Deployment Guide
ICA Proxy for XenApp

Access Gateway Standard Edition

(CAG)

www.citrix.com

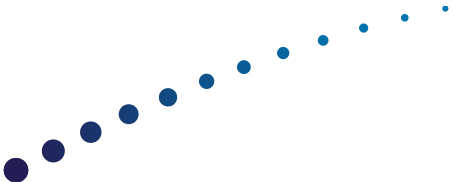


Table of Contents

Introduction

Citrix Access Gateway™, a member of the Citrix Delivery Center, is the only SSL VPN to securely deliver any application with policy-based SmartAccess control. Users will have easy-to-use secure access to all of the enterprise applications and data they need to be productive, and IT can cost effectively extend access to applications while maintaining security through SmartAccess application-level policies. With Access Gateway, organizations are empowered to cost-effectively meet the anywhere access demands of all workers – enabling flexible work options, easier outsourcing and non-employee access, and business continuity readiness – while ensuring the highest level of information security. The newest release of the company's popular Citrix Access Gateway™ appliance now includes integration with Citrix XenDesktop™, allowing companies to deliver virtual desktops securely to thousands of end users based on their unique identity, location and security status.

Citrix XenApp™, a member of the Citrix Delivery Center™ product family, is the industry's de facto standard for delivering Windows-based applications with the best performance, security and cost savings. XenApp is the most complete application virtualization system available with the ability to virtualize applications on both the client side and server side, delivering them on demand based on the user, the application or the location (online or offline). By centralizing applications and data in secure datacenters, IT can reduce the costs of management and support, increase data security and facilitate business continuity. XenApp Platinum Edition adds critical capabilities for application performance monitoring, secure remote access, WAN optimization and single-sign-on application security.

Citrix Delivery Center is the first solution on the market to deliver applications and desktops to any user, anytime, anywhere from a secure central location. Citrix Delivery Center's market leading application delivery technologies - XenServer, NetScaler, XenApp and XenDesktop - enable IT to dramatically improve agility, while enabling the best performance and highest security at the lowest cost.

Solution Requirements

- ICA Proxy for XenApp Web Interface or XenApp Plugin

Prerequisites

- Citrix Access Gateway Standard Edition - 2000 Series, version 4.6+
- Citrix XenApp Server, version 5.0+
- Microsoft Server 2008 SP1, Enterprise Edition
- Microsoft Active Directory

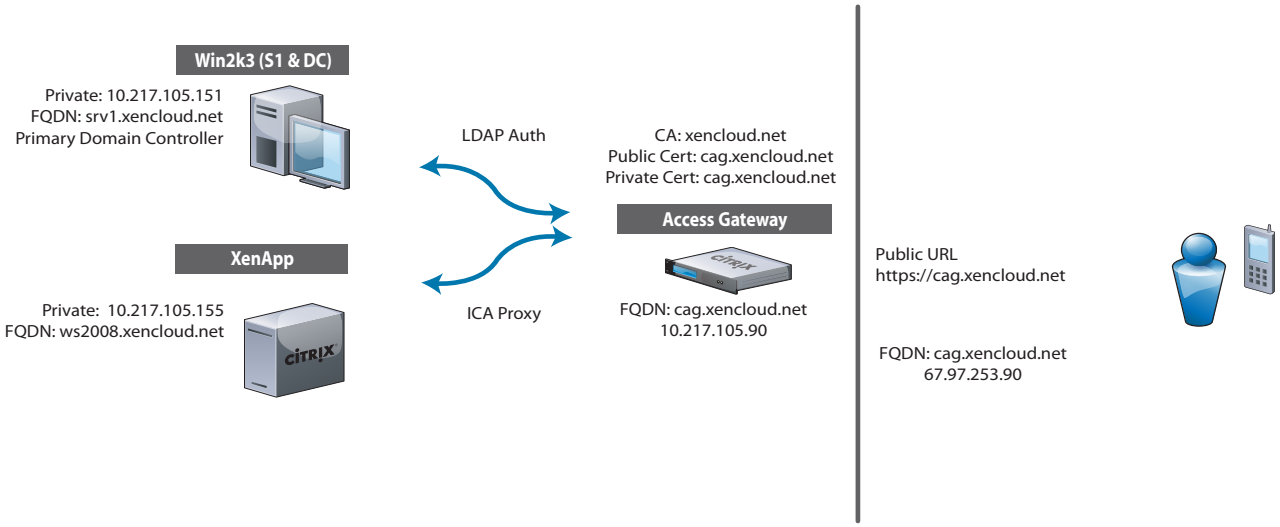
Caveats

- It is not possible to install the Web Interface and Citrix Client (PNAgent) option on the CAG simultaneously. You must choose one deployment over the other. This guide shows how to do both, but you must choose one.

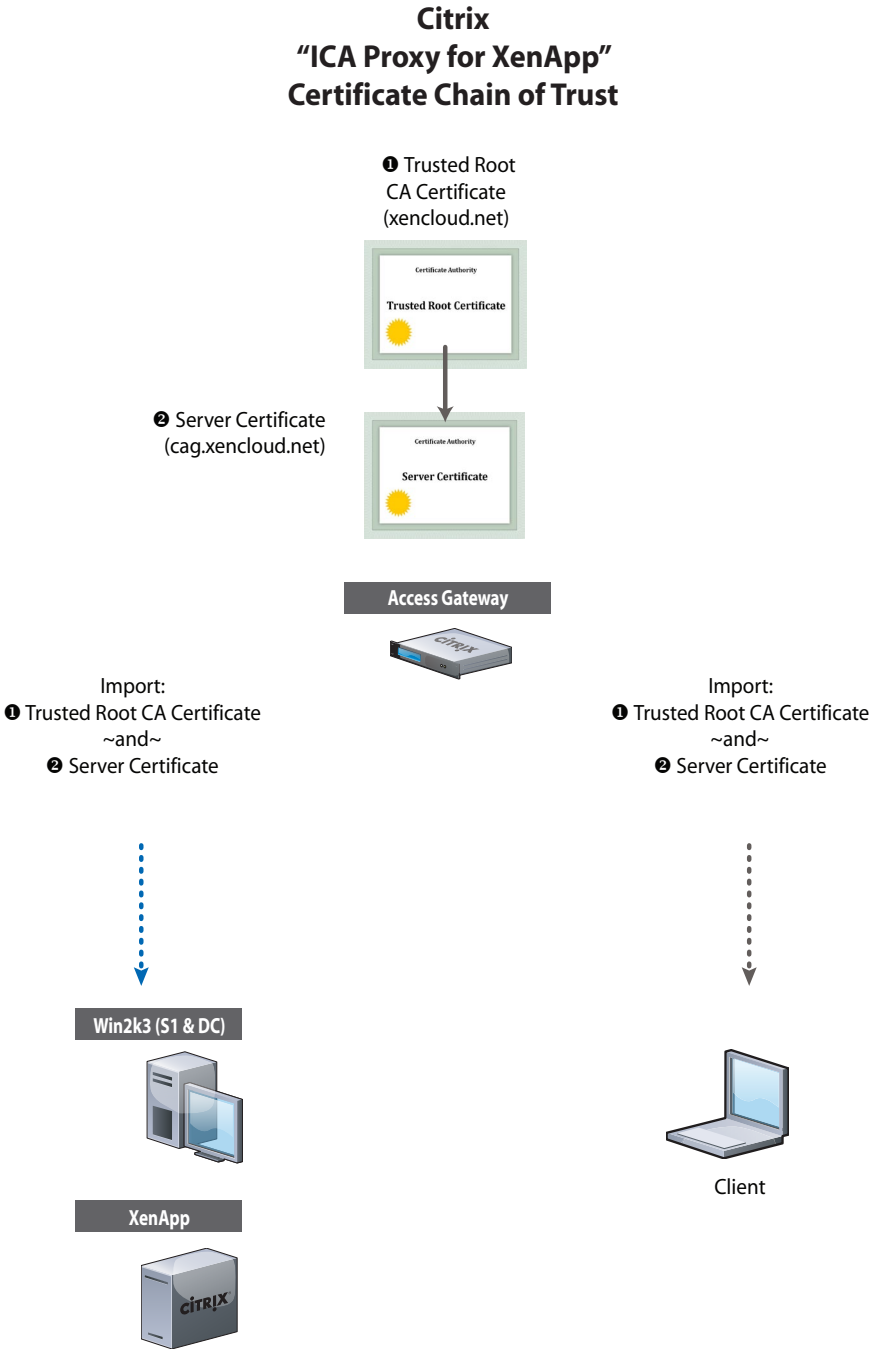
Network Diagram

The following is the Network that was used to develop this deployment guide.

Citrix
"ICA Proxy for XenApp"
Logical Network Diagram



VLAN Legend	Access Gateway
Interface 0 Interface 1	Interface 0: IP: 67.97.253.90 / 24 Interface 1: IP: 10.217.105.90


Citrix
"ICA Proxy for XenApp"
Certificate Chain of Trust
❶ Trusted Root
CA Certificate
(xencloud.net)
Certificate Authority
Trusted Root Certificate
❷ Server Certificate
(cag.xencloud.net)
Certificate Authority
Server Certificate
Access Gateway
Import:
❶ Trusted Root CA Certificate
~and~
❷ Server Certificate
Import:
❶ Trusted Root CA Certificate
~and~
❷ Server Certificate
Win2k3 (S1 & DC)
XenApp
Client

XenApp

Configuration - Web Interface

Once you have installed Citrix XenApp you will need to configure it such that it will work with the Citrix Access Gateway in an ICA Proxy deployment. Creating a Web Interface will publish the XenApp applications in a web browser to the client.

From the Access Management Console:

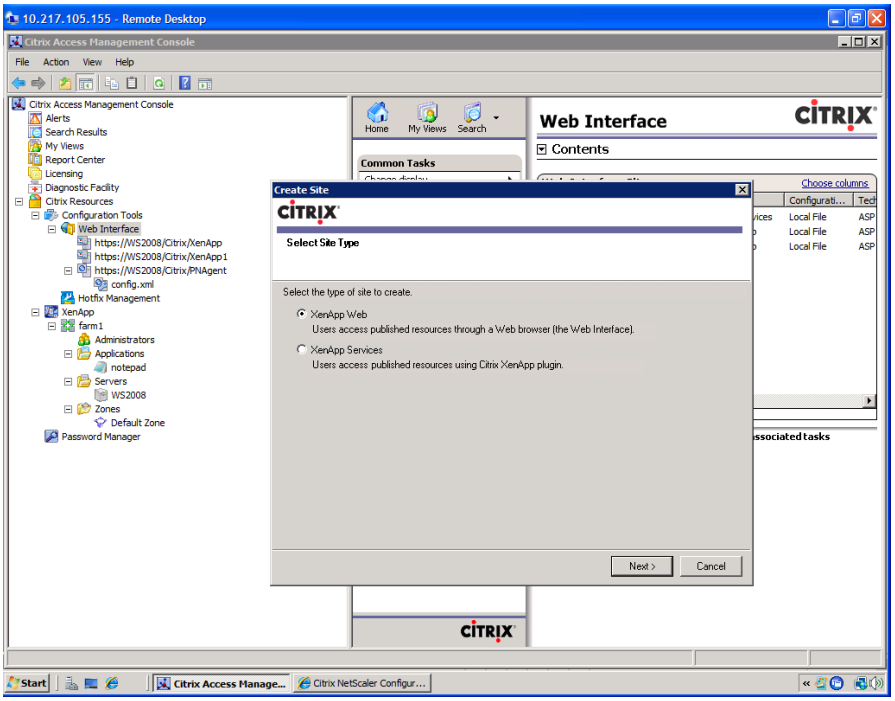
Citrix Resources ➥

Configuration Tools ➥

Web Interface ➥

Action ➥

Create Site.



Select XenApp Web.

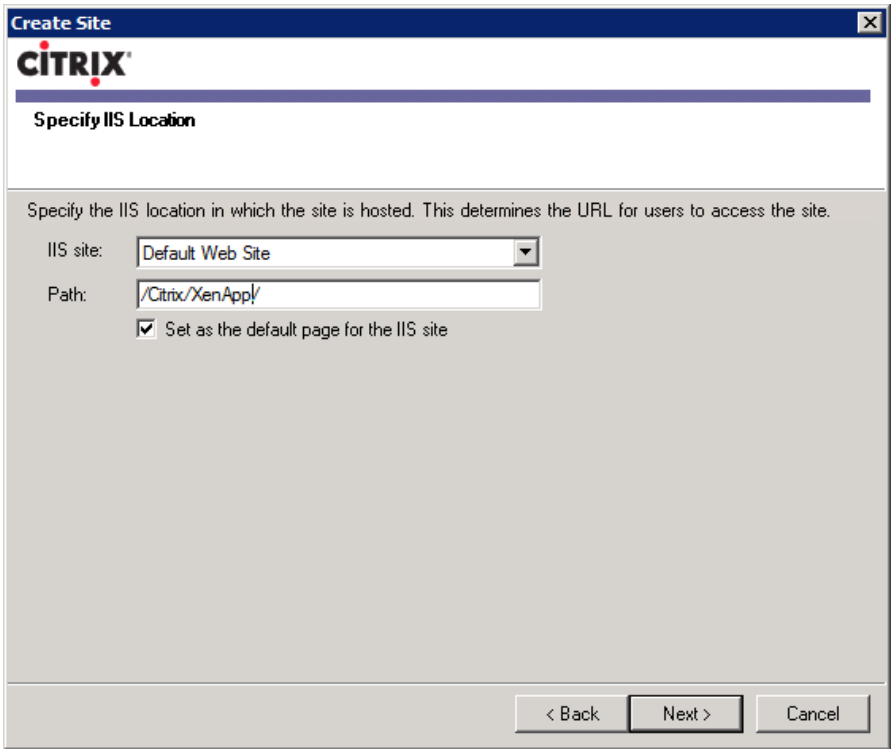
Select Next.

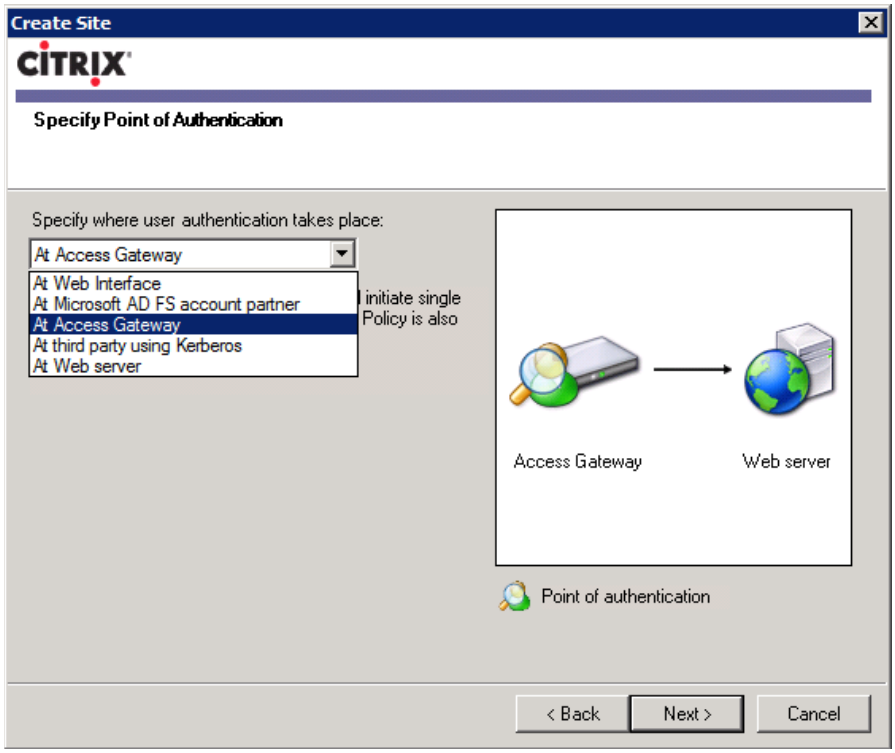
IIS Location:

IIS Site: Default Web Site

Path: /Citrix/XenApp/

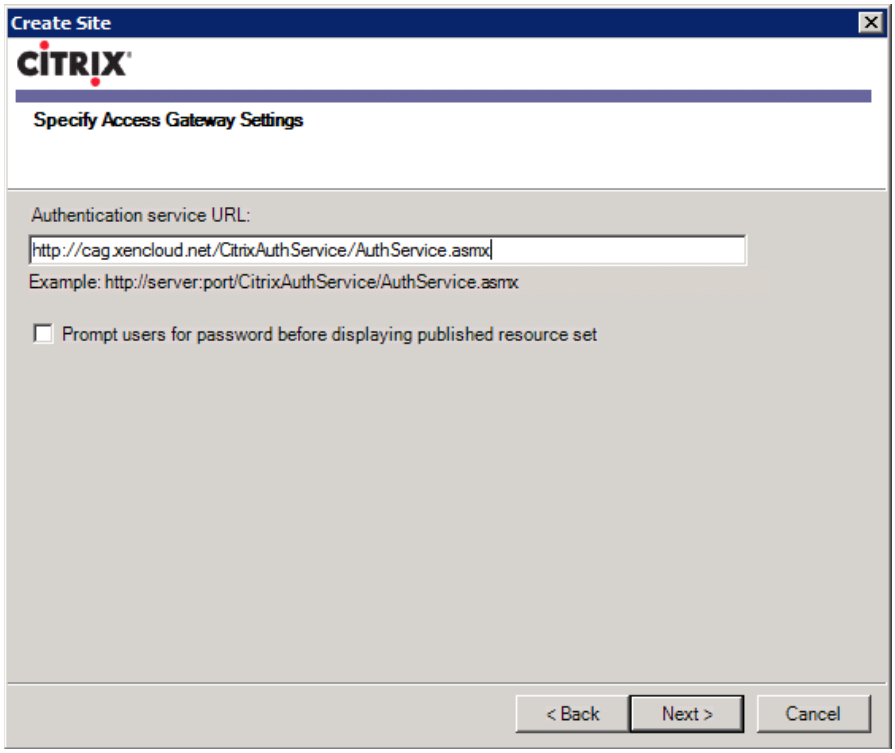
Set as the default page for IIS.





Point of Authentication:

At Access Gateway



Gateway Settings:

Authentication URL:

http://cag.xencloud.net/CitrixAuthService/AuthService.asmx

Note: cag.xencloud.net resolves to 10.217.105.90 on the XenApp servers network and is the inside interface of the Citrix Access Gateway.

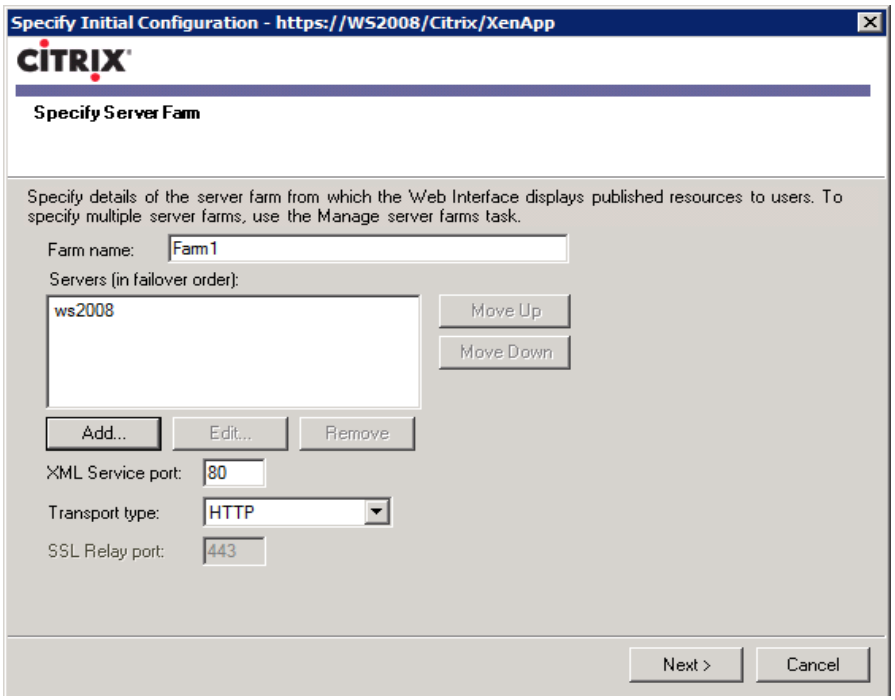
Note: the internal private DNS resolution for cag.xencloud.net is 10.217.105.90, while the external public DNS resolution for cag.xencloud.net is 67.97.253.90.

Next.

Specify Server Farm:

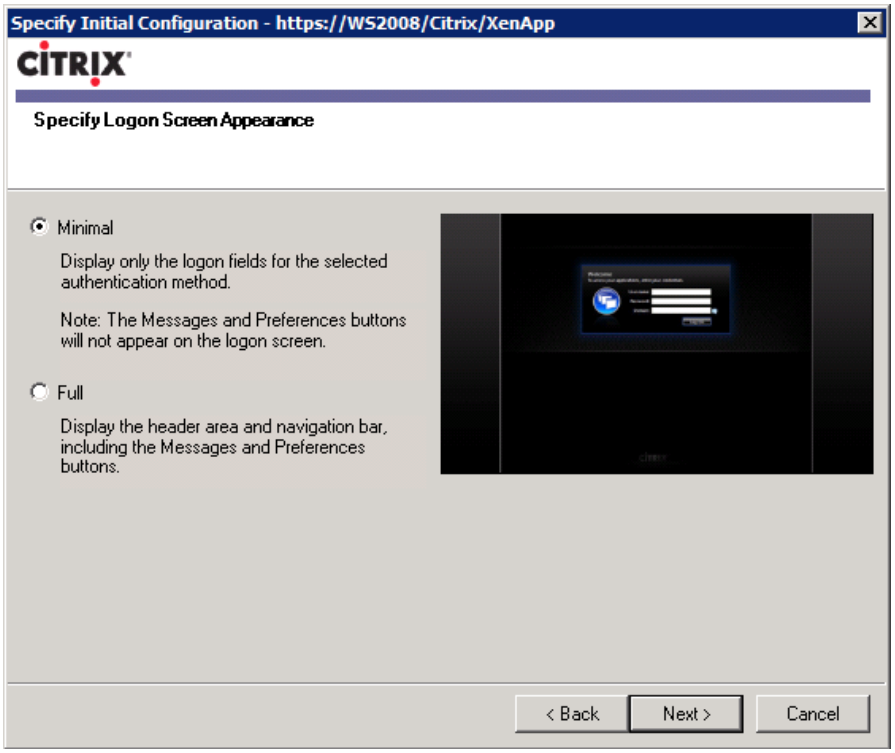
Farm Name: <your farm name>

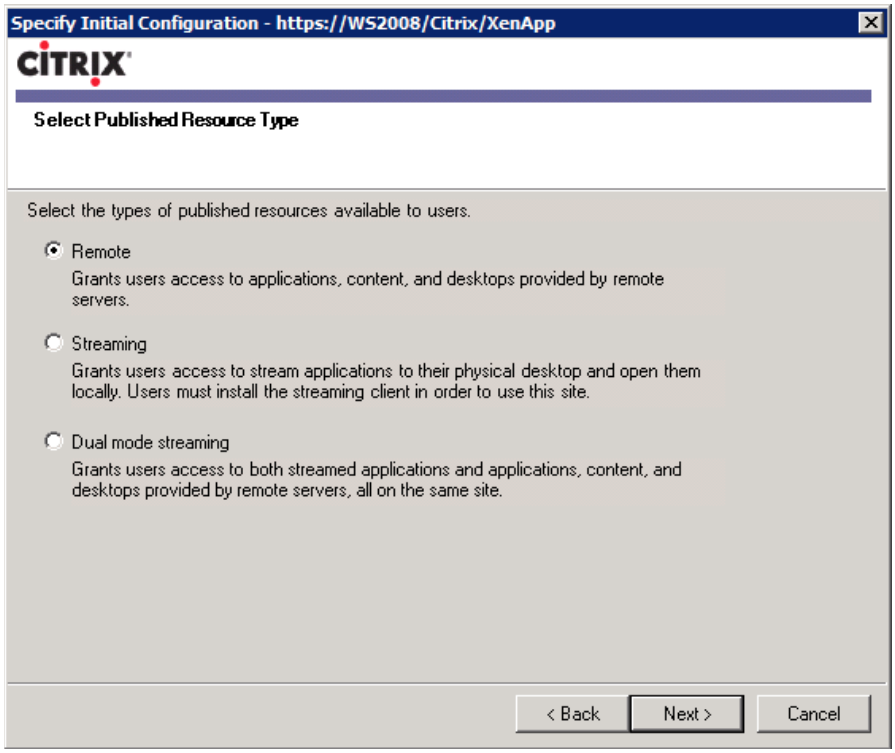
Servers: <XenApp Hostname>



Logon Screen:

Minimal or Full

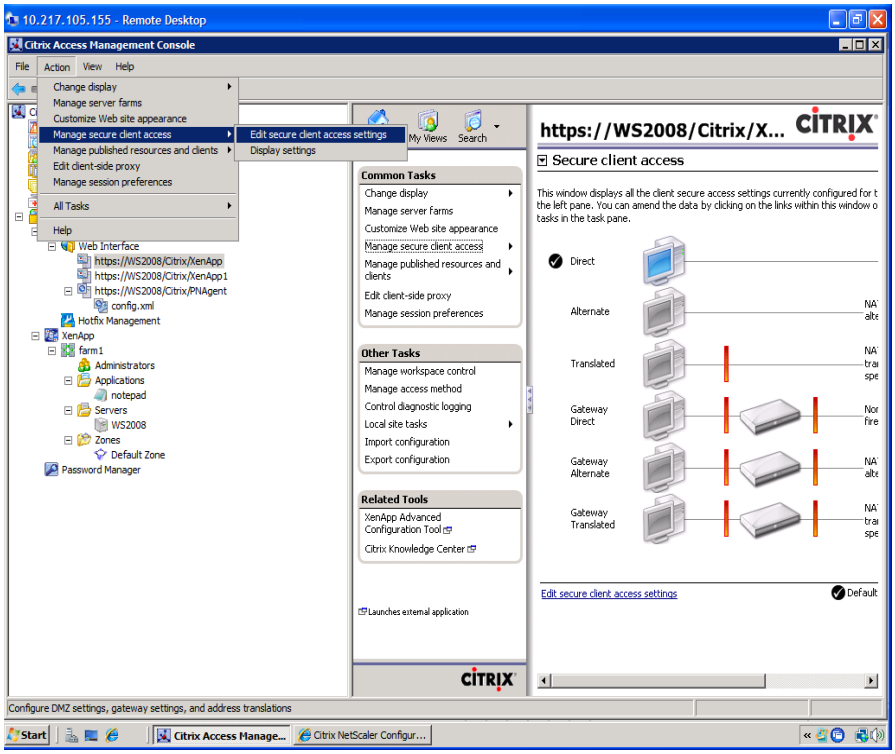




Resource Type:

Remote

Select Finish



From the Access Management Console:

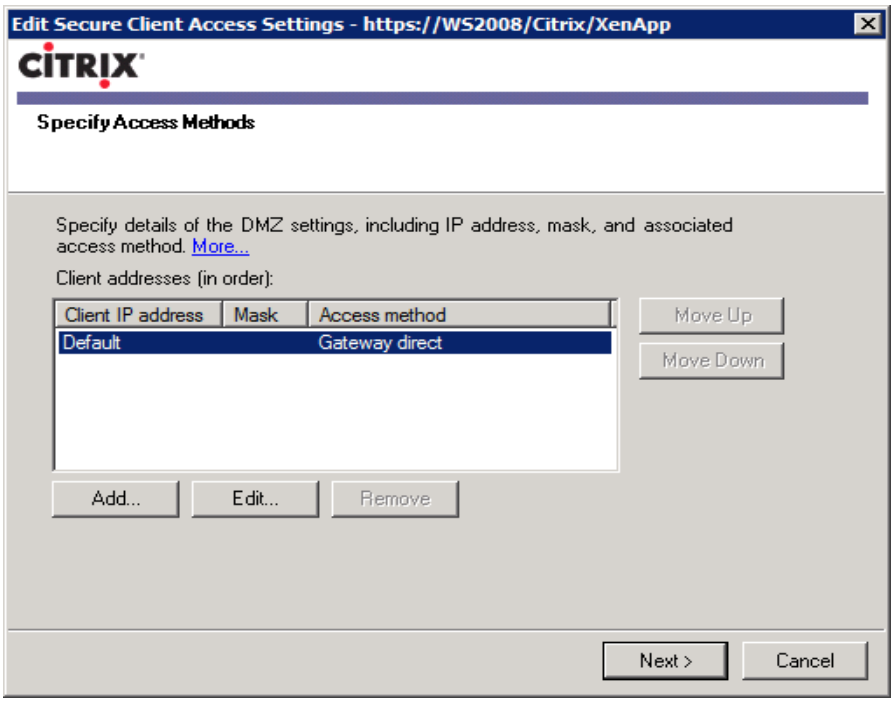
- Actions ➥
  - Manage Secure Client Access ➥
    - Edit Secure Client Access.

Specify Access Method:

Client IP: Default

Method: Gateway Direct

Next.

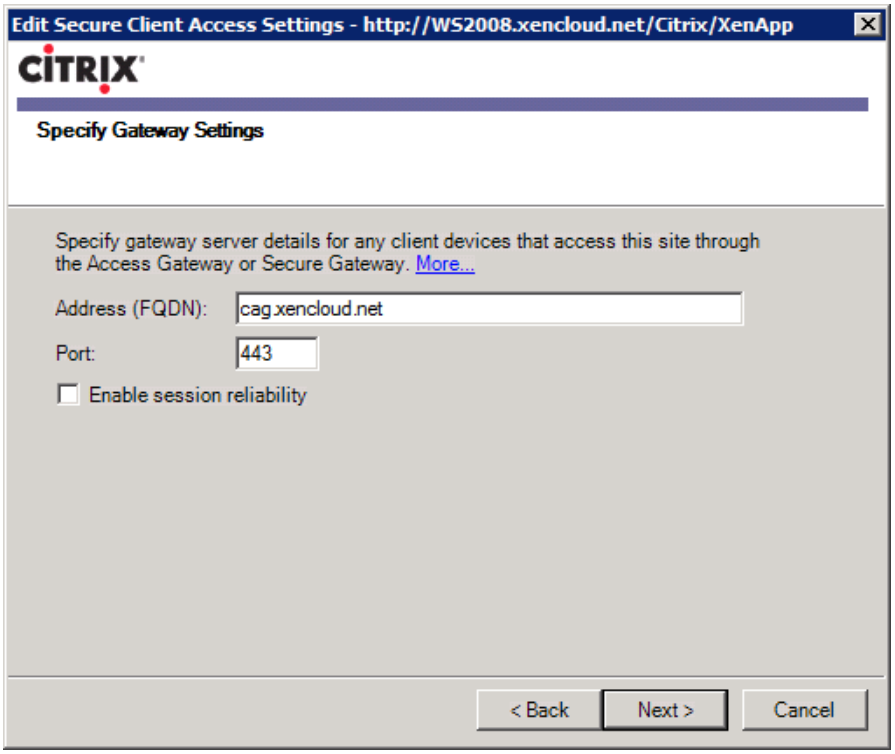


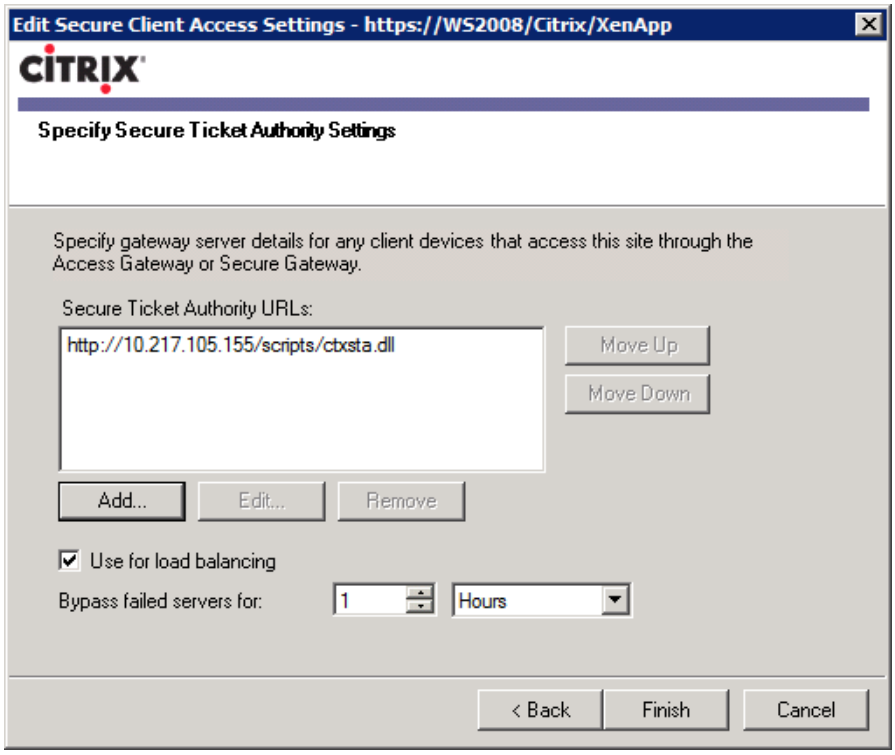
Gateway Settings:

Address: <FQDN of Citrix Access Gateway>

Port: 443

Note: Your first thought might be to configure the private FQDN here, but that isn't the case. According to the sentence in the dialog box, this is the FQDN that public users will use to access the applications - through the Access Gateway. Therefore, this needs to be the public FQDN of the CAG, which in this example is cag.xencloud.net, and resolves to 67.97.253.90.





Secure Ticket Authority:

URL: <ip address of XenApp>/scripts/ctxsta.dll

Select Finish

XenApp

Configuration - XenApp Plugin

Once you have installed Citrix XenApp you will need to configure it such that it will work with the Citrix Access Gateway in an ICA Proxy deployment. Creating a XenApp service will publish the XenApp applications through the Citrix client, such as XenApp client or Citrix Receiver.

From the Access Management Console:

Citrix Resources ➥

Configuration Tools ➥

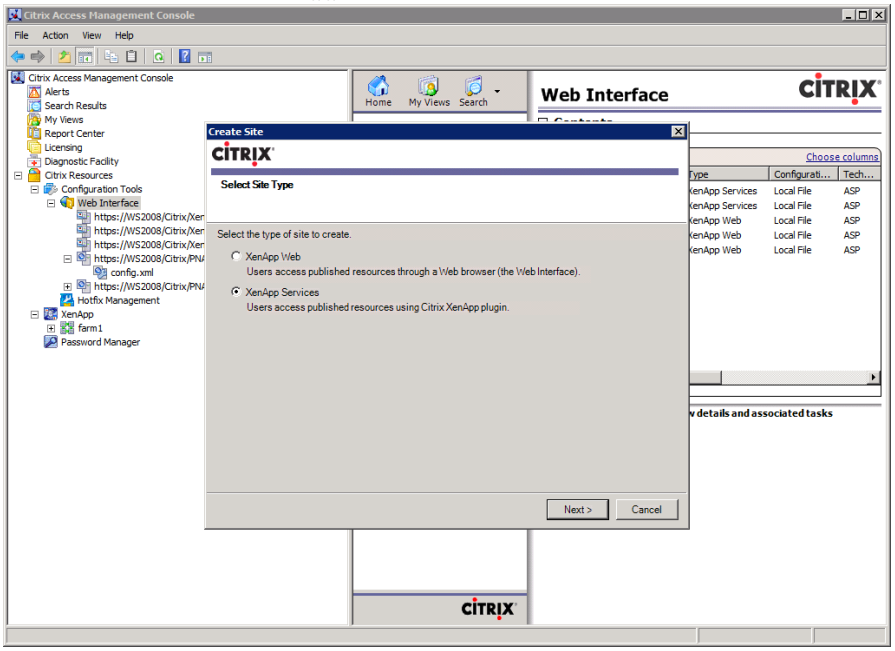
Web Interface ➥

Action ➥

Create Site.

Select XenApp Services.

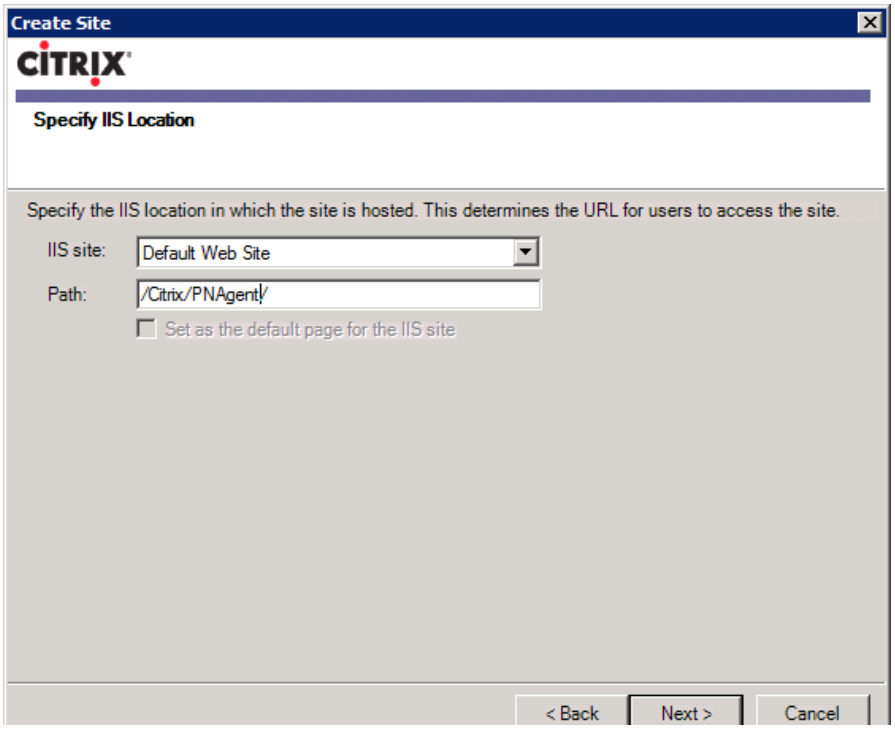
Select Next.

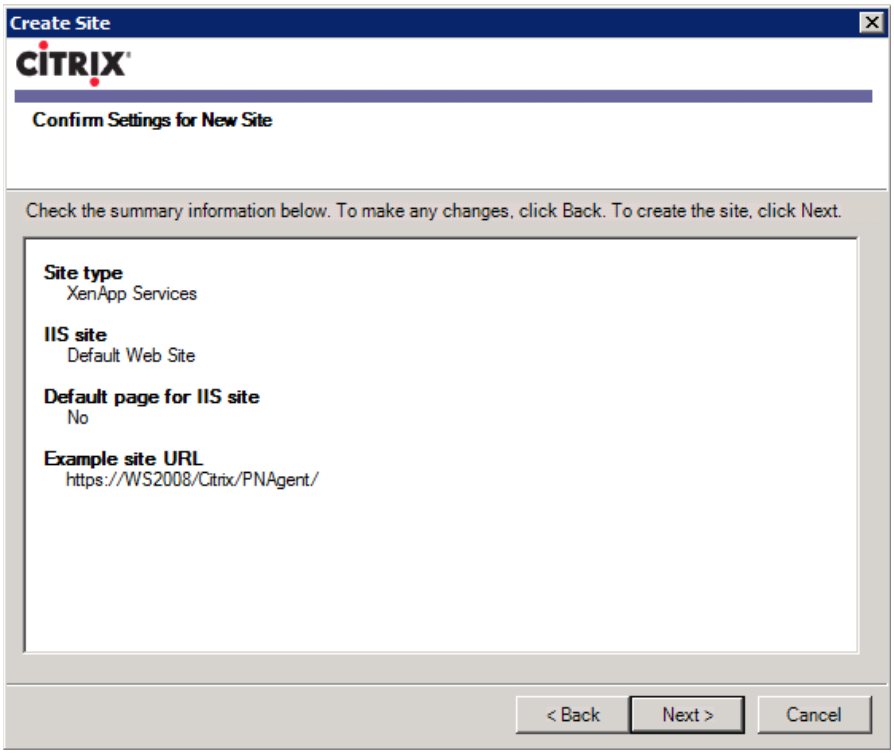


IIS Location:

IIS Site: Default Web Site

Path: /Citrix/PNAgent/



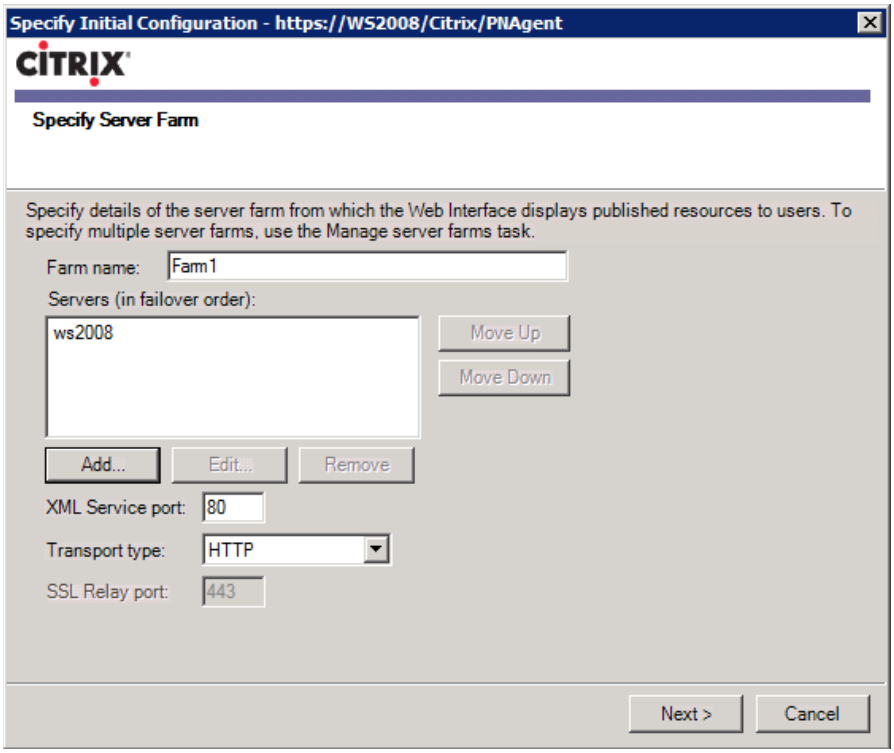


Confirm:

Next.

Finish.

Configure Site Now.



Specify Server Farm:

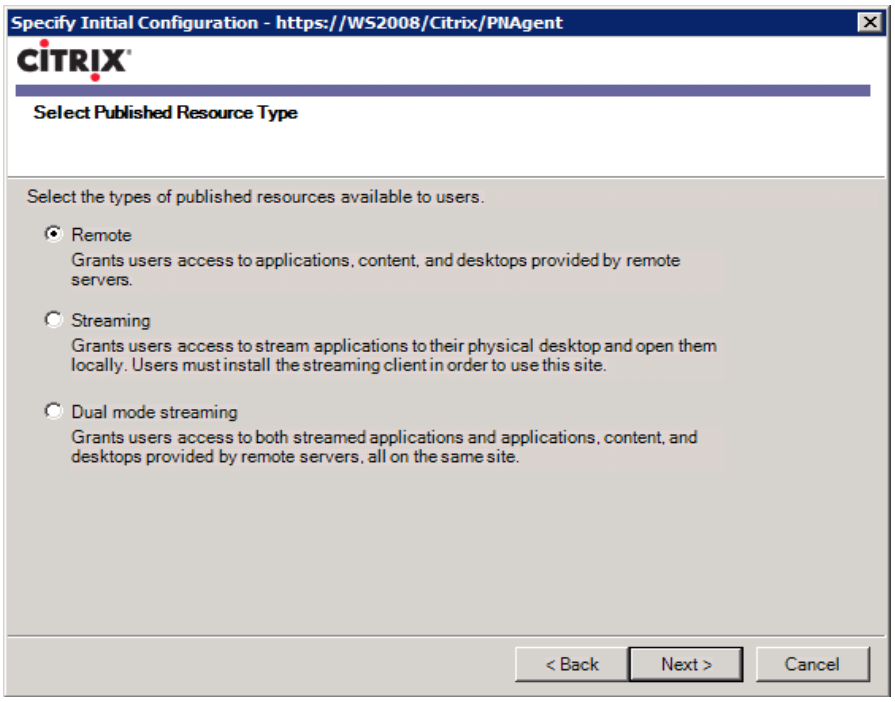
Farm Name: <your farm name>

Servers: <XenApp Hostname>

Resource Type:

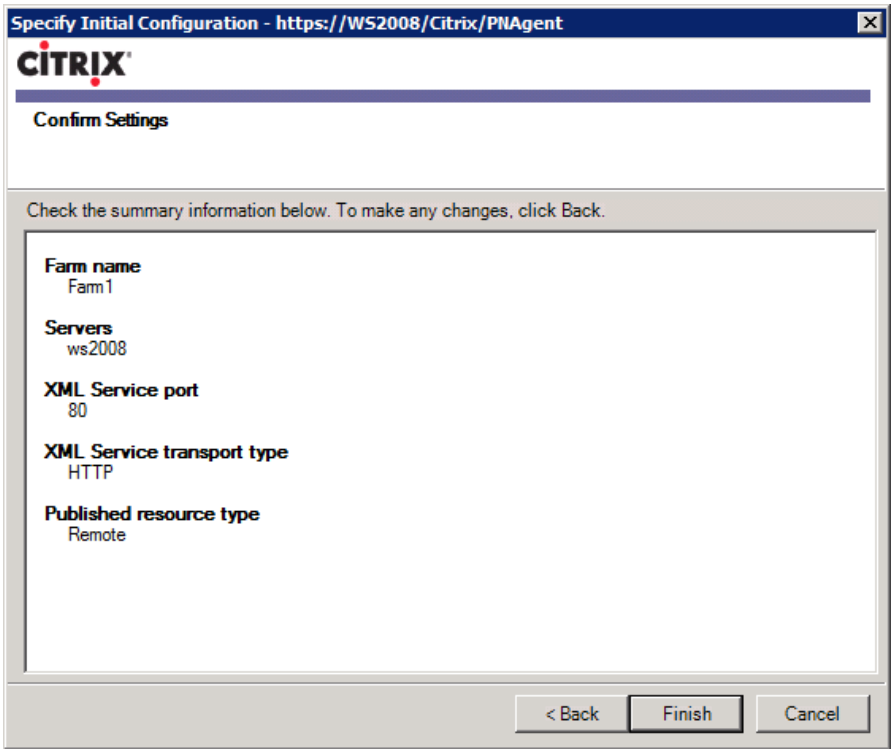
Remote

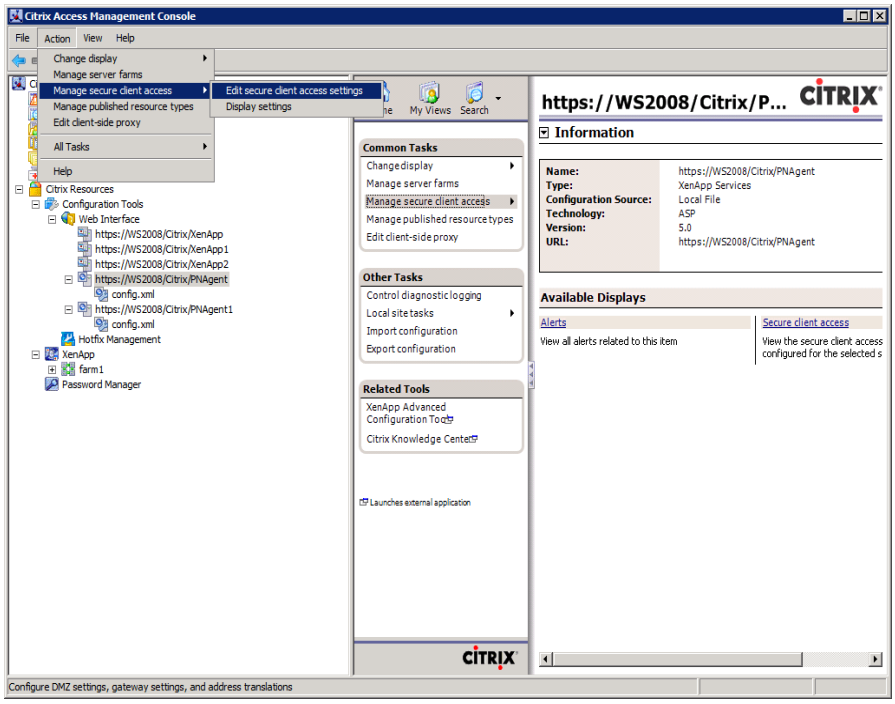
Next



Confirm:

Finish



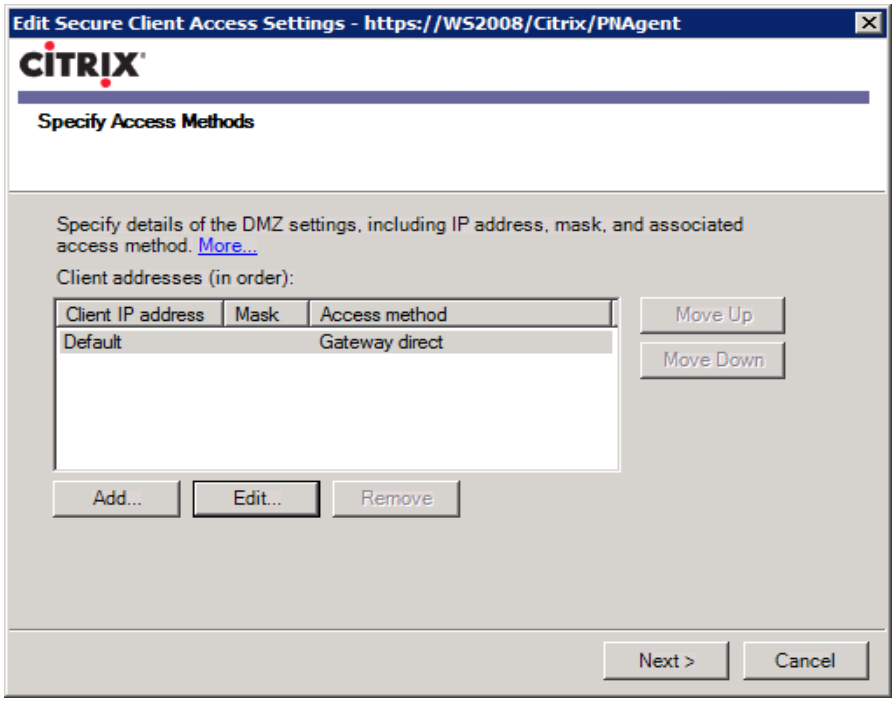


From the Access Management Console:

Actions ➥

Manage Secure Client Access ➥

Edit Secure Client Access.



Specify Access Method:

Client IP: Default

Method: Gateway Direct

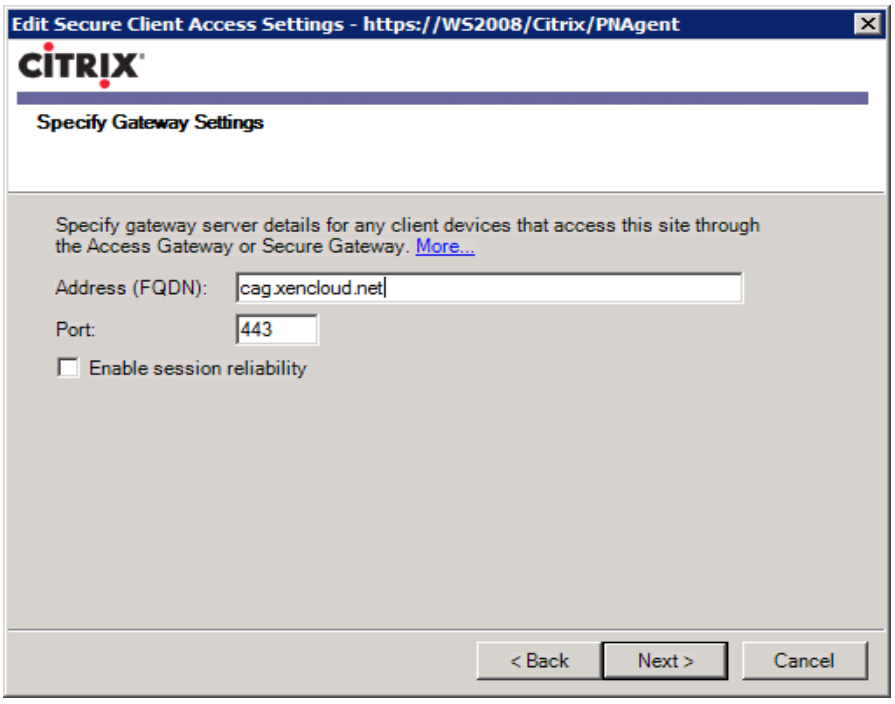
Next.

Gateway Settings:

Address: <FQDN of NetScaler Access Gateway>

Port: 443

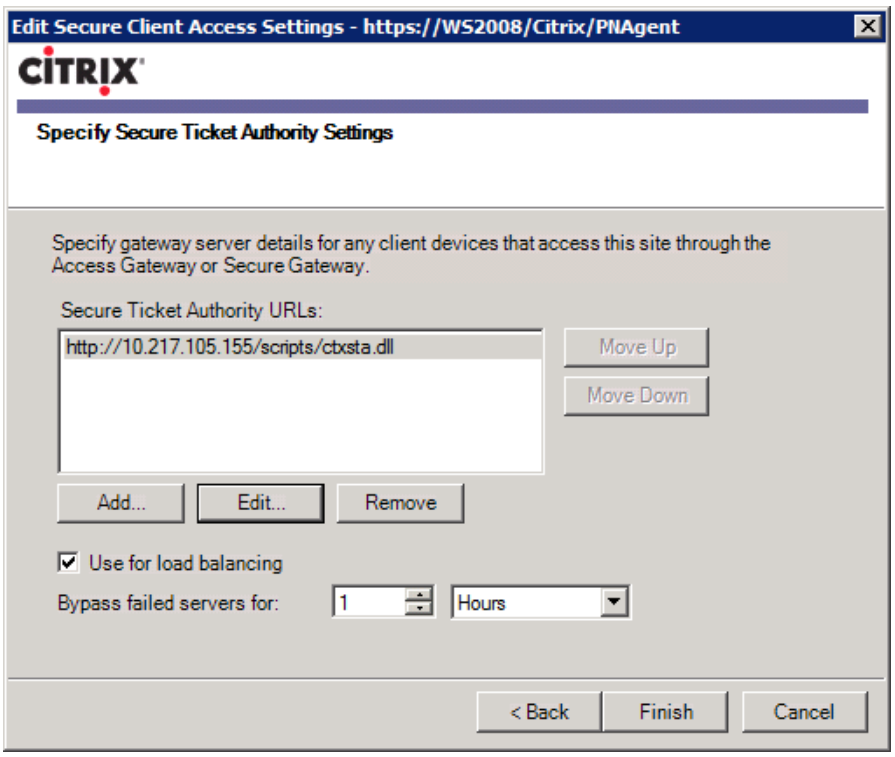
Note: Your first thought might be to configure the private FQDN here, but that isn't the case. According to the sentence in the dialog box, this is the FQDN that public users will use to access the applications - through the Access Gateway. Therefore, this needs to be the public FQDN of the CAG, which in this example is cag.xencloud.net, and resolves to 67.97.253.90.



Secure Ticket Authority:

URL: <ip address of XenApp>/scripts/ctxsta.dll

Select Finish



SSL Certificates

Server Certificate

You will need two certificates. A Root CA, and a server certificate. The procedure for installing a Server Certificate on the Access Gateway is as follows:

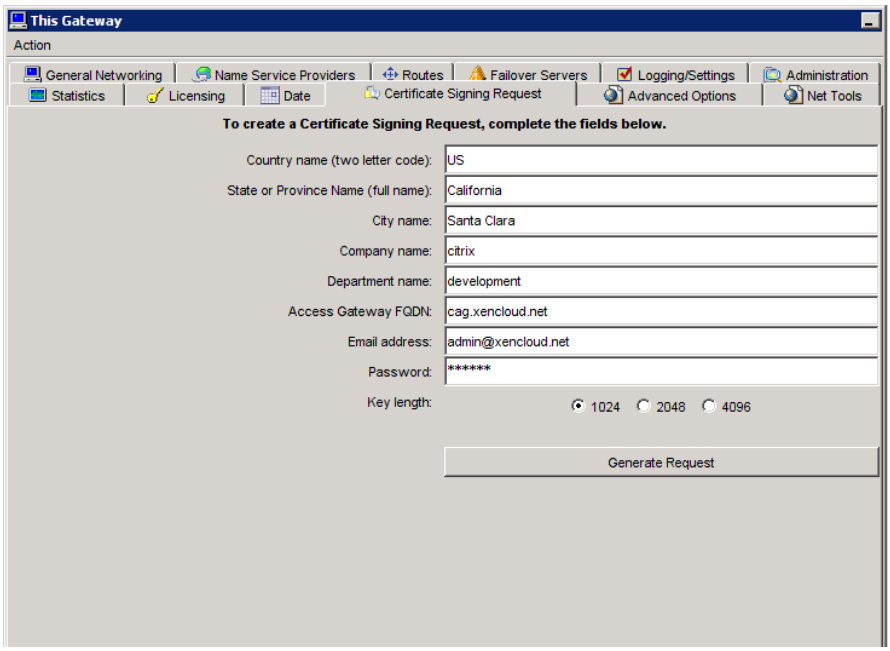
From the CAG:

AG Cluster ➥

This Gateway ➥

Certificate Signing Request.

First create a Certificate Signing Request (CSR) on the Citrix Access Gateway (CAG).



Create CSR:

Country: US

State: California

City: Santa Clara

Company: Citrix

Department: Development

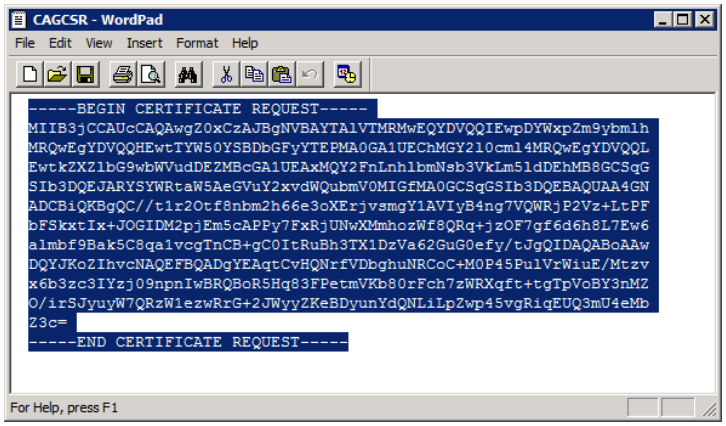
FQDN: cag.xencloud.net

Email: admin@xencloud.net

Password: <passphrase>

Generate Request.

Note: CN of cag.xencloud.net must match the DNS or Hosts file entry name.



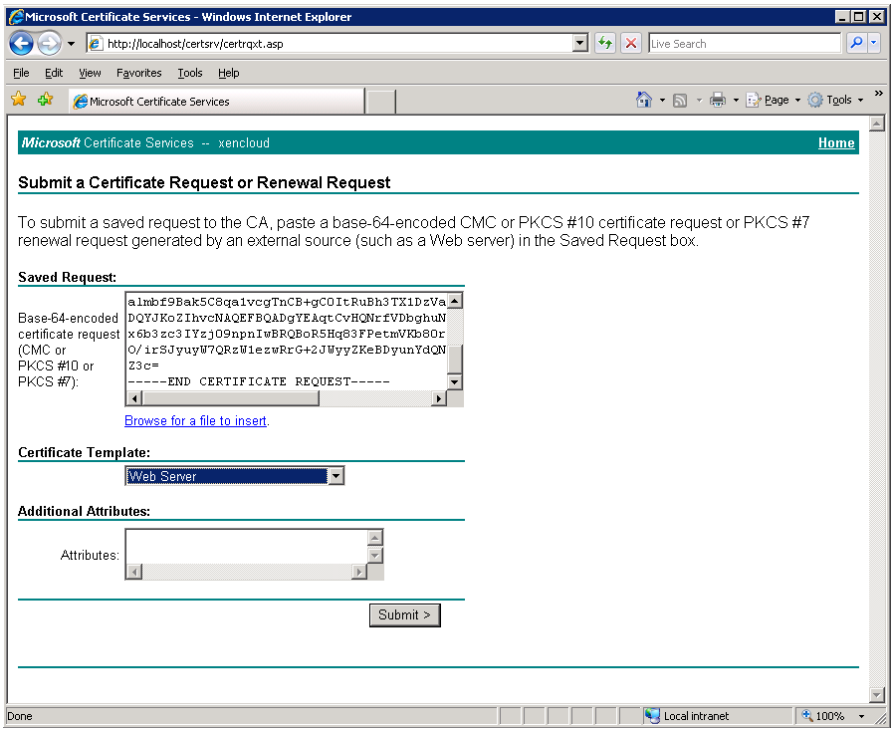
Generate Request:

On the CAG, selecting Generate Request, creates a certificate request.

Save it to the local hard drive.

Open it using notepad or wordpad.

Copy the contents.



Submit Certificate Request:

On the Microsoft Certificate Authority.

Open a browser, and point it to:

http://localhost/certsrv/certrqxt.asp

Paste the contents of the CSR.

Change type to Web Server

Submit.

Download Certificate as Base64 encoded.

Save to local hard drive.

From the CAG:

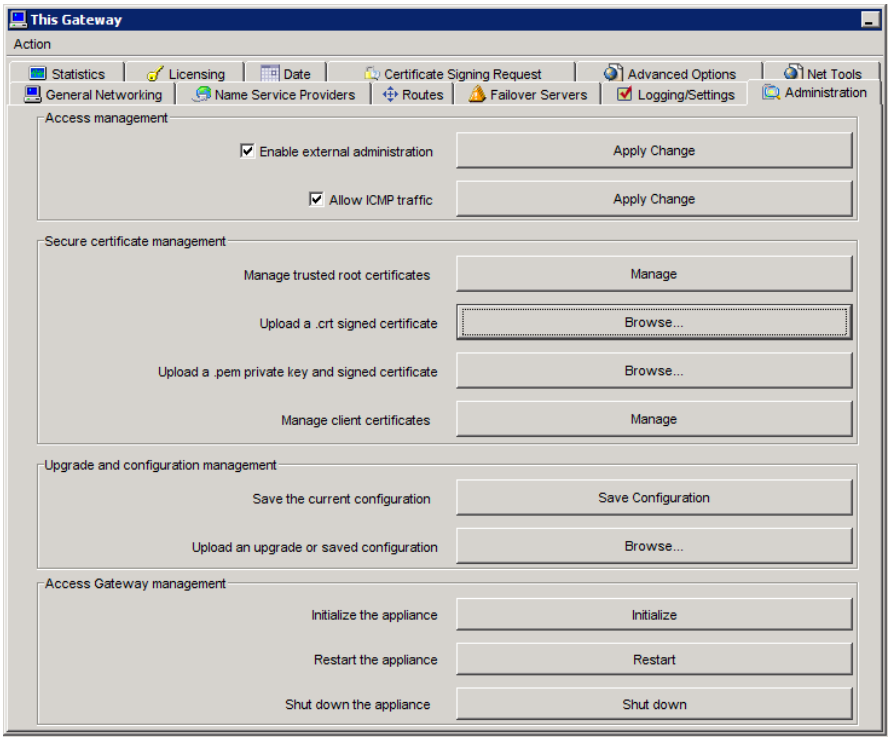
AG Cluster ➥

This Gateway ➥

Administration.

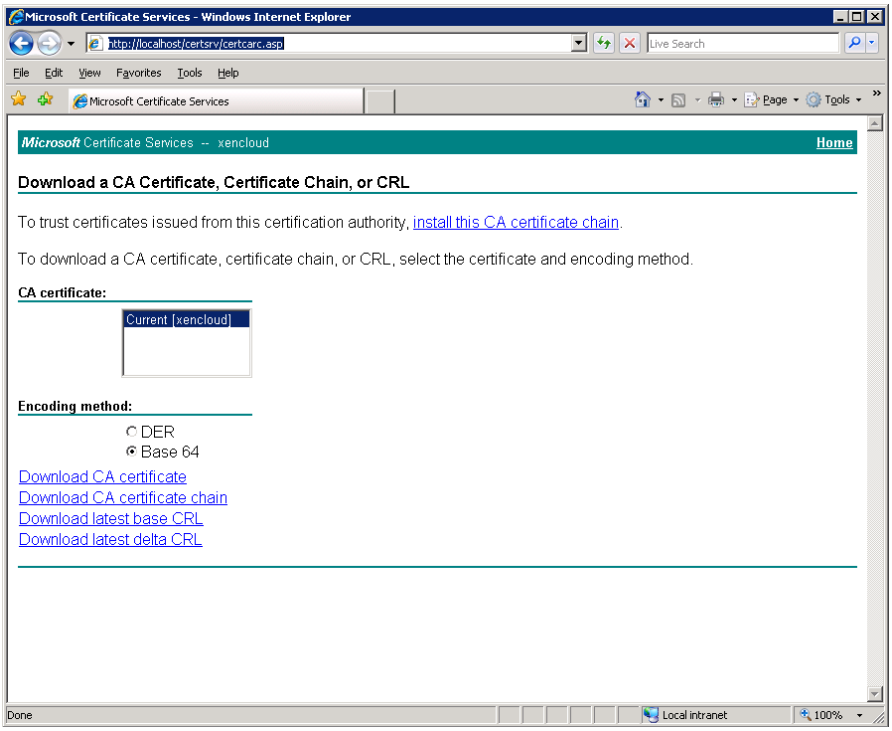
Upload signed cert:

Under Secure Certificate Management ➥ Upload a .crt signed certificate. (second button).



Root Certificate

Now, download the Root Certificate from the Microsoft Certificate Authority.



Download CA Cert:

On the Microsoft Certificate Authority.

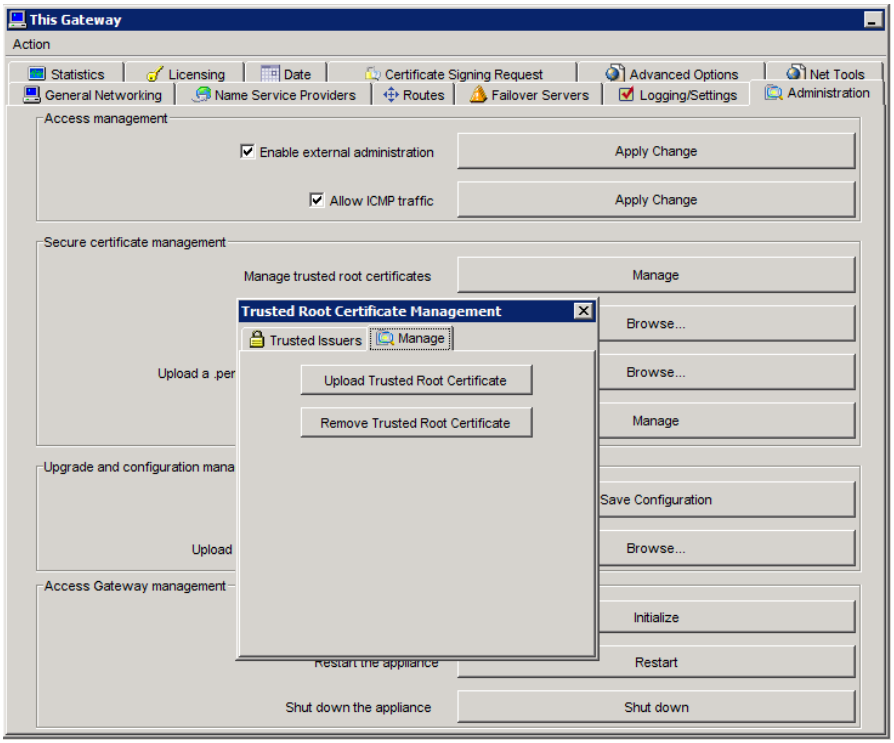
Open a browser, and point it to:

http://localhost/certsrv/certcarc.asp

Select Base64.

Download CA Certificate.

Save to local hard drive.



From the CAG:

AG Cluster ➥

This Gateway ➥

Administration.

Upload CA Cert:

Under Secure Certificate Management ➥ Manage trusted root certificates.

Upload Trusted Root Certificate.

XenApp Server

You will need to install the Certificate Authority onto the XenApp Server. Transfer the Trusted Root CA certificate to the XenApp server.

From XenApp Server:

Login as administrator

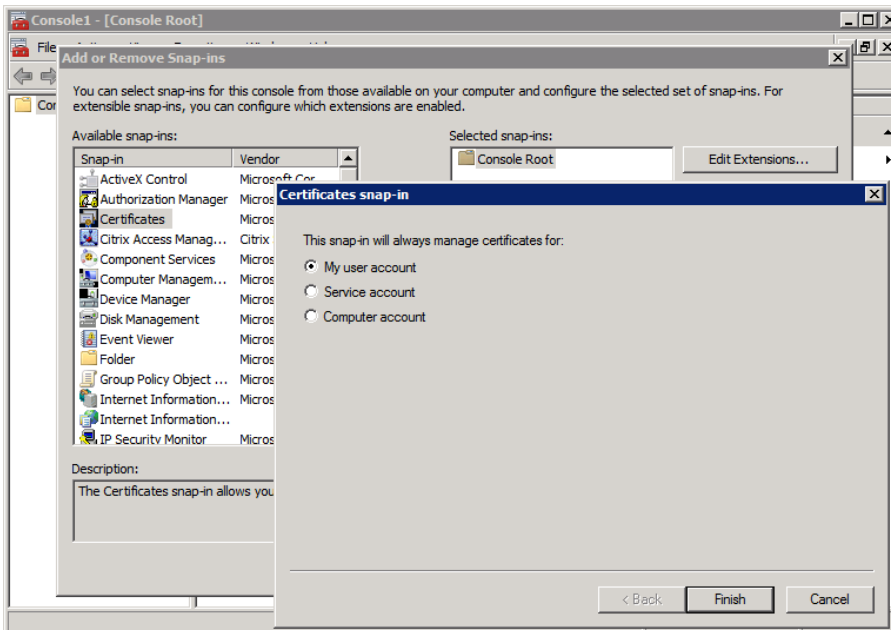
Start ➥ mmc.

File ➥

Add/Remove snap-in.

Certificates ➥

Local User.



From MMC:

Select Trusted Root Certificate Authorities.

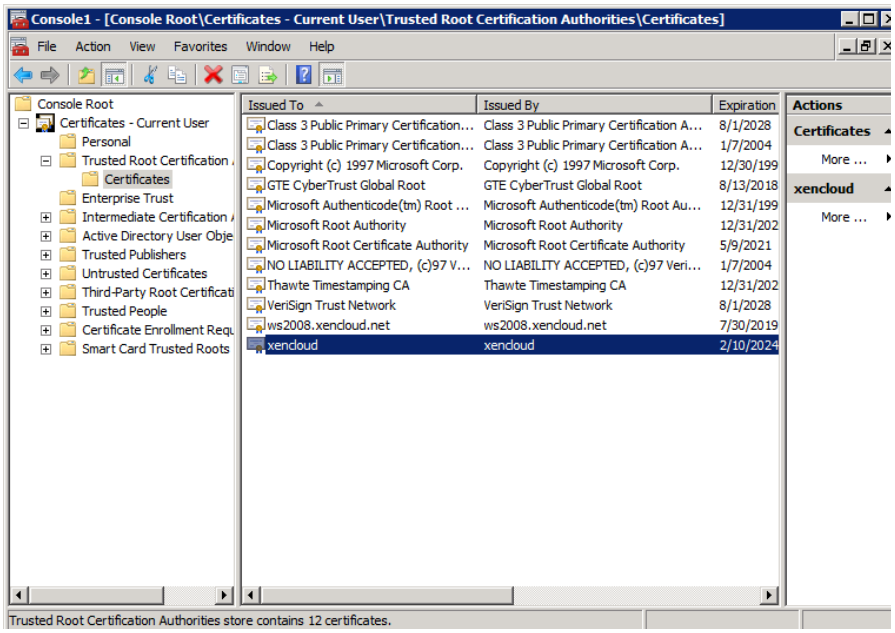
Action ➥

All Tasks ➥

Import.

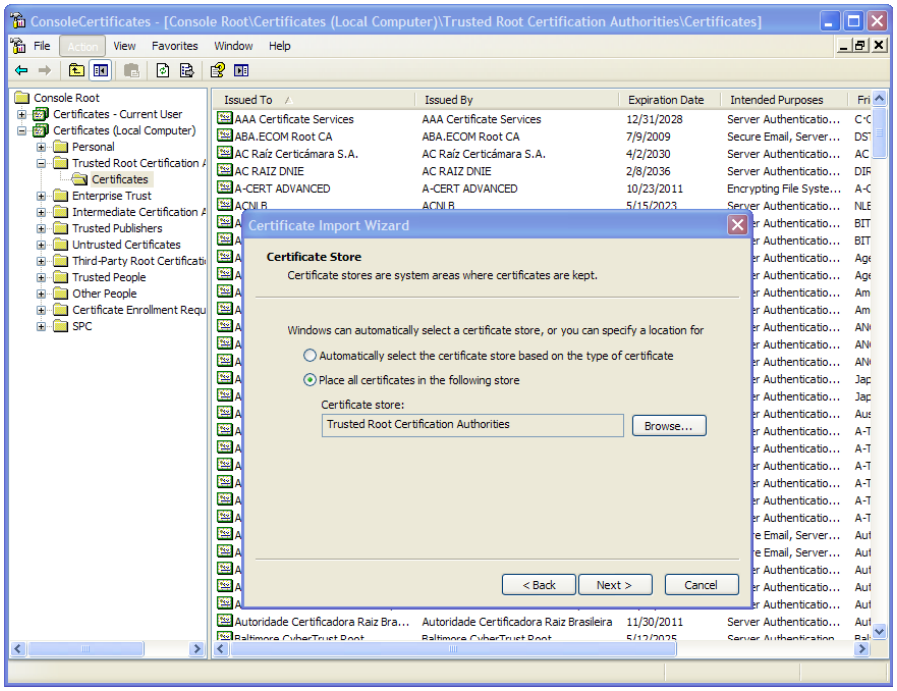
Import the CA Cert and place it in the Trusted Root Certificates Authorities container.

Note: Repeat this procedure for the Local Compute Account.



Client Browser

You will need to install the Certificate Authority certificate onto the clients machine. Transfer the Trusted Root CA certificate to the client device.



From XenApp Server:

Start ➥ mmc.

File ➥

Add/Remove snap-in.

Certificates ➥

Computer Account.

From MMC:

Select Trusted Root Certificate Authorities.

Action ➥

All Tasks ➥

Import.

Import the CA Cert and place it in the Trusted Root Certificates container.

Citrix Access Gateway

Configuration - Web Interface

You will need to configure the Citrix Access Gateway to act as a proxy to the XenApp Web Interface.

Open the Access Gateway Administration Tool:

AG Cluster ↪

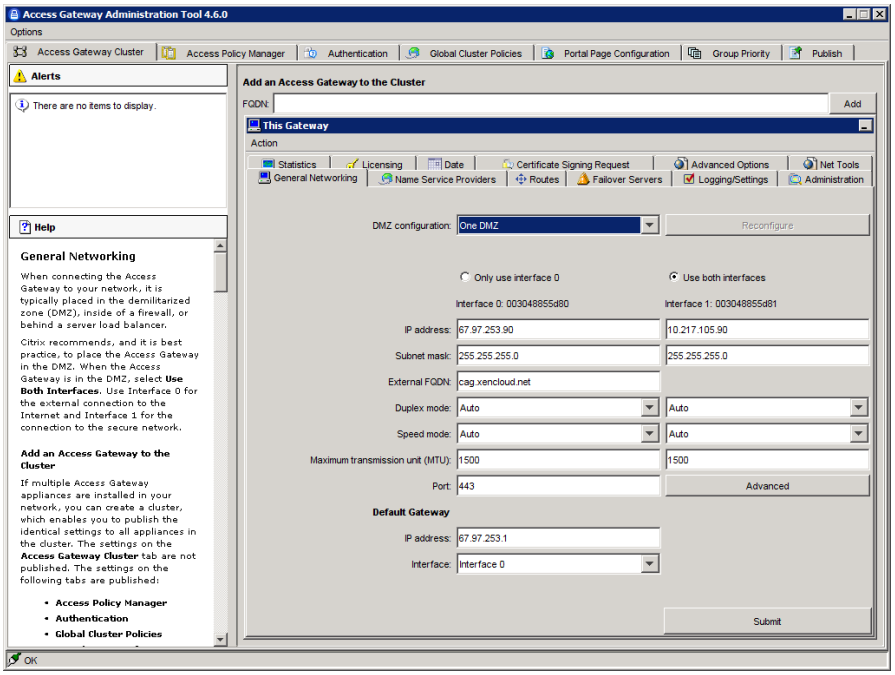
This Gateway ↪

General Networking.

Note: External FQDN:

1) Must match the CN on the Server Certificate

2) Must be the public DNS entry that is used to access the CAG.

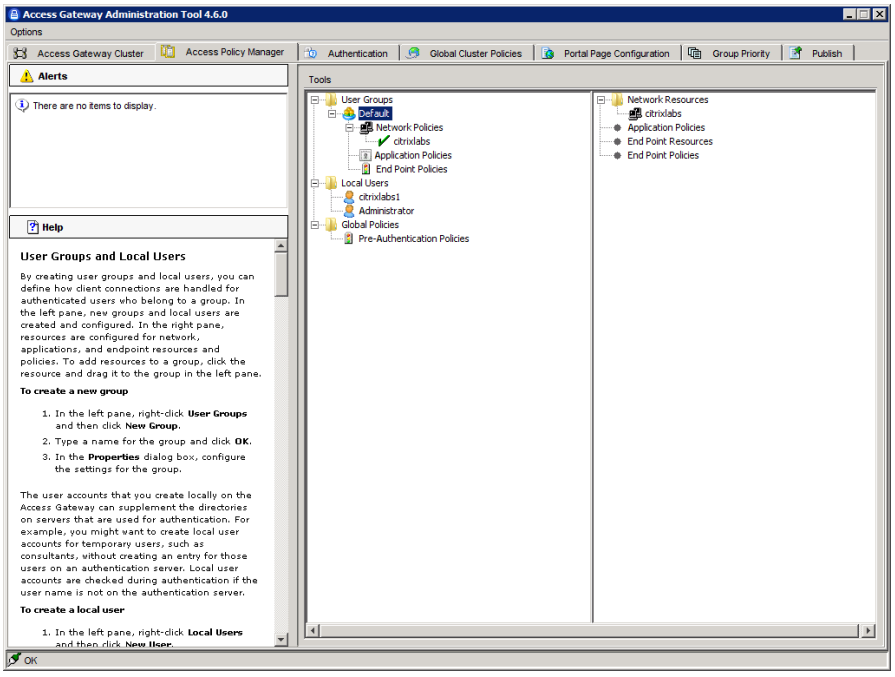


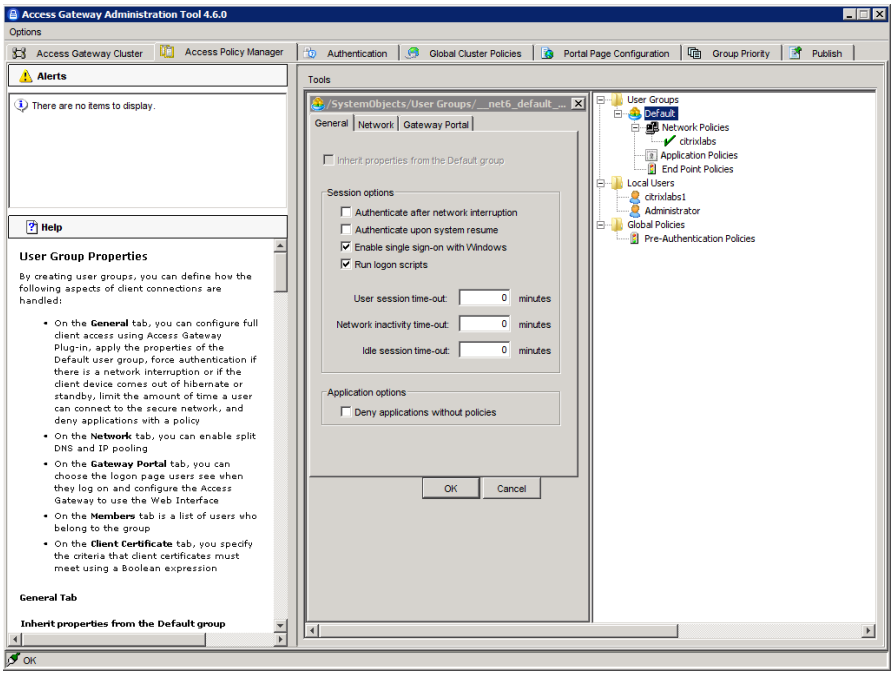
From Gateway Administration Tool:

Access Policy Manager:

Create a user group named ‘Default’.

The same ‘Default’ user group must be defined in Active Directory, and the users that will login through this CAG will need to be a member of the ‘Default’ group.



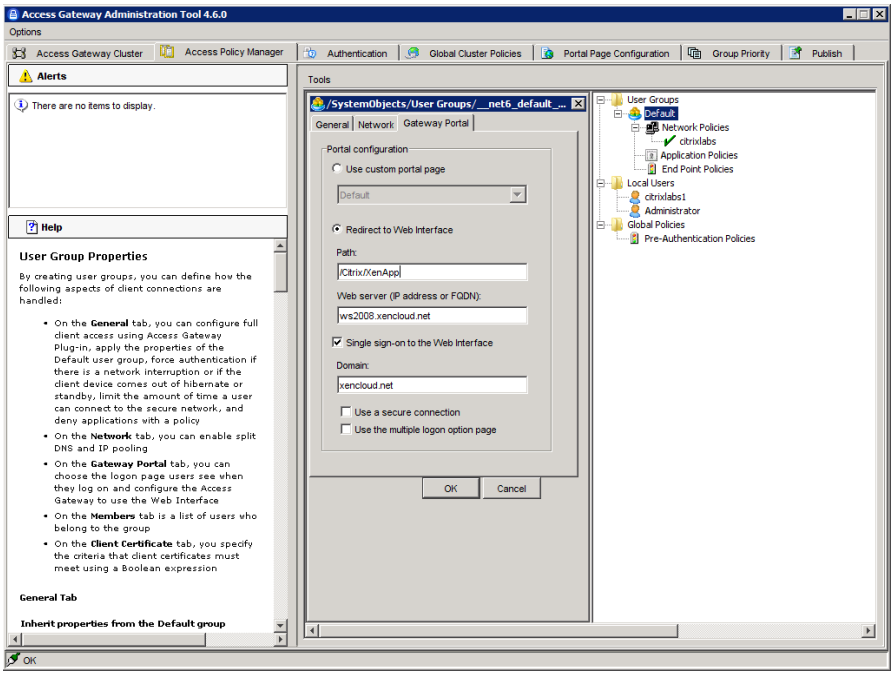


From Access Policy Manager:

Right-click the 'Default' user group, and select properties.

Enable Single Sign-On with Windows.

Enable Run Logon Scripts.



Select the 'Gateway Portal' Tab:

Redirect to Web Interface:

/Citrix/XenApp

Web Server (FQDN):

<XenApp webserver fqdn>

Enable Single Sign-On to the Web Interface.

Domain:

<the top level domain>

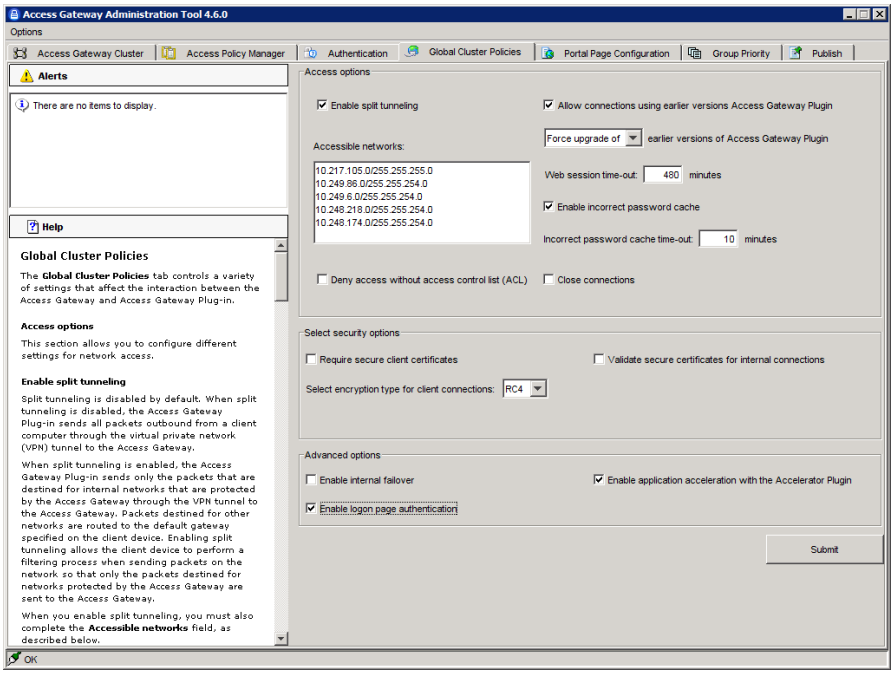
Select 'Ok'.

You will need to configure the Citrix Access Gateway to allow login through the web page at the CAG.

From the Access Gateway Administration Tool:

Global Cluster Policies:

Enable Logon Page Authentication.



Citrix Access Gateway

Configuration - XenApp Plugin

You will need to configure the Citrix Access Gateway to act as a proxy to the XenApp Plugin Client.

Open the Access Gateway Administration Tool:

AG Cluster ↪

This Gateway ↪

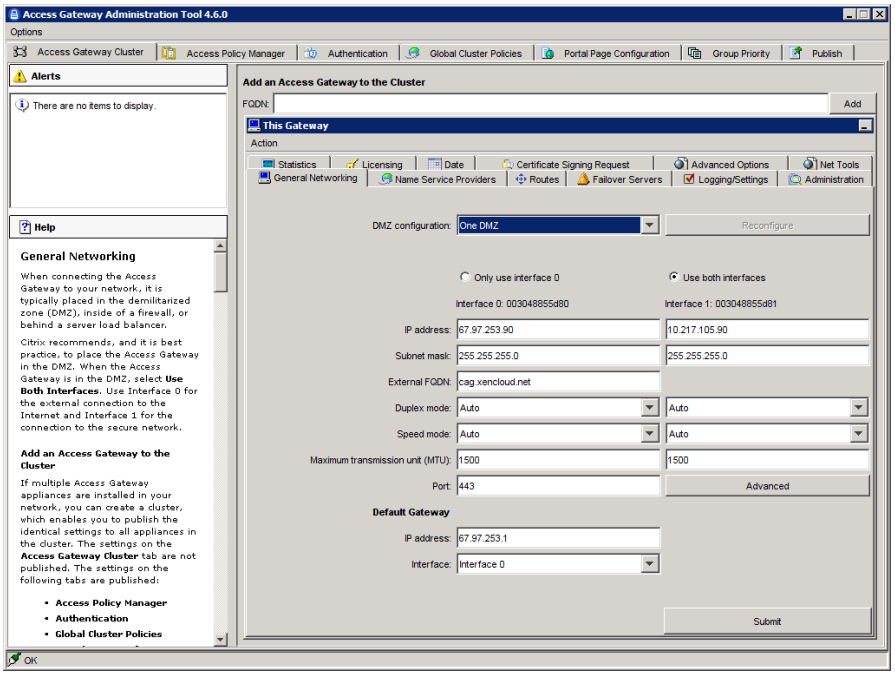
General Networking.

Note: External FQDN:

1) Must match the CN on the Server Certificate

2) Must be the public DNS entry that is used to access the CAG.

In this example the CN on the Server Certificate and the DNS entry name is cag.xencloud.net.

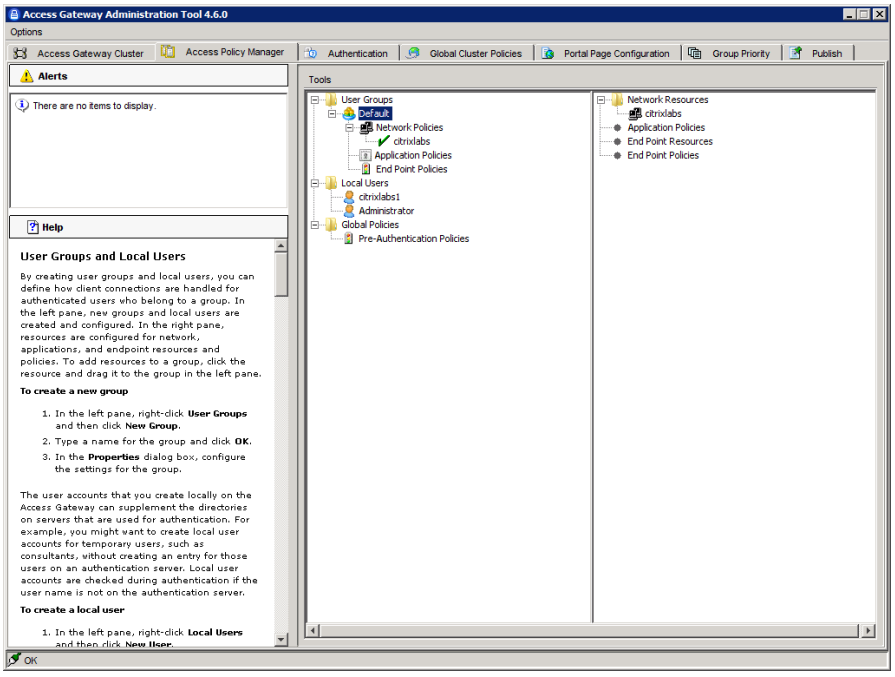


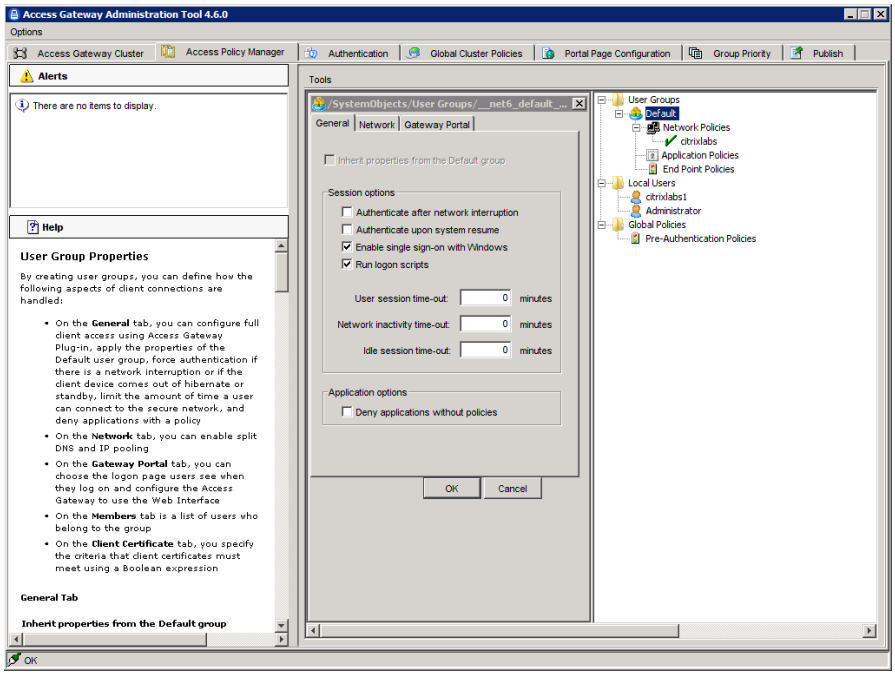
From Gateway Administration Tool:

Access Policy Manager:

Create a user group named 'Default'.

The same 'Default' user group must be defined in Active Directory, and the users that will login through this CAG will need to be a member of the 'Default' group.



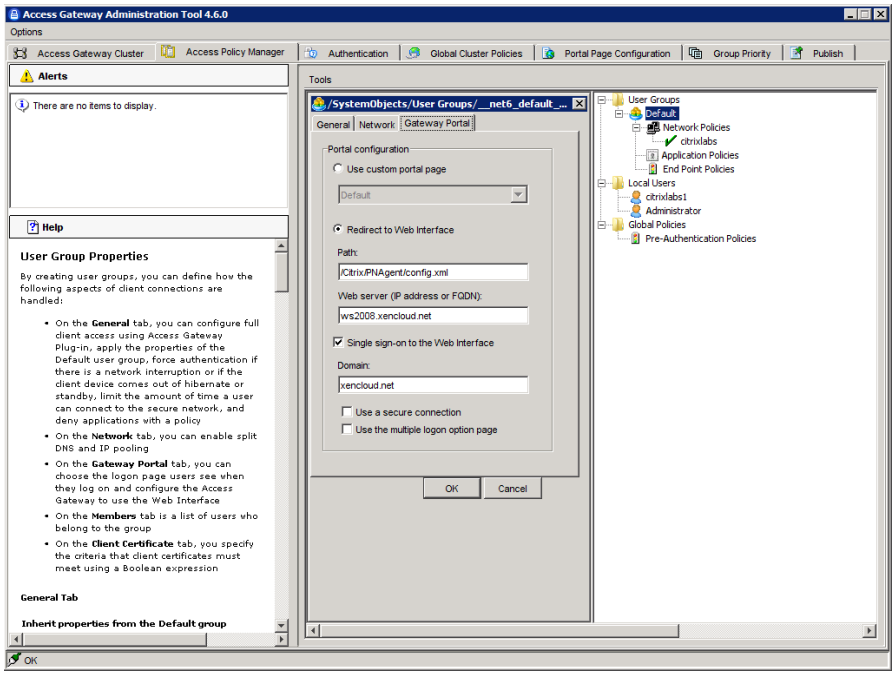


From Access Policy Manager:

Right-click the 'Default' user group, and select properties.

Enable Single Sign-On with Windows.

Enable Run Logon Scripts.



Select the 'Gateway Portal' Tab:

Redirect to Web Interface:

/Citrix/PNAgent/config.xml

Web Server (FQDN):

<XenApp webserver fqdn>

Enable Single Sign-On to the Web Interface.

Domain:

<the top level domain>

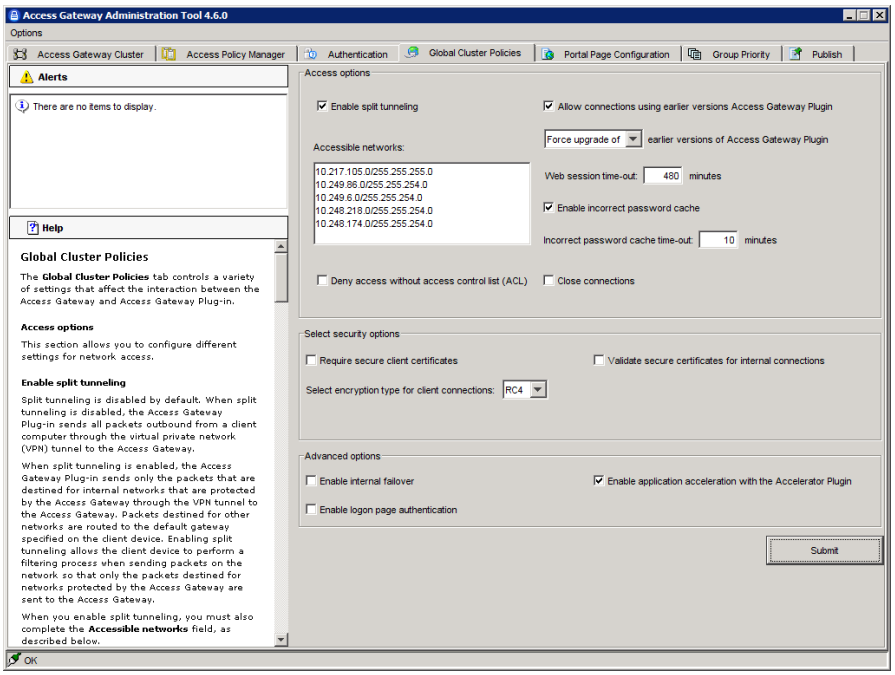
Select 'Ok'.

From the Access Gateway Administration Tool:

Global Cluster Policies:

Disable Logon Page Authentication.

You will need to configure the Citrix Access Gateway to NOT allow login through the web page at the CAG, because the XenApp Plugin on the client machine will be doing the logon authentication.



Citrix Access Gateway

Configuration - LDAP

You will need to configure the Citrix Access Gateway to use LDAP between the CAG and Microsoft Active Directory, for Authentication and Authorization. This configuration applies to both a Web Interface deployment and a Citrix XenApp Client deployment.

From Access Gateway Administration Tool:

Authentication Tab:

Note: Delete the existing 'Default' Realm. Add a new Realm named 'Default'. Select LDAP Authentication.

IP Address or FQDN: <ip address>

Port: 389

Allow unsecure connection:

<optional>

Admin bind DN:

cn=Administrator,cn=Users,dc=<domain>,dc=<tld indicator>

Admin Password:

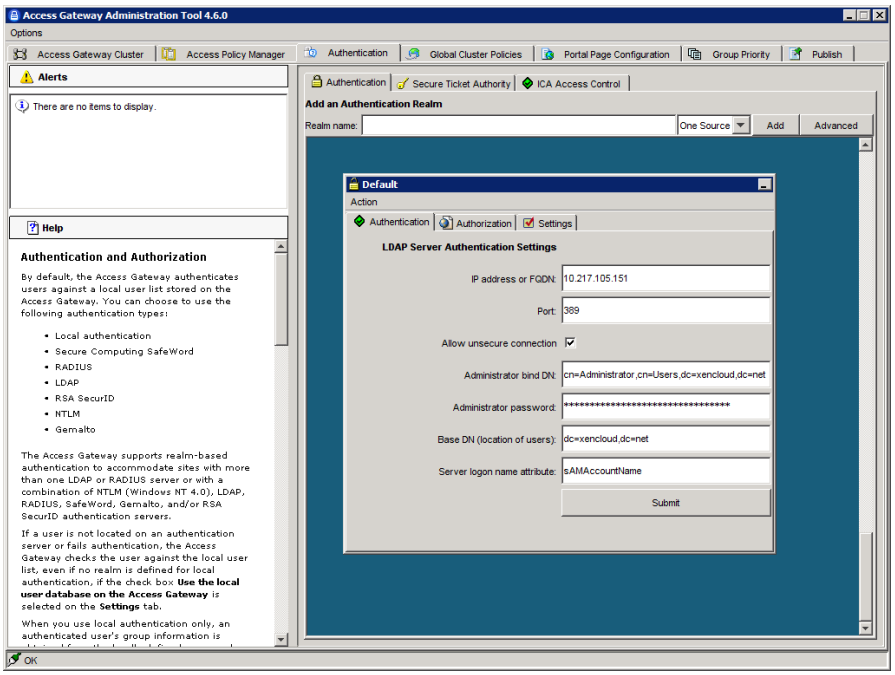
<password>

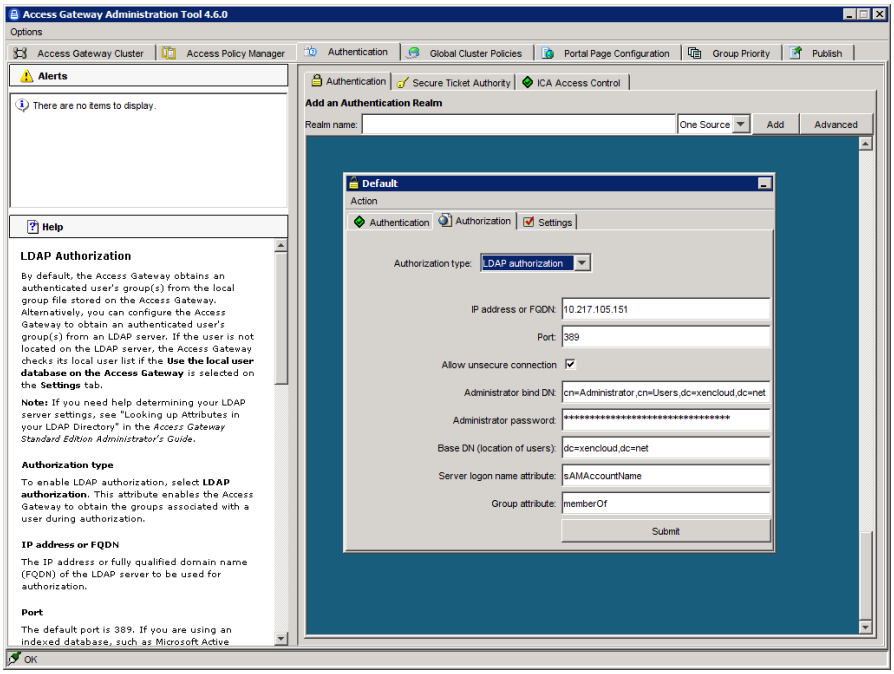
Base DN:

dc=<domain>,dc=<tld indicator>

Server logon attribute:

sAMAccountName





From Access Gateway Administration Tool:

Authorization Tab:

IP Address or FQDN: <ip address>

Port: 389

Allow unsecure connection:

<optional>

Admin bind DN:

cn=Administrator,cn=Users,dc=<domain>,dc=<tld indicator>

Admin Password:

<password>

Base DN:

dc=<domain>,dc=<tld indicator>

Server logon attribute:

sAMAccountName

Group attribute:

memberOf

Select ‘Submit’

Configuration - STA

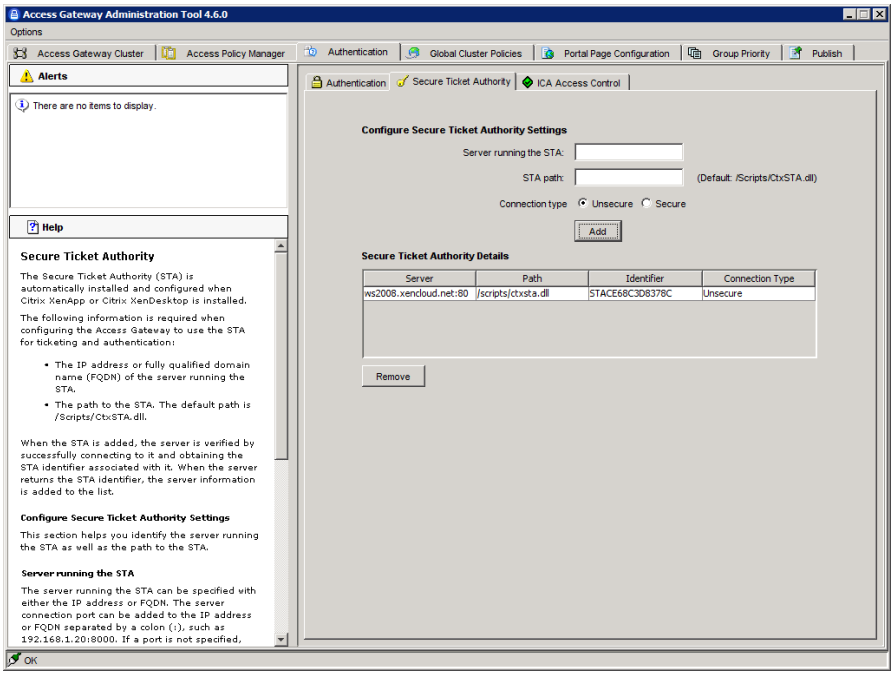
You will need to configure the Citrix Access Gateway to use the Secure Ticket Authority for your XenApp farm. This configuration applies to both a XenApp Web Interface deployment and a Citrix XenApp Client deployment.

From Access Gateway Administration Tool:

Authentication ↪

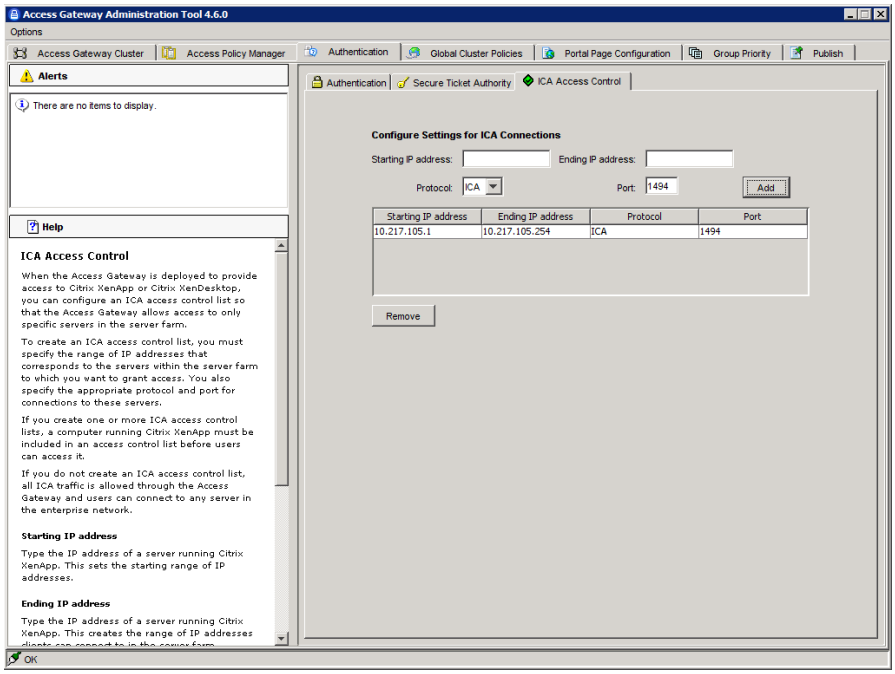
Secure Ticket Authority

Add the STA of the XenApp server farm.



Configuration - ICA

You will need to configure the Citrix Access Gateway to allow ICA connections to the subnet of the XenApp farm. This configuration applies to both a Web Interface deployment and a Citrix XenApp Client deployment.



From Access Gateway Administration Tool:

Authentication ↪

ICA Access Control

Add the IP Addresses that will user ICA.

Testing Web Interface

Once you have installed all of the components of this solution, you should test it, by publishing a test application such as Notepad, in XenApp, then connect and see if Single Sign-On works, and that the application launches.

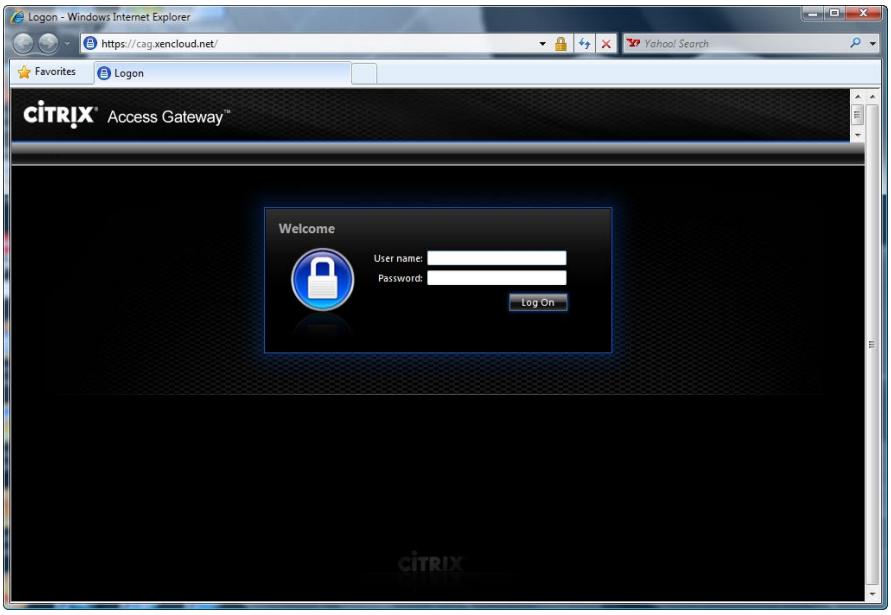
From a web browser, enter the FQDN of the public vip:

In this example it is:

https://cag.xencloud.net

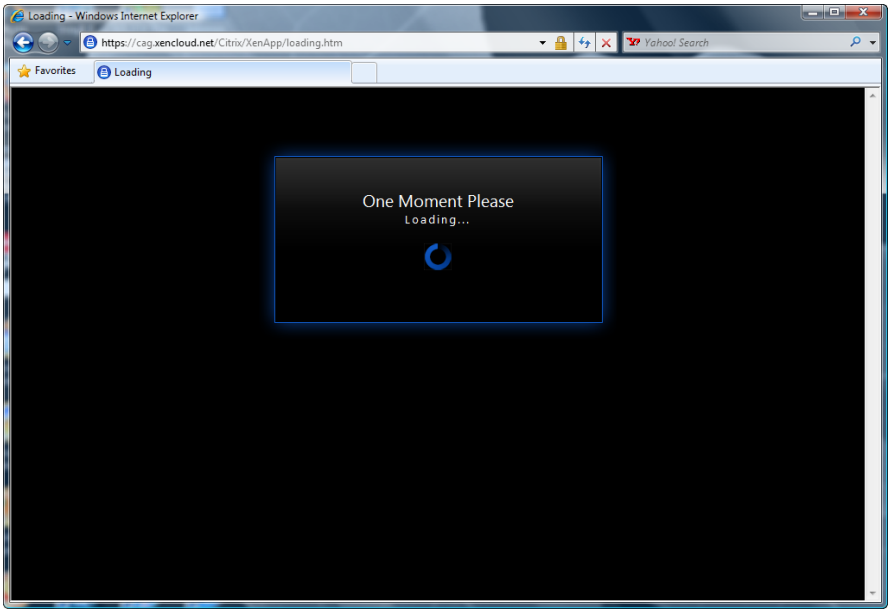
Enter login credentials, which are consequently configured in Active Directory. The user for Web Interface has been added as a memberOf the 'iproxy' group in Active Directory.

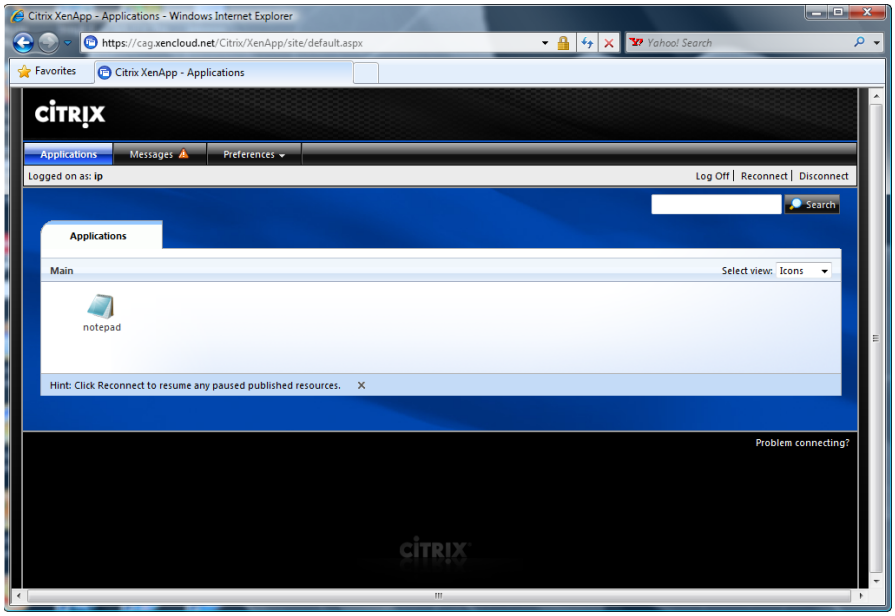
Because we have configured this solution for Single Sign-On, you should only have to enter credentials one time.



Web Interface:

Wait for the Web Interface to load.

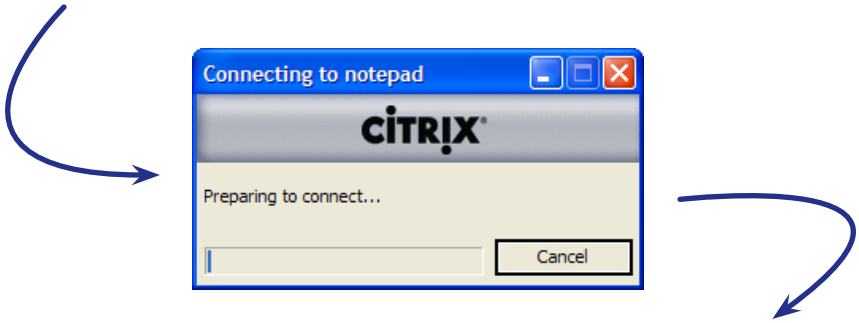


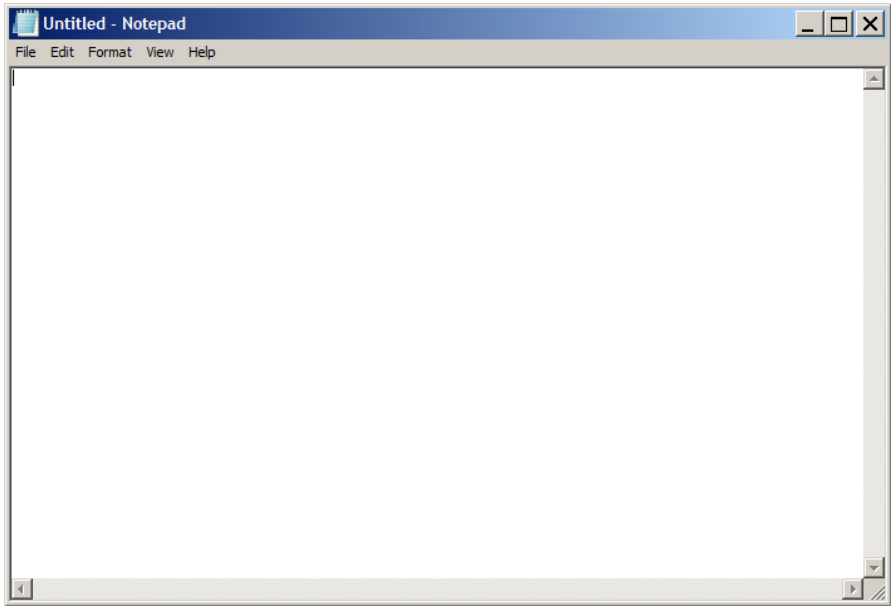


Application:

At this point you should see the Web Interface with the application that is published for this user.

Launch the application.





Application Delivery:

The application should be delivered or proxied from XenApp, through the Citrix Access Gateway, to the end user.

Testing XenApp Plugin

Once you have installed all of the components of this solution, you should test it, by publishing a test application such as Notepad, in XenApp, then connect with Citrix XenApp Client and see if Single Sign-On works, and that the application launches.

Download the Citrix:

Open a web browser, and navigate to the downloads section of http://citrix.com.

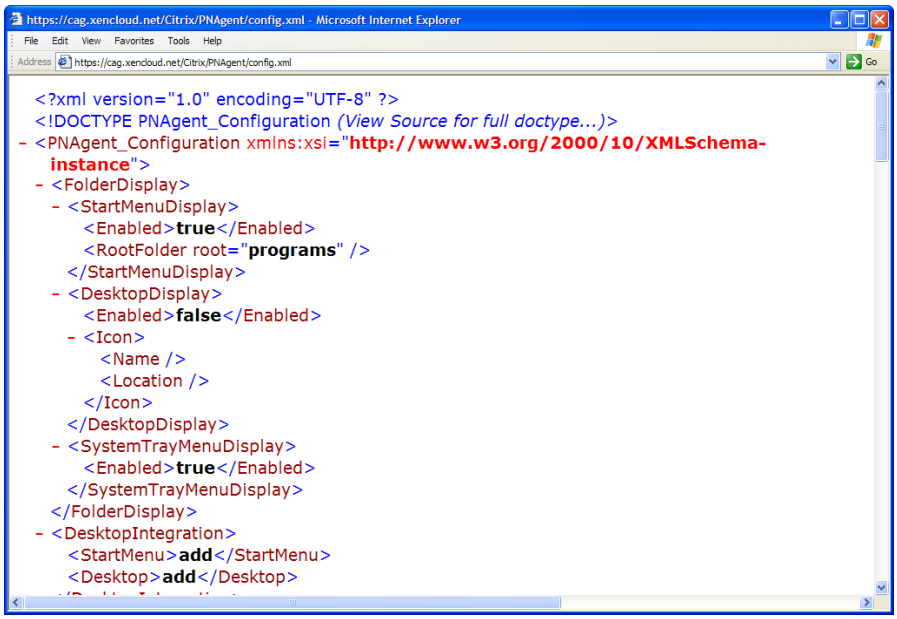
Download and install the XenApp Plugin for Hosted Apps.

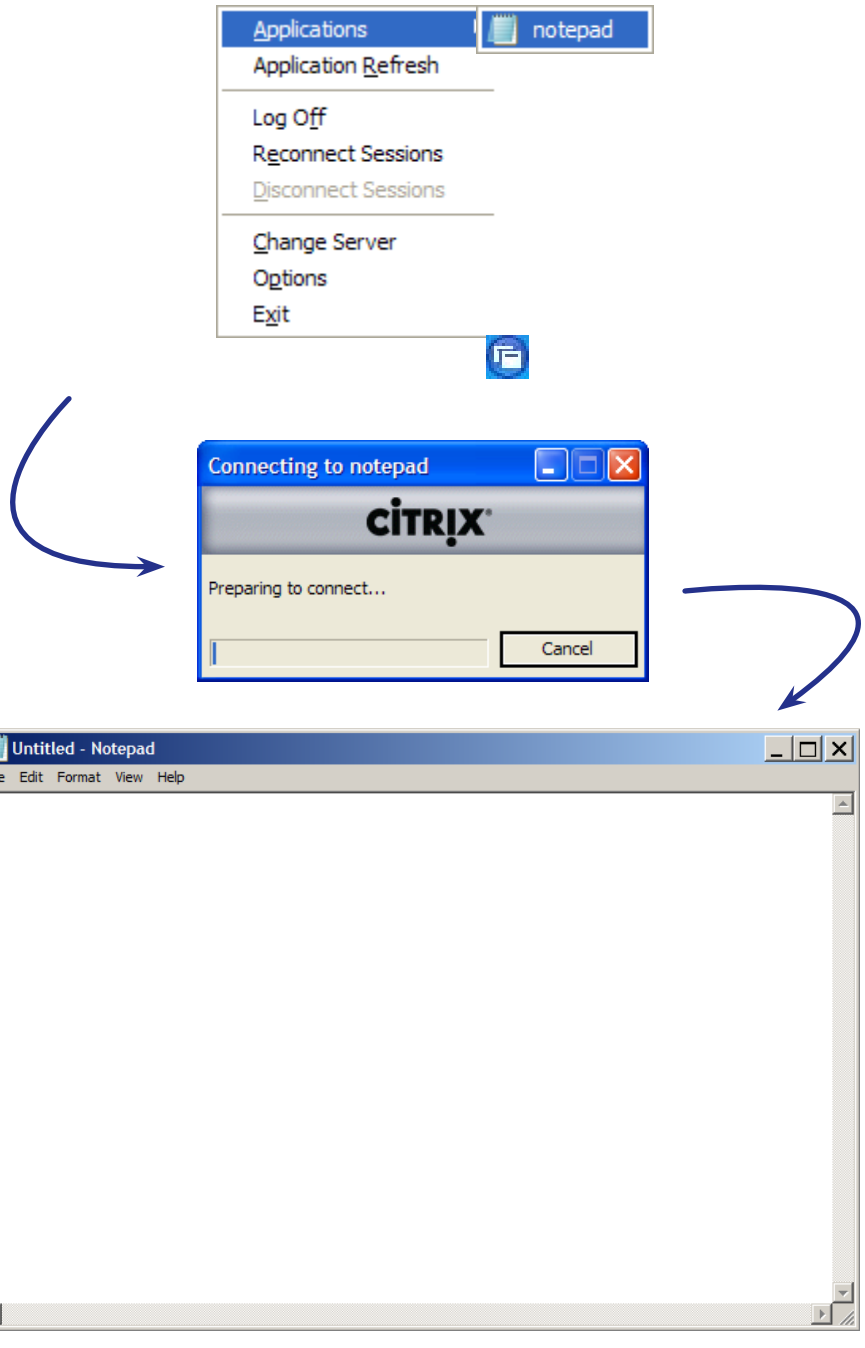
Enter login credentials, which are consequently configured in Active Directory. The user for XenApp Plugin has been added as a memberOf the 'iproxy2' group in Active Directory.

Because we have configured this solution for Single Sign-On, you should only have to enter credentials one time.

Optional Test:

If you open a web browser to cag.xencloud.net, the XenApp Server will return the .xml configuration file.





Application:

At this point you should see the Citrix XenApp Client with the application that is published for this user.

Launch the application.

Application Delivery:

The application should be delivered or proxied from XenApp, through the Citrix Access Gateway, to the end user.

Worldwide Headquarters
Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309, USA
T +1 800 393 1888
T +1 954 267 3000

Americas
Citrix Silicon Valley
4988 Great American Parkway
Santa Clara, CA 95054, USA
T +1 408 790 8000

Europe
Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen, Switzerland
T +41 52 635 7700

Asia Pacific
Citrix Systems Hong Kong Ltd.
Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central, Hong Kong
T +852 2100 5000

Citrix Online Division
6500 Hollister Avenue
Goleta, CA 93117, USA
T +1 805 690 6400

www.citrix.com

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of *Fortune* Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was $1.6 billion.
The information in this publication is subject to change without notice.