Customers who viewed this article also viewed

Article
Common Resolutions to &#8220;Cannot Complete Your Request&#8221; Error

Article
Secure Ticket Authority (STA) Status Is Marked As DOWN on NetScaler Gateway Virtual Server

Article
NetScaler Gateway, StoreFront and XenDesktop Integration Communication Workflow

CTX200287

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

Article | How do I, Configuration | 8 found this helpful | Created: 17 Nov 2014 | Modified: 29 Mar 2018

Applicable Products

XenDesktop StoreFront NetScaler 10.5 NetScaler Gateway 10.5

Objective

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.

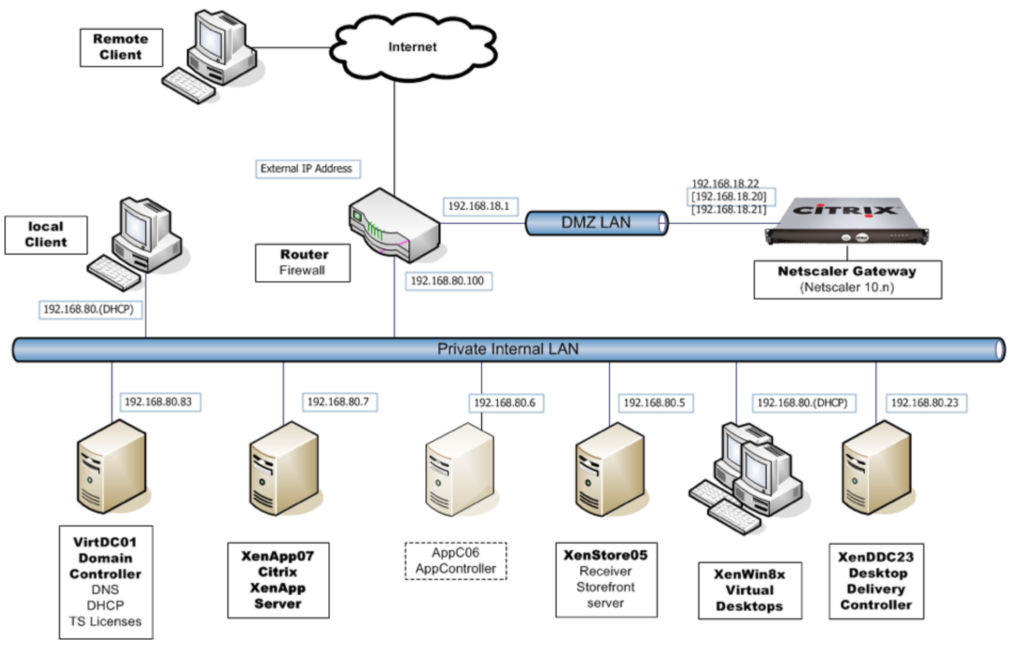
While this document only attempts to record a single configuration, it is hoped that it will act as a stepping stone for those who wish to create similar or more advanced configurations.

Instructions

Contents

Call or Chat

Network Diagram



The NetScaler will use the following network addresses

NetScaler IP	Subnet IP	Virtual IP
192.168.18.20	192.168.18.21	192.168.18.22

Back to top

NetScaler Configuration

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

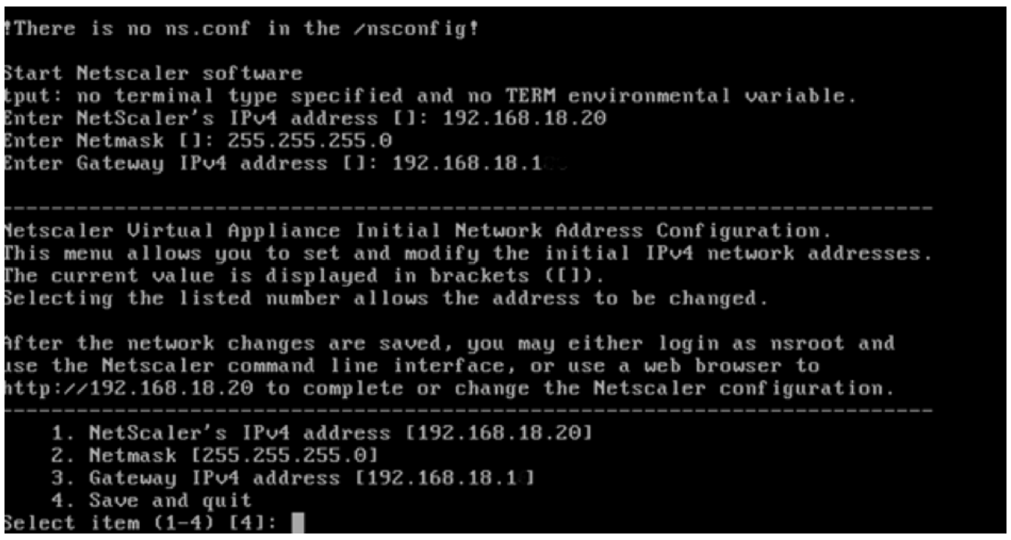
The processes for configuring a physical NetScaler appliance, or a NetScaler VPX virtual appliance hosted on another Hypervisor is similar.

Back to top

Initial setup from XenCenter Console

1. Download the latest NetScaler VPX virtual appliance from 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
tput: 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.

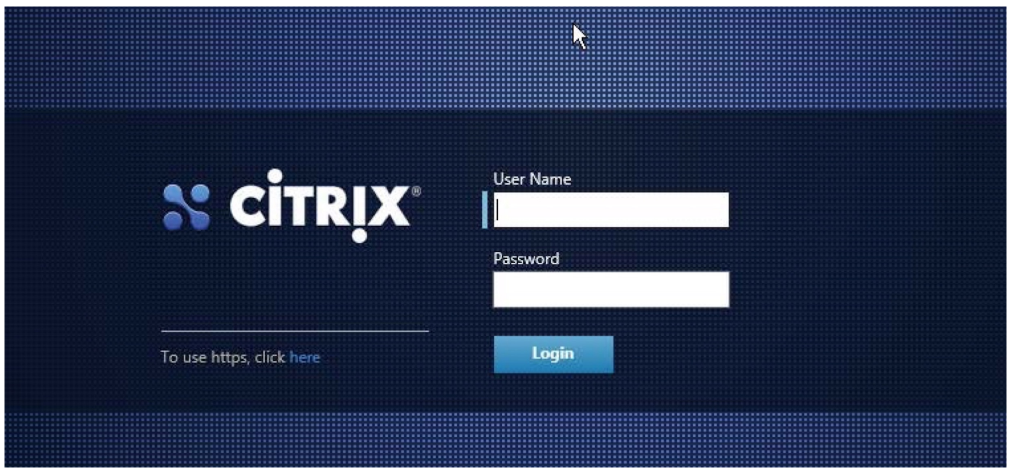
IPv4 address	Netmask	Default Gateway
192.168.18.20	255.255.255.0	192.168.18.1

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

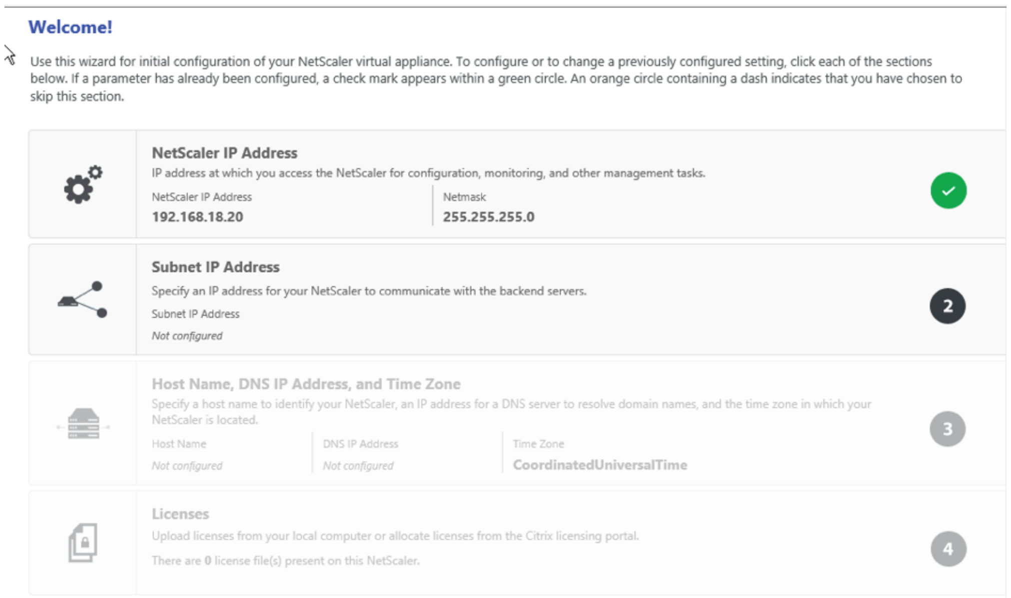
Back to top

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.

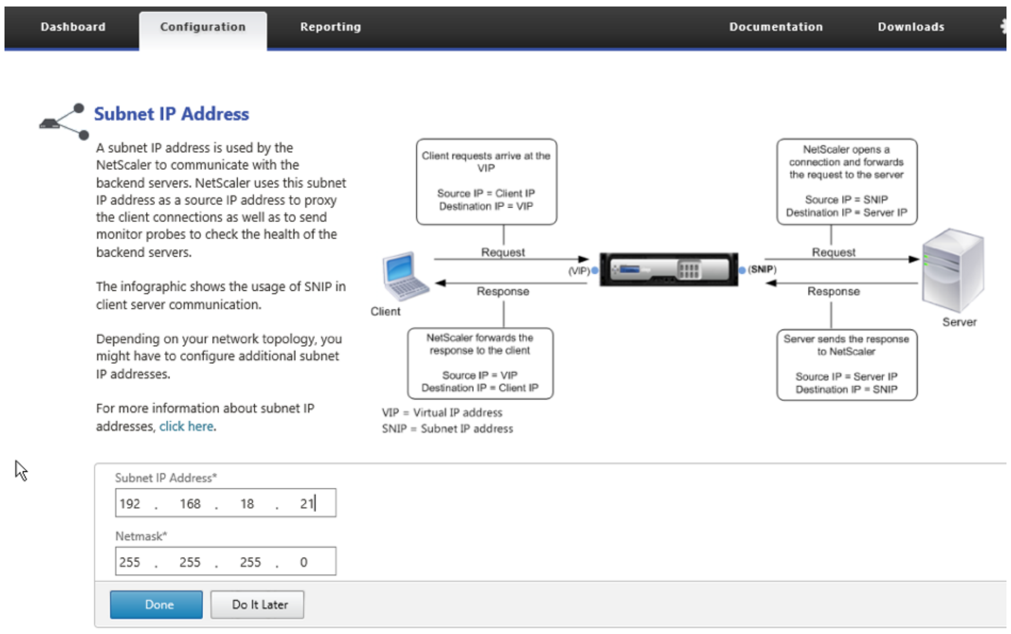
NetScaler IP Address
IP address at which you access the NetScaler for configuration, monitoring, and other management tasks.
NetScaler IP Address: **192.168.18.20**
Netmask: **255.255.255.0**
✓

Subnet IP Address
Specify an IP address for your NetScaler to communicate with the backend servers.
Subnet IP Address: *Not configured*
2

Host Name, DNS IP Address, and Time Zone
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: *Not configured*
DNS IP Address: *Not configured*
Time Zone: **CoordinatedUniversalTime**
3

Licenses
Upload licenses from your local computer or allocate licenses from the Citrix licensing portal.
There are **0** license file(s) present on this NetScaler.
4

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



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.

Client requests arrive at the VIP
Source IP = Client IP
Destination IP = VIP

NetScaler opens a connection and forwards the request to the server
Source IP = SNIP
Destination IP = Server IP

NetScaler forwards the response to the client
Source IP = VIP
Destination IP = Client IP

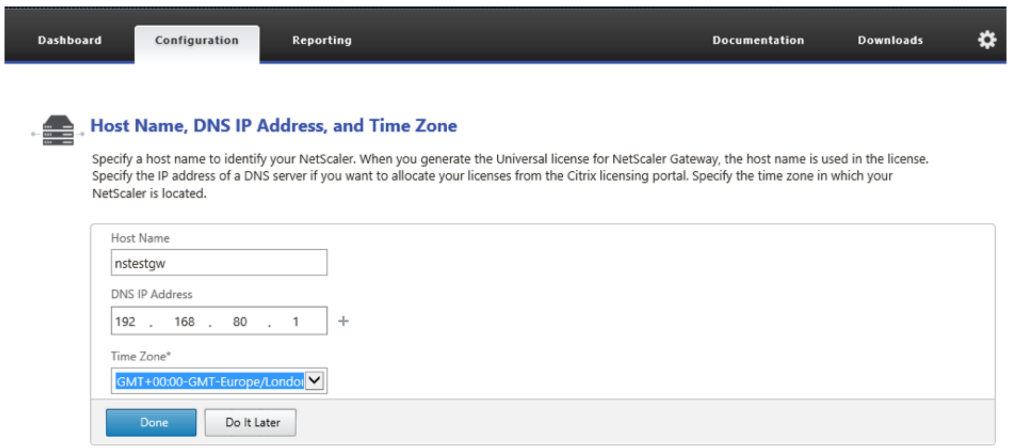
Server sends the response to NetScaler
Source IP = Server IP
Destination IP = SNIP

VIP = Virtual IP address
SNIP = Subnet IP address

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

Netmask*: 255 . 255 . 255 . 0

Done | Do It Later



Host Name, DNS IP Address, and Time Zone

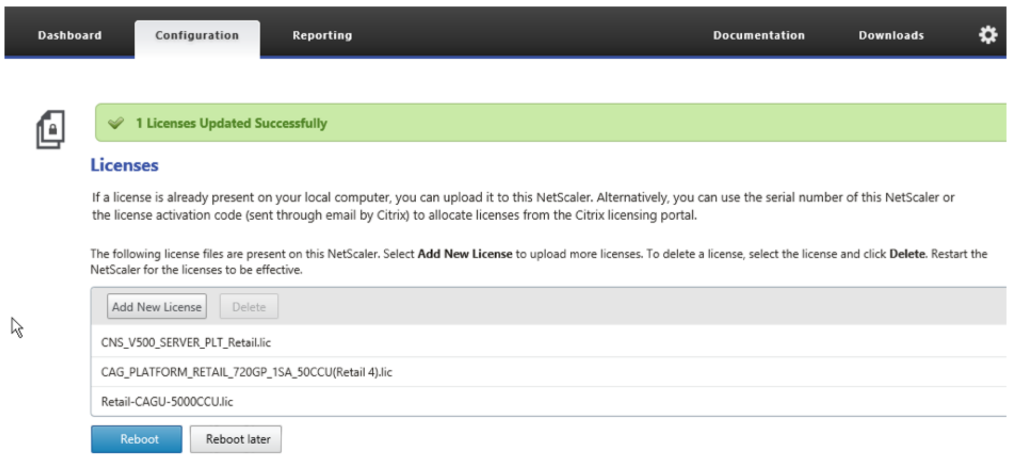
Specify a host name to identify your NetScaler. When you generate the Universal license for NetScaler Gateway, the host name is used in the license. Specify the IP address of a DNS server if you want to allocate your licenses from the Citrix licensing portal. Specify the time zone in which your NetScaler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

Host Name: nstestgw

DNS IP Address: 192 . 168 . 80 . 1

Time Zone*: GMT+00:00-GMT-Europe/Londoı

Done | Do It Later



1 Licenses Updated Successfully

Licenses

If a license is already present on your local computer, you can upload it to this NetScaler. Alternatively, you can use the serial number of this NetScaler or the license activation code (sent through email by Citrix) to allocate licenses from the Citrix licensing portal.

The following license files are present on this NetScaler. Select **Add New License** to upload more licenses. To delete a license, select the license and click **Delete**. Restart the NetScaler for the licenses to be effective.

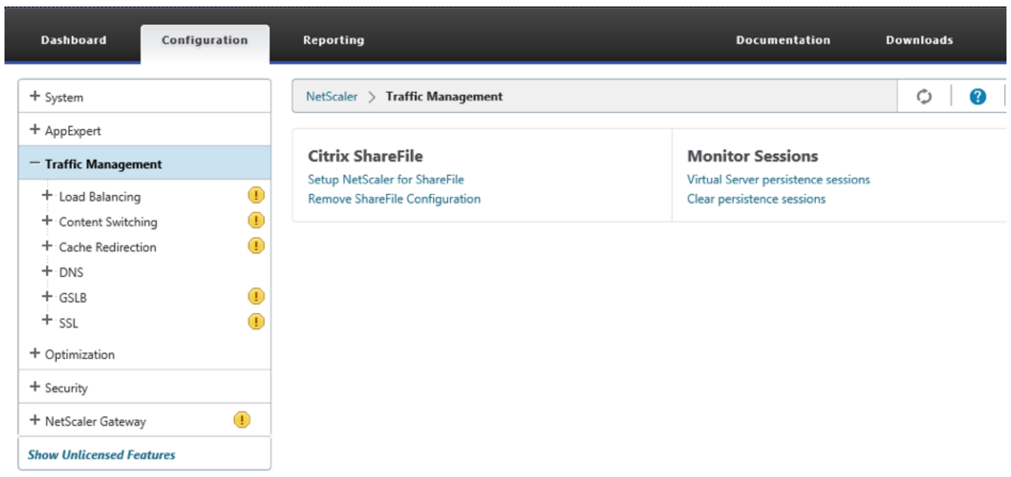
Add New License | Delete

CNS_V500_SERVER_PLT_Retail.lic
CAG_PLATFORM_RETAIL_720GP_1SA_50CCU(Retail 4).lic
Retail-CAGU-5000CCU.lic

Reboot | Reboot later

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

4. Click Reboot.

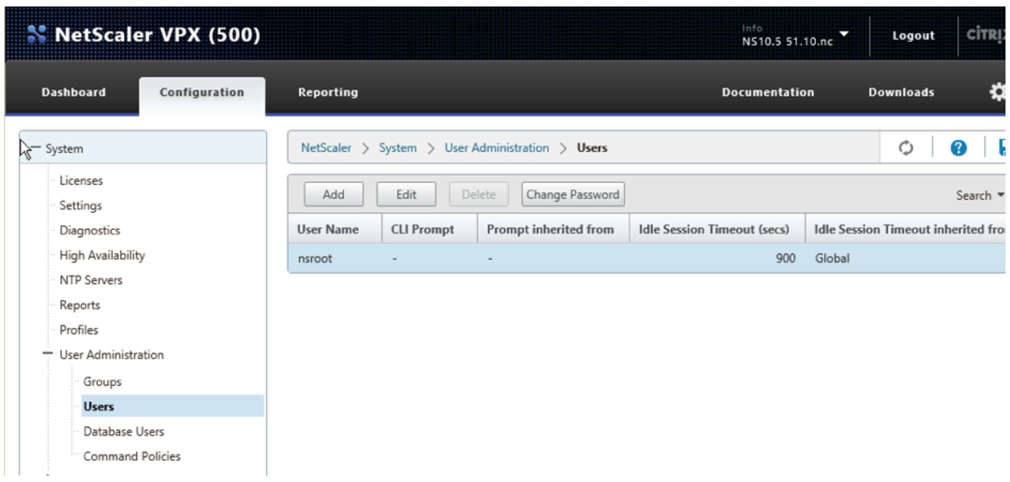


Citrix ShareFile
Setup NetScaler for ShareFile
Remove ShareFile Configuration

Monitor Sessions
Virtual Server persistence sessions
Clear persistence sessions

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**.



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

7. You might need to change the nsroot password.

Back to top

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.

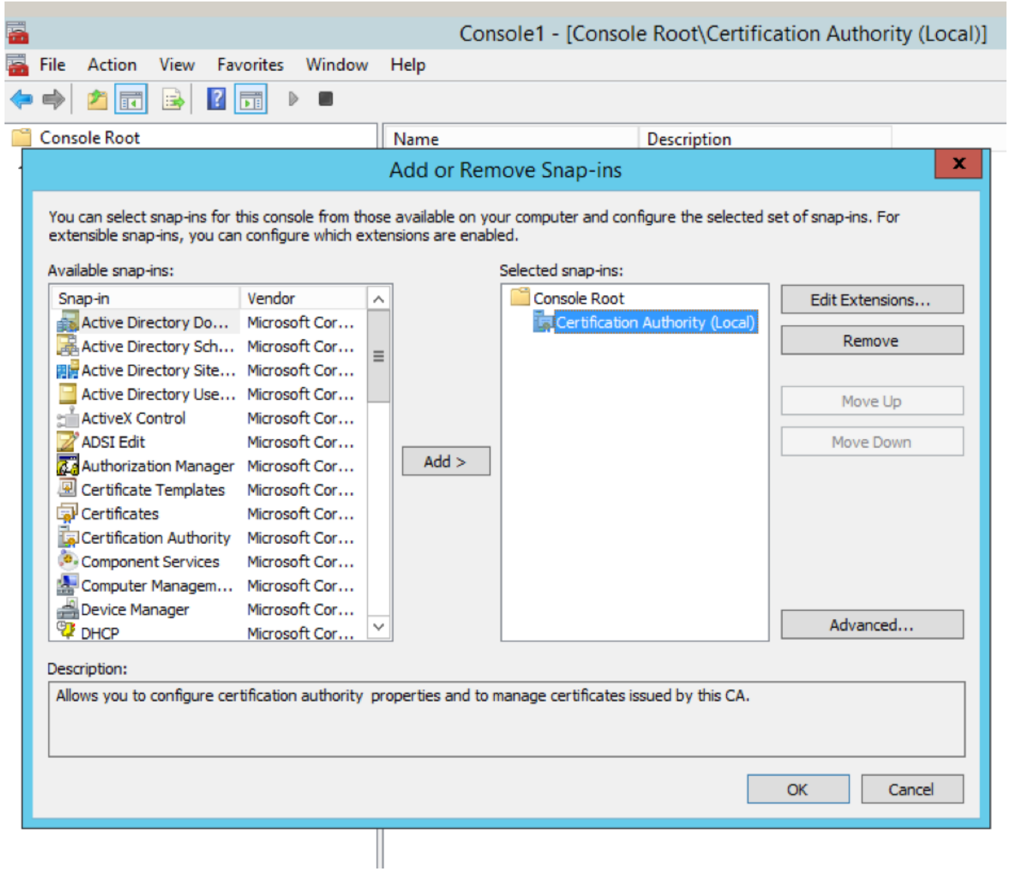
Because the Microsoft Certificate Server is known to Active Directory the trusted CA certificate is automatically installed on all domain-joined systems. The engineers then have to manually add the trusted CA certificate to non-domain-joined systems including domestic PCs, thin clients, tablets and smart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

Back to top

On the Microsoft Certificate Server

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



Console1 - [Console Root\Certification Authority (Local)]

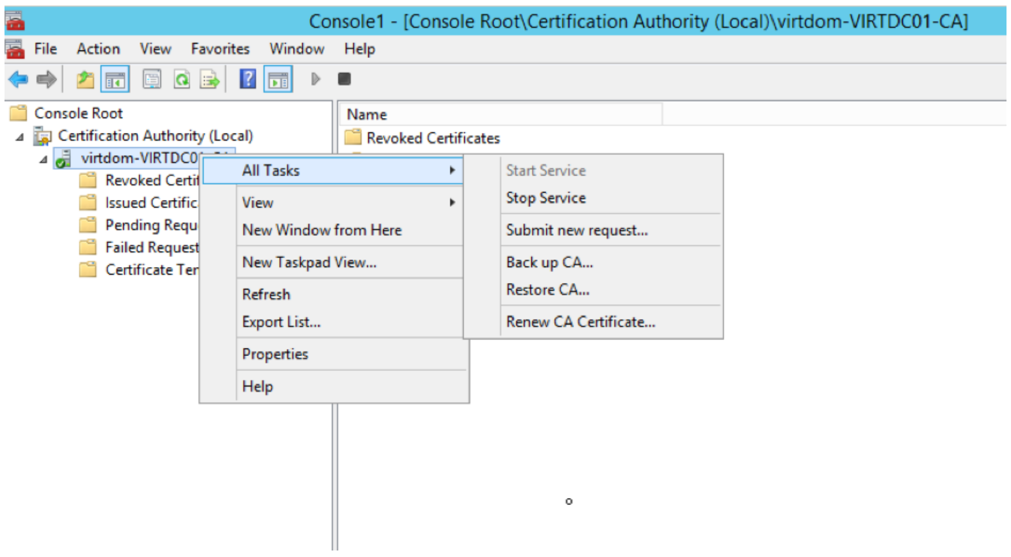
Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Sch...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
DHCP	Microsoft Cor...

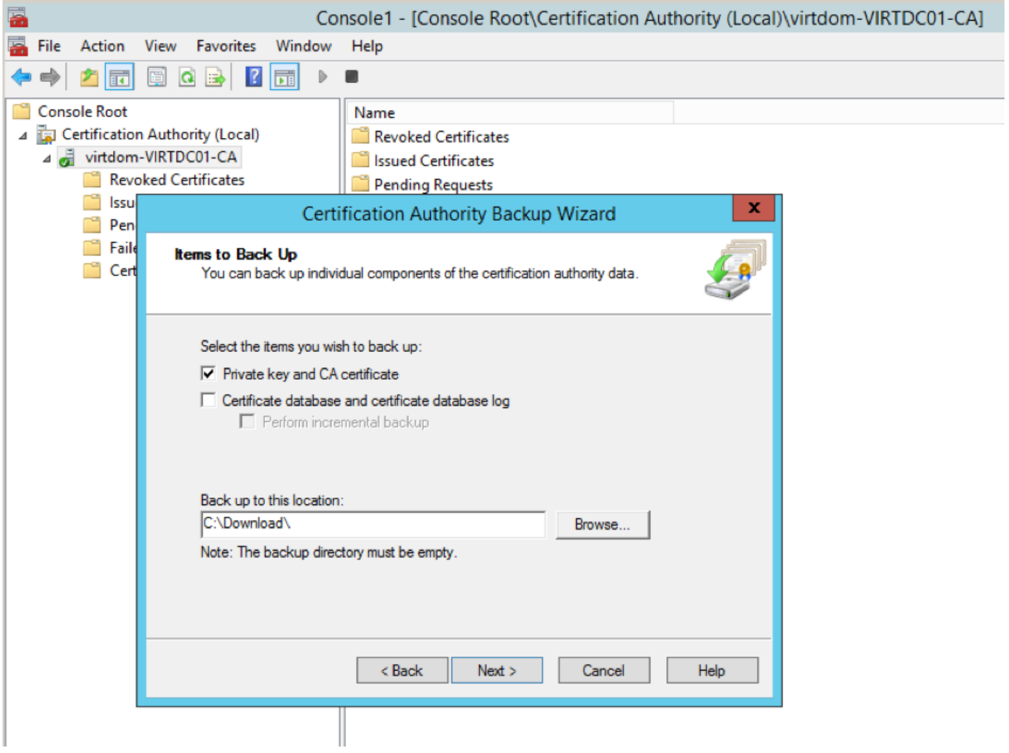
Selected snap-ins: Console Root / Certification Authority (Local)

Description: Allows you to configure certification authority properties and to manage certificates issued by this CA.



Console1 - [Console Root\Certification Authority (Local)\virtdom-VIRTDC01-CA]

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



Console1 - [Console Root\Certification Authority (Local)\virtdom-VIRTDC01-CA]

Certification Authority Backup Wizard

Items to Back Up
You can back up individual components of the certification authority data.

Select the items you wish to back up:

☑ Private key and CA certificate

☐ Certificate database and certificate database log

☐ Perform incremental backup

Back up to this location: C:\Download\

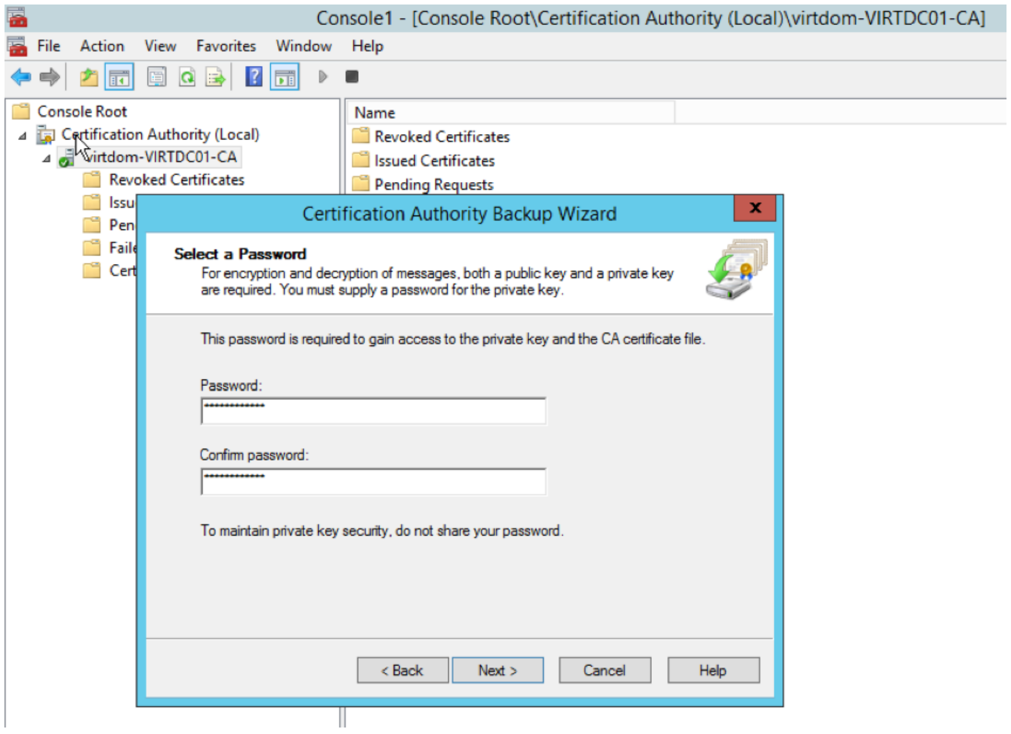
Note: The backup directory must be empty.

3. Back up the Private key and CA certificate to a convenient location.

4. Create a password.

5. Click **Next**.

6. Click **Finish**.



Console1 - [Console Root\Certification Authority (Local)\virtdom-VIRTDC01-CA]
File Action View Favorites Window Help
Console Root
Certification Authority (Local)
virtdom-VIRTDC01-CA
Revoked Certificates
Issu
Pen
Faile
Cert
Name
Revoked Certificates
Issued Certificates
Pending Requests

Certification Authority Backup Wizard

Select a Password

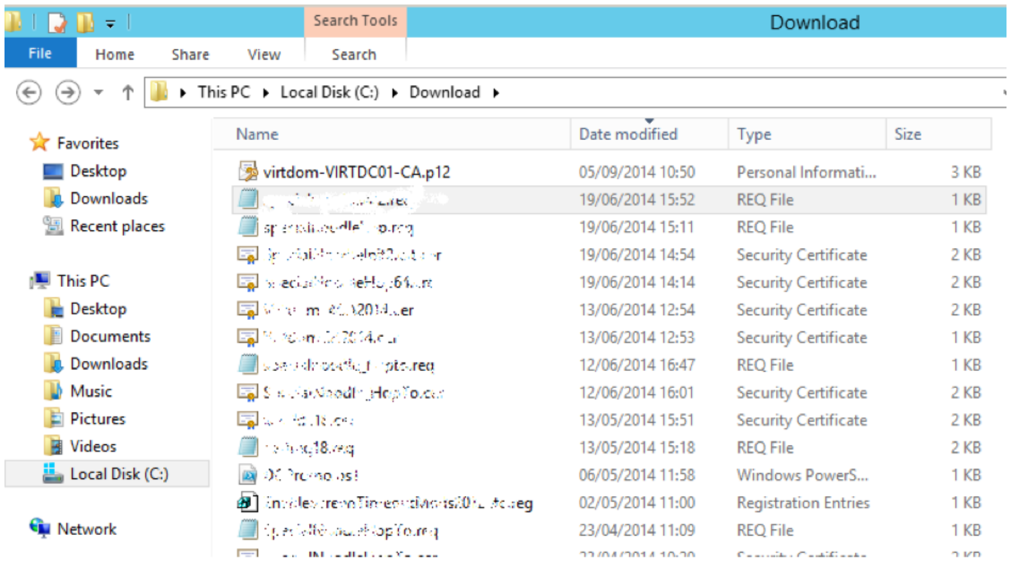
For encryption and decryption of messages, both a public key and a private key are required. You must supply a password for the private key.

This password is required to gain access to the private key and the CA certificate file.

Password: ••••••••••••

Confirm password: ••••••••••••

To maintain private key security, do not share your password.



Name	Date modified	Type	Size
virtdom-VIRTDC01-CA.p12	05/09/2014 10:50	Personal Informati...	3 KB
[illegible]	19/06/2014 15:52	REQ File	1 KB
[illegible]	19/06/2014 15:11	REQ File	1 KB
[illegible]	19/06/2014 14:54	Security Certificate	2 KB
[illegible]	19/06/2014 14:14	Security Certificate	2 KB
[illegible]	13/06/2014 12:54	Security Certificate	2 KB
[illegible]	13/06/2014 12:53	Security Certificate	1 KB
[illegible]	12/06/2014 16:47	REQ File	1 KB
[illegible]	12/06/2014 16:01	Security Certificate	2 KB
[illegible]	13/05/2014 15:51	Security Certificate	2 KB
[illegible]	13/05/2014 15:18	REQ File	2 KB
[illegible]	06/05/2014 11:58	Windows PowerS...	1 KB
[illegible]	02/05/2014 11:00	Registration Entries	1 KB
[illegible]	23/04/2014 11:09	REQ File	1 KB

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

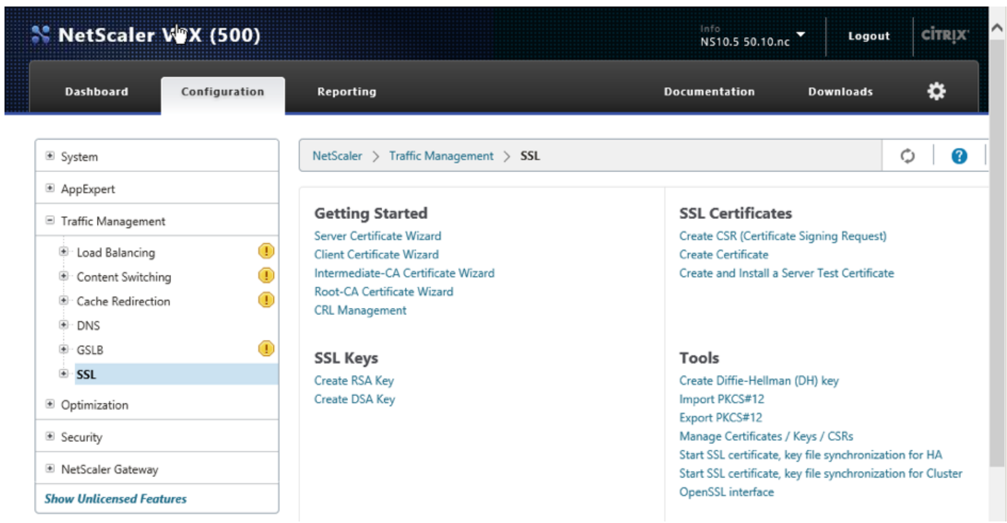
Back to top

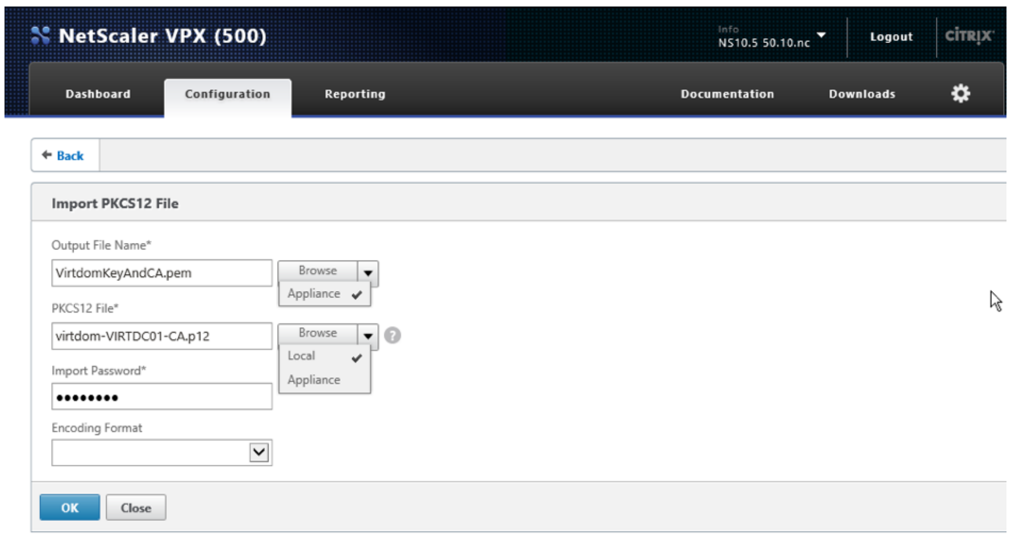
On the NetScaler GUI

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

Call or Chat

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


NetScaler VPX (500)
Info NS10.5 50.10.nc
Logout
CITRIX
Dashboard
Configuration
Reporting
Documentation
Downloads
System
AppExpert
Traffic Management
Load Balancing
Content Switching
Cache Redirection
DNS
GSLB
SSL
Optimization
Security
NetScaler Gateway
Show Unlicensed Features
NetScaler > Traffic Management > SSL
Getting Started
Server Certificate Wizard
Client Certificate Wizard
Intermediate-CA Certificate Wizard
Root-CA Certificate Wizard
CRL Management
SSL Keys
Create RSA Key
Create DSA Key
SSL Certificates
Create CSR (Certificate Signing Request)
Create Certificate
Create and Install a Server Test Certificate
Tools
Create Diffie-Hellman (DH) key
Import PKCS#12
Export PKCS#12
Manage Certificates / Keys / CSRs
Start SSL certificate, key file synchronization for HA
Start SSL certificate, key file synchronization for Cluster
OpenSSL interface



Import PKCS12 File

Output File Name* VirtdomKeyAndCA.pem

PKCS12 File* virtdom-VIRTDC01-CA.p12

Import Password* ••••••••

Encoding Format

2. 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

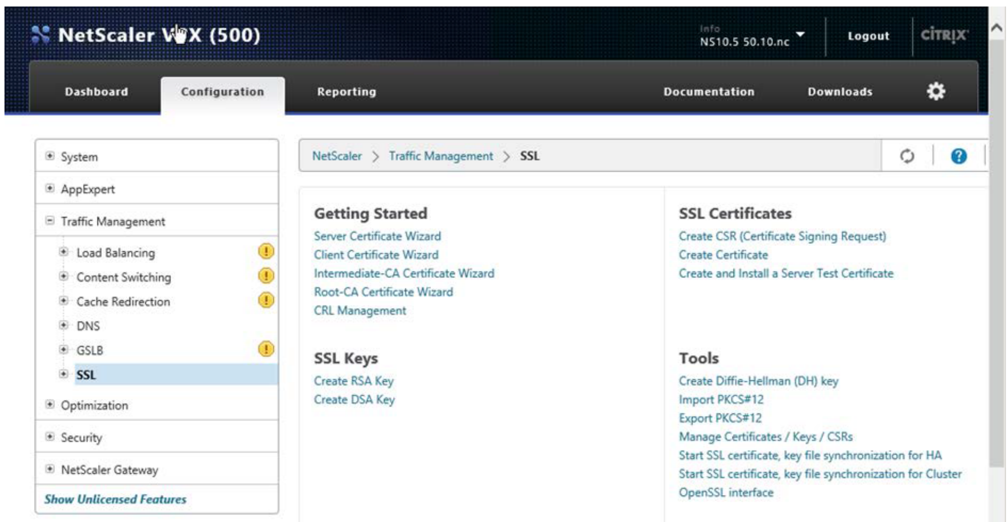
Notes:

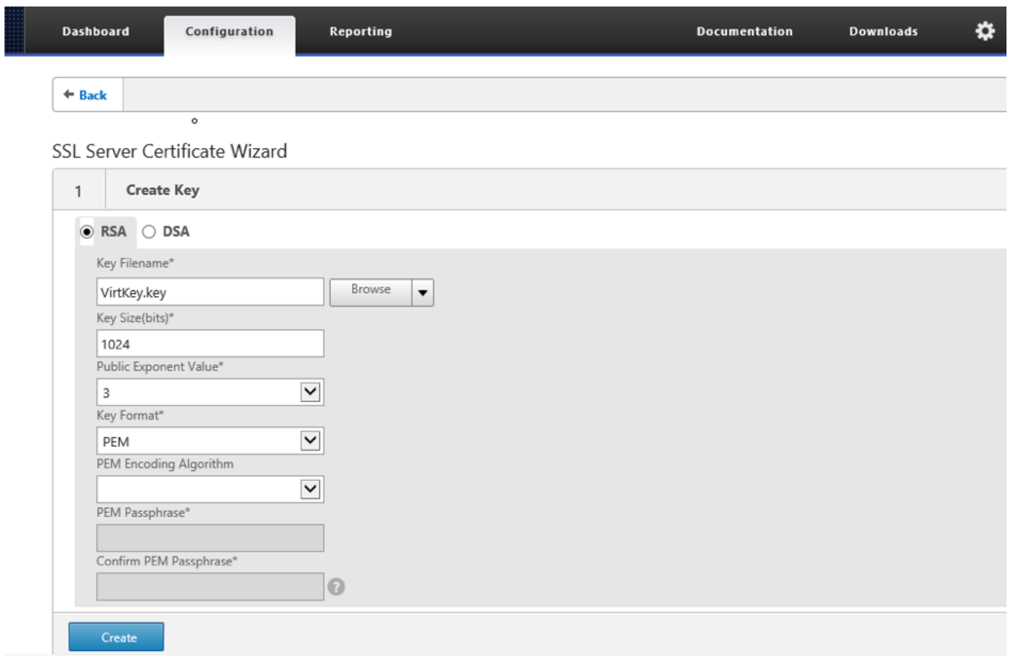
Create the server certificate

To create the server certificate, complete the following steps:

- 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.

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


NetScaler VPX (500)
Info NS10.5 50.10.nc
Logout
CITRIX
Dashboard
Configuration
Reporting
Documentation
Downloads
System
AppExpert
Traffic Management
Load Balancing
Content Switching
Cache Redirection
DNS
GSLB
SSL
Optimization
Security
NetScaler Gateway
Show Unlicensed Features
NetScaler > Traffic Management > SSL
Getting Started
Server Certificate Wizard
Client Certificate Wizard
Intermediate-CA Certificate Wizard
Root-CA Certificate Wizard
CRL Management
SSL Keys
Create RSA Key
Create DSA Key
SSL Certificates
Create CSR (Certificate Signing Request)
Create Certificate
Create and Install a Server Test Certificate
Tools
Create Diffie-Hellman (DH) key
Import PKCS#12
Export PKCS#12
Manage Certificates / Keys / CSRs
Start SSL certificate, key file synchronization for HA
Start SSL certificate, key file synchronization for Cluster
OpenSSL interface



SSL Server Certificate Wizard

1 Create Key

● RSA ○ DSA

Key Filename*: VirtKey.key

Key Size(bits)*: 1024

Public Exponent Value*: 3

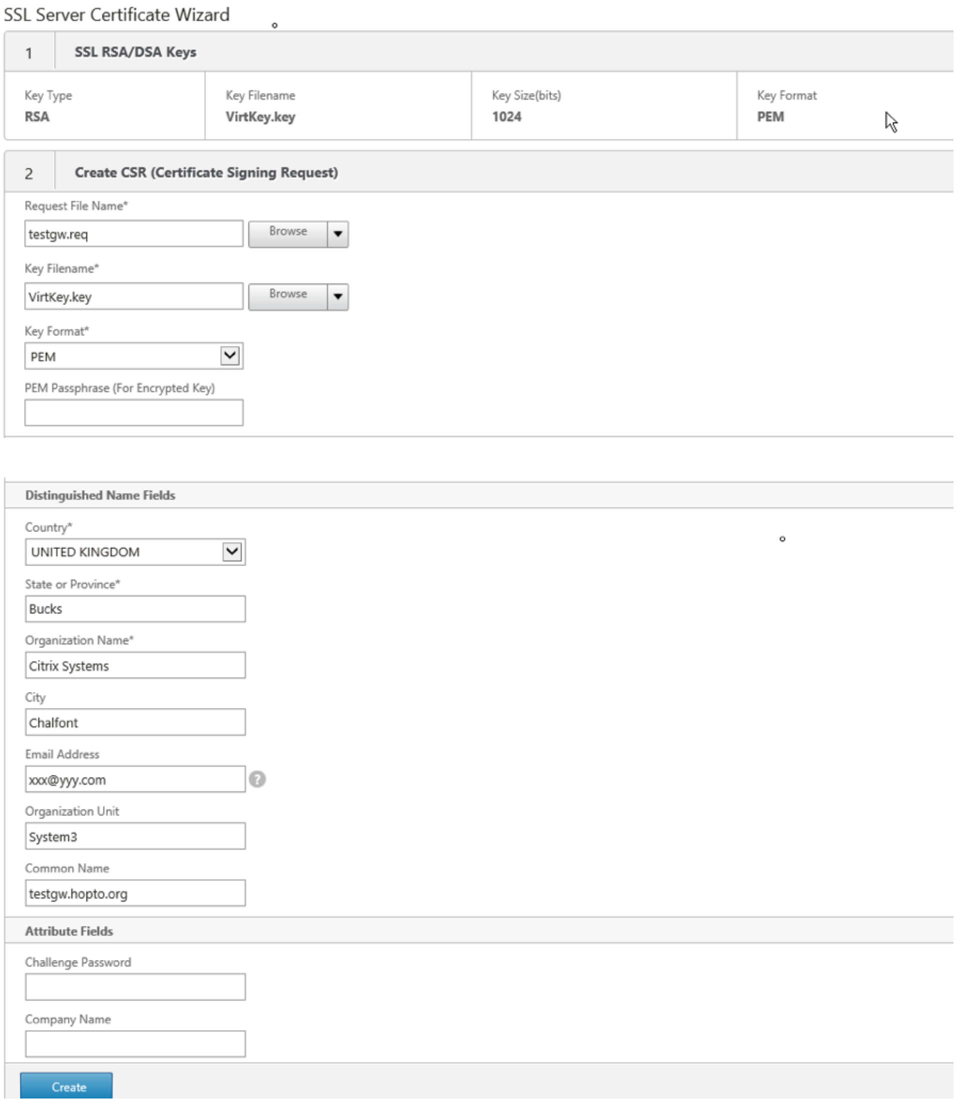
Key Format*: PEM

PEM Encoding Algorithm:

PEM Passphrase*:

Confirm PEM Passphrase*:

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



SSL Server Certificate Wizard

1 SSL RSA/DSA Keys

Key Type	Key Filename	Key Size(bits)	Key Format
RSA	VirtKey.key	1024	PEM

2 Create CSR (Certificate Signing Request)

Request File Name*: testgw.req

Key Filename*: VirtKey.key

Key Format*: PEM

PEM Passphrase (For Encrypted Key):

Distinguished Name Fields

Country*: UNITED KINGDOM

State or Province*: Bucks

Organization Name*: Citrix Systems

City: Chalfont

Email Address: xxx@yyy.com

Organization Unit: System3

Common Name: testgw.hopto.org

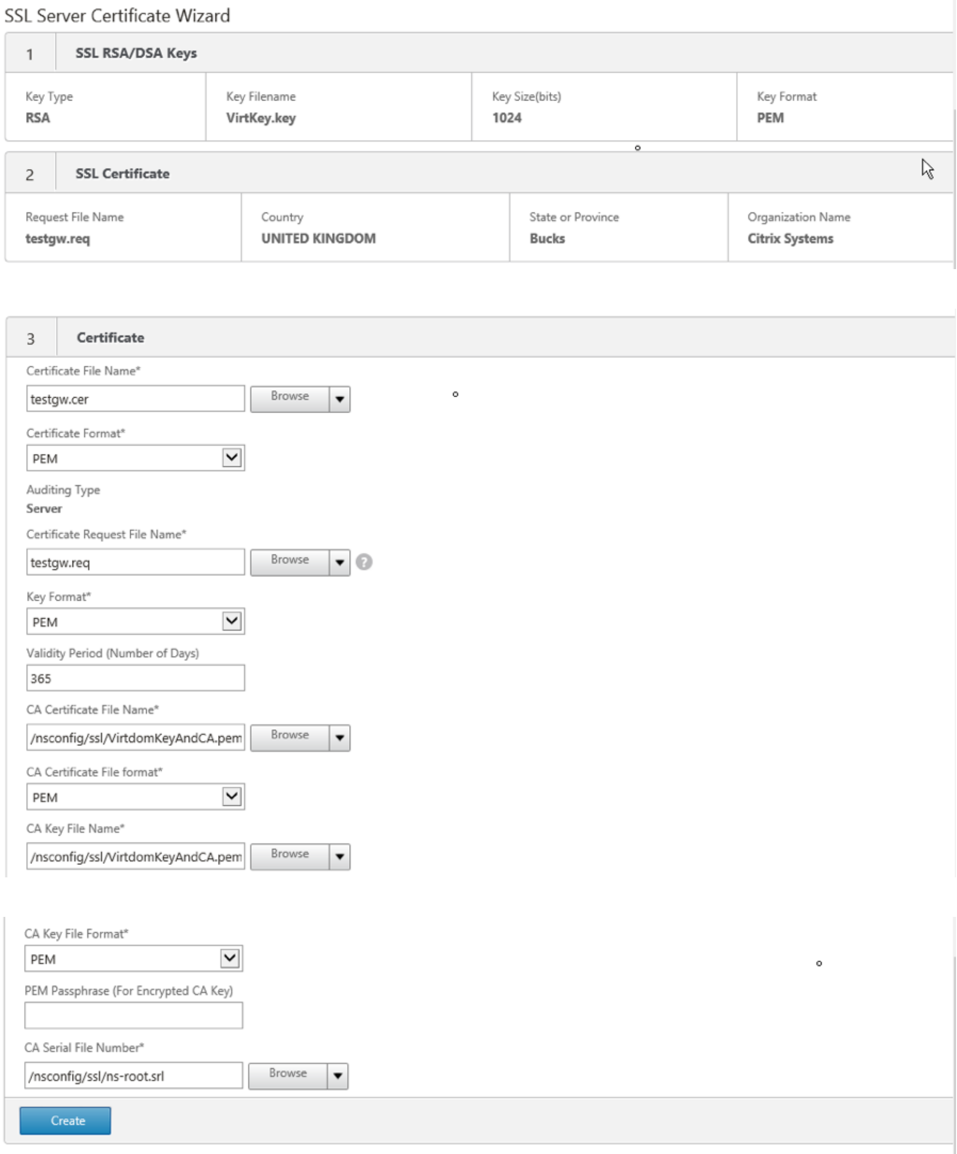
Attribute Fields

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.

Call or Chat



SSL Server Certificate Wizard

1 SSL RSA/DSA Keys

Key Type: RSA
Key Filename: VirtKey.key
Key Size(bits): 1024
Key Format: PEM

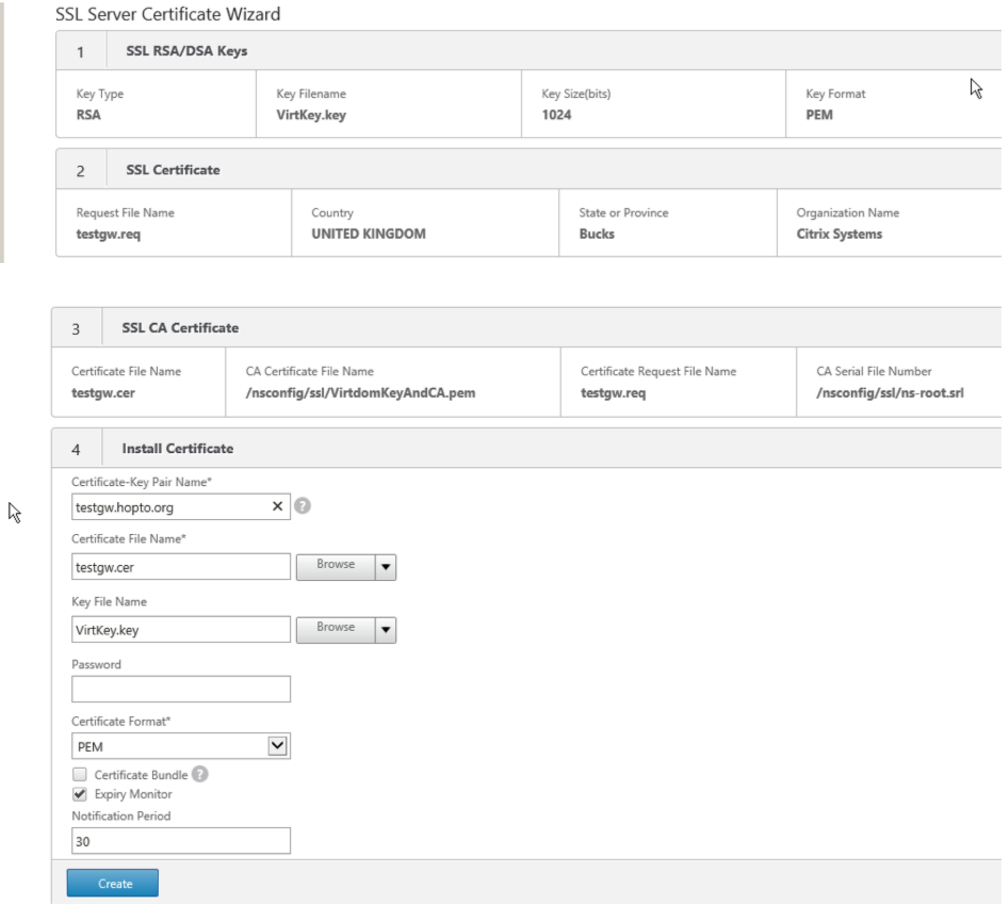
2 SSL Certificate

Request File Name: testgw.req
Country: UNITED KINGDOM
State or Province: Bucks
Organization Name: Citrix Systems

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: RSA
Key Filename: VirtKey.key
Key Size(bits): 1024
Key Format: PEM

2 SSL Certificate

Request File Name: testgw.req
Country: UNITED KINGDOM
State or Province: Bucks
Organization Name: Citrix Systems

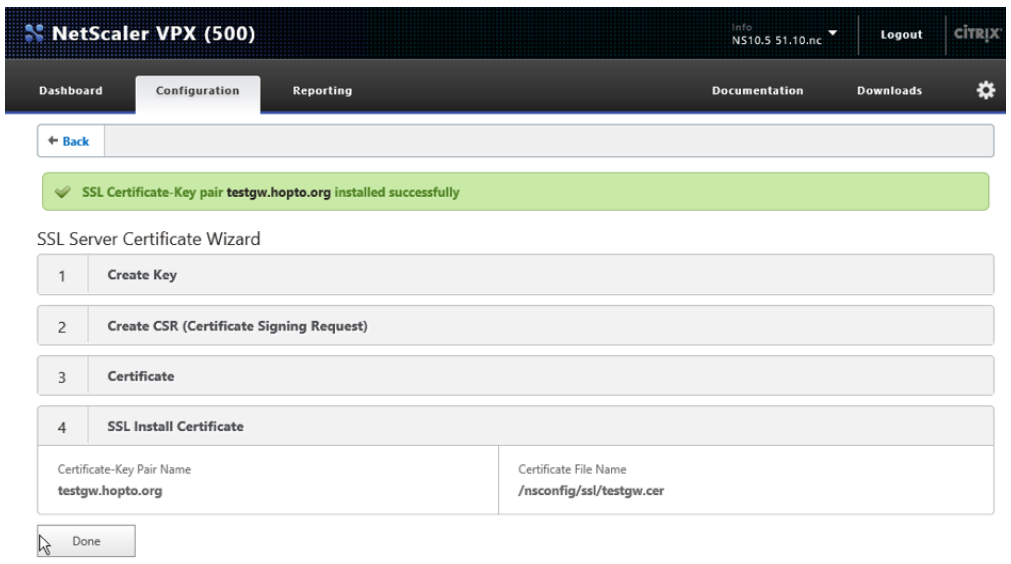
3 SSL CA Certificate

Certificate File Name: testgw.cer
CA Certificate File Name: /nsconfig/ssl/VirtdomKeyAndCA.pem
Certificate Request File Name: testgw.req
CA Serial File Number: /nsconfig/ssl/ns-root.srl

4 Install Certificate

Certificate-Key Pair Name*: testgw.hopto.org
Certificate File Name*: testgw.cer
Key File Name: VirtKey.key
Password:
Certificate Format*: PEM
☐ Certificate Bundle
☑ Expiry Monitor
Notification Period: 30

5. 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**.



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: testgw.hopto.org
Certificate File Name: /nsconfig/ssl/testgw.cer

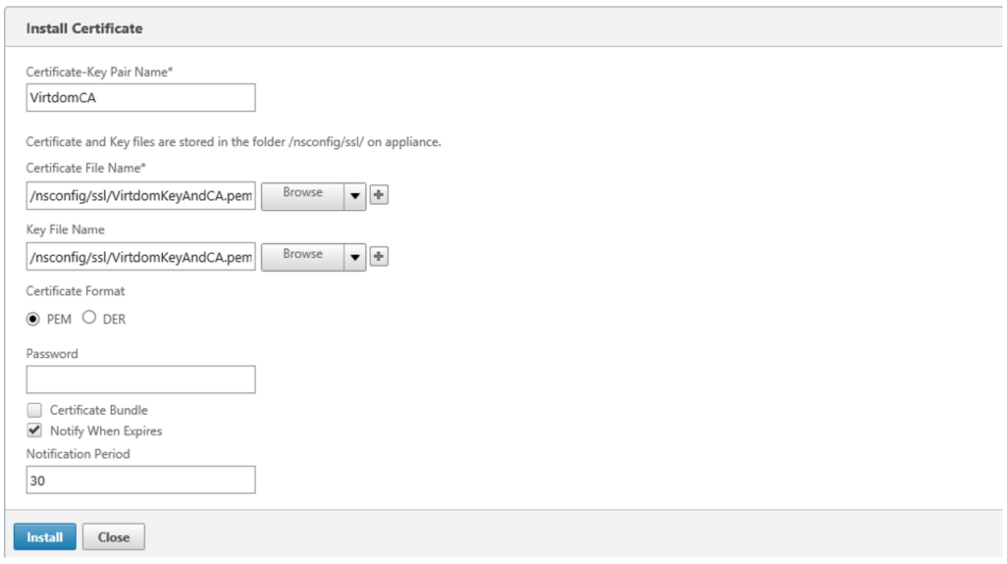
6. All the steps are complete and click **Done**. (**Optional**) **Install the CA certificate**

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

1. 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*: VirtdomCA

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

Certificate File Name*: /nsconfig/ssl/VirtdomKeyAndCA.pem

Key File Name: /nsconfig/ssl/VirtdomKeyAndCA.pem

Certificate Format: ● PEM ○ DER

Password:

□ Certificate Bundle

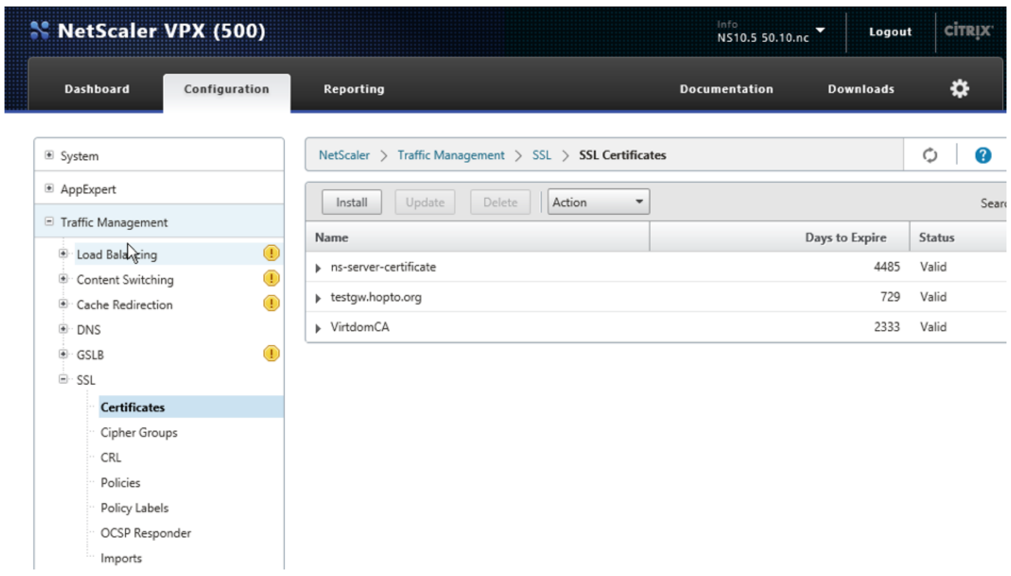
☑ Notify When Expires

Notification Period: 30

Review the installed certificates

1. Go to **Traffic Management** > **SSL** > **Certificates**.

2. Press the refresh icon.



NetScaler VPX (500)

NetScaler > Traffic Management > SSL > SSL Certificates

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

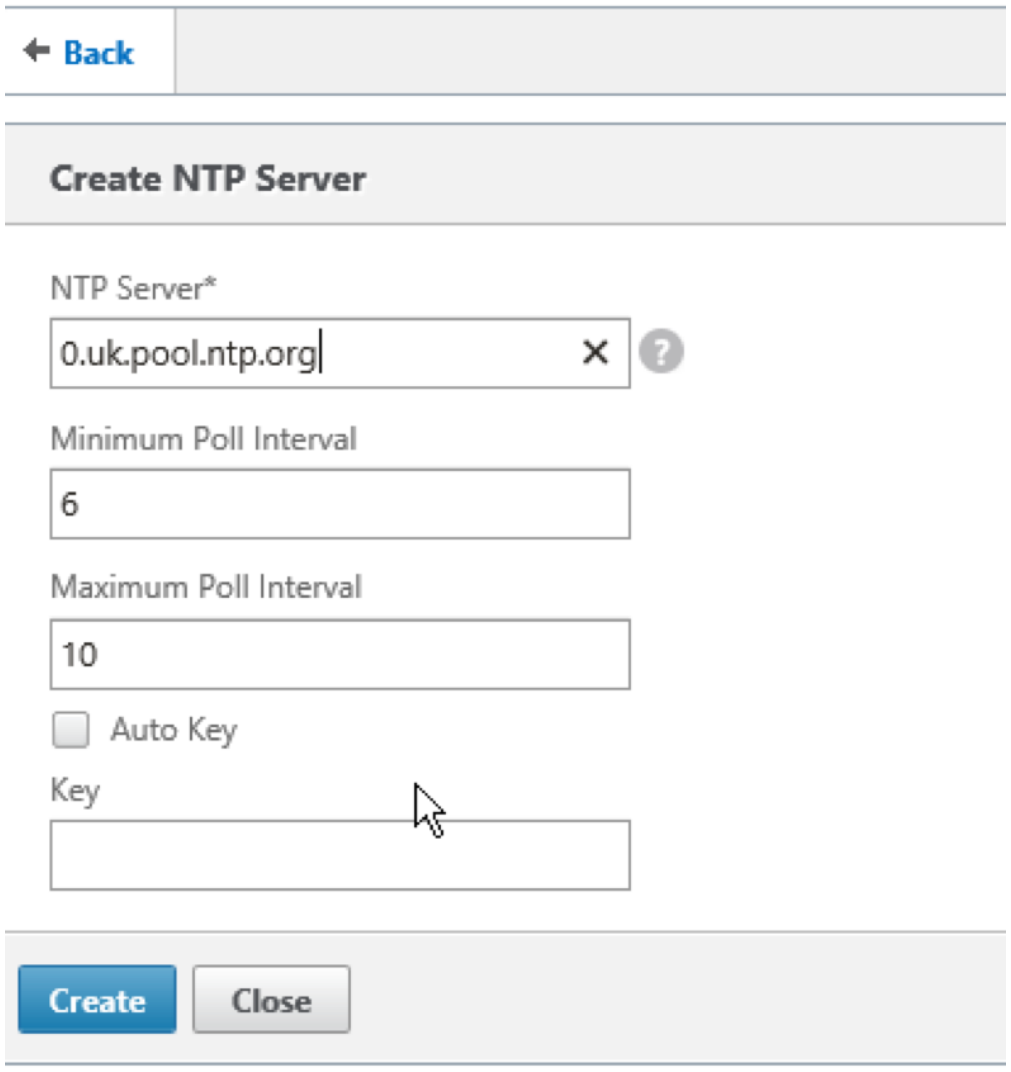
Back to top

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**.

Call or Chat



Create NTP Server

NTP Server*: 0.uk.pool.ntp.org

Minimum Poll Interval: 6

Maximum Poll Interval: 10

□ Auto Key

Key:

[Back to top](#)

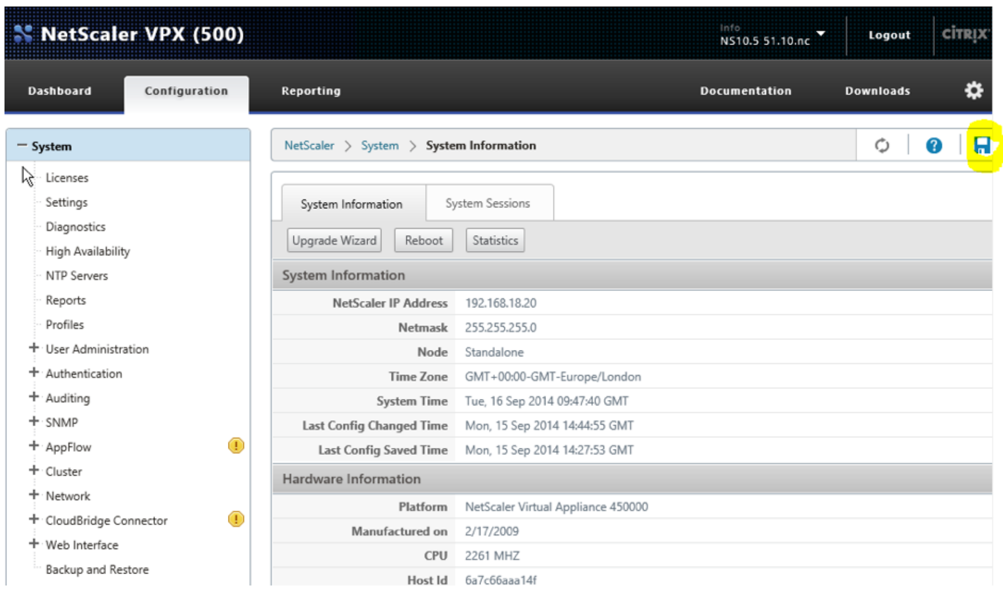
Backups - and why you might want one

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:

1. Accept the resulting configuration and move forward
2. Rerun parts of the wizard
3. Fall back to this point and start again

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



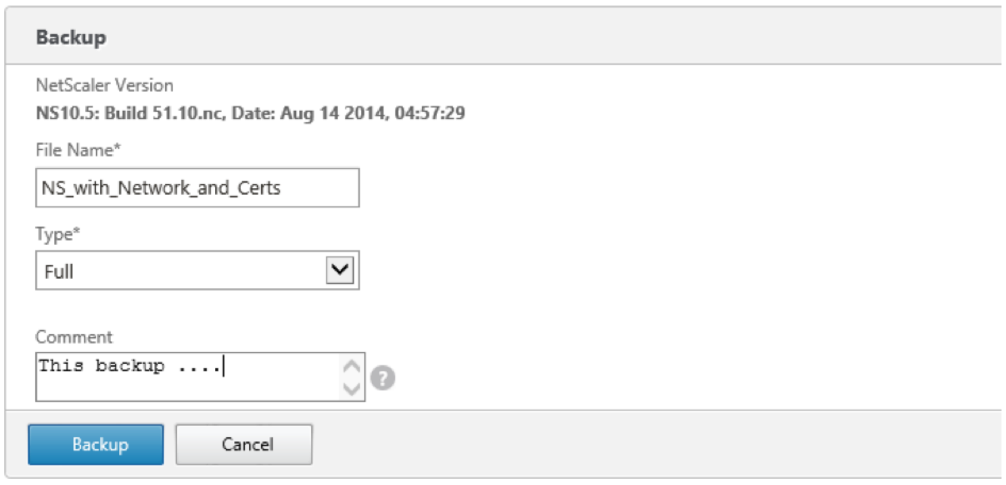
System Information

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

Hardware Information

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

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*: NS_with_Network_and_Certs

Type*: Full

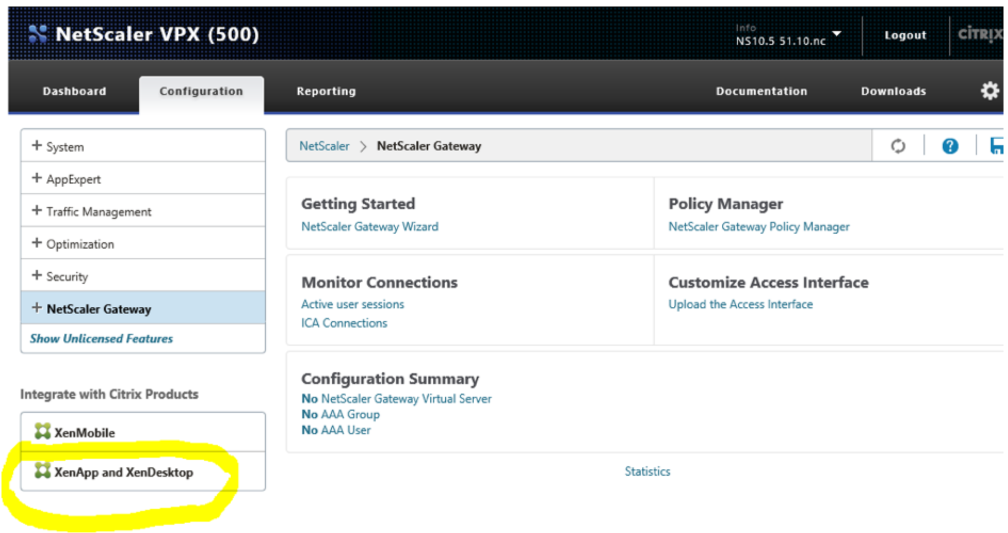
Comment: This backup ....

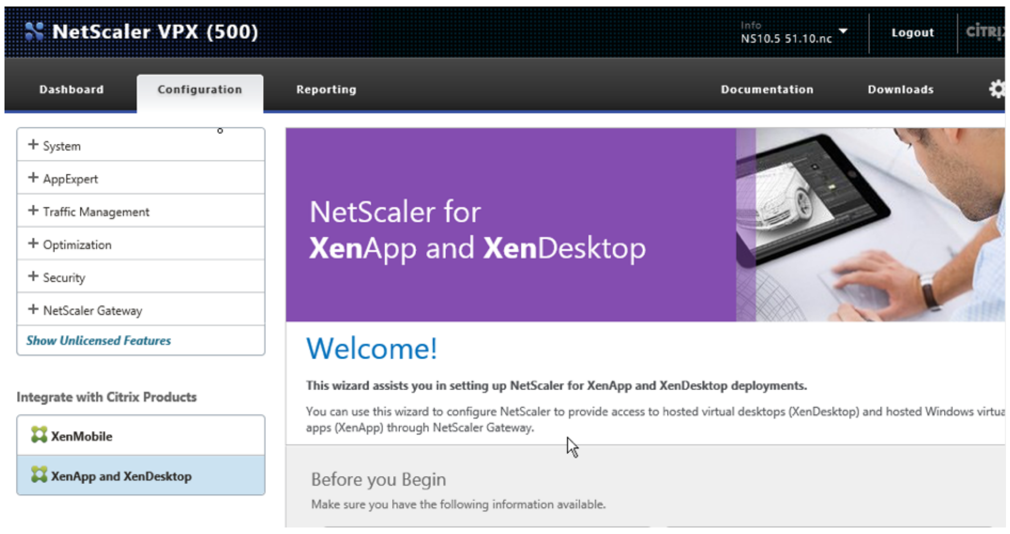
[Back to top](#)

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**.





Welcome!

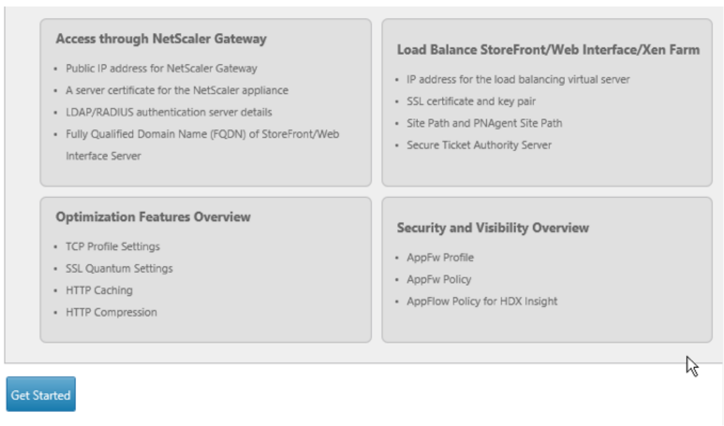
This wizard assists you in setting up NetScaler for XenApp and XenDesktop deployments.

You can use this wizard to configure NetScaler to provide access to hosted virtual desktops (XenDesktop) and hosted Windows virtua apps (XenApp) through NetScaler Gateway.

Before you Begin

Make sure you have the following information available.

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

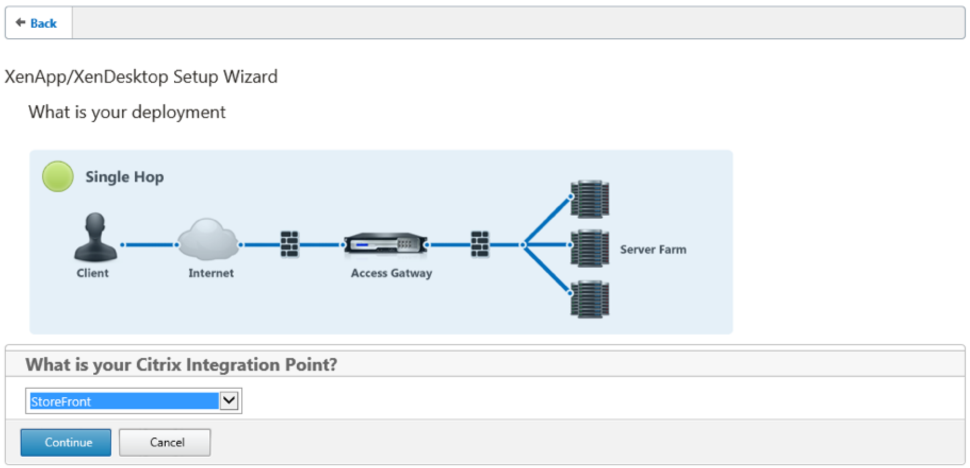
- IP address for the load balancing virtual server
- SSL certificate and key pair
- Site Path and PNAgent Site Path
- Secure Ticket Authority Server

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



XenApp/XenDesktop Setup Wizard

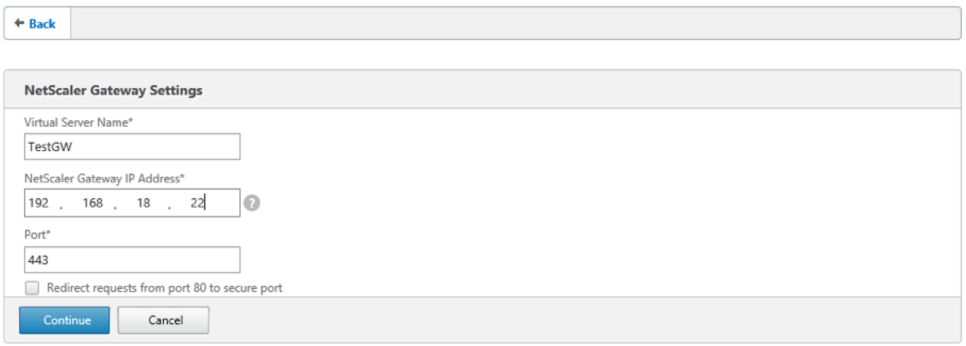
What is your deployment

What is your Citrix Integration Point?

StoreFront

3. Enter the IP for your NetScaler Gateway Virtual Server.

4. Click **Continue**.



NetScaler Gateway Settings

Virtual Server Name*: TestGW

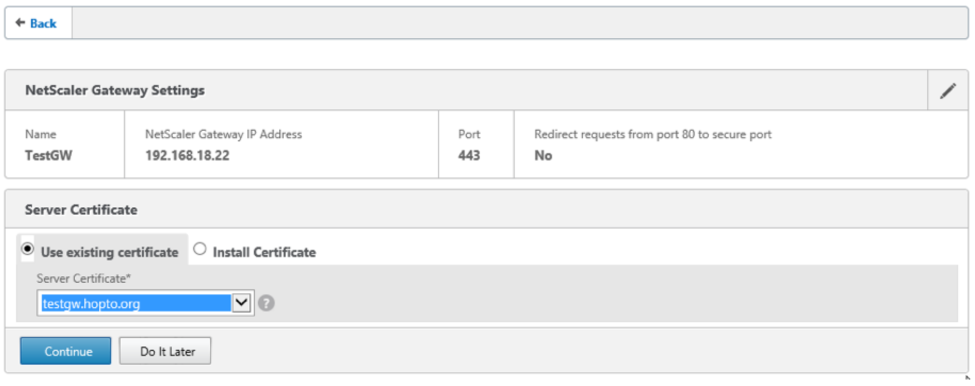
NetScaler Gateway IP Address*: 192 . 168 . 18 . 22

Port*: 443

□ Redirect requests from port 80 to secure port

5. Chose the Server Certificate created before.

6. Click **Continue**.



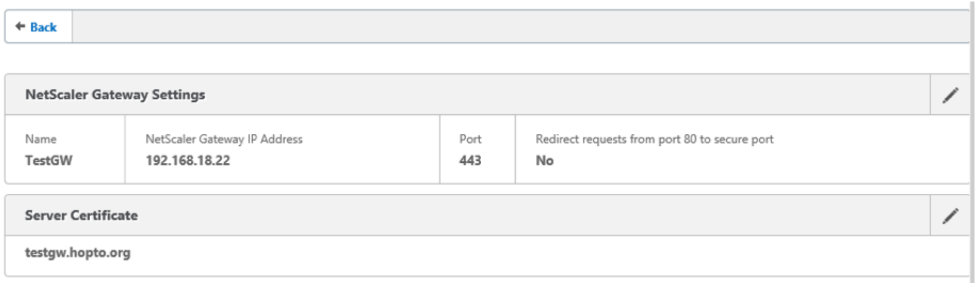
NetScaler Gateway Settings

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

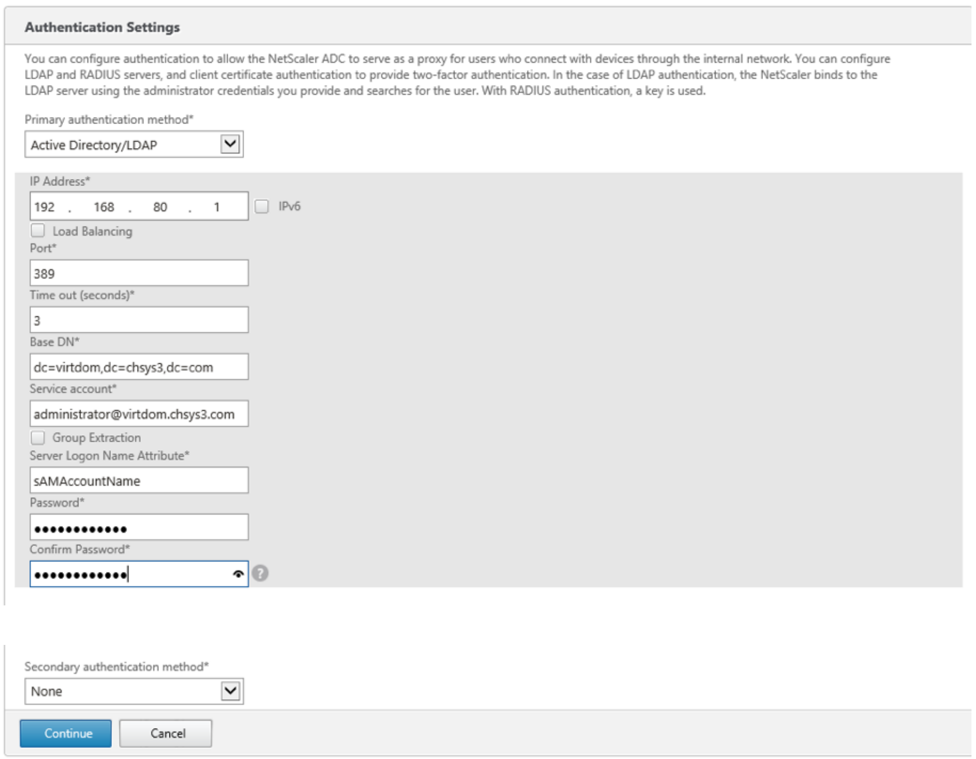


NetScaler Gateway Settings

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=virtdom,dc=chsys3,dc=com

Service account*: administrator@virtdom.chsys3.com

□ Group Extraction

Server Logon Name Attribute*: sAMAccountName

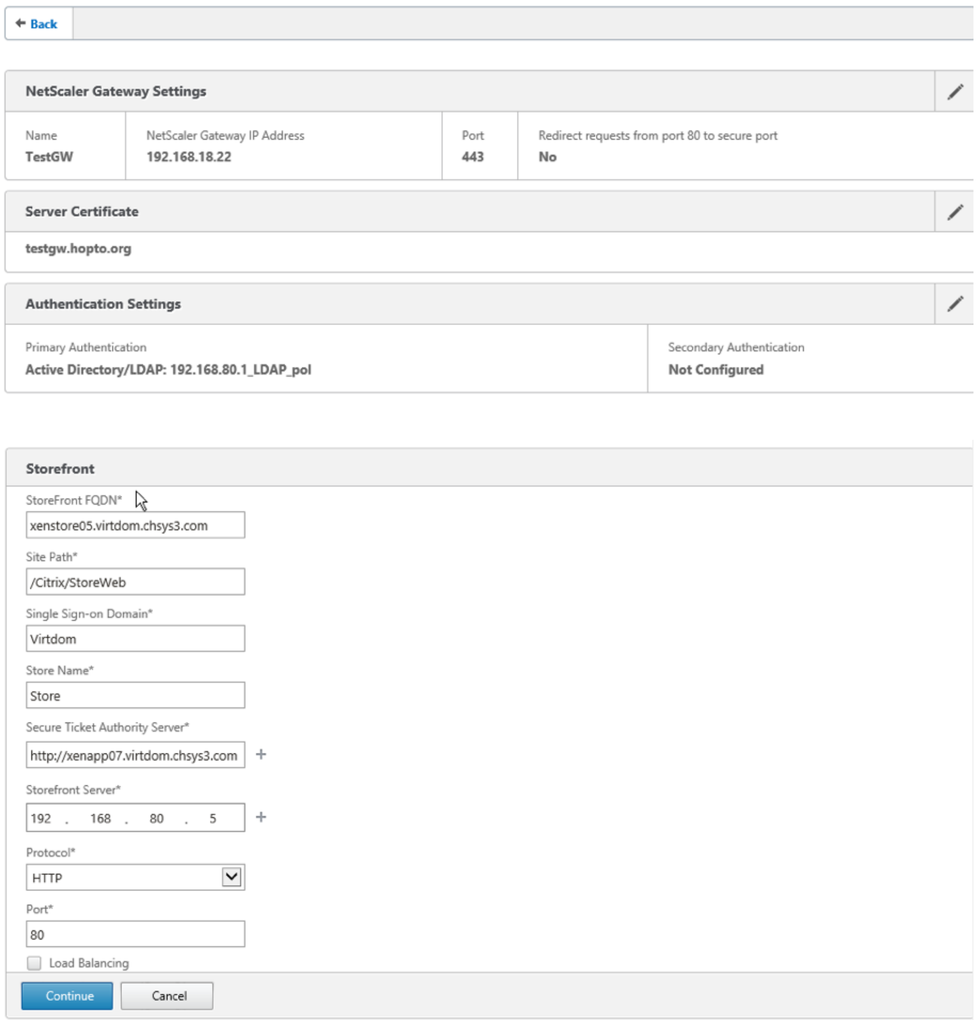
Password*: ••••••••••••

Confirm Password*: ••••••••••••

Secondary authentication method*: None

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**.



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.virtdom.chsys3.com

Site Path*: /Citrix/StoreWeb

Single Sign-on Domain*: Virtdom

Store Name*: Store

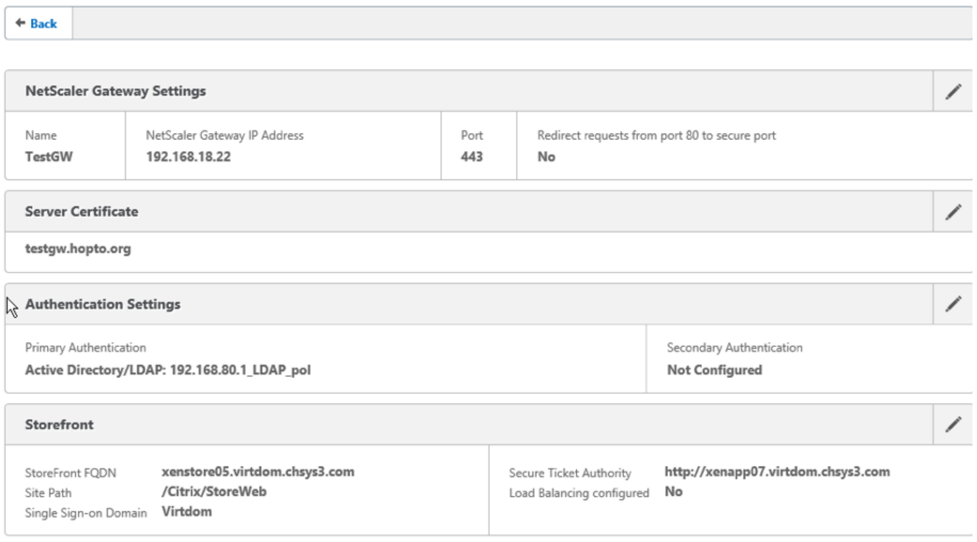
Secure Ticket Authority Server*: http://xenapp07.virtdom.chsys3.com +

Storefront Server*: 192 . 168 . 80 . 5 +

Protocol*: HTTP

Port*: 80

□ Load Balancing



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

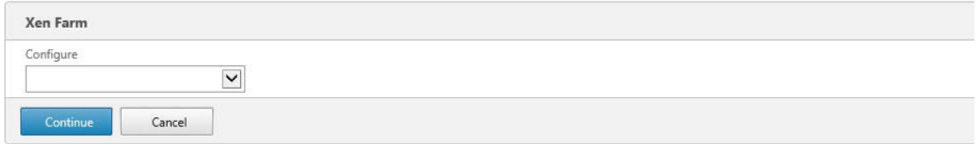
StoreFront FQDN	xenstore05.virtdom.chsys3.com	Secure Ticket Authority	http://xenapp07.virtdom.chsys3.com
Site Path	/Citrix/StoreWeb	Load Balancing configured	No
Single Sign-on Domain	Virtdom		

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.

Call or Chat

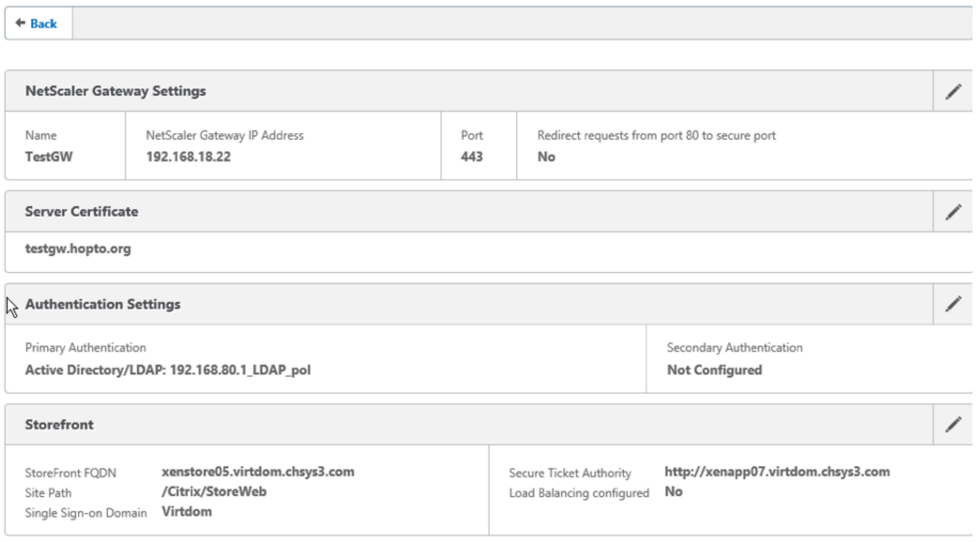
9. Click **Continue**.



Xen Farm

Configure

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

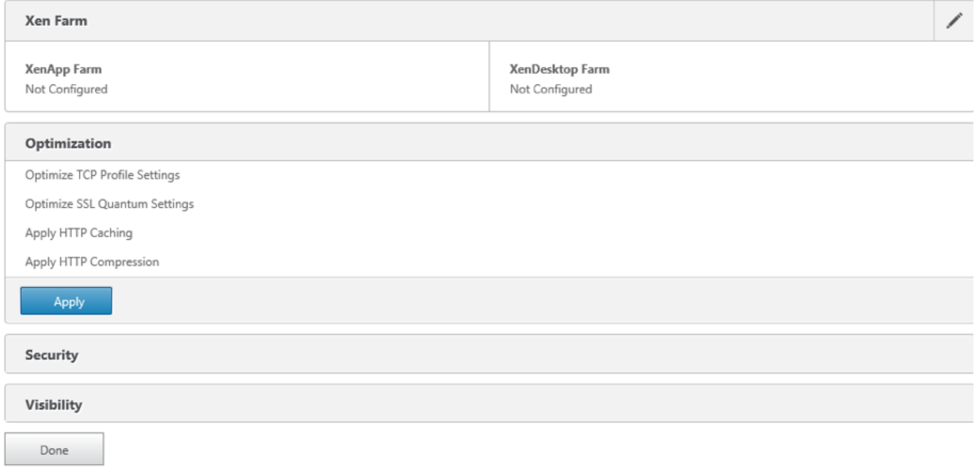
Storefront

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

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**.



Xen Farm

XenApp Farm	XenDesktop Farm
Not Configured	Not Configured

Optimization

Optimize TCP Profile Settings

Optimize SSL Quantum Settings

Apply HTTP Caching

Apply HTTP Compression

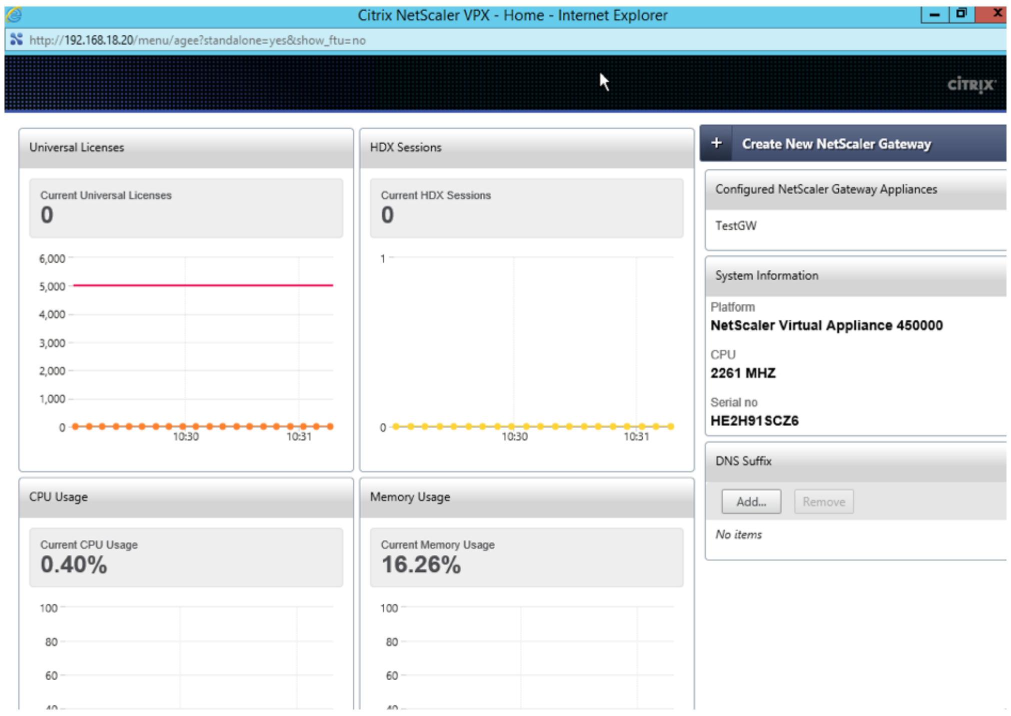
Apply

Security

Visibility

Done

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



Citrix NetScaler VPX - Home - Internet Explorer

http://192.168.18.20/menu/agee?standalone=yes&show_ftu=no

Universal Licenses

Current Universal Licenses: 0

HDX Sessions

Current HDX Sessions: 0

CPU Usage

Current CPU Usage: 0.40%

Memory Usage

Current Memory Usage: 16.26%

Create New NetScaler Gateway

Configured NetScaler Gateway Appliances

TestGW

System Information

Platform: NetScaler Virtual Appliance 450000

CPU: 2261 MHZ

Serial no: HE2H91SCZ6

DNS Suffix

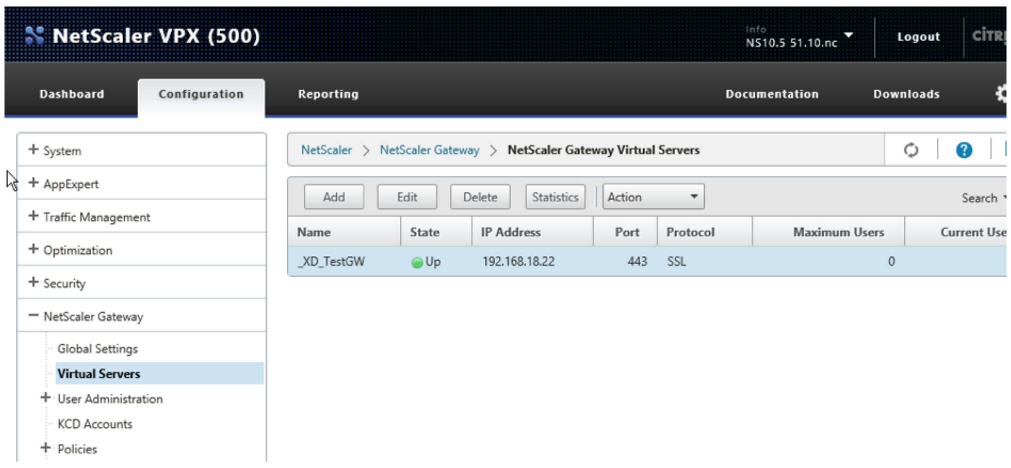
No items

(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.

Call or Chat

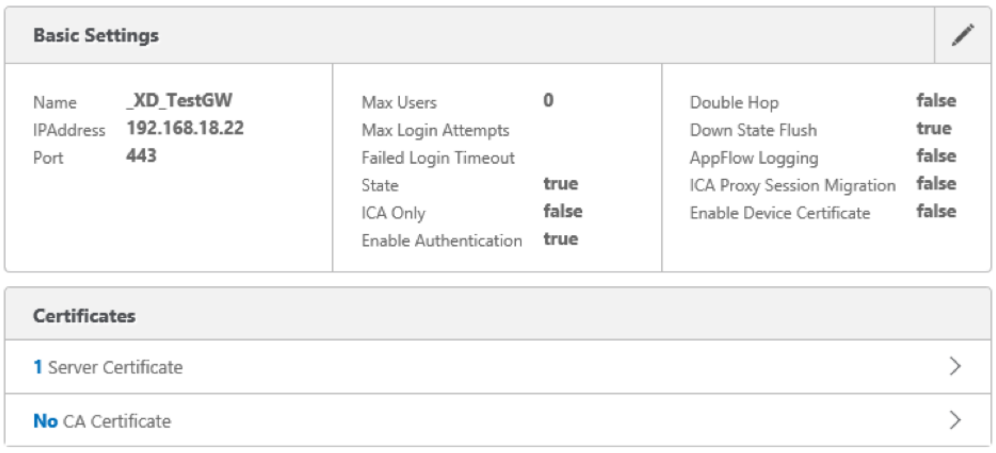
1. Go to **NetScaler** > **NetScaler Gateway** > **NetScaler Gateway Virtual Server**.



Name	State	IP Address	Port	Protocol	Maximum Users	Current Use
_XD_TestGW	Up	192.168.18.22	443	SSL	0	

2. Select **_TestGW** and click **Edit**.

3. Click **No CA Certificate**.

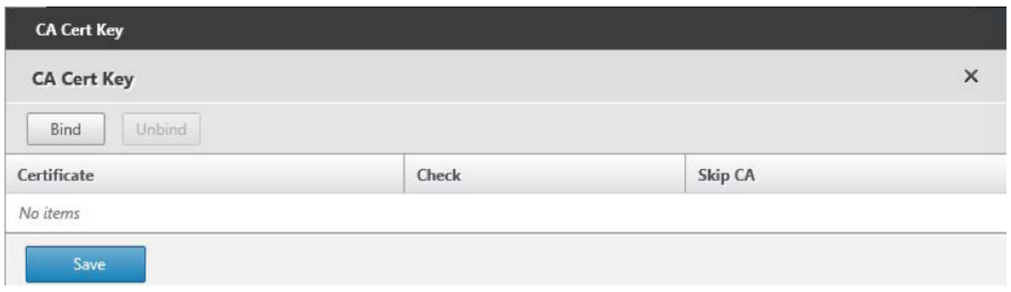


Name	_XD_TestGW	Max Users	0	Double Hop	false
IPAddress	192.168.18.22	Max Login Attempts		Down State Flush	true
Port	443	Failed Login Timeout		AppFlow Logging	false
		State	true	ICA Proxy Session Migration	false
		ICA Only	false	Enable Device Certificate	false
		Enable Authentication	true		

1 Server Certificate

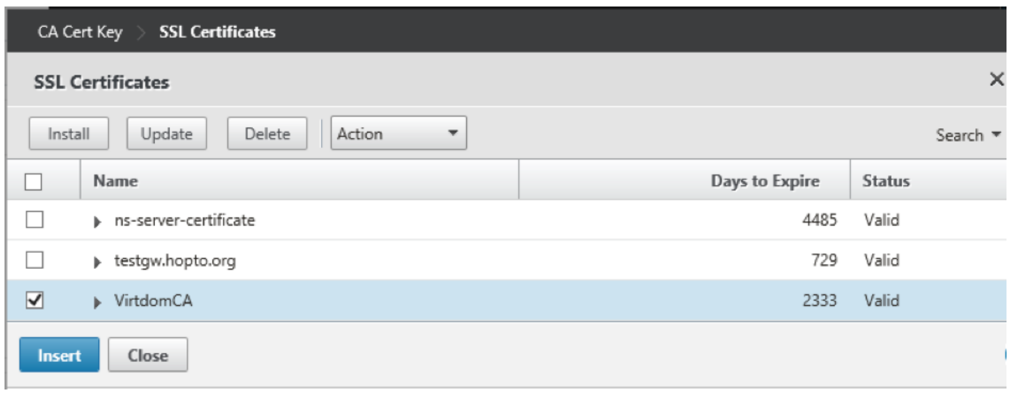
No CA Certificate

4. Click **Bind**.



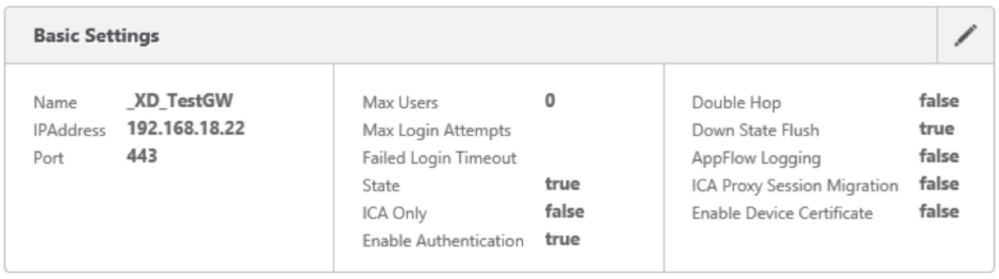
Certificate	Check	Skip CA
No items		

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



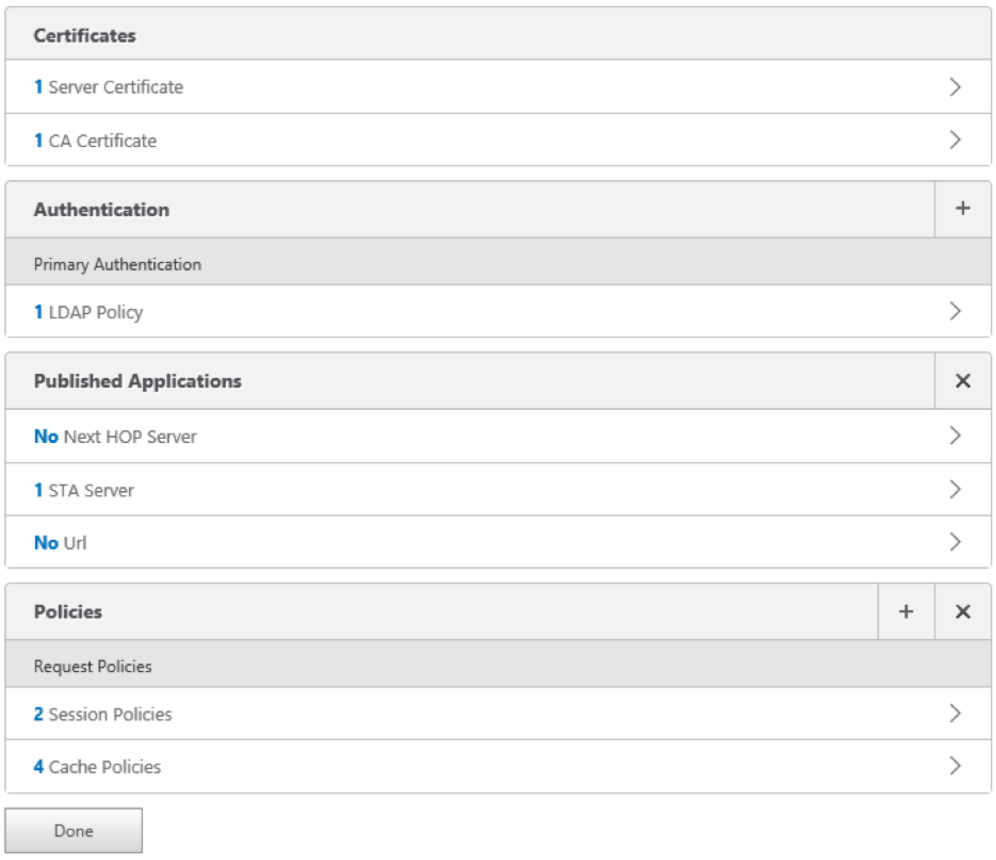
☐	Name	Days to Expire	Status
☐	ns-server-certificate	4485	Valid
☐	testgw.hopto.org	729	Valid
☑	VirtdomCA	2333	Valid

6. Click **Save**.



Name	_XD_TestGW	Max Users	0	Double Hop	false
IPAddress	192.168.18.22	Max Login Attempts		Down State Flush	true
Port	443	Failed Login Timeout		AppFlow Logging	false
		State	true	ICA Proxy Session Migration	false
		ICA Only	false	Enable Device Certificate	false
		Enable Authentication	true		

7. 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

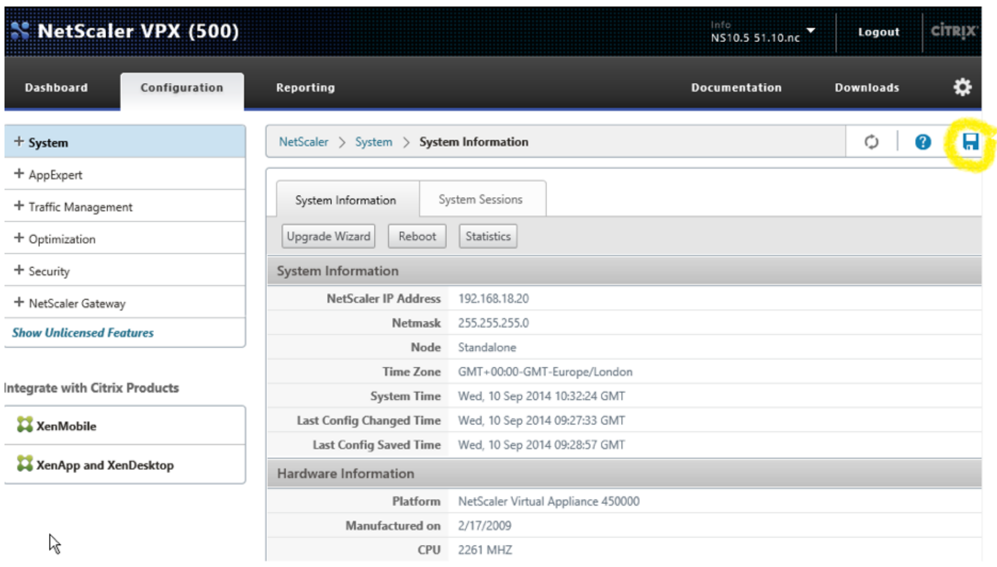
Policies

Request Policies

2 Session Policies

4 Cache Policies

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



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

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.

Back to top

StoreFront

DNS

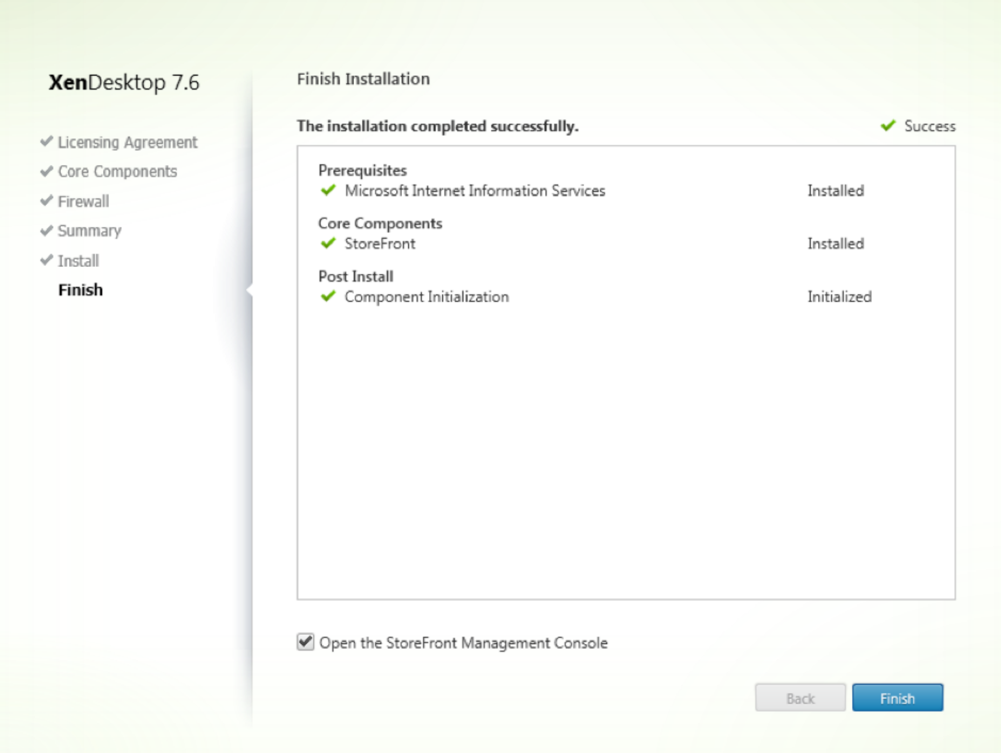
Check that the DNS entries for the NetScaler Gateway Virtual Server (testgw.hopto.org) point to the correct place.

- 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

Back to top

StoreFront – Configuring a new installation

1. Install StoreFront from your distribution media.



Finish Installation

The installation completed successfully. ✓ Success

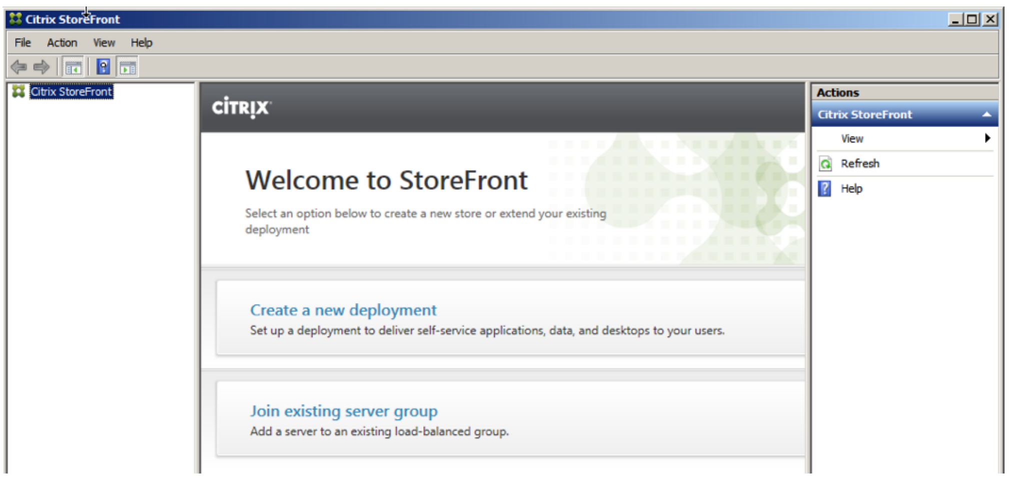
Prerequisites
✓ Microsoft Internet Information Services Installed

Core Components
✓ StoreFront Installed

Post Install
✓ Component Initialization Initialized

☑ Open the StoreFront Management Console

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



Welcome to StoreFront

Select an option below to create a new store or extend your existing deployment

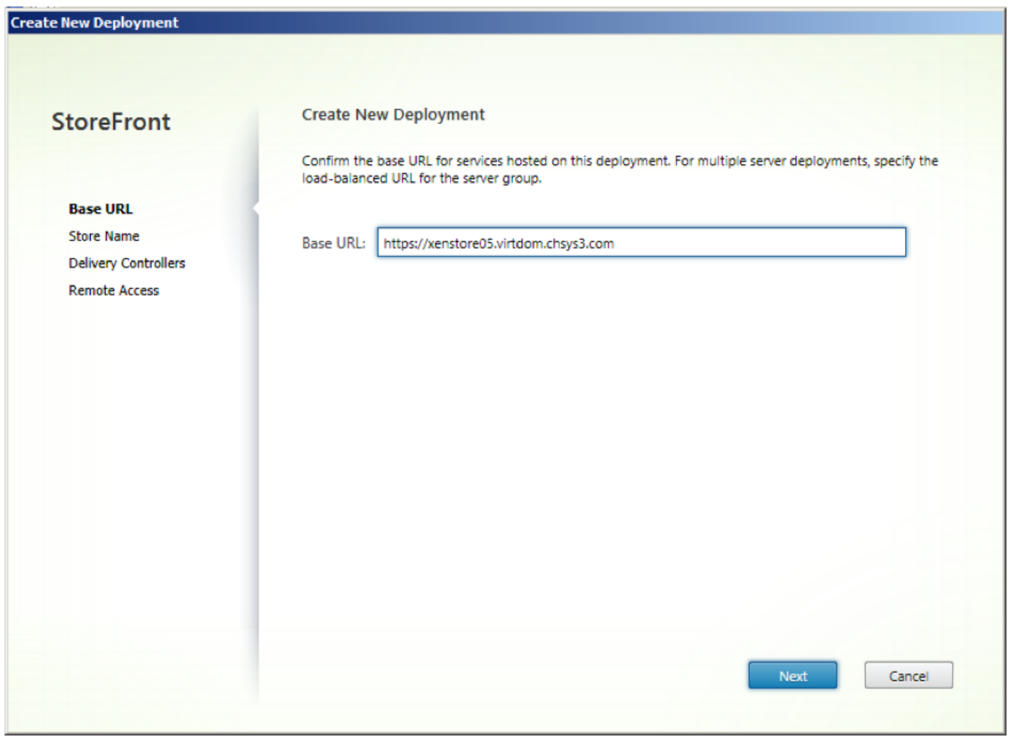
Create a new deployment
Set up a deployment to deliver self-service applications, data, and desktops to your users.

Join existing server group
Add a server to an existing load-balanced group.

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**.



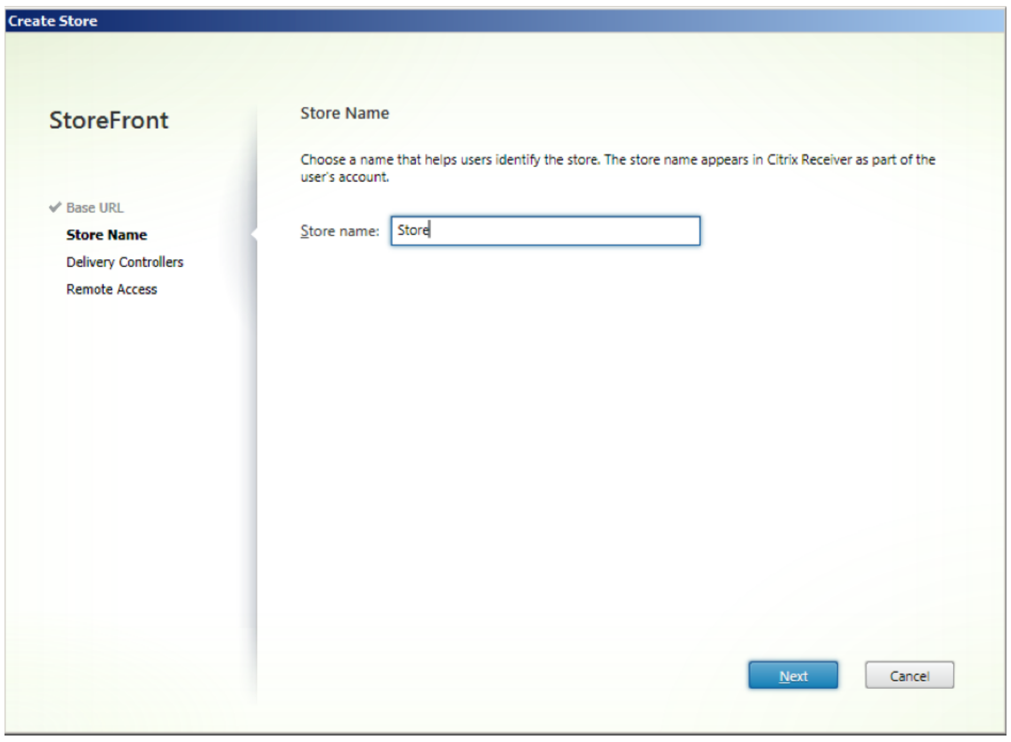
Create New Deployment

Confirm the base URL for services hosted on this deployment. For multiple server deployments, specify the load-balanced URL for the server group.

Base URL: https://xenstore05.virtdom.chsys3.com

6. Enter a store name of Store.

7. Click **Next**.



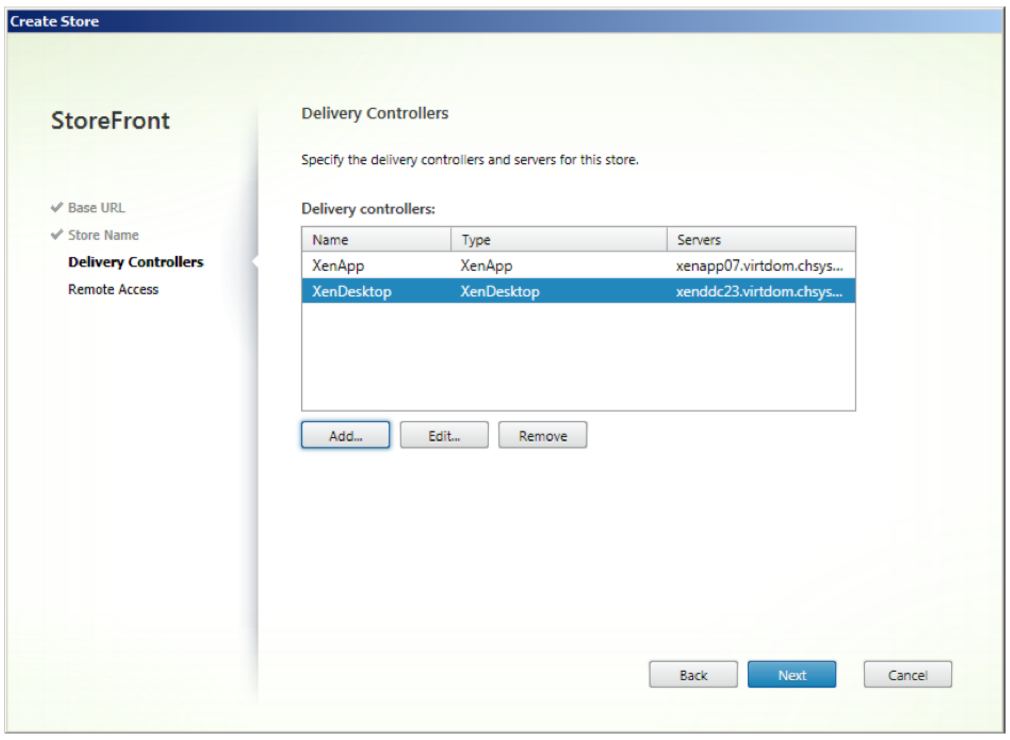
Store Name

Choose a name that helps users identify the store. The store name appears in Citrix Receiver as part of the user's account.

Store name: Store

8. Enter Delivery Controllers.

9. Click **Next**.



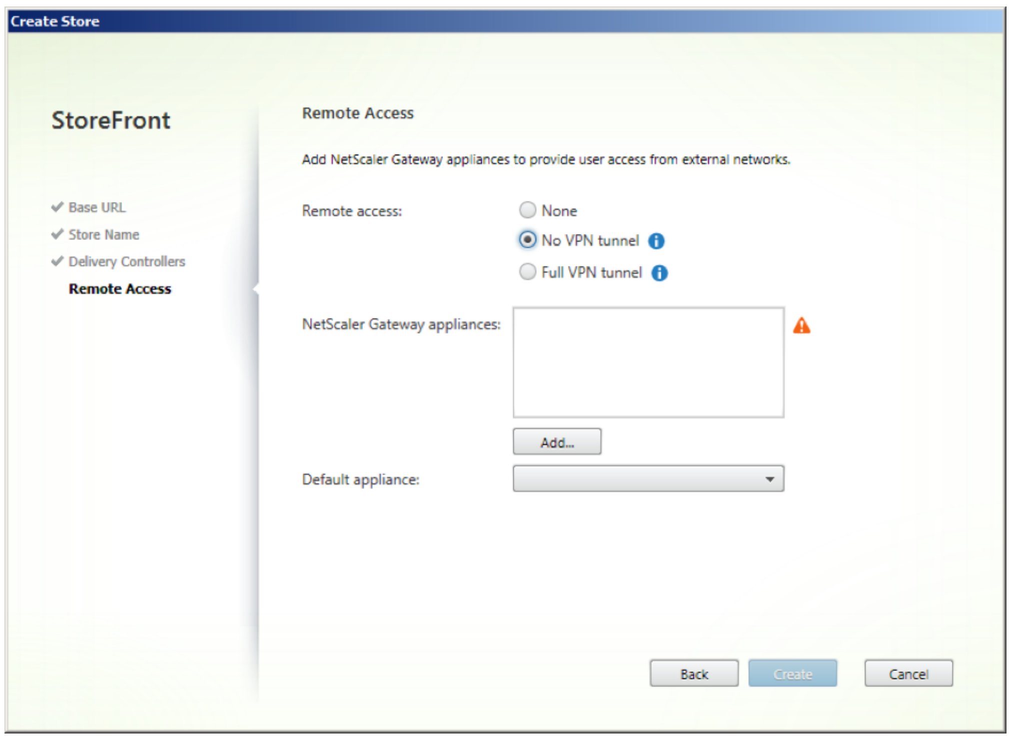
Delivery Controllers

Specify the delivery controllers and servers for this store.

Delivery controllers:

Name	Type	Servers
XenApp	XenApp	xenapp07.virtdom.chsys...
XenDesktop	XenDesktop	xenddc23.virtdom.chsys...

10. Select **No VPN tunnel**.



Remote Access

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

Remote access: ○ None ● No VPN tunnel ○ Full VPN tunnel

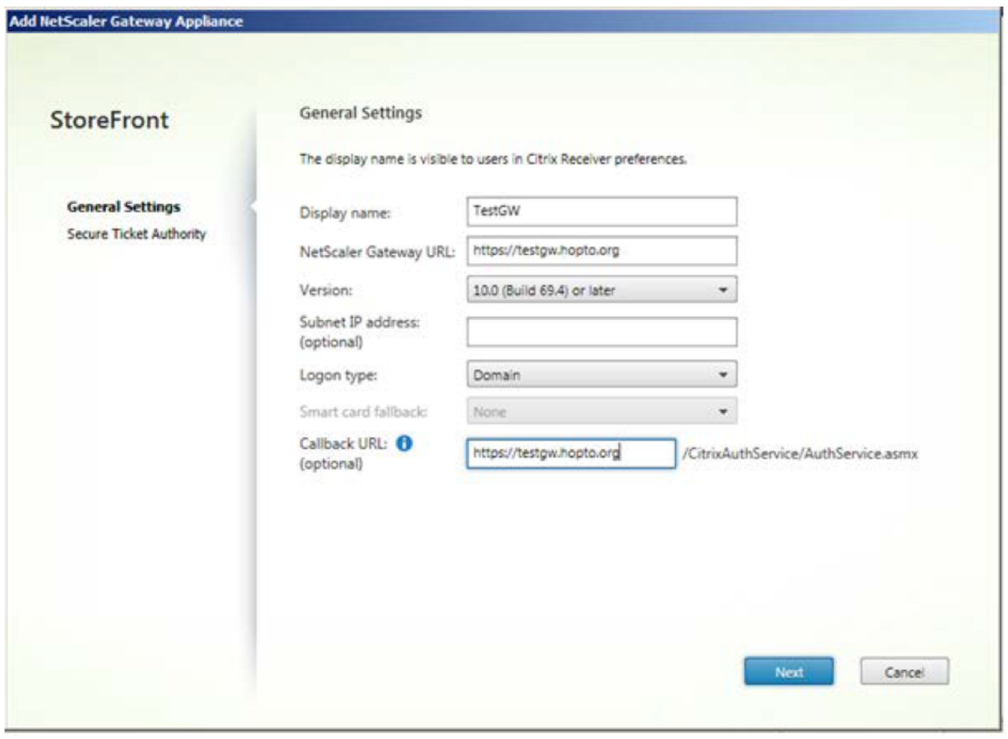
NetScaler Gateway appliances:

Default appliance:

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

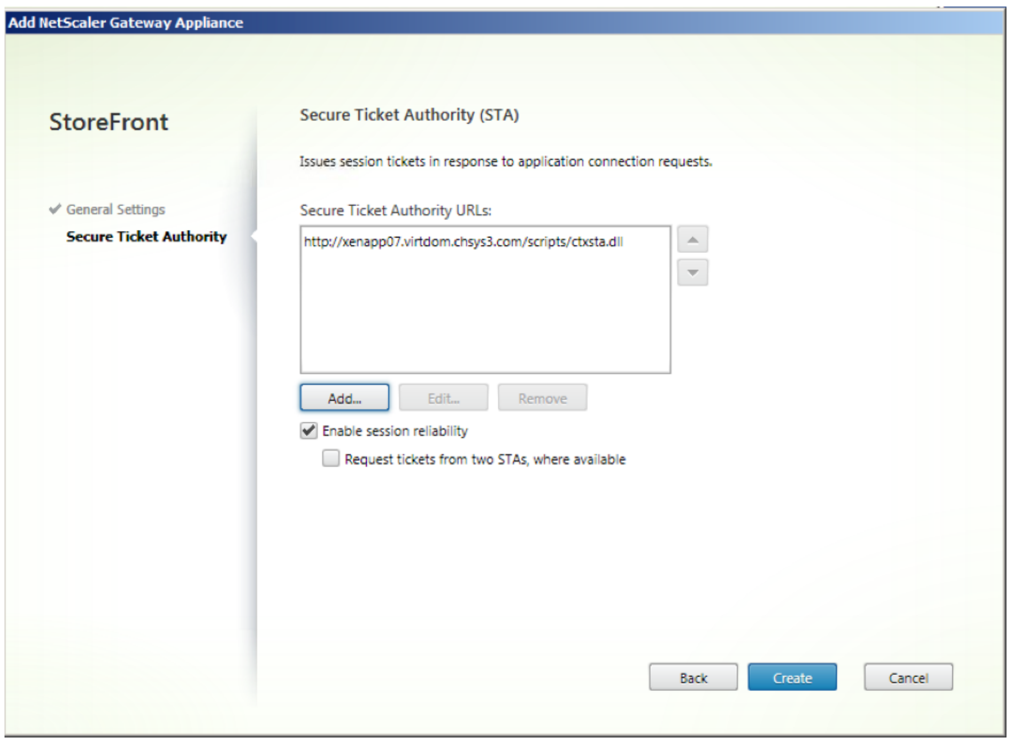
The display name is visible to users in Citrix Receiver preferences.

Display name: TestGW
NetScaler Gateway URL: https://testgw.hopto.org
Version: 10.0 (Build 69.4) or later
Subnet IP address: (optional)
Logon type: Domain
Smart card fallback: None
Callback URL: (optional) https://testgw.hopto.org /CitrixAuthService/AuthService.asmx

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**.



Add NetScaler Gateway Appliance

StoreFront

✓ General Settings
Secure Ticket Authority

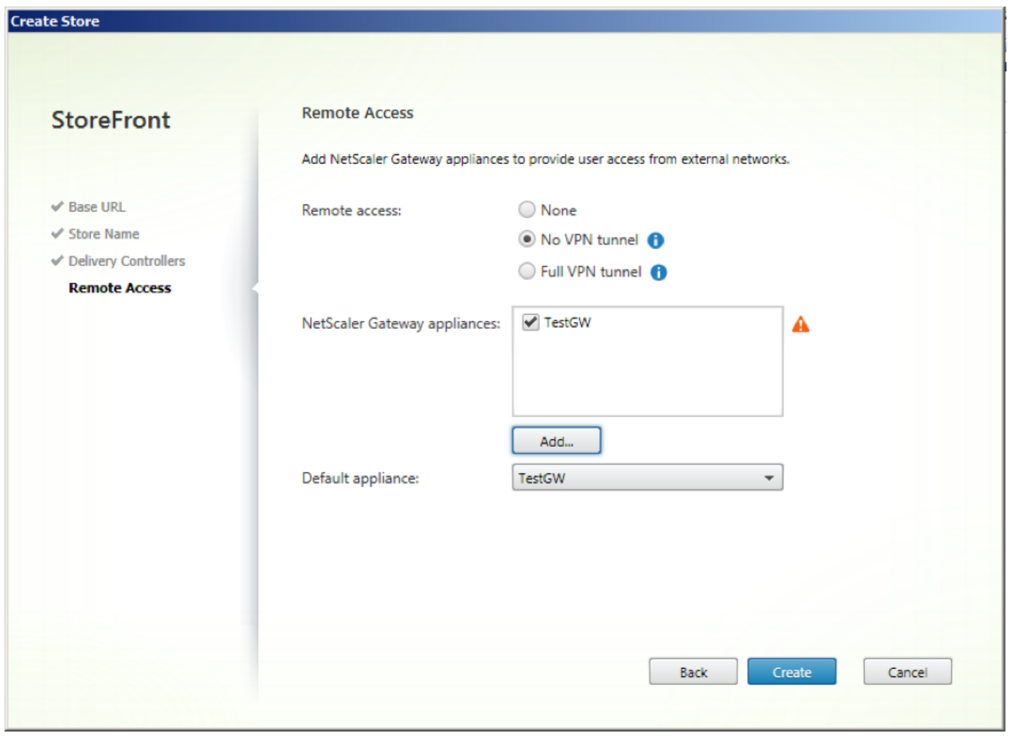
Secure Ticket Authority (STA)

Issues session tickets in response to application connection requests.

Secure Ticket Authority URLs:
http://xenapp07.virtdom.chsys3.com/scripts/ctxsta.dll

☑ Enable session reliability
☐ Request tickets from two STAs, where available

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**.



Create Store

StoreFront

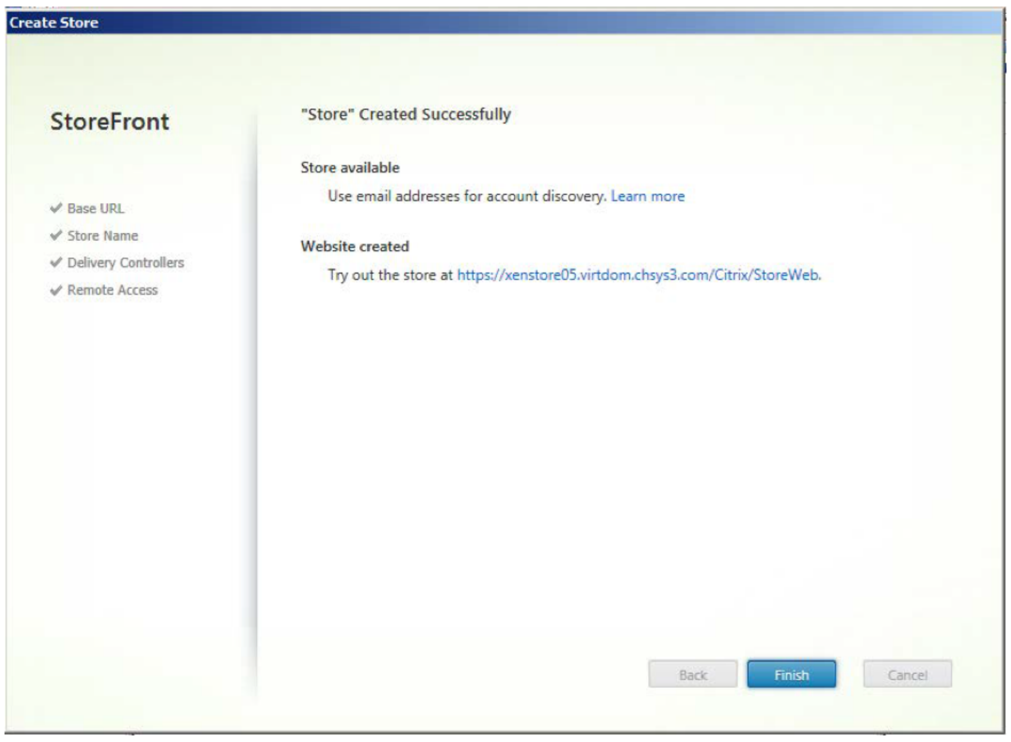
✓ Base URL
✓ Store Name
✓ Delivery Controllers
Remote Access

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: ☑ TestGW
Default appliance: TestGW

18. Click **Finish**.



Create Store

StoreFront

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

"Store" Created Successfully

Store available

Use email addresses for account discovery. Learn more

Website created

Try out the store at https://xenstore05.virtdom.chsys3.com/Citrix/StoreWeb.

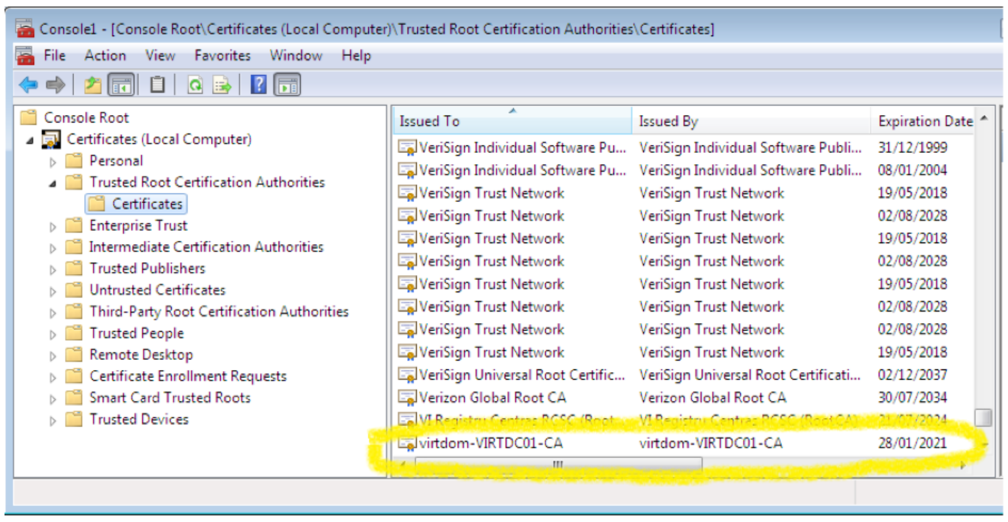
[Back to top](#)

Test the deployment from a Windows PC connected to the Internet

On the Windows PC

1. Confirm that a recent Citrix Receiver is installed.

2. Confirm that the Trusted Root CA Certificate has been installed into the **Trusted Root Certification Authorities** > **Certificates container**.



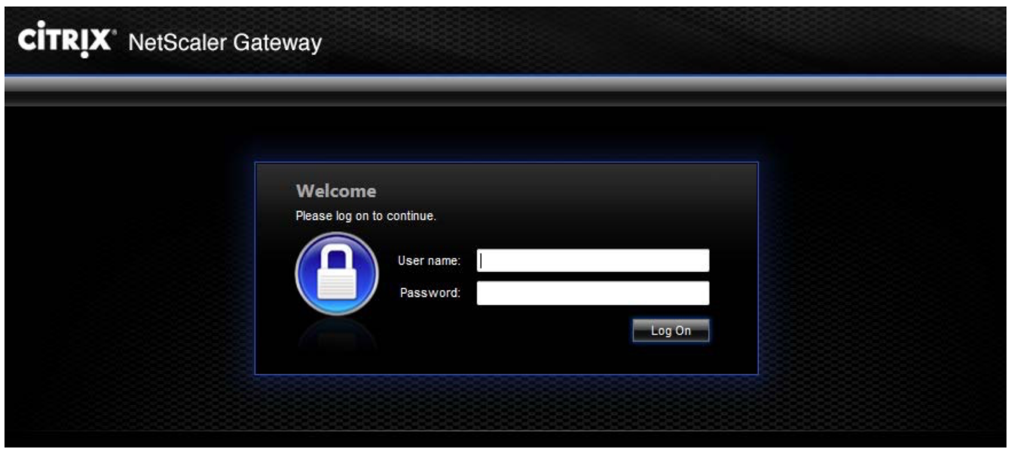
Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

Console Root
- Certificates (Local Computer)
  - Personal
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Remote Desktop
  - Certificate Enrollment Requests
  - Smart Card Trusted Roots
  - Trusted Devices

Issued To	Issued By	Expiration Date
VeriSign Individual Software Pu...	VeriSign Individual Software Publi...	31/12/1999
VeriSign Individual Software Pu...	VeriSign Individual Software Publi...	08/01/2004
VeriSign Trust Network	VeriSign Trust Network	19/05/2018
VeriSign Trust Network	VeriSign Trust Network	02/08/2028
VeriSign Trust Network	VeriSign Trust Network	19/05/2018
VeriSign Trust Network	VeriSign Trust Network	02/08/2028
VeriSign Trust Network	VeriSign Trust Network	19/05/2018
VeriSign Trust Network	VeriSign Trust Network	02/08/2028
VeriSign Trust Network	VeriSign Trust Network	02/08/2028
VeriSign Trust Network	VeriSign Trust Network	19/05/2018
VeriSign Universal Root Certific...	VeriSign Universal Root Certificati...	02/12/2037
Verizon Global Root CA	Verizon Global Root CA	30/07/2034
VI Registru Centras RCSC (Root...	VI Registru Centras RCSC (RootCA)	21/07/2024
virtdom-VIRTDC01-CA	virtdom-VIRTDC01-CA	28/01/2021

3. Turn off certificate revocation checking in Internet Explorer. This is required because our private certificate server is unknown on the Internet. a. Go to **Internet Explorer** > **Internet Options** > **Advanced**. b. Check for publisher's certificate revocation = Off c. Check for server certificate revocation = Off

4. If you use a browser other than Internet Explorer (such as Firefox) you might need to import the Trusted Root CA Certificate into its Certificate Manager, and turn off Online Certificate Status Protocol checking.



CITRIX NetScaler Gateway

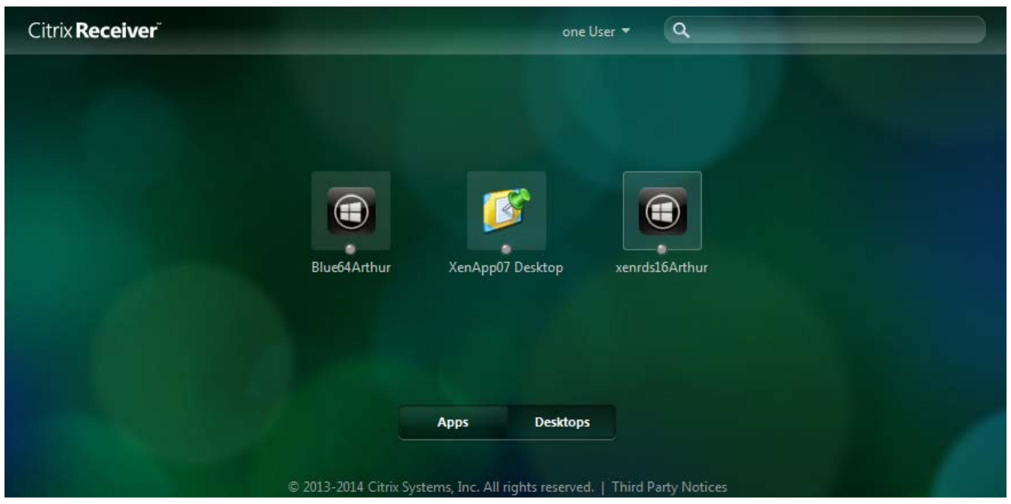
Welcome

Please log on to continue.

User name:

Password:

5. Use Internet Explorer to browse to your NetScaler Gateway. You should be presented with the NetScaler logon page.



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

Back to top

More How Do I Articles

Additional Resources

- CTX202097 - How to Configure NetScaler 11 to use with Web Interface 5.4 and XenApp
- Click on the link to download the latest version of NetScaler Gateway
- Click on the link to download the latest version of XenDesktop

Was this page helpful? 👍 👎 **Please provide article feedback.**

View Common Solutions

Citrix ADC
Citrix App Layering
Citrix Application Delivery Management
Citrix Endpoint Management
Citrix Gateway
Citrix Receiver
Citrix SD-WAN
Citrix SD-WAN WANOP
Citrix Virtual Apps
Citrix Virtual Apps and Desktops
Citrix Virtual Desktops
Citrix Workspace App
ShareConnect
ShareFile
StoreFront
XenServer

Get Additional Support

Call Technical Support

1 800 424 8749 (US)
0800 587 9031 (GB)
0800 182 5549 (DE)
0120 941 133 (JA)

View Additional Numbers

Open a Case

Open a ticket online for technical assistance with troubleshooting, break-fix requests, and other product issues.

Open a Case Online

View Related Sites

Citrix Product Documentation

Citrix Discussions

Share this page

Call or Chat