StoreFront 2507 Long Term Service Release – Übersicht

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

StoreFront wird auf Servern in Ihrem Netzwerk bereitgestellt. Informationen zum von Citrix verwalteten Dienst finden Sie unter Citrix® StoreFront Cloud.

In StoreFront können Sie einen oder mehrere Stores konfigurieren. Jeder Store verfügt über eine eigene Konfiguration, einschließlich:

- Der Authentifizierungsmethoden, die Benutzer zum Anmelden verwenden.
- Der Liste der Sites, die StoreFront abfragt, um die dem Benutzer zur Verfügung stehenden Ressourcen aufzulisten.
- Des Aussehens des Stores.
- Ob ein Store über ein NetScaler Gateway remote zugänglich ist.

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

Um zu beginnen, planen Sie Ihre StoreFront-Bereitstellung, zeigen Sie die Systemanforderungen an und installieren Sie StoreFront.

Was ist neu

Erfahren Sie mehr über die neuen Funktionen, behobenen Probleme und bekannten Probleme in dieser Version über die folgenden Links.

Neuerungen

Frühere Versionen

Weitere Informationen zu früheren Versionen finden Sie hier.

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

Support-Lebenszyklus

Die Produktlebenszyklusstrategie für StoreFront Current Releases (CR) und Long Term Service Releases (LTSR) wird in Lifecycle Milestones beschrieben. Zusätzliche Lebenszyklusinformationen für StoreFront finden Sie unter CTX200356.

Was ist neu

Die 2507 LTSR umfasst die folgenden Releases.

- 2507 LTSR CU2
- 2507 LTSR CU1
- 2507 Erstveröffentlichung

Kumulatives Update 2 (CU2)

Veröffentlichungsdatum: August 18, 2026

Informationen zu diesem Release

Um mehr über Citrix Product Subscription Advantage Eligibility Dates zu erfahren, klicken Sie auf den Link.

Citrix Workspace-App für HTML5

Diese Version enthält Citrix Workspace app for HTML5 2603.10.

Neuerungen in 2507 LTSR CU2

Cumulative Update 2 (CU2) ist die neueste Version von StoreFront 2507 LTSR. Siehe Neuerungen.

Diese Version enthält Korrekturen für StoreFront 2507 LTSR Cumulative Update 2 (CU2). Die folgenden Probleme wurden seitdem gemeldet.

Behobene Probleme in 2507 LTSR CU2

StoreFront 2507 LTSR CU2 enthält die folgenden Korrekturen:

- Wenn StoreFront in Citrix Analytics integriert wird, kann es zu einer erheblich erhöhten CPU-Auslastung kommen.
- Wenn ein Administrator in der Verwaltungskonsole die Benutzeroberfläche ändert und dann **Abbrechen** auswählt, wird die Änderung trotzdem in der Konsole gespeichert.

- Bei der Durchführung von Maschinensteuerungsaktionen übergibt StoreFront den Clientnamen und die Adresse nicht an den DDC, wodurch diese in den Protokolldateien fehlen.
- Die StoreFront-Verwaltungskonsole zeigt zuvor hochgeladene Logos nicht an.
- Der Hilfetext für PowerShell-Befehle zum Festlegen von Stilen ist irreführend.
- Downloads der Citrix Workspace-App werden erneut aktiviert, wenn Sie die Starteinstellungen ändern.
- Das Umbenennen einer Site löscht jegliches optimale HDX-Routing für diese Site.
- Auf der Registerkarte 'Darstellung der Verwaltungskonsole' funktioniert die Schaltfläche 'Auf Standard zurücksetzen' nicht.
- Der X-XSS-Protection-Header ist veraltet und sollte entfernt werden.
- Wenn StoreFront mit einem Citrix Gateway-Diensttyp konfiguriert ist, kann ein Upgrade auf StoreFront 2507 zu Startfehlern führen. In der Gateway-Konfiguration enthält die Registerkarte 'Cloud Connector' fälschlicherweise Port 8090, was StoreFront daran hindert, den Cloud Connector für STA-Ticketanfragen zu erreichen.

Bekannte Probleme in 2507 LTSR CU2

Es gibt keine neuen bekannten Probleme in Cumulative Update 2.

Kumulatives Update 1 (CU1)

Veröffentlichungsdatum: December 16, 2025

Informationen zu diesem Release

StoreFront (Erstveröffentlichung)

Wenn StoreFront bei Citrix Analytics integriert wurde, rät Citrix von der Installation dieser Version ab. Weitere Informationen finden Sie unter Bekannte Probleme.

Berechtigungsdaten für Citrix Product Subscription Advantage

Citrix Workspace-App für HTML5

Diese Version enthält Citrix Workspace-App für HTML5 2511.

Neuerungen in 2507 LTSR CU1

Kumulatives Update 1 (CU1) ist die neueste Version von StoreFront 2507 LTSR. Siehe Neuerungen.

Wenn Sie Ihre Server bei Citrix Analytics integriert haben, empfiehlt Citrix, diese Version nicht zu installieren. Weitere Informationen finden Sie unter Bekannte Probleme.

Ab der CU1-Version können Sie sich bei der Anmeldung bei StoreFront zeitnahe und relevante Informationen zum Startstatus der Citrix Workspace-App für HTML5 anzeigen lassen. Weitere Informationen finden Sie unter Verbesserte Startumgebung für Virtual Apps and Desktops.

Unterstützung für Benutzer mit Entra ID-Identitäten (Vorschau)

Bisher erforderte StoreFront, dass Benutzer in Active Directory vorhanden sind. Mit dieser Version können Benutzer, die sich über OIDC mit Microsoft Entra ID an einem Citrix Gateway authentifizieren, Citrix DaaS-Ressourcen auflisten und starten, die ihren Entra ID-Identitäten zugewiesen sind. Für Benutzer mit Hybrididentitäten listet StoreFront auch alle Ressourcen auf, die ihrer Active Directory-Identität zugewiesen sind.

Es gibt folgende Einschränkungen:

- Benutzer, die sich über SAML authentifizieren, werden weiterhin so behandelt, als hätten sie nur Active Directory-Identitäten und können keine Ressourcen auflisten, die Entra ID-Identitäten zugewiesen sind.
- Benutzer müssen sich über ein Citrix Gateway und nicht direkt bei StoreFront authentifizieren.
- Wenn Benutzer in einer großen Anzahl von Entra-Gruppen sind, kann es zu einem hohen Speicherverbrauch auf dem StoreFront-Server kommen.
- Citrix Virtual Apps and Desktops-Sites werden nicht unterstützt. Ressourcen in Citrix Virtual Apps and Desktops-Sites können möglicherweise nicht aufgelistet werden.
- Die Konfiguration ist in der Verwaltungskonsole nicht verfügbar. Administratoren müssen PowerShell verwenden.
- FAS wird in Stores nicht unterstützt, in denen Benutzer reine Entra ID-Identitäten haben.

Weitere Informationen finden Sie unter Entra ID-Authentifizierung über OIDC.

Entra ID-Single Sign-On bei VDAs (Vorschau)

Wenn Benutzer sich mit Entra ID authentifiziert haben und eine Ressource starten, die auf einem Entra-verbundenen VDA gehostet wird, können sie Single Sign-On bei Entra ID-verbundenen VDAs verwenden.

Es gibt folgende Einschränkungen:

- Dies wird nur bei der Authentifizierung über ein Citrix Gateway unterstützt, wobei eine Verbindung zu Entra ID über OIDC anstelle von SAML verwendet wird.

- Dies muss mit PowerShell konfiguriert werden.
- Die Konfiguration ist in der Verwaltungskonsole nicht verfügbar. Administratoren müssen PowerShell verwenden.
- FAS wird in Stores nicht unterstützt, in denen Entra ID SSO aktiviert ist.

Weitere Informationen finden Sie unter Single Sign-On bei VDAs.

Behobene Probleme

StoreFront 2507 LTSR CU1 enthält die folgenden Korrekturen:

- StoreFront-**Favoriten** werden nicht zwischen StoreFront-Servern synchronisiert, wenn die NTLM-Authentifizierung deaktiviert ist.
- Benutzer erhalten die Fehlermeldung **App kann nicht gestartet werden**, wenn sie versuchen, bestimmte Anwendungen über die interne StoreFront (SF)-URL aufzurufen.
- StoreFront-Server protokollieren zeitweise die Ereignisse 4010 und 4011, was auf XML-Integritätsprüfungsfehler bei den Delivery Controllern (DDCs) hinweist. Dies führt zu gelegentlichen Enumerationsfehlern für Benutzer.
- Wenn Sie die Citrix Web Extension installieren und den Protokollhandler deaktivieren, werden ICA-Dateien heruntergeladen, anstatt Anwendungen zu starten. Dies geschieht, weil das System die Citrix Workspace-App nicht richtig erkennt, wenn der Protokollhandler deaktiviert ist. Die Korrektur zeigt jetzt „Citrix Workspace-App wurde über die Browsererweiterung erfolgreich erkannt“ an und ermöglicht Benutzern, die Clienterkennung bei Bedarf zu wiederholen.

Bekannte Probleme

- Wenn StoreFront an Citrix Analytics angebunden ist, könnten Sie eine deutlich erhöhte CPU-Auslastung feststellen.

Was ist neu in 2507 (Erstveröffentlichung)

StoreFront 2507 LTSR enthält die folgenden neuen Funktionen und Verbesserungen seit StoreFront 2402 LTSR:

Entfernen der Erkennung der Citrix Workspace™-App als Voraussetzung für den App Protection bei hybriden Start-Szenarien

Ab der Version 2507 LTSR ist die Erkennung der Citrix Workspace-App keine Voraussetzung mehr, damit App Protection für hybride Starts funktioniert. Diese Änderung vereinfacht die Aktivierung von App Protection für hybride Start-Szenarien.

Bisher zeigte die Benutzeroberfläche, wenn StoreFront™ so konfiguriert war, dass App Protection für hybride Starts aktiviert wurde, nur Ressourcen an, die App Protection erforderten, wenn bestimmte Versionen der Citrix Workspace-App über Citrix Workspace-Weberweiterungen oder den Citrix Workspace-Launcher erkannt wurden. Dies verhinderte die Verwendung von App Protection in Situationen, in denen der Citrix Workspace-Launcher oder Citrix Workspace-Weberweiterungen nicht verwendet werden konnten. Diese Überprüfung wurde entfernt, und die Benutzeroberfläche zeigt solche Ressourcen nun an, unabhängig davon, ob die Citrix Workspace-App erkannt wurde.

Mit dieser Änderung werden Ressourcen, die App Protection erfordern, in Situationen angezeigt, in denen ICA-Dateien heruntergeladen werden und wenn ältere Versionen der Citrix Workspace-App verwendet werden, die App Protection nicht implementieren. Dies ermöglicht es Benutzern, die Anwendung von App Protection zu umgehen, indem sie die ICA-Datei manipulieren oder eine Version der Citrix Workspace-App verwenden, die App Protection nicht aktiviert. Wenn Sie App Protection für hybride Starts aktiviert haben, ist es daher wichtig, dass Sie auch App Protection Posture Check und Policy Tampering Detection aktivieren.

Erweiterte Scout-Funktionalität

Scout unterstützt jetzt die Anzeige der Schaltfläche „Maschine hinzufügen“ auf der Seite „Sammeln“. Diese Verbesserung ermöglicht es Ihnen, manuell mehrere StoreFront-Servermaschinen im selben Cluster hinzuzufügen und die Sammlung gleichzeitig auszulösen, wodurch die Effizienz der Datenerfassung über StoreFront-Bereitstellungen hinweg verbessert wird.

Entfernung des Citrix Customer Experience Improvement Program

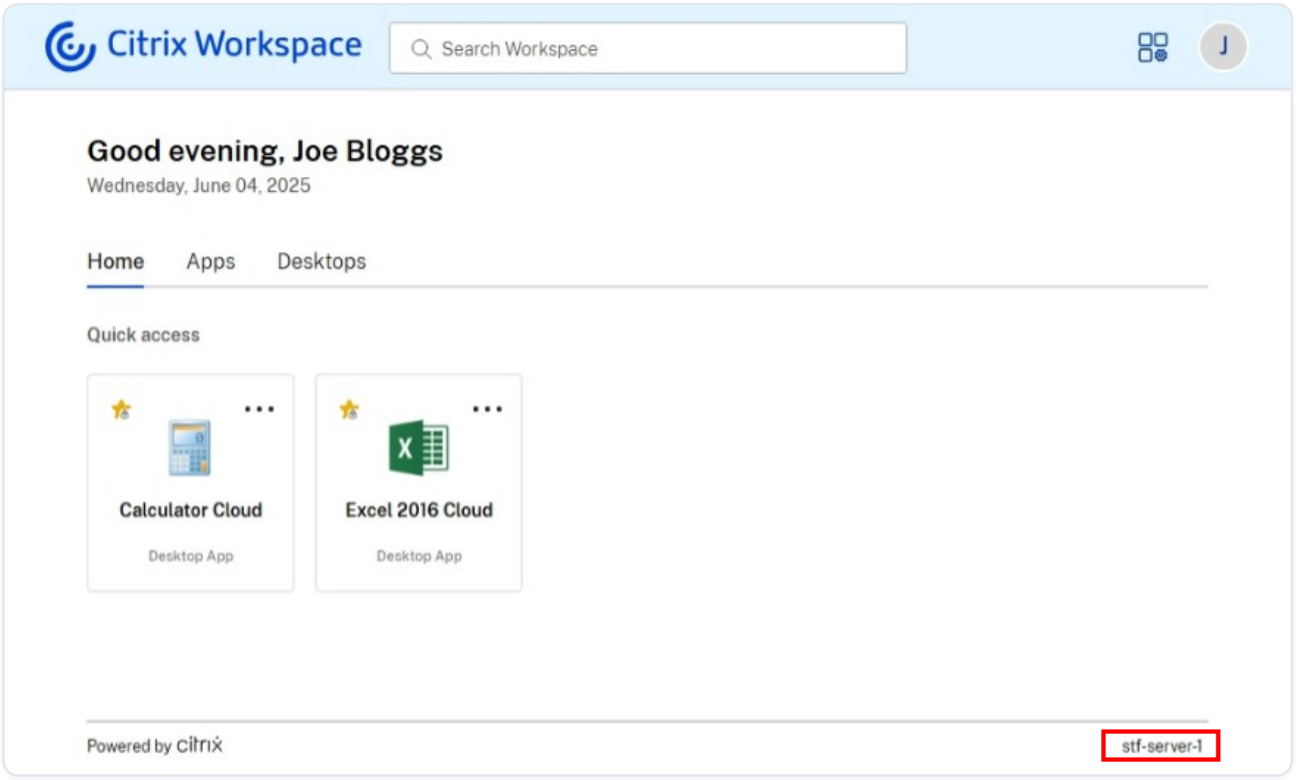
StoreFront sendet keine Daten mehr an das Citrix Customer Experience Improvement Program.

Citrix Workspace-App für HTML5 HDX Client

Diese Version enthält Citrix Workspace-App für HTML5 HDX Client 2505.

Anzeigen des StoreFront-Servernamens in der Endbenutzer-UI

Bei Verwendung der modernen Benutzeroberfläche wird der Name des Servers, mit dem der Benutzer verbunden ist, auf dem Desktop am unteren Bildschirmrand und in Fehlermeldungen auf allen Plattformen angezeigt. Dies hilft dem Support-Team, relevante Serverprotokolle schnell zu finden.



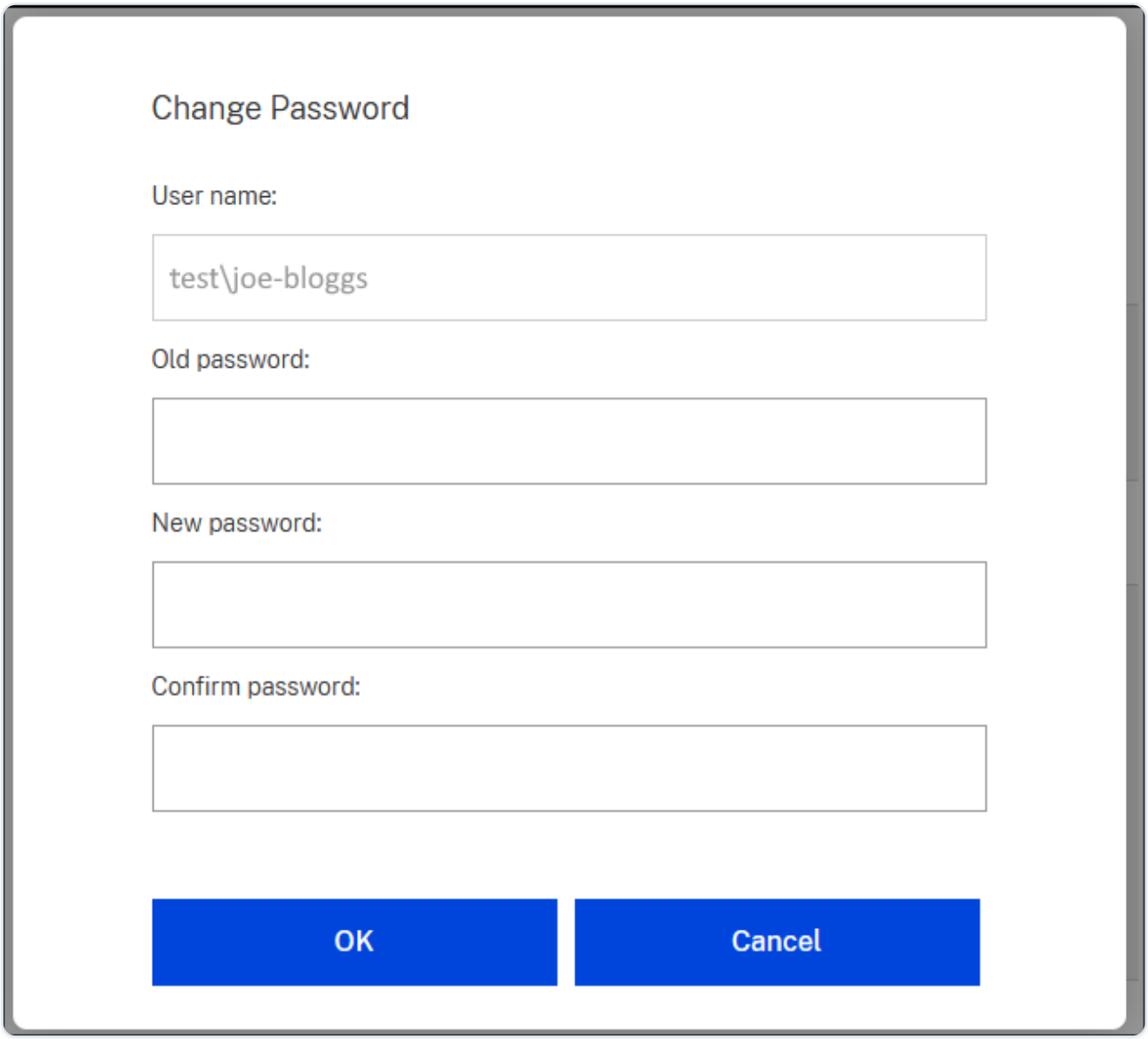
Citrix Workspace Launcher für Android-, iPhone- und iPad-Geräte

Citrix Workspace Launcher ermöglicht Webbrowsern die Kommunikation mit der Citrix Workspace-App, um Ressourcen zu starten, ohne ICA-Dateien herunterzuladen. Zuvor war dies nur unter Windows, macOS und Linux verfügbar. Citrix Workspace Launcher wird jetzt auf Android, iPhone und iPad unterstützt. Wenn ein Android-, iPhone- oder iPad-Benutzer zum ersten Mal eine Store-Website in seinem Webbrowser öffnet, erkennt die Website die Citrix Workspace-App mithilfe von Citrix Workspace Launcher. Bei erfolgreicher Erkennung wird Citrix Workspace Launcher für alle nachfolgenden Starts verwendet. Dies optimiert das Starten und verbessert die Sicherheit, da das Speichern von ICA-Dateien auf dem Gerät vermieden wird.

Dies erfordert die Citrix Workspace-App für Android 25.03 oder höher und die Citrix Workspace-App für iOS 25.03 oder höher. Es ist sowohl mit der klassischen als auch mit der modernen Oberfläche verfügbar.

Passwörter jederzeit mit der modernen Oberfläche ändern

Bisher konnten Benutzer bei Verwendung der modernen Oberfläche abgelaufene Passwörter beim Anmelden ändern, hatten aber keine Möglichkeit, sie zu anderen Zeiten zu ändern. Mit StoreFront 2503 gibt es, sofern in den Passwortoptionen konfiguriert, in den Kontoeinstellungen eine Option, Passwörter jederzeit zu ändern, ähnlich wie bei der klassischen Oberfläche.



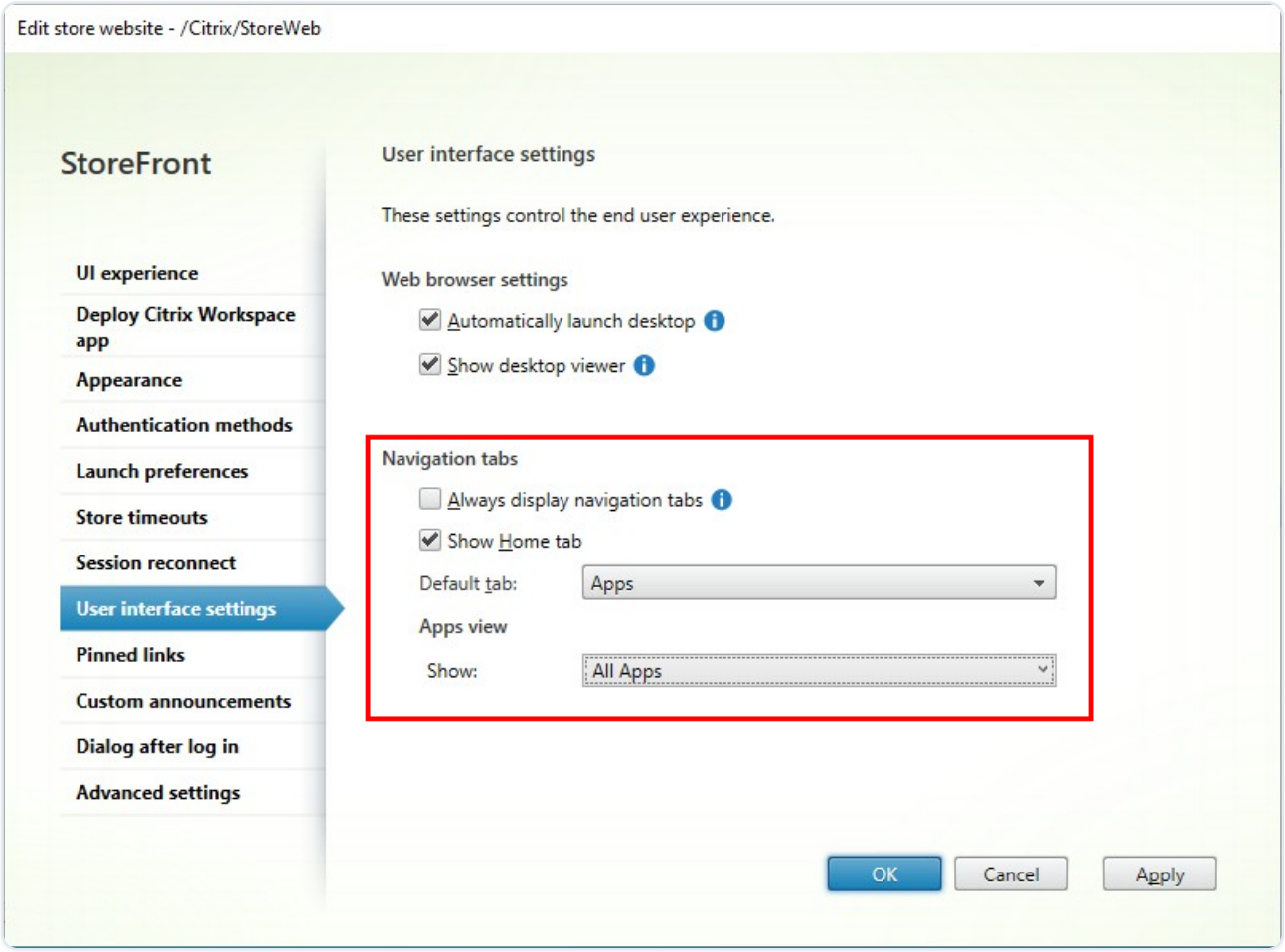
Weitere Informationen finden Sie unter Passwort ändern.

Erweiterte Navigation und Standard-Tab-Konfiguration mit der modernen Oberfläche

Bei Verwendung der modernen Oberfläche können Administratoren die Navigationsregisterkarten für Endbenutzer anpassen. Administratoren können die folgenden Optionen konfigurieren:

- Navigationsregisterkarten immer anzeigen.
- Startregisterkarte anzeigen

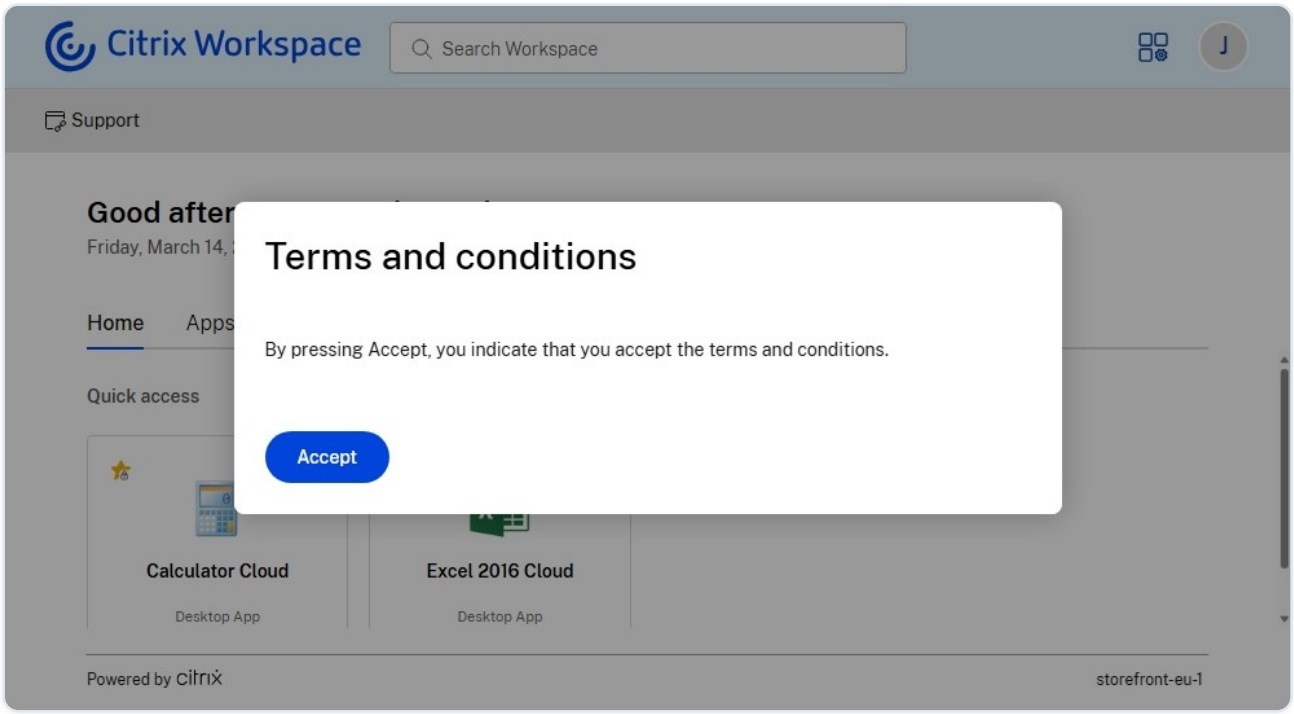
- Standardregisterkarte



Weitere Informationen finden Sie unter Navigationsregisterkarten

Dialogfeld nach der Anmeldung anzeigen

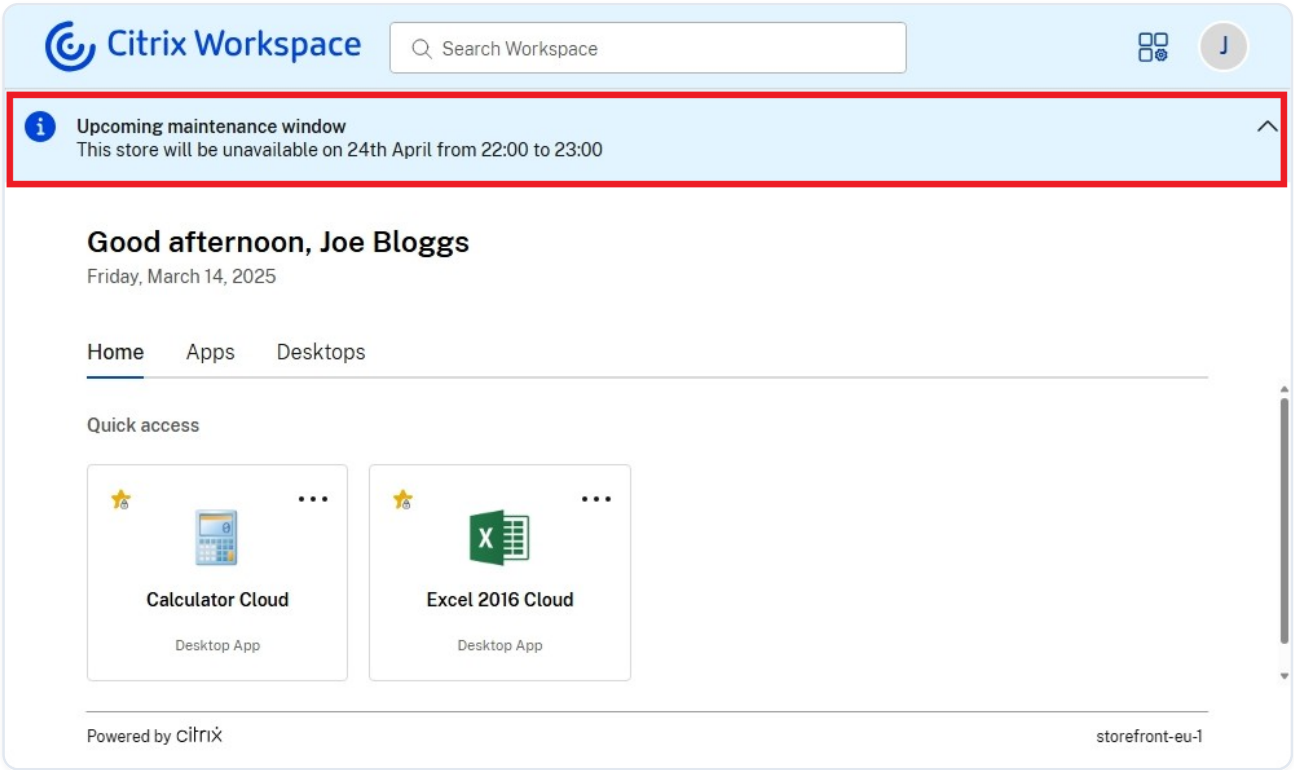
Bei Verwendung der modernen Benutzeroberfläche können Administratoren ein Pop-up-Dialogfeld konfigurieren, das Endbenutzern nach der Anmeldung angezeigt wird und das Benutzer akzeptieren müssen, bevor sie mit StoreFront interagieren. Sie können dies verwenden, um Benutzer über wichtige Informationen wie regulatorische Informationen, Bestätigungen von Richtlinien, interne Richtlinien, Anleitungsinhalte, Sicherheitshinweise, Systemaktualisierungen und rechtliche Hinweise zu informieren. Dies ist nur bei Verwendung der modernen Benutzeroberfläche verfügbar.



Weitere Informationen zur Konfiguration finden Sie unter Dialog nach der Anmeldung.

Benutzerdefinierte Ankündigungen

Bei Verwendung der modernen Benutzeroberfläche können Administratoren ein Banner konfigurieren, das den Endbenutzern angezeigt wird, um sie beispielsweise über bevorstehende Änderungen oder Wartungsfenster zu informieren. Weitere Informationen finden Sie unter Benutzerdefinierte Ankündigungen.



Sitzungswiederverbindung mit der modernen Benutzeroberfläche

Die Sitzungswiederverbindung (früher bekannt als Workspace Control) ist jetzt bei Verwendung der modernen Benutzeroberfläche verfügbar. Zuvor war sie nur bei Verwendung der klassischen Benutzeroberfläche verfügbar. Mit der Sitzungswiederverbindung können Sie die folgenden Einstellungen für Benutzer konfigurieren, die sich über einen Webbrowser verbinden:

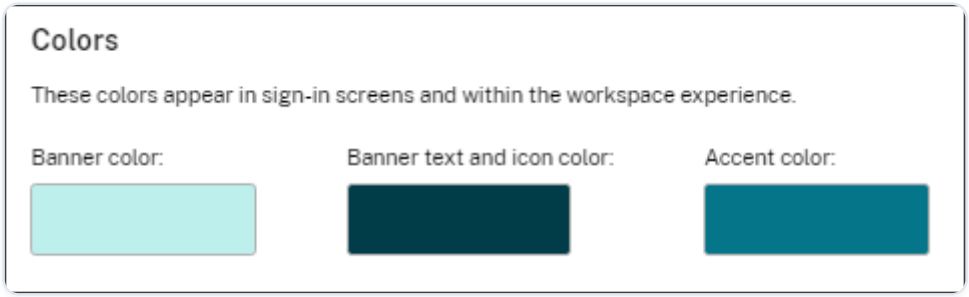
- Abmeldeaktion des Stores – ob Sitzungen aktiv bleiben, sie trennen oder abgemeldet werden sollen.
- Ob automatisch eine Wiederverbindung zu Sitzungen hergestellt werden soll, wenn sich Benutzer anmelden.

Weitere Informationen finden Sie unter Sitzungswiederverbindung

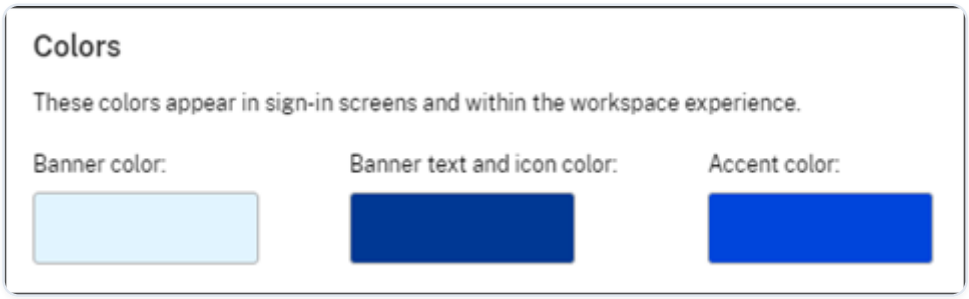
Farbanpassung mit der modernen Benutzeroberfläche

Die Standardfarben wurden aktualisiert.

Alte Standardfarbe:



Neue Standardfarbe:

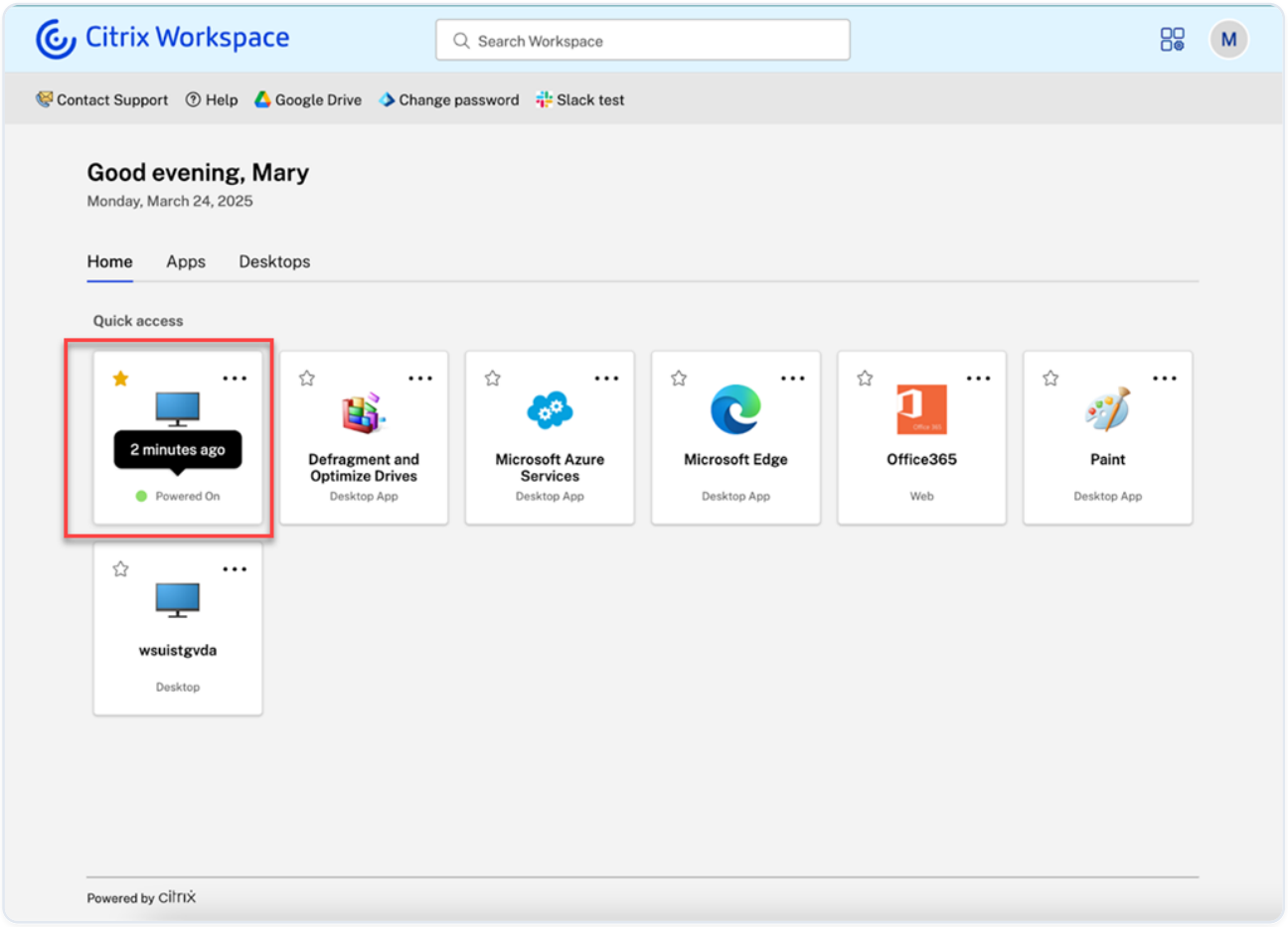


Darüber hinaus werden die Farben jetzt konsistenter auf Schaltflächen, Links und Ladeanzeigen angewendet.

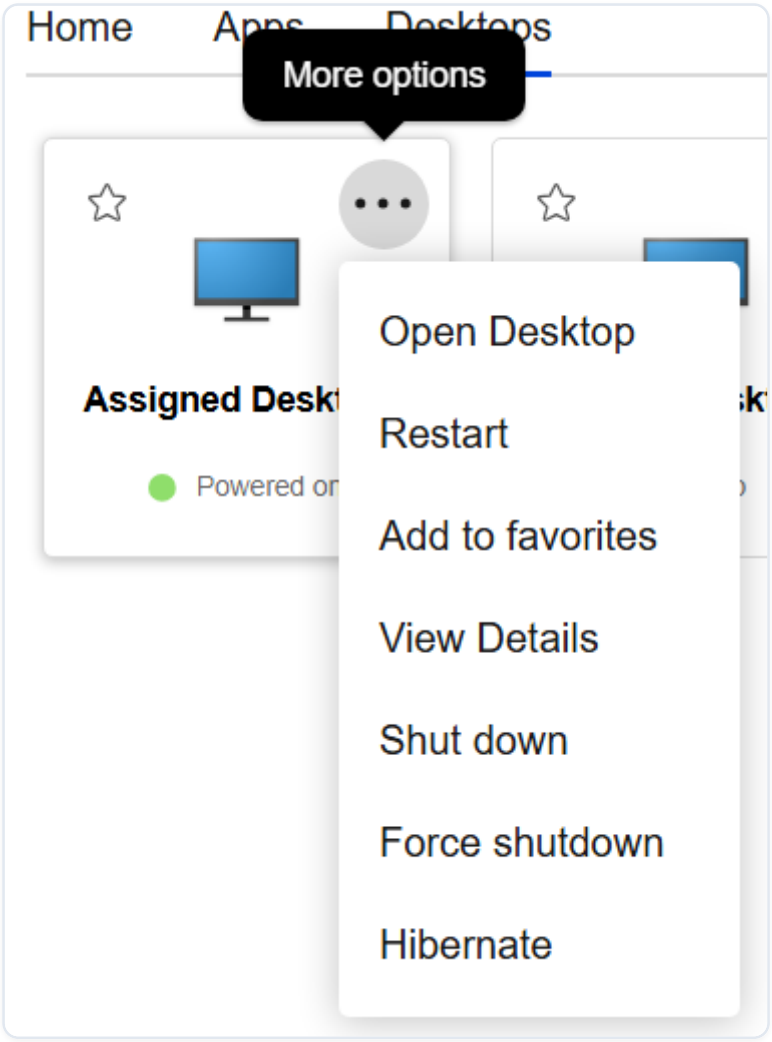
Weitere Informationen finden Sie unter Erscheinungsbild.

Anzeigen des Energiezustands zugewiesener Desktops

Die Endbenutzeroberfläche bietet jetzt, bei Verwendung der modernen Erfahrung mit DaaS, Einblick in den Energiezustand der zugewiesenen Desktops des Benutzers. Der Energiezustand gibt an, ob ein zugewiesener Desktop eingeschaltet, ausgeschaltet oder in einem angehaltenen Zustand (im Ruhezustand) ist. Diese Verbesserung ermöglicht es Benutzern, den Status ihrer Desktops schnell zu erkennen, sodass sie fundierte Entscheidungen treffen und ihre Ressourcen effektiver verwalten können.



Benutzer können energiebezogene Aktionen direkt über die Desktop-Kachel mithilfe des Menüs **Weitere Optionen** (Auslassungspunkte-Symbol) ausführen. Verfügbare Aktionen ändern sich dynamisch basierend auf dem aktuellen Energiezustand des Desktops.



Weitere Informationen finden Sie unter Energiezustand zugewiesener Desktops und Kachelaktionen.

Hinweis:

- Diese Funktionalität erfordert Citrix DaaS. Sie ist derzeit nicht mit Citrix Virtual Apps and Desktops verfügbar.
- Energiezustände werden für Desktops, bei denen App Protection aktiviert ist, nicht angezeigt.
- Energiezustände werden nur für zugewiesene Desktops angezeigt, nicht für gepoolte Desktops.

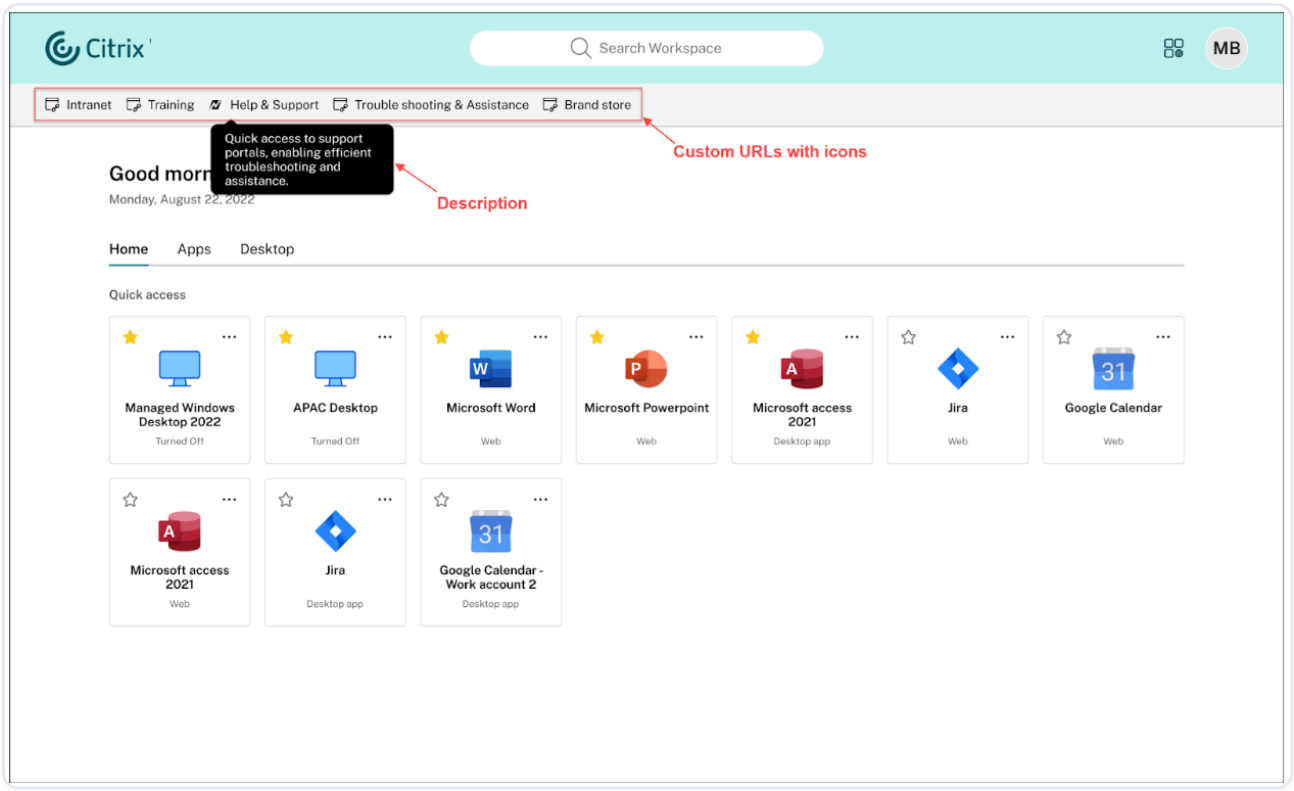
Aktualisierte Terminologie in der Verwaltungskonsole

Die Verwaltungskonsole verwendet eine aktualisierte Terminologie. Insbesondere wurden die folgenden Begriffe aktualisiert:

ALTER BEGRIFF	NEUER BEGRIFF	HINWEISE
Citrix Receiver	Citrix Workspace-App	Citrix Receiver wird nicht unterstützt und wurde durch die Citrix Workspace-App ersetzt.
HDX™ Engine (Plug-in)	Citrix Workspace-App	Der HDX-Client ist eine Komponente der Citrix Workspace-App.
Receiver für Web	Website	
Vereinheitlichte Erfahrung	Klassische Erfahrung	Auf der Registerkarte „UI-Erfahrung“ beim Bearbeiten einer Website.
Erfahrung der nächsten Generation	Moderne Erfahrung	Auf der Registerkarte „UI-Erfahrung“ beim Bearbeiten einer Website.
Vereinheitlichte Erfahrung konfigurieren	Citrix Workspace-App-Website festlegen	Der Link im Aktionsbereich.
Delivery Controller™	Site	Dies spiegelt wider, dass jede Entität eine Site ist, die aus mehreren Delivery Controllern oder einem DaaS-Mandanten oder SPA-Server besteht.
Workspace Control	Sitzungswiederverbindung	

Angeheftete Links

Benutzerdefinierte URLs auf der StoreFront-Benutzeroberfläche beziehen sich auf vom Kunden definierte Hyperlinks, die einen schnellen Zugriff auf bestimmte Websites ermöglichen. Diese Funktion dient als Verknüpfung, die Benutzern hilft, effizient direkt von der StoreFront-Benutzeroberfläche zu Websites zu navigieren. Wichtige Links, wie z. B. Support-Websites oder Unternehmensportale, können den Benutzern zur Verfügung gestellt werden, ohne dass sie diese Links suchen müssen. Dies macht die Navigation mühelos und schneller. Diese Funktion ist nur in der modernen Oberfläche verfügbar.



Weitere Informationen finden Sie unter Angeheftete Links

Endbenutzer dazu verpflichten, nur die lokal installierte Citrix App zu verwenden

Administratoren können die Verwendung der nativen Citrix Workspace-App erzwingen, wodurch die Möglichkeit für Benutzer entfällt, über Browser auf den Citrix Workspace-Webclient zuzugreifen. Diese Funktion wurde für Kunden entwickelt, die die vollen Vorteile der nativen App nutzen möchten. Die native App bietet Vorteile wie den integrierten App Protection-Dienst, keine Kompatibilitätsprobleme mit Browserversionen, verbesserte Sicherheit und Telemetrie zur Überwachung und Fehlerbehebung.

Weitere Informationen finden Sie unter Endbenutzer dazu verpflichten, nur die lokal installierte Citrix App zu verwenden

XenApp® Services standardmäßig für neue Stores deaktiviert

Wenn Sie einen neuen Store erstellen, ist XenApp Services standardmäßig deaktiviert. Sie können es manuell in der GUI oder mithilfe von PowerShell aktivieren. Beachten Sie, dass XenApp Services veraltet ist und in einer zukünftigen Version entfernt wird.

Progressive Web-App

Die Funktion Progressive Web-App (PWA) ermöglicht es Ihnen, die Store-Website zu installieren, sodass sie von Ihrem Startmenü oder Desktop aus gestartet werden kann, ähnlich einer nativen

App. Dies ist nur in der alten Benutzeroberfläche verfügbar. Weitere Informationen finden Sie unter Progressive Web-App

Citrix Lizenzierungs-Telemetrie

StoreFront sammelt Telemetriedaten zu Benutzeranmeldungen und Ihrer Konfiguration. Weitere Informationen finden Sie unter Citrix Licensing-Datenerfassungsprogramme.

Citrix Gateway Service für StoreFront

Der Citrix Gateway Service für StoreFront bietet HDX-Routing zu Ihren Ressourcen, ohne dass Sie Ihr eigenes Gateway hosten müssen. Weitere Informationen finden Sie unter Gateway Service für StoreFront und Citrix Gateway Service hinzufügen.

Wenn Sie den Citrix Gateway Service für StoreFront (Technical Preview) mit StoreFront 2311 oder 2402 gewählt und ein CloudGateway konfiguriert haben, ist die Konfiguration mit StoreFront 2507 nicht mehr gültig. Sie müssen das vorhandene Gateway löschen und neue Gateways gemäß der aktualisierten Dokumentation erstellen.

Citrix Web-Erweiterungen

Citrix Web-Erweiterungen ist für alle Installationen aktiviert, ohne dass StoreFront manuell mit PowerShell konfiguriert werden muss.

Unterstützung für Windows Server 2025

StoreFront 2407 kann auf Windows Server 2025 Datacenter und Standard Editionen installiert werden.

Entfernung der Unterstützung für Windows Server 2016

StoreFront 2407 kann nicht auf Windows Server 2016 installiert werden. Installieren Sie StoreFront auf Windows Server 2019, 2022 oder 2025. Weitere Informationen zu entfernten Elementen finden Sie unter Hinweise zur Einstellung.

Behobene Probleme

Diese Version enthält die folgenden Korrekturen seit 2402 CU2:

- Wenn Sie in der Verwaltungskonsole > Bildschirm „Authentifizierungsmethoden verwalten“ alle Authentifizierungsmethoden außer HTTP Basic deaktivieren und dann auf OK klicken, um die Änderungen zu speichern, wird ein Fehler angezeigt.

- Wenn Sie die **Startoption** in **In Citrix Workspace-App öffnen** ändern und die Änderungen speichern, zeigt StoreFront möglicherweise einen Fehler an. Der Fehler tritt auf, wenn die auf dem Server installierte HTML5 HDX-Version von der standardmäßig von der aktuellen StoreFront-Version installierten Version abweicht.
- Beim Konfigurieren einer benutzerdefinierten Ankündigung ist es möglich, einen sehr langen Titel und eine Beschreibung einzugeben, die nicht korrekt angezeigt werden.
- Wenn Sie einen StoreFront-Server zu einer Servergruppe hinzufügen, wird der `Citrix Receiver for Web` Anwendungspool des neuen Servers so eingestellt, dass er regelmäßig recycelt wird, was Benutzer unerwartet abmelden könnte. Mit dieser Korrektur wird der Anwendungspool so eingestellt, dass er zwischen 01:00 und 03:55 Uhr recycelt wird, um Arbeitszeiten zu vermeiden.
- Mehrere Telemetrie-Ausnahmeereignisse werden protokolliert, wenn StoreFront auf einem nicht-englischen System installiert wird
- Die StoreFront-Verwaltungskonsole bezieht sich auf den veralteten Begriff „Unified Experience“.
- Der PowerShell-Befehl `Get-STFWebReceiverSiteStyle` kann mit dem Fehler `Value cannot be null` fehlschlagen.
- Der PowerShell-Befehl `Set-STFWebReceiverSiteStyle` kann mit dem Fehler `Value cannot be null` fehlschlagen.
- Änderungen auf der Registerkarte **Erscheinungsbild** der Website werden möglicherweise nicht korrekt gespeichert.
- Der PowerShell-Befehl `Set-STFWebReceiverSiteStyle` setzt nicht angegebene Parameter auf den Standardwert zurück, anstatt ihren vorhandenen Wert beizubehalten.
- Wenn Cloud Connectors im LHC-Modus betrieben werden und ein Benutzer versucht, eine Ressource zu starten, die von mehreren Standorten aus zugänglich ist, kann die Sitzung möglicherweise nicht gestartet werden, wenn die Ressource nicht sofort verfügbar ist. Das Problem tritt auf, weil StoreFront nach Überprüfung der Ressourcenbereitschaft die Anforderung möglicherweise an einen anderen Connector sendet als den, der ursprünglich zum Starten der Ressource verwendet wurde.
- Sobald StoreFront einen FAS-Server auswählt, schlägt der Start fehl, wenn dieser FAS-Server später nicht mehr verfügbar ist. Mit dieser Korrektur wählt StoreFront stattdessen einen anderen FAS-Server aus, sodass der Start fortgesetzt werden kann.
- Wenn ein FAS-Server nicht antwortet, versucht StoreFront weiterhin, ihn für jeden Benutzer zu kontaktieren, was die Anmelde- oder Startzeit (je nach Konfiguration) verzögert. Mit dieser

Korrektur vermeidet StoreFront, denselben Server für einen bestimmten Zeitraum zu verwenden, wenn ein FAS-Server nicht antwortet, sodass nachfolgende Benutzer nicht von der Verzögerung betroffen sind.

- Wenn Socket-Pooling aktiviert ist, kann StoreFront einen hohen Speicherverbrauch und Port-Erschöpfung aufweisen, was zu Dienstausfällen führt.
- Ein Upgrade auf eine neuere Version von StoreFront schlägt fehl und die Protokolle enthalten den Text „VersionData:Load Failed due to exception: System.IndexOutOfRangeException“. Das Problem tritt auf, wenn eine von StoreFront erstellte Benutzergruppe eine leere Beschreibung hat.
- Gelegentlich schlägt das StoreFront-Upgrade fehl. Der Installer schlägt entweder stillschweigend fehl, bevor der Assistent angezeigt wird, oder der Assistent reagiert nicht mehr, oder nach dem Durchklicken des Assistenten schlägt das Upgrade fehl. Das Problem tritt auf, weil die Installationsdateien gelöscht werden, bevor sie benötigt werden.
- Das Upgrade schlägt mit der Meldung „Beim Hinzufügen von Benutzerkonten in der lokalen Gruppe „Administrators“ zur lokalen Gruppe „CitrixStorefrontAdministrators“ ist ein Fehler aufgetreten“ oder Ähnlichem fehl. Dies tritt auf, wenn eine von StoreFront verwendete Benutzergruppe einen gelöschten Benutzer enthält.
- Während eines Ausfalls, wenn die Connectors in den Local Host Cache-Modus wechseln, muss StoreFront Startanforderungen an den Connector in derselben Zone wie die Ressource senden. Wenn eine Ressource in mehreren Zonen verfügbar ist, versuchte StoreFront zuvor nur, die Ressource in einer Zone zu starten. Mit dieser Verbesserung versucht der StoreFront-Server in einigen Fällen, wenn der Versuch, eine Ressource in einer Zone zu starten, fehlschlägt, einen weiteren Versuch, die Ressource mithilfe von Connectors in anderen verfügbaren Zonen zu starten, um die Ausfallsicherheit zu verbessern.
- Zusätzliche Benachrichtigung entfernen, die in der Citrix Workspace-App für Windows 2309 oder höher angezeigt wird, wenn eine Verbindung zu StoreFront 2402 über eine XenApp Services-URL hergestellt wird.
- In der StoreFront Web-API sollte der Listenendpunkt `isSubscriptionEnabled` festlegen, je nachdem, ob Favoriten aktiviert sind.
- In der Store Services-API sollte der Ressourcenaufzählungs-Endpunkt den Abonnementstatus festlegen, je nachdem, ob Favoriten aktiviert sind.
- Wenn Sie StoreFront aktualisieren, stellen Sie möglicherweise fest, dass doppelte Kopien von Anpassungsdateien, die im benutzerdefinierten Ordner (`\StoreWeb\custom`) abgelegt wurden, nach Abschluss des Upgrade-Vorgangs auch im Stammverzeichnis des Website-Ordners (`\StoreWeb`) gefunden werden können.

- Bei Verwendung des Citrix Gateway Service und wenn **Tickets von zwei Cloud Connectors anfordern, sofern verfügbar** ausgewählt ist, wird nur ein Ticket ausgestellt.
- Wenn Sie die Startoption von **In Citrix Workspace-App öffnen** in **Benutzer wählen lassen** oder **In einem Webbrowser öffnen** ändern und **OK** auswählen, erhalten Sie möglicherweise die Fehlermeldung **Beim Speichern der Änderungen im Eigenschaftsdialogfeld „Starteinstellungen“ ist ein Fehler aufgetreten. Überprüfen Sie das Protokoll in der Ereignisanzeige und versuchen Sie es erneut.** Dies tritt auf, wenn der HTML5 HDX-Client unerwartet bereits installiert ist.

Korrekturen an der klassischen Benutzeroberfläche:

- Wenn die **Startoption** auf **Benutzer wählen lassen** eingestellt ist, zeigt der Bildschirm **Willkommen bei der Citrix Workspace-App** den Text **undefined** an.
- Nach dem Deaktivieren von **Benutzern erlauben, die Erkennung der Citrix Workspace-App zu überspringen**, sind Benutzer, die zuvor die Erkennung der Citrix Workspace-App übersprungen haben, nicht betroffen. Mit dieser Korrektur müssen solche Benutzer beim nächsten Öffnen der Store-Website die Erkennung der Citrix Workspace-App durchführen.
- Bei Verwendung von Microsoft Edge fehlen nach dem Herunterladen der Citrix Workspace-App die Anweisungen zum Starten des Citrix Workspace-Launchers.
- Bei Verwendung von Safari fehlen auf dem Bildschirm zur Erkennung der Citrix Workspace-App die Anweisungen zum Öffnen des Citrix Workspace-Launchers.
- Wenn die **Startoption** auf **Benutzer wählen lassen** eingestellt ist und die Citrix Web Extension installiert ist und die Citrix Workspace-App erkannt hat, ist es nicht möglich, die Startmethode zum Öffnen von Ressourcen in einem Webbrowser zu ändern.
- Wenn die Citrix Workspace-App von der Citrix Web Extension erfolgreich erkannt wurde, sollte der Link zum **Herunterladen der Citrix Workspace-App** von der Einstellungsseite ausgeblendet werden.
- Der automatische Desktop-Start funktioniert nach einem Jahr nach dem ersten Zugriff des Benutzers auf die Website nicht mehr.
- Die Content Security Policy sollte `default-src: none` enthalten.
- Die Benutzeroberfläche hängt, wenn die Citrix Web Extension nach der Erkennung der Citrix Workspace-App deaktiviert/entfernt wird.
- Das Copyright-Symbol wird bei der Verwendung nicht-englischer Sprachen nicht korrekt angezeigt.

- Geben Sie auf dem Einstellungsbildschirm an, ob die Citrix Workspace Web Extension zum Starten von Apps und Desktops verwendet werden soll.
- Einige Cookies haben `SameSite` nicht gesetzt. Mit dieser Änderung wird `SameSite` für alle Cookies auf `Lax` gesetzt.
- Aktualisieren Sie die Übersetzung auf dem Client-Erkennungsbildschirm, wenn Sie Mozilla Firefox in brasilianischem Portugiesisch verwenden.
- Die im **http-equiv**-Tag der HTML-Datei definierte Content Security Policy wurde aktualisiert, um Inline-Skripte zu blockieren. Wenn Sie StoreFront so angepasst haben, dass es eval verwendet oder Inline-Skripte zum DOM hinzufügt, führt diese Aktion dazu, dass diese Anpassungen fehlschlagen.

Korrekturen an der modernen Benutzeroberfläche:

- Bei Verwendung von Google Chrome unter macOS mit installierter Citrix Web Extension funktioniert die Sitzungswiederherstellung möglicherweise nicht.
- Die Registerkarte „Desktops“ sollte ausgeblendet werden, wenn der Benutzer keine Desktops besitzt.
- Auf der Desktop-Kachel einer in den Ruhezustand versetzten Ressource ist die Option **Fortsetzen** nicht verfügbar.
- Wenn ein Benutzer versucht, einen Desktop über den Activity Manager neu zu starten, erhält er die Fehlermeldung **Desktop kann nicht neu gestartet werden**.
- Ressourcenfilterregeln sollten nicht auf Sitzungen angewendet werden, die vom **Activity Manager** aufgelistet werden.
- Auf Mobilgeräten sollte die Schaltfläche **Abbrechen** neben der Suchleiste schwarz statt blau sein.
- Wenn alle Ressourcen App Protection erfordern und der Benutzer sich entschieden hat, sie im Browser zu starten, ist die Option zum Verbinden mit der Citrix Workspace-App nicht verfügbar.
- Auf einer Kachel für einen persistenten Desktop im Ruhezustand enthält das Menü keine Option zum Fortsetzen des Desktops. .
- Die moderne Benutzeroberfläche wird in der Citrix Workspace-App für Linux nicht geladen.
- Ermöglichen Sie dem Activity Manager, mehr Sites zu verwalten, als gleichzeitig aufgezählt werden können.

Bekannte Probleme

- Bei Verwendung von Safari unter iOS kann die Webseite nach Abschluss der Erkennung der Citrix Workspace-App und der Rückkehr zu Safari auf einem Ladebildschirm hängen bleiben. Um dies zu umgehen, muss der Benutzer die Webseite aktualisieren.
- Auf der Registerkarte „Darstellung“ der Verwaltungskonsole funktioniert die Schaltfläche „Auf Standard zurücksetzen“ nicht.
- Die StoreFront-Verwaltungskonsole zeigt zuvor hochgeladene Logos nicht an.
- Wenn StoreFront ein Gateway vom Typ Citrix Gateway Service hat, dann können beim Upgrade von StoreFront 2407 oder 2411 auf 2507 Starts über dieses Gateway fehlschlagen. Im Gateway-Konfigurationsfenster, auf der Registerkarte Cloud Connector, enthalten die Cloud Connectors fälschlicherweise Port 8090, sodass StoreFront den Cloud Connector nicht erreichen kann, um ein STA-Ticket anzufordern. Um dies zu beheben, entfernen Sie den Port aus der URL jedes Cloud Connectors in der Liste.

Erste Schritte

Voraussetzungen

1. Planen Sie Ihre StoreFront-Bereitstellung
2. Installieren und konfigurieren Sie die Ressourcenanbieter, die StoreFront aggregieren soll:
   - Citrix Virtuelle Apps und Desktops
   - Citrix DaaS
   - Secure Private Access.

   Weitere Informationen zur optimalen Konfiguration der Ressourcen finden Sie unter Ressourcen konfigurieren.
3. Überprüfen Sie die Systemanforderungen und stellen Sie sicher, dass Sie die Voraussetzungen für die Installation von StoreFront erfüllen.

StoreFront bereitstellen

Um Ihre StoreFront™-Bereitstellung zu erstellen, führen Sie die folgenden Schritte aus:

1. StoreFront installieren auf einem neuen Server.
2. Eine neue Bereitstellung erstellen mit Ihrem ersten Store.
3. Festlegen, wie Benutzer auf den Store zugreifen.

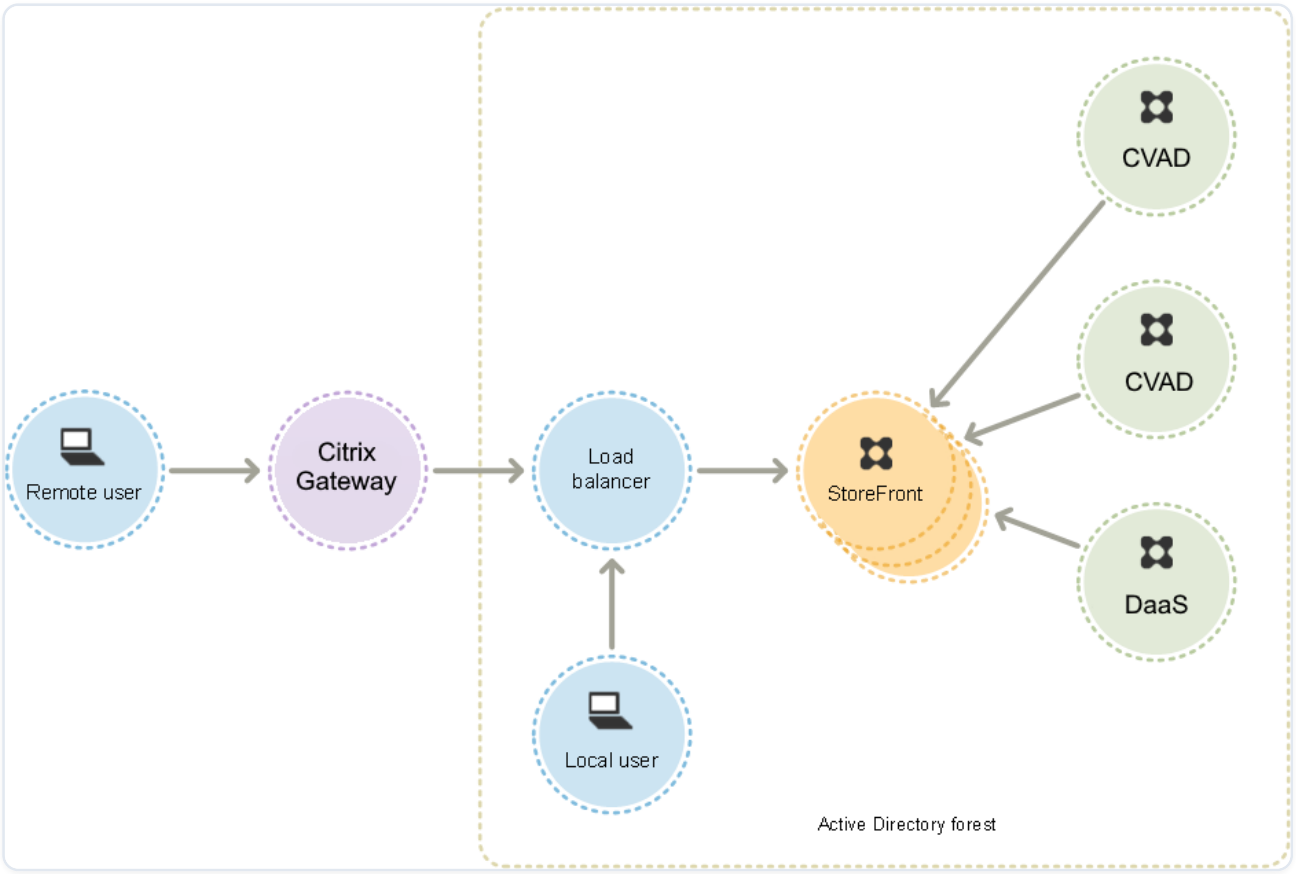
Bereitstellung optimieren

1. Für Redundanz und Skalierbarkeit stellen Sie einen Lastausgleichsdienst bereit und fügen Sie weitere Server zur StoreFront-Servergruppe hinzu.
2. Ihre Bereitstellung sichern.
3. Optimieren Sie die Endbenutzererfahrung.
4. Aktivieren Sie den Remotezugriff über ein Citrix Gateway.

Planen Sie Ihre StoreFront-Bereitstellung

StoreFront lässt sich in Ihre Citrix Virtual Apps and Desktops-Bereitstellungen integrieren und bietet Benutzern einen einzigen Self-Service-Zugriffspunkt für ihre Desktops und Anwendungen.

Die Abbildung zeigt eine typische StoreFront-Bereitstellung.



Active Directory

StoreFront verwendet Active Directory zur Authentifizierung von Benutzern, zum Nachschlagen von Gruppenmitgliedschaften und anderen Details sowie zur Synchronisierung von Daten zwischen StoreFront-Servern.

Für Einzelserver-Bereitstellungen können Sie StoreFront auf einem nicht in die Domäne eingebundenen Server installieren, aber bestimmte Funktionen sind dann nicht verfügbar; andernfalls müssen StoreFront-Server entweder in der Active Directory-Domäne, die die Benutzerkonten enthält, oder in einer Domäne mit einer Vertrauensstellung zur Benutzerkontendomäne residieren, es sei denn, Sie aktivieren die Delegierung der Authentifizierung an die Citrix Virtual Apps and Desktops-Sites oder -Farmen. Alle StoreFront-Server in einer Gruppe müssen sich in derselben Domäne befinden.

StoreFront-Servergruppen

StoreFront kann entweder auf einem einzelnen Server oder als Bereitstellung mit mehreren Servern, einer sogenannten StoreFront-Servergruppe, konfiguriert werden. Servergruppen bieten nicht nur zusätzliche Kapazität, sondern auch eine höhere Verfügbarkeit. StoreFront stellt sicher, dass Konfigurationsinformationen und Details zu den Anwendungsabonnements der Benutzer auf allen Servern einer Servergruppe gespeichert und repliziert werden. Dies bedeutet, dass Benutzer, wenn ein StoreFront-Server aus irgendeinem Grund nicht verfügbar ist, weiterhin über die verbleibenden Server auf ihre Stores zugreifen können. Währenddessen werden die Konfigurations- und Abonnementdaten auf dem ausgefallenen Server automatisch aktualisiert, wenn er sich wieder mit der Servergruppe verbindet. Abonnementdaten werden aktualisiert, wenn der Server wieder online ist, aber Sie müssen Konfigurationsänderungen propagieren, falls der Server während der Offline-Zeit welche verpasst hat. Im Falle eines Hardwarefehlers, der den Austausch des Servers erfordert, können Sie StoreFront auf einem neuen Server installieren und ihn der bestehenden Servergruppe hinzufügen. Der neue Server wird automatisch konfiguriert und mit den Anwendungsabonnements der Benutzer aktualisiert, wenn er der Servergruppe beitritt.

Citrix® empfiehlt maximal sechs Server in einer Servergruppe. Bei mehr als sechs Servern überwiegt der Overhead der Datensynchronisierung den Nutzen der zusätzlichen Server, und die Leistung verschlechtert sich.

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) aufweisen. Idealerweise sollten sich alle Server in einer Servergruppe am selben Standort (Rechenzentrum, Verfügbarkeitszone) befinden, aber Servergruppen können Standorte innerhalb derselben Region umfassen, sofern die Verbindungen zwischen den Servern in der Gruppe diese Latenzkriterien erfüllen. Beispiele hierfür sind Servergruppen, die Verfügbarkeitszonen innerhalb einer Cloud-Region oder zwischen Rechenzentren in Ballungsräumen umfassen. Beachten Sie, dass die Latenz zwischen den Zonen je nach Cloud-Anbieter variiert. Citrix empfiehlt das Überspannen von Standorten nicht als Disaster-Recovery-Konfiguration, es kann jedoch für Hochverfügbarkeit geeignet sein.

Lastenausgleich

Für mehrere Server in einer StoreFront-Servergruppe müssen Sie einen externen Lastenausgleich konfigurieren. Verwenden Sie einen Lastenausgleich mit integrierten Monitoren und Sitzungspersistenz, wie z. B. NetScaler ADC. Weitere Informationen zum Lastenausgleich mit NetScaler ADC finden Sie unter Lastenausgleich.

Citrix Gateway für Fernzugriff

Wenn Sie den Zugriff auf StoreFront von außerhalb des Unternehmensnetzwerks ermöglichen möchten, ist ein Citrix Gateway erforderlich, um sichere Verbindungen für Remote-Benutzer bereitzustellen. Stellen Sie Citrix Gateway außerhalb des Unternehmensnetzwerks bereit, wobei Firewalls Citrix Gateway sowohl vom öffentlichen als auch vom internen Netzwerk trennen. Stellen Sie sicher, dass Citrix Gateway auf die Active Directory-Gesamtstruktur zugreifen kann, die die StoreFront-Server enthält.

Global Server Load Balancer

In großen Citrix-Bereitstellungen verfügen Sie möglicherweise über StoreFront- und NetScaler-Bereitstellungen in mehreren Rechenzentren. Mit einem Global Server Load Balancer (GSLB) können Sie eine einzige globale URL konfigurieren, die der GSLB auf die spezifische URL eines Gateways in einer der Regionen umleitet. Typischerweise wählt der GSLB das nächstgelegene Gateway basierend auf einem Lastenausgleichsalgorithmus wie Round Trip Time (RTT) oder Static Proximity.

Sie könnten beispielsweise 3 regionale Gateways haben:

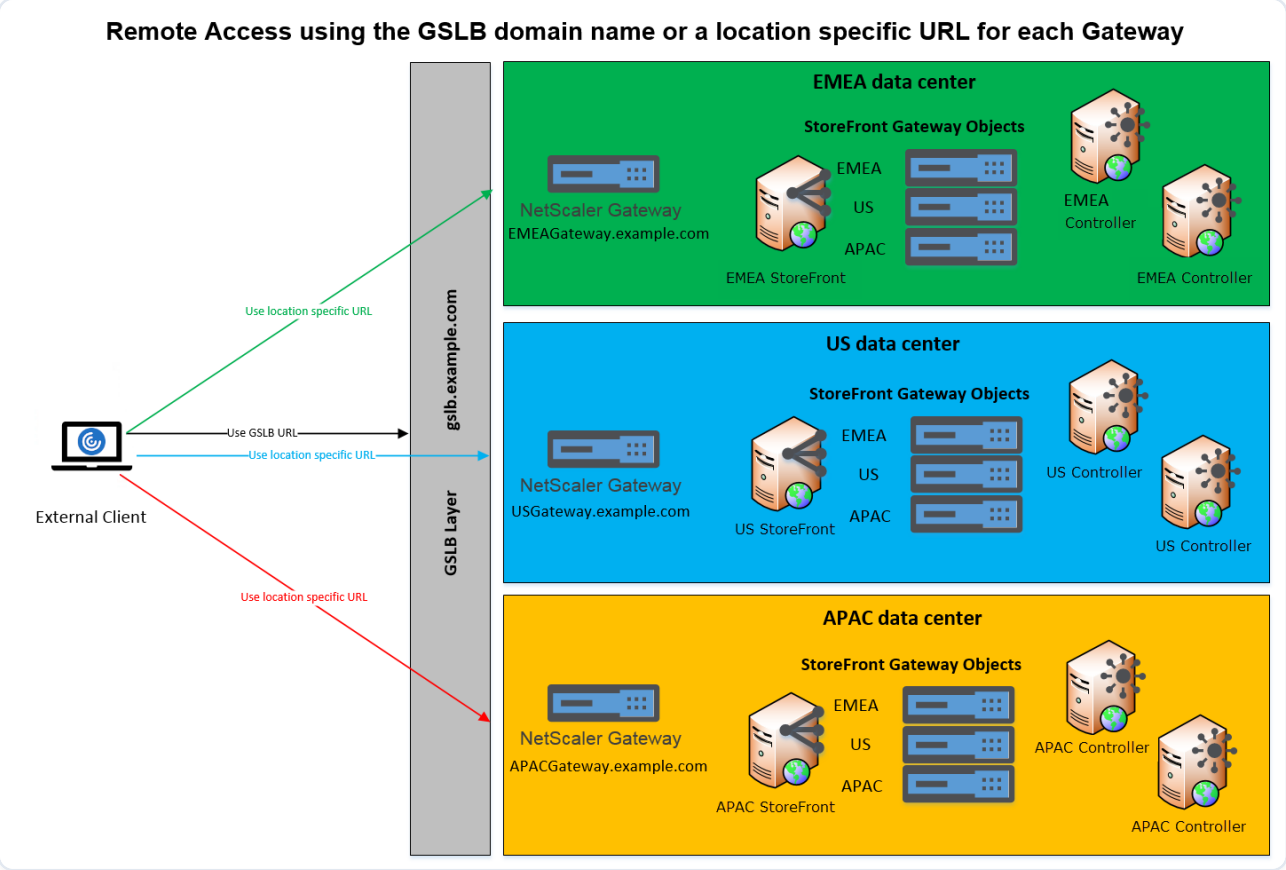
`emeagateway.example.com` – Gateway Europa

`usgateway.example.com` – Gateway USA

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

Zusammen mit einem GSLB:

`gslb.example.com`



Bevor Sie ein GSLB konfigurieren, überprüfen Sie, welche Serverzertifikate Sie verwenden und wie Ihre Organisation die DNS-Auflösung durchführt. Alle URLs, die Sie in Ihrer Citrix Gateway- und StoreFront-Bereitstellung verwenden möchten, müssen in Ihren Serverzertifikaten vorhanden sein.

StoreFront verfügt über keinen integrierten Mechanismus zur Synchronisierung der Konfiguration zwischen Servergruppen. Stattdessen liegt es in der Verantwortung des Administrators, sicherzustellen, dass jede StoreFront-Servergruppe auf die gleiche Weise konfiguriert ist, damit die Benutzer eine konsistente Erfahrung erhalten, unabhängig davon, mit welcher Servergruppe sie sich verbinden.

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

Wenn Sie der Citrix Workspace-App einen Store hinzufügen, identifiziert sie den Store anhand der Basis-URL und des Store-Namens. Wenn Sie also mehrere StoreFront-Bereitstellungen hinter einem GSLB haben, muss jede Bereitstellung dieselbe Basis-URL haben.

> **Hinweis:**

> Wenn die Citrix Workspace-App zwischen verschiedenen StoreFront-Bereitstellungen hinter einem GSLB wechselt, muss sich der Benutzer erneut authentifizieren. Daher sollten Sie die Persistenz konfigurieren, damit die Anforderungen eines Benutzers, wenn möglich, immer an dieselbe Bereitstellung weitergeleitet werden.

Benutzerzugriff

Siehe Optionen für den Benutzerzugriff.

Systemanforderungen

Bevor Sie StoreFront installieren, lesen Sie Planen Sie Ihre StoreFront-Bereitstellung.

Anforderungen an den StoreFront-Server

Software

Citrix hat StoreFront-Installationen auf den folgenden Plattformen getestet und bietet dafür Support:

- Windows Server 2025 Datacenter und Standard Editionen
- Windows Server 2022 Datacenter und Standard Editionen
- Windows Server 2019 Datacenter und Standard Editionen

> **Hinweis:**

> StoreFront erfordert die Windows-Desktop-Oberfläche und kann daher nicht auf Windows Server Core installiert werden.

> Alle StoreFront-Server in einer Servergruppe müssen dieselbe Betriebssystemversion, Sprache und Region verwenden.

Das Upgrade der Betriebssystemversion auf einem Server, auf dem StoreFront ausgeführt wird, wird nicht unterstützt. Citrix empfiehlt, StoreFront auf einer Neuinstallation des Betriebssystems zu installieren.

Bevor Sie StoreFront installieren können, müssen die folgenden Windows-Funktionen auf dem Webserver aktiviert sein. Diese Komponenten sind bei einer neuen Windows-Installation

standardmäßig aktiviert, sodass keine Maßnahmen erforderlich sind, es sei denn, sie wurden explizit deinstalliert.

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

Wenn die installierte Version von .NET Framework älter als 4.8.0 ist, installiert das Installationsprogramm automatisch .NET Framework 4.8.0. Dies erfordert, dass die Windows-Funktion **NET-Framework-45-Core** bereits installiert ist.

```
Starting with 2507 LTSR CU2, StoreFront requires .NET 10. If .NET 10 is
not already installed, the installer automatically installs it.



> **Note:**

>

> Earlier StoreFront builds (that is, 2507 and 2507 LTSR CU1) require .NET
8.
```

Wenn das StoreFront-Installationsprogramm feststellt, dass eine der folgenden Windows-Funktionen fehlt, werden diese 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 derselbe sein.

Hardware

Storefront™-Server müssen die folgenden Anforderungen erfüllen:

- Prozessor: Mindestens 2 virtuelle CPUs, empfohlen 4 virtuelle CPUs
- RAM: 4 GB, zuzüglich 700 Byte pro verfügbarer Ressource pro Benutzer.
- Speicherplatz:
    - 250 MB für StoreFront selbst.

- 30 MB für jeden Store, vorausgesetzt, es gibt eine Website pro Store.
- Für jeden Store, bei dem Favoriten aktiviert sind, 5 MB zuzüglich 8 MB für jeweils 1000 Favoriten.
- Ausreichend Speicherplatz für IIS-Protokolldateien gemäß Ihren Anforderungen, siehe Microsoft-Dokumentation zum Verwalten des IIS-Protokolldateispeichers.
- Ausreichend Speicherplatz für StoreFront-Diagnoseprotokolle. Standardmäßig speichert StoreFront 1 GB Protokolle pro Dienst. Eine StoreFront-Bereitstellung umfasst typischerweise 1 Roaming-Dienst plus 3 Dienste pro Store (Store-Dienst, Authentifizierungsdienst und Receiver für Web-Dienst). Weitere Informationen finden Sie unter Protokolldateien.

Netzwerk

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

- Clients stellen eine Verbindung zu StoreFront über HTTPS oder HTTP her, normalerweise über TCP-Port 443 bzw. 80. Sie können Clients erlauben, sich direkt mit StoreFront zu verbinden, jedoch verbinden sich Clients üblicherweise mit einem Lastenausgleich oder Gateway, der den Datenverkehr an StoreFront weiterleitet. Sie können die verwendeten Ports in der IIS-Konfiguration ändern. Es wird empfohlen, HSTS zu verwenden, um Webbrowser zur Verwendung von HTTPS zu zwingen.
- TCP-Port 808 wird verwendet für:
  - Synchronisierung von Favoriten innerhalb einer Servergruppe. Dies gilt nur, wenn Favoriten aktiviert sind und Sie die lokale Datenbank anstelle einer externen SQL-Server-Datenbank verwenden.
  - Synchronisierung von Abonnements zwischen Servergruppen. Dies gilt nur, wenn Sie Abonnements synchronisieren aktiviert haben.
- Ein zufällig aus allen nicht reservierten Ports ausgewählter TCP-Port wird für die Kommunikation zwischen den StoreFront-Servern in einer Servergruppe verwendet.
- Wenn Sie einen NetScaler-Lastenausgleich mit einem StoreFront-Monitor verwenden, muss dieser eine Verbindung zum Citrix Service Monitor herstellen. Standardmäßig läuft dieser auf TCP-Port 8000, kann aber alternativ so konfiguriert werden, dass er über HTTPS auf Port 443 läuft. Siehe Lastenausgleich mit NetScaler ADC.

Wenn Sie StoreFront installieren, werden Windows-Firewallregeln konfiguriert, die den Zugriff auf die StoreFront-Ausführungsdateien ermöglichen. Sie müssen sicherstellen, dass Firewalls oder andere Geräte in Ihrem internen Netzwerk den Datenverkehr zu nicht zugewiesenen TCP-Ports nicht blockieren.

StoreFront unterstützt sowohl reine IPv6-Netzwerke als auch Dual-Stack-IPv4/IPv6-Umgebungen.

Active Directory

Viele StoreFront-Funktionen erfordern, dass der Windows-Server, auf dem StoreFront installiert ist, einer Active Directory-Domäne beigetreten ist. StoreFront kann nicht auf einem Domänencontroller installiert werden.

Damit StoreFront Benutzer gegenüber Microsoft Active Directory authentifizieren kann, stellen Sie sicher, dass der StoreFront-Server entweder der Domäne mit den Benutzerkonten oder einer Domäne beigetreten ist, die eine Vertrauensstellung zur Benutzerkontendomäne hat. Dies ist immer für Domänen-Pass-Through erforderlich. Für die Benutzername- und Kennwort-Authentifizierung ist dies standardmäßig erforderlich; alternativ können Sie StoreFront so konfigurieren, dass die Authentifizierung an die Delivery Controller delegiert wird.

Wenn Sie StoreFront auf einem Server installieren, der keiner Domäne beigetreten ist, sind die folgenden Funktionen nicht verfügbar:

- Servergruppen
- Favoriten
- Authentifizierungsmethoden außer explizitem Benutzernamen 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

Sie können optional Abonnementdaten mit Microsoft SQL Server speichern. StoreFront unterstützt dafür dieselben Microsoft SQL Server-Versionen wie Citrix Virtual Apps and Desktops für Datenbanken. In den Systemanforderungen von Citrix Virtual Apps and Desktops finden Sie weitere Informationen unter Datenbanken.

Infrastrukturanforderungen

Citrix hat StoreFront getestet und bietet Support für die Verwendung mit den folgenden Citrix Produktversionen.

Citrix Virtuelle Apps und Desktops™

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

- Citrix Virtual Apps und Desktops 2507 LTSR
- Citrix Virtual Apps und Desktops 2503
- Citrix Virtual Apps und Desktops 2411
- Citrix Virtual Apps und Desktops 2407
- Citrix Virtual Apps und Desktops 2402 LTSR
- Citrix Virtual Apps und Desktops 2203 LTSR

Citrix Gateway

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

- Citrix Gateway 14.1
- Citrix Gateway 13.1

Verbindungen über Citrix Gateway können über den ICA-Proxy, das Citrix Gateway Plug-In oder clientloses VPN (cVPN) hergestellt werden.

Anforderungen an Benutzergeräte

StoreFront bietet Benutzern verschiedene Optionen für den Zugriff auf ihre Desktops und Anwendungen. Citrix-Benutzer können entweder über die lokal installierte Citrix Workspace-App oder in ihrem Browser auf Stores zugreifen. Weitere Informationen finden Sie unter Benutzerzugriffsoptionen.

Citrix Workspace-App

Sie können alle derzeit unterstützten Versionen der Citrix Workspace-App verwenden, um von internen Netzwerkverbindungen und über ein Citrix Gateway auf StoreFront-Stores zuzugreifen. Informationen zu den Lebenszyklusdaten der Citrix Workspace-App finden Sie unter `<https://www.citrix.com/support/product-lifecycle/workspace-app.html>`.

Ältere Versionen von Citrix Workspace™ App und Citrix Receiver™ funktionieren möglicherweise, werden aber nicht unterstützt.

Auf Android, iOS und iPadOS ist es mit Citrix Workspace-App-Versionen vor 24.12 nicht möglich, über ein Gateway eine Verbindung zu einem Store herzustellen, der mit der modernen Oberfläche konfiguriert ist.

Webbrowser

Endbenutzer können über einen Webbrowser auf Stores zugreifen. Apps und Desktops können entweder über eine lokal installierte Citrix Workspace-App (bekannt als Hybrid-Start) oder innerhalb des Webbrowsers gestartet werden. Abhängig von Ihrer Websitekonfiguration ist es möglich, dass 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*

* Internet Explorer kann verwendet werden, um eine Verbindung zu Store-Websites herzustellen, die für die klassische Erfahrung und nicht für die moderne Erfahrung konfiguriert sind. Der HTML5 HDX-Client unterstützt Internet Explorer nicht, daher müssen Sie die Citrix Workspace-App verwenden, um eine Verbindung zu Ressourcen herzustellen.

Unter 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.

Citrix Weberweiterungen

Für eine verbesserte Benutzererfahrung wird empfohlen, dass Benutzer die Citrix Weberweiterung zu ihrem Webbrowser hinzufügen. Die Anforderungen finden Sie unter Citrix Weberweiterung.

Legacy-Geräte

Ältere Citrix Clients können XenApp Services-URLs verwenden, um auf StoreFront-Stores mit reduzierter Funktionalität zuzugreifen. XenApp Services-URLs bieten abwärtskompatible Legacy-Unterstützung für Verbindungen, die von Citrix Receiver 3.4 Enterprise und älteren Clients hergestellt werden. Diese Funktionalität ist veraltet und wird in einer zukünftigen Version entfernt.

Smartcard-Anforderungen

Verwenden der Citrix Workspace-App mit Smartcards

Citrix testet die Kompatibilität mit der Common Access Card (CAC) des US-Verteidigungsministeriums, den Personal Identity Verification (NIST PIV)-Karten des US National Institute of Standards and Technology und einigen USB-Smartcard-Tokens. Sie können Kontaktkartenleser verwenden, die der USB Chip/Smart Card Interface Devices (CCID)-Spezifikation entsprechen und vom Zentralen Kreditausschuss (ZKA) als Smartcard-Leser der Klasse 1 klassifiziert sind. ZKA-Kontaktkartenleser der Klasse 1 erfordern, dass Benutzer ihre Smartcards in das Lesegerät einführen. Andere Arten von Smartcard-Lesern, einschließlich Lesegeräten der Klasse 2 (die über Tastaturen zur PIN-Eingabe verfügen), kontaktlosen Lesegeräten und virtuellen Smartcards, die auf Trusted Platform Module (TPM)-Chips basieren, werden nicht unterstützt.

Für Windows-Geräte basiert die Smartcard-Unterstützung auf den Microsoft Personal Computer/Smart Card (PC/SC)-Standardspezifikationen. Als Mindestanforderung müssen Smartcards und Kartenleser vom Betriebssystem unterstützt werden und eine Windows-Hardwarezertifizierung erhalten haben.

Weitere Informationen zu Citrix-kompatiblen Smartcards und Middleware finden Sie unter Smartcards in der Dokumentation zu Citrix Virtual Apps and Desktops und `<http://www.citrix.com/ready>`.

Anforderungen an den Citrix Analytics-Dienst

Sie können Citrix StoreFront so konfigurieren, dass die Citrix Workspace-App Daten an den Citrix Analytics-Dienst senden kann. Konfigurationsdetails werden in Citrix Analytics-Dienst 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.

Ressourcen konfigurieren

Berücksichtigen Sie beim Bereitstellen von Ressourcen mit Citrix Virtual Apps and Desktops, Citrix Desktops as a Service oder Secure Private Access Folgendes bei der Konfiguration von Ressourcen. Weitere Informationen zur Bereitstellung von Anwendungen mit Citrix Virtual Apps and Desktops finden Sie unter Anwendungen.

- Geben Sie den Ressourcennamen so ein, wie er in Ihrem Store angezeigt werden soll.
- Geben Sie optional eine Beschreibung ein. Diese wird im Store angezeigt, wenn Sie die App-Details erweiternieren, zusammen mit allen Schlüsselwörtern.
- Wählen Sie ein Symbol, damit Benutzer eine Anwendung auf der StoreFront-Website visuell erkennen können.
- Geben Sie optional eine Kategorie ein. Fügen Sie `\` in den Kategorienamen ein, um eine Ordnerhierarchie zu erstellen. Sie könnten beispielsweise Anwendungen nach Typ gruppieren oder alternativ Ordner für verschiedene Benutzerrollen in Ihrer Organisation erstellen. Auf der Store-Website zeigt die Registerkarte **Apps**, Ansicht **Kategorie** eine Liste der Kategorien und die Apps in jeder Kategorie an.

Schlüsselwörter

Sie können einer Ressource Schlüsselwörter hinzufügen, indem Sie die Zeichenfolge `KEYWORDS:[keywordname]` an die Anwendungsbeschreibung anhängen. Mehrere Schlüsselwörter müssen nur durch Leerzeichen getrennt werden; zum Beispiel `KEYWORDS:Accounts Featured`. Schlüsselwörter können auf verschiedene Weisen verwendet werden:

- Anwendungen filtern – siehe Erweiterte Store-Einstellungen.
- Empfohlene App-Gruppen erstellen.
- Einige Schlüsselwörter haben eine besondere Bedeutung.

SCHLÜSSELWORTNAME	BESCHREIBUNG
Obligatorisch	Fügt eine Anwendung zur Registerkarte „Startseite“ hinzu. Im Gegensatz zu Favoriten können Benutzer obligatorische Anwendungen

SCHLÜSSELWORTNAME	BESCHREIBUNG
	nicht von der Registerkarte „Startseite“ entfernen. Hat keine Auswirkung, wenn Favoriten für den Store deaktiviert sind.
Auto	Wenn sich Benutzer am Store anmelden, wird die Anwendung oder der Desktop automatisch als Favorit markiert und ihrer Registerkarte „Startseite“ hinzugefügt. Benutzer können solche Anwendungen aus den Favoriten entfernen. Hat keine Auswirkung, wenn Favoriten für den Store deaktiviert sind.
TreatAsApp	Auf Desktops anwenden, um StoreFront zu zwingen, ihn als App zu behandeln. Der Desktop wird auf der Registerkarte **Apps** anstatt auf der Registerkarte **Desktops** angezeigt. Darüber hinaus wird der Desktop nicht automatisch gestartet, wenn sich der Benutzer bei der Store-Website anmeldet, und er wird nicht mit dem Desktop Viewer aufgerufen, selbst wenn die Site so konfiguriert ist, dass dies für andere Desktops geschieht.
prefer="*application*"	Wobei *application* eine lokal installierte Anwendung identifiziert. Gilt nur für veröffentlichte Apps in der Citrix Workspace-App unter Windows. Dies weist darauf hin, dass die lokal installierte Version einer Anwendung gegenüber der entsprechenden bereitgestellten Instanz bevorzugt werden sollte, wenn beide verfügbar sind. Weitere Informationen finden Sie unter Konfigurieren von Local App Access-Anwendungen.
Primary und **Secondary**	Bei Verwendung von Multi-Site-Aggregation wird diejenige mit dem Schlüsselwort **primary** immer derjenigen mit dem Schlüsselwort **secondary** vorgezogen.

Smart Access-Tags

StoreFront™ legt bestimmte Smart Access-Tags fest. Sie können in Studio Zugriffsrichtlinien definieren, die verwendet werden können, um den Zugriff auf eine Bereitstellungsgruppe basierend auf diesen Smart Access-Tags zu erlauben oder zu verweigern. Dies erfordert:

- Citrix Virtual Apps and Desktops 2407 oder höher. Weitere Informationen finden Sie unter Informationen zu Zugriffsrichtlinienregeln.
- Citrix Desktops as a Service. Weitere Informationen finden Sie unter Informationen zu Zugriffsrichtlinienregeln.

StoreFront legt die folgenden Smart Access-Tags fest:

NAME	BESCHREIBUNG	BEISPIEL
`Citrix.ClientUserAgent`	Der User-Agent des Clients	`Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36`
`Citrix.StoreFrontStoreUrl`	Die URL des Stores, mit dem der Benutzer verbunden ist	`https://storefront.example.com/Citrix/Store`

StoreFront installieren

Vor der Installation

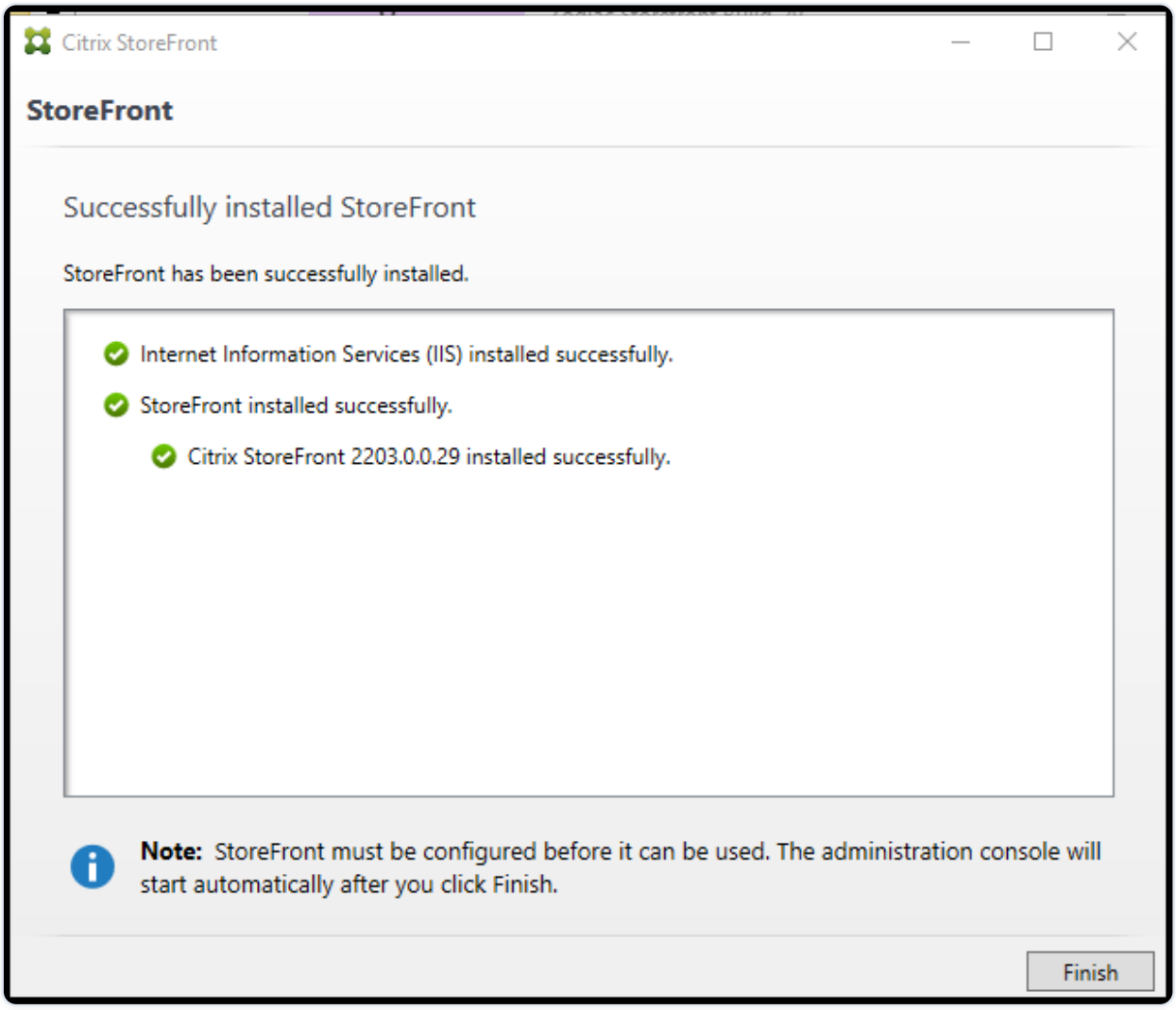
Bevor Sie StoreFront installieren und konfigurieren, lesen Sie die Systemanforderungen.

StoreFront installieren

> **Wichtig**

> Um potenzielle Fehler und Datenverluste bei der Installation von StoreFront zu vermeiden, stellen Sie sicher, dass alle Anwendungen geschlossen sind und keine anderen Aufgaben oder Operationen auf dem Zielsystem ausgeführt werden.

1. Laden Sie das Installationsprogramm von der StoreFront-Downloadseite herunter. Das Installationsprogramm finden Sie auch auf dem Citrix Virtual Apps and Desktops-Image im Verzeichnis `\x64\Storefront`.
2. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen am StoreFront-Server an.
3. Suchen Sie die Datei CitrixStoreFront-x64.exe und führen Sie sie als Administrator aus.
4. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
5. Wenn die Seite „Voraussetzungen überprüfen“ angezeigt wird, klicken Sie auf **Weiter**.
6. Überprüfen Sie auf der Seite „Bereit zur Installation“ die aufgeführten Voraussetzungen und StoreFront-Komponenten für die Installation und klicken Sie auf **Installieren**.
7. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**.



8. StoreFront fordert Sie möglicherweise auf, einen Neustart durchzuführen, um die Installation abzuschließen. Klicken Sie auf **Ja**, um jetzt neu zu starten.

9. Konfigurieren Sie Microsoft Internet Information Services (IIS) für HTTPS. Schritte dazu finden Sie unter StoreFront mit HTTPS sichern.

So installieren Sie StoreFront an einer Eingabeaufforderung

1. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen am StoreFront-Server an.
2. Navigieren Sie zu Ihrem Installationsmedium oder Downloadpaket, suchen Sie die Datei CitrixStoreFront-x64.exe und kopieren Sie die Datei an einen temporären Speicherort auf dem Server.
3. Navigieren Sie an einer Eingabeaufforderung 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]
   ```

   Verwenden Sie das Argument **-silent**, um StoreFront und seine Voraussetzungen im Hintergrund zu installieren. Standardmäßig wird StoreFront unter C:\Program Files\Citrix\Receiver StoreFront installiert. Sie können jedoch einen anderen Installationspfad mit dem Argument **-INSTALLDIR** angeben, wobei *Installationspfad* das Verzeichnis ist, in dem StoreFront installiert werden soll. Wenn der Server Teil einer Servergruppe sein soll, müssen sowohl der StoreFront-Installationspfad als auch die IIS-Websiteeinstellungen, der physische Pfad und die Site-IDs konsistent sein.

   Wenn ein Benutzer einen Store in einem Webbrowser unter Windows oder macOS öffnet und die Citrix Workspace-App standardmäßig nicht erkannt werden kann, wird der Benutzer aufgefordert, die entsprechende Citrix Workspace-App für seine Plattform von der Citrix-Website herunterzuladen und zu installieren. Sie können dieses Verhalten so ändern, dass Benutzer die Installationsdateien der Citrix Workspace-App stattdessen vom StoreFront-Server herunterladen. Weitere Informationen finden Sie unter Konfigurieren der Ressourcenanzeige für Benutzer.

   Wenn Sie diese Konfigurationsänderung vornehmen möchten, geben Sie die Argumente **-WINDOWS_CLIENT** und **-MAC_CLIENT** an, um die Installationsdateien von Citrix Receiver für Windows oder Citrix Workspace-App für Windows bzw. Citrix Receiver für Mac oder Citrix Workspace-App für Mac an den entsprechenden Speicherort in Ihrer StoreFront-Bereitstellung zu kopieren. Ersetzen Sie *Dateispeicherort* durch das Verzeichnis, das die zu kopierende Installationsdatei enthält, und *Dateiname* durch den Namen der Installationsdatei. Die

Installationsdateien von Citrix Workspace-App für Windows und Citrix Receiver für Mac oder Citrix Workspace-App für Mac sind auf Ihrem Installationsmedium für Citrix Virtual Apps and Desktops enthalten.

Neustartschritt für .Net Framework 4.8 unter Windows Server 2019

Das .Net Framework 4.8 ist eine vorinstallierte Komponente unter Windows Server 2022, jedoch nicht unter Windows Server 2019. Der Installer CitrixStoreFront-x64.exe führt den .Net Framework 4.8-Installer aus, falls dieser nicht vorhanden ist. Wenn vorhandene .Net Framework-Bibliotheken verwendet werden, kann ein Serverneustart erforderlich sein, damit die Installation von .Net Framework 4.8 abgeschlossen werden kann, bevor StoreFront installiert werden kann. Dies kann auftreten, wenn eine PowerShell-Sitzung ausgeführt wird.

Wenn ein Neustart erforderlich ist, wird die CitrixStoreFront-x64.exe beendet und muss anschließend manuell neu gestartet werden. Erfolgt die Installation im Hintergrundmodus, wird sie mit einem Fehlercode beendet; andernfalls wird der Benutzer aufgefordert, den Neustart zuzulassen. Der Prozess CitrixStoreFront-x64.exe gibt in diesen Situationen jeden Exit-Code des .Net Framework 4.8-Installers zurück, der keinen Erfolg anzeigt. Die spezifischen Neustart-Exit-Codes sind:

- ERROR_SUCCESS_REBOOT_REQUIRED **3010**
- ERROR_SUCCESS_REBOOT_INITIATED **1641**

Für die unbeaufsichtigte Installation von CitrixStoreFront-x64.exe über ein PowerShell-Skript installieren Sie .Net Framework 4.8 auf dem Server vor, falls es noch nicht vorhanden ist.

Installation als Teil von Citrix Virtual Apps and Desktops™

Sie können StoreFront auf demselben Server wie Citrix Virtual Apps and Desktops installieren. Führen Sie den Citrix Virtual Apps and Desktops-Installer aus und wählen Sie unter **Bereitstellung erweitern** die Option **Citrix StoreFront**.

Installationsprotokolle

Weitere Informationen zu Protokolldateien finden Sie unter Protokolldateien.

StoreFront konfigurieren

Nach Abschluss der Installation wird die Citrix StoreFront-Verwaltungskonsole automatisch gestartet. Sie können StoreFront auch über das Startmenü öffnen. Wenn die Citrix StoreFront-Verwaltungskonsole zum ersten Mal gestartet wird, stehen zwei Optionen zur Verfügung.

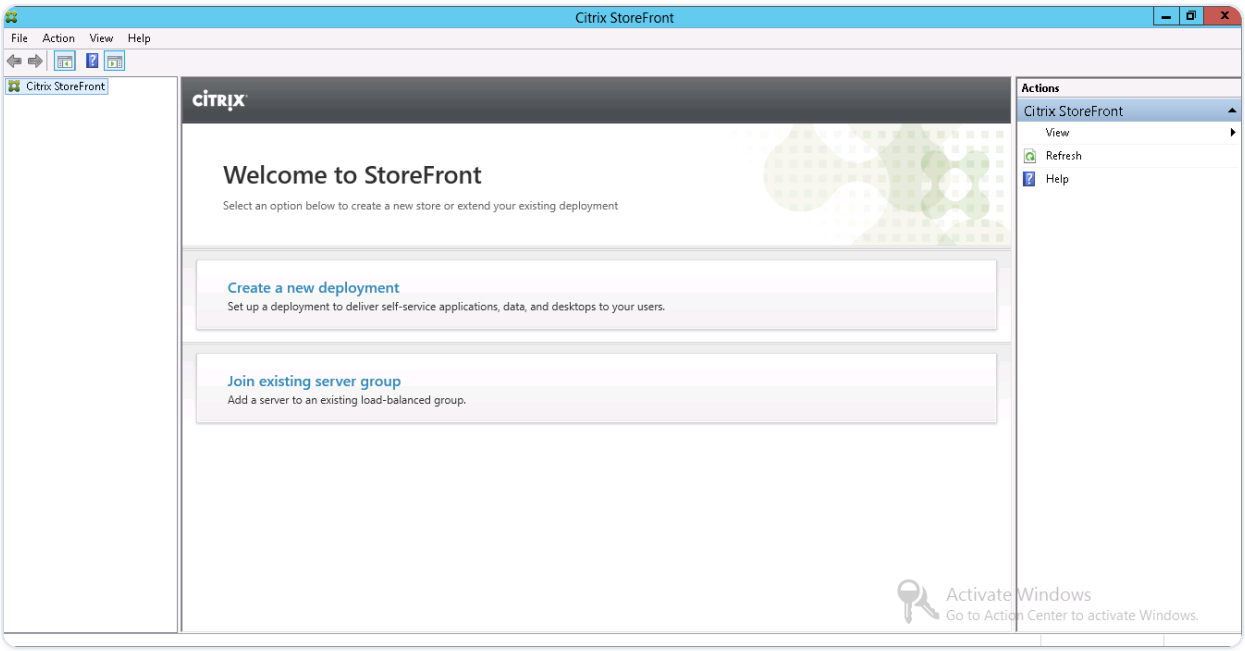
Screenshot von Willkommen bei StoreFront(/en-us/storefront/2507-ltsr/media/get-started/welcome-to-storefront.png)

- Bereitstellung erstellen. Konfigurieren Sie den ersten Server in einer neuen StoreFront-Bereitstellung. Einzelserver-Bereitstellungen sind ideal für die Evaluierung von StoreFront oder für kleine Produktionsbereitstellungen. Sobald Sie Ihren ersten StoreFront-Server konfiguriert haben, können Sie jederzeit weitere Server zur Gruppe hinzufügen, um die Kapazität Ihrer Bereitstellung zu erhöhen.
- Vorhandener Servergruppe beitreten. Fügen Sie einen weiteren Server zu einer vorhandenen StoreFront-Bereitstellung hinzu. Wählen Sie diese Option, um die Kapazität Ihrer StoreFront-Bereitstellung schnell zu erhöhen. Für Bereitstellungen mit mehreren Servern ist ein externes Lastenausgleich erforderlich. Um einen Server hinzuzufügen, benötigen Sie Zugriff auf einen vorhandenen Server in der Bereitstellung.

Ihr Store ist jetzt für Benutzer über einen Browser oder die lokal installierte Citrix Workspace-App zugänglich. Siehe Benutzererfahrung.

Neue Bereitstellung erstellen

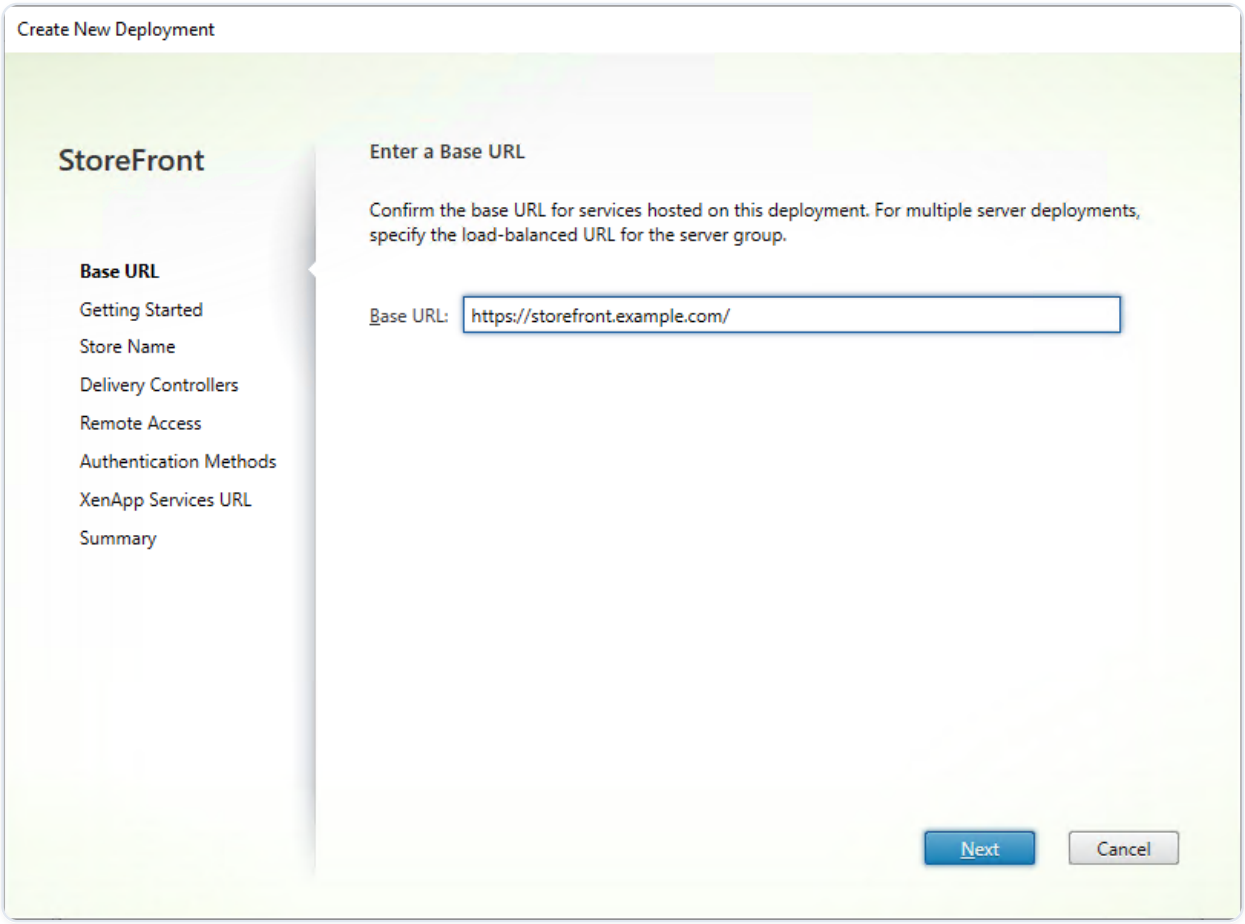
1. Wenn die StoreFront Verwaltungskonsole nach der Installation von StoreFront noch nicht geöffnet ist, öffnen Sie sie.



2. Klicken Sie im Ergebnisbereich der Citrix StoreFront-Verwaltungskonsole auf **Neue Bereitstellung erstellen**.
3. Wenn mehrere IIS-Sites vorhanden sind, wählen Sie im Dropdown-Menü **IIS-Site** die Site aus, die Sie verwenden möchten.

4. Wenn Sie einen einzelnen StoreFront-Server verwenden, geben Sie die Server-URL als **Basis-URL** ein. Wenn Sie mehrere StoreFront-Server hinter einem Lastenausgleich konfigurieren, geben Sie die Lastenausgleichs-URL als **Basis-URL** ein.

   Wenn Sie Ihre Lastenausgleichsumgebung noch nicht eingerichtet haben, geben Sie die Server-URL ein. Sie können die Basis-URL für Ihre Bereitstellung jederzeit ändern.



5. Klicken Sie auf **Weiter**, und konfigurieren Sie Ihren ersten Store, wie unter Store erstellen beschrieben.
6. Nachdem Sie alle Konfigurationsschritte abgeschlossen haben, 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**.

Neue Bereitstellung mit PowerShell erstellen

Um eine Bereitstellung mit PowerShell zu erstellen, führen Sie das Cmdlet Add-STFDeployment aus.

Mehrere Internet Information Services (IIS)-Websites

StoreFront ermöglicht es Ihnen, verschiedene Stores in verschiedenen IIS-Websites pro Windows-Server bereitzustellen, sodass jeder Store einen anderen Hostnamen und eine andere Zertifikatbindung haben kann.

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

Es ist nicht möglich, mehrere StoreFront-Bereitstellungen über die Verwaltungskonsole zu erstellen; Sie müssen PowerShell verwenden. Um beispielsweise zwei IIS-Website-Bereitstellungen zu erstellen, eine für Anwendungen und eine für Desktops, verwenden Sie die folgenden Befehle:

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"

Add-STFDeployment -SiteID 2 -HostBaseURL "https://desktops.example.com"
```

Sobald Sie mehrere Sites aktiviert haben, deaktiviert StoreFront die Verwaltungskonsole, und es ist nicht möglich, StoreFront in den Einzelsite-Modus zurückzuversetzen. Sie müssen die gesamte StoreFront-Konfiguration mithilfe der PowerShell-Module durchführen und `SiteID` in jeden Befehl aufnehmen.

Endbenutzerzugriff

Drei verschiedene Methoden stehen Benutzern zur Verfügung, um auf StoreFront-Stores zuzugreifen.

- Lokal installierte Citrix Workspace-App – Benutzer mit kompatiblen Versionen der Citrix Workspace-App können innerhalb der Benutzeroberfläche der Citrix Workspace-App auf StoreFront-Stores zugreifen. Dies bietet die beste Benutzererfahrung und die größte Funktionalität.
- Webbrowser – Benutzer mit kompatiblen Webbrowsern können auf StoreFront-Stores zugreifen, indem sie die Website des Stores aufrufen. Standardmäßig benötigen Benutzer auch eine kompatible Version der Citrix Workspace-App, um auf ihre Desktops und Anwendungen zuzugreifen, was als hybrider Start bezeichnet wird. Sie können Ihre Website jedoch so konfigurieren, dass Benutzer über ihren Browser auf ihre Ressourcen zugreifen können, ohne die Citrix Workspace-App installieren zu müssen.

- XenApp® Services-URLs – Benutzer mit älteren Citrix®-Clients, die nicht aktualisiert werden können, können über die XenApp Services-URL des Stores auf Stores zugreifen. Wenn Sie einen neuen Store erstellen, ist die XenApp Services-URL standardmäßig aktiviert.

Citrix Workspace™-App

Der Zugriff auf Stores über die lokal installierte Citrix Workspace-App bietet die beste und sicherste Benutzererfahrung. Informationen zu den Versionen der Citrix Workspace-App, die für den Zugriff auf Stores auf diese Weise verwendet werden können, finden Sie unter Systemanforderungen.

Die Citrix Workspace-App bietet im Vergleich zur Verwendung eines Webbrowsers die folgenden Vorteile:

- **Verbesserte Sicherheit**, da `.ica`-Dateien sicher verarbeitet und niemals heruntergeladen werden.
- **Verbesserte Zuverlässigkeit** beim Öffnen von Apps und Desktops, ohne dass Citrix-Weberweiterungen bereitgestellt werden müssen.
- **Integrierter App Protection-Dienst** bietet eine zusätzliche Sicherheitsebene zum Schutz vor Keylogging- und Screen-Capturing-Malware.
- **Bessere Telemetrie**, da die native App umfangreiche Informationen für Überwachungszwecke bietet.
- **Erweiterte HDX™-Funktionen** mit verbesserten Features wie optimierter Codec-Komprimierung und effizienter Audio-Video-Komprimierung. Diese Verbesserungen gewährleisten hohe Qualität und Leistung bei Aufgaben, die hochauflösende Inhalte oder grafikintensive Apps umfassen.

Typischerweise hat ein Store eine einzelne Website, die in der Citrix Workspace-App angezeigt wird. Es ist möglich, mehrere Websites zu konfigurieren. In diesem Fall können Sie konfigurieren, welche Website in der Citrix Workspace-App angezeigt wird.

Beacons

Die Citrix Workspace-App verwendet interne und externe URLs als Beacon-Punkte. Durch den Versuch, diese Beacon-Punkte zu kontaktieren, kann die Citrix Workspace-App feststellen, ob Benutzer mit lokalen oder öffentlichen Netzwerken verbunden sind. Sie verwendet diese Informationen, um direkt eine Verbindung zu StoreFront oder über ein Citrix Gateway herzustellen. Weitere Informationen finden Sie unter Beacon-Punkte konfigurieren.

Nutzung der Citrix Workspace-App erforderlich

Sie können StoreFront so konfigurieren, dass, wenn Benutzer eine Store-Website in ihrem Browser öffnen, die Citrix Workspace-App automatisch geöffnet wird und Benutzer nicht in ihrem Webbrowser fortfahren können. Wird die Citrix Workspace-App nicht erkannt, bietet die Website dem Benutzer die Möglichkeit, sie zu installieren. Darüber hinaus konfiguriert die Website die Citrix Workspace-App automatisch so, dass sie eine Verbindung zum Store herstellt. Weitere Informationen finden Sie unter Verwendung der Citrix Workspace-App erzwingen. Diese Funktionalität kann auch im Citrix Gateway mithilfe eines Plug-Ins implementiert werden; siehe Citrix Workspace-App bei Verbindung über ein Gateway erforderlich.

Store zur Citrix Workspace-App hinzufügen

Nach der Installation muss die Citrix Workspace-App mit den Verbindungsdetails für die Stores konfiguriert werden, die die Desktops und Anwendungen der Benutzer bereitstellen. Sie können die Citrix Workspace-App mithilfe der Store-URL, einer Bereitstellungsdatei oder durch Konfigurieren der E-Mail-Erkennung konfigurieren.

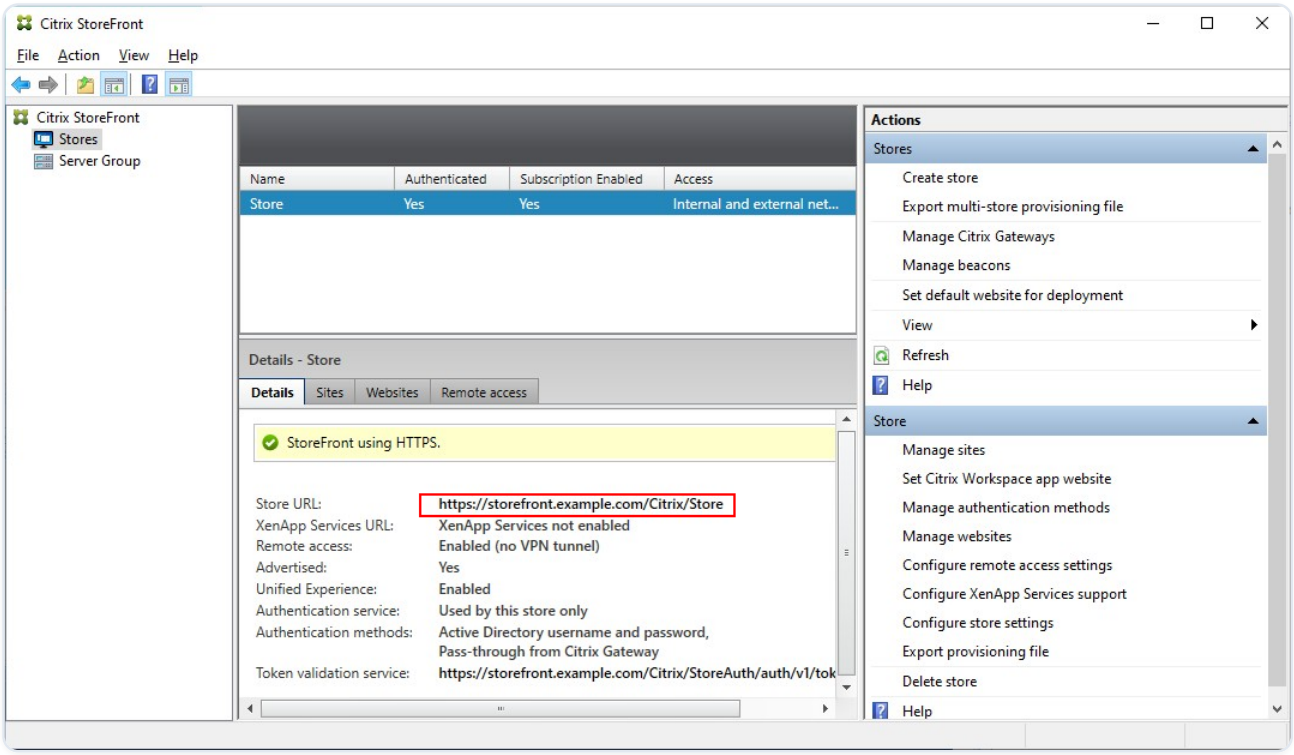
Weitere Informationen zum Konfigurieren der Citrix Workspace-App für Windows finden Sie unter Citrix Workspace-App für Windows-Dokumentation.

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, in einer Produktionsumgebung keine ungesicherten Benutzerverbindungen zu StoreFront zu aktivieren. Weitere Informationen finden Sie unter Store-Konfigurationsparameter in der Dokumentation zur Citrix Workspace-App für Windows.

Store-URL

Um die Store-URL zu erhalten, wählen Sie in der Verwaltungskonsole den Store aus. Die Store-URL wird in den Store-Details angezeigt.



.

Wenn Sie mit der rechten Maustaste auf die Store-URL klicken, gibt es eine Option, diese in die Zwischenablage zu kopieren.

Bereitstellungsdateien

Sie können Benutzern Bereitstellungsdateien mit Verbindungsdetails für ihre Stores zur Verfügung stellen. Nach der Installation der Citrix Workspace-App öffnen Benutzer die CR-Datei, um Konten für die Stores automatisch zu konfigurieren. Standardmäßig bietet die Website Benutzern eine Bereitstellungsdatei für den einzelnen Store an, für den die Site konfiguriert ist. Sie könnten Ihre Benutzer anweisen, die Websites der Stores zu besuchen, auf die sie zugreifen möchten, und Bereitstellungsdateien von diesen Sites herunterzuladen. Alternativ können Sie für ein höheres Maß an Kontrolle die Citrix StoreFront-Verwaltungskonsole verwenden, um Bereitstellungsdateien mit Verbindungsdetails für einen oder mehrere Stores zu generieren. Sie können diese Dateien dann an die entsprechenden Benutzer verteilen. Weitere Informationen finden Sie unter Bereitstellungsdateien für Stores für Benutzer exportieren.

Global App Config Service

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

Webbrowser

Als Alternative zur Verwendung einer lokal installierten Citrix Workspace-App können Benutzer über einen Webbrowser auf ihren Store zugreifen.

Normalerweise gibt es eine einzige Website für einen Store, aber Sie können mehrere Websites konfigurieren, jede mit ihrer eigenen URL und Konfiguration. Weitere Informationen finden Sie unter Websites verwalten.

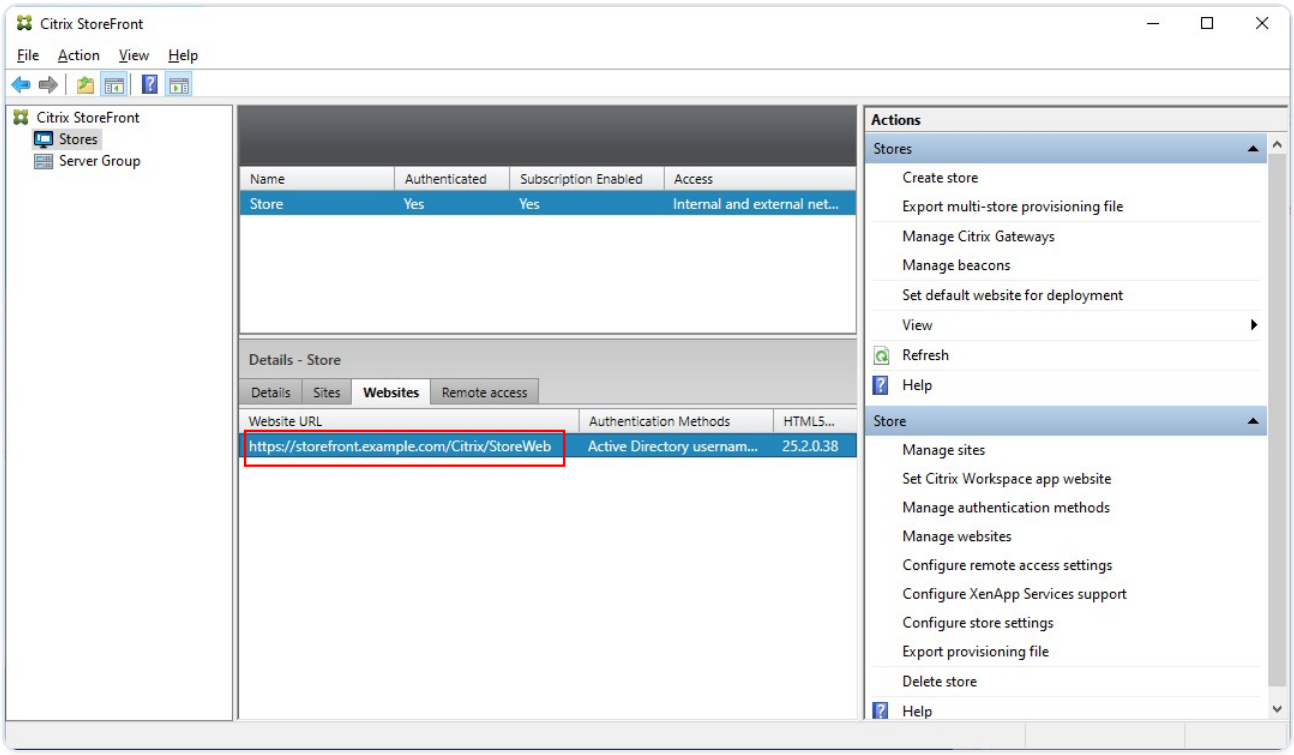
Interne Benutzer können direkt zur Store-Website-URL navigieren. Wenn in Ihrer StoreFront-Bereitstellung mehrere Websites vorhanden sind, können Sie eine davon als Standard-URL konfigurieren, zu der Benutzer umgeleitet werden, wenn sie zur Basis-URL navigieren.

Wenn Sie ein Citrix Gateway bereitgestellt haben, navigieren externe Benutzer zur Gateway-URL. Dies ist normalerweise eine andere URL, kann aber so konfiguriert werden, dass sie dieselbe URL verwendet.

Hinweis:

Die über einen Webbrowser verwendete Store-Website-URL unterscheidet sich von der Store-URL, die zum Konfigurieren der Citrix Workspace-App verwendet wird.

Um die Store-Website-URL zu erhalten, wählen Sie in der Verwaltungskonsole den Store aus. Die Website-URLs werden auf der Registerkarte **Websites** angezeigt.



Wenn Sie mit der rechten Maustaste auf die Website-URL klicken, gibt es eine Option, diese in die Zwischenablage zu kopieren.

Wenn Benutzer ihre Ressourcen starten möchten, gibt es zwei Möglichkeiten:

1. Ressourcen werden in der lokal installierten Citrix Workspace-App gestartet. Dies wird als Hybrid-Start bezeichnet. Dies bietet Benutzern die beste Erfahrung, da die vollständige Betriebssystemintegration genutzt werden kann. Weitere Informationen finden Sie unter Hybrid-Start
2. Ressourcen werden im Browser gestartet. Dies ermöglicht Benutzern den Zugriff auf Ressourcen, ohne dass Software lokal installiert werden muss.

Die Standardkonfiguration erfordert, dass die Citrix Workspace-App für einen Hybrid-Start lokal installiert ist. Sie können die Konfiguration ändern, um Ressourcen entweder immer im Browser zu starten oder dem Benutzer die Wahl zu lassen. Siehe Workspace-App bereitstellen.

Wenn der Administrator **Benutzer wählen lassen** ausgewählt hat, hat der Benutzer, wenn er die Store-Website zum ersten Mal in seinem Browser öffnet, die Möglichkeit, auf **Webbrowser verwenden** zu klicken, um Ressourcen in seinem Webbrowser zu starten.

Anforderungen für das Öffnen von Ressourcen in Ihrem Browser

Für Benutzer im internen Netzwerk ist der Zugriff auf Ressourcen, die von Citrix Virtual Apps and Desktops bereitgestellt werden, über einen Webbrowser standardmäßig deaktiviert. Um den lokalen Zugriff auf Desktops und Anwendungen über einen Webbrowser zu ermöglichen, aktivieren

Sie die ICA-WebSockets-Verbindungsrichtlinie auf Ihren Citrix Virtual Apps and Desktops-Servern. Citrix Virtual Apps and Desktops verwendet Port 8008 für Citrix Workspace-App für HTML5-Verbindungen. Stellen Sie sicher, dass Ihre Firewalls und andere Netzwerkgeräte den Zugriff auf diesen Port zulassen. Weitere Informationen finden Sie unter WebSockets-Richtlinieneinstellungen.

Damit Citrix Virtual Apps and Desktops-Ressourcenstarts erfolgreich sind, konfigurieren Sie die TLS-Verbindungen zu den VDAs, die Apps und Desktops hosten. Remote-Verbindungen über ein Citrix Gateway können Ressourcen mit der Citrix Workspace-App für HTML5 starten, ohne TLS-Verbindungen zum VDA zu konfigurieren.

Hybridstart

Wenn Benutzer einen Store zum ersten Mal in ihrem Webbrowser öffnen, aber Apps in der lokal installierten Citrix Workspace-App starten, wird dies als Hybrid-Start bezeichnet. Es gibt verschiedene Möglichkeiten, wie die Website mit der lokal installierten Workspace-App kommunizieren kann, um Ressourcen zu starten.

Citrix-Weberweiterungen

Für die beste Benutzererfahrung stellen Sie Citrix-Weberweiterungen bereit. Dies sind Erweiterungen für gängige Webbrowser, die die Benutzererfahrung bei der Erkennung der lokal installierten Citrix Workspace-App und dem Start virtueller Apps und Desktops verbessern. Im Vergleich zum Citrix Workspace-Launcher bietet dies eine bessere Benutzererfahrung und vermeidet Probleme mit globalen Server-Lastenausgleichern.

So aktivieren Sie die clientseitige Erkennung basierend auf Browsererweiterungen:

- Stellen Sie die Browsererweiterung auf den Clientgeräten bereit.
- Stellen Sie Citrix Workspace-App für Windows 2303, Mac 2304 oder Linux 2302 oder höher bereit.

Wenn ein Benutzer zum ersten Mal eine Store-Website auf einer unterstützten Plattform aufruft, wird er aufgefordert, die lokal installierte Workspace-App zu erkennen. Zuerst wird versucht, die Web-Erweiterung zu verwenden, und wenn dies fehlschlägt, wird der Citrix Workspace Launcher verwendet. Bestehende Benutzer, die die Erkennung der Workspace-App bereits abgeschlossen haben, können zu den **Kontoeinstellungen** gehen und **Startmethode ändern** (klassische Erfahrung) oder **Verbindung überprüfen** (moderne Erfahrung) auswählen, um die Citrix Workspace-App erneut zu erkennen.

> **Wichtig**
>
> Wenn Benutzer keine Citrix Web-Erweiterungen installiert haben, dauert die Erkennung der Citrix Workspace-App zusätzliche 6 Sekunden, bis der Versuch, die Citrix Web-Erweiterungen zu kontaktieren, ein Timeout erreicht. Wenn Sie keine Citrix Web-Erweiterungen bereitgestellt haben, möchten Sie diese möglicherweise deaktivieren oder die Timeouts ändern. Weitere Informationen finden Sie unter Starteinstellungen.

Citrix Workspace Launcher

Wenn der Benutzer zum ersten Mal eine StoreFront-Website mit einem unterstützten Betriebssystem und Browser aufruft und keine Citrix Web-Erweiterungen installiert sind, versucht die Website, den Citrix Workspace Launcher aufzurufen. Weitere Informationen zur Benutzererfahrung finden Sie unter Klassische Erfahrung und Moderne Erfahrung.

Wenn eine unterstützte Version der Citrix Workspace-App installiert ist, benachrichtigt die App StoreFront. Der Browser merkt sich dies und verwendet beim Starten einer App den Citrix Workspace Launcher.

Die Store-Website ruft den Citrix Workspace Launcher 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 der Citrix Workspace-App oder von Citrix Receiver.

- Citrix Receiver für Windows 4.3 oder höher oder eine beliebige Version der Citrix Workspace-App für Windows mit der WebHelper-Komponente (diese ist standardmäßig installiert)
- Citrix Receiver für Mac 12.0 oder höher oder eine beliebige Version der Citrix Workspace-App für Mac
- Citrix Workspace-App für Linux 2003 oder höher
- Citrix Workspace-App für iOS 2503 oder höher
- Citrix Workspace-App für Android 2503 oder höher

Wenn der Citrix Workspace Launcher nicht verfügbar ist oder der Benutzer das Öffnen nicht zulässt, kann die lokal installierte Citrix Workspace-App nicht erkannt werden. Der Benutzer hat die Möglichkeit, es erneut zu versuchen oder auf **Bereits installiert** zu klicken. In diesem Fall wird auf das Starten von Apps mithilfe von ICA-Dateidownloads zurückgegriffen. Der Benutzer kann es später erneut versuchen, indem er zum Bildschirm „Einstellungen“ navigiert und auf **Citrix Workspace-App ändern** klickt.

Der Citrix Workspace Launcher hat die folgenden Einschränkungen:

- Wenn Sie mehrere aktive StoreFront-Servergruppen hinter einem globalen Server-Lastenausgleich verwenden, kann der Citrix Workspace Launcher zeitweise fehlschlagen. Um dies zu vermeiden, müssen Sie Ihren globalen Server-Lastenausgleich so konfigurieren, dass die Web-Sitzung des Benutzers für die Dauer des Client-Erkennungsprozesses persistent an eine StoreFront-Servergruppe gebunden wird. Weitere Informationen finden Sie unter CTX460312.
- Beim Verbinden mit der Website über ein Citrix Gateway verwendet der Citrix Workspace Launcher das HDX-Routing des Gateways, um Anfragen von der Citrix Workspace-App zurück an den StoreFront-Server zu proxen. Wenn das Gateway nur für die **Authentifizierung** (nicht für HDX-Routing) konfiguriert ist, kann der Citrix Workspace Launcher keine Verbindung zu StoreFront herstellen. Um dies zu umgehen, stellen Sie sicher, dass Ihr Citrix Gateway für HDX-Routing mit entsprechenden STA-Servern konfiguriert ist. Bearbeiten Sie das Citrix Gateway, setzen Sie die **Nutzung oder Rolle** auf **Authentifizierung und HDX-Routing** und konfigurieren Sie die STA-Server.
- Wenn sich ein authentifizierter Proxy vor dem Citrix Gateway befindet, kann die Citrix Workspace-App keine SOCKS-Verbindung zum Citrix Gateway herstellen, sodass der Citrix Workspace Launcher fehlschlägt.
- Der Citrix Workspace Launcher funktioniert nicht, wenn die Smartcard-Authentifizierung über ein Citrix Gateway verwendet wird.

Alternativ können Sie Citrix Web Extensions bereitstellen.

Internet Explorer

Wenn der Benutzer die Store-Website zum ersten Mal im Internet Explorer öffnet, wird er aufgefordert, die Citrix Workspace-App zu installieren, die das Citrix ICA Client Add-on für Internet Explorer enthält. Sobald das Plugin installiert ist, wird es verwendet, um Apps und Desktops über die lokal installierte Citrix Workspace-App zu starten.

ICA-Dateidownloads

Wenn die Website eine lokal installierte Citrix Workspace-App auf andere Weise nicht erkennen kann oder der Benutzer auf **Erkennung überspringen** klickt, wird beim Starten einer App oder eines Desktops eine .ica-Datei heruntergeladen. Der Benutzer kann diese Datei mit der lokal installierten Citrix Workspace-App öffnen. Diese Startmethode wird nicht empfohlen, da:

- Das Speichern von ICA-Dateien auf der Festplatte ein Sicherheitsrisiko darstellt.
- Bei Verwendung von Sitzungswiederverbindung kann die Website keine Verbindung zu bestehenden Sitzungen wiederherstellen.
- Die Domänen-Pass-Through-Authentifizierung nicht verfügbar ist.

Diese Option kann deaktiviert werden. Weitere Informationen finden Sie unter Startpräferenzen.

Ressourcenverknüpfungen

Sie können URLs generieren, die Zugriff auf Desktops und Anwendungen bieten, die in Ihrem Store verfügbar sind. Betten Sie diese Links auf Websites ein, die im internen Netzwerk gehostet werden, um Benutzern einen schnellen Zugriff auf Ressourcen zu ermöglichen. Benutzer klicken auf einen Link und werden zur Store-Website weitergeleitet, wo sie sich anmelden, falls sie dies noch nicht getan haben. Die Store-Website startet die Ressource automatisch. Weitere Informationen zum Generieren von Ressourcenverknüpfungen finden Sie unter Website-Verknüpfungen.

Wenn Sie eine Anwendungsverknüpfung erstellen, stellen Sie sicher, dass keine anderen im Store verfügbaren Anwendungen denselben Namen haben. Verknüpfungen können nicht zwischen mehreren Instanzen einer Anwendung mit demselben Namen unterscheiden. Wenn Sie mehrere Instanzen eines Desktops aus einer einzigen Desktopgruppe im Store verfügbar machen, können Sie ebenfalls keine separaten Verknüpfungen für jede Instanz erstellen. Verknüpfungen können keine Befehlszeilenparameter an Anwendungen übergeben.

Um Anwendungsverknüpfungen zu erstellen, konfigurieren Sie StoreFront mit den URLs der internen Websites, die die Verknüpfungen hosten werden. Wenn ein Benutzer auf eine Anwendungsverknüpfung auf einer Website klickt, überprüft StoreFront diese Website anhand der von Ihnen eingegebenen URL-Liste, um sicherzustellen, dass die Anforderung von einer vertrauenswürdigen Website stammt.

XenApp Services-URLs

> **Hinweis:**

> XenApp Services (auch bekannt als PNAgent) ist ab StoreFront 2308 veraltet. Es wird empfohlen, die Citrix Workspace-App zu verwenden, um über eine Store-URL eine Verbindung zu StoreFront herzustellen.

> Benutzer mit älteren Citrix Clients, die nicht aktualisiert werden können, können auf Stores zugreifen, indem sie ihre Clients mit der XenApp Services-URL für einen Store konfigurieren. Sie können den Zugriff auf Ihre Stores auch über XenApp Services-URLs von in die Domäne eingebundenen Desktop-Appliances und umfunktionierten PCs, auf denen Citrix Desktop Lock ausgeführt wird, ermöglichen. „In die Domäne eingebunden“ bedeutet in diesem Kontext Geräte, die einer Domäne innerhalb der Microsoft Active Directory-Gesamtstruktur beigetreten sind, die die StoreFront-Server enthält.

StoreFront unterstützt die Pass-Through-Authentifizierung mit Proximity-Karten über die Citrix Workspace-App für XenApp Services-URLs. Citrix Ready-Partnerprodukte verwenden die Citrix Fast Connect API, um Benutzeranmeldungen über Citrix Receiver für Windows oder die Citrix Workspace-App für Windows zu optimieren, um eine Verbindung zu Stores über die XenApp Services-URL herzustellen. Benutzer authentifizieren sich an Workstations mithilfe von Proximity-Karten und werden schnell mit Desktops und Anwendungen verbunden, die von Citrix Virtual Apps and Desktops bereitgestellt werden. Weitere Informationen finden Sie in der neuesten Dokumentation zu Citrix Workspace for Windows.

Wenn Sie einen neuen Store erstellen, ist die XenApp Services-URL für den Store standardmäßig aktiviert. Die XenApp Services-URL für einen Store hat die Form `http[s]://serveraddress/Citrix/storename/PNAgent/config.xml`, wobei `serveraddress` der vollqualifizierte Domänenname des Servers oder der Lastenausgleichsumgebung für Ihre StoreFront-Bereitstellung ist und `storename` der Name ist, der beim Erstellen des Stores angegeben wurde. Dies ermöglicht Citrix Workspace-Apps, die nur das PNAgent-Protokoll verwenden können, die Verbindung zu StoreFront. Informationen zu den Clients, die für den Zugriff auf Stores über XenApp Services-URLs verwendet werden können, finden Sie unter Anforderungen an Benutzergeräte.

Wichtige Überlegungen

XenApp Services-URLs sollen Benutzer unterstützen, die nicht auf die Citrix Workspace-App aktualisieren können, sowie in Szenarien, in denen keine alternativen Zugriffsmethoden verfügbar sind. Wenn Sie entscheiden, ob Sie XenApp Services-URLs verwenden möchten, um Benutzern den Zugriff auf Ihre Stores zu ermöglichen, beachten Sie die folgenden Einschränkungen.

- Sie können die XenApp Services-URL für einen Store nicht ändern.
- Sie können die Einstellungen der XenApp Services-URL nicht ändern, indem Sie die Konfigurationsdatei config.xml bearbeiten.
- XenApp Services-URLs unterstützen explizite Authentifizierung, Domänen-Pass-Through, Smartcard-Authentifizierung und Pass-Through mit Smartcard-Authentifizierung. Die explizite Authentifizierung ist standardmäßig aktiviert. Für jede XenApp Services-URL kann nur eine Authentifizierungsmethode konfiguriert werden, und pro Store ist nur eine URL verfügbar. Wenn Sie mehrere Authentifizierungsmethoden aktivieren müssen, müssen Sie für jede Authentifizierungsmethode separate Stores erstellen, jeder mit einer XenApp Services-URL. Ihre Benutzer müssen sich dann mit dem entsprechenden Store für ihre Authentifizierungsmethode verbinden. Weitere Informationen finden Sie unter XML-basierte Authentifizierung.
- Die Workspace Control ist für XenApp Services-URLs standardmäßig aktiviert und kann nicht konfiguriert oder deaktiviert werden.
- Benutzeranfragen zur Kennwortänderung werden direkt über die Citrix Virtual Apps and Desktops-Server, die Desktops und Anwendungen für den Store bereitstellen, an den Domänencontroller weitergeleitet, wodurch der StoreFront-Authentifizierungsdienst umgangen wird.

Bereitstellung verwalten

Dieser Abschnitt beschreibt, wie Sie Ihre StoreFront-Bereitstellung verwalten. Er enthält die folgenden Themen:

THEMA	BESCHREIBUNG
StoreFront-Verwaltungskonsole	Öffnen Sie die StoreFront-Verwaltungskonsole (GUI), um StoreFront zu konfigurieren.
StoreFront PowerShell-Module	Verwenden Sie die StoreFront PowerShell-Module, um die StoreFront-Konfiguration zu automatisieren.
Basis-URL konfigurieren	Konfigurieren Sie die Basis-URL, die Benutzer eingeben, um eine Verbindung zur Bereitstellung herzustellen.
Servergruppe konfigurieren	Fügen Sie Server zu Ihrer StoreFront-Servergruppe hinzu und entfernen Sie sie, und übertragen Sie die Konfiguration auf die anderen Server in der Gruppe.
Abonnementdatenbank verwalten	Wählen Sie, wo StoreFront Abonnements speichert, verwalten Sie die Daten in der Datenbank und synchronisieren Sie Daten zwischen Servergruppen.
StoreFront aktualisieren	Aktualisieren Sie ältere Versionen von StoreFront auf diese Version.
StoreFront-Konfiguration exportieren und importieren	Konfiguration von einer StoreFront-Bereitstellung exportieren und in eine andere Bereitstellung importieren.
Standardwebsite für die Bereitstellung	Konfigurieren Sie, auf welche Website Benutzer umgeleitet werden, wenn sie die Basis-URL in ihrem Webbrowser aufrufen.

THEMA	BESCHREIBUNG
Server auf Werkseinstellungen zurücksetzen	Entfernen Sie die gesamte StoreFront-Konfiguration, damit Sie sie neu konfigurieren oder zu einer vorhandenen Servergruppe hinzufügen können.
StoreFront deinstallieren	StoreFront von Ihrem Server entfernen

StoreFront™ Verwaltungskonsole

Die meisten Aspekte von StoreFront können mit der StoreFront-Verwaltungskonsole konfiguriert werden.

Um die Verwaltungskonsole zu öffnen, öffnen Sie das **Startmenü**, erweitern Sie den Ordner **Citrix** und wählen Sie **Citrix StoreFront**.

Screenshot des Startmenüs mit hervorgehobenem StoreFront(/en-us/storefront/2507-ltsr/media/manage-deployment/start-menu-citrix-storefront.png)

Dadurch wird die StoreFront-Verwaltungskonsole geöffnet.

Screenshot der Verwaltungskonsole(/en-us/storefront/2507-ltsr/media/manage-deployment/management-console.png)

Nachdem Sie eine Bereitstellung erstellt haben, befindet sich auf der linken Seite eine Strukturansicht mit den folgenden Elementen:

- **Stores**. Wählen Sie dies, um Stores anzuzeigen und zu verwalten und Gateways.
- **Servergruppe**. Wählen Sie dies, um die Servergruppe zu verwalten und die Basis-URL zu konfigurieren.

Wenn Sie einen Knoten in der Strukturansicht auswählen, wird der Rest des Bildschirms entsprechend aktualisiert.

Der zentrale Teil des Fensters enthält Informationen zu den Stores oder der Servergruppe.

Auf der rechten Seite befindet sich der Bereich **Aktionen**.

Einige erweiterte Konfigurationsaufgaben sind in der Verwaltungskonsole nicht verfügbar und erfordern die Verwendung von StoreFront PowerShell-Modulen.

StoreFront PowerShell-Module

Citrix StoreFront stellt eine Reihe von Microsoft Windows PowerShell Version 2.0-Modulen bereit, die bei der Installation von StoreFront enthalten sind. Mit den Modulen können Sie dieselben Aufgaben ausführen wie mit der StoreFront-Verwaltungskonsole, sowie Aufgaben, die Sie mit der Konsole allein nicht ausführen können.

> **Hinweis:**

> Die StoreFront PowerShell-Module sind nicht mit PowerShell 6 oder höher kompatibel.

> Eine Referenz zu den PowerShell-Modulen finden Sie in der StoreFront-Entwicklerdokumentation.

Erste Schritte

1. Stellen Sie sicher, dass die StoreFront-Verwaltungskonsole geschlossen ist.
2. Starten Sie eine PowerShell-Befehlszeilenaufforderung oder die **Windows PowerShell ISE** als Administrator.

   Sie müssen die Shell oder das Skript als Mitglied der lokalen Administratorengruppe auf dem StoreFront-Server ausführen.
3. Um Cmdlets in Skripts zu verwenden, setzen Sie die Ausführungsrichtlinie in PowerShell auf RemoteSigned. Weitere Informationen zur PowerShell-Ausführungsrichtlinie finden Sie in der Microsoft-Dokumentation.
4. Sie können die Beispielskripts als Ausgangspunkt verwenden.
5. Verwenden Sie das Cmdlet **Get-Help** mit dem Cmdlet-Namen und dem Parameter **-Full**, um weitere Informationen zu einem bestimmten Befehl zu erhalten.

Virtueller Pfad

Cmdlets zum Abrufen oder Erstellen eines Stores, einer Website oder von Authentifizierungsdiensten verwenden einen `VirtualPath`-Parameter. Dies ist der Pfad, unter dem die Anwendung in IIS gehostet wird. Der Store- und Website-Pfad kann auch in der StoreFront-Verwaltungskonsole gefunden werden. Typischerweise ist der Authentifizierungspfad konventionsgemäß derselbe wie der Store-Pfad mit dem Suffix `Auth`, und die Website ist derselbe wie der Store-Pfad mit dem Suffix `Web`. Z. B. für den virtuellen Store-Pfad `/Citrix/`

`Store` hat der Authentifizierungsdienst den Pfad `/Citrix/StoreAuth` und die Website den Pfad `/Citrix/StoreWeb`.

Z. B. um einen Store-Dienst abzurufen, dessen Pfad `/Citrix/Store` ist, führen Sie den Befehl aus:

```
Get-STFStoreService -VirtualPath '/Citrix/Store'
```

Wenn Sie den VirtualPath weglassen, werden alle Dienste zurückgegeben. Wenn nur ein Dienst vorhanden ist, behandelt PowerShell diesen als einzelnes Objekt.

Site-ID

Einige Cmdlets enthalten einen `SiteId`-Parameter. Wenn Sie mehrere Bereitstellungen auf demselben Server auf verschiedenen IIS-Sites haben, müssen Sie den `SiteId` angeben. Wenn Sie nur eine Site haben, ist der Parameter nicht erforderlich.

Beispielskripte

StoreFront enthält einige Beispielskripte, die sich im Ordner **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** befinden. Sie können diese als Vorlagen zum Erstellen eigener Skripte verwenden.

```
-  Use the PowerShell ISE, Visual Studio Code or a similar tool to edit
the script.

-  Use variables to assign values that are to be reused or modified.

-  Remove any commands that are not required.

-  Note that StoreFront cmdlets can be identified by the prefix STF.
```

BEISPIELE	BESCHREIBUNG
Einfache Bereitstellung erstellen	Skript: Erstellt eine einfache Bereitstellung mit einem StoreFront-Controller, der mit einer einzelnen CVAD-Site konfiguriert ist.
Bereitstellung für Remotezugriff erstellen	Skript: Baut auf dem vorherigen Skript auf, um der Bereitstellung Remotezugriff hinzuzufügen.

BEISPIELE	BESCHREIBUNG
Bereitstellung für Remotezugriff mit optimalem Start-Gateway erstellen	Skript: Baut auf dem vorherigen Skript auf, um bevorzugte optimale Start-Gateways für eine bessere Benutzererfahrung hinzuzufügen.

Einfache Bereitstellung erstellen

Das folgende Beispiel zeigt, wie eine einfache Bereitstellung mit einer CVAD-Site erstellt wird.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Schritte in Erste Schritte befolgen. Dieses Beispiel kann angepasst werden, um ein Skript zur Automatisierung der StoreFront-Bereitstellung zu erstellen.

Dieser Abschnitt erklärt, was jeder Teil des Skripts bewirkt. Dies hilft Ihnen bei der Anpassung Ihres eigenen Skripts.

- Legt die Anforderungen an die Fehlerbehandlung fest und importiert die erforderlichen StoreFront-Module. Importe sind in modernen PowerShell-Versionen nicht erforderlich.

```
Param(

    [Parameter(Mandatory=$true)]

    [Uri]$HostbaseUrl,

    [long]$SiteId = 1,

    [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox")]

    [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"

    )

    # 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.Authentication

    Import-Module Citrix.StoreFront.WebReceiver
```

- Automatisiert den virtuellen Pfad der Authentifizierungs- und Citrix Receiver für Web-Dienste basierend auf dem bereitgestellten `$StoreVirtualPath`. `$StoreVirtualPath` entspricht `StoreIISPath`, 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"
```

- Erstellt eine neue Bereitstellung, falls noch keine vorhanden ist, um die erforderlichen StoreFront-Dienste hinzuzufügen. **-Confirm:$false** unterdrückt die Anforderung, die Fortsetzung der Bereitstellung zu bestätigen.

```
# 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."

}
```

- Erstellt einen neuen Authentifizierungsdienst, falls keiner unter dem angegebenen virtuellen Pfad existiert. Die Standardauthentifizierungsmethode Benutzername und Kennwort ist aktiviert.

```
# Determine if the authentication service at the specified virtual path
exists

$authentication = Get-STFAuthenticationService -VirtualPath
$authenticationVirtualPath

if(-not $authentication)

{
```

```
    # Add an Authentication service using the IIS path of the Store
appended with Auth

    $authentication = Add-STFAuthenticationService
$authenticationVirtualPath

}

else

{

    Write-Output "An Authentication service already exists at the
specified virtual path and will be used."

}
```

- Erstellt den neuen Speicherdienst, der mit einer Site (auch als Farm bekannt) konfiguriert ist, wobei die Server im Array **$XenDesktopServers** unter dem angegebenen virtuellen Pfad definiert sind, falls noch keiner existiert.

```
# Determine if the store service at the specified virtual path exists

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

if(-not $store)

{

# Add a Store that uses the new Authentication service configured to
publish resources from the supplied servers

$store = Add-STFStoreService -VirtualPath $StoreVirtualPath
-AuthenticationService $authentication -FarmName $Farmtype -FarmType
$Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `

        -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
$TransportType

}

else
```

```
{

    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."

    # Get the number of farms configured in the store

    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count

    # Append the farm to the store with a unique name

    Add-STFStoreFarm -StoreService $store -FarmName "Controller$
($farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
-LoadBalance $LoadbalanceServers -Port $Port `

        -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}
```

- Fügt eine Website unter dem angegebenen virtuellen IIS-Pfad hinzu, um auf Anwendungen zuzugreifen, die im 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."

}
```

- Aktiviert XenApp-Dienste für den Store, damit ältere Citrix Receiver- oder Citrix Workspace-App-Clients eine Verbindung zu 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

}
```

Beispiel: Erstellen einer Remotezugriffsbereitstellung

Das folgende Beispiel baut auf dem vorherigen Skript auf, um eine Bereitstellung mit Remotezugriff hinzuzufügen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Schritte in Erste Schritte befolgen. Dieses Beispiel kann mit den beschriebenen Methoden angepasst werden, um ein Skript zur Automatisierung der StoreFront-Bereitstellung zu erstellen.

Dieser Abschnitt erklärt, was jeder Teil des von StoreFront erstellten Skripts bewirkt. Dies hilft Ihnen bei der Anpassung Ihres eigenen Skripts.

- Legt die Anforderungen an die Fehlerbehandlung fest und importiert die erforderlichen StoreFront-Module. In modernen PowerShell-Versionen sind Importe 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
```

- Erstellt eine StoreFront-Bereitstellung für den internen Zugriff, indem das Skript der vorherigen Beispiele aufgerufen wird. Die Basisbereitstellung wird erweitert, um den Remotezugriff zu unterstützen.

```
# 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
```

- Ruft die in der einfachen Bereitstellung erstellten Dienste ab, da diese aktualisiert werden müssen, um das Remotezugriffsszenario zu unterstützen.

```
# 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
```

- Aktiviert CitrixAGBasic für den Citrix Receiver™ für Web-Dienst, der für den Remotezugriff über Citrix Gateway erforderlich ist. Rufen Sie die Authentifizierungsmethode CitrixAGBasic und ExplicitForms des Citrix Receiver für Web aus 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
```

- 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
```

- Fügt ein neues Remotezugriffs-Gateway hinzu, wobei die optionale Subnetz-IP-Adresse angegeben und beim Store registriert wird, um remote darauf zugreifen zu können.

```
# 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
```

Beispiel: Bereitstellung mit Remotezugriff und optimalem Start-Gateway erstellen

Das folgende Beispiel baut auf dem vorherigen Skript auf, um eine Bereitstellung mit Remotezugriff über ein optimales Start-Gateway hinzuzufügen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Schritte in Erste Schritte befolgen. Dieses Beispiel kann mit den beschriebenen Methoden angepasst werden, um ein Skript zur Automatisierung der StoreFront-Bereitstellung zu erstellen.

Das Skript verstehen

Dieser Abschnitt erklärt, was jeder Teil des von StoreFront erstellten Skripts tut. Dies wird Ihnen bei der Anpassung Ihres eigenen Skripts helfen.

- Legt die Anforderungen an die Fehlerbehandlung fest und importiert die erforderlichen StoreFront-Module. In modernen PowerShell-Versionen sind Importe 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
```

- Ruft das Skript für die Remotezugriffsbereitstellung auf, um die grundlegende Bereitstellung zu konfigurieren und Remotezugriff hinzuzufügen.

```
# 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
```

- Fügt das bevorzugte optimale Start-Gateway 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
```

- Ruft den Store-Dienst ab, um das optimale Gateway zu verwenden, registriert es und weist es den Starts von der benannten Site zu.

```
# 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
```

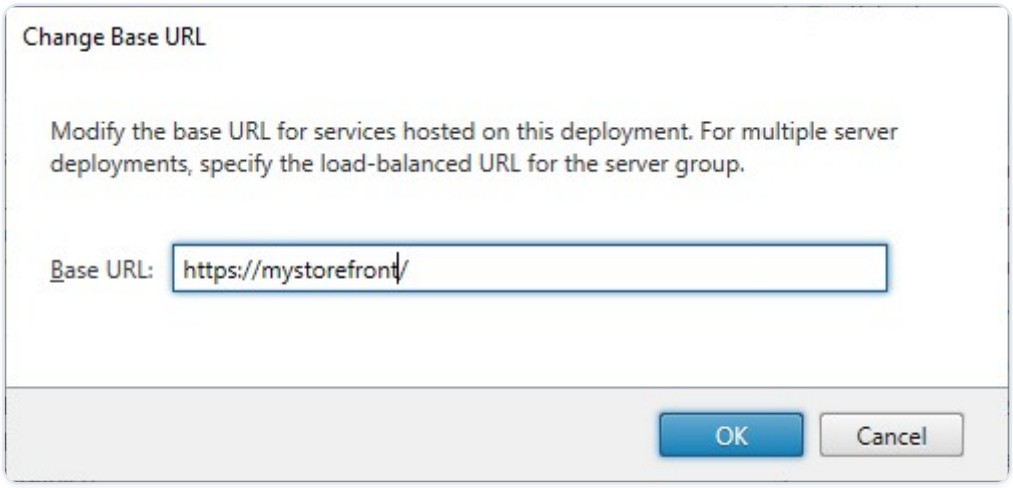
Basis-URL konfigurieren

Die Basis-URL wird als Stamm der URLs für die Stores und andere StoreFront-Dienste verwendet, die auf einer Bereitstellung gehostet werden. Sie müssen die URL eingeben, die Benutzer verwenden, um sich direkt mit der Bereitstellung zu verbinden (nicht über ein Citrix Gateway), z. B. `https://storefront.example.com`. Das Schema muss `http` oder `https` sein. Es wird empfohlen, immer `https` zu verwenden.

- Geben Sie für eine Einzelserverbereitstellung ohne Lastenausgleich die URL des Servers ein.
- Wenn Benutzer über einen Lastenausgleich eine Verbindung herstellen, geben Sie die URL des Lastenausgleichs ein. Sie müssen auch Loopback-Kommunikation aktivieren, damit StoreFront den Lastenausgleich für die interne Kommunikation umgeht.

So ändern Sie die Basis-URL:

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Servergruppe** aus.
2. Klicken Sie im Aktionsbereich auf **Basis-URL ändern...**
3. Geben Sie die neue URL ein.
4. Klicken Sie auf **OK**.



Servergruppen konfigurieren

Für Redundanz und Skalierbarkeit sollten Sie 2 oder mehr identische StoreFront-Server in einer Servergruppe hinter einem Lastenausgleich bereitstellen. StoreFront synchronisiert Konfigurations- und Favoritendaten zwischen den Servern.

Um eine Bereitstellung mit mehreren Servern zu verwalten, verwenden Sie jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Nachdem Sie Ihre Änderungen abgeschlossen haben, (#propagate-local-changes-to-a-server-group), um eine konsistente Konfiguration in der gesamten Bereitstellung sicherzustellen.

Servergruppe anzeigen

Wählen Sie in der StoreFront-Verwaltungskonsole in der Strukturansicht auf der linken Seite **Servergruppe** aus. Dies zeigt die Anzahl der Server in der Servergruppe, die Basis-URL, die Liste der Server und deren Synchronisierungsstatus an.

Server zu einer Servergruppe hinzufügen

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

- Der Server, den Sie hinzufügen, muss dieselbe StoreFront-Version wie die anderen Server in der Gruppe haben.
- Der Server, den Sie hinzufügen, befindet sich am selben Standort wie die anderen Server in der Gruppe. Stellen Sie eine geringe Latenz und eine zuverlässige Verbindung zwischen den Servern sicher.

- Der Server, den Sie hinzufügen, muss dieselbe Betriebssystemversion mit denselben Gebietsschemaeinstellungen wie die anderen Server in der Gruppe ausführen. StoreFront-Servergruppen, die Mischungen aus Betriebssystemversionen und Gebietsschemas enthalten, werden nicht unterstützt.
- IIS ist mit derselben Websitekonfiguration, z. B. physischem Pfad und Site-IDs, wie die anderen Server in der Gruppe konfiguriert.

Hinweis:

Empfehlungen zur Größe von Servergruppen finden Sie unter (/de-de/storefront/2507-ltsr/get-started/plan.html#storefront-server-groups).

Wenn der StoreFront-Server, den Sie hinzufügen, zuvor zu einer Servergruppe gehörte und entfernt wurde, müssen Sie den StoreFront-Server auf die Werkseinstellungen zurücksetzen, bevor er erneut derselben oder einer anderen Servergruppe hinzugefügt werden kann. Siehe (/de-de/storefront/2507-ltsr/manage-deployment/reset-server-to-factory-defaults.html)

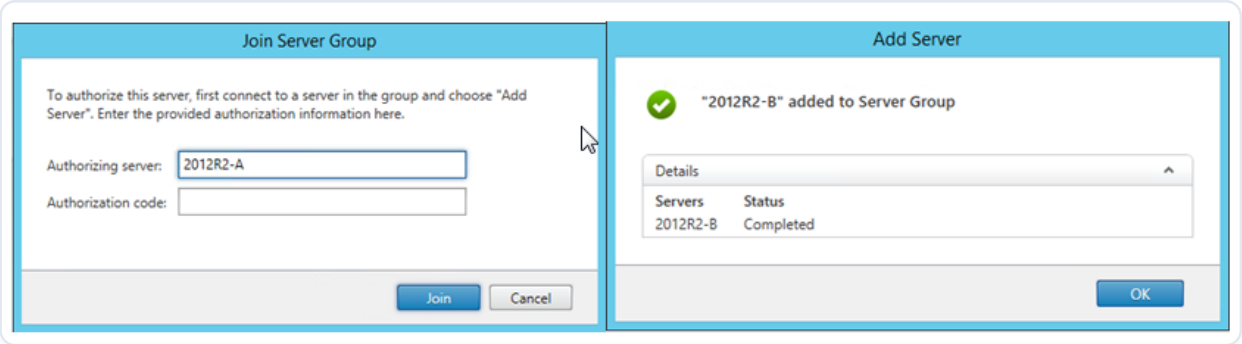
Wichtig:

Wenn Sie einer Servergruppe einen neuen Server hinzufügen, werden StoreFront-Dienstkonten als Mitglieder der lokalen Administratorengruppe auf dem neuen Server hinzugefügt. Diese Dienste benötigen lokale Administratorberechtigungen, um der Servergruppe beizutreten und sich mit ihr zu synchronisieren. Wenn Sie Gruppenrichtlinien verwenden, um das Hinzufügen neuer Mitglieder zur lokalen Administratorengruppe zu verhindern, oder wenn Sie die Berechtigungen der lokalen Administratorengruppe auf Ihren Servern einschränken, kann StoreFront keiner Servergruppe beitreten.

1. Melden Sie sich bei einem Server in der StoreFront-Bereitstellung an, dem Sie beitreten möchten, und öffnen Sie die Citrix StoreFront-Verwaltungskonsole. Wählen Sie im linken Bereich der Konsole den Knoten Servergruppe und im Bereich Aktionen die Option **Server hinzufügen**. Notieren Sie sich den angezeigten Autorisierungscode.
2. Verbinden Sie sich mit dem neuen Server. Wählen Sie in der StoreFront-Verwaltungskonsole **Vorhandener Servergruppe beitreten**.

3. Geben Sie im Dialogfeld „Servergruppe beitreten“ den Namen des vorhandenen Servers im Feld „Autorisierender Server“ an. Geben Sie den von diesem Server erhaltenen Autorisierungscode ein und wählen Sie **Beitreten**.

   Nach dem Beitritt zur Gruppe wird die Konfiguration des neuen Servers an die Konfiguration des vorhandenen Servers angepasst. Alle anderen Server in der Gruppe werden mit den Details des neuen Servers aktualisiert.



4. Fügen Sie den Server dem Lastenausgleich hinzu.

Um eine Bereitstellung mit mehreren Servern zu verwalten, verwenden Sie jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Alle von Ihnen vorgenommenen Konfigurationsänderungen müssen an die anderen Server in der Gruppe weitergegeben werden, um eine konsistente Konfiguration in der gesamten Bereitstellung sicherzustellen.

Server aus einer Servergruppe entfernen

1. Entfernen Sie den Server aus dem Lastenausgleich.
2. Melden Sie sich bei einem der Server in der Servergruppe an, der nicht derjenige ist, den Sie entfernen möchten.
3. Öffnen Sie die StoreFront-Verwaltungskonsole.
4. Wählen Sie in der Strukturansicht **Servergruppe**.
5. Wählen Sie **Server entfernen**.
6. Wählen Sie den Server aus, den Sie entfernen möchten.

Bevor ein entfernter StoreFront-Server erneut derselben oder einer anderen Servergruppe hinzugefügt werden kann, müssen Sie ihn auf die Werkseinstellungen zurücksetzen. Siehe Server auf Werkseinstellungen zurücksetzen

Lokale Änderungen an eine Servergruppe weitergeben

Sobald Sie Konfigurationsänderungen an einem Server vorgenommen haben, müssen Sie diese Änderungen an alle anderen Server in der Servergruppe weitergeben. Die Weitergabe von Konfigurationsinformationen wird manuell initiiert, damit Sie die Kontrolle darüber behalten, wann und ob die Server in der Gruppe mit Konfigurationsänderungen aktualisiert werden. Während dieser Weitergabe können Sie keine weiteren Änderungen vornehmen, bis alle Server in der Gruppe aktualisiert wurden.

Um Änderungen weiterzugeben, wählen Sie **Änderungen weitergeben** im Aktionsbereich aus.

> **Wichtig:**

> Alle auf anderen Servern in der Gruppe vorgenommenen Änderungen werden während der Weitergabe verworfen. Wenn Sie die Konfiguration eines Servers aktualisieren, geben Sie die Änderungen an die anderen Server in der Gruppe weiter, um zu vermeiden, dass diese Änderungen verloren gehen, falls Sie später Änderungen von einem anderen Server in der Bereitstellung weitergeben.

> Die zwischen den Servern in der Gruppe weitergegebenen Informationen umfassen Folgendes:

- Inhalt aller `web.config`-Dateien, die die StoreFront-Konfiguration enthalten.
- Inhalt von `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`, wie 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`.
- Für jede Store-Website, z. B. `c:\inetpub\wwwroot\Citrix\StoreWeb`, die Inhalte der Ordner `contrib`, `custom` und `customweb`. Diese Ordner werden zur Speicherung von Website-Anpassungen verwendet.
- Inhalt des Citrix Delivery Services-Zertifikatspeichers, mit Ausnahme manuell importierter Zertifikatsperrlisten (CRLs). (Details zur Verteilung lokaler CRLs finden Sie unter Überprüfung der Zertifikatsperrliste (CRL)).

> **Hinweis:**

> Abonnementdaten werden unabhängig vom Mechanismus „Änderungen weitergeben“ mit den anderen Servern synchronisiert. Dies geschieht automatisch, ohne dass die Aufgabe „Änderungen weitergeben“ initiiert werden muss.

Datenbank für Abonnements verwalten

Wenn Sie einen Store erstellen, erstellt StoreFront lokal auf dem Server eine Microsoft Extensible Storage Engine (ESENT)-Datenbank, um Favoriten- (auch Abonnement-) Daten zu speichern. In StoreFront-Servergruppenumgebungen verwaltet jeder Server eine eigene Kopie der Datenbank. Alle Änderungen an Favoriten werden an andere Server weitergegeben, um sicherzustellen, dass Benutzer dieselben Favoriten sehen, unabhängig davon, mit welchem Server sie sich verbinden.

Alternativ können Sie Favoriten in einer SQL Server-Datenbank speichern. Weitere Informationen finden Sie unter Abonnementdaten mit Microsoft SQL Server speichern.

Um anzuzeigen, ob ein Store eine lokale ESENT-Datenbank oder eine SQL Server-Datenbank verwendet, verwenden Sie das PowerShell-Skript:

```
$store=Get-STFStoreService -VirtualPath '/Citrix/Store'

Get-STFStoreSubscriptionsDatabase -StoreService $store
```

Verwalten von Favoritendaten

Bei Verwendung einer ESENT-Datenbank können Sie PowerShell verwenden, um die Favoritendaten zu verwalten. Weitere Informationen finden Sie unter Favoritendaten verwalten. Bei Verwendung einer SQL Server-Datenbank können Sie SQL verwenden, um die Datensätze zu verwalten.

Synchronisieren von Favoriten zwischen Servergruppen

Abonnements werden automatisch zwischen Servern in einer Servergruppe synchronisiert. Wenn Sie mehrere Servergruppen haben, können Sie Citrix Files so konfigurieren, dass Abonnements regelmäßig zwischen Servergruppen synchronisiert werden. Weitere Informationen finden Sie unter Abonnementsynchronisierung.

Abonnementdaten verwalten

Wenn Sie eine lokale Datenbank verwenden, können Sie Favoriten für einen Store mithilfe von PowerShell-Cmdlets verwalten.

Abonnementdaten bereinigen

Für jeden Store in Ihrer Bereitstellung existiert ein Ordner und ein Datenspeicher, der Favoritendaten enthält.

1. Beenden Sie den Citrix Subscriptions Store-Dienst auf dem StoreFront-Server. Wenn der Citrix Subscriptions Store-Dienst ausgeführt wird, ist es nicht möglich, Abonnementdaten für Ihre Stores zu löschen.
2. Suchen Sie den Abonnement-Store-Ordner auf dem StoreFront-Server: `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Cit`
3. Löschen Sie den Inhalt des Abonnement-Store-Ordners, aber nicht den Ordner selbst.
4. Starten Sie den Citrix Subscriptions Store-Dienst auf dem StoreFront-Server neu.

Sie können das folgende PowerShell-Skript verwenden, um Abonnementdaten für einen Store zu bereinigen. Führen Sie diese PowerShell-Funktion als Administrator mit Rechten zum Beenden oder Starten von Diensten und zum Löschen von Dateien aus. Diese PowerShell-Funktion erzielt das gleiche Ergebnis wie die oben beschriebenen manuellen Schritte.

Damit die Cmdlets erfolgreich ausgeführt werden können, muss der Citrix Subscriptions Store-Dienst 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
```

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



    Stop-Service -displayname $SubsService



    Remove-Item $SubsPath -Force -Verbose



    Start-Service -displayname $SubsService



    Get-Service -displayname $SubsService

}



Remove-SubscriptionData -Store "YourStore"
```

Abonnementdaten exportieren

Sie können ein Backup der Store-Abonnementdaten in Form einer tabulatorgetrennten .txt-Datei mit dem Cmdlet Export-STFStoreSubscriptions erhalten, zum Beispiel:

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

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

Wenn Sie eine Bereitstellung mit mehreren Servern verwalten, können Sie dieses PowerShell-Cmdlet auf jedem Server innerhalb der StoreFront-Servergruppe ausführen. Jeder Server in der Servergruppe verwaltet eine identische, synchronisierte Kopie der Abonnementdaten von seinen Peers. Wenn Sie der Meinung sind, dass Probleme mit der Abonnementsynchronisierung

zwischen den Storefront-Servern auftreten, exportieren Sie die Daten von allen Servern in der Gruppe und vergleichen Sie sie, um Unterschiede festzustellen.

Abonnementdaten wiederherstellen

Verwenden Sie Restore-STFStoreSubscriptions, um Ihre vorhandenen Abonnementdaten zu überschreiben. Sie können die Abonnementdaten eines Stores mithilfe des zuvor mit Export-STFStoreSubscriptions erstellten tabulatorgetrennten .txt-Datei-Backups wiederherstellen.

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

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

Weitere Informationen zu Restore-STFStoreSubscriptions finden Sie unter `<https://developer-docs.citrix.com/de-de/storefront-powershell-sdk/2507/Restore-STFStoreSubscriptions/>`

Wiederherstellen von Daten auf einem einzelnen StoreFront-Server

In einer Einzelserverbereitstellung ist es nicht erforderlich, den Subscriptions Store-Dienst herunterzufahren. Es ist auch nicht notwendig, die vorhandenen Abonnementdaten vor der Wiederherstellung der Abonnementdaten zu löschen.

Wiederherstellen von Daten in einer StoreFront-Servergruppe

Um Abonnementdaten in einer Servergruppe wiederherzustellen, sind die folgenden Schritte erforderlich.

Beispiel für eine Servergruppenbereitstellung mit drei StoreFront-Servern.

- StoreFrontA
- StoreFrontB
- StoreFrontC

1. Sicherung der vorhandenen Abonnementdaten von einem der drei Server.
2. Beenden Sie den Subscriptions Store-Dienst auf den Servern StoreFrontB und C. Diese Aktion verhindert, dass die Server während der Aktualisierung von StoreFrontA Abonnementdaten senden oder empfangen.

3. Löschen Sie die Abonnementdaten von den Servern StoreFrontB und C. Dies verhindert eine Nichtübereinstimmung der wiederhergestellten Abonnementdaten.
4. Stellen Sie die Daten auf StoreFrontA mit dem Cmdlet **Restore-STFStoreSubscriptions** wieder her. Es ist nicht notwendig, den Subscriptions Store-Dienst zu beenden oder die Abonnementdaten auf StoreFrontA zu löschen (sie werden während des Wiederherstellungsvorgangs überschrieben).
5. Starten Sie den Subscriptions Store-Dienst auf den Servern StoreFrontB und StoreFrontC neu. Die Server können dann eine Kopie der Daten von StoreFrontA empfangen.
6. Warten Sie, bis die Synchronisierung zwischen allen Servern erfolgt ist. Die benötigte Zeit hängt von der Anzahl der Datensätze ab, die auf StoreFrontA vorhanden sind. Wenn sich alle Server in einer lokalen Netzwerkverbindung befinden, erfolgt 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 zu bestätigen, dass die Synchronisierung abgeschlossen ist, oder zeigen Sie die Store-Abonnementzähler an.

Abonnementdaten importieren

Verwenden Sie **Import-STFStoreSubscriptions**, wenn keine Abonnementdaten für den Store vorhanden sind. Dieses Cmdlet ermöglicht auch die Übertragung von Abonnementdaten von einem Store zu einem anderen oder den Import von Abonnementdaten auf neu bereitgestellte StoreFront-Server.

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

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

Weitere Informationen zu Import-STFStoreSubscriptions finden Sie unter `<https://developer-docs.citrix.com/de-de/storefront-powershell-sdk/2507/Import-STFStoreSubscriptions/>`

Details zur Abonnementdatendatei

Die Abonnementdatendatei ist eine Textdatei, die eine Zeile pro Benutzerabonnement enthält. Jede Zeile ist eine tabulatorgetrennte Abfolge von Werten:

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

wobei:

- `<user-identifier>` – Erforderlich. Eine Zeichenfolge, die den Benutzer identifiziert. Dieser Bezeichner ist der Windows-Sicherheitsbezeichner des Benutzers.
- `<resource-id>` – Erforderlich. Eine Zeichenfolge, die die abonnierte Ressource identifiziert.
- `<subscription-id>` – Erforderlich. Eine Zeichenfolge, die das Abonnement eindeutig identifiziert. Dieser Wert wird nicht verwendet (obwohl ein Wert in der Datendatei vorhanden sein muss).
- `<subscription-status>` – Erforderlich. Der Status des Abonnements: abonniert oder abbestellt.
- `<property-name>` und `<property-value>` – Optional. Eine Sequenz von null oder mehr Paaren von Eigenschaftsnamen/-werten. Diese stellen Eigenschaften dar, die einem Abonnement von einem StoreFront-Client (typischerweise einer Citrix Workspace-App) zugeordnet sind. Eine Eigenschaft mit mehreren Werten, die durch mehrere Name/Wert-Paare mit demselben 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 der StoreFront-Serverfestplatte

ANZAHL DER 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

ANZAHL DER DATENSÄTZE	GRÖSSE MB
800.000	1.213,02
1.000.000	1.597,15
1.300.000	1919,15
1.500.000	2205,15
2.000.000	2915,15

Größe der Import- und Export-Textdateien

ANZAHL DER DATENSÄTZE	GRÖSSE IN 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

Store-Abonnementzähler

Sie können Microsoft Windows Leistungsindikatoren (**Start > Ausführen > perfmon**) verwenden, um beispielsweise die Gesamtzahl der Abonnementdatensätze auf dem Server oder die Anzahl der Datensätze anzuzeigen, die zwischen StoreFront-Servergruppen synchronisiert werden.

Abonnementzähler mithilfe von PowerShell anzeigen

```
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"
```

Abonnementdaten mit Microsoft SQL Server speichern

> **Hinweis:**

> Dieses Dokument setzt grundlegende Kenntnisse von MS SQL Server und T-SQL-Abfragen voraus. Administratoren müssen mit der Konfiguration, Verwendung und Verwaltung von SQL Server vertraut sein, bevor sie versuchen, diesem Dokument zu folgen.

Einführung

ESENT ist eine einbettbare, transaktionsfähige Datenbank-Engine, die Windows verwenden 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 für die Verwendung einer SQL-Verbindungszeichenfolge konfiguriert ist.

Der Hauptvorteil der Umstellung von StoreFront auf SQL anstelle von ESENT besteht darin, dass Sie SQL-Update-Anweisungen einfach verwenden können, um Abonnementdatensätze zu verwalten, zu ändern oder zu löschen. Wenn Sie SQL verwenden, müssen Sie nicht die gesamten ESENT-Abonnementdaten exportieren, ändern und erneut importieren, wenn kleinere Änderungen an den Abonnementdaten vorgenommen werden.

Um vorhandene Abonnementdaten von ESENT zu Microsoft SQL Server zu migrieren, müssen die aus StoreFront exportierten flachen ESENT-Daten in ein SQL-freundliches Format für den Massenimport umgewandelt werden. Für neue Bereitstellungen ohne neue Abonnementdaten ist dieser Schritt nicht erforderlich. Der Datenumwandlungsschritt ist nur einmal erforderlich.

Hinweis:

Fehler beim Herstellen einer Verbindung zur SQL Server-Instanz, die von StoreFront zum Speichern der Abonnementdaten verwendet wird, aufgrund von Netzwerkausfällen machen die StoreFront-Bereitstellung nicht unbrauchbar. Ausfälle führen lediglich zu einer vorübergehend beeinträchtigten Benutzererfahrung; Benutzer können keine bevorzugten Ressourcen hinzufügen, entfernen oder anzeigen, bis die Verbindung zum SQL Server wiederhergestellt ist. Ressourcen können während des Ausfalls weiterhin aufgelistet und gestartet werden. Das erwartete Verhalten ist dasselbe, als ob der Citrix Subscription Store-Dienst bei Verwendung von ESENT angehalten würde.

Tipp:

Ressourcen, die mit KEYWORDS:Auto oder KEYWORDS:Mandatory konfiguriert sind, verhalten sich bei Verwendung von ESENT oder SQL gleich. Neue SQL-Abonnementdatensätze werden automatisch erstellt, wenn sich ein Benutzer zum ersten Mal anmeldet, falls eines der KEYWORDS in den Ressourcen des Benutzers enthalten ist.

Vorteile von ESENT und SQL Server

ESENT	SQL
Standard und erfordert keine zusätzliche Konfiguration, um StoreFront „out of the box“ zu verwenden.	Viel besser verwaltbar, und Abonnementdaten können einfach mit T-SQL-Abfragen bearbeitet oder aktualisiert werden. Ermöglicht das Löschen oder Aktualisieren von Datensätzen pro Benutzer. Ermöglicht einfache

ESENT	SQL
	Möglichkeiten zum Zählen von Datensätzen pro Anwendung, Delivery Controller oder Benutzer. Ermöglicht einfache Möglichkeiten zum Entfernen unnötiger Benutzerdaten für Benutzer, die das Unternehmen/die Organisation verlassen haben. Ermöglicht einfache Möglichkeiten zum Aktualisieren von Delivery Controller-Referenzen, z. B. wenn der Administrator zur Aggregation wechselt oder neue Delivery Controller bereitgestellt werden.
Einfachere Konfiguration der Replikation zwischen verschiedenen Servergruppen mithilfe von Abonnement-Synchronisierung und Pull-Zeitplänen. Siehe (/de-de/storefront/2507-ltsr/manage-deployment/subscriptions-database/subscription-synchronization.html#configure-subscription-synchronization)	Von StoreFront entkoppelt, sodass vor einem StoreFront-Upgrade keine Sicherung der Abonnementdaten erforderlich ist, da die Daten auf einem separaten SQL Server verwaltet werden. Die Abonnementsicherung ist unabhängig von StoreFront und verwendet SQL-Sicherungsstrategien und -mechanismen.
SQL ist unnötig, wenn keine Abonnementverwaltung erforderlich ist. Wenn die Abonnementdaten niemals aktualisiert werden müssen, erfüllt ESENT wahrscheinlich die Kundenanforderungen.	Eine einzige Kopie der Abonnementdaten, die von allen Mitgliedern der Servergruppe gemeinsam genutzt wird, wodurch die Wahrscheinlichkeit von Datenunterschieden zwischen Servern oder Problemen bei der Datensynchronisierung verringert wird.

Nachteile von ESENT und SQL Server

ESENT	SQL
Keine einfache Möglichkeit, Abonnementdaten einfach und granular zu verwalten. Erfordert, dass Abonnementmanipulationen in exportierten .txt-Dateien vorgenommen werden. Die gesamte Abonnementdatenbank muss exportiert und erneut importiert werden. Potenziell müssen Tausende von Datensätzen mithilfe von Such- und Ersetzungstechniken geändert werden, was arbeitsintensiv und potenziell fehleranfällig ist.	Erfordert grundlegende SQL-Kenntnisse und -Infrastruktur. Kann den Kauf einer SQL-Lizenz erfordern, was die Gesamtbetriebskosten der StoreFront-Bereitstellung erhöht. Eine Citrix Virtual Apps and Desktops-Datenbankinstanz kann jedoch auch mit StoreFront gemeinsam genutzt werden, um Kosten zu senken.

ESENT	SQL
Eine Kopie der ESENT-Datenbank muss auf jedem StoreFront-Server innerhalb einer Servergruppe vorgehalten werden. In seltenen Fällen kann diese Datenbank innerhalb einer Servergruppe oder zwischen verschiedenen Servergruppen nicht synchron sein.	Die Replikation von Abonnementdaten zwischen Servergruppen ist eine nicht triviale Bereitstellungsaufgabe. Sie erfordert mehrere SQL-Instanzen und Transaktionsreplikation zwischen jeder von ihnen pro Rechenzentrum. Dies erfordert spezialisierte MS SQL-Kenntnisse.
	Datenmigration von ESENT und Transformation in ein SQL-freundliches Format erforderlich. Dieser Prozess ist nur einmal erforderlich.
	Zusätzliche Windows-Server und Lizenzen können erforderlich sein.
	Zusätzliche Schritte zur Bereitstellung von StoreFront.

Bereitstellungsszenarien

> **Hinweis:**

> Jeder in StoreFront konfigurierte Store erfordert entweder eine ESENT-Datenbank oder eine Microsoft SQL-Datenbank, wenn Sie Benutzerabonnements unterstützen möchten. Die Methode zur Speicherung der Abonnementdaten wird auf Store-Ebene innerhalb von StoreFront festgelegt.

> Citrix® empfiehlt, dass sich alle Store-Datenbanken auf derselben Microsoft SQL Server-Instanz befinden, um die Verwaltungskomplexität zu reduzieren und das Risiko von Fehlkonfigurationen zu verringern.

Mehrere Stores können dieselbe Datenbank gemeinsam nutzen, vorausgesetzt, sie sind alle so konfiguriert, dass sie dieselbe identische Verbindungszeichenfolge verwenden. Es spielt keine Rolle, ob sie unterschiedliche Delivery Controller verwenden. Der Nachteil, dass mehrere Stores eine Datenbank gemeinsam nutzen, besteht darin, dass es keine Möglichkeit gibt, zu erkennen, welchem Store jeder Abonnementdatensatz entspricht.

Eine Kombination der beiden Datenspeichermethoden ist technisch auf einer einzelnen StoreFront-Bereitstellung mit mehreren Stores möglich. Es ist möglich, einen Store für die Verwendung von ESENT und einen anderen für die Verwendung von SQL zu konfigurieren. Dies wird jedoch aufgrund der erhöhten Verwaltungskomplexität und des Potenzials für Fehlkonfigurationen nicht empfohlen.

Es gibt vier Szenarien, die Sie zum Speichern von Abonnementdaten in SQL Server verwenden können:

SZENARIO 1: EINZELNER STOREFRONT-SERVER ODER SERVERGRUPPE MIT ESENT (STANDARD)

Standardmäßig verwenden alle StoreFront-Versionen seit Version 2.0 eine flache ESENT-Datenbank, um Abonnementdaten zwischen Mitgliedern einer Servergruppe zu speichern und zu replizieren. Jedes Mitglied der Servergruppe verwaltet eine identische Kopie der Abonnementdatenbank, die mit allen anderen Mitgliedern der Servergruppe synchronisiert wird. Dieses Szenario erfordert keine zusätzlichen Konfigurationsschritte. Dieses Szenario ist für die meisten Kunden geeignet, die keine häufigen Änderungen an Delivery Controller-Namen erwarten oder keine häufigen Verwaltungsaufgaben an ihren Abonnementdaten, wie das Entfernen oder Aktualisieren alter Benutzerabonnements, durchführen müssen.

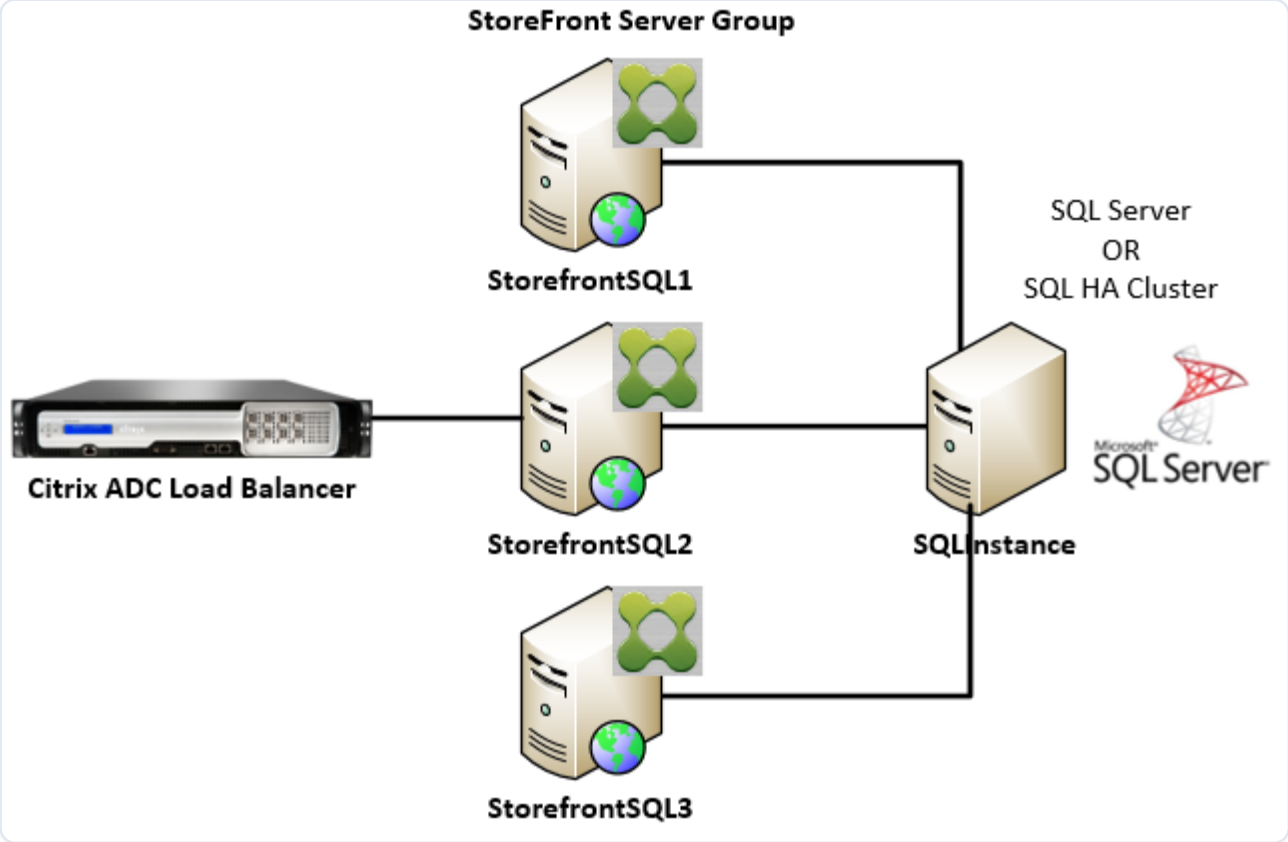
SZENARIO 2: EINZELNER STOREFRONT-SERVER UND EINE LOKAL INSTALLIERTE MICROSOFT SQL SERVER-INSTANZ

StoreFront verwendet eine lokal installierte SQL Server-Instanz, und beide Komponenten befinden sich auf demselben Server. Dieses Szenario eignet sich für eine einfache Einzel-StoreFront-Bereitstellung, bei der Kunden möglicherweise häufige Änderungen an Delivery Controller-Namen vornehmen müssen oder häufige Verwaltungsaufgaben an ihren Abonnementdaten, wie das Entfernen oder Aktualisieren alter Benutzerabonnements, durchführen müssen, aber keine hochverfügbare StoreFront-Bereitstellung benötigen. Citrix empfiehlt dieses Szenario nicht für Servergruppen, da es einen Single Point of Failure auf dem Servergruppenmitglied schafft, das die Microsoft SQL-Datenbankinstanz hostet. Dieses Szenario ist nicht für große Unternehmensbereitstellungen geeignet.

SZENARIO 3: STOREFRONT-SERVERGRUPPE UND EINE DEDIZIERTE MICROSOFT SQL SERVER-INSTANZ, DIE FÜR HOCHVERFÜGBARKEIT KONFIGURIERT IST (EMPFOHLEN)

Alle Mitglieder der StoreFront-Servergruppe stellen eine Verbindung zur selben dedizierten Microsoft SQL Server-Instanz oder einem SQL-Failovercluster her. Dies ist das am besten geeignete Modell für große Unternehmensbereitstellungen, bei denen Citrix-Administratoren häufige Änderungen an Delivery Controller-Namen vornehmen oder häufige Verwaltungsaufgaben

an ihren Abonnementdaten, wie das Entfernen oder Aktualisieren alter Benutzerabonnements, durchführen und Hochverfügbarkeit benötigen.



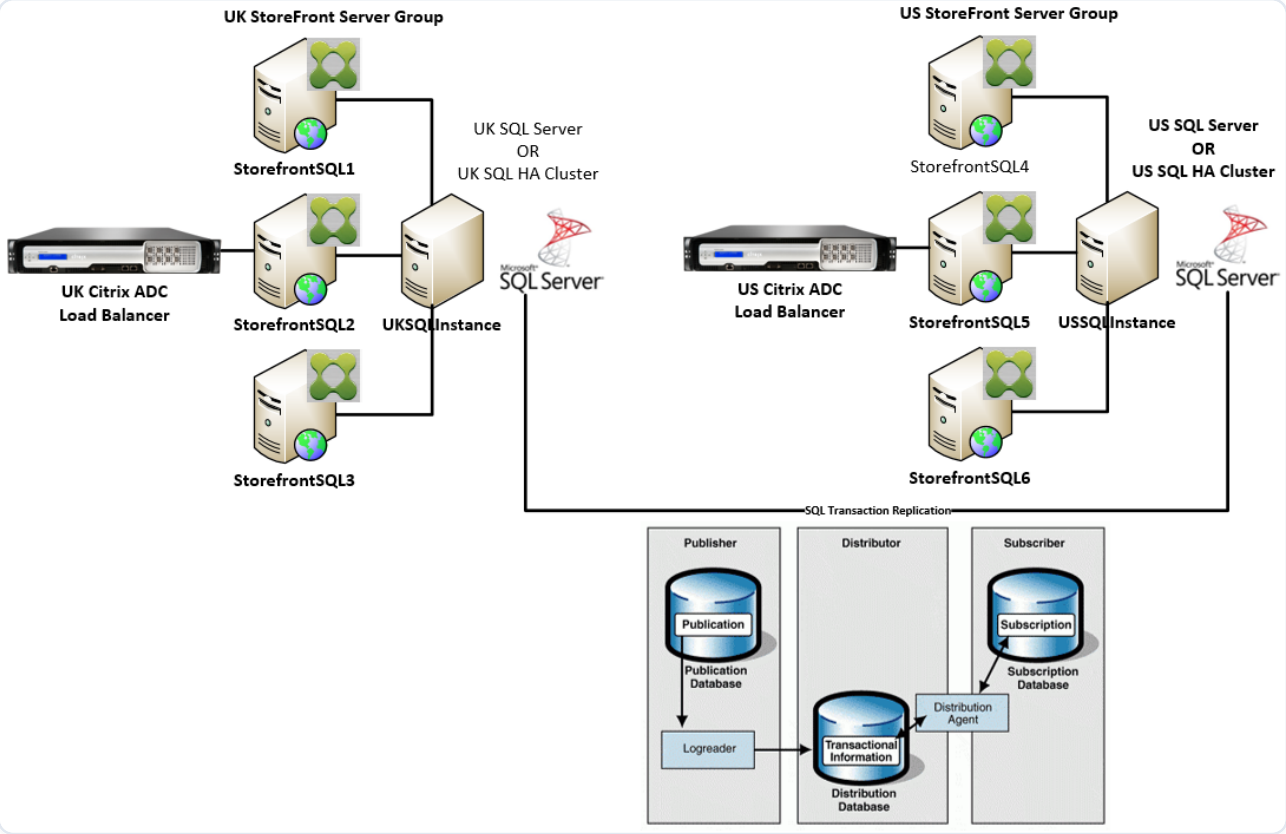
SZENARIO 4: MEHRERE STOREFRONT-SERVERGRUPPEN UND EINE DEDIZIERTE MICROSOFT SQL SERVER-INSTANZ IN JEDEM RECHENZENTRUM PRO SERVERGRUPPE

Hinweis:

Dies ist eine erweiterte Konfiguration. Versuchen Sie dies nur, wenn Sie ein erfahrener SQL Server-Administrator sind, der mit der Transaktionsreplikation vertraut ist und über die notwendigen Fähigkeiten verfügt, um sie erfolgreich bereitzustellen.

Dies ist dasselbe wie Szenario 3, erweitert es jedoch auf Situationen, in denen mehrere StoreFront-Servergruppen in verschiedenen Remote-Rechenzentren erforderlich sind. Citrix-Administratoren können wählen, Abonnementdaten zwischen verschiedenen Servergruppen im selben oder in verschiedenen Rechenzentren zu synchronisieren. Jede Servergruppe im Rechenzentrum stellt eine Verbindung zu ihrer eigenen dedizierten Microsoft SQL Server-Instanz her, um Redundanz, Failover und Leistung zu gewährleisten. Dieses Szenario erfordert eine beträchtliche zusätzliche Microsoft SQL Server-Konfiguration und -Infrastruktur.

> Es basiert vollständig auf der Microsoft SQL-Technologie, um die Abonnementdaten und deren SQL-Transaktionen zu replizieren.



Ressourcen

Sie können die folgenden Skripte von `<https://github.com/citrix/sample-scripts/tree/master/storefront>` herunterladen, um Ihnen zu helfen:

KONFIGURATIONSSKRIPTE

- **Set-STFDatabase.ps1** – legt die MS SQL-Verbindungszeichenfolge für jeden Store fest. Auf dem StoreFront-Server ausführen.
- **Add-LocalAppPoolAccounts.ps1** – gewährt den App-Pools des lokalen StoreFront-Servers Lese- und Schreibzugriff auf die SQL-Datenbank. Für Szenario 2 auf dem SQL-Server ausführen.
- **Add-RemoteSFAccounts.ps1** – gewährt allen StoreFront-Servern in einer Servergruppe Lese- und Schreibzugriff auf die SQL-Datenbank. Für Szenario 3 auf dem SQL-Server ausführen.
- **Create-StoreSubscriptionsDB-2016.sql** – erstellt die SQL-Datenbank und das Schema. Auf dem SQL-Server ausführen.

DATENTRANSFORMATIONS- UND IMPORTSKRIPTS

- **Transform-SubscriptionDataForStore.ps1** – exportiert und transformiert vorhandene Abonnementdaten in ESENT in ein SQL-freundliches Format für den Import.
- **Create-ImportSubscriptionDataSP.sql** – erstellt eine gespeicherte Prozedur zum Importieren der von Transform-SubscriptionDataForStore.ps1 transformierten Daten. Führen Sie dieses 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 eine lokal installierte Microsoft SQL Server-Instanz

Erstellen Sie auf dem Microsoft SQL-Server eine lokale Sicherheitsgruppe namens `<SQLServer>\StoreFrontServers` und fügen Sie die virtuellen Konten für `IIS APPPOOL\DefaultAppPool` und `IIS APPPOOL\Citrix Receiver for Web` hinzu, damit das lokal installierte StoreFront in SQL lesen und schreiben kann. Diese Sicherheitsgruppe wird im .SQL-Skript referenziert, das das Datenbankschema für Abonnements erstellt. Stellen Sie daher sicher, dass der Gruppenname übereinstimmt.

Sie können das Skript Add-LocalAppPoolAccounts.ps1 herunterladen, um Unterstützung zu erhalten.

Installieren Sie StoreFront, bevor Sie das Skript *Add-LocalAppPoolAccounts.ps1* ausführen. Das Skript hängt von der Fähigkeit ab, das virtuelle IIS-Konto `IIS APPPOOL\Citrix Receiver for Web` zu finden, das erst existiert, nachdem StoreFront installiert und konfiguriert wurde. `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



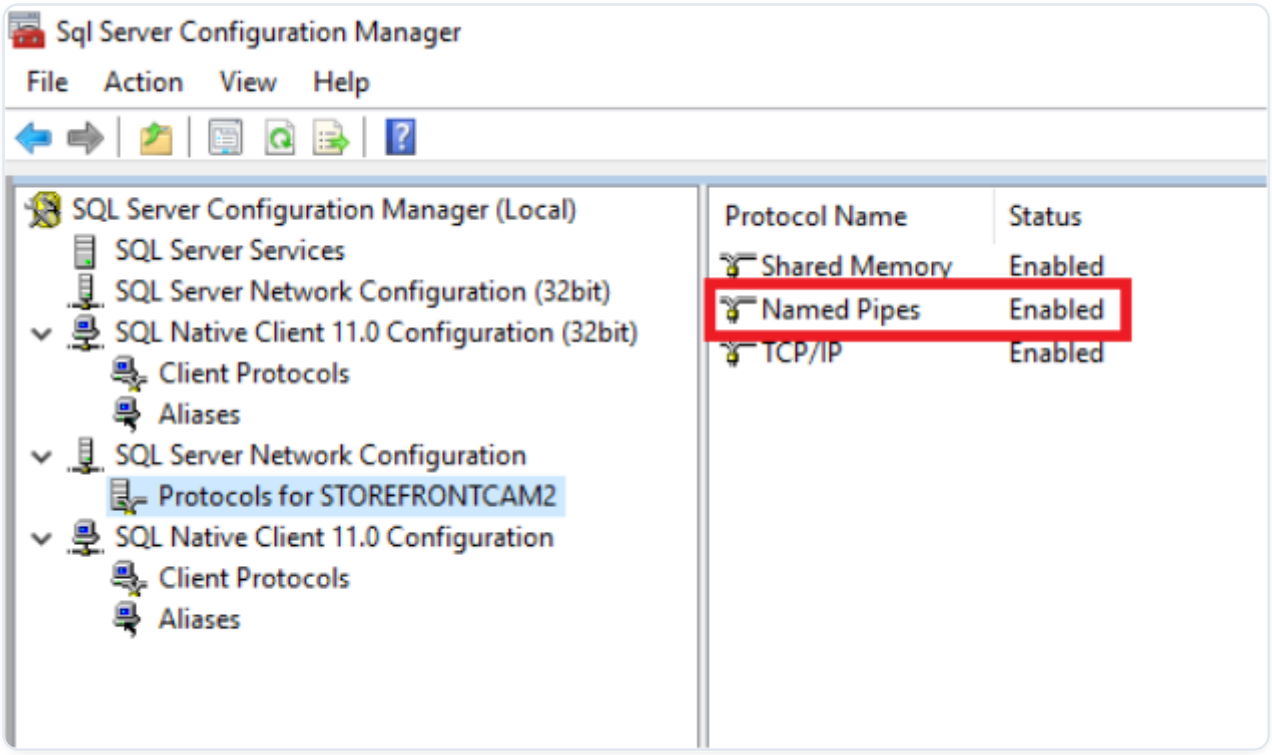
$Account = [ADSI]"WinNT://$WebRSID"

$Group.Add($Account.Path)



Write-Host "AppPools added to $LocalGroupName local group"
-ForegroundColor "Green"
```

Aktivieren Sie benannte Pipes in Ihrer lokalen SQL-Instanz mithilfe des SQL Server-Konfigurations-Managers. Benannte Pipes sind für die Interprozesskommunikation zwischen StoreFront und SQL Server erforderlich.

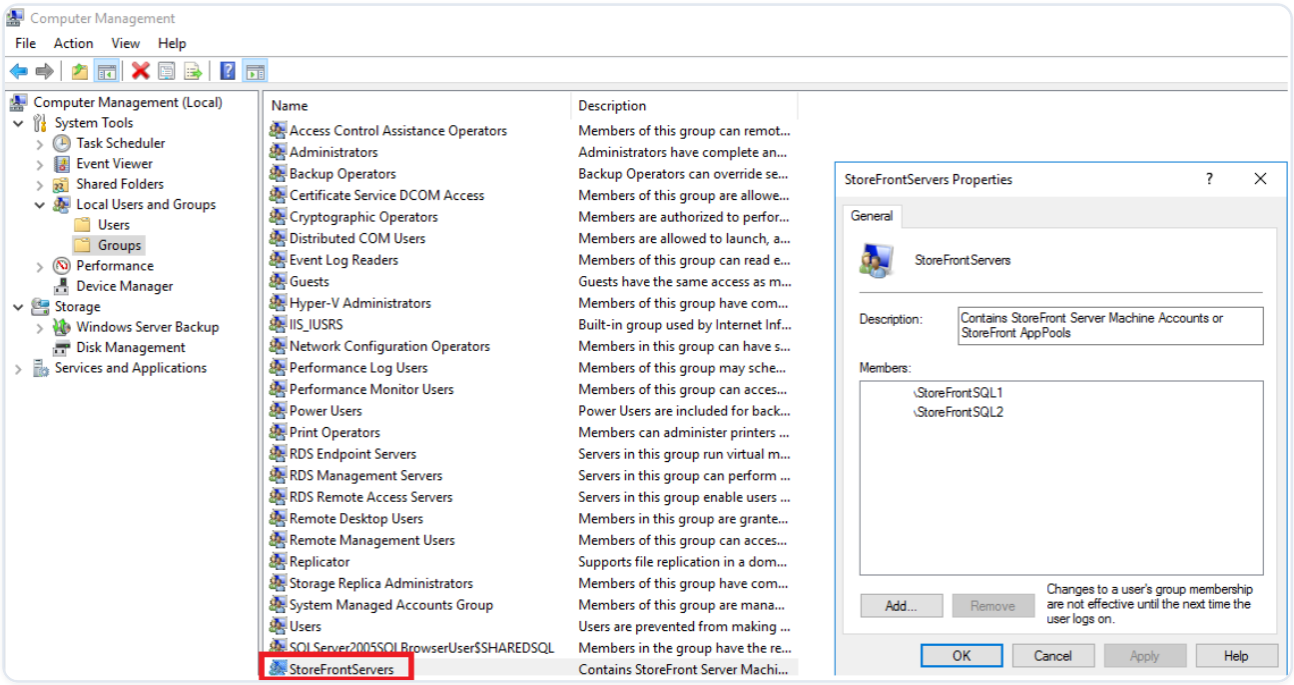


Stellen Sie sicher, dass die Windows-Firewallregeln korrekt konfiguriert sind, um SQL Server-Verbindungen über einen bestimmten Port oder dynamische Ports zuzulassen. Informationen dazu in Ihrer Umgebung finden Sie in der Microsoft-Dokumentation.

> **Tipp:**
>
> Wenn die Verbindung zur lokalen SQL-Instanz fehlschlägt, überprüfen Sie, ob localhost oder `<hostname>`, das in der Verbindungszeichenfolge verwendet wird, in die korrekte IPv4-Adresse aufgelöst wird. Windows versucht möglicherweise, IPv6 anstelle von IPv4 zu verwenden, und die DNS-Auflösung von localhost kann ::1 anstelle der korrekten IPv4-Adresse des StoreFront- und SQL-Servers zurückgeben. Um dieses Problem zu beheben, muss möglicherweise der IPv6-Netzwerkstack auf dem Hostserver vollständig deaktiviert werden.

Szenario 3: StoreFront-Servergruppe und eine dedizierte Microsoft SQL Server-Instanz

Erstellen Sie auf dem Microsoft SQL Server eine lokale Sicherheitsgruppe namens `<SQLServer>\StoreFrontServers` und fügen Sie alle Mitglieder der StoreFront-Servergruppe hinzu. Diese Sicherheitsgruppe wird später im Skript **Create-StoreSubscriptionsDB-2016.sql** referenziert, das das Abonnementdatenbankschema in SQL erstellt.



Fügen Sie alle Domänencomputer-Konten der StoreFront-Servergruppe der Gruppe `<SQLServer>\StoreFrontServers` hinzu. Nur die in der Gruppe aufgeführten Domänencomputer-Konten der StoreFront-Server können Abonnementdatensätze in SQL lesen und schreiben, wenn die Windows-Authentifizierung vom SQL Server verwendet wird. Die folgende PowerShell-Funktion, die im Skript Add-RemoteSFAccounts.ps1 bereitgestellt wird, erstellt die lokale Sicherheitsgruppe und fügt ihr zwei StoreFront-Server mit den 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"



    # Create Local Security Group

    $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"

    $LocalGroup = $Computer.Create("group",$LocalGroupName)

    $LocalGroup.setinfo()

    $LocalGroup.description = $Description

    $Localgroup.SetInfo()

Write-Host "$LocalGroupName local group created" -ForegroundColor "Green"

}

Write-Host "Adding $StoreFrontServers to $LocalGroupName local group"
-ForegroundColor "Yellow"



foreach ($StoreFrontServer in $StoreFrontServers)
```

```
{

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

    $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"

    $Group.Add($Computer.Path)

}

Write-Host "$StoreFrontServers added to $LocalGroupName" -ForegroundColor
"Green"

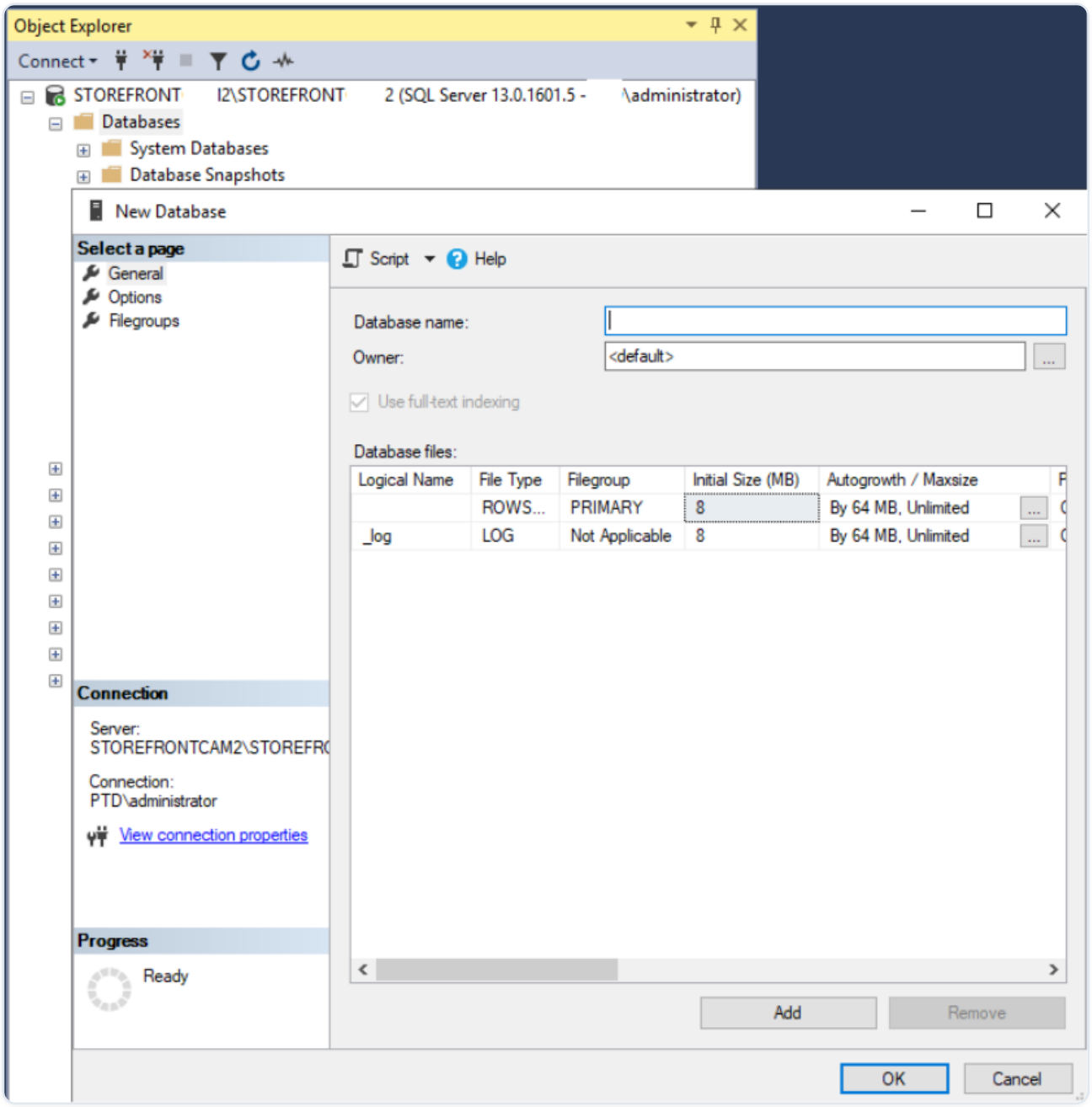
}

Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers
@("StoreFrontSQL1","StoreFrontSQL2")
```

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 im .SQL-Skript so fest, dass er dem Installationsort Ihrer SQL-Version oder dem Speicherort ihrer Datenbankdateien entspricht. Das Beispielskript Create-StoreSubscriptionsDB-2016.sql verwendet SQL Server 2016 Enterprise.

Erstellen Sie eine leere Datenbank mit SQL Server Management Studio (SSMS), indem Sie mit der rechten Maustaste auf **Datenbanken** klicken und dann **Neue Datenbank** auswählen.



Geben Sie einen **Datenbanknamen** ein, der Ihrem Store entspricht, oder wählen Sie einen anderen Namen wie *STFSubscriptions*.

Bevor Sie das Skript ausführen, ändern Sie für jeden Store in Ihrer StoreFront-Bereitstellung die Referenzen im Beispielskript so, dass sie Ihren StoreFront- und SQL-Bereitstellungen entsprechen. Ändern Sie beispielsweise:

- Benennen Sie jede Datenbank, die Sie erstellen, so, dass sie dem Store-Namen in StoreFront in `USE [STFSubscriptions]` entspricht.
- Legen Sie den Pfad zu den Datenbankdateien .mdf und .ldf fest, wo Sie die Datenbank speichern möchten.

`C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.mdf`

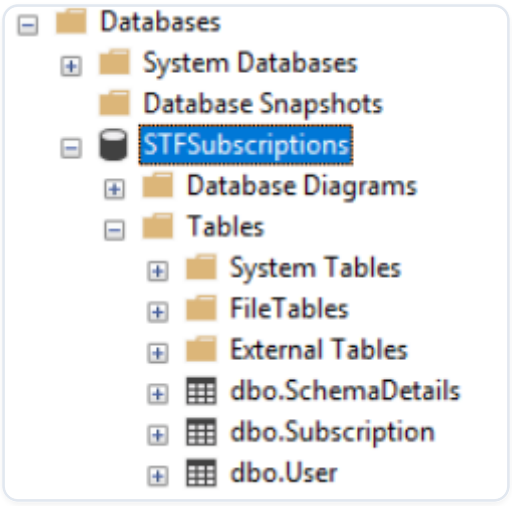
`C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.ldf`

- Legen Sie die Referenz auf den Namen Ihres SQL-Servers innerhalb des Skripts fest:

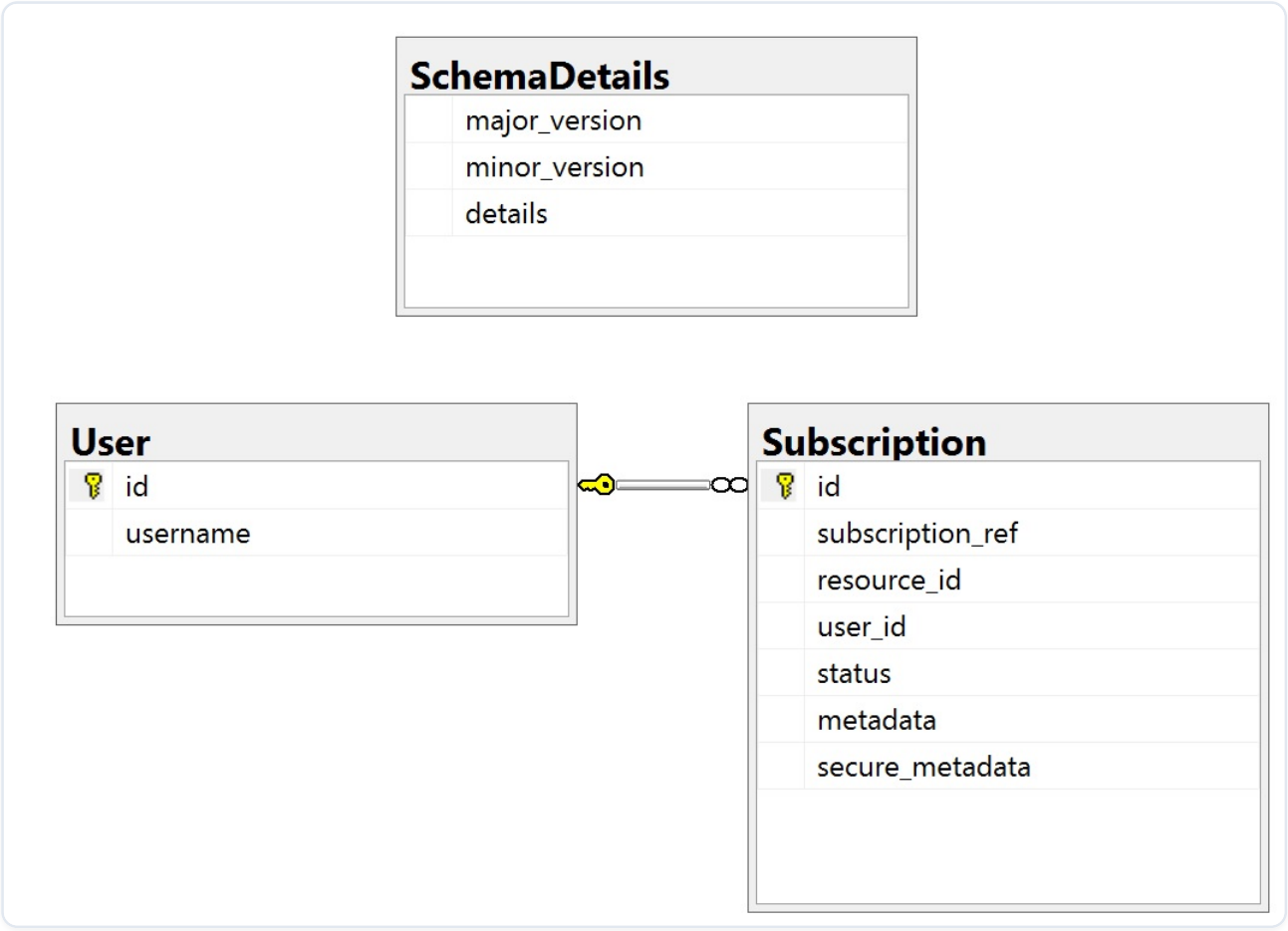
`CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;`;

`ALTER LOGIN [SQL2016\StoreFrontServers]`

Führen Sie das Skript aus. Nach erfolgreicher Konfiguration des Schemas werden drei Datenbanktabellen erstellt: *SchemaDetails*, *Subscription* und *User*.



Das folgende Datenbankdiagramm zeigt das Schema der Abonnementdatenbank, das das Skript *Create-StoreSubscriptionsDB-2016.sql* erstellt:



Konfigurieren der SQL Server-Verbindungszeichenfolge für jeden StoreFront-Store

Szenario 1

> **Tipp:**
>
> Die ursprünglichen Abonnementdaten, die auf der Festplatte in der ESENT-Datenbank gespeichert sind, werden nicht zerstört oder entfernt. Wenn Sie sich entscheiden, von Microsoft SQL Server zur Verwendung von ESENT zurückzukehren, können Sie die Store-Verbindungszeichenfolge entfernen und einfach wieder die ursprünglichen Daten verwenden. Alle zusätzlichen Abonnements, die erstellt wurden, während SQL für den Store verwendet wurde, existieren nicht in ESENT, und Benutzer sehen diese neuen Abonnementdatensätze nicht. Alle ursprünglichen Abonnementdatensätze sind weiterhin vorhanden.

SO AKTIVIEREN SIE ESENT-ABONNEMENTS IN EINEM STORE ERNEUT

Öffnen Sie die 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
```

Szenarien 2, 3 und 4

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

Geben Sie den Store an, für den Sie eine Verbindungszeichenfolge festlegen möchten, indem Sie **\ $StoreVirtualPath** verwenden.

```
$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;"
```

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
```

Wiederholen Sie den Vorgang für jeden Store in Ihrer Bereitstellung, wenn Sie alle so konfigurieren möchten, dass sie eine SQL-Verbindungszeichenfolge verwenden.

Vorhandene Daten von ESENT zu Microsoft SQL Server migrieren

Um Ihre vorhandenen ESENT-Daten zu SQL zu migrieren, ist ein zweistufiger Datentransformationsprozess erforderlich. Zwei Skripte werden bereitgestellt, um Sie bei der Durchführung dieses einmaligen Vorgangs zu unterstützen. Wenn die Verbindungszeichenfolge in StoreFront und die SQL-Instanz korrekt konfiguriert sind, werden alle neuen Abonnements automatisch in SQL im richtigen Format erstellt. Nach der Migration werden die historischen ESENT-Abonnementdaten in ein SQL-Format umgewandelt, und Benutzer können auch ihre zuvor abonnierten Ressourcen sehen.

Beispiel: Vier SQL-Abonnements für denselben Domänenbenutzer



SCHRITT 1: VERWENDEN SIE DAS SKRIPT TRANSFORM-SUBSCRIPTIONDATAFORSTORE.PS1, UM DIE ESENT-DATEN IN EIN SQL-FREUNDLICHES FORMAT FÜR DEN MASSENIMPORT ZU KONVERTIEREN

Melden Sie sich beim StoreFront-Server an, von dem Sie ESENT-Daten transformieren möchten.

Jedes Mitglied einer Servergruppe ist geeignet, vorausgesetzt, alle enthalten die gleiche Anzahl von Abonnementdatensätzen.

Öffnen Sie die 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 liefert ausführliches Feedback zu jeder verarbeiteten Abonnementzeile, um das Debugging zu erleichtern und Ihnen bei der Beurteilung des Erfolgs des Vorgangs zu helfen. Die Verarbeitung kann lange dauern.

Die transformierten Daten werden nach Abschluss des Skripts auf dem Desktop des aktuellen Benutzers nach `<StoreName>SQL.txt` 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 auf den SQL-Server migrieren möchten.

SCHRITT 2: VERWENDEN SIE EINE T-SQL-GESPEICHERTE PROZEDUR, UM DIE TRANSFORMIERTEN DATEN PER MASSEN-SQL-IMPORT ZU IMPORTIEREN

Die Daten jedes Stores müssen einzeln importiert werden.

Kopieren Sie die in Schritt 1 erstellte `<StoreName>SQL.txt`-Datei vom Desktop des StoreFront-Servers nach `C:\` auf den Microsoft SQL-Server und benennen Sie sie in SubscriptionsSQL.txt um.

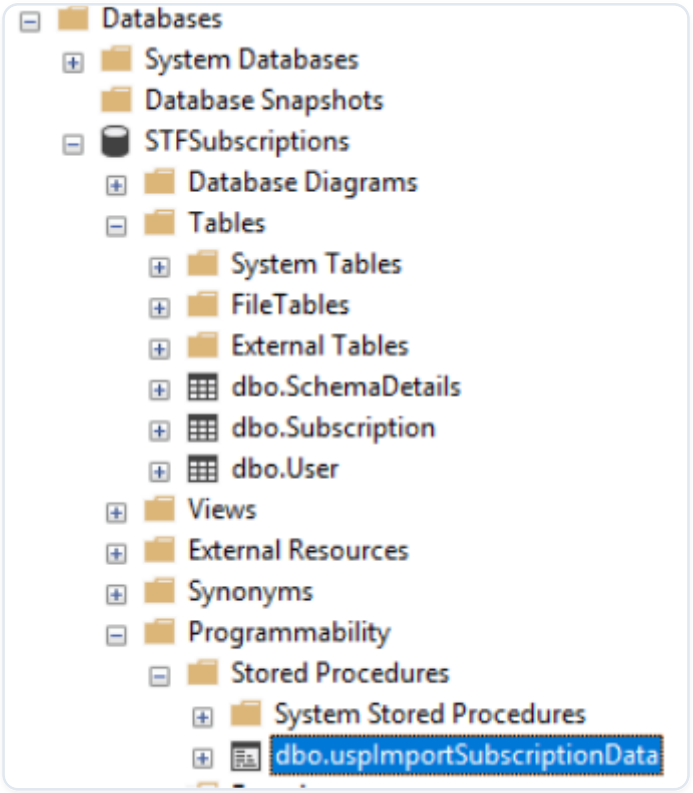
Das Skript Create-ImportSubscriptionDataSP.sql erstellt eine T-SQL-gespeicherte Prozedur, um die Abonnementdaten per Massenimport zu importieren. Es entfernt doppelte Einträge für jeden eindeutigen Benutzer, sodass die resultierenden SQL-Daten korrekt normalisiert und in die richtigen Tabellen aufgeteilt werden.

Bevor Sie *Create-ImportSubscriptionDataSP.sql* ausführen, ändern Sie `USE [STFSubscriptions]`, um sie an die Datenbank anzupassen, unter der Sie die gespeicherte Prozedur erstellen möchten.

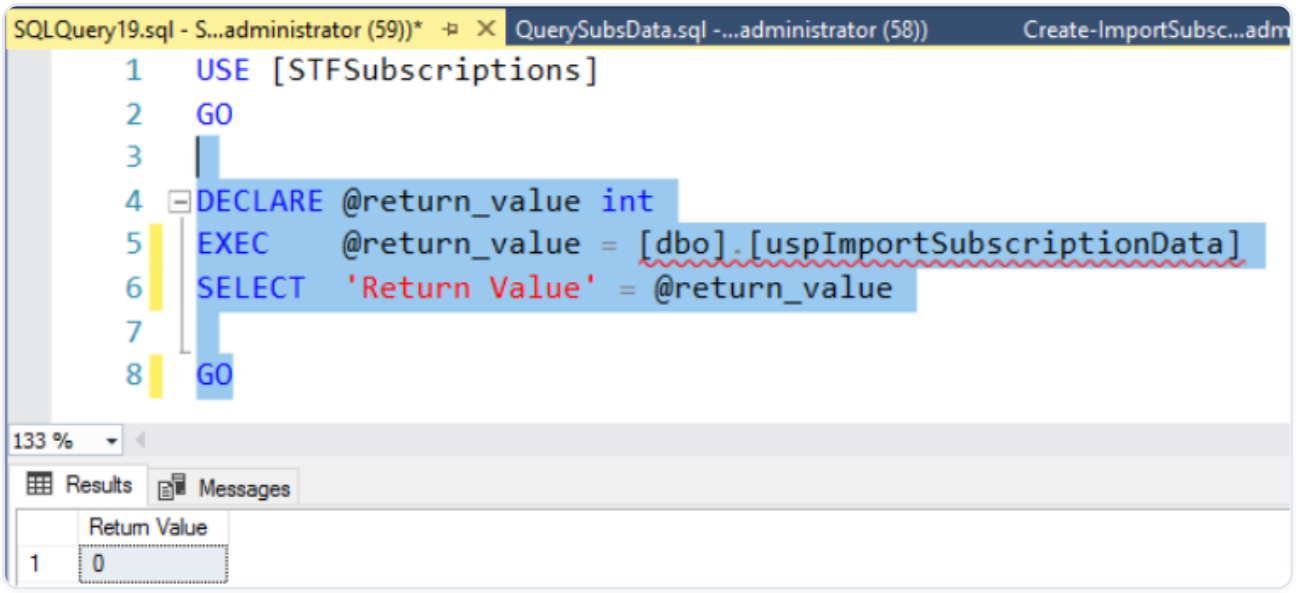
Öffnen Sie die Datei *Create-ImportSubscriptionDataSP.sql* mit SQL Server Management Studio und führen Sie den darin enthaltenen Code aus. Dieses Skript fügt die gespeicherte Prozedur *ImportSubscriptionDataSP* der Datenbank hinzu, die Sie zuvor erstellt haben.

Nach erfolgreicher Erstellung der gespeicherten Prozedur wird die folgende Meldung in der SQL-Konsole 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, dann **Gespeicherte Prozedur ausführen** auswählen und auf **OK** klicken.



Der Rückgabewert 0 zeigt an, dass alle Daten erfolgreich importiert wurden. Alle Probleme beim Import werden in der SQL-Konsole protokolliert. Nachdem die gespeicherte Prozedur erfolgreich ausgeführt wurde, vergleichen Sie die Gesamtzahl der Abonnementdatensätze und eindeutigen Benutzer, die Transform-SubscriptionDataForStore.ps1 bereitstellt, mit dem Ergebnis der beiden unten stehenden SQL-Abfragen. Die beiden Gesamtzahlen sollten übereinstimmen.

Die Gesamtzahl der Abonnements aus dem Transformationsskript sollte mit der von SQL gemeldeten Gesamtzahl übereinstimmen durch

```
SELECT COUNT(*) AS TotalSubscriptions

FROM [Subscription]
```

Die Anzahl der eindeutigen Verwendungen aus dem Transformationsskript sollte mit der Anzahl der Datensätze in der Benutzertabelle übereinstimmen, die von SQL gemeldet wird durch

```
SELECT COUNT(*) AS TotalUsers

FROM [User]
```

Wenn das Transformationsskript 100 eindeutige Benutzer und 1000 Abonnementdatensätze insgesamt anzeigt, sollte SQL nach erfolgreicher Migration dieselben beiden 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 ihre Ressourcen abonnieren oder abbestellen. Neue Benutzer und Abonnementdatensätze werden ebenfalls in SQL erstellt.

SCHRITT 3 FÜHREN SIE T-SQL-ABFRAGEN FÜR IHRE IMPORTIERTEN DATEN AUS

Hinweis:

Alle Delivery Controller-Namen sind Groß- und Kleinschreibung-sensitiv und müssen exakt mit der Groß-/Kleinschreibung und dem Namen übereinstimmen, die in StoreFront verwendet werden.

```
-- Get all SQL subscription records

Use [STFSubscriptions]

SELECT * FROM [Subscription]

SELECT * FROM [User]
```

```
-- 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'
```

```
-- 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'
```

Bestehende Abonnementdatensätze mit T-SQL aktualisieren oder löschen

HAFTUNGSAUSSCHLUSS:

Alle Beispiel-SQL-Update- und Delete-Anweisungen werden ausschließlich auf eigenes Risiko verwendet. Citrix ist nicht verantwortlich für Verluste oder versehentliche Änderungen Ihrer Abonnementdaten durch falsche Verwendung der bereitgestellten Beispiele. Die

folgenden T-SQL-Anweisungen dienen als Leitfaden, um einfache Aktualisierungen zu ermöglichen. Sichern Sie alle Abonnementdaten in vollständigen SQL-Datenbank-Backups, bevor Sie versuchen, Ihre Abonnements zu aktualisieren oder veraltete Datensätze zu entfernen. Wenn die erforderlichen Backups nicht durchgeführt werden, kann dies zu Datenverlust oder -beschädigung führen. Bevor Sie Ihre eigenen T-SQL-UPDATE- oder DELETE-Anweisungen für die Produktionsdatenbank ausführen, testen Sie diese mit Dummy-Daten oder einer redundanten Kopie der Produktionsdaten außerhalb der aktiven Produktionsdatenbank.

Hinweis:

Alle Site-Namen sind Groß-/Kleinschreibung-sensitiv und müssen exakt der in StoreFront verwendeten Groß-/Kleinschreibung und dem dort verwendeten Namen entsprechen.

```
-- Update the site name used in all subscriptions.

Use [STFSubscriptions]

UPDATE [Subscription]

SET [resource_id] = REPLACE(resource_id,'OldSiteName.','NewSiteName.')

WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
-- 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.%'
```

```
-- Delete all subscription records for a particular site

Use [STFSubscriptions]

DELETE FROM [Subscription]

WHERE [resource_id] LIKE 'site.%'
```

```
-- OR for aggregated resources use the name of the aggregation group

Use [STFSubscriptions]

DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
```

```
-- Delete all subscription records for a particular application

Use [STFSubscriptions]

DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] LIKE '%.Application'
```

```
-- Delete all subscription records for an application published via a
specific site

Use [STFSubscriptions]

DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] = 'Site.Application'
```

```
-- 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'
```

```
-- 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)
```

Abonnement-Synchronisierung

StoreFront synchronisiert Favoriten, auch bekannt als Abonnements, automatisch zwischen Servern in einer StoreFront-Servergruppe. Wenn Sie mehrere Servergruppen haben (typischerweise an verschiedenen geografischen Standorten), können Sie eine periodische Pull-Synchronisierung der Benutzerabonnements von Stores in verschiedenen StoreFront-Bereitstellungen konfigurieren. Dies muss mithilfe von PowerShell erfolgen.

> **Hinweis:**

> Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole verwenden, um Ihre StoreFront-Konfiguration zu verwalten. Schließen Sie ebenfalls alle PowerShell-Instanzen, bevor Sie die StoreFront-Konsole öffnen.

> Beachten Sie bei der Einrichtung Ihrer Abonnement-Synchronisierung, dass die konfigurierten Sites zwischen den synchronisierten Stores identisch benannt sein müssen, einschließlich der Groß-/Kleinschreibung. Wenn die Site-Namen nicht exakt dupliziert werden, kann dies dazu führen, dass Benutzer unterschiedliche Abonnements über die synchronisierten Stores hinweg haben. Wenn Sie Abonnements von aggregierten Ressourcen synchronisieren, muss der Name der von beiden Stores verwendeten Aggregationsgruppen ebenfalls übereinstimmen. Site-Namen und Aggregationsgruppennamen sind Groß-/Kleinschreibung-sensitiv; zum Beispiel ist *CVAD_US* anders als *Cvad_Us*.

1. Verwenden Sie ein Konto mit lokalen Administratorberechtigungen, um die Windows PowerShell ISE zu starten.
2. Um die Synchronisierung zu konfigurieren, verwenden Sie den Befehl Publish-STFServerGroupConfiguration. Sie können entweder eine Startzeit und ein wiederkehrendes Intervall oder eine Liste von Zeiten angeben. Zum Beispiel, um die Synchronisierung um 08:00 Uhr zu starten und dann alle 30 Minuten:

   ```
   Add-STFSubscriptionSynchronizationSchedule -RecurringStartTime 08:00:00
   -RecurringInterval 30
   ```

   Wir empfehlen, Pull-Zeitpläne zu staffeln, um zu vermeiden, dass zwei Servergruppen gleichzeitig versuchen, Abonnementdaten voneinander abzurufen. Zum Beispiel würde ein Zeitplan zum Abrufen von Daten von jeder Servergruppe alle 60 Minuten wie folgt konfiguriert werden. Servergruppe 1 ruft Daten von Servergruppe 2 um 01:00, 02:00, 03:00 Uhr usw. ab. Servergruppe 2 ruft Daten von Servergruppe 1 um 01:30, 02:30, 03:30 Uhr usw. ab.
3. Um die Remote-StoreFront-Bereitstellung anzugeben, die den zu synchronisierenden Store enthält, geben Sie den folgenden Befehl ein. Sie müssen dies für jedes Rechenzentrum konfigurieren, in dem sich eine StoreFront-Servergruppe befindet, damit sie Abonnementdaten von anderen Remote-Rechenzentren abrufen kann. Siehe die folgenden Beispiele für Rechenzentren in den USA und Großbritannien:

- Auf StoreFront-Servern im US-Rechenzentrum ausführen, um Daten von den Servern im UK-Rechenzentrum abzurufen:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/Citrix/
Store"

Add-STFSubscriptionSynchronizationSource -FriendlyName
"SyncFromUKStore" -StoreService $StoreObject
-RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.com"
```

- Auf StoreFront-Servern im UK-Rechenzentrum ausführen, um Daten von den Servern im US-Rechenzentrum abzurufen:

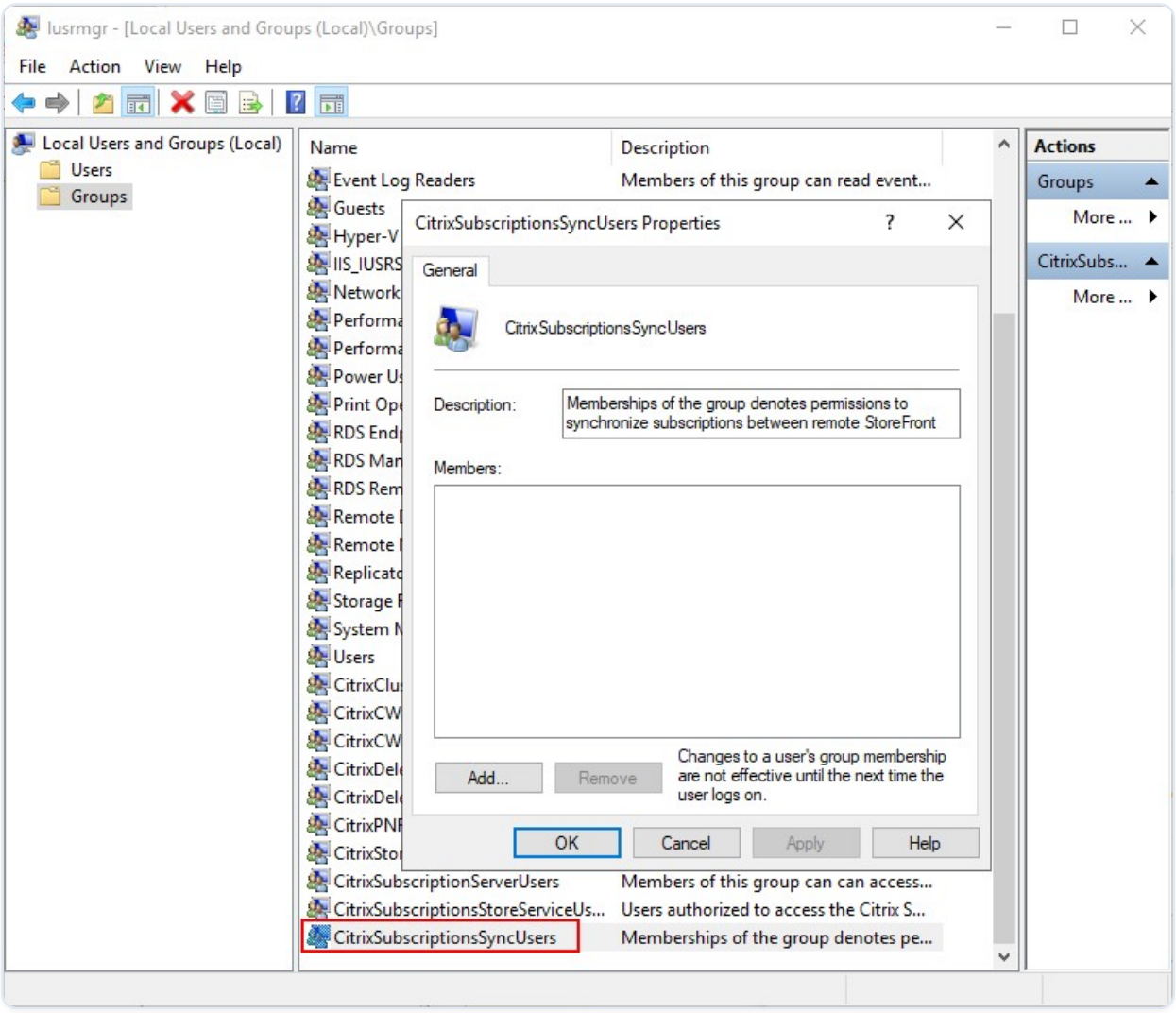
```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/Citrix/
Store"

Add-STFSubscriptionSynchronizationSource -FriendlyName
"SyncFromUSStore" -StoreService $StoreObject
-RemoteStoreFrontAddress "USloadbalancedStoreFront.example.com"
```

wobei *FriendlyName* ein Name ist, der Ihnen hilft, die Remote-Bereitstellung zu identifizieren, und *RemoteStoreFrontAddress* der FQDN des StoreFront-Servers oder der Lastenausgleichs-Servergruppe für die Remote-Bereitstellung ist. Um Anwendungsabonnements zwischen zwei oder mehr Stores zu synchronisieren, müssen alle zu synchronisierenden Stores in ihren jeweiligen StoreFront-Bereitstellungen denselben Namen haben.

4. Fügen Sie die Microsoft Active Directory-Domänenmaschinenkonten für jeden StoreFront-Server in der Remote-Bereitstellung der lokalen Windows-Benutzergruppe CitrixSubscriptionSyncUsers auf dem aktuellen Server hinzu.

   Dies ermöglicht es den aktuellen Servern, neue oder aktualisierte Abonnementdaten von den in CitrixSubscriptionSyncUsers aufgeführten Remote-Servern abzurufen, sobald Sie einen Synchronisierungszeitplan konfiguriert haben. Weitere Informationen zum Ändern lokaler Benutzergruppen finden Sie unter `<https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11)>`.



5. Wenn Sie den Zeitplan wie beabsichtigt konfiguriert haben, verwenden Sie die Citrix StoreFront-Verwaltungskonsole oder die unten stehende PowerShell, um die Abonnement-Synchronisierungszeitpläne und -quellen an alle anderen Server in der Gruppe weiterzugeben.

```
Publish-STFServerGroupConfiguration
```

   Weitere Informationen zum Propagieren von Änderungen in einer StoreFront-Bereitstellung mit mehreren Servern finden Sie unter Servergruppen konfigurieren.

6. Um einen vorhandenen Abonnement-Synchronisierungszeitplan zu entfernen, führen Sie den folgenden Befehl aus und propagieren Sie dann die Konfigurationsänderung an die anderen StoreFront-Server in der Bereitstellung.

```
Clear-STFSubscriptionSynchronizationSchedule

Publish-STFServerGroupConfiguration
```

7. Um eine bestimmte Abonnement-Synchronisierungsquelle zu entfernen, führen Sie den folgenden Befehl aus und propagieren Sie dann die Konfigurationsänderung an die anderen StoreFront-Server in der Bereitstellung.

   ```
   Remove-STFSubscriptionSynchronizationSource -FriendlyName
   "SyncFromUKStore"

   Publish-STFServerGroupConfiguration
   ```

8. Um alle vorhandenen Abonnement-Synchronisierungsquellen zu entfernen, führen Sie den folgenden Befehl aus und propagieren Sie dann die Konfigurationsänderung an die anderen StoreFront-Server in der Bereitstellung.

   ```
   Clear-STFSubscriptionSynchronizationSource

   Publish-STFServerGroupConfiguration
   ```

9. Um die derzeit für Ihre StoreFront-Bereitstellung konfigurierten Abonnement-Synchronisierungszeitpläne aufzulisten, führen Sie den folgenden Befehl aus.

   ```
   Get-STFSubscriptionSynchronizationSchedule
   ```

10. Um die derzeit für Ihre StoreFront-Bereitstellung konfigurierten Abonnement-Synchronisierungsquellen aufzulisten, führen Sie den folgenden Befehl aus.

    ```
    Get-STFSubscriptionSynchronizationSource
    ```

StoreFront™ aktualisieren

Durch ein Upgrade bleiben Ihre StoreFront-Konfiguration und die Favoriten der Benutzer erhalten. Im Gegensatz dazu entfernt die Deinstallation von StoreFront StoreFront und die zugehörigen Dienste, Sites, Favoriten (auf eigenständigen Servern) sowie die zugehörige Konfiguration.

Unterstützte Upgrade-Pfade

Sie können ein Upgrade auf StoreFront 2507 von folgenden Versionen durchführen:

- StoreFront 2503.1

- StoreFront 2503
- StoreFront 2407
- StoreFront 2402 LTSR (beliebiges CU)
- StoreFront 2203 LTSR (beliebiges CU)
- StoreFront 1912 LTSR CU10

Ein Upgrade von 2402 CU2 oder späteren CUs auf 2407 oder 2411 ist nicht möglich.

Gut zu wissen

- StoreFront unterstützt keine Bereitstellungen mit mehreren Servern, die unterschiedliche Produktversionen enthalten, daher müssen alle Server in einer Servergruppe auf dieselbe Version aktualisiert werden, bevor Sie den Zugriff auf die Bereitstellung gewähren.
- Gleichzeitige Upgrades werden für Bereitstellungen mit mehreren Servern nicht unterstützt, Server müssen sequenziell aktualisiert werden.
- Bevor das StoreFront-Upgrade ausgeführt wird, werden einige Vorabprüfungen durchgeführt. Wenn eine Vorabprüfung fehlschlägt, wird das Upgrade nicht gestartet, und Sie werden über die Fehler benachrichtigt. Ihre StoreFront-Installation bleibt unverändert. Nachdem Sie die Ursache der Fehler behoben haben, führen Sie das Upgrade erneut aus.
- Wenn das StoreFront-Upgrade selbst fehlschlägt, kann Ihre vorhandene StoreFront-Installation ihre ursprüngliche Konfiguration verlieren. Stellen Sie Ihre StoreFront-Installation in einen funktionsfähigen Zustand wieder her, und führen Sie das Upgrade dann erneut aus. Um StoreFront in einen funktionsfähigen Zustand wiederherzustellen, ziehen Sie die folgenden Ansätze in Betracht:
  - 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,
  - Ausführen der Ratschläge zur Fehlerbehebung unter Beheben von Upgrade-Problemen.
- Alle StoreFront-Upgradefehler, die durch den Citrix Virtual Apps and Desktops Metainstaller auftreten, werden in einem Dialogfeld mit einem Link zum entsprechenden Fehlerprotokoll gemeldet.

Vorbereitung auf das Upgrade

Bevor Sie mit dem Upgrade beginnen, empfehlen wir Ihnen, die folgenden Schritte auszuführen, um Upgradefehler zu vermeiden:

- Planen Sie Ihre Sicherungsstrategie vor dem Upgrade.
- Stellen Sie sicher, dass Sie von einer unterstützten Version aktualisieren.
- Laden Sie das StoreFront-Installationsprogramm von der Citrix-Website herunter.

Upgrade eines einzelnen StoreFront-Servers

1. Sichern Sie den Server, indem Sie einen VM-Snapshot erstellen.
2. Exportieren Sie die vorhandene StoreFront-Konfiguration. Wenn Sie mehrere Server in einer Servergruppe haben, exportieren Sie die Servergruppenkonfiguration nur von einem Server. Sofern Sie alle Änderungen zwischen ihnen weitergegeben haben, pflegen alle Server in einer Servergruppe identische Kopien der Konfiguration. Diese Sicherung ermöglicht es Ihnen, einfach eine neue Servergruppe zu erstellen, sodass Sie die Konfiguration im Falle von Problemen problemlos wiederherstellen können. Beachten Sie, dass Sie diese Sicherung nur auf einem Server wiederherstellen können, der dieselbe Version ausführt, von der sie exportiert wurde.
3. Wenn Sie Änderungen an Dateien in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` oder `C:\inetpub\wwwroot\Citrix\<StoreName>Auth\App_Data` vorgenommen haben, z. B. default.ica und usernamepassword.tfrm, sichern Sie diese für jeden Store. Nach dem Upgrade können Sie sie wiederherstellen, um Ihre Änderungen wiederherzustellen.
4. Verhindern Sie, dass Benutzer eine Verbindung herstellen, indem Sie den Server von einem Load Balancer entfernen oder Verbindungen anderweitig blockieren.
5. Starten Sie den Server neu.
6. Stellen Sie sicher, dass keine Anwendungen ausgeführt werden, einschließlich der StoreFront-Verwaltungskonsole, Befehlszeilen- und PowerShell-Fenster oder andere Anwendungen, die eine Sperre für StoreFront-Dateien haben könnten. Dadurch wird sichergestellt, dass alle StoreFront-Dateien während des Upgrades für das Installationsprogramm zugänglich sind. Wenn das Installationsprogramm nicht auf Dateien zugreifen kann, werden diese nicht ersetzt und das Upgrade schlägt fehl, was zur Entfernung der vorhandenen StoreFront-Konfiguration führt.
7. Stellen Sie sicher, dass Sie keine Windows Explorer- oder Eingabeaufforderungsfenster in Verzeichnissen geöffnet haben, die StoreFront-Dateien enthalten.
8. Deaktivieren Sie alle Antivirenprogramme.
9. Führen Sie die Installationsdatei für die erforderliche StoreFront-Version aus.

Upgrade einer StoreFront-Servergruppe während geplanter Wartungsarbeiten

Um eine StoreFront-Servergruppe mit mehreren Servern während geplanter Ausfallzeiten zu aktualisieren, führen Sie die folgenden Schritte aus:

1. Deaktivieren Sie den Benutzerzugriff auf die Servergruppe, indem Sie die Lastenausgleichs-URL deaktivieren. Dies verhindert, dass Benutzer während des Upgrade-Vorgangs eine Verbindung zur Bereitstellung herstellen.
2. Aktualisieren Sie jeden Server gemäß den Anweisungen unter Upgrade eines einzelnen StoreFront-Servers.
3. Überprüfen Sie, ob alle Server ordnungsgemäß funktionieren.
4. Aktivieren Sie den Benutzerzugriff auf die aktualisierte Servergruppe, indem Sie die Lastenausgleichs-URL aktivieren.

Upgrade einer StoreFront-Servergruppe ohne geplante Ausfallzeiten

Das gleichzeitige Aktualisieren der Server in einer aktiven StoreFront-Servergruppe wird nicht unterstützt. Sie können jedoch ein Live-Upgrade erreichen, indem Sie eine neue Servergruppe mit identischer Konfiguration erstellen, diese aktualisieren und dann Benutzerverbindungen zur neuen Servergruppe migrieren. Benutzer müssen sich bei StoreFront erneut authentifizieren, wenn sie zwischen Servergruppen übertragen werden.

Beispiel: Um eine StoreFront-Servergruppe mit drei Servern A, B und C zu aktualisieren:

1. Exportieren Sie die StoreFront-Konfiguration mit **Export-STFConfiguration**. Dieses Backup ist notwendig, da Server später im Prozess auf die Werkseinstellungen zurückgesetzt werden, wodurch Konfigurationsdaten gelöscht werden.
2. Exportieren Sie Abonnementdaten von Server A mit **Export-STFStoreSubscriptions**. Dieses Backup ist notwendig, da Server später im Prozess auf die Werkseinstellungen zurückgesetzt werden, wodurch Abonnementdaten gelöscht werden. Siehe Abonnementdaten für einen Store verwalten.
3. Deaktivieren Sie den Benutzerzugriff auf Server C, indem Sie ihn aus dem Lastenausgleich entfernen. Dies verhindert, dass Benutzer während des Upgrade-Vorgangs eine Verbindung zu Server C herstellen. Der Lastenausgleich sendet weiterhin Anfragen an die Server A und B.
4. Verwenden Sie Server A, um Server C aus der Gruppe zu entfernen. Die Server A und B stellen weiterhin den Zugriff auf die Ressourcen Ihrer Benutzer bereit. Server C ist nun von der Servergruppe getrennt und auf die Werkseinstellungen zurückgesetzt.

5. Setzen Sie den verwaisten Server C auf die Werkseinstellungen zurück mithilfe von **Clear-STFDeployment**.
6. Importieren Sie die StoreFront-Konfiguration, die Sie zuvor in Server C exportiert haben, mithilfe von **Import-STFConfiguration**. Server C verfügt nun über eine identische Konfiguration wie die alte Servergruppe. Es ist *nicht* notwendig, diesen Schritt später erneut zu wiederholen. Nur ein Server benötigt eine Kopie der Konfigurationsdaten, um sie an alle anderen Server weiterzugeben, die der Gruppe beitreten.
7. Führen Sie ein Upgrade von Server C durch, indem Sie die Anweisungen unter Upgrade eines einzelnen StoreFront-Servers befolgen. Server C verfügt nun über eine identische Konfiguration wie die alte Servergruppe und wurde auf eine neue Version von StoreFront aktualisiert.
8. Importieren Sie die Abonnementdaten, die Sie zuvor in Server C exportiert haben. Es ist *nicht* notwendig, diesen Schritt später erneut zu wiederholen. Nur ein Server benötigt eine Kopie der Abonnementdaten, um sie an alle anderen Server weiterzugeben, die der Gruppe beitreten.
9. Wiederholen Sie die Schritte 3, 4, 5 und 7 mit Server B (Schritt 6 nicht wiederholen). Während dieser Zeit stellt nur Server A den Benutzern Zugriff auf Ressourcen bereit. Es wird daher empfohlen, diesen Schritt während ruhiger Arbeitszeiten durchzuführen, in denen die Last auf der StoreFront-Servergruppe voraussichtlich minimal ist.
10. Fügen Sie Server B zu Server C hinzu, indem Sie den Prozess Bestehende Servergruppe beitreten verwenden. Dies ergibt eine Einzelserver-Bereitstellung auf der aktuellen Version von StoreFront (Server A) und eine neue Zwei-Knoten-Servergruppe auf der neuen StoreFront-Version (Server B und C).
11. Fügen Sie die Server B und C zum Lastenausgleichsdienst hinzu, damit sie die Aufgaben von Server A übernehmen können.
12. Entfernen Sie Server A aus dem Lastenausgleich, damit Benutzer zu den neu aktualisierten Servern B und C weitergeleitet werden.
13. Wiederholen Sie die Schritte 5, 7, 10 und 11 mit Server A (Schritt 6 nicht wiederholen). Der Upgrade-Vorgang der Servergruppe ist nun abgeschlossen. Die Server A, B und C verfügen über identische Konfigurations- und Abonnementdaten der ursprünglichen Gruppe.

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

> nach dem Upgrade eine leicht veraltete Kopie der Abonnementdatenbank hat und alle neuen Favoriten verloren gehen.

> Dies hat keine funktionellen Auswirkungen, da Favoritendaten für Benutzer nicht wesentlich sind, um sich anmelden und Ressourcen starten zu können. Benutzer müssten jedoch eine Ressource erneut als Favorit markieren, nachdem Server A auf die Werkseinstellungen zurückgesetzt und der neu aktualisierten Gruppe hinzugefügt wurde. Obwohl es unwahrscheinlich ist, dass mehr als ein paar Favoriteneinträge verloren gehen, ist dies eine mögliche Folge eines Upgrades einer aktiven StoreFront-Produktionsumgebung ohne Ausfallzeiten.

Beheben von Upgrade-Problemen

1. Öffnen Sie in *C:\Windows\Temp\StoreFront* die neueste *CitrixMsi*.log* und suchen Sie nach Ausnahmefehlern.

   Thumbs.db-Zugriffsausnahmen: verursacht durch *thumbs.db*-Dateien innerhalb von *C:\inetpub\wwwroot\citrix* oder in dessen Unterverzeichnissen. Löschen Sie alle gefundenen *thumbs.db*-Dateien.

   Exklusiver Dateizugriff nicht möglich \in Verwendung-Ausnahmen: Stellen Sie den Snapshot/das Backup wieder her, falls verfügbar, oder starten Sie den Server neu und beenden Sie alle StoreFront-Dienste manuell.

   Dienst kann nicht gestartet werden-Ausnahmen: Stellen Sie den Snapshot/das Backup wieder her, falls verfügbar, oder installieren Sie die Vollversion von .NET Framework 4.5 (nicht das Clientprofil).

2. Wenn keine Ausnahmefehler in *CitrixMsi*.log* vorhanden sind, überprüfen Sie die **Ereignisanzeige > Delivery Services** des Servers auf Fehler, die die vorhergehenden Ausnahmefehlermeldungen enthalten. Befolgen Sie den entsprechenden Rat.
3. Wenn in der Ereignisanzeige keine Ausnahmefehler vorhanden sind, überprüfen Sie die Admin-Protokolle unter *C:\Program Files\Citrix\Receiver StoreFront\logs* auf Fehler, die die vorhergehenden Ausnahmefehlermeldungen enthalten. Befolgen Sie den entsprechenden Rat.

Weitere Details zu Protokolldateien finden Sie unter Installationsprotokolle.

Exportieren und Importieren der StoreFront-Konfiguration

> Hinweis:

> Sie können nur StoreFront-Konfigurationen importieren, die dieselbe StoreFront-Version wie die Ziel-StoreFront-Installation haben.

> Sie können die gesamte Konfiguration einer StoreFront-Bereitstellung exportieren. Dies umfasst sowohl Einzelserver-Bereitstellungen als auch Servergruppenkonfigurationen. Wenn auf dem importierenden Server bereits eine vorhandene Bereitstellung vorhanden ist, wird die aktuelle Konfiguration gelöscht und dann durch die im Sicherungsarchiv enthaltene Konfiguration ersetzt. Wenn der Zielserver eine saubere Werksinstallation ist, wird eine neue Bereitstellung unter Verwendung der importierten Konfiguration erstellt, die in der Sicherung gespeichert ist. Die exportierte Konfigurationssicherung liegt in Form eines einzelnen .zip-Archivs vor, wenn sie unverschlüsselt ist, oder als .ctxzip, wenn Sie die Sicherungsdatei bei der Erstellung verschlüsseln möchten.

Szenarien, in denen Konfigurationsexport und -import verwendet werden können

- Sichern Sie StoreFront-Bereitstellungen nur in einem funktionierenden und vertrauenswürdigen Zustand. Jede Änderung an der Konfiguration erfordert eine neue Sicherung, um die alte zu ersetzen. Sie können vorhandene Sicherungen nicht ändern, da ein Dateihash der backup.zip-Datei eine Änderung verhindert.
- Sichern Sie VOR dem Upgrade von StoreFront zur Notfallwiederherstellung.
- Klonen bestehender Test-StoreFront-Bereitstellungen zur Überführung in die Produktion
- Erstellen von Benutzerakzeptanzumgebungen durch Klonen von Produktionsbereitstellungen in eine Testumgebung.
- Verschieben von StoreFront während OS-Migrationen, wie z. B. dem Upgrade des Hostings von Windows Server 2019 auf Windows 2022. In-Place-OS-Upgrades werden nicht unterstützt.
- Aufbau zusätzlicher Servergruppen in Multigeo-Bereitstellungen, z. B. in großen Unternehmen mit mehreren Rechenzentren.

Punkte, die beim Exportieren und Importieren einer StoreFront-Konfiguration zu beachten sind

- Verwenden Sie derzeit von Citrix® veröffentlichte Authentifizierungs-SDK-Beispiele, wie z. B. die Magic Word-Authentifizierung oder Anpassungen von Drittanbieter-Authentifizierungen? Wenn ja, müssen Sie diese Pakete auf ALLEN importierenden Servern installieren, BEVOR Sie

eine Konfiguration importieren, die zusätzliche Authentifizierungsmethoden enthält. Der Konfigurationsimport schlägt fehl, wenn die erforderlichen Authentifizierungs-SDK-Pakete auf keinem der importierenden Server installiert sind. Wenn Sie eine Konfiguration in eine Servergruppe importieren, installieren Sie die Authentifizierungspakete auf allen Mitgliedern der Gruppe.

- Sie können Ihre Konfigurationssicherungen verschlüsseln oder entschlüsseln. Die Export- und Import-PowerShell-Cmdlets unterstützen beide Anwendungsfälle.
- Sie können verschlüsselte Sicherungen (.ctxzip) später entschlüsseln, aber StoreFront kann unverschlüsselte Sicherungsdateien (.zip) nicht erneut verschlüsseln. Wenn eine verschlüsselte Sicherung erforderlich ist, führen Sie den Export erneut mit einem PowerShell-Anmeldeinformationsobjekt durch, das ein Passwort Ihrer Wahl enthält.
- Die SiteID der Website in IIS, auf der StoreFront derzeit installiert ist (exportierender Server), muss mit der SiteID der Zielwebsite in IIS (importierender Server) übereinstimmen, auf der Sie die gesicherte StoreFront-Konfiguration wiederherstellen möchten.

PowerShell-Cmdlets

Export-STFConfiguration

PARAMETER	BESCHREIBUNG
-TargetFolder (String)	Der Exportpfad zum Sicherungsarchiv. Beispiel: "\$env:userprofile\desktop\"
-Credential (PSCredential Object)	Geben Sie ein Anmeldeinformationsobjekt an, um während des Exports ein verschlüsseltes .ctxzip-Sicherungsarchiv zu erstellen. Das PowerShell-Anmeldeinformationsobjekt sollte das Kennwort für die Ver- und Entschlüsselung enthalten. Verwenden Sie **-Credential** nicht gleichzeitig mit dem Parameter **-NoEncryption**. Beispiel: \$CredObject
-NoEncryption (Switch)	Geben Sie an, dass das Sicherungsarchiv eine unverschlüsselte .zip-Datei sein soll. Verwenden Sie **-NoEncryption** nicht gleichzeitig mit dem Parameter **-Credential**.

PARAMETER	BESCHREIBUNG
-ZipFileName (String)	Der Name für das StoreFront-Konfigurationssicherungsarchiv. Fügen Sie keine Dateierweiterung wie .zip oder .ctxzip hinzu. Die Dateierweiterung wird automatisch hinzugefügt, je nachdem, ob der Parameter **-Credential** oder **-NoEncryption** während des Exports angegeben wird. Beispiel: "backup"
-Force (Boolean)	Dieser Parameter überschreibt automatisch Sicherungsarchive mit demselben Dateinamen wie vorhandene Sicherungsdateien, die bereits am angegebenen Exportort vorhanden sind.

Wichtig:

Der in StoreFront 3.5 gefundene Parameter **SiteID** wurde in Version 3.6 als veraltet markiert. Es ist nicht mehr erforderlich, die **SiteID** beim Import anzugeben, da die im Sicherungsarchiv enthaltene SiteID immer verwendet wird. Stellen Sie sicher, dass die SiteID mit der vorhandenen StoreFront-Website übereinstimmt, die bereits in IIS auf dem importierenden Server konfiguriert ist. Konfigurationsimporte von **SiteID 1** zu **SiteID 2** werden NICHT unterstützt.

Import-STFConfiguration

PARAMETER	BESCHREIBUNG
-ConfigurationZip (String)	Der vollständige Pfad zum Sicherungsarchiv, das Sie importieren möchten. Dies sollte auch die Dateierweiterung enthalten. Verwenden Sie .zip für unverschlüsselte und .ctxzip für verschlüsselte Sicherungsarchive. Beispiel: `$env:userprofile\desktop\backup.ctxzip`
-Credential (PSCredential Object)	Geben Sie ein Anmeldeinformationsobjekt an, um eine verschlüsselte Sicherung während

PARAMETER	BESCHREIBUNG
	des Imports zu entschlüsseln. Beispiel: `$CredObject`
-HostBaseURL (String)	Wenn dieser Parameter enthalten ist, wird die von Ihnen angegebene Host-Basis-URL anstelle der Host-Basis-URL vom exportierenden Server verwendet. Beispiel: `https://<importingserver>.example.com`

Unprotect-STFConfigurationBackup

PARAMETER	BESCHREIBUNG
-TargetFolder (String)	Der Exportpfad zum Sicherungsarchiv. Beispiel: `$env:userprofile\desktop`
-Credential (PSCredential Object)	Verwenden Sie diesen Parameter, um eine unverschlüsselte Kopie des verschlüsselten Sicherungsarchivs zu erstellen. Geben Sie das PowerShell-Anmeldeinformationsobjekt an, das das zur Entschlüsselung zu verwendende Kennwort enthält. Beispiel: `$CredObject`
-EncryptedConfigurationZip (String)	Der vollständige Pfad des verschlüsselten Sicherungsarchivs, das Sie entschlüsseln möchten. Sie müssen die Dateierweiterung .ctxzip angeben. Beispiel: `$env:userprofile\\desktop\ \backup.ctxzip`
-OutputFolder (String)	Der Pfad zum Erstellen einer unverschlüsselten Kopie (.zip) des verschlüsselten (.ctxzip) Sicherungsarchivs. Die ursprüngliche verschlüsselte Sicherungskopie wird beibehalten, damit sie wiederverwendet werden kann. Geben Sie keinen Dateinamen und keine Dateierweiterung für die unverschlüsselte Kopie an. Beispiel: `$env:userprofile\desktop`

PARAMETER	BESCHREIBUNG
-Force (Boolean)	Dieser Parameter überschreibt Sicherungsarchive automatisch, die denselben Dateinamen wie vorhandene Sicherungsdateien haben, die bereits am angegebenen Exportspeicherort vorhanden sind.

Beispiele für den Export und Import von Konfigurationen

Importieren der StoreFront-Cmdlets in die aktuelle PowerShell-Sitzung

Öffnen Sie die PowerShell Integrated Scripting Environment (ISE) auf dem StoreFront-Server und führen Sie Folgendes aus:

```
$env:PSModulePath =
[Environment]::GetEnvironmentVariable('PSModulePath','Machine')

$SDKModules = 'C:\Program Files\Citrix\Receiver
StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'

Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose

Import-Module
"$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1"
-verbose

Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1"
-verbose

Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose

Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1"
-verbose
```

Szenarien mit einem einzelnen Server

Erstellen Sie eine unverschlüsselte Sicherung einer vorhandenen Konfiguration auf Server A und stellen Sie sie auf derselben Bereitstellung wieder her

Exportieren Sie die Konfiguration des Servers, den Sie sichern möchten.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\"
-zipFileName "backup" -NoEncryption
```

Kopieren Sie die Datei backup.zip an einen sicheren Ort. Sie können diese Sicherung für die Notfallwiederherstellung verwenden, um den Server in seinen vorherigen Zustand zurückzuversetzen.

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.zip" -HostBaseURL "https://
storefront.example.com"
```

Sichern Sie eine vorhandene Konfiguration auf Server A und stellen Sie sie auf Server B wieder her, um einen Klon eines vorhandenen Servers zu erstellen

Exportieren Sie die Konfiguration des Servers, den Sie sichern möchten.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\"
-zipFileName "backup" -NoEncryption
```

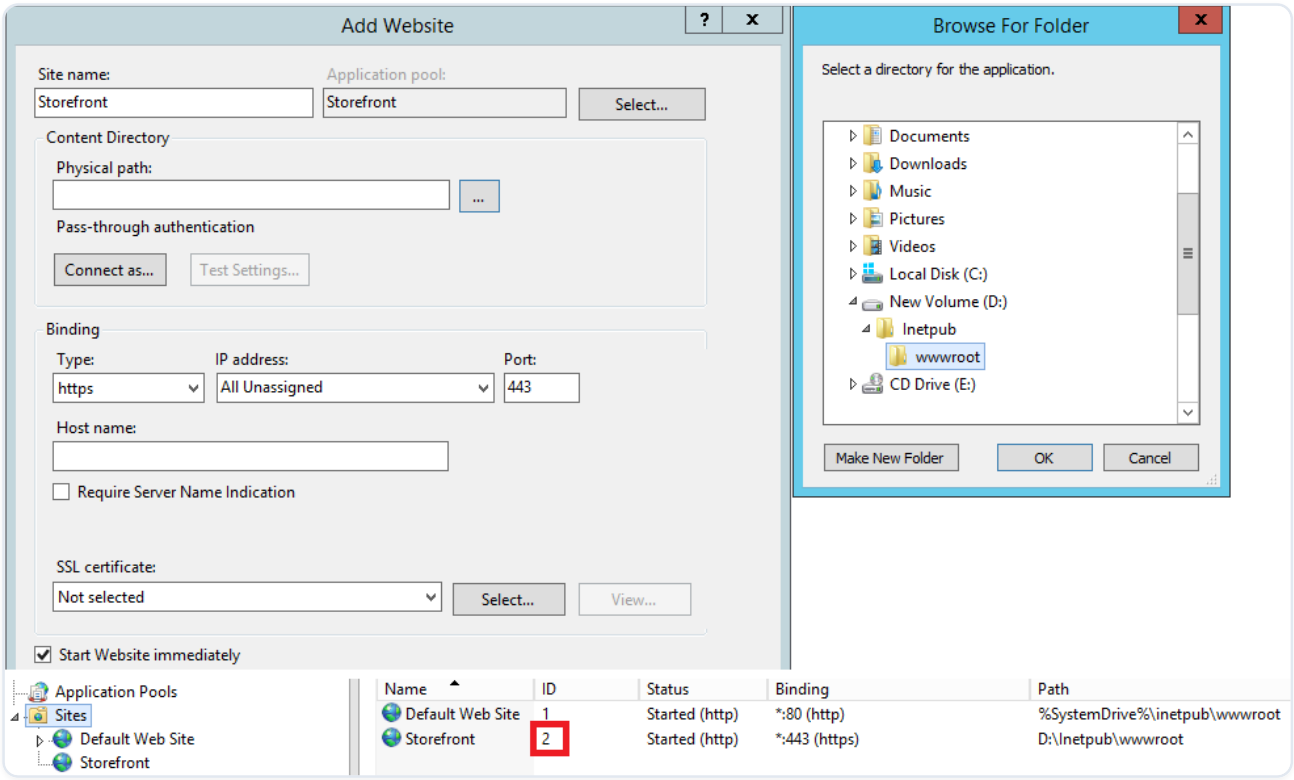
Kopieren Sie die Datei backup.zip auf den Desktop von Server B.

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.zip" -HostBaseURL "https://
serverB.example.com"
```

StoreFront ist bereits auf einer benutzerdefinierten Website in IIS bereitgestellt. Stellen Sie die Konfiguration auf einer anderen benutzerdefinierten Website-Bereitstellung wieder her

Server A hat StoreFront an einem benutzerdefinierten Website-Speicherort bereitgestellt, anstatt auf der üblichen Standardwebsite innerhalb von IIS. Die IIS-SiteID für die zweite in IIS erstellte Website ist 2. Der physische Pfad der StoreFront-Website kann sich auf einem anderen Nicht-Systemlaufwerk wie d:\ oder auf dem Standard-Systemlaufwerk c:\ befinden, sollte aber eine IIS-SiteID größer als 1 verwenden.

Eine neue Website namens StoreFront wurde in IIS konfiguriert, die **SiteID = 2** verwendet. StoreFront ist bereits auf der benutzerdefinierten Website in IIS mit ihrem physischen Pfad auf Laufwerk `d:\inetpub\wwwroot` bereitgestellt.



1. Exportieren Sie eine Kopie der Server A-Konfiguration.
2. Auf Server B konfigurieren Sie IIS mit einer neuen Website namens **StoreFront**, die ebenfalls **SiteID 2** verwendet.
3. Importieren Sie die Server-A-Konfiguration auf Server B. Die im Backup enthaltene Site-ID wird verwendet und muss mit der Ziel-Website übereinstimmen, auf die Sie die StoreFront-Konfiguration importieren möchten.

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -HostBaseURL "https://
serverB.example.com"
```

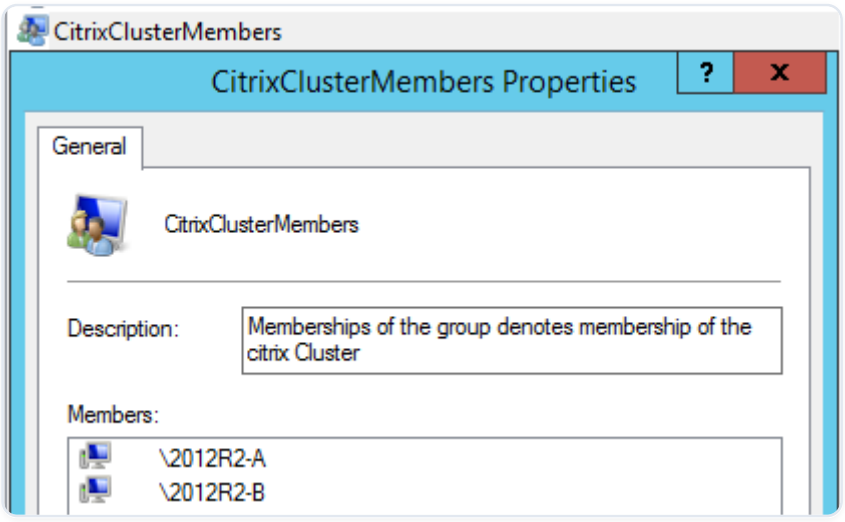
Servergruppen-Szenarien

Szenario 1: Sichern einer vorhandenen Servergruppenkonfiguration und spätere Wiederherstellung auf derselben Servergruppenbereitstellung

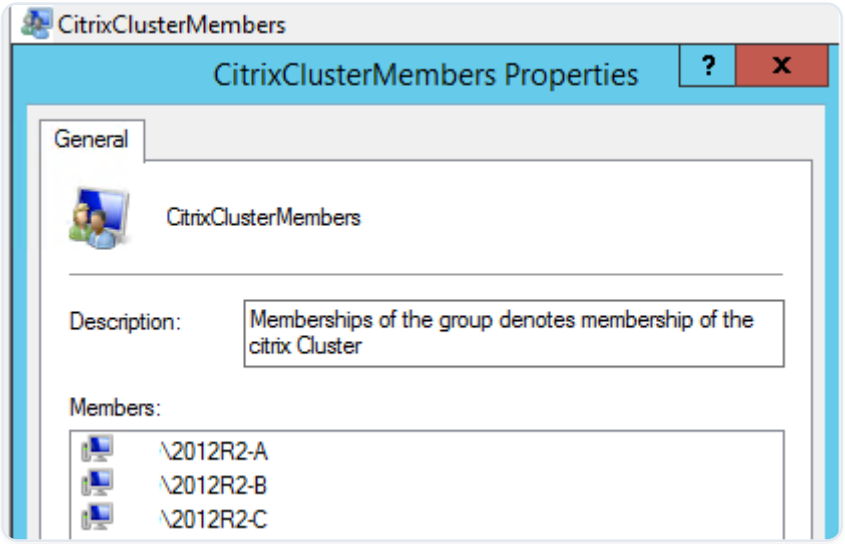
Ein früheres Konfigurations-Backup wurde erstellt, als nur zwei StoreFront-Server, 2012R2-A und 2012R2-B, Mitglieder der Servergruppe waren. Im Backup-Archiv befindet sich ein Eintrag der **CitrixClusterMembership** zum Zeitpunkt der Sicherung, der nur die beiden ursprünglichen Server 2012R2-A und 2012R2-B enthält. Die StoreFront-Servergruppenbereitstellung hat sich seit der ursprünglichen Sicherung aufgrund der geschäftlichen Anforderungen vergrößert, sodass ein zusätzlicher Knoten 2012R2-C zur Servergruppe hinzugefügt wurde. Die zugrunde liegende StoreFront-Konfiguration der im Backup enthaltenen Servergruppe hat sich nicht geändert. Die

aktuelle CitrixClusterMembership von drei Servern muss beibehalten werden, auch wenn ein altes Backup importiert wird, das nur die beiden ursprünglichen Servergruppenknoten enthält. Während des Imports wird die aktuelle Cluster-Mitgliedschaft beibehalten und dann zurückgeschrieben, sobald die Konfiguration erfolgreich auf den primären Server importiert wurde. Der Import bewahrt auch die aktuelle CitrixClusterMembership, wenn Servergruppenknoten seit der ursprünglichen Sicherung aus der Servergruppe entfernt wurden.

1. Exportieren Sie die Konfiguration der Servergruppe 1 von 2012R2-A, dem primären Server, der zur Verwaltung der gesamten Servergruppe verwendet wird.



2. Später fügen Sie der vorhandenen Servergruppe einen zusätzlichen Server, 2012R2-C, hinzu.



3. Die Konfiguration der Servergruppe muss auf einen bekannten, zuvor funktionierenden Zustand wiederhergestellt werden. StoreFront sichert die aktuelle CitrixClusterMembership von drei Servern während des Importvorgangs und stellt sie dann wieder her, nachdem der Import erfolgreich war.
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"
```

5. Verbreiten Sie die neu importierte Konfiguration auf die gesamte Servergruppe, sodass alle Server nach dem Import eine konsistente Konfiguration aufweisen.

Szenario 2: Sichern einer vorhandenen Konfiguration von Servergruppe 1 und Erstellen einer neuen Servergruppe auf einer anderen werkseitigen Standardinstallation. Danach können Sie dem neuen primären Server weitere neue Servergruppenmitglieder hinzufügen

Servergruppe 2 wird mit zwei neuen Servern, 2012R2-C und 2012R2-D, erstellt. Die Konfiguration der Servergruppe 2 basiert auf der Konfiguration einer bestehenden Bereitstellung, Servergruppe 1, die ebenfalls zwei Server, 2012R2-A und 2012R2-B, enthält. Die im Backup-Archiv enthaltene CitrixClusterMembership wird beim Erstellen einer neuen Servergruppe nicht verwendet. Die aktuelle CitrixClusterMembership wird immer gesichert und nach erfolgreichem Import wiederhergestellt. Beim Erstellen einer neuen Bereitstellung mithilfe einer importierten Konfiguration enthält die Sicherheitsgruppe CitrixClusterMembership nur den importierenden Server, bis weitere Server der neuen Gruppe beitreten. Servergruppe 2 ist eine neue Bereitstellung und soll parallel zu Servergruppe 1 existieren. Geben Sie den Parameter -HostBaseURL an. Servergruppe 2 wird mithilfe einer neuen werkseitigen Standardinstallation von StoreFront erstellt.

1. Exportieren Sie die Konfiguration der Servergruppe 1 von 2012R2-A, dem primären Server, der zur Verwaltung der gesamten Servergruppe verwendet wird.
2. Importieren Sie die Konfiguration der Servergruppe 1 auf den Knoten 2012R2-C, der der primäre Server zur Verwaltung der neu erstellten Servergruppe 2 sein wird.

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -HostBaseURL "https://
servergroup2.example.com"
```

3. Fügen Sie alle weiteren Server hinzu, die Teil der neuen Bereitstellung der Servergruppe 2 sein werden. Die Weitergabe der neu importierten Konfiguration von Servergruppe 1 an alle neuen Mitglieder der Servergruppe 2 erfolgt automatisch, da dies Teil des normalen Beitrittsprozesses ist, wenn ein neuer Server hinzugefügt wird.

Szenario 3: Sichern einer vorhandenen Konfiguration von Servergruppe A und Verwenden dieser zum Überschreiben der vorhandenen Konfiguration von Servergruppe B

Servergruppe 1 und Servergruppe 2 existieren bereits in zwei separaten Rechenzentren. Viele StoreFront-Konfigurationsänderungen werden an Servergruppe 1 vorgenommen, die Sie auf Servergruppe 2 im anderen Rechenzentrum anwenden sollten. Sie können die Änderungen von Servergruppe 1 auf Servergruppe 2 übertragen. Verwenden Sie nicht die **CitrixClusterMembership** innerhalb des Sicherungsarchivs auf Servergruppe 2. Geben Sie den Parameter **-HostBaseURL** während des Imports an, da die Host-Basis-URL von Servergruppe 2 nicht auf denselben FQDN geändert werden sollte, der derzeit von Servergruppe 1 verwendet wird. Servergruppe 2 ist eine bestehende Bereitstellung.

1. Exportieren Sie die Konfiguration der Servergruppe 1 von 2012R2-A, dem primären Server, der zur Verwaltung der gesamten Servergruppe verwendet wird.
2. Importieren Sie die Konfiguration der Servergruppe 1 auf die werkseitige Standardinstallation auf Knoten 2012R2-C, der der primäre Server der neuen Servergruppe 2 sein wird.

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.zip" -NoEncryption -HostBaseURL
"https://servergroup2.example.com"
```

Erstellen Sie eine verschlüsselte Sicherung Ihrer Serverkonfiguration

Ein PowerShell-Anmeldeinformationsobjekt umfasst sowohl einen Windows-Kontobenutzernamen als auch ein Kennwort. PowerShell-Anmeldeinformationsobjekte stellen sicher, dass Ihr Kennwort im Speicher geschützt bleibt.

Hinweis:

Um ein Konfigurationssicherungsarchiv zu verschlüsseln, benötigen Sie nur das Kennwort, um die Verschlüsselung und Entschlüsselung durchzuführen. Der im Anmeldeinformationsobjekt gespeicherte Benutzername wird nicht verwendet. Sie müssen ein Anmeldeinformationsobjekt mit demselben Kennwort in der PowerShell-Sitzung erstellen, die sowohl auf den exportierenden als auch auf den importierenden Servern verwendet wird. Innerhalb des Anmeldeinformationsobjekts können Sie einen beliebigen Benutzer angeben.

> PowerShell erfordert, dass Sie einen Benutzer angeben, wenn Sie ein neues Anmeldeinformationsobjekt erstellen. Dieses Beispielcode ruft der Einfachheit halber den aktuell angemeldeten Windows-Benutzer ab.

Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt in Ihrer 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)
```

Exportieren Sie die Konfiguration nach backup.ctxzip, einer verschlüsselten ZIP-Datei.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\"
-zipFileName "backup" -Credential $CredObject
```

Erstellen Sie ein identisches PowerShell-Anmeldeinformationsobjekt in Ihrer PowerShell-Sitzung auf dem importierenden Server.

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
-HostBaseURL "https://storefront.example.com"
```

Schutz eines vorhandenen verschlüsselten Sicherungsarchivs aufheben

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name

$Password = "Pa55w0rd"

$Password = $Password | ConvertTo-SecureString -asPlainText -Force

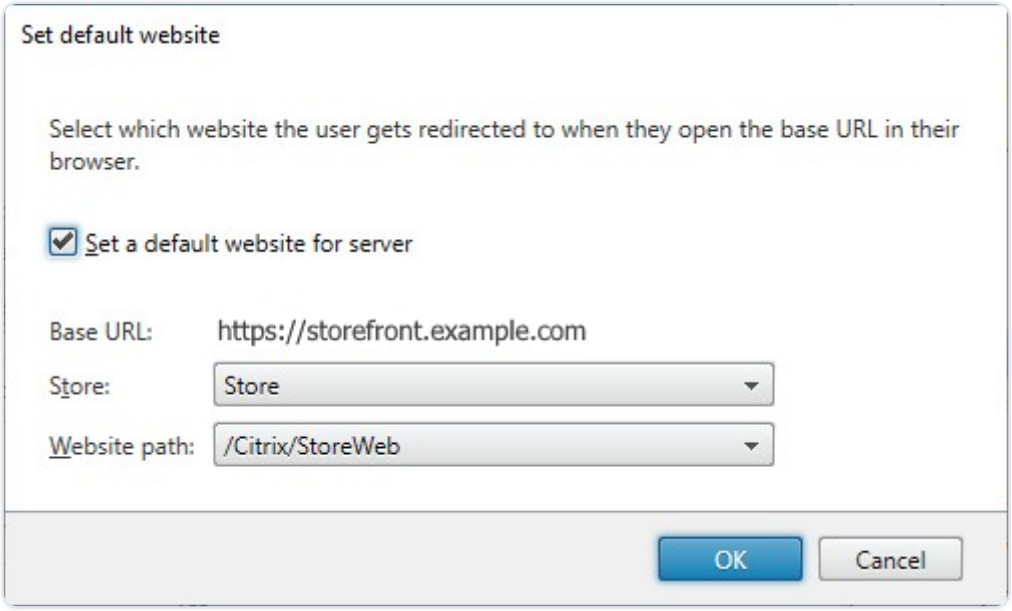
$CredObject = New-Object System.Management.Automation.PSCredential($User,
$Password)
```

```
Unprotect-STFConfigurationExport -encryptedConfigurationZip
"$env:userprofile\desktop\backup.ctxzip" -credential $CredObject
-outputFolder "c:\StoreFrontBackups" -Force
```

Standardwebsite für die Bereitstellung

Wenn Benutzer die Basis-URL in ihrem Webbrowser öffnen, können Sie StoreFront so konfigurieren, dass der Benutzer zu einer bestimmten Website umgeleitet wird.

1. Öffnen Sie die StoreFront-Verwaltungskonsole.
2. Wählen Sie im Bereich **Aktionen** die Option **Standardwebsite für Bereitstellung festlegen**.
3. Wenn Sie eine Standardwebsite festlegen möchten, dann
    a. Wählen Sie **Eine Standardwebsite für den Server festlegen**
    b. Wählen Sie einen **Store**
    c. Wählen Sie einen **Websitepfad**.
4. Wählen Sie **OK**, um die Änderungen zu speichern.



Server auf Werkseinstellungen zurücksetzen

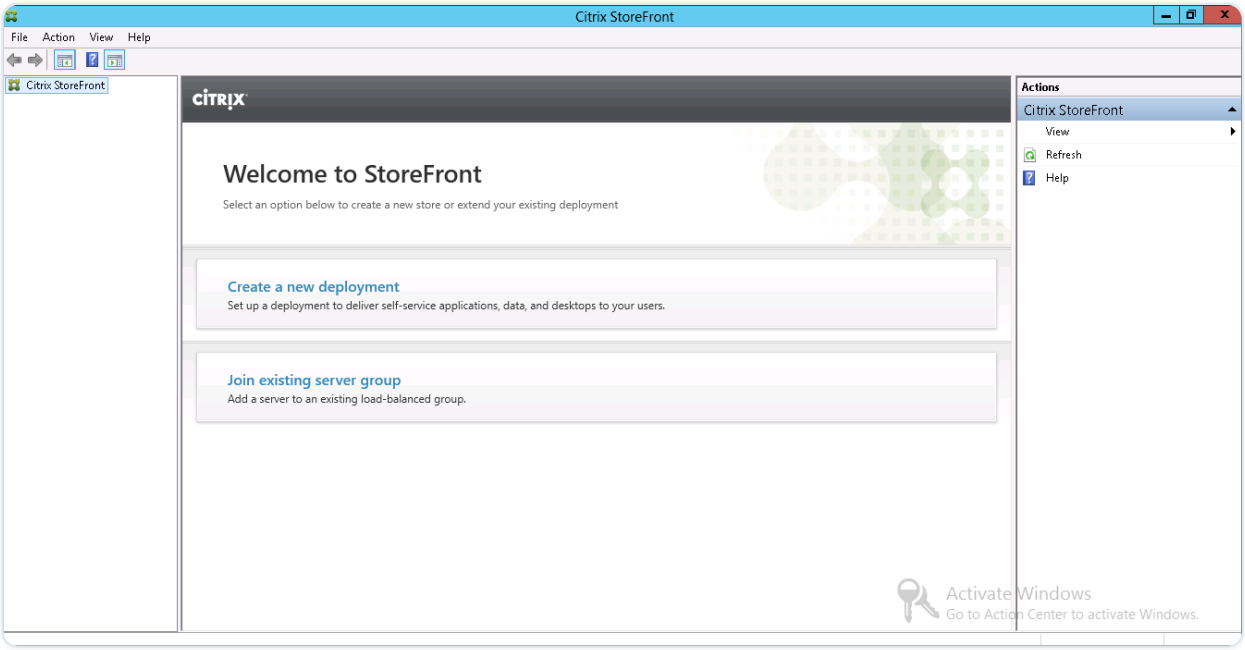
In einigen Situationen ist es erforderlich, eine StoreFront-Installation auf ihren ursprünglichen Installationszustand zurückzusetzen. Dies ist beispielsweise notwendig, bevor Sie einen StoreFront-Server wieder zu einer Servergruppe hinzufügen können. Eine manuelle Deinstallation und Neuinstallation kann durchgeführt werden, ist aber zeitaufwändiger und kann zu anderen

unvorhergesehenen Problemen führen. Stattdessen können Sie PowerShell-Module verwenden, um die Konfiguration auf die Standardwerte zurückzusetzen.

1. Stellen Sie sicher, dass die StoreFront-Verwaltungskonsole geschlossen ist.
2. Öffnen Sie eine PowerShell-Konsole.
3. Führen Sie das Cmdlet Clear-STFDeployment aus.

```
Clear-STFDeployment -Confirm $False
```

4. Wenn der Befehl erfolgreich abgeschlossen wurde, öffnen Sie die StoreFront-Verwaltungskonsole und bestätigen Sie, dass alle Einstellungen zurückgesetzt wurden. Die Optionen **Neue Bereitstellung erstellen** oder **Vorhandener Servergruppe beitreten** sind verfügbar.



StoreFront deinstallieren

Zusätzlich zum Produkt selbst entfernt die Deinstallation von StoreFront den Authentifizierungsdienst, Stores, Websites, XenApp Services-URLs und die zugehörigen Konfigurationen. Der Abonnement-Store-Dienst, der die Anwendungsabonnementdaten der Benutzer enthält, wird ebenfalls gelöscht. Bei Einzelserverbereitstellungen gehen daher die Details der Anwendungsabonnements der Benutzer verloren. Bei Bereitstellungen mit mehreren Servern bleiben diese Daten jedoch auf anderen Servern in der Gruppe erhalten. Vom StoreFront-Installationsprogramm aktivierte Voraussetzungen, wie die .NET Framework-Funktionen und die

Webserver (IIS)-Rollendienste, werden bei der Deinstallation von StoreFront nicht vom Server entfernt.

1. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen am StoreFront-Server an.
2. Schließen Sie die StoreFront-Verwaltungskonsole, falls sie geöffnet ist.
3. Schließen Sie alle PowerShell-Sitzungen, die möglicherweise zur Verwaltung von StoreFront verwendet wurden.
4. Öffnen Sie das **Startmenü**, klicken Sie auf **Einstellungen** (Zahnradsymbol) und gehen Sie dann zu **Apps**.
5. Wählen Sie im Fenster **Programme und Funktionen** die Option **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**.

StoreFront manuell entfernen

Um sicherzustellen, dass StoreFront nach der Deinstallation vollständig entfernt wurde:

1. Entfernen Sie die Rolle **Webserver (IIS)**. Weitere Informationen finden Sie unter Microsoft Learn.
2. Löschen Sie den Ordner `C:\Program Files\Citrix\Receiver StoreFront`.
3. Löschen Sie alle Unterverzeichnisse unter `C:\Program Files\Citrix\StoreFront Install`.
4. Löschen Sie den Ordner `C:\Inetpub`.

Sie können StoreFront jetzt neu installieren.

Installationsprotokolle

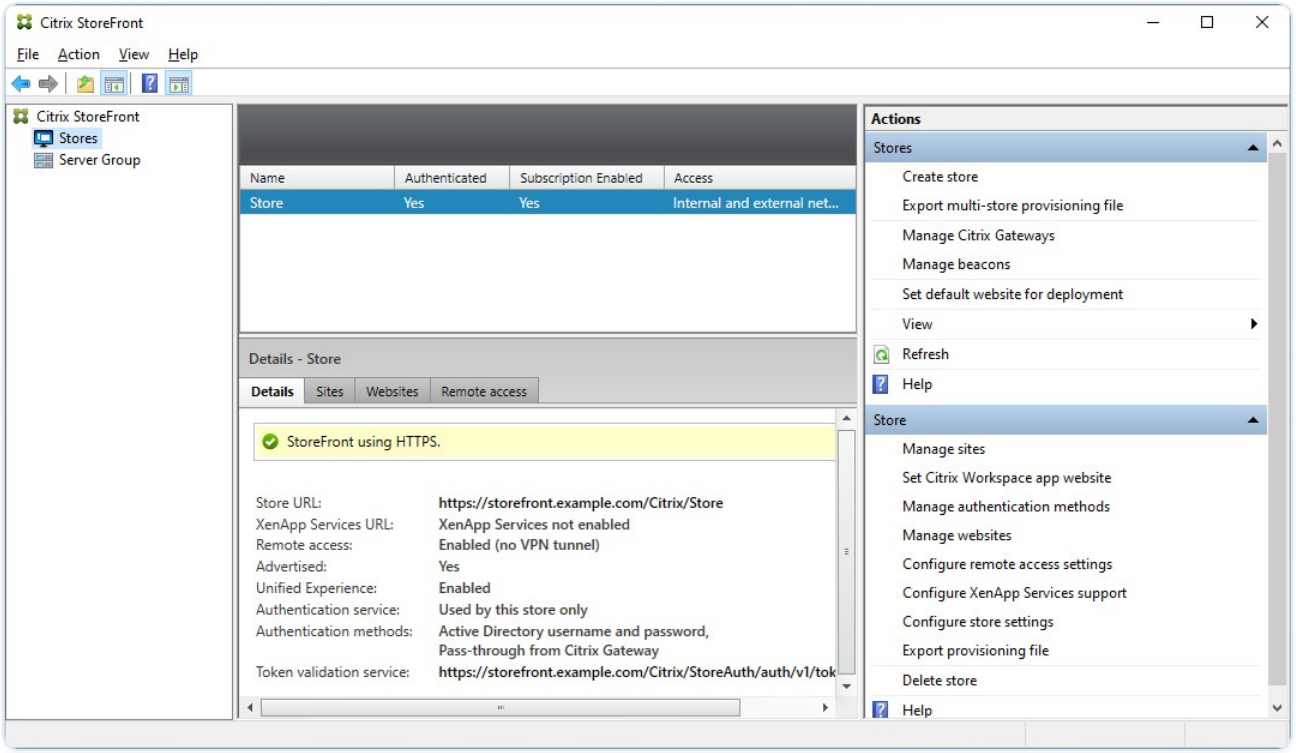
Weitere Informationen zu Protokolldateien finden Sie unter Installationsprotokolle.

Stores verwalten

In Citrix StoreFront erstellen Sie einen oder mehrere Stores, damit Endbenutzer auf ihre Ressourcen zugreifen können. Jeder Store definiert, wie sich der Benutzer authentifiziert, welche Ressourcen aggregiert werden und wie die Darstellung erfolgt. Endbenutzer können diese Stores über einen Webbrowser öffnen oder sie ihrer lokal installierten Citrix Workspace-App hinzufügen.

Stores anzeigen

1. Wählen Sie in der Verwaltungskonsole den Knoten **Stores** im linken Bereich aus.
2. Wählen Sie den Store aus, den Sie anzeigen möchten.



Im Bereich **Details** können Sie die folgenden Registerkarten anzeigen:

REGISTERKARTE	DETAILS
Details	Zeigt Store-Details wie URL und Authentifizierungsmethoden an
Sites	Listet alle für den Store konfigurierten Sites auf

REGISTERKARTE	DETAILS
Websites	Listet alle für den Store konfigurierten Websites auf.
Remotezugriff	Details dazu, ob der Remotezugriff über ein Citrix Gateway aktiviert ist

Store erstellen

Wählen Sie im Bereich **Aktionen** im Abschnitt **Stores** die Option **Store erstellen**. Weitere Informationen finden Sie unter Store erstellen.

Store konfigurieren

Im Bereich Aktionen im Abschnitt **Store** können Sie die folgenden Store-Konfigurationsaktionen ausführen:

AKTION	DETAILS
Sites verwalten	Sites hinzufügen und entfernen.
Citrix Workspace-App-Website festlegen	Konfigurieren Sie, welche Website verwendet wird, wenn Sie über die Citrix Workspace-App auf den Store zugreifen
Authentifizierungsmethoden verwalten	Wählen Sie aus, welche Methoden Benutzer verwenden können, um sich am Store zu authentifizieren
Websites verwalten	Verwalten Sie die Website, die für den Zugriff auf den Store verwendet wird
Einstellungen für den Remotezugriff konfigurieren	Konfigurieren Sie den Zugriff auf Stores über Citrix Gateway für Benutzer, die sich von öffentlichen Netzwerken aus verbinden.
XenApp® Services-Unterstützung konfigurieren	XenApp Services-URL aktivieren oder deaktivieren
Speichereinstellungen konfigurieren	Öffnet die Fenster zur Konfiguration der Speichereinstellungen, in denen Sie Favoriten,

AKTION	DETAILS
	Kerberos-Delegierung, Optimales HDX-Routing, Store bewerben und Erweiterte Einstellungen konfigurieren können.

Sie können die folgenden erweiterten Store-Konfigurationen außerhalb der Verwaltungskonsole durchführen:

AUFGABE	DETAILS
Standard-ICA-Einstellungen	Konfigurieren Sie HDX-Einstellungen, indem Sie sie zu default.ica hinzufügen.
Citrix Workspace-App-Konfiguration	Verwenden Sie StoreFront, um die Citrix Workspace-App zu konfigurieren.
Verbundauthentifizierungsdienst konfigurieren	Konfigurieren Sie den Verbundauthentifizierungsdienst (FAS) für Single Sign-On bei VDAs.

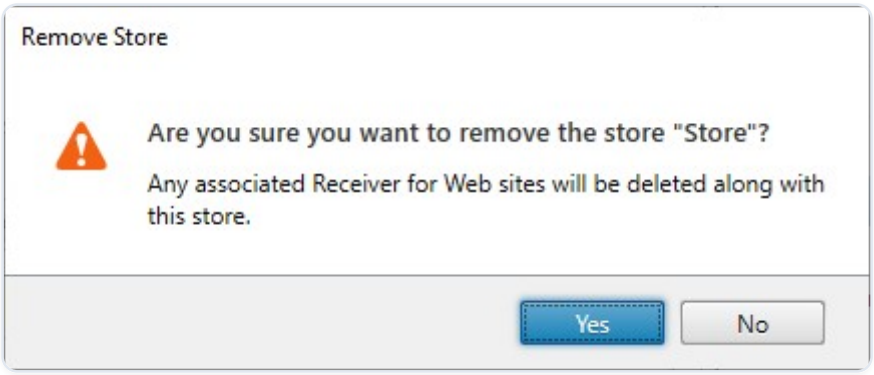
Bereitstellungsdateien exportieren

Sie können Dateien generieren, die Verbindungsdetails für einen oder mehrere Stores enthalten, einschließlich aller Citrix Gateway-Bereitstellungen und Beacons, die für den Store konfiguriert sind. Weitere Informationen finden Sie unter Bereitstellungsdateien exportieren.

Einen Store löschen

So löschen Sie einen Store:

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



Wenn Sie einen Store löschen, werden auch alle zugehörigen Websites gelöscht.

Store erstellen

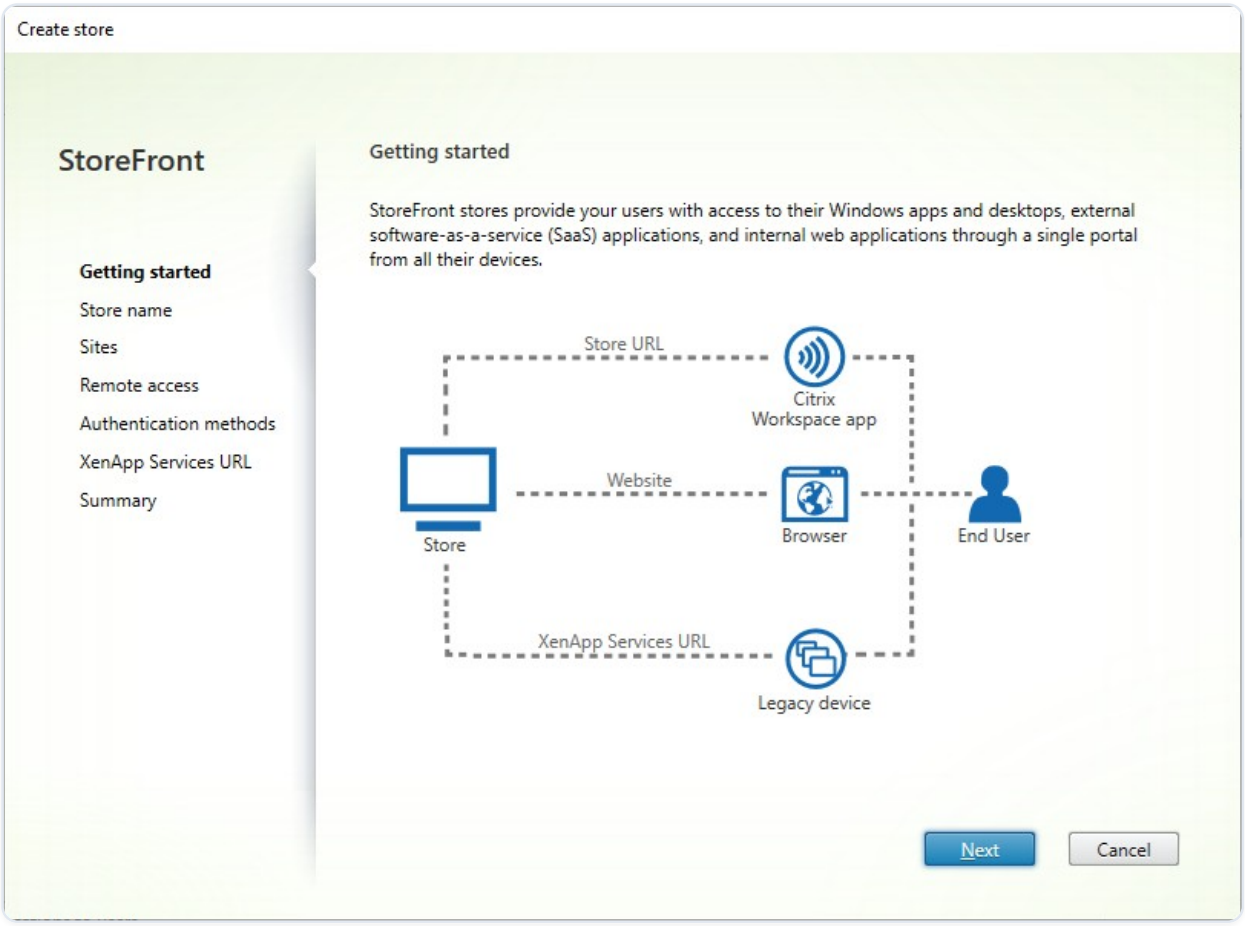
Sie können so viele Stores erstellen, wie Sie benötigen; zum Beispiel können Sie einen Store für eine bestimmte Benutzergruppe oder zur Gruppierung einer spezifischen Reihe von Ressourcen erstellen.

> Wichtig:

> Verwenden Sie in Bereitstellungen mit mehreren Servern immer nur einen Server gleichzeitig, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Sobald dies abgeschlossen ist, übertragen Sie Ihre Konfigurationsänderungen an die Servergruppe, damit die anderen Server in der Bereitstellung aktualisiert werden.

> Um einen Store zu erstellen, identifizieren und konfigurieren Sie die Kommunikation mit den Servern, die die Ressourcen bereitstellen, die Sie im Store verfügbar machen möchten. Anschließend konfigurieren Sie optional den Fernzugriff auf den Store über Citrix Gateway.

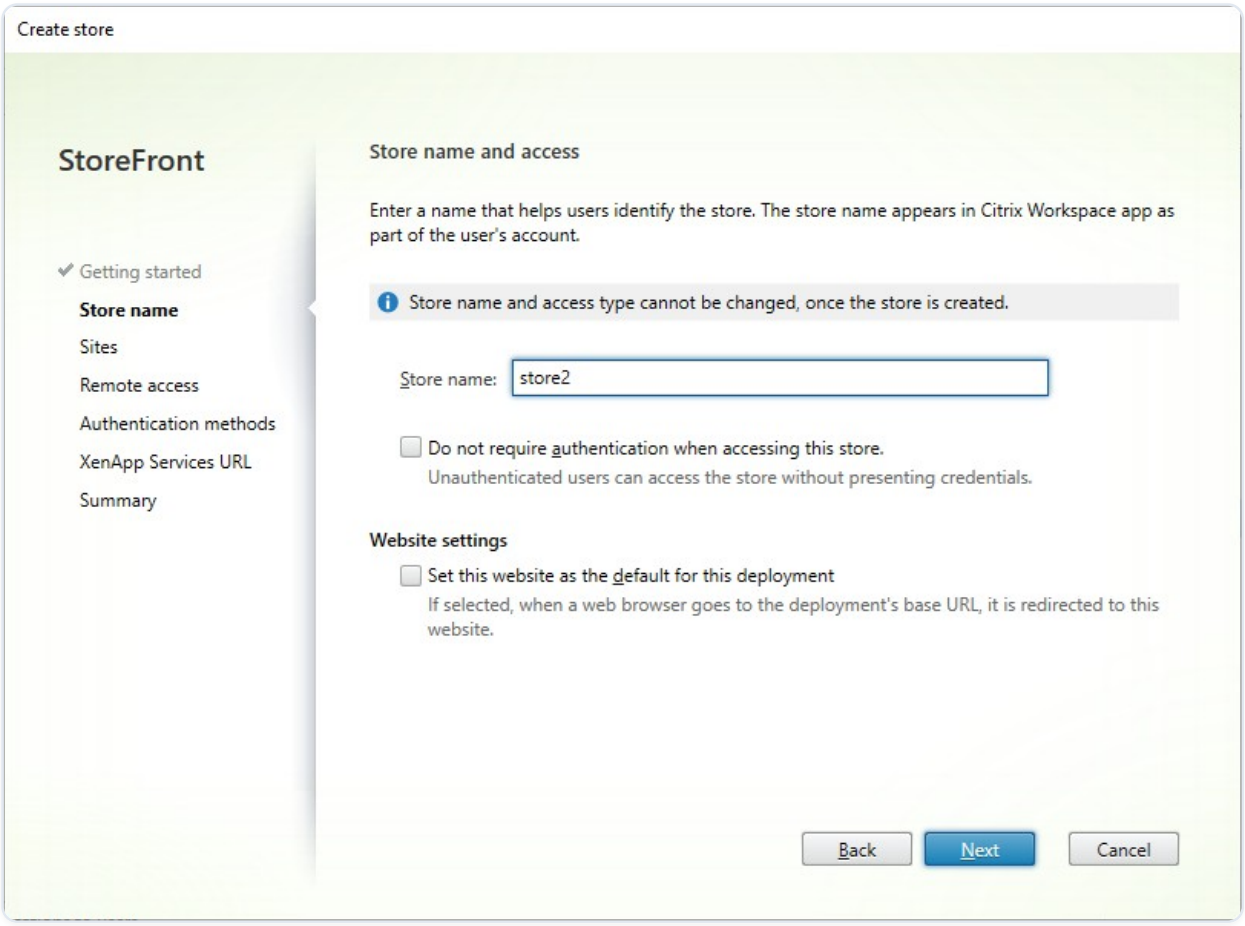
1. Klicken Sie im Aktionsbereich auf **Store erstellen**.



Klicken Sie auf **Weiter**.

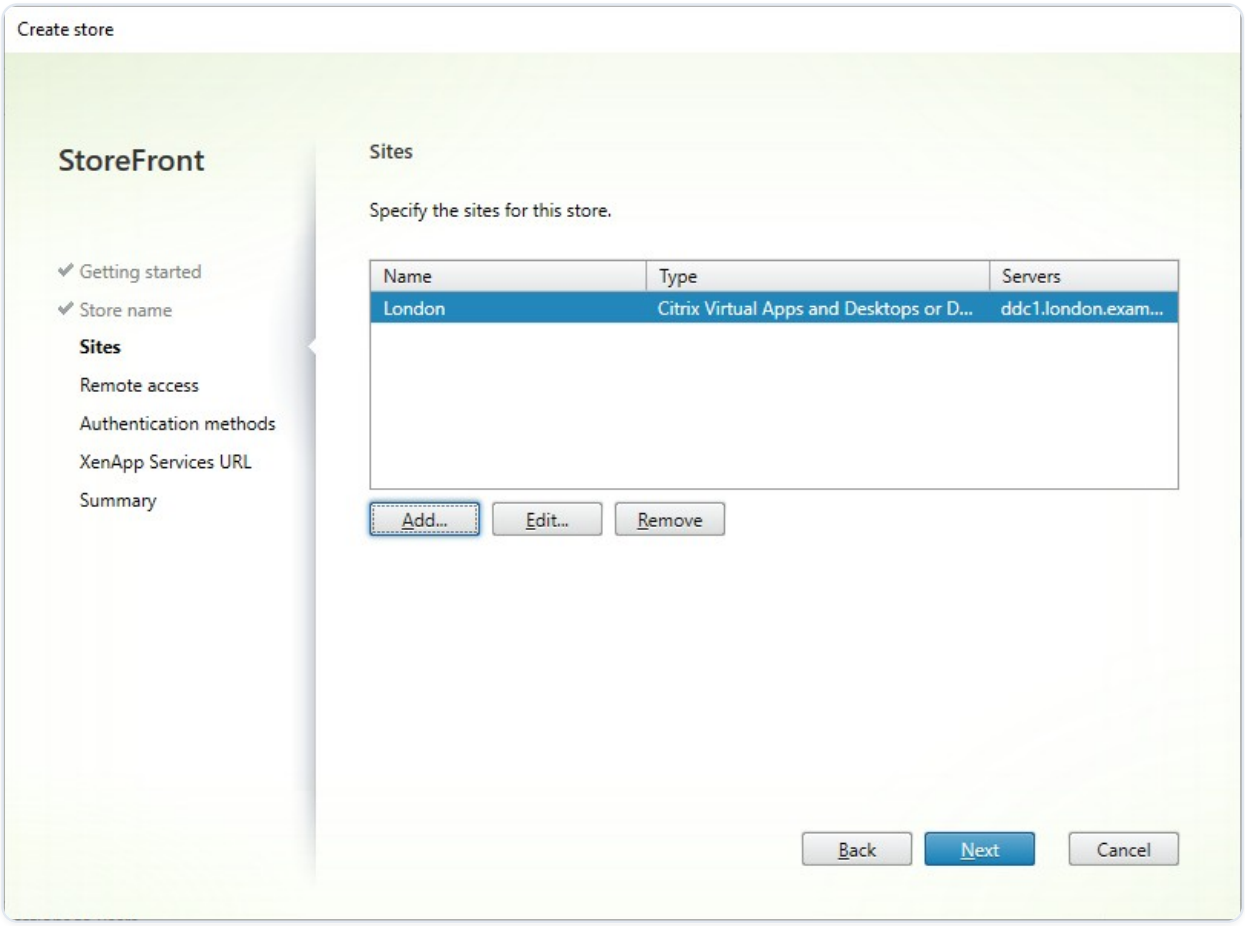
2. Füllen Sie auf der Registerkarte **Store-Name** Folgendes aus:

   - Geben Sie einen Store-Namen ein.
   - Wenn Sie Benutzern den anonymen oder nicht authentifizierten Zugriff auf den Store erlauben möchten, aktivieren Sie **Nur nicht authentifizierten Benutzern den Zugriff auf diesen Store erlauben**. Wenn Sie einen nicht authentifizierten Store erstellen, sind die Seiten **Authentifizierungsmethoden** und **Fernzugriff** nicht verfügbar, und **Servergruppenknoten** im linken und Aktionsbereich werden durch **Basis-URL ändern** ersetzt. (Dies ist die einzige verfügbare Option, da Servergruppen auf Servern, die nicht in eine Domäne eingebunden sind, nicht verfügbar sind.)



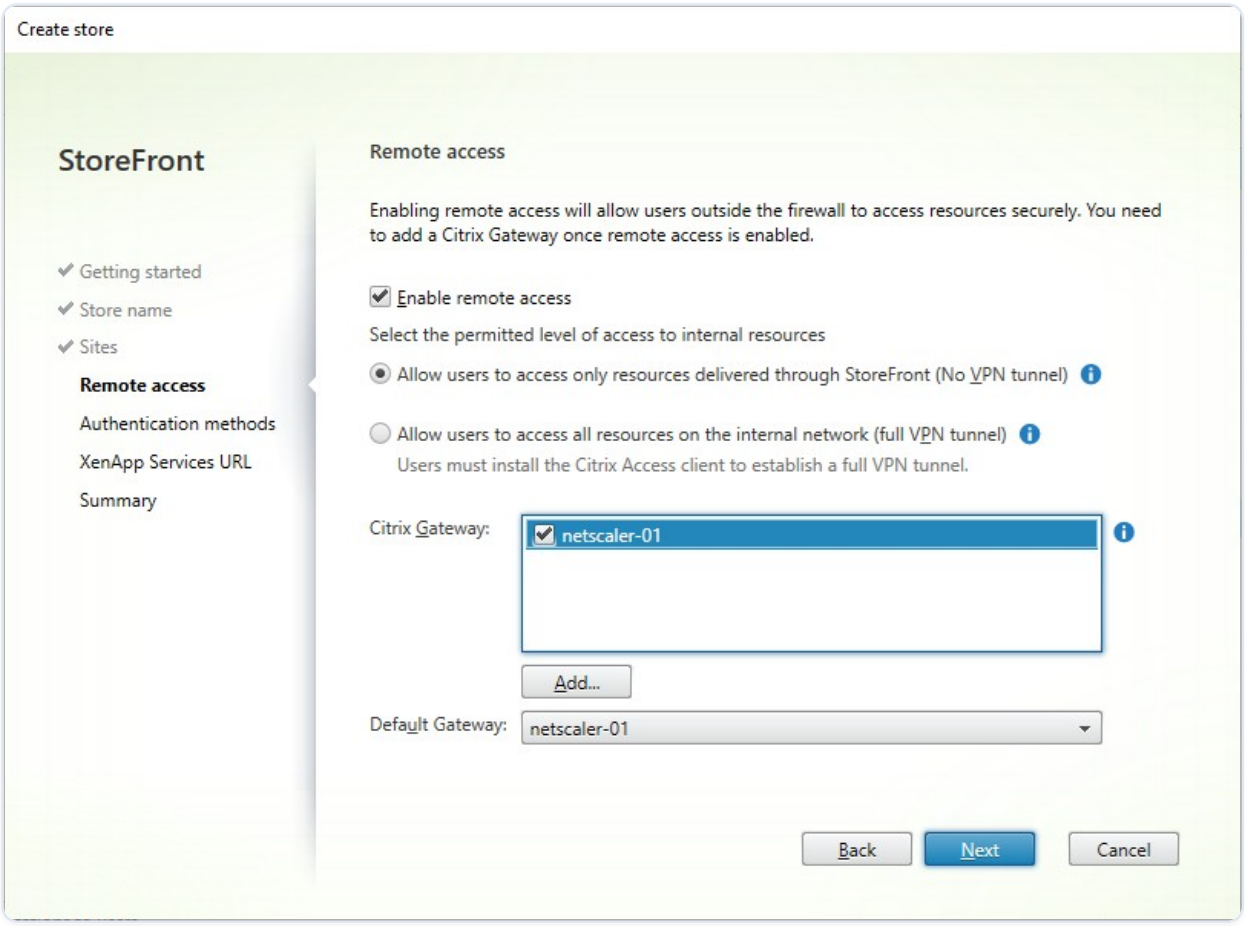
Klicken Sie auf **Weiter**.

3. Fügen Sie auf der Registerkarte **Sites** Sites für Ihre virtuellen Desktops und Anwendungen hinzu. Weitere Informationen finden Sie unter Sites verwalten.



Klicken Sie auf **Weiter**.

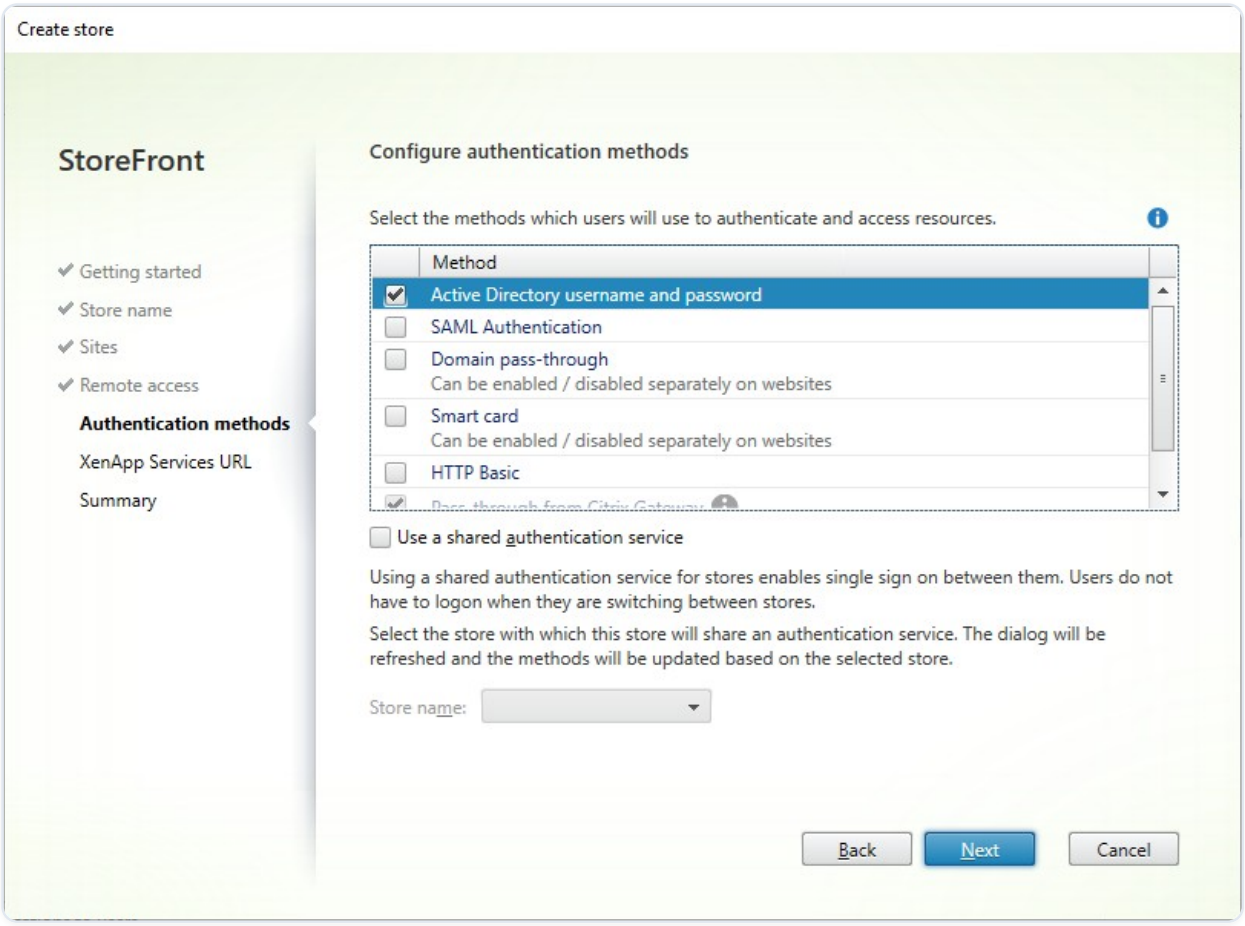
4. Wählen Sie auf der Registerkarte **Remote Access** aus, ob Sie den Store über ein Citrix Gateway verfügbar machen möchten. Weitere Informationen finden Sie unter Verwalten des Remotezugriffs auf Stores über Citrix Gateway.



5. Wählen Sie auf der Registerkarte **Authentication Methods** die Methoden aus, die Ihre Benutzer zur Authentifizierung am Store verwenden sollen, und klicken Sie auf **Next**.

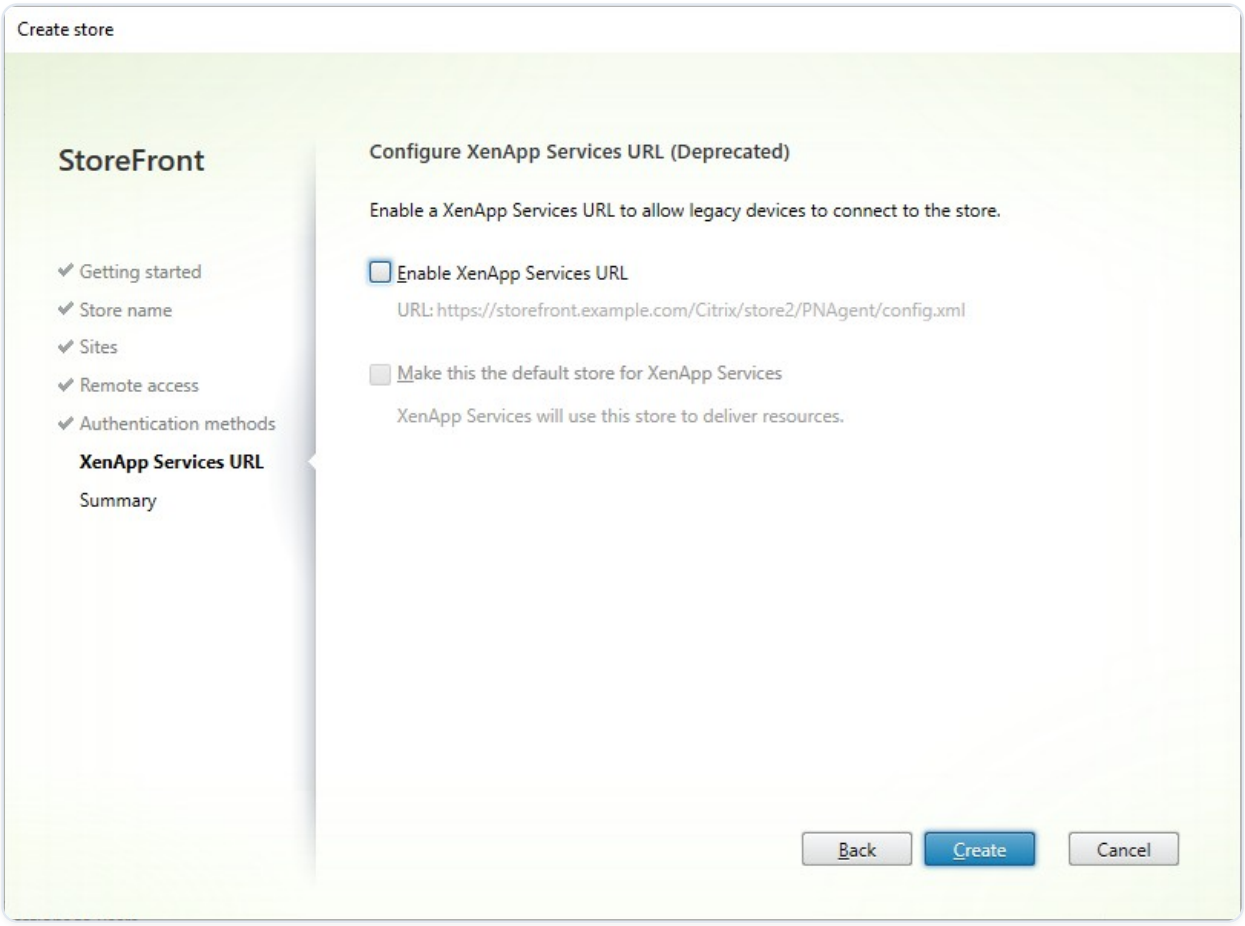
   Weitere Informationen zu den verfügbaren Authentifizierungsmethoden finden Sie unter Authentifizierung konfigurieren.

   Anstatt die Authentifizierungsmethoden für diesen Store separat zu konfigurieren, können Sie die Authentifizierungskonfiguration mit einem anderen Store teilen. Aktivieren Sie dazu **Use a shared authentication service** und wählen Sie dann einen vorhandenen Store aus.



Klicken Sie auf **Next**

6. Wenn Sie auf der Registerkarte **XenApp® Services URL** Legacy-Geräte haben, die PNAgent erfordern, wählen Sie **Enable XenApp Services URL** aus, andernfalls deaktivieren Sie es.



Klicken Sie auf **Create**

> **Hinweis:**
>
> XenApp Services ist veraltet und wird in einer zukünftigen Version entfernt.

7. Nachdem der Store erstellt wurde, klicken Sie auf **Finish**.

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

PowerShell

So erstellen Sie einen Store mit PowerShell:

1. Erstellen Sie einen Authentifizierungsdienst mit Add-STFAuthenticationService. Gemäß Konvention ist der virtuelle Pfad typischerweise `/Citrix/[StoreName]Auth`. Alternativ können Sie einen vorhandenen Authentifizierungsdienst mit Get-STFAuthenticationService abrufen. Dieser Schritt ist für einen anonymen Store nicht erforderlich.

2. Konfigurieren Sie den Authentifizierungsdienst nach Bedarf. Siehe Authentifizierung konfigurieren.
3. Rufen Sie Add-STFStoreService auf.
    - Wählen Sie einen virtuellen Pfad für den Store und legen Sie diesen als `-VirtualPath`-Parameter fest. Typischerweise ist dies /Citrix/.
    - Legen Sie `-AuthenticationService` auf den in Schritt 1 erstellten Authentifizierungsdienst fest. Alternativ legen Sie für einen anonymen Store `-Anonymous $True` fest.
    - Sie können die Details einer Site einschließen. Weitere Sites müssen separat konfiguriert werden.

Sites verwalten

Verwenden Sie den Bildschirm **Sites verwalten**, um Sites hinzuzufügen, zu ändern und zu löschen, die von Citrix Virtual Apps and Desktops, Citrix Desktops as a Service und Citrix Secure Private Access bereitgestellt werden.

Sites anzeigen

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

Sites mit PowerShell anzeigen

Um Sites mit PowerShell anzuzeigen, führen Sie das Cmdlet Get-STFStoreFarm aus.

Site hinzufügen

Citrix Virtual Apps and Desktops™ Site hinzufügen

1. Klicken Sie im Bildschirm **Sites verwalten** auf **Hinzufügen**.
2. Geben Sie einen **Anzeigenamen** ein, der Ihnen hilft, den Feed zu identifizieren.
3. Wählen Sie als **Typ Citrix Virtual Apps and Desktops oder DaaS**.
4. Klicken Sie unter **Server** für jeden DDC auf **Hinzufügen** und geben Sie die Adresse des DDC (oder des entsprechenden Lastenausgleichs) ein.

- Wenn Sie Lastenausgleichsgeräte vor den DDCs platziert haben, geben Sie die Adresse der Lastenausgleichsgeräte ein. Wenn Sie keinen Lastenausgleich verwenden, listen Sie jeden DDC einzeln auf.
- Fügen Sie mindestens 2 DDCs für Redundanz hinzu.
- Wenn Ihre Server HTTPS verwenden (empfohlen), stellen Sie sicher, dass die Namen, die Sie in der Serverliste angeben, exakt (einschließlich der Groß-/Kleinschreibung) mit den Namen auf den Zertifikaten für diese Server übereinstimmen.

5. Wählen Sie optional **Server sind lastverteilt** aus. Wenn diese Option ausgewählt ist, wählt StoreFront zufällig einen Server aus. Wenn die Option deaktiviert ist, verwendet StoreFront den ersten Server in der Liste, es sei denn, dieser ist nicht verfügbar. In diesem Fall wird die Liste durchgegangen, bis ein reagierender Server gefunden wird. Sie können die Pfeile nach oben und unten verwenden, um die Prioritätsreihenfolge festzulegen.

   - Wenn alle DDCs ähnliche Latenzzeiten aufweisen, wird empfohlen, **Server sind lastverteilt** auszuwählen, damit StoreFront die Last auf alle DDCs verteilt.
   - Wenn Sie eine geografisch verteilte Multi-Zonen-Bereitstellung mit DDCs unterschiedlicher Latenzzeiten haben, möchten Sie möglicherweise die DDCs mit der niedrigsten Latenz an den Anfang der Liste setzen und die Option **Server sind lastverteilt** deaktivieren, damit StoreFront Server mit geringerer Latenz bevorzugt. Erwägen Sie die Verwendung eines separaten Lastenausgleichs, um die Last zwischen verschiedenen DDCs am selben Standort zu verteilen.

6. Wählen Sie in der Liste **Transporttyp** den Verbindungstyp aus, den StoreFront für die Kommunikation mit den Servern verwenden soll.

   - Um Daten über unverschlüsselte Verbindungen zu senden (nicht empfohlen), wählen Sie **HTTP**. Wenn Sie diese Option auswählen, müssen Sie selbst Vorkehrungen treffen, um die Verbindungen zwischen StoreFront und Ihren Servern zu sichern.
   - Um Daten über verschlüsselte TLS-Verbindungen zu senden (empfohlen), wählen Sie **HTTPS**. Sie müssen TLS auf Delivery Controllern aktivieren oder auf den Load Balancern vor den DDCs.

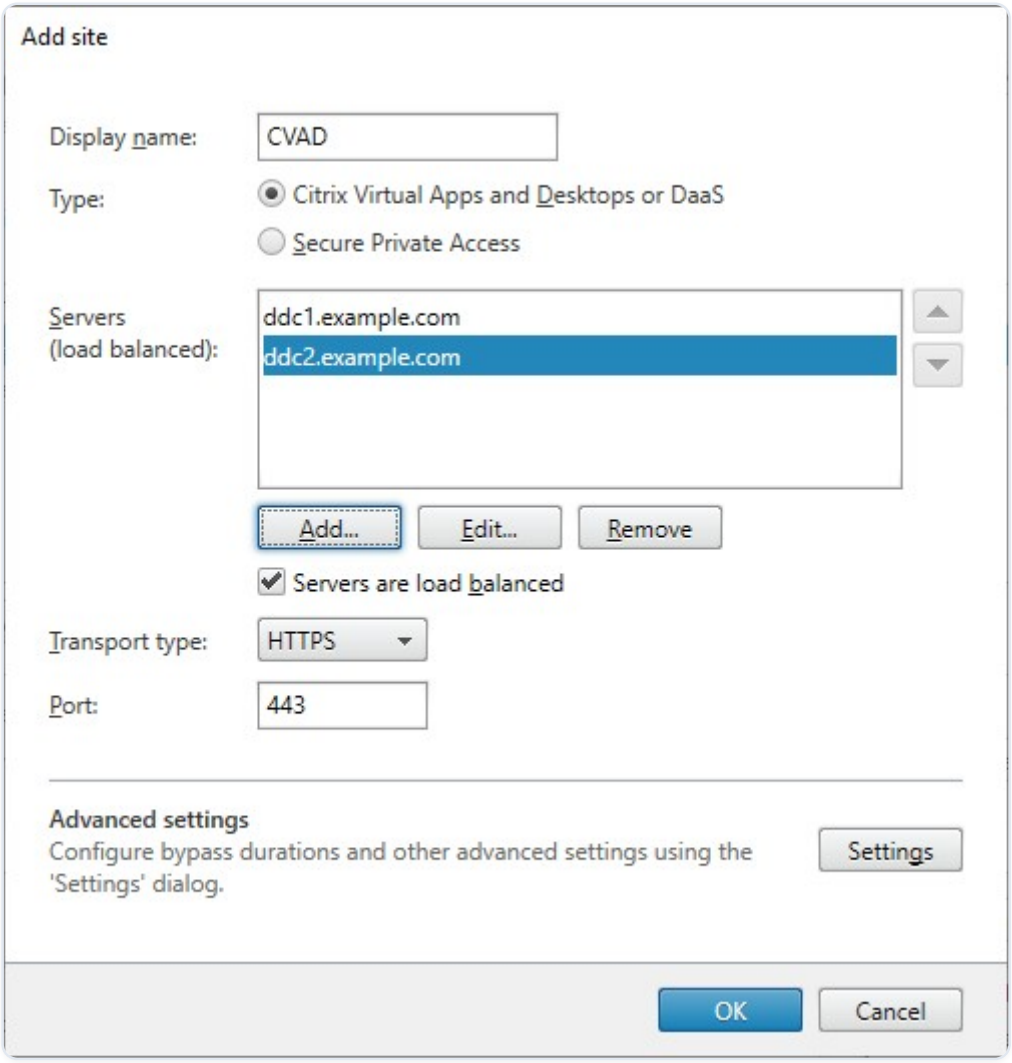
     Die folgenden TLS 1.3-Cipher Suiten werden unterstützt:

     - TLS_AES_256_GCM_SHA384
     - TLS_AES_128_GCM_SHA256

     Die folgenden TLS 1.2-Cipher Suiten werden unterstützt:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

7. Geben Sie den Port an, den StoreFront für Verbindungen zu den Servern verwenden soll. Der Standardport ist 80 für HTTP-Verbindungen und 443 für HTTPS-Verbindungen. Der angegebene Port muss der Port sein, der vom Citrix XML Service verwendet wird.
8. Klicken Sie auf **OK**



9. Wenn Sie Sicherheitsschlüssel konfiguriert haben (empfohlen), müssen Sie den Schlüssel mit PowerShell hinzufügen. Zum Beispiel:

```
$store = Get-STFStoreService -VirtualPath [path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [site name]
```

```
Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [Security key]
```

Citrix Virtual Apps and Desktops™ Site mit PowerShell hinzufügen

Um eine Site, auch als Farm bekannt, hinzuzufügen, führen Sie das Cmdlet Add-STFStoreFarm mit `FarmType` `XenDesktop` aus

Um beispielsweise eine Site namens „CVAD“ mit einem Sicherheitsschlüssel hinzuzufügen:

```
$store = Get-STFStoreService -VirtualPath [path to store]

Add-STFStoreFarm -StoreService $store -FarmName "CVAD" -FarmType
XenDesktop -Port 443 -TransportType HTTPS -Servers
@("ddc1.example.com","ddc2.example.com") -XMLValidationEnabled $true
-XMLValidationSecret "MySecret"
```

Citrix Desktops as a Service Site hinzufügen

1. Klicken Sie im Bildschirm **Sites verwalten** auf **Hinzufügen**.
2. Geben Sie einen **Anzeigenamen** ein, der Ihnen hilft, den Feed zu identifizieren.
3. Wählen Sie als **Typ Citrix Virtual Apps and Desktops oder DaaS**.
4. Klicken Sie unter **Server** für jeden Cloud Connector auf **Hinzufügen** und geben Sie den Namen des Cloud Connectors (oder des entsprechenden Lastausgleichs) ein.

    - Wenn Sie einen Lastausgleich vor den Cloud Connectors oder DDCs platziert haben, geben Sie den Namen des Lastausgleichs ein. Wenn Sie keinen Lastausgleich verwenden, listen Sie jeden DDC oder Cloud Connector einzeln auf.
    - Wenn Sie mehrere Ressourcenstandorte haben, empfiehlt Citrix, die Cloud Connectors von allen Ressourcenstandorten hinzuzufügen, die VDAs enthalten, damit StoreFront im Falle eines Ausfalls den lokalen Hostcache verwenden kann, um VDAs am entsprechenden Standort zu starten.
    - Wenn Sie einen Lastausgleich verwenden, ist es wichtig, dass Sie für jeden Ressourcenstandort einen separaten Lastausgleich verwenden. Wenn ein Lastausgleich Server an mehreren Ressourcenstandorten bedient, spielt dies im Normalbetrieb keine Rolle. Im lokalen Hostcache-Modus würde dies jedoch verhindern, dass StoreFront Startanforderungen an den richtigen Ressourcenstandort weiterleiten kann, was zu fehlgeschlagenen Starts führen würde.

- Wenn Ihre Server HTTPS verwenden (empfohlen), stellen Sie sicher, dass die Namen, die Sie in der Serverliste angeben, genau (einschließlich der Groß-/Kleinschreibung) mit den Namen auf den Zertifikaten für diese Server übereinstimmen.

5. Wählen Sie optional **Server sind lastausgeglichen**. Wenn diese Option ausgewählt ist, wählt StoreFront zufällig einen Server aus. Wenn die Option deaktiviert ist, verwendet StoreFront den ersten Server in der Liste, es sei denn, dieser ist nicht verfügbar. In diesem Fall wird die Liste durchgegangen, bis ein reagierender Server gefunden wird. Sie können die Auf- und Abwärtspfeile verwenden, um die Prioritätsreihenfolge festzulegen.

   - Wenn alle Server ähnliche Latenzzeiten aufweisen, wird empfohlen, **Server sind lastverteilt** auszuwählen, damit StoreFront die Last auf alle DDCs verteilt.
   - Wenn Sie eine geografisch verteilte Bereitstellung mit mehreren Zonen haben, bei der DDCs unterschiedliche Latenzzeiten aufweisen, möchten Sie die Server mit der niedrigsten Latenz möglicherweise an den Anfang der Liste setzen und die Option **Server sind lastverteilt** deaktivieren, damit StoreFront Server mit geringerer Latenz bevorzugt. Erwägen Sie die Verwendung eines separaten Lastenausgleichs, um die Last zwischen verschiedenen Servern am selben Ressourcenstandort oder in derselben Zone zu verteilen.

6. Wählen Sie in der Liste **Transporttyp** den Verbindungstyp aus, den StoreFront für die Kommunikation mit den Servern verwenden soll.

   - Um Daten über unverschlüsselte Verbindungen zu senden (nicht empfohlen), wählen Sie **HTTP**. Wenn Sie diese Option auswählen, müssen Sie selbst Vorkehrungen treffen, um die Verbindungen zwischen StoreFront und Ihren Cloud Connectors zu sichern.
   - Um Daten über verschlüsselte Verbindungen zu senden (empfohlen), wählen Sie **HTTPS**. Sie müssen die Cloud Connectors für HTTPS konfigurieren.

     Die folgenden TLS 1.3-Cipher-Suites werden unterstützt:

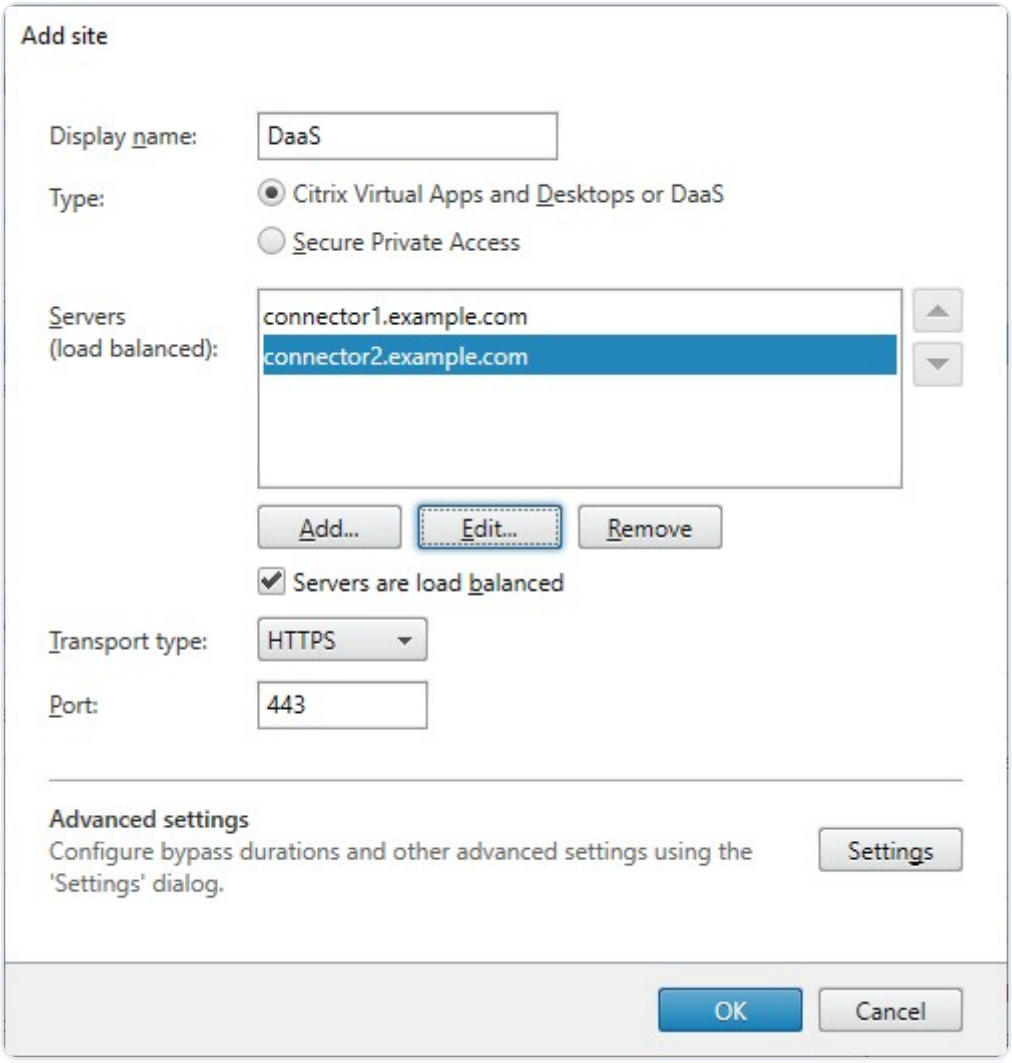
     - TLS_AES_256_GCM_SHA384
     - TLS_AES_128_GCM_SHA256

     Die folgenden TLS 1.2-Cipher-Suites werden unterstützt:

     - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
     - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

7. Geben Sie den Port an, den StoreFront für Verbindungen zu den Servern verwenden soll. Der Standardport ist 80 für HTTP-Verbindungen und 443 für HTTPS-Verbindungen.
8. Klicken Sie auf **OK**.



9. Wenn Sie Sicherheitsschlüssel konfiguriert haben (empfohlen), müssen Sie den Schlüssel mit PowerShell hinzufügen. Zum Beispiel:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Site name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [Security key]
```

Citrix Desktops as a Service-Site mit PowerShell hinzufügen

Um eine Site, auch als Farm bekannt, hinzuzufügen, führen Sie das Cmdlet Add-STFStoreFarm mit `FarmType` `XenDesktop` aus.

Zum Beispiel, um eine Site namens „DaaS“ mit einem Sicherheitsschlüssel hinzuzufügen:

```
$store = Get-STFStoreService -VirtualPath [path to store]

Add-STFStoreFarm -StoreService $store -FarmName "DaaS" -FarmType
XenDesktop -Port 443 -TransportType HTTPS -Servers
@("connector1.example.com","connector2.example.com") -XMLValidationEnabled
$true -XMLValidationSecret "MySecret"
```

Citrix Secure Private Access-Site hinzufügen

Wenn Ihr StoreFront-Server für Citrix Secure Private Access konfiguriert ist, können Sie Citrix Secure Private Access-Sites hinzufügen.

1. Navigieren Sie in StoreFront zu **Stores** > **Manage sites**.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie im Fenster **Add site** einen **Anzeigenamen** ein, um den Feed zu identifizieren.
4. Wählen Sie als **Typ** die Option **Citrix Secure Private Access**.
5. Geben Sie den Namen des Citrix Secure Private Access-Servers ein.
6. Wählen Sie in der Dropdown-Liste **Transporttyp** den Verbindungstyp aus, der für die Kommunikation mit den Servern verwendet werden kann.
   - **HTTP:** sendet Daten über unverschlüsselte Verbindungen (nicht empfohlen).
   - **HTTPS:** sendet Daten über sichere HTTPS-Verbindungen (empfohlen) unter Verwendung von Transport Layer Security (TLS).
7. Geben Sie den Port an, der für Verbindungen zu den Servern verwendet werden soll. Der Standardport für **HTTP** ist 80 und für **HTTPS** ist er 443.
8. Wählen Sie **OK**.
9. Wenn Sie einen Sicherheitsschlüssel konfiguriert haben (empfohlen), müssen Sie den Schlüssel mit PowerShell hinzufügen. Zum Beispiel:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Site name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [Security key]
```

Citrix Secure Private Access-Site mit PowerShell hinzufügen

Um eine Site, auch als Farm bezeichnet, hinzuzufügen, führen Sie das Cmdlet Add-STFStoreFarm mit `FarmType` `SPA` aus.

Beispiel: Hinzufügen einer Site namens „SPA Apps“ mit einem Sicherheitsschlüssel:

```
$store = Get-STFStoreService -VirtualPath [path to store]

$farm = Add-STFStoreFarm -StoreService $store -FarmName "SPA Apps"
-FarmType SPA -Port 443 -TransportType HTTPS -ServiceUrls https://spa-
service.example.com -XMLValidationEnabled $true -XMLValidationSecret
"MySecret"
```

Site bearbeiten

Wählen Sie im Bildschirm **Sites verwalten** eine Site aus und klicken Sie auf **Bearbeiten**.

Warnung:

Wenn Sie eine Site umbenennen, dann:

- Die Site wird aus jeder Optimal HDX-Routing-Konfiguration gelöscht. Sie müssen die Site wieder zu Ihrer Optimal HDX-Routing-Konfiguration hinzufügen.
- Alle Benutzerfavoriten Favoriten für diese Site verschwinden (es sei denn, Sie verwenden die Aggregation mehrerer Sites). Dies liegt daran, dass der Favoriteneintrag auf die Site namentlich verweist. Die Favoriteneinträge werden nicht gelöscht. Wenn Sie die Site also wieder in ihren ursprünglichen Namen umbenennen, werden die Favoriten erneut angezeigt. Um dies zu beheben, können Sie, wenn Sie eine SQL Server-Datenbank verwenden, die Einträge in der Datenbank aktualisieren. Andernfalls können Sie die

> Favoriten exportieren, die Namen korrigieren und erneut importieren. Weitere Informationen finden Sie unter Abonnementdaten verwalten.

Site mit PowerShell bearbeiten

Um eine Site mit PowerShell zu ändern, führen Sie das Cmdlet Set-STFStoreFarm aus.

Site löschen

Wählen Sie im Bildschirm **Sites verwalten** eine Site aus und klicken Sie auf **Entfernen**.

Site mit PowerShell löschen

Um eine Site mit PowerShell zu löschen, verwenden Sie den Befehl Remove-STFStoreFarm.

Integritätsprüfung und Server-Bypass-Verhalten

Um die Leistung zu verbessern, wenn einige der Server, die Ressourcen bereitstellen, nicht verfügbar sind, umgeht StoreFront vorübergehend Server, die nicht reagieren. Während ein Server umgangen wird, ignoriert StoreFront diesen Server und verwendet ihn nicht für den Zugriff auf Ressourcen. Dadurch werden Verzögerungen beim Versuch, eine Verbindung zu nicht verfügbaren Servern herzustellen, vermieden.

Verwenden Sie diese Parameter, um die Dauer des Umgehungsverhaltens anzugeben:

- **Abfrageintervall für Hintergrund-Integritätsprüfung** – Gibt an, wie oft StoreFront prüft, ob jeder Server verfügbar ist. Der Standardwert ist 1 Minute. Informationen zum Konfigurieren finden Sie unter Abfrageintervall für Hintergrund-Integritätsprüfung.
- **Umgehungsdauer** – Wenn die Hintergrund-Integritätsprüfung aktiviert ist, sollte dieser Wert mindestens auf das Abfrageintervall eingestellt werden, darüber hinaus hat der Wert jedoch keine Auswirkungen. Wenn die Hintergrund-Integritätsprüfung deaktiviert ist (nicht empfohlen), werden die Server umgangen, bis die Dauer abläuft. Der Standardwert ist 60 Minuten.
- **Umgehungsdauer bei vollständigem Ausfall** – Wird nur verwendet, wenn die Hintergrund-Integritätsprüfung deaktiviert ist (nicht empfohlen). Gibt eine reduzierte Dauer in Minuten an, die StoreFront anstelle der **Umgehungsdauer** verwendet, wenn alle Server für eine bestimmte Site umgangen werden. Der Standardwert ist 0 Minuten, was bedeutet, dass StoreFront keine Server umgeht.

So ändern Sie die Umgehungsparameter

Normalerweise ist es nicht erforderlich, diese Einstellungen zu ändern.

1. Wählen Sie in der Citrix StoreFront-Verwaltungskonsole im linken Bereich den Knoten **Stores** aus.
2. Wählen Sie einen Store im Ergebnisbereich aus.
3. Klicken Sie im Bereich **Aktionen** auf **Sites verwalten**.
4. Wählen Sie einen Controller aus, klicken Sie auf **Bearbeiten** und dann auf dem Bildschirm **Site bearbeiten** auf **Einstellungen**.
5. Klicken Sie unter Erweiterte Einstellungen auf **Einstellungen**.
6. Im Dialogfeld „Erweiterte Einstellungen konfigurieren“:
    a. Klicken Sie in der Zeile **Umgehungsdauer bei vollständigem Ausfall** 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 mehr reagieren.
    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, nachdem er nicht mehr reagiert.

Benutzer Sites zuordnen

Standardmäßig sehen Benutzer, die auf einen Store zugreifen, eine Zusammenfassung aller Ressourcen, die ihnen von allen für diesen Store konfigurierten Sites zur Verfügung stehen. Um verschiedenen Benutzern unterschiedliche Ressourcen bereitzustellen, können Sie separate Stores oder sogar separate StoreFront-Bereitstellungen konfigurieren. Alternativ können Sie den Zugriff auf bestimmte Bereitstellungen basierend auf der Mitgliedschaft der Benutzer in Microsoft Active Directory-Gruppen ermöglichen. Dadurch können Sie über einen einzigen Store unterschiedliche Erfahrungen für verschiedene Benutzergruppen konfigurieren.

Sie können beispielsweise gemeinsame Ressourcen für alle Benutzer in einer Bereitstellung und Finanzanwendungen für die Buchhaltungsabteilung in einer anderen Bereitstellung gruppieren. In einer solchen Konfiguration sieht ein Benutzer, der kein Mitglied der Benutzergruppe „Buchhaltung“ ist, beim Zugriff auf den Store nur die gemeinsamen Ressourcen. Ein Mitglied der Benutzergruppe „Buchhaltung“ erhält sowohl die gemeinsamen Ressourcen als auch die Finanzanwendungen angezeigt.

Alternativ können Sie eine Bereitstellung für Power-User erstellen, die dieselben Ressourcen wie Ihre anderen Bereitstellungen bereitstellt, jedoch mit schnellerer und leistungsfähigerer Hardware. Dadurch können Sie geschäftskritischen Benutzern, wie z. B. Ihrem Führungsteam, eine verbesserte Erfahrung bieten. Alle Benutzer sehen dieselben Desktops und Anwendungen, wenn sie sich am Store anmelden, aber Mitglieder der Benutzergruppe „Führungskräfte“ werden

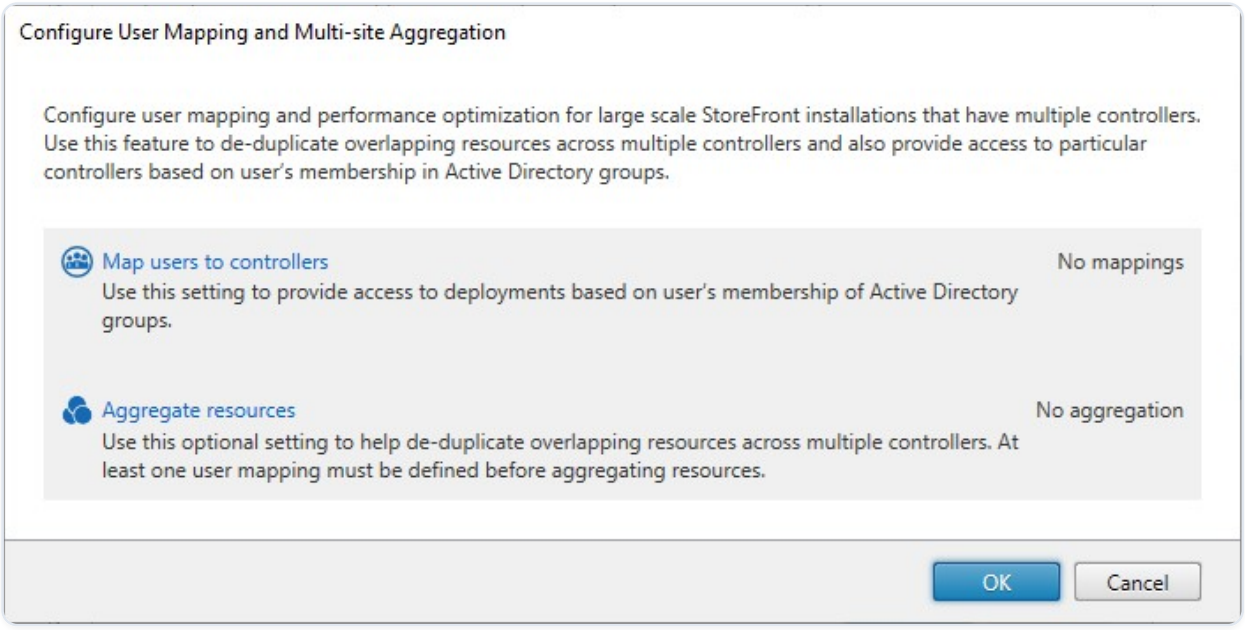
bevorzugt mit Ressourcen verbunden, die von der Power-User-Bereitstellung bereitgestellt werden.

> Hinweis:
>
> Dies filtert ganze Sites. Darüber hinaus können innerhalb einer Site Anwendungen nach Benutzergruppe in der Citrix Virtual Apps and Desktops Studio-Konfiguration gefiltert werden.

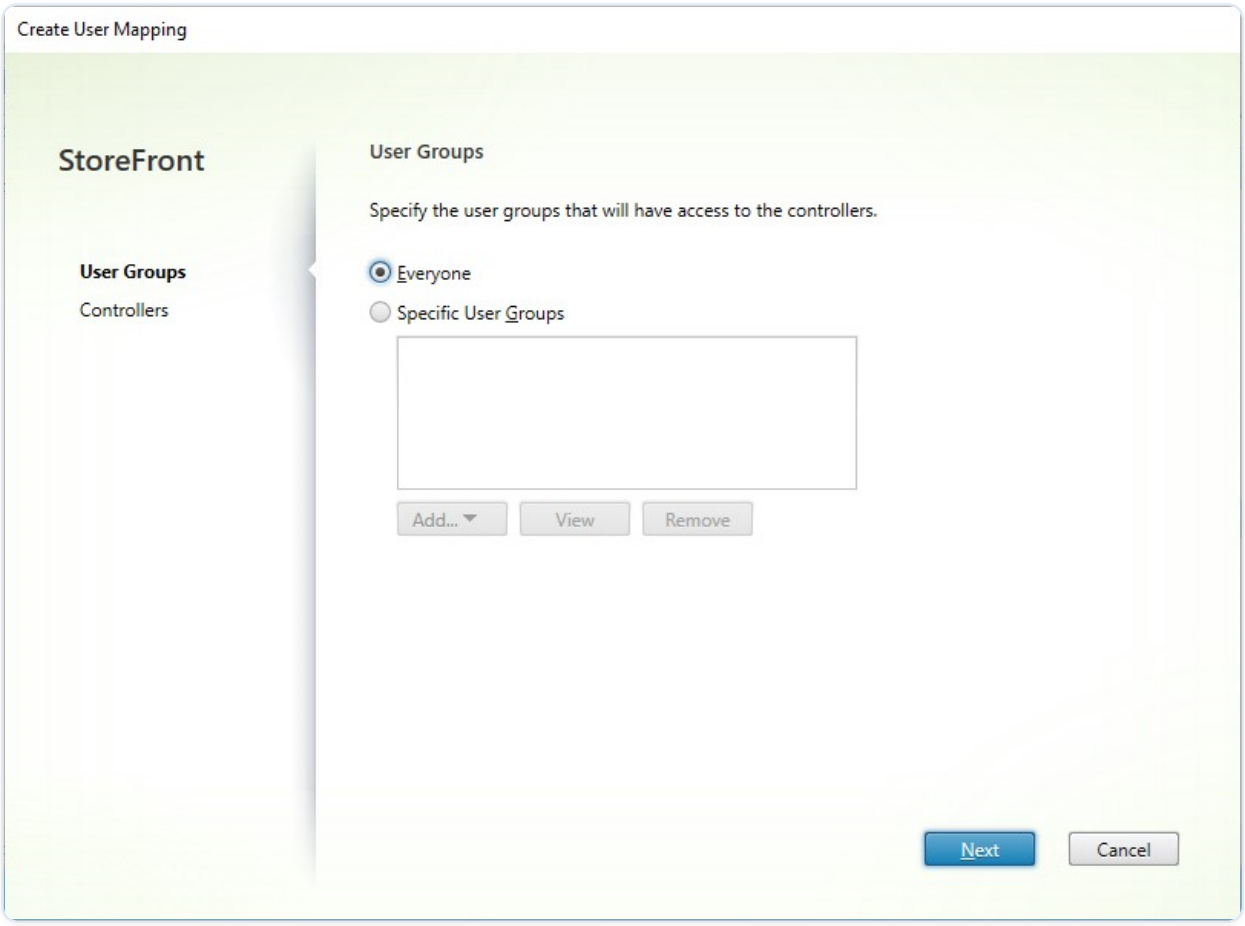
So konfigurieren Sie bestimmte Sites für bestimmte Benutzergruppen:

1. Klicken Sie auf dem Bildschirm **Sites verwalten** unter **Benutzerzuordnung und Multi-Site-Aggregationskonfiguration** auf **Konfigurieren**. Diese Option ist nur verfügbar, wenn zwei oder mehr Sites konfiguriert sind.

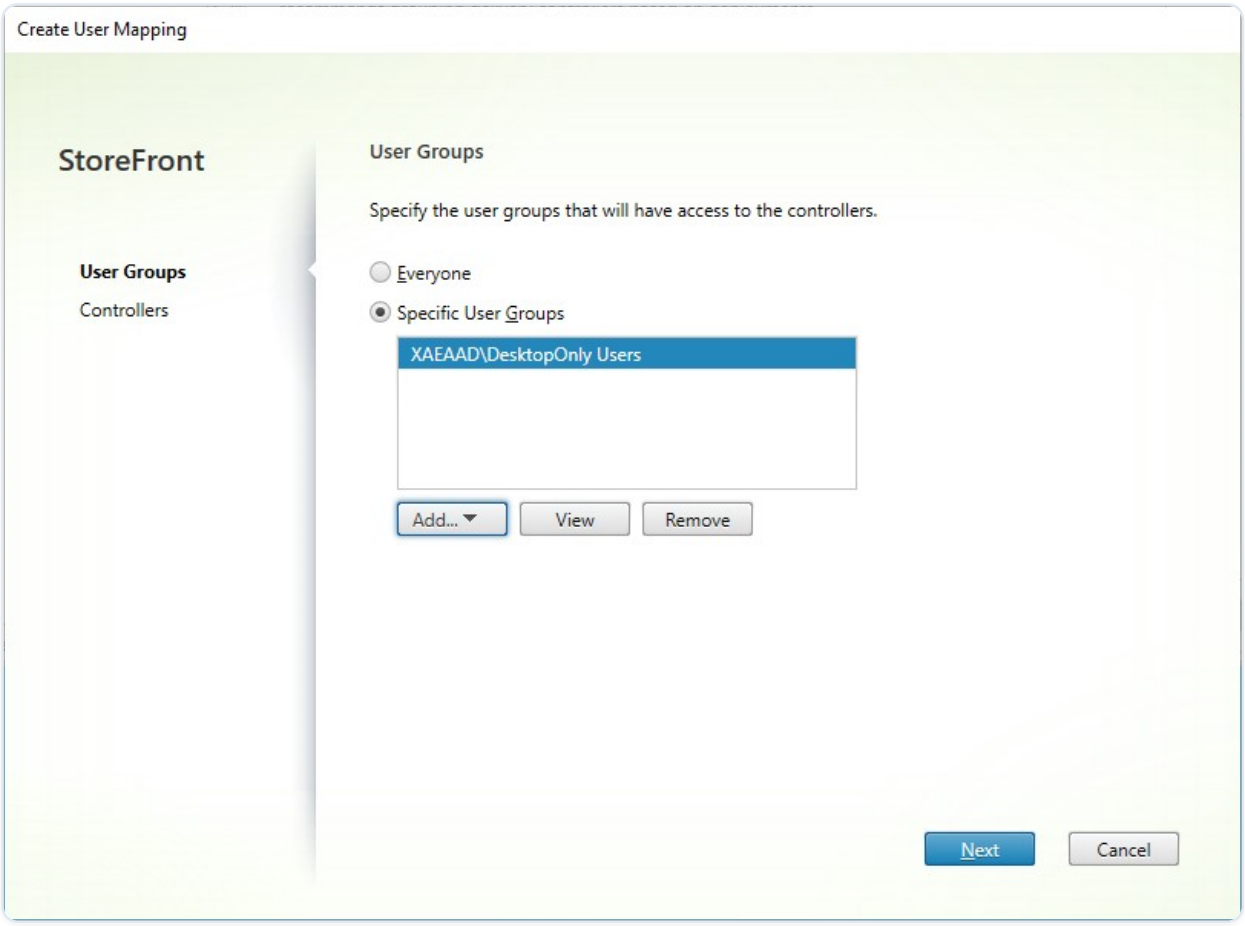
   Dadurch wird der Bildschirm **Benutzerzuordnung und Multi-Site-Aggregation konfigurieren** geöffnet.



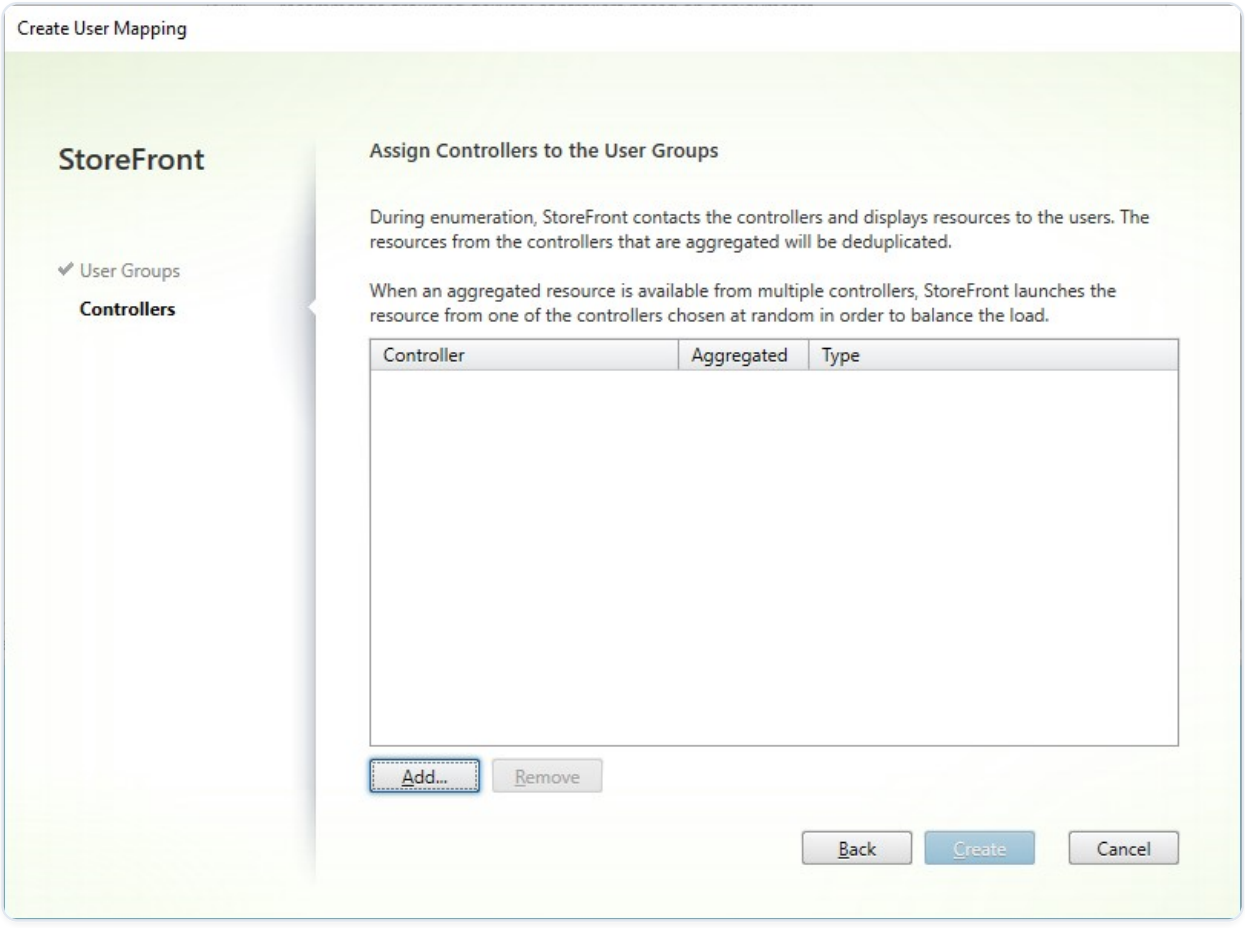
2. Klicken Sie auf **Benutzer Sites zuordnen**. Dadurch wird der Bildschirm **Benutzerzuordnung erstellen** geöffnet, um Ihre erste Zuordnung zu erstellen. Sie können später weitere Zuordnungen erstellen.



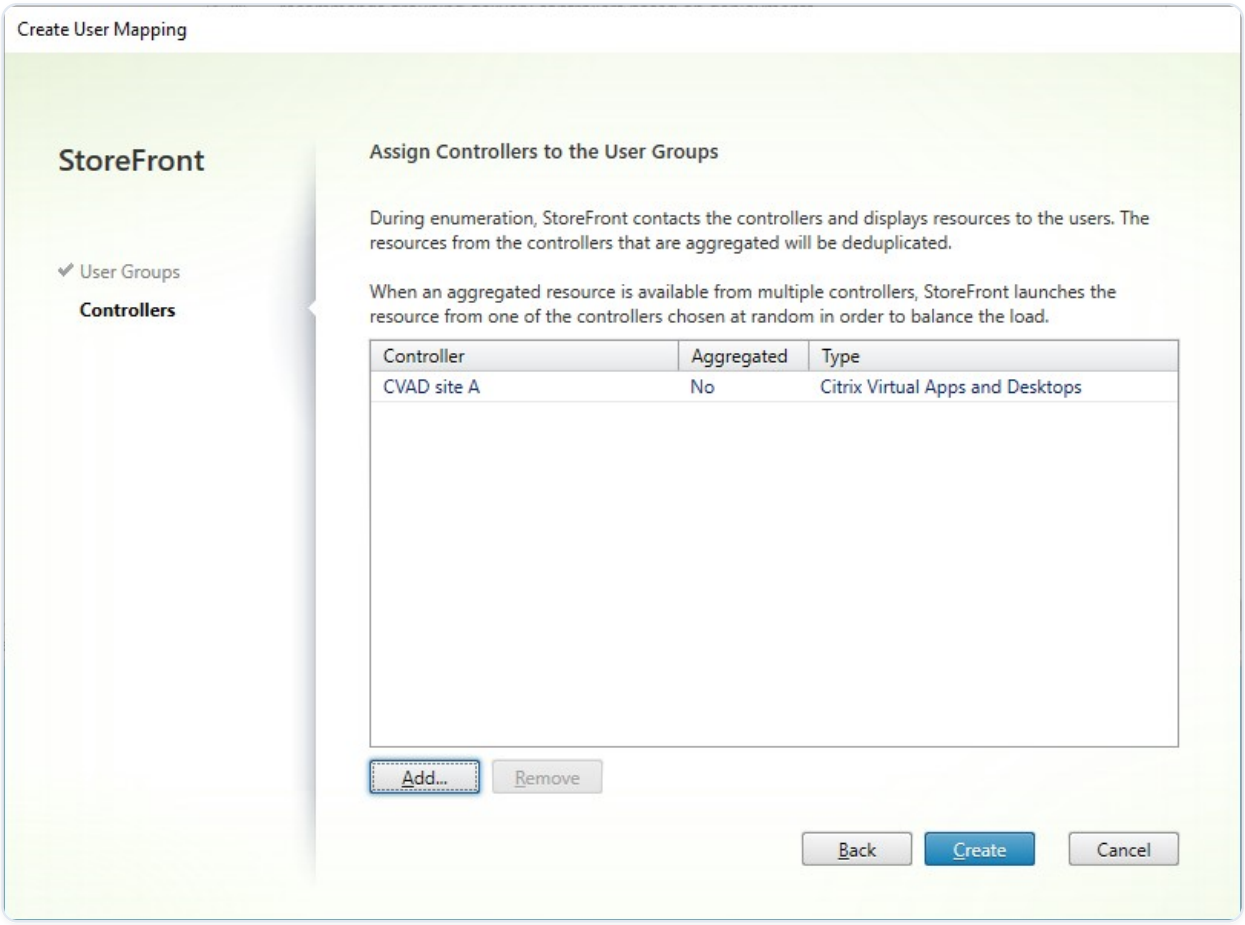
3. Wählen Sie entweder **Jeder** oder **Spezifische Benutzergruppen** und fügen Sie eine oder mehrere Gruppen hinzu.



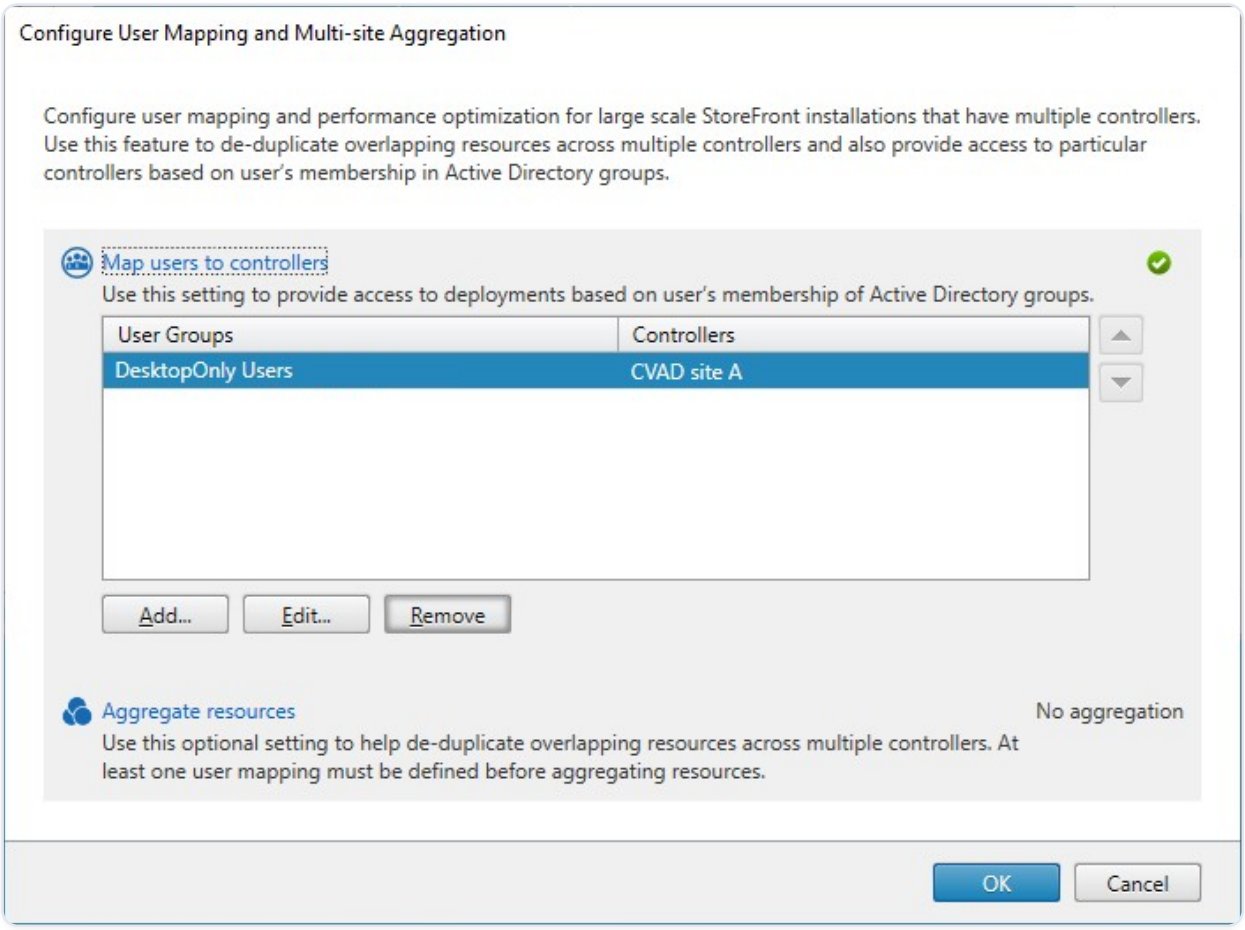
4. Klicken Sie auf **Weiter**. Dadurch gelangen Sie zur Registerkarte **Sites**.



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



6. Klicken Sie auf **Erstellen**.



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

Benutzer mithilfe von PowerShell Ressourcen zuordnen

Sie können Benutzer mithilfe von PowerShell Ressourcen zuordnen.

1. Erstellen Sie für jede Site (im SDK als Farm bezeichnet) ein EquivalentFarmset. Alle Sites müssen Teil eines Farmsets sein, andernfalls stehen sie keinem Benutzer zur Verfügung. Rufen Sie New-STFEquivalentFarmset mit den folgenden Parametern auf:

   - `Name` – ein eindeutiger Name für das EquivalentFarmSet
   - `PrimaryFarms` – der Name der nicht aggregierten Site (Farm).

2. Erstellen Sie für jede Gruppe von Benutzern, die Zugriff auf eine andere Gruppe von Sites benötigen, Zuordnungen zwischen diesen Benutzern und jedem der EquivalentFarmSets. Um die UserFarmMapping zu erstellen, rufen Sie Add-STFUserFarmMapping mit den folgenden Parametern auf:

   - `StoreService` – Der Store-Dienst, dem die UserFarmMapping hinzugefügt werden soll.
   - `Name` – Ein eindeutiger Name für die Zuordnung.

- `GroupMembers` – Eine Hashtabelle, die die Namen und SIDs der Benutzergruppen enthält, die Teil der Zuordnung sind. Der Name dient nur zur Anzeige; 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` – Ein im vorherigen Schritt erstelltes EquivalentFarmSet.

Sie müssen sicherstellen, dass jede Site (Farm) in mindestens einer UserFarmMapping enthalten ist, da sonst keine Benutzer auf diese Ressource zugreifen können.

Multi-Site-Aggregation

Standardmäßig listet StoreFront alle Bereitstellungen auf, die Desktops und Anwendungen für einen Store bereitstellen, und behandelt alle diese Ressourcen als eigenständig. Das bedeutet, dass Benutzer, wenn dieselbe Ressource von mehreren Bereitstellungen verfügbar ist, für jede Ressource ein Symbol sehen, was verwirrend sein kann, wenn die Ressourcen denselben Namen haben. Wenn Sie hochverfügbare Multi-Site-Konfigurationen einrichten, können Sie Citrix Virtual Apps and Desktops-Bereitstellungen, die denselben Desktop oder dieselbe Anwendung bereitstellen, gruppieren, sodass identische Ressourcen für Benutzer aggregiert werden können. Gruppierte Bereitstellungen müssen nicht identisch sein, aber Ressourcen müssen auf jedem Server denselben Namen und Pfad haben, um aggregiert zu werden.

Bei der Multi-Site-Aggregation, wenn ein Desktop oder eine Anwendung von mehreren Citrix Virtual Apps and Desktops-Bereitstellungen, die für einen bestimmten Store konfiguriert sind, verfügbar ist, aggregiert StoreFront alle Instanzen dieser Ressource und präsentiert den Benutzern ein einziges Symbol. Wenn ein Benutzer eine aggregierte Ressource startet, bestimmt StoreFront die am besten geeignete Instanz dieser Ressource für den Benutzer, wobei Folgendes berücksichtigt wird:

- Serververfügbarkeit.
- Ob der Benutzer bereits eine aktive Sitzung hat.
- `Primary`- und `Secondary`-Schlüsselwörter.
- Die Zonenpräferenz des Benutzers.
- Die Reihenfolge der Bereitstellungs-Feeds, die Sie in Ihrer Konfiguration angegeben haben.

StoreFront überwacht dynamisch Server, die nicht auf Anfragen reagieren, da diese Server entweder überlastet oder vorübergehend nicht verfügbar sind. Benutzer werden zu Ressourceninstanzen auf anderen Servern weitergeleitet, bis die Kommunikation wiederhergestellt ist. Sofern von den Servern, die die Ressourcen bereitstellen, unterstützt, versucht StoreFront, vorhandene Sitzungen wiederzuverwenden, um zusätzliche Ressourcen bereitzustellen. Wenn ein

Benutzer bereits eine aktive Sitzung auf einer Bereitstellung hat, die auch die angeforderte Ressource bereitstellt, verwendet StoreFront die Sitzung wieder, wenn sie mit dieser Ressource kompatibel ist. Die Minimierung der Anzahl der Sitzungen pro Benutzer reduziert die Zeit, die zum Starten zusätzlicher Desktops oder Anwendungen benötigt wird, und kann eine effizientere Nutzung von Produktlizenzen ermöglichen.

Sie können die angegebene Bereitstellungsreihenfolge für einzelne Citrix Virtual Apps and Desktops-Ressourcen überschreiben, um bevorzugte Bereitstellungen zu definieren, mit denen Benutzer verbunden werden, wenn sie auf einen bestimmten Desktop oder eine bestimmte Anwendung zugreifen. Dies ermöglicht es Ihnen beispielsweise, festzulegen, dass Benutzer bevorzugt mit einer Bereitstellung verbunden werden, die speziell für die Bereitstellung eines bestimmten Desktops oder einer bestimmten Anwendung angepasst ist, aber andere Bereitstellungen für andere Ressourcen verwenden. Hängen Sie dazu die Zeichenfolge `KEYWORDS:Primary` an die Beschreibung des Desktops oder der Anwendung auf der bevorzugten Bereitstellung und `KEYWORDS:Secondary` an die Ressource auf anderen Bereitstellungen an. Wenn möglich, werden Benutzer mit der Bereitstellung verbunden, die die primäre Ressource bereitstellt, unabhängig von der in Ihrer Konfiguration angegebenen Bereitstellungsreihenfolge. Benutzer werden mit Bereitstellungen verbunden, die sekundäre Ressourcen bereitstellen, wenn die bevorzugte Bereitstellung nicht verfügbar ist.

Als Teil der StoreFront-Site-Konfiguration können Sie angeben, in welchen Zonen sich diese Ressourcen befinden. Wenn Benutzer über ein GSLB auf StoreFront zugreifen, können Sie das GSLB so konfigurieren, dass es einen Zonenpräferenz-Header einfügt. StoreFront versucht dann, auf der bevorzugten Bereitstellung gehostete Anwendungen zu starten, bevor es andere Bereitstellungen kontaktiert.

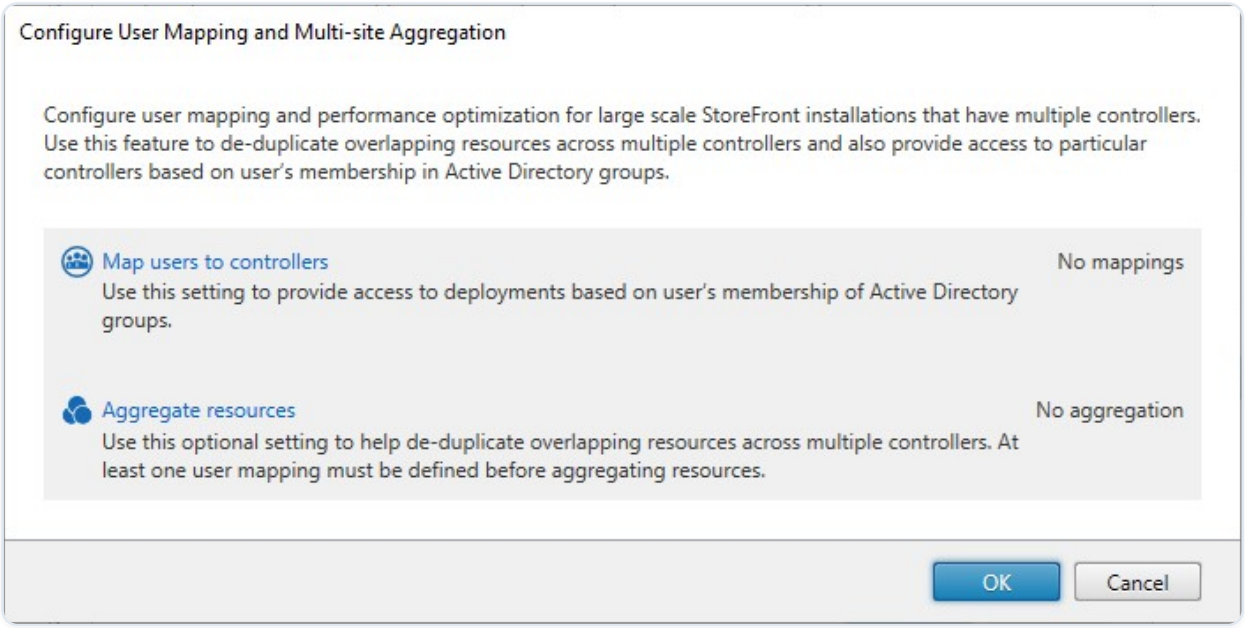
Nach Überprüfung der anderen Faktoren verwendet StoreFront die in Ihrer Konfiguration angegebene Reihenfolge, um die Bereitstellung zu bestimmen, mit der der Benutzer verbunden wird. Wenn dem Benutzer mehrere gleichwertige Bereitstellungen zur Verfügung stehen, können Sie festlegen, dass Benutzer entweder mit der ersten verfügbaren Bereitstellung oder zufällig mit einer beliebigen Bereitstellung in der Liste verbunden werden. Das Verbinden von Benutzern mit der ersten verfügbaren Bereitstellung ermöglicht es Ihnen, die Anzahl der verwendeten Bereitstellungen für die aktuelle Benutzeranzahl zu minimieren. Das zufällige Verbinden von Benutzern sorgt für eine gleichmäßigere Verteilung der Benutzer auf alle verfügbaren Bereitstellungen.

Wenn ein Start von einer Site fehlschlägt, versucht StoreFront andere geeignete Sites, es sei denn:

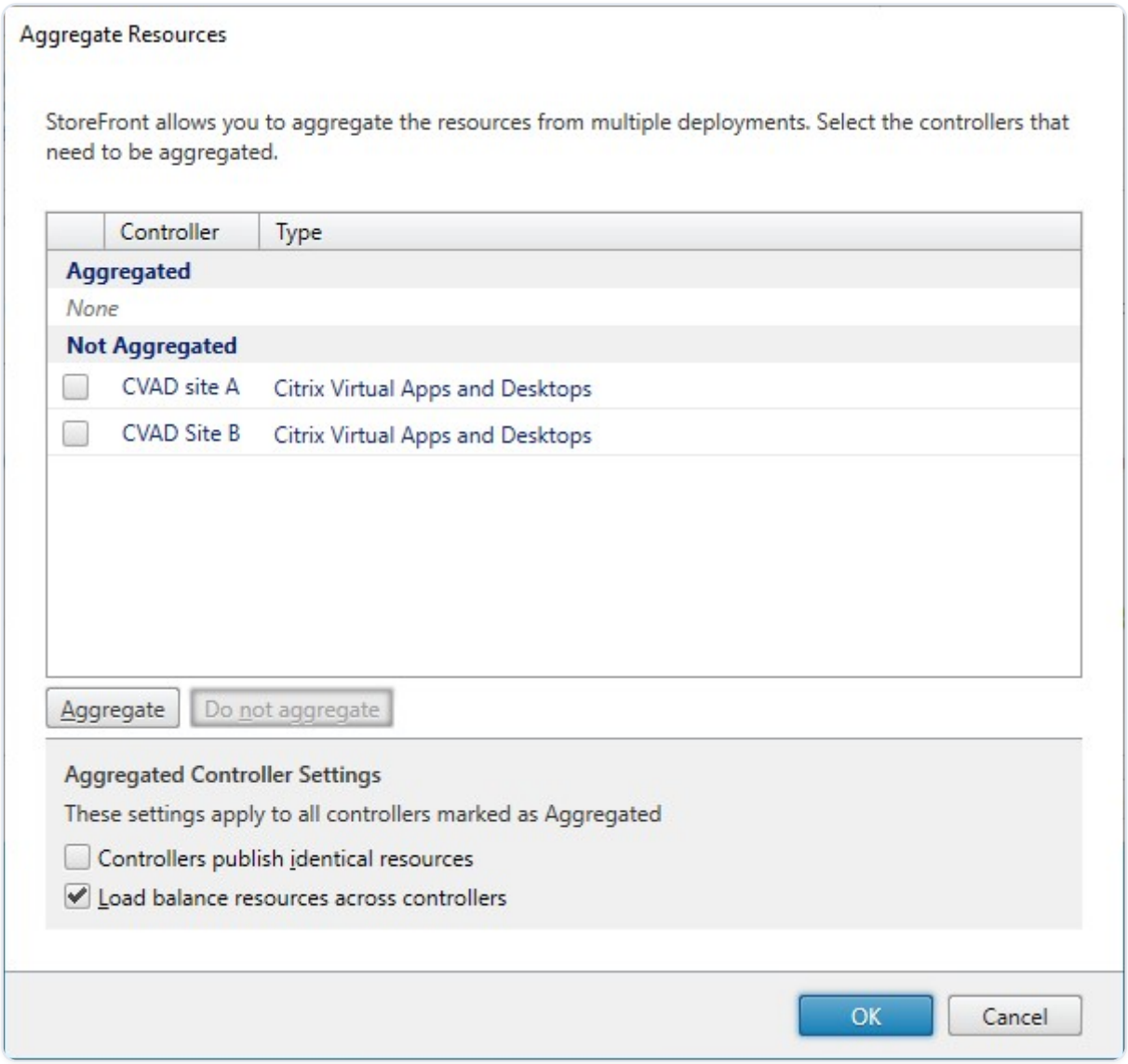
- Ein Controller meldet, dass der Benutzer sein zugewiesenes Desktop-Limit erreicht hat.
- Ein Controller meldet einen Anmeldefehler (z. B. ungültig, abgelaufen oder außerhalb der Geschäftszeiten). StoreFront versucht es nicht erneut mit anderen Delivery Controllern, da es das gleiche Ergebnis erwarten würde und um wiederholte Versuche zu vermeiden, die zu einer Kontosperrung führen könnten.
- Der Startvorgang läuft ab. Dies würde nur in extremen Fällen auftreten, in denen eine große Anzahl von Controllern mit hoher Latenz vorhanden ist.

So konfigurieren Sie die Multi-Site-Aggregation:

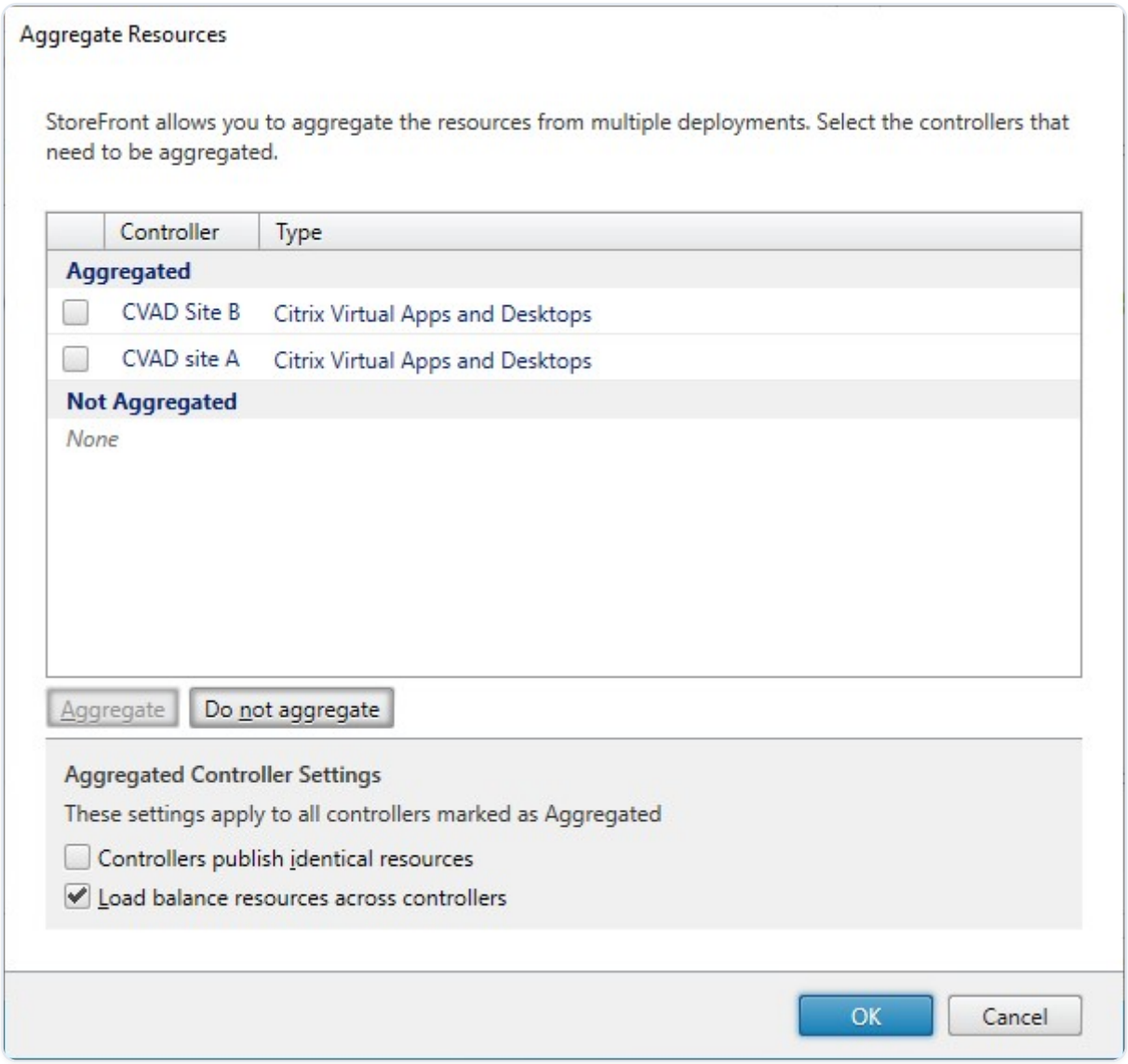
1. Klicken Sie auf dem Bildschirm **Sites verwalten** unter **Benutzerzuordnung und Multi-Site-Aggregationskonfiguration** auf **Konfigurieren**. Diese Option ist nur verfügbar, wenn zwei oder mehr Sites konfiguriert sind.



2. Klicken Sie auf **Ressourcen aggregieren**. Daraufhin wird der Bildschirm **Ressourcen aggregieren** angezeigt.



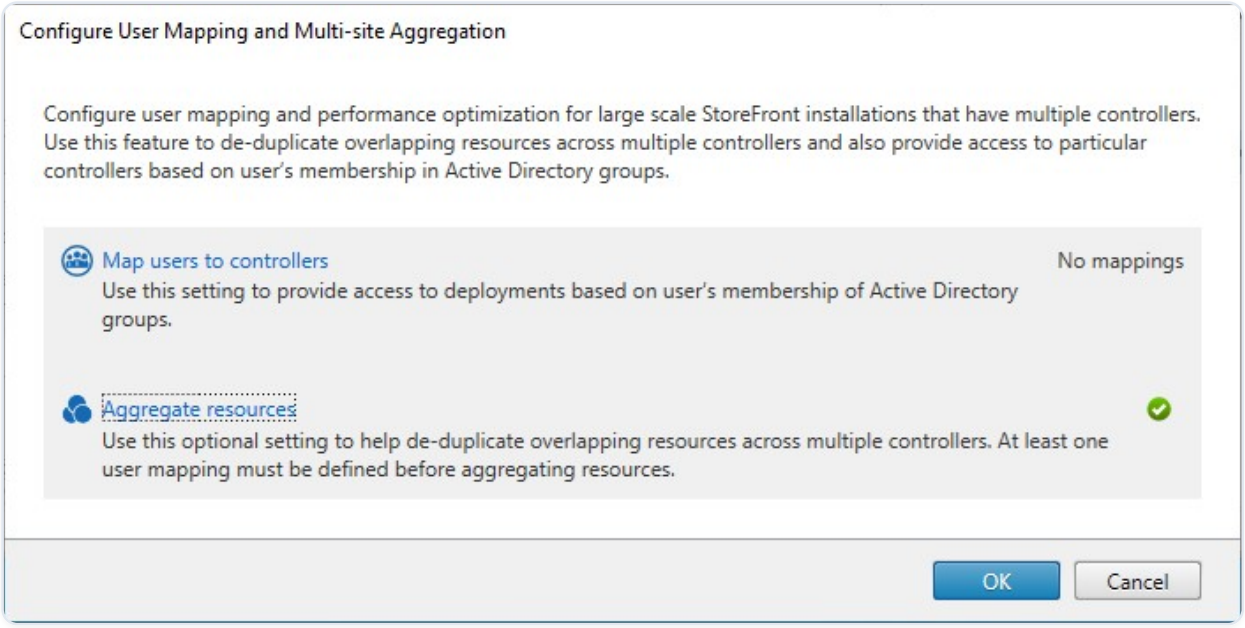
3. Wählen Sie die Sites aus, die dieselben Ressourcen haben, und klicken Sie auf **Aggregieren**.



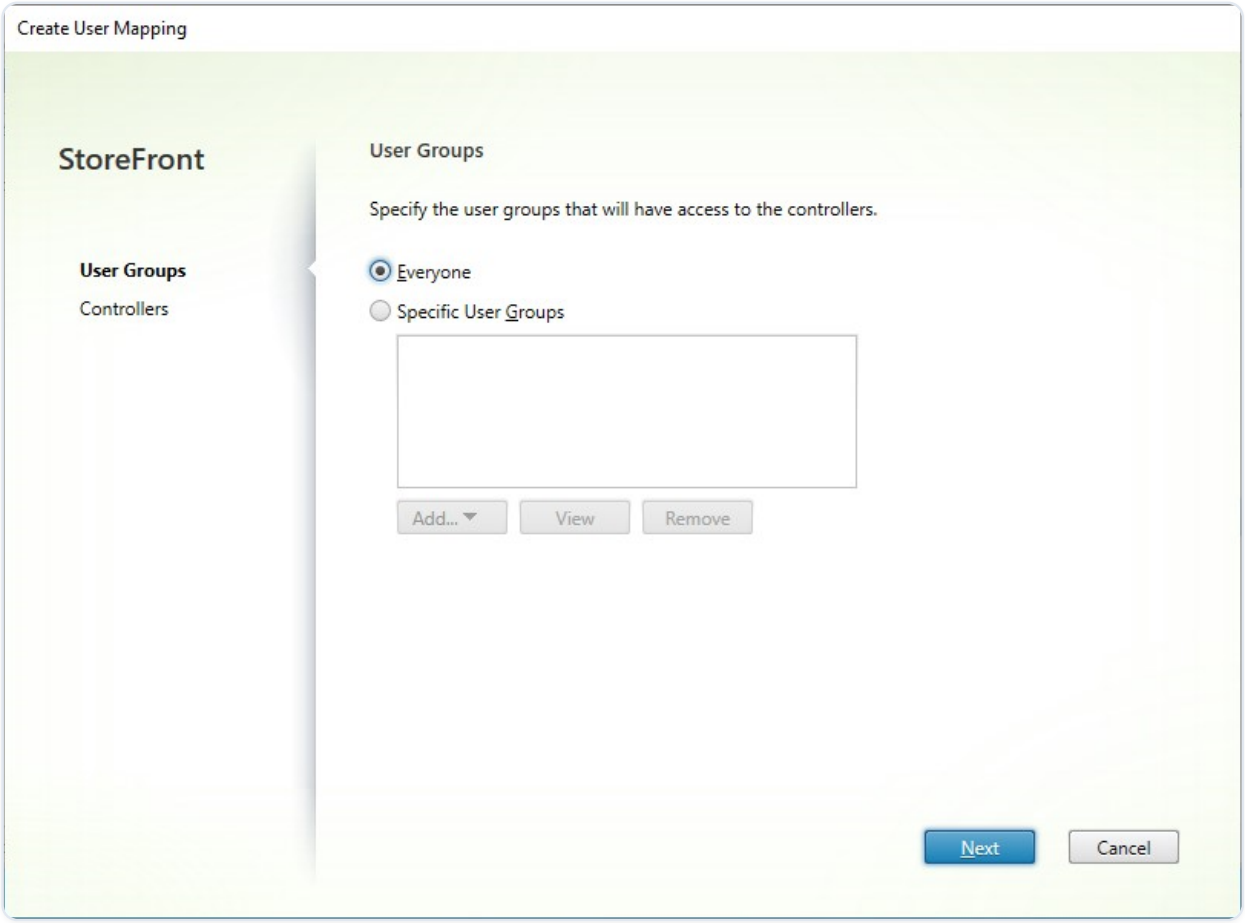
4. Wählen Sie die Optionen unter **Einstellungen für aggregierte Controller** nach Bedarf aus:

   - **Sites veröffentlichen identische Ressourcen** – Wenn diese Option ausgewählt ist, zählt StoreFront Ressourcen nur von einem der Controller im aggregierten Satz auf. Wenn diese Option nicht ausgewählt ist, zählt StoreFront Ressourcen von allen Controllern im aggregierten Satz auf (um den gesamten Satz verfügbarer Ressourcen des Benutzers zu akkumulieren). Die Auswahl dieser Option führt zu einer Leistungsverbesserung bei der Aufzählung von Ressourcen, wir empfehlen sie jedoch nur, wenn Sie sicher sind, dass die Ressourcenliste über alle aggregierten Feeds hinweg identisch ist.
   - **Ressourcen über Controller hinweg lastverteilen** – Wenn diese Option ausgewählt ist, werden Starts gleichmäßig auf die verfügbaren Sites verteilt. Wenn diese Option nicht ausgewählt ist, werden Starts an die erste Site geleitet, die im Dialogfeld für die Benutzerzuordnung angegeben ist, und bei einem Fehler des Starts auf die nachfolgende Site umgeleitet.

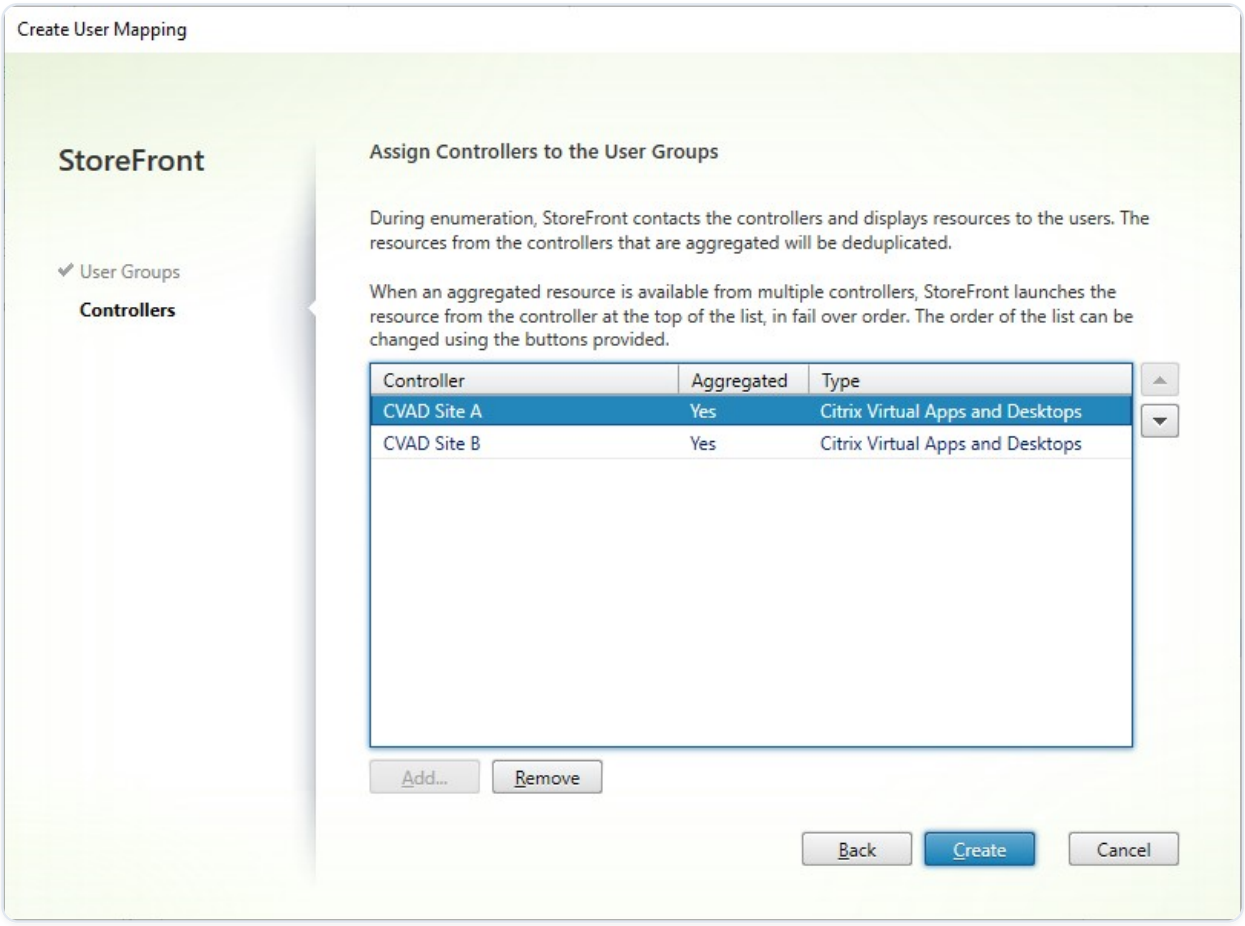
5. Klicken Sie auf **OK**, um zum Bildschirm **Benutzerzuordnung und Multi-Site-Aggregation konfigurieren** zurückzukehren. **Ressourcen aggregieren** ist jetzt aktiviert.



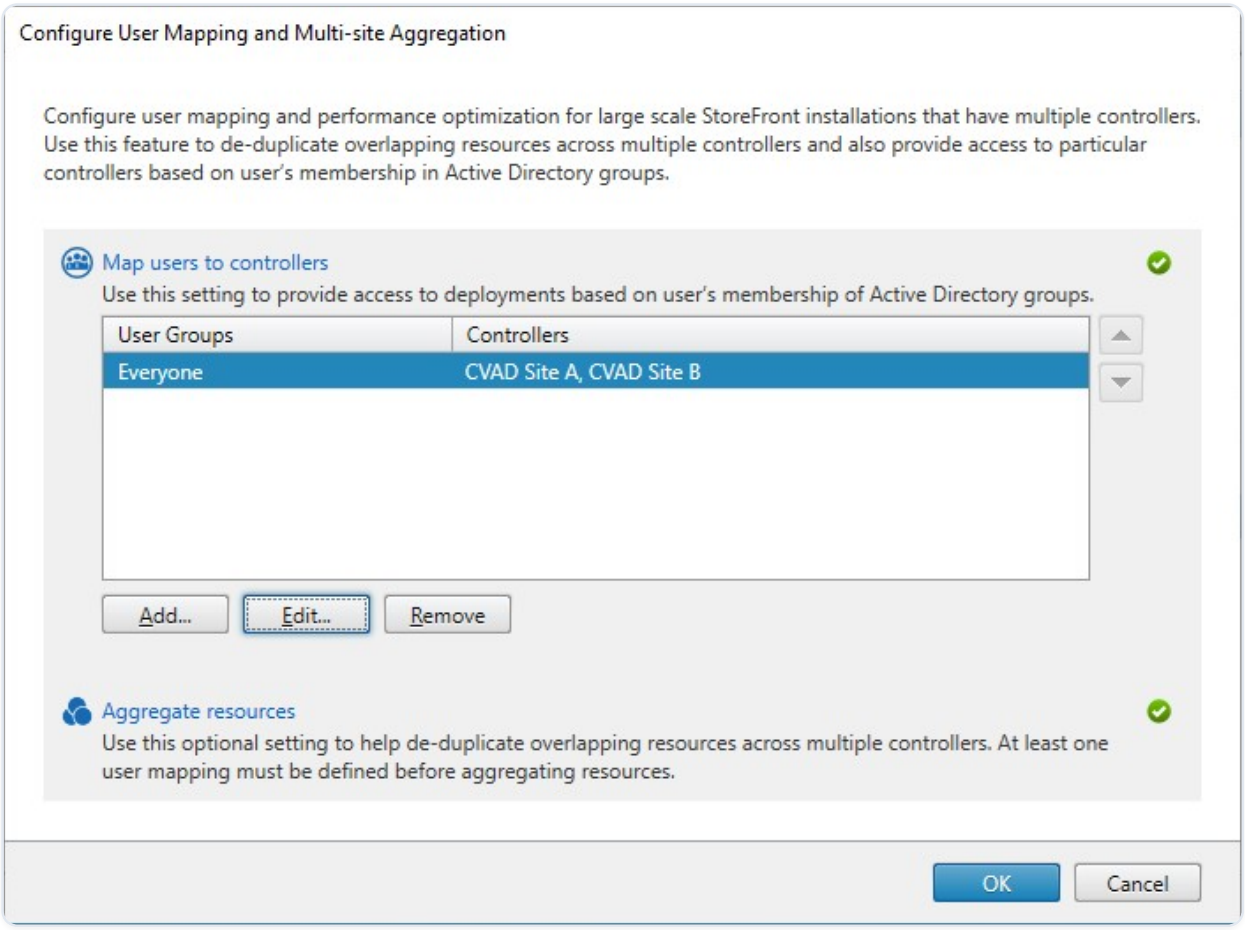
6. Wenn Ressourcen aggregiert werden, haben standardmäßig keine Benutzer Zugriff auf die Ressourcen, daher müssen Sie die Benutzerzuordnungen hinzufügen. Klicken Sie auf **Benutzer Sites zuordnen**. Dadurch wird der Bildschirm **Benutzerzuordnung erstellen** geöffnet.



7. Entweder wählen Sie **Alle** oder **Spezifische Benutzergruppen** und fügen eine oder mehrere Gruppen hinzu. Sie können beispielsweise eine Gruppe auswählen, die Benutzer an einem bestimmten Standort repräsentiert.
8. Fügen Sie die aggregierten Sites hinzu. Sie müssen alle aggregierten Sites hinzufügen; alle nicht enthaltenen Sites werden als „Nicht aggregiert“ behandelt. Sie können auch nicht-aggregierte Ressourcen einschließen.
9. Wenn Sie **Ressourcen über Controller hinweg lastverteilen** nicht aktiviert haben, können Sie die Reihenfolge auswählen, in der StoreFront Ressourcen bevorzugt starten soll.



10. Klicken Sie auf **Erstellen**, um zu **Benutzerzuordnung und Multi-Site-Aggregation konfigurieren** zurückzukehren.



11. Fügen Sie bei Bedarf weitere Zuordnungen hinzu. Stellen Sie sicher, dass jede Site einer Benutzergruppe zugeordnet ist, da diese Ressourcen sonst von niemandem genutzt werden können.
12. Klicken Sie auf **OK**.

Erweiterte Konfigurationen mit PowerShell

Sie können viele gängige Multi-Site- und Hochverfügbarkeitsoperationen mit der StoreFront-Verwaltungskonsole konfigurieren. Sie können StoreFront auch mit PowerShell konfigurieren, was die folgenden zusätzlichen Funktionen bietet:

- Möglichkeit, mehrere Gruppierungen von Bereitstellungen für die Aggregation anzugeben.
  - Die Verwaltungskonsole erlaubt nur eine einzige Gruppierung von Bereitstellungen, was in den meisten Fällen ausreichend ist.
  - Für Stores mit vielen Bereitstellungen und disjunkten Ressourcensätzen könnten mehrere Gruppierungen Leistungsverbesserungen bringen.
- Möglichkeit, komplexe Präferenzreihenfolgen für aggregierte Bereitstellungen anzugeben. Die Verwaltungskonsole ermöglicht es, aggregierte Bereitstellungen lastverteilt zu betreiben oder als einzelne Failover-Liste zu verwenden. Mit PowerShell können Sie mehrere Gruppen von

Feeds haben, die lastverteilt sind und zwischen verschiedenen Gruppen ein Failover durchführen.

Warnung:

Nach der Konfiguration erweiterter Multi-Site-Optionen mit PowerShell ist es nicht möglich, die Optionen über die Verwaltungskonsole zu ändern.

1. Entscheiden Sie, welche Aggregationsgruppen Sie verwenden möchten. Innerhalb einer Aggregationsgruppe werden Anwendungen mit demselben Anzeigenamen zu einem einzigen Symbol aggregiert. Jede Aggregationsgruppe benötigt einen Namen. Mit der Verwaltungskonsole können Sie nur eine Aggregationsgruppe erstellen. Über PowerShell können Sie mehrere Aggregationsgruppen definieren.
2. Für jede Aggregationsgruppe erstellen Sie ein oder mehrere EquivalentFarmset, die die Sites (im SDK als Farms bekannt) auflisten, die Sie aggregieren möchten. Wenn innerhalb der Aggregationsgruppe verschiedene Sites verschiedenen Benutzern zugewiesen werden sollen, müssen Sie für jede Benutzergruppe ein separates EquivalentFarmSet erstellen, das jedoch dasselbe `AggregationGroupName` verwendet. Um das EquivalentFarmSet zu erstellen, rufen Sie New-STFEquivalentFarmset mit den folgenden Parametern auf:
   - `Name` – ein eindeutiger Name für das EquivalentFarmset.
   - `AggregationGroupName` – der Name der Aggregationsgruppe, zu der das Farmset gehört.
   - `LoadBalanceMode` – entweder `LoadBalanced` oder `Failover`.
   - `PrimaryFarms` – Die Farms, die Sie aggregieren möchten. Wenn `LoadBalanceMode` `Failover` ist, stellen Sie sicher, dass die Farms in der erforderlichen Reihenfolge aufgeführt sind. Wenn es mehrere EquivalentFarmSets für eine Aggregationsgruppe gibt, wird diese Reihenfolge mit der im IndexNumber definierten UserFarmMapping kombiniert, wenn bewertet wird, welche Site zum Starten einer Ressource verwendet werden soll.
   - `BackupFarms` – Eine Liste von Farms, die verwendet werden sollen, falls keine der primären Farms verfügbar ist. Diese Funktionalität ist veraltet. Fügen Sie stattdessen zusätzliche EquivalentFarmSets mit einer höheren IndexNumber hinzu.
3. Erstellen Sie für jede Site, die nicht Teil einer Aggregationsgruppe ist, ein EquivalentFarmset, ohne ein `AggregationGroupName` anzugeben. Alle Sites (Farms) müssen Teil eines Farmsets sein. Rufen Sie New-STFEquivalentFarmset mit den folgenden Parametern auf:

- `Name` – ein eindeutiger Name für das EquivalentFarmSet
- `PrimaryFarms` – der Name der nicht aggregierten Farm.

4. Erstellen Sie für jede Benutzergruppe, die Zugriff auf eine andere Gruppe von Sites benötigt, Zuordnungen zwischen diesen Benutzern und jedem der EquivalentFarmSets. Um das UserFarmMapping zu erstellen, rufen Sie Add-STFUserFarmMapping mit den folgenden Parametern auf:

   - `StoreService` – Der Store-Dienst, dem das UserFarmMapping hinzugefügt werden soll.
   - `Name` – Ein eindeutiger Name für die Zuordnung.
   - `GroupMembers` – Eine Hashtabelle, die die Namen und SIDs der Benutzergruppen enthält, 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` – Ein im vorherigen Schritt erstelltes EquivalentFarmSet.
   - `IndexNumber` – Legt die Reihenfolge fest, in der Sites ausgewertet werden. Dies legt die bevorzugte Reihenfolge fest, welche Site zum Starten einer Ressource verwendet werden soll.

   Sie müssen sicherstellen, dass jede Site (Farm) in mindestens einem UserFarmMapping enthalten ist, da sonst keine Benutzer auf diese Ressource zugreifen könnten.

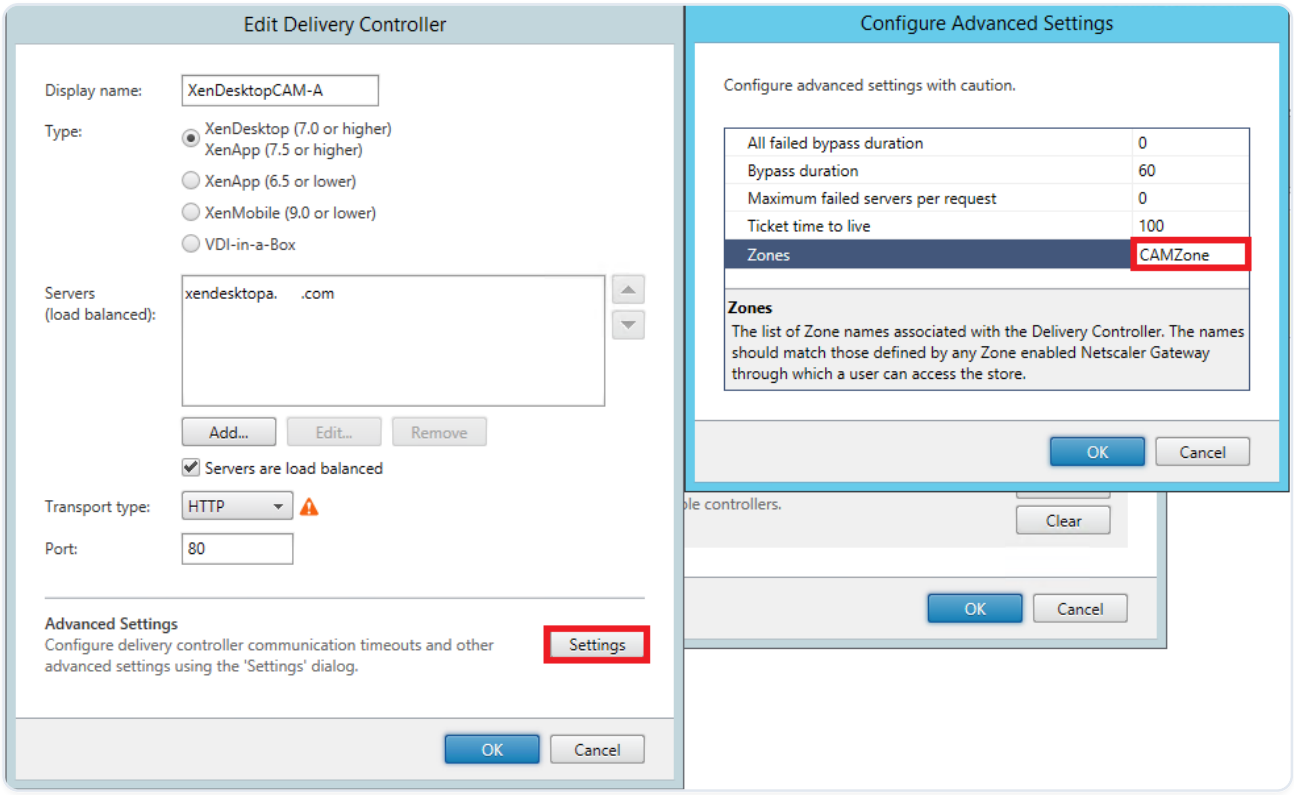
Zonenpräferenz

Wenn Sie mehrere CVAD-Bereitstellungen in verschiedenen Regionen haben, können Sie Ihren NetScaler ADC so konfigurieren, dass StoreFront über die bevorzugten CVAD-Bereitstellungen des Benutzers benachrichtigt wird. Weitere Informationen finden Sie unter Global Server Load Balancing (GSLB) Powered Zone Preference.

Sie müssen StoreFront manuell konfigurieren, um ihm mitzuteilen, welche CVAD-Bereitstellung welche Zonen enthält:

1. Wählen Sie in der Citrix StoreFront-Verwaltungskonsole im linken Bereich den Knoten **Stores** aus.
2. Wählen Sie einen Store im Ergebnisbereich aus.
3. Klicken Sie im Bereich **Aktionen** auf **Sites verwalten**.
4. Wählen Sie eine Site aus, klicken Sie auf **Bearbeiten** und dann auf dem Bildschirm **Site bearbeiten** auf **Einstellungen**.

5. Klicken Sie unter Erweiterte Einstellungen auf **Einstellungen**.
6. Klicken Sie im Dialogfeld Erweiterte Einstellungen konfigurieren in der Zeile **Zonen** in die zweite Spalte.
7. Klicken Sie auf **Hinzufügen...**, geben Sie den Zonennamen ein und drücken Sie die **OK**-Taste. Wiederholen Sie dies für jede Zone in der Bereitstellung.
8. Klicken Sie im Dialogfeld Erweiterte Einstellungen konfigurieren auf **OK**.



Wenn der Benutzer eine aggregierte Ressource startet, durchläuft StoreFront die Liste der Zonen im `X-Citrix-ZonePreference`-Header und sucht nach einer Site, die mit diesem Zonennamen konfiguriert ist. Wenn eine Übereinstimmung gefunden wird, sendet es die Startanforderung an diese CVAD-Bereitstellung. Wenn keine Übereinstimmung gefunden wird, versucht es andere Bereitstellungen.

Wenn die CVAD-Bereitstellung mehrere Zonen enthält, ist es nicht möglich, die Startanforderung an eine bestimmte Zone innerhalb dieser Bereitstellung zu leiten.

Workspace-App-Website festlegen

Wenn Sie einen neuen Store mit StoreFront erstellen, wird automatisch eine Website erstellt und dem Store zugeordnet. Wenn ein Store mehrere Websites hat, wählen Sie aus, welche Website angezeigt wird, wenn Benutzer über die Citrix Workspace-App auf den Store zugreifen.

1. Wählen Sie den **Stores**-Knoten im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus.
2. Wählen Sie einen Store im mittleren Bereich aus, und wählen Sie im Bereich **Aktionen** die Option **Citrix Workspace™-App-Website festlegen**. Wenn Sie keine Website haben, wird eine Meldung mit einem Link zum Assistenten zum Erstellen einer Website angezeigt.
3. Wählen Sie die Website aus, die angezeigt werden soll, wenn Benutzer über die Citrix Workspace-App auf diesen Store zugreifen.
4. Klicken Sie auf **OK**.

Authentifizierung

Authentifizierungsmethoden

Normalerweise authentifizieren sich Benutzer entweder direkt bei StoreFront™ oder bei einem Citrix Gateway vor StoreFront. Je nach Ihren Anforderungen stehen verschiedene Authentifizierungsmethoden zur Verfügung.

METHODE	DETAILS
Active Directory-Benutzername und -Kennwort	Benutzer geben ihren Active Directory-Benutzernamen und ihr Kennwort ein.
Domänen-Pass-Through	Windows-Geräte melden sich per Single Sign-On mit dem Konto an, das sie für die Anmeldung bei Windows verwendet haben.
Smartcard	Benutzer stecken eine Smartcard ein und geben eine PIN ein. Dabei wird das auf der Smartcard gespeicherte Zertifikat zur Authentifizierung des Benutzers verwendet.
SAML	Authentifizierung an Identitätsanbieter von Drittanbietern mithilfe von SAML delegieren.
HTTP Basic	Ermöglicht Drittanbieter-Integrationen, Benutzer mit ihrem Active Directory-Benutzernamen und -Kennwort zu authentifizieren. Siehe die Post Credentials API in der Web-API-Entwicklerdokumentation.

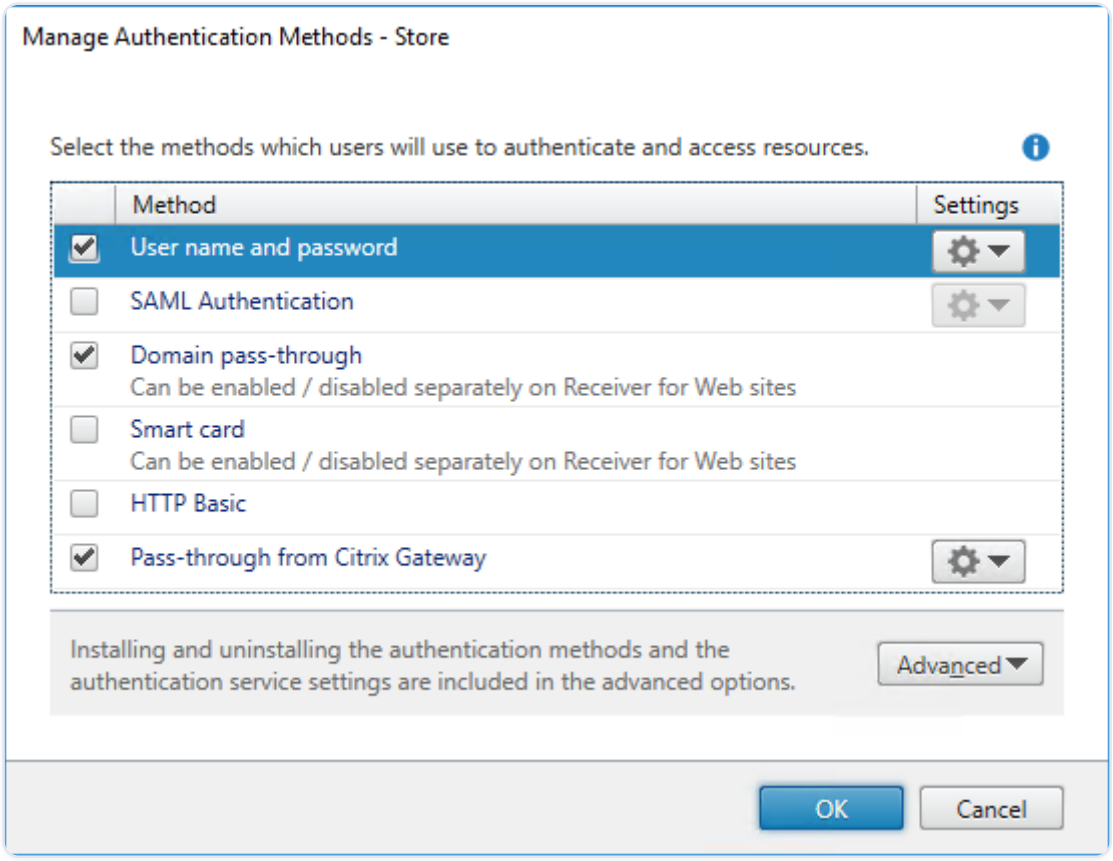
METHODE	DETAILS
	HTTP Basic bietet keine Benutzeroberfläche für die Benutzerauthentifizierung.
Pass-Through von Citrix Gateway	Ermöglicht Benutzern die Authentifizierung an einem Citrix Gateway.

Alternativ können Sie beim Erstellen eines neuen Stores die Authentifizierung deaktivieren und stattdessen anonymen Zugriff auf die Stores zulassen. Siehe Store erstellen.

Authentifizierungsmethoden auswählen

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

1. Wählen Sie den Knoten **Store** im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus und klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
2. Geben Sie die Zugriffsmethoden an, die Sie für Ihre Benutzer aktivieren möchten.



Das Ändern der Authentifizierungsmethoden für einen Store aktualisiert auch die Authentifizierungsmethoden, die beim Zugriff auf den Store über einen Webbrowser verwendet

werden. Informationen zum Ändern der Authentifizierungsmethoden bei der Anmeldung über einen Webbrowser finden Sie unter Authentifizierungsmethoden.

Authentifizierungsmethoden mit PowerShell auswählen

So konfigurieren Sie die Authentifizierung mit PowerShell:

1. Rufen Sie Get-STFAuthenticationService auf, um den Authentifizierungsdienst für einen Store oder ein virtuelles Verzeichnis abzurufen und dessen aktuelle Konfiguration anzuzeigen.
2. Aktivieren oder deaktivieren Sie auf dem Authentifizierungsdienst die erforderlichen Authentifizierungsprotokolle. Um eine Liste der verfügbaren Protokolle zu erhalten, führen Sie Get-STFAuthenticationServiceProtocol aus. 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.

Einstellungen für Authentifizierungsmethoden

Einige Authentifizierungsmethoden verfügen über zusätzliche Einstellungen. Wählen Sie die Dropdown-Liste **Einstellungen** aus, um die verfügbaren Optionen anzuzeigen. Weitere Informationen finden Sie auf der Seite für die jeweilige Authentifizierungsmethode.

Einstellungen für den gemeinsamen Authentifizierungsdienst

Sie können einen Store so konfigurieren, dass er den Authentifizierungsdienst eines anderen Stores gemeinsam nutzt, wodurch Single Sign-On zwischen ihnen ermöglicht wird.

1. Öffnen Sie **Authentifizierungsmethoden verwalten**.
2. Wählen Sie im Dropdown-Menü **Erweitert** die Option **Einstellungen für den gemeinsamen Authentifizierungsdienst**.
3. Aktivieren Sie das Kontrollkästchen **Gemeinsamen Authentifizierungsdienst verwenden** und wählen Sie einen Store aus dem Dropdown-Menü **Storename** aus.

> **Hinweis:**
>
> Es gibt keinen funktionalen Unterschied zwischen einem gemeinsamen und einem dedizierten Authentifizierungsdienst. Ein Authentifizierungsdienst, der von mehr als zwei Stores gemeinsam genutzt wird, wird als gemeinsamer Authentifizierungsdienst behandelt,

> und alle Konfigurationsänderungen wirken sich auf den Zugriff auf alle Stores aus, die den gemeinsamen Authentifizierungsdienst verwenden.

Authentifizierungsmethoden installieren oder deinstallieren

Sie können vorhandene Methoden anpassen oder eigene Authentifizierungsmethoden mit dem Authentication SDK erstellen.

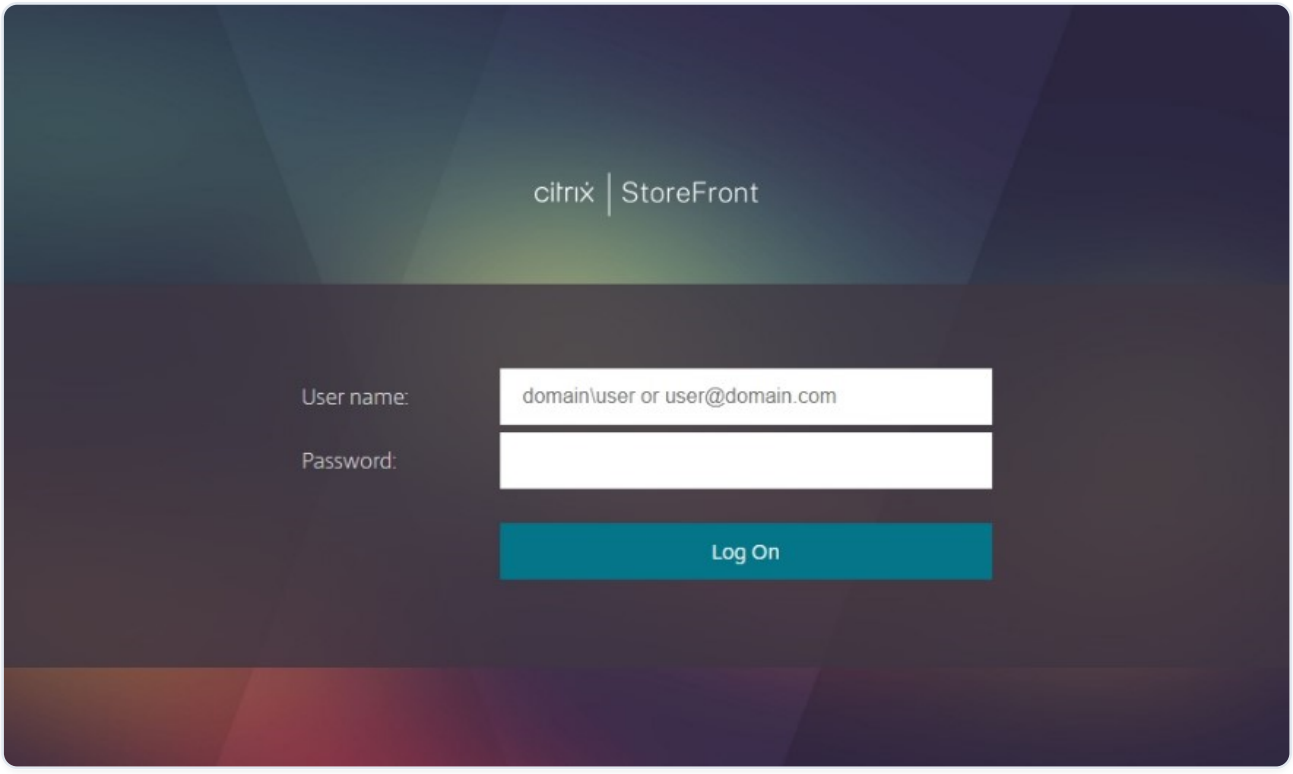
Wenn Sie eine neue benutzerdefinierte Authentifizierungsmethode auf dem Server installiert haben, müssen Sie diese auch für jeden vorhandenen Store installieren, in dem Sie sie verwenden möchten. Wählen Sie auf dem Bildschirm **Authentifizierungsmethoden verwalten** die Option **Erweitert** und dann **Authentifizierungsmethoden installieren oder deinstallieren**.

Single Sign-On bei VDAs

Einige Authentifizierungsmethoden bieten die Möglichkeit zum SSO bei VDAs; weitere Details finden Sie bei der jeweiligen Authentifizierungsmethode. Andernfalls kann Single Sign-On mit dem Federated Authentication Service erreicht werden.

Active Directory-Benutzername- und -Kennwortauthentifizierung

Benutzer werden aufgefordert, ihren Active Directory-Benutzernamen und ihr Kennwort einzugeben.



.

Wenn das Kennwort des Benutzers abgelaufen ist oder bald abläuft, kann der Benutzer je nach Konfiguration die Option erhalten, sein Kennwort zu ändern.

Um die Benutzername- und Kennwortauthentifizierung für einen Store bei Verwendung der Citrix Workspace-App zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie im Fenster Authentifizierungsmethoden die Option **Active Directory-Benutzername und -Kennwort**.

Das Aktivieren der Benutzername- und Kennwortauthentifizierung für einen Store aktiviert diese standardmäßig auch für alle Websites dieses Stores für Benutzer, die einen Webbrowser verwenden. Sie können die Benutzername- und Kennwortauthentifizierung für eine bestimmte Website auf der Registerkarte Authentifizierungsmethoden für Websites verwalten deaktivieren.

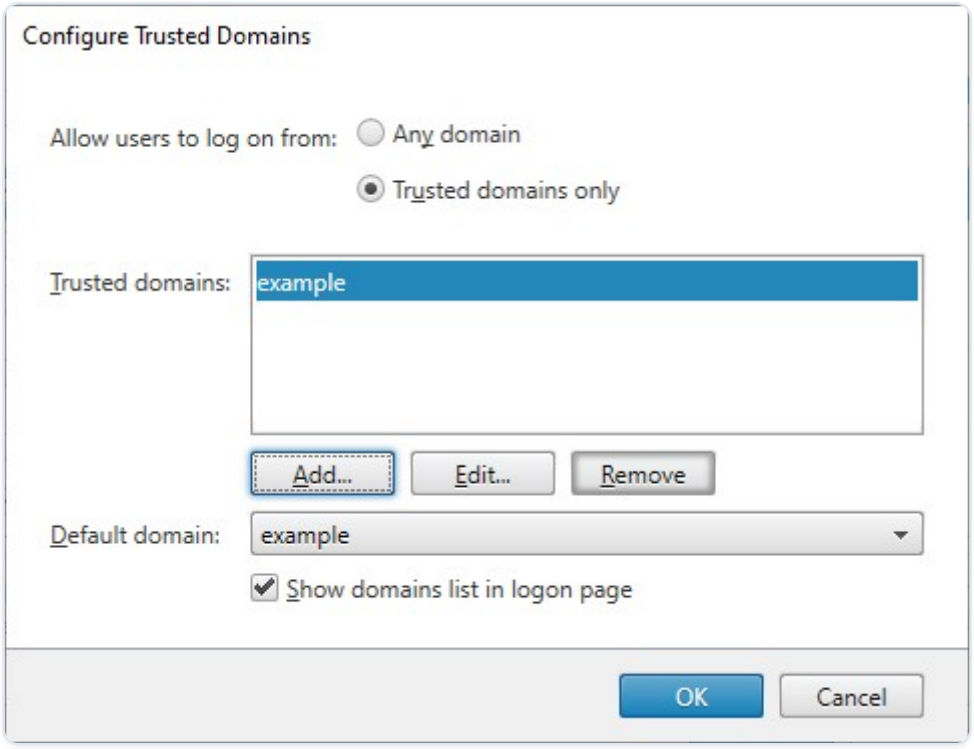
Vertrauenswürdige Benutzerdomänen konfigurieren

Sie können den Zugriff auf Stores für Benutzer einschränken, die sich mit expliziten Domänenanmeldeinformationen anmelden, entweder direkt oder über Pass-Through-Authentifizierung von Citrix Gateway.

1. Wählen Sie den Knoten Stores im linken Bereich der Citrix StoreFront-Verwaltungskonsole und im Ergebnisbereich die entsprechende Authentifizierungsmethode aus. Klicken Sie im Aktionsbereich auf **Authentifizierungsmethoden verwalten**.
2. Wählen Sie in der Liste **Benutzername und Kennwort > Einstellungen** die Option **Vertrauenswürdige Domänen konfigurieren**.
3. Wählen Sie **Nur vertrauenswürdige Domänen** und klicken Sie auf **Hinzufügen**, um den Namen einer vertrauenswürdigen Domäne einzugeben. Benutzer mit Konten in dieser Domäne können sich bei allen Stores anmelden, die den Authentifizierungsdienst verwenden. Um einen Domänennamen zu ändern, wählen Sie den Eintrag in der Liste der vertrauenswürdigen Domänen aus und klicken Sie auf **Bearbeiten**. Um den Zugriff auf Stores für Benutzerkonten in einer Domäne zu unterbinden, wählen Sie die Domäne in der Liste aus und klicken Sie auf **Entfernen**.

   Die Art und Weise, wie Sie den Domänennamen angeben, bestimmt das Format, in dem Benutzer ihre Anmeldeinformationen eingeben müssen. Wenn Benutzer ihre Anmeldeinformationen im Format Domänenbenutzername eingeben sollen, fügen Sie den NetBIOS-Namen zur Liste hinzu. Um zu verlangen, dass Benutzer ihre Anmeldeinformationen im Format Benutzerprinzipalname eingeben, fügen Sie den vollqualifizierten Domänennamen zur Liste hinzu. Wenn Sie Benutzern ermöglichen möchten, ihre Anmeldeinformationen sowohl im Format Domänenbenutzername als auch im Format Benutzerprinzipalname einzugeben, müssen Sie sowohl den NetBIOS-Namen als auch den vollqualifizierten Domänennamen zur Liste hinzufügen.

4. Wenn Sie mehrere vertrauenswürdige Domänen konfigurieren, wählen Sie aus der Liste Standarddomäne die Domäne aus, die standardmäßig ausgewählt wird, wenn sich Benutzer anmelden.
5. Wenn Sie die vertrauenswürdigen Domänen auf der Anmeldeseite auflisten möchten, aktivieren Sie das Kontrollkästchen Domänenliste auf der Anmeldeseite anzeigen.



PowerShell

Um die Liste der konfigurierten Domänen abzurufen, verwenden Sie das Cmdlet `Get-STFExplicitCommonOptions`.

Um die vertrauenswürdigen Domänen zu aktualisieren, verwenden Sie das Cmdlet `Set-STFExplicitCommonOptions`.

Benutzern das Ändern ihrer Kennwörter ermöglichen

Sie können Benutzern jederzeit erlauben, ihre Kennwörter zu ändern. Alternativ können Sie Kennwortänderungen auf Benutzer beschränken, deren Kennwörter abgelaufen sind. Dies bedeutet, dass Sie sicherstellen können, dass Benutzer niemals durch ein abgelaufenes Kennwort am Zugriff auf ihre Desktops und Anwendungen gehindert werden.

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

CITRIX WORKSPACE-APPS	BENUTZER KANN EIN ABGELAUFENES KENNWORT ÄNDERN, WENN IN STOREFRONT AKTIVIERT	BENUTZER WIRD BENACHRICHTIGT, DASS DAS KENNWORT ABLÄUFT	BENUTZER KANN DAS KENNWORT ÄNDERN, BEVOR ES ABLÄUFT, WENN IN STOREFRONT AKTIVIERT
Windows	Ja		
Mac	Ja		
Android			
iOS			
Linux	Ja		
Web	Ja	Ja	Ja

Die Standardkonfiguration verhindert, dass Benutzer von Citrix Workspace-Apps und Webbrowsern ihre Kennwörter ändern können, selbst wenn die Kennwörter abgelaufen sind. Wenn Sie diese Funktion aktivieren möchten, stellen Sie sicher, dass die Richtlinien für die Domänen, die Ihre Server enthalten, Benutzer nicht daran hindern, ihre Kennwörter zu ändern. Wenn Sie Benutzern das Ändern ihrer Kennwörter ermöglichen, werden sensible Sicherheitsfunktionen für jeden zugänglich, der auf einen der Stores zugreifen kann, die den Authentifizierungsdienst verwenden. Wenn Ihre Organisation eine Sicherheitsrichtlinie hat, die Kennwortänderungsfunktionen für Benutzer nur für die interne Verwendung vorsieht, stellen Sie sicher, dass keiner der Stores von außerhalb Ihres Unternehmensnetzwerks zugänglich ist.

Wenn Sie Benutzern jederzeit erlauben, ihre Kennwörter zu ändern, wird lokalen Benutzern, deren Kennwörter bald ablaufen, beim Anmelden eine Warnung angezeigt. Standardmäßig wird der Benachrichtigungszeitraum für einen Benutzer durch die entsprechende Windows-Richtlinieneinstellung bestimmt. Alternativ können Sie einen benutzerdefinierten Benachrichtigungszeitraum konfigurieren.

1. Wählen Sie im Fenster **Authentifizierungsmethoden verwalten** im Dropdown-Menü **Active Directory-Benutzername und -Kennwort** > **Einstellungen** die Option **Kennwortoptionen verwalten**.
2. Um Benutzern das Ändern von Kennwörtern zu ermöglichen, aktivieren Sie das Kontrollkästchen **Benutzern das Ändern von Kennwörtern erlauben**.

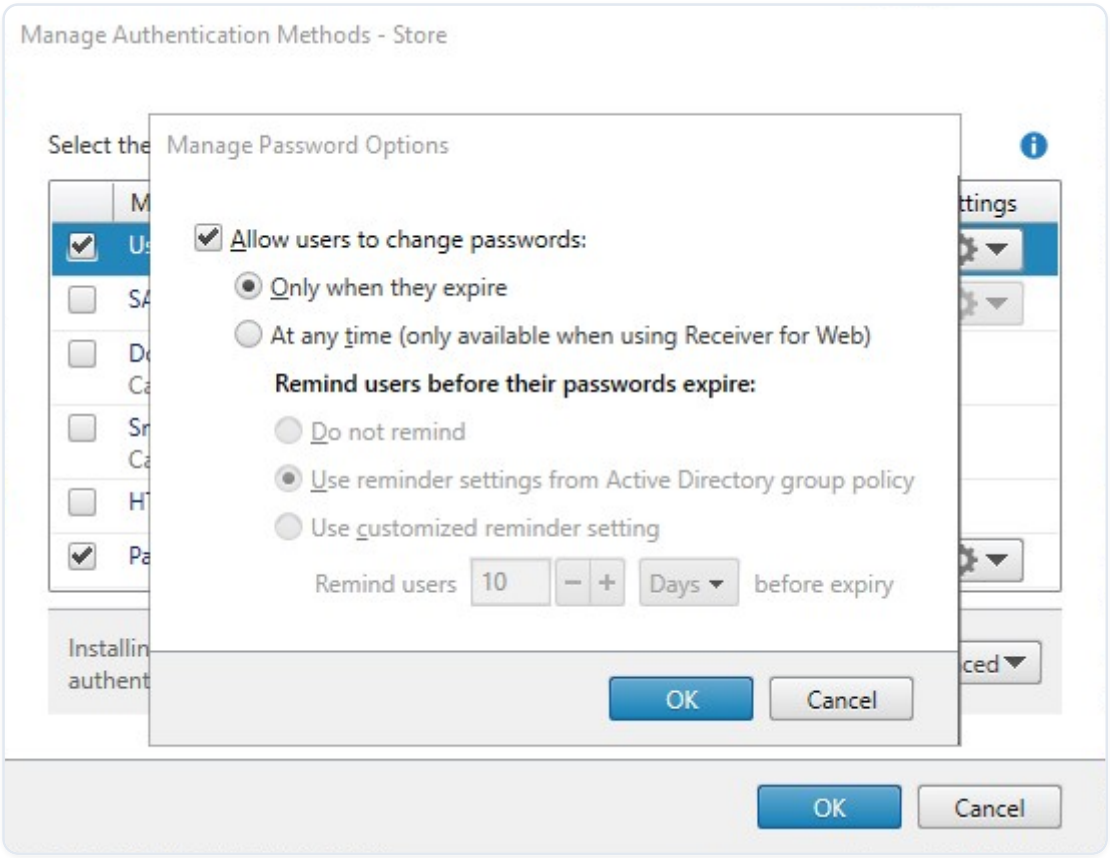
> **Hinweis:**
>
> Wenn Sie diese Option nicht auswählen, müssen Sie selbst Vorkehrungen treffen, um Benutzer zu unterstützen, die aufgrund abgelaufener Kennwörter nicht auf ihre Desktops und Anwendungen zugreifen können.

3. Wählen Sie, ob Benutzer Kennwörter **Nur wenn sie ablaufen** oder **Jederzeit** ändern dürfen.
4. Wählen Sie, ob Benutzer vor Ablauf ihrer Kennwörter erinnert werden sollen. Sie können aus den folgenden Optionen wählen:

   - **Nicht erinnern** – Die Benutzeroberfläche zeigt keine Erinnerungen an den Kennwortablauf an. Sie benachrichtigt Benutzer erst, wenn das Kennwort abgelaufen ist.
   - **Erinnerungseinstellungen aus der Active Directory-Gruppenrichtlinie verwenden** – Nach der Anmeldung benachrichtigt die Benutzeroberfläche den Benutzer, wenn sein Kennwort innerhalb der in der Gruppenrichtlinie konfigurierten Anzahl von Tagen abläuft. Der Benutzer erhält die Option, sein Kennwort zu ändern.

     > **Hinweis:**
     >
     > StoreFront berücksichtigt keine fein abgestuften Kennwortrichtlinien. Wenn Sie also fein abgestufte Kennwortrichtlinien verwenden, sollten Sie diese Option nicht auswählen.

   - **Benutzerdefinierte Erinnerungseinstellung verwenden** – Nach der Anmeldung benachrichtigt die Benutzeroberfläche den Benutzer, wenn sein Kennwort innerhalb der angegebenen Anzahl von Tagen abläuft. Der Benutzer erhält die Option, sein Kennwort zu ändern.



Hinweise

Hinweis 1:

Stellen Sie sicher, dass auf Ihren StoreFront-Servern ausreichend Speicherplatz vorhanden ist, um Profile für alle Ihre Benutzer zu speichern. Um zu überprüfen, ob das Kennwort eines Benutzers bald abläuft, erstellt StoreFront ein lokales Profil für diesen Benutzer auf dem Server. StoreFront muss in der Lage sein, den Domänencontroller zu kontaktieren, um die Kennwörter der Benutzer zu ändern.

Hinweis 2:

Wenn Sie die Sicherheitsrichtlinie **Netzwerkzugriff: Clients einschränken, die Remoteaufrufe an SAM tätigen dürfen** aktivieren, müssen Sie alle Benutzer einschließen, die ihre Kennwörter ändern müssen.

Hinweis 3:

> Wenn Sie die Kennwortänderung jederzeit aktivieren oder deaktivieren, wirkt sich dies auch auf die Einstellungen unter **Optionen zur Kennwortverwaltung** für die Pass-Through-Authentifizierung von Citrix Gateway aus.

PowerShell

Um die Liste der vertrauenswürdigen Domänen abzurufen, verwenden Sie das Cmdlet `Get-STFExplicitCommonOptions`.

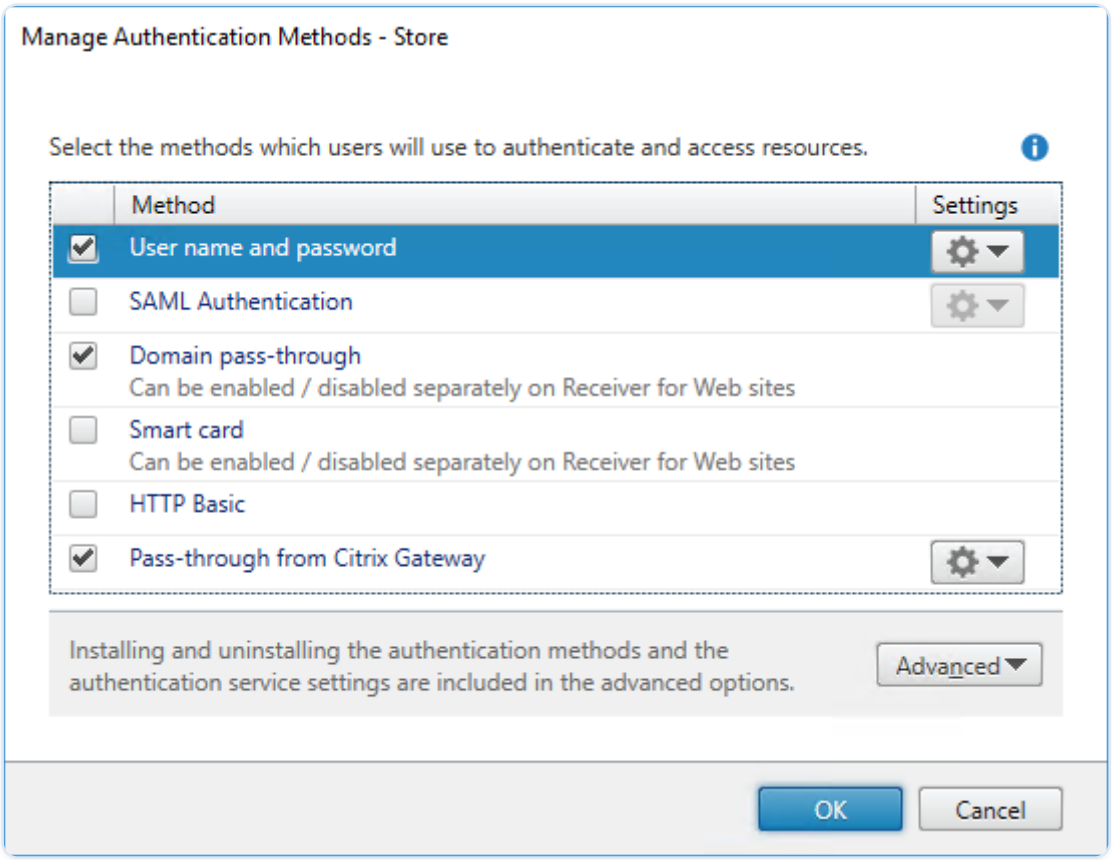
Um die vertrauenswürdigen Domänen zu aktualisieren, verwenden Sie das Cmdlet `Set-STFExplicitCommonOptions`.

Kennwortvalidierung

Normalerweise fordert StoreFront Windows auf, die Anmeldeinformationen in Active Directory zu validieren. Dies erfordert, dass sich der Windows-Server in derselben Domäne wie der Benutzer befindet oder dass eine Vertrauensstellung zwischen den beiden Domänen besteht. Wenn es nicht möglich ist, Active Directory-Vertrauensstellungen einzurichten, können Sie StoreFront so konfigurieren, dass die Citrix Virtual Apps and Desktops Delivery Controller zur Authentifizierung der Anmeldeinformationen verwendet werden. Dies betrifft auch die HTTP Basic- und Gateway-Pass-Through-Authentifizierung.

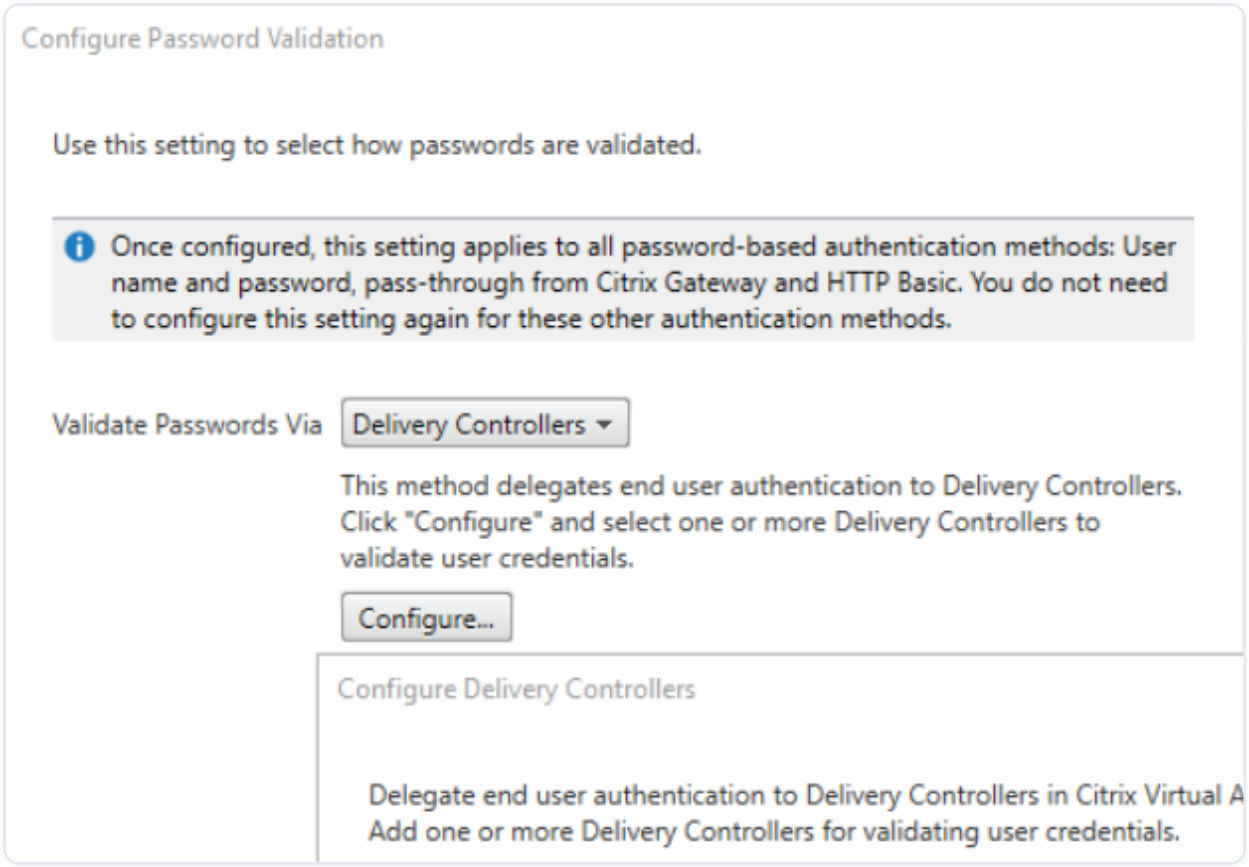
So konfigurieren Sie, wie StoreFront Kennwörter validiert:

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

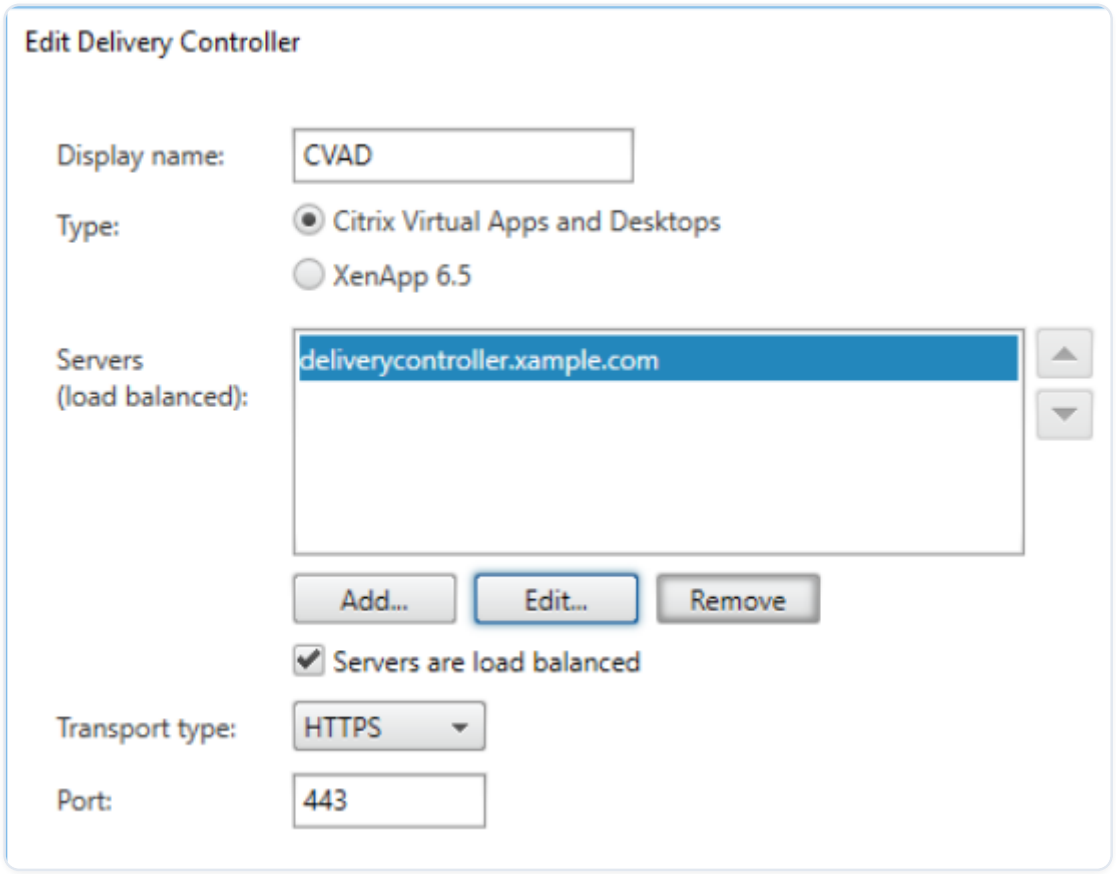


2. Wählen Sie im Dropdown-Menü **Kennwort validieren über** Folgendes aus:

   - **Active Directory** – Fordert Windows auf, Anmeldeinformationen in Active Directory zu validieren
   - **Delivery Controller** – Fordert den konfigurierten Delivery Controller™ auf, Anmeldeinformationen zu validieren.



3. Wenn Sie **Delivery Controller** ausgewählt haben, wählen Sie **Konfigurieren**. Fügen Sie in den Bildschirmen **Delivery Controller konfigurieren** einen oder mehrere **Delivery Controller** zur Validierung der Benutzeranmeldeinformationen hinzu und klicken Sie auf **OK**.



4. Wählen Sie **OK**.

PowerShell

Um zu erfahren, wie Kennwörter validiert werden, verwenden Sie das Cmdlet `Get-STFExplicitAuthenticator`.

Um die Kennwortvalidierung über Delivery Controller durchzuführen, verwenden Sie das Cmdlet `Set-STFExplicitAuthenticator`, um den Validator auf `xmlServiceAuthenticator` festzulegen. Um festzulegen, welcher Delivery Controller zur Authentifizierung von Anmeldeinformationen verwendet werden soll, verwenden Sie das Cmdlet Enable-STFXmlServiceAuthentication

Single Sign-On bei VDAs

Wenn Benutzer eine Ressource starten, leitet StoreFront die Anmeldeinformationen, die der Benutzer zum Anmelden am Store verwendet hat, für das Single Sign-On an die VDAs weiter.

Wenn Federated Authentication Service (FAS) für den Store aktiviert ist, kontaktiert StoreFront einen FAS-Server, um ein Zertifikat für das Single Sign-On am Store bereitzustellen. Dieses Zertifikat wird anstelle der Anmeldeinformationen an den VDA weitergeleitet. Wenn StoreFront keinen FAS-Server kontaktieren kann, gibt es kein Single Sign-On am VDA.

Anmeldebildschirm anpassen

Der Anmeldebildschirm wird aus einer Vorlage generiert, die sich typischerweise unter `C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\Templates\UsernamePassword.tfrm` befindet. Die Vorlage wird mit Forms Template Language definiert.

Die folgenden Beispiele fügen einen Titel hinzu und verhindern, dass die Citrix Workspace-App für Windows Passwörter zwischenspeichert:

Titeltext

Wenn sich Benutzer bei einem Store anmelden, wird standardmäßig kein Titeltext im Anmeldedialogfeld angezeigt. Sie können den Text „Bitte melden Sie sich an“ anzeigen oder Ihre eigene benutzerdefinierte Nachricht verfassen:

1. Öffnen Sie die Datei `UsernamePassword.tfrm` für den Authentifizierungsdienst mit einem Texteditor.
2. Suchen Sie die folgenden Zeilen in der Datei.

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
```

3. Heben Sie die Auskommentierung der Anweisung auf, indem Sie das führende `@*` und das nachfolgende `*@` entfernen.

   ```
   @Heading("ExplicitAuth:AuthenticateHeadingText")
   ```

   Benutzer der Citrix Workspace-App sehen den Standardtiteltext „Bitte melden Sie sich an“ oder die entsprechende lokalisierte Version dieses Textes, wenn sie sich bei Stores anmelden, die diesen Authentifizierungsdienst verwenden.

4. Um den Titeltext zu ändern, öffnen Sie die Datei `ExplicitFormsCommon.xx.resx` für den Authentifizierungsdienst mit einem Texteditor. Diese befindet sich typischerweise im Verzeichnis `C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\resources\`.

5. Suchen Sie die folgenden Elemente in der Datei. Bearbeiten Sie den Text, der im Element `<value>` enthalten ist, um den Titeltext zu ändern, den Benutzer im Anmeldedialogfeld sehen, wenn sie auf Stores zugreifen, die diesen Authentifizierungsdienst verwenden.

   ```
   <data name="AuthenticateHeadingText" xml:space="preserve">

       <value>My Company Name</value>

   </data>
   ```

   Um den Titeltext des Anmeldedialogfelds für Benutzer in anderen Gebietsschemas zu ändern, bearbeiten Sie die lokalisierten Dateien *ExplicitAuth.languagecode.resx*, wobei **languagecode** der Gebietsschema-Bezeichner ist.

Verhindern, dass die Citrix Workspace-App für Windows Passwörter und Benutzernamen zwischenspeichert

Standardmäßig speichert die Citrix Workspace-App für Windows die Passwörter der Benutzer, wenn diese sich bei StoreFront-Stores anmelden. Um zu verhindern, dass die Citrix Workspace-App für Windows die Passwörter der Benutzer zwischenspeichert, bearbeiten Sie die Dateien für den Authentifizierungsdienst.

1. Öffnen Sie die Datei inetpub\wwwroot\Citrix\\Auth\App_Data\Templates\UsernamePassword.tfrm mit einem Texteditor.
2. Suchen Sie die folgende Zeile in der Datei.

```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
"ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
ControlValue("SaveCredentials"))
```

3. Kommentieren Sie die Anweisung wie unten gezeigt.

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

Benutzer müssen ihre Kennwörter jedes Mal eingeben, wenn sie sich bei Stores anmelden, die diesen Authentifizierungsdienst verwenden.

Standardmäßig füllt die Citrix Workspace-App für Windows den zuletzt eingegebenen Benutzernamen automatisch aus. Um das Ausfüllen des Benutzernamenfelds zu unterdrücken oder für einen alternativen Mechanismus zum Unterdrücken des Zwischenspeicherns von Kennwörtern, siehe Verhindern, dass die Citrix Workspace-App für Windows Kennwörter und Benutzernamen zwischenspeichert.

Remotezugriff über Citrix Gateway

Sie können Ihr Citrix Gateway so konfigurieren, dass sich Benutzer mit ihrem Domänenbenutzernamen und Kennwort und optional einem zweiten Faktor beim Gateway anmelden. Diese Anmeldeinformationen werden an StoreFront weitergeleitet, um sich beim Store anzumelden. Um Ihr Citrix Gateway für die LDAP-Benutzernamen- und Kennwortauthentifizierung zu konfigurieren, siehe NetScaler-Dokumentation – LDAP-Authentifizierung. Um StoreFront zu konfigurieren, siehe Pass-Through von Citrix Gateway.

SAML-Authentifizierung

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

Hinweis

Konfigurieren Sie StoreFront mit SAML-Authentifizierung für den internen Zugriff. Für den externen Zugriff konfigurieren Sie Citrix Gateway mit SAML-Authentifizierung und konfigurieren Sie dann StoreFront mit Gateway-Pass-Through-Authentifizierung.

> StoreFront erfordert einen SAML 2.0-kompatiblen Identitätsanbieter (IdP) wie zum Beispiel:

- Microsoft AD Federation Services unter Verwendung von SAML-Bindungen (nicht WS-Federation-Bindungen). Weitere Informationen finden Sie unter CTX220638.
- Citrix Gateway (als IdP konfiguriert).
- Microsoft Entra ID. Weitere Informationen finden Sie unter CTX237490.

Die SAML-Assertion muss ein `<saml:NameID>`-Element enthalten, das mit dem User Principal Name (UPN) des Benutzers gefüllt ist. StoreFront sucht diesen UPN in Active Directory. StoreFront unterstützt keine Benutzer in anderen Verzeichnissen. Bei Verwendung von Entra ID muss der Benutzer eine Hybrididentität besitzen.

Um die SAML-Authentifizierung für einen Store zu aktivieren oder zu deaktivieren, wählen Sie im Fenster Authentifizierungsmethoden die Option **SAML-Authentifizierung**. Die Aktivierung der SAML-Authentifizierung für einen Store aktiviert diese standardmäßig für alle Websites dieses Stores. Sie können die SAML-Authentifizierung für jede Website auf der Registerkarte Authentifizierungsmethoden unabhängig voneinander deaktivieren oder aktivieren.

StoreFront™ SAML-Endpunkte

Um SAML zu konfigurieren, benötigt Ihr Identitätsanbieter möglicherweise die folgenden Endpunkte:

- Die URL der Entitäts-ID. Dies ist der Pfad zum Authentifizierungsdienst des Stores, normalerweise `https://[storefront host]/Citrix/[StoreName]Auth`
- Die URL des Assertion Consumer Service, normalerweise `https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/AssertionConsumerService`
- Der Metadatendienst, normalerweise `https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/ServiceProvider/Metadata`

Zusätzlich gibt es einen Test-Endpunkt, normalerweise `https://[storefront host]/Citrix/[StoreName]Auth/SamlTest`

Sie können das folgende PowerShell-Skript verwenden, um die Endpunkte für einen bestimmten 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"
```

Beispiel der 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
```

Konfigurieren über Metadatenaustausch

Zur Vereinfachung der Konfiguration können Sie Metadaten (Bezeichner, Zertifikate, Endpunkte und andere Konfigurationen) zwischen dem Identitätsanbieter und dem Dienstanbieter austauschen, der in diesem Fall StoreFront ist.

Wenn Ihr Identitätsanbieter den Metadatenimport unterstützt, können Sie ihn auf 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, zum 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



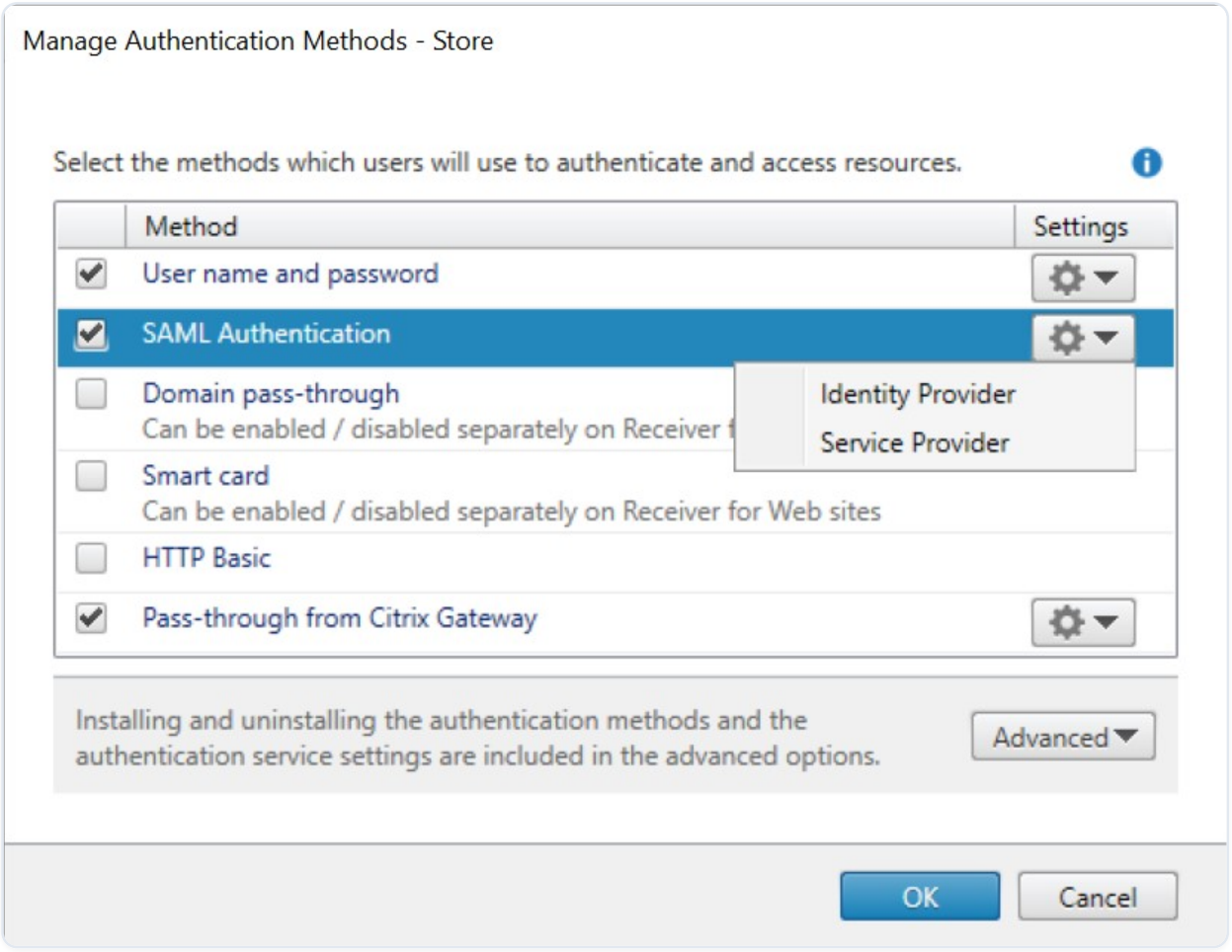
# If the metadata has already been download, use the following:
```

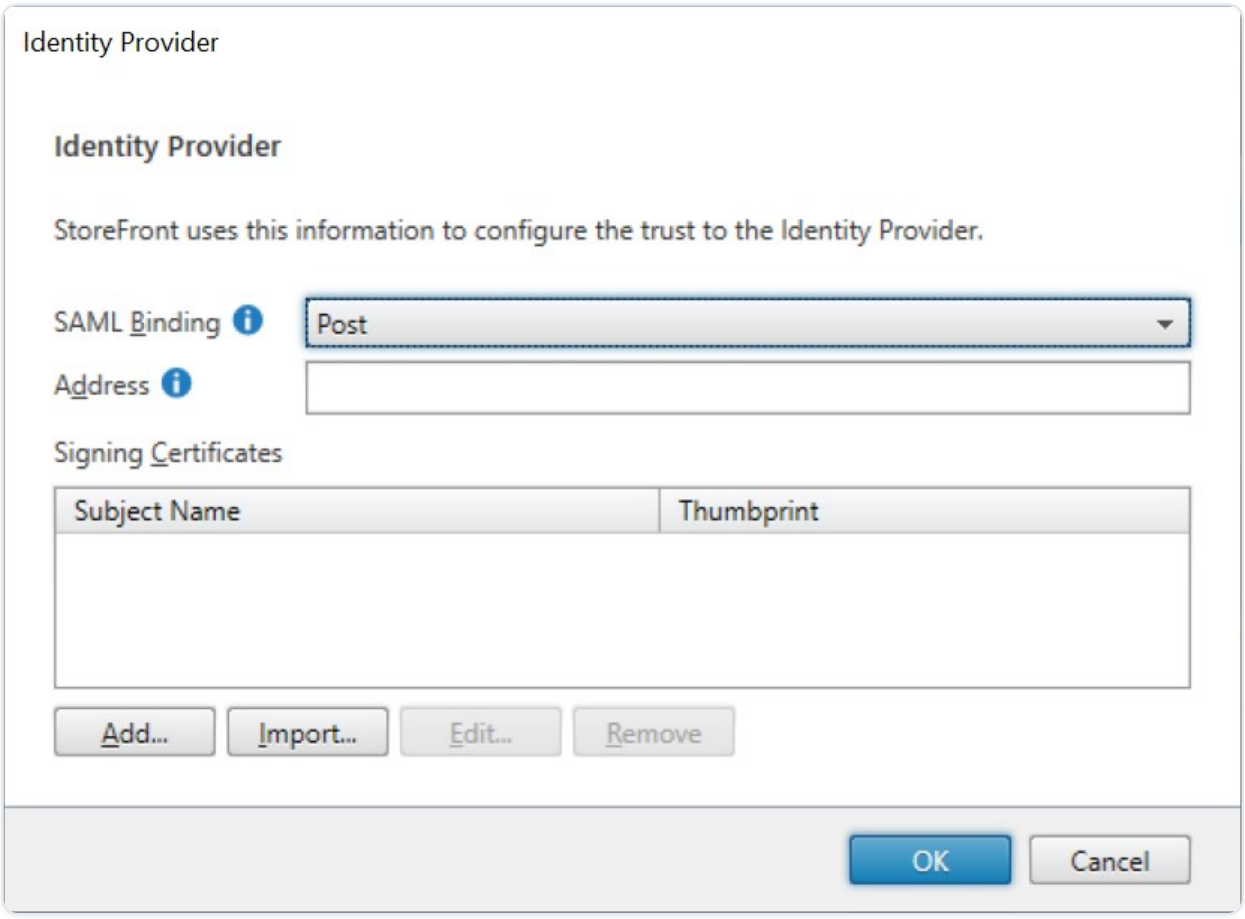
```
# Note: Ensure that the file is encoded as UTF-8

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:
\Users\exampleusername\Downloads\FederationMetadata.xml"
```

Identitätsanbieter konfigurieren

1. Klicken Sie in der Zeile **SAML-Authentifizierung** auf das Dropdown-Menü für Einstellungen und dann auf **Identitätsanbieter**.

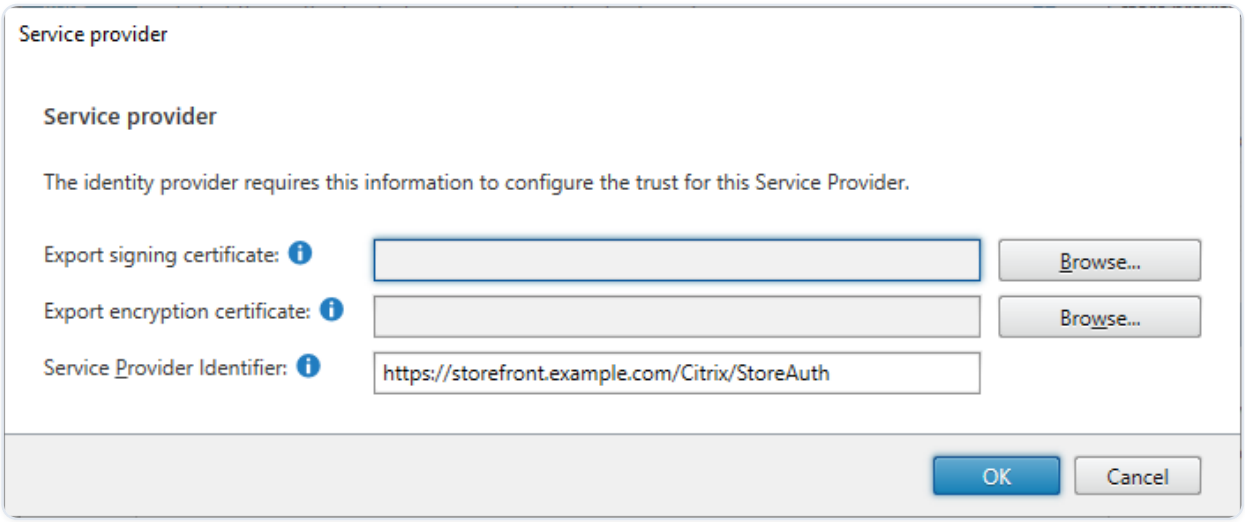




2. Wählen Sie **SAML-Bindung** als **Post** oder **Redirect**.
3. Geben Sie die **Adresse** des Identitätsanbieters ein.
4. Importieren Sie das Zertifikat, das zum Signieren der SAML-Token verwendet wird.
5. Drücken Sie **OK**, um die Änderungen zu speichern.

Dienstanbieter konfigurieren

1. Klicken Sie in der Zeile **SAML-Authentifizierung** auf das Dropdown-Menü für Einstellungen und dann auf **Dienstanbieter**.



2. Wählen Sie optional ein **Export-Signaturzertifikat** aus, das zum Signieren von Nachrichten an den Identitätsanbieter verwendet wird.
3. Wählen Sie optional ein **Export-Verschlüsselungszertifikat** aus, das zum Entschlüsseln von Nachrichten verwendet wird, die vom Identitätsanbieter empfangen werden.
4. Der **Dienstanbieter-Bezeichner** ist mit dem Authentifizierungsdienst für den Store vorausgefüllt.
5. Drücken Sie **OK**, um die Änderungen zu speichern.

PowerShell

Verwenden von PowerShell:

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

Testen

So testen Sie die SAML-Integration:

1. Gehen Sie zur SAML-Testseite, siehe StoreFront SAML-Endpunkte.
2. Dies leitet Sie zum Identitätsanbieter weiter. Geben Sie Ihre Anmeldeinformationen ein.
3. Sie werden zur Testseite zurückgeleitet, die die Identitätsansprüche und -zusicherungen anzeigt.

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 daher den Delivery Controller so konfigurieren, dass er Anfragen von StoreFront vertraut, siehe Citrix Virtual Apps and Desktops Sicherheitsüberlegungen und Best Practices.

Einmaliges Anmelden bei VDAs mit Federated Authentication Service

Bei Verwendung der SAML-Authentifizierung hat StoreFront keinen Zugriff auf die Anmeldeinformationen des Benutzers, sodass das einmalige Anmelden bei VDAs standardmäßig nicht verfügbar ist. Sie können den Federated Authentication Service verwenden, um einmaliges Anmelden bereitzustellen.

Domänen-Pass-Through-Authentifizierung

Benutzer authentifizieren sich bei ihren in die Domäne eingebundenen Windows-Computern, und ihre Anmeldeinformationen werden verwendet, um sie automatisch bei der Citrix Workspace-App anzumelden. Dies ist mit der Citrix Workspace-App für Windows und unterstützten Webbrowsern unter Windows verfügbar.

StoreFront-Konfiguration

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

Die Aktivierung der Domänen-Pass-Through-Authentifizierung für einen Store aktiviert diese standardmäßig auch für die Citrix Workspace-App für HTML5 für alle Websites dieses Stores. Sie können die Domänen-Pass-Through-Authentifizierung für eine bestimmte Website auf der Registerkarte Authentifizierungsmethoden für Websites verwalten deaktivieren.

Delivery Controller™ konfigurieren, um StoreFront zu vertrauen

Bei Verwendung der Domänen-Pass-Through-Authentifizierung hat StoreFront keinen Zugriff auf die Anmeldeinformationen des Benutzers und kann sich daher nicht bei Citrix Virtual Apps and Desktops authentifizieren. Sie müssen daher den Delivery Controller so konfigurieren, dass er Anforderungen von StoreFront vertraut, siehe Citrix Virtual Apps and Desktops – Sicherheitsüberlegungen und Best Practices.

Webbrowser-Konfiguration

Um Domänen-Pass-Through mit einem Webbrowser zu verwenden, muss die Website die Citrix Workspace-App entweder über die Citrix Web Extension oder den Citrix Workspace Launcher erfolgreich erkennen. Möglicherweise müssen Sie die Webbrowser-Konfiguration der Benutzer aktualisieren, um die Domänen-Pass-Through-Authentifizierung zu ermöglichen.

Internet Explorer, Edge und Chrome

Die meisten Webbrowser verwenden die Zonenkonfiguration des Windows Internet Explorer, um zu entscheiden, ob Single Sign-On aktiviert werden soll. Standardmäßig ist dies nur für Websites in der Zone „Lokales Intranet“ aktiviert. So fügen Sie Ihre Website zur Intranetzone hinzu:

1. Systemsteuerung öffnen
2. Internetoptionen öffnen
3. Gehen Sie zur Registerkarte **Sicherheit**.

4. Wählen Sie **Lokales Intranet** aus.
5. Klicken Sie auf **Sites**.
6. Klicken Sie auf **Erweitert**.
7. Fügen Sie Ihre StoreFront-Website hinzu.

Diese Einstellungen können mithilfe von Gruppenrichtlinien bereitgestellt werden.

Weitere Informationen zur Konfiguration von Microsoft Edge für die integrierte Windows-Authentifizierung finden Sie in der Microsoft-Dokumentation.

Firefox

Ändern Sie die erweiterten Browsereinstellungen, um die StoreFront-Website-URI für Single Sign-On als vertrauenswürdig einzustufen.

> **Warnung:**
>
> Eine falsche Bearbeitung der erweiterten Einstellungen kann schwerwiegende Probleme verursachen. Nehmen Sie Änderungen auf eigenes Risiko vor.

1. Öffnen Sie Firefox auf dem Computer, der sich mithilfe der Domänen-Pass-Through-Authentifizierung 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 Unternehmens-Windows-Domäne 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 Unternehmens-Windows-Domäne ein (zum Beispiel mydomain.com).
10. Klicken Sie auf OK.
11. Firefox schließen und neu starten.

Single Sign-On bei VDAs

Um sich mit Domänenanmeldeinformationen bei VDAs anzumelden, müssen Sie die Citrix Workspace-App für Windows mit der Komponente **Single Sign-On aktivieren** verwenden, siehe Domänen-Pass-Through-Authentifizierung konfigurieren. Alternativ können Sie den Federated Authentication Service für das einmalige Anmelden bei VDAs konfigurieren.

Smartcard-Authentifizierung

Bei der Smartcard-Authentifizierung melden sich Benutzer mit Smartcards und PINs an, wenn sie auf ihre Stores zugreifen. Die Smartcard-Authentifizierung kann für Benutzer aktiviert werden, die über die Citrix Workspace-App, Webbrowser und XenApp Services-URLs eine Verbindung zu Stores herstellen.

> **Hinweis:**

> Wenn sich Benutzer mit ihrer Smartcard bei Windows anmelden, wird empfohlen, die Domänen-Passthrough-Authentifizierung zusätzlich zur oder anstelle der Smartcard-Authentifizierung zu aktivieren. Dies ermöglicht Single Sign-On beim Store, ohne dass eine erneute Authentifizierung mit der Smartcard erforderlich ist.

> Verwenden Sie die Smartcard-Authentifizierung, um den Anmeldevorgang für Ihre Benutzer zu optimieren und gleichzeitig die Sicherheit des Benutzerzugriffs auf Ihre Infrastruktur zu erhöhen. Der Zugriff auf das interne Unternehmensnetzwerk wird durch zertifikatbasierte Zwei-Faktor-Authentifizierung unter Verwendung der Public Key Infrastructure geschützt. Private Schlüssel werden durch Hardwarekontrollen geschützt und verlassen niemals die Smartcard. Ihre Benutzer profitieren von der Bequemlichkeit, mit ihren Smartcards und PINs von einer Reihe von Unternehmensgeräten auf ihre Desktops und Anwendungen zuzugreifen.

Um die Smartcard-Authentifizierung zu aktivieren, müssen die Benutzerkonten entweder in der Microsoft Active Directory-Domäne, die die StoreFront-Server enthält, oder in einer Domäne konfiguriert sein, die eine direkte bidirektionale Vertrauensstellung mit der StoreFront-Serverdomäne hat. Multi-Forest-Bereitstellungen mit bidirektionalen Vertrauensstellungen werden unterstützt.

Das Dokument Smartcard-Konfiguration für Citrix-Umgebungen beschreibt, wie eine Citrix-Bereitstellung für Smartcards mit einem bestimmten Smartcard-Typ konfiguriert wird. Ähnliche Schritte gelten für Smartcards anderer Anbieter.

Voraussetzungen

- Stellen Sie sicher, dass die Konten aller Benutzer entweder in der Microsoft Active Directory-Domäne, in der Sie Ihre StoreFront-Server bereitstellen möchten, oder in einer Domäne konfiguriert sind, die eine direkte bidirektionale Vertrauensstellung mit der StoreFront-Serverdomäne hat.
- Wenn Sie Passthrough mit Smartcard-Authentifizierung aktivieren möchten, stellen Sie sicher, dass Ihre Smartcard-Lesertypen, der Middleware-Typ und die Konfiguration sowie die Middleware-PIN-Caching-Richtlinie dies zulassen.
- Installieren Sie die Smartcard-Middleware Ihres Anbieters auf den virtuellen oder physischen Maschinen, auf denen der Virtual Delivery Agent ausgeführt wird, der die Desktops und Anwendungen der Benutzer bereitstellt. Weitere Informationen zur Verwendung von Smartcards mit Citrix Virtual Desktops finden Sie unter Smartcards.
- Stellen Sie sicher, dass Ihre Public-Key-Infrastruktur entsprechend konfiguriert ist. Überprüfen Sie, ob die Zertifikat-zu-Konto-Zuordnung für Ihre Active Directory-Umgebung korrekt konfiguriert ist und die Benutzerzertifikatsvalidierung erfolgreich durchgeführt werden kann.

StoreFront konfigurieren

- Sie müssen HTTPS für die Kommunikation zwischen StoreFront und den Geräten der Benutzer verwenden, um die Smartcard-Authentifizierung zu ermöglichen. Siehe StoreFront mit HTTPS sichern.
- Um die Smartcard-Authentifizierung beim Herstellen einer Verbindung zu einem Store über Citrix Workspace-Apps zu aktivieren, aktivieren oder deaktivieren Sie unter Authentifizierungsmethoden die Option **Smartcard**.
- Das Aktivieren der Smartcard-Authentifizierung für einen Store aktiviert diese standardmäßig auch für alle Websites dieses Stores. Sie können die Smartcard-Authentifizierung für eine bestimmte Website auf der Registerkarte Authentifizierungsmethoden für Websites verwalten unabhängig aktivieren oder deaktivieren.
- Wenn Sie sowohl die Smartcard- als auch die Benutzername- und Kennwortauthentifizierung konfigurieren, werden Benutzer zunächst aufgefordert, sich mit ihren Smartcards und PINs anzumelden, haben aber die Möglichkeit, die explizite Authentifizierung auszuwählen, falls sie Probleme mit ihren Smartcards haben.

Delivery Controller™ so konfigurieren, dass er StoreFront vertraut

Bei der Smartcard-Authentifizierung hat StoreFront keinen Zugriff auf die Anmeldeinformationen des Benutzers und kann sich daher nicht bei Citrix Virtual Apps and Desktops authentifizieren. Sie

müssen daher den Delivery Controller so konfigurieren, dass er Anforderungen von StoreFront vertraut. Siehe dazu Citrix Virtual Apps and Desktops Security considerations and best practices.

Remotezugriff über Citrix Gateway

Für den Remotezugriff können Sie Smartcard auf dem Citrix Gateway aktivieren und dann die Pass-Through-Authentifizierung zu StoreFront mit delegierter Authentifizierung aktivieren. Weitere Informationen finden Sie unter Gateway-Pass-Through.

Um sicherzustellen, dass Benutzer beim Herstellen von Verbindungen zu ihren Ressourcen am virtuellen Server keine zusätzliche Aufforderung zur Eingabe ihrer Anmeldeinformationen erhalten, erstellen Sie ein zweites Gateway und deaktivieren Sie die Clientauthentifizierung in den SSL-Parametern (Secure Sockets Layer). Weitere Informationen finden Sie unter Konfigurieren der Smartcard-Authentifizierung. Beim Zugriff auf StoreFront über ein Gateway mit Smartcard-Authentifizierung. Konfigurieren Sie das optimale Citrix Gateway-Routing über diesen virtuellen Server für Verbindungen zu den Bereitstellungen, die die Desktops und Anwendungen für den Store bereitstellen. Weitere Informationen finden Sie unter Optimales HDX-Routing für einen Store konfigurieren.

Single Sign-On bei VDAs

Sie können Single Sign-On bei den VDAs aktivieren, indem Sie die Smartcard-Anmeldeinformationen der Benutzer weiterleiten. Der Store kann über einen Webbrowser oder die Citrix Workspace™-App für Windows aufgerufen 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. Fügen Sie die Single Sign-On-Komponente bei der Installation von Citrix Workspace für Windows hinzu und konfigurieren Sie sie für Single Sign-On. Siehe Domänen-Pass-Through-Authentifizierung konfigurieren.
2. Öffnen Sie die Datei default.ica für den Store mit einem Texteditor. Siehe Default ICA.
3. Um die Weitergabe von Smartcard-Anmeldeinformationen für Benutzer zu aktivieren, die ohne Citrix Gateway auf Stores zugreifen, fügen Sie die folgende Einstellung im Abschnitt hinzu.

   ```
   DisableCtrlAltDel=Off
   ```

   Diese Einstellung gilt für alle Benutzer des Stores. Um sowohl die Domänen-Pass-Through-Authentifizierung als auch die Pass-Through-Authentifizierung mit Smartcard für Desktops und Anwendungen zu aktivieren, müssen Sie separate Stores für jede Authentifizierungsmethode

erstellen. Leiten Sie dann Ihre Benutzer zum entsprechenden Store für ihre Authentifizierungsmethode.

4. Um die Weitergabe von Smartcard-Anmeldeinformationen für Benutzer zu aktivieren, die über Citrix Gateway auf Stores zugreifen, fügen Sie die folgende Einstellung im Abschnitt hinzu.

   ```
   UseLocalUserAndPassword=On
   ```

   Diese Einstellung gilt für alle Benutzer des Stores. Um die Pass-Through-Authentifizierung für einige Benutzer zu aktivieren und von anderen zu verlangen, dass sie sich anmelden, um auf ihre Desktops und Anwendungen zuzugreifen, müssen Sie separate Stores für jede Benutzergruppe erstellen. Leiten Sie dann Ihre Benutzer zum entsprechenden Store für ihre Authentifizierungsmethode.

Alternativ können Sie den Federated Authentication Service für Single Sign-On bei VDAs konfigurieren.

Wichtige Überlegungen

Die Verwendung von Smartcards zur Benutzerauthentifizierung mit StoreFront unterliegt den folgenden Anforderungen und Einschränkungen.

- Um virtuelle private Netzwerk-(VPN-)Tunnel mit Smartcard-Authentifizierung zu verwenden, müssen Benutzer das Citrix Gateway-Plug-In installieren und sich über eine Webseite anmelden, wobei sie ihre Smartcards und PINs zur Authentifizierung bei jedem Schritt verwenden. Die Pass-Through-Authentifizierung bei StoreFront mit dem Citrix Gateway-Plug-In ist für Smartcard-Benutzer nicht verfügbar.
- Mehrere Smartcards und mehrere Lesegeräte können auf demselben Benutzergerät verwendet werden. Wenn Sie jedoch die Pass-Through-Authentifizierung mit Smartcards aktivieren, müssen Benutzer sicherstellen, dass nur eine Smartcard eingelegt ist, wenn sie auf einen Desktop oder eine Anwendung zugreifen.
- Wenn eine Smartcard innerhalb einer Anwendung verwendet wird, z. B. für digitale Signaturen oder Verschlüsselung, sehen Benutzer möglicherweise zusätzliche Aufforderungen, eine Smartcard einzulegen oder eine PIN einzugeben. Dies kann vorkommen, wenn mehr als eine Smartcard gleichzeitig eingelegt wurde. Es kann auch aufgrund von Konfigurationseinstellungen auftreten – wie z. B. Middleware-Einstellungen wie PIN-Caching, die typischerweise über Gruppenrichtlinien konfiguriert werden. Benutzer, die aufgefordert werden, eine Smartcard einzulegen, obwohl die Smartcard bereits im Lesegerät ist, müssen auf „Abbrechen“ klicken. Wenn Benutzer zur Eingabe einer PIN aufgefordert werden, müssen sie ihre PINs erneut eingeben.

- Wenn Sie die Pass-Through-Authentifizierung mit Smartcards für Citrix Virtual Apps and Desktops für Benutzer der Citrix Workspace-App für Windows mit in die Domäne eingebundenen Geräten aktivieren, die nicht über Citrix Gateway auf Stores zugreifen, gilt diese Einstellung für alle Benutzer des Stores. Um sowohl die Domänen-Pass-Through-Authentifizierung als auch die Pass-Through-Authentifizierung mit Smartcards für Desktops und Anwendungen zu aktivieren, müssen Sie separate Stores für jede Authentifizierungsmethode erstellen. Ihre Benutzer müssen sich dann mit dem entsprechenden Store für ihre Authentifizierungsmethode verbinden.
- Wenn Sie die Pass-Through-Authentifizierung mit Smartcards für Citrix Virtual Apps and Desktops für Benutzer der Citrix Workspace-App für Windows mit in die Domäne eingebundenen Geräten aktivieren, die über Citrix Gateway auf Stores zugreifen, gilt diese Einstellung für alle Benutzer des Stores. Um die Pass-Through-Authentifizierung für einige Benutzer zu aktivieren und andere Benutzer zur Anmeldung an ihren Desktops und Anwendungen aufzufordern, müssen Sie separate Stores für jede Benutzergruppe erstellen. Leiten Sie Ihre Benutzer dann zum entsprechenden Store für ihre Authentifizierungsmethode.
- Für jede XenApp® Services-URL kann nur eine Authentifizierungsmethode konfiguriert werden, und pro Store ist nur eine URL verfügbar. Wenn Sie zusätzlich zur Smartcard-Authentifizierung andere Authentifizierungstypen aktivieren müssen, müssen Sie separate Stores, jeweils mit einer XenApp Services-URL, für jede Authentifizierungsmethode erstellen. Leiten Sie Ihre Benutzer dann zum entsprechenden Store für ihre Authentifizierungsmethode.
- Wenn StoreFront installiert ist, erfordert die Standardkonfiguration in Microsoft Internet Information Services (IIS) nur, dass Clientzertifikate für HTTPS-Verbindungen zur Zertifikatsauthentifizierungs-URL des StoreFront-Authentifizierungsdienstes vorgelegt werden. IIS fordert keine Clientzertifikate für andere StoreFront-URLs an. Diese Konfiguration ermöglicht es Ihnen, Smartcard-Benutzern die Möglichkeit zu geben, auf die explizite Authentifizierung zurückzugreifen, falls sie Probleme mit ihren Smartcards haben. Vorbehaltlich der entsprechenden Windows-Richtlinieneinstellungen können Benutzer ihre Smartcards auch entfernen, ohne sich erneut authentifizieren zu müssen.

  Wenn Sie IIS so konfigurieren, dass Clientzertifikate für HTTPS-Verbindungen zu allen StoreFront-URLs erforderlich sind, müssen der Authentifizierungsdienst und die Stores auf demselben Server untergebracht sein. Sie müssen ein Clientzertifikat verwenden, das für alle Stores gültig ist. Mit dieser IIS-Site-Konfiguration können Smartcard-Benutzer keine Verbindung über Citrix Gateway herstellen und nicht auf die explizite Authentifizierung zurückgreifen. Benutzer müssen sich erneut anmelden, wenn sie ihre Smartcards aus ihren Geräten entfernen.

Pass-Through von Citrix Gateway

Benutzer authentifizieren sich bei Citrix Gateway und werden automatisch angemeldet, wenn sie auf ihre Stores zugreifen. Die Pass-Through-Authentifizierung von Citrix Gateway ist standardmäßig aktiviert, wenn Sie den Remotezugriff auf einen Store zum ersten Mal konfigurieren. Benutzer können über Citrix Gateway mit einer lokal installierten Citrix Workspace-App oder einem Webbrowser eine Verbindung zu Stores herstellen. Weitere Informationen zum Konfigurieren von StoreFront für Citrix Gateway finden Sie unter Citrix Gateway konfigurieren.

StoreFront unterstützt Pass-Through mit den folgenden Citrix Gateway-Authentifizierungsmethoden.

- **Domäne** Benutzer melden sich mit ihrem Active Directory-Benutzernamen und -Kennwort an.
- **RSA** Benutzer melden sich mit Passcodes an, die von Tokencodes abgeleitet werden, die von Sicherheitstokens generiert und manchmal mit persönlichen Identifikationsnummern kombiniert werden. Wenn Sie die Pass-Through-Authentifizierung nur mit Sicherheitstoken aktivieren, stellen Sie sicher, dass die von Ihnen bereitgestellten Ressourcen keine zusätzlichen oder alternativen Authentifizierungsformen erfordern, wie z. B. die Microsoft Active Directory-Domänenanmeldeinformationen der Benutzer.
- **Smartcard** Benutzer melden sich mit einer Smartcard an, die mit ihrem Active Directory-Konto verknüpft ist.
- **RSA + Domäne** Benutzer melden sich sowohl mit ihren Domänenanmeldeinformationen als auch mit Sicherheitstoken-Passcodes an.
- **SAML** Benutzer werden zu einem Drittanbieter-IdP umgeleitet, um sich über SAML anzumelden. Die SAML-Assertion muss den UPN des Active Directory-Kontos des Benutzers enthalten.
- **Entra ID über OIDC** (CU1 und höher) Benutzer werden zur Authentifizierung zu Microsoft Entra ID umgeleitet. Der Benutzer kann entweder eine reine Entra ID oder eine Hybrididentität haben. Weitere Informationen finden Sie unter Entra ID-Authentifizierung mit OIDC.

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

Wenn Sie die Double-Source-Authentifizierung für Citrix Gateway für Remote-Benutzer konfigurieren, die von der Citrix Workspace-App aus auf Stores zugreifen, müssen Sie zwei Authentifizierungsrichtlinien auf 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, um die sekundäre Authentifizierungsmethode im Sitzungsprofil zu verwenden, damit LDAP-Anmeldeinformationen an StoreFront übergeben werden. Wenn Sie die Citrix Gateway-Appliance zu Ihrer StoreFront-Konfiguration hinzufügen, setzen Sie den Anmeldetyp auf Domäne und Sicherheitstoken. Weitere Informationen finden Sie unter `<http://support.citrix.com/article/CTX125364>`

Um die Multi-Domänen-Authentifizierung über Citrix Gateway zu StoreFront zu aktivieren, setzen Sie das SSO-Namensattribut in der Citrix Gateway LDAP-Authentifizierungsrichtlinie für jede Domäne auf userPrincipalName. Sie können von Benutzern verlangen, eine Domäne auf der Citrix Gateway-Anmeldeseite anzugeben, damit die entsprechende LDAP-Richtlinie ermittelt werden kann. Wenn Sie die Citrix Gateway-Sitzungsprofile für Verbindungen zu StoreFront konfigurieren, geben Sie keine Single Sign-On-Domäne an. Sie müssen Vertrauensstellungen zwischen den einzelnen Domänen konfigurieren. Stellen Sie sicher, dass Sie Benutzern die Anmeldung bei StoreFront von jeder Domäne aus ermöglichen, indem Sie den Zugriff nicht nur auf explizit vertrauenswürdige Domänen beschränken.

Sofern von Ihrer Citrix Gateway-Bereitstellung unterstützt, können Sie SmartAccess verwenden, um den Benutzerzugriff auf Citrix Virtual Apps and Desktops-Ressourcen basierend auf Citrix Gateway-Sitzungsrichtlinien zu steuern.

Gateway-Pass-Through aktivieren

Um die Gateway-Pass-Through-Authentifizierung für einen Store beim Verbinden über Workspace-Apps zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie im Fenster Authentifizierungsmethoden die Option **Pass-Through von Citrix Gateway**.

Wenn Sie die Pass-Through-Authentifizierung von Citrix Gateway für einen Store aktivieren, wird sie standardmäßig auch für alle Websites dieses Stores aktiviert. Sie können die Benutzername- und Kennwortauthentifizierung für eine bestimmte Website auf der Registerkarte (/de-de/storefront/2507-ltsr/stores/websites/authentication-methods.html) deaktivieren.

Vertrauenswürdige Benutzerdomänen konfigurieren

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

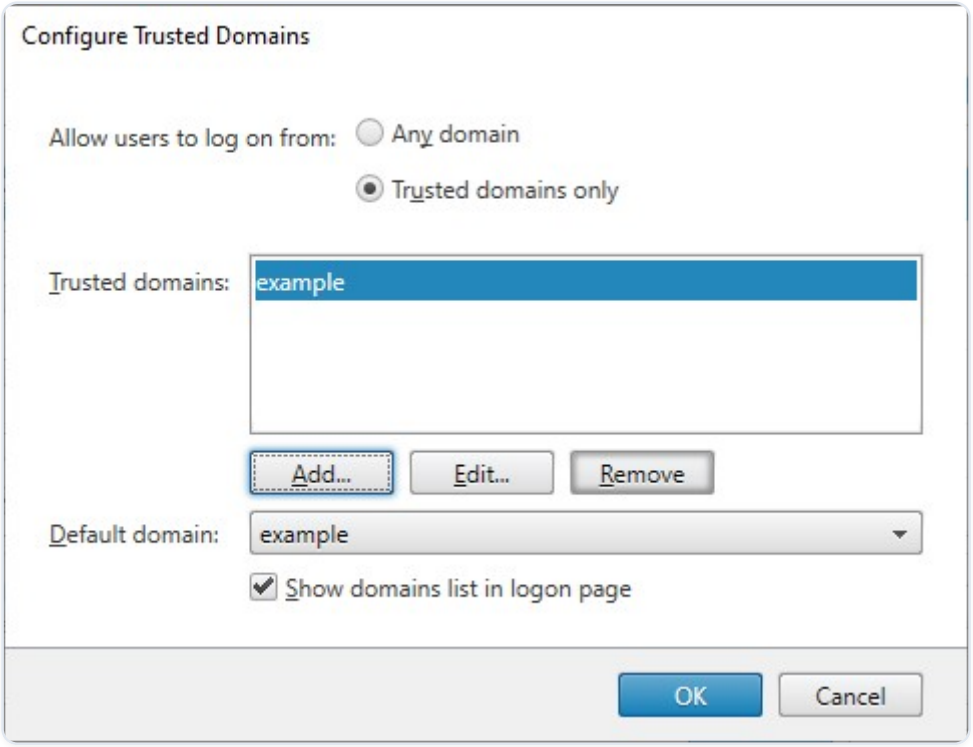
1. Wählen Sie im Fenster „Authentifizierungsmethoden verwalten“ im Dropdownmenü **Pass-Through von Citrix Gateway** > **Einstellungen** die Option **Vertrauenswürdige Domänen konfigurieren**.

2. Wählen Sie **Nur vertrauenswürdige Domänen** und klicken Sie auf **Hinzufügen**, um den Namen einer vertrauenswürdigen Domäne einzugeben. Benutzer mit Konten in dieser Domäne können sich bei allen Stores anmelden, die den Authentifizierungsdienst verwenden. Um einen Domänennamen zu ändern, wählen Sie den Eintrag in der Liste der vertrauenswürdigen Domänen aus und klicken Sie auf **Bearbeiten**. Um den Zugriff auf Stores für Benutzerkonten in einer Domäne zu beenden, wählen Sie die Domäne in der Liste aus und klicken Sie auf **Entfernen**.

   Die Art und Weise, wie Sie den Domänennamen angeben, bestimmt das Format, in dem Benutzer ihre Anmeldeinformationen eingeben müssen. Wenn Benutzer ihre Anmeldeinformationen im Format „Domänenbenutzername“ eingeben sollen, fügen Sie den NetBIOS-Namen zur Liste hinzu. Um zu verlangen, dass Benutzer ihre Anmeldeinformationen im Format „Benutzerprinzipalname“ eingeben, fügen Sie den vollqualifizierten Domänennamen zur Liste hinzu. Wenn Sie Benutzern ermöglichen möchten, ihre Anmeldeinformationen sowohl im Format „Domänenbenutzername“ als auch im Format „Benutzerprinzipalname“ einzugeben, müssen Sie sowohl den NetBIOS-Namen als auch den vollqualifizierten Domänennamen zur Liste hinzufügen.

3. Wenn Sie mehrere vertrauenswürdige Domänen konfigurieren, wählen Sie aus der Liste „Standarddomäne“ die Domäne aus, die standardmäßig ausgewählt wird, wenn sich Benutzer anmelden.

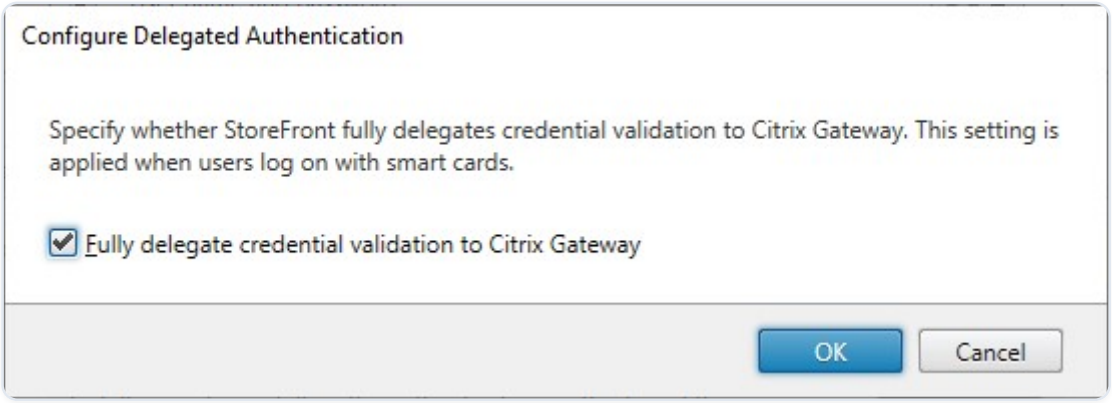
4. Wenn Sie die vertrauenswürdigen Domänen auf der Anmeldeseite auflisten möchten, aktivieren Sie das Kontrollkästchen „Domänenliste auf der Anmeldeseite anzeigen“.



Delegierte Authentifizierung

Standardmäßig validiert StoreFront den Benutzernamen und das Kennwort, die es vom Citrix Gateway erhält. Wenn Ihr Citrix Gateway keine Active Directory-Anmeldeinformationen über LDAP als Faktor verwendet, z. B. bei der Verwendung von SAML oder Smartcards, müssen Sie StoreFront so konfigurieren, dass es der vom Gateway durchgeführten Validierung vertraut. In diesem Fall ist es wichtig, dass Sie beim Konfigurieren des Gateways eine Callback-URL eingeben, damit StoreFront überprüfen kann, ob die Anforderung vom Citrix Gateway stammt. Siehe (/de-de/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/configure-citrix-gateway.html).

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



PowerShell

Um den Store so zu konfigurieren, dass die Authentifizierung mithilfe von PowerShell an das Citrix Gateway delegiert wird, führen Sie das Cmdlet Set-STFCitrixAGBasicOptions aus.

- Um die Authentifizierung an das Gateway zu delegieren, setzen Sie `CredentialValidationMode` auf `Auto`.
- Damit StoreFront die Anmeldeinformationen validiert, setzen Sie `CredentialValidationMode` auf `Password`.

Kennwortvalidierung

Sie können wählen, ob StoreFront die Anmeldeinformationen selbst validiert oder den Delivery Controller bittet, die Anmeldeinformationen zu validieren. Weitere Informationen finden Sie unter Benutzername und Kennwortauthentifizierung – Kennwortvalidierung.

Wenn **Vollständige Delegierung der Anmeldeinformationsvalidierung an Citrix Gateway** ausgewählt ist, hat die Einstellung zur Kennwortvalidierung über den Delivery Controller keine Auswirkung. In diesem Fall muss StoreFront den Benutzer in Active Directory suchen können, sodass die Domäne des StoreFront-Servers immer eine Vertrauensstellung zur Domäne des Benutzers haben muss.

Benutzern das Ändern abgelaufener Kennwörter bei der Anmeldung erlauben

Wenn Ihr Citrix Gateway für die Verwendung der LDAP-Authentifizierung (Benutzername und Kennwort) konfiguriert ist, können Sie NetScaler so konfigurieren, dass das Ändern abgelaufener Kennwörter bei der Anmeldung zugelassen wird.

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

Benutzern das Ändern von Kennwörtern nach der Anmeldung erlauben

Sie können StoreFront so konfigurieren, dass Benutzer ihre Kennwörter nach der Anmeldung ändern können. Diese Funktionalität ist nur verfügbar, wenn das Gateway die LDAP-Authentifizierung verwendet und der Benutzer über einen Browser auf den Store zugreift, nicht über eine lokal installierte Citrix Workspace-App.

Die Standardkonfiguration von StoreFront verhindert, dass Benutzer ihre Kennwörter ändern, selbst wenn die Kennwörter abgelaufen sind. Wenn Sie diese Funktion aktivieren möchten, stellen Sie sicher, dass die Richtlinien für die Domänen, die Ihre Server enthalten, Benutzer nicht daran hindern, ihre Kennwörter zu ändern. Wenn Benutzer ihre Kennwörter ändern können, werden sensible Sicherheitsfunktionen für jeden zugänglich, der auf einen der Stores zugreifen kann, die den Authentifizierungsdienst verwenden. Wenn Ihre Organisation eine Sicherheitsrichtlinie hat, die Funktionen zur Kennwortänderung für Benutzer nur für die interne Verwendung vorsieht, stellen Sie sicher, dass keiner der Stores von außerhalb Ihres Unternehmensnetzwerks zugänglich ist.

1. Wählen Sie im Fenster **Manage Authentication Methods** aus dem Dropdown-Menü **Pass-through from Citrix Gateway** > **Settings** die Option **Manage Password Options**.
2. Um Benutzern das Ändern von Kennwörtern zu ermöglichen, aktivieren Sie das Kontrollkästchen **Benutzern das Ändern von Kennwörtern erlauben**.



Hinweis:

Wenn Sie **Benutzern das Ändern von Kennwörtern erlauben** auswählen oder deaktivieren, wirkt sich dies auch auf die Einstellungen unter **Kennwortoptionen verwalten** für die Benutzername und Kennwort-Authentifizierung aus.

PowerShell

Um die Optionen zum Ändern des Kennworts mithilfe von PowerShell zu ändern, führen Sie das Cmdlet Set-STFExplicitCommonOptions aus.

Delivery Controller™ so konfigurieren, dass er StoreFront vertraut

Wenn das Citrix 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 daher den Delivery Controller so konfigurieren, dass er Anfragen von StoreFront vertraut, siehe Citrix Virtual Apps and Desktops – Sicherheitsüberlegungen und Best Practices.

Single Sign-On bei VDAs

Verwenden von Active Directory-Anmeldeinformationen

Wenn das Gateway mit LDAP-Authentifizierung konfiguriert ist, leitet es die Anmeldeinformationen an StoreFront weiter, sodass Single Sign-On bei VDAs möglich ist. Es ist keine zusätzliche Konfiguration erforderlich.

Verwenden des Federated Authentication Service

Bei Gateway-Authentifizierungsmethoden außer LDAP hat StoreFront keinen Zugriff auf die Anmeldeinformationen des Benutzers, sodass Single Sign-On standardmäßig nicht verfügbar ist. Sie können den Federated Authentication Service verwenden, um Single Sign-On bereitzustellen.

Verwenden von Entra ID

Wenn das Gateway für die Verwendung der Entra ID-Authentifizierung über OIDC konfiguriert ist, können Sie Entra ID Single Sign-On aktivieren. Dies erfordert CU1 oder höher. Weitere Informationen finden Sie unter VDA Entra ID Single Sign-On konfigurieren.

Websites verwalten

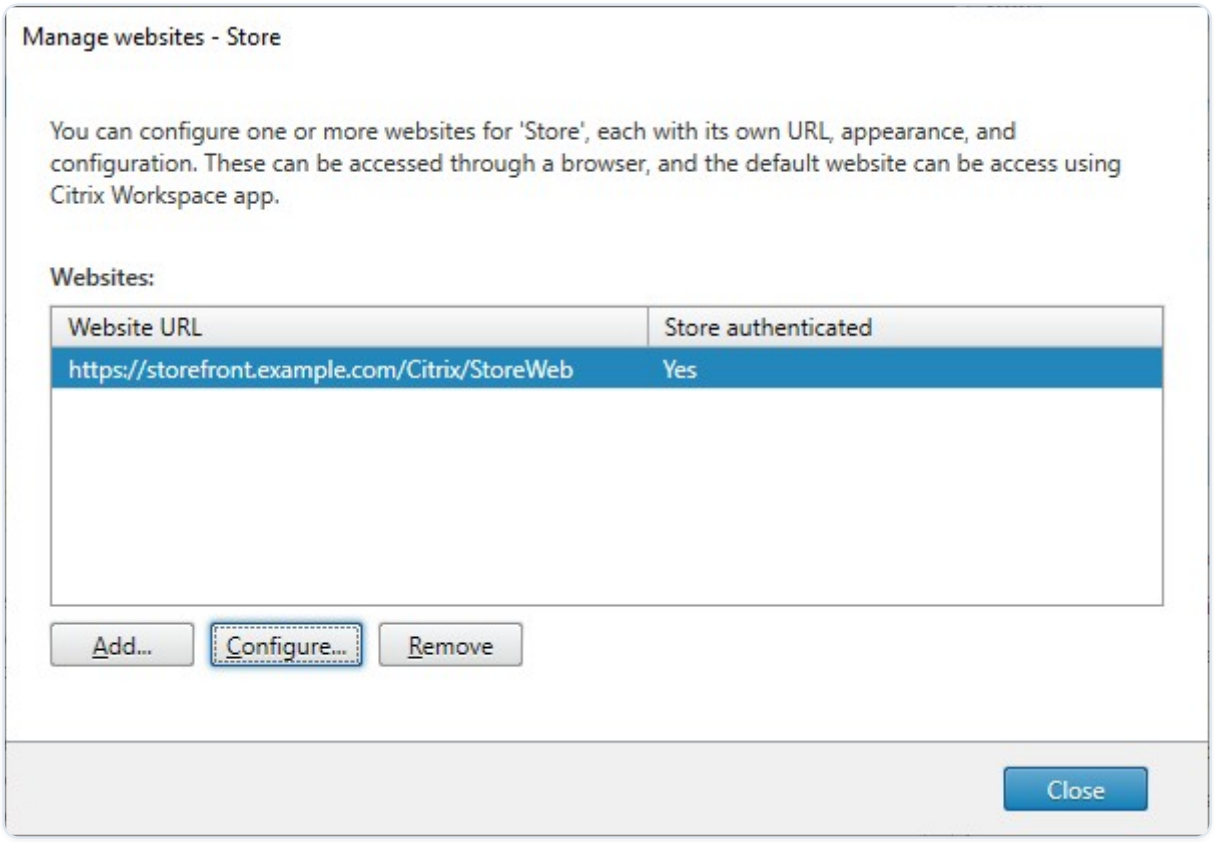
Wenn Sie einen Store erstellen, wird automatisch eine Website dafür erstellt, auf die Benutzer entweder über einen Browser oder über die Citrix Workspace-App zugreifen können. Sie müssen mindestens eine Website haben. Sie können bestehenden Stores zusätzliche Websites hinzufügen. Dadurch können Sie Ihren Benutzern verschiedene URLs mit unterschiedlichen Konfigurationen bereitstellen. Mehrere Websites können jedoch nur über einen Webbrowser aufgerufen werden, da Citrix Workspace-Apps für die Verwendung einer bestimmten Website für einen Store konfiguriert sind. Siehe Workspace-App-Website konfigurieren.

> Wichtig:
>
> Verwenden Sie in Bereitstellungen mit mehreren Servern immer nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Wenn Sie fertig sind, übertragen Sie Ihre Konfigurationsänderungen auf die Servergruppe, damit die anderen Server in der Bereitstellung aktualisiert werden.

Websites anzeigen

So zeigen Sie die Websites für einen Store an:

1. Wählen Sie in der Verwaltungskonsole im linken Bereich den Knoten **Stores** aus.
2. Wählen Sie den Store aus, den Sie konfigurieren möchten.
3. Wählen Sie im Bereich **Aktionen** die Option **Websites verwalten**.



Auf dem Bildschirm **Websites verwalten** können Sie die folgenden Aktionen ausführen:

AKTION	DETAILS
Eine Website erstellen	Erstellen Sie Websites, die es Benutzern ermöglichen, über eine Webseite oder die Workspace-App auf Stores zuzugreifen.
Eine Website konfigurieren	Einstellungen für Ihre Website ändern.
Eine Website entfernen	Entfernen Sie eine Citrix Receiver™ für Web-Site.

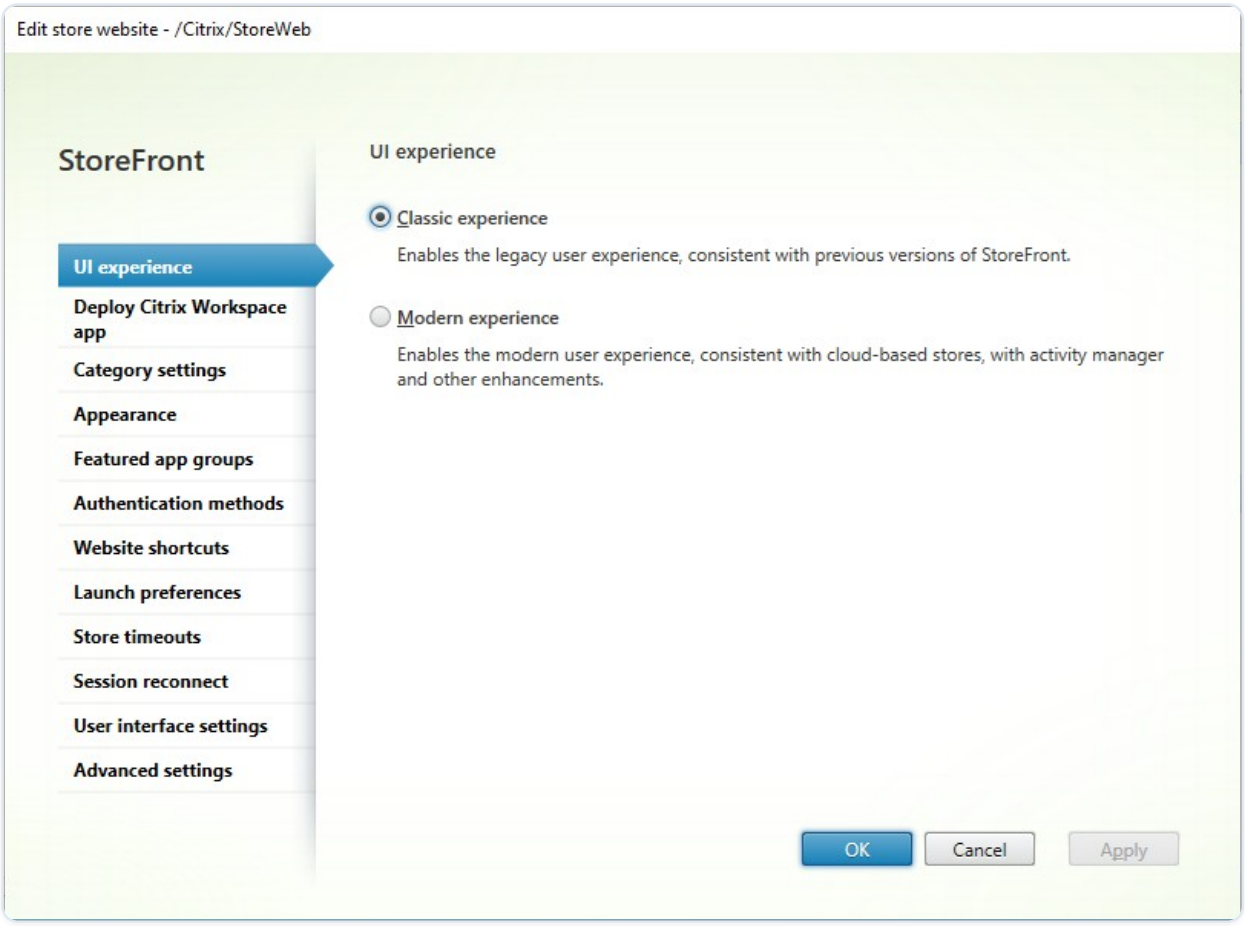
PowerShell

Um eine Liste der Websites abzurufen, verwenden Sie das Cmdlet Get-STFWebReceiverService.

Eine Website konfigurieren

So konfigurieren Sie eine Website:

1. Wählen Sie eine Website aus und klicken Sie auf **Konfigurieren...**



2. Ändern Sie die Einstellungen auf den entsprechenden Registerkarten.

- Benutzeroberflächenerfahrung
- Citrix Receiver/Workspace-App bereitstellen
- Kategorieeinstellungen
- Erscheinungsbild anpassen
- Empfohlene App-Gruppen
- Authentifizierungsmethoden
- Website-Verknüpfungen
- Starteinstellungen
- Sitzungseinstellungen
- Workspace-Steuerung
- Client-Oberflächeneinstellungen
- Angeheftete Links
- Benutzerdefinierte Ankündigungen
- Dialog nach der Anmeldung

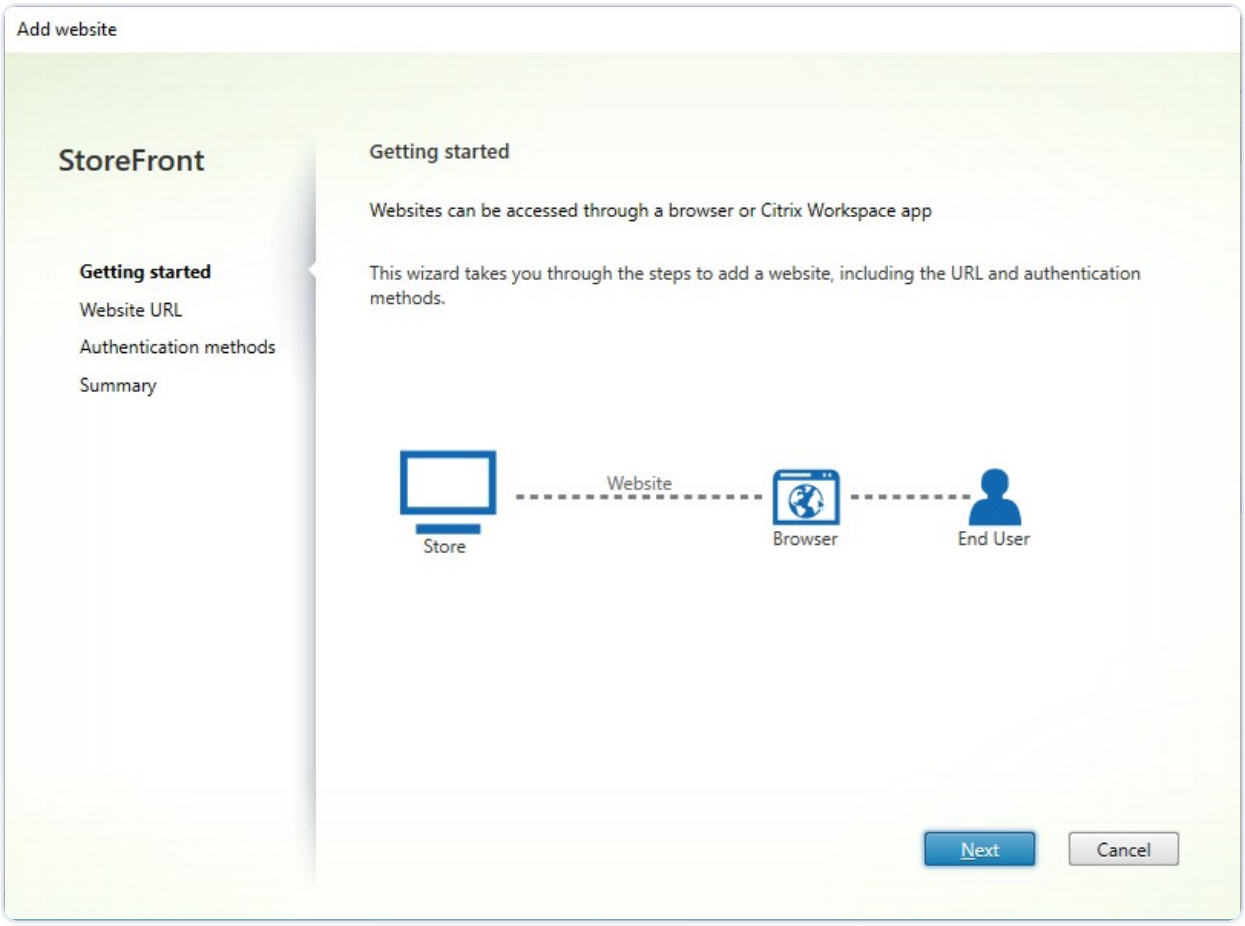
- Erweiterte Einstellungen

3. Nachdem Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **OK**.
4. Um App Protection zu konfigurieren, müssen Sie PowerShell verwenden. Stellen Sie sicher, dass Sie die StoreFront-Verwaltungskonsole schließen, bevor Sie PowerShell-Befehle ausführen.

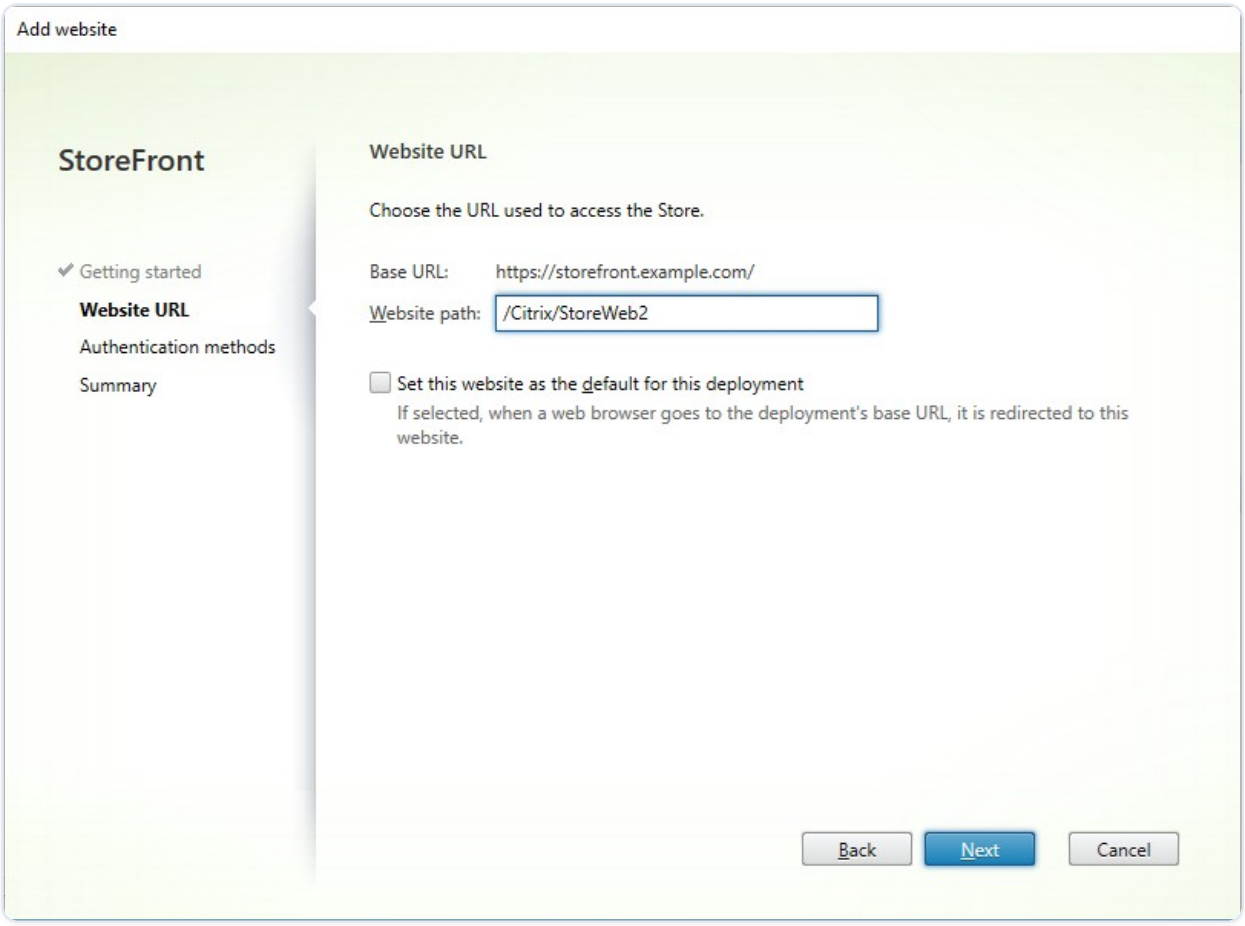
Eine Website erstellen

Wenn Sie einen Store erstellen, wird automatisch eine Website dafür erstellt. Sie können bestehenden Stores zusätzliche Websites hinzufügen. Dadurch können Sie Ihren Benutzern verschiedene URLs mit unterschiedlichen Konfigurationen bereitstellen. Mehrere Websites können jedoch nur über einen Webbrowser aufgerufen werden, da Citrix Workspace-Apps so konfiguriert sind, dass sie eine bestimmte Website für einen Store verwenden. Siehe Workspace-App-Website konfigurieren.

1. Wählen Sie **Hinzufügen...**.



2. Auf der Registerkarte **Erste Schritte** wählen Sie **Weiter**.
3. Geben Sie den gewünschten **Websiterootpfad** ein, wählen Sie, ob dies die Standardwebsite für die Basis-URL sein soll, und wählen Sie **Weiter**.



4. Aktivieren oder deaktivieren Sie die gewünschten Authentifizierungsmethoden. Einige Methoden sind nur verfügbar, wenn sie für den Store konfiguriert wurden. Drücken Sie **Weiter**.

   Screenshot des Bildschirms „Website hinzufügen“, Registerkarte „Authentifizierungsmethoden“(/en-us/storefront/2507-ltsr/media/stores/websites/add-site-authentication.png)

5. Nachdem die Site erstellt wurde, klicken Sie auf **Fertig stellen**.
6. Wählen Sie die neu erstellte Site aus und klicken Sie auf **Bearbeiten**, um Ihre Website nach Bedarf zu konfigurieren (siehe Websites konfigurieren).

PowerShell

Um eine Website mit PowerShell zu erstellen, führen Sie das Cmdlet `Add-STFWebReceiverService` aus.

Website entfernen

1. Wählen Sie den Knoten **Store** im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus, wählen Sie den Store aus, für den Sie die Citrix Receiver für Web-Site erstellen möchten, und klicken Sie im Bereich **Aktionen** auf **Websites verwalten**.

2. Wählen Sie eine Site aus und klicken Sie auf **Entfernen**. Wenn Sie eine Site entfernen, können Benutzer diese Webseite nicht mehr verwenden, um auf den Store zuzugreifen.

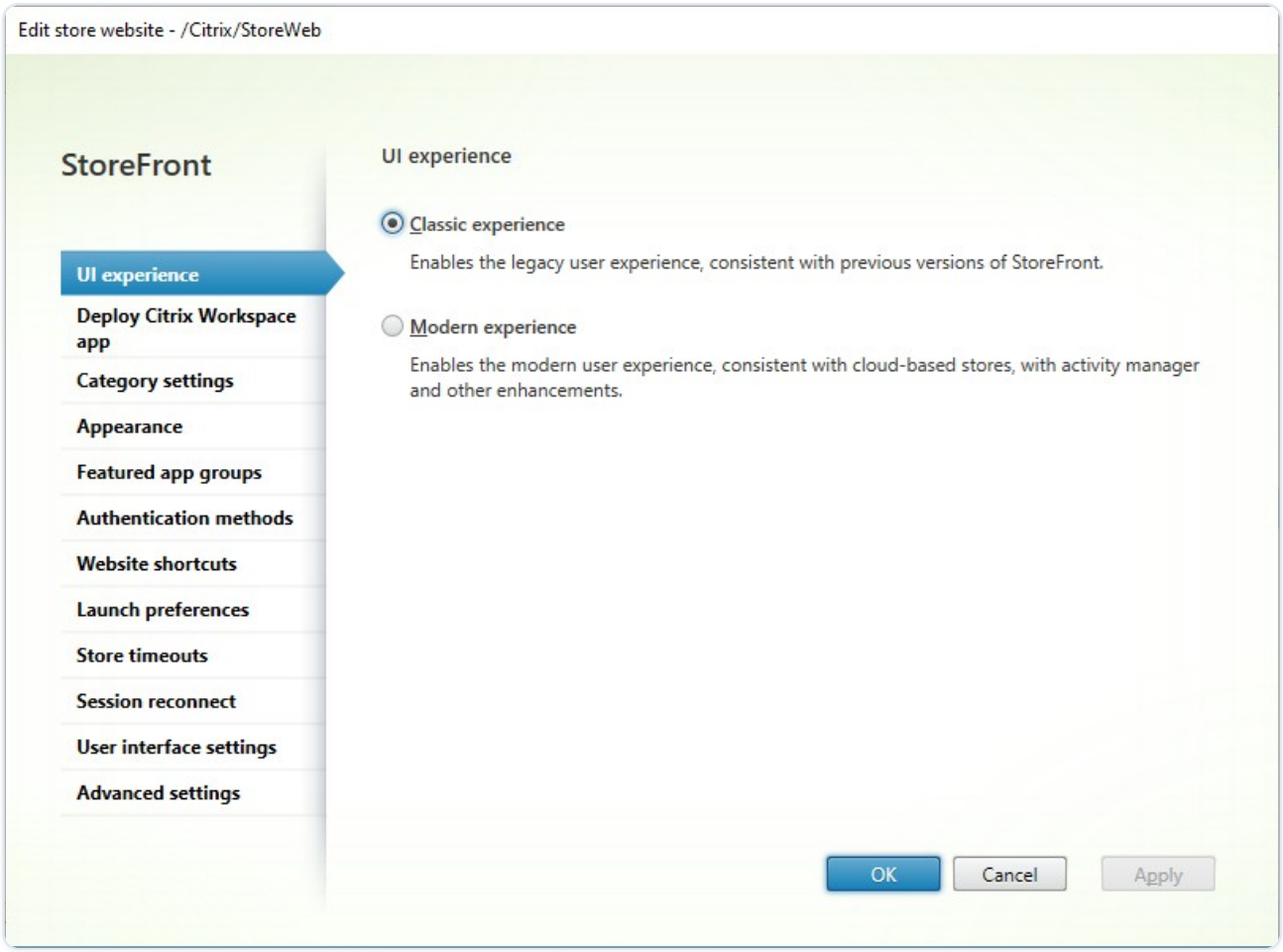
PowerShell

Um eine Website mit PowerShell zu entfernen, führen Sie das Cmdlet `Remove-STFWebReceiverService` aus.

Benutzeroberflächenerfahrung

Auf der Registerkarte „Benutzeroberflächenerfahrung“ können Sie eine Benutzeroberflächenerfahrung für Ihre Endbenutzer auswählen. Sie können wählen zwischen:

- **Klassische Erfahrung** – Weitere Informationen finden Sie unter Klassische Erfahrung.
- **Moderne Erfahrung** – Weitere Informationen finden Sie unter Moderne Erfahrung.



Wenn Sie ein Citrix Gateway für den Fernzugriff verwenden, können Sie ein Thema wählen, das der ausgewählten Erfahrung entspricht. Weitere Informationen finden Sie in der NetScaler-Dokumentation.

PowerShell

Um die Benutzeroberflächenerfahrung mit PowerShell abzurufen, rufen Sie das Cmdlet `Get-STFWebReceiverService` auf und zeigen Sie die Eigenschaft `WebReceiver.WebUIExperience` an.

Zum Beispiel:

```
(Get-STFWebReceiverService -VirtualPath "/Citrix/
StoreWeb").WebReceiver.WebUIExperience
```

`WebUIExperience` nimmt die folgenden Werte an:

- `ReceiverForWeb` – Klassische Erfahrung
- `Workspace` – Moderne Erfahrung

Um die Benutzeroberflächenerfahrung mit PowerShell zu ändern, rufen Sie das Cmdlet `Set-STFWebReceiverService` mit dem Parameter `WebUIExperience` auf.

Zum Beispiel, um die klassische Erfahrung zu verwenden:

```
$rfw=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperience
Workspace
```

Bereitstellung der Citrix Workspace-App

Standardmäßig versucht StoreFront, wenn ein Benutzer zum ersten Mal einen Store in seinem Webbrowser unter Windows, macOS oder Linux öffnet, zu ermitteln, ob die Citrix Workspace-App lokal installiert ist. Wenn eine lokal bereitgestellte Citrix Workspace-App nicht erkannt werden kann, wird der Benutzer aufgefordert, diese herunterzuladen und zu installieren. Der Standard-Downloadspeicherort ist die Citrix-Website, Sie können die Installationsprogramme aber auch auf dem StoreFront-Server oder an einem anderen Ort hosten. Nach der Installation können Benutzer entweder die lokal installierte Citrix Workspace-App öffnen und mit dem Store verbinden oder im Browser fortfahren, sich aber mit virtuellen Apps und Desktops in ihrem lokal installierten Citrix Workspace-App HDX-Client verbinden.

Alternativ können Benutzer, die die Citrix Workspace-App nicht lokal installieren können, einen Webbrowser verwenden, um sowohl auf den Store zuzugreifen als auch sich mit virtuellen Apps und Desktops zu verbinden.

Screenshot der Registerkarte „Citrix Workspace-App bereitstellen“(/en-us/storefront/2507-ltsr/media/stores/websites/deploy-workspace-app.png)

Um die Bereitstellungsoptionen zu ändern, gehen Sie zu Store-Website bearbeiten und wählen Sie die Registerkarte **Citrix Workspace-App bereitstellen**.

Nutzung der Citrix Workspace™-App erzwingen

Administratoren können die Verwendung der nativen Citrix Workspace-App erzwingen, wodurch die Option für Benutzer entfällt, sich über ihren Webbrowser mit dem Store zu verbinden. Diese Funktion wurde für Kunden entwickelt, die die vollen Vorteile der Citrix Workspace-App nutzen möchten. Die Citrix Workspace-App bietet Vorteile wie den integrierten App Protection-Dienst, vermeidet Kompatibilitätsprobleme mit Browserversionen, verbesserte Sicherheit und Telemetrie für Überwachung und Fehlerbehebung. Weitere Informationen finden Sie unter Benutzerzugriffsoptionen.

Diese Funktionalität kann in der Verwaltungskonsole aktiviert werden, wenn die moderne Oberfläche verwendet wird. Sie ist über ein Plug-In verfügbar, wenn entweder die klassische Oberfläche oder ein Citrix Gateway verwendet wird.

Unterstützte Plattformen

Für die automatische Konfiguration der Citrix Workspace-App sind die folgenden Versionen erforderlich.

- Citrix Workspace-App für Windows 24.9.0 oder höher
- Citrix Workspace-App für Mac 24.5.0 oder höher
- Citrix Workspace-App für Android 24.9.0 oder höher
- {Citrix Workspace-App für iOS 24.9.0 oder höher

Konfigurieren in StoreFront mit moderner Oberfläche

Administratoren können die folgenden Schritte ausführen, um die Verwendung der Citrix Workspace-App auf Benutzergeräten zu erzwingen, die eine Verbindung zu StoreFront herstellen:

1. Wählen Sie den Knoten **Stores** im linken Bereich aus und klicken Sie im Bereich **Aktionen** auf **Websites verwalten**.
2. Klicken Sie auf **Konfigurieren** > **Citrix Workspace-App bereitstellen**.

Natives App-Mandat(/en-us/storefront/2507-ltsr/media/stores/websites/native-app-mandate-config.png)

3. Wählen Sie die Option **Endbenutzer müssen ausschließlich die lokal installierte Citrix Workspace-App verwenden** aus.
4. Klicken Sie auf **OK**.

Konfigurieren mit klassischer Oberfläche

1. Laden Sie das Plug-in von Citrix Downloads herunter.
2. Extrahieren Sie die ZIP-Datei und citrix-ui-plugin.tar.gz in ein beliebiges Verzeichnis auf dem StoreFront-Server. Sie enthält PowerShell-Dateien, Javascript-Dateien und Konfigurationsdateien.
3. Öffnen Sie die Datei plugin.config in einem Texteditor. Konfigurieren Sie wie folgt:

   Wenn Sie die Funktion für das native App-Mandat aktivieren möchten, behalten Sie das Schlüssel-Wert-Paar wie folgt bei: `<param name="requireNativeAppUse" value="true" />`

   Wenn Sie die Funktion für das native App-Mandat deaktivieren möchten, behalten Sie das Schlüssel-Wert-Paar wie folgt bei: `<param name="requireNativeAppUse" value="false" />`
4. Öffnen Sie PowerShell als Administrator.
5. Navigieren Sie zum extrahierten Ordner.
6. Führen Sie `./CitrixPluginInstaller.ps1 -VirtualPath /Citrix/<store web name>` aus.
7. Wiederholen Sie dies für jeden Server in der StoreFront-Servergruppe.
8. Überprüfen Sie die korrekte Installation, indem Sie einen Webbrowser öffnen und zur Store-Website navigieren.

Konfigurieren mit einem Citrix Gateway

Wenn Benutzer über ein Citrix Gateway auf ihren Store zugreifen, können Sie ein Plug-in auf dem Gateway installieren, um die Verwendung der Citrix Workspace-App zu erzwingen. Weitere Informationen finden Sie unter Citrix Workspace-App über ein Gateway erforderlich machen.

Benutzererfahrung

Weitere Informationen zur Endbenutzererfahrung für diese Funktion finden Sie unter Endbenutzererfahrung.

Benutzern das Herunterladen der Citrix Workspace-App erlauben

> **Hinweis:**
>
> Wenn Sie nicht verlangt haben, dass Benutzer den Store in der Citrix Workspace-App öffnen, und Sie Startpräferenzen so konfiguriert haben, dass Ressourcen immer in einem Webbrowser geöffnet werden, gelten diese Einstellungen nicht.

> Wenn Sie **Benutzern das Herunterladen der Citrix Workspace-App erlauben** auswählen, wird Benutzern beim ersten Anmelden an einem Gerät unter Windows oder Mac die Option zum Herunterladen der App angeboten.

Workspace-App beim Anmelden aktualisieren

Wenn Sie **Citrix Workspace-App beim Anmelden aktualisieren** auswählen, wird Benutzern beim Anmelden die Möglichkeit angeboten, den lokal installierten Client der Citrix Workspace-App zu aktualisieren. Benutzer können das Upgrade überspringen und werden erst dann erneut zur Aktualisierung aufgefordert, wenn ihre Browser-Cookies gelöscht wurden. Um diese Funktion zu aktivieren, stellen Sie sicher, dass die Dateien der Citrix Workspace-App auf dem StoreFront-Server verfügbar sind.

Download-Quelle

Wenn Endbenutzer auf die Schaltfläche zum Herunterladen klicken, können Sie wählen, ob sie auf die Citrix-Website umgeleitet werden oder Dateien direkt vom Server herunterladen. Sie können **Citrix-Website**, **Lokale Dateien auf dem StoreFront-Server** oder **Dateien auf Remote-Server (über URL)** wählen.

PowerShell

Um diese Einstellungen mit PowerShell zu konfigurieren, führen Sie das Cmdlet Set-STFWebReceiverPluginAssistant aus.

Progressive Web-App (Vorschau)

In Fällen, in denen Benutzer die Citrix Workspace-App nicht installieren können, ermöglicht die Funktion Progressive Web-App (PWA) die Installation der Store-Website, sodass diese von Ihrem Startmenü oder Desktop aus gestartet werden kann, ähnlich einer nativen App. Dies ist nur in der klassischen Erfahrung verfügbar.

Voraussetzungen

Um den Webclient als Progressive Web-App zu verwenden, stellen Sie sicher, dass Sie Folgendes haben:

- Benutzer müssen über HTTPS auf StoreFront zugreifen.
- Die Startoption muss auf **Immer Receiver für HTML5 verwenden** eingestellt sein.
- Verwenden Sie den Google Chrome- oder Microsoft Edge-Browser unter Windows, Mac oder Linux.
- Die Funktion ist standardmäßig deaktiviert und muss aktiviert werden.

Bekannte Einschränkungen

- Wenn Sie den Einzelregisterkartenmodus für die StoreFront-Bereitstellung festlegen, gilt dies nicht für PWA-Starts.
- Hybride Szenarien bei sitzungsfreigegebenen App-Starts werden nicht unterstützt. Das Starten einer App aus der PWA und der anschließende Versuch, eine sitzungsfreigegebene App im Browser zu starten, funktioniert beispielsweise nicht.
- Das Umschalten vom PWA-Sitzungsfenster zum Browserfenster funktioniert nicht.

Progressive Web App aktivieren

Diese Funktion ist standardmäßig deaktiviert. Administratoren können die Funktionalität wie folgt aktivieren:

1. Gehen Sie im Fenster **Store-Website bearbeiten** zur Registerkarte „Startpräferenzen“ und legen Sie die Startoptionen auf **In einem Webbrowser öffnen** fest.
2. Speichern Sie die Einstellungen und schließen Sie die Verwaltungskonsole.
3. Führen Sie den PowerShell-Befehl Set-STFWebReceiverUserInterface aus.

```
$receiver = Get-STFWebReceiverService

Set-STFWebReceiverUserInterface -WebReceiverService $receiver
-ProgressiveWebAppEnabled $true
```

Benutzererfahrung

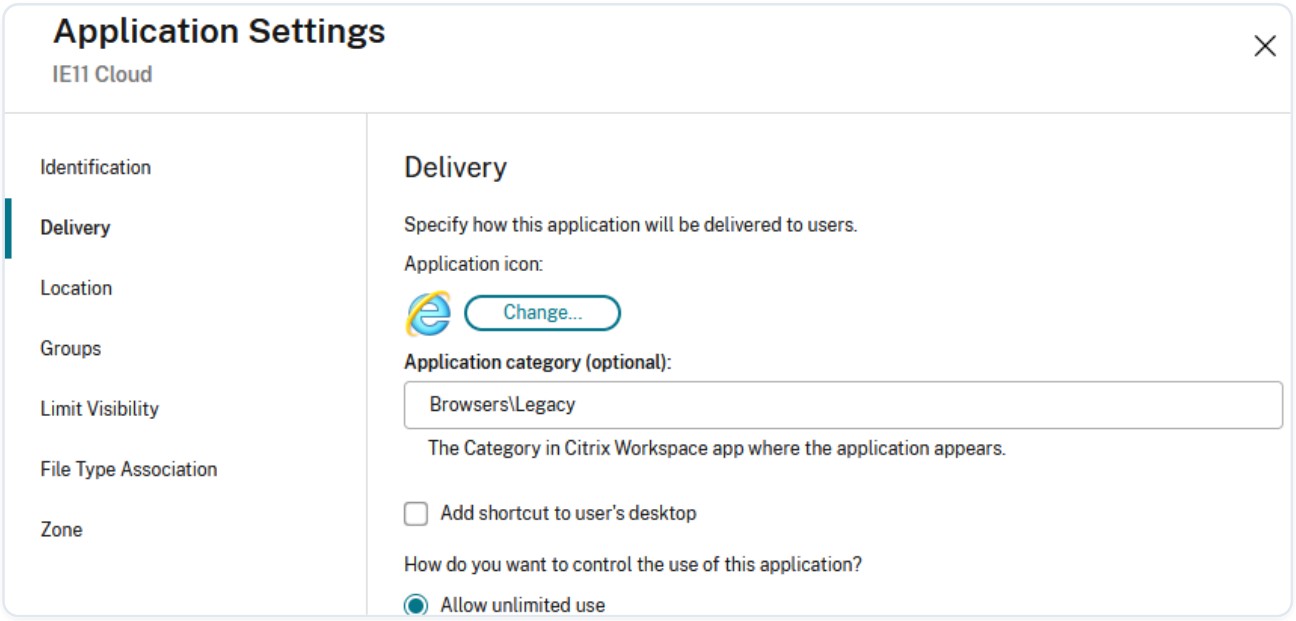
Weitere Informationen zur Installation der App durch Benutzer finden Sie unter Installation als Progressive Web App (Vorschau).

Kategorieeinstellungen

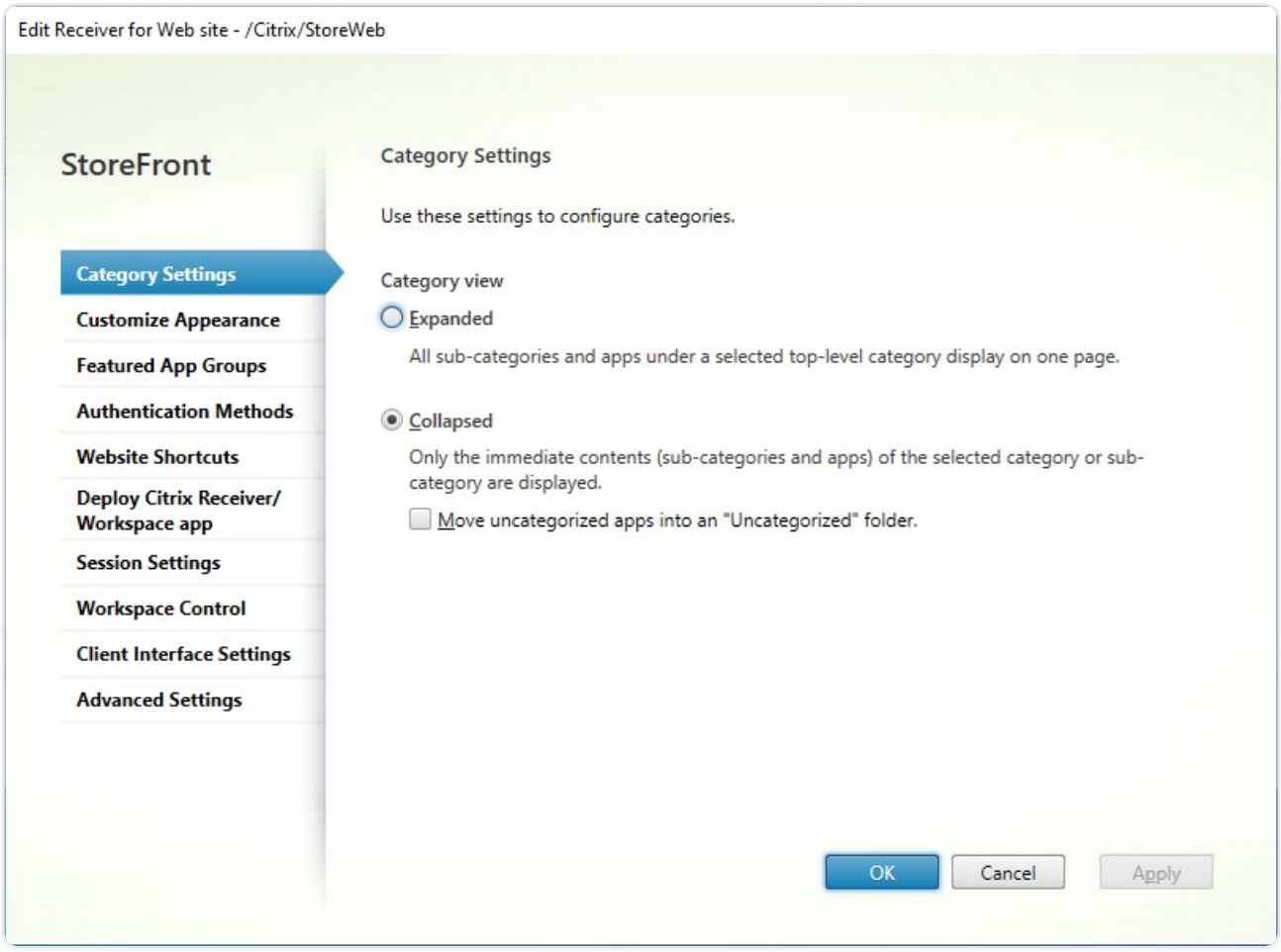
Hinweis:

Diese Funktionalität ist nur mit der klassischen Oberfläche verfügbar.

In Citrix Virtual Apps and Desktops können Sie jede Anwendung einer Kategorie zuweisen, wie im Artikel Anwendungen beschrieben. Verwenden Sie das Symbol `\`, um eine Ordnerhierarchie von Kategorien zu erstellen. In StoreFront können Sie konfigurieren, wie diese Ordnerhierarchie angezeigt wird.



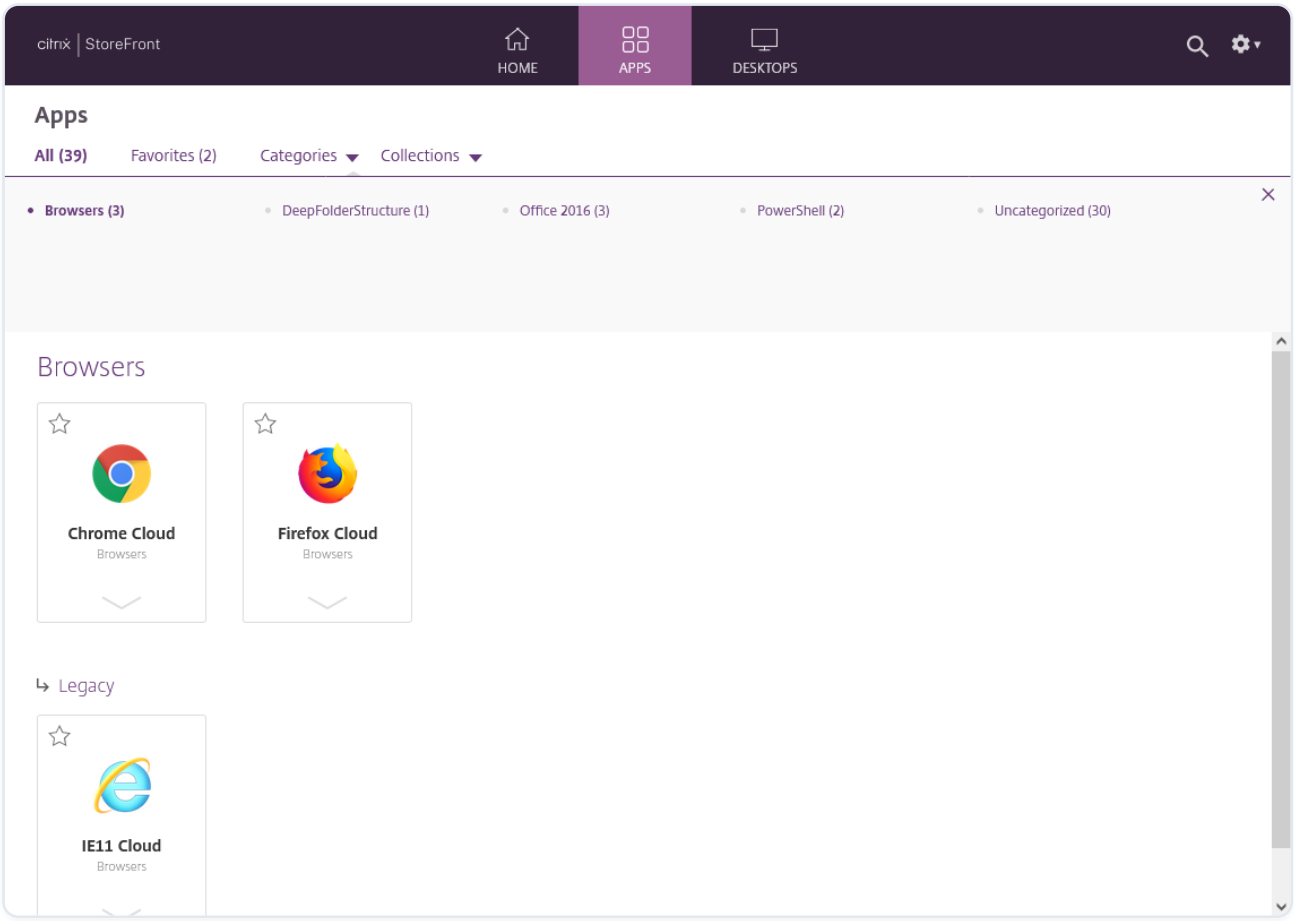
Um die Kategorieeinstellungen zu ändern, gehen Sie zu Store-Website bearbeiten und wählen Sie die Registerkarte **Kategorieeinstellungen**.



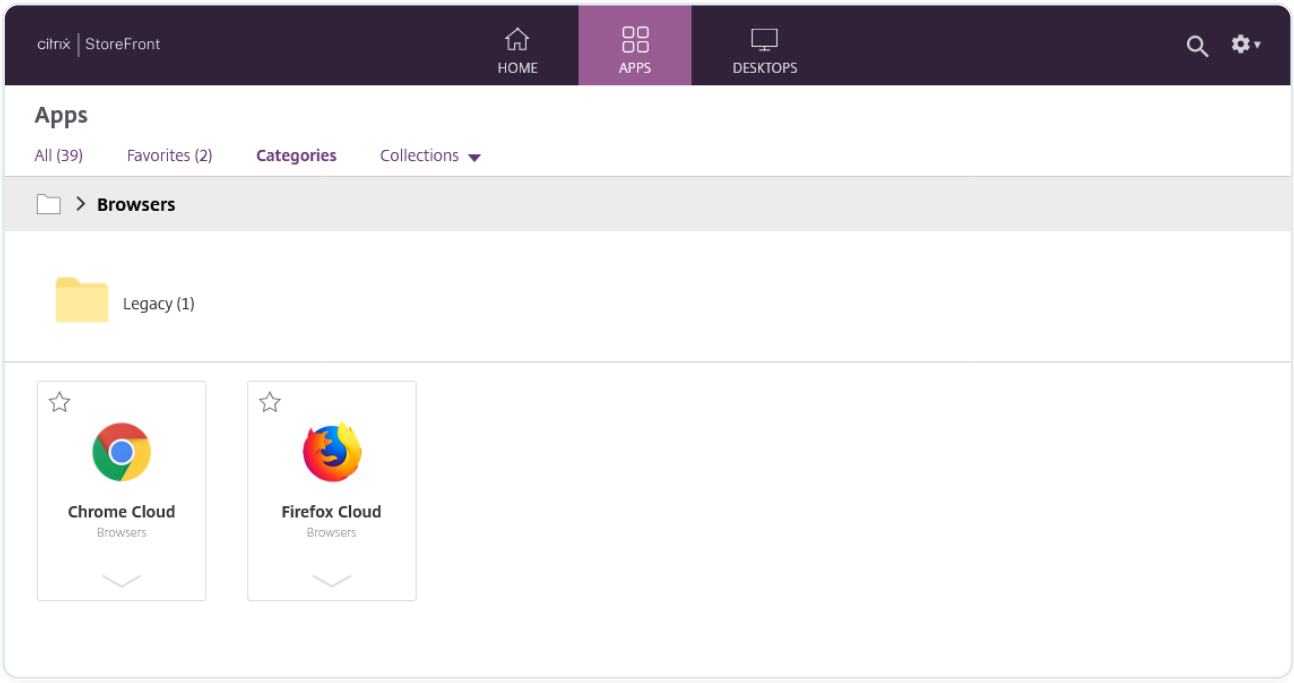
Kategorieansicht

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 StoreFront alle Apps in allen Unterkategorien auf einer Seite an.

Wenn Sie beispielsweise eine Kategorie Browser mit der Unterkategorie Legacy haben, werden alle Browser, einschließlich derer unter Legacy, auf einer Seite angezeigt:

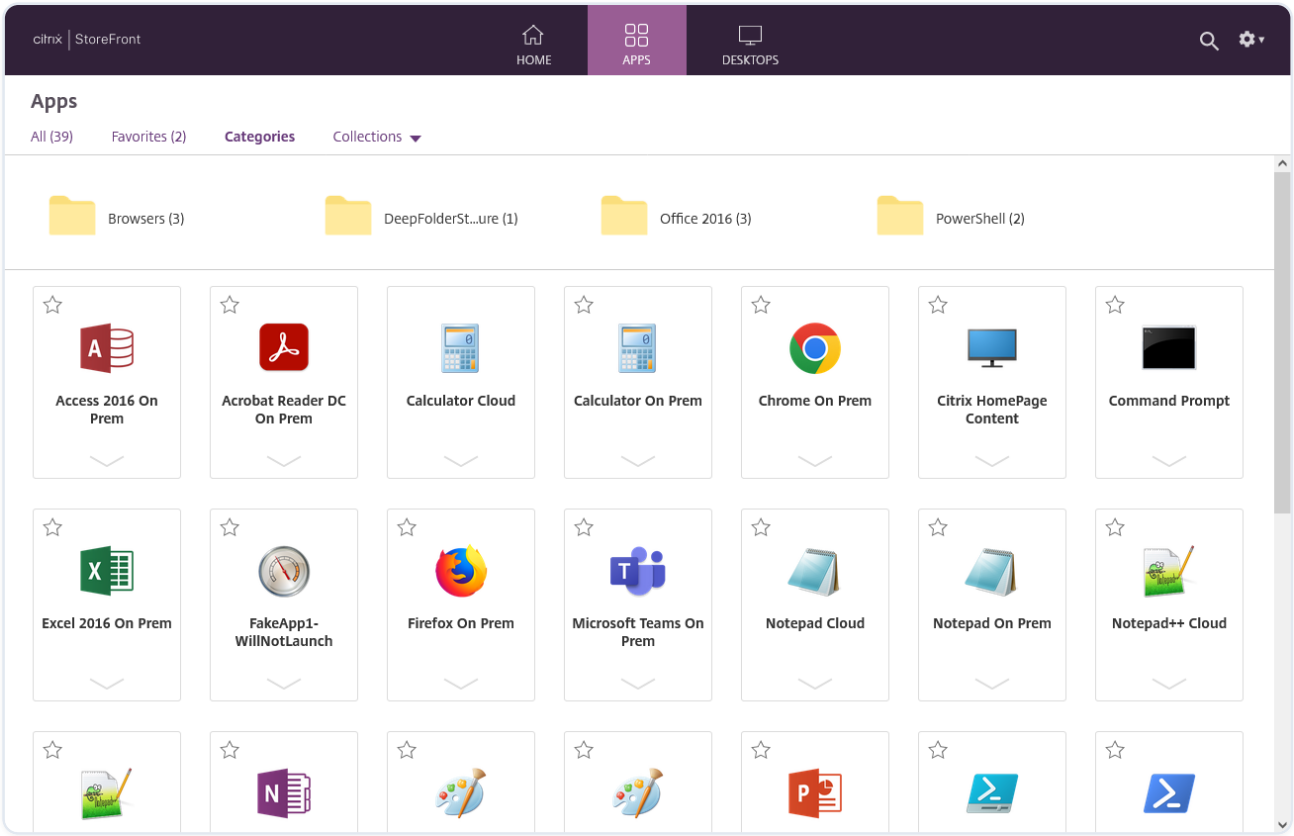


In der reduzierten Ansicht zeigt StoreFront zunächst eine Liste der Kategorien der obersten Ebene und optional alle nicht kategorisierten Apps an. Wenn der Benutzer auf eine Kategorie klickt, zeigt StoreFront nur den unmittelbaren Inhalt (Unterkategorien und Apps) der ausgewählten Kategorie an. Der Benutzer kann auf jede Unterkategorie klicken, um den Inhalt zu erweiternieren.

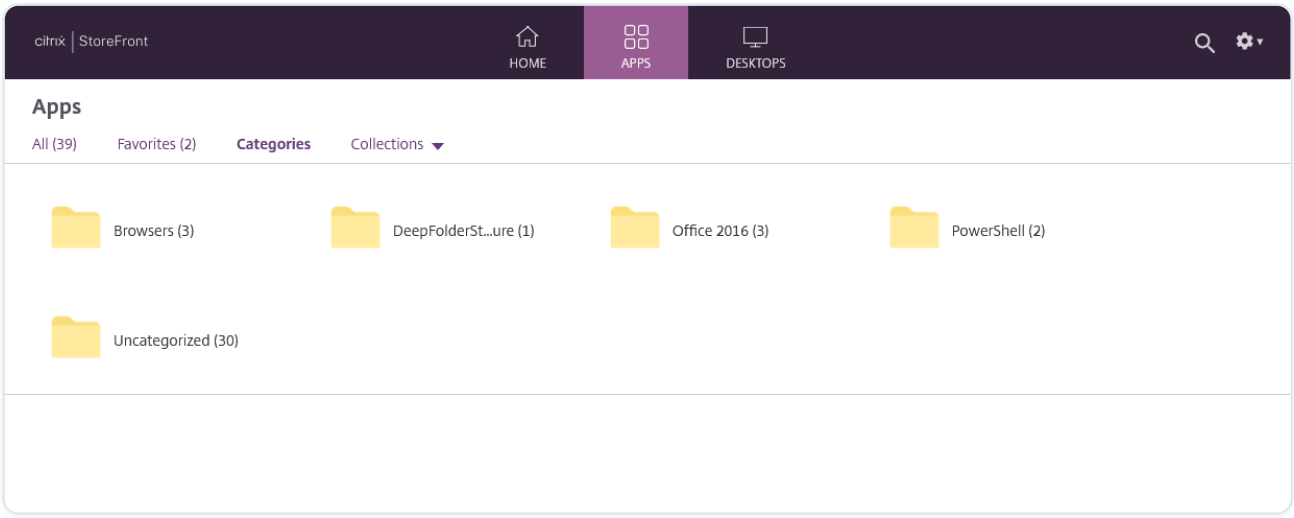


Nicht kategorisierte Apps

Deaktivieren Sie in der reduzierten Ansicht die Option **Nicht kategorisierte Apps in einen Ordner „Nicht kategorisiert“ verschieben**, um alle Apps und Desktops ohne Kategorien in der Anfangsansicht anzuzeigen. Dieses Verhalten ähnelt dem früherer StoreFront-Versionen.



Aktivieren Sie in der reduzierten Ansicht **Nicht kategorisierte Apps in einen Ordner „Nicht kategorisiert“ verschieben**, um alle Apps und Desktops ohne Kategorien in einen separaten Ordner **Nicht kategorisiert** zu verschieben.



Kategorienansicht ausblenden

Um die Ansicht **Kategorien** auszublenden, deaktivieren Sie auf der Registerkarte „Erweiterte Einstellungen“ Ordneransicht aktivieren.

Kategorieeinstellungen konfigurieren PowerShell

Um PowerShell zum Aktivieren oder Deaktivieren der Kategorienansicht zu verwenden, rufen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `EnableAppsFolderView` auf.

Um PowerShell zum Ändern der Kategorienansicht zu verwenden, rufen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `CategoryViewCollapsed` auf.

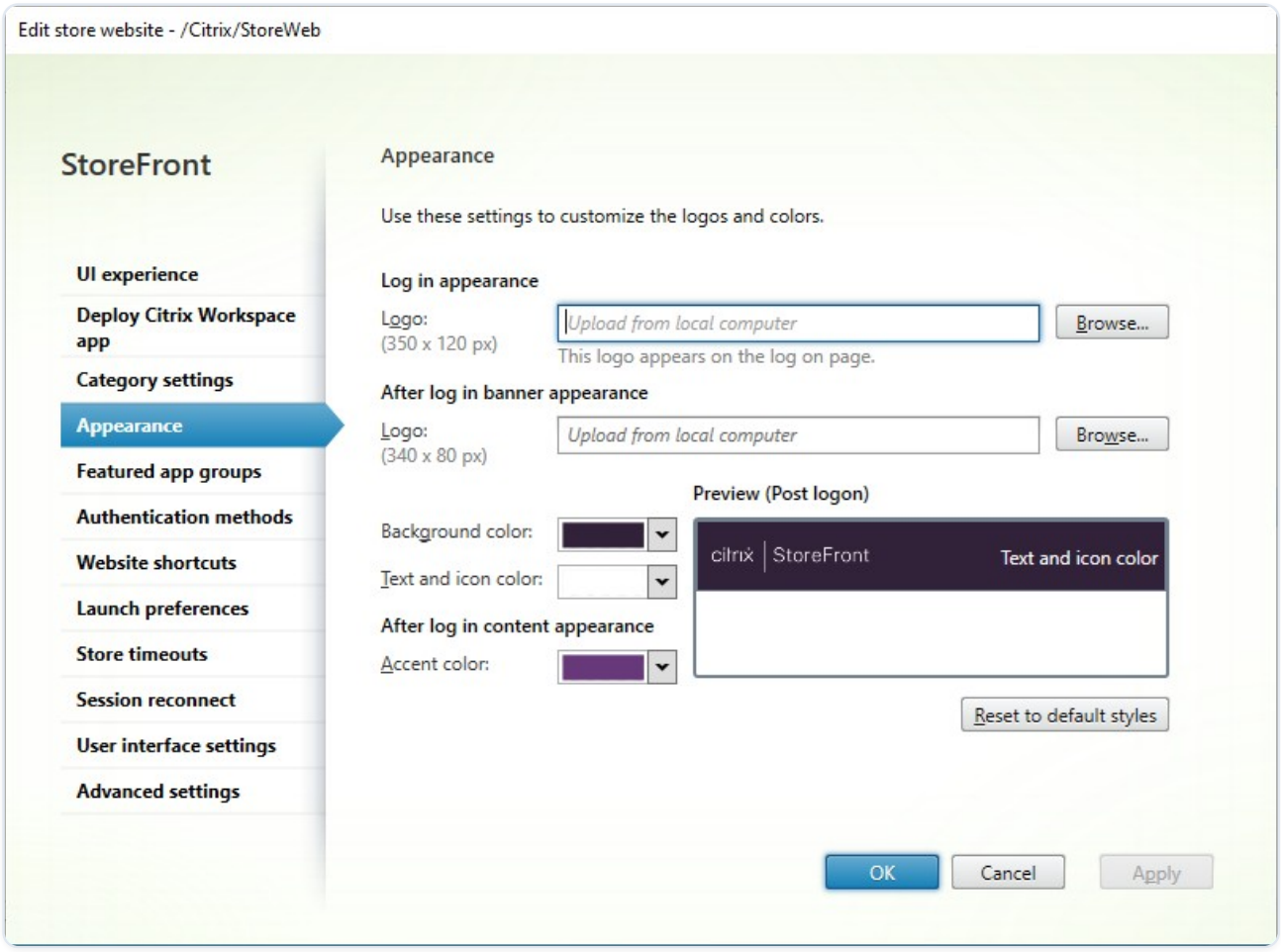
Erscheinungsbild

Sie können das Logo und die Farben Ihrer Store-Website ändern.

Logo und Farben bearbeiten

Um das Erscheinungsbild anzupassen, gehen Sie zu Store-Website bearbeiten und wählen Sie die Registerkarte **Erscheinungsbild anpassen**. Sie können Folgendes ändern:

- **Anmelde-Branding-Logo** – Das Logo, das auf dem Anmeldebildschirm angezeigt wird. Es wird nicht angezeigt, wenn Sie sich über ein Citrix Gateway oder mit der Citrix Workspace-App anmelden. Drücken Sie **Durchsuchen...** und wählen Sie eine Datei vom Typ .jpg, .jpeg, .png, .gif oder .bmp. Es wird empfohlen, ein Bild der Größe 350px x 120px zu verwenden.
- **Header-Branding-Logo**. Das Logo, das nach der Anmeldung in der oberen linken Ecke angezeigt wird. Drücken Sie **Durchsuchen...** und wählen Sie eine Datei vom Typ .jpg, .jpeg, .png, .gif oder .bmp. Es wird empfohlen, ein Bild der Größe 340px x 80px zu verwenden.
- **Hintergrundfarbe** – Die Hintergrundfarbe des Navigationsbereichs oben auf der Seite.
- **Text- und Symbolfarbe** – Die Farbe für Symbole im Navigationsbereich oben auf der Seite.
- **Akzentfarbe** – Die Farbe, die verwendet wird, um anzuzeigen, welches Element den Fokus hat, sowie für Schaltflächen und Links.



Die Standardeinstellungen variieren je nachdem, ob Sie die klassische oder moderne Erfahrung verwenden, aber alle Anpassungen gelten für beide.

Logo und Farben mit PowerShell bearbeiten

Verwenden Sie PowerShell und führen Sie das Cmdlet Set-STFWebReceiverSiteStyle aus.

Erscheinungsbild auf Standard zurücksetzen

Drücken Sie **Auf Standardstil zurücksetzen**, um Logos und Farben auf die Standardeinstellungen zurückzusetzen.

Erscheinungsbild mit PowerShell auf Standard zurücksetzen

Führen Sie mit PowerShell das Cmdlet Clear-STFWebReceiverSiteStyle aus.

Anpassung mit Javascript und CSS

Wenn Sie die klassische Oberfläche verwenden, können Sie die Website mithilfe der StoreFront Client UI Customization API weiter anpassen. Dies gilt nicht bei Verwendung der modernen Oberfläche.

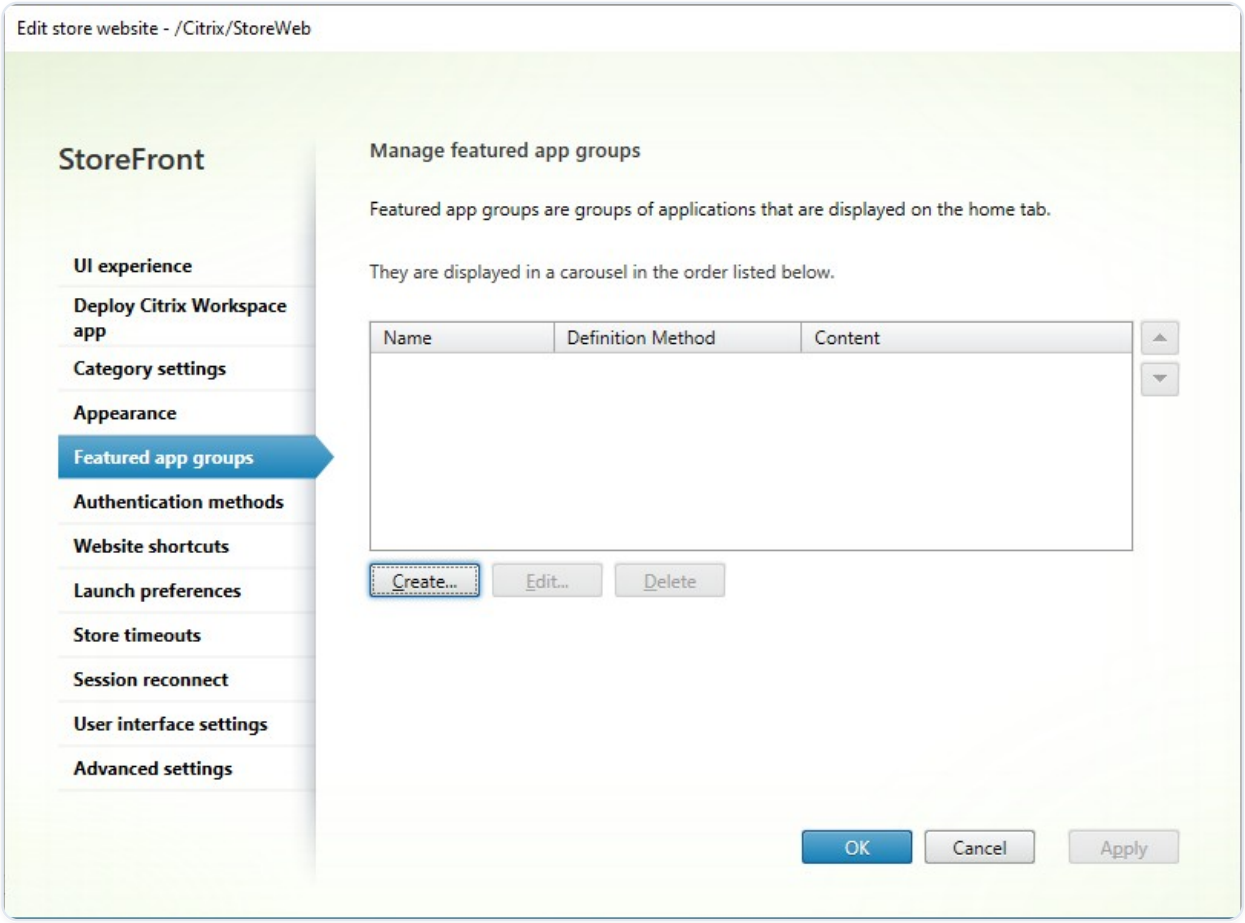
Empfohlene App-Gruppen

> **Hinweis:**
>
> Diese Funktionalität ist nur über die einheitliche Oberfläche verfügbar.

> Sie können produktbezogene empfohlene App-Gruppen für Ihre Endbenutzer erstellen, die sich auf eine bestimmte Kategorie beziehen oder in diese passen. Sie können beispielsweise eine empfohlene App-Gruppe der Vertriebsabteilung erstellen, die Anwendungen enthält, die von dieser Abteilung verwendet werden. Sie können empfohlene Apps in der StoreFront-Verwaltungskonsole definieren, indem Sie Anwendungsnamen oder Schlüsselwörter oder Anwendungskategorien verwenden, die in der Studio-Konsole definiert wurden.

Empfohlene App-Gruppe erstellen

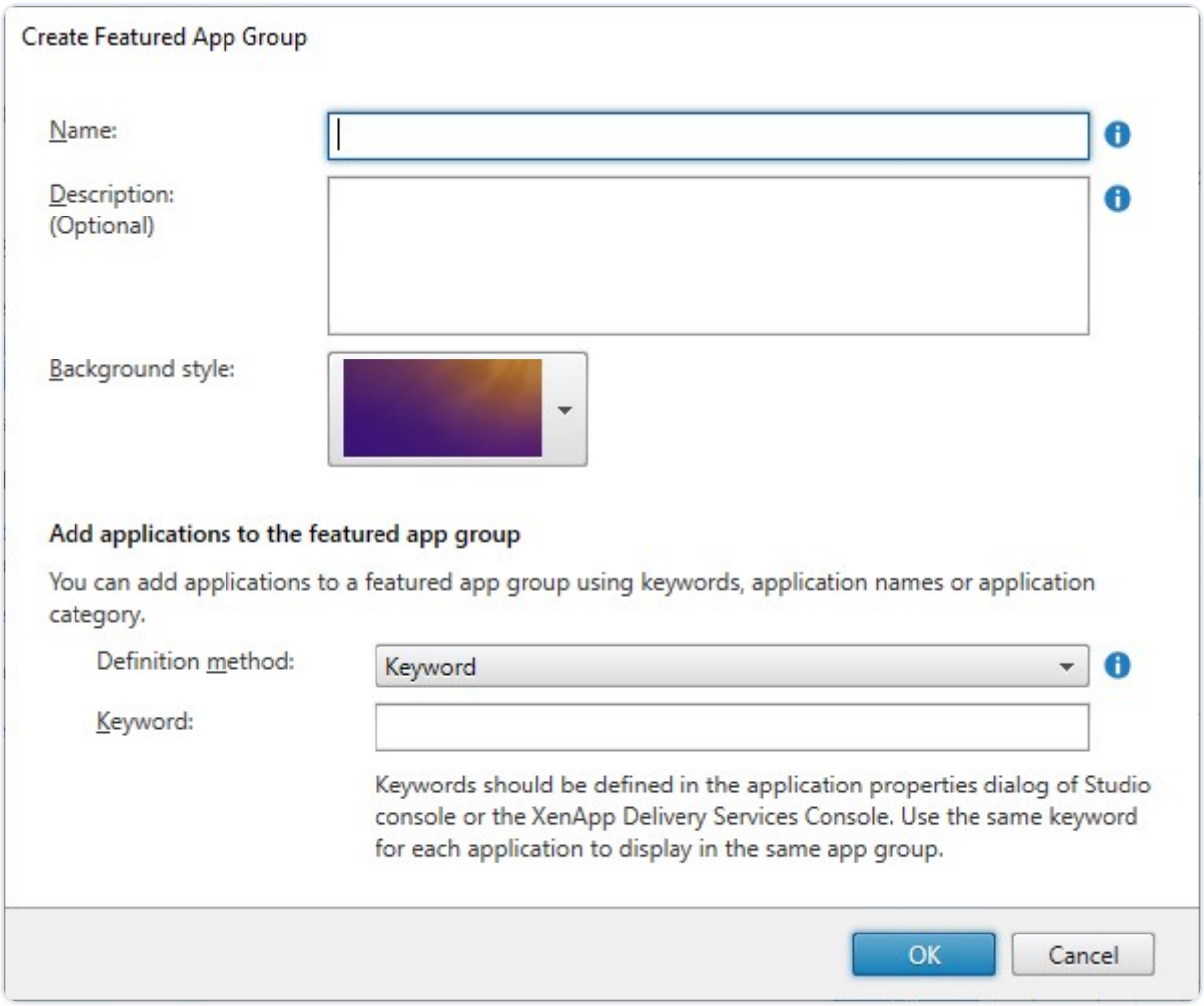
1. Wählen Sie im Bildschirm Website des Stores bearbeiten die Registerkarte **Empfohlene App-Gruppen** aus.



2. Klicken Sie auf **Erstellen**, um eine neue empfohlene App-Gruppe zu definieren.

3. Geben Sie einen Namen für die empfohlene App-Gruppe, eine Beschreibung (optional), einen Hintergrund und die Methode an, mit der Sie die empfohlenen App-Gruppen definieren. Sie können Schlüsselwörter, Anwendungsnamen oder eine Anwendungskategorie auswählen.

OPTION	BESCHREIBUNG
Schlüsselwörter	Gleicht Apps basierend auf dem Schlüsselwort ab, das in Studio durch das Einfügen von Schlüsselwörtern in die App-Beschreibung definiert wurde, zum Beispiel „Zum Senden und Empfangen von E-Mails verwenden SCHLÜSSELWÖRTER:Zusammenarbeit“
Anwendungskategorie	Gleicht Apps in einer bestimmten Anwendungskategorie ab, die in Studio eingegeben wurde.
Anwendungsnamen	Verwenden Sie den Anwendungsnamen, um die empfohlene App-Gruppe zu definieren. Alle Anwendungsnamen, die dem hier im Dialogfeld „Empfohlene App-Gruppe erstellen“ eingegebenen Namen entsprechen, werden in die empfohlene App-Gruppe aufgenommen. StoreFront unterstützt keine Platzhalter in Anwendungsnamen. Die Übereinstimmung ist nicht Groß-/Kleinschreibung-sensitiv, aber es werden ganze Wörter abgeglichen. Wenn Sie beispielsweise Excel eingeben, gleicht StoreFront eine veröffentlichte App namens Microsoft Excel 2013 ab, aber die Eingabe von `Exc` gleicht nichts ab.

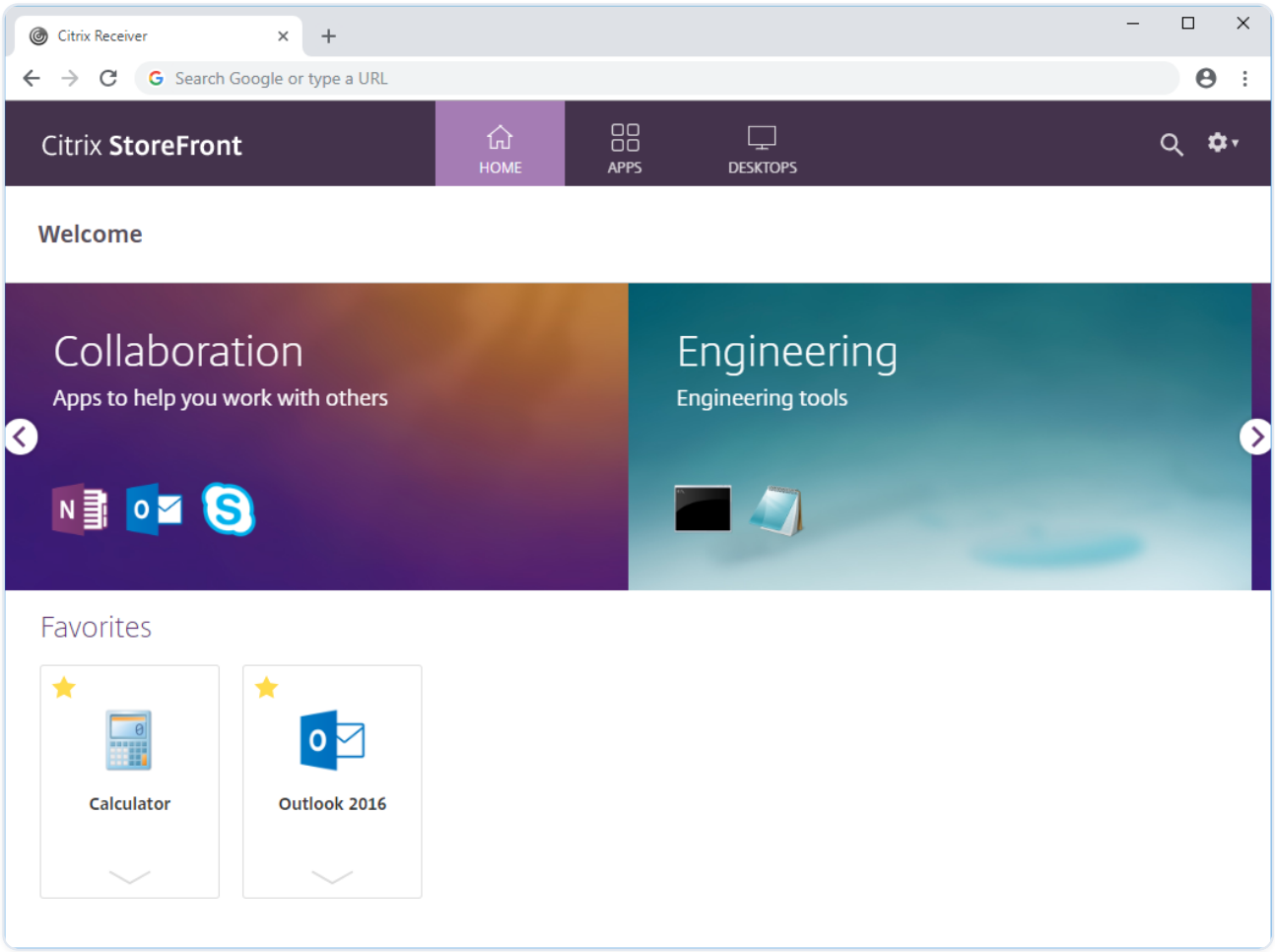


4. Klicken Sie auf **OK**

Beispiel:

Wir haben zwei Featured App-Gruppen erstellt:

- Collaboration – Erstellt durch Abgleich von Apps in der Kategorie **Collaboration** in Studio.
- Engineering – Erstellt durch Benennung der App-Gruppe und Angabe einer Sammlung von App-Namen.



Featured App-Gruppe mit PowerShell erstellen

Um eine Featured App-Gruppe mit PowerShell hinzuzufügen, führen Sie das Cmdlet New-STFWebReceiverFeaturedAppGroup aus.

Featured App-Gruppe bearbeiten

Wählen Sie im Bildschirm Store-Website bearbeiten die Registerkarte **Featured App-Gruppen**. Wählen Sie die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten...**

Featured App-Gruppe mit PowerShell bearbeiten

Um eine Featured App-Gruppe mit PowerShell zu ändern, führen Sie das Cmdlet Set-STFWebReceiverFeaturedAppGroup aus.

Featured App-Gruppe löschen

Wählen Sie im Bildschirm Store-Website bearbeiten die Registerkarte **Featured App-Gruppen**. Wählen Sie die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie auf **Löschen...**

Featured App-Gruppe mit PowerShell löschen

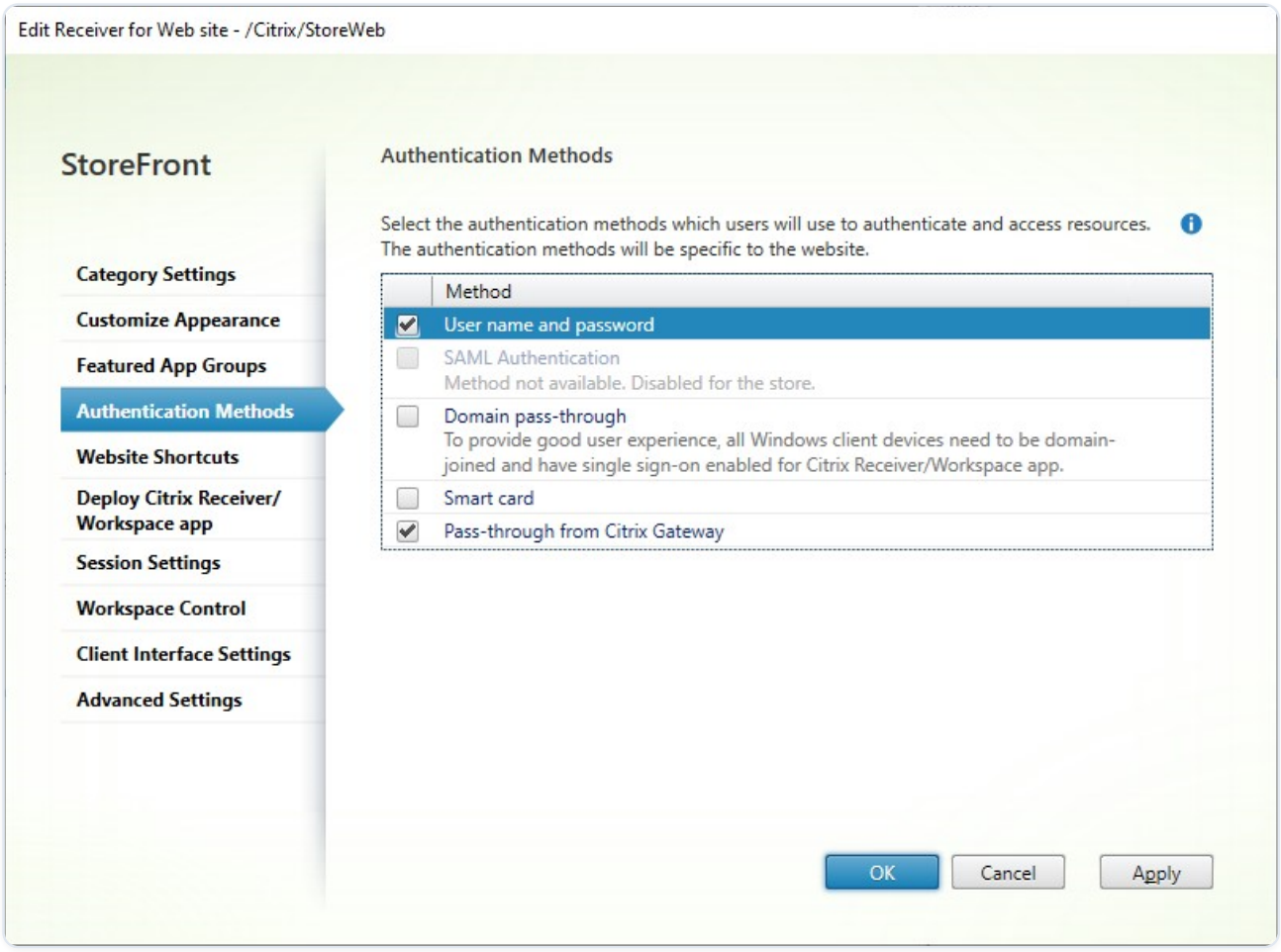
Um eine Featured App-Gruppe mit PowerShell zu löschen, verwenden Sie das Cmdlet Remove-STFWebReceiverFeaturedAppGroup, und um alle Featured App-Gruppen zu löschen, verwenden Sie das Cmdlet Clear-STFWebReceiverFeaturedAppGroup.

Authentifizierungsmethoden

Informationen zum Konfigurieren der für einen Store verfügbaren Authentifizierungsmethoden finden Sie unter Authentifizierung konfigurieren. Sie können einige dieser Einstellungen für eine bestimmte Website überschreiben. Diese Überschreibungen gelten nur, wenn Benutzer den Store in einem Webbrowser öffnen. Die lokal installierte Citrix Workspace-App verwendet die Einstellungen des Stores und nicht die der Website.

> **Warnung:**
>
> Jedes Mal, wenn Sie die Authentifizierungsmethoden für einen Store ändern, werden die Einstellungen für alle Websites dieses Stores überschrieben, sodass alle Änderungen erneut angewendet werden müssen.

> Um Authentifizierungsmethoden bei Verwendung eines Webbrowsers zu ändern, gehen Sie zu Store-Website bearbeiten und wählen Sie die Registerkarte **Authentifizierungsmethoden**.



- Aktivieren Sie das Kontrollkästchen **Active Directory-Benutzername und -Kennwort**, damit sich alle Benutzer durch Eingabe ihres Benutzernamens und Kennworts authentifizieren können. Siehe Authentifizierung mit Benutzername und Kennwort. Diese Option ist nur verfügbar, wenn sie für den Store aktiviert ist.
- Aktivieren Sie das Kontrollkästchen **SAML-Authentifizierung**, um die Integration mit einem SAML-Identitätsanbieter zu ermöglichen. Siehe SAML-Authentifizierung. Diese Option ist nur verfügbar, wenn sie für den Store aktiviert wurde.
- Wählen Sie **Domänen-Passthrough**, um das Passthrough von Active Directory-Domänenanmeldeinformationen von Benutzergeräten zu ermöglichen. Siehe Domänen-Passthrough-Authentifizierung. Diese Option ist nur verfügbar, wenn sie für den Store aktiviert wurde.
- Wählen Sie **Smartcard**, um die Smartcard-Authentifizierung zu ermöglichen. Siehe Smartcard-Authentifizierung.
- Wählen Sie **Passthrough von Citrix Gateway**, um die Passthrough-Authentifizierung von Citrix Gateway zu ermöglichen. Aktivieren Sie diese Option, wenn Benutzer über ein Citrix Gateway mit aktivierter Authentifizierung eine Verbindung zu StoreFront herstellen, um zu

vermeiden, dass sich Benutzer ein zweites Mal bei StoreFront authentifizieren müssen. Siehe Passthrough von Citrix Gateway.

Wenn Sie mehrere Authentifizierungsmethoden auswählen, wird die Standardauthentifizierungsmethode für Benutzer, die sich direkt bei StoreFront™ anmelden, gemäß der folgenden Reihenfolge bestimmt:

1. Domänen-Passthrough
2. Smartcard
3. SAML
4. Benutzername und Kennwort

Der Benutzer kann zu einer anderen Authentifizierungsmethode wechseln. Eine Ausnahme ist, dass Benutzer, wenn Sie sowohl SAML- als auch Benutzername- und Kennwort-Authentifizierung konfigurieren, nicht zur Benutzername- und Kennwort-Authentifizierung wechseln können.

Wenn Benutzer sich abmelden, können sie wählen, ob die Authentifizierungsmethode für das nächste Mal gespeichert werden soll.

Konfigurieren mit PowerShell

Um die verfügbaren Authentifizierungsmethoden mithilfe der PowerShell zu konfigurieren, führen Sie das Cmdlet Set-STFWebReceiverAuthenticationMethods aus.

Website-Verknüpfungen

> **Hinweis:**

> Diese Funktionalität ist nur mit der klassischen Oberfläche verfügbar.

> Verwenden Sie Website-Verknüpfungen, um Benutzern schnellen Zugriff auf Desktops und Anwendungen von vertrauenswürdigen Websites im internen Netzwerk zu ermöglichen. Sie können URLs für Ressourcen generieren und diese Links auf Ihren Websites einbetten. Benutzer klicken auf einen Link und werden zur Store-Website weitergeleitet, wo sie sich anmelden, falls sie dies noch nicht getan haben. Die Website startet die Ressource automatisch.

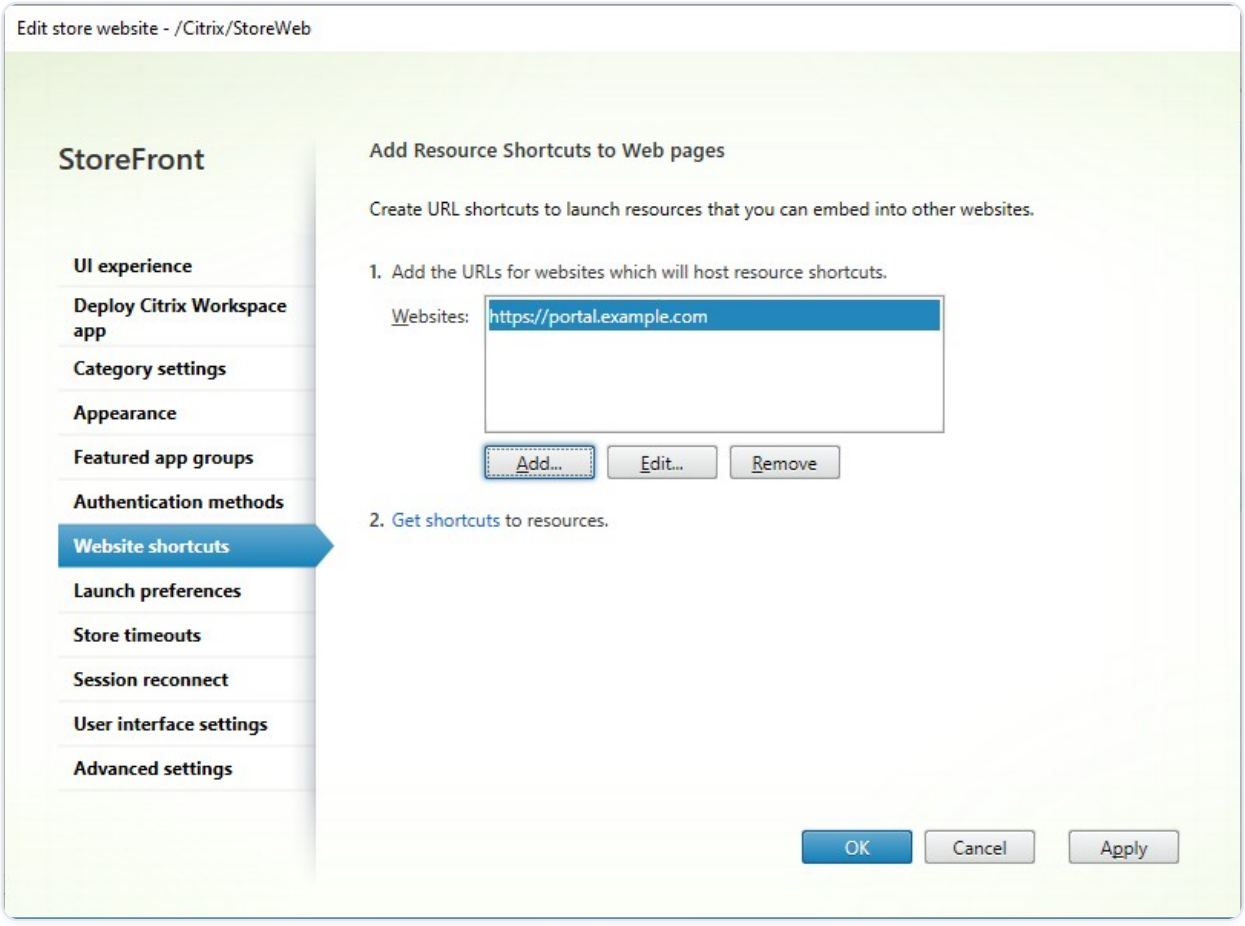
Bevor Sie Ressourcenverknüpfungen generieren können, müssen Sie die URLs der Host-Websites zur Liste der *vertrauenswürdigen URLs* hinzufügen, entweder über die Citrix StoreFront-Verwaltungskonsole oder über PowerShell.

Standardmäßig warnt StoreFront Benutzer, wenn sie versuchen, Ressourcenverknüpfungen von nicht vertrauenswürdigen Websites zu starten, aber Benutzer können die Ressource trotzdem starten. Um diese Warnungen zu unterbinden, deaktivieren Sie unter Erweiterte Einstellungen die Option Zur Bestätigung bei nicht vertrauenswürdigen Verknüpfungen auffordern.

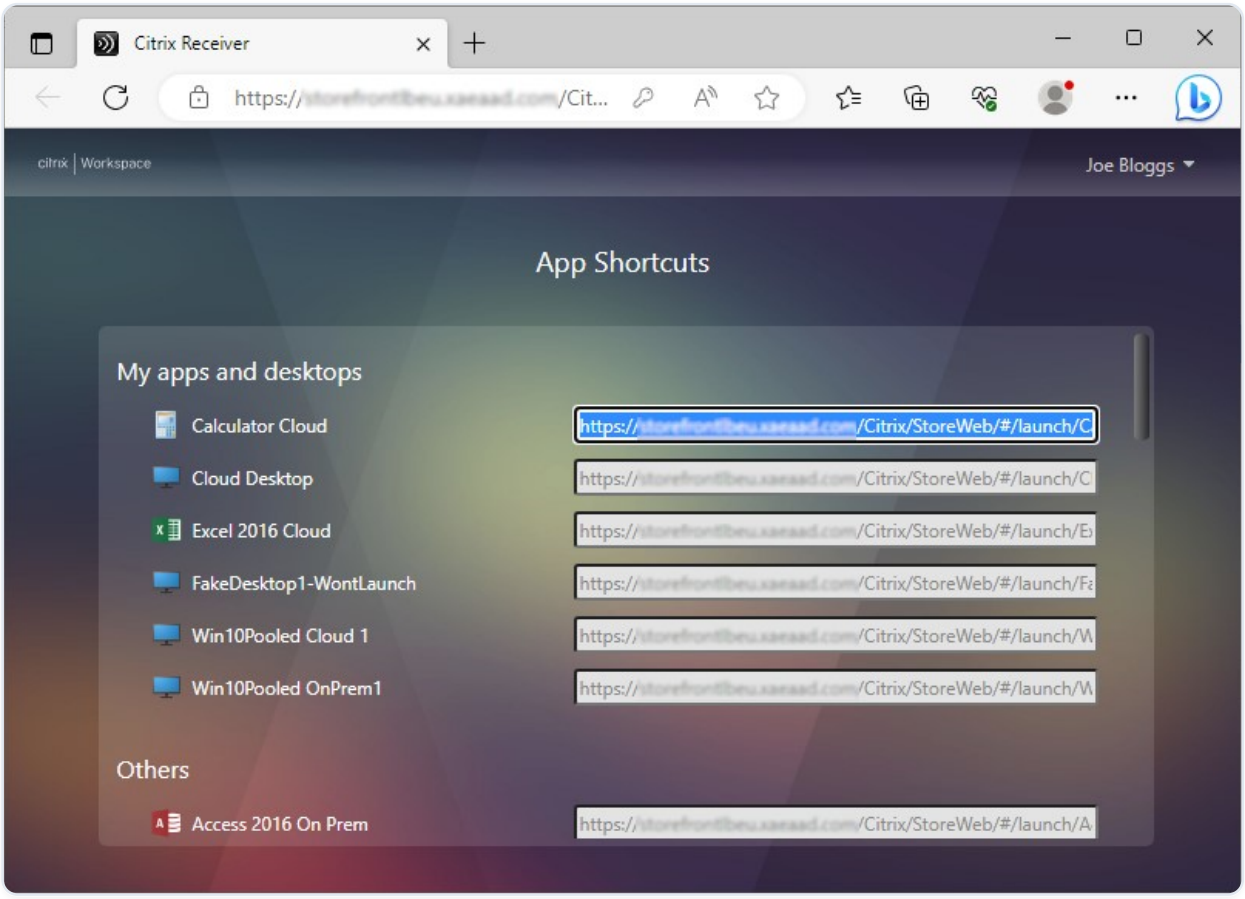
Aus Sicherheitsgründen werden Internet Explorer-Benutzer möglicherweise aufgefordert zu bestätigen, dass sie über Verknüpfungen aufgerufene Ressourcen starten möchten. Weisen Sie Ihre Benutzer an, den FQDN des StoreFront-Servers den Zonen „Lokales Intranet“ oder „Vertrauenswürdige Sites“ in Internet Explorer hinzuzufügen, um diesen zusätzlichen Schritt zu vermeiden.

Vertrauenswürdige Websites über die Verwaltungskonsole hinzufügen

1. Wählen Sie auf dem Bildschirm Store-Website bearbeiten die Registerkarte **Website-Verknüpfungen** aus.



2. Klicken Sie auf **Hinzufügen**, um die URL für eine Website einzugeben, auf der Sie Verknüpfungen hosten möchten. URLs müssen im Format *http\[s\]://hostname\[:port\]* angegeben werden, wobei Hostname der vollqualifizierte Domänenname des Website-Hosts ist 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 bestimmten Seiten auf der Website sind nicht erforderlich. Um eine URL zu ändern, 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**, um die URL für eine Website zu löschen, auf der Sie keine Verknüpfungen mehr zu Ressourcen hosten möchten, die über die Citrix Receiver für Web-Site verfügbar sind.
3. Klicken Sie auf **Verknüpfungen abrufen** und kopieren Sie die URLs, die Sie für Ihre Website benötigen.

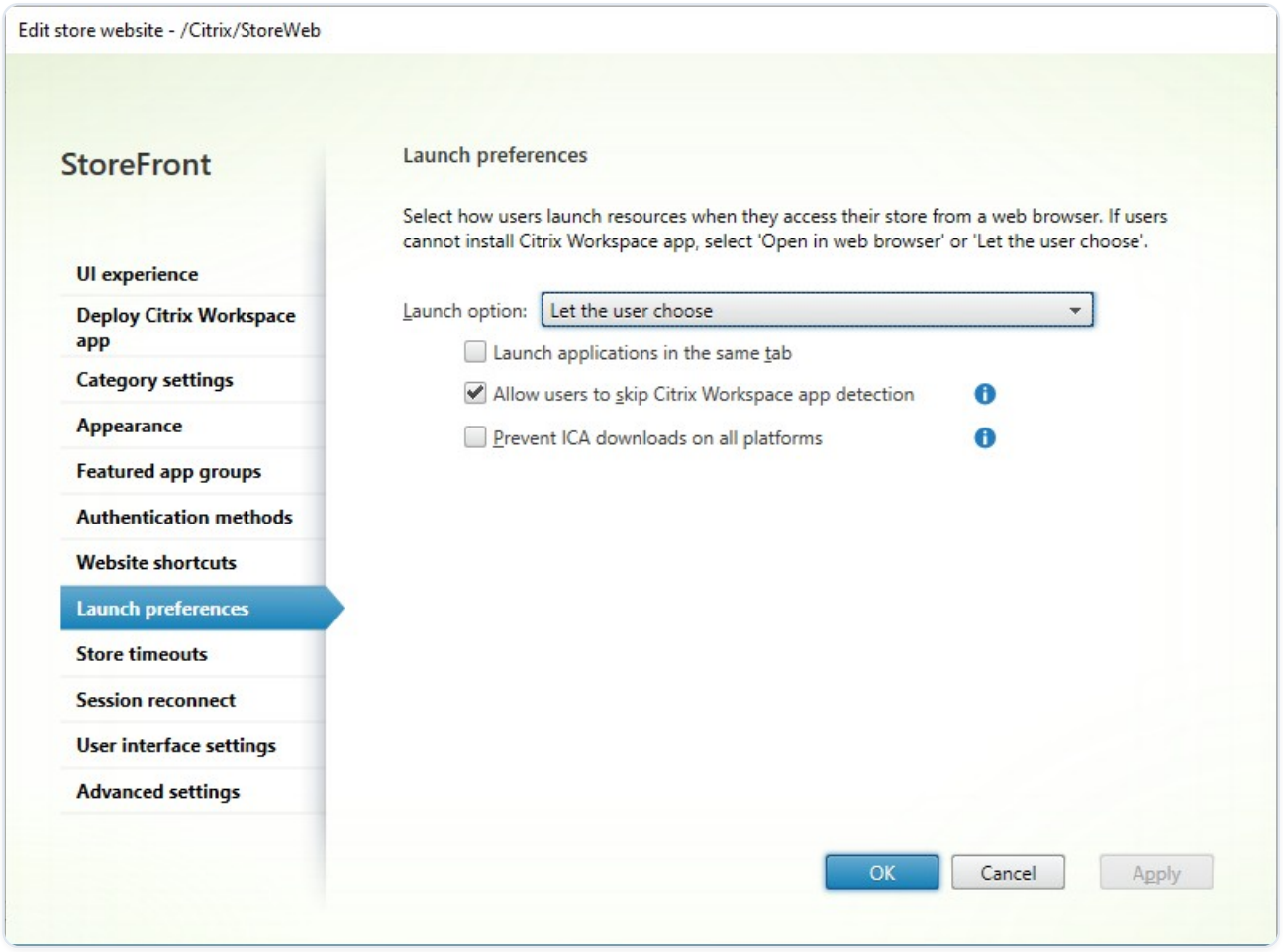


Vertrauenswürdige Websites über PowerShell hinzufügen

Um vertrauenswürdige URLs mit PowerShell hinzuzufügen, führen Sie das Cmdlet Set-STFWebReceiverApplicationShortcuts aus.

Starteinstellungen

Unter **Starteinstellungen** können Sie auswählen, welche Startoptionen den Benutzern zur Verfügung stehen, wenn sie ihren Store in einem Webbrowser öffnen. Diese Einstellungen gelten nicht bei Verwendung der Citrix Workspace-App. Weitere Informationen zu Startoptionen finden Sie unter Benutzerzugriffsoptionen.



Um Startoptionen zu ändern, wechseln Sie zu Store-Website bearbeiten und wählen Sie die Registerkarte **Starteinstellungen**.

Startoption

Sie können aus einer der folgenden Optionen wählen:

- Wählen Sie **Im Webbrowser öffnen**, wenn der Benutzer Ressourcen immer über einen Webbrowser aufrufen soll, ohne den Benutzer zum lokalen Herunterladen und Installieren der Citrix Workspace-App aufzufordern. Wenn diese Option ausgewählt ist, greifen Workspace for HTML5-Benutzer immer direkt über ihre Browser auf Ressourcen zu.
- Wählen Sie **Benutzer wählen lassen**, wenn die Store-Website den Benutzer zum lokalen Herunterladen und Installieren der Citrix Workspace-App auffordern soll, aber auf den Zugriff auf Ressourcen über einen Browser zurückgreifen soll, wenn die Citrix Workspace-App nicht

installiert werden kann. Benutzer ohne Citrix Workspace-App werden jedes Mal, wenn sie sich bei der Site anmelden, zum Herunterladen und Installieren aufgefordert.

- Wählen Sie **In Citrix Workspace-App öffnen**, wenn die Site immer über eine lokal installierte Citrix Workspace-App auf Ressourcen zugreifen soll. Benutzer werden aufgefordert, die entsprechende Citrix Workspace-App für ihre Plattform herunterzuladen und zu installieren. Benutzer können weiterhin über einen Webbrowser auf den Store zugreifen, aber wenn sie eine Ressource starten, wird diese in der lokal installierten Workspace-App geöffnet.

Anwendungen in derselben Registerkarte starten

Wenn Sie **Im Webbrowser öffnen** oder **Benutzer wählen lassen** ausgewählt haben, öffnen im Browser gestartete Ressourcen standardmäßig eine neue Browser-Registerkarte. Wenn Ihre Ressourcen in derselben Registerkarte geöffnet werden sollen und den Store ersetzen, wählen Sie **Anwendungen in derselben Registerkarte starten**.

In der modernen Benutzeroberfläche ist diese Einstellung nicht verfügbar, und Ressourcen werden immer in einer neuen Registerkarte geöffnet.

Benutzern erlauben, die Erkennung der Citrix Workspace™-App zu überspringen

Wenn Endbenutzer zum ersten Mal einen Store in ihrem Browser öffnen, versucht die Website, die lokal installierte App mithilfe des Citrix Workspace Launchers zu erkennen. Wenn ein Benutzer anschließend eine Ressource startet, kommuniziert der Citrix Workspace Launcher mit der lokal installierten Citrix Workspace-App. Wenn Benutzer die Option **Erkennung überspringen** auswählen, wird der Client-Erkennungsprozess übersprungen. Wenn der Benutzer eine Ressource startet, wird infolgedessen eine `.ica`-Datei heruntergeladen, die Benutzer mit ihrer lokal installierten Citrix Workspace-App öffnen können. Dies unterstützt keine Funktionen wie die Sitzungswiederverbindung.

Die heruntergeladene `.ica`-Datei kann ein Sicherheitsrisiko darstellen. Citrix empfiehlt, die Option **Benutzern erlauben, die Erkennung der Citrix Workspace-App zu überspringen** zu deaktivieren.

ICA®-Downloads auf allen Plattformen verhindern

Dies bietet eine zusätzliche Schutzebene, indem `.ica`-Downloads auf allen Plattformen vollständig blockiert werden. Da der Citrix Workspace Launcher auf ChromeOS nicht verfügbar ist, müssen ChromeOS-Benutzer entweder **Webbrowser verwenden** auswählen, falls verfügbar, oder ihren Store zu ihrer lokal installierten Citrix Workspace-App hinzufügen.

> **Wichtig:**

> Diese Option sollte nicht ausgewählt werden, wenn auch **Benutzern erlauben, die Erkennung der Citrix Workspace-App zu überspringen** ausgewählt ist.

Citrix Web-Erweiterung

Standardmäßig wird beim ersten Anmelden eines Benutzers über einen Webbrowser oder beim Aufrufen der **Kontoeinstellungen** und Auswählen von **Startmethode ändern** überprüft, ob die Citrix Web Extension installiert ist. Wird sie gefunden, wird sie verwendet, um die Citrix Workspace-App zu erkennen und virtuelle Apps und Desktops zu starten. Dies bietet die beste und sicherste Erfahrung, indem Browser-Eingabeaufforderungen und das Herunterladen von ICA-Dateien vermieden werden. Der Erkennungsprozess dauert bis zu 6 Sekunden (2 Versuche mit 3s Timeouts), um Situationen zu berücksichtigen, in denen die Webseite langsam geladen wird, z. B. aufgrund geringer Bandbreite oder leistungsschwacher Geräte. Wird die Citrix Web Extension daher nicht erkannt, kann es für Erstbenutzer zu einer Verzögerung von 6 Sekunden kommen. Dies gilt nicht bei Verwendung der modernen Erfahrung oder anderer Webbrowser als Chrome und Edge. Sie können konfigurieren, ob die Website die Citrix Web Extension verwendet und welche Timeouts dabei zum Einsatz kommen.

Um die aktuelle Konfiguration anzuzeigen, verwenden Sie das PowerShell-Cmdlet Get-STFWebReceiverPluginAssistant. Beispiel:

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"

Get-STFWebReceiverPluginAssistant -WebReceiverService $receiver
```

Um die Konfiguration zu ändern, verwenden Sie das Cmdlet Set-STFWebReceiverPluginAssistant mit den Parametern `BrowserExtensionEnabled`, `BrowserExtensionTimeout` und `BrowserExtensionRetries`. Beispiel zum Deaktivieren von Citrix Web Extensions:

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"

Set-STFWebReceiverPluginAssistant -WebReceiverService $receiver
-BrowserExtensionEnabled $False
```

Oder um das Timeout auf 2s mit nur einem Versuch zu reduzieren:

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"
```

```
Set-STFWebReceiverPluginAssistant -WebReceiverService $receiver
-BrowserExtensionTimeout 2000 -BrowserExtensionRetries 1
```

Eine Reduzierung des Timeouts gegenüber dem Standardwert kann dazu führen, dass die Website die Citrix Web Extensions nicht erkennt.

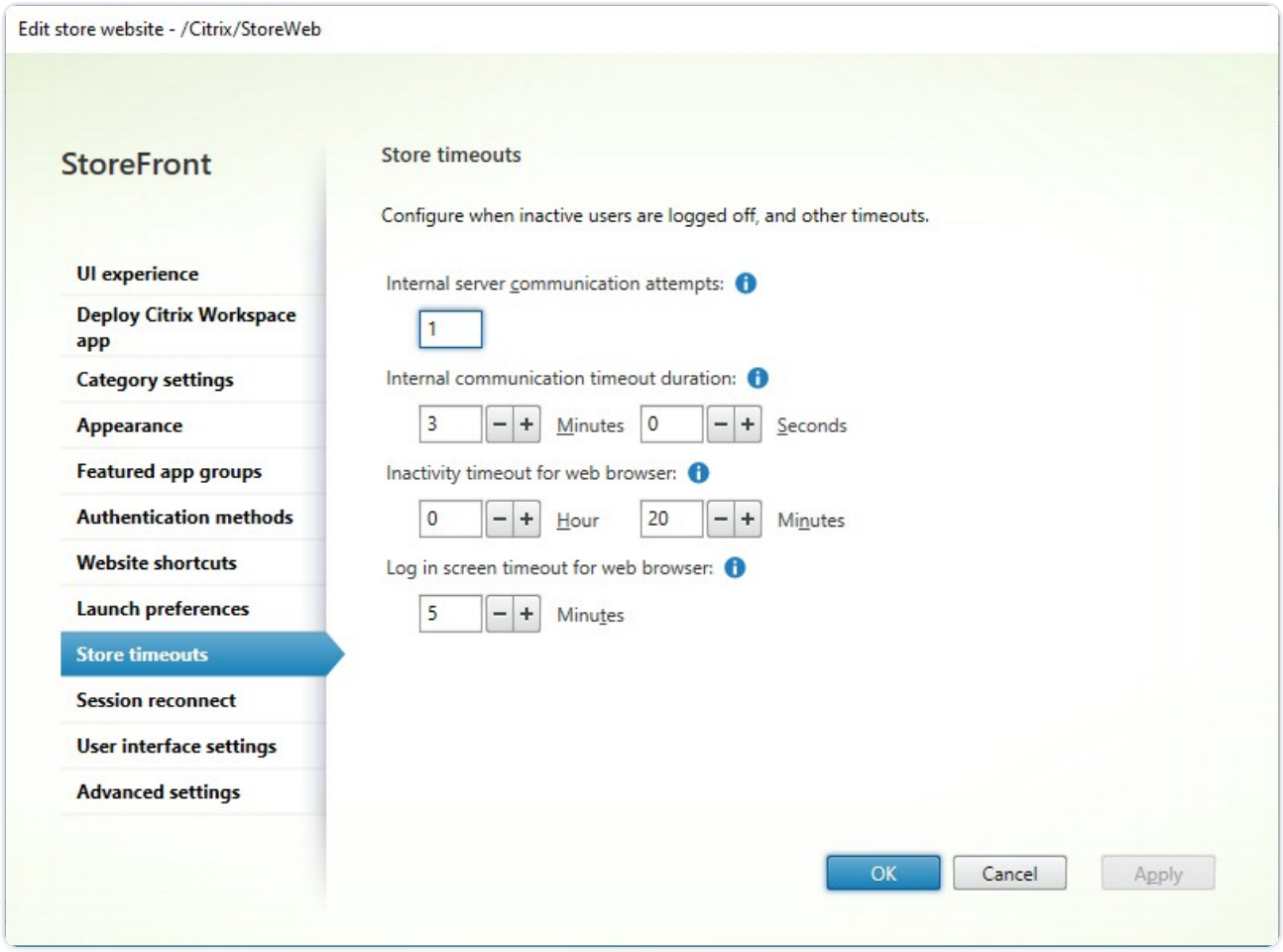
PowerShell

Um diese Einstellungen mit PowerShell zu konfigurieren, führen Sie das Cmdlet Set-STFWebReceiverPluginAssistant aus.

Um Prevent ICA Downloads zu konfigurieren, führen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `PreventIcaDownloads` aus.

Store-Timeouts

Um Store-Timeouts zu ändern, gehen Sie zum Bildschirm Store-Website bearbeiten und wählen Sie die Registerkarte **Store-Timeouts**.



Interne Server-Kommunikationsversuche

Die Anzahl der Versuche für Aufrufe zwischen dem Webproxy und den Store-Diensten, intern zu StoreFront. Normalerweise ist es nicht erforderlich, diese Einstellung zu ändern.

Dauer des Timeouts für interne Kommunikation

Die zulässige Zeit für Aufrufe zwischen dem Webproxy und den Store-Diensten, intern zu StoreFront. Normalerweise ist es nicht erforderlich, diese Einstellung zu ändern.

Inaktivitätstimeout für Webbrowser

Beim Zugriff auf einen StoreFront-Store über einen Webbrowser läuft die Sitzung nach der angegebenen Inaktivitätszeit ab und der Benutzer wird abgemeldet. Das Aktualisieren der Webseite oder das Ausführen einer Aktion auf einer Ressource verlängert die Sitzung. Benutzeraktionen, die keine Netzwerkaktivität zur Folge haben, wie z. B. das Navigieren zwischen Registerkarten, verlängern die Sitzung nicht.

Das Timeout wird sowohl auf dem Client als auch auf dem Server erzwungen. Kurz vor Ablauf der Sitzung fordert die Benutzeroberfläche den Benutzer auf, die Sitzung zu verlängern. Eine Minute vor dem Sitzungs-Timeout benachrichtigt die Benutzeroberfläche StoreFront und gegebenenfalls Citrix Gateway, sich abzumelden. Dies soll dem Client ermöglichen, sich sauber abzumelden, bevor das Server-Timeout abläuft. Wenn das Sitzungs-Timeout auf 1 Minute eingestellt ist, meldet sich der Client nach 30 Sekunden ab. Dies hat keine Auswirkungen auf die lokal installierte Citrix Workspace-App.

Wenn Sie das Sitzungs-Timeout so ändern, dass es länger ist als das Gateway-Sitzungs-Timeout, müssen Sie das Gateway-Sitzungs-Timeout entsprechend erhöhen. Wenn Sie das Sitzungs-Timeout so ändern, dass es länger ist als die Lebensdauer des Authentifizierungstokens oder die Maximale Token-Lebensdauer, werden diese automatisch an das Sitzungs-Timeout angepasst.

PowerShell

Um das Timeout zu konfigurieren, verwenden Sie das Cmdlet Set-STFWebReceiverService mit dem Parameter `-SessionStateTimeout`. Zum Beispiel, um das Timeout für die Website '/Citrix/StoreWeb' auf 30 Minuten einzustellen:

```
$rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'

Set-STFWebReceiverService $rfw -SessionStateTimeout 30
```

Anmelde-Timeout

Wenn Sie sich im Webbrowser auf dem Anmeldebildschirm befinden, läuft die Anmeldung nach einer gewissen Zeit ab und es wird eine Meldung an den Benutzer angezeigt. Der Benutzer kann auf **Anmelden** klicken, um zum Anmeldebildschirm zurückzukehren.

Lebensdauer des Authentifizierungstokens

Wenn ein Benutzer über einen Browser auf einen StoreFront-Store zugreift, wird er standardmäßig nach acht Stunden abgemeldet, unabhängig von jeglicher Aktivität. Dies hat keine Auswirkungen auf lokal installierte Citrix Workspace-Apps. Der Wert wird nicht in der Verwaltungskonsole angezeigt.

Um den aktuellen Wert anzuzeigen, verwenden Sie Get-STFWebReceiverAuthenticationMethods und überprüfen Sie die Eigenschaft `TokenLifeTime`. Zum Beispiel:

```
$rfweb=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$rfauth = Get-STFWebReceiverAuthenticationMethods -WebReceiverService
$rfweb

$rfauth.TokenLifeTime.ToString()
```

Um das Timeout mit PowerShell festzulegen, verwenden Sie das Cmdlet Set-STFWebReceiverAuthenticationMethods mit dem Parameter `TokenLifeTime`. Zum Beispiel:

```
$rfweb=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$rfauth = Get-STFWebReceiverAuthenticationMethods -WebReceiverService
$rfweb

Set-STFWebReceiverAuthenticationMethods -WebReceiverService $rfweb
-TokenLifeTime "07:00:00"
```

Wenn Sie das Sitzungs-Timeout auf mehr als 20 Stunden erhöhen, müssen Sie auch die Maximale Token-Lebensdauer des Authentifizierungsdienstes erhöhen.

Citrix Gateway-Timeouts

Weitere Informationen zu Gateway-Timeouts finden Sie unter Gateway-Dokumentation.

Sitzungs-Timeout

Das Sitzungs-Timeout wird angewendet, wenn für die angegebene Zeitspanne keine Netzwerkaktivität stattfindet. Das Aktualisieren der Webseite oder das Ausführen einer Aktion auf einer Ressource verlängert die Sitzung. Benutzeraktionen, die keine Netzwerkaktivität zur Folge haben, wie das Navigieren zwischen Registerkarten, verlängern die Sitzung nicht.

Für den Zugriff über einen Webbrowser sollten Sie das **Sitzungs-Timeout** des Citrix Gateways auf einen etwas höheren Wert als das **Sitzungs-Timeout** von StoreFront einstellen. Dies soll sicherstellen, dass, wenn die StoreFront-Sitzung abläuft und das Gateway benachrichtigt, das Gateway sich sauber abmelden kann, bevor seine eigene Sitzung abläuft.

Die lokal installierte Citrix Workspace-App wendet kein Inaktivitätstimeout an, wenn sie mit einem StoreFront-Store verbunden ist. Daher ist das Gateway der einzige Ort, an dem Sie ein Inaktivitätstimeout anwenden müssen. Die App aktualisiert regelmäßig die Liste der Ressourcen. Damit dies wirksam wird, muss das Sitzungs-Timeout kürzer sein als die Aktualisierungsperiode der App. Standardmäßig beträgt die Aktualisierungsperiode der App 60 Minuten. Um dies zu ändern, siehe CTX221465.

Erzwungener Timeout

Auf dem Citrix Gateway können Sie ein **erzwungenes Timeout** festlegen, um die Sitzung nach einer bestimmten Zeit, unabhängig von der Benutzeraktivität, zu trennen.

Maximale Token-Lebensdauer des Authentifizierungsdienstes

Der Authentifizierungsdienst stellt Token aus, die beim Verbinden mit einem Store verwendet werden. Standardmäßig läuft das Token nach 20 Stunden ab, wodurch der Benutzer abgemeldet wird.

Wenn sich der Benutzer über ein Citrix Gateway authentifiziert hat und das StoreFront-Token abläuft, sendet StoreFront eine Anforderung an das Citrix Gateway. Wenn die Sitzung des Gateways noch aktiv ist, liefert es die Anmeldeinformationen, um sich wieder bei StoreFront anzumelden. Wenn Sie dies verhindern möchten, müssen Sie das **erzwungene Timeout** des Gateways so konfigurieren, dass es der maximalen Token-Lebensdauer entspricht.

Normalerweise führt das Inaktivitätstimeout bei der Nutzung des Stores in einem Webbrowser dazu, dass die Sitzung abgemeldet wird, bevor das Token abläuft, sodass die Token-Lebensdauer hauptsächlich für die lokal installierte Citrix Workspace-App relevant ist.

Um die maximale Token-Lebensdauer anzuzeigen, führen Sie das folgende PowerShell-Skript aus:

```
$store = Get-STFStoreService -VirtualPath "[store path]"

$auth = Get-STFAuthenticationService -StoreService $store

$relyingParty = $auth.ProducerService.RelyingParties | Where-Object
{ $_.Id -eq $auth.ProducerService.Id }

$relyingParty.MaxLifetime.ToString()
```

Ersetzen Sie `[store path]` durch den entsprechenden Store-Pfad.

Um die maximale Token-Lebensdauer zu konfigurieren, führen Sie das folgende PowerShell aus:

```
$store = Get-STFStoreService -VirtualPath "[store path]"

$auth = Get-STFAuthenticationService -StoreService $store

$relyingParty = $auth.ProducerService.RelyingParties | Where-Object
{ $_.Id -eq $auth.ProducerService.Id }

$relyingParty.MaxLifetime = "[max lifetime]"

Save-STFService -Service $auth
```

Ersetzen Sie `[store path]` durch den entsprechenden Speicherpfad und `[max lifetime]` durch das gewünschte Timeout. Für Werte bis zu einem Tag verwenden Sie das Format `hh:mm:ss`. Für Werte über einen Tag verwenden Sie das Format `d.hh:mm:ss`.

Sitzungswiederverbindung

Wenn Benutzer zwischen Geräten wechseln, stellt die Sitzungswiederverbindung sicher, dass die von ihnen verwendeten Anwendungen ihnen folgen. Benutzer können mit denselben Anwendungsinstanzen auf mehreren Geräten weiterarbeiten, anstatt alle ihre Anwendungen jedes Mal neu starten zu müssen, wenn sie sich an einem neuen Gerät anmelden. Dies ermöglicht es beispielsweise Klinikern in Krankenhäusern, Zeit zu sparen, wenn sie von Arbeitsplatz zu Arbeitsplatz wechseln und auf Patientendaten zugreifen.

Wenn sich Benutzer anmelden, werden sie automatisch wieder mit allen Anwendungen verbunden, die sie zuvor ausgeführt haben. Stellen Sie sich zum Beispiel einen Benutzer vor, der sich bei einem Store anmeldet und einige Anwendungen startet. Wenn sich der Benutzer dann mit derselben Zugriffsmethode, aber auf einem anderen Gerät, bei demselben Store anmeldet, werden

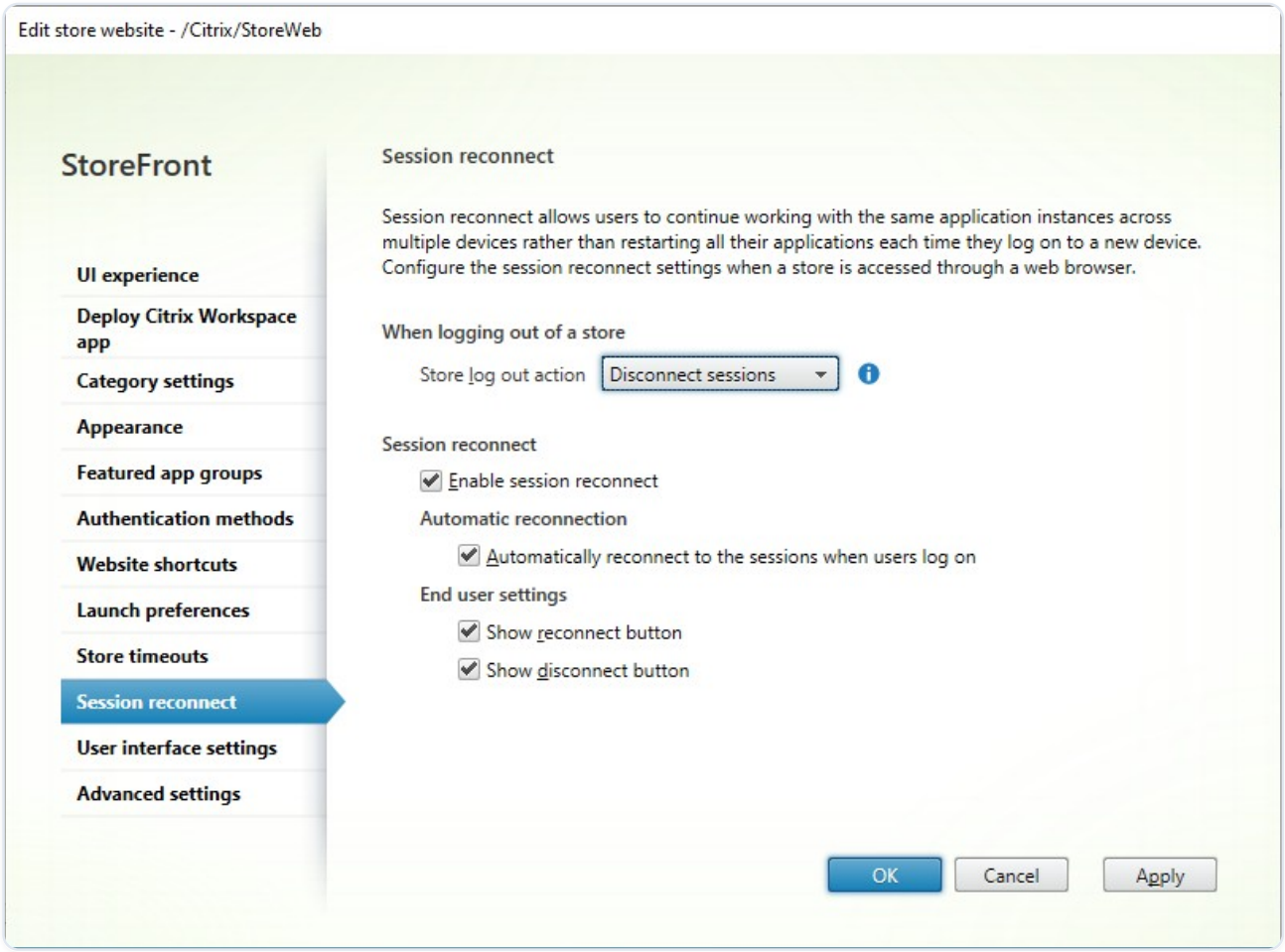
die laufenden Anwendungen automatisch auf das neue Gerät übertragen. Alle Anwendungen, die der Benutzer von einem bestimmten Store aus startet, werden automatisch getrennt, aber nicht heruntergefahren, wenn sich der Benutzer von diesem Store abmeldet. Beim Zugriff auf einen Store über einen Webbrowser muss derselbe Browser zum Anmelden, Starten der Anwendungen und Abmelden verwendet werden.

Sitzungswiederverbindung in einem Webbrowser konfigurieren

Die Einstellungen für die Sitzungswiederverbindung in der StoreFront-Verwaltungskonsole gelten nur beim Zugriff auf den Store über einen Webbrowser. Dies unterliegt den folgenden Anforderungen und Einschränkungen:

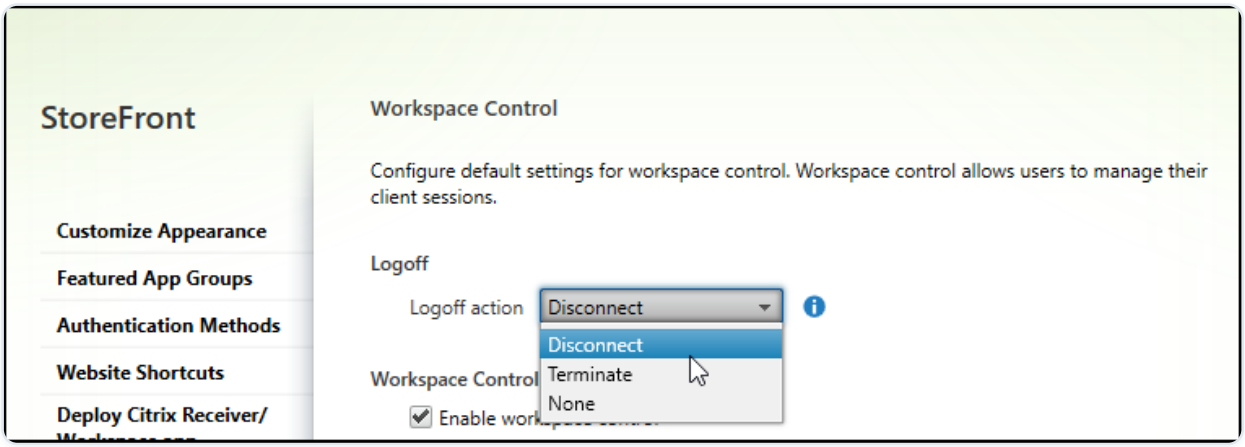
- Die Sitzungswiederverbindung ist nicht verfügbar, wenn der Webbrowser in gehosteten Desktops oder Anwendungen ausgeführt wird.
- Für Benutzer, die von Windows-Geräten auf Websites zugreifen, ist die Sitzungswiederverbindung nur aktiviert, wenn die Site erkennen kann, dass Citrix Workspace-App für Windows auf den Geräten der Benutzer installiert ist oder wenn Ressourcen mit dem Webbrowser geöffnet werden.
- Um die 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 für einen Benutzer auf einer Website, die so konfiguriert ist, dass einzelne Desktops automatisch gestartet werden, wenn sich der Benutzer anmeldet, nur ein Desktop verfügbar ist, werden die Anwendungen dieses Benutzers nicht wieder verbunden, unabhängig von der Konfiguration der Sitzungswiederverbindung.
- Aufgrund von Browserbeschränkungen kann Citrix Workspace launcher nur verwendet werden, um eine App wieder zu verbinden. Um mehrere Apps wieder zu verbinden, sollten Benutzer Citrix web extensions installieren.
- Benutzer müssen sich mit demselben Browser von ihren Anwendungen trennen, der ursprünglich zum Starten der Anwendungen verwendet wurde. Ressourcen, die mit einem anderen Browser gestartet wurden oder lokal vom Desktop oder Startmenü über die Citrix Workspace™-App gestartet wurden, können nicht vom Webclient getrennt oder heruntergefahren werden.
- Die Sitzungswiederverbindung ist nicht verfügbar, wenn Ressourcen innerhalb desselben Browser-Tabs geöffnet werden. Informationen zur Konfiguration finden Sie unter Citrix Workspace app deployment.

Um die Einstellungen für die Sitzungswiederverbindung zu ändern, wenn auf einen Store über einen Webbrowser zugegriffen wird, wählen Sie **Sitzungswiederverbindung** auf dem Bildschirm Edit store website aus.



Konfigurieren Sie die Einstellungen für die Sitzungswiederverbindung wie folgt:

- Geben Sie die **Abmeldeaktion** an. Die Abmeldeaktionen sind wie folgt:
  - **trennen-Sitzungen**: Wenn Sie sich von der Website abmelden, werden die App- und Desktopsitzungen automatisch vom Clientgerät getrennt.
  - **Sitzungen abmelden**: Wenn Sie sich von der Website abmelden, werden die App- und Desktopsitzungen automatisch auf dem Server abgemeldet.
  - **Keine**: Wenn Sie sich von der Website abmelden, bleiben die App- und Desktopsitzungen aktiv.



- **Automatische Wiederverbindung mit den Sitzungen, wenn sich Benutzer anmelden** – Wenn sich der Benutzer anmeldet, werden alle getrennten Sitzungen auf dem lokalen Gerät wiederhergestellt.

Endbenutzereinstellungen

Bei Verwendung der klassischen Oberfläche können Sie Benutzern erlauben, Sitzungen mithilfe der folgenden Einstellungen zu trennen und wiederherzustellen:

- **Schaltfläche „Wiederverbinden“ anzeigen** – Zeigt eine Schaltfläche **Wiederverbinden** an, die alle getrennten Sitzungen auf dem aktuellen Gerät wiederherstellt.
- **Schaltfläche trennen anzeigen** – zeigt eine Schaltfläche **trennen** an, die alle getrennten Sitzungen auf dem aktuellen Gerät wiederherstellt.

Diese Einstellungen haben keine Auswirkung auf die moderne Oberfläche. Verwenden Sie stattdessen den **Aktivitätsmanager**, um Sitzungen zu trennen und wiederherzustellen.

Sitzungswiederverbindung mit PowerShell konfigurieren

Um die Sitzungswiederverbindung mit PowerShell zu konfigurieren, führen Sie das Cmdlet Set-STFWebReceiverUserInterface aus.

Sitzungswiederverbindung in der Workspace-App für Windows konfigurieren

Informationen zum Konfigurieren der Sitzungswiederverbindung in Workspace für Windows finden Sie unter Verwalten der Workspace Control-Wiederverbindung.

Sitzungswiederverbindung in der Workspace-App für Mac konfigurieren

Informationen zum Konfigurieren der Sitzungswiederverbindung in der Workspace-App für Mac finden Sie unter Konfigurieren der Workspace Control-Einstellungen.

Sitzungswiederverbindung für alle Apps deaktivieren

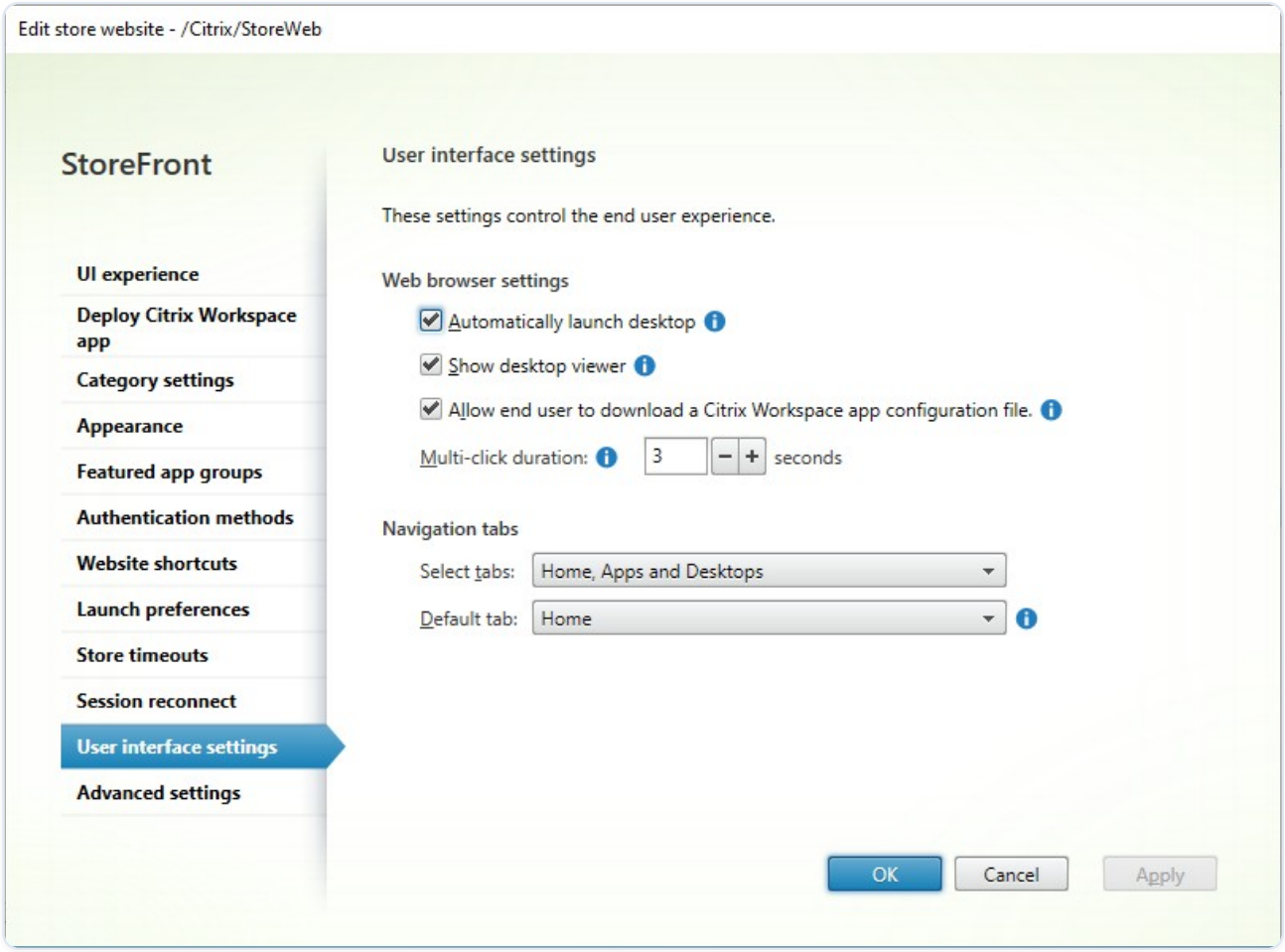
Sie können die Sitzungswiederverbindung in StoreFront für alle Workspace-Apps deaktivieren, unabhängig davon, wie diese konfiguriert sind. Weitere Informationen finden Sie unter Sitzungswiederverbindung zulassen.

Benutzeroberflächeneinstellungen

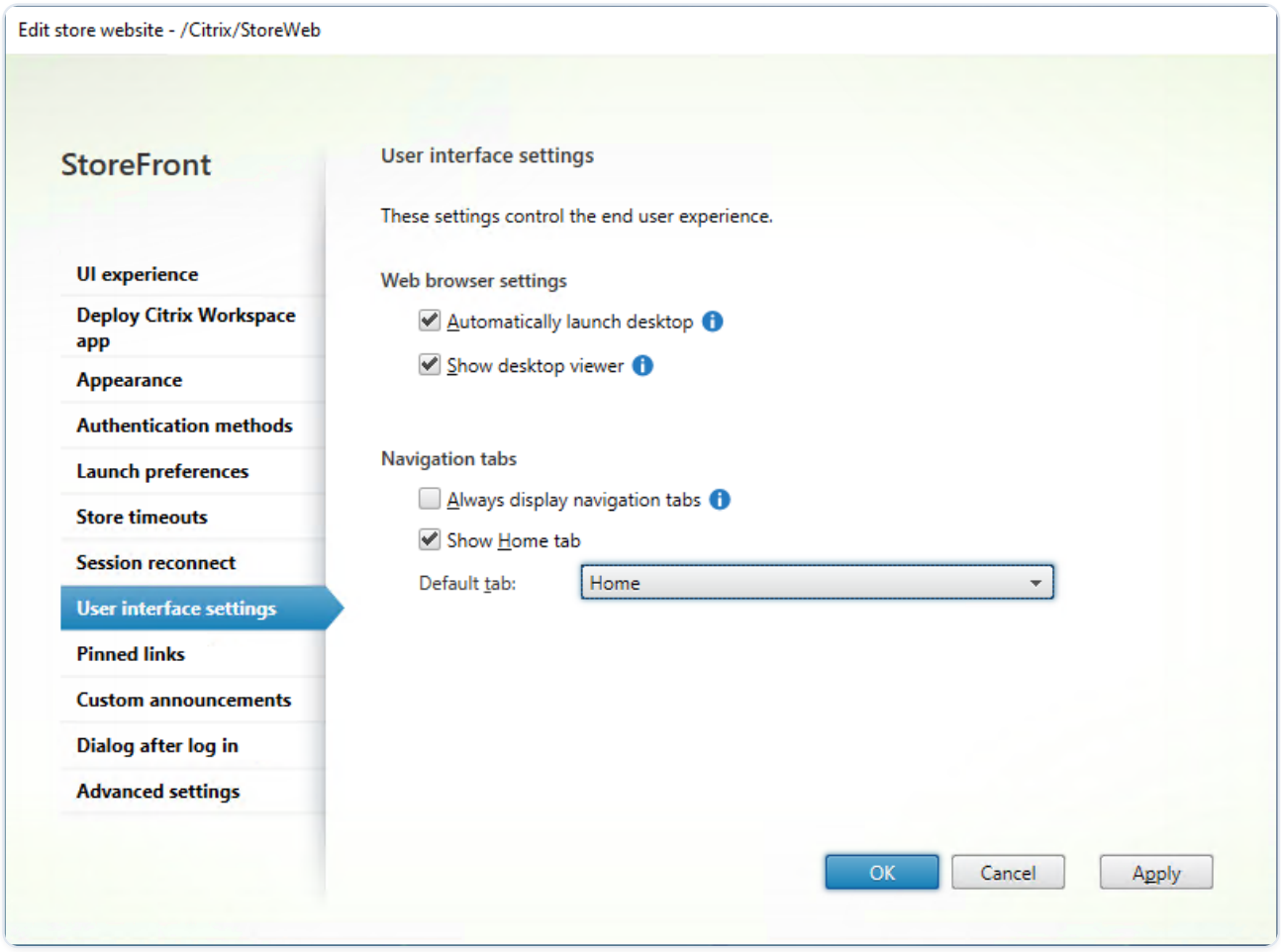
Um Benutzeroberflächeneinstellungen zu ändern, öffnen Sie den Bildschirm Store-Website bearbeiten und die Registerkarte **Benutzeroberflächeneinstellungen**.

Die verfügbaren Einstellungen hängen davon ab, welche Benutzeroberflächenerfahrung ausgewählt ist.

Für die klassische Erfahrung:



Für die moderne Erfahrung:



Desktop automatisch starten

Wenn diese Einstellung aktiviert ist und ein Benutzer nur einen Desktop hat, wird der Desktop gestartet, wenn sich der Benutzer anmeldet.

Um die Einstellung zum automatischen Starten des Desktops mit PowerShell zu ändern, führen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `AutoLaunchDesktop` aus.

Diese Einstellung gilt beim Starten von Ressourcen über einen Webbrowser. Sie gilt nicht beim Starten von Ressourcen über lokal installierte Citrix Workspace™-Apps.

Um diese Option mit PowerShell zu ändern, rufen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `AutoLaunchDesktop` auf.

Desktop Viewer anzeigen

Der Desktop Viewer ist die Symbolleiste, die einfachen Zugriff auf HDX™-Einstellungen bietet. Verwenden Sie diese Einstellung, um festzulegen, ob diese angezeigt wird. Der Desktop Viewer bietet die beste Benutzererfahrung und ist standardmäßig aktiviert.

Diese Einstellung gilt nur, wenn Ressourcen über einen Webbrowser hybrid gestartet werden, unter Verwendung der Windows-, Linux- und anderer lokal installierter HDX-Clients. Wenn ein Benutzer Ressourcen in seinem Webbrowser mit dem HTML5 HDX-Client startet, wird die Symbolleiste unabhängig von dieser Einstellung immer angezeigt.

Um diese Option mit PowerShell zu ändern, rufen Sie das Cmdlet Set-STFWebReceiverResourcesService mit dem Parameter `ShowDesktopViewer` auf.

Endbenutzer das Herunterladen einer Citrix Workspace-App-Konfigurationsdatei erlauben

Wenn diese Option ausgewählt ist, können Benutzer beim Zugriff auf den Store über einen Webbrowser eine Bereitstellungsdatei herunterladen, die die Citrix Workspace-App für den zugehörigen Store konfiguriert. Die Bereitstellungsdateien enthalten Verbindungsdetails für den Store, der die Ressourcen auf der Site bereitstellt, einschließlich Details zu allen Citrix Gateway-Bereitstellungen und Beacons, die für den Store konfiguriert sind.

Um diese Option mit PowerShell zu ändern, rufen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `ReceiverConfigurationEnabled` auf.

Dauer für Mehrfachklicks

Verhindert, dass Benutzer dieselbe Anwendung innerhalb der konfigurierten Dauer mehrmals starten. Dies gilt nur beim Starten von Ressourcen über einen Webbrowser und nicht über eine lokal installierte Citrix Workspace-App.

Um die Dauer für Mehrfachklicks mit PowerShell zu ändern, führen Sie das Cmdlet Set-STFWebReceiverUserInterface mit dem Parameter `MultiClickTimeout` aus.

Diese Einstellung gilt nur beim Starten von Ressourcen über einen Webbrowser. Sie gilt nicht für lokal installierte Citrix Workspace-Apps.

Navigationsregisterkarten

Die verfügbaren Einstellungen hängen davon ab, welche Benutzeroberflächenerfahrung ausgewählt ist.

Moderne Erfahrung

NAVIGATIONSREGISTERKARTEN IMMER ANZEIGEN

Standardmäßig zeigt die Benutzeroberfläche bei weniger als 20 Ressourcen eine einfache Ansicht an, in der alle Ressourcen auf einem Bildschirm ohne Registerkarten angezeigt werden. Administratoren können die Option „Navigationsregisterkarten immer anzeigen“ auswählen,

wodurch die einfache Ansicht effektiv deaktiviert wird. Wenn diese Option ausgewählt ist, sehen Benutzer die Navigationsregisterkarte unabhängig von der Anzahl der Ressourcen.

STARTREGISTERKARTE DEAKTIVIEREN

Standardmäßig enthält die Benutzeroberfläche eine Startregisterkarte (außer in der einfachen Ansicht), die bevorzugte und zuletzt verwendete Apps und Desktops anzeigt. Die Startregisterkarte bietet schnellen Zugriff auf Favoriten und zuletzt verwendete Apps und Desktops. Administratoren können nun die Option „Startregisterkarte anzeigen“ deaktivieren, um sie auszublenden. Favoriten sind weiterhin über die einzelnen Registerkarten „Apps“ oder „Desktops“ verfügbar.

STANDARDREGISTERKARTE

Standardmäßig landen Benutzer nach der Anmeldung auf der Registerkarte „Startseite“. Sie können die Standardregisterkarte ändern, sodass Benutzer auf der Registerkarte **Apps** oder **Desktops** landen. Wenn Sie **Apps** ausgewählt haben, können Sie zusätzlich wählen, ob standardmäßig alle Apps, Apps in einer bestimmten Kategorie oder nicht kategorisierte Apps angezeigt werden sollen.

Klassische Erfahrung

Wenn sowohl Desktops als auch Anwendungen verfügbar sind, zeigt die Website standardmäßig separate Desktop- und Anwendungsansichten an. Favoriten werden in der Ansicht **Startseite** angezeigt. Benutzer sehen die Ansicht **Startseite** zuerst, wenn sie sich bei der Site anmelden.

Wählen Sie in der Dropdown-Liste **Registerkarten auswählen** aus, ob Apps, Desktops oder beides angezeigt werden sollen.

Wählen Sie in der Dropdown-Liste **Standardregisterkartenansicht** die Registerkarte aus, die beim ersten Anmelden des Benutzers angezeigt werden soll.

OPTION	BESCHREIBUNG
Startseite	Startseite anzeigen
Apps	Registerkarte „Apps“ anzeigen
Desktops	Registerkarte „Desktops“ anzeigen

Um diese Optionen mit PowerShell zu ändern, führen Sie das Cmdlet Set-STFWebReceiverUserInterface mit den Parametern `ShowAppsView`, `ShowDesktopsView` und `DefaultView` aus.

„Startbildschirm personalisieren“ für Erstanwender anzeigen

Bei Verwendung der modernen Erfahrung wird beim ersten Anmelden eines Benutzers ohne Favoriten das Fenster **Startbildschirm personalisieren** angezeigt. Um dieses Fenster zu verwalten, müssen Sie PowerShell verwenden.

Um den aktuellen Wert abzurufen, rufen Sie Get-STFWebReceiverUserInterface auf. Beispiel:

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$websiteUI = Get-STFWebReceiverUserInterface -WebReceiverService $website

"Show personalization screen: $($websiteUI.ShowFirstTimeUse)"
```

Um das Fenster zu deaktivieren oder zu aktivieren, rufen Sie Set-STFWebReceiverUserInterface mit dem Parameter `ShowFirstTimeUse` auf. Beispiel:

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Set-STFWebReceiverUserInterface -WebReceiverService $website
-ShowFirstTimeUse $false
```

Aktivitätsmanager anzeigen

Die moderne Erfahrung umfasst den Aktivitätsmanager, damit Benutzer ihre Sitzungen verwalten können. Der Aktivitätsmanager ist standardmäßig aktiviert. Um diese Einstellung zu verwalten, müssen Sie PowerShell verwenden. Um den aktuellen Wert abzurufen, rufen Sie Get-STFWebReceiverUserInterface auf. Beispiel:

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$websiteUI = Get-STFWebReceiverUserInterface -WebReceiverService $website

"Show Activity manager: $($websiteUI.ShowActivityManager)"
```

Um den Aktivitätsmanager zu deaktivieren oder zu aktivieren, rufen Sie Set-STFWebReceiverUserInterface mit dem Parameter `ShowActivityManager` auf. Zum Beispiel:

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Set-STFWebReceiverUserInterface -WebReceiverService $website
-ShowActivityManager $false
```

Angeheftete Links

Hinweis:

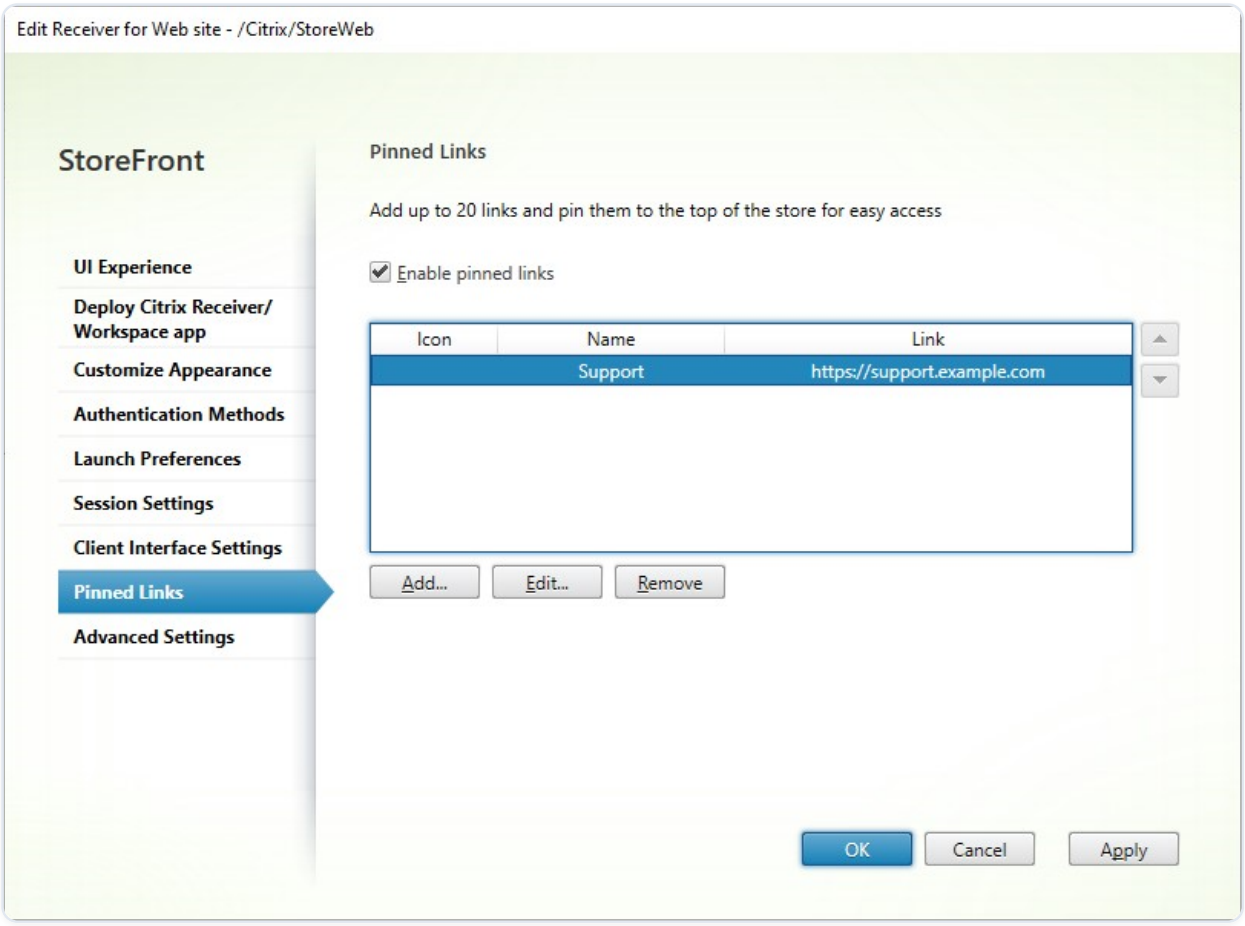
Diese Funktionalität ist nur über die moderne Oberfläche verfügbar.

Benutzerdefinierte URLs in der StoreFront™-Benutzeroberfläche beziehen sich auf vom Kunden definierte Hyperlinks, die einen schnellen Zugriff auf bestimmte Websites ermöglichen. Diese Funktion dient als Verknüpfung, die Benutzern hilft, effizient direkt von der StoreFront-Benutzeroberfläche zu Websites zu navigieren. Wichtige Links, wie Support-Websites oder Unternehmensportale, können den Benutzern zur Verfügung gestellt werden, ohne dass diese nach diesen Links suchen müssen. Dies macht die Navigation mühelos und schneller. Diese Funktion ist nur in der modernen Oberfläche verfügbar.

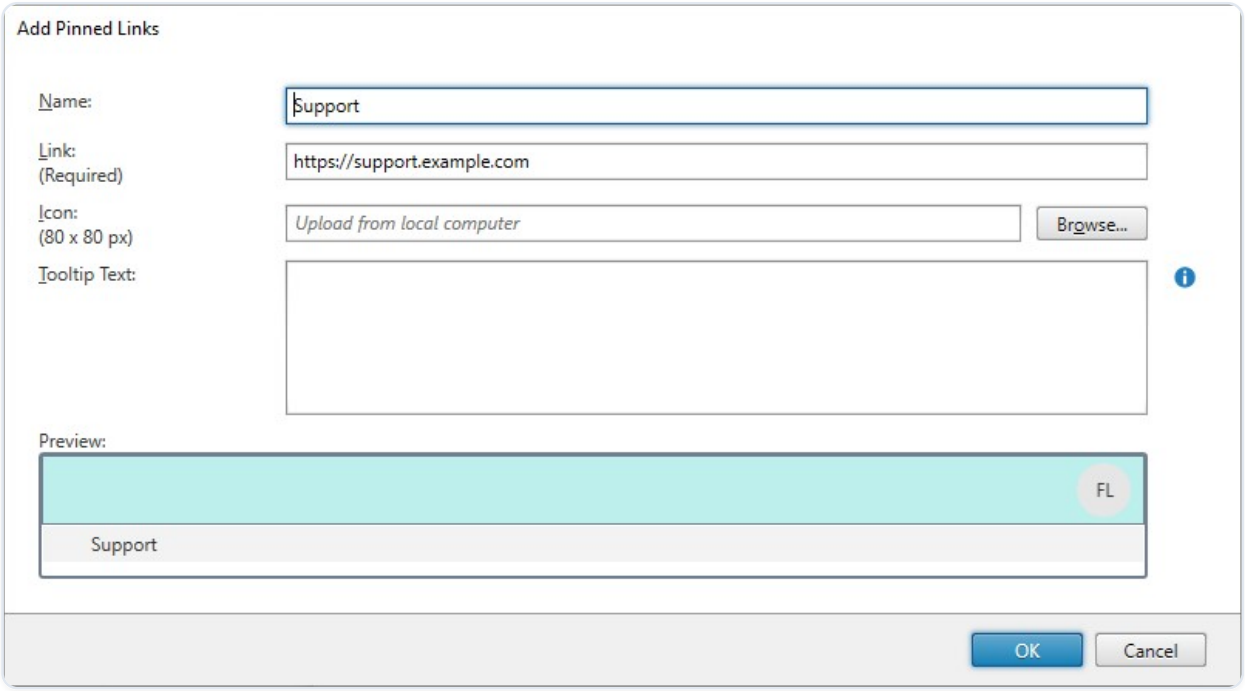
Konfiguration

So fügen Sie einen angehefteten Link hinzu:

1. Gehen Sie zu Store-Website bearbeiten und wählen Sie die Registerkarte **Angeheftete Links** aus.

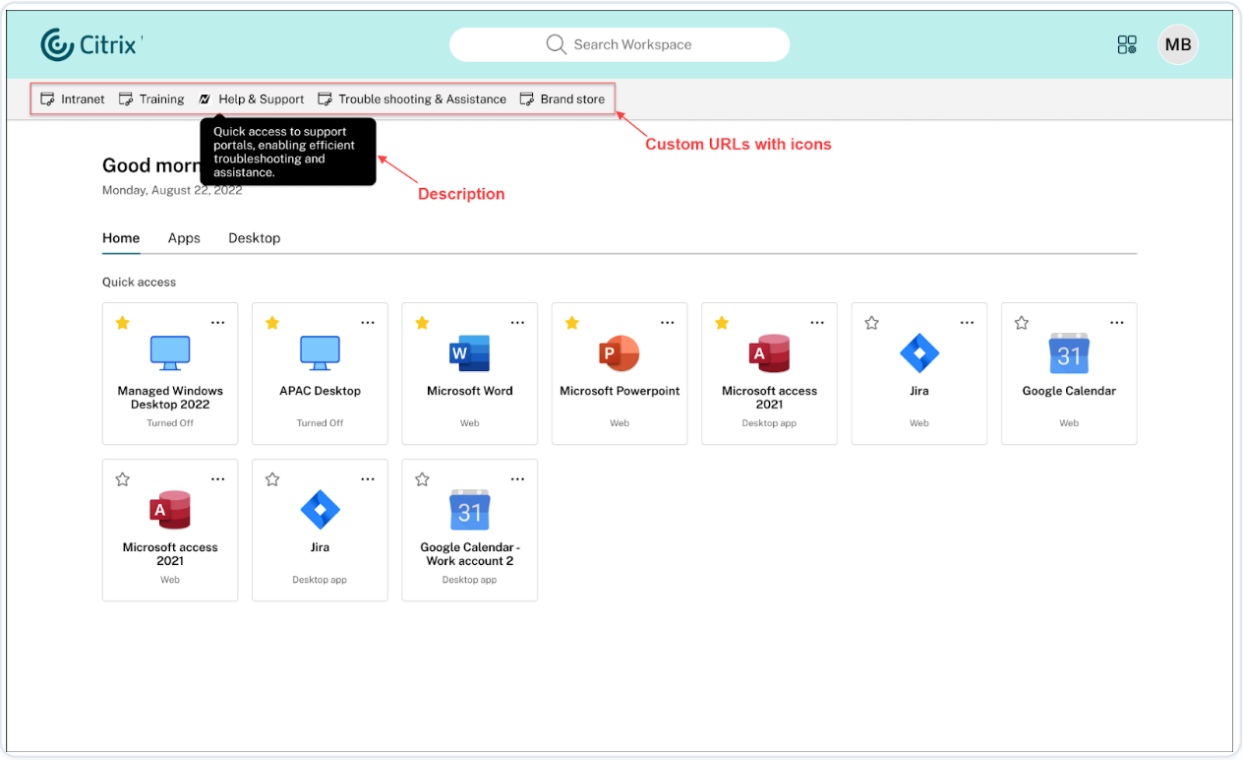


2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie den Namen, den Link, den Tooltip ein und suchen Sie nach dem Symbol.
4. Zeigen Sie eine Vorschau der Aktualisierungen an und klicken Sie auf **OK**.

   Diese Links erscheinen oben im Store für schnellen Zugriff.



Benutzerdefinierte Ankündigungen

Sie können ein Banner konfigurieren, das den Endbenutzern angezeigt wird, beispielsweise um sie über bevorstehende Änderungen oder Wartungsfenster zu informieren.

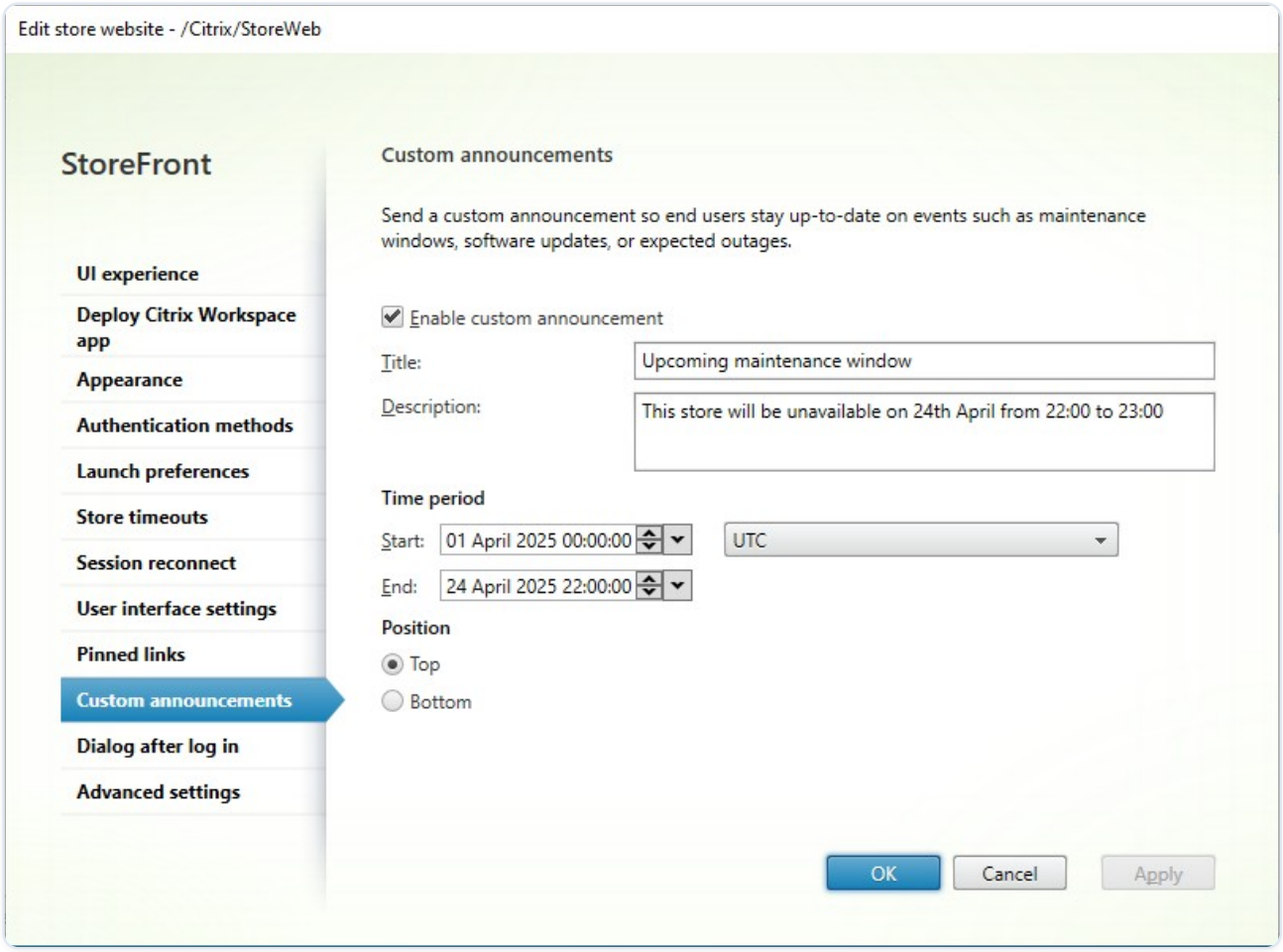
> **Hinweis:**

> Diese Funktionalität ist nur mit der modernen Oberfläche verfügbar. Wenn Sie die klassische Oberfläche verwenden, erstellen Sie eine benutzerdefinierte Ankündigung mithilfe der StoreFront Client UI Customization API. Siehe Beispiel Dynamische Kopfzeile hinzufügen.

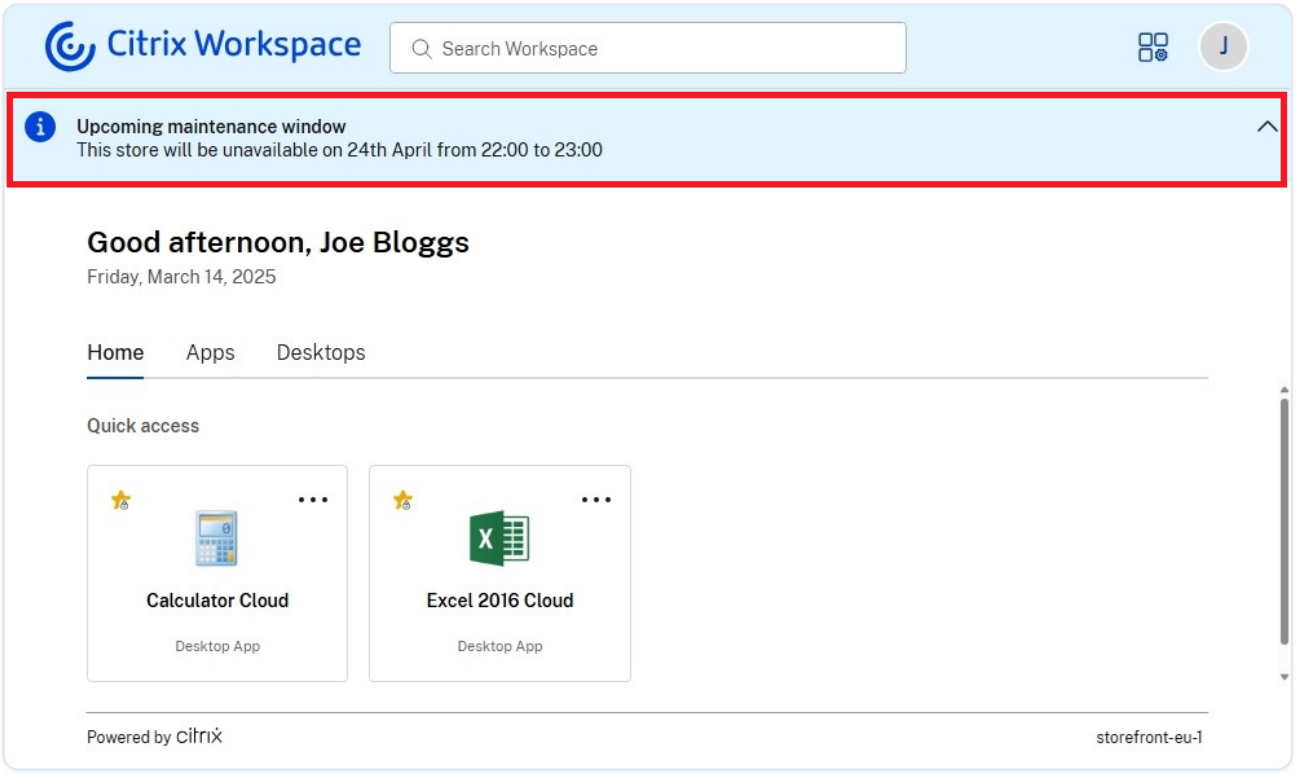
> So legen Sie die benutzerdefinierte Ankündigung fest oder ändern sie:

1. Gehen Sie zu Store-Website bearbeiten
2. Wählen Sie die Registerkarte **Kategorieeinstellungen** aus.
3. Wählen Sie **Benutzerdefinierte Ankündigung aktivieren** aus.
4. Geben Sie einen **Titel** ein.
5. Geben Sie eine **Beschreibung** ein.
6. Geben Sie Datum und Uhrzeit ein, ab der die benutzerdefinierte Ankündigung angezeigt werden soll.

7. Geben Sie Datum und Uhrzeit ein, zu der die Kundenankündigung ausgeblendet werden soll.
8. Wählen Sie aus, ob die Ankündigung oben oder unten auf dem Bildschirm angezeigt werden soll.



Wenn sich Benutzer anmelden, wird die Ankündigung dauerhaft oben oder unten auf dem Bildschirm angezeigt.



Dialog nach der Anmeldung

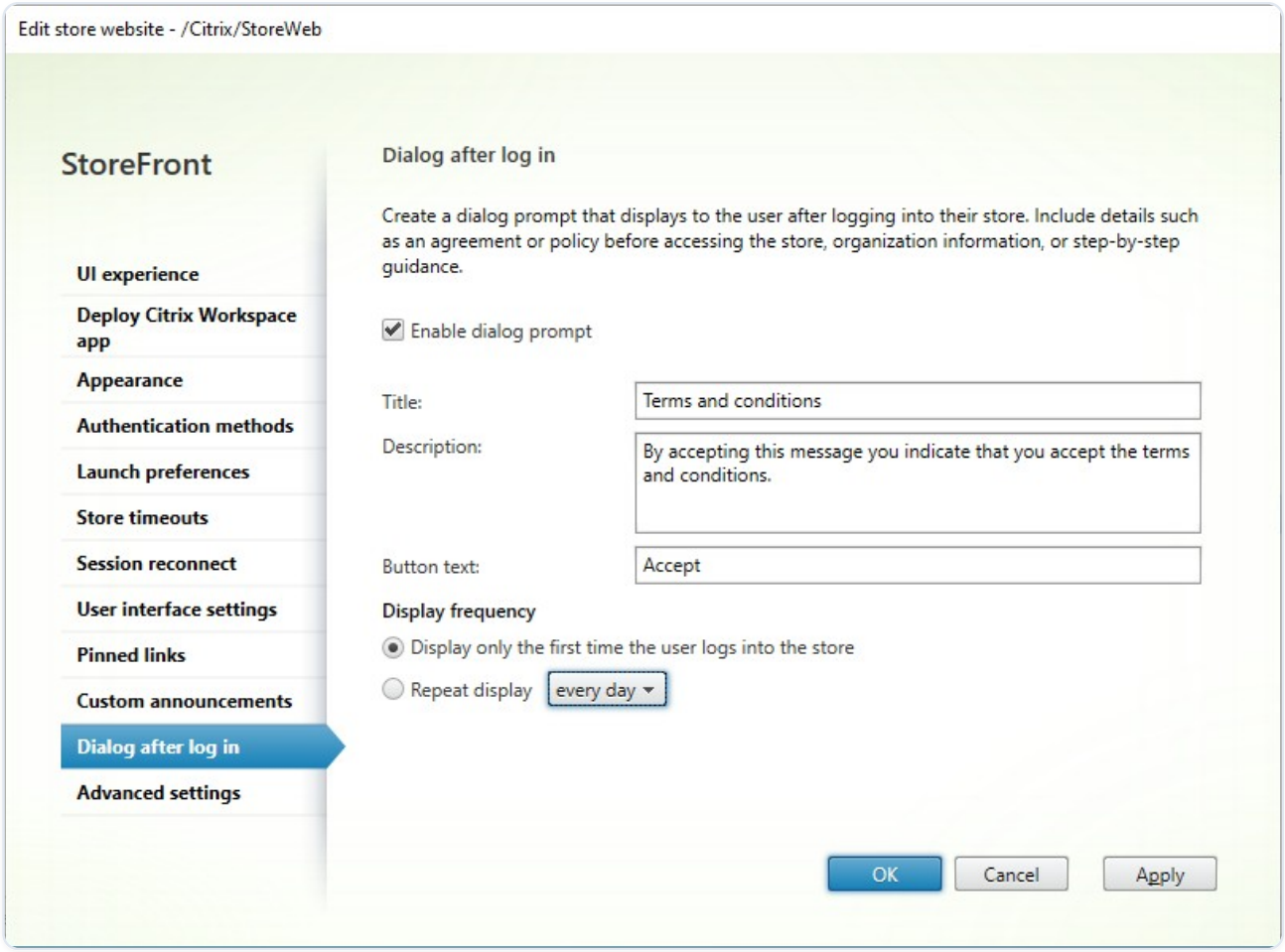
Sie können einen Pop-up-Dialog konfigurieren, der nach der Anmeldung erscheint und den Benutzer akzeptieren müssen, bevor sie mit StoreFront interagieren. Sie können diesen verwenden, um Benutzer über wichtige Informationen wie behördliche Informationen, Richtlinienbestätigungen, interne Richtlinien, Schulungsinhalte, Sicherheitshinweise, Systemaktualisierungen und rechtliche Hinweise zu informieren.

> **Hinweis:**
>
> Diese Funktionalität ist nur mit der modernen Benutzeroberfläche verfügbar. Wenn Sie die klassische Benutzeroberfläche verwenden, fügen Sie einen ähnlichen Dialog mithilfe der StoreFront Client UI Customization API hinzu. Siehe Beispiel Haftungsausschlussmeldung vor oder nach der Anmeldung anzeigen.

So legen Sie den Dialog fest oder ändern ihn:

1. Gehen Sie zu Store-Website bearbeiten
2. Wählen Sie die Registerkarte **Dialog nach der Anmeldung**.
3. Wählen Sie **Dialogaufforderung aktivieren**.
4. Geben Sie den **Titel**, die **Beschreibung** und den **Schaltflächentext** ein.

5. Wählen Sie aus, wie oft die Nachricht angezeigt werden soll. Wenn Sie **Anzeige wiederholen** wählen, können Sie zwischen **täglich**, **alle 7 Tage** und **alle 30 Tage** wählen. Wenn Sie die Nachricht ändern, wird die Aufforderung immer beim nächsten Login des Benutzers angezeigt.



Weitere Informationen zur Endbenutzererfahrung finden Sie unter Moderne Benutzeroberfläche.

App-Schutz

App Protection bietet eine zusätzliche Sicherheitsebene, indem es Tastenprotokollierung und Bildschirmaufnahmen blockiert. Weitere Informationen finden Sie in der App Protection-Dokumentation.

> **Wichtig:**
>
> Beim Zugriff auf einen Store über einen Webbrowser sind Apps, die App Protection erfordern, standardmäßig ausgeblendet. StoreFront muss so konfiguriert werden, dass geschützte Apps angezeigt werden. Beim Zugriff auf einen Store über die Citrix Workspace-App ist keine StoreFront-Konfiguration erforderlich.

App Protection für Starts von der Citrix Workspace-App

Wenn Benutzer über eine unterstützte Version der Citrix Workspace-App auf den Store zugreifen, zeigt StoreFront alle Ressourcen an, die App Protection erfordern. Es ist keine zusätzliche StoreFront-Konfiguration erforderlich.

App Protection für hybride Starts

Wenn Benutzer über einen Webbrowser auf einen Store zugreifen, sind virtuelle Apps und Desktops, die App Protection erfordern, standardmäßig ausgeblendet. StoreFront 2308 und höher kann so konfiguriert werden, dass geschützte Ressourcen angezeigt werden, es sei denn, es wird ChromeOS verwendet oder der Benutzer hat sich entschieden, Ressourcen in seinem Webbrowser zu starten, da diese App Protection nicht unterstützen.

Warnung

Es ist möglich, Apps mit älteren Versionen der Citrix Workspace-App zu starten, die App Protection nicht anwenden. Bevor Sie App Protection für hybride Starts aktivieren, empfiehlt Citrix daher, die App Protection-Haltungsprüfung zu aktivieren, die das Starten virtueller Apps und Desktops von Citrix Workspace-App-Versionen blockiert, die App Protection nicht unterstützen.

Wenn Ressourcen über ICA-Downloads gestartet werden, könnte der Benutzer die ICA-Datei bearbeiten, um die Anweisung zur Anwendung von App Protection zu entfernen. Bevor Sie App Protection für hybride Starts aktivieren, empfiehlt Citrix daher, die Erkennung von Richtlinienmanipulationen zu aktivieren.

Versionen von StoreFront vor 2507 versuchten, die installierte Version der Citrix Workspace-App mithilfe von Citrix Web-Erweiterungen oder dem Citrix Workspace-Launcher zu erkennen und zeigten Ressourcen mit App Protection nur an, wenn der Client bestimmte Mindestversionen erfüllte. Es konnte jedoch nicht garantiert werden, dass die Version korrekt erkannt wurde, was dazu führte, dass Ressourcen falsch angezeigt oder ausgeblendet wurden. Daher wurde diese Überprüfung entfernt.

App Protection für hybride Starts aktivieren

Um StoreFront zu ermöglichen, geschützte Apps auf unterstützten Versionen der Citrix Workspace-App anzuzeigen, verwenden Sie das PowerShell-Cmdlet Set-STFWebReceiverAppProtection.

1. Öffnen Sie eine PowerShell-Konsole als Administrator.
2. Wenn Sie mehr als eine Website haben, suchen Sie den virtuellen Pfad der Website, die Sie konfigurieren möchten. Dies ist der Pfad, der im Webbrowser des Benutzers angezeigt wird, z. B. `/Citrix/StoreWeb`. Sie können eine Liste aller Websites und deren Pfad mit dem Befehl `Get-STFWebReceiverService` abrufen.
3. Führen Sie das PowerShell-Skript aus:

   ```
   $receiver = Get-STFWebReceiverService -VirtualPath "[virtual path]"

   Set-STFWebReceiverAppProtection -WebReceiverService $receiver -Enabled
   On
   ```

   Ersetzen Sie `[virtual path]` durch den im ersten Schritt gefundenen Pfad. `-VirtualPath` kann weggelassen werden, wenn nur eine Website vorhanden ist.
4. Wenn der Benutzer Ressourcen in seinem Webbrowser öffnen möchte, entweder über die Administratorkonfiguration oder weil der Benutzer **Webbrowser verwenden** gewählt hat, ist App Protection nicht verfügbar. Sie können den Store optional so konfigurieren, dass er immer mit der lokal installierten Citrix Workspace-App gestartet wird. Weitere Informationen finden Sie unter Bereitstellung der Citrix Workspace-App.
5. Wenn der Benutzer zum ersten Mal eine Store-Website öffnet und die Citrix Web Extension nicht verfügbar ist, wird der Bildschirm **Citrix Workspace-App erkennen** angezeigt. Wenn der Benutzer **Erkennung überspringen** wählt, kann StoreFront die App-Version nicht ermitteln und zeigt daher keine geschützten Apps und Desktops an. Es wird daher empfohlen, die Option **Erkennung überspringen** zu deaktivieren. Weitere Informationen finden Sie unter Benutzern das Überspringen der Citrix Workspace-App-Erkennung erlauben.

Anzeigen, ob App Protection für den hybriden Start aktiviert ist

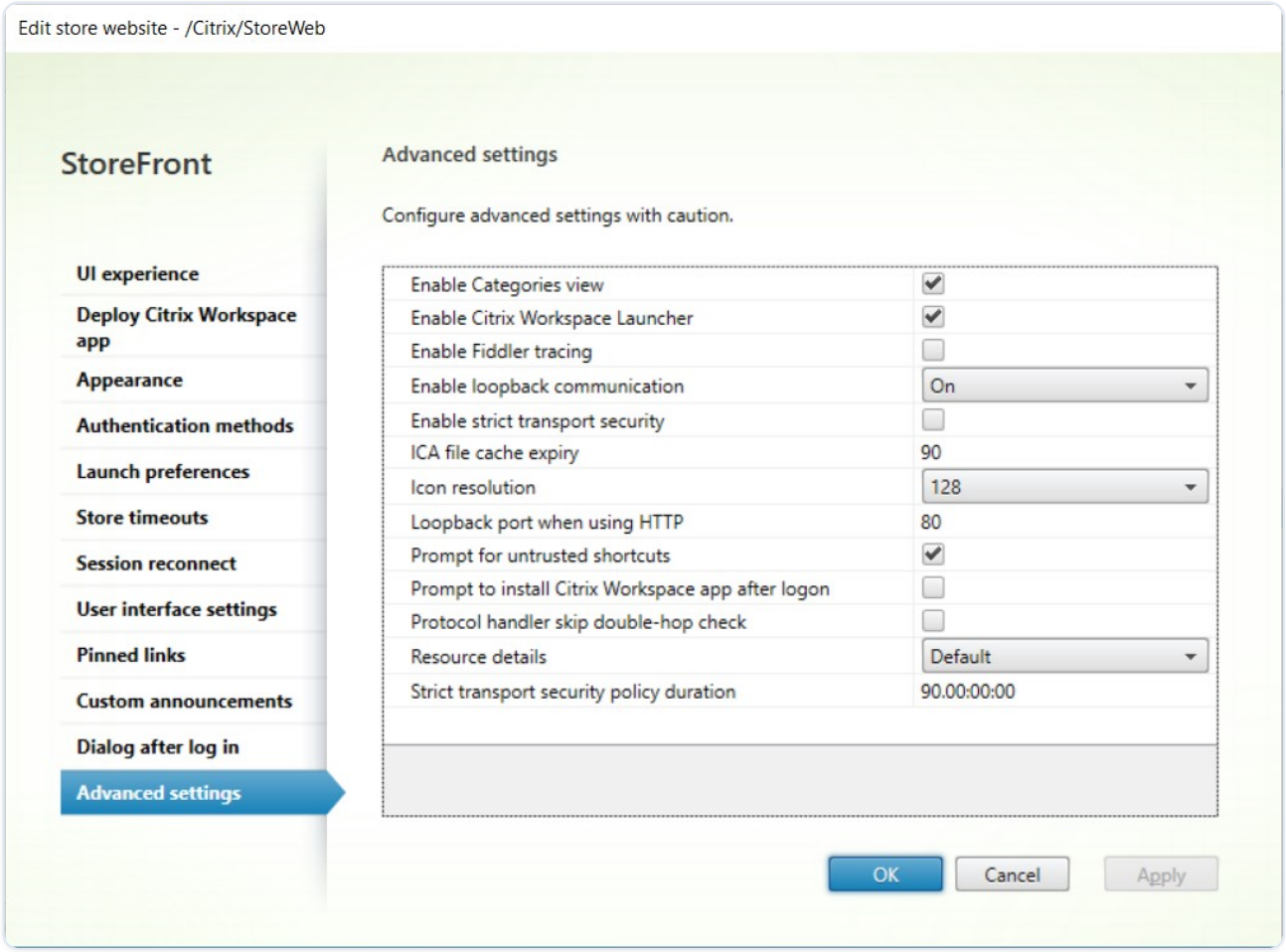
Um herauszufinden, ob App Protection für den hybriden Start für eine Store-Website verfügbar ist, führen Sie mit PowerShell das Cmdlet Get-STFWebReceiverAppProtection aus. Beispiel:

```
$receiver = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Get-STFWebReceiverAppProtection -WebReceiverService $receiver
```

Erweiterte Einstellungen

Um erweiterte Einstellungen für eine Website zu ändern, öffnen Sie den Bildschirm Edit store website und wählen Sie die Registerkarte **Erweiterte Einstellungen**.



Fiddler-Tracing aktivieren

Aktiviert das Fiddler-Tracing des Datenverkehrs zwischen StoreFront-Diensten zu Debugging-Zwecken. Die Loopback-Kommunikation muss ebenfalls deaktiviert sein. Dies ist standardmäßig deaktiviert und sollte nur auf Anfrage des Supports aktiviert werden. Deaktivieren Sie das Fiddler-Tracing, sobald Sie die Fehlerbehebung abgeschlossen haben.

Ordneransicht aktivieren

Standardmäßig gibt es auf der Registerkarte **Apps** die Ansicht **Kategorien**. Um die Ansicht **Kategorien** auszublenden, deaktivieren Sie **Ordneransicht aktivieren**. Gilt nur für die klassische Oberfläche. Hat keine Auswirkung bei Verwendung der modernen Oberfläche. Weitere Informationen zur Anzeige von Kategorien finden Sie unter Kategorieeinstellungen.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverUserInterface` mit dem Parameter `EnableAppsFolderView` aus.

Loopback-Kommunikation aktivieren

Ermöglicht die direkte Kommunikation zwischen StoreFront™-Diensten, ohne über die Basis-URL zu gehen. Aktivieren Sie dies bei Verwendung eines Lastenausgleichs. Kann auf die folgenden Werte eingestellt werden:

WERT	BESCHREIBUNG
Ein	Der StoreFront-Webproxy kommuniziert mit dem Store-Dienst über die Loopback-Adresse, wodurch sichergestellt wird, dass die Kommunikation auf dem StoreFront-Server verbleibt.
Aus	Der StoreFront-Webproxy kommuniziert mit dem Store-Dienst über den in der Basis-URL definierten FQDN. Wenn die Basis-URL ein Lastenausgleich ist, könnte dies dazu führen, dass die Kommunikation über den Lastenausgleich an einen anderen StoreFront-Server geleitet wird, was zu fehlgeschlagenen Anforderungen führt.
Ein mit HTTP	Wie **Ein**, ändert aber das Protokoll von HTTP auf HTTPS. Wählen Sie diese Option, wenn Sie einen Lastenausgleich verwenden, der HTTPS beendet und eine Verbindung zu StoreFront über HTTP herstellt. Informationen zum Ändern des Ports finden Sie unter Loopback-Port bei Verwendung von HTTP.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverCommunication` mit dem Parameter `Loopback` aus.

Citrix Workspace Launcher aktivieren

Standardmäßig aktiviert. Wenn Benutzer einen Store über einen Webbrowser öffnen, ermöglicht dies der Website, den Citrix Workspace Launcher zu verwenden, um zu versuchen, zu erkennen, ob die Citrix Workspace-App installiert ist, und anschließend Ressourcen zu starten.

Wenn der Citrix Workspace Launcher deaktiviert ist und die Startoption auf **Benutzer wählen lassen** eingestellt ist, fordert die Store-Website Erstbenutzer nicht auf, eine Startmethode zu wählen. Bei Verwendung der modernen Oberfläche wird die Startmethode standardmäßig auf das

Herunterladen einer ICA-Datei eingestellt, Benutzer können dies jedoch über den Einstellungsbildschirm ändern. Bei Verwendung der klassischen Oberfläche werden Ressourcen in einem Webbrowser gestartet.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverPluginAssistant` mit dem Parameter `Enabled` aus.

Das Deaktivieren dieser Option kann dazu führen, dass Benutzer ICA-Dateien herunterladen, was nicht empfohlen wird.

Strikte Transportsicherheit aktivieren

Wenn aktiviert, wird der `Strict-Transport-Security` Header hinzugefügt, um Browsern mitzuteilen, dass sie sich nur über HTTPS mit der Website verbinden sollen.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverStrictTransportSecurity` mit dem Parameter `Enabled` aus.

Es gibt andere Möglichkeiten, HSTS zu aktivieren. Weitere Informationen finden Sie unter HTTPS.

Ablauf des ICA-Dateicaches

Die Anzahl der Sekunden, für die eine ICA-Datei im Speicher auf dem Server zwischengespeichert wird. Nachdem der Client den Start initiiert hat und die ICA-Datei bereit ist, muss der Client die ICA-Datei innerhalb dieser Zeit abrufen. Standardmäßig 90 Sekunden.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverResourcesService` mit dem Parameter `IcaFileCacheExpiry` aus.

Symbolauflösung

Die Symbol-Dateigröße, die vom Server angefordert werden soll. Beachten Sie, dass dies nicht direkt der in der Benutzeroberfläche angezeigten Symbolgröße entspricht. Der Standardwert ist 128.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverResourcesService` mit dem Parameter `IconSize` aus.

Loopback-Port bei Verwendung von HTTP

Wenn Loopback-Kommunikation aktivieren auf **Bei Verwendung von HTTP** festgelegt ist, wird dieser Port eingestellt.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverCommunication` mit dem Parameter `LoopbackPortUsingHttp` aus.

Eingabeaufforderung für nicht vertrauenswürdige Verknüpfungen

Beim Starten von Websiteverknüpfungen wird standardmäßig eine Bestätigung vom Benutzer angefordert, wenn der Referrer nicht in der Liste der vertrauenswürdigen Sites enthalten ist. Wenn Sie dies deaktivieren, können Benutzer Ressourcen von nicht vertrauenswürdigen Websites starten.

Aufforderung zur Installation der Citrix Workspace-App nach der Anmeldung

Wenn ein Benutzer zum ersten Mal die Store-Website aufruft, versucht die Website, die Citrix Workspace-App zu erkennen, und bietet die Möglichkeit, die Citrix Workspace-App herunterzuladen. Standardmäßig geschieht dies beim direkten Zugriff auf StoreFront, bevor sich der Benutzer anmeldet. Alternativ können Sie **Aufforderung zur Installation der Citrix Workspace-App nach der Anmeldung** auswählen. Dies hat keine Auswirkung, wenn Benutzer sich über ein Citrix Gateway anmelden, da dies immer geschieht, bevor der Benutzer den Erkennungsbildschirm der StoreFront Citrix Workspace-App erreicht.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverPluginAssistant` mit dem Parameter `ShowAfterLogin` aus.

Ressourcendetails

Ob **Standard**- oder **Vollständige** Ressourcendetails abgerufen werden sollen, wenn die klassische Oberfläche verwendet wird. Normalerweise ist **Standard** ausreichend. Wenn Sie JavaScript-Anpassungen haben, die preProcessAppData verwenden, können Sie die zusätzlichen Daten nutzen, die von **Vollständig** zurückgegeben werden. Hat keine Auswirkung bei Verwendung der modernen Oberfläche.

Dauer der Strict Transport Security-Richtlinie

Wenn Strict Transport Security aktiviert ist, die Dauer, für die die Strict Transport-Richtlinie erzwungen wird, im Format TT.hh:mm:ss. Der Standardwert ist 90 Tage.

Um diese Einstellung mit PowerShell zu ändern, führen Sie das Cmdlet `Set-STFWebReceiverStrictTransportSecurity` mit dem Parameter `PolicyDuration` aus.

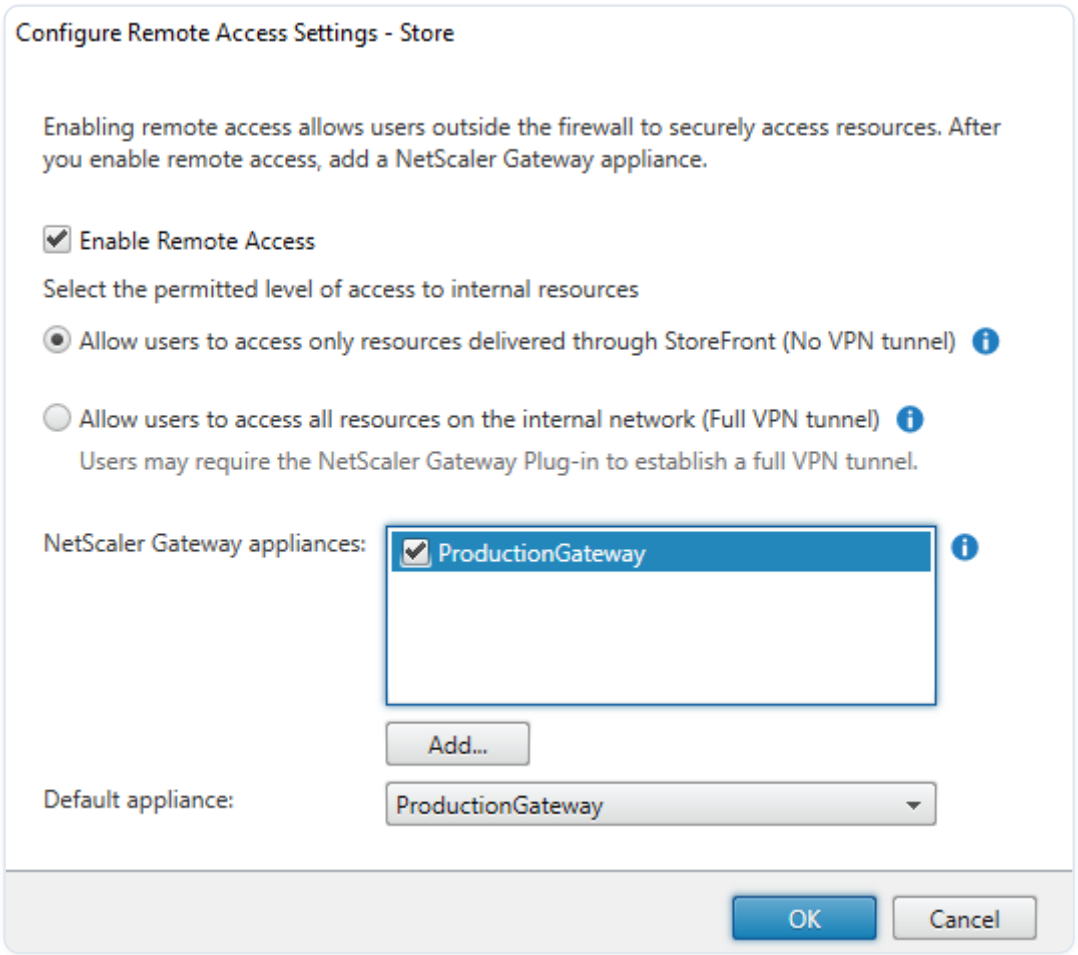
Remotzugriffseinstellungen konfigurieren

Sie können den Zugriff auf Stores über Citrix Gateway für Benutzer konfigurieren, die sich von öffentlichen Netzwerken aus verbinden. Remotzugriff über ein Citrix Gateway kann nicht auf nicht authentifizierte Stores angewendet werden.

Wichtig:

Verwenden Sie in Bereitstellungen mit mehreren Servern immer nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Nach Abschluss, übertragen Sie Ihre Konfigurationsänderungen an die Servergruppe, damit die anderen Server in der Bereitstellung aktualisiert werden.

1. Wählen Sie den Knoten Stores im rechten Bereich der Citrix StoreFront-Verwaltungskonsole und wählen Sie im Ergebnisbereich einen Store aus.
2. Klicken Sie im Bereich Aktionen auf **Remotzugriffseinstellungen konfigurieren**.



3. Geben Sie im Dialogfeld Remotzugriffseinstellungen konfigurieren an, ob und wie Benutzer, die sich von öffentlichen Netzwerken aus verbinden, über Citrix Gateway auf den Store zugreifen können.

    - Um den Store für Benutzer in öffentlichen Netzwerken nicht verfügbar zu machen, aktivieren Sie **Remotzugriff aktivieren** nicht. Nur lokale Benutzer im internen Netzwerk können auf den Store zugreifen.
    - Um den Remotzugriff zu aktivieren, aktivieren Sie **Remotzugriff aktivieren**.
        - Um über den Store bereitgestellte Ressourcen über Citrix Gateway verfügbar zu machen, wählen Sie **Kein VPN-Tunnel**. Benutzer melden sich entweder über ICAProxy oder clientloses VPN (cVPN) bei Citrix Gateway an und benötigen das Citrix Gateway Plug-In nicht, um ein vollständiges VPN einzurichten.
        - Um den Store und andere Ressourcen im internen Netzwerk über einen SSL-VPN-Tunnel (Secure Sockets Layer Virtual Private Network) verfügbar zu machen, wählen Sie **Vollständiger VPN-Tunnel**. Benutzer benötigen das Citrix Gateway Plug-In, um den VPN-Tunnel einzurichten.

    Wenn Sie den Remotzugriff auf den Store aktivieren, wird die Authentifizierungsmethode **Pass-Through von Citrix Gateway** automatisch aktiviert. Benutzer authentifizieren sich bei Citrix Gateway und werden automatisch angemeldet, wenn sie auf ihre Stores zugreifen.

4. Wenn Sie den Remotzugriff aktiviert haben, wählen Sie aus der Liste **Citrix Gateway-Appliances** die Bereitstellungen aus, über die Benutzer auf den Store zugreifen können. Alle Bereitstellungen, die Sie zuvor für diesen und andere Stores konfiguriert haben, stehen in der Liste zur Auswahl. Wenn Sie der Liste eine weitere Bereitstellung hinzufügen möchten, klicken Sie auf **Hinzufügen** und folgen Sie den Schritten unter (/de-de/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/configure-citrix-gateway.html).
5. Wenn Sie den Zugriff über mehrere Appliances aktivieren, indem Sie mehr als einen Eintrag in der Liste auswählen, geben Sie die **Standard-Appliance** an, die für den Zugriff auf den Store über die Citrix Workspace-App verwendet werden soll.
6. Klicken Sie auf **OK**, um die Konfiguration zu speichern und das Dialogfeld Remotzugriff konfigurieren zu schließen.

Die Citrix Workspace-App verwendet Beacon-Punkte, um festzustellen, ob Benutzer mit lokalen oder öffentlichen Netzwerken verbunden sind, und wählt dann die entsprechende Zugriffsmethode

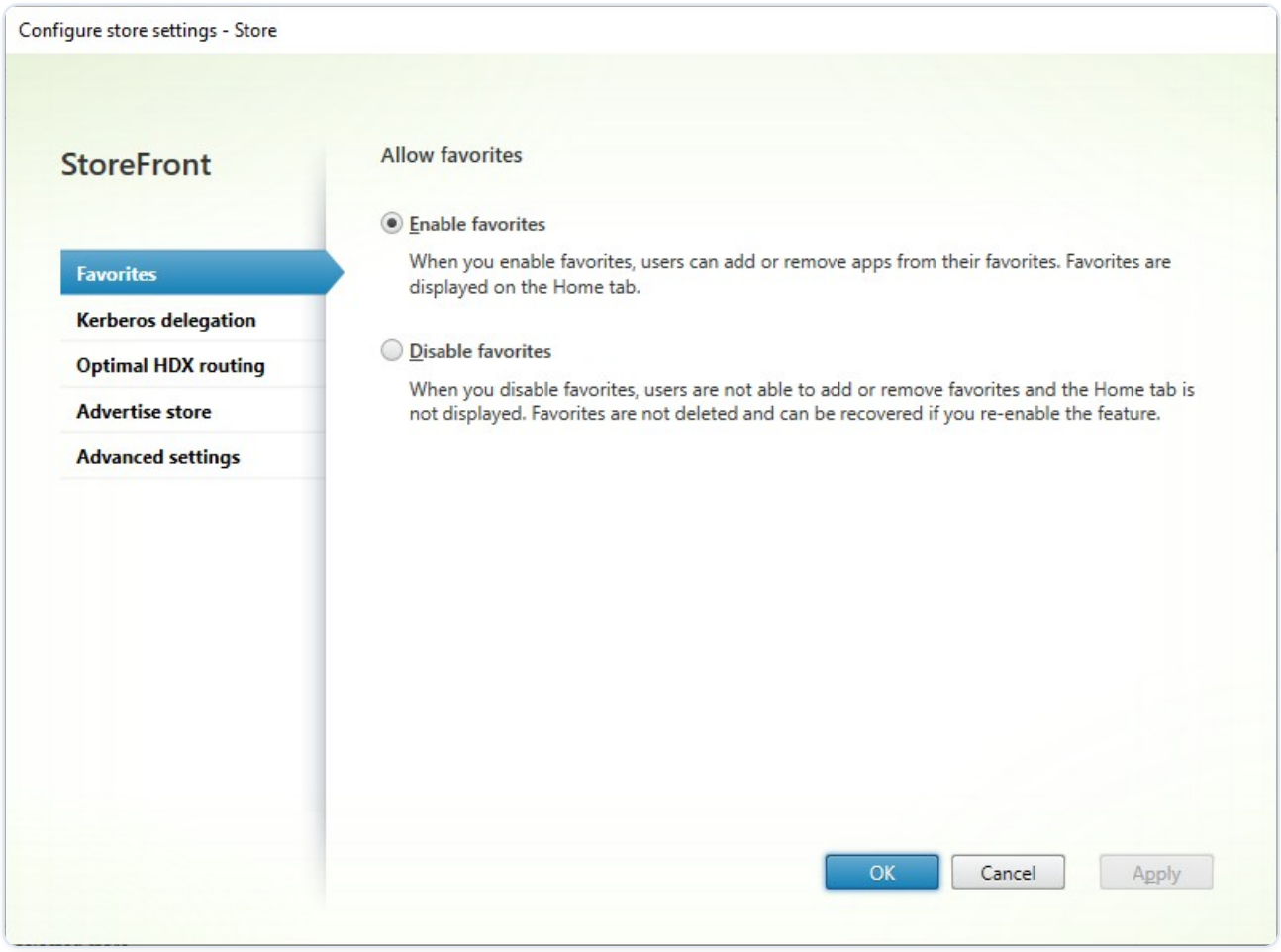
aus. Weitere Informationen zum Ändern von Beacon-Punkten finden Sie unter Beacon-Punkte konfigurieren.

Standardmäßig verwendet StoreFront das Gateway, über das der Benutzer mit dem Store verbunden ist, um Ressourcen zu starten. Informationen zum Konfigurieren von StoreFront für den Start von Ressourcen über ein alternatives Gateway oder ohne Gateway finden Sie unter Optimales HDX-Routing.

Einen Store konfigurieren

So ändern Sie die Store-Einstellungen:

1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus, und klicken Sie im Bereich **Aktionen** auf **Store-Einstellungen konfigurieren**.
2. Gehen Sie zur Registerkarte Benutzerabonnements, um zu konfigurieren, ob Favoriten aktiviert sind.
3. Gehen Sie zur Registerkarte Kerberos-Delegierung, um zu konfigurieren, ob der Store die Kerberos-Delegierung zur Authentifizierung beim Delivery Controller verwendet.
4. Gehen Sie zur Registerkarte Optimales HDX-Routing, um zu konfigurieren, welches Gateway zum Starten von Apps und Desktops entsprechend ihrem Standort verwendet wird.
5. Gehen Sie zur Registerkarte Store bewerben, um zu konfigurieren, ob die Workspace-App den Store dem Benutzer anzeigt, wenn dieser den FQDN oder die E-Mail-Adresse eingibt.



Favoriten

Sie können Benutzern erlauben, Ressourcen als Favoriten festzulegen. Diese Favoriten werden auf der Startseite des Benutzers für schnellen Zugriff angezeigt. Wenn Sie die klassische Oberfläche verwenden und Favoriten deaktivieren, wird die Registerkarte **Startseite** ausgeblendet.

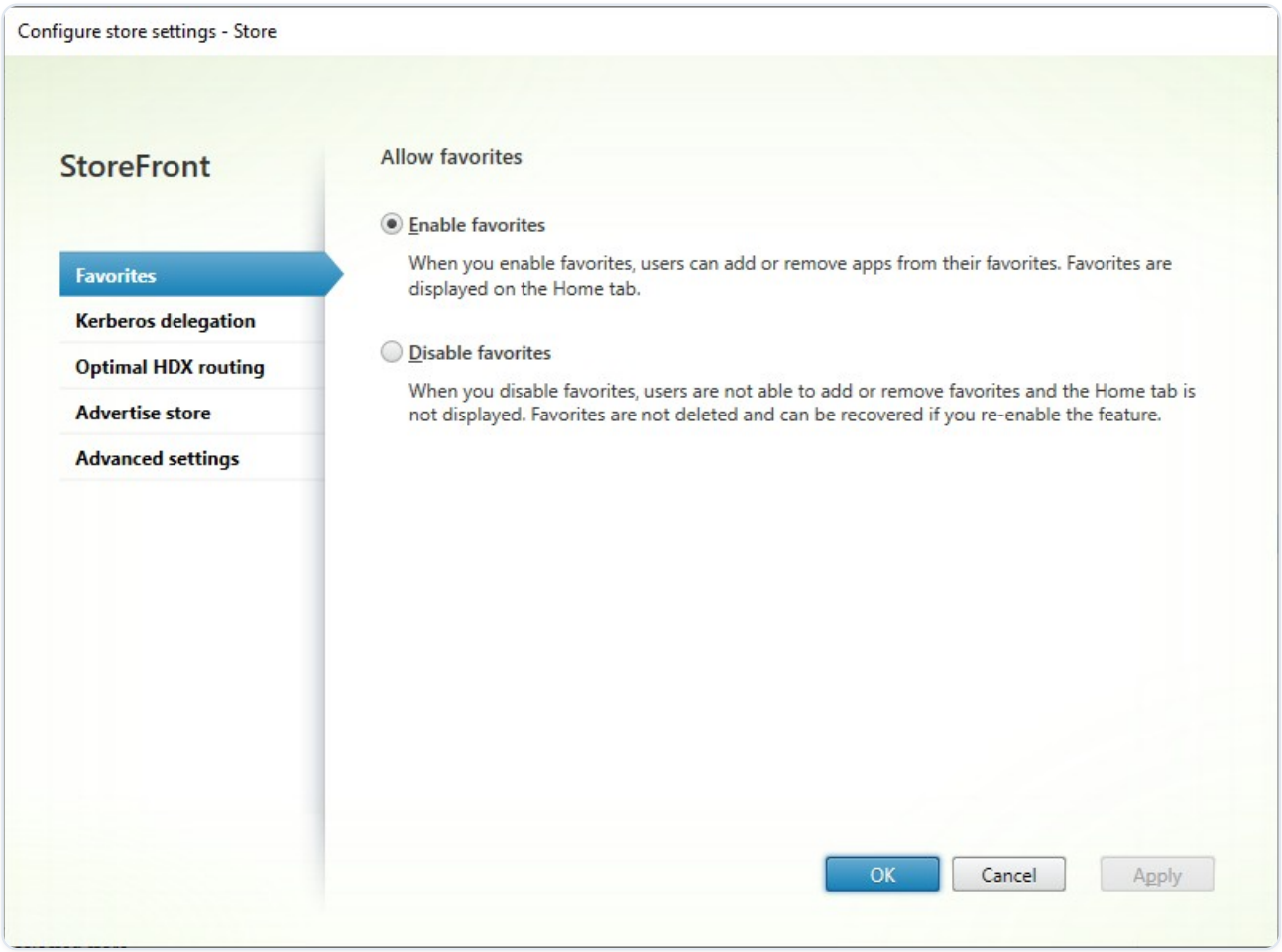
Favoriten aktivieren oder deaktivieren

Verwenden Sie die Favoriten, um eine der folgenden Optionen auszuwählen:

- Benutzern erlauben, Favoriten zu erstellen und zu entfernen. Benutzer können eine App als Favorit festlegen, indem sie auf den Stern auf der App-Kachel klicken. Benutzer können erneut auf den Stern klicken, um eine App aus den Favoriten zu entfernen. Favorisierte Apps werden auf der Registerkarte **Startseite** angezeigt.
- Favoriten deaktivieren. Benutzer können Apps weder als Favoriten festlegen noch aus den Favoriten entfernen. Die Startseite wird nicht angezeigt.

Das Deaktivieren von Abonnements löscht die Abonnementdaten des Stores nicht. Wenn Abonnements für den Store wieder aktiviert werden, kann der Benutzer seine Favoriten beim nächsten Anmelden sehen.

1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus und wählen Sie im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Store-Einstellungen konfigurieren**.
2. Klicken Sie auf die Registerkarte **Benutzerfavoriten**, um die Funktion für Benutzerfavoriten zu aktivieren oder zu deaktivieren.
3. Wählen Sie **Benutzerfavoriten aktivieren**, um Favoriten zu aktivieren.
4. Wählen Sie **Benutzerfavoriten deaktivieren**, um Favoriten zu deaktivieren.



Alternativ können Sie das PowerShell-Cmdlet Set-STFStoreService mit dem Parameter `LockedDown` verwenden. Beispiel zum Deaktivieren von Favoriten:

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

Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:
$False
```

Favoritendatenbank

Standardmäßig werden Favoriten in einer lokalen Datenbank gespeichert, die zwischen Servern in der Servergruppe repliziert wird. Alternativ können Sie Favoriten in einer externen SQL Server-Datenbank speichern.

Um zu sehen, ob der Store eine lokale oder externe Datenbank verwendet, führen Sie das PowerShell-Cmdlet `Get-STFStoreSubscriptionsDatabase` aus. Zum Beispiel:

```
$store = Get-STFStoreService -VirtualPath [store path]

Get-STFStoreSubscriptionsDatabase -StoreService $store
```

Dies gibt zurück:

- `UseLocalStorage` – wenn `True`, werden Favoriten in der lokalen Datenbank gespeichert (Standard). Wenn `False`, werden Favoriten in einer externen Datenbank gespeichert.
- `DatabaseConnectionString` – wenn eine externe Datenbank verwendet wird, enthält dies die Verbindungszeichenfolge. Andernfalls ist es leer.

Weitere Informationen finden Sie unter Verwalten der Abonnementdatenbank.

SQL Server-Datenbank verwenden

Um eine externe SQL Server-Datenbank zu verwenden, führen Sie das PowerShell-Cmdlet `Set-STFStoreSubscriptionsDatabase` aus und geben Sie die Verbindungszeichenfolge an. Weitere Informationen finden Sie unter Abonnementdaten mit Microsoft SQL Server speichern.

Zwei StoreFront-Stores zur gemeinsamen Nutzung des Abonnement-Datenspeichers konfigurieren

Wenn unterschiedliche Konfigurationseinstellungen erforderlich sind, ist es üblich, dass Administratoren StoreFront mit zwei verschiedenen Stores für dieselben Ressourcen konfigurieren; z. B. einen für den externen Zugriff auf Ressourcen über Citrix Gateway und einen anderen für den internen Zugriff über das Unternehmens-LAN. Wenn Sie eine SQL Server-Datenbank verwenden, stellen Sie beide Stores so ein, dass sie dieselbe Datenbankverbindungszeichenfolge verwenden. Bei Verwendung einer lokalen Datenbank erstellt StoreFront standardmäßig eine separate Datenbank für jeden Store. Daher muss ein Benutzer dieselbe Ressource zweimal als Favorit markieren, einmal in jedem Store. Sie können beide Stores so konfigurieren, dass sie dieselbe Datenbank verwenden, damit Benutzer dieselben Favoriten sehen, unabhängig davon, mit welchem Store sie sich verbinden.

Wichtig:

Da der Site-Name Teil des Schlüssels für einen Favoriten ist, müssen Sie sicherstellen, dass die Sites in beiden Stores genau denselben Namen haben.

Angenommen, Sie haben Stores namens „Internal“ und „External“. Wenn Sie eine lokale Datenbank verwenden, verwenden Sie das folgende Skript, um den Store „External“ so zu konfigurieren, dass er dieselbe Abonnementdatenbank wie der Store „Internal“ verwendet.

```
$internalStore=Get-STFStoreService -VirtualPath '/Citrix/Internal'

$internalUri =
$internalStore.SubscriptionStoreClient.ClientEndpoint.Uri.ToString()



$externalStore=Get-STFStoreService -VirtualPath '/Citrix/External'

$externalStore.SubscriptionStoreClient.ClientEndpoint.Uri = $internalUri

Save-STFService $externalStore
```

Übertragen Sie die Konfiguration auf andere Server in der Servergruppe.

Um zu überprüfen, welche lokale Datenbank ein Store verwendet, führen Sie das folgende Skript aus:

```
$store=Get-STFStoreService -VirtualPath '/Citrix/External'

$store.SubscriptionStoreClient.ClientEndpoint.Uri.ToString()
```

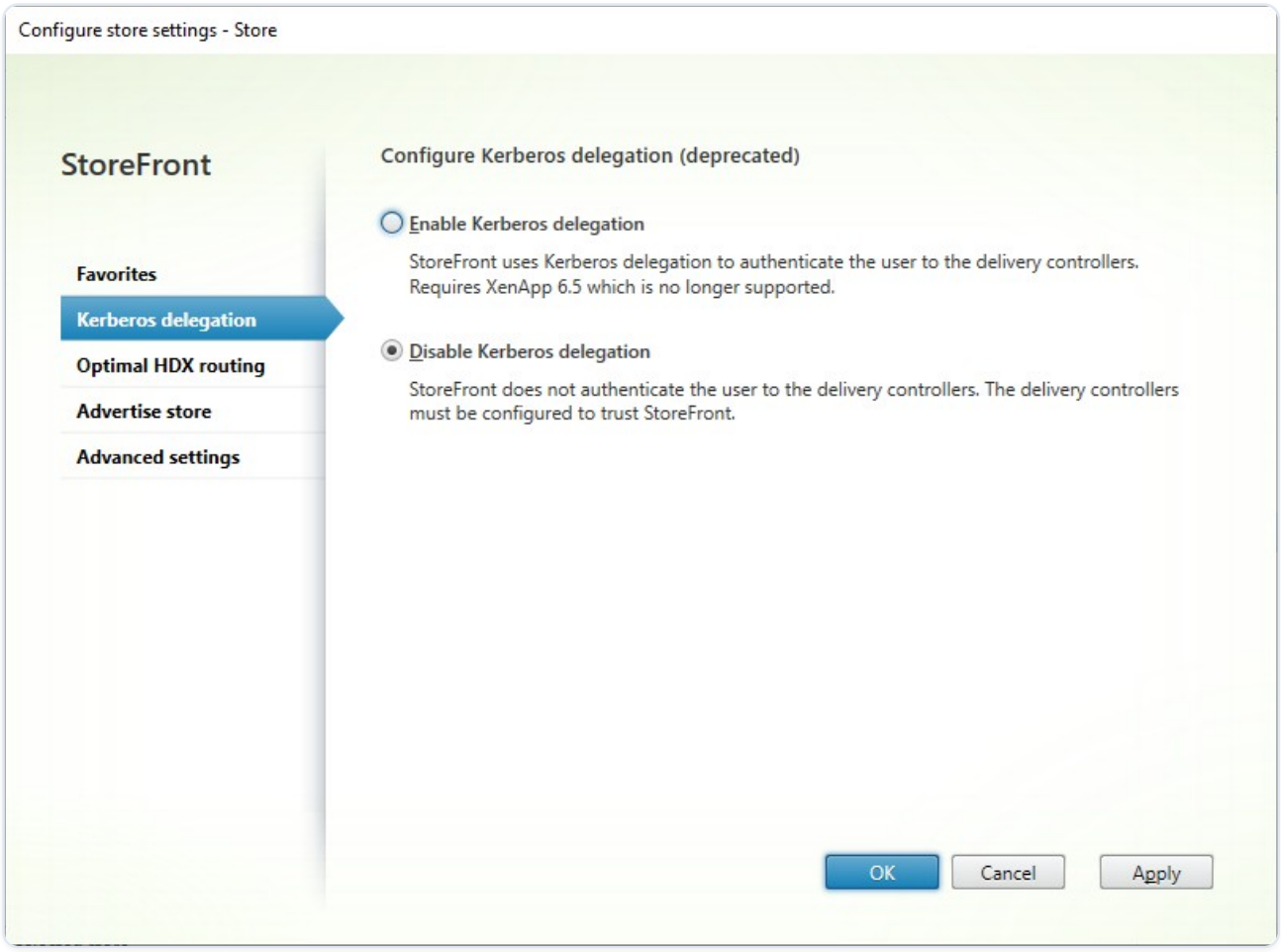
Kerberos-Delegierung

Hinweis:

> Die Kerberos-Delegierung ist veraltet und kann nur mit XenApp 6.5 und früher verwendet werden. Sie kann nicht mit einer unterstützten Version von Citrix Virtual Apps and Desktops verwendet werden.

> Bei Verwendung der Domänen-Pass-Through- 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. Bei Verwendung von XenApp 6.5 und früher können Sie die Kerberos-Delegierung aktivieren, um StoreFront zu ermöglichen, den Benutzer zu imitieren, um sich beim Delivery Controller zu authentifizieren. Dies erfordert, dass die Delegierung in Active Directory konfiguriert wird.

1. Wählen Sie einen Store aus und klicken Sie im Bereich „Aktionen“ auf **Store-Einstellungen konfigurieren**.
2. Wählen Sie die Registerkarte **Kerberos-Delegierung** aus.
3. Wählen Sie, ob Sie **Kerberos-Delegierung aktivieren** oder **Kerberos-Delegierung deaktivieren** möchten.
4. Klicken Sie auf **Übernehmen** oder **OK**, um die Änderungen zu speichern.



PowerShell

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

Optimales HDX™-Routing für einen Store konfigurieren

Konfigurieren Sie das optimale Citrix Gateway-Routing, um die Handhabung des ICA-Verbindungsroutings von der HDX-Engine zu mit StoreFront veröffentlichten Citrix Virtual Apps and Desktops-Anwendungen zu optimieren. Typischerweise befindet sich das optimale Gateway für einen Standort am selben geografischen Ort.

Sie müssen optimale Citrix Gateway-Appliances nur für Bereitstellungen definieren, bei denen die Appliance, über die Benutzer auf StoreFront zugreifen, nicht das optimale Gateway ist. Wenn Starts über das Gateway zurückgeleitet werden sollen, das die Startanforderung stellt, erledigt StoreFront dies automatisch.

Sie können Gateways entweder bestimmten Sites oder Zonen zuordnen. Eine Zone stellt normalerweise ein Rechenzentrum an einem geografischen Standort dar. Sie können ein optimales Gateway mehreren Zonen zuordnen, aber typischerweise sollten Sie eine einzelne Zone

verwenden. Es wird erwartet, dass jede Zone mindestens ein optimales Citrix Gateway hat, das für HDX-Verbindungen zu Ressourcen innerhalb dieser Zone verwendet wird.

Bei Verwendung von Citrix Virtual Apps and Desktops werden Zonen in Studio definiert, und alle in StoreFront definierten Zonen müssen exakt mit den in Studio definierten Zonennamen übereinstimmen. Weitere Informationen finden Sie unter Zonen.

Bei Verwendung von Citrix Desktops as a Service entspricht eine Zone einem Ressourcenstandort. Ressourcenstandorte werden in der Citrix Cloud-Konsole definiert, und alle in StoreFront definierten Zonen müssen exakt mit dem in der Citrix Cloud-Konsole definierten Namen des Ressourcenstandorts übereinstimmen. Weitere Informationen finden Sie unter Ressourcenstandorte einrichten.

Beispielszenario mit Sites

1 x UK Gateway -> 1 x UK StoreFront

- UK-Apps und -Desktops lokal
- US-Apps und -Desktops nur für UK-Failover verwendet

1 x US Gateway -> 1 x US StoreFront

- US-Apps und -Desktops lokal
- UK-Apps und -Desktops nur für US-Failover verwendet

Ein UK-Gateway bietet Remotezugriff auf in Großbritannien gehostete Ressourcen wie Apps und Desktops über ein UK-StoreFront.

Das UK-StoreFront hat sowohl ein in Großbritannien als auch ein in den USA ansässiges Citrix Gateway definiert sowie UK- und US-Sites in seiner Siteliste. UK-Benutzer greifen über ihr geografisch gemeinsam untergebrachtes Gateway, StoreFront und ihre Sites auf Remote-Ressourcen zu. Wenn ihre UK-Sites nicht verfügbar sind, können sie als temporäre Failover-Alternative eine Verbindung zu US-Ressourcen herstellen.

Ohne optimale Gateway-Weiterleitung würden alle ICA-Starts über das UK-Gateway erfolgen, das die Startanfrage gestellt hat, unabhängig davon, wo sich die Ressourcen geografisch befinden. Standardmäßig werden Gateways, die für Startanfragen verwendet werden, von StoreFront dynamisch identifiziert, wenn die Anfrage gestellt wird. Die optimale Gateway-Weiterleitung überschreibt dies und leitet US-Verbindungen über das Gateway, das dem US-Standort am nächsten ist, der Apps und Desktops bereitstellt.

> **Hinweis:**
>
> Sie können pro Standort nur ein optimales Gateway für jeden StoreFront Store zuordnen.

Beispielszenario mit Zonen

1 x CAMZone -> 2 x UK StoreFronts

- Cambridge, UK: Apps und Desktops
- Fort Lauderdale, Eastern US: Apps und Desktops
- Bangalore, Indien: Apps und Desktops

1 x FTLZone -> 2 x US StoreFronts

- Fort Lauderdale, Eastern US: 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, Eastern US: Apps und Desktops

Abbildung 1. Suboptimales Gateway-Routing

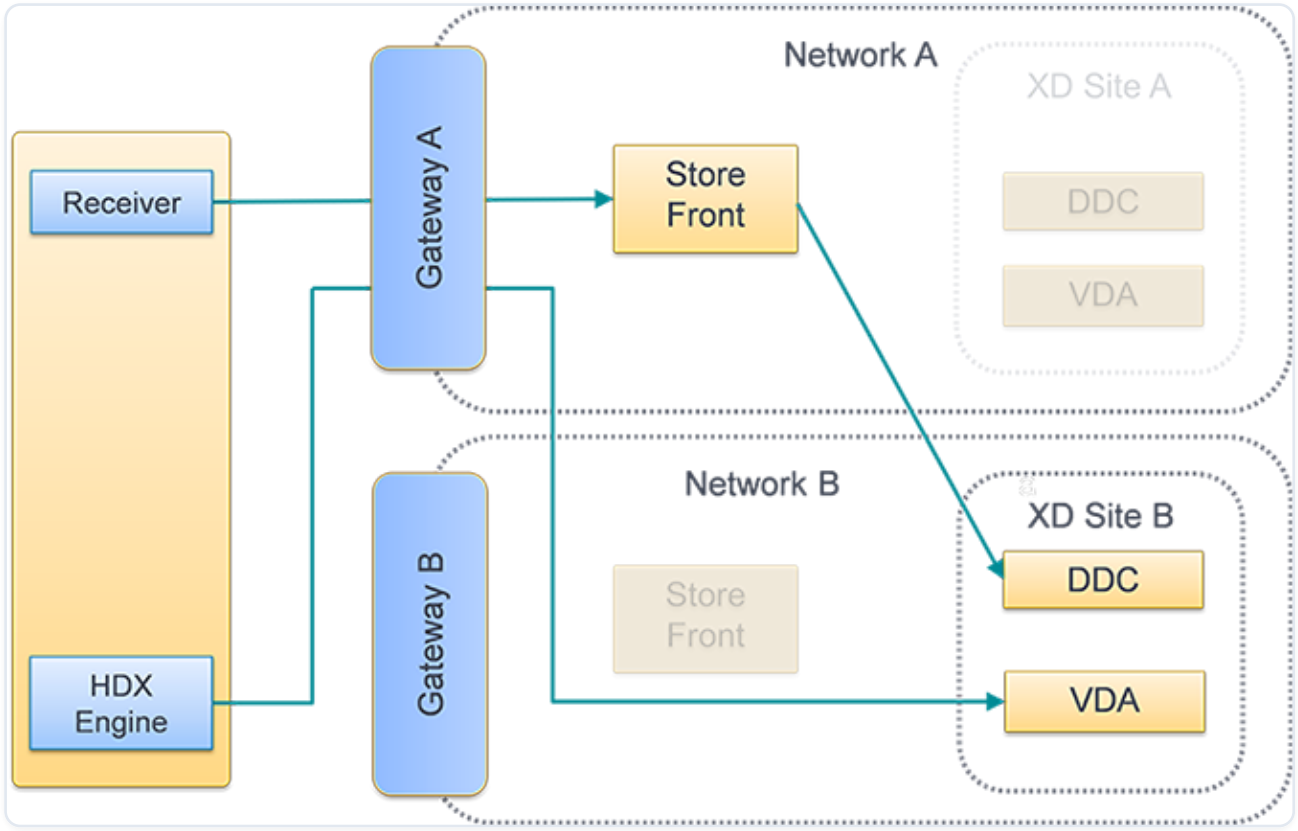
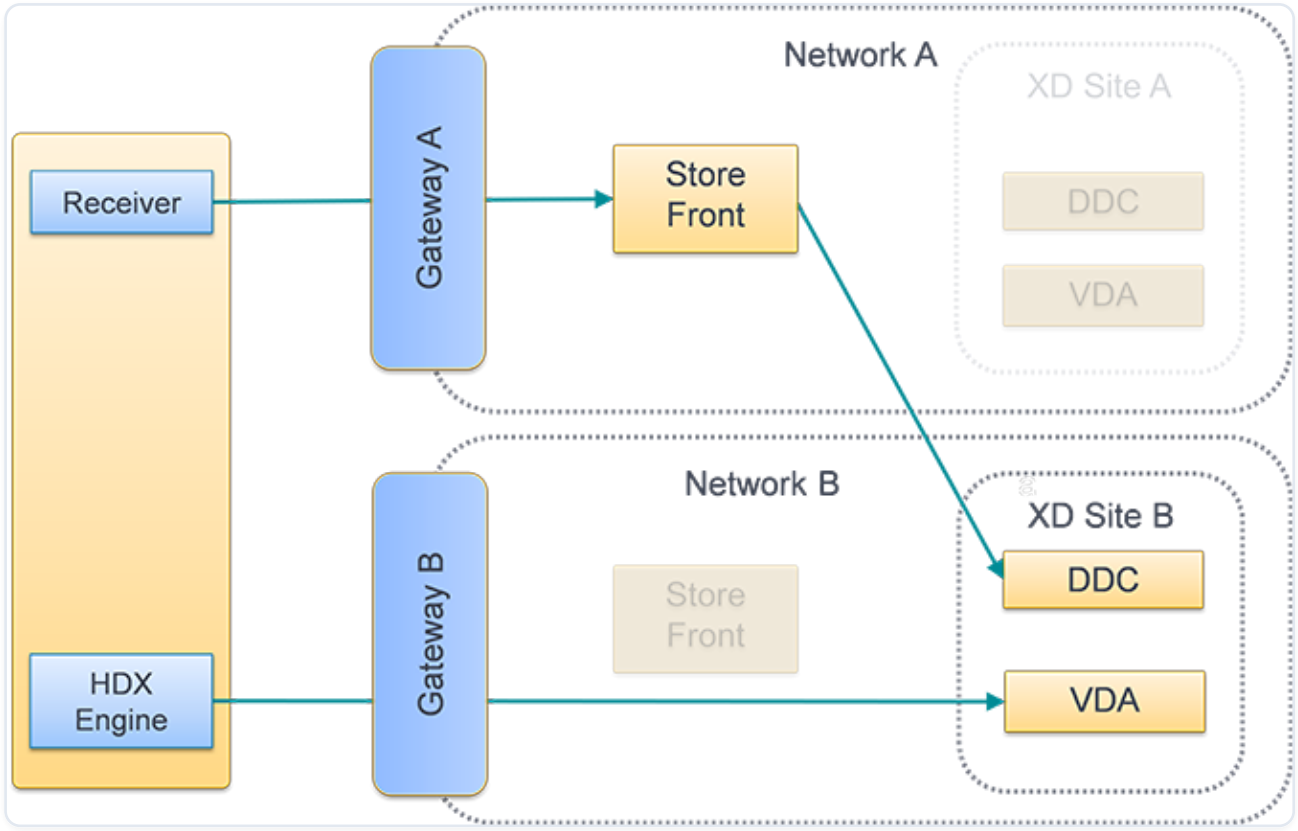


Abbildung 2. Optimales Gateway-Routing



Optimales HDX-Routing konfigurieren

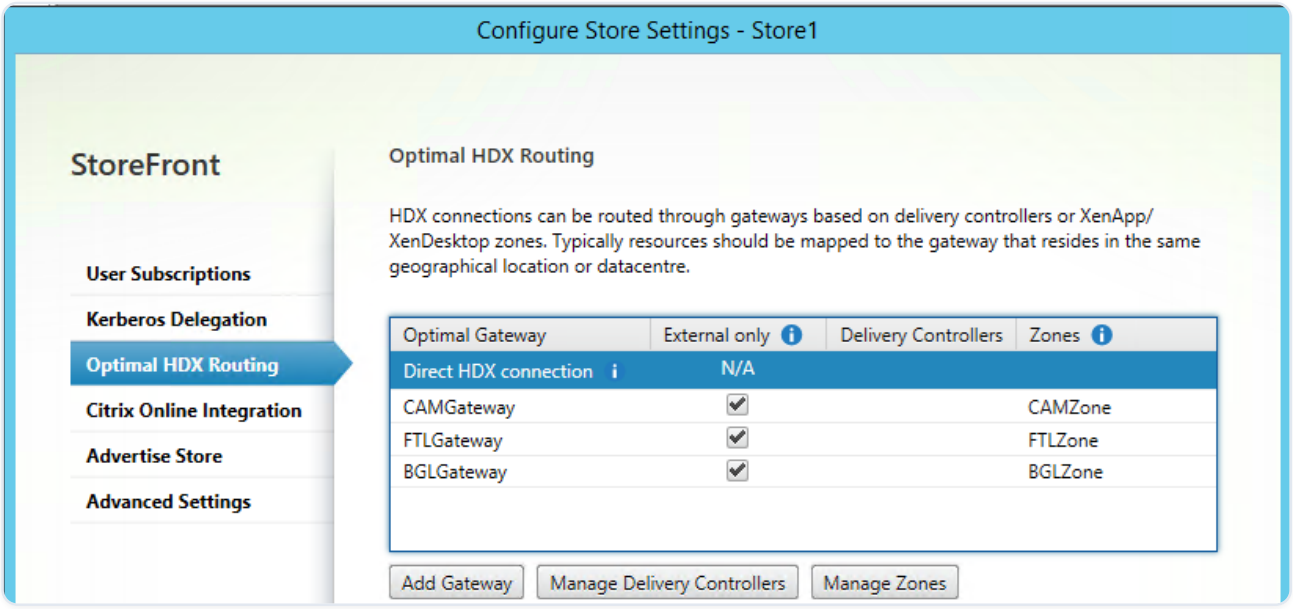
1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole und wählen Sie im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Store-Einstellungen konfigurieren**.
2. Wählen Sie die Registerkarte **Optimales HDX-Routing**.
3. Wählen Sie ein Gateway aus.

    a. Um das Gateway beim Zugriff auf Ressourcen von bestimmten Sites zu verwenden, klicken Sie auf **Sites verwalten** und aktivieren Sie eine oder mehrere Sites.

    b. Um das Gateway beim Zugriff auf Ressourcen von bestimmten Zonen zu verwenden, klicken Sie auf **Zonen verwalten** und geben Sie eine oder mehrere Zonen ein.

    c. Standardmäßig ist nach dem Hinzufügen einer Site oder Zone **Nur extern** aktiviert, was bedeutet, dass 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 sich direkt mit StoreFront verbunden haben, ohne ein Gateway zu verwenden, deaktivieren Sie **Nur extern**.

4. Wenn Sie sich immer direkt mit bestimmten Ressourcen verbinden möchten, ohne ein Gateway zu verwenden, selbst für Benutzer, die remote über ein Gateway auf StoreFront zugreifen, wählen Sie **Direkte HDX-Verbindung** und wählen Sie einige Sites oder Zonen aus.



.

PowerShell zum Konfigurieren des optimalen Citrix Gateway-Routings für einen Store verwenden

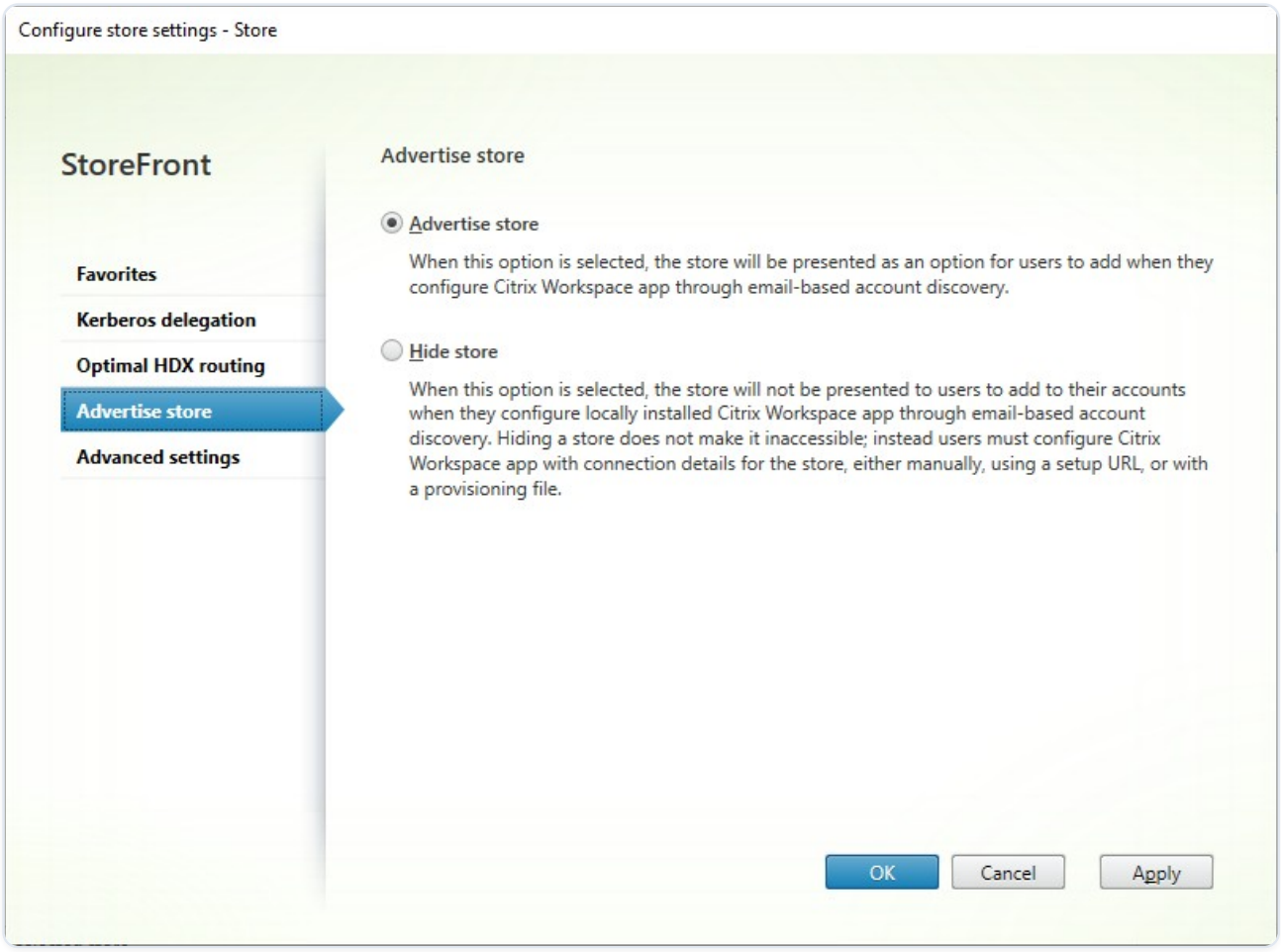
- Um das optimale Gateway-Routing für einen Store zu konfigurieren, verwenden Sie Register-STFStoreOptimalLaunchGateway.
- Um die optimale Gateway-Weiterleitung für einen Store zu entfernen, verwenden Sie Unregister-STFStoreOptimalLaunchGateway.
- Um die optimale Weiterleitung für einen Store anzuzeigen, verwenden Sie Get-STFStoreRegisteredOptimalLaunchGateway.

Stores für Benutzer bewerben oder ausblenden

Sie können wählen, ob Stores Benutzern zur Verfügung gestellt werden, damit sie diese zu ihren Konten hinzufügen können, wenn sie die Citrix Workspace-App über die E-Mail-basierte Kontoerkennung oder FQDN konfigurieren. Standardmäßig wird ein Store, wenn Sie ihn erstellen, als Option für Benutzer angezeigt, die sie in Citrix Receiver hinzufügen können, wenn sie die StoreFront-Bereitstellung entdecken, die den Store hostet. Das Ausblenden eines Stores macht ihn nicht unzugänglich; stattdessen müssen Benutzer die Citrix Workspace-App mit den Verbindungsdetails für den Store konfigurieren, entweder manuell, über eine Setup-URL oder mit einer Bereitstellungsdatei.

> Wichtig:
>
> Bei Bereitstellungen mit mehreren Servern verwenden Sie jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Nach Abschluss, Ihre Konfigurationsänderungen an die Servergruppe weitergeben, damit die anderen Server in der Bereitstellung aktualisiert werden.

1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole und klicken Sie im Bereich **Aktionen** auf **Store-Einstellungen konfigurieren** > **Store bewerben**.
2. Wählen Sie auf der Seite **Store bewerben** entweder **Store bewerben** oder **Store ausblenden**.



Erweiterte Speichereinstellungen

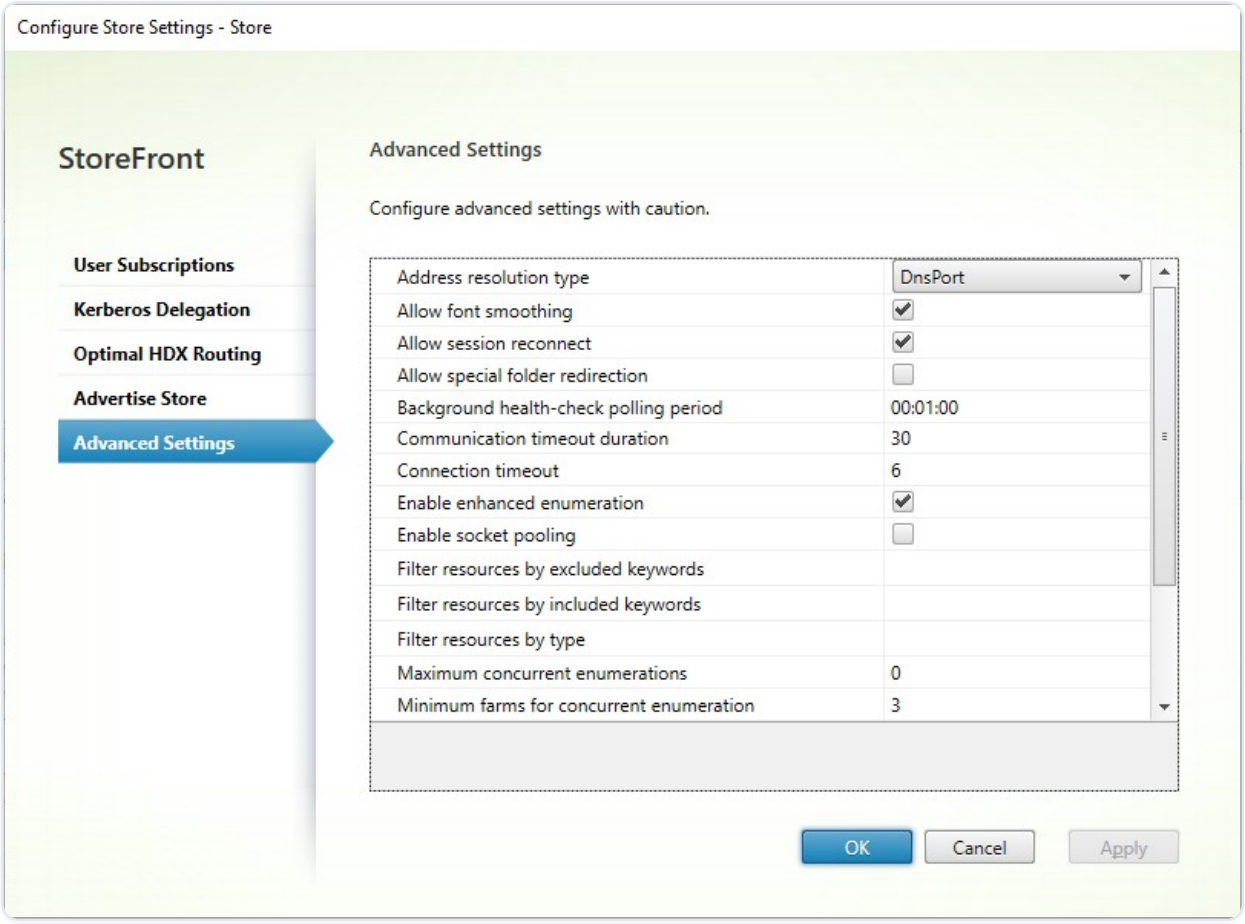
Die meisten erweiterten Speichereigenschaften können Sie über die Registerkarte „Erweiterte Einstellungen“ in Speichereinstellungen konfigurieren konfigurieren. Einige Einstellungen können nur mit PowerShell geändert werden.

> **Wichtig:**

> Verwenden Sie in Bereitstellungen mit mehreren Servern jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Wenn Sie fertig sind, übertragen Sie Ihre Konfigurationsänderungen an die Servergruppe, damit die anderen Server in der Bereitstellung aktualisiert werden.

1. Wählen Sie den Knoten „Stores“ im linken Bereich der Citrix StoreFront-Verwaltungskonsole, wählen Sie einen Store im mittleren Bereich und wählen Sie im Aktionsbereich die Option **Speichereinstellungen konfigurieren**.

2. Wählen Sie auf der Seite **Speichereinstellungen konfigurieren** die Option **Erweiterte Einstellungen** und nehmen Sie die erforderlichen Änderungen vor.



3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Typ der Adressauflösung

Sie können den Typ der vom Server anzufordernden Adresse angeben. Der Standardwert ist DnsPort.

Wählen Sie im Fenster **Erweiterte Einstellungen** einen Wert aus der Dropdown-Liste **Typ der Adressauflösung**.

- Dns
- DnsPort
- IPV4
- IPV4Port
- Dot
- DotPort
- Uri

- NoChange

Schriftglättung zulassen

Sie können festlegen, ob Sie Schriftglättung für HDX™-Sitzungen wünschen. Die Standardeinstellung ist Ein.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Schriftglättung zulassen** aus, und klicken Sie auf **OK**.

Sitzungswiederverbindung zulassen

Sie können festlegen, ob HDX-Sitzungen wiederhergestellt werden sollen. Die Standardeinstellung ist Ein.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Sitzungswiederverbindung zulassen** aus.

Umleitung spezieller Ordner zulassen

Wenn die Umleitung spezieller Ordner konfiguriert ist, können Benutzer spezielle Windows-Ordner für den Server auf die Ordner ihrer lokalen Computer abbilden. Spezielle Ordner beziehen sich auf Standard-Windows-Ordner wie *Dokumente* und *Desktop*, die unabhängig vom Betriebssystem immer auf die gleiche Weise dargestellt werden.

Wählen oder deaktivieren Sie im Fenster **Erweiterte Einstellungen** die Option **Umleitung spezieller Ordner zulassen**, um die Umleitung spezieller Ordner zu aktivieren oder zu deaktivieren, und klicken Sie auf **OK**.

Erweiterte Integritätsprüfung

StoreFront führt regelmäßige Integritätsprüfungen auf jedem Citrix Virtual Apps and Desktops Delivery Controller, Cloud Connector und Secure Private Access Server durch, um die Auswirkungen einer zeitweiligen Serververfügbarkeit zu reduzieren. Mit der erweiterten Integritätsprüfung führt StoreFront eine detailliertere Prüfung durch, die Probleme mit größerer Wahrscheinlichkeit erkennt.

Beim Verbinden mit Citrix Desktops as a Service über einen Cloud Connector bietet die erweiterte Integritätsprüfung den zusätzlichen Vorteil, dass sie weitere Informationen darüber abruft, welche VDAs sich am selben Standort wie der Cloud Connector befinden. Für den Fall, dass die Cloud Connectors Citrix Desktops as a Service nicht kontaktieren können, verwenden die Cloud Connectors ihren lokalen Host-Cache, um Verbindungen zu VDAs zu ermöglichen, die sich am selben Standort befinden. StoreFront verwendet die zusätzlichen Informationen aus den

Ergebnissen der erweiterten Integritätsprüfung, um den am besten geeigneten Online-Connector zu kontaktieren und Apps und Desktops zu starten.

Um die Ressourcenverfügbarkeit während eines Ausfalls zu gewährleisten, ohne Ressourcen in jeder Zone (Ressourcenstandort) veröffentlichen zu müssen, stellen Sie sicher, dass Sie auf allen StoreFront-Servern die Site so konfigurieren, dass alle Cloud Connectors an allen Ressourcenstandorten in der Serverliste enthalten sind und die erweiterte Integritätsprüfung aktiviert ist.

Die erweiterte Integritätsprüfung ist standardmäßig aktiviert. Um die erweiterte Integritätsprüfung zu aktivieren oder zu deaktivieren, verwenden Sie das PowerShell-Cmdlet Set-STFStoreFarmConfiguration mit dem Parameter `AdvancedHealthCheck`. Das Deaktivieren der erweiterten Integritätsprüfung wird nicht empfohlen, da dies die Ausfallsicherheit verringern würde.

Abfrageintervall für Hintergrund-Integritätsprüfung

StoreFront führt regelmäßige Integritätsprüfungen auf jedem Citrix Virtual Apps and Desktops Delivery Controller, Cloud Connector und Secure Private Access-Server durch, um die Auswirkungen einer zeitweiligen Serververfügbarkeit zu reduzieren. Der Standardwert ist jede Minute (00:01:00). Geben Sie im Fenster **Erweiterte Einstellungen** eine Zeit für das **Abfrageintervall für Hintergrund-Integritätsprüfung** an und klicken Sie auf **OK**, um die Häufigkeit der Integritätsprüfung zu steuern. Um die Integritätsprüfung zu deaktivieren, setzen Sie das Abfrageintervall auf 00:00:00; dies wird nicht empfohlen. Das Festlegen eines niedrigen Werts für das Abfrageintervall wird nicht empfohlen, wenn die Erweiterte Integritätsprüfung aktiviert ist, da dies die Leistung beeinträchtigen kann.

Dauer des Kommunikations-Timeouts

Standardmäßig treten bei Anforderungen von StoreFront an einen Server, der Ressourcen für einen Store bereitstellt, nach 30 Sekunden Timeouts auf. Der Server wird nach 1 fehlgeschlagenen Kommunikationsversuch als nicht verfügbar betrachtet. Nehmen Sie im Fenster **Erweiterte Einstellungen** Ihre Änderungen an der Standardzeit vor und klicken Sie auf **OK**, um diese Einstellungen zu ändern.

Verbindungs-Timeout

Sie können die Anzahl der Sekunden angeben, die gewartet werden soll, wenn eine Erstverbindung mit einem Delivery Controller hergestellt wird. Der Standardwert ist 6.

Geben Sie im Fenster **Erweiterte Einstellungen** die Sekunden an, die beim Herstellen der Erstverbindung gewartet werden sollen, und klicken Sie auf **OK**.

Erweiterte Enumeration aktivieren

Diese Option steuert, ob StoreFront Delivery Controller gleichzeitig oder sequenziell abfragt, wenn Apps und Desktops über mehrere Citrix Virtual Apps and Desktops Sites hinweg aufgezählt werden. Die gleichzeitige Enumeration bietet schnellere Antworten auf Benutzeranfragen, wenn Ressourcen über mehrere Sites hinweg aggregiert werden. Wenn diese Option ausgewählt ist (Standard), sendet StoreFront Enumerationsanfragen gleichzeitig an alle Delivery Controller und aggregiert die Antworten, sobald alle geantwortet haben. Sie können die Optionen **Maximale gleichzeitige Enumerationen** und **Minimale Farms für gleichzeitige Enumeration** verwenden, um dieses Verhalten anzupassen.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Erweiterte Enumeration aktivieren** aus (oder deaktivieren Sie sie) und klicken Sie auf **OK**.

Socket-Pooling aktivieren

Socket-Pooling ist in Stores standardmäßig deaktiviert. Wenn Socket-Pooling aktiviert ist, verwaltet StoreFront einen Pool von Sockets, anstatt jedes Mal einen Socket zu erstellen, wenn er benötigt wird, und ihn an das Betriebssystem zurückzugeben, wenn die Verbindung geschlossen wird. Das Aktivieren des Socket-Poolings verbessert die Leistung, insbesondere bei Secure Sockets Layer (SSL)-Verbindungen. Um das Socket-Pooling zu aktivieren, bearbeiten Sie die Store-Konfigurationsdatei. Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Socket-Pooling aktivieren** aus und klicken Sie auf **OK**, um das Socket-Pooling zu aktivieren.

Dateitypzuordnung

Standardmäßig ist die Dateitypzuordnung in Stores aktiviert, sodass Inhalte nahtlos an die abonnierten Anwendungen der Benutzer umgeleitet werden, wenn diese lokale Dateien der entsprechenden Typen öffnen. Um die Dateitypzuordnung zu aktivieren oder zu deaktivieren, verwenden Sie den PowerShell-Befehl Set-STFStoreFarmConfiguration. Beispiel:

```
$storeService = Get-STFStoreService –VirtualPath '/Citrix/Store'

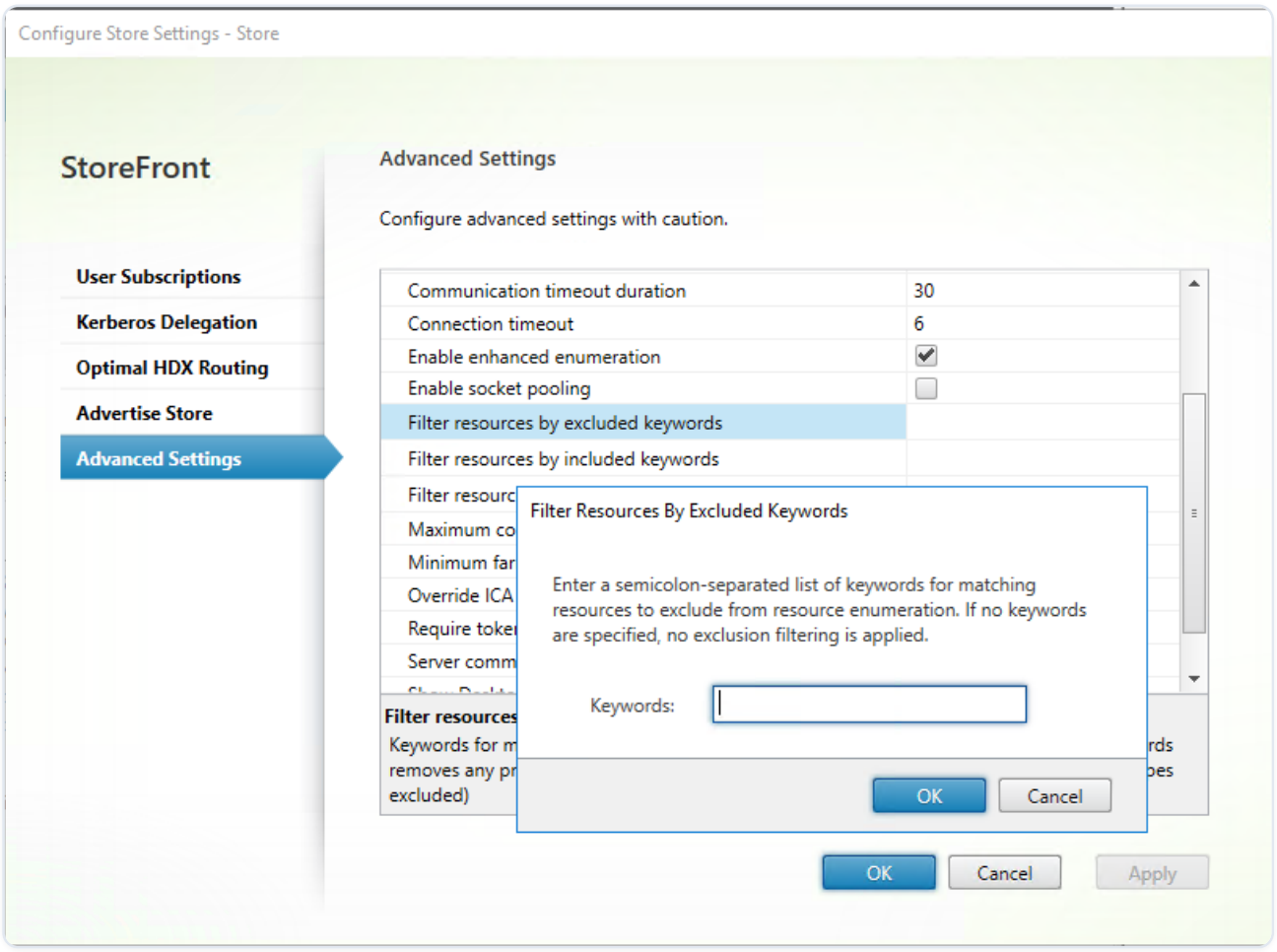
Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
$false
```

Ressourcen nach ausgeschlossenen Schlüsselwörtern filtern

Sie können übereinstimmende Ressourcen nach ausgeschlossenen Schlüsselwörtern filtern. Die Angabe von Ausschluss-Schlüsselwörtern entfernt alle zuvor konfigurierten Einschluss-

Schlüsselwörter. Standardmäßig wird keine Filterung vorgenommen (keine Ressourcentypen ausgeschlossen).

1. Suchen Sie im Fenster **Erweiterte Einstellungen** die Zeile **Ressourcen nach ausgeschlossenen Schlüsselwörtern filtern**.
2. Klicken Sie in die rechte Spalte, um das Fenster **Ressourcen nach ausgeschlossenen Schlüsselwörtern filtern** aufzurufen.
3. Geben Sie eine durch Semikolons getrennte Liste von Schlüsselwörtern in das Feld für Schlüsselwörter ein.
4. Klicken Sie auf **OK**.



Um die Einstellung mit PowerShell zu ändern, verwenden Sie das Cmdlet Set-STFStoreEnumerationOptions mit dem Parameter `-FilterByKeywordsExclude`.

Die folgenden Schlüsselwörter sind reserviert und dürfen nicht zur Filterung verwendet werden:

- Auto
- Mandatory

Ressourcen nach eingeschlossenen Schlüsselwörtern filtern

Sie können übereinstimmende Ressourcen nach Einschluss-Schlüsselwörtern filtern. Die Angabe von Einschluss-Schlüsselwörtern entfernt alle zuvor konfigurierten Ausschluss-Schlüsselwörter. Standardmäßig wird keine Filterung vorgenommen (keine Ressourcentypen ausgeschlossen).

1. Suchen Sie im Fenster **Erweiterte Einstellungen** die Zeile **Ressourcen nach eingeschlossenen Schlüsselwörtern filtern**.
2. Klicken Sie in die rechte Spalte, um das Fenster **Ressourcen nach eingeschlossenen Schlüsselwörtern filtern** aufzurufen.
3. Geben Sie eine durch Semikolons getrennte Liste von Schlüsselwörtern in das Feld für Schlüsselwörter ein.
4. Klicken Sie auf **OK**.

Um die Einstellung mit PowerShell zu ändern, verwenden Sie das Cmdlet Set-STFStoreEnumerationOptions mit dem Parameter `-FilterByKeywordsInclude`.

Die folgenden Schlüsselwörter sind reserviert und dürfen nicht zur Filterung verwendet werden:

- Auto
- Obligatorisch

Ressourcen nach Typ filtern

Wählen Sie die Ressourcentypen aus, die in die Ressourcenaufzählung aufgenommen werden sollen. Die Standardeinstellung ist Keine Filterung (alle Ressourcentypen enthalten).

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Ressourcen nach Typ filtern** aus, klicken Sie rechts daneben, wählen Sie die Ressourcentypen aus, die in die Aufzählung aufgenommen werden sollen, und klicken Sie auf **OK**.

Um die Einstellung mit PowerShell zu ändern, verwenden Sie das Cmdlet Set-STFStoreEnumerationOptions mit dem Parameter `-FilterByTypesInclude`, und geben Sie ein Array von Ressourcentypen an (Anwendungen, Desktops oder Dokumente).

Maximale gleichzeitige Aufzählungen

Geben Sie die maximale Anzahl gleichzeitiger Anforderungen an, die an alle Delivery Controller gesendet werden sollen. Diese Option wird wirksam, wenn die Option **Erweiterte Aufzählung aktivieren** aktiviert ist. Der Standardwert ist 0 (Keine Begrenzung).

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Maximale gleichzeitige Aufzählungen** aus, geben Sie eine Zahl ein und klicken Sie auf **OK**.

Mindestanzahl von Farms für gleichzeitige Aufzählung

Geben Sie die Mindestanzahl von Delivery Controllern an, die erforderlich ist, um eine gleichzeitige Aufzählung auszulösen. Diese Option wird wirksam, wenn die Option **Erweiterte Aufzählung aktivieren** aktiviert ist. Der Standardwert ist 3.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Mindestanzahl von Farms für gleichzeitige Aufzählungen** aus, geben Sie eine Zahl ein und klicken Sie auf **OK**.

ICA®-Clientnamen überschreiben

Überschreibt die Clientnameneinstellung in der .ica-Startdatei mit einer eindeutigen ID, die vom Webbrowser generiert wird. Wenn diese Option deaktiviert ist, gibt die Citrix Workspace-App den Clientnamen an. Standard ist Aus.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **ICA-Clientnamen überschreiben** und klicken Sie auf **OK**.

Token-Konsistenz erforderlich

Wenn diese Option aktiviert ist, erzwingt StoreFront die Konsistenz zwischen dem Gateway, das zur Authentifizierung verwendet wird, und dem Gateway, das für den Zugriff auf den Store verwendet wird. Wenn die Werte inkonsistent sind, müssen sich Benutzer erneut authentifizieren. Sie müssen dies für Smart Access aktivieren. Sie müssen dies deaktivieren, wenn Benutzer über ein Gateway mit deaktivierter Authentifizierung auf den Store zugreifen. Standard ist Ein.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Token-Konsistenz erforderlich** und klicken Sie auf **OK**.

Serverkommunikationsversuche

Geben Sie die Anzahl der Versuche zur Kommunikation mit Delivery Controllern an, bevor diese als nicht verfügbar markiert werden. Standard ist 1.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Serverkommunikationsversuche**, geben Sie eine Zahl ein und klicken Sie auf **OK**.

Desktop Viewer für ältere Clients anzeigen

Geben Sie an, ob das Citrix Desktop Viewer-Fenster und die Symbolleiste angezeigt werden sollen, wenn Benutzer von älteren Clients auf ihren Desktop zugreifen. Standard ist Aus.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Desktop Viewer für ältere Clients anzeigen** und klicken Sie auf **OK**.

Desktops als Apps behandeln

Geben Sie an, ob beim Zugriff auf den Store Desktops in der Ansicht „Apps“ statt in der Ansicht „Desktops“ angezeigt werden. Standard ist Aus.

Wählen Sie im Fenster **Erweiterte Einstellungen** die Option **Desktops als Apps behandeln** und klicken Sie auf **OK**.

Konfiguration des Federated Authentication Service

Der Federated Authentication Service (FAS) bietet Single Sign-On für VDAs mittels Zertifikatsauthentifizierung. Dies ist nützlich bei der Verwendung von Authentifizierungsmethoden wie SAML, bei denen StoreFront keinen Zugriff auf die Active Directory-Anmeldeinformationen hat.

FAS für einen Store aktivieren

Bevor Sie FAS für einen Store aktivieren, müssen Sie die Liste der FAS-Server mithilfe einer Gruppenrichtlinie konfigurieren. Weitere Informationen finden Sie in der FAS-Dokumentation.

Um FAS für einen Store zu aktivieren, müssen Sie das PowerShell-Cmdlet Set-STFStoreLaunchOptions verwenden, um den Anmeldedatenanbieter für die VDA-Anmeldung auf `FASLogonDataProvider` festzulegen.

Beispiel: So aktivieren Sie FAS für einen Store und wählen den Server bei der Anmeldung aus:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider
"FASLogonDataProvider"
```

So deaktivieren Sie FAS für einen Store:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

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

Bei der Verwendung der Benutzername- und Kennwortauthentifizierung in einem Store mit aktiviertem FAS verwendet StoreFront immer FAS anstelle der bereitgestellten Anmeldeinformationen für Single Sign-On.

FAS-Server bei der Anmeldung auswählen

Standardmäßig wählt StoreFront den FAS-Server beim Start aus. Sie können dies ändern, sodass StoreFront den FAS-Server bei der Anmeldung auswählt. Dies ist normalerweise nicht erforderlich, aber Sie können es aktivieren, wenn die FAS-Auswahl langsam ist, um Verzögerungen beim Start zu vermeiden. Um das Verhalten zu konfigurieren, führen Sie das PowerShell-Cmdlet Set-STFClaimsFactoryNames mit dem Parameter `ClaimsFactoryName` aus. Um den FAS-Server bei der Anmeldung auszuwählen, setzen Sie ihn auf `FASClaimsFactory`. Um das Standardverhalten wiederherzustellen und einen FAS-Server beim Start auszuwählen, setzen Sie ihn auf `standardClaimsFactory`.

Beispiel: So wählen Sie einen FAS-Server bei der Anmeldung aus:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"FASClaimsFactory"
```

Nichtverfügbarkeit des FAS-Servers

Wenn der FAS-Server nicht verfügbar ist, schlägt der Start standardmäßig fehl. Sie können StoreFront jedoch so konfigurieren, dass sich Benutzer, wenn der FAS-Server nicht verfügbar ist, beim VDA anmelden können, indem sie ihre Anmeldeinformationen eingeben. Um die Konfiguration zu ändern, verwenden Sie das PowerShell-Cmdlet Set-STFStoreLaunchOptions mit dem Parameter `FederatedAuthenticationServiceFailover`. Beispiel: So aktivieren Sie Failover für einen Store:

```
$storeService = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions $storeService
-FederatedAuthenticationServiceFailover $True
```

Store-Bereitstellungsdateien für Benutzer exportieren

Sie können Dateien generieren, die Verbindungsdetails für Stores enthalten, einschließlich aller für die Stores konfigurierten Citrix Gateway-Bereitstellungen und Beacons. Stellen Sie diese Dateien Benutzern zur Verfügung, damit sie die Citrix Workspace-App automatisch mit den Details der Stores konfigurieren können. Benutzer können auch Bereitstellungsdateien der Citrix Workspace-App herunterladen, wenn sie über einen Webbrowser auf eine Store-Website zugreifen.

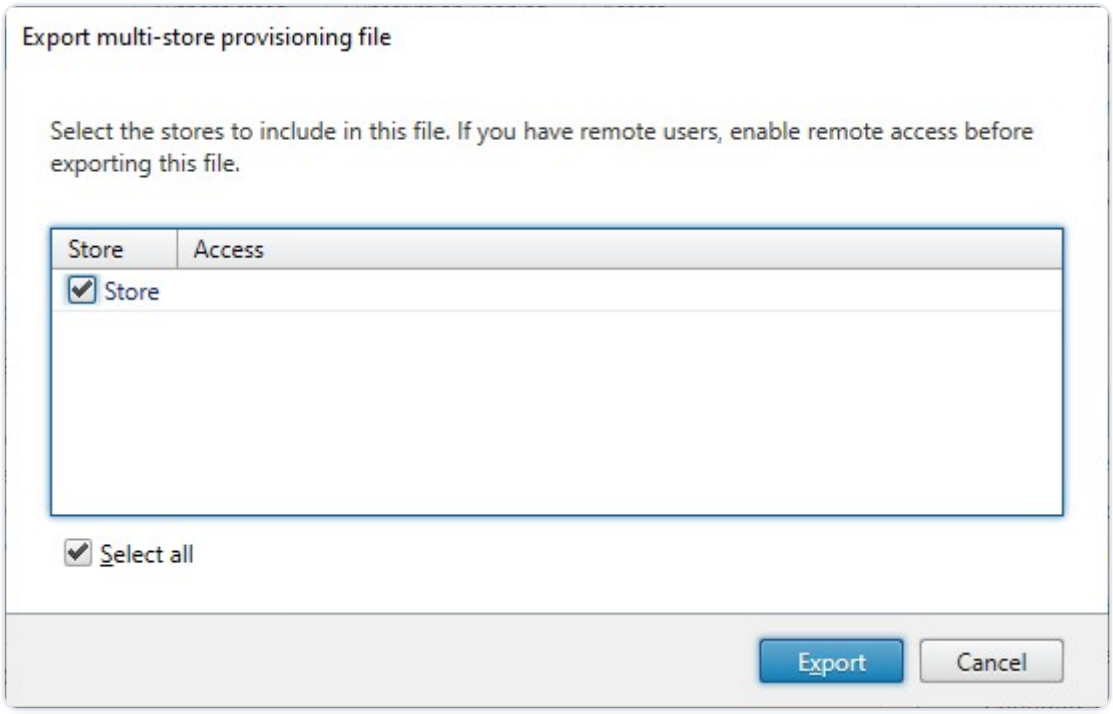
So generieren Sie eine Bereitstellungsdatei, die Details für einen einzelnen Store enthält

1. Wählen Sie in der StoreFront-Verwaltungskonsole den Knoten **Store** aus.
2. Wählen Sie den Store aus, für den Sie eine Bereitstellungsdatei exportieren möchten.
3. Wählen Sie im Bereich **Aktionen** die Option **Bereitstellungsdatei exportieren** aus.
4. Wählen Sie **Exportieren** aus.
5. Wählen Sie einen Speicherort für die Datei und wählen Sie **Speichern** aus.

Screenshot des Bildschirms zum Exportieren von Bereitstellungsdateien(/en-us/storefront/2507-ltsr/media/stores/export-provisioning-file.png)

So generieren Sie Bereitstellungsdateien für mehrere Stores:

1. Wählen Sie in der StoreFront-Verwaltungskonsole den Knoten **Store** aus.
2. Klicken Sie im Bereich Aktionen auf **Bereitstellungsdatei für mehrere Stores exportieren**
3. Wählen Sie die Stores aus, die in die Datei aufgenommen werden sollen.
4. Wählen Sie **Exportieren** aus.
5. Wählen Sie einen Speicherort für die Datei und wählen Sie **Speichern** aus.



Sitzungseinstellungen konfigurieren

Wenn ein Benutzer eine Anwendung startet, generiert StoreFront ein Dokument (bekannt als ICA-Datei), das alle Einstellungen enthält, die die Citrix Workspace-App zum Starten und Konfigurieren dieser Sitzung benötigt.

In den meisten Fällen wird empfohlen, Sitzungseinstellungen mithilfe von Citrix Virtual Apps and Desktops-Richtlinien oder Citrix DaaS-Richtlinien zu ändern. In einigen Fällen ist es jedoch nützlich, diese Einstellungen für einen bestimmten Store zu überschreiben. Dies kann nützlich sein, wenn ein Store Ressourcen von mehreren Sites aggregiert und Sie dieselben Einstellungen auf alle Ressourcen für diesen Store anwenden möchten.

Um Sitzungseinstellungen für einen Store zu definieren, gehen Sie wie folgt vor:

- Verwenden Sie den Global App Config Service. Dies ist ein Dienst in Citrix Cloud. Weitere Informationen finden Sie unter Konfigurieren der Citrix Workspace-App mit dem Global App Configuration Service.
- Fügen Sie auf dem StoreFront-Server Einstellungen zur Datei default.ica des Stores hinzu.

Sie finden default.ica auf dem StoreFront-Server im Verzeichnis `\inetpub\wwwroot\Citrix\[StoreName]\App_Data`.

Eine Liste der verfügbaren Einstellungen finden Sie unter ICA-Einstellungen – Referenz. Einige Einstellungen gelten global. Sie können auch Abschnitte hinzufügen, die für bestimmte Apps

gelten, indem Sie einen Abschnitt hinzufügen, dessen Name genau mit dem in Studio konfigurierten Anwendungsnamen übereinstimmt.

Beispiel: Notepad im Fenstermodus starten

Um eine Anwendung so zu konfigurieren, dass sie im Fenstermodus gestartet wird, fügen Sie in default.ica einen Abschnitt für die Anwendung mit den folgenden Einstellungen hinzu:

- TWIMode – auf „Off“ setzen, um den Fenstermodus zu aktivieren.
- DesiredHRES – optional die horizontale Pixelanzahl.
- DesiredVRES – optional die vertikale Pixelanzahl.

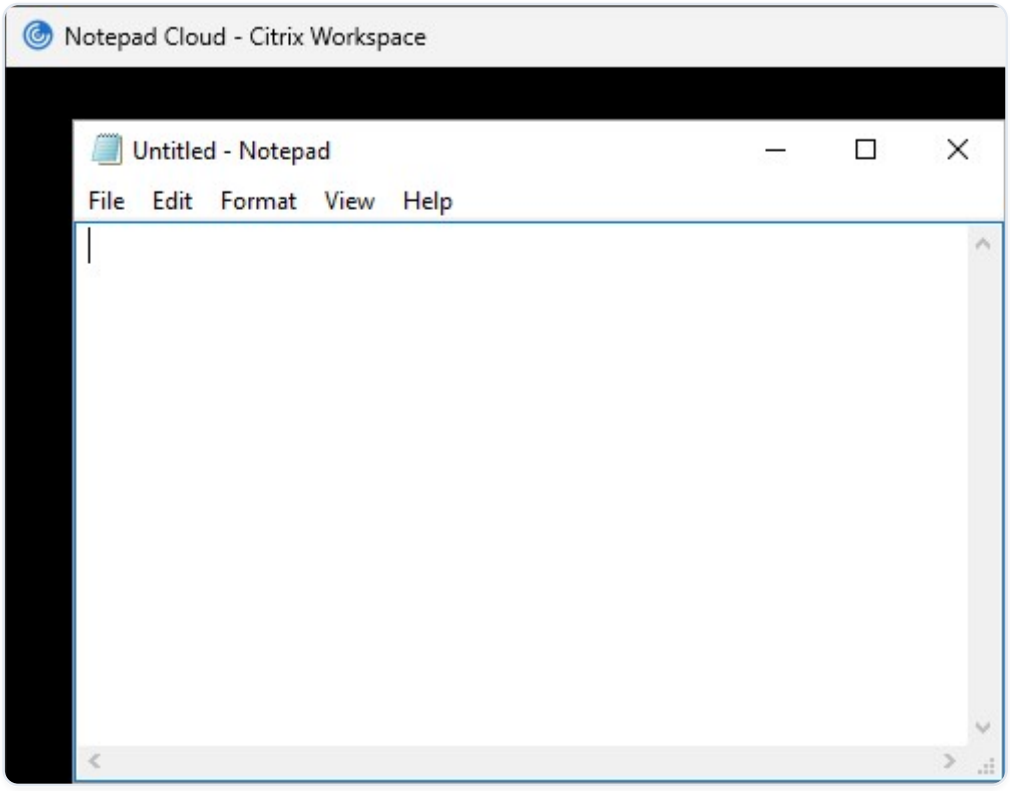
Zum Beispiel:

```
[Notepad]

TWIMode=Off

DesiredHRES=1024

DesiredVRES=768
```



Citrix Workspace™-App-Konfiguration

Global App Config-Dienst

Der Global App Config-Dienst ist ein Cloud-Dienst zur Verwaltung der Citrix Workspace-App-Konfiguration. Innerhalb Ihres Citrix Cloud-Kontos können Sie Ihre Store-URLs beanspruchen und die Konfiguration für jeden Ihrer Stores definieren. Weitere Informationen finden Sie unter Einstellungen für lokale Stores konfigurieren.

Store-Kontoeinstellungen

Als Alternative zum Global App Config-Dienst können Sie die Citrix Workspace-App über die Store-Kontoeinstellungen konfigurieren. Wenn ein Benutzer einen Store zu einer lokal installierten Citrix Workspace-App hinzufügt, ruft diese die Store-Kontoeinstellungen von StoreFront ab. Dies kann Konfigurationseigenschaften umfassen, z. B. um der Citrix Workspace-App für Windows mitzuteilen, ob sie Startmenüverknüpfungen für Apps erstellen soll. Details zu den Eigenschaften finden Sie in der Workspace-App-Dokumentation, z. B. unter Anpassen von App-Verknüpfungsspeicherorten mithilfe von StoreFront-Kontoeinstellungen.

So ändern Sie diese 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 unter dem Abschnitt `Account` den Abschnitt `<annotatedServices>/<annotatedServiceRecord>/<metadata>/<properties>`.
4. Fügen Sie nach dem Element `<clear/>` die Eigenschaften in der Form `<property name="[name]" value="[value]"/>` hinzu. Zum Beispiel:

```
<properties>

    <clear/>

    <property name="PutShortcutsOnDesktop" value="true"/>

    <property name="DesktopDir" value="Citrix Applications"/>

</properties>
```

> **Wichtig**
>
> In Bereitstellungen mit mehreren Servern verwenden Sie jeweils nur einen Server, um die Konfiguration der Servergruppe zu ändern. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Wenn Sie fertig sind, übertragen Sie Ihre Konfigurationsänderungen an die Servergruppe, damit die anderen Server in der Bereitstellung aktualisiert werden.

Workspace-App-Website

Informationen zum Konfigurieren, welche Website-Konfiguration von der lokal installierten Citrix Workspace-App verwendet wird, finden Sie unter Workspace-App-Website konfigurieren.

Integration mit Citrix Gateway und NetScaler ADC

Verwenden Sie Citrix Gateway mit StoreFront, um sicheren Remotezugriff für Benutzer außerhalb des Unternehmensnetzwerks bereitzustellen, und NetScaler ADC für den Lastausgleich.

AUFGABE	DETAILS
Citrix Gateway importieren	Exportieren Sie die Konfiguration von Ihrem Citrix Gateway und importieren Sie sie in StoreFront
Citrix Gateways verwalten	Citrix Gateway-Verbindungseinstellungen hinzufügen, entfernen und bearbeiten
Lastausgleich mit NetScaler ADC	Konfigurieren Sie NetScaler ADC als Lastausgleich vor einer StoreFront-Servergruppe
NetScaler ADC und StoreFront für die delegierte Formularauthentifizierung (DFA) konfigurieren	
Authentifizierung mit verschiedenen Domänen	Konfigurieren Sie StoreFront und Citrix Gateway so, dass sich Benutzer zuerst über das Gateway in einer Domäne und dann bei StoreFront in einer anderen Domäne authentifizieren.
Beacon-Punkte konfigurieren	Konfigurieren Sie Beacon-URLs, die die Citrix Workspace-App verwenden kann, um festzustellen, ob sie sich innerhalb oder außerhalb Ihres Unternehmensnetzwerks befindet.
Ein einzelnes FQDN für interne und externe Nutzung erstellen	Erstellen Sie einen einzelnen vollqualifizierten Domänennamen (FQDN), der direkt aus Ihrem

AUFGABE	DETAILS
	Unternehmensnetzwerk und remote über das Citrix Gateway auf einen Store zugreifen kann.
Citrix Workspace-App erforderlich bei Verbindung über ein Gateway(/de-de/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/require-app.html)	
Entra ID-Authentifizierung über OIDC und Single Sign-On zu VDA(/de-de/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/entra-id-oidc.html)	

Citrix Gateways konfigurieren

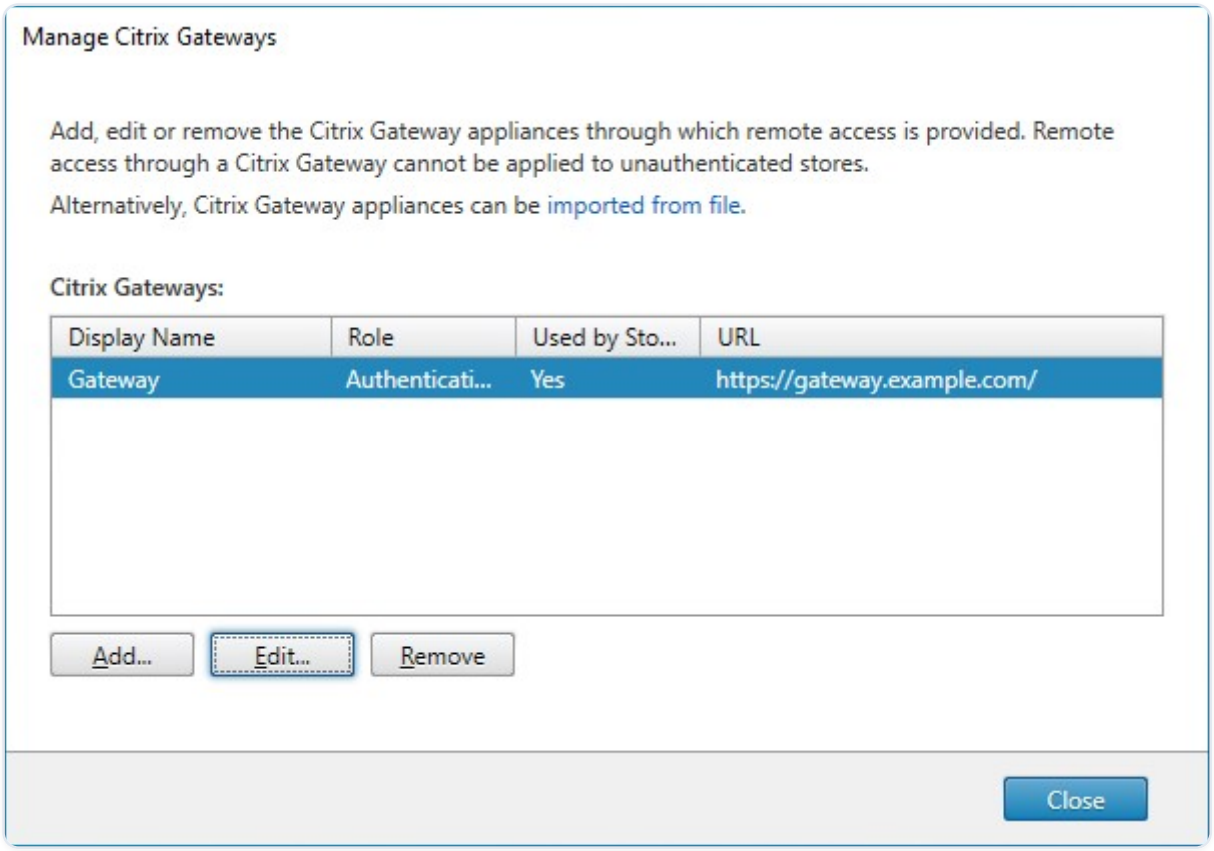
Verwenden Sie Citrix Gateways, um Authentifizierung und Fernzugriff auf StoreFront und Ihre Virtual Delivery Agents (VDAs) bereitzustellen. Citrix Gateways laufen auf Hardware- oder Software-NetScaler ADCs. Der Citrix Gateway Service wird von Citrix verwaltet und kann für HDX-Routing, aber nicht für Authentifizierung oder Fernzugriff auf StoreFront verwendet werden.

Weitere Informationen zum Konfigurieren 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 den Knoten „Stores“ im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus und klicken Sie auf **Citrix Gateways verwalten**. Daraufhin wird das Fenster **Citrix Gateways verwalten** angezeigt.



PowerShell

Um eine Liste der Gateways und ihrer Konfiguration zu erhalten, rufen Sie Get-STFRoamingGateway auf.

Citrix Gateway-Appliance hinzufügen

1. Klicken Sie im Fenster **Citrix Gateways verwalten** auf **Hinzufügen**.
2. Geben Sie auf der Registerkarte „Allgemeine Einstellungen“ die Einstellungen ein und klicken Sie dann auf **Weiter**.

    - Geben Sie einen **Anzeigenamen** für die Citrix Gateway-Bereitstellung an, der Benutzern hilft, diese zu identifizieren.

      Benutzer sehen den von Ihnen angegebenen Anzeigenamen in der Citrix Workspace-App. Fügen Sie daher relevante Informationen in den Namen ein, damit Benutzer entscheiden können, ob sie diese Bereitstellung verwenden möchten. Sie können beispielsweise den geografischen Standort in die Anzeigenamen Ihrer Citrix Gateway-Bereitstellungen aufnehmen, damit Benutzer die für ihren Standort am besten geeignete Bereitstellung leicht identifizieren können.
    - Legen Sie den **Gatewaytyp** auf **Citrix Gateway-Appliance** fest.
    - Geben Sie die URL des Gateways ein.

Der vollqualifizierte Domänenname (FQDN) für Ihre StoreFront-Bereitstellung muss eindeutig und vom FQDN des virtuellen Citrix Gateway-Servers abweichen. Die Verwendung desselben FQDN für StoreFront und den virtuellen Citrix Gateway-Server wird nicht unterstützt. Das Gateway fügt die URL dem `X-Citrix-Via` HTTP-Header hinzu. StoreFront verwendet diesen Header, um zu bestimmen, welches Gateway verwendet wird.

Über die GUI kann nur eine einzige Gateway-URL hinzugefügt werden. Wenn ein Gateway über mehrere URLs zugänglich ist, müssen Sie dasselbe Gateway zweimal mit identischer Konfiguration hinzufügen, abgesehen von der URL. 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 sie mit PowerShell konfigurieren. Sie sollten die Verwaltungskonsole schließen, bevor Sie PowerShell-Befehle ausführen. Wenn Sie beispielsweise mehrere Gateways hinter einem globalen Server-Lastenausgleich haben, ist es in der Regel nützlich, sowohl die GSLB-URL als auch eine URL hinzuzufügen, die für den Zugriff auf jedes spezifische regionale Gateway verwendet werden kann, z. B. zu Test- oder Fehlerbehebungszwecken. Sobald Sie das Gateway erstellt haben, können Sie eine zusätzliche URL mit `Set-STFRoamingGateway` hinzufügen, wobei Sie den Parameter `-GSLBurl` für die sekundäre URL verwenden. Obwohl der Parameter `GSLBurl` heißt, kann er für jede Situation verwendet werden, in der Sie eine zweite URL hinzufügen möchten. Zum Beispiel:

```
Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl
"eugateway.example.com" -GatewayUrl "gslb.example.com"
```

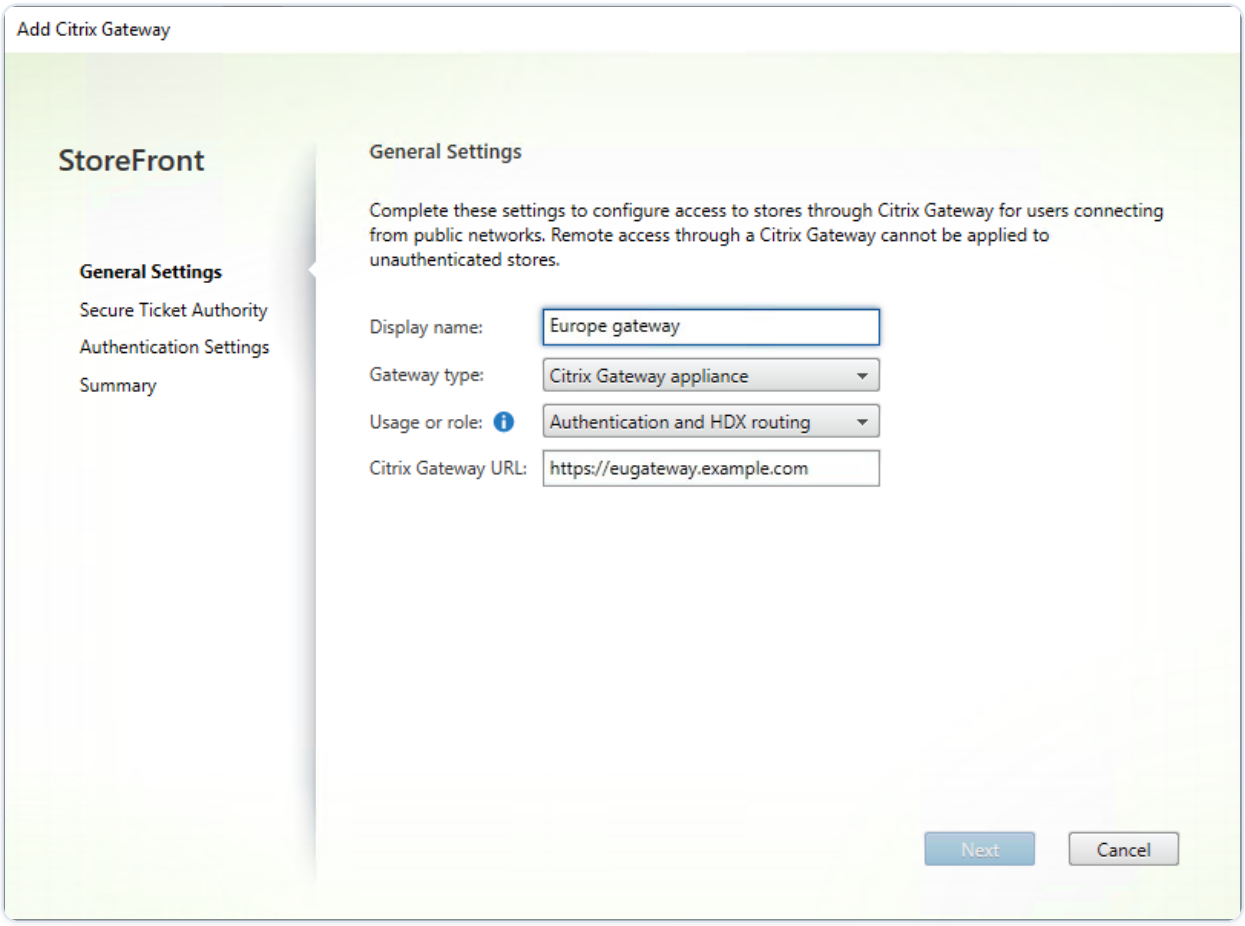
Hinweis:

Entgegen der Intuition enthält in diesem Beispiel der Parameter `GSLBurl` die regionale URL, während der Parameter `GatewayUrl` die GSLB-URL enthält. Für die meisten Zwecke werden die URLs identisch behandelt, und wenn der Store nur über einen Webbrowser aufgerufen wird, können sie auf beide Arten konfiguriert werden. Beim Zugriff auf StoreFront über die Citrix Workspace-App liest diese jedoch die `GatewayUrl` von StoreFront und verwendet sie anschließend für den Fernzugriff, und es ist vorzuziehen, dass sie so konfiguriert ist, dass sie immer eine Verbindung zur 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	Verwenden Sie das Gateway sowohl für die Bereitstellung des Fernzugriffs auf StoreFront als auch für den Zugriff auf die VDAs.
Nur Authentifizierung	Wählen Sie diese Option, wenn das Gateway nur für den Fernzugriff auf StoreFront verwendet wird. Diese Option verhindert, dass Citrix Workspace launcher funktioniert. Wenn Sie daher hybride Starts verwenden müssen, wählen Sie **Authentifizierung und HDX-Routing**, auch wenn das Gateway nur für die Authentifizierung verwendet wird.
Nur HDX-Routing	Wählen Sie diese Option, wenn das Gateway nur für die Bereitstellung des HDX-Zugriffs auf VDAs verwendet wird, z. B. an einem Standort, der keine StoreFront-Instanz hat.



3. Füllen Sie die Einstellungen auf der Registerkarte **Secure Ticketing Authority** aus.

   Die Secure Ticketing Authority stellt Sitzungstickets als Reaktion auf Verbindungsanfragen aus. Diese Sitzungstickets bilden die Grundlage für die Authentifizierung und Autorisierung zur Erkennung der Citrix Workspace-App und für den Zugriff auf VDAs.

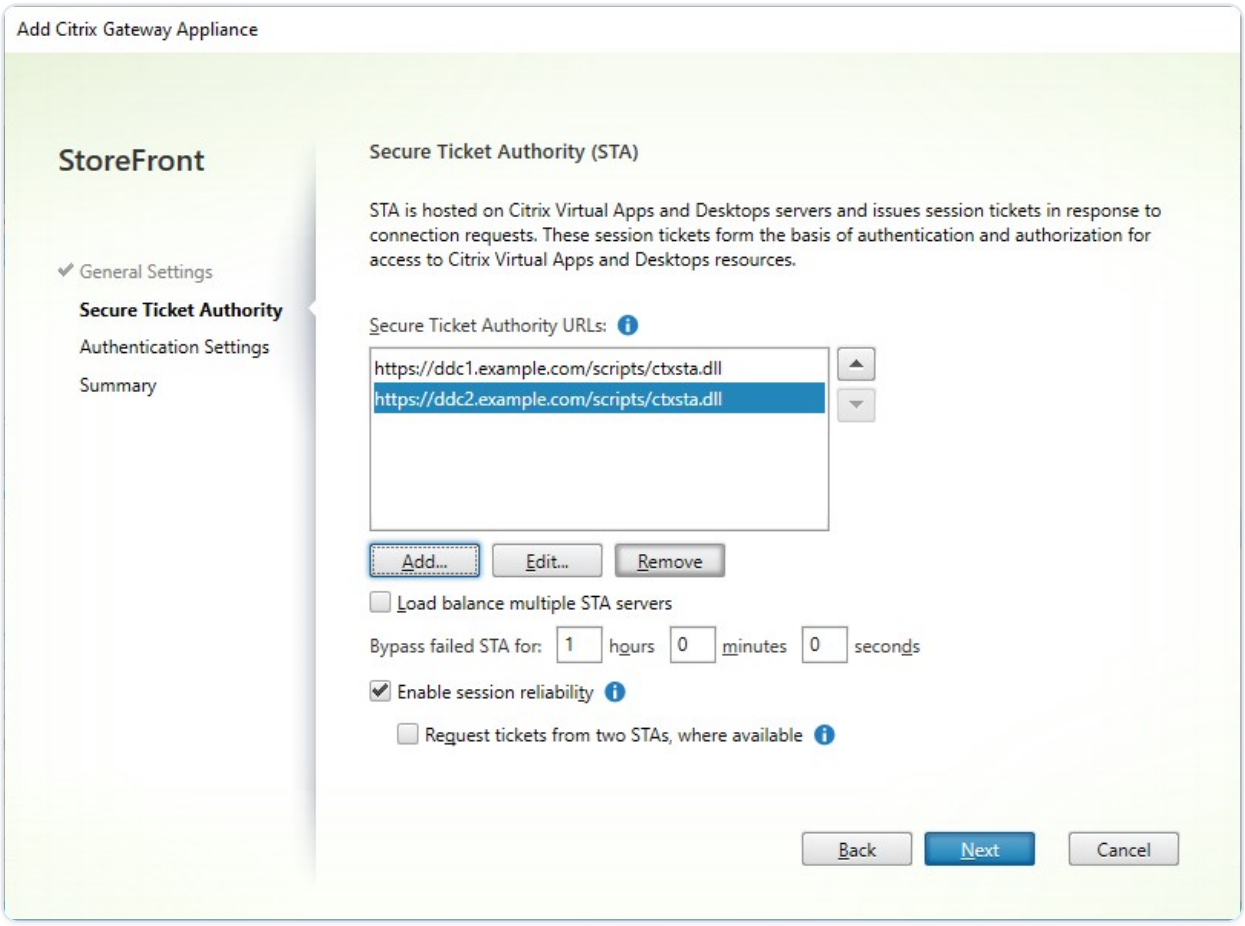
   - Geben Sie eine oder mehrere URL des Secure Ticket Authority-Servers ein.
     - Wenn Sie Citrix Virtual Apps and Desktops™ verwenden, können Sie die Delivery Controller als STA-Server verwenden.
     - Wenn Sie Citrix Desktop as a Service verwenden, können Sie Ihre Cloud Connectors als STA-Server verwenden. Diese leiten entweder Anfragen an die Citrix Cloud™ Ticketing Authority weiter oder generieren im LHC-Modus eigene Tickets. Zukünftig wird sich dies ändern, sodass sie immer eigene Tickets generieren, um die Ausfallsicherheit zu verbessern.
     - Es wird empfohlen, zur Redundanz mindestens 2 STA-Server zu verwenden.
     - Bei der Verwendung von Cloud Connectors als STA-Server wird empfohlen, alle Cloud Connectors in mindestens einem Ressourcenstandort einzuschließen. Erstens stellt Citrix Cloud innerhalb eines Ressourcenstandorts sicher, dass jeweils nur ein Cloud Connector aktualisiert wird, sodass das Einschließen aller Connectors gewährleistet,

dass immer mindestens ein Connector nicht aktualisiert wird. Zweitens, wenn der Ressourcenstandort in den LHC-Modus wechselt, kann nur der einzelne Cloud Connector, der als „gewählter Broker“ bezeichnet wird, STA-Tickets ausstellen. Da Sie nicht im Voraus wissen können, welcher Connector dies sein wird, schließen Sie alle Cloud Connectors am Ressourcenstandort ein.

    - Stellen Sie sicher, dass alle in StoreFront aufgeführten STA-Server auch als STA-Server im virtuellen Citrix Gateway-Server aufgeführt sind. Wenn Server im Citrix Gateway fehlen, kann dies dazu führen, dass Starts fehlschlagen. Wenn heute Cloud Connectors als STAs verwendet werden, ist dies im normalen Betrieb möglicherweise nicht offensichtlich, da jeder Connector verwendet werden kann, um Tickets von der Citrix Cloud Ticketing Authority einzulösen. Im Local Host Cache-Modus generiert der Connector jedoch seine eigenen Tickets, und in Zukunft wird dies das Standardverhalten sein.
    - Der Delivery Controller oder Cloud Connector kann so konfiguriert werden, dass StoreFront einen Sicherheitsschlüssel enthalten muss. Es ist nicht möglich, Sicherheitsschlüssel über die GUI hinzuzufügen; siehe den späteren Schritt zum Hinzufügen über PowerShell.

- Wählen Sie **Mehrere STA-Server lastverteilen**, um Anfragen auf die STA-Server zu verteilen. Wenn diese Option deaktiviert ist, versucht StoreFront die Server in der Reihenfolge, in der sie aufgeführt sind.
- Wenn StoreFront einen STA-Server nicht erreichen kann, vermeidet es die Verwendung dieses Servers für einen bestimmten Zeitraum. Standardmäßig beträgt dieser 1 Stunde, Sie können diesen Wert jedoch anpassen.
- Wenn Citrix Virtual Apps and Desktops getrennte Sitzungen offen halten soll, während die Citrix Workspace-App versucht, automatisch wieder eine Verbindung herzustellen, wählen Sie **Sitzungszuverlässigkeit aktivieren**.
- Wenn Sie mehrere STAs konfiguriert haben, wählen Sie optional **Tickets von zwei STAs anfordern, falls verfügbar**.

  Wenn **Tickets von zwei STAs anfordern, falls verfügbar** ausgewählt ist, ruft StoreFront Sitzungstickets von zwei verschiedenen STAs ab, sodass Benutzersitzungen nicht unterbrochen werden, wenn eine STA während der Sitzung nicht verfügbar wird. Wenn StoreFront aus irgendeinem Grund keine zwei STAs kontaktieren kann, greift es auf die Verwendung einer einzelnen STA zurück.



Nachdem Sie die Einstellungen ausgefüllt haben, klicken Sie auf **Weiter**.

4. Füllen Sie die Einstellungen auf der Registerkarte **Authentifizierungseinstellungen** aus.

   - Wählen Sie die NetScaler® **Version**.
   - Wenn mehrere Gateways dieselbe URL verwenden (typischerweise bei Verwendung eines globalen Server-Lastenausgleichs) und Sie eine Callback-URL eingegeben haben, müssen Sie die VIP des Gateways eingeben. Dadurch kann StoreFront ermitteln, von welchem Gateway die Anforderung stammt und somit, welchen Server es über die Callback-URL kontaktieren 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.

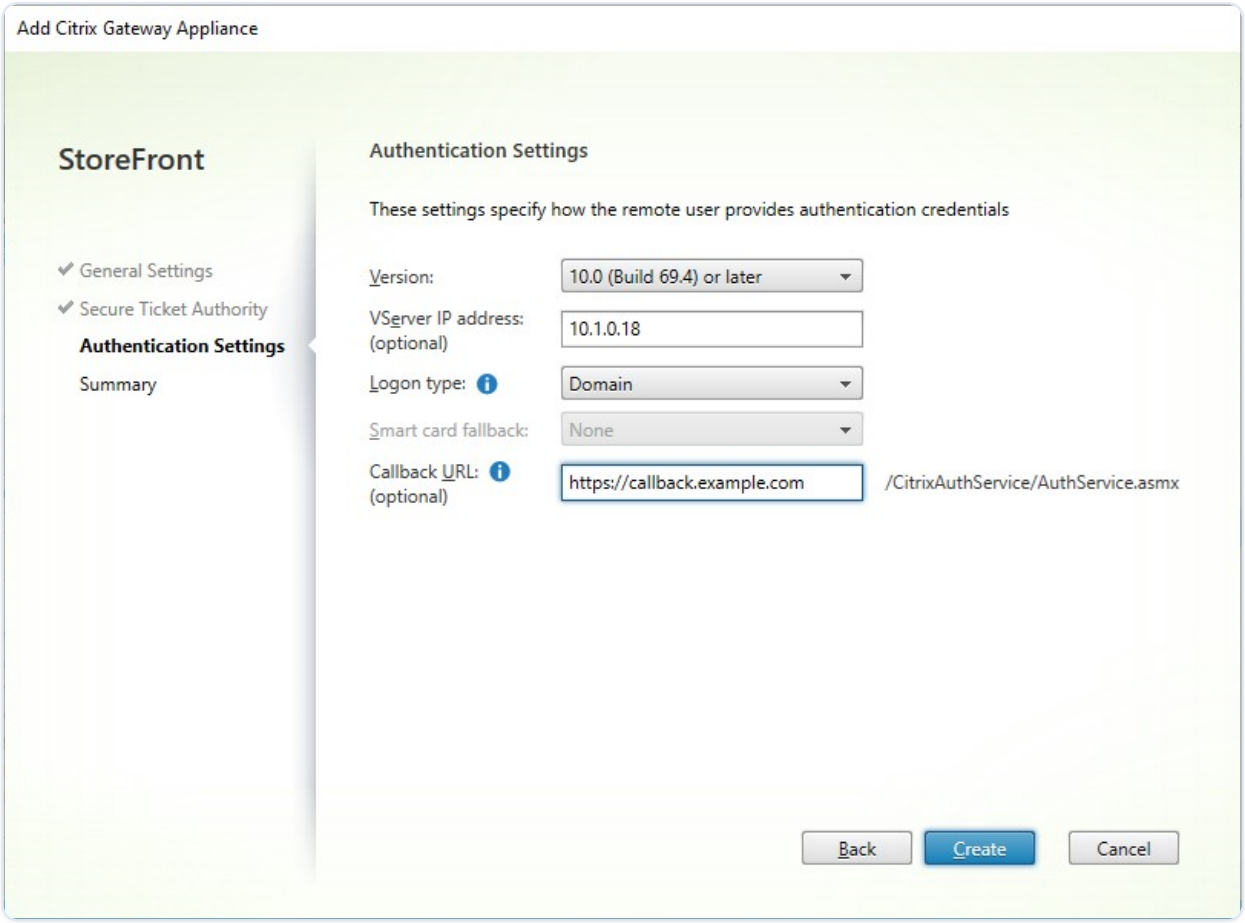
   Die Informationen, die Sie zur Konfiguration Ihres Citrix Gateway-Geräts bereitstellen, werden der Bereitstellungsdatei für den Store hinzugefügt. Dies ermöglicht der Citrix Workspace-App, die entsprechende Verbindungsanforderung zu senden, wenn sie das Gerät zum ersten Mal kontaktiert.

   - Wählen Sie für die LDAP-Authentifizierung **Domäne**.
   - Wählen Sie für die native OTP-Authentifizierung **Sicherheitstoken**.

- Wählen Sie für die LDAP-plus-OTP-Authentifizierung **Domäne und Sicherheitstoken**.
- Wählen Sie für OTP per Textnachricht **SMS-Authentifizierung**.
- Wählen Sie für die Zertifikatsauthentifizierung **Smartcard**.
- Wählen Sie für die SAML-Authentifizierung **Domäne**.
- Wählen Sie für die OIDC-Authentifizierung **Domäne**.

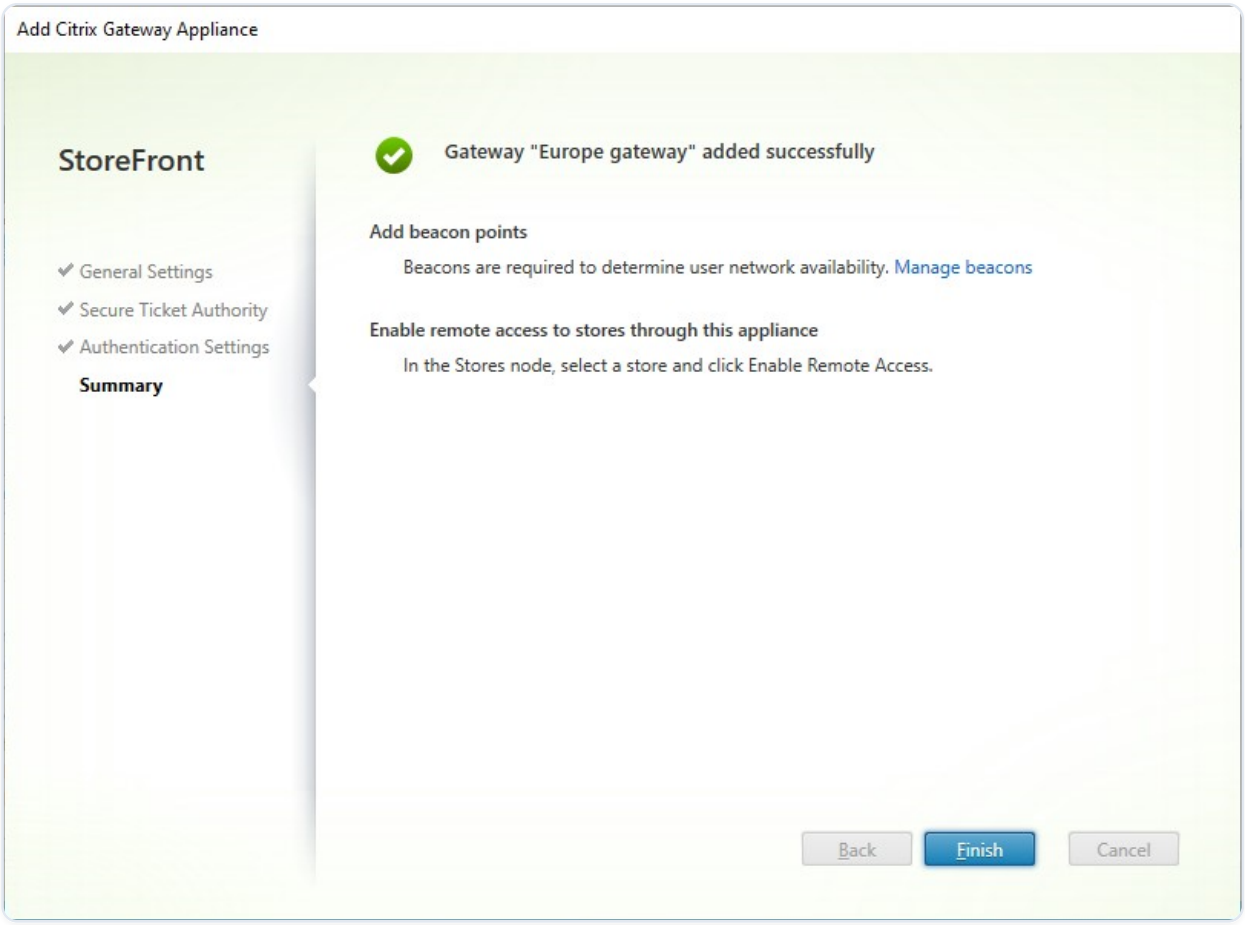
Wenn Sie die Smartcard-Authentifizierung mit einer sekundären Authentifizierungsmethode konfigurieren, auf die Benutzer zurückgreifen können, falls sie Probleme mit ihren Smartcards haben, wählen Sie die sekundäre Authentifizierungsmethode aus der Liste Smartcard-Fallback aus.

- Geben Sie optional die intern zugängliche URL des Gateways in das Feld „Callback-URL“ ein. Dadurch kann StoreFront den Citrix Gateway-Authentifizierungsdienst kontaktieren, um zu überprüfen, ob von Citrix Gateway empfangene Anforderungen von diesem Gerät stammen. Dies ist für Smart Access und für passwortlose Authentifizierungsszenarien wie Smartcard 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.



Nachdem Sie die Einstellungen ausgefüllt haben, klicken Sie auf **Weiter**.

5. Klicken Sie auf **Erstellen**, um die Konfiguration anzuwenden.



6. Nachdem die Bereitstellung angewendet wurde, klicken Sie auf **Fertig stellen**.
7. Wenn Sie Sicherheitsschlüssel konfiguriert haben (empfohlen), müssen Sie die Verwaltungskonsole schließen und diese mithilfe von PowerShell konfigurieren. Zum Beispiel:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

8. Damit Benutzer über das Gateway auf Ihre Stores zugreifen können, konfigurieren Sie den Remote-Benutzerzugriff.

9. Standardmäßig verwendet StoreFront das Gateway, das den Benutzer für das HDX-Routing zu seinen Ressourcen authentifiziert hat. Sie können StoreFront optional so konfigurieren, dass das Gateway beim Zugriff auf bestimmte Ressourcen mithilfe von Optimal HDX routing verwendet wird.

PowerShell

Um ein Gateway mithilfe von PowerShell hinzuzufügen, führen Sie das Cmdlet New-STFRoamingGateway aus.

Citrix Gateway Service hinzufügen

Wenn Sie den Citrix Gateway Service for StoreFront in Citrix Cloud aktiviert haben, müssen Sie ihn als Gateway in StoreFront konfigurieren.

1. Klicken Sie im Fenster **Citrix Gateways verwalten** auf **Hinzufügen**.
2. Geben Sie auf der Registerkarte „Allgemeine Einstellungen“ die Einstellungen ein und klicken Sie dann auf **Weiter**.

   - Geben Sie einen **Anzeigenamen** für die Citrix Gateway-Bereitstellung an, der Benutzern hilft, diese zu identifizieren.

     Benutzer sehen den von Ihnen in der Citrix Workspace-App angegebenen Anzeigenamen. Fügen Sie daher relevante Informationen in den Namen ein, um Benutzern die Entscheidung zu erleichtern, ob sie diese Bereitstellung verwenden sollen. Sie können beispielsweise den geografischen Standort in die Anzeigenamen Ihrer Citrix Gateway-Bereitstellungen aufnehmen, damit Benutzer die für ihren Standort am besten geeignete Bereitstellung leicht identifizieren können.
   - Setzen Sie den **Gateway-Typ** auf **Citrix Gateway Service**. Dadurch wird die **Nutzung oder Rolle** auf **Nur HDX™-Routing** gesetzt und die **Citrix Gateway-URL** deaktiviert.
   - Geben Sie optional eine **Citrix Gateway Service-URL** ein. Wenn die URL leer gelassen wird, wird die standardmäßige kommerzielle URL `https://global.g.nssvc.net` verwendet, die den optimalen Point of Presence für den Standort des Benutzers auswählt. Wenn Sie eine bestimmte Gateway-Region verwenden möchten, z. B. für eine bestimmte Region, können Sie deren URL hier eingeben. Eine Liste der verfügbaren Gateway-Dienst-URLs finden Sie in der Citrix Gateway Service-Dokumentation.
   - Wenn Sie eine **Citrix Gateway Service-URL** eingegeben haben, müssen Sie auch die entsprechende **Citrix Gateway Service-URL (STA-Connector-Modus)** eingeben. Dies gibt die Gateway-Dienst-URL an, die verwendet werden soll, wenn der Cloud Connector

Citrix Cloud nicht erreichen kann und daher eigene STA-Tickets ausstellt. Wenn die URL leer gelassen wird, wird die Standard-URL `https://global-s.g.nssvc.net` verwendet.

Screenshot des Tabs „Allgemeine Einstellungen“ des Bildschirms „Gateway-Appliance hinzufügen“(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/gateway-general-settings-cgs.png)

3. Füllen Sie die Einstellungen auf der Registerkarte **Cloud Connectors** aus.

   Cloud Connectors ermöglichen StoreFront, Citrix Cloud zu erreichen, um die Gateway-Konfiguration nachzuschlagen und die Cloud-Ticketing-Autorität zu erreichen, um Sitzungstickets anzufordern.

   - Geben Sie mindestens eine Cloud Connector-Server-URL ein.

     StoreFront ruft diese Cloud Connectors auf, um STA-Tickets abzurufen, die die Citrix Workspace-App zur Authentifizierung von Anfragen über das Citrix Gateway verwenden kann. Im Normalbetrieb leiten die Cloud Connectors Anfragen an die Citrix Cloud Ticketing Authority weiter oder generieren im LHC-Modus eigene Tickets. Zukünftig wird sich dies ändern, sodass sie immer ihre eigenen Tickets generieren, um die Ausfallsicherheit zu verbessern.

     - Es wird empfohlen, mehrere Cloud Connectors am selben Ressourcenstandort einzuschließen, da an jedem Ressourcenstandort immer nur ein Cloud Connector gleichzeitig aktualisiert wird, wodurch sichergestellt wird, dass mindestens ein Cloud Connector immer verfügbar ist. Für zusätzliche Redundanz fügen Sie Cloud Connectors an mehreren Ressourcenstandorten hinzu.
     - Anstatt jeden Cloud Connector an einem Ressourcenstandort einzeln aufzulisten, können Sie einen Lastenausgleich hinzufügen, der Anfragen zwischen den Cloud Connectors an diesem Standort verteilt. In der Citrix Gateway VServer-Konfiguration müssen Sie jedoch jeden Connector einzeln auflisten.
     - Citrix DaaS kann so konfiguriert werden, dass StoreFront einen Sicherheitsschlüssel enthalten muss. Es ist nicht möglich, Sicherheitsschlüssel über die GUI hinzuzufügen; siehe den späteren Schritt zum Hinzufügen mit PowerShell.

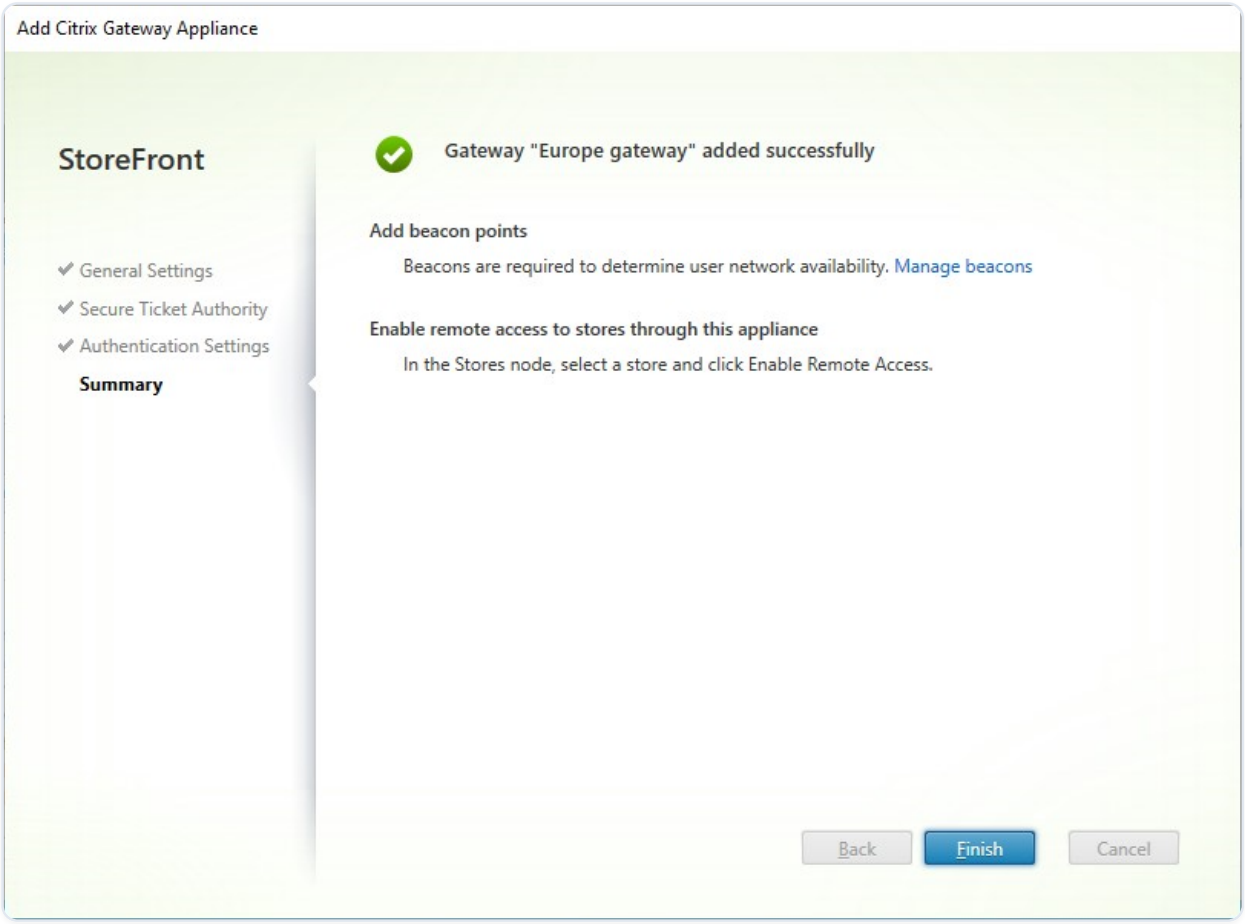
   - Wählen Sie **Mehrere Server lastverteilen**, um Anfragen zwischen den Servern zu verteilen. Wenn diese Option deaktiviert ist, versucht StoreFront die Server in der Reihenfolge, in der sie aufgelistet sind.

- Wenn StoreFront einen Server nicht erreichen kann, vermeidet es die Verwendung dieses Servers für einen bestimmten Zeitraum. Standardmäßig beträgt dieser Zeitraum 1 Stunde, Sie können diesen Wert jedoch anpassen.
- Wählen Sie optional **Sitzungszuverlässigkeit aktivieren**.
- Wählen Sie optional **Tickets von zwei Cloud Connectors anfordern, falls verfügbar**.

Screenshot des Tabs „Cloud Connectors“ des Bildschirms „Gateway-Appliance hinzufügen“(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/gateway-cloud-connectors.png)

Nachdem Sie die Einstellungen ausgefüllt haben, wählen Sie **Weiter**.

4. Wählen Sie **Erstellen**, um die Konfiguration anzuwenden.



5. Nachdem die Bereitstellung angewendet wurde, wählen Sie **Fertig stellen**.
6. Wenn Sie Sicherheitsschlüssel (empfohlen) konfiguriert haben, müssen Sie die Verwaltungskonsole schließen und diese mithilfe von PowerShell konfigurieren. Zum Beispiel:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
```

```
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

7. Standardmäßig verwendet StoreFront dasselbe Gateway für den Zugriff auf Ressourcen, das auch zur Authentifizierung verwendet wurde, weshalb der Citrix Gateway-Dienst nie verwendet wird. Sie müssen Optimales HDX-Routing verwenden, um zu konfigurieren, wann StoreFront den Citrix Gateway-Dienst verwenden soll.

PowerShell

Um ein Gateway mithilfe von PowerShell hinzuzufügen, führen Sie das Cmdlet New-STFRoamingGateway aus und legen Sie `-IsCloudGateway $true` fest.

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-Appliance hinzufügen

2. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

PowerShell

Um die Gateway-Konfiguration mithilfe von PowerShell zu ändern, führen Sie das Cmdlet Set-STFRoamingGateway aus.

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

Um das Gateway mithilfe von PowerShell zu entfernen, führen Sie das Cmdlet Remove-STFRoamingGateway aus.

Citrix Gateway importieren

Die in der Citrix Gateway-Verwaltungskonsole konfigurierten Remotezugriffseinstellungen müssen mit den in StoreFront konfigurierten Einstellungen identisch sein. Dieser Artikel zeigt Ihnen, wie Sie die Details eines virtuellen Citrix Gateway-Servers importieren, damit Citrix Gateway und StoreFront korrekt für die Zusammenarbeit konfiguriert sind.

Anforderungen

- NetScaler 11.1.51.21 oder höher ist erforderlich, um mehrere Gateway-vServer in eine ZIP-Datei zu exportieren.

  > **Hinweis:**
  >
  > Citrix Gateways können nur Gateway-vServer exportieren, die mit dem Citrix Virtual Apps and Desktops™-Assistenten erstellt wurden.

- Es muss möglich sein, dass DNS alle STA (Secure Ticket Authority)-Server-URLs in der von Citrix Gateway generierten Datei GatewayConfig.json innerhalb der ZIP-Datei auflöst und dass StoreFront diese kontaktieren kann.
- Die Datei GatewayConfig.json innerhalb der von Citrix Gateway generierten ZIP-Datei muss die URL einer vorhandenen Citrix Receiver für Web-Site auf dem StoreFront-Server enthalten. Citrix Gateway 11.1 und höher erledigt dies, indem es den StoreFront-Server kontaktiert und alle vorhandenen Stores und Websites auflistet, bevor die ZIP-Datei für den Export generiert wird.
- StoreFront muss in der Lage sein, die Callback-URL im DNS zur IP-Adresse des Gateway-VPN-vServers aufzulösen, damit die Authentifizierung über das importierte Gateway erfolgreich ist.

  Die von Ihnen verwendete Kombination aus Callback-URL und Port ist in der Regel dieselbe wie die Kombination aus Gateway-URL und Port, solange StoreFront diese URL auflösen kann.

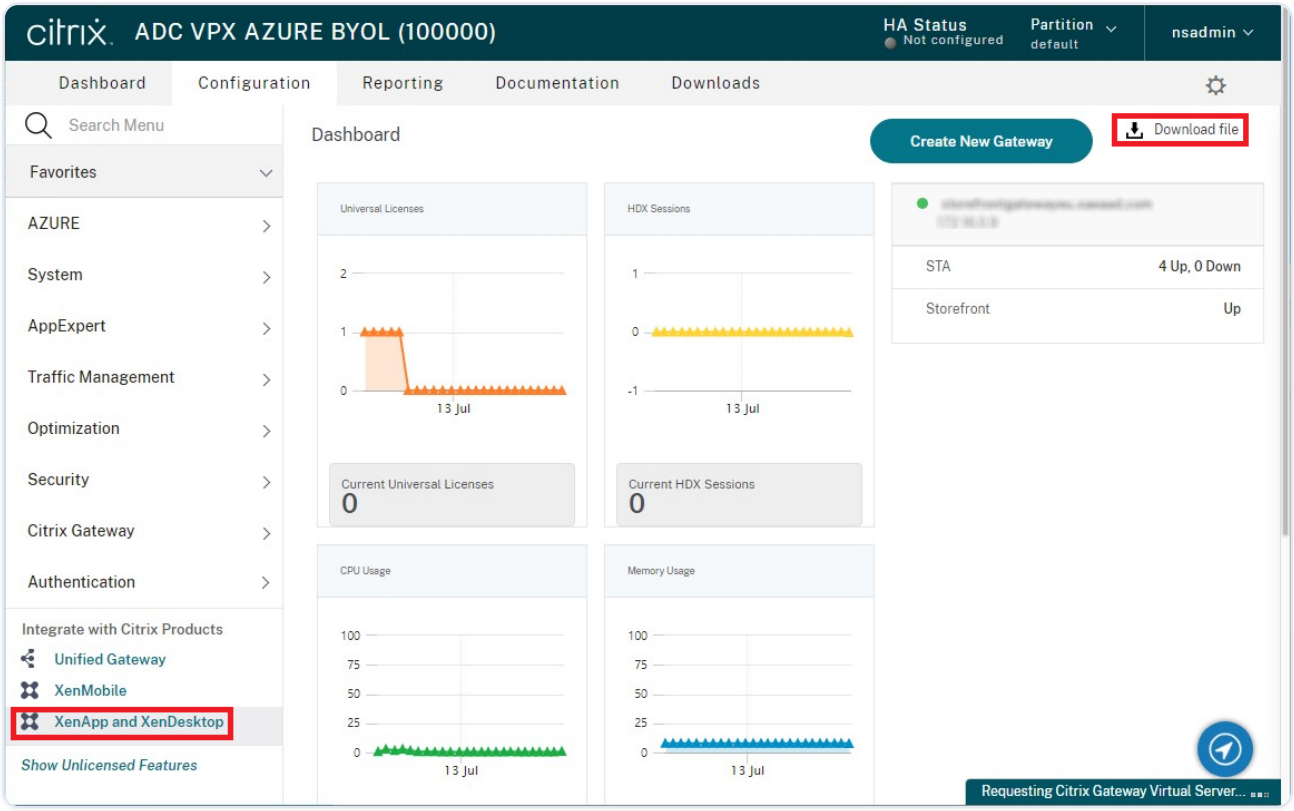
  oder

  Die Kombination aus Callback-URL und Port kann sich von der Kombination aus Gateway-URL und Port unterscheiden, wenn Sie in Ihrer Umgebung unterschiedliche externe und interne DNS-Namespaces verwenden. Wenn sich Ihr Gateway in einer DMZ befindet und eine `<example.com>` URL verwendet und StoreFront sich in Ihrem privaten

Unternehmensnetzwerk befindet und eine `<example.local>` URL verwendet, können Sie eine `<example.local>` Callback-URL verwenden, um auf den Gateway-vServer in der DMZ zurückzuverweisen.

Konfiguration von Citrix Gateway exportieren

1. Melden Sie sich bei Citrix Gateway an.
2. Gehen Sie zur Registerkarte „Configuration“ (Konfiguration).
3. Klicken Sie unter „Integrate with Citrix Products“ (In Citrix Produkte integrieren) auf „XenApp and XenDesktop®“.
4. Klicken Sie oben rechts auf „Download file“ (Datei herunterladen).



1. Wählen Sie, ob Sie die Konfiguration für alle Gateways oder ein bestimmtes Gateway herunterladen möchten.

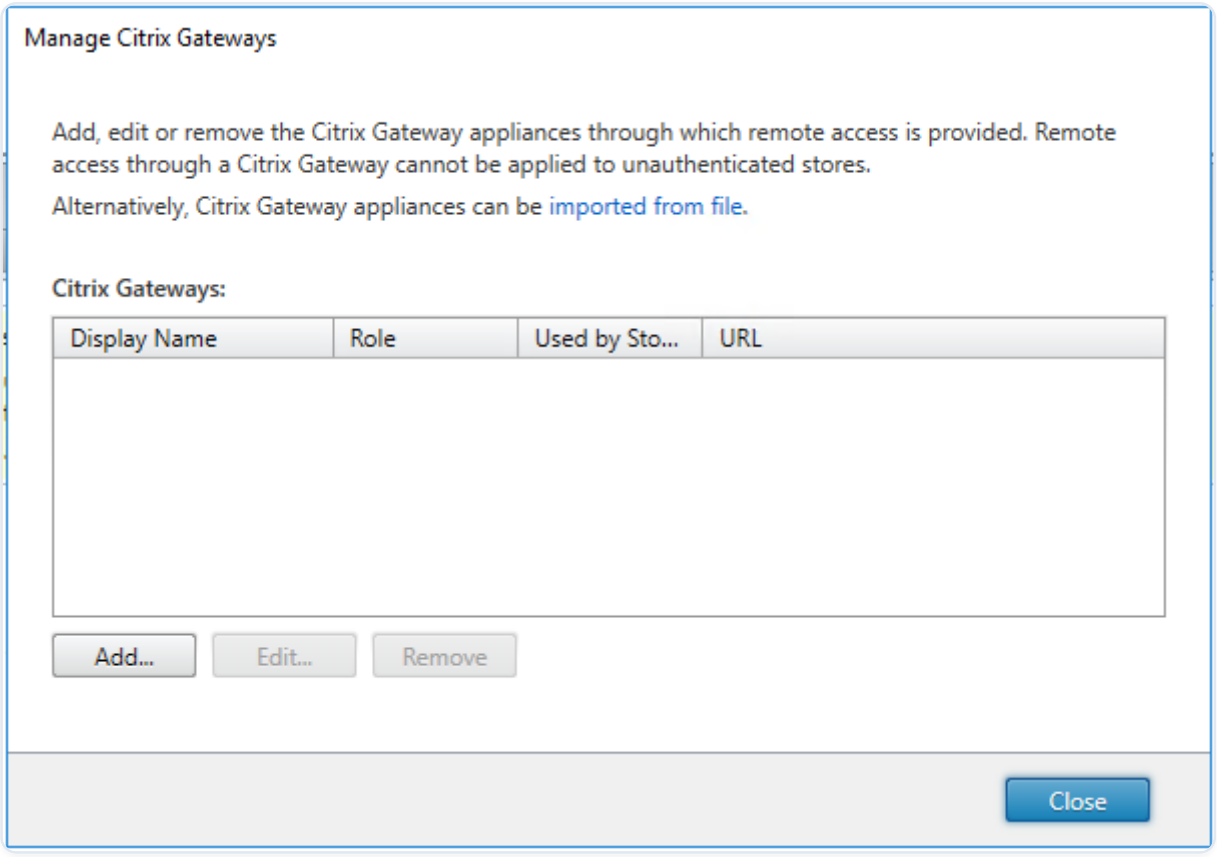
Importieren eines Citrix Gateways über die Konsole

Sie können eine oder mehrere virtuelle Citrix Gateway-Serverkonfigurationen mit derselben Importdatei importieren. Wenn Sie mehrere virtuelle Gateway-Server von verschiedenen Citrix Gateways haben, müssen Sie mehrere Importdateien verwenden.

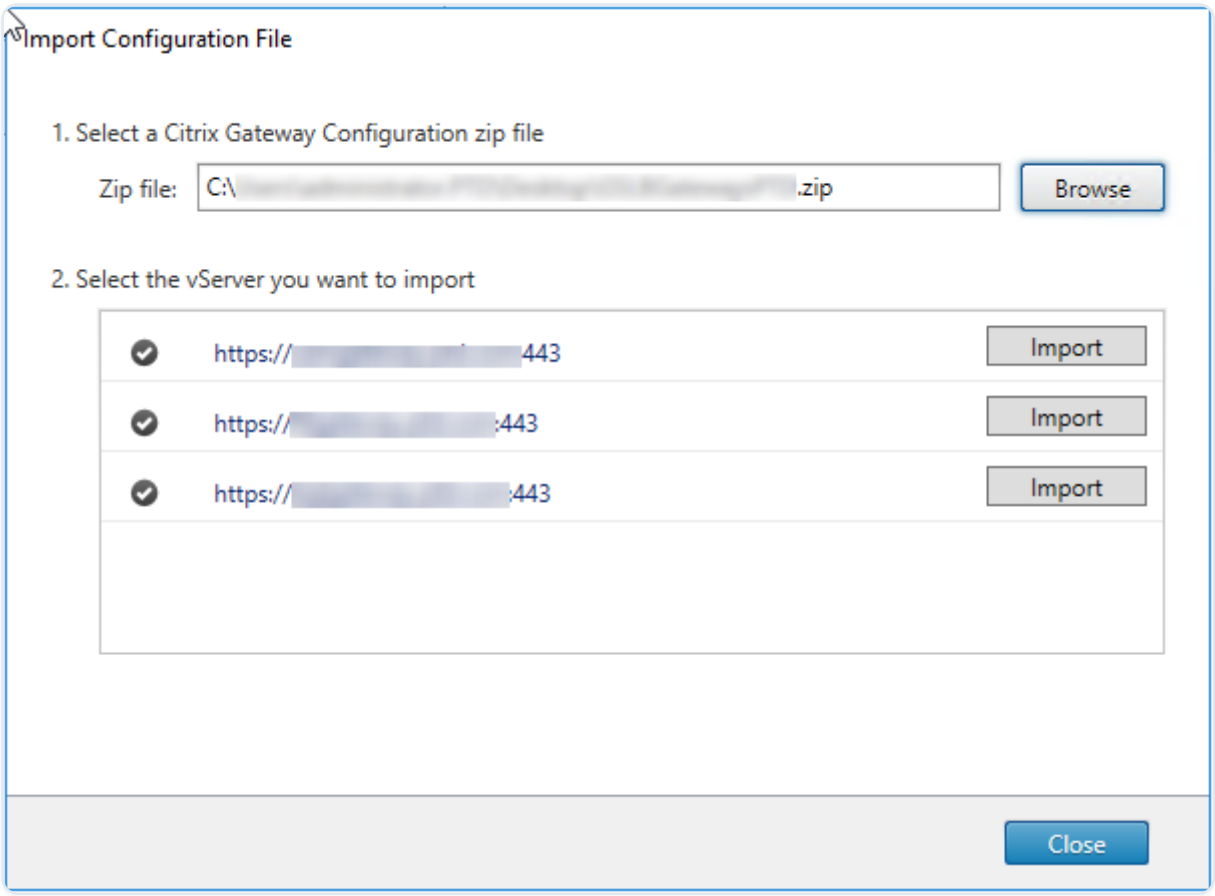
> Wichtig:

> Citrix unterstützt die manuelle Bearbeitung der aus Citrix Gateway exportierten Konfigurationsdatei nicht.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus, und klicken Sie im Bereich **Aktionen** auf **Citrix Gateways verwalten**.
2. Klicken Sie auf dem Bildschirm „Citrix Gateways verwalten“ auf den Link **aus Datei importiert**.

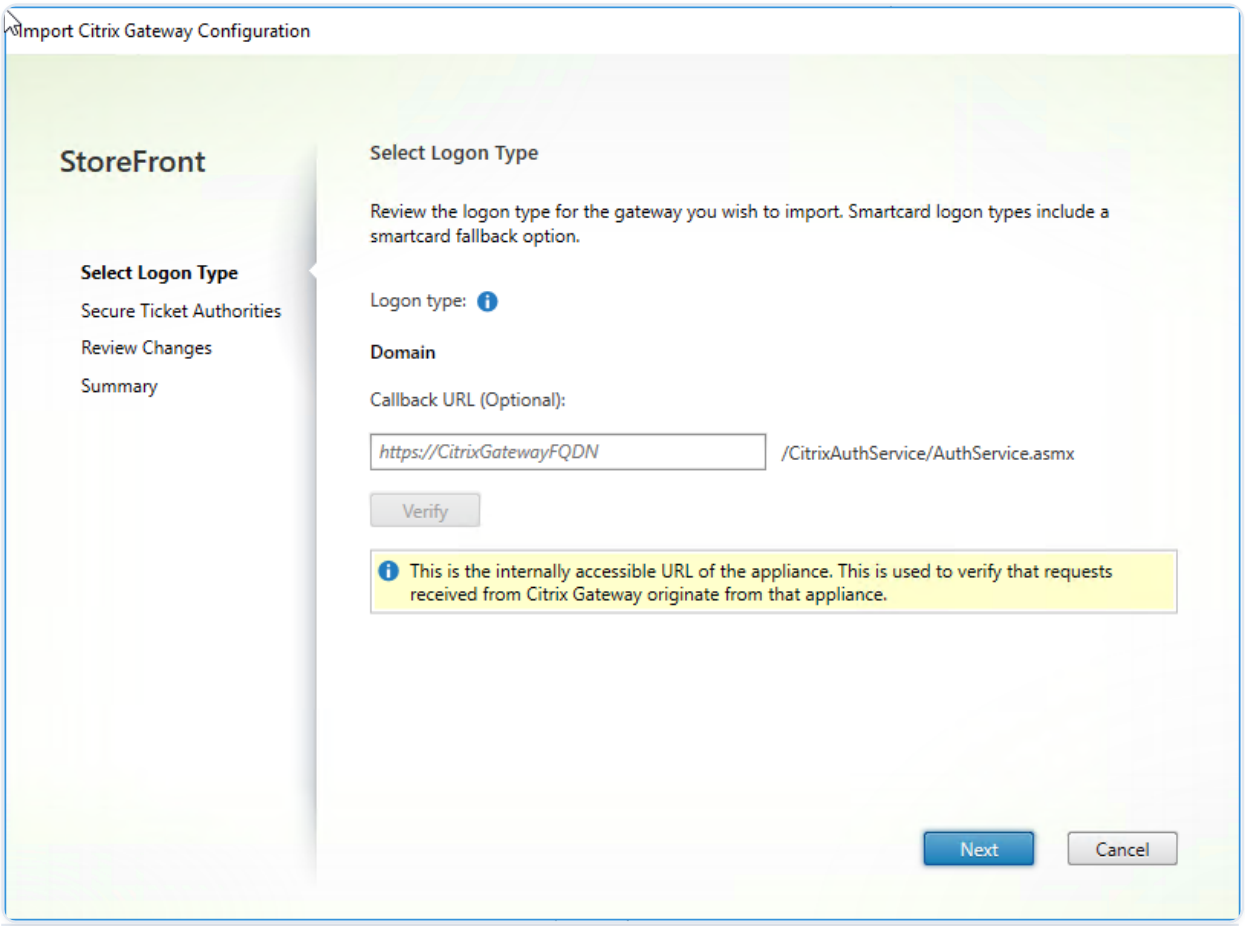


3. Navigieren Sie zur Konfigurationsdatei des virtuellen Citrix Gateway-Servers.
4. Eine Liste der Gateway-vServer aus der ausgewählten ZIP-Datei wird angezeigt. Wählen Sie den Gateway-vServer aus, den Sie importieren möchten, und klicken Sie auf **Importieren**. Wenn Sie einen vServer-Import wiederholen, wird die Schaltfläche „Importieren“ als „Aktualisieren“ angezeigt. Wenn Sie **Aktualisieren** wählen, haben Sie später die Möglichkeit, ein vorhandenes Gateway zu überschreiben oder ein neues zu erstellen.



5. Überprüfen Sie den **Anmeldetyp** für das ausgewählte Gateway und geben Sie bei Bedarf eine **Callback-URL** an. Der Anmeldetyp ist die Authentifizierungsmethode, die Sie auf dem Citrix Gateway für Benutzer der Citrix Workspace-App konfiguriert haben. Einige Anmeldetypen erfordern Callback-URLs (siehe Tabelle).

    - Klicken Sie auf **Überprüfen**, um zu prüfen, ob die Callback-URL gültig und vom StoreFront-Server aus erreichbar ist.



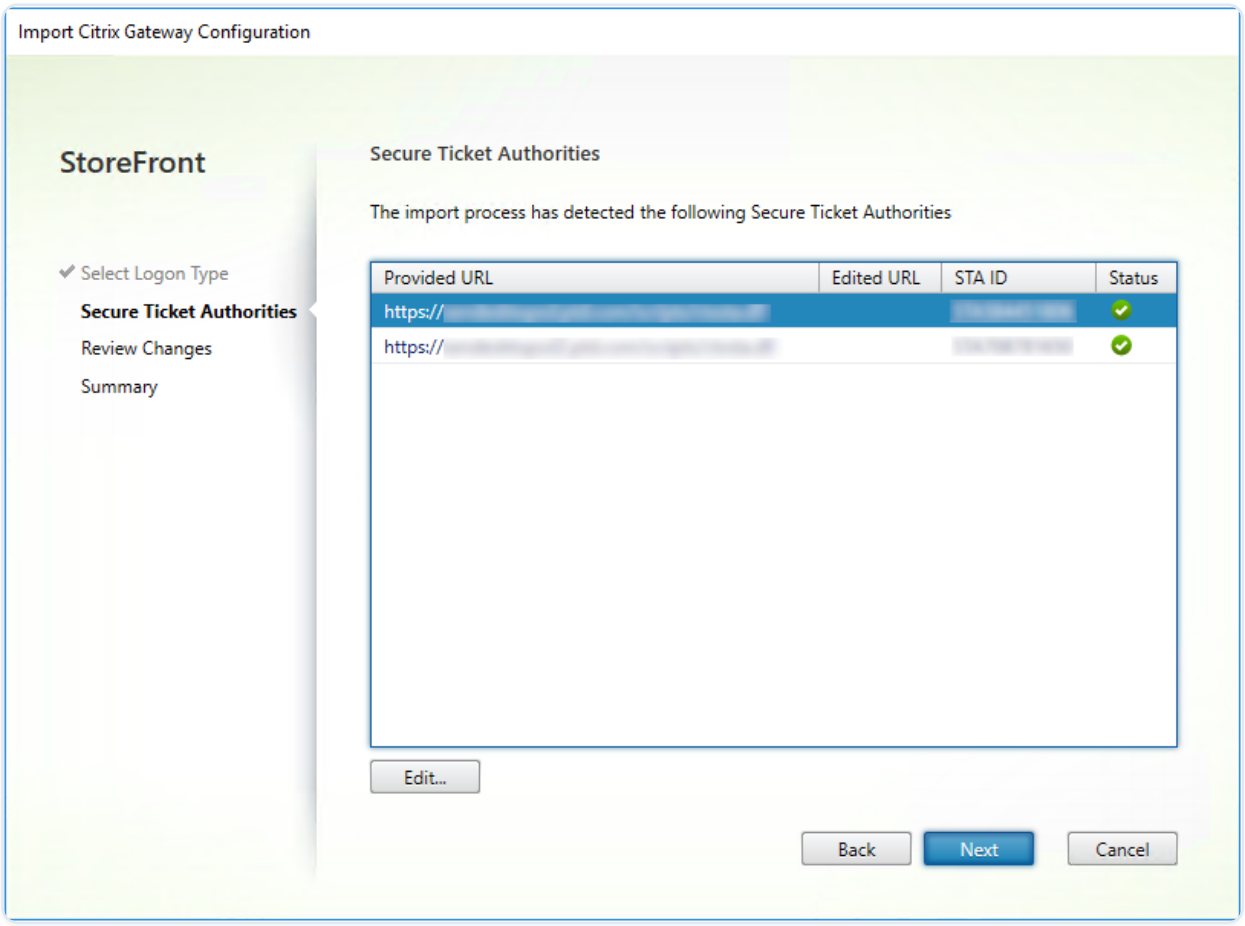
ANMELDETYP IN DER KONSOLE	LOGONTYPE IN JSON-DATEI	CALLBACK-URL ERFORDERLICH
Domäne	Domäne	Nein
Domäne und Sicherheitstoken	DomainAndRSA	Nein
Sicherheitstoken	RSA	Ja
Smartcard – kein Fallback	SmartCard	Ja
Smartcard – Domäne	SmartCardDomain	Ja
Smartcard – Domäne und Sicherheitstoken	SmartCardDomainAndRSA	Ja
Smartcard – Sicherheitstoken	SmartCardRSA	Ja
Smartcard – SMS-Authentifizierung	SmartCardSMS	Ja

ANMELDETYP IN DER KONSOLE	LOGONTYPE IN JSON-DATEI	CALLBACK-URL ERFORDERLICH
SMS-Authentifizierung	SMS	Ja

Wenn eine Callback-URL erforderlich ist, füllt StoreFront die Callback-URL automatisch basierend auf der im ZIP-Archiv gefundenen Gateway-URL aus. Sie können dies in eine beliebige gültige URL ändern, die auf die richtige Citrix Gateway VIP zurückverweist. Für GSLB-Gateways sind eindeutige Callback-URLs für jedes der von Ihnen importierten Gateways erforderlich.

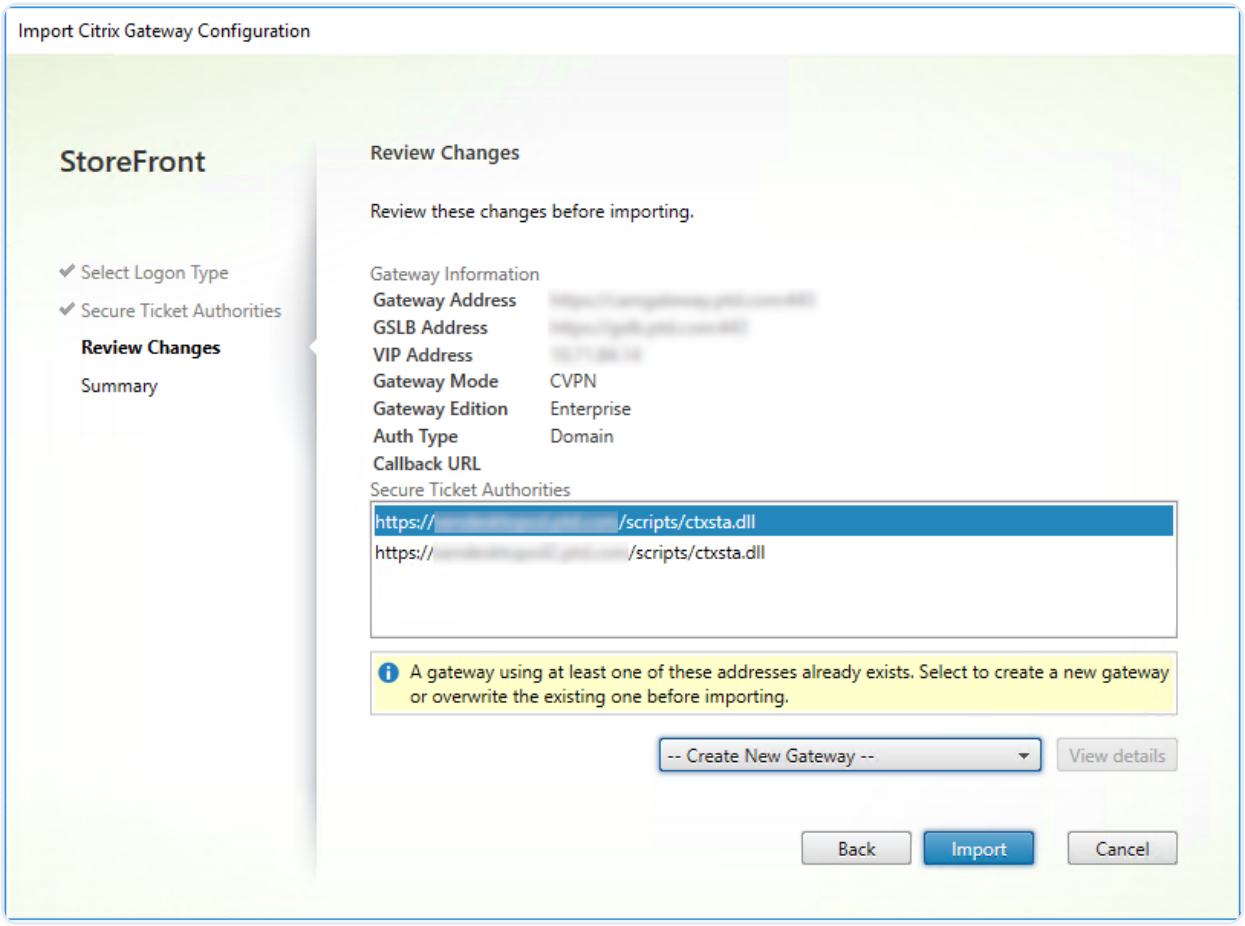
Um Smart Access oder die passwortlose Authentifizierung zu verwenden, ist eine Callback-URL erforderlich.

6. Klicken Sie auf **Weiter**.
7. StoreFront kontaktiert alle in der ZIP-Datei aufgeführten STA-Server-URLs (Secure Ticket Authorities) über DNS und überprüft, ob es sich um funktionale STA-Ticketing-Server handelt. Der Import wird nicht fortgesetzt, wenn eine oder mehrere der STA-URLs ungültig sind.



8. Klicken Sie auf **Weiter**.

9. Überprüfen Sie die Details des Imports. Wenn ein Gateway mit derselben Gateway-URL- und Port-Kombination (GatewayURL:Port) bereits existiert, verwenden Sie das Dropdown-Menü, um ein Gateway zum Überschreiben auszuwählen oder ein neues Gateway zu erstellen.



StoreFront verwendet die GatewayURL:Port-Kombination, um festzustellen, ob ein Gateway, das Sie importieren möchten, mit einem vorhandenen Gateway übereinstimmt, das Sie möglicherweise aktualisieren möchten. Wenn ein Gateway eine andere GatewayURL:Port-Kombination hat, behandelt StoreFront es als neues Gateway. Diese Tabelle der Gateway-Einstellungen zeigt, welche Einstellungen Sie aktualisieren können.

GATEWAY-EINSTELLUNG	KANN AKTUALISIERT WERDEN
Gateway-URL:Port-Kombination	Nein
GSLB-URL	Ja
Netscaler® Vertrauenszertifikat & Fingerabdruck	Ja
Callback-URL	Ja

GATEWAY-EINSTELLUNG	KANN AKTUALISIERT WERDEN
Receiver für Web-Site-URL	Ja
Gateway-Adresse/VIP	Ja
STA-URL und STA-ID	Ja
Alle Anmeldetypen	Ja

10. Klicken Sie auf **Importieren**. Wenn der StoreFront-Server Teil einer Servergruppe ist, wird eine Meldung angezeigt, die Sie daran erinnert, die importierten Gateway-Einstellungen auf die anderen Server in der Gruppe zu übertragen.
11. Klicken Sie auf **Fertig stellen**.

Um eine weitere vServer-Konfiguration zu importieren, wiederholen Sie die obigen Schritte.

> **Hinweis:**

> Das Standard-Gateway für einen Store ist das Gateway, über das Citrix Workspace™-Apps versuchen, eine Verbindung herzustellen, es sei denn, sie sind für die Verwendung eines anderen Gateways konfiguriert. Wenn keine Gateways für den Store konfiguriert sind, wird das erste aus der ZIP-Datei importierte Gateway zum Standard-Gateway, das von Citrix Workspace-Apps verwendet wird. Das Importieren nachfolgender Gateways ändert das bereits für den Store festgelegte Standard-Gateway nicht.

Mehrere Citrix Gateways mit PowerShell importieren

Read-STFNetScalerConfiguration

- Kopieren Sie die ZIP-Datei auf den Desktop des aktuell angemeldeten StoreFront-Administrators.
- Lesen Sie den Inhalt der ZIP-Datei der virtuellen Serverkonfiguration des Citrix Gateways in den Speicher ein und betrachten Sie die drei darin enthaltenen Gateways anhand ihrer Indexwerte.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Zeigen Sie die drei Gateway-Objekte im Speicher an, die aus dem Netscaler ZIP-Importpaket mit dem Cmdlet **Read-STFNetScalerConfiguration** eingelesen wurden.

```
$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/

Address                 : https://emeagateway.example.com:445

GslbAddress             : https://gslb.example.com:443

VipAddress              : 10.0.0.2

Stas                    : {STA298854503, STA909374257}
```

```
StaLoadBalance          : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType         :SmartCard

GatewayEdition          : Enterprise

ReceiverForWebSites     :
{Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite
}
```

Import-STFNetScalerConfiguration ohne Angabe einer CallbackURL

Kopieren Sie die ZIP-Datei auf den Desktop des aktuell angemeldeten StoreFront-Administrators. Lesen Sie das Citrix Gateway Konfigurations-ZIP-Importpaket in den Speicher ein und betrachten Sie die drei darin enthaltenen Gateways anhand ihrer Indexwerte.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet **Import-STFNetScalerConfiguration** und geben Sie die benötigten Gateway-Indizes an. Die Verwendung des Parameters **-Confirm:$False** verhindert, dass die PowerShell-GUI Sie auffordert, jedes Gateway zu importieren. Entfernen Sie diesen Parameter, wenn Sie jedes Gateway einzeln und sorgfältig importieren möchten.

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 0 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 1 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 2 -Confirm:$False
```

Import-STFNetScalerConfiguration mit Angabe einer eigenen CallbackURL

Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet **Import-STFNetScalerConfiguration** und geben Sie eine Callback-URL Ihrer Wahl mit dem Parameter -callbackURL 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
```

Import-STFNetScalerConfiguration überschreibt die in der Importdatei gespeicherte Authentifizierungsmethode und gibt eine eigene CallbackURL an

Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet **Import-STFNetScalerConfiguration** und geben Sie eine Callback-URL Ihrer Wahl mit dem Parameter -callbackURL 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
```

Lastenausgleich mit NetScaler® ADC

Dieser Artikel enthält Anleitungen zur Bereitstellung einer StoreFront-Servergruppe, die zwei oder mehr StoreFront-Server in einer vollständig aktiven, lastenausgeglichenen Konfiguration enthält. Der Artikel enthält Details zur Konfiguration einer NetScaler ADC-Appliance zum Lastenausgleich eingehender Anforderungen von der Citrix Workspace-App und Webbrowsern zwischen StoreFront-Servern in der Servergruppe.

Erstellen Sie DNS-Einträge für den Lastenausgleich der StoreFront-Servergruppe

Erstellen Sie einen DNS-A- und PTR-Eintrag für Ihren ausgewählten gemeinsamen FQDN. Clients in Ihrem Netzwerk verwenden diesen FQDN für den Zugriff auf die StoreFront-Servergruppe über den NetScaler ADC-Appliance-Lastenausgleich.

Beispiel: `storefront.example.com` wird zur virtuellen IP (VIP) des virtuellen Lastenausgleichsservers aufgelöst.

Konfigurieren Sie StoreFront-Server

Alle StoreFront-Server, zwischen denen Sie einen Lastenausgleich durchführen möchten, sollten als Teil einer StoreFront-Servergruppe konfiguriert werden, die die Konfiguration zwischen den Servern synchronisiert, um sicherzustellen, dass sie identisch konfiguriert sind. Weitere Informationen zum Hinzufügen von Servern zu einer Servergruppe finden Sie unter Einer vorhandenen Servergruppe beitreten.

Jeder Server sollte für HTTPS konfiguriert werden, damit die Kommunikation zwischen dem Lastenausgleich und den StoreFront-Servern verschlüsselt ist. Siehe StoreFront mit HTTPS sichern. Das Zertifikat muss den lastenausgeglichenen FQDN als Common Name (CN) oder als Subject Alternative Name (SAN) enthalten.

Legen Sie die Basis-URL der Servergruppe als URL des Lastenausgleichs fest. Um die Basis-URL zu ändern, klicken Sie in der Citrix StoreFront-Verwaltungskonsole im linken Bereich mit der rechten Maustaste auf **Servergruppe** und dann auf **Basis-URL ändern**. Geben Sie die URL des virtuellen Servers des Lastenausgleichs ein.

Optional Citrix Service Monitor für HTTPS konfigurieren

Eine StoreFront-Installation umfasst den Windows-Dienst **Citrix Service Monitor**. Dieser Dienst hat keine weiteren Dienstabhängigkeiten und überwacht den Zustand kritischer StoreFront-Dienste. Dies ermöglicht dem NetScaler ADC und anderen Drittanbieteranwendungen, den relativen Zustand einer StoreFront-Serverbereitstellung zu überwachen.

Standardmäßig verwendet der Monitor HTTP auf Port 8000. Sie können dies optional ändern, um HTTPS auf Port 443 zu verwenden.

1. Öffnen Sie die PowerShell Integrated Scripting Environment (ISE) auf dem primären StoreFront-Server und führen Sie die folgenden Befehle aus, um den Standardmonitor auf HTTPS 443 zu ändern:

   ```
   $ServiceUrl = "https://localhost:443/StorefrontMonitor"

   Set-STFServiceMonitor -ServiceUrl $ServiceUrl

   Get-STFServiceMonitor
   ```

2. Nach Abschluss übertragen Sie die Änderungen auf alle anderen Server in der StoreFront-Servergruppe.
3. Um einen schnellen Test des Monitors durchzuführen, geben Sie die folgende URL in den Browser auf dem StoreFront-Server oder einem anderen Computer mit Netzwerkzugriff auf den StoreFront-Server ein. Der Browser gibt eine XML-Zusammenfassung des Status jedes StoreFront-Dienstes zurück.

   `https://<loadbalancingFQDN>/StoreFrontMonitor/GetSFServicesStatus`

```
<ArrayOfServiceStatus xmlns="http://schemas.datacontract.org/2004/07/
Citrix.DeliveryServices.ServiceMonitor.Contract" xmlns:i="http://
www.w3.org/2001/XMLSchema-instance">

<ServiceStatus>

    <name>Citrix Peer Resolution Service</name>

    <status>running</status>

</ServiceStatus>

<ServiceStatus>

    <name>CitrixConfigurationReplication</name>

    <status>running</status>

</ServiceStatus>

<ServiceStatus>

    <name>CitrixCredentialWallet</name>

    <status>running</status>

</ServiceStatus>

<ServiceStatus>

    <name>CitrixDefaultDomainService</name>

    <status>running</status>

</ServiceStatus>

<ServiceStatus>

    <name>CitrixSubscriptionsStore</name>

    <status>running</status>

</ServiceStatus>
```

```
<ServiceStatus>
    <name>NetTcpPortSharing</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>WAS</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>W3SVC</name>
    <status>running</status>
</ServiceStatus>
</ArrayOfServiceStatus>
```

NetScaler Load Balancer konfigurieren

Stammzertifikat installieren

Wenn Ihre StoreFront-Server ein von einer internen Zertifizierungsstelle signiertes Zertifikat verwenden, müssen Sie das Stammzertifikat auf dem NetScaler installieren. Dies ist erforderlich, damit NetScaler dem Zertifikat des StoreFront-Servers vertraut.

1. Melden Sie sich bei der Verwaltungs-GUI der NetScaler ADC Appliance an.
2. Wählen Sie **Traffic Management** > **SSL** > **Certificates** > **CA Certificates**.
3. Klicken Sie auf **Installieren**.
4. Geben Sie auf der Seite **Install CA Certificate** einen Zertifikat-Schlüsselpaar-Namen ein, klicken Sie auf **Choose File** und suchen Sie nach der Zertifikatdatei.
5. Klicken Sie auf **Installieren**.

Serverzertifikat installieren

Um HTTPS zu aktivieren, benötigen Sie ein Zertifikat, dessen alternativer Antragstellernamen den FQDN des Load Balancers enthält. Sie können das Zertifikat mit einer Unternehmens- oder öffentlichen Zertifizierungsstelle signieren.

Sie müssen separate Zertifikats- und Schlüsseldateien im PEM-Format haben. Wenn Sie ein Zertifikat mit dem privaten Schlüssel im PKCS12-Format haben, können Sie `openssl` verwenden, um die Datei zu konvertieren. Z.B.:

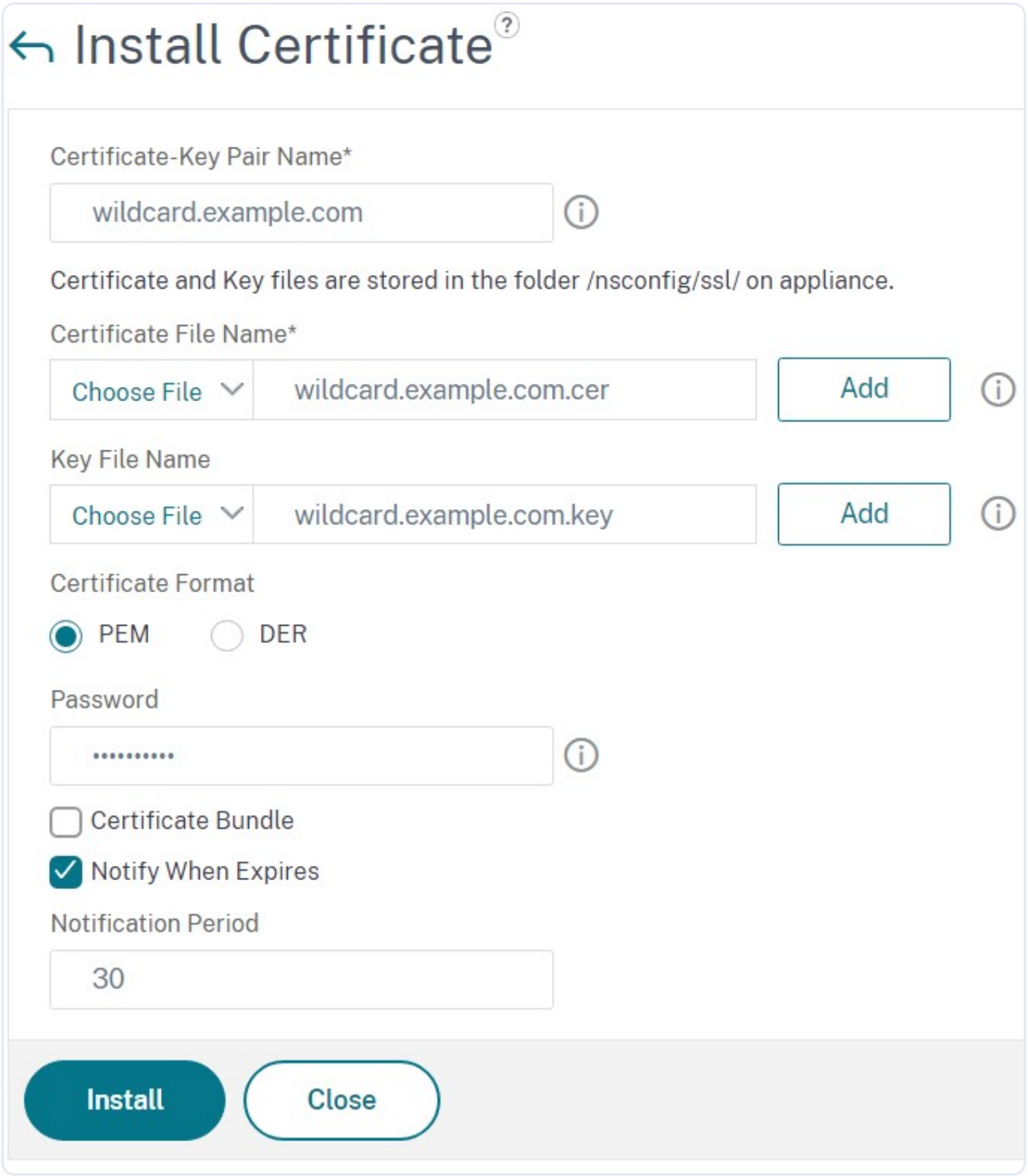
```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out cert.cer

openssl pkcs12 -in cert.pfx -nocerts -out storefrontlbeu.key
```

Eine Aufforderung zur Eingabe des vorhandenen Kennworts und einer neuen PEM-Passphrase wird angezeigt.

So installieren Sie das Zertifikat:

1. Melden Sie sich bei der Verwaltungs-GUI der NetScaler ADC Appliance an.
2. Wählen Sie **Traffic Management** > **SSL** > **Certificates** > **CA Certificates**.
3. Klicken Sie auf **Installieren**.
4. Auf der Seite **Install CA Certificate**:
    a. Geben Sie einen **Certificate-Key Pair Name** ein.
    b. Klicken Sie unter **Zertifikatdateiname** auf **Datei auswählen** und suchen Sie nach der Zertifikatdatei.
    c. Klicken Sie unter **Schlüsseldateiname** auf **Datei auswählen** und suchen Sie nach der Schlüsseldatei.
    d. Geben Sie unter **Kennwort** die Passphrase ein.
    e. Klicken Sie auf **Installieren**.
5. Klicken Sie auf **Verknüpfen**, um das Zertifikat mit dem Stammzertifikat zu verknüpfen.

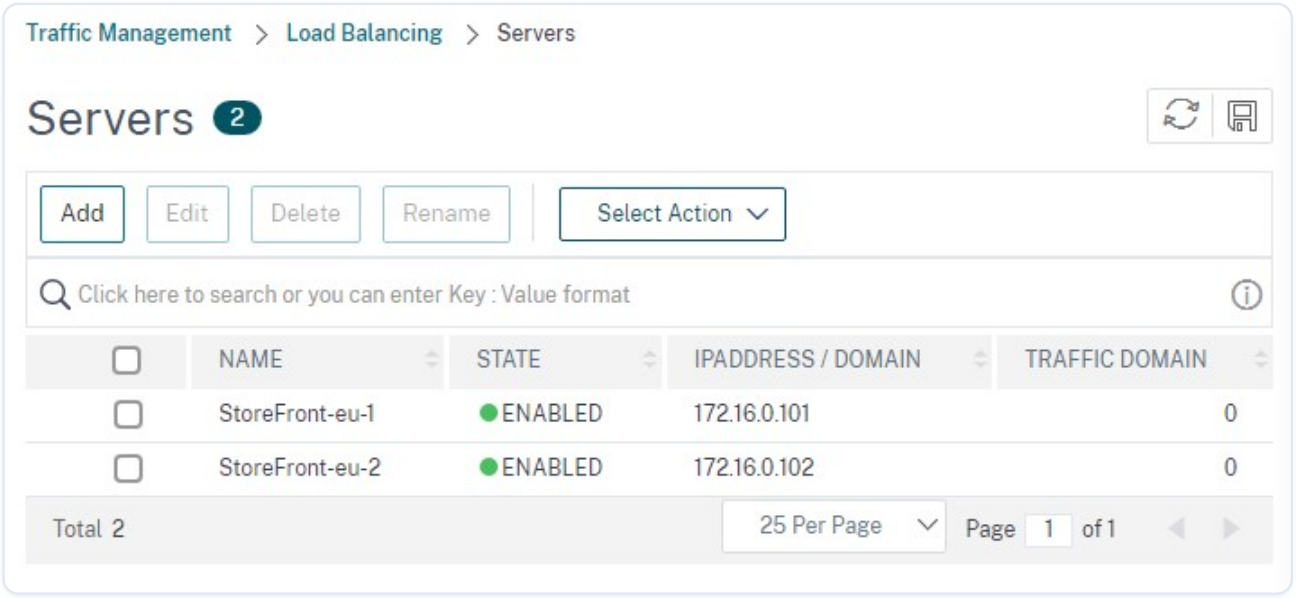


Hinzufügen einzelner StoreFront-Serverknoten zum NetScaler ADC Appliance Load Balancer

1. Navigieren Sie zu **Traffic Management > Load Balancing > Servers**. Klicken Sie auf **Hinzufügen** und fügen Sie jeden der StoreFront-Server hinzu, die per Lastenausgleich verteilt werden sollen.

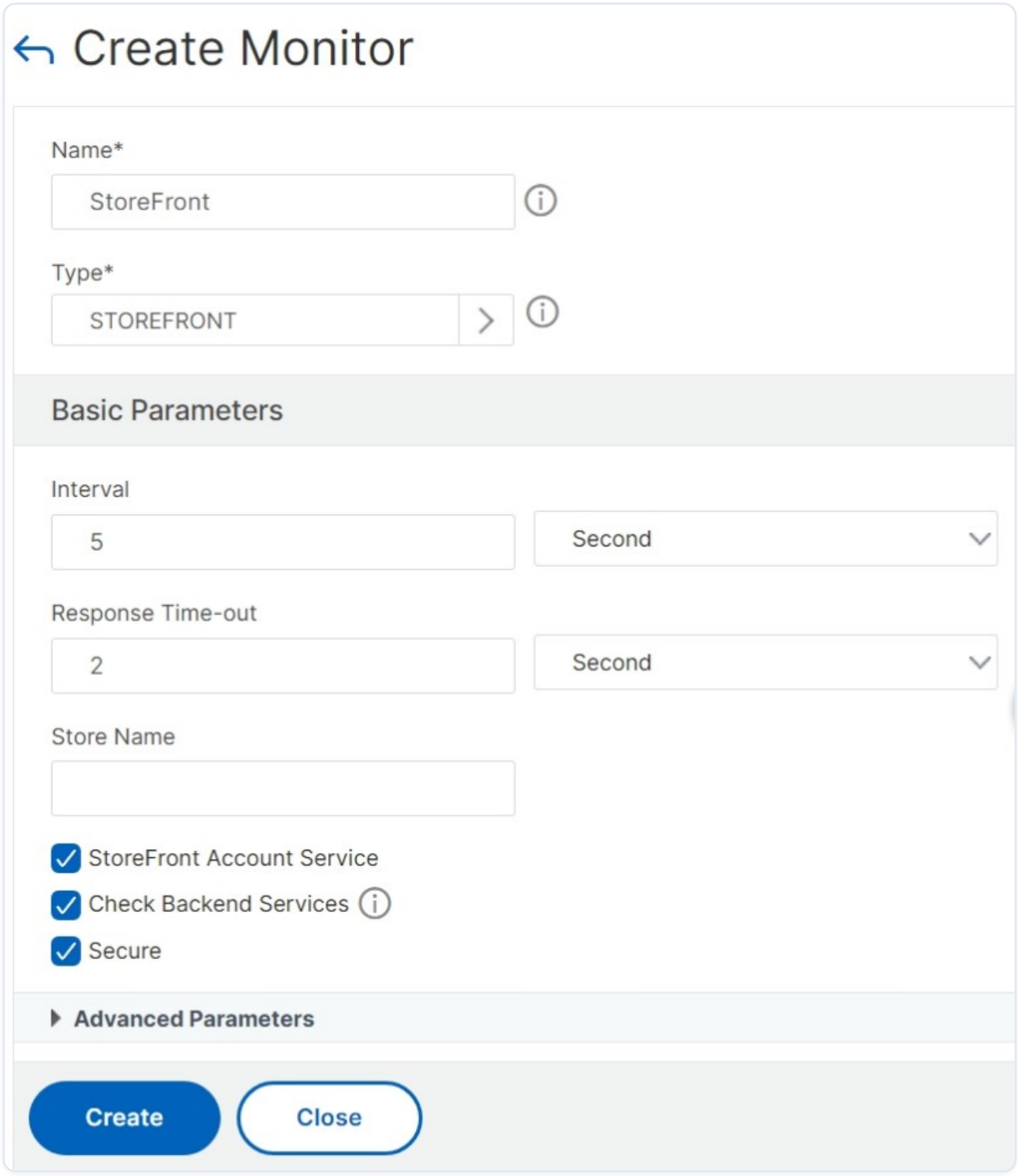
   Beispiel = 2 StoreFront-Server mit den Namen StoreFront-eu-1 und StoreFront-eu-2

2. Verwenden Sie die IP-basierte Serverkonfiguration und geben Sie die Server-IP-Adresse für jeden StoreFront-Knoten ein.



Definieren Sie einen StoreFront-Monitor, um den Status aller StoreFront-Knoten in der Servergruppe zu überprüfen

1. Melden Sie sich bei der NetScaler ADC-Verwaltungs-GUI an.
2. Wählen Sie **Traffic Management > Load Balancing > Monitors > Add** und fügen Sie einen neuen Monitor namens *StoreFront* hinzu und übernehmen Sie alle Standardeinstellungen.
3. Wählen Sie im Dropdown-Menü **Typ** die Option **StoreFront** aus.
4. Wenn Sie Ihren StoreFront-Monitor für HTTPS konfiguriert haben, stellen Sie sicher, dass die Option **Sicher** ausgewählt ist. Andernfalls lassen Sie diese Option deaktiviert und geben Sie Port 8000 ein.
5. Wählen Sie die Option **Backend-Dienste prüfen** aus. Diese Option ermöglicht die Überwachung von Diensten, die auf dem StoreFront-Server ausgeführt werden. StoreFront-Dienste werden überwacht, indem ein Windows-Dienst auf dem StoreFront-Server abgefragt wird, der den Status der folgenden Dienste zurückgibt:
   - W3SVC (IIS)
   - WAS (Windows Process Activation Service)
   - CitrixCredentialWallet
   - CitrixDefaultDomainService



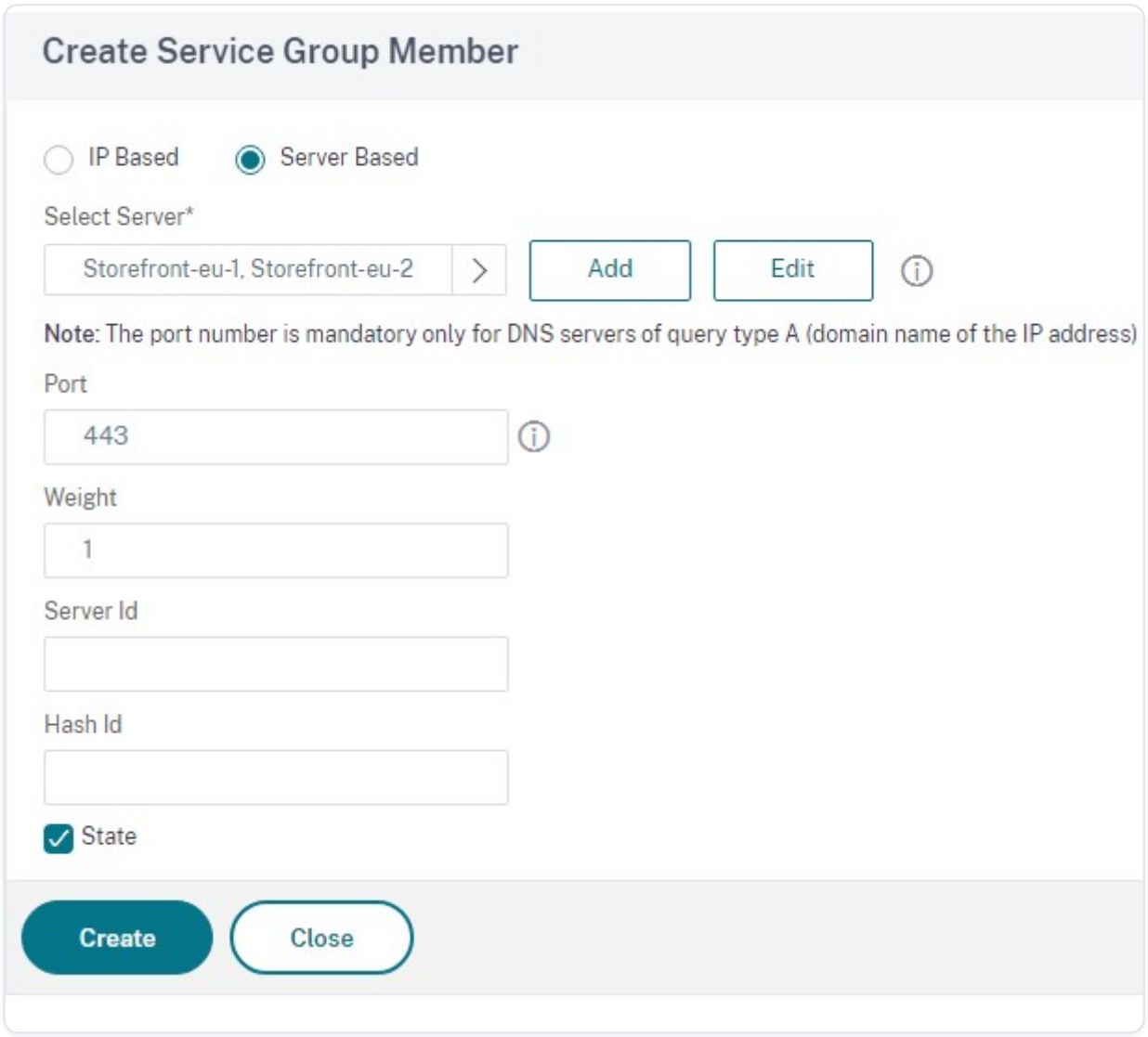
Eine Dienstgruppe erstellen, die alle StoreFront-Server enthält

1. Navigieren Sie zu **Traffic Management > Lastenausgleich > Dienstgruppen**. Klicken Sie auf **Hinzufügen**. Um über HTTPS eine Verbindung zu den StoreFront-Servern herzustellen, wählen Sie das Protokoll SSL aus. Belassen Sie andere Einstellungen als Standard. Klicken Sie auf **OK**.
2. Innerhalb Ihrer Dienstgruppe klicken Sie unter **Dienstgruppenmitglieder** auf **Kein Dienstgruppenmitglied**.

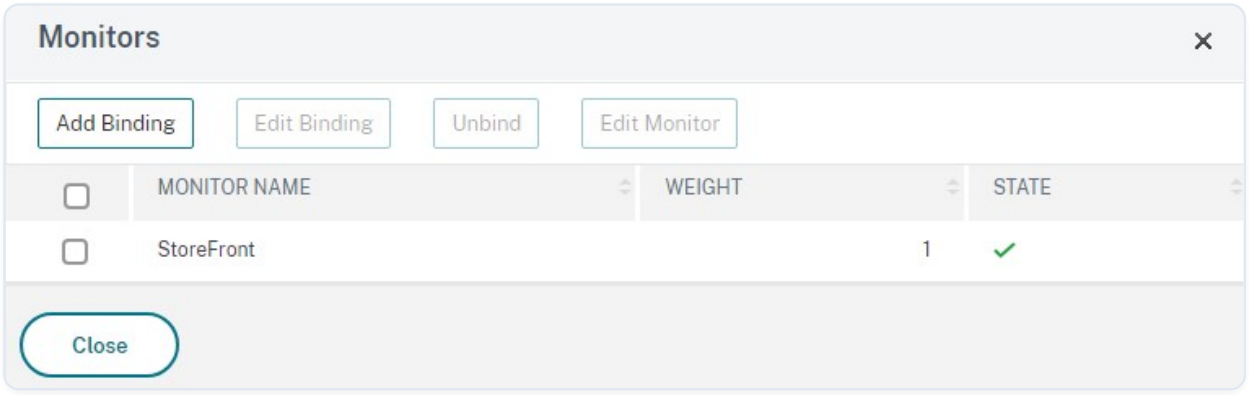
a. Klicken Sie auf **Dienstbasiert**.

b. Wählen Sie alle Server aus, die Sie zuvor definiert haben.

c. Um SSL zwischen dem Lastenausgleich und dem StoreFront-Server zu verwenden, geben Sie Port 443 ein. Andernfalls geben Sie Port 80 ein.



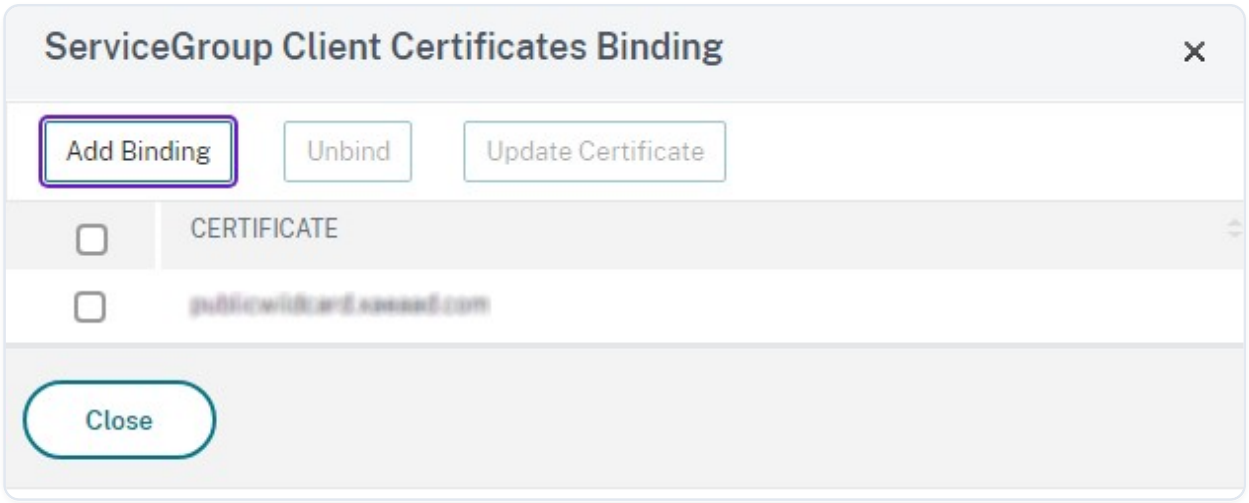
3. Fügen Sie den Abschnitt **Monitore** hinzu und wählen Sie den zuvor erstellten StoreFront-Monitor aus.



4. Fügen Sie den Abschnitt **Zertifikate** hinzu.

   a. Binden Sie das Clientzertifikat.

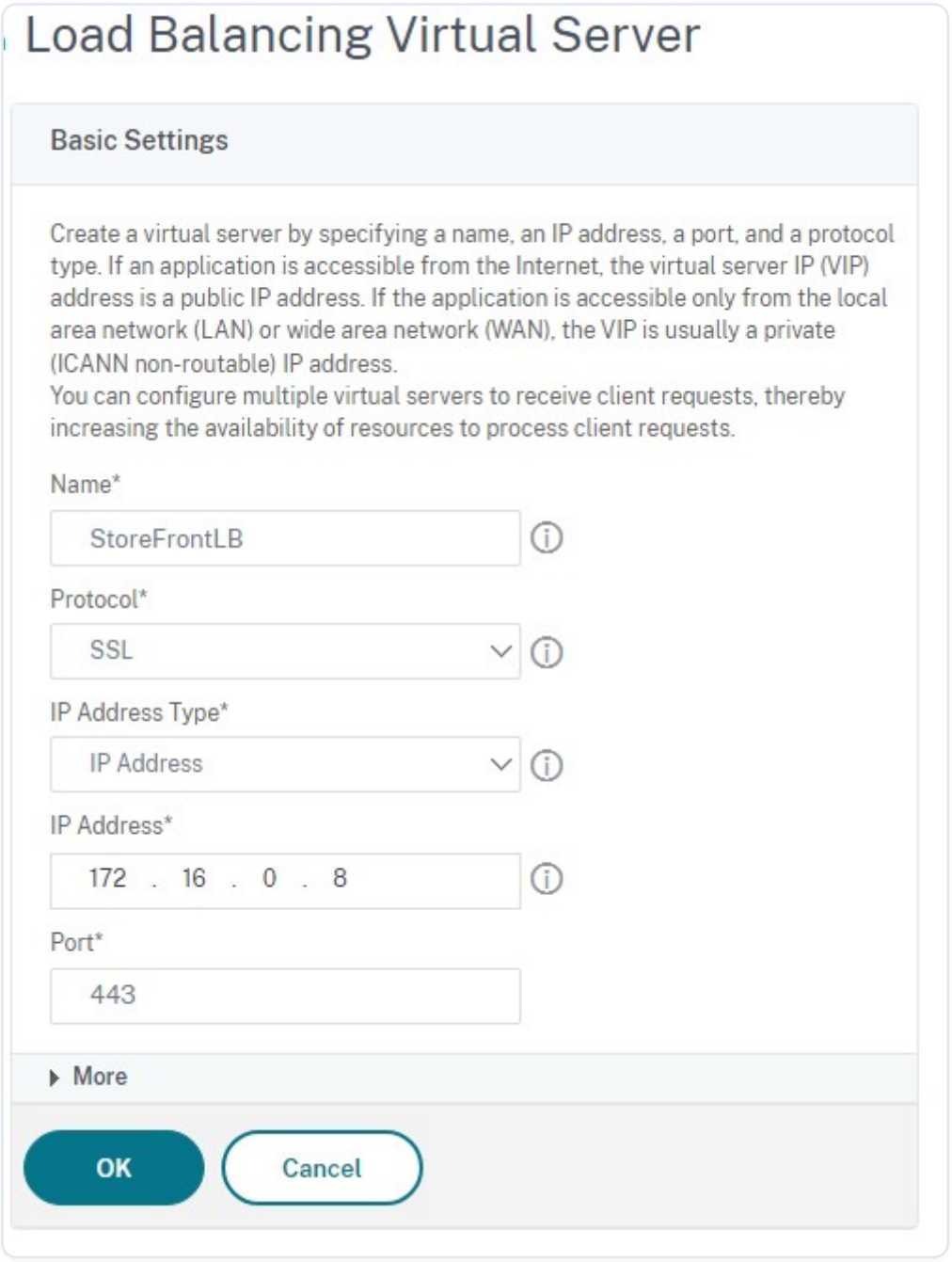
   b. Binden Sie das CA-Zertifikat, das zum Signieren des zuvor importierten Serverzertifikats verwendet wurde, und alle anderen CAs, die Teil der PKI-Vertrauenskette sein könnten.



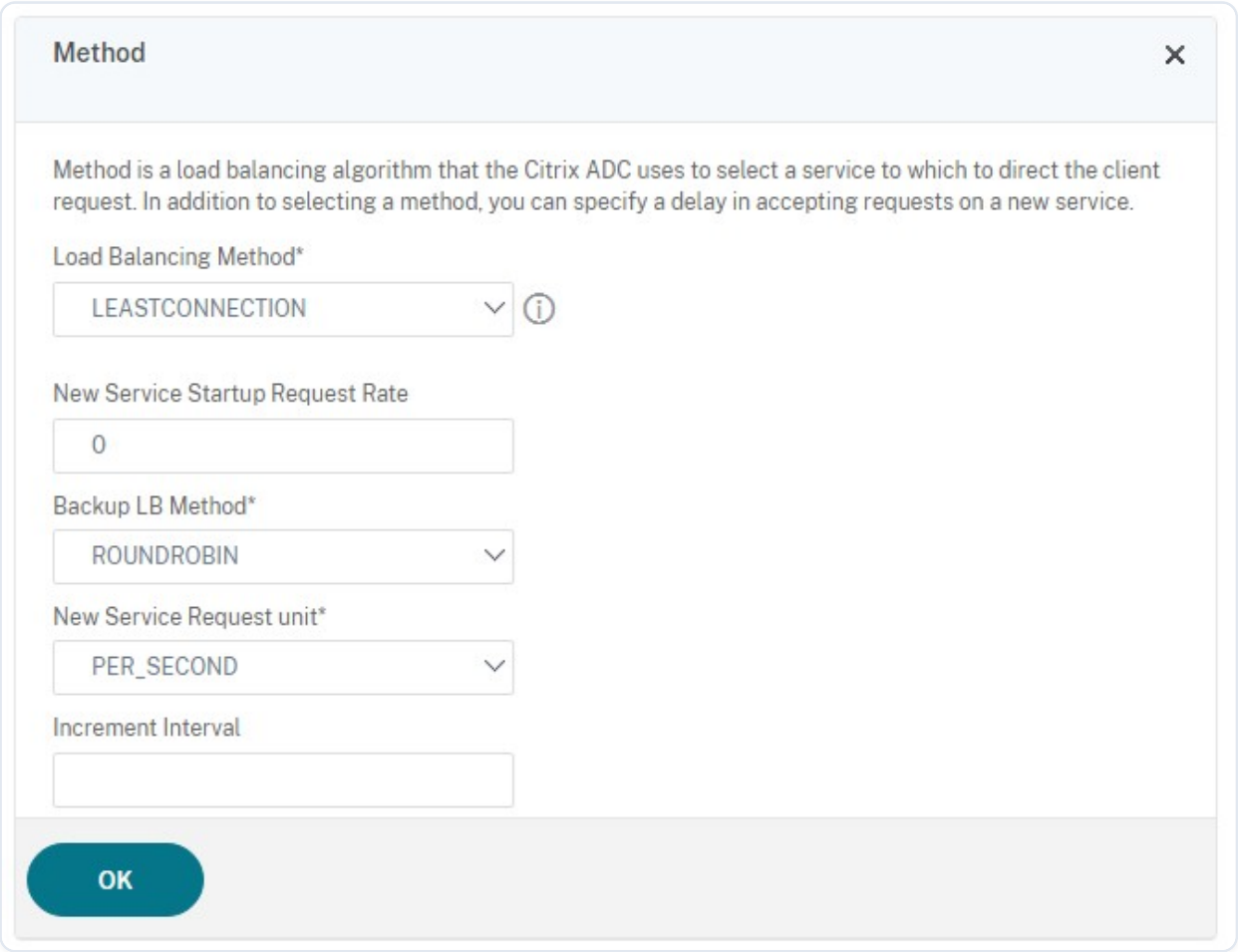
5. Fügen Sie den Abschnitt **Einstellungen** hinzu. Wählen Sie **Client-IP-Header einfügen** und geben Sie als Headernamen **X-Forwarded-For** ein. Dadurch kann die Client-IP-Adresse in Citrix Virtual Apps and Desktops-Richtlinien verwendet werden.

Erstellen eines virtuellen Lastausgleichsservers für den Benutzerdatenverkehr

1. Melden Sie sich bei der Verwaltungs-GUI der NetScaler ADC Appliance an.
2. Wählen Sie **Traffic Management > Load Balancing > Virtual Servers > Add**, um einen neuen virtuellen Server zu erstellen.
3. Geben Sie einen Namen ein, wählen Sie das Protokoll SSL und geben Sie den **Port** ein. Klicken Sie auf OK, um den virtuellen Server zu erstellen.



4. Binden Sie die zuvor erstellte **Dienstgruppe** an den virtuellen Lastausgleichsserver.
5. Binden Sie dasselbe Server- und CA-Zertifikat, das Sie zuvor an die Dienstgruppe gebunden haben.
6. Fügen Sie den Abschnitt **Methode** hinzu und wählen Sie die Lastausgleichsmethode. Gängige Optionen für den StoreFront-Lastausgleich sind **Round Robin** oder **Least Connection**.



7. Fügen Sie den Abschnitt **Persistenz** hinzu.

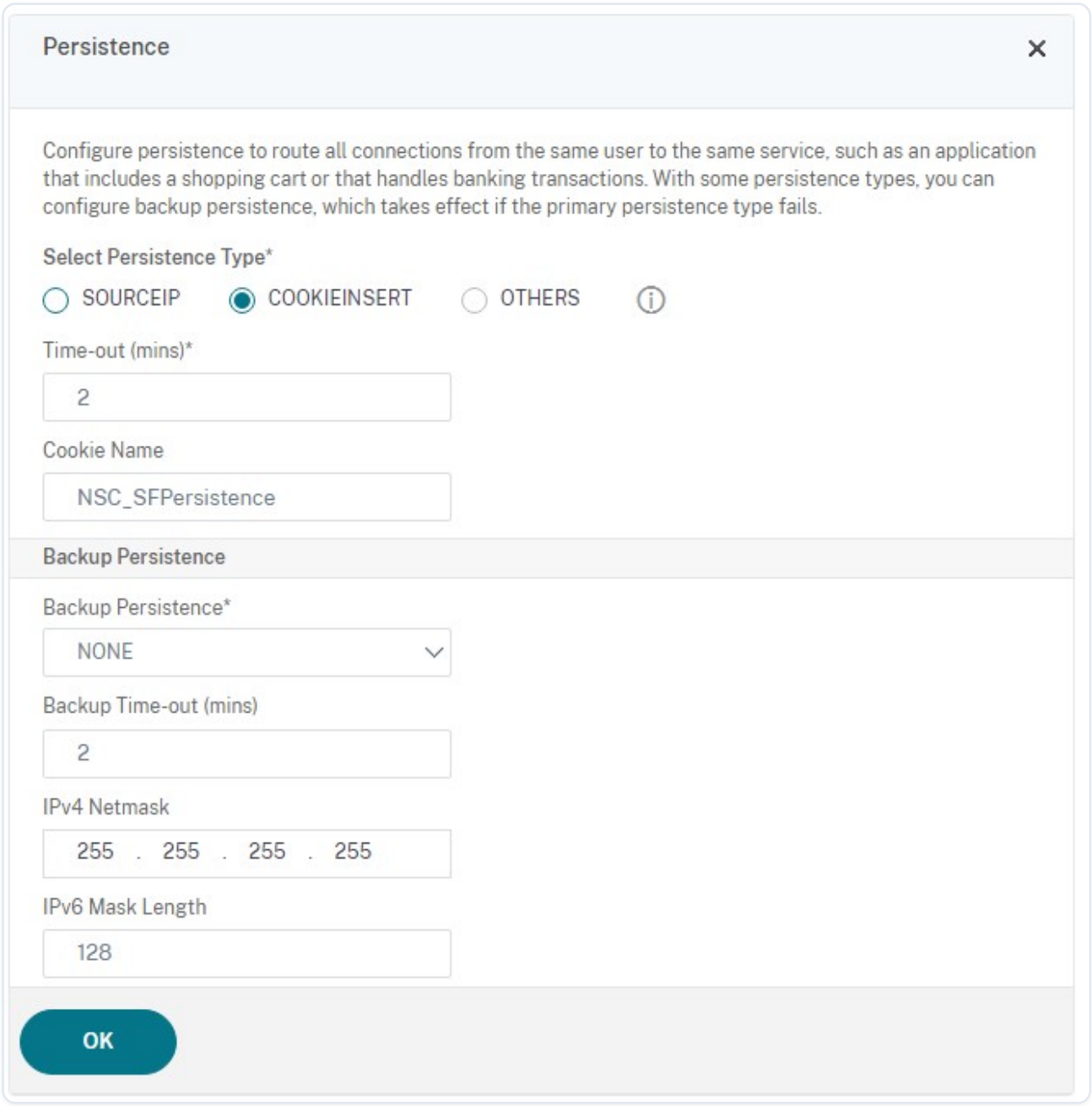
   a. Legen Sie die Persistenzmethode auf **COOKIEINSERT** fest.

   b. Legen Sie das Zeitlimit so fest, dass es dem Sitzungszeitlimit in StoreFront entspricht, das standardmäßig 20 Minuten beträgt.

   c. Benennen Sie das Cookie. Zum Beispiel **NSC_SFPersistence**, da dies die Identifizierung während des Debuggings erleichtert.

   d. Legen Sie die Backup-Persistenz auf **NONE** fest.

> **Hinweis:**
>
> Wenn der Client das HTTP-Cookie nicht speichern darf, enthalten die nachfolgenden Anfragen das HTTP-Cookie nicht, und die Persistenz wird nicht verwendet.



StoreFront-Loopback konfigurieren

Wenn die Basisadresse ein Lastenausgleichsdienst ist, könnte dies bei der internen Kommunikation zwischen StoreFront-Diensten dazu führen, dass der Datenverkehr an den Lastenausgleichsdienst und möglicherweise an einen anderen Server weitergeleitet wird. Dies führt zu schlechter Leistung und unerwartetem Verhalten. Verwenden Sie die StoreFront-Einstellung Loopback-Kommunikation aktivieren, um dies zu vermeiden. Standardmäßig ist diese auf **On** gesetzt, was bedeutet, dass der Host-Teil der Dienstadresse durch die Loopback-IP-Adresse 127.0.0.1 ersetzt wird, während das Schema (HTTP oder HTTPS) unverändert bleibt. Dies funktioniert für eine Einzelserver-Bereitstellung und Bereitstellungen mit einem nicht SSL-terminierenden Lastenausgleichsdienst. Wenn der Lastenausgleichsdienst SSL-terminierend ist und mit StoreFront über HTTP kommuniziert (nicht empfohlen), ist es notwendig, die StoreFront-

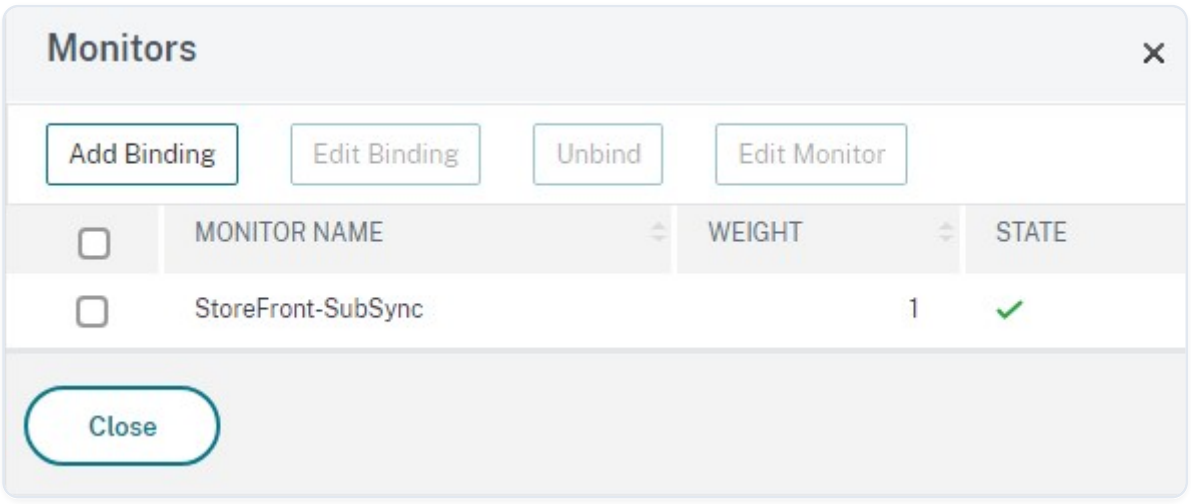
Loopback-Kommunikation auf **OnUsingHttp** zu konfigurieren, was bedeutet, dass StoreFront auch das Schema von HTTPS auf HTTP ändert.

NetScaler ADC-Lastenausgleichsdienst für die Abonnement-Synchronisierung zwischen Servergruppen konfigurieren

Wenn Sie eine Multisite-Bereitstellung mit zwei oder mehr StoreFront-Servergruppen haben, können Sie Abonnementdaten zwischen diesen mithilfe einer Pull-Strategie nach einem wiederkehrenden Zeitplan replizieren. Die StoreFront-Abonnementreplikation verwendet TCP-Port 808, daher schlägt die Verwendung eines vorhandenen virtuellen Lastenausgleichsservers auf HTTP-Port 80 oder HTTPS 443 fehl. Um eine hohe Verfügbarkeit für diesen Dienst zu gewährleisten, erstellen Sie einen zweiten virtuellen Server auf jeder NetScaler ADC-Appliance in Ihrer Bereitstellung, um den TCP-Port 808 für jede der StoreFront-Servergruppen auszugleichen.

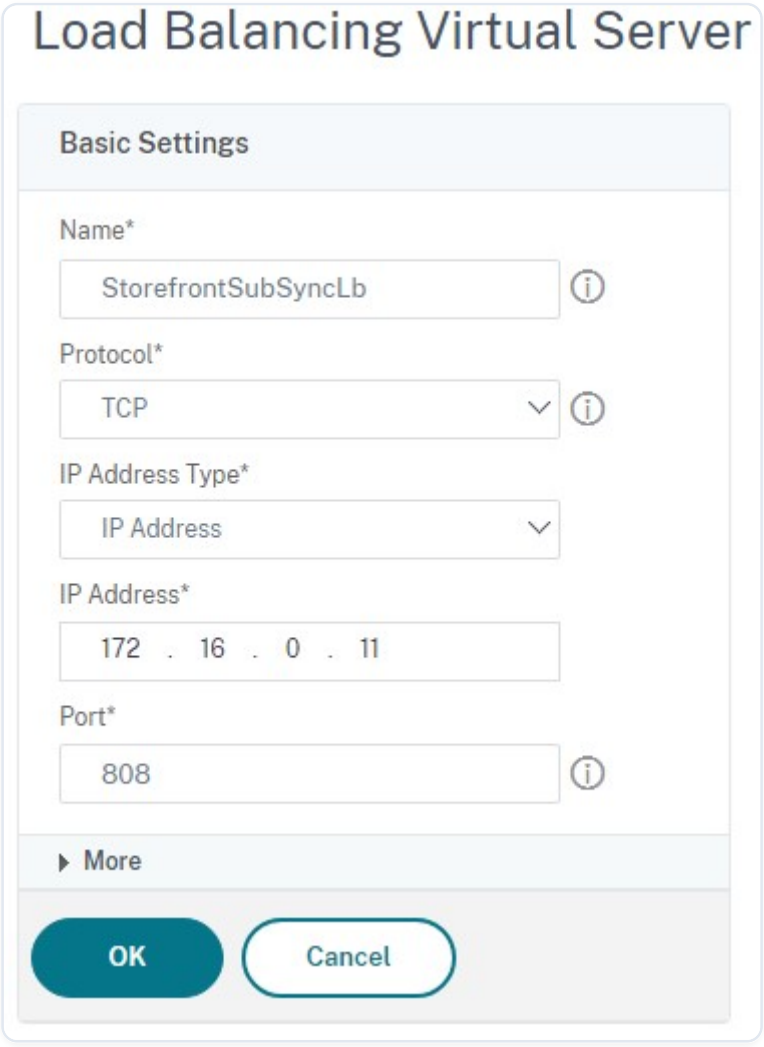
Dienstgruppe für die Abonnement-Synchronisierung konfigurieren

1. Melden Sie sich bei der Verwaltungs-GUI der NetScaler ADC-Appliance 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 auf **OK**, um zu speichern.
4. **Im Abschnitt Dienstgruppenmitglieder** fügen Sie alle StoreFront-Serverknoten hinzu, die Sie zuvor im Abschnitt Server definiert haben, und geben Sie **Port** als **808** an.
5. Fügen Sie den Abschnitt **Monitore** hinzu.
    a. Klicken Sie auf die Stelle, an der **No Service Group to monitor Binding** steht.
    b. Klicken Sie auf Hinzufügen. Geben Sie einen Monitor-**Namen** ein und legen Sie den **Typ** auf **TCP** fest. Klicken Sie auf **Erstellen**.
    c. Klicken Sie auf **Binden**.



Erstellen Sie einen virtuellen Lastausgleichsserver für die Abonnementsynchronisierung

1. Melden Sie sich bei der Verwaltungs-GUI der NetScaler ADC-Appliance an.
2. Wählen Sie **Traffic Management> Load Balancing > Virtual Servers > Add** aus 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 einen **Port** von **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 **Binden**.
9. Fügen Sie den Abschnitt **Methode** hinzu und legen Sie die **Lastausgleichsmethode** auf **ROUNDROBIN** fest

10. Klicken Sie auf **Fertig**, um Ihre Änderungen abzuschließen.

StoreFront konfigurieren, um Abonnementdaten über den Load Balancer abzurufen

Siehe Abonnementsynchronisierung konfigurieren.

Beim Konfigurieren des Replikationszeitplans geben Sie eine Servergruppenadresse an, die der IP-Adresse des virtuellen Load Balancers des virtuellen Servers für die Abonnementsynchronisierung entspricht.

Citrix Gateway und StoreFront für die delegierte Formularauthentifizierung (DFA) konfigurieren

Die erweiterbare Authentifizierung bietet einen einzigen Anpassungspunkt zur Erweiterung der formularbasierten Authentifizierung von Citrix Gateway und StoreFront. Um eine Authentifizierungslösung mit dem Extensible Authentication SDK zu realisieren, müssen Sie die delegierte Formularauthentifizierung (DFA) zwischen Citrix Gateway und StoreFront konfigurieren. Das Protokoll für die delegierte Formularauthentifizierung ermöglicht es, die Generierung und Verarbeitung von Authentifizierungsformularen, einschließlich der Anmeldeinformationsvalidierung, an eine andere Komponente zu delegieren. Citrix Gateway delegiert beispielsweise seine Authentifizierung an StoreFront, das dann mit einem Authentifizierungsserver oder -dienst eines Drittanbieters interagiert.

Die Konfiguration der delegierten Formularauthentifizierung auf Citrix Gateway wird in CTX200383 beschrieben.

Empfehlungen zur Installation

- Um sicherzustellen, dass die Kommunikation zwischen Citrix Gateway und StoreFront geschützt ist, verwenden Sie HTTPS anstelle des HTTP-Protokolls.
- Stellen Sie bei einer Clusterbereitstellung sicher, dass alle Knoten dasselbe Serverzertifikat installiert und in der IIS-HTTPS-Bindung konfiguriert haben, bevor Sie die Konfigurationsschritte ausführen.
- Stellen Sie sicher, dass Citrix Gateway den Aussteller des StoreFront-Serverzertifikats als vertrauenswürdige Zertifizierungsstelle hat, wenn HTTPS in StoreFront konfiguriert ist.

Überlegungen zur Installation von StoreFront-Clustern

- Installieren Sie ein Authentifizierungs-Plug-in eines Drittanbieters auf allen Knoten, bevor Sie diese miteinander verbinden.

- Konfigurieren Sie alle Einstellungen für die delegierte Formularauthentifizierung auf einem Knoten und übertragen Sie die Änderungen auf die anderen. Siehe „Delegierte Formularauthentifizierung aktivieren“.

Delegierte Formularauthentifizierung aktivieren

Da es keine grafische Benutzeroberfläche zum Einrichten der Citrix Pre-Shared Key-Einstellung in StoreFront gibt, verwenden Sie die PowerShell-Konsole, um die delegierte Formularauthentifizierung zu installieren.

1. Installieren Sie die delegierte Formularauthentifizierung. Sie ist standardmäßig nicht installiert und muss über die 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
```

2. Fügen Sie einen vertrauenswürdigen Citrix-Client hinzu. Konfigurieren Sie den gemeinsamen geheimen Schlüssel (Passphrase) zwischen StoreFront und Citrix Gateway. Ihre Passphrase und Client-ID müssen mit den auf Citrix Gateway konfigurierten übereinstimmen.

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-
DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase
secret
```

3. Legen Sie die Konversationsfabrik für die delegierte Formularauthentifizierung so fest, dass der gesamte Datenverkehr an das benutzerdefinierte Formular weitergeleitet wird. Um die Konversationsfabrik zu finden, suchen Sie nach ConversationFactory in C:\inetpub\wwwroot\Citrix\Authentication\web.config. Dies ist ein Beispiel dafür, was Sie sehen könnten.

```
<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>
```

4. Legen Sie in PowerShell die Konversationsfabrik für die delegierte Formularauthentifizierung fest. In diesem Beispiel auf ExampleBridgeAuthentication.

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
```

PowerShell-Argumente sind nicht groß-/kleinschreibungsempfindlich: **-ConversationFactory** ist identisch mit **-conversationfactory**.

StoreFront deinstallieren

Bevor Sie StoreFront deinstallieren, deinstallieren Sie alle Authentifizierungs-Plugins von Drittanbietern, da dies die Funktionalität von StoreFront beeinträchtigen würde.

Authentifizierung mit verschiedenen Domänen

Einige Organisationen haben Richtlinien, die es ihnen nicht erlauben, Drittentwicklern oder Auftragnehmern Zugriff auf veröffentlichte Ressourcen in einer Produktionsumgebung zu gewähren. Dieser Artikel zeigt Ihnen, wie Sie Zugriff auf veröffentlichte Ressourcen in einer Testumgebung gewähren, indem Sie sich über Citrix Gateway mit einer Domäne authentifizieren. Sie können dann eine andere Domäne verwenden, um sich bei StoreFront und der Receiver für Web-Site zu authentifizieren. 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 für Benutzer nativer Desktop- oder mobiler Citrix Receiver- oder Citrix Workspace-Apps nicht unterstützt.

Eine Testumgebung einrichten

Dieses Beispiel verwendet eine Produktionsdomäne namens production.com und eine Testdomäne namens development.com.

`production.com`-Domäne

Die `production.com`-Domäne in diesem Beispiel ist wie folgt eingerichtet:

- Citrix Gateway mit konfigurierter `production.com` LDAP-Authentifizierungsrichtlinie.
- Die Authentifizierung über das Gateway erfolgt mit einem production\testuser1-Konto und -Passwort.

`development.com`-Domäne

Die `development.com`-Domäne in diesem Beispiel ist 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 development\testuser1-Konto und -Passwort.

- Es besteht keine Vertrauensstellung zwischen den beiden Domänen.

Ein Citrix Gateway für den Store konfigurieren

So konfigurieren Sie ein Citrix Gateway für den Store:

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus, und klicken Sie im Bereich **Aktionen** auf **Citrix Gateways verwalten**.
2. Klicken Sie auf dem Bildschirm „Citrix Gateways verwalten“ auf **Hinzufügen**.
3. Führen Sie die Schritte für Allgemeine Einstellungen, Secure Ticket Authority und Authentifizierung aus.

   Screenshot des Fensters „Citrix Gateway hinzufügen“, Abschnitt „Allgemeine Einstellungen“(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/netscaler-gateway-general-settings.png)

   Screenshot des Fensters „Citrix Gateway hinzufügen“, Abschnitt „Secure Ticket Authority“(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/netscaler-gateway-secure-ticket-authority.png)

   Screenshot des Fensters „Citrix Gateway hinzufügen“, Abschnitt „Authentifizierungseinstellungen“(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/netscaler-gateway-authentication.png)

> **Hinweis:**

> Möglicherweise müssen bedingte DNS-Weiterleitungen hinzugefügt werden, damit die auf beiden Domänen verwendeten DNS-Server FQDNs auf der anderen Domäne auflösen können. Das Citrix Gateway muss die FQDNs des STA-Servers auf der `development.com` Domäne über seinen `production.com` DNS-Server auflösen können. StoreFront sollte auch in der Lage sein, die Callback-URL auf der `production.com` Domäne über seinen `development.com` DNS-Server aufzulösen. Alternativ kann ein `development.com` FQDN verwendet werden, der auf die virtuelle IP (VIP) des virtuellen Citrix Gateway-Servers aufgelöst wird.

Pass-Through vom Citrix Gateway aktivieren

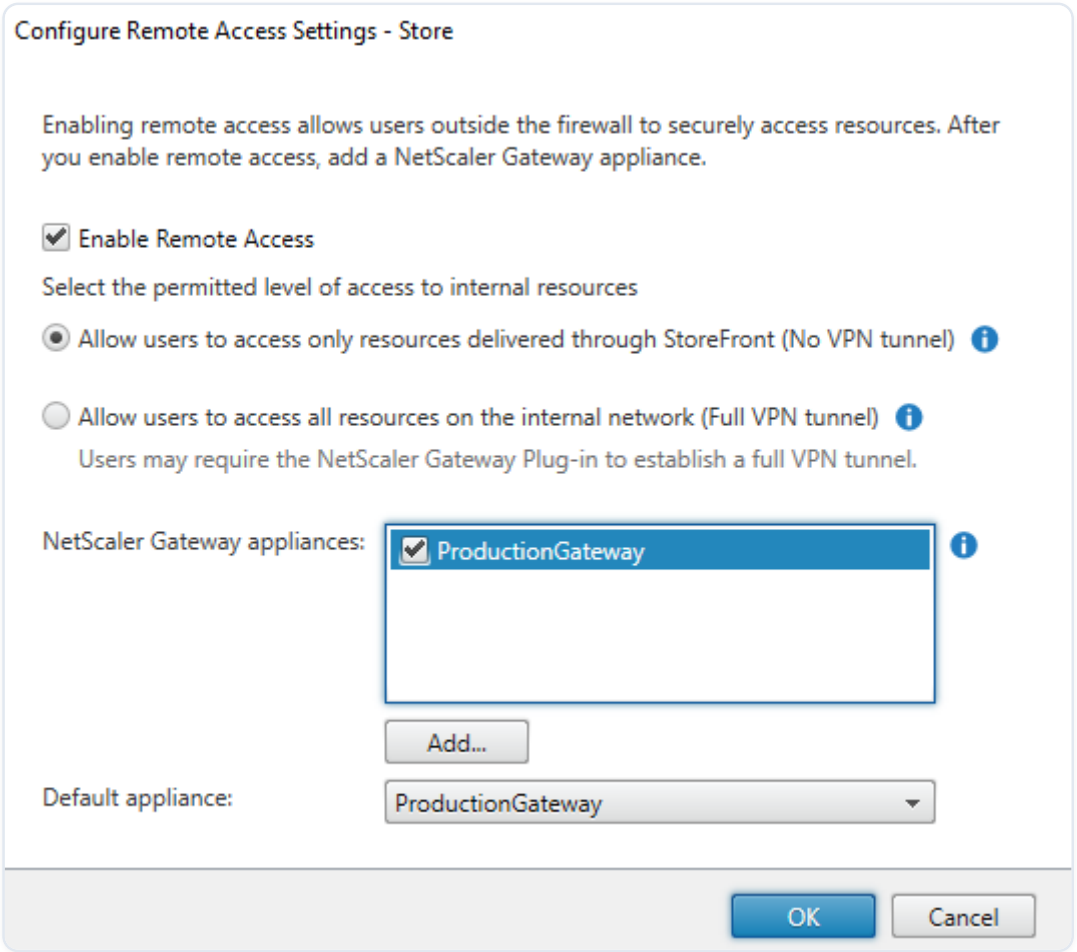
1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus, und klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.

2. Wählen Sie auf dem Bildschirm „Authentifizierungsmethoden verwalten“ die Option **Pass-Through vom Citrix Gateway** aus.
3. Klicken Sie auf **OK**.

Screenshot des Fensters „Authentifizierungsmethoden verwalten“(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/manage-authentication-methods.png)

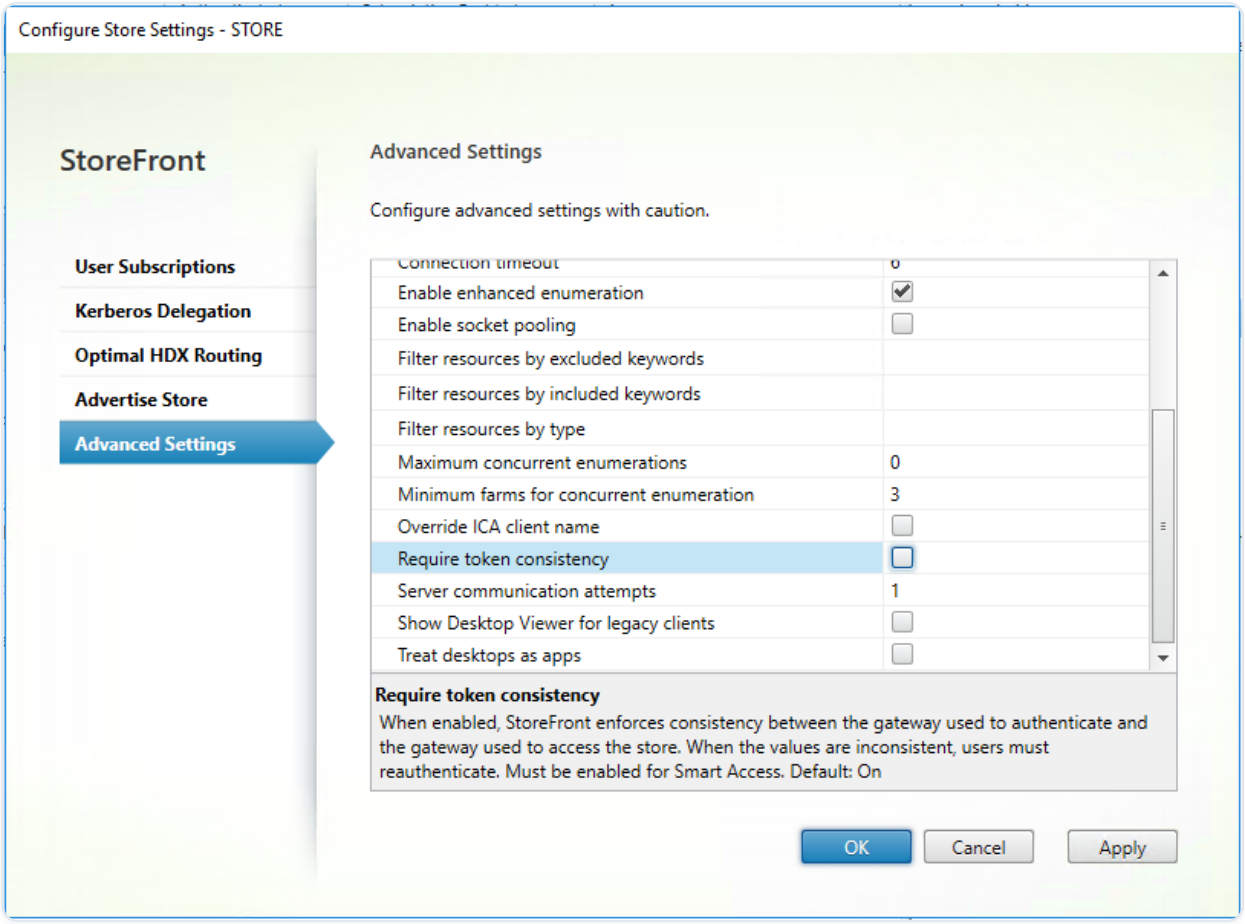
Den Store für den Remotezugriff über das Gateway konfigurieren

1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus, und wählen Sie im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Remotezugriffseinstellungen konfigurieren**.
2. Wählen Sie **Remotezugriff aktivieren** aus.
3. Stellen Sie sicher, dass Sie das Citrix Gateway bei Ihrem Store registriert haben. Wenn Sie das Citrix Gateway nicht registrieren, funktioniert das STA-Ticketing nicht.



Tokenkonsistenz deaktivieren

1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole und wählen Sie im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Store-Einstellungen konfigurieren**.
2. Wählen Sie auf der Seite „Store-Einstellungen konfigurieren“ die Option **Erweiterte Einstellungen**.
3. Deaktivieren Sie das Kontrollkästchen **Tokenkonsistenz erforderlich**. Weitere Informationen finden Sie unter Erweiterte Store-Einstellungen.



4. Klicken Sie auf **OK**.

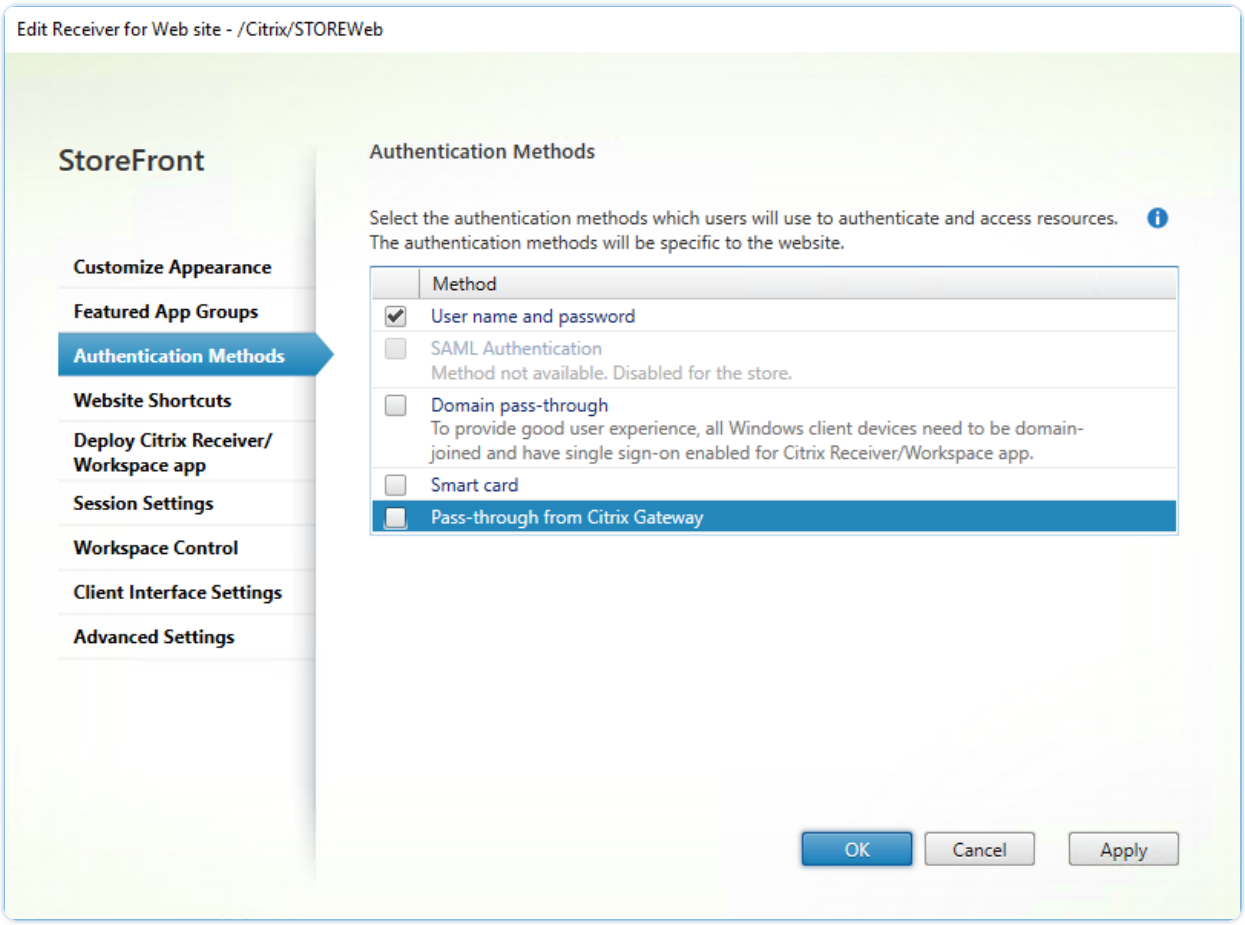
> Hinweis:
>
> Die Einstellung „Tokenkonsistenz erforderlich“ ist standardmäßig aktiviert. Wenn Sie diese Einstellung deaktivieren, funktionieren die SmartAccess-Funktionen, die für die Citrix Gateway End Point Analysis (EPA) verwendet werden, nicht mehr.

Pass-Through von Citrix Gateway für die Website deaktivieren

Wichtig:

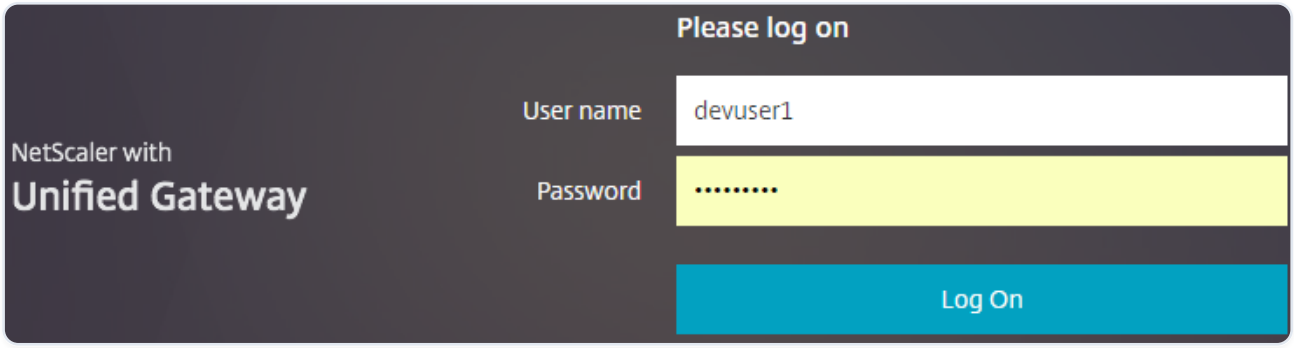
Das Deaktivieren des Pass-Through von Citrix Gateway verhindert, dass die Website versucht, die falschen Anmeldeinformationen aus der `production.com`-Domäne zu verwenden, die vom Citrix Gateway übergeben wurden. Das Deaktivieren des Pass-Through von Citrix Gateway bewirkt, dass die Website den Benutzer zur Eingabe von Anmeldeinformationen auffordert. Diese Anmeldeinformationen unterscheiden sich von den Anmeldeinformationen, die für die Anmeldung über das Citrix Gateway verwendet werden.

1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole.
2. Wählen Sie den **Store** aus, den Sie ändern möchten.
3. Klicken Sie im Bereich **Aktionen** auf **Websites verwalten**.
4. Deaktivieren Sie unter „Authentifizierungsmethoden“ die Option **Pass-Through von Citrix Gateway**.
5. Klicken Sie auf **OK**.

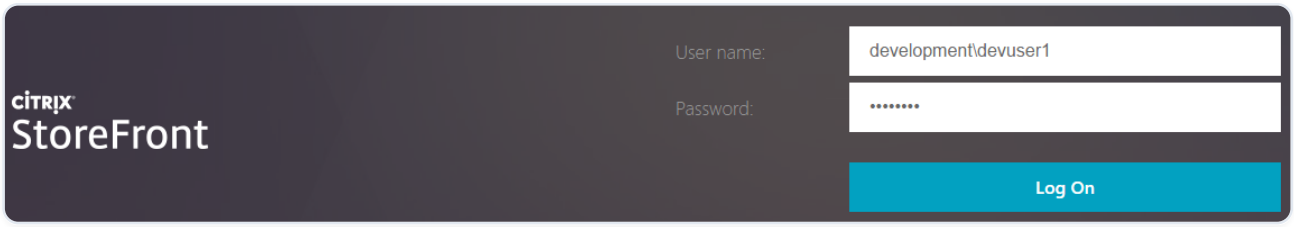


Melden Sie sich mit einem `production.com`-Benutzer und Anmeldeinformationen am Gateway an

Melden Sie sich zum Testen mit einem `production.com` Benutzer und den entsprechenden Anmeldeinformationen bei Gateway an.



Nach der Anmeldung wird der Benutzer aufgefordert, `development.com` Anmeldeinformationen einzugeben.

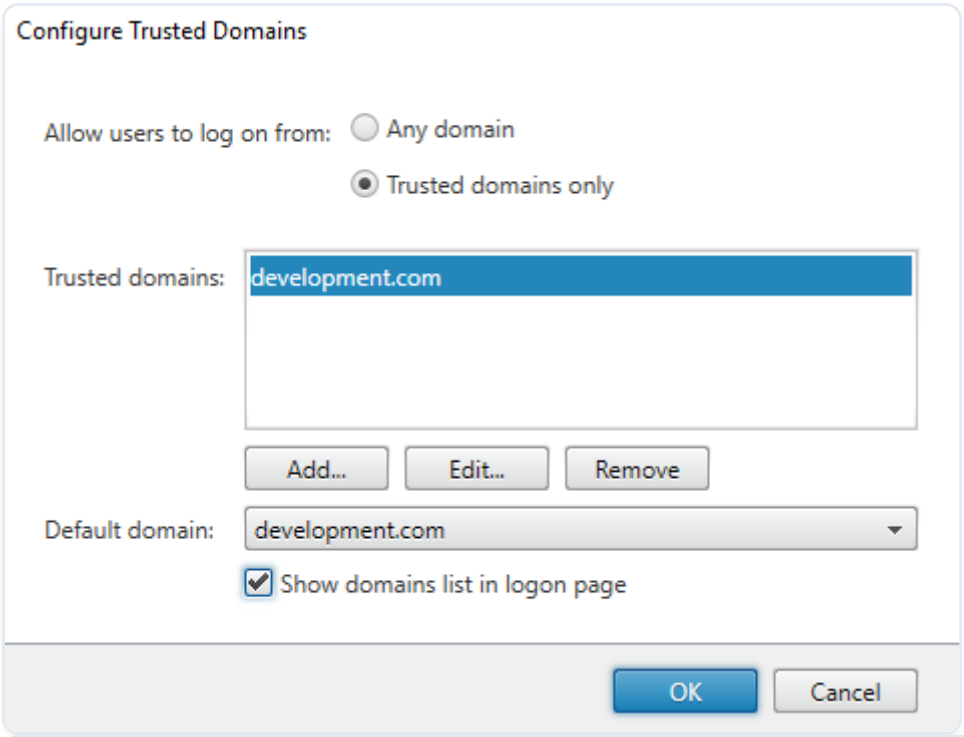


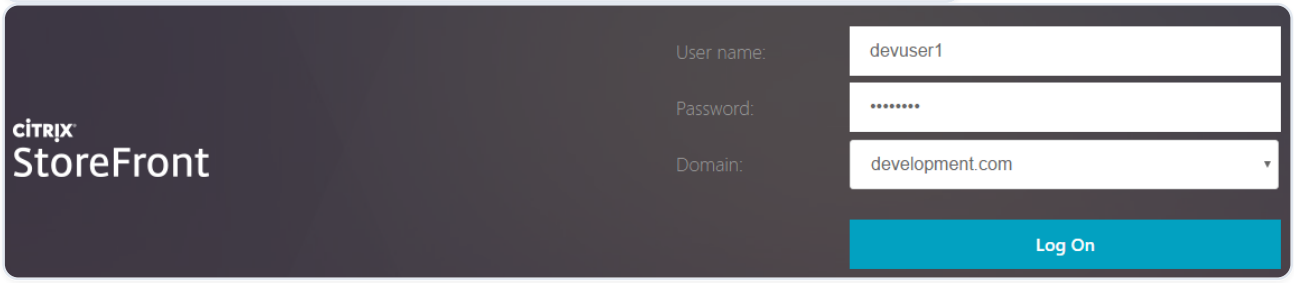
Vertrauenswürdige Domänen-Dropdown-Liste in StoreFront hinzufügen (optional)

Diese Einstellung ist optional, kann aber dazu beitragen, dass der Benutzer nicht versehentlich die falsche Domäne für die Authentifizierung über das Citrix Gateway eingibt.

Wenn der Benutzername für beide Domänen derselbe ist, ist die Eingabe der falschen Domäne wahrscheinlicher. Neue Benutzer sind es möglicherweise auch gewohnt, die Domäne wegzulassen, wenn sie sich über das Citrix Gateway anmelden. Benutzer vergessen dann möglicherweise, Domäne\Benutzername für die zweite Domäne einzugeben, wenn sie zur Anmeldung an der Receiver für Web-Site aufgefordert werden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus, und klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
2. Wählen Sie den Dropdown-Pfeil neben **Benutzername und Kennwort** aus.
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:

Das Zwischenspeichern von Browser-Passwörtern wird in diesem Authentifizierungsszenario nicht empfohlen. Wenn Benutzer unterschiedliche Passwörter für die beiden verschiedenen Domänenkonten haben, kann das Zwischenspeichern von Passwörtern zu einer schlechten Benutzererfahrung führen.

NetScaler® Sitzungsaktionsrichtlinie

- Wenn Single Sign-On für Webanwendungen in Ihrer Citrix Gateway-Sitzungsrichtlinie aktiviert ist, werden falsche Anmeldeinformationen, die von Citrix Gateway an die Website gesendet werden, ignoriert, da Sie die Authentifizierungsmethode **Pass-through von Citrix Gateway** auf der Website deaktiviert haben. Die Website fordert Anmeldeinformationen an, unabhängig davon, wie diese Option eingestellt ist.
- Das Ausfüllen der Single Sign-on-Einträge in den Registerkarten „Client Experience“ und „Published App“ in Citrix Gateway ändert das in diesem Artikel beschriebene Verhalten nicht.

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration | **Client Experience** | Security | Published Applications

Accounting Policy

Override Global

Display Home Page

Home Page

https://sf.development.com/Citrix/S

URL for Web-Based Email

Split Tunnel*

OFF

Session Time-out (mins)

60

Client Idle Time-out (mins)

Clientless Access*

On

Clientless Access URL Encoding*

Clear

Clientless Access Persistent Cookie*

ALLOW

Plug-in Type*

Windows/MAC OS X

Windows Plugin Upgrade

Always

Linux Plugin Upgrade

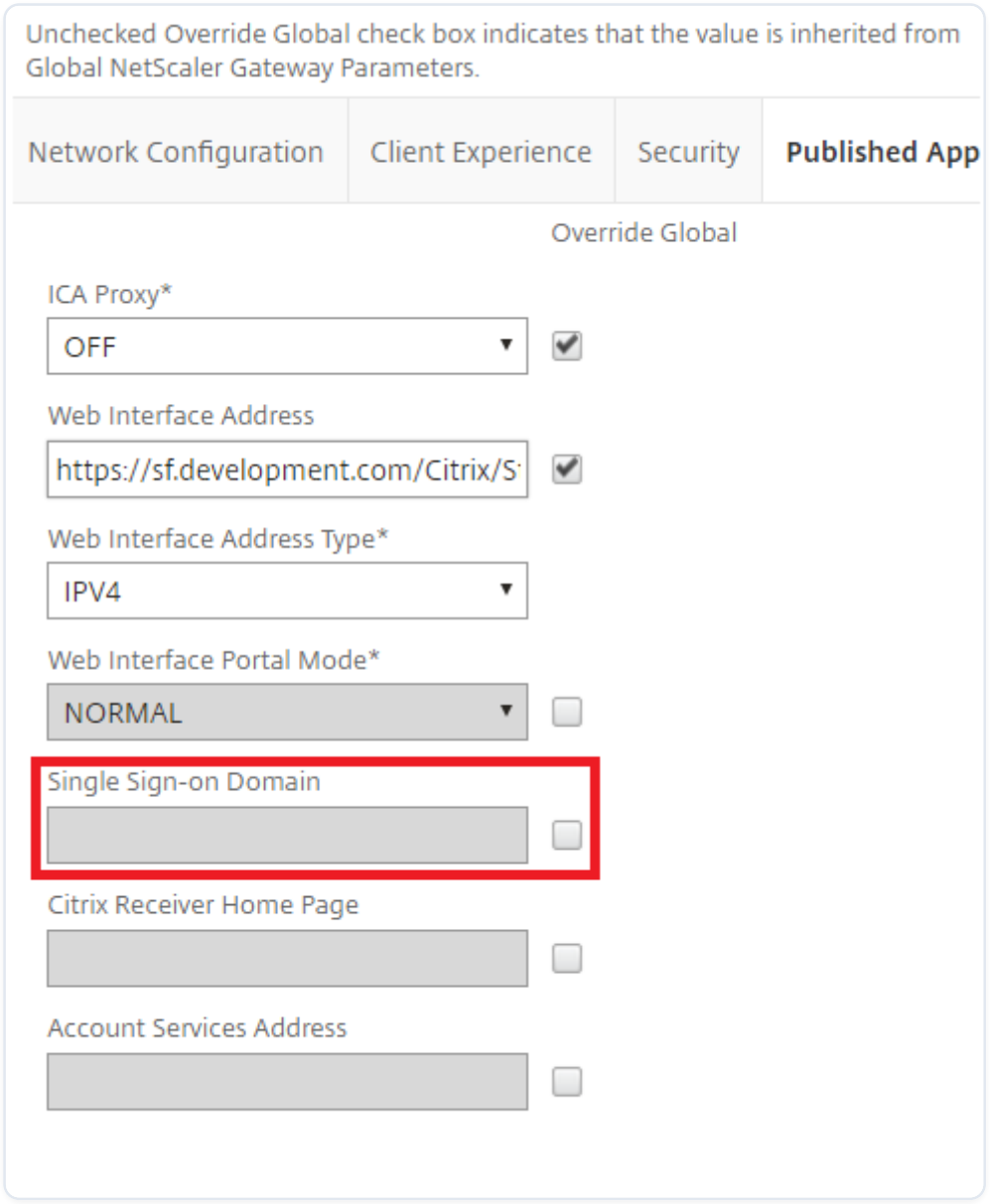
Always

MAC Plugin Upgrade

Always

AlwaysON Profile Name

Single Sign-on to Web Applications



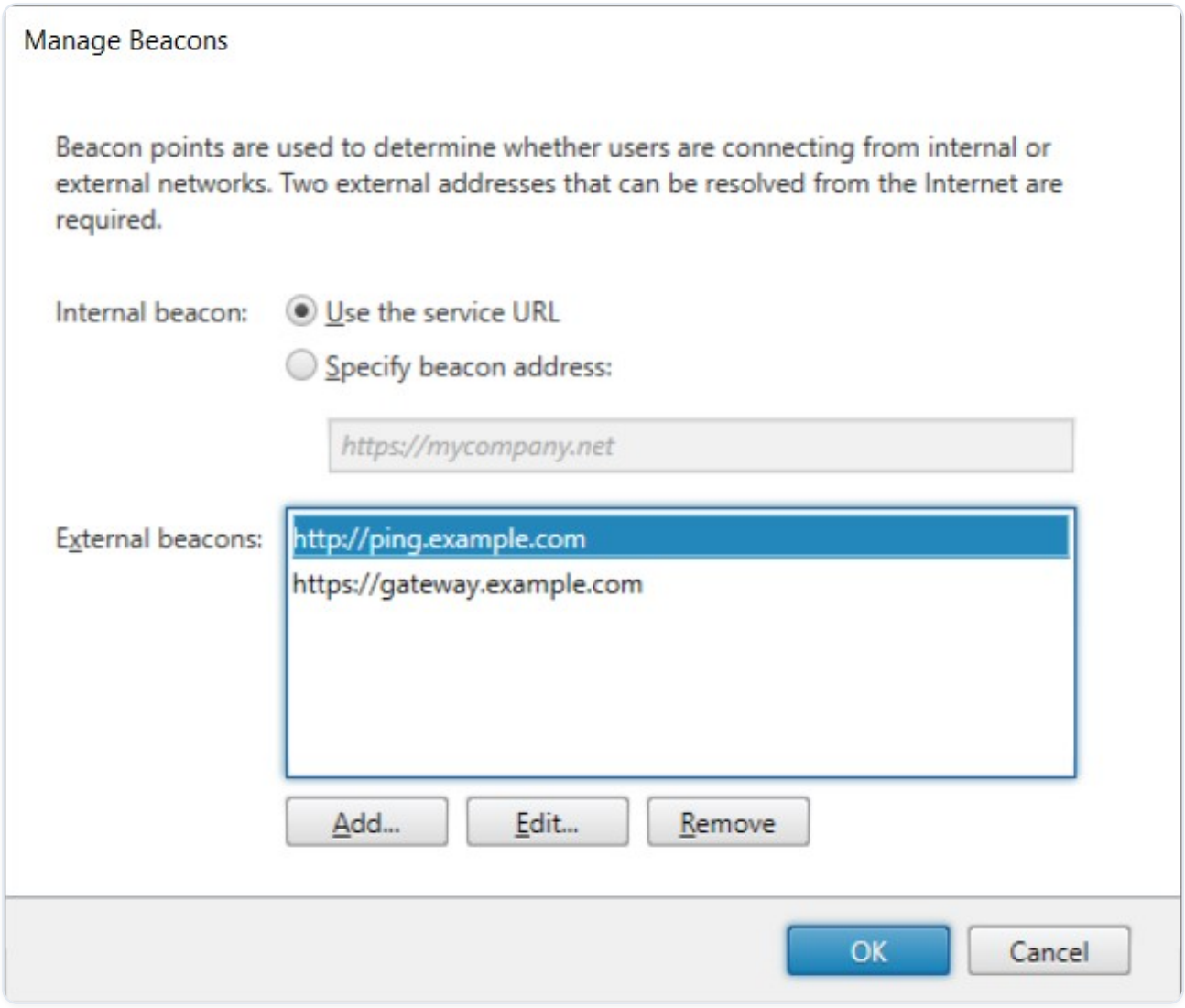
Beacon-Punkte konfigurieren

Wichtig:

- `http://ping.citrix.com` ist nicht mehr verfügbar und sollte nicht verwendet werden.
- Verwenden Sie keine Websites von Drittanbietern, die Sie nicht besitzen, als externen Beacon. Verwenden Sie stattdessen Websites, die von Ihrer Organisation kontrolliert werden.

- Die internen und externen Beacon-URLs sollten vollqualifizierte Domänennamen (FQDN) wie (`http://example.com`) und nicht den abgekürzten NetBIOS-Namen (`http://example`) sein.

Geben Sie im Bildschirm „Beacons verwalten“ URLs innerhalb und außerhalb Ihres internen Netzwerks an, die als Beacon-Punkte verwendet werden sollen. Die lokal installierte Citrix Workspace-App versucht, Beacon-Punkte zu kontaktieren, und verwendet die Antworten, um festzustellen, 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 übermittelt, der die Ressource bereitstellt, damit die entsprechenden Verbindungsdetails an die Citrix Workspace-App zurückgegeben werden können. Dadurch wird sichergestellt, dass Benutzer nicht erneut zur Anmeldung aufgefordert werden, wenn sie auf einen Desktop oder eine Anwendung zugreifen. Beacons werden vom browserbasierten HDX-Client nicht verwendet. Die Citrix Workspace-App für Windows ab Version 2503 verwendet nur den internen Beacon, nicht externe Beacons. Ältere Versionen und die Citrix Workspace-App auf anderen Plattformen verwenden sowohl interne als auch externe Beacons.



Wenn beispielsweise der interne Beacon-Punkt zugänglich ist, bedeutet dies, dass der Benutzer mit dem lokalen Netzwerk verbunden ist. Wenn die Citrix Workspace-App jedoch den internen Beacon-Punkt nicht kontaktieren kann und Antworten von beiden externen Beacon-Punkten empfängt, bedeutet dies, dass der Benutzer eine Internetverbindung hat, sich aber außerhalb des Unternehmensnetzwerks befindet. Daher muss der Benutzer Desktops und Anwendungen über Citrix Gateway verbinden. Wenn der Benutzer auf einen Desktop oder eine Anwendung zugreift, wird der Server, der die Ressource bereitstellt, benachrichtigt, die Details der Citrix Gateway-Appliance bereitzustellen, über die die Verbindung geleitet werden muss. Dies bedeutet, dass sich der Benutzer beim Zugriff auf den Desktop oder die Anwendung nicht an der Appliance anmelden muss.

Standardmäßig legt StoreFront Folgendes fest:

- Den internen Beacon auf die Basis-URL Ihrer Bereitstellung.
- Externe Beacons auf:

- `http://ping.citrix.com`. Dies ist nicht mehr verfügbar und muss durch Ihren eigenen Beacon ersetzt werden.
- Die URL der ersten Citrix Gateway-Bereitstellung, die Sie hinzufügen.

So konfigurieren Sie Beacon-Punkte:

1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus und klicken Sie im Bereich „Aktionen“ auf **Beacons verwalten**.
2. Geben Sie die URL an, die als interner Beacon-Punkt verwendet werden soll.
   - Um die Server-URL oder die Lastenausgleichs-URL Ihrer StoreFront-Bereitstellung zu verwenden, wählen Sie **Dienst-URL verwenden**.
   - Um eine alternative URL zu verwenden, wählen Sie **Beacon-Adresse angeben** und geben Sie eine hochverfügbare URL in Ihrem internen Netzwerk ein.
3. Klicken Sie auf **Hinzufügen**, um die URL eines externen Beacon-Punkts einzugeben. Um einen Beacon-Punkt zu ändern, 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 diese Adresse nicht mehr als Beacon-Punkt zu verwenden.

   Sie müssen mindestens zwei hochverfügbare externe Beacon-Punkte angeben, die über das Internet aufgelöst werden können. Diese müssen auf HTTP-HEAD-Anfragen antworten. Sie sollten URLs verwenden, die von Ihrer Organisation kontrolliert werden, nicht Websites Dritter.

Wenn Sie Beacon-Punkte ändern, stellen Sie sicher, dass Benutzer die Citrix Workspace-App mit den geänderten Beacon-Informationen aktualisieren. Benutzer können eine aktualisierte Bereitstellungsdatei der Citrix Workspace-App erhalten, indem sie sich über einen Webbrowser anmelden und zu den Kontoeinstellungen navigieren. Andernfalls können Sie eine Bereitstellungsdatei exportieren für den Store und diese Datei Ihren Benutzern zur Verfügung stellen.

PowerShell

Um die aktuellen Beacons abzurufen, verwenden Sie Get-STFRoamingBeacon.

Um einen Beacon hinzuzufügen, verwenden Sie Set-STFRoamingBeacon.

Um die Beacons auf ihre Standardwerte zurückzusetzen, verwenden Sie Clear-STFRoamingBeacon.

Ein einzelnes FQDN für die interne und externe Nutzung erstellen

Sie können einen einzelnen vollqualifizierten Domänennamen (FQDN) erstellen, der den direkten Zugriff auf einen Store innerhalb Ihres Unternehmensnetzwerks und remote über ein Citrix Gateway ermöglicht.

Sie könnten beispielsweise die folgenden URLs verwenden:

- `https://storefront.example.com` als die einzige URL, die Benutzer für den Zugriff auf StoreFront verwenden. Innerhalb des Netzwerks wird sie zum StoreFront-Server oder Lastenausgleich aufgelöst. Außerhalb des Netzwerks wird sie zum Gateway aufgelöst.
- `https://storefrontcb.example.com` als Callback-URL. Innerhalb Ihres Netzwerks wird diese zum Gateway aufgelöst. Dies ist nur für Smart Access oder passwortlose Authentifizierung erforderlich. Sie müssen sicherstellen, dass das Zertifikat auf dem Gateway diese Adresse als SAN enthält oder ein Wildcard-Zertifikat verwenden.

Basis-URL der Servergruppe

Ändern Sie die Basis-URL in die einzelne URL. Siehe Basis-URL für eine Bereitstellung ändern.

StoreFront-Beacons für lokal installierte Citrix Workspace-App

Die lokal installierte Citrix Workspace™-App versucht, Beacon-Punkte zu kontaktieren, und verwendet die Antworten, um festzustellen, 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 einstellen, von der Sie wissen, dass sie nur intern zugänglich ist.

Siehe Beacon konfigurieren.

Externes DNS

- storefront.example.com wird zur externen IP des virtuellen Citrix Gateway-Servers aufgelöst.

Internes DNS

- storefront.example.com wird zum StoreFront-Lastenausgleich oder zur IP des einzelnen StoreFront-Servers aufgelöst.

- storefrontcb.example.com wird zur Gateway-vServer-VIP aufgelöst. Wenn eine Firewall zwischen der DMZ und dem lokalen Unternehmensnetzwerk vorhanden ist, muss dies zugelassen werden.

Citrix Workspace™-App bei Verbindung über ein Gateway vorschreiben

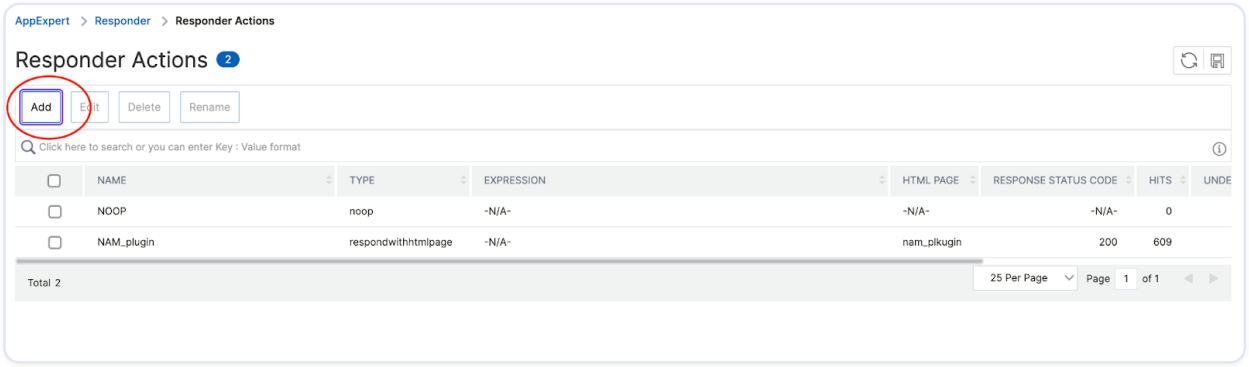
Sie können Benutzer dazu verpflichten, die Citrix Workspace-App zu verwenden, wenn sie sich über ein Gateway verbinden, indem Sie ein Plug-in verwenden.

So stellen Sie das Plug-in auf Ihrem Gateway bereit:

1. Laden Sie das Plug-in von Citrix Downloads herunter.
2. Extrahieren Sie die Zip-Datei und citrix-gateway-plugin.tar.gz. Sie besteht aus einer HTML-Datei und einer JavaScript-Datei.
3. Kopieren Sie die Dateien auf das NetScaler Gateway unter `/var/netscaler/gui/vpn/init`
4. Konfigurieren über die Management-GUI oder Konfigurieren über die CLI

Konfigurieren über die Management-GUI

1. Melden Sie sich bei der NetScaler® Admin-GUI an.
2. Erstellen Sie eine Responder-Aktion und klicken Sie auf Hinzufügen.

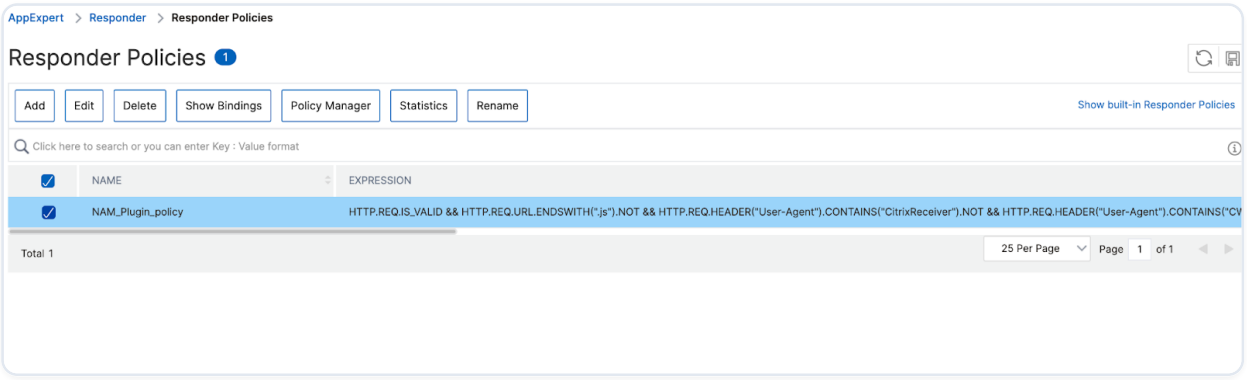


3. Konfigurieren Sie die Responder-Aktion:

   Typ: Mit HTML-Seite antworten

   Hinzufügen: Pfad eingeben `/vpn/init/native-app-mandate.html`

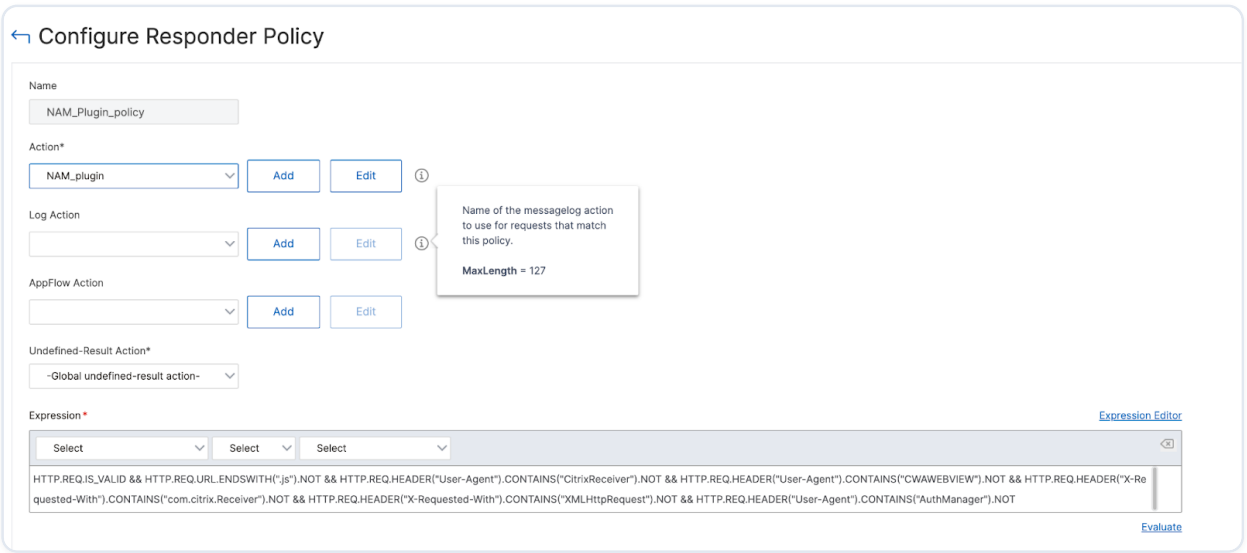
4. Erstellen Sie eine Responder-Richtlinie.



5. Konfigurieren Sie die Responder-Richtlinie:

   Aktion: Der Name der Aktion, die Sie oben erstellt haben.

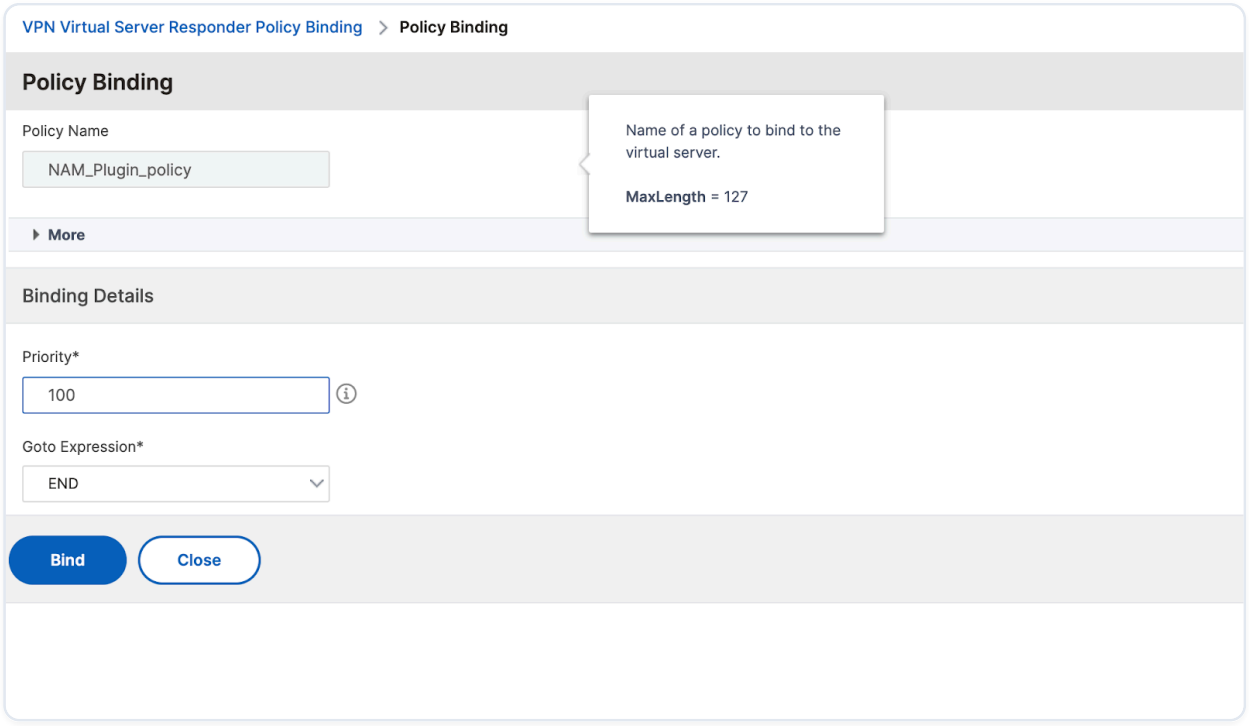
   Ausdruck: `HTTP.REQ.IS_VALID && HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CWAWEBVIEW").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("XMLHttpRequest").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("AuthManager").NOT`



6. Navigieren Sie zu dem virtuellen Server, auf dem Sie die Responder-Richtlinie binden möchten.



7. Binden Sie die von Ihnen erstellte Richtlinie.



8. Um zu überprüfen, ob es korrekt konfiguriert ist, öffnen Sie die Gateway-URL, um zu bestätigen, dass der Bildschirm **Citrix Workspace-App erforderlich** angezeigt wird. Fügen Sie die Netscaler-URL zur Citrix Workspace-App hinzu und bestätigen Sie, dass der Bildschirm **Citrix Workspace-App erforderlich** nicht angezeigt wird.

Konfigurieren über die CLI

Um die Funktion „Citrix Workspace-App erforderlich“ über die CLI zu konfigurieren, führen Sie Folgendes aus:

1. Erstellen Sie eine Responder-Aktion mit einer HTML-Datei (Sie können die Konfiguration in der GUI bearbeiten)

```
add responder action respond_with_html_act respondwithhtmlpage
sample_page -responseStatusCode 200
```

2. Erstellen Sie eine Responder-Richtlinie, um Anfragen von einem Webbrowser zu bearbeiten, nicht von der Citrix Workspace-App.

```
add responder policy respond_with_html_pol "HTTP.REQ.IS_VALID &&
HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-
Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-
Agent").CONTAINS("CWAWEBVIEW").NOT && HTTP.REQ.HEADER("X-Requested-
```

```
With").CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-
Requested-With").CONTAINS("XMLHttpRequest").NOT &&
HTTP.REQ.HEADER("User-Agent").CONTAINS("AuthManager").NOT"
respond_with_html_act
```

3. Binden Sie die Richtlinie an den VPN-vServer

```
bind vpn vserver vpn_vs -policy respond_with_html_pol -priority 100
-gotoPriorityExpression END -type AAA_REQUEST
```

Entra ID-Authentifizierung über OIDC und Single Sign-On zu VDA

Dieser Artikel beschreibt, wie StoreFront und ein NetScaler ADC konfiguriert werden, um Benutzern die Authentifizierung mit Entra ID über OIDC zu ermöglichen und sich dann per Single Sign-On bei einem Entra-verbundenen VDA anzumelden.

> **WICHTIG:**
>
> Die Entra ID-Authentifizierung über OIDC und Single Sign-On zu VDA befindet sich derzeit in der Vorschau. Diese Funktion wird ohne Support bereitgestellt und wird noch nicht für den Einsatz in Produktionsumgebungen empfohlen.

Voraussetzungen

- NetScaler ADC
- StoreFront 2507 LTSR CU1 oder höher
- Moderne Erfahrung
- Microsoft Entra ID und ein Konto mit einer der folgenden Berechtigungen:
  - Cloud Application Administrator
  - Application Administrator
  - Global Administrator
- DaaS-Abonnement mit Konnektoren. Dies ist nicht mit CVAD verfügbar.
- Veröffentlichte Desktops und/oder Apps

- Für Starts aus einem Webbrowser in die Citrix Workspace-App, um SSO zu VDAs zu ermöglichen, Citrix Web Extension.

Bekannte Probleme und Einschränkungen

- Die Aktivierung von Föderierter Authentifizierungsdienst in einem Store, der die Entra ID-Authentifizierung verwendet, wird nicht unterstützt und kann zu Startfehlern führen.
- Wenn ein Store eine Citrix Virtual Apps and Desktops Site enthält und ein Benutzer sich über Entra ID via OIDC authentifiziert, listet StoreFront keine Ressourcen von dieser Site auf.
- Entra ID SSO zu VDAs wird nur bei Verwendung der OIDC-basierten Authentifizierung unterstützt. Es wird nicht mit SAML unterstützt.
- StoreFront verwendet eine große Menge RAM, wenn ein Benutzer Mitglied vieler Entra-Gruppen ist.

Entra ID-Authentifizierung mit OIDC

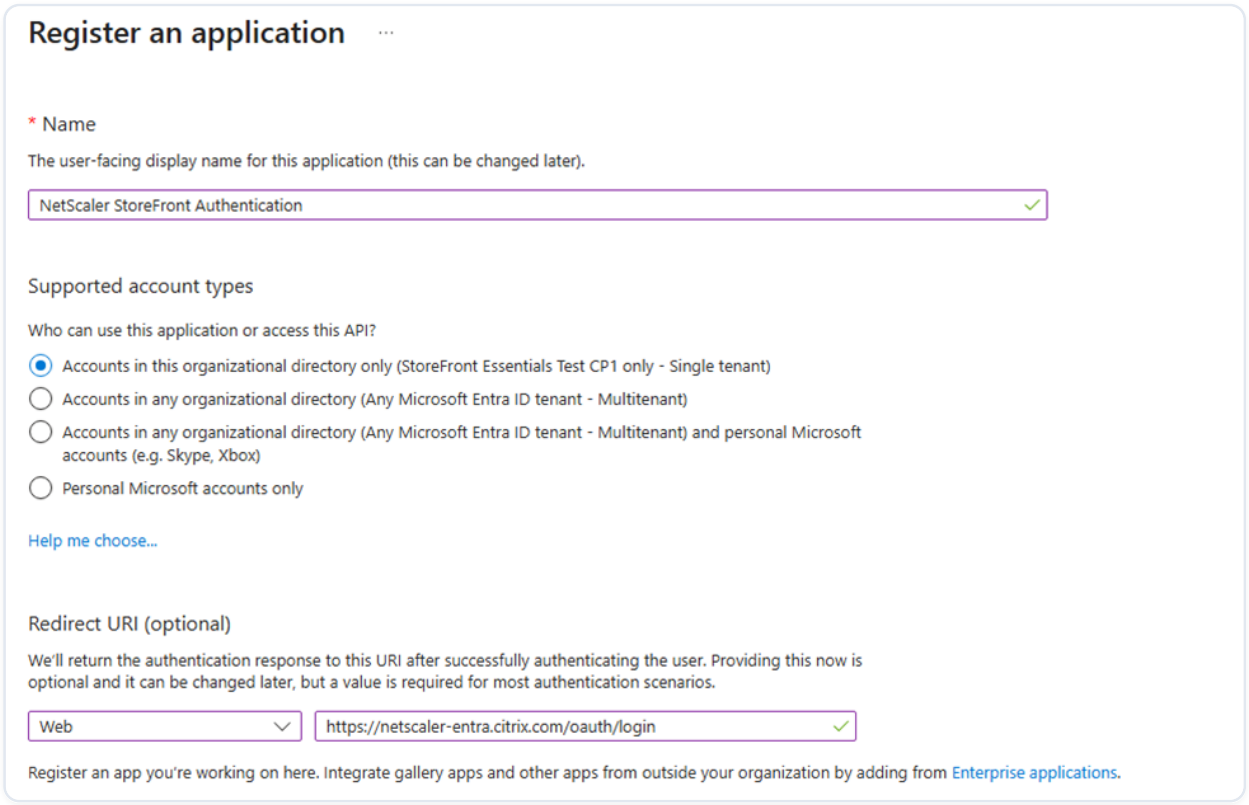
Dieser Abschnitt beschreibt, wie NetScaler und StoreFront konfiguriert werden, damit Benutzer sich mit Entra ID authentifizieren können. In dieser Konfiguration können Benutzer entweder eine hybride Identität oder eine reine Entra-Identität ohne Active Directory-Konto haben.

Eine Microsoft Azure Entra ID-Anwendung erstellen

Eine App-Registrierung in Microsoft Entra ID definiert Ihre Anwendung, sodass Entra ID sie erkennt – in diesem Fall NetScaler OIDC. Diese Registrierung verwaltet auch die Authentifizierungs- und Autorisierungsanfragen der Anwendung. Da OAuth einen vertrauenswürdigen Identitätsanbieter (IdP) benötigt, um Benutzer zu authentifizieren und Token auszustellen, teilt die Registrierung Ihrer App Entra ID mit: „Diese Anwendung verwendet Sie als ihren IdP für OAuth-Flows.“

1. Melden Sie sich beim Azure-Portal für den Entra ID-Mandanten an, den Sie für die NetScaler- oder StoreFront-Authentifizierung verwenden.
2. Gehen Sie zu **Microsoft Entra ID resource** > **Manage** > **App registrations**, und wählen Sie dann **New registration**.
3. Benennen Sie die Anwendung, zum Beispiel NetScaler StoreFront Authentication.
4. Wählen Sie unter **Supported account types** die Option **Accounts in this organizational directory only**.
5. Wählen Sie unter **Redirect URI** die Option **Web** für den Typ der Anwendung, die Sie erstellen möchten. Geben Sie die URI ein, an die das Zugriffstoken gesendet wird. Verwenden Sie das

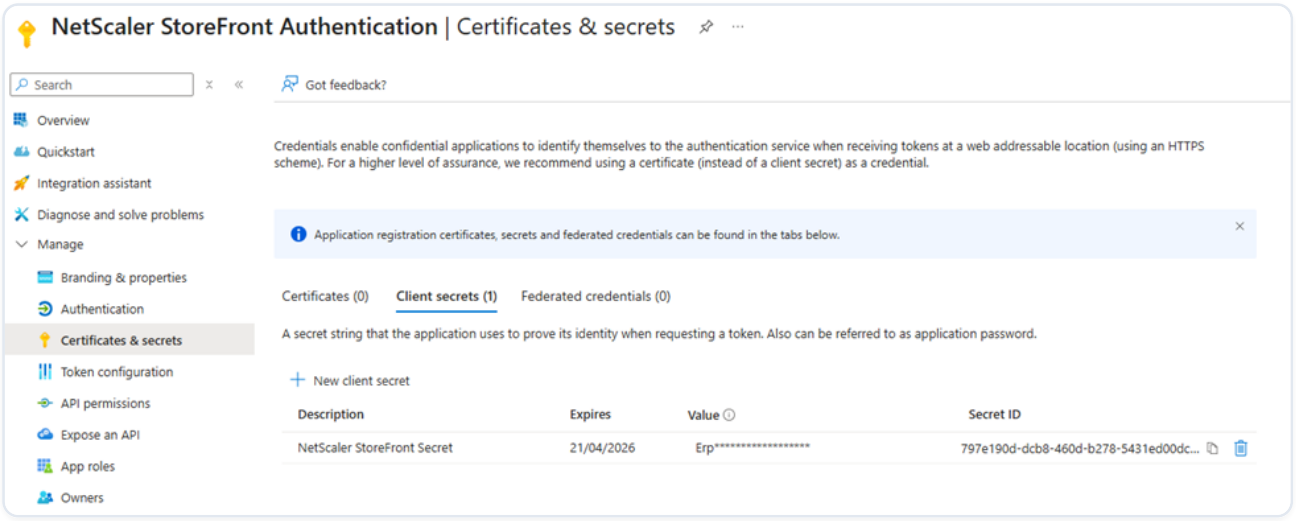
Format \<NetScaler Virtual Server URL>/oauth/login, zum Beispiel `https://netscalerentra.customer.com/oauth/login`.



Clientgeheimnis erstellen

So erstellen Sie ein Clientgeheimnis:

1. Nachdem Sie die Anwendung registriert haben, wechseln Sie zu **Verwalten** > **Zertifikate & Geheimnisse**.
2. Wählen Sie **Clientgeheimnisse** und dann **Neues Clientgeheimnis**. Ihre App verwendet diese Anmeldeinformationen, um sicher mit dem IdP zu kommunizieren und Token anzufordern.
3. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
4. Nachdem Sie das Geheimnis erstellt haben, notieren Sie den Geheimniswert, da Sie ihn später im Einrichtungsprozess benötigen und er nur während dieser Erstellungsphase sichtbar ist.

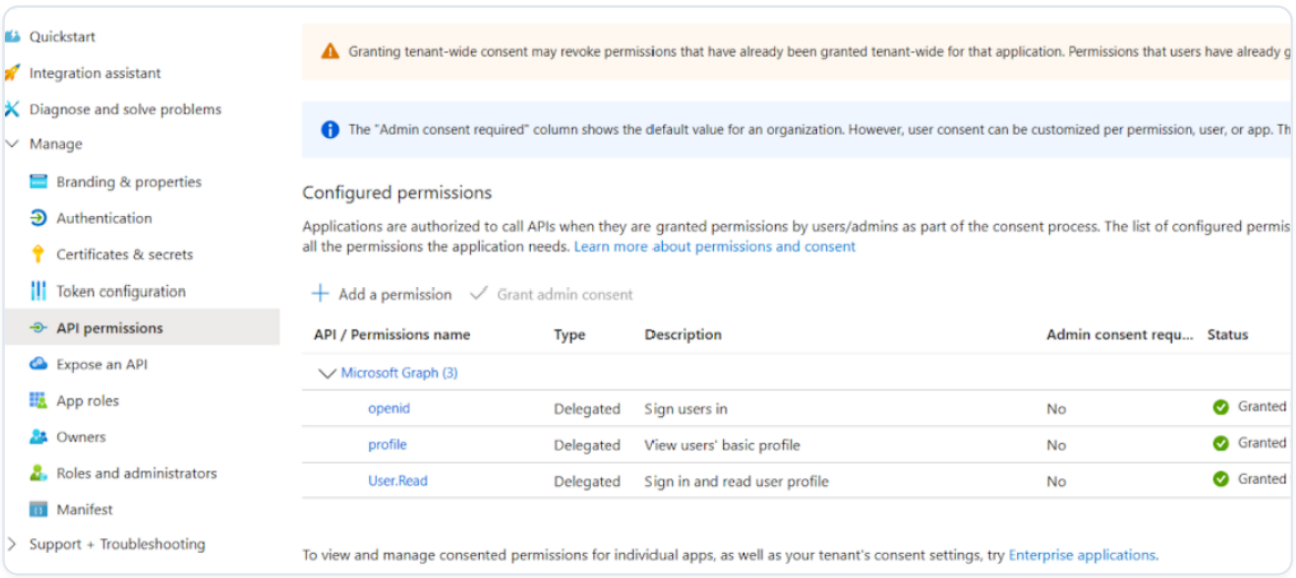


Anwendungsberechtigungen konfigurieren

So konfigurieren Sie App-Berechtigungen:

1. Wechseln Sie zu **Verwalten** > **App-Registrierungen**, und wählen Sie dann Ihre Anwendung aus.
2. Wählen Sie **Verwalten** > **API-Berechtigungen**.
3. Die Berechtigung **User.Read** ist standardmäßig bereits hinzugefügt.
4. Fügen Sie **openid** und **profile** hinzu.
5. Wählen Sie **Administratoreinwilligung erteilen für \<tenant name>** und akzeptieren Sie.

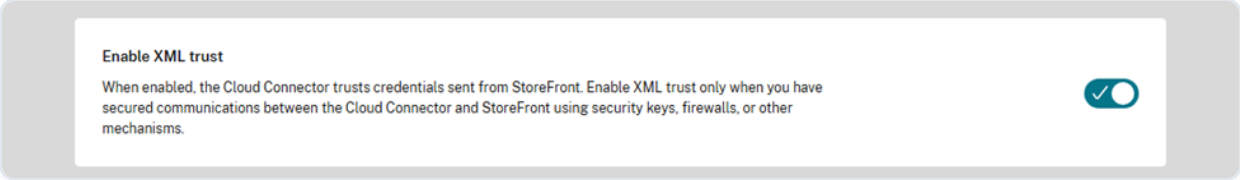
„Administratoreinwilligung erteilen für“ in den API-Berechtigungen in Microsoft Entra ID bedeutet, dass ein Administrator im Namen aller Benutzer in der Organisation die Genehmigung erteilt, damit eine Anwendung auf bestimmte Ressourcen oder APIs mit den angeforderten Berechtigungen zugreifen kann.



Citrix DaaS konfigurieren, um XML-Vertrauen zu aktivieren

Standardmäßig authentifiziert Citrix DaaS Anfragen mithilfe der Active Directory-Anmeldeinformationen des Benutzers. Bei der Entra ID-Authentifizierung verfügt StoreFront nicht über die Anmeldeinformationen. Daher müssen Sie DaaS so konfigurieren, dass es StoreFront vertraut, ohne eine Authentifizierung zu verlangen. Es wird dringend empfohlen, stattdessen Sicherheitsschlüssel zu aktivieren, um eine Authentifizierung auf Dienstebene bereitzustellen.

1. Melden Sie sich bei Citrix Cloud an und rufen Sie die DaaS-Konsole auf.
2. Gehen Sie zu **Einstellungen**.
3. Aktivieren Sie **XML-Vertrauen**.



4. (Optionaler Schritt) Für zusätzliche Sicherheit können Sie Sicherheitsschlüssel zwischen DaaS und StoreFront aktivieren. Weitere Informationen finden Sie unter Sicherheitsschlüssel verwalten in der Citrix DaaS™-Dokumentation.

NetScaler-Authentifizierungsprofil konfigurieren

Dieser Abschnitt beschreibt, wie Sie ein NetScaler-Authentifizierungsprofil konfigurieren, das Sie an Ihren Gateway-VPN-Virtual-Server binden können. Diese Konfiguration weist den ADC an, wie Benutzer zur Anmeldung an einen externen OAuth-IdP (wie Microsoft Entra ID) umgeleitet werden und wie die nach der Authentifizierung empfangenen OAuth-Token verarbeitet werden. Sie legt Endpunkte, Client-Anmeldeinformationen, Bereiche und die Art und Weise fest, wie der ADC Benutzerinformationen aus Token extrahiert.

Sie benötigen das Client-Geheimnis aus den vorherigen Schritten und die Microsoft Entra ID-Authentifizierungsendpunkte. Die Authentifizierungsendpunkte finden Sie im Azure-Portal, indem Sie zu Ihrer App-Registrierungsübersicht navigieren und auf die Registerkarte **Endpunkte** klicken.

Authentifizierungs-Virtual-Server erstellen

Der Authentifizierungs-Virtual-Server übernimmt die Benutzerauthentifizierung.

```
add authentication vserver EntraId_Authentication_VirtualServer SSL
0.0.0.0 443 \

  -state ENABLED \
```

```
  -authentication ON \

  -td 0 -appflowLog ENABLED \

  -noDefaultBindings NO

bind ssl vserver EntraId_Authentication_VirtualServer \

  -certkeyName <Certificate Key Name>
```

OAuth-Richtlinie und -Aktion erstellen

Die OAuth-Aktion gibt an, wie NetScaler ADC mit einem OAuth-IdP wie Microsoft Entra ID interagiert. Diese Aktion ermöglicht es dem Citrix Gateway, Benutzer zur Anmeldung an den IdP umzuleiten und das zurückgegebene OAuth-Token zu verarbeiten. Sie setzt `userNameField` auf `oid`, wodurch das Gateway die OID als Benutzernamen bei der Authentifizierung gegenüber StoreFront übergibt. StoreFront überprüft, ob die OID mit den Details übereinstimmt, die es beim Nachschlagen des Entra ID-Zugriffstokens erhält, andernfalls schlägt die Authentifizierung fehl.

Sie benötigen die Client-ID und das Client-Geheimnis aus den vorherigen Schritten.

```
add authentication OAuthAction EntraId_Oauth_Server \

  -authorizationEndpoint "https://login.microsoftonline.com/<TenantId>/
oauth2/v2.0/authorize\?prompt=login" \

  -tokenEndpoint "https://login.microsoftonline.com/<TenantId>/oauth2/
v2.0/token" \

  -clientID <ClientId> \

  -clientSecret <ClientSecret> \

  -Attribute1 email \

  -Attribute2 family_name \

  -Attribute3 given_name \

  -Attribute4 upn \

  -CertEndpoint "https://login.microsoftonline.com/<TenantId>/discovery/
```

```
v2.0/keys" \
  -userNameField oid \
  -allowedAlgorithms HS256 RS256 RS512 \
  -PKCE ENABLED \
  -tokenEndpointAuthMethod client_secret_post \
  -OAuthType GENERIC \
  -grantType CODE \
  -refreshInterval 1440
add authentication Policy EntraId_Authentication_Policy \
  -rule true \
  -action EntraId_Oauth_Server
```

Der `authorizationEndpoint` enthält den Abfragezeichenfolgenparameter `prompt=login`, sodass Benutzer zur erneuten Authentifizierung gezwungen werden, wenn sie versuchen, über den NetScaler auf StoreFront zuzugreifen.

Authentifizierungsrichtlinie an den virtuellen Server binden

```
bind authentication vserver EntraId_Authentication_VirtualServer \
  -policy EntraId_Authentication_Policy \
  -priority 100 \
  -gotoPriorityExpression END
```

Authentifizierungsprofil erstellen

```
add authentication authnProfile EntraId_Auth_Profile \
  -authnVsName EntraId_Authentication_VirtualServer \
```

```
  -AuthenticationLevel 0
```

VPN-Virtual-Server erstellen und Authentifizierungsprofil binden

Führen Sie die Schritte 1, 2 und 4 aus NetScaler Gateway in StoreFront integrieren aus, indem Sie das in den vorherigen Schritten erstellte Authentifizierungsprofil verwenden.

Alternativ können Sie, wenn Sie bereits ein geeignetes Citrix Gateway besitzen, das neue Authentifizierungsprofil daran binden. Das Ausführen dieses Befehls ersetzt das vorhandene Authentifizierungsprofil.

```
set vpn vserver <StoreFront ICA Proxy vServer> \

  -authentication ON \

  -authnProfile EntraId_Auth_Profile
```

Entra ID-Token-Injektionskonfiguration für SSO bei StoreFront

Nachdem das Citrix Gateway den Benutzer authentifiziert hat, muss es ausreichende Informationen an StoreFront übergeben, damit dieses überprüfen kann, ob der Benutzer authentifiziert ist, und die Gruppenmitgliedschaft nachschlagen kann. Standardmäßig sendet das Citrix Gateway nur den Active Directory-Benutzernamen und das Kennwort. Im Falle der Entra ID-Authentifizierung muss es das Entra ID-Zugriffstoken übergeben, damit StoreFront Benutzerinformationen mithilfe der Microsoft Graph API nachschlagen kann. Um dies zu erreichen, müssen Sie eine Rewrite-Richtlinie hinzufügen, die das Entra ID-Token dem Aufruf hinzufügt, den es zur Authentifizierung des Benutzers bei StoreFront tätigt. Wenn die Rewrite-Richtlinie für das Entra ID-Zugriffstoken nicht wirksam wird, schlägt die Anmeldung fehl. Wenn die Rewrite-Richtlinienfunktion standardmäßig deaktiviert ist und noch nicht aktiviert wurde, müssen Sie sie zuerst aktivieren.

```
enable ns feature Rewrite

add rewrite action EntraId_Oauth_Insert_AccessToken_Header
insert_http_header X-Citrix-OIDC-Access-Token
"AAA.USER.ATTRIBUTE(\"accesstoken\")" \

  -comment "A rewrite policy to add the OAUTH access_token to subsequent
user authentication requests"
```

```
add rewrite policy EntraId_Oauth_Insert_AccessToken_Policy
"HTTP.REQ.URL.TO_LOWER.ENDSWITH(\"gatewayauth/login\") ||
HTTP.REQ.URL.TO_LOWER.ENDSWITH(\"citrixagbasic/authenticate\")"
EntraId_Oauth_Insert_AccessToken_Header \

  -comment "A rewrite policy to add the OAUTH access_token to subsequent
user authentication requests"

bind vpn vserver <StoreFront ICA Proxy vServer> \

  -policy EntraId_Oauth_Insert_AccessToken_Policy \

  -priority 100 \

  -gotoPriorityExpression END \

  -type REQUEST
```

Citrix Gateway in StoreFront konfigurieren

1. Eine NetScaler Gateway-Instanz in StoreFront hinzufügen.
2. Die Citrix Gateways konfigurieren.
   - Anmeldetyp auf **Domäne** festlegen.
   - Geben Sie eine gültige Callback-URL an. Dies ist für die Entra ID-Authentifizierung mit StoreFront erforderlich.
3. Das Gateway für den Remotezugriff konfigurieren für den Store, der die Citrix DaaS-Ressourcen aggregiert.
4. Aktivieren und konfigurieren Sie die Entra ID-Authentifizierung vom NetScaler Gateway aus. Führen Sie das folgende PowerShell-Skript aus und ersetzen Sie dabei die Mandanten-ID durch die ID Ihres Entra ID-Mandanten und `/Citrix/EntraStore` durch den Store-Pfad.

```
$store = Get-STFStoreService /Citrix/EntraStore

$authenticationService = Get-STFAuthenticationService -Store $store

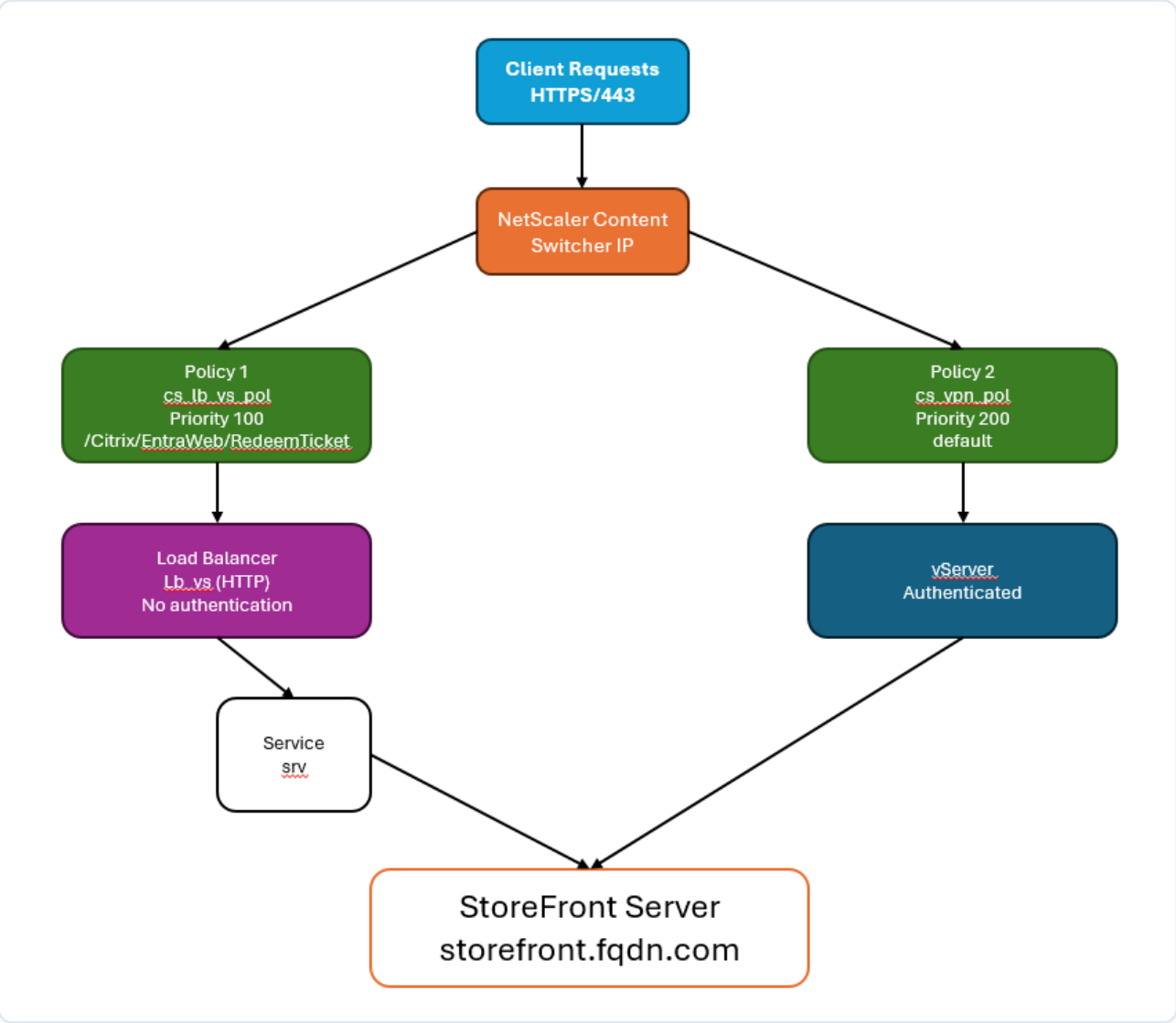
Set-STFEntraIdSettings -AuthenticationService $authenticationService
-TenantId "<Your tenant id>" -Enabled $true
```

Entra ID-SSO für VDAs konfigurieren

Sobald Sie StoreFront und Ihr Citrix Gateway für die Authentifizierung von Benutzern mit Entra ID konfiguriert haben, können Sie Entra ID SSO für VDAs ohne FAS aktivieren. Aktivieren Sie dies erst, nachdem Sie die DaaS-Konfiguration abgeschlossen haben. Weitere Informationen finden Sie unter Microsoft Entra Single Sign-On. Dies erfordert die folgende zusätzliche Konfiguration für StoreFront und den NetScaler ADC.

NetScaler ADC Content Switching konfigurieren

Normalerweise gehen alle Anfragen an StoreFront über den Gateway-VServer und erfordern daher eine Authentifizierung. Wenn der Benutzer einen Entra ID-verbundenen VDA startet, muss die Citrix Workspace-App sich erneut bei Azure authentifizieren (SSO, wenn die Entra ID-Sitzung noch gültig ist) und ein Zugriffstoken abrufen. Im Rahmen dieses Ablaufs generiert StoreFront ein Token, das von einem Dienst, der in Citrix Cloud ausgeführt wird, validiert werden muss. Dieser Dienst muss in der Lage sein, den StoreFront-Endpunkt `/Citrix/<StoreWeb>/Tickets/RedeemStoreTicket` aufzurufen, um das Token zu validieren. Da dieser Dienst keinen Zugriff auf die NetScaler-Sitzung hat, ist es notwendig, den VPN-Virtual-Service für Aufrufe zum Einlösen des Tickets zu umgehen. Um dies zu erreichen, können Sie einen Content Switcher verwenden.



Aufrufe an `/Citrix/<StoreWeb>/Tickets/RedeemStoreTicket` werden an einen Load Balancer geleitet, der die Anfragen an StoreFront weiterleitet und dabei das Gateway umgeht. Beachten Sie, dass der Load Balancer erforderlich ist, da der Content Switcher nicht so konfiguriert werden kann, dass er den Datenverkehr direkt an eine URL leitet, und einen virtuellen Server als Ziel benötigt. Der Load Balancer führt kein Load Balancing durch, sondern leitet den Datenverkehr lediglich an StoreFront weiter. Wenn Sie bereits einen geeigneten StoreFront-Load Balancer auf demselben Computer haben, können Sie diesen stattdessen verwenden.

Alle anderen Aufrufe werden an den VPN-Virtual-Server des Gateways geleitet.

Load Balancer für die Weiterleitung vom Content Switcher zu StoreFront erstellen

Wenn Sie bereits einen virtuellen Load-Balancer-Server vor Ihrer StoreFront-Servergruppe haben und dieser auf demselben Computer wie das Gateway ausgeführt wird, können Sie diesen Schritt überspringen und den Content Switch so konfigurieren, dass er den Datenverkehr direkt an diesen virtuellen Server sendet. Andernfalls müssen Sie einen Load Balancer erstellen, um den

Datenverkehr an die StoreFront-Server weiterzuleiten. Dies liegt daran, dass Content-Switcher-Aktionen auf einen virtuellen Server verweisen müssen.

Die Schritte unterscheiden sich geringfügig, je nachdem, ob StoreFront für HTTPS (empfohlen) oder HTTP konfiguriert ist.

STOREFRONT IST FÜR HTTPS KONFIGURIERT

Erstellen Sie einen Dienst `stf_srv`, der StoreFront über seine IP-Adresse darstellt, und binden Sie ihn an einen SSL-Load Balancer ohne Persistenz.

```
add service stf_srv <StoreFront Ip Address> SSL 443

add lb vserver lb_vs SSL <lb_vs Ip Address> 443 -persistenceType NONE
-cltTimeout 180

bind lb vserver lb_vs stf_srv
```

STOREFRONT IST FÜR HTTP KONFIGURIERT

Erstellen Sie einen Dienst `stf_srv`, der StoreFront über seinen FQDN darstellt, und binden Sie ihn an einen HTTP-Load Balancer ohne Persistenz.

```
add server storefront1 <storefront fqdn>

add service stf_srv storefront1 HTTP 80

add lb vserver lb_vs HTTP 0.0.0.0 0 -persistenceType NONE -cltTimeout 180

bind lb vserver lb_vs stf_srv
```

SSL Content Switching Virtual Server erstellen

Erstellen Sie einen SSL Content Switching Virtual Server, um Clientanfragen zu verarbeiten. Dieser Content Switching Virtual Server überwacht den HTTPS-Datenverkehr auf Port 443 und leitet Anfragen entweder an den VPN-Virtual-Server des Gateways oder über den Load Balancer an StoreFront weiter.

Standardmäßig ist das Content Switching deaktiviert, daher müssen Sie es aktivieren, falls Sie dies noch nicht getan haben.

```
enable feature CS

add cs vserver cs_vs SSL <cs_vs Ip Address> 443 -cltTimeout 180
-persistenceType NONE

bind ssl vserver cs_vs -certkeyName <Certificate Name>
```

Content Switching-Richtlinie für die Ticket-Einlösung erstellen

Erstellen Sie eine Content Switching-Richtlinie für den Lastausgleich basierend auf einer URL, die einen StoreFront-Ticket-Einlösungspfad enthält.

Diese Richtlinie gleicht Anfragen ab, wenn die URL `/Citrix/<StoreWeb>/Tickets/RedeemStoreTicket` enthält, und leitet sie an den Load Balancer weiter, ohne den VPN Virtual Server zu durchlaufen.

Ersetzen Sie `StoreEntraWeb` durch den Namen der StoreFront-Website aus der Webrichtlinie des StoreFront Virtual Servers. Sie können entweder den im vorherigen Schritt erstellten Load Balancer `lb_vs` oder einen vorhandenen Load Balancer Virtual Server verwenden, der Ihren StoreFront-Servern vorgeschaltet ist.

```
add cs action cs_lb_vs -targetLBVserver lb_vs

add cs policy cs_lb_vs_pol -rule "HTTP.REQ.URL.CONTAINS(\"/Citrix/
<StoreWeb>/Tickets/RedeemStoreTicket\")" -action cs_lb_vs

bind cs vserver cs_vs -policyName cs_lb_vs_pol -priority 100
```

Content Switching-Richtlinie für den gesamten anderen Datenverkehr erstellen

Erstellen Sie eine Catch-All-Content Switching-Richtlinie, um den gesamten anderen StoreFront-Datenverkehr zur Authentifizierung über den VPN Virtual Server zu senden.

```
add cs action cs_vpn_vs -targetVserver <VPN vServer>

add cs policy cs_vpn_pol -rule TRUE -action cs_vpn_vs

bind cs vserver cs_vs -policyName cs_vpn_pol -priority 110
```

VDA Entra ID Single Sign-On konfigurieren

Single Sign-On ermöglicht es Benutzern, sich einmal anzumelden, wenn sie sich bei Citrix Gateway anmelden, und dann auf ihre virtuellen Desktops und Anwendungen zuzugreifen, ohne ihre Anmeldeinformationen erneut beim VDA eingeben zu müssen.

```
$store = Get-STFStoreService /Citrix/EntraStore

Set-STFStoreLaunchOptions -StoreService $store -EntraIdSsoEnabled $true
```

Überlegungen zum Aktivieren oder Deaktivieren von Entra ID SSO

1. Aktivieren Sie Entra ID Single Sign-On erst, wenn Sie alle unter Microsoft Entra Single Sign-On beschriebenen Konfigurationen abgeschlossen haben. Andernfalls schlägt Single Sign-On fehl, und Benutzer können Startverzögerungen oder Fehler erfahren.

Endbenutzererfahrung

Endbenutzer können die Stores entweder in einem Webbrowser oder in der Citrix Workspace-App anzeigen. Siehe Endbenutzerzugriff.

StoreFront bietet die folgenden Benutzererfahrungen:

Moderne Erfahrung

Die moderne Benutzererfahrung ist konsistent mit Citrix Workspace. Sie umfasst den Activity Manager zur Verwaltung Ihrer Sitzungen und eine verbesserte Suchfunktion.

Die moderne Erfahrung weist die folgenden Einschränkungen auf:

- Es ist nicht möglich, eingebettete URL-Verknüpfungen zu erstellen, die Sie direkt zu Ihrer App oder Ihrem Desktop führen.
- Es ist nicht möglich, umfassende Anpassungen mithilfe von JavaScript und CSS mit der StoreFront™ Client UI Customization API vorzunehmen. Viele Anpassungen können jedoch mithilfe der Verwaltungskonsole vorgenommen werden, wodurch die Notwendigkeit von JavaScript oder CSS entfällt.

Weitere Informationen finden Sie unter Moderne Erfahrung

Klassische Erfahrung

Dies ist die Standard-Benutzererfahrung, die mit früheren Versionen von StoreFront konsistent ist. Sie können die Benutzeroberfläche mithilfe von JavaScript und CSS anpassen.

Weitere Informationen finden Sie unter Klassische Erfahrung

Citrix Gateway cVPN

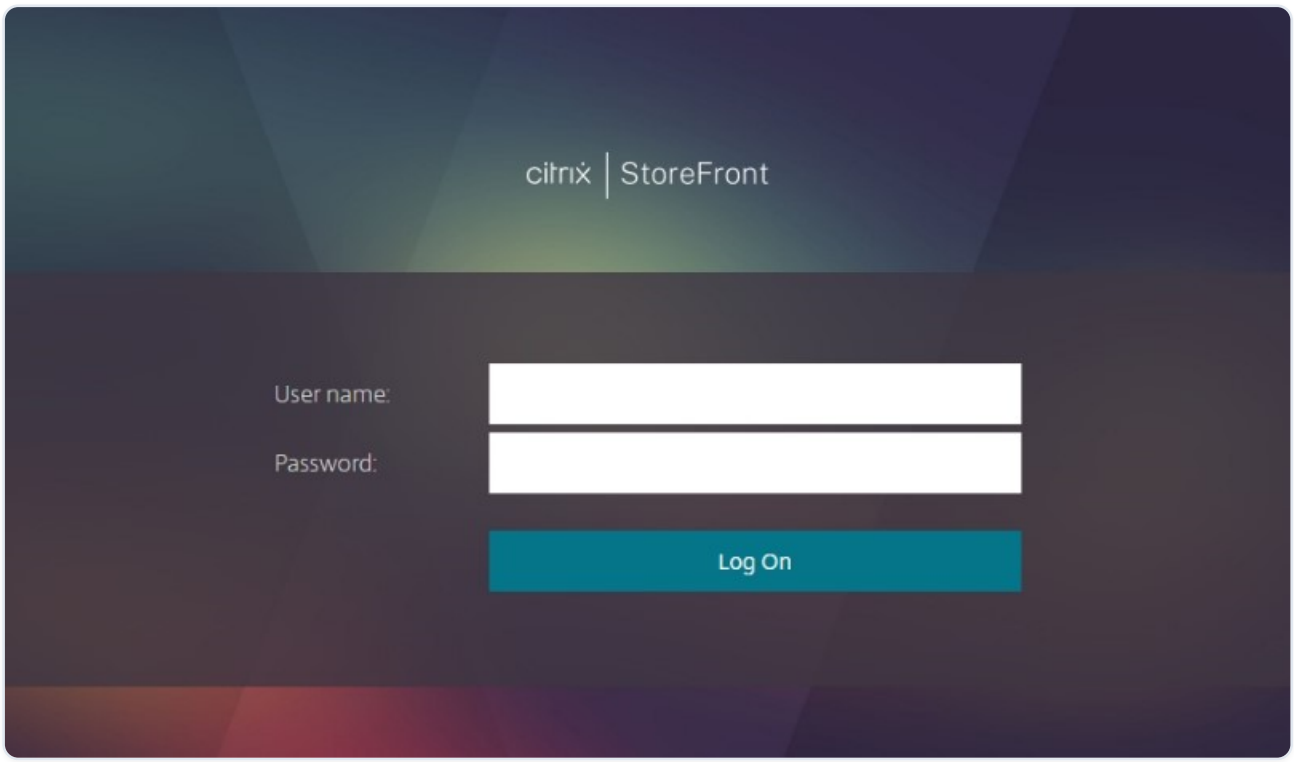
Wenn Benutzer über ein Citrix Gateway auf StoreFront zugreifen, das für clientloses VPN (CVPN) konfiguriert ist, dann stellt es eine eigene Benutzeroberfläche bereit, anstatt die Benutzeroberfläche von StoreFront anzuzeigen. In diesem Fall gelten einige UI-Konfigurationseinstellungen innerhalb von StoreFront nicht.

Klassische Erfahrung

Dieser Abschnitt beschreibt, wie Benutzer mithilfe der klassischen Erfahrung auf ihre Stores zugreifen und mit ihnen interagieren können.

Anmelden

Je nach den konfigurierten Authentifizierungsmethoden und ob Single Sign-On aktiviert ist, müssen sich Benutzer möglicherweise anmelden.



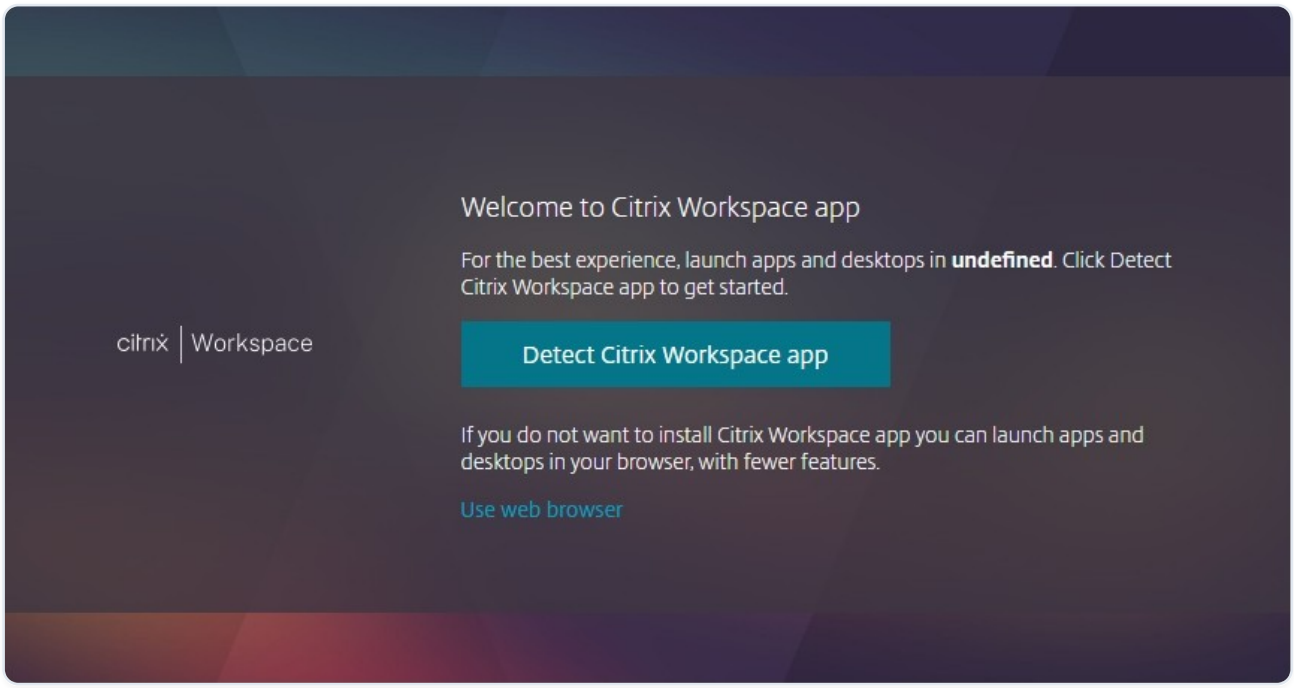
Wenn mehrere Authentifizierungsmethoden verfügbar sind, kann der Benutzer zu einer anderen Authentifizierungsmethode wechseln.

Erkennung der Citrix Workspace-App

> **Hinweis:**
>
> Dieser Abschnitt gilt nur, wenn der Store über einen Webbrowser aufgerufen wird und die Startoption auf **In Citrix Workspace-App öffnen** oder **Benutzer wählen lassen** festgelegt ist. Dieser Schritt kann je nach Konfiguration vor oder nach der Anmeldung erfolgen.

> Wenn die Citrix Web Extension installiert ist und die Citrix Workspace-App erkannt hat oder der Citrix Workspace Launcher deaktiviert ist, wird dieser Schritt übersprungen. Benutzer können stattdessen die Startpräferenz in den Erweiterten Einstellungen ändern.

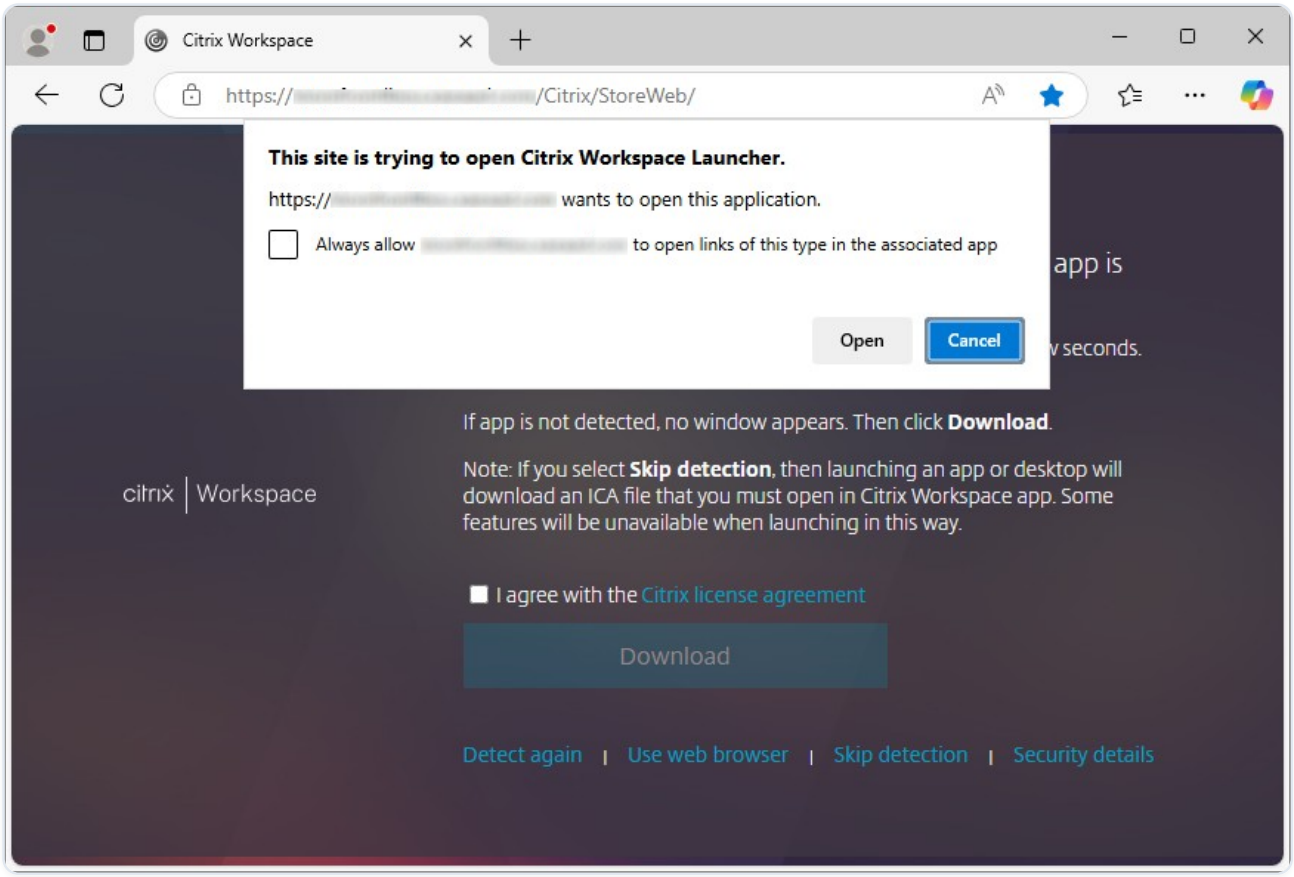
> Wenn der Benutzer zum ersten Mal oder nach dem Löschen seiner Cookies über einen Webbrowser auf den Store zugreift, wird der Bildschirm **Willkommen bei der Citrix Workspace-App** angezeigt.



Sie können entweder:

- Wählen Sie **Citrix Workspace-App erkennen**, um Ressourcen in der lokal installierten Citrix Workspace-App zu starten. Dies wird für die beste Erfahrung empfohlen.
- Wählen Sie **Webbrowser verwenden**, um Ressourcen immer im Browser zu starten. Diese Option ist nur verfügbar, wenn die Startoption auf **Benutzer wählen lassen** festgelegt ist.

Wenn der Benutzer **Citrix Workspace-App erkennen** auswählt, wird versucht, den **Citrix Workspace Launcher** zu öffnen, der eine Komponente der Citrix Workspace-App ist. Wenn die Citrix Workspace-App installiert ist, öffnet der Browser ein Fenster, in dem gefragt wird, ob der **Citrix Workspace Launcher** ausgeführt werden soll. Sie sollten **Citrix Workspace Launcher öffnen**, **Link öffnen**, **Öffnen** oder **Immer öffnen** auswählen (je nach Browser). Es wird empfohlen, dass sie auch **Immer zulassen, dass *Domäne* Links dieses Typs in der zugehörigen App öffnet** (oder Ähnliches, je nach Browser) auswählen, um zu vermeiden, dass dieses Fenster jedes Mal angezeigt wird, wenn sie eine Ressource starten.



Wenn eine lokal installierte Citrix Workspace-App erkannt wird, wird nach einigen Sekunden der nächste Bildschirm angezeigt. Wenn der Benutzer anschließend eine Ressource startet, wird diese entweder mit Citrix Web Extensions oder dem Citrix Workspace Launcher (je nachdem, was erkannt wurde) in der lokal installierten Citrix Workspace-App geöffnet.

Wenn die Citrix Workspace-App nicht installiert ist oder der Benutzer den Launcher abbricht, stehen ihm je nach Konfiguration die folgenden Optionen zur Verfügung:

- **Download** – Lädt die Citrix Workspace-App von der Citrix-Website oder vom StoreFront-Server herunter. Um diese Option auszublenden, siehe Benutzern das Herunterladen der Citrix Workspace-App erlauben.
- **Erneut erkennen** – Versucht, die lokal installierte Citrix Workspace-App erneut zu erkennen.
- **Webbrowser verwenden** – Überspringt die Erkennung der Workspace-App und öffnet Ressourcen immer im Webbrowser. Um diese Option anzuzeigen, setzen Sie die Startoption auf **Benutzer wählen lassen**.
- **Erkennung überspringen** – Benutzer können diese Option verwenden, wenn sie eine ältere Version von Citrix Receiver installiert haben, die den Citrix Workspace Launcher oder Citrix Web-Erweiterungen nicht unterstützt. Wenn sie diese Option auswählen, lädt ihr Browser beim Starten einer virtuellen App oder eines Desktops eine Datei **launch.ica** herunter, die sie mit

Citrix Receiver öffnen können. Diese Option führt zu reduzierter Funktionalität und Sicherheit, daher wird Administratoren empfohlen, diese Option zu deaktivieren.

Start-Tab

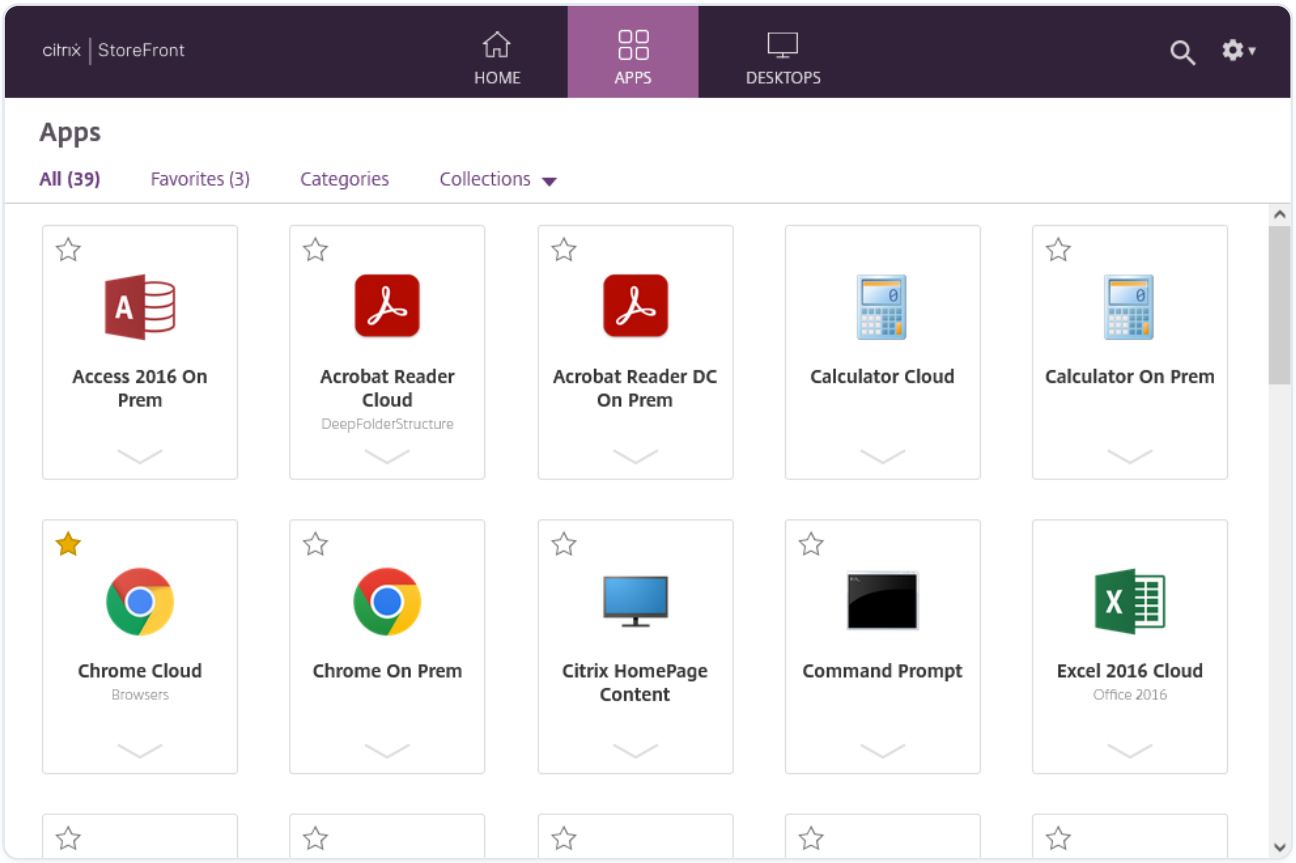
Die Registerkarte **Startseite** zeigt alle hervorgehobenen App-Gruppen zusammen mit allen bevorzugten oder obligatorischen Apps und Desktops an. Die Registerkarte **Startseite** wird nur angezeigt, wenn Favoriten für den Store aktiviert sind.



Registerkarte Apps

Die Registerkarte **Apps** verfügt über eine Reihe von Unteransichten:

- **Alle** – zeigt alle Apps an.
- **Favoriten** – Zeigt alle bevorzugten Apps an.
- **Kategorien** – Zeigt Kategorien und die Apps innerhalb dieser Kategorien an. Die Art und Weise, wie Kategorien angezeigt werden, hängt von den Kategorieeinstellungen ab.
- **Sammlungen** Zeigt die Hervorgehobenen App-Gruppen an.



.

Registerkarte Desktops

Die Registerkarte **Desktops** verfügt über zwei Unteransichten:

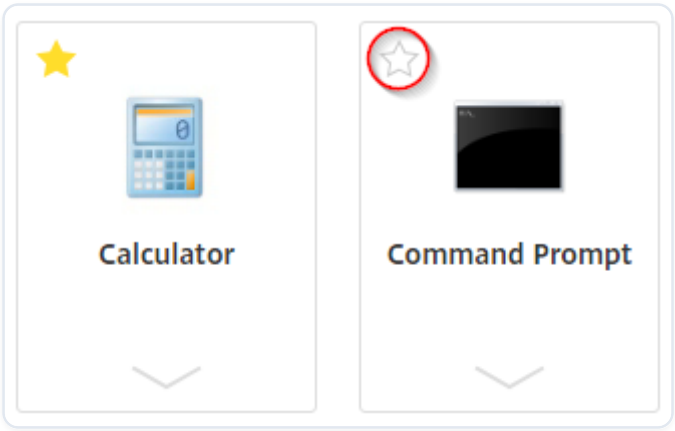
- **Alle** – Zeigt alle Desktops an.
- **Favoriten** – Zeigt die bevorzugten Desktops des Benutzers an.

App- und Desktop-Kacheln

Klicken Sie auf ein Symbol, um die App oder den Desktop zu starten.

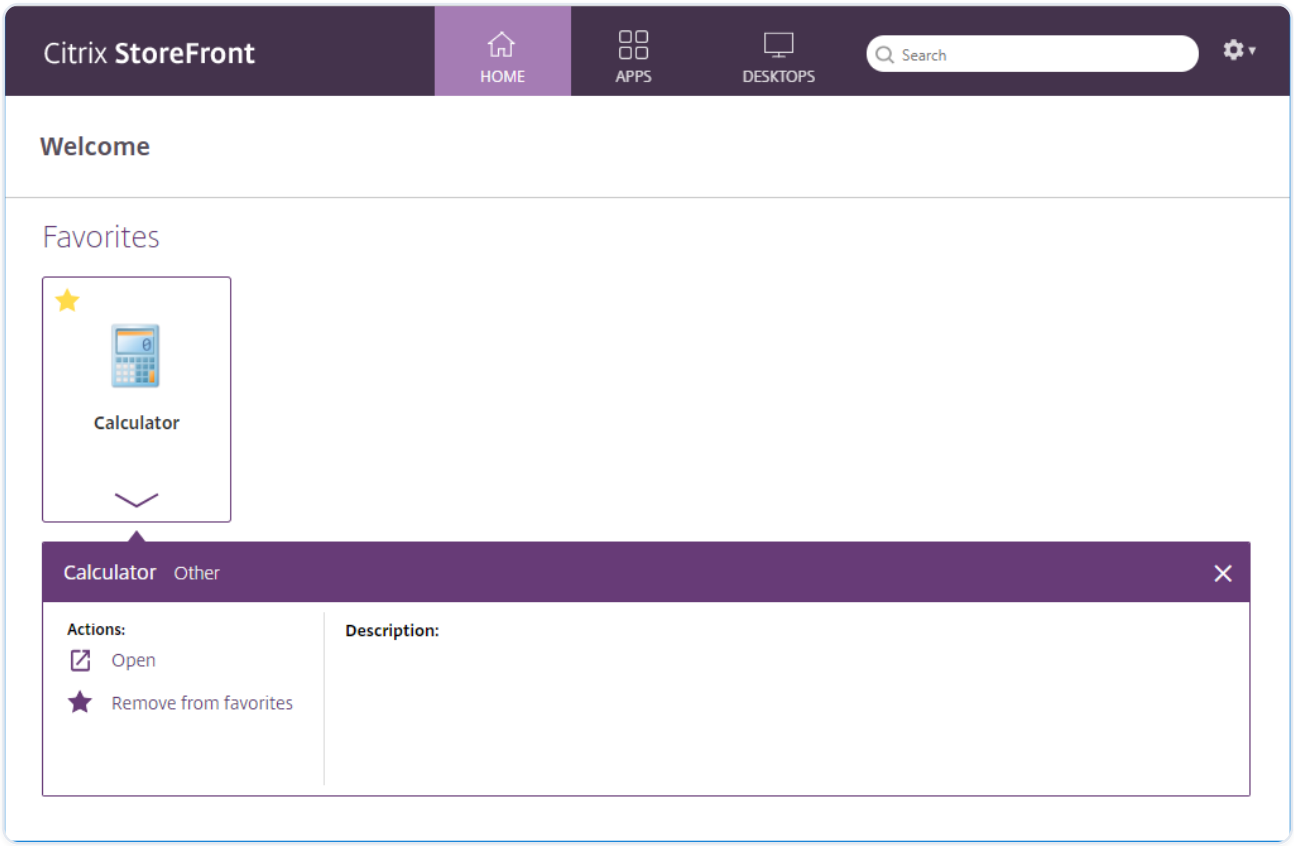
Favoriten

Wenn Favoriten aktiviert sind, kann der Benutzer auf einer Kachel einer Ressource den Stern auswählen, um sie zu einem Favoriten zu machen:



Details und Aktionen anzeigen

Der Benutzer kann unter jedem Symbol ein Panel erweiternieren, um die App-Beschreibung und Aktionen anzuzeigen.



Die folgenden Aktionen sind möglicherweise verfügbar:

- **Öffnen** – Startet die App oder den Desktop oder stellt die Verbindung wieder her.
- **Zu Favoriten hinzufügen** – Wenn das Element kein Favorit und nicht obligatorisch ist und Favoriten für den Store aktiviert sind, wird die App oder der Desktop zu einem Favoriten gemacht.

- **Aus Favoriten entfernen** – Wenn das Element ein Favorit und nicht obligatorisch ist und Favoriten für den Store aktiviert sind, wird die App oder der Desktop aus den Favoriten entfernt.
- **Neustart** – Für zugewiesene Desktops, bei denen ein Neustart verfügbar ist, wird der Desktop neu gestartet.

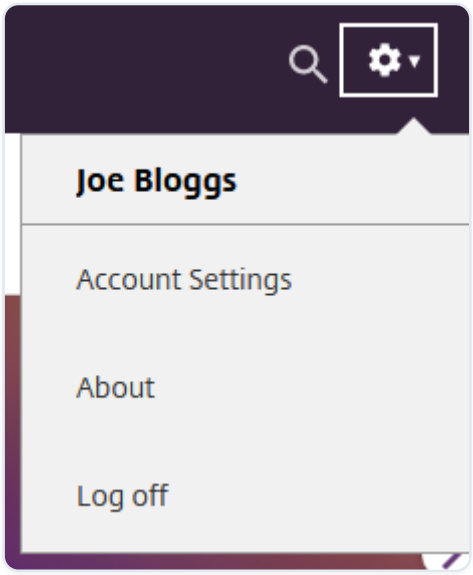
Suche

Benutzer können das Lupensymbol auswählen, um das Suchfeld aufzurufen. Suchen Sie über alle Apps, Desktops und Kategorien hinweg:



Einstellungen-Menü

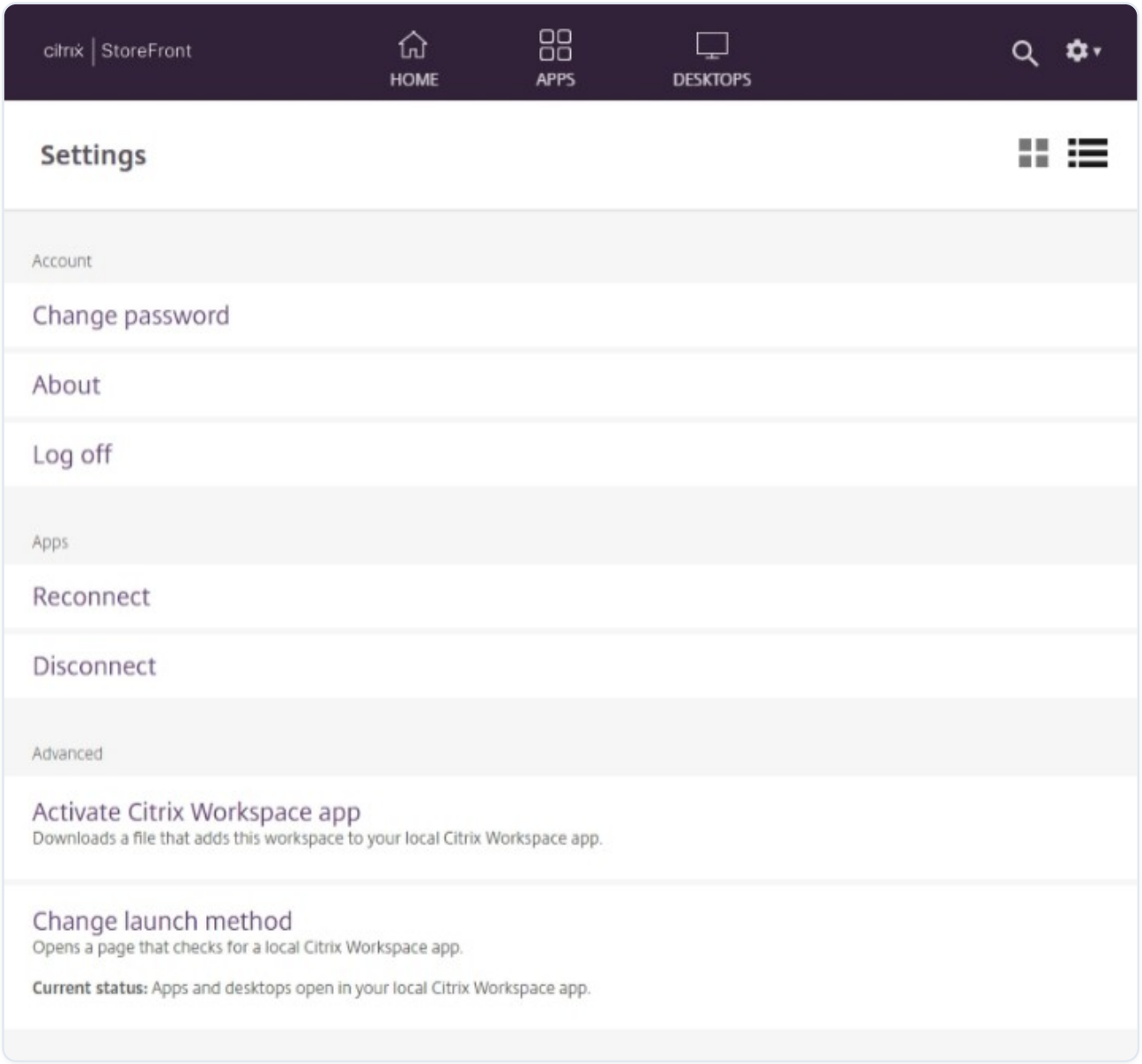
Das Einstellungen-Menü ist nur verfügbar, wenn Sie den Store über einen Webbrowser aufrufen.



Das Einstellungen-Menü bietet die folgenden Optionen:

- **Kontoeinstellungen** – öffnet die Seite Einstellungen.
- **Info** – Zeigt Informationen zur Anwendung an.
- **Abmelden** – Meldet sich von der Website ab.

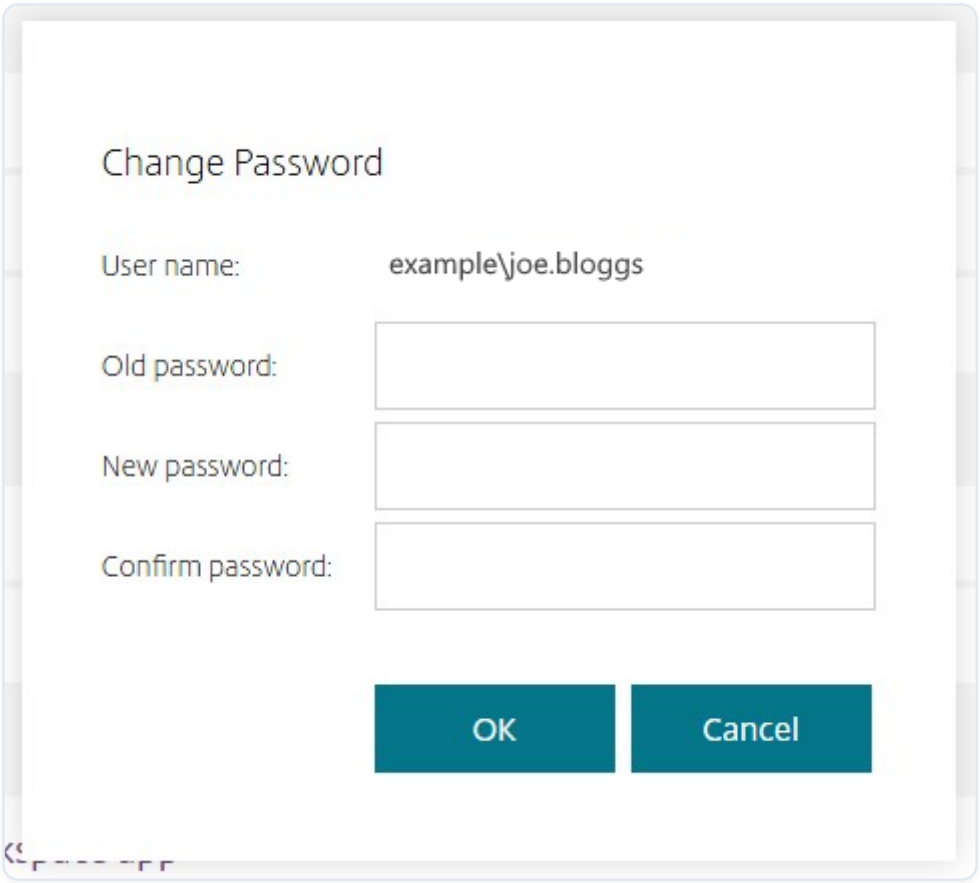
Einstellungen



Die Seite mit den Kontoeinstellungen kann die folgenden Abschnitte enthalten.

Konto

Passwort ändern. Nur bei Verwendung der Benutzername- und Passwort-Authentifizierung. Informationen zum Konfigurieren der Anzeige dieser Option finden Sie unter Benutzername und Passwort.



Info. Bietet Links zu Hinweisen Dritter.

Abmelden. Meldet den Benutzer ab.

Apps

Verbinden. Setzt alle getrennten Sitzungen fort. Informationen zum Konfigurieren der Anzeige dieser Option finden Sie unter Workspace Control.

trennen. Trennt alle aktuellen Sitzungen und meldet sich ab. Informationen zum Konfigurieren der Anzeige dieser Option finden Sie unter Workspace Control.

Erweitert

Citrix Workspace-App aktivieren. Lädt eine Datei herunter, die diesen Store zur lokalen Citrix Workspace-App hinzufügt. Informationen zum Konfigurieren der Anzeige dieser Option finden Sie unter Benutzeroberflächeneinstellungen.

Startmethode ändern. Öffnet eine Seite, die nach einer lokal installierten Citrix Workspace-App sucht. Dies ermöglicht Benutzern auch, zwischen dem Starten von Ressourcen mit der lokal installierten Citrix Workspace-App und dem Starten in einem Webbrowser zu wechseln.

Abmelden

Um sich abzumelden, öffnen Sie das Einstellungsmenü und klicken Sie auf **Abmelden**. Dadurch wird der Benutzer vom Store abgemeldet. Wenn sie mit Ressourcen verbunden sind, wird je nach Konfiguration entweder:

- Die Ressourcen beenden.
- trennen von den Ressourcen
- Die Ressourcen verbunden lassen.

Installation als Progressive Web App (Vorschau)

Wenn der Administrator Progressive Web App aktiviert hat, können Benutzer die Store-Website als Progressive Web App installieren.

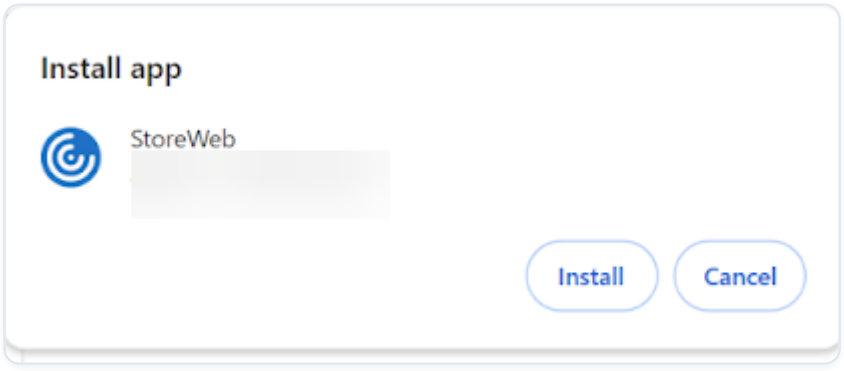
Progressive Web App mit Google Chrome installieren

Benutzer können die Store-Website wie folgt installieren:

1. Öffnen Sie den Store im Google Chrome-Browser.
2. Wählen Sie das folgende Symbol in der Symbolleiste aus:

   Die Option zur Installation der PWA wird angezeigt.

3. Wählen Sie **Installieren**, um den Store zum Desktop und Startmenü hinzuzufügen:

Wenn der Benutzer mehrere StoreFront™ Stores hat, kann er jede Store-Website separat installieren. Jede Installation erstellt eine Verknüpfung mit dem Namen `<Store website name>`, die bei Bedarf umbenannt werden kann.

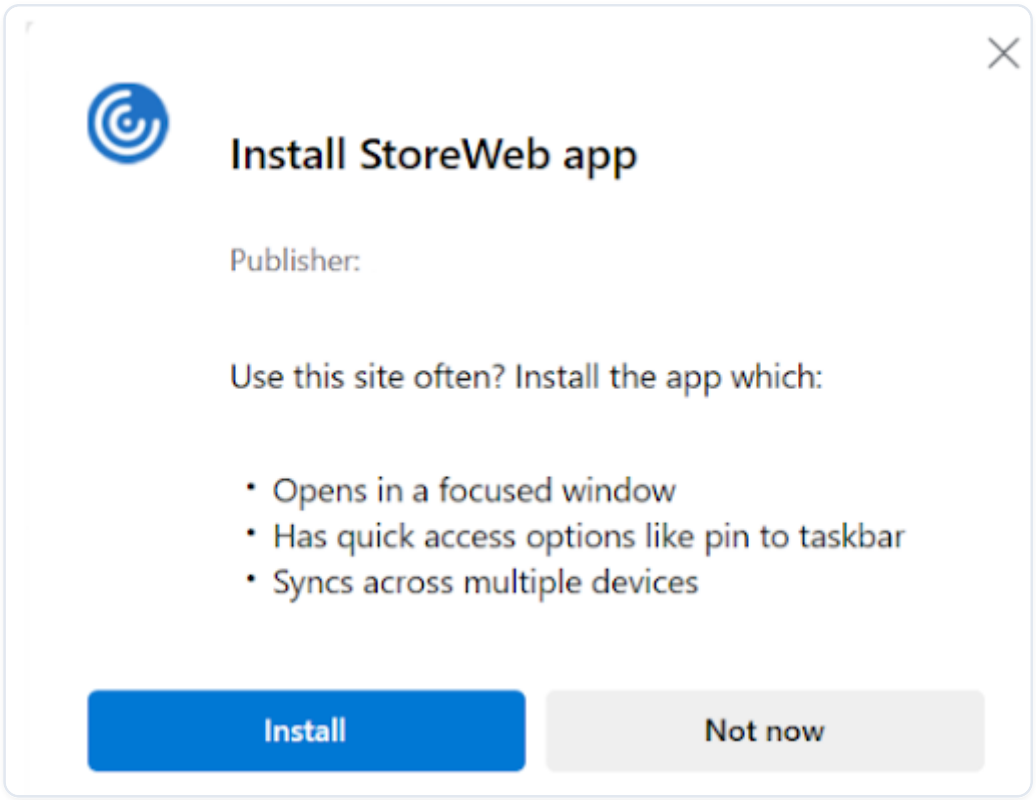
Progressive Web App mit Microsoft Edge installieren

Benutzer können die Store-Website wie folgt installieren:

1. Öffnen Sie den Store im Microsoft Edge-Browser.
2. Wählen Sie das folgende Symbol in der Symbolleiste:

   Die Option zur Installation wird angezeigt.

3. Wählen Sie **Installieren**, um den Store zum Desktop und Startmenü hinzuzufügen:

   Wenn der Benutzer mehrere StoreFront Stores hat, kann er jede Store-Website separat installieren. Jede Installation erstellt eine Verknüpfung mit dem Namen `<Store website name>`, die bei Bedarf umbenannt werden kann.

Moderne Benutzeroberfläche

Dieser Abschnitt beschreibt, wie Benutzer mithilfe der modernen Benutzeroberfläche auf ihre Stores zugreifen und mit ihnen interagieren können. Die moderne Benutzeroberfläche ist standardmäßig nicht aktiviert. Informationen zum Aktivieren finden Sie unter UI experience.

Erforderlicher Bildschirm der Citrix Workspace-App

Wenn der Benutzer den Store im Webbrowser öffnet, der Store aber so konfiguriert ist, dass die Citrix Workspace-App erforderlich ist, wird der Benutzer angewiesen, die Citrix Workspace-App zu installieren und zu konfigurieren. Weitere Informationen finden Sie unter Citrix Workspace-App erforderlich.

Erkennung der Citrix Workspace-App

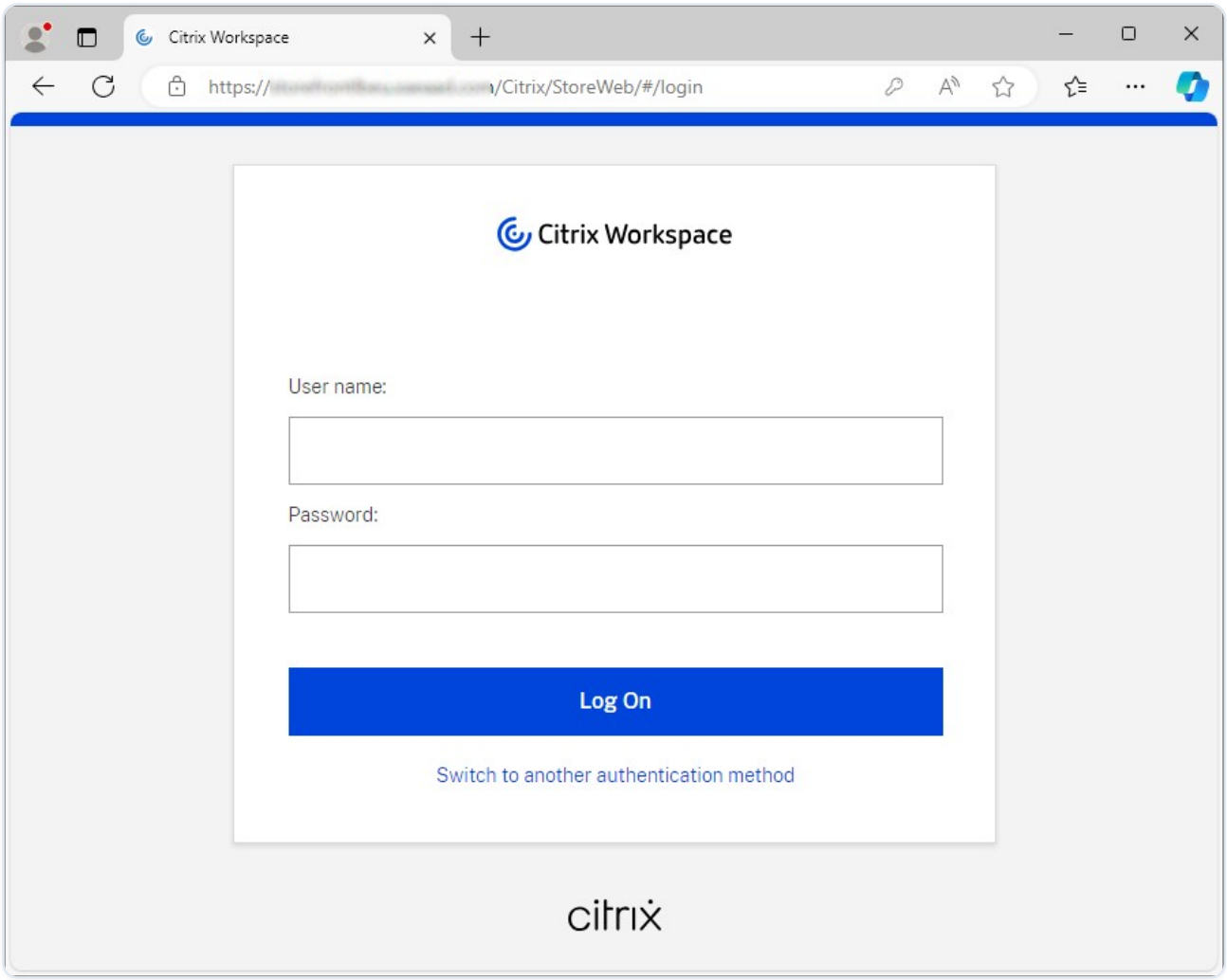
Wenn der Benutzer den Store zum ersten Mal in einem Webbrowser öffnet oder nachdem Cookies gelöscht wurden, wird auf der Webseite möglicherweise der Bildschirm **Willkommen bei der Citrix Workspace-App** angezeigt, der den Benutzer auffordert, die Citrix Workspace-App zu erkennen. Dieser Schritt kann je nach Konfiguration vor oder nach der Anmeldung erfolgen. Weitere Informationen finden Sie unter Citrix Workspace app detection-Bildschirm.

Wenn Benutzer sich am NetScaler Gateway authentifizieren, wird dieser Bildschirm nach der Authentifizierung angezeigt. Wenn Benutzer sich direkt bei StoreFront authentifizieren, wird dieser Bildschirm normalerweise vor der Authentifizierung angezeigt, es sei denn, Sie haben prompt to install Citrix Workspace app after logon konfiguriert.

Wenn die Citrix Web Extension installiert ist und die Citrix Workspace-App erkannt hat, wird dieser Schritt übersprungen und standardmäßig in der Citrix Workspace-App gestartet. Benutzer können die Startmethode auf der Seite Einstellungen ändern.

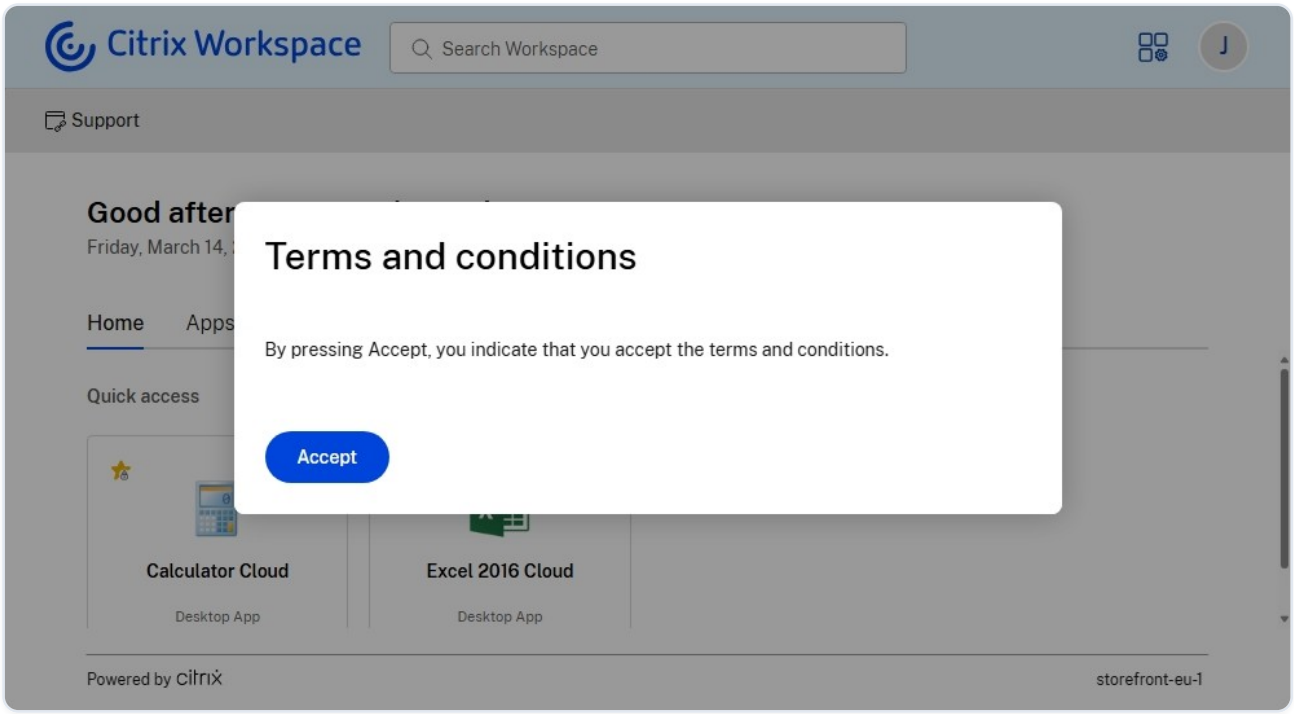
Authentifizierung

Je nach den konfigurierten authentication methods und ob Single Sign-On aktiviert ist, müssen sich Benutzer möglicherweise anmelden.



Wenn mehrere Authentifizierungsmethoden verfügbar sind, kann der Benutzer zu einer anderen Authentifizierungsmethode wechseln.

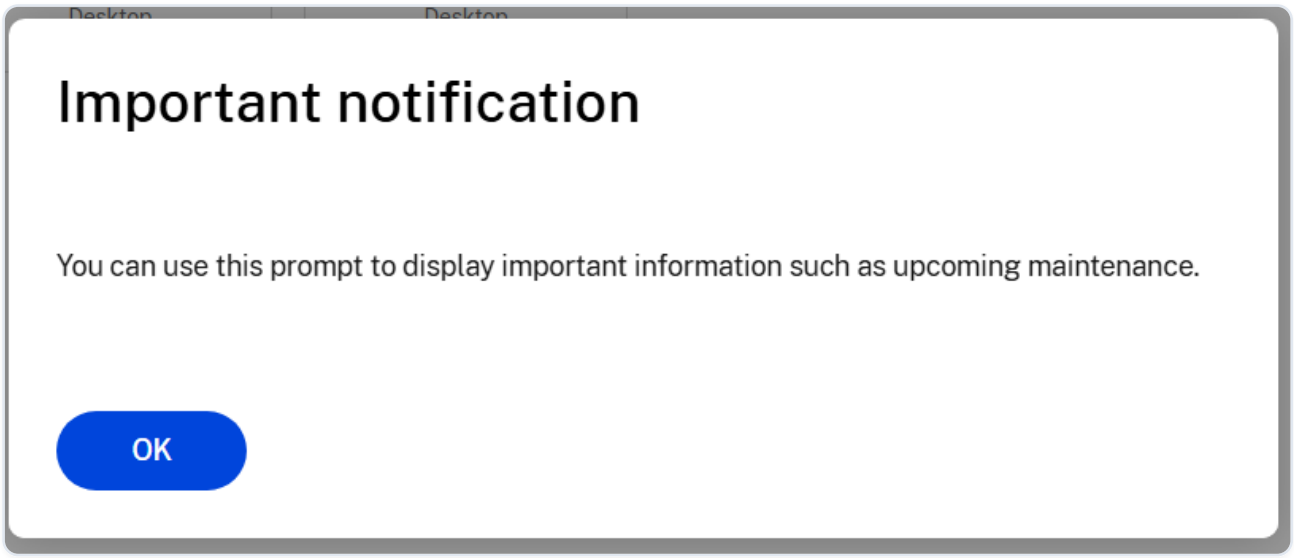
Nach der Anmeldung wird Benutzern, falls configured, möglicherweise eine Meldung angezeigt, die sie akzeptieren müssen, um fortzufahren.



Weitere Informationen zum Konfigurieren finden Sie unter Dialog after login.

Dialogfeld nach der Anmeldung

Dem Benutzer wird möglicherweise ein Dialogfeld angezeigt. Weitere Informationen finden Sie unter Configure a custom dialog to be displayed after log in.



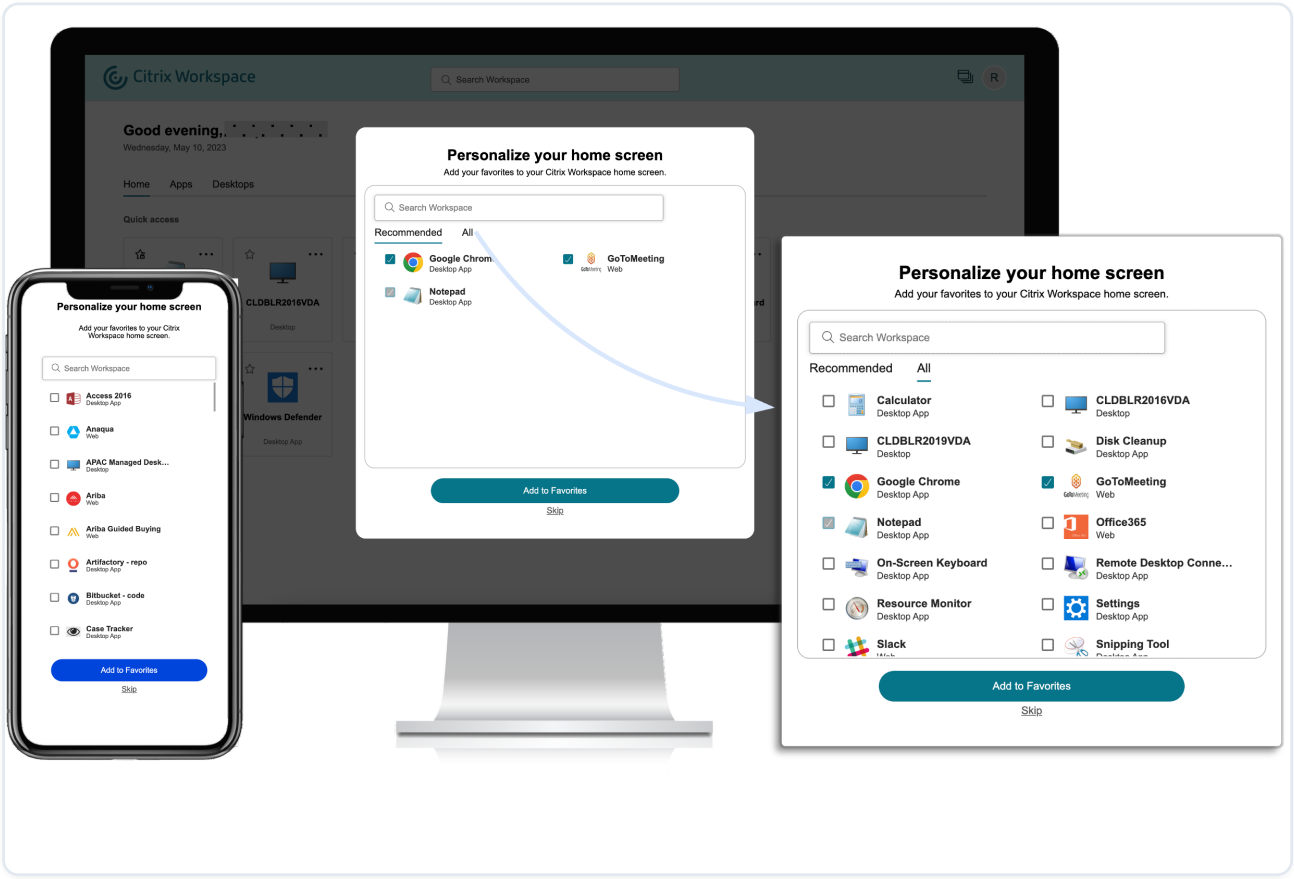
Der Benutzer muss die Meldung akzeptieren, bevor er auf seine Ressourcen zugreifen kann. Sie können konfigurieren, wie oft die Meldung angezeigt wird.

Benutzererfahrung bei der ersten Anmeldung

Beim erstmaligen Zugriff auf die Benutzeroberfläche wird den Benutzern ein Pop-up angezeigt, in dem sie mehrere Apps in einem einfachen Schritt als Favoriten markieren können.

Die Erstanwendererfahrung wird aktiviert, wenn Benutzer mehr als 20 Apps haben und noch keine davon zu den Favoriten hinzugefügt haben. Die Erfahrung wird auf allen Browsern und nativen Clients (Mac, Windows, Linux und ChromeOS) sowie auf Mobilgeräten (iOS und Android) unterstützt. Informationen zum Konfigurieren, ob dieses Fenster angezeigt wird, finden Sie unter Display Personalize your home screen for first time users.

Die empfohlenen oder obligatorischen Apps werden auf der Registerkarte **Empfohlen** des Erstanwenderbildschirms angezeigt, wie von Administratoren in der DaaS-Konsole für Citrix Virtual Apps and Desktops™ und in der Secure Private Access-Konsole für Web- und SaaS-Apps festgelegt. Obligatorische Apps sind standardmäßig ausgewählt und die Überprüfung ist deaktiviert. **Empfohlene** und automatisch favorisierte Apps sind standardmäßig ausgewählt und die Überprüfung ist für Benutzer aktiviert. Endbenutzer können auch andere Apps auswählen, um sie zu den Favoriten hinzuzufügen. Alle ausgewählten Apps werden automatisch zu den Favoriten hinzugefügt und auf der Startseite angezeigt.



Einschränkungen

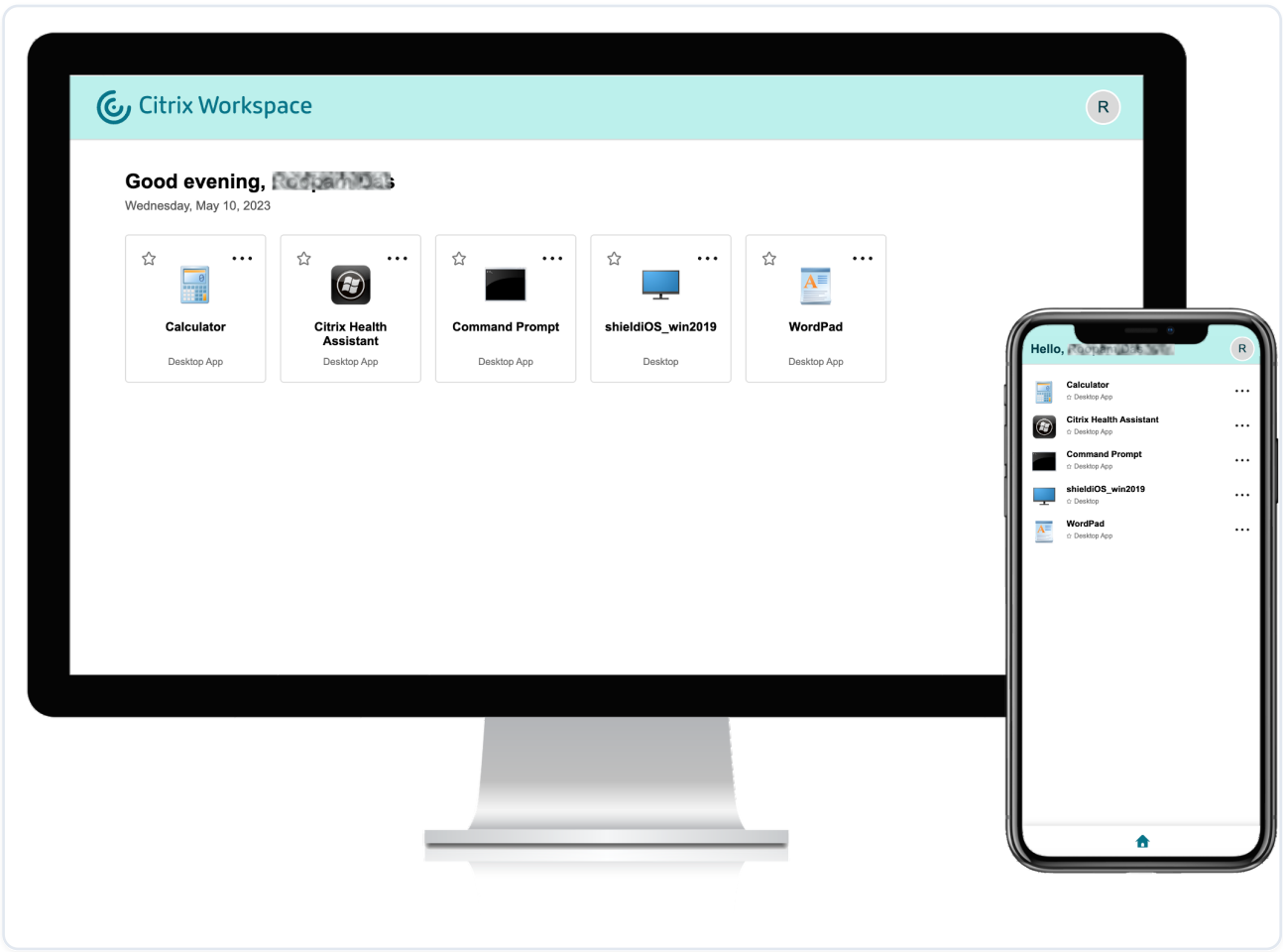
- Der Bildschirm **Personalisierung** wird einmal pro Gerät und Browser angezeigt, und jedes Mal im Inkognito-Modus, es sei denn, Benutzer markieren einen Favoriten.
- Wenn der Administrator das obligatorische oder empfohlene Tag von den Apps entfernt, hat dies keine Auswirkungen auf die Apps in den **Favoriten**.

- Wenn der Endbenutzer keine Apps zu den **Favoriten** hinzugefügt hat, wird der Bildschirm **Personalisierung** jedes Mal angezeigt, wenn die Workspace-App geöffnet wird. Um dies zu vermeiden:
  - Endbenutzer können eine oder mehrere Apps zu den **Favoriten** hinzufügen. Dies verhindert, dass der Personalisierungsbildschirm jedes Mal angezeigt wird, wenn sie die App starten.
  - Administratoren können eine oder mehrere Apps zu den Favoriten hinzufügen. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops configuration.

Navigationsregisterkarten

Einfache Ansicht

Wenn Benutzer weniger als 20 Ressourcen haben, landen sie standardmäßig auf dem Bildschirm mit der einfachen Ansicht, der keine Registerkarten oder Kategorien enthält. Alle Apps und Desktops erscheinen auf derselben Seite. Auf diesem Bildschirm werden zuerst ihre Favoriten angezeigt, gefolgt von allen anderen Apps in alphabetischer Reihenfolge.



Sie können den Store so konfigurieren, dass Navigationsregisterkarten immer angezeigt werden, wodurch die einfache Ansicht deaktiviert wird.

Vollansicht

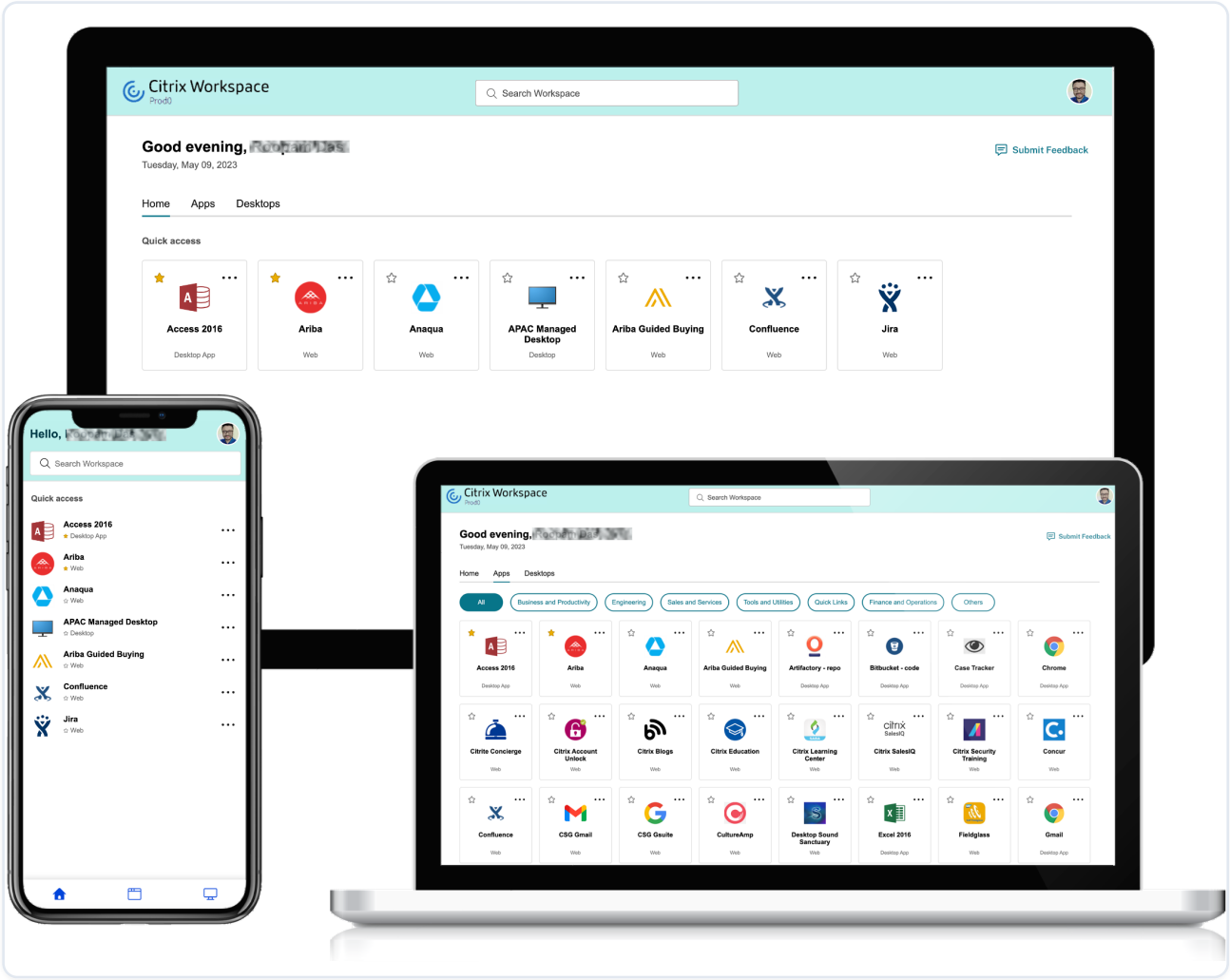
Wenn Benutzer mehr als 20 Ressourcen haben oder die Store-Website so konfiguriert ist, dass Navigationsregisterkarten immer angezeigt werden, werden bis zu drei Registerkarten angezeigt – **Startseite**, **Apps** und **Desktops**. Standardmäßig landen Benutzer beim Anmelden auf der Registerkarte **Startseite**, falls diese vorhanden ist, andernfalls auf der Registerkarte **Apps**. Sie können (/de-de/storefront/2507-ltsr/stores/websites/client-interface-settings.html#navigation-tabs) konfigurieren, ob die Startseite und die Standardregisterkarte angezeigt werden.

Start-Tab

Auf der Registerkarte Startseite werden zuerst obligatorische und bevorzugte Apps angezeigt, gefolgt von den fünf zuletzt verwendeten Apps. Die Sternsymbole für die **obligatorischen** Apps sind gesperrt, und Benutzer können sie nicht aus den Favoriten entfernen.

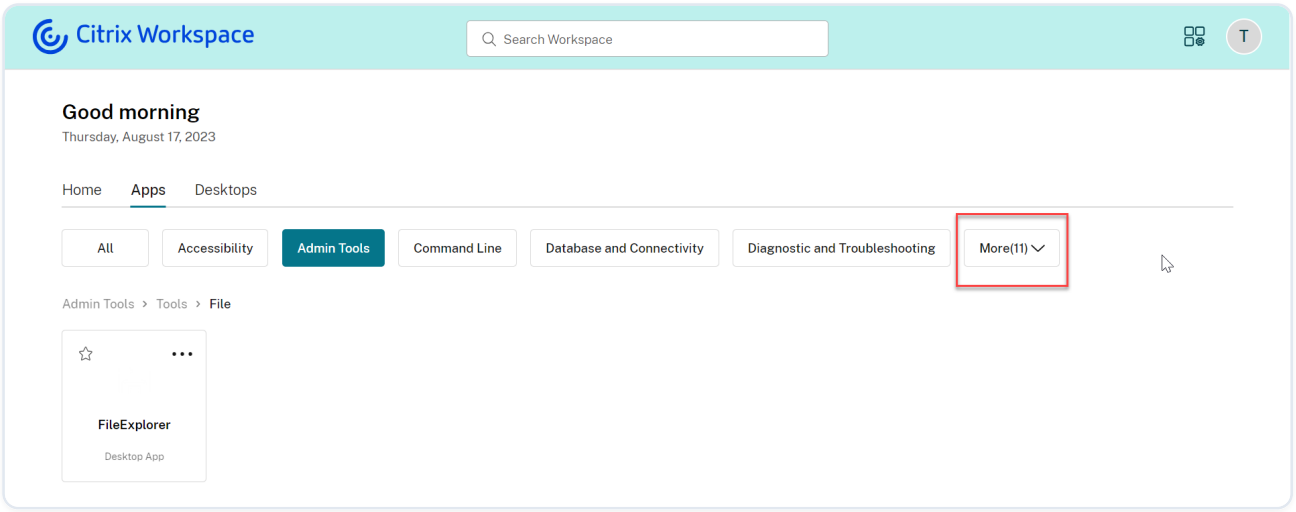
Registerkarte Apps

Auf der Registerkarte **Apps** werden zuerst Favoriten angezeigt, gefolgt von allen anderen Apps in alphabetischer Reihenfolge. Wenn der Administrator Kategorien erstellt und die Apps diesen zugewiesen hat, werden die verschiedenen Kategorien angezeigt, und Benutzer können die Kategorie der Apps auswählen, die sie anzeigen möchten.

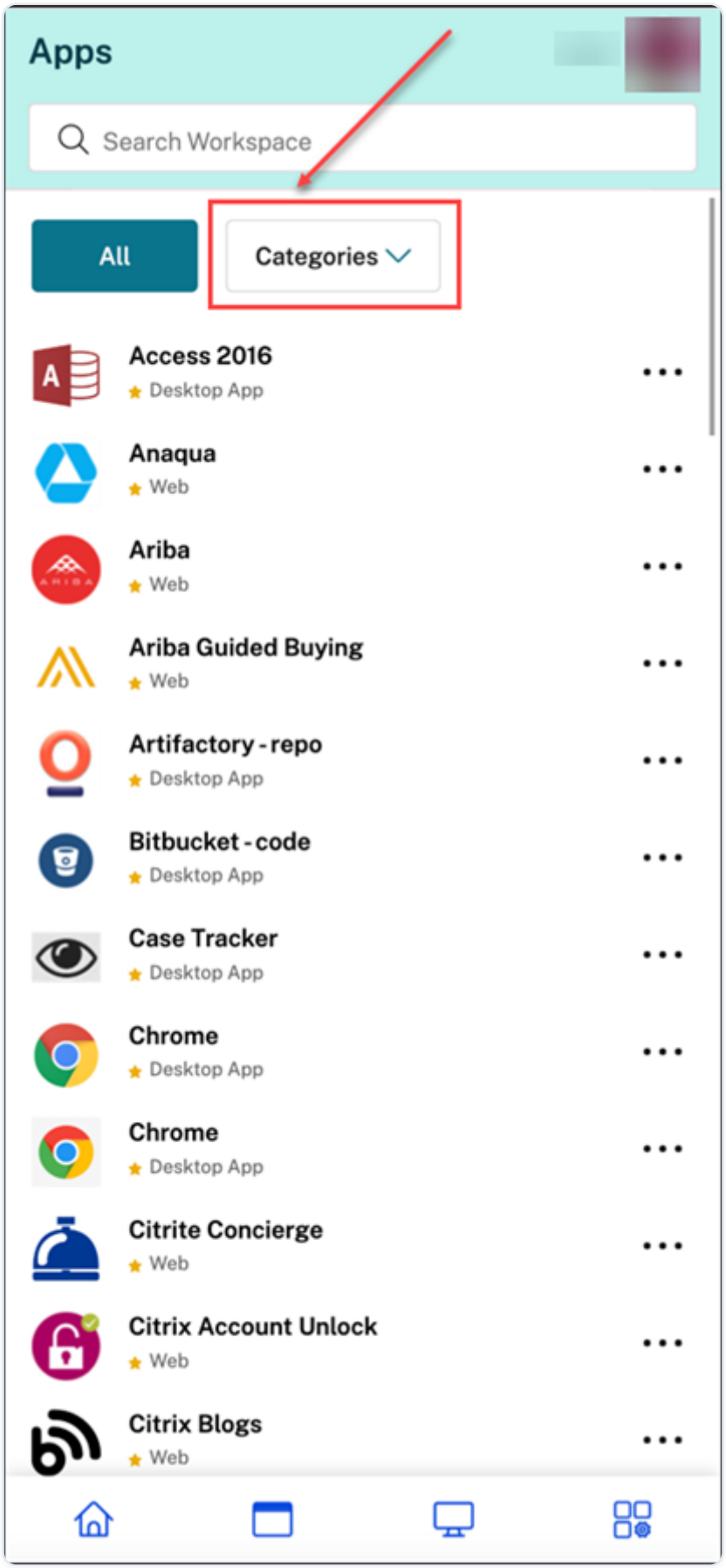


Für jede Anwendung können Sie eine Kategorie definieren. Die Kategorie stellt die Ordnerstruktur dar, die Endbenutzern auf dem Bildschirm angezeigt wird. Betrachten Sie beispielsweise eine App, für die der Ordner als `Optimisation tools/Cleaning` definiert ist. Um auf diese App zuzugreifen, müssen Endbenutzer nun zu Optimisation tools > Cleaning navigieren, wobei Optimisation tools eine Kategorie und Cleaning eine Unterkategorie ist. Weitere Informationen zum Konfigurieren von Kategorien finden Sie unter Anwendungen.

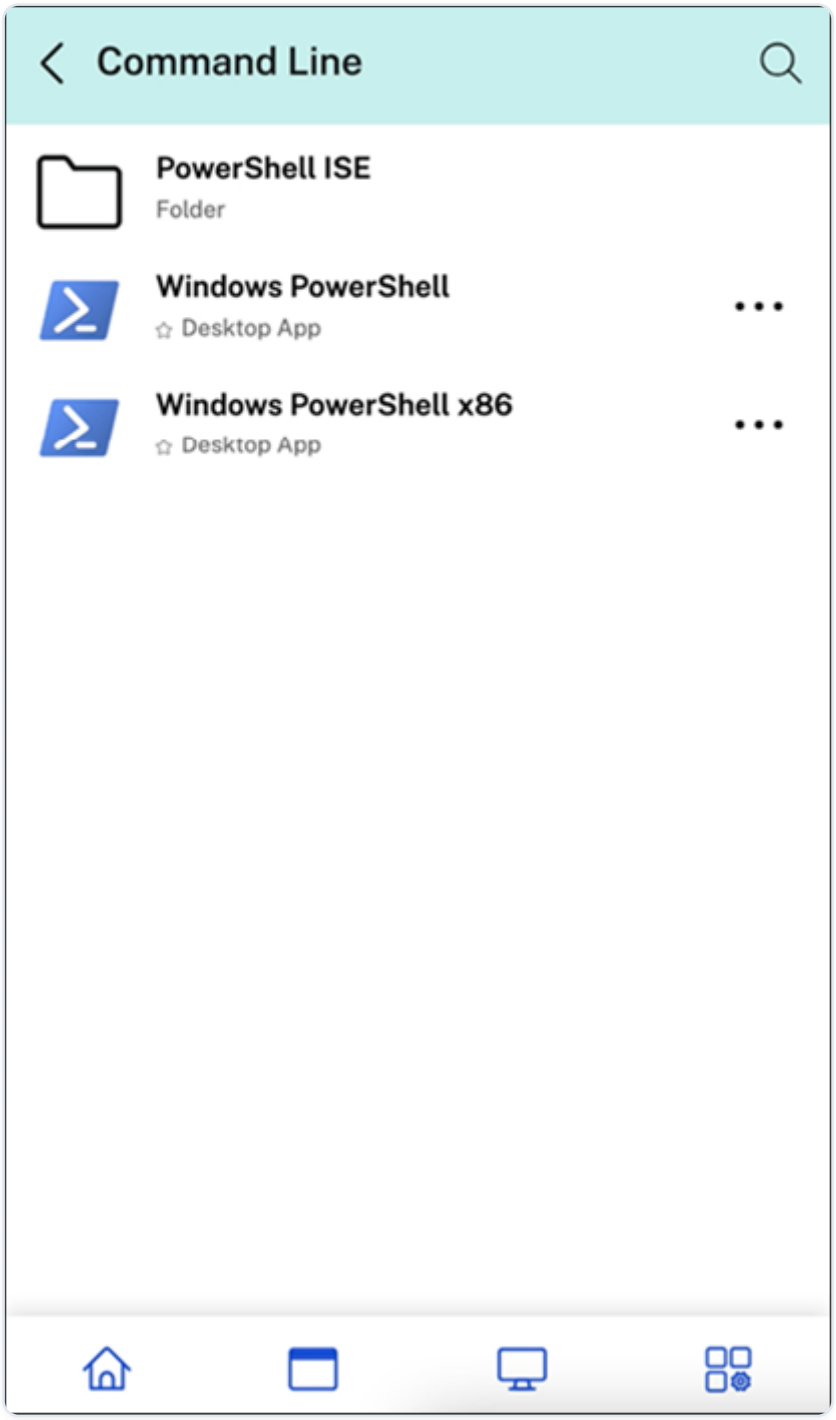
Wenn die Anzahl der vom Administrator erstellten primären Kategorien den verfügbaren Platz auf dem Bildschirm des Benutzers überschreitet, passt sich die Benutzeroberfläche an die Bildschirmgröße an und verschiebt Kategorien dynamisch unter das Dropdown-Menü **Mehr**. Die Navigationspfade werden den Benutzern ebenfalls angezeigt.



Navigieren Sie auf mobilen Plattformen zur Registerkarte Apps und klicken Sie auf das Dropdown-Menü **Kategorien**, um eine Liste der verfügbaren Kategorien anzuzeigen. Unterkategorien werden als Ordner angezeigt, die je nach Administratorkonfiguration weitere Unterordner oder Anwendungen enthalten können.



Wählen Sie die entsprechende Kategorie aus; eine Liste der verfügbaren Unterkategorien und Anwendungen wird basierend auf der vom Administrator vorgenommenen Konfiguration angezeigt.



Registerkarte Desktops

Der Reiter **Desktops** zeigt alle verfügbaren virtuellen Desktops an.

Bevorzugte und obligatorische Apps

Standardmäßig können Benutzer Favoriten erstellen und entfernen, indem sie das Sternsymbol auf der Kachel auswählen.

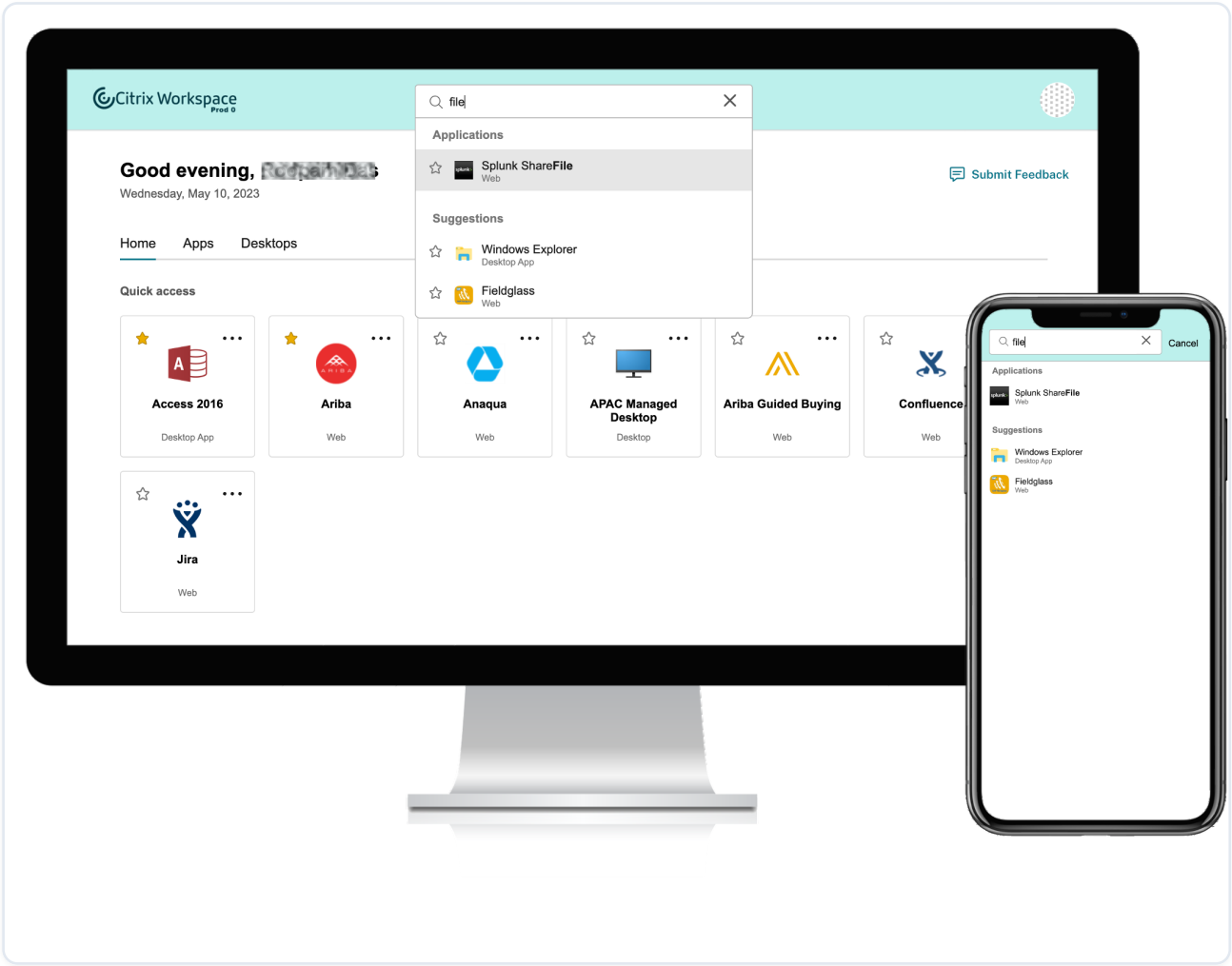
Administratoren können auch Folgendes mithilfe von Schlüsselwörtern Schlüsselwörter konfigurieren:

- **auto** – Apps werden automatisch als Favoriten erstellt, können aber vom Benutzer entfernt werden.
- **mandatory** – Apps sind immer Favoriten und können vom Benutzer nicht entfernt werden.

Informationen zum Deaktivieren von Favoriten finden Sie unter Enable or disable favorites. Wenn Favoriten deaktiviert sind, werden alle Apps auf der Registerkarte **Startseite** angezeigt.

Nach Apps und Desktops suchen

Benutzer können Suchbegriffe eingeben, um nach Apps und Desktops nach Name und Kategorie zu suchen. Favoriten werden oben in der Liste angezeigt.



Aktivitätsmanager

Benutzer können ihre Sitzungen mit dem Aktivitätsmanager verwalten.

App- und Desktop-Kacheln

Die Kachel zeigt den Anwendungsnamen an, wie er in Studio konfiguriert ist. Benutzer können auf die Kachel klicken, um die Anwendung zu starten.

Für zugewiesene Desktops wird zusätzlich der Energiestatus angezeigt. Weitere Informationen finden Sie unter Energiestatus.

Kachelaktionen

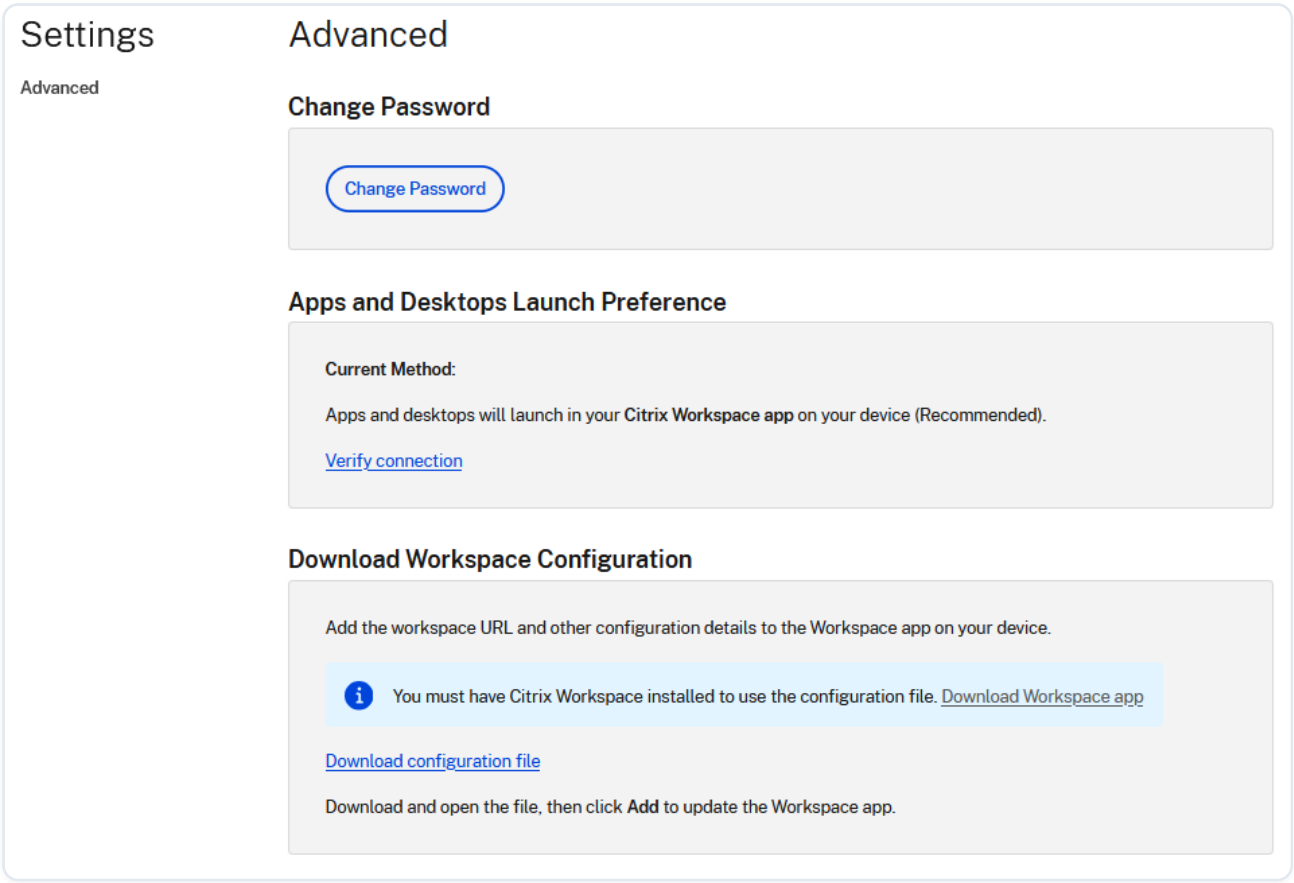
Das Menü **Weitere** Optionen (Ellipsen-Symbol) auf der Kachel bietet Benutzern Zugriff auf relevante Aktionen. Die angezeigten Optionen sind kontextsensitiv.

Diese Aktionen können Folgendes umfassen:

- **Desktop öffnen** oder **App öffnen** – Startet die App oder den Desktop oder stellt die Verbindung wieder her. Wenn der Desktop ausgeschaltet ist oder sich im Ruhezustand befindet, wird er zuerst eingeschaltet, bevor die Sitzung gestartet wird.
- **Zu Favoriten hinzufügen** – Fügt die App zu den Favoriten hinzu, sodass sie auf der Registerkarte **Startseite** angezeigt wird. Dies hat denselben Effekt wie das Klicken auf den **Stern**. Nur aktiviert, wenn Favoriten aktiviert sind.
- **Details anzeigen** – Öffnet ein Pop-up-Fenster mit der Beschreibung der App oder des Desktops.
- Für zugewiesene Desktops sind möglicherweise zusätzliche Energieverwaltungsaktionen verfügbar. Weitere Informationen finden Sie unter Energieaktionen.

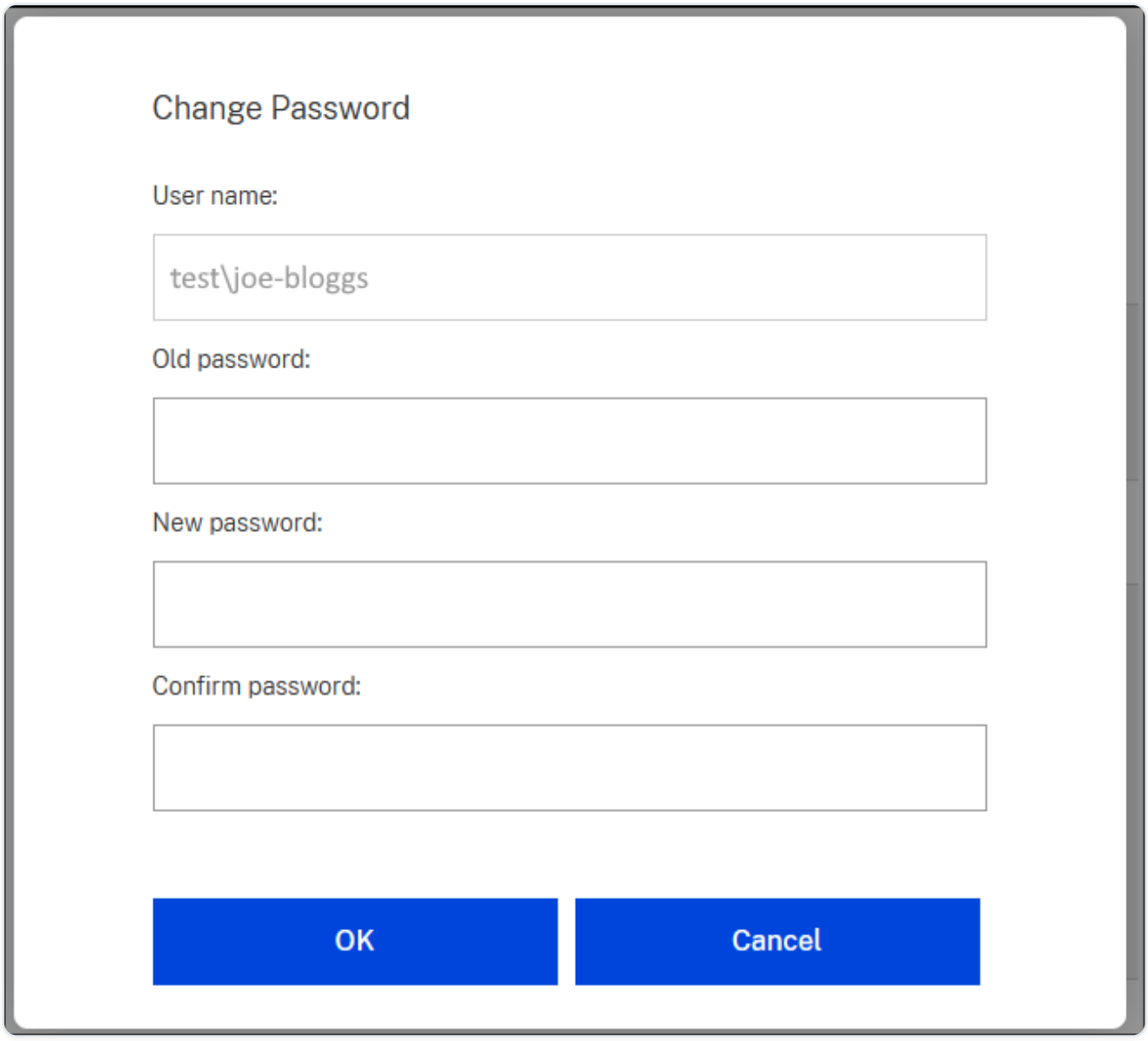
Einstellungen

Benutzer greifen über ein Menü auf die **Kontoeinstellungen** zu, das angezeigt wird, wenn sie ihr Profilsymbol in der oberen rechten Ecke der Benutzeroberfläche auswählen.



Kennwort ändern

Wenn sich Benutzer mit Benutzername- und Kennwortauthentifizierung angemeldet haben und StoreFront so konfiguriert ist, dass Benutzer ihr Kennwort jederzeit ändern können, wird ihnen die Option **Kennwort ändern** angezeigt. Wenn der Benutzer diesen Bildschirm auswählt, wird ein Fenster angezeigt, in dem er sein altes und neues Kennwort eingeben kann:



Startpräferenz für Apps und Desktops

Bei Verwendung eines Webbrowsers wird hier angezeigt, ob Apps im Webbrowser oder in der Citrix Workspace-App gestartet werden oder indem eine ICA-Datei heruntergeladen wird, die der Benutzer in der Citrix Workspace-App öffnen kann.

Der Benutzer kann **Verbindung überprüfen** auswählen, um den Citrix Workspace-App-Erkennungsbildschirm zu öffnen.

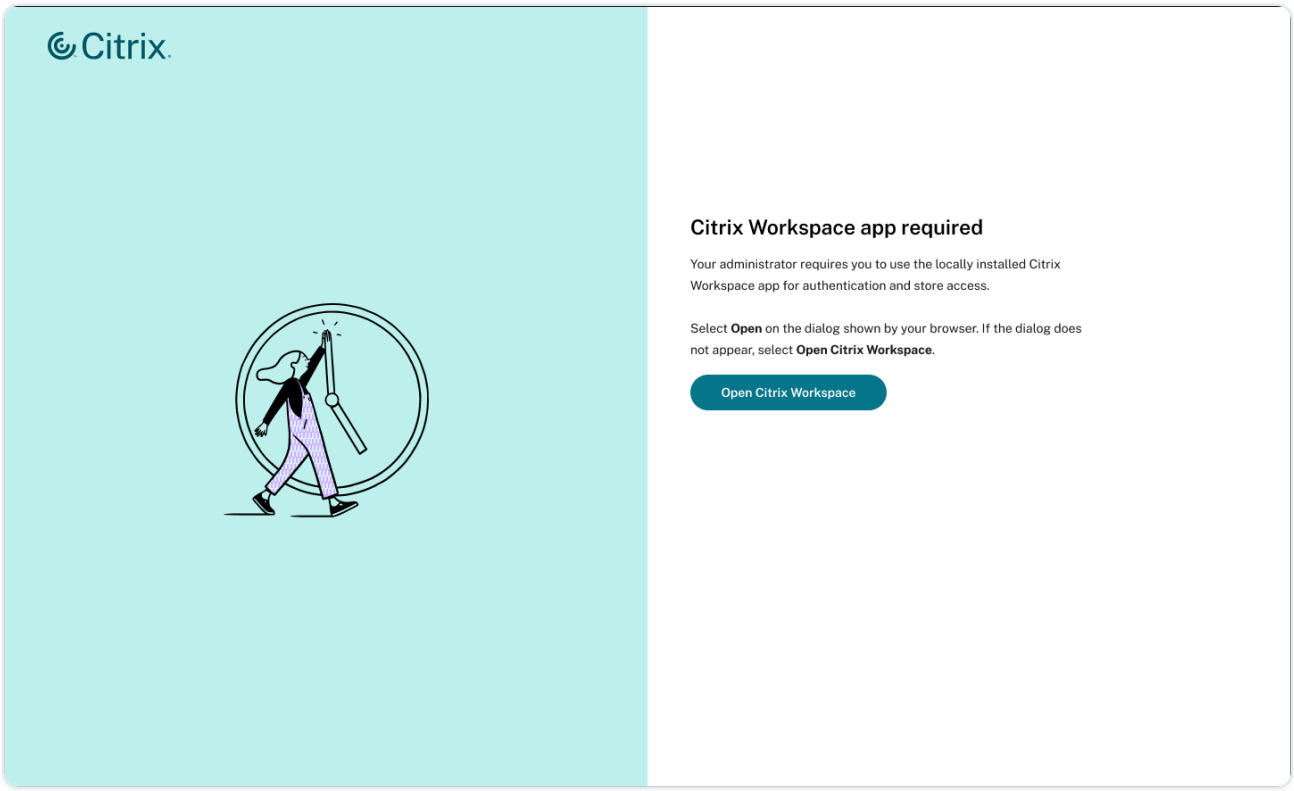
Workspace-Konfiguration herunterladen

Bei Verwendung eines Webbrowsers können Benutzer eine Datei herunterladen, die die Citrix Workspace-App für die Verbindung mit dem Store konfiguriert. Informationen zum Aktivieren dieser Funktion finden Sie unter Endbenutzern das Herunterladen einer Citrix Workspace-App-Konfigurationsdatei erlauben

Citrix Workspace-App erforderlich

Sobald Administratoren Citrix Workspace-App erforderlich aktiviert haben, können Endbenutzer den Citrix Workspace-Webclient in Browsern nicht mehr verwenden.

Wenn Benutzer versuchen, auf den Webclient zuzugreifen, indem sie eine Store-URL in einen Browser eingeben, sehen sie die folgende Webseite, die sie auffordert, die native App zu öffnen.



1. Klicken Sie auf **Citrix Workspace öffnen**.

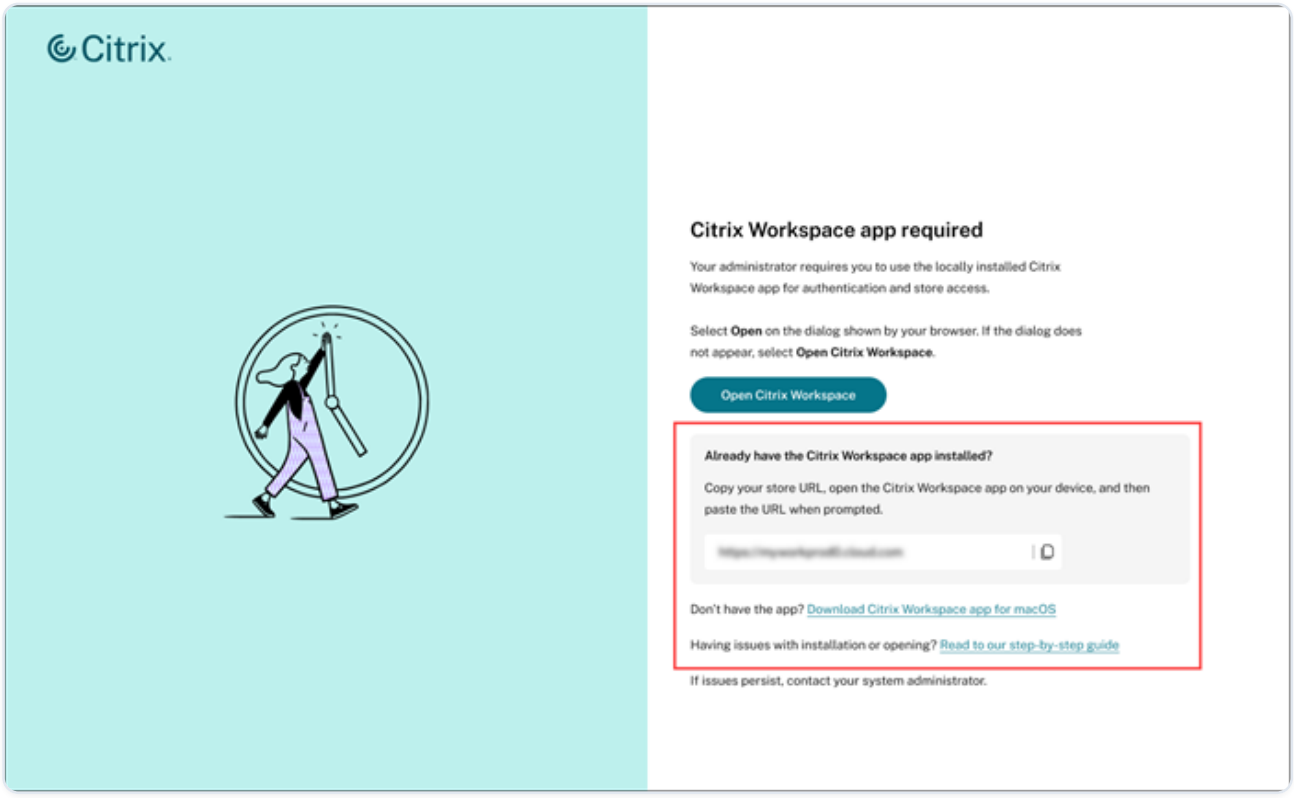
   Der Client-Erkennungsprozess beginnt und prüft, ob die Citrix Workspace-App lokal auf dem Benutzergerät installiert ist.

   Die Aufforderung **Citrix Workspace Launcher öffnen** wird angezeigt und fordert Benutzer auf, die native App zu öffnen.
2. Klicken Sie auf **Citrix Workspace-App öffnen**.

Wenn ein Benutzer die Aufforderung nicht sieht oder nicht innerhalb von 5 Sekunden auf **Citrix Workspace-App öffnen** in der Aufforderung klickt, bietet die Webseite die folgenden zusätzlichen Optionen zur Fortsetzung:

- Die Store-URL zum Kopieren und manuellen Hinzufügen in der nativen Citrix Workspace-App.
- Ein Download-Link zur Installation der Citrix Workspace-App. Informationen zum Konfigurieren der Download-Links finden Sie unter Bereitstellung der Citrix Workspace-App.

- Der Link zum Endbenutzerhandbuch, das Schritt-für-Schritt-Anleitungen zur Installation und zum Öffnen der Citrix Workspace-App enthält.



Hinweis:

Wenn ein Benutzer den Safari-Browser auf einem iPad verwendet, kann der Browser ihn nicht von einem Mac-Desktop unterscheiden. Daher muss der Benutzer auf den Link **Ich bin auf einem iPad** klicken, um mit der automatischen Store-Hinzufügung fortzufahren.

Die automatische Store-Hinzufügung wird unter Linux und ChromeOS nicht unterstützt. Daher wird die Aufforderung **Citrix Workspace Launcher öffnen** auf diesen Geräten nicht angezeigt. In solchen Fällen müssen Benutzer die Store-URL manuell in der nativen App hinzufügen. Weitere Informationen finden Sie unter Manuelle Store-Hinzufügung.

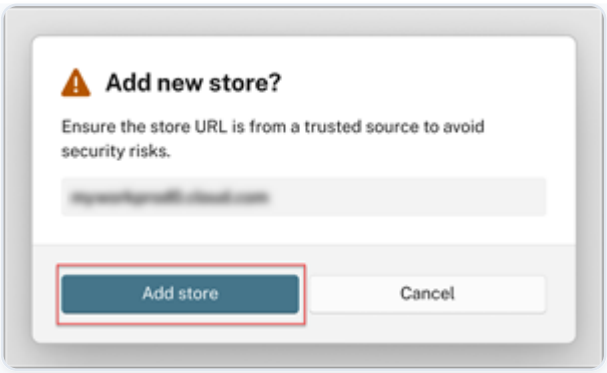
Automatische Store-Hinzufügung

Bei unterstützten Versionen der Citrix Workspace-App wird der Store automatisch hinzugefügt. Die Mindestversionen sind wie folgt:

BETRIEBSSYSTEM	KOMPATIBLE VERSION
Windows	24.9.0 oder höher
Mac	24.5.0 oder höher
Android und iOS	24.9.0 oder höher

Hinweis:

Die automatische Store-Hinzufügung wird auf Linux- und ChromeOS-Plattformen nicht unterstützt und hat Versionsanforderungen auf Windows- und Mac-Plattformen. In solchen Fällen müssen Benutzer die Store-URL manuell in der nativen App hinzufügen. Weitere Informationen finden Sie unter Manuelle Store-Hinzufügung.

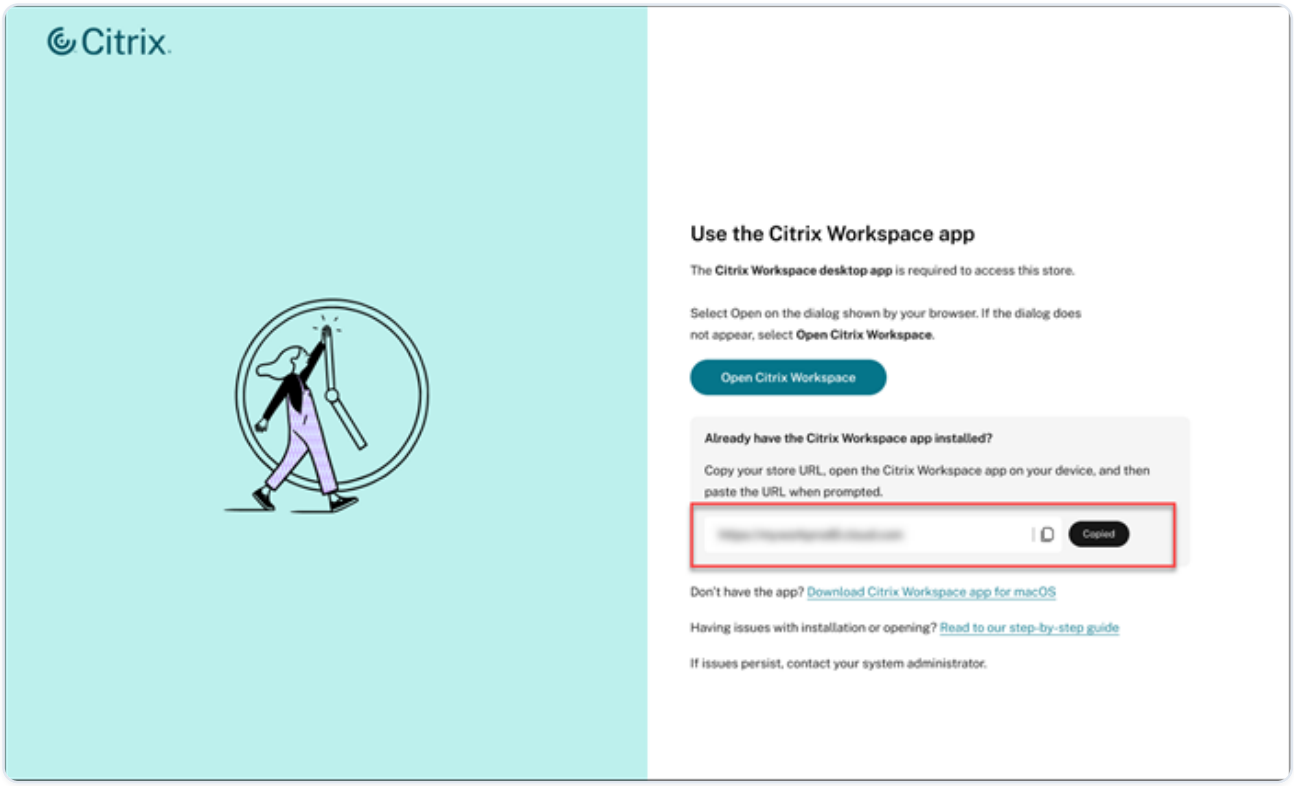


Klicken Sie auf **Store hinzufügen**.

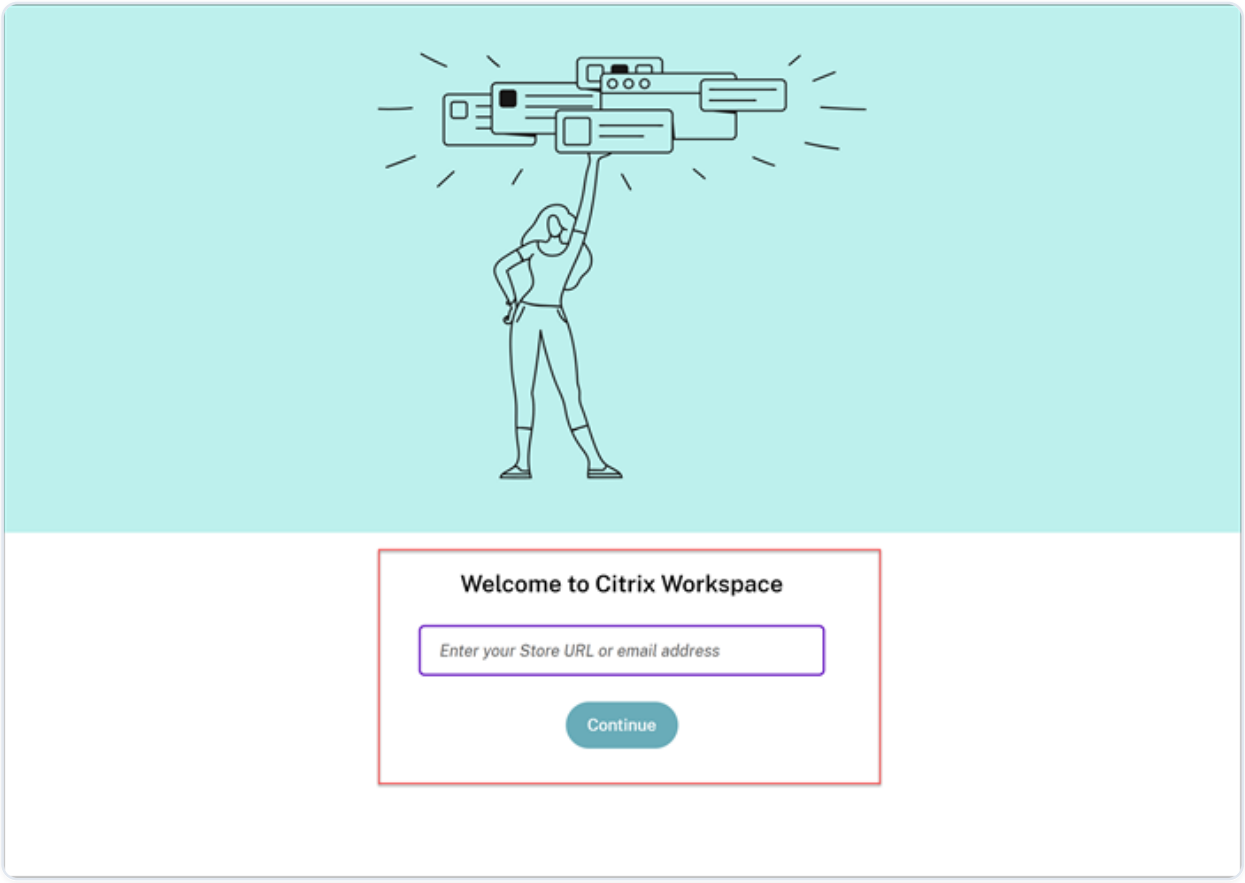
Nach dem Klicken erfasst die native App automatisch die im Browser eingegebene Store-URL und zeigt die Authentifizierungsseite an, auf der sich der Benutzer anmelden kann. Nach erfolgreicher Authentifizierung sieht der Benutzer die Startseite der nativen Citrix Workspace-App.

Manuelle Store-Hinzufügung

Benutzer können der Citrix Workspace-App manuell einen Store hinzufügen, wenn die native App die Store-URL nicht automatisch erfasst, wenn sie auf die Option **Store hinzufügen** klicken.



1. Kopieren Sie die Store-URL von der nativen Mandatswebseite und fügen Sie sie auf der Seite **Willkommen bei Citrix Workspace** ein.



2. Klicken Sie auf **Weiter**.

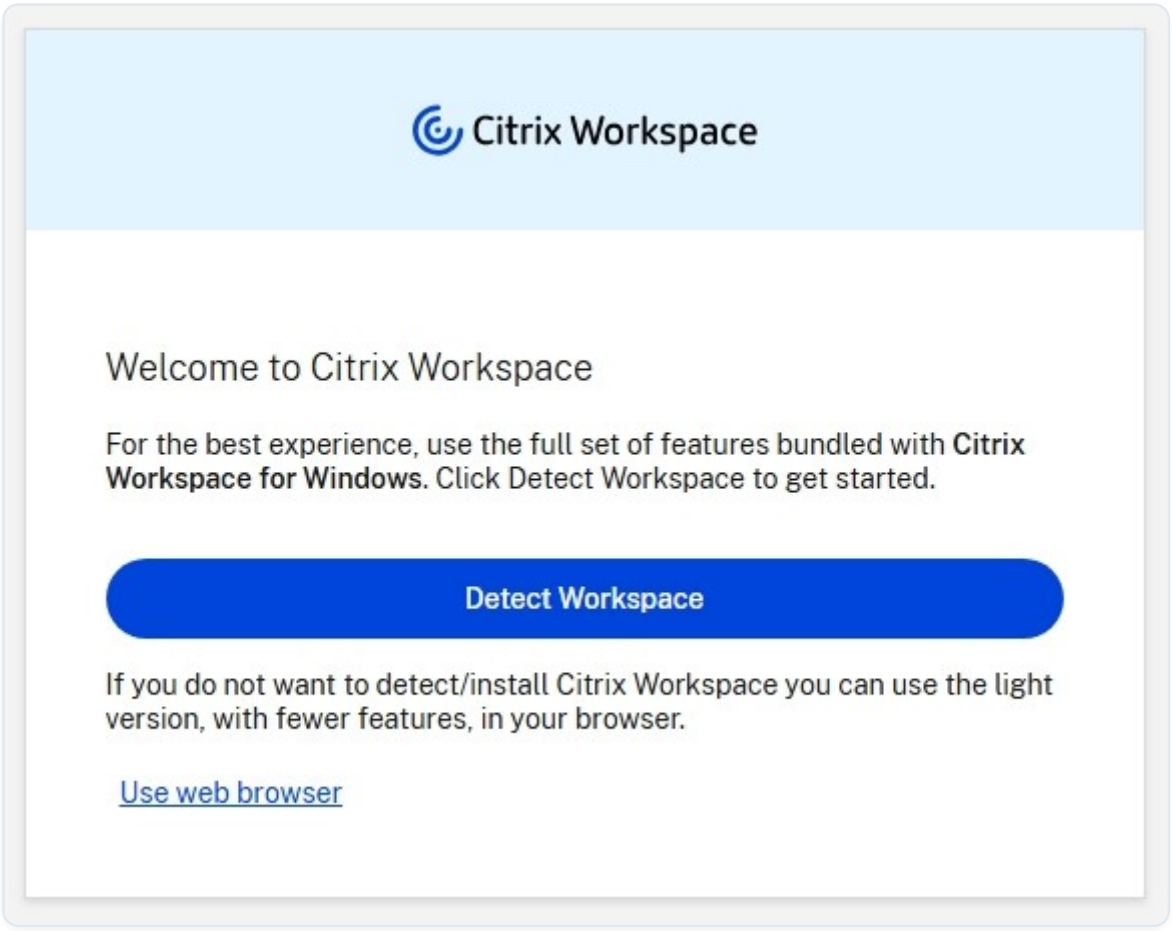
Nach dem Übermitteln einer gültigen Store-URL zeigt die Citrix Workspace-App die Authentifizierungsseite an, auf der sich der Benutzer anmelden kann. Nach erfolgreicher Authentifizierung sieht der Benutzer die Startseite der nativen Citrix Workspace-App.

Erkennung der Citrix Workspace-App

Willkommen beim Citrix Workspace-Bildschirm

Beim Zugriff auf den Store über einen Webbrowser wird möglicherweise der Bildschirm **Willkommen bei Citrix Workspace** angezeigt. Dies trifft zu, wenn:

- Der Benutzer den Store zum ersten Mal in seinem Webbrowser öffnet oder nachdem er die Websitedaten aus dem Webbrowser gelöscht hat.
- Startpräferenz auf **In Citrix Workspace-App öffnen** oder **Benutzer wählen lassen** eingestellt ist.
- Die Citrix Web Extension nicht installiert ist oder die Citrix Workspace-App nicht erkannt hat. Wenn die Citrix Web Extension die Citrix Workspace-App erkennt, wird dieser Schritt übersprungen und standardmäßig der Start in der Citrix Workspace-App durchgeführt.
- Das Betriebssystem des Geräts den (/de-de/citrix-workspace/get-started/user-access#citrix-workspace-launcher) unterstützt.

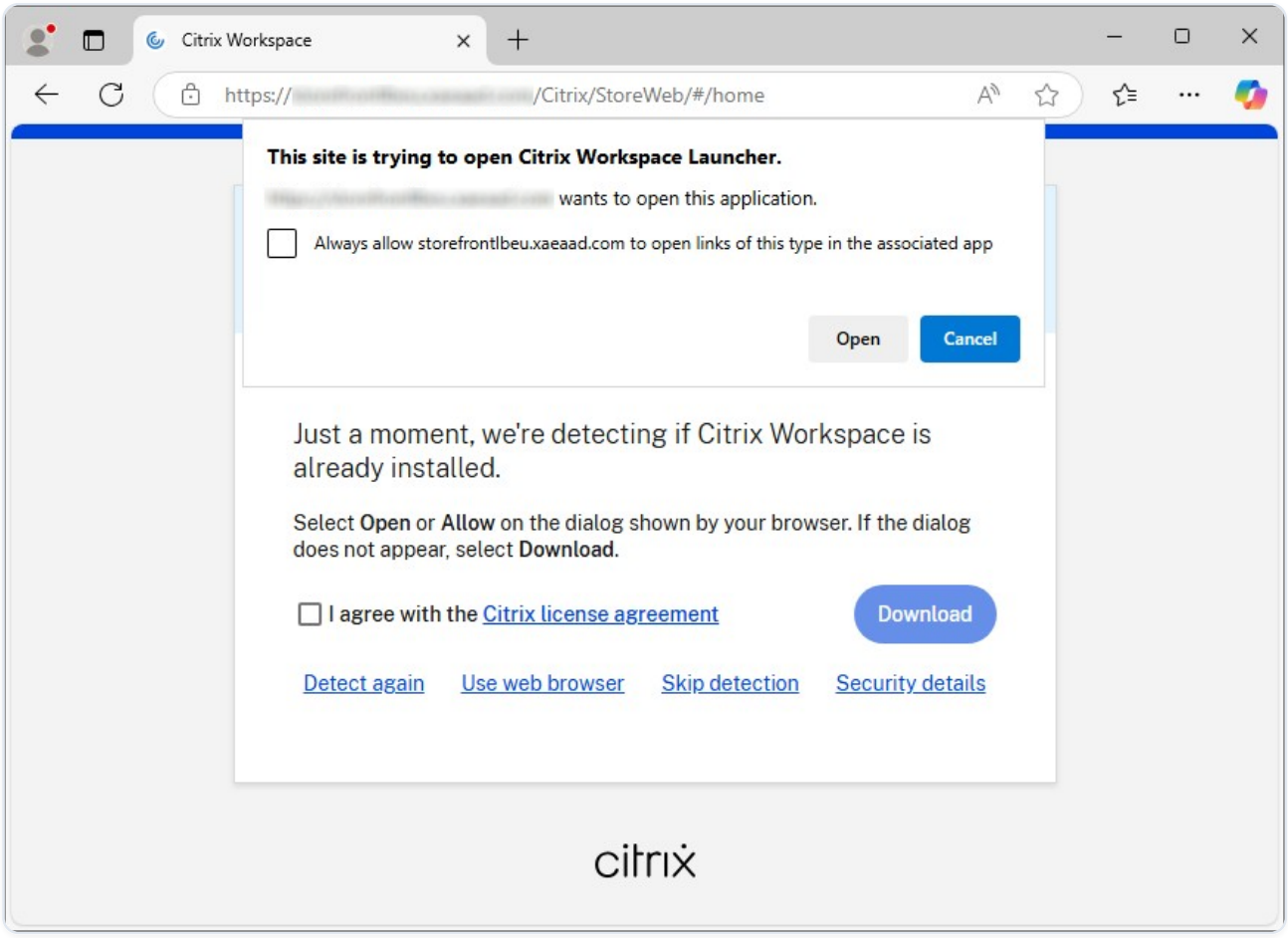


Benutzer können entweder:

- **Citrix Workspace-App erkennen** auswählen, wenn sie Ressourcen in der lokal installierten Citrix Workspace-App starten möchten. Dies wird für die beste Benutzererfahrung empfohlen.
- Wählen Sie **Webbrowser verwenden**, um Ressourcen immer im Browser zu starten. Diese Option ist nur verfügbar, wenn die Startpräferenz auf **Benutzer wählen lassen** eingestellt ist.

Bildschirm zur Erkennung der Citrix Workspace-App

Wenn der Benutzer **Citrix Workspace-App erkennen** auswählt, zeigt die Website den Erkennungsbildschirm der Citrix Workspace-App an. Dabei wird versucht, den **Citrix Workspace Launcher** zu öffnen, eine Komponente der Citrix Workspace-App. Wenn die Citrix Workspace-App installiert ist, zeigt Ihr Browser eine Meldung an, in der Sie aufgefordert werden, den **Citrix Workspace Launcher** auszuführen. Klicken Sie auf **Citrix Workspace Launcher öffnen** oder **Link öffnen** (je nach Browser). Es wird empfohlen, auch **Immer zulassen, dass *Domäne* Links dieses Typs in der zugehörigen App öffnet** (oder Ähnliches, je nach Browser) auszuwählen, um zu vermeiden, dass diese Meldung bei jedem Start einer Ressource angezeigt wird.



Der Benutzer kann dies auch über den Einstellungsbildschirm erreichen.

Wird eine lokal installierte Citrix Workspace-App erkannt, wird nach einigen Sekunden der nächste Bildschirm angezeigt. Wenn der Benutzer anschließend eine Ressource startet, verwendet er den Citrix Workspace Launcher, um Ressourcen in der lokal installierten Citrix Workspace-App zu öffnen.

Wenn die Citrix Workspace-App nicht installiert ist oder der Benutzer den Citrix Workspace Launcher abbricht, stehen möglicherweise die folgenden Optionen zur Verfügung:

- **Herunterladen** – Lädt die Citrix Workspace-App von der Citrix-Website herunter. Informationen zum Konfigurieren dieser Option finden Sie unter Bereitstellung der Citrix Workspace-App.
- **Erneut erkennen** – Versucht, die lokal installierte Citrix Workspace-App erneut zu erkennen.
- **Webbrowser verwenden** – Überspringt die Erkennung der Workspace-App und öffnet Ressourcen immer im Webbrowser. Diese Option ist nur verfügbar, wenn die Startpräferenz auf **Benutzer wählen lassen** eingestellt ist.
- **Erkennung überspringen** – Benutzer können diese Option verwenden, wenn sie eine ältere Version von Citrix Receiver installiert haben, die den Citrix Workspace Launcher oder Citrix Web Extensions nicht unterstützt. Wenn sie diese Option auswählen, lädt ihr Browser beim Starten einer virtuellen App oder eines Desktops eine `.ica`-Datei herunter, die sie mit der Citrix Workspace-App öffnen können. Diese Option führt zu einer eingeschränkten Funktionalität und Sicherheit, daher wird Administratoren empfohlen, diese Option zu deaktivieren.

Aktivitätsmanager

Der Activity Manager ist eine einfache, aber leistungsstarke Funktion, die Benutzern die effektive Verwaltung ihrer Ressourcen ermöglicht. Er steigert die Produktivität, indem er schnelle Aktionen für aktive Apps und Desktops von jedem Gerät aus ermöglicht. Benutzer können nahtlos mit ihren Sitzungen interagieren, nicht mehr benötigte Sitzungen beenden oder trennen, Ressourcen freigeben und die Leistung unterwegs optimieren.

Das Aktivitätsmanager-Panel zeigt eine konsolidierte Liste von Apps und Desktops an, die nicht nur auf dem aktuellen Gerät, sondern auch auf jedem Remote-Gerät mit aktiven Sitzungen aktiv sind. Benutzer können diese Liste anzeigen, indem sie auf das Aktivitätsmanager-Symbol klicken, das sich neben dem Profilsymbol auf dem Desktop und am unteren Bildschirmrand auf Mobilgeräten befindet.

> **Hinweis:**

> Wenn Sie das Activity Manager-Symbol in einem dunkleren Banner-Design nicht sehen können, sollten Sie die in der Einstellung **Bannertext- und Symbolfarbe** ausgewählte Farbe ändern und testen. Das Symbol ist möglicherweise aufgrund eines geringen Kontrasts zwischen dem Banner und dem Activity Manager-Symbol nicht deutlich sichtbar. Weitere Informationen finden Sie unter Erscheinungsbild.

Voraussetzungen

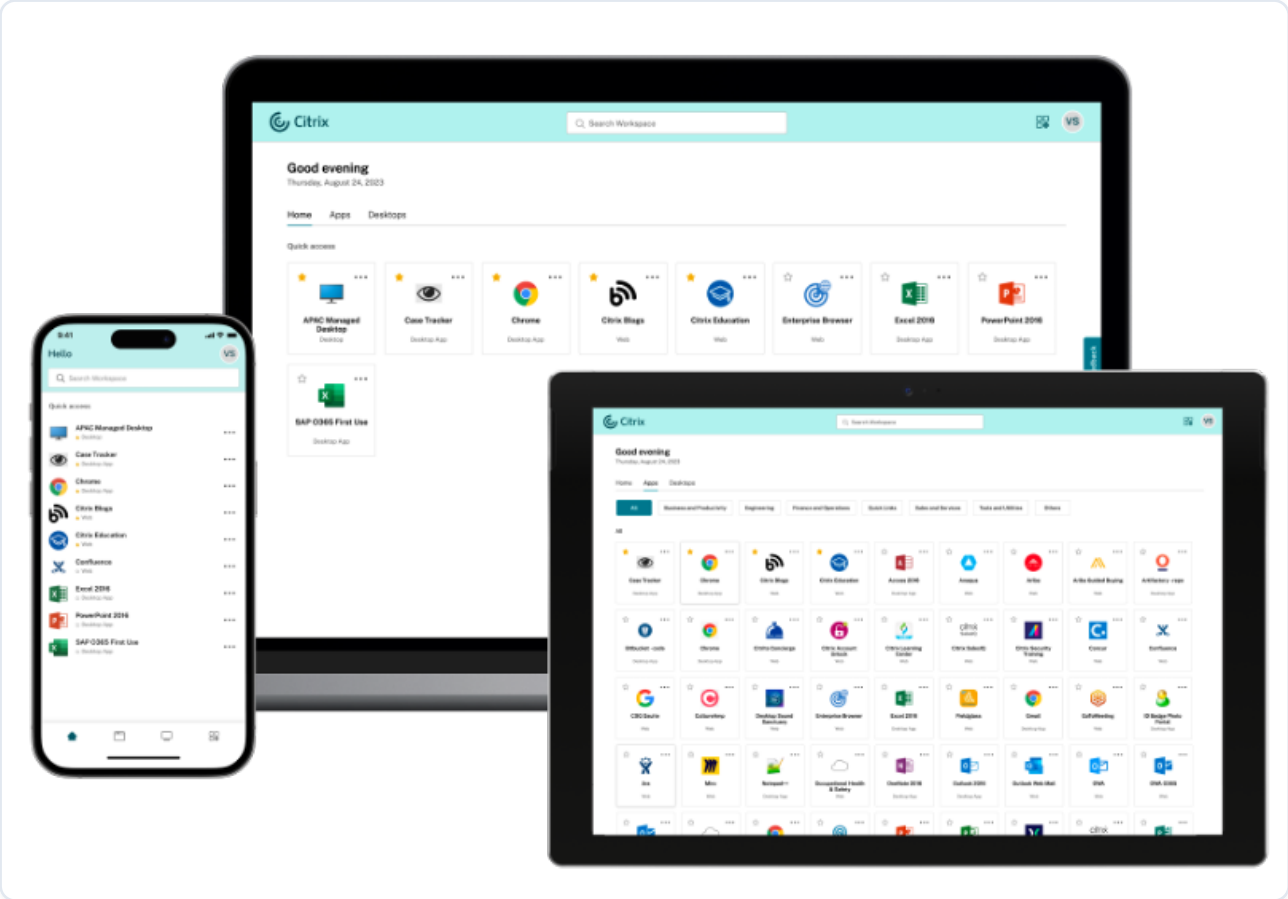
Die Activity Manager-Funktion erfordert Citrix Desktops as a Service oder Citrix Virtual Apps™ and Desktop 2311 und höher. Wenn Sie eine frühere Version von Citrix Virtual Apps and Desktops verwenden, zeigt der Activity Manager keine Sitzungen an, daher wird empfohlen, den Activity Manager auszublenden.

Um zu steuern, ob die Schaltfläche **Activity Manager** angezeigt wird, siehe Activity Manager anzeigen.

Verwenden des Aktivitätsmanagers

Aktive Apps und Desktops werden im Aktivitätsmanager wie folgt gruppiert.

- Eine Liste der Apps und Desktops, die auf dem aktuellen Gerät aktiv sind, wird unter **Auf diesem Gerät** gruppiert.
- Eine Liste der Apps und Desktops, die auf anderen Geräten aktiv sind, wird unter **Remote ausgeführt** gruppiert.



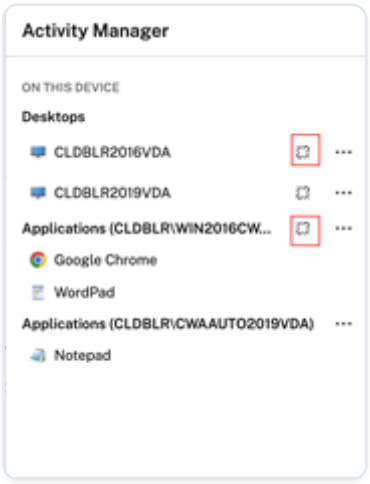
Benutzer können die folgenden Aktionen für eine App oder einen Desktop ausführen, indem sie auf die entsprechende Schaltfläche mit den Auslassungspunkten (...) klicken.

- **trennen**: Die Remote-Sitzung wird getrennt, aber die Apps und Desktops sind im Hintergrund aktiv.
- **Abmelden**: Meldet sich von der aktuellen Sitzung ab. Alle Apps in den Sitzungen werden geschlossen, und alle nicht gespeicherten Dateien gehen verloren.
- **Herunterfahren**: Schließt Ihre getrennten Desktops.
- **Herunterfahren erzwingen**: Fährt Ihren Desktop im Falle eines technischen Problems zwangsweise herunter.
- **Neustart**: Fährt Ihren Desktop herunter und startet ihn erneut.
- **Ruhezustand**: Speichert den aktuellen Zustand und schaltet die Maschine aus.
- **Fortsetzen**: Startet und stellt den Zustand einer Maschine im Ruhezustand wieder her.

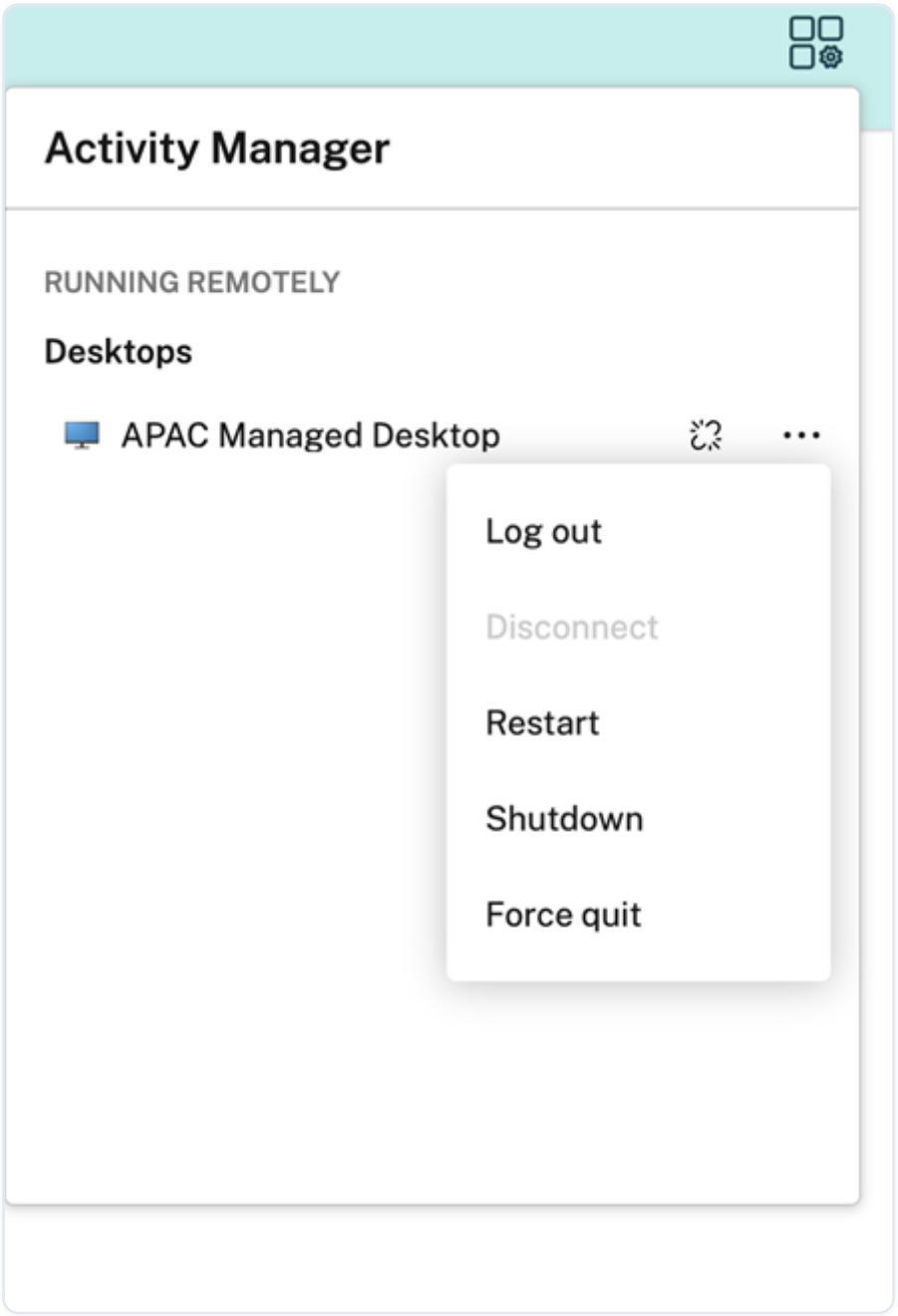
Getrennte Apps und Desktops

Der Aktivitätsmanager ermöglicht Endbenutzern, Apps und Desktops anzuzeigen und Aktionen darauf auszuführen, die im getrennten Modus, lokal oder remote, ausgeführt werden. Sitzungen können von mobilen oder Desktop-Geräten aus verwaltet werden, sodass Endbenutzer unterwegs Aktionen ausführen können. Das Ausführen von Aktionen bei getrennten Sitzungen, wie z. B.

Abmelden oder Herunterfahren, fördert die optimierte Nutzung von Ressourcen und reduziert den Energieverbrauch.



- Die getrennten Apps und Desktops werden im Aktivitätsmanager-Panel angezeigt und sind durch ein Trennsymbol gekennzeichnet.
- Die getrennten Apps sind unter den jeweiligen Sitzungen gruppiert und die Sitzungen sind durch ein Trennsymbol gekennzeichnet.



Endbenutzer können die folgenden Aktionen auf ihren getrennten Desktops ausführen, indem sie auf die Schaltfläche mit den Auslassungspunkten klicken:

- **Abmelden**: Verwenden Sie diese Option, um sich von Ihrem getrennten Desktop abzumelden. Alle Apps in der Sitzung werden geschlossen, und alle nicht gespeicherten Dateien gehen verloren.
- **Herunterfahren**: Verwenden Sie diese Option, um Ihre getrennten Desktops zu schließen.
- **Ausschalten**: Verwenden Sie diese Option, um Ihre getrennten Desktops im Falle eines technischen Problems zwangsweise auszuschalten.
- **Neustart**: Verwenden Sie diese Option, um den getrennten Desktop herunterzufahren und erneut zu starten.

Das Verhalten getrennter Sitzungen im Aktivitätsmanager unterscheidet sich wie folgt.

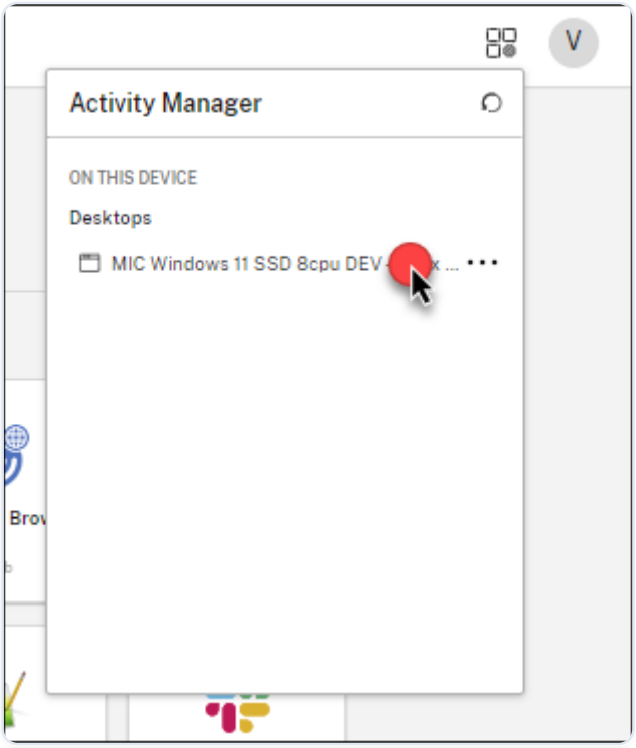
- Wenn der Benutzer über einen Browser bei Citrix® Workspace angemeldet ist und eine lokale Sitzung trennt, wird die Sitzung zunächst unter **Auf diesem Gerät** angezeigt. Sobald der Benutzer den Activity Manager jedoch schließt und erneut öffnet, wird die getrennte Sitzung unter „Remote ausgeführt“ verschoben.
- Wenn der Benutzer bei der Citrix Workspace-App angemeldet ist und eine lokale Sitzung trennt, verschwindet die getrennte Sitzung aus der Liste. Sobald der Benutzer jedoch den Aktivitätsmanager erneut schließt und öffnet, wird die getrennte Sitzung unter **Remote ausgeführt** verschoben.

Wiederverbindung mit getrennten Apps und Desktops herstellen

Die Wiederverbindungsfunktion ermöglicht es Endbenutzern, ihre getrennten Apps und Desktopsitzungen mühelos wieder zu öffnen und gewährleistet so einen reibungslosen Übergang zwischen Geräten ohne Fortschrittsverlust. Diese Funktion stellt den Zugriff auf die vorherige Arbeitsumgebung nahtlos wieder her, wodurch die Notwendigkeit entfällt, Apps und Desktops zu suchen und erneut zu öffnen.

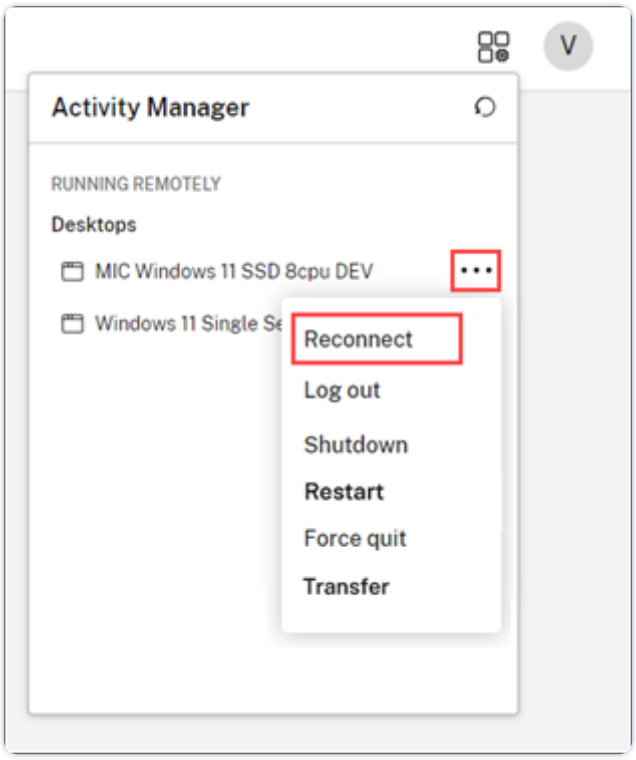
So stellen Sie die Verbindung zu einer getrennten App oder einem getrennten Desktop wieder her:

- Öffnen Sie den Aktivitätsmanager und klicken Sie dann auf das Ressourcenelement.



ODER

- Klicken Sie auf die Schaltfläche mit den Auslassungspunkten (**...**) und klicken Sie dann auf **Wiederverbinden**.

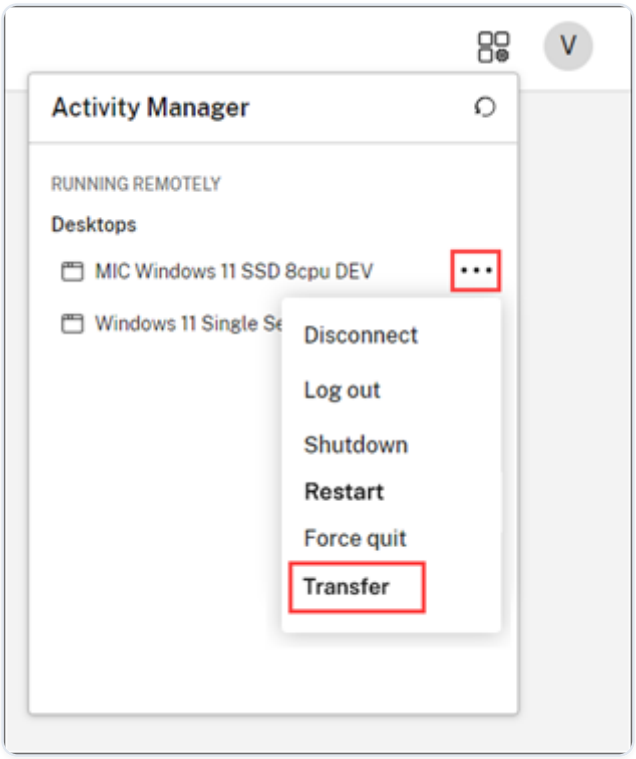


Durch Klicken auf **Wiederverbinden** wird die getrennte Ressource an der Stelle wieder geöffnet, an der Sie sie verlassen haben.

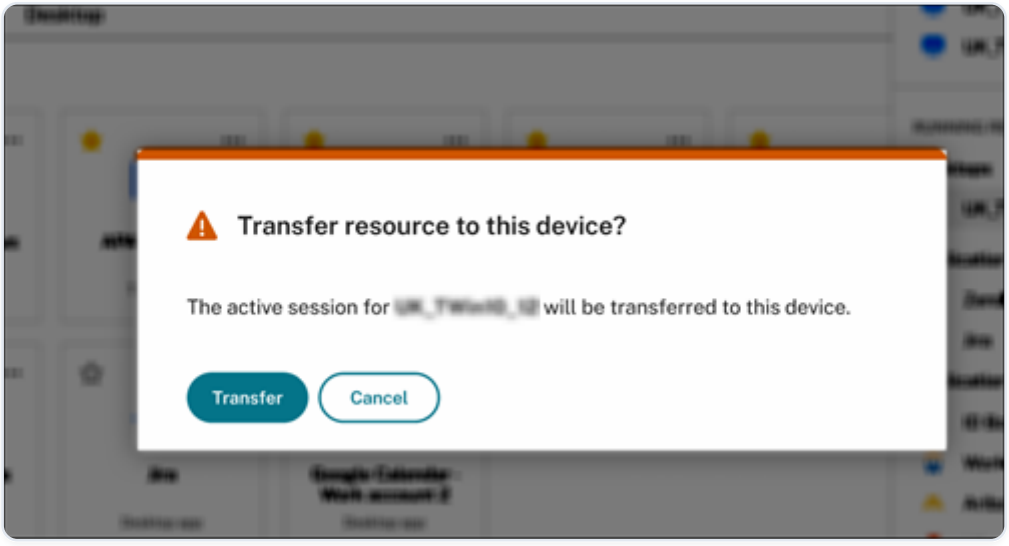
Ihre Apps und Desktops übertragen

Die Übertragungsfunktion ermöglicht es Endbenutzern, ihre aktiven Apps und Desktops von anderen Geräten auf das aktuelle Gerät zu übertragen. Um die Apps und Desktops zu übertragen, gehen Sie wie folgt vor:

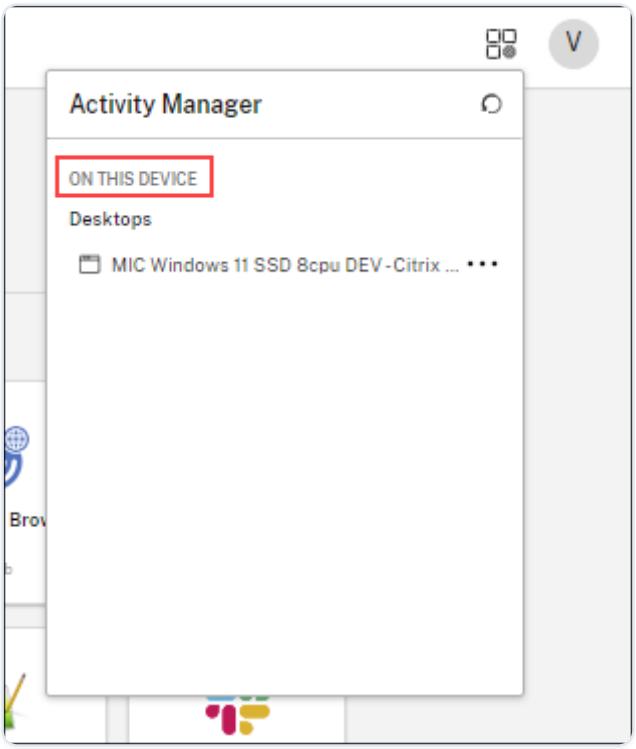
1. Klicken Sie auf die Schaltfläche mit den Auslassungspunkten (**...**) und klicken Sie dann auf **Übertragen**.



2. Klicken Sie auf **Übertragen** im Bestätigungsdialogfeld.



Sobald die Ressourcen auf das aktuelle Gerät übertragen wurden, werden sie im Aktivitätsmanager unter dem Abschnitt **AUF DIESEM GERÄT** aufgeführt.



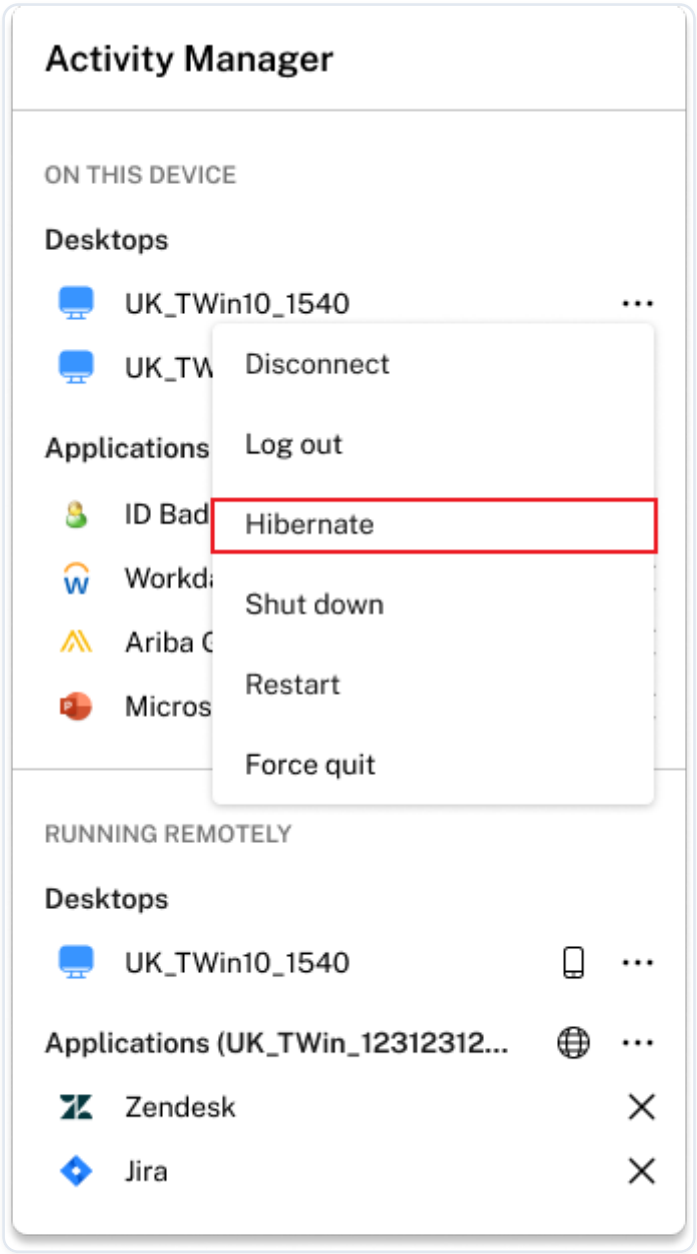
Virtuelle Desktopsitzungen in den Ruhezustand versetzen und fortsetzen

Die Funktion „Ruhezustand und Fortsetzen“ ermöglicht es Benutzern, die Ressourcennutzung zu optimieren, indem virtuelle Desktops bei Nichtgebrauch in den Ruhezustand versetzt und bei Bedarf nahtlos fortgesetzt werden. Dies spart nicht nur Kosten und Energie, sondern verbessert auch den Benutzer-Workflow durch schnellere Wiederaufnahmezeiten der Sitzungen.

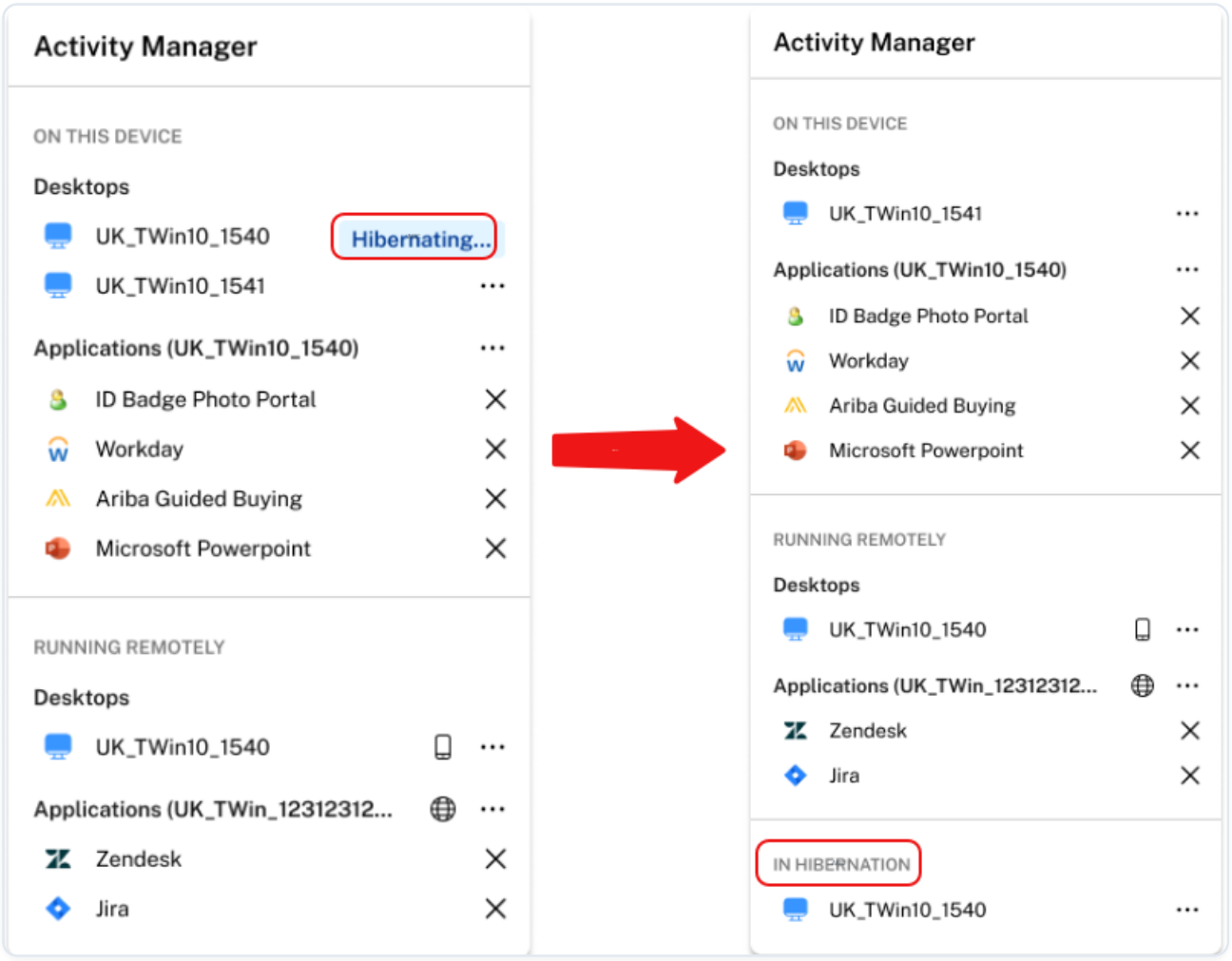
Beim Initiieren des Ruhezustands kommuniziert der Hypervisor mit dem Gastbetriebssystem und löst eine Suspend-to-Disk-Aktion aus. Während dieses Vorgangs werden die Speicherinhalte (RAM) der virtuellen Desktops auf der OS-Festplatte gespeichert, während der virtuelle Desktop selbst freigegeben wird. Beim anschließenden Start werden die RAM-Inhalte des virtuellen Desktops von der OS-Festplatte wiederhergestellt, wodurch sichergestellt wird, dass Anwendungen und Prozesse nahtlos aus ihrem letzten Zustand fortgesetzt werden.

Der Ruhezustand ist für zugewiesene, energieverwaltete Desktops auf unterstützten Hypervisoren verfügbar. Um die Ruhezustandsfunktion zu aktivieren, muss ein Administrator bestimmte Richtlinien befolgen und Vorschaufunktionen sowohl in Azure als auch in Citrix DaaS aktivieren. Weitere Informationen finden Sie unter Ruhezustandsfähige VMs erstellen (Vorschau).

Eine Desktopsitzung in den Ruhezustand versetzen:

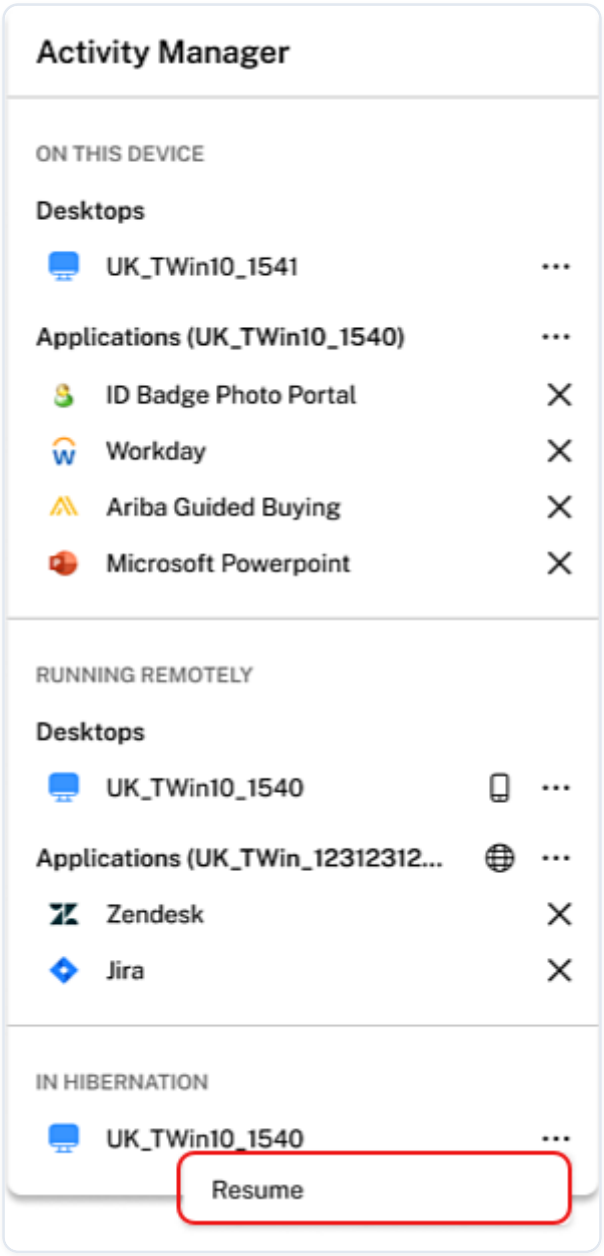


Um eine Desktopsitzung in den Ruhezustand zu versetzen, können Benutzer auf die Schaltfläche mit den drei Punkten (**...**) und dann auf die Option **Ruhezustand** klicken. Der Desktop leitet den Ruhezustand ein, sobald die Benutzer auf die Option **Ruhezustand** klicken. Sobald der Desktop in den Ruhezustand versetzt wurde, wird die Desktop-Ressource im **Aktivitätsmanager** in den Abschnitt **Im Ruhezustand** verschoben.



Eine Desktopsitzung aus dem Ruhezustand fortsetzen:

Desktopsitzungen im Ruhezustand sind im **Aktivitätsmanager** unter dem Abschnitt **Im Ruhezustand** verfügbar. Um die Desktopsitzung aus dem Ruhezustand fortzusetzen, können Benutzer auf die Schaltfläche mit den drei Punkten (**…**) und dann auf die Option **Fortsetzen** klicken.



Sobald Benutzer auf die Option **Fortsetzen** klicken, wird der Desktop wiederhergestellt.

Desktop wird wiederhergestellt(/en-us/storefront/2507-ltsr/media/end-user-experience/resuming-to-desktop-resumed.PNG)

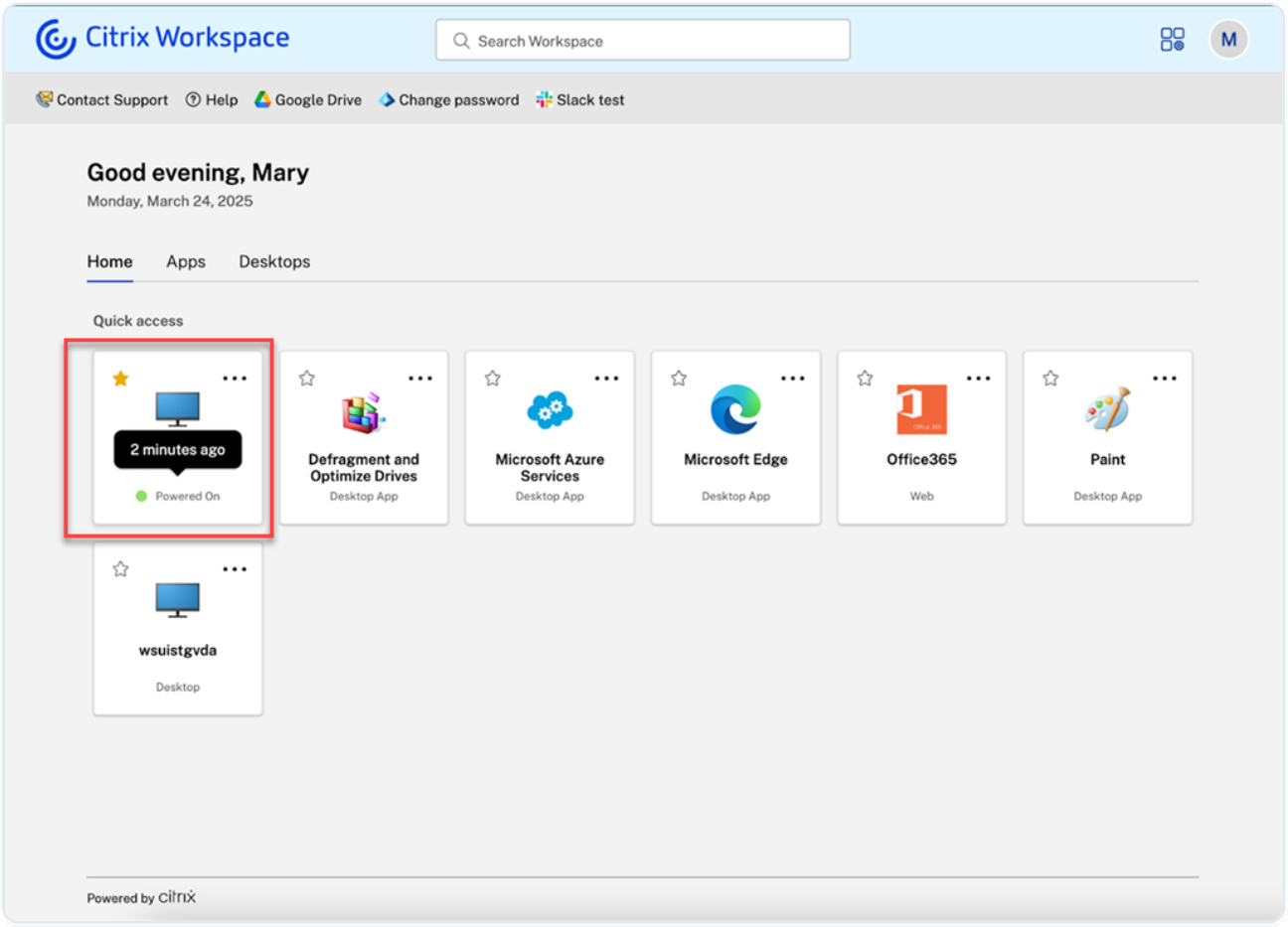
Zugewiesene Desktop-Energieverwaltung

Energiestatus

Die Desktop-Kachel zeigt den Energiestatus möglicherweise an, wenn:

- Der Maschinenkatalog verfügt über ein Einzelsitzungs-Betriebssystem, bei dem die Desktop-Erfahrung auf **Jedes Mal, wenn sich Benutzer anmelden, mit demselben (statischen) Desktop verbinden.** eingestellt ist.
- Der Maschinenkatalog muss als energieverwaltet konfiguriert sein.

- Die Maschine wird von Citrix DaaS oder Citrix Virtual Apps™ and Desktops 2511 oder höher veröffentlicht.



Die folgenden Energiestatusse können angezeigt werden:

- **Ausgeschaltet:** Die Maschine wurde heruntergefahren und läuft derzeit nicht.
- **Im Ruhezustand:** Die Maschine befindet sich im Ruhezustand, wobei die aktuelle Sitzung auf der Festplatte gespeichert wird und die Maschine nur minimale Energie verbraucht.
- **Wird eingeschaltet:** Eine Maschine, die sich im Zustand **Ausgeschaltet** oder **Im Ruhezustand** befand, wurde kürzlich gestartet, ist aber noch nicht betriebsbereit.
- **Eingeschaltet:** Der Desktop ist aktiv und läuft. Bei dedizierten Ressourcen bleibt der Energiestatus typischerweise im Zustand „Eingeschaltet“, selbst wenn der Benutzer die Verbindung zu seiner Sitzung trennt.
- **Wird heruntergefahren:** Der Benutzer hat ein Herunterfahren initiiert.

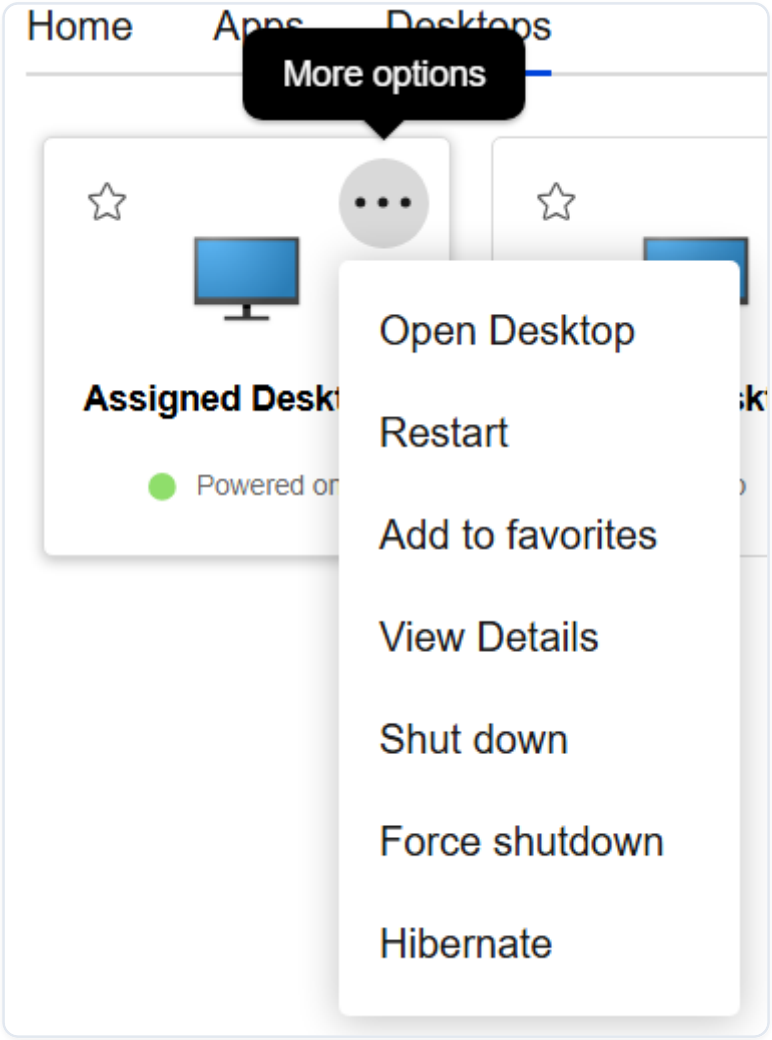
Der Status wird alle zwei Minuten oder wenn der Benutzer auf das Ellipsenmenü auf der Desktop-Kachel klickt, aktualisiert. Wenn der Benutzer den Mauszeiger über den Energiestatus bewegt, wird angezeigt, wann die letzte Aktualisierung erfolgte.

Bekannte Probleme

- Wenn Sie einen von mehreren energieverwalteten Desktops starten, zeigt der Store möglicherweise inkonsistente Energiestatus für die anderen Desktops an, bis der erste Desktop vollständig gestartet ist.

Energieaktionen

Das Menü **Weitere Optionen** (Auslassungspunkte-Symbol) auf der Kachel bietet Benutzern Zugriff auf relevante Aktionen. Für energieverwaltete zugewiesene Maschinen gibt es zusätzliche Aktionen, die vom aktuellen Energiezustand der Ressource abhängen.



Diese Aktionen können Folgendes umfassen:

- **App öffnen** – Startet die App oder stellt die Verbindung wieder her.
- **Neustart** – Leitet einen erzwungenen Neustart ein. Nur für zugewiesene energieverwaltete Desktops verfügbar.
- **Herunterfahren** – Leitet ein ordnungsgemäßes Herunterfahren ein. Nur für zugewiesene energieverwaltete Desktops verfügbar.

- **Erzwungenes Herunterfahren** – Schaltet die Maschine zwangsweise aus. Nur für zugewiesene energieverwaltete Desktops verfügbar.
- **Ruhezustand** – Versetzt den dedizierten Desktop in den Ruhezustand. Nur für zugewiesene energieverwaltete Desktops verfügbar, bei denen der Ruhezustand aktiviert ist.
- **Fortsetzen** – Weckt den dedizierten Desktop aus dem Ruhezustand auf. Nur für zugewiesene energieverwaltete Desktops verfügbar, bei denen der Ruhezustand aktiviert ist.

Sichern Sie Ihre StoreFront-Bereitstellung

Dieser Artikel beleuchtet Bereiche, die sich auf die Systemsicherheit bei der Bereitstellung und Konfiguration von StoreFront auswirken können.

Authentifizierung von Endbenutzern

Normalerweise müssen sich Endbenutzer entweder direkt bei StoreFront oder bei einem Citrix Gateway vor StoreFront authentifizieren. Weitere Informationen zu den verfügbaren Authentifizierungsmethoden finden Sie unter Authentifizierung.

Kommunikation mit Endbenutzern

Citrix empfiehlt, die Kommunikation zwischen den Geräten der Benutzer und StoreFront mit HTTPS zu sichern. Dies stellt sicher, dass Passwörter und andere Daten, die zwischen Client und StoreFront gesendet werden, verschlüsselt werden. Darüber hinaus können unverschlüsselte HTTP-Verbindungen durch verschiedene Angriffe, wie z. B. Man-in-the-Middle-Angriffe, kompromittiert werden, insbesondere wenn Verbindungen von unsicheren Standorten wie öffentlichen Wi-Fi-Hotspots hergestellt werden. Ohne die entsprechende IIS-Konfiguration verwendet StoreFront HTTP für die Kommunikation.

Je nach Konfiguration können Benutzer über ein Gateway oder einen Lastenausgleich auf StoreFront zugreifen. Sie können die HTTPS-Verbindung am Gateway oder Lastenausgleich beenden. In diesem Fall empfiehlt Citrix jedoch weiterhin, die Verbindungen zwischen dem Gateway oder Lastenausgleich und StoreFront mit HTTPS zu sichern.

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

Auf Ihrem NetScaler Gateway oder dem virtuellen Server des Lastenausgleichs können Sie konfigurieren, welche TLS-Versionen aktiviert sind. Es wird empfohlen, ältere TLS-Versionen vor 1.2 zu deaktivieren.

Auf StoreFront-Servern bestimmen Windows und IIS, welche TLS-Versionen für eingehende Verbindungen zugelassen sind. Es wird empfohlen, ältere TLS-Versionen als 1.2 zu deaktivieren. Unter Windows Server 2025 sind TLS 1.0 und 1.1 standardmäßig deaktiviert. Unter Windows

Server 2022 können Sie IIS so konfigurieren, dass TLS 1.0 und 1.1 für Clientverbindungen deaktiviert werden, siehe Sichern von StoreFront mit HTTPS. Auf allen Windows-Serverversionen können Sie TLS 1.0 und 1.1 mithilfe von Gruppenrichtlinien oder Windows-Registrierungseinstellungen deaktivieren, siehe Microsoft-Dokumentation.

Ältere Versionen von Citrix Receiver können keine Verbindung mit TLS 1.2 herstellen, weitere Details finden Sie unter CTX232266.

Kommunikation mit Delivery Controllern

Citrix empfiehlt die Verwendung des HTTPS-Protokolls, um die Datenübertragung zwischen StoreFront und Ihren Citrix Virtual Apps and Desktops Delivery Controllern zu sichern. Weitere Informationen finden Sie unter HTTPS auf Delivery Controllern aktivieren. Informationen zum Konfigurieren von StoreFront für die Verwendung von HTTPS finden Sie unter Sites für Citrix Virtual Apps and Desktops hinzufügen und Citrix Gateway-Appliance hinzufügen. Falls die Zertifikate kompromittiert werden, können Sie die Überprüfung der Zertifikatsperrliste (CRL) verwenden. StoreFront verwendet TLS 1.2 oder höher für die Kommunikation mit Delivery Controllern.

Es wird empfohlen, den Delivery Controller und StoreFront so zu konfigurieren, dass nur vertrauenswürdige StoreFront-Server mit dem Delivery Controller kommunizieren können, siehe Sicherheitsschlüssel verwalten.

Kommunikation mit Cloud Connectors

Citrix empfiehlt die Verwendung des HTTPS-Protokolls, um die Datenübertragung zwischen StoreFront und Ihren Cloud Connectors zu sichern. Siehe HTTPS-Konfiguration. Informationen zur Konfiguration von StoreFront finden Sie unter Sites für Citrix Desktops as a Service hinzufügen und Citrix Gateway-Appliance hinzufügen. Falls die Zertifikate kompromittiert sind, können Sie die Überprüfung der Zertifikatsperrliste (CRL) verwenden. StoreFront verwendet TLS 1.2 oder höher zur Kommunikation mit Cloud Connectors.

Es wird empfohlen, DaaS und StoreFront so zu konfigurieren, dass nur vertrauenswürdige StoreFront-Server mit den Cloud Connectors kommunizieren können. Weitere Informationen finden Sie unter Sicherheitsschlüssel verwalten.

Kommunikation mit dem Federated Authentication Service

Informationen zur Kommunikation zwischen StoreFront- und Federated Authentication Service (FAS)-Servern finden Sie unter Federated Authentication Service – Sicherheits- und Netzwerkkonfiguration.

Remotezugriff

Citrix empfiehlt nicht, Ihren StoreFront-Server direkt dem Internet auszusetzen. Citrix empfiehlt die Verwendung eines Citrix Gateways, um die Authentifizierung und den Zugriff für Remote-Benutzer bereitzustellen.

Härtung von Microsoft Internet Information Services (IIS)

Sie können StoreFront mit einer eingeschränkten IIS-Konfiguration einrichten. Beachten Sie, dass dies nicht die Standard-IIS-Konfiguration ist.

Dateinamenerweiterungen

Sie können die Anforderungsfilterung verwenden, um Listen zulässiger Dateierweiterungen zu konfigurieren und nicht aufgelistete Dateinamenerweiterungen zu verbieten. Siehe IIS-Dokumentation.

StoreFront erfordert die folgenden Dateinamenerweiterungen:

- . (leere Erweiterung)
- .appcache-Datei
- Dateiendung .aspx
- .cr
- Dateiendung .css
- .dtd-Datei
- .gif Dateierweiterung
- HTML-Datei
- „.html“
- ICA®-Datei
- .ico-Datei
- JPG-Bild

- .js
- .png-Datei
- Die Erweiterung .svg
- Textdatei
- XML-Datei

Wenn der Download oder das Upgrade der Citrix Workspace-App für eine Store-Website aktiviert ist, benötigt StoreFront auch diese Dateinamenerweiterungen:

- DMG-Image
- Ausführbare Datei

Wenn die Citrix Workspace-App für HTML5 aktiviert ist, benötigt StoreFront auch diese Dateinamenerweiterungen:

- „.eot“
- .ttf-Dateiendung
- .woff-Dateiendung
- WebAssembly-Modul

Verben

Sie können die Anforderungsfilterung verwenden, um eine Liste zulässiger Verben zu konfigurieren und nicht aufgelistete Verben zu verbieten. Siehe IIS-Dokumentation.

- GET
- POST
- HEAD

Nicht-ASCII-Zeichen in URLs

Wenn Sie sicherstellen, dass der Store-Name und der Website-Name nur ASCII-Zeichen verwenden, enthalten StoreFront-URLs keine Nicht-ASCII-Zeichen. Sie können die Anforderungsfilterung verwenden, um Nicht-ASCII-Zeichen zu verbieten. Siehe IIS-Dokumentation.

MIME-Typen

Sie können OS-Shell-MIME-Typen entfernen, die den folgenden Dateierweiterungen entsprechen:

- .exe-Datei

- .dll-Datei
- die .com-Endung
- die .bat-Datei
- .csh

Siehe IIS-Dokumentation.

X-Powered-By-Header entfernen

Standardmäßig enthält IIS einen Header `X-Powered-By` mit dem Wert `ASP.NET` auf Serverebene. StoreFront entfernt diesen Header auf allen StoreFront-Websites. Sie können den Header auch auf Serverebene entfernen, was für alle Websites auf dem Server gilt. Weitere Informationen finden Sie in der IIS-Dokumentation zu benutzerdefinierten Headern.

Server-Header mit IIS-Version entfernen

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

StoreFront-Website auf eine separate Partition verschieben

Sie können die StoreFront-Websites auf einer separaten Partition von den Systemdateien hosten. Innerhalb von IIS müssen Sie die **Standardwebsite** verschieben oder eine separate Website auf der entsprechenden Partition erstellen, bevor Sie Ihre StoreFront-Bereitstellung erstellen.

IIS-Funktionen

Eine Liste der von StoreFront installierten und verwendeten IIS-Funktionen finden Sie unter Systemanforderungen. Sie können andere IIS-Funktionen entfernen.

Obwohl StoreFront ISAPI-Filter nicht direkt verwendet, wird die Funktion von ASP.NET benötigt und kann daher nicht deinstalliert werden.

Handlerzuordnungen

StoreFront erfordert die folgenden Handlerzuordnungen. Sie können andere Handlerzuordnungen entfernen.

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

- StaticFile

Siehe IIS-Handler-Dokumentation.

ISAPI-Filter

StoreFront erfordert keine ISAPI-Filter. Sie können alle ISAPI-Filter entfernen. ASP.NET erfordert jedoch die ISAPI-Windows-Funktion. Siehe IIS ISAPI-Filter-Dokumentation.

.NET-Autorisierungsregeln

Standardmäßig ist auf IIS-Servern die ".NET Authorization Rule" auf „Allow All Users“ (Alle Benutzer zulassen) eingestellt. Standardmäßig erbt die von StoreFront verwendete Website diese Konfiguration.

Wenn Sie die .NET-Autorisierungsregel auf Serverebene entfernen oder ändern, müssen Sie die Regeln auf der von StoreFront verwendeten Website überschreiben, um eine Zulassungsregel für „All Users“ hinzuzufügen und alle anderen Regeln zu entfernen.

Einzelhandelsmodus

Sie können den Einzelhandelsmodus aktivieren, siehe IIS-Dokumentation.

Anwendungspools

StoreFront erstellt die folgenden Anwendungspools:

- Citrix Configuration API
- Citrix Delivery Services Authentifizierung
- Citrix Delivery Services Ressourcen
- und Citrix Receiver™ für Web

Ändern Sie nicht die Anwendungspools, die von jeder IIS-Anwendung verwendet werden, oder die Identität jedes Pools. Wenn Sie mehrere Sites verwenden, ist es nicht möglich, jede Site so zu konfigurieren, dass sie separate Anwendungspools verwendet.

Unter den Recycling-Einstellungen können Sie das Leerlauf-Zeitlimit des Anwendungspools und das Limit für den virtuellen Speicher festlegen. Beachten Sie, dass beim Recycling des Anwendungspools "Citrix Receiver for Web" Benutzer, die über einen Webbrowser angemeldet sind, abgemeldet werden. Daher ist er standardmäßig so eingestellt, dass er täglich um 02:00 Uhr recycelt wird, um Störungen zu minimieren. Wenn Sie eine der Recycling-Einstellungen ändern, kann dies dazu führen, dass Benutzer zu anderen Tageszeiten abgemeldet werden.

Standard-IIS-Startseite

Sie können Dateien `iisstart.htm`, `welcome.png` aus `c:\inetpub\wwwroot` löschen.

Erforderliche Einstellungen

- Ändern Sie nicht die IIS-Authentifizierungseinstellungen. StoreFront verwaltet die Authentifizierung und konfiguriert Verzeichnisse der StoreFront-Site mit den entsprechenden Authentifizierungseinstellungen.
- Wählen Sie für den StoreFront-Server unter **SSL-Einstellungen** nicht **Clientzertifikate: Erforderlich** aus. Die StoreFront-Installation konfiguriert die entsprechenden Seiten der StoreFront-Site mit dieser Einstellung.
- StoreFront benötigt Cookies für den Sitzungsstatus und andere Funktionen. In bestimmten Verzeichnissen muss unter **Sitzungsstatus**, **Cookie-Einstellungen**, **Modus** auf **Cookies verwenden** eingestellt sein.
- StoreFront erfordert, dass die **.NET-Vertrauensstufe** auf **Volles Vertrauen** eingestellt ist. Stellen Sie die .NET-Vertrauensstufe nicht auf einen anderen Wert ein.

Dienste

Die StoreFront-Installation erstellt die folgenden Windows-Dienste:

- Citrix Konfigurationsreplikation (NT SERVICE\CitrixConfigurationReplication)
- Citrix Clusterbeitritt (NT SERVICE\CitrixClusterService)
- Citrix Peer-Auflösung (NT SERVICE\Citrix Peer Resolution Service)
- Citrix Anmeldeinformations-Wallet (NT SERVICE\CitrixCredentialWallet)
- Citrix Abonnementspeicher (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 Kerberos-Delegierung von StoreFront für XenApp 6.5 konfigurieren, wird zusätzlich der Dienst Citrix StoreFront Protocol Transition (NT SERVICE\CitrixStoreFrontProtocolTransition) erstellt. Dieser Dienst wird als `NT AUTHORITY\SYSTEM` ausgeführt. Ändern Sie diese Konfiguration nicht.

Zuweisung von Benutzerrechten

Das Ändern der Zuweisung von Benutzerrechten gegenüber den Standardeinstellungen kann zu Problemen mit StoreFront führen. Insbesondere:

- Microsoft IIS wird im Rahmen der StoreFront-Installation aktiviert. Microsoft IIS gewährt der integrierten Gruppe IIS_IUSRS das Anmelde-Recht **Als Stapelverarbeitungsauftrag anmelden** und das Privileg **Einen Client nach der Authentifizierung imitieren**. Dies ist ein normales Installationsverhalten von Microsoft IIS. Ändern Sie diese Benutzerrechte nicht. Weitere Informationen finden Sie in der Microsoft-Dokumentation.
- Wenn Sie StoreFront installieren, werden Anwendungspools erstellt, denen IIS die Benutzerrechte **Als Dienst anmelden**, **Arbeitsspeicherkontingente für einen Prozess anpassen**, **Sicherheitsüberwachungen generieren** und **Ein Token auf Prozessebene ersetzen** gewährt.
- Um eine Bereitstellung zu erstellen oder zu ändern, muss der Administrator die Rechte **Dateien und Verzeichnisse wiederherstellen** haben.
- Damit ein Server einer Servergruppe beitreten kann, muss die Gruppe Administratoren die Rechte **Dateien und Verzeichnisse wiederherstellen**, **Auf diesen Computer vom Netzwerk aus zugreifen** und **Überwachungs- und Sicherheitsprotokoll verwalten** haben.
- Damit sich Benutzer mit Benutzername und Kennwort (direkt oder über ein Gateway) anmelden können, müssen sie die Rechte für **Lokale Anmeldung zulassen** haben, es sei denn, Sie haben StoreFront so konfiguriert, dass Kennwörter über den Delivery Controller validiert werden.

Dies ist keine umfassende Liste, und andere Benutzerzugriffsrechte können erforderlich sein.

Gruppenmitgliedschaften konfigurieren

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

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService). Dieser Dienst ist nur auf Servern sichtbar, die Teil einer Gruppe sind, und wird nur ausgeführt, während der Beitritt läuft.

Diese Gruppenmitgliedschaften sind erforderlich, damit StoreFront ordnungsgemäß funktioniert, um:

- Zertifikate erstellen, exportieren, importieren und löschen sowie Zugriffsrechte dafür festlegen

- Die Windows-Registrierung lesen und schreiben
- Microsoft .NET Framework-Assemblies im Global Assembly Cache (GAC) hinzufügen und entfernen
- Auf den Ordner **Program Files\\Citrix**<*StoreFrontLocation*> zugreifen
- IIS-Anwendungspool-Identitäten und IIS-Webanwendungen hinzufügen, ändern und entfernen
- Lokale Sicherheitsgruppen und Firewallregeln hinzufügen, ändern und entfernen
- Windows-Dienste und PowerShell-Snap-Ins hinzufügen und entfernen
- Microsoft Windows Communication Framework (WCF)-Endpunkte registrieren

Bei Updates für StoreFront kann sich diese Liste der Vorgänge ohne vorherige Ankündigung ändern.

Die StoreFront-Installation erstellt auch die folgenden lokalen Sicherheitsgruppen:

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSReplicators
- CitrixPNRSUsers
- CitrixStoreFrontAdministrators
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront verwaltet die Mitgliedschaft dieser Sicherheitsgruppen. Sie werden für die Zugriffssteuerung innerhalb von StoreFront verwendet und nicht auf Windows-Ressourcen wie Dateien und Ordner angewendet. Ändern Sie diese Gruppenmitgliedschaften nicht.

NTLM

Wenn Sie Favoriten über die lokale ESENT-Datenbank aktiviert haben, verwendet StoreFront möglicherweise NTLM, wenn Favoriten in einer Servergruppe synchronisiert werden. Wenn Sie

NTLM deaktivieren, schlägt die Synchronisierung der Favoriten möglicherweise fehl. Alternativ können Sie eine SQL Server-Datenbank verwenden.

Wenn sich Benutzer mit der Domänen-Pass-Through-Authentifizierung authentifizieren, verwendet IIS standardmäßig Kerberos, falls möglich, andernfalls wird auf NTLM zurückgegriffen. Befindet sich ein Lastenausgleich vor StoreFront, wird immer auf NTLM zurückgegriffen.

Sie können den Server so konfigurieren, dass er nur NTLMv2 verwendet und NTLMv1 ablehnt. Weitere Informationen finden Sie in der Microsoft-Dokumentation. In Windows Server 2025 und höher wurde NTLMv1 entfernt, sodass immer NTLMv2 verwendet wird.

Zertifikate in StoreFront

Serverzertifikate

Serverzertifikate werden für die Maschinenidentifikation und die Transport Layer Security (TLS)-Transportsicherheit in StoreFront verwendet. Wenn Sie die ICA-Dateisignierung aktivieren, kann StoreFront Zertifikate auch zum digitalen Signieren von ICA-Dateien verwenden.

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

Zertifikate für die Tokenverwaltung

Authentifizierungsdienste und Stores benötigen jeweils Zertifikate für die Tokenverwaltung. StoreFront generiert ein selbstsigniertes Zertifikat, wenn ein Authentifizierungsdienst oder Store erstellt wird. Von StoreFront generierte selbstsignierte Zertifikate sollten nicht für andere Zwecke verwendet werden.

Citrix Delivery Services-Zertifikate

StoreFront speichert eine Reihe von Zertifikaten in einem benutzerdefinierten Windows-Zertifikatspeicher (Citrix Delivery Services). Die Dienste Citrix Configuration Replication, Citrix Credential Wallet und Citrix Subscriptions Store verwenden diese Zertifikate. Jeder StoreFront-Server in einem Cluster verfügt über eine Kopie dieser Zertifikate. Diese Dienste verlassen sich nicht auf TLS für sichere Kommunikation, und diese Zertifikate werden nicht als TLS-Serverzertifikate verwendet. Diese Zertifikate werden erstellt, wenn ein StoreFront-Store erstellt oder StoreFront installiert wird. Ändern Sie den Inhalt dieses Windows-Zertifikatspeichers nicht.

Codesignaturzertifikate

StoreFront enthält eine Reihe von PowerShell-Skripten (.ps1) im Ordner unter <*InstallDirectory*>\Scripts. Die Standardinstallation von StoreFront verwendet diese Skripte nicht. Sie vereinfachen die Konfigurationsschritte für spezifische und seltene Aufgaben. Diese Skripte sind signiert, wodurch StoreFront die PowerShell-Ausführungsrichtlinie unterstützen kann. Wir empfehlen die Richtlinie **AllSigned**. (Die Richtlinie **Restricted** wird nicht unterstützt, da sie die Ausführung von PowerShell-Skripten verhindert.) StoreFront ändert die PowerShell-Ausführungsrichtlinie nicht.

Obwohl StoreFront kein Codesignaturzertifikat im Speicher für vertrauenswürdige Herausgeber installiert, kann Windows das Codesignaturzertifikat dort automatisch hinzufügen. Dies geschieht, wenn das PowerShell-Skript mit der Option **Immer ausführen** ausgeführt wird. (Wenn Sie die Option **Nie ausführen** wählen, wird das Zertifikat dem Speicher für nicht vertrauenswürdige Zertifikate hinzugefügt, und StoreFront-PowerShell-Skripte werden nicht ausgeführt.) Sobald das Codesignaturzertifikat dem Speicher für vertrauenswürdige Herausgeber hinzugefügt wurde, wird dessen Ablauf von Windows nicht mehr überprüft. Sie können dieses Zertifikat aus dem Speicher für vertrauenswürdige Herausgeber entfernen, nachdem die StoreFront-Aufgaben abgeschlossen wurden.

StoreFront-Sicherheitstrennung

Wenn Sie Webanwendungen auf Ihrem StoreFront-Server in derselben Webdomäne (Domänenname und Port) wie StoreFront bereitstellen, könnten Sicherheitsrisiken in diesen Webanwendungen potenziell die Sicherheit Ihrer StoreFront-Bereitstellung beeinträchtigen. Wo ein höheres Maß an Sicherheitstrennung erforderlich ist, empfiehlt Citrix, StoreFront in einer separaten Webdomäne bereitzustellen.

ICA-Downloads

ICA-Dateien enthalten die Informationen, um eine Verbindung zu VDAs herzustellen und sich oft ohne weitere Authentifizierung bei diesen anzumelden. Stellen Sie daher sicher, dass ICA-Dateien geschützt sind. Bei hybriden Starts können ICA-Dateien je nach Konfiguration auf das Gerät des Benutzers heruntergeladen werden. Es wird empfohlen, ICA-Downloads zu deaktivieren. Weitere Informationen finden Sie unter Starteinstellungen.

ICA-Dateisignierung

StoreFront bietet die Möglichkeit, ICA-Dateien mithilfe eines angegebenen Zertifikats auf dem Server digital zu signieren, sodass Versionen der Citrix Workspace-App, die diese Funktion unterstützen, überprüfen können, ob die Datei aus einer vertrauenswürdigen Quelle stammt. ICA-Dateien können mit jedem Hash-Algorithmus signiert werden, der vom Betriebssystem des StoreFront-Servers unterstützt wird, einschließlich SHA-1 und SHA-256. Weitere Informationen finden Sie unter ICA-Dateisignierung aktivieren.

App-Schutz

Sie können App Protection verwenden, um Bildschirmaufnahmen und Screen Logger zu verhindern. Bei hybriden Starts ist App Protection standardmäßig deaktiviert. Um sie zu aktivieren, siehe App Protection.

Kennwortänderung durch Benutzer

Sie können Benutzern, die sich über einen Webbrowser mit Active Directory-Domänenanmeldeinformationen anmelden, erlauben, ihre Kennwörter jederzeit oder nur bei Ablauf zu ändern. Dies macht jedoch sensible Sicherheitsfunktionen für jeden zugänglich, der auf einen der Stores zugreifen kann, die den Authentifizierungsdienst verwenden. Wenn Ihre Organisation eine Sicherheitsrichtlinie hat, die Kennwortänderungsfunktionen für Benutzer nur für den internen Gebrauch vorsieht, stellen Sie sicher, dass keiner der Stores von außerhalb Ihres Unternehmensnetzwerks zugänglich ist. Wenn Sie den Authentifizierungsdienst erstellen, verhindert die Standardkonfiguration, dass Benutzer ihre Kennwörter ändern, selbst wenn diese abgelaufen sind. Weitere Informationen finden Sie unter Benutzern das Ändern ihrer Kennwörter ermöglichen.

Anpassungen

Um die Sicherheit zu erhöhen, blockiert die Content Security Policy Skripte von anderen Servern. Beim Schreiben von Anpassungen legen Sie Skripte in den Website-Ordner `custom`. Wenn StoreFront für HTTPS-Verbindungen konfiguriert ist, stellen Sie sicher, dass alle Links zu benutzerdefinierten Inhalten oder Skripten ebenfalls HTTPS verwenden.

Sicherheits-Header

Beim Anzeigen einer Store-Website über einen Webbrowser gibt StoreFront die folgenden sicherheitsrelevanten Header zurück, die Einschränkungen für den Webbrowser festlegen.

HEADER-NAME	WERT	BESCHREIBUNG
`content-security-policy`	`frame-ancestors 'none'`	Dies verhindert, dass andere Websites StoreFront-Websites in einem Frame einbetten, wodurch Clickjacking-Angriffe vermieden werden. Zusätzlich enthält die HTML-Seite ein `meta`-Tag mit einem `content-security-policy`, das Skriptquellen einschränkt, um XSS-Angriffe zu mindern.
`X-Content-Type-Options`	`nosniff`	Dies verhindert MIME-Typ-Sniffing.
`X-Frame-Options`	`deny`	Dies verhindert, dass andere Websites StoreFront-Websites in einem Frame einbetten, wodurch Clickjacking-Angriffe vermieden werden. Es wird durch `content-security-policy` bis `frame-ancestors 'none'` obsolet, wird aber von einigen älteren Browsern verstanden, die `content-security-policy` nicht unterstützen.
`X-XSS-Protection`	`1; mode=block`	Wird von einigen Browsern verwendet, um XSS-Angriffe (Cross-Site-Scripting) zu verhindern.

`Strict-Transport-Security` ist standardmäßig nicht festgelegt, kann aber konfiguriert werden. Weitere Informationen finden Sie unter HSTS.

Cookies

StoreFront verwendet mehrere Cookies. Einige der beim Betrieb der Website verwendeten Cookies sind die folgenden:

COOKIE	BESCHREIBUNG
`ASP.NET_SessionId`	Verfolgt die Benutzersitzung einschließlich des Authentifizierungsstatus. Hat `HttpOnly` festgelegt.
`CtxsAuthId`	Um Session-Fixation-Angriffe zu verhindern, verfolgt StoreFront zusätzlich mit diesem Cookie, ob der Benutzer authentifiziert ist. Es hat `HttpOnly` festgelegt.
`CsrfToken`	Wird verwendet, um Cross-Site-Request-Forgery über das Standardmuster Cookie-to-header token zu verhindern. Der Server legt ein Token im Cookie fest. Der Client liest das Token aus dem Cookie und fügt das Token in die Abfragezeichenfolge oder einen Header in nachfolgenden Anfragen ein. Dieses Cookie muss `HttpOnly` nicht gesetzt haben, damit das Client-JavaScript es lesen kann.
`CtxsDeviceId`	Identifiziert das Gerät. Hat `HttpOnly` festgelegt.

StoreFront setzt eine Reihe weiterer Cookies, um den Benutzerstatus zu verfolgen, von denen einige von JavaScript gelesen werden müssen und daher `HttpOnly` nicht gesetzt haben. Diese Cookies enthalten keine Informationen zur Authentifizierung oder andere vertrauliche Informationen.

Wenn der Client über HTTPS verbunden ist, wird das Attribut `secure` beim Erstellen oder Aktualisieren von Cookies gesetzt.

Zusätzliche Sicherheitsinformationen

> **Hinweis:**

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

> Ihre Organisation möchte möglicherweise aus regulatorischen Gründen Sicherheitsüberprüfungen von StoreFront durchführen. Die vorstehenden Konfigurationsoptionen können dazu beitragen, einige Feststellungen in Sicherheitsüberprüfungsberichten zu eliminieren.

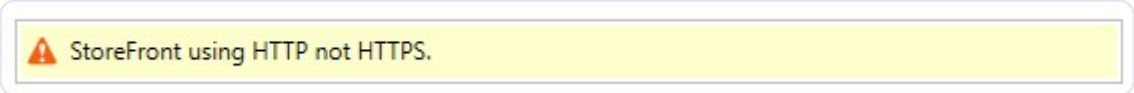
Wenn sich ein Gateway zwischen dem Sicherheitsscanner und StoreFront befindet, können sich bestimmte Feststellungen auf das Gateway und nicht auf StoreFront selbst beziehen. Sicherheitsüberprüfungsberichte unterscheiden diese Feststellungen (z. B. TLS-Konfiguration) normalerweise nicht. Aus diesem Grund können technische Beschreibungen in Sicherheitsüberprüfungsberichten irreführend sein.

StoreFront mit HTTPS sichern

Citrix empfiehlt dringend, die Kommunikation zwischen StoreFront und den Geräten der Benutzer mithilfe von HTTPS zu sichern. Dies stellt sicher, dass Passwörter und andere Daten, die zwischen dem Client und StoreFront gesendet werden, verschlüsselt sind. Darüber hinaus können einfache HTTP-Verbindungen durch verschiedene Angriffe, wie z. B. Man-in-the-Middle-Angriffe, kompromittiert werden, insbesondere wenn Verbindungen von unsicheren Standorten wie öffentlichen Wi-Fi-Hotspots hergestellt werden. Ohne die entsprechende IIS-Konfiguration verwendet StoreFront HTTP für die Kommunikation.

Je nach Konfiguration können Benutzer über ein Gateway oder einen Lastenausgleich auf StoreFront zugreifen. Sie können die HTTPS-Verbindung am Gateway oder Lastenausgleich beenden. In diesem Fall empfiehlt Citrix jedoch weiterhin, dass Sie sichere Verbindungen zwischen dem Gateway, dem Lastenausgleich und StoreFront über HTTPS herstellen. Bei Verwendung eines NetScaler-Lastenausgleichs finden Sie die Zertifikatsanforderungen unter dem Link Serverzertifikat-Supportmatrix auf der ADC-Appliance.

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



Zertifikat erstellen oder importieren

- Stellen Sie sicher, dass die StoreFront-Basis-URL im DNS-Feld als Common Name oder Subject Alternative Name (SANs) enthalten ist. Wenn Sie einen Lastenausgleich vor Ihren StoreFront-Servern verwenden, wird empfohlen, sowohl den Server-FQDN als auch den

Lastenausgleich-FQDN als SANs aufzunehmen. Dies ermöglicht Ihnen, sich zur Fehlerbehebung direkt mit einem bestimmten StoreFront-Server zu verbinden.

- Signieren Sie das Zertifikat mit einer Unternehmens-Stammzertifizierungsstelle (CA) für Ihre Organisation oder einer öffentlichen CA.
- Wenn Benutzer über einen Lastenausgleich oder ein Gateway auf StoreFront zugreifen, muss das Zertifikat nur vom Lastenausgleich oder Gateway als vertrauenswürdig eingestuft werden. Wenn Benutzer sich direkt mit dem StoreFront-Server verbinden, müssen die Clients dem Zertifikat vertrauen.

Sie müssen ein Zertifikat im Zertifikatspeicher **Persönlich** unter Windows erstellen oder importieren. So zeigen Sie installierte Zertifikate an:

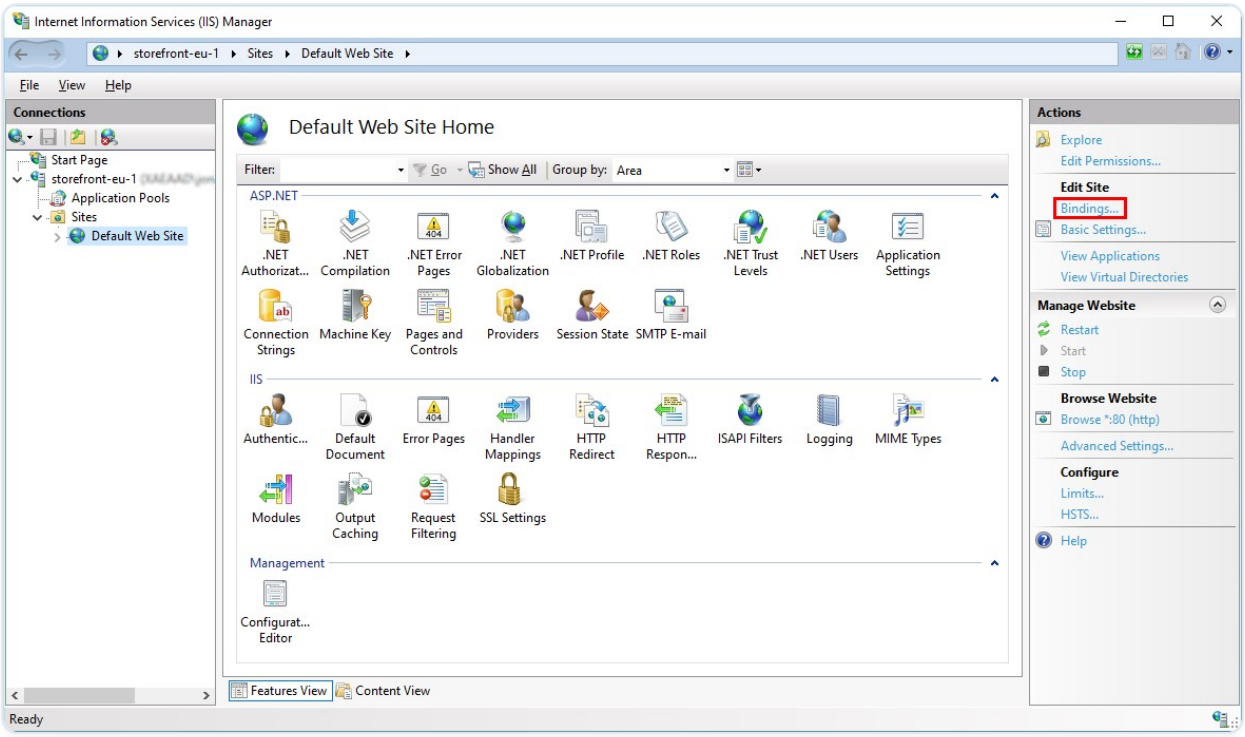
1. Öffnen Sie den **IIS-Manager (Internetinformationsdienste)**.
2. Wählen Sie im Bereich **Verbindungen** den Server aus.
3. Öffnen Sie **Serverzertifikate**.

Weitere Informationen zur Verwaltung von Zertifikaten finden Sie unter Zertifikate verwalten.

IIS für HTTPS konfigurieren

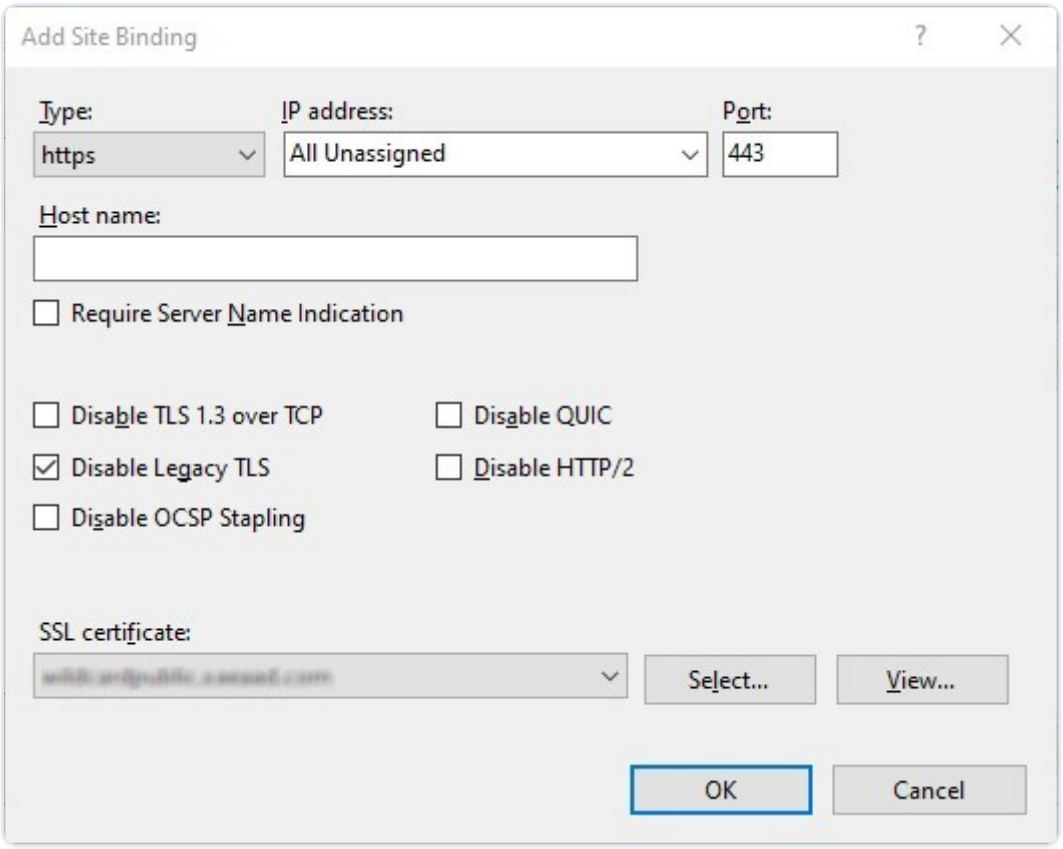
So konfigurieren Sie Microsoft Internet Information Services (IIS) für HTTPS auf dem StoreFront-Server:

1. Wählen Sie in der Strukturansicht auf der linken Seite **Default Web Site** (oder die entsprechende Website) aus.
2. Klicken Sie im Bereich Aktionen auf **Bindungen...**

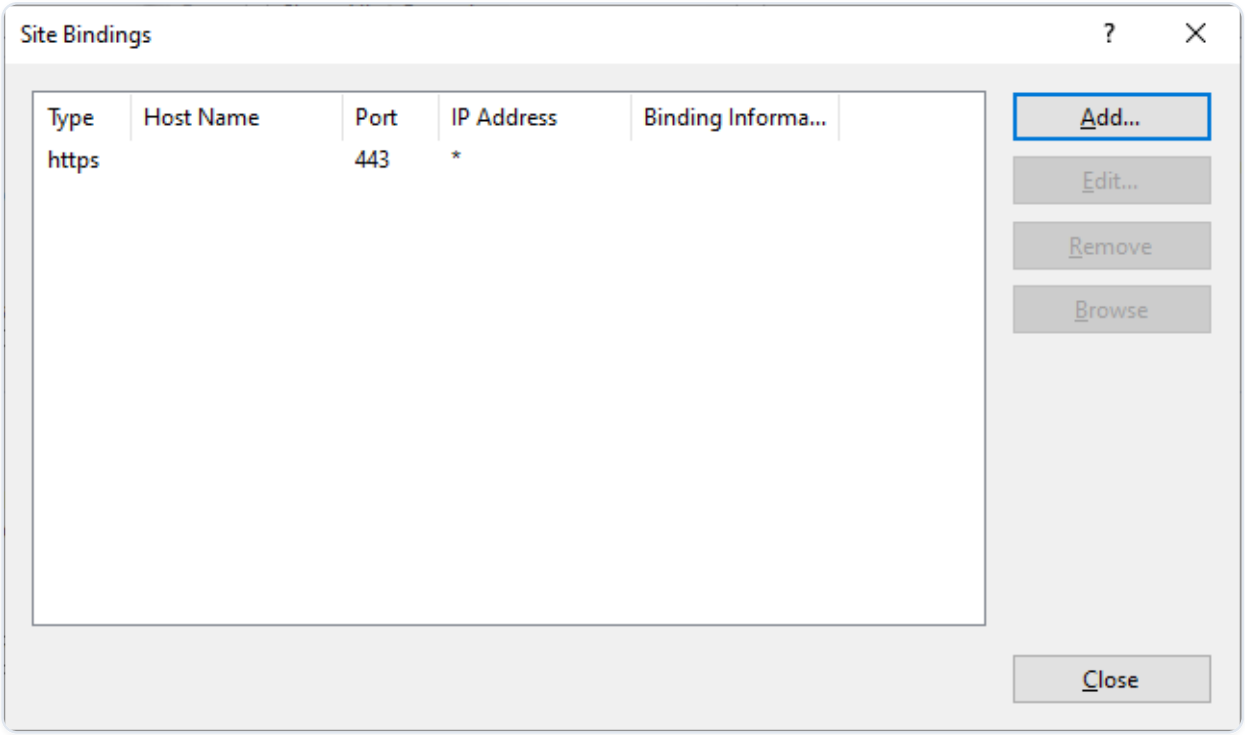


3. Klicken Sie im Fenster Bindungen auf **Hinzufügen...**
4. Wählen Sie in der Dropdown-Liste **Typ** die Option **https** aus.
5. Klicken Sie unter Windows Server 2022 oder höher auf **Legacy-TLS deaktivieren**, um TLS-Versionen älter als 1.2 zu deaktivieren.

   Auf älteren Windows Server-Versionen können Sie ältere TLS-Versionen mithilfe von Windows-Registrierungseinstellungen deaktivieren. Siehe Windows Server-Dokumentation.
6. Wählen Sie das zuvor importierte Zertifikat aus. Drücken Sie OK.



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



8. Aktualisieren Sie die Basis-URL, um das HTTPS-Protokoll zu verwenden.

HSTS

Das Clientgerät des Benutzers ist auch dann anfällig, wenn Sie HTTPS auf der Serverseite aktiviert haben. Beispielsweise könnte ein Man-in-the-Middle-Angreifer den StoreFront-Server fälschen und den Benutzer dazu verleiten, sich über unverschlüsseltes HTTP mit dem gefälschten Server zu verbinden. Dadurch könnten sie Zugriff auf sensible Informationen wie die Anmeldeinformationen des Benutzers erhalten. Die Lösung besteht darin, sicherzustellen, dass der Browser des Benutzers nicht versucht, über HTTP auf den Server zuzugreifen. Dies erreichen Sie mit HTTP Strict Transport Security (HSTS).

Wenn HSTS aktiviert ist, weist der Server Webbrowser an, dass Anfragen an die Website immer nur über HTTPS erfolgen sollen. Wenn ein Benutzer versucht, die URL über HTTP aufzurufen, wechselt der Browser automatisch zu HTTPS. Dies gewährleistet eine clientseitige Validierung einer sicheren Verbindung sowie die serverseitige Validierung in IIS. Der Webbrowser behält diese Validierung für einen konfigurierten Zeitraum bei.

> **Hinweis:**
>
> Das Aktivieren von HSTS betrifft alle Websites auf derselben Domäne. Wenn die Website beispielsweise unter `https://www.company.com/Citrix/StoreWeb` zugänglich ist, gilt die HSTS-Richtlinie für alle Websites unter `https://www.company.com`, was möglicherweise nicht erwünscht ist.
>
> Es gibt mehrere Optionen zum Aktivieren von HSTS. Sie sollten nur eine Option wählen, um zu vermeiden, dass derselbe Header mehrmals gesetzt wird.

Option 1 – IIS

Ab Windows Server 2019 können Sie HSTS in IIS konfigurieren.

1. Öffnen Sie den **Internetinformationsdienste (IIS)-Manager**.
2. Wählen Sie **Standardwebsite** (oder die entsprechende Website) aus.
3. Klicken Sie im Aktionsbereich auf der rechten Seite auf **HSTS...**.
4. Wählen Sie **Aktivieren**.
5. Geben Sie ein maximales Alter ein, z. B. 31536000 für ein Jahr.
6. Wählen Sie optional **HTTP zu HTTPS umleiten**.
7. Drücken Sie **OK**.

Screenshot der HSTS-Einstellung(/en-us/storefront/2507-ltsr/media/secure/iis-hsts.png)

Option 2 – StoreFront™-Verwaltungskonsole

Für jede Store-Website:

1. Wählen Sie den Store aus und klicken Sie auf **Websites verwalten**.
2. Wählen Sie die Website aus und klicken Sie auf **Konfigurieren...**.
3. Gehen Sie zur Registerkarte **Erweiterte Einstellungen**.
4. Wählen Sie **Strikte Transportsicherheit aktivieren**.
5. Aktualisieren Sie **Dauer der Richtlinie für strikte Transportsicherheit** auf den erforderlichen Wert.
6. Klicken Sie auf **OK**.

Option 3 – NetScaler®-Lastenausgleich

Wenn Sie einen NetScaler-Lastenausgleich vor Ihren StoreFront-Servern verwenden, können Sie HSTS auf dem virtuellen Server konfigurieren. Weitere Informationen finden Sie in der NetScaler-Dokumentation.

Option 4 – NetScaler Gateway

Wenn Benutzer über ein NetScaler Gateway eine Verbindung zu StoreFront herstellen, können Sie HSTS auf dem virtuellen VPN-Server konfigurieren. Dies hat den Vorteil, dass es sowohl für das NetScaler-Anmeldeformular als auch für die von StoreFront gehosteten Seiten gilt.

Überprüfung der Zertifikatsperrliste (CRL)

Einführung

Sie können StoreFront so konfigurieren, dass der Status von TLS-Zertifikaten, die von CVAD-Delivery Controllern verwendet werden, mithilfe einer veröffentlichten Zertifikatsperrliste (CRL) überprüft wird. Möglicherweise müssen Sie den Zugriff auf ein Zertifikat widerrufen, wenn:

- Sie glauben, dass der private Schlüssel kompromittiert wurde
- die CA kompromittiert ist
- die Zugehörigkeit geändert wurde
- das Zertifikat ersetzt wurde

> **Hinweis:**

> Dieses Thema ist nur relevant, wenn HTTPS-Verbindungen zwischen StoreFront und Citrix Virtual Apps and Desktops Delivery Controllern verwendet werden. HTTP-Verbindungen zu Delivery Controllern erfordern kein Zertifikat, daher hat die hier beschriebene Einstellung -CertRevocationPolicy für den Store keine Auswirkung.

> StoreFront unterstützt die Überprüfung des Zertifikatswiderrufs mithilfe von CRL Distribution Point (CDP)-Zertifikatserweiterungen und lokal installierten Zertifikatsperrlisten (CRLs). StoreFront unterstützt nur vollständige CRLs: Delta-CRLs werden nicht unterstützt.

CRL-Verteilungspunkte (CDP)-Erweiterungen

StoreFront listet keine Ressourcen von Citrix Virtual Apps and Desktops Delivery Controllern auf, die widerrufene Zertifikate verwenden, deren Seriennummern in der veröffentlichten CRL aufgeführt sind. Um zu erkennen, welche Zertifikate widerrufen wurden, muss StoreFront in der Lage sein, auf die veröffentlichte CRL zuzugreifen, indem eine der in den CDP-Zertifikatserweiterungen definierten URLs verwendet wird.

Screenshot eines Zertifikats mit CLR-Erweiterungspunkterweiterungen(/en-us/storefront/2507-ltsr/media/stores/clr-distribution-point-extensions-blur.png)

CRL-Veröffentlichungsintervall

Damit StoreFront widerrufene Zertifikate auf dem Delivery Controller schneller erkennt, reduzieren Sie das CRL-Veröffentlichungsintervall auf der CA. Bearbeiten Sie die Eigenschaften der CLR-Verteilungspunkte-Erweiterung, um einen niedrigeren CLR-Veröffentlichungsintervallwert festzulegen, der für Ihre Public-Key-Infrastruktur geeignet ist.

Eigenschaften des widerrufenen Zertifikats(/en-us/storefront/2507-ltsr/media/stores/revoked-certificate-properties.png)

Client-CRL-Caching

Der Windows-Client für die Public Key Infrastructure speichert CRLs lokal zwischen. Eine aktuellere CRL wird erst heruntergeladen, wenn die lokal zwischengespeicherte CRL abgelaufen ist.

Zugriff von StoreFront auf Zertifikatsperrlisten (CRLs)

Die Überprüfung des Zertifikatswiderrufs hängt von der Fähigkeit von StoreFront ab, auf CRLs zuzugreifen. Überlegen Sie sorgfältig, wie StoreFront den Webserver oder die Zertifizierungsstelle (CA) kontaktiert, die die CRL veröffentlicht, und wie StoreFront CRL-Updates empfängt.

Interne Unternehmens-CAs und private Zertifikate auf Delivery Controllern

Um private CAs und Zertifikate zu verwenden, benötigt StoreFront eine korrekt konfigurierte Unternehmens-CA und eine veröffentlichte CRL, auf die es innerhalb Ihrer Organisation und Ihres internen Netzwerks zugreifen kann. Informationen zum Konfigurieren der Unternehmens-CA zum Veröffentlichen von CDP-Erweiterungen finden Sie in der Microsoft-Dokumentation. Alle Zertifikate auf Ihren Delivery Controllern, die vor der Konfiguration der CA zur Aufnahme von CDP-Erweiterungen existierten, müssen möglicherweise neu ausgestellt werden.

Es ist typisch, dass StoreFront- und Citrix Virtual Apps and Desktops-Server in isolierten privaten Netzwerken ohne Internetzugang betrieben werden. In diesem Szenario sollten private CAs verwendet werden.

Externe öffentliche CAs und öffentliche Zertifikate auf Delivery Controllern

StoreFront-Server und Citrix Virtual Apps and Desktops Delivery Controller können Zertifikate verwenden, die von öffentlichen CAs ausgestellt wurden. StoreFront muss in der Lage sein, den Webserver der öffentlichen CA über das Internet zu kontaktieren, indem es die in den CDP-Erweiterungen referenzierte URL verwendet. Wenn StoreFront nach dem Widerruf eines öffentlichen Zertifikats keine Kopie der CRL über eine CDP-URL herunterladen kann, kann StoreFront die CRL-Prüfung nicht durchführen.

Zertifikatswiderrufsrichtlinie anzeigen

Um die Richtlinieneinstellung mit PowerShell anzuzeigen, führen Sie das Cmdlet `Get-STFStoreFarmConfiguration` aus und zeigen Sie im resultierenden Objekt die Eigenschaft `CertRevocationPolicy` an. Zum Beispiel:

```
$store=Get-STFStoreService -VirtualPath '/Citrix/Store'

(Get-STFStoreFarmConfiguration -StoreService $store).CertRevocationPolicy
```

Zertifikatswiderrufsrichtlinie konfigurieren

Um die Zertifikatswiderrufsrichtlinie für einen Store mit PowerShell festzulegen, führen Sie das Cmdlet `Set-STFStoreFarmConfiguration` mit dem Parameter `-CertRevocationPolicy` aus.

Die Option `CertRevocationPolicy` kann auf die folgenden Werte eingestellt werden:

EINSTELLUNG	BESCHREIBUNG
NoCheck	StoreFront überprüft den Widerrufsstatus des Zertifikats auf dem Delivery Controller nicht. StoreFront listet weiterhin Ressourcen von Delivery Controllern auf, die widerrufene Zertifikate verwenden. Dies ist die Standardeinstellung.
MustCheck	Dies ist die sicherste Option. StoreFront versucht, eine CRL zu erhalten, indem es die in den CDP-Erweiterungen des Zertifikats auf dem Delivery Controller referenzierten URLs kontaktiert. StoreFront kann keine Enumeration vom Delivery Controller durchführen, wenn die CRL nicht verfügbar ist oder wenn das auf dem Delivery Controller verwendete Zertifikat widerrufen wurde. 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 CA ausgestellt wurde.
FullCheck	StoreFront versucht, die in den CDP-Erweiterungen des Delivery Controller-Zertifikats veröffentlichten URLs zu kontaktieren. Wenn StoreFront keine Kopie der CRL von den URLs abrufen kann, erlaubt es dennoch die Enumeration von Ressourcen vom Delivery Controller. Wenn StoreFront die CRL erfolgreich abruft und das Zertifikat des Delivery Controllers widerrufen wurde, enumeriert StoreFront keine Ressourcen. 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 CA ausgestellt wurde.

EINSTELLUNG	BESCHREIBUNG
NoNetworkAccess	Es werden nur CRLs geprüft, die lokal in den Zertifikatspeicher der Citrix Delivery Server auf dem StoreFront-Server importiert wurden. StoreFront versucht nicht, die in den CDP-Erweiterungen angegebenen URLs zu kontaktieren. Wenn StoreFront keine lokale Kopie der CRL abrufen kann, erlaubt es dennoch die Enumeration von Ressourcen vom Delivery Controller. Wenn StoreFront erfolgreich eine lokale Kopie der CRL aus dem Zertifikatspeicher der Citrix Delivery Server abruft und das Zertifikat des Delivery Controllers widerrufen wurde, enumeriert StoreFront keine Ressourcen.

Zum Beispiel:

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

$StoreObject = Get-STFStoreService -VirtualPath $StoreVirtualPath

Set-STFStoreFarmConfiguration -StoreService $StoreObject
-CertRevocationPolicy "MustCheck"
```

Wenn Sie mehrere Stores haben, wiederholen Sie dieses Verfahren für alle. -CertRevocationPolicy ist eine Store-Einstellung, die alle Delivery Controller betrifft, die für den in $StoreVirtualPath angegebenen Store konfiguriert sind.

Verwenden von lokal importierten CRLs auf dem StoreFront-Server

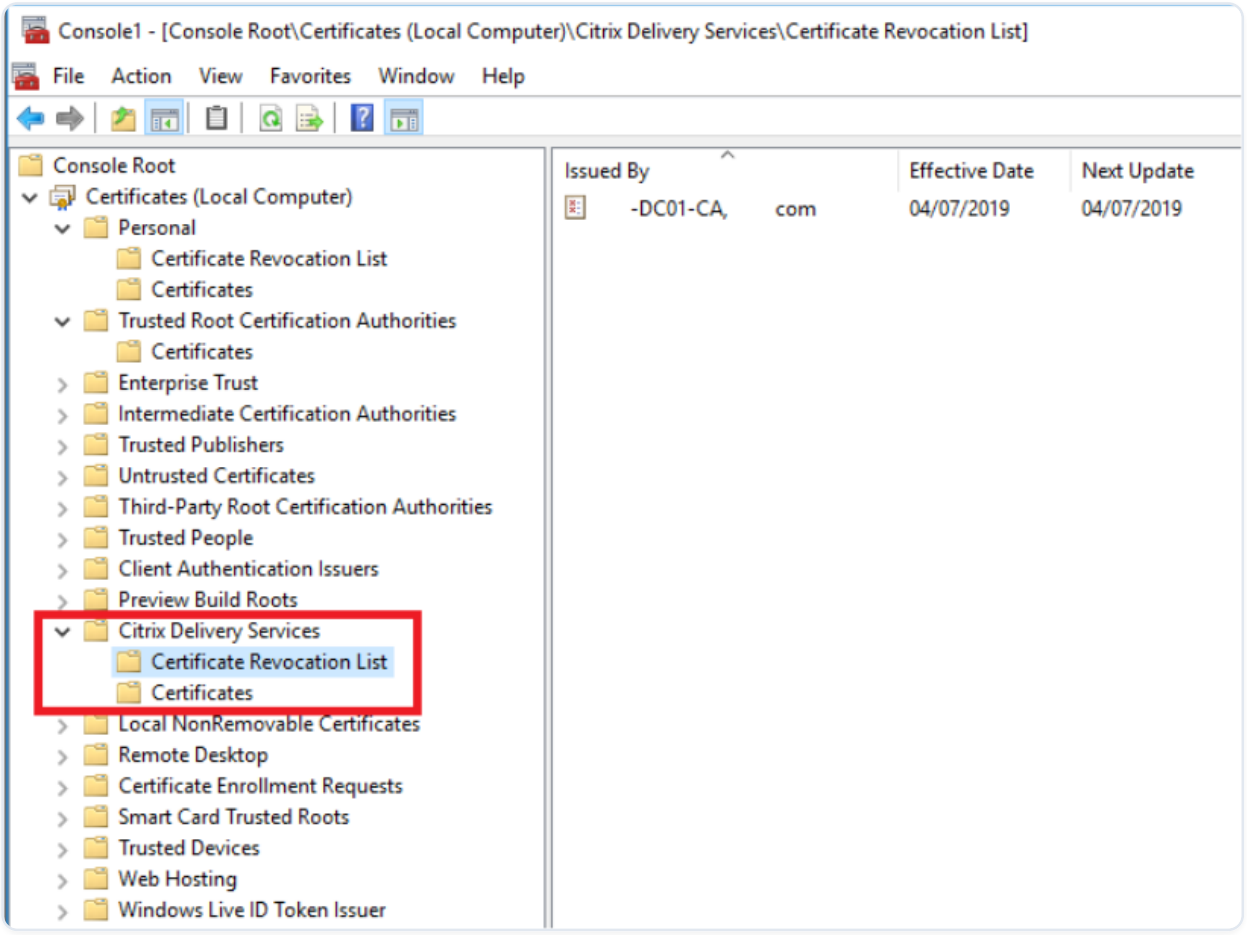
Die Verwendung von lokal importierten CRLs wird unterstützt, aber Citrix® empfiehlt dies nicht, weil:

- Sie in großen Unternehmensbereitstellungen, in denen mehrere StoreFront-Servergruppen beteiligt sein können, schwierig zu verwalten und zu aktualisieren sind.
- Das manuelle Aktualisieren von CRLs auf jedem StoreFront-Server, jedes Mal, wenn ein Zertifikat widerrufen wird, ist viel weniger effizient als die Verwendung von CDP-Erweiterungen und veröffentlichten CRLs in der gesamten Active Directory-Domäne.

Lokal installierte oder aktualisierte CRLs können verwendet werden, wenn -CertRevocationPolicy auf „NoNetworkAccess“ gesetzt ist und Sie die Möglichkeit haben, die CRL effizient auf alle StoreFront-Server zu verteilen.

So verwenden Sie lokal importierte CLRs

1. Kopieren Sie die CRL auf den Desktop des StoreFront-Servers. Wenn der StoreFront-Server Teil einer Servergruppe ist, kopieren Sie sie auf alle StoreFront-Server in der Gruppe.
2. Öffnen Sie das MMC-Snap-In und wählen Sie **Datei > Snap-Ins hinzufügen/entfernen > Zertifikate > Computerkonto > Citrix Delivery Services-Zertifikatspeicher**.
3. Rechtsklicken Sie und wählen Sie **Alle Aufgaben > Importieren**, navigieren Sie dann zur .CRL-Datei und wählen Sie **Alle Dateien auswählen > Öffnen > Alle Zertifikate im folgenden Speicher platzieren > Citrix Delivery Services**.



So fügen Sie die CRL dem Citrix Delivery Services-Zertifikatspeicher über PowerShell oder die Befehlszeile hinzu

1. Melden Sie sich bei StoreFront an und kopieren Sie die .CRL-Datei auf den Desktop des aktuellen Benutzers.
2. Öffnen Sie die PowerShell ISE und wählen Sie **Als Administrator ausführen**.

3. Führen Sie Folgendes 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 Beispiel verwenden, um die CRL automatisch über Skripte 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. Benutzer können sich nicht bei StoreFront anmelden, wenn das Zertifikat auf dem Delivery Controller widerrufen 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, der für ihre Authentifizierung zuständig ist, widerrufen wurde.

So delegieren Sie die Benutzerauthentifizierung an Delivery Controller

1. Konfigurieren Sie den Store für den Zertifikatswiderruf, wie im vorherigen Abschnitt Einen Store für die Überprüfung des Zertifikatswiderrufs konfigurieren beschrieben.
2. Konfigurieren Sie den Delivery Controller für die Verwendung von HTTPS, indem Sie das Verfahren befolgen, das unter XML-dienstbasierte Authentifizierung beschrieben ist.

Einen XML-Authentifizierungsdienst für die Überprüfung des Zertifikatswiderrufs konfigurieren

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

Hinweis:

StoreFront unterstützt zwei Modelle für die Zuordnung von Stores zu einem Authentifizierungsdienst. Der empfohlene Ansatz ist eine Eins-zu-Eins-Zuordnung zwischen Store und Authentifizierungsdienst. In diesem Fall müssen Sie die Schritte in diesem Abschnitt für alle Stores und ihre jeweiligen Authentifizierungsdienste ausführen.

Stellen Sie sicher, dass der Zertifikatsperrmodus für den Store und den Authentifizierungsdienst auf denselben Wert eingestellt ist. Alternativ können, wenn die Authentifizierungskonfiguration für alle Stores identisch ist, mehrere Stores so konfiguriert werden, dass sie einen einzigen Authentifizierungsdienst gemeinsam nutzen.

Die PowerShell-Cmdlets des Authentifizierungsdienstes haben kein Äquivalent zu **Set-STFStoreFarmConfiguration**, daher ist ein etwas anderer PowerShell-Ansatz erforderlich. Verwenden Sie die gleichen Einstellungen für die Zertifikatsperrrichtlinie, 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"
```

2. Wählen Sie den Store-Dienst, den Authentifizierungsdienst und den Delivery Controller™ aus, die für die XML-Authentifizierung verwendet werden sollen. 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
```

3. Ändern Sie die Eigenschaft CertRevocationPolicy des Authentifizierungsdienstes direkt.

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"

$AuthObject.Save()

Enable-STFXmlServiceAuthentication -AuthenticationService $AuthObject
-Farm $FarmObject
```

4. Bestätigen Sie, dass Sie den korrekten Zertifikatsperrmodus eingestellt haben.

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
$AuthVirtualPath

$AuthObject.FarmsConfiguration.CertRevocationPolicy
```

Zu erwartende Fehler in der Windows-Ereignisanzeige

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

So öffnen Sie die Ereignisanzeige:

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

Beispielfehler: Store kann keinen Delivery Controller mit einem gesperrten Zertifikat kontaktieren

```
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.
```

Beispielfehler: Von Receiver for Web, wenn sich der Benutzer aufgrund fehlgeschlagener XML-Authentifizierung nicht anmelden kann

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



Citrix.DeliveryServicesClients.Authentication.Exceptions.ExplicitAuthentic
ationFailure,

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.GetExplicitA
```

```
uthResult(ActionType

type, Dictionary`2 postParams)
```

ICA®-Dateisignierung

StoreFront bietet die Möglichkeit, ICA-Dateien digital zu signieren, sodass Versionen der Citrix Workspace-App, die diese Funktion unterstützen, überprüfen können, ob die Datei aus einer vertrauenswürdigen Quelle stammt. Wenn die Dateisignierung in StoreFront aktiviert ist, wird die ICA-Datei, die generiert wird, wenn ein Benutzer eine Anwendung startet, mit einem Zertifikat aus dem persönlichen Zertifikatspeicher des StoreFront-Servers signiert. ICA-Dateien können mit jedem Hash-Algorithmus signiert werden, der vom Betriebssystem des StoreFront-Servers unterstützt wird. Die digitale Signatur wird von Clients ignoriert, die die Funktion nicht unterstützen oder nicht für die ICA-Dateisignierung konfiguriert sind. Wenn der Signiervorgang fehlschlägt, wird die ICA-Datei ohne digitale Signatur generiert und an die Citrix Workspace-App gesendet, deren Konfiguration bestimmt, ob die unsignierte Datei akzeptiert wird.

Für die ICA-Dateisignierung mit StoreFront müssen Zertifikate den privaten Schlüssel enthalten und innerhalb des zulässigen Gültigkeitszeitraums liegen. Wenn das Zertifikat eine Schlüsselverwendungserweiterung enthält, muss diese die Verwendung des Schlüssels für digitale Signaturen zulassen. Wenn eine erweiterte Schlüsselverwendungserweiterung enthalten ist, muss diese auf Codesignierung oder Serverauthentifizierung eingestellt sein.

Für die ICA-Dateisignierung empfiehlt Citrix®, ein Codesignatur- oder SSL-Signaturzertifikat zu verwenden, das von einer öffentlichen Zertifizierungsstelle oder von der privaten Zertifizierungsstelle Ihrer Organisation bezogen wurde. Wenn Sie kein geeignetes Zertifikat von einer Zertifizierungsstelle erhalten können, können Sie entweder ein vorhandenes SSL-Zertifikat, z. B. ein Serverzertifikat, verwenden oder ein neues Stammzertifizierungsstellenzertifikat erstellen und an die Geräte der Benutzer verteilen.

Die ICA-Dateisignierung ist standardmäßig deaktiviert. Um die ICA-Dateisignierung zu aktivieren, müssen Sie ein Zertifikat installieren und den Store so konfigurieren, dass er dieses Zertifikat verwendet. Das Signieren der ICA-Datei hat keine Auswirkung, es sei denn, Sie konfigurieren auch die Citrix Workspace-App für Windows so, dass ein Zertifikat erforderlich ist. Weitere Informationen finden Sie unter ICA-Dateisignierung.

> Hinweis:

> Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zur Verwaltung Ihrer StoreFront-Konfiguration verwenden. Schließen Sie ebenso alle PowerShell-Instanzen, bevor Sie die StoreFront-Konsole öffnen.

1. Öffnen Sie auf Ihrem StoreFront-Server **Computerzertifikate verwalten**.
2. Fügen Sie Ihr Zertifikat dem Zertifikatspeicher **Citrix Delivery Services** hinzu.
3. Öffnen Sie das Zertifikat, wechseln Sie zur Registerkarte **Details** und notieren Sie den Fingerabdruck.
4. Aktivieren Sie die Signierung für einen Store mit dem PowerShell-Cmdlet Set-STFStoreService:

   ```
   $storeService = Get-STFStoreService

   Set-STFStoreService $storeService -IcaFileSigning $true
   -IcaFileSigningCertificateThumbprint [certificatethumbprint]
   ```

   Dabei ist der Digest (oder Fingerabdruck) der Zertifikatsdaten, der vom Hash-Algorithmus erzeugt wird.

   Wenn Sie einen anderen Hash-Algorithmus als SHA-1 verwenden möchten, fügen Sie einen Parameter **-IcaFileSigningHashAlgorithm** hinzu, der je nach Bedarf auf sha256, sha384 oder sha512 gesetzt ist.

Protokolle und Analysen

StoreFront generiert eine Reihe von Protokolldateien und Telemetriedaten. Siehe die folgenden Themen.

THEMA	BESCHREIBUNG
Protokolldateien	StoreFront erstellt verschiedene Protokolldateien für Diagnosezwecke.
Ereignisprotokolle	StoreFront schreibt wichtige Ereignisse und Fehler in das Windows-Ereignisprotokoll.
Leistungsindikatoren	StoreFront zeichnet Leistungsindikatoren auf, die Sie mit dem Leistungsmonitor anzeigen können.
Telemetrie	StoreFront sendet Informationen zu Ihrer Konfiguration an Citrix Cloud.
Citrix Workspace-App-Analysen	Konfigurieren Sie die Citrix Workspace-App so, dass Daten an Citrix Analytics gesendet werden.
Citrix Scout	Führen Sie Citrix Scout aus, um Protokolldateien und andere Systeminformationen zur Übermittlung an den Support zu sammeln.

Protokolldateien

Installationsprotokolle

Wenn StoreFront installiert oder deinstalliert wird, erstellt das StoreFront-Installationsprogramm die folgenden Protokolldateien im Verzeichnis *C:\Windows\Temp\StoreFront*. Die Dateinamen spiegeln die Komponenten wider, die sie erstellt haben, und enthalten Zeitstempel.

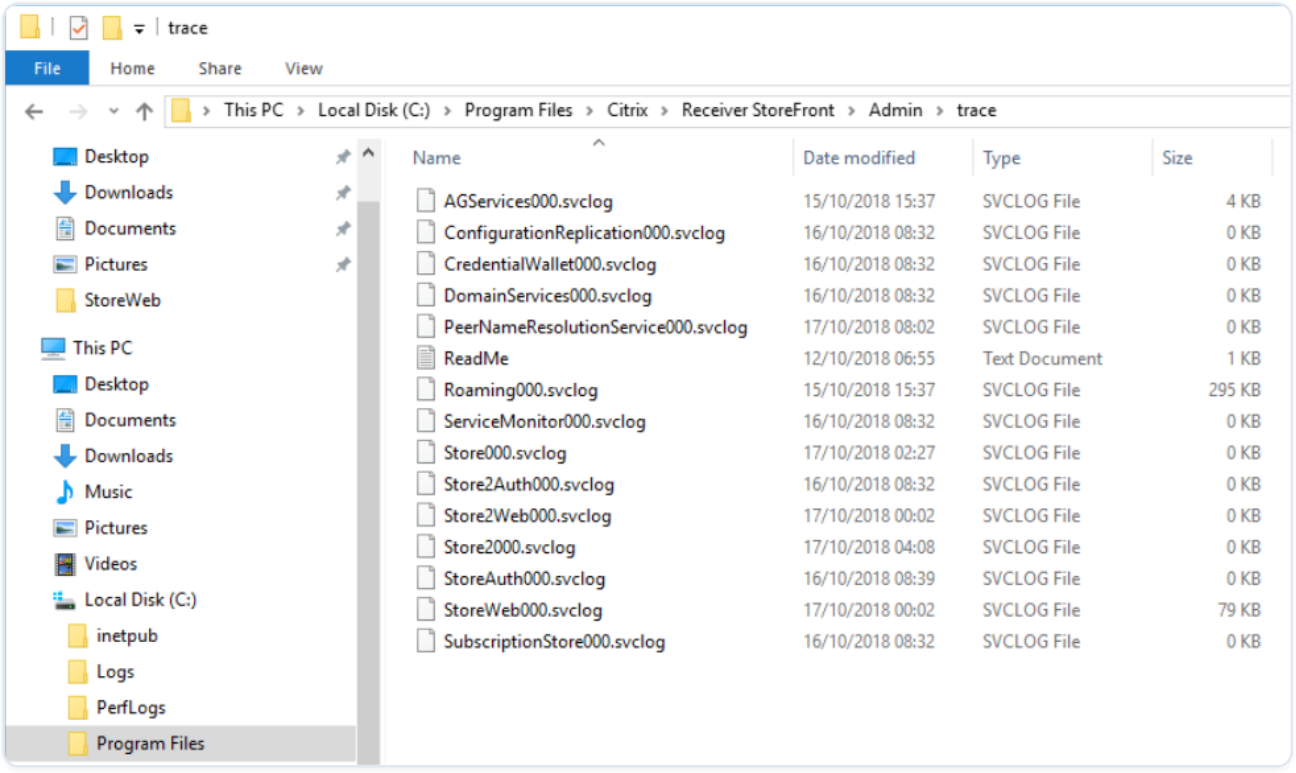
- Citrix-DeliveryServicesRoleManager-*.log – Wird erstellt, wenn StoreFront interaktiv installiert wird.
- Citrix-DeliveryServicesSetupConsole-*.log – Wird erstellt, wenn StoreFront unbeaufsichtigt installiert und wenn StoreFront deinstalliert wird, entweder interaktiv oder unbeaufsichtigt.
- CitrixMsi-CitrixStoreFront-x64-*.log – Wird erstellt, wenn StoreFront installiert und deinstalliert wird, entweder interaktiv oder unbeaufsichtigt.

PowerShell- und Verwaltungskonsolenprotokolle

Konfigurationsänderungen, die über PowerShell oder die Verwaltungskonsole vorgenommen werden, werden unter `C:\Program Files\Citrix\Receiver StoreFront\Admin\logs` protokolliert. Die Protokolldateinamen enthalten Befehlsaktionen und -subjekte sowie Zeitstempel, die zur Unterscheidung von Befehlssequenzen verwendet werden können.

Diagnoseprotokollierung

StoreFront schreibt Diagnoseprotokolle nach `c:\Program Files\Citrix\Receiver StoreFront\admin\trace`



Standardmäßig werden Meldungen der Stufen **Error**, **Warning** und **Info** protokolliert. In den meisten Fällen enthält dies ausreichende Informationen, um Probleme zu diagnostizieren.

Um die Protokollierung mit PowerShell anzupassen, führen Sie das Cmdlet `Set-STFDiagnostics` aus.

- StoreFront schreibt für jeden Dienst eine separate Protokolldatei. Standardmäßig ist jede Protokolldatei bis zu 200 MB groß, und StoreFront schreibt bis zu fünf Protokolldateien pro Dienst, bevor alte Protokolldateien gelöscht werden. Wenn Sie die Größe oder Anzahl der geschriebenen Protokolle anpassen müssen, können Sie dies mit den Parametern `-FileSizeKb` und `-FileCount` tun.
- Um den Detaillierungsgrad der Protokollierung zu ändern, verwenden Sie den Parameter `-TraceLevel`. Zulässige Werte sind `Off`, `Error`, `Warning`, `Info` oder `Verbose`.
- Um die Protokollierungsparameter für alle Dienste festzulegen, verwenden Sie den Parameter `-All`. Sie können die Protokollierung für einen einzelnen Dienst mit `-Service [Service name]` anpassen.

Ausführliche Protokollierung

Sie können zusätzliche ausführliche Protokollierung zu Fehlerbehebungszwecken aktivieren. Dies ist nur erforderlich, wenn vom Citrix® Support angefordert. Dies kann sich auf die Leistung auswirken, daher sollten Sie die `TraceLevel` auf `Info` zurücksetzen, sobald die Fehlerbehebung abgeschlossen ist.

So aktivieren Sie die ausführliche Protokollierung:

1. Starten Sie Windows PowerShell mit einem Konto mit lokalen Administratorberechtigungen
2. Geben Sie den Befehl ein:

   ```
   Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
   ```

   Dies aktiviert die „ausführliche“ Protokollierung für alle Dienste, ohne zur Bestätigung aufzufordern. Wenn dieser Befehl eingegeben wird, werden die StoreFront-Dienste neu gestartet. Warten Sie, bis die PowerShell-Eingabeaufforderung zurückkehrt, um zu überprüfen, ob die Dienste neu gestartet wurden. Während diese Dienste neu gestartet werden, ist der StoreFront-Server für Benutzer nicht zugänglich.
3. Reproduzieren Sie das Problem, um die Protokolle zu erstellen.
4. Setzen Sie die Protokollierung für alle Dienste auf die Standardstufe zurück

   ```
   Set-STFDiagnostics -All -TraceLevel "Info" -confirm:$False
   ```

IIS-Protokolldateien

Standardmäßig schreibt IIS ein Protokoll jeder Anforderung nach `%SystemDrive%\inetpub\logs\LogFiles`. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

Ereignisprotokoll

StoreFront unterstützt die Windows-Ereignisprotokollierung für den Authentifizierungsdienst, Stores und Websites. Alle generierten Ereignisse werden in das StoreFront-Anwendungsprotokoll geschrieben, das mit der Ereignisanzeige unter **Anwendungs- und Dienstprotokolle > Citrix Delivery Services** oder **Windows-Protokolle > Anwendung** angezeigt werden kann. Sie können die Anzahl doppelter Protokolleinträge für ein einzelnes Ereignis steuern, indem Sie die Konfigurationsdateien für den Authentifizierungsdienst, Stores und Websites bearbeiten.

Protokolldrosselung

1. Öffnen Sie mit einem Texteditor die Datei *web.config* für den Authentifizierungsdienst, den Store oder die Receiver für Web-Site, die sich typischerweise in den Verzeichnissen `C:\inetpub\wwwroot\Citrix\Authentication\`, `C:\inetpub\wwwroot\Citrix\storename\` bzw. `C:\inetpub\wwwroot\Citrix\storenameWeb\` befinden, wobei „storename“ der Name ist, der für den Store bei seiner Erstellung angegeben wurde.
2. Suchen Sie das folgende Element in der Datei.

   ```
   <logger duplicateInterval="00:01:00" duplicateLimit="10">
   ```

   Standardmäßig ist StoreFront so konfiguriert, dass die Anzahl doppelter Protokolleinträge auf 10 pro Minute begrenzt ist.
3. Ändern Sie den Wert des Attributs duplicateInterval, um den Zeitraum in Stunden, Minuten und Sekunden festzulegen, über den doppelte Protokolleinträge überwacht werden. Verwenden Sie das Attribut duplicateLimit, um die Anzahl doppelter Einträge festzulegen, die innerhalb des angegebenen Zeitintervalls protokolliert werden müssen, um die Protokolldrosselung auszulösen.

Wenn die Protokolldrosselung ausgelöst wird, wird eine Warnmeldung protokolliert, die darauf hinweist, dass weitere identische Protokolleinträge unterdrückt werden. Sobald die Zeitbegrenzung abgelaufen ist, wird die normale Protokollierung fortgesetzt und eine Informationsmeldung protokolliert, die anzeigt, dass doppelte Protokolleinträge nicht mehr unterdrückt werden.

Leistungsindikatoren

StoreFront schreibt eine Reihe von Leistungsindikatoren. So zeigen Sie die Indikatorwerte an:

1. Öffnen Sie im **Startmenü** die **Leistungsüberwachung**. Diese finden Sie im Ordner **Windows-Verwaltungsprogramme**.
2. Wählen Sie in der Strukturansicht **Überwachungstools** > **Leistungsüberwachung**.
3. Wählen Sie die Schaltfläche + (**Hinzufügen**) in der Symbolleiste.
4. Wählen Sie die Leistungsindikatoren aus, die Sie anzeigen möchten. Sie finden diese unter Kategorien, die mit **Citrix®** beginnen.

Telemetrie

StoreFront sendet Telemetriedaten zu Ihrer StoreFront-Konfiguration und Anmeldeereignissen an Citrix Cloud. Dies wird entweder über einen lokalen On-Premises-DDC und Lizenzserver oder über Cloud Connectors an DaaS gesendet. Weitere Informationen finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

StoreFront™-Konfiguration

Verwendung

Header

FELD	BESCHREIBUNG	BEISPIEL
Version	Die Version des Lizenznutzungsereignisses	1.0
ID	Der eindeutige Bezeichner des Nutzungsereignisses	d4ce7919-5d80-44de-a8fa-102923fe0ead
Typ	Der Ereignistyp, der von CAS zur Identifizierung von Cloud-Nutzungsereignissen verwendet wird	Konfiguration
Zeitstempel	Der Zeitstempel, wann das Ereignis im Broker generiert wird	2011-08-12T20:17:46.384Z

FELD	BESCHREIBUNG	BEISPIEL
Produktion	Das ursprüngliche Produkt und die Bereitstellung des Nutzungsereignisses	OnPrem.StoreFront
prodVer	Die StoreFront-Version	3.30.0.0

Nutzlast

FELD	BESCHREIBUNG	BEISPIEL
serverName	Der Hostname des Dienstes, auf dem StoreFront ausgeführt wird	storefront-01.storefront.local
deploymentId	Die eindeutige Kennung der StoreFront-Bereitstellung	f47ac10b-58cc-4372-a567-0e02b2c3d479
installedWithCVAD	Gibt an, ob StoreFront zusammen mit CVAD installiert wurde	falsch
cpuCores	Die Gesamtzahl der CPU-Kerne	4
cpuModel	Die CPU, auf der StoreFront ausgeführt wird	12th Gen Intel(R) Core(TM) i7-1255U 1.70 GHz
ramGb	Die Gesamtmenge des RAM in GB	16
numServersInGroup	Die Anzahl der Server in der Servergruppe	3
Filialen	Der JSON-Blob der StoreFront Store-Konfiguration. Ein Array von Store-Objekten. **Einige Werte sind verschleiert**	Beispiel
rfWebSites	Der JSON-Blob der StoreFront Website-	Beispiel

FELD	BESCHREIBUNG	BEISPIEL
	Konfiguration. Ein Array von RFWeb Config-Objekten	
Gateways	Die Gateway-Konfigurationsobjekte als JSON-Blob. Ein Array von Gateway-Objekten.	Beispiel
AuthServices	Die Auth-Dienstkonfigurationsobjekte als JSON-Blob. Ein Array von Auth-Dienstobjekten.	Beispiel
IsPiiScrambled	wahr	

Beispiel für das Feld Stores

```
[{

            "BaseUrl": "baseUrl",

            "StorePath": "/",

            "EnabledFeatures": 21 bit bitmap,

            "ResourceTypeFilteringEnabled": "disabled|
Citrix.MPS.Application;Citrix.MPS.Desktop",

            "DefaultRfWebSite": "/Citrix/StoreWeb",

            "GatewaysUsed": [

                "gatewayId"

            ],

            "VdaLogonDataProvider": "",

            "ResourceFeeds": [

                {
```

```
                    "FeedName": "<resourceFeedName>|scrambled",
                    "Type": "CVAD",
                    "LoadBalancingEnabled": true,
                }
            ],
            "AdvancedAggregation": {
                 "Enabled": true,
                 "GroupingCount": 1,
                 "ControllersPushIdenticalResources": true,
                 "LoadBalanced": true,
                 "AnyPrimaryFarms": true,
                 "AnyBackupFarms": true,
            }
}]
```

Wenn keine Stores gefunden werden, ist es ein leeres Array .

Beispiel für das Feld rfWebSites

```
[{
    "SiteId": "siteId",
    "BaseUrl": "baseUrl",
    "StorePath": "storePath",
    "UiExperienced": 0,
```

```
    "EnabledFeatures": 9 bit,
    "AuthMethodsEnabled": [
        "ad"
    ],
    "CanUsersDownloadApps": {
        "Enabled": true,
        "Windows": "exe",
        "MacOS": "dmg"
    },
    "WorkspaceControl": {
        "Enabled": true,
        "LogoffAction": 0,
        "AutoReconnectAtLogon": true,
        "ShowReconnectButton": true,
        "ShowDisconnectButton": true
    },
    "MultiClickTimeout": 1,
    "UiViews": [
        "apps",
        "desktops"
    ],
    "DefaultTab": 0,
```

```
}]
```

Wenn keine rfWebSites gefunden werden, ist es ein leeres Array .

Beispiel für das Feld Gateways

```
[{
            "GatewayId": "gatewayId",
            "IsCloudGateway": true,
            "LoadBalancingSTAEnabled": true,
            "SessionReliabilityEnabled": true,
            "RequestTicketsFromTwoSTA": true,
            "Version": "1234",
            "LogonType": "domain",
            "SmartCardFallbackEnabled": true
}]
```

Wenn keine Gateways gefunden werden, ist es ein leeres Array .

Beispiel für das Feld AuthServices

```
[{
    "SiteId": "SiteId",
    "Store": "StoreAuth",
    "AuthMethodsEnabled": [
        "ad"
    ],
```

```
    "PasswordChangeWhenExpired": 0,

    "PasswordRemindersForm": 1,

    "DelegateCredentialValidationToCitrix": true,

    "ValidatePasswordsOnDeliveryControllers": true

}]
```

Wenn keine Auth-Dienste gefunden werden, ist es ein leeres Array .

Storefront-Anmeldung

Verwendung

Header

FELD	BESCHREIBUNG	BEISPIEL
Version	Die Version des Lizenznutzungsereignisses	1.0
id	Der eindeutige Bezeichner des Nutzungsereignisses	d4ce7919-5d80-44de-a8fa-102923fe0ead
Typ	Der Ereignistyp, der von CAS zur Identifizierung von Cloud-Nutzungsereignissen verwendet wird	Anmeldung
st	Der Zeitstempel, wann das Ereignis im Broker generiert wird	2011-08-12T20:17:46.384Z
Produkt	Das Ursprungsprodukt und die Bereitstellung des Nutzungsereignisses	OnPrem.StoreFront
prodVer	Die StoreFront-Version	3.30.0.0

Nutzdaten

FELD	BESCHREIBUNG	BEISPIEL
Benutzer	Der Benutzer, der den Start initiiert hat. **Der Wert ist verschlüsselt**	fullName: C648FE671A44B3F7 **(immer verschlüsselt)** samName:C758LH671A44B3F7 **(immer verschlüsselt)** upn: C7948FE671A44B3F7 **(immer verschlüsselt)** userLicenseId:C265FE671A44B3F7 **(immer verschlüsselt)** userSid: C097FE671A44B3F7 **(immer verschlüsselt)**
serverName	Der Hostname des Dienstes, auf dem StoreFront ausgeführt wird	storefront-01.storefront.local
loginMethodRfWeb	Nicht verwendet	
loginMethodAuth	Die Methode, die der Benutzer für die Anmeldung bei StoreFront verwendet hat	0

FELD	BESCHREIBUNG	BEISPIEL
gatewayURL	Die URL des Netscaler Gateways, das während der Anmeldung verwendet wurde	netscaler-gateway.com
enabledFeatures	Eine Bitmaske der aktivierten Funktionen	12
userAgent	Der UserAgent des Clients, der für die Anmeldung verwendet wurde	CitrixReceiver/ 22.11.0.19 Linux/ 5.17.15 X1Class CWACapable CWA/ 22.11.0.19
baseUrl	Die Basis-URL des Stores, bei dem sich der Benutzer angemeldet hat	storefront-dev.storefront.dev
storePath	Der Store-Pfad, bei dem sich der Benutzer angemeldet hat	/Citrix/StoreWeb
apiUsed	Gibt an, ob der Client die Store-API, Web-API oder PNAgent-API verwendet	0
deviceId	Der Name des Geräts, das für die Anmeldung bei StoreFront verwendet wurde. **Der Wert ist verschlüsselt**	john-doe
transactionId	Bezeichner, der zum Gruppieren	773aba9e-5b91-4ef9-8782-c4afb75698e7

FELD	BESCHREIBUNG	BEISPIEL
	verwandter Ereignisse verwendet wird	

Citrix Workspace-App-Analysen

Wenn Sie Citrix Analytics verwenden, können Sie StoreFront so konfigurieren, dass die Citrix Workspace-App Benutzerereignisse zur Verarbeitung an Citrix Analytics sendet. Citrix Analytics aggregiert Metriken zu Benutzern, Anwendungen, Endpunkten, Netzwerken und Daten, um umfassende Einblicke in das Benutzerverhalten zu ermöglichen. Informationen zu dieser Funktion finden Sie in der Citrix Analytics-Dokumentation unter Onboard Virtual Apps and Desktops Sites using StoreFront.

So konfigurieren Sie dieses Verhalten:

- Laden Sie eine Konfigurationsdatei von Citrix Analytics herunter.
- Importieren Sie Citrix Analytics-Daten mithilfe von PowerShell in Ihre lokale StoreFront-Bereitstellung.

Nachdem StoreFront konfiguriert wurde, kann die Citrix Workspace-App Daten aus StoreFront-Stores senden, wenn der Citrix Analytics-Dienst dies anfordert.

> **Wichtig:**

> Ihre StoreFront-Bereitstellung muss in der Lage sein, Citrix API Services zu kontaktieren. Siehe Netzwerkanforderungen für Analytics.

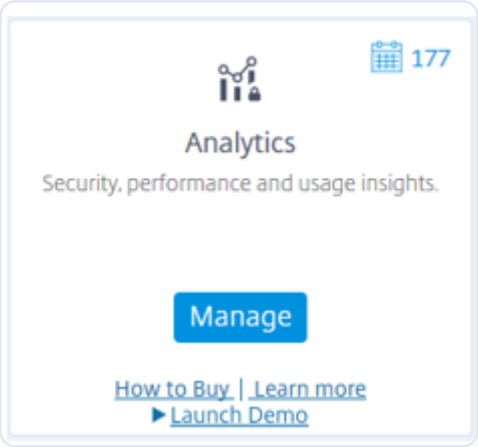
Konfigurationsdatei von Citrix Analytics herunterladen

> **Wichtig:**

> Für die Erstkonfiguration ist eine Konfigurationsdatei mit vertraulichen Informationen erforderlich. Bewahren Sie die Datei nach dem Herunterladen sicher auf. Geben Sie diese Datei nicht an Personen außerhalb Ihrer Organisation weiter. Nach der Konfiguration können Sie diese Datei löschen. Wenn Sie die Konfiguration auf einem anderen Computer erneut

anwenden müssen, können Sie die Datei erneut von der Citrix Analytics-Dienstverwaltungskonsole herunterladen.

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



4. Wählen Sie in der Citrix Analytics-Dienstverwaltungskonsole **Einstellungen > Datenquellen** aus.
5. Wählen Sie auf der Karte „Virtual Apps and Desktops“ das Menüsymbol (⋮) aus und wählen Sie dann **StoreFront-Bereitstellung verbinden**.
6. Wählen Sie auf der Seite „Connect StoreFront Deployment“ die Option **Download File**, um die Datei *StoreFrontConfigurationFile.json* herunterzuladen.

Beispielkonfigurationsdatei

```
{

  "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"

}
```

wobei

customerId die eindeutige ID für den aktuellen Monitor-Kunden ist.

cwsServiceKey ein eindeutiger Schlüssel ist, der das aktuelle Monitor-Kundenkonto identifiziert.

instanceID ist eine generierte ID, die zum Signieren (Sichern) von Anfragen verwendet wird, die von der Citrix Workspace-App an Citrix Analytics gesendet werden. Wenn Sie mehrere StoreFront-Server oder Servergruppen bei Monitor registrieren, hat jeder eine eindeutige instanceID.

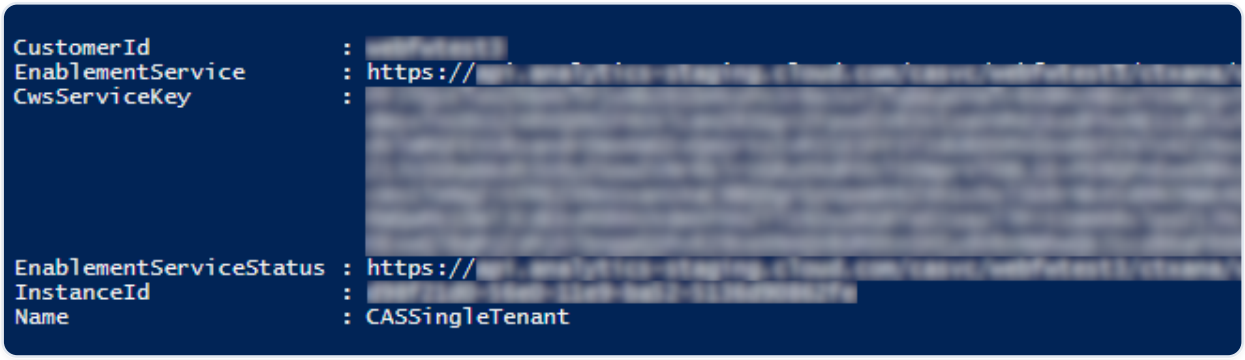
Citrix Analytics-Daten in Ihre StoreFront™-Bereitstellung importieren

1. Kopieren Sie die Datei *StoreFrontConfigurationFile.json* in einen geeigneten Ordner auf dem lokalen StoreFront-Server (oder einem Server in einer StoreFront-Servergruppe). Die folgenden Befehle gehen davon aus, dass die Datei 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
```

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



Hinweis:

On-Premises StoreFront-Server, die auf Windows Server 2012 R2 installiert sind, erfordern möglicherweise die manuelle Installation der C++-Laufzeitsoftwarekomponenten, damit sie sich bei CAS registrieren können. Wenn StoreFront während der Installation von Citrix Virtual Apps and Desktops installiert wird, ist dieser Schritt nicht erforderlich, da der CVAD-Metainstaller die C++-Laufzeitkomponenten bereits installiert. Wenn StoreFront nur mit dem CitrixStoreFront-x64.exe-Metainstaller ohne die C++-Laufzeit installiert wird, kann die Registrierung bei Monitor nach dem Import der CAS-Konfigurationsdatei fehlschlagen.

Citrix Analytics-Daten an eine StoreFront-Servergruppe weitergeben

Wenn Sie diese Aktionen in einer StoreFront-Servergruppe ausführen, müssen Sie die importierten Citrix Analytics-Daten an alle Mitglieder der Servergruppe weitergeben. Dieser Schritt ist bei einer einzelnen StoreFront-Serverbereitstellung nicht erforderlich.

Um die Daten weiterzugeben, verwenden Sie eine der folgenden Methoden:

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

StoreFront-Servergruppen-ID überprüfen

Um zu überprüfen, ob Ihre Bereitstellung erfolgreich beim Citrix Analytics-Dienst registriert wurde, können Sie PowerShell verwenden, um die ServerGroupID für Ihre Bereitstellung zu ermitteln.

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:

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

$XMLObject = (Get-Content $WebConfigPath) -as [Xml]

$XMLObject.framework.properties.property
```

Diese Befehle erzeugen beispielsweise eine Ausgabe wie die folgende:

```
name value

---- -----

ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432

HostBaseUrl https://storefront.example.com/

SelectedIISWebSiteId 1

AdminConsoleOperationMode Full
```

Senden von Daten von StoreFront an Citrix Analytics beenden

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

   `Remove-STFCasConfiguration`

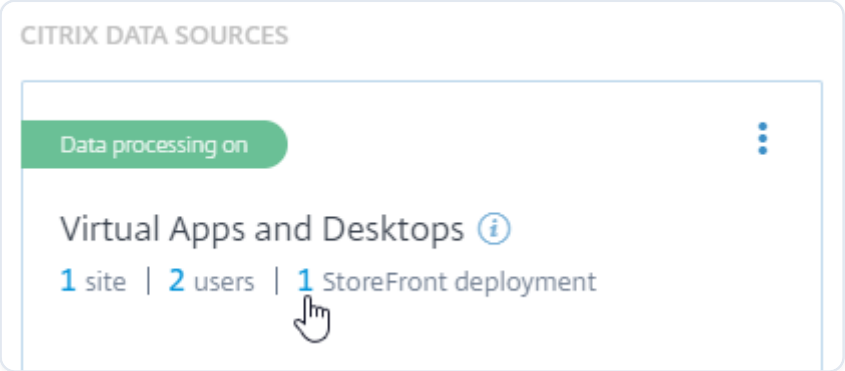
   `Get-STFCasConfiguration`

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

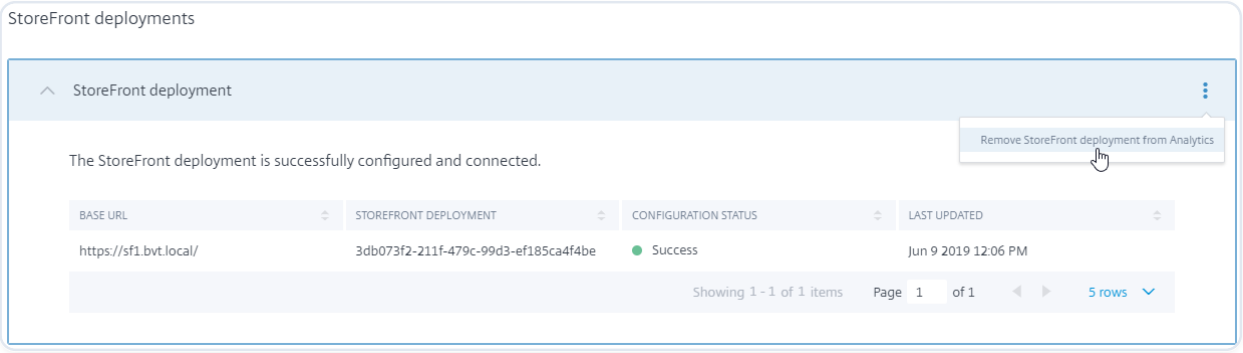
   `Publish-STFServerGroupConfiguration`
4. Führen Sie auf allen anderen Servergruppenmitgliedern den folgenden Befehl aus, um zu bestätigen, dass die Citrix Analytics-Konfiguration erfolgreich von allen Servern in der Gruppe entfernt wurde:

   `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 Verwaltungskonsole des Citrix Analytics-Dienstes, indem Sie auf **Verwalten** klicken.
8. Wählen Sie in der Verwaltungskonsole des Citrix Analytics-Dienstes **Einstellungen > Datenquellen**.
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, indem Sie sich auf die Host-Basis-URL und die ServerGroupID beziehen.
11. Wählen Sie im (⋮)-Menü **StoreFront-Bereitstellung aus Analytics entfernen**.



Hinweis:

Wenn Sie die Konfiguration serverseitig, aber nicht aus Citrix Analytics entfernen, bleibt der Eintrag der StoreFront-Bereitstellung in Citrix Analytics erhalten, empfängt jedoch keine Daten von StoreFront. Wenn Sie die Konfiguration nur aus Citrix Analytics entfernen, wird der Eintrag der StoreFront-Bereitstellung beim nächsten App-Pool-Recycle (durchgeführt bei einem IIS-Reset oder automatisch alle 24 Stunden) erneut hinzugefügt.

StoreFront für die Verwendung eines Webproxys konfigurieren, um Citrix Analytics zu kontaktieren, zu überwachen und sich dort zu registrieren

Wenn StoreFront auf einem Host-Webserver hinter einem Webproxy platziert wird, schlägt die Registrierung bei Citrix Analytics fehl. Wenn StoreFront-Administratoren einen HTTP-Proxy in ihrer Citrix-Bereitstellung verwenden, muss der für das Internet bestimmte StoreFront-Datenverkehr den Webproxy passieren, bevor er Citrix Analytics in der Cloud erreicht. StoreFront verwendet die Proxy-Einstellungen des Host-Betriebssystems nicht automatisch; es ist eine zusätzliche Konfiguration erforderlich, um den Store anzuweisen, ausgehenden Datenverkehr über den Webproxy zu senden. Sie können eine `<system.net>` Proxy-Konfiguration einrichten, indem Sie einen neuen Abschnitt zur web.config-Datei des Stores hinzufügen. Tun Sie dies für jeden Store auf dem StoreFront-Server, der zum Senden von Daten an Citrix Analytics verwendet werden soll.

Methode 1: Store-Proxy-Konfiguration über PowerShell für einen oder mehrere Stores festlegen (empfohlen)

Das Ausführen des PowerShell-Skripts Config-StoreProxy.ps1 automatisiert diesen Prozess für einen oder mehrere Stores und fügt automatisch gültiges XML zur Konfiguration von `<system.net>` ein. Das Skript sichert auch die web.config-Datei des Stores auf dem Desktop des aktuellen Benutzers, sodass die unveränderte web.config-Datei bei Bedarf wiederhergestellt werden kann.

> **Hinweis:**
>
> Das mehrfache Ausführen des Skripts kann dazu führen, dass mehrere Kopien des `<system.net>` XML hinzugefügt werden. Jeder Store sollte nur einen einzigen Eintrag für `<system.net>` haben. Das Hinzufügen mehrerer Kopien verhindert, dass die Store-Proxy-Konfiguration ordnungsgemäß funktioniert.

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 entweder an:
   - eine IP-Adresse, ODER
   - einen FQDN für den Webproxy
4. Führen Sie das folgende 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)



    foreach($Store in $Stores)

    {

        Write-Host "Backing up the Store web.config file for store
$Store before making changes..." -ForegroundColor "Yellow"

        Write-Host "`n"
```

```
        if(!(Test-Path "$env:UserProfile\desktop\$Store\"))

        {

            Write-Host "Creating $env:UserProfile\desktop\$Store\
directory for backup..." -ForegroundColor "Yellow"

            New-Item -Path "$env:UserProfile\desktop\$Store\" -ItemType
"Directory" | Out-Null

            Write-Host "`n"

        }



        Write-Host "Copying c:\inetpub\wwwroot\Citrix\$Store\web.config
to $env:UserProfile\desktop\$Store\..." -ForegroundColor "Yellow"

        Copy-Item -Path "c:\inetpub\wwwroot\Citrix\$Store\web.config"
-Destination "$env:UserProfile\desktop\$Store\" -Force | Out-Null



        if(Test-Path "$env:UserProfile\desktop\$Store\web.config")

        {

            Write-Host "$env:UserProfile\desktop\$Store\web.config file
backed up" -ForegroundColor "Green"

        }

        else

        {

            Write-Host "$env:UserProfile\desktop\$Store\web.config file
NOT found!" -ForegroundColor "Red"

        }
```

```
        Write-Host "`n"



        Write-Host "Setting the proxy server to $ProxyAddress for Store
$Store..." -ForegroundColor "Yellow"

        Write-Host "`n"



        $StoreConfigPath = "c:\inetpub\wwwroot\Citrix\
$Store\web.config"

        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]



        if([string]::IsNullOrEmpty($ProxyFQDN))

        {

            $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)

        }

        else

        {

            $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)

        }



        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]



        # Create 3 elements

        $SystemNet = $XMLObject.CreateNode("element","system.net","")
```

```
        $DefaultProxy =
$XMLObject.CreateNode("element","defaultProxy","")

        $Proxy = $XMLObject.CreateNode("element","proxy","")

        $Proxy.SetAttribute("proxyaddress","$ProxyServer")

        $Proxy.SetAttribute("bypassonlocal","true")



        # Move back up the XML tree appending new child items in
reverse order

        $DefaultProxy.AppendChild($Proxy)

        $SystemNet.AppendChild($DefaultProxy)

        $XMLObject.configuration.AppendChild($SystemNet)



        # Save the modified XML document to disk

        $XMLObject.Save($StoreConfigPath)



        Write-Host "Getting the proxy configuration for c:
\inetpub\wwwroot\Citrix\$Store..." -ForegroundColor "Yellow"

        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]

        $ConfiguredProxyServer =
$XMLObject.configuration.'system.net'.defaultProxy.proxy.proxyaddress |
Out-Null

        Write-Host ("Configured proxy server for Store $Store"+": "+
$ConfiguredProxyServer) -ForegroundColor "Green"

        Write-Host "`n"

    }
```

```
    Write-Host "Restarting IIS..." -ForegroundColor "Yellow"

    IISReset /RESTART

}



Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -ProxyPort
$ProxyPort

# OR

Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
$ProxyPort
```

5. Überprüfen Sie, ob `C:\inetpub\wwwroot\Citrix\<Store>\web.config` jetzt einen `<system.net>` Abschnitt am Ende der Datei enthält.

```
        </dependentAssembly>

    </assemblyBinding>

</runtime>

<system.net>

    <defaultProxy>

    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
bypassonlocal="true" />

    </defaultProxy>

</system.net>

</configuration>
```

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

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

Dies muss für jeden Store auf dem StoreFront-Server erfolgen, der zum Senden von Daten an Citrix Analytics verwendet wird.

1. Sichern Sie die web.config-Datei für den Store und kopieren Sie sie an einen anderen Speicherort außerhalb von `C:\inetpub\wwwroot\Citrix\<Store>\web.config`.
2. Ändern Sie die folgende XML mit Ihren Proxy-Einstellungen, entweder unter Verwendung einer FQDN-und-Port-Kombination oder einer IP-und-Port-Kombination.

   Beispielsweise bei Verwendung einer FQDN-und-Port-Kombination, verwenden Sie das folgende `<system.net>` Element:

   ```
   <system.net>

       <defaultProxy>

       <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
   bypassonlocal="true" />

       </defaultProxy>

   </system.net>
   ```

   Beispielsweise bei Verwendung einer IP-und-Port-Kombination, verwenden Sie das folgende `<system.net>` Element:

   ```
   <system.net>

       <defaultProxy>

       <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true" />

       </defaultProxy>

   </system.net>
   ```

3. Am Ende der web.config-Datei des Stores fügen Sie das entsprechende `<system.net>` Element ein, wie hier angegeben:

```
<runtime>

<gcServer enabled="true" />

<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">

    <dependentAssembly>

    <assemblyIdentity name="System.Web.MVC"
publicKeyToken="31BF3856AD364E35" culture="neutral" />

    <bindingRedirect oldVersion="0.0.0.0-5.0.0.0"
newVersion="5.0.0.0" />

    </dependentAssembly>

    <dependentAssembly>

    <assemblyIdentity name="Newtonsoft.Json"
publicKeyToken="30ad4fe6b2a6aeed" 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>
```

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

Einstellungshinweise

Die Ankündigungen in diesem Artikel sollen Sie frühzeitig über Plattformen, Citrix-Produkte und Funktionen informieren, die eingestellt werden, damit Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Kundennutzung und das Feedback, um zu bestimmen, wann diese zurückgezogen werden. Ankündigungen können sich in nachfolgenden Releases ändern und enthalten möglicherweise nicht jede veraltete Funktion oder Funktionalität. Details zur Produktlebenszyklusunterstützung finden Sie im Artikel Product Lifecycle Support Policy. Informationen zur Wartungsoption für Long Term Service Release (LTSR) finden Sie unter `<https://support.citrix.com/article/CTX205549>`.

Veraltete Funktionen

Veraltete Elemente werden nicht sofort entfernt. Citrix® unterstützt sie weiterhin, aber sie werden in einer zukünftigen Version entfernt.

FUNKTION	EINSTELLUNG ANGEKÜNDIGT IN VERSION	ALTERNATIVE
XenApp® Services (auch bekannt als PNAgent)	2308	Verbinden Sie sich innerhalb der Workspace-App mit Stores über die Store-URL anstatt über die XenApp Services-URL.

Entfernungen

Entfernte Elemente werden entweder entfernt oder nicht mehr unterstützt.

FUNKTION	EINSTELLUNG ANGEKÜNDIGT IN VERSION	ENTFERNT IN VERSION	ALTERNATIVE
Citrix Programm zur Verbesserung der Kundenzufriedenheit	2507	2507	

FUNKTION	EINSTELLUNG ANGEKÜNDIGT IN VERSION	ENTFERNT IN VERSION	ALTERNATIVE
Windows Server 2016	2402	2407	Installieren Sie StoreFront auf Windows Server 2019 oder höher
Unterstützung für Microsoft .NET Framework-Versionen vor 4.8.0.	2407	2407	Führen Sie ein Upgrade auf .NET Framework Version 4.8.0 oder höher durch. (Das Installationsprogramm installiert .NET Framework 4.8.0 automatisch, falls es noch nicht installiert ist.)
Internet Explorer 11 zum Verbinden mit Ressourcen über die Workspace-App für HTML5	2308	2308	Verwenden Sie entweder einen unterstützten Webbrowser oder installieren Sie die Citrix Workspace™-App für Windows. Es ist weiterhin möglich, Internet Explorer 11 für den Zugriff auf Ihren Store zu verwenden, aber zum Starten von Ressourcen muss die Citrix Workspace-App für Windows installiert sein.
XenApp 6.5-Sites.	2308	2308	Führen Sie ein Upgrade auf die neueste Version von

FUNKTION	EINSTELLUNG ANGEKÜNDIGT IN VERSION	ENTFERNT IN VERSION	ALTERNATIVE
			Citrix Virtual Apps and Desktops durch.
Unterstützung für Self-Service-Passwortzurücksetzung (SSPR)	2203	2203	-
Unterstützung für TLS 1.0- und TLS 1.1-Protokolle zwischen Citrix Virtual Apps and Desktops und der Citrix Workspace-App.	3.14	2203	Citrix Receivers auf eine Citrix Workspace-App aktualisieren, die TLS 1.2 unterstützt
Installieren von StoreFront unter 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	Aktualisieren Sie auf .NET Framework Version 4.7.2 oder höher. (Das Installationsprogramm installiert .NET Framework 4.7.2 automatisch, falls es noch nicht installiert ist.)
Entfernung der Delivery Controller-Optionen für die folgenden End-of-Life-Produkte: VDI-in-a-Box und	1903	1903	---

FUNKTION	EINSTELLUNG ANGEKÜNDIGT IN VERSION	ENTFERNT IN VERSION	ALTERNATIVE
XenMobile (9.0 und früher).			
Internet Explorer 9 und 10	1903	1903	---
Unterstützung für Benutzer, um auf Desktops auf Desktop Appliance-Sites zuzugreifen	1811	1912	Verwenden Sie Desktop Lock für nicht in die Domäne eingebundene Anwendungsfälle.
Klassische Citrix-Benutzeroberfläche („grüne Blasen“)	3.12	1903	Verwenden Sie die Unified UI
Installieren von StoreFront unter Windows Server 2012 und Windows Server 2008 R2 (einschließlich Service Packs).	3.12 LTSR	3.15	Installieren Sie Komponenten auf einem unterstützten Betriebssystem.
Citrix Online Integration (Goto-Produkt) Integration	3.11	3.12	---
Direkte Upgrades von 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 aktuelle Version
Installation von StoreFront auf 32-Bit- (x86-) Maschinen.	3.8	3.13	Installieren Sie auf einem unterstützten x64-Betriebssystem.

Informationen zu Veraltungen in der Citrix Workspace-App für HTML5 finden Sie auf der Seite Veraltung.

Hinweise zu Drittanbietern

StoreFront kann Softwarekomponenten Dritter enthalten, die unter den folgenden Bedingungen lizenziert sind. Diese Liste wurde mit Software Dritter zum angegebenen Datum erstellt. Diese Liste kann sich mit bestimmten Versionen des Produkts ändern und ist möglicherweise nicht vollständig; sie wird „wie besehen“ bereitgestellt. SOWEIT NACH GELTENDEM RECHT ZULÄSSIG, GEBEN CITRIX UND SEINE LIEFERANTEN KEINE ZUSICHERUNGEN ODER GARANTIEN, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, GESETZLICH ODER ANDERWEITIG, HINSICHTLICH DER LISTE ODER IHRER RICHTIGKEIT ODER VOLLSTÄNDIGKEIT ODER HINSICHTLICH DER ERGEBNISSE, DIE SICH AUS DER VERWENDUNG ODER VERBREITUNG DER LISTE ERGEBEN. DURCH DIE VERWENDUNG ODER VERBREITUNG DER LISTE ERKLÄREN SIE SICH DAMIT EINVERSTANDEN, DASS CITRIX IN KEINEM FALL FÜR BESONDERE, DIREKTE, INDIREKTE ODER FOLGESCHÄDEN ODER SONSTIGE SCHÄDEN HAFTBAR GEMACHT WERDEN KANN, DIE SICH AUS DER VERWENDUNG ODER VERBREITUNG DIESER LISTE ERGEBEN.

Castle Windsor 3.3.0

Copyright 2004-2013 Castle Project - `<http://www.castleproject.org/>`

Lizenziert unter der Apache-Lizenz, Version 2.0

Microsoft Unity Application Block (Unity) 2.1

Copyright © 2011 Microsoft Corporation.

Lizenziert unter der Microsoft Public License (MS-PL) `<https://msdn.microsoft.com/de-de/library/hh237493.aspx>`

Microsoft Muster und Praktiken: Prism 2.2

Copyright © 2010 Microsoft Corporation.

Lizenziert unter der Microsoft Public License (MS-PL).

Microsoft Muster & Praktiken: Common Service Locator 1.0

Copyright © Microsoft Corporation.

Lizenziert unter der Microsoft Public License (MS-PL)

Microsoft .Net Reference Source

Copyright © Microsoft Corporation. Lizenziert unter der MIT-Lizenz.

Microsoft.IdentityModel.JsonWebTokens

Copyright © Microsoft Corporation. Lizenziert unter der MIT-Lizenz.

Microsoft.IdentityModel.Logging

Copyright © Microsoft Corporation. Lizenziert unter der MIT-Lizenz.

Microsoft.IdentityModel.Tokens

Copyright © Microsoft Corporation. Lizenziert unter der MIT-Lizenz.

ManagedEsent Release 1.9.4

Copyright © Microsoft Corporation.

Lizenziert unter der Microsoft Public License (MS-PL).

jQuery UI - v1.10.4 - 2014-03-12

`<http://jqueryui.com/>`

Copyright 2014 jQuery Foundation und andere Mitwirkende; Lizenziert unter MIT

jQuery JavaScript Library v1.12.4

`<http://jquery.com/>`

Enthält 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

Copyright (c) 2010 Kelvin Luck

Doppelt lizenziert unter den MIT- und GPL-Lizenzen.

jquery.contextmenu.js

jQuery-Plugin für Kontextmenüs

Copyright (c) 2008 Matt Kruse (javascripttoolbox.com)

Doppelt lizenziert unter den MIT- und GPL-Lizenzen.

jQuery-Plugin für Hammer.JS - v1.0.0 - 2014-01-02

`<http://eightmedia.github.com/hammer.js>`

Copyright (c) 2014 Jorik Tangelder <j.tangelder@gmail.com>;

Lizenziert unter der MIT-Lizenz

jQuery MouseWheel

Copyright (c) 2011 Brandon Aaron (http://brandonaaron.net)

Lizenziert unter der MIT-Lizenz (LICENSE.txt).

WPF Toolkit 3.5

WPF Toolkit Copyright (c) 2006-2014 Microsoft

MS-PL-Lizenz

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.

Für weitere Funktionen, Steuerelemente und schnellen professionellen Support erhalten Sie die Plus Edition unter `<http://xceed.com/wpf_toolkit>`

Bleiben Sie auf dem Laufenden: folgen Sie @datagrid auf Twitter.

WiX Toolset

Copyright (c) .NET Foundation und Mitwirkende. Microsoft Reciprocal License (Ms-RL)

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 der MIT-Lizenz

Newtonsoft JSON

Copyright (c) 2007 James Newton-King

Lizenziert unter der MIT-Lizenz.

jQuery JavaScript Library v3.7.1

(c) OpenJS Foundation und andere Mitwirkende

Veröffentlicht unter der MIT-Lizenz

`<https://jquery.org/license>`

jQuery UI - v1.13.2 - 2022-07-14

`<http://jqueryui.com>`

Copyright jQuery Foundation und andere Mitwirkende; Lizenziert unter MIT

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 der MIT-Lizenz

VelocityJS.org (1.5.0)

velocity-animate (C) 2014-2017 Julian Shapiro.

Lizenziert unter der MIT-Lizenz. Details finden Sie in der Datei LICENSE im Projektstammverzeichnis.

slick.js - 1.8.0

Die MIT-Lizenz (MIT)

Copyright (c) 2013-2016

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furfero

Doppelt lizenziert unter der MIT- oder GPL Version 2-Lizenz.

Microsoft.WebApi.Collection

Die MIT-Lizenz (MIT)

Copyright (c) Microsoft Corporation

Polly

Copyright (c) 2015-2024, App vNext

Lizenziert unter der BSD 3-Klausel-Lizenz

Polly.Core

Copyright (c) 2015-2024, App vNext

Lizenziert unter der BSD 3-Klausel-Lizenz

Microsoft.Security.Crypto

Die MIT-Lizenz (MIT)

Copyright (c) Microsoft Corporation

Microsoft .NET 8

Die MIT-Lizenz (MIT)

Copyright (c) .NET Foundation und Mitwirkende

ANHANG: Referenzierte 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.
```

Apache-Lizenz, 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.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner

or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright 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 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 that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor,

except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all

other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only 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

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.

(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.

(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.

(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.

BSD 3-Klausel-Lizenz

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,

```
this

   list of conditions and the following disclaimer.



2. Redistributions in binary form must reproduce the above copyright
notice,

   this list of conditions and the following disclaimer in the
documentation

   and/or other materials provided with the distribution.



3. Neither the name of the copyright holder nor the names of its

   contributors may be used to endorse or promote products derived from

   this software without specific prior written permission.



THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS
IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
LIABLE

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER

CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY,
```

OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE

OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Microsoft Reciprocal License (Ms-RL)

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) Reciprocal Grants- For any file you distribute that contains code from the software (in source code or binary format), you must provide recipients the source code to that file along with a copy of this license, which license will govern that file. You may license other files that are entirely your own work and do not contain code from the software under any terms you choose.

(B) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(C) 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.

(D) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(E) 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.

(F) 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.