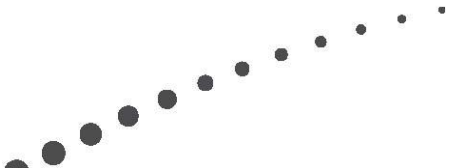




Citrix StoreFront 2.0

Proof of Concept Implementation Guide

www.citrix.com



Contents

Contents.....	2
Introduction	3
Architecture	4
Installation and Configuration	5
Section 1: StoreFront Initial Deployment	6
Initial Server Configuration.....	10
Create New StoreFront Deployment	13
Enable the Pass-Through Authentication Service.....	26
Section 2: Configure Second Receiver StoreFront Server	27
Section 3: Accessing Applications through Receiver	32
Receiver for Web	36
Section 4: NetScaler Load Balancing Configuration.....	36
Section 5: NetScaler Gateway for Remote Access	45
Conclusion	47
Acknowledgments.....	47
References	Error! Bookmark not defined.
Revision History	47

Introduction

Citrix StoreFront provides users an enterprise app store that aggregates resources from XenDesktop, XenApp, XenMobile App Controller, and VDI-in-a-Box in one place. Each StoreFront user is able to subscribe to their favorite application and desktop resources, these favorite resources then automatically follow the user between devices. With Citrix Web Interface reaching end-of-life in 2015, it is important that administrators become familiar with StoreFront to facilitate a successful transition between products.

StoreFront's new modular architecture improves upon the existing design of Web Interface. It includes a new user authentication method which directly queries Active Directory rather than the existing double-hop Web Interface process where user credentials are sent from the Web Interface server to the XML broker who then negotiates authentication with the Domain Controller. StoreFront also makes the process of deploying multiple servers easier through its configuration synchronization feature.

Customers that require a single point of access and self-service for Windows, Web, and SaaS applications should consider integrating StoreFront with XenMobile AppController. AppController, which is part of XenMobile App Edition, is an additional product that must be purchased. StoreFront is a no-cost product that is freely available for download for Citrix XenDesktop and XenApp customers. For a complete list of XenMobile AppController features, visit the [product page](#).

The goal of this document is to guide the reader through the steps required to create a successful StoreFront proof of concept environment. Citrix Consulting recommends implementing StoreFront in a phased approach beginning with mobile users. This user group will receive the greatest benefit since they access resources from multiple devices both inside and outside the corporate network. Selecting the correct user group will ensure that the full breadth of StoreFront's features and self-service capabilities are showcased within this proof of concept.

Architecture

Citrix StoreFront employs a modular architecture, as shown in the following diagram:

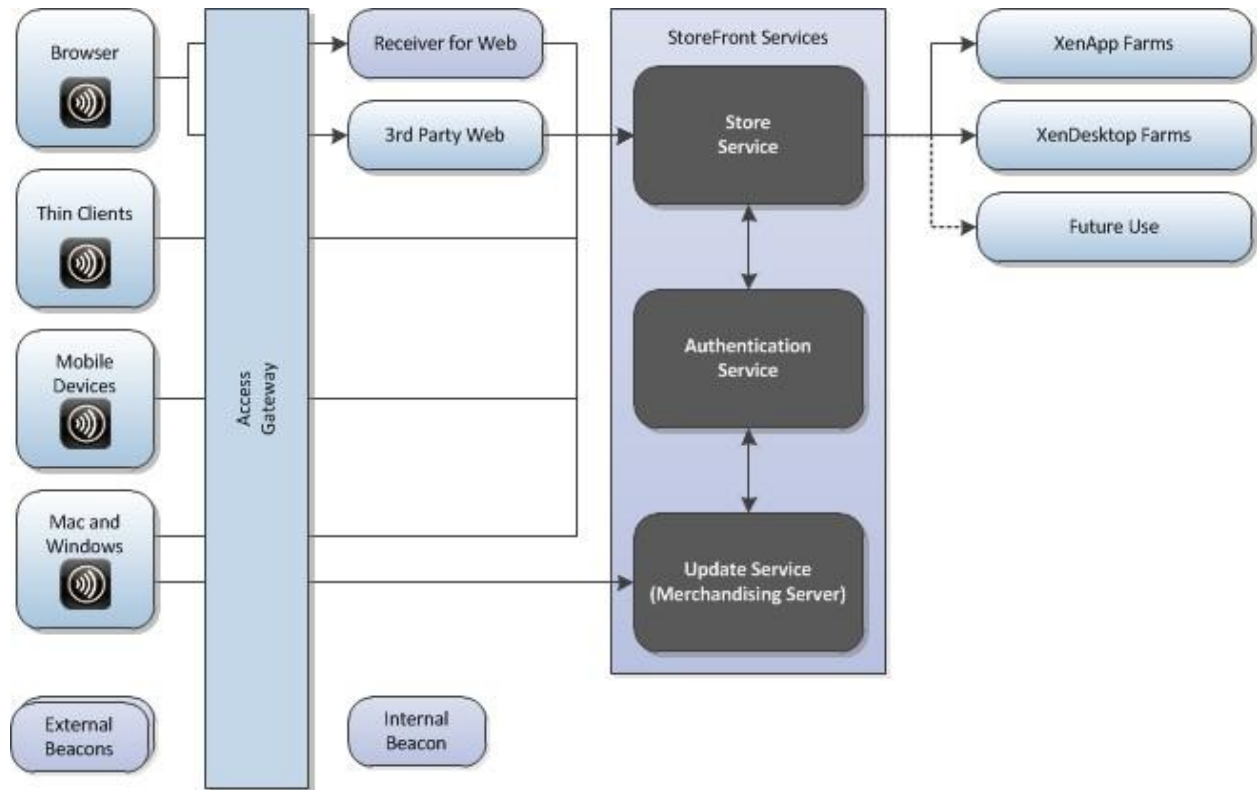


Figure 1: Citrix Storefront Receiver Architecture

- **Authentication Service.** Authenticates users to XenDesktop sites, XenApp farms, and AppController, handling all interactions to ensure that users only need to log on once.
- **Store Services.** Retrieves user credentials from the authentication service to authenticate users to the XenApp and XenDesktop servers providing the application and desktop resources. Enumerates the resources currently available from the servers and sends the details to Citrix Receiver.
- **Receiver for Web.** Enables users to access applications and desktop resources through a web page providing the same user experience as accessing those resources through Citrix Receiver.
- **Resource Subscription Database.** Stores details of individualized user subscriptions plus associated shortcut names and locations.
- **Beacon.** Citrix Receiver uses beacon points to determine whether users are connected to internal or public networks and then selects the appropriate access method.

Hardware and Software Requirements

In preparation for executing all the steps outlined in this Proof of Concept (PoC) Implementation Guide, the following components will be required:

- Windows Server 2008 R2 SP1 / Windows Server 2012: Receiver Storefront is only available for installation on these versions of Windows Server.
- Citrix Receiver 3.3+ (Standard) Windows/ 11.6+ Mac: The Citrix Receiver versions that supports direct connections to StoreFront and take advantage of automatic account provisioning. Receiver 3.1+ for Windows and 11.5 for Mac support direct connections to StoreFront but do not support automatic account provisioning. Previous versions of Citrix Receiver, Citrix Online Plugin, and Receiver Enterprise can be used, but applications and desktops will only be available from the Receiver for Web site or by a legacy site.
- NetScaler Access Gateway 10.0.69.4nc+: While not required for internal access to resources, Access Gateway is a key feature to enable secure remote access and allow the HTML5 client and Account Services features to function.

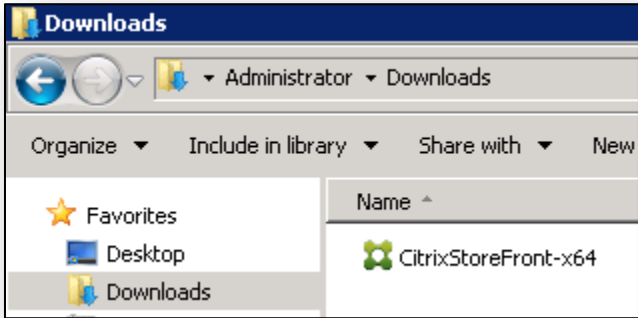
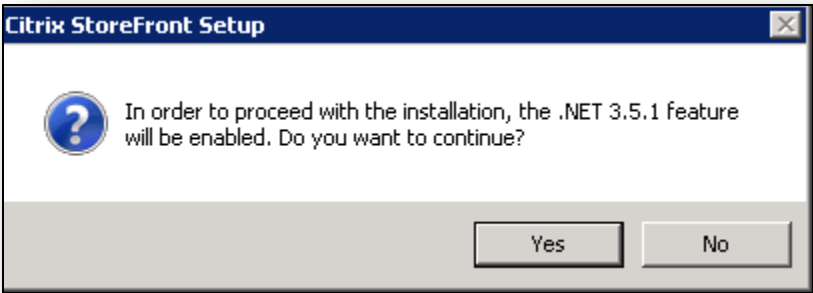
Installation and Configuration

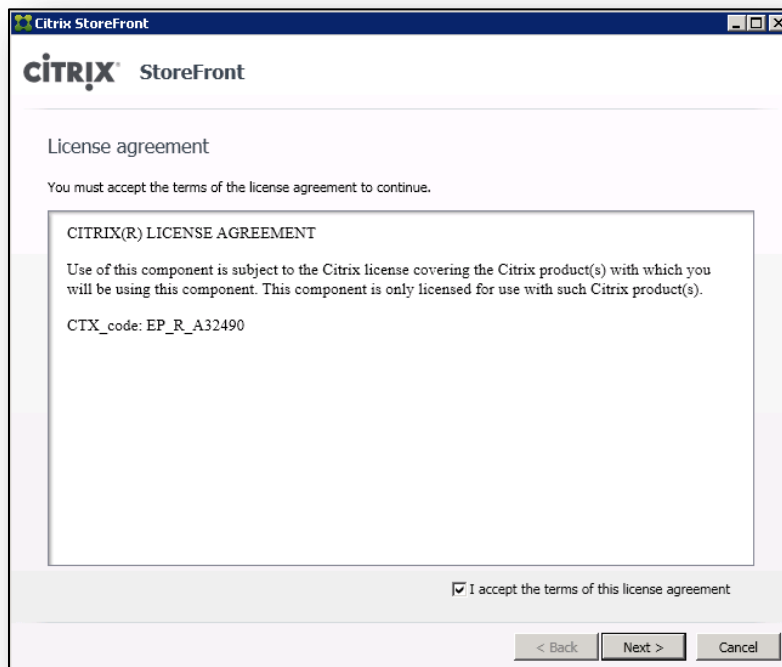
The purpose of this document is to provide step-by-step instructions for the implementation of each component within the Proof of Concept environment. Each step is broken down into the following individual sections:

- **Section 1:** [StoreFront Initial Deployment](#)
- **Section 2:** [Configure Second StoreFront Server](#)
- **Section 3:** [Accessing Applications through Receiver](#)
- **Section 4:** [Configure NetScaler Gateway Authentication](#)
- **Section 5:** [NetScaler Load Balancing Configuration](#)

Section 1: StoreFront Initial Deployment

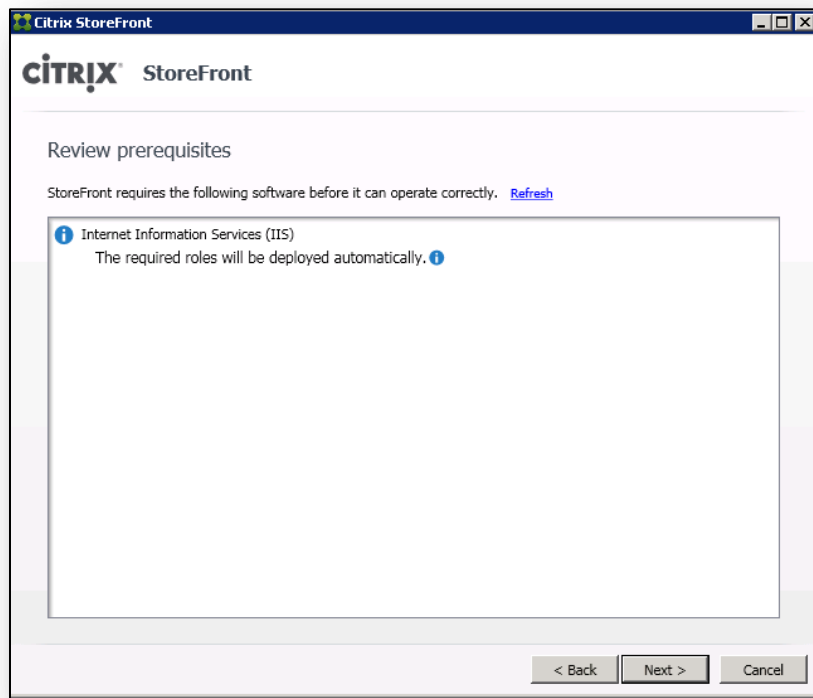
Citrix StoreFront can be setup in a single or multi-server deployment. Citrix Consulting recommends that StoreFront be deployed in a multi-server configuration to ensure high availability. The following steps detail the installation of StoreFront.

1	<p>Choose the StoreFront installation file</p> 
2	<p>Click Yes to install the .NET framework</p> 
	<p>Check the accept terms of license box</p>



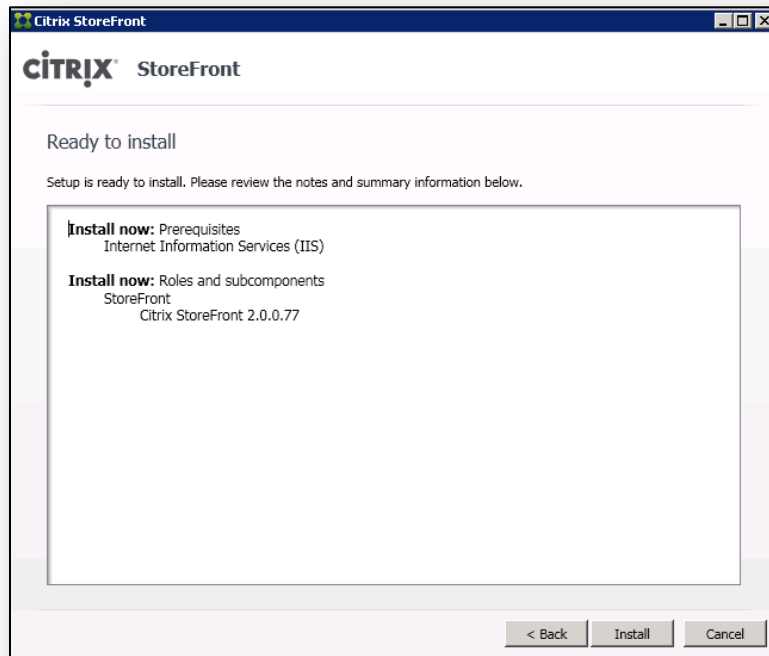
7

Internet Information Server (IIS) will be deployed as part of the installation
Select **Next**



Select **Install**

Any pre-requisites missing will be installed automatically by Receiver StoreFront installer

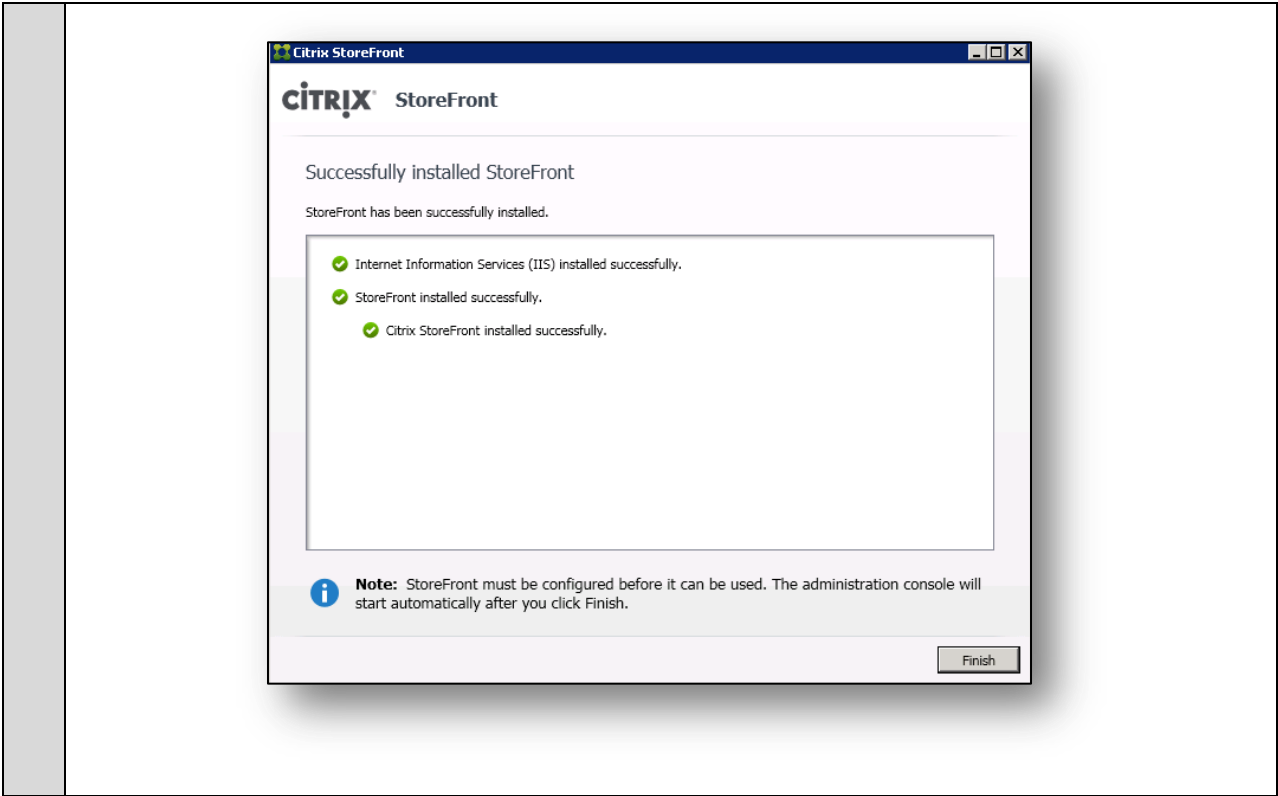


8

The installation has now been completed

Select **Finish**

The StoreFront Receiver administration console will automatically appear



Initial Server Configuration

The first step in configuring Receiver StoreFront is importing and binding a SSL certificate inside Internet Information Server (IIS). The following section walks through the steps needed to complete these tasks.

Initial Server Configuration		
	Screenshot	Description
1	A screenshot of the Internet Information Services (IIS) Manager console. The left-hand 'Connections' pane shows a tree view with 'Start Page', 'Application Pools', 'Sites', and 'Default Web Site'. The 'Sites' folder is expanded, showing 'CLOUDGATEWAY2 (CCSLAB\Administrator)'. The main pane shows the 'CLOUDGATEWAY2 Home' page with various feature icons. The 'Server Certificates' icon is highlighted with a red rectangular box. The right-hand 'Actions' pane shows options for 'Manage Server', including 'Restart', 'Start', 'Stop', 'View Application Pools', 'View Sites', 'Change .NET Framework Version', 'Help', and 'Online Help'.	<ul style="list-style-type: none">• Before beginning the configuration, a SSL certificate matching the hostname chosen must be imported and bound to the default IIS Web Site• This is accomplished in IIS Manager• Select the local Server from the left menu• Select Server Certificates from the features menu

2

The screenshot shows the IIS Manager console for 'CLOUDGATEWAY2'. The 'Server Certificates' feature is selected in the left-hand tree. The main pane displays the 'Server Certificates' task, which includes instructions on how to use the feature. On the right, the 'Actions' pane is visible, and the 'Import...' button is highlighted with a red rectangular box. Other buttons in the Actions pane include 'Create Certificate Request...', 'Complete Certificate Request...', 'Create Domain Certificate...', 'Create Self-Signed Certificate...', 'Help', and 'Online Help'. The status bar at the bottom indicates 'Ready'.

- Select **Import** on the Actions menu

3

The screenshot shows the 'Import Certificate' dialog box. It has a title bar with a question mark and a close button. The dialog contains three main sections: 'Certificate file (.pfx):' with a text box and a browse button (...), 'Password:' with a text box, and a checkbox labeled 'Allow this certificate to be exported' which is checked. At the bottom, there are 'OK' and 'Cancel' buttons.

- Select the certificate file to import
- Select **OK**

4

The screenshot shows the 'Server Certificates' section in IIS Manager. It includes the same instructions as in step 2. Below the instructions is a table showing the imported certificate. The table has four columns: 'Name', 'Issued To', 'Issued By', and 'Expiration Date'. The first row contains the following information: 'cloudgateway.ccslab.net' under 'Issued To', 'www.ns.com' under 'Issued By', and '3/19/2013 1' under 'Expiration Date'. The 'Name' column is empty. The status bar at the bottom indicates 'Ready'.

- The certificate is now imported

5

- Select **Default Web Site**
- Select **Bindings**

6

Type	Host Name	Port	IP Address	Binding Information
http		80	*	
net.tcp			808:	*
net.pipe			*	
net.m...			localhost	
msmq...			localhost	

- Select **Add**

7

Type: **https** IP address: **All Unassigned** Port: **443**

Host name:

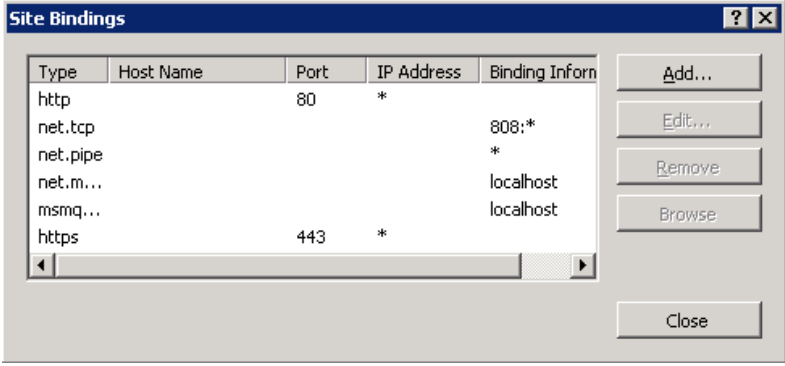
SSL certificate: **cloudgateway.ccslab.net**

View...

OK Cancel

- Select **https** as the Type
- Select the **SSL Certificate** from the dropdown menu
- Select **OK**

8



Type	Host Name	Port	IP Address	Binding Information
http		80	*	
net.tcp				808:*
net.pipe				*
net.m...				localhost
msmq...				localhost
https		443	*	

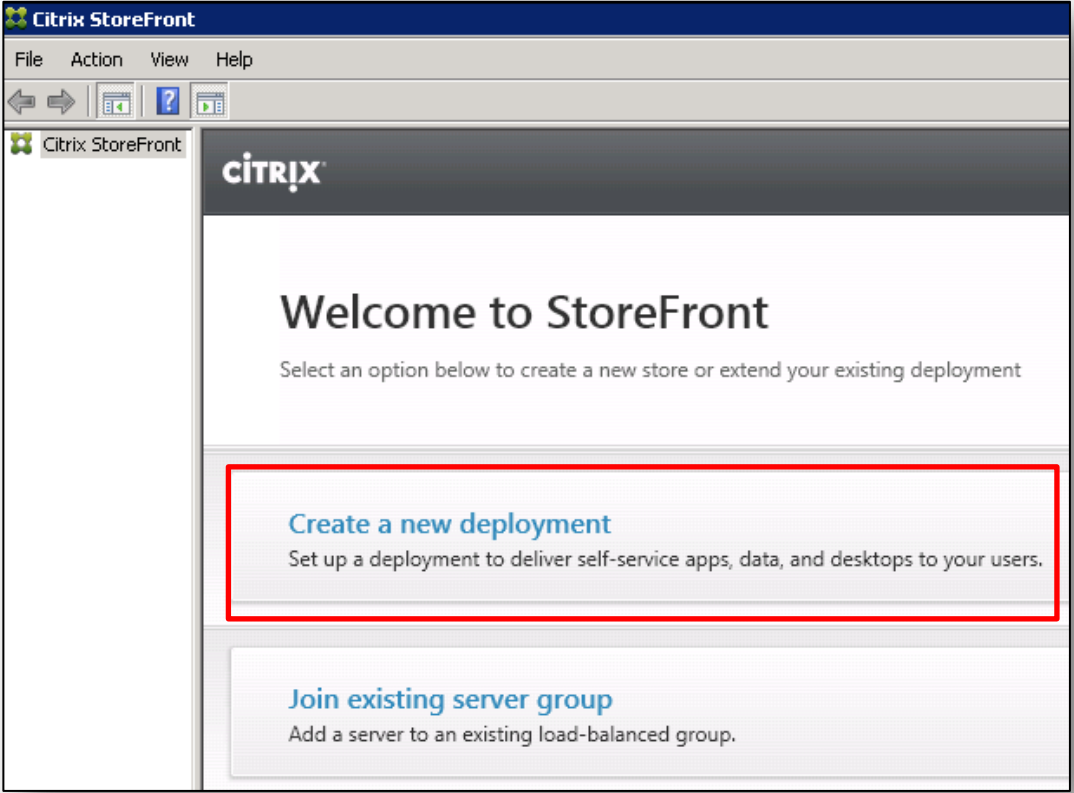
- The **https** binding is now listed
- Return to the **Receiver Storefront console**

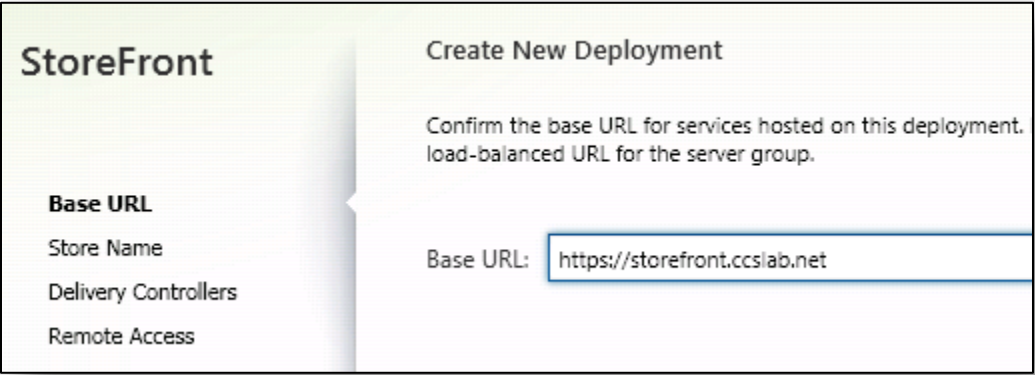
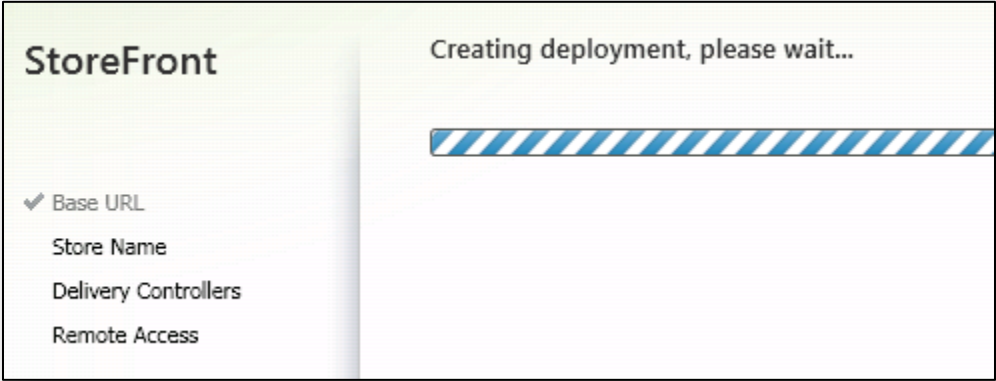
Create New StoreFront Deployment

The section walks through the steps to configure the first StoreFront server in a deployment.

1

When the administration console opens, two options are available. Since this is the first server in the deployment, select **Create a new deployment**



2	<p>Since a SSL certificate has already been bound, the hostname will automatically be filled in. This is the Hostname of the load balancing vServer on the NetScaler for the Storefront servers. If the hostname is blank, go back to the SSL certification installation steps</p> <p>Select Next</p> 
3	<p>Wait for the Store to be created...</p> 
4	<p>Enter in a Store Name</p> <p>It is recommended choosing a name that helps users identify the apps and desktops. This is the name that will appear inside Receiver.</p>

StoreFront

✓ Base URL

Store Name

Delivery Controllers

Remote Access

Store Name

Choose a name that helps users identify the store. The store name a user's account.

Store name:

- 5 This menu allows **XenApp**, **XenDesktop**, and **Cloud Gateway Enterprise** resources to be added to the Store.

To begin adding resources, select **Add**

StoreFront

✓ Base URL

✓ Store Name

Delivery Controllers

Remote Access

Delivery Controllers

Specify the delivery controllers and servers for this store

Delivery controllers:

Name	Type

Add... Edit... Remove

- 7 First, a XenApp server will be added to the Store.

Choose a **Display name**

Choose **XenApp** from the Type list

Change the **Transport type** and **Port** accordingly


Select **Add**

Add Delivery Controller

Display name:

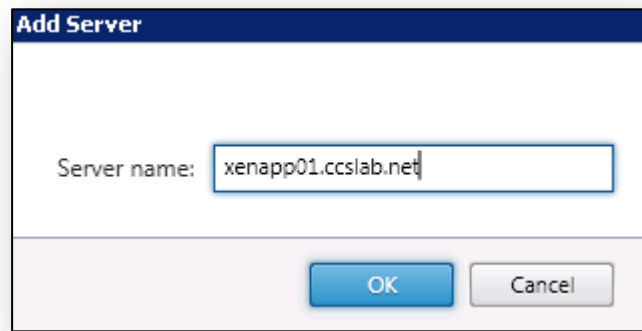
Type: ☐ XenDesktop ☒ XenApp ☐ AppController ☐ VDI-in-a-Box

Servers (in failover order):

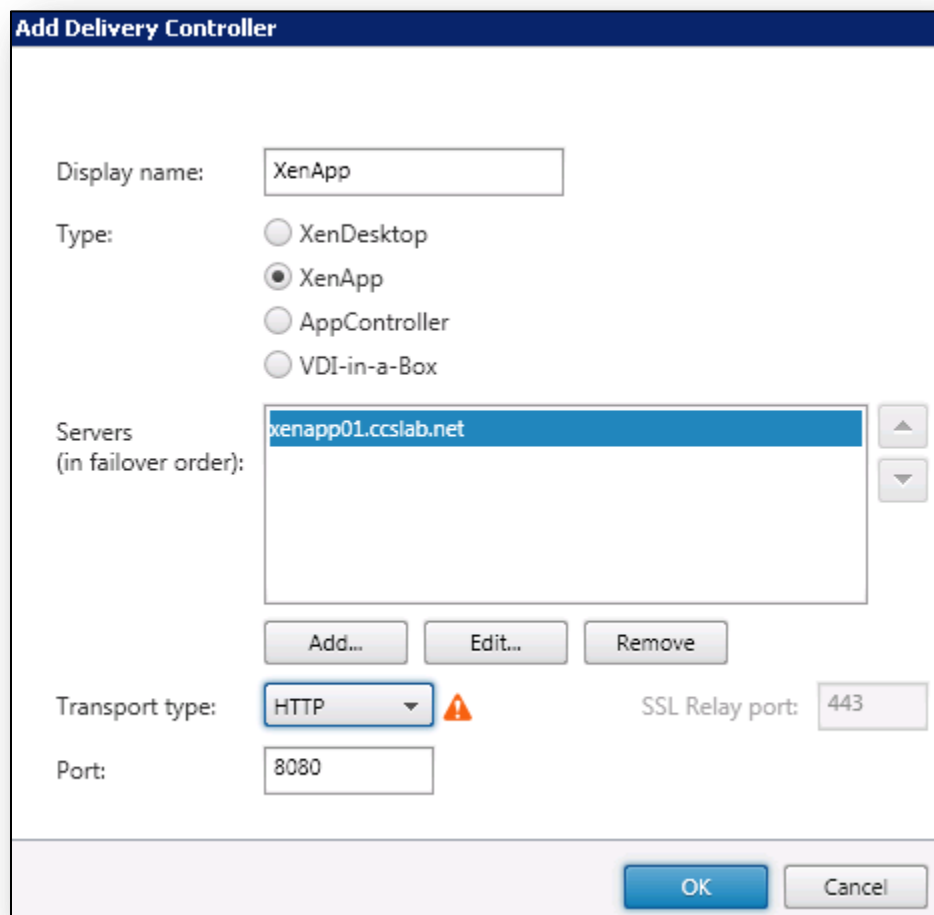
Transport type:  SSL Relay port:

Port:

8 Enter the FQDN of the XenApp server. Select **OK**



- 9 The XenApp server is now listed. Select OK



- 10 To add a XenDesktop resource, the same steps are followed.

Begin by selecting **Add**

The screenshot shows the 'StoreFront' configuration window, specifically the 'Delivery Controllers' tab. On the left, there is a sidebar with options: 'Base URL' (checked), 'Store Name' (checked), 'Delivery Controllers' (selected), and 'Remote Access'. The main area is titled 'Delivery Controllers' and contains the instruction 'Specify the delivery controllers and servers for this store.' Below this, there is a section 'Delivery controllers:' followed by a table. The table has three columns: 'Name', 'Type', and 'Servers'. One entry is visible: 'XenApp' under 'Name', 'XenApp' under 'Type', and 'xenapp01.ccslab.net' under 'Servers'. At the bottom of the window, there are three buttons: 'Add...', 'Edit...', and 'Remove'. The 'Add...' button is highlighted with a red rectangle.

Name	Type	Servers
XenApp	XenApp	xenapp01.ccslab.net

- 11 The XenDesktop type is now selected.
Once a server has been added, select **OK**

Add Delivery Controller

Display name:

Type: ☒ XenDesktop
☐ XenApp
☐ AppController
☐ VDI-in-a-Box

Servers (in failover order):

Transport type: SSL Relay port:

Port:

- 12 Now both XenApp and XenDesktop are listed.
Select **Next**

StoreFront

- ✓ Base URL
- ✓ Store Name
- Delivery Controllers**
- Remote Access

Delivery Controllers

Specify the delivery controllers and servers for this store.

Delivery controllers:

Name	Type	Servers
XenApp	XenApp	xenapp01.ccslab.net
XenDesktop	XenDesktop	xendesktop01.ccslab.net

- 13 This step will begin the Remote Access configuration through NetScaler Gateway. There are two options available: **No VPN tunnel** and **Full VPN tunnel**

Choose one and then select **Add**

StoreFront

- ✓ Base URL
- ✓ Store Name
- ✓ Delivery Controllers
- Remote Access**

Remote Access

Add NetScaler Gateway appliances to provide user access from external networks.

Remote access:

☐ None
☒ No VPN tunnel ⓘ
☐ Full VPN tunnel ⓘ

NetScaler Gateway appliances:

ⓘ

Default appliance:

- 14 Entera **Display Name**, **Gateway URL**, and **Callback URL**

The SubNet IP address field can be left blank

Select Next

StoreFront

General Settings

The display name is visible to users in Citrix Receiver preferences.

Display name: Consulting Lab

NetScaler Gateway URL: https://remote.ccsllab.net

Version: 10.0 (Build 69.4) or later

Subnet IP address: SNIP or MIP (optional)

Logon type: Domain

Smart card fallback: None

Callback URL: <https://remote.ccsllab.net> /CitrixAuth

15 Select Add

StoreFront

Secure Ticket Authority (STA)

Issues session tickets in response to application connection requests.

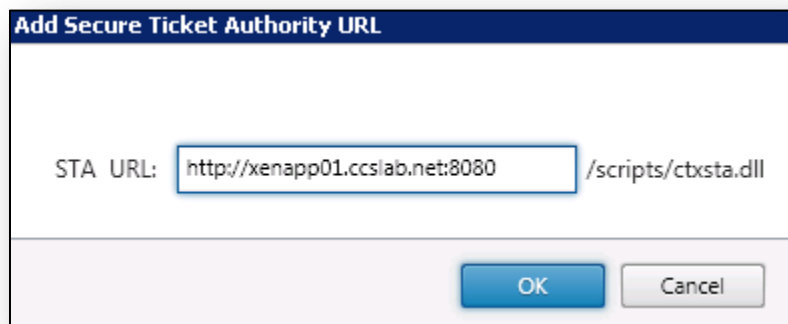
Secure Ticket Authority URLs:

Add... Edit... Remove

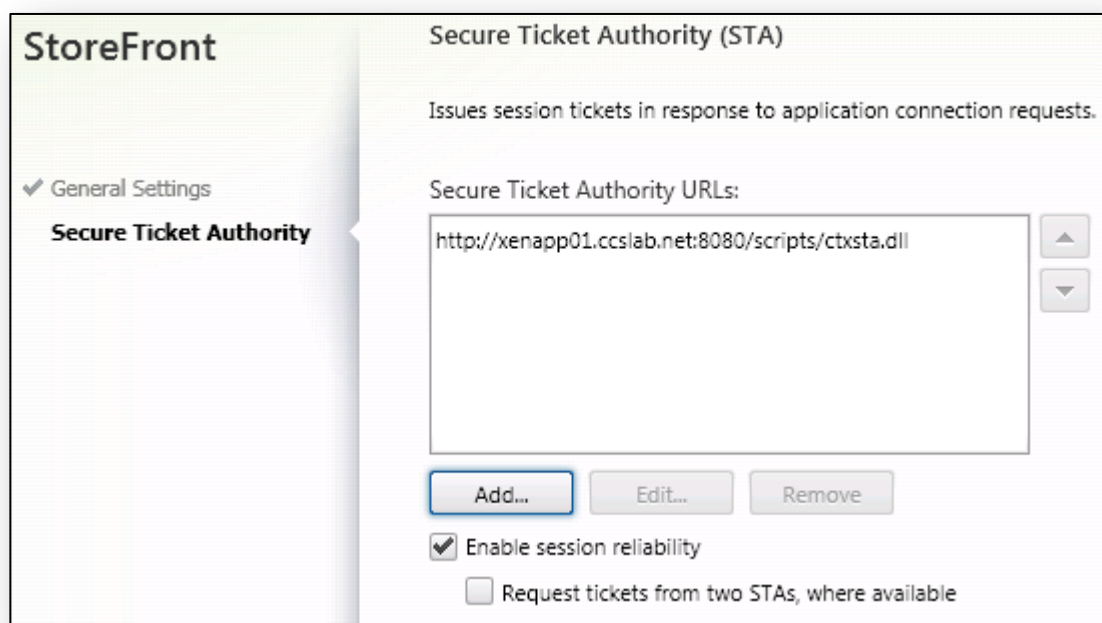
☒ Enable session reliability

☐ Request tickets from two STAs, where available

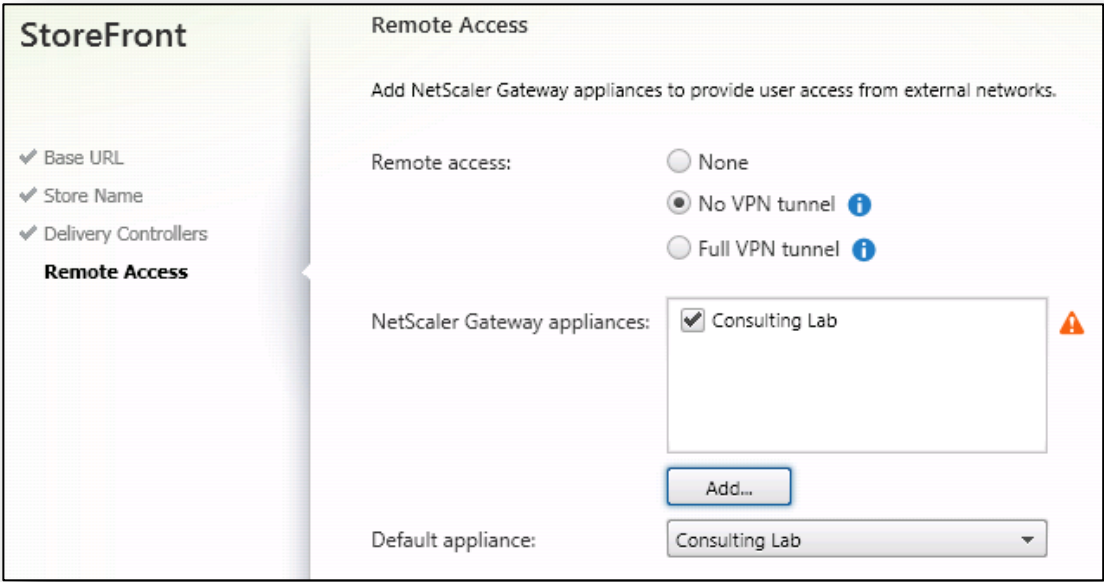
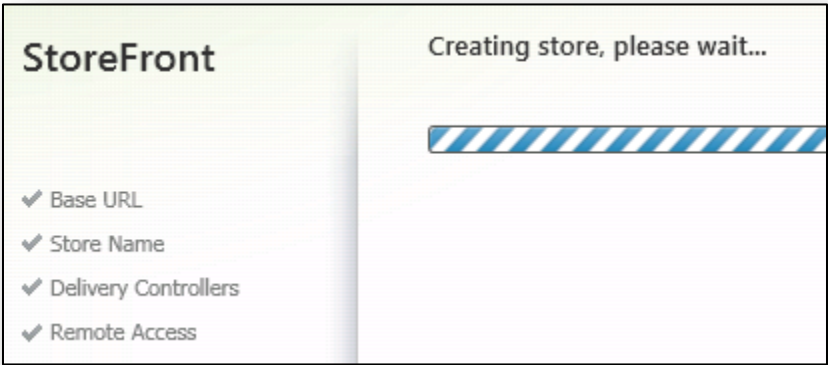
16 Enter the STA URL and select OK

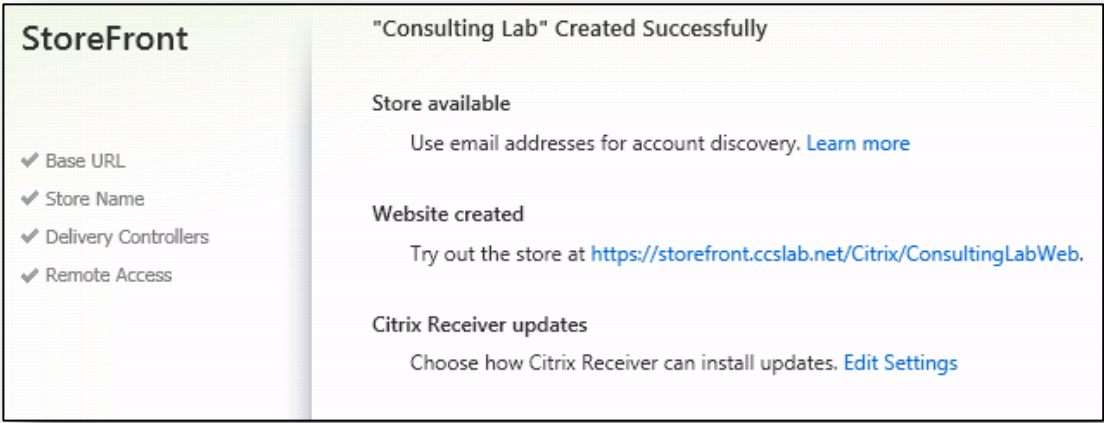


17 Select Create



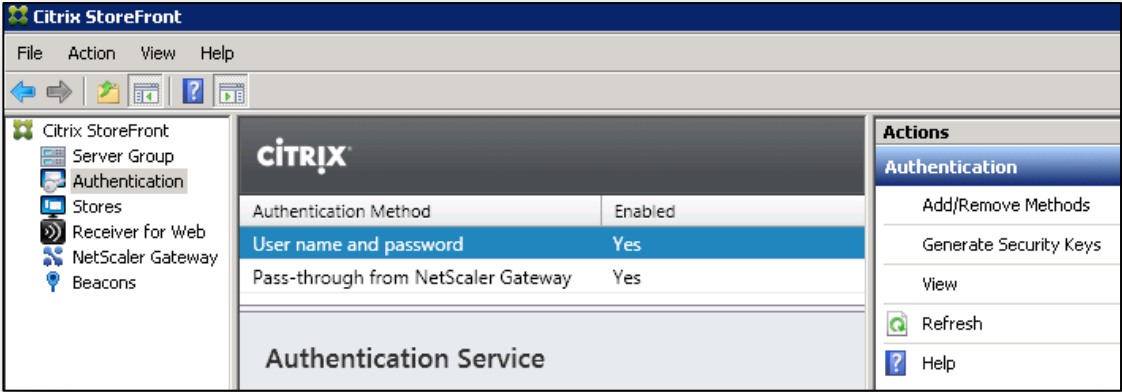
18 Select Create

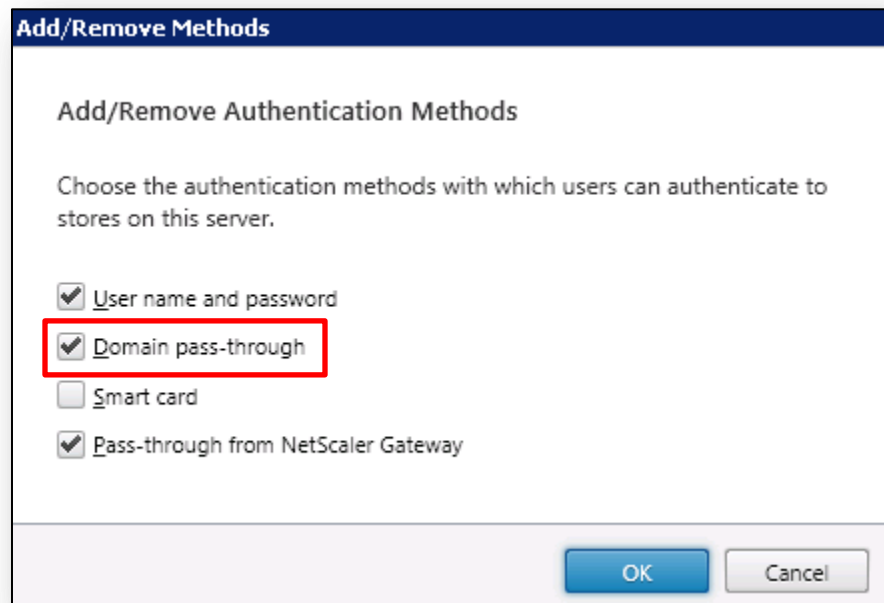
	
19	<p>Wait for the Store to be created ...</p> 
20	<p>Click Finish</p>

	 <p>The screenshot displays the StoreFront configuration interface. On the left, a sidebar lists four items with checkmarks: Base URL, Store Name, Delivery Controllers, and Remote Access. The main area is titled '"Consulting Lab" Created Successfully' and contains three sections: 'Store available' with a link to 'Learn more', 'Website created' with a URL 'https://storefront.ccsllab.net/Citrix/ConsultingLabWeb', and 'Citrix Receiver updates' with a link to 'Edit Settings'.</p>
21	<p>Click on Authentication</p> <p>Observe that the configuration wizard enabled access through NetScaler Gateway and explicit username/password.</p>

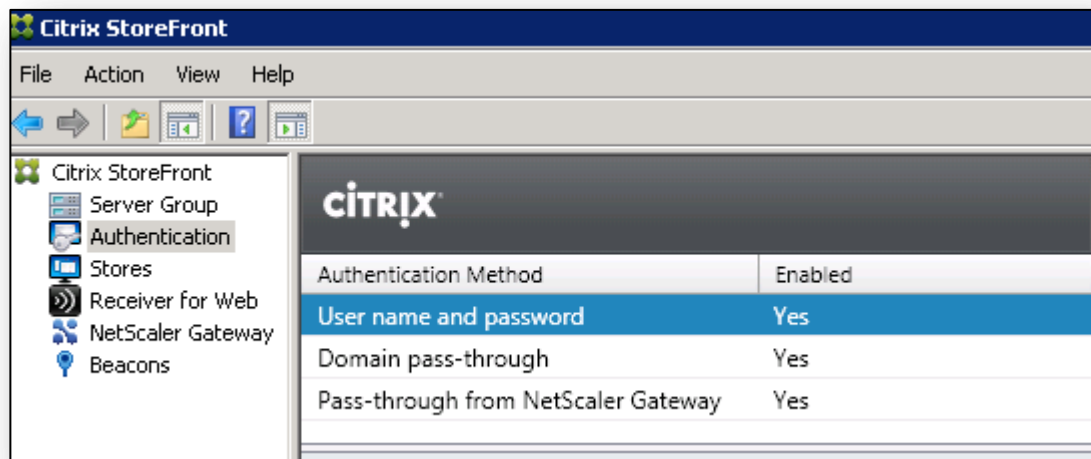
Enable the Pass-Through Authentication Service

By default, during the initial configuration of StoreFront, only Explicit and NetScaler Access Gateway pass-through authentications are enabled. To allow users on the domain to pass-through their Windows credentials to Citrix Receiver, the Domain Pass-Through method must be enabled. This pass-through option only works with the desktop Receiver, not the Receiver for Web page. For Citrix Receiver to utilize single sign-on, it must be installed with the following parameter: CitrixReceiver.exe /includeSSON.

Initial Server Configuration	
Screenshot	
1	<div>Select Add/Remove Methods</div> 



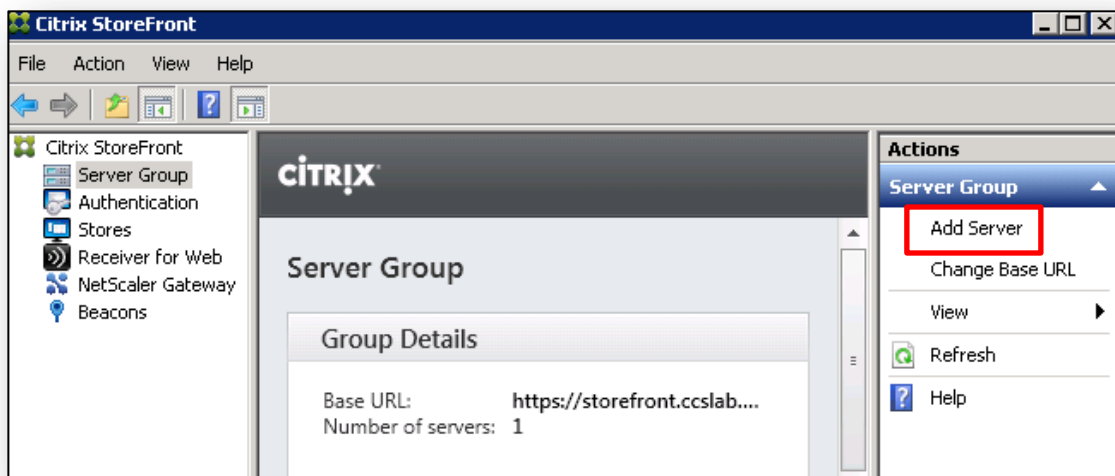
- 3 Domain pass-through authentication has now been enabled.



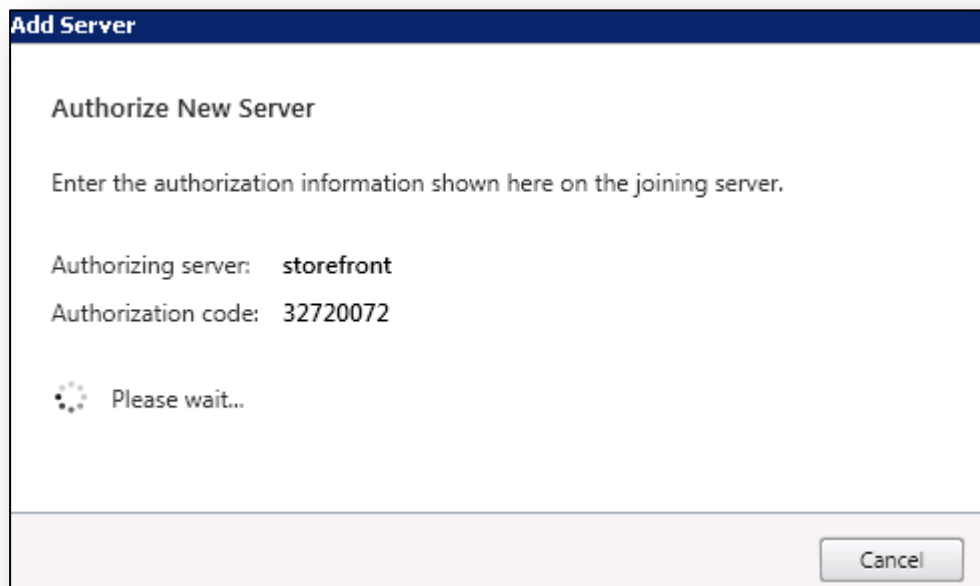
Section 2: Configure Second Receiver StoreFront Server

Once the first server has been configured, a second server should be added to the multi-server deployment.

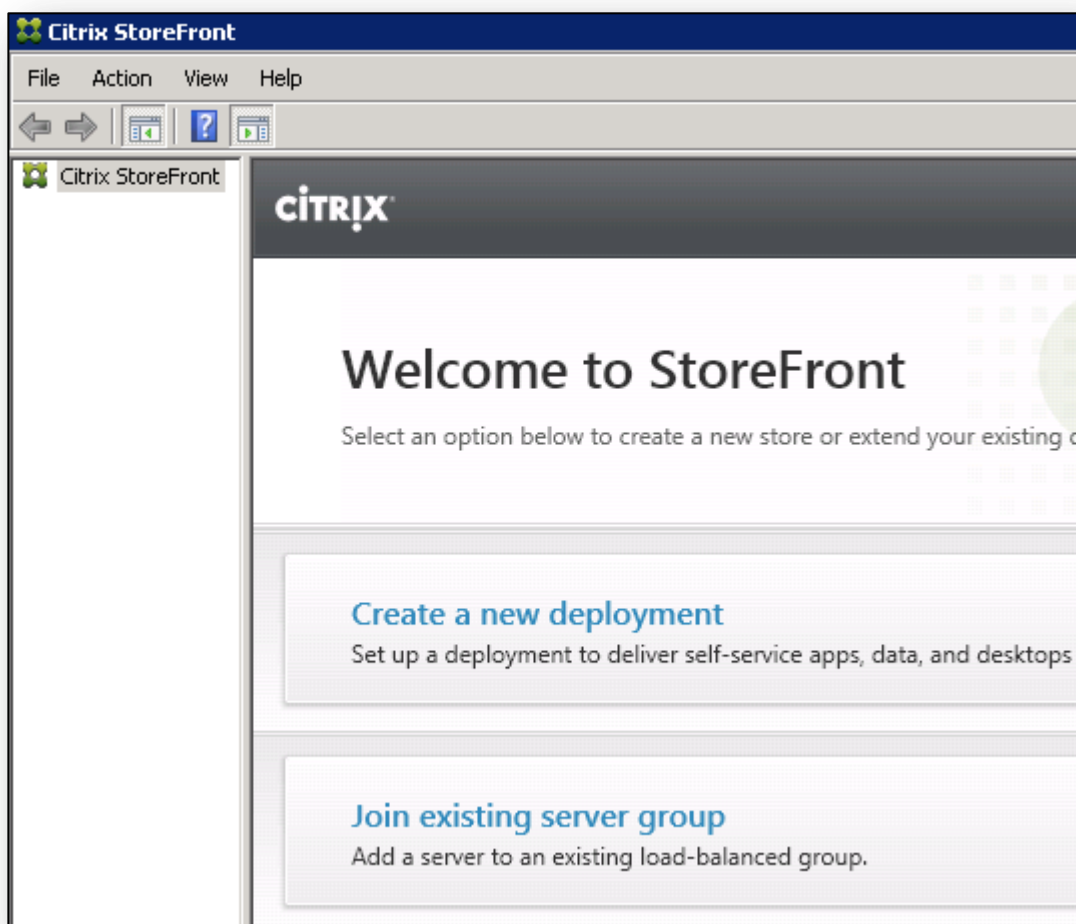
- 1 On the first server deployed select **Add Server** from the **Server Group** menu.



- 2 This server will now show an **Authorization code** that must be entered on the next server joined to the deployment.



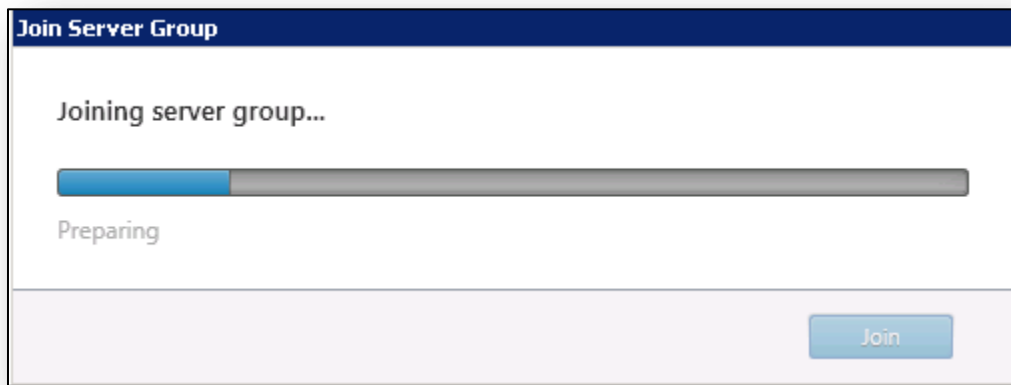
- 3 On the second server select **Join existing server group**



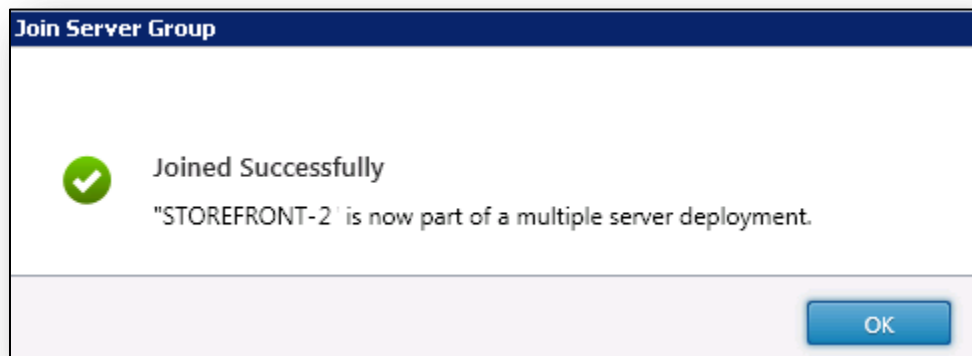
4

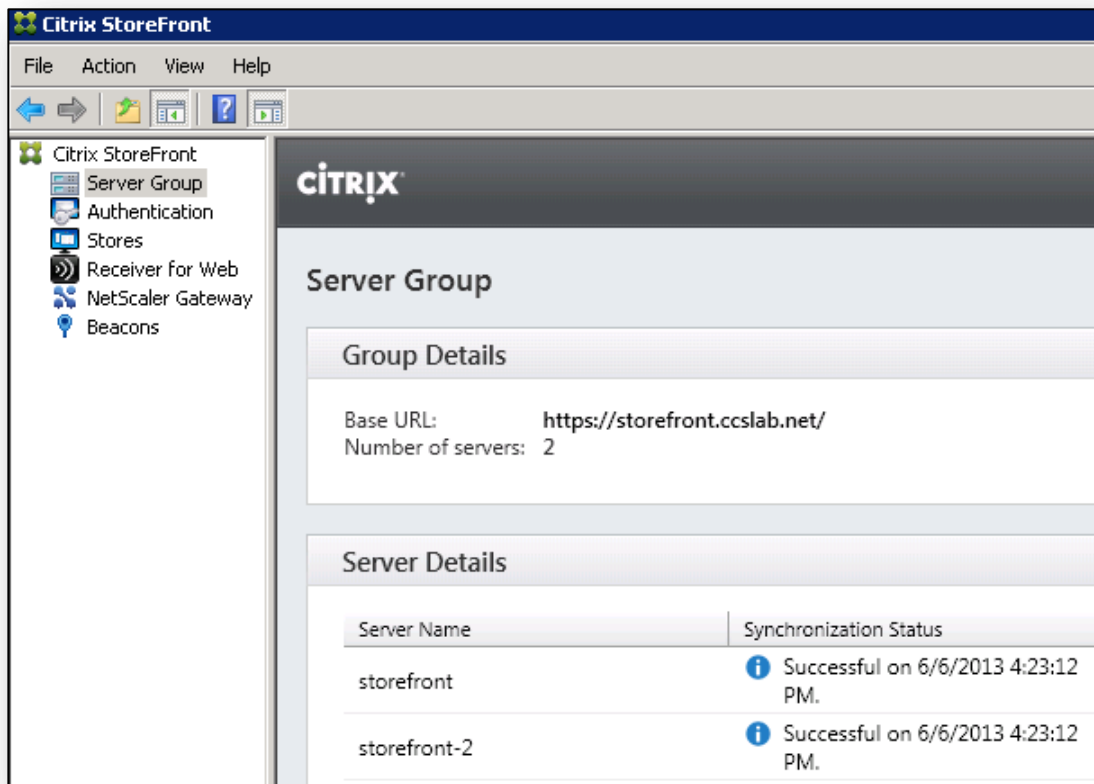
The screenshot shows a 'Join Server Group' dialog box. The title bar reads 'Join Server Group'. The main text says 'Join Server Group' followed by 'To authorize this server, first connect to a server in the group and choose "Add Server". Enter the provided authorization information here.' There are two input fields: 'Authorizing server:' with the value 'storefront' and 'Authorization code:' with the value '32720072'. At the bottom right, there are two buttons: 'Join' and 'Cancel'.

5



6





Section 3: Accessing Applications through Receiver

To simplify the Receiver provisioning process, StoreFront has introduced an auto-discovery service called Account Services. Available beginning with Receiver 3.3 Standard for Windows (Mac 11.6, iOS 5.6, Android 3.1), this feature allows Receiver to automatically provision a user for internal and remote access. This service eliminates the need for users to download Provisioning files and manually import them into Receiver.

To allow users outside the corporate network to provision Receiver, NetScaler 10 build 69.4.nc and higher now includes a new entry in the session policy profile where the StoreFront Account Services URL is specified. The following steps walk through the process of a user provisioning their account inside Receiver through NetScaler Gateway.

1 Configure the Account Services Address on the NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

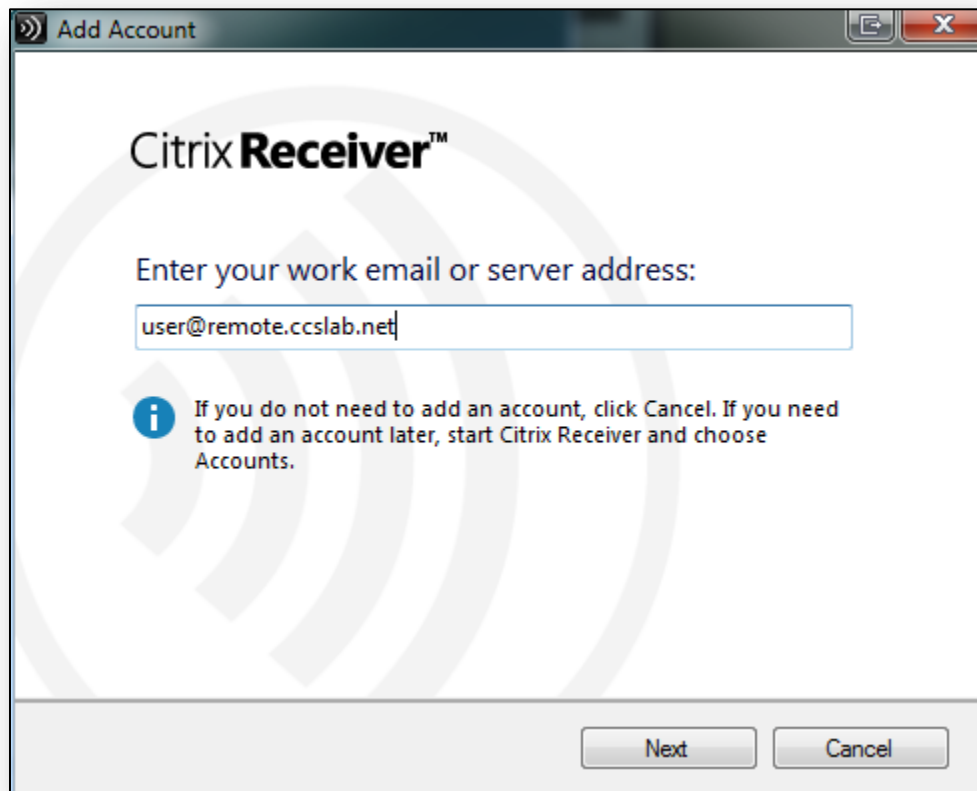
Name* NativeReceiverSF

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

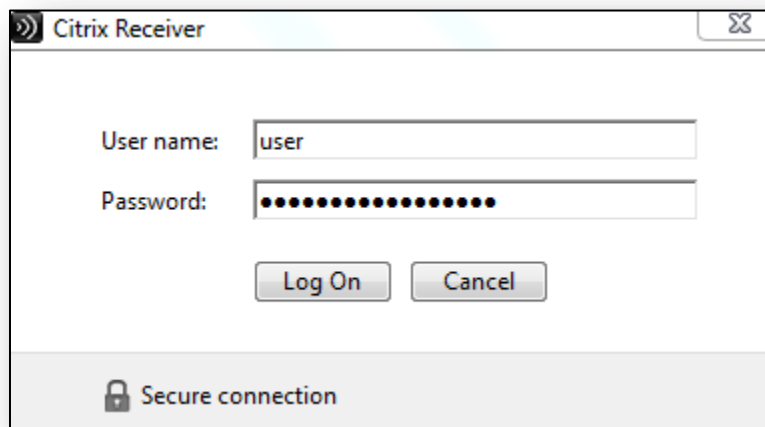
Network Configuration | Client Experience | Security | Published Applications

		Override Global
ICA Proxy	OFF	<input checked="" type="checkbox"/>
Web Interface Address		<input type="checkbox"/>
Web Interface Portal Mode	NORMAL	<input type="checkbox"/>
Single Sign-on Domain		<input type="checkbox"/>
Citrix Receiver Home Page		<input type="checkbox"/>
Account Services Address	https://storefront.ccsllab.net	<input checked="" type="checkbox"/>

2

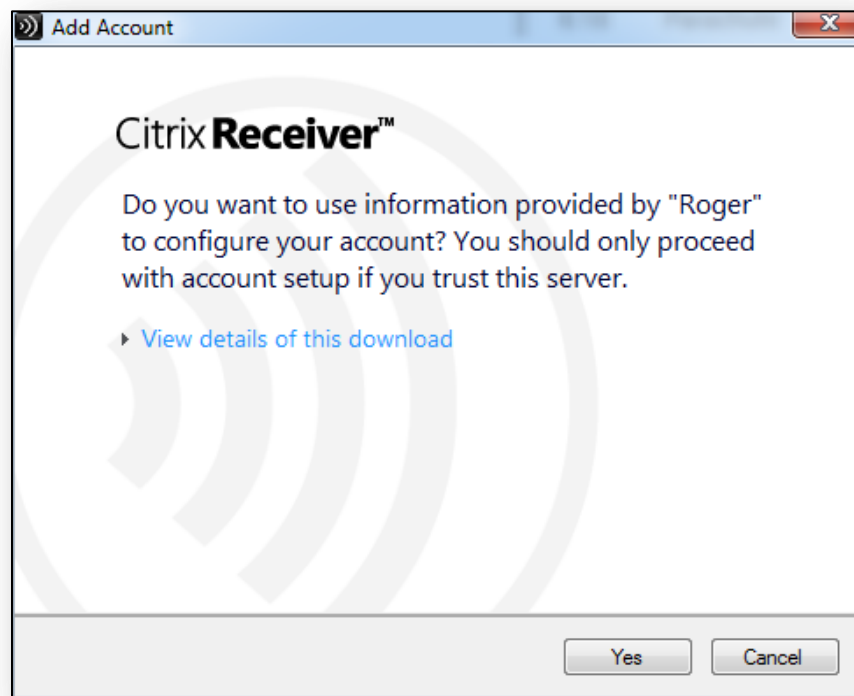


3

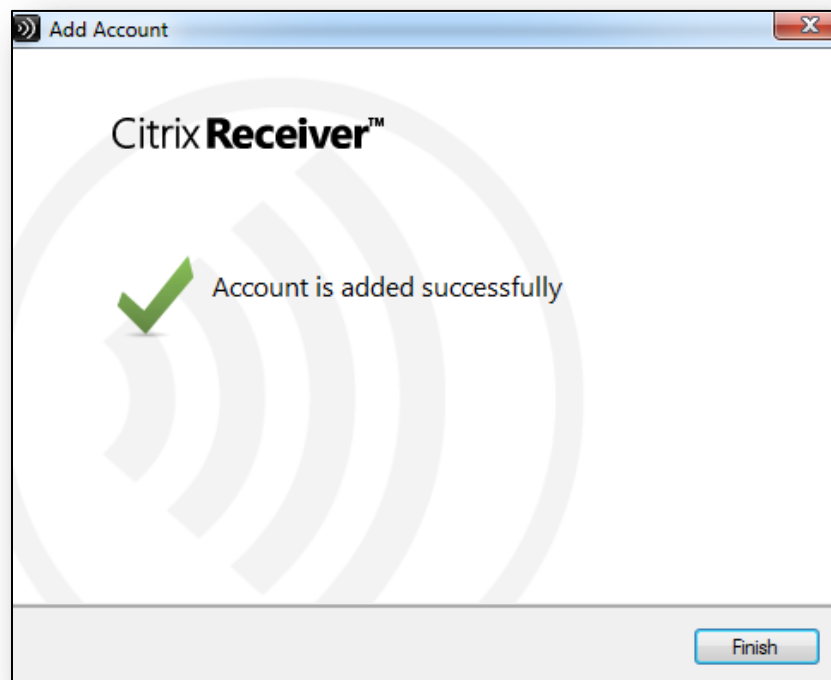


4

Click Yes



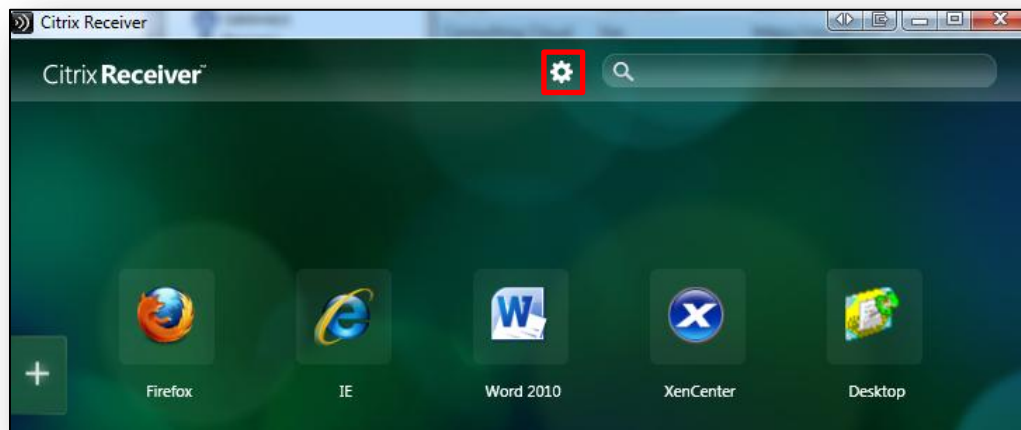
5 Click **Finish**



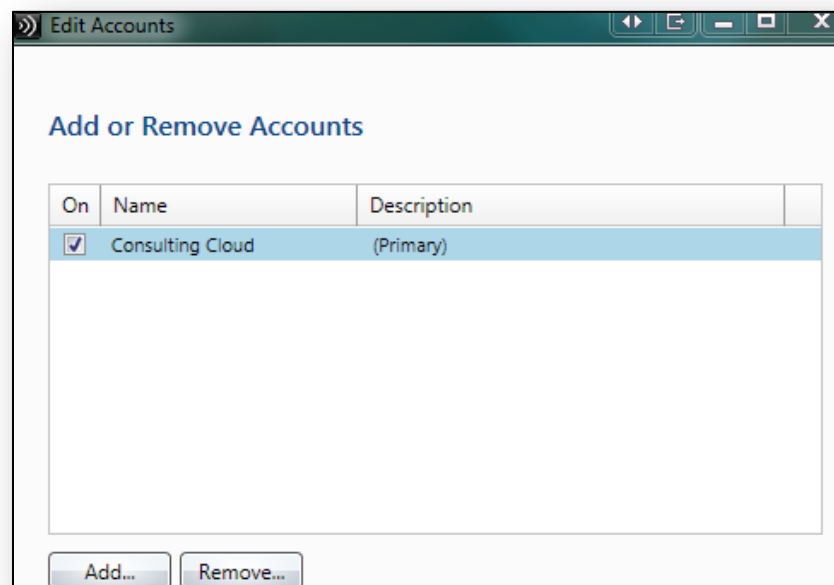
6 Receiver will now display the subscribed resources. Applications and desktops are now

ready to be launched

Click the **Settings** icon



7 Stores can be added and removed from this menu



Receiver for Web

In addition to accessing StoreFront Stores within Citrix Receiver Standard, users can also access applications and desktops through a web page. The Receiver for Web site allows users to easily connect to their resources on devices that might not have Citrix Receiver installed. It supports launching applications with the full Receiver, Receiver Web Plug-in, or HTML5 client. This gives users the flexibility to access resources on devices on which they do not have permission to install the full Receiver. Receiver for Web also separates applications and desktops and into tabs, with all desktops available to the user automatically appearing on the desktop page. It also provides user driven desktop restarts functionality for XenDesktop resources.



Figure2: Apps View

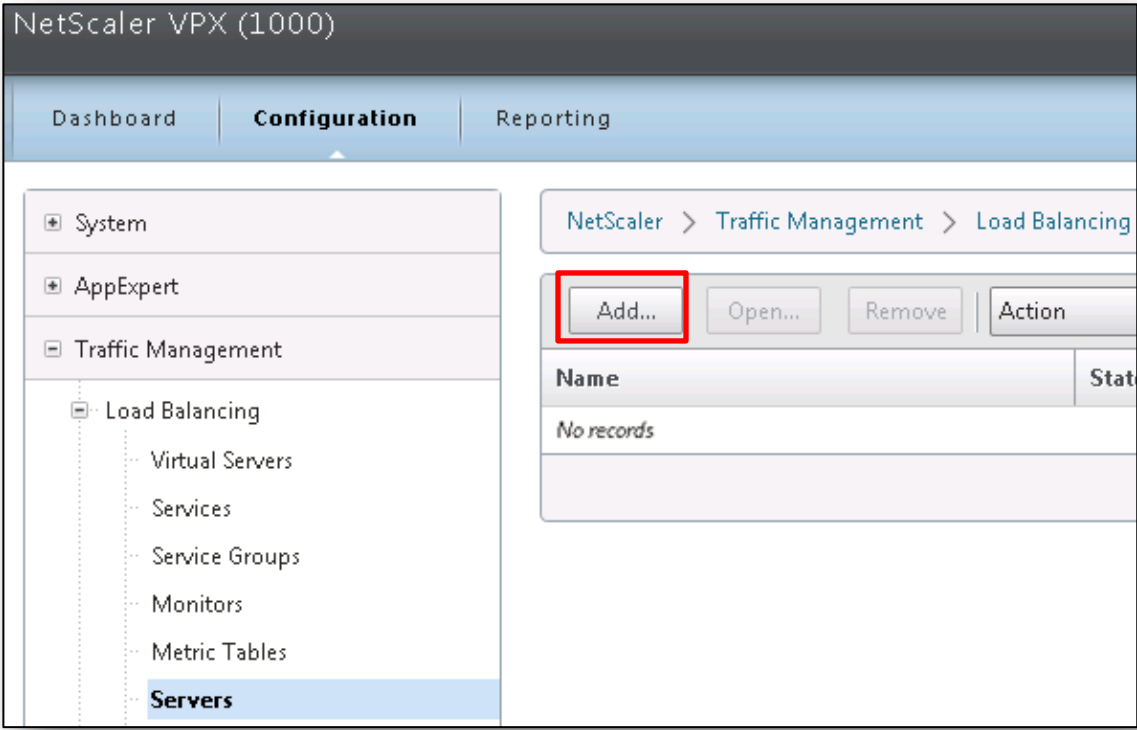


Figure 3: Desktops View

Section 4: NetScaler Load Balancing Configuration

This section will give an overview of the steps necessary to configure a NetScaler to load balance StoreFront. NetScaler 10.1 includes a new health monitor designed to intelligently monitor StoreFront. This allows NetScaler to provide a high level of reliability to the deployment.

1	From the Load Balancing menu, select Servers Select Add
---	--

	 <p>NetScaler VPX (1000)</p> <p>Dashboard Configuration Reporting</p> <p>System</p> <p>AppExpert</p> <p>Traffic Management</p> <p>Load Balancing</p> <ul style="list-style-type: none"> Virtual Servers Services Service Groups Monitors Metric Tables Servers <p>NetScaler > Traffic Management > Load Balancing</p> <p>Add... Open... Remove Action</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td colspan="2">No records</td> </tr> </tbody> </table>	Name	Status	No records	
Name	Status				
No records					
2	<p>Choose a name and enter in the IP Address for both StoreFront servers</p> <p>Select Create after each server is entered</p>				

Create Server

Server Name*

☒ IP Address ☐ Domain Name

IPAddress* . . . ☐ IPv6

Traffic Domain ID

Translation IP Address

Translation Mask

Resolve Retry (secs)

☐ IPv6 Domain

☒ Enable after Creating

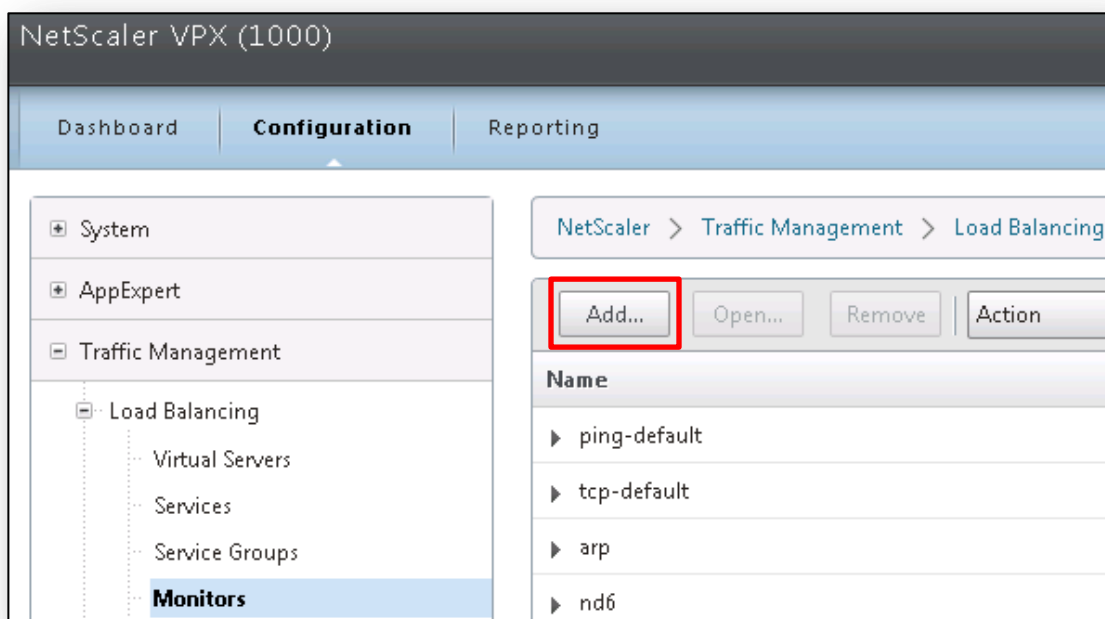
Comments

3 Both StoreFront servers are now listed

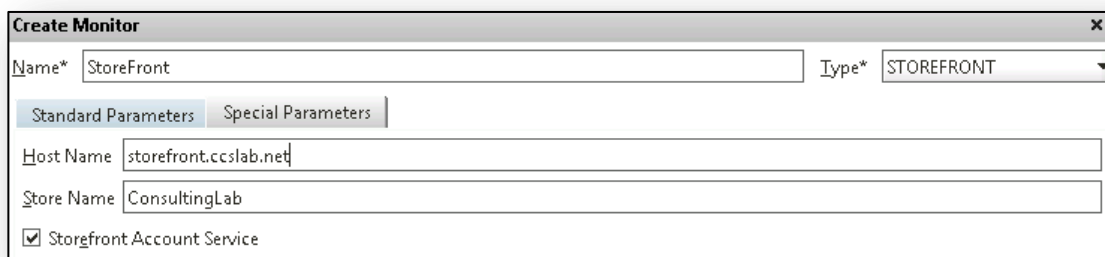
NetScaler > Traffic Management > Load Balancing > Servers

Name	State	IPAddress / Domain
StoreFront	Enabled	192.168.1.122
StoreFront-2	Enabled	192.168.1.177

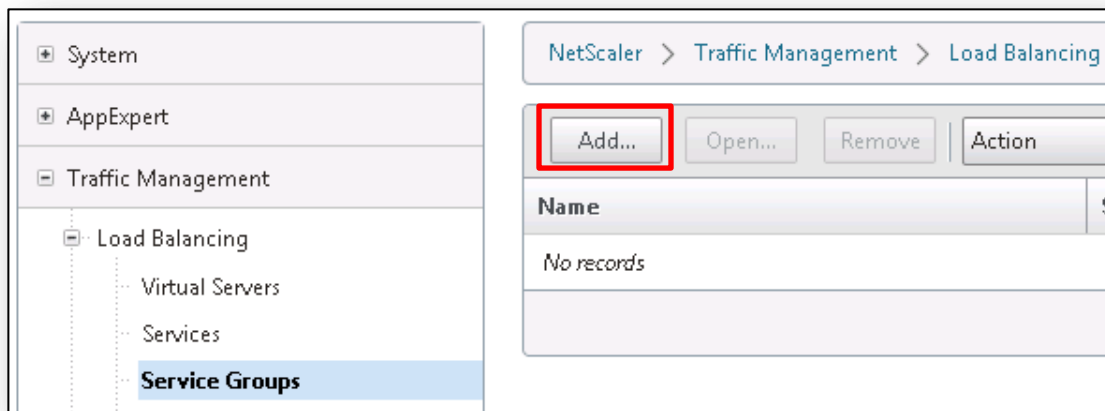
4 From the Load Banacing menu, choose **Monitors**
Select **Add**



- 5 Choose a name for the Monitor and select **StoreFront** as the **Type**
 Leave the Standard Parameters settings default and choose the **Special Parameters** tab
 Enter in the **Hostname** used for the StoreFront group along with the **Store Name**
 Check **StoreFront Account Services**
 Click **Create**



- 6 Choose Service Groups from the Load Balancing menu
 Creating a Service Group allows a single health monitor to be attached to both servers
 Select **Add**



- 7 Enter in a **Service Group Name**. Choose **SSL** for the **Protocol**
Select the two StoreFront servers and enter **443** as the Port and then click **Add**

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
StoreFront	192.168.1.122	443	1	"None"		To be Enabled
StoreFront-2	192.168.1.177	443	1	"None"		To be Enabled

- 8 Select the **Monitors** tab and choose the previously created StoreFront monitor and click **Add**.
It will then appear as a configured monitor

Create Service Group

Service Group Name* StoreFront Protocol* SSL

Traffic Domain ID

☒ Enable Service Group ☒ Enable Health Monitoring ☐ AppFlow Logging

Members Monitors Profiles Advanced SSL Settings

Available

Monitors

arp

nd6

ping

tcp

http

tcp-ecv

http-ecv

udp-ecv

Add >

Configured

Monitors	Weight	State	Passive
StoreFront	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- 9 Choose the **Advanced** tab
Click **Override Global**, uncheck **Use Source IP**
Click **Client IP Header** and enter in **X-Forwarded-For**

Create Service Group

Service Group Name* StoreFront

Traffic Domain ID

☒ Enable Service Group ☒ Enable Health Monitoring ☐ AppFlow Logging

Members Monitors Profiles Advanced SSL Settings

Thresholds

☐ Override Global

Max Requests 0

Max Clients 0

Idle Time-out (secs)

Client

Settings ☒ Override Global

☐ Use Source IP ☐ Client Keep-Alive ☐ TCP Buffering ☒ Compression

☒ Client IP Header X-Forwarded-For

- 10 Choose the **SSL Settings** tab
Select the SSL certificate for the StoreFront servers and click **Add**

Click Create

Create Service Group

Service Group Name*

Traffic Domain ID

☒ Enable Service Group ☒ Enable Health Monitoring ☐ AppFlow Logging

Members Monitors Profiles Advanced **SSL Settings**

Available

Certificates
ns-server-certificate
WildCard Cert

Configured

Certificates
WildCard Cert

- 11 Select **Virtual Servers** from the Load Balancing menu.
Select **Add**

NetScaler VPX (1000)

Dashboard **Configuration** Reporting

System AppExpert Traffic Management Load Balancing **Virtual Servers**

NetScaler > Traffic Management > Load Balancing

Name

No records

- 12 Enter a **Name** and **IP Address** for the Virtual Server
Choose **SSL** for the **Protocol**

Create Virtual Server (Load Balancing)

Name* ☒ IP Address Based ☐ IP Pattern Based

Protocol* IP Address* ☐ IPv6

☐ Network VServer Range Port*

☒ Directly Addressable ☒ State ☐ AppFlow Logging Traffic Domain ID

Services Service Groups Policies Method and Persistence Advanced Profiles SSL Settings

- 13** Choose the **Service Groups** tab
Choose the previously created **StoreFront** Service Group

Create Virtual Server (Load Balancing)

Name* ☒ IP Address Based ☐ IP Pattern Based

Protocol* IP Address* ☐ IPv6

☐ Network VServer Range Port*

☒ Directly Addressable ☒ State ☐ AppFlow Logging Traffic Domain ID

Services **Service Groups** Policies Method and Persistence Advanced Profiles SSL Settings

[Activate All](#) [Deactivate All](#)

Active	Service Group Name	Protocol
<input checked="" type="checkbox"/>	StoreFront	SSL

- 14** Choose the **Method and Persistence** tab
Select **SOURCEIP** as the **Persistence**

Create Virtual Server (Load Balancing)

Name* ☒ IP Address Based ☐ IP Pattern Based

Protocol* IP Address* ☐ IPv6

☐ Network VServer Range Port*

☒ Directly Addressable ☒ State ☒ AppFlow Logging Traffic Domain ID

Services | Service Groups | Policies | Method and Persistence | **Advanced** | Profiles | SSL Settings

LB Method

Method New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence Time-out (min)

IPv4 Netmask IPv6 Mask Length

Backup Persistence

Persistence Time-out (min)

IPv4 Netmask IPv6 Mask Length

Comments

[Help](#)

- 15 Choose the **SSL Settings** tab
Select the SSL certificate and click **Add**
Click **Create**

Create Virtual Server (Load Balancing)

Name* ☒ IP Address Based ☐ IP Pattern Based

Protocol* IP Address* ☐ IPv6

☐ Network VServer Range Port*

☒ Directly Addressable ☒ State ☐ AppFlow Logging Traffic Domain ID

Services | Service Groups | Policies | Method and Persistence | **Advanced** | Profiles | **SSL Settings**

Available

Certificates
ns-server-certificate
Wildcard Cert

Configured

Certificates	Type	Check	Skip CA
Wildcard Cert	Server Certificate	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Section 5: NetScaler Gateway for Remote Access

To provide remote access for users located outside the corporate network, it is recommended that StoreFront be deployed in conjunction with NetScaler Gateway, formally known as Access Gateway. NetScaler Gateway acts as a reverse proxy, tunneling all Citrix HDX traffic over SSL. Remote users have the option of accessing their resources from either the locally installed Citrix Receiver or via the Receiver for Web site. For an optimal deployment that allows users to easily connect from inside and outside the organization, it is recommended that the Account Services feature be implemented. This feature will allow users to seamlessly configure their locally installed Receiver for external access through NetScaler Gateway. This feature essentially automates the process of downloading and importing a Provisioning file.

A Provisioning file is a XML file that includes the necessary information to allow Receiver to decide whether it should connect directly to StoreFront or through NetScaler Gateway. This decision is made by using the beacon addressees included in the file. If Receiver is able to resolve the internal Beacon address, it will connect directly to StoreFront. By default, the internal Beacon address is set to the load balancing hostname for the StoreFront servers, although this can be changed in the Beacons menu inside StoreFront. For more information on configuring the Receiver Provisioning file, please reference [Citrix eDocs](#).

Session Policies

To direct remote users to the optimal location, multiple session policies should be created on NetScaler Gateway. Using HTTP headers, the NetScaler is able to detect if the connection is being made from a web browser or directly from inside Receiver. Below is an example of the session policies required for Native Receiver and Receiver for Web access.

Priority	Policy Name	Expression	Profile
10	Native Receiver	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS	Native Receiver
20	Receiver for Web	ns_true	Receiver for Web

Profile Name	Settings
Native Receiver	ICA Proxy: On Clientless Access: On Account Services URL: StoreFront Server FQDN WebInterface URL: StoreFront Server FQDN SSO Domain
Receiver for Web	ICA Proxy: On WebInterface URL: StoreFront Receiver for Web page SSO Domain

To function correctly, Citrix Receiver requires that the StoreFront Services traffic not be rewritten, as would normally be the case when NetScaler Gateway is operating in Clientless Access (CVPN) mode. To disable rewriting, it is necessary to define a custom rewrite policy for Clientless mode. Under the Clientless Session Policies tab, a new policy should be created and binded. The URL Rewrite policy should be set to ns_cvpn_default_inet_url_label and the expression set to true.

Certificates

Authentication

Bookmarks

Policies

Intranet Applications

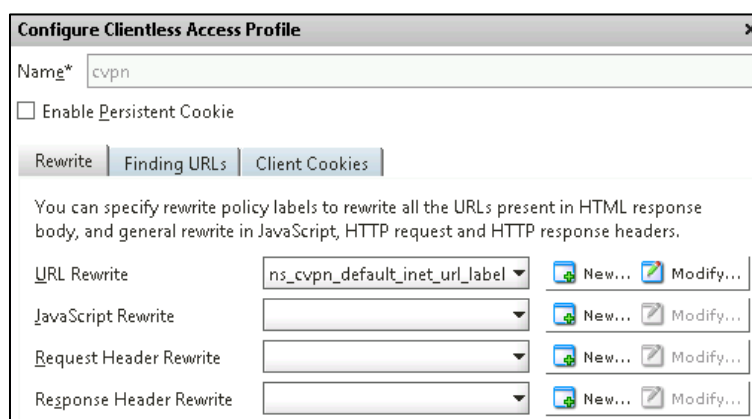
Int

Session
 Traffic
 Auditing
 Pre-authentication

Clientless
 Cache

Priority	Policy Name	Expression
100	cvpn	true

Figure 4. Clientless Access Policy



Configure Clientless Access Profile

Name* cvpn

☐ Enable Persistent Cookie

Rewrite Finding URLs Client Cookies

You can specify rewrite policy labels to rewrite all the URLs present in HTML response body, and general rewrite in JavaScript, HTTP request and HTTP response headers.

URL Rewrite ns_cvpn_default_inet_url_label New... Modify...

JavaScript Rewrite New... Modify...

Request Header Rewrite New... Modify...

Response Header Rewrite New... Modify...

Figure 5. Clientless Access Profile

HTML5 Receiver Client

StoreFront 2.0 is packaged with a native HTML5 Citrix Receiver client that can be used as a fallback client if the native Receiver is not installed. Receiver for HTML5 allows connections to through a browser without having to install any software on the endpoint. The Java client, which was previously used as the fallback option with Web Interface is no longer supported with StoreFront. The HTML5 client can be enabled during the initial StoreFront configuration or afterwards on the Receiver for Web section of the administration console. Administrators have the option of configuring the HTML Receiver the primary client for all users or configuring it as a fallback if the native Receiver is not installed. The only exception to the configured options is ChromeOS which always will use the HTML5 client. Before deploying the HTML5 client, please verify your environment against [Citrix eDocs](#) for a list the prerequisites that must be in place.

Conclusion

Citrix Consulting currently recommends StoreFront be implemented in a phased approach beginning with pilot environment for mobile users. This user group will see the greatest benefit from having a seamless experience between devices regardless of their location. The pilot environment should deliver resources from the production XenDesktop & XenApp deployments. Additionally, StoreFront should be deployed in parallel to the existing Web Interface environment on a separate Windows server instance. This will ensure a smooth transition while not disturbing any user groups that are utilizing Web Interface.

Acknowledgments

Citrix Consulting Solutions would like to thank all of the individuals that offered guidance and technical assistance during the course of this project – Roger LaMarca, Carisa Stringer, Andy Baker, Peter Schulz, and Adolfo Montoya. Additionally, thanks go to Peter Smeryage who helped with the build out of the environment.

Revision History

Revision	Change Description	Updated By	Date
----------	--------------------	------------	------

1.0	Initial Document	Citrix Consulting Solutions	March 27, 2012
1.2	Document Update	Citrix Consulting Solutions	April 12, 2012
1.3	Document Update	Citrix Consulting Solutions	July 31, 2012
1.4	Document Update	Citrix Consulting Solutions	June 28 , 2013
1.5	Document Update	Citrix Consulting Solutions	August 15, 2013

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of Fortune Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2009 was \$1.61 billion.

©2013 Citrix Systems, Inc. All rights reserved. Citrix®, Access Gateway™, Branch Repeater™, Citrix Repeater™, Citrix Receiver™, HDX™, XenServer™, XenApp™, XenDesktop™, XenClient™ and Citrix Delivery Center™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.