

# How to Configure NetScaler Gateway 10.5 to use with StoreFront 2.6 and XenDesktop 7.6.

## Introduction

The purpose of this document is to record the steps required to configure a NetScaler Gateway for use with StoreFront and XenDesktop.

Particular attention has been paid to the use of on-board NetScaler tools for creating a server certificate for the NetScaler Gateway. It will be seen that the NetScaler is using an exported root CA from a Microsoft Certificate Server so that client systems only need a single CA certificate.

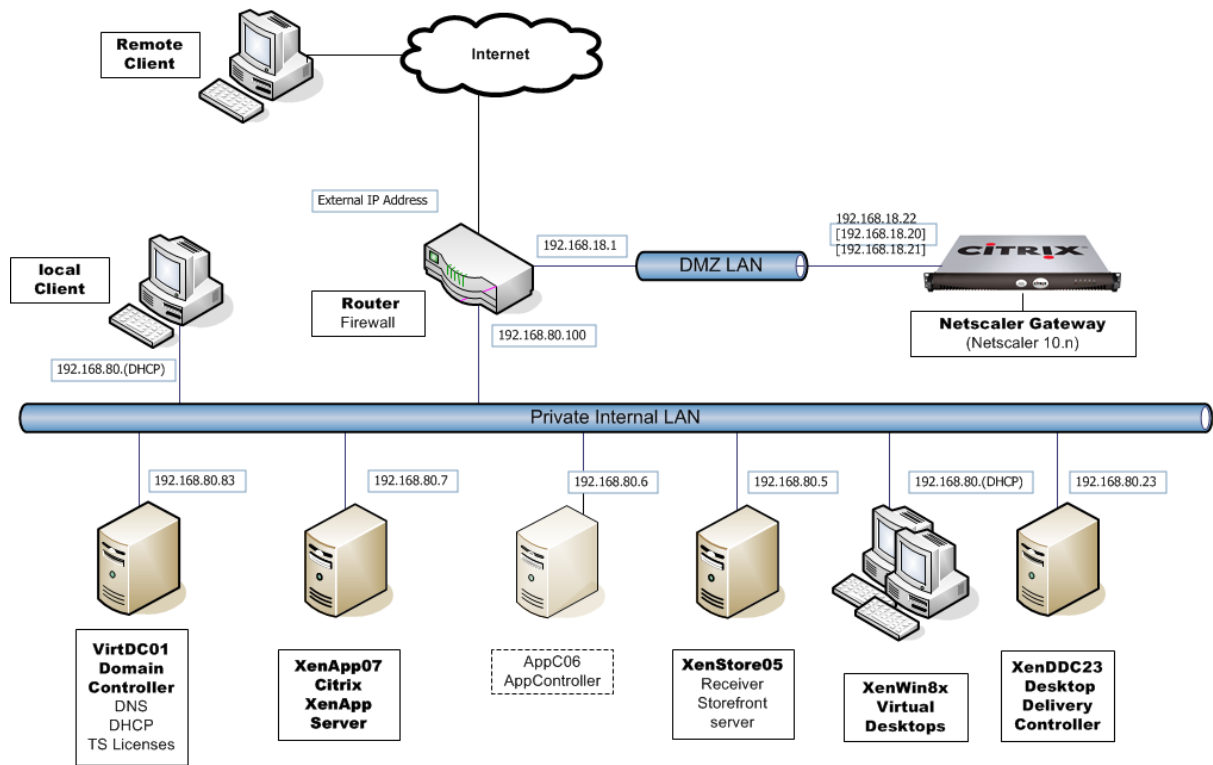
The target audience for this document includes developers and testers who wish to set up a representative environment for testing external access scenarios.

While this document only attempts to record a single configuration, it is hoped that it will act as a stepping stone for those who wish to create similar or more advanced configurations.

## Contents

Introduction .....	1
Network Diagram.....	2
NetScaler Configuration .....	3
Initial setup from XenCenter Console.....	3
Continue setup from NetScaler GUI.....	4
Server Certificates, CA Certificates, and SSL.....	8
On the Microsoft Certificate Server .....	8
On the NetScaler GUI.....	10
NTP Server .....	17
Backups - and why you might want one.....	18
Create a NetScaler Gateway Virtual Server.....	20
StoreFront .....	30
DNS.....	30
StoreFront – Configuring a new installation.....	30
Test the deployment from a Windows PC connected to the Internet.....	37
On the Windows PC.....	37

# Network Diagram



The NetScaler will use the following network addresses

NetScaler IP	192.168.18.20
Subnet IP	192.168.18.21
Virtual IP	192.168.18.22

## NetScaler Configuration

This section assumes that you will be creating a NetScaler VPX virtual appliance and hosting it on XenServer.

The processes for configuring a physical NetScaler appliance, or a NetScaler VPX virtual appliance hosted on another Hypervisor is similar.

### Initial setup from XenCenter Console

1. Download the latest NetScaler VPX virtual appliance from [www.citrix.com](http://www.citrix.com) and import it into XenServer.
2. Using XenCenter, start the new NetScaler VM and go to the VM console.

```
!There is no ns.conf in the /nsconfig!

Start Netscaler software
Input: no terminal type specified and no TERM environmental variable.
Enter NetScaler's IPv4 address []: 192.168.18.20
Enter Netmask []: 255.255.255.0
Enter Gateway IPv4 address []: 192.168.18.1

-----
Netscaler Virtual Appliance Initial Network Address Configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.

After the network changes are saved, you may either login as nsroot and
use the Netscaler command line interface, or use a web browser to
http://192.168.18.20 to complete or change the Netscaler configuration.
-----

1. NetScaler's IPv4 address [192.168.18.20]
2. Netmask [255.255.255.0]
3. Gateway IPv4 address [192.168.18.1]
4. Save and quit
Select item (1-4) [4]:
```

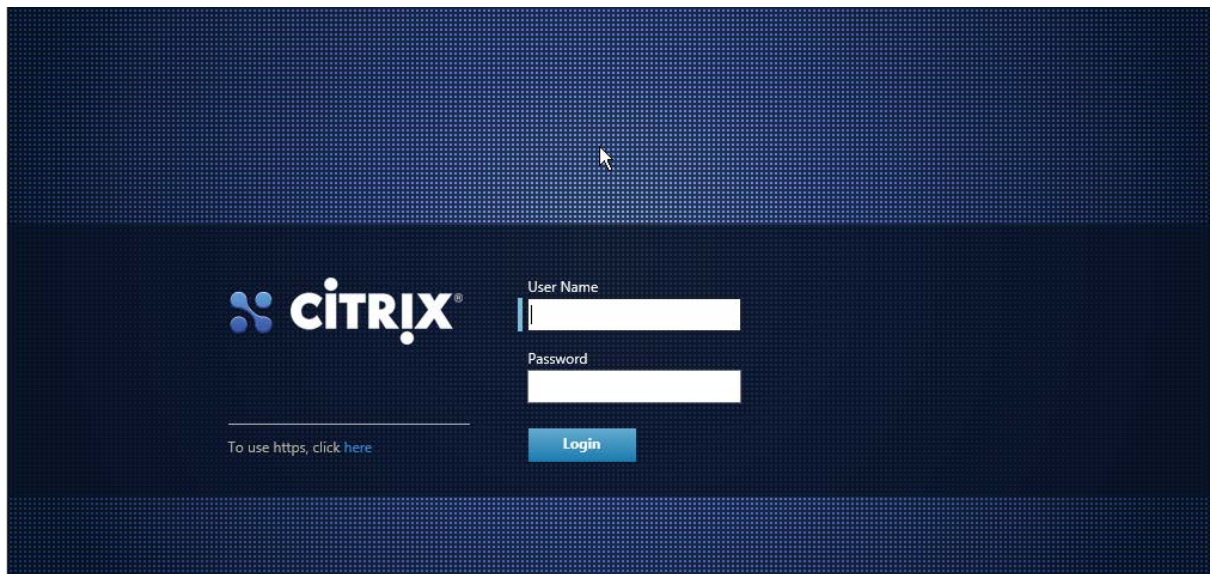
3. Enter the following information into the first time wizard.

IPv4 address	192.168.18.20
Netmask	255.255.255.0
Default Gateway	192.168.18.1

4. Select **4** to Save and quit.  
The NetScaler will reboot.

## Continue setup from NetScaler GUI









1. From a convenient PC, workstation, or server, launch a browser and point to <http://192.168.18.20>



2. Log on using the following credentials:  
Username nsroot  
Password nsroot

**Welcome!**

Use this wizard for initial configuration of your NetScaler virtual appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<b>NetScaler IP Address</b> IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. NetScaler IP Address: <b>192.168.18.20</b> Netmask: <b>255.255.255.0</b>	
	<b>Subnet IP Address</b> Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: <i>Not configured</i>	
	<b>Host Name, DNS IP Address, and Time Zone</b> Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Host Name: <i>Not configured</i> DNS IP Address: <i>Not configured</i> Time Zone: <b>CoordinatedUniversalTime</b>	
	<b>Licenses</b> Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. There are 0 license file(s) present on this NetScaler.	

The NetScaler “Welcome Wizard” now walks you through the configuration of the Subnet IP Address, Host Name, DNS details, Time Zone and Licenses.

Dashboard Configuration Reporting Documentation Downloads

### Subnet IP Address

A subnet IP address is used by the NetScaler to communicate with the backend servers. NetScaler uses this subnet IP address as a source IP address to proxy the client connections as well as to send monitor probes to check the health of the backend servers.

The infographic shows the usage of SNIP in client server communication.

Depending on your network topology, you might have to configure additional subnet IP addresses.

For more information about subnet IP addresses, [click here](#).

VIP = Virtual IP address  
SNIP = Subnet IP address

Subnet IP Address\*  
192 . 168 . 18 . 21

Netmask\*  
255 . 255 . 255 . 0

Done Do It Later

Dashboard Configuration Reporting Documentation Downloads

### Host Name, DNS IP Address, and Time Zone

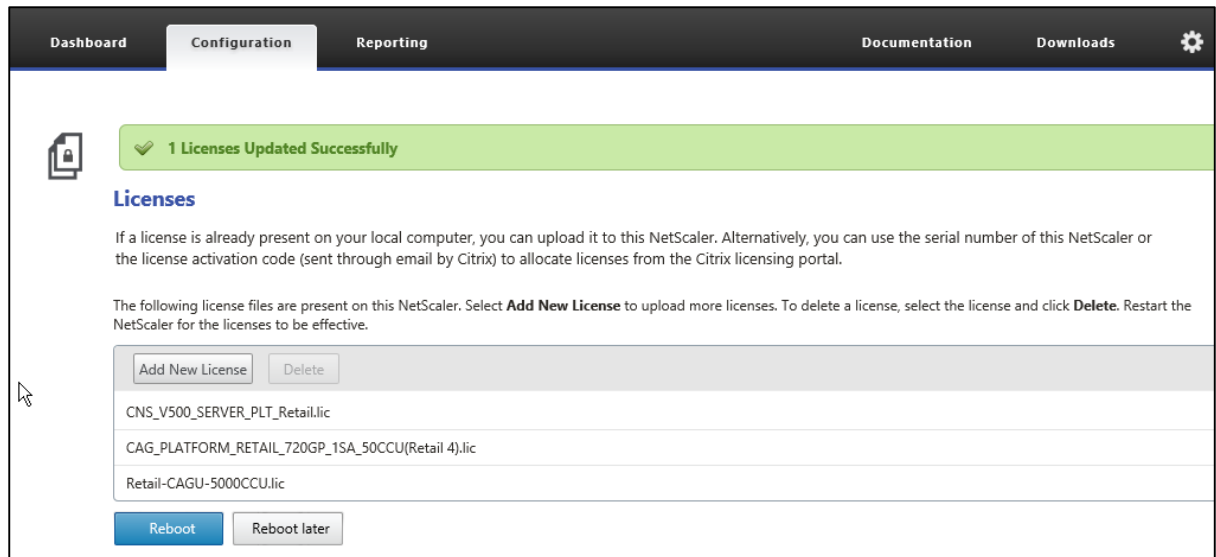
Specify a host name to identify your NetScaler. When you generate the Universal license for NetScaler Gateway, the host name is used in the license. Specify the IP address of a DNS server if you want to allocate your licenses from the Citrix licensing portal. Specify the time zone in which your NetScaler is located.

Host Name  
nstestgw

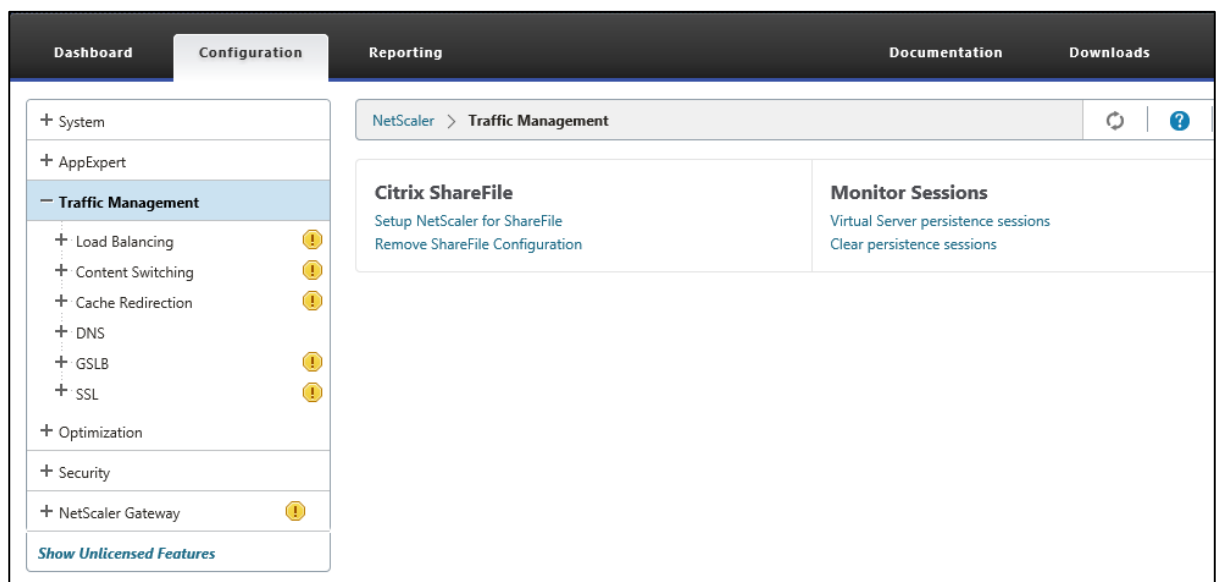
DNS IP Address  
192 . 168 . 80 . 1 +

Time Zone\*  
GMT+00:00-GMT-Europe/London

Done Do It Later



3. Add your licenses (the preceding are Citrix test licenses. Your experience will probably differ).
4. Click **Reboot**.



5. After logging back in to the GUI it can be seen that some features are disabled by default.
6. Enable NetScaler Gateway and SSL by selecting the feature, and using right-click and **Enable**.

NetScaler VPX (500) Info NS10.5 51.10.nc Logout

Dashboard Configuration Reporting Documentation Downloads

System

- Licenses
- Settings
- Diagnostics
- High Availability
- NTP Servers
- Reports
- Profiles
- User Administration
  - Groups
  - Users**
  - Database Users
  - Command Policies

NetScaler > System > User Administration > Users

Add Edit Delete Change Password Search

User Name	CLI Prompt	Prompt inherited from	Idle Session Timeout (secs)	Idle Session Timeout inherited from
nsroot	-	-	900	Global

7. You might need to change the nsroot password.

## Server Certificates, CA Certificates, and SSL

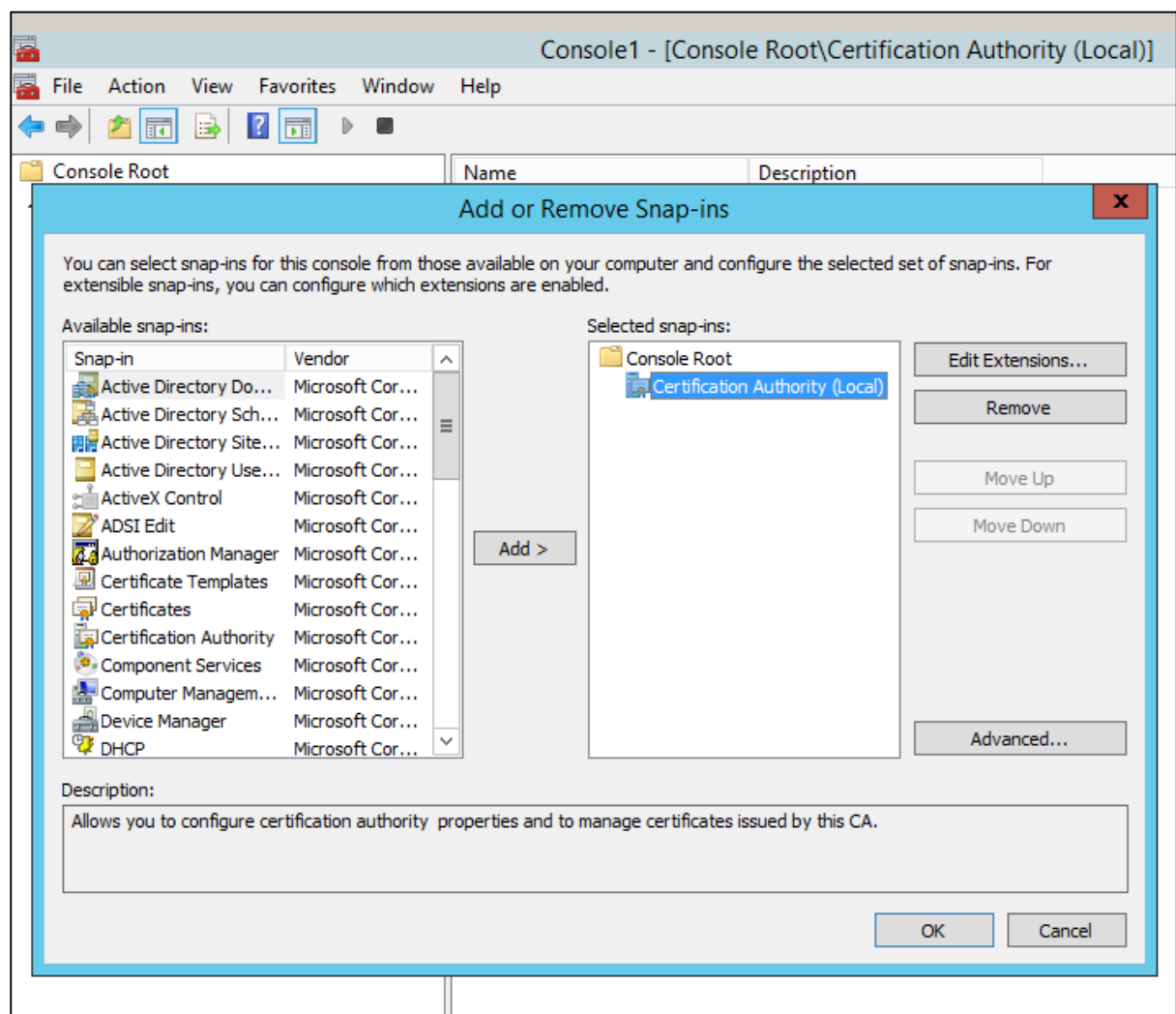
The System 3 test team try to build environments which reflect real world cases and generally server certificates are created for all servers, and use SSL to communicate whenever possible. To create these certificates, engineers use their Microsoft Certificate Server, rather than using public Certificate Authorities which would be expensive for multiple test environments. Because they do not use one of the well-known public Certificate Authorities, they have to ensure that they are installed on trusted CA certificate on all client devices.

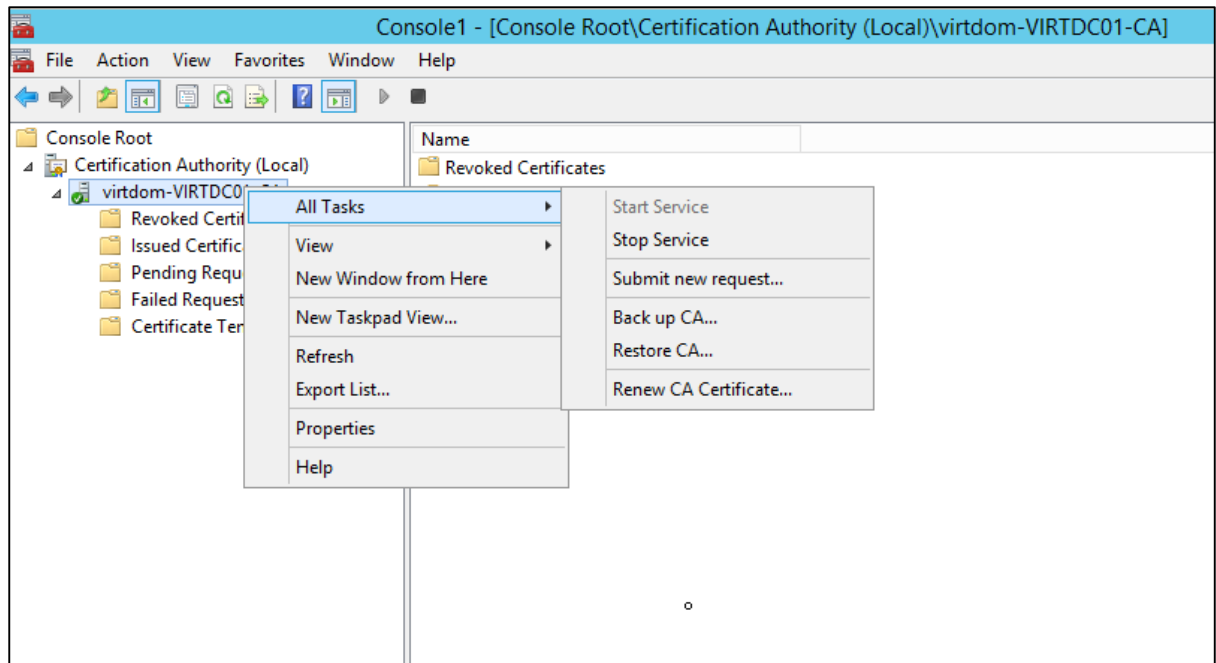
Because the Microsoft Certificate Server is known to Active Directory the trusted CA certificate is automatically installed on all domain-joined systems. The engineers then have to manually add the trusted CA certificate to non-domain-joined systems including domestic PCs, thin clients, tablets and smart phones.

This section describes how to create server certificates for NetScaler Gateways using the tools on the NetScaler appliance. It will be seen that the NetScaler is using an exported root CA from our Microsoft Certificate Server so that we do not have to distribute additional CA certificates to our client systems.

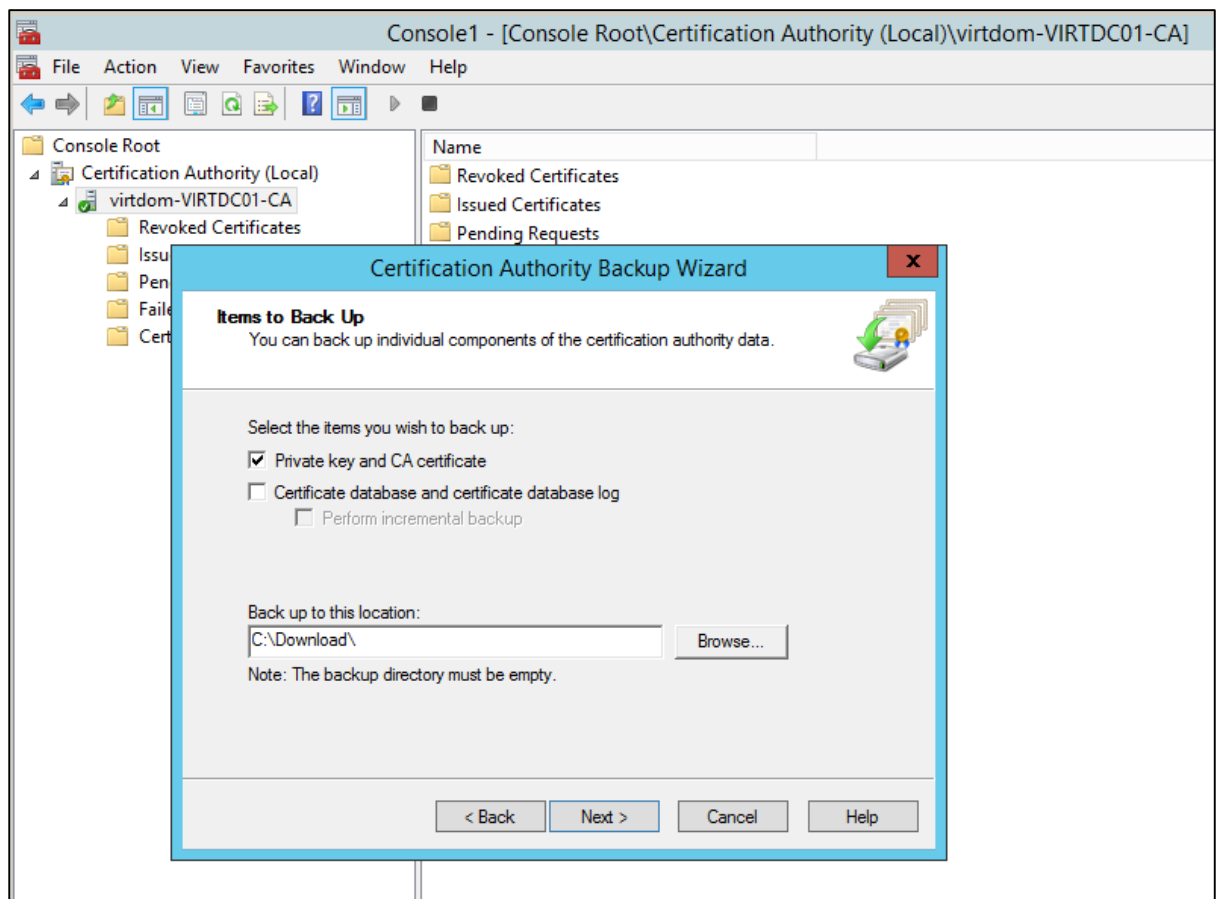
### On the Microsoft Certificate Server

1. Run **mmc** and load the Certification Authority Snap-in.

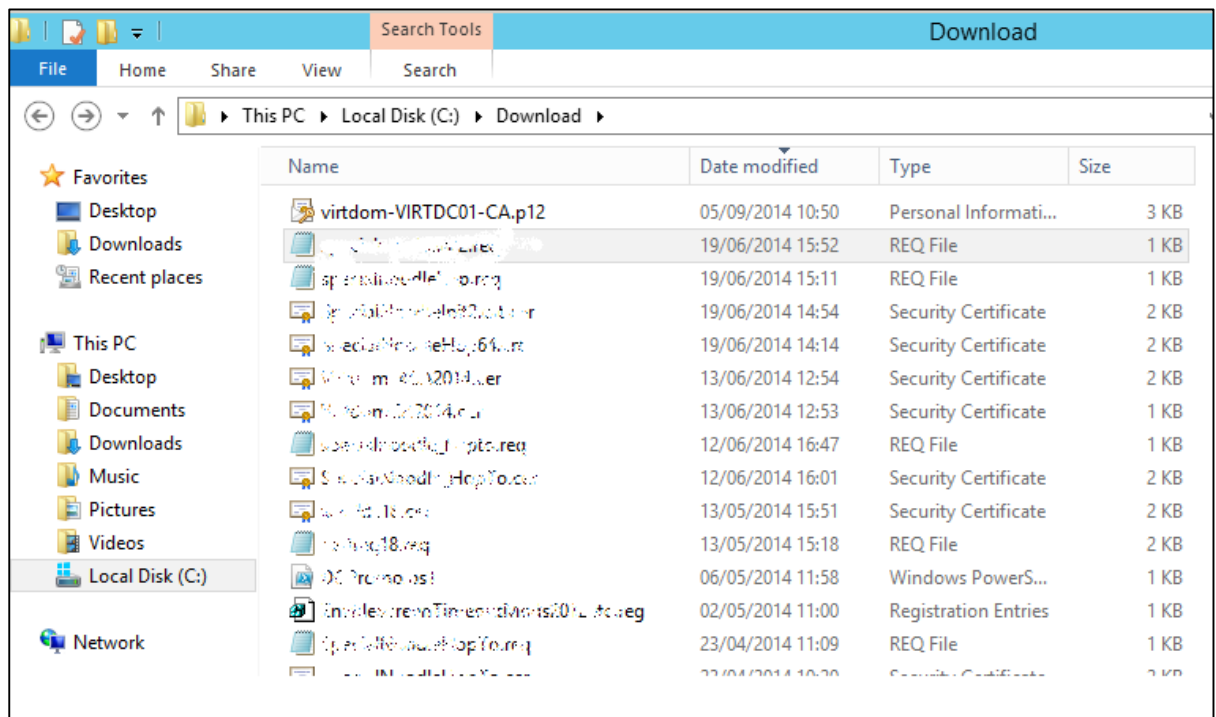
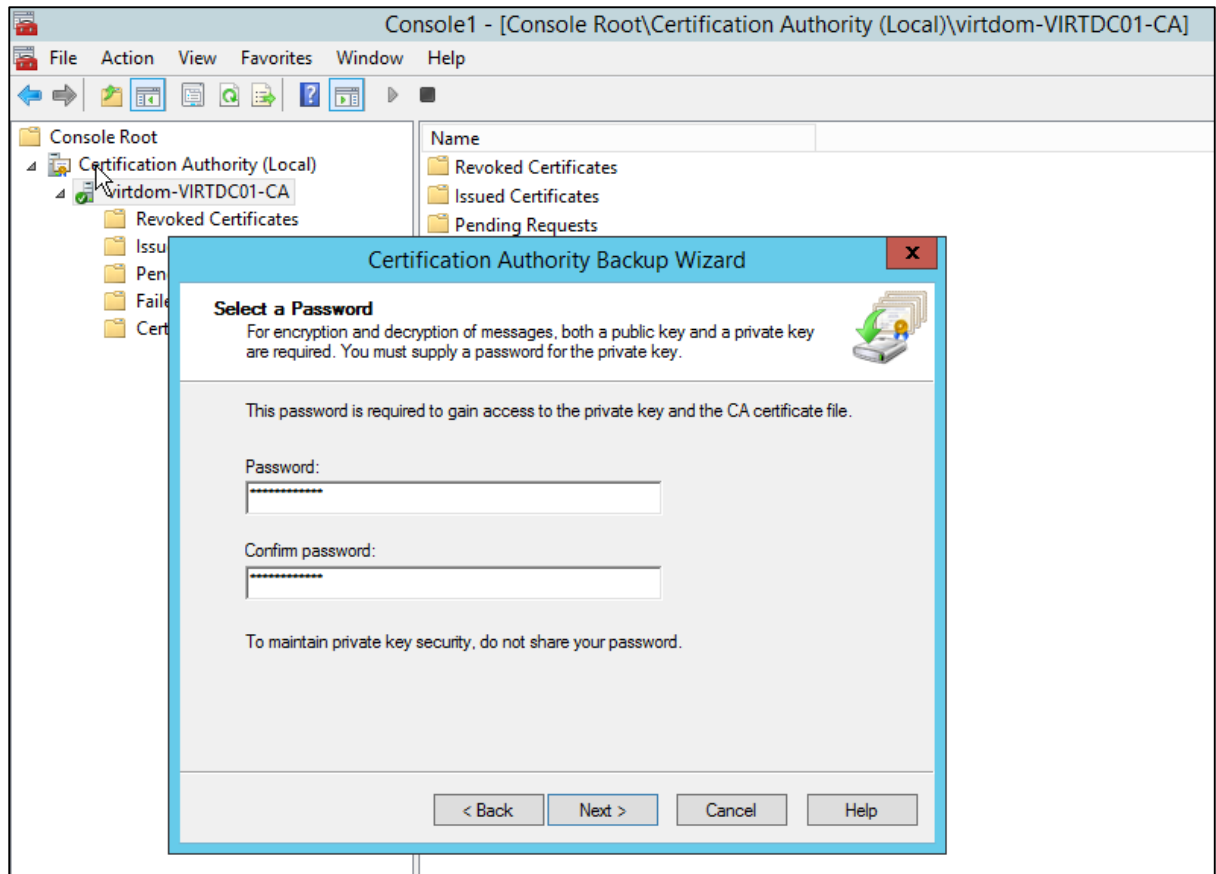




2. Right click the authority > **All Tasks** > **Back up CA**.



3. Back up the Private key and CA certificate to a convenient location.
4. Create a password.
5. Click **Next**.
6. Click **Finish**.

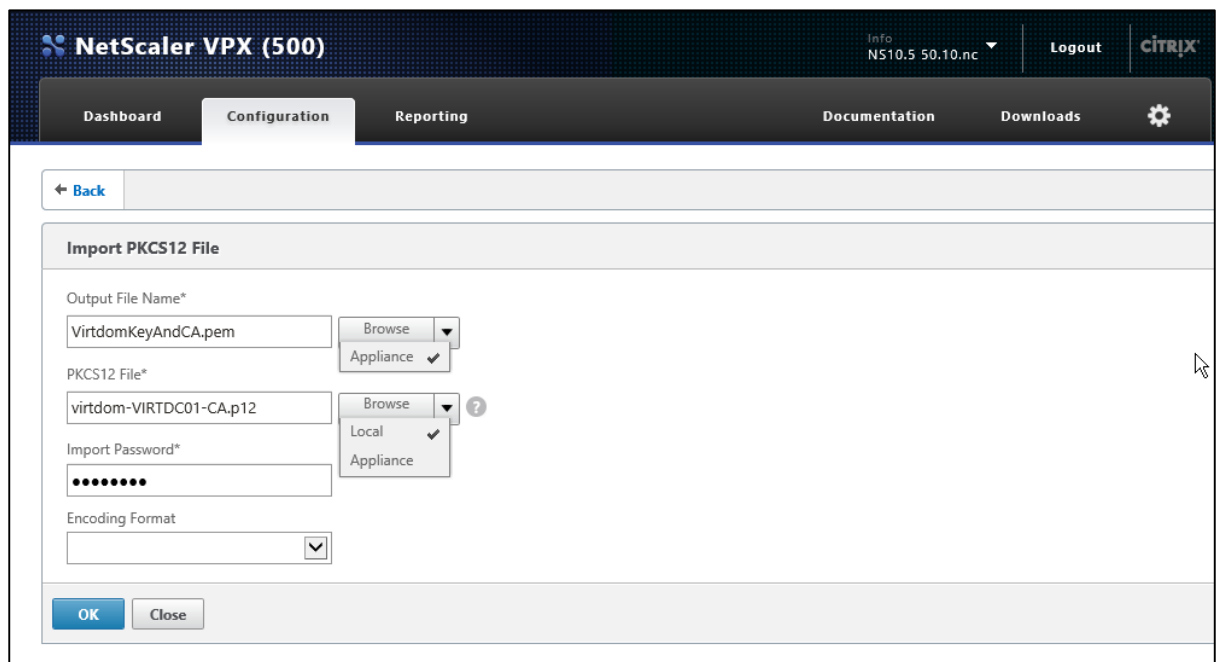
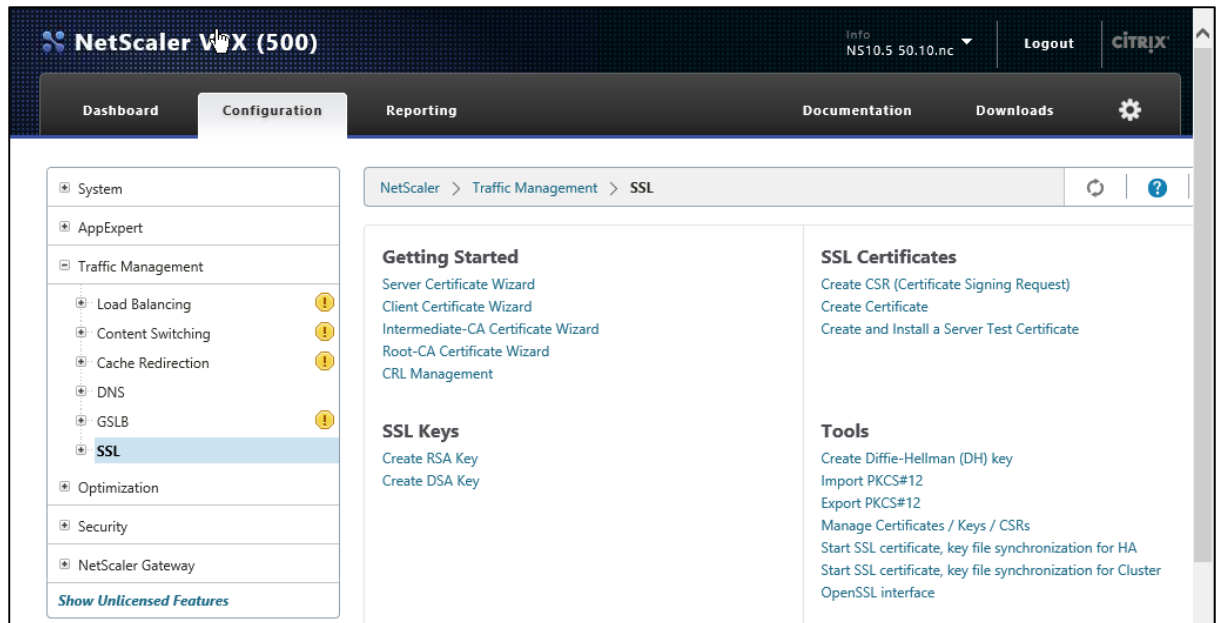


The backup creates a .p12 file with the name of your Certificate authority.

### On the NetScaler GUI

To import the backed up key and certificate, complete the following steps:

1. Go to **Traffic Management > SSL > Tools > Import PKCS#12.**



- Output file name is xxxxx.pem in the /flash/nsconfig/ssl folder on the appliance.  
PKCS12 File is the p12 backup file created.  
Password is the password used during the backup

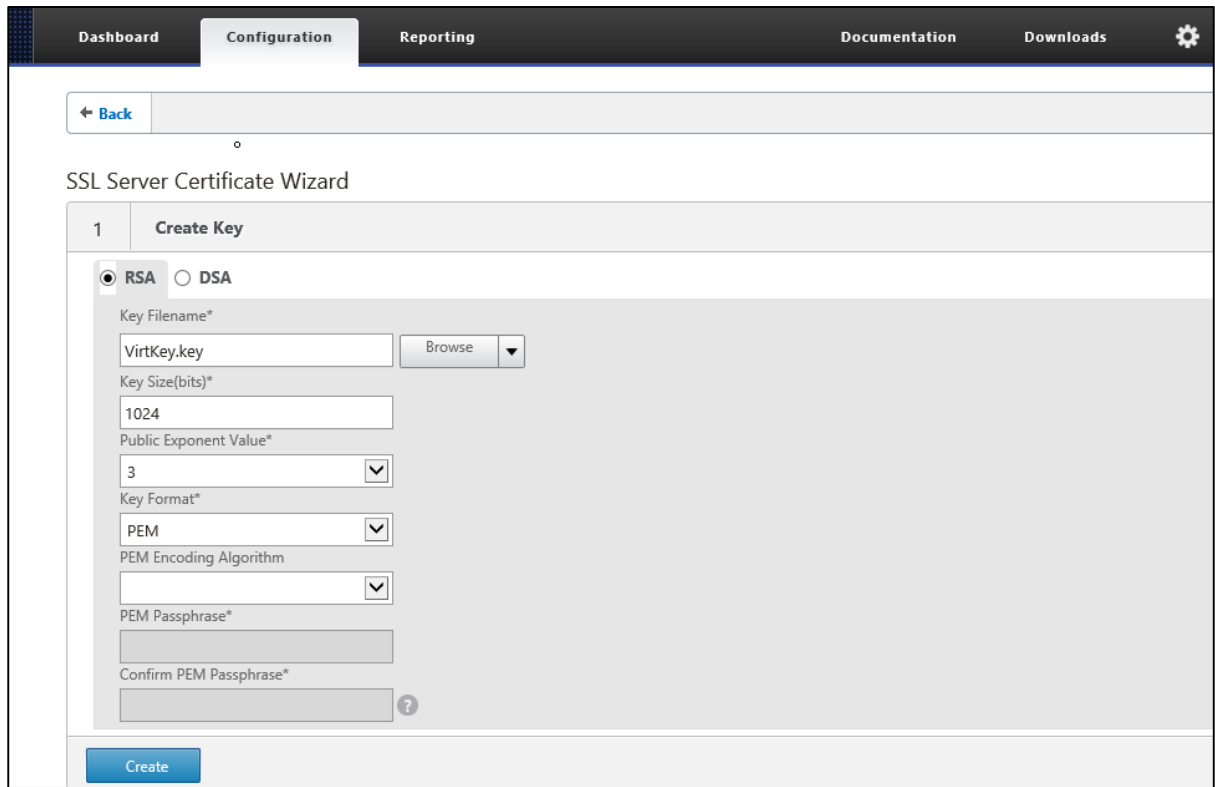
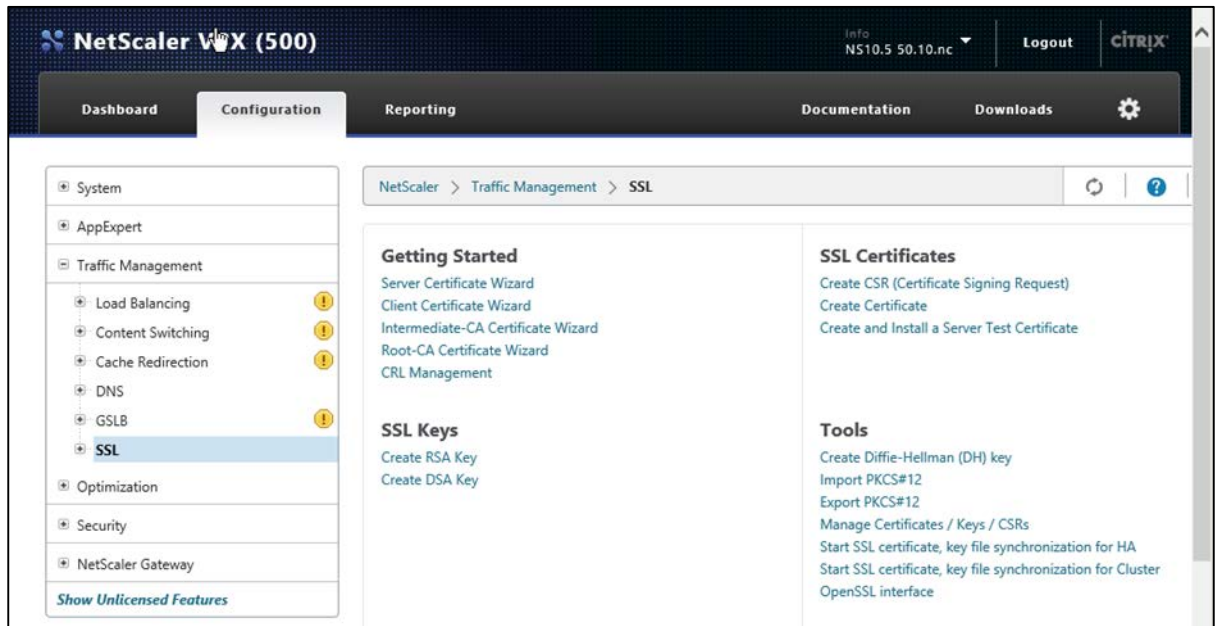
**Notes:**

- By using the dropdown arrows next to the browse buttons, it is possible to read the .p12 file from the local PC/Server where you did the Backup, and output the new .pem file to NetScaler appliance.
- The .pem file output by this process will contain both the RSA Private Key and the CA Certificate required to create server certificates on the NetScaler.

**Create the server certificate**

To create the server certificate, complete the following steps:

1. Go to **Traffic Management > SSL > Getting Started > Server Certificate Wizard**.



2. Create a Key. Key Filename is a name of your choice.

SSL Server Certificate Wizard

1 **SSL RSA/DSA Keys**

Key Type <b>RSA</b>	Key Filename <b>VirtKey.key</b>	Key Size(bits) <b>1024</b>	Key Format <b>PEM</b>
------------------------	------------------------------------	-------------------------------	--------------------------

2 **Create CSR (Certificate Signing Request)**

Request File Name\*  
  ▼

Key Filename\*  
  ▼

Key Format\*  
 ▼

PEM Passphrase (For Encrypted Key)

**Distinguished Name Fields**

Country\*  
 ▼

State or Province\*

Organization Name\*

City

Email Address  
 ?

Organization Unit

Common Name

**Attribute Fields**

Challenge Password

Company Name

3. Create a Certificate Signing Request. Request File Name is a name of your choice. Key Filename is carried forward from the previous step. Common name is the name that must match the FQDN of the NetScaler Gateway that you will create in a later section of this document.

SSL Server Certificate Wizard

1 SSL RSA/DSA Keys			
Key Type <b>RSA</b>	Key Filename <b>VirtKey.key</b>	Key Size(bits) <b>1024</b>	Key Format <b>PEM</b>

2 SSL Certificate			
Request File Name <b>testgw.req</b>	Country <b>UNITED KINGDOM</b>	State or Province <b>Bucks</b>	Organization Name <b>Citrix Systems</b>

3 Certificate

Certificate File Name\*  
testgw.cer

Certificate Format\*  
PEM

Auditing Type  
Server

Certificate Request File Name\*  
testgw.req  ?

Key Format\*  
PEM

Validity Period (Number of Days)  
365

CA Certificate File Name\*  
/nsconfig/ssl/VirtDomKeyAndCA.pem

CA Certificate File format\*  
PEM

CA Key File Name\*  
/nsconfig/ssl/VirtDomKeyAndCA.pem

CA Key File Format\*  
PEM

PEM Passphrase (For Encrypted CA Key)

CA Serial File Number\*  
/nsconfig/ssl/ns-root.srl

4. Create the Certificate.

SSL Server Certificate Wizard

1 SSL RSA/DSA Keys			
Key Type <b>RSA</b>	Key Filename <b>VirtKey.key</b>	Key Size(bits) <b>1024</b>	Key Format <b>PEM</b>

2 SSL Certificate			
Request File Name <b>testgw.req</b>	Country <b>UNITED KINGDOM</b>	State or Province <b>Bucks</b>	Organization Name <b>Citrix Systems</b>

3 SSL CA Certificate			
Certificate File Name <b>testgw.cer</b>	CA Certificate File Name <b>/nsconfig/ssl/VirtKeyAndCA.pem</b>	Certificate Request File Name <b>testgw.req</b>	CA Serial File Number <b>/nsconfig/ssl/ns-root.srl</b>

4 Install Certificate	
Certificate-Key Pair Name*	testgw.hopto.org <input type="text"/>
Certificate File Name*	testgw.cer <input type="text"/> <input type="button" value="Browse"/>
Key File Name	VirtKey.key <input type="text"/> <input type="button" value="Browse"/>
Password	<input type="text"/>
Certificate Format*	PEM <input type="text"/>
<input type="checkbox"/> Certificate Bundle ?	
<input checked="" type="checkbox"/> Expiry Monitor	
Notification Period	30 <input type="text"/>
<input type="button" value="Create"/>	

- Install the certificate.  
**Important!** The GUI also shows a **Done** button as shown in the following screen shot. Do **not** click this before you click **Create**.

NetScaler VPX (500)		Info NS10.5 51.10.nc	Logout	CITRIX
Dashboard	Configuration	Reporting	Documentation	Downloads
<input type="button" value="Back"/>				
<input checked="" type="checkbox"/> SSL Certificate-Key pair testgw.hopto.org installed successfully				
SSL Server Certificate Wizard				
1	Create Key			
2	Create CSR (Certificate Signing Request)			
3	Certificate			
4	SSL Install Certificate			
Certificate-Key Pair Name <b>testgw.hopto.org</b>		Certificate File Name <b>/nsconfig/ssl/testgw.cer</b>		
<input type="button" value="Done"/>				

- All the steps are complete and click **Done**.

#### (Optional) Install the CA certificate

Install the CA certificate if you want to use SSL to communicate from the NetScaler Gateway to your StoreFront and XenDesktop farm.

- Go to **Traffic Management > SSL > Certificates > Install**.

2. Browse and select the imported .pem file at **Certificate File Name** and the **Key File Name** fields.
3. Click **Install**.

**Install Certificate**

Certificate-Key Pair Name\*

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name\*

Key File Name

Certificate Format  
 PEM  DER

Password

Certificate Bundle  
 Notify When Expires

Notification Period

### Review the installed certificates

1. Go to **Traffic Management > SSL > Certificates**.
2. Press the refresh icon.

The screenshot shows the NetScaler VPX (500) Configuration page. The breadcrumb navigation is **NetScaler > Traffic Management > SSL > SSL Certificates**. The page includes a table of installed certificates with the following data:

Name	Days to Expire	Status
ns-server-certificate	4485	Valid
testgw.hopto.org	729	Valid
VirtdomCA	2333	Valid

## NTP Server

You can use an NTP server to keep time on the NetScaler. SSL is so much easier when all the clocks are in step with each other.

Go to **System > NTP Servers > Add**.

[← Back](#)

**Create NTP Server**

NTP Server\*

 × ?

Minimum Poll Interval

Maximum Poll Interval

Auto Key

Key

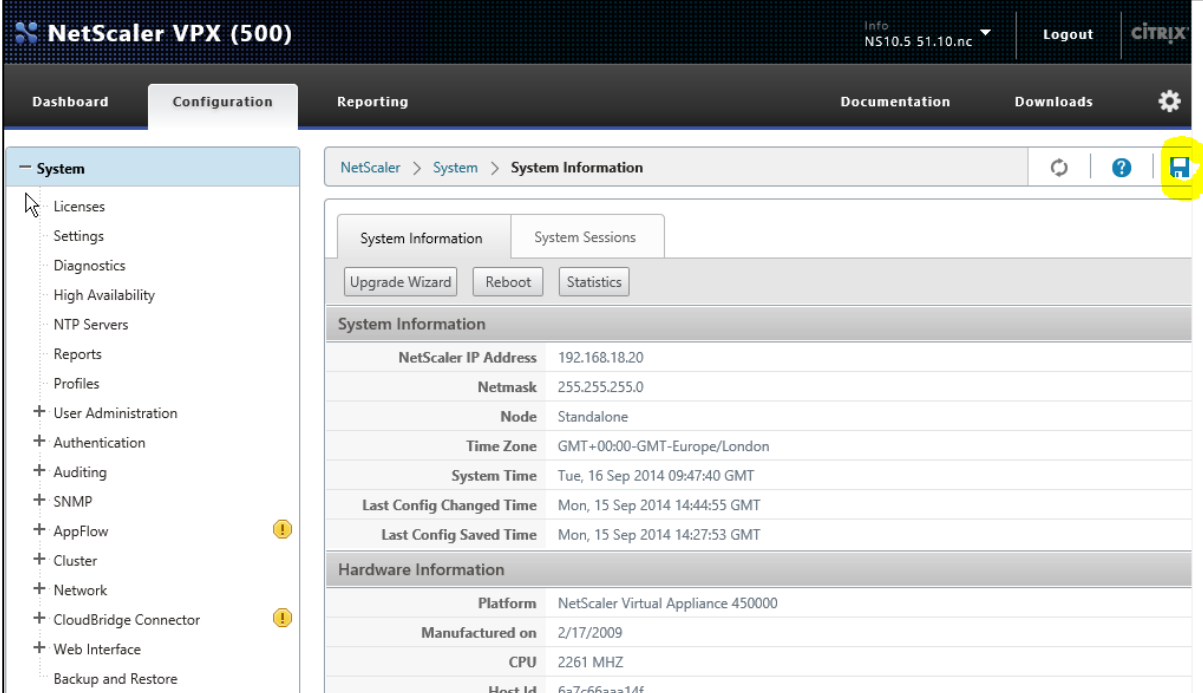
## Backups - and why you might want one

The NetScaler appliance now has its network configuration, licences and certificates in place, and the next stage is to run a wizard to create the NetScaler Gateway Virtual Server and its associated elements.

A point to note about the wizard used to establish the NetScaler Gateway Virtual Server is that it is really a series of sub-wizards, and the NetScaler configuration is updated after each sub-wizard. By having a backup or snapshot at this point one has an option to:

- a) Accept the resulting configuration and move forward
- b) Rerun parts of the wizard
- c) Fall back to this point and start again

First save the configuration by using the **Save** button at the top right of the GUI.



The screenshot shows the NetScaler VPX (500) GUI. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The 'Configuration' tab is active. The left sidebar shows a tree view under 'System' with various sub-items like Licenses, Settings, Diagnostics, etc. The main content area displays 'System Information' with tabs for 'System Information' and 'System Sessions'. Below the tabs are buttons for 'Upgrade Wizard', 'Reboot', and 'Statistics'. The 'System Information' section contains a table with the following data:

System Information	
NetScaler IP Address	192.168.18.20
Netmask	255.255.255.0
Node	Standalone
Time Zone	GMT+00:00-GMT-Europe/London
System Time	Tue, 16 Sep 2014 09:47:40 GMT
Last Config Changed Time	Mon, 15 Sep 2014 14:44:55 GMT
Last Config Saved Time	Mon, 15 Sep 2014 14:27:53 GMT

Below this is the 'Hardware Information' section with another table:

Hardware Information	
Platform	NetScaler Virtual Appliance 450000
Manufactured on	2/17/2009
CPU	2261 MHZ
Host Id	6a7c66aaa14f

The 'Save' button in the top right corner of the main content area is highlighted in yellow.

The NetScaler Backup and Restore tool is at **System > Backup and Restore**.

## Backup

NetScaler Version

**NS10.5: Build 51.10.nc, Date: Aug 14 2014, 04:57:29**

File Name\*

Type\*



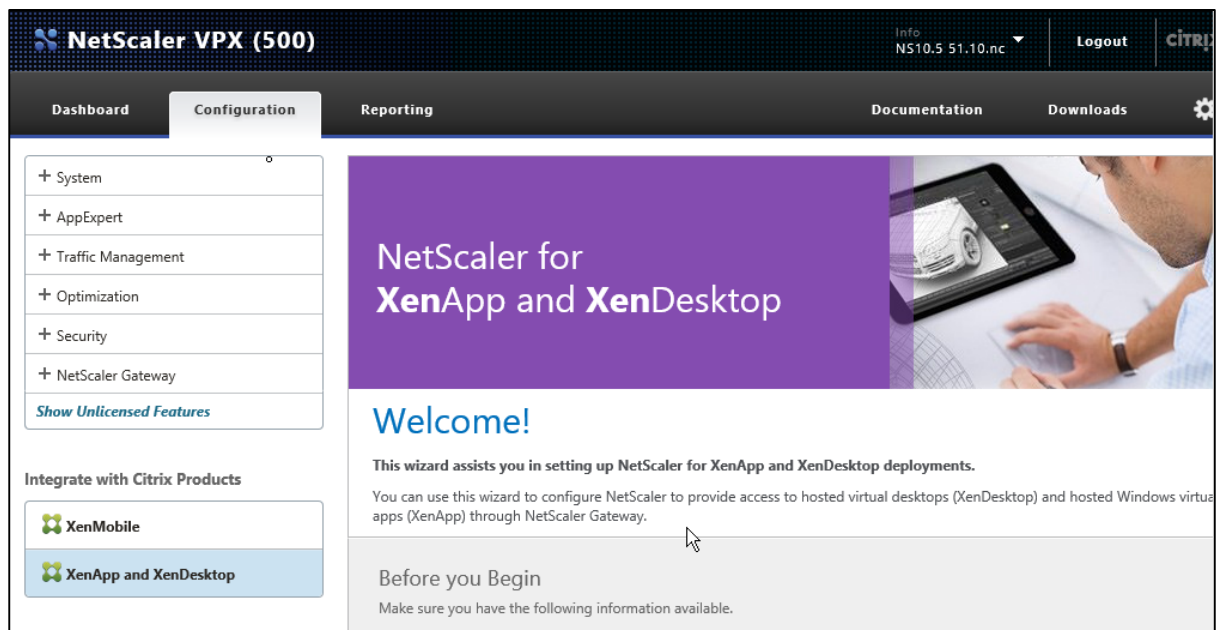
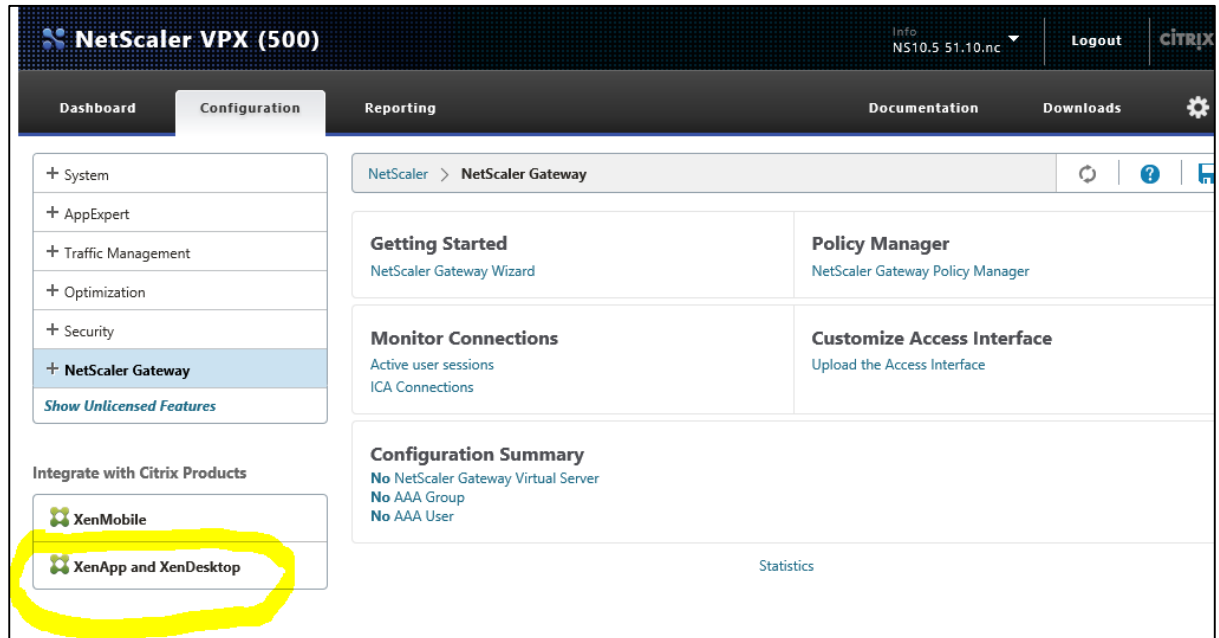
Comment



## Create a NetScaler Gateway Virtual Server

To create a virtual server, complete the following steps:

1. Go to **NetScaler > NetScaler Gateway > Integrate with Citrix Products > XenApp and XenDesktop**.



2. Click **Get Started**.

**Access through NetScaler Gateway**

- Public IP address for NetScaler Gateway
- A server certificate for the NetScaler appliance
- LDAP/RADIUS authentication server details
- Fully Qualified Domain Name (FQDN) of StoreFront/Web Interface Server

**Load Balance StoreFront/Web Interface/Xen Farm**

- IP address for the load balancing virtual server
- SSL certificate and key pair
- Site Path and PNAgent Site Path
- Secure Ticket Authority Server

**Optimization Features Overview**

- TCP Profile Settings
- SSL Quantum Settings
- HTTP Caching
- HTTP Compression

**Security and Visibility Overview**

- AppFw Profile
- AppFw Policy
- AppFlow Policy for HDX Insight

[Get Started](#)

← Back

### XenApp/XenDesktop Setup Wizard

What is your deployment

**Single Hop**

The diagram illustrates a 'Single Hop' deployment architecture. It starts with a 'Client' (represented by a person icon) connected to the 'Internet' (cloud icon). From the Internet, traffic goes through an 'Access Gateway' (server rack icon) to reach the 'Server Farm' (multiple server rack icons).

**What is your Citrix Integration Point?**

StoreFront

Continue
Cancel

3. Enter the IP for your NetScaler Gateway Virtual Server.
4. Click **Continue**.

← Back

**NetScaler Gateway Settings**

Virtual Server Name\*

NetScaler Gateway IP Address\*  
 ?

Port\*

Redirect requests from port 80 to secure port

Continue
Cancel

5. Chose the Server Certificate created before.
6. Click **Continue**.

← Back

### NetScaler Gateway Settings

Name	NetScaler Gateway IP Address	Port	Redirect requests from port 80 to secure port
TestGW	192.168.18.22	443	No

### Server Certificate

Use existing certificate
  Install Certificate

Server Certificate\*

testgw.hopto.org

Continue Do It Later

← Back

### NetScaler Gateway Settings

Name	NetScaler Gateway IP Address	Port	Redirect requests from port 80 to secure port
TestGW	192.168.18.22	443	No

### Server Certificate

testgw.hopto.org

### Authentication Settings

You can configure authentication to allow the NetScaler ADC to serve as a proxy for users who connect with devices through the internal network. You can configure LDAP and RADIUS servers, and client certificate authentication to provide two-factor authentication. In the case of LDAP authentication, the NetScaler binds to the LDAP server using the administrator credentials you provide and searches for the user. With RADIUS authentication, a key is used.

Primary authentication method\*

Active Directory/LDAP

IP Address\*

192 . 168 . 80 . 1  IPv6

Load Balancing

Port\*

389

Time out (seconds)\*

3

Base DN\*

dc=virtom,dc=chsys3,dc=com

Service account\*

administrator@virtom.chsys3.com

Group Extraction

Server Logon Name Attribute\*

sAMAccountName

Password\*

.....

Confirm Password\*

.....

Secondary authentication method\*

None


Continue Cancel

In this example, users are authenticated against Active Directory. The IP Address 192.168.80.1 is the address of the Domain Controller.

7. Enter details and click **Continue**.


← Back

---

**NetScaler Gateway Settings** 


Name	NetScaler Gateway IP Address	Port	Redirect requests from port 80 to secure port
TestGW	192.168.18.22	443	No

---

**Server Certificate** 


testgw.hopto.org

---

**Authentication Settings** 

Primary Authentication	Secondary Authentication
Active Directory/LDAP: 192.168.80.1_LDAP_pol	Not Configured

**Storefront**

StoreFront FQDN\* 

xenstore05.virtom.chsys3.com

Site Path\*

/Citrix/StoreWeb

Single Sign-on Domain\*

Virtom

Store Name\*

Store


Secure Ticket Authority Server\*

http://xenapp07.virtom.chsys3.com +

Storefront Server\*

192 . 168 . 80 . 5 +

Protocol\*

HTTP 


Port\*

80


Load Balancing

**Continue** **Cancel**


← Back

**NetScaler Gateway Settings** 


Name	NetScaler Gateway IP Address	Port	Redirect requests from port 80 to secure port
TestGW	192.168.18.22	443	No

**Server Certificate** 

testgw.hopto.org

**Authentication Settings** 

Primary Authentication	Secondary Authentication
Active Directory/LDAP: 192.168.80.1_LDAP_pol	Not Configured

**Storefront** 

StoreFront FQDN	xenstore05.virtom.chsys3.com	Secure Ticket Authority	http://xenapp07.virtom.chsys3.com
Site Path	/Citrix/StoreWeb	Load Balancing configured	No
Single Sign-on Domain	Virtom		

8. Leave Xen Farm > Configure = Blank.

**Note:** This section relates to load balancing the XenDesktop Controllers and XenApp servers, which is not covered in this document. However, this sub-wizard can be revisited at any time.


9. Click **Continue**.

**Xen Farm**


Configure




← Back

**NetScaler Gateway Settings** 


Name	NetScaler Gateway IP Address	Port	Redirect requests from port 80 to secure port
TestGW	192.168.18.22	443	No

**Server Certificate** 

testgw.hopto.org

**Authentication Settings** 

Primary Authentication	Secondary Authentication
Active Directory/LDAP: 192.168.80.1_LDAP_pol	Not Configured

**Storefront** 

StoreFront FQDN	xenstore05.virtom.chsys3.com	Secure Ticket Authority	http://xenapp07.virtom.chsys3.com
Site Path	/Citrix/StoreWeb	Load Balancing configured	No
Single Sign-on Domain	Virtom		

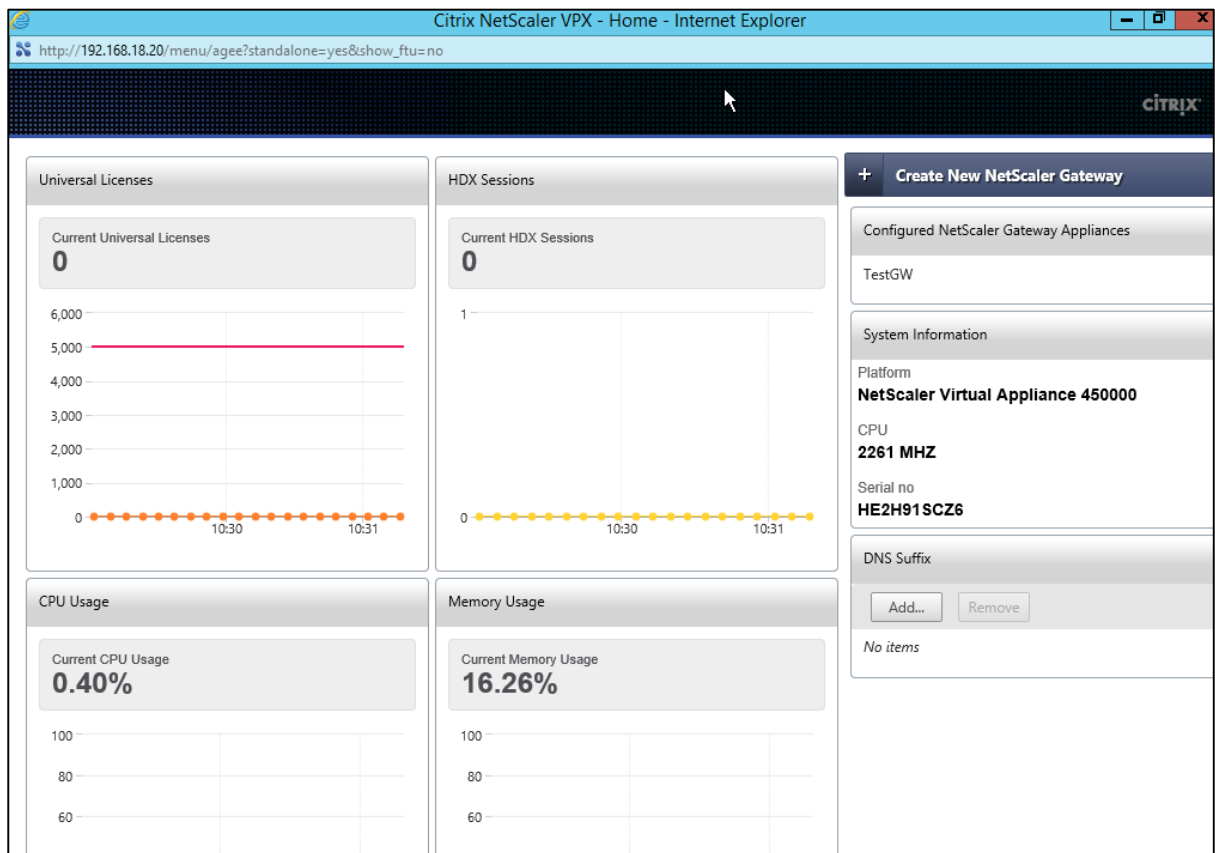
10. Do **not** click **Apply**.

**Note:** Optimization is not covered by this document. However, this section can be revisited at any time.

11. Review settings and click **Done**.



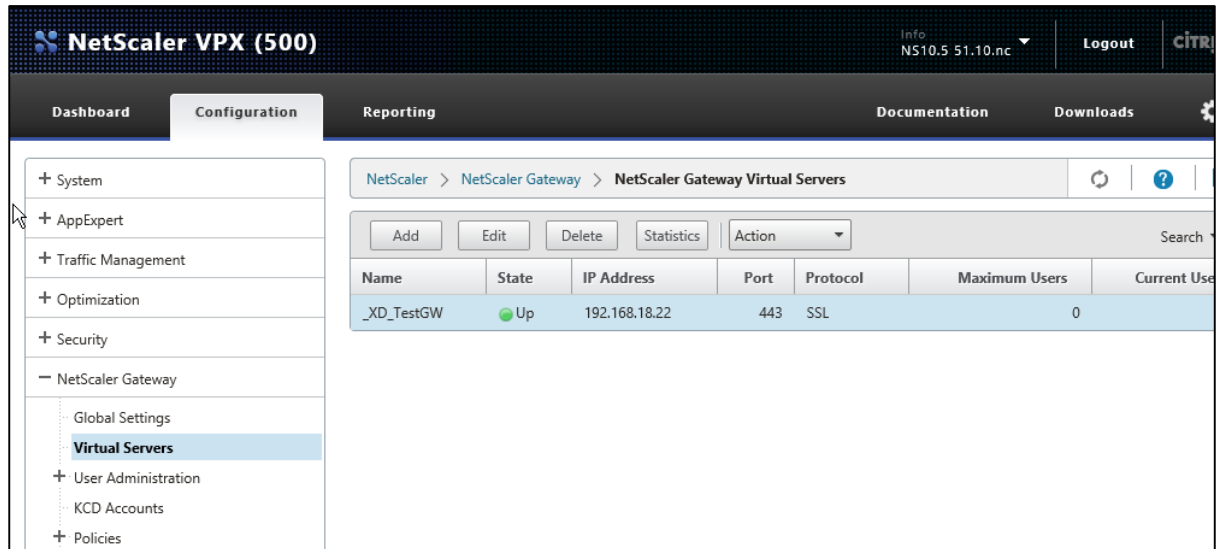
A dashboard page is displayed. You can close this and return to the Configuration GUI.



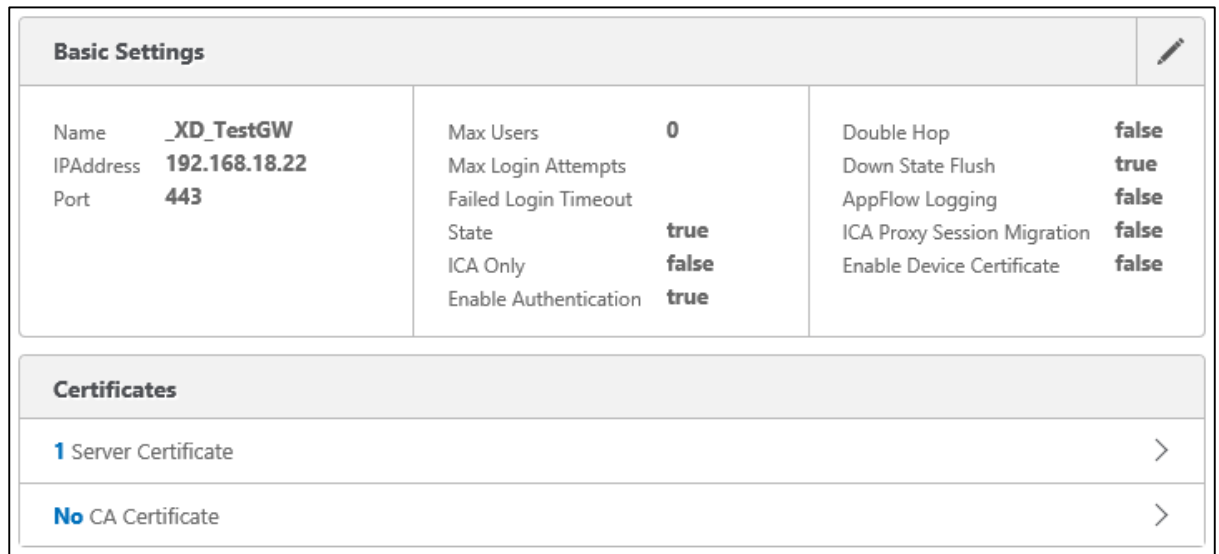
**(Optional) Add the CA certificate to the NetScaler Gateway Virtual Server**

If you want to use SSL to communicate from the NetScaler Gateway to StoreFront and XenDesktop, you will need to add the CA certificate to the NetScaler Gateway Virtual Server.

1. Go to **NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Server**.



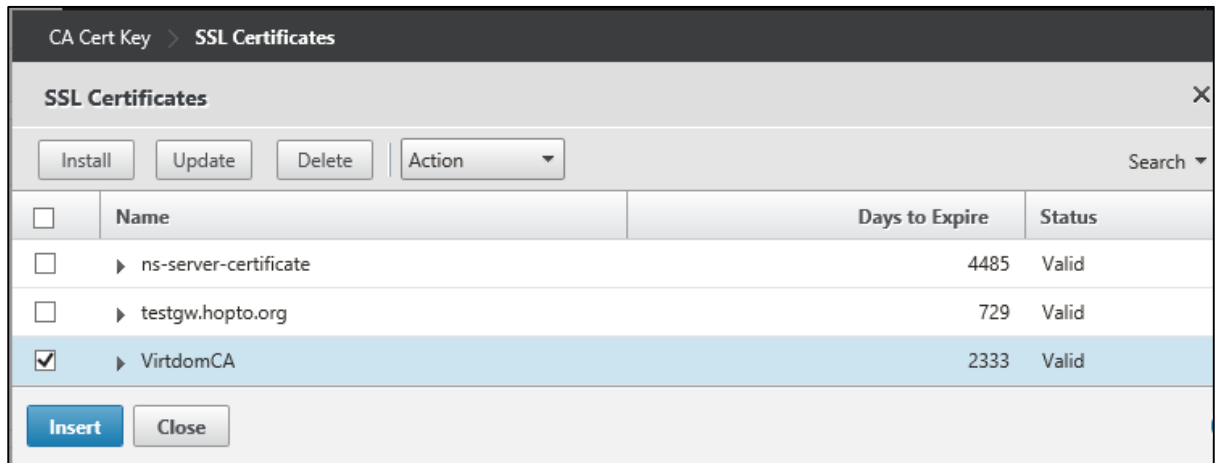
2. Select **\_TestGW** and click **Edit**.
3. Click **No CA Certificate**.



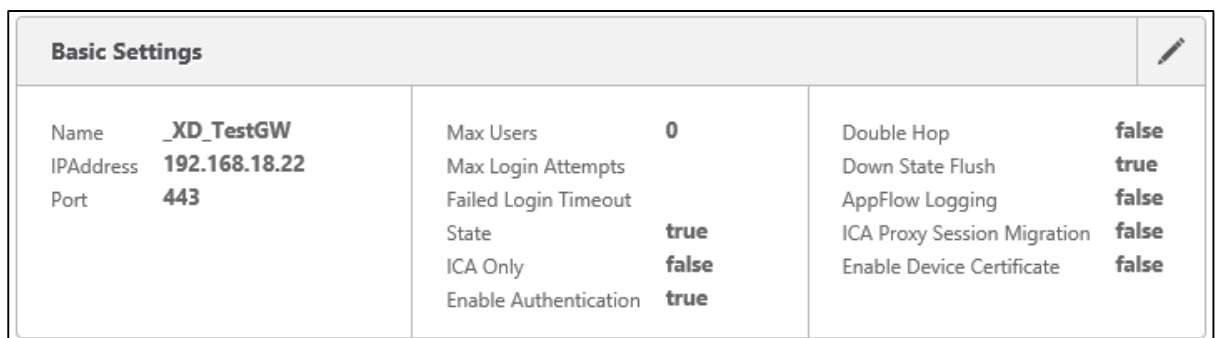
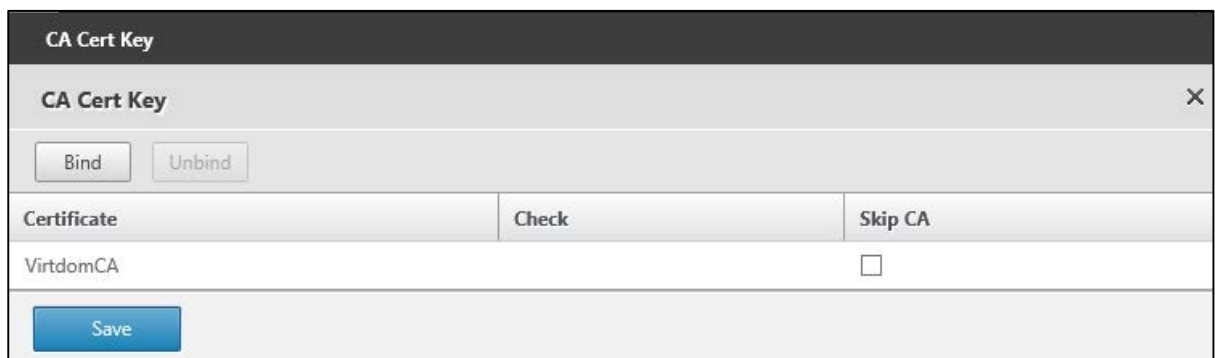
4. Click **Bind**.



- Select the CA certificate imported and click **Insert**.



- Click **Save**.



- Scroll down to the bottom of the screen and click **Done**.

Certificates	
1 Server Certificate	>
1 CA Certificate	>
Authentication	
Primary Authentication	
1 LDAP Policy	>
Published Applications	
No Next HOP Server	>
1 STA Server	>
No Url	>
Policies	
Request Policies	
2 Session Policies	>
4 Cache Policies	>
Done	

8. Save your work to date by clicking on the **Save** icon on the upper right corner.

The screenshot shows the NetScaler VPX (500) configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The left sidebar lists various configuration categories like System, AppExpert, Traffic Management, etc. The main content area is titled 'System Information' and displays the following details:

System Information	
NetScaler IP Address	192.168.18.20
Netmask	255.255.255.0
Node	Standalone
Time Zone	GMT+00:00-GMT-Europe/London
System Time	Wed, 10 Sep 2014 10:32:24 GMT
Last Config Changed Time	Wed, 10 Sep 2014 09:27:33 GMT
Last Config Saved Time	Wed, 10 Sep 2014 09:28:57 GMT
Hardware Information	
Platform	NetScaler Virtual Appliance 450000
Manufactured on	2/17/2009
CPU	2261 MHZ

A yellow circle highlights the 'Save' icon (a floppy disk) in the top right corner of the configuration page.

If you do not save after making changes to the NetScaler configuration, there is a risk that those changes will be lost when the NetScaler reboots.

# StoreFront

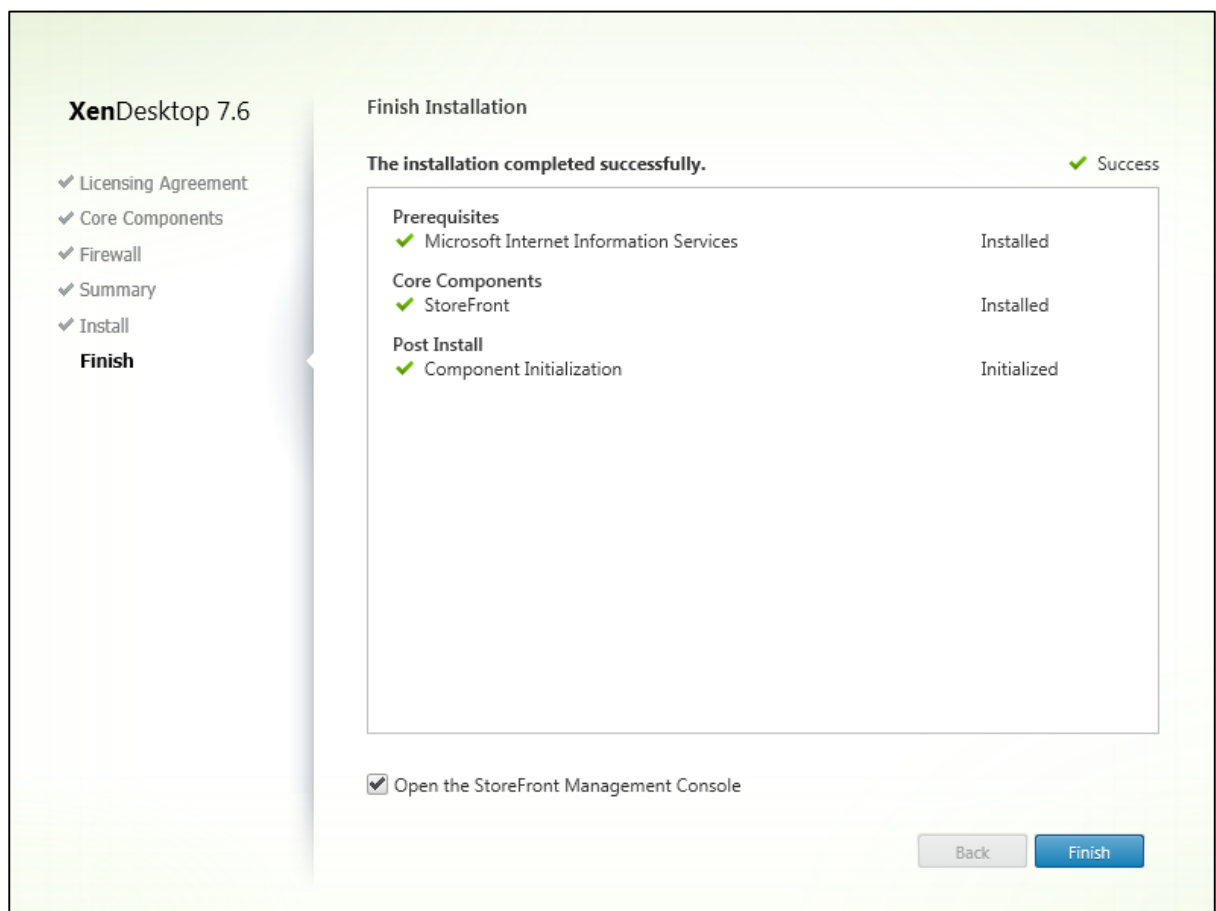
## DNS

Check that the DNS entries for the NetScaler Gateway Virtual Server (testgw.hopto.org) point to the correct place.

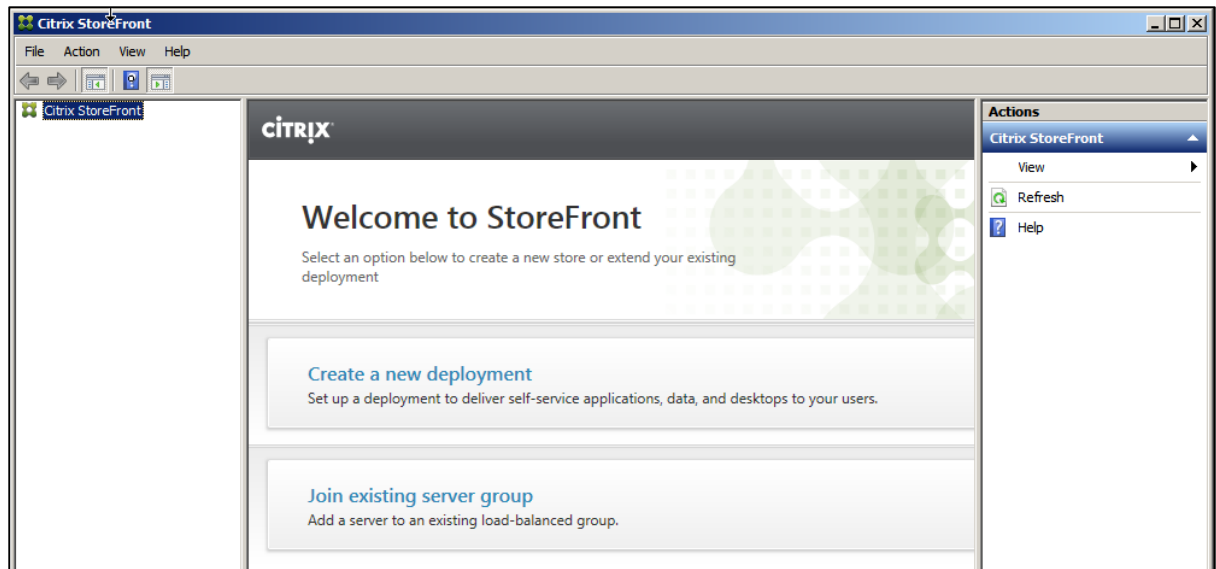
- On Internet - DNS needs to point to a public address that is accessible from the Internet. This will typically be a public address on a firewall/router that is forwarded to the NetScaler Gateway Virtual Server IP
- On the private internal LAN – DNS needs to point to the local address of the NetScaler Gateway Virtual Server in the DMZ – 192.168.18.22

## StoreFront – Configuring a new installation

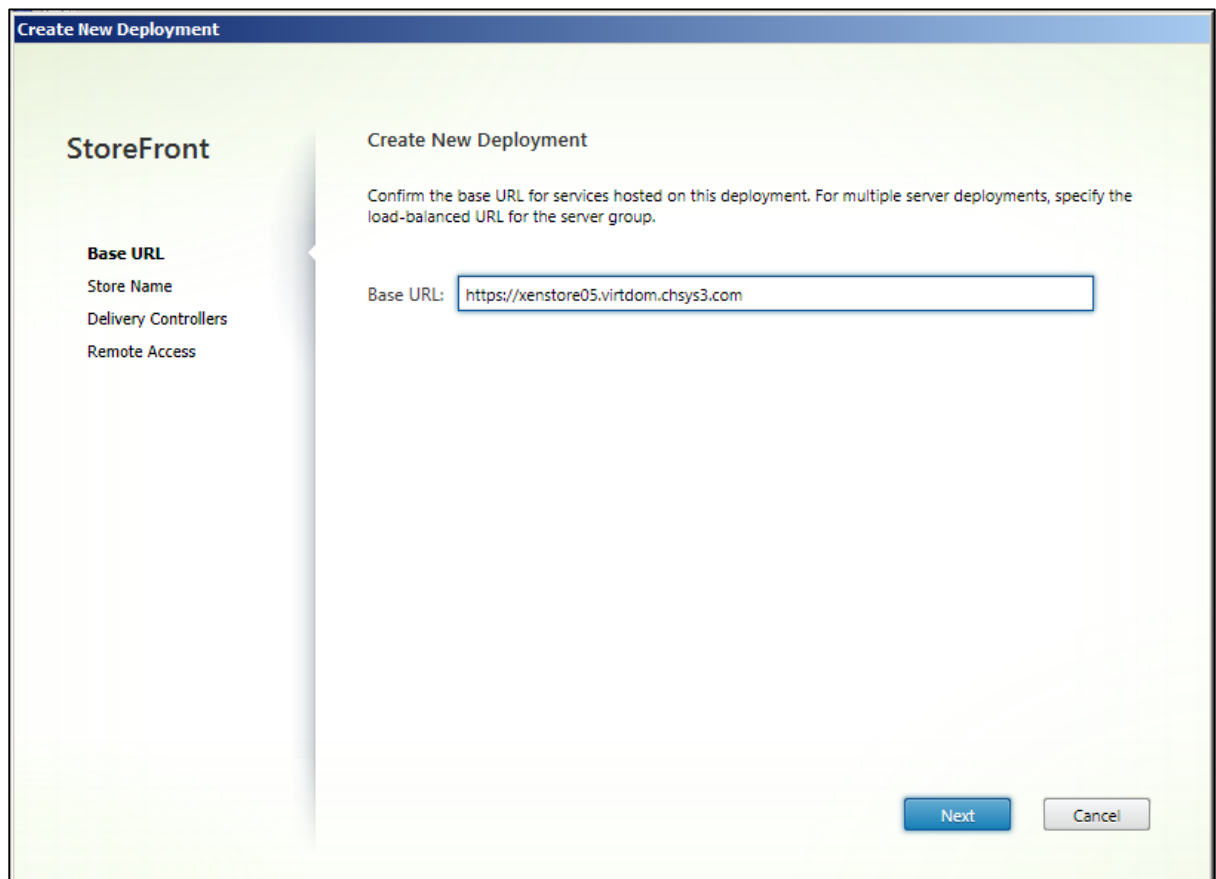
1. Install StoreFront from your distribution media.



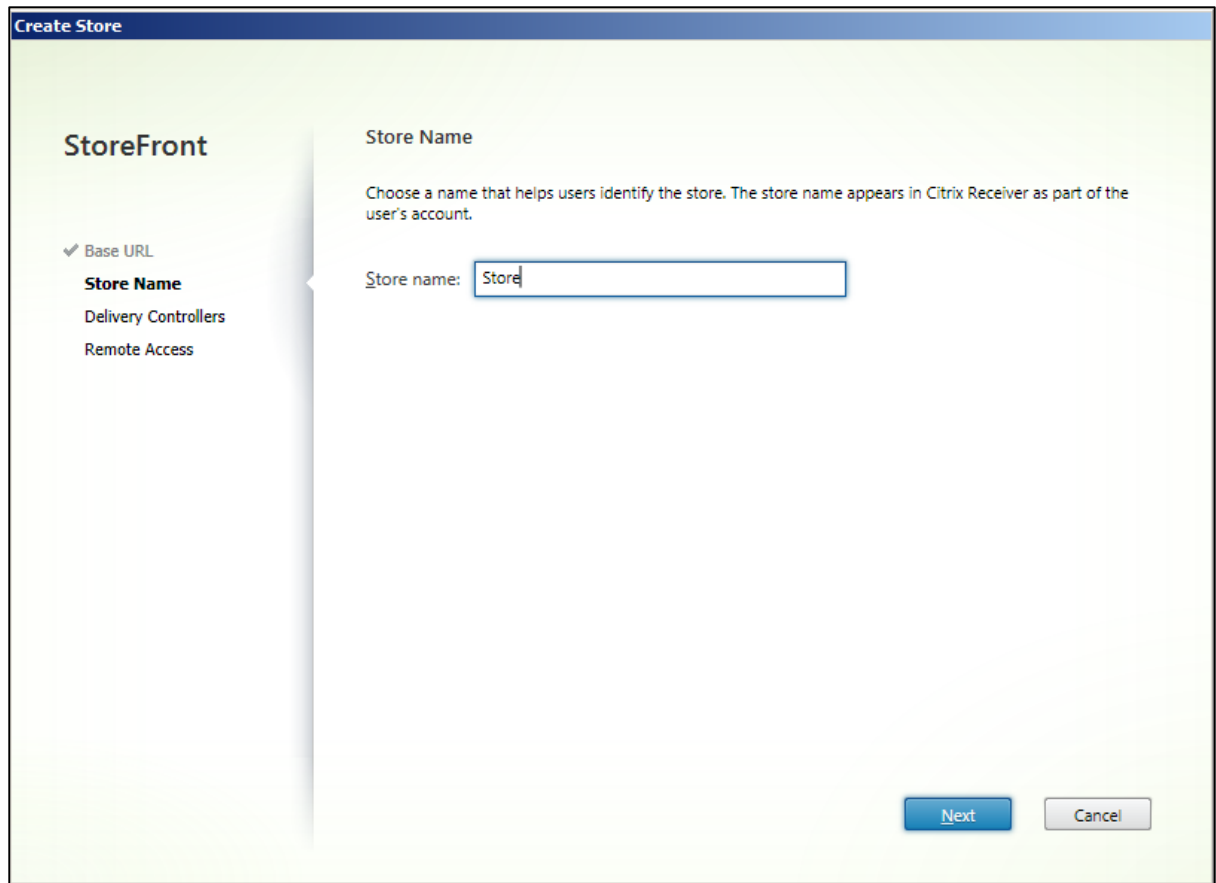
2. On completion, click **Finish** and open the StoreFront Management Console.



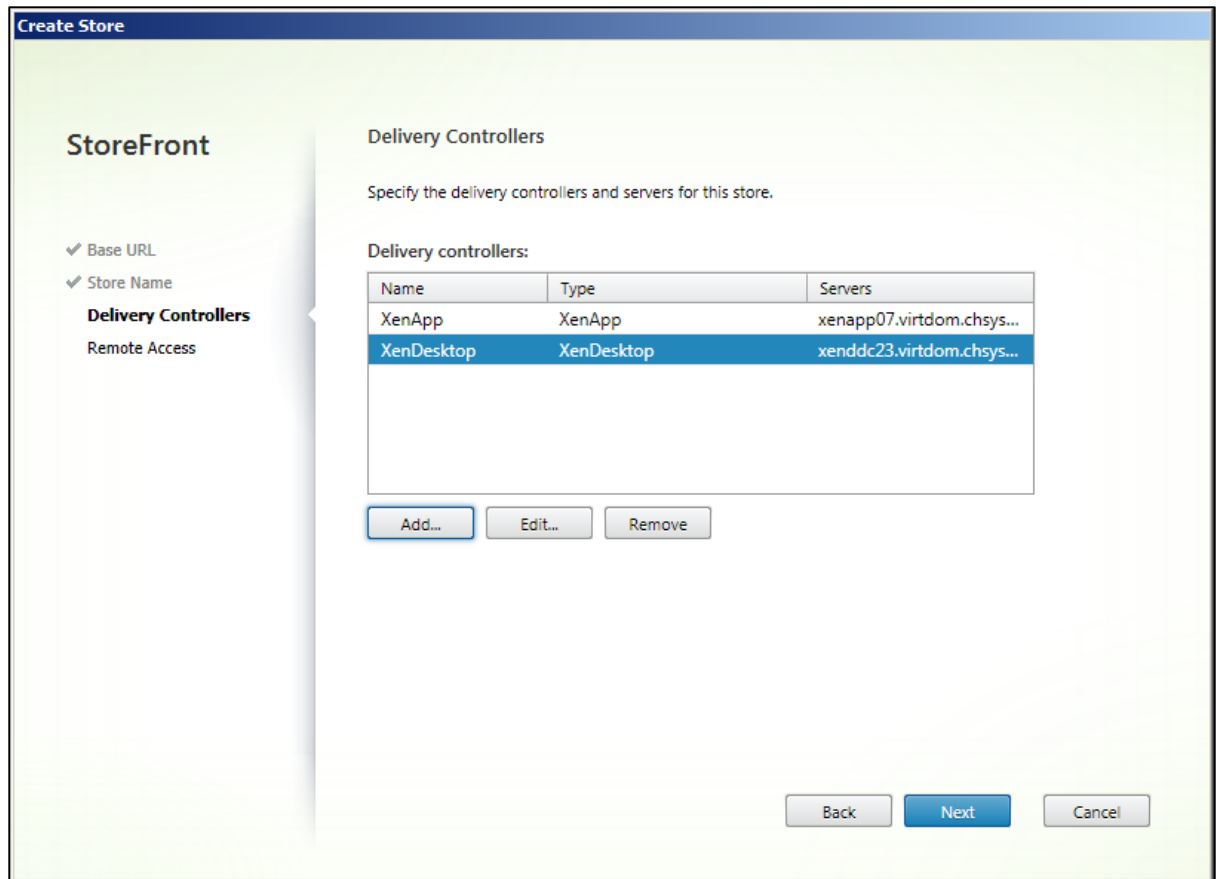
3. When opened, the Management Console will notice that this is a new installation and will offer a choice of options.
4. Click **Create a new deployment**.
5. Accept the default Base URL and click **Next**.



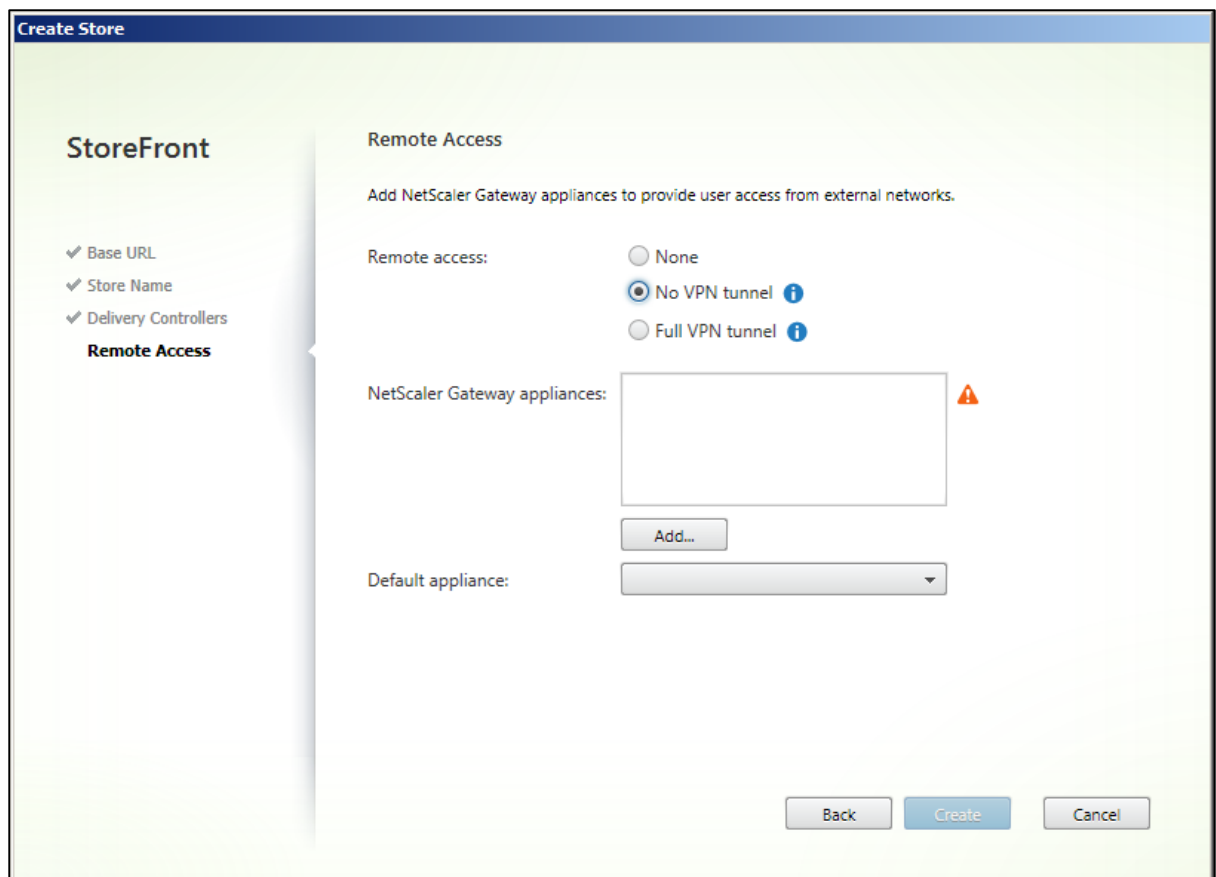
6. Enter a store name of Store.
7. Click **Next**.



8. Enter Delivery Controllers.
9. Click **Next**.



10. Select **No VPN tunnel**.



11. Add a NetScaler Gateway appliance.
12. Fill out the details of the NetScaler Gateway Appliance. Unless you have a complex environment, the Subnet IP address may be left blank.
13. Click **Next**.

**Add NetScaler Gateway Appliance**

**StoreFront**

**General Settings**  
Secure Ticket Authority

**General Settings**

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

Display name:

NetScaler Gateway URL:

Version:

Subnet IP address: (optional)

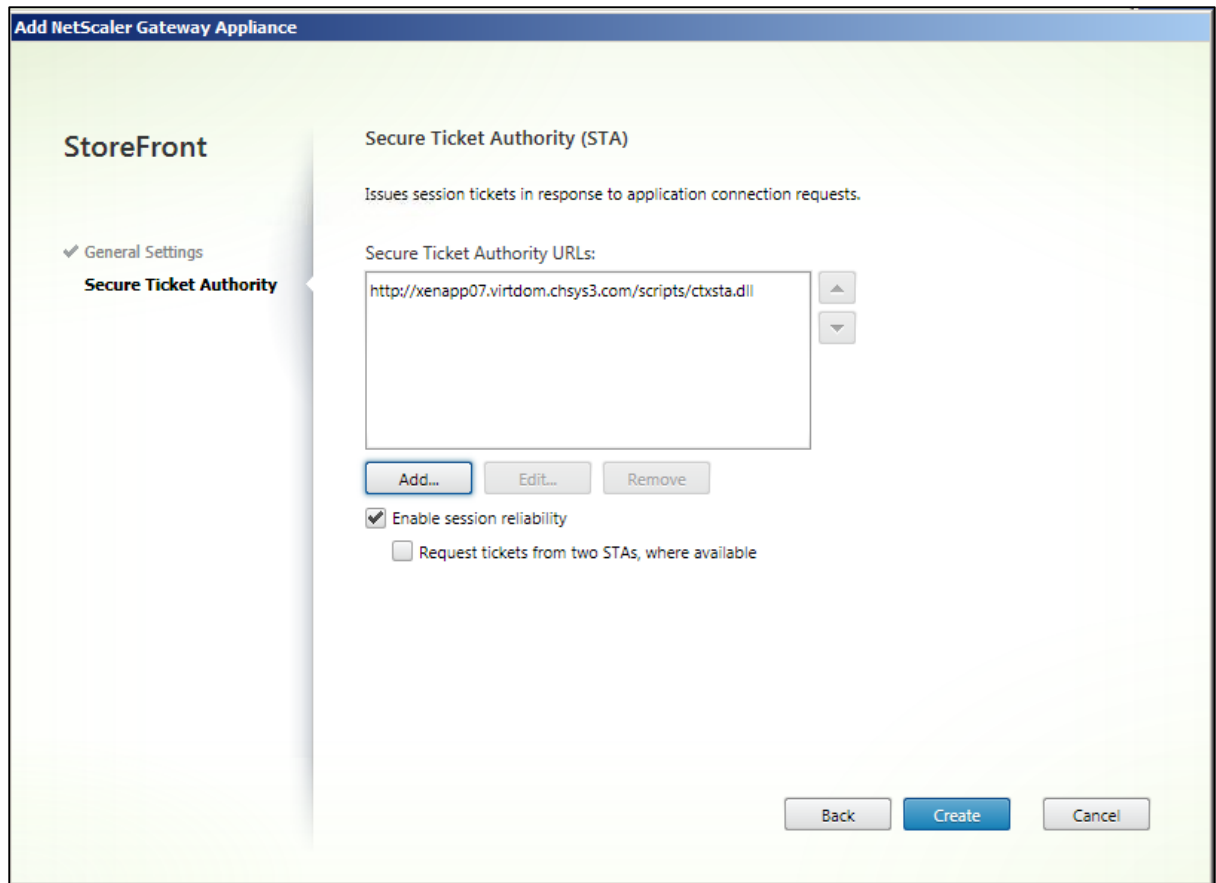
Logon type:

Smart card fallback:

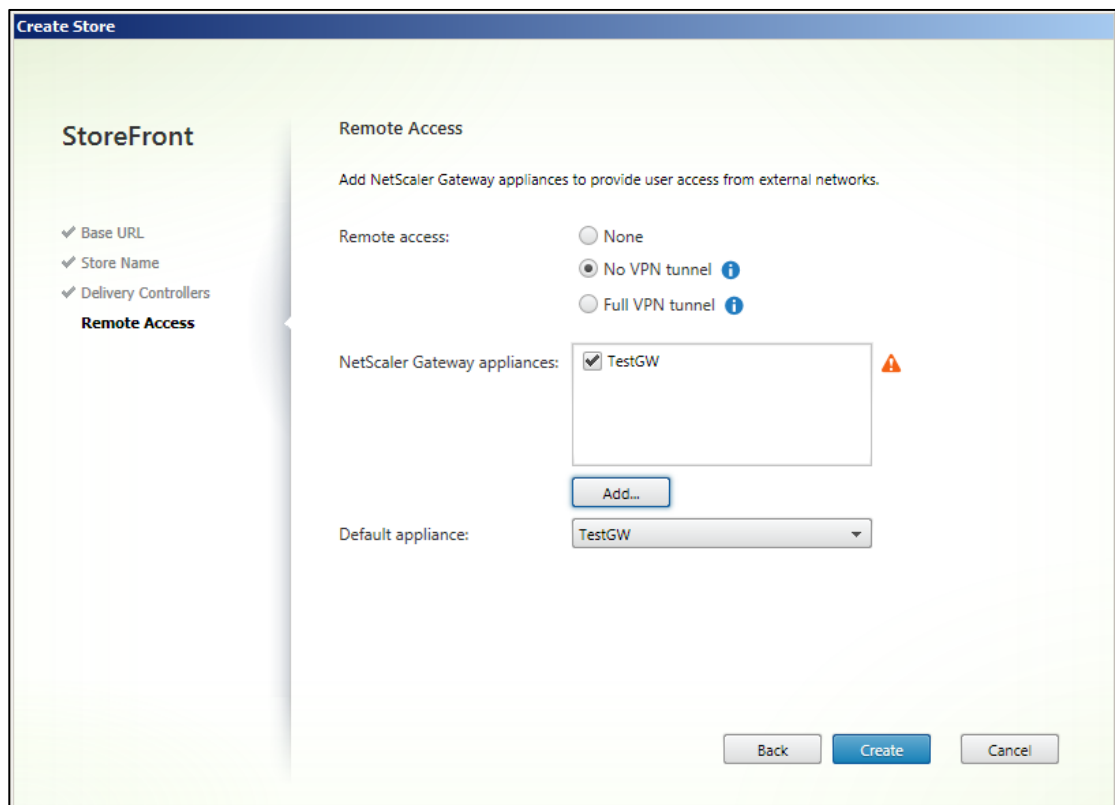
Callback URL: (optional)  /CitrixAuthService/AuthService.asmx

**Next** **Cancel**

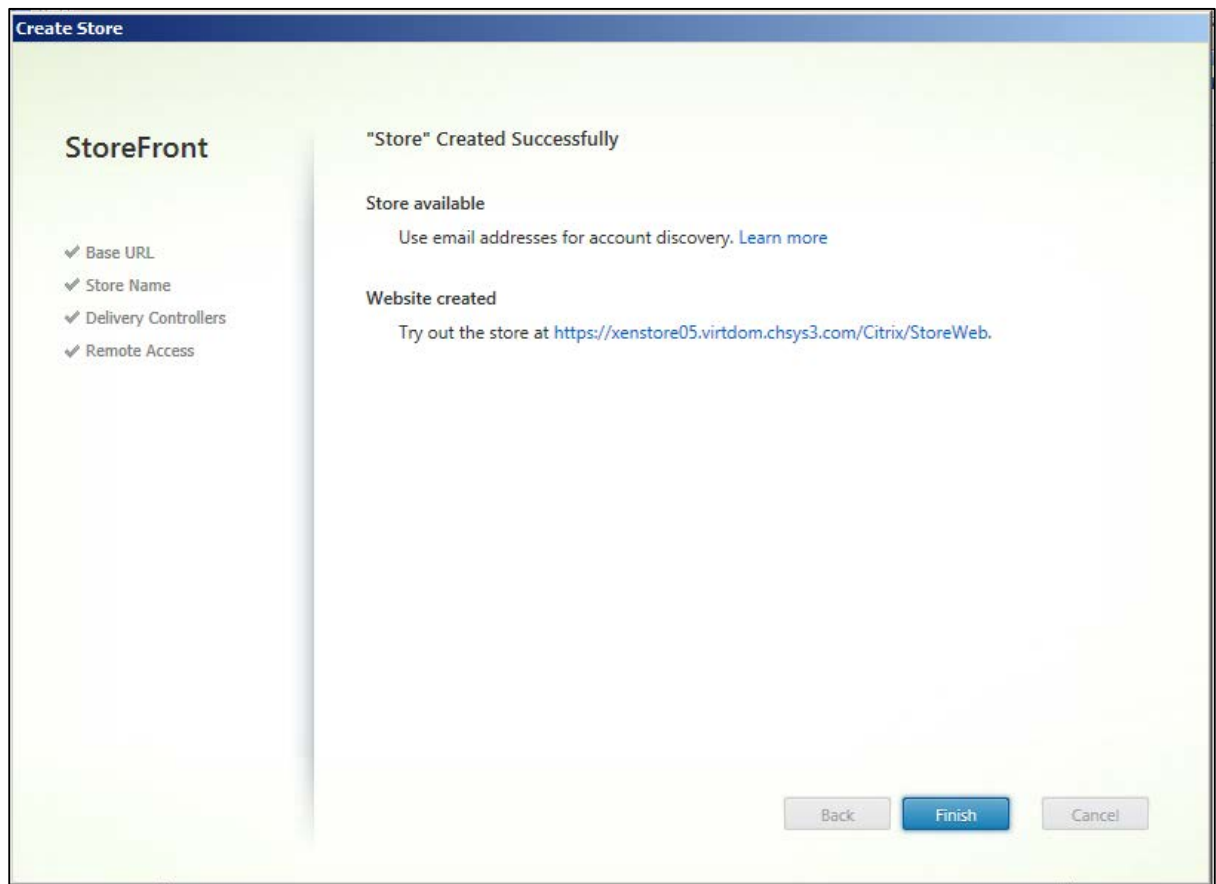
14. Add a Secure Ticket Authority.
15. Ensure that any STA referenced here is also included in the NetScaler Gateway Virtual Server list of STAs.
16. Click **Create**.



17. There appears a warning symbol indicating that enabling remote access will automatically enable pass-through authentication from the NetScaler Gateway. This is what is expected. Click **Create**.



18. Click **Finish**.







6. When logged in you should be presented with the StoreFront page, and be able to launch Apps and Desktops.