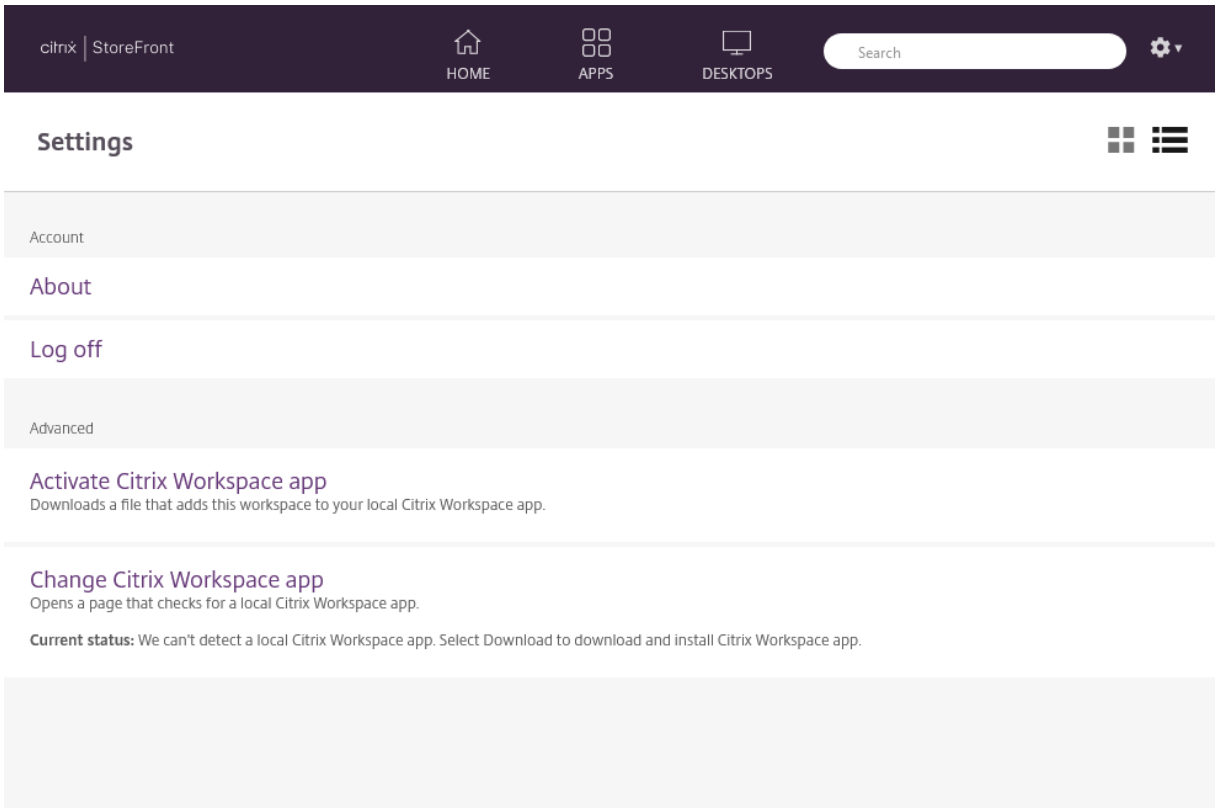
Das Einstellungsmenü ist nur verfügbar, wenn Sie über einen Webbrowser auf den Store zugreifen.



Das Einstellungsmenü enthält die folgenden Optionen:

- **Kontoeinstellungen** öffnet die Einstellungsseite.
- **Info** zeigt Informationen über die Anwendung an.
- **Abmelden** bewirkt die Abmeldung von der Website.

Kontoeinstellungen



Die folgenden Optionen sind möglicherweise verfügbar:

Verbinden. Setzt getrennte Sitzungen fort.

Trennen: Trennt aller aktuellen Sitzungen und meldet Sie ab.

Citrix Workspace-App aktivieren. Lädt eine Datei herunter, die diesen Store der lokalen Citrix Workspace-App hinzufügt.

Citrix Workspace-App ändern. Öffnet eine Seite, die nach einer lokal installierten Citrix Workspace-App sucht. So können Benutzer zwischen dem Starten von Ressourcen mit der lokal installierten Citrix Workspace-App und dem Starten der Ressourcen in einem Browser wechseln.

Abmelden

Öffnen Sie zum Abmelden das Einstellungsmenü und klicken Sie auf **Abmelden**. Dadurch erfolgt die Abmeldung vom Store. Wenn Sie mit Ressourcen verbunden sind, geschieht je nach Konfiguration Folgendes:

- Die Ressourcen werden beendet.
- Die Verbindung zu den Ressourcen wird getrennt.
- Die Verbindung zu den Ressourcen bleibt bestehen.

StoreFront SDK

April 17, 2024

Citrix StoreFront bietet ein SDK, das auf Modulen von Windows PowerShell Version 2.0 beruht. Mit dem SDK können Sie die gleichen Tasks wie mit der Citrix StoreFront-MMC-Konsole ausführen und darüber hinaus weitere Tasks, die mit der Konsole allein nicht möglich sind.

> **Hinweis:**
>
> Das PowerShell SDK ist nicht mit PowerShell 6 oder höher kompatibel.

Die SDK-Referenz finden Sie unter StoreFront SDK.

Verwenden des SDKs

Das SDK enthält mehrere PowerShell-Snap-Ins, die automatisch vom Installationsassistenten installiert werden, wenn Sie verschiedene StoreFront-Komponenten installieren und konfigurieren.

Zugreifen auf die Cmdlets:

1. Starten Sie eine PowerShell-Eingabeaufforderung oder **Windows PowerShell ISE** als Administrator.

   Zum Ausführen der Shell bzw. des Skripts müssen Sie als Mitglied der lokalen Administratorgruppe auf dem StoreFront-Server angemeldet sein.

2. Legen Sie die Ausführungsrichtlinie in PowerShell fest, um SDK-Cmdlets in Skripts zu verwenden.

   Weitere Informationen zur PowerShell-Ausführungsrichtlinie finden Sie in der Dokumentation von Microsoft.

3. Fügen Sie mit dem Befehl **Add -Module** in der Windows PowerShell-Konsole die Module hinzu, die Sie in der PowerShell-Umgebung benötigen. Geben Sie beispielsweise Folgendes ein:

   ```
   Import-Module Citrix.StoreFront
   ```

   Geben Sie Folgendes ein, um alle Cmdlets zu importieren:

   ```
   Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("
   Citrix.StoreFront")} | Import-Module
   ```

Nach dem Import haben Sie Zugriff auf die Cmdlets und die zugehörige Hilfe.

Erste Schritte mit dem SDK

Führen Sie folgende Schritte für das Erstellen eines Skripts aus:

1. Verwenden Sie eines der SDK-Beispiele, die zusammen mit StoreFront im Ordner **%Program-Files%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** installiert wurden.
2. Das Beispielsskript zeigt die Aufgaben der verschiedenen Teile und hilft Ihnen, Ihr eigenes Skript anzupassen. Weitere Informationen finden Sie im Beispiel eines Anwendungsfalls, in dem die Skriptaktionen ausführlich beschrieben werden.
3. Passen Sie die Beispielskripts für Ihre Zwecke an. Gehen Sie hierzu folgendermaßen vor:
    - Verwenden Sie die PowerShell-ISE oder ein ähnliches Tool zum Bearbeiten des Skripts.
    - Verwenden Sie Variablen für Werte, die wiederverwendet oder geändert werden sollen.
    - Entfernen Sie alle Befehle, die nicht erforderlich sind.
    - StoreFront-Cmdlets können mit dem Präfix "STF"gekennzeichnet werden.
    - Verwenden Sie das Cmdlet **Get-Help**, geben Sie den Cmdlet-Namen und den Parameter **-Full** an, um Informationen zu einem bestimmten Befehl aufzurufen.

Beispiele

> **Hinweis:**
>
> Um beim Erstellen eines Skripts sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den oben erläuterten Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Beispiele	Beschreibung
Erstellen einer einfachen Bereitstellung	Skript: erstellt eine einfache Bereitstellung mit einem StoreFront-Controller, der mit einem einzelnen XenDesktop-Server konfiguriert ist.
Erstellen einer Remotezugriffbereitstellung	Skript: erstellt eine Bereitstellung wie im vorherigen Skript plus Remotezugriff.
Erstellen einer Remotezugriffbereitstellung mit Gateway für den optimalen Start	Skript: erstellt eine Bereitstellung wie im vorherigen Skript und ermöglicht das Hinzufügen bevorzugter Gateways für den optimalen Start zur Verbesserung der Benutzererfahrung.

Beispiel: Erstellen einer einfachen Bereitstellung

Anhand des folgenden Beispiels wird die Erstellung einer einfachen Bereitstellung mit einem einzelnen XenDesktop-Controller erläutert.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die in Erste Schritte mit dem SDK aufgeführten Schritte ausführen. Das Beispiel kann unter Verwendung der beschriebenen Methoden zur Erstellung eines Skripts für die Automatisierung der StoreFront-Bereitstellung angepasst werden.

> **Hinweis:**
>
> Um sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den in diesem Dokument beschriebenen Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Inhalt des Skripts In diesem Abschnitt wird die Funktion jedes Teils des Skripts erläutert, das StoreFront erstellt. Dies hilft Ihnen bei der Anpassung des eigenen Skripts.

- Legt Fehlerbehandlungsanforderungen fest und importiert die erforderlichen StoreFront-Module. Importe sind in neueren Versionen von PowerShell nicht erforderlich.

```
1  Param(
2      [Parameter(Mandatory=$true)]
3      [Uri]$HostbaseUrl,
4      [long]$SiteId = 1,
5      [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox
           ")]
6      [string]$Farmtype = "XenDesktop",
7      [Parameter(Mandatory=$true)]
8      [string[]]$FarmServers,
9      [string]$StoreVirtualPath = "/Citrix/Store",
10     [bool]$LoadbalanceServers = $false,
11     [int]$Port = 80,
12     [int]$SSLRelayPort = 443,
13     [ValidateSet("HTTP","HTTPS","SSL")]
14     [string]$TransportType = "HTTP"
15     )
16     # Import StoreFront modules. Required for versions of
           PowerShell earlier than 3.0 that do not support
           autoloading
17     Import-Module Citrix.StoreFront
18     Import-Module Citrix.StoreFront.Stores
19     Import-Module Citrix.StoreFront.Authentication
20     Import-Module Citrix.StoreFront.WebReceiver
21 <!--NeedCopy-->
```

- Automatisiert den virtuellen Pfad der Authentifizierungs- und Citrix Receiver für Web-Dienste basierend auf dem angegebenen **$StoreVirtualPath**. **$StoreVirtualPath** entspricht **$StoreI-**

ISpath, da Virtuelle Pfade immer der Pfad in IIS sind. Daher haben sie in Powershell einen Wert wie "/Citrix/Store", "/Citrix/StoreWeb"oder "/Citrix/StoreAuth".

```
# Determine the Authentication and Receiver virtual path to use
    based of the Store
$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
<!--NeedCopy-->
```

- Erstellt eine neue Bereitstellung, sofern es noch keine gibt, zur Vorbereitung auf das Hinzufügen der erforderlichen StoreFront-Dienste. **-Confirm:$false** unterdrückt die Anforderung einer Bestätigung zum Fortfahren der Bereitstellung.

```
# Determine if the deployment already exists
$existingDeployment = Get-STFDeployment
if(-not $existingDeployment)
{

    # Install the required StoreFront components
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
        Confirm:$false
 }

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{

    # The deployment exists but it is configured to the desired
        hostbase url
    Write-Output "A deployment has already been created with the
        specified hostbase url on this server and will be used."
 }

else
{

    Write-Error "A deployment has already been created on this
        server with a different host base url."
 }

<!--NeedCopy-->
```

- Erstellt, sofern noch nicht vorhanden, einen neuen Authentifizierungsdienst an dem angegebenen virtuellen Pfad. Die Standardauthentifizierungsmethode mit Benutzernamen und Kennwort ist aktiviert.

```
# Determine if the authentication service at the specified
    virtual path exists
$authentication = Get-STFAuthenticationService -VirtualPath
    $authenticationVirtualPath
if(-not $authentication)
{

```



```
6       # Add an Authentication service using the IIS path of the
            Store appended with Auth
7       $authentication = Add-STFAuthenticationService
            $authenticationVirtualPath
8    }
9
10   else
11   {
12
13      Write-Output "An Authentication service already exists at the
             specified virtual path and will be used."
14   }
15
16   <!--NeedCopy-->
```

- Erstellt einen neuen Storedienst mit einem XenDesktop-Controller und mit im Array **$XenDesktopServers** definierten Servern an dem angegebenen Pfad, sofern noch nicht vorhanden.

```
1    # Determine if the store service at the specified virtual path
        exists
2    $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3    if(-not $store)
4    {
5
6    # Add a Store that uses the new Authentication service configured
         to publish resources from the supplied servers
7    $store = Add-STFStoreService -VirtualPath $StoreVirtualPath -
        AuthenticationService $authentication -FarmName $Farmtype -
        FarmType $Farmtype -Servers $FarmServers -LoadBalance
        $LoadbalanceServers `
8            -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
                $TransportType
9    }
10
11   else
12   {
13
14      Write-Output "A Store service already exists at the specified
             virtual path and will be used. Farm and servers will be
            appended to this store."
15      # Get the number of farms configured in the store
16      $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.
            Count
17      # Append the farm to the store with a unique name
18      Add-STFStoreFarm -StoreService $store -FarmName "Controller$(
            $farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
             -LoadBalance $LoadbalanceServers -Port $Port `
19           -SSLRelayPort $SSLRelayPort -TransportType $TransportType
20   }
21
22   <!--NeedCopy-->
```

- Fügt einen Citrix Receiver für Web-Dienst an dem angegebenen virtuellen IIS-Pfad ein für den

Zugriff auf Anwendungen, die in dem oben erstellten Store veröffentlicht wurden.

```
# Determine if the receiver service at the specified virtual path
    exists
$receiver = Get-STFWebReceiverService -VirtualPath
   $receiverVirtualPath
if(-not $receiver)
{

    # Add a Receiver for Web site so users can access the
       applications and desktops in the published in the Store
    $receiver = Add-STFWebReceiverService -VirtualPath
       $receiverVirtualPath -StoreService $store
 }

else
{

    Write-Output "A Web Receiver service already exists at the
       specified virtual path and will be used."
 }

<!--NeedCopy-->
```

- Aktiviert XenApp-Dienste für den Store, damit ältere Citrix Receiver-/Citrix Workspace-App-Clients eine Verbindung mit veröffentlichten Anwendungen herstellen können.

```
# Determine if PNA is configured for the Store service
$storePnaSettings = Get-STFStorePna -StoreService $store
if(-not $storePnaSettings.PnaEnabled)
{

# Enable XenApp services on the store and make it the default for
    this server
Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
   -DefaultPnaService
 }

<!--NeedCopy-->
```

Beispiel: Erstellen einer Remotezugriffbereitstellung

Das folgende, auf dem vorherigen Skript aufbauende Beispiel dient zum Erstellen einer Bereitstellung mit Remotezugriff.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die in Erste Schritte mit dem SDK aufgeführten Schritte ausführen. Das Beispiel kann unter Verwendung der beschriebenen Methoden zur Erstellung eines Skripts für die Automatisierung der StoreFront-Bereitstellung angepasst werden.

> **Hinweis:**
>
> Um sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den in diesem Dokument beschriebenen Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Inhalt des Skripts In diesem Abschnitt wird die Funktion jedes Teils des Skripts erläutert, das StoreFront erstellt. Dies hilft Ihnen bei der Anpassung des eigenen Skripts.

- Legt Fehlerbehandlungsanforderungen fest und importiert die erforderlichen StoreFront-Module. Importe sind in neueren Versionen von PowerShell nicht erforderlich.

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [Parameter(Mandatory=$true)]
    [long]$SiteId = 1,
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName
)
Set-StrictMode -Version 2.0

# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Import StoreFront modules. Required for versions of PowerShell
   earlier than 3.0 that do not support autoloading
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
<!--NeedCopy-->
```

- Erstellt eine StoreFront-Bereitstellung mit internem Zugriff unter Aufruf des vorherigen Beispiel-

skripts. Die Basisbereitstellung wird um Unterstützung des Remotezugriffs erweitert.

```
# Create a simple deployment by invoking the SimpleDeployment
    example
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
    Definition -Parent
$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
    FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
    Farmtype $Farmtype `
     -LoadbalanceServers $LoadbalanceServers -Port $Port  -
        SSLRelayPort $SSLRelayPort -TransportType $TransportType
<!--NeedCopy-->
```

- Ruft die für die einfache Bereitstellung erstellten Dienste ab, da sie für die Unterstützung des Remotezugriffs aktualisiert werden müssen.

```
# Determine the Authentication and Receiver sites based on the
    Store
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$authentication = Get-STFAuthenticationService -StoreService
    $store
$receiverForWeb = Get-STFWebReceiverService -StoreService $store
<!--NeedCopy-->
```

- Aktiviert CitrixAGBasic in dem für Remotezugriff mit Citrix Gateway erforderlichen Citrix Receiver für Web-Dienst. Ruft die Citrix Receiver für Web CitrixAGBasic- und die ExplicitForms-Authentifizierungsmethode von den unterstützten Protokollen ab.

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms
    authentication method from the supported protocols
# Included for demonstration purposes as the protocol name can be
    used directly if known
$receiverMethods = Get-
    STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
 $_ -match "Explicit" -or $_ -match "CitrixAG"  }

# Enable CitrixAGBasic in Receiver for Web (required for remote
    access)
Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
    $receiverMethods
<!--NeedCopy-->
```

- Aktiviert CitrixAGBasic für den Authentifizierungsdienst. Dies ist für den Remotezugriff erforderlich.

```
# Get the CitrixAGBasic authentication method from the protocols
    installed.
# Included for demonstration purposes as the protocol name can be
    used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-
    Object {
```



```
 $_ -match "CitrixAGBasic"  }

# Enable CitrixAGBasic in the Authentication service (required
    for remote access)
Enable-STFAuthenticationServiceProtocol -AuthenticationService
    $authentication -Name $citrixAGBasic
<!--NeedCopy-->
```

- Fügt ein neues Remotezugriffsgateway hinzu sowie die optionale Subnetz-IP-Adresse, falls diese angegeben wird, und registriert es bei dem Store für den Remotezugriff.

```
# Add a new Gateway used to access the new store remotely
Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
    Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
    $GatewaySTAUrls
# Get the new Gateway from the configuration (Add-
    STFRoamingGateway will return the new Gateway if -PassThru is
    supplied as a parameter)
$gateway = Get-STFRoamingGateway -Name $GatewayName
# If the gateway subnet was provided then set it on the gateway
    object
if($GatewaySubnetIP)
{

    Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
        $GatewaySubnetIP
 }

# Register the Gateway with the new Store
Register-STFStoreGateway -Gateway $gateway -StoreService $store -
    DefaultGateway
<!--NeedCopy-->
```

Beispiel: Erstellen einer Remotezugriffbereitstellung mit Gateway für den optimalen Start

Das folgende, auf dem vorherigen Skript aufbauende Beispiel dient zum Erstellen einer Bereitstellung mit Remotezugriff und Gateway für den optimalen Start.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die in Erste Schritte mit dem SDK aufgeführten Schritte ausführen. Das Beispiel kann unter Verwendung der beschriebenen Methoden zur Erstellung eines Skripts für die Automatisierung der StoreFront-Bereitstellung angepasst werden.

> **Hinweis:**
>
> Um sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den in diesem Dokument beschriebenen Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Inhalt des Skripts In diesem Abschnitt wird die Funktion jedes Teils des Skripts erläutert, das StoreFront erstellt. Dies hilft Ihnen bei der Anpassung des eigenen Skripts.

- Legt Fehlerbehandlungsanforderungen fest und importiert die erforderlichen StoreFront-Module. Importe sind in neueren Versionen von PowerShell nicht erforderlich.

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Import StoreFront modules. Required for versions of PowerShell
   earlier than 3.0 that do not support autoloading
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
<!--NeedCopy-->
```

- Ruft das Skript zur Erstellung einer Remotezugriffbereitstellung zum Konfigurieren der einfachen Bereitstellung mit Remotezugriff auf.

```
# Create a remote access deployment
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
```



```
    Definition -Parent
$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
    ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
    FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
    Farmtype $Farmtype `
     -LoadbalanceServers $LoadbalanceServers -Port $Port  -
        SSLRelayPort $SSLRelayPort -TransportType $TransportType `
     -GatewayUrl $GatewayUrl -GatewayCallbackUrl
        $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
        GatewayName $GatewayName
<!--NeedCopy-->
```

- Fügt das bevorzugte Gateway für den optimalen Start hinzu und ruft es aus der Liste der konfigurierten Gateways ab.

```
# Add a new Gateway used for remote HDX access to desktops and
    apps
$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -
    LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -
    SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
<!--NeedCopy-->
```

- Bewirkt, dass der Storedienst das optimale Gateway verwendet und es für Startvorgänge aus der angegebenen Farm registriert.

```
# Get the Store configured by SimpleDeployment.ps1
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
# Register the Gateway with the new Store for launch against all
    of the farms (currently just one)
$farmNames = @($store.FarmsConfiguration.Farms | foreach {
 $_.FarmName  }
)
Register-STFStoreOptimalLaunchGateway -Gateway $gateway -
    StoreService $store -FarmName $farmNames
<!--NeedCopy-->
```

Problembehandlung bei StoreFront

April 17, 2024

Installationsprotokolle

Wenn StoreFront installiert oder deinstalliert wird, werden die folgenden Protokolldateien vom StoreFront-Installationsprogramm im Verzeichnis *C:\Windows\Temp\StoreFront* erstellt. Die Dateinamen lassen die Komponenten erkennen, die sie erstellt haben, und enthalten einen Zeitstempel.

- Citrix-DeliveryServicesRoleManager-*.log: wird bei der interaktiven Installation von StoreFront erstellt.
- Citrix-DeliveryServicesSetupConsole-*.log: wird bei der Installation von StoreFront ohne Benutzereingriffe und bei Deinstallation mit oder ohne Benutzereingriffe erstellt.
- CitrixMsi-CitrixStoreFront-x64-*.log: wird bei der Installation und Deinstallation von StoreFront mit oder ohne Benutzereingriffe erstellt.

Ereignisprotokolle

StoreFront unterstützt die Windows-Ereignisprotokollierung für den Authentifizierungsdienst, Stores und Receiver für Web-Sites. Alle generierten Ereignisse werden in das StoreFront-Anwendungsprotokoll geschrieben, das über die Ereignisanzeige unter **Anwendungs- und Dienstprotokolle > Citrix Delivery Services** oder **Windows-Protokolle > Anwendung** angezeigt werden kann. Sie können die Anzahl der doppelten Protokolleinträge für ein einzelnes Ereignis steuern, indem Sie die Konfigurationsdateien für den Authentifizierungsdienst, die Stores und Receiver für Web-Sites bearbeiten.

Protokolldrosselung

1. Öffnen Sie die Datei *web.config* für den Authentifizierungsdienst, Store oder die Receiver für Web-Site mit einem Texteditor. Die Dateien sind normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\Authentication, C:\inetpub\wwwroot\Citrix\storename und C:\inetpub\wwwroot\Citrix\storenameWeb\, wobei "storename"für den Namen steht, der beim Erstellen des Stores angegeben wurde.
2. Suchen Sie das folgende Element in der Datei.

   ```
   <logger duplicateInterval="00:01:00"duplicateLimit="10">
   ```

   Standardmäßig wird in der Konfiguration von StoreFront die Anzahl der doppelten Protokolleinträge auf 10 pro Minute beschränkt.
3. Ändern Sie den Wert des Attributs duplicateInterval, um den Zeitraum, in dem doppelte Protokolleinträge überwacht werden, in Stunden, Minuten und Sekunden festzulegen. Legen Sie mit dem Attribut duplicateLimit fest, wie viele doppelte Einträge im angegebenen Zeitraum protokolliert werden müssen, um die Protokolldrosselung auszulösen.

Wenn die Protokolldrosselung ausgelöst wird, wird eine Warnmeldung aufgezeichnet, um anzugeben, dass weitere identische Protokolleinträge unterdrückt werden. Nach Ablauf des Zeitraums wird die normale Protokollierung fortgesetzt und es wird eine Informationsmeldung aufgezeichnet, die angibt, dass doppelte Protokolleinträge nicht mehr unterdrückt werden.

PowerShell- und Verwaltungskonsolenprotokolle

Konfigurationsänderungen, die über PowerShell oder die Verwaltungskonsole vorgenommen wurden, werden in `C:\Program Files\Citrix\Receiver StoreFront\Admin\logs` protokolliert. Die Protokolldateinamen enthalten Befehlsaktionen und Themen sowie einen Zeitstempel, anhand derer zwischen den Befehlssequenzen unterschieden werden kann.

Diagnoseprotokollierung

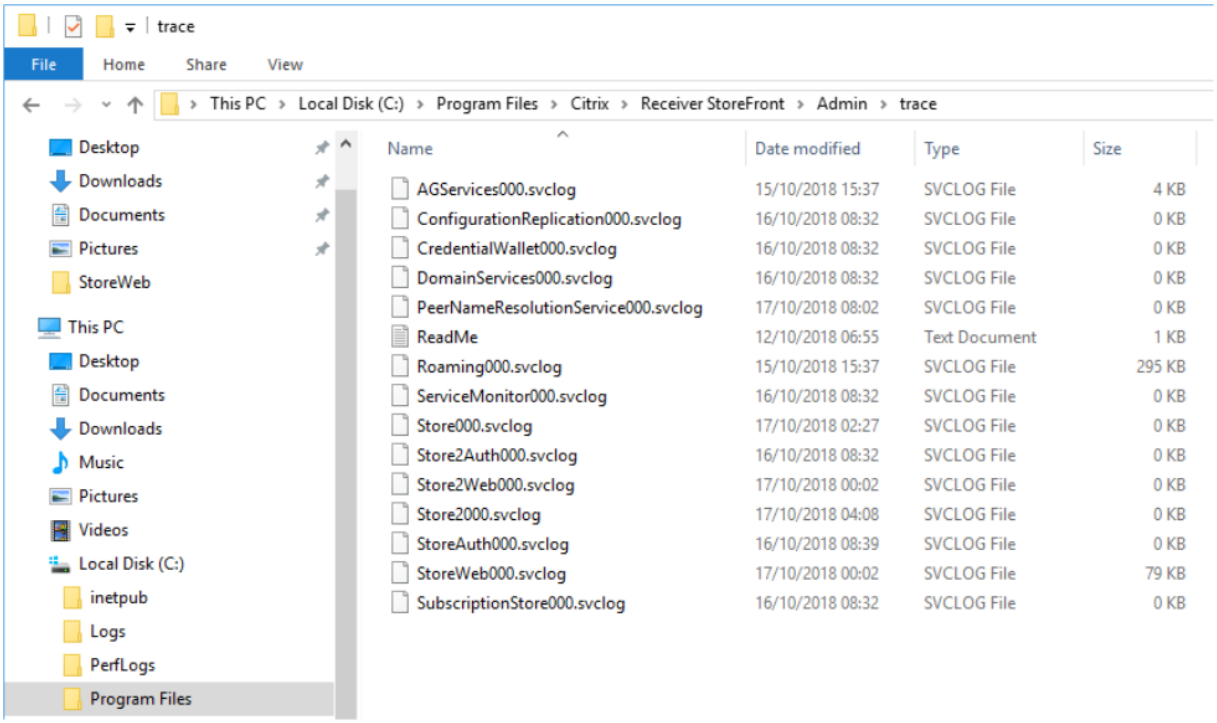
Standardmäßig werden für die Diagnose nur Fehler protokolliert. Um die Tracing-Protokollierung zu aktivieren, starten Sie Windows PowerShell mithilfe eines Kontos mit lokalen Administratorberechtigungen und verwenden Sie den Befehl `Set-STFDiagnostics` mit den folgenden Parametern:

- **-All**. Ein Flag, das angibt, dass die Ablaufverfolgung für alle Instanzen und Dienste aktualisiert werden soll.
- **-TraceLevel**. In aufsteigender Detaildichte sind die zulässige Werte für "-TraceLevel": Off, Error, Warning, Info, Verbose. Aufgrund der großen Datenmenge, die generiert werden kann, kann die Ablaufverfolgung die Leistung von StoreFront erheblich beeinträchtigen. "Info"oder "Verbose" werden nicht empfohlen, es sei denn, sie sind speziell für die Problembehandlung erforderlich.

Optionale Parameter:

- **-FileSizeKb**. Die Größe der Ablaufverfolgungsdatei in KB.
- **-FileCount**. Die Anzahl der Ablaufverfolgungsdateien, die gleichzeitig auf dem Datenträger verwaltet werden sollen.
- **-confirm:$False**. Unterdrückt Windows-Aufforderungen, damit das Cmdlet StoreFront jedes Mal ausgeführt werden kann.

Die Tracing-Ausgabe wird an `c:\Program Files\Citrix\Receiver StoreFront\admin\trace` gesendet.



Beispiele

Aktivieren der Ablaufverfolgung mit der Stufe “Verbose”für alle Dienste für das Debugging:

```
Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
<!--NeedCopy-->
```

Deaktivieren der Ablaufverfolgung mit der Stufe “Verbose”und Zurücksetzen der Ablaufverfolgung auf den Standardwert für alle Dienste:

```
Set-STFDiagnostics -All -TraceLevel "Error" -confirm:$False
<!--NeedCopy-->
```

Weitere Informationen zum Cmdlet Set-STFDiagnostics finden Sie in der Dokumentation zum StoreFront PowerShell SDK.

Protokollierung der Launch.ica-Datei

Wenn ein Benutzer eine App oder einen Desktop startet, generiert StoreFront eine Datei namens “launch.ica”, anhand derer die Workspace-App ermittelt, wie eine Verbindung mit der App oder dem Desktop hergestellt werden soll. Je nach Konfiguration wird diese Datei evtl. im Arbeitsspeicher abgelegt und ist nicht direkt zugänglich. Um Startfehler zu diagnostizieren, kann es nützlich sein, sich den Inhalt von launch.ica anzusehen.

Führen Sie die folgenden Schritte aus, um die Protokollierung der Datei launch.ica zu aktivieren:

1. Navigieren Sie mit dem Registrierungs-Editor zum folgenden Registrierungsschlüssel:

   32-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

   64-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. Legen Sie die folgenden Zeichenfolgenwert fest:

   - LogFile=”Pfad zur Protokolldatei”
   - LogICAFile=true

   Beispiel:

```
LogFile=C:\ica\ica.log
LogICAFile=true
<!--NeedCopy-->
```

> Hinweis:
>
> Die Verwendung einer ICA-Datei in Ihrer Umgebung für andere Zwecke als die Problembehandlung wird in CTX200126näher erläutert.

Hinweise zu Drittanbietern

February 28, 2024

StoreFront kann Softwarekomponenten von Drittanbietern enthalten, für die die folgenden Lizenzbedingungen gelten: Diese Liste gilt zu dem angegebenen Datum korrekt. Diese Liste kann sich im Zusammenhang mit bestimmten Versionen des Produkts ändern und ist möglicherweise nicht vollständig. IN DEM NACH DEM ANWENDBAREN RECHT ZULÄSSIGEN UMFANG GEBEN CITRIX UND SEINE LIEFERANTEN KEINE AUSDRÜCKLICHE ODER STILLSCHWEIGENDEN ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN BEZÜGLICH DER LISTE, DEREN RICHTIGKEIT ODER VOLLSTÄNDIGKEIT ODER DEN AUS DER NUTZUNG ODER VERTEILUNG DER LISTE ERGEHENDEN FOLGEN. DURCH NUTZUNG ODER VERTEILUNG DER LISTE STIMMEN SIE ZU, DASS CITRIX UNTER KEINEN UMSTÄNDEN FÜR SPEZIELLE, DIREKTE, INDIREKTE, ODER FOLGESCHÄDEN ODER JEGLICHE ANDEREN SCHÄDEN HAFTET, DIE AUS DER NUTZUNG ODER VERTEILUNG DIESER LISTE ERWACHSEN.

Castle Windsor 3.3.0

Copyright 2004–2013 Castle Project –http://www.castleproject.org/

Lizenziert unter Apache License, Version 2.0

Microsoft Unity Application Block (Unity) 2.1

Copyright © 2011 Microsoft Corporation.

Lizenziert unter Microsoft Public License (Ms-PL) https://msdn.microsoft.com/en-us/library/hh237493.aspx

Microsoft Patterns and Practices: Prism 2.2

Copyright © 2010 Microsoft Corporation.

Lizenziert unter Microsoft Public License (Ms-PL) http://compositewpf.codeplex.com/releases/view/46046

Microsoft patterns & practices: Common Service Locator 1.0

Copyright © Microsoft Corporation.

Lizenziert unter Microsoft Public License (MS-PL)

Microsoft .Net-Referenz

Copyright © Microsoft Corporation. Lizenziert unter MIT-Lizenz.

ManagedEsent Release 1.9.4

Copyright © Microsoft Corporation.

Lizenziert unter Microsoft Public License (Ms-PL) http://managedesent.codeplex.com/license

jQuery UI - v1.10.4 - 2014-03-12

http://jqueryui.com/

Copyright 2014 jQuery Foundation und andere Mitwirkende; MIT-Lizenz

jQuery JavaScript Library v1.12.4

http://jquery.com/

Beinhaltet Sizzle.js

http://sizzlejs.com/

Copyright jQuery Foundation und andere Mitwirkende

Veröffentlicht unter der MIT-Lizenz

http://jquery.org/license

Datum: 2016-05-20T17:17Z

jQuery jScrollPane v2.0.0beta11

jScrollPane - v2.0.0beta11 - 2011-07-04 http://jscrollpane.kelvinluck.com/

Copyright (c) 2010 Kelvin Luck

Duale Lizenz unter MIT und GPL.

jquery.contextmenu.js

jQuery-Plug-In für Kontextmenüs

http://www.JavascriptToolbox.com/lib/contextmenu

Copyright (c) 2008 Matt Kruse (javascripttoolbox.com)

Duale Lizenz unter MIT und GPL.

jQuery-Plug-In für Hammer.JS - v1.0.0 - 02.01.2014

http://eightmedia.github.com/hammer.js

Copyright (c) 2014 Jorik Tangelder j.tangelder@gmail.com;

Lizenziert unter MIT-Lizenz

jQuery MouseWheel

Copyright (c) 2011 Brandon Aaron (http://brandonaaron.net)

Lizenziert unter MIT-Lizenz (LICENSE.txt).

WPF-Toolkit 3.5

WPF Toolkit (http://wpf.codeplex.com/) Copyright (c) 2006-2014 Microsoft

Ms-PL-Lizenz http://wpf.codeplex.com/license

Extended WPF Toolkit 3.0

Copyright (C) 2007-2013 Xceed Software Inc.

Dieses Programm wird Ihnen unter den Bedingungen der Microsoft Public License (Ms-PL) zur Verfügung gestellt (siehe http://wpftoolkit.codeplex.com/license).

Für mehr Features, Steuerelemente und schnellen professionellen Support holen Sie sich die Plus Edition auf http://xceed.com/wpf_toolkit.

Bleiben Sie auf dem Laufenden: folgen Sie @datagrid auf Twitter oder http://facebook.com/datagrids.

WiX Toolset

Copyright (c) Outercurve Foundation. Common Public License Version 1.0.

CLR Security

Copyright (c) Microsoft Corporation. Microsoft Limited Permissive License (Ms-LPL)

Stack Exchange Redis 1.1

StackExchange.Redis.StrongName 1.1 https://stackexchange.github.io/StackExchange.Redis Copyright (c) 2014 Stack Exchange

Lizenziert unter MIT-Lizenz

Newtonsoft JSON 9.0

Copyright (c) 2007 James Newton-King

Lizenziert unter MIT-Lizenz.

jQuery JavaScript Library v3.7.1

https://jquery.com/

Copyright OpenJS Foundation und andere Mitwirkende

Veröffentlicht unter der MIT-Lizenz

https://jquery.org/license

Datum: 2023-08-28T13:37Z

jQuery UI - v1.13.2 -2022 -07-14

http://jqueryui.com

Copyright jQuery Foundation und andere Mitwirkende; MIT-lizenziert

Hammer.JS - v2.0.4 - 2014-09-28

Hammer.JS - v2.0.8 - 2016-04-23

http://hammerjs.github.io/

Copyright (c) 2016 Jorik Tangelder;

Lizenziert unter MIT-Lizenz

VelocityJS.org (1.5.0)

velocity-animate (C) 2014-2017 Julian Shapiro.

Lizenziert unter MIT-Lizenz. Einzelheiten siehe Datei LICENSE im Projektstamm.

slick.js - 1.8.0

MIT-Lizenz (MIT)

Copyright (c) 2013-2016

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furfero

Duale Lizenzierung unter MIT- oder GPL Version 2-Lizenz.

ANHANG: Aufgeführte Lizenzen

MIT-Lizenz

```
Permission is hereby granted, free of charge, to any person obtaining a
    copy
of this software and associated documentation files (the "Software"),
    to deal
in the Software without restriction, including without limitation the
    rights
```



```
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
<!--NeedCopy-->
```

Apache License, Version 2.0

```
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/


TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction,
   and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by
   the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all
   other entities that control, are controlled by, or are under common
   control with that entity. For the purposes of this definition,
   "control" means (i) the power, direct or indirect, to cause the
   direction or management of such entity, whether by contract or
   otherwise, or (ii) ownership of fifty percent (50%) or more of the
   outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity
   exercising permissions granted by this License.
```



```
26
27      "Source" form shall mean the preferred form for making modifications
            ,
28      including but not limited to software source code, documentation
29      source, and configuration files.
30
31      "Object" form shall mean any form resulting from mechanical
32      transformation or translation of a Source form, including but
33      not limited to compiled object code, generated documentation,
34      and conversions to other media types.
35
36      "Work" shall mean the work of authorship, whether in Source or
37      Object form, made available under the License, as indicated by a
38      copyright notice that is included in or attached to the work
39      (an example is provided in the Appendix below).
40
41      "Derivative Works" shall mean any work, whether in Source or Object
42      form, that is based on (or derived from) the Work and for which the
43      editorial revisions, annotations, elaborations, or other
            modifications
44      represent, as a whole, an original work of authorship. For the
            purposes
45      of this License, Derivative Works shall not include works that
            remain
46      separable from, or merely link (or bind by name) to the interfaces
            of,
47      the Work and Derivative Works thereof.
48
49      "Contribution" shall mean any work of authorship, including
50      the original version of the Work and any modifications or additions
51      to that Work or Derivative Works thereof, that is intentionally
52      submitted to Licensor for inclusion in the Work by the copyright
            owner
53      or by an individual or Legal Entity authorized to submit on behalf
            of
54      the copyright owner. For the purposes of this definition, "submitted
            "
55      means any form of electronic, verbal, or written communication sent
56      to the Licensor or its representatives, including but not limited to
57      communication on electronic mailing lists, source code control
            systems,
58      and issue tracking systems that are managed by, or on behalf of, the
59      Licensor for the purpose of discussing and improving the Work, but
60      excluding communication that is conspicuously marked or otherwise
61      designated in writing by the copyright owner as "Not a Contribution.
            "
62
63      "Contributor" shall mean Licensor and any individual or Legal Entity
64      on behalf of whom a Contribution has been received by Licensor and
65      subsequently incorporated within the Work.
66
67  2. Grant of Copyright License. Subject to the terms and conditions of
68     this License, each Contributor hereby grants to You a perpetual,
```



```
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   copyright license to reproduce, prepare Derivative Works of,
   publicly display, publicly perform, sublicense, and distribute the
   Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   (except as stated in this section) patent license to make, have made
      ,
   use, offer to sell, sell, import, and otherwise transfer the Work,
   where such license applies only to those patent claims licensable
   by such Contributor that are necessarily infringed by their
   Contribution(s) alone or by combination of their Contribution(s)
   with the Work to which such Contribution(s) was submitted. If You
   institute patent litigation against any entity (including a
   cross-claim or counterclaim in a lawsuit) alleging that the Work
   or a Contribution incorporated within the Work constitutes direct
   or contributory patent infringement, then any patent licenses
   granted to You under this License for that Work shall terminate
   as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
       do not modify the License. You may add Your own attribution
       notices within Derivative Works that You distribute, alongside
       or as an addendum to the NOTICE text from the Work, provided
```



```
121         that such additional attribution notices cannot be construed
122         as modifying the License.
123
124     You may add Your own copyright statement to Your modifications and
125     may provide additional or different license terms and conditions
126     for use, reproduction, or distribution of Your modifications, or
127     for any such Derivative Works as a whole, provided Your use,
128     reproduction, and distribution of the Work otherwise complies with
129     the conditions stated in this License.
130
131  5. Submission of Contributions. Unless You explicitly state otherwise,
132     any Contribution intentionally submitted for inclusion in the Work
133     by You to the Licensor shall be under the terms and conditions of
134     this License, without any additional terms or conditions.
135     Notwithstanding the above, nothing herein shall supersede or modify
136     the terms of any separate license agreement you may have executed
137     with Licensor regarding such Contributions.
138
139  6. Trademarks. This License does not grant permission to use the trade
140     names, trademarks, service marks, or product names of the Licensor,
141     except as required for reasonable and customary use in describing
           the
142     origin of the Work and reproducing the content of the NOTICE file.
143
144  7. Disclaimer of Warranty. Unless required by applicable law or
145     agreed to in writing, Licensor provides the Work (and each
146     Contributor provides its Contributions) on an "AS IS" BASIS,
147     WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
148     implied, including, without limitation, any warranties or conditions
149     of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
150     PARTICULAR PURPOSE. You are solely responsible for determining the
151     appropriateness of using or redistributing the Work and assume any
152     risks associated with Your exercise of permissions under this
           License.
153
154  8. Limitation of Liability. In no event and under no legal theory,
155     whether in tort (including negligence), contract, or otherwise,
156     unless required by applicable law (such as deliberate and grossly
157     negligent acts) or agreed to in writing, shall any Contributor be
158     liable to You for damages, including any direct, indirect, special,
159     incidental, or consequential damages of any character arising as a
160     result of this License or out of the use or inability to use the
161     Work (including but not limited to damages for loss of goodwill,
162     work stoppage, computer failure or malfunction, or any and all
163     other commercial damages or losses), even if such Contributor
164     has been advised of the possibility of such damages.
165
166  9. Accepting Warranty or Additional Liability. While redistributing
167     the Work or Derivative Works thereof, You may choose to offer,
168     and charge a fee for, acceptance of support, warranty, indemnity,
169     or other liability obligations and/or rights consistent with this
170     License. However, in accepting such obligations, You may act only
171     on Your own behalf and on Your sole responsibility, not on behalf
```



```
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS
<!--NeedCopy-->
```

Microsoft Public License (Ms-PL)

```
This license governs use of the accompanying software. If you use the
    software, you accept this license. If you do not accept the license,
     do not use the software.

1. Definitions
The terms "reproduce," "reproduction," "derivative works," and "
    distribution" have the
same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or
    changes to the software.

A "contributor" is any person that distributes its contribution under
     this license.

"Licensed patents" are a contributor's patent claims that read
    directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including
    the license conditions and limitations in section 3, each
    contributor grants you a non-exclusive, worldwide, royalty-free
    copyright license to reproduce its contribution, prepare derivative
    works of its contribution, and distribute its contribution or any
    derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the
    license conditions and limitations in section 3, each contributor
    grants you a non-exclusive, worldwide, royalty-free license under
    its licensed patents to make, have made, use, sell, offer for sale,
    import, and/or otherwise dispose of its contribution in the software
     or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use
     any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents
    that you claim are infringed by the software, your patent license
```



```
    from such contributor to the software ends automatically.
24
25  (C) If you distribute any portion of the software, you must retain all
    copyright, patent, trademark, and attribution notices that are
    present in the software.
26
27  (D) If you distribute any portion of the software in source code form,
    you may do so only under this license by including a complete copy
    of this license with your distribution. If you distribute any
    portion of the software in compiled or object code form, you may
    only do so under a license that complies with this license.
28
29  (E) The software is licensed “as-is.” You bear the risk of using it.
    The contributors give no express warranties, guarantees or
    conditions. You may have additional consumer rights under your local
     laws which this license cannot change. To the extent permitted
    under your local laws, the contributors exclude the implied
    warranties of merchantability, fitness for a particular purpose and
    non-infringement.
30  <!--NeedCopy-->
```