



Deployment Guide

ICA Proxy for
XenApp & XenDesktop for
Citrix Receiver for
iPhone, iPod, iPad

*Access Gateway Enterprise Edition
(NetScaler AGEE)*

Table of Contents

- Introduction3
- Solution Requirements4
- Prerequisites.....4
- Network Diagram5
- XenApp Services Site.....7
- NetScaler AGEE Certificates12
 - Self Signed Certificates12
- NetScaler AGEE13
 - Public VIP13
- NetScaler AGEE16
 - Private VIP16
- NetScaler AGEE21
 - Proxy Group, Session Profile21
 - Secure Ticket Authority26
- Testing Citrix Receiver27

Introduction

A member of the Citrix Delivery Center™ product family, Citrix NetScaler is a purpose-built web application delivery solution that accelerates application performance up to five times while improving security and reducing web infrastructure costs.

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. 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).

Citrix XenDesktop™, a member of the Citrix Delivery Center™ product family, is a comprehensive desktop delivery system that allows customers to virtualize Windows desktops in the datacenter and deliver them on-demand to office workers in any location. By dynamically assembling each user's unique personal desktop from new, pristine components each time they log on, XenDesktop offers an unparalleled end-user experience, dramatically simplifies desktop management and reduces the cost of traditional desktop computing by up to 40 percent. XenDesktop Enterprise and Platinum Editions tightly integrates the industry's most proven application virtualization via the XenApp for Virtual Desktops feature.

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.

Citrix Receiver is a lightweight software client that makes accessing virtual applications and desktops on any device as easy as turning on your TV. Citrix Receiver provides iPhone users with fast, secure, and easy access to their enterprise applications. With Citrix Receiver for iPhone, users can access any XenApp application or any XenDesktop from their Apple iPhone, iPad or iPod Touch.

Solution Requirements

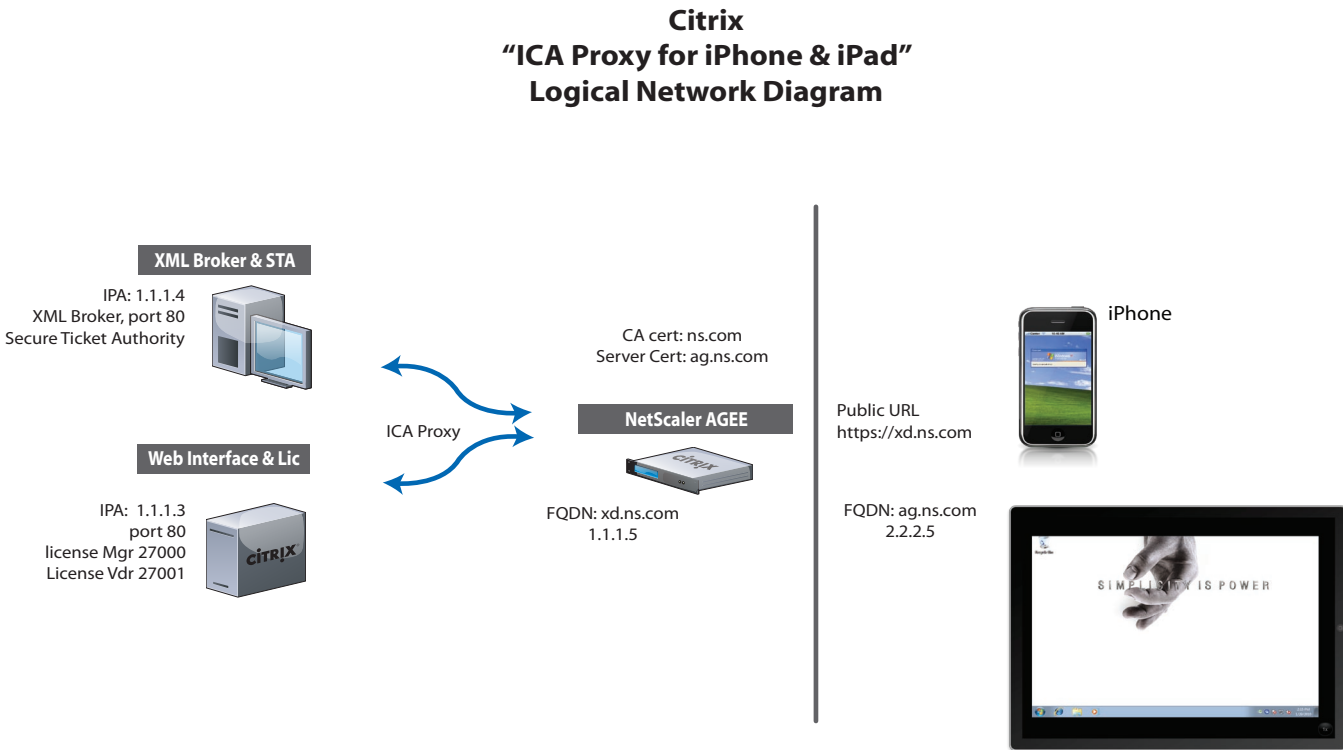
- Windows Desktops delivered to iPhone, iPod or iPad
- Windows Applications delivered to iPhone, iPod, iPad
- ICA Proxy for Citrix Receiver iPhone, iPod & iPad
- ICA Proxy for XenApp & XenDesktop
- ICA Proxy for NetScaler Access Gateway Enterprise Edition - AGEE

Prerequisites

- Citrix NetScaler L4/7 Application Switch, version 9.1 build 101.5+ running Access Gateway (Quantity x 2 for High Availability)
- Citrix XenApp Server 5.0+ or XenDesktop 4.0+
- Microsoft Server with Active Directory
- iPhone Configuration Utility
- iPhone OS 3.0+, iPad OS
- Citrix Receiver for iPhone v2.1+

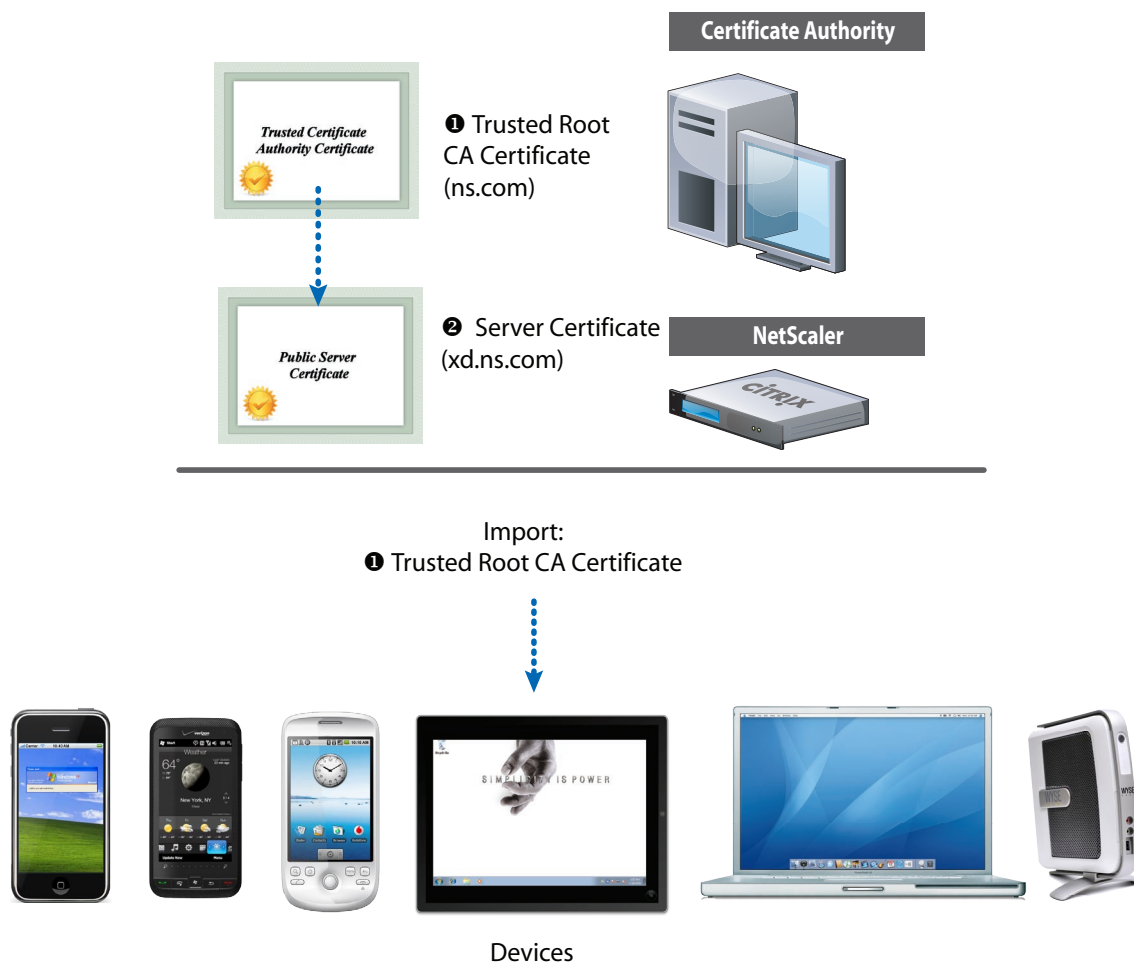
Network Diagram

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



| VLAN Legend | NetScaler |
|--------------------|--|
| <div></div> VLAN 1 | VLAN 1 (Private): Interface 1/1, Untagged NSIP: 1.1.1.10 / 24 SNIP: 1.1.1.1 / 24 private-VIP: 1.1.1.5 / 24 |
| <div></div> VLAN 2 | VLAN 2 (Public): Interface 1/8, Untagged SNIP: 2.2.2.2 / 24 public-VIP: 2.2.2.5 / 24 |

Citrix "Receiver / Access Gateway" Certificate Chain of Trust



XenApp Services Site

Once you have installed Citrix Web Interface Management you will need to configure it such that it will work with the Citrix NetScaler in an ICA Proxy deployment. Creating a XenApp service will publish the XenApp applications or XenDesktop through the Citrix client, such as XenApp client or Citrix Receiver for iPhone or iPad.

From the Citrix Web
Interface Management
console:

XenApp Services Sites ➔

Action ➔

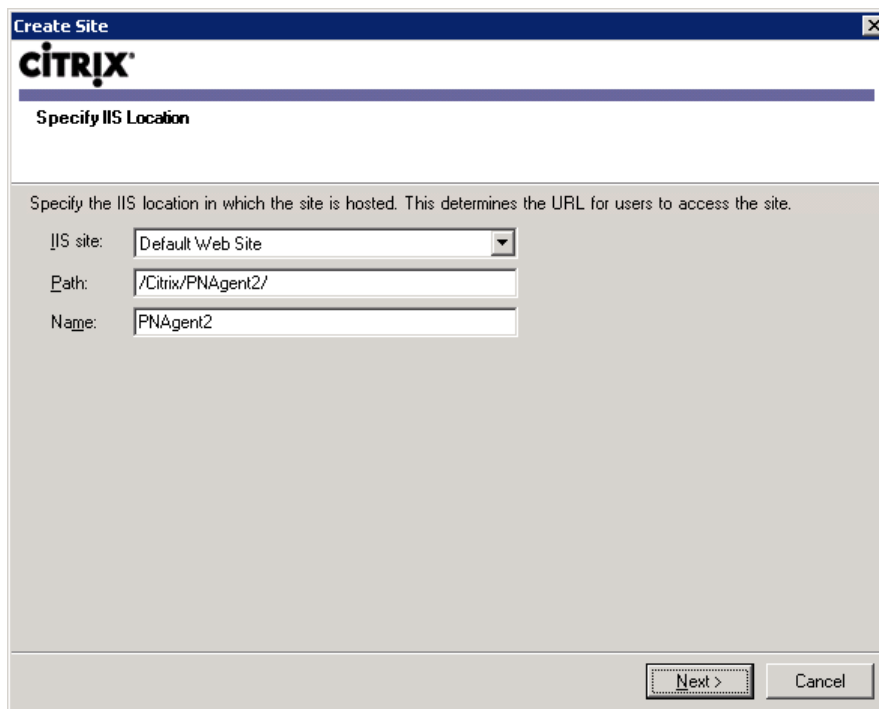
Create Site.

IIS Location:

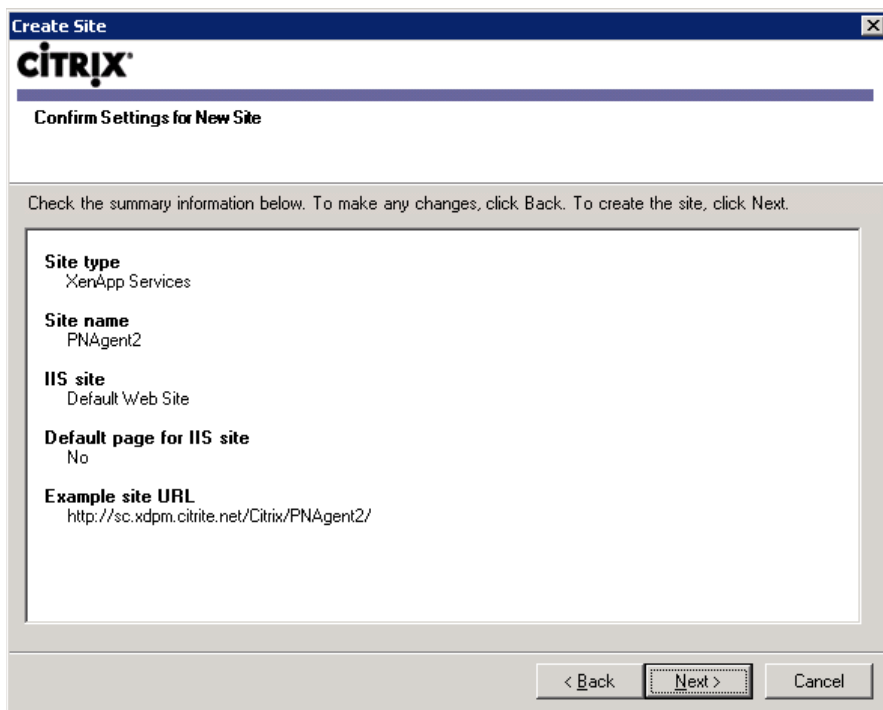
IIS Site: Default Web Site

Path: /Citrix/PNAgent2/

Name: PNAgent2



The screenshot shows a 'Create Site' dialog box with the Citrix logo at the top. Below the logo, the title 'Specify IIS Location' is displayed. A descriptive text states: 'Specify the IIS location in which the site is hosted. This determines the URL for users to access the site.' There are three input fields: 'IIS site:' with a dropdown menu showing 'Default Web Site', 'Path:' with a text box containing '/Citrix/PNAgent2/', and 'Name:' with a text box containing 'PNAgent2'. At the bottom right, there are two buttons: 'Next >' and 'Cancel'.



Create Site

CITRIX

Confirm Settings for New Site

Check the summary information below. To make any changes, click Back. To create the site, click Next.

| | |
|----------------------------------|--|
| Site type | XenApp Services |
| Site name | PNAgent2 |
| IIS site | Default Web Site |
| Default page for IIS site | No |
| Example site URL | http://sc.xdpm.citrix.net/Citrix/PNAgent2/ |

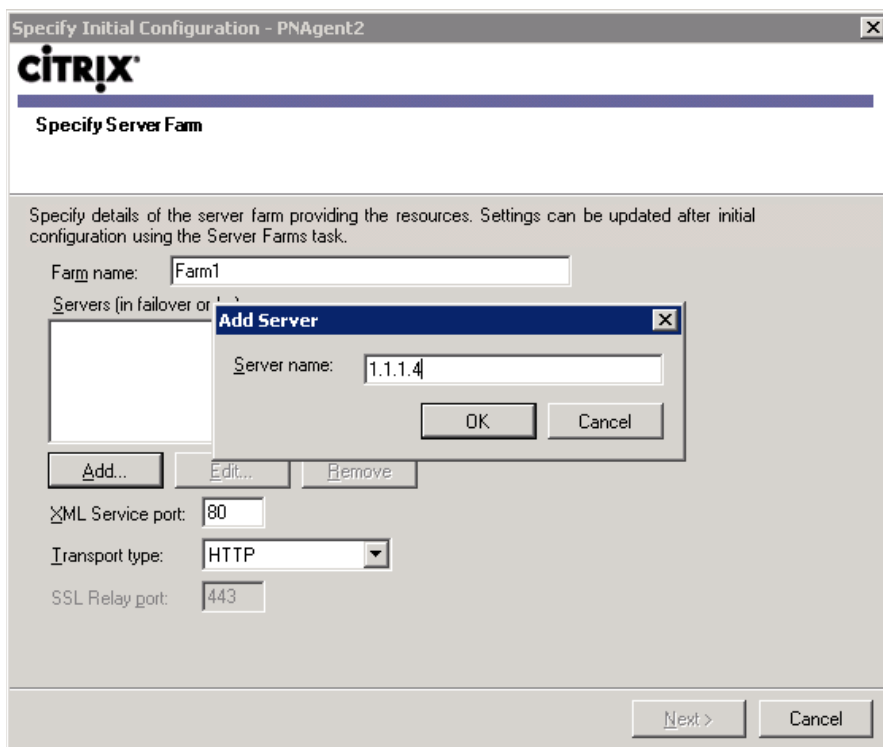
< Back **Next >** Cancel

Confirm:

Next.

Finish.

Configure Site Now.



Specify Initial Configuration - PNAgent2

CITRIX

Specify Server Farm

Specify details of the server farm providing the resources. Settings can be updated after initial configuration using the Server Farms task.

Farm name: Farm1

Servers (in failover order):

| |
|--|
| |
|--|

Add... Edit... Remove

XML Service port: 80

Transport type: HTTP

SSL Relay port: 443

Next > Cancel

Specify Server Farm:

Farm Name: <your farm name>

Servers: <Hostname or IP Address>

Note: this is the Desktop Delivery Controller that provides the server instances.

Resource Type:

Online

Next

Specify Initial Configuration - PNAgent2

CITRIX®

Select Published Resource Type

Select the types of resources available to users. Settings can be updated after initial configuration using the Published Resource Types task.

☒ **Online**
Users access applications, content, and desktops hosted on remote servers.

☐ **Offline**
Users stream applications to their desktops and open them locally. Users must install the Citrix offline plug-in.

☐ **Dual mode**
Users access both offline applications and online applications, content, and desktops, all on the same site.

< Back **Next >** Cancel

Confirm:

Finish

Specify Initial Configuration - PNAgent2

CITRIX®

Confirm Settings

Check the summary information below. To make any changes, click Back.

Farm name
Farm1

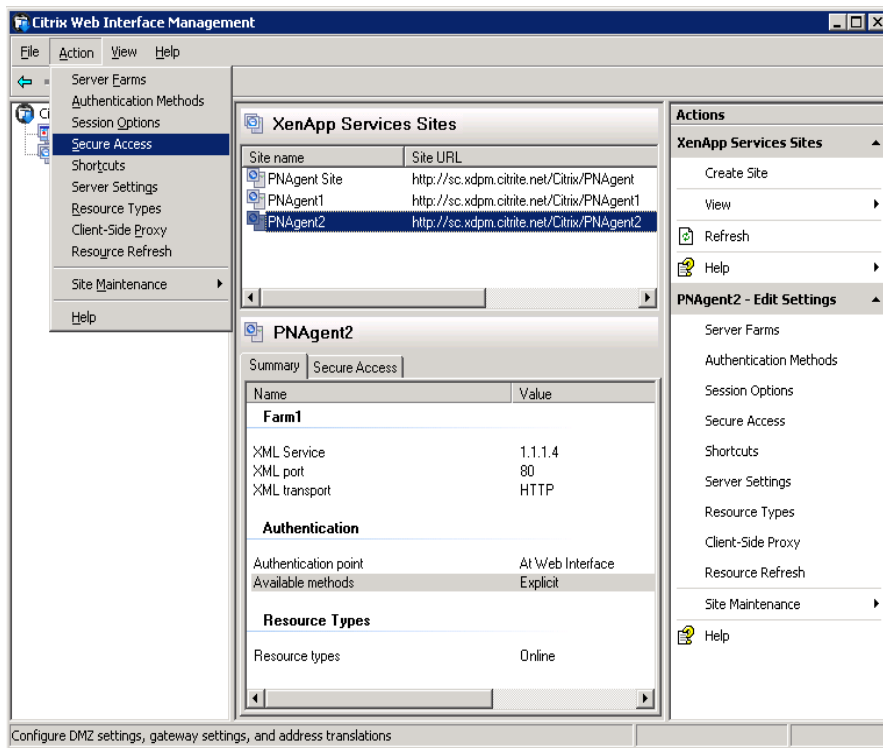
Servers
1.1.1.4

XML Service port
80

XML Service transport type
HTTP

Resource type
Online

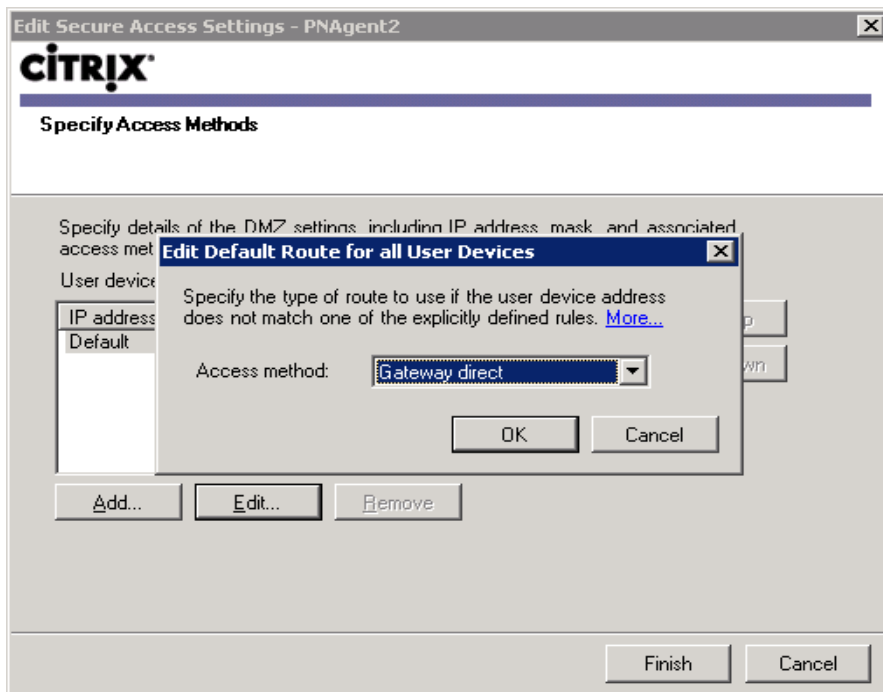
< Back **Finish** Cancel



From Citrix Web Interface Management:

Actions ➔

Secure 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 AG, which in this example is ag.ns.com, and resolves to 2.2.2.5.

Edit Secure Access Settings - PNAgent2

CITRIX

Specify Gateway Settings

Specify gateway server details for any user devices that access this site through the Access Gateway or Secure Gateway. [More...](#)

Address (FQDN):

Port:

☐ Enable session reliability

☐ Request tickets from two STAs, where available

< Back Next > Cancel

Secure Ticket Authority:

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

Select Finish

Edit Secure Access Settings - PNAgent2

CITRIX

Specify Secure Ticket Authority Settings

Specify gateway server details for any user devices that access this site through the Access Gateway

Add Secure Ticket Authority URL

Secure Ticket Authority URL
(Citrix recommends using FQDN for server names):

Example: http[s]://servername.fullyqualifieddomain/scripts/ctxsta.dll

OK Cancel

Add... Edit... Remove

☒ Use for load balancing

Bypass failed servers for:

< Back Finish Cancel

NetScaler AGEE

Certificates

Self Signed Certificates

You will need two certificates. A self signed Root CA, and a server certificate unless you purchased a certificate for example from Verisign, then you only need the server certificate.

Follow the deployment guide located here to create a Self Signed Server Certificate and download a Root CA Certificate: <http://community.citrix.com/display/ocb/2010/05/10/Citrix+Receiver+Certificate+Chain>

Link them together and bind them to the Access Gateway VIP.

NetScaler AGEE

Public VIP

Create the public facing VIP that users will connect to when they type in <https://xd.ns.com> into their browser Uniform Resource Locator (URL).

From the NetScaler GUI:

NetScaler ➔

Access Gateway ➔

Access Gateway Wizard.

Create Virtual Server:

Type: New

IP Address: 2.2.2.5

Port: 443

Name: public-vip

Next.

The screenshot shows the 'Access Gateway Wizard' window with the 'Create or choose a virtual server' step selected in the left-hand navigation pane. The main area contains a form with the following fields:

- Radio buttons:** 'New' (selected) and 'Existing'.
- IP Address:** A text box containing '2 . 2 . 2 . 5' and a checkbox for 'IPv6'.
- Port:** A text box containing '443'.
- Virtual Server Name:** A text box containing 'public-vip'.

At the bottom of the window are buttons for '< Back', 'Next >', and 'Close'.

Server Certificate:

Options: Use an installed certificate and private key pair

Certificate: xdserver.keypair

Next.

Note:

1) xd.ns.com must resolve to ip address 2.2.2.5 &

2) Common Name in Server Certificate xdserver.cer must contain xd.ns.com.

The screenshot shows the 'Access Gateway Wizard' window with the 'Specify a server certificate' step selected in the left-hand navigation pane. The main area contains the following elements:

- Text:** 'Choose a certificate from the list of installed certificates.'
- Form:**
 - Certificate Options:** A dropdown menu set to 'Use an installed certificate and private key pair'.
 - Server Certificate:** A dropdown menu set to 'xdserver.keypair'.
- Link:** A blue link labeled 'Create a Certificate Signing Request'.

At the bottom of the window are buttons for 'Skip >', '< Back', 'Next >', and 'Close'.

Access Gateway Wizard

Name Service Providers
For name resolution, configure the DNS or WINS servers.

Configured DNS Server* 1.1.1.9

WINS Server IP Address . . .

Name Lookup Priority ☐ WINS ☒ DNS

Retry DNS Connection (number of times)* 5

Help Skip > < Back Next > Close

DNS:

DNS Server: 1.1.1.6

Note:

Enter the ip address of your DNS server.

Next.

Access Gateway Wizard

Configure authentication
Select the authentication type for your users. If you are using local authentication, create a user name and password. To create additional users, in the navigation pane, click Users.

Select an authentication type LOCAL

User Name* deletethisuser

Password

Enter this keyword to create or change the user's password.

Help Skip > < Back Next > Close

Authentication:

Type: Local

User: deletethisuser1

Pass: <password>

Note: Because we are authenticating at the Web Interface, set this to Local authentication.

You are required to create a user, but you can delete it later.

Next.

Additional:

Authorization: Deny

Redirect:

Redirect to secure web address

Address:

https://xd.ns.com

Next.

Access Gateway Wizard

Configure additional settings

You can configure authorization settings and port redirection on this page. With port redirection, if users log on to the Web page using an unsecure connection on port 80, they are redirected to a secure connection (usually on port 443).

Introduction

- Create or choose a virtual server
- Specify a server certificate
- Name Service Providers
- Configure authentication
- Configure additional settings**
- Configure clientless access
- Summary

Configure Authorization

☐ Allow ☒ Deny

Select authorization requirements for your users. Authorization is applied globally and can be overridden by configuring additional authorization policies. This setting can be changed in Access Gateway global settings.

Redirect Requests for Port 80 to a Secure Port

☒ Redirect to secure Web address

Type the secure Web address

Users might leave off the "s" in https:// when typing in a Web address to the Access Gateway. If this occurs, you can enable the request to automatically be redirected to a secure Web address.

Help Skip > < Back Next > Close

Clientless Access:

Use the Access Gateway Plugin and allow access scenario fallback.

Next.

Finish.

Access Gateway Wizard

Configure clientless access

You can configure clientless access on this page. Enter the host names of SharePoint servers to configure clientless access for SharePoint.

Introduction

- Create or choose a virtual server
- Specify a server certificate
- Name Service Providers
- Configure authentication
- Configure additional settings
- Configure clientless access**
- Summary

Clientless Access

☐ Access Gateway Plugin
Users are allowed to log on using the Access Gateway Plugin only.

☒ Use the Access Gateway Plugin and allow access scenario fallback
Users log on using the Access Gateway Plugin. If users fail an endpoint analysis scan, they are permitted to log on using clientless access with limited access to network resources.

☐ Allow users to log on using Clientless Access only
Users log on with a Web browser and are permitted limited access to network resources. [Configure Domains for Clientless Access](#)

Clientless Access Persistent Cookie

☐ Allow ☒ Deny ☐ Prompt
Disabling persistent cookies could prevent some features from working correctly, such as opening Microsoft Word, Excel or PowerPoint documents in SharePoint. Select Deny to work without these features, Allow for enabling persistent cookies, or Prompt to let users select an option.

Clientless Access for SharePoint

Host name of SharePoint server

Add Remove

Help Skip > < Back Next > Close

NetScaler AGEE

Private VIP

Create the private facing VIP that users will connect to when they type in `https://xd.ns.com` into their browser Uniform Resource Locator (URL).

The screenshot shows the 'Access Gateway Wizard' window with the 'Create or choose a virtual server' step selected in the left-hand navigation pane. The main area contains instructions and a form. The form has two radio buttons: 'New' (selected) and 'Existing'. Below them are input fields for 'IP Address' (1 . 1 . 1 . 5), 'Port*' (443), and 'Virtual Server Name*' (private-vip). There is also a checkbox for 'IPv6'. At the bottom are buttons for '< Back', 'Next >', and 'Close'.

From the NetScaler GUI:

NetScaler ➔

Access Gateway ➔

Access Gateway Wizard.

Create Virtual Server:

Type: New

IP Address: 1.1.1.5

Port: 443

Name: private-vip

Next.

The screenshot shows the 'Access Gateway Wizard' window with the 'Specify a server certificate' step selected in the left-hand navigation pane. The main area contains instructions and a form. The 'Certificate Options' dropdown is set to 'Use an installed certificate and private key pair'. There is a link 'Create a Certificate Signing Request'. Below, the 'Server Certificate' dropdown is set to 'xdserver.keypair'. At the bottom are buttons for 'Skip >', '< Back', 'Next >', and 'Close'.

Server Certificate:

Options: Use an installed certificate and private key pair

Certificate: xdserver.keypair

Next.

Note:

1) xd.ns.com must resolve to internal ip address 1.1.1.5 & (Do this with internal DNS)

2) Common Name in Server Certificate xdserver.cer must contain xd.ns.com.

DNS:

DNS Server: 1.1.1.9

Next.

Access Gateway Wizard

Name Service Providers
For name resolution, configure the DNS or WINS servers.

Introduction
Create or choose a virtual server
Specify a server certificate
Name Service Providers
Configure authentication
Configure additional settings
Configure clientless access
Summary

Configured DNS Server* 1.1.1.9
WINS Server IP Address . . .
Name Lookup Priority ☐ WINS ☒ DNS
Retry DNS Connection (number of times)* 5

Help Skip > < Back Next > Close

Authentication:

Type: Local

User: deletethisuser2

Pass: <password>

Note: Because we are authenticating at the Web Interface, set this to Local authentication.

You are required to create a user, but you can delete it later.

Next.

Access Gateway Wizard

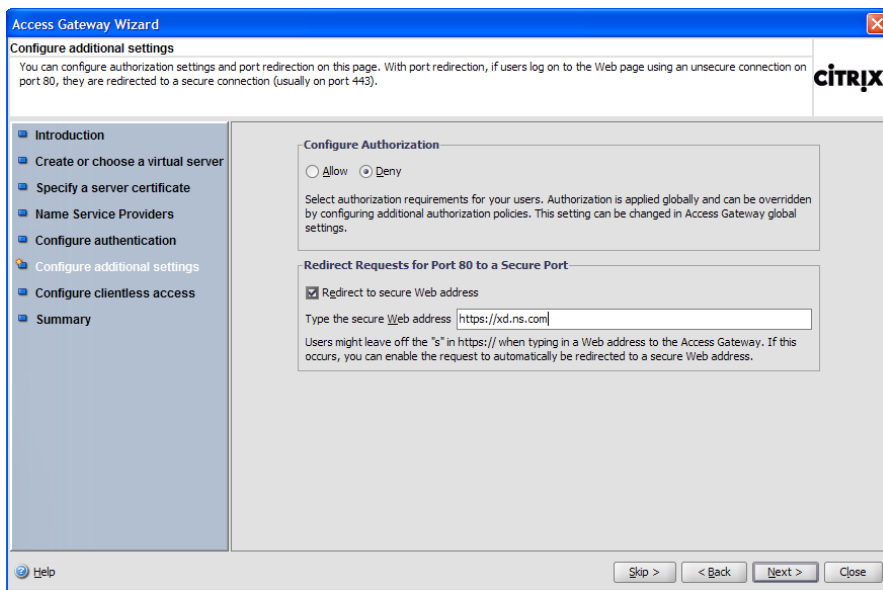
Configure authentication
Select the authentication type for your users. If you are using local authentication, create a user name and password. To create additional users, in the navigation pane, click Users.

Introduction
Create or choose a virtual server
Specify a server certificate
Name Service Providers
Configure authentication
Configure additional settings
Configure clientless access
Summary

Select an authentication type LOCAL

User Name* deletethisuser2
Password *

Help Skip > < Back Next > Close



Access Gateway Wizard

Configure additional settings

You can configure authorization settings and port redirection on this page. With port redirection, if users log on to the Web page using an insecure connection on port 80, they are redirected to a secure connection (usually on port 443).

Configure Authorization

☐ Allow ☒ Deny

Select authorization requirements for your users. Authorization is applied globally and can be overridden by configuring additional authorization policies. This setting can be changed in Access Gateway global settings.

Redirect Requests for Port 80 to a Secure Port

☒ Redirect to secure Web address

Type the secure Web address:

Users might leave off the "s" in https:// when typing in a Web address to the Access Gateway. If this occurs, you can enable the request to automatically be redirected to a secure Web address.

Navigation: Skip > < Back Next > Close

Additional:

Authorization: Deny

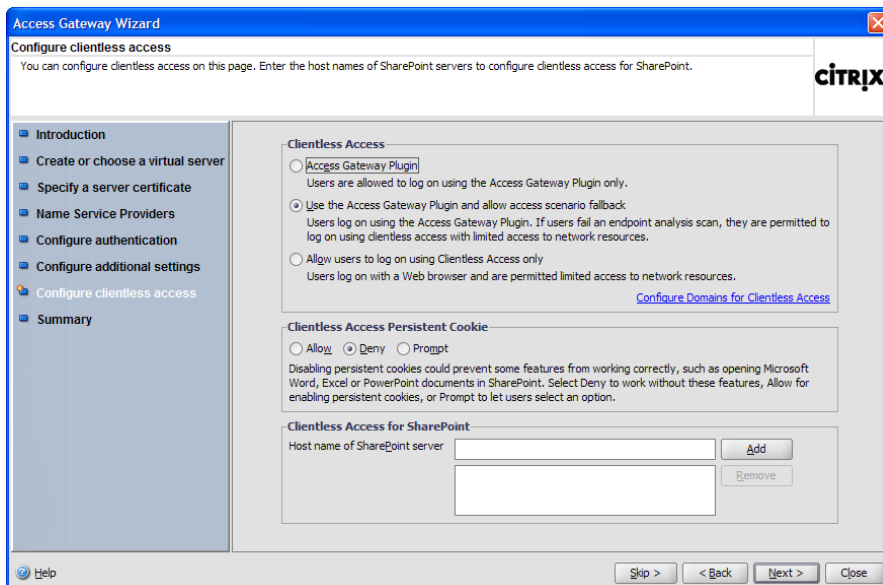
Redirect:

Redirect to secure web address

Address:

https://xd.ns.com

Next.



Access Gateway Wizard

Configure clientless access

You can configure clientless access on this page. Enter the host names of SharePoint servers to configure clientless access for SharePoint.

Clientless Access

☐ Access Gateway Plugin
Users are allowed to log on using the Access Gateway Plugin only.

☒ Use the Access Gateway Plugin and allow access scenario fallback
Users log on using the Access Gateway Plugin. If users fail an endpoint analysis scan, they are permitted to log on using clientless access with limited access to network resources.

☐ Allow users to log on using Clientless Access only
Users log on with a Web browser and are permitted limited access to network resources. [Configure Domains for Clientless Access](#)

Clientless Access Persistent Cookie

☐ Allow ☒ Deny ☐ Prompt

Disabling persistent cookies could prevent some features from working correctly, such as opening Microsoft Word, Excel or PowerPoint documents in SharePoint. Select Deny to work without these features, Allow for enabling persistent cookies, or Prompt to let users select an option.

Clientless Access for SharePoint

Host name of SharePoint server:

Navigation: Skip > < Back Next > Close

Clientless Access:

Use the Access Gateway Plugin and allow access scenario fallback.

Next.

Finish.

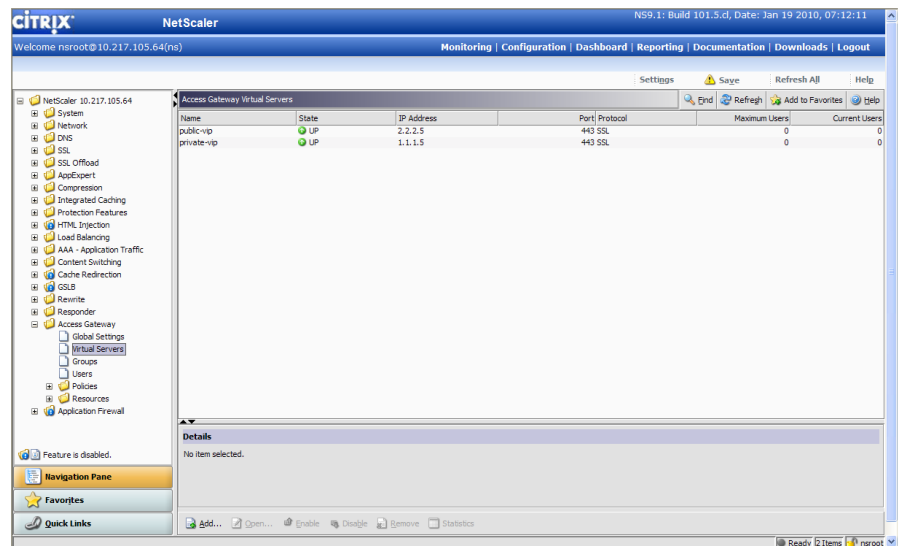
VIPs:

After configuring the Public VIP and Private VIP you should see them in the Access Gateway -> Virtual Servers in the NetScaler config GUI.

Public VIP: is used for client connections coming from outside the organization, or Internet.

Private VIP: is used for client connections coming from inside the organization, or Intranet.

The Server certificate should be bound to both the Public and Private VIPs.



From the NetScaler GUI:

NetScaler →

Access Gateway →

Policies →

Session →

Add.

Type in policy name, in this example `iphone_and_ipad`.

At Request Profile, select 'New' to create a new profile. In this example, the request profile is the same as the group name: `iphone_and_ipad`

Note: This session profile will be used to identify the Citrix Receiver sessions coming from the iPhone, iPod or iPad, and tunnel traffic accordingly.

Expression:

Configure the following expressions and select **Match All Expressions** as the operator for the expressions:

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver

REQ.HTTP.HEADER User-Agent CONTAINS CFNetwork

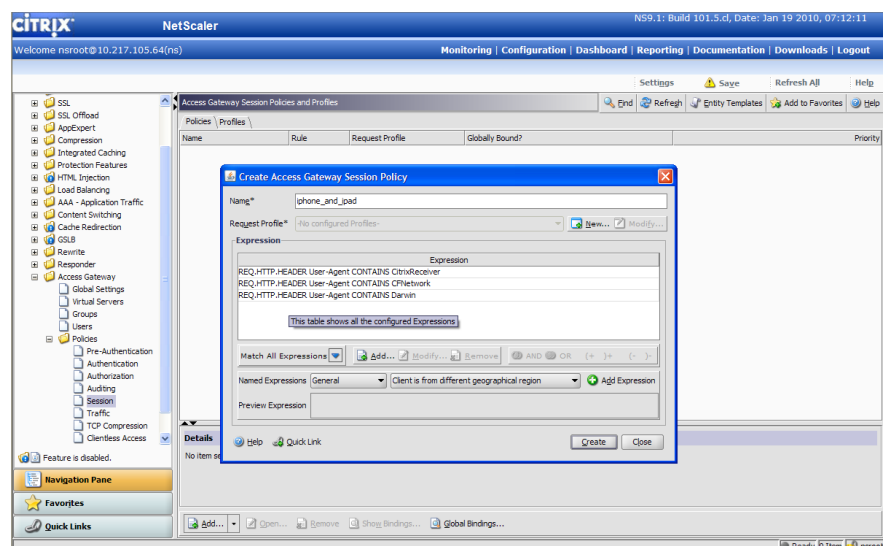
REQ.HTTP.HEADER User-Agent CONTAINS Darwin

Next to Request Profile, select 'New'.

NetScaler AGEE

Proxy Group, Session Profile

To proxy the ICA connections from the XenApp or XenDesktop server to the Citrix Receiver, the NetScaler AGEE needs to be configured to do so. You do this by creating a session profile.



Create Access Gateway Session Profile

Name*

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

Network Configuration Client Experience Security Published Applications

Override Global

| | | | |
|--|--|---|-------------------------------------|
| Home Page | <input type="text" value="rix/PNAgent2/config.xml"/> | <input checked="" type="checkbox"/> Display Home Page | <input checked="" type="checkbox"/> |
| URL for Web-Based Email | <input type="text"/> | | <input type="checkbox"/> |
| Split Tunnel | <input type="text" value="OFF"/> | | <input type="checkbox"/> |
| <input type="checkbox"/> Kill Existing Connections | | | <input type="checkbox"/> |
| Session Time-out (mins) | <input type="text" value="30"/> | | <input type="checkbox"/> |
| Client Idle Time-out (mins) | <input type="text"/> | | <input type="checkbox"/> |
| Clientless Access | <input type="text" value="Allow"/> | | <input checked="" type="checkbox"/> |
| Clientless Access URL Encoding | <input type="text" value="Obscure"/> | | <input type="checkbox"/> |
| Clientless Access Persistent Cookie | <input type="text" value="ALLOW"/> | | <input type="checkbox"/> |
| Plugin Type | <input type="text" value="Windows"/> | | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Single Sign-on to Web Applications | | | <input checked="" type="checkbox"/> |
| Credential Index | <input type="text" value="PRIMARY"/> | | <input type="checkbox"/> |
| <input type="checkbox"/> Single Sign-on with Windows | | | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Client Cleanup Prompt | | | <input type="checkbox"/> |

[Advanced](#)

Help Quick Link

Create Close

Client Experience:

Home Page: <http://1.1.1.3/Citrix/PNAgent2/config.xml>

Select Override Global.

Clientless Access: Allow.

Select Override Global.

Single Sign-on to Web Applications: Selected

Select Override Global.

Published Applications:

ICA Proxy:

On

Select Override Global

Web Interface Portal Mode:

Normal

Select Override Global

Select Create - to create the Session profile.

Then Create again - to create the Session policy.

Close.

Create Access Gateway Session Profile

Name*

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

Network Configuration \ Client Experience \ Security \ **Published Applications**

Override Global

| | | |
|---------------------------|-------------------------------------|-------------------------------------|
| ICA Proxy | <input type="text" value="ON"/> | <input checked="" type="checkbox"/> |
| Web Interface Address | <input type="text"/> | <input type="checkbox"/> |
| Web Interface Portal Mode | <input type="text" value="NORMAL"/> | <input checked="" type="checkbox"/> |
| Single Sign-on Domain | <input type="text"/> | <input type="checkbox"/> |
| Citrix Receiver Home Page | <input type="text"/> | <input type="checkbox"/> |

Help Quick Link

Create Close

Policy Binding: From the NetScaler GUI: NetScaler → Access Gateway → Virtual Servers.

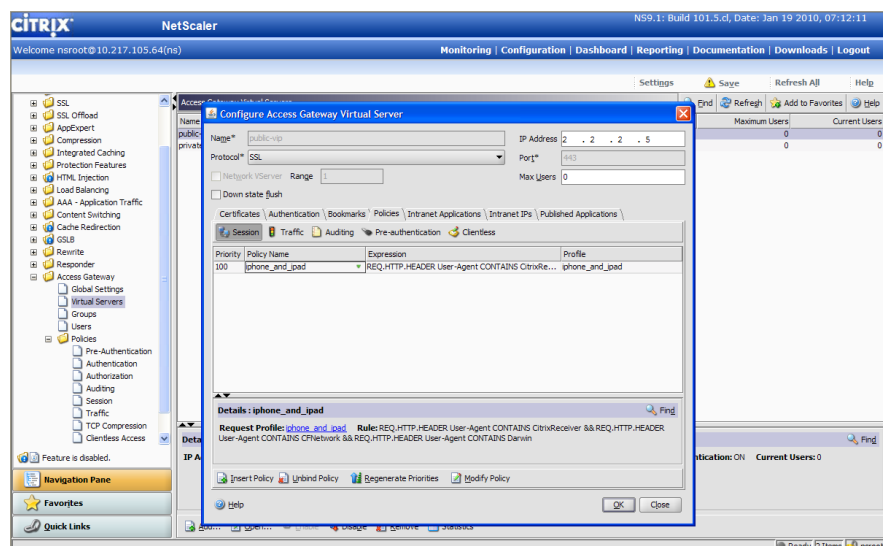
The iphone_and_ipad session policy should be bound to the public-vip and private-vip.

Open the public-vip and select the Policies tab.

Insert policy - select iphone_and_ipad.

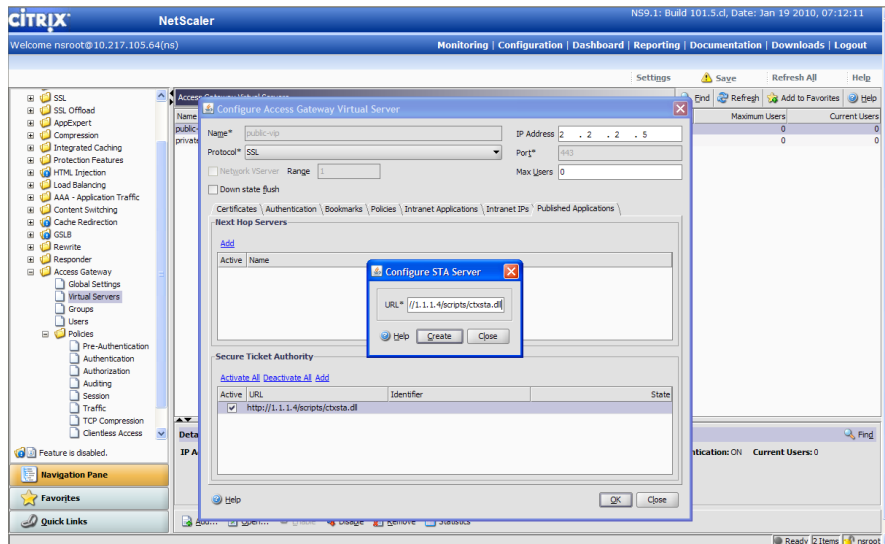
Select Ok.

Repeat this for the private-vip.



Secure Ticket Authority

Communication between the XenApp or XenDesktop server and the NetScaler AGEE depends on the Citrix Secure Ticket Authority. You must configure this in the NetScaler AGEE. In this case the CTX STA resides on a separate server.



From the NetScaler GUI:
NetScaler →
Access Gateway →
Virtual Servers.

Open the public vip. In this example it is public-vip at IP Address 2.2.2.5.

Select Published Applications.

Under Secure Ticket Authority, Add.

Enter the URL to the Secure Ticket Authority, in this example the same as the XenApp Server, `http://1.1.1.4/scripts/ctxsta.dll`

Create.

Ok.

Repeat this for the private-vip.

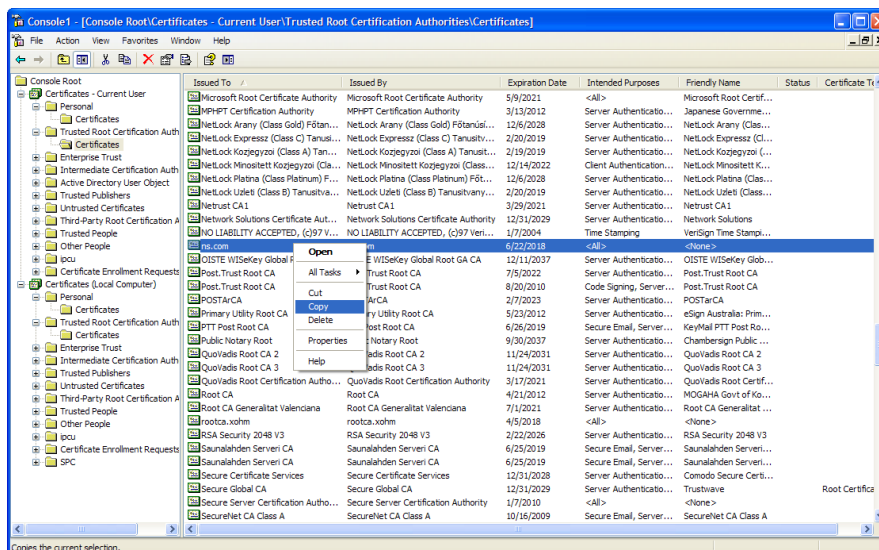
Testing Citrix Receiver

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 or a Desktop in XenDesktop, then connect with the Citrix Receiver.

Install AGEE Cert locally:

On a Windows PC, run the MMC and then add the certificate snap-in for the current user.

Copy the root certificate from the Trusted Root Authorities to the personal keystore (make sure to copy and not move).



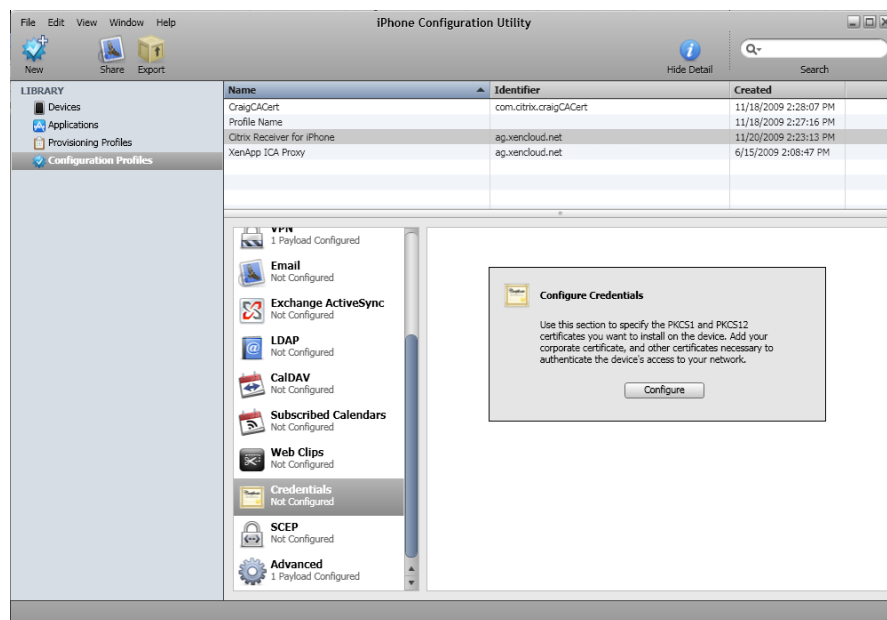
Download and Install the iPhone Configuration Utility:

Select Configuration Profiles.

Create a new Configuration Profile.

Fill out the General profile information.



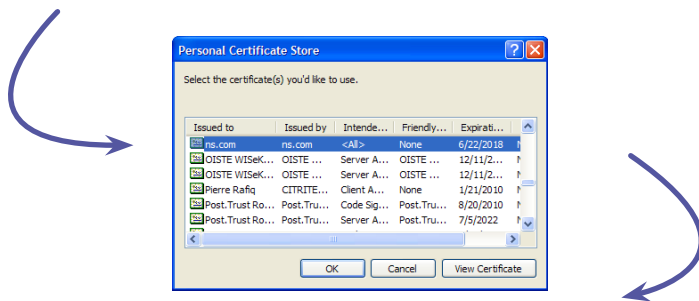


Credentials:

Select Credentials -> Configure.

Select the Root CA Certificate.

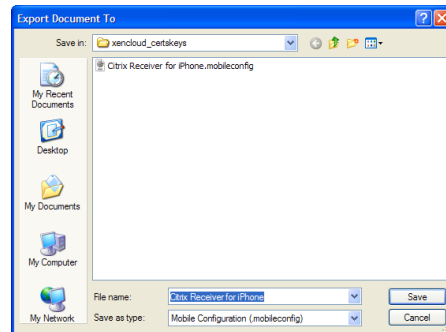
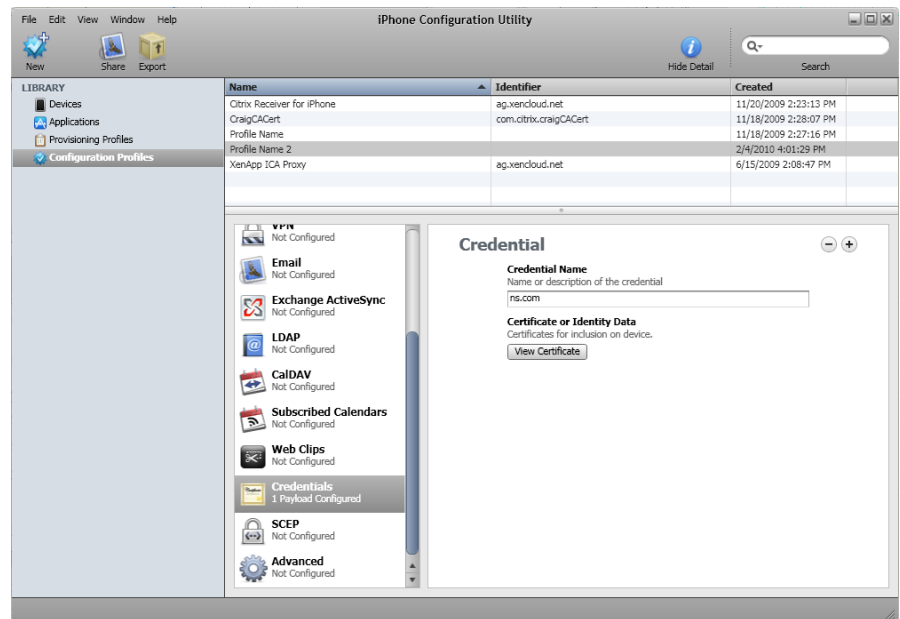
Note: If using an Intermediate Certificate, you should install the Root CA Certificate and the Intermediate Root CA Certificate.

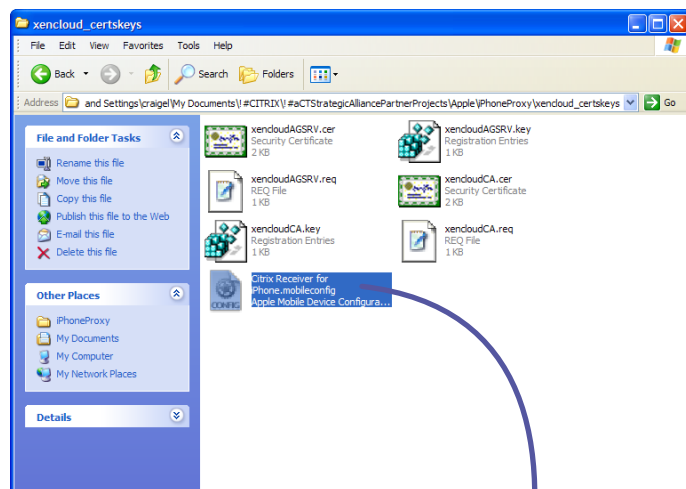


Export:

Select Export.

Save locally.





iPhone Certificate:

At this point you can:

1) eMail the profile to yourself, and open it with the iPhone.

or

2) eMail the Root CA Certificate to yourself, and open it with the iPhone.

or

3) Install it to your iPhone locally using iTunes.

In this example, we install the profile locally using iTunes



Install the Cert & Profile onto the iPhone:

In this example we emailed the cert to the iPhone, and installed it.

Note: If you purchased a certificate for an Certificate Authority, then you don't need to install any certificates in your iPhone, iPod or iPad.



Download the Citrix Receiver for iPhone:

Install and open iTunes by Apple. Navigate to the Apple Application Store, search, download and install the Citrix Receiver for iPhone.





Account Settings:

At this point you should see the Citrix Receiver on your iPhone.

Tap on it to open it, and configure with the gateway settings to the AGEE iPhone Proxy.

For this example:

Address: <https://xd.ns.com>

User: <username>

Pass: <password>

Domain: ns.com

Citrix Access Gateway:

Access Gateway:

On

Gateway Type:

Enterprise Edition

Gateway Authentication:

No Authentication

Apps:

Tap on Save. Tap on the save profile, and Citrix Receiver should login through the AGEE, and receive the Applications published on XenApp or a Desktop from XenDesktop.

Open the account:

Tap on the saved account settings and watch the magic of Citrix unfold.

Windows XP streamed to an iPhone



Windows 7 streamed to an iPad



**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.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

© 2009 Citrix Systems, Inc., 851 West Cypress Creek Road, Ft. Lauderdale, Florida 33309-2009 U.S.A. All rights reserved.