Optimal Gateway Routing for Storefront & NetScaler

Abstract

Citrix XenApp and Citrix XenDesktop are the best way to deliver apps and data securely. Citrix NetScaler is the best and most secure way to deliver XenApp and XenDesktop, as well as web and SaaS apps to your users so that they can work anywhere, on any device.

At Citrix, we deliver these services to our users from multiple data centers around the globe to ensure the best experience whether they are working from Singapore, London, Sao Paolo or San Francisco. We use Citrix NetScaler GSLB to deliver these services via a single URL, so that our users have a single URL to remember regardless of where they live and work. We also leverage NetScaler GSLB to provide high-availability for our users in the event of an Internet circuit outage or other unplanned event that might prevent users from accessing their local data center.

NetScaler GSLB works great the vast majority of the time. However, the fact that it is a DNS-based technology means that a number of users experience GSLB misdirects to a sub-optimal NetScaler Gateway. This can result in a sub-optimal user experience for those users.

To learn more about NetScaler GSLB, please visit this page: https://docs.citrix.com/en-us/netscaler/11/traffic-management/gslb/how-gslb-works.html

Our NetScaler team listened to our customers, and delivered a solution that uses NetScaler Gateway and Citrix Storefront to deliver the best user experience by ensuring that HDX launches occur via the closest NetScaler Gateway, even if the users connect to a sub-optimal gateway.

The idea behind optimal NetScaler Gateway routing for a Storefront store is quite simple and useful in our specific scenario. This architecture and related configurations allows you to route the user authentication to any of your StoreFront servers, but will ensure that the HDX app or desktop launch connects through the local NetScaler so that the connection is secure, and he user experience optimized. The credential handling is secured between the client machine and the StoreFront servers via SSL. With the customization completed on the StoreFront servers, the ICA Ticket then routes the user connection through the optimal NetScaler, regardless of which NetScaler is used during authentication.

In order to configure your NetScaler and Storefront environments for NetScaler Gateway Routing, you must have both NetScaler 11.0 build 66.11 or later and Storefront 3.x in place in your environment.

NetScaler Gateway Routing – Sub-optimal vs. Optimal

To illustrate the problem, image having two (2) data centers, one in the United Kingdom (UK) (Network A) and one in the United States (US) (Network B). You want to simplify the experience for your users, as well as provide high-availability for apps and data, so you use NetScaler GSLB to deliver both sites via a single URL. However, some users are experiencing high-latency due to GSLB misdirects. The problem is that when they authenticate on the sub-optimal Gateway, the HDX or ICA launch occurs via the sub-optimal Gateway. See Figure 1 below for a visual representation. Please note that both the authentication and HDX launch are completed via the same Gateway – this is the default behavior.

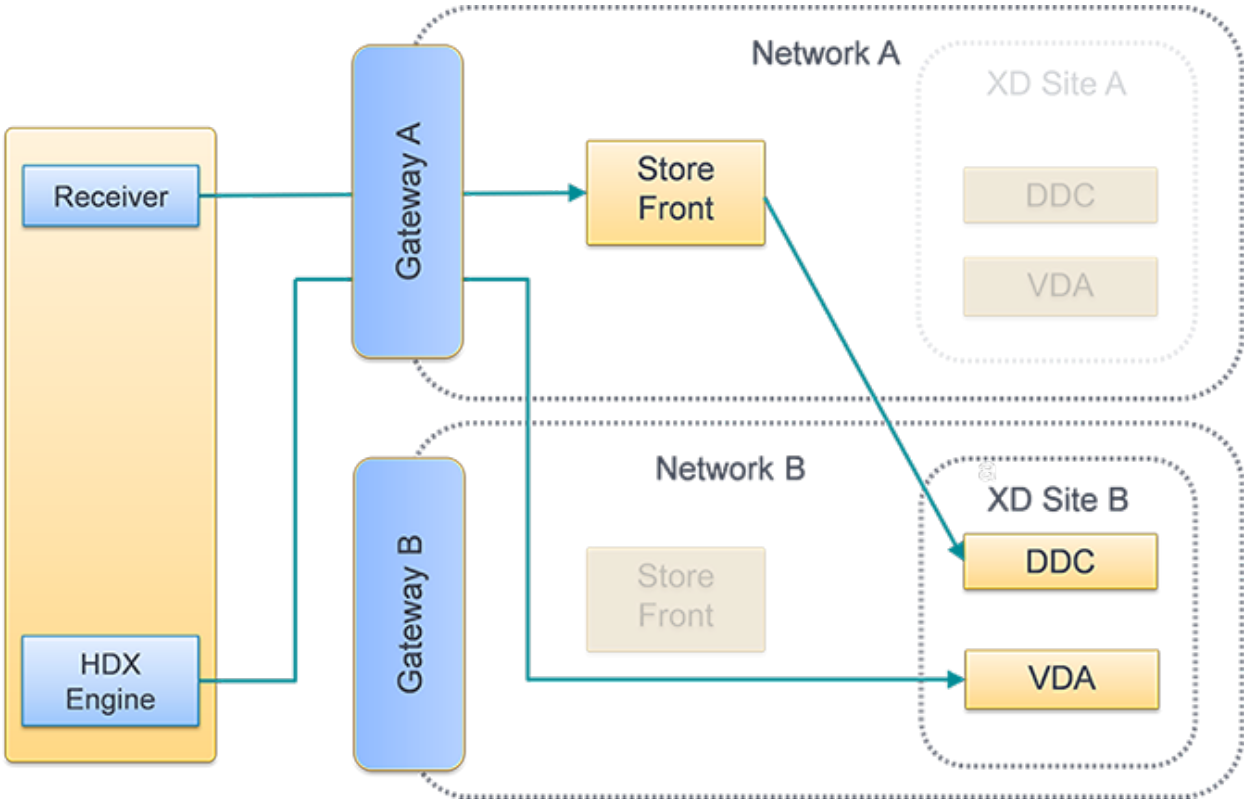


Figure 1. Suboptimal gateway routing

The NetScaler Gateway Routing solution essentially de-couples or separates the initial logon Gateway from the HDX launch Gateway, based on where the app or desktop is located, not where you log on. This helps solve the GSLB misdirection problem that some users may be experiencing, while maintaining the integrity of the system. See Figure 2 below for a visual representation of the NetScaler Gateway Routing behavior. Please note that while the initial logon is completed through Gateway A, the subsequent HDX launch is completed via Gateway B, thus ensuring an optimal user experience.

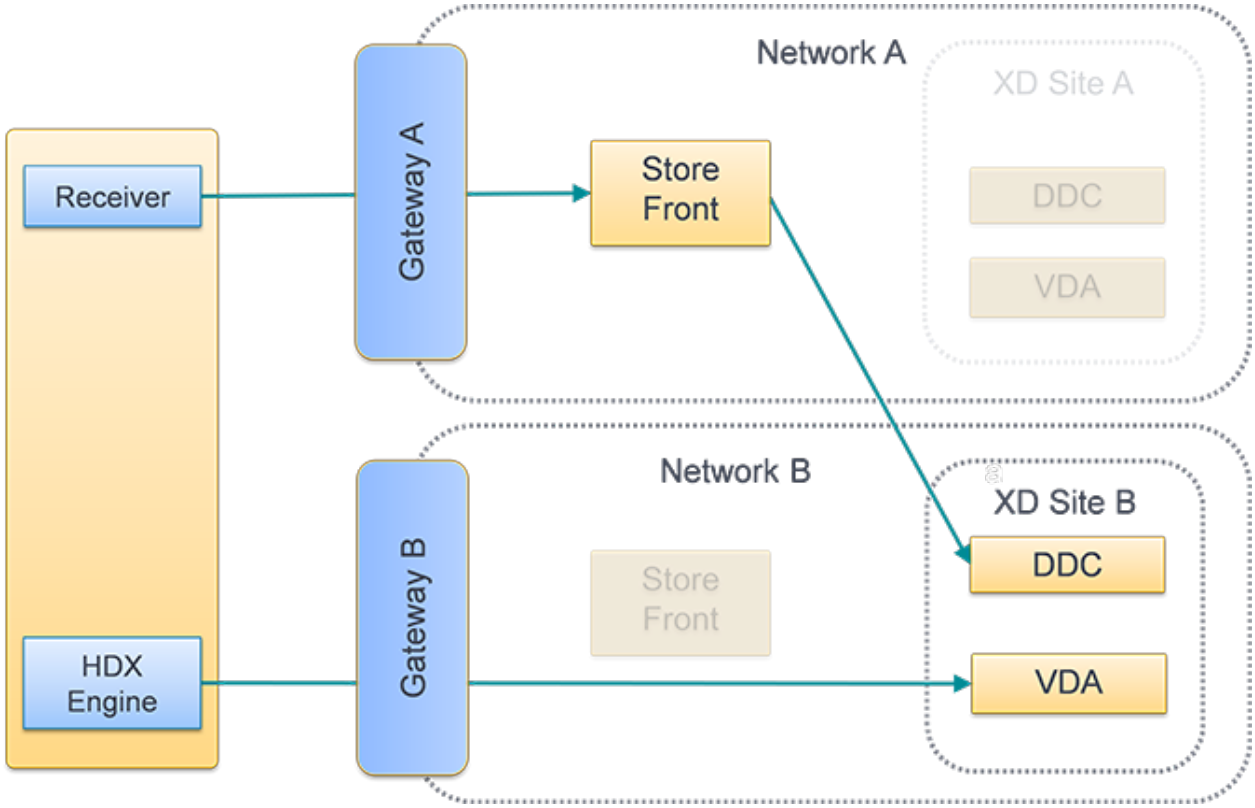


Figure 2. Optimal gateway routing

Configuration

Configuring the NetScaler Gateway routing behavior is straight-forward. There is no special configuration needed on the NetScaler; however, you must have NetScaler 11.0 build 66.11 or later installed on all of your NetScaler Gateway devices.

The configuration items necessary to enable NetScaler Gateway Routing are completed on the Citrix StoreFront servers. Note that you must have StoreFront version 3.x or later installed on all of your StoreFront servers, and that you must complete the configuration change on all of your StoreFront servers for NetScaler Gateway routing to work as expected.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

Use PowerShell to configure optimal gateway routing for a store

Configure optimal NetScaler Gateway routing to optimize the handling of ICA connection routing from the HDX engine to published resources such as XenDesktop VDAs or XenApp or XenDesktop published applications using StoreFront. Typically, the optimal gateway for a site is collocated in the same geographical location as apps and desktops.

You need only define optimal NetScaler Gateway appliances for deployments where the appliance through which users access StoreFront is not the optimal gateway. If launches should be directed back through the gateway making the launch request, StoreFront does this automatically.

Example scenario

1 x UK Gateway >> 1 x UK StoreFront	>> UK Apps and Desktops local >> US Apps and Desktops used only for UK failover
1 x US Gateway >> 1 x UK StoreFront	>> US Apps and Desktops local >> UK Apps and Desktops used only for US failover

A UK gateway provides remote access to UK hosted resources such as apps and desktops using a UK StoreFront.

The UK StoreFront has both a UK based and US based NetScaler Gateway defined and UK and US farms in its delivery controller list. UK users access remote resources through their geographically collocated gateway, StoreFront, and farms. If their UK resources become unavailable, they can connect to US resources as a temporary failover alternative.

Without optimal gateway routing all ICA launches would pass through the UK gateway that made the launch request regardless of where the resources are geographically located. By default, gateways used to make launch requests are identified dynamically by StoreFront when the request is made. Optimal gateway routing overrides this and forces US connections through the gateway closest to the US farms that provides apps and desktops.

Note: You can map only a single optimal gateway per site for each StoreFront store.

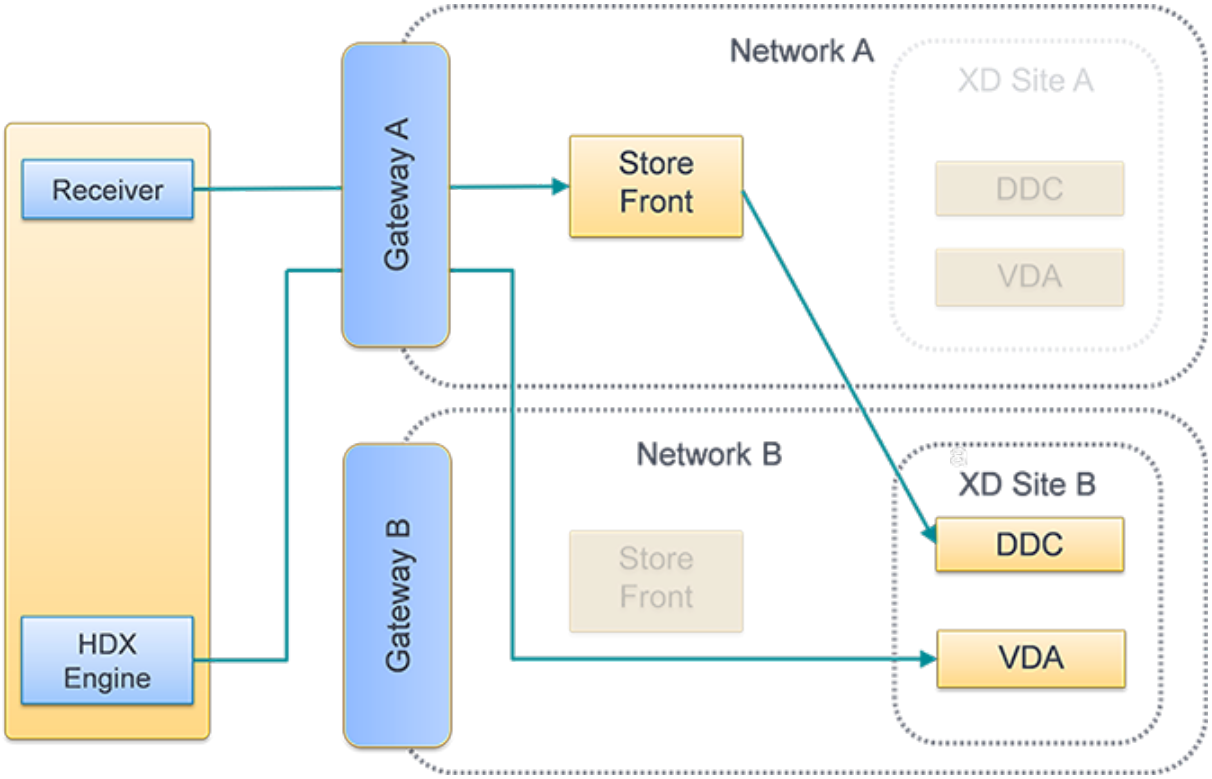


Figure 1. Suboptimal gateway routing

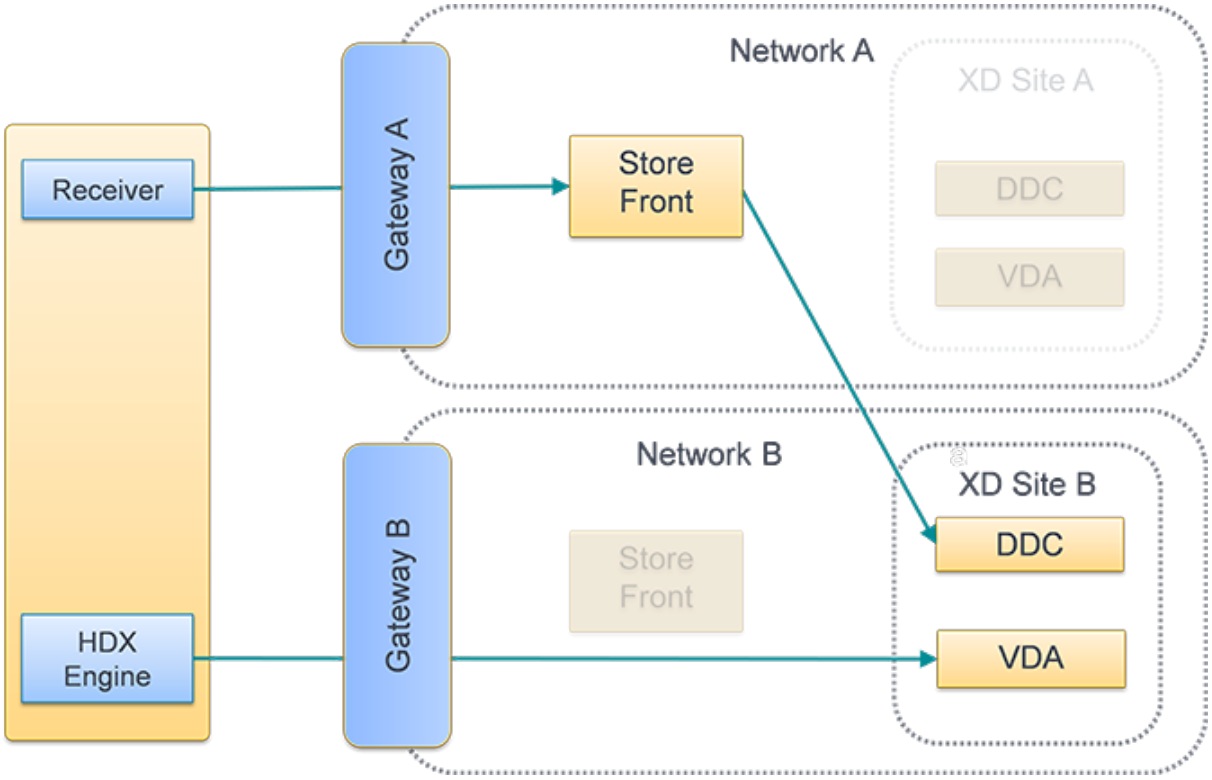


Figure 2. Optimal gateway routing

PowerShell API parameters

Parameter	Description
-SiteId (Int)	Site ID within IIS. This is typically 1 for the site in IIS where StoreFront is installed by default.
-ResourcesVirtualPath (String)	Path to the store that is to be configured to have a farm to optimal gateway mapping. Example: "/Citrix/Store"

-GatewayName (String)	Name given to identify the Netscaler Gateway within StoreFront. Example 1: ExternalGateway Example 2: InternalGateway
-Hostnames (String Array)	Specifies the fully qualified domain name (FQDN) and port of the optimal NetScaler Gateway appliance. Example1 for standard vServer port 443: gateway.example.com Example2 for nonstandard vServer port 500: gateway.example.com:500
-Farms (String Array)	Specifies a set of (typically collocated) XenDesktop, XenApp, and VDI-in-a-Box deployments that share a common optimal NetScaler Gateway appliance. A farm can contain just a single delivery controller or multiple delivery controller that provides published resources. You can configure a XenDesktop site in StoreFront under delivery controllers as “XenDesktop”. This represents a single farm. This could contain multiple delivery controllers in its failover list: Example: “XenDesktop" XenDesktop-A.example.com XenDesktop-B.example.com XenDesktop-C.example.com
-staUrls (String Array)	Specifies the URLs for XenDesktop, XenApp, and VDI-in-a-Box servers running the Secure Ticket Authority (STA). If using multiple farms, list the STA servers on each using a comma

	separated list: Example: "http://xenapp-a.ptd.com/scripts/ctxsta.dll","http://xendesktop-a.ptd.com/scripts/ctxsta.dll"
-StasUseLoadBalancing (Boolean)	Set to true: randomly obtains session tickets from all STAs, evenly distributing requests across all the STAs. Set to false: users are connected to the first available STA in the order in which they are listed in the configuration, minimizing the number of STAs in use at any given time.
-StasBypassDuration	Set the time period, in hours, minutes, and seconds, for which an STA is considered unavailable after a failed request. Example: 00.02:00:00
-EnableSessionReliability (Boolean)	Set to true: keeps disconnected sessions open while Receiver attempts to reconnect automatically. If you configured multiple STAs and want to ensure that session reliability is always available, set the value of the useTwoTickets attribute to true to obtain session tickets from two different STAs in case one STA becomes unavailable during the session.
-UseTwoTickets (Boolean)	Set to true: obtains session tickets from two different STAs in case one STA becomes unavailable during the session. Set to false: uses only a single STA server.
-EnabledOnDirectAccess (Boolean)	Set to true: ensures that when local users on the internal network log on to StoreFront directly, connections to their resources are still routed through the optimal appliance defined for the farm. Set to false: connections to resources are not routed through the optimal appliance for the farm unless users access

	StoreFront through a NetScaler Gateway.

Note: When PowerShell scripts span multiple lines such as shown below, each line must end with the backtick control character (').

Copy the following code examples into the Windows PowerShell Integrated Scripting Environment (ISE) to validate the code using the dynamic compiler before you run it.

Configure an optimal gateway for a farm.

Example: Create or overwrite OptimalGatewayForFarms mappings for the store Internal.

```
& "$Env:PROGRAMFILES\Citrix\Receiver
StoreFront\Scripts\ImportModules.ps1"
Set-DSOptimalGatewayForFarms -SiteId 1 `
                        -ResourcesVirtualPath /Citrix/Internal  `
                        -GatewayName "gateway1"  `
                        -Hostnames "gateway1.example.com:500" `
                        -Farms "XenApp","XenDesktop" `
                        -StaUrls
"https://xenapp.example.com/scripts/ctxsta.dll","https://xendesktop.
example.com/scripts/ctxsta.dll"  `
                        -StasUseLoadBalancing:$false `
                        -StasBypassDuration 00.02:00:00 `
                        -EnableSessionReliability:$false `
                        -UseTwoTickets:$false `
                        -EnabledOnDirectAccess:$true
```

Example: This script returns configured OptimalGatewayForFarms for the store called Internal.

```
Get-DSOptimalGatewayForFarms -SiteId 1 –ResourcesVirtualPath
“/Citrix/Internal”
```

Example: Remove all optimal gateway for farms mappings for store called Internal.

```
Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath
“/Citrix/Internal”
```

Configure a NULL gateway for a farm.

Example: This script prevents all ICA launches from passing through a gateway for the list of specified farms for the store called Internal.

```
Set-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath
/Citrix/Store -Farms "Farm1","Farm2"
```

Example: This script returns all farms that are configured to prevent ICA launches from passing through a gateway for a store called Internal.

```
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath
“/Citrix/Internal”
```

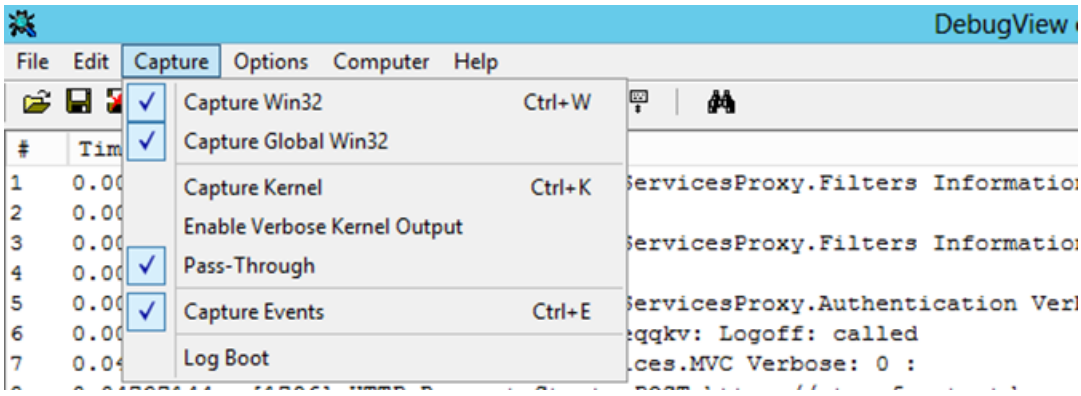
Determine if your OptimalGatewayForFarms mappings are being used by StoreFront

1. Enable StoreFront tracing on all server group nodes using PowerShell by running:

```
& "$Env:PROGRAMFILES\Citrix\Receiver
StoreFront\Scripts\ImportModules.ps1"

#Traces output is to c:\Program Files\Citrix\Receiver
Storefront\admin\trace\
Set-DSTraceLevel -All -TraceLevel Verbose
```

2. Open the Debug View tool on the desktop of a StoreFront server. If you are using a StoreFront server group, you might have to do this on all nodes to ensure you obtain traces from the node that receives the launch request.



3. Enable Capture Global Win32 events.

4. Save the trace output as a .log file and open the file with Notepad. Search for the log entries shown in the example scenarios below.

5. Turn tracing off afterwards, as it consumes a lot of disk space on your StoreFront servers.

```
Set-DSTraceLevel -All -TraceLevel Off
```

Tested optimal gateway scenarios

- External client logs on **Gateway1**. Launch is directed through the designated optimal gateway **Gateway2** for the farm **Farm2**.

```
Set-DSOptimalGatewayForFarms -onDirectAccess=false
```

Farm2 is configured to use the optimal gateway **Gateway2**.

Farm2 has optimal gateway on direct access disabled.

The optimal gateway **Gateway2** will be used for the launch.

- Internal client logs on using StoreFront. Launch is directed through the designated optimal gateway **Gateway1** for the farm **Farm1**.

```
Set-DSOptimalGatewayForFarms -onDirectAccess=true
```

No dynamically identified gateway in request. StoreFront was contacted directly.

Farm1 is configured to use the optimal gateway **Gateway1**.

Farm1 has optimal gateway on direct access enabled.

The optimal gateway **Gateway1** will be used for the launch.

- Internal client logs on using **Gateway1**. Launches of resources on Farm1 are prevented from passing through any gateway and StoreFront is contacted directly.

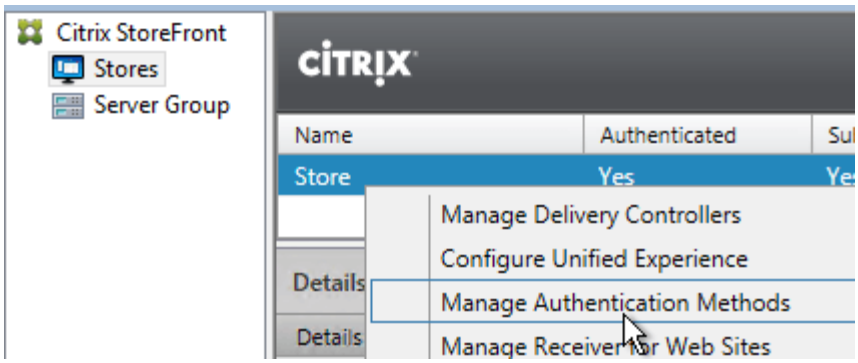
```
Set-DSFarmsWithNullOptimalGateway
```

Dynamically identified gateway in request: **Gateway1**

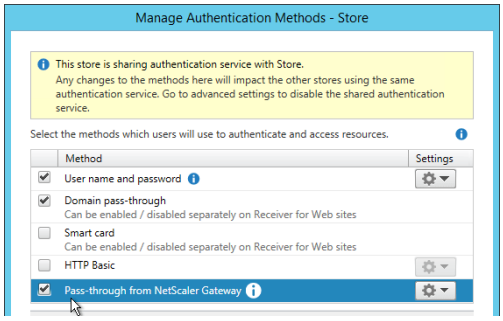
Farm1 is configured to not use a gateway. No gateway will be used for launch.

Use Storefront GUI to configure optimal gateway routing for a store

1. See the NetScaler documentation for instructions on configuring NetScaler Gateway for StoreFront.
2. In the StoreFront Console, right-click the Store and click **Manage Authentication Methods**.



3. Ensure Pass-through from NetScaler Gateway is selected and click **OK**.



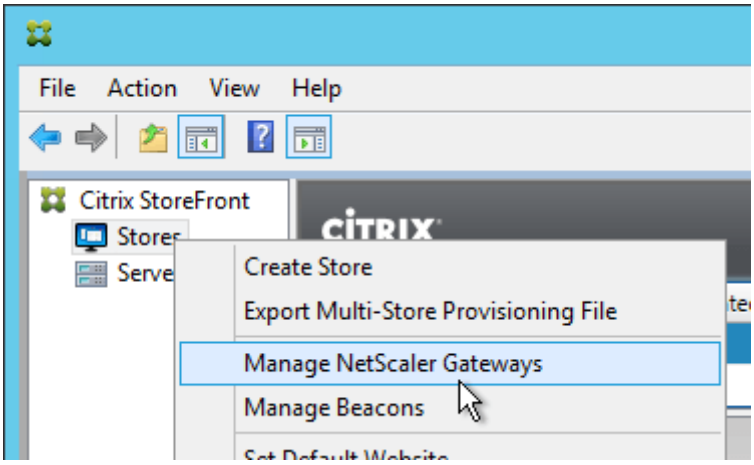
4. If you need the SmartAccess feature, then you need to configure StoreFront to perform an authentication callback to a NetScaler Gateway Virtual Server on the same appliance that authenticated the user.

   - If you need SmartAccess and have a Single FQDN then the Callback FQDN must be different than the Single FQDN.
   - If you need SmartAccess and are doing different FQDNs for Gateway and StoreFront, then the Callback FQDN is usually the same as the Gateway FQDN.
   - Make sure the StoreFront server can resolve the Callback FQDN to a Gateway VIP (with matching certificate). One option is to edit the C:\Windows\System32\drivers\etc\hosts file and add an entry for the Callback FQDN.

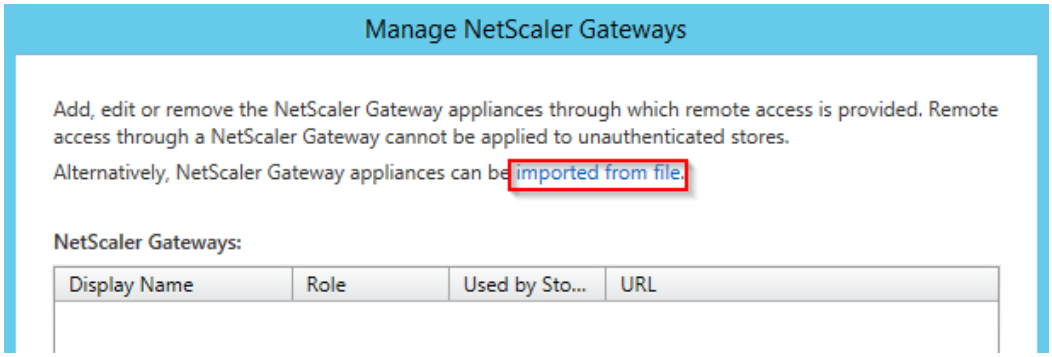
```
18
19  # localhost name resolution is handled within DNS itself.
20  #   127.0.0.1       localhost
21  #   ::1             localhost
22  10.2.2.200  callback.corp.com
```

   - After configuring the HOSTS file, on the StoreFront server, open a browser and navigate to the DNS name. Make sure the Gateway vServer logon page appears.

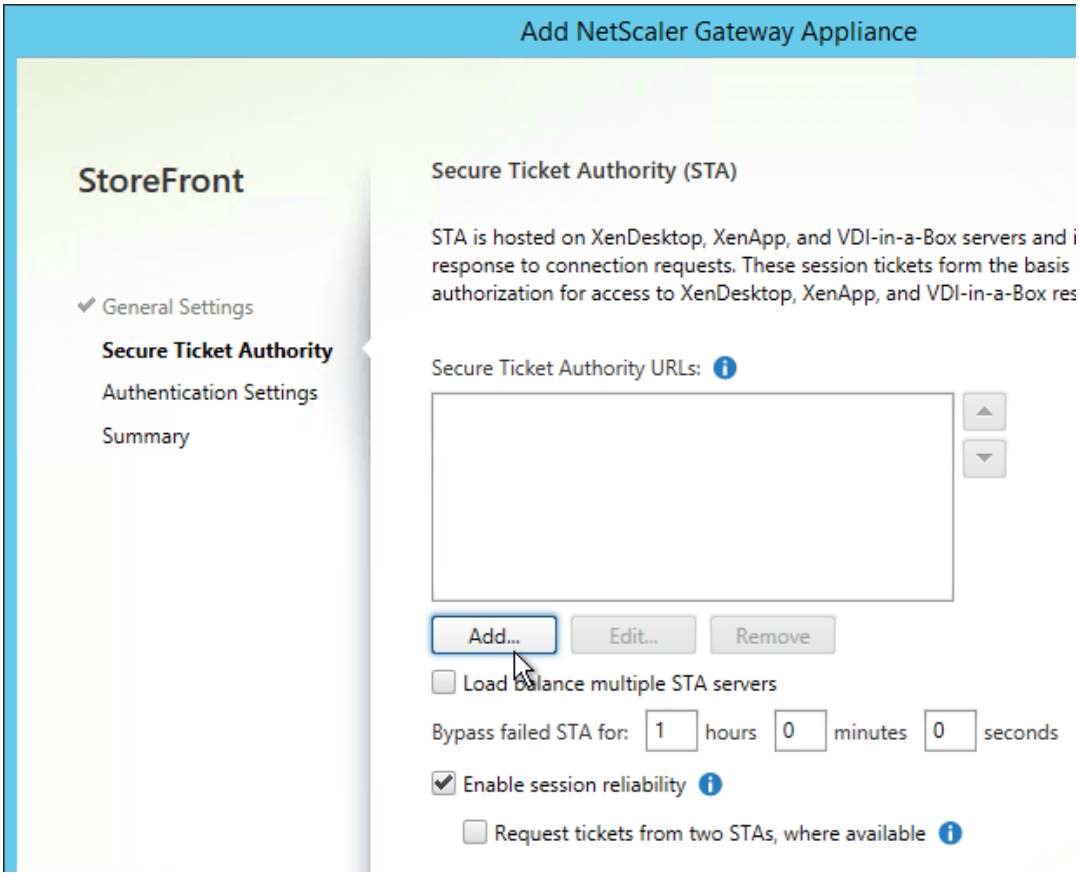
5. In the StoreFront Console, right-click **Stores** and click **Manage NetScaler Gateways**.



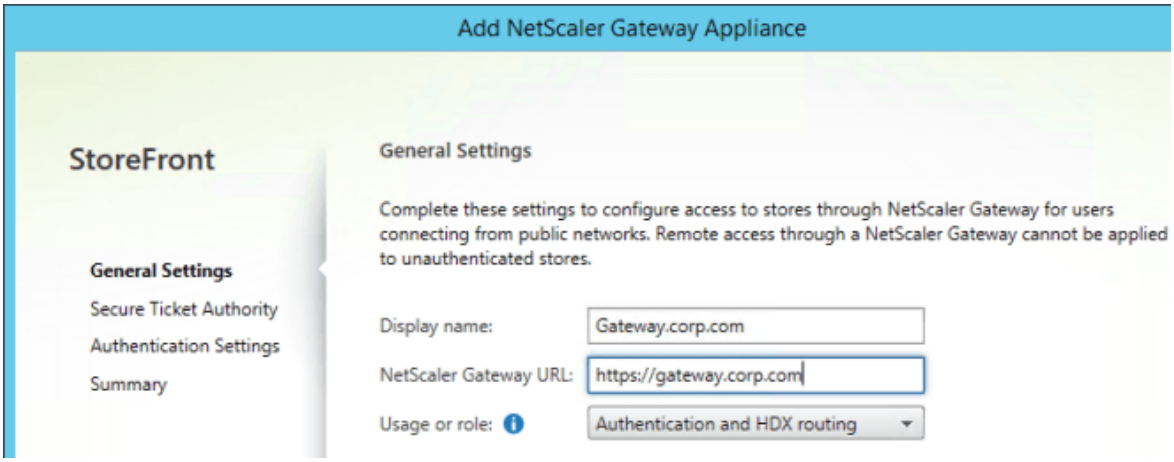
6. If StoreFront 3.6 or newer, notice the imported from file link on top. This is a new feature of NetScaler 11.1.



7. If you are not using the config file from NetScaler 11.1 and newer, click **Add**.



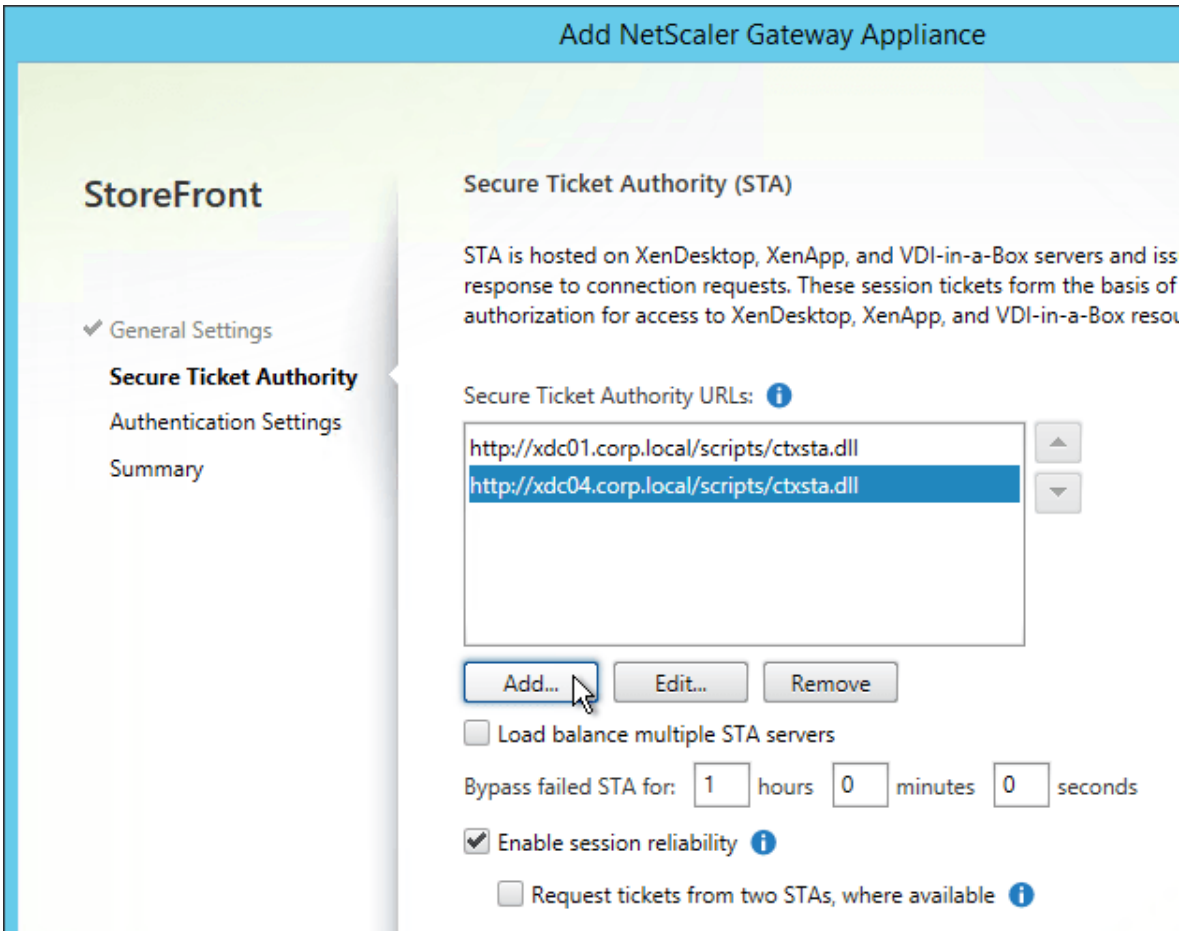
8. In the **General Settings** page, enter a display name. This name appears in Citrix Receiver so make it descriptive.
9. Enter the NetScaler Gateway Public URL. This can be a GSLB-enabled DNS name. Click **Next**.



10. In the Secure Ticket Authority page, click **Add**.

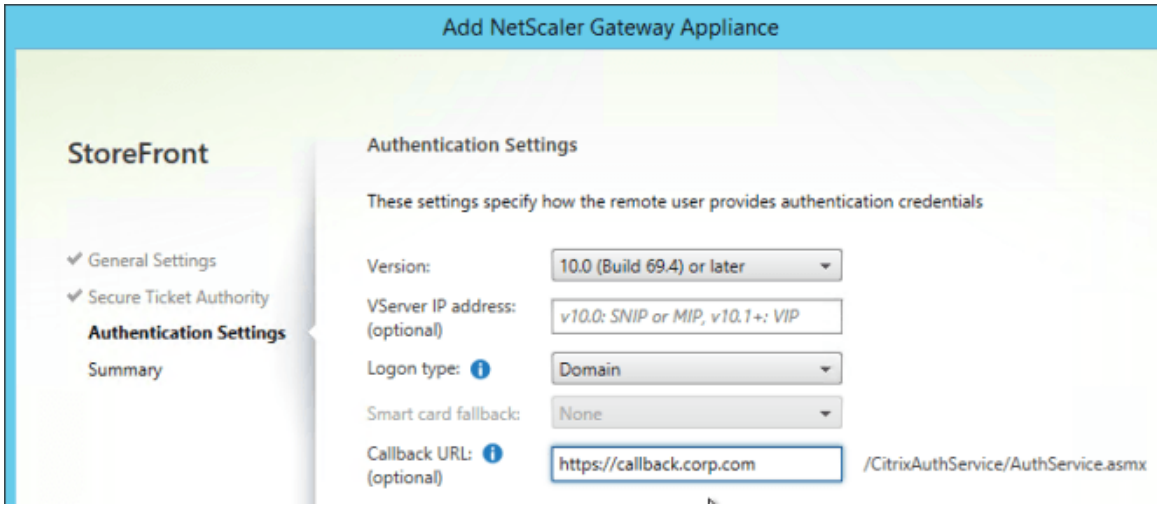
11. Enter the URL to a XenDesktop Controller. This can be http or https.

12. Continue adding Secure Ticket Authorities (XenDesktop Controllers). Whatever Secure Ticket Authorities you add here must also be configured on the NetScaler Gateway Virtual Server on the NetScaler Gateway appliance. Click **Next**.

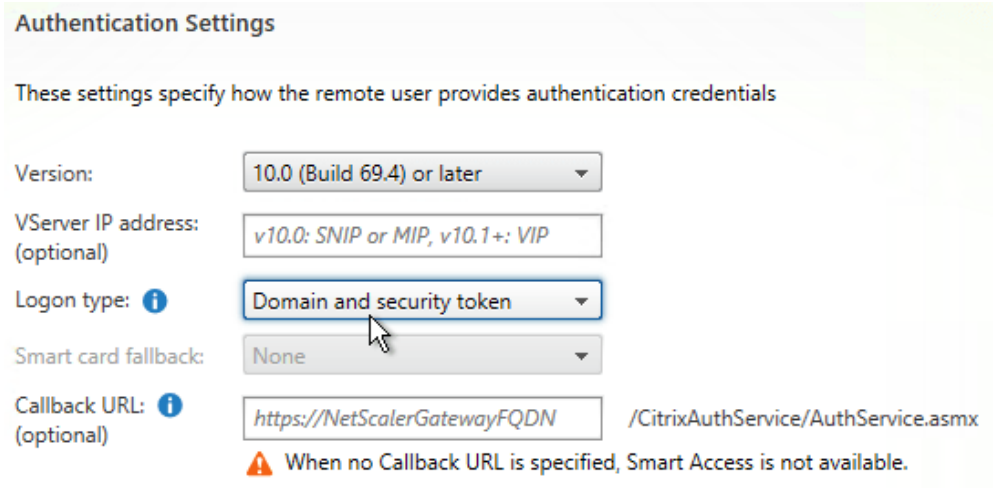


13. In the **Authentication Settings** page, if you have multiple Gateways (on separate appliance pairs) connecting to one StoreFront server then then you'll need to enter the vServer IP address (VIP) of the NetScaler Gateway Virtual Server so StoreFront can differentiate one NetScaler Gateway from another. If there's only one Gateway communicating with this StoreFront server group, then leave the **VServer IP address** field empty.
14. If you need SmartAccess, then enter the Callback URL.
    - The Callback URL must resolve to any NetScaler Gateway VIP on the same appliance that authenticated the user. For multi-datacenter, edit the HOSTS file on the StoreFront server so it resolves to NetScaler appliances in the same datacenter.
    - The Callback URL Gateway Virtual Server must have a trusted and valid (matches the FQDN) certificate.
    - The Callback URL Gateway Virtual Server must not have client certificates set to Mandatory.

15. If you don't need SmartAccess then leave the **Callback URL** field empty.

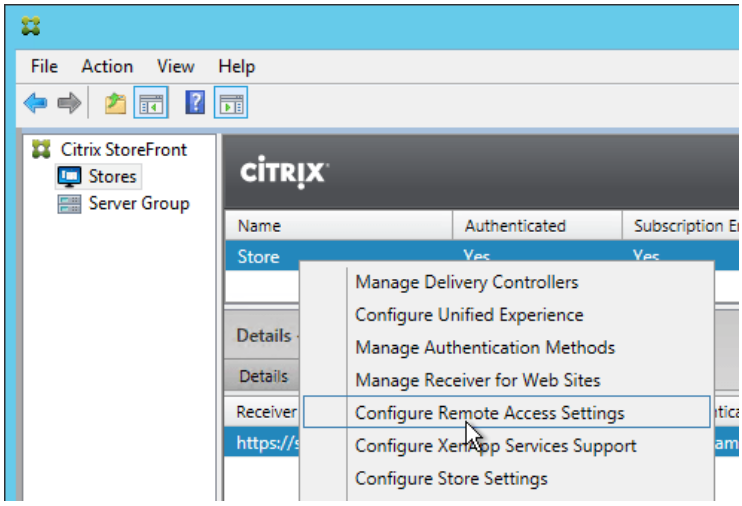


16. If you enabled two-factor authentication on your NetScaler (e.g. LDAP and RADIUS), change the **Logon type** to **Domain and security token**. Otherwise leave it set to **Domain** only.

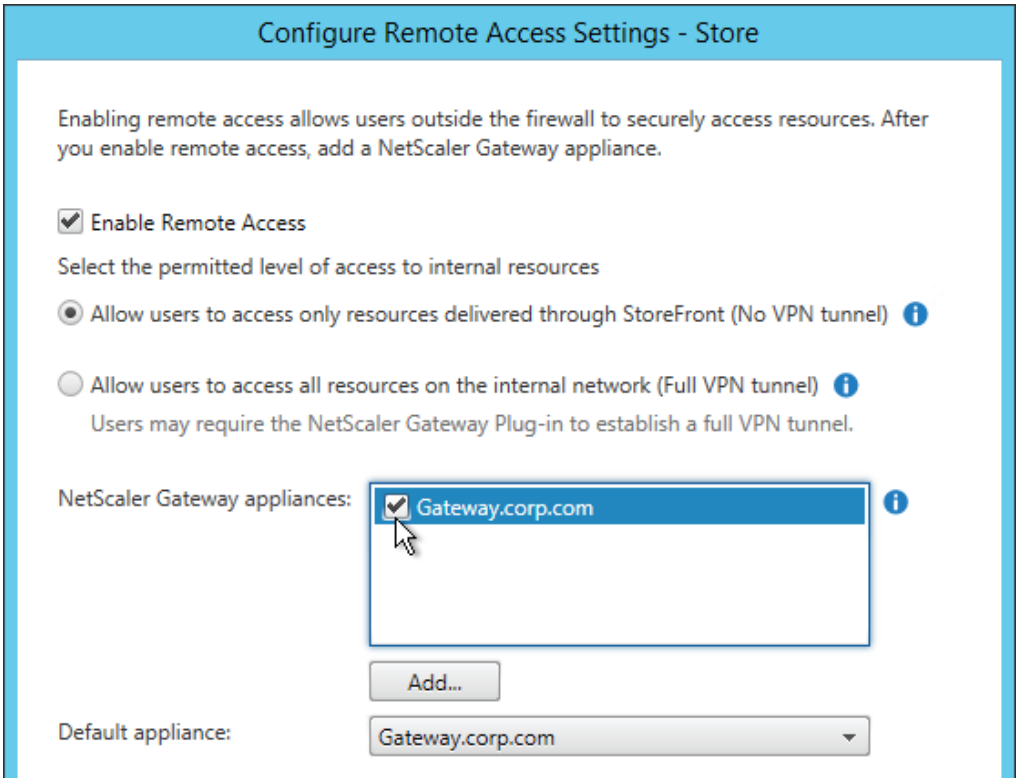


17. Click **Create**.
18. Then click **Finish**.

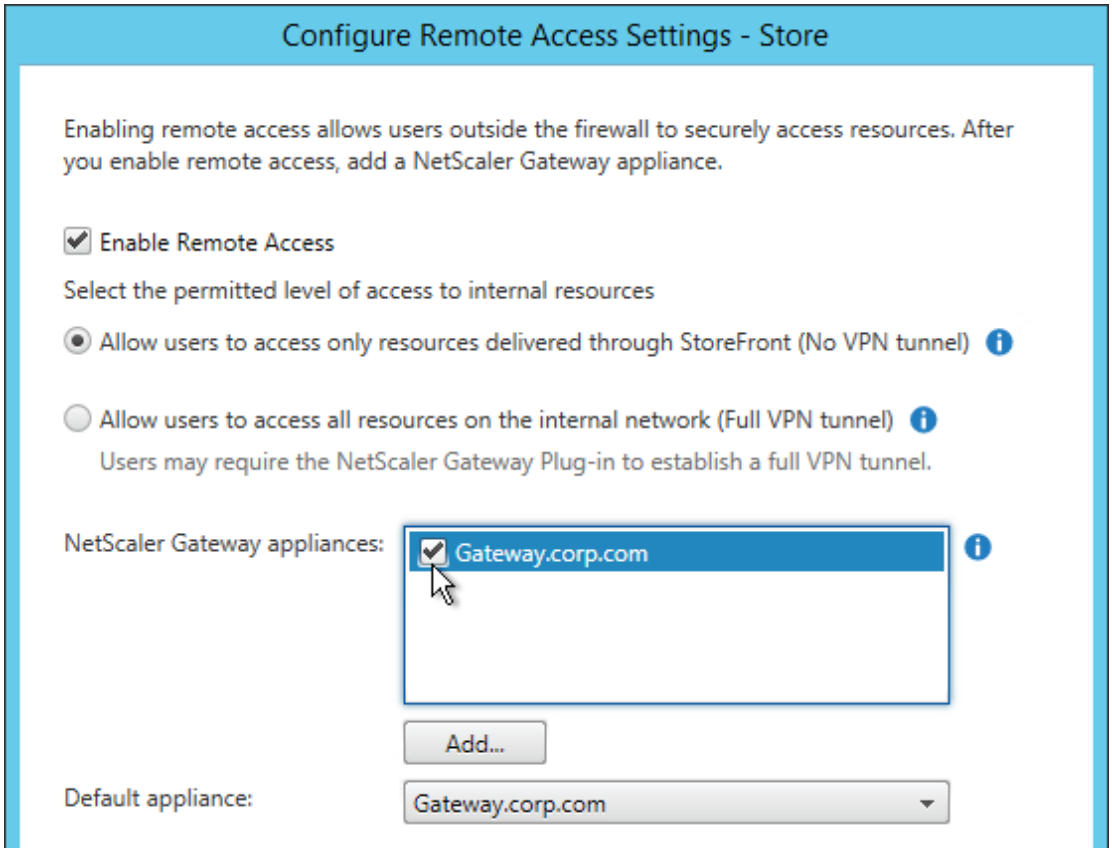
19. Right-click a store and click **Configure Remote Access Settings**.



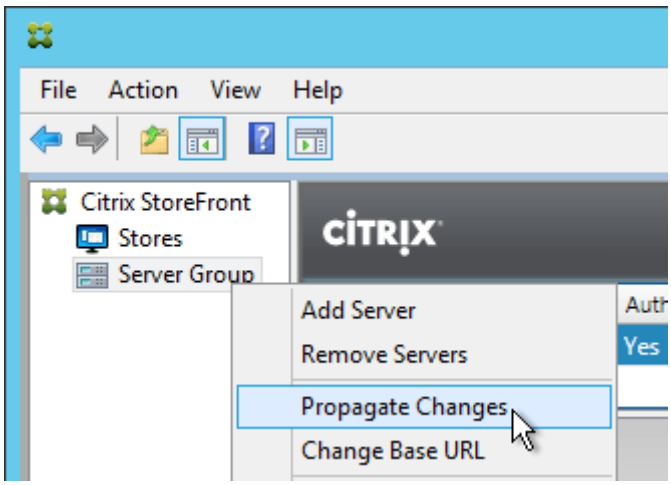
20. Check the box next to Enable Remote Access.
21. Leave it set to No VPN tunnel.
    - Note: if you want Receiver to launch a VPN tunnel automatically, then see CTX200664 How to Configure Receiver for Seamless Experience Through NetScaler Gateway.



22. Check the box next to the NetScaler Gateway object you just created and then click **OK**.
    - Then in the StoreFront console, right-click **Server Group** and click **Propagate Changes**.



23. Then in the StoreFront console, right-click **Server Group** and click **Propagate Changes**.



Summary

Citrix ensures that you are able to deliver the best app and desktop user experience with XenApp and XenDesktop. Simplifying the user experience with GSLB makes it easy for users to access apps, desktops and data. However, GSLB can sometimes lead to a suboptimal user experience.

Optimal Gateway Routing via NetScaler and Storefront is a good technique for ensuring that the user experience is both simple and consistent by de-coupling the authentication gateway from the optimal launch gateway.

This ensures that you users always launch their apps and desktops from the local gateway, thus ensuring a better user experience when working from anywhere, on any device.